

SonicWall™ SonicOS 6.5 系统设置 管理

SONICWALL™

目录

关于设置您的 SonicOS 系统	13
关于 SonicOS 管理界面	13
配置基本设置	16
关于设备 基本设置	17
配置防火墙名称	18
更改管理员名称和密码	19
配置登录安全	19
配置多管理员访问	22
启用增强的审核记录支持	26
配置管理界面	26
配置前板管理界面（仅限 SuperMassive 防火墙）	31
配置客户端证书验证	32
检查证书过期	35
配置 SSH 管理	36
配置高级管理选项	36
手动下载 SonicPoint 镜像	38
选择语言	39
管理 SNMP	41
关于设备 SNMP	41
关于 SNMP	41
设置 SNMP 访问权限	42
将 SNMP 配置为服务并添加规则	50
关于 SNMP 日志	50
管理证书	51
关于证书	51
关于数字证书	51
关于证书和证书请求表	52
导入证书	54
删除证书	56
生成证书签名请求	56
配置简单证书注册协议	60
配置时间设置	62
关于设备 时间	62
设置系统时间	62
配置 NTP 设置	64
设置日程	66
关于日程	66

关于设备 日程	66
添加自定义日程	67
修改日程	68
删除自定义日程	69
关于管理用户	72
关于用户管理	72
使用本地用户和群组进行验证	73
使用 RADIUS 进行身份验证	76
使用 LDAP/Active Directory/eDirectory 验证	76
关于单点登录	80
安装单点登录代理和/或终端服务代理	90
关于多管理员支持	107
配置多管理员支持	108
配置用于管理用户的设置	111
用户 设置	111
配置用户验证和登录设置	112
配置用户会话	120
自定义	123
配置 RADIUS 身份验证	129
配置 SonicWall 以支持 LDAP	134
关于对多个 LDAP 服务器的扩展支持	140
关于从 LDAP 导入和镜像	141
关于增强版 LDAP 测试	143
配置 SonicOS 以使用 SonicWall SSO 代理	143
管理身份验证分区	165
关于身份验证分区	165
关于用户身份验证分区	166
关于子分区	167
关于分区间用户漫游	169
关于身份验证分区选择	170
关于对多个 LDAP 服务器的扩展支持	172
每个分区的 DNS 服务器和分割 DNS	172
关于 RADIUS 身份验证	172
从非分区配置升级	173
配置身份验证分区和策略	173
显示和过滤用户/分区	173
配置和管理分区	175
配置分区选择策略	186
配置进行身份验证分区的服务器、代理和客户端	189
配置本地用户和群组	191
配置本地用户	191

查看本地用户	192
添加本地用户	192
编辑本地用户	197
从 LDAP 导入本地用户	198
配置访客管理员	198
配置本地群组	199
创建或编辑本地群组	200
从 LDAP 导入本地群组	208
按 LDAP 位置设置用户成员身份	208
管理访客服务	209
用户 访客服务	209
全局访客设置	209
访客配置文件	210
管理访客帐户	213
用户 访客帐户	213
查看访客帐户统计	213
添加访客帐户	215
启用访客帐户	221
启用访客帐户自动删除	221
编辑访客帐户	221
删除访客帐户	221
打印帐户详细信息	222
配置接口	224
关于接口	225
物理和虚拟接口	225
SonicOS 安全对象	227
透明模式	228
IPS 探查器模式	228
Firewall Sandwich	230
HTTP/HTTPS 重定向	230
在接口上启用 DNS 代理	230
网络 接口	230
显示/隐藏 PortShield 接口（仅限 IPv4）	232
接口设置	233
接口流量统计	233
配置接口	234
配置静态接口	234
配置路由模式	239
在接口上启用带宽管理	241
配置透明 IP 模式下的接口（连接 L3 子网）	242
配置无线接口	245
配置 WAN 接口	248

配置隧道接口	252
配置链路聚合和端口冗余	255
配置虚拟接口 (VLAN 子接口)	259
配置 IPS 探查器模式	260
配置安全服务 (统一威胁管理)	263
配置有线和 Tap 模式	264
带有链路聚合的有线模式	267
二层桥接模式	267
配置二层桥接模式	283
非对称路由	290
配置 IPv6 接口	291
31 位网络	291
PPPoE 未编号接口支持	292
PortShield 配置接口	295
网络 PortShield 群组	295
关于 PortShield	295
X-系列交换机的 SonicOS 支持	296
管理端口	305
配置 PortShield 群组	313
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
网络 故障切换和负载均衡	321
配置故障切换和负载均衡组	324
配置群组成员的探测设置	327
配置网络区域	329
关于区域	329
区域的工作方式	330
预定义区域	330
安全类型	331
允许接口信任	331
对区域启用 SonicWall 安全服务	331
网络 区域	332
区域设置表	333
添加新区域	333
配置访客访问的区域	335
配置用于开放式验证和社交登录的区域	338
配置 WLAN 区域	338
删除区域	340
配置有线模式 VLAN 转换	341

网络 VLAN 转换	341
关于 VLAN 转换	341
创建和管理 VLAN 映射	342
配置 DNS 设置	349
网络 DNS	349
关于分割 DNS	351
管理 DNS 服务器	352
DNS 和 IPv6	357
DNS 和 IPv4	358
配置 DNS 代理设置	361
网络 > DNS 代理	362
关于 DNS 代理	363
启用 DNS 代理	365
配置 DNS 代理设置	367
监控 DNS 服务器状态	367
监控分割 DNS 服务器状态	368
查看和管理静态 DNS 缓存条目	369
查看 DNS 代理缓存条目	370
配置路由通告和路由策略	372
关于路由	372
关于度量和管理距离	373
路由通告	374
ECMP 路由	374
基于策略的路由	375
基于策略的 TOS 路由	375
基于 PBR 度量值的优先级	376
基于策略的路由和 IPv6	377
OSPF 和 RIP 高级路由服务	377
丢弃隧道接口	384
网络 路由	384
网络 路由 > 设置	384
网络 路由 > 路由策略	385
网络 路由 > 路由通告	386
网络 路由 > OSPFv2	387
网络 路由 > RIP	388
网络 路由 > OSPFv3	389
网络 路由 > RIPng	391
配置路由	392
按度量值设置路由的优先级	392
为通过路由公告学习的默认路由配置度量值	393
配置路由通告	393
配置静态和基于策略的路由	394

为丢弃隧道接口配置静态路由	397
配置 OSPF 和 RIP 高级路由服务	399
配置 BGP 高级路由	408
管理 ARP 流量	409
网络 ARP	409
静态 ARP 条目	410
ARP 设置	413
ARP 缓存	414
配置邻居发现协议	415
网络 邻居发现（仅 IPv6）	415
静态 NDP 条目	416
NDP 设置	417
NDP 缓存	417
配置静态 NDP 条目	418
编辑静态 NDP 条目	418
清除 NDP 缓存	419
配置 MAC-IP 反欺骗	420
关于 MAC-IP 反欺骗保护	420
IP 助手扩展	421
网络 MAC-IP 反欺骗	421
接口设置	422
反欺骗缓存	423
检测到的反欺骗列表	425
配置 MAC-IP 反欺骗保护	425
显示流量统计信息	426
编辑 IPv6 接口的 MAC-IP 反欺骗设置	426
编辑 IPv4 接口的 MAC-IP 反欺骗设置	427
将设备添加到反欺骗缓存中	429
删除反欺骗缓存条目	429
过滤所显示的内容	430
从检测到的欺骗列表中添加静态条目	431
设置 DHCP 服务器	432
网络 DHCP 服务器	432
DHCP 服务器选项功能	434
每个接口上的多个 DHCP 作用域	435
关于 DHCP 服务器的持续性	437
配置 DHCP 服务器	437
DHCP 服务器租用范围	439
当前 DHCP 租用	439
配置高级选项	441
配置高级 DHCP 服务器选项	441

配置用于动态范围的 DHCP 服务器	446
配置静态 DHCP 条目	451
配置用于 DHCP 租用范围的 DHCP 常规选项	453
RFC 定义的 DHCP 选项编号	453
DHCP 和 IPv6	459
使用 IP 助手	460
关于 IP 助手	460
IP 助手的 VPN 隧道接口支持	461
网络 > IP 助手	462
中继协议	463
策略	464
DHCP 中继租赁	464
配置 IP 助手	465
启用 IP 助手	465
管理中继协议	465
管理 IP 助手策略	467
过滤所显示的 DHCP 中继租约	469
通过 TSR 显示 IP 助手缓存	469
设置 Web 代理转发	471
网络 Web 代理	471
配置自动代理转发（仅用于 Web）	472
配置用户代理服务器	473
配置动态 DNS	475
网络 动态 DNS	475
关于动态 DNS	475
支持的 DDNS 提供商	476
动态 DNS 配置文件表	476
配置动态 DNS 配置文件	478
编辑 DDNS 配置文件	480
删除 DDNS 配置文件	480
关于交换	483
关于交换	483
什么是交换？	483
交换的优点	484
交换的工作原理	484
术语	485
配置 VLAN 中继	486
交换 VLAN 中继	487
关于中继	488
查看 VLAN	488
编辑 VLAN	490

添加 VLAN 中继端口	490
启用中继端口上的 VLAN	491
删除 VLAN 中继端口	491
查看第 2 层发现	493
交换 L2 发现	493
查看 L2 发现	493
激活 L2 发现	494
配置链路聚合	496
交换 链路聚合	496
关于链路聚合	496
查看链路聚合	498
创建逻辑链路 (LAG)	499
删除 LAG	500
配置端口镜像	501
交换 端口镜像	501
关于端口镜像	501
查看被镜像端口	502
配置端口镜像群组	502
启用被镜像组	503
编辑端口镜像群组	503
删除端口镜像群组	504
关于高可用性和 Active/Active 集群	508
高可用性	508
关于高可用性	509
关于 Active/Standby HA	513
关于状态同步	514
关于 Active/Active DPI HA	515
Active/Standby 和 Active/Active DPI 前提条件	516
维护	519
Active/Active 集群	521
关于 Active/Active 集群	521
配置高可用性	534
高可用性 基本设置	534
配置 Active/Standby 高可用性设置	535
配置动态 WAN 接口的高可用性	536
配置 Active/Active DPI 高可用性设置	538
配置 Active/Active 集群	539
验证 Active/Active 集群配置	546
IPv6 高可用性监控	547
配置网络 DHCP 和接口设置	548
Active/Active 集群全网格	550

微调高可用性	556
高可用性 高级设置	556
配置高级高可用性	556
监控高可用性	559
高可用性 监控设置	559
配置 Active/Standby 高可用性监控	560
使用 WAN 加速	563
关于 WAN 加速	563
支持的平台	564
传输控制协议加速	564
Windows 文件共享加速	564
Web 缓存	565
部署 WAN 加速服务的前提条件	565
关于 WXA 集群	566
WXA 集群的工作原理是什么?	567
允许对路由策略加速	568
系统设置 > WAN 加速	569
启用 WAN 加速	569
管理群组	570
通过 WXA 表来管理 WXA	574
配置 VPN 策略的 WXA	589
配置 SSL VPN 流量加速	590
显示和编辑 WXA 的路由策略	590
监控群组连接	591
关于 VoIP	594
关于 VoIP	594
什么是 VoIP?	594
VoIP 安全性	594
VoIP 协议	595
SonicWall 的 VoIP 功能	596
配置 SonicWall VoIP 功能	604
配置任务	604
配置 VoIP	604
配置 VoIP 日志	609
配置虚拟助手	611
关于虚拟助手	611
最大限度提高虚拟助手灵活性	611
配置虚拟助手	613
配置开放式验证、社交登录和 LHM	619
关于开放式验证和社交登录	619

什么是 OAuth 和社交登录?	620
OAuth 和社交登录的好处	620
OAuth 和社交登录如何工作?	621
支持的平台	622
开发和生产要求	622
关于轻量级热点新闻 (LHM)	623
配置 Facebook 进行社交登录	624
Facebook 设置	625
客户端 OAuth 设置	626
访客状态 (演示)	626
配置开放式验证和社交登录	626
关于配置访客服务	626
关于配置社交登录	626
在 SonicOS 中配置社交登录	627
验证社交登录配置	628
使用社交登录、LHM 和 ABE	628
关于 ABE	628
会话生命周期	629
会话更新	635
消息格式	635
常见问题解答 (FAQ)	642
LHM 脚本库	648
IPv6	762
IPv6	762
关于 IPv6	762
配置 IPv6	767
IPv6 可视化	789
IPv6 高可用性监控	789
IPv6 诊断和监控	790
BGP 高级路由	792
BGP 高级路由	792
关于 BGP	792
注意	799
配置 BGP	799
验证 BGP 配置	809
IPv6 BGP	812
SonicWall 支持	834
关于本文档	835

关于系统设置

- 关于设置您的 SonicOS 系统

关于设置您的 SonicOS 系统

- 第 13 页的[关于 SonicOS 管理界面](#)

关于 SonicOS 管理界面

通过基于 Web 的 SonicOS 管理界面，您可以配置运行 SonicOS 6.5 的 SonicWall 网络安全设备（防火墙）：

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 2650		
	NSA 2600		

i | 注：本文档可能包含在某些国家或地区未发布的平台/版本的说明。

SonicOS 提供了一个易于使用的图形化管理界面来配置您的 SonicWall 安全设备。如需动态管理界面及其功能（如工具提示和动态表）的信息，请参阅关于 SonicOS 指南。

本指南提供了有关配置下列内容的说明：

- 密码、登录安全、Web 管理、证书和日程。
- 用户身份验证、群组、访客服务和帐户以及分区。
- 网络设置，如接口、区域和路由。
- VLAN 中继的交换设置、L2 发现、链路聚合和端口镜像。
- 高可用性。
- WAN 加速。
- VOIP
- 虚拟助手

如需配置以下内容的信息

连接：VPN、SSL VPN、SonicPoint/SonicWave、无线

策略：访问规则、NAT 策略以及所有对象，如地址、机器和带宽
许可证、更新固件以及支持/重启您的系统

监控：公告板、威胁防护、流量、捕获 ATP

请参阅

SonicOS 连接

SonicOS 策略

SonicOS 更新

SonicOS 监控

如需配置以下内容的信息

请参阅

安全：安全设备设置、安全服务、反垃圾邮件、深层数据包检查 (DPI) SonicOS 安全配置

日志和报告：AppFlow 设置、日志、合法 SonicOS 日志和报告

快速配置 SonicOS 快速配置

- 配置基本设置
- 管理 SNMP
- 管理证书
- 配置时间设置
- 设置日程

配置基本设置

- 第 17 页的[关于设备 | 基本设置](#)
 - 第 18 页的[配置防火墙名称](#)
 - 第 19 页的[更改管理员名称和密码](#)
 - 第 19 页的[配置登录安全](#)
 - 第 22 页的[配置多管理员访问](#)
 - 第 26 页的[启用增强的审核记录支持](#)
 - 第 26 页的[配置管理界面](#)
 - 第 31 页的[配置前板管理界面（仅限 SuperMassive 防火墙）](#)
 - 第 32 页的[配置客户端证书验证](#)
 - 第 35 页的[检查证书过期](#)
 - 第 36 页的[配置 SSH 管理](#)
 - 第 36 页的[配置高级管理选项](#)
 - 第 38 页的[手动下载 SonicPoint 镜像](#)
 - 第 39 页的[选择语言](#)

关于设备 | 基本设置

管理 | 系统设置 | 设备 | 基本设置提供用于配置 SonicWall 安全设备进行安全和远程管理的设置。

防火墙名称

防火墙名称：

自动追加 HA/Clustering 后缀到防火墙名称

防火墙域名：

管理员名称 & 密码

管理员名称：

旧密码：

新密码：

确认密码：

登录安全

修改密码的间隔天数为：

自上次更改以来，不能在以下时间（小时）内更改密码：

在限定次数内不能使用重复密码：

新密码必须有 8 个字符和旧密码不一样

限定最短密码长度：

限定密码复杂度：

复杂度需求

大写字符：

小写字符：

数字：

符号：

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

注：如需将所有更改应用于 SonicWall 设备，请单击**接受**；浏览器窗口底部会显示一条确认更新的消息。

访问设备 | 基本设置页面：

- 1 通过单击**管理**来显示**管理视图**。
- 2 在**系统设置**下，单击**设备**以展开导航窗格。
- 3 单击**基本设置**。

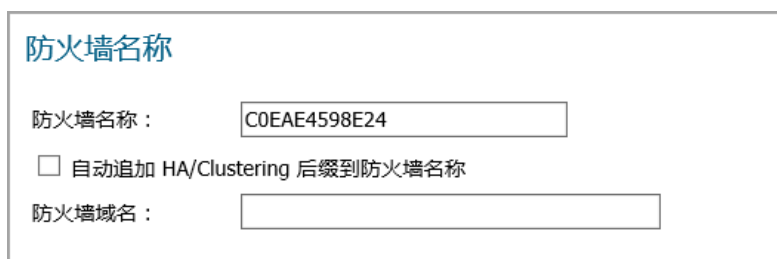
主题：

- 第 18 页的[配置防火墙名称](#)
- 第 19 页的[更改管理员名称和密码](#)
- 第 19 页的[配置登录安全](#)
- 第 22 页的[配置多管理员访问](#)
- 第 26 页的[启用增强的审核记录支持](#)
- 第 26 页的[配置管理界面](#)
- 第 31 页的[配置前板管理界面（仅限 SuperMassive 防火墙）](#)
- 第 32 页的[配置客户端证书验证](#)
- 第 35 页的[检查证书过期](#)
- 第 36 页的[配置 SSH 管理](#)
- 第 36 页的[配置高级管理选项](#)
- 第 38 页的[手动下载 SonicPoint 镜像](#)
- 第 39 页的[选择语言](#)

配置防火墙名称

配置防火墙名称的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 防火墙名称。



防火墙名称

防火墙名称：

自动追加 HA/Clustering 后缀到防火墙名称

防火墙域名：

- 2 在防火墙名称字段中输入防火墙的十六进制序列号。此序列号用于唯一标识 SonicWall 安全设备且默认为防火墙的序列号。该序列号也是设备的 MAC 地址。如需更改防火墙名称，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。
- 3 为便于识别事件日志中的主要/次要防火墙，请选中**自动追加 HA/Clustering 后缀到防火墙名称**。启用此选项后，系统会在调查视图的日志 > 事件日志中自动添加适当的后缀到防火墙名称：
 - 主要
 - 备用
 - 主要节点 <nodeNumber>
 - 次要节点 <nodeNumber>

默认情况下未选中该选项。如需事件日志的更多信息，请参阅 [SonicOS 调查](#)。

- 4 在防火墙域名中输入一个好记的名称。此名称可以是供内部用户使用的专用名称或外部注册的域名。此域名与系统设置 | 用户 > 设置视图上的用户 Web 登录设置一起用于用户身份验证重定向。如需用户 Web 登录设置的更多信息，请参阅第 XXX 页的配置用户 Web 登录设置。

更改管理员名称和密码

每个 SonicWall 安全设备都具有默认管理员名称 admin 和密码 password。如果未通过“初始设置指南”、“初始启动指南”或“设置快速配置指南”更改密码，则强烈建议您立即执行此操作。审校问题：是否可以更改管理员名称？

更改管理员名称和/或密码的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 管理员名称 & 密码。

管理员名称 & 密码

管理员名称：

旧密码：

新密码：

确认密码：

- 2 在管理员名称字段中输入新的名称。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符串。
- 3 单击接受。

设置用于访问 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。新密码最多可以包含 32 个字母数字和特殊字符。

重要： 建议将默认密码 password 更改为您自己的自定义密码。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 在确认密码字段中再次输入新密码。
- 4 单击接受。

配置登录安全

在协商 HTTPS 管理会话时，内部 SonicOS Web 服务器支持 TLS 1.1 及更高版本和强密码（128 位或更高）。不支持 SSL 实施。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。SonicWall 推荐使用最新版本的 Chrome、Firefox、Internet Explorer 或 Safari（无法在 Windows 平台上运行）浏览器管理 SonicOS。不建议使用移动设备浏览器进行 SonicWall 系统管理。

配置 SonicOS 密码限制强制措施可确保管理员和用户使用安全密码。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。

登录安全

修改密码的间隔天数为：

自上次更改以来，不能在以下时间（小时）内更改密码：

在限定次数内不能使用重复密码：

新密码必须有 8 个字符和旧密码不一样

限定最短密码长度：

限定密码复杂度：

复杂度需求

大写字符：

小写字符：

数字：

符号：

以上密码限制的应用对象为：
 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
 系统管理员 Crypto 管理员 审核管理员

注销不活动管理员时间（分钟数）：

启用管理员/用户锁定

锁定前失败的登录尝试次数 每 分钟

锁定期限（分钟）（0 表示永久锁定）：

通过 CLI 的最多登录尝试次数：

主题：

- 第 20 页的 [配置密码合规性](#)
- 第 22 页的 [配置登录限制](#)

配置密码合规性

配置密码合规性的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 登录安全。

修改密码的间隔天数为：

自上次更改以来，不能在以下时间（小时）内更改密码：

在限定次数内不能使用重复密码：

新密码必须有 8 个字符和旧密码不一样

限定最短密码长度：

限定密码复杂度：

复杂度需求

大写字符：

小写字符：

数字：

符号：

以上密码限制的应用对象为：
 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

- 2 要求用户在经过指定的天数后更改其密码的步骤如下：

- a 选中修改密码的间隔天数为。将激活该字段。默认情况下未选中该选项。
- b 在此字段中输入经过的时间。默认天数为 90，最小值为 1 天，最大值为 9999。

当用户尝试使用已过期的密码登录时，系统会显示一个弹出窗口，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，以使用户随时更改其密码。

- 3 指定两次密码更改之间允许的最小时间长度（小时）的步骤如下：
 - a 选中自上次更改以来，不能在以下时间（小时）内更改密码。将激活该字段。默认情况下未选中该选项。
 - b 输入小时数。最短时间（默认值）为 **1** 小时；最长时间为 9999 小时。
- 4 要求用户在指定的密码更改次数内必须使用唯一密码的步骤如下：
 - a 选中在限定次数内不能使用重复密码。此字段将激活。默认情况下未选中该选项。
 - b 输入更改次数。默认次数为 **4**，最小次数为 **1**，最大次数为 **32**。
- 5 如要求用户在创建新密码时至少更改旧密码中的 **8** 个字母数字/符号字符，请选中**新密码必须有 8 个字符和旧密码不一样**。如需了解指定允许使用的字符的方法，请参阅**步骤 7**。
- 6 指定允许的最短密码，在**限定最短密码长度**字段中输入最少字符数。默认值为 **8**，最小值为 **1**，最大值为 **99**。
- 7 从**限定密码复杂度**下拉菜单中选择用户密码必须采用的可接受复杂程度：
 - 无（默认）
 - 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
- 8 选择了无以外的密码复杂度选项时，**复杂度需求**下的选项将激活。输入用户密码中所需的最少字母数字和符号字符数。每个选项的默认数量为 **0**，但是所有选项的总字符数不得超过 **99**。
 - 大写字符
 - 小写字符
 - 数字
 - 符号

① | 注：只有在选中**必须有字母、数字和符号字符**时，**符号字符**字段才会激活。
- 9 在以上密码限制的应用对象为下选择对哪些用户类别应用密码限制。默认情况下，所有选项都处于选中状态：
 - 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

配置登录限制

配置登录限制的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 登录安全。

注销不活动管理员时间（分钟数）：	<input type="text" value="300"/>
<input type="checkbox"/> 启用管理员/用户锁定	
锁定前失败的登录尝试次数 <input type="text" value="5"/> 每 <input type="text" value="1"/> 分钟	
锁定期限（分钟）（0 表示永久锁定）：	<input type="text" value="5"/>
通过 CLI 的最多登录尝试次数：	<input type="text" value="5"/>

- 2 如需指定在您自动从管理界面中注销之前经过的不活动时间长度，请在注销不活动管理员时间（分钟数）字段中输入时间（分钟）。默认情况下，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。

i 提示：如果管理员不活动超时超过了五分钟，您应该通过单击视图右上角的注销来结束每个管理会话，以防止出现对防火墙管理界面进行未授权访问的情况。

- 3 如需将 SonicWall 安全设备配置为在登录凭据错误时锁定管理员或用户，请选中启用管理员/用户锁定。在指定的错误登录尝试次数后，管理员和用户都已锁定，而无法访问防火墙。默认已禁用该选项。启用此选项后，以下字段将激活。

△ 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。

- a 在第一个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指定期限内的失败尝试次数。默认次数为 5，最小值为 1，最大值为 99。
 - b 输入可以进行失败尝试的最长时间。默认值为 5 分钟，最小值为 1 分钟，最大值为 240 分钟（4 小时）
 - c 在锁定期限（分钟）字段中，输入允许用户再次尝试登录防火墙之前必须经过的时间长度。默认值为 5 分钟，最小值为 0 分钟（永久锁定），最大值为 60 分钟。
- 4 在通过 CLI 的最多登录尝试次数字段中，输入在触发锁定前能够从命令行接口 (CLI) 进行的错误登录尝试次数。默认值为 5，最小值为 3，最大值为 15。
 - 5 单击接受。

配置多管理员访问

SonicOS 支持拥有完全管理员权限、只读权限和受限制权限的多个并发管理员。

主题：

- 第 23 页的[关于多管理员支持](#)
- 第 25 页的[配置多管理员访问](#)

关于多管理员支持

主题：

- 第 23 页的[什么是多管理员支持？](#)
- 第 23 页的[优点](#)
- 第 23 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

多管理员支持有以下优点：

- | | |
|--------|---|
| 提高生产力 | 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

主题：

- 第 23 页的[配置模式](#)
- 第 24 页的[用户群组](#)
- 第 25 页的[抢占管理员的优先级](#)
- 第 25 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 | 管理员具有编辑配置的完全权限。如果无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界面（CLI，请参阅 SonicOS 6.5 CLI 参考指南）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。
只有属于 SonicWall 只读管理员 用户群组的管理员才授予只读访问权限，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 管理员** 用户群组的管理人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。

配置模式可获得的访问权限 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。

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 管理员

该群组的成员具有编辑配置的完全管理员权限。

SonicWall 只读管理员

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，则以下行为适用：

如果此用户群组的成员	是
SonicWall 管理员	也包含在限制的管理员或 SonicWall 只读管理员用户群组中，则成员将具有完全管理员权限。
限制的管理员	包含在 SonicWall 只读管理员用户群组中，则成员将具有受限制的管理员权限。
只读管理员	稍后包含在其他管理群组中，则 SonicWall 只读管理员群组配置中的如果此只读管理员群组与其他管理群组一起使用选项将确定这些成员仍然限制为只读访问权限还是具有其他群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) 都具有最高优先级，且可以抢占任何用户。
- 2 除了管理员和 SonicWall GMS 之外，属于 **SonicWall 管理员** 用户群组的用户可以优先于任何用户。
- 3 属于限制的**管理员**用户群组的用户仅优先于限制的**管理员**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。

配置多管理员访问

配置多管理员访问的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 多个管理员。

多管理员

其它管理员抢占：

允许低优先级的管理员抢占，当不活动（分钟数）：

启用管理员内部通信

启用多个管理角色

转入非配置模式 注销

消息轮询频率（秒数）：

- 2 如需配置一个管理员抢占另一个管理员时发生的情况，请从**其他管理员抢占**选项中选择可以将被抢占的管理员转换到非配置模式还是注销：

如需允许	选择
多个管理员在非配置模式下访问设备，而不干扰其他管理员。默认情况下未选中该选项。	转入非配置模式
新管理员抢占其他会话。	注销

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。

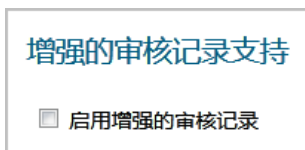
- 3 如需允许优先级较低的管理员在指定时间后抢占当前管理员，请在**允许低优先级的管理员抢占，当不活动（分钟数）**字段中输入时间（分钟）。默认值为**10**分钟，最小值为**1**分钟，最大值为**9999**分钟。
- 4 借助 SonicOS 管理界面，管理员可以通过管理界面向其他已登录设备的管理员发送文本消息。该消息将显示在浏览器的状态栏中。默认情况下未选中该选项。启用此选项的步骤如下：
 - a 选中**启用管理员内部通信**。**消息轮询频率（秒数）**字段将激活。
 - b 在**消息轮询频率（秒数）**字段中，指定管理员的浏览器检查管理员内部消息的频率。指定合理的较短间隔以确保及时传输消息，尤其在可能有多个需要访问此设备的管理员时。默认值为**10**秒，最小值为**1**秒，最大值为**99**秒。
- 5 如需由系统管理员、加密 (Crypto) 管理员和审核管理员启用访问，请选中**启用多个管理角色**。禁用此选项后，这些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。默认情况下未选中该选项。

启用增强的审核记录支持

在**调查 | 日志 > 事件日志**页面中，增强的日志条目包含已更改的参数和用户名。如需日志的更多信息，请参阅 [SonicOS 调查](#)。

在**调查 | 日志 > 事件日志**页面中启用对所有配置更改的记录步骤如下：

- 1 在**管理视图**中，转至**系统设置 | 设备 | 基本设置 | 增强的审核记录支持**。



- 2 选中**启用增强的审核记录**。默认情况下未选中该选项。
- 3 单击**接受**。

配置管理界面

在此部分中，可以配置：

- 管理界面表的显示方式。
- 证书使用情况。
- 哪个页面显示为起始页面。
- 在配置模式还是在非配置模式下运行。
- 工具提示行为。
- 其他管理选项。

Web 管理设置

允许通过 HTTP 管理

HTTP 端口:

删除 COOKIES

HTTPS 端口:

结束配置模式

证书选择: ▾

证书公用名:

重新生成证书

默认表大小: 条每页 ▾

自动更新表单的刷新间隔: 秒 ▾

使用威胁保护视图作为起始页

启用提示

表单提示延迟: 毫秒

按钮提示延迟: 毫秒

文本提示延迟: 毫秒

强制 TLS 1.1 及以上版本

主题:

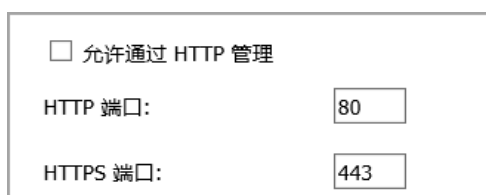
- [第 27 页的通过 HTTP/HTTPS 进行管理](#)
- [第 28 页的删除浏览器 Cookie](#)
- [第 28 页的切换配置模式](#)
- [第 28 页的切换配置模式](#)
- [第 30 页的控制管理界面表](#)
- [第 30 页的指定起始页面](#)
- [第 31 页的管理工具提示](#)
- [第 31 页的强制 TLS 版本](#)

通过 HTTP/HTTPS 进行管理

可以使用 HTTP 或 HTTPS 和 Web 浏览器来管理 SonicWall 安全设备。默认已禁用基于 Web 的 HTTP 管理。使用 HTTPS 登录包含出厂默认设置的 SonicOS 管理界面。

通过 HTTP 或 HTTPS 进行管理的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。



允许通过 HTTP 管理

HTTP 端口:

HTTPS 端口:

- 2 如需全局启用 HTTP 管理，请选中允许通过 HTTP 管理。默认情况下未选中该选项。
- 3 HTTP 的默认端口为端口 **80**，也可以配置通过其他端口访问。在 HTTP 端口字段中输入所需端口号。
i **重要：** 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，您必须在 Web 浏览器中输入 LAN IP 地址:76，例如 `http://192.18.16.1:76`。
- 4 用于 HTTPS 管理的默认端口为 **443**。如需通过更改默认端口来添加用于登录 SonicWall 安全设备的另一个安全层，请在 HTTPS 端口字段中输入首选端口号。
i **重要：** 如果配置了另一个端口作为 HTTPS 管理端口，您必须在使用 IP 地址登录 SonicWall 安全设备时包含该端口号。例如，如果将 700 用于端口，您必须使用该端口号及 IP 地址登录 SonicWall；例如，`https://192.18.16.1:700`。

删除浏览器 Cookie

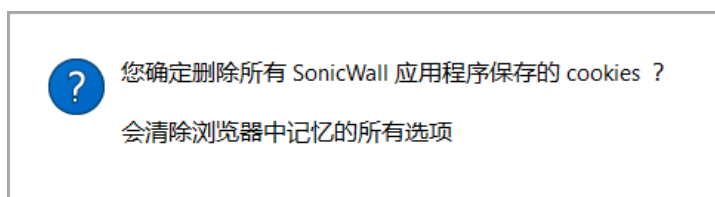
- i** **重要：** 删除 cookie 将导致您丢失在管理界面中执行的所有未保存更改。

删除由安全设备保存的所有浏览器 cookie 的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。



- 2 单击删除 Cookie。将显示确认消息。



- 3 单击确定。将删除自上次您删除 cookie 后保存的所有 cookie。

切换配置模式

每台设备都包含一个模式选项，用于切换管理界面的配置模式。如果处于配置模式，您可以随时切换到非配置模式。如果处于非配置模式，您可以切换到配置模式。

- i** **提示：** 此方法是除了从每个视图模式设置切换模式之外的附加方法。如需模式的更多信息，请参阅[关于 SonicOS 指南](#)。

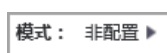
切换模式的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。
- 2 如果

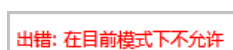
- 您处于配置模式，单击结束配置模式。该按钮将更改为：



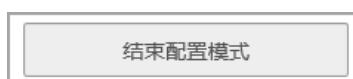
页面右上方的模式指示器显示非配置模式：



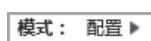
如果您尝试在任何视图中保存任何更改，将显示一条错误消息：



- 如果您处于非配置模式，单击配置模式。该按钮将更改为：



页面右上方的模式指示器显示配置：



无需单击接受。

- 3 要返回
 - 配置模式，请单击配置模式。
 - 要返回非配置模式，请单击结束配置模式。

选择安全证书

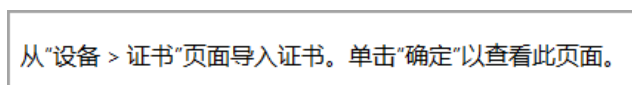
安全证书提供数据加密和安全的网站。

指定安全证书类型的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。

证书选择：	<input type="text" value="使用自签名证书"/>	
证书公用名：	<input type="text" value="192.168.168.168"/>	<input type="button" value="重新生成证书"/>

- 2 从证书选择下拉菜单中，为网站选择证书类型：
 - 使用自签名证书，允许您继续使用证书，而无需在每次登录 SonicWall 安全设备时下载新证书。默认情况下已选中该选项。转至步骤 3。
 - 导入证书，以便从设备 > 证书页面中选择一个已导入的证书，用于向管理界面进行身份验证。将显示确认消息：



- a) 单击确定。随即显示设备 > 证书页面。

b) 转至设备证书。

- 3 在证书公用名字段中，输入防火墙的 IP 地址或公用名。如果选择使用自签名证书，则 SonicOS 将使用防火墙的 IP 地址填写此字段。
- 4 单击接受。

重新生成自签名证书的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。
- 2 单击重新生成证书。将显示确认消息：

是否重新生成自签名 HTTPS 服务器证书？

- 3 单击确定。

控制管理界面表

借助 SonicWall 管理界面，您可更改以下内容来控制管理界面中所有表之间大型信息表的显示：

- 页面上显示的表条目数。
- 表的背景自动刷新频率。

一些表有单独的每页条目数设置，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。

更改表的显示和刷新的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。

默认表大小：	<input type="text" value="50"/>	条每页 `
自动更新表单的刷新间隔：	<input type="text" value="10"/>	秒 `

- 2 在默认表大小字段中输入需要的条每页。最小值为 1，最大值为 5000，默认值为 50。
- 3 在自动更新表单的刷新间隔字段中输入所需的刷新间隔（秒）。最小值为 1 秒，最大值为 300 秒，默认值为 10 秒。
- 4 单击接受。

指定起始页面

在您登录管理界面时，系统会显示您从管理界面注销时的视图。可以改为显示系统公告板视图。

在登录时首先看到监控 | 公告板页面的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。

<input type="checkbox"/> 使用威胁保护视图作为起始页
--

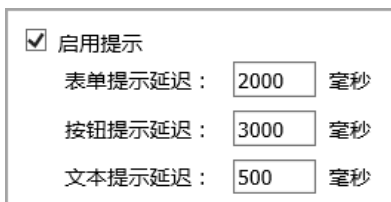
- 2 选中使用威胁保护视图作为起始页。
- 3 单击接受。在您下次登录时，将显示“监控公告板”页面，而与注销时显示的视图无关。

管理工具提示

SonicOS 管理界面嵌入了很多元素的工具提示。如需工具提示的更多信息，请参阅关于 SonicOS。

配置工具提示行为的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。



<input checked="" type="checkbox"/> 启用提示
表单提示延迟： <input type="text" value="2000"/> 毫秒
按钮提示延迟： <input type="text" value="3000"/> 毫秒
文本提示延迟： <input type="text" value="500"/> 毫秒

- 2 如需启用工具提示，请选中启用提示。

i | 提示：默认已启用工具提示。如需禁用工具提示，请清除启用提示复选框。

- 3 如需配置显示工具提示之前的延迟（毫秒），请输入适当的时间：

在这个字段中	输入以下项的延迟
表单提示延迟	字段。默认值为 2000 毫秒，最小值为 500 毫秒，最大值为 5000 毫秒。
按钮提示延迟	单选按钮和复选框。默认值为 3000 毫秒，最小值为 500 毫秒，最大值为 5000 毫秒。
文本提示延迟	管理界面文本。默认值和最小值为 500 毫秒，最大值为 5000 毫秒。

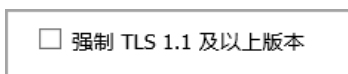
- 4 单击接受。

强制 TLS 版本

SonicOS 支持版本 1.0、1.1 和 1.2 的传输层安全性 (TLS) 协议。可以确保使用更安全的版本 1.1 及以上版本。

强制使用 TLS 版本 1.1 及以上版本的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | Web 管理设置。



<input type="checkbox"/> 强制 TLS 1.1 及以上版本

- 2 选中强制 TLS 1.1 及以上版本。

- 3 单击接受。

配置前板管理界面（仅限 SuperMassive 防火墙）

i | 注：此部分仅对前部有 LCD 面板的 SuperMassive 安全设备显示。

可以在前板管理界面中启用或禁用对配置菜单的访问权。

i | 提示：在首次安装 SuperMassive 安全设备时，系统会自动启用此功能。

在前板管理接口中允许访问配置菜单的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 前板管理界面。

前板管理接口

启用前面板的管理接口

启用前板管理接口

必须输入 PIN 才能进入前板

PIN:

确认 PIN:

掩码 PIN

- 2 选中启用前面板的管理界面。默认情况下已选中该选项。
- 3 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。
- 4 通过选中**掩码 PIN**复选框来选择是否在 PIN 字段和确认 PIN 字段中掩蔽 PIN。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）此选项，则 PIN 可见。默认情况下已选中该选项。
- 5 单击接受。

配置客户端证书验证

可以使用或不使用通用访问卡 (CAC) 来配置证书验证。

客户端证书检查

启用客户端证书检查

启用客户端证书缓存

用户名字段:

客户端证书发行者:

CAC 用户群组成员检索方法:

启用 OCSP 检查

启用定期 OCSP 检查

OCSP 检查间隔:
1~72 (小时)

① 注：默认情况下，未选中任何选项。

主题：

- 第 33 页的[关于通用存取卡](#)
- 第 33 页的[配置客户端证书验证](#)

- 第 34 页的[使用客户端证书检查](#)
- 第 35 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。

配置客户端证书验证

注：默认情况下，未选中任何选项。

配置客户端证书检查的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 客户端证书检查。



启用客户端证书检查

启用客户端证书缓存

用户名字段： 主题: 公用名

客户端证书发行者： ComSign CA

CAC 用户群组成员检索方法： 本地已配置

- 2 如需在 SonicWall 安全设备上启用客户端证书检查和 CAC 支持，请选中启用客户端证书检查。如果启用此选项，则其他选项将激活。随即显示一条警告确认消息：

警告！没有有效的客户端证书您将不能再使用 HTTPS 管理设备，您可能需要在用户页面上配置用户群组，是否要继续？

- 3 单击确定。
- 4 如需激活客户端证书缓存，请选中启用客户端证书缓存。

注：缓存会在启用 24 小时后过期。

- 5 如需指定从中获取用户名的证书字段，请从用户名字段下拉菜单中选择一个选项：

- 主题：公用名（默认）
- Sub Alt：电子邮件
- Sub Alt：Microsoft 通用主体名称

- 6 如需选择证书颁发机构 (CA) 证书发行者，请从**客户端证书发行者**下拉菜单中选择一项。默认值为 **ComSign CA**。

i 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。请参阅第 51 页的**管理证书**。

- 7 如需选择获取 CAC 用户群组成员资格的方式及确定正确的用户权限，请从**CAC 用户群组成员检索方法**下拉菜单中进行选择：

- **本地已配置**（默认）- 选择此选项后，应创建有适当成员资格的本地用户群组。
- **从 LDAP** - 如果选中了此选项，您需要在**管理 | 用户 | 设置**上配置 LDAP 服务器（请参阅第 134 页的**配置 SonicWall 以支持 LDAP**）。

- 8 如需启用在线证书状态协议 (OCSP) 检查以验证客户端证书是否有效且尚未撤销，请选中**启用 OCSP 检查**。启用此选项后，将显示 **OCSP 响应者 URL** 字段和**启用定期 OCSP 检查**选项。

<input type="checkbox"/> 启用 OCSP 检查
<input type="checkbox"/> 启用定期 OCSP 检查

- a 在 **OCSP 响应者 URL** 字段中输入用于验证客户端证书状态的 OSCP 服务器的 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`。

- 9 启用针对客户端证书的定期 OCSP 检查以验证证书是否仍然有效且尚未撤销的步骤如下：

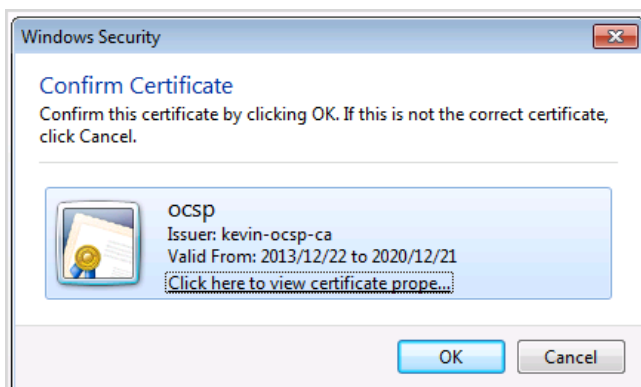
- a 选中**启用定期 OCSP 检查**。OCSP 检查间隔字段将激活。
- b 在 **OCSP 检查间隔 1~72**（小时）字段中输入两次 OCSP 检查之间的间隔（小时）。最短间隔为 1 小时，最长为 72 小时，默认值为 **24** 小时。

- 10 单击接受。

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。通过 HTTPS 开始管理会话时，将显示要求您确认证书的证书选择窗口。



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颁发方，以验证该客户端证书是否具有 CA 签名。如果找到了匹配项，则显示管理员登录页面。如果未找到匹配项，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。

如果未找到匹配项，则浏览器将显示：

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，但浏览器中未安装客户端证书。
- 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，但未选择任何客户端证书发行者或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 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：

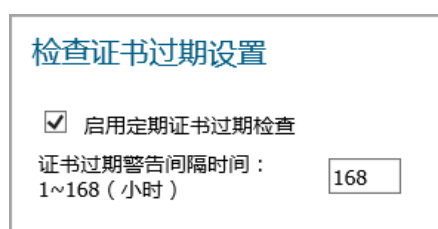
- `web-management client-cert disable`
- `web-management obsp disable`

① 注：如需 CLI 命令的完整列表和说明，请参阅 [SonicOS 6.2 CLI 参考指南](#)。

检查证书过期

激活证书过期的定期检查的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 检查证书过期设置。



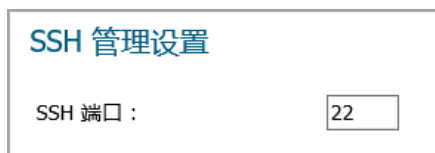
- 2 选中启用定期证书过期检查。默认情况下已选中该选项。启用后，证书过期提醒间隔字段将激活。
- 3 如需设置两次证书检查之间的间隔（小时），请在证书过期警告间隔时间：1 - 168（小时）字段中输入间隔。最短时间为 1 小时，最长为 168 小时，默认值为 168。
- 4 单击接受。

配置 SSH 管理

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。

更改 SSH 端口的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | SSH 管理设置。



- 2 在 SSH 端口字段中输入端口。默认 SSH 端口号是 22。
- 3 单击接受。

配置高级管理选项

通过高级管理选项，您可以指定：

- SonicWall 安全设备由 SNMP（默认）还是 SonicWall 全局管理系统 (GMS) 进行管理。如需 GMS 的更多信息，请参阅 [GMS 指南](#)。
- 为 MGMT 接口创建一个管理界面地址对象。

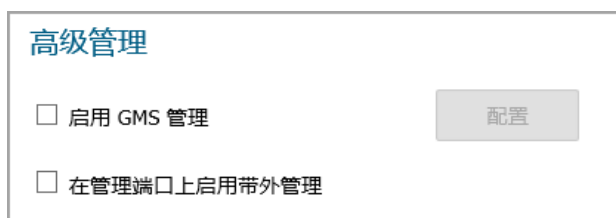
此管理界面提供了管理设备的受信任接口。该接口对网络连接有诸多限制。如果在 MGMT 子网中配置了 NTP、DNS 和 SYSLOG 服务器，则设备会将 MGMT IP 用作源 IP 并自动创建 MGMT 地址对象和路由策略。所有来自管理界面的流量都将按照该策略进行路由。已创建的路由显示在 [系统设置 | 网络 | 路由](#) 页面上（如需路由的更多信息，请参阅第 372 页的 [配置路由通告和路由策略](#)）。

MGMT 地址对象和路由策略用于创建/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。

注：默认情况下，这些选项都未启用。

配置高级管理选项的步骤如下：

- 1 在管理视图中，转至系统设置 | 设备 | 基本设置 | 高级管理。



- 2 如需允许 SonicWall GMS 管理防火墙，请选中 **启用 GMS 管理**。配置按钮将激活。如需配置 GMS 管理，请参阅第 37 页的 [启用 GMS 管理](#)。
- 3 对于用作带外接口且为新创建的地址对象配置路由策略的 MGMT 接口，如需为其启用自动创建管理界面地址对象，请选中 **在管理端口上启用带外管理**。

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。

启用 GMS 管理

① | 注：如需 SonicWall 全局管理系统的更多信息，请访问 <http://www.sonicwall.com/GMS> 指南。

对安全设备进行 GMS 管理配置的步骤如下：

- 1 转至管理 | 系统设置 > 设备 | 基本设置 | 高级管理。
- 2 选中启用 GMS 管理。配置按钮将激活。
- 3 单击配置。随即显示配置 GMS 设置对话框。

GMS 设置

GMS 主机名称或 IP 地址:

GMS Syslog 服务器端口:

仅发送心跳状态消息

NAT 设备之后的 GMS

NAT 设备 IP 地址:

管理模式:

- 4 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。
- 5 在 GMS Syslog 服务器端口字段中输入端口。默认值为 514。
- 6 如需仅发送检测信号而不是日志消息，请选中仅发送心跳状态消息。默认已禁用该选项。
- 7 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。默认已禁用该选项。
选择此选项后，NAT 设备 IP 地址字段将激活。
 - a 在 NAT 设备 IP 地址字段中输入 NAT 设备的 IP 地址。
- 8 从管理模式下拉菜单中选择以下 GMS 模式之一。

IPSEC 管理隧道

现有隧道

允许通过 GMS 管理控制台的 IPsec VPN 隧道来管理防火墙。转至步骤 9。
使用 GMS 服务器与防火墙的连接上现有的 VPN 隧道。将显示一条消息。

管理模式:

注：将会使用已建立的隧道。

转至步骤 11。

HTTPS

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。SonicWall 防火墙还使用 3DES 和防火墙管理员的密码发送加密的 syslog 数据包和 SNMP 陷阱。用于配置 GMS 报告服务器显示的选项。转至步骤 10。

- 9 将显示默认 IPsec VPN 设置，其值由 SonicOS 填写。验证设置。

管理模式:	IPSEC 管理隧道
入站/出站 SPI:	E4598E24
加密算法:	加密并认证 (DES MD5)
加密密钥:	8f35b871a3243673
认证密钥:	1b67272027393d323d102e405bdf49ed

- 从加密算法下拉菜单中，选择适当的算法。
- (可选) 在加密密钥字段中输入新的加密密钥：

对于	密钥必须是
DES	16 个十六进制字符
3DES	48 个十六进制字符

- (可选) 在身份验证密钥字段中输入新的身份验证密钥：

对于	密钥必须是
MD5	32 个十六进制字符
SHA1	40 个十六进制字符

- 转至 [步骤 11](#)。

10 SonicOS 需要知道 GMS 报告服务器。

管理模式:	HTTPS
<input type="checkbox"/> 向“分布式 GMS 报告服务器”发送 Syslog 消息	
GMS 报告服务器 IP 地址:	
GMS 报告服务器端口:	514

- 选中向分布式 GMS 报告服务器发送 Syslog 消息。默认情况下未选中该选项。以下选项将激活。
- 在 GMS 报告服务器 IP 地址字段中，输入 GMS 服务器的 IP 地址。
- 在 GMS 报告服务器端口字段中，输入 GMS 服务器的端口。默认端口号是 514。

11 单击确定。

手动下载 SonicPoint 镜像

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，则在您连接 SonicPoint 设备时，它将从 SonicWall 服务器自动下载 SonicPoint 镜像的正确版本。
- 无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

如需更多信息，请参阅[更新指南](#)。

小心：您必须下载安全设备上正在运行的 SonicOS 固件版本所对应的 SonicPoint 镜像。MySonicWall 网站提供了相应版本的相关信息。升级 SonicOS 固件时，请确保升级为正确的 SonicPoint 镜像。

选择要下载的一个或多个 SonicPoint 镜像的类型的步骤如下：

- 1 转至管理 | 系统设置 > 设备 | 基本设置 | 下载 URL。

下载 URL

- 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 固件 URL (http://)
- 手动指定 SonicWave 4320/e/i 镜像 URL (http://)

- 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 固件 URL (http://)
- 手动指定 SonicPoint-AC Wave2 镜像 URL (http://)

- 2 单击相应的 SonicPoint 镜像 URL。随即显示该 URL 的字段。

- 手动指定 SonicPoint-NDR 固件 URL (http://)
- 手动指定 SonicPoint-ACe/ACi/N2 固件 URL (http://)
- 手动指定 SonicWave 4320/e/i 镜像 URL (http://)

- 3 在关联的字段中输入镜像下载位置。

- 4 单击接受。

选择语言

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 管理界面的语言要求重启安全设备。

选择管理界面的语言的步骤如下：

- 1 转至管理 | 系统设置 > 设备 | 基本设置 | 语言。

语言

语言选择：

- 2 从语言选择下拉菜单中选择语言。
- 3 单击接受。

管理 SNMP

- 第 41 页的[关于设备 | SNMP](#)
 - 第 41 页的[关于 SNMP](#)
 - 第 42 页的[设置 SNMP 访问权限](#)
 - 第 50 页的[将 SNMP 配置为服务并添加规则](#)
 - 第 50 页的[关于 SNMP 日志](#)

关于设备 | SNMP

您可以使用 SNMP 或 SonicWall 全局管理系统 (GMS) 来管理 SonicWall 安全设备。本节介绍如何配置 SonicWall 以使用 SNMP 进行管理。如需使用 GMS 管理 SonicWall，请参阅 SonicOS GMS 指南。

主题：

- 第 41 页的[关于 SNMP](#)
- 第 42 页的[设置 SNMP 访问权限](#)
- 第 50 页的[将 SNMP 配置为服务并添加规则](#)
- 第 50 页的[关于 SNMP 日志](#)

关于 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 SonicWall 安全设备的状态和接收网络中发生的重要事件通知。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 (MIB-II) 群组。

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。

基于 SNMP 版本的安全级别、身份验证和加密表显示不同版本的 SNMP 如何处理安全级别、身份验证和加密。

基于 SNMP 版本的安全级别、身份验证和加密

版本	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
	noAuthNoPriv	用户名	否	用户名匹配
	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。

SonicWall 安全设备使用任意接口回复用于 MIB-II 的 SNMP Get 命令，并支持用于生成陷阱消息的自定义 SonicWall MIB。自定义 SonicWall MIB 可以在 SonicWall 网站下载，并加载到 HP Openview、Tivoli 或 SNMPc 等第三方 SNMP 管理软件中。

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，还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 设置可以配置 SNMP 对话框的常规设置菜单下进行配置。引擎 ID 用于授权接收到的 SNMP 数据包。只处理匹配的数据包 EngineID。

设置 SNMP 访问权限

设置 SNMP 包括：

- 第 42 页的[启用和配置 SNMP 访问权限](#)
- 第 45 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 以提供基本功能或配置 SonicWall 安全设备使用功能更丰富的 SNMPv3 选项。

如需使用 SNMP，您必须先启用它。

主题：

- 第 43 页的[配置基本功能](#)
- 第 44 页的[配置 SNMPv3 引擎 ID](#)
- 第 46 页的[配置 SNMPv3 视图的对象 ID](#)
- 第 47 页的[创建群组并添加用户](#)
- 第 49 页的[添加访问](#)

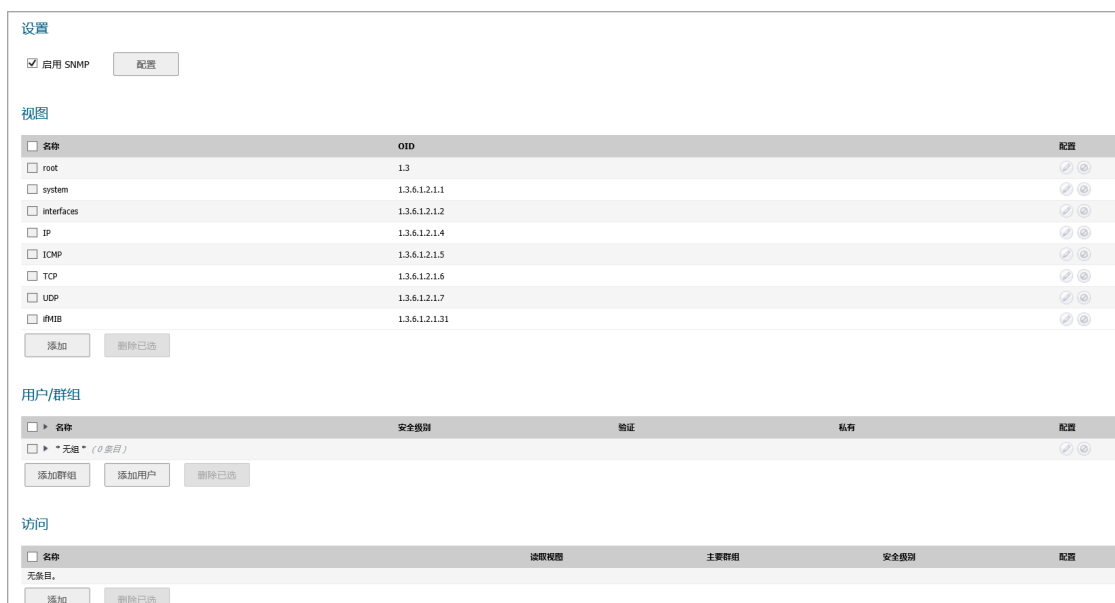
配置基本功能

启用 SNMP 的步骤如下：

- 1 转至设备 | 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 信息在 SNMP 页面上填写且配置按钮将激活。



4 如需配置 SNMP 接口，请单击配置。随即显示配置 SNMP 对话框。

The screenshot shows a configuration dialog box with two tabs: '常规' (Basic) and '高级' (Advanced). The '常规设置' (Basic Settings) section contains the following fields:

- 系统名称: []
- 系统联系人: []
- 系统位置: []
- 资产编号: []
- 获取团体名称: public
- 捕获团体名称: []
- 主机 1: []
- 主机 2: []
- 主机 3: []
- 主机 4: []

- 5 在常规页面上的系统名称字段中，输入 SonicWall 安全设备的主机名。
- 6 也可在系统联系人字段中输入网络管理员的姓名。
- 7 也可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。否则，该字段为可选字段。
- 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。默认名称为 **public**。
- 10 也可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 n 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，但您的系统最多可以使用地址或主机名的最大数目。
- 12 如果您：
 - 如需设置 SNMPV3，请转至第 44 页的[配置 SNMPv3 引擎 ID](#)。
 - 现在设置 SNMP 已完成，请单击确定。

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 转至设备 | SNMP。
- 2 如果尚未为系统配置 SNMP，请遵循第 43 页的[配置基本功能](#)中的[步骤 1 到步骤 11](#)。

- 3 单击高级。将显示高级页面。

常规 高级

SNMPPV3 设置

强制使用 SNMPPV3

引擎 ID:

SNMPP 可选设置

增加 SNMPP 子系统优先级

- 4 选中强制使用 **SNMPPV3** 复选框。这会禁用 SNMPPV1/v2，仅允许 SNMPPV3 访问，从而为 SNMPP 管理提供最高的安全性。

重要： 如果选择了此选项，则在单击确定之前，必须在常规页面上指定资产编号。

- 5 在引擎 ID 字段中输入十六进制的引擎 ID 号。SonicOS 会自动填写此字段，但可以更改它。此号码与接收的 SNMPP 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。

- 6 也可以选中增加 **SNMPP 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 SNMPP 查询的响应。启用该项会使 SNMPP 子系统始终在较高的系统优先级响应和操作。

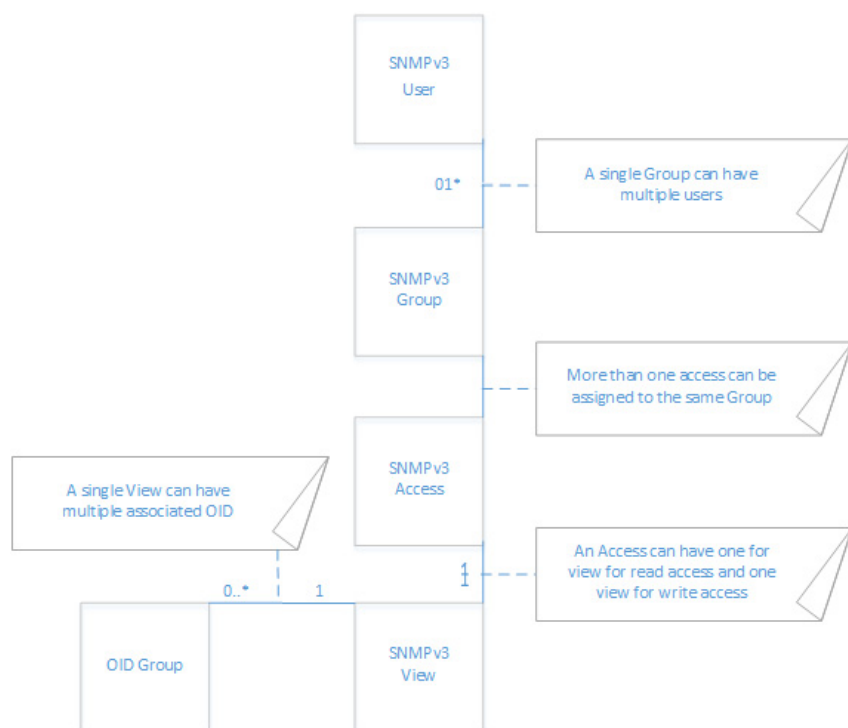
重要： 启用该选项可能会影响整个系统的性能。

- 7 单击确定。现在将使用 SNMPPV3 安全选项来处理数据包。

设置 SNMPPV3 群组 and 访问权限

SNMPPV3 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。**SNMPPV3 群组和用户访问权限** 显示群组和用户的访问如何与这些不同的权限相关联。

SNMPv3 群组 and 用户访问权限



配置 SNMPv3 视图的对象 ID

SNMPv3 视图显示用户和群组的访问设置。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 转至设备 | SNMP。
- 2 如需添加视图，请在视图部分单击添加。随即显示添加 SNMP 视图对话框。



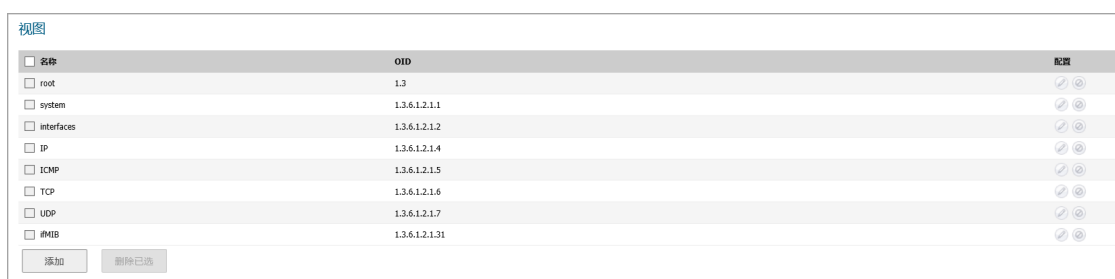
- 3 在视图名称字段中输入一个有意义的名称。默认的名称是新增 SNMP 视图。

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。如需从 OID 列表中删除 OID，请选择 OID，然后单击删除。

- 6 添加其他任意视图和关联的 OID。
- 7 单击确定。新视图已添加到视图表中。



名称	OID	操作
<input type="checkbox"/> root	1.3	
<input type="checkbox"/> system	1.3.6.1.2.1.1	
<input type="checkbox"/> interfaces	1.3.6.1.2.1.2	
<input type="checkbox"/> IP	1.3.6.1.2.1.4	
<input type="checkbox"/> ICMP	1.3.6.1.2.1.5	
<input type="checkbox"/> TCP	1.3.6.1.2.1.6	
<input type="checkbox"/> UDP	1.3.6.1.2.1.7	
<input type="checkbox"/> #MIB	1.3.6.1.2.1.31	

创建群组并添加用户

默认情况下，有一个无法配置或删除的群组 *无群组*。但是，可以将用户添加到此默认群组中。

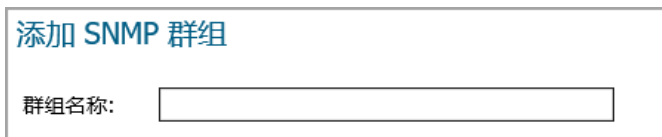
主题：

- 第 48 页的 [创建群组](#)
- 第 48 页的 [添加用户](#)

创建群组

创建群组的步骤如下：

- 1 转至设备 | **SNMP**。
- 2 单击用户/群组表下的添加群组。随即显示添加 **SNMP** 群组对话框。



添加 SNMP 群组

群组名称:

- 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。更新用户/群组表，并且配置列中的编辑和删除图标可用。



用户/群组

名称	安全级别	验证	私有	配置
* 无组 * (0 成员)				

添加群组 添加用户 删除已选

添加用户

添加用户的步骤如下：

- 1 转至设备 | **SNMP**。
- 2 单击用户/群组表下的添加用户。随即显示添加 **SNMP** 用户对话框。



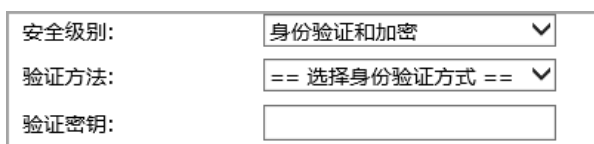
添加 SNMP 用户

用户名:

安全级别:

群组:

- 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）
 - 身份验证 - 显示以下两个新选项：



安全级别:

验证方法:

验证密钥:

- 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：

安全级别:	身份验证和加密	▼
验证方法:	== 选择身份验证方式 ==	▼
验证密钥:	<input type="text"/>	
加密方式:	== 选择加密方式 ==	▼
私有密钥:	<input type="text"/>	

- 验证方法 - 请参阅上文。
 - 验证密钥 - 请参阅上文。
 - 从加密方式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。
- 从群组下拉菜单中选择一个群组。（默认为*无组*。）
 - 完成时，单击确定。此用户将添加到用户/群组表中以及适当的群组中（包括 *无组*）。

用户/群组				
名称	安全级别	验证	私有	配置
1 (0 条目)				ⓘ ⓧ
无组 (0 条目)				ⓘ ⓧ

添加群组 添加用户 删除已选

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：

- 转至设备 | **SNMP**。
- 在访问表下，单击添加。随即显示添加 **SNMP** 访问对话框。

添加 SNMP 访问	
访问名称:	新增 SNMP 访问
读取视图:	== 选择视图 == ▼
主 SNMPv3 群组:	== 选择群组 == ▼
访问安全级别:	无 ▼

- 在访问名称字段中输入一个简单易记的名称。
- ⓘ | 注：现有条目的名称不可编辑。
- 从读取视图下拉菜单在可用视图列表中选择一视图。

5 从主 **SNMPv3** 群组下拉菜单在可用群组列表中选择一个群组。

i **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。
访问权限不能分配给*无组*。

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。



名称	访问权限	主要群组	安全级别	配置
<input type="checkbox"/> 新增 SNMP 访问	UDP	1	无	 

添加 删除已选

将 SNMP 配置为服务并添加规则

默认情况下，SonicWall 安全设备禁用 SNMP。如需启用 SNMP，您必须先要在**设备 | SNMP**页面上启用 SNMP，然后再为各个接口启用 SNMP。为此，请转至**网络 | 接口**页面，然后单击要为其启用 SNMP 的接口对应的**配置**。如需将 SNMP 配置为服务并添加规则的更多信息，请参阅第 224 页的**配置接口**。

如果您的 SNMP 管理系统支持发现，SonicWall 安全设备代理将自动发现网络上的 SonicWall 安全设备。否则，您必须将 SonicWall 安全设备添加到 SNMP 管理系统上的 SNMP 管理设备的列表中。

关于 SNMP 日志

可以在**日志 | 事件日志**页面上查看 SNMP 日志。如需事件日志的更多信息，请参阅 **SonicOS 调查指南**。

仅对 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。如果未在**日志 | 事件日志**页面上选择任何类别，则不会生成任何陷阱消息。

管理证书

- 第 51 页的[关于证书](#)
 - 第 51 页的[关于数字证书](#)
 - 第 52 页的[关于证书和证书请求表](#)
 - 第 54 页的[导入证书](#)
 - 第 56 页的[删除证书](#)
 - 第 56 页的[生成证书签名请求](#)
 - 第 60 页的[配置简单证书注册协议](#)

关于证书

如需实施用于 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[设备 > 证书](#)页面将有效的 CA 证书导入到防火墙。导入有效的 CA 证书后，可以使用它来验证您的本地证书。

SonicOS 通过 SonicWall 安全设备提供大量证书，这些是内置证书，不能删除或配置。

关于数字证书

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 (SA) 之前使用数字证书对对端设备进行身份验证。若无数字证书，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。

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。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

主题:

- 第 52 页的关于证书和证书请求表
- 第 54 页的导入证书
- 第 56 页的删除证书
- 第 56 页的生成证书签名请求
- 第 60 页的配置简单证书注册协议

关于证书和证书请求表

证书和证书请求					项目 1 至 50 (/ 228)	
视图类型: <input checked="" type="radio"/> 所有证书 <input type="radio"/> 已导入的证书和请求 <input type="radio"/> 内置证书 <input type="checkbox"/> 包括已过期的内置证书						
#	证书	类型	验证	过期	详细信息	配置
1	HTTPS 管理证书	本地证书	Self-signed	Jan 19 03:14:07 2038 GMT		
2	ComSign CA	CA 证书		Mar 19 15:02:18 2029 GMT		
3	thawte Primary Root CA - G3	CA 证书		Dec 1 23:59:59 2037 GMT		
4	VeriSign, Inc.	CA 证书		Aug 1 23:59:59 2028 GMT		
5	VeriSign Class 3 International Server CA - G3	CA 证书		Feb 7 23:59:59 2020 GMT		
6	AddTrust External CA Root	CA 证书		May 30 10:48:38 2020 GMT		
7	TC TrustCenter Class 2 CA II	CA 证书		Dec 31 22:59:59 2025 GMT		
8	ACCVRAIZ1	CA 证书		Dec 31 09:37:37 2030 GMT		
9	GlobalSign	CA 证书		Mar 18 10:00:00 2029 GMT		
10	PSCProcert	CA 证书		Dec 25 23:59:59 2020 GMT		
11	ACEDICOM Root	CA 证书		Apr 13 16:24:22 2028 GMT		
12	COMODO Certification Authority	CA 证书		Dec 31 23:59:59 2029 GMT		
13	DigiCert High Assurance EV Root CA	CA 证书		Jul 25 17:57:44 2019 GMT		
14	Microsoft Internet Authority	CA 证书		Apr 25 17:40:35 2020 GMT		
15	Atos TrustedRoot 2011	CA 证书		Dec 31 23:59:59 2030 GMT		
16	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcı	CA 证书	在 7 天内过期	Dec 22 18:37:19 2017 GMT		
17	DST Root CA X3	CA 证书		Sep 30 14:01:15 2021 GMT		
18	GeoTrust DV SSL CA	CA 证书		Feb 25 21:32:31 2020 GMT		
19	Cybertrust Public SureServer SV CA	CA 证书		Sep 8 17:34:08 2020 GMT		
20	T-TeleSec GlobalRoot Class 3	CA 证书		Oct 1 23:59:59 2033 GMT		
21	SwissSign Platinum CA - G2	CA 证书		Oct 25 08:36:00 2036 GMT		
22	Chambers of Commerce Root	CA 证书		Sep 30 16:13:44 2037 GMT		
23	S-TRUST Authentication and Encryption Root CA 2005:PW	CA 证书		Jun 21 23:59:59 2030 GMT		
24	VeriSign Class 3 Public Primary Certification Authority - G5	CA 证书		Jul 16 23:59:59 2036 GMT		
25	QuoVadis Root Certification Authority	CA 证书		Mar 17 18:33:33 2021 GMT		
26	AffirmTrust Networking	CA 证书		Dec 31 14:08:24 2030 GMT		
27	TC TrustCenter Universal CA I	CA 证书		Dec 31 22:59:59 2025 GMT		
28	TWCA Global Root CA	CA 证书		Dec 31 15:59:59 2030 GMT		
29	Secure Global CA	CA 证书		Dec 31 19:52:06 2029 GMT		
30	GlobalSign	CA 证书		Dec 15 08:00:00 2021 GMT		
31	Digital Signature Trust Co.	CA 证书		Dec 9 19:47:26 2018 GMT		
32	VeriSign Class 3 Public Primary Certification Authority - G5	CA 证书		Nov 7 23:59:59 2021 GMT		
33	Cybertrust Global Root	CA 证书		Dec 15 08:00:00 2021 GMT		
34	Digital Signature Trust Co.	CA 证书		Dec 10 18:40:23 2018 GMT		
35	VeriSign Class 3 Secure Server CA - G3	CA 证书		Feb 7 23:59:59 2020 GMT		
36	TeliaSonera Root CA v1	CA 证书		Oct 18 12:00:50 2032 GMT		
37	AffirmTrust Commercial	CA 证书		Dec 31 14:06:06 2030 GMT		
38	Thawte SSL CA	CA 证书		Feb 7 23:59:59 2020 GMT		
39	GlobalSign Domain Validation CA - G2	CA 证书		Apr 13 10:00:00 2022 GMT		
40	Entrust.net Certification Authority (2048)	CA 证书		Jul 24 14:15:12 2029 GMT		
41	GeoTrust Global CA	CA 证书		May 21 04:00:00 2022 GMT		
42	The Go Daddy Group, Inc.	CA 证书		Jun 29 17:06:20 2034 GMT		
43	QuoVadis Root CA 3	CA 证书		Nov 24 19:06:44 2031 GMT		
44	NetLock Minostett Kozlegző (Class Q4) Tanúsítványkiadó	CA 证书		Dec 15 01:47:11 2022 GMT		
45	DigiCert Assured ID Root CA	CA 证书		Nov 10 00:00:00 2031 GMT		
46	Thawte SGC CA - G2	CA 证书		Jul 28 23:59:59 2020 GMT		
47	http://www.valicert.com/	CA 证书		Jun 25 22:23:48 2019 GMT		
48	VeriSign Class 1 Public Primary Certification Authority - G3	CA 证书		Jul 16 23:59:59 2036 GMT		
49	Chunghwa Telecom Co., Ltd.	CA 证书		Dec 20 02:31:27 2034 GMT		
50	Certum CA	CA 证书		Jun 11 10:46:39 2027 GMT		

证书和证书请求表提供用于管理 CA 和本地证书的所有设置。

视图样式菜单允许根据以下条件显示证书：

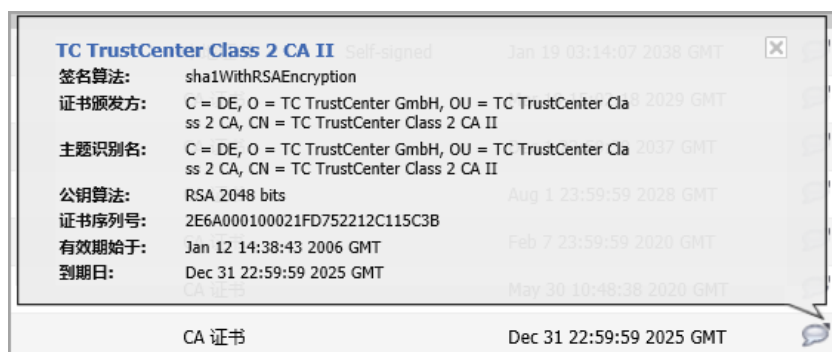
此条件	显示
所有证书	所有内置和导入的证书和证书请求。这是默认值。
已导入的证书和请求	仅导入的证书和生成的证书请求。默认情况下未选中该选项。
内置证书	仅内置证书。默认情况下未选中该选项。
包括已过期和内置证书	所有已过期和内置的证书。默认情况下未选中该选项。

证书和证书请求表显示有关证书的这些信息：

此列	显示
证书	证书的名称。
类型	证书类型： <ul style="list-style-type: none">• CA 证书• 本地证书• 待处理的请求
已验证	验证信息： <ul style="list-style-type: none">• 自签名• 将于 n 天后过期• 已过期
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。如需证书的详细信息，请参阅第 53 页的 关于证书详细信息 。
配置	包含 <ul style="list-style-type: none">• 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）。 <p>注：不能删除或导入内置证书。</p>

关于证书详细信息

单击详细信息列中的备注图标将会显示证书的相关信息。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）

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 协商中使用的对端证书。

主题：

- [第 54 页的导入本地证书](#)
- [第 55 页的导入证书机构证书](#)
- [第 55 页的创建 PKCS-12 格式证书文件（仅 Linux 系统）](#)

导入本地证书

导入本地证书的步骤如下：

- 1 转至设备 > 证书。
- 2 单击导入。显示导入证书对话框。

导入证书

从 PKCS#12 (.p12 或 .pfx) 编码文件导入具有私有密钥的最终用户本地证书
 从 PKCS#7 (.p7b)、PEM (.pem) 或 DER (.der 或 .cer) 编码文件导入 CA 证书

证书名称：

证书管理密码：

请选择要导入的文件：

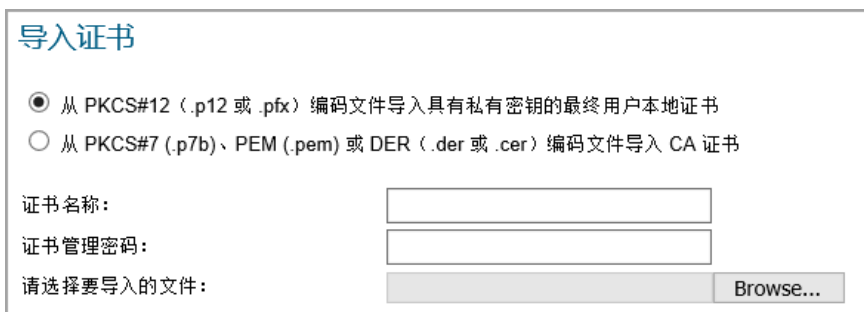
- 3 在证书名称字段中输入证书的名称。
- 4 在证书管理密码字段中输入您的证书机构所使用的密码以加密 PKCS#12 文件。
- 5 单击浏览以找到证书文件。
- 6 单击打开设置证书的目录路径。
- 7 单击导入，将证书导入防火墙。完成导入后，可以在证书和证书请求表中查看该证书条目。
- 8 将指针移到详细信息列中的备注图标将会显示证书的详细信息。

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。

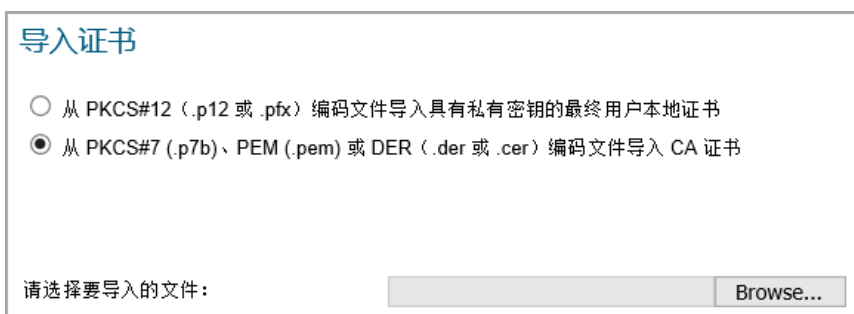
导入证书机构证书

导入证书机构提供的证书的步骤如下：

- 1 转至设备 > 证书。
- 2 单击导入。显示导入证书对话框。



- 3 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。



- 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。

创建 PKCS-12 格式证书文件（仅 Linux 系统）

可使用带有 OpenSSL 的 Linux 系统创建 PKCS12 格式证书文件。如需创建 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）
- 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。

运行 `openssl` 命令后，系统将提示您输入密码，以保护/加密文件。选择密码后，完成 PKCS-12 格式的证书文件的创建，并将其导入到设备中。

删除证书

注：无法删除内置证书。

如果证书已过期或您决定不使用第三方证书进行 VPN 身份验证，您可以删除导入的证书。也可以随时删除您自己创建的证书。

如需删除：

- 单个证书，单击其删除图标。
- 一个或多个证书：
 - a 单击它们的复选框。删除和全部删除按钮变为可用。
 - b 单击删除或全部删除。
- 所有非内置证书：
 - a 单击表标题中的复选框。删除和全部删除按钮变为可用。
 - b 单击删除或全部删除。

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。

生成证书签名请求的步骤如下：

- 1 转至设备 > 证书。
- 2 单击新签名请求。随即显示证书签名请求对话框。

生成证书签名请求

证书别名：	<input type="text"/>
国家或地区 ▼	<input type="text"/>
州/省 ▼	<input type="text"/>
县市、市或县 ▼	<input type="text"/>
公司或组织 ▼	<input type="text"/>
部门 ▼	<input type="text"/>
组 ▼	<input type="text"/>
小组 ▼	<input type="text"/>
公用名 ▼	<input type="text"/>
主题识别名：	<input type="text"/>
主题备用名（可选）：	
域名 ▼	<input type="text"/>
签名算法：	SHA1 ▼
主题密钥类型：	RSA ▼
主题密钥大小/曲线：	1024 位 ▼

- 3 在证书别名字段中输入证书的别名。
- 4 使用**识别名组件**表中显示的下拉菜单创建可分辨名称 (DN)，然后在相关字段中输入证书的信息。

i 注：您可以从相关下拉菜单为每个 DN 选择您的国家或地区；对于其它组件，在相关文本字段中输入信息。

识别名组件

从这个下拉菜单中 选择/输入合适的信息。

国家/地区	国家或地区（默认） 州/省 县市或县 公司或组织
州/省	国家/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 组 小组

识别名组件

从这个下拉菜单中	选择/输入合适的信息。
公司或组织	公司或组织（默认） 部门 组 小组 公用名 序列号 电子邮件地址
部门	部门（默认） 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

在输入组件信息时，将在主题识别名字段中创建可分辨名称 (DN)。

国家或地区 ▼	CHINA (CN) ▼
州/省 ▼	<input type="text"/>
县市、市或县 ▼	<input type="text"/>
公司或组织 ▼	<input type="text"/>
部门 ▼	<input type="text"/>
组 ▼	<input type="text"/>
小组 ▼	<input type="text"/>
公用名 ▼	<input type="text"/>
主题识别名:	C=CN

5 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
- 电子邮件地址
- IPv4 地址

6 从签名算法下拉菜单中选择签名算法：

- MD5
- 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） 用于加密数据的公钥加密算法。

ECDSA 使用椭圆曲线数字签名算法对数据进行加密，该算法具有较高强度的每按键位安全性。

8 从主题密钥大小/曲线下拉菜单中选择主题密钥大小或曲线。

注：并非所有密钥大小或曲线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。

如果选择的密钥类型为

RSA，选择密钥大小 **ECDSA，选择曲线**

1024 位（默认） **prime256v1：**通过 256 位素数域的 X9.62.SECP 曲线（默认）

1536 位 **secp384r1：**通过 384 位素数域的 NIST/SECP 曲线

2048 位 **secp521r1：**通过 521 位素数域的 NIST/SECP 曲线

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。

证书	类型	验证	过期	详细信息	配置
1 123	待处理的请求				
2 HTTPS 管理证书	本地证书	Self-signed	Jan 19 03:14:07 2038 GMT		
3 ComSign CA	CA 证书		Mar 19 15:02:18 2029 GMT		

10 单击导出图标。显示导出证书请求对话框。

导出证书请求

名称： 123
主题识别名： C=CN
主题密钥标识符： 0x0E2F57BAE1BE7F1356B6F8B3C5ACCCF45CA10D98
公钥算法： RSA 1024 bits

已生成 PKCS#10 验证请求，现可以将其导出。请将此文件保存到本地磁盘上，以用于提交至注册或证书颁发机构。将会以 PEM 证书请求格式保存该文件，默认情况下 '123.p10'（可在下载时根据需要更改文件名）。

- 11 单击**导出**图标将文件下载到计算机上。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。
- 13 单击**上传**图标以上传用于签名请求的签名证书。显示**上传证书**对话框。

上传签名请求的已签名证书

名称:	123
主题识别名:	C=CN
主题密钥标识符:	0x0E2F57BAE1BE7F1356B6F8B3C5ACCCF45CA10D98
公钥算法:	RSA 1024 bits

请选择要上传的文件: **Browse...**

文件应为 PEM (.pem) 或 DER (.der 或 .cer) 编码文件

- 14 单击**浏览**选择一个文件。将显示“打开文件”对话框。
- 15 选择该文件。
- 16 单击**打开**。
- 17 单击**上传**。

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，请参阅：<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 56 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**。随即显示**简单证书注册协议配置**窗口。

简单证书注册协议配置

证书签发请求列表:	<input type="text" value="123"/>
CA URL:	<input type="text"/>
撤销密码 (可选):	<input type="text"/>
请求数目:	<input type="text" value="256"/>
轮询间隔:	<input type="text" value="30"/>
最大轮询时间:	<input type="text" value="28800"/>

- 3 从证书签发请求列表中，SonicOS 自动选择一个默认的 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**以提交简单证书注册协议注册。

防火墙联系 CA 以请求证书。这一过程需要的时间取决于 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。

配置时间设置

- [第 62 页的关于设备 | 时间](#)
 - [第 62 页的设置系统时间](#)
 - [第 64 页的配置 NTP 设置](#)

关于设备 | 时间

管理 | 系统设置 | 设备 | 时间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。

系统时间

时间 (时:分:秒): 02 : 03 : 54
日期: 十二月 15, 2017
时区: 太平洋时间 (美国和加拿大) (GMT-8:00)

使用 NTP 自动设置时间
 自动为夏令时调整时钟
 在日志中显示 UTC (而不是本地时间)
 按国际格式显示日期
 仅使用自定义的 NTP 服务器

NTP 设置

① 默认情况下，将使用内部 NTP 列表，而下面的列表是可选的。

更新间隔 (分钟数): 60

NTP 服务器	配置
无条目	

添加 全部删除

默认情况下，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 62 页的设置系统时间](#)
- [第 64 页的配置 NTP 设置](#)

设置系统时间

可以在设备 | 时间的系统时间部分中设置系统时间。

系统时间

时间（时：分：秒）： : :

日期：

时区：

使用 NTP 自动设置时间

自动为夏令时调整时钟

在日志中显示 UTC（而不是本地时间）

按国际格式显示日期

仅使用自定义的 NTP 服务器

设置系统时间的步骤如下：

- 1 转至设备 | 时间。
- 2 从时区中选择所在的时区。
- 3 设定时间的步骤如下：
 - 选择使用 **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。默认情况下已选中该选项。
 - 清除使用 **NTP 自动设置时间**以手动设置时间。时间和日期选项可用。

时间（时：分：秒）： : :

日期：

- 1) 使用时间（时：分：秒）下拉菜单选择 24 小时制时间。
 - 2) 从日期下拉菜单中选择日期。
- 4 如需启用自动调整夏令时，请选择**自动为夏令时调整时钟**。对于那些遵守夏令时的地区，默认情况下已选中该选项。
 - 5 如需对日志事件使用世界时 (UTC) 而非本地时间，请选择**在日志中显示 UTC（而不是本地时间）**。默认情况下未选中该选项。
 - 6 如需以国际格式显示日期，即在月份前面显示日期，请选择**按国际格式显示日期**。

日期：

默认情况下未选中该选项。

- 7 如果要使用手动输入的 NTP 服务器列表，而非使用内部 NTP 服务器列表来设置防火墙时钟，请选择**仅使用自定义的 NTP 服务器**。
 - 重要：**仅当配置了一个或多个 NTP 服务器时才选择此选项。如需 NTP 服务器的更多信息，请参阅第 64 页的**配置 NTP 设置**。
- 8 单击接受。

配置 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： 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。



主题：

- 第 64 页的[使用 NTP 服务器更新防火墙时钟](#)
- 第 64 页的[添加 NTP 服务器](#)
- 第 65 页的[编辑 NTP 服务器条目](#)
- 第 65 页的[删除 NTP 服务器条目](#)

使用 NTP 服务器更新防火墙时钟

使用本地服务器设置防火墙时钟的步骤如下：

- 1 转至设备 | 时间。
- 2 按照第 64 页的[配置 NTP 设置](#)中的描述添加一个或多个 NTP 服务器。
- 3 选择使用 NTP 来自动设置时间（请参阅第 62 页的[设置系统时间](#)默认情况下未选中该选项。）。
- 4 如需配置 NTP 服务器更新防火墙的频率，请在更新间隔（分钟）中输入时间间隔。默认值为 60 分钟。
- 5 单击接受。

添加 NTP 服务器

将 NTP 服务器添加到防火墙配置中的步骤如下：

- 1 转至设备 | 时间。
- 2 在 NTP 设置部分中，单击添加。随即显示添加 NTP 服务器对话框。

NTP 服务器：	<input type="text"/>
NTP 验证类型：	无身份验证 ▾
受信密钥序号：	<input type="text"/>
密钥序号：	<input type="text"/>
密码：	<input type="password"/>

- 3 在 NTP 服务器字段中输入远程 NTP 服务器的 IP 地址。

- 4 从 **NTP 验证类型** 下拉菜单中选择验证类型：
 - 无身份验证 - 不需要执行身份验证且以下三个选项处于灰显状态。转至 [步骤 8](#)。
 - MD5 - 需要执行身份验证且以下三个选项将激活。
- 5 在 **受信密钥序号** 字段中输入受信密钥序号。最小值为 1，最大值为 99999。
- 6 在 **密钥序号** 字段中输入密钥序号。最小值为 1，最大值为 99999。
- 7 在 **密码** 字段中输入密码。
- 8 单击 **确定**。**NTP 服务器** 部分将显示服务器。



编辑 NTP 服务器条目

编辑 NTP 服务器条目的步骤如下：

- 1 转至 **设备 | 时间**。
- 2 在 **NTP 服务器** 表中，单击条目的 **编辑** 图标。将显示 **编辑 NTP 服务器** 对话框，它与 **添加 NTP 服务器** 对话框相同；请参阅第 64 页的 [添加 NTP 服务器](#)。
- 3 做出更改。
- 4 单击 **确定**。

删除 NTP 服务器条目

删除 NTP 服务器条目的步骤如下：

- 1 转至 **设备 | 时间**。
- 2 在 **NTP 服务器** 表中，单击条目的 **删除** 图标。

删除所有服务器的步骤如下：

- 3 转至 **设备 | 时间**。
- 4 在 **NTP 服务器** 表下，单击 **全部删除**。

设置日程

- 第 66 页的[关于日程](#)
- 第 66 页的[关于设备 | 日程](#)
 - 第 67 页的[添加自定义日程](#)
 - 第 68 页的[修改日程](#)
 - 第 69 页的[删除自定义日程](#)

关于日程

SonicOS 将日程对象与其安全功能和策略结合使用。可以使用[管理 | 系统设置 | 设备 | 日程](#)创建日程对象。应用日程对象的特定安全功能或策略（规则）。例如，如果在[管理 | 策略 | 规则 | 访问规则](#)页面添加访问规则，[添加规则](#)对话框将列出所有可用的预定义日程对象以及您使用[设备 | 日程](#)页面创建的日程对象。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。

关于设备 | 日程

名称	星期	时间	开始时间	结束时间	配置	备注
Work Hours	M-T-W-TH-F	08:00-17:00				
After Hours	M-T-W-TH-F	00:00-08:00				
	M-T-W-TH-F	17:00-24:00				
Weekend Hours						
无条目						
Appflow Report Hours						
无条目						
TSR Report Hours						
无条目						
App Visualization Report Hours						
Guest Cycle Quota Update	SU-M-T-W-TH-F-SA	00:00-24:00				
	SU-M-T-W-TH-F-SA	00:00-00:15				
Cloud Backup Hours	SU-M-T-W-TH-F-SA	02:00-03:00				

[管理 | 系统设置 | 设备 | 日程](#)用于创建和管理默认和自定义日程对象，以执行各种 SonicWall 安全设备功能的日程时间。

注：可以修改默认日程，但不能将之删除。

日程表显示了所有的预定义和自定义日程。默认日程包括：

办公时间
下班后
双休日

应用程序流量报告小时数
应用程序可视化报告小时数
TSR 报告小时数

云备份小时数
访客循环配额更新

主题：

- 第 67 页的[添加自定义日程](#)
- 第 68 页的[修改日程](#)
- 第 69 页的[删除自定义日程](#)

添加自定义日程

创建自定义日程的步骤如下：

- 1 转至[管理 | 系统设置 | 设备 | 日程](#)。
- 2 单击添加。将显示添加日程对话框。

日程名称：

日程类型： 单次 循环 混合

单次

起始： 年 月 日 时 分

结束： 年 月 日 时 分

循环

日： 周日 周一 周二 周三
 周四 周五 周六 全部

开始时间： : (24 小时格式)

停止时间： : (24 小时格式)

日程列表：

- 3 在日程名称字段中输入日程的描述性名称。
- 4 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， 单次 下面的字段将变为可用， 循环 下面的字段将变灰。
循环 (默认)	用于在配置的相同小时和星期时段内重复发生的日程（无开始或结束日期）。选择该选项后， 循环 下面的字段将变为可用， 单次 下面的字段将变灰。
混合	用于在配置的开始日期和结束日期之间配置的开始时间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。

重要： 时间必须为 24 小时制，例如 17:00 代表下午 5 点。

5 如果**单次**下的字段可用，请

- 通过在**起始行**的下拉菜单中选择**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。
- 通过在**结束行**的下拉菜单表中选择**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**循环**下的字段可用，

- 则选择星期对应的复选框以应用于日程，或选择**全部**。
- 在**开始时间**字段中，输入日程的开始日时间。
- 在**停止时间**字段中，输入日程的停止日时间。

7 单击**添加**将日程添加到**日程列表**。

8 如需删除：

- 来自**日程列表**的现有日程：
 - 1) 请选择一个日程。
 - 2) 单击**删除**。
- 如需删除现有日程，请单击**全部删除**。

9 单击**确定**。日程表已更新。

修改日程

修改默认和自定义日程的步骤如下：

- 1 转至**管理 | 系统设置 | 设备 | 日程**。
- 2 单击要修改的日程的**编辑**图标。将显示**编辑日程**对话框。

日程名称：

日程类型： 单次 循环 混合

单次

起始：年 月 日 时 分

结束：年 月 日 时 分

循环

日： 周日 周一 周二 周三
 周四 周五 周六 全部

开始时间： : (24 小时格式)

停止时间： : (24 小时格式)

日程列表：

- 3 可以更改日程的任何组成部分，例如时间、类型和 / 或天数，但默认计划的名称不能更改且字段显示为灰色。如需进行更改，请按照第 67 页的[添加自定义日程](#)中的步骤进行。
- 4 单击确定。

删除自定义日程

可以删除自定义日程，但不能删除默认日程。

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 转至[管理 | 系统设置 | 设备 | 日程](#)。
- 2 在日程表中，
 - 如需删除自定义日程，点击其删除图标。
 - 如需删除多个自定义日程，
 - 1) 选择要删除的自定义日程旁边的复选框。删除将变为可用。
 - 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 转至管理 | 系统设置 | 设备 | 日程。
- 2 在日程表中，选中名称列标题旁边的复选框以选中所有自定义日程。删除将变为可用。
- 3 单击删除。

用户管理

- 关于管理用户
- 配置用于管理用户的设置
- 管理身份验证分区
- 配置本地用户和群组
- 管理访客服务
- 管理访客帐户

关于管理用户

- 第 72 页的[关于用户管理](#)
 - 第 73 页的[使用本地用户和群组进行验证](#)
 - 第 76 页的[使用 RADIUS 进行身份验证](#)
 - 第 76 页的[使用 LDAP/Active Directory/eDirectory 验证](#)
 - 第 80 页的[关于单点登录](#)
 - 第 90 页的[安装单点登录代理和/或终端服务代理](#)
 - 第 107 页的[关于多管理员支持](#)
 - 第 108 页的[配置多管理员支持](#)

关于用户管理

i 注：本主题概述了 SonicWall 安全设备的管理功能。

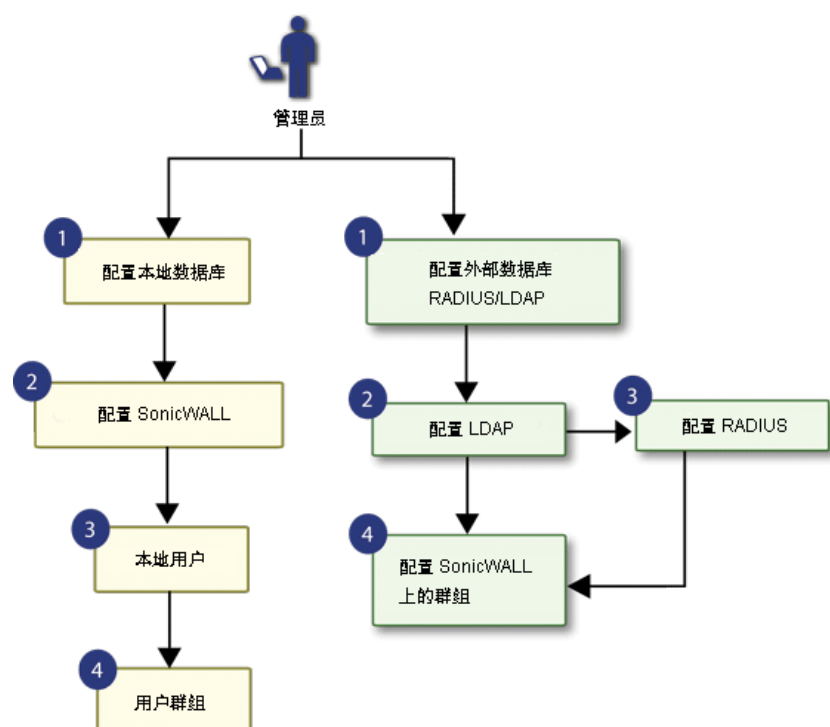
如需以下内容的详细信息和程序	请参阅这些主题
设置用户验证、Web 登录、会话管理、RADIUS 计费 和策略	第 111 页的 配置用于管理用户的设置 。
在具有多个非互连域的环境中为用户身份验证创建 分区	第 165 页的 管理身份验证分区
创建和管理本地用户和本地群组	第 191 页的 配置本地用户和群组 。
设置访客服务和帐户	第 209 页的 管理访客服务 和第 213 页的 管理 访客帐户

SonicWall 安全设备（防火墙）提供了一种本地和远程管理已验证用户的机制。用户级别的身份验证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。请参阅[用户管理拓扑](#)。

用户管理拓扑



主题:

- 第 73 页的[使用本地用户和群组进行验证](#)
- 第 76 页的[使用 RADIUS 进行身份验证](#)
- 第 76 页的[使用 LDAP/Active Directory/eDirectory 验证](#)
- 第 80 页的[关于单点登录](#)
- 第 90 页的[安装单点登录代理和/或终端服务代理](#)
- 第 107 页的[关于多管理员支持](#)
- 第 108 页的[配置多管理员支持](#)

使用本地用户和群组进行验证

主题:

- 第 73 页的[关于用户数据库](#)
- 第 74 页的[关于用户群组](#)

关于用户数据库

防火墙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耗时，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平台支持的用户值表显示的平台而不同。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。

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				
NSA 3600	40,000	1,500	8	SOHO W	250	150	8
NSA 2650	30,000	1,000	8				
NSA 2600	30,000	1,000	8				

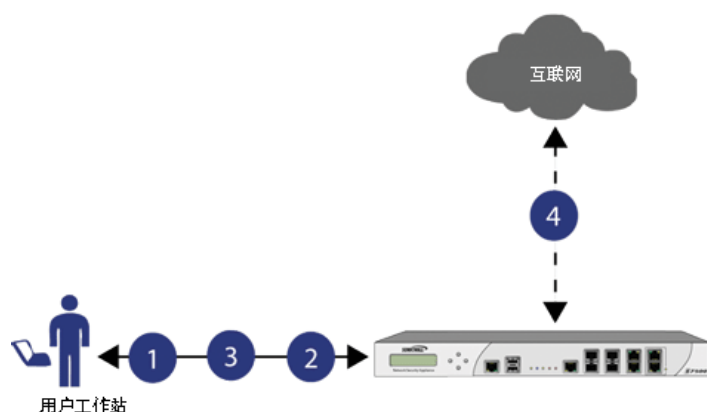
重要： 为达到处理数字的最大效率，SonicWall 推荐

- 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。

关于用户群组

如需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。如需使用 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。请参阅[用户管理：使用本地用户和群组进行验证](#)。

用户管理：使用本地用户和群组进行验证



- 1 用户试图访问此网站。
- 2 SNWL 需要验证用户: 重定向工作站以验证。
- 3 使用证书验证用户。
- 4 SNWL 本地数据库根据用户库权限验证或拒绝访问权限。

SonicOS 管理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：

- 群组成员身份** 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。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“允许”列表。

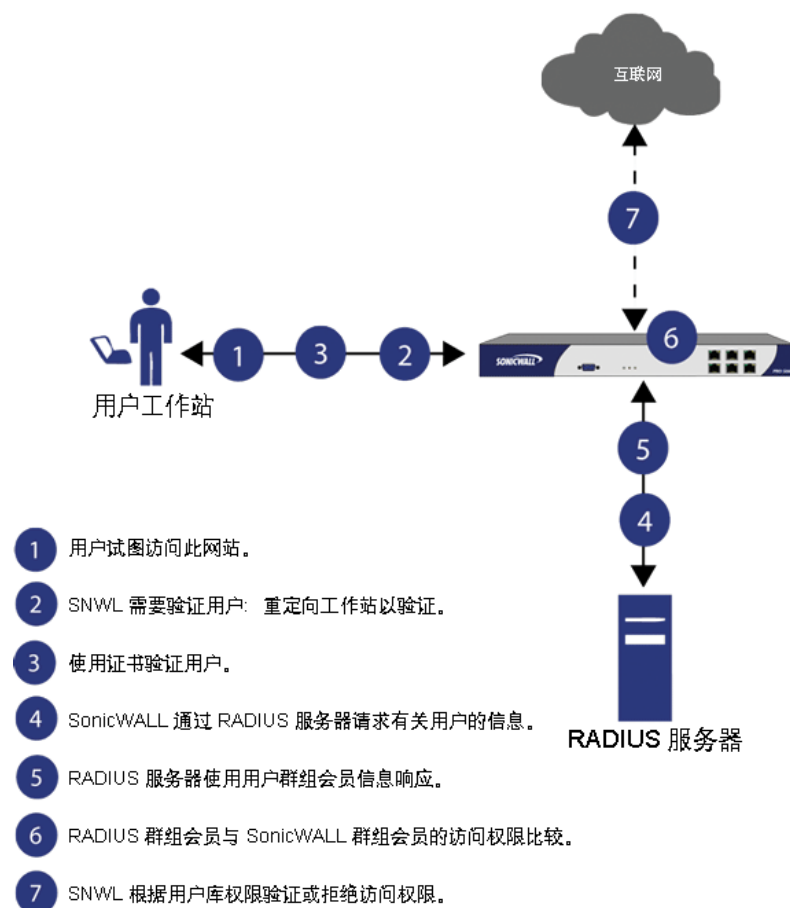
您还可以添加或编辑本地群组。以下是群组的可配置设置：

- 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) 是一项网络协议，它提供了集中式身份验证、授权和计费，SonicWall 安全设备以此来验证尝试访问网络的用户。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。请参阅[用户管理：使用 RADIUS 进行身份验证](#)。

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，如果有许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 SonicOS 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 SonicWall 单点登录和 SonicWall SSO 代理。如需更多信息，请参阅第 80 页的[关于单点登录](#)。

主题：

- 第 77 页的 [LDAP 术语](#)
- 第 77 页的 [SonicOS 中支持的 LDAP 目录服务](#)
- 第 78 页的 [LDAP 用户群组镜像](#)

LDAP 术语

在使用 LDAP 及其变式时，这些术语很有用：

活动目录	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。
特性	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。
cn	“常用名”属性是 LDAP 中很多对象类别的必需组件。
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。
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’
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	存储在 LDAP 目录中的数据。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	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。
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。
ou	“组织单位”属性是大多数 LDAP 方案实施的必需组件。
方案	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。
TLS	传输层安全性，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 支持集成这些 LDAP 方案：

Microsoft Active Directory	Samba SMB
RFC2798 InetOrgPerson	Novell eDirectory
RFC2307 网络信息服务	用户定义的方案

SonicOS 为运行这些协议的目录服务器提供支持：

LDAPv3 (RFC2251-2256, RFC3377)	LDAPv2 (RFC3494)
通过 TLS 的 LDAPv3 (RFC2830)	LDAP 提名 (RFC2251)
带有 STARTTLS 的 LDAPv3 (RFC2830)	

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。可以在 LDAP 服务器上独占管理 LDAP 用户群组，且不需要手动复制防火墙上的配置。用户群组配置定期从 LDAP 服务器上读取和复制到防火墙。

复制到防火墙的 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。

这些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，位于防火墙上的镜像群组也自动删除。
- 您只能编辑 LDAP 服务器上的 LDAP 用户群组名称（及其备注字段）。他们不能编辑防火墙上的镜像 LDAP 用户群组名或其备注字段。备注字段在防火墙上显示为 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。
- 可以在 SonicWall 安全设备上为 LDAP 用户群组配置诸如 VPN、SSL VPN、CFS 策略和 ISP 策略之类的内容（如需有关策略的详细信息，请参阅 SonicOS 策略。

i 注：LDAP 用户群组如果已在任何访问规则、应用程序控制规则或其他策略中配置，则不会将其删除。

- 如果您禁用 LDAP 用户群组镜像，SonicWall 安全设备上的镜像用户群组不会删除。它们已更改，所以可以手动删除它们。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。为原群组的用户赋予 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 安全设备。

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，请参阅第 76 页的[使用 LDAP/Active Directory/eDirectory 验证](#)。

主题：

- 第 79 页的[准备 LDAP 服务器以进行集成](#)
- 第 79 页的[配置 Active Directory 服务器上的 CA](#)

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 越过 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

配置 Active Directory 服务器上的 CA 的步骤如下：

i | **提示：** 如果已安装证书服务，请跳过前五个步骤。

- 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 系统上的证书的信息，请参阅 <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 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。

关于单点登录

主题：

- [第 80 页的什么是单点登录？](#)
- [第 81 页的 SonicWall SSO 的优点](#)
- [第 82 页的平台和支持的标准](#)
- [第 82 页的单点登录的工作方式](#)
- [第 84 页的 SSO 代理的工作方式](#)
- [第 85 页的终端服务代理的工作方式](#)
- [第 86 页的浏览器 NTLM 验证的工作方式？](#)
- [第 87 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。

SonicWall 安全设备提供使用单点登录代理 (SSO 代理) 的 SSO 功能，并提供 SonicWall 终端服务代理 (TSA) 来识别用户活动。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，安全设备查询 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，消息显示要求手动登录到安全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)、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 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。SonicWall SSO 的其他优点包括：

配置简单	用户只需要登录一次，即可获得多个资源的自动访问权限。
改进的用户体验	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。
对用户的透明度	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。
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 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 SonicOS SSO 的所有 SonicWall 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。为使 SonicWall SSO 的所有功能有效，SonicOS 应使用 Directory Connector 3.1.7 或更高版本。

如需结合使用 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。

如需结合使用 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

i 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。如需更多信息，请参阅第 103 页的 [Mac 和 Linux 用户调试](#)。

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。

在这些情况下触发 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（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 and 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，安全设备查询 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）。
- 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。如果找到了对象，则其识别名将用作目录子树以搜索用户对象。例如，如果返回的用户名是 sv/bob，则将搜索包含 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，则将删除已保存的域信息，并且将对域对象进行另一次搜索。

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。安全设备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。与安全设备进行轮询不同，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安全设备终止 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 通常用于无域控制器的情况，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。

如需对 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。若无响应，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。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或服务器上。但是，建议在不同的独立工作站或服务服务器上安装 SSO 代理。如需 SSO 代理的安装说明，请参阅第 90 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。

- i** 注：使用 NetAPI 或 WMI 时，一个 SSO 代理最多可以支持大约 2500 名用户，具体取决于运行它的硬件的性能级别、它在防火墙上的配置方式以及其他依赖于网络的因素。取决于相似的因素，当配置为从域控制器安全日志中读取时，一个 SSO 代理可以通过该机制支持很多用户，最多可能超过 5 万名用户

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。

- i** 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：

- i** 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。如需日志消息的更多信息，请参阅 SonicOS 调查。

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
 已拒绝用户登录 - SSO 代理通信问题
 已拒绝用户登录 - SSO 名称解析失败
 SSO 代理返回的用户名太长
 SSO 代理返回的域名太长

SSO 代理未正确配置，无法允许该用户访问。
 与运行 SSO 代理的工作站通信时出现问题。
 SSO 代理无法解析用户名。
 用户名太长。
 域名太长。

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 90 页的[安装 SonicWall 终端服务代理](#)。

主题：

- 第 85 页的[多 TSA 支持](#)
- 第 85 页的[TSA 消息的加密和会话 ID 的使用](#)
- 第 86 页的[与本地子网的连接](#)
- 第 86 页的[来自终端服务器的非域用户流量](#)
- 第 86 页的[来自终端服务器的非用户流量](#)

多 TSA 支持

如需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[每个型号支持的终端服务代理](#)表所示。

每个型号支持的终端服务代理

SonicWall 网络安全设备	支持的 TS 代理	SonicWall 网络安全设备	支持的 TS 代理	SonicWall 网络安全设备	支持的 TS 代理
SM 9800	512	NSA 6600	256	TZ600	4
SM 9600	512	NSA 5600	128	TZ500/TZ500 W	4
SM 9400	512	NSA 4600	64	TZ400/TZ400 W	4
SM 9200	512	NSA 3600	16	TZ300/TZ300 W	4
		NSA 2650	8		
		NSA 2600	8	SOHO W	4

对于 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）。每个终端服务器都无用户限制。

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，而非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 未“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，请选择探测用户并选中 **NetAPI** 或 **WMI** 对应的单选按钮，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。若无响应，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。

如需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。

i **注：**来自 TSA 的 Ping (ICMP) 流量被识别为非用户流量，但不是系统服务流量。因此，不允许绕过用户验证，并在代理超时后丢弃。为防止 ICMP 流量被丢弃，请在策略 | 规则 > 访问规则页面中添加访问规则，以允许来自终端服务器的 ICMP，而不需要用户身份验证。如需关于访问规则的更多信息，请参阅 SonicOS 策略。

浏览器 NTLM 验证的工作方式？

主题：

- 第 86 页的域用户的 NTLM 验证
- 第 86 页的非域用户的 NTLM 验证
- 第 87 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。如需有关 NTLM 身份验证的更多信息，请参阅第 111 页的[配置用于管理用户的设置](#)。

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。用户群组成员身份是从本地帐户设置而非从 LDAP 设置的，并且包含“Trusted Users”群组的成员身份（因为密码已在本地进行验证）。

如果用户名不匹配本地用户帐户，则用户无法登录。允许受限访问非域名用户选项不适用于通过 NTLM 进行验证的用户。

浏览器中的 NTLM 验证凭据

对于 NTLM 验证，浏览器使用域登录凭据（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防火墙（SonicWall 安全设备）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 <code>network.automatic-ntlm-auth.trusted-uris</code> 条目中（通过在 Firefox 地址栏输入 <code>about:config</code> 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（这可能由于用户无所需的访问权限），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，必须在 **管理 | 策略 > 规则 > 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（如需更多信息，请参阅 SonicOS 策略）。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止用户的 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，也可以选择用户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，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 SonicWall SMA 1000 系列设备配置为外部 RADIUS 计费客户端，其中 SonicWall 防火墙充当 RADIUS 计费服务器。

在远程用户通过 SonicWall SMA 或第三方设备连接时，SMA 或第三方设备向 SonicWall 设备（配置为 RADIUS 计费服务器）发送计费消息。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，SonicWall SMA 或第三方设备向 SonicWall 安全设备发送另一条计费消息，然后使用户注销。

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 88 页的 [RADIUS 计费消息](#)
- 第 88 页的 [SonicWall 与第三方网络设备的兼容性](#)
- 第 89 页的 [代理转发](#)
- 第 89 页的 [非域用户](#)
- 第 89 页的 [IPv6 注意事项](#)
- 第 89 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：

这个请求	发送于
开始	用户登录时。
停止	用户注销时。
临时更新	用户登录会话期间定期。

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。

这些与 SSO 相关的属性在**计费请求**中设置：

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。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。
Framed-IP-Address	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	用户的 IP 地址的字符串表示，由 SMA 等一些设备使用。
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。

SonicWall 与第三方网络设备的兼容性

如需使 SonicWall 安全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：

- 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，但并非必须的。用户名属性必须包含用户的帐户名称，还可包含域或必须包含用户的识别名 (DN)。

代理转发

充当 RADIUS 计费服务器的 SonicWall 安全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。可以通过选择这些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：

- 只有在设置了允许受限访问非域名用户时，用户才可以登录。
- 用户不会成为“Trusted Users”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** IANA 特定端口。SonicWall 安全设备默认监听端口 1813。
- 1646** 一个更旧的非官方标准端口。

可以为 RADIUS 计费端口配置其他端口编号，但 SonicWall 安全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。

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，请参阅第 80 页的[关于单点登录](#)。

主题：

- 第 90 页的[安装 SonicWall SSO 代理](#)
- 第 90 页的[安装 SonicWall 终端服务代理](#)
- 第 92 页的[配置 SonicWall SSO 代理](#)
- 第 97 页的[配置 SonicWall 终端服务代理](#)
- 第 100 页的[单点登录高级功能](#)
- 第 103 页的[配置访问规则](#)
- 第 105 页的[管理从终端服务器使用 HTTP 登录的 SonicOS](#)
- 第 105 页的[查看和管理 SSO 用户会话](#)

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。建议这些工作站或服务器为不同的独立工作站或服务器。SonicWall SSO 代理必须能访问您的防火墙。

如需安装 SonicWall SSO 代理，请参阅 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 必须能访问 SonicWall 安全设备，且安全设备必须能访问 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安全设备的消息。

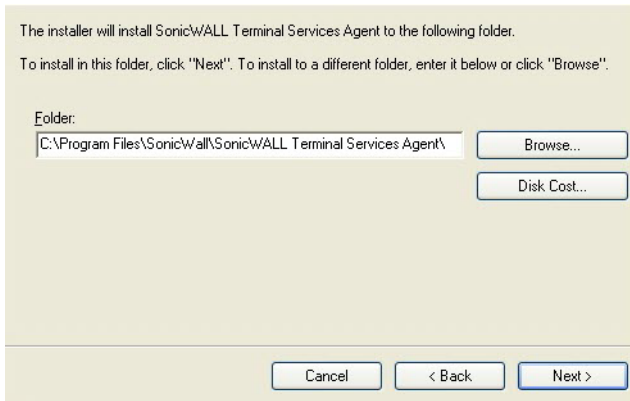
SonicWall TSA 可以从 MySonicWall 免费下载。

安装 SonicWall TSA：

- 1 在 Windows 终端服务器系统上，根据您的计算机下载这些中的一个安装程序：
 - 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。

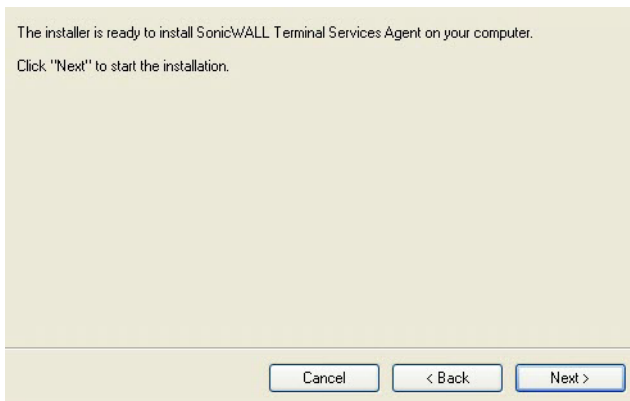
- 2 双击安装程序开始安装。
- 3 在欢迎页面，单击下一步继续。“许可证协议”显示。
- 4 选择我同意。
- 5 单击下一步继续。显示“选择安装文件夹”窗口。



6 选择目标文件夹。如需：

- 使用默认文件夹 C:\Program Files\SonicWall\SonicWall Terminal Services Agent\，请单击下一步。
- 指定一个自定义位置：
 - a) 单击浏览。
 - b) 选择文件夹。
 - c) 单击下一步。

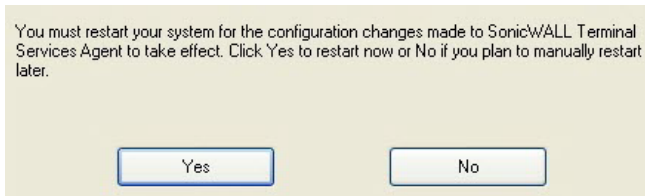
显示“确认安装”窗口。



7 单击下一步开始安装。

8 等待 SonicWall 终端服务代理安装。进度栏指示安装状态。

9 安装完成时，单击关闭退出安装程序。显示一条确认系统重新启动的消息。



10 在启动 SonicWall 终端服务代理之前，您必须重启系统。重启的步骤如下：

- 立即重启，单击是。
- 稍后重启，单击否。在使用 TSA 之前，必须重启系统。

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 Server 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 4.0 或更高版本。.NET Framework 可以从 www.microsoft.com 下载。

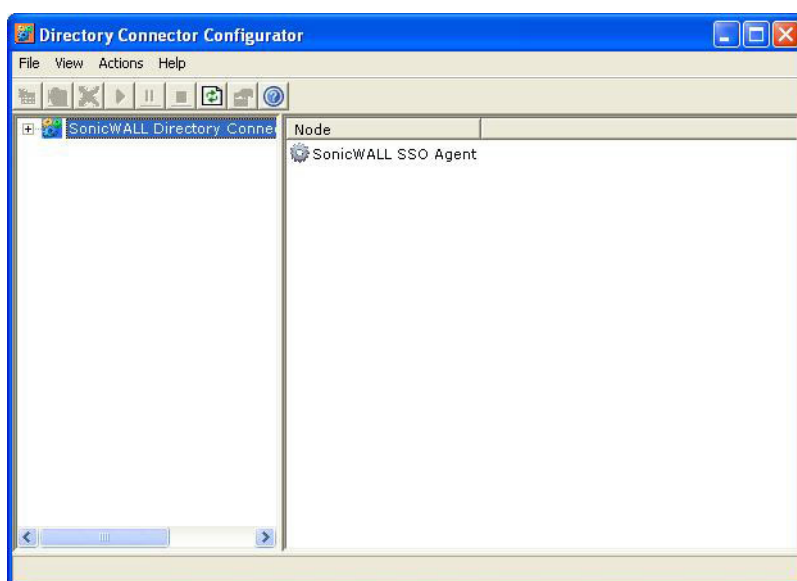
主题：

- 第 92 页的[配置 SonicWall SSO 代理的通讯属性](#)
- 第 96 页的[添加 SonicWall 网络安全设备](#)
- 第 97 页的[在 SonicWall SSO 代理中编辑设备](#)
- 第 97 页的[在 SonicWall SSO 代理中删除设备](#)
- 第 97 页的[在 SonicWall SSO 代理中修改服务](#)

配置 SonicWall SSO 代理的通讯属性

如需配置 SonicWall SSO 代理的通信属性，请执行以下步骤：

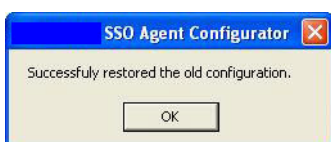
- 1 通过双击桌面快捷方式或转至开始 > 所有程序 > SonicWall > SonicWall Directory Connector > SonicWall 配置工具启动 SonicWall 配置工具。



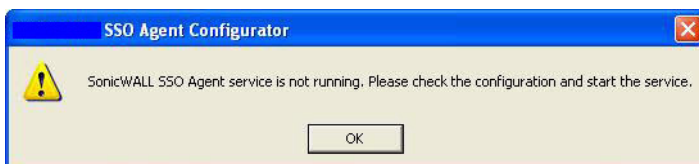
注： 如果未配置默认防火墙的 IP 地址或者配置错误，则会显示弹出窗口。单击是是使用默认的 IP 地址 (192.168.168.168) 或单击否使用当前配置。



如果您单击是，将显示已成功恢复旧配置消息。单击确定。

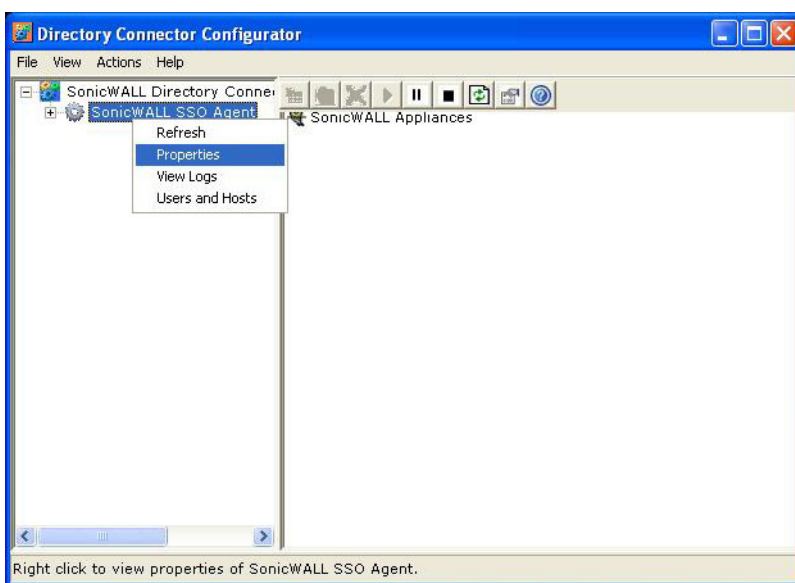


如果单击否或单击是但默认配置不正确，将显示 **SonicWall SSO** 代理服务未运行。请检查配置并启动服务。显示。单击确定。

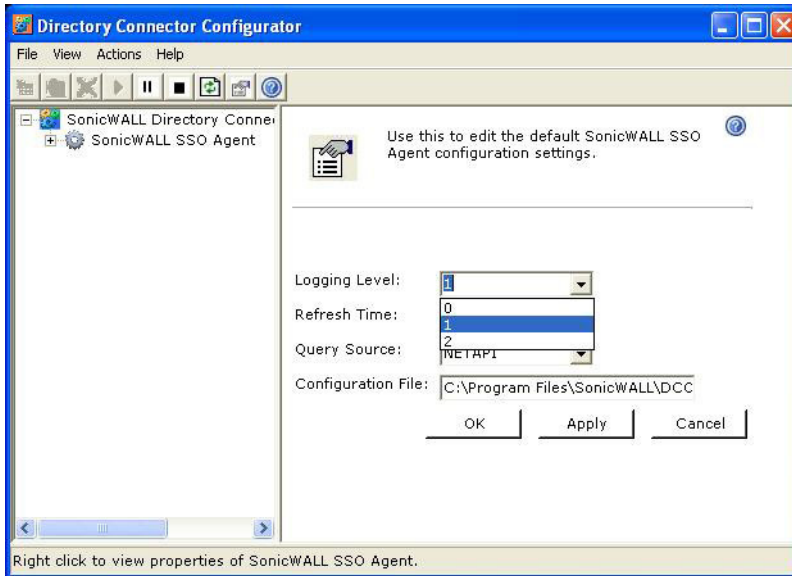


如果显示 **SonicWall SSO** 代理服务未运行。请检查配置并启动服务消息，将默认禁用 SSO 代理服务。启用该服务的步骤如下。

- 1) 在左侧导航面板中，通过单击 + 图标展开 SonicWall Directory Connector 配置工具。
 - 2) 突出显示它下面的 SonicWall SSO 代理。
 - 3) 单击启动图标。
- 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。



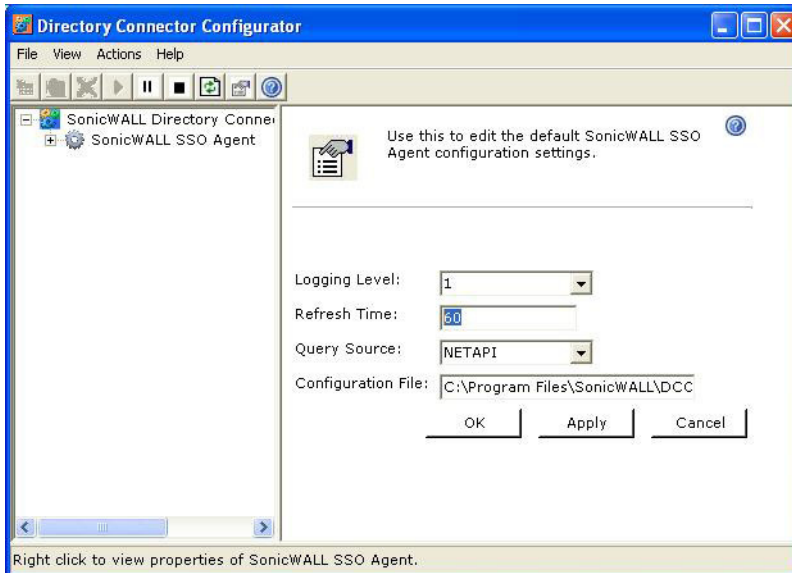
- 3 从记录级别下拉菜单，选择要在 Windows 事件日志中记录的事件级别。



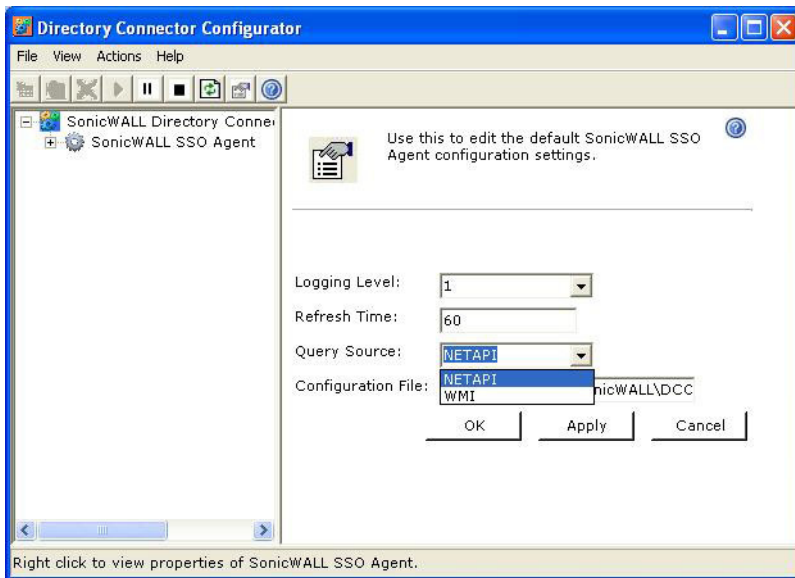
选择以下级别之一：

- 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。这是默认纪录级别。
- 记录级别 2 使用调试级严重性记录来自设备的所有请求。
注：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。



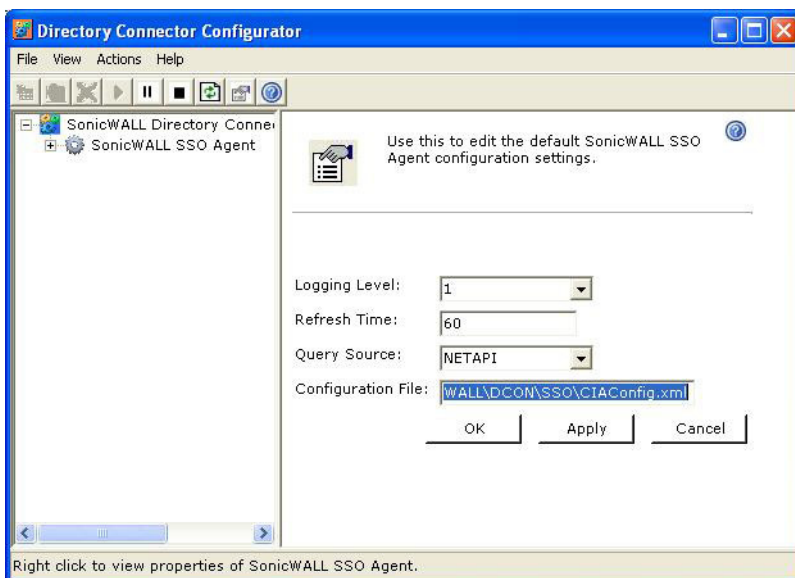
- 5 从查询源下拉菜单中选择 SSO 代理用于与工作站通信的协议：NETAPI 或 WMI。



- 注：** NetAPI 提供更快的性能，但准确率稍低。借助 NetAPI，Windows 会将上次登录报告给工作站，无论用户是否仍然登录。这意味着用户从他的计算机注销后，设备仍然显示用户已登录。如果另一个用户登录到同一台计算机，那时前一个用户从 SonicWall 注销。
- WMI 提供更慢的性能，但准确率更高。

WMI 预安装在 Windows Server 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用户的信息，包括域用户、本地用户和 Windows 服务。

- 在配置文件中，输入配置文件的完整路径。默认路径是 `C:\Program Files\SonicWall\DCCON\SSO\CIAConfig.xml`。



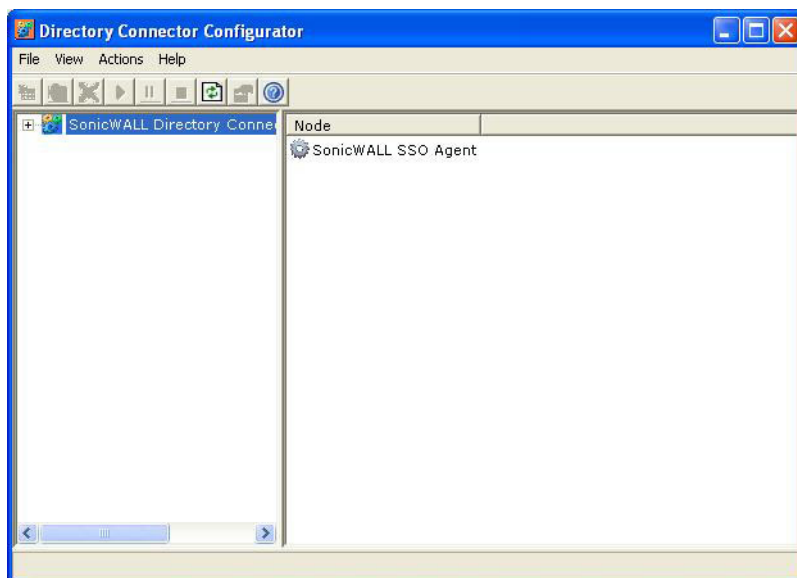
- 单击接受。
- 单击确定。

添加 SonicWall 网络安全设备

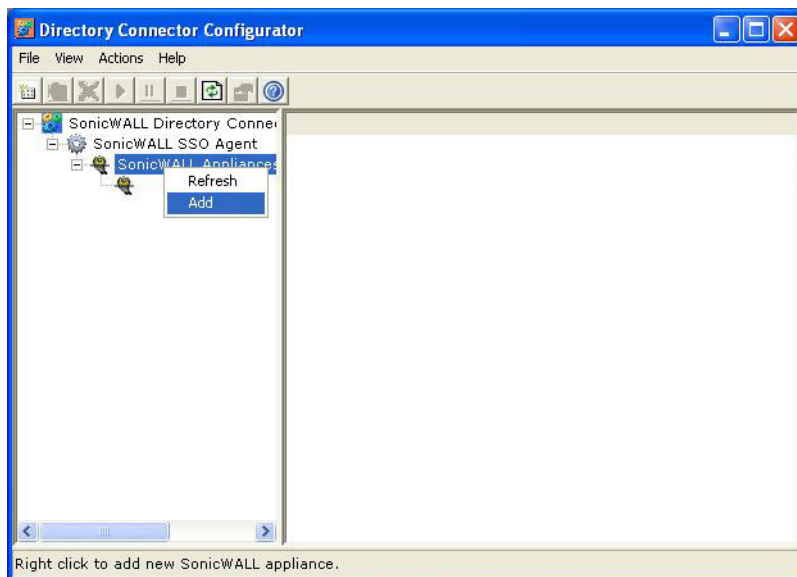
如果在安装期间未添加安全设备，则使用这些说明手动添加或添加附加防火墙。

添加 SonicWall 安全设备的步骤如下：

- 1 启动 SonicWall SSO 代理配置。



- 2 通过单击 + 图标展开左侧列中的 SonicWall Directory Connector 和 SonicWall SSO 代理树。
- 3 右键单击 **SonicWall** 设备。



- 4 选择添加。
- 5 在设备 IP 字段输入 SonicWall 安全设备的设备 IP 地址。
- 6 在设备端口字段输入同一设备的端口。默认端口号是 **2258**。
- 7 在友好名称字段为安全设备指定友好名称。

- 8 您可以
 - 在**共享密匙**字段中输入共享密匙。
 - 单击**生成密匙**以生成共享密匙。

- 9 完成时，单击**确定**。

您的安全设备将显示在左侧导航面板的 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 代理中的安全设备的所有设置，包括 IP 地址、端口编号、友好名称和共享密匙。

在 SonicWall SSO 代理中编辑安全设备的步骤如下：

- 1 从左侧的导航面板中选择安全设备。
- 2 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

删除之前添加在 SonicWall SSO 代理中的安全设备的步骤如下：

- 1 从左侧的导航面板中选择安全设备。
- 2 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、停止和暂停安全设备的 SonicWall SSO 代理服务。

如需：

- 暂停安全设备的服务，请从左侧导航面板中选择安全设备，然后单击**暂停**图标。
- 停止安全设备的服务，请从左侧导航面板中选择设备，然后单击**停止**图标。
- 恢复服务，请单击**启动**图标。

注：在 SonicWall SSO 代理中对安全设备作出配置更改后，您可能收到重启服务的提示。如需重启服务，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。



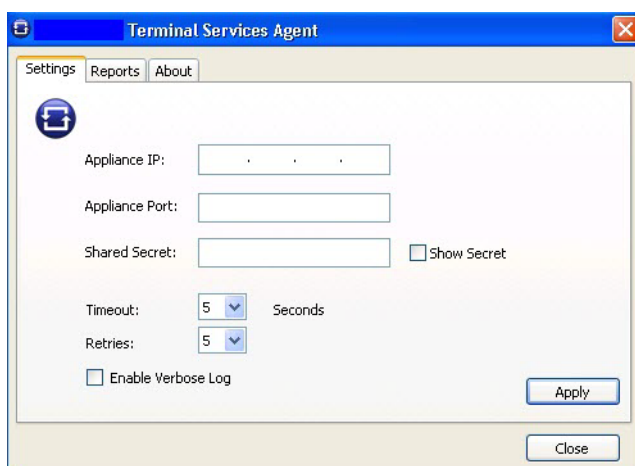
主题：

- 第 98 页的[将 SonicWall 安全设备添加到 SonicWall TSA 设置](#)
- 第 99 页的[创建 SonicWall TSA 故障排除报告](#)
- 第 100 页的[查看 SonicWall TSA 状态和版本](#)

将 SonicWall 安全设备添加到 SonicWall TSA 设置

将 SonicWall 安全设备添加到 SonicWall TSA 的步骤如下：

- 1 双击 SonicWall TSA 桌面图标。随即显示 SonicWall 终端服务代理窗口。



- 2 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**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**下拉菜单中，选择代理在重新发送通知前等待设备回复的秒数。范围为 5 至 10 秒，默认为 5 秒。
- 6 在**重试次数**下拉菜单中，选择代理在未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 如需在日志消息中启用完整的详细信息，请选择**启用详细日志**。
提示： 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**。弹出消息告知 SonicWall TSA 服务已重启，新设置已生效。



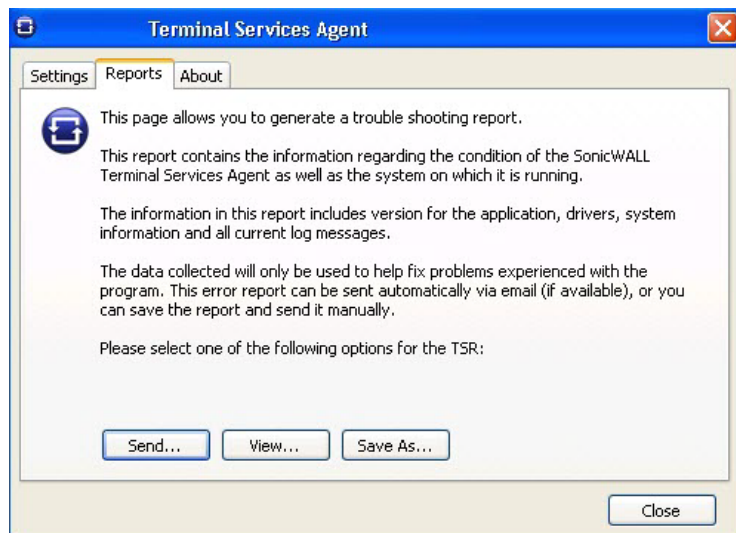
- 9 单击**确定**。

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。随即显示 **SonicWall 终端服务代理** 窗口。
- 2 单击**报告**选项卡。

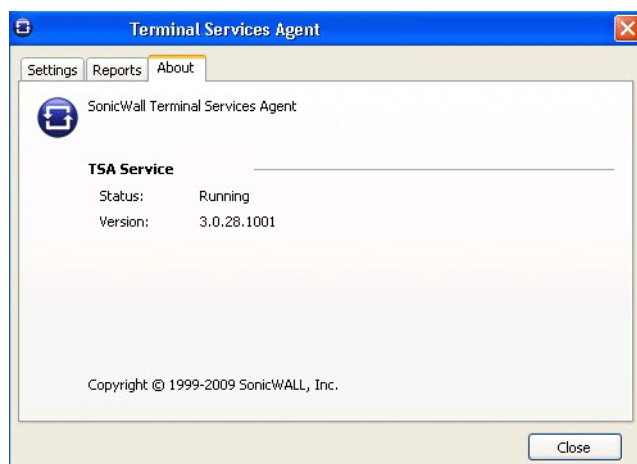


- 3 如需生成 TSR 并
 - 自动向 SonicWall 技术支持发送电子邮件，请单击**发送**。
 - 在默认文本编辑器中进行检查，请单击**查看**。
 - 要将其保存至文本文件，请单击**另存为**。
- 4 完成时，单击**关闭**。

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。随即显示 **SonicWall 终端服务代理** 窗口。
- 2 单击关于选项卡。



- 3 单击关闭。

单点登录高级功能

主题：

- 第 100 页的[关于单点登录](#)
- 第 101 页的[关于高级设置](#)
- 第 101 页的[查看 SSO 鼠标悬停统计](#)
- 第 102 页的[使用 TSR 中的单点登录统计](#)
- 第 102 页的[检查代理](#)
- 第 102 页的[补救措施](#)

关于单点登录

当用户首次尝试通过使用单点登录 (SSO) 的 SonicWall 安全设备发送流量时，安全设备向 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，安全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，或通过在一个单独的 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

在配置 SSO 代理（如需有关配置 SSO 代理的更多信息，请参阅第 143 页的[配置 SonicOS 以使用 SonicWall SSO 代理](#)）时，一次发送的最大请求数目设置可用。

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，则会将有请求置于内部“环形缓冲区”（参阅第 102 页的[使用 TSR 中的单点登录统计](#)和第 101 页的[查看 SSO 鼠标悬停统计](#)）。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

SSO 验证配置对话框提供有关每个代理和所有 SSO 代理的鼠标悬停统计信息。在 SSO 代理页面，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。

如需查看以下内容的统计信息：

- 特定代理，将鼠标悬停在 SSO 代理的统计图标上。
- 所有 SSO 代理，将鼠标悬停在表格下方的统计图标上。

 **提示：**这也适用于终端服务选项卡上的各 TSA。



端口	超时	重试	最大请求	分区	启用
2258	10	6	32	Default	<input checked="" type="checkbox"/>

SSO 统计

所有 SSO 验证尝试:	0
验证尝试成功:	0
验证尝试失败, 输出错误:	0, 0
所有用户鉴别请求发送:	0
用户鉴别请求成功:	0
用户鉴别请求输出域用户:	0
用户鉴别请求输出本地用户:	0
用户鉴别请求表明非 Windows PC:	0
用户鉴别尝试返回无名称:	0
失败用户鉴别尝试 (超时, 错误):	0, 0
在固定时间轮询的用户:	0
用户轮询成功:	0
用户轮询失败 (无用户名, 超时, 错误):	0, 0, 0
所有 SSO pings 尝试:	0
SSO pings 成功, 超时:	0, 0

确定 取消 [单击重置](#)

如需关闭统计显示，请单击关闭。

如需清除所有显示值，请单击单击重置。

使用 TSR 中的单点登录统计

技术支持报告 (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。在调查 > 工具 > 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，或显示任何环形缓冲区溢出，则表示未能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，请参阅**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 来自设备而非 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，请参阅第 103 页的 **Mac 和 Linux 用户调试**。

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 TSR 报告中的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，请参阅上文的**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来降低在 **SSO 验证对话框的用户部分** 中配置的轮询速率。这将减少代理的负载，但可能检测注销的速度会变慢。

注：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。

配置访问规则

启用 SonicWall SSO 会影响 SonicOS 管理界面的 **规则 > 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 **规则 > 访问规则** 下设置的规则，并自动应用规则。

主题：

- [第 103 页的自动生成的 SonicWall SSO 规则](#)
- [第 103 页的 Mac 和 Linux 用户调试](#)
- [第 104 页的允许从终端服务器的 ICMP Ping](#)
- [第 104 页的关于访问规则](#)

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，各配置的代理都具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，访问规则和 NAT 策略将添加到各适用区域。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 用户调试

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，安全设备使用 SonicWall SSO 自动验证 Windows 域中的用户。这允许用户通过安全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 Windows 域中使用 Samba 的 Linux PC 或 Mac 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：

- 为了对 Linux/Mac 用户使用 SonicWall SSO，必需配置 SonicWall SSO 代理使用 **NetAPI** 而非 **WMI** 获得来自用户机器的用户登录信息。
- 为了使 Samba 能接收和响应来自 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。

i | 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，但未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。

为避免这些问题，在 **规则 > 访问规则** 页面上配置访问规则（如需有关配置访问规则的更多信息，请参阅 SonicOS 策略）时，**不要调用单点登录来验证用户** 选项可用。只有在启用了 SonicWall SSO 时，此选项才可见。如果选中该选项，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，将源下拉菜单设为包含 Mac 和 Linux 系统的 IP 地址的地址对象。

对于使用 CFS 的情况，可将启用该选项的规则添加到 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。

i | 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，所以安全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。


关于访问规则

访问规则使您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从 **规则 > 访问规则** 页面设置的规则，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安全设备远程管理的网络管理工具。**规则 > 访问规则** 页面提供了可排序的访问规则管理界面。

i | 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，请参阅 SonicOS 策略。

管理从终端服务器使用 HTTP 登录的 SonicOS

SonicWall 安全设备通常根据一个 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安全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。这在安全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安全设备。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）。取而代之的是转至显示由于网络问题，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。

主题：

- 第 105 页的[注销 SSO 用户](#)
- 第 106 页的[配置附加 SSO 用户设置](#)
- 第 106 页的[使用数据包监控查看 SSO 和 LDAP 消息](#)
- 第 106 页的[捕获 SSO 消息](#)
- 第 106 页的[捕获 LDAP 越过 TLS 消息](#)

注销 SSO 用户

监控 | 当前状态 > 用户会话 > 活动用户页面在安全设备上显示用户会话。如需有关查看用户设置以及如何注销用户的信息，请参阅 SonicOS 监控。

 **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。

在用户会话下限制用户会话的选项适用于使用 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

调查 | 工具 > 数据包监控 中的“数据包监控”功能提供选项，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。如需更多信息，请参阅 SonicOS 调查。

捕获 SSO 消息

如需有关使用数据包监控的更多信息，请参阅 SonicOS 调查。

捕获发送至或来自 SSO 验证代理的解密消息的步骤如下：

- 1 转到调查 | 工具 > 数据包监控。
- 2 在十六进制转储部分下，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。
- 4 单击监控中间数据包。
- 5 选择监视中间解码单点登陆代理消息。
- 6 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 消息在工具 > 数据包监控 页面显示为完全解码的形式。

捕获 LDAP 越过 TLS 消息

捕获解密的 LDAP 越过 TLS (LDAPS) 数据包的步骤如下：

- 1 转到调查 | 工具 > 数据包监控。
- 2 在十六进制转储部分下，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。
- 4 单击监控中间数据包。
- 5 选择监视中间解码 LDAP 越过 TLS 的数据包。
- 6 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。已捕获的 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 客户端通过防火墙的 LDAP 越过 TLS 连接。

关于多管理员支持

可以按照第 191 页的[配置本地用户和群组](#)中所述配置多个管理员配置文件。

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 LDAP 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 管理员** 和/或 **SonicWall 只读管理员**，并将相关的用户分配到这些群组。

注： 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。

主题：

- 第 107 页的[抢占管理员](#)
- 第 108 页的[使用管理员权限登录](#)

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：

确定要强占已有的管理员？

管理员已登录进行配置。

如果您要继续管理 SonicWall 在配置模式下，管理员的会话将被丢弃转至非配置模式。

目前的配置模式管理员 admin，登录通过 GUI (192.168.95.233)。

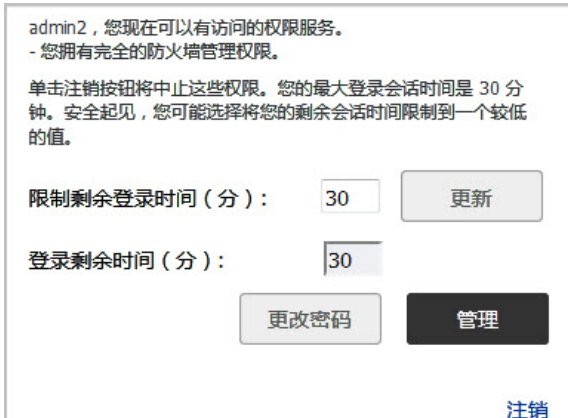
单击“配置”以抢占该用户并继续处于配置模式，“非配置”以切换到非配置模式，底部的链接进行取消。

这个消息给三个选项：

配置	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。
非配置模式	您以非配置模式登录 SonicWall 安全设备。当前管理员的会话不受干扰。
请勿开始管理	返回到登录屏幕。

使用管理员权限登录

在以拥有管理员权限的用户（非管理员用户）身份登录时，将显示用户登录状态消息。



The screenshot shows a user interface for an administrator user named 'admin2'. The text reads: 'admin2, 您现在可以有访问的权限服务。 - 您拥有完全的防火墙管理权限。' Below this, it says: '单击注销按钮将中止这些权限。您的最大登录会话时间是 30 分钟。安全起见，您可能选择将您的剩余会话时间限制到一个较低的值。' There are two input fields for time limits: '限制剩余登录时间 (分):' with a value of '30' and a '更新' button; and '登录剩余时间 (分):' with a value of '30'. At the bottom, there are two buttons: '更改密码' and '管理'. A '注销' link is located at the bottom right of the interface.

