# 《PAN-OS® 管理员指南》

***Version 10.0 (EoL)***

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

## Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

## About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

## Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

December 10, 2020

# Table of Contents


入门指南 ..... 19
将防火墙集成到管理网络 ..... 20
确定管理策略 ..... 20
执行初始配置 ..... 20
设置外部服务的网络访问权 ..... 25
注册防火墙 ..... 30
创建新支持账户，并注册防火墙 ..... 30
注册防火墙 ..... 32
（可选）执行第 1 天配置 ..... 34
使用接口和区域对网络进行分段 ..... 37
减小攻击面的网络分段 ..... 37
配置接口和区域 ..... 37
设置基本安全策略 ..... 41
访问网络流量 ..... 44
启用免费 WildFire 转发 ..... 45
完成防火墙部署的最佳实践 ..... 47
确保管理员访问安全的最佳实践 ..... 48
隔离管理网络 ..... 48
使用服务路由访问外部服务 ..... 48
限制访问管理接口 ..... 49
管理管理员访问权限 ..... 50
创建强大的管理员密码 ..... 51
扫描所有发往管理接口的流量 ..... 51
入站流量管理之证书替换 ..... 53
使内容和软件更新保持最新 ..... 53

订阅 ..... 55
您可配合防火墙使用的订阅 ..... 56
激活订阅许可证 ..... 58
许可证到期后会发生什么？ ..... 59
增强 Palo Alto Networks 云服务的应用日志 ..... 61

软件和内容更新 ..... 63
PAN-OS 软件更新 ..... 64
动态内容更新 ..... 65
安装内容更新 ..... 67
应用程序和威胁内容更新 ..... 70
部署应用程序和威胁内容更新 ..... 70
内容更新提示 ..... 71
应用程序和威胁内容更新的最佳实践 ..... 73
内容更新的最佳实践——任务关键型 ..... 73
内容更新的最佳实践 ——安全第一 ..... 76
内容交付网络基础架构 ..... 79

防火墙管理 ..... 81
管理接口 ..... 82
使用 Web 界面 ..... 83

启动 Web 界面 ..... 83
配置横幅、当日消息及徽标 ..... 83
使用管理员登录活动指标检测帐户不当使用 ..... 85
管理和监控管理任务 ..... 86
提交、验证和预览防火墙配置更改 ..... 87
导出配置表格数据 ..... 88
利用全局查找搜索防火墙或 Panorama 管理服务器 ..... 89
管理配置更改限制锁 ..... 91
管理配置备份 ..... 92
保存并导出防火墙配置 ..... 92
还原防火墙配置更改 ..... 93
管理防火墙管理员 ..... 95
管理角色类型 ..... 95
配置管理角色配置文件 ..... 96
管理身份验证 ..... 96
配置管理帐户和身份验证 ..... 97
参考资料：Web 界面管理员访问 ..... 103
Web 界面访问权限 ..... 103
Panorama Web 界面访问权限 ..... 146
参考资料：端口码使用 ..... 149
用于管理功能的端口 ..... 149
用于 HA 的端口 ..... 150
用于 Panorama 的端口 ..... 150
用于 GlobalProtect 的端口 ..... 151
用于 User-ID 的端口 ..... 152
将防火墙重置为出厂默认设置 ..... 154
自举防火墙 ..... 155
USB 闪存盘支持 ..... 155
init-cfg.txt 样本文件 ..... 156
为防火墙自举准备 USB 闪存盘 ..... 157
使用 USB 闪存盘自举防火墙 ..... 159

设备遥测 ..... 161
设备遥测概述 ..... 162
设备遥测收集和传输间隔 ..... 163
管理设备遥测 ..... 164
启用设备遥测 ..... 164
禁用设备遥测 ..... 164
管理设备遥测收集的数据 ..... 164
管理历史设备遥测 ..... 165
监视设备遥测 ..... 167
采样设备遥测收集的数据 ..... 168

身份验证 ..... 169
身份验证类型 ..... 170
外部身份验证服务 ..... 170
多重因素身份验证 ..... 170
SAML ..... 171
Kerberos ..... 172
TACACS+ ..... 172
RADIUS ..... 173
LDAP ..... 174

本地身份验证 174
计划您的身份验证部署 176
配置多重因素身份验证 177
在 RSA SecurID 和防火墙之间配置 MFA 180
在 Okta 和防火墙之间配置 MFA 186
在 Duo 和防火墙之间配置 MFA 194
配置 SAML 身份验证 203
配置 Kerberos 单一登入 207
配置 Kerberos 服务器身份验证 208
配置 TACACS+ 身份验证 209
配置 RADIUS 身份验证 211
配置 LDAP 身份验证 214
身份验证服务器连接超时 216
设置身份验证服务器超时的原则 216
修改 PAN-OS Web 服务器超时 217
修改身份验证门户会话超时 217
配置本地数据库身份验证 218
配置身份验证配置文件和序列 219
测试身份验证服务器连接 222
身份验证策略 224
身份验证时间戳 224
配置身份验证策略 224
身份验证问题故障排除 227

证书管理 229
密钥和证书 230
默认可信证书颁发机构(CA) 232
证书撤消 233
证书吊销列表 (CRL) 233
在线证书状态协议 (OCSP) 233
证书部署 235
设置证书吊销状态验证 236
配置 OCSP 响应者 236
配置证书吊销状态验证 237
配置用于 SSL/TLS 解密的证书吊销状态验证 237
配置主密钥 239
主密钥加密 241
配置主密钥加密级别 241
防火墙 HA 对上主密钥加密 242
主密钥加密日志 243
AES-256-GCM 唯一主密钥加密 243
获取证书 244
创建自签名根 CA 证书 244
生成证书 245
导入证书和私钥 246
从外部 CA 获取证书 247
安装设备证书 248
使用 SCEP 部署证书 248
导出证书和私钥 251
配置证书配置文件 252
配置 SSL/TLS 服务配置文件 254
配置 SSH 服务配置文件 255
创建 SSH 管理配置文件 255

创建 SSH HA 配置文件 262
入站流量管理之证书替换 270
配置 SSL 转发代理服务器证书的密钥大小 271
吊销和续订证书 272
吊销证书 272
续订证书 272
安全密钥与硬件安全模块 273
建立与 HSM 的连接 273
使用 HSM 加密主密钥 278
在 HSM 上存储私钥 279
管理 HSM 部署 279

高可用性 281
HA 概述 282
HA 概念 283
HA 模式 283
HA 链路和备份链路 284
设备优先级和抢先 287
故障转移 288
主动/被动 HA 的 LACP 及 LLDP 预先协商 289
浮动 IP 地址和虚拟 MAC 地址 289
ARP 加载共享 290
基于路由的冗余 292
高可用性计时器 293
会话所有者 294
会话设置 295
处于主动/主动模式的 NAT 296
处于主动/主动 HA 模式的 ECMP 297
设置主动/被动 HA 298
主动/被动 HA 的先决条件 298
主动/被动 HA 的配置原则 298
配置主动/被动 HA 300
定义 HA 故障转移条件 304
验证故障转移 306
设置主动/主动 HA 307
主动/主动 HA 的先决条件 307
配置主动/主动 HA 307
确定主动/主动用例 312
HA 集群概述 325
HA 集群最佳实践和配置 327
配置 HA 集群 328
刷新 HA1 SSH 密钥和配置密钥选项 331
HA 防火墙状态 337
参考资料：高可用性同步 339
哪些设置不会在主动/被动 HA 中同步？ 339
哪些设置不会在主动/主动 HA 中同步？ 341
系统运行时信息同步 344

监控 347
使用仪表板 348
使用应用程序命令中心 349
ACC—第一印象 349

ACC 选项卡 ..... 351
ACC 小部件 ..... 352
小部件说明 ..... 353
ACC 筛选器 ..... 358
与 ACC 交互 ..... 359
用例：ACC — 信息发现路径 ..... 362
使用 App-Scope 报告 ..... 368
摘要报告 ..... 368
异动监控报告 ..... 369
威胁监控报告 ..... 370
威胁地图报告 ..... 370
网络监控报告 ..... 371
通信地图报告 ..... 372
使用自动关联引擎 ..... 374
自动关联引擎概念 ..... 374
查看关联项目 ..... 375
解释关联事件 ..... 375
使用 ACC 中的“受影响主机”小部件 ..... 377
执行数据包捕获 ..... 378
数据包捕获类型 ..... 378
禁用硬件卸载 ..... 378
执行自定义数据包捕获 ..... 379
执行威胁数据包捕获 ..... 383
执行应用程序数据包捕获 ..... 384
在管理接口上执行数据包捕获 ..... 387
监视应用程序和威胁 ..... 389
查看和管理日志 ..... 390
日志类型和严重性级别 ..... 390
查看日志 ..... 395
筛选日志 ..... 396
导出日志 ..... 397
配置日志存储配额和过期期限 ..... 397
计划将日志导出至 SCP 或 FTP 服务器 ..... 398
监控阻止列表 ..... 399
查看和管理报告 ..... 400
报告类型 ..... 400
查看报告 ..... 400
配置报告的过期期限和运行时间 ..... 401
禁用预定义的报告 ..... 402
自定义报告 ..... 402
生成定制报告 ..... 404
生成 Botnet 报告 ..... 406
生成 SaaS 应用程序使用情况报告 ..... 408
管理 PDF 摘要报告 ..... 410
生成用户/组活动报告 ..... 412
管理报告组 ..... 413
计划通过电子邮件传递的报告 ..... 414
管理报告存储容量 ..... 415
查看策略规则使用情况 ..... 416
使用外部服务进行监控 ..... 419
配置日志转发 ..... 420
配置电子邮件警报 ..... 423
使用 Syslog 进行监控 ..... 425
配置 Syslog 监控 ..... 425

Syslog 字段说明 427
SNMP 监控和陷阱 475
SNMP 支持 475
使用 SNMP 管理器浏览 MIB 和对象 476
为防火墙保护的网元启用 SNMP 服务 478
使用 SNMP 监控统计信息 479
将陷阱转发至 SNMP 管理器 480
支持的 MIB 481
将日志转发到 HTTP/S 目标 489
NetFlow 监控 492
配置 NetFlow 导出 492
NetFlow 模板 493
SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符 498
监视收发器 500

User-ID 501
User-ID 概述 502
User-ID 概念 503
组映射 503
用户映射 503
启用 User-ID 507
将用户映射到组 510
将 IP 地址映射到用户 515
为 User-ID 代理创建专用服务帐户 515
使用 Windows User-ID 代理配置用户映射 531
使用 PAN-OS 集成的 User-ID 代理来配置用户映射 540
使用 WinRM 配置服务器监控 543
配置 User-ID 以监控用户映射的 Syslog 发件人 549
使用身份验证门户将 IP 地址映射到用户名 556
为终端服务器用户配置用户映射 559
使用 XML API 将用户映射发送到 User-ID 567
启用基于用户和基于组的策略 568
为具有多个帐户的用户启用策略 569
验证用户标识配置 571
在大规模网络中部署 User-ID 573
为大量映射信息源部署 User-ID 573
在 HTTP 标头中插入用户名 576
重新分发数据和身份验证时间戳 578
共享跨虚拟系统的 User-ID 映射 582

App-ID 585
App-ID 概述 586
简化 App-ID 策略规则 587
使用标签创建应用程序筛选器 587
创建基于自定义标签的应用程序过滤器 587
应用程序 ID 和 HTTP/2 检查 589
管理自定义应用程序或未知应用程序 591
管理新建和修改过的 App-ID 592
最佳工作流程包含新的和修改过的 App-ID 592
请参阅内容发布中新建和修改过的 App-ID 593
请参阅新的和修改过的 App-ID 如何影响您的安全策略 594
确保允许新的关键 App-ID 594

监控新的 App-ID ..... 596
禁用或启用 App-ID ..... 596
在策略中使用应用程序对象 ..... 598
创建应用程序组 ..... 598
创建应用程序筛选器 ..... 598
创建定制应用程序 ..... 599
解析应用程序相关性 ..... 602
在默认端口上安全启用应用程序 ..... 604
应用程序与隐式支持 ..... 605
安全策略规则优化 ..... 609
策略优化器概念 ..... 610
从基于端口迁移至基于 App-ID 安全策略规则 ..... 615
规则克隆迁移用例：Web 浏览和 SSL 流量 ..... 620
添加应用程序至现有规则 ..... 622
通过未使用的应用程序识别安全策略规则 ..... 624
应用程序使用统计信息的高可用性 ..... 627
如何禁用策略优化器 ..... 627
应用层网关 ..... 628
禁用 SIP 应用层网关 (ALG) ..... 630
使用 HTTP 标头管理 SaaS 应用程序访问 ..... 631
了解 SaaS 自定义标头 ..... 631
预定义 SaaS 应用程序类型使用的域 ..... 633
使用预定义类型创建 HTTP 标头插入条目 ..... 633
创建自定义 HTTP 标头插入条目 ..... 634
保留数据中心应用程序的自定义超时 ..... 636

设备 ID ..... 639
Device-ID 概述 ..... 640
准备部署 Device-ID ..... 642
配置设备 ID ..... 644
管理设备 ID ..... 646
设备 ID 的 CLI 命令 ..... 648

威胁防护 ..... 649
防止网络免遭第 4 层和第 7 层逃避的最佳实践 ..... 650
设置防病毒威胁、防间谍软件和漏洞保护 ..... 660
DNS 安全 ..... 663
关于 DNS 安全 ..... 663
云 DNS 签名和保护 ..... 663
DNS 安全分析 ..... 664
启用 DNS 安全 ..... 665
使用 DNS 查询来确定网络上受感染的主机 ..... 671
DNS Sinkholing 的工作原理 ..... 671
配置 DNS Sinkholing ..... 672
为自定义域列表配置 DNS Sinkholing ..... 673
将 Sinkholing IP 地址配置为网络上的本地服务器 ..... 674
查看试图连接到恶意域的受感染主机 ..... 677
数据筛选 ..... 680
创建数据筛选配置文件 ..... 680
预定义的数据筛选模式 ..... 682
WildFire Inline ML ..... 684
配置 WildFire Inline ML ..... 684

设置文件阻止 ..... 687
防止暴力攻击 ..... 689
自定义暴力签名的操作和触发条件 ..... 690
启用规避签名 ..... 693
监控阻止 IP 列表 ..... 694
威胁签名类别 ..... 696
创建威胁异常 ..... 701
自定义签名 ..... 703
监控并获取威胁报告 ..... 704
监控活动并根据威胁类别创建自定义报告 ..... 704
进一步了解威胁签名 ..... 705
AutoFocus 网络流量威胁情报 ..... 707
与 Palo Alto Networks 共享威胁情报 ..... 713
威胁阻止资源 ..... 714

解密 ..... 715
解密概述 ..... 716
解密概念 ..... 717
适用于解密策略的密钥和证书 ..... 717
SSL 转发代理 ..... 718
SSL 转发代理解密配置文件 ..... 719
SSL 入站检查 ..... 722
SSL 入站检查解密配置文件 ..... 722
SSL 协议设置解密配置文件 ..... 723
SSH 代理 ..... 725
SSH 代理解密配置文件 ..... 726
不解密配置文件 ..... 727
用于椭圆曲线加密法 (ECC) 证书的 SSL 解密 ..... 728
用于 SSL 解密的完全正向保密 (PFS) ..... 728
SSL 解密和主题备用名称(SAN) ..... 729
TLSv1.3 解密 ..... 730
解密会话的高可用性支持 ..... 732
正在解密镜像 ..... 733
准备部署解密 ..... 734
与利益相关者联合制定解密部署策略 ..... 734
制定 PKI 推出计划 ..... 735
调整防火墙解密部署规模 ..... 736
规划分阶段的优先部署 ..... 737
确定解密流量 ..... 739
创建解密配置文件 ..... 739
创建解密策略规则 ..... 741
配置 SSL 转发代理 ..... 744
配置 SSL 入站检查 ..... 748
配置 SSH 代理 ..... 750
为未加密流量配置服务器证书验证 ..... 751
解密排除 ..... 752
Palo Alto Networks 预定义解密排除 ..... 752
出于技术原因从解密中排除服务器 ..... 753
本地解密排除缓存 ..... 754
创建基于策略的解密排除 ..... 756
阻止私钥导出 ..... 759
生成私钥并阻止它 ..... 759
导入和阻止私钥 ..... 760

导入和阻止 IKE 网关私钥 761
验证私钥阻止 763
让用户选择停用 SSL 解密 764
暂时禁用 SSL 解密 766
配置解密端口镜像 767
验证解密 769
排除故障并监视解密 772
解密应用程序命令中心小部件 773
解密日志 776
自定义解密报告模板 787
按代理类型和 TLS 版本划分的不受支持的参数 789
解密故障排除工作流程示例 789
解密代理 807
解密代理的工作方式 807
解密代理概念 808
第三层安全链指南 815
配置具有一个或多个第三层安全链的解密代理 815
透明桥接安全链指南 817
配置具有单一透明桥接安全链的解密代理 817
配置具有多个透明桥接安全链的解密代理 819
激活免费许可证以使用解密功能 820

URL 筛选 823
关于 URL 筛选 824
URL 筛选工作原理 825
URL 过滤 Inline ML 826
URL 筛选用例 827
URL 分类 829
以安全为中心的 URL 类别 829
恶意 URL 类别 830
经过验证的 URL 类别 831
可基于 URL 类别采取的策略操作 831
规划您的 URL 过滤部署 834
URL 筛选最佳实践 836
启用 PAN-DB 838
配置 URL 筛选 840
配置 URL 过滤 Inline ML 843
监控 Web 活动 846
监控网络用户的 Web 活动 846
查看用户活动报告 848
配置自定义 URL 筛选报告 849
仅记录用户访问页面 852
创建自定义 URL 类别 853
URL 类别异常 855
URL 类别异常列表的基本指南 855
URL 类别异常列表的通配符指南 855
URL 类别异常列表 — 通配符示例 856
使用 URL 筛选配置文件中的外部动态列表 857
允许密码访问某些站点 859
预防凭证网络钓鱼 861
检查公司凭据提交的方法 861
使用 Windows User-ID 代理配置凭据检测 862
设置凭据网络钓鱼防护 864

安全搜索执行 ..... 867
搜索提供商的安全搜索设置 ..... 867
阻止未启用严格安全搜索时的搜索结果 ..... 868
透明启用用户安全搜索 ..... 870
URL 筛选响应页面 ..... 875
自定义 URL 筛选响应页面 ..... 879
HTTP 标头日志记录 ..... 880
请求更改 URL 类别 ..... 881
在线提交更改请求 ..... 881
提交批量更改请求 ..... 882
从防火墙提交更改请求 ..... 883
对 URL 筛选进行故障排除 ..... 884
激活 PAN-DB 问题 ..... 884
PAN-DB 云连接问题 ..... 884
将 URL 分类为未解析 ..... 885
分类不正确 ..... 885
PAN-DB 私有云 ..... 888
用于 PAN-DB 私有云的 M-600 设备 ..... 888
设置 PAN-DB 私有云 ..... 889