如需转至 SonicWall 管理界面，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 SonicWall 安全设备的目的而非允许安全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。如需禁用弹出窗口，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**选项。

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对话框），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**选项。
- 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选项。
- 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。

配置多管理员支持

主题：

- 第 109 页的**配置附加管理员用户配置文件**
- 第 109 页的**使用 LDAP 和 RADIUS 时在本地配置管理员**
- 第 107 页的**抢占管理员**
- 第 108 页的**使用管理员权限登录**
- 第 109 页的**验证多管理员支持配置**
- 第 110 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

像配置其他本地用户一样配置其他管理员，然后将其添加到适当的本地群组：

此群组	授予用户
限制的管理员	受限制的管理员配置权限。
SonicWall 管理员	完全管理员配置权限。
SonicWall 只读管理员	仅有查看整个管理界面的权限。

有关如何配置本地用户和本地群组，请参阅第 191 页的[配置本地用户和群组](#)。

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 SonicWall 安全设备，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 LDAP 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 管理员** 和/或 **SonicWall 只读管理员**，并将相关的用户分配到这些群组。

注：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。

如需了解如何在使用 LDAP 或 RADIUS 时配置管理员，请参阅第 191 页的[配置本地用户和群组](#)。

验证多管理员支持配置

可以在用户 > 本地用户和群组 > 本地群组页面查看具有管理员和只读管理员权限的用户帐户。

#	名称	访客服务	管理员	VPN 访问	注释	配置
1	Audit Administrators		审核			
2	Content Filtering Bypass					
3	Cryptographic Administrators		Crypto			
4	Everyone					
5	Guest Administrators		访客			
6	Guest Services					
7	Limited Administrators		受限制的			
8	SonicWALL Administrators		完全管理员权限			
9	SonicWALL Read-Only Admins		只读			
10	SSLVPN Services					
11	System Administrators		系统			
12	Trusted Users					

可以通过查看管理界面右上角的**模式**来确定所处的配置模式：

模式：配置

进行更改时，状态栏显示：

状态：配置已更新。

模式：非配置

当尝试进行更改时，状态栏将显示：

状态：出错：在目前模式下不允许

查看多管理员相关的日志消息

生成这些事件的日志消息：

- 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）。

配置用于管理用户的设置

- 第 111 页的[用户 | 设置](#)
 - 第 112 页的[配置用户验证和登录设置](#)
 - 第 120 页的[配置用户会话](#)
 - 第 129 页的[配置 RADIUS 身份验证](#)
 - 第 134 页的[配置 SonicWall 以支持 LDAP](#)
 - 第 143 页的[配置 SonicOS 以使用 SonicWall SSO 代理](#)

用户 | 设置



身份验证 Web 登录 身份验证旁路 用户会话 计费 自定义

用户验证设置

用户验证方法：

单点登录方法：
 SSO 代理
 终端服务代理
 RADIUS 计费
 浏览器 NTLM 验证

用户名区分大小写
 强制登录唯一性
 更改密码后必须重新登录
 显示上次登录以来的用户登录信息

一次性密码：
 一次性密码的限定密码复杂度
 一次性密码电子邮件格式： 文本 HTML
 一次性密码格式：
 一次性密码长度： - 字符 密码强度：好

在管理|系统设置|用户|设置，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 112 页的[配置用户验证和登录设置](#)
- 第 120 页的[配置用户会话](#)

- 第 129 页的[配置 RADIUS 身份验证](#)
- 第 134 页的[配置 SonicWall 以支持 LDAP](#)
- 第 143 页的[配置 SonicOS 以使用 SonicWall SSO 代理](#)

配置用户验证和登录设置

重要：完成用户 | 设置页面的配置后，单击接受。

主题：

- 第 112 页的[用户验证设置](#)
- 第 115 页的[用户 Web 登录设置](#)
- 第 116 页的[身份验证旁路设置](#)
- 第 121 页的[用户会话设置](#)
- 第 122 页的[SSO 验证用户的用户会话设置](#)
- 第 123 页的[用于 Web 登录的用户会话设置](#)
- 第 125 页的[登录后可接受使用策略](#)
- 第 127 页的[自定义登录页面](#)

用户验证设置

身份验证
Web 登录
身份验证旁路
用户会话
计费
自定义

用户验证设置

用户验证方法：配置 RADIUS
LDAP 配置 LDAP

单点登录方法：配置 SSO
 SSO 代理 ✔
 终端服务代理 ✘
 RADIUS 计费 ✘
 浏览器 NTLM 验证 ✘

用户名区分大小写

强制登录唯一性

更改密码后必须重新登录

显示上次登录以来的用户登录信息

一次性密码：

一次性密码的限定密码复杂度

一次性密码电子邮件格式：● 文本 ○ HTML

一次性密码格式：字符

一次性密码长度：10 - 10 字符 密码强度：好

配置用户验证设置的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 设置。
- 2 如果分区：
 - 未启用，请转至 [步骤 4](#)。
 - 已启用，显示每个身份验证分区的单独设置（仅适用于特定设置）选项。选择选项。显示选分区设置选项。

用户验证设置

每个身份验证分区的单独设置 (仅适用于特定设置)

Default 2

分区设置 Default

用户验证方法: RADIUS + 本地用户

单点登录方法: SSO 代理, 终端服务代理, RADIUS 计费, 浏览器 NTLM 验证

配置 RADIUS 配置 LDAP 配置 SSO

用户名区分大小写

- 3 对于每个分区，继续执行 [步骤 4](#)。
- 4 从用户验证方法选择您的网络使用的用户帐户管理类型：

本地用户 使用 [用户 | 本地用户和群组](#) 页面在安全设备中配置本地数据库中的用户。如需有关使用本地数据库进行身份验证和详细配置描述的信息，请参阅 [这些部分](#)，请参阅第 [73](#) 页的 [使用本地用户和群组进行验证](#)。

RADIUS 您有 1,000 名以上用户或者想增加额外的安全层验证访问安全设备的用户。如果您选择 RADIUS 进行用户验证，用户必须使用 HTTPS 登录安全设备以加密发送至安全设备的密码。如果用户尝试使用 HTTP 登录安全设备，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 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，请参阅第 76 页的[使用 RADIUS 进行身份验证](#)。

如需详细的配置说明，请参阅第 129 页的[配置 RADIUS 身份验证](#)。

RADIUS + 本地用户

想要使用 RADIUS 和安全设备本地用户数据库进行身份验证。

LDAP

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，请参阅第 76 页的[使用 LDAP/Active Directory/eDirectory 验证](#)。

如需详细的配置说明，请参阅第 78 页的[将 LDAP 集成到 SonicWall 安全设备](#)。

LDAP + 本地用户

想要使用 LDAP 和安全设备本地用户数据库进行身份验证。

- 5 对于单点登录方法，选择以下一种方法：

i | **注：**如果未使用单点登录验证用户，请勿选择任何这些选项。

SonicWallSSO 代理

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。如需详细的 SSO 配置说明，请参阅第 100 页的[关于单点登录](#)。

终端服务代理

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)。

仅浏览器 NTLM 验证

如果您不使用 SSO 代理或 TSA 验证 Web 用户。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](#)。

RADIUS 计费

想要网络访问服务器 (NAS) 向计费服务器发送用户登录会话计费信息。

- 6 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。
- 7 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。此选项适用于本地用户和 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选项。
- 8 如需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](#)。默认情况下未选中该选项。
- 9 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](#)。

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[调查 | 日志 | 事件日志](#)中。如需有关日志的更多信息，请参阅 SonicOS 调查。

- 10 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。

i | **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

身份验证 **Web 登录** 身份验证旁路 用户会话 计费 自定义

用户 Web 登录设置

显示页面验证时间（分钟数）：

重定向浏览器到该应用程序通过：

- 接口 IP 地址
- 使用可逆 DNS 查找接口 IP 地址的域名 显示缓存
- 配置的域名
- 来自管理证书的名称

当用户完成登录以后从 HTTPS 导向到 HTTP

允许使用 RADIUS CHAP 模式的 HTTP 登录

允许框架中的身份验证页面

配置用户 Web 登录设置的步骤如下：

1 转至管理 | 系统设置 | 用户 | 设置。

2 单击 Web 登录。

3 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。

4 从重定向浏览器到该应用程序通过中选择选项，用于确定如何初次将用户的浏览器重定向至 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。

单击显示缓存验证用于重定向用户浏览器的域名（DNS 名称）。

- 接口 IP 地址
- 使用可逆 DNS 查找接口 IP 地址的域名 显示缓存
- 配置的域名
- 来自管理证书的名称

接口主机名反查 DNS 缓存			
接口	IP 地址	DNS 名称	TTL (秒数)

- 配置的域名 - 选择此选项可重定向到在系统设置 | 设备 > 基本设置上配置的域名。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：此选项仅当在系统设置 | 设备 > 基本设置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。在系统设置 | 设备 > 基本设置上配置域名。

① **注：**只有在系统设置 | 设备 > 基本设置的 **Web 管理设置**部分中为 HTTPS 管理导入了证书时，此选项才可用。请参阅第 16 页的**配置基本设置**。

① **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。

如需进行 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，而非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，而非 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。

- 5 如果您希望用户在通过 HTTPS 登录后通过 HTTP 经由安全设备连接到网络，请选择在用户登录时，将用户从 HTTPS 重定向到 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。
- 6 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。

① **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。

① **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。

- 7 对于强制网络门户访客身份验证，如需允许验证页面在网络门户主机页面中显示为框架，请选择允许框架中的身份验证页面。默认情况下未选中该选项。
- 8 单击接受。

身份验证旁路设置

SonicOS 访客服务允许访客用户通过网络直接访问互联网，而无需访问受保护的网路。为此，SonicOS 使用用户计算机的 IP 地址。

当访客用户流量通过网络路由器时，使用 IP 地址作为标识符非常有用，因为这将源 MAC 地址更改为路由器的源 MAC 地址。但是，用户 IP 地址通过的时候保持不变。

如果仅使用 MAC 地址进行标识，则到达安全设备后，同一路由器后面的两个客户端将具有相同的 MAC。当一个客户端得到验证时，来自另一个客户端的流量也将被视为已验证，并绕过访客服务验证。

通过使用客户端 IP 地址进行标识，路由设备后面的所有访客客户端都需要独立进行验证。

主题:

- 第 117 页的将 URL 添加到身份验证旁路
- 第 118 页的配置自动配置
- 第 120 页的转化通配符匹配的 URL
- 第 120 页的转化网络

将 URL 添加到身份验证旁路

在访问规则中添加 HTTP URL 用户身份验证旁路的步骤如下:

- 1 转至系统设置 | 用户 | 设置 > 身份验证旁路。

身份验证 Web 登录 身份验证旁路 用户会话 计费 自定义

身份验证旁路

允许这些 HTTP URL 绕过访问规则中的用户验证：

--无--

添加 编辑 删除 自动配置

- 2 单击添加。显示添加 URL 弹出窗口。

添加 URL

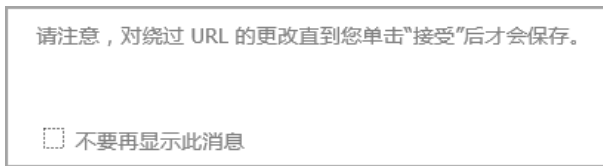
输入 URL:

对于通配符匹配, 前缀 '*' 或者后缀 '...', 例如: *.windowsupdate.com...

允许访问一个文件, 前缀 '*/', 例如: */wpad.dat

确定 取消

- 3 在输入 URL 字段中输入 URL。
- 4 单击确定。显示弹出确认消息。



- 5 单击确定。
- 6 添加完 URL 后，单击接受。

配置自动配置

绕过用户验证的自动配置的 URL 在防火墙规则中被那些允许通过（仅来自同一个 IP 地址）的流量访问，否则将被规则阻止，那些规则需要用户验证和记录已访问的目的地址。

配置自动配置的步骤如下：

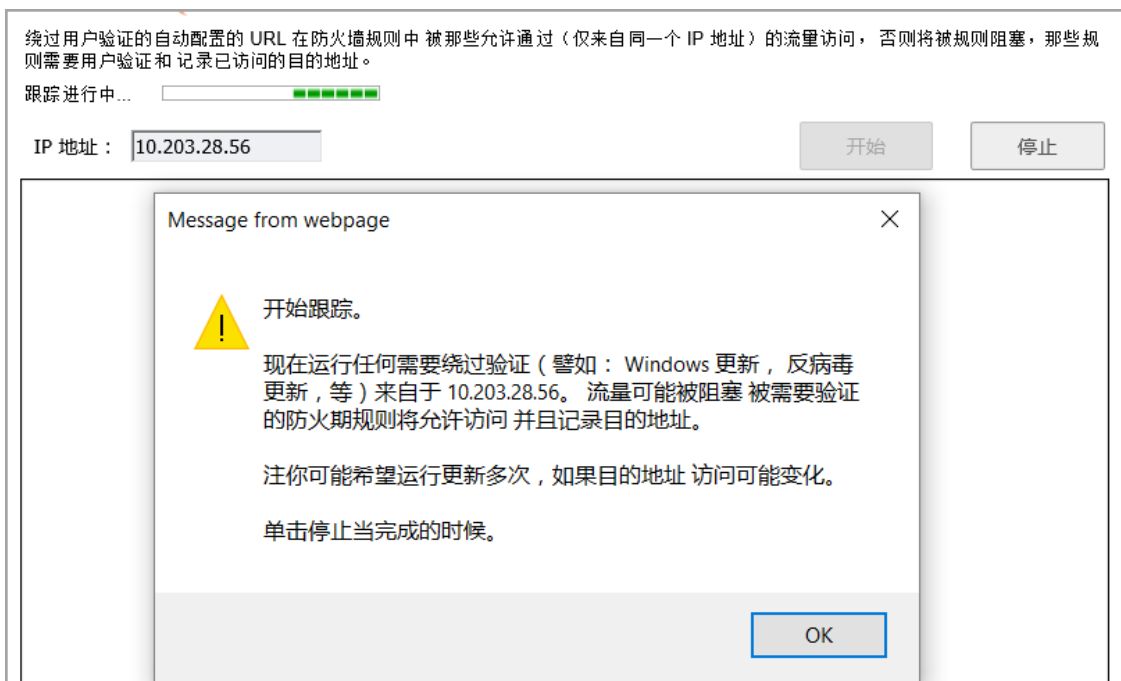
- 1 转至系统设置 | 用户 | 设置 > 身份验证旁路。



- 2 单击自动配置。随即显示绕过自动配置的用户验证策略对话框。



- 3 在 **IP 地址** 字段中输入源 IP 地址。开始变为可用。
- 4 单击开始。显示正在跟踪指示器和跟踪已开始消息。



- 5 单击确定。

转化通配符匹配的 URL

旁路验证支持通配符匹配。这样可以将一个或多个跟踪的 URL 转化为与当前选定的所有 URL 匹配的单个通配符。

注：所选的 URL 必须位于同一个域中。

转化网络

Windows 更新会通过 HTTPS 访问一些目的地，而那些目的地只能通过 IP 地址跟踪。然而，每次访问的实际 IP 地址可能不同，因此，与其为每个此类 IP 地址设置绕过验证，不如对该网络中的所有 IP 地址设置允许 HTTPS 绕过。

转化为网络旁路允许将跟踪的 HTTPS 目标 IP 地址转换为以下之一：

- 类 B（16 位）网络（默认）
- 类 C（24 位）网络

配置用户会话

身份验证 | Web 登录 | 身份验证旁路 | **用户会话** | 计费 | 自定义

用户会话设置

不活动超时 (分钟数):

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:

用于未在其上识别用户的连接的日志:

如果 SSO 未能识别用户:	<input type="radio"/> 不记录任何用户名	<input checked="" type="radio"/> 记录用户名: <input type="text" value="알 수 없음(SSO 실패)"/>
对于绕过 SSO 的连接:	<input type="radio"/> 不记录任何用户名	<input checked="" type="radio"/> 记录用户名: <input type="text" value="SSO 바이패스"/>
对于源自外部的连接:	<input checked="" type="radio"/> 不记录任何用户名	<input type="radio"/> 记录用户名: <input type="text" value="알 수 없음(외부)"/>
对于其他未识别的连接:	<input checked="" type="radio"/> 不记录任何用户名	<input type="radio"/> 记录用户名: <input type="text" value="알 수 없음"/>

对于注销时的任何剩余用户连接:

由于不活动而注销时:	<input type="text" value="使它们处于活动状态"/>	对于需要用户验证的连接:	<input type="text" value="使它们处于活动状态"/>
在活动/报告的注销时:	<input type="text" value="终止它们"/>	对于其他连接:	<input type="text" value="在以下时间后终止..."/> <input type="text" value="15"/> 分钟

SSO 验证用户的用户会话设置

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

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

在以下时间 (分钟) 后使非活动用户超时:

用于 Web 登录已验证用户的用户会话设置

启用登录会话限制

登录会话限制 (分钟数):

显示用户登录状态窗口

用户登录状态窗口发送心跳时间间隔 (秒数):

启用断开连接的用户检测

用户登录状态窗口心跳超时 (分钟数):

在同一个窗口打开用户的登录状态窗口而不是以弹出方式

主题：

- 第 121 页的[用户会话设置](#)

用户会话设置

用户会话设置

不活动超时 (分钟数) :

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 :

用于未在其上识别用户的连接的日志 :

如果 SSO 未能识别用户 :	<input type="radio"/> 不记录任何用户名	<input checked="" type="radio"/> 记录用户名 : <input type="text" value="알 수 없음(SSO 실패)"/>
对于绕过 SSO 的连接 :	<input type="radio"/> 不记录任何用户名	<input checked="" type="radio"/> 记录用户名 : <input type="text" value="SSO 바이패스"/>
对于源自外部的连接 :	<input checked="" type="radio"/> 不记录任何用户名	<input type="radio"/> 记录用户名 : <input type="text" value="알 수 없음(외부)"/>
对于其他未识别的连接 :	<input checked="" type="radio"/> 不记录任何用户名	<input type="radio"/> 记录用户名 : <input type="text" value="알 수 없음"/>

对于注销时的任何剩余用户连接 :

由于不活动而注销时 :	<input type="text" value="使它们处于活动状态"/>	对于其他连接 :	<input type="text" value="使它们处于活动状态"/>
在活动/报告的注销时 :	<input type="text" value="终止它们"/>	在以下时间后终止... :	<input type="text" value="15"/> 分钟

如需配置适用于通过安全设备验证的所有用户的设置，请执行以下步骤：

- 1 在不活动超时（分钟数）字段中指定安全设备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非注销用户，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）
i | 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 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 ^a	对于其他连接 ^b
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）

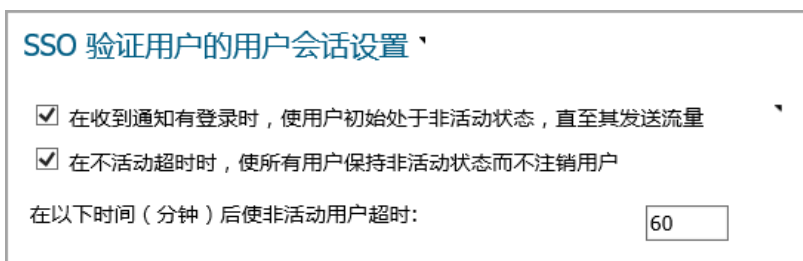
a. 适用于通过仅允许特定用户的访问规则的连接。

b. 适用于无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，无法确定用户是否仍登录到该域/计算机
- 用户主动注销或将注销情况报告给 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



如需指定处理不活动的 SSO 验证用户的方法，请执行以下步骤：

- 1 如需使已通过 SSO 机制为 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 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。为了使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，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设置。
- 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。

i 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

用于 Web 登录已验证用户的用户会话设置

启用登录会话限制

登录会话限制（分钟数）：

30

显示用户登录状态窗口

用户登录状态窗口发送心跳时间间隔（秒数）

120

启用断开连接的用户检测

用户登录状态窗口心跳超时（分钟数）

10

在同一个窗口打开用户的登录状态窗口而不是以弹出方式

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 登录登录到安全设备的时间。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。

i | 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。

i | 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安全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，请参阅第 108 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，请参阅第 191 页的配置本地用户和群组。

- 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 - 让安全设备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设置。
 - 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，而非弹出窗口。

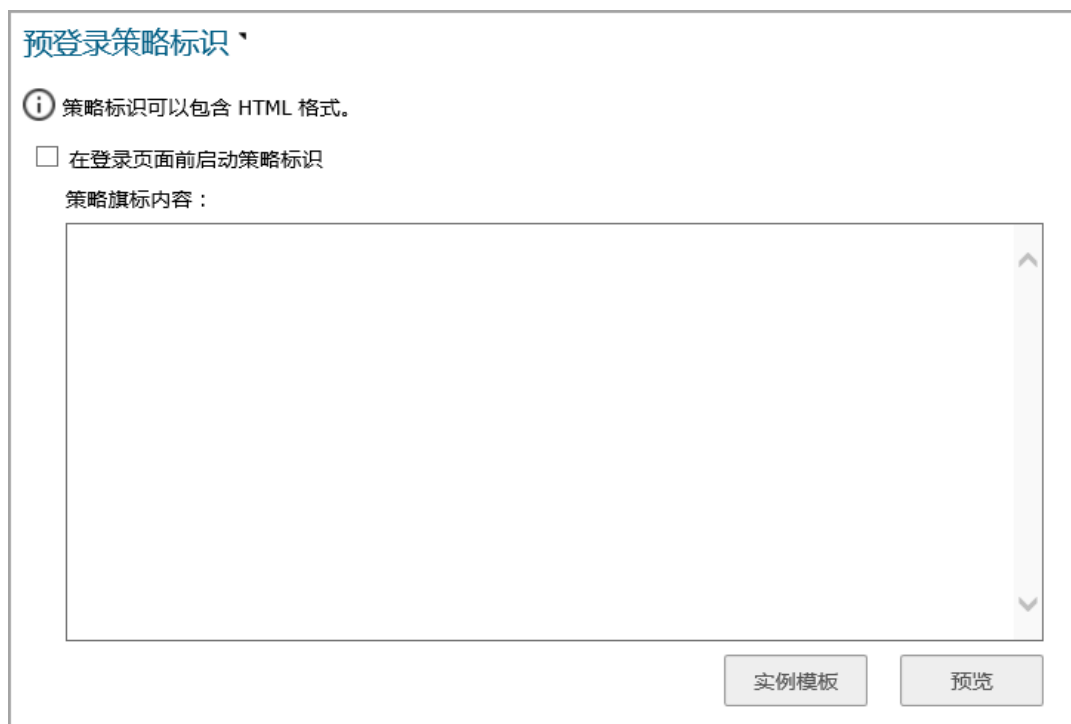
自定义

主题：

- 第 124 页的预登录策略标识

预登录策略标识

在本部分中，可以创建 Web 登录之前在窗口中以标识形式呈现给所有用户的策略声明。策略标识可以包括 HTML 格式。



创建预登录策略标识的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 设置。
- 2 单击自定义。
- 3 滚动到预登录策略标识部分。
- 4 在预登录策略标识部分，选择在登录页面前启动策略标识。默认情况下未选中该选项。
- 5 在策略旗标内容字段中，输入策略文本。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。

i | 提示：单击实例模板将为策略标识窗口创建预定义格式的 HTML 模板；请参阅第 124 页的实例模板。

- 6 单击接受。

主题：

- 第 126 页的实例模板
- 第 125 页的预览消息

实例模板

单击实例模板以使用默认的 AUP 模板来填写内容，您可对此进行更改：

```
<font face=arial size=3>
```

```
<center><b><i>欢迎</i></b></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>
```

仅当您希望接受这些条款并继续进行操作是单击“我接受”，否则选择“取消”。

预览消息

单击预览以显示将要想用户展示的 AUP 消息。

登录后可接受使用策略

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安全设备访问网络或访问互联网时同意可接受的使用策略。



登录后可接受使用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。单击实例模板将为 AUP 窗口创建预定义格式的 HTML 模板；请参阅第 126 页的实例模板。

创建登录后的 AUP 消息窗口的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 设置。
- 2 单击自定义。
- 3 滚动到登录后可接受使用策略部分。
- 4 指定设置：
 - 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。
 - 宽度：最小为 400 像素，最大为 1280 像素，默认为 460 像素。
 - 高度：最小尺寸为 200 像素，最大尺寸为 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。默认情况下已选中该选项。
 - 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**。
- 5 单击接受。

主题：

- 第 126 页的实例模板
- 第 127 页的预览消息

实例模板

单击实例模板以使用默认的 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</i></b></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

单击预览以显示将要想用户展示的 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。您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。

虽然整个 SonicOS 管理界面可以显示为多种不同语言，但有时候您不希望将整个 UI 语言更改为特定本地语言。

然而，如果安全设备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 转至**管理 | 系统设置 | 用户 | 设置**。
- 2 单击**自定义**。
- 3 滚动到**自定义登录页面**部分。
- 4 从**选择登录页面**中选择要自定义的页面。
- 5 滚动到页面底部。
- 6 单击**默认加载页面的默认内容**。
- 7 编辑该页面的内容。

① 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。

- 8 单击**预览**，预览自定义页面的外观。将显示一条消息。



- 9 单击**确定**。显示自定义的页面。
- 10 关闭窗口。
- 11 做出更改。
- 12 完成页面编辑后，单击**接受**。

△ 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无效。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。如需访问备用登录页面，请直接手动输入以下 URL：[https://\(device_ip\)/defauth.html](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。

① 提示：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。

配置 RADIUS 身份验证

注：如需为 SonicPoint 或 SonicWave 配置 RADIUS，请参阅 SonicOS 连接。

如需 SonicOS 中 RADIUS 身份验证的说明，请参阅第 76 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 129 页的[配置 RADIUS 设置](#)
- 第 132 页的[RADIUS 用户选项卡](#)
- 第 133 页的[使用 LDAP 设置用户群组的 RADIUS](#)
- 第 133 页的[RADIUS 客户端测试](#)

配置 RADIUS 设置

配置 RADIUS 设置的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 设置。
- 2 单击计费。



- 3 要在 SonicOS 中设置 RADIUS 服务器设置，请单击发送 RADIUS 计费信息。默认情况下未选中该选项。显示 RADIUS 计费和用户计费部分。

身份验证 Web 登录 身份验证旁路 用户会话 **计费** 自定义

RADIUS 计费

发送 RADIUS 计费信息

RADIUS 计费服务器：

#	主机名/IP 地址	端口	用户名格式	分区	启用
添加...					

测试

RADIUS 计费服务器超时 (秒)： 重试次数：

将计费数据发送到所有服务器

用户计费

发送以下对象的计费数据：

通过 Web 登录验证的用户 远程客户端用户 访客用户

SSO 验证的用户 是否包括通过 RADIUS 计费识别的 SSO 用户？

包含：

域用户 本地用户 域和本地用户

发送临时更新

- 4 在 RADIUS 计费服务器表中，单击添加。显示添加 RADIUS 计费服务器弹出窗口。

添加 RADIUS 计费服务器

主机名或者 IP 地址： 端口： 身份验证分区：

共享的密钥：

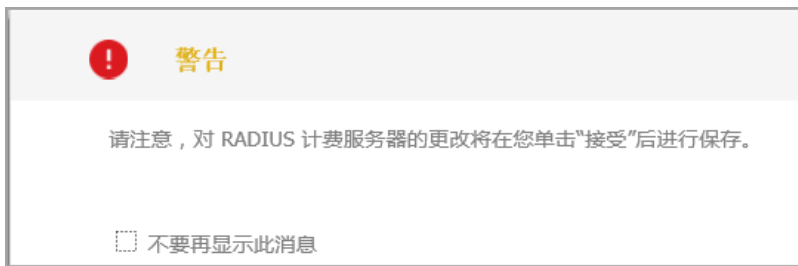
确认共享密钥：

用户名格式：

保存 取消

- 5 在主机名或 IP 地址字段中输入 IP 地址或主机名称。默认值为 0.0.0.0。
- 6 在端口字段中输入服务器的端口。默认值为 1813。
- 7 在共享的密钥和确认共享密钥字段中输入您的共享密钥。由区分大小写的字母数字组成的共享的密钥的长度范围为 1 至 31 个字符。
- 8 从用户名格式中选择用户名的格式：
- 用户名
 - 用户名@域（默认）
 - Domain\User-Name
 - User-Name.Domain

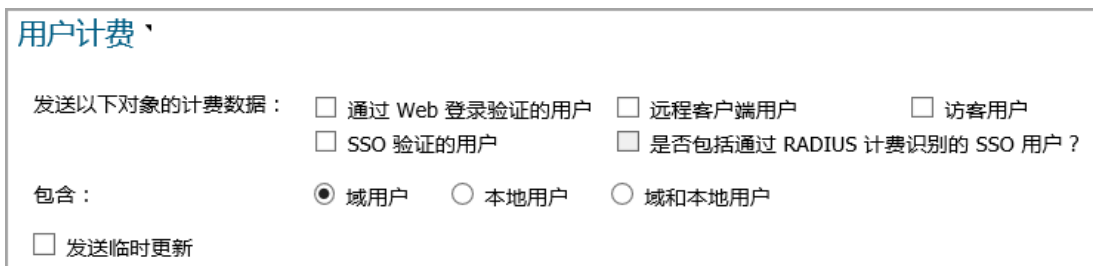
- 9 单击保存。将显示确认消息。



- 10 单击确定。服务器被添加到 RADIUS 计费服务器表中。



- 11 在 RADIUS 服务器超时（秒）字段中输入超时值。允许的范围为 1-60 秒，默认值为 5。审校问题：更好的定义。
- 12 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。
- 13 如果使用身份验证分区，如需将每个计费请求消息发送到所有配置的计费服务器或用户分区中的全部，请选择将计费数据发送到所有服务器。默认情况下未选中该选项。
- 14 如需配置与生成用户计费数据相关的设置，请滚动至用户计费部分。



- 15 选择一个或多个要发送数据的用户类型（无默认选中）：

- 通过 Web 登录验证的用户
- 远程客户端用户
- 访客用户
- SSO 验证的用户；下一个选项变为可用
- 是否包括通过 RADIUS 计费识别的 SSO 用户

- 16 选择要包括的用户：

- 域用户（默认）
- 本地用户
- 域和本地用户

17 如需将临时更新发送到计费服务器，请选择**发送临时更新**。默认情况下未选中该选项。

18 单击**接受**。

19 如需测试对已配置服务器的访问权限，请单击**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**：

i **注：**如果选择在 **RADIUS 服务器上使用 SonicWall 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 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，请参阅技术说明，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://www.sonicwall.com/zh-cn/support/>。

- 在 **RADIUS 服务器上使用 SonicWall 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，请参阅第 134 页的**配置 SonicWall 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。如需创建新的用户群组，请参阅第 133 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，请参阅第 200 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，请参阅第 79 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，所以如果无 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。在这种情况下，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：

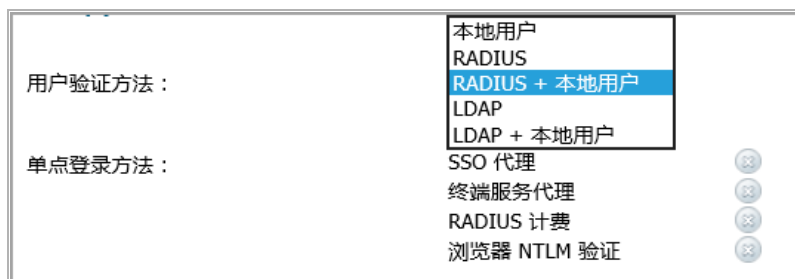
- 1 单击测试选项卡。
- 2 在用户字段，输入有效的 RADIUS 登录名称。
- 3 在密码字段，输入密码。
- 4 为进行测试，选择以下一种方法：
 - **密码验证：**选中该选项使用密码进行身份验证。
 - **CHAP：**选中该选项使用“质询握手身份验证协议”。在初始验证后，CHAP 通过使用三次握手定期验证客户端身份。
 - **MSCHAP：**选中该选项使用“Microsoft CHAP 实施”。MSCHAP 适用于 Windows Vista 之前的所有 Windows 版本。
 - **MSCHAPv2：**选中该选项使用“Microsoft 第 2 版 CHAP 实施”。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 如需完成 RADIUS 配置，请单击确定。

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 SonicWall 以支持 LDAP

管理 LDAP 集成的步骤如下：

- 1 转至用户 | 设置。
- 2 从用户验证方法下拉菜单，选择 **LDAP** 或 **LDAP + 本地用户**。



- 3 单击配置 **LDAP**。
- 4 如果通过 HTTP 而非 HTTPS 连接安全设备，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。如果您对连接的界面启用了 HTTPS 管理（建议），则单击是。显示 **LDAP** 配置对话框。



i | 注：动态学习的次要服务器显示为蓝色，以区别于配置的服务器。

主题：


- 第 135 页的 [设置](#)
- 第 136 页的 [方案选项卡](#)
- 第 137 页的 [目录选项卡](#)
- 第 138 页的 [提名选项卡](#)
- 第 138 页的 [用户和群组选项卡](#)
- 第 139 页的 [LDAP 中继](#)
- 第 140 页的 [测试选项卡](#)

设置

配置 LDAP 服务器设置的步骤如下：

1 配置以下字段：

- **名称或者 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 越过 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，而非其登录 ID（例如 John Smith，而非 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。强烈建议使用 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，而非使用本机 LDAP 越过 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，只是未验证发布。
- **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 能登录其他服务器，各服务器必须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：

i **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。

i **注：** 对于 **Microsoft Active Directory**，通常使用 `name@domain` 将其设置为用于登录的 **userPrincipalName**，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，而非用户对象，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。
 - ① 注：必须先要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。将所有方案默认设为 **mydomain.com**，但 Novell eDirectory 除外，并设为 **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无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。
 - ① 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* 而非 *ou*），但 SonicOS 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。

- ① 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。如需使用自动配置，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，而非配置的主服务器上，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 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。

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，其中包含可导入到安全设备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，您还可以在 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，安全设备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 的低端安全设备与之相连的中央 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。

i 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/或帧 IP 地址。

关于对多个 LDAP 服务器的扩展支持

可以配置多个主要 LDAP 服务器，每个身份验证分区一个，外加一个额外的服务器列表。每个主要 LDAP 服务器按照当前的 LDAP 服务器进行配置。对于其他服务器，配置是最小的（应用主要服务器的常用配置），但包括登录（绑定）凭据和服务器控制的子域。

- 注：**Active Directory 具有 LDAP 服务器到域的 1: 1 映射，其他 LDAP 服务器可能不会如此。当存在 1: 1 映射时，为每个 LDAP 服务器配置一个域可使服务器的选择高效，但是如果不是这种情况，则选择效率不高。

可按服务器分别配置的设置是当前位于管理界面中的 **系统设置 | 用户 | 设置 > 配置 LDAP** 对话框中的设置。如需配置 LDAP 的更多信息，请参阅第 134 页的 **配置 SonicWall 以支持 LDAP**。

- 重要：**为了正确操作，分区中的所有 LDAP 服务器必须设置为相同的模式。如果情况并非如此，则会发出警告。

提名设置是全局配置的，在所有身份验证分区中的所有 LDAP 服务器上都是通用的。

- 注：**显式配置辅助服务器是可选操作。每个主要和辅助服务器都可以单独配置，或者主要服务器可配置通过其使用提名访问的所有用户/群组树。

主题：

- 第 140 页的 **关于配置辅助服务器**
- 第 140 页的 **关于动态学习的辅助服务器**
- 第 141 页的 **关于备份服务器**

关于配置辅助服务器

除了主要/次要设置，创建/配置永久辅助服务器的步骤与主要服务器相同。它们之间的唯一功能区别在于，当进行搜索并且在配置的用户/群组树中未知位置时，搜索被发送到主要服务器，在主要服务器将搜索传递到辅助服务器（如果需要的话）时主要服务器发送引用/提名。

关于动态学习的辅助服务器

当第一次通过提名或引用来访问辅助服务器时，在可能尝试基于各种配置的用户树的多个绑定域名 [DNs] 之后，安全设备绑定到辅助服务器。安全设备在内部为辅助服务器创建一个记录，安全设备保存绑定信息以供将来尝试使用。此流程包括未配置的辅助服务器，从而创建一个动态服务器对象，该服务器对象与配置的服务器的服务器对象一起保存在内部。

这些动态学习的服务器对象允许按照配置的服务器存储额外的信息以及当前的绑定信息。这些信息包括由服务器学习的用户/群组树，以及该对象的统计信息。

注： 这些信息在重新启动后不会持久，必要时会重新学习。然而，动态辅助服务器的用户/群组树的配置与主要服务器一起保存。

关于备份服务器

Active Directory 提供对备份服务器的支持，通过 DNS 名称系统实现备份。Active Directory 域控制器通过计算机或域的 DNS 名称访问；在后一种情况下，域名解析为所有域控制器副本的 IP 地址列表。当 LDAP 服务器 DNS 名称解析为 IP 地址列表时，SonicWall 安全设备会依次尝试每个 IP 地址，直到有响应为止。因此，将 LDAP 服务器 DNS 名称配置为主要域名而非域控制器计算机名称，会导致冗余，如果主服务器没有响应，则会使用备份服务器。

此机制在 Active Directory 中也适用于提名和引用，因为它在域提名中返回次要域的 DNS 名称。

注： 在 Active Directory 中，备份服务器通常称为副本服务器。

可以为每个配置的主要或次要 LDAP 服务器配置一个或多个备份。通过此配置，可以为每台服务器记录状态和统计信息，并在上述 DNS 名称机制不提供冗余支持时，在非 Active Directory 安装中为备份服务器提供冗余支持。

备份服务器只有为其他服务器设置的一部分配置，因为大部分配置与其备份的服务器相同。默认情况下，只需要备份服务器的主机名或 IP 地址。

关于从 LDAP 导入和镜像

如需在启用 LDAP 用户群组镜像后创建与 LDAP 目录中的用户群组形成镜像的本地用户群组，SonicWall 安全设备定期自动从 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）。

可以在任何可以选择常规用户群组的位置选择镜像用户群组，例如访问规则和 CFS 策略。但是，镜像用户群组确实有一些限制，例如不能在 SonicWall 安全设备上将其他用户群组添加为成员，但镜像用户群组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 服务器上用户群组成员的用户自动接收任何通过其本地镜像群组设置的访问权限。

主题：

- [第 141 页的用户导入](#)
- [第 142 页的用户群组导入和镜像](#)

用户导入

当从 **LDAP 配置对话框**或**系统设置 | 用户 | 本地用户和群组**页面启动从 LDAP 导入用户时，有一选项用于指定要从中导入的 LDAP 服务器：

- 一台特定的 LDAP 服务器
- 身份验证分区中的所有服务器（启用后者时）
- 所有 LDAP 服务器

为了能够区分从不同 LDAP 服务器上的不同域中导入的用户，这些服务器可能具有相同的用户名，还可以选择使用包含该域的众多限定的用户名格式之一来创建本地用户对象。除了使用简单的用户名之外，这个选项也是。

如果用限定的用户名格式之一导入用户帐户，则：

- 对于使用该帐户的 Web 或客户端登录，完全限定的用户名必须与导入的完全一致。
- 当通过 SSO 标识用户时，由于名称格式可能因 SSO 源而异，因此用户名和域组件将与用户对象的信息分别匹配。例如，如果用户以 `jd@mydomain.com` 和 SSO 代理报表 `MYDOMAIN / jd` 从 LDAP 导入，则这些用户匹配，并且该用户帐户用于为用户设置其他群组会员资格。因此，对于 SSO 来说，选择限定的名字格式并不重要，选择主要是为了显示偏好。

注：这仅适用于在系统设置 | 用户 | 设置中已设置使用 LDAP 以获得用户群组信息或仅允许本地列出的用户选项时。如需更多信息，请参阅第 134 页的 [配置 SonicWall 以支持 LDAP](#) 和第 143 页的 [配置 SonicOS 以使用 SonicWall SSO 代理](#)。

用户群组导入和镜像

使用身份验证分区时，分区中的用户必须为从该分区导入的用户群组设置访问权限，而不是从其他分区导入的同名用户群组的访问权限。

例如，在策略中使用导入/镜像的用户组，通过将策略中的群组名与登录时从 LDAP 中读取的群组名进行匹配来为用户选择适用的用户群组。导入和镜像的用户群组的工作方式有点不同（主要出于历史原因）：

- 当手动导入用户群组时，使用没有域组件的简单群组名创建本地用户组对象。然后，当用户的群组成员身份与本地群组名相匹配时，只比较简单的群组名，并忽略任意域组件。因此，在不同域中存在相同名称的用户群组的情况下，来自任何域的用户将获得为本地群组设置的成员资格。
- 当 LDAP 用户群组镜像一个群组时，使用名称 `group-name@domain.com` 创建本地用户群组对象，以区分从不同域镜像的群组。然后，从 LDAP 中读取用户的群组成员资格时，将它们置于相同的格式中，并比较完整的群组名（包括域组件）。在不同域中存在相同名称的用户群组的情况下，来自一个域的用户只能获得从自己的域镜像的群组成员身份。

手动导入的用户群组也可以选择导入限定的群组名，因此可以按照上面的镜像群组使用它们，以便为每个域的用户分别设置成员资格。当从系统设置 | 用户 | 设置 > 配置 LDAP 对话框或用户 | 本地用户和群组页面启动群组导入时，该对话框与用户导入时的对话框具有相同的选项，除了格式的选择只能是简单名称或 `name@domain.com`（默认）。

注：对于导入/镜像的用户群组，不需要显式身份验证分区记录/检查，因为隐式匹配域组件可确保仅选择用户分区中的域中的组。

为了实现向后兼容，并且易于为不同分区上的标准群组成员设置通用访问权限，如果用简单名称从 LDAP（或手动创建）导入用户组，则匹配时将忽略该域；因此，可以使用简单名称为任何域/分区中的用户设置访问权限。

例如，如果您有：

- 分区 A: `domain dom_a.com`
- 分区 B: `domain dom_b.com`

然后从两分区中导入管理员群组，选择导入为 `name@domain.com`，您导入本地用户群组

`Administrators@dom_a.com` 和 `Administrators@dom_b.com`。每个分区中的用户只能获得为相关群组设置的访问权限；即是：

- 当来自分区 A 的管理用户登录并且 LDAP 查找发现他们是 `dom_a.com` 中的管理员群组成员时，他们会获得 `Administrators@dom_a.com` 中的成员资格。
- 同样地，当来自分区 B 的管理用户登录时，他们将收到 `Administrators@dom_b.com` 中的成员资格。

但是，如果从任一域以简单名称方式导入管理员群组，那么您将获得一个名为 Administrators 的本地用户群组，任一分区中的管理员用户都将获得为该组设置的任何访问权限。

镜像是全局启用的。启用后，用户群组将从所有已配置和学习的 LDAP 服务器进行镜像。

注：可以使用通配符排除功能来排除服务器上的所有组。

关于增强版 LDAP 测试

在 LDAP 测试中，可以选择要测试的 LDAP 服务器，除了当前的用户身份验证测试以外，还可以添加连接和搜索测试。请参阅 [LDAP 测试表](#)。

LDAP 测试

测试	功能
连接/绑定	只需尝试使用配置的绑定凭据绑定到 LDAP 服务器即可。
用户验证	测试给定的用户名和密码可以发送到 LDAP 服务器并进行验证。
LDAP 搜索	具有基本和高级模式： 基本模式搜索： <ul style="list-style-type: none">具有给定登录名、限定登录名或公用名的用户具有给定名称或成员的用户群组 高级模式允许： <ul style="list-style-type: none">明确的搜索过滤器（可选）更改搜索基础和范围（默认情况下是从域子树的顶部进行搜索，范围是搜索整个子树）正在搜索多个对象限制返回的信息

配置 SonicOS 以使用 SonicWall SSO 代理

配置安全设备以使用 SonicWall SSO 代理的步骤如下：

- 1 转至用户 | 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 144 页的 [SSO 代理选项卡](#)
- 第 146 页的 [用户选项卡](#)
- 第 148 页的 [实施选项卡](#)
- 第 150 页的 [终端服务选项卡](#)
- 第 150 页的 [NTLM 选项卡](#)
- 第 151 页的 [Radius 计费选项卡](#)
- 第 155 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）。

i | 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，将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**。

i | 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，请参阅第 **100** 页的 [单点登录高级功能](#)。

i | 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设置。
- 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。

i | 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：另请参阅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。

- 如需使所有 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。

i | **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 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。

i | **注：**域组件可以有如下格式：

- **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，不会给予这些用户“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。

i | **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 设备或运行了个人安全设备的 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**

i | **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。
- 在有个人安全设备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，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。

① 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，会导致安全设备在请求 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 探测功能是否有效，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。
 - 如需配置 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 156 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，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 重新验证用户而非通过代理轮询，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，而非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。

① 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。

① 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。

① 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：转至步骤 a。

默认情况下，通过 SSO 识别的用户登录 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）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 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。
 - ① 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。

如果有多个安全设备与 SSO 代理通信，应该仅在一个设备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。

① 注：在将安全服务策略或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访问规则未触发 SSO。

- 3 如需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。

i | **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。

i | **注：**在要求用户验证的访问规则触发 SSO 时，将不会应用 SSO 绕过设置。如需配置这种类型的 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，请参阅 SonicOS 策略。

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。如需将不接受 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，请参阅 SonicOS 策略。

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，而非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。

i | **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。

i | 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。

i | 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，而非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无活动用户。

- 在主机名或者 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 地址而非 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。

i | 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。

i | 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。安全设备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。

如需有关 NTLM 的更多信息，请参阅第 86 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”形式输入安全设备域的完整 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安全设备自己的 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** 页面配置的安全设备域名。
 - **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。
- ① **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 策略将阻止用户的 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 如需添加新 RADIUS 客户端，请单击**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。

i **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 SMA**
- 其他 - 非标准格式

i **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，请转至**步骤 8**。
- 如果选择**其他**，会显示更多设置，以便您能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。

i **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)

i **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。

i **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**。

如需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 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间值，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**超时间值**。
- **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间值。

i **注：**如果在一段时间后，重新加载页面后超时间值停留在 0（零），则设备并未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。

i **提示：**可以单击**显示信息**链接，以在弹出对话框中查看进度。

i **提示：**如需重新运行自动检测，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**。

如需确定哪些用户已注销，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。如需配置安全设备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**通过 RADIUS 计费的 SSO**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”消息以向安全设备告知连接/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，安全设备将追踪 RADIUS 计费消息以查找此“启动/停止”序列。如果找到此序列，则安全设备会将“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，则安全设备认定“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。

i **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 使安全设备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**带有**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，请单击**测试**选项卡。

i | **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。如果安全设备不能连接至 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。

i | **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，请参阅第 151 页的 [Radius 计费选项卡](#)。
- 4 单击应用。

高级 LDAP 配置

如果您在第 143 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。

如需配置 LDAP 以获得用户群组信息，请执行以下步骤：

- 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 156 页的 [“设置”选项卡](#)
- 第 158 页的 [方案选项卡](#)
- 第 159 页的 [目录选项卡](#)
- 第 160 页的 [提名选项卡](#)
- 第 161 页的 [用户和群组选项卡](#)
- 第 163 页的 [LDAP 中继选项卡](#)
- 第 164 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，安全设备等待来自 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，输入在超时前安全设备执行自动操作的分钟数。允许值从 1 至 99999。默认为 5 分钟。

i | **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**。

i | **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** 使用标识名访问树。“登录用户名”字段将更改为“绑定标识名”字段，且“登录密码”字段可用。转至 **步骤 8**。

- 7 如需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。转至 **步骤 9**。

i | **注：**在登录用户名字段中使用用户的姓名，即用户的标识名的第一个组件，而非用户名或登录 ID。例如，John Doe 通常以 jdoe 登录，但是在此处以 John Doe 而非 jdoe 登录。

- 8 在绑定标识名字段中，指定用于绑定到 LDAP 服务器的完全标识名 (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。

i | **重要：**强烈建议使用 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。

i | **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，而非使用本机 LDAP 越过 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。

i | **注：**取消选择该默认选项将显示一条警报，但安全设备和 LDAP 服务器之间的信息交换仍使用 TLS，只是无验证发布。

- 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。

i | **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，而非用户对象，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。

i | **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 使用安全设备 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，请参阅**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，且安全设备将搜索目录直至找到匹配项，否则将查找完整个列表。

添加新的树的步骤如下：

- 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，或为提高搜索效率，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，请参阅 RFC2253。

- c 单击**确定**。该树添加到表中。

编辑表中的现有树的步骤如下：

- 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。

删除表中的现有树的步骤如下：

- 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。调整表中的条目位置的步骤如下：

- 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**。

- 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无用户组成员身份属性且不使用 AD 的情况。添加新的树的步骤如下：

- 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，请参阅**步骤 4**。
- c 单击**确定**。该树添加到表中。

编辑表中的现有树的步骤如下：

- 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。

删除表中的现有树的步骤如下：

- 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。调整表中的条目位置的步骤如下：

- 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**。

- 8 **自动配置**按钮使安全设备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**。

i | **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**。

i | **注：**这可能需要一些时间。

i | **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 服务器而非配置的主服务器上，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 用户还必须存在于安全设备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 用户所属的安全设备上默认群组和 LDAP 服务器上配置的群组成员身份。

i **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安全设备上创建与现有 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，安全设备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 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 SonicWall 的用户名。
 - a 选中您要导入 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。

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 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，则需要先在 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 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 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。

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 SonicWall 群组成员身份和权限。

另外，您也可以 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，SonicWall 设备可以高效检索群组成员。

7 如需启用 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，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 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。

i 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。如需获取设备尝试镜像的所有用户群组的 XML 列表，请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（请参阅第 159 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。

编辑表中的现有树的步骤如下：

- 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。

删除表中的现有树的步骤如下：

- 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。调整表中的条目位置的步骤如下：
- 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 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使用可能不支持 LDAP 的安全设备与之相连的中央安全设备。在这种情况下，中央安全设备可以作为远程安全设备的 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，输入所有远程安全设备共用的共享密钥。
- 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 Internet 访问

对于运行不支持用户群组的非增强版固件的远程 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 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/或帧 IP 地址。

- 2 在**用户和密码**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）。

i **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**。

管理身份验证分区

- 第 165 页的关于身份验证分区
 - 第 166 页的关于用户身份验证分区
 - 第 167 页的关于子分区
 - 第 169 页的关于分区间用户漫游
 - 第 170 页的关于身份验证分区选择
 - 第 172 页的关于对多个 LDAP 服务器的扩展支持
 - 第 172 页的每个分区的 DNS 服务器和分割 DNS
 - 第 172 页的关于 RADIUS 身份验证
 - 第 173 页的从非分区配置升级
- 第 173 页的配置身份验证分区和策略
 - 第 173 页的显示和过滤用户/分区
 - 第 175 页的配置和管理分区
 - 第 186 页的配置分区选择策略
 - 第 189 页的配置进行身份验证分区的服务器、代理和客户端

关于身份验证分区

主题：

- 第 166 页的关于用户身份验证分区
- 第 167 页的关于子分区
- 第 169 页的关于分区间用户漫游
- 第 170 页的关于身份验证分区选择
- 第 172 页的关于对多个 LDAP 服务器的扩展支持
- 第 172 页的每个分区的 DNS 服务器和分割 DNS
- 第 173 页的从非分区配置升级

关于用户身份验证分区

i | 注：有关本节中使用的术语的定义，请参阅[本节中使用的术语和首字母缩略词表](#)。

SonicWall 安全设备为管理多个非互连域的环境中的 LDAP、RADIUS 和/或单点登录 (SSO) 验证提供了一种机制。这样的环境需要特定域中的用户通过以下特定方式进行身份验证：

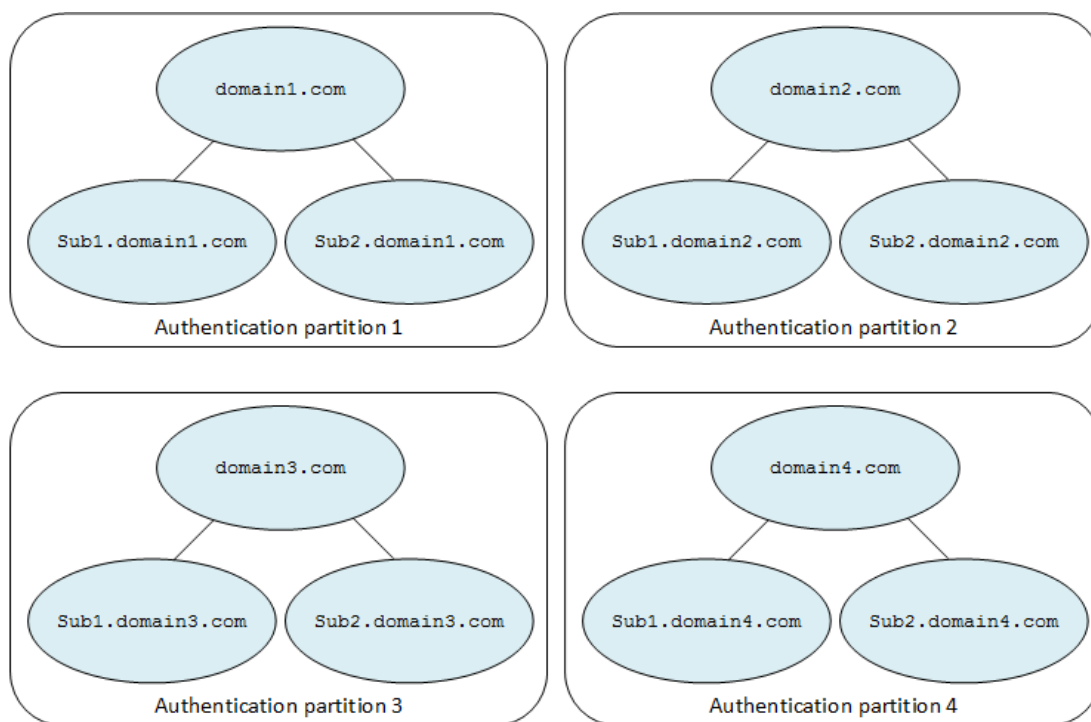
- 该域的 LDAP/RADIUS 服务器
- 位于该域中的 SSO 代理

这种环境的机制是用户身份验证分区，这意味着：

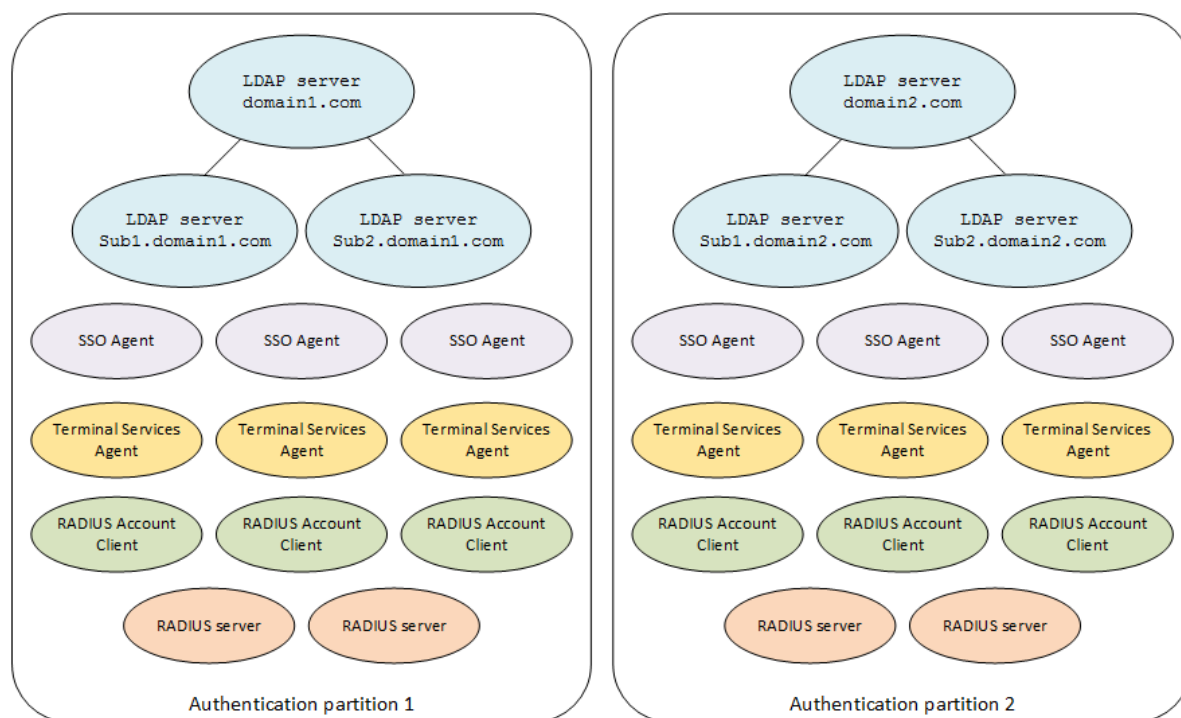
- 首先，将网络划分为独立的分区，每个分区都有自己的验证服务器/代理/客户端
- 然后，根据用户所在的验证分区，针对相关的验证设备（服务器/代理/客户端）对每个用户进行验证用户的分区是通过以下任一种方法选择的：
 - 将用户的域名与域中配置的域名进行匹配。
 - 如果用户的域名不可用，则根据分区选择策略设置其物理位置。

身份验证分区通常对应于一个或多个域。例如，在 Windows 域中，一个分区通常对应于一个 Active Directory 林。每个分区都有独立的 LDAP 服务器、RADIUS 服务器、SSO 代理和/或终端服务代理 (TSA)。参阅[身份验证分区](#)和[安装中央和远程站点](#)。

身份验证分区



分区内容



本节中使用的术语和首字母缩略词

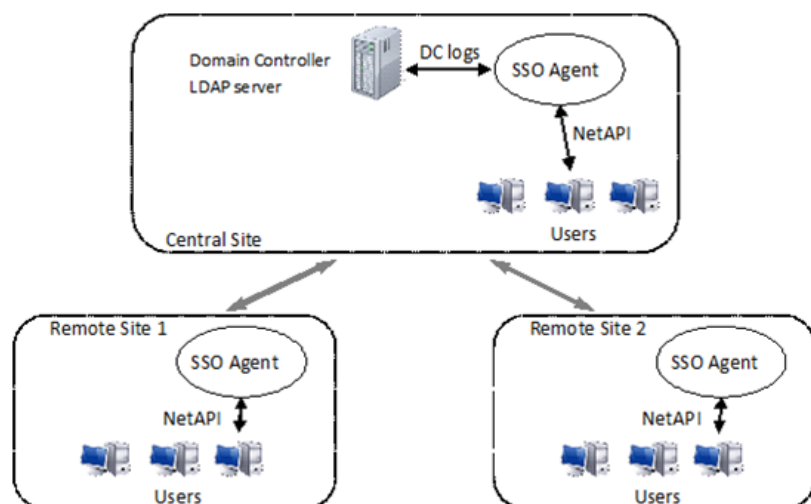
身份验证分区	带有自己的身份验证服务器/代理/客户端的网络的一部分，独立于网络的其他部分
DC	域控制器
LDAP	轻量级目录访问协议
RADIUS	远程验证拨入用户服务
SSO	单点登录
TSA	终端服务代理

关于子分区

身份验证分区选择用于对特定用户进行身份验证的 LDAP 服务器、RADIUS 服务器、SSO 代理和 TSA。除了将服务器和代理分配给分区之外，可能还需要将其中的某些分配给分区中的不同用户子集。子分区允许为分区用户的某些子集分配特定的代理（如果它们需要使用特定的代理）。如果将身份验证分区设置为另一个分区的子分区，则可以将特定于顶级身份验证分区或父身份验证分区用户的代理分配给子分区。子分区的代理在相关时使用，但是可以根据需要使用父分区的服务器和代理。

例如，带有中央站点和远程站点的安装具有位于中央站点的域控制器 (DC)/LDAP 服务器。但是，访问策略会阻止位于中央站点的 SSO 代理访问远程用户计算机。对于使用 NetAPI 或 WMI 在此拓扑中工作的 SSO，除了中央站点之外，还必须在每个远程站点上放置一个或多个 SSO 代理；请参阅[安装中央和远程站点](#)。对于 NetAPI/WMI，SSO 代理直接与用户的计算机对话，而 DC 安全日志中的用户标识使用域控制器的 SSO 代理。

安装中央和远程站点



顶级分区的子分区解决了以下问题：

- 告诉设备每个单独站点的 SSO 代理用于位于该处的用户的 NetAPI 或 WMI 标识。
- 将中央站点上的 SSO 代理和 LDAP 服务器用于对所有站点的所有用户进行 DC 日志标识和用户组查找。

通过将远程站点的 SSO 代理分配到子分区，可将每个远程站点配置为中央站点的子分区。通过以不同的选择策略定义每个分区用户子集的位置，可将一个或多个分区配置为一个父分区的子分区。在[安装中央和远程站点](#)中，整个安装是一个分区，远程站点都是该分区内的子分区。从子分区中选择相关代理以识别远程站点的用户后，随后通过父分区的 LDAP 服务器查找用户的组成员资格。

子分区的一些特殊情况如下：

- 不能将 LDAP 服务器分配给子分区。如果子分区对应于具有自己的 LDAP 服务器的子域，则可以将这些服务器分配给父分区。LDAP 服务器管理对子域的引用请求。
- 对于 RADIUS 服务器，子分区将使用分配给它的服务器或父分区的服务器，但不会同时使用这两种服务器。如果 RADIUS 服务器分配给子分区，则它们将用于此分区中的用户，否则将使用父分区的 RADIUS 服务器。
- 对借助使用 NetAPI 或 WMI 的 SSO 代理（相对于从域控制器日志中读取等），如果子分区及其父分区中都存在代理，则仅将子分区自己的 SSO 代理用于该子分区中用户的 NetAPI/WMI 标识；子分区的 SSO 代理可直接访问用户的电脑。如果子分区的 SSO 代理进行了相应配置，则域控制器日志读取由父分区和/或子分区中的 SSO 代理完成。

具有子分区的服务器、代理和客户端的操作

通常，分配给子分区的任何服务器、代理和/或客户端被用于位于其中的用户，但也会使用父分区的某些服务器、代理和/或客户端；请参阅[使用具有子分区的服务器、代理和客户端表](#)。

使用具有子分区的服务器、代理和客户端

服务器、代理、客户端 使用

LDAP 服务器	<p>只能分配给顶级分区，而不能分配给子分区。</p> <p>如果子分区对应于具有自己的 LDAP 服务器的子域，则应该将这些分配给父分区，且 LDAP 的引用机制将请求引用到子域的服务器。</p> <p>但是，如果子分区对应于具有自己的 LDAP 服务器的子域，您可能会认为将这些服务器分配给子分区更为合理，而且此操作是允许的。分配给子分区的服务器在内部链接到父分区。</p>
RADIUS 服务器	<p>子分区将使用分配给它的 RADIUS 服务器或父分区的 RADIUS 服务器，但不会同时使用这两种服务器。如果 RADIUS 服务器分配给子分区，则它们将用于此分区中的用户，否则将使用父分区的 RADIUS 服务器。</p>
SSO 代理	<p>使用 NetAPI 或 WMI 时，代理需要位于可以直接访问用户 PC 的位置。从 DC（域控制器）日志读取时，代理需要访问 DC。SSO 代理可以配置为执行这两个活动。</p> <p>同时使用 DC 日志和 NetAPI / WMI 时，SonicWall 安全设备控制使用哪个工具以及使用顺序。安全设备：</p> <ol style="list-style-type: none">1 让代理在从每个 DC 读取的 DC 日志中查找用户。2 如果未在日志中找到用户，请单独尝试 NetAPI / WMI 的后续请求。 <p>当使用子分区时，该机制进行如下操作，以识别位于子分区中的用户：</p> <ol style="list-style-type: none">1 如果分配给子分区的任何 SSO 代理启用了 DC 日志，则会将请求发送到这些 SSO 代理，以便在其 DC 日志中查找用户。2 如果在 步骤 1 中未标识用户，则当分配给父分区的任何 SSO 代理启用了 DC 日志后，会向这些 SSO 代理发送请求以在其 DC 日志中查找用户。3 如果在 步骤 2 中未标识用户，则当分配给该子分区的任何 SSO 代理启用了 NetAPI 或 WMI 后，会向这些代理中的一个发送请求以标识该用户。 <p>注：对于位于子分区中的用户，不通过父分区中的 SSO 代理尝试 NetAPI / WMI。如果在启用 NetAPI 或 WMI 的情况下未向子分区分配代理，则不会尝试进行验证。</p>
TSA 和 RADIUS 计费客户端	<p>这些代理/客户端发送用户分配到的分区仅影响用于用户组查找的 LDAP 服务器的选择。由于父分区的 LDAP 服务器也用于其所有子分区，因此可以将 TSA 和 RADIUS 计费客户端分配给其中的任一个。唯一的区别是为用户显示哪个分区，并根据用户的实际位置向其分配用户。</p> <p>注：这仅适用于未提供域的情况。</p>

关于分区间用户漫游

如果已经设置了网络拓扑以允许他们从登录分区访问他们自己的分区的域服务器，那么登录到一个分区中的域的用户能够漫游并从不同分区的物理网络进行连接。如果在这种情况下使用 SSO 代理，则设备将根据用户的实际位置（而不是其主分区的代理）选择本地分区的 SSO 代理。

本地分区的 SSO 代理无法从域控制器日志中识别漫游用户，因为代理未从正确的域控制器读取。如果代理具有正确的权限，可以通过 NetAPI 或 WMI 识别漫游用户，这需要 Windows 域间信任。因此，当安全设备从 SSO 代理获取用户名时，安全设备会检查指定域所在的分区，并允许根据用户的物理位置覆盖最初选定的分区。

识别漫游用户并设置其访问权限的流程是：

- 1 登录到（分区 1 中的）域 1 的用户与分区 2 中的子网连接；用户的分区最初记录为分区 2。

- 2 如果分区 2 代理正在读取域控制器日志，则首先会发送请求以检查这些日志。这些请求无法找到该用户，该用户未登录到分区 2 的域。
- 3 将请求发送到分区 2 中的 SSO 代理以尝试 NetAPI。代理执行此操作，并将该用户标识为来自域 1 的用户。
- 4 安全设备看到域 1 在分区 1 中，并将用户的分区切换到分区 1。然后安全设备通过分区 1 中的 LDAP 服务器查找用户的群组成员资格。

关于身份验证分区选择

主题：

- 第 170 页的[选择策略](#)
- 第 170 页的[远程用户](#)
- 第 171 页的[用户登录的设备通知](#)
- 第 171 页的[Web 用户登录](#)

选择策略

网络拓扑可能会影响 SonicOS 在网络上查找身份验证分区用户的方式。SonicOS 提供了多个选项来定位和选择用户的分区。

选择选项

当被以下方式选中时 每个身份验证分区

IP 地址	对应于通过在其配置中的地址对象（网络、范围或群组）选择的一组 IP 地址。
网络接口	对应于通过在其配置中选择一个或多个接口访问的网络。
网络区域	对应于在其配置中选择一个或多个网络区域。
用户名域组件	<p>是一个或多个域的成员，并通过匹配用户在登录时给出的域名进行选择。此选项要求用户使用限定名称登录，例如 domain\user 或 user@domain.com。</p> <p>当给定域名时，该选项将覆盖上述基于位置的选项。</p> <p>此选项应用于验证 GVC、L2TP 和 SSL VPN 客户端用户；请参阅第 170 页的远程用户。</p> <p>注：对于 SSO 代理身份验证，应使用基于位置的选项之一，因为 SonicWall 安全设备需要在进程开始时派生分区以选择要使用的 SSO 代理，并且此时安全设备还没有用户的登录名；请参阅第 169 页的关于分区间用户漫游。</p>

这些选项被配置为一组单独的选择策略，为每个分区设置一个或多个策略，以定义如何选择该分区。在用户验证期间，如果没有给出域，则通过与访问规则匹配非常相似的方式将区域、接口和 IP 地址与配置的策略进行匹配来选择分区。指定默认分区的默认选择策略对于与显式配置的策略不匹配的所有内容都是全面的。默认分区最初命名为“默认”，但可以重命名或者可以将默认选择策略设置为其他分区，之后可以删除自动创建的“默认”分区。

远程用户

选择用于 GVC/L2TP 客户端和 SSL VPN 用户的身份验证分区的处理方式不同，因为这些远程用户是正在连接到身份验证分区，而不是来自这些分区。安全设备需要知道这些用户的身份验证分区，以选择正确的

LDAP 服务器来查找他们的用户组成员资格，并从中找到他们可以访问的子网。有两个选项用于验证远程用户：

- 使用用户名域组件进行选择，并要求远程用户提供包括域的限定名称。
- 有多个 WAN 接口和/或 WAN 区域，并且每个身份验证分区用户都连接到不同的公共 IP 地址。则使用远程用户所经过的 WAN 接口或区域来选择身份验证分区，而不需要远程用户提供限定用户名。

注：对于 GVC/L2TP 用户，具有独立的 WAN 区域允许每个区域使用不同的群组 VPN 策略，从而可能更加安全地将访问强制执行到正确的验证区域。

当有多个 WAN 接口时，可以设置分区选择策略来选择通过每个 WAN 接口进行远程访问的分区。如果只有一个 WAN 接口，那么可以设置一个特殊的选择策略来选择用于远程访问的默认分区，而这个分区不能从所提供的用户名中得到。

注：如果未设置选择策略，则远程访问用户需要提供限定用户名，除非对其进行身份验证的服务器分配给默认选择的分区。

用户登录的设备通知

如果代理/客户端通知 SonicWall 安全设备用户登录，但未发送识别请求（例如，终端服务、RADIUS 计费 and 来自读取 DC 日志的 SSO 代理的登录通知），则安全设备不需要知道用于选择代理/客户端的身份验证分区，因为它将请求发送到 SSO 代理。如需选择正确的 LDAP 服务器来查找其用户群组成员身份，安全设备确实需要知道这些用户的身份验证分区。该选择是通过用户名域组件（当存在时）或通过手动将每个这样的代理/客户端分配给身份验证分区来完成的。

Web 用户登录

当用户通过 SonicWall 安全设备的 Web 登录门户登录时，不管他们来自哪里，他们可以使用任何帐户名称。通常情况下，身份验证分区是根据用户从哪里登录（请参阅第 170 页的 [选择策略](#)）来选择的，但是如果用户提供了包含该域的用户名，那么他们可以通过使用包含域的用于选择身份验证分区的限定名称登录来覆盖。

CLI 登录

当用户使用内置管理员帐户通过 CLI 登录时，分区不相关，因为该分区始终在本地进行身份验证。但是，当使用通过 LDAP 或 RADIUS 进行身份验证的其他管理员帐户时，则需要知道该分区以选择服务器来对其进行身份验证。对此有三种不同的情况：

登录到控制台端口	没有从中派生分区的 IP 地址，所以当需要时，用户需要使用限定用户名登录。
来自防火墙内部的本地 SSH 连接	根据第 170 页的 选择策略 ，通过 SSH 连接的源 IP 地址选择用户所在的身份验证分区。
从防火墙外部进行远程 SSH 连接	分区选择不是基于用户的位置，而是可能根据远程客户端用户，按照他们连接的 WAN 接口选择分区。请参阅第 170 页的 选择策略 。

如果已经配置了按用户名域组件的选择（请参阅第 170 页的 [选择策略](#)），则在任何情况下，用户都可以通过使用包含从中选择身份验证分区的域的限定用户名登录来覆盖该用户名。当分区不能从所提供的用户名中派生时，也可以设置一个特殊的选择策略来选择用于控制台端口登录的默认分区。

注：如果未设置选择策略，则用户需要提供限定用户名以在控制台端口登录，除非对其进行身份验证的服务器分配给默认选择的分区。

每个分区用户验证设置

在某些情况下，可能需要在不同分区中以不同方式设置管理用户身份验证的特定设置。例如，如果一个分区只有 RADIUS 服务器，而另一个分区只有 LDAP 服务器，那么对于用户验证，第一个分区中必须选择 RADIUS，在另一个分区中选择 LDAP。

默认情况下，所有这些设置全局适用，并且仅限于用户身份验证方法和单点登录方法。这些设置仅适为顶级分区而设；对于子分区，则应用其父分区的身份验证设置。

关于对多个 LDAP 服务器的扩展支持

分区需要多个 LDAP 服务器。可以配置多个主要 LDAP 服务器，每个身份验证分区一个，外加一个额外的服务器列表。如需有关多个 LDAP 服务器以及如何配置它们的更多信息，请参阅第 140 页的[关于对多个 LDAP 服务器的扩展支持](#)。

每个分区的 DNS 服务器和分割 DNS

无论是否有身份验证分区，通常都需要使用域自己的 DNS 服务器来解析域中设备的名称，而且偶尔也可能需要使用不同的外部 DNS 服务器来解析外部主机名。但是，多个身份验证分区通常需要使用不同的 DNS 服务器来解析不同分区中的主机名。

具有分割 DNS 功能的 DNS 代理允许配置与不同域名关联的不同 DNS 服务器。该功能与 DNS 代理分离，因此可以直接由安全设备用来解析域中设备的名称，而无需启用 DNS 代理，包括多个不相关的具有身份验证分区的域。如需有关分割 DNS 的更多信息，请参阅第 165 页的[管理身份验证分区](#)。

关于 RADIUS 身份验证

使用 RADIUS 身份验证还有一些额外的考虑事项，因为无法像使用 LDAP 那样保证 SonicWall 安全设备派生用户域的方式，也无法保证在 RADIUS 属性中返回的用户群组域。因此，安全设备可以找到选择正确的域用户和用户群组对象的域，安全设备尝试以下方式通过 RADIUS 验证来学习用户的域：

- 1 让用户在登录时提供包含域的限定用户名。如果 RADIUS 服务器返回 RADIUS 属性（Filter-ID 或 SonicWall 供应商特定属性）中的用户群组，则将其配置为返回给出包含域名的完全限定群组名称。
- 2 在通过 RADIUS（这是首选方法）对用户进行身份验证后，使用 LDAP 进行用户组查找。然后，如果用户没有给出包含用户名的域，可以从 LDAP 搜索中学习以找到他们的用户组。
- 3 如果两者都失败，那么当用户从物理位置上的 IP 地址登录时，可以从身份验证分区查找该域，但是如果每个分区只有一个域，则只能确定地给出用户的域；因此，要使用这种方法，每个子域都必须要有单独的子分区。

ⓘ | 注： 这方法对跨域用户群组的成员身份无效。

总之，使用 RADIUS 身份验证的最佳选择是使用 LDAP 进行用户群组查找。如果这不可行（无 LDAP 服务器），则下一个最佳选择是让 RADIUS 服务器在 RADIUS 属性中返回限定的用户群组名称。

如果这些都不能用于派生从 RADIUS 返回的用户群组的域，则有必要将用户/用户群组对象配置为在任何域中匹配。

从非分区配置升级

从没有身份验证分区的现有配置启动时，启用分区时：

- 使用其中的所有现有服务器、代理和客户端创建名为默认的单个人身份验证分区。
- 会配置单个默认分区选择策略以将默认分区选择作为所有内容的默认分区。

在这个基础上，可以添加新的分区，可以容易地将相关的服务器、代理和客户端从默认分区移动到新分区，或从新添加的分区移动。

配置身份验证分区和策略

可以使用用户 > 分区页面创建身份验证分区列表和策略用以选择。对于每个分区，可以配置：

- 身份验证分区的名称（例如，它所对应的域或林的名称）。
- 分区包括的域。
- 如何为用户选择身份验证分区（例如，配置为单独的分区选择策略）。

在配置身份验证分区和分区选择策略之前，可以从监控 > 当前状态 > 用户会话 > 活动用户页面确定分区中的用户位置。

如果配置了身份验证分区，则会在各种服务器/代理/客户端配置中添加一个选择，以便在添加/编辑服务器、代理或客户端时可以选择身份验证分区。可以从用户 > 设置页面配置服务器、代理和客户端。

主题：

- 第 173 页的 [显示和过滤用户/分区](#)
- 第 175 页的 [配置和管理分区](#)
- 第 186 页的 [配置分区选择策略](#)
- 第 189 页的 [配置进行身份验证分区的服务器、代理和客户端](#)

显示和过滤用户/分区

监控 | 用户会话 > 活动用户页面显示每个用户所在的分区。

 注：如需有关此页面的详细信息，请参阅 SonicWall 安全设备的 SonicOS 监控。

<input type="checkbox"/> 用户名	IP 地址	会话时间	剩余时间	不活动剩余	类型/模式	Partition	设置	注销
<input type="checkbox"/> admin	192.168.95.233	5 分钟	无限制	300 分钟	Web 登录, 配置模式	Default		

包含非活动用户 显示未授权的用户

主题：

- 第 174 页的 [查看用户信息](#)
- 第 174 页的 [过滤用户](#)

查看用户信息

可以按各种类别查看用户数量：

- 活动/非活动
- 按识别方式的 SSO 用户
- 按客户端类型的客户端用户
- Web 用户
- SSL VPN 入口用户

如需查看此信息，请单击活动用户会话表下的统计图标。显示用户计数弹出对话框：



过滤用户

过滤器字段允许过滤分区，以仅显示所选分区中的用户。通过指定一个或多个完全或部分用户名、域、IP 地址和/或用户类型，可搜索用户。通过为条目添加感叹号 (!) 前缀来排除用户。当组合字符串时，要匹配：

- 任何列出的条目，用逗号分隔条目；即 a,b 包含与 a 或 b 匹配的用户
- 所有列出的条目，用分号 (;) 分隔条目；即 a;b 包含与 a 和 b 都匹配的用户

如需搜索终端服务器用户，请输入 user-num=usernumber。类型过滤器与类型/模式列中的文本匹配，指示鼠标移动到该列上时显示的任何内容。支持 IPv6 地址，但仅用于完全匹配；例如，ip=2012::1、!ip=2012::1 或与过滤器示例表中所示的其他条目组合。

过滤器示例

```
name=bob                name=bob, john, sue          domain=mydomain
ip=192.1.1.1            ip=192.1.1.1,192.1.1.2      ip=192.1.1.0/24
type=config mode        type=sso,web                 type=sso;netapi
type=sso;from logs on domain controller 192.1.1.10
partition=somePartition group=Trusted Users
name=bob;ip=192.1.1.1 (匹配名称和 IP 地址)
!name=bob !ip=192.1.1.1 (排除用户)
```

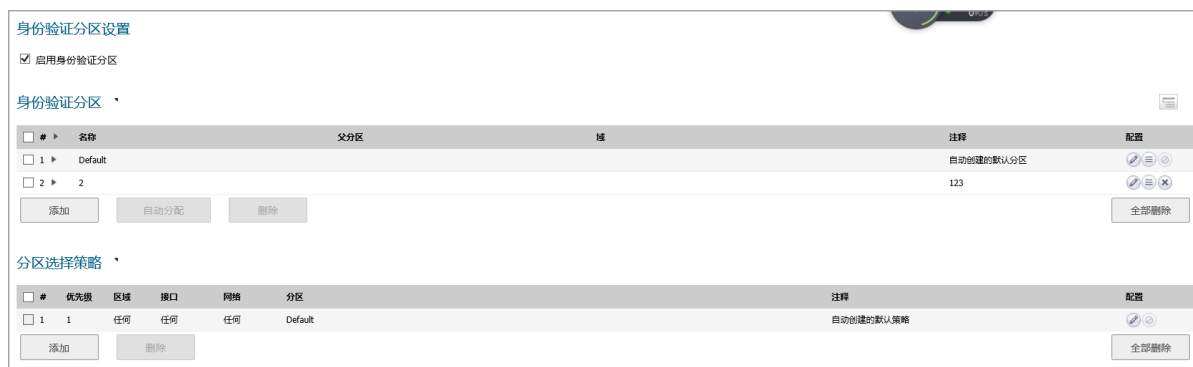
也可以使用简单的字符串，例如：bob 192.1.1.1 mydomain

配置和管理分区

主题：

- 第 175 页的[系统设置 | 用户 > 分区页面](#)
- 第 178 页的[启用/禁用身份验证分区](#)
- 第 179 页的[添加分区和子分区](#)
- 第 180 页的[删除分区和子分区](#)
- 第 182 页的[分配服务器、代理和客户端](#)
- 第 184 页的[编辑分区](#)

系统设置 | 用户 > 分区页面



系统设置 | 用户 > 分区页面包含三个部分：

- 第 175 页的[身份验证分区设置部分](#)
- 第 176 页的[身份验证分区部分](#)
- 第 178 页的[分区选择策略部分](#)

身份验证分区设置部分

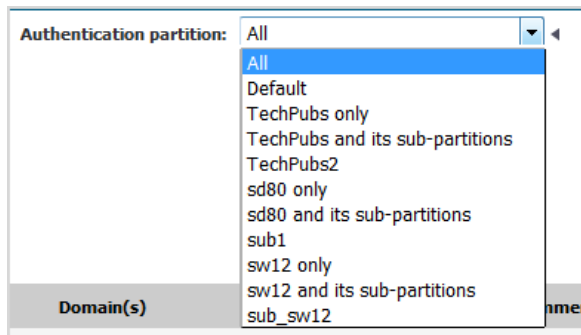
本部分启用/禁用身份验证分区。如果身份验证分区处于禁用状态，不显示其他部分。

身份验证分区设置

启用身份验证分区

启用身份验证分区时，会显示身份验证分区和身份验证选择策略这两个部分。

当启用分区时，页面顶部还会显示身份验证分区下拉菜单，可以从中选择用户 > 设置和用户 > 本地用户和群组页面中的设置也适用的分区。默认值是全部，即设置适用于所有分区。



身份验证分区部分

i | 注：此部分仅在启用身份验证分区时显示。

本部分显示身份验证分区表，并允许创建、编辑、删除和管理分区。在此处配置的分区控制哪个验证服务器用于哪些用户。

可以展开分区的树以显示分配其中的服务器、代理和客户端。

#	名称	父分区	域	注释	配置
<input checked="" type="checkbox"/>	1 ▶ Default			自动创建的默认分区	
<input type="checkbox"/>	2 ▶ 2			123	
<input type="checkbox"/>	4 ▶ ↳ 21	2		123	
<input type="checkbox"/>	5 ▶ ↳ 22	2		123	
<input type="checkbox"/>	3 ▶ 3			456	

群组子分区 图标 在将子分区与其父身份验证分区进行分组，或取消子分区分组并将其与顶级分区进行排序之间切换。

注：已分组的子分区随即显示在他们的父分区之后，并带有链接 图标作为子分区标志。

选择复选框 允许在表中选择一个或多个分区和/或子分区。选择表标题中的复选框将选择除默认分区以外的所有条目。

名称 指定身份验证分区的名称。子分区由名称前面的链接 图标指示。

父分区 指定子分区的父身份验证分区。父分区的此列为空白。

域 指定分区或子分区所属的域。默认分区的此列为空白。

注释 显示添加分区时包含的注释。默认分区的注释是自动创建的默认分区。

配置 显示分区的编辑、选择 和删除图标。

注：默认分区的编辑和删除图标均处于灰显状态。

添加 显示用于添加身份验证分区或子分区的添加身份验证分区弹出对话框。

自动分配 根据 IP 地址或主机名称，将所有未分配的 LDAP 服务器、RADIUS 服务器、SSO 代理、TSA 和 RADIUS 计费客户端自动分配到相关分区。

注：至少选择了一个分区或子分区之后，自动分配和删除按钮才可用。

删除 删除所选的身份验证分区或子分区。

注：不能删除默认分区。

全部删除 删除除默认分区外的所有分区和子分区。

该表中总有一个身份验证分区，即自动创建的默认分区。不能删除这个分区。但是，可以编辑它并为其选择服务器、代理和客户端以及子分区。如果禁用身份验证分区，则所有 LDAP 服务器、SSO 代理、TSA 和 RADIUS 计费客户端将重新分配给默认分区；当重新启用身份验证分区时，必须对它们进行重新分配。RADIUS 服务器不受影响，并保留其分配的分区。

展开树

展开身份验证分区的树显示分配给该分区的服务器、客户端和代理：

#	名称	父分区	域	注释	配置
1	Default			自动创建的默认分区	
2	2			123	
4	↳ 21	2		123	
5	↳ 22	2		123	
3	3			456	
6	↳ 31	3		456	
7	↳ 32	3		456	

添加 自动分配 删除 全部删除

您可以：

- 通过单击标题中复选框旁边的三角形展开所有表格条目的树。
- 通过单击每个展开图标展开一个或多个表条目的树。

显示层次结构

默认情况下，子分区显示在其父分区下方，并在子分区名称前有一个链接图标

#	名称	父分区	域
1	Default		
2	2		
4	↳ 21	2	
5	↳ 22	2	
3	3		
6	↳ 31	3	
7	↳ 32	3	

通过单击群组 图标，可以将子分区与其父分区显示在相同的级别上。





#	名称	父分区	域
1	Default		
2	2		
3	3		
4	21	2	
5	22	2	
6	31	3	
7	32	3	

分区选择策略部分

i | 注：此部分仅在启用身份验证分区时显示。


本部分显示影响选择身份验证分区的策略表，并允许创建、删除和编辑策略，以及更改创建的任何策略的优先级。这些策略根据进行身份验证的用户的物理位置，选择身份验证分区表中的分区。在对域名无法用于与所选分区中的域名匹配的用户进行身份验证时，将根据这些策略设置的物理位置来选择用户的分区。这些选择策略还用于根据设备的物理位置自动将验证设备分配给分区。

不能删除“默认”分区的“默认”选择策略，也不能更改其优先级；它始终是最低优先级。

#	优先级	区域	接口	网络	分区	注释	配置
<input type="checkbox"/>	1	LAN	X2	All Interface IP	3		 
<input type="checkbox"/>	2	任何	任何	任何	Default	自动创建的默认策略	 

添加 删除 全部删除

选择复选框 允许在表中选择一个或多个条目。选择表标题中的复选框将选择除默认选择策略条目以外的所有条目。

优先级 根据分配的优先级来对分区选择策略进行排序。单击优先级箭头  将显示更改选择策略优先级弹出对话框。不能更改默认选择策略的优先级；它始终是最低优先级。

区域 显示分配给分区选择策略的区域。

接口 显示分配给身份验证分区选择策略的接口。

分区 显示选择策略适用的身份验证分区。

注释 显示创建或编辑选择策略时输入的任何注释。默认分区的选择策略带有注释自动创建的默认策略。

配置 显示编辑和删除图标，默认策略的这些图标处于灰显状态。

添加 显示用于为身份验证分区或子分区添加选择策略的添加分区选择策略弹出对话框。

删除 删除所选的一个或多个策略。

注：不能删除默认分区的策略。至少选择一个策略之后，删除才可用。

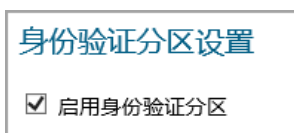
全部删除 从表中删除除默认分区的策略之外的所有策略。

该表中总有一个选择策略，即自动创建的默认分区的默认策略。除选择适用的分区外，不能选择此策略、删除此策略、更改其优先级或对其进行编辑。

启用/禁用身份验证分区

启用分区的步骤如下：

- 1 转至用户 > 分区页面。



- 2 在身份验证分区设置部分，选择启用身份验证分区。显示身份验证分区和分区选择策略部分。

禁用分区的步骤如下：

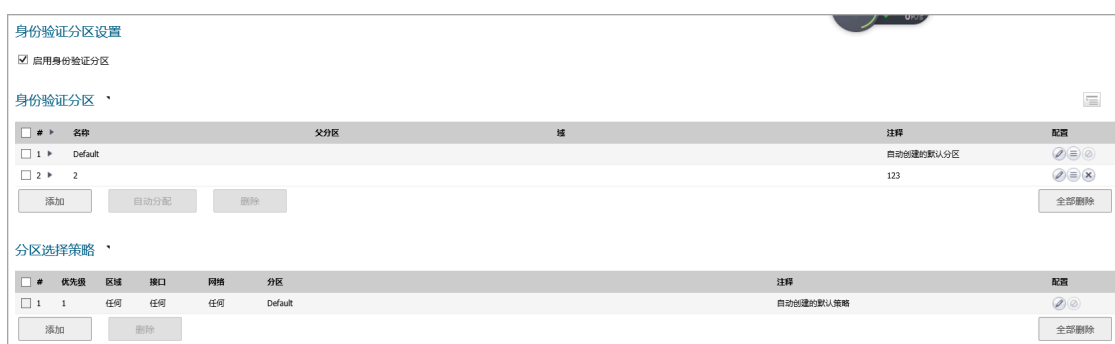
- 1 转至用户 > 分区页面。
- 2 在身份验证分区设置部分，取消选择启用身份验证分区复选框。不再显示身份验证分区和分区选择策略部分。

重要：当禁用身份验证分区时，所有已分区的 LDAP 服务器、SSO 代理、TSA 和 RADIUS 计费客户端都将移至默认身份验证分区；RADIUS 服务器不受影响，并保留在其配置的身份验证分区中。如果随后启用身份验证分区，则需要重新配置所有其他服务器、代理和客户端。

添加分区和子分区

添加分区的步骤如下：

- 1 转至用户 > 分区页面。



- 2 在身份验证分区部分中，单击添加。显示添加身份验证分区弹出对话框。

- 3 在分区名称字段中输入分区的名称。名称长度可以为 1 到 32 个字母数字字符。
- 4 对于分区类型，根据身份验证分区选择，如果是：
 - 顶级分区，请转至步骤 6。

- 子分区，显示父分区下拉菜单：

分区类型：	<input type="radio"/> 顶级分区	<input checked="" type="radio"/> 子分区
父分区：	Default ▾	

5 从下拉菜单中选择一个父分区。默认分区为默认。

提示： 如果安装中没有多个分区，则创建子分区作为默认分区的子分区。

6 在域列表下，单击添加。显示添加域弹出对话框。

输入域名
<input type="text"/>

7 输入域名。

8 单击确定。

9 对要添加的每个域重复步骤 6 到步骤 8。

10 可以选择在备注字段中输入备注。

11 单击保存。分区和 / 或子分区添加到身份验证分区表中。子分区随即位于他们的父分区之后，并带有链接图标作为子分区标志。

删除分区和子分区

注： 在本节中，分区指的是分区和子分区。

可以删除单个分区、多个分区或所有分区。如果删除单个分区，则服务器、代理和客户端将重新分配给默认分区。

注： 不能删除默认分区。

主题：

- 第 180 页的删除单个分区
- 第 181 页的删除多个分区
- 第 181 页的删除所有分区（“默认”分区除外）

删除单个分区

删除单个分区的步骤如下：

1 转至用户 > 分区。

2 在身份验证分区表下，单击要删除分区的配置列中的删除图标。显示验证消息：

是否确定要删除分区 '21'？
当前分配给它的任何服务器、客户端或代理 将移动到默认分区 (Default)。

3 单击确定。如果分区：

- 没有子分区，则分区被删除，服务器/代理/客户端重新分配到默认分区。
- 有子分区，显示这个消息：

为分区且它有子分区设置了一些选择策略。是否也希望删除那些内容？
如果您选择否，则将对前者进行更新以选择默认分区 (Default)，而后者将更新为没有父级。

- a) 请执行以下步骤之一：
- 如需将子分区和父分区一起删除，请单击**是**。所有服务器/代理/客户端重新分配到默认分区。
 - 如需在删除父分区时将子分区转换为顶级分区，请单击**否**。所有服务器/代理/客户端重新分配到默认分区。
 - 如不删除父子分区，请单击**取消**。

删除多个分区

删除多个分区的步骤如下：

- 1 转至用户 > 分区。
- 2 在身份验证分区表中，单击要删除的身份验证分区的复选框。可以选择多个分区。
- 3 单击删除。显示验证消息：

是否确定要删除所选分区？
当前分配给它们的任何服务器、客户端或代理将移动到默认分区 (Default)。

- 4 单击确定。如果任意分区：
 - 没有子分区，则分区被删除，服务器/代理/客户端重新分配到默认分区。
 - 有子分区，显示这个消息：

分区有子分区。是否也希望删除那些内容？
如果您选择否，则会将它们更新为没有父级。

- a) 请执行以下步骤之一：
- 如需将子分区和父分区一起删除，请单击**是**。所有服务器/代理/客户端重新分配到默认分区。
 - 如需在删除父分区时将子分区转换为顶级分区，请单击**否**。所有服务器/代理/客户端重新分配到默认分区。
 - 如不删除父子分区，请单击**取消**。

删除所有分区（“默认”分区除外）

删除所有分区（“默认”分区除外）的步骤如下

- 1 转至用户 > 分区。
- 2 在身份验证分区表中，单击全部删除。显示验证消息：

是否确定要删除所有分区？

(除了不会删除的默认值)

- 3 单击确定。所有服务器/代理/客户端重新分配到默认分区。

分配服务器、代理和客户端

在添加身份验证分区后，将服务器、代理和/或客户端分配给分区。也可以随时按照相同的步骤将它们分配到身份验证分区。

可以将未分配的服务器、代理和客户端自动分配到分区。

主题：

- 第 182 页的[手动分配](#)
- 第 183 页的[自动分配](#)

手动分配

分配服务器、代理和客户端的步骤如下：

- 1 转至用户 > 分区。

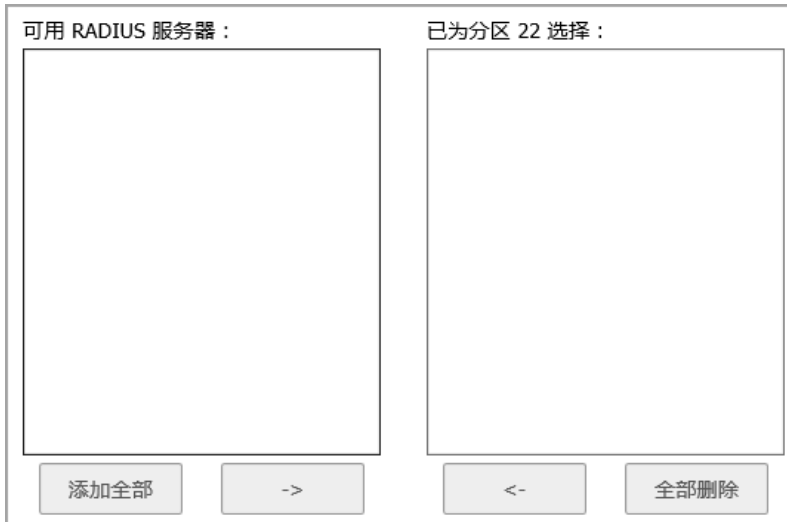


- 2 在身份验证分区表中，单击配置列中分区的选择图标。显示选择什么？弹出对话框。

选择分区的：

- RADIUS 服务器s
- SSO 代理s
- RADIUS 计费客户端s
- LDAP 服务器s
- 终端服务代理s
- RADIUS 计费服务器s

- 3 选择要分配的服务器、代理或客户端的类型。适当的为 `partitionName` 分区选择服务器/代理/客户端弹出菜单显示可用服务器、代理或客户端列表。



4 执行以下某个操作：

- 从可用列表选择一个服务器/代理/客户端，然后单击右箭头按钮。
- 通过按住 **Ctrl** 键选择每个项目并单击右箭头按钮，从可用列表中选择多个项目。
- 单击全部添加选择所有项目。

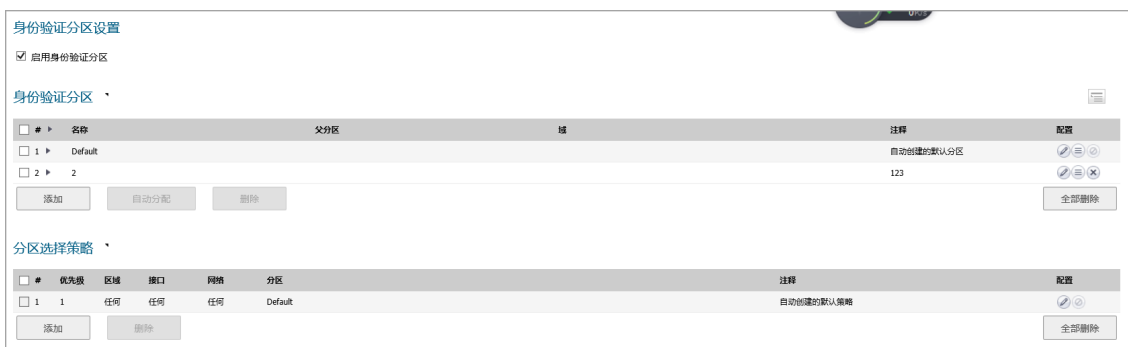
5 单击保存。

自动分配

有一个自动分配按钮，用于根据各自 IP 地址或主机名将所有未分配的服务器、代理和客户端自动分配给相关的分区。

自动分配服务器、代理和客户端的步骤如下：

1 转至用户 > 分区。



2 在身份验证分区表中，单击要分配未分配的服务器、代理和/或客户端的认证分区的复选框。可以选择多个分区。自动分配按钮随即激活。

3 单击自动分配。出现自动分配消息。

是否自动将项目分配给所选分区？

根据其网络位置和/或 DNS 名称，LDAP/RADIUS 服务器，SSO 代理等将从以下任何一项中进行选择：

- 尚未分配给任何分区，
- 已分配给默认分区 (Default)。

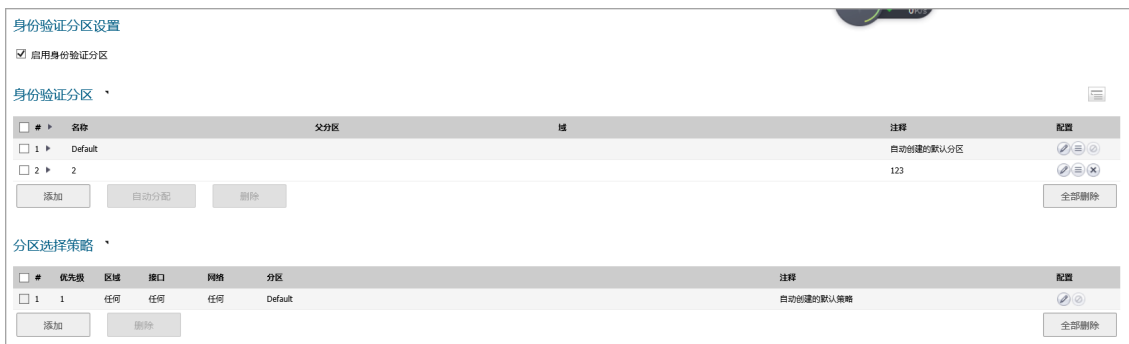
4 单击确定。

编辑分区

您可以编辑所有分区，包括默认分区。

编辑分区的步骤如下：

1 转至用户 > 分区。



2 在身份验证分区表中，单击要修改的身份验证分区的配置列中的编辑图标。显示编辑身份验证分区弹出窗口。

The edit partition dialog box contains the following fields and options:

- 分区名称: 22
- 分区类型: 顶级分区 子分区
- 父分区: Default
- 域: (Empty text area)
- Buttons: 添加, 编辑, 删除
- 备注: 123

如果分区需要自己的 DNS 服务器，您可以在“网络/DNS”页面上的分割 DNS 下为其域配置这些服务器。

3 可以在分区名称字段中更改分区的名称。名称长度可以为 1 到 32 个字母数字字符。

4 可以通过更改分区类型来将分区从顶级分区更改为子分区或从子分区更改为顶级分区。选择身份验证分区现在是：

注：具有子分区的顶级分区不能更改为子分区，除非先删除子分区，将其重新分配给不同的顶级分区，或将其设置为顶级分区。

- 顶级分区，请转至 [步骤 6](#)。
- 子分区，显示父分区下拉菜单：

5 从父分区下拉菜单中选择一个父分区。默认分区为默认。

6 如需：

- 编辑一个域，转到 [步骤 10](#)。
- 删除一个域，转到 [步骤 15](#)。
- 添加一个域，在域列表下，单击添加。显示添加域弹出对话框。

7 输入一个域名，可以是 1 到 32 个字母数字字符。

8 单击确定。

9 转至 [步骤 17](#)。

10 通过单击选择一个要编辑的域。

11 单击编辑按钮。显示编辑域对话框。

12 更改域名。

13 单击确定。

14 转至 [步骤 17](#)

15 选择一个要删除的域。

16 单击删除按钮。





17 对于要添加、编辑或删除的每个域，重复 [步骤 6](#)。

18 可以选择在备注字段中输入备注。

19 单击保存。

配置分区选择策略

分区选择策略指定如何为用户选择身份验证分区。可以在用户 > 分区页面的分区选择策略部分添加、编辑和管理身份验证分区选择策略。如需有关分区选择策略的完整描述，请参阅第 170 页的[关于身份验证分区选择](#)。

#	优先级	区域	接口	网络	分区	注释	配置
1	1	LAN	X2	All Interface IP	3		 
2	2	任何	任何	任何	Default	自动创建的默认策略	 

添加 删除 全部删除

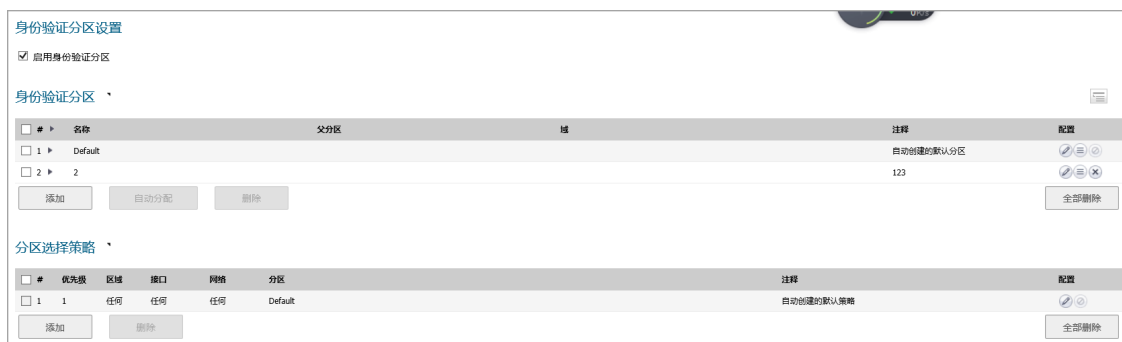
主题：

- 第 186 页的[添加身份验证分区选择策略](#)
- 第 187 页的[改变选择策略的优先级](#)
- 第 188 页的[修改选择策略](#)
- 第 188 页的[删除分区选择策略](#)

添加身份验证分区选择策略

添加分区选择策略的步骤如下：





- 1 转至用户 > 分区页面。



身份验证分区设置


启用身份验证分区

身份验证分区

#	名称	子分区	值	注释	配置
1	Default			自动创建的默认分区	 
2				123	 

添加 自动分配 删除 全部删除

分区选择策略

#	优先级	区域	接口	网络	分区	注释	配置
1	1	任何	任何	任何	Default	自动创建的默认策略	

添加 删除 全部删除

- 2 在分区选择策略部分中，单击添加。显示添加分区选择策略弹出对话框。

添加分区选择策略

对于 位于以下位置的用户... 通过以下方式连接的远程用户... 控制台端口登录：

区域：

接口：

网络：

选择分区：

注释：

3 选择用户的登录位置，显示的内容取决于您的选择：

对于此选择， 转至
位于以下位置的用户... [步骤 4](#)，这是默认值
远程用户 [步骤 7](#)
控制台端口登录 [步骤 9](#)

4 如果选择位于以下位置的用户...，请从区域、接口和网络下拉菜单中选择分区所在的位置：

i **注：**如需选择分区，通常不需要指定区域、接口和网络。为了达到最佳效率，最好指定必要的最小值。
例如，如果通过特定接口定位了某个分区，则仅选择该接口，并将**区域**保留为默认值任何。如果某个分区位于特定子网中，则只需将该子网选择为**网络**，并将**区域**和**接口**都设置为默认值任何。

i **注：**每个下拉菜单中提供的选项因站点而异。

- 区域 - 默认为任何
 - 接口 - 默认为任何
 - 网络 - 默认为任何，有创建新的地址对象和/或地址组的选项
- 5 从选择分区下拉菜单中选择一个分区或子分区。默认分区为默认。
- 6 转至 [步骤 10](#)。
- 7 如果选择了远程用户，则选项会改变。从**选择分区**下拉菜单中选择一个分区或子分区。默认分区为默认。
- 8 转至 [步骤 10](#)。
- 9 如果选择了控制台端口登录，则选项会改变。从**选择分区**下拉菜单中选择一个分区或子分区。默认分区为默认。
- 10 可以选择在备注字段中输入备注。
- 11 单击保存。

改变选择策略的优先级

在确定要使用的身份验证分区时，SonicOS 从顶部 (1) 到底部 (n) 按顺序搜索分区**选择策略表**。在创建选择策略时，它们的优先顺序如下：

- 1 区域，组中最后列出任何
- 2 接口，组中最后列出任何
- 3 网络，组中最后列出任何

除了始终为最低优先级的默认分区选择策略之外，可以更改任何策略的优先级。

更改选择策略的优先级会将策略在优先级列表中向上或向下移动。移动之后，优先级会重新设置以匹配新的顺序。

更改策略优先级的步骤如下：


- 1 在分区选择策略表中，单击选择策略的优先级  图标。显示更改选择策略优先级弹出对话框。

优先权：

更改此选择策略的优先级将导致其在列表中向上或向下移动（在操作中，它们从上到下匹配以选择身份验证分区）。在移动后，优先级将重置为从 1 开始按顺序编号，而且此策略将放置在具有给定优先级值的位置（即，如果您选择的优先级值等于另一项策略的优先级值，则此策略将移动到后者之前或之后）。

为自动优先排序输入 0。

- 2 在优先级字段中，输入所需的优先级。

 注：输入“0”作为自动优先。

- 3 单击确定。分区选择策略表会更新以反映新顺序，包括其他策略的重新排序。

修改选择策略

除了自动创建的默认策略之外，可以修改任何分区选择策略。对于“默认”策略，只能更改所选分区。

更改分区选择策略的步骤如下：

- 1 在分区选择策略表中，单击选择策略的配置列中的编辑图标。显示编辑分区选择策略弹出对话框

对于 位于以下位置的用户... 通过以下方式连接的远程用户... 控制台端口登录：

区域：

接口：

网络：

选择分区：

注释：

- 2 此对话框与“添加分区选择策略”对话框相同，如需有关该对话框的信息，请参阅第 186 页的[添加身份验证分区选择策略](#)。

删除分区选择策略

除了自动创建的默认身份验证分区的默认策略以外，可以删除任何分区选择策略。您可以删除创建的单个策略、多个策略或所有策略。

删除策略的步骤如下：

- 1 在用户 > 分区页面的分区选择策略部分中，单击要删除的策略对应配置列中的删除图标。显示验证消息：

是否确定要删除区域 'LAN', 接口 'X2', 网络 'All Interface IP' 的分区选择策略？

- 2 单击确定。

删除多个策略的步骤如下：

① | 注：无法删除默认分区选择策略。

- 1 在用户 > 分区页面的分区选择策略部分中，通过单击其复选框选择要删除的一个或多个策略。删除按钮随即激活。
- 2 单击删除按钮。显示验证消息：

是否确定要删除所选策略？

- 3 单击确定。

删除所有策略的步骤如下：

- 1 在用户 > 分区页面的分区选择策略部分中，单击全部删除按钮。显示验证消息：

是否确定要删除所有分区选择策略？

- 2 单击确定。

配置进行身份验证分区的服务器、代理和客户端

对于可以配置的每个分区：

用户验证方法	本地用户 RADIUS RADIUS + 本地用户 LDAP LDAP + 本地用户
单点登录办法	SSO 代理 终端服务代理 (TSA) RADIUS 计费 浏览器 NTLM 验证

所有服务器、代理和客户端的身份验证分区都是从用户 > 设置页面配置的；如需有关如何配置这些实体和用户 > 设置页面的完整描述，请参阅第 111 页的[配置用于管理用户的设置](#)。如需有关分区如何影响服务器和代理的配置的描述，请参阅[配置服务器和代理表](#)。

① | 注：服务器、代理和客户端的操作在第 168 页的[具有子分区的服务器、代理和客户端的操作](#)中有进一步描述。

配置服务器和代理

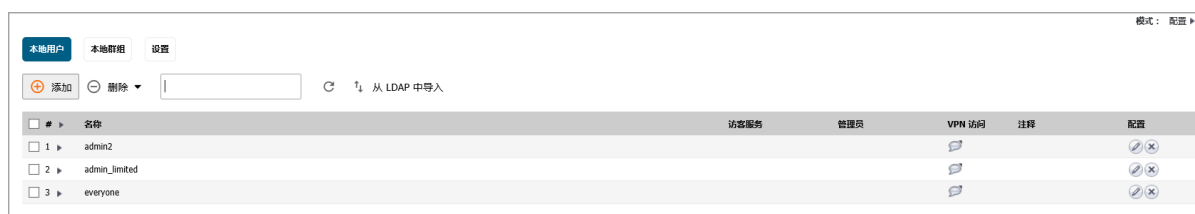
服务器/代理	分区配置
RADIUS 服务器	最多两台 RADIUS 服务器可配置为主要/次要冗余对。可以配置多个 RADIUS 服务器对，每个身份验证分区一个主要/次要对。
LDAP 服务器	可以配置很多个主要 LDAP 服务器，每个身份验证分区一个，外加一个次要服务器列表（请参阅第 140 页的 关于对多个 LDAP 服务器的扩展支持 ）。通常，一个域或一组相互连接的域（活动目录术语中的林）的 LDAP 服务器被分配到每个身份验证分区。
SSO 代理	除了支持负载分担和冗余外，多个 SSO 代理还支持将代理分配给身份验证分区。一组一个或多个代理被分配给每个身份验证分区，并且在每个组内发生负载分担和冗余。
TS 代理	只有用户群组成员资格查找的 LDAP 服务器选择才需要对 TSA 进行分区。由于 TSA 始终提供带有用户名的完整 Windows NetBIOS 域名，所以配置是可选的。因此，在大多数情况下，可以从用户名中派生身份验证分区。
RADIUS 计费客户端	只有用户群组成员查找的 LDAP 服务器选择才需要对 SSO RADIUS 计费客户端进行分区。因为有些（但不是全部）RADIUS 计费客户端在其计费消息中提供带有用户名的域名，所以配置是可选的。因此，在某些情况下，可以从用户名中派生身份验证分区。

配置本地用户和群组

- 第 191 页的[配置本地用户](#)
 - 第 192 页的[查看本地用户](#)
 - 第 192 页的[添加本地用户](#)
 - 第 197 页的[编辑本地用户](#)
 - 第 198 页的[从 LDAP 导入本地用户](#)
 - 第 198 页的[配置访客管理员](#)
- 第 199 页的[配置本地群组](#)
 - 第 200 页的[创建或编辑本地群组](#)
 - 第 208 页的[从 LDAP 导入本地群组](#)
 - 第 208 页的[按 LDAP 位置设置用户成员身份](#)

配置本地用户

本地用户是在 SonicWall 安全设备的本地数据库中存储和管理的用户。在[管理 | 系统设置 | 用户 | 本地用户和群组](#)中，您可以查看和管理所有本地用户、添加新的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 192 页的[查看本地用户](#)
- 第 192 页的[添加本地用户](#)
- 第 197 页的[编辑本地用户](#)
- 第 198 页的[从 LDAP 导入本地用户](#)
- 第 198 页的[配置访客管理员](#)

查看本地用户

您可以在用户 | 本地用户和群组上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。

用户名称右侧的列列出了用户拥有的权限。展开的视图显示用户各项权限的来源群组。

如需：

- 查看用户拥有 VPN 访问权限的网络资源，请将鼠标指针悬停在 VPN 访问列中的备注图标上。
- 从群组中删除用户，请在展开的视图中单击该用户的配置列中的删除图标。请参见  注：如果无法从群组中删除用户，则图标将显示为灰色。
- 编辑用户，请单击该用户的配置列中的编辑图标。请参阅第 197 页的编辑本地用户。
- 删除该行中的用户或群组，请单击该用户的配置列中的删除图标。请参见  注：如果无法从群组中删除本地用户，则图标将显示为灰色。

用户 | 本地用户和群组页面的底部显示本地用户的总数：


全部：3 项

添加本地用户

您可以从用户 | 本地用户和群组页面将本地用户添加到安全设备上的内部数据库中。

 注：如需了解为 SSL VPN 客户端创建用户的过程，请参阅连接指南。

将本地用户添加到数据库的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 本地用户和群组。
- 2 如果分区：
 - 未启用，请转至步骤 3。
 - 已启用，请从身份验证分区下拉菜单中选择这些设置适用的分区。默认设置为全部。 提示：只有在启用了分区时，才会显示此菜单。
- 3 单击添加用户。将显示添加用户对话框。

- 4 在设置中，通过选中**这表示域用户**来指示群组成员身份、访问权限和其他属性是否适用于使用注册域帐户登录的任何域用户。默认情况下未选中该选项。选中后，将显示其他选项。

如果这表示域用户：

- 已选中，则任何属性（如，群组成员身份和访问权限）均适用于使用指定域帐户（通过 RADIUS 或 LDAP 进行身份验证）登录的用户，或由 SSO 标识为帽子域用户的人员。可以将此属性应用于特定域中的指定用户帐户或任何域中拥有给定名称的用户。
- 未选中，则本地用户是本地帐户，而且设置的所有内容仅适用于使用帐户登录并在本地进行身份验证的用户，在这种情况下密码必须在**步骤 8**中进行设置。

- 5 在**名称**字段中输入用户名。

- 6 如果本地用户：

- 代表域用户，则选项会发生更改；请转至**步骤 7**。

- 不代表域用户，请转至**步骤 8**。

- 7 在**域**字段输入域名。可以从下拉菜单中选择**域**范围。如果您输入未列出的域名，则必须输入完整域名，否则将显示一条消息：

请输入完整的域 DNS 名称（例如，“mydom.com”）

如果域是本地域，则必须输入密码。如果不这样做，则会显示一条消息：

注意：因为你正在使用本地认证，用户将不能登录除非用户设置了密码。
您要继续吗？

8 在密码字段，输入用户的密码。密码区分大小写且应该包含 32 个字母和数字的组合，而不得是家人、朋友或宠物的名字。

i | **注：**如果未选中这表示域用户，则必须输入密码。

9 通过在确认密码字段重新输入确认密码。

10 此外，也可以选择性选中用户必须修改密码强制用户在首次登录时更改其密码。

11 选中需要一次性密码，以启用要求 SSL VPN 用户提交系统生成的密码进行双因素身份验证的功能。

i | **提示：**如果未对本地用户启用一次性密码，但已为其所属群组启用，请确保配置了用户的电子邮件地址，否则此用户无法登录。

12 输入用户的电子邮件地址，以使其能收到一次性密码。

13 从帐户生命期中，选择某个用户帐户将存在的持续时间，在此时间之后系统会将其删除或禁用。根据您的选择，将显示更多的选项：

- 从不过期使帐户永久有效。这是默认值。转至步骤 16。
- 分钟、小时或天，指定在删除或禁用用户帐户之前的生命期。如果您选择有限的生命期，则该选项会发生更改：

电子邮件地址：	<input type="text"/>
帐号生命期：	<input type="text"/> 分钟 <input checked="" type="checkbox"/> 当过期时剪除帐号
注释：	<input type="text"/>

14 在帐户生命期字段中输入生命期。最多可以指定 9999 小时、分钟或天。

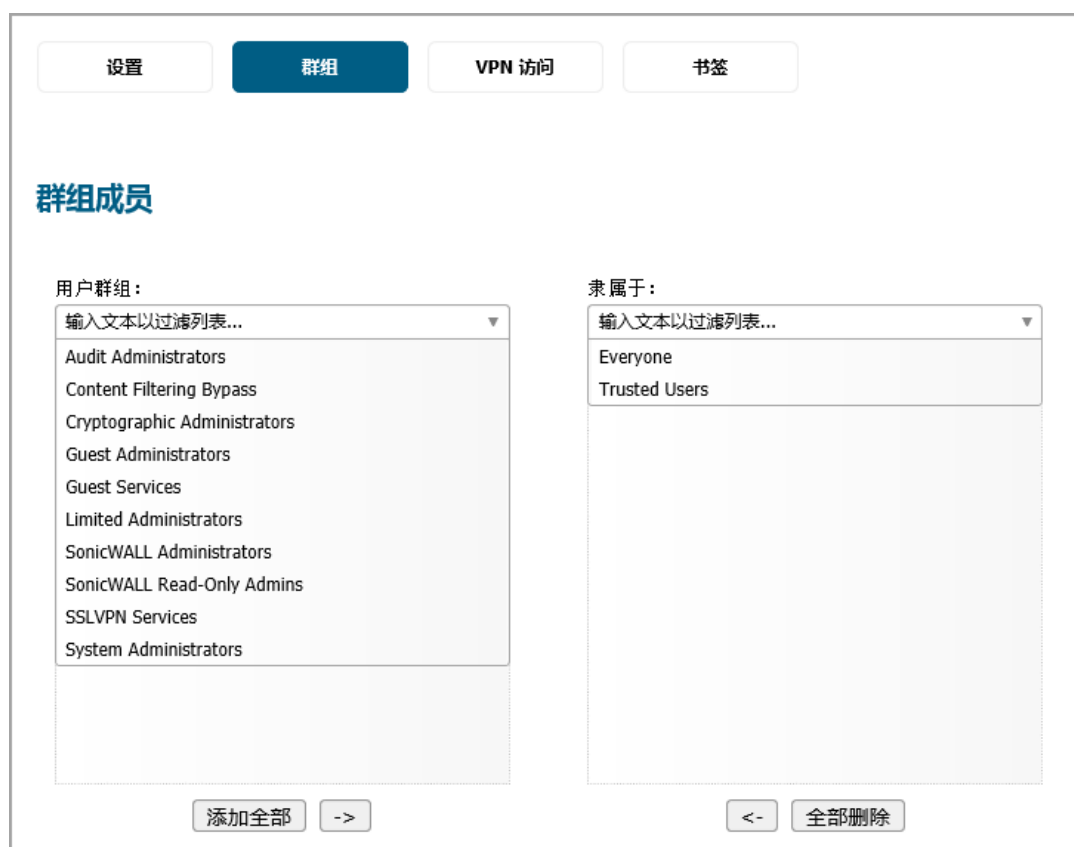
15 如需

- 在生命期过期后删除用户帐户，请选中当过期时剪除帐号。默认情况下已选中该选项。
- 在生命期过期后仅禁用该帐户，请禁用此选项。然后，您可以通过重置帐户生存期来重新启用帐户。

16 可以选择在备注字段中输入备注。

17 单击群组。

群组



1 来自用户群组:

- a 选择用户将属于的一个或多个群组。
- b 您可以

- 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。
- 单击全部添加。

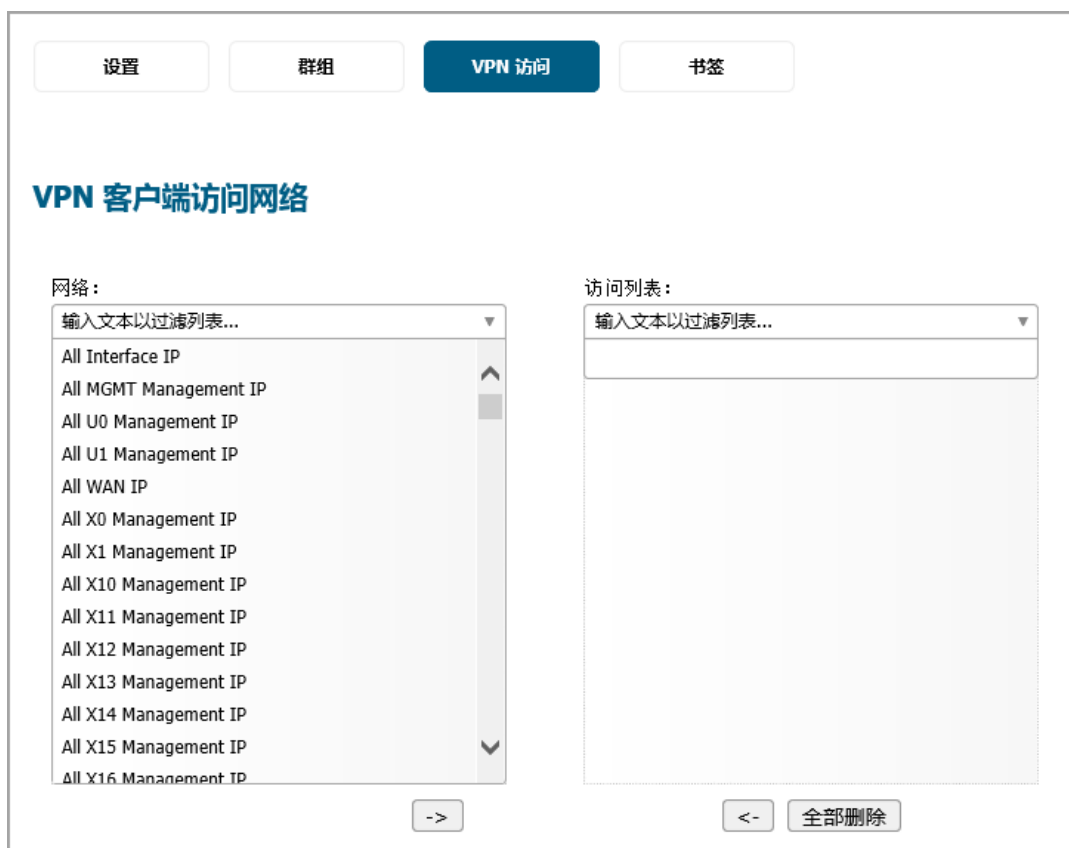
(i) 注：从群组中删除用户的步骤如下：

- 1 从成员列表中选择群组
- 2 您可以
 - 单击左箭头 <- 按钮。
 - 单击全部删除。

注：无法从成员中删除每个人和可信用户。

- 2 如需配置 VPN 用户可以访问的网络资源（GVC、NetExtender 或虚拟办公室书签），请单击 **VPN 访问**。

VPN 访问



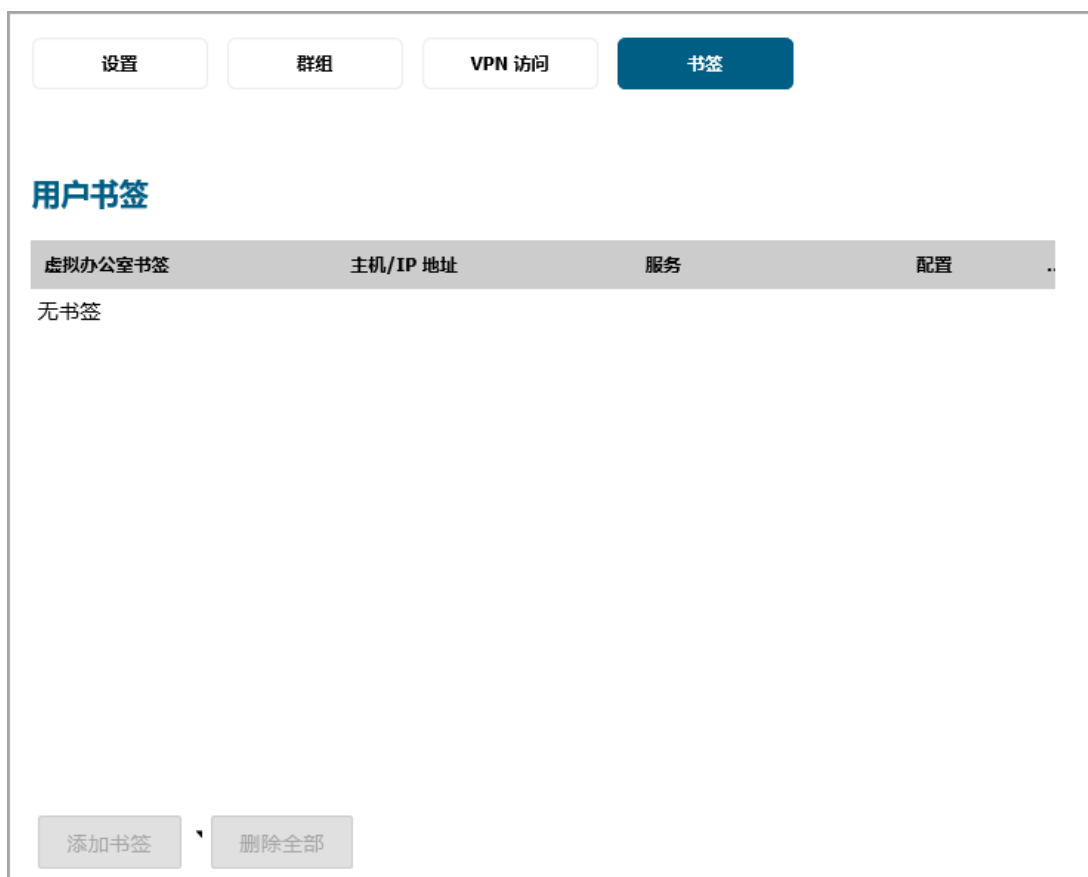
- 1 从网络中选择一个或多个网络。
- 2 单击向右箭头按钮可以将它们移动到访问列表。

注：VPN 访问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。如需允许用户访问网络资源，必须向访问列表中添加网络地址对象或群组。

删除用户对网络的访问权限的步骤如下：

- 从访问列表中选择网络，然后单击左箭头按钮。
 - 单击全部删除。
- 3 如需为属于相关群组的每个用户添加、编辑或删除虚拟办公室书签，请单击书签。

书签



- 4 如需添加书签，请单击**添加书签**按钮。如需**配置 SSL VPN 书签**的信息，请参阅第 X 页的**配置 SSL VPN 书签**。

注：首先用户必须是 SSL VPN 服务群组的成员，然后您才能为他们配置书签。如果用户不是成员，则必须将他们添加到 SSL VPN 服务群组中，并提交更改以启用书签。

- 5 单击**确定**完成用户配置。

编辑本地用户

可以从**用户 | 本地用户和群组**页面编辑本地用户。

编辑本地用户的步骤如下：

- 1 在本地用户表中，单击配置下用户的编辑图标。将显示编辑用户对话框。

设置 群组 VPN 访问 书签

用户设置

这表示域用户

名称: user1

域: 任何域

密码:

确认密码:

用户必须修改密码

需要一次性密码

电子邮件地址:

帐号生命期: 从不过期

注释:

- 2 像添加新用户一样，配置设置、群组、VPN 访问和书签选项。请参阅第 192 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。提供了从列表中删除按钮以及选择不需要用户的多种方法。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。如需了解从 LDAP 服务器中导入用户的方法信息，请参阅[用户 | 设置](#)。

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 | 本地用户和群组。
- 2 单击添加。将显示添加用户对话框。

设置 群组 VPN 访问 书签

用户设置

这表示域用户

名称:

密码:

确认密码:

用户必须修改密码

需要一次性密码

电子邮件地址:

帐号生命期:

注释:

- 3 在名称字段中，指定用户的名称。
- 4 单击**群组**。
- 5 在用户群组列表中选择**访客管理员**。
- 6 单击向右箭头将**访客管理员**移至**成员**列表。
- 7 单击**确定**。
- 8 转至**网络 | 接口**。
- 9 单击 LAN 接口的**编辑**图标。将显示**编辑接口**对话框。
- 10 如需允许访客管理员帐户通过 LAN 登录安全设备，请在**用户登录**下面选中 **HTTP** 和 **HTTPS**。
- 11 单击**确定**。

登录为访客管理员

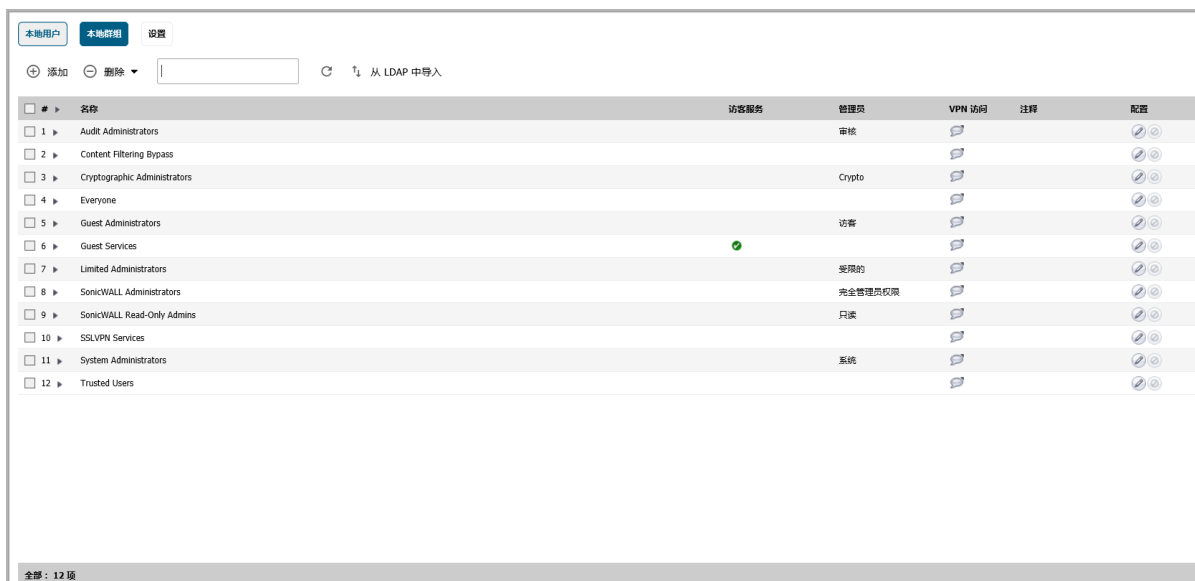
以访客管理员身份登录的步骤如下：

- 1 以访客管理员身份登录安全设备。将出现一个对话框，显示对权限服务的访问权。
- 2 单击**管理**按钮。

登录后，访客管理员可以通过**监控 | 用户会话 > 活动的访客用户**页面来管理访客帐户和会话，但无法访问任何其他资源或管理界面页面。

配置本地群组

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

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

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。

对于远程用户，将显示不适用远程验证的注释图标。

管理员

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。

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。

注释

列出为本地群组提供的任何注释。

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。

主题：

- 第 200 页的[创建或编辑本地群组](#)
- 第 208 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 201 页的添加本地群组](#)
- [第 207 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 | 本地用户和群组。
- 2 单击添加。显示添加群组对话框。



设置 成员 VPN 访问 书签 管理

群组设置

这可以匹配域用户群组 仅在本地设置成员

成员资格根据用户在 LDAP 目录中的位置进行设置

名称:

域: 选择域... ▼

注释:

需要一次性密码

主题：

- [第 202 页的设置](#)
- [第 204 页的成员](#)
- [第 205 页的VPN 访问](#)
- [第 206 页的书签](#)
- [第 207 页的管理](#)

设置

- 1 选择如何设置在用户登录或通过 SSO 进行识别时向其给予此群组的成员身份的方式：

i | **注：** 获得此用户群组的成员身份的用户将获得授予该群组的任何权限和访问权限。

这可以匹配域用户群组（默认值） 将为属于和此用户群组同名的域用户群组的任何用户给予此群组的成员身份。您可以选择具有以下对象的成员身份：

- 仅属于特定域中域用户群组的成员。
- 属于任何域中指定群组的用户。

注： 选择此项后，选项会发生更改。

仅在本地设置成员

本地用户是群组中唯一获得成员身份的用户。默认情况下未选中该选项。

成员身份根据用户在 LDAP 目录中的位置进行设置

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。

注： LDAP 服务器上没有相应的用户群组，并且该群组的成员身份与该域用户群组中设置的任何成员身份都无关。

注： 选择此项后，选项会发生更改。

i | **注：** 在所有情况下，也可以在此对话框的 **成员** 页面上将本地用户（包括代表域用户的用户）和其他用户群组设置为群组成员。

- 2 在名称字段中输入本地群组的名称。

i | **注：** 预定义用户或群组的名称不能编辑，且字段变灰。

- 3 如果选择：

- 这可以匹配域用户群组，选项将发生更改。请转至 **步骤 4**。

这可以匹配域用户群组 仅在本地设置成员

成员资格根据用户在 LDAP 目录中的位置进行设置

名称:

域:

注释:

- 仅在本地设置成员，请转至 **步骤 5**。
- 成员资格根据用户在 LDAP 目录中的位置进行设置，选项将发生更改。请转至 **步骤 5**。

i | **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。

成员资格根据用户在 LDAP 目录中的位置进行设置

名称:

注释:

LDAP 位置:

用户位置 指定位置或指定位置以下 指定位置

需要一次性密码

- 4 在域字段输入域名。可以从下拉菜单中选择域范围。如果您输入未列出的域名，则必须输入完整域名，否则将显示一条消息：

请输入完整的域 DNS 名称（例如，“mydom.com”）

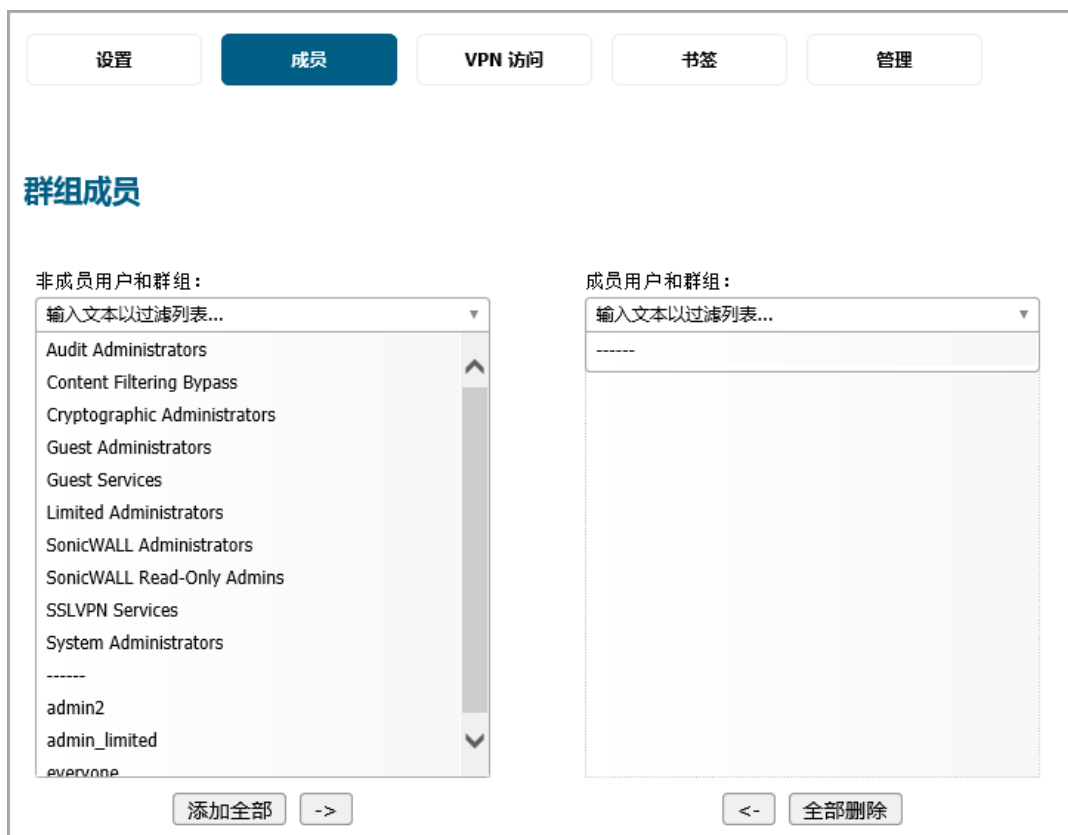
如果域是本地域，则必须输入密码。如果不这样做，则会显示一条消息：

注意：因为你正在使用本地认证，用户将不能登录除非用户设置了密码。您要继续吗？

- 5 可以选择在备注字段中输入描述备注。
- 6 如果选择了这可以匹配域用户群组或仅在本地设置成员，请转至 [步骤 9](#)。
- 7 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。
- 8 从用户位置选项中选择位置所在：
- 指定位置或指定位置以下（默认值）
 - 指定位置
- 9 或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。
- 10 如需：
- 完成添加群组，请单击 **确定**。
 - 添加成员，请转至第 [204](#) 页的 **成员**。

成员

- 1 单击成员。



- 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 如需：

- 将用户和/或群组添加到成员用户和群组列表中：
 - a) 请从非成员用户和群组列表中选择用户和/或群组。
 - b) 单击向右箭头 -> 按钮。
- 添加所有用户和群组，请单击全部添加。

i 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。

如需删除用户和/或群组，请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。如需删除所有的用户和群组，请单击全部删除。

- 4 如需：

- 完成添加群组，请单击确定。
- 指定 VPN 访问，请转至第 205 页的 VPN 访问。

VPN 访问

- 1 单击 VPN 访问。



- 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。

如需删除资源，请从访问列表中选择资源，然后单击左箭头 <- 按钮。如需删除所有资源，请单击全部删除。

- 4 如需：

- 完成添加群组，请单击确定。
- 指定书签，请转至第 206 页的书签。

书签

- 1 单击书签。



- 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。如需配置 SSL VPN 书签的信息，请参阅 SonicOS 连接指南。

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。

- 3 如需：

- 完成添加群组，请单击**确定**。
- 指定该群组是否将具有管理权限，请转至第 207 页的**管理**。

管理

- 1 单击管理。

- 2 如果通过给予新群组其他管理群组的成员身份来使其成为管理群组，请选中成员从网页直接登录到管理界面。默认情况下未选中该选项。
- 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可控制用户开始获得用户群组成员身份时发生的情况，该用户群组提供只读管理（即，SonicWall 只读管理员群组或拥有其成员身份的用户），然后将添加至其他管理用户群组中。如需向用户授予：
 - 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权限（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。在本地用户表中，该用户的**管理员**列将显示另一个群组的指定，如受限的或“完全管理员权限”。
 - 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管理级别，请选择其他群组的管理权限将被限制为只读。在本地用户表中，该用户的**管理员**列将显示双重指定，如只读，受限。
 - ① **提示：**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）。
 - ① **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。将显示“编辑群组”对话框，并且此对话框与“添加组”相同
- 2 遵照第 201 页的添加本地群组中的步骤。

从 LDAP 导入本地群组

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。您可以通过检索 LDAP 服务器中的用户群组名称配置 SonicOS 上的本地用户群组。如需导入本地群组的更多信息，请参阅第 138 页的[用户和群组选项卡](#)。

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 80 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 133 页的[创建 RADIUS 用户的新用户群组](#)。

管理访客服务

- [第 209 页的用户 | 访客服务](#)
 - [第 209 页的全局访客设置](#)
 - [第 210 页的访客配置文件](#)

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。[管理 | 系统设置 | 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](#) 中，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。

全局访客设置

显示带有注销按钮的访客登录状态窗口

访客配置文件

#	名称	用户名前缀	帐户生命周期	会话生命周期	闲置超时	接收限制	传输限制	配额循环	配置
1	Default	guest	7 天	1 小时	10 分钟	无限制	无限制	非循环	

主题：

- [第 209 页的全局访客设置](#)
- [第 210 页的访客配置文件](#)

全局访客设置

“全局访客设置”部分提供了用于显示访客登录状态窗口的选项。窗口会在当前会话中显示剩余时间。用户必须在其登录会话期间保持此窗口处于打开状态，并且可以通过单击登录状态窗口中的注销按钮来注销。

全局访客设置

显示带有注销按钮的访客登录状态窗口

如需配置访客登录状态窗口：

- 1 请选择显示有注销按钮的访客登录状态窗口，以便在用户已登录的情况下显示用户登录窗口中的“注销”按钮。默认情况下已选中该选项。
- 2 单击接受。

访客配置文件

访客配置文件表列出了您已创建的配置文件，并使您可以添加、编辑和删除这些配置文件。始终有一个访客配置文件默认，它由 SonicOS 生成且无法删除，但可以对其进行编辑。

访客配置文件									
#	名称	用户名前缀	帐户生命期	会话生命期	闲置超时	接收限制	传输限制	配额循环	配置
1	Default	guest	7天	1小时	10分钟	无限制	无限制	非循环	 

添加 删除

主题：

- 第 210 页的[添加访客配置文件](#)
- 第 212 页的[编辑访客配置文件](#)
- 第 212 页的[删除访客配置文件](#)

添加访客配置文件

添加配置文件的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 访客服务。
- 2 单击访客配置文件表下方的添加。将显示添加访客配置文件对话框。

配置文件名称：	<input type="text"/>
用户名前缀：	<input type="text" value="guest"/>
<input checked="" type="checkbox"/> 自动生成用户名	
<input checked="" type="checkbox"/> 自动生成密码	
<input checked="" type="checkbox"/> 启用帐户	
<input checked="" type="checkbox"/> 自动删除帐户	
<input checked="" type="checkbox"/> 强制登录唯一性	
<input type="checkbox"/> 首次登录时激活帐户	
帐户生命期：	<input type="text" value="7"/> <input type="text" value="天"/>
闲置超时：	<input type="text" value="10"/> <input type="text" value="分钟"/>
配额循环类型设置：	<input type="text" value="非循环"/>
会话生命期：	<input type="text" value="1"/> <input type="text" value="小时"/>
接收限制 (0 以禁用)：	<input type="text" value="Unlimited"/> MB
传输限制 (0 以禁用)：	<input type="text" value="Unlimited"/> MB
注释：	<input type="text" value="已自动生成"/>

- 3 在**配置文件名称**字段中，输入配置文件的名称。
- 4 在**用户名前缀**字段中，输入根据此配置文件生成的每个用户帐户名称的第一部分。如需允许根据此配置文件生成的访客帐户具有自动生成的用户名，请选中**自动生成用户名**。用户名通常为前缀加上两或三位的数字。默认情况下已选中该选项。
- 5 如需允许根据此配置文件生成的访客帐户具有自动生成的密码，请选中**自动生成密码**。生成的密码为八个字符的唯一字母字符串。默认情况下已选中该选项。
- 6 如需在创建时启用根据此配置文件生成的所有访客帐户，请选中**启用帐户**。默认情况下已选中该选项。
- 7 如需在帐户的生存期过期后将帐户从数据库中删除，请选中**自动删除帐户**。默认情况下已选中该选项。
- 8 如需在任一时间都只允许使用某个帐户的单个实例，请选中**强制登录唯一性**。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。
- 9 如需将帐户过期计时器延迟至用户首次登录帐户，请选中**首次登录时激活帐户**。默认情况下未选中该选项。
- 10 如需定义帐户在过期前保留在安全设备上的时间长度，请在**帐户生命期**中输入持续时间。可以在**会话生命周期**字段中指定 1 到 9999，并从下拉菜单中选择持续时间类型：
 - 分钟
 - 小时
 - 天

默认值为 **7 天**。

- 11 如需定义没有流量通过激活的访客服务会话时的最长时间，请在**闲置超时**：中输入超时持续时间。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。

可以在**会话生命周期**字段中指定 1 到 9999，并从下拉菜单中选择持续时间类型：

- 分钟
- 小时
- 天

默认为 **10 分钟**。

- 12 如需指定配额循环类型，请从**配额循环类型**设置下拉菜单中选择：

- 非循环（默认）
- 每天
- 每周
- 每月

- 13 如需定义访客登录会话在激活后保持有效的持续时间，请在**会话生命周期**中指定此持续时间。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。

可以在**会话生命周期**字段中指定 1 到 9999，并从下拉菜单中选择持续时间类型：

- 分钟
- 小时

- 天

默认值为 **1 小时**。

- 14 要限制用户可以接收的数据量，请在**接收限制（0 禁用）**字段中输入数量，单位为 MB。范围从 0（无法接收数据）到 999999999 MB 到**无限制（默认）**。
- 15 要限制用户可以发送的数据量，请在**发送限制（0 禁用）**字段中输入数量，单位为 MB。范围从 0（无法接收数据）到 999999999 MB 到**无限制（默认）**。
- 16 可以选择在**备注**字段中输入描述备注。默认设置为**已自动生成**。
- 17 单击**确定**。

编辑访客配置文件

编辑访客配置文件的步骤如下：

- 1 单击该配置文件的**配置**列中的**编辑**图标。
- 2 遵照第 210 页的**添加访客配置文件**中的步骤。

i | **注：**编辑默认配置文件时，您可以编辑除配置文件名称和用户名前缀以外的所有选项；这些选项将显示为灰色。

删除访客配置文件

可以删除默认配置文件以外的所有访客配置文件。

删除访客配置文件的步骤如下：

- 1 选择以下其中一种格式：
 - 要删除的访客配置文件的复选框。
 - 访客配置文件表中的复选框。所有复选框（默认配置文件除外）都处于选中状态。

删除按钮随即激活。

- 2 单击**删除**。将显示确认消息：

是否确定要删除所选择的条目？

- 3 单击**确定**。

管理访客帐户

- 第 213 页的[用户 | 访客帐户](#)
 - 第 213 页的[查看访客帐户统计](#)
 - 第 215 页的[添加访客帐户](#)
 - 第 221 页的[启用访客帐户](#)
 - 第 221 页的[启用访客帐户自动删除](#)
 - 第 222 页的[打印帐户详细信息](#)

用户 | 访客帐户

管理 | 系统设置 | 用户 | 访客帐户列出 SonicWall 安全设备上的访客服务帐户。您可以启用或禁用各帐户、帐户群组或所有帐户，可以设置帐户的自动删除功能，而且可以添加、编辑、删除和打印帐户。

#	名称	启用	自动删除	帐号过期	会话过期	闲置超时	接收限制	传输限制	配置循环	统计	注释	配置
1	guest98937	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 分钟			非循环			

添加访客 生成 导出 删除 删除所有

主题：

- 第 213 页的[查看访客帐户统计](#)
- 第 215 页的[添加访客帐户](#)
- 第 221 页的[启用访客帐户](#)
- 第 221 页的[启用访客帐户自动删除](#)
- 第 222 页的[打印帐户详细信息](#)

查看访客帐户统计

访客帐户表显示有关访客帐户的统计信息。

主题：

- 第 214 页的[查看流量统计信息](#)
- 第 214 页的[查看帐户过期](#)
- 第 214 页的[查看会话过期](#)
- 第 214 页的[查看接收和发送限制统计信息](#)
- 第 215 页的[导出访客帐户](#)

查看流量统计信息

查看访客帐户的相关流量统计信息的步骤如下：

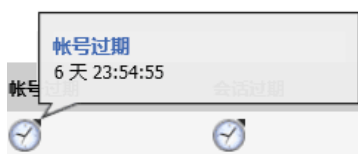
- 1 将鼠标指针悬停在访客帐户的统计信息列中的统计信息图标上。流量统计信息弹出窗口显示为所有已完成会话发送和接收的累计总字节数和数据包数。当前活动的会话不会添加到统计信息中，直到访客用户注销。



查看帐户过期

查看帐户过期前的剩余时间的步骤如下：

- 1 将鼠标指针悬停在访客帐户的帐号过期列中的时钟图标上。帐号过期弹出窗口显示访客帐户的剩余时间。



查看会话过期

查看会议过期前的剩余时间的步骤如下：

- 1 将鼠标指针悬停在访客帐户的帐户过期列中的时钟图标上。帐户过期弹出窗口显示访客帐户的剩余时间。



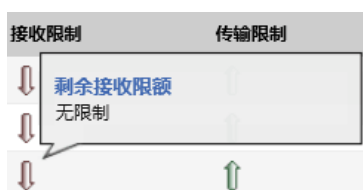
注： 如果用户的会话尚未开始，则会话过期弹出窗口会显示未使用。

查看接收和发送限制统计信息

对于表中的每个用户帐户，接收限制列包含一个红色的向下箭头图标，而发送限制列包含一个绿色的向上箭头图标。

查看接收/发送限制统计信息的步骤如下：

- 1 将鼠标指针悬停在访客帐户的接收限制/发送限制列中的箭头图标上。剩余接收限额弹出窗口显示访客用户可以下载或发送的剩余数据量。

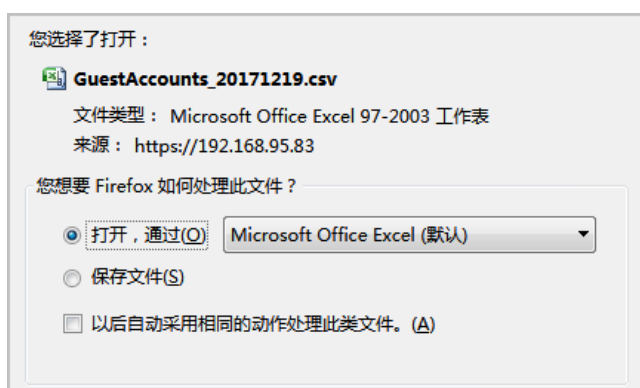


导出访客帐户

可以将访客帐户表导出为 .csv 文件。此文件不仅包含所有显示的数据，还包含限制和剩余的接收和发送数据统计信息。

将访客帐户导出为 .csv 文件的步骤如下：

- 1 在访客帐户表下，单击导出。将显示正在打开 `guestaccounts_nnn.csv` 对话框。



- 2 您可以：
 - 打开文件以进行查看。
 - 稍后保存该文件。
- 3 单击确定。

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。

主题：

- 第 216 页的[添加访客帐户](#)
- 第 218 页的[生成多访客帐户](#)

添加访客帐户

添加单独的帐户的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 访客帐户。
- 2 在访客帐户表下，单击添加访客。将显示添加访客对话框。

The screenshot shows a web interface for adding a guest user. At the top, there are two tabs: '设置' (Settings) and '访客服务' (Guest Services). Below the tabs is the title '用户设置' (User Settings). The form contains the following fields and controls:

- 配置文件:** A dropdown menu with 'Default' selected.
- 名称:** A text input field containing 'guest23454' and a '生成' (Generate) button to its right.
- 注释:** An empty text input field.
- 密码:** A text input field and a '生成' (Generate) button to its right.
- 确认密码:** An empty text input field.