服务质量 ..... 897
QoS 概述 ..... 898
QoS 概念 ..... 899
用于应用程序和用户的 QoS ..... 899
QoS 策略 ..... 899
QoS 配置文件 ..... 899
QoS 类 ..... 900
QoS 优先级队列 ..... 900
QoS 带宽管理 ..... 900
QoS 出口接口 ..... 901
针对明文与隧道通信的 QoS ..... 901
配置 QoS ..... 902
为虚拟系统配置 QoS ..... 907
基于 DSCP 分类实施 QoS ..... 912
QoS 用例 ..... 914
用例：单个用户的 QoS ..... 914
用例：语音和视频应用程序的 QoS ..... 916

VPN ..... 919
VPN 部署 ..... 920
站点到站点 VPN 概述 ..... 921
站点到站点 VPN 概念 ..... 922
IKE 网关 ..... 922
隧道接口 ..... 922
隧道监控 ..... 922
VPN 的 Internet 密钥交换 (IKE) ..... 923
IKEv2 ..... 925
设置站点到站点 VPN ..... 928
设置 IKE 网关 ..... 928
定义加密配置文件 ..... 933
建立 IPSec 隧道 ..... 935
设置隧道监控 ..... 937

启用/禁用，刷新或重新启动 IKE 网关或 IPSec 隧道 938
测试 VPN 连接 940
解释 VPN 错误消息 941
站点到站点 VPN 快速配置 942
使用静态路由的站点到站点 VPN 942
使用 OSPF 的站点与站点 VPN 945
使用静态和动态路由的站点到站点 VPN 948

大规模 VPN (LSVPN) 955
LSVPN 概述 956
为 LSVPN 创建接口和区域 957
在 GlobalProtect LSVPN 组件之间启用 SSL 959
关于证书部署 959
将服务器证书部署到 GlobalProtect LSVPN 组件 959
通过 SCEP 部署客户端证书到 GlobalProtect 卫星 961
配置门户以验证卫星 964
为 LSVPN 配置 GlobalProtect 网关 966
为 LSVPN 配置 GlobalProtect 门户 969
GlobalProtect 门户的 LSVPN 前提任务 969
配置门户 969
定义卫星配置 970
准备卫星加入 LSVPN 973
验证 LSVPN 配置 975
LSVPN 快速配置 976
基本 LSVPN 配置和静态路由 976
高级 LSVPN 配置和动态路由 978
使用 iBGP 进行高级 LSVPN 配置 980

Networking（网络） 985
配置接口 986
旁接接口 986
虚拟线路接口 987
第 2 层接口 993
第 3 层接口 998
配置聚合接口组 1007
用于网络分段的 Bonjour Reflector 1009
使用接口管理概要文件限制访问 1011
虚拟路由器 1013
服务路由 1015
静态路由 1016
静态路由概述 1016
基于路径监控删除静态路由 1016
配置静态路由 1019
为静态路由配置路径监控 1020
RIP 1023
OSPF 1025
OSPF 概念 1025
配置 OSPF 1026
配置 OSPFv3 1028
配置 OSPF 平稳重启 1031
确认 OSPF 运行 1031
BGP 1033

BGP 概述 1033
MP-BGP 1033
配置 BGP 1034
为 IPv4 或 IPv 6 单播配置带 MP-BGP 的 BGP 对等设备 1039
为 IPv4 多播配置带 MP-BGP 的 BGP 对等设备 1041
BGP 联合 1042
IP 多播 1047
IGMP 1047
PIM 1048
配置 IP 多播 1051
查看 IP 多播信息 1056
路由重新分发 1059
GRE 隧道 1061
GRE 隧道概述 1061
创建 GRE 隧道 1062
DHCP 1065
DHCP 概述 1065
防火墙作为 DHCP 服务器和客户端 1065
DHCP 消息 1066
DHCP 寻址 1067
DHCP 选项 1068
将接口配置为 DHCP 服务器 1070
将接口配置为 DHCP 客户端 1073
将管理接口配置为 DHCP 客户端 1074
将接口配置为 DHCP 中继代理 1075
对 DHCP 进行监控和故障排除 1076
DNS 1079
DNS 概述 1079
DNS 代理对象 1080
DNS 服务器配置文件 1080
多租户 DNS 部署 1081
配置 DNS 代理对象 1081
配置 DNS 服务器配置文件 1083
用例 1：防火墙要求执行 DNS 解析 1084
用例 2：ISP 租户使用 DNS 代理在其虚拟系统中对安全策略、报告和服务执行 DNS 解析。 1085
用例 3：防火墙充当客户端和服务器之间的 DNS 代理 1087
DNS 代理规则和 FQDN 匹配 1088
动态 DNS 概述 1092
为防火墙接口配置动态 DNS 1094
NAT 1096
NAT 策略规则 1096
源 NAT 和目标 NAT 1098
NAT 规则容量 1103
动态 IP 和端口 NAT 超额订阅 1103
数据面板 NAT 内存统计信息 1105
配置 NAT 1105
NAT 配置示例 1112
NPTv6 1119
NPTv6 概述 1119
NPTv6 的运作方式 1120
NDP 代理 1121
NPTv6 和 NDP 代理示例 1122
创建 NPTv6 策略 1123

NAT64 ..... 1126
NAT64 概况 ..... 1126
嵌入 IPv4 的 IPv6 地址 ..... 1126
DNS64 服务器 ..... 1127
路径 MTU 发现 ..... 1127
IPv6 启动的通信 ..... 1127
为 IPv6 启动的通信配置 NAT64 ..... 1129
为 IPv4 启动的通信配置 NAT64 ..... 1131
通过端口转换为 IPv4 启动的通信配置 NAT64 ..... 1132
ECMP ..... 1135
ECMP 负载均衡算法 ..... 1135
ECMP 型号、接口和 IP 路由支持 ..... 1136
在虚拟路由器上配置 ECMP ..... 1136
为多个 BGP 自治系统启用 ECMP ..... 1138
验证 ECMP ..... 1139
LLDP ..... 1140
LLDP 概述 ..... 1140
LLDP 内支持的 TLV ..... 1141
LLDP Syslog 消息和 SNMP 陷阱 ..... 1142
配置 LLDP ..... 1142
查看 LLDP 设置和状态 ..... 1143
清除 LLDP 统计信息 ..... 1144
BFD ..... 1145
BFD 概述 ..... 1145
配置 BFD ..... 1147
参考资料：URL 详细信息 ..... 1151
会话设置和超时 ..... 1155
传输层会话 ..... 1155
TCP ..... 1155
UDP ..... 1159
ICMP ..... 1159
控制特定 ICMP 或 ICMPv6 类型和代码 ..... 1160
配置会话超时 ..... 1161
配置会话设置 ..... 1162
会话分发策略 ..... 1165
阻止 TCP 分离握手会话建立 ..... 1167
隧道内容检测 ..... 1169
隧道内容检测概述 ..... 1169
配置隧道内容检测 ..... 1172
查看已检测的隧道活动 ..... 1176
查看日志中的隧道信息 ..... 1177
基于标记的隧道流量创建自定义报告 ..... 1178
禁用隧道加速 ..... 1178

策略 ..... 1179
策略类型 ..... 1180
安全策略 ..... 1181
安全策略的组件规则 ..... 1181
安全策略操作 ..... 1183
创建安全策略规则 ..... 1184
策略对象 ..... 1187
安全配置文件 ..... 1188
创建安全配置文件组 ..... 1192

设置或替代默认安全配置文件组 1193
跟踪规则库内规则 1195
规则号 1195
规则 UUID 1196
实施策略规则描述、标记和审核注释 1200
将策略规则或对象移动或克隆到不同的虚拟系统 1202
使用地址对象表示 IP 地址 1203
地址对象 1203
创建地址对象 1204
使用标记分组并以可视方式区分对象 1206
创建并应用标记 1206
修改标记 1207
按标记组查看规则 1207
在策略中使用外部动态列表 1210
外部动态列表 1210
格式化外部动态列表方针 1212
内置外部动态列表 1214
将防火墙配置为访问外部动态列表 1214
从 Web 服务器检索外部动态列表 1216
查看外部动态列表条目 1217
从外部动态列表中排除条目 1217
在外部动态列表上实施策略 1218
查找身份验证失败的外部动态列表 1220
禁用外部动态列表的身份验证 1221
动态注册 IP 地址和标记 1223
在策略中使用动态用户组 1224
使用自动标记实现安全操作自动化 1226
监控虚拟环境中的变化 1229
启用 VM 监控以跟踪虚拟网络上的更改 1229
云平台虚拟机上受监控的属性 1230
在策略中使用动态地址组 1234
动态 IP 地址和标记的 CLI 命令 1237
对上游设备背后的端点和用户实施策略 1239
在基于源用户的策略中使用 XFF 值 1239
在安全策略和日志记录中使用 XFF IP 地址值 1240
使用 XFF 标头中的 IP 地址来对事件进行故障排查 1242
基于策略的转发 1244
PBF 1244
创建基于策略的转发规则 1245
用例：采用双 ISP 的出站访问的 PBF 1247
测试策略规则 1255

虚拟系统 1257
虚拟系统概述 1258
虚拟系统组件和分段 1258
虚拟系统的优势 1259
虚拟系统的用例 1259
虚拟系统的平台支持和许可 1259
虚拟系统的管理角色 1260
虚拟系统的共享对象 1260
虚拟系统之间的通信 1261
必须离开防火墙的 VSYS 间流量 1261
留在防火墙的 VSYS 间流量 1261

VSYS 间的通信使用两个会话 1263
共享网关 1264
外部区域和共享网关 1264
共享网关的注意事项 1264
配置虚拟系统 1266
在防火墙中配置虚拟系统间通信 1271
配置共享网关 1272
自定义虚拟系统的服务路由 1273
将服务路由自定义为虚拟系统的服务 1273
将 PA-7000 系列防火墙配置为对每个虚拟系统进行记录 1274
配置每个虚拟系统或防火墙的管理员访问权限 1276
包含其他特征的虚拟系统功能 1278

区域保护和 DoS 保护 1279
使用区域进行网络分段 1280
区域如何保护网络？ 1281
区域防御 1282
区域防御工具 1282
区域防御工具如何运行？ 1283
适用于 Dos 保护的防火墙布置 1284
用于设置泛滥阈值的 CPS 基线测量 1284
区域保护配置文件 1285
数据包缓冲区保护 1288
DoS 保护配置文件和策略规则 1290
配置区域保护以提高网络安全性 1295
配置侦察保护 1295
配置基于数据包的攻击保护 1295
配置协议保护 1296
配置数据包缓冲区保护 1300
配置基于延迟的数据包缓冲区保护 1301
配置以太网 SGT 保护 1302
DoS 保护新会话不受泛滥攻击 1303
多会话 DoS 攻击 1303
单会话 DoS 攻击 1306
针对新会话的泛滥攻击配置 DoS 保护 1306
结束单会话 DoS 攻击 1308
识别在包缓冲区中占太多百分比的会话 1309
不提交丢弃会话 1311

认证 1313
启用 FIPS 和通用条件支持 1314
访问维护恢复工具 (MRT) 1314
将操作模式更改为 FIPS-CC 模式 1315
FIPS-CC 安全功能 1317
刷洗正在 FIPS-CC 模式下运行的防火墙或设备的交换内存 1318

# 入门指南

以下主题提供了帮助您部署新的 Palo Alto Networks 下一代防火墙的详细步骤。其提供了集成新防火墙到网络中以及如何设置基本安全策略的详细信息。关于继续部署安全平台功能以解决您网络安全需要的指南，请参见 完成防火墙部署的最佳实践。

- 将防火墙集成到管理网络
- 注册防火墙
- 使用接口和区域对网络进行分段
- 设置基本安全策略
- 访问网络流量
- 启用免费 WildFire 转发
- 完成防火墙部署的最佳实践
- 确保管理员访问安全的最佳实践

# 将防火墙集成到管理网络

所有 Palo Alto Networks 防火墙都提供一个可用于执行防火墙管理功能的带外管理端口 (MGT)。通过使用该 MGT 端口，可以将防火墙的管理功能与数据处理功能分开，从而保护对防火墙的访问权并提高性能。使用 Web 界面时，必须从 MGT 端口执行所有初始配置任务，即使您计划将来使用带内数据端口来管理防火墙。

某些管理任务（例如在防火墙上检索许可证及更新威胁和应用程序签名）需要访问 Internet。如果您不希望启用对 MGT 端口的外部访问权，则需要设置带内数据端口以访问所需的外部服务（使用服务路由），或者计划手动定期上传更新。



请勿从互联网管理接口或企业安全边界内其他不信任区域访问。无论是使用专用管理端口*(MGT)*，还是将数据端口配置为管理接口，这都适用。将您的防火墙集成到您的管理网络时，务必按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙和其他安全设备的管理访问权限。

以下主题介绍了如何执行将新防火墙集成到管理网络并在基本安全配置中进行部署所需的初始配置步骤。

- 确定管理策略
- 执行初始配置
- 设置外部服务的网络访问权



以下主题介绍了如何将单个 *Palo Alto Networks* 下一代防火墙集成到网络。但是为了实现冗余性，可考虑在高可用性配置中部署一对防火墙。

## 确定管理策略

Palo Alto Networks 防火墙可以在本地进行配置和管理，或者可以使用 Panorama 来集中管理，Panorama 是 Palo Alto Networks 的集中安全管理系统。如果您在网络中部署了六个或更多防火墙，使用 Panorama 可以获得以下优势：

- 降低管理配置、策略、软件和动态内容更新的复杂性和管理开销。使用 Panorama 上的设备组和模板，可以在一道防火墙上本地高效管理防火墙特定配置，并在所有防火墙或设备组之间实施共享的策略。
- 汇聚来自所有受管防火墙的数据，并了解网络上所有通信的信息。Panorama 上的应用程序命令中心 (ACC) 提供单个玻璃窗格来实现跨所有防火墙的统一报告，从而可以集中分析、调查和报告网络通信、安全事件和管理修改。

下述过程介绍如何使用本地 Web 界面管理防火墙。如果要使用 Panorama 进行集中管理，请先执行初始配置，并确认防火墙可以与 Panorama 建立连接。之后，您可以使用 Panorama 集中配置防火墙。

## 执行初始配置

默认情况下，防火墙的 IP 地址为 192.168.1.1，用户名/密码为 admin/admin。为了安全起见，在继续执行其他防火墙配置任务之前，必须更改这些设置。必须从 MGT 接口（即使计划不使用此接口进行防火墙管理），或使用直接连接到防火墙控制台端口的串行连接来执行这些初始配置任务。

STEP 1 | 安装防火墙，并连接电源。



如果防火墙型号具有双电源，则连接第二个电源以实现冗余。有关型号的详细信息，请参阅硬件参考指南。

STEP 2 | 从网络管理员处收集必要的信息。

- MGT 端口的 IP 地址
- 子网掩码



© 2019 Palo Alto Networks, Inc.

- 默认网关
- DNS 服务器地址

STEP 3 | 将您的计算机连接到防火墙。

可以使用以下方法之一连接到防火墙：

- 使用串行电缆将计算机连接到控制台端口，并使用终端模拟软件 (9600-8-N-1) 连接到防火墙。需要等待几分钟时间启动过程才能完成；当防火墙准备就绪时，提示信息将更改为防火墙的名称，例如 `PA-220 login`。
- 使用 RJ-45 Ethernet 电缆将计算机连接到防火墙的 MGT 端口。从浏览器中访问 **`https://192.168.1.1`**。

您可能需要将计算机上的 *IP* 地址更改为 *192.168.1.0/24* 网络中的地址（例如 *192.168.1.2*）才能访问此 *URL*。

STEP 4 | 收到提示时，登录到防火墙。

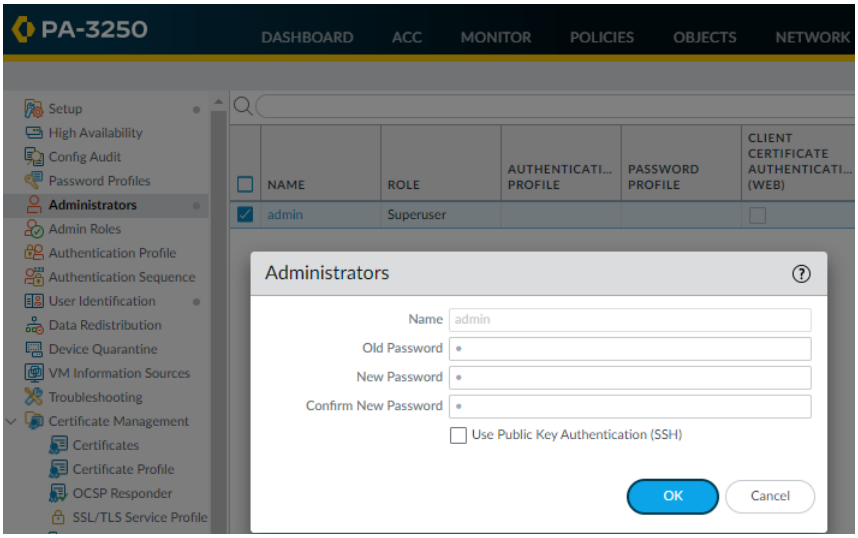
必须使用默认用户名和密码 (admin/admin) 登录。防火墙将开始初始化。

STEP 5 | 为管理员帐户设置安全密码。

从 *PAN-OS 9.0.4* 开始，在首次登录到设备时，必须更改预定义的默认管理员密码 *(admin/admin)*。新密码至少包含 *8* 个字符，其中至少 *1* 个小写字母和 *1* 个大写字母以及 *1* 个数字或特殊字符。

请务必使用密码强度最佳实践来确保密码强度，并查看密码复杂性设置。

1. 选择**Device**（设备）> **Administrators**（管理员）。
2. 选择 **admin** 角色。
3. 输入当前的默认密码和新密码。




4. 单击 **OK**（确定）以保存设置。

STEP 6 | 配置 MGT 接口。

1. 选择 **Device**（设备）> **Setup**（设置）> **Interfaces**（接口），然后编辑 **Management**（管理）接口。
2. 通过以下的其中一种方法配置 MGT 界面的地址设置：


© 2019 Palo Alto Networks, Inc.

- 要配置 MGT 界面的静态 IP 地址设置，将 **IP Type**（**IP** 类型）设置为 **Static**（静态），输入 **IP Address**（**IP** 地址）、**Netmask**（网络掩码）和 **Default Gateway**（默认网关）。
- 要动态配置 MGT 接口地址设置，将 **IP Type**（**IP** 类型）设置为 **DHCP Client**（**DHCP** 客户端）。要使用此方法，必须将管理接口配置为 DHCP 客户端。

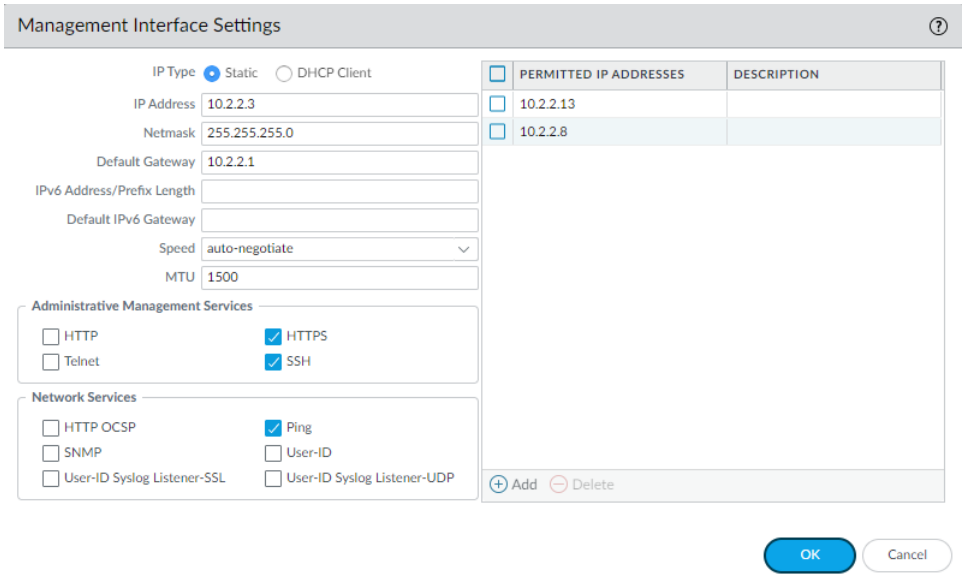


若要防止对管理接口进行未经授权的访问，最好 *Add*（添加）管理员可以从其中访问 *MGT* 接口的 *Permitted IP Addresses*（允许的 *IP* 地址）。

3. 将 **Speed**（速度）设置为 **auto-negotiate**（自动协商）。
4. 选择允许在该接口上执行哪些管理服务。



确保不选择 *Telnet* 和 *HTTP*，因为这些服务使用明文，不像其他服务一样安全，可能会泄露管理员凭据。




5. 单击 **OK**（确定）。

## STEP 7 | 配置 DNS、更新服务器和代理服务器设置。

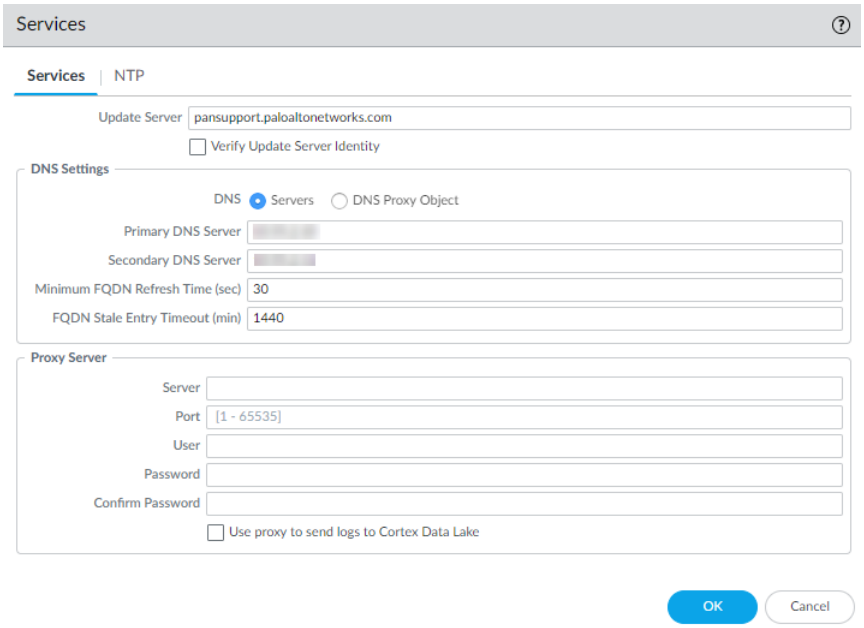


必须在防火墙上手动配置至少一个 *DNS* 服务器，否则无法解析主机名；它不会使用其他资源（如 *ISP*）上的 *DNS* 服务器设置。

1. 选择**Device**（设备）> **Setup**（设置）> **Services**（服务）。
   - 对于多虚拟系统平台，请选择 **Global**（全局）并编辑“服务”部分。
   - 对于单个虚拟系统平台，请编辑“服务”部分。
2. 在 **Services**（服务）选项卡上，请为 **DNS** 选择以下选项之一：
   - **Servers**（服务器）— 输入 **Primary DNS Server**（主 **DNS** 服务器）地址和 **Secondary DNS Server**（辅助 **DNS** 服务器）地址。
   - **DNS Proxy Object**（**DNS** 代理对象）— 从下拉列表中选择要用于配置全局 DNS 服务的 **DNS Proxy**（**DNS** 代理），或单击 **DNS Proxy**（**DNS** 代理）以配置新的 DNS 代理对象。



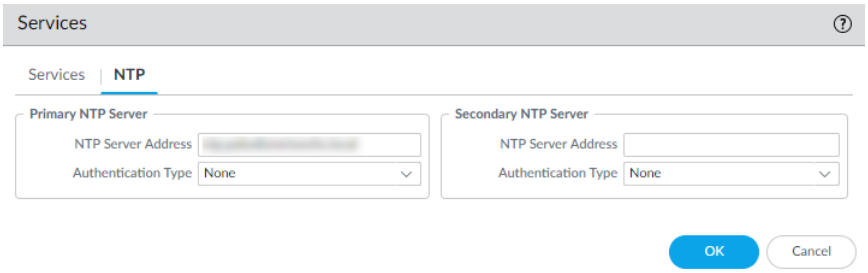
© 2019 Palo Alto Networks, Inc.




3. 单击 **OK**（确定）。

STEP 8 | 配置日期和时间 (NTP) 设置。

1. 选择**Device**（设备）> **Setup**（设置）> **Services**（服务）。
   - 对于多虚拟系统平台，请选择 **Global**（全局）并编辑“服务”部分。
   - 对于单个虚拟系统平台，请编辑“服务”部分。
2. 在 **NTP** 选项卡上，要使用互联网上的虚拟时间服务器群集，请输入主机名 `pool.ntp.org` 作为 **Primary NTP Server**（主 **NTP** 服务器）或输入您的主 NTP 服务器的 IP 地址。




3. （可选）输入 **Secondary NTP Server**（辅助 **NTP** 服务器）地址。
4. （可选）要对 NTP 服务器中的时间更新进行身份验证，对于 **Authentication Type**（身份验证类型），请为各个服务器选择以下选项之一：
   - **None**（无）— （默认）禁用 NTP 身份验证。
   - **Symmetric Key**（对称式密钥）— 防火墙使用对称式密钥交换（共享密钥）对时间更新进行身份验证。
     - **Key ID**（密钥 **ID**）— 输入密钥 ID (1-65534)。
     - **Algorithm**（算法）— 选择要用于 NTP 身份验证的算法（**MD5** 或 **SHA1**）。
   - **Autokey**（自动密钥）— 防火墙使用自动密钥（公钥加密）对时间更新进行身份验证。
5. 单击 **OK**（确定）。

STEP 9 | （可选）按需配置常规防火墙设置。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。


© 2019 Palo Alto Networks, Inc.

2. 输入防火墙的 **Hostname**（主机名）并输入您的网络 **Domain**（域）名。域名只是一个标签；不会使用它来加入域。
3. 输入 **Login Banner**（登录横幅），通知准备登录的用户他们需要通过验证才能访问防火墙管理功能。

   最佳实践是避免使用欢迎赘词。此外，您应当请法律部门审核横幅信息，以确保其起到了相应地禁止未授权访问的警示作用。
4. 输入 **Latitude**（纬度）和**Longitude**（经度）以支持在世界地图上准确放置防火墙。
5. 单击 **OK**（确定）。

STEP 10 | 提交更改。

保存配置更改时，您将失去与 *Web* 界面的连接，因为 *IP* 地址已经发生更改。

单击 Web 界面右上角的 **Commit**（提交）。防火墙最长可能需要 90 秒才能保存您的更改。

STEP 11 | 将防火墙连接到网络。

1. 断开防火墙与您的计算机的连接。
2. 使用 RJ-45 Ethernet 电缆将 MGT 端口连接到管理网络上的交换机端口。请确保将防火墙连接到的交换机端口已配置为自动协商。

STEP 12 | 打开对防火墙的 SSH 管理会话。

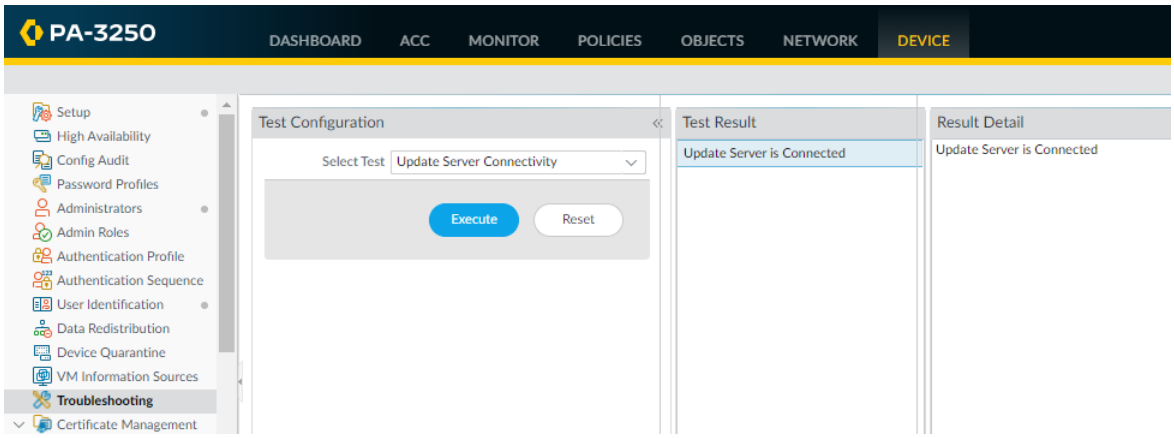
通过终端模拟软件（例如 PuTTY），使用您分配的新 IP 地址启动对防火墙的 SSH 会话。

STEP 13 | 验证防火墙管理所需外部服务（例如 Palo Alto Networks 更新服务器）的网络访问权限。

您可以使用以下方法之一连接到防火墙：

- 如果您不希望允许对 MGT 接口进行外部网络访问，则需要设置数据端口来检索所需的服务更新。继续设置外部服务的网络访问。
- 如果计划允许外部网络访问 MGT 接口，请验证是否已连接，然后继续执行注册防火墙和激活订阅许可证。

1. 使用更新服务器连接测试验证是否能联网到 Palo Alto Networks 更新服务器，如以下示例所示：
   1. 选择 **Device**（设备）> **Troubleshooting**（故障排除），然后从 Select Test（选择测试）下拉列表中选择 **Update Server Connectivity**（更新服务器连接）。
   2. **Execute**（执行）更新服务器连接测试。




2. 使用以下 CLI 命令从 Palo Alto Networks 更新服务器检索关于防火墙支持授权的信息：


© 2019 Palo Alto Networks, Inc.

```
request support
check
```

如果网络畅通，更新服务器响应防火墙的支持状态。如果防火墙尚未注册，则更新服务器将返回以下消息：

```
Contact Us

https://www.paloaltonetworks.com/company/contact-us.html

Support Home

https://www.paloaltonetworks.com/support/tabs/overview.html

Device not found on this update server
```

## 设置外部服务的网络访问权

默认情况下，防火墙使用 MGT 接口来访问远程服务，例如 DNS 服务器、内容更新和许可证检索。如果您不希望启用对 MGT 端口的外部网络访问，则必须设置带内数据端口以访问所需的外部服务或设置服务路由以指示防火墙应使用何种端口访问外部服务。

请勿从 *Internet* 或企业安全边界内其他不信任区域启用管理访问。要确保正确保护防火墙的安全，请遵循确保管理员访问安全的最佳实践。

此任务要求熟悉防火墙接口、区域和策略。有关这些主题的更多信息，请参阅配置接口和区域和设置基本安全策略。

STEP 1 | 确定要用于访问外部服务的接口并将其连接到交换机或路由器端口。

您使用的接口必须具有静态 IP 地址。

STEP 2 | 登录到 Web 界面。

在 Web 浏览器中使用安全连接 (https)，通过初始配置期间分配的新 IP 地址和密码登录 (https://<IP address>)。您将看到证书警告；这属于正常情况。继续浏览网页。

STEP 3 | （可选）防火墙在端口 Ethernet 1/1 和 Ethernet 1/2 之间预配置了一个默认虚拟线路接口（及相应的默认安全策略和区域）。如果不打算使用此虚拟线路配置，则必须手动删除此配置，以防止其干扰您定义的其他接口设置。

必须按照下列顺序删除此配置：

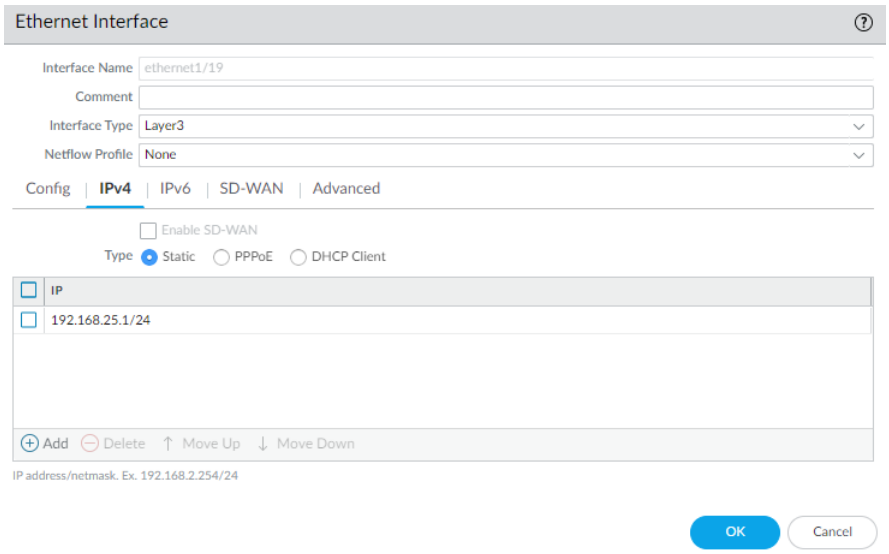
1. 要删除默认安全策略，请选择 **Policies**（策略）> **Security**（安全），选中规则，然后单击 **Delete**（删除）。
2. 要删除默认虚拟线路，请选择 **Network**（网络）> **Virtual Wires**（虚拟线路），选中虚拟线路，然后单击 **Delete**（删除）。
3. 要删除默认可信区域和不可信区域，请选择 **Network**（网络）> **Zones**（区域），选中每个区域，然后单击 **Delete**（删除）。
4. 要删除接口配置，请选择 **Network**（网络）> **Interfaces**（接口），选中每个接口（ethernet1/1 和 ethernet1/2），然后单击 **Delete**（删除）。
5. **Commit**（提交）更改。

STEP 4 | 配置您计划使用，以从外部访问管理服务的界面。



© 2019 Palo Alto Networks, Inc.

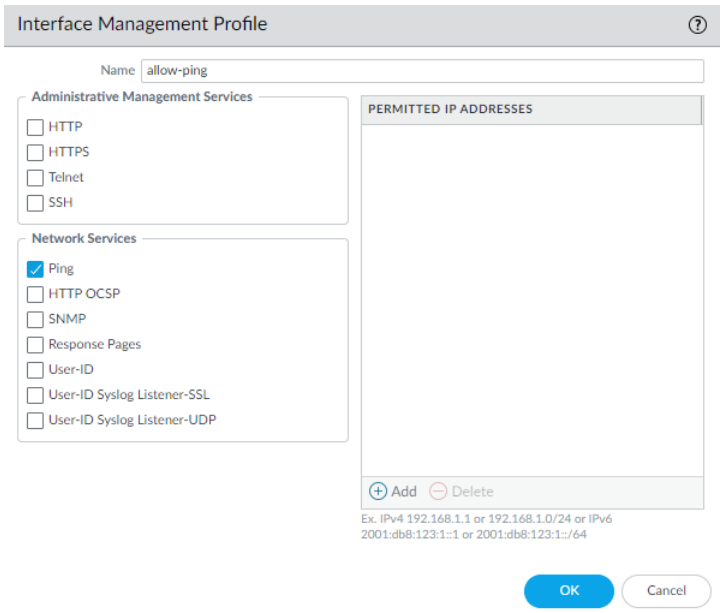
1. 请选择 **Network**（网络）> **Interfaces**（接口），然后选择步骤 1 中已使用电缆连接到相应接口的接口。
2. 选择 **Interface Type**（接口类型）。此示例显示了针对 **Layer3**（第 3 层）的步骤，但是您在此处的选择取决于网络拓扑。
3. 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。
4. 在 Zone（区域）对话框中，定义新区域的 **Name**（名称），例如“默认”，然后单击 **OK**（确定）。
5. 选择 **IPv4** 选项卡，选中 **Static**（静态）单选按钮，单击 IP 部分的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.1.254/24。您必须在该界面上使用静态 IP 地址。




6. 选择 **Advanced**（高级）> **Other Info**（其他信息），展开 **Management Profile**（管理配置文件）下拉列表，然后选择 **New Management Profile**（新建管理配置文件）。
7. 输入配置文件的 **Name**（名称），例如 allow_ping，然后选择希望允许在该接口上执行的服务。为了允许访问外部服务，您可能仅需要启用 **Ping**，然后单击 **OK**（确定）。

这些服务提供对防火墙的管理访问，因此请只选择希望在此接口上允许执行的管理活动对应的服务。例如，请勿启用 *HTTP* 或 *Telnet*，因为这些协议会以明文形式传输，不安全。或者，如果计划使用 *MGT* 接口通过 *Web* 界面或 *CLI* 执行防火墙配置任务，则不要启用 *HTTP*、*HTTPS*、*SSH* 或 *Telnet*，以便可以防止通过此接口进行未经授权的访问（如果您必须允许 *HTTPS* 或 *SSH*，在这种情况下，应当限制对特定 *Permitted IP Addresses*（允许的 *IP* 地址）组的访问）。有关详细信息，请参阅使用接口管理配置文件限制访问。


© 2019 Palo Alto Networks, Inc.



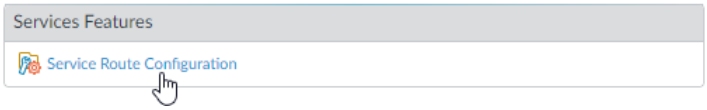

8. 要保存接口配置，请单击 **OK**（确定）。

## STEP 5 | 配置服务路由。

默认情况下，防火墙使用 MGT 界面访问其所需的外部服务。要更改防火墙用来发送请求至外部服务的界面，您必须编辑服务路由。

本例介绍如何设置全局服务理由。有关在虚拟系统基础而非全局基础上设置对外部服务的网络访问的信息，请参阅将服务路由自定义为虚拟系统的服务。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Global**（全局）并单击 **Service Route Configuration**（服务路由配置）。

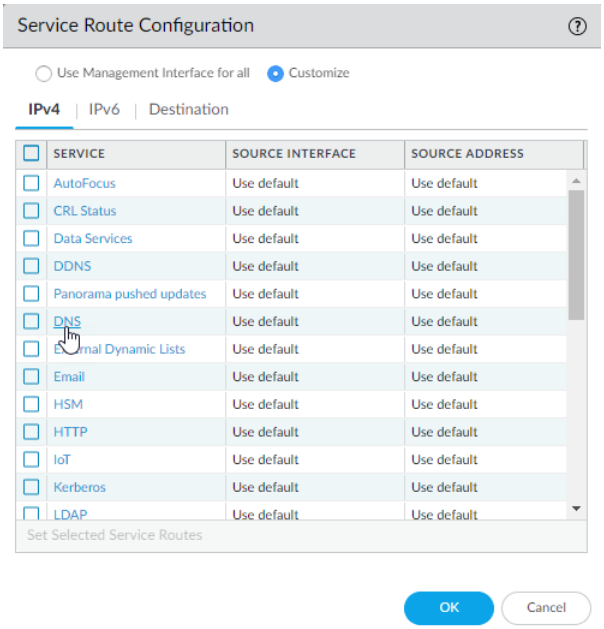



为了激活您的许可证并获取最新的内容和软件更新，您需要更改 *DNS*、*Palo Alto Networks Services*（*Palo Alto Networks* 服务）、*URL Updates*（*URL* 更新）和 *AutoFocus* 的服务路由。

2. 单击 **Customize**（自定义）单选按钮，然后选择下列其中一项：
   - 对于预定义服务，选择 **IPv4** 或 **IPv6**，并单击服务链接。要限制源地址的下拉列表，选择 **Source Interface**（源接口），然后选择刚刚配置的接口。然后（从该接口）选择一个源地址作为服务路由。

     如果为所选接口配置了不止一个 IP 地址，则可以从 **Source Address**（源地址）下拉列表中选择一个 IP 地址。
   - 要为自定义目标创建服务路由，请选择 **Destination**（目标），然后单击 **Add**（添加）。输入 **Destination**（目标）IP 地址。具有与此地址相匹配的目标地址的传入数据包将作为您为此服务路由指定的源地址的地址来源。要限制源地址的下拉列表，请选择 **Source Interface**（源接口）。如果为所选接口配置了不止一个 IP 地址，则可以从 **Source Address**（源地址）下拉列表中选择一个 IP 地址。


© 2019 Palo Alto Networks, Inc.