- 3 从配置文件中，选择要根据其生成此帐户的访客配置文件。默认配置文件是默认。
- 4 可以通过下列两种方式之一命名访客帐户：
 - 在名称字段中输入帐户的名称。
 - 单击生成使 SonicOS 生成名称。所生成的名称是配置文件的第一个名称，它由 guest 这个词和一个随机的两到五位数字组成。例如：
 - guest1235（用于默认配置文件）
 - TechPubs guest51026（用于 TechPubs 访客配置文件）
- 5 可以选择在注释字段中输入描述备注。默认备注是自动生成的。
- 6 通过下列两种方式之一创建用户帐户密码：
 - 在密码字段和“确认”字段中输入密码。此密码最多可以包含 32 个字母数字字符。
 - 单击生成。生成的密码是随机的八位字母字符串。

提示： 记下密码。否则，您必须重置它。

7 单击访客服务。

设置 访客服务

访客服务

启用访客服务特权

强制登录唯一性

帐号过期时自动删除帐号

首次登录时激活帐号

帐号过期: 7 天

闲置超时: 10 分钟

配额循环类型设置: 非循环

会话生命期: 1 小时

接收限制 (0 以禁用): Unlimited MB

传输限制 (0 以禁用): Unlimited MB

- 8 如需在创建时启用帐户，请选中**启用访客服务特权**。默认情况下已选中该选项。
- 9 如需一次只允许此帐户的一个实例登录安全设备，请选中**强制登录唯一性**。取消选中该选项将允许多个用户同时使用此帐户。默认情况下已选中该选项。
- 10 如需在帐户生存期过期后将其从数据库中删除，请选中**帐号过期时自动删除帐号**。默认情况下已选中该选项。
- 11 如需开始对帐户过期进行计时，请选中**首次登录时激活帐号**。
- 12 如需定义帐户过期之前在安全设备上的剩余时间，请在**帐号过期**中输入过期日期。可以在**帐号过期**字段中指定从 1 到 9999 的值，然后从下拉菜单中选择持续时间类型：
 - 分钟
 - 小时
 - 天

默认值为 7 天。

如果**帐号过期时自动删除帐号**：

- 已启用，则帐户将在过期后删除。
- 已禁用，帐户将以**已过期**状态保留在**访客帐户表**中，以实现轻松重新激活。

注：此设置将覆盖第 210 页的**访客配置文件**中设置的帐户生存期。

- 13 如需定义没有流量通过激活的访客服务会话时的最长时间，请在**闲置超时**：中输入超时持续时间。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**会话生命期**中设置的值。

注：该设置替代配置文件中的**闲置超时**设置。

可以在**会话生命期**字段中指定 1 到 9999，并从下拉菜单中选择持续时间类型：

- 分钟

- 小时
- 天

默认为 **10 分钟**。

14 如需指定配额循环类型，请从**配额循环类型设置**下拉菜单中选择：

- 非循环（默认）
- 每天
- 每周
- 每月

15 如需定义访客登录会话在激活后保持有效的持续时间，请在**会话生命期**中指定此持续时间。默认为在访客用户首次登录帐户时激活。**会话生命期**不能超过在**帐户生命周期**中设置的值。

i | **注：**该设置替代配置文件中的会话生命周期设置。

可以在**会话生命期**字段中指定 **1** 到 **9999**，并从下拉菜单中选择持续时间类型：

- 分钟
- 小时
- 天

默认值为 **1 小时**。

16 **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。

17 **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。

18 要限制用户可以接收的数据量，请在**接收限制 (0 禁用)**字段中输入数量，单位为 MB。范围从 **0**（无法接收数据）到 **999999999 MB** 到**无限制（默认）**。

19 要限制用户可以发送的数据量，请在**发送限制 (0 禁用)**字段中输入数量，单位为 MB。范围从 **0**（无法接收数据）到 **999999999 MB** 到**无限制（默认）**。

20 单击**确定**生成帐户。

生成多访客帐户

生成多个帐户的步骤如下：

- 1 转至**管理 | 系统设置 | 用户 | 访客帐户**。
- 2 在**访客帐户表**下，单击**生成**。随即显示**生成访客帐户**对话框。

- 3 从配置文件中，选择生成帐户时依据的访客配置文件。默认值为默认。
- 4 输入要在帐号数字段中生成的帐户数。可以创建 1 到 6000 个帐户
- 5 在用户名字段中输入生成帐户名称时依据的前缀。例如，如果您输入 **Guest**，则已生成帐户的名称将类似于 Guest123 和 Guest234。默认前缀是 **guest**。
- 6 在注释字段中，输入最多包含 16 个字母数字字符的描述性备注。
- 7 单击访客服务。

- 8 如需在创建时启用帐户，请选中**启用访客服务特权**。默认情况下已选中该选项。
- 9 如需一次只允许此帐户的一个实例登录安全设备，请选中**强制登录唯一性**。取消选中该选项将允许多个用户同时使用此帐户。默认情况下已选中该选项。
- 10 如需在帐户生存期过期后将其从数据库中删除，请选中**帐号过期时自动删除帐号**。默认情况下已选中该选项。

注：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。

- 11 如需开始对帐户过期进行计时，请选中**首次登录时激活帐号**。
- 12 如需定义帐户过期之前在安全设备上的剩余时间，请在**帐号过期**中输入过期日期。可以在**帐号过期**字段中指定从 1 到 9999 的值，然后从下拉菜单中选择持续时间类型：

- 分钟
- 小时
- 天

默认值为 **7 天**。

如果帐号过期时自动删除帐号：

- 已启用，则帐号将在过期后删除。
- 已禁用，帐号将以**已过期**状态保留在**访客帐户表**中，以实现轻松重新激活。

i | 注：此设置将覆盖第 **210** 页的**访客配置文件**中设置的帐户生存期。

- 13 如需定义没有流量通过激活的访客服务会话时的最长时间，请在**闲置超时**：中输入超时持续时间。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**会话生命期**中设置的值。

i | 注：该设置替代配置文件中的**闲置超时**设置。

可以在**会话生命期**字段中指定 **1** 到 **9999**，并从下拉菜单中选择持续时间类型：

- 分钟
- 小时
- 天

默认为 **10 分钟**。

- 14 如需指定配额循环类型，请从**配额循环类型**设置下拉菜单中选择：

- 非循环（默认）
- 每天
- 每周
- 每月

- 15 如需定义访客登录会话在激活后保持有效的持续时间，请在**会话生命期**中指定此持续时间。默认为在访客用户首次登录帐户时激活。**会话生命期**不能超过在**帐户生命周期**中设置的值。

i | 注：该设置替代配置文件中的**会话生命周期**设置。

可以在**会话生命期**字段中指定 **1** 到 **9999**，并从下拉菜单中选择持续时间类型：

- 分钟
- 小时
- 天

默认值为 **1 小时**。

- 16 **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。
- 17 **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。
- 18 要限制用户可以接收的数据量，请在**接收限制 (0 禁用)** 字段中输入数量，单位为 **MB**。范围从 **0**（无法接收数据）到 **999999999 MB** 到**无限制**（默认）。

19 要限制用户可以发送的数据量，请在**发送限制**（**0 禁用**）字段中输入数量，单位为 MB。范围从 0（无法接收数据）到 999999999 MB 到**无限制**（默认）。

20 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的名称旁边**启用**列中的复选框。如需启用所有帐户，请选中表标题中的**启用**复选框。
- 2 单击**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。

注：这将覆盖在配置用户配置文件或访客帐户时设置的自动删除选项。

启用自动删除的步骤如下：

- 1 选中帐户名称旁边**自动删除**列中的复选框。如需在所有帐户上启用它，请在表标题中选择**自动删除**复选框。
- 2 单击**接受**。

编辑访客帐户

编辑访客帐户的步骤如下：

- 1 单击该配置文件的**配置**列中的**编辑**图标。
- 2 遵照第 210 页的**添加访客配置文件**中的步骤。

注：编辑默认配置文件时，您可以编辑除配置文件名称和用户名前缀以外的所有选项；这些选项将显示为灰色。

删除访客帐户

可以删除默认配置文件以外的所有访客配置文件。

删除访客帐户的步骤如下

- 1 单击访客帐户的删除图标。将显示确认消息：

是否确定要删除 用户 "guest71534"?

- 2 单击**确定**。

删除一个或多个访客帐户的步骤如下：

- 1 转至管理 | 系统设置 | 用户 | 本地用户和群组。
- 2 选中要删除的访客配置文件的复选框。删除按钮随即激活。
- 3 单击删除。将显示确认消息：

是否确定要删除所选择的条目？

- 4 单击确定。

删除所有访客帐户的步骤如下：

- 1 选中访客帐户表标题中的复选框。所有复选框（默认配置文件除外）都处于选中状态。全部删除按钮将激活。
- 2 单击全部删除。将显示确认消息：

您确定要删除所有的条目吗？

- 3 单击确定。

打印帐户详细信息

您可以打印访客帐户的摘要信息。

打印访客帐户的详细信息的步骤如下

- 1 单击打印图标以显示摘要帐户报告和打印对话框。

访客帐户详细信息	
说明	值
帐户名:	guest98937
密码:	
已启用:	是
备注:	
已创建:	MON DEC 18 01:13:59 2017
帐户过期:	MON DEC 25 01:13:59 2017
会话过期:	未使用
会话生命周期:	1 小时
闲置超时:	10 分钟
接收限制:	无限制
发送限制:	无限制
配额循环:	非循环

- 2 单击确定可以将摘要发送到打印机。

- 配置接口
- PortShield 配置接口
- 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 DNS 代理设置
- 配置路由通告和路由策略
- 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

配置接口

- 第 225 页的关于接口
 - 第 225 页的物理和虚拟接口
 - 第 227 页的 SonicOS 安全对象
 - 第 228 页的透明模式
 - 第 228 页的 IPS 探查器模式
 - 第 230 页的 Firewall Sandwich
 - 第 230 页的 HTTP/HTTPS 重定向
 - 第 230 页的在接口上启用 DNS 代理
- 第 230 页的网络 | 接口
 - 第 232 页的显示/隐藏 PortShield 接口（仅限 IPv4）
 - 第 233 页的接口设置
 - 第 233 页的接口流量统计
- 第 234 页的配置接口
 - 第 234 页的配置静态接口
 - 第 239 页的配置路由模式
 - 第 241 页的在接口上启用带宽管理
 - 第 242 页的配置透明 IP 模式下的接口（连接 L3 子网）
 - 第 245 页的配置无线接口
 - 第 248 页的配置 WAN 接口
 - 第 252 页的配置隧道接口
 - 第 255 页的配置链路聚合和端口冗余
 - 第 259 页的配置虚拟接口（VLAN 子接口）
 - 第 260 页的配置 IPS 探查器模式
 - 第 263 页的配置安全服务（统一威胁管理）
 - 第 264 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 267 页的二层桥接模式
 - 第 283 页的配置二层桥接模式
 - 第 290 页的非对称路由

- 第 291 页的[配置 IPv6 接口](#)
- 第 291 页的[31 位网络](#)
- 第 292 页的[PPPoE 未编号接口支持](#)

关于接口

- 第 225 页的[物理和虚拟接口](#)
- 第 227 页的[SonicOS 安全对象](#)
- 第 228 页的[透明模式](#)
- 第 228 页的[IPS 探查器模式](#)
- 第 230 页的[Firewall Sandwich](#)
- 第 230 页的[HTTP/HTTPS 重定向](#)
- 第 230 页的[在接口上启用 DNS 代理](#)

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，并使物理接口能承载分配至多个接口的流量。

主题：

- 第 225 页的[物理接口](#)
- 第 226 页的[虚拟接口 \(VLAN\)](#)
- 第 227 页的[子接口](#)

物理接口

SonicWall 安全设备的前面板上有一些物理接口。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，请参阅相关入门指南）：

- **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^a
- **10 GE SFP+** - 10 千兆热插接式端口^a
- **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，请参阅 SonicOS 5.0 升级指南。MGMT 端口的默认 IP 地址是 192.168.1.254。

a. 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。若无接口，流量将无法访问或退出该区域。

如需区域的更多信息，请参阅第 329 页的[关于区域](#)。

NSA 6600 和 SuperMassive 9000 系列上的 10 千兆以太网 SFP+ 端口

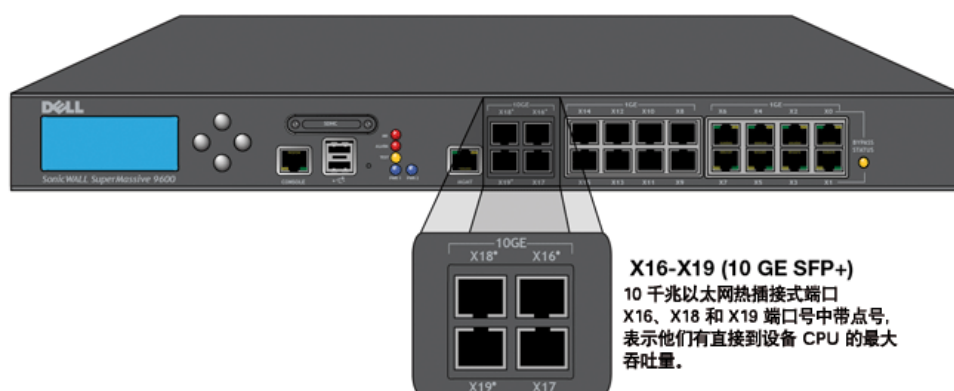
在 NSA 6600 和 SuperMassive 9000 系列设备上，增强的小型插接式 (SFP+) 端口 X16、X18 和 X19 均指定了一个圆点，表示拥有直达 CPU 的最大吞吐量。这些带圆点的端口拥有直达 CPU 的专用（非共享）上行链路。

例如，在您使用 10Gb 企业主干网并使用 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。

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 需要能感知 VLAN 的联网设备来提供这种虚拟化 - 这些设备包括能根据网络设计和安全策略识别、处理、移除和插入 VLAN 标签 (ID) 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 能提供逻辑广播域而非物理广播域（或 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关的 LAN 联合成为在逻辑上相邻的虚拟 LAN。其优点包括：

- **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 - 并非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（且使用相同的工作组交换机），或相反 - 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 未参与任何 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。

i | **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。

i | **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。地址和服务对象分别在 **管理 | 策略 | 对象 > 地址对象** 和 **管理 | 策略 | 对象 > 服务对象** 中进行定义。

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，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，一个或多个 WAN 接口可以主动传输流量，具体取决于 **网络 | 故障切换和负载均衡** 上的 WAN 故障切换和负载均衡配置。

如需 SonicWall 安全设备上 WAN 故障切换和负载均衡的更多信息，请参阅第 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次的顶层。透明模式支持独特的寻址和接口路由。

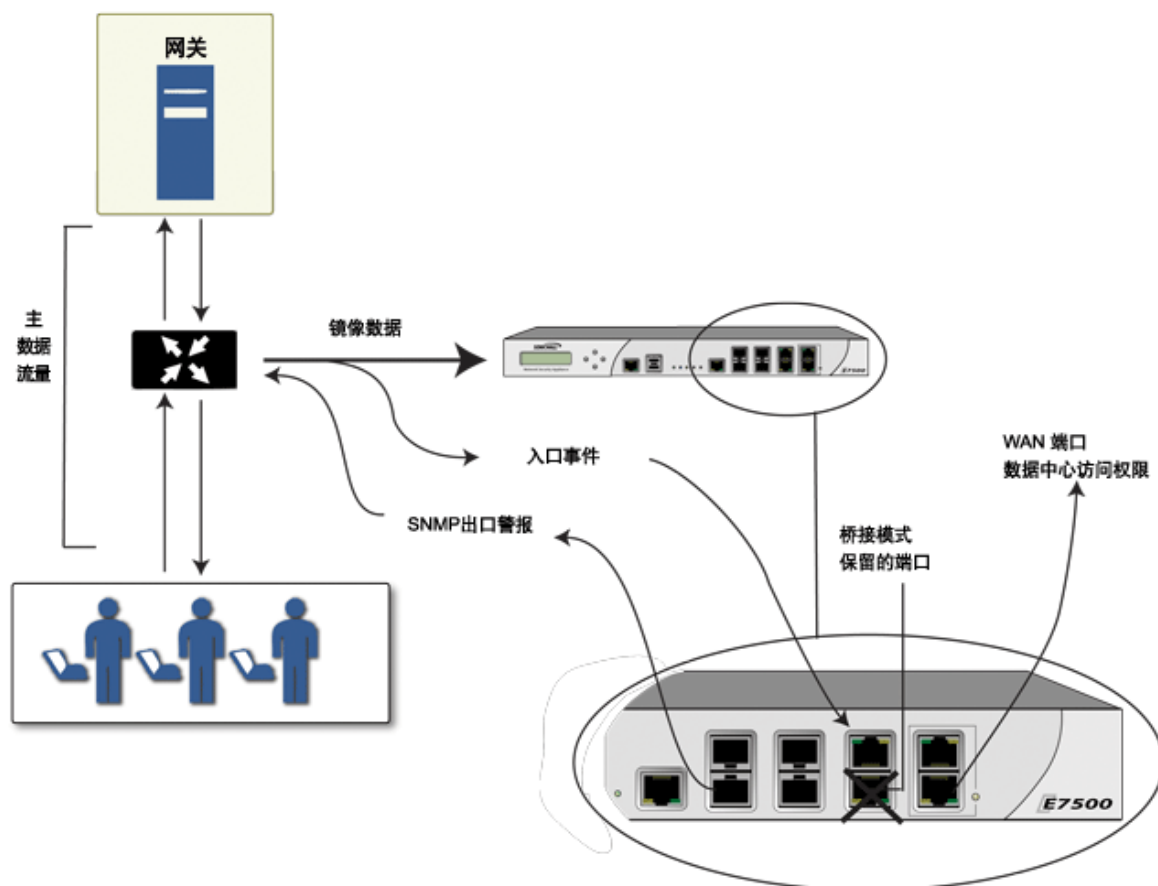
IPS 探查器模式

SonicWall 安全设备支持的 IPS 探查器模式是用于入侵检测的二层桥接模式的变体。IPS 探查器模式配置允许将安全设备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 **IPS 探查器模式：网络图** 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 SonicWall 安全设备上的 IPS 探查器模式端口中。安全设备根据桥接对上配置的设置检查数据包。警报可能会触发 SNMP 陷阱，并通过安全设备上的另一个接口将其发送到指定的 SNMP 过滤器。网络流量在经过安全设备检测后丢弃。

安全设备的 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。

IPS 探查器模式：网络图



在 IPS 探查器模式中，安全设备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，该流量还将发送到镜像端口，并通过镜像端口流入安全设备进行深度包检测。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 探查器模式不会使安全设备接入网络流量，而是仅提供一种方法来检测流量。

可以从网络 | 接口页面访问的编辑接口对话框提供在配置 IPS 探查器模式时使用的选项，即仅捕获该桥接对上的流量。选中该选项时，将使得安全设备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选项，以确保不会将来自镜像交换机端口的流量发回到网络中。

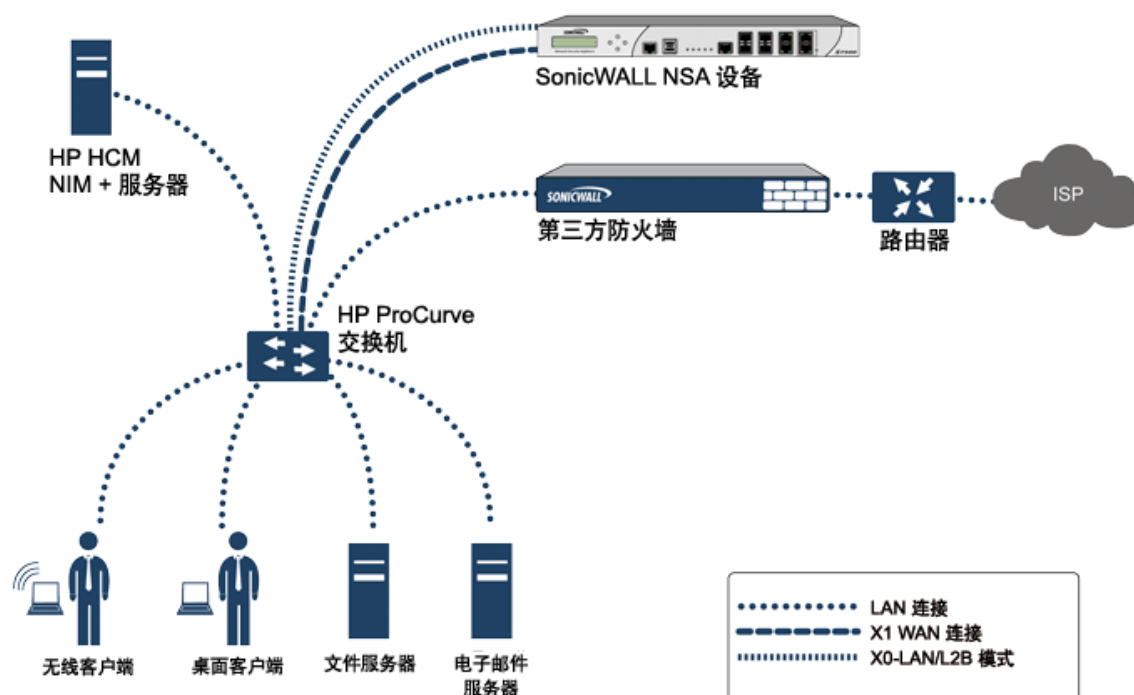
如需在 IPS 探查器模式下配置接口的详细说明，请参阅第 260 页的[配置 IPS 探查器模式](#)。

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：存在现有的安全设备并将继续使用，但希望使用安全设备的安全服务作为探测器。

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。

Firewall Sandwich

您可以部署和配置 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
- SonicWall NSA 2600 和更高版本设备以及 SuperMassive 系列设备。
- 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。

HTTP/HTTPS 重定向

当防火墙配置要求进行用户身份验证时，来自未验证来源的 HTTP/HTTPS 流量会重定向到 SonicOS 登录页面，以使用户输入其凭据。当来自用户未登录的源的 HTTP 和 HTTPS 流量到达且一个或多个此类源反复尝试打开会触发此重定向的新连接时，将发生问题。这些设备可能是有效地尝试获得访问权限的非用户设备，也可能是尝试发起拒绝服务 (DOS) 攻击的恶意代码。它对防火墙的影响是导致 CP 中的 CPU 负载较高，通常出现在发起重定向的数据平面任务以及提供目标重定向页面的 Web 服务器线程任务中。

为了减少这种影响，请确保在添加或编辑接口时选中添加规则，以启用从 HTTP 到 HTTPS 的重定向复选框。启用此复选框可使 SonicOS 向接口中添加允许使用 HTTP 的访问规则；此规则的副作用是在没有任何安全问题的特定情况下还允许 SonicOS 将 HTTPS 重定向到 HTTP。重定向需验证流量的第一步便属于这样一种情况，此时并没有需要隐藏的任何敏感数据。接下来，可以在数据平面 (DP) 而非 CP 上进行 HTTP 处理。

注：在添加或编辑 VPN 隧道接口或为模式/IP 分配选择了有线模式（2-端口有线）、分接模式（1-端口分接）或 PortShield 交换机模式时，该选项不可用。

在接口上启用 DNS 代理

全局启用 DNS 代理后，可以在各个接口上启用它。通过此操作，用户可以单独对不同网段启用此功能。如需了解在接口上启用 DNS 代理的方法，请参阅第 365 页的[启用 DNS 代理](#)。

网络 | 接口

网络 | 接口页面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 与上述安全设备以及 TZ 和 SOHO 安全设备之间有一些细微差别。在这些差异发生的地方对其进行了注释。

NSA 2600 和上述安全设备

接口设置
视图 IP 版本: IPv4 IPv6

名称	区域	群组	IP 地址	子网掩码	IP 分配	状态	已启用	备注	配置
X0	LAN		192.168.168.168	255.255.255.0	静态	无链接	<input checked="" type="checkbox"/>	Default LAN	
X1	WAN	Default LB Group	192.168.95.83	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	Default WAN	
X2	LAN		192.168.94.83	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	WXA series appliance	
X2-V402	WLAN		172.16.16.83	255.255.255.0	静态	VLAN 子接口	<input checked="" type="checkbox"/>		
X3	WAN		0.0.0.0	0.0.0.0	PPPoE	连接	<input checked="" type="checkbox"/>	1 Gbps 全双工	
X4	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X5	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X6	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X7	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X8	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X9	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X10	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X11	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X12	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X13	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X14	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X15	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X16*	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X17	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X18*	未分配		0.0.0.0	0.0.0.0	N/A	10 Gbps 全双工	<input checked="" type="checkbox"/>		
X19*	未分配		0.0.0.0	0.0.0.0	N/A	10 Gbps 全双工	<input checked="" type="checkbox"/>		
MGMT*	MGMT		192.168.1.254	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	Default MGMT	
U0	WAN		0.0.0.0	0.0.0.0	拨号	管理	<input checked="" type="checkbox"/>	Module	

添加接口: 显示 PORTSHIELD 接口

接口流量统计 显示所有流量 [清除](#)

名称	收到的单播数据包	接收的广播数据包	收到的错误数	接收的字节数	发送的单播数据包	发送的广播数据包	发送的错误数	发送的字节数
X0	0	0	0	0	0	14,116	0	903,650
X1	251,931	175,508	0	43,157,401	330,634	169	0	91,774,063
X2	42,090	843,846	0	91,293,930	230,871	14,074	0	18,798,562
X2-V402	8,662	130,788	0	13,990,301	13,648	14,031	0	2,086,203
X3	0	102,756	0	6,576,384	0	7,367	0	279,950
X4	0	0	0	0	0	0	0	0
X5	0	0	0	0	0	0	0	0
X6	0	0	0	0	0	0	0	0
X7	0	0	0	0	0	0	0	0
X8	0	0	0	0	0	0	0	0
X9	0	0	0	0	0	0	0	0
X10	0	0	0	0	0	0	0	0
X11	0	0	0	0	0	0	0	0
X12	0	0	0	0	0	0	0	0
X13	0	0	0	0	0	0	0	0
X14	0	0	0	0	0	0	0	0
X15	0	0	0	0	0	0	0	0
X16*	0	0	0	0	0	0	0	0
X17	0	0	0	0	0	0	0	0
X18	0	0	0	0	0	0	0	0
X19	0	0	0	0	0	0	0	0
MGMT	0	0	0	0	0	10	0	974
U0	0	0	0	678,985	0	0	0	301,624

TZ 和 SOHO 安全设备

Interface Settings
View IP Version: IPv4 IPv6

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Enabled	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	<input checked="" type="checkbox"/>	Default LAN	
X1	WAN	Default LB Group	10.203.28.31	255.255.255.0	Static	1 Gbps Full Duplex	<input checked="" type="checkbox"/>	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	<input checked="" type="checkbox"/>		
W0	WLAN		172.16.31.1	255.255.255.0	Static	1300 Mbps Half Duplex	<input checked="" type="checkbox"/>	Default WLAN	

Add Interface: SHOW PORTSHIELD INTERFACES

Interface Traffic Statistics Display All Traffic [Clear](#)

Name	Rx Unicast Packets	Rx Broadcast Pack...	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Pack...	Tx Errors	Tx Bytes
X0	0	0	0	0	0	0	0	0
X1	160,599	1,538,132	0	133,842,486	123,148	1,001	0	74,628,243
X2	0	0	0	0	0	0	0	0
W0	0	0	0	0	0	10	0	866

主题：

- 第 232 页的显示/隐藏 PortShield 接口（仅限 IPv4）
- 第 233 页的接口设置
- 第 233 页的接口流量统计
- 第 225 页的物理和虚拟接口
- 第 227 页的 SonicOS 安全对象
- 第 228 页的透明模式
- 第 228 页的 IPS 探查器模式
- 第 234 页的配置接口
- 第 260 页的配置 IPS 探查器模式
- 第 264 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 267 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
- 第 291 页的 31 位网络
- 第 292 页的 PPPoE 未编号接口支持

显示/隐藏 PortShield 接口（仅限 IPv4）

在 IPv4 模式下，您可以通过单击显示 PortShield 接口来显示接口设置和接口流量统计表中的 PortShield 接口。这将显示 PortShield 接口且该按钮变为隐藏 PortShield 接口。

The screenshot displays the 'Interface Settings' page in SonicOS. At the top right, there is a 'View IP Version' selector with 'IPv4' selected. Below this is a table of interfaces with columns: Name, Zone, Group, IP Address, Subnet Mask, IP Assignment, Status, Enabled, Comment, and Configure. Interfaces X3 and X4 are marked as 'PortShield to X0'. Below the table are buttons for 'Add Interface: --Select Interface Type--', 'PORTSHIELD WIZARD', and 'HIDE PORTSHIELD INTERFACES'. A section titled 'Interface Traffic Statistics' includes a 'Display All Traffic' checkbox and a 'Clear' button. Below this is a traffic statistics table with columns: Name, Rx Unicast Packets, Rx Broadcast Pack..., Rx Errors, Rx Bytes, Tx Unicast Packets, Tx Broadcast Pack..., Tx Errors, and Tx Bytes.

Name	Rx Unicast Packets	Rx Broadcast Pack...	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Pack...	Tx Errors	Tx Bytes
X0	0	0	0	0	0	0	0	0
X1	162,860	1,539,013	0	134,307,205	125,836	1,002	0	76,358,058
X2	0	0	0	0	0	0	0	0
X3	0	0	0	0	0	0	0	0
X4	0	0	0	0	0	0	0	0
W0	0	0	0	0	0	10	0	866

如需隐藏 PortShield 接口，请单击隐藏 PortShield 接口。

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。未配置的区域指定为未分配的。
- 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 - 为接口分配的 IP 地址。
- 子网掩码 - 为子网分配的网络掩码。
- IP 分配 - 可用的 IP 分配方法取决于将接口分配到的区域：

 注：有线模式和分接模式仅在 NSA 2600 及更高版本的安全设备上可用。

- LAN：静态、透明、二层桥接模式、有线模式、Tap 模式、PortShield 交换机模式、IP 未编号模式
- 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、IP 未编号模式
- WLAN：静态、二层桥接模式、PortShield 交换机模式
- PortShield 到 Xn（仅限 IPv4 视图）：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。
- 注释 - 任何用户指定的注释。
- 配置 - 单击编辑图标可显示编辑接口对话框，可以在其中配置指定接口的设置。如需配置接口的信息，请参阅第 234 页的[配置接口](#)。

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。

- 名称 - 接口的名称。
- 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。
- 接收的广播数据包数或接收的组播数据包数 - 指示该接口所接收的多点通讯数。
- 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）。

如需清除当前统计信息，请单击网络 | 接口右上方的清除按钮。

配置接口

主题：

- [第 234 页的配置静态接口](#)
- [第 239 页的配置路由模式](#)
- [第 241 页的在接口上启用带宽管理](#)
- [第 242 页的配置透明 IP 模式下的接口（连接 L3 子网）](#)
- [第 245 页的配置无线接口](#)
- [第 248 页的配置 WAN 接口](#)
- [第 252 页的配置隧道接口](#)
- [第 255 页的配置链路聚合和端口冗余](#)
- [第 259 页的配置虚拟接口（VLAN 子接口）](#)
- [第 260 页的配置 IPS 探查器模式](#)
- [第 263 页的配置安全服务（统一威胁管理）](#)
- [第 264 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 267 页的二层桥接模式](#)
- [第 283 页的配置二层桥接模式](#)
- [第 290 页的非对称路由](#)
- [第 291 页的配置 IPv6 接口](#)
- [第 291 页的 31 位网络](#)
- [第 292 页的 PPPoE 未编号接口支持](#)

配置静态接口

如需接口的常规信息，请参阅第 225 页的[物理和虚拟接口](#)。

静态意味着为接口分配固定 IP 地址。

配置静态接口的步骤如下：

- 1 转至[管理 | 网络 | 接口](#)。
- 2 在[接口设置表](#)中，单击您要配置的接口的[编辑图标](#)。将显示[编辑接口对话框](#)。

3 从区域中选择一个要分配给该接口的区域：

- 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框。如需添加区域的说明，请参阅第 329 页的[关于区域](#)。

i 注：显示的选项随着您选择的区域而变化。

4 从 IP 分配中，选择：

- 静态（WAN 的默认值）
- 静态 IP 模式（LAN 的默认值）

5 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。

i 注：不能输入与其他区域位于同一子网中的 IP 地址。

6 如果要配置：

- WAN 区域接口或 MGMT 接口，请在默认网关字段中输入网关设备的 IP 地址。

i 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。默认网关 IP 在 LAN 接口上是可选的。

- LAN 区域接口或 DMZ 区域接口，请有选择地在默认网关（可选）字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。

7 如果要配置：

- LAN 区域接口，请转至[步骤 8](#)。
- WAN 区域接口，请在 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，请参阅第 248 页的[配置 WAN 接口](#)。

8 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设置表的注释列中。

9 如果要启用通过此接口远程管理安全设备，请选择支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。如果选择了 **HTTPS**，则添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向将激活并处于选中状态。

如需允许访问 WAN 接口，以便从同一安全设备的其他区域进行管理，则必须创建访问规则。如需允许从 LAN 区域访问 WAN 主要 IP 的更多信息，请参阅 SonicOS 策略。

10 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。

11 单击确定。

i | 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

配置静态接口的高级设置的步骤如下。

1 在编辑接口对话框中，单击高级。

i | 注：静态接口的高级中提供的选项随所选区域而异。

编辑接口高级设置 - WAN

常规 **高级**

高级设置

链接速度: 自动协商

使用默认 MAC 地址: C0:EA:E4:59:8E:25

覆盖默认 MAC 地址:

关闭端口

启用流量报告

启用组播支持

启用 802.1p 标记

从路由通知中排除 (NSM, OSPF, BGP, RIP)

启用非对称路由支持

冗余/聚合端口: 无

专门的模式设置

使用路由模式 - 添加 NAT 策略以阻止出站/入站转换

NAT 策略出站/入站接口: Any

接口 MTU: 1500

对大于该接口 MTU 的非 VPN 出口数据包进行分片

忽略不分片 (DF) 位

当出口数据包大于该接口的 MTU 时不要发送 ICMP 分片消息

编辑接口高级设置 - LAN

常规 高级

高级设置

链接速度:

使用默认 MAC 地址:

覆盖默认 MAC 地址:

关闭端口

启用流量报告

启用组播支持

启用 802.1p 标记

从路由通知中排除 (NSM, OSPF, BGP, RIP)

启用非对称路由支持

冗余/聚合端口:

专门的模式设置

使用路由模式 - 添加 NAT 策略以阻止出站/入站转换

NAT 策略出站/入站接口:

接口 MTU:

- 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 - 全工
100 Mbps - 全双工	
100 Mbps - 半工	
10 Mbps - 全双工	
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安全设备的连接速度和双工模式。

- 默认选择使用默认 **MAC** 地址。您可以通过选择覆盖默认 **MAC** 地址且在字段中输入 **MAC** 地址来覆盖接口的使用默认 **MAC** 地址。
- 出于维护或其他原因，可以选中关闭端口以暂时使此接口脱机。如果已连接，链路将断开。默认情况下未选中该选项。

取消选择此选项以激活接口，并使链接恢复。默认情况下未选中该选项。

i 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：

关闭端口将断开在此接口上的连接。
要继续吗？

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：

您要以管理员身份关闭端口 X2 ？

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：

您要以管理员身份启用端口 X2 ？

如果单击确认，则禁用图标变为启用图标。

- 5 对于 AppFlow 功能，选中启用流量报告允许报告该接口产生的流量。默认情况下已选中该选项。
- 6 （可选）选中启用组播支持可允许在此接口上接收组播。默认情况下未选中该选项。
- 7 （可选）选中启用默认 802.1p CoS 可以标记经过此接口且拥有 802.1p 优先级的信息进行服务质量 (QoS) 管理。默认情况下未选中该选项。

i 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。如需使用此优先级信息，请连接到此接口的设备应支持优先级帧。QoS 管理受管理 | 策略 | 规则 > 访问规则上的访问规则控制。如需 QoS 和带宽管理的信息，请参阅 SonicOS 策略。

- 8 （可选）如需从路由通告中排除该接口，请选中从路由通告中排除（NSM、OSPF、BGP、RIP）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。

i 注：只有 TZ 系列和 SOHO W 设备有这个选项。

- 10 （可选）如果已启用 DNS 代理，将对 LAN、DMZ 或 WLAN 接口显示启用 DNS 代理选项。如需在接口上启用 DNS 代理，请选择该选项。默认情况下未选中该选项。
- 11 也可通过选择启用非对称路由支持，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选项。如需非对称路由的更多信息，请参阅第 531 页的集群配置中的非对称路由。
- 12 如果要配置 LAN 接口，请转至第 239 页的配置路由模式。
- 13 （可选）从冗余/聚合端口中选择链路聚合或端口冗余。如需更多信息，请参阅第 255 页的配置链路聚合和端口冗余。

i 注：此选项仅在 NSA 2600 及更高版本的设备中可用。

- 14 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（MTU - 最大传输单元），请在接口 MTU 字段中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，请参阅 SonicOS 策略中的解释。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。

15 (可选) 如需将大于接口 MTU 的非 VPN 出站数据包分片，请选择对大于此接口的 MTU 的非 VPN 出站数据包进行分片。默认情况下已选中该选项。选中后，下列选项将激活。

重要：可以在管理 | 连接性 | 高级设置中指定出站 VPN 流量的分片。如需更多信息，请参阅 SonicOS 连接。

16 (可选) 如需覆盖不分片数据包位，请选择忽略不分片 (DF) 位。默认情况下未选中该选项。

17 如果要配置此接口的带宽管理，请转至第 241 页的在接口上启用带宽管理。

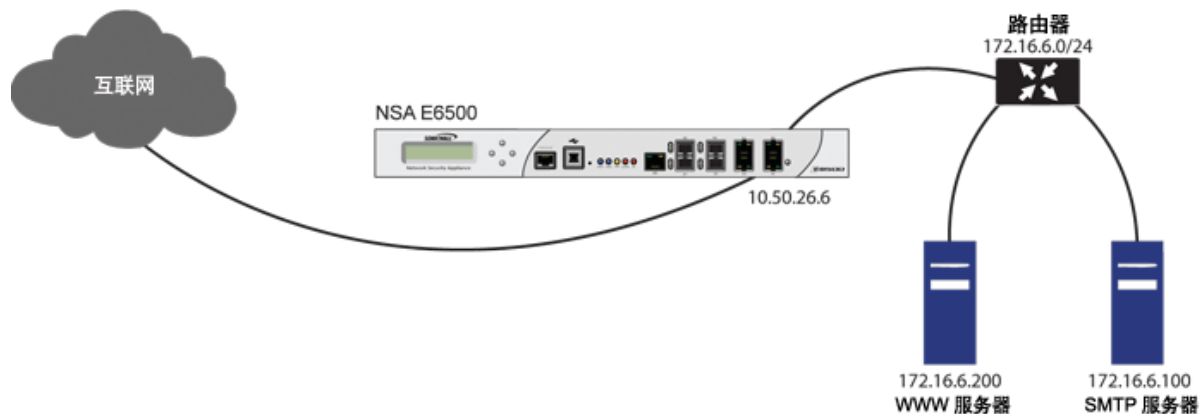
18 单击确定。

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。考虑路由模式配置中的拓扑，其中安全设备将路由由以下两个公用 IP 地址范围之间的流量：

- 10.50.26.0/24
- 172.16.6.0/24

路由模式配置



在 172.16.6.0 网络的接口上启用路由模式后，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。路由模式不适用于 WAN 模式。

配置路由模式的步骤如下：

- 1 转至管理 | 系统设置 | 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。

- 单击高级选项卡。

常规 高级

高级设置

链接速度: 自动协商

使用默认 MAC 地址: C0:EA:E4:59:8E:24

覆盖默认 MAC 地址:

关闭端口

启用流量报告

启用组播支持

启用 802.1p 标记

从路由通知中排除 (NSM, OSPF, BGP, RIP)

启用非对称路由支持

冗余/聚合端口: 无

专门的模式设置

使用路由模式 - 添加 NAT 策略以阻止出站\进站转换

NAT 策略出站/进站接口: Any

接口 MTU: 1500

- 如需为接口启用路由模式，请在专门的模式设置下，选择专门的模式设置标题，选择使用路由模式 - 添加 NAT 策略以阻止出站\进站转换。默认情况下未选中该选项。选择该选项后，下一个专门的模式设置将可用。
- 在 NAT 策略出站/进站接口下拉菜单中，选择将用于传送该接口的流量的 WAN 接口。默认设置为任何。
- 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（MTU - 最大传输单元），请在接口 MTU 字段中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，请参阅 SonicOS 策略中的解释。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。

- 如果在安全设备上启用了带宽管理，则将显示“带宽管理”部分。如需为此接口配置 BWM，请转至第 241 页的[在接口上启用带宽管理](#)。
 - 单击确定。
- 重要：**安全设备创建用于已配置的接口和所选 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。

在接口上启用带宽管理

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 [管理 | 安全配置 | 防火墙设置 > 带宽管理](#)；如需带宽管理 (BWM) 的信息，请参阅 [SonicOS 安全配置](#)。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。

可以启用各种类型的带宽管理：

- **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。
- **无 (默认)** - 禁用带宽管理。

如需配置带宽管理和各种 BWM 类型的效果的信息，请参阅 [SonicOS 安全配置](#)。

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 转至 [管理 | 系统设置 | 网络 | 接口](#)。
- 2 单击某个接口的编辑图标。将显示添加/编辑接口对话框。
- 3 如果这是未分配的接口，请根据第 [234](#) 页的 [配置接口](#) 中包含的部分配置此接口。
- 4 单击高级选项卡。
- 5 滚动至带宽管理。

带宽管理

启用接口出口带宽限制
最大接口出口带宽 (kbps):

启用接口入口带宽限制
最大接口入口带宽 (kbps):

注：BWM 类型：高级；要更改选项，请转至 [防火墙设置 > BWM](#) 页面

i | 注：高级设置可能会有所不同，具体取决于安全设备型号和所选区域类型。

- 6 可以对此接口启用带宽管理。如需带宽管理的更多信息，请参阅 [SonicOS 安全配置](#)。
 - a 如需限制流出流量到接口上的最大带宽，请选择 **启用接口出口带宽限制**。默认情况下未选中该选项。
 - 在最大接口出口带宽字段，指定最大带宽（单位为 kbps）。默认值为 **384.000000** kbps。

- b 如需限制流入流量到接口上的最大带宽，请选择启用接口入口带宽限制。默认情况下未选中该选项。
 - 在**最大接口入口带宽**字段，指定最大带宽（单位为 kbps）。默认值为 **384.000000** kbps。

如果以下两个选项之一为：

- 若选中，将定义已选的最大可用出口 BWM，但由于高级 BWM 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。
- 若未选中，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流量。

7 单击确定。

配置透明 IP 模式下的接口（连接 L3 子网）

通过透明 IP 模式，SonicWall 安全设备可以将 WAN 子网桥接到内部接口。

配置用于透明模式的接口的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
 - 2 对于您要配置的**未分配**接口，请单击**配置**图标。将显示**编辑接口**对话框。
 - 3 选择
 - **LAN 或 DMZ**（对于**区域**）。
 - ① **注：**可用的选项根据您选择的区域类型而改变。
 - 可以通过选择**创建新区域**来为该可配置接口创建新区域。随即显示**添加区域**对话框。如需添加区域的说明，请参阅第 329 页的**关于区域**。
 - 4 从**模式/IP 分配**中，选择**透明 IP 模式（连接 L3 子网）**。
 - 5 从**透明范围**中，选择一个地址对象，该对象包含您要通过此接口访问的 IP 地址的范围。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。
如果您尚未配置满足您需求的地址对象，请选择**创建新地址对象**。此时会显示**添加地址对象**对话框。如需创建地址对象的信息，请参阅 **SonicOS 策略**。
 - 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。默认情况下未选中该选项。
 - 7 如需启用通过此接口远程管理安全设备，请选择支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。
默认情况下未选中该选项。
如需允许访问 WAN 接口，以便从同一安全设备的其他区域进行管理，则必须创建访问规则。如需了解允许从 LAN 区域访问 WAN 主 IP 的方法，请参阅 **SonicOS 策略**。
 - 8 如需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**。
 - 9 如果为**管理**和/或**用户登录**协议选择了 **HTTPS**，则添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向将激活并处于选中状态。如需阻止从 **HTTP** 到 **HTTPS** 的重定向，请取消选择该选项。
① **注：**为用户登录协议选择 **HTTP** 将禁用重定向。
 - 10 单击确定。
- ① **注：**在更改安全设备的地址之后，需要提供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

配置透明 IP 模式接口的高级设置的步骤如下：

- 1 在编辑接口对话框中，单击高级。

高级设置

链接速度: 自动协商

使用默认 MAC 地址: C0:EA:E4:59:8E:29

覆盖默认 MAC 地址:

关闭端口

启用流量报告

启用组播支持

启用 802.1p 标记

从路由通知中排除 (NSM, OSPF, BGP, RIP)

启用 DNS 代理

启用非对称路由支持

冗余/聚合端口: 无

使无偿 ARP 能够转发到 WAN

使无偿 ARP 能够自动生成到 WAN

接口 MTU: 1500

- 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 - 全双工	
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安全设备的连接速度和双工模式。

- 3 默认选择使用默认 MAC 地址。您可以通过选择覆盖默认 MAC 地址且在字段中输入 MAC 地址来覆盖接口的使用默认 MAC 地址。
- 4 出于维护或其他原因，可以选中关闭端口以暂时使此接口脱机。如果已连接，链路将断开。默认情况下未选中该选项。

取消选择此选项以激活接口，并使链接恢复。默认情况下未选中该选项。

i | 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：

关闭端口将断开在此接口上的连接。
要继续吗？

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：

您要以管理员身份关闭端口 X2 ？

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：

您要以管理员身份启用端口 X2 ？

如果单击确认，则禁用图标变为启用图标。

- 5 对于 AppFlow 功能，选中启用流量报告允许报告该接口产生的流量。默认情况下已选中该选项。
- 6 （可选）选中启用组播支持可允许在此接口上接收组播。默认情况下未选中该选项。
- 7 （可选）选中启用默认 802.1p CoS 可以标记经过此接口且拥有 802.1p 优先级的信息进行服务质量 (QoS) 管理。默认情况下未选中该选项。

i | 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。如需使用此优先级信息，请连接到此接口的设备应支持优先级帧。QoS 管理受管理 | 策略 | 规则 > 访问规则上的访问规则控制。如需 QoS 和带宽管理的信息，请参阅 SonicOS 策略。

- 8 （可选）如需从路由通告中排除该接口，请选中从路由通告中排除 (NSM、OSPF、BGP、RIP) 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。

i | 注：只有 TZ 系列和 SOHO W 设备有这个选项。

- 10 （可选）如果已启用 DNS 代理，则将显示启用 DNS 代理选项。如需在接口上启用 DNS 代理，请选择该选项。默认情况下未选中该选项。
- 11 也可通过选择启用非对称路由支持，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选项。如需非对称路由的更多信息，请参阅第 531 页的集群配置中的非对称路由。
- 12 如果要配置 TZ 系列和 SOHO 系列安全设备，请转至步骤 14。
- 13 （可选）从冗余/聚合端口中选择链路聚合或端口冗余。如需更多信息，请参阅第 255 页的配置链路聚合和端口冗余。

i | 注：此选项仅在 NSA 2600 及更高版本的设备中可用。

- 14 选中启用免费 ARP 转发到 WAN 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 数据包转至 WAN。
- 15 选中启用自动免费 ARP 生成到 WAN 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。

16 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（MTU - 最大传输单元），请在接口 **MTU** 字段中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

i **注：**在端口可以处理巨型帧之前，必须启用巨型帧支持，请参阅 SonicOS 策略中的解释。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。

17 在已启用带宽管理的情况下，如需为此接口配置 **BWM**，请转至第 241 页的[在接口上启用带宽管理](#)。

18 单击确定。

配置无线接口

无线接口是分配给无线区域并用于支持 SonicWallSonicPoint 安全接入点的接口。

i **注：**只能使用安全类型无线（默认为 WLAN）来配置和管理 SonicPoint。

配置无线接口的步骤如下：

- 1 在编辑接口对话框中，单击高级。
- 2 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。
- 3 从区域中，选择 **WLAN** 或先前已定义的自定义无线区域。
- 4 对于模式/IP 分配，选择以下选项之一：
 - 静态 IP 模式（默认值）；转至
 - 二层桥接模式；如需更多信息，请参阅第 267 页的[二层桥接模式](#)。如果选择了此模式，将显示一条消息：

接口网桥未更改其区域。仅自动添加网桥对之间的允许规则。请手动添加其他必需的访问规则。
可能会删除主接口上的静态 DHCP 条目。

i **重要：**选择此模式需要为桥接对配置访问规则。如需配置访问规则的信息，请参阅 SonicOS 策略。

5 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。

i **注：**子网掩码的上限取决于您从 **SonicPoint/SonicWave 限制** 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。

6 从 **SonicPoint/SonicWave 限制** 中，选择此接口上允许的最大 SonicPoint 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。

允许的最大子网掩码大小

每个接口的 SonicWave/SonicPoint 数量	最大子网掩码	可用的 IP 地址总数	可用的客户端 IP 地址
无	30 位 - 255.255.255.252	2	2
2	29 位 - 255.255.255.248	6	3
4	29 位 - 255.255.255.248	6	1
8	28 位 - 255.255.255.240	14	5
16	27 位 - 255.255.255.224	30	13
24	26 位 - 255.255.255.192	62	29
32	26 位 - 255.255.255.192	62	29
48	25 位 - 255.255.255.128	126	77
64	25 位 - 255.255.255.128	126	61
96	24 位 - 255.255.255.0	190	93
128	23 位 - 255.255.254.0	254	125

i 注：允许的最大子网掩码大小表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。

- 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。
- 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**。
如需允许访问 WAN 接口，以便从同一安全设备的其他区域进行管理，则必须创建访问规则。如需了解允许从 LAN 区域访问 WAN 主 IP 的方法，请参阅 SonicOS 策略。
- 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**。
- 单击确定。

配置无线接口的高级设置

配置无线接口的高级设置的步骤如下：

- 在编辑接口对话框中，单击高级选项卡。
- 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**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 - 全工
100 Mbps - 全工	

对于 1 Gbps 接口

对于 10 Gbps 接口

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安全设备的连接速度和双工模式。

- 默认选择使用默认 **MAC** 地址。您可以通过选择覆盖默认 **MAC** 地址且在字段中输入 **MAC** 地址来覆盖接口的使用默认 **MAC** 地址。
- 出于维护或其他原因，可以选中关闭端口以暂时使此接口脱机。如果已连接，链路将断开。默认情况下未选中该选项。

取消选择此选项以激活接口，并使链接恢复。默认情况下未选中该选项。

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：

关闭端口将断开在此接口上的连接。
要继续吗？

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：

您要以管理员身份关闭端口 X2 ？

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：

您要以管理员身份启用端口 X2 ？

如果单击确认，则禁用图标变为启用图标。

- 对于 AppFlow 功能，选中启用流量报告允许报告该接口产生的流量。默认情况下已选中该选项。
- （可选）选中启用组播支持可允许在此接口上接收组播。默认情况下未选中该选项。
- （可选）选中启用默认 **802.1p CoS** 可以标记经过此接口且拥有 **802.1p** 优先级的信息进行服务质量 (QoS) 管理。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。如需使用此优先级信息，请连接到此接口的设备应支持优先级帧。QoS 管理受管理 | 策略 | 规则 > 访问规则上的访问规则控制。如需 QoS 和带宽管理的信息，请参阅 SonicOS 策略。

- （可选）如需从路由通告中排除该接口，请选中从路由通告中排除（NSM、OSPF、BGP、RIP）默认情况下未选中该选项。
- 如果要配置 SuperMassive 或 NSA 系列设备，请转至步骤 11。
- 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 系列安全设备有这个选项。

- （可选）如果已启用 DNS 代理，则将显示启用 DNS 代理选项。如需在接口上启用 DNS 代理，请选择该选项。默认情况下未选中该选项。

12 也可通过选择**启用非对称路由支持**，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选项。如需非对称路由的更多信息，请参阅第 531 页的**集群配置中的非对称路由**。

13 如果要配置 TZ 系列和 SOHO 系列安全设备，请转至**步骤 14**。

14 (可选) 从**冗余/聚合端口**中选择**链路聚合或端口冗余**。如需更多信息，请参阅第 255 页的**配置链路聚合和端口冗余**。

i | **注：**此选项仅在 NSA 2600 及更高版本的设备中可用。

15 选中**启用免费 ARP 转发到 WAN** 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 数据包转至 WAN。

16 选中**启用自动免费 ARP 生成到 WAN** 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。

17 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 (MTU - 最大传输单元)，请在**接口 MTU** 字段中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

i | **注：**在端口可以处理巨型帧之前，必须启用巨型帧支持，请参阅 SonicOS 策略中的解释。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。

18 如果要为此接口配置路由模式，请转至第 239 页的**配置路由模式**。

19 在已启用带宽管理的情况下，如需为此接口配置 BWM，请转至第 241 页的**在接口上启用带宽管理**。

20 单击**确定**。

配置 WAN 接口

i | **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 SonicWall 安全设备上最多配置 $N - 2$ 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。

如需配置 WAN 接口：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 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。
- 3 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**。
- 4 从**IP 分配**中，选择以下 WAN 网络寻址模式之一。

i | **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 地址的网络配置安全设备。

- **DHCP** - 配置安全设备向因特网上的 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安全设备插入网络。如需更多信息，请参阅第 264 页的**配置有线和 Tap 模式**。
- **分接模式 (1 端口分接)** - 允许将安全设备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，请参阅第 264 页的**配置有线和 Tap 模式**。

5 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。

6 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**管理 | 系统设置 | 设备 > 基本设置**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。

7 如果想要启用通过此接口远程管理安全设备，请选择支持的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

如需允许访问 WAN 接口，以便从同一安全设备的其他区域进行管理，则必须创建访问规则。如需创建访问规则的信息，请参阅 SonicOS 策略。

8 如果使用 **PPPoE**、**PPTP** 或 **L2TP**，将显示附加字段：

- 对于 **PPPoE**，请选择以下项之一：
 - 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。
 - 选择**未编号的接口**，并执行以下操作之一：
 - 选择一个未编号的接口
 - 通过选择**创建新的未编号接口**来创建新的未编号接口。

① | 注：接口必须未分配。

- 对于 **PPTP** 或 **L2TP**，配置以下选项：
 - 选择**不活动断开连接**并输入连接终止之前的非活动分钟数。取消选择此选项以禁用不活动超时。
 - 从 **IP 分配**中，选择：
 - **DHCP**；“IP 地址”、“子网掩码”和“网关地址”字段将由服务器自动提供。
 - **静态**，请输入这些字段的相应值。

9 如果使用 DHCP，可以选择：

- 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。配置之后，以下按钮可用；选择：

- 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。

10 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。

11 选中添加规则，以启用从 HTTP 到 HTTPS 的重定向，前提是要将 HTTP 连接自动重定向到与安全设备的安全 HTTP 连接。有关此选项的更多信息，请参阅第 230 页的 HTTP/HTTPS 重定向。

12 继续在高级和协议选项卡（如显示）中配置，如第 250 页的配置 WAN 接口的高级设置所述。

13 如需继续进行高级设置，请转至第 250 页的配置 WAN 接口的高级设置。

14 如果为 IP 分配选择了 PPPoE、PPTP 或 L2TP，请转至第 251 页的配置 WAN 接口的协议设置。

15 单击确定。

配置 WAN 接口的高级设置

配置 WAN 接口的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。

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 - 全双工
 - 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。

i **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以允许使用为此接口生成的流量的相关流量报告。

- 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 管理受 [管理 | 安全配置 | 防火墙规则 > 服务质量映射](#) 上的服务规则控制。如需 QoS 和带宽管理的信息，请参阅 [SonicOS 安全配置](#)。
- 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](#)。如需更多信息，请参阅第 255 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：必须先启用巨型帧支持，然后才能处理巨型帧。如需巨型帧的更多信息，请参阅 [SonicOS 安全配置](#)。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 VPN 出站数据包的分片在 [管理 | 连接 | VPN](#) 中设置；如需 VPN 流量的更多信息，请参阅 [SonicOS 连接性](#)。
 - 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：
 - 如果服务器可能更改，请选中使用 **DHCP** 时启动带发现功能的续租。
 - 选中在租约购买期间使用 秒的 **DHCP** 发现间隔，并在 DHCP 服务器未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，请参阅第 241 页的 [在接口上启用带宽管理](#)。

配置 WAN 接口的协议设置

如果在配置 WAN 接口时为 IP 分配指定了 **PPPoE**、**PPTP** 或 **L2TP**，则编辑接口对话框将显示协议选项卡。

常规
高级
协议

通过 PPPoE 获取的设置

SonicWall IP 地址：	0.0.0.0
子网掩码：	0.0.0.0
网关地址：	0.0.0.0
DNS 服务器 1：	0.0.0.0
DNS 服务器 2：	0.0.0.0

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**）。在您将安全设备连接到 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。



The screenshot shows the 'Protocol' configuration tab for an interface. It is divided into two main sections:

- 通过 PPPoE 获取的设置 (Settings obtained through PPPoE):** This section contains several input fields, all currently set to 0.0.0.0:
 - SonicWall IP 地址 (SonicWall IP address)
 - 子网掩码 (Subnet mask)
 - 网关地址 (Gateway address)
 - DNS 服务器 1 (DNS server 1)
 - DNS 服务器 2 (DNS server 2)
 - 服务器 MRU (Server MRU) set to 0.
- PPPoE 客户端设置 (PPPoE Client Settings):** This section contains three checkboxes:
 - 不活动时断开连接 (分钟数) : 10 (Disconnect on inactivity (minutes): 10)
 - 为保持服务器活动, 严格使用 LCP 回应数据包 (Strictly use LCP response packets to keep server active)
 - 断开 PPPOE 客户端如果服务器不能发送流量为 5 分钟 (Disconnect client if server cannot send traffic for 5 minutes)

- 2 在 PPPoE 客户端设置部分中，启用下列选项：

- **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。默认情况下未选中该选项。
- **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。默认情况下未选中该选项。
- **断开 PPPOE 客户端如果服务器不能发送流量为 _ 分钟：** 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，然后重新连接默认情况下已选中该选项。

配置隧道接口

您可以在 SonicOS 中配置多种类型的隧道接口。在**网络 | 接口**上配置有编号隧道接口、WLAN 隧道接口和 IPv6 6to4 隧道接口。丢弃隧道接口是从**网络 | 路由**配置的，而未编号的隧道接口配置为来自**管理 | 连接 | VPN**的 VPN 策略的一部分；如需 VPN 策略的信息，请参阅 SonicOS 连接。

有编号和未编号的隧道接口与 VPN 一起使用。有编号的隧道接口分配有自己的 IP 地址，但未编号的隧道接口从现有物理或虚拟 (VLAN) 接口借用 IP 地址。

有编号和未编号隧道接口类型都支持使用 RIP 和 OSPF 的静态路由和动态路由，而有编号隧道接口也可以与 BGP 配合使用。

如需配置各种类型的隧道接口，请参阅以下各节：

- 有编号隧道接口；请参阅第 253 页的[配置 VPN 隧道接口](#)
- 未编号隧道接口；请参阅 [SonicOS 连接](#)。
- 丢弃隧道接口；请参阅第 384 页的[丢弃隧道接口](#)
- IPv6 6to4 隧道接口；请参阅第 777 页的[配置 6 至 4 自动隧道](#)

配置 VPN 隧道接口

您可以通过从“添加”接口下拉列表中选择 VPN 隧道接口创建有编号隧道接口。将 VPN 隧道接口添加到“接口设置”表中，然后可以与动态路由（包括 RIP，OSPF 和 BGP）一起使用，或静态路由策略可以在配置中使用 VPN 隧道接口作为接口基于静态路由的 VPN。

VPN 隧道接口可以像标准接口一样配置，除了组播，流报告，非对称路由，分段数据包处理和不分片 (DF) 设置之外，还包括启用设备管理或用户使用 HTTP，HTTPS，Ping 或 SSH。

① 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。

[VPN 隧道接口部署](#)表列出 VPN 隧道接口的部署方式

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
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
BGP	DHCP 服务器接口

对于所有平台，最多支持的 VPN 隧道接口数（有编号隧道接口）为 64。未编号隧道接口的最大数目因平台而异，并直接对应于每个平台上支持的最大 VPN 策略数。

配置 VPN 隧道接口的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 接口。
- 2 从接口设置表下的添加接口中，选择 **VPN** 隧道接口。此时会显示添加隧道接口对话框。

常规 高级

接口设置

区域: VPN

VPN 策略: --请选择 VPN 策略--

名称:

模式 / IP 分配: 静态 IP 模式

IP 地址: 0.0.0.0

子网掩码: 255.255.255.0

接口 MTU: 已通过 VPN 策略自动配置

备注:

管理: HTTPS Ping SNMP SSH

用户登录: HTTP HTTPS

此区域定义为 VPN 且无法进行更改。

- 3 从 **VPN 策略** 中，选择一项 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。
- 5 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。
- 6 在子网掩码字段，输入子网掩码。默认值为 **255.255.255.0**。
- 7 可以选择在备注字段中添加备注。
- 8 也可指定该接口允许的管理协议：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。
- 9 也可指定该接口允许的用户登录协议：**HTTP** 和/或 **HTTPS**。

10 单击高级。

常规 高级

高级设置

启用流量报告

启用组播支持

启用非对称路由支持

专门的模式设置

使用路由模式 - 添加 NAT 策略以阻止出站/入站转换

NAT 策略出站/入站接口: Any

启用分段数据包控制

忽略不分片 (DF) 位

- 11 如需为此隧道接口创建的流量启用流量报告，请选择**启用流量报告**。默认情况下已选中该选项。
- 12 （可选）可以通过选择**启用组播支持**在接口上启用组播接收。默认情况下未选中该选项。
- 13 也可通过选择**启用非对称路由支持**在隧道接口上启用非对称路由支持。默认情况下未选中该选项。如需非对称路由的更多信息，请参阅第 531 页的**集群配置中的非对称路由**。
- 14 如需使用“路由模式”和添加 NAT 策略以阻止出站/入站转换，请选择**用户路由模式 - 添加 NAT 策略以阻止出站/入站转换**。选中后，以下选项将激活。默认情况下未选中该选项。
- 15 在选择了“路由模式”的情况下，如需为 NAT 策略指定接口，请从 **NAT 策略出站/入站接口** 中选择一个接口。可用接口取决于您的安全设备。默认设置为任何。
- 16 如需在此接口上启用分片数据包处理，请选择**启用分段数据包控制**。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。
- 17 选择**忽略不分片 (DF) 位**以忽略数据包标头中的 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。启用此选项后，它会导致安全设备忽略 DF 位并始终对数据包进行分片。
- 18 单击**确定**。将有编号 VPN 隧道接口添加到**接口设置表**。

配置链路聚合和端口冗余

① | 注：NSA 2600 及更高版本安全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 管理界面**编辑接口**对话框的高级选项卡中配置。

- 第 256 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。可以实现在两个以太网域之间发送几千兆位流量的能力。

i **注：**NSA 2600 及更高版本的安全设备支持链路聚合。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，第 496 页的[交换 | 链路聚合](#)中介绍了相关内容。
二层桥接模式不支持链路聚合。

- 第 258 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。

i **注：**NSA 2600 及更高版本的安全设备支持端口冗余。HA 控制接口不支持链路聚合和端口冗余。

主题：

- 第 256 页的[链路聚合](#)
- 第 257 页的[链路聚合配置](#)
- 第 258 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。安全设备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 256 页的[链路聚合故障切换](#)
- 第 257 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。如果在安全设备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 中的每个链路都承载相同份额的负载，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无效时起作用。

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 或更高版本的安全设备进行手动配置/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 转至管理 | 系统设置 | 网络 | 接口。
- 2 单击要指定为链路聚合群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。
- 3 单击高级。

常规 高级

高级设置

链接速度: 自动协商

使用默认 MAC 地址: C0:EA:E4:59:8E:24

覆盖默认 MAC 地址:

关闭端口

启用流量报告

启用组播支持

启用 802.1p 标记

从路由通知中排除 (NSM, OSPF, BGP, RIP)

启用非对称路由支持

冗余/聚合端口: 无

专门的模式设置

使用路由模式 - 添加 NAT 策略以阻止出站/进站转换

NAT 策略出站/进站接口: Any

接口 MTU: 1500

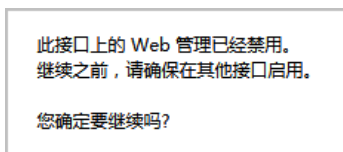
- 4 从冗余/聚合端口中，选择链路聚合。将显示更多选项。



- 5 冗余 / 聚合端口选项与安全设备上当前未分配的每个接口一起显示。未选择任何端口。选择其他最多三个接口以分配至该 LAG。

i **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。

- 6 将接口的链接速度设为自动协商。
- 7 单击**确定**。如果未对接口配置 Web 管理，则会显示一条消息。



- a 单击**确定**。
- b 在另一个接口上启用 Web 管理。

i **重要：**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因供应商而异。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。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。如果在安全设备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。如果主要端口和次要冗余端口都发生了故障，则将发生 HA 故障切换（假定次要安全设备已激活相应的端口）。

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：

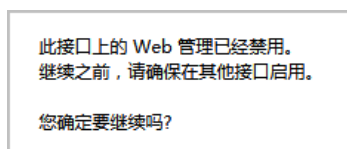
- 1 转至管理 | 系统设置 | 网络 | 接口。
- 2 单击要指定为链路聚合群组主接口的接口所对应的配置图标。将显示编辑接口对话框。
- 3 单击高级。
- 4 将接口的链接速度设为自动协商。
- 5 从冗余/聚合端口中，选择端口冗余。此时会显示另一个选项。



The screenshot shows a configuration dialog box with the following elements:

- Two checkboxes: 从路由通知中排除 (NSM, OSPF, BGP, RIP) and 启用非对称路由支持.
- A label "冗余/聚合端口:" followed by a dropdown menu showing "端口冗余".
- A label "冗余端口:" followed by a dropdown menu showing "无".

- 6 冗余端口选项会显示所有当前未分配的可用接口。选择接口之一；默认值为无。
i 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，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。
- 7 单击确定。如果未对接口配置 Web 管理，则会显示一条消息。



- a 单击确定。
- b 在另一个接口上启用 Web 管理。

配置虚拟接口（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。

添加虚拟接口的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 接口。
- 2 在接口设置表的底部，从添加接口中选择虚拟接口。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 在 **VLAN 标签** 字段中将 VLAN 标签 (ID) 分配给子接口。有效的 VLAN ID 介于 0（默认值）至 4094，但一些交换机会保留 VLAN 1 用于指定本机 VLAN，并将保留 VLAN 0 用于 QoS。您需要使用相应的 VLAN ID 为希望通过防火墙保护的每个 VLAN 创建一个 VLAN 子接口。
 - 5 从父接口中选择此子接口所属的父（物理）接口。您可以分配的子接口数量无每接口限制 - 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。请参阅接口配置说明：
 - 第 234 页的[配置静态接口](#)
 - 第 236 页的[配置静态接口的高级设置](#)
 - 第 242 页的[配置透明 IP 模式下的接口（连接 L3 子网）](#)
 - 第 245 页的[配置无线接口](#)
 - 第 248 页的[配置 WAN 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

如需针对 IPS 探查器模式配置安全设备，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，X2 和 X3 用于桥接对，并在 LAN 区域中进行配置。WAN 接口 (X1) 由安全设备用于根据需要访问安全设备数据中心。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 262 页的[配置 IPS 探查器模式](#)

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

配置主桥接接口的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击接口 X2 右边列中的**配置**图标。将显示**编辑接口**对话框。
- 3 从**区域**下拉菜单中选择 **LAN**。此时显示更多选项。
i | 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**，请选择**静态 IP 模式**。
- 5 为接口配置静态 IP 地址（例如 10.1.1.3）。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。
i | 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：**HTTPS、Ping、SNMP、SSH**。
- 9 选择用户登录选项：**HTTP、HTTPS**。
- 10 如需启用从 HTTP 到 HTTPS 的重定向，请选择添加规则，以启用从 **HTTP 到 HTTPS** 的重定向。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。
- 11 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。

配置次要桥接接口的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击接口 X2 右边列中的**配置**图标。将显示**编辑接口**对话框。
- 3 从**区域**下拉菜单中选择 **LAN**。此时显示更多选项。
i | 注：您不必配置“高级”或“VLAN 过滤”选项卡中的设置。
- 4 从 **IP 分配**中，选择**二层桥接模式**。
- 5 从**桥接到**中，选择 **X2** 接口。
- 6 如果想要监控非 IPv4 流量，请勿启用**阻止所有非 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 为接口选择**管理**选项：**HTTPS**、**Ping**、**SNMP**、**SSH**。
- 11 选择用户登录选项：**HTTP**、**HTTPS**。
- 12 如需启用从 HTTP 到 HTTPS 的重定向，请选择添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。
- 13 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。

如需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。

如需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**管理 | 系统设置 | 设备 | SNMP**。
- 2 选择**启用 SNMP**。
- 3 单击**接受**。配置按钮将激活，并将显示视图、用户/群组 and 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，输入将接收发自安全设备的陷阱的 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 IPS 探查器模式

配置 IPS 探查器模式的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 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 选择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。该对话框将关闭，并重新显示**网络 | 接口**页面。
 - 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，也是安全设备用来发送其 **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安全设备上的 **X0**，而非 **X2**（实际上，完全不会插入 **X2**）
 - 并将 **X1** 连接到内部网络
- i** | **重要：**小心地设定 SPAN/镜像至 **X0** 的端口。
- i** | **视频：**可以在线访问包含接口配置示例的参考视频。例如，可参阅 [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://www.sonicwall.com/zh-cn/support/videos-product-select>。

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。

如需启用安全服务，您的 **SonicWall** 安全设备必须已获得这些服务的授权且必须从 **SonicWall** 数据中心下载特征码。如需启用和配置 **IPS**、**GAV** 及防间谍软件的完整说明，请参阅 **SonicOS** 安全配置。

主题：

- 第 **263** 页的[配置日志](#)
- 第 **263** 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](#)

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。如需了解启用日志的方法，请参阅 **SonicOS** 日志和报告。

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可以对其进行检查的安全设备。

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

将安全设备上的 WAN 端口（通常为端口 X1）连接到您的网关或具有网关访问权的设备。安全设备将自动与 SonicWall 数据中心进行通信。如需配置 WAN 接口的详细说明，请参阅第 248 页的[配置 WAN 接口](#)。

配置有线和 Tap 模式

SonicOS 支持有线模式和分接模式，这两种模式提供了实现无干扰的网络增量插入的方法。[有线和 Tap 模式设置](#)表说明有线和 Tap 模式。

i | 注：NSA 2600 及更新设备支持有线模式。

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安全设备硬件引入网络中。在选择网络插入点（例如核心交换机与外围安全设备之间、虚拟机服务器场前面、数据分类域之间的转换点）后，将把安全设备插入物理数据路径，且只需极短的维护时间窗。安全设备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安全设备的 240 Gbps 交换机结构上，而非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，在网络中引入安全设备，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。您即可通过简单的用户界面驱动力的重新配置，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，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。数据包继续通过安全设备的交换机结构，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。无需任何实际的中间处理，这揭示了安全设备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，它将安全设备的多核处理器主动介入到数据包处理路径中。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，但却无任何 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，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，它通过安全设备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。

有线模式：功能区别表总结了几种接口配置模式之间的主要功能差异：

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 ^a	否	否	否	否	是
应用程序控制	否	否	是	否	是

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
应用程序可见性	否	是	是	是	是
ARP/路由/NAT ^a	否	否	否	否	是
综合反垃圾邮件服务 ^a	否	否	否	否	是
内容过滤	否	否	是	否	是
DHCP 服务器 ^a	否	否	否	否	是 ^b
DPI 检测	否	是	是	是	是
DPI 保护	否	否	是	否	是
DPI-SSL ^a	否	否	是	否	是
高可用性	是	是	是	是	是
链路状态传播 ^c	是	是	是	否	否
状态数据包检测	否	是	是	是	是
强制 TCP 握手 ^d	否	否	否	否	是
虚拟组 ^a	否	否	否	否	是
VLAN 转换 ^e	否	否	是	否	否

a. 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。

b. 在 L2 桥接模式下不可用。

c. 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。通过 VLAN 接口的有线模式不支持链路状态传播。

d. 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安全设备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。

e. 通过 VLAN 接口的有线模式不支持 VLAN 转换。

注：在有线模式下运行时，防火墙的专用“管理”接口将用于本地管理。如需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**。

配置用于有线模式的接口的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击您要为有线模式配置的接口对应的**配置**图标。将显示**编辑接口**对话框。
- 3 从**区域**中，选择除 **WLAN** 之外的任何区域类型。
- 4 从**模式/IP 分配**中，如需配置用于以下项的接口：
 - 分接模式，请选择**分接模式（1-端口分接）**
 - 有线模式，请选择**有线模式（2-端口有线）**。
- 5 从**有线模式类型**中，选择适当的模式：
 - 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**）
- 6 从**配对接口**中，选择将连接到上游安全设备的接口。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：**配对接口中仅提供未分配的接口。如需让接口处于未分配状态，请单击其**配置**，然后从**区域**中选择**未分配**。
- 7 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**管理 | 系统设置 | 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 从**IP 分配**中，选择**有线模式（2-端口有线）**。
- 4 从**区域**中，选择 **WAN**。
- 5 从**配对接口区**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。接口设置表更新：

带有链路聚合的有线模式

i | 注：通过 VLAN 接口的有线模式不支持链路聚合。

链路聚合 (LAG) 用于将多个链路捆绑为单个接口以增加带宽。如需检测 LAG 接口上的流量，可以内联方式连接 SonicWall 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。支持链接状态传播等现有的有线模式功能。每个 LAG 支持多达 8 个成员。

有线模式和链路聚合都从网络 | 接口中配置。在编辑接口 > 高级对话框中选择链路聚合后，还将列出未分配的接口。您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 转至管理 | 系统设置 | 网络 | 接口。
- 2 单击想要配置的接口的配置图标。
- 3 从区域中，选择您需要的区域。
- 4 从模式/IP 分配中，选择有线模式（2-端口有线）。
- 5 从有线模式类型中，选择安全（内联流量的主动 DPI）。
- 6 从配对接口中，选择需要的接口。
- 7 从配对接口区域中，选择需要的接口。
- 8 选择禁用状态检测选项。默认情况下已选中该选项。
- 9 如果需要，也可以选择启用链接状态传播选项。默认情况下未选中该选项。
- 10 单击高级。

继续进行高级设置的步骤如下：

- 1 从冗余/聚合端口中，选择链路聚合。这些选项将发生更改。
- 2 从聚合端口中，选择需要的端口。
- 3 从配对接口聚合端口中，选择需要的端口。
- 4 单击确定。该配置显示在网络 | 接口上的接口设置表中。

二层桥接模式

SonicOS 包括 L2（2 层）桥接模式，以不显眼的方式将安全设备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，因为它使安全设备能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，使其能传递和检查很多其他透明安全设备集成方法无法处理的流量类型。利用二层桥接模式，可以无干扰地将 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。在此方案中，安全设备未用于增强安全性，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、组播、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。SonicWall 安全设备支持的 IPS 探查器模式使用桥接对的单个接口来监控来自交换机上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，因为安全设备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，请参阅第 228 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：已具备现有安全设备，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）。如果您未订阅 SonicWall 安全服务，可以从 MySonicWall 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 [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 268 页的 [SonicOS 二层桥接模式的主要功能](#)
- 第 269 页的 [配置二层桥接模式和透明模式的重要概念](#)
- 第 270 页的 [二层桥接模式与透明模式的比较](#)
- 第 275 页的 [二层桥接路径确定](#)
- 第 276 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

[SonicOS 二层桥接模式密钥功能和优点](#) 表总结了二层桥接模式各项主要功能的优点。

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 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。很多其他透明操作方法仅支持 IPv4 流量，二层桥接模式将检查所有 IPv4 流量，并传递（或在需要时阻止）所有其他流量，包括 LLC、所有以太网类型，甚至包括专用帧格式。

SonicOS 二层桥接模式密钥功能和优点

功能	优点
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 SonicWall 安全设备安全设备作为单纯的二层桥接，并提供到完整安全服务操作的平滑迁移路径。
无线二层桥接 注：不适用于 SuperMassive 9800。	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。通过此功能，无线和有线客户端可以无缝共享相同的网络资源，包括 DHCP 地址。二层协议可以在配对的接口之间运行，从而允许多种流量类型流经网桥，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 L2 桥接模式的操作和配置时，将使用以下术语：

- **二层桥接模式** - 一种配置 SonicWall 安全设备的方法。利用此方法，设备能以内联方式插入现有网络，并拥有绝对的透明性（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 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。
- **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具有完全二层透明性的两端口学习桥接相似，并将对所有经过桥接对的 IP 流量进行完全状态故障切换和深层数据包检查。
- **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止所有非 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。换言之，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，则该地址将用于安全设备的出站通信，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), 安全设备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 至非桥接接口。激活捕获桥接模式可确保进入二层桥接的流量退出二层桥接, 而不是采用在逻辑上最优的路径。一般而言, 仅在存在冗余路径并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** - 指的是将安全设备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。这意味着, 会对桥接对一端绑定所有进入另一端的流量, 而且这些流量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并非一种功能限制, 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** - 指桥接对并非通过安全设备的唯一入口/出口点的部署。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。这在安全设备同时用于为一个或多个桥接对提供安全性时较为常见; 还提供下列服务:
 - 为桥接对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进行。

二层桥接模式与透明模式的比较

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 安全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:

- 极少或无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)

主题:

- 第 271 页的[透明模式中的 ARP](#)
- 第 271 页的[透明模式中的 VLAN 支持](#)
- 第 271 页的[透明模式中的多个子网](#)
- 第 271 页的[透明模式中的非 IPv4 流量](#)
- 第 271 页的[二层桥接模式中的 ARP](#)
- 第 272 页的[二层桥接模式中的 VLAN 支持](#)
- 第 272 页的[二层桥接 IP 数据包路径](#)
- 第 273 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 274 页的[二层桥接模式与透明模式的比较](#)
- 第 275 页的[透明模式相对二层桥接模式有的优点](#)

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，要使这些主机能通过安全设备进行通信，必须先清除这条缓存的 ARP 条目。这是因为，安全设备为连接到以透明模式工作的接口的代理（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 请求将由安全设备使用自己的 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，安全设备还代理了在透明范围（192.168.0.100 至 192.168.0.250）内为以透明模式工作的接口指定和分配的 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，要使路由器能通过安全设备与该主机进行通信，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，该路由器可能会为 192.168.0.100 发送新的 ARP 请求，安全设备将使用其 X1 MAC 00:06:B1:10:10:11 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 安全设备能将 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。尽管透明模式能通过使用静态 ARP 和路由条目来支持多个子网。

透明模式中的非 IPv4 流量

透明模式会丢弃（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，以下各节将对此进行说明：

- 第 271 页的 [二层桥接模式中的 ARP](#)
- 第 272 页的 [二层桥接模式中的 VLAN 支持](#)
- 第 272 页的 [二层桥接 IP 数据包路径](#)
- 第 273 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 274 页的 [二层桥接模式与透明模式的比较](#)
- 第 275 页的 [透明模式相对二层桥接模式有的优点](#)

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端方的实际主机 MAC 地址。例如，与路由器 (192.168.0.1) 通讯的工作站会将路由器视为 00:99:10:10:10:10，而该路由器会将工作站 (192.168.0.100) 视为 00:AA:BB:CC:DD:EE。

这种行为允许将以二层桥接模式工作的 SonicWall 安全设备引入现有网络中，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。

注：在插入二层桥接模式安全设备时，需要重新建立基于流的 TCP 协议通信（例如客户端与服务端之间的 FTP 会话）。这是设计决定的，目的是维护状态数据包检查所提供的安全性。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数据包，并记录在不存在/已关闭的连接上收到 TCP 数据包；TCP 数据包已丢弃等日志事件。

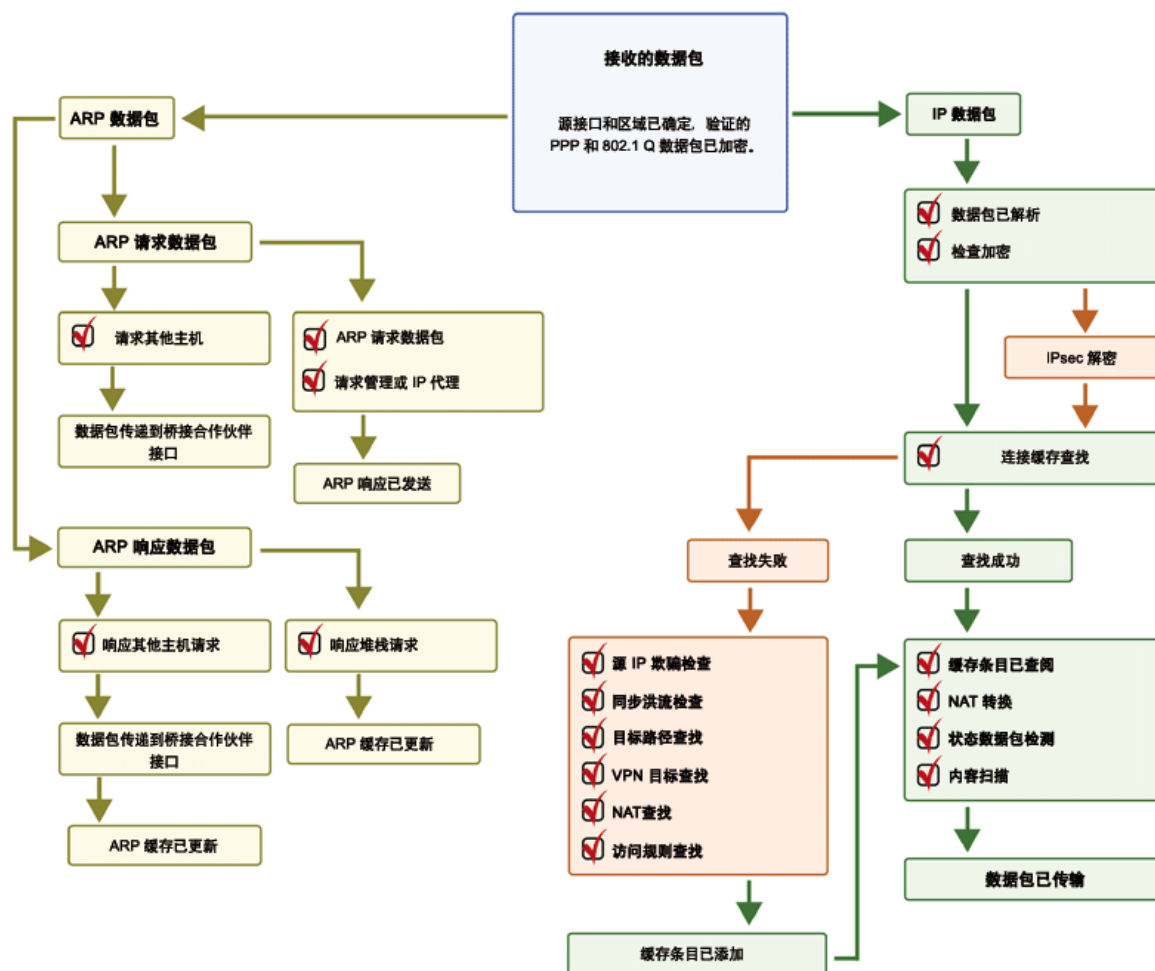
二层桥接模式中的 VLAN 支持

在 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安全设备插入（例如以内联方式）到承载任何数量的 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 流量应用访问规则。

二层桥接 IP 数据包路径

二层桥接 IP 数据包流



以下事件序列说明了 **二层桥接 IP 数据包流** 中的流：

- 1 采用 802.1Q 封装的帧进入二层桥接接口（第一步、**步骤 2** 和 **步骤 12** 仅适用于 802.1Q VLAN 流量）。
- 2 根据 VLAN ID 白/黑名单检查 802.1Q VLAN ID。如果 VLAN ID：
 - 不允许使用，则将丢弃并记录该数据包。
 - 允许使用，则将解除数据包封装，存储 VLAN ID，并使内层数据包（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。可以使用访问规则将二层桥接配置为仅支持一个或多个特定子网。
- 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)、组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。
 - 通常，进入二层桥接的数据包的目的地是桥接合作伙伴接口（即，桥接的另一端）。在这种情况下，无需执行转换。
 - 在 L2 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（如需更多详细信息，请参阅第 275 页的 **二层桥接路径确定**）。
- 7 对数据包应用访问规则。例如，在 SonicWall 安全设备上，以下数据包解码显示：ICMP 数据包承载 VLAN ID 10，源 IP 地址 110.110.110.110，目标 IP 地址 4.2.2.1。

```
▣ Frame 219 (102 bytes on wire, 102 bytes captured)
▣ Ethernet II, Src: 08:00:46:a2:eb:4d (08:00:46:a2:eb:4d), Dst: 99:88:77:66:55:44 (99:88:77:66:55:44)
▣ 802.1Q Virtual LAN
  000. .... .. = Priority: 0
  ...0 .... .. = CFI: 0
  ... 0000 0000 1010 = ID: 10
  Type: IP (0x0800)
▣ Internet Protocol, Src: 110.110.110.110 (110.110.110.110), Dst: 4.2.2.1 (4.2.2.1)
▣ Internet Control Message Protocol
```

可以设置一条访问规则，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，使其继续通过。

- 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，使其继续通过。
- 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，使其继续通过。客户端通知将按配置执行。
- 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并非 VPN/WAN/已连接的接口，则将恢复已存储的 VLAN 标签，而且数据包（再次携带原始的 VLAN 标签）将发送到桥接合作伙伴接口。

二层桥接模式中的多个子网

如第 272 页的 **二层桥接 IP 数据包路径** 中所示，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。这使安全设备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 数据包仅通过网桥传递，数据包处理程序不会检查或控制这些数据。如果不需要这些流量类型，可通过在次要桥接接口配置对话框中启用阻止所有非 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

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 安全设备的 MAC 地址为目的地的数据包，传递其他数据包，并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（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，但安全设备将终止而非传递 VLAN。

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
VLAN 子接口	可以在桥接接口上配置 VLAN 子接口，但这些接口通过桥接传递至桥接合作伙伴接口，除非 VLAN 帧中的目标 IP 地址与安全设备上的 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）。	可以为 VLAN 子接口分配以透明模式工作的物理接口，但其工作模式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，将终止而非传递 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。详细信息请参阅第 289 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 服务或使用 IP 助手传递 DHCP。
路由和 NAT	可智能地将来自/发往其他路径的流量传入/传出 L2 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。可以根据需要添加自定义路由和 NAT 策略。	可智能地传递来自/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。可以根据需要添加自定义路由和 NAT 策略。
状态数据包检测	完全状态数据包检测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/发往由透明模式地址对象分配定义的子网的流量。
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。
组播流量	只要已在 管理 安全配置 防火墙设置 > 组播 中激活组播，就会通过二层桥接对检查和传递组播流量。它不依赖于 IGMP 消息传送，也没必要在单独的接口上启用组播支持。	只要已在 管理 安全配置 防火墙设置 > 组播 中激活组播，并在相关接口上启用了组播支持，透明模式就会检查和传递拥有 IGMP 依赖性的组播流量。

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

安全设备在桥接接口上收到的数据包必须转发到通往其目的地的适当、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 如果未找到 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 如果数据包从其他路径到达，安全设备会在桥接对的两个接口分别发送一条 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。这使安全设备在完成路径确定之前无法应用相应的访问规则。完成时，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)，如果确定为对以下项进行绑定：

- 1 桥接合作伙伴接口，不执行 IP 转换 (NAT)。
- 2 不同的路径，适用适当的 NAT 策略；如果路径为：
 - a 另一个已连接的（本地）接口，可能未转换。也就是说，由于触发了最终的任意 -> 原始 NAT 策略，因此将对其进行有效路由。
 - b 已确定将通过 WAN，将应用默认的用于 X1 WAN 的自动添加的 [接口] 出站 NAT 策略，而且将转换数据包的源以发送至互联网。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）。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项入站服务，用于检查入站 HTTP、FTP、IMAP、SMTP、POP3 是否会交付（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）进行检索，因此将使用传出分类器（如 IPS: 流量方向中所述）。参考 IPS: 流量方向，它将为传出连接，并需要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。IPS: 流量方向中说明了传入和传出，而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。在安全设备收到数据包时，通常可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流入或流出（不要与入站和出站相混淆），IPS: 流量方向表中显示的条件用于确定方向。

IPS: 流量方向^a

目的地/源	不受信任	公用	无线	加密	受信任	组播
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

a. 表格数据可能发生更改。

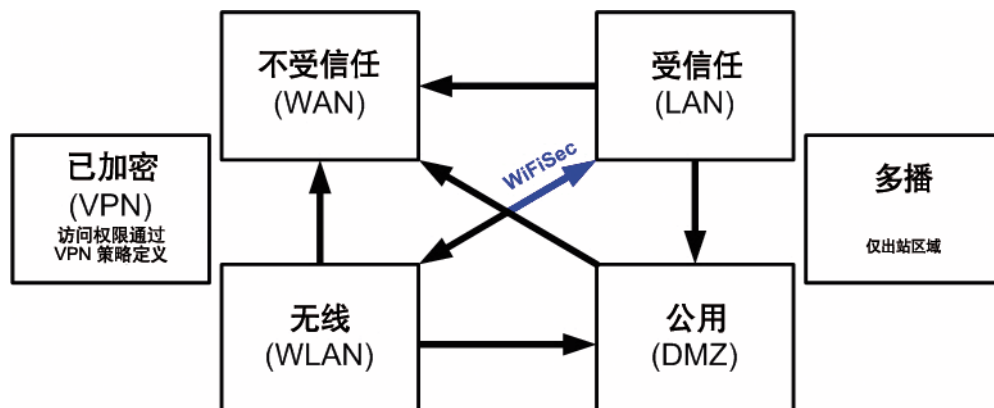
除了上述分类以外，对于流入/流出拥有附加信任级别的区域（这些区域内在拥有增强级别的安全性 [LAN|无线|加密<-->LAN|无线|加密]）的数据包，还提供了专门的信任分类。有信任分类的流量已应用所有特征（传入、传出和双向）。

- 3 特征方向。这主要与 IPS 相关。在 IPS 中，每个特征都由 SonicWall 特征开发团队分配了一个方向。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。如需触发某个特征，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。[访问规则默认值](#)中显示了默认值：

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无任何影响。

① | 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.mysonicwall.com/>)。

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表示增加 SonicWall 安全设备以便在已部署现有安全设备的网络中提供安全服务。
- 外围安全表示在靠近网络外围的位置部署安全设备的现有网络中增加处于单纯的二层桥接模式的 SonicWall 安全设备。
- 内部安全表示处于混合模式的 SonicWall 安全设备的完全集成，在此设备中它提供同时二层桥接、WLAN 服务和经过 NAT 的 WAN 访问。
- 具有高可用性的二层桥接模式表示防火墙安全设备 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 L2 桥接模式联合部署 SonicWall SMA SSL VPN 或 SonicWall SSL VPN 系列设备的场景。

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 280 页的 [外围安全](#)
- 第 280 页的 [内部安全](#)

- 第 280 页的[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

i | 注：无线二层桥接不适用于 SuperMassive 9800。

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端方相同的子网和 DHCP 池。

配置 WLAN 到 LAN 二层接口桥接的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击想要桥接的无线接口的**配置**图标。将显示**编辑接口**对话框。
 - i** | 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**二层桥接模式**中，选择**模式/IP 分配**。
 - i** | 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**中选择应将 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，请参阅第 245 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：存在现有的安全设备并将继续使用，但希望在不对网络做重大更改的前提下使用安全设备的防火墙服务。通过将安全设备置于二层桥接模式，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。

此示例指的是安装在 Hewlett Packard ProCurve 交换环境中的 SonicWall 安全设备。

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 SonicWall 安全设备的一些方面。

配置内联式二层桥接模式的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击 **X0 LAN** 接口的**配置**图标。
- 3 在**编辑接口**对话框中，将 IP 分配设置为**二层桥接模式 (IP 路由选项)**。这些选项将发生更改。
- 4 将**桥接到**：接口设置为 **X0**。
- 5 如需阻止桥接对上的所有非 IP 流量，请选择**阻止所有非 IP 流量**。默认情况下未选中该选项。
- 6 如需阻止在桥接对上路由流量，请选择**不在此桥对上路由流量**。默认情况下未选中该选项。
- 7 如需仅侦听桥接对上的流量，请选择**仅捕获该桥接对上的流量**。默认情况下未选中该选项。
- 8 如需阻止桥接对上的状态检查，请选择**禁用该桥接对上的状态检测**。默认情况下未选中该选项。
- 9 确保针对 **HTTPS** 和 **SNMP** 配置接口，以便能由 **PCM+/NIM** 从 DMZ 管理该接口。
- 10 按正常方法配置其余选项。

11 单击**确定**以保存和激活该更改。

您还必须确保修改访问规则，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。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

外围安全是将安全设备添加到外围以提供安全服务（不确定网络是否在安全设备与路由器之间具有现有安全设备）的网络方案。在此方案中，安全设备下的所有部分（主桥接接口分段）通常视为具有比安全设备左侧所有部分（次要桥接接口网段）更低的信任级别。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

在此网络方案中，安全设备将用作外围安全设备且保护无线平台的安全。与此同时，它还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安全设备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给受信任的 (LAN) 区域，因此以下规则适用：

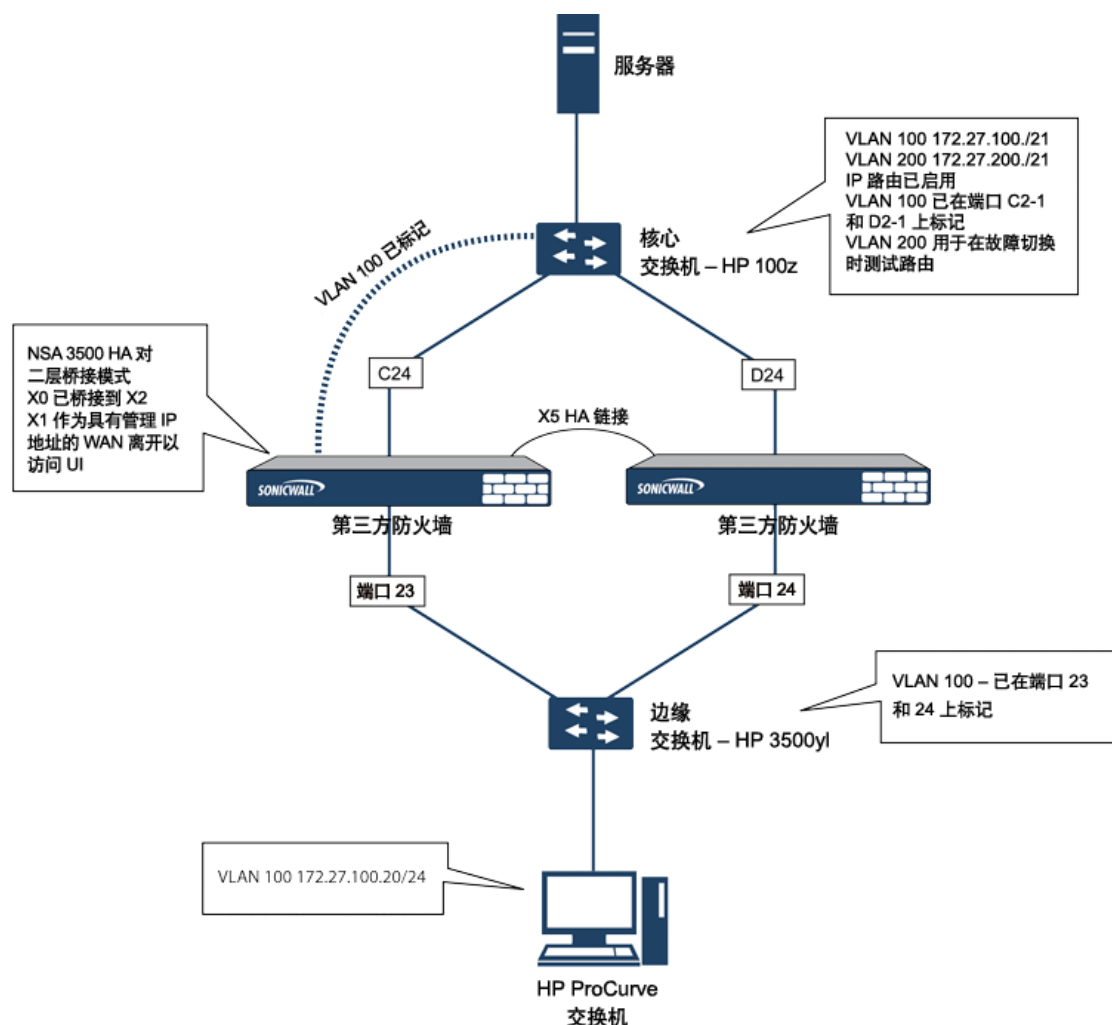
- 默认情况下将允许所有流量，但也可以根据需要构建访问规则。
从对比的角度出发，考虑如果将 X2（主桥接接口）分配到公用 (DMZ) 区域，将会发生怎样的情况：将允许所有工作站访问服务器，但服务器无法向工作站发起通信。尽管这样做可能会支持流量流动要求（即，工作站向服务器发起会话），但它会造成两种不利影响：
- DHCP 服务器将位于 DMZ 中。来自工作站的 DHCP 请求将通过二层桥接到达 DHCP 服务器 (192.168.0.100)，但由于默认的 DMZ->LAN 拒绝访问规则，将丢弃来自服务器的 DHCP 供应。因此必须添加一条访问规则或修改默认访问规则，以允许从 DMZ 到 LAN 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。可能这并非最优选择，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双向安全性。

如需配置二层桥接模式下的接口的详细说明，请参阅第 283 页的[配置二层桥接模式](#)。

有高可用性的二层桥接模式

此方法适用于同时需要高可用性 (HA) 和二层桥接模式的网络。此示例针对 SonicWall 安全设备，并假定使用已配置 VLAN 的交换机。请参阅[内部安全示例：同时需要高可用性和二层桥接模式](#)。

内部安全示例：同时需要高可用性和二层桥接模式



安全设备 HA 对包含指定的 HA 端口 X5 上连接在一起的两个安全设备。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，安全设备和交换机上都需要注意若干事宜。

在安全设备上：

- 在配置高可用性时，请勿启用虚拟 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 建议将分配给交换机的管理 VLAN 网络用于安全和管理用途。

注：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**内部安全示例：同时需要高可用性和二层桥接模式**中所示，在边缘交换机（端口 23 和 24）和核心交换机（C24 - D24）上为 VLAN 100 创建了两个标签（802.1q）端口。将以内联方式在这两个交换机之间连接安全设备。在高性能环境中，通常建议（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，还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

此示例拓扑介绍将 SonicWall 安全设备正确安装到您现有的 SonicWall EX 系列 SSL VPN 或 SonicWall SSL VPN 网络环境中的方法。将安全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。在此方案中，安全设备未用于增强安全性，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。本节将介绍 SonicWall 安全设备的单端口和双端口部署。

WAN 到 LAN 访问规则

由于在此部署场景中，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。如需允许流量在 WAN 和 LAN 之间双向传递的信息，请参阅 SonicOS 策略。

配置网络接口和激活 L2B 模式

在此方案中，WAN 接口将用于：

- 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）

安全设备上的 LAN 接口用于监控来自 SSL VPN 设备的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（而非重新配置 SSL VPN 设备的外部接口，从而将 LAN 接口视为默认路由）。

在 **网络 | 接口** 上，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，以便安全设备获取特征更新以及与 NTP 进行通讯。

网关和内部/外部 DNS 地址设置必须与您的 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，请选择 **HTTPS** 和 **Ping**。单击 **确定** 以保存并激活更改。

配置 LAN 接口设置的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | 接口**。
- 2 单击 **LAN** 接口的 **配置** 图标。
- 3 对于 IP 分配设置，选择 **二层桥接模式**。
- 4 对于 **桥接到** 设置，选择 **X1**。
- 5 如果还需要传递安全设备支持的带 VLAN 标记的流量，请单击 **VLAN 过滤**。
- 6 添加所有需要传递的 VLAN。
- 7 单击 **确定** 以保存和激活该更改。

您可以自动断开与安全设备管理接口的连接。现在，您可以断开管理笔记本电脑或台式机与安全设备的 X0 接口的连接，并关闭安全设备，然后再将其物理连接到您的网络。

在网络与 SSL VPN 设备之间安装安全设备

不论采用哪种部署方法（单宿主或多宿主），都应该将安全设备置于 SSL VPN 设备的 X0/LAN 接口与内部网络连接之间。设备即可向外连接 SonicWall 的授权和特征更新服务器，并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 将安全设备上的 X0/LAN 端口连接到 SSL VPN 设备上的 X0/LAN 端口。
- 2 将安全设备上的 X1/WAN 端口连接到先前连接 SSL VPN 的端口。
- 3 打开安全设备。

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 将安全设备上的 X0/LAN 端口连接到 SSL VPN 设备的 X0/LAN 端口。
- 2 将安全设备上的 X1/WAN 端口连接到先前连接 SSL VPN 的端口。
- 3 打开安全设备。

配置或验证设置

在网络中的管理工作站上，现在应该能通过安全设备的 WAN IP 地址访问其管理界面。

配置或验证设置的步骤如下：

- 1 确保 SonicWall 安全设备的所有安全服务已启用。参阅第 285 页的[授权服务](#)和第 286 页的[在每个区域激活安全服务](#)。
- 2 在该设备与 SonicWall SMA SSL VPN 设备进行联合部署之前，必须禁用 SonicWall 内容过滤服务。
 - a 转至管理 | 系统设置 | 网络 > 区域页面。
 - b 单击 LAN (X0) 区域旁边的配置。
 - c 取消选择强制内容过滤服务。
 - d 单击确定。
- 3 如果您尚未更改 SonicWall 安全设备上的管理密码，则可以在管理 | 系统设置 | 设备 > 基本设置上执行该操作。
- 4 如需从外部客户端测试网络访问，请连接到 SSL VPN 设备并登录。
- 5 连接后，尝试访问内部网络资源。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 284 页的[用于二层桥接模式的配置任务列表](#)
- 第 286 页的[二层桥接模式配置过程](#)

- [第 288 页的 VLAN 与二层桥接模式的集成](#)
- [第 289 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
 - 创建访问规则
 - 配置日志设置
 - 配置无线区域设置
- [第 287 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 287 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

需要在您的 SonicWall 安全设备上配置下列设置，然后才能在大多数二层桥接模式拓扑中使用它：

- [第 285 页的授权服务](#)
- [第 285 页的禁用 DHCP 服务器](#)
- [第 285 页的配置 SNMP 设置](#)
- [第 285 页的在接口上启用 SNMP 和 HTTPS](#)
- [第 285 页的启用 Syslog](#)
- [第 286 页的在每个区域激活安全服务](#)
- [第 286 页的创建访问规则](#)
- [第 286 页的配置日志设置](#)
- [第 286 页的配置无线区域设置](#)

授权服务

当安全设备成功注册时：

- 1 转至**管理 | 更新 | 许可证**。
- 2 单击**管理安全在线服务下的同步**。

这将联系安全设备许可服务器，并确保安全设备获得正确的许可。

如需检查授权状态，请转至**监控 | 当前状态 | 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

在另一台设备用作 DHCP 服务器的网络配置中以二层桥接模式使用 SonicWall 安全设备时，必须先禁用安全设备的内部 DHCP 引擎（默认情况下，已配置并运行此引擎）。

禁用 DHCP 服务器的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | DHCP 服务器**。
- 2 取消选择启用 DHCP 服务器。
- 3 单击**接受**。

配置 SNMP 设置

配置 SNMP 设置的步骤如下：

- 1 转至**管理 | 系统设置 | 设备 | SNMP**。
- 2 选择启用 SNMP。
- 3 单击**接受**。配置按钮将激活，并填写了 SNMP 信息。
- 4 单击**配置**。随即显示配置 SNMP 对话框。如需了解配置 SNMP 的方法，请参阅第 42 页的[设置 SNMP 访问权限](#)。

在接口上启用 SNMP 和 HTTPS

在接口上启用 SNMP 和 HTTPS 的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击管理设备时所用接口的**编辑**图标。将显示**编辑接口**对话框。
- 3 对于**管理选项**，启用 **HTTPS** 和 **SNMP**。
- 4 单击**确定**。

启用 Syslog

可以在**日志 > Syslog**页面上启用 Syslog。如需了解启用 Syslog 的方法，请参阅 SonicOS 日志和报告。

在每个区域激活安全服务

在**管理 | 系统设置 | 网络 | 区域**上，确保为您将使用的每个区域激活安全服务。

然后，对于**管理 | 安全配置 | 安全服务**上的每项服务，激活并配置最适合您的环境的设置。如需激活和配置安全服务的信息，请参阅 [SonicOS 安全配置](#)。

创建访问规则

如果您计划从其他区域管理安全设备或将第三方服务器用于管理、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**管理 | 策略 | 规则 > 访问规则**上，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。如需访问规则的信息，请参阅 [SonicOS 策略](#)。

配置日志设置

在**管理 | 日志和报告 | 日志设置 | 名称解析**上，将名称解析方法设置为先 **DNS** 后 **NetBios**。如需配置日志设置的信息，请参阅 [SonicOS 日志和报告](#)。

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。

配置无线区域设置的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 区域**。
- 2 选择无线区域。
- 3 在无线上，取消选择仅允许由 **SonicPoint** 和 **WiFiSec** 增强生成的流量选项。
- 4 单击确定。

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，请参阅第 [276](#) 页的**二层桥接接口区域选择**。此示例使用一种很类似于简单二层桥接拓扑的拓扑。

选择一个接口作为主桥接接口。如需进行此项选择的信息，请参阅第 [276](#) 页的**二层桥接接口区域选择**。此示例使用 X1（自动分配给主要 WAN）：

主题：

- 第 [287](#) 页的**配置主桥接接口**
- 第 [287](#) 页的**配置次要桥接接口**
- 第 [288](#) 页的**配置用于硬件故障的 L2 旁路**

配置主桥接口

配置主桥接接口的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 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）。
i | **注：**主桥接口必须拥有静态 IP 分配。
- 4 仅限 WAN 接口：
 - a 配置默认网关。这是安全设备自身访问互联网所必需的。
 - b 配置 DNS 服务器。
- 5 为接口选择一个或多个**管理选项**：**HTTPS**、**Ping**（默认情况下处于选中状态）、**SNMP**、**SSH**。
i | **注：**选择 **HTTPS** 将自动激活并选择添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向。
- 6 选择用户登录选项：**HTTP**、**HTTPS**。
- 7 如需启用从 **HTTP** 到 **HTTPS** 的重定向，请选择添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。
- 8 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，请参阅第 276 页的**二层桥接接口区域选择**。

配置次要桥接接口

此示例使用 **X0**（自动分配给 LAN）：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击 **X0**（局域网）接口右边列中的**配置**图标。
- 3 从 **IP 分配**中，选择**二层桥接模式**。
- 4 从**桥接到**中，选择 **X1** 接口。
- 5 为接口选择一个或多个**管理选项**：**HTTPS**、**Ping**（默认情况下处于选中状态）、**SNMP**、**SSH**。
i | **注：**选择 **HTTPS** 将自动激活并选择添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向。
- 6 选择用户登录选项：**HTTP**、**HTTPS**。
- 7 如需启用从 **HTTP** 到 **HTTPS** 的重定向，请选择添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。
- 8 您可以选择启用**阻止所有的非 IPv4 流量**，以防止二层桥接传递非 IPv4 流量。
- 9 如需通过 L2 网桥控制 VLAN 流量，请单击 **VLAN 过滤**。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。将阻止添加到右侧窗格的所有 VLAN，而允许保留在左侧窗格的所有 VLAN 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。将允许添加到右侧窗格的所有 VLAN 通过，而阻止保留在左侧窗格的所有 VLAN。

10 单击**确定**。接口设置表显示已更新的配置：

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安全设备的物理绕过。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**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**选项自动设置如下：

- **阻止所有的非 IPv4 流量** - 已禁用。如启用，该选项将阻止所有非 IPv4 以太网帧。所以，该选项禁用。
- **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，该选项启用。
- **仅捕获该桥接对上的流量** - 已禁用。启用时，不转发在桥接对接口上收到的流量。所以，该选项禁用。
- **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 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 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。
- 3 选择**当出错时出口物理绕过**。
 **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**选项才可用。
- 4 单击**确定**。

VLAN 与二层桥接模式的集成

SonicWall 安全设备支持 VLAN。在有 VLAN 标签的数据包到达物理接口时，将对 VLAN ID 进行评估，以确定其是否受支持。将去除 VLAN 标签，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 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（而非简单的数据包过滤）。

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 流量正确地穿过安全设备。

配置 VPN 与二层桥接模式的集成的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 单击**添加图标**。随即显示**添加路由策略**对话框。
- 3 按照以下所示内容配置路由：
 - 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

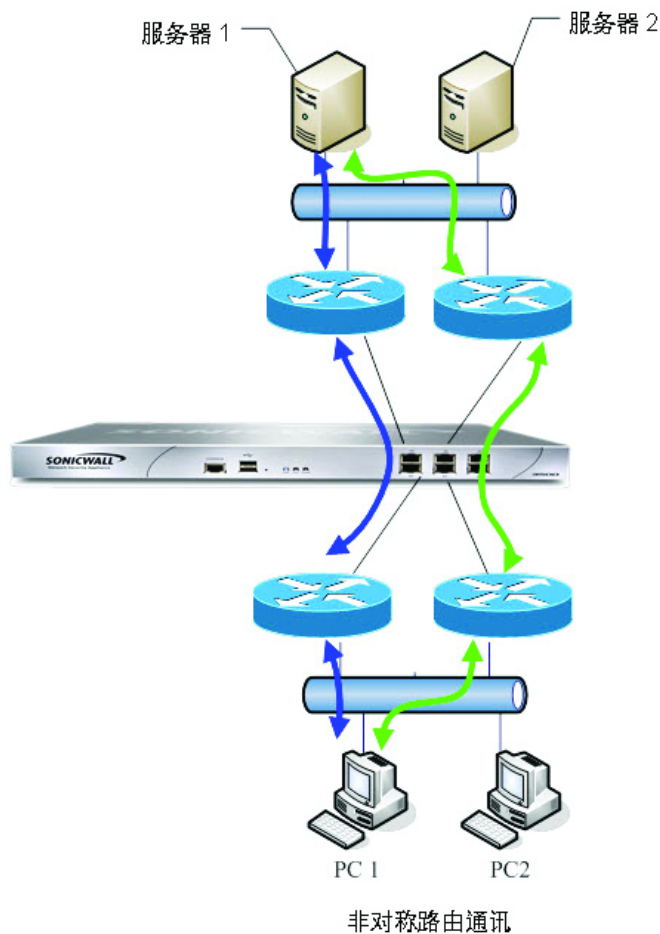
4 单击确定。

非对称路由

SonicOS 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。当流量流过安全设备中的不同二层桥接接口或它流过高可用性集群中的不同安全设备时，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安全设备都必须“看到”与数据包流关联的所有数据包。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安全设备集群带来问题，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同时丢弃，因为任一节点都未“看到”流中的所有流量。请参阅[非对称路由](#)。

非对称路由



在**非对称路由**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。经过安全设备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（即便在流经不同接口时也是如此）并提供有状态深层数据包检查。

❶ | 注：非对称路由不同于无回复的单向连接，即 TCP 状态绕过。

配置 IPv6 接口

如需配置 IPv6 接口的完整描述，请参阅第 768 页的 [IPv6 接口配置](#)。

31 位网络

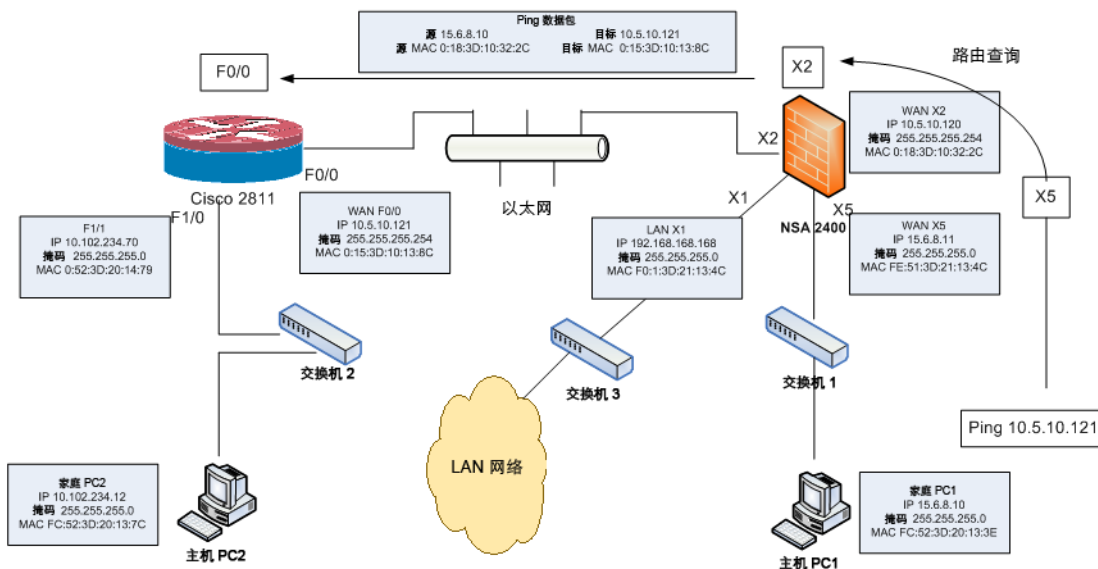
SonicOS 6.2.7 引入了对 [RFC 3021](#) 的支持，它定义了 31 位子网掩码的使用方法。该掩码在子网中仅允许两个主机地址，无任何“网络”、“网关”或广播地址。这样的配置可以用在更大的网络中，以使用点到点链路将两个主机连接起来。由于在大型网络中每个点到点链路都将使用两个地址而非四个地址，用户可以很容易看到由于这种变化而节省出来的地址空间。

在这种情况下，点到点链路不同于 PPP（点对点协议）。使用 31 位掩码的点到点链路可以使用或不使用 PPP 协议。点到点链路上的 31 位前缀 IPv4 地址也可以用在以太网网络中。

主题：

- 第 291 页的[网络环境示例](#)
- 第 292 页的[配置 SonicOS](#)

网络环境示例



在此网络环境中，“主机 PC1”和“主机 PC2”可以互相访问，同时 LAN 网络中的主机可以访问“主机 PC2”。

如需配置此环境的设置，请执行以下步骤：

1 对于“主机 PC1”，添加以下两个路由条目：

- `Route add 10.5.10.0 mask 255.255.255.0 15.6.8.10`
- `Route add 10.102.234.0 mask 255.255.255.0 15.6.8.10`

2 对于“主机 PC2”，添加以下两个路由条目：

- `Route add 10.5.10.0 mask 255.255.255.0 10.102.234.70`
- `Route add 15.6.8.0 mask 255.255.255.0 10.102.234.70`

3 在 Cisco 路由器 (F0/0) 上：

- `interface fastEthernet 0/0`
- `ip address 10.5.10.120 255.255.255.254`

4 在 Cisco 2811 上，添加以下路由条目：

```
!  
ip route 15.6.8.0 255.255.255.0 10.5.10.120  
!
```

5 在防火墙上，添加以下路由条目，使 WAN 区域的数据流量在 X2 和 X5 之间传输：

```
Any 10.102.234.0 Any X2 Default Gateway X2
```

配置 SonicOS

如需配置 31 位子网的接口，请执行以下步骤：

- 1 转至 **管理 | 系统设置 | 网络 | 接口**。
- 2 编辑所需接口。
- 3 将子网掩码设置为 255.255.255.254。
- 4 在 **IP 地址** 字段中输入一个主机 IP 地址。
- 5 在 **默认网关** 字段中输入其他的主机 IP 地址。
- 6 根据需要，根据网络情况设置其他字段。
- 7 单击 **确定**。

PPPoE 未编号接口支持

“PPPoE 未编号”接口允许仅使用一个 PPPoE 连接来管理一系列 IP 地址。互联网服务提供商 (ISP) 提供可以在子网内分配的多个静态 IP 地址。第一个地址指定为网络地址，最后一个地址指定为广播地址。

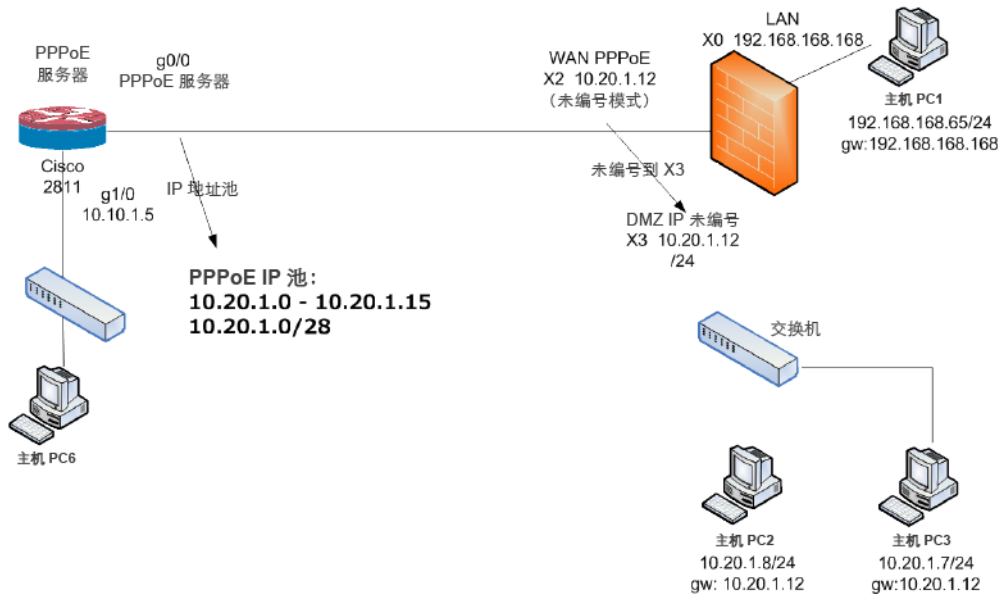
PPPoE 的默认 MTU 为 **1492**。

主题：

- 第 293 页的 [示例网络拓扑](#)
- 第 293 页的 [注意](#)

- 第 293 页的 [配置 PPPoE 未编号接口](#)
- 第 294 页的 [配置 PPPoE 未编号的高可用性](#)

示例网络拓扑



在这种拓扑结构中，X2 是 PPPoE 未编号的接口，而 X3 是未编号的接口。

SonicOS 会向网络 | 路由 > 路由策略表中添加两项策略。

SonicOS 还添加了两种 NAT 策略：

注意

如需在配置 X2 未编号到 X3 时将 X3 更改为另一个模式，则首先通过将 X2 更改为另一个模式来终止与 X2 的关系。否则，如果更改接口 X3 的 IP 地址或掩码，则会导致 X3 重新连接到 PPPoE 服务器。

如果 X3 设置为未编号的接口，则其他接口无法使用二层桥接连接到 X3。

配置 PPPoE 未编号接口

配置 PPPoE 未编号接口的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 接口。
- 2 通过单击编辑图标在 WAN 接口上配置 PPPoE 客户端设置：将显示编辑接口对话框。
- 3 选择未编号的接口。该下拉菜单随即激活。
- 4 选择创建新的未编号接口。将显示添加未编号的接口对话框。
- 5 对于区域，选择 LAN、DMZ 或创建一个新区域。
 - ① 注：模式/IP 分配设置为 IP 未编号且显示为灰色。
- 6 对于 IP 地址，输入 ISP 提供的地址。该地址通常是提供商分配的第二个 IP 地址。

- 7 在子网掩码字段中输入由 ISP 分配的子网掩码。
- 8 完成配置此接口。
- 9 单击**确定**。
- 10 完成配置第一个接口。
- 11 单击**确定**。

配置 PPPoE 未编号的高可用性

如需了解配置 PPPoE 未编号的高可用性的方法，请参阅第 535 页的[配置 Active/Standby 高可用性设置](#)。

PortShield 配置接口

注：NSA 2600 安全设备不支持 PortShield，而 SOHO W 安全设备不支持 X-系列解决方案。

- 第 295 页的[网络 | PortShield 群组](#)
 - 第 295 页的[关于 PortShield](#)
 - 第 296 页的[X-系列交换机的 SonicOS 支持](#)
 - 第 305 页的[管理端口](#)
 - 第 313 页的[配置 PortShield 群组+](#)

网络 | PortShield 群组

主题：

- 第 295 页的[关于 PortShield](#)
- 第 296 页的[X-系列交换机的 SonicOS 支持](#)
- 第 305 页的[管理端口](#)
- 第 313 页的[配置 PortShield 群组](#)

关于 PortShield

PortShield 接口是一个分配有一组端口（包括 Dell X-Series 或扩展交换机上的端口）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，每个上下文都有它自己的线速 PortShield，享受专用的深层数据包检查安全设备的保护。

提示：即使不使用 PortShield 分组，也始终可以在[管理 | 系统设置 | 网络 | 接口](#)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给 PortShield 接口。未分配给 PortShield 接口的所有端口将分配给 LAN 接口。

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

以静态模式工作

以静态模式创建 PortShield 接口时，您可以手动创建要应用于 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 接口未在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，您会创建一系列要应用于 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 接口都必须位于唯一的子网中。不能在多个子网中重叠 PortShield 接口。

X-系列交换机的 SonicOS 支持

主题：

- [第 296 页的关于 X-系列解决方案](#)
- [第 304 页的支持的拓扑](#)

关于 X-系列解决方案

- 注：**NSA 2600 或 SOHO W 安全设备不支持 X-系列解决方案。

关键网络元素，如安全设备和交换机，通常需要分别进行管理。SonicOS 允许使用安全设备管理界面和 GMS 统一管理安全设备和 Dell X-系列交换机。

SonicWall 安全设备上可用的最大接口数因型号而异，如[每个安全设备的接口](#)表中所示。

每个安全设备的接口

防火墙型号	可用接口数
SM 9600	20 个接口（4 个 10 GbE SFP+ 接口，8 个 1 GbE SFP 接口，8 个 1GE 铜线接口），1 个 GbE 管理接口和 1 个控制台接口
SM 9400	20 个接口（4 个 10 GbE SFP+ 接口，8 个 1 GbE SFP 接口，8 个 1GE 铜线接口），1 个 GbE 管理接口和 1 个控制台接口
SM 9200	20 个接口（4 个 10 GbE SFP+ 接口，8 个 1 GbE SFP 接口，8 个 1GE 铜线接口），1 个 GbE 管理接口和 1 个控制台接口
NSA 6600	20 个接口（4 个 10 GbE SFP+ 接口，8 个 1 GbE SFP 接口，8 个 1GE 铜线接口），1 个 GbE 管理接口和 1 个控制台接口

每个安全设备的接口

防火墙型号	可用接口数
NSA 5600	18 个接口（2 个 10 GbE SFP+ 接口，4 个 1 GbE SFP 接口，12 个 1GE 铜线接口）和 1 个管理接口
NSA 4600	18 个接口（2 个 10 GbE SFP+ 接口，4 个 1 GbE SFP 接口，12 个 1GE 铜线接口）和 1 个管理接口
NSA 3600	18 个接口（2 个 10 GbE SFP+ 接口，4 个 1 GbE SFP 接口，12 个 1GE 铜线接口）和 1 个管理接口
NSA 2650	
TZ600	10 GbE
TZ500 系列	8 GbE
TZ400 系列	7 GbE
TZ300 系列	5 GbE

在某些部署中，所需的端口数可能会超出安全设备提供的最大可用接口数。通过使用 X-系列解决方案，就可以将 Dell X-系列交换机上的端口看作安全设备的扩展接口，从而使可用的接口数增加到最多 192 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和/或进行高可用性 (HA) 配置，并可以将其视为安全设备上的任何其他接口。

注： X-系列交换机、X-交换机、外部交换机和扩展交换机可互换使用。

SonicWall 安全设备支持的 X-系列交换机表中显示的 SonicWall 安全设备最多支持所列出的 X-系列交换机中的四个。

注： 如需 X-系列交换机及配置它们的方法的完整信息，请参阅 [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](#)。

SonicWall 安全设备支持的 X-系列交换机

这些 SonicWall 安全设备

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2650
- TZ600
- TZ500/TZ500W
- TZ400/TZ400W
- TZ300/TZ300W

SonicWall 安全设备支持的 X-系列交换机

这些 SonicWall 安全设备

支持以下 X-系列交换机（端口）

- X1008 (8 10/100/1000Base-T GbE)
- X1008P (8 个 10/100/1000Base-T GbE 端口, 2 个 1GbE SFP 光纤端口, 8 个 PoE 端口, 最高共计 123W)
- X1018 (16 个 10/100/1000Base-T GbE 端口, 2 个 1GbE SFP 光纤端口)
- X1018P (16 个 10/100/1000Base-T GbE 端口, 2 个 1GbE SFP 光纤端口, 16 个 PoE 端口, 最高共计 246W)
- X1026 (24 个 10/100/1000Base-T GbE 端口, 2 个 1GbE SFP 光纤端口)
- X1026P (24 个 10/100/1000Base-T GbE 端口, 2 个 1GbE SFP 光纤端口, 24 个 PoE 端口/12 个 PoE+ 端口, 最高共计 369W)
- X1052 (48 个 10/100/1000Base-T GbE 端口, 2 个 10GbE SFP/SFP+ 光纤端口)
- X1052P (48 个 10/100/1000Base-T GbE 端口, 24 个 PoE 端口/12 个 PoE+ 端口, 最高共计 369W)
- X4012 (12 个 10GbE SFP/SFP+ 光纤端口)

i | 注: NSA 2600 或 SOHO W 安全设备不支持 X-系列解决方案。

主题:

- 第 298 页的术语
- 第 299 页的性能要求
- 第 299 页的 X-系列交换机支持的主要功能
- 第 300 页的 PortShield 功能和 X-系列交换机
- 第 301 页的 Dell X 系列菊花式链接支持
- 第 302 页的 PoE/PoE+ 和 SFP/SFP+ 支持
- 第 302 页的 X-系列解决方案和 SonicPoint
- 第 303 页的使用 GMS 管理扩展交换机
- 第 303 页的扩展交换机全局参数
- 第 303 页的关于链路
- 第 304 页的记录和系统记录支持

术语

HA 高可用性

扩展交换机 与 X-系列交换机相同。

外部交换机 与 X-系列交换机相同。

IDV 通过 VLAN 消除接口歧义 - 将扩展交换机上已对安全设备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。
SPM	单点管理
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

SonicWall 安全设备现在可以：

- 最多设置四台 X-系列交换机。
- 管理更多的端口。

X-系列交换机支持的主要功能

注：如需这些功能的信息，请参阅 [SonicWall X-系列解决方案部署指南](#)。

- 提供 X-系列交换机作为扩展交换机
- PortShield 功能
- 配置扩展交换机的接口设置
- 管理基本扩展交换机全局参数
- 使用 GMS 管理扩展交换机
- 利用 PortShield 功能实现高可用性 (HA)

使用“共同上行链路”时，可以在 HA 模式下支持 PortShield 功能。在此配置中，Active/Standby 安全设备和 X-系列交换机之间的链路用作共同上行链路，以承载所有的 PortShield 流量。在此配置中，用作 PortShield 主机的安全设备接口应连接到单独的交换机，而并非连接到与活动设备和备用设备相连的同一 X-系列交换机。这将避免针对同一 PortShield VLAN 出现数据包循环。PortShield 成员可以连接到由 Active/Standby 安全设备控制的 X-系列交换机上的端口。

- 支持诊断扩展交换机
- 使用 SPM 的共同上行链路配置中的 VLAN 支持
- 专用上行链路配置中的 VLAN 支持
- 共同上行链路上的 VLAN 流量单点管理

“共同上行链路”也支持 VLAN。安全设备和 X-系列交换机之间的单个链路即可承载管理 X-系列交换机的安全设备的管理流量，以及用于和安全设备接口对应的通过 VLAN 消除接口歧义 (IDV) VLAN 的 PortShield 流量和“共同上行链路”接口下 VLAN 子接口的流量。

① **注：**在对同一台交换机配置为专用上行链路或共同上行链路的安全设备接口下不能存在重叠 VLAN。这是因为 X-系列交换机上的 VLAN 空间是全局空间。

① **注：**不支持将“扩展交换机接口”的 PortShield 连接到“共同上行链路接口”，而不为访问/中继配置选择任何 VLAN。

- 某些 Dell X-系列交换机提供的适用于 SonicWall 安全设备的 PoE/PoE+ 和 SFP/SFP+ 功能
- 批处理配置消息 - 如需促进对 X-系列交换机的支持，可在将配置消息发送到 X-系列交换机之前对其进行批处理。

PortShield 功能和 X-系列交换机

PortShield 架构允许将安全设备端口配置到不同的安全区域中，从而实现对跨区域设备间的流量的深度数据包检查安全设备的保护。如需 PortShield 功能的更多信息，请参阅第 295 页的 [PortShield 配置接口](#)。

SonicWall X-系列解决方案支持对到安全设备接口的扩展交换机上的接口进行端口屏蔽。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。当扩展交换机上的端口对安全设备接口进行了端口屏蔽时，这些端口对应于将 PortShield VLAN 重新配置为的 VLAN 的访问端口，也称为 PortShield 主机接口的 IDV VLAN。

主题：

- 第 300 页的 [不同 PortShield 流量场景](#)
- 第 300 页的 [对 X-系列交换机进行 PortShield 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连接到属于同一 PortShield 群组的安全设备上的端口相连的设备之间的流量将由安全设备上的内部交换机交换。
- 与扩展交换机（目的地为安全设备接口）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安全设备安全服务的影响。
- 与扩展交换机上的端口相连的网络设备及与连接到属于不同区域或不同 PortShield 群组的安全设备上的端口相连的设备之间的流量将由软件中的数据路径转发。该流量受软件中安全设备安全服务的影响。

对 X-系列交换机进行 PortShield 的前提条件

① **重要：**如果拓扑包含两个或更多的 X-系列交换机，X-系列交换机可以级联或以菊花式链接，即一个 X-系列交换机可以连接到另一个已连接到安全设备的 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。

在交换机的初始设置中，如需确保在安全设备接口上启用 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**，而非**动态 IP**。

如需详细信息，请参阅 [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。这样会使安全设备与 X-系列交换机的配置状态不同步。
- 如需从安全设备中管理 X-系列交换机，安全设备的其中一个接口必须与 X-系列交换机位于同一子网中。例如，如需管理默认 IP 为 192.168.2.1 的 X-系列交换机，安全设备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。
- 在从安全设备中设置/管理交换机之前，先从安全设备对 X-系列交换机执行 ping 操作，以确保安全设备可以访问 X-系列交换机。
- VLAN 支持：
 - VLAN 支持可用于共享上行链路和共同上行链路。例如，可以在设置为 X-系列交换机的共享上行链路的安全设备接口下配置 VLAN。
 - 如需 VLAN 支持的详细信息，请参阅 [SonicWall X-系列解决方案部署指南](#)。
 - 在配置为专用上行链路的安全设备接口下，不得存在重叠 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。

Dell X 系列菊花式链接支持

注：此功能在 NSA 2600 平台上不受支持。

Dell TZ-X 菊花式链接解决方案可将 SonicWall 安全设备与菊花式链接模式连接的 Dell X-系列交换机集成在一起。在菊花式链接模式下，支持与所有 Dell X-系列交换机型号（如，X1008/X1008P，X1018/X1018P、X1026/X1026P、X1052/X1052P 和 X4012）的集成。

通过菊花式链接，可以将那些拥有大型设施的对象（例如仓库）在给定站点上部署两台相距 1000 英尺以上的 X 系列交换机，彼此通过光纤连接，第一个交换机（即，父交换机）连接到安全设备并管理安全设备中的两个交换机。通过此部署，您还可以使用安全设备上的单个接口访问 X 系列交换机上增加的接口数。父交换机和子交换机的所有接口都可以从安全设备进行的管理。

主题：

- 第 301 页的 [假设和依赖项](#)
- 第 301 页的 [菊花式链接支持](#)

假设和依赖项

- Dell X-系列交换机菊花式链接解决方案仅支持单一级别的链接。不支持两个以上交换机串联在一起的多级链接。例如，父交换机可以连接到子交换机，但子交换机不得连接到另一个子交换机。
- 可以配置的扩展交换机的最大数量限制为 4 台。例如，父交换机最多可以有三个子交换机。
- 在菊花式链接模式下，子交换机唯一支持的拓扑是共同上行链路，其中子交换机通过单个上行链路连接到父交换机。子交换机不支持其他变体，如专用上行链路、隔离链路等。

菊花式链接支持

两个以菊花式链接模式连接的交换机必须具有位于同一子网中的 IP 地址，并且安全设备必须能够访问此子网。以菊花式链接模式配置交换机的过程包含两个步骤：

- 1 将父交换机配置为独立交换机。
- 2 将子交换机配置为菊花式链接交换机。

PoE/PoE+ 和 SFP/SFP+ 支持

SonicWall 安全设备不支持 PoE/PoE+，但可以通过某些 X-系列交换机添加此功能，如 [X-系列交换机 PoE/PoE+ 和 SFP/SFP+ 支持](#) 表中所示。此附加功能改善了 SonicWall 安全设备的 SonicPoint 使用情况，尤其是支持 802.11ac 的新 SonicPoint（802.11ac 最高支持 30W 最大功率；802.11a/b/g/h 可支持最高 15.4 W 最大功率）。

有些 X-系列交换机还支持 SFP/SFP+，如 [X-系列交换机 PoE/PoE+ 和 SFP/SFP+ 支持](#) 表中所示。

i 注：X-系列交换机上 PoE/PoE+ 端口的配置从 X-系列交换机的 UI 进行管理，而不从 SonicWall 安全设备上的管理 | 系统设置 | 网络 | PortShield 群组进行管理。

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： <ul style="list-style-type: none">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+
X1052P	24 个 PoE/12 个 PoE+ 端口，总共多达 369W；默认情况下： <ul style="list-style-type: none">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+

i 重要：在 X1026P 或 X1052P X-系列交换机上，无外部电源的 SonicPoint AC 必须对端口 1 到 12 进行端口屏蔽。

无外部电源的任何 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

扩展交换机上的端口可以端口屏蔽至安全设备的 WLAN 区域，并可以将 SonicPoint 连接到这些端口。

将 SonicPoint 连接到 X-系列交换机时，必须考虑 SonicPoint 的电源要求。SonicPointACe/ACi/N2 最少需要 25.5 W。如果您的 X-系列交换机型号不支持 PoE+，必须使用 SonicPoint 供电。如需支持 PoE+ 的交换机型号的信息，请参阅第 302 页的 [PoE/PoE+ 和 SFP/SFP+ 支持](#)。如需了解管理 SonicPoint 的更多信息，请参阅知识库文章 [管理 SonicPoint ACe/ACi/N2 接入点的 SonicWall TZ 系列和 SonicWall X-系列解决方案\(SW13970\)](#)。

使用 GMS 管理扩展交换机

X-系列交换机集成功能允许使用 SonicOS 管理界面和 SonicWall GMS 版本 8.1 SP1 或更高版本对安全设备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

扩展交换机全局参数表显示可通过 SonicOS 管理界面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 [SonicWall X-系列解决方案部署指南](#)。

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) 链路仅承载管理流量且无法进行端口屏蔽。

数据链接承载所有 PortShield 流量。如果其承载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，数据链路也承载管理流量，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。

一个专用链路只能承载一个端口屏蔽的组且必须将该组端口屏蔽到安全设备上的专用端口。

关于上行链路接口

可以将上行链路接口视为设置用于承载标记/未标记的流量的“中继”端口。当扩展交换机添加了安全设备上行链路和 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。通过已标记流量的 IDV VLAN，固件可以获得流量的 PortShield 主机接口。

配置上行链路接口的条件

- 接口必须为物理接口；不允许使用虚拟接口。
- 接口必须为交换机接口。（在一些平台上，部分安全设备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（某个安全设备接口不能对其进行端口屏蔽）或 PortShield 群组成员（不能对另一安全设备接口进行端口屏蔽）。
- 接口不能为桥接主要或桥接次要接口。
- 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 PortShield 及端口可上行/下行等网络事件。

支持的拓扑

① **重要：** 在设置安全设备和 X-系列交换机之间的接口前，请按照 [SonicWall X-系列解决方案部署指南](#) 中的描述设置交换机。

① **注：** 如需提供和配置这些拓扑的更多信息，请参阅 [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 接口的基本详细信息，请参阅第 305 页的 [管理端口](#)。

X-系列交换机支持的主要支持拓扑为：

- 共同上行链路配置
- 专用上行链路配置
 - ① **重要：** 必须通过作为专用链路一部分的端口对 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
- 用于管理和数据上行链路的独立链路
- 包含专用上行链路的 HA 和 PortShield 配置
- 包含共同上行链路的 HA 和 PortShield 配置
- 包含使用 SPM 的共同上行链路配置的 VLAN
- 包含专用上行链路配置的 VLAN
- 用于 SonicPoint 访问的专用链路

管理端口

重要：SOHO W 安全设备不支持 X-系列解决方案。尽管以相同方式管理所有的安全设备端口，但是对于这些安全设备，[管理 | 系统设置 | 网络 | PortShield 群组](#)不同；请参阅第 313 页的[管理 SOHO W 防火墙上](#)的端口。



[管理 | 系统设置](#)借助 [网络 | PortShield 群组](#)，您可以通过下列对象对 PortShield 接口的端口分配：

- 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[查看端口图形上的接口（端口）](#)
- 第 308 页的[在“端口配置”选项卡上查看 PortShield 接口的状态并对这些接口进行编辑](#)
- 第 310 页的[查看并管理外部交换机配置](#)
- 第 311 页的[监控外部交换机诊断并管理固件](#)
- 第 313 页的[管理 SOHO W 防火墙上](#)的端口

查看端口图形上的接口（端口）



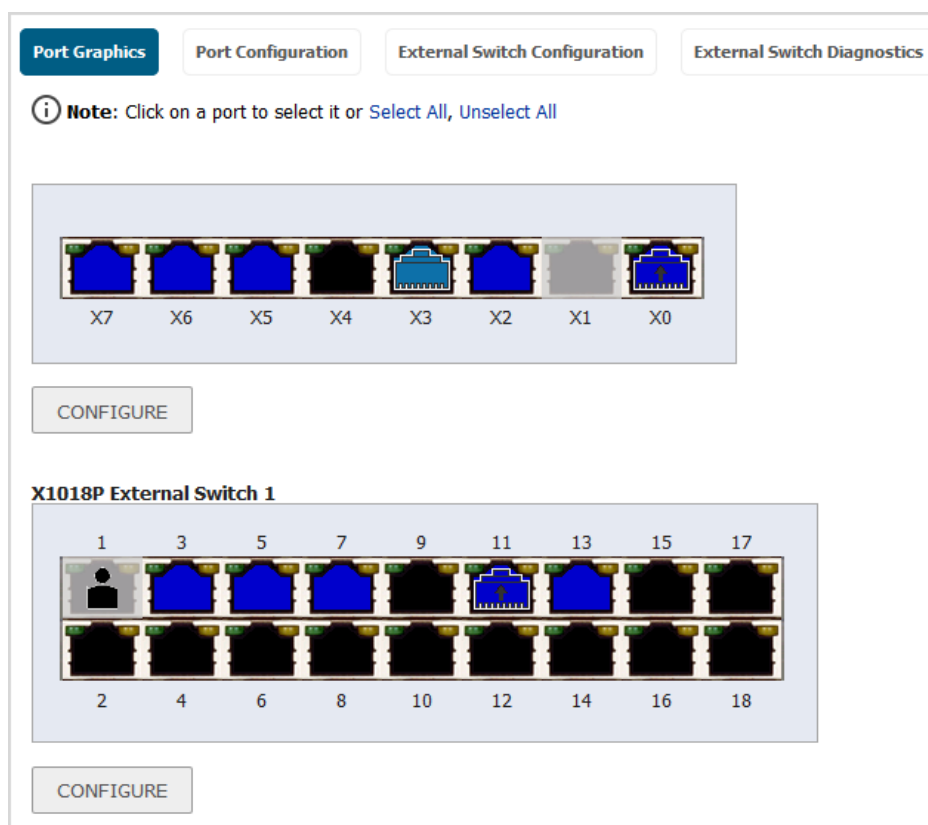
端口图形显示安全设备的 PortShield 接口（端口）。大图形表示安全设备的接口。接口的颜色代码反应其配置：

接口配置的颜色代码

此颜色	指定此类型的接口
黑色	未分配，即不属于 PortShield 群组
黄色	已选择进行配置
相同颜色（黑色、黄色或灰色除外）	属于 PortShield 群组且主接口的颜色周围有一个白色的轮廓
变灰	无法分配，即无法添加到 PortShield 群组中
有人形图形的灰色接口	切换 MGMT
带向上箭头的任何（黑色、黄色或灰色除外）	上行

每个端口图形标签为其相关端口名：X0 - Xn。选择一个或多个接口后，可以按照第 313 页的[配置 PortShield 群组](#)的说明进行配置。

配置了扩展交换机时



配置一个或多个扩展交换机时，端口图形显示安全设备和交换机的 PortShield 接口（端口）：

- 第一个图形显示安全设备的端口且未进行标记。
- 下一个图形显示第一个外部交换机 External Switch 1 的端口，标记为 **SwitchModel External Switch 1**，例如 X1018P External Switch 1。
- 如果提供更多的外部交换机，后续图形按其 ID 顺序（即，External Switch 2、External Switch 3 和 External Switch 4）显示其他外部交换机的端口。

外部接口的颜色编码与安全设备的颜色编码相同；请参阅[接口配置的颜色代码表](#)。

在“端口配置”选项卡上查看 PortShield 接口的状态并对这些接口进行编辑

无扩展交换机

端口图形 **端口配置** 外部交换机配置 外部交换机诊断

清除统计

名称	PortShield 接口	类型	连接设置	链接状态	已启用	注释	配置
X0	LAN	铜线	自动协商	无链接	✓	Default LAN	
X1	WAN	铜线	自动协商	1 Gbps 全双工	✓	Default WAN	
X2	独立的	铜线	手动	1 Gbps 全双工	✓	WXA series appliance	
X3	WAN	铜线	自动协商	1 Gbps 全双工	✓		
X4	WAN	铜线	自动协商	无链接	✓		
X5	未分配	铜线	自动协商	无链接	✓		
X6	未分配	铜线	自动协商	无链接	✓		

有扩展交换机

Port Graphics **Port Configuration** External Switch Configuration External Switch Diagnostics

CLEAR STATISTICS

Name	PortShield Interface	Type	Link Settings	Link Status	Enabled	Comment	Configure
X0	LAN	Copper	Auto Negotiate	No link	✓	Default LAN	
X1	WAN	Copper	Auto Negotiate	1 Gbps Full Duplex	✓	Default WAN	
X2	X0	Copper	Auto Negotiate	No link	✓		
X3	Independent	Copper	Auto Negotiate	1 Gbps Full Duplex	✓		
X4	Unassigned	Copper	Auto Negotiate	No link	✓		
X5	X0	Copper	Auto Negotiate	No link	✓		
X6	X0	Copper	Auto Negotiate	No link	✓		
X7	X0	Copper	Auto Negotiate	No link	✓		
ES1 : 1	MGMT	Copper	Auto Negotiate	No Link	✓	Switch MGMT - ES1	
ES1 : 2	Unassigned	Copper	Auto Negotiate	1 Gbps Full Duplex	✓		
ES1 : 3	X0	Copper	Auto Negotiate	No Link	✓	PortShield to X0	
ES1 : 4	Unassigned	Copper	Auto Negotiate	No Link	✓		
ES1 : 5	X0	Copper	Auto Negotiate	No Link	✓	PortShield to X0	
ES1 : 6	Unassigned	Copper	Auto Negotiate	No Link	✓		
ES1 : 7	X0	Copper	Auto Negotiate	No Link	✓	PortShield to X0	
ES1 : 8	Unassigned	Copper	Auto Negotiate	No Link	✓		
ES1 : 11	X0	Copper	Auto Negotiate	No Link	✓	Dedicated Uplink for X0	
ES1 : 12	Unassigned	Copper	Auto Negotiate	No Link	✓		
ES1 : 13	X0	Copper	Auto Negotiate	No Link	✓	PortShield to X0	
ES1 : 17	Unassigned	Copper	Auto Negotiate	No Link	✓		
ES1 : 18	Unassigned	Copper	Auto Negotiate	No Link	✓		

端口配置选项卡包含一个表，其中列出了 PortShield 接口的相关信息：

名称	与 PortShield 接口关联的端口名，如 X0 或 X15。任何外部交换机的端口以 ESs:n 格式显示，其中 s 是交换机 ID，而 n 是端口号（如果适用）。
PortShield 接口	颜色编码的图形反映了 PortShield 接口的分配和所属的 PortShield 群组。此图形是端口图形上较大图形的缩小版。
类型	端口类型： <ul style="list-style-type: none">• 铜线• 无线
连接设置	链路速度： <ul style="list-style-type: none">• 自动协商• 1000 Mbps - 全工• 100 Mbps - 全工• 100 Mbps - 半工• 10 Mbps - 全工• 10 Mbps - 半工
链路状态	显示以下内容之一： <ul style="list-style-type: none">• 当前链路速度（绿色），例如 1000 Mbps - 全双工。• 无链路。
启用	启用图标 <ul style="list-style-type: none">• 为绿色（如果启用了接口）。• 处于灰显状态（如果禁用了接口）。
注释	配置接口后输入的任何备注。
配置	包含以下两个图标： <ul style="list-style-type: none">• 统计 - 单击该图标后，将显示包含接口统计的弹出摘要：



注：如需清除所有统计信息，请单击网络 | PortShield 群组 > 端口配置顶部的清除统计信息。

- 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，请参阅第 315 页的在 [网络 | PortShield 群组上配置 PortShield 接口](#) 中的步骤。

查看并管理外部交换机配置

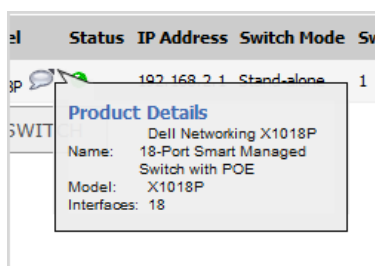
ID	Model	Status	IP Address	Switch Mode	Switch Management	Firewall Uplink	Switch Uplink	Parent Switch ID	Parent Switch Uplink	Configure
1	X1018P		192.168.2.1	Stand-alone	1	None	None	N/A	N/A	

ADD SWITCH

注： 如果未提供外部交换机，此表将显示无条目。

ID 外部交换机的 ID 编号：**1、2、3 或 4。**

型号 外部交换机的型号。此列还包含每个交换机的备注图标，该图标会显示包含产品详细信息的弹出式摘要。



状态 交换机的状态：绿色的启用图标表示交换机正常、可用。

注： 当扩展交换机已关闭然后安全设备重启时，可能要花费 5 分钟安全设备才能发现扩展交换机，并将交换机的状态报告为“正常且可用”。

IP 地址 扩展交换机的 IP 地址。

交换机模式 交换机的模式，如**独立**。

交换机管理 用于管理流量的交换机端口。

防火墙上行链路 安全设备上配置为安全设备上行链路的端口。如果安全设备端口未配置为安全设备上行链路，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**。

父交换机 ID 对于菊花式链接的交换机，父交换机的 ID。如果任何交换机端口都未配置为父交换机，此列将显示**无**。

父交换机上行链路 配置为交换机上行链路的菊花式链接的父交换机上的端口。如果任何交换机端口都未配置为父交换机上行链路，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。

外部交换机配置提供了安全设备上配置的外部交换机的相关信息并允许您管理交换机。用户还可以配置或删除扩展交换机。如需配置扩展交换机，请参阅第 313 页的**配置 PortShield 群组**。如需删除扩展交换机，请参阅 **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

i | 注：如果未提供外部交换机，此表将显示无条目。

通过外部交换机诊断，您可以：

- 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 311 页的 [更改显示](#)
- 第 311 页的 [监控统计信息](#)
- 第 312 页的 [重启外部交换机](#)
- 第 312 页的 [管理外部交换机固件](#)

更改显示

外部交换机诊断一次只能显示一个交换机的统计信息及其他相关信息。默认情况下，会显示外部交换机 1 ES1 的数据。您有两个或两个以上的外部交换机时，如需显示另一个外部交换机的相关数据，请从交换机名称中选择 **ES2**、**ES3** 或 **ES4**：

监控统计信息

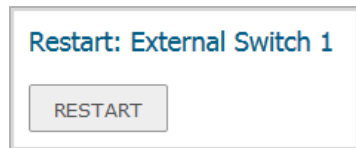
统计表显示了所有统计信息。如需重启统计信息收集，请单击清除以重置计数器。

名称	端口名称，1 - n。
状态	端口为正常还是关闭。
收到的单播数据包数	从该端口接收的单播数据包数。
接收的组播数据包数	从该端口接收的组播数据包数。
接收的广播数据包数	从该端口接收的广播数据包数。
接收的字节数	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。
FCS 错误	从该端口接收的 FCS（帧校验序列）错误数。
单个冲突帧数	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。

接收的暂停帧数 通过该端口接收的暂停帧数。

发送的暂停帧数 通过该端口发送的暂停帧数。

重启外部交换机





重要：当扩展交换机已关闭，然后安全设备重启时，安全设备可能需要 5 分钟时间才能发现扩展交换机并将该交换机的状态报告为已连接。

重启外部交换机的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | PortShield 群组。
- 2 单击外部交换机诊断。
- 3 从交换机名称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

Firmware Management: External Switch 1				
Type	Version	Date Created	Time Created	Upload
Firmware	3.0.0.64	02252015	09:05:11	
Boot Code	1.0.0.14	12032014	15:04:07	

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。

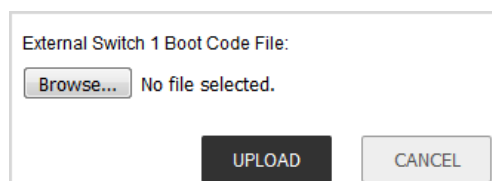
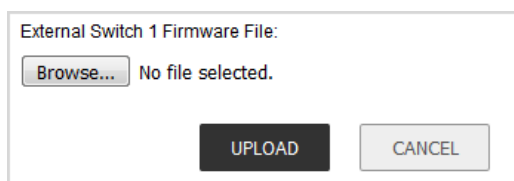
创建时间 固件或启动代码的创建时间。

上传 上传图标；对于

- 固件，显示上传外部交换机固件对话框；
- 引导代码，显示上传外部交换机启动代码对话框；

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。

管理 SOHO W 防火墙上的端口

SOHO W 安全设备的网络 | PortShield 群组页面有不同的外观。此页面上的信息包含有关端口图形（请参阅第 306 页的查看端口图形上的接口（端口））和端口配置（第 308 页的在“端口配置”选项卡上查看 PortShield 接口的状态并对这些接口进行编辑）的信息。

Note: Click on a port to select it or [Select All](#), [Unselect All](#)



CONFIGURE

Name	PortShield Interface	Type	Link Settings	Link Status	Enabled	Comment	Configure
X0	LAN	Copper	Auto Negotiate	No link	<input checked="" type="checkbox"/>		
X1	WAN	Copper	Auto Negotiate	1 Gbps Full Duplex	<input checked="" type="checkbox"/>	Default WAN	
X2	Unassigned	Copper	Auto Negotiate	No link	<input checked="" type="checkbox"/>		
X3	Independent	Copper	Manual	No link	<input checked="" type="checkbox"/>	WXA series appliance	
X4	X0	Copper	Auto Negotiate	No link	<input checked="" type="checkbox"/>		
W0	WLAN	Wireless	Auto Negotiate	450 Mbps Half Duplex	<input checked="" type="checkbox"/>	Default WLAN	

可以按照第 313 页的[配置 PortShield 群组](#)中所述配置安全设备接口。

配置 PortShield 群组

可以在 SonicOS 管理界面的几个不同页面上配置 PortShield 群组：

- 第 314 页的[在网络 | 接口上配置 PortShield 接口](#)
- 第 314 页的[配置 PortShield 接口与 PortShield 接口指南](#)（仅限 TZ 系列和 SOHO W 防火墙）
- 第 315 页的[在网络 | PortShield 群组上配置 PortShield 接口](#)
- 第 317 页的[从端口图形配置外部交换机 PortShield 群组](#)

在网络 | 接口上配置 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，该端口不会在 **PortShield** 接口中列出。

配置 **PortShield** 接口的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | 接口**。
- 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。



The screenshot shows a configuration window titled "接口 'X12' 设置" (Interface 'X12' Settings). At the top, there are two tabs: "常规" (General) and "高级" (Advanced). Below the tabs, there are two dropdown menus. The first is labeled "区域:" (Zone) and is set to "未分配" (Unassigned). The second is labeled "模式 / IP 分配:" (Mode / IP Allocation) and is also set to "未分配" (Unassigned).