3. 单击 **OK**（确定）以保存设置。
4. 为要修改的每个服务路由重复执行步骤 5.2 - 5.3。
5. **Commit**（提交）更改。

STEP 6 | 配置面向外部的接口和关联区域，然后创建安全策略规则，从而允许防火墙将服务请求从内部区域发送到外部区域。

1. 选择 **Network**（网络）> **Interfaces**（接口），然后选择面向外部网络的接口。选择 **Layer3**（第 3 层）作为 **Interface Type**（接口类型），**Add**（添加）**IP** 地址（在 **IPv4** 或 **IPv6** 选项卡上），然后创建关联 **Security Zone**（安全区域）（在 **Config**（配置）选项卡上），例如 Internet。该界面必须具备静态 IP 地址，您无需在该界面上设置管理服务。
2. 要设置允许流量从内部网络流动到 Palo Alto Networks 更新服务器的安全规则，请选择 **Policies**（策略）> **Security**（安全），然后单击 **Add**（添加）。



创建安全策略规则的最佳实践是，使用基于应用程序而非基于端口的规则，以确保您不受当前使用端口、协议、规避策略或加密的限制正确识别底层应用程序，始终将 *Service*（服务）设置为 *application-default*（应用程序-默认）。在该情况下，创建准许访问更新服务器（及其他 *Palo Alto Networks* 服务）的安全策略规则。

| | NAME | Source ZONE | Destination ZONE | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|
| 1 | Palo Alto Networks Services | Management | Internet | paloalto-dns-security<br>paloalto-logging-service<br>paloalto-updates<br>paloalto-wildfire-cloud | application-... | Allow |

STEP 7 | 创建 NAT 策略规则。

1. 如果在面向内部的接口上使用的是私有 IP 地址，则需要创建源 NAT 规则以将该地址转换为可公开路由地址。选择 **Policies**（策略）> **NAT**，然后单击 **Add**（添加）。您必须至少为该规则定义一个名称（**General**（常规）选项卡），指定源和目标区域，此例中为管理到到互联网（**Original Packet**（原始数据包）选项卡），定义源地址转换设置（**Translated Packet**（转换后的数据包）选项卡），然后单击 **OK**（确定）。
2. **Commit**（提交）更改。



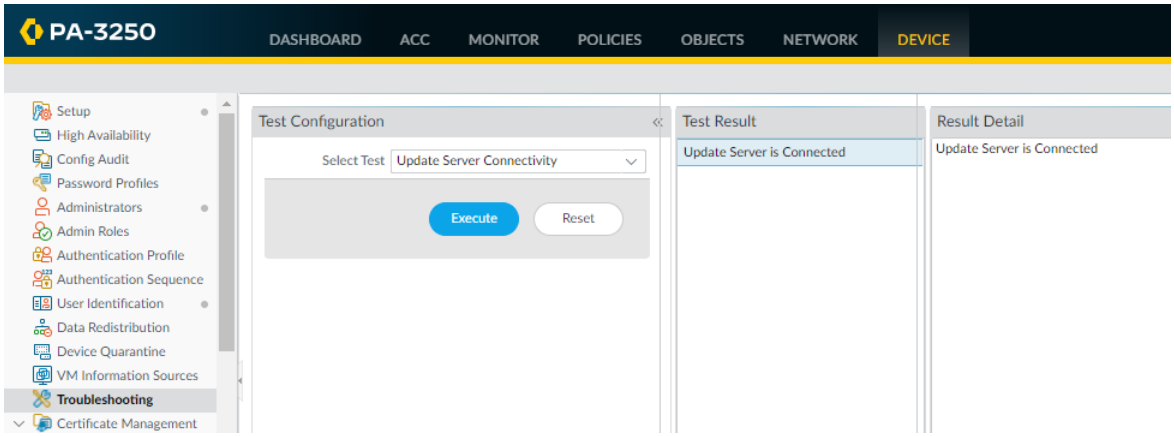
© 2019 Palo Alto Networks, Inc.

| | NAME | Original Packet | | | Translated Packet | |
|---|---|---|---|---|---|---|
| | | SOURCE ZONE | DESTINATION ZONE | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| 1 | Source NAT | Management | Internet | any | dynamic-ip-and-port | none |

STEP 8 | 选择 **Device**（设备）> **Troubleshooting**（故障排除），并验证您是否已从数据端口连接到外部服务，包括默认网关（使用 **Ping** 连接测试）以及 Palo Alto Networks 更新服务器（使用**Update Server Connectivity**（更新服务器连接）测试）。在此示例中，可对防火墙与 Palo Alto Networks 更新服务器之间的连接进行测试。

在确认您已经具备必要的网络连接后，继续执行注册防火墙和激活订阅许可证。

1. 从选择测试下拉列表中选择 **Update Server**（更新服务器）。
2. **Execute**（执行）Palo Alto Networks 更新服务器连接测试。




3. 访问防火墙 CLI，并使用以下 CLI 命令从 Palo Alto Networks 更新服务器检索关于防火墙支持授权的信息：

```
request support
check
```

如果网络畅通，更新服务器响应防火墙的支持状态。因为防火墙没有注册，所以更新服务器将返回以下消息：

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```


© 2019 Palo Alto Networks, Inc.

# 注册防火墙

您必须首先注册防火墙才能激活支持及其他许可证及订阅。但是，注册防火墙之前，必须首先拥有一个激活的支持账户。根据您是否拥有激活的支持账户，执行以下任务之一：

- 如果您没有激活的支持账户，则创建新支持账户，并注册防火墙。
- 如果您已拥有激活的支持账户，则可以注册防火墙。
- （可选）执行第 1 天配置在注册防火墙上。

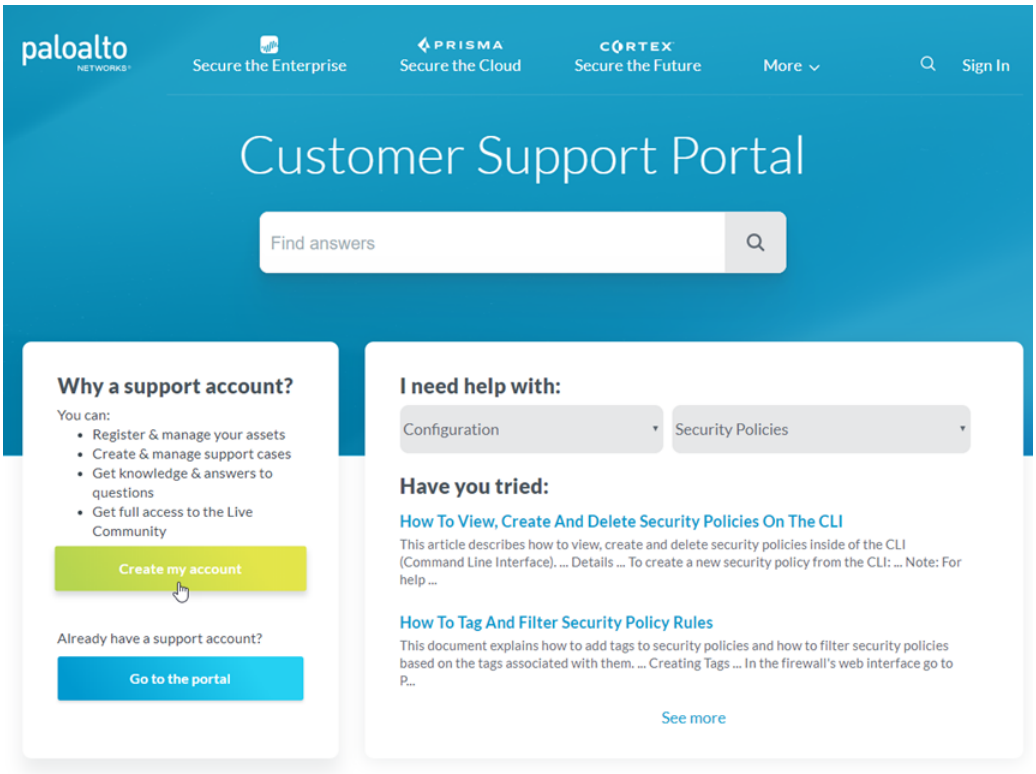
如果您准备注册 VM 系列防火墙，有关说明，请参考《VM 系列防火墙部署指南》。

## 创建新支持账户，并注册防火墙

如果您尚未拥有激活的 Palo Alto Networks 支持账户，则需要在创建新支持账户时注册防火墙。

STEP 1 | 前往 Palo Alto Networks 客户支持门户。

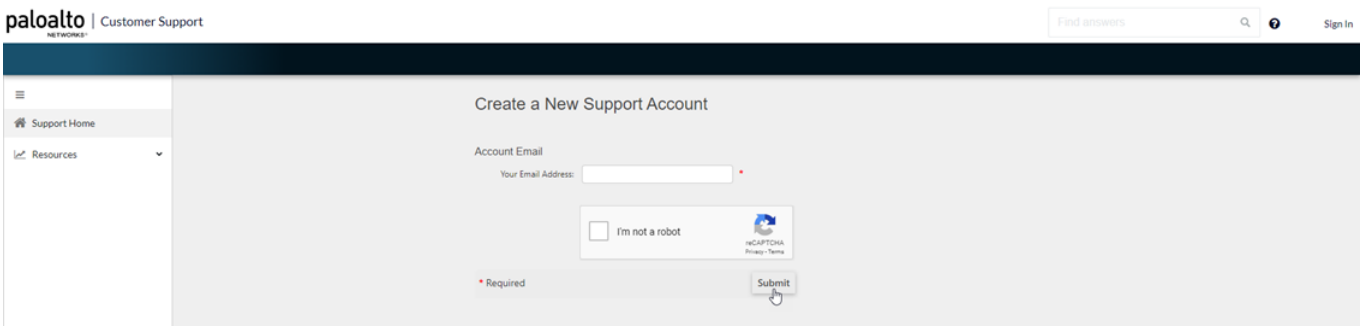
STEP 2 | 单击 **Create my account**（创建我的帐户）。



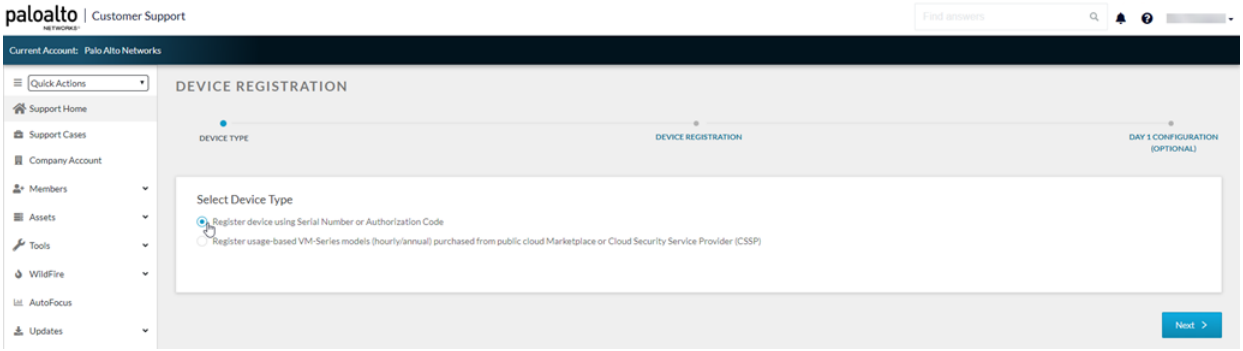

STEP 3 | 输入 **Your Email Address**（您的电子邮件地址），勾选 **I'm not a robot**（我不是机器人），然后单击 **Submit**（提交）。



© 2019 Palo Alto Networks, Inc.



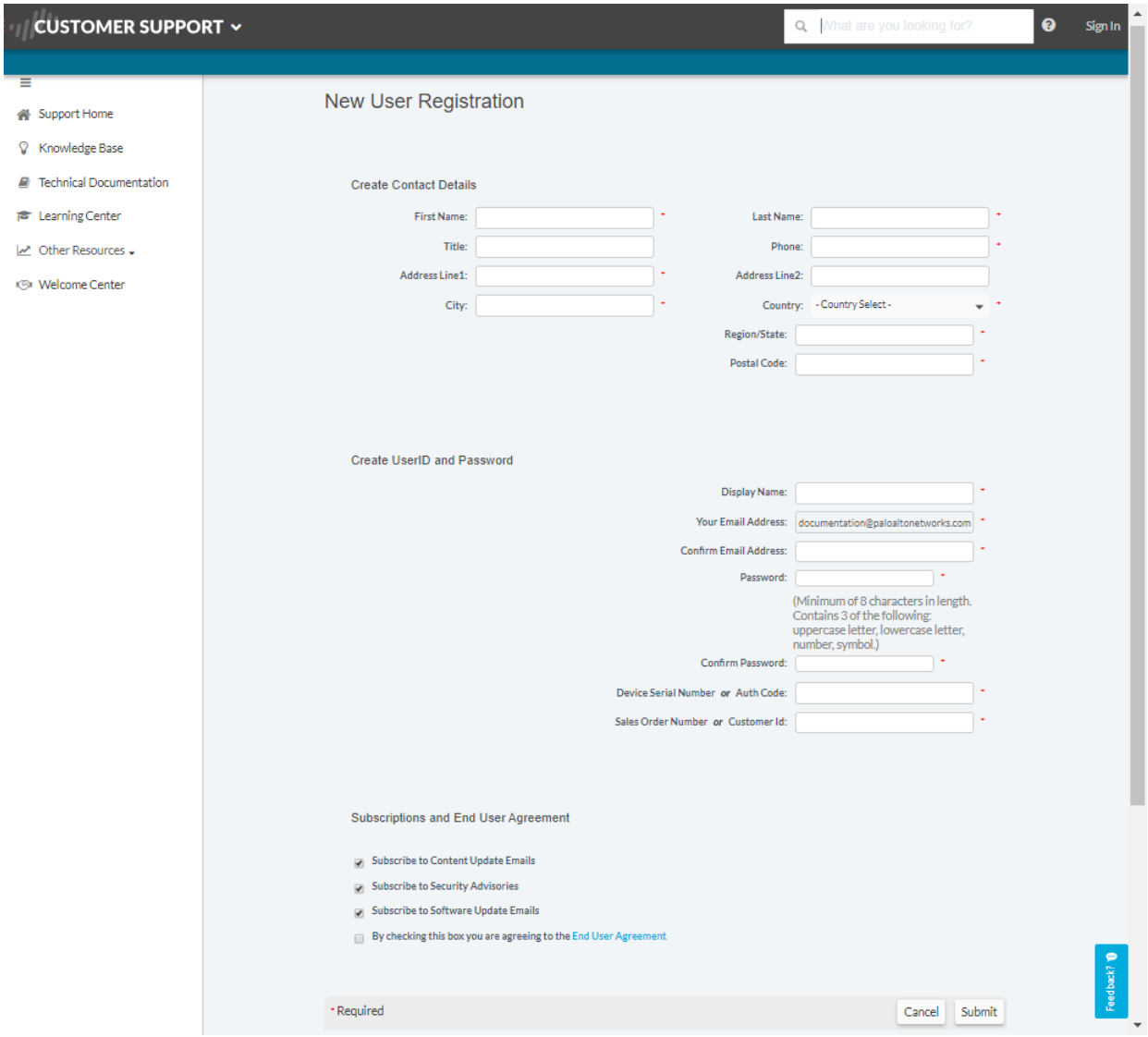

STEP 4 | 选择 **Register device using Serial Number or Authorization Code**（使用序列号或授权代码注册设备），并单击 **Next**（下一步）。




STEP 5 | 填写注册表。

1. 输入组织中将拥有此账户的人员详细联系信息。必填字段以红色星号表示。
2. 创建账户的 UserID 和密码。必填字段以红色星号表示。
3. 输入 **Device Serial Number**（设备序列号）或 **Auth Code**（身份验证代码）。
4. 输入您的 **Sales Order Number**（销售订单号）或 **Customer Id**（客户 **Id**）。
5. 要始终收到最新更新和安全通知警报，请 **Subscribe to Content Update Emails**（订阅内容更新电子邮件）、**Subscribe to Security Advisories**（订阅安全通知）和 **Subscribe to Software Update Emails**（订阅软件更新电子邮件）。
6. 选择复选框以同意终端用户协议，并 **Submit**（提交）。


© 2019 Palo Alto Networks, Inc.