- 3 从区域中，选择一个您要在此接口映射到的区域类型选项。此时显示更多选项。
注：您只能将 **PortShield** 接口添加到受信任的、公用和无线区域中。
- 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 从 **PortShield** 到中，选择您要在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。

配置 PortShield 接口与 PortShield 接口指南（仅限 TZ 系列和 SOHO W 防火墙）

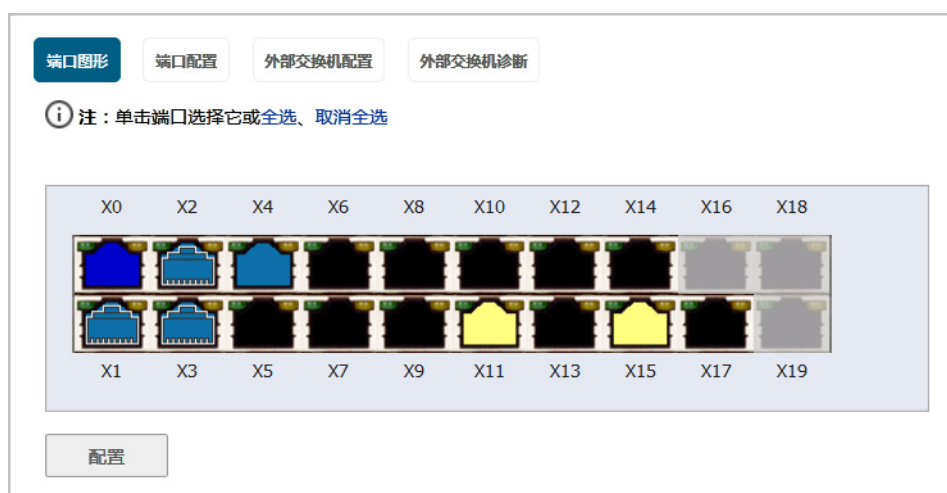
可以按照 SonicOS 快速配置指南中的描述通过 **PortShield** 接口指南配置 **PortShield** 接口。可以通过下列方式访问 **PortShield** 接口指南：

- 在任何管理界面页面上单击 **快速配置指南**。将显示 **配置指南**；选择 **PortShield** 接口指南。
- 在 TZ 系列或 SOHO W 安全设备上的 **管理 | 系统设置 | 网络 | 接口** 页面中，单击 **PORTSHIELD** 向导以显示 **PortShield** 接口指南。

在网络 | PortShield 群组上配置 PortShield 接口



端口图形显示 PortShield 接口的当前配置的图形表示。如需图形显示的描述，请参阅第 306 页的[查看端口图形上的接口（端口）](#)。

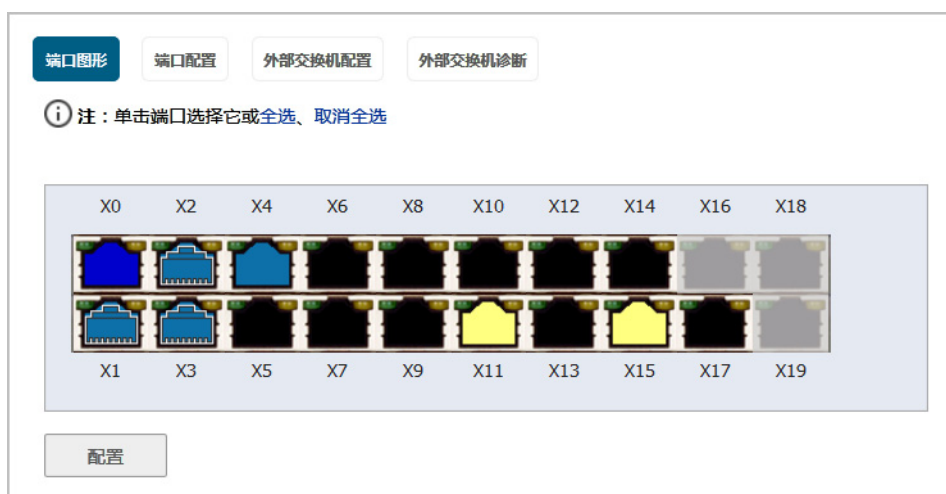


通过单击要分组的端口，可以使用图形 **PortShield** 群组界面手动对端口进行分组。通过组合端口，它们可以共享共同的网路子网以及共同的区域设置。

注：必须在分组为 PortShield 之前对接口进行配置。

配置 PortShield 群组的步骤如下：

- 1 在端口图形中，选择要配置为 PortShield 群组的组成部分的接口。这些接口将变成黄色。



- 2 单击配置。随即显示编辑交换机端口对话框。



注：此端口的接口名称将显示为灰色且无法进行更改。

- 3 从启用端口中，选择启用还是禁用这些接口。默认为已启用。
- 4 从 PortShield 接口中，选择要作为此 PortShield 接口的主接口分配的接口。默认值是未分配。

注：可以对外部交换机端口禁用 PortShield 选项。

- 5 从链路速度中，选择接口的链路速度：

- 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。

从端口图形配置外部交换机 PortShield 群组

重要：当扩展交换机已关闭，然后安全设备重启时，安全设备可能需要 5 分钟时间才能发现扩展交换机并将该交换机的状态报告为已连接。

在 PortShield 群组中配置扩展交换机时，该配置可能需要 5 分钟时间才能显示在 **网络 | PortShield 群组** 上。

重要：必须在分组为 PortShield 之前对接口进行配置。

注：如需了解为各种剖析图配置 PortShield 群组的方法，请参阅 [SonicWall X-系列解决方案部署指南](#)。

注：SOHO W 安全设备不支持扩展交换机。

网络 | PortShield 群组 显示安全设备和扩展（外部）交换机上 PortShield 接口的当前配置的图形表示。如果有一个外部交换机，有两个图形。有两个外部交换机则有三个图形，依此类推。交换机图形标有交换机型号和外部交换机 ID：1、2、3、4。

通过单击要分组的端口，可以使用图形 PortShield 群组界面手动将安全设备和交换机上的端口分组到一起。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。

配置包含外部交换机的 PortShield 群组的步骤如下：

- 1 按照第 315 页的 [在网络 | PortShield 群组上配置 PortShield 接口](#) 中的过程配置安全设备上的端口。
- 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。它显示您选择的安全设备和外部交换机的端口的名称（n 为所选端口）：

- 防火墙端口命名为 **Xn**。
- 外部交换机 1 端口命名为 **ES1n**。
- 外部交换机 2 端口命名为 **ES2: n**。
- 外部交换机 3 端口命名为 **ES3: n**。
- 外部交换机 4 端口命名为 **ES4: n**。

4 从启用端口中，选择：

- 禁用
- 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 从 **PortShield** 接口中，选择要作为这些 PortShield 接口的主接口分配的接口：

- 未分配
- 端口名称
 - ① **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，该端口不会在 **PortShield** 接口中列出。
- -保存当前设置-（默认）
 - ① **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** 中，选择接口的链路速度：

- 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**。

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[网络 | 故障切换和负载均衡](#)
 - 第 324 页的[配置故障切换和负载均衡组](#)
 - 第 327 页的[配置群组成员的探测设置](#)

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[网络 | 故障切换和负载均衡](#)
- 第 324 页的[配置故障切换和负载均衡组](#)
- 第 327 页的[配置群组成员的探测设置](#)

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，也建议始终启用“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

管理 | 网络 | 接口允许配置两个以上的 WAN 接口用于路由。可以在网络 | 接口中配置 WAN 接口，但不能将它们包含在网络 | 故障切换和负载均衡中。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。

接口设置									
名称	区域	群组	IP 地址	子网掩码	IP 分配	状态	已启用	备注	配置
X0	LAN		192.168.168.168	255.255.255.0	静态	无链接	<input checked="" type="checkbox"/>	Default LAN	
X1	WAN	Default LB Group	192.168.95.83	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	Default WAN	
X2	LAN		192.168.94.83	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	WXA series appliance	
X3	WAN		0.0.0.0	0.0.0.0	PPPoE 连接	1 Gbps 全双工	<input checked="" type="checkbox"/>		

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。

网络 | 故障切换和负载均衡

设置											
<input checked="" type="checkbox"/> 启用负载均衡 <input type="checkbox"/> 对探针的响应 目前探测比率：< 1 每秒钟，0 全部 <input type="checkbox"/> 任何 TCP-SYN 针对端口 0											
群组											
名称	类型	IP 地址	连接状态	负载均衡状态	主要目标	可选目标	配置	注释			
<input type="checkbox"/> Default LB Group 基本故障切换											
X1		192.168.95.83 (WAN)	链路连接	可用	已禁用	已禁用					
统计											
显示统计为：Default LB Group 清除											
接口	总计连接	新建连接	当前比率	平均比率	总计单播字节	Rx 单播	接收字节数	Tx 单播	发送字节数	吞吐量 (KB/s)	吞吐量 (Kbits/s)
X1	646947	54	100	100	241909477	520799	70972376	646945	170937101	0	0

主题：

- 第 322 页的 [设置](#)
- 第 322 页的 [群组](#)
- 第 323 页的 [统计](#)

设置

设置

启用负载均衡

对探针的响应

目前探测比率：< 1 每秒钟，0 全部

任何 TCP-SYN 针对端口

- 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，也建议始终启用“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。默认情况下未选中该选项。

随即显示当前探测速率和探测总数。

 - 任何 TCP-SYN 针对端口 - 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。默认情况下未选中该选项。

群组

群组

名称	类型	IP 地址	连接状态	负载均衡状态	主要目标	可选目标	配置	注释
▼ Default LB Group	基本故障切换							
X1		192.168.95.83 (WAN)	链路连接	可用	已禁用	已禁用		

添加到负载均衡组的负载均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。
- 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

接口	总计连接	新建连接	当前比率	平均比率	总计单播字节	Rx 单播	接收字节数	Tx 单播	发送字节数	吞吐量 (KB/s)	吞吐量 (Kbits/s)
X1	647467	54	100	100	242153122	521163	71060858	647454	171092264	1	11

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
- 总计连接
- 新建连接
- 当前比率
- 平均比率
- 总计单播字节
- Rx 单播
- 接收字节数
- Tx 单播
- 发送字节数

- 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 页的常规设置
- 第 326 页的探测设置

常规设置

配置“组”设置的步骤如下：

- 1 转至管理 | 网络 | 故障切换和负载均衡。
- 2 单击要配置的群组的配置图标。将显示编辑 LB 群组对话框。

- 3 编辑名称字段中群组的显示名称。默认群组的名称无法更改且字段将显示为灰色。
- 4 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

轮询机制随即返回主要 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。

5 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	如有可能，抢占并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。

6 在**群组成员**：选择此处：/已选的列表中添加、删除及对成员接口排序。 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：

7 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。

8 您可以按如下步骤对**已选**的列中的条目进行排序：

- 选择一个条目。
- 单击**上/下**按钮。

9 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。请参阅第 326 页的**将带宽配置为比率**。

i | **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。

10 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。

11 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。

12 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。

i | **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。

13 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。如需指定“最后的备份”接口，请在“群组成员”列表中选择一条目，然后单击双右箭头按钮。如需删除**最后的备份**接口，请单击双左箭头按钮。

14 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。

i | **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。

探测设置

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。

i | **注：** 用于可替换的 WAN 的 VLAN 不支持 QoS 或 VPN 终止。

配置特定组的探测选项的步骤如下：

- 1 转至管理 | 网络 | 故障切换和负载均衡
- 2 单击要配置的群组的配置图标。将显示编辑 LB 群组对话框。
- 3 单击探测。

常规 探测

检查接口的时间间隔： 5 秒

使接口在： 6 次丢失的间隔后无效

使接口在： 3 次成功的间隔后有效

探测 responder.global.sonicwall.com 在该群组上的所有接口

- 4 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。
- ① 注：拨号 WAN 探测设置也会恢复为默认的内置设置。

- 5 单击确定。

配置群组成员的探测设置

配置群组成员探测设置的步骤如下：

- 1 转至管理 | 网络 | 故障切换和负载均衡
- 2 单击要配置的群组成员的配置图标。随即显示探测设置对话框。

X1 探测设置

仅物理监控
 逻辑的/探测监控启用

总是成功（无探测）。

	主要目标：	主机：	端口：
主要目标：	TCP	responder.global.sonicwall.com	50000
可选目标：	TCP	responder.global.sonicwall.com	50000
默认目标 IP：	204.212.170.23		

注：IP 地址：0.0.0.0 或者 DNS 解析失败将使用默认目标 IP 配置。

- 3 选择要完成的探测类型：
 - 仅物理监控（默认；所有其他选项显示为灰色）。转至 [步骤 9](#)。
 - 逻辑的/探测监控启用 - 所有其他选项可用。
- 4 从逻辑的/探测监控启用中，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。转至 [步骤 9](#)。
- 5 从主要目标中，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**。
- 6 如果选择了“当主要目标响应时，探测成功”，请转至 [步骤 8](#)。
- 7 从可选目标下拉菜单中，选择：

i 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**。
- 8 在默认目标 IP 字段中，输入默认网关的 IP 地址。

i 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。
- 9 单击确定。

配置网络区域

- 第 329 页的[关于区域](#)
 - 第 330 页的[区域的工作方式](#)
 - 第 330 页的[预定义区域](#)
 - 第 331 页的[安全类型](#)
 - 第 331 页的[允许接口信任](#)
 - 第 331 页的[对区域启用 SonicWall 安全服务](#)
- 第 332 页的[网络 | 区域](#)
 - 第 333 页的[区域设置表](#)
 - 第 333 页的[添加新区域](#)
 - 第 340 页的[删除区域](#)
 - 第 335 页的[配置访客访问的区域](#)
 - 第 338 页的[配置用于开放式验证和社交登录的区域](#)
 - 第 338 页的[配置 WLAN 区域](#)

关于区域

区域是一个或多个用于进行管理工作的接口的逻辑分组，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，它使管理员能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，请参阅第 230 页的[网络 | 接口](#)。

SonicOS 区域可用于将安全策略应用到网络内部。这样，您可以通过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来实现此目的。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，以便您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 330 页的[区域的工作方式](#)
- 第 330 页的[预定义区域](#)

- 第 331 页的 [安全类型](#)
- 第 331 页的 [允许接口信任](#)
- 第 331 页的 [对区域启用 SonicWall 安全服务](#)

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。以上示例是区域有多个绑定的接口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。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。SonicWall 安全设备上的预定义安全区域无法修改：

此区域	包含此功能
DMZ	通常用于可公开访问的服务器，可以由一到四个接口组成，具体取决于网络设计。
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。
组播	此区域提供 IP 组播支持，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	此区域用于使用 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	此区域支持 SonicWall SonicPoint 和 SonicWave。在分配给 Opt 端口后，它会实施 SonicPoint 强制措施，并自动丢弃所有从非 SonicPoint 设备接收的数据包。WLAN 区域支持： <ul style="list-style-type: none"> • 发现协议 (SDP)，以自动轮询和识别已连接的 SonicPoint 和 SonicWave

此区域	包含此功能
	<ul style="list-style-type: none"> • SonicWall 简单设置协议，以使用配置文件来配置 SonicPoint 和 SonicWave • 无线和访客服务配置
WAN:	可以包含多个接口。如果您使用的是安全设备的 WAN 故障切换功能，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：

受信任	提供最高的信任级别 - 这意味着，仅对来自受信任区域的流量应用最少的审查。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	对于 MGMT 区域和 MGMT 接口唯一，而且还提供最高的信任级别。
加密	仅由 VPN 和 SSLVPN 区域使用。流入和流出加密区域的所有流量都已经过加密。
无线	适用于 WLAN 区域或网络的唯一接口由 SonicWall SonicPoint 和 SonicWave 设备组成的任何区域。无线安全类型专门设计用于和 SonicPoint 与 SonicWave 一起使用。将接口放入无线区域中可激活该接口上的 SDP（SonicWall 发现协议）和 SSPP（SonicWall 简易配置协议），以自动发现和配置 SonicPoint 与 SonicWave。仅允许通过 SonicPoint 或 SonicWave 的流量通过无线区域；系统会丢弃所有其他流量。
公用	提供的信任级别高于不受信任的区域，但低于受信任的区域。可以将公用区域视为介于安全设备的 LAN（受保护）一侧与 WAN（未受保护）一侧之间的安全区域。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，将拒绝从 DMZ 到 LAN 的流量，但允许从 LAN 到 ANY 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 仅拥有对 WAN 的默认访问权，而没有对 LAN 的访问权。
不受信任	代表最低的信任级别。由 WAN 和虚拟组播区域使用。可以将不受信任区域认为处于安全设备的 WAN（未受保护的）一侧。默认情况下，如果没有明确规则，不允许来自不受信任区域的流量进入其他任何区域类型，但允许来自所有其他区域类型的流量流入不受信任的区域。

允许接口信任

添加区域对话框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，使这些接口上的主机能相互通信。

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。可以在区域上启用以下 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 GroupVPN 策略，该策略显示在管理 连接 VPN > 基本设置上的 VPN 策略表中。您可以在 VPN > 设置上自定义 GroupVPN 策略。如果取消选中创建群组 VPN，则将从 VPN > 设置中删除 GroupVPN 策略。如需创建 VPN 策略的更多信息，请参阅 SonicOS 连接。
启用 SSL 控制	在区域中启用 SSL 控制。从该区域发起的所有新 SSL 连接现在都将接受检查。必须先管理 防火墙设置 SSL 控制上全局启用 SSL 控制。如需 SSL 控制的更多信息，请参阅 SonicOS 安全配置。
启用 SSLVPN 访问	对区域启用 SSLVPN 安全远程访问。

网络 | 区域

#	名称	安全类型	成员接口	接口信任	客户端防病毒	客户端 CF	网关防病毒	防间谍软件	IPS	应用程序控制	SSL 控制	SSLVPN 访问	配置
<input type="checkbox"/>	1	LAN	受信任的	X0, X2	✓		✓	✓	✓	✓			
<input type="checkbox"/>	2	WAN	不信任的	X1, X3, X4, U0			✓	✓	✓	✓			
<input type="checkbox"/>	3	DMZ	公用		✓								
<input type="checkbox"/>	4	VPN	加密的										
<input type="checkbox"/>	5	SSLVPN	SSLVPN									✓	
<input type="checkbox"/>	6	MGMT	管理	MGMT	✓		✓	✓	✓	✓			
<input type="checkbox"/>	7	MULTICAST	不信任的										
<input type="checkbox"/>	8	WLAN	无线	X2:V402									

- 第 333 页的[区域设置表](#)
- 第 333 页的[添加新区域](#)
- 第 340 页的[删除区域](#)
- 第 335 页的[配置访客访问的区域](#)
- 第 338 页的[配置用于开放式验证和社交登录的区域](#)
- 第 338 页的[配置 WLAN 区域](#)

区域设置表

区域设置表显示了 SonicWall 安全设备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	安全类型	成员接口	接口信任	客户端防病毒	客户端 CF	网关防病毒	防间谍软件	IPS	应用程序控制	SSL 控制	SSLVPN 访问	配置
<input type="checkbox"/> 1	LAN	受信任的	X0, X2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 2	WAN	不信任的	X1, X3, X4, U0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 3	DMZ	公用		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 4	VPN	加密的		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 5	SSLVPN	SSLVPN		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 6	MGMT	管理	MGMT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 7	MULTICAST	不信任的		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 
<input type="checkbox"/> 8	WLAN	无线	X2:V402	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	 

- 名称** 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** 安全类型：受信任的、不受信的、公用、无线或加密。
- 成员接口** 作为区域成员的接口。
- 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。
- 客户端防病毒** 复选标记表示为流入和流出该区域的流量启用了 SonicWall 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。
- 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。
- SSL VPN 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** 对话框。单击 **删除** 图标将删除该区域。对于预定义区域，删除图标显示为灰色；您无法删除这些区域。

添加新区域

添加新区域的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | 区域**。
- 2 单击 **添加** 图标。随即显示 **添加区域** 对话框。

常规

常规设置

名称：

安全类型：

- 允许接口信任
- 自动添加访问规则以允许相同信任级别的区域间的流量
- 自动添加访问规则以允许到更低信任级别的区域的流量
- 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
- 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
- 启用客户端防病毒增强服务
- 启用客户端内容过滤服务
- 启用 SSLVPN 访问
- 创建群组 VPN
- 启用 SSL 控制
- 启用网关防病毒服务
- 启用 IPS
- 启用防间谍软件服务
- 启用应用程序控制服务

3 在名称字段中输入新区域的名称。

4 从安全类型中选择：

受信任 用于最高信任级别的区域（例如内部 LAN 网段）。

公用 信任要求级别较低的区域（例如，DMZ 接口）。

无线 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。

注： 选择此安全类型将禁用此对话框上的 VPN 和 SSL VPN 选项。

5 如需允许区域内通讯，请选中允许接口信任。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。

6 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。例如 CUSTOM_LAN -> CUSTOM_LAN 或 CUSTOM_LAN -> LAN。默认情况下已选中该选项。

注： 对于此选项和以下访问规则选项，请参阅 SonicOS 策略以获取访问规则的相关信息。

7 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。例如 CUSTOM_LAN -> WAN 或 CUSTOM_LAN -> 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。例如 LAN -> CUSTOM_DMZ 或 CUSTOM_LAN -> CUSTOM_DMZ。默认情况下已选中该选项。

9 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。例如 WAN -> CUSTOM_LAN 或 DMZ -> CUSTOM_LAN。默认情况下已选中该选项。

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**。默认情况下未选中该选项。

i | **注：**此选项将显示为灰色并且不可用，直到您从**安全类型**中选择安全类型。

i | 对于此选项和以下安全服务选项，请参阅 SonicOS 安全配置以了解这些服务的更多相关信息。

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**。默认情况下未选中该选项。

i | **注：**此选项将显示为灰色并且不可用，直到您从**安全类型**中选择安全类型。

12 如需对区域启用 SSLVPN 安全远程访问，请选中**启用 SSLVPN 访问**。默认情况下未选中该选项。

i | **注：**如果选择 **SSLVPN** 作为**安全类型**，该选项将显示为灰色。

13 如需自动为此区域创建 SonicWall 群组 VPN 策略，请选中**创建群组 VPN**。可以在**管理 | 连接性 | VPN | 设置**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”将删除所有对应的群组 VPN 策略。

i | **注：**如果选择 **SSLVPN** 作为**安全类型**，该选项将显示为灰色。

对于此连接选项和其他连接选项，请参阅 SonicOS 连接以了解更多信息。

14 如需在区域上启用 SSL 控制，请选中**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。默认情况下未选中该选项。

i | **注：**必须首先在**管理 | 安全配置 | 防火墙 | SSL 控制**上全局启用 SSL 控制。

15 如需在您的安全设备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，请选中**启用网关防病毒服务**。SonicWall 网关防病毒用于管理安全设备上的防病毒服务。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 区域中的多个接口强制实施入侵检测和保护，请选中**启用 IPS**。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，请选中**启用防间谍软件服务**。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，请选中**启用应用程序控制服务**。默认情况下未选中该选项。如需应用程序控制的更多信息，请参阅 SonicOS 策略。

19 单击**确定**。现在，新区域已添加到安全设备中。

配置访客访问的区域

i | **重要：**无法配置不受信任、已加密、SSL VPN 或管理区域用于访客访问。

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 转至管理 | 系统设置 | 网络 | 区域。
- 2 单击想要为其添加访客服务的区域的配置按钮。将显示编辑区域对话框。

常规 | **访客服务**

常规设置

名称：

安全类型：

- 允许接口信任
- 自动添加访问规则以允许相同信任级别的区域间的流量
- 自动添加访问规则以允许到更低信任级别的区域的流量
- 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
- 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
- 启用客户端防病毒增强服务
- 启用客户端内容过滤服务
- 启用 SSLVPN 访问
- 创建群组 VPN
- 启用 SSL 控制
- 启用网关防病毒服务
- 启用 IPS
- 启用防间谍软件服务
- 启用应用程序控制服务

- 3 单击访客服务。仅启用访客服务选项可用。

The screenshot shows the '访客服务' (Guest Services) configuration page. At the top, there are two tabs: '常规' (General) and '访客服务' (Guest Services), with '访客服务' being the active tab. Below the tabs, the title '访客服务' is displayed. The main content area contains a list of configuration options, each with a checkbox and a '配置' (Configure) button. The options are: '启用访客服务' (Enable Guest Services), '允许访客之间的通信' (Allow communication between guests), '为访客绕过 AV 检测' (Allow guests to bypass AV detection), '对访客绕过客户端内容过滤检查' (Allow guests to bypass client content filtering), '启用外部访客验证' (Enable external guest authentication), '启用捕获入口身份验证' (Enable capture of entry authentication), '启用无验证的策略页面' (Enable strategy page without authentication), '自定义验证页面' (Customize authentication page), '发布验证页面' (Publish authentication page), '绕过访客验证' (Bypass guest authentication), '重定向 SMTP 通讯至' (Redirect SMTP traffic to), '拒绝网络' (Deny network), '通过网络' (Allow network), and '最大访客数' (Maximum number of guests) set to 10.

- 4 单击启用访客服务。所有其他选项将激活，但默认情况下处于未选中状态。
5 从以下用于访客服务的配置选项中进行选择：

允许访客之间的通信	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。
对访客绕过客户端内容过滤检查	允许访客流量绕过客户端 CF 实施。
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。选择此选项将激活其配置按钮。单击配置将显示外部访客身份验证对话框。
启用捕获入口身份验证	注： 选择此选项时，以下四个选项将显示为灰色且不可用。允许您使用 RADIUS 身份验证创建自定义登录页面。选择此选项将激活其配置按钮。单击配置将显示自定义登录页面对话框。
启用无验证的策略页面	当用户首次连接到 SonicPoint 或 SonicWave 时，将用户定向到访客服务使用策略页面。将通过接受策略而不是提供用户名和密码对访客用户进行身份验证。选择此选项将激活其配置按钮。如需设置可自定义的 HTML 策略使用页面，请单击配置。随即显示自定义策略消息对话框。
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。选择此选项将激活其配置按钮。如需设置自定义身份验证页面，请单击配置以显示定制登录页面。

发布验证页面	身份验证成功后，立即将用户重定向到指定页面。选择此选项将激活其字段。在字段中输入验证后页面的 URL。
绕过访客验证	<p>运行访客服务功能集成到已使用某种形式的用户级别身份验证的环境中。此功能可自动完成身份验证过程，使无线用户无需身份验证即可使用不受限制的无线访客服务。选中后此选项的下拉菜单可用，选择：</p> <ul style="list-style-type: none"> • 所有 MAC 地址（默认） • 地址对象 • 地址群组 • 创建新 MAC 对象 - 显示添加地址对象对话框。^a <p>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，或在其他设备上游已强制实施验证的情况下使用。</p>
重定向 SMTP 通讯至	<p>将进入该区域的 SMTP 流量重定向至您所指定的 SMTP 服务器。选中后此选项的下拉菜单可用，选择：</p> <ul style="list-style-type: none"> • 地址对象 • 创建新地址对象 - 显示添加地址对象对话框。^a
拒绝网络	<p>阻止流向您指定的网络的流量。选中后此选项的下拉菜单可用，选择：</p> <ul style="list-style-type: none"> • 地址对象 • 地址对象群组 • 创建新地址对象 a • 创建新地址对象群组 a
通过网络	<p>允许通过启用访客服务的区域的流量自动流向所选网络。选中后此选项的下拉菜单可用，选择：</p> <ul style="list-style-type: none"> • 地址对象 • 地址对象群组 • 创建新地址对象 a • 创建新地址对象群组 a <p>注： 显示添加地址对象对话框。</p>
最大访客数	<p>指定允许连接到此区域的最大访客用户数。最小数为 1，最大数为 4500，默认设置为 10。</p>

a. 如需创建地址对象和地址对象群组的信息，请参阅 SonicOS 策略。

6 单击**确定**，对此区域应用上述设置。

配置用于开放式验证和社交登录的区域

SonicOS 支持开放式验证和社交登录：

- OAuth 可帮助用户在应用程序之间共享数据。
- 社交登录可以简化各种社交媒体的登录过程

如需使用这些功能，请创建区域，如第 619 页的[配置开放式验证、社交登录和 LHM](#) 中所述。

配置 WLAN 区域

- 1 转至**管理 | 系统设置 | 网络 | 区域**。
- 2 如果正在配置：

- 新的区域，单击添加...按钮。
- 现有区域，单击 WLAN 区域的编辑图标。

将显示添加/编辑区域对话框。

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 333 页的添加新区域描述了如何配置常规选选项卡。

- 3 如需自动创建允许流量在区域实例的接口之间流动的服务规则，请选中允许接口信任。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，使这些接口上的主机能相互通信。
- 4 如果无线不可用，请从安全类型中选择无线。
- 5 单击无线选项卡。

- 6 在无线设置部分中，如要求所有进入 WLAN 区域的流量都通过 SonicWall SSL VPN 设备进行身份验证，请选中 **SSL-VPN 增强**。选择此选项将激活以下两个选项。默认情况下未选中该选项。
- 7 从 **SSL-VPN 服务器**中，选择一个地址对象将流量定向到 SonicWall SSL VPN 设备，或创建新的地址对象。如需创建地址对象和地址对象群组的信息，请参阅 SonicOS 策略。
- 8 从 **SSL-VPN 服务**中，选择服务或服务群组，以允许客户端通过 SSL VPN 进行身份验证。
- 9 在 **SonicPoint/SonicWave 设置**部分中，选择要应用于连接到此区域的所有 SonicPoint/SonicWave 的 **SonicPoint/SonicWave 配置文件**。除非使用了不同设置对其进行单独配置，否则只要 SonicPoint/SonicWave 连接到此区域，就会自动使用 SonicPoint/SonicWave 配置文件中的设置对其进行配置。如需 SonicPoint/SonicWave 配置文件的信息，请参阅 SonicOS 连接。

注：对于以下四项设置，也可选中**自动规范**以允许与配置文件相连的 SonicPoint/SonicWave 在配置文件已修改时自动进行配置。默认情况下未选中该选项。

- 10 在您要应用于所有连接到此区域的 SonicPointN/Ni/Ne 时，请选择 **SonicPointN/Ni/Ne** 配置文件。除非单独为 SonicPointN/Ni/Ne 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。默认配置文件为 **SonicPointN**。
- 11 当您想要应用于所有连接到此区域的 SonicPointNDR 时，选择 **SonicPoint NDR** 供应商配置文件。除非单独为 SonicPointNDR 配置了不同的设置，否则任何时候在将 SonicPointNDR 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。默认配置文件为 **SonicPointNDR**。
- 12 在您要应用于所有连接到此区域的 SonicPointACe/ACi/N2 时，请选择 **SonicPoint AC** 配置文件。除非单独为 SonicPointACe/ACi/N2 配置了不同的设置，否则任何时候在将 SonicPointACe/ACi/N2 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。默认配置文件为 **SonicPointACe/ACi/N2**。
- 13 在您要应用于所有连接到此区域的 SonicPointNDR 时，请选择 **SonicWave 432o/e/i** 配置文件。除非单独为 SonicPointNDR 配置了不同的设置，否则任何时候在将 SonicPointNDR 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。默认配置文件为 **SonicWave**。
- 14 选中仅允许 **SonicPoint/SonicPointN** 生成的流量可以仅允许来自 SonicWall SonicPoint 的流量进入 WLAN 区域接口。这令您的 WLAN 拥有最高的安全性。如果想要 WLAN 区域允许任何流量（不管流量是来自无线连接），请清除此选项。
 - i** | 提示：如需使 WLAN 区域允许任何流量（不管流量是来自无线连接），请清除仅允许 **SonicPoint/SonicPointN** 生成的流量。
 - i** | 注：如需访客服务配置信息，请参阅第 335 页的 **配置访客访问的区域**。
- 15 单击确定，对 WLAN 区域应用上述设置。

删除区域

删除用户创建的区域的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | 区域**。
 - i** | 注：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。
- 2 单击区域的配置列中的删除图标。

删除一个或多个用户创建的区域的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | 区域**。
 - i** | 注：对于预定义区域，这些复选框不可用。不能删除这些区域。可以删除您所创建的任何区域。
- 2 选择要删除的区域。
- 3 从删除中，选择要删除的区域：
 - 删除所选组
 - 全部删除

配置有线模式 VLAN 转换

- 第 341 页的[网络 | VLAN 转换](#)
 - 第 341 页的[关于 VLAN 转换](#)
 - 第 342 页的[创建和管理 VLAN 映射](#)

网络 | VLAN 转换

① | 注：所有支持有线模式的平台中都提供 VLAN 转换。

① | 注：不能同时启用“VLAN 转换”和“通过 VLAN 接口的有线模式”。

- 第 341 页的[关于 VLAN 转换](#)
- 第 342 页的[创建和管理 VLAN 映射](#)

关于 VLAN 转换

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 SonicWall 安全设备的流量重选路由，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。

有线模式的一个优点是您可以预先配置 VLAN 映射。这样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 341 页的[映射模式](#)
- 第 342 页的[映射持久性](#)
- 第 342 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 等安全设备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。如果有线模式对（安全模式）具有与它们关联的映射，则除非删除了映射策略，否则无法更改有线模式。

映射多接口对

您可以同时为多对接口创建 VLAN 映射。这些接口必须在创建 VLAN 映射时构成现有安全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的映射才可在任意给定时间使用。

如果配对的接口已更改，则将显示消息当接口的 WireMode VLAN 条目存在时，无法更改有线模式对接口。

示例

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**多接口对映射**中，存在 X12 到 X13（策略 1）以及 X12 到 X15（策略 2）的映射。

由于当前只有 X12 和 X13（策略 1 和 3）以及 X14 和 X15（策略 4 和 6）构成了有线模式对，因此只有策略 1、3、4 和 6 处于活动状态，如活动列中的绿色复选标记所示。

注：对于该接口，如果有线模式 VLAN 条目存在，则线模式对接口无法更改。

创建和管理 VLAN 映射

网络 | VLAN 转换允许您创建和管理接口的 VLAN 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			

“添加”图标	显示添加 VLAN 转换 对话框。
删除图标	显示删除下拉菜单： <ul style="list-style-type: none"> • 删除所选组 • 全部删除
搜索字段	允许您仅显示感兴趣的 VLAN 转换 。
刷新图标	刷新 VLAN 转换表 。
策略编号和复选框	策略数量及其关联的复选框。
入口接口	传入接口的名称。
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	指示映射是单向还是双向： <ul style="list-style-type: none"> • 已禁用 - 单向；列空白。 • 已启用 - 双向；绿色复选标记。
活动	映射对状态： <ul style="list-style-type: none"> • 活动 - 有线模式对已映射并处于活动状态；绿色复选标记。 • 不活动 - 有线模式对已映射但处于不活动状态（预先配置）；列空白。
配置	显示映射对的编辑和删除图标。

主题：

- [第 343 页的创建 VLAN 映射](#)
- [第 347 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 344 页的在安全模式下创建有线模式对](#)
- 2 [第 346 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 转至管理 | 系统设置 | 网络 | 接口。

名称	区域	群组	IP 地址	子网掩码	IP 分配	状态	已启用	备注	配置
X0	LAN		192.168.168.168	255.255.255.0	静态	无链接	<input checked="" type="checkbox"/>	Default LAN	
X1	WAN	Default LB Group	192.168.95.83	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	Default WAN	
X2	LAN		192.168.94.83	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	WXA series appliance	
X2-V402	WLAN		172.16.16.83	255.255.255.0	静态	VLAN 子接口	<input checked="" type="checkbox"/>		
X3	WAN		0.0.0.0	0.0.0.0	PPPoE	1 Gbps 全双工	<input checked="" type="checkbox"/>		
X4	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X5	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X6	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X7	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X8	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X9	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X10	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X11	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X12	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X13	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X14	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X15	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X16	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X17	未分配		0.0.0.0	0.0.0.0	N/A	无链接	<input checked="" type="checkbox"/>		
X18	未分配		0.0.0.0	0.0.0.0	N/A	10 Gbps 全双工	<input checked="" type="checkbox"/>		
X19	未分配		0.0.0.0	0.0.0.0	N/A	10 Gbps 全双工	<input checked="" type="checkbox"/>		
MGMT	MGMT		192.168.1.254	255.255.255.0	静态	1 Gbps 全双工	<input checked="" type="checkbox"/>	Default MGMT	
U0	WAN		0.0.0.0	0.0.0.0	拨号	永久	<input checked="" type="checkbox"/>	Module	

添加接口: --选择接口类型--

显示 PORTSHIELD 接口

接口流量统计

显示所有流量 [清除](#)

名称	收到的单播数据包数	接收的广播数据包数	收到的错误数	接收的字节数	发送的单播数据包数	发送的广播数据包数	发送的错误数	发送的字节数
X0	0	0	0	0	0	14,116	0	903,650
X1	251,931	175,508	0	43,157,401	330,634	169	0	91,774,063
X2	42,090	843,846	0	91,293,930	230,871	14,074	0	18,798,562
X2-V402	8,662	130,788	0	13,990,301	13,648	14,031	0	2,086,203
X3	0	102,756	0	6,576,384	0	7,367	0	279,950
X4	0	0	0	0	0	0	0	0
X5	0	0	0	0	0	0	0	0
X6	0	0	0	0	0	0	0	0
X7	0	0	0	0	0	0	0	0
X8	0	0	0	0	0	0	0	0
X9	0	0	0	0	0	0	0	0
X10	0	0	0	0	0	0	0	0
X11	0	0	0	0	0	0	0	0
X12	0	0	0	0	0	0	0	0
X13	0	0	0	0	0	0	0	0
X14	0	0	0	0	0	0	0	0
X15	0	0	0	0	0	0	0	0
X16	0	0	0	0	0	0	0	0
X17	0	0	0	0	0	0	0	0
X18	0	0	0	0	0	0	0	0
X19	0	0	0	0	0	0	0	0
MGMT	0	0	0	0	0	10	0	974
U0	0	0	0	678,985	0	0	0	301,624

- 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。

常规 高级

接口 'X12' 设置

区域: 未分配

模式 / IP 分配: 未分配

- 3 从区域中，选择有线模式对的区域。这些选项将发生更改。

常规
高级

接口 'X12' 设置

区域: LAN ▼

模式 / IP 分配: 静态 IP 模式 ▼

IP 地址:

子网掩码:

默认网关 (可选):

备注:

管理: HTTPS Ping SNMP SSH

用户登录: HTTP HTTPS

添加规则, 以启用从 HTTP 到 HTTPS 的重定向

- 4 从模式/IP 分配中, 选择有线模式 (2-端口有线)。这些选项将再次发生更改。

常规
高级

接口 'X12' 设置

区域: LAN ▼

模式 / IP 分配: 有线模式 (2-端口有线) ▼

有线模式类型: 旁路 (通过内部交换机/中继) ▼

成对接口: --选择接口-- ▼

配对接口区域: LAN ▼

禁用状态检测

启用链接状态传播

- 5 从有线模式类型中, 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 从配对接口区域中, 选择配对接口的区域。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 264 页的[配置有线和 Tap 模式](#)和第 264 页的[配置有线和 Tap 模式](#)所示。

9 单击确定。网络 | 接口页面已更新。

X10	LAN	192.168.166.1	255.255.255.0	静态	无链接	✓	
X11	LAN			PortShield 到 X10	无链接	✓	
X12	LAN	N/A	N/A	N/A	无链接	✓	无线模式 旁路 - X15
X13	LAN			PortShield 到 X10	无链接	✓	
X14	未分配	0.0.0.0	0.0.0.0	N/A	无链接	✓	
X15	LAN	N/A	N/A	N/A	无链接	✓	无线模式 旁路 - X12

创建 VLAN 映射

创建 VLAN 映射的步骤如下：

1 转至网络 | VLAN 转换。

#	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 单击添加图标。随即显示添加 VLAN 转换对话框。

入口接口：	X3
入口 VLAN：	0
出口接口：	X3
出口 VLAN：	0
<input checked="" type="checkbox"/> 反向转换	

3 选择您期望从入口接口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，请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。

① 注：默认情况下已选中该选项。

- 双向映射，请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。

#	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			 

管理 VLAN 映射

主题：

- 第 347 页的[编辑映射](#)
- 第 347 页的[过滤映射](#)
- 第 347 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

如果您有许多 VLAN 映射，则可仅显示感兴趣的映射，步骤如下：

- 1 在搜索字段中输入接口名称或 VLAN 标签。
- 2 按回车键。

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：

- 1 删除搜索字段中的条件。
- 2 按 Enter 键。

删除映射

删除映射的步骤如下：

- 1 如需删除：
 - 单个映射，步骤如下：
 - 单击配置列中其“删除”图标。

将显示确认消息：

是否确定要删除此 VLAN 转换？

- 单击其选择复选框，然后从删除下拉菜单中选择删除已选。

将显示确认消息：

您确定要删除选择的条目吗？

- 多个映射，通过单击其**选择**复选框，然后从删除下拉菜单中选择**删除已选**。

将显示确认消息：

您确定要删除选择的条目吗？

- 所有映射，通过从**全部删除**下拉菜单中选择**删除已选**。

将显示确认消息：

您要删除所有的条目吗？

2 单击**确定**。

如果策略为双向，则在删除一个方向时两个方向均将删除。

配置 DNS 设置

- 第 349 页的[网络 | DNS](#)
 - 第 351 页的[关于分割 DNS](#)
 - 第 352 页的[管理 DNS 服务器](#)
 - 第 357 页的[DNS 和 IPv6](#)
 - 第 358 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，而非使用不便记忆的数字 IP 地址来识别互联网上的主机。通过[网络 | DNS](#)，您可以在必要时手动配置 DNS 设置。此页面有两个版本，具体取决于您使用的 IP 版本：[IPv6 网络 | DNS](#) 和 [IPv4 网络 | DNS](#)。

IPv6 网络 | DNS

视图 IP 版本: IPv4 IPv6

IPv6 DNS 设置

手动指定 IPv6 DNS 服务器

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

从 WAN 区域动态继承 IPv6 DNS 设置

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

首选 IPv6 DNS 服务器

IPv6 Split DNS

启用分割 DNS 服务器的代理

#	域名	DNS 服务器	本地接口	配置
<input type="checkbox"/> 1	tb20dc3.sonicwall.com	::	X2	<input type="button" value="编辑"/> <input type="button" value="删除"/>

视图 IP 版本: IPv4 IPv6

IPv4 DNS 设置

手动指定 IPv4 DNS 服务器

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

从 WAN 区域动态继承 IPv4 DNS 设置

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

IPv4 Split DNS

启用分割 DNS 服务器的代理

<input type="checkbox"/> #	域名	DNS 服务器	本地接口	配置
无条目				

DNS 绑定攻击预防

启用 DNS 绑定攻击预防

操作:

允许域:

针对 FQDN 的 DNS 绑定

FQDN 对象只缓存来自于被认可服务器的 DNS 回复

DNS 缓存

主题:

- [第 351 页的关于分割 DNS](#)
- [第 352 页的管理 DNS 服务器](#)

关于分割 DNS

分割 DNS 是一项增强功能，它允许用户配置一组服务器并将其关联到给定的域名（可以是通配符）。当 SonicOS 接收到与域名相匹配的查询时，会将此名称传输到指定的 DNS 服务器。[分割 DNS 示例](#)显示了此功能的工作方式：

分割 DNS 示例



- 此拓扑包含两个拥有网络连接的防火墙：
 - 一个防火墙已连接到互联网。
 - 另一个防火墙是连接到公司网络的 VPN 隧道。
- 默认的 DNS 查询将转至公共 ISP DNS 服务器。
- 所有发送到 *.sonicwall.com 的查询将转至位于 VPN 隧道后的 DNS 服务器。

如需查看和配置分割 DNS 条目，请参阅第 353 页的[为分割 DNS 配置特定于域的 DNS 服务器](#)。

通过添加分割 DNS 条目，所有发送到 sonicwall.com 的查询将发送到特定的服务器（请参阅第 353 页的[为分割 DNS 配置特定于域的 DNS 服务器](#)）。

也可以将多个 DNS 服务器配置为处理发送到 sonicwall.com 的查询。

关于每个分区的 DNS 服务器和分割 DNS

无论是否有身份验证分区，通常都需要使用域自己的 DNS 服务器来解析域中设备的名称，而且偶尔也可能需要使用不同的外部 DNS 服务器来解析外部主机名。现在，对于多个身份验证分区，这种情况会加剧，因为这些分区通常需要使用不同的 DNS 服务器来解析不同分区中的主机名。

- 注：**可能会意外需要使用域自己的 DNS 服务器，因为即使在 LDAP 服务器按 IP 地址配置的情况下，LDAP 引用通常也会按 DNS 名称提供引用服务器。
- 需要使用不同的外部 DNS 服务器来解析外部主机名称的示例涉及无法由内部域的 DNS 服务器解析的外部使用云服务。

“分割 DNS”功能由 SonicWall 安全设备直接用于解析域中设备的名称，而无需启用 DNS 代理，包括拥有身份验证分区的多个不相关的域。

在分割 DNS 中配置的 DNS 服务器将直接用于内部域中主机名的 DNS 查找，如下所示：

- 这适用于在安全设备的主 DNS 缓存中具有条目的任何内容：
 - SMTP 服务器
 - Syslog 服务器
 - Web 代理服务器和用户（内部）代理服务器
 - GMS 和 GMS 备用

- POP 服务器
 - RADIUS 身份验证和计费服务器
 - LDAP 服务器
 - SSO/终端服务代理和 RADIUS 计费客户端
- 如果启用了分区并且分区具有一个域或一个父/子域（也称为一个 AD 林）树，则在为分区的顶级域配置了分割 DNS 服务器的情况下，这些分区将复制到内部分区结构中。然后，这些 DNS 服务器用于解析分区中代理、服务器和客户端的名称。
 - 如果启用了分区并且分区配置有多个单独的域（允许出现这种情况但不常见），则不会将任何 DNS 服务器复制到分区结构中，而是依赖于下面描述的机制。
 - 如果禁用了分区、未对分区设置 DNS 服务器或分区的 DNS 服务器用于解析与分区无关的项目，则将通过分割 DNS 提供的 API 为每个请求选择要使用的 DNS 服务器。

管理 DNS 服务器

网络 | DNS 上的选项会发生变化，具体取决于您指定 IPv6 还是 IPv4。两个版本的管理界面页面都有 DNS 设置和分割 DNS 部分，并一起进行描述。

主题：

- [第 352 页的选择 IP 版本](#)
- [第 352 页的指定使用哪些 DNS 服务器](#)
- [第 353 页的为分割 DNS 配置特定于域的 DNS 服务器](#)
- [第 356 页的编辑分割 DNS 条目](#)
- [第 357 页的删除分割 DNS 条目](#)

选择 IP 版本

选择 IP 版本的步骤如下：

- 1 转至网络 | DNS。
- 2 从页面右上方的视图 IP 版本中，选择：
 - IPv4
 - IPv6

网络 | DNS 上的选项会发生变化，具体取决于您指定 IPv6 还是 IPv4。

指定使用哪些 DNS 服务器

无论 IP 版本如何，您都可以指定 SonicOS 选择 DNS 服务器的方式。对于这两种 IP 版本，此方法相同。

IPv4 DNS 设置/IPv6 DNS 设置部分

IPv4 DNS 设置	IPv6 DNS 设置
<input checked="" type="radio"/> 手动指定 IPv4 DNS 服务器	<input type="radio"/> 手动指定 IPv6 DNS 服务器
DNS 服务器 1: <input type="text" value="0.0.0.0"/>	DNS 服务器 1: <input type="text" value="::"/>
DNS 服务器 2: <input type="text" value="0.0.0.0"/>	DNS 服务器 2: <input type="text" value="::"/>
DNS 服务器 3: <input type="text" value="0.0.0.0"/>	DNS 服务器 3: <input type="text" value="::"/>
<input type="radio"/> 从 WAN 区域动态继承 IPv4 DNS 设置	<input checked="" type="radio"/> 从 WAN 区域动态继承 IPv6 DNS 设置
DNS 服务器 1: <input type="text" value="192.168.95.1"/>	DNS 服务器 1: <input type="text" value="::"/>
DNS 服务器 2: <input type="text" value="8.8.8.8"/>	DNS 服务器 2: <input type="text" value="::"/>
DNS 服务器 3: <input type="text" value="0.0.0.0"/>	DNS 服务器 3: <input type="text" value="::"/>
	<input type="checkbox"/> 首选 IPv6 DNS 服务器

指定使用哪些 DNS 服务器的步骤如下：

- 1 转至网络 | DNS。
 - 2 在 IPv4/IPv6 DNS 设置部分中，选择以下项之一：
 - 手动指定 DNS 服务器的步骤如下
 - a) 选中手动指定 IPv4/IPv6 DNS 服务器。
 - b) 在 DNS 服务器字段中最多输入三个 IP 地址。
 - c) 如果使用的是：
 - IPv4，请转至步骤 4。
 - IPv6，请转至步骤 3。
 - 使用为 WAN 区域配置的 DNS 设置的步骤如下：
 - a) 选中从 WAN 区域动态继承 IPv4 DNS 设置。IP 地址将自动填充到 DNS 服务器字段中。
 - b) 转至步骤 4。
 - 3 如需仅使用 IPv6 服务器，请选中首选 IPv6 DNS 服务器。
- 小心：** 仅当已正确配置 IPv6 DNS 服务器后，才选中此选项。
- 4 单击接受以保存您的更改。

为分割 DNS 配置特定于域的 DNS 服务器

可以有选择地配置单独的域特定 DNS 服务器，以与 IPv6 或 IPv4 一起使用。对于这两种 IP 版本，此方法相同。

IPv6 分割 DNS 部分

IPv6 Split DNS



启用分割 DNS 服务器的代理

#	域名	DNS 服务器	本地接口	配置
1	sonicwall	2000::1	X0	 

IPv4 分割 DNS 部分

IPv4 Split DNS

启用分割 DNS 服务器的代理

#	域名	DNS 服务器	本地接口	配置
1	sonicwall	0.0.0.0	X0	 

- 域名 DNS 服务器的名称。
- DNS 服务器 DNS 服务器的 IPv4/IPv6 IP 地址。
注： DNS 服务器的状态显示在网络 | DNS 代理页面上。
- 本地接口 分配给 DNS 服务器的接口。
- 配置 包含每个服务器的编辑和删除图标。

添加域特定的 DNS 服务器并将其关联到指定域名的步骤如下：

① | 重要： 分割 DNS 的最大条目数为 32。如果列表已满，将无法添加新的条目。

- 1 转至网络 | DNS。
- 2 从视图 IP 版本中选择 IP 版本。
- 3 如需启用分割 DNS 服务器的代理，请选中启用分割 DNS 服务器的代理。默认情况下已选中该选项。
- 4 在分割 DNS 表下，单击添加。将显示添加分割 DNS 条目对话框。

② | 提示： 如果选择了 DNS 代理，则它的页面 DNS 代理也会显示在添加分割 DNS 条目对话框中。

IPv6 添加分割 DNS 条目

设置

IPv4 IPv6 两者都

域名:

主要服务器 (v6):

辅助服务器 (v6):

第三服务器 (v6):

本地接口:

IPv4 添加分割 DNS 条目

设置

IPv4 IPv6 两者都

域名:

主要服务器 (v4):

辅助服务器 (v4):

第三服务器 (v4):

本地接口:

IPv6 和 IPv4 添加分割 DNS 条目

设置

IPv4 IPv6 两者都

域名:

主要服务器 (v4):

辅助服务器 (v4):

第三服务器 (v4):

主要服务器 (v6):

辅助服务器 (v6):

第三服务器 (v6):

本地接口:

5 选择 IP 版本:

- IPv4
- IPv6
- 两者都

- 在域名字段中输入域名。此名称可以包含通配符（*；例如 *.sonicwall.com）。
- 如需为此域配置一个或多个 IPv4/IPv6 分割 DNS 服务器，请在相应的字段中输入 IP 地址：
 - 主要服务器 (v4/v6):
 - 辅助服务器 (v4/v6) (可选)
 - 第三服务器 (v4/v6) (可选)
- 从本地接口中选择一个接口。
- 如果尚未启用 DNS 代理，请转至 [步骤 13](#)。
- 单击 DNS 代理。



- 如需指定生存时间，请选中手动设置 DNS 回复中的 TTL 值。
- 输入缓存条目存在的最长时间。
- 单击确定。

提示： DNS 服务器显示在两个 IP 版本的分割 DNS 表中，而与配置 IP 版本时选择哪个 IP 版本无关。

编辑分割 DNS 条目

编辑分割 DNS 条目的步骤如下。

- 转至网络 | DNS。
- 在分割 DNS 表中，单击条目的编辑图标。将显示编辑分割 DNS 条目对话框。



- 做出更改。
- 单击确定。

删除分割 DNS 条目

删除分割 DNS 条目的步骤如下：

- 1 单击条目的删除图标。

删除两个或两个以上分割 DNS 条目的步骤如下：

- 1 选中要删除的条目的复选框。删除按钮将激活。
- 2 单击删除按钮。

删除所有分割 DNS 条目的步骤如下：

- 1 单击全部删除按钮。

DNS 和 IPv6

如需 SonicOS 的 IPv6 实施的完整信息，请参阅第 762 页的 IPv6。

视图 IP 版本: IPv4 IPv6

IPv6 DNS 设置

手动指定 IPv6 DNS 服务器

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

从 WAN 区域动态继承 IPv6 DNS 设置

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

首选 IPv6 DNS 服务器

IPv6 Split DNS

启用分割 DNS 服务器的代理

<input type="checkbox"/>	#	域名	DNS 服务器	本地接口	配置
<input type="checkbox"/>	1	tb20dc3.sonicwall.com	::	X2	 

IPv6 网络 | DNS 页面包含以下部分：

- 版本选择：请参阅第 352 页的 [选择 IP 版本](#)
- IPv6 DNS 设置：请参阅第 352 页的 [指定使用哪些 DNS 服务器](#)
- IPv6 分割 DNS：请参阅第 353 页的 [为分割 DNS 配置特定于域的 DNS 服务器](#)

DNS 和 IPv4

视图 IP 版本: IPv4 IPv6

IPv4 DNS 设置

手动指定 IPv4 DNS 服务器

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

从 WAN 区域动态继承 IPv4 DNS 设置

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

IPv4 Split DNS

启用分割 DNS 服务器的代理

#	域名	DNS 服务器	本地接口	配置
无条目				

DNS 绑定攻击预防

启用 DNS 绑定攻击预防

操作:

允许域:

针对 FQDN 的 DNS 绑定

FQDN 对象只缓存来自于被认可服务器的 DNS 回复

DNS 缓存

IPv4 网络 | DNS 页面包含以下部分:

- 版本选择: 请参阅第 352 页的[选择 IP 版本](#)
- IPv4 DNS 设置: 请参阅第 352 页的[指定使用哪些 DNS 服务器](#)
- IPv4 分割 DNS: 请参阅第 353 页的[为分割 DNS 配置特定于域的 DNS 服务器](#)
- 第 359 页的[DNS 绑定攻击预防](#)

- 第 359 页的[针对 FQDN 的 DNS 绑定](#)
- 第 360 页的[DNS 缓存](#)

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（请参阅“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生存时间 (TTL) 参数作出响应，这可以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有效的 DNS 答复中的地址，该脚本能扫描网络和执行其他恶意活动。

启用 DNS 重绑攻击保护的步骤如下：

- 1 转至网络 | DNS。
- 2 滚动到 DNS 重新绑定攻击预防部分。



- 3 选中启用 DNS 绑定攻击预防。默认情况下未选中该选项。这两个选项将激活。
- 4 在操作中，选择在检测到 DNS 重绑攻击时执行的操作：
 - 日志攻击（默认）
 - 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
- 5 从允许域中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[创建 FQDN 地址对象组...](#)创建新的 FQDN 地址对象或 FQDN 地址对象组。
- 6 单击接受。

针对 FQDN 的 DNS 绑定

为 FQDN 的 DNS 绑定启用的步骤如下：

- 1 转至网络 | DNS。
- 2 滚动到针对 FQDN 的 DNS 绑定部分。

针对 FQDN 的 DNS 绑定

FQDN 对象只缓存来自于被认可服务器的 DNS 回复

- 3 选中 **FQDN** 对象只缓存来自于被认可服务器的 **DNS** 回复。默认情况下未选中该选项。
- 4 单击接受。

DNS 缓存

如需显示常规 DNS 缓存内容，请单击**显示 DNS 缓存**按钮。弹出窗口显示缓存内容：

The screenshot shows a configuration window titled '针对 FQDN 的 DNS 绑定'. It contains a checkbox for 'FQDN 对象只缓存来自于被认可服务器的 DNS 回复'. Below this is a table titled '常规 DNS 缓存' with columns: What, DNS 名称, IP 地址, TTL (秒), and a '清除' (Clear) button. The table contains one entry for 'syslog server' with IP '192.168.168.66' and TTL '-1'. A '显示 DNS 缓存' button is located below the table.

What	DNS 名称	IP 地址	TTL (秒)	清除
syslog server	192.168.168.66	192.168.168.66	-1	清除

What DNS 服务器名称

DNS 名称 服务器的 IP 地址

IP 地址 IPv4 地址

TTL (秒) 生存时间

清除 单击此按钮可以清除服务器的 DNS 缓存条目。

全部清除 单击此选项将清空所有列出的服务器的所有 DNS 缓存条目。

配置 DNS 代理设置

- 第 362 页的[网络 > DNS 代理](#)
 - 第 363 页的[关于 DNS 代理](#)
 - 第 365 页的[启用 DNS 代理](#)
 - 第 367 页的[配置 DNS 代理设置](#)
 - 第 367 页的[监控 DNS 服务器状态](#)
 - 第 368 页的[监控分割 DNS 服务器状态](#)
 - 第 369 页的[查看和管理静态 DNS 缓存条目](#)
 - 第 370 页的[查看 DNS 代理缓存条目](#)

网络 > DNS 代理

设置

启用 DNS 代理

DNS 代理设置

DNS 代理模式: IPv4 到 IPv4 IPv4 到 IPv6

为所有 DNS 请求实施 DNS 代理

启用 DNS 代理缓存

DNS 服务器状态

i 如需配置 DNS 服务器, 请转至 [网络 > DNS](#)。

DNS 服务器 1: 192.168.95.1

DNS 服务器 2: 8.8.8.8

DNS 服务器 3: 0.0.0.0

分割 DNS

i 如需配置分割 DNS 服务器, 请转至 [网络 > DNS](#)。

分割 DNS 域名 1: sonicwall 2000::1

静态 DNS 代理缓存条目

项目 0 至 0 (0)

添加 删除 全部删除

#	域名	IPv4 地址 1	IPv4 地址 2	IPv6 地址 1	IPv6 地址 2	配置
无条目						

添加 删除 全部删除

DNS 代理缓存

项目 0 至 0 (0)

视图 IP 版本: IPv4 IPv6

清除 全部清空

#	域名	类型	IP 地址	生存时间	清除
无条目					

清除 全部清空

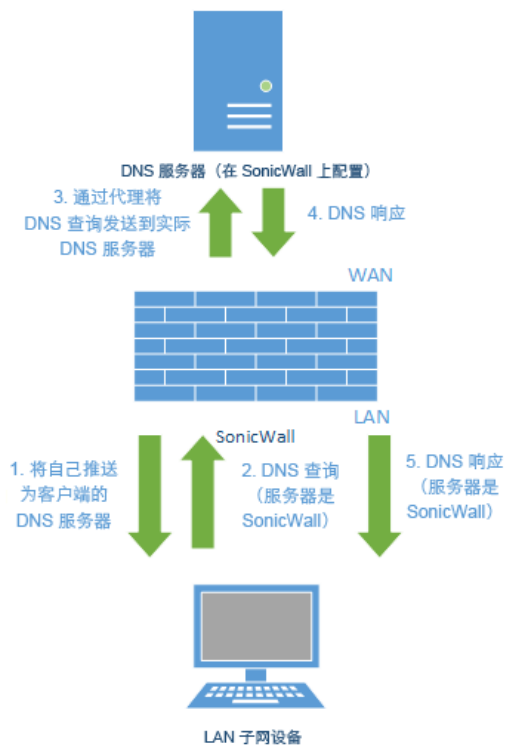
主题:

- [第 363 页的关于 DNS 代理](#)
- [第 365 页的启用 DNS 代理](#)
- [第 367 页的配置 DNS 代理设置](#)
- [第 367 页的监控 DNS 服务器状态](#)
- [第 368 页的监控分割 DNS 服务器状态](#)
- [第 370 页的查看 DNS 代理缓存条目](#)
- [第 369 页的查看和管理静态 DNS 缓存条目](#)

关于 DNS 代理

IPv4 接口可以在 IPv4 互联网上进行名称解析，而 IPv6 接口只能通过 DNS 代理在 IPv6 互联网上进行名称解析。为了允许 IPv4 客户端访问混合有 IPv4 和 IPv6 接口的网络中的 DNS 服务，SonicOS 支持 DNS 代理；请参阅 [DNS 代理](#)。

DNS 代理



DNS 代理功能提供了一种透明机制，设备可以通过该机制代表客户端代理主机名解析请求。代理可以使用现有的 DNS 缓存直接对查询做出响应，该缓存由用户以静态方式配置或以动态方式学习。

代理可以根据部分或完整的域规范有选择地将 DNS 查询重定向到特定的 DNS 服务器。当 VPN 隧道或 PPPoE 虚拟链接提供多种网络连接，并必须将一些 DNS 查询定向到一个网络，而将其他查询定向到另一网络时，此功能非常有用。

借助 DNS 代理，LAN 子网设备使用 SonicWall 安全设备作为 DNS 服务器，并将 DNS 查询发送到安全设备。该安全设备会通过代理将 DNS 查询发送到实际 DNS 服务器。在这种方式下，安全设备成为网络 DNS 流量的集中管理点，并提供在单个点管理网络的 DNS 查询的功能。

注： 为了保持安全，只有在访问规则和 DPI 检查后，才会通过代理发送流入 DNS 查询。

在接口上启用 DNS 代理后，SonicOS 会自动添加一条“允许规则”。如需了解与接口关联的访问规则，请参阅 [SonicOS 策略](#)。

当启用 TCP 上的 DNS 代理后，会自动添加另一个“允许规则”。

主题：

- [第 364 页的支持的接口](#)
- [第 364 页的 DNS 服务器活动检测和故障切换](#)

- [第 364 页的 DNS 缓存](#)
- [第 365 页的 DHCP 服务器](#)
- [第 365 页的启用日志设置](#)
- [第 365 页的监控数据包](#)

支持的接口

支持物理接口、VLAN 接口或 VLAN Trunk 接口上的 DNS 代理功能。每个接口的区域只能为 LAN、DMZ 或 WLAN。

DNS 服务器活动检测和故障切换

配置了多个 DNS 服务器后，SonicOS 会考虑下列因素以确定“最佳”服务器：

- DNS 服务器优先级。
- DNS 服务器状态（正常、故障、未知）。
- 故障切换后的持续时间。

DNS 缓存

在 DNS 代理中，DNS 缓存内存将保存最常用的域和主机地址，并在它接收到与 DNS 缓存中的域相匹配的 DNS 查询时，安全设备会使用缓存记录直接对客户端做出响应，而无需处理 DNS 查询且回复代理。

有两种 DNS 缓存：

静态 由用户手动配置。

动态 由 SonicOS 自动学习。对于每个 DNS 查询，SonicOS DNS 代理会对 URI 执行深层检查，并记录对缓存的有效响应。

当 DNS 查询与现有缓存条目相匹配时，SonicOS DNS 代理会直接使用缓存的 URI 做出响应。这通常会减少网络流量，并因此提高整体网络性能。

最大 DNS 代理缓存大小

静态 DNS 代理缓存大小

静态 DNS 缓存条目的大小始终为 256，而与平台无关。除非手动删除静态 DNS 缓存，否则永远不会将其删除。

动态 DNS 代理缓存大小

动态 DNS 代理缓存大小取决于平台，如[动态缓存大小](#)表中所示。

动态缓存大小

平台	最大缓存大小
SM 9600/SM 9400	4096
SM 9200	2048

动态缓存大小

平台	最大缓存大小
NSA 6600/NSA 5600/NSA 4600	2048
NSA 3600/NSA 2600/NSA 2650	1024
TZ600	512
TZ500/TZ500 W/TZ400/TZ400 W/ TZ300/TZ300 W	512
SOHO W	512

如果在安全设备尝试将条目添加到代理缓存中时已达到最大 DNS 代理缓存大小，则安全设备：

- 1 删除到期时间最早的 DNS 代理缓存条目。
- 2 添加新的 DNS 代理缓存条目。

DNS 缓存的高可用性状态同步

DNS 代理支持 DNS 代理缓存的状态同步。在动态添加、删除或更新 DNS 代理缓存时，它将同步到闲置安全设备。

DHCP 服务器

在接口上启用 DNS 代理时，设备需要将接口 IP 作为 DNS 服务器地址推送到客户端，因此必须手动配置 DHCP 服务器，并在 **DNS/WINS** 选项卡上将接口地址用作 **DHCP 服务器** 设置中的 **DNS 服务器 1** 地址。**动态范围配置** 对话框中的 **接口预绑定** 选项使这一步骤变得更易配置；如果所选接口已启用 DNS 代理，DNS 服务器 IP 将自动添加到 **DNS/WINS** 页面中。如需了解以静态方式配置 DHCP 服务器的方法，请参阅第 451 页的 **配置静态 DHCP 条目**。

启用日志设置

一些事件日志与 DNS 代理相关，并需要按照 SonicOS 调查中所述进行配置。

监控数据包

DNS 代理过程使用“公告板 > 数据包监控”进行监控。如需数据包监控的信息，请参阅 SonicOS 调查。

启用 DNS 代理



必须先**网络 > DNS 代理**页面上全局启用 DNS 代理，然后再在每个接口上进行启用。这实现了对不同网段单独启用此功能的逐步控制

启用 DNS 代理的步骤如下：

- 1 转至网络 | DNS 代理。
- 2 选中启用 DNS 代理。默认情况下未选中该选项。
- 3 单击接受。
- 4 转至网络 | 接口。
- 5 单击要启用 DNS 代理的接口的编辑图标。将显示编辑接口对话框。
- 6 单击高级。

高级设置

链接速度: 1 Gbps - 全双工

使用默认 MAC 地址: C0:EA:E4:59:8E:2C

覆盖默认 MAC 地址:

关闭端口

启用流量报告

启用组播支持

启用 802.1p 标记

从路由通知中排除 (NSM, OSPF, BGP, RIP)

启用非对称路由支持

冗余/聚合端口: 无

接口 MTU: 1500

- 7 选中启用 DNS 代理。只有在全局启用了 DNS 代理时，才会显示此选项。
- 8 单击确定。
- 9 对每个要启用 DNS 代理的接口重复步骤 5 到步骤 8。
- 10 单击接受。

如需了解与接口关联的访问规则，请参阅 SonicOS 策略指南。

配置 DNS 代理设置

配置 DNS 的步骤如下：

- 1 转至网络 | DNS 代理 | DNS 代理设置。



- 2 从 DNS 代理模式中，选择用于在安全设备和 DNS 服务器之间发送/接收 DNS 代理数据包的 IP 版本：
 - IPv4 到 IPv4（默认）
 - IPv4 到 IPv6
- 3 如需允许所有类型的 DNS 请求（包括由 SonicOS 发送的堆栈 DNS 数据包）由 DNS 代理处理，包括使用外部 DNS 服务器的目标地址转发 DNS 查询，请选择为所有 DNS 请求强制执行 DNS 代理。如果禁用此选项，则只处理发送到 SonicWall 安全设备的请求。默认情况下未选中该选项。

注： 此选项仅影响 UDP 上的 DNS。如果未选择此选项，则仅启用发送到 SonicWall 安全设备的 DNS 代理请求。
- 4 仅对 UDP 上的 DNS 请求，选择启用 DNS 代理缓存。默认情况下已选中该选项。
- 5 单击接受。

注： 有多项可以配置的高级设置，例如 DNS 代理协议。如需这些设置的更多信息，请联系技术支持。

监控 DNS 服务器状态



注： 对于已配置的 DNS 服务器，显示其 IP 地址。如果未配置某个服务器，IP 地址为 0.0.0.0。如需配置服务器，请单击指向网络 > DNS 的链接；请参阅第 349 页的 [配置 DNS 设置](#)。

可以在 DNS 服务器状态部分中监控每个已配置的上游 DNS 服务器的状态。服务器状态由来自服务器的 DNS 回复决定：

- | | |
|------------|--|
| 向上（绿色 LED） | 回复成功。 |
| 未知（黄色 LED） | 服务器未接收 DNS 回复。 |
| 向下（红色 LED） | 失败计数超过了限制次数 20。在下一成功 DNS 查询之前，状态仍然为“故障”。 |

将鼠标指针悬停在 LED 上可以显示一个弹出窗口，其中包含有关已发送的代理 DNS 数据包的数量及成功 DNS 代理程序查询的数量的更多信息：



监控分割 DNS 服务器状态

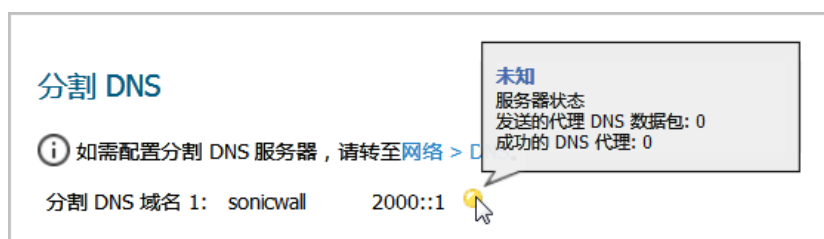


i 注：对于已配置的分割 DNS 服务器，显示其 IP 地址。如需配置分割服务器，请单击指向 [网络 > DNS](#) 的链接；请参阅第 349 页的 [配置 DNS 设置](#)。

可以在分割 DNS 部分中监控每个已配置的上游 DNS 服务器的状态。服务器状态由来自服务器的 DNS 回复决定：

- | | |
|------------|---|
| 向上（绿色 LED） | 回复成功。 |
| 未知（黄色 LED） | 服务器未接收 DNS 回复。 |
| 向下（红色 LED） | 失败计数超过了限制次数 20。在下次成功的 DNS 查询之前，状态仍然为“故障”。 |

将鼠标指针悬停在 LED 上可以显示一个弹出窗口，其中包含有关已发送的代理 DNS 数据包的数量及成功 DNS 代理程序查询的数量的更多信息：



查看和管理静态 DNS 缓存条目

静态 DNS 代理缓存条目							项目 1 至 1 (/ 1)
#	域名	IPv4 地址 1	IPv4 地址 2	IPv6 地址 1	IPv6 地址 2	配置	
1	sample	10.208.28.12	10.208.28.21	::	::	 	

- 域名** 域的名称。
- IPv4 地址 1** 静态 DNA 缓存的主要 IPv4 地址。0.0.0.0（如果未指定）。
- IPv4 地址 2** 静态 DNA 缓存的次要 IPv4 地址。0.0.0.0（如果未指定）。
- IPv6 地址 1** 静态 DNA 缓存的主要 IPv6 地址。::（如果未指定）。
- IPv6 地址 2** 静态 DNA 缓存的次要 IPv6 地址。::（如果未指定）。
- 配置** 包含每个条目的编辑和删除图标。

添加静态 DNS 缓存条目的步骤如下：

- 1 转至网络 | DNS 代理。
- 2 滚动到静态 DNS 代理缓存条目。
- 3 单击表上方或下方的添加按钮。将显示添加静态 DNS 缓存对话框。

域名:	<input type="text"/>
IPv4 地址 1:	<input type="text"/>
IPv4 地址 2:	<input type="text"/>
IPv6 地址 1:	<input type="text"/>
IPv6 地址 2:	<input type="text"/>

- 4 在域名字段中输入名称。
- 5 对于 IPv4 静态 DNS 缓存，请在 IPv4 地址 1 字段中输入主要 IPv4 地址。
- 6 （可选）对于 IPv4 静态 DNS 缓存，请在 IPv4 地址 2 字段中输入次要 IPv4 地址。
- 7 对于 IPv6 静态 DNS 缓存，请在 IPv6 地址 1 字段中输入主要 IPv6 地址。
- 8 （可选）对于 IPv6 静态 DNS 缓存，请在 IPv6 地址 2 字段中输入次要 IPv6 地址。
- 9 单击确定。
- 10 如需添加另一个静态 DNS 缓存条目，请重复步骤 4 到步骤 9。
- 11 单击取消。

删除静态 DNS 缓存条目

删除静态 DNS 缓存条目的步骤如下：

- 1 单击条目的删除图标。

删除两个或两个以上静态 DNS 缓存条目的步骤如下：

- 1 选中要删除的条目的复选框。删除按钮将激活。
- 2 单击删除按钮。

删除所有静态 DNS 缓存条目的步骤如下：

- 1 单击全部删除按钮。

查看 DNS 代理缓存条目



视图 IP 版本

选择 IPv4 或 IPv6。

域名

DNS 服务器的名称。

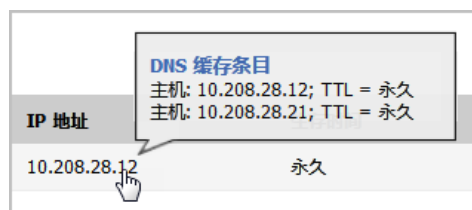
类型

动态

静态

IP 地址

DNS 服务器的 IPv4 或 IPv6 地址。将鼠标指针悬停在某个条目上可以显示该条目的主机和生存时间 (TTL) 信息：



生存时间

您可以

- 在 n 分 x 秒内过期（动态 DNS）
- 已过期（动态 DNS）
- 永久（静态 DNS）

清除

每个条目的清除图标。

在 DNS 代理过程中，系统将自动添加动态 DNS 缓存；在用户配置了静态 DNS 缓存后，将会添加该缓存。动态 DNS 缓存包含 TTL 值且可以进行清除。必须删除静态 DNS 缓存；请参阅第 370 页的[删除静态 DNS 缓存条目](#)

清除动态 DNS 缓存条目

清除动态 DNS 缓存条目的步骤如下：

- 1 单击条目的清除图标。

清除两个或两个以上动态 DNS 缓存条目的步骤如下：

- 1 选中要删除的条目的复选框。清除按钮将激活。
- 2 单击清空按钮。

清除所有动态 DNS 缓存条目的步骤如下：

- 1 单击全部清空按钮。

配置路由通告和路由策略

- 第 372 页的[关于路由](#)
 - 第 373 页的[关于度量和和管理距离](#)
 - 第 374 页的[路由通告](#)
 - 第 374 页的[ECMP 路由](#)
 - 第 375 页的[基于策略的路由](#)
 - 第 375 页的[基于策略的 TOS 路由](#)
 - 第 376 页的[基于 PBR 度量值的优先级](#)
 - 第 377 页的[基于策略的路由和 IPv6](#)
 - 第 377 页的[OSPF 和 RIP 高级路由服务](#)
 - 第 384 页的[丢弃隧道接口](#)
- 第 384 页的[网络 | 路由](#)
 - 第 384 页的[网络 | 路由 > 设置](#)
 - 第 386 页的[网络 | 路由 > 路由通告](#)
 - 第 387 页的[网络 | 路由 > OSPFv2](#)
 - 第 388 页的[网络 | 路由 > RIP](#)
 - 第 389 页的[网络 | 路由 > OSPFv3](#)
 - 第 391 页的[网络 | 路由 > RIPng](#)
- 第 392 页的[配置路由](#)
 - 第 392 页的[按度量值设置路由的优先级](#)
 - 第 393 页的[为通过路由公告学习的默认路由配置度量值](#)
 - 第 393 页的[配置路由通告](#)
 - 第 394 页的[配置静态和基于策略的路由](#)
 - 第 397 页的[为丢弃隧道接口配置静态路由](#)
 - 第 399 页的[配置 OSPF 和 RIP 高级路由服务](#)
 - 第 408 页的[配置 BGP 高级路由](#)

关于路由

SonicWall 安全设备支持这些路由协议：

- RIPv1（路由信息协议）
- RIPv2
- OSPFv2（开放最短路径优先）
- OSPFv3
- PBR（基于策略的路由）

主题：

- 第 373 页的[关于度量和](#)[管理距离](#)
- 第 374 页的[路由通告](#)
- 第 374 页的[ECMP 路由](#)
- 第 375 页的[基于策略的 TOS 路由](#)
- 第 376 页的[基于 PBR 度量值的优先级](#)
- 第 377 页的[基于策略的路由和 IPv6](#)
- 第 377 页的[OSPF 和 RIP 高级路由服务](#)
- 第 377 页的[基于策略的路由和 IPv6](#)

关于度量和

度量和

关于指标

度量是分配给静态和动态路由的加权成本。度量确定了几个路由中的最佳路由，通常是度量值最低的网关。此网关通常是默认网关。

度量值介于 1 和 254 之间；见[度量值描述](#)表。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。

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
200	内部 BGP

关于管理距离

管理距离（管理距离）是影响应该将哪个路由源用于来自不同源的两条相同路由的值。管理距离值越小，路由越可信。

设置管理距离时，它仅由 ZebOS 组件在选择路由时使用：

- 填充到 PBR
- 当静态路由与从特定路由协议接收到的路由竞争时，重新分配至其他路由协议。

管理距离不用于设置 PBR 自身内的路由的优先级，因此除非动态路由正在使用中，否则为静态路由设置的管理距离不起作用。要使用动态路由时，管理距离提供了一种机制，通过该机制可以将 PBR 中定义的静态路由与可能从 OSPF、RIP 或 BGP 等协议接收的其他等效动态路由进行比较。默认情况下，插入网络服务模块 (NSM) 中的 PBR 静态路由的管理距离等于为 PBR 路由定义的度量值。为管理距离输入自定义值后，每个静态路由的管理距离可以选择性地设置为不同值。

例如，如果定义了度量值为 10 且管理距离设置为其默认值自动的简单（仅限目的地）静态路由（例如，目的地 = 14.1.1.0/24），则该路由将填充到管理距离和度量值为 10 的 NSM 中。

现在，假设从 RIP 和 OSPF 收到同一 14.1.1.0/24 路由。RIP 路由的默认管理距离为 120，而 OSPF 路由的默认管理距离为 110，因此默认管理距离（== 度量值）为 10 的静态路由将优于这两条路由，而且 NSM 不会将 OSPF 或 RIP 路由填充到 PBR 中。但是，如果将静态路由的管理距离设置为 115（度量值仍为 10），则 OSPF 路由（在 110 处）将优于静态路由，但 RIP 路由不优于静态路由。如果 OSPF 路由消失，则 NSM 将撤销 OSPF 路由且不会填充 RIP 路由，因为它的 120 AD 大于静态路由的 115 AD。

在上述任何一种情况下，静态路由在 PBR 中仍然是首选，因为从 NSM 填充到 PBR 中的所有非默认路由都会添加度量值 110，该度量值大于静态路由的度量值 10。

如果管理距离为 110 且大于 110 的度量值用于静态路由，则当它将静态路由的度量值与任何竞争 OSPF 路由的 OSPF 度量值（或成本）进行比较时，OSPF 将使用传递给 NSM 的度量值。

路由通告

SonicWall 安全设备使用 RIPv1 或 RIPv2 向网络中的其他路由器通告其静态和动态路由。安全设备与远程 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。请根据路由器的功能或配置在以下选项中进行选择：

- RIPv1，它是该协议的较早版本，包含的功能较少且通过广播而非组播发送数据包。
- RIPv2，它是该协议的更高版本，在将路由表组播到相邻路由器以及路由标签以用于学习路由时包含子网信息。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）”选项对数据包进行广播而非组播，适用于混合了 RIPv1 和 RIPv2 路由器的异构网络。

ECMP 路由

SonicOS 6.5 支持等成本多路径 (ECMP) 路由，这是一种用于沿着相同成本的多条路径路由数据包的技术。转发引擎通过下一跳标识路径。在转发数据包时，路由器必须决定要使用哪个下一跳（路径）。多路径路由可以与大多数路由协议一起使用。

在 SonicOS 中，您可以使用 ECMP 路由为给定路由的目的地指定多个下一跳。在有实质要求的环境中，这样做有几个原因。大多数时候路由器只能使用一个 ISP，当第一个 ISP 出于某种原因失败时，可以切换到另一个 ISP。多路径的另一个应用是保持路径备用，并只有在带宽要求超过预定义阈值时才启用它。SonicOS 最多支持四个下一跳路径。

各种路由协议（包括开放最短路径优先 (OSPF) 和中间系统到中间系统 (ISIS)）明确允许 ECMP 路由。一些路由器实现也允许将同等成本的多路径与 RIP 和其他路由协议一起使用。

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。

FQDN 不能用作 PBR 条目的来源或目的地。

基于策略的 TOS 路由

当通过服务类型 (TOS) 和 TOS 掩码值定义基于策略的路由 (PBR) 策略时，SonicOS 支持基于策略的 TOS（服务类型）路由。定义后，在查找路由匹配时，会将 TOS 和掩码值与 IP 标头中关联 IP 数据包的 TOS/DSCP 字段进行比较。

将 TOS 值与 IP 数据包标头中的 8 位字段进行比较（如需此标头的信息，请参阅 [RFC 2474](#)，[差异化服务](#)和 [RFC 2168](#)，[显式拥塞通知](#)）。TOS 值可用于定义与定量性能要求（例如，峰值带宽）相关的服务和基于相对性能（例如，类别区分）的服务。

TOS 路由与现有的 SonicOS QoS 标记不同，它不会影响数据包的路由，也无法根据进站数据包的 TOS 字段以不同方式转发数据包。TOS 路由通过允许策略路由定义 TOS 值/TOS 掩码对以与差分转发的进站数据包进行比较来提供此功能。TOS 路由仅在数据包进入安全设备时适用于这些数据包。

通过 TOS 路由，可以定义多个具有相同源 IP、目标 IP 和服务值但不同 TOS/TOS 掩码值的策略路由。这允许根据进站数据包中 TOS 字段的值以不同方式转发包含已标记 TOS 字段的数据包。

SonicOS 6.5 之前定义的任何 PBR 策略路由都未对 TOS/TOS 掩码定义任何值。同样，TOS/TOS 掩码字段的默认值为零（未定义任何值）。

TOS 值不等于零的策略路由的优先级高于所有简单的仅目的地路由，但低于任何定义源或服务的策略路由。比较两个 TOS 策略路由，并假设两者定义或未定义同一组源、目的地和服务值时，拥有更多设置为 1 的 TOS 掩码比特的 TOS 路由优先于设置了更少 TOS 掩码位的 TOS 路由。

PBR 路由的一般优先级（高到低）如下，基于定义为任何以外的任何值的策略字段或对 TOS 定义为零的策略字段：

目标、源、服务、TOS

目标、源、服务

目标、源、TOS

目标、源

目标、服务、TOS

目标、服务

目标、TOS

目标

源、服务、TOS

源、服务
源、TOS
源
服务、TOS
服务
TOS

基于 PBR 度量值的优先级

SonicOS 支持为基于策略的路由 (PBR) 向路由策略分配度量值加权成本，此路由允许已配置的度量值在路由优先级上高于默认情况下使用的路由特性。度量值介于 0 到 255 之间。度量值越低越好且低度量值优先于高度量值。

PBR 路由的一般优先级（高到低）如下，基于定义为任何以外的任何值的策略字段或对 TOS 定义为零的策略字段：

目标、源、服务、TOS
目标、源、服务
目标、源、TOS
目标、源
目标、服务、TOS
目标、服务
目标、TOS
目标
源、服务、TOS
源、服务
源、TOS
源
服务、TOS
服务
TOS

在这 15 个分类内，将根据所定义路由条目的累计特定性进一步设置路由的优先级。对于源和目标字段，将通过统计以地址对象表示的 IP 地址的数量来评估特定性。例如，网络地址对象 10.0.0.0/24 包含 256 个 IP 地址，而网络地址对象 10.0.0.0/20 表示 4096 个 IP 地址。较长的 /24（24 位）网络前缀表示较少的主机 IP 地址，因此更加具体。

新的度量值加权选项允许已配置的度量值优先于路由特定性。启用该选项后，优先级排序中使用的优先级如下（高到低）：

- 1 路由类（由源、目的地、服务和值不是“任何”或值为零的 TOS 字段的组合确定）
- 2 度量的值
- 3 源、目标、服务和 TOS 字段的累计特定性

基于策略的路由和 IPv6

如需 SonicOS 的 IPv6 实施的完整信息，请参阅第 762 页的 [IPv6](#)。

通过在 [网络 | 路由](#) 上为路由策略选择 IPv6 地址对象和网关，IPv6 完全支持基于策略的路由。您可以在 [IPv4](#) 和 [IPv6](#) 之间的 [路由策略表](#) 中切换条目。

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。

如需路由通告的信息，请参阅第 374 页的 [路由通告](#)。如需设置路由策略的信息，请参阅第 374 页的 [路由通告](#)。

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，但网络规模并非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。[路由信息协议区别表](#) 说明了 RIPv1、RIPv2 和 OSPFv2/OSPFv3 之间的主要区别：

路由信息协议区别

	RIPv1	RIPv2	OSPFv2/OSPFv3
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

主题：

- 第 377 页的 [关于路由服务](#)
- 第 380 页的 [OSPF 术语](#)

关于路由服务

主题：

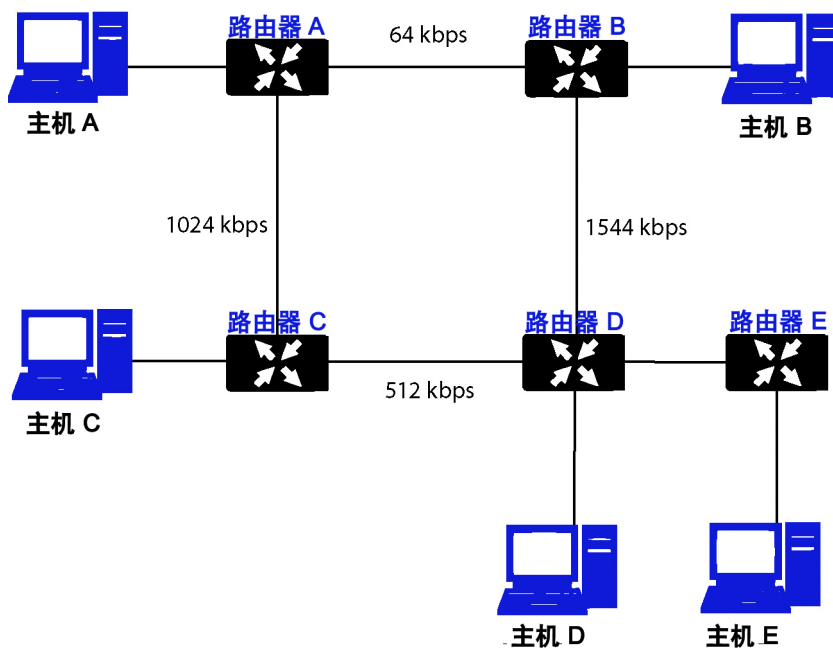
- 第 378 页的 [协议类型](#)
- 第 378 页的 [最大跃点数](#)
- 第 379 页的 [水平分割](#)

- 第 379 页的毒性逆转
- 第 379 页的路由表更新
- 第 379 页的支持的子网大小
- 第 380 页的自治系统拓扑

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**决定最低成本路由的示例网络**中显示的示例网络：

决定最低成本路由的示例网络



在**决定最低成本路由的示例网络**中显示的示例网络中，使用 RIP 时，如果主机 A 要访问主机 B，费用最低的路是从路由器 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**决定最低成本路由的示例网络**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未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，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：

- 第 379 页的[水平分割](#)
- 第 379 页的[毒性逆转](#)
- 第 379 页的[路由表更新](#)
- 第 379 页的[支持的子网大小](#)
- 第 380 页的[自治系统拓扑](#)

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，且支持的跃点数并无限制。

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） |
| | <ul style="list-style-type: none">• 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，每个有 16,777,214 个主机 |
| 类 B | 192.0.0.0 至 223.255.255.0 |
| | <ul style="list-style-type: none">• 最左边位 10；14 个网络位；16 个主机位• 10nnnnnnn nnnnnnnn hhhhhhhh hhhhhhhh（16 位分类子网掩码）• 16,384 个 B 类网络，每个有 65,532 个主机 |
| 类 C | 192.0.0.0 至 223.255.255.0 |
| | <ul style="list-style-type: none">• 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)。如需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: $2^{16}=65,536$ 。您可以获得 65,536 个网络,其中每个网络拥有 254 个可用主机,而非获得一个拥有 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。区域 ID 是管理标识符。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 不会变得过大导致无法管理,或变得计算过于密集导致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。**不同接口的成本计算**表中显示了一些常见的路径成本。

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

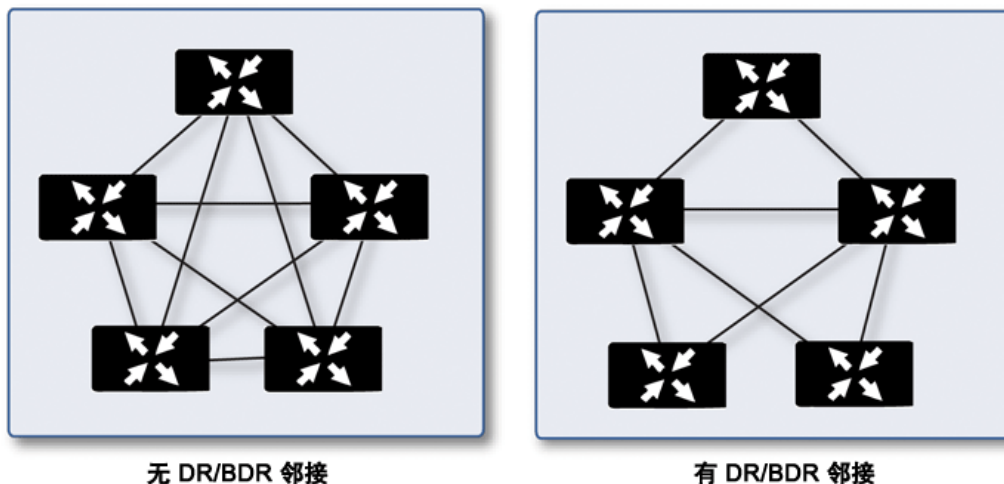
不同接口的成本计算

接口	除以 10^8 (100 兆位) = OSPF 成本
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（请参阅上文的邻居）。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（参阅下文的“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，而非网段上的每个可能的路由器配对组合之间交换 LSA；请参阅**路由邻接：指定的路由 (DR)**。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“OSPF 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“OSPF 所有路由器”将接收 LSA。

路由邻接：指定的路由 (DR)



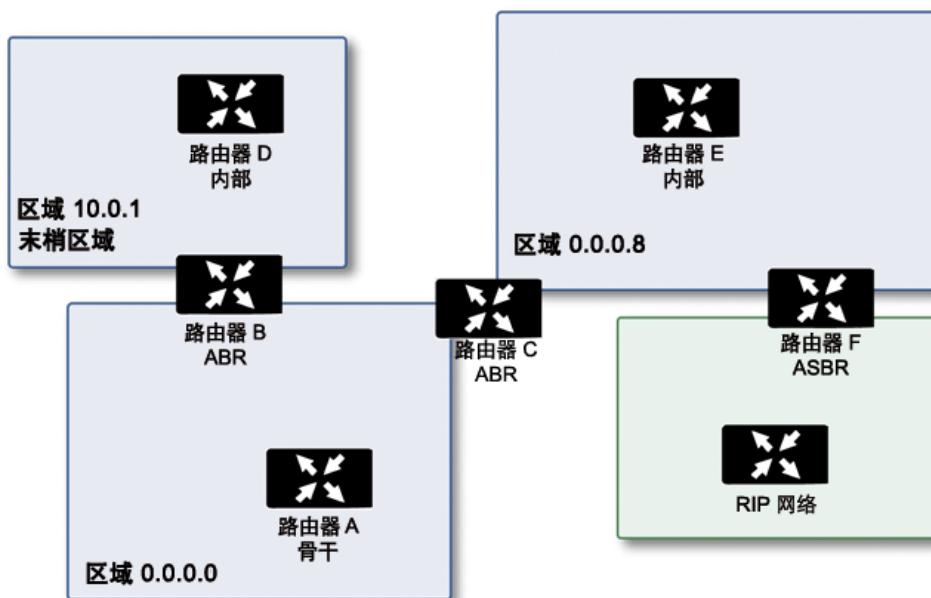
- **OSPF 数据包类型** - 五种类型的 OSPF 数据包为：
 - **Hello** (1 类 OSPF) - 按一定间隔发送，以建立和维护与相邻 OSPF 路由器的关系以及推选指定路由器。（在 LSDB 同步的初始化和 2-WAY 阶段发送）。
 - **数据库说明** (2 类 OSPF) - 在创建邻接关系时在 OSPF 路由器之间发送。在 LSDB 同步的 Exstart 阶段，DD 数据包将建立一个用于跟踪 LSA 的 ISN（初始序列号），它们将在相邻 OSPF 路由器之间建立主/从关系。在 LSDB 同步的 Exchange 阶段，它们包含简短版本的链路状态通告。因为 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，请参阅 [RFC1584 - Multicast Extensions to OSPF](#)。
- **7 类** (NSSA AS 外部链路通告) - 由作为 NSSA (参阅“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 (并非最佳路由) 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) 还能将 7 类 LSA 转换为 5 类 LSA (只能从 SonicOS CLI 执行此操作。请参阅 SonicOS CLI 参考指南)。
- **路由器类型** - OSPF 支持 4 种类型的路口 (基于其角色)；请参阅 [OSPF 支持的路由器类型示例](#)。

OSPF 支持的路由器类型示例



- **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。

丢弃隧道接口

丢弃隧道接口用于在已配置的路由关闭时避免使用不正确的路由发送流量。发送到丢弃隧道接口的流量不会离开安全设备，而是表面上丢弃。

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。如果静态路由绑定到隧道接口，SonicWall 建议为相同的网络流量配置绑定到丢弃隧道接口的静态路由。这样，如果隧道接口关闭，则使用第二个静态路由，有效地丢弃流量。这样可以防止数据在另一个路由上以明文形式转发。

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。

网络 | 路由

如果您的接口上有路由器，则可以在[管理 | 系统设置 | 网络 | 路由](#)页面上配置 SonicWall 安全设备上的静态路由。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。

主题：

- [第 384 页的网络 | 路由 > 设置](#)

网络 | 路由 > 设置

[管理 | 系统设置 | 网络 | 路由 > 设置](#)的外观因您选择的路由模式而异：

- 简单 RIP 通告
- 高级路由

简单 RIP 通告

路由策略 路由通告 设置

按路由类中的度量设置路由的优先级

路由模式：简单 RIP 通告

高级路由

路由策略 OSPFv2 RIP OSPFv3 RIPng 设置

按路由类中的度量设置路由的优先级

路由模式：高级路由

BGP：禁用 BGP 状态

网络 | 路由 > 路由策略

网络 | 路由 > 路由策略显示 IPv4 或 IPv6 的所有默认和/或自定义路由。对于任一 IP 版本，显示是相同的，除了 IPv6 显示所显示的是 IPv6 链接本地地址而不是 IP 地址。

通过选择下列选项，您可以更改路由策略表中路由策略的视图：

- IPv4 或 IPv6
- 视图中的一项视图设置：

所有类型	包括自定义策略和默认策略在内的所有路由策略。最初，在您选择所有类型后，路由策略表中仅显示默认策略。
自定义策略	您创建的策略。
默认策略	由 SonicOS 创建的策略。

您可以通过在搜索字段中输入源、目标或接口来过滤显示。

路由策略 路由通告 设置

添加 删除 IPv6 IPv6 视图 所有类型 刷新 设置

#	源	目标	服务	TOS/掩码	网关	接口	Metric	优先级	探测	注释	配置
1	IPv6 MGMT IPv6 主要静态地址	任何	任何	任何	::	MGMT	1	3			
2	IPv6 任何	MGMT IPv6 主要静态地址	任何	任何	::	MGMT	1	4			
3	IPv6 任何	ffff:ffff:ffff:ffff:ffff:ffff:128	任何	任何	::	X0	20	5			
4	IPv6 任何	::/0	任何	任何	::	X1	255	15			

列	路由策略配置
源	源的 IP 版本图标和名称。
目标	目的地 IP 地址 (IPv4) 或 MAC 地址 (IPv6)。

列	路由策略配置
服务	为路由策略配置的服务对象。
TOS/掩码	为路由配置的 TOS 和 TOS 掩码。
网关	网关 IP 地址 (IPv4) 或 MAC 地址 (IPv6)。
接口	为路由策略配置的接口。
Metric	为路由优先级配置的度量值。
优先级	路由策略的优先级。
探测	是否配置了探测。
注释	包含在配置自定义路由时输入的备注的备注图标；默认策略的自动添加的路由策略。
配置	编辑和删除图标；默认策略的图标显示为灰色。

网络 | 路由 > 路由通告

网络 | 路由仅当为路由模式选择了简单 RIP 通告时，才会显示 > 路由通告。

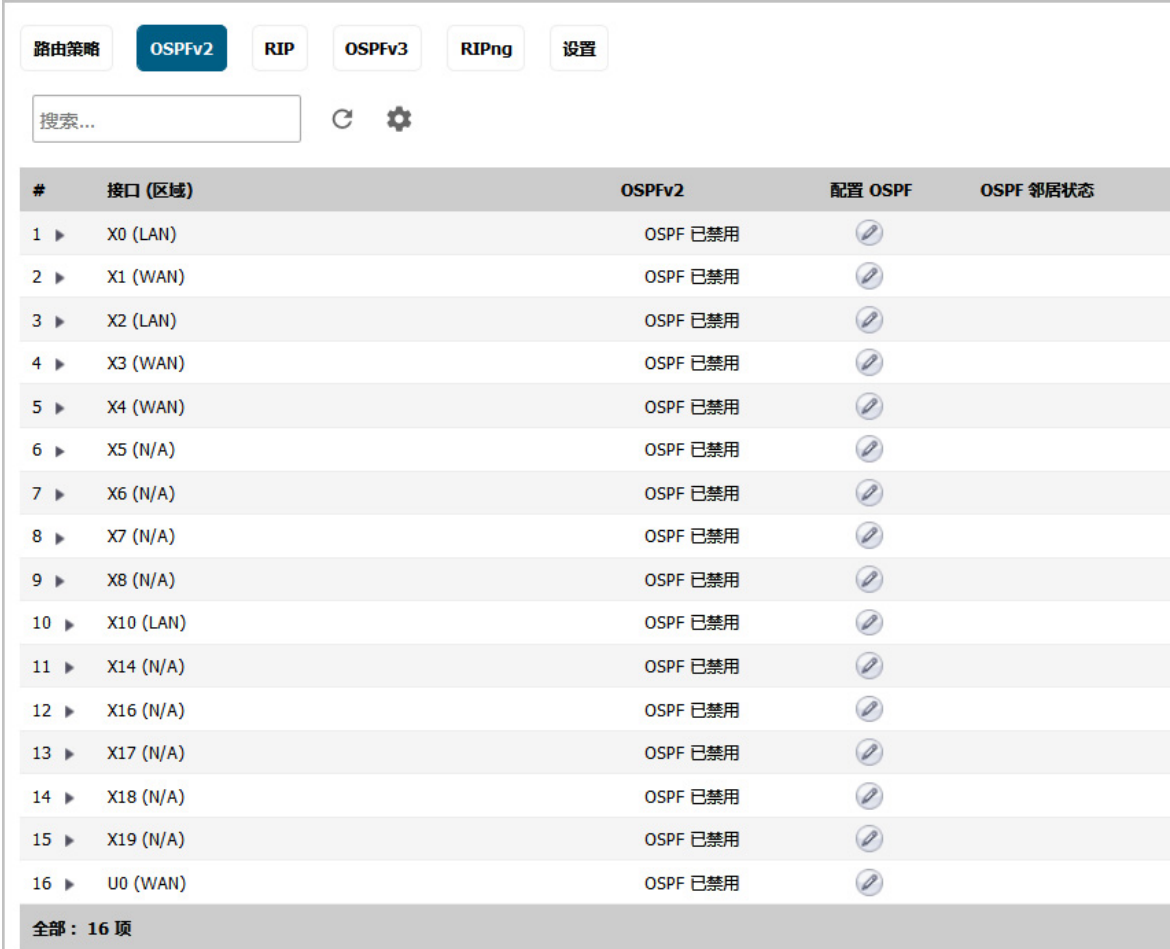
#	接口 (区域)	状态	配置
1	X0 (LAN)	已禁用	
2	X1 (WAN)	已禁用	
3	X2 (LAN)	已禁用	
4	X3 (WAN)	已禁用	
5	X4 (WAN)	已禁用	
6	X5 (N/A)	已禁用	
7	X6 (N/A)	已禁用	
8	X7 (N/A)	已禁用	
9	X8 (N/A)	已禁用	
10	X10 (LAN)	已禁用	
11	X14 (N/A)	已禁用	
12	X16 (N/A)	已禁用	
13	X17 (N/A)	已禁用	
14	X18 (N/A)	已禁用	
15	X19 (N/A)	已禁用	

全部：16 项

接口 (区域)	为路由通告配置的接口。如果未对接口配置区域，则 (区域) 指定为 (不适用)。
状态	已启用或已禁用。
配置	包含编辑图标。

网络 | 路由 > OSPFv2

网络 | 路由 > OSPFv2 仅在为路由模式选择了高级路由时显示，它显示了 OSPFv2 的状态且允许您为接口配置 OSPFv2。



#	接口 (区域)	OSPFv2	配置 OSPF	OSPF 邻居状态
1	X0 (LAN)	OSPF 已禁用		
2	X1 (WAN)	OSPF 已禁用		
3	X2 (LAN)	OSPF 已禁用		
4	X3 (WAN)	OSPF 已禁用		
5	X4 (WAN)	OSPF 已禁用		
6	X5 (N/A)	OSPF 已禁用		
7	X6 (N/A)	OSPF 已禁用		
8	X7 (N/A)	OSPF 已禁用		
9	X8 (N/A)	OSPF 已禁用		
10	X10 (LAN)	OSPF 已禁用		
11	X14 (N/A)	OSPF 已禁用		
12	X16 (N/A)	OSPF 已禁用		
13	X17 (N/A)	OSPF 已禁用		
14	X18 (N/A)	OSPF 已禁用		
15	X19 (N/A)	OSPF 已禁用		
16	U0 (WAN)	OSPF 已禁用		

全部: 16 项

设置

显示用于配置默认路由的度量值的设置弹出式菜单的图标。

接口 (区域)

为 OSPFv2 配置的接口及其区域。如果未对接口配置区域，则 (区域) 指定为 (不适用)。

OSPFv2

指示是否在接口上启用了 OSPF:

- OSPF 已启用
- OSPF 已启用(被动)
- OSPF 已禁用

配置 OSPF

显示接口的编辑图标。

OSPF 邻居状态

显示状态图标，此图标指示存在活动还是不活动的邻居；单击此图标将显示接口 **OSPFv2 邻居** 弹出窗口，可获取有关该接口的邻居的更多详细信息。请参阅第 388 页的 [网络 | 路由 > OSPFv2 > 接口 OSPFv2 邻居](#)。

网络 | 路由 > OSPFv2 > 接口 OSPFv2 邻居

通过单击界面的状态图标来显示此弹出窗口。

接口 X2:V402 (WLAN) OSPFv2 区域 0.0.0.0 邻居

路由器 ID	当前状态	优先级	IP 地址
192.168.166.1	Full / BDR	1	172.16.16.60
192.168.95.91	Full / DR	1	172.16.16.91

- 路由器 ID** 邻居的路由器 ID。
- 当前状态** OSPFv2 邻居在建立时的状态：
- 初始
 - 双向
 - **ExStart**
 - 交换
 - 正在加载
 - 全
- 优先级** 邻居路由器的优先级。
- IP 地址** 邻居路由器的 IP 地址。

网络 | 路由 > RIP

网络 | 路由 > RIP 仅在为路由模式选择了高级路由时显示，它显示 RIP 的状态且允许您为接口配置 RIP。

#	接口 (区域)	RIP	配置 RIP
1	X0 (LAN)	RIP 已禁用	
2	X1 (WAN)	RIP 已禁用	
3	X2 (LAN)	RIP 已禁用	
	X2:V402 (WLAN)	RIP 已禁用	
4	X3 (WAN)	RIP 已禁用	
5	X4 (WAN)	RIP 已禁用	
6	X5 (N/A)	RIP 已禁用	
7	X6 (N/A)	RIP 已禁用	
8	X7 (N/A)	RIP 已禁用	
9	X8 (N/A)	RIP 已禁用	
10	X10 (LAN)	RIP 已禁用	
11	X14 (N/A)	RIP 已禁用	
12	X16 (N/A)	RIP 已禁用	
13	X17 (N/A)	RIP 已禁用	
14	X18 (N/A)	RIP 已禁用	
15	X19 (N/A)	RIP 已禁用	
全部：16 项			

设置 显示用于配置默认路由的度量值的设置弹出式菜单的图标。

接口 (区域) 为 RIP 配置的接口及其区域。如果未对接口配置区域，则 (区域) 指定为 (不适用)。

RIP 指示是否在接口上启用 RIP:

- 已启用 RIP
- RIP 已启用(被动)
- RIP 已禁用

配置 RIP 显示接口的编辑图标。

网络 | 路由 > OSPFv3

网络 | 路由 > OSPFv3 仅在为路由模式选择了高级路由时显示，它显示了 OSPFv3 的状态且允许您为接口配置 OSPFv3。

#	接口 (区域)	OSPFv3	配置 OSPFv3	OSPFv3 邻居状态
1 ▶	X0 (LAN)	OSPFv3 已禁用		
2 ▶	X1 (WAN)	OSPFv3 已禁用		
3 ▼	X2 (LAN)	OSPFv3 已禁用		
	X2:V402 (WLAN)	OSPFv3 已禁用		
4 ▶	X3 (WAN)	OSPFv3 已禁用		
5 ▶	X4 (WAN)	OSPFv3 已禁用		
6 ▶	X5 (N/A)	OSPFv3 已禁用		
7 ▶	X6 (N/A)	OSPFv3 已禁用		
8 ▶	X7 (N/A)	OSPFv3 已禁用		
9 ▶	X8 (N/A)	OSPFv3 已禁用		
10 ▶	X10 (LAN)	OSPFv3 已禁用		
11 ▶	X14 (N/A)	OSPFv3 已禁用		
12 ▶	X16 (N/A)	OSPFv3 已禁用		
13 ▶	X17 (N/A)	OSPFv3 已禁用		
14 ▶	X18 (N/A)	OSPFv3 已禁用		
15 ▶	X19 (N/A)	OSPFv3 已禁用		
全部: 16 项				

设置

显示用于配置默认路由的度量值的设置弹出式菜单的图标。

接口 (区域)

为 OSPFv3 配置的接口及其区域。如果未对接口配置区域，则 (区域) 指定为 (不适用)。

OSPFv3

指示是否在接口上启用了 OSPF:

- OSPFv3 已启用
- OSPFv3 已启用 (被动)
- OSPFv3 已禁用

配置 OSPFv3

显示接口的编辑图标。

OSPFv3 邻居状态

显示状态图标，此图标指示存在活动还是不活动的邻居；单击此图标将显示接口 OSPFv3 邻居弹出窗口，可获取有关该接口的邻居的更多详细信息。请参阅第 390 页的 [网络 | 路由 > OSPFv3 > 接口 OSPFv3 邻居](#)。

网络 | 路由 > OSPFv3 > 接口 OSPFv3 邻居

通过单击界面的状态图标来显示此弹出窗口。

接口 X2:V402 (WLAN) OSPFv3 邻居		
路由 ID	目前状态	优先级
192.168.95.91	Full/DR	1

- 路由 ID** 邻居路由器的 ID。
- 目前状态** OSPFv3 邻居在建立时的状态：
- 初始
 - 双向
 - **ExStart**
 - 交换
 - 正在加载
 - 全
- 优先级** 邻居路由器的优先级。

网络 | 路由 > RIPng

网络 | 路由 > RIPng 仅在为路由模式选择了高级路由时显示，它显示了 RIPng 的状态且允许您为接口配置 RIPng。

#	接口 (区域)	RIPng	配置 RIPng
1	X0 (LAN)	RIPng 已禁用	
2	X1 (WAN)	RIPng 已禁用	
3	X2 (LAN)	RIPng 已禁用	
	X2:V402 (WLAN)	RIPng 已禁用	
4	X3 (WAN)	RIPng 已禁用	
5	X4 (WAN)	RIPng 已禁用	
6	X5 (N/A)	RIPng 已禁用	
7	X6 (N/A)	RIPng 已禁用	
8	X7 (N/A)	RIPng 已禁用	
9	X8 (N/A)	RIPng 已禁用	
10	X10 (LAN)	RIPng 已禁用	
11	X14 (N/A)	RIPng 已禁用	
12	X16 (N/A)	RIPng 已禁用	
13	X17 (N/A)	RIPng 已禁用	
14	X18 (N/A)	RIPng 已禁用	
15	X19 (N/A)	RIPng 已禁用	

全部: 16 项

- 设置** 显示用于配置默认路由的度量值的设置弹出式菜单的图标。
- 接口 (区域)** 为 RIPng 配置的接口及其区域。如果未对接口配置区域，则 (区域) 指定为 (不适用)。
- RIPng** 指示是否在接口上启用 RIPng：
- 已启用 RIP
 - **RIP 已启用(被动)**
 - RIP 已禁用
- 配置 RIPng** 显示接口的编辑图标。

配置路由

主题：

- 第 392 页的[按度量值设置路由的优先级](#)
- 第 393 页的[为通过路由公告学习的默认路由配置度量值](#)
- 第 394 页的[配置静态和基于策略的路由](#)
- 第 397 页的[为丢弃隧道接口配置静态路由](#)
- 第 399 页的[配置 OSPF 和 RIP 高级路由服务](#)
- 第 408 页的[配置 BGP 高级路由](#)

按度量值设置路由的优先级

❗ 重要： 更改为度量值加权路由优先级要求重启 SonicWall 安全设备。

“度量值加权”选项允许度量值优先于路由特定性。度量值选项为以下内容时优先级排序中使用的优先级（高到低）：

- 未选择（默认值）：
 - a 路由分类（由源、目标、服务和 TOS 字段 [具有除任何以外的值] 的组合确定）
 - b 源、目标、服务和 TOS 字段的累计特定性。
 - c 度量。
- 已选的：
 - a 路由分类。
 - b 度量。
 - c 源、目标、服务和 TOS 字段的累计特定性

更改为度量值加权路由优先级的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | 路由 > 设置**。
- 2 选择按路由类中的度量设置路由的优先级。将显示确认消息。

警告！更改为度量加权路由优先级？需要重启。单击“确定”以继续。

- 3 单击确定。
- 4 转至 **管理 | 更新 | 重启** 以手动重启 SonicOS。

为通过路由公告学习的默认路由配置度量值

i | 注：此设置仅对通过路由公告学习的 IPv6 默认路由起作用。

配置通过路由公告学习的默认路由的度量值的步骤如下：

- 1 转至管理 | 网络 | 路由。
- 2 单击路由策略。
- 3 单击设置图标。随即显示设置对话框。

将以下度量应用于通过路由公告学习的 IPv6 默认路由: 50

- 4 此路由度量值适用于通过路由公告学习的默认路由。在将以下度量应用于通过路由公告学习的 IPv6 默认路由由字段中输入度量值。最小值为 1，最大值为 255，默认值为 50。

i | 提示：度量值越低越好且低度量值优先于高度量值。

- 5 单击接受。

配置路由通告

为网络接口启用路由通告的步骤如下：

- 1 转至管理 | 网络 | 路由。
- 2 单击路由通告。
- 3 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。
- 4 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。

- 5 从通告默认路由由下拉菜单，选择：
 - 从不（默认）
 - WAN 接口活动的时候（不可用于 WAN 接口）
 - 始终
- 6 如果在安全设备中配置了静态路由，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。
- 7 如果想要通告 VPN 网络，则启用通告远程 VPN 网络。
- 8 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。

- 9 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。
- 10 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。
 - ① 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 13。
- 11 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。
- 12 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。
- 13 单击确定。

配置静态和基于策略的路由

在 SonicOS 中，静态路由是通过基本路由策略进行配置的。如需了解每个安全设备的最大路由数，请参阅 SonicOS 策略中配置路由策略的描述。

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。

配置静态或基于策略的路由的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 路由 > 路由策略。
- 2 单击添加图标。随即显示添加路由策略对话框。

常规
高级

路由策略设置

源：

目标：

服务：

标准路由
 多路径路由

接口：

网关：

度量：

备注：

当接口断开时，禁用路由
 允许 VPN 路径优先

WXA 群组：

探测：

当探测成功时禁用路由
 探测状态默认为启用

- 3 从源中，选择静态路由的源地址对象或选择创建新地址对象以动态创建新的地址对象。默认设置为任何。
- 4 从目标中，选择目的地地址对象或选择创建新地址对象以动态创建新的地址对象。默认设置为任何。
- 5 从服务中，选择服务对象。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 选择要使用的路由的类型：
 - 标准路由（默认）- 转至 [步骤 8](#)。
 - 多路径路由 - 将显示网关号选项：

标准路由
 多路径路由

网关号：

接口：

网关：

度量：

- 7 从网关号中，选择最大网关数：
 - 2
 - 3
 - 4

- 8 从接口中，选择要用于路由的接口，或选择**创建 VPN 隧道接口**以动态创建新的 VPN 策略。如需创建 VPN 策略的信息，请参阅 SonicOS 连接。
- 9 从网关中，选择要用于路由的网关地址对象，或选择**创建新地址对象**以动态创建新的地址对象。默认值为 0.0.0.0。如需创建地址对象的信息，请参阅 SonicOS 策略。
- 10 输入路由的**度量值**（加权成本）。最小值为 1，最大值为 254。默认度量值
 - 对于静态路由为 **1**
 - 动态路由：
 - 从 RIP/RIPng 中学习到的为 **120**
 - 从 OSPFv2/OSPFv3 中学习到的为 **110**
 - 从 BGP 中学习到的为 **20**

如需度量值的更多信息，请参阅第 373 页的[关于度量和距离](#)和第 375 页的[基于策略的路由](#)。

i **提示：**度量值越低越好且低度量值优先于高度量值（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。

- 11 也可以输入路由的**备注**。此字段用于输入新静态路由策略的描述性备注。
- 12 如需在接口断开连接时禁用路由，请选中**当接口断开时，禁用路由**。默认情况下已选中该选项。
- 13 （可选）如需为 VPN 隧道创建备份路由，请选中**允许 VPN 路径优先**。默认情况下未选中该选项。

默认情况下，用户配置的 VPN 隧道静态路由的度量值为 1 且优先于 VPN 流量。对于同一目标地址对象，**允许 VPN 路径优先**选项将使 VPN 流量优先于静态路由。当 VPN 路径处于这些状态时，将导致以下结果：

 - **活动：**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。
 - **关闭：**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。

14 如果 WXA 获得许可，请从 **WXA 群组**中选择 WXA 群组。默认设置为无。

15 如需：

- 使用支持探测且基于策略的路由，请转至**步骤 16**。
- 忽略支持探测的路由并配置 TOS 和管理距离值，请转至**步骤 20**。
- 应用配置，请转至**步骤 24**。

16 从探测中，选择：

- 无（默认）。转至**步骤 19**。
- 网络监视器对象；以下两个选项可用于配置支持探测且基于策略的路由。
- **创建新的网络监视对象**。随即显示**添加策略**对话框。如需了解创建网络监视器对象的方法，请参阅 SonicOS 调查中的过程。

17 如需在探测成功时禁用路由，请选中**当探测成功时禁用路由**。默认情况下未选中该选项。

i **重要：**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。

18 选择**探测状态默认为启用**，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”。

- 19 如需使用默认 TOS 和管理距离值，请转至 [步骤 24](#)。
- 20 单击高级。



The screenshot shows the '高级路由策略设置' (Advanced Routing Policy Settings) configuration page. At the top, there are two tabs: '常规' (General) and '高级' (Advanced), with '高级' being the active tab. Below the tabs, the title '高级路由策略设置' is displayed. The configuration area includes the following fields and options:

- TOS (十六进制): [Input field]
- TOS 掩码 (十六进制): [Input field]
- 制: [Input field]
- 管理距离: [Input field] 自动

- 21 在 **TOS**（十六进制）字段中输入一个 TOS 值。最大值为 FF。如果未配置 **TOS** 和 **TOS 掩码** 字段，则 will 使用值 0。如需 TOS 和 TOS 掩码值的更多信息，请参阅第 [375](#) 页的 [基于策略的 TOS 路由](#)。
- 22 在 **TOS 掩码**（十六进制）字段中输入相同值。
- 23 手动指定管理距离的步骤如下：
 - a 取消选中 **自动**。**管理距离** 字段将激活。默认情况下已选中该选项。如需管理距离的信息，请参阅第 [373](#) 页的 [关于度量和和管理距离](#)。
 - b 在 **管理距离** 字段中输入管理距离。
- 24 单击确定。

为丢弃隧道接口配置静态路由

为丢弃隧道接口添加静态路由的步骤如下：

- 1 转至 [管理 | 系统设置 | 网络 | 路由 > 路由策略](#)。

- 单击添加图标。随即显示添加路由策略对话框。

常规 高级

路由策略设置

源：

目标：

服务：

标准路由 多路径路由

接口：

网关：

度量：

备注：

当接口断开时，禁用路由

允许 VPN 路径优先

WXA 群组：

探测：

当探测成功时禁用路由

探测状态默认为启用

- 按照第 394 页的[配置静态和基于策略的路由](#)中的描述，配置源、目标、服务和路径选项的值。
- 在接口下，选择 **Drop_TunnelIf**。这些选项将发生更改。

路由策略设置

源：

目标：

服务：

标准路由 多路径路由

接口：

网关：

度量：

备注：

WXA 群组：

- 按照第 394 页的[配置静态和基于策略的路由](#)中的描述，完成选项配置。
- 单击确定。此路由已启用且显示在路由策略表中。

配置 OSPF 和 RIP 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。SonicOS 管理界面中未限制 ARS 功能，而是提供了其功能的缩写表示，从而提供对最密切相关的路由功能的控制，同时通过 CLI 提供了完整的命令套件（请参阅 SonicOS CLI 参考指南）。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 提供将安全设备集成到多数 RIP 和 OSPF 环境所需的所有功能。利用 CLI 的更多功能，可以进行更多高级配置。

默认已禁用高级路由服务，必须先将其启用才能使用。

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单独配置 RIP 和 OSPF 设置，且每个接口都可以运行 RIP 和 OSPF 路由器。

主题：

- 第 399 页的 [启用高级路由服务和 BGP](#)
- 第 400 页的 [配置 OSPF](#)
- 第 404 页的 [配置 RIP 和 RIPng](#)
- 第 407 页的 [配置隧道接口高级路由](#)

启用高级路由服务和 BGP

启用高级路由服务的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 路由 > 设置。
- 2 从路由模式中，选择高级路由。将显示确认消息。

警告! 是否确定要切换到高级路由? 单击“确定”以继续。

- 3 单击确定。网络 | 路由上的选项将发生更改：

路由策略 OSPFv2 RIP OSPFv3 RIPng 设置

按路由类中的度量设置路由的优先级

路由模式： 高级路由

BGP： 禁用 BGP 状态

- 4 如需启用 BGP，请从 BGP 中选择已启用（使用 CLI 配置）。默认值为禁用。将显示确认消息。

警告! 是否确定启用 BGP? 单击确定继续。

- 5 单击确定。BGP 状态按钮将激活。

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 安全设备集成到 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 380 页的 [OSPF 术语](#)。

主题：

- 第 400 页的 [配置 OSPFv2](#)
- 第 401 页的 [配置 OSPFv3](#)

配置 OSPFv2

为 OSPFv2 配置接口的步骤如下：

- 1 转至 [管理 | 系统设置 | 网络 | 路由 > OSPFv2](#)。
- 2 单击接口的编辑图标。随即显示接口 OSPFv2 配置对话框。

接口 X0 (LAN) OSPFv2 配置

OSPFv2:	<input type="text" value="已启用"/>
宕机间隔 (1 - 65535):	<input type="text" value="40"/>
Hello 间隔 (1 - 65535):	<input type="text" value="10"/>
验证:	<input type="text" value="已禁用"/>
密码:	<input type="password"/>
OSPF 区域	<input type="text" value="0"/>
OSPFv2 区域类型:	<input type="text" value="正常"/>
接口成本 (1 - 65535):	<input type="text"/> <input checked="" type="checkbox"/> 自动
路由器优先级: (0 - 255):	<input type="text" value="1"/>
<input type="checkbox"/> 启用 MTU 兼容性 (mtu-ignore):	

- 3 从 OSPFv2 中，选择：

已禁用（默认）	已在此接口上禁用 OSPF 路由器。转至 步骤 13 。
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。除 OSPF 区域 以外的所有选项都显示为灰色；请转至 步骤 9 。

- 4 如果未收到 Hello，则如需指定删除 LSDB 中的条目之前经过的时间段，请在 **无效时间间隔 (1 - 65535)** 字段中输入以秒为单位的时间。默认值为 40 秒，最小值为 1 秒，最大值为 65,535 秒。

重要： 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。

- 5 如需指定 Hello 数据包之间的时间段，请在 **Hello 间隔 (1 - 65535)** 字段中输入以秒为单位的时间。默认值为 **10** 秒，最小值为 **1** 秒，最大值为 **65,535** 秒。

i | **重要：** 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。

- 6 从身份验证中，选择在此接口上使用的身份验证类型：

禁用	未使用身份验证；请转至 步骤 8 。
简单密码	纯文本密码由 OSPF 路由器用于识别目的。
消息摘要	MD5 用于安全地识别 OSPF 路由。

i | **重要：** 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。

- 7 如果指定了：

简单密码	输入包含 1 至 15 个字符的字母数字密码。
消息摘要	输入包含 1 至 15 个字符的字母数字密码。

- 8 在 **OSPF 区域** 字段中输入区域 ID。OSPF 区域可采用 IP 或十进制表示法。例如，连接到 x4:100 的区域表示为 100.100.100.100 或 1684300900。默认值为 **0**。

- 9 从 **OSPFv2 区域类型** 中选择 OSPFv2 区域类型（如需这些设置的详细描述，请参阅第 380 页的 **OSPF 术语**）：

正常	默认值；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。
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 类的 LSA。

- 10 如需：

- 指定通过此接口发送数据包的开销，在 **接口成本 (1 - 65535)** 字段中输入开销。默认值为 **0**，通常用于指示以太网接口。默认最小值为 **0**（例如，快速以太网），最大值为 **65,535**（例如，pudding）。
- 自动确定成本，选择 **自动**，这会使 **接口成本** 字段显示为灰色。默认情况下已选中该选项。

- 11 如需指定确定网段的指定路由器 (DR) 时使用的路由器优先级值，请在 **路由器优先级 (0-255)** 字段中输入值。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**。

- 12 如需启用 MTU 兼容性，请选中启用 **MTU 兼容性 (mtu-ignore)**。默认情况下未选中该选项。

- 13 单击 **确定**。

配置 OSPFv3

为 **OSPFv3** 配置接口的步骤如下：

- 转至 **管理 | 系统设置 | 网络 | 路由 > OSPFv3**。
- 单击接口的 **编辑** 图标。随即显示 **接口 OSPFv3 配置** 对话框。

接口 X0 (LAN) OSPFv3 配置

OSPFv3:	禁用
OSPFv3 区域:	0
OSPFv3 区域类型:	正常
宕机间隔 (1 - 65535):	40
Hello 间隔 (1 - 65535):	10
接口成本 (1 - 65535):	1 <input checked="" type="checkbox"/> 自动
路由优先级: (0 - 255):	1
实例-ID: (0 - 255):	0

3 从 **OSPFv3** 中，选择：

- | | |
|---------|---|
| 已禁用（默认） | 已在此接口上禁用 OSPF 路由器。转至 步骤 12 。 |
| 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。除 OSPFv3 区域 以外的所有选项都显示为灰色。 |

4 在 **OSPF 区域** 字段中输入区域 ID。OSPF 区域可采用 IP 或十进制表示法。例如，连接到 x4:100 的区域表示为 100.100.100.100 或 1684300900。默认值为 0。

5 如果为 **OSPFv3** 选择了被动，请转至 [步骤 12](#)。

6 如果未收到 Hello，则如需指定删除 LSDB 中的条目之前经过的时间段，请在 **无效时间间隔（1 - 65535）** 字段中输入以秒为单位的时间。默认值为 40 秒，最小值为 1 秒，最大值为 65,535 秒。

重要： 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。

7 从 **OSPFv3 区域类型** 中选择 OSPFv3 区域类型（如需这些设置的详细描述，请参阅第 380 页的 [OSPF 术语](#)）：

- | | |
|--------|-------------------------|
| 正常 | 默认值；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。 |

8 如需指定 Hello 数据包之间的时间段，请在 **Hello 间隔（1 - 65535）** 字段中输入以秒为单位的时间。默认值为 10 秒，最小值为 1 秒，最大值为 65,535 秒。

重要： 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。

9 如需：

- 指定通过此接口发送数据包的开销，在 **接口成本（1 - 65535）** 字段中输入开销。默认值为 0，通常用于指示以太网接口。默认最小值为 0（例如，快速以太网），最大值为 65,535（例如，pudding）。
- 自动确定成本，选择 **自动**，这会使 **接口成本** 字段显示为灰色。默认情况下已选中该选项。

10 如需指定确定网段的指定路由器 (DR) 时使用的路由器优先级值，请在 **路由器优先级（0-255）** 字段中输入值。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。

11 如需为接口配置实例 ID，请在实例-ID（0 - 255）字段中输入值。最小值为 0（默认值），而最大值为 255。默认情况下未选中该选项。

重要：此选项通常显示为灰色，并只应通过 SonicOS 命令行接口（如需 SonicOS CLI 的信息，请参阅 SonicOS 命令行接口）。

12 单击确定。

全局 OSPFv3 配置

配置全局 OSPFv3 的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 路由。
- 2 单击 **OSPFv3**。
- 3 单击设置图标。随即显示设置弹出对话框：



设置

将以下度量应用于从高级路由协议中接收的默认路由: 110

允许学习来自高级路由协议的 ECMP 路由

OSPFv3 路由 ID (n.n.n.n): 192.168.95.8 默认度量 (1 - 16777214): Undefined

ABR 类型: Cisco 自动成本参考 BW (Mb/s): 100

重新分配静态路由

度量 (1 - 16777214): Default 度量类型: 外部类型 2

重新分配已连接的网络

度量 (1 - 16777214): Default 度量类型: 外部类型 2

重新分配 RIP 路由

接受 取消

4 配置以下选项：

- **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。它与安全设备上的所有 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。
 - **快捷方式** - “快捷方式区域”使 ABR 路由器无论是否连接到区域 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。
- **重新分配静态路由** - 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。

- **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。

5 单击**接受**。

路由协议部分将按接口显示所有活动 OSPF 路由器的状态。

路由策略部分将 OSPF 所学习的路由显示为 **OSPF** 或 **RIP** 路由。

状态按钮将激活。

配置 RIP 和 RIPng

主题：

- 第 [404](#) 页的 **配置 RIP**

配置 RIP

在接口上配置 RIP 路由的步骤如下：

- 1 转至**管理 | 网络 | 路由**。
- 2 单击 **RIP**。
- 3 单击接口的编辑图标。随即显示**接口 RIP** 配置对话框。

接口 X0 (LAN) RIP 配置

RIP: 已禁用

接收: RIPv2

水平分割

毒性逆转

发送: RIPv2

使用密码

密码:

4 从 RIP 中，选择一种模式：

已禁用（默认）	RIP 在此接口上处于禁用状态；请转至 步骤 12 。
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。
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 <code>CLneighbor</code> 命令指定的临近 RIP 路由器。 重要： 此模式只应在通过 ARS-RIP CLI 配置高级 RIP 选项时使用（请参阅 SonicOS CLI 参考指南）。选中后，所有其他选项将显示为灰色。

5 如果指定了：

- 仅发送，请转至 [步骤 8](#)。
- 被动，请转至 [步骤 12](#)。

6 从接收中，选择用于接收 RIP 数据包的 RIP 版本：

RIPv1	仅接收广播 RIPv1 数据包。
RIPv2（默认）	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 <code>ars-rip</code> 路由器将不会处理这些更新。

7 如果为 RIP 选择了仅接收，请转至 [步骤 11](#)。

8 如需禁止在更新中包含发送到它们从中进行学习的路由器，请选中 **水平分割**。这是用于防止路由循环的常用 RIP 机制；请参阅第 [378](#) 页的 **最大跃点数**。默认情况下已选中该选项。

9 如需指定“水平分割”操作的可选模式，请选中 **毒性逆转**。该模式不禁止包含学习到的路由，而是使用极限量（16）来发送这些路由，表明它们是不可到达的；请参见第 [378](#) 页的 **最大跃点数**。默认情况下已选中该选项。

10 从发送中，选择用于发送数据包的 RIP 版本：

RIPv1	发送广播 RIPv1 数据包。
RIPv2 - v1 兼容	发送与 RIPv1 兼容的组播 RIPv2 数据包。
RIPv2（默认）	发送组播 RIPv2 数据包。

11 如需强制使用密码，请选中 **使用密码**。密码字段将激活。默认情况下未选中该选项。

- a 在 **密码** 字段中输入密码。

12 单击 **确定**。

配置 RIPng

在接口上配置 RIPng 路由的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 路由 > RIPng。
- 2 单击接口的编辑图标。随即显示接口 RIPng 配置对话框。



- 3 从 RIPng 中，选择一种模式：

已禁用（默认）	RIPng 在此接口上处于禁用状态；请转至 步骤 6 。
启用	此接口上的 RIPng 路由器将发送更新并处理已接收的更新。
被动	此接口上的 RIPng 路由器不处理已接收的更新，并仅将更新发送到使用 CLI neighbor 命令指定的相邻 RIPng 路由器。 重要： 此模式只应在通过 ARS-RIP CLI 配置高级 RIPng 选项时使用（请参阅 SonicOS CLI 参考指南）。

- 4 如需禁止在更新中包含发送到它们从中进行学习的路由器，请选中[水平分割](#)。这是用于防止路由循环的常用 RIP 机制；请参阅第 [378](#) 页的[最大跃点数](#)。默认情况下已选中该选项。
- 5 如需指定“水平分割”操作的可选模式，请选中[毒性逆转](#)。该模式不禁止包含学习到的路由，而是使用极限量度 (16) 来发送这些路由，表明它们是不可到达的；请参见第 [378](#) 页的[最大跃点数](#)。默认情况下已选中该选项。
- 6 单击确定。

全局 RIPng 配置

配置全局 OSPFv3 的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 路由。
- 2 单击 **OSPFv3**。
- 3 单击设置图标。随即显示设置弹出对话框：



4 配置以下选项：

- 默认度量 - 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 系统通告安全设备的默认路由。
- 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使用默认度量设置中指定的值（默认值）。
- 重新分配已连接的网络 - 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使用默认度量设置中指定的值（默认值）。

5 单击接受。

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。如需更多信息，请参阅第 X 页的添加隧道接口。

为隧道接口启用高级路由后，它将与其它接口一同显示在 **网络 | 路由** 上各种视图的表中。

配置高级路由选项的步骤如下：

- 1 对于您要配置的隧道接口，单击 **配置 RIP/RIPng** 或 **配置 OSPF/OSPFv3** 列中的编辑图标。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

由于无编号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：

- 借用的 IP 地址来自于 - 将其 IP 地址用作隧道接口的源 IP 地址的接口。

i | 注：借用的 IP 地址必须为静态 IP 地址。

- 远程 IP 地址 - 隧道接口连接到的远程对端接口的 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。

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高级路由的隧道接口：

- 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。

i | 提示：SonicWall 建议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，此建议可避免发生冲突。

- 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

i | 注：以下设备支持 BGP：

- NSA 2600 及更高版本的安全设备。
- 购买了 SonicOS 扩展许可证的 TZ400 系列、TZ500 系列和 TZ600 安全设备。

TZ300 系列或 SOHO 无线安全设备不支持 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 支持允许使用安全设备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/多宿主”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 将在 SonicOS 管理界面的网络 | 路由页面上启用，然后通过 SonicOS 命令行接口 (CLI；请参阅 SonicOS CLI 参考指南) 进行完全配置。

如需 SonicWall 的 BGP 实施的完整信息，请参阅第 792 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 推荐配置要用于 BGP 会话的 IPsec 隧道。如需了解为 BGP 配置 IPsec 隧道和启用 BGP 的方法，请参阅第 792 页的 [BGP 高级路由](#)。

在通过管理界面启用 BGP 后，BGP 配置的具体设置使用 SonicOS 命令行接口 (CLI) 执行。如需 SonicWall 安全设备上 BGP 实施的完整信息，请参阅第 792 页的 [BGP 高级路由](#)。

管理 ARP 流量

- 第 409 页的[网络 | ARP](#)
 - 第 410 页的[静态 ARP 条目](#)
 - 第 413 页的[ARP 设置](#)
 - 第 414 页的[ARP 缓存](#)

网络 | ARP

静态 ARP 条目

#	IP 地址	MAC 地址	供应商	接口	已发布	绑定 MAC	配置
无条目							

添加 删除 删除所有

ARP 设置

ARP 缓存条目超时(分钟数): 不要从 ARP 请求收集源数据

ARP 缓存

项目 1 至 12 (/ 12) « » »»

#	IP 地址	类型	MAC 地址	供应商	接口	超时	清除
<input type="checkbox"/>	1 172.16.16.60	动态	C0:EA:E4:59:8E:52	SONICWALL	X2:V402	将于 10 分钟后过期	<input type="checkbox"/>
<input type="checkbox"/>	2 172.16.16.83	静态	C0:EA:E4:59:8E:26	SONICWALL	X2:V402	永久 已发布	<input type="checkbox"/>
<input type="checkbox"/>	3 172.16.16.91	动态	C0:EA:E4:59:94:56	SONICWALL	X2:V402	将于 10 分钟后过期	<input type="checkbox"/>
<input type="checkbox"/>	4 192.168.1.254	静态	C0:EA:E4:59:8E:38	SONICWALL	MGMT	永久 已发布	<input type="checkbox"/>
<input type="checkbox"/>	5 192.168.94.83	静态	C0:EA:E4:59:8E:26	SONICWALL	X2	永久 已发布	<input type="checkbox"/>
<input type="checkbox"/>	6 192.168.94.229	动态	00:0C:29:C8:18:23	VMWARE	X2	将于 10 分钟后过期	<input type="checkbox"/>
<input type="checkbox"/>	7 192.168.95.1	动态	00:17:C5:0F:6E:84	SONICWALL	X1	将于 10 分钟后过期	<input type="checkbox"/>
<input type="checkbox"/>	8 192.168.95.55	动态	18:81:69:09:15:81	SONICWALL	X1	将于 10 分钟后过期	<input type="checkbox"/>
<input type="checkbox"/>	9 192.168.95.83	静态	C0:EA:E4:59:8E:25	SONICWALL	X1	永久 已发布	<input type="checkbox"/>
<input type="checkbox"/>	10 192.168.95.233	动态	00:0C:29:22:36:E0	VMWARE	X1	将于 2 分钟后过期	<input type="checkbox"/>
<input type="checkbox"/>	11 192.168.166.1	静态	C0:EA:E4:59:8E:2E	SONICWALL	X10	永久 已发布	<input type="checkbox"/>
<input type="checkbox"/>	12 192.168.168.168	静态	C0:EA:E4:59:8E:24	SONICWALL	X0	永久 已发布	<input type="checkbox"/>

清除 清除 ARP 缓存

ARP 统计: ARP 统计: 条目数 12, 查找数 6066, 失败数 4338, 命中数 1723, 丢失数 5, 命中率 99%

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 410 页的 [静态 ARP 条目](#)
- 第 413 页的 [ARP 设置](#)
- 第 414 页的 [ARP 缓存](#)

静态 ARP 条目

通过静态 ARP 功能，可以在第 2 层 MAC 地址与第 3 层 IP 地址之间创建静态映射。

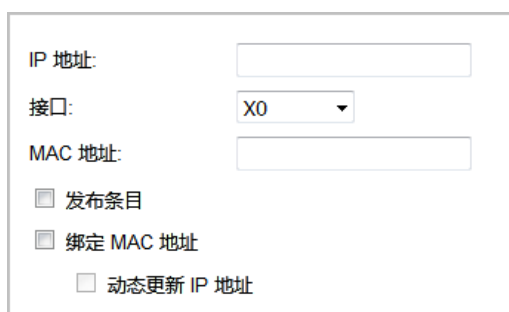
主题：

- 第 410 页的 [配置静态 ARP](#)
- 第 411 页的 [编辑静态 ARP 条目](#)
- 第 411 页的 [使用静态 ARP 的次要子网](#)
- 第 413 页的 [查看静态 ARP 条目](#)

配置静态 ARP

配置静态 ARP 的步骤如下：

- 1 转至网络 | ARP。
- 2 在静态 ARP 条目表下，单击添加。将显示添加静态 ARP 对话框。



IP 地址:

接口:

MAC 地址:

发布条目

绑定 MAC 地址

动态更新 IP 地址

- 3 在 IP 地址字段，输入 SonicWall 安全设备的 IP 地址。
- 4 从接口中，选择安全设备上要与此静态 ARP 条目关联的 LAN 接口。
- 5 在 MAC 地址字段中，输入安全设备的 MAC 地址。
- 6 如需让安全设备响应对指定 IP 地址和指定 MAC 地址的 ARP 查询，请选中发布条目选项。默认情况下未选中该选项。

例如，可以使用此选项使安全设备通过添加安全设备的 MAC 地址来答复特定接口上的次要 IP 地址。请参阅第 411 页的 [使用静态 ARP 的次要子网](#)。选择此选项将使 MAC 地址字段和绑定 MAC 地址选项处于灰显状态。

- 7 如果选中了发布条目，请转至 [步骤 10](#)。
- 8 如需将指定的 MAC 地址绑定到指定的 IP 地址和接口，请选中绑定 MAC 地址。默认情况下未选中该选项。

此选项可确保只能在安全设备的指定接口上使用特定工作站（通过网卡的唯一 MAC 地址进行识别）。将 MAC 地址绑定到某个接口后，安全设备：

- 不会在任何其他接口上对该 MAC 地址做出响应。
- 删除可能已存在的对该 MAC 地址的任何动态缓存引用。
- 禁止对该 MAC 地址进行更多（非唯一）静态映射。

选中了“绑定 MAC 地址”后，动态更新 IP 地址将激活。

- 9 如需允许在使用 DHCP 动态分配 IP 寻址的情况下将 MAC 地址绑定到某个接口，请选中**动态更新 IP 地址**选项，这是**绑定 MAC 地址**选项的子功能。

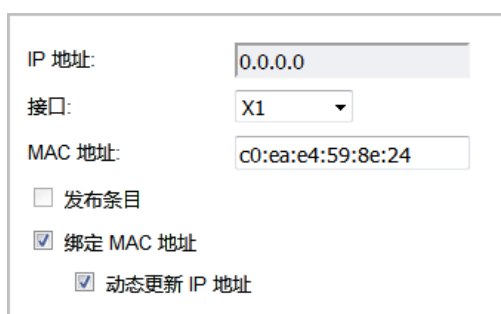
启用此选项将使 IP 地址字段显示为灰色且将其设置为 0.0.0.0，激活 MAC 地址字段，并使用由安全设备的内部 DHCP 服务器或外部 DHCP 服务器（如果正在使用 IP 助手）分配的 IP 地址来填充 ARP 缓存。

- 10 单击确定。

编辑静态 ARP 条目

编辑静态 ARP 条目的步骤如下：

- 1 转至网络 | ARP。
- 2 在静态 ARP 条目表中，单击配置列中该条目的编辑图标。将显示编辑静态 ARP 对话框。



IP 地址:	0.0.0.0
接口:	X1
MAC 地址:	c0:ea:e4:59:8e:24
<input type="checkbox"/> 发布条目	
<input checked="" type="checkbox"/> 绑定 MAC 地址	
<input checked="" type="checkbox"/> 动态更新 IP 地址	

- 3 做出更改。
- 4 单击确定。条目已更新。

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且无需添加自动 NAT 规则。

主题：

- 第 412 页的[添加次要子网](#)
- 第 412 页的[示例](#)

添加次要子网

使用静态 ARP 方法添加次要子网的步骤如下：

- 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安全设备的 MAC 地址。
- 2 添加用于该子网的静态路由，使安全设备将其视为有效流量，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。

示例

考虑以下网络示例（请参阅第 412 页的[添加次要子网](#)）。

支持所添加的配置的步骤如下：

- 1 为将用作次要子网的网关的 192.168.50.1 创建一个发布的静态 ARP 条目。
- 2 将其与相应的 LAN 接口关联。从网络 | ARP 中，在静态 ARP 条目表下单击添加。
- 3 添加此条目：



The screenshot shows a configuration form for a Static ARP entry. It includes the following fields and options:

- IP 地址: 10.203.28.77
- 接口: X1
- MAC 地址: c0:ea:e4:59:8e:25
- 发布条目
- 绑定 MAC 地址
- 动态更新 IP 地址

- 4 单击确定。此条目将显示在静态 ARP 条目表中。



The screenshot shows a table titled "静态 ARP 条目" (Static ARP Entries). The table has the following columns: #, IP 地址, MAC 地址, 供应商, 接口, 已发布, 绑定 MAC, and 配置. There is one entry in the table with IP 10.203.28.77, MAC c0:ea:e4:59:8e:25, and interface X1. Below the table are buttons for "添加" (Add), "删除" (Delete), and "删除所有" (Delete All).