# 注册防火墙

如果已拥有激活的 Palo Alto Networks 客户支持账户，请执行以下任务以注册防火墙。

STEP 1 | 登录到防火墙 Web 界面。

在 Web 浏览器中使用安全连接 (HTTPS)，通过初始配置期间分配的新 IP 地址和密码登录 (https://<IP address>)。

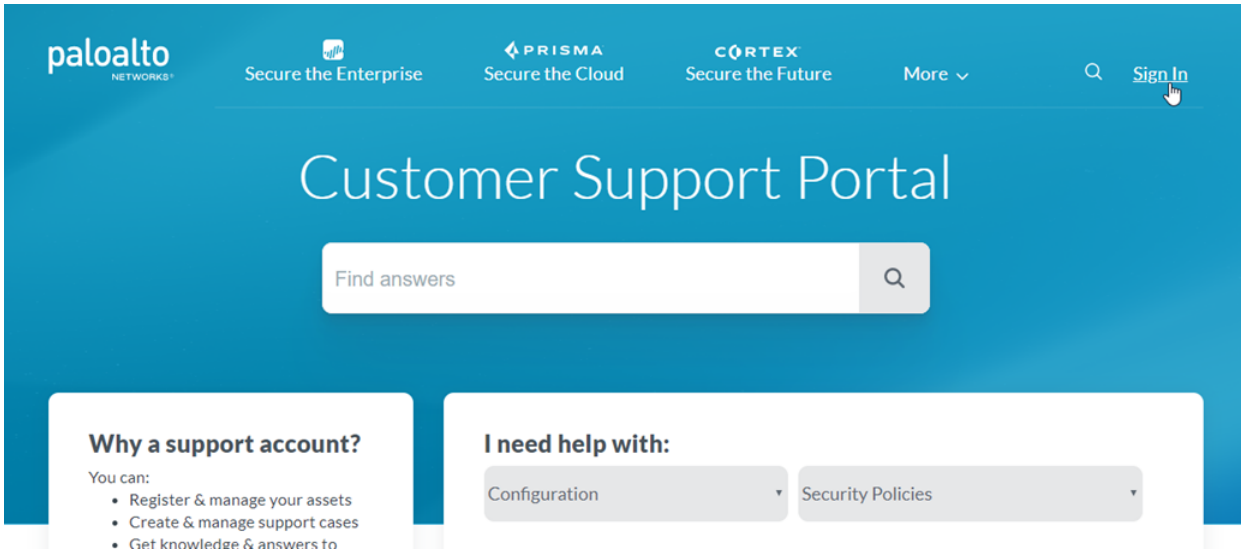
STEP 2 | 找到序列号并将其复制到剪贴板。

在**Dashboard**（仪表板）上，可在屏幕上的“常规信息”部分中查找到**Serial Number**（序列号）。

STEP 3 | 前往 Palo Alto Networks 客户支持门户，如果尚未登录，请立即 **Sign In**（登录）。

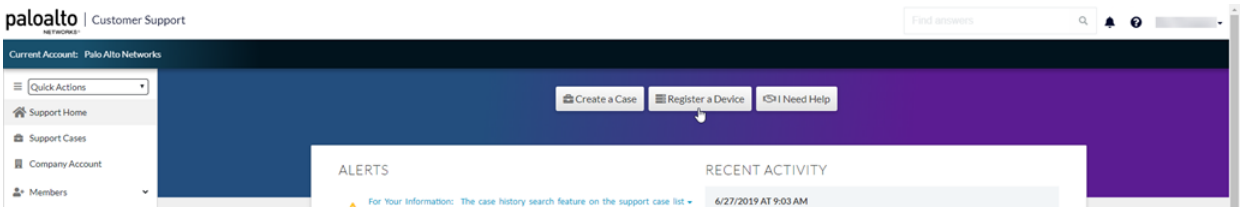


© 2019 Palo Alto Networks, Inc.

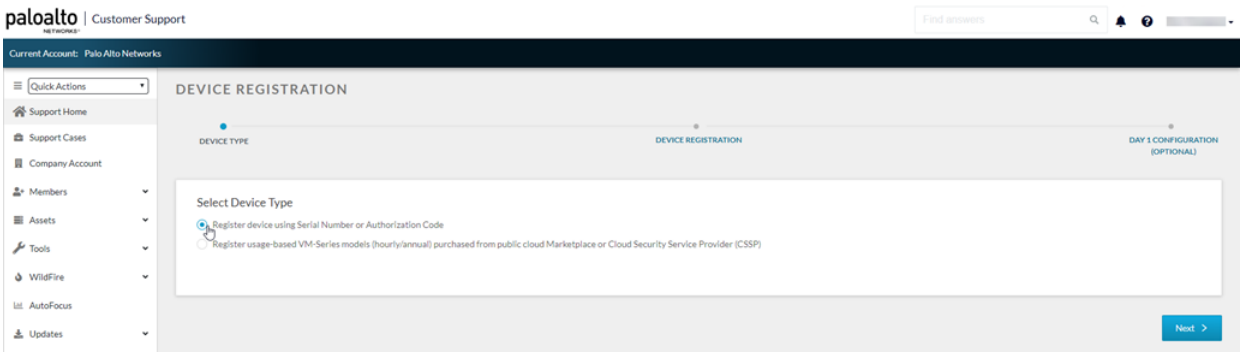



STEP 4 | 注册防火墙。

1. 在 Support Home（支持中心）页面上，单击 **Register a Device**（注册设备）。

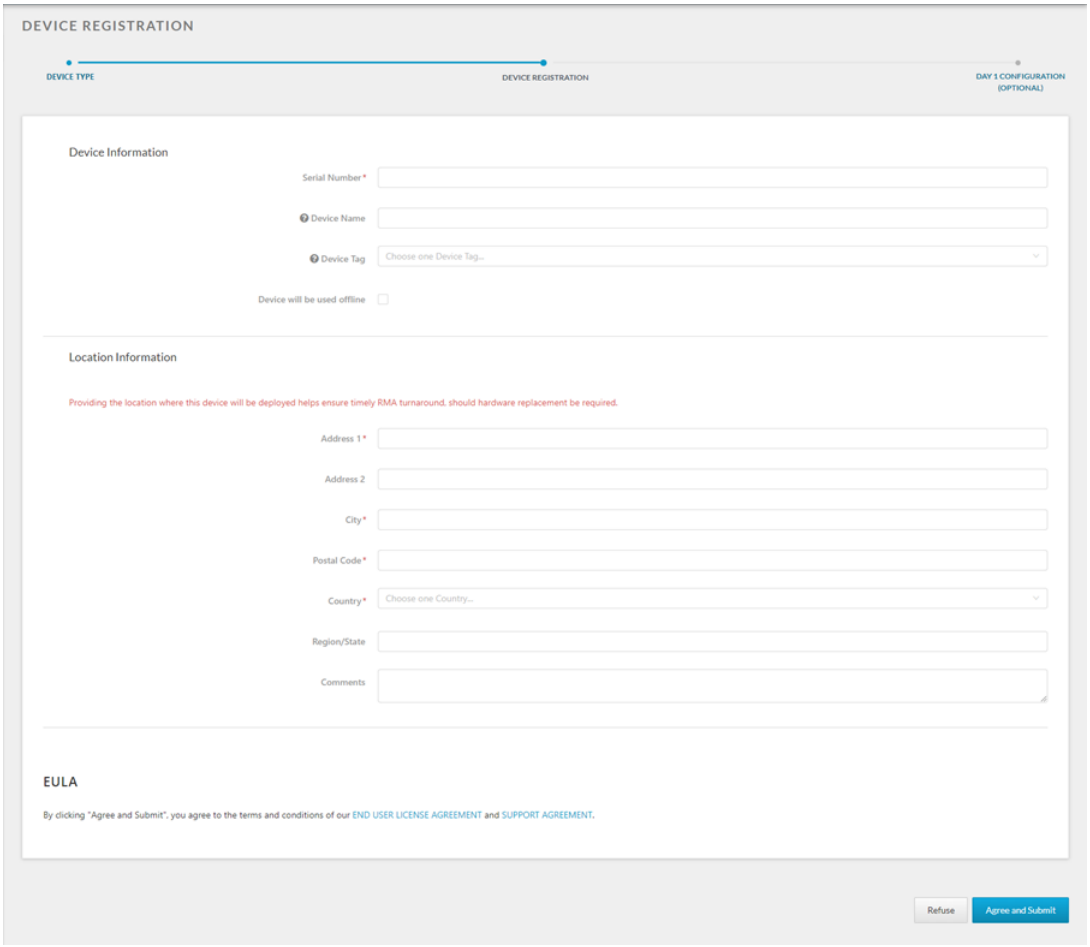



2. 选择 **Register device using Serial Number or Authorization Code**（使用序列号或授权代码注册设备），然后单击 **Next(下一步)**。




3. 输入防火墙 **Serial Number**（序列号）（您可从防护墙“仪表板”复制并粘贴序列号）。
4. （可选）输入 **Device Name**（设备名称）和 **Device Tag**（设备标签）。
5. （可选）如果设备没有连接到互联网，则选择 **Device will be used offline**（设备将脱机使用）复选框，然后从下拉列表中选择您计划使用的 **OS Release**（OS 发布）。
6. 提供您打算部署防火墙的位置信息，包括**Address**（地址）、**City**（城市）、**Postal Code**（邮编）和 **Country**（国家）。
7. 阅读终端用户许可证协议 (EULA) 和支持协议，然后 **Agree and Submit**（同意并提交）。


© 2019 Palo Alto Networks, Inc.




您可以在 **Devices**（设备）下方查看刚刚注册的防火墙条目。

# （可选）执行第 1 天配置

注册防火墙后，您可以选择运行第 1 天配置。第 1 天配置工具提供 Palo Alto Networks 最佳实践提示的配置模板，您可将此模板用作构建其余配置的起点。

使用“第 1 天配置”模板的好处包括：

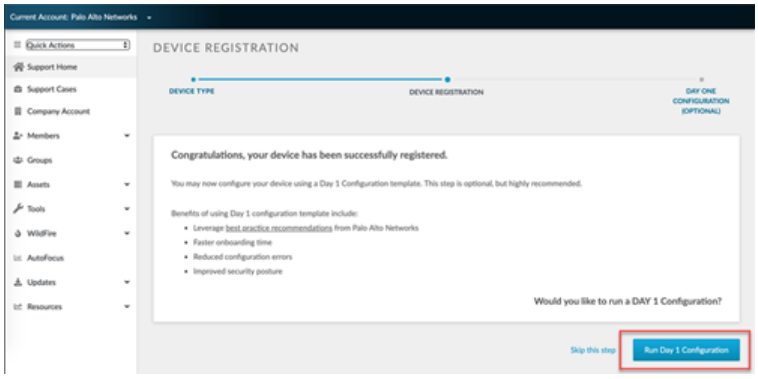
- 实现时间更快
- 配置错误更少
- 安全状态更佳

按照以下步骤执行第 1 天配置：

STEP 1 | 注册防火墙后，从显示的页面中选择 **Run Day 1 Configuration**（运行第 **1** 天配置）。

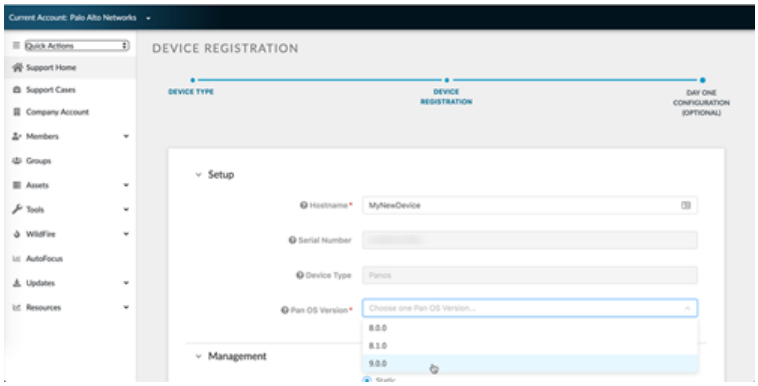


© 2019 Palo Alto Networks, Inc.



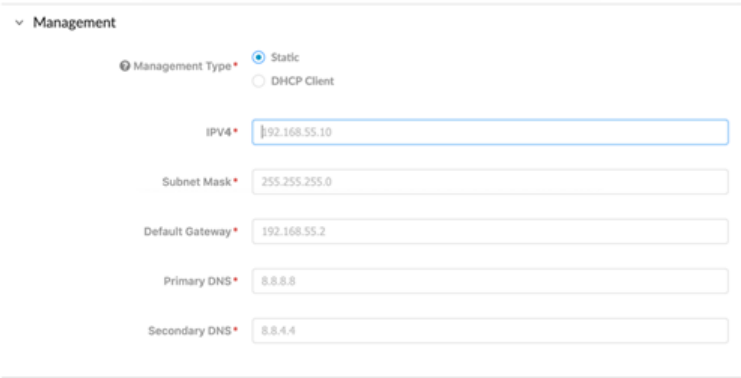

如果已注册防火墙，但尚未运行第 *1* 天配置，您还可以通过选择 *Tools*（工具）> *Run Day 1 Configuration*（运行第 *1* 天配置）从客户支持门户主页运行它。

STEP 2 | 输入新设备的 **Hostname**（主机名）和 **Pan OS Version**（**Pan OS** 版本），以及 **Serial Number**（序列号）和 **Device Type**（设备类型）（可选）。




STEP 3 | 在 **Management**（管理）中，选择 **Management Type**（管理类型）为 **Static**（静态）或 **DHCP Client**（DHCP 客户端）。

选择 **Static**（静态）将要求您填写 **IPV4**、**Subnet Mask**（子网掩码）和 **Default Gateway**（默认网关）字段。



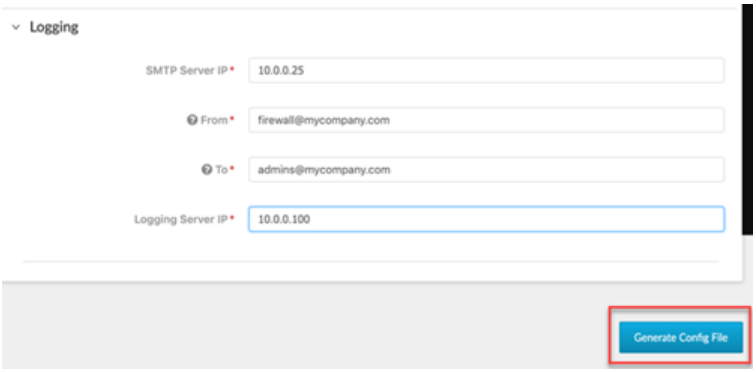

若选择 **DHCP Client**（**DHCP** 客户端），仅需要您输入 **Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）。设备若在 DHCP 客户端模式下完成配置，可确保管理接口接收来自本地 DHCP 服务器的 IP 地址，或在已知情况下填写所有参数。


© 2019 Palo Alto Networks, Inc.



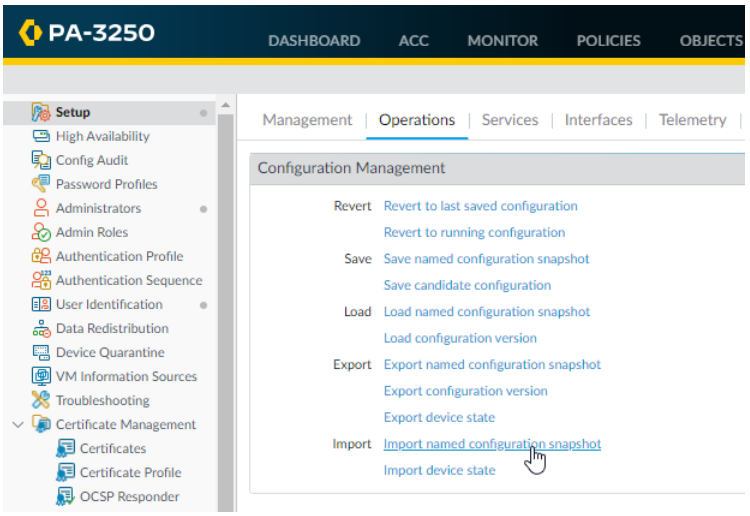

STEP 4 | 填写 **Logging**（日志记录）中的所有字段。

STEP 5 | 单击 **Generate Config File**（生成配置文件）。




STEP 6 | 要导入并加载第 1 天配置文件，只需将其下载到您的防火墙即可：

1. 登录到防火墙 Web 界面。
2. 选择**Device**（设备）> **Setup**（设置）> **Operations**（操作）。
3. 单击 **Import named configuration snapshot**（导入已命名配置快照）。
4. 选择文件。






© 2019 Palo Alto Networks, Inc.

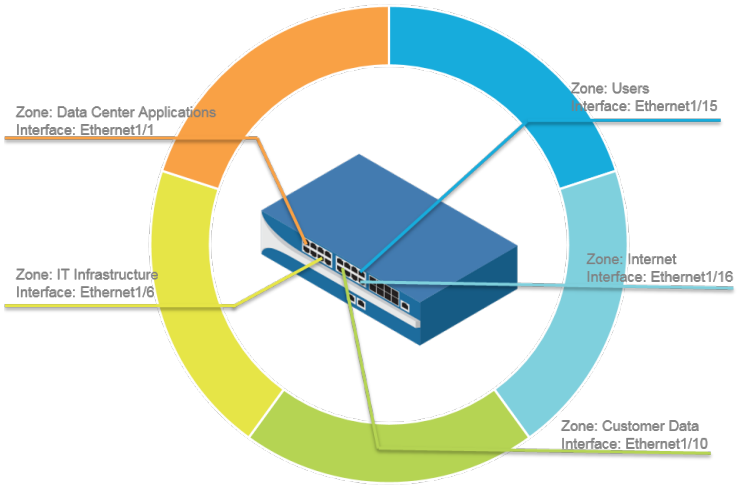
# 使用接口和区域对网络进行分段

通信必须通过防火墙，防火墙才能对其进行管理和控制。实际上，通信通过接口进入和退出防火墙。防火墙根据数据包是否匹配安全策略规则来决定如何处理数据包。作为最基本的要求，每个安全策略规则必须识别通信来自哪里及去往何方。在 Palo Alto Networks 的下一代防火墙上，区域之间会应用安全策略规则。区域指一组代表您连接至防火墙并由其控制的网络分段的（物理或虚拟）接口。如果存在控制流量的安全策略规则（您的第一道安全防线），那么流量仅可在各区域间流动。您所创建的区域粒度越高，您对敏感应用程序及数据访问权限的控制力度越大，因而能加大对在网络中横向移动的恶意软件的防御。例如，您可能想要将储存客户数据的数据库服务器的访问权限细分为叫做“客户数据”的区域。您可以定义安全策略，仅允许某些用户或用户组访问“客户数据”区域，从而防止对存储于该分段数据的外部或内部未授权访问。

- 减小攻击面的网络分段
- 配置接口和区域

## 减小攻击面的网络分段

下图展示的是使用区域进行网络分段的非常基本的示例。区域（及控制流量在各区域间流动的相应安全策略规则）的粒度越高，您所能减少的网络攻击面就越大。原因是通信可在某个区域内自由流动（区域内流量），但无法在区域之间流动（区域间流量），除非您定义一个允许这样做的安全策略规则。此外，在分配接口至区域前，界面无法处理流量。因此，将网络细分为粒度区域可让您加大对敏感应用程序或数据的访问权限的控制，您还可在网络内建立通信隧道来阻止恶意流量，从而减少网络攻击的成功概率。




## 配置接口和区域

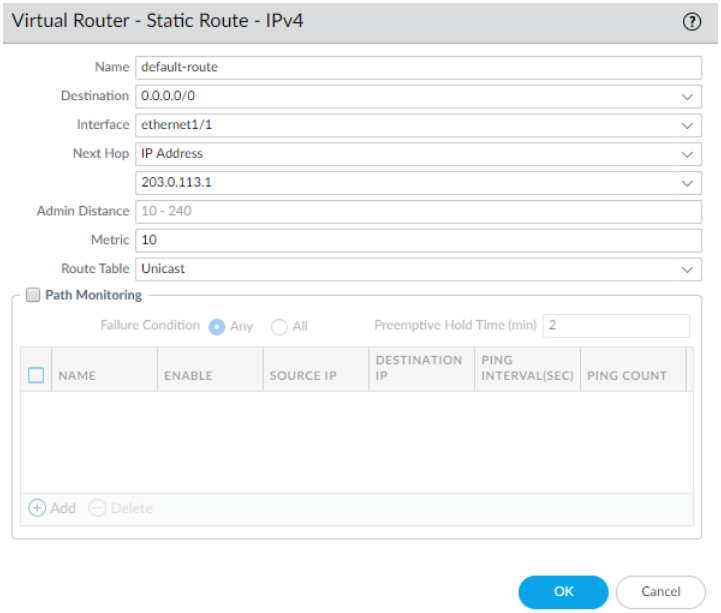
在确定您希望如何细分网络及您需要创建以实现细分的区域（以及映射到各区域的接口）后，您便可开始配置防火墙上的接口及区域。在防火墙上配置接口，以支持您所连接的各网络部分的拓扑。以下工作流对如何配置第三层接口及将它们分配至各区域进行了介绍。了解使用不同类型的接口部署（如虚拟线路接口或第 2 层接口）集成防火墙的详细信息，请参阅联网。

防火墙在端口 *Ethernet 1/1* 与 *Ethernet 1/2* 之间预配置了默认 *Virtual Wire* 接口（及相应的默认安全策略和虚拟路由器）。如果您不打算使用默认的 *Virtual Wire*，则应将此配置手动删除并提交更改，然后再继续操作，以免与您定义的其他设置发生冲突。有关如何删除默认虚拟线路及其关联安全策略和区域的说明，请参阅设置外部服务的网络访问权中的步骤 *3*。

STEP 1 | 配置互联网路由器的默认路由：


© 2019 Palo Alto Networks, Inc.