#	IP 地址	MAC 地址	供应商	接口	已发布	绑定 MAC	配置
1	10.203.28.77	c0:ea:e4:59:8e:25	SONICWALL	X1	✓		 

- 5 转至网络 | 路由。
- 6 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。如需添加静态路由的信息，请参阅第 372 页的[配置路由通告和路由策略](#)。
- 7 如需使流量到达 192.168.50.0/24 子网，并使 192.168.50.0/24 子网到达 LAN 中的主机，请转至[策略 | 规则 > 访问规则](#)页面。
- 8 添加相应的访问规则，以允许流量通过。如需添加访问规则的信息，请参阅 SonicOS 策略。

查看静态 ARP 条目

静态 ARP 条目								
<input type="checkbox"/>	#	IP 地址	MAC 地址	供应商	接口	已发布	绑定 MAC	配置
<input type="checkbox"/>	1	10.203.28.77	c0:ea:e4:59:8e:25	SONICWALL	X1	<input checked="" type="checkbox"/>		 

- IP 地址** 用作网关的安全设备的 IP 地址。
- MAC 地址** 用作网关的安全设备的 MAC 地址。
- 供应商** 安全设备的制造商的名称。
- 接口** 与此条目关联的 LAN 接口。
- 已发布** 以绿色复选标记指示安全设备是否响应对有指定 MAC 地址的指定 IP 地址进行的 ARP 查询。
- 绑定 MAC** 以绿色复选标记指示是否将 MAC 地址绑定到指定的 IP 地址和接口。
- 配置** 显示条目的编辑和删除图标。

ARP 设置

ARP 设置	
ARP 缓存条目超时(分钟数):	<input type="text" value="10"/> <input type="checkbox"/> 不要从 ARP 请求收集源数据

- ARP 缓存条目超时 (分钟数)** 指定条目超以及从缓存刷新的时间段。最短时间为 2 分钟，最长时间为 600 分钟（10 小时），默认值为 10 分钟。
- 不要从 ARP 请求收集源数据** 选择此设置可以禁止从 ARP 请求获取源数据。默认情况下未选中该选项。

ARP 缓存

#	IP 地址	类型	MAC 地址	供应商	接口	超时	清除	
<input type="checkbox"/>	1	10.203.28.77	静态	C0:EA:E4:59:8E:25	SONICWALL	X1	永久 已发布	
<input type="checkbox"/>	2	172.16.16.83	静态	C0:EA:E4:59:8E:26	SONICWALL	X2:V402	永久 已发布	
<input type="checkbox"/>	3	192.168.1.254	静态	C0:EA:E4:59:8E:38	SONICWALL	MGMT	永久 已发布	
<input type="checkbox"/>	4	192.168.94.83	静态	C0:EA:E4:59:8E:26	SONICWALL	X2	永久 已发布	
<input checked="" type="checkbox"/>	5	192.168.94.229	动态	00:0C:29:C8:18:23	VMWARE	X2	将于 10 分钟后过期	
<input checked="" type="checkbox"/>	6	192.168.95.1	动态	00:17:C5:0F:6E:84	SONICWALL	X1	将于 10 分钟后过期	
<input type="checkbox"/>	7	192.168.95.83	静态	C0:EA:E4:59:8E:25	SONICWALL	X1	永久 已发布	
<input checked="" type="checkbox"/>	8	192.168.95.233	动态	00:0C:29:22:36:E0	VMWARE	X1	将于 10 分钟后过期	
<input type="checkbox"/>	9	192.168.166.1	静态	C0:EA:E4:59:8E:2E	SONICWALL	X10	永久 已发布	
<input type="checkbox"/>	10	192.168.168.168	静态	C0:EA:E4:59:8E:24	SONICWALL	X0	永久 已发布	

清除 ARP 缓存

ARP 统计: ARP 统计: 条目数 10, 查找数 7107, 失败数 5085, 命中数 2017, 丢失数 5, 命中率 99%

- IP 地址** 安全设备的 IP 地址。
- 类型** 指示 ARP 为静态 ARP 还是动态 ARP。
- MAC 地址** 与 IP 地址关联的 MAC 地址。
- 供应商** 安全设备的制造商的名称。
- 接口** 与此 ARP 条目关联的 LAN 接口。
- 超时** 指示此条目的缓存中的剩余时间。如果配置时此条目已发布，超时将显示永久已发布。
- 清除** 显示用于从 ARP 缓存中清除条目的删除图标。
注： 只有动态条目才具有删除图标。

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。

提示： 如需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。请参阅第 413 页的 **ARP 设置**。

清除 ARP 缓存表中某个动态条目的步骤如下：

- 1 单击清除列中的删除图标。

清除 ARP 缓存表中一个或多个动态条目的步骤如下：

- 1 选中一个或多个要清除的条目的复选框。清除按钮随即激活。
- 2 单击清除。

清除 ARP 缓存表中所有动态条目的步骤如下：

- 1 单击清除 ARP 缓存。

配置邻居发现协议

- 第 415 页的 [网络 | 邻居发现（仅 IPv6）](#)
 - 第 416 页的 [静态 NDP 条目](#)
 - 第 417 页的 [NDP 设置](#)
 - 第 417 页的 [NDP 缓存](#)
 - 第 418 页的 [配置静态 NDP 条目](#)
 - 第 418 页的 [编辑静态 NDP 条目](#)
 - 第 419 页的 [清除 NDP 缓存](#)

网络 | 邻居发现（仅 IPv6）

静态 NDP 条目

#	IP 地址	MAC 地址	供应商	接口	配置
无条目					

NDP 设置

邻居发现基础连接时间 (秒):

NDP 缓存

条目 至 0 (/ 0)

#	IP 地址	类型	MAC 地址	供应商	接口	超时	清除
无条目							

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，且您可以配置静态邻居发现条目。[IPv4/IPv6 邻居消息和功能](#)表显示类似于传统 IPv4 邻居消息的 IPv6 邻居消息和功能。

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 回复消息	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。

主题：

- [第 416 页的静态 NDP 条目](#)
- [第 417 页的 NDP 设置](#)
- [第 417 页的 NDP 缓存](#)
- [第 418 页的配置静态 NDP 条目](#)
- [第 418 页的编辑静态 NDP 条目](#)
- [第 419 页的清除 NDP 缓存](#)

静态 NDP 条目

静态 NDP 条目

<input type="checkbox"/>	#	IP 地址	MAC 地址	供应商	接口	配置
无条目						

- IP 地址** 远程设备的 IPv6 IP 地址。
- MAC 地址** 远程设备的 MAC 地址。
- 供应商** 远程设备制造商的名称。
- 接口** 与远程设备关联的接口。
- 配置** 包含条目的编辑和删除图标。

NDP 设置

NDP 设置

邻居发现基础连接时间 (秒):

在 NDP 设置中指定到达邻居的最长时间。

i | 注：对于 IPv6，也可以在网络 | 接口 > 编辑接口 > 高级对话框中为每个接口设置此值。如果在接口上启用路由公告，则为该接口设置的值仅用于该接口。如需更多信息，请参阅第 234 页的[配置接口](#)。

指定最长时间的步骤如下：

- 1 在邻居发现基础连接时间（秒）字段中输入数字。最小时长为 0 秒，最大时长为 3600 秒，默认值为 20 秒。
 - i** | 提示：此选项的值设置为 0 时，将使用 NDP 设置的全局值。
- 2 单击更改。

NDP 缓存

NDP 缓存

条目 至 0 (/ 0)

#	IP 地址	类型	MAC 地址	供应商	接口	超时	清除
无条目							

NDP 缓存表显示所有当前的 IPv6 邻居。

IP 地址	邻居设备的 IPv6 IP 地址。
类型	邻居的类型： <ul style="list-style-type: none">• 可达 - 已知可在 30 秒内到达此邻居。• 过时 - 已知不再能到达此邻居，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。
MAC 地址	邻居设备的 IPv6 MAC 地址。
供应商	邻居设备制造商的名称。
接口	与此邻居设备关联的接口。
超时	用户超时前的不活动时间长度。
清除	包含条目的删除图标。

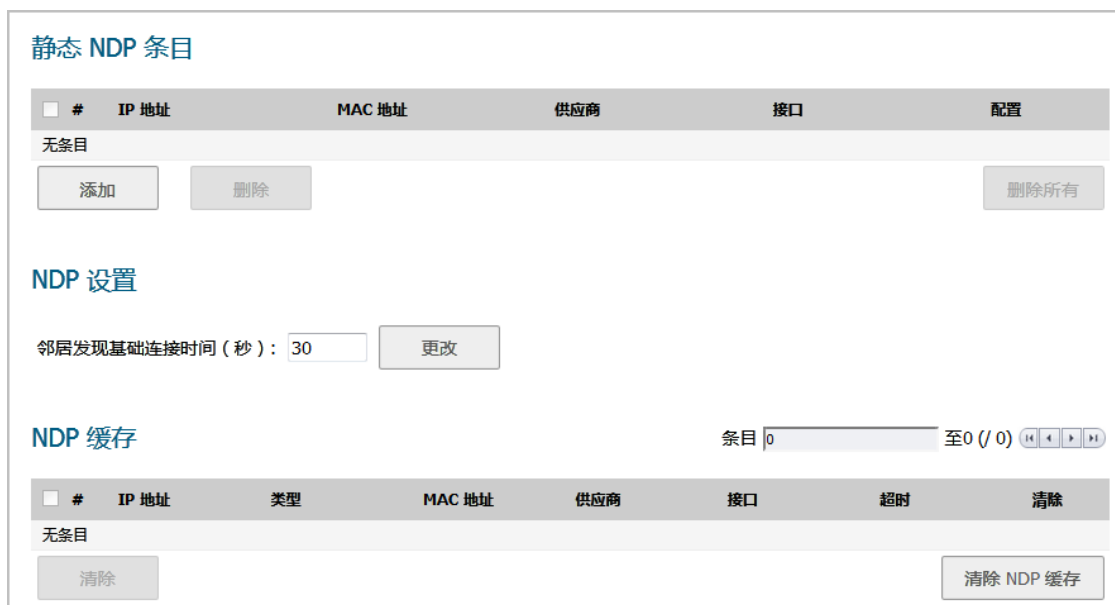
将显示以下类型的邻居：

- 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。

配置静态 NDP 条目

配置静态 NDP 条目的步骤如下：

- 1 转至网络 | 邻居发现页面。



- 2 在静态 NDP 条目表下方，单击添加。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 从接口中，选择 SonicWall 安全设备上将用于条目的接口。
- 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。

编辑静态 NDP 条目

配置静态 NDP 条目的步骤如下：

- 1 在静态 NDP 条目表中，单击配置列中该条目的编辑图标。将显示编辑静态 NDP 对话框。

- 2 做出更改。
- 3 单击确定。条目已更新。

清除 NDP 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 NDP 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 NDP 缓存中的物理地址相关联。清除 NDP 缓存可以在 NDP 缓存中收集和存储新信息。

提示：如需配置条目超时的具体时间长度，请在 **NDP 缓存条目超时（分钟）** 字段中输入以分钟为单位的值。请参阅第 417 页的 **NDP 设置**。

清除 NDP 缓存表中某个条目的步骤如下：

- 1 单击清除列中的删除图标。

清除 NDP 缓存表中一个或多个条目的步骤如下：

- 1 选中一个或多个要清除的条目的复选框。两个清除按钮随即激活。
- 2 单击清除或清除 NDP 缓存。

清除 NDP 缓存表中所有条目的步骤如下：

- 1 选中 NDP 缓存表标题中的复选框。两个清除按钮随即激活。
- 2 单击清除或清除 NDP 缓存。

配置 MAC-IP 反欺骗

- 第 420 页的[关于 MAC-IP 反欺骗保护](#)
 - 第 421 页的[IP 助手扩展](#)
- 第 421 页的[网络 | MAC-IP 反欺骗](#)
 - 第 422 页的[接口设置](#)
 - 第 423 页的[反欺骗缓存](#)
 - 第 425 页的[检测到的反欺骗列表](#)
- 第 425 页的[配置 MAC-IP 反欺骗保护](#)
 - 第 426 页的[显示流量统计信息](#)
 - 第 426 页的[编辑 IPv6 接口的 MAC-IP 反欺骗设置](#)
 - 第 427 页的[编辑 IPv4 接口的 MAC-IP 反欺骗设置](#)
 - 第 429 页的[将设备添加到反欺骗缓存中](#)
 - 第 429 页的[删除反欺骗缓存条目](#)
 - 第 430 页的[过滤所显示的内容](#)
 - 第 431 页的[从检测到的欺骗列表中添加静态条目](#)

关于 MAC-IP 反欺骗保护

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 反欺骗功能的作用集中体现在两个方面：

- 许可控制，用户可以利用它选择能访问网络的设备。
- 消除第 2 层的欺骗攻击，例如拒绝服务攻击。

为了实现上述目标，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进行构建：

- 基于 DHCP 服务器的租约（SonicWall - DHCP 服务器；仅限 IPv4）
- 基于 DHCP 中继的租约（SonicWall - IP 助手；仅限 IPv4）

- 静态 ARP 条目；仅限 IPv4
- 用户创建的静态条目

ARP 缓存是通过以下子系统构建的：

- ARP 数据包；包括 ARP 请求和响应；仅限 IPv4
- 来自用户创建的条目的静态 ARP 条目；仅限 IPv4
- 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）。这可以防止 SonicWall 安全设备根据映射将数据包路由到意外设备。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。

IP 助手扩展

为了支持来自 IP 助手的 DHCP 中继子系统的租约（网络 | IP 助手）：

- 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。
- 这些学习到的租约将作为 IP 助手状态同步消息的一部分同步到闲置的 SonicWall 安全设备。

将来自这些租约的 MAC 和 IP 地址绑定传输到 MAC-IP 反欺骗缓存。

如需 IP 助手的更多信息，请参阅第 460 页的[使用 IP 助手](#)。

网络 | MAC-IP 反欺骗

IPv6

针对 X0 接口
视图 IP 版本: IPv4 IPv6

接口	强制的	启用	NDP 锁定	静态 NDP	欺骗检测	允许管理	配置
X0						✔	⚙️

反欺骗缓存 项目 0 至 0 (0) ⏪ ⏩

<input type="checkbox"/> IP 地址	类型	接口	MAC 地址	供应商	主机名称	路由	黑名单	配置
无条目								

添加
删除
清除统计
刷新
过滤

IPv6 反欺骗查找统计信息：条目数 0、查找数 0、通过数 0、丢弃数 0、成功数 0、通过数 (发送给我们) 0

检测到的欺骗列表 条目 0 至 0 (0) ⏪ ⏩

IP 地址	接口	MAC 地址	供应商	名称	数据包	添加
无条目						

清除
解析
刷新
过滤

IPv4

针对 X0 接口 视图 IP 版本: IPv4 IPv6

接口	强制的	启用	ARP 锁定	ARP 监控	静态 ARP	DHCP 服务器	DHCP 中继	欺骗检测	允许管理	配置
X0		<input checked="" type="checkbox"/>						<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

反欺骗缓存 项目 0 至 0 (/ 0)

IP 地址	类型	接口	MAC 地址	供应商	主机名称	路由	黑名单	配置
无条目								

添加 删除 清除统计 刷新 过滤

反欺骗查找统计信息: 条目数 0、查找数 0、通过数 0、丢弃数 0、成功数 0、通过数 (发送给我们) 0

检测到的欺骗列表 条目 0 至 0 (/ 0)

IP 地址	接口	MAC 地址	供应商	名称	数据包	添加
无条目						

清除 解析 刷新 过滤

本章节介绍如何计划、设计和在 SonicWall SonicOS 中实施 MAC-IP 反欺骗反欺骗保护。

主题:

- 第 422 页的[接口设置](#)
- 第 423 页的[反欺骗缓存](#)
- 第 425 页的[检测到的反欺骗列表](#)

接口设置

注: 绿色复选标记图标表示已启用了哪些设置。

IPv6

针对 X1 接口 视图 IP 版本: IPv4 IPv6

接口	强制的	启用	NDP 锁定	静态 NDP	欺骗检测	允许管理	配置
X1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

接口设置

列出可以应用 MAC-IP 反欺骗设置的所有接口。显示的默认值为全部。

接口

从接口的设置中选择的接口。

强制的

指示是否对此接口实施入口反欺骗。

启用

指示是否对此接口启用 MAC-IP 反欺骗。

NDP 锁定

指示是否对此接口上的每个传输数据包启用 MAC-IP 反欺骗检查。

静态 NDP

指示是否为每个静态 NDP 条目创建对应的 MAC-IP 反欺骗表条目。

欺骗检测

指示是否为不匹配反欺骗缓存的数据包创建 MAC-IP 反欺骗检测列表。

注：从 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
- 第 2 层网桥对接口
- 高可用性接口
- 高可用性数据接口

允许管理

指示在无有效的 MAC-IP 反欺骗缓存的情况下是否允许所有发送到安全设备的流量。

配置

包含条目的统计和编辑图标。

IPv4

接口	强制的	启用	ARP 锁定	ARP 监控	静态 ARP	DHCP 服务器	DHCP 中继	欺骗检测	允许管理	配置
X0	✓	✓	✓	✓	✓	✓	✓	✓	✓	 

接口设置

列出可以应用 MAC-IP 反欺骗设置的所有接口。显示的默认值为全部。

接口

从接口的设置中选择的接口。

强制的

指示是否对此接口实施入口反欺骗。

启用

指示是否对此接口启用 MAC-IP 反欺骗。

ARP 锁定

指示是否对此接口上的每个传输数据包启用 MAC-IP 反欺骗检查。

ARP 监控

指示是否启用阻止连接的机器 ARP 中毒。

静态 ARP

指示是否为每个静态 ARP 条目创建对应的 MAC-IP 反欺骗表条目。

DHCP 服务器

指示是否根据 DHCP 租赁（MAC-IP 反欺骗的 DHCP 服务器）填写 SonicWall 条目。

DHCP 中继

指示是否根据 DHCP 租赁（DHCP 中继 - IP 助手）填写 MAC-IP 反欺骗条目。

欺骗检测

指示是否为不匹配反欺骗缓存的数据包创建 MAC-IP 反欺骗检测列表。

注：从 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
- 第 2 层网桥对接口
- 高可用性接口
- 高可用性数据接口

允许管理

指示是否无需有效的 MAC-IP 反欺骗缓存就可以允许所有发送到防火墙的流量。

配置

包含条目的统计和编辑图标。

反欺骗缓存

MAC-IP 反欺骗缓存列出了所有 MAC 地址到 IP 地址的绑定，其中包括目前符合下列条件的所有设备：

- 列为“已获授权”访问网络。
- 标记为可以像后接网络的路由器一样工作的设备。
- 标记为已加入网络“黑名单”（拒绝访问）。

即使已启用 MAC-IP 反欺骗功能，仍将绕过一些数据包类型：

- 非 IP 数据包。
- 源 IP 为 0 的 DHCP 数据包。
- 来自 VPN 隧道的数据包。
- 使用无效的单播 IP 作为其源 IP 的数据包。
- 来自未在反欺骗设置下启用管理状态的接口的数据包。

反欺骗查找统计信息显示在表的底部。

反欺骗缓存

<input type="checkbox"/> IP 地址	类型	接口	MAC 地址	供应商	主机名称	路由	黑名单	配置
无条目								

反欺骗查找统计信息：条目数 0、查找数 0、通过数 0、丢弃数 0、成功数 0、通过数 (发送给我们) 0

IP 地址	设备的 IP 地址
类型	条目的类型：静态或租约
接口	接收传入流量的接口
MAC 地址	设备的 MAC 地址
供应商	设备的制造商（如已知）
主机名称	设备的主机名（如已知）
路由	在配置设备时将其指定为可能的路由器
黑名单	在配置设备时将其指定为已加入黑名单
配置	显示每个条目的统计信息、编辑和删除图标

清除一个或多个设备上的缓存统计信息的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 选择一个或多个设备。
- 3 单击清除统计信息。

查看可用的最新缓存信息的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 单击反欺骗缓存表底部的刷新。

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反欺骗缓存表中的静态反欺骗条目。



IP 地址	设备的 IP 地址。
接口	接收传入流量的接口。
MAC 地址	设备的 MAC 地址。
供应商	设备的制造商（如已知）。
名称	设备的名称。
数据包	已接收的数据包数。
添加	显示编辑图标。

从欺骗检测列表中清空条目的步骤如下：

- 1 单击清除。

使用 NetBios 解析每个设备的名称的步骤如下：

- 1 单击解析。

查看可用的最新缓存信息的步骤如下：

- 1 单击检测到的欺骗列表底部的刷新。

配置 MAC-IP 反欺骗保护

主题：

- [第 426 页的显示流量统计信息](#)
- [第 426 页的编辑 IPv6 接口的 MAC-IP 反欺骗设置](#)
- [第 427 页的编辑 IPv4 接口的 MAC-IP 反欺骗设置](#)
- [第 429 页的将设备添加到反欺骗缓存中](#)
- [第 429 页的删除反欺骗缓存条目](#)
- [第 430 页的过滤所显示的内容](#)
- [第 431 页的从检测到的欺骗列表中添加静态条目](#)

显示流量统计信息

在“设置”或“反欺骗缓存”表中显示接口的流量统计信息的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 如需在设置表中显示接口的流量统计信息，请从接口的设置中选择要显示的接口；默认值为全部。
- 3 将鼠标指针悬停在接口的统计信息图标上。
- 4 将显示流量统计信息弹出窗口：

设置表



反欺骗缓存表



编辑 IPv6 接口的 MAC-IP 反欺骗设置

为特定接口配置 MAC-IP 反欺骗设置的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 在接口的设置表中，单击所需接口的配置图标。将显示编辑 MAC-IP 反欺骗设置对话框。



- 3 如需通过此接口启用基于反欺骗的 MAC 地址和 IP 地址流量，请在反欺骗设置部分中选中启用 - 启用基于 MAC-IP 的反欺骗。默认情况下未选中该选项。
- 4 如需在 MAC-IP 反欺骗表中为每个静态 NDP 条目创建相应的条目，请选中静态 NDP - 根据静态 NDP 条目填充 MAC-IP 反欺骗。默认情况下未选中该选项。
- 5 如需为反欺骗缓存内的每个 MAC-IP 绑定添加一个 NDP 缓存条目，请在 NDP 设置部分中选中 NDP 锁定 - 锁定 NDP 缓存中的 MAC-IP 绑定以避免其他设备遭受 NDP 中毒。默认情况下未选中该选项。
- 6 如需对每个中转数据包启用 MAC-IP 反欺骗检查，请在其他设置部分中选中强制 - 强制入口反欺骗 - 丢弃不匹配 MAC-IP 反欺骗缓存的数据包。默认情况下未选中该选项。
- 7 如需为每个未通过 MAC-IP 反欺骗缓存检查的设备创建一个欺骗检测列表，请选中欺骗检测 - 为不匹配反欺骗缓存的数据包创建 MAC-IP 欺骗检测列表。默认情况下未选中该选项。
- 8 如需允许发送到安全设备的所有流量（包括在没有有效 MAC-IP 反欺骗缓存的情况下），请选中允许管理 - 在没有有效的 MAC-IP 反欺骗缓存的情况下允许所有发送到该盒子的流量。默认情况下已选中该选项。

小心： 如果禁用了此选项，系统可能会阻止您通过此接口登录 SonicWall 安全设备。确保您有其他接口可用于管理安全设备，并且有适当的规则和策略。如果禁用了此选项，则将显示一条警告消息：

您确定吗？禁用管理可能会锁定您通过这个接口登录到防火墙。请确定您有其他可用的接口用于管理盒子并且防火墙规则已设置。

- 9 单击确定。

编辑 IPv4 接口的 MAC-IP 反欺骗设置

为特定接口配置 MAC-IP 反欺骗设置的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 在接口的设置表中，单击所需接口的配置图标。将显示编辑 MAC-IP 反欺骗设置对话框。

接口： X1`

反欺骗设置

- 启用 - 启动基于 MAC-IP 的反欺骗。`
- 静态 ARP - 对于所有的静态 ARP 项，一个相应 MAC-IP 项将被创建在反欺骗表中。`
- DHCP 服务器 - 从 DHCP 租赁 (SonicWall 的 DHCP 服务器) 获得 MAC-IP 反欺骗条目。`
- DHCP 中继 - 从 DHCP 租赁 (DHCP 中继 - IP 助手) 获得 MAC-IP 反欺骗条目。`

ARP 设置

- ARP 锁定 - 在 ARP 缓存中锁定 MAC-IP 以阻止别处 ARP 中毒。`
- ARP 监控 - 阻止连接的机器 ARP 中毒。`

杂项设置

- 加强 - 加强入口反欺骗 - 丢弃数据包不匹配 MAC-IP 反欺骗缓存。`
- 欺骗检测 - 为丢失的数据包创建 MAC-IP 欺骗检测列表以匹配反欺骗缓存。`
- 允许管理 - 无需有效的 MAC-IP 反欺骗缓存就可以允许所有发到该盒子的流量。`

- 3 如需通过此接口启用基于反欺骗的 MAC 地址和 IP 地址流量，请在反欺骗设置部分中选中启用 - 启用基于 **MAC-IP** 的反欺骗。默认情况下未选中该选项。
- 4 如需在 MAC-IP 反欺骗表中为每个静态 ARP 条目创建相应的条目，请选中静态 **ARP** - 根据静态 **ARP** 条目填充 **MAC-IP** 反欺骗。默认情况下未选中该选项。
- 5 如需在 MAC-IP 反欺骗反欺骗表中为 DHCP 服务器分配的每个 DHCP 租约创建相应的条目，请选中 **DHCP 服务器** - 根据 **DHCP** 租约 (**SonicWall** 的 **DHCP** 服务器) 填充 **MAC-IP** 反欺骗条目。默认情况下未选中该选项。
- 6 如需在 MAC-IP 反欺骗反欺骗表中根据 DHCP 中继配置为远程 DHCP 服务器分配的每个 DHCP 租约创建相应的条目，请选中 **DHCP 中继** - 根据 **DHCP** 租约 (**DHCP** 中继 - **IP** 助手) 填充 **MAC-IP** 反欺骗条目。默认情况下未选中该选项。
- 7 如需为反欺骗缓存内的每个 MAC-IP 绑定添加一个 ARP 缓存条目，请在 **ARP** 设置部分中选中 **ARP** 锁定 - 锁定 **ARP** 缓存中的 **MAC-IP** 绑定以避免其他设备遭受 **ARP** 中毒。默认情况下未选中该选项。
- 8 如需防止已连接的设备发生 ARP 中毒，并保护所有客户端 PC 免受中间人攻击，请选中 **ARP** 监控 - 避免已连接的机器发生 **ARP** 中毒。默认情况下未选中该选项。
- 9 如需对每个中转数据包启用 MAC-IP 反欺骗检查，请在其他设置部分中选中强制 - 强制入口反欺骗 - 丢弃不匹配 **MAC-IP** 反欺骗缓存的数据包。默认情况下未选中该选项。
- 10 如需为每个未通过 MAC-IP 反欺骗缓存检查的设备创建一个欺骗检测列表，请选中欺骗检测 - 为不匹配反欺骗缓存的数据包创建 **MAC-IP** 欺骗检测列表。默认情况下未选中该选项。

- 11 如需允许发送到安全设备的所有流量（包括在没有有效 MAC-IP 反欺骗缓存的情况下），请选中允许管理 - 在没有有效的 MAC-IP 反欺骗缓存的情况下允许所有发送到该盒子的流量。默认情况下已选中该选项。

小心：如果禁用了此选项，系统可能会阻止您通过此接口登录 SonicWall 安全设备。确保您有其他接口可用于管理安全设备，并且有适当的规则和策略。如果禁用了此选项，则将显示一条警告消息：

您确定吗？禁用管理可能会锁定您通过这个接口登录到防火墙。请确定您有其他可用的接口用于管理盒子并且防火墙规则已设置。

- 12 单击确定。

将设备添加到反欺骗缓存中

向反欺骗缓存中添加设备的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 单击反欺骗缓存表下方的添加。将显示添加静态 MAC-IP 反欺骗对话框。

接口： X0

IPv6 地址：

MAC 地址：

路由器（存在于此设备后的网络）。`

记于黑名单列表中的设备`

- 3 从接口中，选择来自设备的流量到达的接口。
- 4 在 IP 地址字段，输入设备的 IP 地址。
- 5 在 MAC 地址字段，输入设备的 MAC 地址。
- 6 如需将设备指定为可能后接网络的路由器，请选中路由器。默认情况下已选中该选项。
- 7 如需将设备加入黑名单并阻止来自该设备的流量，请选中记于黑名单列表中的设备。默认情况下未选中该选项。

将设备加入黑名单会导致阻止来自此设备的数据包（无论设备的 IP 地址如何）。

- 8 单击确定。

删除反欺骗缓存条目

删除单个静态反欺骗缓存条目的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 单击条目的删除图标。

删除一个或多个静态反欺骗缓存条目的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 选择要删除的条目。删除按钮随即激活。
- 3 单击删除。

删除所有静态反欺骗缓存条目的步骤如下

- 1 转至网络 | MAC-IP 反欺骗。
- 2 选中反欺骗缓存表标题中的复选框。删除按钮随即激活。
- 3 单击删除。

过滤所显示的内容

通过使用过滤器功能，可以在反欺骗缓存和检测到的欺骗列表表中只显示特定设备。

过滤表显示的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 在要过滤的表下方的“过滤器”字段中，指定设备的 IP 地址、接口、MAC 地址、主机名或名称。必须使用 [过滤器操作符语法选项](#) 表中显示的运算符的相应语法来填写该字段

过滤器操作符语法选项

运算符	语法选项
包含类型的值	<ul style="list-style-type: none">• Ip=1.1.1.1 或 ip=1.1.1.0/24• Mac=00:01:02:03:04:05• lface=x1
字符串	<ul style="list-style-type: none">• X1• 00:01• Tst-mc• 1.1.
和	<ul style="list-style-type: none">• Ip=1.1.1.1;lface=x1• Ip=1.1.1.0/24;lface=x1;just-string
或	<ul style="list-style-type: none">• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24• lface=x1,x2,x3
负值	<ul style="list-style-type: none">• !ip=1.1.1.1;!just-string• !lface=x1,x2
混合	<ul style="list-style-type: none">• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05;just-string;lface=x1,x2

从检测到的欺骗列表中添加静态条目

从“检测到的欺骗列表”中添加静态条目的步骤如下：

- 1 转至网络 | MAC-IP 反欺骗。
- 2 在检测到的欺骗列表中，单击所需设备的添加列下面的编辑图标。将显示一条警告消息，询问您是否要添加此静态条目。
- 3 单击确定。

设置 DHCP 服务器

- 第 432 页的[网络 | DHCP 服务器](#)
 - 第 434 页的[DHCP 服务器选项功能](#)
 - 第 435 页的[每个接口上的多个 DHCP 作用域](#)
 - 第 437 页的[关于 DHCP 服务器的持续性](#)
 - 第 437 页的[配置 DHCP 服务器](#)
 - 第 439 页的[DHCP 服务器租用范围](#)
 - 第 439 页的[当前 DHCP 租用](#)
- 第 441 页的[配置高级选项](#)
 - 第 441 页的[配置高级 DHCP 服务器选项](#)
 - 第 446 页的[配置用于动态范围的 DHCP 服务器](#)
 - 第 451 页的[配置静态 DHCP 条目](#)
 - 第 453 页的[配置用于 DHCP 租用范围的 DHCP 常规选项](#)
 - 第 453 页的[RFC 定义的 DHCP 选项编号](#)
 - 第 459 页的[DHCP 和 IPv6](#)

网络 | DHCP 服务器

IPv6 和 IPv4 版本的[网络 | DHCP 服务器](#)之间只有细微的差别。

IPv6 网络 | DHCP 服务器

DHCPv6 服务器设置

视图 IP 版本: IPv4 IPv6

启用 DHCPv6 服务器 高级

DHCPv6 服务器租约范围

条目 0 至 0 (0)

视图类型: 所有 动态 静态

#	类型	前缀	租约范围	细节	启用	配置
无条目						

添加动态 添加静态 删除 全部删除

目前 DHCPv6 租约

条目 0 至 0 (0)

#	IPv6 地址	租约过期	IAID	DUID	类型	删除
当前无任何租约。						

删除 刷新 全部删除

目前: 0. 剩余: 16384. 可用动态: 0. 可用静态: 0. 所有可用: 0. 所有配置: 0.

IPv4 网络 | DHCP 服务器

DHCPv4 服务器设置

视图 IP 版本: IPv4 IPv6

启用 DHCPv4 服务器 高级

启用冲突检测

启用 DHCP 服务器租约保持

DHCP 服务器租约保持监测的间隔: 5 分钟

DHCPv4 服务器租约范围

条目 1 至 2 (2)

视图类型: 所有 动态 静态

#	类型	租约范围	接口	细节	启用	配置
1	动态	范围: 172.16.16.84 - 172.16.16.252	X2:V402		<input checked="" type="checkbox"/>	
2	动态	范围: 192.168.94.84 - 192.168.94.254	X2		<input checked="" type="checkbox"/>	

添加动态 添加静态 删除 全部删除

目前 DHCPv4 租约

条目 1 至 2 (2)

#	IP 地址	主机名	租约过期	以太网地址	供应商	类型	删除
1	192.168.94.229		2017-12-20 16:40:38	00:0C:29:C8:18:23	VMWARE	动态	
2	192.168.94.246		2017-12-20 16:10:10	00:0C:29:C8:18:23	VMWARE	动态	

删除 刷新 全部删除

目前: 2. 可用动态: 337. 可用静态: 0. 所有可用: 340. 所有配置: 340.

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 服务器包括配置安全设备的 DHCP 服务器的设置。

您可以使用安全设备的 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，请确保已取消选中启用 DHCP 服务器。

安全设备的 DHCP 服务器能分配的地址范围和 IP 地址数量取决于防火墙的型号、操作系统和许可证。允许的最大 DHCP 租用数表显示了 SonicWall 安全设备允许的最大 DHCP 租约数。

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
	16384	NSA 6600	16384	TZ600	4096
SM 9600	16384	NSA 5600	8192	TZ500/TZ500 W	4096
SM 9400	16384	NSA 4600	8192	TZ400/TZ400 W	4096
SM 9200	16384	NSA 3600	4096	TZ300/TZ300 W	4096
		NSA 2600	4096	SOHO W	4096

主题：

- [第 434 页的 DHCP 服务器选项功能](#)
- [第 435 页的每个接口上的多个 DHCP 作用域](#)
- [第 437 页的关于 DHCP 服务器的持续性](#)
- [第 437 页的配置 DHCP 服务器](#)
- [第 439 页的 DHCP 服务器租用范围](#)
- [第 439 页的当前 DHCP 租用](#)
- [第 441 页的配置高级 DHCP 服务器选项](#)
- [第 446 页的配置用于动态范围的 DHCP 服务器](#)
- [第 451 页的配置静态 DHCP 条目](#)
- [第 453 页的配置用于 DHCP 租用范围的 DHCP 常规选项](#)
- [第 453 页的 RFC 定义的 DHCP 选项编号](#)
- [第 459 页的 DHCP 和 IPv6](#)

DHCP 服务器选项功能

SonicWall DHCP 服务器选项功能为 DHCP 选项（也称为“供应商扩展”，基本定义请参阅 RFC 2131 和 2132）提供支持。DHCP 选项使用户能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 453 页的 RFC 定义的 DHCP 选项编号](#)部分按 RFC 分配的选项编号列出 DHCP 选项。

主题：

- [第 435 页的优点](#)
- [第 435 页的 DHCP 服务器选项功能如何工作](#)
- [第 435 页的支持的标准](#)

优点

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 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 435 页的什么是每个接口上的多个 DHCP 作用域？](#)
- [第 435 页的多个 DHCP 作用域的优点](#)
- [第 436 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 客户端和服务端都驻留在同一 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，不论它来自 VPN 隧道还是 DHCP 中继代理。
用于站点到站点的多个作用域	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）”选项。

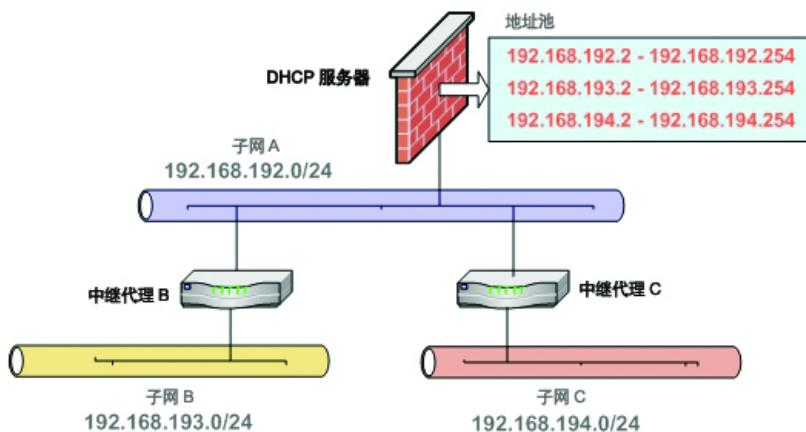
兼容冲突检测 目前，在启用此功能时，DHCP 服务器将执行服务器端冲突检测。服务器端冲突检测的优势在于，即使在 DHCP 客户端未运行客户端冲突检测时，它仍会检测冲突。但是，如果网络中有大量 DHCP 客户端，服务器端冲突检测可能导致更长的等待时间，等待完成完整的 IP 地址分配。对于属于“中继”子网范围的 IP 地址，将不执行冲突检测（和网络预发现）。DHCP 服务器仅对连接到其接口的子网范围执行冲突检测 ICMP 检查。

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 客户端和服务端驻留在同一 IP 网络或子网。

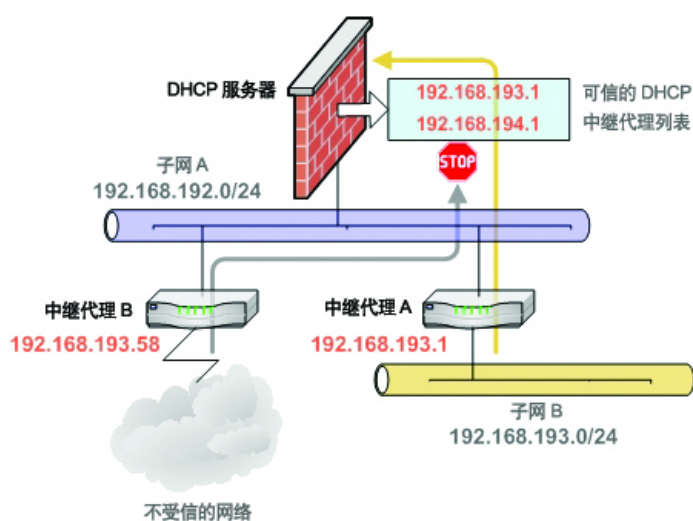
如果 DHCP 客户端及其关联的 DHCP 服务器不在同一子网中，需要某种类型的第三方代理（BOOTP 中继代理、IP 助手等）在客户端与服务端之间传输 DHCP 消息；请参阅[共享同一 DHCP 服务器的多个子网](#)。DHCP 中继代理使用其入口接口 IP 地址填充 giaddr 字段，然后将其转发至已配置的 DHCP 服务器。当 DHCP 服务器收到消息时，它会查看 giaddr 字段，以确认其是否拥有能用来向客户端提供 IP 地址租用的 DHCP 作用域。

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 高级设置对话框利用“可信的代理”选项卡提供安全性，此选项卡用于指定可信的 DHCP 中继代理；请参阅[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。

可信的 DHCP 中继代理



关于 DHCP 服务器的持续性

DHCP 服务器持续性是安全设备保存 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。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。在通常出于维护或升级原因重启防火墙时，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。

配置 DHCP 服务器

使用 SonicWall 安全设备的 DHCP 服务器的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | DHCP 服务器。
- 2 从查看 IP 版本中选择要使用的 IP 版本：
 - IPv4

DHCPv4 服务器设置

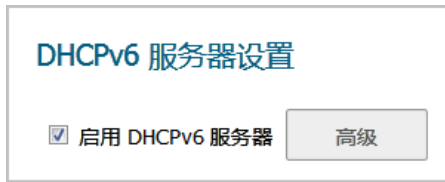
启用 DHCPv4 服务器 高级

启用冲突检测

启用 DHCP 服务器租约保持

DHCP 服务器租约保持监测的间隔: 分钟

- IPv6



- 3 如需向您的网络客户端分配 IP 地址、子网掩码、网关地址及 DNS 服务器地址，请选中启用 **DHCPv4/6 服务器**。默认情况下已选中该选项。高级，并且对于 IPv4，服务器设置选项将激活。
- 4 如需配置 DHCPv6，请转至 [步骤 7](#)。
- 5 如需在另一个 DHCP 服务器存在的情况下在每个区域中开启自动 DHCP 作用域冲突检测，请选中 **启用冲突检测**。默认情况下已选中该选项。

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。

- 6 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。默认情况下已选中该选项。选择此选项后，**DHCP 服务器持久性监控间隔**选项将激活。
 - 如需控制检查网络中的更改以及必要时将这些更改写入 Flash 的频率，请在 **DHCP 服务器持久性监控间隔**中输入时间（分钟）。默认值为 5 分钟，最小值为 5 分钟，最大值为 1440 分钟（24 小时）。
- 7 如需配置选项对象、选项群组和可信的代理，请单击高级。如需这些功能的配置的详细信息，请参阅第 441 页的 [配置高级 DHCP 服务器选项](#)。
- 8 单击接受。

主题：

- 第 438 页的 [为 DNS 代理配置 DHCP 服务器](#)
- 第 440 页的 [目前 DHCPv4 租约](#)

为 DNS 代理配置 DHCP 服务器

在接口上启用 DNS 代理时，设备需要将接口 IP 作为 DNS 服务器地址推送到客户端，因此用户需要手动配置 DHCP 服务器：在 **DNS/WINS** 选项卡上将接口地址用作 DHCP 服务器设置中的 **DNS 服务器 1** 地址。在 DHCP 页面中，**接口预绑定**复选框使这一步骤变得更易配置；如果所选接口已启用 DNS 代理，DNS 服务器 IP 将自动添加到 **DNS/WINS** 页面中。

DHCP 服务器租用范围

DHCPv6 服务器租用范围

DHCPv6 服务器租用范围

条目 0 至 0 (/ 0) [Navigation icons]

视图类型: 所有 动态 静态

<input type="checkbox"/>	#	类型	前缀	租用范围	细节	启用	配置
无条目							

DHCPv4 服务器租用范围

DHCPv4 服务器租用范围

条目 1 至 2 (/ 2) [Navigation icons]

视图类型: 所有 动态 静态

<input type="checkbox"/>	#	类型	租用范围	接口	细节	启用	配置
<input checked="" type="checkbox"/>	1	动态	范围: 172.16.16.84 - 172.16.16.252	X2:V402	[Info icon]	<input checked="" type="checkbox"/>	[Edit] [Delete]
<input checked="" type="checkbox"/>	2	动态	范围: 192.168.94.84 - 192.168.94.254	X2	[Info icon]	<input checked="" type="checkbox"/>	[Edit] [Delete]

DHCP 服务器租用范围表中显示了当前已配置的 DHCP IP 范围。

- 类型: 动态或静态。
- 前缀: 仅 IPv6。
- 租用范围: IP 地址范围, 例如 172.16.31.2 - 172.16.31.254。
- 接口: 仅 IPv4。将该范围分配到的接口。
- 细节: 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: 选中此复选框以启用 DHCP 范围。清除复选框将禁用该范围。
- 配置: 包含表条目的配置和删除图标。

当前 DHCP 租用

主题:

- 第 440 页的 [目前 DHCPv6 租约](#)
- 第 440 页的 [目前 DHCPv4 租约](#)

目前 DHCPv6 租约

目前 DHCPv6 租约 条目 0 至 0 (0) << >>

<input type="checkbox"/>	#	IPv6 地址	租约过期	IAID	DUID	类型	删除
当前无任何租约。							

目前: 0. 剩余: 16384. 可用动态: 0. 可用静态: 0 所有可用: 0. 所有配置: 0.

当前 DHCP 租用信息显示在当前 DHCP 租用表中。每个绑定条目将显示：

- IPv6 地址
- 租约过期
- IAID
- DUID
- 绑定类型（动态、动态 BOOTP 或静态 BOOTP）
- 删除图标

删除某个绑定，从而释放 DHCP 服务器上的 IP 地址的步骤如下：

- 1 单击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。
- 2 单击接受。

目前 DHCPv4 租约

目前 DHCPv4 租约 条目 1 至 2 (2) << >>

<input type="checkbox"/>	#	IP 地址	主机名	租约过期	以太网地址	供应商	类型	删除
<input type="checkbox"/>	1	192.168.94.229		2017-12-20 16:40:38	00:0C:29:C8:18:23	VMWARE	动态	<input type="button" value="X"/>
<input type="checkbox"/>	2	192.168.94.246		2017-12-20 16:10:10	00:0C:29:C8:18:23	VMWARE	动态	<input type="button" value="X"/>

目前: 2. 可用动态: 337. 可用静态: 0. 所有可用: 340. 所有配置: 340.

当前 DHCP 租用信息显示在当前 DHCP 租用表中。每个绑定条目将显示：

- IP 地址
- 主机名
- 租约过期
- 以太网地址
- 供应商
- 绑定类型（动态、动态 BOOTP 或静态 BOOTP）
- 删除图标

删除某个绑定，从而释放 DHCP 服务器上的 IP 地址的步骤如下：

- 1 单击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。
- 2 单击接受。

配置高级选项

主题：

- 第 441 页的[配置高级 DHCP 服务器选项](#)

配置高级 DHCP 服务器选项

i | 注：配置 DHCP 服务器选项在 IPv4 和 IPv6 上基本相同。例外情况将在过程中说明。

主题：

- 第 441 页的[配置 DHCP 选项对象](#)
- 第 443 页的[配置 DHCP 选项群组](#)
- 第 445 页的[配置可信的 DHCP 中继代理地址群组（仅限 IPv4）](#)
- 第 445 页的[启用可信的 DHCP 中继代理](#)

第 453 页的 RFC 定义的 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 转至管理 | 系统设置 | 网络 | DHCP 服务器。
- 2 在 DHCPv4/6 服务器设置下，单击高级。将显示 DHCP 高级设置对话框。

IPv6 DHCP 高级设置

选项对象 选项群组

选项对象 条目 0 至 0 (0)

#	名称	选项细节	类型	配置
无条目				

ADD OPTION 删除 全部删除

IPv4 DHCP 高级设置

- 单击添加选项。此时会显示添加 DHCP 选项对象对话框。

- 在选项名称字段中输入选项的名称。
- 从选项编号中，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 453 页的 RFC 定义的 DHCP 选项编号。
- 如果选项数组：
 - 显示为灰色，请转至步骤 8。
 - 可用，可以选择它以允许在选项值字段中输入多个选项值。
- 如果：
 - 只有一个选项类型可用（例如，对于选项编号 2（时间偏移）），选项数组将显示为灰色。转至步骤 8。
 - 有多个选项类型可用（例如，对于选项编号 77（用户类信息）），选项类型将激活并显示选项类型。如果：
 - 只有一种选项类型与选项编号关联，选项类型将显示为灰色。转至步骤 8。
 - 多个选项类型与选项编号关联，选项类型将激活并列出选项。选择选项类型。
- 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。
- 单击确定。该对象显示在选项对象表中。

DHCPv6 选项对象表

选项对象 选项群组

选项对象 条目 1 至 1 (/1) << >>

<input type="checkbox"/> #	名称	选项细节	类型	配置
<input type="checkbox"/> 1	DHCP Option 1	21/30.40.50.60;40.50.60.70	域名	 

ADD OPTION 删除 全部删除

DHCPv4 选项对象表

选项对象 选项群组 可信的代理

选项对象 项目 1 至 0 (/0) << >>

<input type="checkbox"/> #	名字	选项细节	类型	配置
<input type="checkbox"/> 1	DHCP Option 1	2/12	4 个字节的数据	 

ADD OPTION 删除 全部删除

配置 DHCP 选项群组

配置 DHCP 选项群组的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | DHCP 服务器。
- 2 在 DHCPv4/6 服务器设置下，单击高级。将显示 DHCP 高级设置对话框。

IPv6 DHCP 高级设置

选项对象 选项群组

选项对象 条目 0 至 0 (/0) << >>

<input type="checkbox"/> #	名称	选项细节	类型	配置
无条目				

ADD OPTION 删除 全部删除

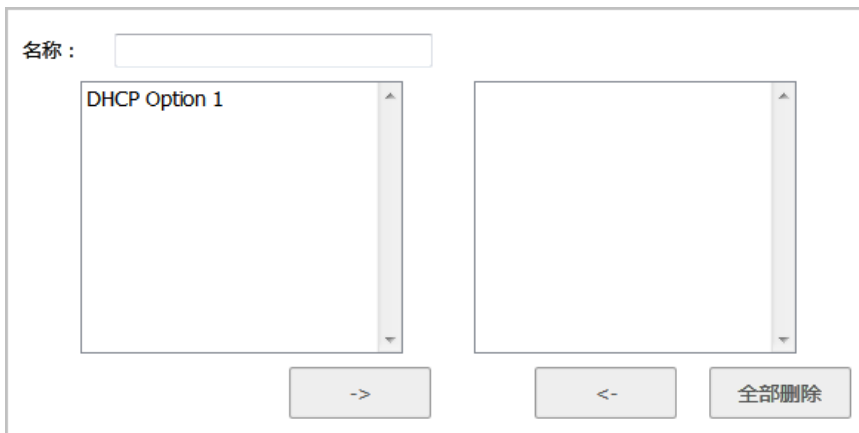
IPv4 DHCP 高级设置



- 3 单击选项群组。



- 4 单击添加组。将显示添加 DHCP/v6 选项群组对话框。



- 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，然后单击向右箭头按钮，将该选项对象添加到群组中。如需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。

DHCPv6 选项群组表

选项群组		条目 1 至 1 (/ 1)		
#	名称	选项细节	类型	配置
1	DHCP Option Group 1		组	 
	DHCP Option 1	21/30.40.50.60;40.50.60.70	域名	 

添加群组 删除 全部删除

DHCPv4 选项群组表

选项组		项目 1 至 1 (/ 1)		
#	名字	选项细节	类型	配置
1	DHCP Option Group 1		组	 
	DHCP Option 1	2/12	4 个字节的数据	 

添加群组 删除 全部删除

配置可信的 DHCP 中继代理地址群组（仅限 IPv4）

如需配置默认受信中继代理列表地址组，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默认受信中继代理列表地址组或自定义地址组中。

地址对象和地址群组在 **管理 | 策略 | 对象 > 地址对象** 中配置。如需配置地址对象和地址群组的方法信息，请参阅 SonicOS 策略。

启用可信的 DHCP 中继代理

在 **DHCP 高级设置** 对话框中，可以使用默认受信中继代理列表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。

启用受信中继代理列表选项且选择所需地址群组的步骤如下：

- 1 转至 **管理 | 系统设置 | 网络 | DHCP 服务器**。
- 2 在 **DHCPv4/6 服务器设置** 下，单击 **高级**。将显示 **DHCP 高级设置** 对话框。
- 3 单击 **可信的代理**。

可信的 DHCP 中继代理列表

启用可信的 DHCP 中继代理列表

可信的中继代理列表：

注：当该服务器被作为一个内部的 DHCP 服务器分配给 DHCP over VPN 中央网关，来自 VPN 隧道的 DHCP 消息总是被绕过。

- 选中启用可信的 DHCP 中继代理列表。默认情况下未选中该选项。可信的中继代理列表将激活。

启用可信的 DHCP 中继代理列表

可信的中继代理列表：

- 从可信的中继代理列表中选择地址群组。此下拉菜单包含所有的现有地址群组以及创建新地址对象群组选项。

i 注：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对话框。如需配置地址群组的方法信息，请参阅 SonicOS 策略。

- 单击确定以使用所选地址群组来启用可信的中继代理列表选项。

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。

配置用于动态 IP 地址范围的 DHCP 服务器的步骤如下：

- 转至管理 | 系统设置 | 网络 | DHCP 服务器。
- 在 DHCPv4/6 服务器租用范围表下，单击添加动态。对于：
 - IPv6，将显示添加 DHCPv6 动态范围对话框。转至第 447 页的添加 DHCPv6 动态范围。
 - IPv4，将显示动态范围配置对话框。转至第 448 页的动态范围配置。

添加 DHCPv6 动态范围

常规 DNS 高级

动态 DHCPv6 范围设置

启用该 DHCPv6 范围

名称:

前缀: /64

起始范围:

终止范围:

有效生命期 (分钟):

首选生命期 (分钟):

备注:

- 1 如需启用此范围，请确保启用该 **DHCPv6** 范围处于选中状态。默认情况下已选中该选项。
- 2 在名称字段中，输入范围的名称。
- 3 在前缀字段中，输入范围用于分配 IPv6 地址的前缀。
- 4 分别在起始范围和终止范围字段中输入起始范围和终止范围。这两个地址都必须在前缀的范围内。
- 5 在有效生命期字段中，输入由范围租用的 IPv6 地址的有效生命期（分钟）。最小值为 0，最大值为 71582789，默认值为 **2160**。
- 6 在首选生命期字段中，输入由范围租用的 IPv6 地址的首选生命期（分钟）。最小值为 0，最大值为 71582789，默认值为 **1440**。
- 7 可以选择在备注字段中输入备注。
- 8 单击 **DNS**。

DNS

DNS 服务器

域名:

从 SonicWall DNS 动态继承 DNS 设置

手动指定

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

- 1 在域名字段中，输入域名。
- 2 选择是否：

- 从 SonicWall DNS 动态继承 DNS 设置；转至 [步骤 4](#)。
 - 手动指定。DNS 服务器 1/2/3 字段将激活。
- 3 在相应的 DNS 服务器 1/2/3 字段中，输入 DNS 服务器的 IP 地址。
 - 4 单击高级。

高级

- 1 从 DHCPv6 常规选项中选择 DHCP 选项对象或群组。默认设置为无。如需配置新的 DHCPv6 选项或群组，请参阅第 441 页的 [配置 DHCP 选项对象](#)和/或第 443 页的 [配置 DHCP 选项群组](#)。
- 2 如需发送此范围的所有已配置 DHCPv6 选项，而不考虑 DHCPv6 客户端的消息中包含的“选项请求”选项，请选中总是发送 DHCPv6 选项。默认情况下未选中该选项。
- 3 单击确定。

动态范围配置

- 1 如需启用此范围，请确保启用此 DHCP 范围处于选中状态。默认情况下已选中该选项。
- 2 如需使用特定接口的默认值填充开始范围、终止范围、默认网关和子网掩码字段，请选中对话框底部附近的接口预绑定。该下拉菜单将激活。默认情况下未选中该选项。

a 从下拉菜单中选择接口。所填充的 IP 地址与所选的接口位于同一专用子网中。

i **重要：**如需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。

- 3 使用在开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。
- 4 在租用时间（分钟数）字段中，输入在范围颁发另一个 IP 地址之前租用某个 IP 地址的分钟数。最小值为 0，最大值为 71582789，默认值为 1440 分钟（24 小时）。
- 5 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。
- 6 使用已填写的子网掩码或在子网掩码字段中输入网关子网掩码。
- 7 可以选择在备注字段中输入备注。
- 8 如果网络中有 BOOTP 客户端，请选中允许 BOOTP 客户端使用范围。默认情况下未选中该选项。

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 配置信息及其引导镜像文件的 TCP/IP 协议和服务。

- 9 单击 **DNS/WINS** 以继续配置 DHCP 服务器功能。

DNS/WINS

常规 **DNS/WINS** 高级

DNS 服务器

域名:

从 SonicWall 的 DNS 设置动态继承 DNS 设置
 手动指定

DNS 服务器 1:

DNS 服务器 2:

DNS 服务器 3:

WINS 服务器

WINS 服务器 1:

WINS 服务器 2:

- 10 如果您有 DNS 服务器的域名，请在域名字段中输入它。
- 11 选择是否：
 - 从 SonicWall 的 DNS 设置动态继承 DNS 设置；转至步骤 13。
 - 手动指定。DNS 服务器 1/2/3 字段将激活。
- 12 在相应的 DNS 服务器 1/2/3 字段中，输入 DNS 服务器的 IP 地址。
- 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。

- 单击高级。通过高级选项卡，你可以将 DHCP 服务器配置为向网络中的 VoIP 客户端发送 Cisco 呼叫管理程序信息。

高级

The screenshot shows the 'Advanced' configuration page for DHCP. It is divided into three sections:

- VoIP 呼叫管理器**: Three input fields labeled '呼叫管理器 1:', '呼叫管理器 2:', and '呼叫管理器 3:'.
- 网络启动设置**: Three input fields labeled '下一个服务器:', '启动文件:', and '服务器名称:'.
- DHCP 常规选项**: A dropdown menu for 'DHCP 常规选项群组:' set to '无', and a checked checkbox for '总发送常规选项'.

- 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。
- 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。

i **重要：**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。
- 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。
- 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。
- 如需配置 DHCP 常规选项的信息，请参阅第 453 页的[配置用于 DHCP 租用范围的 DHCP 常规选项](#)。
- 单击确定。
- 单击接受，以便设置在防火墙中生效。

如需 SonicWall 安全设备中的 VoIP 支持功能的更多信息，请参阅第 594 页的[关于 VoIP](#)。

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 转至管理 | 系统设置 | 网络 | DHCP 服务器。
- 2 在 DHCPv4/6 服务器租用范围表下，单击添加静态。对于：
 - IPv6，将显示添加 DHCPv6 静态范围对话框。转至第 451 页的添加 DHCPv6 静态范围。
 - IPv4，将显示静态条目配置对话框。转至第 452 页的静态条目配置。

添加 DHCPv6 静态范围



常规 DNS 高级

静态 DHCPv6 范围设置

启用 DHCPv6 范围

条目名称:

前缀: /64

静态 IPv6 地址:

IAID:

DUID:

有效的生命期 (分钟):

首选的生命期 (分钟):

备注:

- 1 如需启用此范围，请确保启用 DHCPv6 范围处于选中状态。默认情况下已选中该选项。
- 2 在条目名称字段中，输入静态 DHCPv6 条目的名称。
- 3 在前缀字段中，输入范围用于分配 IPv6 地址的前缀。
- 4 在静态 IPv6 地址字段中，输入 IPv6 地址。地址必须在前缀的范围内。
- 5 在 IAID 字段中，输入十进制格式的 IAID（接口关联标识符）。最大长度是 10 个数字，最大长度是 4294967295。
- 6 在 DUID 字段中输入一个 DUID（设备唯一标识符）。最大长度为 128 个字符。
- 7 在有效的生命期字段中，输入由范围租用的 IPv6 地址的有效生命期（分钟）。最小值为 0，最大值为 71582789，默认值为 2160。
- 8 在首选的生命期字段中，输入由范围租用的 IPv6 地址的首选生命期（分钟）。最小值为 0，最大值为 71582789，默认值为 1440。

9 可以选择在备注字段中输入备注。

10 如需了解配置 DNS 和高级设置的方法，请分别参阅第 447 页的 DNS 和第 448 页的高级。

静态条目配置

常规 DNS/WINS 高级

静态 DHCP 范围设置

启用此 DHCP 范围

条目名称：

静态 IP 地址：

以太网地址：

租用时间 (分钟数)：

默认网关：

子网掩码：

注释：

接口预绑定：

1 如需启用此范围，请确保启用此 DHCP 范围处于选中状态。默认情况下已选中该选项。

2 在条目名称字段中，输入静态条目的名称。

3 在静态 IP 地址字段中，输入设备 IP 地址。

4 在以太网地址字段中，输入设备以太网 (MAC) 地址。

5 如需使用某个接口的默认值填写租用时间、默认网关和子网掩码字段，请选择靠近对话框的底部接口预填充。该下拉菜单将激活。默认情况下未选中该选项。

a 从下拉菜单中选择接口。所填充的 IP 地址与所选的接口位于同一专用子网中。

i 重要：如需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。

6 在租用时间 (分钟数) 字段中，输入在范围颁发另一个 IP 地址之前租用某个 IP 地址的分钟数。最小值为 0，最大值为 71582789，默认值为 1440 分钟 (24 小时)。

7 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。

8 使用已填写的子网掩码或在子网掩码字段中输入网关子网掩码。

9 可以选择在备注字段中输入备注。

10 如需了解配置 DNS/WINS 和高级设置的方法，请分别参阅第 449 页的 DNS/WINS 和第 450 页的高级。

11 单击确定将设置添加到防火墙。

12 单击接受，以便设置在防火墙中生效。

如需 SonicWall 安全设备中的 VoIP 支持功能的更多信息，请参阅第 594 页的关于 VoIP。

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 453 页的 RFC 定义的 DHCP 选项编号中按照 RFC 分配的选项编号提供了 DHCP 选项列表。

配置用于 DHCP 服务器租用范围的 DHCP 常规选项的步骤如下：

- 1 如果：
 - 修改现有的 DHCP 租约范围：
 - 1) 在网络 | DHCP 服务器上的 DHCP 服务器租赁范围下找到租约范围。
 - 2) 单击配置图标。
 - 3) 在所显示的对话框中，单击高级。
 - 创建一个新的 DHCP 租约范围：
 - 1) 在常规和 DNS/WINS 选项卡下配置选项后单击高级选项卡（请参阅第 446 页的配置用于动态范围的 DHCP 服务器或第 451 页的配置静态 DHCP 条目）。
- 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 如需始终对此 DHCP 服务器租用范围使用 DHCP 选项，请选中总发送常规选项。
- 4 单击确定。

RFC 定义的 DHCP 选项编号

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，如（服务器单播）
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

选项编号	名称	说明
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 持续间隔	TCP 持续间隔
39	TCP 持续无用数据	TCP 持续无用数据
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

选项编号	名称	说明
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
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

选项编号	名称	说明
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	N/A
111	未定义	N/A
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
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特定
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

选项编号	名称	说明
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	N/A
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
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

选项编号	名称	说明
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	不适用
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
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

选项编号	名称	说明
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
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，请参阅第 762 页的 IPv6。

使用 IP 助手

- 第 460 页的[关于 IP 助手](#)
 - 第 461 页的[IP 助手的 VPN 隧道接口支持](#)
- 第 462 页的[网络 > IP 助手](#)
 - 第 463 页的[中继协议](#)
 - 第 464 页的[策略](#)
 - 第 464 页的[DHCP 中继租赁](#)
- 第 465 页的[配置 IP 助手](#)
 - 第 465 页的[启用 IP 助手](#)
 - 第 465 页的[查看流量统计信息](#)
 - 第 465 页的[管理中继协议](#)
 - 第 467 页的[管理 IP 助手策略](#)
 - 第 469 页的[过滤所显示的 DHCP 中继租约](#)

关于 IP 助手

重要：WAN 接口或配置用于 NAT 的接口不支持 IP 助手。

很多用户数据报协议 (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同一广播子网中。为了支持服务器与客户端位于不同子网中的情况，需要一种机制将这些 UDP 广播/多播转发到这些子网。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 SonicWall 安全设备接口并基于策略转发到其他接口。IP Helper 允许安全设备将来自其接口的 DHCP 请求转发到集中的 DHCP 服务器。

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：

扩展的内置中继应用程序

协议	UDP 端口号
DHCP	67/68
Net-Bios NS	137
Net-Bios 数据报	138
DNS	53
时间服务	37

扩展的内置中继应用程序

协议	UDP 端口号
LAN 唤醒 (WOL)	
mDNS	5353
	多播地址: 224.0.0.251

IP 助手的 VPN 隧道接口支持

VPN 隧道接口可支持 IP 助手。有隧道接口支持的 IP 助手中的 DHCP 中继显示了 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。

有隧道接口支持的 IP 助手中的 DHCP 中继



配置拥有 VPN 隧道接口的 IP 助手的步骤如下：

① **注：**有隧道接口支持的 IP 助手中的 DHCP 中继中的数字对应于排序的任务。

- 1 在 PC 中：
 - a 连接到网关 A 的 LAN (X0) 子网。
 - b 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：
 - a 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。
 - b 添加隧道接口的出站接口。
 - c 添加 IP 地址范围作为 PC 的 DHCP 范围。
- 4 在网关 A 中：
 - a 启用 IP 助手。
 - b 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。

网络 > IP 助手

IP 助手设置

启用 IP 助手

中继协议

项目 1 到 7 (/ 7)

添加 删除

<input type="checkbox"/> 名称	端口	端口	Raw	协议	超时 (...)	模式	组播 IP	IP 转换	启用	配置
<input type="checkbox"/> DHCP	67	68		UDP	30	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/> NetBIOS	138	137		UDP	40	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/> DNS	53	--		UDP	30	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/> TIME	37	--		UDP	30	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/> WOL	7	9	✓	UDP	N/A	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/> mDNS (Bonjour)	5353	--	✓	UDP	N/A	组播	224.0.0.251	✓	<input type="checkbox"/>	
<input type="checkbox"/> SSDP (DLNA)	1900	1901	✓	UDP	N/A	两者	239.255.255.250	✓	<input type="checkbox"/>	

添加 删除

策略

项目 0 到 0 (/ 0)

添加 删除

<input type="checkbox"/> 中继协议	源	目标	备注	启用	配置
无条目					

添加 删除

DHCP 中继租约

项目 0 到 0 (/ 0)

刷新

客户 IP 地址	接口	客户 MAC 地址	客户端的供应商	服务器 IP 地址	租约时间	剩余时间
无条目						

刷新 过滤

主题:

- [第 463 页的中继协议](#)
- [第 464 页的策略](#)
- [第 464 页的 DHCP 中继租赁](#)

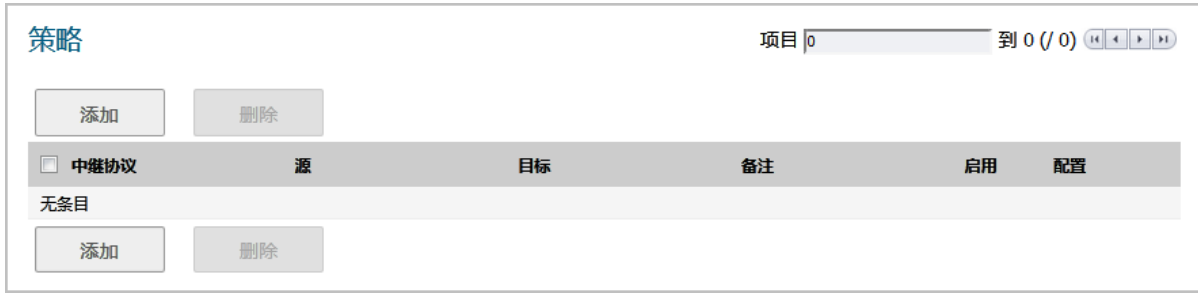
中继协议

中继协议 项目 1 到 7 (/ 7)

<input type="checkbox"/>	名称	端口	端口	Raw	协议	超时 (...)	模式	组播 IP	IP 转换	启用	配置
<input type="checkbox"/>	DHCP	67	68		UDP	30	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/>	NetBIOS	138	137		UDP	40	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/>	DNS	53	--		UDP	30	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/>	TIME	37	--		UDP	30	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/>	WOL	7	9	✓	UDP	N/A	广播	0.0.0.0	✓	<input type="checkbox"/>	
<input type="checkbox"/>	mDNS (Bonjour)	5353	--	✓	UDP	N/A	组播	224.0.0.251	✓	<input type="checkbox"/>	
<input type="checkbox"/>	SSDP (DLNA)	1900	1901	✓	UDP	N/A	两者	239.255.255.250		<input type="checkbox"/>	

- 名称** IP 助手应用程序名称。
- 端口** IP 助手应用程序的第一个 UDP 端口号。
- 端口** IP 助手应用程序的可选的第二个 UDP 端口号。
- Raw** 指示在已配置 IP 助手应用程序时是否选择原始模式。如果启用了此选项，则将忽略超时。
- 协议**
- 超时 (秒)** IP 助手高速缓存超时。不适用表示已选择原始模式且将忽略超时。
- 模式** 指示协议支持的模式：
- 广播
 - 组播
 - 两者
- 组播 IP** 协议使用的多播 IP。
- IP 转换** 指示 IP 助手策略转发数据包时是否转换源 IP 地址。
- 启用** 指示是否启用 IP 助手策略。
- 配置** 包含条目的统计信息、编辑和删除图标。
- 注：** 只能删除用户生成的中继协议。

策略



- 中继协议** 策略的协议。
- 源** 策略的接口或区域。
- 目标** 网络目的地。
- 备注** 配置策略时输入的注释。
- 启用** 指示是否启用 IP 助手策略。
- 配置** 包含每个条目的统计信息、编辑和删除图标。

DHCP 中继租赁



- 客户 IP 地址** 客户端设备的 IP 地址。
- 接口** 安全设备上的接收接口。
- 客户 MAC 地址** 客户端设备的 MAC 地址。
- 客户端的供应商** 客户端设备的制造商。
- 服务器 IP 地址** DHCP 服务器的 IP 地址。
- 租约时间** 中继租约的时间。
- 剩余时间** 中继租约的剩余时间。

刷新 DHCP 中继租约表的步骤如下：

- 1 单击刷新。

配置 IP 助手

主题：

- 第 465 页的[启用 IP 助手](#)
- 第 465 页的[管理中继协议](#)
- 第 467 页的[管理 IP 助手策略](#)

启用 IP 助手

激活 IP 助手功能的步骤如下：

- 1 转至网络 > IP 助手。
- 2 在 IP 助手设置中选择启用 IP 助手。

管理中继协议

主题：

- 第 465 页的[查看流量统计信息](#)
- 第 466 页的[添加用户定义的中继协议](#)
- 第 467 页的[删除自定义协议](#)

查看流量统计信息

可以查看中继协议表和策略表的流量统计信息。

查看流量统计信息的步骤如下：

- 1 将光标指针悬停在协议或策略的统计信息图标上。弹出窗口将显示该条目的流量状态。

中继协议表



策略表



添加用户定义的中继协议

添加中继协议的步骤如下：

- 1 转至网络 > IP 助手。
- 2 单击中继协议部分中的添加。将显示添加 IP 助手应用程序对话框。

The dialog box is titled '启动应用程序' (Start Application). It contains the following fields and options:

- 启动应用程序
- 名称: [Text Input Field]
- 端口 1: [Text Input Field]
- 端口 2: [Text Input Field]
- 超时: [Text Input Field]
- 模式: 广播 组播 两者都
- 组播 IP: [Text Input Field]
- 允许源IP转换
- 原始模式

- 3 通过选择启用应用程序来启用 IP 助手应用程序。

注：如果禁用了此选项，系统将删除所有 IP 助手缓存。

- 4 在名称字段中，为 IP 助手应用程序输入区分大小写的唯一名称。
- 5 在端口 1 字段中，为应用程序指定一个唯一的 UDP 端口号。
- 6 （可选）在端口 2 字段中，为应用程序指定另一个唯一的 UDP 端口号。
- 7 （可选）在超时字段中，指定 IP 助手缓存超时（以秒为单位，10 为增量，范围介于 10 到 60）。如果未指定超时，则将选择默认值 30 秒。

提示：如果选择原始模式，忽略此字段。

- 8 选择模式：

- 广播
- 组播
- 两者

- 9 如果为模式选择了组播或两者，请指定此协议将在组播 IP 字段中使用有效多播 IP。
- 10 通过 IP 助手策略转发数据包时，如需允许转换源 IP 地址，请选中允许源 IP 转换。默认情况下已选中该选项。
- 11 如需避免在 IP 助手策略转发数据包时创建缓存，请选中原始模式。支持单向转发。默认情况下未选中该选项。

注：将忽略超时字段中设置的任何时间。

- 12 单击确定。

删除自定义协议

删除自定义协议的步骤如下：

- 1 转至网络 > IP 助手。
- 2 选择该协议的删除图标。

删除一个或多个自定义中继协议的步骤如下：

- 1 转至网络 > IP 助手。
- 2 选中所需协议最左侧的复选框（按协议名称）。删除按钮将激活。
- 3 单击删除。

删除所有自定义中继协议的步骤如下：

- 1 转至网络 > IP 助手。
- 2 选中中继协议表标题中的复选框。删除按钮将激活。
- 3 单击删除。

管理 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 467 页的添加 IP 助手策略](#)
- [第 468 页的编辑 IP 助手策略](#)
- [第 468 页的删除 IP 助手策略](#)
- [第 469 页的通过 TSR 显示 IP 助手缓存](#)

添加 IP 助手策略

最多可以添加 128 项策略。

添加 IP 助手策略的步骤如下：

- 1 转至网络 > IP 助手。
- 2 对于 IP 助手策略表，单击添加。将显示添加 IP 助手策略对话框。



启用策略

协议：

从：

至：

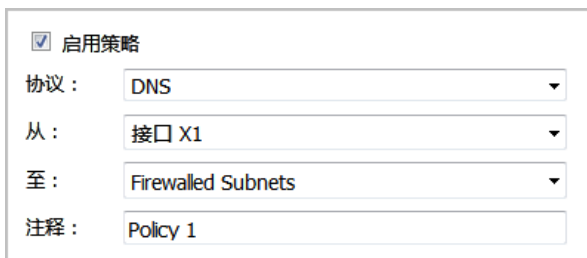
注释：

- 3 默认将启用策略。如需配置策略而不启用它，请取消选中启用复选框。
- 4 从协议菜单中选择一项协议。默认值为 **DHCP**。
- 5 从从中，选择源接口或区域。
- 6 从至中，选择以下两项之一：
 - 目标地址群组或地址对象。
 - 创建新网络以创建新的地址对象。此时会显示添加地址对象对话框。如需创建地址对象的更多信息，请参阅 **SonicOS 策略指南**。
- 7 在注释字段中输入任何可选的备注。
- 8 单击确定。

编辑 IP 助手策略

编辑 IP 助手策略的步骤如下：

- 1 转至网络 > IP 助手。
- 2 单击 IP 助手策略表中条目的配置列中的编辑图标。将显示编辑 IP 助手策略对话框。



<input checked="" type="checkbox"/> 启用策略
协议： DNS
从： 接口 X1
至： Firewalled Subnets
注释： Policy 1

- 3 设置与添加 IP 助手策略对话框相同。如需对话框的信息，请参阅第 467 页的添加 IP 助手策略。

删除 IP 助手策略

删除自定义策略的步骤如下：

- 1 转至网络 > IP 助手。
- 2 为该策略选择策略表中的删除图标。

删除一项或多项自定义策略的步骤如下：

- 1 转至网络 > IP 助手。
- 2 选中所需策略最左侧的复选框（按中继协议）。删除按钮将激活。
- 3 单击删除。

删除所有自定义策略的步骤如下：

- 1 转至网络 > IP 助手。
- 2 选中策略表标题中的复选框。删除按钮将激活。
- 3 单击删除。

过滤所显示的 DHCP 中继租约

通过使用过滤器功能，可以在反欺骗缓存和检测到的欺骗列表表中只显示特定设备。

过滤表显示的步骤如下：

- 1 转至网络 > MAC-IP 反欺骗。
- 2 在要过滤的表下方的过滤器字段中，指定设备的 IP 地址、接口、MAC 地址、主机名或名称。必须使用过滤器操作符语法选项表中显示的运算符的相应语法来填写该字段。

过滤器操作符语法选项

运算符	语法选项
包含类型的值	<ul style="list-style-type: none">• Ip=1.1.1.1 或 ip=1.1.1.0/24• Mac=00:01:02:03:04:05• lface=x1
字符串	<ul style="list-style-type: none">• X1• 00:01• Tst-mc• 1.1.
和	<ul style="list-style-type: none">• Ip=1.1.1.1;iface=x1• Ip=1.1.1.0/24;iface=x1;just-string
或	<ul style="list-style-type: none">• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24• lface=x1,x2,x3
负值	<ul style="list-style-type: none">• !ip=1.1.1.1;!just-string• !iface=x1,x2
混合	<ul style="list-style-type: none">• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

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 -----
名称: DHCP
端口: 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
```

```

名称: NetBIOS
  端口: 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
名称: DNS
  端口: 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
名称: TIME
  端口: 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
名称: WOL
  端口: 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
  端口: 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

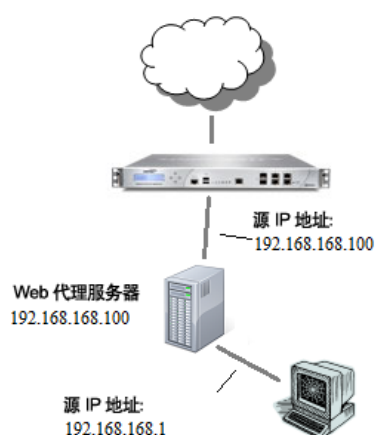
```

设置 Web 代理转发

- 第 471 页的[网络 | Web 代理](#)
 - 第 472 页的[配置自动代理转发（仅用于 Web）](#)
 - 第 473 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（介于用户与 SonicWall 安全设备之间）的代理服务器访问 Web 时，安全设备看到的 HTTP/HTTPS 连接源自代理服务器，而非用户。



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 区域，并使用[网络 | Web 代理](#)页面上的设置来启用 Web 代理转发，而不必将每台计算机的 Web 浏览器配置为指向该代理服务器。安全设备自动将所有 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 472 页的[配置自动代理转发（仅用于 Web）](#)
- 第 473 页的[配置用户代理服务器](#)

配置自动代理转发（仅用于 Web）

- ① 注：如需启用 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。
① 注：代理服务器必须位于 WAN 或 DMZ 区域中；它不得位于 LAN 中。
- 3 转至网络 > Web 代理。

自动代理转发(仅用于 Web)

代理 Web 服务器（名称或 IP 地址）：

代理 Web 服务器端口：

代理服务器失败时绕过代理服务器

将公用区域客户端请求转发到代理服务器

用户代理服务器

用户的 Web 请求通过的代理服务器：

--无--

- 4 如需将所有 Web 代理请求自动转发至代理服务器，请在自动代理转发（仅用于 Web）部分的代理 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。最小长度为 0 个字符，最大长度为 39 个字符。
- 5 在代理 Web 服务器端口字段中输入代理 IP 端口。默认值为 0。
- 6 如需在 Web 代理服务器不可用时让客户端直接访问互联网，请选中代理服务器失败时绕过代理服务器。默认已禁用该选项。
① 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，如同未指定 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 单击接受。

在安全设备已更新后，浏览器窗口底部会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 转至网络 | Web 代理。
- 2 转至用户代理服务器部分。



- 3 单击添加。将显示添加代理服务器弹出对话框。



i **注：** 如果用户的 Web 请求在到达 SonicWall 安全设备之前经过代理服务器，则安全设备看到的 Web 请求来自代理服务器，而不是直接来自用户。因此，安全设备无法根据源 IP 地址识别用户。但是，用于标识每个 Web 请求的源的代理服务器通常将此信息包含在 HTTP 标头中。如果在此处配置了任何内部代理服务器，则安全设备将使用来自服务器的信息识别用户。这适用于识别通过内部网络上的代理服务器访问网络的用户，以及通过 WAN 侧外部代理服务器对安全设备进行远程 HTTP 管理。

- 4 输入代理服务器的名称或 IP 地址。
- 5 单击确定。
- 6 重复步骤 3 到步骤 5 以添加更多代理服务器。
- 7 单击接受。
- 8 在配置好接口后，可将其连接到主机。请参阅第 224 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 转至网络 | Web 代理。
- 2 转至用户代理服务器部分。
- 3 在用户代理服务器表中，选择要编辑的代理服务器。

- 4 单击**编辑**按钮。将显示**编辑代理服务器**弹出对话框。

输入代理服务器的主机名或 IP 地址:

- 5 更改代理服务器的名称或 IP 地址。
- 6 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 转至**网络 | Web 代理**。
- 2 转至**用户代理服务器**部分。
- 3 在**用户代理服务器**表中, 选择要删除的代理服务器。
- 4 单击**删除**按钮。
- 5 单击**接受**。

配置动态 DNS

- 第 475 页的[网络 | 动态 DNS](#)
 - 第 475 页的[关于动态 DNS](#)
 - 第 476 页的[支持的 DDNS 提供商](#)
 - 第 476 页的[动态 DNS 配置文件表](#)
 - 第 478 页的[配置动态 DNS 配置文件](#)
 - 第 480 页的[编辑 DDNS 配置文件](#)
 - 第 480 页的[删除 DDNS 配置文件](#)

网络 | 动态 DNS

								视图 IP 版本: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
配置文件名称	域名	提供商	状态	接口	已启用	在线	配置	
无条目								
<input type="button" value="添加"/>								<input type="button" value="全部删除"/>

主题:

- 第 475 页的[关于动态 DNS](#)
- 第 476 页的[支持的 DDNS 提供商](#)
- 第 476 页的[动态 DNS 配置文件表](#)
- 第 478 页的[配置动态 DNS 配置文件](#)
- 第 480 页的[编辑 DDNS 配置文件](#)
- 第 480 页的[删除 DDNS 配置文件](#)

关于动态 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，也能通过域名而非 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，并无严格的标准。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。

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 当前支持来自[动态 DNS 提供商](#)表中列出的提供商的服务：

动态 DNS 提供商

dns.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

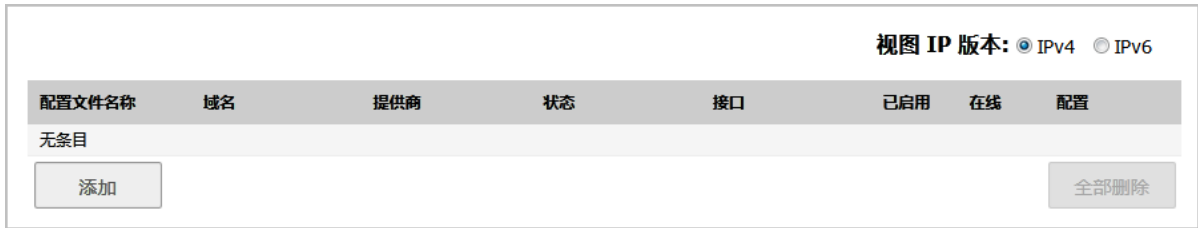
由动态 DNS 提供商提供的一些常见的附加服务包括：

通配符	允许对子域使用通配符引用。例如，如果您注册了 <code>yourdomain.dyndns.org</code> ，则可通过 <code>*.yourdomain.dyndyn.org</code> （例如 <code>server.yourdomain.dyndyn.org</code> 、 <code>www.yourdomain.dyndyn.org</code> 、 <code>ftp.yourdomain.dyndyn.org</code> ）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 <code>dns.org</code> 、 <code>yi.org</code> 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	如果主要的注册 IP 处于离线状态，则允许为已注册的主机名指定备用地址。

如需设置 DDNS 配置文件的信息，请参阅第 478 页的[配置动态 DNS 配置文件](#)。

动态 DNS 配置文件表

动态 DNS 配置文件表提供了有关已配置的 DDNS 配置文件的信息。



视图 IP 版本	允许在 IPv4 和 IPv6 DDNS 配置文件之间切换表。						
配置文件名称	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。						
域名	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 条目的最近报告状态/当前状态：						
在线	以管理方式将 DDNS 条目设置为在线。此条目的当前 IP 设置将与时间戳一同显示。						
设置为离线模式	以管理方式将 DDNS 条目设置为离线。如果已启用该条目，则将执行添加 DDNS 配置文件的高级页面上的离线设置部分中配置的操作。						
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	滥用可能。一些 DDNS 提供商可能将无 IP 地址更改时的强制更新视为滥用行为。自动更新仅在地址或状态发生更改时进行。手动或强制更新仅在绝对必要时进行，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。						
已启用	选中时，将以管理方式启用此配置文件，而且安全设备将执行在添加 DDNS 配置文件的高级页面上配置的在线设置。也可以使用条目的添加 DDNS 配置文件的启用此 DDNS 配置文件选项来控制此设置。取消选中此选项将禁用该配置文件，并且此配置文件将不会与 DDNS 提供商进行任何通讯，直到再次启用配置文件。						
在线	选中时，将以管理方式将此配置文件设为在线。也可以通过该条目的添加 DDNS 配置文件上的使用在线设置选项来控制此设置。在已启用配置文件的情况下取消选中此选项将使配置文件离线，而且安全设备将执行在高级页面上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。						

配置动态 DNS 配置文件

如需设置 DDNS 配置文件的常规信息，请参阅第 475 页的[关于动态 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。请参阅[动态 DNS 提供商](#)表中列出的不同提供商。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](#) 页面提供了用于将 SonicWall 安全设备配置为使用 DDNS 服务的设置。

在 SonicWall 安全设备上配置动态 DNS 的步骤如下：

- 1 转至网络 | 动态 DNS。



- 2 单击添加按钮。随即显示添加 DDNS 配置文件对话框。

- 3 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，安全设备将执行在高级页面上在线设置部分中定义的操作。默认情况下已选中该选项。
- 4 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。
- 5 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。
- 6 从提供商中，选择动态 DNS 提供商；这些提供商在[动态 DNS 提供商](#)表中描述。默认值为 dyn.com。

重要：必须使用选择的 DNS 提供商创建动态服务记录。

i | **提示：**并非所有选项都适用于所有 DNS 提供商。此外，页面底部的注意显示 DNS 提供商使用 HTTP 还是 HTTPS 协议以及提供商网站的链接。

- 7 在用户名字段中，输入 DNS 提供商帐户的用户名。最小长度为 1 个字符，最大长度为 63 个字符。
- 8 在密码字段中，输入 DNS 密码。最小长度为 1 个字符，最大长度为 31 个字符。
- 9 输入向域名字段中的 DNS 提供商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。
- 10 (可选) 如需将此 DDNS 配置文件分配给特定的 WAN 接口，请从绑定到中选择该 WAN 接口。如果要配置多 WAN 负载均衡，则此选项允许您向 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安全设备上的任意 WAN 接口。
- 11 如果为提供商选择了 **dyn.com**，请转至 **步骤 13**。
- 12 使用 **dyn.org** 时，从 **服务类型** 中选择与服务类型对应的服务类型：

动态 免费的动态 DNS 服务。这是默认值。

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。

- 13 单击高级。

i | **提示：**通常可以保留该页面中的默认设置。

配置文件 高级

在线设置

- 允许 DDNS 提供商检测 IP 地址。
- 自动将 IP 地址设置为主 WAN 接口 IP 地址。
- 手动指定 IP 地址：

离线设置

- 不做任何操作。
- 使用以前在提供商站点配置的离线 IP 地址。

- 14 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。选择：

允许 DDNS 提供商检测 IP 地址

安全设备允许 DNS 提供商指定 IP 地址
注：仅 IPv4。默认情况下已选中该选项。

自动将 IP 地址设置为主 WAN 接口 IP 地址

导致安全设备断言其 WAN IP 地址为注册 IP 地址，从而覆盖动态 DNS 服务器的自动检测。适用于不能正常检测的情况。默认情况下已选中该选项。

注：在 IPv6 中：默认情况下已选中该选项。

手动指定 IP 地址 允许手动指定和断言要注册的 IP 地址。

15 离线设置部分在安全设备中的动态 DNS 条目已在本地离线（已禁用）的情况下，提供对在动态 DNS 提供商处注册的 IP 地址的控制。选择：

不做任何操作 允许先前注册的地址仍然使用动态 DNS 提供商。默认情况下已选中该选项。

使用以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，在管理方式将此配置文件设为离线时使用离线设置。

16 单击确定。

编辑 DDNS 配置文件

编辑 DDNS 配置文件的步骤如下：

- 1 转至网络 | 动态 DNS。
- 2 在“动态 DNS 配置文件”表中，单击配置文件的编辑图标。将显示“编辑 DDNS 配置文件”对话框。

配置文件 高级

动态 DNS 配置文件设置

启用此动态 DNS 配置文件

使用在线设置

配置文件名称：

提供商：

用户名：

密码：

域名：

绑定到：

服务类型：

注： DDNS 提供商 [dyn.com](#) 使用 HTTPS 协议。

- 3 执行更改；如需选项描述，请按照第 478 页的[配置动态 DNS 配置文件的说明](#)进行操作。
- 4 单击确定。

删除 DDNS 配置文件

可以删除一个或全部 DDNS 配置文件。

删除 DDNS 配置文件的步骤如下

- 1 转至网络 | 动态 DNS。
- 2 单击要删除的配置文件的删除图标。将显示确认消息：

是否确定要删除所选择的条目？

- 3 单击确定。

删除所有的 DDNS 条目的步骤如下：

- 1 转至网络 | 动态 DNS。
- 2 单击全部删除。将显示确认消息：

是否确定要删除所有条目？

- 3 单击确定。

① 注：本部分介绍了 SonicOS 的高级交换功能，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，请参阅第 296 页的 [X-系列交换机的 SonicOS 支持](#)。

- [关于交换](#)
- [配置 VLAN 中继](#)
- [查看第 2 层发现](#)
- [配置链路聚合](#)
- [配置端口镜像](#)

关于交换

- ① | 注：NSA 2600、TZ 系列和 SOHO W 安全设备以外的所有产品中提供了交换功能。
- ① | 注：本节介绍了 SonicOS 中的高级交换功能，它不同于从 SonicWall 安全管理 Dell X-系列交换机。如需管理 X-系列交换机的更多信息，请参阅第 296 页的 X-系列交换机的 SonicOS 支持。

- 第 483 页的[关于交换](#)
 - 第 483 页的[什么是交换？](#)
 - 第 484 页的[交换的优点](#)
 - 第 484 页的[交换的工作原理](#)
 - 第 485 页的[术语](#)

关于交换

主题：

- 第 483 页的[什么是交换？](#)
- 第 484 页的[交换的优点](#)
- 第 484 页的[交换的工作原理](#)
- 第 485 页的[术语](#)

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** - 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** - 聚合端口以提高性能和冗余。
 - ① | 注：NSA 3600 及更高版本的防火墙支持链路聚合。在 NSA 2600 上，网络接口的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（请参阅第 496 页的[配置链路聚合](#)），但 NSA 2600 不支持交换，因此它不支持交换的链路聚合。
- **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 能处理负载在 1500-9000 字节之间的以太网帧。

i | 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。

i | 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。

i | 注：NSA 3600 及更新设备支持巨型帧。

交换的工作原理

一些交换功能在 PortShield 群组上运行，并需要在 **网络 > PortShield 组** 页面上进行初步配置。一些功能在现有的 **网络 > 接口** 配置上运行。如需在 SonicOS 中配置这些相关功能的更多信息，请参阅：

- [第 224 页的配置接口](#)
- [第 295 页的 PortShield 配置接口](#)

如需每项交换功能工作方式的详细信息，请参阅：

- [第 486 页的配置 VLAN 中继](#)
- [第 493 页的查看第 2 层发现](#)
- [第 496 页的配置链路聚合](#)
- [第 501 页的配置端口镜像](#)

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 位字段来运行。
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) 上运行。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。

配置 VLAN 中继

① | 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 487 页的 [交换 | VLAN 中继](#)
 - 第 488 页的 [关于中继](#)
 - 第 488 页的 [查看 VLAN](#)
 - 第 490 页的 [编辑 VLAN](#)
 - 第 490 页的 [添加 VLAN 中继端口](#)
 - 第 491 页的 [启用中继端口上的 VLAN](#)
 - 第 491 页的 [删除 VLAN 中继端口](#)

交换 | VLAN 中继

保留的 VLAN 信息

开始 VLAN ID : 2
结束 VLAN ID : 26

VLAN 表

VLAN ID	接口	成员端口	中继	配置
2	X0	X0		
3	X1	X1		
4	X2	X2		
5	X3	X3		
6	X4	X4		
7	X5	X5		
8	X6	X6		
9	X7	X7		
10	X8	X8		
12	X10	X9, X11, X13, X10		
14	X12	X12		
16	X14	X14		
17	X15	X15		
18	X17	X17		

VLAN 中继

▶... 中继端口	VLAN ID	配置
无条目		

主题:

- [关于中继](#)
- [第 488 页的查看 VLAN](#)
- [第 490 页的编辑 VLAN](#)
- [第 490 页的添加 VLAN 中继端口](#)
- [第 491 页的删除 VLAN 中继端口](#)
- [第 491 页的启用中继端口上的 VLAN](#)

关于中继

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 使用且所保留的范围将显示在[管理 | 系统设置 | 交换 | VLAN 中继](#)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，请参阅第 295 页的[PortShield 配置接口](#)。

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。

[管理 | 系统设置 | 网络 | 接口](#)上的名称列显示 VLAN 中继的 VLAN 中继接口的 VLAN ID。

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 345，该端口上还启用了两个远程 VLAN。

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。

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。

查看 VLAN

主题：

- 第 489 页的[保留的 VLAN 信息](#)
- 第 489 页的[VLAN 表](#)
- 第 490 页的[VLAN 中继表](#)















保留的 VLAN 信息

保留的 VLAN 信息	
开始 VLAN ID :	2
结束 VLAN ID :	26

保留的 VLAN 信息表列出了所保留的 VLAN ID 的范围：

- 开始 VLAN ID
- 结束 VLAN ID

VLAN 表

VLAN 表				
VLAN ID	接口	成员端口	中继	配置
2	X0	X0		
3	X1	X1		
4	X2	X2		
5	X3	X3		
6	X4	X4		
7	X5	X5		
8	X6	X6		
9	X7	X7		
10	X8	X8		
12	X10	X9, X11, X13, X10		
14	X12	X12		
16	X14	X14		
17	X15	X15		
18	X17	X17		

VLAN ID	VLAN 的 ID。
接口	分配给 VLAN 的接口。
成员端口	与接口关联的端口。
中继	指示是否对此 VLAN 进行中继。
配置	包含 VLAN 的编辑图标。

VLAN 中继表

VLAN 中继		
... 中继端口	VLAN ID	配置
<input type="checkbox"/> X5 (2 VLAN 条目)		<input type="button" value="X"/>
	63	<input type="button" value="X"/>
	66	<input type="button" value="X"/>
<input type="checkbox"/> X7 (0 VLAN 条目)		<input type="button" value="X"/>

中继端口 中继端口的接口以及与之关联的 VLAN 条目的数量

VLAN ID VLAN 的 ID

配置 包含 VLAN 的删除图标

如需显示中继端口的 VLAN ID，请单击中继端口的展开图标。如需显示所有中继端口的 VLAN ID，请单击 VLAN 中继表标题中的展开图标。如需隐藏 VLAN ID，请单击相应的折叠图标。

编辑 VLAN

如需编辑 VLAN，请执行以下步骤：

- 1 转至交换 | VLAN 中继。
- 2 单击 VLAN 表中您要编辑的 VLAN ID 对应的配置图标。将显示编辑 PortShield 主机的 VLAN 对话框。
- 3 执行以下某个操作：
 - 将其他 VLAN ID 输入 VLAN ID 字段中。除了系统指定的原始 VLAN ID 和保留的 VLAN 信息表中的任何其他 VLAN ID 之外，用户可以输入任何 VLAN ID。
 - 使用 VLAN ID 字段中的 VLAN ID 编号，它与用户单击其配置图标的 VLAN ID 相匹配。
- 4 如需启用对该 VLAN 的中继，请选中中继复选框。如需禁用对该 VLAN 的中继，请取消选中该复选框。
- 5 单击确定。

添加 VLAN 中继端口

添加 VLAN 中继端口的步骤如下：

- 1 转至交换 | VLAN 中继。
- 2 在 VLAN 中继下，单击添加。将显示添加 VLAN 中继端口对话框。

添加 VLAN 中继端口

中继端口

- 3 从中继端口下拉菜单中选择要添加的端口。
- 4 单击确定。

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 转至交换 | VLAN 中继。
- 2 在 VLAN 中继表下，单击启用 VLAN。将显示启用 VLAN 对话框。

中继端口

VLAN ID

- 3 从中继端口下拉菜单中选择一个中继端口。这是您希望用来中继 VLAN ID 字段所示 VLAN ID 的端口。
- 4 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。
- 5 单击确定。

删除 VLAN 中继端口

可以一次删除一个 VLAN 中继端口或多个端口，也可以删除所有端口。

删除 VLAN 中继端口的步骤如下：

- 1 转至交换 | VLAN 中继。
- 2 展开要删除的 VLAN 中继端口。
- 3 单击要删除的 VLAN 的配置列中的删除图标。将显示确认消息：

是否确定要删除此 VLAN？

- 4 单击确定。
- 5 单击要删除端口的配置列中的删除图标。将显示确认消息：

是否确定要删除此 VLAN 中继端口？

- 6 单击确定。

删除多个 VLAN 中继端口的步骤如下：

- 1 转至交换 | VLAN 中继。
- 2 在 VLAN 中继表中，展开要删除的 VLAN 中继端口。
- 3 单击每个要删除的 VLAN 的配置列中的删除图标。将显示确认消息：

是否确定要删除此 VLAN ？

- 4 对每个项单击确定。
- 5 选中要删除的 VLAN 中继端口的复选框。删除按钮将激活。
- 6 单击删除。将显示确认消息。

是否确定要删除所有选定的 VLAN 中继端口？

- 7 单击确定。

删除所有 VLAN 中继端口的步骤如下：

- 1 转至交换 | VLAN 中继。
- 2 在 VLAN 中继表中，通过单击 VLAN 中继表标题中的展开图标来展开 VLAN 中继端口。
- 3 单击每个要删除的 VLAN 的配置列中的删除图标。将显示确认消息：

是否确定要删除此 VLAN ？

- 4 选中 VLAN 中继表标题中的复选框。删除按钮将激活。
- 5 单击删除。将显示确认消息。

是否确定要删除所有选定的 VLAN 中继端口？

- 6 单击确定。

查看第 2 层发现

① | 注：在 NSA 2600、TZ 系列和 SOHO W 设备以外的所有防火墙中提供了交换功能。

- 第 493 页的 [交换 | L2 发现](#)
 - [查看 L2 发现](#)
 - [激活 L2 发现](#)

交换 | L2 发现

SonicWall 安全设备使用 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。如需这些协议的更多信息，请访问：

- https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery
- https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

主题：

- [查看 L2 发现](#)
- [激活 L2 发现](#)

查看 L2 发现

默认情况下，L2 发现表仅显示接口、通过端口可见的节点数以及接口的刷新图标。

▶ <input type="checkbox"/> 接口	MAC 地址	供应商	IP 地址	系统名称	描述
▶ <input type="checkbox"/> X0 (0 条目)					
▶ <input type="checkbox"/> X1 (2 条目)					
▶ <input type="checkbox"/> X2 (5 条目)					
▶ <input type="checkbox"/> X3 (1 条目)					
▶ <input type="checkbox"/> X4 (0 条目)					
▶ <input type="checkbox"/> X5 (0 条目)					
▶ <input type="checkbox"/> X6 (0 条目)					
▶ <input type="checkbox"/> X7 (0 条目)					
▶ <input type="checkbox"/> X8 (0 条目)					
▶ <input type="checkbox"/> X9 (0 条目)					
▶ <input type="checkbox"/> X10 (0 条目)					
▶ <input type="checkbox"/> X11 (0 条目)					
▶ <input type="checkbox"/> X12 (0 条目)					
▶ <input type="checkbox"/> X13 (0 条目)					
▶ <input type="checkbox"/> X14 (0 条目)					
▶ <input type="checkbox"/> X15 (0 条目)					
▶ <input type="checkbox"/> X17 (0 条目)					

刷新已选

如需显示 L2 发现信息，请单击所需接口的展开图标。将显示有关对接口发现的节点的信息。

- MAC 地址
- 供应商
- IP 地址或 N/A（如果适用）
- 系统名称（如果适用）
- 描述（如果适用）

激活 L2 发现

发现在系统启动时激活，然后便不再启动，除非您刷新 L2 发现表。

重启接口上的第 2 层发现的步骤如下：

- 1 转至交换 | L2 发现。
- 2 单击特定接口的刷新图标。

重启多个接口上的第 2 层发现的步骤如下：

- 1 转至交换 | L2 发现。
- 2 选择所需接口。刷新已选按钮变为可用。
- 3 单击刷新已选。

重启所有接口上的第 2 层发现的步骤如下：


- 1 转至交换 | L2 发现。
- 2 选中表标题中的复选框。刷新已选按钮变为可用。
- 3 单击刷新已选。

配置链路聚合

注： 交换功能在所有 NSA 3600 和更高版本及 SuperMassive 设备上可用。

- 第 496 页的 [交换 | 链路聚合](#)
 - 第 496 页的 [关于链路聚合](#)
 - 第 498 页的 [查看链路聚合](#)
 - 第 499 页的 [创建逻辑链路 \(LAG\)](#)
 - 第 500 页的 [删除 LAG](#)

交换 | 链路聚合

状态								
系统 ID:		C0:EA:E4:59:8E:24						
端口	LAG ID	密钥	聚合	启用 LACP	状态	合作伙伴	供应商	操作
X3	0	11	✔	✔	连接,ena 匹配	00:00:00:00:00:00	XEROX CORPORATION	  
X6	0	11		✔	断开	00:00:00:00:00:00	XEROX CORPORATION	 
X8	0	11		✔	断开	00:00:00:00:00:00	XEROX CORPORATION	 

主题：

- 第 496 页的 [关于链路聚合](#)
- 第 498 页的 [查看链路聚合](#)
- 第 499 页的 [创建逻辑链路 \(LAG\)](#)

关于链路聚合

注： NSA 3600 及更新防火墙支持链路聚合(LAG)。

链路聚合允许您将 SonicWall 安全设备与两个或多个链路连接在一起，使得多个链路组合成一个更大的虚拟管道，携带更高的组合带宽，从而支持第 2 层网络中的端口冗余和负载平衡。由于两台设备之间存在多条链路，如果一条链路出现故障，流量将通过其他链路传输而不中断。在存在多条链路的情况下，流量也可以通过负载均衡来实现均匀分配。负载平衡由 SonicWall 安全设备依据来源和目标 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。

SonicOS 支持两种 LAG 类型：

- 第 497 页的静态 LAG
- 第 497 页的动态 LAG

静态 LAG

在静态链路聚合中，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)。通过静态链路聚合，所有配置设置都在参与的两个 LAG 组件上进行设置。

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，但由于安全设备的硬件限制，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。负载均衡由硬件自动执行。安全设备支持一种基于来源和目标 MAC 地址对的负载均衡算法。

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。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。

注：该键与 LAG ID 不一样，与接口编号一致，不能修改。在配置 LAG 组时必须分配密钥。所有非聚合器应该与聚合端口具有相同的密钥。

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。

动态 LAG

SonicOS 支持动态链路聚合，在所有支持高级交换功能的 SonicWall 安全设备上使用链路聚合控制协议（由 IEEE 802.3ad 定义的 LACP）。

关于使用 LACP 的动态 LAG

LACP 允许链路聚合控制协议数据单元 (PDU) 协议包中的 LAG 组成员之间交换与链路聚合相关的信息。使用 LACP，可以快速检测到配置错误、接线错误和链路故障。

使用 LACP 可以有效地实现 LAG 的两个主要优点，提高的吞吐量和链路冗余。LACP 是 LAG 中成员之间使用的信令协议。它确保链路只有在正确配置和布线的情况下才能聚合成一个捆绑链路。LACP 可以配置为以下两种模式之一：

- **主动模式** - 端口启动时，设备立即发送 LACP PDU。

注：SonicOS 6.5 仅支持 LACP 的主动模式。

- **被动模式** - 端口处于被动协商状态，其中端口只响应接收到的 LACP PDU，但不发起 LACP 协商。

如果双方都配置为主动状态，则在成功协商其他参数的情况下可以形成 LAG。如果一方配置为主动而另一方配置为被动，当被动端口响应从主动方接收到的 LACP PDU 时可以形成 LAG。如果双方都是被动的，LACP 不能协商捆绑。被动模式在部署中很少使用。

在配置中，同一个 LAG 的所有成员端口必须与聚合器端口设置在同一个 VLAN 上。在 LAG 成员上收到的数据包与使用 VLAN 的父聚合器端口相关联。当 LAG 的聚合器/成员端口状态达到稳定的收集/分发状态时，端口准备好发送和接收数据流量。

所有与 LAG 相关的信息，例如配置的聚合器端口，这些信息都显示在 **交换 | 链路聚合** 页面上：

- 成员端口是 LAG 的一部分。
- 形成 LAG 的每个端口的状态。
- 通过 LACP 收到的合作伙伴 MAC 地址。

六个负载平衡选项可用于配置。创建 LAG 和聚合器端口时，必须选择负载平衡选项。

重要： 在创建 LAG 之后，无法修改负载平衡选项。

查看链路聚合

主题：

- 第 498 页的 [查看状态](#)
- 第 498 页的 [查看链路聚合端口](#)

查看状态



状态表显示防火墙的 MAC 地址系统 ID。

查看链路聚合端口

如需查看链路聚合端口，请转至 **系统设置 | 交换 | 链路聚合**

端口	LAG ID	密钥	聚合	启用 LACP	状态	合作伙伴	供应商	操作
X3	0	11	✓	✓	连接,ena 匹配	00:00:00:00:00:00	XEROX CORPORATION	  
X6	0	11		✓	断开	00:00:00:00:00:00	XEROX CORPORATION	 
X8	0	11		✓	断开	00:00:00:00:00:00	XEROX CORPORATION	 

端口	用作聚合器端口或成员端口的接口
LAG ID	系统配置的链路聚合器。非聚合器的端口有一个成员聚合器的 LAG ID。
密钥	指示添加 LAG 端口对话框中的端口成员资格。
聚合	以绿色复选标记指示聚合器端口；否则此项为空。
启用 LACP	指示是否启用了 LACP。
状态	指示端口为正常还是关闭。

- 合作伙伴 链路伙伴完成物理连接后，链路伙伴的 MAC 地址。
- 静态 LAG，显示 00:00:00:00:00:00
 - 动态 LAG，显示合作伙伴的 MAC 地址
- 供应商 显示设备制造商的名称。
- 操作 显示以下图标：
- 统计 - 将鼠标指针悬停在此图标上时，将显示 LAG 端口统计弹出对话框：



- 编辑（只能编辑一个聚合器端口）
- 删除

创建逻辑链路 (LAG)

创建逻辑链路 (LAG) 的步骤如下：

- 1 转至交换 | 链路聚合。
- 2 单击添加。将显示添加 LAG 端口对话框。

- 3 从聚集端口中选择接口。
- 4 通过在密钥字段中输入所需密钥，指定端口成员到 LAG 组。最小值为 1，最大值为 255。该字段的默认值是 0，必须替换。
- 5 从成员端口下拉菜单中选择要聚合的端口。通过选中要聚合的每个端口的复选框可以选择列表中任意数量的端口。

注： 列出的端口取决于步骤 3 中选择的接口。

- 6 如需为此端口启用链路聚合控制协议 (LACP)，请选择 **LACP 启用**。默认情况下未选中该选项。
- 7 从负载均衡类型中，选择如何执行负载均衡：

ⓘ | 重要： 在创建 LAG 之后，无法修改负载均衡选项。

- SRC_MAC、ETH_TYPE、VLAN、INTF（默认）
- DST_MAC、ETH_TYPE、VLAN、INTF
- SRC_MAC、DST_MAC、ETH_TYPE、VLAN、INTF
- SRC_IP、SRC_PORT
- DST_IP、DST_PORT
- SRC_IP、SRC_PORT、DST_IP、DST_PORT

- 8 单击确定。

删除 LAG

删除 LAG 成员的步骤如下：

- 1 转至系统设置 | 交换 | 链路聚合。
- 2 通过单击删除图标删除 LAG 的成员端口。

删除聚合器端口的步骤如下：

- 1 转至系统设置 | 交换 | 链路聚合。
- 2 通过单击删除图标删除所有成员端口。
ⓘ | 注： 在删除聚合器端口之前，必须从 LAG 删除所有成员端口。
- 3 通过单击删除图标删除聚合器端口。

配置端口镜像

 注：交换功能在所有 NSA 3600 和上述防火墙上可用。

- 第 501 页的 [交换 | 端口镜像](#)
 - 第 501 页的 [关于端口镜像](#)
 - 第 502 页的 [查看被镜像端口](#)
 - 第 502 页的 [配置端口镜像群组](#)
 - 第 503 页的 [编辑端口镜像群组](#)
 - 第 504 页的 [删除端口镜像群组](#)

交换 | 端口镜像

群组						
群组名称	镜像端口	方向	入口	出口	启用	配置
新增群组	X12	入口	0	0	<input checked="" type="checkbox"/>	 
<input type="checkbox"/> X14			0	0		
<input type="checkbox"/> X15			0	0		

主题：

- 第 501 页的 [关于端口镜像](#)
- 第 502 页的 [查看被镜像端口](#)
- 第 502 页的 [配置端口镜像群组](#)
- 第 503 页的 [编辑端口镜像群组](#)
- 第 504 页的 [删除端口镜像群组](#)

关于端口镜像

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。

在 NSA 2650 上，VLAN 中继端口可以是镜像端口或被镜像端口。对于所有其它平台，可以镜像 VLAN 中继端口，但不能将之用作镜像端口本身。

管理 | 系统设置 | 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。

查看被镜像端口

连接镜像端口后，就可以监视被镜像端口上的流量。

群组						
群组名称	镜像端口	方向	入口	出口	启用	配置
新增群组	X12	入口	0	0	<input checked="" type="checkbox"/>	 
X14			0	0		
X15			0	0		

群组名称	接口群组的名称。
镜像端口	用作镜像端口的接口，即用于监控所选方向上的其他端口的端口。
方向	要镜像的流量的方向： <ul style="list-style-type: none">• 两者（双向）• 入口• 出口
入口	到达镜像端口的数据包数目。对于仅出口端口，这始终为 0。
出口	镜像端口上发送的数据包数目。对于仅入口端口，这始终为 0。
启用	指示组的镜像是已启用（已选中复选框）还是已禁用（复选框为空）。
配置	包含组条目的编辑和删除图标和组中每个端口的删除图标。

配置端口镜像群组

创建新端口镜像群组的步骤如下：

- 1 转至交换 | 端口镜像。
- 2 单击新建群组。将显示编辑镜像群组对话框。

- 3 在接口群组名称字段中输入描述性的群组名称。默认名称为新增群组。
- 4 对于方向，选择以下选项之一：
 - 入端口 - 监控到达被镜像端口的流量。
 - 出端口 - 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。
- 5 在所有接口列表中：
 - a 选择流量的镜像端口。镜像端口必须使用未分配的端口。
 - b 单击上方的右箭头按钮以将端口移入镜像端口字段。
- 6 在所有接口列表中：
 - a 选择一个或多个要监视的端口。连接镜像端口后，就可以监视被镜像端口上的流量。
 - b 单击下方的右箭头按钮以将其移入被镜像端口列表。
- 7 如需启用这些端口的端口镜像，请选中启用复选框。

注：一次只能启用一个入口组和一个出口组。如果一个组既有两个方向又处于启用状态，则不能启用单个入口和出口组或另一个具有两个方向的组。单个入口和出口组可以单独启用。在指定镜像端口及其被镜像端口之前，此选项为灰显。
- 8 单击确定。

启用被镜像组

如果在创建镜像组时未启用被镜像组，则可以通过为被镜像组选择启用来在群组表上启用镜像。

编辑端口镜像群组

您可以编辑被镜像组的所有属性，除了灰显的镜像端口。

编辑端口镜像组的步骤如下：

- 1 转至交换 | 端口镜像。
- 2 单击镜像端口的编辑图标。将显示组的编辑镜像群组对话框。



- 3 对任意选项进行更改。

注：可以添加或删除被镜像端口，但不是镜像端口本身。如果删除了群组的某个成员，不会显示任何确认消息。

- 4 如果已为组启用镜像，则选择**启用**。如需禁用这些端口的端口镜像，请取消选择**启用**。

注：一次只能启用一个入口组和一个出口组。如果一个组既有两个方向又处于启用状态，则不能启用单个入口和出口组或另一个具有两个方向的组。单个入口和出口组可以单独启用。

- 5 单击**确定**。

删除端口镜像群组

可以删除镜像组成员、镜像组、多个组或全部组。

主题：

- 第 504 页的[删除端口群组成员](#)
- 第 505 页的[删除端口镜像群组](#)
- 第 505 页的[删除多个端口镜像群组](#)
- 第 506 页的[删除所有端口镜像群组](#)

删除端口群组成员

可以按照第 503 页的[编辑端口镜像群组](#)中所述删除端口群组的成员，也可以在**群组表**中将其删除。

在组表中删除端口群组成员的步骤如下：

- 1 转至交换 | 端口镜像。
- 2 单击群组的展开按钮以显示群组成员。
- 3 您可以
 - 对于要删除的成员，单击删除图标。将显示确认消息。

您确定要删除该镜像成员吗？

- 单击一个或多个要删除的成员的复选框，然后单击删除群组。将显示确认消息。

您确定要删除所有已选条目吗？

- 4 单击确定。

删除端口镜像群组

在“群组”表中删除端口镜像群组的步骤如下：

- 1 您可以
 - 对于要删除的组，单击删除图标。将显示确认消息：

您确定要删除镜像群组吗？

- 选中该组的复选框，然后单击删除群组。将显示确认消息：

您确定要删除所有已选条目吗？

- 2 单击确定。

删除多个端口镜像群组

删除多个端口镜像群组的步骤如下：

- 1 在组表中，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。将显示确认对话框。

您确定要删除所有已选条目吗？

- 3 单击确定。

删除所有端口镜像群组

删除所有端口镜像群组的步骤如下：

- 1 在群组表中，选中表标题中的复选框。
- 2 单击删除群组按钮。将显示确认对话框。

您确定要删除所有已选条目吗？

- 3 单击确认对话框中的确定。

- 关于高可用性和 Active/Active 集群
- 配置高可用性
- 微调高可用性
- 监控高可用性

关于高可用性和 Active/Active 集群

i 注：TZ 系列及以上的安全设备支持高可用性 (HA)。TZ500 系列及以上的安全设备支持状态 HA 和双主机 DPI。请参阅第 516 页的 [Active/Standby](#) 和 [Active/Active DPI 前提条件](#)。NSA 3600 及以上安全设备支持 Active/Active 集群。请参阅第 531 页的 [Active/Active 集群的授权要求](#)。
NAT64 不支持高可用性。

- 第 508 页的高可用性
 - 第 509 页的关于高可用性
 - 第 513 页的关于 Active/Standby HA
 - 第 514 页的关于状态同步
 - 第 515 页的关于 Active/Active DPI HA
 - 第 516 页的 Active/Standby 和 Active/Active DPI 前提条件
 - 第 519 页的维护
- 第 521 页的 Active/Active 集群
 - 第 521 页的关于 Active/Active 集群

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 连接安全设备的方法。

主题：

- 第 509 页的关于高可用性
- 第 513 页的关于 Active/Standby HA
- 第 514 页的关于状态同步
- 第 515 页的关于 Active/Active DPI HA
- 第 516 页的 Active/Standby 和 Active/Active DPI 前提条件
- 第 517 页的物理连接安全设备
- 第 517 页的在 MySonicWall 上注册和关联安全设备
- 第 518 页的授权高可用性功能

关于高可用性

主题:

- [第 509 页的什么是高可用性?](#)
- [第 510 页的高可用性模式](#)
- [第 511 页的崩溃检测](#)
- [第 511 页的虚拟 MAC 地址](#)
- [第 511 页的拥有 PPPoE HA 的动态 WAN 接口](#)
- [第 512 页的利用 DHCP 的状态同步](#)
- [第 512 页的关于 HA 监控](#)

什么是高可用性?

高可用性 (HA) 为冗余设计, 支持配置两个运行 SonicOS 的相同 SonicWall 安全设备来提供可靠、连续的公共互联网连接。一个 SonicWall SuperMassive 配置为主要设备, 另一个相同的安全设备配置为次要设备。如果主要安全设备失效, 次要安全设备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安全设备也称为高可用性对 (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 SonicWall 安全设备可以通过高可用性共享 SonicWall 许可证。两个安全设备必须是相同的 SonicWall 模型。

如需使用该功能, 您必须在 MySonicWall 上将 SonicWall 安全设备注册为已关联产品。如需更多信息, 请参阅 [第 517 页的在 MySonicWall 上注册和关联安全设备](#)。

高可用性术语

活动	硬件设备有效运行的状态。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。
故障切换	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 第 534 页的配置高可用性 中所述的各种可配置物理和逻辑监控设施来判断。
HA	高可用性: 非状态, 硬件故障切换功能。
IDV	通过 VLAN 消除接口歧义。
PoE	以太网供电是一种使网线承载电力的技术。
PPP	点对点协议提供了一种通过点对点链接传输多协议图的标准方法。
PPPoE	通过以太网传输 PPP 的方法。
PPPoE HA	HA PPPoE 支持功能, 无状态。
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。
主要	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 (备份)	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。正常运行条件下, 次要硬件设备处于备用模式。主要设备失效时, 次要设备进入活动模式。

SHF	状态硬件故障切换为 SonicOS 功能，当主安全设备发生故障并且备份安全设备接管时，允许现有网络流保持活动状态。
备用（闲置）	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。
STP	生成树协议。

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 | 基本设置](#)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。
- **Active/Standby** - Active/Standby 模式为基本高可用性功能提供两个完全相同的安全设备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，备用安全设备成为活动安全设备，现有网络连接无中断。

注： 状态监控 HA 已：

- 包含到 NSA 4600 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许可证的 NSA 2600 和 NSA 3600 平台才受支持。
- 仅在含 SonicOS 扩展许可证或高可用性（状态）升级许可证的 TZ500 和更高版本 TZ 平台才受支持。

如需许可信息，请参阅第 517 页的[在 MySonicWall 上注册和关联安全设备](#)和第 518 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安全设备上处理；与此同时，其他服务则在活动安全设备上处理，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 及以上版本平台才受支持。

如需许可信息，请参阅第 517 页的[在 MySonicWall 上注册和关联安全设备](#)和第 518 页的[授权高可用性功能](#)。

- **Active/Active 集群** - 在该模式下，多个安全设备归为一组，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：

- 包含在 SM 9000 系列平台。
- 只有在购买 SonicOS 扩展许可证后，NSA 3600 及以上版本平台才支持 Active/Active 集群。

如需许可信息，请参阅第 517 页的[在 MySonicWall 上注册和关联安全设备](#)和第 518 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。

注： Active/Active DPI 集群：

- 包含在 SM 9000 系列平台。
- 只有在购买 SonicOS 扩展许可证后，NSA 3600 及以上版本平台才支持 Active/Active 集群。

如需许可信息，请参阅第 517 页的在 [MySonicWall 上注册和关联安全设备](#) 和第 518 页的 [授权高可用性功能](#)。

崩溃检测

对于活动和备用安全设备，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，或安全设备断电时，就会切换到备用单元。

自检机制由软件诊断程序管理，用于检查安全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，活动和备用安全设备各有自己的 MAC 地址。这些安全设备使用同一 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。次要安全设备必须发送 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，以主要安全设备的 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，因为主要和次要安全设备使用同一 MAC 地址。发生故障切换时，主要安全设备的所有来往路由对备用安全设备仍然有效。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，此虚拟 MAC 地址由 SonicWall 固件提供，并且不同于主要或次要安全设备的物理 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。您也可以在 [高可用性 | 监控设置](#) 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。

拥有 PPPoE HA 的动态 WAN 接口

注： SuperMassive 9800 不支持拥有 PPPoE HA 的动态 WAN 接口。只支持 DHCP 服务器动态 WAN 模式。

从 SonicOS 6.2.7.0 开始，可以在处于无状态模式、HA Active/Standby 模式的接口上启用 PPPoE。PPPoE HA 提供 HA，当处于活动状态的安全设备发生故障时，次要安全设备承担到 PPPoE 服务器的连接任务。

注： 必须有一个 WAN 接口配置为 PPPoE；请参阅第 248 页的 [配置 WAN 接口](#)。

活动设备连接到 PPPoE 服务器后，安全设备会将 PPPoE 会话 ID 和服务器名称同步到次要设备。

在活动安全设备发生故障时，将通过超时来终止客户端上的 PPPoE HA 连接。然后，次要安全设备连接到 PPPoE 服务器，终止服务器端的原始连接并启动新的 PPPoE 连接。重新建立所有原有的网络连接，重新建立 PPPoE 会话并重新协商 PPP 进程。

利用 DHCP 的状态同步

使用 SonicOS 6.2.7，现在可以在 Active/Standby（无状态）和状态同步模式下的接口上启用 DHCP。

只有活动安全设备才能获得 DHCP 租约。活动安全设备会将 DHCP IP 地址与 DNS 和网关地址同步到次要安全设备。DHCP 客户端 ID 也会进行同步，允许此功能可以在不启用“虚拟 MAC”的情况下也有效。

在故障切换期间，活动安全设备会释放 DHCP 租约且次要安全设备会在变为活动设备时使用现有的 DHCP IP 地址和客户端 ID 续订 DHCP 租约。IP 地址不变，且网络流量（包括 VPN 隧道流量）继续通过。

如果活动安全设备在发生故障切换时无 IP 地址，则次要安全设备将启动新的 DHCP 发现。

利用 DNS 代理的状态同步

DNS 代理支持 DNS 缓存的状态同步。在动态添加、删除或更新 DNS 缓存时，会同步到闲置安全设备。

关于 HA 监控

在高可用性 | 监控设置上，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 对中无任何设备能连接到该设备，则不会采取任何操作。

在高可用性 | 监控设置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。主要和次要安全设备的唯一 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 XO 监控 IP 地址。如果未配置 WAN 监控 IP 地址，则需要 XO 监控 IP 地址，因为在该情况中，备用设备使用 XO 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 SonicWall 许可证服务器进行许可证同步，许可证服务器按安全设备（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 地址访问次要安全设备，同时使用系统管理 | 更新 | 许可证上的链接连接到 SonicWall 服务器（如需更多信息，请参阅 SonicOS 更新）。

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，而非安全设备。但是，如果一个安全设备能 ping 通目标而另一个不能，HA 对将故障切换到能 ping 通目标的设备。

高可用性 | 监控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。

关于 Active/Standby HA

HA 支持配置两个运行 SonicOS 的相同安全设备来提供可靠、连续的公共互联网连接。一个安全设备配置为主要设备，另一个相同的安全设备配置为次要设备。如果主要安全设备失效，备用安全设备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安全设备也称为高可用性对（HA 对）。

Active/Standby HA 提供标准、高可用性和硬件故障切换功能，可以选择启用状态 HA 和 Active/Active DPI。

当一个安全设备用作另一个安全设备的高可用性系统时，这两个安全设备可以通过 HA 共享许可证。如需使用该功能，您必须在 MySonicWall 上将安全设备注册为已关联产品。两个安全设备必须是相同的 SonicWall 模型。

主题：

- 第 513 页的 [Active/Standby HA 的优点](#)
- 第 513 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，次要安全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** - 对于通过使用冗余安全设备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，不同于主要或次要安全设备的物理 MAC 地址。

Active/Standby HA 的工作方式

i 注：TZ300 系列和 TZ400 系列安全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 安全设备配置为主要 SonicWall，另一个相同的安全设备配置为次要 SonicWall。正常运行期间，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 SonicWall 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。故障切换到次要安全设备之后，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，请参阅第 514 页的 [关于状态同步](#)。

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。

关于状态同步

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，当主要安全设备失效时，次要防火墙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，请参阅第 517 页的[在 MySonicWall 上注册和关联安全设备](#)和第 518 页的[授权高可用性功能](#)。

主题：

- 第 514 页的[状态监控同步的优点](#)
- 第 514 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安全设备故障引起停机 and 连接丢失。
- **更快速的故障切换性能** - 通过维护主要和次要安全设备之间的持续同步，状态监控同步支持次要安全设备在故障情况下接管，几乎无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，主要安全设备处理所有流量。状态监控同步启用时，主要安全设备主动与次要设备通信，更新大部分网络连接信息。当主要安全设备创建和更新网络连接信息（例如 VPN 隧道、活动用户、连接缓存条目等）时，它会立即告知次要安全设备。这样就确保了次要安全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安全设备上进行，并自动传播到次要安全设备。无论哪一台安全设备当前是活动的，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) 管理安全设备时，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安全设备的 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。

[已同步和未同步的信息](#)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。

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	同步泛洪攻击保护信息
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

已同步和未同步的信息

已同步的信息	未同步的信息
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，主要安全设备为该用户创建一个会话。
- 2 主要安全设备与次要安全设备同步。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 次要安全设备开始向 LAN 和 WAN 交换机发送无故 ARP 消息，使用与主要安全设备相同的虚拟 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，次要安全设备拥有该用户的所有会话信息，能不间断地继续该用户的会话。

关于 Active/Active DPI HA

重要：但是，在 Active/Active DPI 模式下不支持捕获功能。

状态监控 HA 对启用 Active/Active DPI 时，深层数据包检查服务在 HA 对的备用安全设备上处理，与此同时，安全设备、NAT 和其他模块的处理则在活动安全设备上处理。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

如需使用 Active/Active DPI 功能，您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 5600 和 NSA 6600 上支持 Active/Active DPI。如需许可信息，请参阅第 517 页的在 [MySonicWall 上注册](#) 和 [关联安全设备](#) 和第 518 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。

主题：

- 第 516 页的 [HA 的支持平台](#)
- 第 517 页的 [物理连接安全设备](#)
- 第 517 页的 [连接 Active/Active DPI 的 Active/Active DPI 接口](#)
- 第 517 页的 [在 MySonicWall 上注册和关联安全设备](#)
- 第 518 页的 [授权高可用性功能](#)

HA 的支持平台

购买 SonicWall 安全设备时包括的许可证显示在 [HA](#)、[有状态 HA](#) 和 [A/A DPI](#) 的 [授权要求表](#)。有些平台需要附加授权才能使用 HA 特性。HA 升级和扩展许可证可通过 [MySonicWall](#) 或 SonicWall 分销商购买。

注： HA 许可证必须在各个安全设备上激活，方法是在 SonicOS 管理界面的 [MySonicWall](#) 上注册设备，或将许可证密钥组应用到各设备（如果互联网访问不可用）。

HA、有状态 HA 和 A/A DPI 的授权要求

平台	HA	状态监控 HA	A/A DPI
SM 9600	包含	包含	包含
SM 9400	包含	包含	包含
SM 9200	包含	包含	包含
NSA 6600	包含	包含	扩展许可证
NSA 5600	包含	包含	扩展许可证
NSA 4600	包含	包含	N/A
NSA 3600	包含	扩展许可证或 HA 许可证	N/A
NSA 2600	包含	扩展许可证或 HA 许可证	N/A
TZ600	包含	有状态的 HA 升级或扩展许可证	不适用
TZ500/TZ500 W	包含	有状态的 HA 升级或扩展许可证	N/A
TZ400/TZ400 W	包含	N/A	N/A
TZ300/TZ300 W	包含	N/A	N/A
SOHO W	N/A	N/A	N/A

可以在 [管理 | 更新 | 许可证](#) 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，请参阅第 517 页的 [在 MySonicWall 上注册和关联安全设备](#)。

物理连接安全设备

注：如需连接安全设备的完整步骤，请参阅安全设备的入门指南。如需连接 Active/Active 集群安全设备的步骤，请参阅第 532 页的[连接 Active/Active 集群的 HA 端口](#)和第 532 页的[连接冗余端口接口](#)。

如果将主要和次要安全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 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 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 SonicWall 安全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无 X0，则 HA 控制链路断开时，两个设备都变为活动设备。

WAN 互联网连接可用于在 MySonicWall 上注册安全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安全设备之间连接至少一个附加接口，称为 **Active/Active DPI 接口**。两个安全设备的相连接口必须是同一号码，且必须是**管理|系统设置网络|接口**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 有端口冗余，可以在各 HA 对的两台安全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。

如需连接 Active/Active DPI 的 Active/Active DPI 接口，请执行以下步骤：

- 1 决定将哪一个接口用于 HA 对的安全设备之间的附加连接。各台安全设备必须选择同一接口。
- 2 在 SonicOS 管理界面上，转至**管理|系统设置|网络|接口**，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 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 上注册和关联安全设备

如需使用高可用性，您必须注册这两个安全设备并进行关联，以用于 MySonicWall 的高可用性。在 MySonicWall 页面单击已注册安全设备的链接时，将显示该安全设备的“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。如需注册安全设备的更多信息，请参阅安全设备的入门指南。

安全设备关联为 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。

主要和次要安全设备不要求启用相同的安全服务。安全服务设置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安全设备保持与故障切换之前相同的网络保护级别。

MySonicWall 提供了几种关联两个安全设备的方法。可以注册一台新安全设备，然后选择一台已注册设备与之关联。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，再添加一台新安全设备与之关联。

重要：即使您已先在 MySonicWall 注册您的安全设备，在登录每个防火墙单独的管理 IP 地址时，仍需要在 SonicOS 管理界面上分别注册主要和次要安全设备。这将使次要设备可以和 SonicWall 许可证服务器同步，并与关联的主要安全设备共享许可证。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安全设备。

授权高可用性功能

购买 SonicWall 安全设备时包括的 HA 许可证显示在随 SonicWall 安全设备提供的 HA 许可证表。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 SonicWall 分销商购买。

注：状态监控高可用性许可证必须在各个安全设备上激活，方法是在 SonicOS 管理界面的 MySonicWall 上注册设备，或将许可证密钥组应用到各设备（如果互联网访问不可用）。

随 SonicWall 安全设备提供的 HA 许可证

平台	Active/Standby HA ^a	状态监控 HA	A/A 集群	A/A DPI
SM 9600	包含	包含	包含	包含
SM 9400	包含	包含	包含	包含
SM 9200	包含	包含	包含	包含
NSA 6600	包含	包含	扩展许可证	扩展许可证
NSA 5600	包含	包含	扩展许可证	扩展许可证
NSA 4600	包含	包含	扩展许可证	N/A
NSA 3600	包含	扩展许可证 HA 许可证	扩展许可证	N/A
NSA 2650	包含	扩展许可证 HA 许可证	N/A	N/A
NSA 2600	包含	扩展许可证 HA 许可证	不适用	N/A
TZ600	包含	扩展许可证 有状态 HA 升级许可证	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
TZ400/TZ400 W	包含	N/A	N/A	N/A
TZ300/TZ300 W	包含	N/A	N/A	N/A
SOHO W	N/A	N/A	N/A	N/A

a. NA = 功能不可用

可以在 [管理](#) | [更新](#) | [许可证](#) 上查看系统许可证。通过此页面还可以登录 MySonicWall 及将许可证应用到安全设备。如需更多信息，请参阅 [SonicOS 升级](#)。

如果 HA 对中的安全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安全设备。在 MySonicWall 上注册安全设备时，会生成该安全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安全设备时，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 对中的两个安全设备均必须应用许可证密钥组。

维护

主题：

- [第 519 页的移除 HA 关联](#)
- [第 520 页的更换 SonicWall 安全设备](#)

移除 HA 关联

可以随时在 MySonicWall 上移除两个 SonicWall 安全设备之间的关联。如果更换安全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 SonicWall 安全设备失效，就需要更换。您也可以需要将 HA 主要与次要安全设备或 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，新关联将使用新安全设备或改变两台设备之间的父子关系（请参阅 [第 520 页的更换 SonicWall 安全设备](#)）。

如需移除两台已注册的 SonicWall 安全设备之间的关联，请执行以下步骤：

- 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安全设备。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，移除该安全设备的关联的步骤如下：
 - 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。

PARENT PRODUCT			
Parent Product Type	Friendly Name	Serial Number	
HF Primary	Techpubs1 NSA E7500	0017C51A2D0D	Remove

Are you sure you want to remove this Parent product Association? If yes then click 'Remove' again.

PARENT PRODUCT			
Parent Product Type	Friendly Name	Serial Number	
HF Primary	Techpubs1 NSA E7500	0017C51A2D0D	Remove

更换 SonicWall 安全设备

如果您的 SonicWall 安全设备发生硬件故障并还在保修期内，SonicWall 可进行更换。您需要在 MySonicWall 上移除包含故障安全设备的 HA 关联，并添加包含替换设备的新 HA 关联。如果您联系 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。

使用新设备替换设备架中发生故障的安全设备后，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 520 页的[更换 HA 主要设备](#)
- 第 520 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 SonicOS 安全设备（次要设备）的 SonicWall 管理界面的“高可用性”页面中，取消选中启用高可用性以禁用该功能。
- 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 SonicWall 序列号”字段中。
- 3 在次要 **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。请参阅第 519 页的[移除 HA 关联](#)。
- 6 在 MySonicWall 中，注册替换 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。请参阅第 517 页的[在 MySonicWall 上注册和关联安全设备](#)。
- 7 请联系 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 519 页的[移除 HA 关联](#)的说明移除旧的 HA 关联。
- 2 在 MySonicWall 中，注册替换的 SonicWall 安全设备。
- 3 按照第 520 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。

Active/Active 集群

i 注：NSA 3600 及以上安全设备支持 Active/Active 集群。请参阅 [A/A 集群的授权要求表](#) 和 [随 SonicWall 安全设备提供的 HA 许可证表](#)

关于 Active/Active 集群

Active/Active 集群由一组最多四个集群节点组成，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。一个集群节点可以包含状态监控 HA 对、具有标准故障切换的无状态 HA 对或单个独立设备，这种情况下，状态监控故障切换和 Active/Active DPI 不可用。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。

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。

典型的建议设置包括四个相同型号的 SonicWall 安全设备，配置为两个集群节点，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 个安全设备，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 并非必需的，但强烈建议使用，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安全设备，这种情况下，Active/Active 集群设置可以利用两个安全设备来构建。其中一个安全设备发生故障时，故障切换不是状态监控式，因为集群节点中的任一安全设备都没有 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，次要安全设备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安全设备或节点。
- 可以启用 Active/Active DPI，提高各集群节点内的吞吐量。

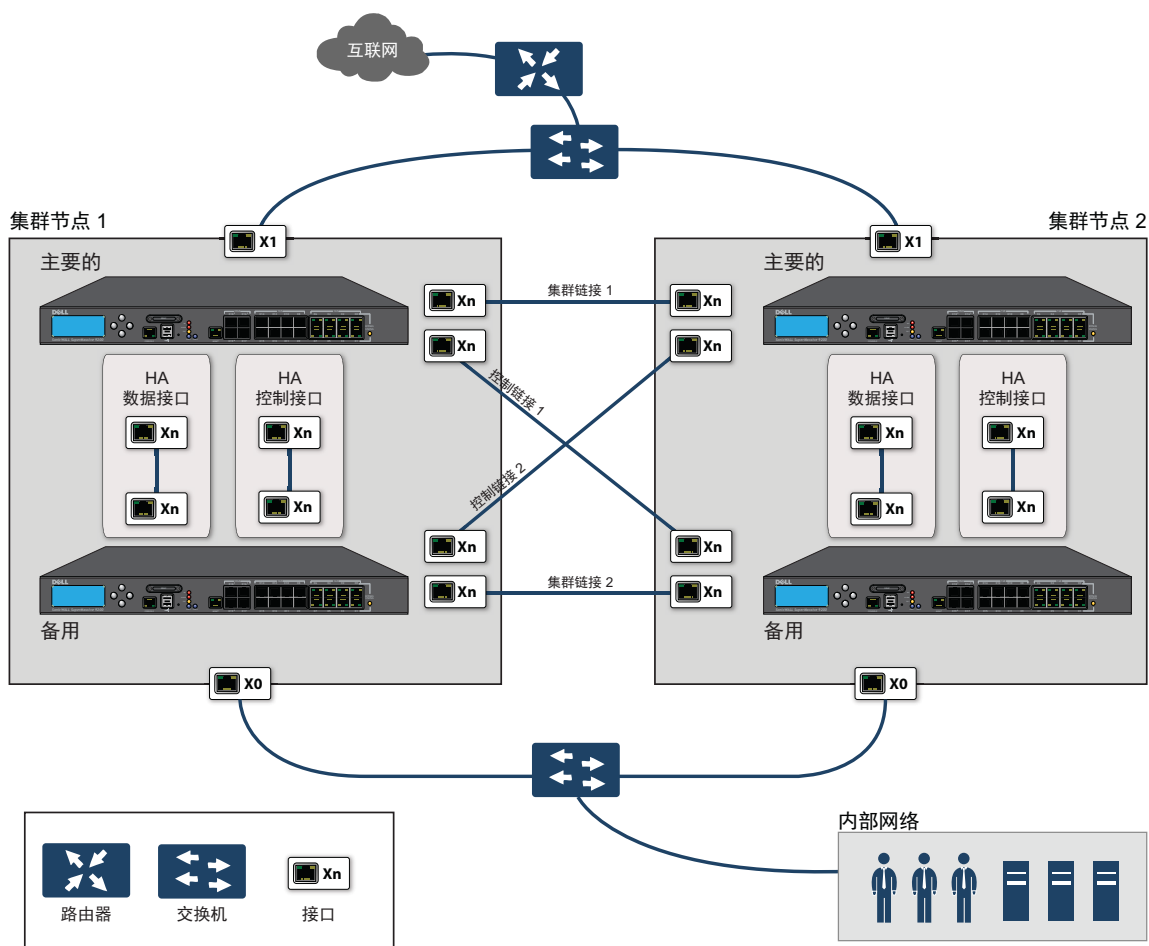
主题：

- [第 522 页的示例：Active/Active 集群 - 四设备部署](#)
- [第 523 页的示例：Active/Active 集群 - 二设备部署](#)
- [第 523 页的 Active/Active 集群的优点](#)
- [第 524 页的 Active/Active 集群的工作方式](#)
- [第 529 页的 Active/Active 集群支持的功能](#)

示例：Active/Active 集群 - 四设备部署

Active/Active 四设备集群显示了一个四设备集群。各集群节点包含一个 HA 对。所有四台安全设备的指定 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。

Active/Active 四设备集群

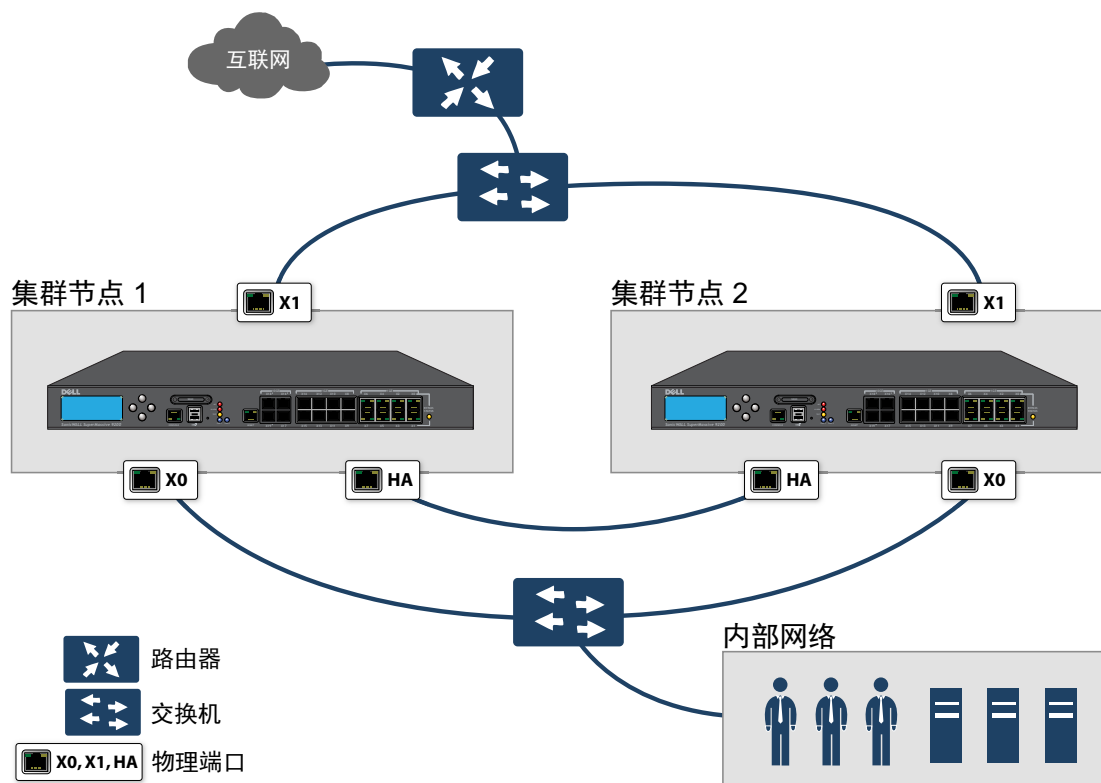


如需物理连接冗余端口和冗余交换机的更多信息，请参阅“Active/Active 集群全网格部署技术说明”。

示例：Active/Active 集群 - 二设备部署

Active/Active 二设备集群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安全设备。两台安全设备上的指定 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安全设备传送。HA 端口连接还用于集群节点间的配置同步。

Active/Active 二设备集群



Active/Active 集群的优点

Active/Active 集群拥有如下优点：

- 集群中的所有安全设备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 对的备用安全设备上并行处理 IPS、GAV、防间谍软件 and 应用程序规则服务（这些都是处理器需求最为密集的服务），同时在活动安全设备上执行其他处理。
- 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。

主题：

- [第 524 页的关于集群节点](#)
- [第 524 页的关于集群](#)
- [第 526 页的关于虚拟群组](#)
- [第 527 页的关于 SVRRP](#)
- [第 527 页的关于故障切换](#)
- [第 528 页的关于 DPI 和 Active/Active 集群](#)
- [第 528 页的关于使用活动/集群的高可用性监控](#)

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

集群中所有安全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，所有安全设备彼此相连和通信；请参阅 [Active/Active 二节点集群](#)。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。

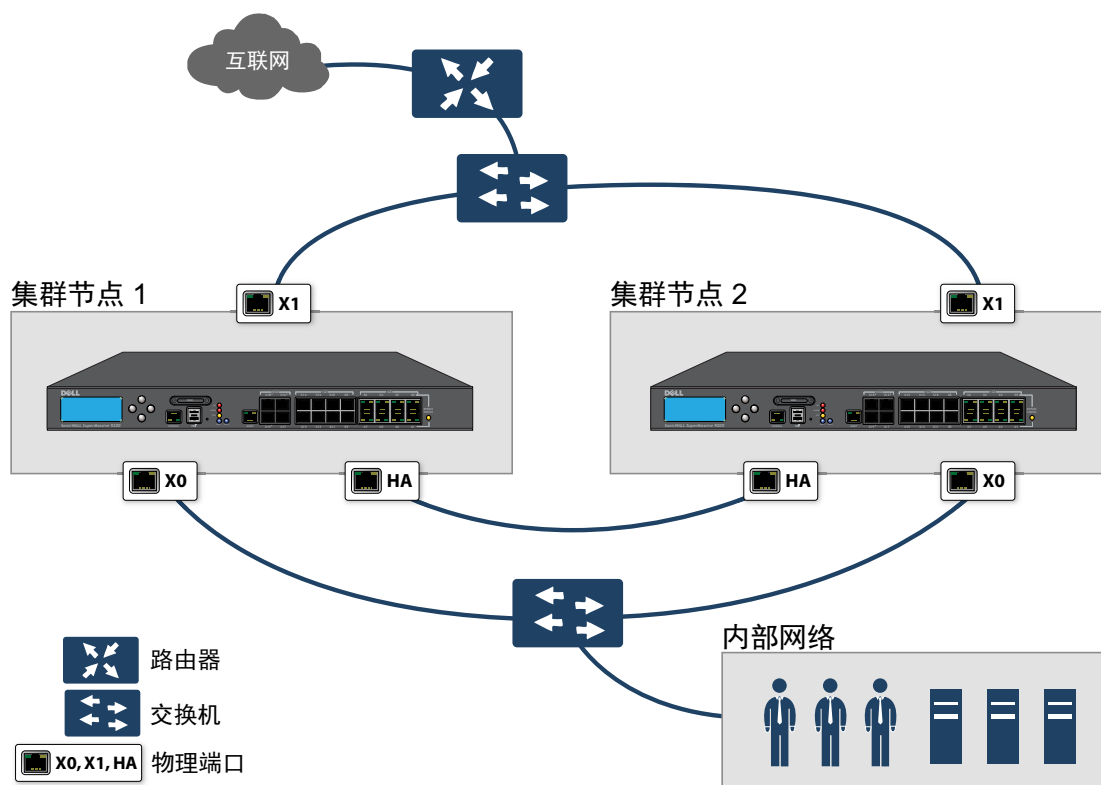
所有集群节点共享同一配置，由主节点同步。主节点还负责将固件同步到集群中的其他节点。HA 端口连接用于同步配置和固件更新。

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 527 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，则该集群包括八个安全设备。

Active/Active 二节点集群



集群内允许的操作

允许的管理操作类型取决于集群中安全设备的状态。在主节点的活动安全设备上，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。在非主节点的活动安全设备上，仅允许执行一部分操作，在处于备用状态的安全设备上可以执行的操作更少。**允许的管理操作**表列出了非主节点的活动安全设备和集群中的备用安全设备允许的操作。

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
在调查 工具 系统诊断中的诊断工具（如需这些工具的更多信息，请参阅 SonicOS 调查 ）。	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 对端）	不允许	不允许
HA 同步固件（固件同步到节点内的 HA 对端）	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/未分配的接口无虚拟 IP 地址）。首次启用 Active/Active 集群时，该安全设备上的接口的已配置 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，将集群中其他安全设备的序列号输入 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**管理 | 系统设置网络 | 接口**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** - 指虚拟群组中正常运行且配置了虚拟 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安全设备。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感知多重网关的外部 DHCP 服务器，以便发布网关分配。

i | **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**管理 | 系统设置 | 网络 | 接口**上查看这些虚拟 IP 地址。

i | **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**管理 | 策略 | 规则**上查看这些 NAT 策略！**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。如需 NAT 策略的信息，请参阅 SonicOS 策略。

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。

如果 Active/Active 集群链路发生故障，SVRRP 心跳消息通过 X0 接口发送。然而，在 Active/Active 集群链路停止运行期间，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：

- 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 对中的备用安全设备负载很轻，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 对中的备用安全设备进行 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 对中的备用安全设备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**管理 | 系统设置 | 高可用性 | 监控设置**上逐个节点地增加监控配置。

i | **注：**高可用性 | 监控设置仅适用于您登录的 HA 对，而非整个集群。

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。

i | **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**管理 | 系统设置 | 高可用性 | 监控设置**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。主要和次要安全设备的唯一 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。

i | **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，许可证服务器按安全设备（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 地址访问备用安全设备，同时使用**管理 | 更新 | 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 SonicWall 认为问题出在目标，而非 SonicWall。但是，如果一个 SonicWall 能 ping 通目标，另一个 SonicWall 不能，HA 对将故障切换到能 ping 通目标的 SonicWall。

管理 | 系统设置 | 高可用性 | 监控设置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 集群支持的功能

主题：

- 第 529 页的 [注意](#)
- 第 529 页的 [向后兼容性](#)
- 第 529 页的 [SonicPoint 兼容性](#)
- 第 529 页的 [WAN 负载均衡兼容性](#)
- 第 530 页的 [路由拓扑和协议兼容性](#)

注意

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
- 有线模式

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 SonicPoint 或 SonicWave 与 Active/Active 集群一同使用时，有两点需要考虑：

- SonicPoint 和 SonicWave 仅与主节点通信，用于下载固件和其他方面的操作。
- SonicPoint 和 SonicWave 需要访问独立 DHCP 服务器。SonicPoint 和 SonicWave 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。

主题：

- 第 530 页的 [2 层网桥支持](#)
- 第 530 页的 [OSPF 支持](#)
- 第 530 页的 [RIP 支持](#)
- 第 531 页的 [BGP 支持](#)
- 第 531 页的 [集群配置中的非对称路由](#)

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，并将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（请参阅 SonicOS 6.2 CLI 参考指南）。

集群配置中的非对称路由

当流量流过安全设备上的不同二层桥接对接口或它流过高可用性集群中的不同安全设备时，SonicOS 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 516 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 集群链接** - 各 Active/Active 集群链接必须至少是 100MB 接口，但最好是 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 534 页的 [高可用性 | 基本设置](#)。

主题：

- 第 531 页的 [Active/Active 集群的授权要求](#)
- 第 532 页的 [连接 Active/Active 集群的 HA 端口](#)
- 第 532 页的 [连接冗余端口接口](#)

Active/Active 集群的授权要求

购买 SonicWall 安全设备时包括的 Active/Active 集群许可证显示在 [A/A 集群的授权要求表](#)。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 SonicWall 分销商购买。

注：Active/Active 集群许可证必须在各个安全设备上激活，方法是在 SonicOS 管理界面的 [MySonicWall](#) 上注册设备或将许可证密钥组应用到各设备（如果互联网访问不可用）。

A/A 集群的授权要求

平台	许可证要求 ^a
SM 9600	包含
SM 9400	包含
SM 9200	包含
NSA 6600	扩展许可证
NSA 5600	扩展许可证
NSA 4600	扩展许可证
NSA 3600	扩展许可证
NSA 2650	N/A
NSA 2600	N/A

A/A 集群的授权要求

平台	许可证要求 ^a
TZ600	N/A
TZ500/TZ500 W	N/A
TZ400/TZ400 W	N/A
TZ300/TZ300 W	N/A
SOHO W	N/A

a. N/A = 不适用；包含 = 包含在基本许可证中

可以在[管理 | 更新 | 许可证](#)上查看系统许可证。通过此页面还可以登录 MySonicWall。如需许可证信息：

- 通常，请参阅 SonicOS 更新。
- HA 安全设备，请参阅第 517 页的[在 MySonicWall 上注册和关联安全设备](#)。

如果 Active/Active 集群中的安全设备可以接入互联网，则必须在您登录各个安全设备的管理 IP 地址的同时，从 SonicOS 管理界面分别注册集群中的各个安全设备。这将使次要设备可以和 SonicWall 许可证服务器同步，并与关联的主要安全设备共享许可证。

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 建议将所有指定 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安全设备，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安全设备传送。

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。

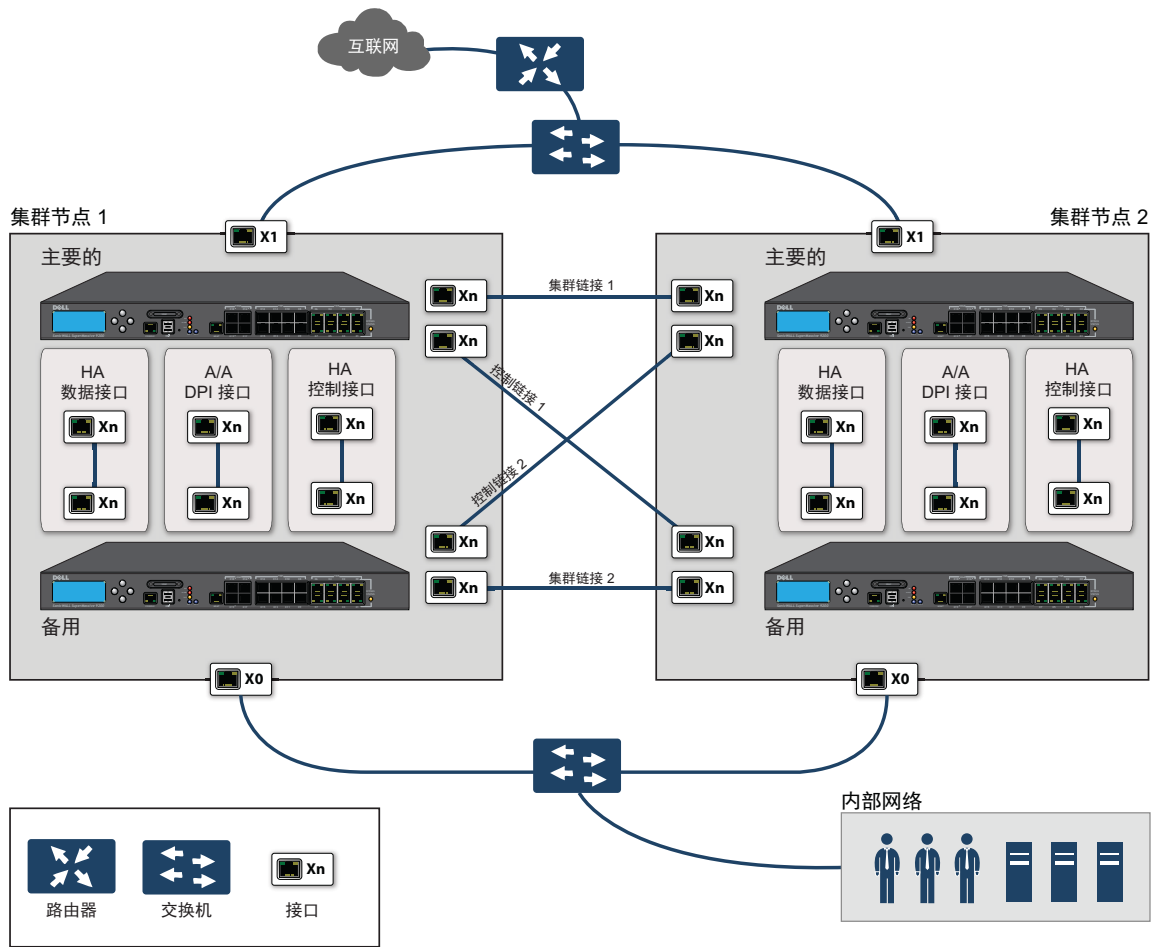
注：由于所有集群节点共享同一配置，因此各节点必须配置相同的冗余端口并将其连接到相同的交换机。

如需使用 Active/Active 集群，必须在 SonicWall 安全设备上注册集群中的所有 MySonicWall。各 HA 对中的两个安全设备还必须在 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 对中的两台安全设备，再关联集群节点 2 的 HA 对中的两台安全设备，依此类推关联所有其它集群节点。

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。请参阅 [Active/Active DPI 集群高可用性](#)。

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。

配置高可用性

重要：高可用性不能和 PortShield 一起使用，但是 SonicWall X-系列解决方案除外。在配置 HA 之前，从管理 | 系统设置 | 网络 | PortShield 组中删除任何已有的 PortShield 配置。如需将 HA 与 PortShield 一起使用，请参阅第 296 页的 X-系列交换机的 SonicOS 支持和 *SonicWall X-系列解决方案部署指南*。

- 第 534 页的高可用性 | 基本设置
 - 第 535 页的配置 Active/Standby 高可用性设置
 - 第 538 页的配置 Active/Active DPI 高可用性设置

高可用性 | 基本设置

The screenshot shows the 'HA 设备' configuration page. At the top, there are three tabs: '常规', 'HA 设备', and 'HA 接口'. The 'HA 设备' tab is active. Below the tabs, there is a '模式:' label followed by a dropdown menu currently showing '无'. Underneath, there are four checkboxes, all of which are unchecked:

- 启用状态同步
- 当升级固件时生成/重写备份固件和设置
- 启用抢占模式
- 启用虚拟 MAC

可以在管理 | 系统设置 | 高可用性 | 基本设置上配置高可用性 (HA)：

- 第 535 页的配置 Active/Standby 高可用性设置
- 第 536 页的配置动态 WAN 接口的高可用性
- 第 538 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 509 页的关于高可用性和第 516 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 配置后参阅第 546 页的配置 Active/Active 集群的 VPN 和 NAT。

只有当 X0 或任一 WAN 接口配置了 HA 监控 IP 地址后，备用安全设备上的许可证和签名才会更新。如果这些接口尚未设置，将显示一条消息：

只有当 X0 或任何一个 WAN 接口配置了 HA 监测 IP 后，备用防火墙上的许可证和签名才会更新。

配置 Active/Standby 高可用性设置

高可用性 | 基本设置页面上的配置任务在主要防火墙上进行，然后自动同步到次要防火墙。

配置活动/备用的步骤如下：

- 1 转至系统设置 | 高可用性 | 基本设置。

- 2 从模式中，选择主动/备用。
- 3 选择启用状态同步。默认情况下未选中该选项。

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。

将显示推荐消息。

状态同步的推荐设置：
1000 毫秒的检测间隔
5 秒的探测间隔。

- 4 单击确定。
- 5 如需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。默认情况下未选中该选项。
- 6 如需配置高可用性对使主要防火墙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。默认情况下未选中该选项。

提示： 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防火墙可能极不友好。

- 7 选中启用虚拟 MAC，以允许主要防火墙和次要防火墙共享一个 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。默认情况下未选中该选项。

重要： 如果配置“PPPoE 未编号”，则必须选择启用虚拟 MAC。

只需要通知这两个防火墙与之相连的交换机。所有外围设备将继续发送到该单一共享 MAC 地址。

- 单击 **HA 设备** 以配置次要防火墙序列号。将显示主要设备的序列号，该字段为灰色且无法编辑。

常规 HA 设备 HA 接口

主要设备 备份设备

序列号: C0EAE4598E24 序列号: 000000000000

- 输入备份设备的序列号。

- 单击 **HA 接口**。

常规 HA 设备 HA 接口

HA 控制接口: --选择接口--

HA 数据接口: --选择接口--

- 选择用作 **HA 控制接口** 的接口。如果防火墙检测到已配置该接口，此选项将以灰色显示并显示该接口。
- 选择用作 **Active/Active DPI** 接口的接口。如果防火墙检测到已配置该接口，此选项将以灰色显示并显示该接口。
- 完成所有高可用性配置后，单击**接受**。所有设置将同步到次要防火墙，然后重启次要防火墙。

配置动态 WAN 接口的高可用性

高可用性 | 基本设置页面上的配置任务在主要防火墙上进行，然后自动同步到次要防火墙。

配置动态 WAN 接口的高可用性的步骤如下：

- 转至管理 | 系统设置 | 网络 | 接口。
- 配置 WAN 接口作为 PPPoE，如第 248 页的[配置 WAN 接口](#)中所述。
- 转至高可用性 | 基本设置。

常规 HA 设备 HA 接口

模式: 无

启用状态同步

当升级固件时生成/重写备份固件和设置

启用抢占模式

启用虚拟 MAC

- 从模式中选择 HA 模式。如果选择 **Active/Active DPI** 或 **Active/Active 集群**，则会显示有关许可证和签名更新的消息。

只有当 X0 或任何一个 WAN 接口配置了 HA 监测 IP 后，备用防火墙上的许可证和签名才会更新。

- 5 单击确定。
- 6 确保未选中启用状态同步。默认情况下未选中该选项。
- 7 确保启用抢占模式为不选中。默认情况下未选中该选项。
- 8 选择启用虚拟 MAC。默认情况下未选中该选项。
- 9 按照第 535 页的 [配置 Active/Standby 高可用性设置](#) 中的描述配置 HA 设备和 HA 接口选项。
- 10 单击应用。
- 11 转至高可用性 | 监控设置。

监控设置							
视图 IP 类型: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6							
名称	主要 IP 地址	次要 IP 地址	探测 IP 地址	物理/链接...	逻辑/探测...	管理	配置
X0	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X4	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V63	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V66	0.0.0.0	0.0.0.0	0.0.0.0				
X7	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X10	0.0.0.0	0.0.0.0	0.0.0.0				
X11	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				
X16	0.0.0.0	0.0.0.0	0.0.0.0				
X17	0.0.0.0	0.0.0.0	0.0.0.0				

- 12 单击 PPPoE 接口的配置图标。将显示编辑 HA 监控对话框。

接口 X0 监控设置

启用物理/链接监控

主要 IPv4 地址:

次要 IPv4 地址:

允许主要/次要 IPv4 地址的管理

逻辑/探测 IPv4 地址:

覆盖虚拟 MAC:

- 13 选择启用物理/链接监控复选框。默认情况下未选中该选项。
- 14 确保主要 IPv4 地址和次要 IPv4 地址字段设置为 0.0.0.0。
- 15 确保未选中其他选项。
- 16 单击确定。

配置 Active/Active DPI 高可用性设置

管理 | 系统设置 | 高可用性 | 基本设置页面上的配置任务在主要防火墙上进行，然后自动同步到次要防火墙。

配置 Active/Active DPI 的步骤如下：

- 1 转至高可用性 | 基本设置。

常规 HA 设备 HA 接口

模式: 无

启用状态同步

当升级固件时生成/重写备份固件和设置

启用抢占模式

启用虚拟 MAC

- 2 在模式下拉菜单中，选择 **Active/Active DPI**。显示有关许可证和签名更新的消息。

只有当 X0 或任何一个 WAN 接口配置了 HA 监测 IP 后，备用防火墙上的许可证和签名才会更新。

- 3 单击确定。

Active/Active DPI 的启用状态同步选项会自动启用，该选项为灰色。

- 4 如需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。默认情况下未选中该选项。
- 5 一般情况下，应禁用 Active/Active DPI 的抢占模式。确保启用抢占模式为不选中。默认情况下未选中该选项。

注：此选项要求主要防火墙在失效重启后立即恢复主要角色，因此仅适用于 Active/Standby 配置。

- 6 如需允许 HA 对的两个安全设备共享一个 MAC 地址，请选择启用虚拟 MAC。此选项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。只需要通知这两个安全设备与之相连的交换机。所有外围设备将继续发送到该单一共享 MAC 地址。默认情况下未选中该选项。

7 单击 **HA 设备** 选项卡。将显示主要设备的序列号，该字段为灰色且无法编辑。



8 输入备份设备的序列号。

9 单击 **HA 接口**。



10 从 **HA 控制接口** 中选择 HA 控制接口。如果安全设备检测到已配置该接口，此选项将以灰色显示并显示该接口。

11 选择 **HA 数据接口** 的接口号。如果安全设备检测到已配置该接口，此选项将以灰色显示并显示该接口。

12 选择用作 **Active/Active DPI 接口** 的接口号。如果安全设备检测到已配置该接口，此选项将以灰色显示并显示该接口。

在 Active/Active DPI 处理期间，此接口用于在这两个安全设备之间传输数据。下拉菜单中仅出现未分配的可用接口。两台安全设备的相连接口必须是同一号码，且必须是**管理 | 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**接受**。所有设置将同步到备用安全设备，备用安全设备将重启。

配置 Active/Active 集群

主题：

- 第 539 页的[配置 Active/Active 集群高可用性](#)
- 第 541 页的[配置 Active/Active 集群高可用性监控](#)
- 第 543 页的[配置 Active/Active DPI 集群高可用性](#)
- 第 546 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。各节点可以包含一个安全设备或一个 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 转至管理 | 系统设置 | 高可用性 | 基本设置。

常规 HA 设备 HA 接口

模式: 无

启用状态同步

当升级固件时生成/重写备份固件和设置

启用抢占模式

启用虚拟 MAC

- 3 在模式下拉菜单中，选择主动/主动聚类。显示有关许可证和签名更新的消息。

只有当 X0 或任何一个 WAN 接口配置了 HA 监测 IP 后，备用防火墙上的许可证和签名才会更新。

- 4 单击确定。HA 设备更改为 HA 设备和节点。
- 5 选择启用状态同步。
- 6 如需在上传新固件到安全设备时自动创建固件和配置设置的备份，请选择当升级固件时生成/重写备份固件和设置。当主节点将新安全设备同步到集群中的其他安全设备时，就会在这些安全设备上创建备份设备。
- 7 如需配置 Active/Active 集群信息，请单击 HA 设备和节点。

常规 HA 设备和节点 HA 接口

⊕ 添加 ⊖ 删除 ✓ 接受 ✕ 取消

集群节点 ID	主要设备序列号 #	备份设备序列号 #	虚拟群组 1 级别	虚拟群组 2 级别
1	C0EAE4598E24	000000000000	主机	备用
2	000000000000	000000000000	备用	主机

- 8 在集群节点表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安全设备的序列号。
- 9 从虚拟群组 n 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，通常将其确定为其它群组的备用节点。
如需从一个集群中排除一个安全设备，其虚拟群组 n 级别请选择无。
- 10 在第二行，在虚拟群组 n 级别下拉菜单中选择集群节点 2 针对各虚拟群组的等级。

11 单击 HA 接口。



12 从 HA 控制接口中选择 HA 控制接口。如果安全设备检测到已配置该接口，此选项将以灰色显示并显示该接口。

13 选择启用切换的 Active/Active 集群链接。这些选项将发生更改。



14 从 Active/Active 集群链接中选择在 Active/Active 处理期间用于在这两台设备之间传输数据的接口。仅列出了未分配的可用接口。

15 如果选择启用切换的 Active/Active 集群链接，请转至 [步骤 17](#)。

16 从 Active/Active 集群链接 2 中选择在 Active/Active 处理期间用于在这两台设备之间在第二条链接传输数据的接口。仅列出了未分配的可用接口。

17 单击应用。所有设置将同步到备用设备，备用设备将重启。

18 转到高可用性 | 监控设置并按照第 541 页的 [配置 Active/Active 集群高可用性监控](#) 中的步骤进行操作。

19 转到高可用性 | 高级设置并按照第 556 页的 [高可用性 | 高级设置](#) 中的步骤进行操作。

20 转到 [管理 | 系统设置 | 网络 | 接口](#) 页面，验证您已成功配置所需的 Active/Active 接口。

21 转到高可用性 | 监控设置以验证 Active/Active 集群设置。

配置 Active/Active 集群高可用性监控

高可用性 | 监控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。这些设置仅影响页面顶部选择的集群节点中的 HA 对。

监控设置

视图 IP 类型: IPv4 IPv6

名称	主要 IP 地址	次要 IP 地址	探测 IP 地址	物理/链接...	逻辑/探测...	管理	配置
X0	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X4	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V63	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V66	0.0.0.0	0.0.0.0	0.0.0.0				
X7	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X10	0.0.0.0	0.0.0.0	0.0.0.0				
X11	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				
X16	0.0.0.0	0.0.0.0	0.0.0.0				
X17	0.0.0.0	0.0.0.0	0.0.0.0				

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 转至管理 | 系统设置 | 高可用性 | 监控设置。
- 3 在页面右上侧，从下拉菜单中选择要配置的设备。
- 4 单击 LAN 上某个接口的配置图标，例如 X0。
- 5 如需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。

接口 X0 监控设置

启用物理/链接监控

主要 IPv4 地址:

次要 IPv4 地址:

允许主要/次要 IPv4 地址的管理

逻辑/探测 IPv4 地址:

覆盖虚拟 MAC:

- 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 选中允许主要/次要 IPv4 地址的管理复选框。启用某一接口的这个选项时，在管理 | 系统设置 | 高可用性 | 监控设置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 IPv4 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）。主要和次要防火墙将定期 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，如果一个防火墙能 ping 通目标，另一个不能，则会故障切换到能 ping 通目标的防火墙。

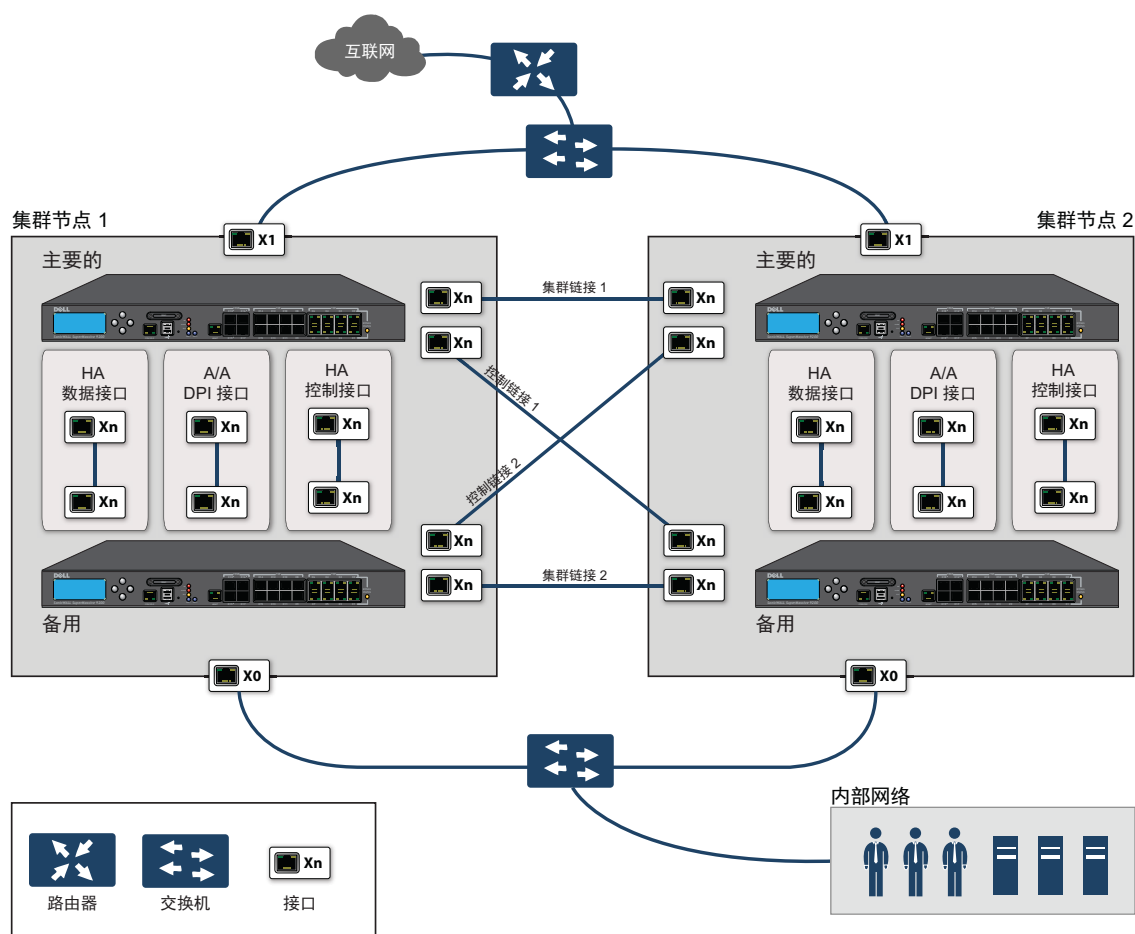
主要 IP 地址和次要 IP 地址字段必须用 LAN 接口（如 X0）或 WAN 接口（如 X1，用于探测 WAN）上的独立 IP 地址配置，以便对功能是否正常进行逻辑探测。
- 10 单击确定。
- 11 如需配置任何其他接口的监控，请重复上述步骤。
- 12 完成选定集群节点的所有高可用性监控配置后，单击应用。
- 13 也可选择其他集群节点，重复上述配置步骤，单击应用。

如需验证配置的其他信息，请参阅第 546 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。请参阅[Active/Active DPI 集群高可用性](#)。

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：

i 注：如果您已按照第 517 页的 [物理连接安全设备](#) 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 转至管理 | 系统设置 | 高可用性 | 基本设置。



- 3 从模式中，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安全设备时，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安全设备时，就会在这些安全设备上创建备份。
- 6 单击 **HA 设备** 以配置 Active/Active 集群信息。
- 7 对于选项卡顶部的 **HA 备用设备** 选项，
 - 如果所配置的次要安全设备是该安全设备所属集群节点的一部分，请选择**内部**。
 - 如果所配置的次要安全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安全设备的序列号。

i | 提示：主要设备的序列号可能会填充并变暗。
- 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。如需从一个集群中排除一个防火墙，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。如果安全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。如果安全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**接受**。所有设置将同步到备用设备，备用设备将重启。
- 16 转到**管理 | 系统设置 | 高可用性 | 监控设置**并按照第 541 页的**配置 Active/Active 集群高可用性监控**中的步骤进行操作。
- 17 转到**管理 | 系统设置 | 高可用性 | 高级设置**并按照第 556 页的**微调高可用性**中的步骤进行操作。
- 18 转到**管理 | 系统设置 | 网络 | 接口**，验证您已成功配置所需的 Active/Active 接口。
- 19 转到**监控 | 当前状态 | 高可用性状态**以验证 Active/Active 集群设置。如需有关高可用性状态的信息，请参阅 SonicOS 监控。

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 546 页的[配置 Active/Active 集群的 VPN](#)
- 第 546 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。可以在[管理 | 连接 | VPN | 基本设置](#)上配置创建此关联的选项。如需有关配置 VPN 策略的信息，请参阅 SonicOS 连接。

虚拟群组地址对象可用于本地网络。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，自定义名称 **Active-Active-Lan-Host-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。可以在创建自定义 NAT 策略时指定虚拟群组，例如，为接口 X1 上的虚拟群组 2 自动创建的 NAT 策略。如需创建 NAT 策略的信息，请参阅 SonicOS 策略。

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。请参阅以下章节：

- 第 546 页的[比较集群中的防火墙的 CPU 活动](#)
- 第 547 页的[在监控 | 当前状态 | 高可用性状态中验证设置](#)
- 第 547 页的[TSR 中的其他参数](#)
- 第 547 页的[对 DPI 匹配的响应](#)
- 第 547 页的[日志](#)

比较集群中的防火墙的 CPU 活动

状态监控 HA 对启用 Active/Active DPI 后，可以观察到 HA 对中的安全设备的 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。在主节点的活动安全设备上，转至[监控 | 设备健康 | 实时监控](#)，滚动至“多核监控”以显示 Active/Active 集群中所有安全设备的活动。如需多核监控的信息，请参阅 SonicOS 监控。

在“多核监控”上查看集群中的活动设备时，集群中的所有安全设备都会显示。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 对中两个安全设备的核心使用情况。

i 注：如需查看集群中所有安全设备的核心使用情况，SonicWall 建议在主节点的活动设备上查看“多核监控”。

在监控 | 当前状态 | 高可用性状态中验证设置

在 **Active/Active** 集群节点状态表中，**监控 | 当前状态 | 高可用性状态** 提供部署中整个 **Active/Active** 集群的状态和各集群节点的状态。如需有关查看 HA 状态的信息，请参阅 **SonicOS 监控**。

TSR 中的其他参数

可以在 **调查 | 工具 | 系统诊断** 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”中应出现这些配置参数并显示正确的值：

- 启用 **Active/Active DPI**
- **Active/Active DPI** 接口配置

如需有关生成 TSR 的信息，请参阅 **SonicOS 调查**。

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 **调查 | 工具 | 系统诊断**。
- 3 在 **技术支持报告** 下，单击 **下载报告**。

对 DPI 匹配的反应

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。

i | **注：** 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** 会话承载一个病毒附件时，**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** 数据包是备用安全设备上的 **DPI** 处理的结果。所产生的数据包通过 **Active/Active DPI** 接口发送至活动安全设备，并从活动安全设备发出，好像处理是发生在活动安全设备上。这可确保无缝操作，似乎 **DPI** 处理是在活动安全设备上完成。

日志

如果启用了 **Active/Active DPI**，且备用安全设备上的 **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 **调查 | 工具 | 日志 | 事件日志** 上查看。如需有关日志的信息，请参阅 **SonicOS 调查**。

IPv6 高可用性监控

如需 **SonicOS** 的 **IPv6** 实施的完整信息，请参阅第 **762** 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安全设备，且 IPv6 探测可以检测 HA 对的网络状态。

为了便于配置两个 IP 版本，可以在[管理 | 系统设置 | 高可用性 | 监控设置](#)上的 IPv6 和 IPv4 显示之间进行切换。

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 并参考第 509 页的[关于高可用性](#)和第 548 页的[IPv6 HA 监控考虑因素](#)了解配置细节。

IPv6 HA 监控考虑因素

在配置 IPv6 HA 监控时请考虑以下因素：

- 在编辑 HA 监控设置对话框中，启用物理/链接监控和覆盖虚拟 MAC 显示为灰色不可用，因为它们都是二层属性。也就是说，IPv4 和 IPv6 使用这些属性，所以必须在 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/备用安全设备的全局 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。
- 如果启用了允许主要/备用 IPv6 地址的管理，则主要/备用监控 IPv6 地址不能为未指定（即 ::）。
- 如果启用了逻辑/探测 IPv6 地址，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[管理 | 系统设置 | 网络 | 接口](#)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，请参阅：

- 第 548 页的[禁用 SonicOS DHCP 服务器](#)
- 第 549 页的[配置虚拟 IP 地址](#)
- 第 549 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[管理 | 系统设置 | 网络 | DHCP 服务器](#)。
- 2 选择 IP 版本：IPv4 或 IPv6。
- 3 清除启用 DHCPv4/6 服务器。
- 4 在 DHCPv4/6 服务器租用范围下，为视图类型选择全部以选择表中的所有租用范围。
- 5 单击全部删除按钮。
- 6 单击确认对话框中的确定。
- 7 单击接受。

配置虚拟 IP 地址

首次启用 Active/Active 集群时，该安全设备上的接口的已配置 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，如果其接口未配置相应的虚拟 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 **管理 | 系统设置 | 网络 | 接口**。
- 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** 对话框中，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物理链路故障时，无需进行设备故障切换。

可以在 **管理 | 系统设置 | 网络 | 接口 > 编辑接口 > 高级** 对话框上配置冗余端口。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 **管理 | 系统设置 | 网络 | 接口**。
- 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。将显示 **编辑接口** 对话框。
- 4 单击 **高级**。
- 5 从 **冗余/聚合端口**中，选择 **端口冗余**。对话框的选项将改变。
- 6 从 **冗余端口**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，并列出主要接口。接口还会出现在主要端口的 **编辑接口** 对话框中的 **冗余端口** 字段中。

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 550 页的 [Active/Active 集群全网格概述](#)
- 第 552 页的 [配置 Active/Active 集群全网格](#)
- 第 555 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。全网格确保部署中无单点故障，无论是设备（安全设备/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：安全设备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 550 页的 [关于全网格部署](#)
- 第 550 页的 [Active/Active 集群全网格的优点](#)
- 第 551 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，不仅是安全设备，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、安全设备同时发生故障，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，**管理 | 系统设置 | 网络 | 接口 > 编辑接口**对话框中的冗余端口字段变为可用。

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。

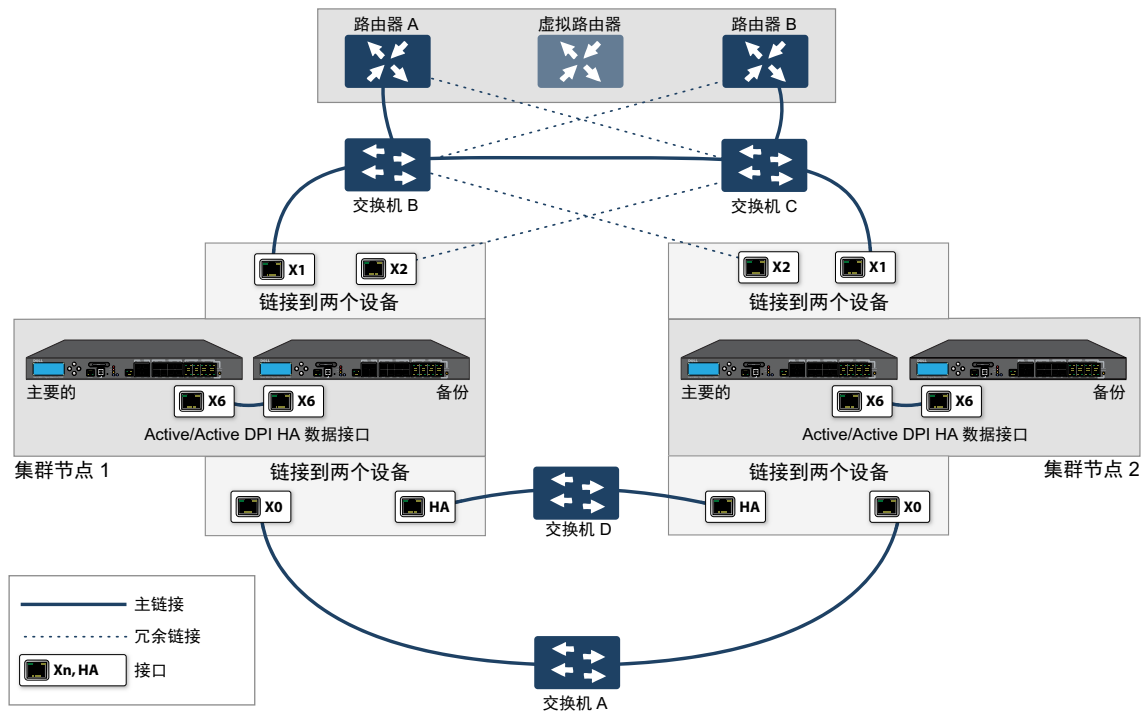
所有集群节点均正常工作并处理流量时，冗余端口保持待命，一旦伙伴端口因为任何原因停止工作便可使用。如果一个集群节点停止工作，引起 Active/Active 故障切换，剩余集群节点中的冗余端口就会立即投入使用，处理故障节点拥有的虚拟群组的流量。这就是负载分担。

例如，部署中虚拟群组 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 建议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。

WAN 侧冗余所示的部署包括 WAN 侧的冗余路由器、交换机和端口，但并非全网络部署，因为 LAN 侧未使用冗余。

WAN 侧冗余



部署冗余端口或交换机时不需要全网络，但全网络部署包括它们。全网络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。

如需全网络部署的更多信息，请参阅“Active/Active 集群全网络部署技术说明”。

配置 Active/Active 集群全网格

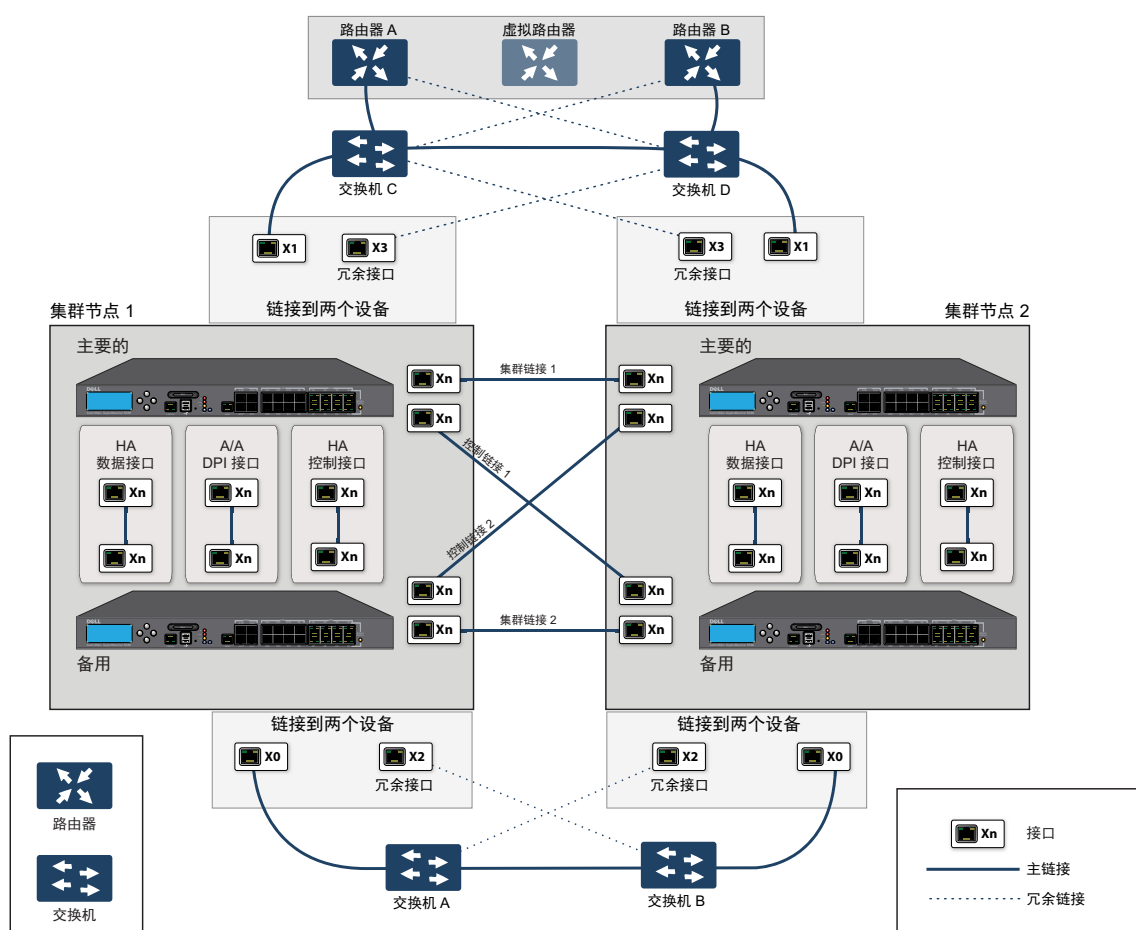
本节介绍 4 设备 Active/Active 集群全网格部署的设置程序（请参阅 [Active/Active 四设备集群全网格](#)）：

- 第 552 页的 [Active/Active 全网格的布线](#)
- 第 554 页的 [配置 Active/Active 群集安全设备](#)
- 第 555 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

Active/Active 四设备集群全网格



Active/Active 全网格的布线

以下程序说明 [Active/Active 四设备集群全网格](#) 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 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 如果路由器无冗余端口支持，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 而非端口。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 [Active/Active 四设备集群全网格](#) 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安全设备。实施如下布线（为简明起见，[Active/Active 四设备集群全网格](#) 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 群集安全设备

主题：

- 第 554 页的[配置程序](#)
- 第 554 页的[单点故障测试](#)

配置程序

配置 Active/Active 群集安全设备的步骤如下：

- 1 关闭除 CN1-主要设备以外的所有其他防火墙。
- 2 在管理|系统设置 | 高可用性 | 基本设置页面：
 - a 从模式中选择 **Active/Active** 集群。
 - b 选择启用状态同步。
 - c 单击 **HA** 设备和节点。
 - 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 级别中选择所有者，从虚拟群组 2 级别中选择备用。
 - f 对于 CN2，从虚拟群组 1 级别中选择所有者，从虚拟群组 2 级别中选择备用。
 - g 启用 Active/Active DPI，X6 和 X7 用作两个 HA 数据端口。
 - h 单击应用。
- 3 在管理|系统设置网络 | 接口网络 | 接口上：
 - 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 在管理|系统设置 | 高可用性 | 监控设置上，在集群中各设备的 X0 和 X1 上添加监控/管理 IP 地址。
- 5 开启所有其他安全设备。CN1-主要设备的配置完全同步到所有其他安全设备。
- 6 使用专用监控/管理地址登录各安全设备并执行以下操作：
 - a 在 MySonicWall 上注册安全设备。
 - 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。您可以利用不同方法实现这一设置：

- 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。
- 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。

在所有设备和链路上进行单点故障测试的步骤如下：

- 1 设备故障：在这些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：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：在这些各种链路故障情况下，流量应继续流动：
 - a 在集群节点各活动安全设备上，断开 X0 电缆，X2 保持连接。
 - b 在集群节点各活动安全设备上，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

您可以采用两台安全设备部署 Active/Active 集群全网格，其中各集群节点仅包含一个安全设备（无 HA 备用）。不过，这种设置有如下局限：

- 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安全设备容量的 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）。

微调高可用性

- 第 556 页的高可用性 | 高级设置
 - 第 556 页的配置高级高可用性

高可用性 | 高级设置

心跳间隔 (毫秒):	<input type="text" value="1000"/>
故障切换触发级别 (丢失的心跳数):	<input type="text" value="5"/>
探测间隔 (秒):	<input type="text" value="20"/>
探测计数:	<input type="text" value="3"/>
选择延迟时间 (秒):	<input type="text" value="3"/>
动态路由保持时间 (秒):	<input type="text" value="45"/>
<input type="checkbox"/> 仅当所有的聚合链接断开时进行活动/备用故障切换	
<input type="button" value="同步设置"/>	<input checked="" type="checkbox"/> 包含证书/密钥
<input type="button" value="同步固件"/>	
<input type="button" value="强制活动/备用故障切换"/>	

管理 | 系统设置 | 高可用性 | 高级设置能微调高可用性配置，以及同步高可用性安全设备间的设置和固件。Active/Standby 和 Active/Active 配置的高可用性 | 高级设置完全相同。

心跳间隔和故障切换触发级别（丢失的心跳数）设置同时适用于 SVRRP 心跳（Active/Active 集群心跳）和 HA 心跳。高可用性 | 高级设置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 509 页的关于高可用性和第 516 页的 Active/Standby 和 Active/Active DPI 前提条件。

配置高级高可用性

配置高级设置的步骤如下：

- 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 转至管理 | 系统设置 | 高可用性 | 高级设置。

心跳间隔 (毫秒):	<input type="text" value="1000"/>
故障切换触发级别 (丢失的心跳数):	<input type="text" value="5"/>
探测间隔 (秒):	<input type="text" value="20"/>
探测计数:	<input type="text" value="3"/>
选择延迟时间 (秒):	<input type="text" value="3"/>
动态路由保持时间 (秒):	<input type="text" value="45"/>
<input type="checkbox"/> 仅当所有的聚合链接断开时进行活动/备用故障切换	
<input type="button" value="同步设置"/>	<input checked="" type="checkbox"/> 包含证书/密钥
<input type="button" value="同步固件"/>	
<input type="button" value="强制活动/备用故障切换"/>	

- 3 可调整心跳间隔以控制 Active/Active 集群中的安全设备多长时间通信一次。该设置适用于 Active/Active 集群中的所有设备。默认值为 **1,000** 毫秒 (1 秒)，最小值为 1,000 毫秒，最大值 300000。

i | 注：SonicWall 推荐将心跳间隔设置为至少 1000。

如果您的部署要处理大量网络流量，可以使用较高的值。较低的值有可能导致不必要的故障切换，尤其是当安全设备处于较大负载的情况下。

此计时器连接到故障切换触发级别（丢失的心跳数）计时器。

- 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。该设置适用于 Active/Active 集群中的所有设备。默认值为 **5**，最小值为 4，最大值为 99。

此计时器连接到心跳间隔计时器。如果故障切换触发级别设置为 5，心跳间隔设置为 10000 毫秒 (10 秒)，则 50 秒钟无心跳后将触发故障切换。

- 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)。此间隔用于本地 HA 对的逻辑监控。默认值是 **20** 秒，容许范围是 5 到 255 秒。

i | 提示：SonicWall 建议将该间隔至少设置为 5 秒。

可以在管理 | 系统设置 | 高可用性 | 高级设置设置探测 IP 地址。请参阅第 559 页的[高可用性 | 监控设置](#)。

- 6 设置探测计数，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。此计数用于本地 HA 对的逻辑监控。默认值是 **3**，容许范围是 3 到 10。

- 7 将选择延迟时间设置为主要安全设备等判断一个接口激活和稳定的秒数。默认值为 **3** 秒，最小值为 3 秒，最大值为 255 秒。

i | 提示：此计时器对于拥有生成树延迟设置的交换机端口非常有用。

- 8 设置动态路由保持时间，即新激活的安全设备将之前获取的动态路由保持在其路由表中的秒数。默认值为 **45** 秒，最小值为 0 秒，最大值为 1200 秒 (20 分钟)。

i | 注：仅当管理 | 系统设置 | 网络 | 路由上选择了高级路由选项时，动态路由保持时间设置才会显示。

i | **提示：** 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

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。

- 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断开时进行活动 / 备用故障切换**。
- 10 选中**包含证书/密钥**，使设备同步 HA 对内的所有证书和密钥。
- 11 （可选）如需同步主要和次要 HA 防火墙之间的 SonicOS 首选项设置，请单击**同步设置**。
- 12 （可选）如需同步主要和次要 HA 防火墙之间的固件版本，请单击**同步固件**。
- 13 （可选）如需通过尝试活动/备用 HA 故障切换到次要安全设备来测试 HA 故障切换功能，请单击**强制活动/备用故障切换**。
- 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次要安全设备或其他设备。

监控高可用性

- 第 559 页的高可用性 | 监控设置
 - 第 560 页的配置 Active/Standby 高可用性监控

高可用性 | 监控设置

监控设置							
视图 IP 类型: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6							
名称	主要 IP 地址	次要 IP 地址	探测 IP 地址	物理/链接...	逻辑/探测...	管理	配置
X0	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X4	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V63	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V66	0.0.0.0	0.0.0.0	0.0.0.0				
X7	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X10	0.0.0.0	0.0.0.0	0.0.0.0				
X11	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				
X16	0.0.0.0	0.0.0.0	0.0.0.0				
X17	0.0.0.0	0.0.0.0	0.0.0.0				

在管理|系统设置 | 高可用性 | 监控设置上，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，请参阅第 508 页的关于高可用性和 Active/Active 集群。

配置 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 安全设备上以管理员身份登录到 SonicOS 管理界面。
- 2 转至管理 | 系统设置 | 高可用性 | 监控设置。

监控设置							
视图 IP 类型: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6							
名称	主要 IP 地址	次要 IP 地址	探测 IP 地址	物理/链接...	逻辑/探测...	管理	配置
X0	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X4	0.0.0.0	0.0.0.0	0.0.0.0	✓			
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V63	0.0.0.0	0.0.0.0	0.0.0.0				
X5:V66	0.0.0.0	0.0.0.0	0.0.0.0				
X7	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X10	0.0.0.0	0.0.0.0	0.0.0.0				
X11	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				
X16	0.0.0.0	0.0.0.0	0.0.0.0				
X17	0.0.0.0	0.0.0.0	0.0.0.0				

- 3 单击 LAN 上某个接口的配置图标，例如 X0。将显示编辑 HA 监控对话框。

接口 X0 监控设置	
<input checked="" type="checkbox"/> 启用物理/链接监控	
主要 IPv4 地址:	<input type="text" value="0.0.0.0"/>
次要 IPv4 地址:	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> 允许主要/次要 IPv4 地址的管理	
<input type="checkbox"/> 逻辑/探测 IPv4 地址:	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> 覆盖虚拟 MAC:	<input type="text" value="c2:ea:e4:59:8e:24"/>

- 4 如需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。默认情况下已选中该选项。
- 5 在主要 IPv4 地址字段，输入主要设备的唯一 LAN 管理 IP 地址。默认值为 0.0.0.0。

- 6 在**次要 IPv4 地址**字段，输入次要设备的唯一 LAN 管理 IP 地址。默认值为 **0.0.0.0**。
- 7 选中**允许从主要/次要 IP 地址的管理**。启用某一接口的这个选项时，在**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。默认情况下未选中该选项。
- 8 在**逻辑/探测 IPv4 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。）默认情况下未选中该选项。

主要和次要安全设备将定期 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，而非安全设备。但是，如果一个安全设备能 ping 通目标，另一个不能，HA 对将故障切换到能 ping 通目标的安全设备。

主要 IPv4/v6 地址和**次要 IPv4/v6 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。默认情况下未选中该选项。

ⓘ | 重要：应谨慎选择虚拟 MAC 地址，防止配置错误。

当**管理 | 系统设置 | 高可用性 | 高级设置**上的**启用虚拟 MAC**选中时，SonicOS 固件自动生成所有接口的虚拟 MAC 地址。使 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 如需配置任何其他接口的监控，请对每个接口重复**步骤 3**到**步骤 10**。
- 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次要设备。

WAN 加速

- 使用 WAN 加速

使用 WAN 加速

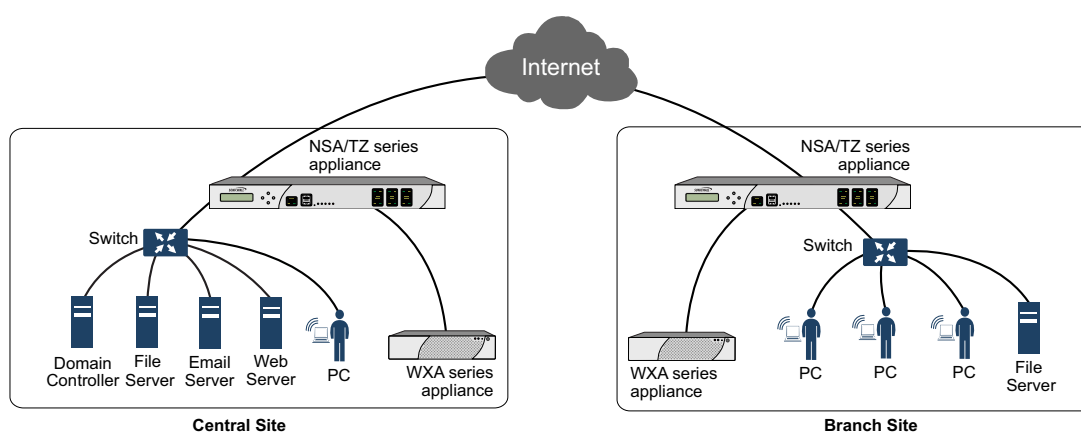
- [第 563 页的关于 WAN 加速](#)
 - [第 564 页的支持的平台](#)
 - [第 564 页的传输控制协议加速](#)
 - [第 564 页的 Windows 文件共享加速](#)
 - [第 565 页的 Web 缓存](#)
 - [第 565 页的部署 WAN 加速服务的前提条件](#)
 - [第 566 页的关于 WXA 集群](#)
 - [第 567 页的 WXA 集群的工作原理是什么？](#)
 - [第 568 页的允许对路由策略加速](#)
- [第 569 页的系统设置 > WAN 加速](#)
 - [第 569 页的启用 WAN 加速](#)
 - [第 570 页的管理群组](#)
 - [第 574 页的通过 WXA 表来管理 WXA](#)
 - [第 589 页的配置 VPN 策略的 WXA](#)
 - [第 590 页的配置 SSL VPN 流量加速](#)

关于 WAN 加速

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。SonicWall WXA 系列设备与 SonicWall NSA 系列设备一起部署。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 NSA 系列设备性能。

[SonicWall WXA 系列设备拓扑](#)显示 SonicWall WXA 系列设备和 SonicWall 安全设备的基本网络拓扑。

SonicWall WXA 系列设备拓扑



主题:

- 第 564 页的 [支持的平台](#)
- 第 564 页的 [传输控制协议加速](#)
- 第 564 页的 [Windows 文件共享加速](#)
- 第 565 页的 [Web 缓存](#)

支持的平台

在这些平台上，SonicOS 6.2 及更高版本可以使用 WAN 加速:

- SuperMassive 9200、9400 和 9600
- TZ600、TZ500/500W、TZ400/400W、TZ300/300W
- NSA 6600/5600/4600/3600/2650/2600

WXA 集群目前只适用于 NSA 和 SuperMassive 系列安全设备。

传输控制协议加速

TCP 加速服务是通过使用压缩方式减少流经 WAN 的数据量的过程。这将加速中央站点与分支站点之间传输的选定流量。选定的流量在 SonicWallWXA 系列设备的共享数据库中存储为数据块，并使用参考索引进行标记。这允许 WXA 系列设备仅通过 WAN 发送较小的参考索引，而非发送实际数据。

Windows 文件共享加速

WAN 加速是指用于加速应用程序、增加吞吐量，减少延迟的多种技术。Windows 文件共享 (WFS) 加速是 WAN 共享的子集。

在您的网络中使用 WFS 加速可通过执行近似流的行为减少高延迟和低带宽链接的影响，并且使用预读和后写功能以及差别性文件传输，避免了重复传输未更改的文件部分。WFS 加速允许分支用户通过 WAN 以接近 LAN 的速度访问和共享共同使用的文件。

部署 WFS 加速解决方案的分布式企业可能将存储合并到企业中央站点中，无需备份和管理之前分支站点上存在的数据。

在没有合并存储的情况下，从其他站点访问本地和分支存储数据的成本和延迟也会下降。

WXA 系列设备可针对以下流量提供 WFS 加速：

- 未签名 SMB 流量 - 在支持未签名 SMB 流量的网络中，配置 WFS 加速将会大幅简化，因为未签名 SMB 流量没有安全层。因此，WXA 系列设备无需加入域就能拦截流量，因而无需配置自定义 DNS 区域、反向查找和文件共享。
- 已签名 SMB 流量 - 在要求 SMB 签名的网络中，WXA 系列设备必须加入某个域，因为签名 SMB 流量有安全层。签名 SMB 配置比未签名 SMB 配置更加复杂，但能提供更精确的配置。签名 SMB 配置还提供了包含更多选项的高级配置模式。

对签名 SMB 的扩展支持

对签名 SMB 流量的扩展支持是由单个 WXA 处理的，且与在 WXA 集群中别处使用的群组设置单独配置。通过在 Windows 域中配置，用户能够充分受益于支持签名 SMB 的网络中 WFS 加速模块的附加功能。将 WXA 系列设备加入域后，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。

重要：强烈建议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。

Web 缓存

“Web 缓存”功能存储了频繁请求以及最近请求通过网络的网页和 Youtube 视频的副本。当用户请求其中一个网页时，就会从本地 Web 缓存检索，而不是从因特网，从而节省带宽和响应时间。提供最低、中等和主动缓存策略。这些策略可确定哪些对象将处于 Web 缓存中以及存在多长时间。

部署 WAN 加速服务的前提条件

部署 SonicWall WXA 系列设备需要 SonicWall 安全设备。

通过 SonicWall WXA 系列设备的流量需要 Internet 协议版本 4 (IPv4)。WAN 加速服务与 IPv6 不兼容。

部署注意事项

部署 SonicWall WXA 系列设备时请考虑以下事项：

- NSA 和 SuperMassive 系列安全设备支持 WXA 集群，可以将多个 WXA 连接到安全设备。
- 对于 WXA 集群，WXA 系列设备支持配合 SonicWall NSA 2600 或更高版本以及运行 SonicOS 6.2.2 或更高版本固件的 SuperMassive 系列安全设备使用。
- 通过使用插入的光盘启动 PC，可以在内存模式下运行 WXA 500。或者，也可以将其安装到硬盘上。在后一种情形下，可使用更多功能。
- 通常，WXA 系列设备是通过各自的 SonicWall 安全设备部署在站点到站点 VPN 配置。但是，也可以使用路由或 L2 桥接模式。
- 如果在高可用性配置中使用 WXA 系列设备，将需要连接到两个高可用性对的交换连接。

- WXA 系列设备的初始配置应使用 WXA 设置向导执行，通过单击 SonicWall 安全设备管理界面中的快速配置即可使用该向导。如需有关 WXA 设置向导的更多信息，请参阅 SonicOS 快速配置。
- 加密的流量有高度随机性，不会通过 WXA 系列设备的 WAN 加速服务获得实际受益。因此，不会加速 SSL 和 TLS 流量类型。
- 使用签名 SMB 的 WFS 加速支持 Windows 文件服务，并使用 Active Directory、Kerberos 和 NTLM 进行身份验证和授权。
- 使用已签名 SMB 和 NTLM 客户端的 WFS 加速提供在域中有效的 SonicWallWXA 系列设备凭据。SonicWall WXA 系列设备通过域控制器获取 Kerberos 凭据。这将使那些客户代表使用的未加入域的客户端设备拥有有效域凭据。
- 在物理连接 WXA 系列设备之前，在管理 SonicWall 安全设备上创建 DHCP 范围。
- 如果分支办公室有域控制器和 DNS 服务器，则推荐您使用 DHCP 范围中的这些 DNS 服务器地址和域 DNS 名称。在配置的 DHCP 范围中配置仅有的域名和域 DNS 服务器 IP 地址。WXA 系列设备将根据此类型的信息自动发现 Kerberos、LDAP 和 NTP 服务器，帮助设备加入域。
- 查看 LDAP、Kerberos 和 NTP 服务。在未明确配置站点和服务的多站点域中，WXA 系列设备可能不会选择最近的服务器。
- SonicWall 推荐 WXA 系列设备从域控制器检索 NTP 更新。如果 NTP 服务器未配置，则将自动进行配置。
- SonicWall 建议将保留了 WXA 名称或 IP 地址的活动目录 DNS 区域配置为仅接受安全更新。
- 给作为 LAN 区域连接的 WXA 系列设备配置接口区域属性。

关于 WXA 集群

 注：NSA 2600 及更新设备支持 WXA 集群。

SonicOS 支持两个或多个 NSA 系列设备或 SuperMassive 设备的 WXA 集群。最大型的 SonicWall WXA 系列设备支持最多 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 系列设备并为每个 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 系列设备之间平均分配。
- 当其中一个 WXA 达到连接能力后，使用群组中的下一个 WXA。

主题：

- [第 567 页的集群的支持平台](#)
- [第 567 页的什么是 WXA 集群？](#)
- [第 567 页的 WXA 集群的工作原理是什么？](#)

集群的支持平台

支持 WXA 集群的固件：

- WXA 固件版本 1.3.2 及以上。
- 在这些 SonicWall 安全设备：

SM 9600	NSA 6600
SM 9400	NSA 5600
SM 9200	NSA 4600
	NSA 2600
	NSA 3600

什么是 WXA 集群？

WXA 集群是指两个或更多的 WXA 系列设备配合使用以提高吞吐量和适应性。

优点

集群 WXA 系列设备能够大幅增加可以同时访问的连接数量。只要增加更多的 WXA 设备，您即可使该容量成倍增加。[WXA 型号的最大用户数和连接数](#)表列出每个 WXA 平台可用的最大用户和连接数量。

WXA 型号的最大用户数和连接数

	WXA 系列设备				
	WXA 6000	WXA 4000	WXA 2000	WXA 5000	WXA 500 Live
平台	软件	硬件			
设备	硬件				
设备	虚拟				
设备	软件				
最大用户数	2000	240	120	360	20
最大					
连接数	10,000	1,200	600	1,800	100

集群 WXA 设备有以下优势：

- 为用户和 WAN 基础结构的加速解决方案提高可扩展性
- 是可以通过扩展来满足企业和应用要求的弹性解决方案
- 是可以将一个或多个 WXA 专门用于特定任何或网段的灵活解决方案
- 是用于 WAN 加速设备的弹性基础结构

WXA 集群的工作原理是什么？

WXA 集群通过将多个 WXA 系列设备连接在一起并使用负载均衡和连接均衡增加可以同时连接的数量来实现。没有必要在远程和本地位置都实施 WXA 集群，但每个位置必须至少有一个 WXA。

当连接多个 WXA 并且配合使用时，可以通过 WAN 加速的数据量会显著增加。

在 WXA 集群配置中，WXA 是群组成员，可以有多个群组。每个群组中的 WXA 有相同的配置，但不同的 WXA 群组可以有不同的配置。

WXA 配置从 SonicWall 安全设备上的 SonicOS 推送。

主题：

- [第 568 页的限制](#)
- [第 568 页的 WXA 集群的许可证](#)

限制

WXA 集群不支持已签名 SMB 的 WFS 加速。如果使用专门用于加速已签名 SMB 单个 WXA 设备，则支持已签名 SMB 的 WFS 加速。该 WXA 可以属于或不属于某个群组。但是，如果它一直不属于集群群组，则只能用于加速已签名 SMB 流量。

WXA 集群的许可证

WXA 集群的许可证取决于您希望支持的同时加速连接的最大数量。客户可以为将要加速的特定数量的连接购买 WXA 集群许可证。

在 WXA 500、WXA 5000 和 WXA 6000 上，将根据所需的连接数量购买 WXA 集群许可证。每个许可证代表允许的最大连接数量。仅许可的最大连接数量会得到加速。如果通过 SonicWall 安全设备的连接数量超过最大数量，超出的连接仍会建立，但不会得到加速。

在 WXA 2000 和 WXA 4000 上，无需额外的许可证。对于这些型号，设备内置的最大连接数量也是将要加速的最大连接数量。

如果将 WXA 2000 或 WXA 4000 添加到包含 WXA 500、WXA 5000 或 WXA 6000 的集群中，连接数量则会相应增加。例如，将 WXA 2000 添加到集群会为允许的限额增加 600 个同时连接。

可以将任意数量的虚拟 WXA 500s、WXA 5000s 和 WXA 6000s 添加到 SonicWall 安全设备，但加速的连接数量取决于已经购买的许可证。

如果超过允许的加速连接数量，所有超出的连接会绕过集群，无论该集群中有多少 WXA。管理员负责确保将足够数量的 WXA 连接到安全设备以处理他们希望支持的许可连接数量。

允许对路由策略加速

配置 WXA 后，您可以允许对路由策略加速。您可以在 [系统设置 | WAN 加速](#) 页面或 [网络 | 路由](#) 页面上允许对路由策略加速（请参阅第 [372](#) 页的 [配置路由通告和路由策略](#)）。

如果您的网络上未配置 VPN，并且您使用了自定义路由策略，则需要每个站点上添加两个路由策略：一个用于传出流量，一个用于传入流量。

系统设置 > WAN 加速



主题：

- 第 569 页的 [启用 WAN 加速](#)
- 第 570 页的 [管理群组](#)
- 第 574 页的 [通过 WXA 表来管理 WXA](#)
- 第 589 页的 [配置 VPN 策略的 WXA](#)
- 第 590 页的 [配置 SSL VPN 流量加速](#)

启用 WAN 加速

启用 WAN 加速的步骤如下：

- 1 转至系统设置 > WAN 加速。



- 2 在 WAN 加速部分中，选择启用 WAN 加速。
- 3 通过单击接口编辑图标选择连接 WXA 的接口。显示 WXA 的接口弹出窗口。

WXA 的接口

接口: X2

区域: LAN

IP 地址: 192.168.94.83

子网掩码: 255.255.255.0

保持已有的接口配置

- 4 从接口中选择 WXA 连接的接口。
- 5 从区域中选择该接口的区域。
- 6 在 IP 地址字段，输入所选接口的 IP 地址。
 ⓘ | **重要：** 用来为 WXA 分配地址的 DHCP 范围由接口的 IP 地址和网络掩码确定。
- 7 在网络掩码字段中，输入所选接口的网络掩码。
- 8 单击确定。

管理群组

群组											
<input type="button" value="+"/> <input type="button" value="x"/> <input type="button" value="设置为默认"/> <input type="button" value="取消默认设置"/>											
<input type="checkbox"/> 名称	TCP 加速	WFS 加速	Web 缓存	WXA	VPNs	SSL VPN	路由	连接	默认	配置	监控
<input type="checkbox"/> Group One	启用	启用	启用; 策略 = 中等	1/1	0		0	0	●	<input type="button" value="⚙️"/> <input type="button" value="x"/>	<input type="button" value="监控"/>

此列	表明或显示
名称	群组的名称
TCP 加速	TCP 加速是否为已启用或已禁用。
WFS 加速	WFS 加速是否为已启用或已禁用。
Web 缓存	<ul style="list-style-type: none"> • Web 缓存是否为已启用或已禁用。 • 缓存策略：最小、中等或主动。
WXA	找到的可用 WXA（在线和集群就绪）数量和为该群组配置的数量：已找到/已配置。
VPN	其加速由群组管控的 VPN 的数量。
SSL VPN	其加速由群组管控的 SSL VPN 的数量。
路由	其加速由群组管控的路由的数量。
连接	群组中当前通过 WXA 的连接数。如果将鼠标悬停在数字上，弹出窗口显示以下内容： <ul style="list-style-type: none"> • 群组中每个 WXA 模型的受支持连接的总数。 • 可以加速的并发连接的总许可数。
默认	用于表明默认组的绿色图标。
配置	群组的编辑和删除图标。
监控	用于显示 WXA 连接监视器的监控按钮。

主题：

- 第 571 页的[添加群组](#)
- 第 573 页的[设置默认群组](#)
- 第 573 页的[编辑群组](#)
- 第 573 页的[删除群组](#)

添加群组

添加群组的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组部分中，单击添加图标。显示新建群组对话框。



群组详细信息 TCP 加速 WFS 加速 Web 缓存

名称： 群组名称

用作默认群组

- 3 在名称字段中输入有意义的群组名称。
- 4 如需指定群组为默认组，请选择用作默认群组。默认情况下未选中该选项。
- 5 如果：
 - 不使用 TCP 加速，请转到[步骤 10](#)。
 - 使用 TCP 加速，请单击 TCP 加速。



群组详细信息 TCP 加速 WFS 加速 Web 缓存

启用 TCP 加速

TCP 加速模式： 除了被默认排除之外的所有 TC

服务对象： AD Directory Services

始终排除的地址对象： 无

- 6 单击启用 TCP 加速。
- 7 从 TCP 加速模式中选择模式：
 - 除了被默认排除之外的所有 TCP 服务（此为默认值，“服务对象”下拉菜单为灰显状态），转至[步骤 9](#)
 - 除了那些在 TCP 加速服务对象之外的所有 TCP 服务
 - 除了那些在 TCP 加速服务对象和被默认排除之外的所有 TCP 服务
 - 仅在 TCP 加速服务对象指定的 TCP 服务（仅为“服务对象”启用 TCP 加速）

① 提示：如需查看排除的 TCP 服务，请将鼠标悬停在 TCP 加速模式上以显示列出排除的服务的弹出窗口。
- 8 从服务对象中，选择要排除或包含的服务对象。

- 9 如需从 TCP 加速中排除地址对象，请从始终排除的地址对象中选择地址对象，默认值是无。
- 10 如果：
- 不使用 WFS 加速，请转到步骤 12。
 - 使用 WFS 加速，请单击 **WFS 加速**。



11 选择启用 **WFS 加速**。

- 12 如果：
- 不使用 Web 缓存，请转到步骤 19。
 - 使用 Web 缓存，单击 **Web 缓存**。



13 选择启用 **Web 缓存**。

- 14 从 **Web 服务器端口**中，选择代表 Web 服务器端口的服务对象，流量会在此端口上被拦截并发送到 WXA Web 缓存。默认为 **HTTP**。
- 15 从**客户端包含地址对象**中，选择代表本地子网的地址对象或群组，这些子网的 Web 流量应该通过 WXA Web 缓存转移。默认值为 **LAN 子网**。
- 16 从**服务器排除地址对象**中，选择包含 Web 服务器目标地址的地址对象或群组，这些服务器的流量不应通过 WXA Web 缓存转移。默认值为**无**：表示不排除任何 **Web 服务器**，并将通过 WXA 发送所有合适的流量。
- 17 从**缓存策略**中，选择缓存策略，该策略用于确定缓存的对象的字节数以及指示对象留在缓存中的时长的属性：

- | | |
|----|--|
| 最小 | 提供了基本的缓存功能，Web 缓存将缓存对象，除非 HTTP 标头特别指名不缓存（例如无缓存或过去发生的过期时间）。 |
| 中等 | 严格程度稍微降低，在缓存中存储的时间较长。这是默认值。 |
| 主动 | 忽略标头选项，例如无存储和重新加载，并覆盖过期时间。 |

小心：此策略应慎重使用，因为它违反了 HTTP 标准，可能会导致不想要的结果。

i | **注：**中等和主动模式都包括缓存 YouTube 视频。

18 也可以在**管理员电子邮件**字段中输入管理员电子邮件地址。

19 单击**确定**。

设置默认群组

通常情况下，配置组时会指定默认群组（请参阅第 571 页的[添加群组](#)），但可以随时更改默认群组。

更改默认群组的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表中，取消选择默认群组。
- 3 选择要设为默认值的群组。设置为默认按钮变为可用。
- 4 单击设置为默认。将显示确认消息。

是否确定要使该群组为: Group One 默认群组？
所有新发现的 WXA 将自动分配给此群组。

- 5 单击是。绿色指示器现在显示在默认群组的默认列中。

编辑群组

编辑群组的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表中，单击要编辑的组的编辑图标。将显示编辑群组对话框。



群组详细信息 TCP 加速 WFS 加速 Web 缓存

名称： Group One

用作默认群组

- 3 依照第 571 页的[添加群组](#)中的步骤 3 到步骤 19。

删除群组

可以删除一个或多个群组。不能删除有关联的 WXA 的群组或者用来控制一个或多个 VPN、SSL VPN 或路由。

删除群组的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表中，选择要删除的群组。
- 3 单击群组的删除图标。将显示确认消息。

是否确定要从配置中删除群组:Group Two？

- 4 单击是。


删除多个文件的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表中，选择要删除的群组。表格上方的“删除”图标变为可用。
- 3 单击删除图标。将显示确认消息。

您即将删除所选的群组。
注：不能删除有关联的 WXA 的群组或者用来控制一个或多个 VPN、SSLVPN 或路由中的加速的群组。
是否确定要继续？

- 4 单击是。

通过 WXA 表来管理 WXA



ID	名称	组	IP	模块	固件	Op.Status	组件	连接	配置	管理	探测	
00:0C:29:C8:18:23	WXA5000-9C81823	Group One	192.168.94.229	WXA 5000	1.3.2-0-7	集群就绪：● 运行时间：41 days, 3 hrs 负载：5.50%	● TCP 加速 ● WFS ● SSMB ● Web 缓存	0	ⓘ	ⓧ	管理	探测

ID WXA 系列设备的 MAC 地址。

名称 WXA 系列设备的名称。

组 WXA 系列设备所属的群组。

IP WXA 系列设备的 IP 地址。

型号 WXA 系列设备的型号。

固件 安装在 WXA 系列设备上的固件版本。

注：单击 WXA 系列设备的固件版本，即可进入管理 | 更新 | WXA 固件。如需有关 WXA 固件及其更新的信息，请参阅 SonicOS 更新。

操作状态 显示 WXA 系列设备的操作状态：

- 集群就绪 - 绿色圆点表示 WXA 可用于群集。
- 运行时间 - WXA 运行的天数和小时数。
- 负载 - WXA 上滚动平均负载，以百分比表示。

组件

- TCP 加速
- WFS 加速
- 对签名 SMB 的 WFS 扩展支持
- Web 缓存

显示加速组件的状态：

- 绿点表示该服务正在 WXA 上运行。
- 白点表示该服务正在 WXA 上运行，并可用于加速流量，但该组件目前在 WXA 的群组设置中被禁用。

连接

当前通过 WXA 的连接数。工具提示还显示：

- 此特定 WXA 模型支持的最大连接数。
- 可以访问的并发连接的总许可数。

配置	编辑和删除图标。 注： 不能删除活动的 WXA 系列设备。
管理	管理按钮，用于显示 管理 WXA 对话框。
探测	探针按钮，用于探测 WXA 并更新表中的统计。

主题：

- 第 575 页的[过滤 WXA 表](#)
- 第 575 页的[探测](#)
- 第 575 页的[刷新 WXA 表](#)
- 第 576 页的[启用对签名 SMB 的扩展支持](#)。

过滤 WXA 表

默认情况下，所有 WXA 都显示在表中。可以将显示限定于仅所选的组或未分配的 WXA。

过滤 WXA 表格显示的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 从显示中，选择要显示的内容：

全部（默认值）	显示所有 WXA
对于所选群组	仅显示属于所选群组的 WXA
未分配	仅显示未分配给任何群组的 WXA

- 3 如果选择了对于所选群组，请在群组表中选择包含要显示的 WXA 的群组。

探测

探测验证 WXA 系列设备的存在性和状态，还可将最新的群组设置推送到 WXA 系列设备。可以探测单个 WXA 或所有 WXA。

探测所有 WXA 的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击探测全部。WXA 表已更新。

探测单个 WXA 的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在 WXA 表中，单击 WXA 的探测列的管理按钮。该 WXA 的显示已更新。

刷新 WXA 表

刷新 WXA 表即刷新 WXA 列表以及每个 WXA 上的不同加速组件的状态。

刷新 WXA 表的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击刷新图标。

启用对签名 SMB 的扩展支持。

提示： 使用“已签名 SMB 的 WFS 安装指南”为已签名 SMB 快速配置 WXA 扩展支持。如需访问“已签名 SMB 的 WFS 安装指南”，请单击 SonicOS 管理界面上的快速配置。如需有关本指南的更多信息，请参阅 SonicOS 快速配置。

注： 对签名 SMB 的 WFS 扩展支持是在群组配置之外配置的。

当配置“对签名 SMB 的 WFS 扩展支持”时，选择专用于加速签名 SMB 流量的 WXA 系列设备。

主题：

- 第 576 页的[分机支持签名 SMB](#)
- 第 579 页的[高级模式](#)
- 第 581 页的[域详细信息](#)
- 第 583 页的[本地/远程服务器表](#)

分机支持签名 SMB

配置对签名 SMB 加速的扩展支持的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。



- 3 选择启用对签名 **SMB** 的扩展支持。默认情况下已选中该选项。
- 4 单击编辑图标以选择专用于扩展支持的 WXA。

重要：更改已经专用于签名 **SMB** 加速的扩展支持的 WXA，会使任何活动的会话和文件传输终止，从而可能导致数据丢失。

新 WXA 必须加入域而且必须配置相关的服务器和共享。必须更改最终用户设备上的路径，以反映新 WXA 的配置。或者，要保持相同的路径，第一个 WXA 必须脱离域且删除所有域记录，然后再用相同的主机名和完全相同的设置来配置新 WXA。

- 5 对 SPN 别名和“委派的受信任项”，通过单击**更新域记录**添加任何缺失的域记录并删除陈旧记录。显示更新域记录弹出窗口。

添加任何缺失的域记录并删除陈旧记录，以使 WFS 加速能正常起作用。

输入域管理员或其他具有合适资质用户的用户名和密码。

用户名：

密码：

- 6 在用户名和密码字段分别输入域管理员的用户名和密码。
- 7 单击**更新记录**。
- 8 如果未使用存储转发，请转至**步骤 17**。
- 9 如需配置存储转发的设置，请单击**配置**。显示配置存储和转发对话框。

配置存储和转发 ✕

启用存储和转发

文件扩展名：

[输入要在存储和转发中包括的文件类型扩展名。
扩展名应以点号 "." 开始，并用逗号、
空格或新行隔开。]
注：必须对每个远程共享启用缓存。

- 10 选择启用存储和转发。默认情况下未选中该选项。
 - 11 在文件扩展名字段中输入要存储和转发的文件类型的扩展名。扩展名必须以点号 (.) 开始，并用逗号、空格或新行隔开。
- 注：**必须对每个远程共享启用缓存。

- 12 单击**确定**。
- 13 如需查看存储和转发的当前文件操作，请单击**查看**。显示存储和转发对话框。

✕ 🔄 刷新： 秒 ⏸

未找到正在进行的存储和转发操作。

- 14 如需：

- 刷新显示，请单击刷新图标。
 - 暂停显示，请单击暂停图标。
- 15 如需更改刷新频率，请在刷新字段中输入频率。最小值为 1 秒，最大值为 999 秒，默认值为 600 秒。
- 16 如果不想测试签名，请转至 [步骤 24](#)。
- 17 如需测试到指定服务器的流量是否需要签名，请单击签名测试。此时显示签名测试对话框。

输入服务器的完全限定名称或 IP 地址，以测试它是否必须为自己的 SMB 数据包添加签名。或者，如果该选项可用，请从列表中选择一台或多台服务器。

服务器：

18 您可以

- 输入服务器的完全限定名称或 IP 地址。
- 通过单击列表 (...) 按钮显示服务器列表。显示选择要测试的服务器弹出窗口：

选择您要测试的一台或多台服务器。

文件服务器	
<input type="checkbox"/>	L10N095181.tb20dc3.sonicwall.com
<input type="checkbox"/>	L10N094188.tb20dc3.sonicwall.com
<input type="checkbox"/>	L10N094189.tb20dc3.sonicwall.com

- 19 选择一个或多个服务器。
- 20 单击确定。弹出窗口关闭。
- 21 单击确定。请耐心等待，因为显示测试结果可能需要几分钟的时间。

已在测试中确定其 SMB 流量已签名的文件服务器。为了实现对此流量进行加速的扩展支持，必须将那些服务器添加到位于服务器站点和远程客户端 PC 站点的 WXA 的配置中。此外，其中每个 WXA 还必须加入域。

此特定 WXA 已加入域。

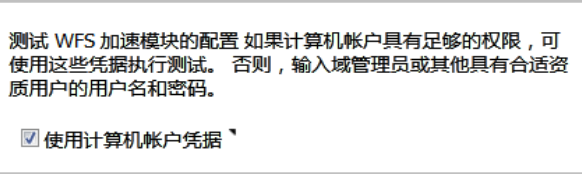
延迟界限： ms 用于判断服务器是本地服务器还是远程服务器。

服务器	需要签名	延迟 (ms)	添加到配置
L10N095181.tb20dc3.sonicwall.com	是	0.27	<input checked="" type="checkbox"/> 添加为远程服务器 下一个跃点 WXA : L10N095181-via-WXA-TB20-RS.tb20dc3.sonicwall.com 本地 WXA 名称: WXA Server

- i** **重要：** 如果需要 SMB 签名，WXA 系列设备必须加入域。测试结果表明 WXA 系列设备是否加入了域。
- i** **提示：** 如果需要签名，请通过以下方式将鼠标悬停在工具提示上：
- 是显示签名所需的地址
 - 延迟时间显示服务器超出在延迟阈值中所设时间的的时间。

- 22 如需指定阈值以确定服务器是本地还是远程，请在延迟界限中输入时间（以毫秒为单位）。最小时长为 1 毫秒，最大时长为 99999999 毫秒，默认值为 5 秒。
- 23 单击确定。
- 24 如果不想测试 WFS 加速模块，请转至 [步骤 29](#)。

25 如需测试 WFS 加速模块的配置，请单击测试配置。显示测试配置弹出窗口。



26 如果 WXA 系列设备具有其自己的计算机帐户和合适的权限，请选择使用计算机帐户凭据。默认情况下已选中该选项。

注：如果 WXA 没有适当的权限，则需要输入域管理员的管理员用户名和密码。

27 单击运行测试。请耐心等待，因为显示测试结果可能需要几分钟的时间。

服务器	解析为	用于共享配置	短 SPN	长 SPN	受信于委托	接受委托	已接受连接	已传播连接
L10N095181-via-WXA-TB20-RS.tb20dc3.sonicwall.com	192.168.141.1	服务器	✓	✓		✓	✓	
L10N95181.tb20dc3.sonicwall.com	10.20.1.12	本地 WXA	✓	✓			✓	✓
wxa-tb20-rs.tb20dc3.sonicwall.com	192.168.141.1		✓	✓	特定主机			
wxa5000-9c81823.tb20dc3.sonicwall.com	10.20.1.12		✓	✓	特定主机			

服务器	被测试服务器的服务主体名称 (SPN)
解析为	IP 地址，绿色复选标记指示正确的分辨率
用于共享配置	指示如何将 SPN 用作名称来识别设备
短 SPN	指示短 SPN 是否存在于计算机中
长 SPN	指示长 SPN 是否存在于计算机中
受信于委托	绿色复选标记指示服务器是否可信任委派： <ul style="list-style-type: none">通常 - 一般来说，此服务器可信任委派。特定主机 - 鼠标悬停在工具提示上显示受信任委派服务器的主机
接受委托	绿色复选标记指示服务器接受委派。将鼠标悬停在工具提示上显示可以使用服务器的短名称或长名称提供凭据的主机。
已接受连接	绿色复选标记指示服务器已接受授权的连接。将鼠标悬停在工具提示上可显示连接。
已传播连接	绿色复选标记指示服务器传播授权的连接。将鼠标悬停在工具提示上可显示连接。
反向 DNS	显示反向 DNS 解决方式

28 单击关闭。

29 如需使用高级模式，请选择高级模式。默认情况下未选中该选项。

高级模式

当选择高级模式时，“对签名 SMB 加速的扩展支持”对话框中的选项会更改：



配置高级模式的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 选择高级模式。这些选项将发生更改。
- 4 单击高级选项。显示高级选项对话框。
- 5 从客户端签名中，选择客户端必须使用的签名选项：
 - 自动（默认）
 - 强制
 - 禁用
- 6 从服务器签名中，选择服务器必须使用的签名选项：
 - 自动（默认）
 - 强制
 - 禁用
- 7 在最大传输字段中输入一个客户端可传输的最大数据量（以字节为单位）。默认值为 4096。
- 8 单击确定。
- 9 如需重启“对签名 SMB 的 WFS 扩展支持”服务，请单击重启。
- 10 如需清除缓存，请单击清除缓存。
- 11 在域详细信息部分中，通过单击域控制器的编辑图标配置 Kerberos 服务器。随即显示配置 Kerberos 服务器对话框。

您可以选择自动选择 Kerberos 服务器，并根据它们的优先级、权重和往返时间 (RTT)，手动输入一个或从域发现列表中选择一个。

允许自动选择发现的 Kerberos 服务器

当前选择： l10n095181.tb20dc3.sonicwall.com:88

手动输入 Kerberos 服务器：

:

选择发现的 Kerberos 服务器

Kerberos 服务器	端口	优先级	权重	RTT
<input type="radio"/> l10n095181.tb20dc3.sonicwall.com	88	0	100	0.713 ms 0.711 ms 0.709 ms

12 指定选择 Kerberos 服务器的方式：

- 允许自动选择发现的 **Kerberos 服务器** - 显示当前选择及其端口。
- 手动输入 **Kerberos 服务器** - 名称和端口字段变为可用。
 - 输入用于在域中进行身份验证的 Kerberos 服务器的名称和端口。
- 选择发现的 **Kerberos 服务器** - 在 **Kerberos 服务器**表中发现的条目变为可用。
 - 选择其中一个条目。

13 单击确定。

域详细信息

域详细信息

域: tb20dc3.sonicwall.com WXA 已加入域。

WXA 主机名: WXA5000-9C81823

WFS 加速地址: 10.20.1.12

域 域的名称以及 WXA 是否已加入。

WXA 主机名 WXA 的名称

WFS 加速地址 WFS 加速模块的 IP 地址

主题：

- 第 581 页的 [重新加入域](#)
- 第 582 页的 [脱离域](#)
- 第 582 页的 [加入域](#)
- 第 583 页的 [删除域](#)

重新加入域

重新加入域的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 **SMB** 的扩展支持。显示对签名 **SMB** 加速的扩展支持对话框。
- 3 单击重新加入。

脱离域

脱离域的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击脱离。将显示确认消息。

是否确定要将设备脱离域？

- 4 单击是。将显示确认消息。

设备已脱离域。

现在必须手动删除域控制器中的计算机帐户，并从 DNS 服务器中删除任何相关的条目。

- 5 单击确定。重新加入按钮变为删除图标。
- 6 手动删除域控制器中的计算机帐户。
- 7 从 DNS 服务器中删除任何相关条目。

加入域

加入域的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击加入。随即显示加入域对话框。

要使 WXA 系列设备加入域，请输入管理员的凭据，并单击以下按钮。

用户名：

密码：

- 4 在用户名和密码字段中分别输入管理员的用户名和密码。
- 5 单击加入域。

加入域可能需要一些时间。

是否要继续？

- 6 单击是。加入域结果弹出窗口显示加入是否成功以及进程的详细信息。

结果摘要

- 成功加入域

详细信息

- ✓ 检查 WFS (已签名 SMB) 配置
- ✓ 检查 l10n095181.tb20dc3.sonicwall.com 的域控制器名称
- ✓ 检查 l10n095181.tb20dc3.sonicwall.com 的域控制器地址。
- ✓ 设置前检查 wadmin 凭据。
- ✓ 检查 NETBIOS 域。
- ✓ NETBIOS 域为 TB20DC3。
- ✓ 准备将 WXA 加入域。
- ✓ 将 WXA 加入域 tb20dc3.sonicwall.com。
- ✓ 启动时钟同步
- ✓ 检查 WFS (已签名 SMB) 配置
- ✓ 设置委派的受信任项
- ✓ 在 DNS 中注册 WFS (已签名 SMB) 服务器

7 单击关闭。

删除域

删除域的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击删除图标。

删除域也将删除 Kerberos 服务器以及配置中的任何服务器和共享。

是否确定要继续？

4 单击是。

本地/远程服务器表

本地服务器		远程服务器	
文件服务器	本地 WXA 名称	共享	域记录 配置
L10N094188.tb20dc3.sonicwall.com	L10N094188-via-WXA5000-9C81823.tb20dc3.sonicwall.com	全部	✓

文件服务器 文件服务器的名称。

本地 WXA 名称 本地 WXA 服务器的名称。

共享

域记录 绿色复选标记表示域记录是最新的，红色的 X 表示记录需要更新。如需更新，请单击更新域记录。

配置 显示删除图标。

主题：

- 第 584 页的删除服务器
- 第 584 页的添加本地文件服务器

删除服务器

删除服务器的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 在服务器表中，单击要删除的服务器的删除图标。将显示确认消息。

是否确定要从配置中删除文件服务器:L10N094188.tb20dc3.sonicwall.com？这也会删除所有关联的共享。

删除服务器后，系统将提示您添加管理员凭据，以便从域中删除所有陈旧的记录。

- 4 单击删除。将显示对话框。
- 5 在用户名和密码字段中分别输入管理员的用户名和密码。
- 6 单击确定。

添加本地文件服务器

添加本地文件服务器的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 在本地服务器下，单击添加图标。显示添加本地文件服务器对话框。

从网络中这些发现的文件服务器中选择一个本地文件服务器。

添加服务器后，系统将提示您添加管理员凭据，以便在域中创建必要的记录。

将加速对文件的共享文件夹和文档的文件操作。如果想要将 WFS 加速（已签名 SMB）限制为指定共享，可在“高级模式”中配置。

文件服务器: L10N094188.tb20dc3.sonicwall.com ▾

- 4 从文件服务器中选择文件服务器。
- 5 单击确定。
- 6 显示更新域记录对话框。

添加任何缺失的域记录并删除陈旧记录，以使 WFS 加速能正常起作用。

输入域管理员或其他具有合适资质用户的用户名和密码。

用户名:

密码:

- 7 在用户名和密码字段中分别输入管理员的用户名和密码。
- 8 单击更新记录。
- 9 单击是。更新域结果弹出窗口显示加入是否成功以及进程的详细信息。

结果摘要

- 成功更新域记录

详细信息

- ✓ 检查 WFS (已签名 SMB) 配置
- ✓ 检查 110n095181.tb20dc3.sonicwall.com 的域控制器名称
- ✓ 检查 110n095181.tb20dc3.sonicwall.com 的域控制器地址。
- ✓ 设置前检查 wadmin 凭据。
- ✓ 检查 NETBIOS 域。
- ✓ NETBIOS 域为 TB20DC3。
- ✓ 检查 WFS (已签名 SMB) 配置
- ✓ 设置委派的受信任项
- ✓ 在 DNS 中注册 WFS (已签名 SMB) 服务器

- 10 单击关闭。

显示远程服务器

在服务器表中显示远程服务器的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 在域详细信息下，单击远程服务器。服务器表显示所有已配置的远程服务器。

添加远程服务器

添加远程服务器的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击远程服务器。显示远程服务器表。
- 4 在远程服务器下，单击添加图标。显示添加远程文件服务器对话框。

从网络中这些发现的文件服务器中选择一个远程文件服务器。远程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 配置的用于提供加速访问该服务器功能的“下一个跃点”。

键入本地 WXA 的唯一名称或别名（添加点号将使用该域的名称自动填充）。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。

例如，如果当前路径为： \\remote_server\docs，则在“WFS 加速”下，它将是 \\local_wxa\docs

添加服务器后，系统将提示您添加管理员凭据，以便在域中创建必要的记录。

将加速对文件的共享文件夹和文档的文件操作。如果想要将 WFS 加速（已签名 SMB）限制为指定共享，可在“高级模式”中配置。

文件服务器: L10N094188.tb20dc3.sonicwall.com

本地 WXA 名称: wxa5000-9c81823.tb20dc3

- 5 从文件服务器中选择文件服务器。
- 6 在本地 WXA 名称字段中输入 WXA 服务器的唯一名称或别名。
- 7 单击确定。
- 8 显示更新域记录对话框。

添加任何缺失的域记录并删除陈旧记录，以使 WFS 加速能正常起作用。

输入域管理员或其他具有合适资质用户的用户名和密码。

用户名:

密码:

- 9 在用户名和密码字段中分别输入管理员的用户名和密码。
- 10 单击更新记录。
- 11 单击是。更新域结果弹出窗口显示加入是否成功以及进程的详细信息。

使用已签名的 SMB 工具

主题:

- 第 586 页的 [DNS 名查找](#)
- 第 587 页的 [可用共享](#)

DNS 名查找

查找 DNS 名称的步骤如下:

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击已签名的 SMB 工具



- 4 输入服务器以在查找名称或 IP 字段中查找。执行按钮变为可用。
- 5 单击执行。将显示结果：



可用共享

查找可用的共享的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击已签名的 SMB 工具
- 4 单击可用共享。



- 5 输入服务器以在主机字段中查找。
- 6 在用户名和密码字段分别输入管理员的用户名和密码。执行按钮变为可用。
- 7 单击执行。显示“可用共享”弹出窗口。
- 8 单击确定。

Kerberos 服务器列表

列出 Kerberos 服务器的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击对签名 SMB 的扩展支持。显示对签名 SMB 加速的扩展支持对话框。
- 3 单击已签名的 SMB 工具
- 4 单击 Kerberos 服务器列表。



The screenshot shows a configuration dialog box with three tabs: "DNS 名查找", "可用共享", and "Kerberos 服务器列表". The "Kerberos 服务器列表" tab is selected. Below the tabs, there are two radio buttons: "基本列表" (selected) and "包括可访问性测试". A text field labeled "域:" contains the value "tb20dc3.sonicwall.com". At the bottom right, there is a button labeled "执行".

- 5 选择如何列出服务器：
 - 基本列表 - 仅显示 Kerberos 服务器的端口和已解析的 IP。
 - 包括可访问性测试（默认）- 包括服务器的优先级、权重和 RTT。
- 6 单击执行。将显示测试结果：
 - 基本列表：



The screenshot shows the same configuration dialog box as above, but with the "基本列表" radio button selected. Below the configuration fields, there is a section labeled "结果" (Results). Under "结果", the domain "域: tb20dc3.sonicwall.com" is displayed. Below this, there is a table with the following data:

Kerberos 服务器	端口	解析的 IP
l10n095181.tb20dc3.sonicwall.com	88	192.168.145.181

- 包括可访问性测试：

基本列表
 包括可访问性测试

域:

结果

域: **tb20dc3.sonicwall.com**

Kerberos 服务器	端口	解析的 IP	优先级	权重	RTT
110n095181.tb20dc3.sonicwall.com	88	192.168.94.181	0	100	0.412 ms 0.413 ms 0.413 ms

- Kerberos 服务器** Kerberos 服务器的名称。
- 端口** Kerberos 服务器的端口。
- 解析的 IP** 服务器名称解析的 IP 地址。
- 优先级** Kerberos 服务器的优先级。首选较低的值。
- 权重** 具有相同优先级的 Kerberos 服务器的相对权重。首选较高的值。
- RTT** 探测到 Kerberos 服务器的往返时间。

配置 VPN 策略的 WXA

显示: 仅 IPv4

名称	组	编辑
VPN Tunnel Policy		

VPN 策略表显示所有使用 WXA 加速设置的 VPN 策略。

编辑 VPN 策略的 WXA 加速设置的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击 **VPN 策略**。
- 3 如需筛选策略，请从**群组**表中选择 WXA 群组。
- 4 从**显示**中选择对于所选群组。默认设置为**全部**。
- 5 单击策略的编辑图标。将显示**编辑 VPN**对话框。

为了加速路由中的流量，请选择应使用的 WXA 群组。

名称: VPN Tunnel Policy

群组:

- 6 从**群组**中选择将应用于 VPN 策略的 WXA 群组。
- 7 单击**确定**。

配置 SSL VPN 流量加速

您可以启用或禁用 WXAC 客户端的 NetExtender SSL VPN 流量加速。

注：WXA 必须获得许可才能支持 NetExtender WAN 加速客户端 (WXAC)。

启用 WXAC 的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 单击 SSL VPN。



- 3 从群组中选择要启用 WXAC 的群组（默认为无）。“接受”按钮变为可用。
- 4 单击接受。
- 5 当前正在使用的活动许可证数显示在群组下拉菜单下。

显示和编辑 WXA 的路由策略



源	VPN 流量源自的网关。
目标	VPN 流量的目标。
备注	在配置路由时包含的可选注释。
组	适用于该路线的群组。
编辑	显示编辑图标。

过滤路由表中显示的路由的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表下，从显示中选择特定群组的路由。默认设置为全部。

编辑路线策略的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表下，单击路由策略。
- 3 单击所需路由的编辑图标。显示编辑路由弹出窗口。

源： Any

目标： Any

备注：

群组：

- 4 从群组中选择要应用该路由的群组。
- 5 单击确定。

监控群组连接

您可以用线型图或条形（堆栈）图查看通过 WXA 的连接总数。也可以查看特定群组的总连接数。



显示连接的步骤如下：

- 1 转至系统设置 > WAN 加速。
- 2 在群组表下，单击**监控**。
提示： 还可以通过单击**群组表**中的所需组的**监控**来显示连接。
- 3 从**群组**中选择显示连接的群组。默认设置为**全部**。
- 4 从**图表类型**中，选择想要显示数据的方式：
 - **线型**（默认）
 - **堆栈**（条形图）
- 5 如需放大图表中选定的区域，请在所需区域上拖动鼠标。
- 6 如需将图表恢复到其默认缩放，请单击**重置缩放**。

- 关于 VoIP
- 配置 SonicWall VoIP 功能

关于 VoIP

- [第 594 页的关于 VoIP](#)
 - [第 594 页的什么是 VoIP?](#)
 - [第 594 页的 VoIP 安全性](#)
 - [第 595 页的 VoIP 协议](#)
 - [第 596 页的 SonicWall 的 VoIP 功能](#)

关于 VoIP

主题:

- [第 594 页的什么是 VoIP?](#)
- [第 594 页的 VoIP 安全性](#)
- [第 595 页的 VoIP 协议](#)
- [第 596 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，而非公用电话交换网 (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 安全设备要求

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，且安全设备通过网络地址转换 (NAT) 修改源地址和源端口信息时还会引入不一致性，因此 VoIP 难以有效穿越标准安全设备。下面是几个原因。

- **VoIP 采用两个单独的协议运行** - 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，因而需要额外的安全设备处理。
- **源和目标 IP 地址嵌入 VoIP 信令数据包中** - 支持 NAT 的安全设备在数据包的 IP 头级别转换 IP 地址和端口。完全对称的 NAT 安全设备会频繁调整其 NAT 绑定且可能任意关闭针孔，使入站数据包无法传入其所保护的网路，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 安全设备有必要在数据包穿越安全设备时，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 位于安全设备的 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。实质上，对于不支持 VoIP 的安全设备，SBC 是充当 VoIP 流量的代理。SonicWall 安全设备是支持 VoIP 的安全设备，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 SonicWall 6.2 的 SonicOS 设备上支持 VoIP。

VoIP 协议

VoIP 技术基于两个主要协议：H.323 和 SIP。这些协议可以全局应用，也可以按照防火墙规则应用。

主题：

- [第 595 页的 H.323](#)
- [第 596 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（但其并非 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并执行其它电话任务。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 596 页的 VoIP 安全性](#)
- [第 597 页的 VoIP 网络](#)
- [第 597 页的 VoIP 网络互操作性](#)
- [第 598 页的支持的接口](#)
- [第 598 页的支持的 VoIP 协议](#)
- [第 601 页的 BWM 和 QoS](#)
- [第 601 页的 SonicOS 如何处理 VoIP 呼叫](#)

VoIP 安全性

- 流量合法性 - 对穿越安全设备的每一个 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。SonicWall 安全设备能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。
 - 利用同步泛洪攻击保护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。

i 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 SonicWall 网站 <http://www.sonicwall.com> 上提供的“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）可用于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次要 WAN 端口。此次要 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，流量才会通过次要端口路由。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 能自动处理 VoIP 设备的增加、更改和移除，确保无任何 VoIP 设备不受保护。利用先进的监控和跟踪技术，一旦有 VoIP 设备插入安全设备背后的网络，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，安全设备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安全设备动态分配。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，从而为安全设备背后的 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，它根据从安全设备收到的 syslog 数据流，提供关于安全和网络活动的详尽细致的报告。几乎可以针对安全设备活动的任何方面产生报告，包括各用户或组的使用模式、特定安全设备或各组安全设备上发生的事件、攻击的类型和时间、资源消耗和限制。

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 599 页的 [H.323](#)
- 第 599 页的 [SIP](#)
- 第 599 页的 [SonicWall VoIP 供应商互操作性](#)

- 第 600 页的[编解码器](#)
- 第 600 页的[SonicOS 不能执行深度包检测的 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 终端使用组播发现网关守卫
- 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

与 [SonicWall VoIP 互操作的部分设备列表](#) 表列出了许多领先制造商制造的能与 SonicWall VoIP 互操作的设备。

与 SonicWall VoIP 互操作的部分设备列表

H.323

软件电话:

Avaya
Microsoft NetMeeting
OpenPhone
PolyCom
SILabs SJ Phone

电话/可视电话:

Avaya
Cisco
D-Link
PolyCom
Sony

网关守卫:

Cisco
OpenH323 Gatekeeper

网关:

Cisco

SIP

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 - 媒体流承载由 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 不能执行深度包检测的 VoIP 协议

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

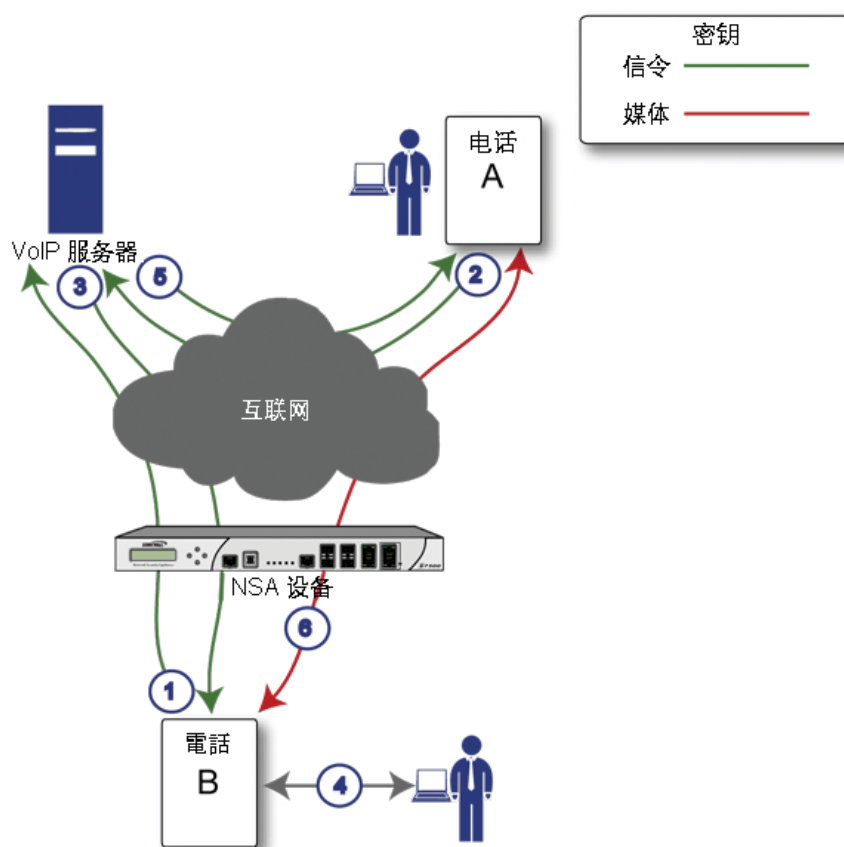
SonicOS 为所有 VoIP 呼叫情况提供高效且安全的解决方案。下面是 SonicOS 如何处理 VoIP 呼叫流程的一些例子：

- [第 601 页的来电](#)
- [第 603 页的本地呼叫](#)

来电

[来电事件顺序](#)显示了来电期间发生的事件顺序。

来电事件顺序



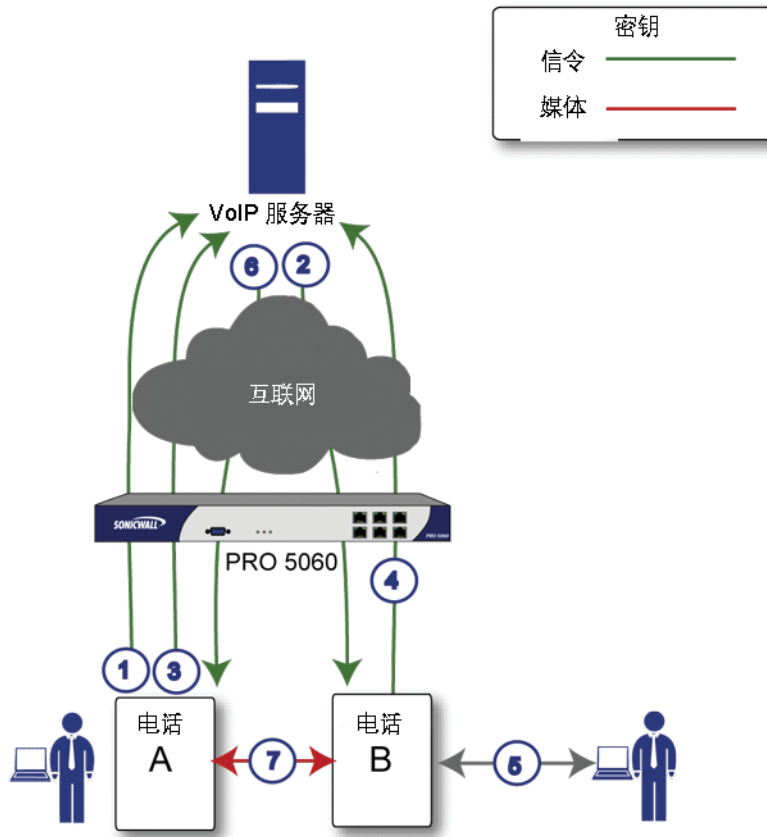
下面说明来电事件顺序所示的事件顺序：

- 1 电话 B 在 VoIP 服务器中注册 - 安全设备通过监控传出的 VoIP 注册请求，建立可接入 IP 电话的数据库。SonicOS 在电话 B 的专用 IP 地址和注册消息中使用的安全设备公共 IP 地址之间进行转换。VoIP 服务器不知道电话 B 位于安全设备之后并有一个私有 IP 地址，它将安全设备的公共 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 服务器向安全设备的公共 IP 地址发送呼叫请求。当它到达安全设备时，SonicOS 验证请求的来源和内容。然后，安全设备确定电话 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 转换此专用 IP 信息以使用安全设备的公共 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 位于安全设备之后，因为它得到的是 VoIP 服务器提供的安全设备公共地址。
- 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

本地 VoIP 来电事件顺序显示了本地 VoIP 呼叫期间发生的事件顺序。

本地 VoIP 来电事件顺序



下面说明本地 VoIP 来电事件顺序所示的事件顺序：

- 1 电话 A 和电话 B 在 VoIP 服务器中注册 - 安全设备通过监控传出的 VoIP 注册请求，建立可接入 IP 电话的数据库。SonicOS 在电话的专用 IP 地址和安全设备公共 IP 地址之间进行转换。VoIP 服务器不知道电话位于安全设备之后。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 - 即使它们位于同一安全设备之后，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 服务器向安全设备的公共 IP 地址发送呼叫请求。然后，安全设备确定电话 B 的私有 IP 地址。
- 4 电话 B 振铃并接听 - 当电话 B 接听时，安全设备转换其私有 IP 信息以使用安全设备的公共 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 - 安全设备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，且无需安全设备执行地址转换。

配置 SonicWall VoIP 功能

- 第 604 页的[配置任务](#)
 - 第 604 页的[配置 VoIP](#)
 - 第 609 页的[配置 VoIP 日志](#)

配置任务

针对 VoIP 部署配置 SonicWall 安全设备要以 SonicWall 管理界面中的基本网络配置为基础。本章节假设安全设备已针对网络环境进行配置。

注：如需 VoIP 的常规信息，请参阅第 594 页的[关于 VoIP](#)。

主题：

- 第 604 页的[配置 VoIP](#)
- 第 609 页的[配置 VoIP 日志](#)

配置 VoIP

您可通过[管理 | 系统设置 | VOIP](#) 上的设置来配置 VoIP。此页面分为三个部分：[常规设置](#)、[SIP 设置](#)和 [H.323 设置](#)。

常规设置

启用一致的 NAT

SIP 设置

使用全局控制启用 SIP 转换 使用防火墙基于规则的控制启用 SIP 转换

启用 SIP 转换

在 TCP 连接上启用转换

在服务对象中对 TCP/UDP 端口执行转换： SIP

允许信令端口传输非 SIP 数据包

启用 SIP 背对背用户代理 (B2BUA) 支持

SIP 信令不活动超时(秒数): 3600

SIP 媒体不活动超时(秒数): 120

用于转换的其它 SIP 信令端口 (UDP)(可选): 0

启用 SIP 终端注册异常跟踪

注册跟踪间隔 (秒): 300

注册失败的阈值: 5

终端阻塞间隔 (秒): 3600

H.323 设置

使用全局控制启用 H323 转换 使用防火墙基于规则的控制启用 H323 转换

启用 H.323 转换

仅接受来自 Gatekeeper 的传入呼叫

H.323 信令/媒体不活动超时(秒数): 300

默认 WAN/DMZ Gatekeeper IP 地址: 0.0.0.0

主题:

- [第 605 页的常规设置](#)
- [第 606 页的 SIP 设置](#)
- [第 608 页的 H.323 设置](#)

常规设置

常规设置

启用一致的 NAT

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 **IP 地址和端口对** 表所示：

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 **IP 地址和端口对** 表相同的端口）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。如果无一致的 NAT，端口以及可能包括 IP 地址都会在每次请求时发生变化。

i 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，否则请勿启用它。

启用一致的 NAT

启用一致的 NAT 的步骤如下：

- 1 选择启用一致的 NAT 选项。默认情况下未选中该选项。
- 2 单击接受。

SIP 设置

SIP 设置

使用全局控制启用 SIP 转换 使用防火墙基于规则的控制启用 SIP 转换

启用 SIP 转换

在 TCP 连接上启用转换

在服务对象中对 TCP/UDP 端口执行转换： SIP

允许信令端口传输非 SIP 数据包

启用 SIP 背对背用户代理 (B2BUA) 支持

SIP 信令不活动超时(秒数): 3600

SIP 媒体不活动超时(秒数): 120

用于转换的其它 SIP 信令端口 (UDP)(可选): 0

启用 SIP 终端注册异常跟踪

注册跟踪间隔 (秒): 300

注册失败的阈值: 5

终端阻塞间隔 (秒): 3600

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

启用 SIP 的步骤如下：

- 1 转到**管理 | 系统设置 | VOIP | SIP 设置**。
- 2 选择是全局启用 SIP 转换还是按防火墙规则启用：
 - 使用全局控制启用 SIP 转换。默认情况下已选中该选项。
 - 使用防火墙基于规则的控制启用 SIP 转换。请确保按照 SonicOS 策略中的描述配置防火墙规则以控制 SIP 转换。
- 3 如果未配置 SIP 转换，请转至**步骤 12**。
- 4 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。

若希望安全设备执行 SIP 转换，则需要检查此设置。如果 SIP 代理位于安全设备的公共 (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，因而这些消息不会被改变，SIP 代理不知道如何返回到安全设备之后的客户端。

- 使安全设备能浏览各条 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。

i | **提示：**一般而言，应当选择**启用 SIP 转换**，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。

- 5 如需在基于 TCP 的 SIP 会话上执行 SIP 转换，请选择在**TCP 连接上启用 SIP 转换**。默认情况下已选中该选项。
- 6 从“执行”转换到在服务对象中的**TCP/UDP 端口**选择服务对象。默认值为**SIP**。
- 7 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。默认情况下未选中该选项。

i | **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。

- 8 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，仅当安全设备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。

i | **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。

- 9 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。指定以下情况的最大空闲时间：

- 在 SIP 信令不活动超时中没有交换信令（控制）消息。最小时长为 30 秒，最大时长为 1000000 秒（~1.2 天），默认值为 **3600** 秒（60 分钟）。
 - 在 SIP 媒体不活动超时中没有正在交换的媒体（如音频或视频）数据包。最小时长为 30 秒，最大时长为 3600 秒（1 小时），默认时间值为 **120** 秒（2 分钟）。
- 10 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 为默认值，最大值为 65535）时，安全设备可在这些非标准端口上执行 SIP 转换。
- i** | 提示：Vonage 的 VoIP 服务使用 UDP 端口 5061。
- 11 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。
 - 终端阻止间隔 (秒) - 默认值为 **3600** 秒（60 分钟）。
- 12 您可以
- 单击接受。
 - 转至第 608 页的 **H.323 设置**。

H.323 设置

H.323 设置

使用全局控制启用 H323 转换
 使用防火墙基于规则的控制启用 H323 转换

启用 H.323 转换

仅接受来自 Gatekeeper 的传入呼叫

H.323 信令/媒体不活动超时(秒数):

默认 WAN/DMZ Gatekeeper IP 地址:

配置 H.323 设置

配置 H.323 设置的步骤如下：

- 转到管理 | 系统设置 | VOIP | H.323 设置。
- 选择是全局启用 H.323 转换还是按防火墙规则启用：
 - 使用全局控制启用 H.323 转换。默认情况下已选中该选项。
 - 使用防火墙基于规则的控制启用 H.323 转换。请确保按照 SonicOS 策略中的描述配置防火墙规则以控制 H.323 转换。
- 如果未配置 H.323 转换，请转至 **步骤 5**。

- 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。默认时间值为 **300 秒**（5 分钟），最小时长为 **60 秒**（1 分钟），最大时长为 **122400 秒**（34 小时）。
- 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 设备的组播发现消息将接受已配置的组播处理。
- 5 单击**接受**。

主题：

- 第 609 页的**配置 WAN 接口的带宽**
- 第 609 页的**配置 VoIP 访问规则**

配置 WAN 接口的带宽

i | 注：如需在 WAN 接口进行带宽管理 (BWM) 和配置 BWM 的信息，请参阅 SonicOS 策略。

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。

i | 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。

i | 注：配置网络访问规则的带宽管理之前，必须在**管理 | 系统设置 | 网络 > 接口**上选择 **WAN** 接口的带宽管理。

如需了解如何为 SonicWall 安全设备上的 VoIP 流量添加访问规则，请参阅 SonicOS 策略。

配置 VoIP 日志

可以启用**调查 | 日志 | 事件**日志中显示的 VoIP 事件的日志记录。如需启用 VoIP 日志，请参阅 SonicOS 调查。

- 配置虚拟助手

配置虚拟助手

- 第 611 页的[关于虚拟助手](#)
- 第 611 页的[最大限度提高虚拟助手灵活性](#)

关于虚拟助手

虚拟助手使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。

注：提供虚拟助手的技术员或管理员必须位于 SonicWall 安全设备的本地网络内部。

最大限度提高虚拟助手灵活性

可以通过系统设置 | 虚拟助手上的设置来控制虚拟助手。

常规设置

i 客户将看到此链接可以访问您的设备。
请检查以确保它是正确的链接。 <https://192.168.95.83/sslvpnSupportLogin.html>

帮助编码：

启用支持没有邀请

免责声明：

客户访问链接：

从入口登录显示虚拟帮助链接

提醒设置

i 如需更改电子邮件设置，请转至 [日志 > 自动](#) 页面。

邮件服务器：(未设置)

发件人地址：(未设置)

邮件服务器应该正确的设置用于该产品的任何电子邮件的功能。

技术员电子邮件列表：

邀请的主题：

邀请的消息：(最多800个字符)

已经生成了帮助邀请函：
%EXPERTNAME%

%CUSTOMERMSG%

%SUPPORTLINK%

如果你不能登录连接请通过复制粘贴连接来请求帮助：

%ACCESSLINK%
请不要回复。该消息是自动生成的。

请求设置

最大请求：

限制消息：
(最大256个字符)

来自一个 IP 的最大请求：
0 用于无限制

等待请求的过期时间：
0 用于无过期

限制设置

从已定义的地址中拒绝请求：

地址

添加

删除

配置虚拟助手

如需最大限度提高虚拟助手功能的灵活性，您应该花些时间正确调整所有设置。

主题：

- 第 613 页的 [为用户提供访问权限](#)
- 第 614 页的 [自定义通知](#)
- 第 615 页的 [管理请求](#)
- 第 615 页的 [阻止来自某些 IP 地址的请求](#)

为用户提供访问权限

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。
- 通过为客户设置全局帮助编码，您可以限制谁能进入系统请求帮助。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。

为用户提供访问权限的步骤如下：

- 1 转至 [管理 | 系统设置 | 虚拟助手](#)。

常规设置

i 客户将看到此链接可以访问您的设备。
请检查以确保它是正确的链接。 <https://192.168.95.83/sslvpnSupportLogin.html>

帮助编码：

启用支持没有邀请

免责声明：

客户访问链接：

从入口登录显示虚拟帮助链接

- 2 如需在可以请求帮助之前为客户提供一个全局的代码，请在 **帮助编码** 字段中输入最多 8 个字母数字字符。如需指示该代码不是必需的，请将此字段留空。

i | **提示：** 帮助编码可用于限制某人进入系统请求帮助。

- 3 允许客户在没有受到技术员邀请的情况下通过技术支持登录网页请求帮助的步骤如下：

- a 将 **帮助编码** 字段留空。
- b 选择 **启用支持没有邀请**。

i | **注：** 如果未选择此选项，则客户只能通过技术员的电子邮件邀请才能获得帮助。选择此选项可让客户从登录页面请求帮助。

- 4 如需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，请在 **免责声明** 字段中输入免责声明。

- 5 如需从网络外部访问 SSL VPN 安全设备，请在客户访问链接字段中输入 URL。如果将此字段留空，则发送给客户的支持邀请将使用技术员访问安全设备所使用的 URL。

i | 提示：如果是通过网络外的其他 URL 访问 SSL VPN 安全设备，请配置此选项。

- 6 如需将转到技术员登录页面的客户重定向到支持登录页面，请选择从入口登录显示虚拟帮助链接。
- 7 单击接受。
- 8 如需确保客户看到的访问链接是正确的，请单击常规设置信息描述中的链接。例如，显示在步骤 5 中配置的访问链接。

系统不接受未收到邀请的请求您的管理员必须选择“启用未收到邀请的支持”选项。

自定义通知

在提醒设置部分，自定义邀请和技术员提醒的各个特性。

自定义邀请和技术人员通知的步骤如下：

i | **重要：**在配置通知设置之前，请在管理 | 日志和报告 | 日志设置 | 自动化中配置电子邮件服务器和电子邮件地址。如需快速显示此页面，请单击通知设置部分中的信息描述中的链接。如需关于设置电子邮件服务器的信息，请参阅 SonicOS 日志和报告。

- 1 转至管理 | 系统设置 | 虚拟助手。
- 2 滚动到通知设置。

提醒设置

i 如需更改电子邮件设置，请转至日志 > 自动页面。

邮件服务器：(未设置)
发件人地址：(未设置)

邮件服务器应该正确的设置用于该产品的任何电子邮件的功能。

技术员电子邮件列表：

邀请的主题： %EXPERTNAME% 已经给你发送了支持邀请

邀请的消息：(最多800个字符)

已经生成了帮助邀请函：
%EXPERTNAME%

%CUSTOMERMSG%

%SUPPORTLINK%

如果你不能登录连接请通过复制粘贴连接来请求帮助：

%ACCESSLINK%
请不要回复。该消息是自动生成的。

- 3 在技术员电子邮件列表字段中创建技术员电子邮件地址列表，以便在未受邀请的客户进入支持队列时收到通知电子邮件。最多可以在此列表中添加 10 个电子邮件，之间以分号分隔。

- 如需自定义支持邀请电子邮件的主题行，使用**变量**表列出的变量在**邀请的主题**字段中输入所需文字。将提供邀请主题行样本。

变量

如需	使用
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%

- 如需自定义支持邀请电子邮件的正文，使用**变量**表列出的变量在**邀请消息**字段中输入所需文字。该消息最多可以包含 **800** 个字符。将提供邀请主题样本。
- 单击**接受**。

管理请求

可以在请求设置部分管理和限制支持请求。

管理和限制支持请求的步骤如下：

- 转至**管理 | 系统设置 | 虚拟助手**。
- 滚动到请求设置。

请求设置

最大请求：

限制消息：
(最大256个字符)

来自一个 IP 的最大请求：
0 用于无限制

等待请求的过期时间：
0 用于无过期

- 如需限制队列中一次包含的等待帮助客户数，请在**最大请求**字段中输入限制。到达限值时，将阻止新的请求。默认队列大小为 **10** 个请求。
- 如需在请求数达到最大限制因而队列中无可用位置时向客户显示消息，请在**限制消息**字段中输入消息。您可以创建最多含 **256** 个字符的消息。将提供样本消息。
- 如需限制来自单个 IP 的请求数，请在**来自一个 IP 的最大请求**字段中输入限制。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放入队列。输入 **0**（默认）表示无限制。
- 为了避免客户在高峰期间无限期等待虚拟助手的支持，您可以通过在**等待请求的过期时间**字段中输入限制（分钟）以设置客户保持在队列中等待获得支持的时间限制。如果您不想设置限制，则输入 **0**（默认）。
- 单击**接受**。

阻止来自某些 IP 地址的请求

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。

阻止来自 IP 地址的请求的步骤如下：

- 1 转至管理 | 系统设置 | 虚拟助手。
- 2 滚动到限制设置。

限制设置

从已定义的地址中拒绝请求：

地址
10.200.50.31/255.255.255.255

添加 删除

- 3 单击添加。将显示管理员地址对话框。

源地址类型： IP 地址

IP 地址：

- 4 从源地址类型中选择源地址的类型：

- IP 地址 - 默认
- IP 网络 - 选项发生改变，转到[步骤 7](#)。

源地址类型： IP 网络

网络地址：

子网掩码：

- 5 在 IP 地址字段中输入要阻止的 IP 地址。
- 6 转至[步骤 9](#)。
- 7 在网络地址字段中输入要阻止的网络地址。
- 8 在子网掩码字段中输入地址的子网掩码。
- 9 单击确定。条目被添加到从已定义的地址中拒绝请求表中。

从已定义的地址中拒绝请求：

地址
10.200.50.31/255.255.255.255

- 10 单击接受。

删除已阻止的地址

从“从已定义的地址中拒绝请求”字段中删除条目的步骤如下：

- 1 转至管理 | 系统设置 | 虚拟助手。
- 2 滚动到限制设置。
- 3 选择要删除的条目。
- 4 单击删除。

- 配置开放式验证、社交登录和 LHM
- BGP 高级路由
- IPv6
- SonicWall 支持

配置开放式验证、社交登录和 LHM

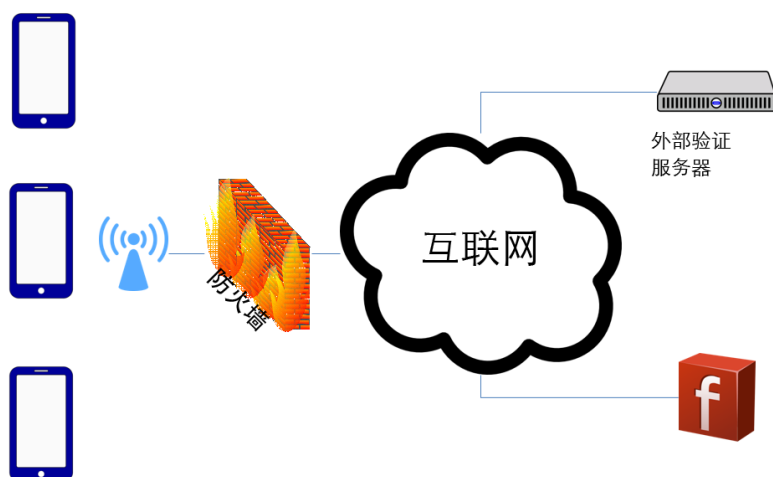
注：SuperMassive 9800 上不支持配置开放式授权、社交登录和 LHM。

- 第 619 页的[关于开放式验证和社交登录](#)
- 第 623 页的[关于轻量级热点消息 \(LHM\)](#)
- 第 624 页的[配置 Facebook 进行社交登录](#)
- 第 626 页的[配置开放式验证和社交登录](#)
- 第 628 页的[验证社交登录配置](#)
- 第 628 页的[使用社交登录、LHM 和 ABE](#)

关于开放式验证和社交登录

社交登录是一种单点登录验证形式，利用来自 Facebook、Twitter 或 Google+ 等社交网络服务的现有用户凭据来登录第三方网站，而不用专门为该网站创建新的登录帐户。开放式验证 (OAuth) 社交登录功能可以与使用通过验证的无线区域、LAN 区域或 DMZ 区域的访客服务结合使用；请参阅[外部验证服务器登录拓扑](#)。通过式验证是对驻留在受信任域中的域控制器执行验证的方法。无线访客服务广泛应用于为访客设置的公共 WiFi 热点和企业 WiFi 服务。

外部验证服务器登录拓扑



主题：

- 第 620 页的[什么是 OAuth 和社交登录？](#)
- 第 620 页的[OAuth 和社交登录的好处](#)
- 第 621 页的[OAuth 和社交登录如何工作？](#)
- 第 622 页的[支持的平台](#)

什么是 OAuth 和社交登录？

OAuth 是授权的开放标准。OAuth 授权客户端应用程序代表资源所有者“安全访问”服务器资源，并指定了资源所有者授权第三方访问其服务器资源而不用分享其凭据的过程。

社交登录也称为社交注册，是使用 Facebook、Twitter 或 Google+ 等社交网络服务的现有登录信息登录第三方网站的一种单点登录 (SSO) 形式，而不用专门为该网站创建新的登录帐户。

OAuth 和社交登录的好处

主题：

- [OAuth](#)
- [社交登录](#)

OAuth

OAuth 是一种受欢迎的机制，可帮助用户在应用程序之间共享数据。可以利用 OAuth 作为 Web 应用程序的登录提供程序。

其它优点

- 限制网上的客户配置文件
- 要跟踪的密码更少
- 不需要提交可能存在信任问题的密码
- 仍然可以阻止 OAuth 提供程序的访问
- 身份盗用的风险较低。由提供程序承担验证
- 使用先前验证的 API，通过验证降低故障风险
- 对数据服务器的存储需求减少

缺点

- 不能为自己的应用程序定制用户配置文件
- 用户在无现有帐户时通过 OAuth 提供程序创建帐户时会混淆

社交登录

社交登录旨在简化登录流程，并实现更高的注册转换率。

其它优点

- 快速注册
- 记住更少的登录信息
- 目标丰富的内容
- 使用多个身份
- 收集访客数据
- 详细或个性化的用户体验
- 熟悉的登录环境
- 登录失败更少
- 便于手机使用

缺点

- 低信任级别
- 排除非社交用户
- 可能伪造数据准确性
- 阻止来自社交网络的内容
- 安全问题

OAuth 和社交登录如何工作？

开放式验证 (OAuth) 和社交登录功能都可以与内部无线服务和作为无线区域访客服务的 SonicPoint 一起使用。访客可以使用公司的企业 WiFi 登录互联网。无线访客服务广泛应用于为访客设置的公共 WiFi 热点和企业 WiFi 服务。

OAuth 和社交登录都使用包含互联网访问的无线访客服务，并可配置为使用以下任一方法或两种连接方法：

- 第 621 页的[无重定向](#)
- 第 622 页的[重定向到登录页面](#)

无重定向

无重定向为访客提供开放式互联网访问权限，无需加密，因此访客可以自由连接到提供的 WiFi。

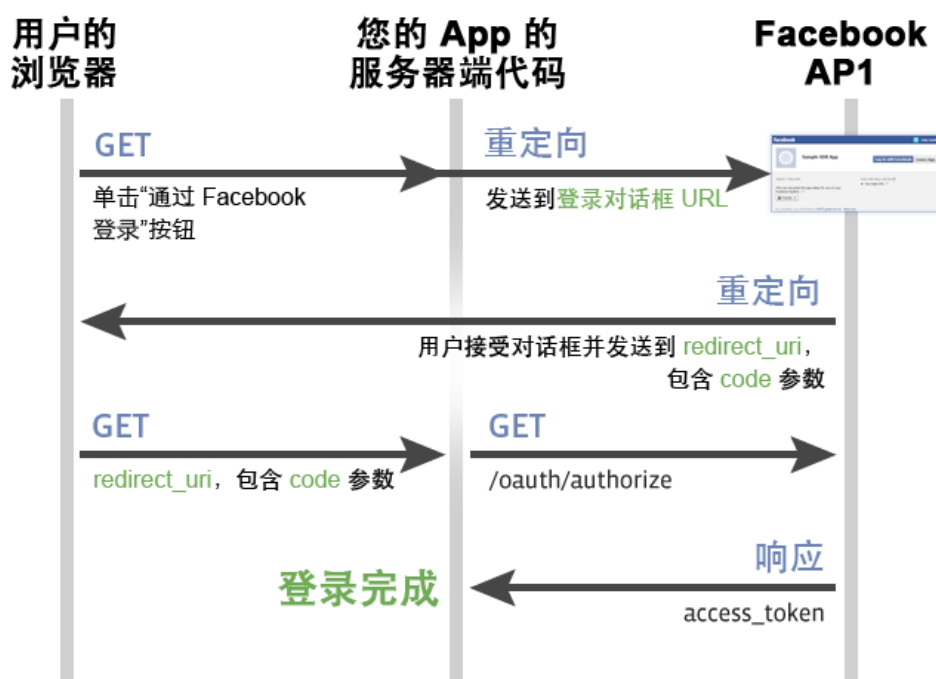
无重定向也可以提供 WPA/WEP 密码访问，访客需要密码才能使用可用的 WiFi。可以通过其他方式提供密码，例如在收据上。

重定向到登录页面

登录 Web 页面提供最广泛使用的热点访问。当第 2 层 WiFi 访问为开放时，访客在访问第一层时定向至登录 Web 页面；请参阅 [OAuth 流程](#)。其他一些重定向访问选项包括：

- 登录页面上无验证
- 访客可以创建新的登录帐户，然后使用它登录
- 访客可以使用通过短信发送至他们的手机、电子邮件或其他方式的代码来登录
- 使用移动应用扫描 QR 码
- 使用社交登录

OAuth 流程



支持的平台

在以下 SonicWall 防火墙上支持开放式验证和社交登录：

- 运行 SonicOS 6.2.7 及更高版本
- 在运行 GMS 8.3 的 GMS 管理下

开发和生产要求

- Facebook 帐户
 - 为开发人员启用 Facebook

- 外部服务器
 - 公共可访问
 - 拥有域名
 - PHP 支持
 - SSL 证书
- Sonicwall 防火墙
 - 外部服务器可以访问（通过 IP 或 FQDN）
 - 无线（内部或 SonicPoint）

关于轻量级热点消息 (LHM)

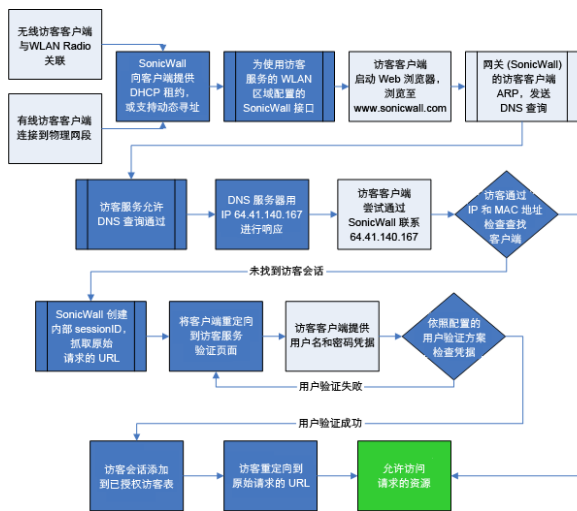
轻量级热点消息 (LHM) 利用 SonicWall 访客服务模式，其中可以通过 SonicWall 安全设备对用户进行分类和授权以实现差异化的网络访问。例如，可以配置 SonicWall，使任何通过属于启用访客服务的 WLAN（无线局域网）区域的接口连接的用户只能访问互联网（不受信任网络），但无法访问 LAN（受信任网络）。这允许单个防火墙为受信任和访客用户提供同时访问。

LHM 通过分离验证和授权过程来扩展访客服务模式，从而允许验证发生在 SonicWall 外部。这允许验证接口的广泛定制，还允许使用任何类型的可想象的验证方案。

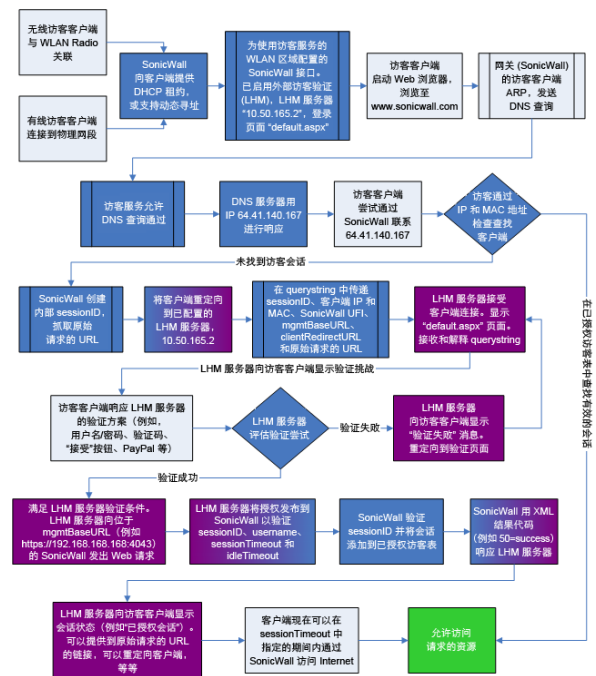
原始访客服务授权流程和 LHM 授权流程的并排视图显示在[授权流程比较表](#)中：

授权流程比较

原始访客服务授权流程

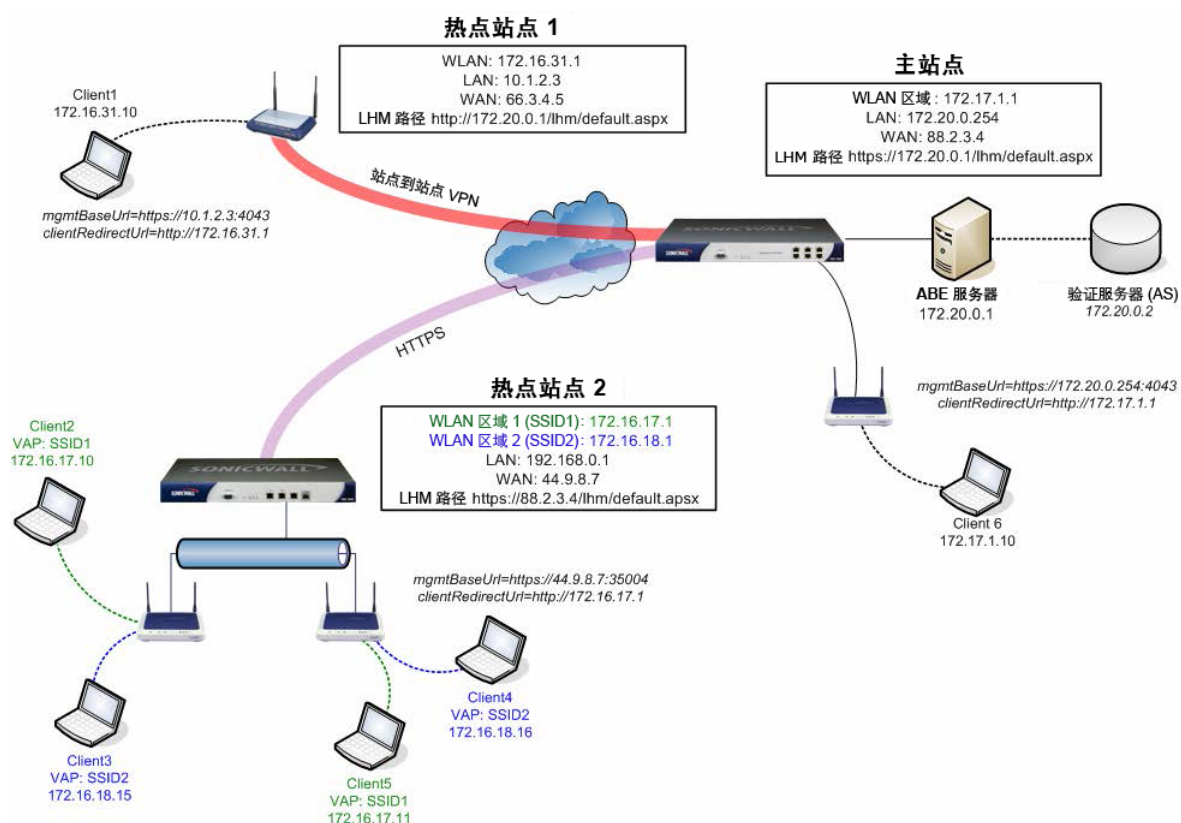


LHM 授权流程



LHM 定义了 SonicWall 无线接入设备（例如 SOHO W 防火墙、TZ 无线系列防火墙或拥有管理 SonicWall 安全设备的 SonicPoint）和用于验证热点用户并为其提供参数绑定的网络访问的验证后端 (ABE) 之间的通讯的方法和语法。[LHM 配置示例](#)描述了通用配置。

LHM 配置示例



LHM 通过提供 SonicWall 的无线访客服务和任何现有的 ABE 之间的接口，允许网络运营商提供对多个热点位置的集中管理。LHM 是广义 WISPr 和 GIS 规范的改编。

LHM 旨在满足特别常见的操作环境的要求，而非广泛的环境。具体来说，LHM 允许热点用户管理和验证完全发生在网络运营商的 ABE 上，支持任何帐户创建和管理方法，以及任何程度的站点定制和品牌设计。这种方法可集成到任何现有环境中而不依赖于特定的计费、会计或数据库系统，还为网络运营商提供了对站点设计（从外观到重定向）的无限制控制。

配置 Facebook 进行社交登录

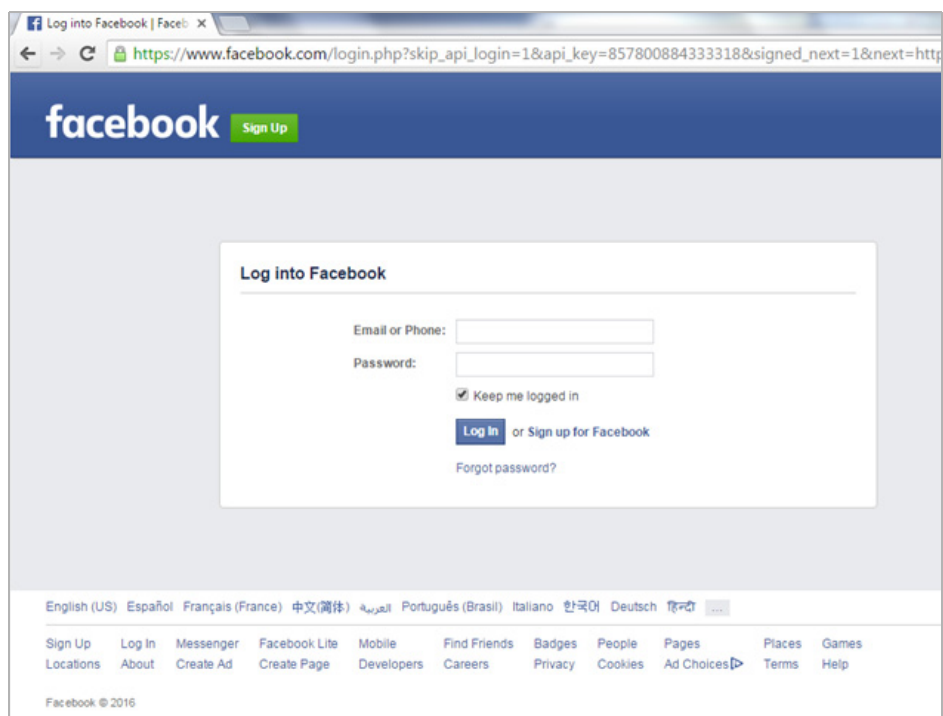
主题：

- 第 625 页的 [Facebook 设置](#)
- 第 626 页的 [客户端 OAuth 设置](#)
- 第 626 页的 [访客状态（演示）](#)

Facebook 设置

登录开发人员 Facebook 的步骤如下：

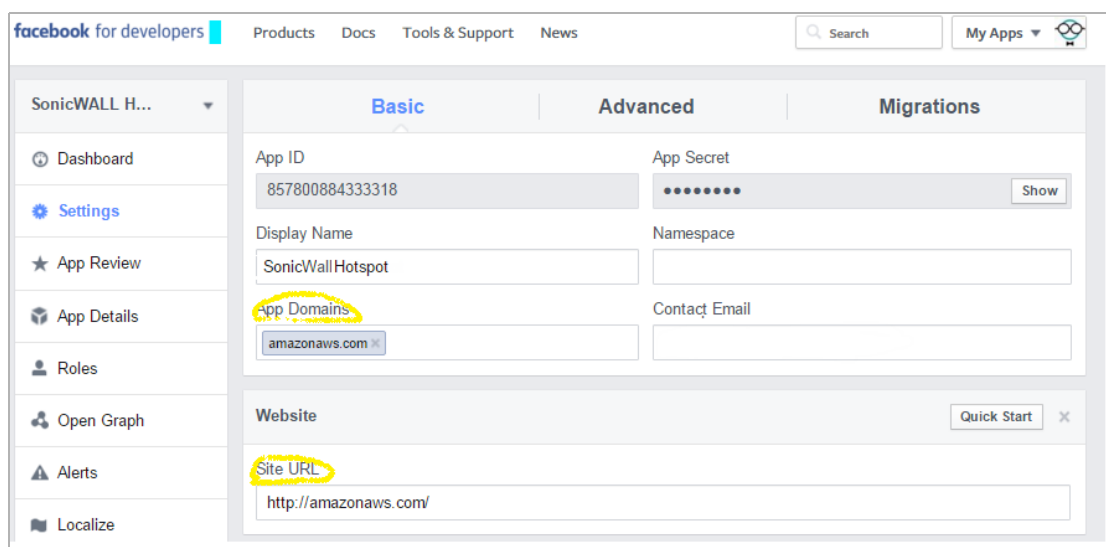
- 1 打开 Web 浏览器
- 2 登录开发人员 Facebook 帐户：<https://developers.facebook.com/>。



- 3 完成登录流程或注册新的开发人员帐户。
- 4 单击左栏中的设置。

请参阅[开发人员 Facebook 设置示例](#)填写表单，但调整 Facebook 设置以用于您的 LHM 服务器。

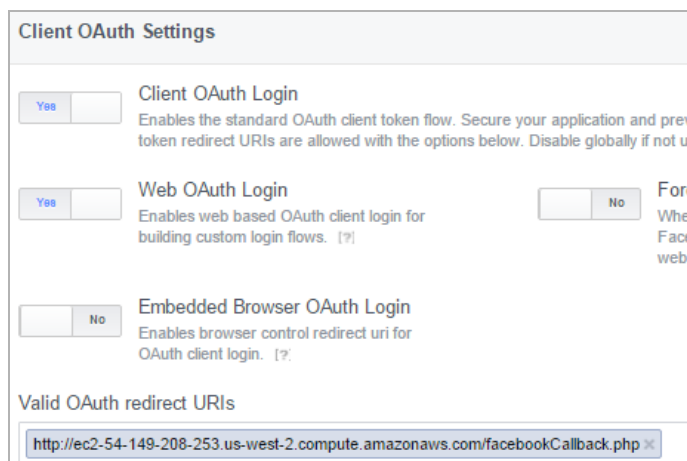
开发人员 Facebook 设置示例



客户端 OAuth 设置

应该在开发人员 Facebook 上调整客户端 OAuth 设置：<https://developers.facebook.com/>（产品 > Facebook 登录 > 设置），类似 [OAuth Facebook 设置示例](#) 中所示。

OAuth Facebook 设置示例



访客状态（演示）

当无线客户端允许访问 SonicWall WiFi 时，所有者的帐户名称和信息将发送到 SonicOS。可以将这些信息收集并存储在自己的数据库中。

配置开放式验证和社交登录

主题：

- 第 626 页的[关于配置访客服务](#)
- 第 626 页的[关于配置社交登录](#)
- 第 627 页的[在 SonicOS 中配置社交登录](#)

关于配置访客服务

虽然 SonicOS 提供自己的访客帐户管理，但您可以使用自己的 IT 基础架构来更好地满足业务需求。此配置可以通过设置外部访客验证或社交登录来完成。在 SonicOS 无线区域、LAN 区域或 DMZ 区域（[管理 | 系统设置 | 网络 | 区域](#)）的添加/编辑区域对话框中提供访客服务。

关于配置社交登录

此功能可简化最终用户的繁琐登录，并为 Web 开发人员提供可靠的人口统计信息。

准备配置社交登录的步骤如下：

- 1 按照第 333 页的[添加新区域](#)中所述创建无线区域、LAN 区域或 DMZ 区域，并设置或编辑拥有安全功能的网络区域。
- 2 在 SonicOS 中，外部服务器也可以创建或选择为轻量级热点消息 (LHM) 服务器 IP 或 FQDN 地址对象。

在 SonicOS 中配置社交登录

正确设置安全设备需要进行一些配置。安全设备阻止大多数 Internet 应用程序，但应该允许若干应用程序以使这个功能正常运行。

❗ | 重要： 在配置社交登录之前，LHM 服务器应该处于服务状态。

配置安全设备进行社交登录的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 区域**以设置或编辑拥有无线安全功能的网络区域。如需添加网络区域的更多信息，请参阅第 333 页的[添加新区域](#)。

❗ | 注： 外部服务器也可以创建或选择为轻量级热点消息 (LHM) 服务器 IP 或 FQDN 地址对象。

- 2 单击 **WLAN 编辑** 图标以访问 WLAN 网络区域。将显示 **编辑区域** 对话框。
- 3 单击 **访客服务**。
- 4 选择 **启用访客服务**。其他选项将激活。
- 5 选中 **启用外部访客验证**。配置将激活。
- 6 单击 **配置**。将显示 **外部访客验证** 对话框。
- 7 对于 **外部 Web 服务器** 设置，应该已经在使用 LHM 服务器。从主机中选择与该服务器关联的地址对象。
- 8 按照第 335 页的[配置访客访问的区域](#)中的描述配置其余选项。
- 9 在 **社交网络登录** 部分中，选中 **启用社交网络登录**。社交网络激活。
- 10 选择一个或多个社交网络以启用开放式验证：

- **Facebook**
- **Google**
- **Twitter**

SonicOS 自动创建必需的通过验证网络域，以允许验证服务器和用户之间的验证流程流量。自动添加的地址对象群组名为 **默认社交登录通行群组**。此地址对象群组附加到当前配置的通过网络（如果存在）或名为 **社交登录通行群组** 的新群组中。

- 11 单击 **验证页面** 选项卡。
- 12 输入 **登录页面** 的位置，例如 `login.php`，但是基于开发人员的输入页面。这些脚本由您自己的 LHM 服务器托管，因此您应该能确保它们正常运行。
- 13 填写剩余的字段。
- 14 单击 **确定**。

验证社交登录配置

可以通过查看[管理 | 策略 | 对象](#)来验证“开放式验证和社交登录”的正确配置。如需对象的更多信息，请参阅 SonicOS 策略。

验证设置的步骤如下：

- 1 转至[管理 | 策略 | 对象 | 地址对象](#)。
- 2 选择地址群组，这应显示：
 - 已自动添加域。
 - Facebook、Google 和/或 Twitter 登录流量可以成功通过。

使用社交登录、LHM 和 ABE

主题：

- [第 628 页的关于 ABE](#)
- [第 629 页的会话生命周期](#)
- [第 635 页的消息格式](#)
- [第 642 页的常见问题解答 \(FAQ\)](#)
- [第 648 页的 LHM 脚本库](#)

关于 ABE

ABE 由用于托管用户交互的主机内容的 Web 服务器 (WS) 和用于提供目录服务验证的（可选的）验证服务器 (AS) 组成。AS 可以是任何类型的用户验证机制，包括但不限于 RADIUS、LDAP 或 AD；唯一的要求是 WS 可以与 AS 通讯以进行验证。WS 和 AS 可以在单个服务器上或不同的服务器上进行管理。

LHM 还提供了 AS 使用 SonicWall 安全设备的内部用户数据库进行用户验证的能力。如需消息传送的详细信息，请参阅[第 635 页的消息格式](#)、[第 637 页的本地验证请求](#)和[第 637 页的本地验证回复](#)。

ABE 需要与热点 SonicWall 进行通讯，以交换结果代码和会话信息。所有通讯都是 HTTPS，可以直接发生（例如，到 SonicWall 安全设备的 LAN、WAN、X0 接口）或通过 VPN 隧道发送到 SonicWall 安全设备的管理接口地址之一。LHM 管理接口通过路由（路径）查找自动导出，只有管理接口通过自动添加的访问规则接受 LHM 管理消息传递。

LHM 通讯发生在必须在 SonicWall 安全设备上定义的特定 LHM 管理端口上，LHM 管理端口必须与标准 HTTPS 管理端口不同。

为了允许 ABE 与 SonicWall 通讯，并将客户端重定向到 SonicWall 上的相应接口，两个参数由 SonicWall 构建，并通过客户端重定向到 ABE。对于 ABE 和 SonicWall 之间的所有通讯，必须使用以下通讯参数。

- `mgmtBaseUrl`—ABE 用于与 SonicWall 通讯的 IP 地址和端口。它由 HTTPS 协议指示符、所选 LHM 管理接口的 IP 和 LHM 端口（例如 `https://10.1.2.3:4043`）组成。
- `clientRedirectUrl`—在会话的各个阶段，客户端被重定向到的 SonicWall 上的 IP 地址（和可选的端口），即 TZW 上的 LAN 管理 IP，或 SonicOS 设备上的 WLAN IP（例如 `http://172.16.31.1`）。

在会话创建（请参阅第 629 页的[会话创建](#)）期间和会话状态同步（请参阅第 635 页的[消息格式](#)）期间，参数值通过 SonicWall 传递给 ABE，并应该为 ABE 用作构建所有相关 URL 的基础。以下是由 ABE 引用的 SonicWall 安全设备上的页面：

- wirelessServicesUnavailable.html—ABE 不可用的消息。此重定向通常由 SonicWall 发送，但也可以由 ABE 引用。文本是可配置的。
- externalGuestRedirect.html— SonicWall 在会话创建时提供的初始重定向消息。文本是可配置的。
- externalGuestLogin.cgi—ABE 发布会话创建数据的页面。
- externalGuestLogout.cgi—ABE 发布会话终止数据的页面。
- localGuestLogin.cgi —ABE 发布的用于根据 SonicWall 的内部用户数据库验证用户凭据的页面。
- createGuestAccount.cgi—ABE 发布的在 SonicWall 的内部用户数据库中创建访客帐户的页面。
- externalGuestUpdateSession.cgi—ABE 发布的更新现有会话的 *sessionLifetime* 和 *idleTimeout* 参数的页面（请参阅第 635 页的[会话更新](#)）。

对于从 SonicWall 到 ABE 的通讯，ABE 上托管的 URL（包括主机、端口和页面/资源）在 SonicWall 安全设备中完全可配置。可以使用 IP 地址或完全限定域名 (FQDN) 来指定主机。使用 FQDN 时，在首次使用时解析名称，并由 SonicWall 存储为 IP 地址。

会话生命周期

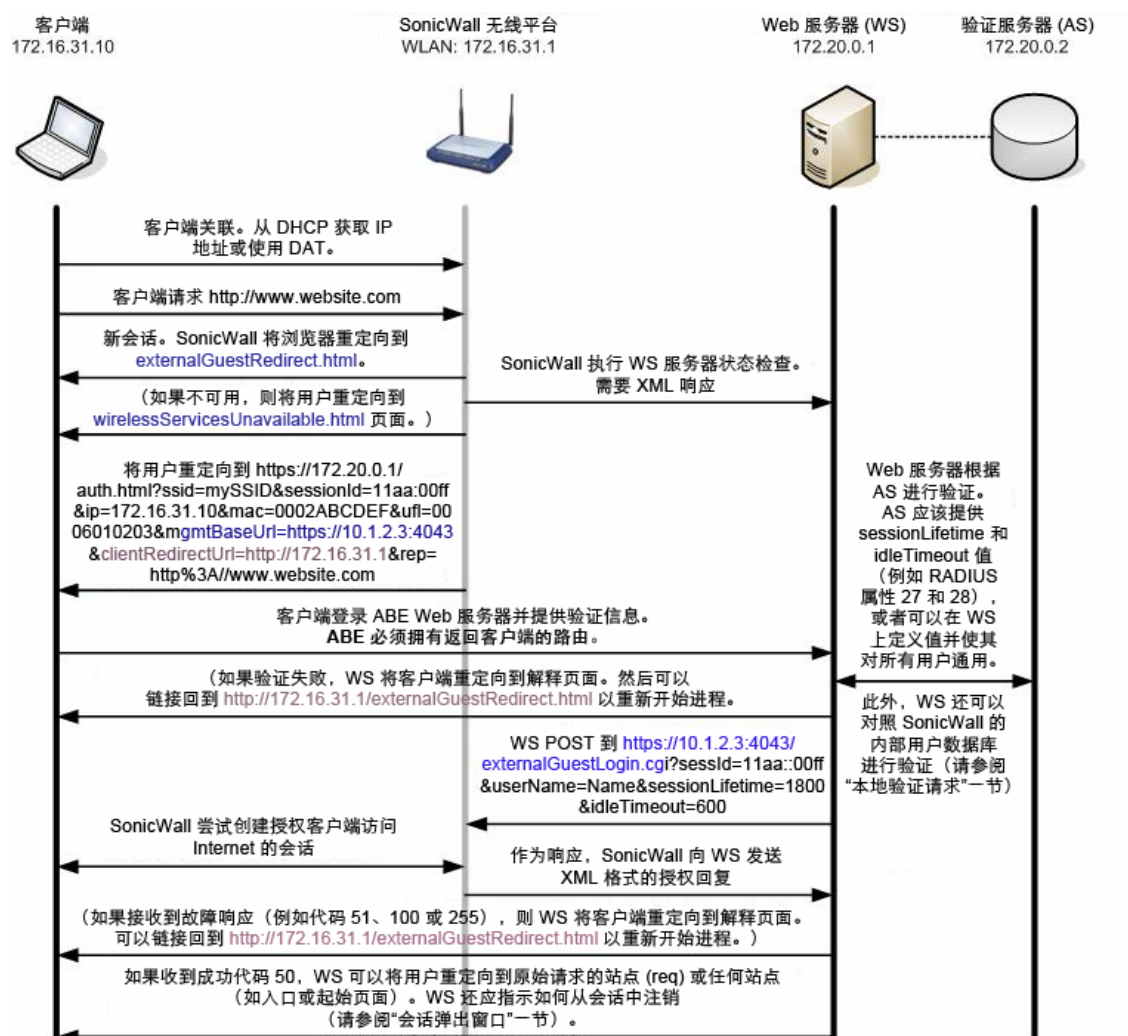
以下部分描述会话生命周期的阶段，以及会话弹出窗口和 Web 服务器 (WS) 状态检查组件：

- 第 629 页的[会话创建](#)
- 第 631 页的[会话弹出窗口](#)
- 第 632 页的[闲置超时](#)
- 第 632 页的[会话超时](#)
- 第 632 页的[用户注销](#)
- 第 633 页的[管理员注销（可选）](#)
- 第 634 页的[Web 服务器状态检查](#)
- 第 634 页的[会话状态同步](#)
- 第 635 页的[消息验证](#)
- 第 635 页的[会话更新](#)

会话创建

会话创建发生在无线客户端尝试访问时且 SonicWall 安全设备根据 MAC 地址未提供该客户端的活动会话信息。

会话创建流程



- 无线客户端与 SonicWall 关联。从内部 DHCP 服务器获取 IP 地址或使用动态地址转换 (DAT) 功能的静态寻址。
- 客户端请求 Web 资源, `http://www.website.com`。
 - SonicWall 安全设备确定这是新会话。
- SonicWall 安全设备将客户端重定向到内部托管的 `externalGuestRedirect.html` 页面。`externalGuestRedirect.html` 页面提供管理员可配置的文本, 说明会话被重定向以进行验证。
- 在此重定向期间, 安全设备通过对配置的目标重定向页面的 JavaScript 重定向尝试来检查 ABE 的可用性。
 - 如果在指定时间段 (该值在 SonicWall 上可配置, 在 1 到 30 秒之间) 内重定向到 WS 失败, 则安全设备将会话重定向到内部 `wirelessServicesUnavailable.html` 页面。
- 除了 JavaScript 可用性检查之外, 还可以从 SonicWall 进行可选的完整 Web 服务器状态检查 (请参阅第 634 页的 **Web 服务器状态检查**)。此选项可以配置为以 1 到 60 分钟之间的可配置间隔运行。如果错误响应代码为 1、2 或 255, 则安全设备会记录响应并将浏览器重定向到内部 `wirelessServicesUnavailable.html` 页面。该页面提供管理员可配置的文本解释资源。
- 如果可用, 安全设备将客户端重定向到 AS 上托管的验证入口:
`https://172.20.0.1/auth.html?ssid=mySSID&sessionId=11aa::00ff&ip=172.1`

6.31.10&mac=0002ABCDEF&ufi=0006010203&mgmtBaseUrl=https://10.1.2.3:4043&clientRedirectUrl=http://172.16.31.1&req=http%3A//www.website.com

- ssid—与重定向客户端相关联的无线网络的 ESSID（无线网络名称）。
- sessionId—由 SonicWall 生成的 16 字节 MD5 哈希值的 32 字节十六进制表示，SonicWall 和 WS 用于索引客户端（例如“11aa3e2f5da3e12ef978ba120d2300ff”）。
- ip—客户端 IP 地址。
- mac—客户端 MAC 地址。
- req—原始请求的网站作为参数传递给验证服务器
- ufi—SonicWall 唯一的防火墙标识符。根据需要，用于站点识别。
- mgmtBaseUrl—随后 IP 通讯的 SonicWall 上的协议、IP 地址和端口。
- clientRedirectUrl—ABE 用于客户端重定向的 SonicWall 上的协议、IP 地址（和可选端口）。
- req—客户端原始请求的 URL、已编码的 URL（如果有）。

7 客户端提供验证信息（如用户名、密码、令牌等）。

 **注：**WS 必须能通过 VPN、NAT 或路由到达客户端。

8 WS 根据 AS 验证用户。

- AS 提供会话特定信息，即会话超时和闲置超时值。
- 会话特定值可以可选地由 WS 在全局应用，而非从 AS 获得；一些值只需要传递给安全设备。
- 超时值以秒为单位显示，范围为 1 到 863,913,600（等于 9999 天）。

9 如果验证失败，则 WS 应将客户端重定向到解释故障的页面。应提供链接回到 `http(s)://172.16.31.1/externalGuestRedirect.html` 以重新启动该流程。

10 如果成功，WS 通过 HTTPS 或通过 VPN 和 POST 连接到安全设备 `https://10.1.2.3:4043/externalGuestLogin.cgi?sessId=11aa::00ff&userName=Name&sessionLifetime=1800&idleTimeout=600`。

- 安全设备尝试创建会话并将结果发送到同一连接中的 WS。结果在第 635 页的消息格式中描述。

11 如果接收到故障响应（例如代码 51、100 或 255），则 WS 应将客户端重定向到解释故障的页面。可以提供链接回到 `http(s)://172.16.31.1/externalGuestRedirect.html` 以重新开始进程。

12 如果成功（代码 50），WS 可以将用户重定向到原始请求的站点 (req) 或任何站点（如入口或起始页面）。WS 还应指示如何从会话中注销（如书签页面、弹出窗口、URL）。

会话弹出窗口

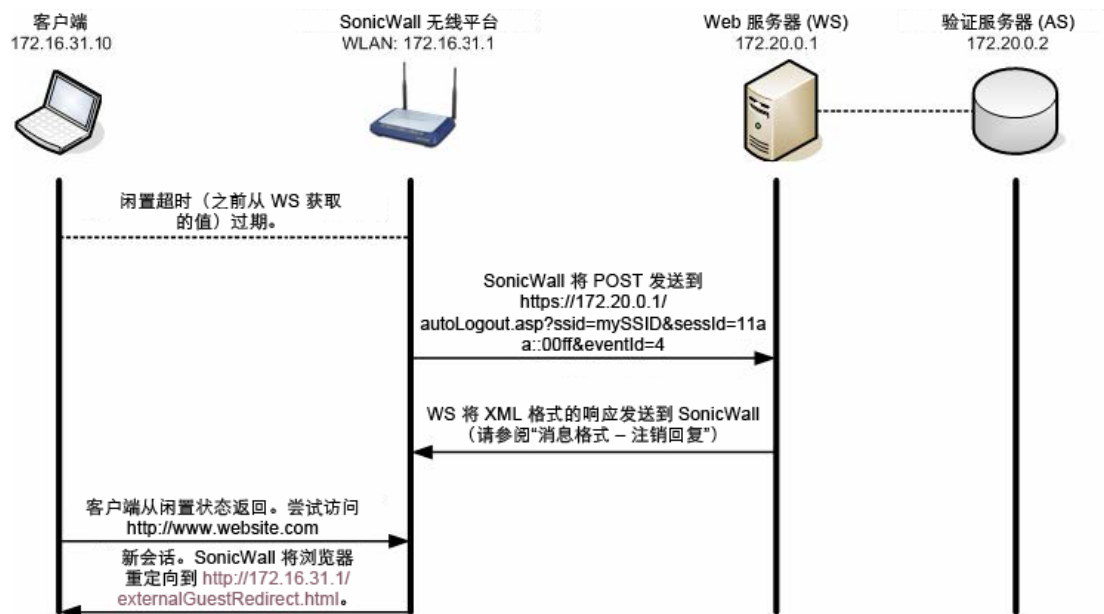
推荐通过会话弹出窗口管理会话。这应该是在会话创建时实例化的浏览器窗口，提供会话时间信息（如生命周期、闲置超时值、计时器倒计时）和“注销”按钮。提供示例代码。

- 单击**注销**可结束会话并触发用户注销事件。
- 尝试关闭窗口应该提供警告消息，指示关闭窗口将会结束会话。
- 关闭窗口可结束会话并触发用户注销事件。

闲置超时

当超出闲置超时（在第 629 页的[会话创建步骤 8](#) 中指定）时，会发生闲置超时。

闲置超时流程



- 1 闲置计时器（在第 629 页的[会话创建](#)期间设置）过期。
- 2 由于客户端的浏览器此时可能未打开，因此我们不会通过重定向启动此流程。相反，SonicWall 发送 POST 到 WS：
`https://172.20.0.1/autoLogout.asp?ssid=mySSID&sessId=11aa::00ff&eventId=4`（如需注销事件 ID，请参阅第 635 页的[消息格式](#)）。
 - POST 发送到的资源可以在管理 | 系统设置 | 网络 | 区域中配置：编辑 WLAN 区域（在编辑区域对话框中：访客服务 > 外部访客身份验证 > 高级 > 自动会话退出 > 退出 CGI。
 - WS 托管页面必须提供并解释 `sessId` 和 `eventId` 值。
- 3 WS 将 XML 结果发送到同一连接中的 WS。结果在第 638 页的[注销回复](#)中描述。
- 4 如果客户端从闲置状态返回并尝试访问 Web 资源，则安全设备将用户重定向到内部 `externalGuestRedirect.html` 页面，重新开始会话创建流程（请参阅第 629 页的[会话创建](#)）。

① | 注：为了节省资源，推荐将闲置超时设置为最多 10 分钟。

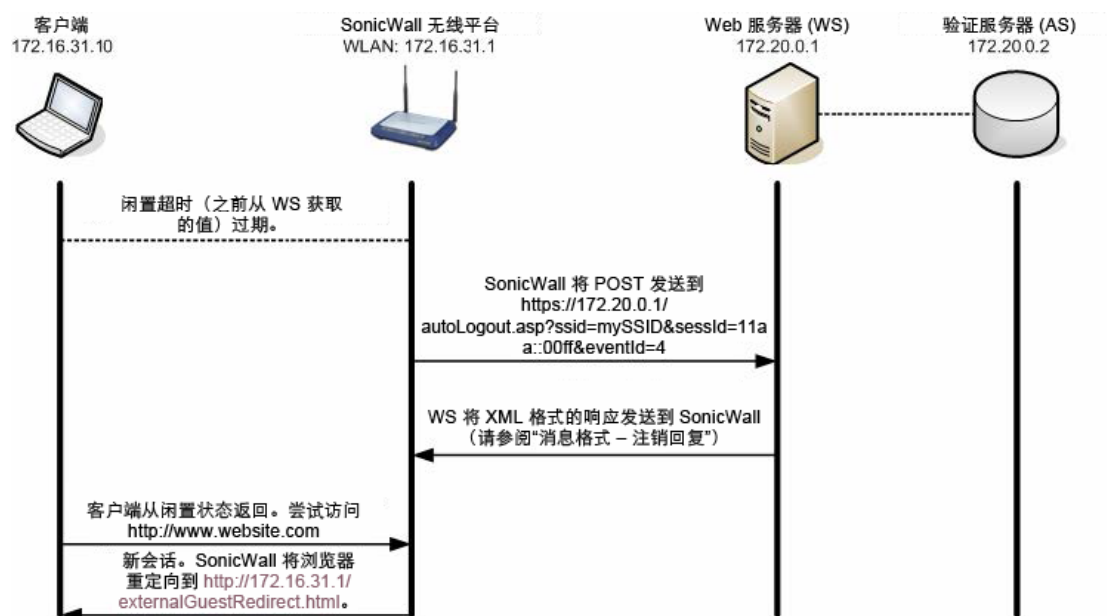
会话超时

事件发生在会话生命周期到期时。交换与上面的闲置超时相同，除了闲置超时的会话超时 `eventId` 值为 3 而非 4。

用户注销

当用户通过关闭其“会话弹出”窗口或使用“会话弹出”窗口中提供的“注销”按钮来主动结束会话时，会发生此事件。“会话弹出”窗口是用户注销的首选方法；然而，通过允许会话的生命周期到期，可以不使用此方法而实现相同的结果。可以消除对“会话弹出”窗口的依赖，但是管理资源效率较低。

用户注销流程

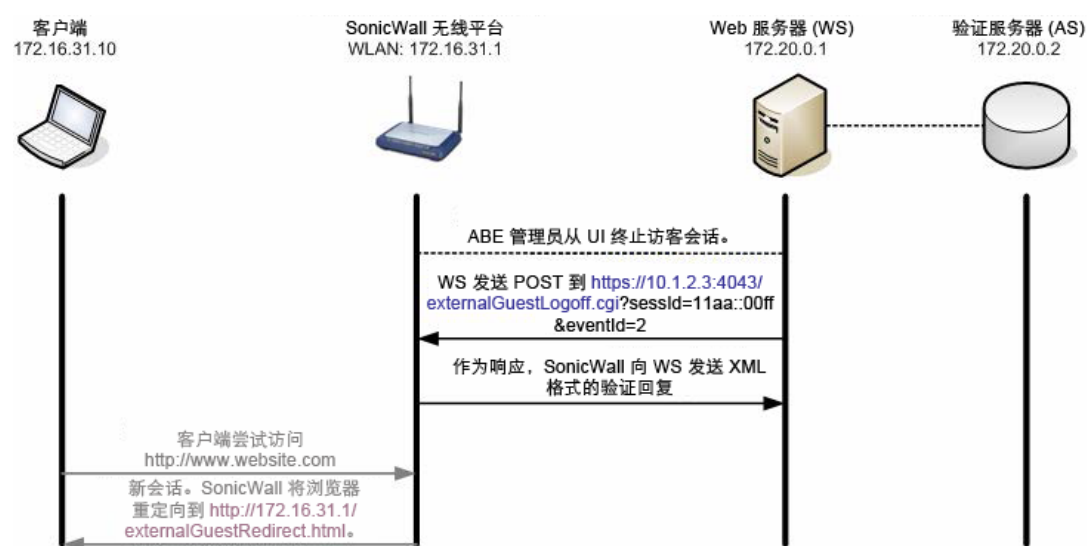


- 1 客户端使用“注销”按钮注销或关闭会话弹出窗口。
- 2 WS 发送 POST 到：
`https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=1`（如需注销事件 ID，请参阅第 635 页的消息格式）。
 - `sessId`—会话创建（请参阅第 629 页的会话创建）期间由安全设备生成的值，由安全设备和 WS 用于索引客户端。
 - `eventId`—描述注销请求事件。
- 3 SonicWall 安全设备通过将结果发送到同一连接中的 WS 进行响应。结果在第 638 页的注销回复中描述。
- 4 如果客户端尝试访问 Web 资源，则安全设备将用户重定向到内部 `http://172.16.31.1/externalGuestRedirect.html` 页面，重新开始会话创建流程（请参阅第 629 页的会话创建）。

管理员注销（可选）

当 ABE 管理员从管理界面从“访客”会话中注销时，会发生该事件。目前无法从 SonicOS 管理界面自身终止 ABE 建立的访客会话。ABE 建立的访客会话以此方式显示在 SonicOS 管理界面上（或不同于内部 WGS 访客会话）且不可编辑。

管理员注销流程



- 1 ABE 管理员从管理界面终止访客会话。
- 2 WS 发送 POST 到安全设备：
`https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=2`。（如需注销事件 ID，请参阅第 635 页的消息格式）。
 - sessId—会话创建期间由安全设备生成的值，由安全设备和 WS 用于索引客户端。
 - eventId—描述注销请求事件。
- 3 SonicWall 将结果发送到同一连接中的 WS。结果在第 638 页的注销回复中描述。
- 4 如果客户端从闲置状态返回并尝试访问 Web 资源，则安全设备将用户重定向到内部 `http://172.16.31.1/externalGuestRedirect.html` 页面，重新开始会话创建流程（请参阅第 629 页的会话创建）。

Web 服务器状态检查

为了提供比简单的 Web 服务器 (WS) 可用性更精确的 ABE 状态（如同第 630 页的会话创建流程的强制步骤 4 提供的 JavaScript 重定向），SonicWall 可以可选地向 WS 发送安全的 HTTP GET 操作以确定服务器的运行状态。目标 URL 是可配置的，如同查询的间隔时间（1 到 60 分钟）。WS 以列出服务器当前状态的 XML 格式做出响应。如需详细信息，请参阅第 635 页的消息格式。

如果接收到错误响应代码（1、2 或 255）（指示 WS 本身可用，但发生了一些 ABE 错误状况），则 SonicWall 将记录响应并将所有后续验证请求重定向到内部 `wirelessServicesUnavailable.html` 页面。该页面提供管理员可配置的文本解释资源。

当接收到响应代码为 0（服务器正常运行）时，安全设备将继续尝试以配置的时间间隔查询 ABE，并恢复重定向到 WS（而非到 `wirelessServicesUnavailable.html` 页面）。

会话状态同步

以可配置的时间间隔（1 到 60 分钟之间），安全设备可选地向包含所有当前活动的访客会话的 XML 列表的 WS 发送安全 HTTP POST 操作。CGI POST 将 `sessionList` 作为所有活动的访客会话的 XML 列表。如需详细信息，请参阅第 635 页的消息格式。

功能本身通过安全设备上的复选框启用，但默认情况下禁用。目标 URL 是可配置的。

消息验证

此功能确保了安全设备和 ABE 之间交换的 CGI 数据源自 SonicWall 安全设备/ABE 设备且未篡改。如果启用，则会将另外的 CGI 参数（名为 hmac）添加到所有交换的 CGI 数据中。以下是启用消息验证的重定向 URL 的示例：