1. 请选择 **Network**（网络）> **Virtual Router**（虚拟路由器），然后选择 **default**（默认）链接来打开虚拟路由器对话框。
2. 选择 **Static Routes**（静态路由）选项卡并单击 **Add**（添加）。输入路由的**Name**（名称），并在**Destination**（目标）字段中输入路由（如 0.0.0.0/0）。
3. 选择 **Next Hop**（下一个跃点）字段中的 **IP Address**（IP 地址）单选按钮，然后输入 Internet 网关的 IP 地址和子网掩码（如 203.0.113.1）。

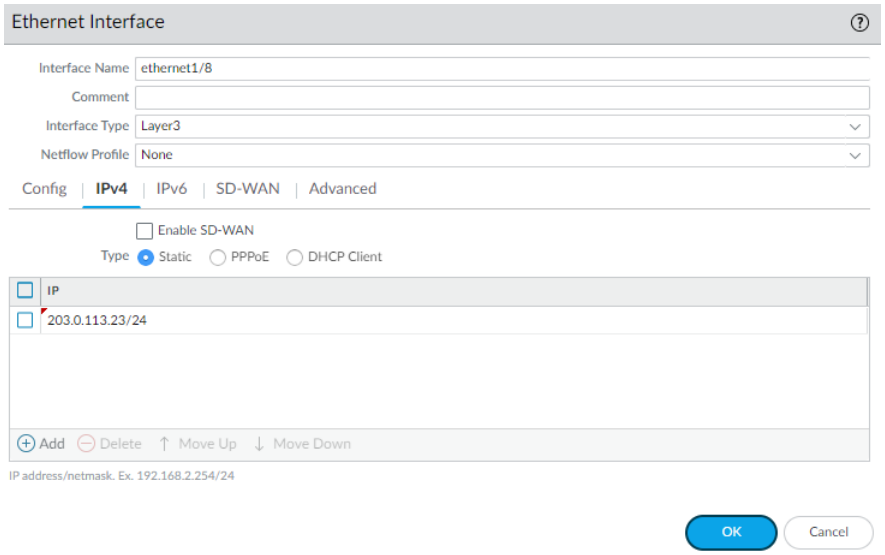



4. 单击 **OK**（确定）两次，以保存虚拟路由器配置。

STEP 2 | 配置外部接口（连接到 Internet 的接口）。

1. 选择 **Network**（网络）> **Interfaces**（接口），然后选择要配置的接口。在此示例中，我们要将 Ethernet1/8 配置为外部接口。
2. 选择 **Interface Type**（接口类型）。此示例显示了针对 **Layer3**（第 3 层）的步骤，但是您在此处的选择取决于接口拓扑。
3. 在 **Config**（配置）选项卡上，选择 **New Zone**（安全区域）下拉列表中的 **Security Zone**（新区域）。在区域对话框中，定义新区域的 **Name**（名称），例如 Internet，然后单击 **OK**（确定）。
4. 在 **Virtual Router**（虚拟路由器）下拉列表中，选择 **default**（默认）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (添加)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 203.0.113.23/24。


© 2019 Palo Alto Networks, Inc.




6. 若要让您能够 ping 该接口，请选择 **Advanced**（高级）> **Other Info**（其他信息），展开 **Management Profile**（管理配置文件）下拉列表，然后选择 **New Management Profile**（新管理配置文件）。输入配置文件的 **Name**（名称），选中 **Ping**，然后单击 **OK**（确定）。
7. 要保存接口配置，请单击 **OK**（确定）。

STEP 3 | 配置连接到内部网络的接口。

在此示例中，接口连接到使用私有 *IP* 地址的网段。因为无法在外部路由私有 *IP* 地址，所以您必须配置 NAT。

1. 选择 **Network**（网络）> **Interfaces**（接口）并选择要配置的接口。在此示例中，我们要将 Ethernet1/15 配置为用户连接的内部接口。
2. 选择 **Layer3**（第三层）作为 **Interface Type**（接口类型）。
3. 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。在区域对话框中，定义新区域的 **Name**（名称），例如 Users，然后单击 **OK**（确定）。
4. 选择您之前使用的同一虚拟路由器，此例中为默认。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (添加)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.1.4/24。
6. 要让您能够 Ping 该接口，请选择您刚创建的管理配置文件。
7. 要保存接口配置，请单击 **OK**（确定）。

STEP 4 | 配置连接到数据中心应用程序的接口。

务必定义粒度区域以防止未经授权访问敏感应用程序或数据，并消除恶意软件在数据中心内横向移动的可能性。

1. 选择要配置的接口。
2. 从 **Interface Type**（接口类型）下列列表中选择 **Layer3**（第 3 层）。在此示例中，我们要将 Ethernet1/1 配置为提供访问数据中心应用程序权限的接口。
3. 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。在区域对话框中，定义新区域的 **Name**（名称），例如 Data Center Applications，然后单击 **OK**（确定）。
4. 选择您之前使用的同一虚拟路由器，此例中为默认。

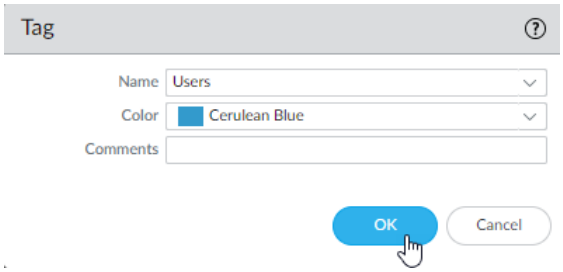

© 2019 Palo Alto Networks, Inc.

5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (**添加**)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 10.1.1.1/24。
6. 要让您能够 Ping 该接口，请选择您创建的管理配置文件。
7. 要保存接口配置，请单击 **OK**（确定）。

STEP 5 | （可选）为每个区域创建标签。

标签是浏览策略规则的可视化方法。

1. 选择 **Objects**（对象）> **Tags**（标签），然后 **Add**（添加）。
2. 选择区域 **Name**（名称）。
3. 选择标签 **Color**（颜色）并单击 **OK**（确定）。




STEP 6 | 保存接口配置。

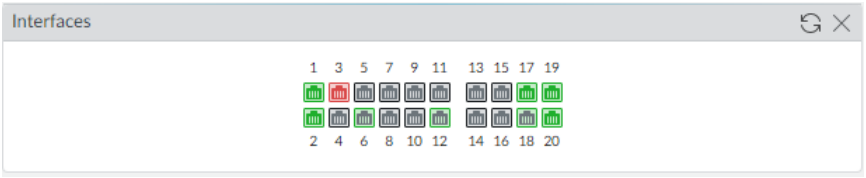
单击 **Commit**（提交）。

STEP 7 | 连接防火墙。

使用直通线缆将已配置的接口连接到每个网段上的相应交换机或路由器。

STEP 8 | 验证接口处于活动状态。

选择 **Dashboard**（仪表板）并确认您配置的接口在接口部件中显示为绿色。






© 2019 Palo Alto Networks, Inc.

# 设置基本安全策略

现在，您已定义一些区域并将其分配至接口，可准备开始创建安全策略。在未创建安全策略规则前，防火墙不允许流量在各区域间的流动。数据包进入防火墙接口后，防护墙会根据安全策略规则匹配数据包属性，从而基于属性（例如源和目标安全区域、源和目标 IP 地址、应用程序、用户和服务）确定是阻止还是允许某个会话。根据安全策略规则库，防火墙会按从左至右、从上到下的顺序检查流入流量，然后按第一条安全规则的规定操作，执行匹配（如是否允许、拒绝或丢弃数据包）。这意味着您必须对安全策略规则库中规则进行排序，从而让特定性更强的规则位于规则库的顶部，一般性更强的规则位于顶部，确保防火墙按预期执行策略。

即使安全策略规则允许数据包，这并不意味着流量没有威胁。要使防火墙根据安全策略规则扫描其允许的流量，还必须将安全配置文件（包括 URL 筛选、防病毒、防间谍软件、文件阻止和 WildFire 分析）附加到每个规则（可以使用的配置文件取决于您购买的订阅）。创建基本安全策略时，请使用预定义的安全配置文件确保扫描您网络中允许的流量，以查找威胁。您可以根据环境需要随时自定义这些配置文件。

使用以下工作流程设置一个非常基本的安全策略，可以访问网络基础设施、数据中心应用程序和 Internet。这让您可以启动并运行防火墙，并据此确认防火墙是否配置成功。但是，该初始策略并不能为网络提供全面的综合保护。在确认防火墙已成功配置并集成到网络后，继续创建最佳实践之互联网网关安全策略，从而在保障安全访问应用程序的同时防止网络受到攻击。

STEP 1 | （可选）删除默认安全策略规则。

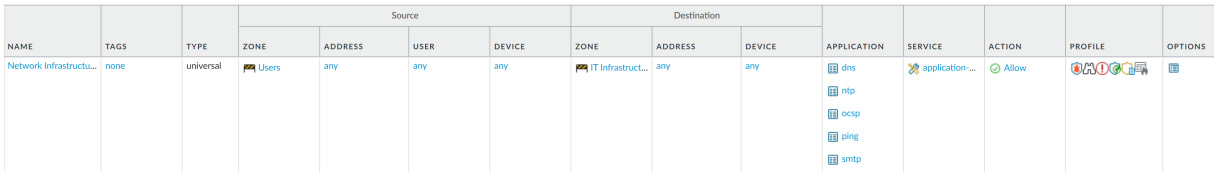
默认情况下，防火墙包含一个名为 *rule1* 的安全策略规则，它允许从信任区域到不信任区域的所有通信。您可以删除该规则，或修改该规则以反映您的区域命名约定。

STEP 2 | 允许访问网络基础设施资源。

1. 选择 **Policies**（策略）> **Security**（安全），并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称）。
3. 在 **Source**（源）选项卡中，将 **Source Zone**（源区域）设置为 **Users**（用户）。
4. 在 **Destination**（目标）选项卡中，将 **Destination Zone**（目标区）设置为 **IT Infrastructure**（IT 基础设施）。

   最佳实践是，使用 *Destination Address*（目标地址）字段中的地址对象以便仅能够访问特定服务器或服务器组，尤其是对于 *DNS* 和 *SMTP* 等经常被利用的服务。通过仅限用户访问特定目标服务器地址，您可以防止数据泄露以及通过 *DNS* 隧道等技术建立通信的命令和控制流量。
5. 在 **Applications**（应用程序）选项卡，**Add**（添加）您想要安全启用的网络服务所对应的应用程序。例如，选择 **dns**、**ntp**、**ocsp**、**ping** 和 **smtp**。
6. 在 **Service/URL Category**（服务/URL 类别）选项卡，将 **Service**（服务）设置为 **application-default**。
7. 在 **Actions**（操作）选项卡中，将 **Action Setting**（操作设置）设置为 **Allow**（允许）。
8. 将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件），然后选择以下安全配置文件以附加到策略规则：
   - 对于 **Antivirus**（防病毒），请选择 **default**（默认）
   - 对于 **Vulnerability Protection**（漏洞保护），请选择 **strict**（严格）
   - 对于 **Anti-Spyware**（防间谍软件），请选择 **strict**（严格）
   - 对于 **URL Filtering**（URL 筛选），请选择 **default**（默认）
   - 对于 **File Blocking**（文件阻止），请选择 **basic file blocking**（基本文件阻止）
   - 对于 **WildFire Analysis**（WildFire 分析），请选择 **default**（默认）
9. 确认 **Log at Session End**（会话端日志）已启用。只有与安全策略规则相匹配的通信才会被记录。
10. 单击 **OK**（确定）。

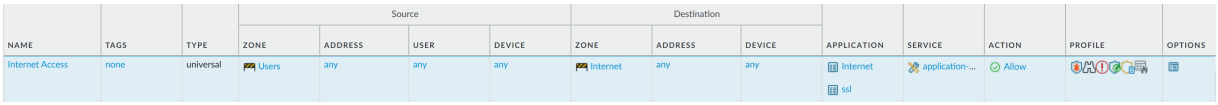

© 2019 Palo Alto Networks, Inc.




STEP 3 | 启用访问常规互联网应用程序。

该临时规则可允许您收集网络中的流量信息。在您对用户所需访问的应用程序有更多了解后，您便可据此做出允许哪些应用程序的决定，同时为用户组创建粒度更高的应用程序规则。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）规则。
2. 在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称）。
3. 在 **Source**（源）选项卡中，将 **Source Zone**（源区域）设置为 **Users**（用户）。
4. 在 **Destination**（目标）选项卡中，将 **Destination Zone**（目标区）设置为 **Internet**。
5. 在 **Applications**（应用程序）选项卡，**Add**（添加）**Application Filter**（应用程序筛选器）并输入一个**Name**（名称）。要安全访问合法的基于 Web 的应用程序，将应用程序筛选器中的 **Category**（类别）设置为 **general-internet**（常规 **Internet**），然后单击 **OK**（确定）。要启用对加密站点的访问，请 **Add**（添加）**ssl** 应用程序。
6. 在 **Service/URL Category**（服务/URL 类别）选项卡，将 **Service**（服务）设置为 **application-default**。
7. 在 **Actions**（操作）选项卡中，将 **Action Setting**（操作设置）设置为 **Allow**（允许）。
8. 将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件），然后选择以下安全配置文件以附加到策略规则：
   - 对于 **Antivirus**（防病毒），请选择 **default**（默认）
   - 对于 **Vulnerability Protection**（漏洞保护），请选择 **strict**（严格）
   - 对于 **Anti-Spyware**（防间谍软件），请选择 **strict**（严格）
   - 对于 **URL Filtering**（URL 筛选），请选择 **default**（默认）
   - 对于 **File Blocking**（文件阻止），请选择 **strict file blocking**（严格文件阻止）
   - 对于 **WildFire Analysis**（**WildFire** 分析），请选择 **default**（默认）
9. 确认 **Log at Session End**（会话端日志）已启用。只有与安全规则相匹配的通信才会被记录。
10. 单击 **OK**（确定）。




STEP 4 | 启用访问数据中心应用程序。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）规则。
2. 在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称）。
3. 在 **Source**（源）选项卡中，将 **Source Zone**（源区域）设置为 **Users**（用户）。
4. 在 **Destination**（目标）选项卡中，将 **Destination Zone**（目标区）设置为 **Data Center Applications**（数据中心应用程序）。
5. 在 **Applications**（应用程序）选项卡，**Add**（添加）您想要安全启用的网络服务所对应的应用程序。例如，选择 **activesync**、**imap**、**kerberos**、**ldap**、**ms-exchange** 和 **ms-lync**。
6. 在 **Service/URL Category**（服务/URL 类别）选项卡，将 **Service**（服务）设置为 **application-default**。
7. 在 **Actions**（操作）选项卡中，将 **Action Setting**（操作设置）设置为 **Allow**（允许）。
8. 将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件），然后选择以下安全配置文件以附加到策略规则：



© 2019 Palo Alto Networks, Inc.

- 对于 **Antivirus**（防病毒），请选择 **default**（默认）
- 对于 **Vulnerability Protection**（漏洞保护），请选择 **strict**（严格）
- 对于 **Anti-Spyware**（防间谍软件），请选择 **strict**（严格）
- 对于 **URL Filtering**（URL 筛选），请选择 **default**（默认）
- 对于 **File Blocking**（文件阻止），请选择 **basic file blocking**（基本文件阻止）
- 对于 **WildFire Analysis**（WildFire 分析），请选择 **default**（默认）

9. 确认 **Log at Session End**（会话端日志）已启用。只有与安全规则相匹配的通信才会被记录。
10. 单击 **OK**（确定）。

| | | | Source | | | | Destination | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| NAME | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | ACTION | PROFILE | OPTIONS |
| Data Center Applica... | none | universal | Users | any | any | any | Datacenter ... | any | any | activesync<br>imap<br>kerberos<br>ldap<br>ms-exchange<br>ms-lync | application-... | Allow | | |

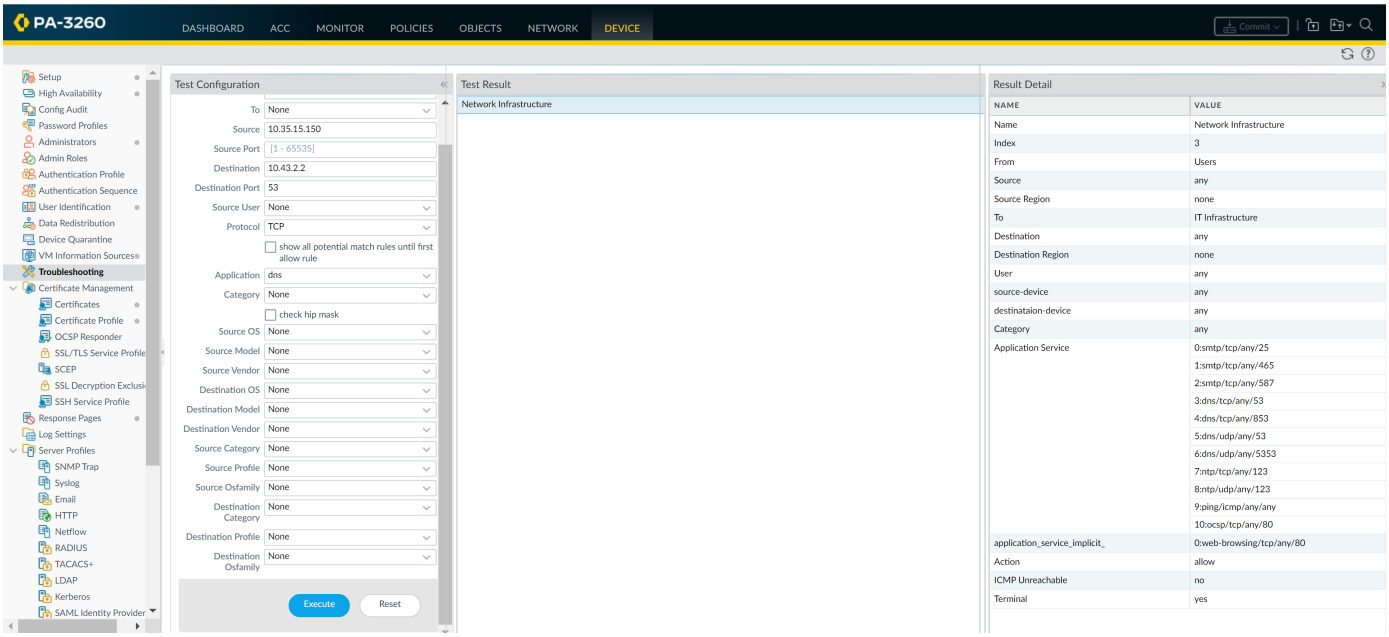
STEP 5 | 将您的策略规则保存到防火墙上正在运行的配置。

单击 **Commit**（提交）。

STEP 6 | 为了验证是否已有效设置基本策略，请测试是否正在评估安全策略规则，并确定哪项安全策略规则适用于通信流。

例如，若要验证用户区域内 IP 地址为 10.35.14.150 的客户端在向位于数据中心的 DNS 服务器发送 DNS 查询时将应用的策略规则，应尝试以下命令：

1. 选择 **Device**（设备）> **Troubleshooting**（故障排除），然后选择 **Security Policy Match**（安全策略匹配）（**Select Test**（选择测试））。
2. 输入 **Source**（源）和 **Destination**（目标）IP 地址。
3. 输入 **Protocol**（协议）。
4. 选择 **dns**（**Application**（应用程序））
5. **Execute**（执行）安全策略匹配测试。





© 2019 Palo Alto Networks, Inc.