```
https://10.1.2.3/login.asp?sessionId=faad7f12ac26d5c2fe3236de2c149a22&ip=172.16.31.2&mac=00:90:4b:6a:37:32&ufi=0006B1020148&mgmtBaseUrl=https://10.0.61.222:4043/&clientRedirectUrl=http://192.168.168.168:80/&req=http%3A//www.google.com/&hmac=cd2399aeff26d5c2fe3236d211549acc
```

注：SonicWall 安全设备 URL 会对 req（且只有 req）变量的值中的以下字符编码：

```
% = %25
: = %3A
= = %20（空格）
? = %3F
+ = %2B
& = %26
= = %3D
```

在上述示例中，使用以下数据生成 HMAC 签名：

```
HMAC (
  faad7f12ac26d5c2fe3236de2c149a22 +
  172.16.31.2 +
  00:90:4b:6a:37:32 +
  0006B1020148 +
  https://10.0.61.222:4043/ +
  https://10.0.61.222:4043/ +
  http%3A//www.google.com/
)
```

如果启用了消息验证，则 SonicWall 设备希望将 HMAC 签名作为源自 ABE 的 CGI POST 数据的一部分。如果 SonicWall 检测到 HMAC 丢失或不正确，则返回错误代码 251 并中止所请求的操作（如访客登录，帐户创建）。

会话更新

会话更新允许 ABE 更新安全设备上现有会话的会话生命周期和闲置超时值。这允许例如由访客用户购买额外的时间并添加到现有会话中。

- 会话更新可以在会话生命周期的任何时间从 ABE 发送到 SonicWall。
- 必须在消息中指定 `userName` 和 `sessionLifetime` 值
- 可以指定 `sessID` 值。如果包含，则更新属于指定的会话。如果省略，则更新属于与指定的 `userName` 匹配的所有会话。

如需详细信息，请参阅第 635 页的[消息格式](#)。

消息格式

主题：

- 第 636 页的[外部验证请求](#)
- 第 637 页的[本地验证请求](#)

- 第 637 页的本地验证请求
- 第 637 页的本地验证回复
- 第 638 页的注销请求
- 第 638 页的注销回复
- 第 634 页的 Web 服务器状态检查
- 第 634 页的会话状态同步
- 第 640 页的会话状态同步回复
- 第 640 页的本地帐户创建请求
- 第 640 页的本地帐户创建回复
- 第 641 页的更新会话请求
- 第 641 页的更新会话回复

注：XML 架构位置可能会更改。
SonicWall 安全设备 IP 地址和端口在 mgmtBaseUrl 变量中定义。

外部验证请求

WS 将安全的 HTTP POST 操作发送至：

https://sonicwall.ip.add.ress:port/externalGuestLogin.cgi。POST 参数包括以下参数：

- sessId: 会话 ID
- userName: 完整的用户 ID
- sessionLifetime: 用户的会话生命周期（以秒为单位）
- idleTimeout: 最大闲置超时（秒）

外部验证回复

安全设备以下列格式返回 XML 响应：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <AuthenticationReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

{response code} 包含外部验证响应代码表中列出的值之一。

外部验证响应代码

响应代码	响应含义
50	登录成功
51	超出会话限制

外部验证响应代码

响应代码	响应含义
100	登录失败 — 访问拒绝
251	消息验证失败 — HMAC 无效
253	会话 ID 无效
254	CGI 参数无效或缺失
255	内部错误

本地验证请求

WS 将安全的 HTTP POST 操作发送至：

`https://sonicwall.ip.add.ress:port/localGuestLogin.cgi`。POST 参数包括以下参数：

- `sessId`：会话 ID
- `userName`：完整的用户 ID
- `passwd`：访客的明文密码

本地验证回复

SonicWall 以下列格式返回 XML 响应：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <AuthenticationReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

{response code} 包含 [本地验证响应代码](#)表中列出的值之一。

本地验证响应代码

响应代码	响应含义
50	登录成功
51	超出会话限制
52	用户名/密码无效
100	登录失败 — 访问拒绝
251	消息验证失败 — HMAC 无效
253	会话 ID 无效
254	CGI 参数无效或缺失
255	内部错误

注销请求

WS 将安全的 HTTP POST 操作发送至:

https://sonicwall.ip.add.ress:port/externalGuestLogoff.cgi。POST 参数包括以下参数:

- sessId: GW 会话 ID
- eventId: 注销事件 ID。必须是以下之一:

注销事件 ID	事件含义
1	访客手动注销
2	管理员注销指定的访客
3	访客会话已过期
4	访客闲置超时已过期

注销回复

安全设备以下列格式返回 XML 响应:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <LogoffReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </LogoffReply>
</SonicWallAccessGatewayParam>
```

{response code} 包含 [注销响应代码](#) 表中列出的值之一。

注销响应代码

响应代码	响应含义
150	注销成功
251	消息验证失败 — HMAC 无效
253	会话 ID 无效
254	CGI 参数无效或缺失
255	内部错误

Web 服务器状态检查

WS 以下列格式返回 XML 响应:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <ServerStatus >{status code}</ ServerStatus >
</SonicWallAccessGatewayParam>
```

{response code} 包含 **Web 服务器状态检查响应代码**表中列出的值之一。

Web 服务器状态检查响应代码

响应代码	响应含义
0	服务器正常运行
1	数据库故障
2	配置错误
255	内部错误

会话状态同步

GW 定期向包含所有当前活动访客会话的 XML 列表的 AS 发送安全的 HTTP POST 操作。目标 URL 和时间段均由 GW 管理员配置。

CGI POST 参数包括以下参数：

- sessionList: 所有活动 GW 访客会话的 XML 列表。

该会话列表以以下格式返回 XML 响应：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <SessionSync>
    <SessionCount>{Session Count}</SessionCount>
    <SessionList>
      <Session>
        <Ssid>{ESSID}</Ssid>
        <ID>{Session ID}</ID>
        <UserName>{User Name}</UserName>
        <IP>{IP Address}</IP>
        <MAC>{MAC Address}</MAC>
        <Idle>
          {Time Idle (expressed in seconds)}
        </Idle>
        <SessionRemaining>
          {Session Remaining (expressed in seconds)}
        <SessionRemaining>
        <BaseMgmtUrl>
          {https://ip.add.re.ss:port}
        </BaseMgmtUrl>
        <RxBytes>
          {total bytes received}
        </RxBytes>
        <TxBytes>
          {total bytes transmitted}
        </TxBytes>
      </Session>
    </SessionList>
  </SessionSync>
</SonicWallAccessGatewayParam>
```

会话状态同步回复

WS 以下列格式返回 XML 响应:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <SessionSync>
    <ResponseCode>{response code}</ResponseCode>
  </SessionSync>
</SonicWallAccessGatewayParam>
```

{response code} 包含 [会话状态同步回复响应代码表](#) 中列出的值之一。

会话状态同步回复响应代码

响应代码	响应含义
200	同步成功
201	同步失败
255	内部错误

本地帐户创建请求

WS 将安全的 HTTP POST 操作发送至:

<https://sonicwall.ip.add.ress:port/createGuestAccount.cgi>。POST 参数包括以下参数:

- **userName**: 完整的用户 ID (最大长度: 32)
- **passwd**: 访客的明文密码 (最大长度: 64)
- **comment**: 可选 (最大长度: 16)。默认值 = **NULL**
- **enforceUniqueLogin**: 可选: 1=true, 0=false。Default=1
- **activateNow**: 可选: 1=true, 0=false。Default=0
- **autoPrune**: 可选: 1=true, 0=false。Default=1
- **accountLifetime**: 用户的帐户生命周期 (以秒为单位)
- **sessionLifetime**: 用户的会话生命周期 (以秒为单位)
- **idleTimeout**: 最大闲置超时 (以秒为单位)

本地帐户创建回复

安全设备以下列格式返回 XML 响应:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <AccountCreationReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
```



```
</AccountCreationReply>
</SonicWallAccessGatewayParam>
```

{response code} 包含 **本地帐户创建回复响应代码**表中列出的值之一。

本地帐户创建回复响应代码

响应代码	响应含义
10	帐户创建成功
11	最大帐户限制
12	帐户已存在
251	消息验证失败 — HMAC 无效
254	CGI 参数无效或缺失
255	内部错误

更新会话请求

来自 ABE 的 POST 可以以下列格式发送到安全设备的 externalGuestUpdateSession.cgi:

```
https://10.1.2.3:4043/externalGuestUpdateSession.cgi?sessId=11aa::00ff&userName=guest&sessionLifetime=600&idleTimeout=180
```

POST 参数包括以下参数:

- **sessID:** 可以指定该值。如果未指定该值,则会更新与指定用户名匹配的所有访客会话。
- **userName:** 必须指定该值,因为它定义了更新的用户会话的名称(或潜在的会话,如果未提供会话 ID)。
- **sessionLifetime:** 必须指定该值,因为它定义了分配给会话的秒数。可以是 1 到 863,913,600 之间的任何数字。
- **idleTimeout:** 可以指定该值。它:
 - 定义分配给会话的秒数。
 - 可以是 1 到 863,913,600 之间的任何数字。
 - 必须小于或等于 sessionLifetime。

如果未提供 idleTimeout,则会保留会话的现有 idleTimeout 值。

更新会话回复

安全设备以下列格式返回 XML 响应:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWallAccessGatewayParam.xsd">
  <UpdateSessionReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </ UpdateSessionReply >
</SonicWallAccessGatewayParam>
```

{response code} 包含 **更新会话回复响应代码**表中列出的值之一。

更新会话回复响应代码

响应代码	响应含义
210	会话更新成功
211	会话更新失败
251	消息验证失败 — HMAC 无效
254	CGI 参数无效或缺失
255	内部错误

常见问题解答 (FAQ)

主题:

- 第 642 页的 LHM 服务器脚本是否必须在 ASP 中编写?
- 第 642 页的为什么这些新脚本以 ASP.NET 编写?
- 第 643 页的如何使用 LHM 向有线用户提供访客服务访问?
- 第 643 页的作为验证者, 我可以使用 LDAP、RADIUS、按钮、时间、占卜、调查、相对气压、密码等使用 LHM 来提供访问权限吗?
- 第 643 页的 SonicWall 可以为我编写这种脚本吗?
- 第 643 页的我想使用 SonicWall 提供的示例脚本。我需要做什么才能使用它们?
- 第 644 页的 LHM 服务器可以驻留在哪里?
- 第 644 页的为什么我的访客无法访问 LHM 服务器或为什么 LHM 服务器上的页面无法加载?
- 第 644 页的 SonicWall 和 LHM 服务器之间的 LHM 交换如何工作 (简明版本, 典型环境)?
- 第 645 页的所有的 LHM 设置是什么意思? 如何配置它们?
- 第 647 页的是否可以更改 LHM 管理端口的默认值 TCP 4043 吗?
- 第 647 页的需要使用 HMAC 选项吗? 如果我想使用, 应该如何使用?
- 第 647 页的 SonicWall 是否为这些脚本提供任何支持?
- 第 648 页的我写了新的脚本, 对你们的脚本做了很大的改进, 或者我刚刚使脚本比你们做的好多了; SonicWall 是否感兴趣?
- 第 648 页的 LHM 脚本库

LHM 服务器脚本是否必须在 ASP 中编写?

否。可以使用任何能处理 Web 请求和 XML (LHM 的两个核心组件) 的平台来编写 LHM 服务器脚本。这包括 Perl、PHP、ASP、ASP.NET 和 J2EE。

为什么这些新脚本以 ASP.NET 编写?

ASP.NET 选为新脚本语言的原因包括其通用性及某些显而易见的优势, 比如它可以轻松处理 XML。

如何使用 LHM 向有线用户提供访客服务访问？

虽然访客服务（以前称为 WGS 或无线访客服务）是为无线（热点）用户设计的，但访客服务也可以用于有线用户，将有线接口（或接口，如可能在具有 PortShield 的 PRO 1260 上）接入禁用 SonicPoint Enforcement 的无线区域。所有访客服务选项然后适用于有线用户，包括 LHM、动态地址转换、允许/拒绝网络等。

“验证”和“授权”有什么区别？

验证描述了用户对某种挑战提供响应的流程。挑战可以是任何事情，尽管传统上是 `username:password`。LHM 通过抽取验证来打破传统模式的这种依赖。验证器的作用由 LHM 服务器实现，验证方法只能通过想象力来约束。考虑以下验证方法：

- 提供有效的用户名和密码
- 猜想计算机产生的数字
- 填写此问卷
- 通过测试，分数至少达到 80%
- 单击**我接受**按钮。

验证后，客户端可以获得授权做某事。

授权是授予访问权限的流程。为了使授权变得有用，授权者必须有方法来阻止客户访问受保护的资源。在 LHM 的情况下，SonicWall 是客户端的网关（有线或无线），因此它可以非常有效地充当授权者。在 SonicWall 从客户端的验证器收到 OK 后，会创建访客服务会话，并允许客户端访问 Internet。

作为验证者，我可以使用 LDAP、RADIUS、按钮、时间、占卜、调查、相对气压、密码等使用 LHM 来提供访问权限吗？

是。

SonicWall 可以为我编写这种脚本吗？

我们提供了一系列示例脚本作为示例并可供您自由修改，但我们不提供自定义脚本。然而，我们可以使您与可提供自定义脚本的人联系。有许多 SonicWall 合作伙伴拥有能提供这些服务的员工 Web 开发团队。

我想使用 SonicWall 提供的示例脚本。我需要做什么才能使用它们？

您需要：

- 运行 IIS 5.0 或更高版本的 Microsoft Windows 2000、XP、2003 平台，其运行最新的 Service Pack 和 Hotfix。
- Microsoft .NET 1.1（或更高版本）Framework：
<http://www.microsoft.com/downloads/details.aspx?FamilyId=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en>
- 最新的 .NET Framework Service Pack：
<http://www.microsoft.com/downloads/details.aspx?familyid=A8F5654F-088E-40B2-BBDB-A83353618B38&displaylang=en>

使用脚本的步骤如下：

- 1 将要使用的 LHM 脚本复制到 wwwroot 目录（通常在 C:\inetpub\wwwroot）中。
- 2 在 SonicWall 上配置访客服务以使用外部访客验证，如第 645 页的**所有的 LHM 设置是什么意思？如何配置它们？**中所述。

某些脚本需要写入权限，特别是使用数据库的脚本。根据配置，两个或三个独立的“用户”需要对需要写入的脚本目录具有写入访问权限。

- 第一个帐户（所有平台）是 **IUSR_MACHINENAME**（其中 machinename = 本地计算机的名称）。
- 第二个帐户：
 - 在 Windows XP 上，是 **ASPNET**（ASP.NET 计算机帐户）。
 - 其他平台是 **IWAM_MACHINENAME**（其中 machinename = 本地计算机的名称）。
- 如果在分配这些权限后数据库读/写访问继续失败，可能需要为 **NETWORK SERVICE** 帐户添加读/写权限。

① 注： 1.1 之前的 .NET Framework 上的版本在域控制器上有用户权限问题 (<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315158>)。强烈推荐安装 1.1（或更高版本）。

- 3 设置好环境后，需要自定义脚本。已通过 `myvars.aspx` 文件中放置所有相关的可配置位，使其尽可能简单。所有条目都有注释，它们的用途和语法应该是显而易见的。可以对脚本本身进一步定制，但通常不是必需的。

LHM 服务器可以驻留在哪里？

LHM 服务器可以在网络中的几乎任何位置，只要访客可以访问。它可以位于一个集中的网络运行中心，可以为多个热点管理 LHM，也可以与单个 SonicWall 安全设备放在一起。

为什么我的访客无法访问 LHM 服务器或为什么 LHM 服务器上的页面无法加载？

访客客户端与 LHM 服务器直接通讯；该通讯不由 SonicWall 安全设备代理。换句话说：

- 访客客户端的子网必须能访问 LHM 服务器。
- LHM 服务器必须知道如何访问访客客户端的子网（通过路由、NAT 或 VPN）。
- 防火墙访问规则必须配置为允许访客客户端子网访问 LHM 服务器。

SonicWall 和 LHM 服务器之间的 LHM 交换如何工作（简明版本，典型环境）？

- 1 访客客户端关联，获取 DHCP 租约，并启动 Web 浏览器。
- 2 通过 SonicWall 安全设备允许 DNS。URL FQDN 解析为其 IP 地址。
- 3 SonicWall 安全设备将检查访客客户端是否有已验证的会话。
 - 如果是新的，SonicWall 安全设备将客户端重定向到内部重定向（正在重定向，请稍候...）页面。

- 4 内部重定向页面尝试将访客客户端重定向到 LHM 服务器。
 - 如果失败，则将客户端重定向到内部服务器（无线访问暂时不可用。请单击此处以重试）页面。
- 5 访客客户端重定向至 LHM 服务器。在重定向 URL 中，安全设备嵌入描述初级会话的 `querystring` 信息（例如 `sessionID`、客户端的 MAC 和 IP 地址、安全设备的 LHM 管理 IP 和端口、UFI、原始请求的 URL）。
 - LHM 服务器脚本抓取 `querystring` 信息。
 - 客户端直接从 LHM 服务器检索 LHM 登录页面。
- 6 根据所使用的授权模式（例如 `username:password`、`passcode`、**我接受按钮**），LHM 服务器决定访客客户端是否可以访问。
- 7 LHM 服务器在 `externalGuestLogin.cgi` 页面的已配置管理端口（例如 TCP 4043）向 SonicWall 安全设备发出 Web 请求。
 - LHM 服务器发送 `sessionID`（在步骤 5 中获得）以及 `username`（从用户或组合获得）和 `session-lifetime` 和 `idle-timeout`（均由它确定）。
- 8 安全设备会验证 `sessionID`，尝试创建会话，然后用描述是否能授权（创建）访客会话的结果代码来响应 POST。
- 9 LHM 服务器解释结果代码并向访客客户端报告结果（例如 `Session Authorized - You may now start browsing`、`Session creation failed - Rats`、`Max sessions`）。

所有的 LHM 设置是什么意思？如何配置它们？

不像第 623 页的[关于轻量级热点新闻 \(LHM\)](#) 中提供完整的详细信息，这里只是解释一下这些设置的意义以及如何配置它们：

无线 SonicOS 上的 LHM 配置在[编辑区域 — WLAN](#) 对话框中完成。

主题：

- 第 645 页的[常规](#)
- 第 646 页的[验证页面](#)
- 第 646 页的[Web 内容](#)
- 第 647 页的[高级](#)

常规

本地 Web 服务器设置

客户端重定向协议

通过正在重定向，请稍候... 页面执行初始内部客户端重定向时，SonicWall 安全设备使用的协议（HTTP 或 HTTPS）。（此消息可从 **Web 内容** 选项卡上的 **重定向消息** 区域进行配置。）此步骤在重定向到 LHM 服务器之前。

外部 Web 服务器设置

Web 服务器协议	在 LHM 服务器上运行的协议（HTTP 或 HTTPS）。
Web 服务器主机	LHM 服务器的 IP 或可解析的 FQDN。
Web 服务器端口	LHM 服务器上所选协议的操作的 TCP 端口。
连接超时	LHM 服务器在重定向尝试中被认为不可用之前持续的时间（以秒为单位）。在超时时，客户端将显示在 Web 内容 选项卡上配置的服务器宕机消息。

消息验证

启用消息验证	使用 HMAC 摘要和嵌入式查询与 LHM 服务器通讯。如果在使用 HTTP 与 LHM 服务器进行通讯时担心消息篡改，这很有用。可选。
验证方法	选择 MD5 或 SHA1 。
共享密钥	哈希 MAC 的共享密钥。如果使用，还需要在 LHM 服务器脚本上进行配置。

验证页面

外部验证页面

① **注：** 这些页面可能各自是 LHM 服务器上的唯一页面，或是相同的页面但其每个状态消息的事件处理程序互相独立。下面提供了与新开发的脚本一起使用的示例。

登录页面	客户端重定向到的第一个页面（例如 <code>lhm/accept/default.aspx</code> ）。
会话超时页面	会话过期时客户端重定向到的页面（例如 <code>lhm/accept/default.aspx?cc=2</code> ）。会话过期后，用户必须创建新的 LHM 会话。
闲置超时页面	超过闲置计时器时客户端重定向到的页面（例如 <code>lhm/accept/default.aspx?cc=3</code> ）。超过闲置计时器后，只要会话还有剩余时间，用户就可以使用相同的凭据重新登录。
最大会话页面	达到最大会话次数后，客户端重定向到的页面（例如 <code>lhm/accept/default.aspx?cc=4</code> ）。

Web 内容

重定向报文

显示给客户端的默认或自定义消息（通常不超过一秒），说明会话正在重定向到 LHM 服务器。使用此插播式页面（而非直接进入 LHM 服务器），以便安全设备可以验证 LHM 服务器的可用性。

服务器宕机消息

当重定向器确定 LHM 服务器不可用时，显示给客户端的默认或自定义消息。

高级

这些参数是可选的。

自动会话注销	时间增量和 SonicWall 安全设备在会话注销时（自动或手动）POST 到的页面。
服务器状态检查	时间增量和 SonicWall POST 到的页面，用于确定 LHM 服务器上或后面的组件（例如后端数据库）可用性。
会话同步	时间增量和 SonicWall 将整个访客服务会话表发送到的页面。这允许 LHM 服务器同步访客用户的状态，以用于会计、计费或预测。

是否可以更改 LHM 管理端口的默认值 TCP 4043 吗？

是。可以在 SonicOS 中通过修改外部访客验证服务对象的端口值轻松完成。

需要使用 HMAC 选项吗？如果我想使用，应该如何使用？

HMAC 功能是可选的。它可以确保由 SonicWall 发送到 LHM 服务器的消息和 LHM 服务器发送到 SonicWall 安全设备的消息未篡改。HMAC 通过计算在两个对等体之间传递的信息上的加密（密码辅助）消息验证码，并将该计算的摘要添加到数据中来实现此功能。在接收到数据后，另一方计算摘要本身，并将其与发送的 MAC 进行比较；如果两者匹配，则数据传送完整。如果您处于不安全的环境或担心安全性，则应该考虑使用 HMAC 选项。

如果选择使用 HMAC，可以实施您自己的 HMAC 例程，但最简单的方法是使用 SonicWall 编写的 SonicSSL.dll 库，以及 libeay32.dll，它可以作为 OpenSSL 的一部分免费提供；都可以通过请求从 SonicWall 获得。

使用 HMAC 的步骤如下：

- 1 将 libeay32.dll 文件复制到 LHM (IIS) 服务器上的路径（例如，复制到 C:\Windows\system32 文件夹中）。
- 2 将 SonicSSL.dll 文件复制到同一服务器上的任何位置。
- 3 使用命令 `regsvr32 SonicSSL.dll` 注册 SonicSSL.dll 文件。

完成之后，LHM 脚本能使用 HMAC 计算的 `Server.CreateObject(SonicSSL.Crypto)` 对象。HMAC 功能包含在第 648 页的 [LHM 脚本库](#) 中描述的脚本中。

重要： SonicWall 安全设备 URL 将 `querystring` 的 `req`（原始请求的 URL）部分进行编码（某些字符从其 ASCII 符号转换为十六进制符号），但 SonicWall 的 URL 编码方法与 Microsoft 方法（例如，由 `Request.QueryString` 使用）略有不同。由于这种方法上的差异，执行 HMAC 的字符串可以在安全设备和 LHM 服务器之间不同。提供的脚本通过以与 SonicWall 方法一致的方法手动编码 `querystring` 的 `req` 部分来补偿此问题。

SonicWall 是否为这些脚本提供任何支持？

这些脚本是作为示例提供的，并不会由 SonicWall 技术支持提供支持，SonicWall 支持也不会协助配置 LHM 后端环境。未来的咨询支持服务可能会解决这个问题。

我写了新的脚本，对你们的脚本做了很大的改进，或者我刚刚使脚本比你们做的好多了； SonicWall 是否感兴趣？

是！我们一直在寻求使用 LHM 的新途径，并寻找能为可用脚本库做出贡献的人。我们考虑在任何平台上编写的使用任何验证方法的 LHM 脚本。请发送电子邮件至 products@sonicwall.com，描述您的脚本，我们将考虑将其添加到我们的库中。提交脚本将允许 SonicWall 自由修改和/或重新分发所提交的脚本。

LHM 脚本库

成立 SonicWall LHM 脚本库的目的是为正在使用或希望使用 LHM 实现访客服务的人员提供资源。目标是吸引众多贡献者和用户，使这个库壮大，以包含大型、多样化和有用的脚本集合，任何人都可以修改或按原样使用。

该库的首批内容包括六个脚本：对常见的用户请求做出响应的（`accept`、`guestbook` 和 `adauth`）和一些较不常见的（`lhmquiz`、`random` 和 `paypal`）。它们是在 Visual Studio .NET 开发环境外编写的，因此它们的样式可以是多样的。然而，所有脚本的共同之处在于：

- 可配置变量的模块化，例如文件路径、服务器 IP 地址、弹出式注销窗口的使用、加密盐值和计时器设置。这些可配置值会收集到 `myvars.aspx` 文件中，因此可以在一个地方进行环境编辑，而不必搜索可配置的元素。
- 广泛的解释，逐步说明所执行的操作。

脚本目录的顶层提供了 `chooser.aspx` 登录页面。此脚本专为演示环境而设计，以允许选择较低级别（特定）脚本，而无需重新配置 SonicWall 安全设备上的 LHM 设置以指向特定脚本。换句话说，可以将安全设备上的 LHM 配置为指向顶层 `chooser.aspx` 脚本，然后枚举所有子目录（较低层级脚本，例如 `random`、`accept`、`adauth`）。顶层 `chooser.aspx` 脚本在新窗口中打开目标下级 `default.aspx` 脚本，并完整地传递原始的 `querystring`。

所有脚本以 `default.aspx` 页面开始，根据需要自动执行客户端重定向。因此，SonicWall 上的 LHM 配置应该指向相应路径的 `default.aspx` 页面（例如 `lhm/accept/default.aspx` 或 `lhm/adauth/default.aspx`）。某些脚本具有单独的管理功能页面；会在脚本描述中注明。

每个脚本还提供了 `logout.aspx` 页面。可以在 `myvars` 中使用 `logoutPopup` 变量对此页面的使用进行控制。设置值 1 可以使用弹出式注销窗口。在从安全设备接收到成功的响应代码 (50) 后，由 LHM 验证流程调用该窗口。该脚本将 `sessID`、`mgmtBaseUrl` 和 `sessTimer` 变量传递到 `logout.aspx` 窗口，以便该窗口可以跟踪会话时间；当/如果用户想要手动终止会话时，还可以将注销事件发回到安全设备（在 `mgmtBaseUrl`）以获取正确的会话 (`sessID`)。

关于使用注销弹出窗口

- 使用注销弹出窗口不是必需的。会话在其配置的生命周期到期后自动超时。弹出窗口只是为用户提供一种手动终止其会话的机制。
- 该窗口通过 javascript 弹出窗口启动，所以弹出窗口阻止程序可以阻止该窗口。
- 关闭窗口不会中断会话。只有“注销”按钮可以结束会话。
- 由于倒计时计时器在客户端运行，因此已采取步骤来防止刷新页面。刷新页面会重置客户端倒计时计时器，但不会影响实际的会话计时器。会捕获和禁止 F5 键和右键单击鼠标事件，但并不适用于所有浏览器。
- 使用注销弹出窗口应该与脚本验证方案的性质一致：

- 某些脚本具有非独占登录进程，这意味着用户可以重复登录（例如 Accept 和 ADAuth 脚本）。鼓励对这些非独占脚本使用注销弹出窗口。
- 某些脚本是非独占的，但会收集应该保持唯一的数据（例如 Guestbook 和 LHMQuiz 脚本）。对这些脚本使用注销弹出窗口是可以接受的，但可能会导致收集冗余数据。
- 某些脚本是独占的，这意味着在用户验证后，不可能零成本重复验证流程（例如 PayPal 脚本或 Random 脚本，其中启用了 useDB）。对这些脚本不建议使用注销弹出窗口，因为用户没有简单的重新登录方法。

脚本还可为 .NET 流程错误提供隐藏的输出，通过将文本与背景颜色相匹配来隐藏文本。在发生某种故障或错误的情况下，可以通过在网页上单击 CTRL-A 来提供并显示错误输出，以选择所有文本。

以下是每个脚本的描述，它们的功能以及它们的作用方式。在将新的脚本添加到库中时，会随之添加类似的描述以帮助理解、定制和集成。

主题：

- 第 649 页的 [Accept 脚本](#)
- 第 662 页的 [ADAuth 脚本](#)
- 第 677 页的 [Guestbook 脚本](#)
- 第 694 页的 [LHMQuiz 脚本](#)
- 第 714 页的 [PayPal 脚本](#)
- 第 737 页的 [Random 脚本](#)
- 第 759 页的 [Chooser.aspx 脚本](#)

Accept 脚本

验证模式	访客客户端单击 我接受 按钮。
目的	向客户端提供可接受的使用策略、服务条款或欢迎页面。
myvars 变量	<p>logoutPopup 控制注销弹出窗口的使用。设置为：</p> <ul style="list-style-type: none"> • 0 以禁用弹出窗口。 • 1 以启用弹出窗口。 <p>sessTimer 会话计时器，以秒为单位。</p> <p>idleTimer 闲置计时器，以秒为单位。</p> <p>用户名 应用于访客会话的用户名。因为脚本不会从客户端获取用户名，因此它可以是：</p> <ul style="list-style-type: none"> • 在此处明确地为所有客户端设定。 • 设置为 useMAC 以将用户名设置为 MAC 地址。 <p>strHmac 可选 HMAC 功能的共享密钥。</p> <p>hmacType HMAC 在使用中时使用的摘要类型：MD5 或 SHA1。</p> <p>logo 要在页眉上使用的徽标（图像）文件的名称。</p>
会话流程	<ol style="list-style-type: none"> 1 访客客户端单击我接受按钮。 2 LHM POST 字符串与 sessionID、用户名（或 MAC 的默认值）、默认会话生命周期和闲置生命周期组合在一起。 3 该脚本执行到 SonicWall 安全设备的 LHM POST 以授权会话。
其他注意事项	只需要基本的 LHM 配置。

主题:

- 第 650 页的 [default.aspx](#)
- 第 656 页的 [logout.aspx](#)
- 第 661 页的 [myvars.aspx](#)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/accept/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

    LHMResult.Text=""
    catchError.Text=""

    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
    ufi=Request.QueryString("ufi")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
```

```

clientRedirectUrl=Request.QueryString("clientRedirectUrl")
req=Request.QueryString("req")
hmac=Request.QueryString("hmac")
customCode=Request.QueryString("cc")

'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
If customCode <> "" Then
    Select Case customCode
        Case "2"
            LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
        Case "3"
            LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
        Case "4"
            LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
    End Select
End If

'Set the userName to the grabbed client MAC address if so configured in myvars
If userName = "useMAC" Then
    userName = mac
End If

'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
If hmac <> "" Then

    'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
    req=Replace(req,"%","%25")
    req=Replace(req,":","%3A")
    req=Replace(req," ","%20")
    req=Replace(req,"?","%3F")
    req=Replace(req, "+", "%2B")
    req=Replace(req, "&", "%26")
    req=Replace(req, "=", "%3D")

    Dim strHmacText as String
    Dim objCrypto as Object
    Dim strHmacGenerated
    Dim loginError as String

    'Initialize the Crypto object
    objCrypto = Server.CreateObject("SonicSSL.Crypto")

    'The text to be encoded
    strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

```

```

        'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
        'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
        If hmacType = "MD5" Then
            strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
        Else
            strHmacGenerated = objCrypto.hmac_shal(strHmacText, strHmac)
        End If

        If strHmacGenerated <> hmac Then
            Dim hmacFail as String
            hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
            hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
            hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
            hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
            catchError.Text=hmacFail
        End If

    End If

End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    'Let the user know that we are setting up the session, just in case it takes more
than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogin.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try
        'Create the webrequest to the SonicWALL
        Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

        'Calculate the length of the byte array
        toSNWL.ContentLength = byteArray.Length

        'Set the method for the webrequest to POST
        toSNWL.Method = "POST"

        'Set the content type
        toSNWL.ContentType = "application/x-www-form-urlencoded"

        'Open the request stream

```

```

Dim dataStream As Stream = toSNWL.GetRequestStream()

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 50 - Login Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

'Do we want to provide a logout popup window?
If logoutPopup = "1" Then
    'Popup hack using Javascript for logout window
    Dim sb As New System.Text.StringBuilder()
    sb.Append("<script language='javascript'>")
    sb.Append("window.open('logout.aspx?sessId=")
    sb.Append(Server.URLEncode(CStr(sessionId)))
    sb.Append("&mgmtBaseUrl=")
    sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
    sb.Append("&sessTimer=")
    sb.Append(Server.URLEncode(CStr(sessTimer)))
    sb.Append("'", 'logOut', 'toolbar=no,")
    sb.Append("addressbar=no,menubar=no,")
    sb.Append("width=400,height=250');")
    sb.Append("<")
    sb.Append("/")
    sb.Append("<script>")
    RegisterStartupScript("stp", sb.ToString)
End If

    LHMResult.Text = "<br><b><font color=""green"">Session
Authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href="" & req & "">" & req & "</a>"

'Response code 51 - Session Limit Exceeded
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
    LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 100 - Login Failed.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"

```

```

        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        'Response code 251 - Bad HMAC.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        'Response code 253 - Invalid SessionID.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

        'Response code 254 - Invalid CGI.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        'Response code 255 - Internal Error.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        End If

        'Close the streams
        dataStream.Close()
        snwlReply.Close()

        'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
        Catch ex as Exception
            catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
        End Try
    End Sub

</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    background-color: #006699;
}

```

```

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Accept Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=3 align="center"><font color="white">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td width="50%" valign="center"><font color="white"><b>Welcome <%=
ip%></b></font></td>
        <td align="center"></center></td>
        <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
    </tr>
    <tr class="heading">
        <td colspan=3 align="center"><font color="white">&nbsp;</td>
    </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

    <tr>
        <td><br></td>
    </tr>
    <tr>
        <td align=left>
            By clicking the <b>Accept</b> button below, you accept the following terms of
            service:<br><br><b>
            1. You will not try to download bad things.<br>
            2. You will not try to upload bad things.<br>
            3. You will not try to use all the bandwidth so that others have none.<br>
            4. You will be happy when the SonicWALL blocks bad things from reaching
            you.</b><br><br>
        </td>
        <td>
        </tr>
    <tr>
        <td><br><asp:button id="btnSubmit" class="button" text=" Accept "
onClick="btnSubmit_Click" runat="server" /></td>
    </tr>
    <tr>
        <td><asp:Label id=LHMResult runat="server" /></td>
    </tr>
    <tr>
        <td><asp:Label id=catchError runat="server" /></td>
    </tr>
</table>
</form>
</BODY>
</HTML>

```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
    sessionId=Request.QueryString("sessId")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    sessTimer=Request.QueryString("sessTimer")

    'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'When the page loads, make the loggedIn span visible
    loggedIn.Visible=True
    loggedOut.Visible=False

    Me.Button1.Attributes.Add("OnClick", "self.close()")
End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    'Let the user know that we are setting up the session, just in case it takes more
than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogoff.cgi"
```



```

'Assemble the data to post back to the SonicWALL to authorize the LHM session
Dim loginParams as String = "sessId=" & sessionId & eventId

'Combine mgmtBaseUrl from the original redirect with the login cgi
Dim postToSNWL as String = mgmtBaseUrl & loginCgi

'Convert the loginParams to a well behaved byte array
Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

Try
    'Make the loggedOut span visible
    loggedIn.Visible=False
    loggedOut.Visible=True

    'Create the webrequest to the SonicWALL
    Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

    'Calculate the length of the byte array
    toSNWL.ContentLength = byteArray.Length

    'Set the method for the webrequest to POST
    toSNWL.Method = "POST"

    'Set the content type
    toSNWL.ContentType = "application/x-www-form-urlencoded"

    'Open the request stream
    Dim dataStream As Stream = toSNWL.GetRequestStream()

    'Write the byte array to the request stream
    dataStream.Write(byteArray, 0, byteArray.Length)

    'Close the Stream object
    dataStream.Close()

    'Get the response
    Dim snwlReply As WebResponse = toSNWL.GetResponse()

    'Display the status - looking for 200 = OK.
    'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

    'Grab the response and stuff it into an xml doc for possible review
    Dim snwlResponse as XmlDocument = New XmlDocument()
    snwlResponse.Load(snwlReply.GetResponseStream())

    'Set the xPath to the SNWL reply, and get the response
    Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

    'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

    'Response code 150 - Logout Succeeded
    If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

    'Response code 251 - Bad HMAC.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

```

```

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
End Try
End Sub

</script>
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    font-size: 10pt;
    background-color: #006699;
}

tr.smalltext {
    font-size: 8pt;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
    font-size: 8pt;
}
</STYLE>

```

```

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function Countdown()
{
    clockStr="";

    dayStr=Math.floor(SecondsToCountDown/86400)%100000
    if(dayStr>0){
        if(dayStr>1){
            dayStr+=" days ";
        } else dayStr+=" day ";
        clockStr=dayStr;
    }
    hourStr=Math.floor(SecondsToCountDown/3600)%24
    if(hourStr>0){
        if(hourStr>1){
            hourStr+=" hours ";
        } else hourStr+=" hour ";
        clockStr+=hourStr;
    }
    minuteStr=Math.floor(SecondsToCountDown/60)%60
    if(minuteStr>0){
        if(minuteStr>1){
            minuteStr+=" minutes ";
        } else minuteStr+=" minute ";
        clockStr+=minuteStr;
    }
    secondStr=Math.floor(SecondsToCountDown/1)%60
    if(secondStr>0){
        if(secondStr>1){
            secondStr+=" seconds ";
        } else secondStr+=" second ";
        clockStr+=secondStr;
    }

    if(SecondsToCountDown > 0)
    {
        --SecondsToCountDown;
    }

    if(originalTime.length < 2)
    {
        originalTime = clockStr;
    }

    // Make sure the form is still there before trying to set a value
    if(document.frmValidator){
        document.frmValidator.originalTime.value = originalTime;
        document.frmValidator.countdown.value = clockStr;
    }

    setTimeout("Countdown()", 1000);
    if(SecondsToCountDown == 0)

```

```

    {
        document.frmValidator.countdown.value = "Session Expired";
    }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
    return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
    var key_f5 = 116;
    if (key_f5==event.keyCode)
    {
        event.keyCode=0;
        return false;
    }
    return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="smalltext"><td><br></td></tr>
    <tr class="smalltext">
        <td>Original Session Time:</td>
        <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
    </tr>
    <tr class="smalltext">
        <td>Remaining Session Time:</td>
        <td><asp:textbox width=250 id="countdown" runat="server" /></td>
    </tr>
    <tr class="smalltext">
        <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
    </td>
    <tr>

```

```

        <td colspan=2><center><asp:button id="btnSubmit" class="button" text=" Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr>
        <td><asp:Label id=LHMResult runat="server" /></td>
    </tr>
    <tr>
        <td><asp:Label id=catchError runat="server" /></td>
    </tr>
    <tr><td><br></td></tr>
    <tr>
        <td><center><asp:button id="Button1" class="button" text=" Close "
runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

</BODY>
</HTML>

```

myvars.aspx

```

<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the username to record for LHM session since this does not gather one. Set to
userName="useMAC" to use the MAC address.
Dim userName="useMAC"
'Dim userName = "LHM Guest User"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

```

```
'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'-----End of Configurable Settings-----

</script>
```

ADAuth 脚本

验证模式	访客客户端提供其用户名和密码。然后，将依照 Active Directory 或 LDAP 数据库验证这些凭据。
目的	通过 LDAP 使用 Active Directory 的典型授权模式。支持每用户会话计时器和闲置计时器设置，通过在授权期间可选地从数据库抓取 LDAP 属性。
myvars 变量	<p>logoutPopup 控制注销弹出窗口的使用。设置为：</p> <ul style="list-style-type: none"> • 0 以禁用弹出窗口。 • 1 以启用弹出窗口。 <p>myLdapServer 提供验证的 LDAP/AD 服务器的 IP 地址或可解析的 FQDN。</p> <p>myLdapDomain LDAP/AD 域名</p> <p>retrAttr 指定是否从验证用户的 LDAP 属性（稍后定义）检索会话和闲置计时器值。设置为：</p> <ul style="list-style-type: none"> • 0 以禁用检索。 • 1 以尝试检索。 <p>useCN 如果 reAttr = 1，则此标志设置是使用公用名 (cn) 来检索属性，还是使用 AD 默认登录名 (sAMAccountName)。 设置为 1 以使用 cn。当对照 AD 进行验证时，此标志应设置为 0。</p> <p>sessAttr 检索会话计时器的 LDAP 属性（以秒为单位）。如果未检索到值或检索到的值不是数字，则使用默认会话计时器 (sessTimer，在下面定义)。</p> <p>idleAttr 检索闲置计时器的 LDAP 属性（以秒为单位）。如果无法检索到值或检索到的值不是数字，则使用默认闲置计时器 (idleTimer，在下面定义)。</p> <p>sessTimer 默认会话计时器，以秒为单位。</p> <p>idleTimer 默认闲置计时器，以秒为单位。</p> <p>strHmac 可选 HMAC 功能的共享密钥。</p> <p>hmacType HMAC 在使用中时使用的摘要类型：MD5 或 SHA1。</p> <p>logo 要在页眉上使用的徽标（图像）文件的名称。</p>

会话流程

- 1 访客客户端输入其 LDAP/AD 用户名和密码。
- 2 提供的凭据用于与配置的 LDAP 服务器绑定。
- 3 如果绑定尝试成功，则用户通过验证。
- 4 如果设置了 reAttr 标志，则尝试从 LDAP 数据库检索定义的 sessAttr 和 idleAttr 属性（例如 pager 和 mobile）。如果检索到有效结果，则使用它们；否则使用默认值。
- 5 该脚本执行到 SonicWall 安全设备的 LHM POST 以授权会话。

其他注意事项

要求 LHM 服务器能通过路由、NAT 或 VPN 与配置的 LDAP/AD 服务器进行通讯。如果使用 reAttr 选项，则要求定义 LDAP 属性以使用户特定的值生效。

注：选择了 pager 和 mobile 属性，因为它们不经常使用，也因为可以通过 Microsoft 的用户和计算机 MMC 直接设置。）

主题：

- 第 663 页的 [default.aspx](#)
- 第 670 页的 [logout.aspx](#)
- 第 676 页的 [myvars.aspx](#)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Math" %>
<%@ Import Namespace="System.DirectoryServices" %>
<%@ Import Namespace="System.Collections" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Assembly name="System.DirectoryServices, Version=1.0.3300.0,
Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/adauth/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig
```

```

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

    LHMResult.Text=""
    catchError.Text=""
    authResult.Text=""

    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
    ufi=Request.QueryString("ufi")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    clientRedirectUrl=Request.QueryString("clientRedirectUrl")
    req=Request.QueryString("req")
    hmac=Request.QueryString("hmac")
    customCode=Request.QueryString("cc")

    'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
    you to use the same
    'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
    (?cc=3) and "Max Sessions" (?cc=4) page.
    If customCode <> "" Then
        Select Case customCode
            Case "2"
                LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
                You may try to initiate a new session.</font></H3>"
            Case "3"
                LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
                timeout. Please log back in.</font></H3>"
            Case "4"
                LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
                has been reached. Please try again later.</font></H3>"
        End Select
    End If

    'Use the override class in myvars.aspx to accept untrusted certificates from the
    SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'Note - the routine below for handling the hmac requires the use of the
    SonicSSL.dll and libeay.dll libraries.
    'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
    with "regsvr32 sonicssl.dll"
    If hmac <> "" Then

        'SonicWALL URL Encode routine is different from Microsoft - this is the
        SonicWALL method
        req=Replace(req,"%","%25")
        req=Replace(req,":","%3A")
        req=Replace(req," ","%20")
        req=Replace(req,"?","%3F")

```



```

req=Replace(req,"+","%2B")
req=Replace(req,"&","%26")
req=Replace(req,"=","%3D")

Dim strHmacText as String
Dim objCrypto as Object
Dim strHmacGenerated
Dim loginError as String

'Initialize the Crypto object
objCrypto = Server.CreateObject("SonicSSL.Crypto")

'The text to be encoded
strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
If hmacType = "MD5" Then
    strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
Else
    strHmacGenerated = objCrypto.hmac_shal(strHmacText, strHmac)
End If

If strHmacGenerated <> hmac Then
    Dim hmacFail as String
    hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
    hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
    hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
    hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
    catchError.Text=hmacFail
    End If

End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
    txtName.Text = ""
    txtPassword.Text = ""
    authResult.Text=""
    LHMResult.Text=""
    catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

'Try to connect to LDAP with the user supplied attributes
Try
    Dim ldapPath as String = "LDAP://" & myLdapServer
    Dim ldapUser as String = myLdapDomain & "\" & txtName.Text
    Dim validateUser as New DirectoryEntry(ldapPath,ldapUser,txtPassword.Text)

'This is the actual authentication piece
Dim nativeCheck as Object = validateUser.NativeObject

```

```

'If retrAttr is set in the myvars file, attempt to retrieve the session and
idle values from LDAP
If retrAttr = "1" Then
    Dim mySearch as New DirectorySearcher(validateUser)

    'Check the myvars for selecting either sAMAccountName or cn
    If useCN = "0" Then
        mySearch.Filter = "(sAMAccountName=" & Server.URLEncode(txtName.Text) &
    ") "
    Else
        mySearch.Filter = "(cn=" & Server.URLEncode(txtName.Text) & ")"
    End If
    mySearch.PageSize="1"
    mySearch.PropertiesToLoad.Add(sessAttr)
    mySearch.PropertiesToLoad.Add(idleAttr)
    Dim adResult as SearchResult

    'If we get results on the attribute query, set timer values
    adResult = mySearch.FindOne
    If Not (adResult is Nothing) Then
        If (adResult.Properties.Contains(sessAttr)) Then
            'Check to see if the LDAP value returned is a number
            Dim isNumber as New RegEx("^\d+$")
            If (isNumber.IsMatch(adResult.Properties(sessAttr)(0).ToString()))
Then
                sessTimer=adResult.Properties(sessAttr)(0).ToString()
            End If
        End If 'End If sessAttr
        If (adResult.Properties.Contains(idleAttr)) Then
            'Check to see if the LDAP value returned is a number
            Dim isNumber as New RegEx("^\d+$")
            If (isNumber.IsMatch(adResult.Properties(idleAttr)(0).ToString()))
Then
                idleTimer=adResult.Properties(idleAttr)(0).ToString()
            End If
        End If 'End if idleAttr
    End If 'End if adResult is present
End If 'End if retrAttr is in use

    authResult.Text="<font color=""green""><b>Credentials
Accepted.</b></font><br>Session Lifetime: " & round(sessTimer/60) & "
minutes.<br>Idle Timer: " & round(idleTimer/60) & " minutes."

    'Auth succeeded - move on to LHM Auth
    LHM()

    Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        authResult.Text="<font color=""Red""><b>Credentials
Rejected.</b></font><br>Please enter a valid username and password. "
    End Try

End Sub

Sub LHM()

    'Let the user know that we are setting up the session, just in case it takes
more than a second
    LHMResult.Text = "Authorizing session. Please wait."

```

```

'The LHM cgi on the SonicWALL - this does not change
Dim loginCgi as String = "externalGuestLogin.cgi"

'Assemble the data to post back to the SonicWALL to authorize the LHM session
Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

'Combine mgmtBaseUrl from the original redirect with the login cgi
Dim postToSNWL as String = mgmtBaseUrl & loginCgi

'Convert the loginParams to a well behaved byte array
Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

Try
'Create the webrequest to the SonicWALL
Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

'Calculate the length of the byte array
toSNWL.ContentLength = byteArray.Length

'Set the method for the webrequest to POST
toSNWL.Method = "POST"

'Set the content type
toSNWL.ContentType = "application/x-www-form-urlencoded"

'Open the request stream
Dim dataStream As Stream = toSNWL.GetRequestStream()

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 50 - Login Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

'Do we want to provide a logout popup window?
If logoutPopup = "1" Then
'Popup hack using Javascript for logout window
Dim sb As New System.Text.StringBuilder()
sb.Append("<script language='javascript'>")
sb.Append("window.open('logout.aspx?sessId=")

```

```

        sb.Append(Server.URLEncode(CStr(sessionId)))
        sb.Append("&mgmtBaseUrl=")
        sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
        sb.Append("&sessTimer=")
        sb.Append(Server.URLEncode(CStr(sessTimer)))
        sb.Append("'", 'logOut', 'toolbar=no,")
        sb.Append("addressbar=no,menubar=no,")
        sb.Append("width=400,height=250');")
        sb.Append("<")
        sb.Append("/")
        sb.Append("script>")
        RegisterStartupScript("stp", sb.ToString)
    End If

    LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href="" & req & """"> & req & ""</a>"

    'Response code 51 - Session Limit Exceeded
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
        LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

    'Response code 100 - Login Failed.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

    'Response code 251 - Bad HMAC.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

    'Response code 253 - Invalid SessionID.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

    'Response code 254 - Invalid CGI.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

    'Response code 255 - Internal Error.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

    End If

    'Close the streams
    dataStream.Close()
    snwlReply.Close()

```

'If there is some asp.net error trying to talk to the SonicWALL, print it in the same color as the background.

```
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
End Try
End Sub
</script>
```

```
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;
    background-color:#9CBACE;
}
```

```
tr.heading {
    background-color:#006699;
}
```

```
.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>
```

```
<HTML>
<HEAD>
<TITLE>LHM ADAuth Script</TITLE>
</HEAD>
```

```
<BODY>
<form id="frmValidator" runat="server">
```

```
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td width="50%" valign="center"><font color="white"><b>LDAP/AD LHM
Authentication</b></font></td>
    <td><center><img width="216" height="51" src=""%= logo %"></center></td>
    <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
  </tr>
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>
```

```
<table width="90%" border="0" cellpadding="2" cellspacing="0">
  <tr>
    <td><b>Welcome <%= ip%> to SonicWALL's LHM AD/LDAP
Authenticator.</b><br><br>Enter your LDAP or Active Directory username and password
to obtain secure guest internet access.<br><br>If your domain account specifies
session timeout values, those values will be applied to your account, otherwise you
```



```

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
    sessionId=Request.QueryString("sessId")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    sessTimer=Request.QueryString("sessTimer")

    'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'When the page loads, make the loggedIn span visible
    loggedIn.Visible=True
    loggedOut.Visible=False

    Me.Button1.Attributes.Add("OnClick", "self.close()")
End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    'Let the user know that we are setting up the session, just in case it takes more
than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogoff.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & eventId

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try

```

```

'Make the loggedOut span visible
loggedIn.Visible=False
loggedOut.Visible=True

'Create the webrequest to the SonicWALL
Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

'Calculate the length of the byte array
toSNWL.ContentLength = byteArray.Length

'Set the method for the webrequest to POST
toSNWL.Method = "POST"

'Set the content type
toSNWL.ContentType = "application/x-www-form-urlencoded"

'Open the request stream
Dim dataStream As Stream = toSNWL.GetRequestStream()

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 150 - Logout Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
    LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"

```



```

        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        'Response code 255 - Internal Error.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
            LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        End If

        'Close the streams
        dataStream.Close()
        snwlReply.Close()

        'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
        Catch ex as Exception
            catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
            LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
            End Try
        End Sub

</script>
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;
    background-color:#9CBACE;
}

tr.heading {
    font-size: 10pt;
    background-color:#006699;
}

tr.smalltext {
    font-size: 8pt;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
    font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

```

```

function Countdown()
{
    clockStr="";

    dayStr=Math.floor(SecondsToCountDown/86400)%100000
    if(dayStr>0){
        if(dayStr>1){
            dayStr+=" days ";
        } else dayStr+=" day ";
        clockStr=dayStr;
    }
    hourStr=Math.floor(SecondsToCountDown/3600)%24
    if(hourStr>0){
        if(hourStr>1){
            hourStr+=" hours ";
        } else hourStr+=" hour ";
        clockStr+=hourStr;
    }
    minuteStr=Math.floor(SecondsToCountDown/60)%60
    if(minuteStr>0){
        if(minuteStr>1){
            minuteStr+=" minutes ";
        } else minuteStr+=" minute ";
        clockStr+=minuteStr;
    }
    secondStr=Math.floor(SecondsToCountDown/1)%60
    if(secondStr>0){
        if(secondStr>1){
            secondStr+=" seconds ";
        } else secondStr+=" second ";
        clockStr+=secondStr;
    }

    if(SecondsToCountDown > 0)
    {
        --SecondsToCountDown;
    }

    if(originalTime.length < 2)
    {
        originalTime = clockStr;
    }

    // Make sure the form is still there before trying to set a value
    if(document.frmValidator){
        document.frmValidator.originalTime.value = originalTime;
        document.frmValidator.countdown.value = clockStr;
    }

    setTimeout("Countdown()", 1000);
    if(SecondsToCountDown == 0)
    {
        document.frmValidator.countdown.value = "Session Expired";
    }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()

```

```

{
    return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
    var key_f5 = 116;
    if (key_f5==event.keyCode)
    {
        event.keyCode=0;
        return false;
    }
    return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown() '>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="smalltext"><td><br></td></tr>
    <tr class="smalltext">
        <td>Original Session Time:</td>
        <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
    </tr>
    <tr class="smalltext">
        <td>Remaining Session Time:</td>
        <td><asp:textbox width=250 id="countdown" runat="server" /></td>
    </tr>
    <tr class="smalltext">
        <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
    </td>
    <tr>
        <td colspan=2><center><asp:button id="btnSubmit" class="button" text=" Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">

```

```

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;  </td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;  </td>
  </tr>
  <tr>
    <td><asp:Label id=LHMResult runat="server" /></td>
  </tr>
  <tr>
    <td><asp:Label id=catchError runat="server" /></td>
  </tr>
  <tr><td><br></td></tr>
  <tr>
    <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
  </tr>
</table>
</form>
</span>

</BODY>
</HTML>

```

myvars.aspx

```

<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LDAP server IP or Name
Dim myLdapServer as String = "10.50.128.40"

'Set the LDAP domain
Dim myLdapDomain as String = "sv.us.sonicwall.com"

'Set the retrAttr to 0 to use default session and idle timeouts
'Set the retrAttr to 1 to try to retrieve the session and idle timeouts from LDAP
attributes.
Dim retrAttr as String ="1"

'Set useCN=1 to use common name (e.g. "joe levy", non-Active Directory LDAP) for
attribute retrieval (retrAttr).
'Set useCN=0 to use saMAccountName (e.g. "jlevy", Active Directory / Windows) for
attribute retrieval.
Dim useCN as String = "0"

'If using retrAttr=1, you must define the ldap attributes from which to retrieve the
values
'Set the ldap attribute from which to retrieve the session timeout value (use is
optional)
Dim sessAttr as String = "pager"

```

```

'Set the ldap attribute from which to retrieve the idle timeout value (use is
optional)
Dim idleAttr as String = "mobile"

'If retrAttr=0, of if no attributes value can be retrieved, use the following
timeout values
'Set the default LHM Session Timeout (for when no attributes is retrieved)
Dim sessTimer as String = "3600"

'Set the default LHM Idle Timeout (for when no attributes is retrieved)
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'-----End of Configurable Settings-----
</script>

```

Guestbook 脚本

验证模式	访客客户端提供他们的姓名、地址、电话、电子邮件、URL（可选）和注释（可选）信息。
目的	收集市场信息；将这些信息写入数据库供以后使用。
myvars 变量	<p>logoutPopup 控制注销弹出窗口的使用。设置为：</p> <ul style="list-style-type: none"> • 0 以禁用弹出窗口。 • 1 以启用弹出窗口。 <p>sessTimer 会话计时器，以秒为单位。</p> <p>idleTimer 闲置计时器，以秒为单位。</p> <p>strHmac 可选 HMAC 功能的共享密钥。</p> <p>hmacType HMAC 在使用中时使用的摘要类型：MD5 或 SHA1。</p> <p>logo 要在页眉上使用的徽标（图像）文件的名称。</p>
会话流程	<ol style="list-style-type: none"> 1 访客客户端输入个人信息并单击“提交”。 2 输入的信息将写入本地的 .mdb 数据库文件供以后使用。 3 LHM POST 字符串与 sessionID、用户名（如 Web 表单中所提供）、默认会话生命周期和闲置生命周期组合在一起。 4 该脚本执行到 SonicWall 安全设备的 LHM POST 以授权会话。
其他注意事项	由于脚本正在写入数据库，因此必须为 IUSR_MACHINENAME 和 IWAM_MACHINENAME （或 ASPNET ）帐户配置写入权限，如第 643 页的我想使用 SonicWall 提供的示例脚本。我需要做什么才能使用它们？中所述。

主题:

- 第 678 页的 [default.aspx](#)
- 第 685 页的 [logout.aspx](#)
- 第 693 页的 [myvars.aspx](#)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDb" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

    LHMResult.Text=""
    catchError.Text=""

    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
```

```

ufi=Request.QueryString("ufi")
mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
clientRedirectUrl=Request.QueryString("clientRedirectUrl")
req=Request.QueryString("req")
hmac=Request.QueryString("hmac")
customCode=Request.QueryString("cc")

'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
If customCode <> "" Then
    Select Case customCode
        Case "2"
            LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
        Case "3"
            LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
        Case "4"
            LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
    End Select
End If

'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
If hmac <> "" Then

    'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
    req=Replace(req,"%","%25")
    req=Replace(req,":","%3A")
    req=Replace(req," ","%20")
    req=Replace(req,"?","%3F")
    req=Replace(req, "+", "%2B")
    req=Replace(req, "&", "%26")
    req=Replace(req, "=", "%3D")

    Dim strHmacText as String
    Dim objCrypto as Object
    Dim strHmacGenerated
    Dim loginError as String

    'Initialize the Crypto object
    objCrypto = Server.CreateObject("SonicSSL.Crypto")

    'The text to be encoded
    strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

    'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.

```

```

    'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
    If hmacType = "MD5" Then
        strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
    Else
        strHmacGenerated = objCrypto.hmac_shal(strHmacText, strHmac)
    End If

    If strHmacGenerated <> hmac Then
        Dim hmacFail as String
        hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
        hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
        hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
        hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
        catchError.Text=hmacFail
    End If

End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
    txtName.Text = ""
    txtAddress.Text = ""
    txtCity.Text = ""
    txtState.Text = ""
    txtZip.Text = ""
    txtPhone.Text = ""
    txtEMail.Text = ""
    txtURL.Text = ""
    txtComment.Text = ""
    LHMResult.Text=""
    catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    Try
        'Try to write the submitted info to the database file
        Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

        Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
',' & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
        Dim MyConn as New OleDbConnection (strConn)
        Dim cmd as New OleDbCommand (MySQL, MyConn)
        MyConn.Open ()
        cmd.ExecuteNonQuery ()
        MyConn.Close ()

        Catch ex as Exception
            catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        End Try
    End Try

```



```

'Let the user know that we are setting up the session, just in case it takes more
than a second
LHMResult.Text = "Authorizing session. Please wait."

'The LHM cgi on the SonicWALL - this does not change
Dim loginCgi as String = "externalGuestLogin.cgi"

'Assemble the data to post back to the SonicWALL to authorize the LHM session
Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

'Combine mgmtBaseUrl from the original redirect with the login cgi
Dim postToSNWL as String = mgmtBaseUrl & loginCgi

'Convert the loginParams to a well behaved byte array
Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

Try
'Create the webrequest to the SonicWALL
Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

'Calculate the length of the byte array
toSNWL.ContentLength = byteArray.Length

'Set the method for the webrequest to POST
toSNWL.Method = "POST"

'Set the content type
toSNWL.ContentType = "application/x-www-form-urlencoded"

'Open the request stream
Dim dataStream As Stream = toSNWL.GetRequestStream()

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the XPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 50 - Login Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

'Do we want to provide a logout popup window?
If logoutPopup = "1" Then

```

```

'Popup hack using Javascript for logout window
Dim sb As New System.Text.StringBuilder()
sb.Append("<script language='javascript'>")
sb.Append("window.open('logout.aspx?sessId=")
sb.Append(Server.URLEncode(CStr(sessionId)))
sb.Append("&mgmtBaseUrl=")
sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
sb.Append("&sessTimer=")
sb.Append(Server.URLEncode(CStr(sessTimer)))
sb.Append("'", 'logOut', 'toolbar=no,")
sb.Append("addressbar=no,menubar=no,")
sb.Append("width=400,height=250');")
sb.Append("<")
sb.Append("/")
sb.Append("</script>")
RegisterStartupScript("stp", sb.ToString)
End If

LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href="" & req & "">" & req & "</a>"

'Response code 51 - Session Limit Exceeded
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 100 - Login Failed.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

End If

```

```

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
    End Try
End Sub
</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    background-color: #006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan="3" align="center"><font color="white">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
        <td><center></center></td>
        <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
    </tr>
    <tr class="heading">
        <td colspan="3" align="center"><font color="white">&nbsp;</td>
    </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
    <tr>

```

```

        <td>Welcome <%= ip%> to SonicWALL's LHM Guestbook. In exchange for providing us
with your contact information,
        along with your permission to occasionally contact you while you are in the
middle of dinner, we will
        provide you with <b>one complimentary hour of secure internet access.</b><br>
</td>
</tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
    </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
    <tr>
        <td width="30%"><br>Enter your full name:</td>
        <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
        <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
    </tr>
    <tr>
        <td width="30%"><br>Enter your address:</td>
        <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
        <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
    </tr>
    <tr>
        <td width="30%"><br>Enter your city:</td>
        <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
        <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
    </tr>
    <tr>
        <td width="30%"><br>Enter your State:</td>
        <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
        <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
    </tr>
    <tr>
        <td width="30%"><br>Enter your zip code:</td>
        <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
        <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip code."
Display="Dynamic" runat="server" />
        <asp:RegularExpressionValidator id="regEx1" runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="\d{5}"></asp:RegularExpressionValidator>
    </td>
    </tr>
    <tr>
        <td width="30%"><br>Enter your phone number:</td>
        <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
        <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone number."
Display="Dynamic" runat="server" />

```



```

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

    LHMResult.Text=""
    catchError.Text=""

    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
    ufi=Request.QueryString("ufi")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    clientRedirectUrl=Request.QueryString("clientRedirectUrl")
    req=Request.QueryString("req")
    hmac=Request.QueryString("hmac")
    customCode=Request.QueryString("cc")

    'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
    'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
    If customCode <> "" Then
        Select Case customCode
            Case "2"
                LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
            Case "3"
                LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
            Case "4"

```

```

        LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
    End Select
End If

'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
If hmac <> "" Then

    'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
    req=Replace(req,"%","%25")
    req=Replace(req,":","%3A")
    req=Replace(req," ","%20")
    req=Replace(req,"?","%3F")
    req=Replace(req, "+", "%2B")
    req=Replace(req, "&", "%26")
    req=Replace(req, "=", "%3D")

    Dim strHmacText as String
    Dim objCrypto as Object
    Dim strHmacGenerated
    Dim loginError as String

    'Initialize the Crypto object
    objCrypto = Server.CreateObject("SonicSSL.Crypto")

    'The text to be encoded
    strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

    'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
    'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
    If hmacType = "MD5" Then
        strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
    Else
        strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
    End If

    If strHmacGenerated <> hmac Then
        Dim hmacFail as String
        hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
        hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
        hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
        hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
        catchError.Text=hmacFail
    End If

```

```

End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
    txtName.Text = ""
    txtAddress.Text = ""
    txtCity.Text = ""
    txtState.Text = ""
    txtZip.Text = ""
    txtPhone.Text = ""
    txtEMail.Text = ""
    txtURL.Text = ""
    txtComment.Text = ""
    LHMResult.Text=""
    catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    Try
        'Try to write the submitted info to the database file
        Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

        Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES (' & txtName.Text & ',' & txtAddress.Text &
',' & txtCity.Text & ',' & txtState.Text & ',' & txtZip.Text & ',' &
txtPhone.Text & ',' & txtEMail.Text & ',' & txtURL.Text & ',' &
txtComment.Text & ')"
        Dim MyConn as New OleDbConnection (strConn)
        Dim cmd as New OleDbCommand (MySQL, MyConn)
        MyConn.Open ()
        cmd.ExecuteNonQuery ()
        MyConn.Close ()

        Catch ex as Exception
            catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        End Try

        'Let the user know that we are setting up the session, just in case it takes more
than a second
        LHMResult.Text = "Authorizing session. Please wait."

        'The LHM cgi on the SonicWALL - this does not change
        Dim loginCgi as String = "externalGuestLogin.cgi"

        'Assemble the data to post back to the SonicWALL to authorize the LHM session
        Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

        'Combine mgmtBaseUrl from the original redirect with the login cgi
        Dim postToSNWL as String = mgmtBaseUrl & loginCgi

        'Convert the loginParams to a well behaved byte array
        Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try
        'Create the webrequest to the SonicWALL
        Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

```



```

'Calculate the length of the byte array
toSNWL.ContentLength = byteArray.Length

'Set the method for the webrequest to POST
toSNWL.Method = "POST"

'Set the content type
toSNWL.ContentType = "application/x-www-form-urlencoded"

'Open the request stream
Dim dataStream As Stream = toSNWL.GetRequestStream()

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 50 - Login Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

'Do we want to provide a logout popup window?
If logoutPopup = "1" Then
    'Popup hack using Javascript for logout window
    Dim sb As New System.Text.StringBuilder()
    sb.Append("<script language='javascript'>")
    sb.Append("window.open('logout.aspx?sessId=")
    sb.Append(Server.URLEncode(CStr(sessionId)))
    sb.Append("&mgmtBaseUrl=")
    sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
    sb.Append("&sessTimer=")
    sb.Append(Server.URLEncode(CStr(sessTimer)))
    sb.Append(", 'logOut', 'toolbar=no,")
    sb.Append("addressbar=no,menubar=no,")
    sb.Append("width=400,height=250');")
    sb.Append("<")
    sb.Append("/")
    sb.Append(">script>")
    RegisterStartupScript("stp", sb.ToString)
End If

LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href="" & req & """"> & req & """"></a>"

```

```

'Response code 51 - Session Limit Exceeded
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
    LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 100 - Login Failed.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
End Try
End Sub
</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;

```

```

    background-color:#9CBACE;
}

tr.heading {
    background-color:#006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
    <td align="center"></center></td>
    <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
  </tr>
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
  <tr>
    <td>Welcome <%= ip%> to SonicWALL's LHM Guestbook. In exchange for providing us
with your contact information,
    along with your permission to occasionally contact you while you are in the
middle of dinner, we will
    provide you with <b>one complimentary hour of secure internet access.</b><br>
    </td>
  </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
  </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
    <td width="30%"><br>Enter your full name:</td>
    <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
    <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
  </tr>

```

```

<tr>
  <td width="30%"><br>Enter your address:</td>
  <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
  <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
</tr>
<tr>
  <td width="30%"><br>Enter your city:</td>
  <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
  <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
</tr>
<tr>
  <td width="30%"><br>Enter your State:</td>
  <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
  <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
</tr>
<tr>
  <td width="30%"><br>Enter your zip code:</td>
  <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
  <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip code."
Display="Dynamic" runat="server" />
  <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
</td>
</tr>
<tr>
  <td width="30%"><br>Enter your phone number:</td>
  <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
  <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone number."
Display="Dynamic" runat="server" />
  <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\d{3}\d?) | (\d{3}-))?\d{3}-
\d{4}"></asp:RegularExpressionValidator>
</td>
</tr>
<tr>
  <td width="30%"><br>Enter your email address:</td>
  <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
  <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*" ErrorMessage="Please
enter a valid email address." Display="Dynamic" />
  </asp:RegularExpressionValidator>
  <asp:RequiredFieldValidator id="valTxtEmail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email address."
Display="Dynamic" />
  </asp:RequiredFieldValidator>
</td>
</tr>
<tr>
  <td width="30%"><br>Enter your web site URL (optional):</td>
  <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
</tr>

```


LHMQuiz 脚本

验证模式	访客客户端进行测验。通过分数作为验证凭据
目的	通常在教室环境中提供网络访问。通过使用对所教材料的测试通过分数作为验证方法，教师可以确保在互联网的不可抗拒的诱惑转移注意力之前掌握课程材料。该脚本还通过电子邮件向接受测试者发送完成的通过测试，并向监考官/教师发送未通过的测试。
myvars 变量	<p>logoutPopup 控制注销弹出窗口的使用。设置为：</p> <ul style="list-style-type: none">• 0 以禁用弹出窗口。• 1 以启用弹出窗口。 <p>passingScore 通过测验所需的分数（代表百分比的整数）。</p> <p>quizFile 测验的 XML 源的文件名（例如 quiz.xml、shortquiz.xml）。</p> <p>quizName 整个脚本中使用的测验名称。</p> <p>quizFrom 用电子邮件发送测验时使用的 From: email 地址。</p> <p>quizTo 发送未通过的测验的 To: email 地址（如测试监考官或教师）。</p> <p>imagePath 电子邮件包含正确和错误答案的附件。这将设置这些图像文件的路径。这通常设置为脚本文件本身的路径。</p> <p>smtpServer 用于测验结果传达的 SMTP 服务器的 IP 地址或可解析的 FQDN。如果要使用本地 IIS SMTP 服务器实例，可以将其设置为 127.0.0.1。</p> <p>sessTimer 会话计时器，以秒为单位。</p> <p>idleTimer 闲置计时器，以秒为单位。</p> <p>strHmac 可选 HMAC 功能的共享密钥。</p> <p>hmacType HMAC 在使用中时使用的摘要类型：MD5 或 SHA1。</p> <p>logo 要在页眉上使用的徽标（图像）文件的名称。</p>
会话流程	<ol style="list-style-type: none">1 提示访客客户端输入他们的全名和电子邮件地址。传送完成的通过测验需要正确/有效的电子邮件地址。2 输入姓名和电子邮件后，访客客户端将重定向到 quiz.aspx 页面。此页面是管理多项选择测试的地方。3 测试问题本身包含在 quiz.xml 文件中，由 quiz.xsd (XML 架构定义) 文件定义。可以且应该编辑 quiz.xml 文件以自定义测验，但除非绝对必要，否则不得编辑 quiz.xsd 文档。 包括两个版本的测验：quiz.xml（包含 10 个问题）和 shortquiz.xml（包含 2 个问题，用于测试脚本的工作原理）。测验支持任何数量的问题，每个问题都支持任何数量的答案，必须通过 correct=yes 将其中一个答案标明为正确答案。根据需要修改提供的 quiz.xml 文件应该是相当简单的。

- 4 在测验结束时，显示结果。如果是：
 - 未通过分数，则将测试结果通过电子邮件发送给教师（myvars 中定义的电子邮件地址），并提示访客客户端再次进行测试。LHM 会话未获授权。
 - 通过分数，则将测试结果通过电子邮件发送给测试者，LHM 会话获得授权。
 通过电子邮件发送的测试为 HTML 格式且包含 checkmark.gif 和 block.gif（正确和错误）图形，以附件形式显示在电子邮件中。
- 5 如果测试通过，LHM POST 字符串与 sessionID、用户名（如 Web 表单中所提供）、默认会话生命周期和闲置生命周期组合在一起。
- 6 该脚本执行到 SonicWall 安全设备的 LHM POST 以授权会话。

其他注意事项

传送测试结果需要访问 SMTP 服务器。由于脚本正在通过服务器中继邮件，因此需要配置 SMTP 服务器以允许从 LHM 服务器进行中继。最好通过配置 SMTP 服务器来允许从 LHM 服务器的 IP 地址进行中继来实现。

大多数 IIS 安装包括本地 SMTP 服务器，因此通过将 myvars 中的 smtpServer 变量配置为 127.0.0.1 可以方便地使用本地 SMTP 服务器进行邮件传送。

即使使用本地 SMTP 服务器进行邮件传送，也需要允许中继。在大多数配置中，这通过以下方式执行：

- 1 进入 IIS MMC 配置器。
- 2 右键单击默认 SMTP 虚拟服务器。
- 3 选择属性。
- 4 选择访问选项卡。
- 5 单击中继按钮。
- 6 将 127.0.0.1 添加到访问许可列表。

当使用非本地 SMTP 服务器时，应将 SMTP 服务器配置为允许 LHM 服务器通过其实际 IP 地址进行中继。

主题：

- 第 695 页的 [default.aspx](#)
- 第 699 页的 [logout.aspx](#)
- 第 705 页的 [myvars.aspx](#)
- 第 706 页的 [quiz.aspx](#)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>

<!-- #INCLUDE file="myvars.aspx" -->

<script runat="server">

'Sample LHM redirect querystring:
'http://10.50.165.231/xmlquiz/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b100
4f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.
50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.goog
le.com/ig

Dim ip as String
Dim sessionId as String
```

```

Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim emailAddr as String
Dim userName as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)
    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
    ufi=Request.QueryString("ufi")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    clientRedirectUrl=Request.QueryString("clientRedirectUrl")
    req=Request.QueryString("req")
    hmac=Request.QueryString("hmac")
    customCode=Request.QueryString("cc")

    'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
    you to use the same
    'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
    (?cc=3) and "Max Sessions" (?cc=4) page.
    If customCode <> "" Then
        Select Case customCode
            Case "2"
                LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
                You may try to initiate a new session.</font></H3>"
            Case "3"
                LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
                timeout. Please log back in.</font></H3>"
            Case "4"
                LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
                has been reached. Please try again later.</font></H3>"
        End Select
    End If

    'Note - the routine below for handling the hmac requires the use of the
    SonicSSL.dll and libeay.dll libraries.
    'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
    with "regsvr32 sonicssl.dll"
    If hmac <> "" Then

        'SonicWALL URL Encode routine is different from Microsoft - this is the
        SonicWALL method
        req=Replace(req,"%","%25")
        req=Replace(req,":","%3A")
        req=Replace(req," ","%20")
        req=Replace(req,"?","%3F")
        req=Replace(req, "+", "%2B")
        req=Replace(req, "&", "%26")
        req=Replace(req, "=", "%3D")

        Dim strHmacText as String
        Dim objCrypto as Object
        Dim strHmacGenerated
        Dim loginError as String

        'Initialize the Crypto object

```



```

objCrypto = Server.CreateObject("SonicSSL.Crypto")

'The text to be encoded
strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
If hmacType = "MD5" Then
    strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
Else
    strHmacGenerated = objCrypto.hmac_shal(strHmacText, strHmac)
End If

If strHmacGenerated <> hmac Then
    Dim hmacFail as String
    hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
    hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
    hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
    hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
    catchError.Text=hmacFail
End If

End If

End Sub

'When the submit button is clicked, pass the variables we need and load the quiz
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    Context.Items.Add("req", req)
    Context.Items.Add("sessionId", sessionId)
    Context.Items.Add("emailAddr", clientEmail.Text)
    Context.Items.Add("userName", clientName.Text)
    Context.Items.Add("mgmtBaseUrl", mgmtBaseUrl)
    Server.Transfer("quiz.aspx", true)

End Sub

</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    background-color: #006699;
}

.button {
    border: 1px solid #000000;

```

```

    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td width="50%" valign="center"><font color="white"><b>LHM Quiz
Authorization</b></font></td>
    <td><center></center></td>
    <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
  </tr>
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr>
    <td width="30%"><br>Enter your full name:</td>
    <td width="20%"><asp:TextBox id="clientName" runat="server" /></td>
    <td ><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="clientName" ErrorMessage="Please enter your name."
Display="Dynamic" runat="server" /></td>
  </tr>
  <tr>
    <td width="30%"><br>Enter your real email address:</td>
    <td width="20%"><asp:TextBox id="clientEmail" runat="server" /></td>
    <td ><asp:RegularExpressionValidator id="fromEmail" runat="server"
ControlToValidate="clientEmail" ValidationExpression=".*@.*\..*"
ErrorMessage="Please enter a valid email address." Display="Dynamic" />
</asp:RegularExpressionValidator>
    <asp:RequiredFieldValidator id="fromRequired" runat="server"
ControlToValidate="clientEmail" ErrorMessage="Please enter your email address."
Display="Dynamic" />
</asp:RequiredFieldValidator>
  </td>
  </tr>
  <tr>
    <td><asp:button id="btnSubmit" class="button" text=" Submit "
onClick="btnSubmit_Click" runat="server" /><br></td>
  </tr>

  <tr class="heading">
    <td colspan=3 align="left"><font color="white"><b>Welcome Quiztaker <%=
ip%></b></font></td>
  </tr>
</table>
<table width="70%" border="0" cellpadding="2" cellspacing="0">
  <tr>

```

```

        <td>
        <br>You have been redirected here by Lightweight Hotspot Messaging.
        This environment has been setup to demonstrate the flexibility of LHM,
including
        support for both wired and wireless clients, and also the ability for LHM to
use
        more than just username and password authentication for providing
access.<br><br>
        The page that you are about to continue on to is a <%= quizName %> written in
ASP.net.
        A passing score of <%= passingScore%>% will serve as the authentication for
LHM, and will grant
        you network access. You must pass the test to continue, and will be prompted to
retake
        the entire quiz if you you do not pass. <br><br>
        When you are done, the completed test will be emailed to you at the address you
specify above.<br><br>
        So it's not just a good way to prove your understanding of some
key SonicOS concepts, but also a practical example of the versatility of LHM.
        </td>
</tr>
<tr>
        <td><asp:Label id=LHMResult runat="server" /></td>
</tr>
<tr>
        <td colspan=2><asp:Label id=catchError runat="server" /></td>
</tr>
</table>
</form>
</BODY>
</HTML>

```

logout.aspx

```

<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

Dim sessionId as String

```

```

Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
    sessionId=Request.QueryString("sessId")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    sessTimer=Request.QueryString("sessTimer")

    'Use the override class in myvars.aspx to accept untrusted certificates from the
    SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'When the page loads, make the loggedIn span visible
    loggedIn.Visible=True
    loggedOut.Visible=False

    Me.Button1.Attributes.Add("OnClick", "self.close()")
End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    'Let the user know that we are setting up the session, just in case it takes more
    than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogoff.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & eventId

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try
        'Make the loggedOut span visible
        loggedIn.Visible=False
        loggedOut.Visible=True

        'Create the webrequest to the SonicWALL
        Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

        'Calculate the length of the byte array
        toSNWL.ContentLength = byteArray.Length

        'Set the method for the webrequest to POST
        toSNWL.Method = "POST"

        'Set the content type
        toSNWL.ContentType = "application/x-www-form-urlencoded"

        'Open the request stream
        Dim dataStream As Stream = toSNWL.GetRequestStream()

```

```

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 150 - Logout Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
    LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception

```

```

        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
    End Try
End Sub

</script>
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;
    background-color:#9CBACE;
}

tr.heading {
    font-size: 10pt;
    background-color:#006699;
}

tr.smalltext {
    font-size: 8pt;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
    font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
    clockStr="";

    dayStr=Math.floor(SecondsToCountDown/86400)%100000
    if(dayStr>0){
        if(dayStr>1){
            dayStr+=" days ";
        } else dayStr+=" day ";
        clockStr=dayStr;
    }
    hourStr=Math.floor(SecondsToCountDown/3600)%24
    if(hourStr>0){
        if(hourStr>1){
            hourStr+=" hours ";
        } else hourStr+=" hour ";
        clockStr+=hourStr;
    }
}

```

```

minuteStr=Math.floor(SecondsToCountDown/60)%60
if(minuteStr>0){
    if(minuteStr>1){
        minuteStr+=" minutes ";
    } else minuteStr+=" minute ";
    clockStr+=minuteStr;
}
secondStr=Math.floor(SecondsToCountDown/1)%60
if(secondStr>0){
    if(secondStr>1){
        secondStr+=" seconds ";
    } else secondStr+=" second ";
    clockStr+=secondStr;
}

if(SecondsToCountDown > 0)
{
    --SecondsToCountDown;
}

if(originalTime.length < 2)
{
    originalTime = clockStr;
}

// Make sure the form is still there before trying to set a value
if(document.frmValidator){
    document.frmValidator.originalTime.value = originalTime;
    document.frmValidator.countdown.value = clockStr;
}

setTimeout("CountDown()", 1000);
if(SecondsToCountDown == 0)
{
    document.frmValidator.countdown.value = "Session Expired";
}
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
    return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
    var key_f5 = 116;
    if (key_f5==event.keyCode)
    {
        event.keyCode=0;
        return false;
    }
    return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

```

```

</SCRIPT>

</HEAD>

<BODY onload='CountDown() '>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;&nbsp;&nbsp;</td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;&nbsp;&nbsp;</td>
  </tr>
  <tr class="smalltext"><td><br></td></tr>
  <tr class="smalltext">
    <td>Original Session Time:</td>
    <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
  </tr>
  <tr class="smalltext">
    <td>Remaining Session Time:</td>
    <td><asp:textbox width=250 id="countdown" runat="server" /></td>
  </tr>
  <tr class="smalltext">
    <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
  </td>
  <tr>
    <td colspan=2><center><asp:button id="btnSubmit" class="button" text=" Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
  </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;&nbsp;&nbsp;</td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;&nbsp;&nbsp;</td>
  </tr>
  <tr>
    <td><asp:Label id=LHMResult runat="server" /></td>
  </tr>
  <tr>
    <td><asp:Label id=catchError runat="server" /></td>
  </tr>
  <tr><td><br></td></tr>
  <tr>

```



```

        <td><center><asp:button id="Button1" class="button" text=" Close "
runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

</BODY>
</HTML>

```

myvars.aspx

```

<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the passing score
Dim passingScore as Integer = 80

'Set the filename of the quiz XML source
Dim quizFile as String = "quiz.xml"
'Dim quizFile as String = "shortquiz.xml"

'Set the name of the Quiz
Dim quizName as String = "SonicOS Quiz"

'Set the emailed quiz results "from" email address
Dim quizFrom as String = "joelevy@sonicwall.com"

'Set the email address to send failed test results to (the proctor/instructor)
Dim quizTo as String = "joelevy@sonicwall.com"

'Set the path for check and block embedded images - usually the same path as the quiz
Dim imagePath as String = "C:\inetpub\wwwroot\lhm\lhmquiz\"

'Set the IP or resolvable FQDN for the SMTP Server
'Make sure the server is configured to relay from the IP address of this server
'If setting to 127.0.0.1 (local IIS SMTP), you need to allow IIS SMTP to relay from
127.0.0.1
Dim smtpServer as String = "127.0.0.1"

'Set the LHM Session Timeout
Dim sessTimer as String = "86400"

'Set the LHM Idle Timeout
Dim idleTimer as String = "3600"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

```

```
'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'-----End of Configurable Settings-----

</script>
```

quiz.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Import Namespace="System.Web" %>
<%@ Import Namespace="System.Web.Mail" %>

<!-- Original quiz code from www.codeproject.com -->

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Set the path to the XML quiz data
Dim strXmlFilePath as String = Server.MapPath(quizFile)

'Setup our variables
Dim emailAddr as String
Dim userName as String
Dim req as String
Dim sessionId as String
Dim mgmtBaseUrl as String
Dim xDoc as XmlDocument = New XmlDocument()
Dim intTotalQuestion as Integer
Dim intQuestionNo as Integer = 1
Dim intScore as Integer = 0
Dim arrAnswerHistory as new ArrayList()
Dim arrRightOrWrong as new ArrayList()
Dim arrCorrect as new ArrayList()

Sub Page_Load(src as Object, e as EventArgs)

    LHMResult.Text=""
    catchError.Text=""
```

```

'Grab context items set in default.aspx
emailAddr = Context.Items("emailAddr")
userName = Context.Items("userName")
req = Context.Items("req")
sessionId = Context.Items("sessionId")
mgmtBaseUrl = Context.Items("mgmtBaseUrl")

'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

'Load xml data
xDoc.Load(strXmlFilePath)

'Start a new quiz?
If Not Page.IsPostBack Then

    'Yes. Count total question
    intTotalQuestion = xDoc.SelectNodes("/quiz/mchoice").Count

    'Record start time
    ViewState("StartTime") = DateTime.Now

    ShowQuestion(intQuestionNo)
End If
End Sub

Sub btnSubmit_Click(src as Object, e as EventArgs)

    'Retrieve variables from ViewState
    intTotalQuestion = ViewState("TotalQuestion")
    intQuestionNo = ViewState("QuestionNo")
    intScore = ViewState("Score")
    arrAnswerHistory = ViewState("AnswerHistory")
    arrRightOrWrong = ViewState("RightOrWrong")
    arrCorrect = ViewState("AnswerList")
    req = ViewState("origReq")
    userName = ViewState("origUserName")
    emailAddr = ViewState("origEmailAddr")
    mgmtBaseUrl = ViewState("mgmtUrl")
    sessionId = ViewState("sessID")

    'Correct answer?
    If rblAnswer.SelectedItem.Value = ViewState("CorrectAnswer") Then
        intScore += 1
        arrRightOrWrong.Add(0)
    Else
        arrRightOrWrong.Add(rblAnswer.SelectedItem.Value)
    End If

    'Remember all selected answers
    arrAnswerHistory.Add(rblAnswer.SelectedItem.Value)
    arrCorrect.Add(ViewState("CorrectAnswer"))

    'End of quiz?
    If intQuestionNo=intTotalQuestion Then

        'Yes. Show the result.
        QuizScreen.Visible = False
        ResultScreen.Visible = True

```

```

        'Render result screen
        ShowResult()

Else

    'Not yet. Show another question.
    QuizScreen.Visible = True
    ResultScreen.Visible = False
    intQuestionNo += 1

    'Render next question
    ShowQuestion(intQuestionNo)
End If
End Sub

Sub ShowQuestion(intQuestionNo as Integer)
    Dim xNodeList as XmlNodeList
    Dim xNodeAttr as Object
    Dim strXPath as String
    Dim i as Integer
    Dim tsTimeSpent as TimeSpan

    strXPath = "/quiz/mchoice[" & intQuestionNo.ToString() & "]"

    'Extract question
    lblQuestion.Text = intQuestionNo.ToString() & ". " &
xDoc.SelectSingleNode(strXPath & "/question").InnerText

    'Extract answers
    xNodeList = xDoc.SelectNodes(strXPath & "/answer")

    'Clear previous listitems
    rblAnswer.Items.Clear

    For i = 0 to xNodeList.Count-1

        'Add item to radiobuttonlist
        rblAnswer.Items.Add(new ListItem(xNodeList.Item(i).InnerText, i+1))

        'Extract correct answer
        xNodeAttr = xNodeList.Item(i).Attributes.ItemOf("correct")
        If not xNodeAttr is Nothing Then
            If xNodeAttr.Value = "yes" Then
                ViewState("CorrectAnswer") = i+1
            End If
        End If
    Next

    'Output Total Question and passing score
    lblTotalQuestion.Text = intTotalQuestion
    lblPassingScore.Text = passingScore

    'Output Time Spent
    tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))
    lblTimeSpent.Text = tsTimeSpent.Minutes.ToString() & ":" &
tsTimeSpent.Seconds.ToString()

    'Store data to viewstate
    ViewState("TotalQuestion") = intTotalQuestion
    ViewState("Score") = intScore

```

```

ViewState("QuestionNo") = intQuestionNo
ViewState("AnswerHistory") = arrAnswerHistory
ViewState("RightOrWrong") = arrRightOrWrong
ViewState("AnswerList") = arrCorrect
ViewState("origReq")=req
ViewState("origUserName")=userName
ViewState("origEmailAddr")=emailAddr
ViewState("mgmtUrl")=mgmtBaseUrl
ViewState("sessID")=sessionID

End Sub

Sub ShowResult()
    Dim strResult as String
    Dim intCompetency as Integer
    Dim i as Integer
    Dim strXPath as String
    Dim tsTimeSpent as TimeSpan

    tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))

    strResult = "<center>"

    if passingScore <= Int(intScore/intTotalQuestion*100).ToString()
        strResult += "<h2><font color=""green"">You Passed!</h3></font>"
    else
        strResult += "<h2><font color=""red"">You Failed!</h3><b>Please review the
answers and retake the test.</b><br></font>"
    End If

    strResult += "User Name: " & userName & "<br>"
    strResult += "Elapsed Time: " & tsTimeSpent.Minutes.ToString() & ":" &
tsTimeSpent.Seconds.ToString() & "<br>"
    strResult += "Correct Answers: " & intScore.ToString() & " out of " &
intTotalQuestion.ToString() & "<br>"
    strResult += "Your Percentage: " & Int(intScore/intTotalQuestion*100).ToString()
& "%<br>"
    strResult += "Required Percentage:" & passingScore.ToString() & "%<br>"
    strResult += "</center>"

    strResult += "<h3>Quiz Results</h3>"
    For i = 1 to intTotalQuestion
        strXPath = "/quiz/mchoice[" & i.ToString() & "]"
        strResult += "<b>" & i.ToString() & ". " & xDoc.SelectNodes(strXPath &
"/question").Item(0).InnerXml & "</b><br>"
        If arrRightOrWrong.Item(i-1)=0 Then
            strResult += "<img src = ""checkMark.gif""><font color=""green"">&nbsp;"
            strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
        Else
            strResult += "<img src = ""Block.gif""><font color=""red"">&nbsp;"
            strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml & "<br>"
            strResult += "The correct anwer is: " & xDoc.SelectNodes(strXPath &
"/answer[" & arrCorrect.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
        End If
    Next

    'Setup the common Mail settings

```

```

Dim objMail As MailMessage
objMail = New MailMessage()
objMail.From = quizFrom
objMail.Body = strResult
objMail.BodyFormat = MailFormat.Html

'Path to the attachments for the Check and X images - update these in myvars.aspx
objMail.Attachments.Add(New MailAttachment(imagePath & "block.gif"))
objMail.Attachments.Add(New MailAttachment(imagePath & "checkMark.gif"))

'Address of the SMTP server - can be localhost if SMTP is running on IIS - in
myvars.aspx
SmtpMail.SmtpServer = smtpServer

'Determine pass/fail
If passingScore <= Int(intScore/intTotalQuestion*100).ToString()

    'Mail the passing test result to the test-taker
    'Be sure to update the mail fields in myvars.aspx
    objMail.To =emailAddr
    objMail.Subject = quizName & " Results for " & emailAddr

    'Send the mail
    SmtpMail.Send(objMail)
    strResult += "Your test is being emailed to you at " & emailAddr

    'Send the session Auth message to LHM
    postLHM()

else
    'Mail failing test results to the instuctor
    objMail.To =quizTo
    objMail.Subject = "Failing " & quizName & " Test Results for " & emailAddr

    'Send the mail
    SmtpMail.Send(objMail)
    strResult += "<a href=""quiz.aspx"">Click here to retake the quiz</a>"
End If

'Write it
lblResult.Text = strResult

End Sub

Sub postLHM()

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogin.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try

```

```

'Let the user know that we are setting up the session, just in case it takes
more than a second
LHMResult.Text = "Authorizing session. Please wait."

'Create the webrequest to the SonicWALL
Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

'Calculate the length of the byte array
toSNWL.ContentLength = byteArray.Length

'Set the method for the webrequest to POST
toSNWL.Method = "POST"

'Set the content type
toSNWL.ContentType = "application/x-www-form-urlencoded"

'Open the request stream
Dim dataStream As Stream = toSNWL.GetRequestStream()

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

'Response code 50 - Login Succeeded

If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

'Do we want to provide a logout popup window?
If logoutPopup = "1" Then
'Popup hack using Javascript for logout window
Dim sb As New System.Text.StringBuilder()
sb.Append("<script language='javascript'>")
sb.Append("window.open('logout.aspx?sessId=")
sb.Append(Server.URLEncode(CStr(sessionId)))
sb.Append("&mgmtBaseUrl=")
sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
sb.Append("&sessTimer=")
sb.Append(Server.URLEncode(CStr(sessTimer)))
sb.Append("'", 'logOut', 'toolbar=no,")
sb.Append("addressbar=no,menubar=no,")
sb.Append("width=400,height=250');")
sb.Append("<")
sb.Append("/")
sb.Append("<script>")
RegisterStartupScript("stp", sb.ToString)

```

```

End If

LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href="" & req & "">" & req & ""</a>"

'Response code 51 - Session Limit Exceeded
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
    LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 100 - Login Failed.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it
'in the same color as the background, but still show the quiz results.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
End Try
End Sub

</script>

```



```

<html>
<head>
<title><%= quizName %> </title>
</head>
<style>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    background-color: #006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</style>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<body>
<span id="QuizScreen" runat="server">
<form runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan="3" align="center"><font color="white">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td width="50%" valign="center"><font color="white"><b><%= quizName %> - <%=
userName%></b></font></td>
        <td align="center"></center></td>
        <td width="50%" align="right" valign="center"><font color="white"><b>This quiz
has <asp:label id="lblTotalQuestion" runat="server" /> questions</b></font></td>
    </tr>
    <tr class="heading">
        <td colspan="3" align="center"><font color="white">&nbsp;</td>
    </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr>
        <td colspan="2">
            <b><asp:label id="lblQuestion" runat="server" /></b><br>
            <asp:radiobuttonlist id="rblAnswer" RepeatDirection="vertical"
TextAlign="right" RepeatLayout="table" runat="server" /><br>
            <asp:button id="btnSubmit" class="button" text=" Submit "
onClick="btnSubmit_Click" runat="server" />
            <asp:requiredfieldvalidator ControlToValidate="rblAnswer"
ErrorMessage="Please select an answer" runat="server" />
        </td>
    </tr>
    <tr class="heading">
        <td width="70%"><font color="white"><b>Score required to pass <asp:label
id="lblPassingScore" runat="server" />%</b></font></td>

```

```

        <td width="30%" align="right"><font color="white"><b>Time spent <asp:label
id="lblTimeSpent" runat="server" /></b></font></td>
    </tr>
</table>
</form>
</span>

<span id="ResultScreen" runat="server"> <asp:label id="lblResult" runat="server" />
<br>
<asp:Label id=LHMResult runat="server" />
<asp:Label id=catchError runat="server" />
</span>

</body>
</html>

```

PayPal 脚本

验证模式

访客通过**立即购买**按钮使用其 PayPal 帐户购买 1 小时或 24 小时访问权限。通过 PayPal 付款到热点提供商的 PayPal 商家帐户。

目的

几乎所有在互联网上购买或销售的人都使用 PayPal。设置买家帐户并将其链接到任何形式的付款（如信用卡、银行卡、支票账户）非常容易。

将仅限买家的帐户升级到商家帐户几乎同样容易。拥有商家帐户可使 PayPal 用户接受其他 PayPal 用户的货物或服务的付款。资金转帐通过 PayPal 运行，为商家提供在线业务，接受任何形式的付款方式，而无需设置任何复杂的付款处理方式。这消除了作为收费热点提供商的一个最大障碍。

Paypal 提供名为**立即购买**按钮的功能，允许进行一键交易。这些按钮是在 PayPal 的帮助下生成的，包含有关正在购买的商品或服务的信息的表单。当买方单击**立即购买**按钮时，会话将重定向到 PayPal 站点，其中 querystring 包含交易的所有详细信息（例如卖家、商品、价钱）。PayPal 脚本不使用基本的**立即购买**按钮（这是客户端而非服务器端代码），而是使用自定义的服务器端“立即购买”例程。

“立即购买”重定向中还包含自动返回的路径。自动返回是 PayPal 的一种功能，可在 PayPal 交易后使买方返回商家网站。使用 PDT (pdtPath, 如下所述) 需要自动返回。

自定义“立即购买”重定向还将 LHM sessionId 和 mgmtBaseUrl 嵌入到“立即购买”重定向的自定义字符串中。这允许我们跟踪会话，即使它离开 LHM 服务器，转到 PayPal，然后再返回（通过 PDT 的自动返回）。

基本的 PayPal 支付系统通过电子邮件向商家提供付款通知。对于实际货物，这是可以接受的，因为采购/运送交易不必实时发生；商家在运送产品之前可以等待几个小时或几天的通知。对于需要即时交付的交易，例如购买热点访问，需要更实时的付款方式。

PayPal 提供两种付款通知方式：

- 即时付款通知 (IPN)，由 PayPal 进行 Web 服务呼叫到商家网站，指示特定交易的付款已经结算。遗憾的是，这并不总是实时发生（这个异步通知可能需要 20 分钟才能到达），所以在此脚本中未使用它。（如需 IPN 的更多信息，请参阅 <https://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/ipn-intro-outside>）

- 付款数据传输（PDT：请参阅 <http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-intro-outside>）。此方法使用 PayPal 的自动返回方法，绝对实时发生。PDT 向商家提供交易状态（SUCCESS 或 FAIL）以及 payment_status（已完成、待处理、拒绝、失败、退款、撤销或取消_反转）的即时通知。通过立即了解交易的状态和付款，可以立即提供服务，不会有丢失付款的风险。

myvars 变量

logoutPopup	控制注销弹出窗口的使用。设置为： <ul style="list-style-type: none"> • 0 以禁用弹出窗口。 • 1 以启用弹出窗口。
debugFlag	设置 PayPal PDT 传输的调试输出： <ul style="list-style-type: none"> • 0 = 关 • 1 = 开
pdtPath	PDT 自动返回（在“目的”部分中描述）将访客客户端重定向到的路径。
paypalCGI	作为 PayPal 交易网关的 PayPal CGI 的 URL。URL 本身不应该更改，但有两个选项： <ul style="list-style-type: none"> • 实时（真实）PayPal 网站。 • PayPal 沙盒（PayPal 开发人员网络的一部分），可用于测试。
myBusiness	热点提供商的电子邮件地址（PayPal 识别企业的方式）。这必须与正在接收交易付款的商家帐户的电子邮件地址相匹配。
token	“付款数据传输”选项为每个商家生成唯一的令牌。在这里指定 PayPal 提供的唯一令牌。令牌必须正确，否则 PDT 交易（并非实际的 PayPal 交易）将失败。
itemName1 itemName2	两个访问选项的名称，例如 1 小时安全 Internet 访问和 24 小时安全 Internet 访问。
itemNumber1 itemNumber2	两个访问选项的项目编号（大多是任意内部的 PayPal 参考），例如 1hour 和 24hour。
itemTimer1 itemTimer2	两个访问选项的会话计时器（以秒为单位），例如 1 小时对应 3600，24 小时对应 86400。
itemAmount1 itemAmount2	两个访问选择的美元价格，例如 0.01（一美分）和 0.02（两美分）。限时促销优惠价。
itemButton1 itemButton2	两个访问选项的按钮文本，例如 1 Hour Access - \$0.01 和 24 Hours Access - \$0.02。
strHmac	可选 HMAC 功能的共享密钥。
hmacType	HMAC 在使用中时使用的摘要类型： MD5 或 SHA1 。
logo	要在页眉上使用的徽标（图像）文件的名称。

会话流程

- 1 访客启动他们的 Web 浏览器，并由 LHM 重定向到 `http://<lhmserver>/paypal/default.aspx`，其中 `<lhmserver>` 是您的 LHM 服务器。
- 2 访客（买家）单击其中一个**立即购买**按钮，例如 **1 Hour Access - \$0.01**。
- 3 该客户重定向至 PayPal 站点，`querystring` 包含有关商家、项目、LHM 会话（在自定义变量中）和自动返回 URL（在 `myvars` 中定义为 `pdtPath`）的所有信息。

`pdtPath` 驻留在 LHM 服务器上。该路径应与 `default.aspx` 路径（在 SonicWall 安全设备上配置）相同，但应指向 `pdt.aspx` 文件。这样，当 PayPal 交易完成并且 PayPal 将客户端重定向到商家站点时，客户端重定向回到 `http://<lhmserver>/paypal/pdt.aspx` 页面。

可以在 LHM 服务器上使用 HTTP，因为 LHM 服务器本身未输入敏感信息；PayPal 交易通过 HTTPS 直接在访客和 PayPal 之间进行。

“立即购买”重定向字符串示例：

```
https://www.sandbox.paypal.com/cgi-bin/webscr?cmd=_xclick&business=demo@sonicwall.com&item_name=1%20Hour%20Access&item_number=1hour&amount=0.01&currency_code=USD&lc=US&bn=PP-BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://lhmserverpaypal/default.aspx&return=http://lhmserver/lhm/paypal/pdt.aspx&custom=35378e67833faa3de83aa3b771https%3a%2f%2f172.16.17.1%3a4043%2f
```
- 4 访客登录到 PayPal（或根据需要创建新帐户），并使用 PayPal 完成交易。交易完成后，客户端将重定向回到 `http://<lhmserver>/paypal/pdt.aspx`。重定向中包含的 `querystring` 包含交易 ID (`tx`)、状态 (`st`)、金额 (`amt`)、货币类型 (`cc`)、自定义值 (`cm`) 和加密签名 (`sig`)。

重定向字符串示例：

```
http://lhmserver/lhm/paypal/pdt.aspx?tx=4LN76482JF4605045&st=Completed&amt=0.01&cc=USD&cm=35378e67833faa3b771https%3a%2f%2f172%2e16%2e17%2e1%3a4043%2f&sig=qdsNC4f1KwtPviggoGAXCpeV9gS%2f2E%2bGGVbTZ3STrUV1Ci9K3c2zTdJMuuKcmRiif1SybsZtUqDYqzzfMg64AF3PKCk85rrPubYT4K4aC
```
- 5 访问上面 URL 处的 `pdt.aspx` 脚本的访客在 LHM 服务器上启动 PDT 进程。该脚本构建了 `querystring`，其中包含 `cmd= notify-synch`（表示它是 PDT 交易）以及 `tx`（交易 ID）和 `at` 变量设置为商家的令牌（在 `myvars` 中定义）。然后将其发布到 `paypalCGI` URL（如 `myvars` 中所定义）。
- 6 PayPal 使用 SUCCESS 或 FAIL 代码来响应 POST。
 - FAIL — 脚本向客户指示 PayPal 交易失败，并提示他们寻求帮助。

•SUCCESS — 提供有关交易的详细信息:

```
SUCCESS
txn_type=web_accept
payment_date=00%3A39%3A48+Oct+30%2C+2005+PDT
last_name=Niqua1
item_name=1+Hour+Secure+Internet+Access
payment_gross=0.01
mc_currency=USD
business=lhmdemo%40sonicwall.com
payment_type=instant
payer_status=verified
tax=0.00
payer_email=lhmClient%40sonicwall.com
txn_id=84K306380G150640T
quantity=1
receiver_email=lhmdemo%40sonicwall.com
first_name=Sah
payer_id=XWRZGABD6UV2W
receiver_id=REW4W5WANU294
item_number=1hour
payment_status=Completed
payment_fee=0.01
mc_fee=0.01
shipping=0.00
mc_gross=0.01
custom=35378e67833faa3de833755d3aa3b771https%3A//172.16.17.1%3A4043/
charset=windows-1252
```

- 7 脚本检查 `payment_status` 以确保付款完成。如果未完成，则向用户提供未完成支付消息。
- 8 如果 `payment_status` 为已完成，脚本还会获取客户名称、项目名称、金额、交易 ID、业务和自定义变量，用于生成客户收据、LHM 会话的用户名，以及识别 LHM `sessionID` 和 `mgmtBaseUrl`。
- 9 该脚本将 PayPal 交易收据显示给访客。
- 10 该脚本执行到 SonicWall 安全设备的 LHM POST 以授权会话。

其他注意事项

需要 PayPal 商家帐号。

要求为自动返回和 PDT 设置 PayPal 帐户（请参阅

<http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside>）

对于测试，强烈建议通过 PayPal 开发人员网络

（<https://developer.paypal.com>）和（<https://www.sandbox.paypal.com>）设置（免费）PayPal 沙盒帐号。

重要：由于访客直接重定向到 PayPal 站点，所以必须 SonicWall 安全设备上设置所有 PayPal 站点 IP 地址作为“访客服务配置”中的允许网络。其中包括：

www.paypal.com

```
64.4.241.32
64.4.241.33
216.113.188.32
216.113.188.35
216.113.188.66
216.113.188.67
```

www.paypalobjects.com

```
216.113.188.25
64.4.241.62
216.113.188.9
```

www.sandbox.paypal.com

66.135.197.160

developer.paypal.com

66.135.197.163

主题:

- 第 718 页的 [default.aspx](#)
- 第 723 页的 [logout.aspx](#)
- 第 729 页的 [myvars.aspx](#)
- 第 730 页的 [pdt.aspx](#)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Note: For PayPal authorization to work, it is necessary to set up the PayPal sites
(www.paypal.com, www.paypalobjects.com, and www.sandbox.paypal.com) as a bypass
network on WGS. This is so that WGS/LHM users can access PayPal directly to complete
the payment transactions. This list currently includes the following addresses:
[64.4.241.32, 64.4.241.33, 216.113.188.32, 216.113.188.35, 216.113.188.66,
216.113.188.67], [216.113.188.25, 64.4.241.62, 216.113.188.9] and [66.135.197.160].

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
```

```

Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
    ufi=Request.QueryString("ufi")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    clientRedirectUrl=Request.QueryString("clientRedirectUrl")
    req=Request.QueryString("req")
    hmac=Request.QueryString("hmac")
    customCode=Request.QueryString("cc")

    'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
    you to use the same
    'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
    (?cc=3) and "Max Sessions" (?cc=4) page.
    If customCode <> "" Then
        Select Case customCode
            Case "2"
                LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
                You may try to initiate a new session.</font></H3>"
            Case "3"
                LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
                timeout. Please log back in.</font></H3>"
            Case "4"
                LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
                has been reached. Please try again later.</font></H3>"
        End Select
    End If

    'Set the button Text for the two buttons with the variable configured in myvars
    btnBuyNow1.Text=itemButton1
    btnBuyNow2.Text=itemButton2

    'Use the override class in myvars.aspx to accept untrusted certificates from the
    SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'Note - the routine below for handling the hmac requires the use of the
    SonicSSL.dll and libeay.dll libraries.
    'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
    with "regsvr32 sonicssl.dll"
    If hmac <> "" Then

        'SonicWALL URL Encode routine is different from Microsoft - this is the
        SonicWALL method
        req=Replace(req,"%","%25")
        req=Replace(req,":","%3A")
        req=Replace(req," ","%20")
        req=Replace(req,"?","%3F")
        req=Replace(req, "+", "%2B")
        req=Replace(req, "&", "%26")
        req=Replace(req, "=", "%3D")

```

```

Dim strHmacText as String
Dim objCrypto as Object
Dim strHmacGenerated
Dim loginError as String

'Initialize the Crypto object
objCrypto = Server.CreateObject("SonicSSL.Crypto")

'The text to be encoded
strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
If hmacType = "MD5" Then
    strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
Else
    strHmacGenerated = objCrypto.hmac_shal(strHmacText, strHmac)
End If

If strHmacGenerated <> hmac Then
    Dim hmacFail as String
    hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
    hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
    hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
    hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
    catchError.Text=hmacFail
    End If

End If

End Sub

Sub btnBuyNow_Click(Sender As Object, E As EventArgs)

'sample redirect generated by this routine:
'https://www.paypal.com/cgi-
bin/webscr?cmd=_xclick&business=jlevy@sonicwall.com&item_name=24%20Hour%20Secure%20
Internet%20Access&item_number=24hour&amount=0.02&currency_code=USD&lc=US&bn=PP-
BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://127.0.0.1/lhm/paypal/default.
aspx&return=http://www.moosifer.com/pdt.aspx

'sample redirect from the paypal server back the LHM server on transaction
completion (modified).
'http://127.0.0.1/lhm/paypal/pdt.aspx?tx=4PG453F7LS133715V&st=Completed&amt=0.02&cc
=USD&cm=&sig=EZhZtJygi7RTXulJt4SEhVBRi%2bJwLaC9z9kRLsrsXk4gQKnzvI5vjGy0vdhKPXAVyhbh
%2bwBxWon2cieEQDJ9P6R9qqjuKnzvI5vjGy0vdhKPXAVyJ3GtOq5Jd3%2fvTY3s7FrRcKdKnzvI5vjGy0v
dhKPXAVyyEKNxY3d

Dim str, itemName, itemNumber, itemAmount As String
Dim sb As New StringBuilder()

'Determine which button was pressed, and set item attributes appropriately
Select Case Sender.Text
    Case itemButton1

```



```

        itemName = itemName1
        itemNumber = itemNumber1
        itemAmount = itemAmount1
    Case itemButton2
        itemName = itemName2
        itemNumber = itemNumber2
        itemAmount = itemAmount2
    End Select

    'The paypal CGI URL - You can select either the real CGI or the sandbox CGI in
myvars
    sb.Append(paypalCGI & "?")
    'The cmd passed to PayPal - do not change!
    sb.Append("cmd=_xclick")
    'The email address of the paypal merchant receiving payment. Replace in myvars
with your paypal email address.
    sb.Append("&business=" & myBusiness)
    'The name of the item being purchased. This is the first item option (e.g. 1
hour). Set in myvars
    sb.Append("&item_name=" & itemName)
    'The optional item id
    sb.Append("&item_number=" & itemNumber)
    'The price being charged for the item (access)
    sb.Append("&amount=" & itemAmount)
    'The currency
    sb.Append("&currency_code=USD")
    'The country
    sb.Append("&lc=US")
    'The banana nullifier
    sb.Append("&bn=PP-BuyNowBF")
    'Disables the note option on the transaction
    sb.Append("&no_note=1")
    'Disables the shipping option on the transaction
    sb.Append("&no_shipping=1")
    'Build the path to return the client to (the LHM server address) on a cancelled
transaction
    sb.Append("&cancel_return=http://" & Request.ServerVariables("SERVER_NAME") &
Request.ServerVariables("URL"))
    'The return (success page) path to return the buyer to after the transaction. This
is the PDT receiver/processor page.
    sb.Append("&return=" & pdtPath)
    'The LHM sessionID - append this so that it can be returned to us later by the PDT
transaction - do not change!
    sb.Append("&custom=" & sessionId & Server.URLEncode(mgmtBaseUrl))
    'Optional notify_url that paypal will asynchronously send IPN confirmation to. Not
used since it's not real-time.
    'sb.Append("&notify_url=http://www.moosifer.com/ipn.aspx")
    str = sb.ToString
    Response.Redirect(str)

End Sub

</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

```

```

tr.heading {
    background-color:#006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
    <td align="center"></td>
    <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
  </tr>
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

  <tr>
    <td colspan=3><br></td>
  </tr>
  <tr>
    <td colspan=3 align="left">Purchase Secure Internet Access through SonicWALL's
LHM and PayPal's Buy Now feature.
    <br><br>The two Buy Now buttons below will send you to PayPal's website where
you can use your PayPal account to pay <b>$<%= itemAmount1 %> for <%= itemName1
%></b>, or <b>$<%= itemAmount2 %> for <%= itemName2 %></b>.
    <br><br>
    PayPal will then redirect you to this site to initiate the Payment Data
Transfer (PDT) exchange. The PDT exchange begins with the LHM server posting a
paypal constructed querystring back to paypal. The response to the post will then be
parsed by the LHM server to determine if the PayPal transaction was successful. Once
all data are exchanged and verified, LHM will authorize access on the SonicWALL for
the period of time purchased.
    <br><br>
    The clock for access will start immediately upon successful session
authorization, and can be used on the local SonicWALL appliance by the client (as
tracked by IP and MAC address) so long as session time remains. The idle timeout will
effectively be disabled by setting the idle timer to the same value as the session
timer.
    <br><br>

```

Please select "<%= itemName1 %>" or "<%= itemName2 %>" below. You will be redirected to the PayPal site, and will be returned to this site on transaction completion.

```

        <br><br>
    </td>
</tr>
<tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;&nbsp;&nbsp;</td>
</tr>
<tr class="heading">
    <td align="center"><asp:Button ID="btnBuyNow1" Class="button"
OnClick="btnBuyNow_Click" runat="server" />
    &nbsp;&nbsp;&nbsp;<asp:Button ID="btnBuyNow2" Class="button" OnClick="btnBuyNow_Click"
runat="server" /></td>
</tr>
<tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;&nbsp;&nbsp;</td>
</tr>
<tr>
    <td colspan=3><asp:Label id=LHMResult runat="server" /></td>
</tr>
<tr>
    <td colspan=3><asp:Label id=catchError runat="server"/></td>
</tr>
</table>

</form>
</BODY>
</HTML>

```

logout.aspx

```

<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String

```

```

Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
    sessionId=Request.QueryString("sessId")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    sessTimer=Request.QueryString("sessTimer")

    'Use the override class in myvars.aspx to accept untrusted certificates from the
    SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'When the page loads, make the loggedIn span visible
    loggedIn.Visible=True
    loggedOut.Visible=False

    Me.Button1.Attributes.Add("OnClick", "self.close()")
End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    'Let the user know that we are setting up the session, just in case it takes more
    than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogoff.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & eventId

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try
        'Make the loggedOut span visible
        loggedIn.Visible=False
        loggedOut.Visible=True

        'Create the webrequest to the SonicWALL
        Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

        'Calculate the length of the byte array
        toSNWL.ContentLength = byteArray.Length

        'Set the method for the webrequest to POST
        toSNWL.Method = "POST"

        'Set the content type
        toSNWL.ContentType = "application/x-www-form-urlencoded"

        'Open the request stream
        Dim dataStream As Stream = toSNWL.GetRequestStream()

```

```

'Write the byte array to the request stream
dataStream.Write(byteArray, 0, byteArray.Length)

'Close the Stream object
dataStream.Close()

'Get the response
Dim snwlReply As WebResponse = toSNWL.GetResponse()

'Display the status - looking for 200 = OK.
'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

'Grab the response and stuff it into an xml doc for possible review
Dim snwlResponse as XmlDocument = New XmlDocument()
snwlResponse.Load(snwlReply.GetResponseStream())

'Set the xPath to the SNWL reply, and get the response
Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

'Response code 150 - Logout Succeeded
If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
    LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
    LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"

```

```
LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
```

```
End Try
End Sub
```

```
</script>
<STYLE>
body {
font-size: 10pt;
font-family: verdana,helvetica,arial,sans-serif;
color:#000000;
background-color:#9CBACE;
}
```

```
tr.heading {
font-size: 10pt;
background-color:#006699;
}
```

```
tr.smalltext {
font-size: 8pt;
}
```

```
.button {
border: 1px solid #000000;
background-color: #ffffff;
font-size: 8pt;
}
</STYLE>
```

```
<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>
```

```
<SCRIPT LANGUAGE="Javascript">
```

```
//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";
```

```
function CountDown()
{
clockStr="";

dayStr=Math.floor(SecondsToCountDown/86400)%100000
if(dayStr>0){
if(dayStr>1){
dayStr+=" days ";
} else dayStr+=" day ";
clockStr=dayStr;
}
hourStr=Math.floor(SecondsToCountDown/3600)%24
if(hourStr>0){
if(hourStr>1){
hourStr+=" hours ";
} else hourStr+=" hour ";
clockStr+=hourStr;
}
minuteStr=Math.floor(SecondsToCountDown/60)%60
```

```

if (minuteStr > 0) {
    if (minuteStr > 1) {
        minuteStr += " minutes ";
    } else minuteStr += " minute ";
    clockStr += minuteStr;
}
secondStr = Math.floor(SecondsToCountDown / 1) % 60
if (secondStr > 0) {
    if (secondStr > 1) {
        secondStr += " seconds ";
    } else secondStr += " second ";
    clockStr += secondStr;
}

if (SecondsToCountDown > 0)
{
    --SecondsToCountDown;
}

if (originalTime.length < 2)
{
    originalTime = clockStr;
}

// Make sure the form is still there before trying to set a value
if (document.frmValidator) {
    document.frmValidator.originalTime.value = originalTime;
    document.frmValidator.countdown.value = clockStr;
}

setTimeout("CountDown()", 1000);
if (SecondsToCountDown == 0)
{
    document.frmValidator.countdown.value = "Session Expired";
}
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
    return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
    var key_f5 = 116;
    if (key_f5 == event.keyCode)
    {
        event.keyCode = 0;
        return false;
    }
    return false;
}

document.onkeydown = noF5
document.onmousedown = disableRightClick

</SCRIPT>

```

```

</HEAD>

<BODY onload='CountDown() '>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;</td>
  </tr>
  <tr class="smalltext"><td><br></td></tr>
  <tr class="smalltext">
    <td>Original Session Time:</td>
    <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
  </tr>
  <tr class="smalltext">
    <td>Remaining Session Time:</td>
    <td><asp:textbox width=250 id="countdown" runat="server" /></td>
  </tr>
  <tr class="smalltext">
    <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</td>
  </tr>
  <tr>
    <td colspan=2><center><asp:button id="btnSubmit" class="button" text=" Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
  </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
  </tr>
  <tr class="heading">
    <td colspan=2 align="center">&nbsp;</td>
  </tr>
  <tr>
    <td><asp:Label id=LHMResult runat="server" /></td>
  </tr>
  <tr>
    <td><asp:Label id=catchError runat="server" /></td>
  </tr>
  <tr><td><br></td></tr>
  <tr>

```



```

        <td><center><asp:button id="Button1" class="button" text=" Close "
runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

</BODY>
</HTML>

```

myvars.aspx

```

<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
Dim logoutPopup as String = "0"

'Set the debug flag (0 = off, 1 = on)
Dim debugFlag as String = "0"

'Set the path and file for the PDT responder script - this should be the same path as
the LHM settings
'configured on the SonicWALL "External Web Server Settings" page, but pointing to
the PDT handler script.
'Refer to http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside
for information on PDT
Dim pdtPath as String = "http://10.50.165.2/lhm/paypal/pdt.aspx"

'Set the path the PayPal processing CGI. Use the sandbox
(https://developer.paypal.com) and (https://www.sandbox.paypal.com) for testing
'Using the sandbox requires a developer network account and login.
Dim paypalCGI as String = "https://www.sandbox.paypal.com/cgi-bin/webscr"
'Dim paypalCGI as String = "https://www.paypal.com/cgi-bin/webscr"

'Set the email adres of the paypal merchant account to which payment will be made
'The following is a valid sandbox account, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox account) for use.
Dim myBusiness as String = "lhmdemo@sonicwall.com"

'Set this to token from PayPal account. It must be your actual, valid token.
'Refer to http://paypaltech.com/PDTGen/PDTtokenhelp.htm for information on the
identity token
'The following is a valid sandbox token, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox token) for use.
Dim token as String = "ucistq6vmKGWPxwJbrTJFDhFq889RxYt_6Mkz_3viraSzjiQJ5iPYCZ5Mdq"

'Set the names for the purchase item options (e.g. 1 hour Access, 3 hours access,
etc.)
Dim itemName1 as String = "1 Hour Secure Internet Access"
Dim itemName2 as String = "24 Hours Secure Internet Access"

'Set the paypal querystring number for purchase item options (e.g. 1hour, 60mins,
itemone, etc.)
Dim itemNumber1 as String = "1hour"
Dim itemNumber2 as String = "24hour"

```

```

'Set the purchase item options session and idle timers (timers use the same value
since we do not want sessions idling out)
Dim itemTimer1 as String = "3600"'One hour, in minutes
Dim itemTimer2 as String = "86400"'24 hours

'Set the costs in dollars for purchase item options (e.g. one penny = 0.01, one
dollar = 1.00, etc.)
Dim itemAmount1 as String = "0.01"
Dim itemAmount2 as String = "0.02"

'Set the button names and descriptions for purchase item options
Dim itemButton1 as String = "1 Hour Access - $0.01"
Dim itemButton2 as String = "24 Hours Access - $0.02"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"
'-----End of Configurable Settings-----

</script>

```

pdt.aspx

```

<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

```

```

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim sessTimer as String
Dim idleTimer as String
Dim userName as String
Dim hmac as String
Dim firstname, lastName, itemName, mcGross, mcCurrency, itemNumber, business, txn,
payStatus As String

Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load

    'Use the override class to accept untrusted certificates from the SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    Dim tx, PDTvalidateQuery As String
    Dim strResponse As HttpWebResponse
    Dim temp As String
    Dim PDTArray() As String
    Dim iParts, sResults(0, 0), aParts(), sParts(), sKey, sValue, snwlCustom As String
    Dim i As Integer

    'Set tx to value of tx passed in via Querystring from PayPal
    tx = Request.QueryString("tx")

    'Set string = to the cmd value, tx and at that needs to be
    'POSTed back to PayPal to validate the PDT
    PDTvalidateQuery = "cmd=_notify-synch&tx=" & tx & "&at=" & token

    'Now we need to POST this info back to PayPal for validation of the PDT
    'Create the request back
    Dim req As HttpRequest = CType(WebRequest.Create paypalCGI, HttpRequest)

    'Set values for the request back
    'set method
    req.Method = "POST"
    'set content type
    req.ContentType = "application/x-www-form-urlencoded"
    'set length
    req.ContentLength = PDTvalidateQuery.Length

    'Write the request back to PayPal
    Dim stOut As StreamWriter = New StreamWriter(req.GetRequestStream(),
Encoding.ASCII)
    stOut.Write(PDTvalidateQuery)
    stOut.Close()

    Try
        strResponse = CType(req.GetResponse(), HttpWebResponse)
    Catch ex As SystemException
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    End Try

    'Once we write the stream back to PayPal, we need to read the response.

```

```

Dim IPNResponseStream As Stream = strResponse.GetResponseStream
Dim encode As Encoding = System.Text.Encoding.GetEncoding("utf-8")
Dim readStream As New StreamReader(IPNResponseStream, encode)

'Read the response in String variable "temp"
temp = readStream.ReadToEnd

'Debug flag, set in myvars - prints the whole output from the POST reply
If debugFlag = "1" Then
    OutputEntirePDTString(temp)
End If

'Check to see if the 1st line of the response was "SUCCESS"
If Mid(temp, 1, 7) = "SUCCESS" Then

    'if it is SUCCESS, the code below puts the response in a nice array
    temp = Mid(temp, 9)
    sParts = Split(temp, vbCrLf)
    iParts = UBound(sParts) - 1
    ReDim sResults(iParts, 1)

    For i = 0 To iParts

        aParts = Split(sParts(i), "=")
        sKey = aParts(0)
        sValue = aParts(1)
        sResults(i, 0) = sKey
        sResults(i, 1) = sValue

        'You can add more case statements here for other returned variables

    Try
        Select Case sKey
            Case "first_name"
                firstname = Server.URLDecode(sValue)
            Case "last_name"
                lastName = Server.URLDecode(sValue)
            Case "item_name"
                itemName = Server.URLDecode(sValue)
            Case "mc_gross"
                mcGross = sValue
            Case "mc_currency"
                mcCurrency = sValue
            Case "item_number"
                itemNumber = Server.URLDecode(sValue)
            Case "business"
                business = Server.URLDecode(sValue)
            Case "txn_id"
                txn = sValue
            Case "payment_status"
                payStatus = sValue
                Case "custom"
                    snwlCustom = sValue
                    sessionID = snwlCustom.SubString(0, 32)
                    mgmtBaseUrl=(Server.URLDecode(Mid(snwlCustom, 33)))
        End Select
    Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    End Try

```

```

        Next

    If payStatus = "Completed" Then
        'Transaction Succeeded - Give the Guest a receipt
        Dim receipt as String

        receipt = "<h3>Transaction Succeeded. Thank you for selecting SonicWALL
LHM.</h3><br>"
        receipt + = "<b>Transaction Invoice:</b><br><br>"
        receipt + = "Name: " & firstname & " " & lastName & "<br>"
        receipt + = "Description: " & itemName & "<br>"
        receipt + = "Amount: " & mcCurrency & " " & mcGross & "<br>"
        receipt + = "Paid to: " & business & "<br>"
        receipt + = "Transaction ID: " & txn & "<br>"
        receipt + = "<br><br>"

        paypalResult.Text = receipt

        LHMResult.Text = "Authorizing your LHM session."

        'Setup the LHM session variables and call LHM Routine
        'Set the session and idle timers to match the variables set in myvars
        If itemNumber = itemNumber1 Then
            sessTimer=itemTimer1
            idleTimer=itemTimer1
        Else
            sessTimer=itemTimer2
            idleTimer=itemTimer2
        End If

        userName = firstname & " " & lastName

        LHM()
    Else
        'The transaction itself was a success, but the payment status was not
        Completed.
        paypalResult.Text = "The transaction succeeded, but the payment was not
        completed. The session cannot be authorized at this time."
        End If

    Else
        ' If PDT response is not "SUCCESS"
        paypalResult.Text = "The PayPal transaction did not succeed. The returned
        status is: <b>" & temp & "</b>"
        End If

        'Close the streams
        readStream.Close()
        strResponse.Close()

    End Sub

    'This is the parser for the debug function to print the entire resonse to the PDT
    POST
    Private Function OutputEntirePDTString(ByVal myPDTString As String) As String
        Dim tempString() As String = Split(myPDTString, vbLf)
        Dim x As Integer
        For x = 0 To tempString.GetUpperBound(0)
            Response.Write(tempString(x) & "<br>")
        Next
    End Function

```

```

Sub LHM()

    'Let the user know that we are setting up the session, just in case it takes more
    than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogin.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
    Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
    idleTimer

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

Try
    'Create the webrequest to the SonicWALL
    Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

    'Calculate the length of the byte array
    toSNWL.ContentLength = byteArray.Length

    'Set the method for the webrequest to POST
    toSNWL.Method = "POST"

    'Set the content type
    toSNWL.ContentType = "application/x-www-form-urlencoded"

    'Open the request stream
    Dim dataStream As Stream = toSNWL.GetRequestStream()

    'Write the byte array to the request stream
    dataStream.Write(byteArray, 0, byteArray.Length)

    'Close the Stream object
    dataStream.Close()

    'Get the response
    Dim snwlReply As WebResponse = toSNWL.GetResponse()

    'Display the status - looking for 200 = OK.
    'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

    'Grab the response and stuff it into an xml doc for possible review
    Dim snwlResponse as XmlDocument = New XmlDocument()
    snwlResponse.Load(snwlReply.GetResponseStream())

    'Set the xPath to the SNWL reply, and get the response
    Dim codePath as String =
    "SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

    'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

    'Response code 50 - Login Succeeded

```

```

If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

    'Do we want to provide a logout popup window?
    If logoutPopup = "1" Then
        'Popup hack using Javascript for logout window
        Dim sb As New System.Text.StringBuilder()
        sb.Append("<script language='javascript'">")
        sb.Append("window.open('logout.aspx?sessId=")
        sb.Append(Server.URLEncode(CStr(sessionId)))
        sb.Append("&mgmtBaseUrl=")
        sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
        sb.Append("&sessTimer=")
        sb.Append(Server.URLEncode(CStr(sessTimer)))
        sb.Append(", 'logOut', 'toolbar=no,")
        sb.Append("addressbar=no,menubar=no,")
        sb.Append("width=400,height=250');")
        sb.Append("<")
        sb.Append("/")
        sb.Append(">script">")
        RegisterStartupScript("stp", sb.ToString)
    End If

    LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now begin your secure Internet access session."

    'Response code 51 - Session Limit Exceeded
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
        LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

    'Response code 100 - Login Failed.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

    'Response code 251 - Bad HMAC.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

    'Response code 253 - Invalid SessionID.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

    'Response code 254 - Invalid CGI.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

    'Response code 255 - Internal Error.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

```

```

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
End Try
End Sub

</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    background-color: #006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
    <td><center><img width="216" height="51" src=""%= logo%"></center></td>
    <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
  </tr>
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>

```



```

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr>
    <td><br></td>
  </tr>
  <tr>
    <td><asp:Label id=paypalResult runat="server" /></td>
  </tr>
  <tr>
    <td><asp:Label id=LHMResult runat="server" /></td>
  </tr>
  <tr>
    <td><asp:Label id=catchError runat="server" /></td>
  </tr>
</table>
</BODY>
</HTML>

```

Random 脚本

验证模式

目的

访客输入经过算法验证的随机生成的密码。

传统的密码验证要求在使用之前生成密码并存储在验证平台上。例如，无线访客服务要求在使用它们的特定 SonicWall 安全设备上生成帐户。Random 脚本通过使用加密盐算法生成和验证密码来消除这种依赖性。这意味着密码永远不需要存储在任何地方，只要加密盐是相同的，密码就完全是迁移的（也就是说，它们可以在任何站点使用，甚至可以用于不同的 LHM 服务器）。

这样做的实际意义在于，可以在未来的任何时间批量生成、分发和使用访客帐号密码。例如，可以生成（使用特定的加密盐）、打印（例如，在证书、名片、刮刮卡上）、分发并在其 LHM 服务器采用相同的算法加密盐的任何站点使用密码。密码可以有绝对的（而非相对的）到期日期，此时可以更改加密盐以使过期的密码无效。

同样可以使用常用的加密盐来验证跨多个站点的一组密码，唯一的加密盐可以确保在一个站点生成的密码不能在另一个使用不同加密盐的站点使用；因此，虽然使用了常用的算法来生成和验证所有的密码，但根据需要将加密盐添加到哈希函数中可提供唯一性。

除了 default.aspx 脚本还有 generator.aspx 脚本，它是生成密码的地方。一次可以生成 1 到 999 个密码。生成后，可以打印单个密码，也可以将整个列表导出到 .csv 文件。

支持两类密码：1 小时和 24 小时。生成器脚本可以生成任一种类型的密码。

生成算法的工作方式：

- 1 生成 randChars（整数，默认值为六）字符的随机代码（root-passcode），如 myvars 中所定义。可以在 default.aspx 文件中修改随机代码生成器的字符集。
- 2 加密盐（在 myvars 中定义为加密盐字符串）作为根密码的前缀。
- 3 然后在生成的字符串上计算 SHA1 哈希值。然后从哈希中获得三对字符；对于：
 - 1 小时密码，获得 408 对（字符 4,5 + 0,1 + 8,9）。
 - 24 小时密码，获得 752 对（字符 7,8 + 5,6 + 2,3）。
- 4 从哈希中选择的六个字符然后连接到根密码。
- 5 结果是可分配密码。

验证算法相反:

- 1 访客输入他们的密码（调用 enteredCode）。
- 2 该脚本抓取输入代码的第一个 randChars 字符（调用此根密码）。
- 3 加密盐作为根密码的前缀，并计算 SHA1 哈希值。获取 408 对字符并附加到根密码。然后将 408 对匹配到 enteredCode：
 - 如果 408 对匹配，则验证为 1 小时密码。
 - 如果 408 对不匹配，则尝试 752 对。如果符合 enteredCode，则验证为 24 小时密码。
 - 如果两者都不匹配，则代码无效。

在 enteredCode 已经验证之后，查询 usedcodes.mdb 数据库以查看代码是否已使用。如果在数据库找不到 enteredCode，则会使用 MAC 地址作为 userName 开始 LHM 会话授权序列。在 LHM 会话获得授权并且 LHM 服务器已经接收到确认之后，来自 enteredCode 的根密码将写入 usedcodes.mdb 数据库中，使它不能重新使用。当（如果）更改加密盐时，建议刷新数据库。

myvars 变量

logoutPopup 控制注销弹出窗口的使用。设置为:

- 0 以禁用弹出窗口。
- 1 以启用弹出窗口。

useDB 控制对已用密码数据库的使用。如果 useDB 是:

- 0, 则不会读取或写入数据库, 允许重复使用密码。
- 1, 则将已用密码写入数据库, 新的验证流程将检查数据库以确定密码是否已使用。

randChars 包含在根密码中的随机字符数。默认为六。这导致 12 个字符的密码, 因为哈希组件总是增加六个字符。

salt 用于计算哈希的加密盐。确保使用良好的加密盐以防止不必要的密码迁移/冲突。

sessTimer 会话计时器, 以秒为单位。

idleTimer 闲置计时器, 以秒为单位。

strHmac 可选 HMAC 功能的共享密钥。

hmacType HMAC 在使用中时使用的摘要类型: MD5 或 SHA1。

logo 要在页眉上使用的徽标 (图像) 文件的名称。

会话流程

- 1 访客输入他们的密码。
- 2 通过使用上述目的部分所述的算法验证来验证该密码。
- 3 如果代码经过验证, 将在 usedcodes.mdb 数据库中检查以前是否使用过。
- 4 如果不存在, 则使用 MAC 地址作为用户名, 启动 LHM 会话 (1 小时或 24 小时)。
- 5 在 LHM 会话启动之后, 脚本将根密码写入 usedcodes.mdb 数据库, 以便不能重复使用。
- 6 该脚本执行到 SonicWall 安全设备的 LHM POST 以授权会话。

其他注意事项

由于脚本正在写入数据库, 因此必须为 IUSR_MACHINENAME 和 IWAM_MACHINENAME (或 ASPNET) 帐户配置写入权限, 如第 643 页的我想使用 SonicWall 提供的示例脚本。我需要做什么才能使用它们? 中所述 generator.aspx 脚本应位于 Web 服务器上的安全 (公开不可访问) 区域中。

主题:

- 第 739 页的 [default.aspx](#)
- 第 747 页的 [generator.aspx](#)
- 第 752 页的 [logout.aspx](#)
- 第 757 页的 [myvars.aspx](#)
- 第 758 页的 [print.aspx](#)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDb" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/random/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Dim passCode as String
Dim grabCode as String
```

```

Sub Page_Load(Source as Object, E as EventArgs)

    LHMResult.Text=""
    catchError.Text=""
    authResult.Text=""

    ip=Request.QueryString("ip")
    sessionId=Request.QueryString("sessionId")
    mac=Request.QueryString("mac")
    ufi=Request.QueryString("ufi")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    clientRedirectUrl=Request.QueryString("clientRedirectUrl")
    req=Request.QueryString("req")
    hmac=Request.QueryString("hmac")
    customCode=Request.QueryString("cc")

    'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
    you to use the same
    'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
    (?cc=3) and "Max Sessions" (?cc=4) page.
    If customCode <> "" Then
        Select Case customCode
            Case "2"
                LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
                You may try to initiate a new session.</font></H3>"
            Case "3"
                LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
                timeout. Please log back in.</font></H3>"
            Case "4"
                LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
                has been reached. Please try again later.</font></H3>"
        End Select
    End If

    'Use the override class in myvars.aspx to accept untrusted certificates from the
    SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'Note - the routine below for handling the hmac requires the use of the
    SonicSSL.dll and libeay.dll libraries.
    'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
    with "regsvr32 sonicssl.dll"
    If hmac <> "" Then

        'SonicWALL URL Encode routine is different from Microsoft - this is the
        SonicWALL method
        req=Replace(req,"%","%25")
        req=Replace(req,":","%3A")
        req=Replace(req," ","%20")
        req=Replace(req,"?","%3F")
        req=Replace(req, "+", "%2B")
        req=Replace(req, "&", "%26")
        req=Replace(req, "=", "%3D")

        Dim strHmacText as String
        Dim objCrypto as Object
        Dim strHmacGenerated
        Dim loginError as String

        'Initialize the Crypto object

```

```

objCrypto = Server.CreateObject("SonicSSL.Crypto")

'The text to be encoded
strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
If hmacType = "MD5" Then
    strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
Else
    strHmacGenerated = objCrypto.hmac_shal(strHmacText, strHmac)
End If

If strHmacGenerated <> hmac Then
    Dim hmacFail as String
    hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
    hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
    hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
    hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
    catchError.Text=hmacFail
End If

End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
    enteredCode.Text = ""
    LHMResult.Text=""
    catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

'The following subroutine validates client provided passcodes.
'The first 6 characters (definable in myars) are grabbed.
'These characters are then run though a SHA1 hash with a salt that is defined in
myvars.

'3 pairs of substrings are then retrieved from the hash.
'The code is validated if the 3 pairs concatenated to the randChars (defined in
myvars) characters consist of the following:

'Validating the 4 0 8 pairs (4,5+0,1+8,9 characters) will provide 1 hour of guest
access.
'Validating the 7 5 2 pairs (7,8+5,6+2,3 characters) will provide 24 hours of
guest access.

grabCode = enteredCode.Text.SubString(0,randChars)

'Manually compute SHA1 on salt+randomCode, and convert result to base64 - gives
stranger output
Dim shal As sha1 = sha1.Create()

```

```

    Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
grabCode))
    Dim hashResult as String = Convert.ToBase64String(manualHash)

    'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
    'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

    'First try to match on 1 hour code
passCode = ""
passCode = grabCode & hashResult.SubString(4, 2)
passCode = passCode & hashResult.SubString(0, 2)
passCode = passCode & hashResult.SubString(8, 2)
If enteredCode.Text = passCode Then
    sessTimer = "3600"
    authResult.Text="<font color=""green""><b>1 hour code validated.</b></font>"

    'Check the used passcode DB if useDB is enabled in myvars.
    If useDB = "1" Then
        wasItUsed()
    End If
Else
    'Now try to match on 24 hour code
passCode = ""
passCode = grabCode & hashResult.SubString(7, 2)
passCode = passCode & hashResult.SubString(5, 2)
passCode = passCode & hashResult.SubString(2, 2)
If enteredCode.Text = passCode Then
    sessTimer = "86400"
    authResult.Text="<font color=""green""><b>24 hour code
validated.</b></font>"

    'Check the used passcode DB if useDB is enabled in myvars.
    If useDB = "1" Then
        wasItUsed()
    End If

Else
    authResult.Text="<font color=""Red""><b>Passcode cannot be
validated.</b><br><b>The passcode is case-sensitive.<br>Please try again.</font>"
    End if
End If

End Sub

Sub wasItUsed ()

    'Check to see if the root (randChars) of the passcode is already in the used
database.
    Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"
    Dim MySQL as string = "SELECT * From passCodes Where passCode = '" & grabCode &
""
    Dim MyConn as New OleDbConnection (strConn)
    Dim cmd as New OleDbCommand (MySQL, MyConn)
    Dim objDR As OleDbDataReader
    Dim isUsed As Boolean

    MyConn.Open()
    objDR = cmd.ExecuteReader()

```

```

isUsed = objDR.Read()
objDR.Close()
MyConn.Close()

'If the passcode is not found in the database
if isUsed = False
    LHM()
Else
    authResult.Text="<font color=""Red""><b>Passcode has already been
used.</b><br>Please see an attendant for assistance.</font>"
End If

End Sub

Sub writeToDB ()

'Try to write the submitted (only randChars characters instead of the whole
passcode) info to the database file
Try
    Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"

    Dim MySQL as string = "INSERT INTO passCodes (passCode) VALUES ('" & grabCode &
""'"
    Dim MyConn as New OleDbConnection (strConn)
    Dim cmd as New OleDbCommand (MySQL, MyConn)
    MyConn.Open ()
    cmd.ExecuteNonQuery ()
    MyConn.Close ()

    Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
    End Try

End Sub

Sub LHM()

'The writeToDB sub is in the Response code 50 - Login Succeeded routine, after the
LHM exchange succeeds. You may move it to the top to write the passcode to the DB
before the LHM transaction for testing purposes.
'writeToDB ()

enteredCode.Text = "Code Accepted."

'Let the user know that we are setting up the session, just in case it takes more
than a second
LHMResult.Text = "Authorizing session. Please wait."

'The LHM cgi on the SonicWALL - this does not change
Dim loginCgi as String = "externalGuestLogin.cgi"

'Assemble the data to post back to the SonicWALL to authorize the LHM session
Dim loginParams as String = "sessId=" & sessionId & "&userName=" & mac &
"&sessionLifetime=" & sessTimer & "&idleTimeout=" & idleTimer

'Combine mgmtBaseUrl from the original redirect with the login cgi
Dim postToSNWL as String = mgmtBaseUrl & loginCgi

'Convert the loginParams to a well behaved byte array
Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

```

```

Try
    'Create the webrequest to the SonicWALL
    Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

    'Calculate the length of the byte array
    toSNWL.ContentLength = byteArray.Length

    'Set the method for the webrequest to POST
    toSNWL.Method = "POST"

    'Set the content type
    toSNWL.ContentType = "application/x-www-form-urlencoded"

    'Open the request stream
    Dim dataStream As Stream = toSNWL.GetRequestStream()

    'Write the byte array to the request stream
    dataStream.Write(byteArray, 0, byteArray.Length)

    'Close the Stream object
    dataStream.Close()

    'Get the response
    Dim snwlReply As WebResponse = toSNWL.GetResponse()

    'Display the status - looking for 200 = OK.
    'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

    'Grab the response and stuff it into an xml doc for possible review
    Dim snwlResponse as XmlDocument = New XmlDocument()
    snwlResponse.Load(snwlReply.GetResponseStream())

    'Set the xPath to the SNWL reply, and get the response
    Dim codePath as String =
    "SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

    'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

    'Response code 50 - Login Succeeded

    If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

        'Do we want to provide a logout popup window?
        If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("'", 'logOut', 'toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append(">script>")
            RegisterStartupScript("stp", sb.ToString)

```



```

End If

LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href="" & req & """" & req & """"> & req & ""/>"

'Write the passcode the DB if the LHM session succeeds and if useDB = 1.
If useDB = "1" Then
    writeToDB ()
End If

'Response code 51 - Session Limit Exceeded
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
    LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

'Response code 100 - Login Failed.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

'Response code 251 - Bad HMAC.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 253 - Invalid SessionID.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

'Response code 254 - Invalid CGI.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

'Response code 255 - Internal Error.
ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

End If

'Close the streams
dataStream.Close()
snwlReply.Close()

'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
Catch ex as Exception
    catchError.Text = "<font color=""9CBACE"">" & ex.ToString & ""/>"
    LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.

```

Sorry for the inconvenience. Please close and relaunch your browser to try again. If the problem persists, please notify an attendant."

```
    End Try
End Sub
```

```
</script>
```

```
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;
    background-color:#9CBACE;
}
```

```
tr.heading {
    background-color:#006699;
}
```

```
.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
```

```
</STYLE>
```

```
<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>
```

```
<BODY>
<form id="frmValidator" onKeyPress="if(event.keyCode==13)
{document.getElementById('btnSubmit').click(); return false}" runat="server">
```

```
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan="3" align="center"><font color="white">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
        <td align="center"></center></td>
        <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b>&nbsp;</font></td>
    </tr>
    <tr class="heading">
        <td colspan="3" align="center"><font color="white">&nbsp;</td>
    </tr>
</table>
```

```
<table width="90%" border="0" cellpadding="2" cellspacing="0">
    <tr>
        <td><b>Welcome <%= ip%> to SonicWALL's LHM Algorithmic
Authenticator.</b><br><br><b>Enter your unique randomly generated passcode to obtain
secure guest internet access.<br><br>Valid passcodes are not stored anywhere, so
validation is not performed against any kind of database. Instead, when a passcode
is entered, it is algorithmically validated. Once a passcode is successfully used,
it is written to a "used passcode" database so that it cannot be reused.<br><br>The
validator will recognize 1 hour and 24 hour passcodes - these characteristics were
encoded within the passcodes themselves during generation.<br><br>
```



```

Sub Page_Load(Source as Object, E as EventArgs)
    If Not isPostBack Then
        Heading.Text="&nbsp;"
        btnExport.Visible = False
    End If
End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)
    'The following generates passcodes beginning with a random character generator.
    'The number of characters in randomCode is configurable in myvars.
    'The randomCode output is then run through a SHA1 hash with a salt that is defined
    in myvars.
    'Note: If you are using this in a live environment, it is important to change the
    salt to prevent algorithm compromise.

    '3 pairs of substrings are then retrieved from the hash, and concatenated to the
    randomCode to form the passcode.

    'In the current sample implementation:
    'The 4 0 8 pairs (4,5+0,1+8,9 characters) from the hash will provide 1 hour of
    guest access.
    'The 7 5 2 pairs (7,8+5,6+2,3 characters) from the hash will provide 24 hours of
    guest access.

    Dim myLooper As Integer
    Dim passCode as String

    For myLooper = 1 to Convert.ToInt32(codeCount.Text)

        Dim x As Integer = 0
        Dim isItRand as boolean = False
        Dim intRand as Integer = 0
        Dim randomCode as String = ""

        For x = 1 to randChars
            Do Until isItRand = True
                '48 to 57 for numbers, 65 to 90 for uppercase, 97 to 122 for lowercase
                intRand = Int((122 - 48 + 1) * Rnd + 48)
                'Select the legal character set for randomCode by including legal
                characters below.
                If InStr(1, "abcdefghjklmnpqrstuvwxyzABCDEFGHIJKLMN PQRSTUVWXYZ
23456789 ", Chr(intRand), 1) Then
                    isItRand = True
                End If
            Loop
            randomCode = randomCode & Chr(intRand)
            isItRand = False
        Next

        'Manually compute SHA1 on salt+randomCode, and convert result to base64 -
        gives stranger output
        Dim sha1 As sha1 = sha1.Create()
        Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
randomCode))
        Dim hashResult as String = Convert.ToBase64String(manualHash)

        'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
        output.
        'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode, "SHA1")

```

```

    If DropDownList1.SelectedItem.Value = "1 Hour" Then
        passCode = randomCode & hashResult.SubString(4, 2)
        passCode = passCode & hashResult.SubString(0, 2)
        passCode = passCode & hashResult.SubString(8, 2)
        genCodes.Add(passCode)
    Else
        passCode = randomCode & hashResult.SubString(7, 2)
        passCode = passCode & hashResult.SubString(5, 2)
        passCode = passCode & hashResult.SubString(2, 2)
        genCodes.Add(passCode)
    End If

Next

    btnExport.Visible = True
    heading.Text = "Your " & codeCount.Text & " <b>" &
dropDownList1.SelectedItem.Value & "</b> Passcodes:"
    genOutput.DataSource = genCodes
    genOutput.DataBind()
    codeCount.Text=""

    'Store the genCodes array in session state for retrieval for printing and
exporting
    Session("myGenCodes") = genCodes
    Session("codeType") = DropDownList1.SelectedItem.Value

End Sub

Sub printIt(Src As Object, e As DataListCommandEventArgs)
    If not Session.Item("myGenCodes") is Nothing Then
        genCodes=Session.Item("myGenCodes")
        codeType=Session.Item("codeType")
        'response.write(CStr(genCodes.Item(e.Item.ItemIndex)))

        'Popup hack using Javascript so that individual entries can be printed from
the DataList
        Dim sb As New System.Text.StringBuilder()
        sb.Append("<script language='javascript'>")
        sb.Append("window.open('print.aspx?genCode=")
        sb.Append(Server.URLEncode(CStr(genCodes.Item(e.Item.ItemIndex))))
        sb.Append("&sessLife=")
        sb.Append(Server.URLEncode(codeType))
        sb.Append(", 'printCode', 'toolbar=no,")
        sb.Append("addressbar=no,menubar=no,")
        sb.Append("width=400,height=250');")
        sb.Append("<")
        sb.Append("/")
        sb.Append(">script>")
        RegisterStartupScript("stp", sb.ToString)
    End If

End Sub

Sub exporter(Sender As Object, E As EventArgs)

    If not Session.Item("myGenCodes") is Nothing Then
        genCodes=Session.Item("myGenCodes")

        'Convert the genCodes array to a string with CRs for later conversion to a byte
array
        Dim i as Integer

```

```

Dim genCodeString as String
for i = 0 To genCodes.Count - 1
    genCodeString += CStr(genCodes.Item(i)) & Chr(13)
Next

'response.write(genCodeString)

'Create the byte array and send it to the browser as genCodes.csv
Dim data() As Byte = System.Text.ASCIIEncoding.ASCII.GetBytes(genCodeString)
Response.Clear()
Response.AddHeader("Content-Type", "application/Excel")
Response.AddHeader("Content-Disposition", "inline;filename=genCodes.csv")
Response.BinaryWrite(data)
Response.End()
End If

End Sub

</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;
    background-color:#9CBACE;
}

tr.heading {
    background-color:#006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=3 align="center"><font color="white">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
        <td><center></center></td>
        <td width="50%" align="right" valign="center"><font color="white"><b>Passcode
Generator</b>&nbsp;</font></td>
    </tr>
    <tr class="heading">
        <td colspan=3 align="center"><font color="white">&nbsp;</td>
    </tr>
</table>

```

```

<table width="90%" border="0" cellpadding="2" cellspacing="0">
  <tr>
    <td><b>Welcome to SonicWALL's LHM Algorithmic Generator.</b><br><br>This will
    allow you to create randomly generated passcodes for secure guest internet
    access.<br><br>Valid passcodes are not stored anywhere, so validation is not
    performed against any kind of database. Instead, when a passcode is entered, it is
    algorithmically validated. Once a passcode is successfully used, it is written to a
    "used passcode" database so that it cannot be reused.<br><br>The validator will
    recognize 1 hour and 24 hour passcodes - these characteristics were encoded within
    the passcodes themselves during generation.<br><br>
    </td>
  </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr><br>
    <td width="15%">Passcode type:</td>
    <td width="10%"><asp:DropDownList id="DropDownList1" runat="server">
      <asp:ListItem>1 Hour</asp:ListItem>
      <asp:ListItem>24 Hours</asp:ListItem>
    </asp:DropDownList></td>
    <td width="20%">Number to generate:</td>
    <td width="20%"><asp:TextBox id="codeCount" runat="server" /></td>
    <td width="50%"><asp:RequiredFieldValidator id="valcodeCount"
    ControlToValidate="codeCount" ErrorMessage="Enter a value." Font-Size="10"
    Display="Dynamic" runat="server" />
    <asp:RangeValidator id="Rangel" ControlToValidate="codeCount" MinimumValue="1"
    MaximumValue="999" Type="Integer" Font-Size="10" ErrorMessage="Values from 1 to
    999." runat="server" /></td>
  </tr>
  <tr>
    <td colspan=3></td>
    <td><asp:button id="btnSubmit" class="button" text=" Submit "
    onClick="btnSubmit_Click" runat="server" />&nbsp;&nbsp;&nbsp;<asp:button id="btnExport"
    class="button" text=" Export " CausesValidation="False" onClick="exporter"
    runat="server" /><br></td>
  </tr>
  <tr>
    <td colspan=3></td>
  </tr>
  <tr class="heading">
    <td colspan=5><font color="white"><asp:Label id=heading runat="server" /></td>
  </tr>
  <tr><td><br></td></tr>
</table>

<asp:DataList id="genOutput" Runat="Server" RepeatColumns="4"
RepeatDirection="Horizontal" CellPadding="0" Cellspacing="0" GridLines="Both"
align="center" OnItemCommand="printIt">
  <ItemTemplate>
    <td>
    <asp:Label Text='<%# Container.DataItem %>' Runat="Server"/>
    </td>
    <td>
    <asp:ImageButton id="print" runat="server" ImageUrl="print.gif"
    EnableViewState="False" CausesValidation="False" CommandName='<%#
    Container.DataItem %>' />

```

```

        </td>
    </ItemTemplate>
</asp:DataList>

</form>
</BODY>
</HTML>

```

logout.aspx

```

<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
    Implements System.Net.ICertificatePolicy
    Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
        ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
        As Boolean Implements ICertificatePolicy.CheckValidationResult
        Return True
    End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
    sessionId=Request.QueryString("sessId")
    mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
    sessTimer=Request.QueryString("sessTimer")

    'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
    'This is necessary for the POST to the SonicWALL authorizing the LHM session.
    System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

    'When the page loads, make the loggedIn span visible
    loggedIn.Visible=True
    loggedOut.Visible=False

    Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button

```



```

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

    'Let the user know that we are setting up the session, just in case it takes more
    than a second
    LHMResult.Text = "Authorizing session. Please wait."

    'The LHM cgi on the SonicWALL - this does not change
    Dim loginCgi as String = "externalGuestLogoff.cgi"

    'Assemble the data to post back to the SonicWALL to authorize the LHM session
    Dim loginParams as String = "sessId=" & sessionId & eventId

    'Combine mgmtBaseUrl from the original redirect with the login cgi
    Dim postToSNWL as String = mgmtBaseUrl & loginCgi

    'Convert the loginParams to a well behaved byte array
    Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

    Try
        'Make the loggedOut span visible
        loggedIn.Visible=False
        loggedOut.Visible=True

        'Create the webrequest to the SonicWALL
        Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

        'Calculate the length of the byte array
        toSNWL.ContentLength = byteArray.Length

        'Set the method for the webrequest to POST
        toSNWL.Method = "POST"

        'Set the content type
        toSNWL.ContentType = "application/x-www-form-urlencoded"

        'Open the request stream
        Dim dataStream As Stream = toSNWL.GetRequestStream()

        'Write the byte array to the request stream
        dataStream.Write(byteArray, 0, byteArray.Length)

        'Close the Stream object
        dataStream.Close()

        'Get the response
        Dim snwlReply As WebResponse = toSNWL.GetResponse()

        'Display the status - looking for 200 = OK.
        'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

        'Grab the response and stuff it into an xml doc for possible review
        Dim snwlResponse as XmlDocument = New XmlDocument()
        snwlResponse.Load(snwlReply.GetResponseStream())

        'Set the xPath to the SNWL reply, and get the response
        Dim codePath as String =
        "SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

        'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

        'Response code 150 - Logout Succeeded
    
```

```

    If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

        'Response code 251 - Bad HMAC.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        'Response code 253 - Invalid SessionID.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

        'Response code 254 - Invalid CGI.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        'Response code 255 - Internal Error.
    ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

    End If

    'Close the streams
    dataStream.Close()
    snwlReply.Close()

    'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
    Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
    End Try
End Sub

</script>
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana,helvetica,arial,sans-serif;
    color:#000000;
    background-color:#9CBACE;
}

tr.heading {
    font-size: 10pt;
    background-color:#006699;
}

tr.smalltext {
    font-size: 8pt;

```

```

}

.button {
  border: 1px solid #000000;
  background-color: #ffffff;
  font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
  clockStr="";

  dayStr=Math.floor(SecondsToCountDown/86400)%100000
  if(dayStr>0){
    if(dayStr>1){
      dayStr+=" days ";
    } else dayStr+=" day ";
    clockStr=dayStr;
  }
  hourStr=Math.floor(SecondsToCountDown/3600)%24
  if(hourStr>0){
    if(hourStr>1){
      hourStr+=" hours ";
    } else hourStr+=" hour ";
    clockStr+=hourStr;
  }
  minuteStr=Math.floor(SecondsToCountDown/60)%60
  if(minuteStr>0){
    if(minuteStr>1){
      minuteStr+=" minutes ";
    } else minuteStr+=" minute ";
    clockStr+=minuteStr;
  }
  secondStr=Math.floor(SecondsToCountDown/1)%60
  if(secondStr>0){
    if(secondStr>1){
      secondStr+=" seconds ";
    } else secondStr+=" second ";
    clockStr+=secondStr;
  }

  if(SecondsToCountDown > 0)
  {
    --SecondsToCountDown;
  }

  if(originalTime.length < 2)
  {
    originalTime = clockStr;
  }
}

```

```

// Make sure the form is still there before trying to set a value
if(document.frmValidator){
    document.frmValidator.originalTime.value = originalTime;
    document.frmValidator.countdown.value = clockStr;
}

setTimeout("CountDown()", 1000);
if(SecondsToCountDown == 0)
{
    document.frmValidator.countdown.value = "Session Expired";
}
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
    return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
    var key_f5 = 116;
    if (key_f5==event.keyCode)
    {
        event.keyCode=0;
        return false;
    }
    return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown() '>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="smalltext"><td><br></td></tr>
    <tr class="smalltext">
        <td>Original Session Time:</td>
        <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
    </tr>
    <tr class="smalltext">

```

```

        <td>Remaining Session Time:</td>
        <td><asp:textbox width=250 id="countdown" runat="server" /></td>
    </tr>
    <tr class="smalltext">
        <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
    </td>
    <tr>
        <td colspan=2><center><asp:button id="btnSubmit" class="button" text=" Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
    </tr>
    <tr class="heading">
        <td colspan=2 align="center">&nbsp;</td>
    </tr>
    <tr>
        <td><asp:Label id=LHMResult runat="server" /></td>
    </tr>
    <tr>
        <td><asp:Label id=catchError runat="server" /></td>
    </tr>
    <tr><td><br></td></tr>
    <tr>
        <td><center><asp:button id="Button1" class="button" text=" Close "
runat="server" /></center></td>
    </tr>
</table>
</form>
</span>

</BODY>
</HTML>

```

myvars.aspx

```

<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
'The login event can be made non exclusive in this script by setting useDB to 0.
Dim logoutPopup as String = "0"

'Set the use of the database for storing and checking used passcodes. 0 = do not use
DB, 1 = use DB.
Dim useDB as String = "1"

```

```
'The number of characters in the randomCode
Dim randChars as Integer = 6

'Set the salt the generation of the SHA1 hash
Dim salt as String = "moosifer"

'The LHM Session Timeout is set by the passcode in this script
Dim sessTimer as String

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'-----End of Configurable Settings-----

</script>
```

print.aspx

```
<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

Dim genCode as String
Dim sessLife as String

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
    genCode=Request.QueryString("genCode")
    sessLife=Request.QueryString("sessLife")
End Sub

</script>
<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}
tr.heading {
    background-color: #006699;
}
</STYLE>
<BODY>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
    <tr class="heading">
        <td colspan=2 align="center"><font color="white">&nbsp;</td>
    </tr>
```

```

<tr class="heading">
  <td colspan=2 align="center"></td>
</tr>
<tr class="heading">
  <td colspan=2 align="center"><font color="white">&nbsp;</td>
</tr>
<tr><td><br><br></td></tr>
<tr>
  <td>Your Pass Code is:</td>
  <td><b><%= genCode%></b></td>
</tr>
<tr><td><br></td></tr>
<tr>
  <td>Session Lifetime is:</td>
  <td><b><%= sessLife%></b></td>
</tr>
</table>

<script language='javascript'>window.print();</script>

</BODY>
</HTML>

```

Chooser.aspx 脚本

```

<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<script language="VB" runat="server">

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String
Dim qString as String

Sub Page_Load(src as Object, e as EventArgs)

  'Grab the querystring one element at a time since we need to do a custom URL
  encode on the req variable
  sessionId=Request.QueryString("sessionId")
  ip=Request.QueryString("ip")
  mac=Request.QueryString("mac")
  ufi=Request.QueryString("ufi")
  mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
  clientRedirectUrl=Request.QueryString("clientRedirectUrl")
  req=Request.QueryString("req")
  hmac=Request.QueryString("hmac")

```

```

customCode=Request.QueryString("cc")

'SonicWALL URL Encode routine is different from Microsoft - this is the SonicWALL
method
req=Replace(req,"%","%25")
req=Replace(req,":","%3A")
req=Replace(req," ","%20")
req=Replace(req,"?","%3F")
req=Replace(req, "+", "%2B")
req=Replace(req, "&", "%26")
req=Replace(req, "=", "%3D")

'Rebuild the querystring variable
qString = "sessionId=" & sessionId & "&ip=" & ip & "&mac=" & mac & "&ufi=" & ufi &
"&mgmtBaseUrl=" & mgmtBaseUrl & "&clientRedirectUrl=" & clientRedirectUrl & "&req="
& req

'Add the optional hmac and cc vars if they are there.
If hmac <> "" Then
    qString+="&hmac=" & hmac
End If

If customCode <> "" Then
    qString+="&cc=" & customCode
End If

'Bind the directory data
Dim lhmDir As New DirectoryInfo(Server.MapPath("."))
lhmList.DataSource = lhmDir.GetDirectories
lhmList.DataBind()

End Sub

</script>

<STYLE>
body {
    font-size: 10pt;
    font-family: verdana, helvetica, arial, sans-serif;
    color: #000000;
    background-color: #9CBACE;
}

tr.heading {
    background-color: #006699;
}

.button {
    border: 1px solid #000000;
    background-color: #ffffff;
}

tr.hidden {
    font-size: 5pt;
    color: #9CBACE;
}

</STYLE>

<HTML>

```



```

<HEAD>
<TITLE>LHM Script Chooser</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
  <tr class="heading">
    <td width="50%" valign="center"><font color="white"><b>LHM Script
Chooser</b></font></td>
    <td><center></center></td>
    <td width="50%" align="right" valign="center"><font
color="white"><b></b>&nbsp;</font></td>
  </tr>
  <tr class="heading">
    <td colspan=3 align="center"><font color="white">&nbsp;</td>
  </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
  <tr><td><br></td></tr>
  <tr><td><H3>Please select one of the LHM Scripts below</H3></td></tr>
  <tr><td>Your original querystring information will be passed to the target script,
and it will open in a new window.</td></tr>
  <tr><td><br></td></tr>
</table>

<asp:Repeater id="lhmList" runat="server">
  <ItemTemplate >
    <li><a href = <%# DataBinder.Eval(Container.DataItem, "Name").ToString() &
"/default.aspx?" & qString & " target="_blank"" %> >
    <%# DataBinder.Eval(Container.DataItem, "Name").ToString() %>
    </a>
    </li>
  </ItemTemplate>
</asp:Repeater>

<table>
<tr class="hidden">
<td>default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00
:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRed
irectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig</td></tr>
</table>

</BODY>
</HTML>

```

IPv6

- [第 762 页的 IPv6](#)
 - [第 762 页的关于 IPv6](#)
 - [第 767 页的配置 IPv6](#)
 - [第 789 页的 IPv6 可视化](#)
 - [第 789 页的 IPv6 高可用性监控](#)
 - [第 790 页的 IPv6 诊断和监控](#)

IPv6

本附录介绍 IPv6 的 SonicOS 实施，IPv6 的运行方式以及如何为网络配置 IPv6。

主题：

- [第 762 页的关于 IPv6](#)
- [第 767 页的配置 IPv6](#)
- [第 789 页的 IPv6 可视化](#)
- [第 789 页的 IPv6 高可用性监控](#)
- [第 790 页的 IPv6 诊断和监控](#)

关于 IPv6

主题：

- [第 763 页的 IPv6 就绪认证](#)
- [第 763 页的 IPv6 技术概述](#)
- [第 765 页的 IPv6 优点](#)
- [第 766 页的目前支持的 SonicWall IPv6 服务和功能](#)
- [第 766 页的目前不支持的 SonicWall IPv6 功能](#)
- [第 766 页的支持的 IPv6 RFC](#)
- [第 767 页的不支持的 IPv6 RFC](#)

IPv6 就绪认证

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。

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。

如需更多信息，请参阅：<http://www.ipv6ready.org/>

i | 注：SonicOS 不支持 IPv6 向导。

IPv6 技术概述

每台连接到互联网的设备（计算机、打印机、智能手机、智能电表等）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: 340,282,366,920,938,463,374,607,431,768,211,456 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：

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

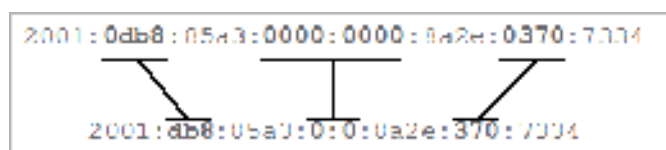
IPv6 地址在逻辑上分为两部分：64 位（子）网络前缀和 64 位接口识别符。以下是一个 IPv6 地址示例：

2001:0db8:85a3:0000:0000:8a2e:0370:7334

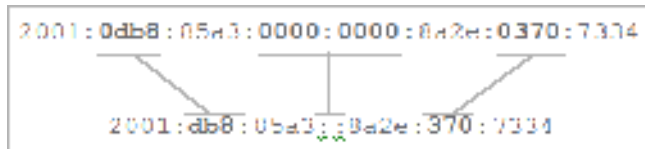
i | 注：IPv6 地址中的十六进制数值不区分大小写。

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缩写如下：



- 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 (::) 表示。结合这两个规则，本例的地址可以从完整形式缩写如下：



① | 提示：空地址或 0:0:0:0:0:0:0:0 的缩写为 ::。

IPv6 地址类型

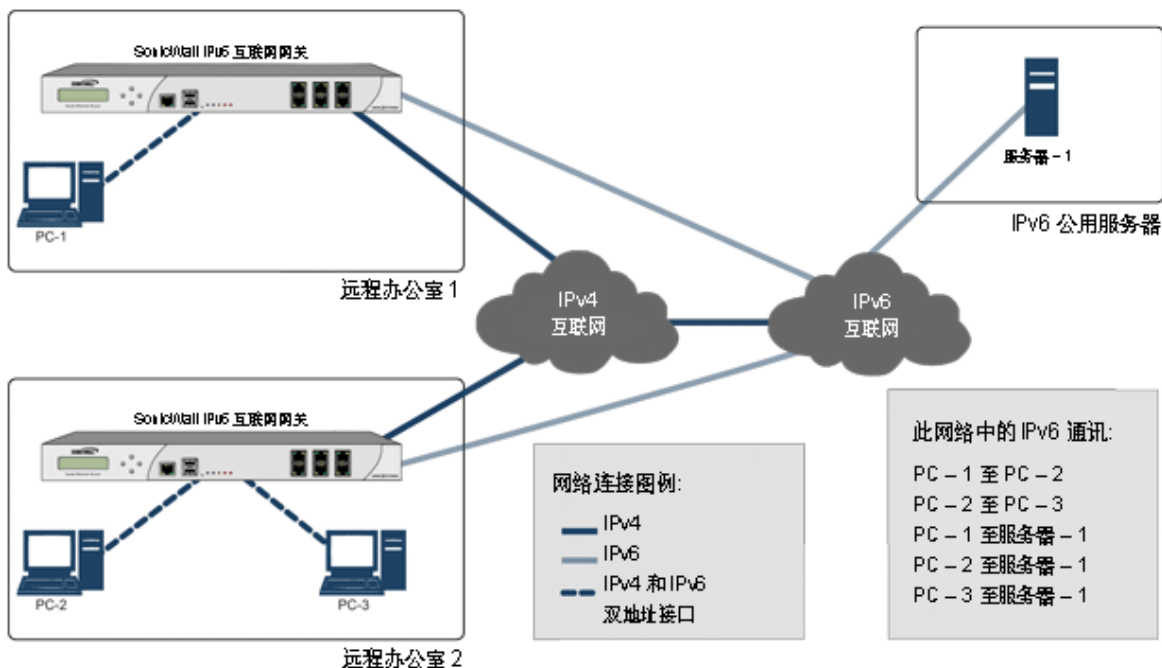
地址类型	完整的地址	缩写的地址
单播地址	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
组播地址	FF01:0:0:0:0:0:101	FF01::101
环回地址	0:0:0:0:0:0:1	::1
未指定地址	0:0:0:0:0:0:0	::

① | 注：网络必须具备 IPv4 互联网连接才能连至 IPv6 互联网。

① | 注：本地网络站点的计算机必须启用 IPv6 栈。

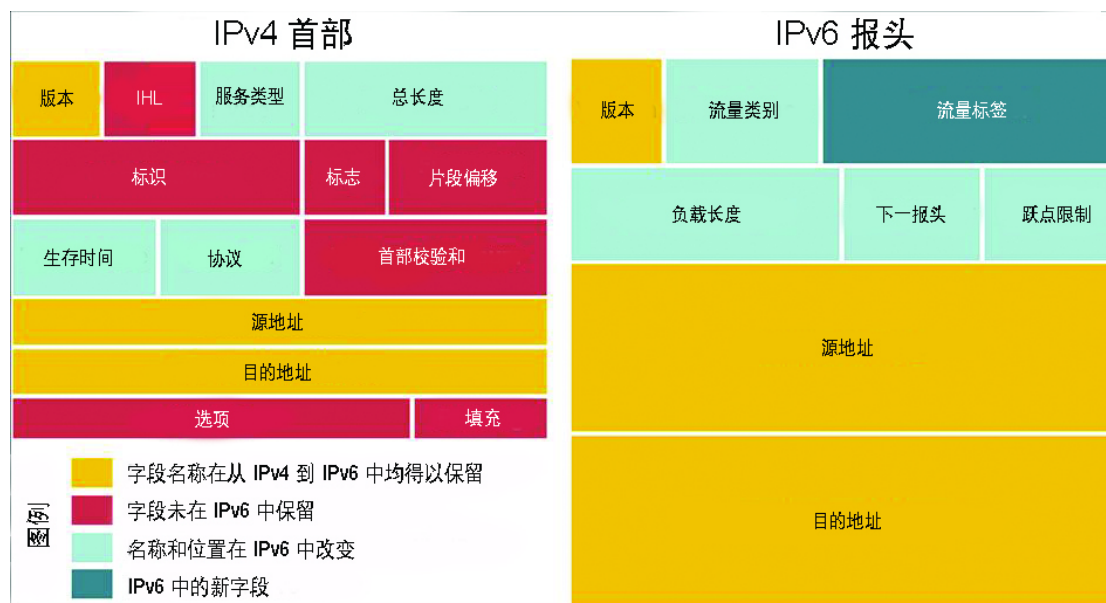
典型 IPv6 部署是一幅典型 IPv6 部署的连接模型简化图。

典型 IPv6 部署



IPv4 和 IPv6 标头元素的对比将比较 IPv4 和 IPv6 之间的标头元素。

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）
 - 6to4 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 - 强烈建议 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 SonicWall IPv6 服务和功能

如需当前支持的 IPv6 服务和功能的完整列表，请参阅知识库文章 [SonicOS 6.2.x 固件中支持/不支持的 IPv6 功能](#)。

目前不支持的 SonicWall IPv6 功能

i | 注：SonicOS 6.2 是双 IP 栈固件。IPv4 仍支持 IPv6 尚不支持的功能。

如需当前不支持的 IPv6 服务和功能的完整列表，请参阅知识库文章 [SonicOS 6.2.x 固件中支持/不支持的 IPv6 功能](#)。

支持的 IPv6 RFC

本章节列出 SonicOS 6.2 支持的 IPv6 RFC：

- 第 766 页的 [TCP/IP 栈和网络协议](#)
- 第 767 页的 [IPsec 合规](#)
- 第 767 页的 [NAT 合规](#)
- 第 767 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 768 页的 IPv6 接口配置](#)
- [第 777 页的配置 IPv6 隧道接口](#)
- [第 786 页的使用 IPv6 访问 SonicWall 管理界面](#)
- [第 786 页的 IPv6 网络配置](#)

- [第 788 页的 IPv6 访问规则配置](#)
- [第 788 页的 IPv6 高级防火墙设置](#)
- [第 788 页的 IPv6 IPsec VPN 配置](#)
- [第 789 页的 IPv6 的 SSL VPN 配置](#)

IPv6 接口配置

在 **网络 | 接口** 页面通过单击 **接口设置** 表右上角的视图 **IP 版本** 单选按钮的 **IPv6** 选项配置 IPv6 接口。

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。

i | **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。

i | **注：** 在切换到 IPv6 模式之前，必须通过 IPv4 接口页面配置接口的区域分配。

主题：

- [第 768 页的 IPv6 接口配置的限制性](#)
- [第 769 页的为 IPv6 静态模式配置接口](#)
- [第 770 页的配置高级 IPv6 接口选项和多个 IPv6 地址](#)
- [第 771 页的配置路由公告设置](#)
- [第 772 页的配置路由公告前缀设置](#)
- [第 772 页的配置 DHCPv6 模式的接口](#)
- [第 774 页的配置 IPv6 接口的高级设置](#)
- [第 775 页的查看 DHCPv6 协议信息](#)
- [第 775 页的配置自动模式的接口](#)
- [第 776 页的 PPPoE](#)
- [第 776 页的配置 VLAN 子接口](#)
- [第 777 页的配置有线模式的接口](#)

IPv6 接口配置的限制性

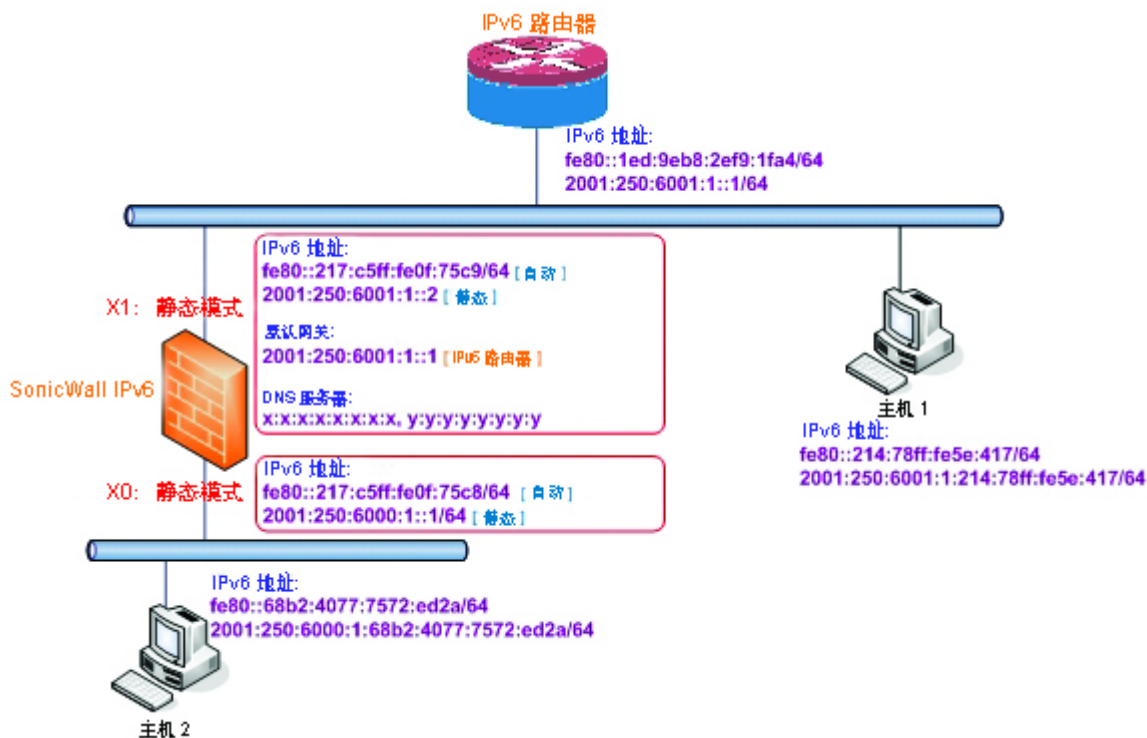
- 无法为 IPv6 配置 HA 接口。
- 只能将 SwitchPort 群组的父级接口配置为 IPv6 接口，因此交换机端口群组的所有子级都必须从该列表中排除。
- 区域和二层桥接群组是 IPv4 和 IPv6 在接口上共享的配置。在 IPv4 侧配置时，接口的 IPv6 侧将使用相同的配置。
- 只能为 WAN 区域接口配置默认网关和 DNS 服务器。
- IPv6 支持有线模式，但无法编辑任何设置。SonicOS 使用为 IPv4 设置的相同配置选项代替。

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。

IPv6 静态模式配置显示在静态模式中配置的 IPv6 样本拓扑结构。

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。将显示编辑接口对话框。

注：必须在 IPv4 寻址页面配置接口的区域分配。如需修改 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 ::。（双冒号是空地址或 0:0:0:0:0:0:0:0 的缩写。）
- 8 如果这是主要 WAN 接口，请输入最多三个 DNS 服务器 IPv6 地址。同样地，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 在编辑接口对话框中，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。将显示添加接口 IPv6 地址对话框。
 - ① 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 地址的子网前缀以向接口公告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。默认情况下未选中该选项。
 - ① 提示：如果防火墙在纯 IPv4 环境中部署，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。默认情况下已选中该选项。
 - ① 注：禁用此选项时，将从此接口移除所有分配的自治 IPv6 地址。

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，将从此接口移除所有分配的自治 IPv6 地址。

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。最小值为 0，最大值为 9，默认值为 1。值 0 表示未在接口执行 DAD。
- 在邻居发现的基本可访问时间 (秒) 中，输入用于计算接口的随机可达时间值的基础值（以秒为单位）。最小值为 0，最大值为 9999，默认值为 30。

值为 0 表示未指定参数并使用网络 | 邻居发现中的全局设置。但是，如果在该接口上启用了 RA，则使用路由公告选项卡中的可达时间选项中的值。

- 选择启用每接口的最大 NDP 大小，为每个接口启用最大 NDP 大小。每个接口都应该有最大 NDP 大小以防止系统资源消耗殆尽。
 - 在“每接口的最大 NDP 大小”字段中输入最大 NDP 大小。最小值为 64，最大值为 9999，默认值为：WAN 接口为 **128**，其他接口为 **1200**。
- 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。SonicWall 的 IPv6 实施与路由器和前缀发现中的 RFC 4861 完全兼容。

i | 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 在编辑接口对话框中，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 (秒)** - 输入从接口发送主动提供的组播路由公告之间的时间间隔（秒）。以最小和最大间隔之间的随机值发送公告：
 - 最小间隔 - 输入路由公告之间允许的最短间隔。最短时间为 3 秒，最长为 1350 秒，默认最短时间为 **200** 秒。
 - 最大间隔 - 输入路由公告之间允许的最长间隔。最短时间为 4 秒，最长为 1800 秒，默认最长时间为 **600** 秒。
 - **链路 MTU** - 输入为接口链路推荐的 MTU。最小值为 0，最大值为 99999，默认值为 **0**，表示防火墙不发布链路的 MTU。
 - **可达时间 (秒)** - 输入节点在收到可达到确认后认为可达到邻居的时间。最小值为 0，最大值为 9999999999，默认值为 **0**，表示此防火墙未指定此参数。
 - **重传时间** - 输入重新传输的邻居请求消息之间的时间。最小值为 0，最大值为 9999999999，默认值为 **0**，表示此防火墙未指定此参数。
 - **目前跳数限制** - 输入应填写到出站 IP 数据包的 IP 标头跃点数字段中的默认值。最小值为 0，表示此防火墙未指定此参数；最大值为 **255**；默认值为 **64**。
 - **路由生命期 (秒)** - 输入将接受防火墙为默认路由器的生命期。最小值为 0 秒，这意味着路由器并非默认路由器；最大值为 9000 秒，默认值为 **1800** 秒。
 - **路由器偏好设置** - 指示公告默认路由器是否应优先于其他默认路由器。从下拉菜单中选择高、中（默认）或低。
- 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，该标志表示通过动态主机配置协议可以使用 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，该标志表示可通过动态主机配置协议获得其他配置信息。

配置路由公告前缀设置

公告前缀为主机提供用于连接确定和地址自动配置的前缀。

配置路由公告前缀的步骤如下：

- 1 转至编辑接口对话框的路由公告选项卡上的前缀列表设置表。
- 2 单击添加前缀按钮。将显示添加公告前缀对话框。
- 3 输入将与路由公告消息一起发布的前缀。
- 4 输入有效生命期 (分钟)，设置前缀可用于连接确定的时间长度。最小值为 1；最大值为 71582789，这意味着生命期是无限的，默认值为 43200 分钟。
- 5 输入首选生命期 (分钟)，设置通过无状态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。最小值为 1；最大值为 71582789，这意味着生命期是无限的；默认值为 10080 分钟。
- 6 可选地，选择连接复选框以在“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。
- 7 可选地，选择自治的复选框以在“前缀信息”选项中启用自治地址配置标志，以指示该前缀可用于无状态地址配置。
- 8 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。

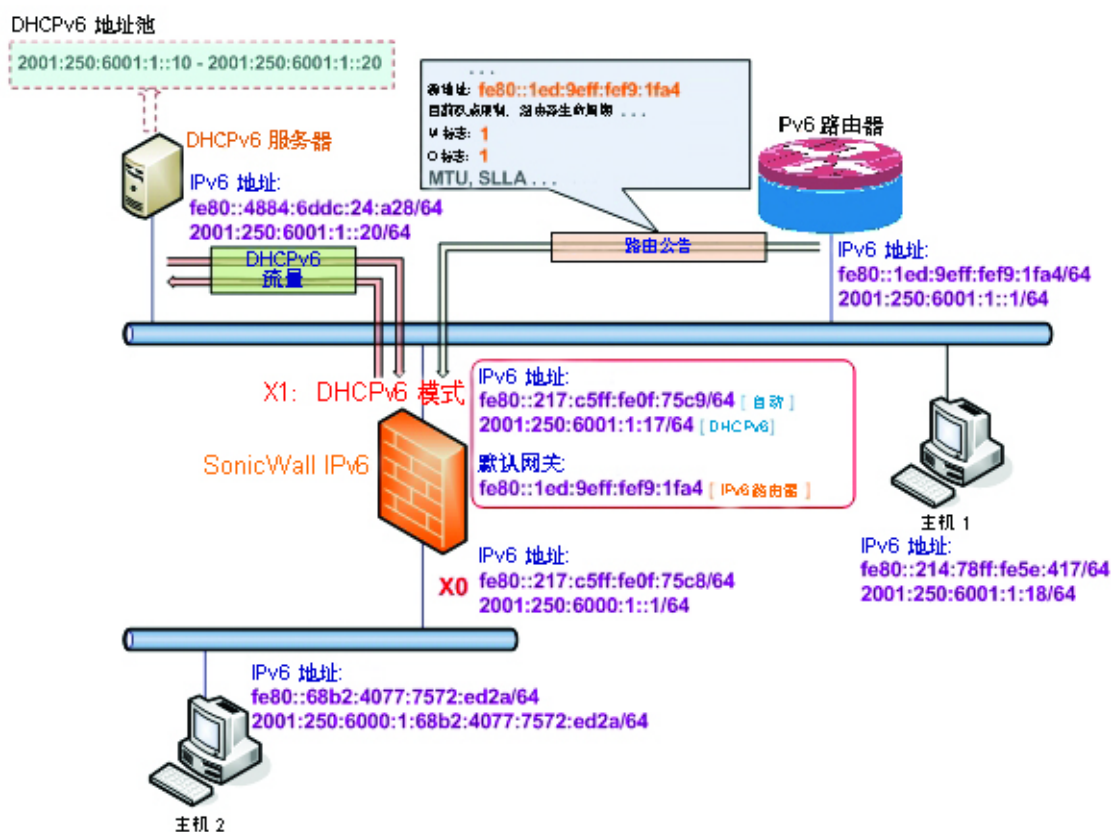
选择哪种模式取决于发布的路由公告消息中的受管理 (M) 地址配置及其他 (O) 配置标志：

DHCPv6 基础结构

标志		配置
M	O	
0	0	无 DHCPv6 基础结构。
1	1	IPv6 主机对 IPv6 地址和其他网络参数设置使用 DHCPv6。
0	1	IPv6 主机只对 IPv6 地址分配使用 DHCPv6。
1	0	IPv6 主机仅对其他网络参数设置使用 DHCPv6，称为 DHCPv6 无状态。

DHCPv6 拓扑显示 DHCPv6 拓扑结构示例。

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 转至管理 | 系统设置 | 网络 | 接口。
- 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 DHCPv6 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 DHCPv6 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 选择接口的 **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。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** - 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。请参阅 **DHCPv6 基础结构表**。
 - **手动** - 不管收到的路由公告如何，总是手动配置 DHCPv6 模式。
- 仅请求无状态信息选项确定使用哪种 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

配置高级 IPv6 接口设置的步骤如下：

- 1 在编辑接口对话框中，单击高级选项卡。
 - 2 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。默认情况下未选中该选项。
- i | 提示：** 如果防火墙在纯 IPv4 环境中部署，SonicWall 建议启用该选项。
- 3 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。默认情况下未选中该选项。

i | 注： 如果禁用此选项，则将从此接口移除所有分配的自治 IPv6 地址。

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。

选择此选项后，“启用无状态地址自动配置”选项可用。

- 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，将从此接口移除所有分配的自治 IPv6 地址。

i | 注： 如果禁用此选项，则将从此接口移除所有分配的自治 IPv6 地址。

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。

- 4 输入**重复地址检测重传**的数值以指定在执行重复地址检测 (DAD) 时向此接口分配暂定地址前发送的连续邻居请求消息数。最小值为 0，表示不在接口上执行 DAD；最大值为 9；默认值为 1。

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）。

- 5 在邻居发现的基本可访问时间 (秒) 中，输入用于计算接口的随机可达时间值的基础值（以秒为单位）。最小值为 0，最大值为 9999，默认值为 30。

值为 0 表示未指定参数并使用网络 | 邻居发现中的全局设置。但是，如果在该接口上启用了 RA，则使用路由公告选项卡中的可达时间选项中的值。

- 6 选择启用每接口的最大 NDP 大小，为每个接口启用最大 NDP 大小。每个接口都应该有最大 NDP 大小以防止系统资源消耗殆尽。默认情况下已选中该选项。

在“每接口的最大 NDP 大小”字段中输入最大 NDP 大小。最小值为 64，最大值为 9999，默认值为：WAN 接口为 128，其他接口为 1200。

查看 DHCPv6 协议信息

在 DHCPv6 模式中配置 IPv6 接口时，协议选项卡显示附加 DHCPv6 信息。

- **DHCPv6 常规信息**
 - **DHCPv6 状态：** 如果为：
 - 无状态模式配置了接口，DHCPv6 状态将为无状态。
 - 状态模式配置了接口，DHCPv6 状态将为已启用或已禁用。

当接口处于状态 DHCPv6 模式时，将鼠标移到备注图标上会显示该接口的当前路由公告信息。
 - **DHCPv6 服务器：** DHCPv6 服务器的 IPv6 地址。
 - **DHCPv6 DUID：** DUID（DHCP 唯一标识符）或主机标识符。
- **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：
 - IAID（身份关联标识符） • 类型 • IPv6 地址 • 租约过期
- **无状态配置设置需要通过 DHCPv6**
 - **DNS 服务器 1/2/3：** 任何 DNS 服务器的 IPv6 地址。

可以通过单击适当的按钮来更新、发布或刷新 DNS 服务器。
- **通过 DHCPv6 授权已取得的前缀：** 显示任何获得的状态 IPv6 地址的授权前缀的信息：
 - IAID • 类型 • IPv6 前缀 • 前缀长度 • 租约过期

可以通过单击适当的按钮来更新、发布或刷新前缀。

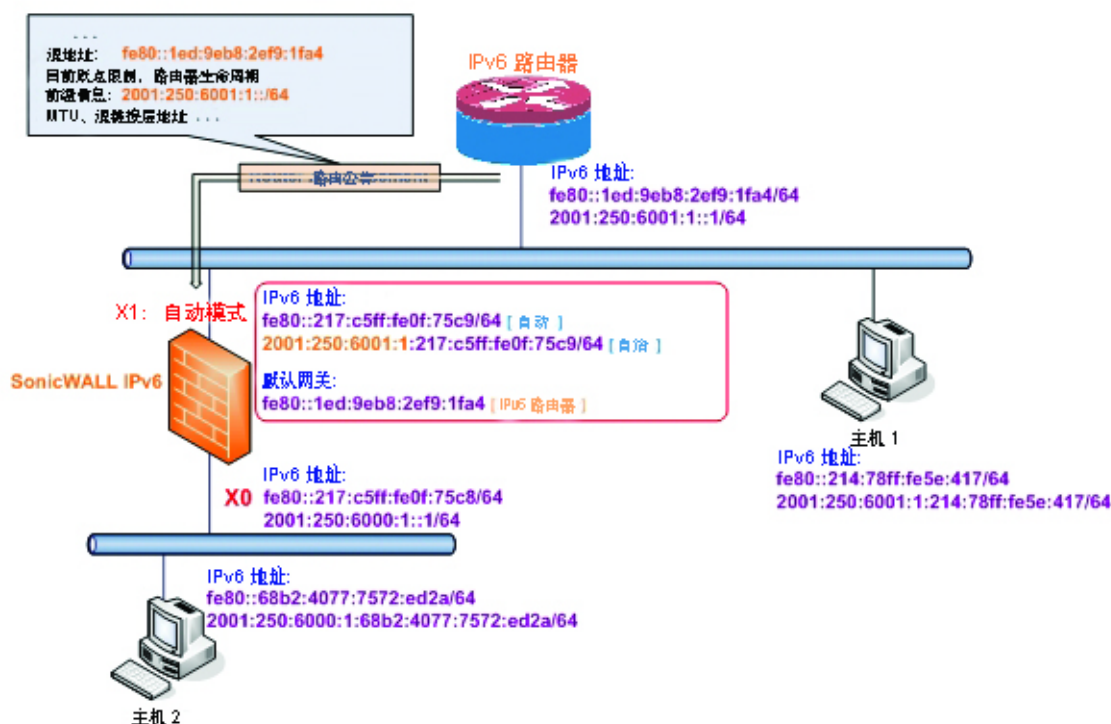
配置自动模式的接口

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。安全设备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 区域接口上无自动模式。

IPv6 自动模式配置显示在自动模式下配置的 IPv6 示例拓扑。

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 转至管理 | 系统设置 | 网络 | 接口。
- 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 中仅支持 PPPoE 客户端模式。

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 [配置虚拟接口 \(VLAN 子接口\)](#)。

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

① | 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 265 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。

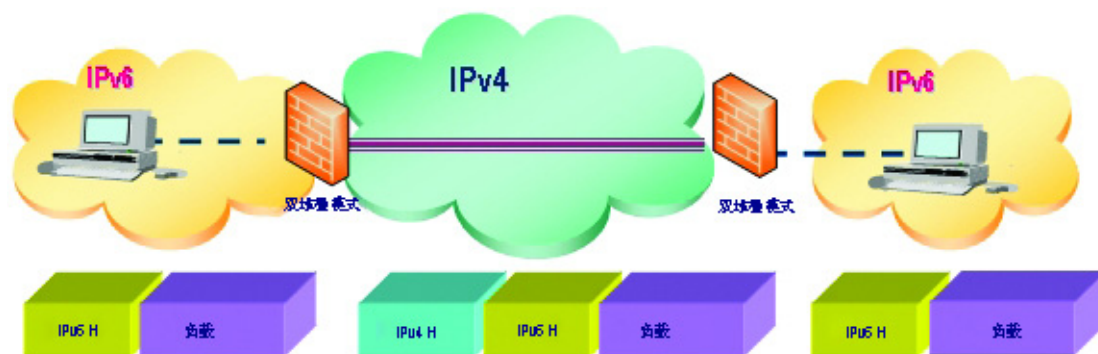
配置 IPv6 隧道接口

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 数据包的地址确定 IPv4 端点。IPv4 组播隧道通过邻居发现机制确定端点。

[IPv6 至 IPv4 隧道接口](#)描述了 IPv6 至 IPv4 隧道。

IPv6 至 IPv4 隧道接口



主题：

- 第 777 页的[配置 6 至 4 自动隧道](#)
- 第 779 页的[配置用于非 2002 前缀访问的 6to4 中继](#)
- 第 779 页的[配置手动 IPv6 隧道](#)
- 第 780 页的[配置 GRE IPv6 隧道](#)
- 第 780 页的[IPv6 前缀授权](#)
- 第 782 页的[6rd 隧道接口](#)
- 第 783 页的[配置 ISATAP 隧道](#)

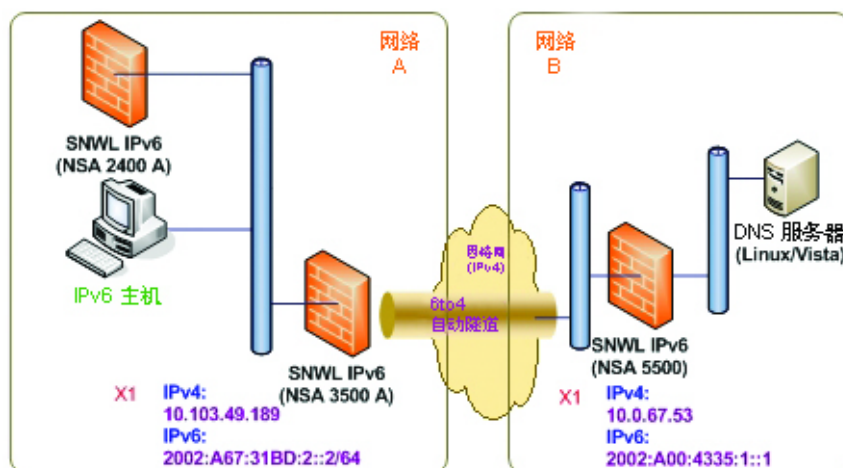
配置 6 至 4 自动隧道

6to4 自动隧道是自动隧道：隧道端点提取自封装式 IPv6 数据包。无需手动配置。

6to4 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 6to4 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，请参阅 RFC 3056。

6to4 自动隧道拓扑结构显示 6to4 自动隧道拓扑结构的示例。

6to4 自动隧道拓扑结构



在 IPv6 至 IPv4 隧道接口中，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：只能在安全设备上配置一个 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 6to4 自动隧道的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 接口。
- 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此选项。有关此选项的更多信息，请参阅第 230 页的 HTTP/HTTPS 重定向。

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**。

i | 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。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。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 6to4 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。

启用 **6to4** 中继的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 路由**。
- 2 单击**添加**按钮以创建路由策略，该策略可以通过 6to4 自动隧道接口路由以 2003 前缀为目标的所有流量：

可以向 6to4 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 6to4 隧道访问有非 2002：前缀的 IPv6 目标。

i | 注：网关必须是有 2002：前缀的 IPv6 地址。

配置手动 IPv6 隧道

在防火墙上配置 **6to4** 隧道的步骤如下：

- 1 转至**管理 | 系统设置 | 网络 | 接口**。
- 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 地址**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**。

i | 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。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。无法为其他协议选择此选项。

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**。

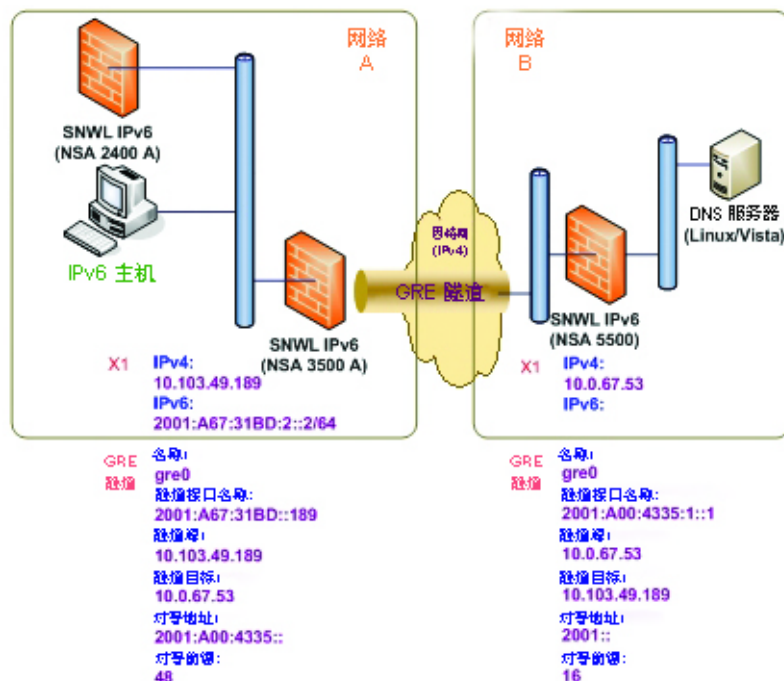
i | 注：仅选择 **HTTPS** 可自动启用添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向选项。有关此选项的更多信息，请参阅第 230 页的 **HTTP/HTTPS 重定向**。如果您还选择了 **HTTP**，则系统将取消选择添加规则，以启用从 **HTTP** 到 **HTTPS** 的重定向选项，且您无法选择该选项。

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。[GRE IPv6 隧道配置](#)显示 GRE IPv6 示例隧道。

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 DHCPv6 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 781 页的[在上游接口配置 IPv6 前缀授权](#)

- 第 781 页的在下游接口上配置 IPv6 前缀授权

i | **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 转至**管理 | 系统设置 | 网络 | 接口**。
- 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。编辑接口对话框显示。
i | **注：** 区域始终为 **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 如需查看配置的 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 转至**管理 | 系统设置 | 网络 | 接口**。
- 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。编辑接口对话框显示。
- 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 如需查看新的 IPv6 PD 接口，请转至**管理 | 系统设置 | 网络 | 路由**页面。

13 选择 IPv6 选项。

显示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。

i | 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**管理 | 系统设置 | 网络 | 路由上的路由策略**面板中，有四项用于 6rd 隧道接口的默认路由策略。

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 转至**管理 | 系统设置 | 网络 | 接口**。
- 2 在视图 IP 版本中，选择 **IPv6**。
- 3 在接口设置面板，单击**添加接口**按钮。
i 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**步骤 3**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**字段中，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**。
i 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。

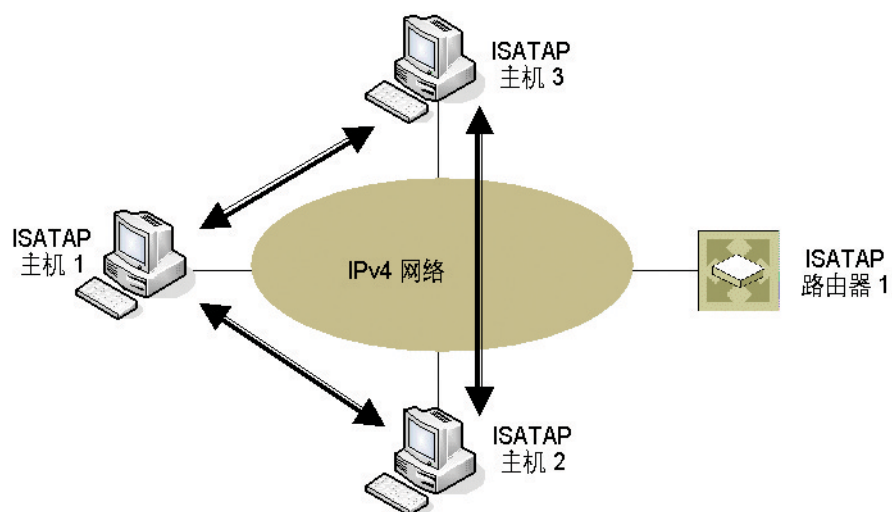
配置 ISATAP 隧道

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。

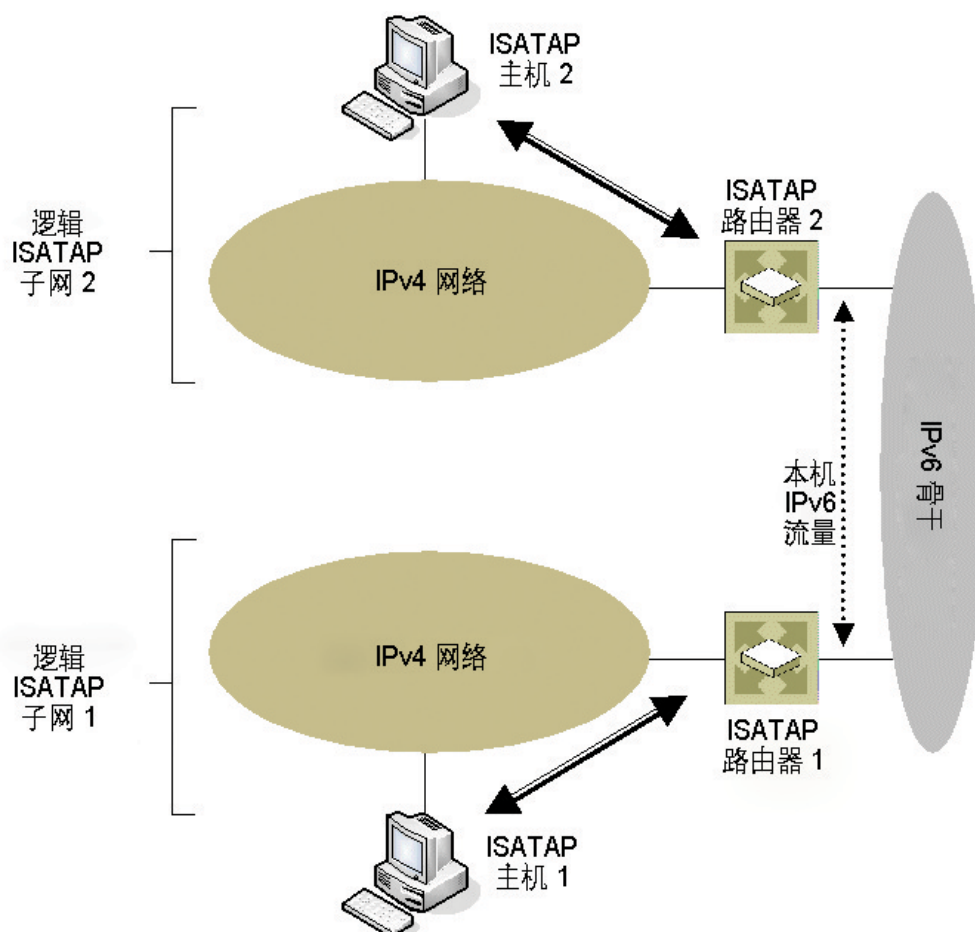
在 **ISATAP 主机和相同逻辑 ISATAP 子网之间**传送流量显示在相同逻辑 ISATAP 子网上的 ISATAP 主机之间传送 ISATAP 流量：

在 ISATAP 主机和相同逻辑 ISATAP 子网之间传送流量



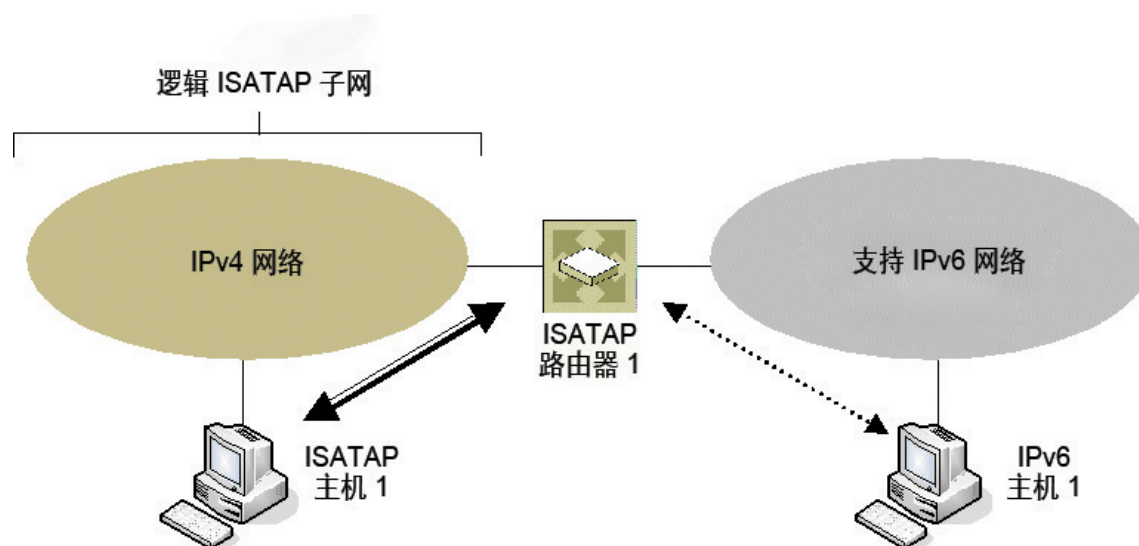
在 ISATAP 主机和不同 ISATAP 子网之间传送流量显示在不同 ISATAP 子网上的主机之间传送 ISATAP 流量:

在 ISATAP 主机和不同 ISATAP 子网之间传送流量



在 ISATAP 主机与启用 IPv6 的网络上的主机之间传送数据包显示在 ISATAP 主机与启用 IPv6 的网络上的主机之间传送数据包。

在 ISATAP 主机与启用 IPv6 的网络上的主机之间传送数据包



在在 ISATAP 主机与启用 IPv6 的网络上的主机之间传送数据包显示的場景中，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 支持允许安全设备在面向 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。

配置 ISATAP 隧道的步骤如下：

- 1 在管理 | 系统设置 | 网络 | 接口的视图 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 - 从下拉菜单中选择接口。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 - 从下拉菜单中选择地址对象（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。

另外，可以在管理 | 安全配置 | 防火墙设置 | 高级设置中指定 SonicOS 解析 ISATAP 主机查询的方法。如需配置高级防火墙设置的信息，请参阅 SonicOS 安全配置。

使用 IPv6 访问 SonicWall 管理界面

在安全设备上配置 IPv6 寻址后，可以通过在浏览器的 URL 字段输入安全设备的 IPv6 来访问 SonicWall 管理界面。

IPv6 网络配置

主题：

- [第 786 页的 IPv6 DNS](#)
- [第 786 页的地址对象](#)
- [第 786 页的基于策略的路由](#)
- [第 787 页的 IPv6 NAT 策略](#)
- [第 787 页的邻居发现协议](#)
- [第 788 页的 DHCPv6 配置](#)

IPv6 DNS

IPv6 的 DNS 使用与 IPv4 相同的配置方法。单击**管理 | 系统设置 | 网络 | DNS**左上方的视图 **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。如需配置地址对象的信息，请参阅 SonicOS 策略。

i | 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 群组，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。由于可以为一个接口分配多个 IPv6，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**管理 | 系统设置 | 网络 | 路由**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。

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

可以在**管理 | 策略 | 规则 | NAT 策略**上为 IPv6 或 NAT64 配置 NAT 策略。配置 IPv6 NAT 策略时，除非指定了 NAT64 的 IP 版本，否则源和目标对象只能是 IPv6 地址对象。如需配置 NAT 策略的更多信息，请参阅 SonicOS 策略。

i | 注：当前不支持 IPv6 探查 NAT 策略。

NAT64 状态检测网络流支持

状态检测网络流（通常包括应用层数据）需要即时创建缓存条目。根据数据包过滤器的规则表，这些缓存条目通常是非法的，但是由于应用层数据中的特定指令（例如，添加了用于 FTP 数据连接的入站缓存条目）而允许它们。

在 SonicOS 中，这些网络流与一般应用层协议流（例如 HTTPS 或 SNMP）的处理方式不同。这些状态检测网络流包括 FTP、TFTP、H.323、MSN、Oracle、PPTP、RTSP 和 RealAudio。当客户端和服务器通过控制信道相互通讯时，状态检测网络流需要预测数据缓存的创建。

我们的系统支持 FTP（包括主动和被动模式）和 TFTP 协议，适用于 NAT64。

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。

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**管理 | 系统设置 | 网络 | 邻居发现**。
- 2 单击**添加**按钮。
- 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：

- 可访问 - 已知可在 30 秒内访问此邻居。

- 过时 - 已知不再能访问此邻居，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。

DHCPv6 配置

在**管理 | 系统设置 | 网络 | DNS**上选中视图 **IP 版本** 单选按钮中的 **IPv6** 选项后，可以通过类似于配置 IPv4 的方式配置 DHCPv6 服务器。

IPv6 访问规则配置

IPv6 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，而非 IPv4 地址对象。如需防火墙访问规则的更多信息，请参阅 SonicOS 策略。

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**管理 | 安全配置 | 防火墙设置 | 高级设置**中配置 IPv6 的高级防火墙设置，包括数据包限制和流量限制。如需配置高级防火墙设置的信息，请参阅 SonicOS 安全配置。

IPv6 IPsec VPN 配置

在**管理 | 连接 | VPN | 设置**左上方的视图 **IP 版本** 单选按钮中选择 **IPv6** 选项后，可以通过类似于配置 IPv4 VPN 的方式为 IPv6 配置 IPsec VPN。如需配置 VPN 的信息，请参阅 SonicOS 连接。

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。

配置 IPv6 VPN 策略时，在对话框的**常规**中，网关必须使用 IPv6 地址进行配置。不支持 FQDN。在配置 IKE 身份验证时，IPv6 地址可用于本地和对端 IKE ID。

在 VPN 策略的**网络**上，必须对**本地网络**和**远程网络**选择 IPv6 地址对象（或仅包含 IPv6 地址对象的地址群组）。

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**中，IPv6 和 IPv4 的配置完全相同，不过 IPv6 仅支持 **IKEv2 模式**。

在**高级**上，只能为 IPv6 VPN 策略配置启用 **Keep Alive** 和 **IKEv2** 设置。

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非区域，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**管理 | 连接 | SSL VPN | 客户端设置**上，首先配置传统的 IPv6 IP 地址池，然后再配置 IPv6 IP 池。客户端将分配两个内部地址：一个 IPv4 和一个 IPv6。如需配置 SSL VPN 的更多信息，请参阅 SonicOS 连接。自我注释：[连接](#)

在**管理 | 连接 | SSL VPN | 客户端设置**的编辑设备配置文件对话框中，您可以从所有地址对象（包括所有预定义的 IPv6 地址对象）中选择客户端路由。

注：支持 IPv6 FQDN。

IPv6 可视化

App 流量报告和实时监控的 IPv6 可视化是 IPv4 可视化的扩展，在管理界面中提供了接口/应用程序速率的实时监控和会话的可视性。您可以查看员工正在访问的网站、其网络中正在使用的应用程序和服务及其使用程度，从而监督向贵组织内/外传输的内容。如需这些可视化工具的更多信息，请分别参阅 SonicOS 调查和 SonicOS 监控。

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

App 流量报告和实时监控可视化在 IPv6 和 IPv4 中的配置相同。如需这些可视化工具的更多信息，请分别参阅 SonicOS 调查和 SonicOS 监控。

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。

在**管理 | 系统设置 | 高可用性 | 监控设置**上的 IPv6 和 IPv4 视图之间进行切换，以便轻松配置这两个 IP 版本。审校问题：[如何设置 HA 监控？](#)

主题：

- [第 790 页的 IPv6 高可用性监控功能限制](#)
- [第 790 页的 IPv6 高可用性探测](#)
- [第 790 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。如果活动的安全设备无法访问已探测的 IPv6 地址，但闲置的安全设备可以，则备用安全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 并参考第 762 页的 IPv6 以了解配置详细信息。

在配置 IPv6 HA 监控时请考虑以下因素：

- 物理/链接监控和虚拟 MAC 显示为灰色，因为它们是第二层属性。也就是说，IPv4 和 IPv6 使用这些属性，所以必须在 IPv4 监控页面进行配置。
- 主要/备用 IPv6 地址必须位于接口的同一子网中，并且不得与主要/备用安全设备的全局 IP 或 Link-Local-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，则主要/备用监控 IP 不得为未指定（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 790 页的 [数据包监控](#)
- 第 791 页的 [IPv6 Ping](#)
- 第 791 页的 [IPv6 DNS 名查找和反向名称解析](#)

数据包监控

调查 | 工具 | 数据包监控完全支持 IPv6。此外，IPv6 关键字可用于过滤数据包捕获。如需数据包监控的更多信息，请参阅 SonicOS 调查。

IPv6 Ping

Ping 一个域名时，工具使用返回的第一个 IP 地址，并显示实际的 Ping 地址。如果同时返回了 IPv4 和 IPv6 地址，则默认情况下安全设备会对 IPv4 地址执行 ping 操作。ping 工具包含一个**首选 IPv6 网络**选项，启用此选项后，可以使安全设备对 IPv6 地址执行 ping 操作。如需 IPv6 Ping 的更多信息，请参阅 SonicOS 调查。

IPv6 DNS 名查找和反向名称解析

执行 IPv6 DNS 名称查找或 IPv6 反向名称解析时，您必须输入 DNS 服务器地址。可以使用 IPv6 或 IPv4 地址。如需这些工具的更多信息，请参阅 SonicOS 调查。

BGP 高级路由

- [第 792 页的 BGP 高级路由](#)
 - [第 792 页的关于 BGP](#)
 - [第 799 页的注意](#)
 - [第 799 页的配置 BGP](#)
 - [第 809 页的验证 BGP 配置](#)
 - [第 812 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。

i | **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 792 页的关于 BGP](#)
- [第 799 页的注意](#)
- [第 799 页的配置 BGP](#)
- [第 809 页的验证 BGP 配置](#)
- [第 812 页的 IPv6 BGP](#)

关于 BGP

主题：

- [第 793 页的什么是 BGP?](#)
- [第 793 页的后台信息](#)
- [第 794 页的自治系统](#)
- [第 795 页的通过 VPN 隧道接口的 BGP](#)
- [第 795 页的为什么使用 BGP?](#)
- [第 795 页的 BGP 的工作方式](#)
- [第 798 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 支持允许使用 SonicWall 安全设备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/多宿主”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 管理界面的**网络 | 路由**页面上启用，然后再通过 SonicOS 命令行接口 (CLI；请参阅《SonicOS CLI 参考指南》) 对其进行完全配置。

BGP 授权要求表中显示了 BGP 授权要求。

BGP 授权要求

平台	需要附加许可证
SM 9600	无，已包含 BGP
SM 9400	无，已包含 BGP
SM 9200	无，已包含 BGP
NSA 6600	无，已包含 BGP
NSA 5600	无，已包含 BGP
NSA 4600	无，已包含 BGP
NSA 3600	SonicOS 扩展 01-SSC-7091
NSA 2650	SonicOS 扩展许可证
NSA 2600	SonicOS 扩展许可证
TZ600	SonicOS 扩展许可证
TZ500/TZ500 W	SonicOS 扩展许可证
TZ400/TZ400 W	SonicOS 扩展许可证
TZ300/TZ300 W	N/A
SOHO W	N/A

 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。

为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

为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有效发布 (BGP 的优势之一)，所以上述担心并无必要。

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 以外的所有流量转至其 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)。

通过 VPN 隧道接口的 BGP

BGP 接口同时支持已编号和未编号的隧道接口。可以设置 BGP 和未编号的隧道接口的所有平台都支持此功能。

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。

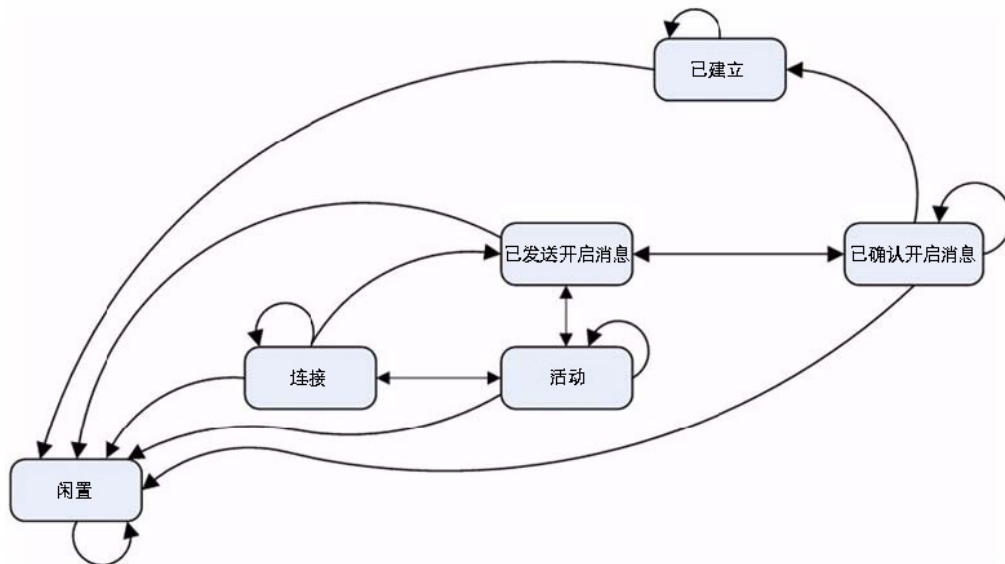
No. .	Time	Source	SPort	Destination	DPort	Protocol	Info
8	2010-07-18 09:42:54.581409	172.16.228.228	179	172.16.237.237	55856	BGP	OPEN Message
9	2010-07-18 09:42:54.581441	172.16.237.237	55856	172.16.228.228	179	TCP	55856 > 179 [ACK] Seq=854323707 Ack=225817942
10	2010-07-18 09:42:54.581555	172.16.237.237	55856	172.16.228.228	179	BGP	KEEPALIVE Message
11	2010-07-18 09:42:54.581576	172.16.228.228	179	172.16.237.237	55856	BGP	KEEPALIVE Message
12	2010-07-18 09:42:54.581599	172.16.237.237	55856	172.16.228.228	179	TCP	55856 > 179 [ACK] Seq=854323726 Ack=225817961
13	2010-07-18 09:42:54.582248	172.16.228.228	179	172.16.237.237	55856	BGP	KEEPALIVE Message
14	2010-07-18 09:42:54.582294	172.16.237.237	55856	172.16.228.228	179	BGP	KEEPALIVE Message
15	2010-07-18 09:42:54.622267	172.16.228.228	179	172.16.237.237	55856	TCP	179 > 55856 [ACK] Seq=225817980 Ack=854323745
16	2010-07-18 09:42:55.581894	172.16.237.237	55856	172.16.228.228	179	BGP	UPDATE Message
17	2010-07-18 09:42:55.582293	172.16.228.228	179	172.16.237.237	55856	TCP	179 > 55856 [ACK] Seq=225817980 Ack=854323799
18	2010-07-18 09:42:55.582500	172.16.228.228	179	172.16.237.237	55856	BGP	UPDATE Message
19	2010-07-18 09:42:55.582593	172.16.237.237	55856	172.16.228.228	179	TCP	55856 > 179 [ACK] Seq=854323799 Ack=225818035
20	2010-07-18 09:42:55.582754	172.16.228.228	179	172.16.237.237	55856	BGP	UPDATE Message


```
Border Gateway Protocol
├── UPDATE Message
│   ├── Marker: 16 bytes
│   ├── Length: 52 bytes
│   ├── Type: UPDATE Message (2)
│   ├── Unfeasible routes length: 0 bytes
│   └── Total path attribute length: 25 bytes
├── Path attributes
│   ├── ORIGIN: IGP (4 bytes)
│   ├── AS_PATH: 7675 12345 (14 bytes)
│   ├── NEXT_HOP: 172.16.228.228 (7 bytes)
│   └── Network layer reachability information: 4 bytes
```

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。

BGP 有限状态机



BGP 有限状态说明

州/省	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。如果无 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	尝试与对端项建立 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端项的连接。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端项。
已发送开启消息	等待来自对端项的“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，与对端项交换更新信息。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 对端项之间的第一条消息。包含建立对端会话的必需信息，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**通知子代码**表中所示：

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 - 对端项未配置	已移除对端配置
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** - 用于对端项重新发送其路由的请求。

BGP 功能

BGP 更新消息可以包含如 **BGP 更新消息属性**表所示的属性：

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

BGP 更新消息属性

值	代码
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)
27-254	未分配
255	保留用于开发

如需 BGP 属性的更多信息，请参阅：<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。
由于	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路由信息。

注意

缩放	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 中无多路径支持 (“最多路径”功能)。这样就阻止了负载均衡，且不拆分网络。
环回	目前无环回接口支持。
NAT	BGP 适用于路由。但不能与 NAT 良好共存。
非对称路径	状态安全设备目前不处理非对称路径，尤其对于穿越多个安全设备的情况。

配置 BGP

主题：

- [第 799 页的 BGP 的 IPSec 配置](#)
- [第 801 页的基本 BGP 配置](#)
- [第 802 页的 BGP 路径选择过程](#)
- [第 805 页的 AS_Path 预置](#)
- [第 805 页的多出口标识 \(MED\)](#)
- [第 806 页的 BGP 团体](#)
- [第 807 页的同步和自动汇总](#)
- [第 807 页的防止意外中转 AS](#)
- [第 809 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，SonicWall 推荐配置 IPSec 隧道用于 BGP 会话。IPSec 隧道和 BGP 彼此独立配置。如需为 BGP 配置 IPSec 隧道的信息，请参阅 SonicOS 连接。

配置用于 BGP 的 IPsec 隧道的步骤如下：

- 1 IPsec 隧道完全在 SonicOS 管理界面的**管理 | 连接 | VPN** 配置部分进行配置。配置 IPsec 隧道时，请确保下列选项已设置：

选项	值
策略类型	站点到站点 注： 通过 IPsec 的 BGP 必须使用站对站 VPN 隧道。
IPsec 主要网关名或地址	远程对等项的 IP 地址
本地 IKE ID	SonicWall 安全设备的 IP 地址
对等 IKE ID	远程对等项的 IP 地址
网络 从列表中选择目标网络	远程对等项的 IP 地址
高级 启用 Keep Alive	启用

i | **重要：**在 IPsec 上配置 BGP 时：

- 1 配置 IPsec 隧道。
- 2 在配置 BGP 之前验证通过隧道的连接。

i | **注：**如需配置 VPN 策略的方法信息，请参阅 SonicOS 连接。

- 2 通过在添加路由策略时为**服务选项**选择 **BGP**，可以在**管理 | 系统设置 | 网络 | 路由**页面上启用 BGP。如需了解添加路由策略的方法，请参阅第 408 页的**配置 BGP 高级路由**；对于基本的 BGP 配置，请参阅第 801 页的**基本 BGP 配置**。
 - 3 通过 SonicOS 命令行界面完成路由配置。如需 SonicOS CLI 的信息，请参阅《SonicOS **命令行界面指南**》。
 - 4 在安全设备上配置了 VPN 策略时，请在远程对等项上完成相应的 IPsec 配置。
 - 5 当远程对等项上的 IPsec 配置完成时，请返回到**管理 | 连接 | VPN | 基本设置**，并启用 VPN 策略以启动 IPsec 隧道。
 - 6 在 SonicWall 安全设备上使用 ping 诊断对 BGP 对等项 IP 地址执行 ping 操作。如需 ping 诊断的更多信息，请参阅 SonicOS 调查。
 - 7 使用 Wireshark 确保请求和响应封装在 ESP 数据包中。
- i** | **注：**按照本示例中的配置，已路由的流量不会通过用于 BGP 的 IPsec 隧道。该流量的发送和接收畅通无阻，这很可能是预期行为，因为目标是保护 BGP 而非所有已路由的网络流量。

基本 BGP 配置

在 SonicWall 安全设备上配置 BGP 的步骤如下：

- 1 转至管理 | 系统设置 | 网络 | 路由。

#	源	目标	服务	TOS/掩码	网关	接口	Metric	优先级
1	IPv4 MGMT IP	任何	任何	任何	MGMT Default Gateway	MGMT	1	1
2	IPv4 任何	MGMT IP	任何	任何	0.0.0.0	MGMT	1	2
3	IPv4 任何	255.255.255.255/32	任何	任何	0.0.0.0	X0	20	6
4	IPv4 任何	X1 Default Gateway	任何	任何	0.0.0.0	X1	20	7
5	IPv4 任何	X0 Subnet	任何	任何	0.0.0.0	X0	20	8
6	IPv4 任何	X1 Subnet	任何	任何	0.0.0.0	X1	20	9
7	IPv4 任何	X2 Subnet	任何	任何	0.0.0.0	X2	20	10
8	IPv4 任何	X10 Subnet	任何	任何	0.0.0.0	X10	20	11
9	IPv4 任何	X2:V402 Subnet	任何	任何	0.0.0.0	X2:V402	20	12
10	IPv4 任何	192.168.142.0/24	任何	任何	172.16.16.60	X2:V402	110	13
11	IPv4 X1 IP	任何	任何	任何	X1 Default Gateway	X1	20	14
12	IPv4 任何	0.0.0.0/0	任何	任何	192.168.95.1	X1	20	15

- 2 单击设置。

路由策略 OSPFv2 RIP OSPFv3 RIPng **设置**

按路由类中的度量设置路由的优先级

路由模式： 高级路由

BGP： 禁用 BGP 状态

- 3 从路由模式中，选择高级路由。
- 4 从 BGP 中，选择已启用（使用 CLI 进行配置）。将显示确认消息。

警告! 是否确定启用 BGP ? 单击确定继续。

i 注：在通过管理界面启用 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 的方法的详细信息，请参阅《SonicOS 命令行接口指南》。

- 5 通过控制台界面登录 SonicOS CLI。
- 6 通过输入 `configure` 命令进入配置模式。
- 7 通过键入配置路由 `bgp` 命令来输入 BGP CLI。此提示显示：

```
ZebOS version 7.7.0 IPIRouter 7/2009  
ARS BGP>
```
- 8 现在，您在 BGP 非配置模式中。类型 `?` 以查看非配置命令的列表。
- 9 输入 `show running-config` 查看当前的 BGP 运行配置。
- 10 如需进入 BGP 配置模式，请输入 `configure terminal` 命令。输入 `?` 查看配置命令的列表。

11 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

BGP 路径选择过程属性表描述了用于配置 BGP 路径选择过程的属性。

BGP 路径选择过程属性

特性	说明
重	首选向邻居学习的路由有最高权重值。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。

如为对端组设置权重，则对等组中的所有成员都有相同的权重。该命令还可用于向特定的对端组成员分配不同的权重。

此示例显示权重配置：

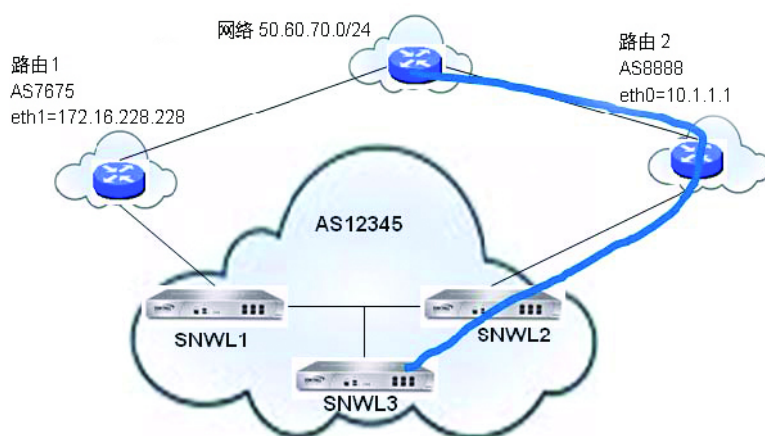
```
router bgp 12345
  neighbor 12.34.5.237 remote-as 12345
  neighbor 12.34.5.237 weight 60
```

```
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。**BGP 本地首选项拓扑结构**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。

BGP 本地首选项拓扑结构



SNWL1 和 SNWL2 配置表中显示的 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。

SNWL1 和 SNWL2 配置

SNWL1 配置

```
x0 = 12.34.5.228  
x1 = 172.16.228.45  
-----
```

```
router bgp 12345  
neighbor 172.16.228.228 remote-as 7675  
neighbor 12.34.5.237 remote-as 12345  
bgp default local-preference 150
```

SNWL2 配置

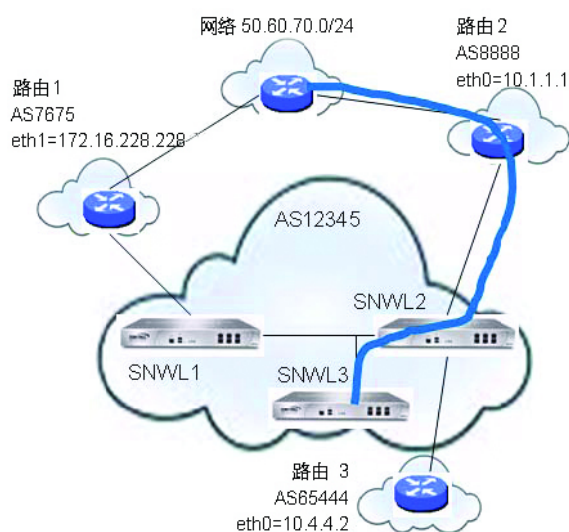
```
x0 = 12.34.5.237  
x1 = 10.1.1.2  
-----
```

```
router bgp 12345  
neighbor 10.1.1.1 remote-as 8888  
neighbor 12.34.5.228 remote-as 12345  
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，而非出站流量。[使用路由映射的 BGP 本地首选项拓扑结构](#)显示使用路由映射配置本地首选项的拓扑结构示例。

使用路由映射的 BGP 本地首选项拓扑结构



具有路由映射的 SNWL1 和 SNWL2 配置表中显示的 BGP 配置在 SNWL1 和 SNWL2 中输入。

具有路由映射的 SNWL1 和 SNWL2 配置

SNWL1 配置

```
x1 = 172.16.228.45
```

```
-----
```

```
router bgp 12345
```

```
neighbor 172.16.228.228 remote-as 7675
```

```
neighbor 12.34.5.237 remote-as 12345
```

```
bgp default local-preference 150
```

SNWL2 配置

```
x0 = 12.34.5.237
```

```
x1 = 10.1.1.2
```

```
x4 = 10.4.4.1
```

```
-----
```

```
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 20:** 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。

出站和入站路径配置

出站路径配置	入站路径配置
<pre>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</pre>	<pre>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</pre>

本配置将使路由安装到邻近的 10.50.165.233，AS_Path Prepend 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，请考虑使用第 806 页的 **bgp always-compare-med** 命令和第 806 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端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。

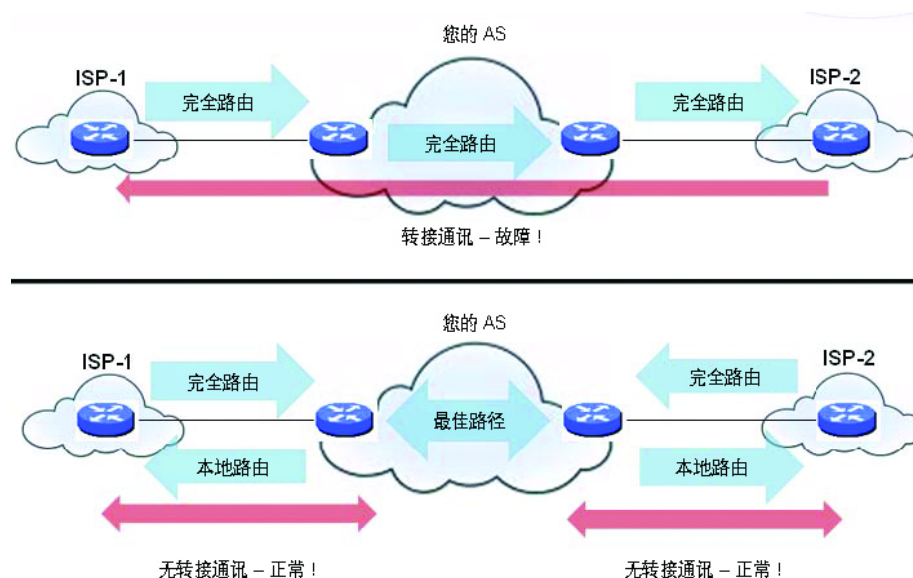
自动总结设置控制是否按类别发布路由。自动总结是发生 BGP 配置问题的另一个常见原因。

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）。请参阅[中转对等项与非中转对等项](#)。中转对等项显著扩大了路由表。通常，您不希望将 SonicWall 安全设备配置为中转对等项。

中转对等项与非中转对等项



为了防止您的安全设备意外成为中转对等项，请配置入站和出站过滤器：

- 第 808 页的出站过滤器
- 第 808 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。

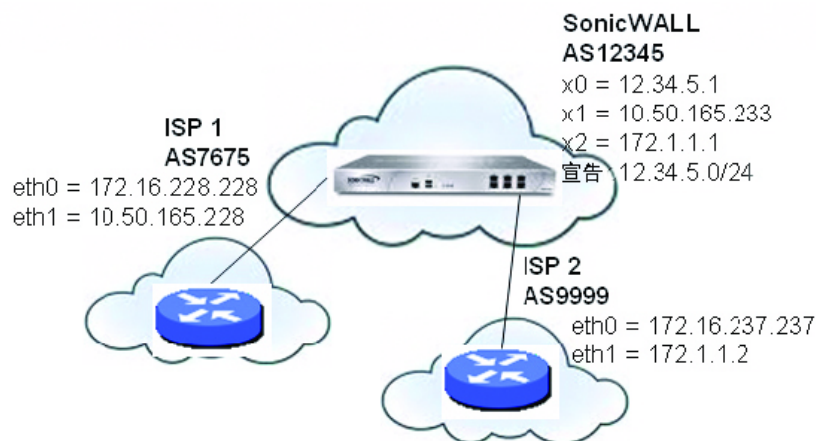
```
ip prefix-list unwantedPrefixes seq 5 deny 12.34.5.0/24 le 32
ip prefix-list unwantedPrefixes seq 10 deny 23.45.6.0/24 le 32
ip prefix-list unwantedPrefixes seq 20 deny 10.0.0.0/8 le 32
ip prefix-list unwantedPrefixes seq 21 deny 172.16.0.0/12 le 32
ip prefix-list unwantedPrefixes seq 22 deny 192.168.0.0/16 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

用于负载分担拓扑结构的多宿主 BGP 中显示的拓扑是 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。

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：

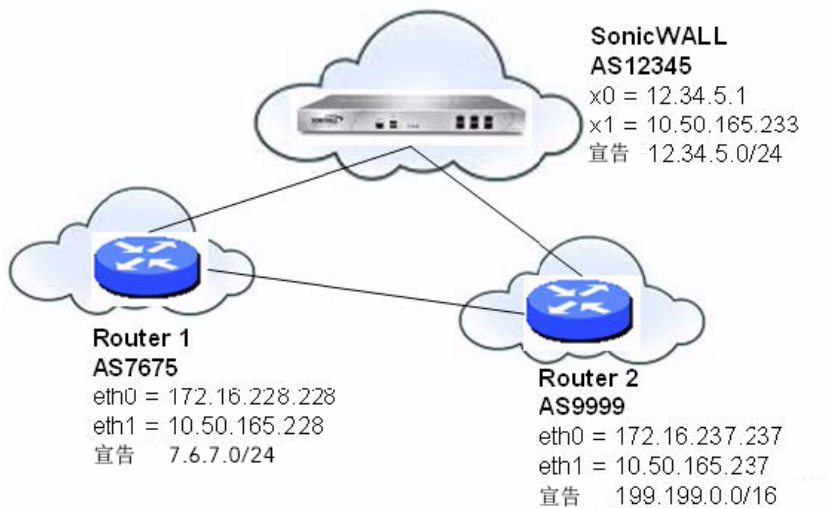
- 第 810 页的[查看 BGP 路由](#)

- 第 811 页的[配置 BGP 调试和日志](#)

查看 BGP 路由

BGP 拓扑结构显示基本 BGP 拓扑结构，其中 SonicWall 安全设备配置为可使 BGP 连接到两个不同 AS 上的两个路由器。

BGP 拓扑结构



可以在 SonicOS 管理界面中或通过使用 CLI 查看此网络的 FIB 中的路由。

主题：

- 第 810 页的[在管理界面中查看 FIB 路由](#)
- 第 810 页的[在 CLI 中查看 FIB 路由](#)
- 第 811 页的[查看 CLI 中的 RIB 路由](#)

在管理界面中查看 FIB 路由

可以单击 **BGP 状态**，以通过[管理 | 系统设置 | 网络 | 路由](#) > 设置在 SonicOS 管理界面上查看 BGP 配置摘要。**BGP 状态**对话框显示 `show ip bgp summary` 和 `show ip bgp neighbor` 命令的输出。

FIB 中的 BGP 路由也可以通过 CLI 进行查看，如第 810 页的[在 CLI 中查看 FIB 路由](#)中所述。

在 CLI 中查看 FIB 路由

在 CLI 中查看 FIB 路由的步骤如下：

```
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      199.199.0/16 [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

在 CLI 中查看 RIB 路由的步骤如下：

```

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 调试和日志

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 中使用 `调试 bgp` 命令加上 **BGP 调试关键字** 表中显示的关键字之一来配置 BGP 日志记录。

BGP 调试关键字

BGP 调试关键字	启用
全部	所有 BGP 调试。
衰减	对 BGP 衰减的调试。
事件	对 BGP 事件的调试。
过滤器	对 BGP 过滤器的调试。
fsm	对 BGP 有限状态机 (FSM) 的调试。
保持活动	对 BGP 保持活动的调试。
nht	对 NHT 消息的调试。
nsm	对 NSM 消息的调试。
更新	对入站/出站 BGP 更新的调试。

如需禁用 BGP 调试，请输入“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 上从 [管理 | 调查 | 日志 | 事件日志](#) 进行查看。BGP 消息作为日志消息中 [高级路由](#) 类别的一部分显示。如需日志和日志记录的更多信息，请参阅 [SonicOS 日志和报告](#)。

如需允许未直接连接的 BGP 对端项，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 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 [管理 | 系统设置 | 网络 | 路由](#) 上启用，但必须在 SonicOS 命令行接口 (CLI) 上进行配置。

以下限制适用于：

- 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：

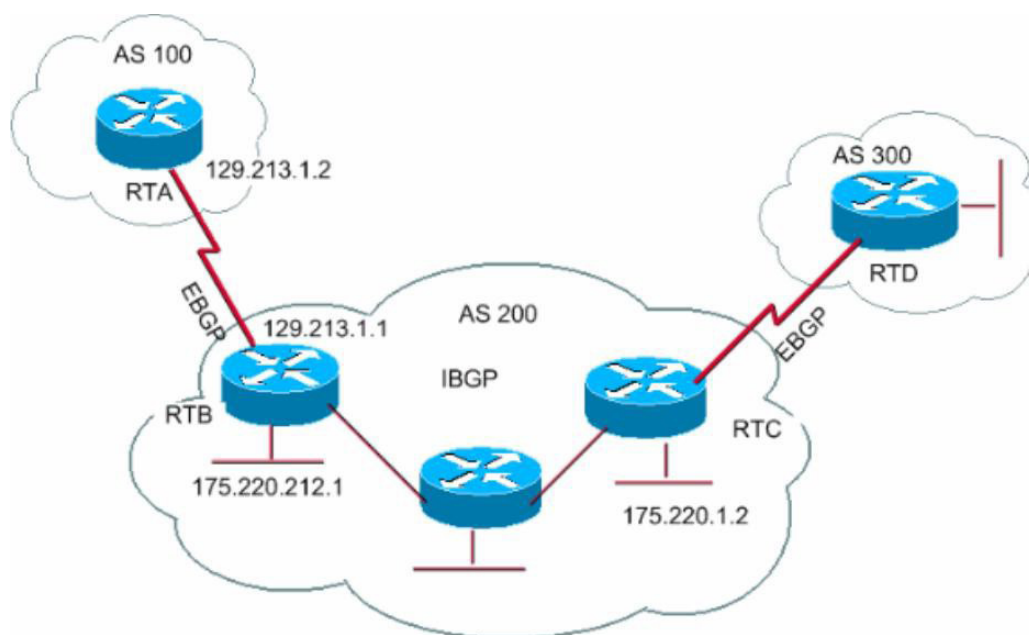
- [第 812 页的配置多个自治系统](#)
- [第 814 页的配置基本 BGP over IPv6](#)
- [第 814 页的配置 EBGMP Multihop](#)
- [第 815 页的配置 IPv6 BGP 出站路由过滤器](#)
- [第 816 页的配置 IPv6 BGP 分布列表](#)
- [第 817 页的 IPv6 BGP 路由映射](#)
- [第 818 页的配置 AS 正则表达式](#)
- [第 820 页的 EBGMP 路由选择](#)
- [第 822 页的 IPv6 BGP 同步](#)
- [第 824 页的 BGP 路由反射](#)
- [第 826 页的 IPv6 BGP 本地首选](#)
- [第 830 页的 BGP 对端组更新策略](#)
- [第 832 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 (iBGP)。

在 [包含多种 BGP 路由器配置的自治系统](#) 中，AS 200 是 AS 100 和 AS 300 的转换 AS。

包含多种 BGP 路由器配置的自治系统



如需按包含多种 BGP 路由器配置的自治系统所示配置多个 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:

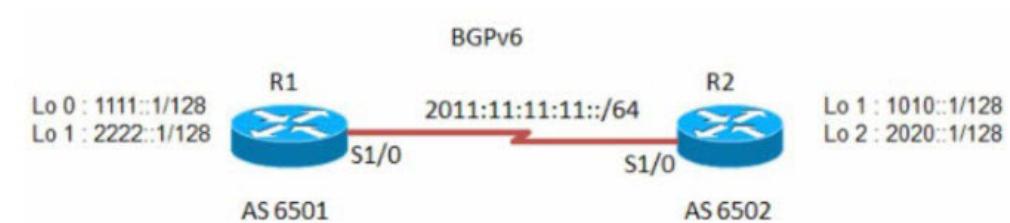
```
router bgp 200
  neighbor 175.220.212.1 remote-as 200

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 对端路由器以通过 IPv6 地址族或 IPv4 地址族传输 IPv4 或 IPv6 路由信息。请参阅[基本 BGP over IPv6 配置表](#)。

基本 BGP over IPv6 配置



配置基本 BGP over IPv6 的步骤如下：

- 1 配置路由器 R1 和 R2：

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端机之间建立相邻连接。Multihop 仅可用于 eBGP，不适用于 iBGP。如果安全设备拥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。

配置 EBGP Multihop 的步骤如下：

- 1 配置路由器 R1 和 R2：

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) 可用于通过过滤除来源处的多余路由更新来最大限度减少在对端路由器之间发送的 BGP 更新数。

配置 IPv6 BGP 出站路由过滤器 (ORF) 的步骤如下:

- 1 配置路由器 R1 和 R2:

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
```

如需检查 R1 和 R2 上的路由，请使用 **show bgp ipv6 unicast** 命令。

R1 上的路由应有 IPv6 地址 1010::1/128。

R2 上的路由应有 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过滤除来源处的多余路由更新来最大限度减少在对端路由器之间发送的 BGP 更新数。

配置 IPv6 BGP 分布列表的步骤如下：

- 1 配置路由器 R1 和 R2:

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
```

如需检查 R1 和 R2 上的路由，请使用 **show bgp ipv6 unicast** 命令。

R1 上的路由应有 IPv6 地址 1010::1/128。

R2 上的路由应有 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端路由器之间发送的 BGP 更新数。

配置 IPv6 BGP 路由映射的步骤如下:

- 1 配置路由器 R1 和 R2:

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
```

如需检查 R1 和 R2 上的路由, 请使用 **show bgp ipv6 unicast** 命令。

在 R1:

```
R1> show bgp ipv6 unicast
```

R1 上的路由应有 IPv6 地址 1010::1/128。

在 R2:

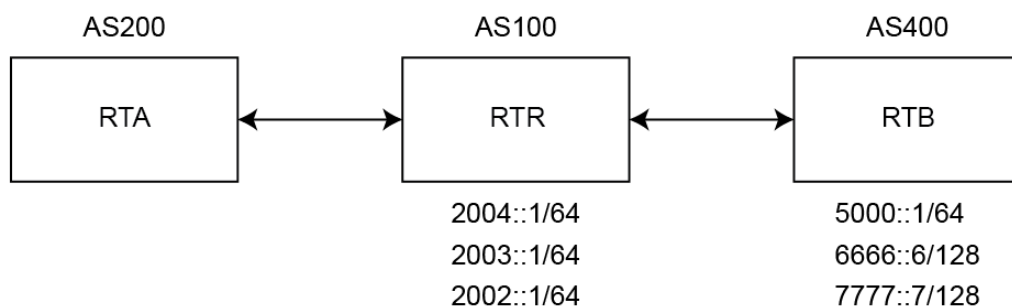
```
R2> show bgp ipv6 unicast
```

R2 上的路由应有 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。请参阅[自治系统正则表达式配置表](#)。

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

如需检查路由器 RTA 上的路由:

- 1 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
```

如需配置 RTA 上的 AS 正则表达式并拒绝来源于 AS100 的所有路由，请执行以下步骤：

```
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 .*
```

如需检查路由器 RTA 上的路由：

- 1 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
```

修改 AS 路径以拒绝学习自 AS100 的所有路由的步骤如下：

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 .*
```

如需检查路由器 RTA 上的路由：

- 1 请使用 `show bgp ipv6 unicast` 命令。

在 RTA：

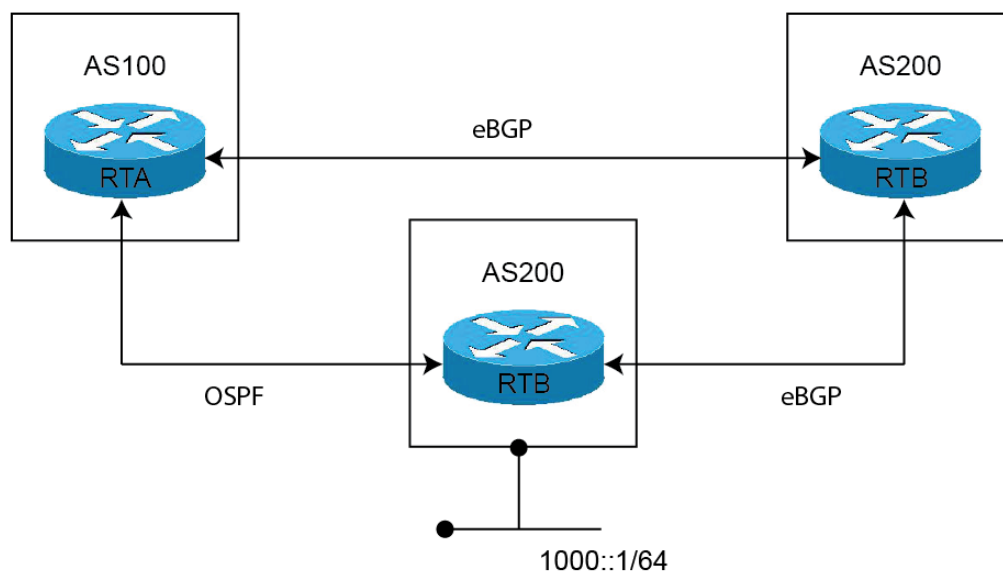
```
RTA> show bgp ipv6 unicast
```

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有更高的优先级。EBGP 的管理距离为 20。OSPF 的管理距离为 110。

自治系统 **EBGP 路由选择配置** 表显示 BGP 路由器使用的三个 AS 和路由协议。

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
```

如需检查路由器 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** 命令将 BGP 路由设置为首选路由。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
```

如需检查路由器 RTA 上的路由：

- 1 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
```

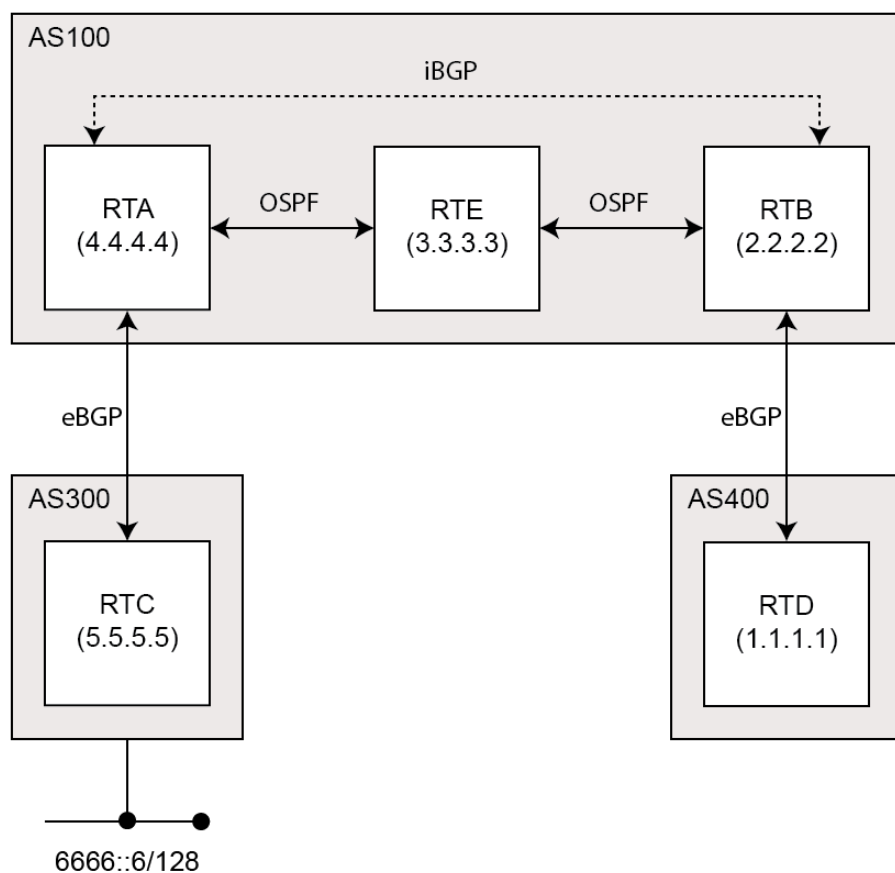
IPv6 BGP 同步

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。在这种情况下，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。

IPv6 BGP 同步示例



注：您可以通过向 RTB 上的 6666::6/128 添加静态路由并确保其他路由可以达到 6666::6/128 使 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，因此系统将在 RTE 处丢弃所有数据包。

在 AS100 中配置 RTB 上的 BGP 同步的步骤如下：

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。

在 AS100 中禁用 RTB 上的 BGP 同步的步骤如下：

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
```

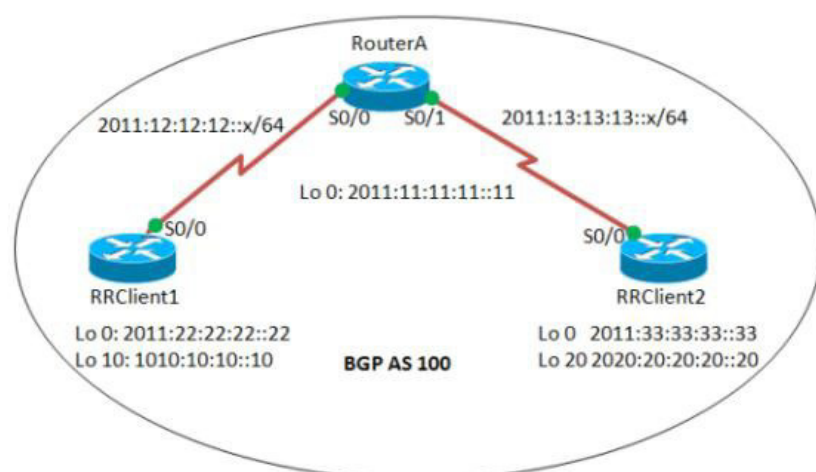
BGP 路由反射

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端路由器。

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。路由反射器充当服务器，而非 AS 中的每个其他路由器的对端路由器。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。

BGP 路由反射配置



在 AS 中配置路由反射的步骤如下：

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
```

如需检查路由:

- 1 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:

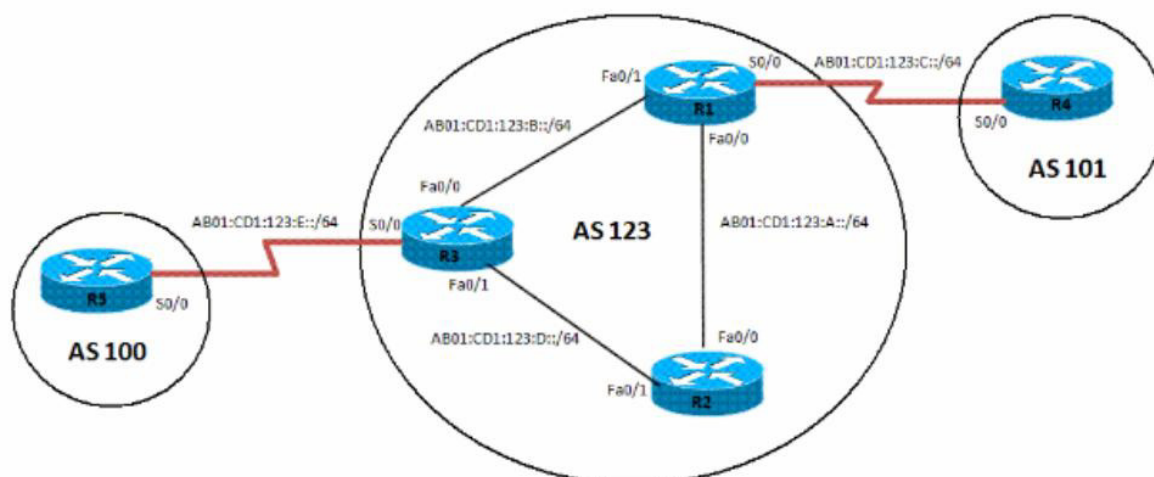
```
RRClient2> show bgp ipv6 unicast
```

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。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** 命令进行更改。

IPv6 BGP 本地首选配置



配置 AS 中首选路由的本地首选的步骤如下：

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
```

如需验证路由：

- 1 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 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 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。

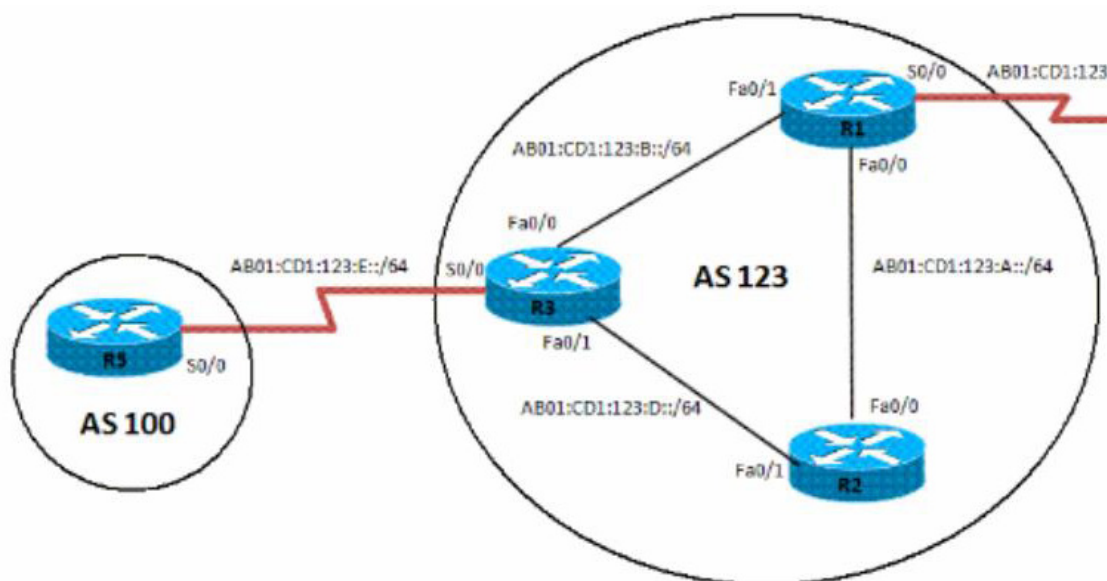
BGP 对端组更新策略

BGP 对端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。

在您定义对端组和向其添加邻居时，分配到该对端组的所有更新策略均应用于对端组的所有邻居。您无需定义各邻居的策略。

对端组的成员继承该对端组的所有配置设置。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。

BGP 对等组更新策略配置



配置 IPv6 BGP 对端组及其更新策略的步骤如下：

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
```

如需验证是否已配置正确的本地首选路由：

- 1 请使用 **show bgp ipv6 unicast** 命令：

在 R3：

```
R3> show bgp ipv6 unicast
```

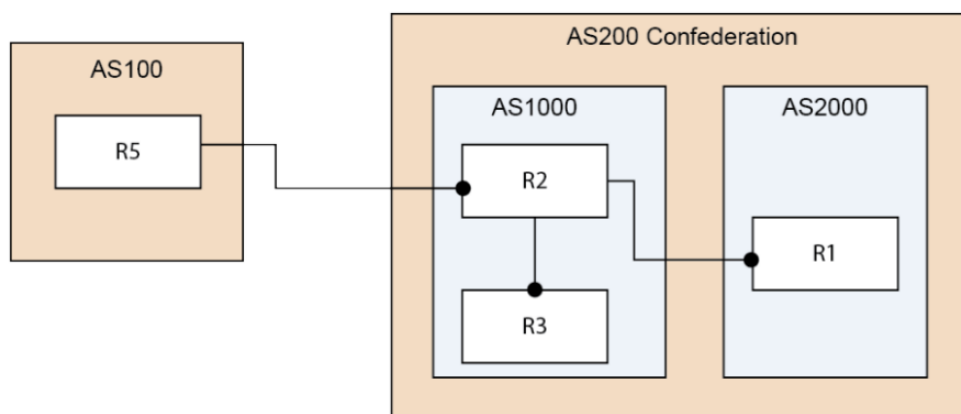
验证 IPv6 地址 BC01:BC1:10:A::/64 从 AS100 传递至 R1 和 R2，且将度量和本地首选设为相应的路由映射设置。

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 向外部对端系统发布路由。

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 对端系统像使用 iBGP 一样交换路由信息。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。

BGP 联盟配置



配置 BGP 联盟的步骤如下：

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

① | **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。

① | **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。

SonicWall 支持

购买了拥有有效维护合同的 SonicWall 产品的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。如需访问支持门户，请访问 <https://www.sonicwall.com/zh-cn/support/>。

支持门户使您能：


- 查看知识库文章和技术文档
- 下载软件
- 查看视频教程
- 与用户论坛中的同行和专家合作
- 获得许可帮助
- 访问 MySonicWall
- 了解 SonicWall 的专业服务
- 注册培训和认证


如需联系 SonicWall 支持，请参阅 <https://www.sonicwall.com/zh-cn/support/contact-support>。


如需查看 SonicWall 最终用户产品协议 (EUPA)，请参阅 <https://www.sonicwall.com/zh-cn/legal/eupa.aspx>。可根据地理位置选择语言，以查看适用于所在地区的 EUPA。

关于本文档

图例

 **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。

 **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。

 **重要、注意、提示、手机或视频：**信息图标表示支持的信息。

SonicOS 管理
更新日期 - 2017 年 12 月
软件版本 - 6.5
232-004123-00 修订版 A

版权所有 © 2017 SonicWall Inc. 保留所有权利。

SonicWall 是 SonicWall Inc. 和/或其附属公司在美国和/或其他国家/地区的商标或注册商标。所有其他商标和注册商标均为其各自所有者的财产。

本文档中的信息与 SonicWall Inc. 和/或其附属公司的产品一起提供。本文档或者通过销售 SonicWall 产品不以禁止反言或其他方式授予任何知识产权的许可，无论是明示的还是暗示的。除了本产品的许可协议中规定的条款与条件，SonicWall 和/或其附属公司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 SonicWall 和/或其附属公司发生此类损害的可能性，SonicWall 和/或其附属公司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。SonicWall 和/或其附属公司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。SonicWall Inc. 和/或其附属公司不作任何承诺更新本文档中包含的信息。

如需获取更多信息，请访问 <https://www.sonicwall.com/zh-cn/legal>。

最终用户产品协议

如需查看 SonicWall 最终用户产品协议，请访问：<https://www.sonicwall.com/zh-cn/legal/license-agreements>。可根据地理位置选择语言，以查看适用于所在地区的 EUPA。

开源代码

SonicWall 能在适用于每项许可证要求的情况下提供一张具有限制性许可证（例如，GPL、LGPL、AGPL）的开源代码的机读光盘。如需获得完整版机读光盘，请将您的书面申请，附带保付支票或汇票（金额 25 美元，收款人为 "SonicWall Inc."）邮寄至以下地址：

通用公共许可证源代码请求
SonicWall Inc. Attn: Jennifer Anderson
5455 Great America Parkway
Santa Clara, CA 95054