# 访问网络流量

现在，您已配置一个基本安全策略，您可以在应用程序命令中心 (ACC) 中查看统计信息和数据，还可以查看通信日志和威胁日志以观察网络上的趋势。您可通过该信息确定您是否需要创建粒度更高的安全策略规则。

- 使用应用程序命令中心和使用自动关联引擎。

  在 ACC 中，查看您的网络上最常使用的应用程序和高风险应用程序。ACC 以图表形式概括日志信息，从而突出显示遍历网络的应用程序、使用这些应用程序的用户（启用 User-ID）以及内容的可能安全影响，以帮助您实时地掌握网络上发生的情况。然后，可以使用此信息来创建相应的安全策略规则，让该策略阻止不需要的应用程序，同时以安全的方式允许并启用应用程序。

  在 **ACC** > **Threat Activity**（威胁活动）中的“受影响的主机”小部件上显示您的网络上可能受影响的主机以及用于确定这些事件的日志和匹配证据。

- 确定需要为您的网络安全策略规则进行什么更新/修改，并实施这些更改。

  例如：

  - 评估是否根据计划、用户或组允许 Web 内容。
  - 允许或控制特定应用程序或应用程序中的功能。
  - 解密并检查内容。
  - 允许但扫描威胁和攻击。

  有关改进安全策略及附加自定义安全配置文件的信息，请参阅如何创建安全策略规则和安全配置文件。

- 查看日志。

  具体来说，查看流量和威胁日志（**Monitor**（监控）> **Logs**（日志））。

  流量日志取决于安全策略的定义方式和流量记录设置。但是，无论怎样配置策略，“应用程序使用”部件中的*ACC* 选项卡都会记录应用程序和统计信息；它将显示网络上允许的所有通信，因此它会包括策略允许的区域间通信以及隐式允许的区域内通信。

- 配置日志存储配额和过期期限。

  查看 AutoFocus 情报摘要中的日志构件。构件是与防火墙上记录活动相关的项目、属性、活动或行为。情报概览显示了会话次数及 WildFire 检测到构件的样本数目。使用 WildFire 判定信息（良性、灰色或恶意）及 AutoFocus 匹配标签以检查网络中的潜在风险。

  Unit 42 创建的 *AutoFocus* 标签，*Palo Alto Networks* 威胁情报团队提醒相关人士注意高级、针对性攻击活动及威胁。

  您可从 AutoFocus 情报概览中启动 AutoFocus 搜索，检索构件并评估其在全局、行业及网络环境下的普遍性。

- 监控网络用户的 Web 活动。

  查看 URL 筛选日志以扫描警报、拒绝的类别/URL。当流量与拥有通过警报、继续、覆盖或阻止操作附加的 URL 筛选配置文件的安全规则匹配时，将生成 URL 日志。



© 2019 Palo Alto Networks, Inc.

# 启用免费 WildFire 转发

WildFire 是基于云端的虚拟环境，旨在分析并执行未知样本（文件及邮件链接），确定样本属于恶意软件、网络钓鱼、灰色软件或良性软件。启用 WildFire 后，Palo Alto Networks 将转发未知样本至 WildFire 进行分析。对于新发现的恶意软件，WildFire 将生成签名来检测恶意软件，这使实时检索所有具备有效 WildFire 订阅的防火墙成为可能。这将启用全球所有 Palo Alto 下一代防火墙来检测并阻止由某道防火墙发现的恶意软件。恶意软件签名通常与恶意软件同一系列的多个变体相匹配，从而阻止防火墙从未见过的新的恶意软件变体。Palo Alto Networks 威胁研究团队使用从恶意软件变体收集的威胁情报来阻止恶意 IP 地址、域和 URL。

Palo Alto Networks 下一代防火墙包含 WildFire 基本服务，无需订阅 WildFire。通过 WildFire 基础服务，防火墙即可转发可移植可执行 (PE) 文件。此外，在未订阅 WildFire 但具备威胁预防订阅的情况下，您可收到 WildFire 每 24-48 小时发现的恶意软件签名（防病毒更新的部分内容）。

除 WildFire 基础服务外，防火墙需要 WildFire 订阅来：

- 实时获取最新 WildFire 签名。
- 使用WildFire Inline ML防止恶意可移植可执行文件和 PowerShell 脚本进入您的网络。
- 转发用于分析的高级文件类型及邮件链接。
- 使用 WildFire API。
- 使用 WildFire 设备作为 WildFire 私有云端或 WildFire 混合云端的主机。

如果您已订阅 WildFire，前往开始使用 WildFire 了解如何最大化利用该服务。或者，采用以下步骤启用 WildFire 基本转发：

STEP 1 | 确认已注册防火墙，且具有有效的支持帐户及所需的订阅服务。

1. 登录到 Palo Alto Networks 客户支持门户 (CSP)，并在左侧导航窗格中选择 **Assets**（资产）> **Devices**（设备）。
2. 验证是否已列出防火墙。如果没有，则选择 **Register New Device**（注册新设备），然后继续注册防火墙。
3. （可选）如果您已订阅威胁防护，则必须激活订阅许可证。

STEP 2 | 登录到防火墙，并配置 WildFire 转发设置。

1. 选择 **Device**（设备）> **Setup**（设置）> **WildFire**，然后编辑常规设置。
2. 设置 **WildFire Public Cloud**（**WildFire** 公共云）字段，并将文件转发到 WildFire 全局云：`wildfire.paloaltonetworks.com`。

   还可以根据您的位置和组织要求将文件转发到区域云或私有云。
3. 查看防火墙转发用于 WildFire 分析的 PE 的 **File Size Limits**（文件大小限制）。将防火墙可以转发的 PE 的 **Size Limit**（大小限制）设置为 10 MB 的最大可用限制。

   作为 WildFire 最佳实践，将 *PE* 的 *Size Limit*（大小限制）设置为 *10 MB* 的最大可用限制。
4. 单击 **OK**（确定）保存更改。

STEP 3 | 启用防火墙以转发用于分析的 PE。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **WildFire Analysis**（**WildFire** 分析）并 **Add**（添加）新的配置文件规则。
2. **Name**（命名）新配置文件规则。
3. **Add**（添加）转发规则，然后输入规则 **Name**（名称）。
4. 在 **File Types**（文件类型）列中，添加 **pe** 文件至转发规则。



© 2019 Palo Alto Networks, Inc.

5. 在 **Analysis**（分析）列中，选择 **public-cloud**（公共云）以转发 PE 至 WildFire 公共云。
6. 单击 **OK**（确定）。

STEP 4 | 应用新 WildFire 分析配置文件至防护墙允许的流量。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择一项现有策略或创建一项新策略规则，如设置基本安全策略中所述。
2. 选择 **Actions**（操作），然后在配置文件设置部分，将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）。
3. 选择刚创建的 **WildFire Analysis**（**WildFire** 分析）配置文件，将该配置文件规则应用于此策略规则允许的所有流量。
4. 单击 **OK**（确定）。

STEP 5 | 启用防火墙转发解密后的 SSL 通信进行 WildFire 分析。

STEP 6 | 查看并实施 WildFire 最佳实践，以确保您充分利用 WildFire 的检测和预防功能。

STEP 7 | **Commit**（提交）您的配置更新。

STEP 8 | 确认防火墙是否正将 PE 文件转发至 WildFire 公共云。

选择 **Monitor**（监控）> **Logs**（日志）> **WildFire SubmissionsWildFire** 提交）以查看防火墙成功提交进行 WildFire 分析的 PE 日志条目。Verdict（判定）列将显示 WildFire 对 PE 的类型划分，恶意、灰色型或良性。（WildFire 仅将网络钓鱼判定分配给电子邮件链接）。Action（操作）列显示防火墙已允许或阻挡了样本。严重性 列通过下列值指示样本向组织构成的威胁程度：关键、高、中、低和参考。

STEP 9 | （仅威胁防止订阅）如果您已订阅威胁防止，但未订阅 WildFire，您仍可每隔 24-48 小时收到 WildFire 的签名更新。

1. 选择**Device**（设备）> **Dynamic Updates**（动态更新）。
2. 检查防火墙是否计划下载，并安装防病毒更新。



© 2019 Palo Alto Networks, Inc.

# 完成防火墙部署的最佳实践

现在，在将防火墙集成到网络并启用基本安全策略功能后，可以开始配置更多高级功能。以下是要考虑的一项事项：

- 要确保正确保护管理界面的安全，请遵循确保管理员访问安全的最佳实践。
- 按最佳实践配置安全策略规则库旨在安全启用应用程序并保护您的网络免受攻击。转到最佳实践页面，然后选择适用于防火墙部署的安全策略最佳实践。
- 设置高可用性 — 高可用性 (HA) 是一种配置，在该配置中，两个防火墙结合成组，且其配置及会话表保持同步，从而防止网络上出现单点故障。防火墙对等端之间的检测信号连接可以确保当某个对等端关闭时提供无缝故障转移。在由两道防火墙组成的群集中设置防火墙可以提供冗余，并且可以确保业务连续性。
- 启用用户标识 (User-ID) — 用户标识 (User-ID) 是 Palo Alto Networks 的下一代防火墙功能，允许您根据用户和组（而不是单独的 IP 地址）来创建策略以及执行报告。
- 启用解密 — Palo Alto Networks 防火墙可提供用于解密和检查流量的功能，实现卓越的可见性、控制和粒度安全。在防火墙上使用解密可防止恶意内容进入网络或网络泄露隐藏作为加密或隧道流量的敏感内容。
- 请遵循防止网络免遭第 4 层和第 7 层逃避的最佳实践。
- 与 Palo Alto Networks 分享威胁情报 —允许防火墙定期收集并向 Palo Alto Networks 发送有关应用程序、威胁和设备运行状况的信息。遥测包括启用被动 DNS 监控，允许实验测试签名在后台运行的选项，而不会影响您的安全策略规则、防火墙日志或防火墙性能。所有 Palo Alto Networks 客户均能从遥测收集到的情报中获益，而 Palo Alto Networks 通过这些情报来提高防火墙的威胁防御功能。


© 2019 Palo Alto Networks, Inc.

# 确保管理员访问安全的最佳实践

要保护您的网络免受网络攻击，请从防火墙安全部署开始。如果用于管理敏感 IT 设备的网络保护不当，包括 Palo Alto Networks 下一代防火墙和 Panorama，您将无法检测并预防可能会导致敏感数据渗透和/或丢失的漏洞利用。确保防火墙访问安全的最终目的是，即使攻击者获得了对特权凭据的访问权限，您仍然可以阻止其进入，避免造成损失。请遵循这些最佳实践指南，以确保管理员以能够成功阻止攻击的方式安全访问您的防火墙和其他安全设备。


- 隔离管理网络
- 使用服务路由访问外部服务
- 限制访问管理接口
- 管理管理员访问权限
- 创建强大的管理员密码
- 扫描所有发往管理接口的流量
- 入站流量管理之证书替换
- 使内容和软件更新保持最新


## 隔离管理网络

所有 Palo Alto Networks 防火墙都提供一个可用于执行防火墙管理功能的带外管理端口 (MGT)。或者，您可以选择使用 MGT 端口进行初始配置，然后配置防火墙管理访问的数据端口。无论采用哪种方式，因为可以通过管理接口访问安全配置，因此您都必须采用以下预防措施来保护对此接口的访问：

请勿从互联网管理接口或企业安全边界内其他不信任区域访问。无论是使用专用管理端口*(MGT)*，还是将数据端口配置为管理接口，这都适用。

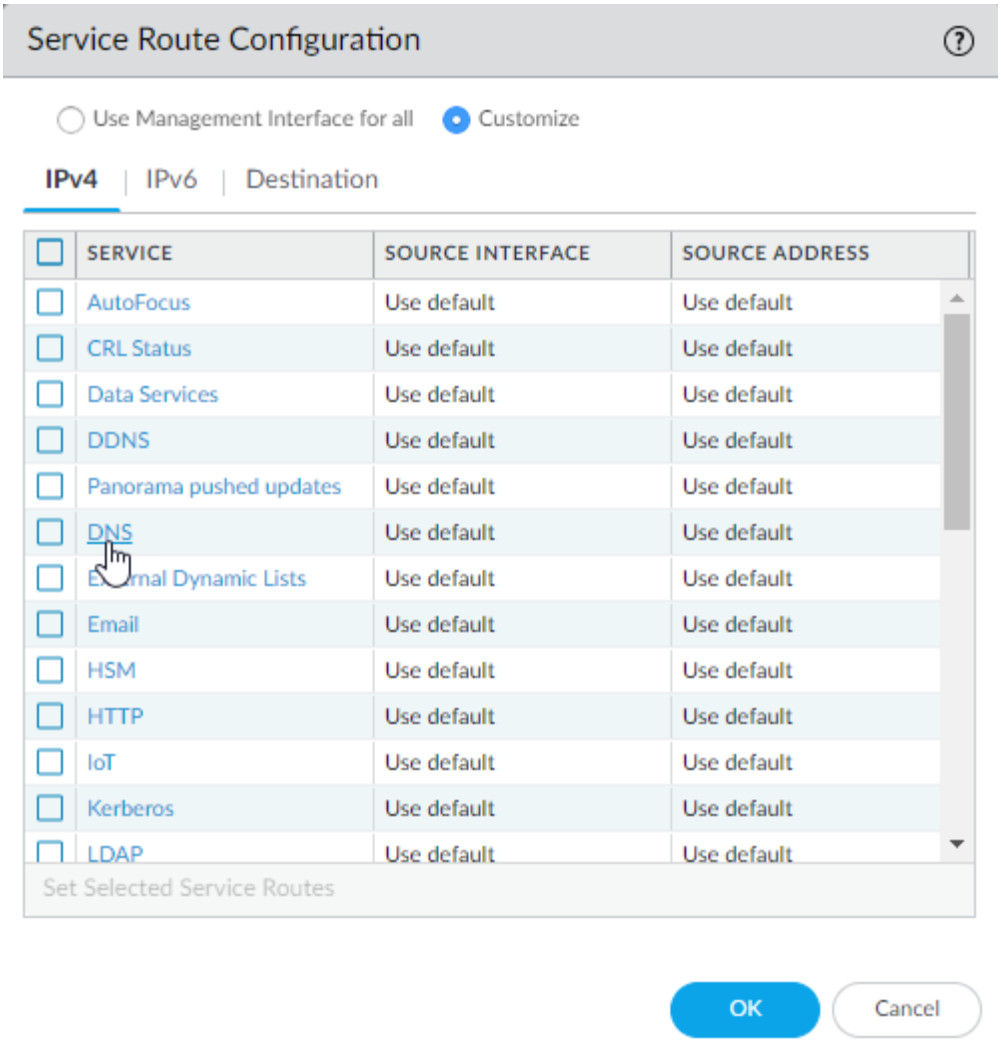
- 隔离专用管理 VLAN 上的管理接口。
- 允许进入管理接口的源 IP 地址被限制为允许进入您的这些专用管理设备，例如跳转服务器或堡垒主机。
- 使用跳转服务器或堡垒主机（带屏幕录制）提供从企业网络到专用管理接口的安全访问，并要求用户进行身份验证，获得授权以访问您的管理接口。
- 如果您没有堡垒主机，则应在允许管理员继续登录防火墙 Web 界面登录页面或 CLI 登录提示之前，使用带多重因素身份验证 (MFA) 的身份验证策略，要求管理员成功进行身份验证。这可以防止使用窃取凭据或通过漏洞利用访问管理接口。
- 需要限制登录的用户包括安全管理员、网络管理员或 IT 用户组，具体视您的组织而定。
- 如果必须启用对管理网络的远程访问，则需要使用 GlobalProtect 通过 VPN 隧道进行访问。管理员在 VPN 区域成功建立 VPN 隧道后，仍必须通过您的堡垒主机在管理网络中进行身份验证。
- 请勿在已配置 GlobalProtect 门户或网关的接口上使用允许 HTTP、HTTPS、Telnet 或 SSH 的接口管理配置文件，因为该配置暴露出可以从 Internet 访问管理接口。请勿在内部使用 HTTP 或 Telnet，因为这些协议以明文形式传输。
- 如果使用模板部署 VM 系列防火墙，且该防火墙包含用于限制管理访问特定 IP 地址的字段，应确保提供与专用管理 IP 地址或网络相对应的 CIDR 块。必要时，请在模板启动后修改相应的安全组，以添加其他主机或网络。不要将允许的源网络范围设置得比所需的大，并且不要将允许的源配置为 0.0.0.0/0。

## 使用服务路由访问外部服务

默认情况下，防火墙使用 DNS 服务器、NTP 服务器和身份验证服务器等管理 (MGT) 端口访问可能不被信任的网络上的管理网络之外的服务，包括需要互联网访问的服务，例如 Palo Alto Networks 服务和 AutoFocus。因为管理接口（无论是在 MGT 端口，还是在数据端口）必须在管理网络上进行隔离，您必须使用服务路由（**Device**（设备）> **Setup**（设置）> **Services**（服务）> **Service Route Configuration**（服务路由配置））来启用对这些服务的访问。配置服务路由时，相反地，防火墙会使用指定的源接口和地址访问需要的服务。在未启用管理访问（HTTPS 或 SSH）的接口上，为您的服务路由指定源 IP 地址/接口。



© 2019 Palo Alto Networks, Inc.

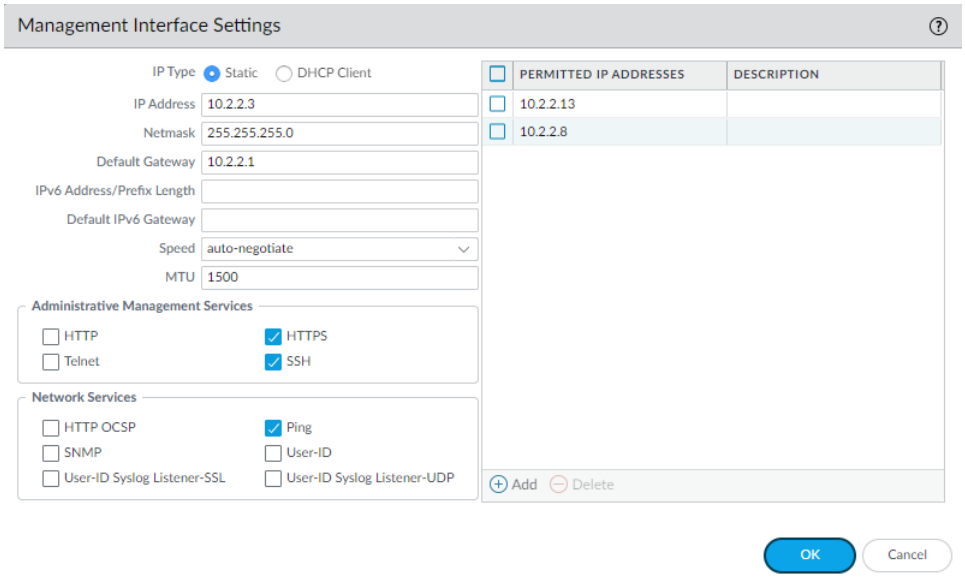



# 限制访问管理接口

- 限制允许访问该管理接口的 IP 地址。

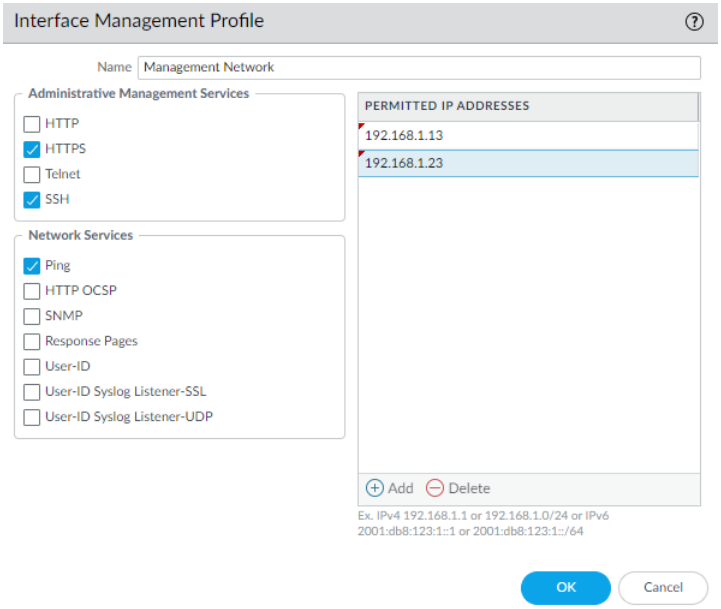
  即使您的防火墙位于仅通过相同 VLAN 上设备，或通过堡垒主机或 VPN 隧道进行访问的专用管理网络上，您可以通过将可以访问管理接口的源 IP 地址限制为您的管理员源 IP 地址，来进一步保护防火墙的安全。限制对管理接口的访问有助于防止从意外 IP 地址或子网的访问，或是使用盗窃凭据进行的访问，从而减少攻击面。
- 限制管理接口上可用的服务。
  - 请勿允许通过 Telnet 和 HTTP 进行访问，因为这些服务使用明文，不像其他服务一样安全，可能会泄露管理员凭据。相反，应要求管理员通过 SSH 或 HTTPS 访问防火墙接口。
  - 如果想要测试与接口的连接情况，启用 ping，但不得启用管理界面上的任何其他服务。
- 配置这些设置的方式取决于您是使用 MGT 端口，还是使用数据端口访问防火墙管理接口：
  - 如果使用 MGT 端口作为您的管理接口，请选择 **Device**（设备）> **Setup**（设置）> **Interfaces**（接口），然后选择 **Management**（管理）接口配置设置，以限制可以访问管理接口的人员以及接口允许的服务。


© 2019 Palo Alto Networks, Inc.




- 如果使用数据端口作为您的管理接口，请在配置完接口后，选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理），并 **Add**（添加）接口管理 配置文件 ，以限制可以访问管理接口的人员和接口允许的服务。

  请勿将允许 *Telnet*、*SSH*、*HTTP* 或 *HTTPS* 的接口管理配置文件附加到已配置 *GlobalProtect* 门户或网关的接口，因为这会将管理接口暴露给互联网。请勿对任何管理接口配置文件使用 *HTTP* 或 *Telnet*，因为这些协议以明文形式传输。




# 管理管理员访问权限

- 防火墙已预配置一个默认管理帐户 (admin)，该帐户具有对防火墙的完全读写权限（也称为超级用户权限）。必须在初始配置结束后立即更改默认管理员帐户密码（**Device**（设备）> **Administrators**（管理员）> **admin**（管理））。



© 2019 Palo Alto Networks, Inc.

如果合规、审核或安全要求规定，必须删除您设备中的默认管理帐户，您可以在创建至少一个其他超级用户管理帐户后进行删除。在设备上配置至少一个其他超级用户管理帐户之前，无法删除默认管理帐户。

- 请为需要访问防火墙管理或报告功能的每个用户配置防火墙管理员帐户。这样可以更好地保护防火墙防止未经授权即对其进行配置（或修改），并且可以记录每位管理员的操作。
- 为每个管理员帐户分配一个管理员角色配置文件，以限制管理权限至仅单个管理员所需的这些功能。
- 对于具有更改权限的管理员，必须使用外部身份验证进行 MFA，并通过 RADIUS 或 SAML 授权。有关如何使用 MFA 配置外部身份验证额详细信息，请参阅为防火墙管理员配置本地或外部身份验证。



如果您拥有使用智能卡的强大的身份验证基础架构，请配置基于证书的管理员 Web 界面身份验证和配置基于 SSH 密钥的管理员 CLI 身份验证。

如果可用，请使用特权帐户管理 *(PAM)* 和/或特权身份管理 *(PIM)* 解决方案，以从外部保护管理员凭据安全。

- 监控“系统”日志，识别任何管理员帐户上的异常帐户活动。例如，如果日志显示同一天某个特定时间内登录尝试过多或重复登录，则可能表示管理员帐户已受到影响。此外，培训所有管理员关于使用管理员登录活动指标检测帐户不当使用的内容。

## 创建强大的管理员密码

配置严格的密码策略，包括要求频繁更改密码（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Minimum Password Complexity**（最低密码复杂性））。

您负责对所在组织的相应密码要求进行评估；但是，创建强密码的最佳实践具有如下特征。密码应：

- 至少包含八个字符
- 不得基于词典中的单个单词
- 不得上下文相关词（例如，网站名称）
- 不得包含用户名或用户名派生词（例如，@dmin、Johnny）
- 不得使用重复或连续字符（例如，aaaaaa、1234abcd）
- 包含大小写字符、数字和特殊字符（包括空格）

一种创建强密码的方式是创建长密码短语，而不是使用复杂的密码。行业标准建议，使用包含词典单词在内的、您想要使用的任何字符创建独特且容易记住的长密码短语，而不是创建绕口复杂且容易忘记的密码。要想填补词典单词使用的空白，可以使用至少由 15 个字符组成的较长密码。尝试基于一种只有您知晓的、熟悉的长短语，或是通过将至少四个单词串在一起的方式创建密码短语。

更多有关如何为您的组织确定适当密码要求的信息，我们建议您使用以下资源：

- NIST SP 800-63B，数字身份准则
- NIST，轻松创建最佳 P@$5w0rd 的方法

## 扫描所有发往管理接口的流量



因为安全策略和解密策略无法评估管理层流量，因此不能直接扫描 *MGT* 端口以查找威胁。如果您使用 *MGT* 端口作为管理接口，请考虑通过数据端口或另一个防火墙路由发往 *MGT* 端口的流量，这样，您才有可能将这些重要的安全检查应用于流量管理。

- 创建安全策略规则，允许访问防火墙和 Panorama（Web 接口或 CLI）的管理接口。策略的定义取决于您是否使用堡垒主机来启用对管理网络的访问。
  - 如果您未使用堡垒主机来隔离管理网络，创建一个安全策略规则，允许从“用户”区到“IT 基础架构”区域的访问。此安全策略规则必须非常精细，并指定用户尝试访问管理接口的源区域、源 IP 地址（如有）和源用户组，以及目标区域、设备（防火墙或 Panorama）的 IP 地址、和用于识别应用程序默认端口上运行的指定管理应用程序（Web 接口或 CLI）的 App-ID。例如，您可以使用 panos-web-interface


© 2019 Palo Alto Networks, Inc.

App-ID 以允许访问 Web 接口和 ssh App-ID 以允许访问 CLI。此外，您还必须根据下节所述将“漏洞保护配置文件”附加到规则中。

在以下示例规则中，允许从用户区直接访问 IT 基础架构区，限制视图访问管理接口 IP 地址的 IT 管理员组中用户的访问至仅应用程序默认端口上 panos-web-interface 应用程序的访问：

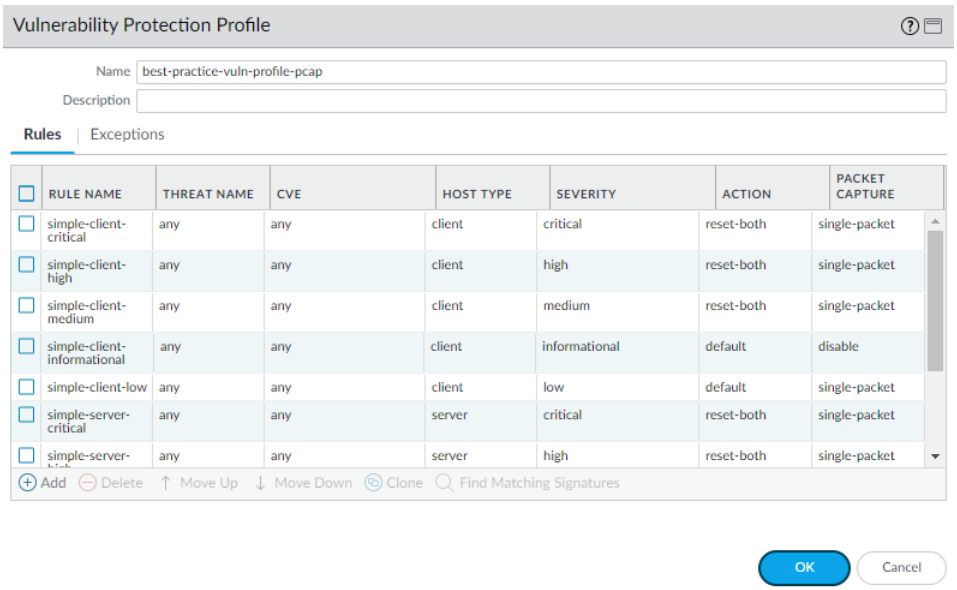
| | Source | | Destination | | | | |
|---|---|---|---|---|---|---|---|
| NAME | ZONE | USER | ZONE | APPLICATION | SERVICE | ACTION | PROFILE |
| FW-mgt | Users | IT-admins | IT-infrastruc... | panos-web-interface<br>ssh | application-default | Allow | |

- 如果您使用堡垒主机启用对管理网络的访问，则需要两个安全策略规则：一个规则用于允许从用户区到堡垒主机区的访问，另一个规则用于允许从堡垒主机区到 IT 基础架构区的访问。同样，这两个安全策略规则应尽可能精细化，且包含源区域、地址（如有）、用户和目标区域和地址、以及 App-ID。请记住，如果使用堡垒主机，则用户 IP 地址通常是堡垒主机的 IP 地址，这时，您不能识别管理员的用户 ID，除非您使用堡垒主机上的终端服务器代理来识别个人用户。在这种情况下，您还必须根据下节所述将“漏洞保护配置文件”附加到两个规则中。

  在随后的示例规则中，第一个规则允许试图通过 SSH 和/或 RDP 访问指定堡垒主机 IP 地址的 IT 管理员组中的用户从用户区访问堡垒主机区。第二个规则允许用户从堡垒主机区访问 IT 基础架构区，从而试图访问带指定目标地址的防火墙上默认端口上的 panos-web-interface 应用程序。

| | Source | | Destination | | | | |
|---|---|---|---|---|---|---|---|
| NAME | ZONE | USER | ZONE | APPLICATION | SERVICE | ACTION | PROFILE |
| Bastion-host-access | Users | IT-admins | Bastion-host | ms-rdp<br>ssh | application-default | Allow | |
| FW-mgt | Bastion-host | IT-admins | IT-infrastruc... | panos-web-interface<br>ssh | application-default | Allow | |

- ☐ 为允许访问您管理网络的安全策略附加漏洞保护配置文件的最佳实践，防止缓冲区溢出，不合法的代码执行，以及其他试图探测客户端和服务器端漏洞的行为。要创建用于保护管理接口的配置文件，请克隆严格的配置文件，然后启用扩展数据包捕获来帮助您跟踪任何潜在攻击源。




- ☐ 为进出管理接口的流量配置 SSL 入站检查或配置 SSL 转发代理，确保您能解密并扫描威胁流量。将解密配置文件的最佳实践附加到解密策略规则，确保您能阻止 TLS1.0 和 SSLv3 等易受攻击的 SSL/TLS 版本，并通过 RC4 和 3DES 等弱加密算法和 MD5 和 SHA1 等弱身份验证算法拒绝会话。



© 2019 Palo Alto Networks, Inc.

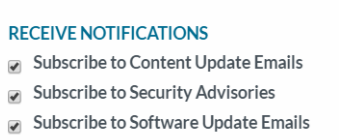
## 入站流量管理之证书替换

默认情况下，防火墙包含启用 HTTPS 通过管理 (MGT) 界面或任何其他支持 HTTPS 管理流量的界面来访问 Web 界面权限的默认证书。要提高入站管理流量的安全性，您需要将默认证书替换为向您组织专门发放的新证书。使用企业 CA 签名的证书，使用户将不再忽略证书警告。此外，在 SSL/TLS 配置文件中，设置 **Min version**（最低版本）为 **TLSv1.2** 以使用最强协议，并设置 **Max version**（最高版本）为**Max**（最高），从而可以在更强版本可用时使用最强协议。

## 使内容和软件更新保持最新

内容和软件更新保持最新，确保您始终受到最新安全修补程序和威胁更新的保护。

- 要始终收到最新更新和安全通知警报，请转至 Palo Alto Networks 支持门户，选择 **Edit Profile**（编辑配置文件）、**Subscribe to Content Update Emails**（订阅内容更新电子邮件）、**Subscribe to Security Advisories**（订阅安全通知）和 **Subscribe to Software Update Emails**（订阅软件更新电子邮件）。必须 **Save Edits**（保存编辑）。




- 更新至最新内容版本时，请遵循应用程序和威胁内容更新的最佳实践。
- 升级 PAN-OS 前，请阅读最新的发布说明。


© 2019 Palo Alto Networks, Inc.

# 订阅

了解可配合防火墙使用的所有订阅和服务，并通过激活订阅许可证开始：

- 您可配合防火墙使用的订阅
- 激活订阅许可证
- 许可证到期后会发生什么？
- 增强 Palo Alto Networks 云服务的应用日志



特定云服务（例如 *Cortex XDR*™）不会与防火墙直接集成，而是依靠 *Cortex* 数据湖上存储的数据查看网络活动。增强应用程序日志记录是 *Cortex* 数据湖订阅附带的功能，它允许防火墙专门收集 *Cortex XDR* 的数据，以用于检测异常网络活动。*Cortex XDR* 最佳实践是打开增强应用程序日志记录。

# 您可配合防火墙使用的订阅

通过下列 Palo Alto Networks 订阅，可以解锁防火墙某些功能，或使防火墙利用 Palo Alto Networks 云提供的服务（或两者）。您可以在此了解更多有关需要订阅才能与防火墙一起使用的每个服务或功能。要启用订阅，首先必须激活订阅许可证；一旦激活，大多数订阅服务都可使用动态内容更新，从而为防火墙提供新的和更新过的功能。

| 您可配合防火墙使用的订阅 | |
|---|---|
| **IoT Security** | IoT Security 解决方案与下一代防火墙一起使用，以动态发现并维护网络上 IoT 设备的实时库存。IoT Security 解决方案采用 AI 和机器学习算法，可实现较高的准确性，甚至可对首次遇到的 IoT 设备类型进行分类。由于 IoT 设备库存将动态变化，因此，可始终保持最新状态。此外，IoT Security 还能自动生成用于控制 IoT 设备流量的策略建议，自动创建用于防火墙策略的 IoT 设备属性。<br>• IoT Security 入门。 |
| **SD-WAN** | 提供的智能和动态路径选择基于 PAN-OS 软件已交付的行业领先安全性。SD-WAN 受 Panorama 管理，实施内容包括：<br>• 集中配置管理<br>• 自动创建 VPN 拓扑结构<br>• 流量分发<br>• 监控和故障排除<br>• SD-WAN 入门 |
| 威胁防护 | 威胁防护可提供：<br>• 防病毒、防间谍软件（命令和控制）以及漏洞保护。<br>• 内置外部动态列表，可用于保护您的网络免遭恶意主机的攻击。<br>• 确定受感染主机 的能力，这些主机尝试连接到恶意域。<br>• 威胁防护入门 |
| **DNS 安全** | 通过查询 DNS 安全（一种可扩展的基于云的服务，能够通过使用高级预测分析和机器学习生成 DNS 签名）提供增强的 DNS sinkholing。此服务提供对基于 DNS 的威胁情报（由 Palo Alto Networks 生成并将持续扩展）的完全访问权限。<br>要设置 DNS 安全，首先必须购买并安装威胁防护许可证。<br>• DNS 安全入门 |
| **URL 筛选** | 不仅可以控制 Web 访问，还可以根据动态 URL 类别确定用户与在线内容的交互方式。此外，通过控制用户可提交其公司凭据的站点，还可防止凭据被盗。<br>要设置 URL 筛选，必须购买和安装一个受支持的 URL 筛选数据库 PAN-DB 订阅。使用 PAN-DB，可以设置对 PAN-DB 公共云或 PAN-DB 私有云的访问。<br>• URL 筛选入门 |



© 2019 Palo Alto Networks, Inc.

| 您可配合防火墙使用的订阅 | |
|---|---|
| **WildFire** | 尽管在威胁阻止许可证中包含了基本 WildFire® 支持，但是 WildFire 订阅服务可以为需要即时阻止威胁的组织提供增强服务，频繁 WildFire 签名更新，发送高级文件类型（APK、PDF、Microsoft Office 和 Java Applet）以及使用 WildFire API 上传文件的功能。如果防火墙要发送文件到预置型 WF-500 设备，也需要购买 WildFire 订阅服务。<br>• WildFire 入门 |
| **AutoFocus** | 提供对防火墙流量日志的图形分析并通过 AutoFocus 门户的威胁情报识别潜在网络风险。通过有效许可证，您还可根据防火墙记录的日志打开 AutoFocus 搜索。<br>• AutoFocus 入门 |
| **Cortex Data Lake Cortex** 数据湖 | 提供基于云的集中式日志储存和聚合。必须或强烈建议使用 Cortex 数据湖，以支持其他几种通过云提供的服务，包括 Cortex XDR、IoT Security、Prisma Access 和 Traps 管理服务。<br>• Cortex 数据湖入门 |
| **GlobalProtect** | 提供移动解决方案和/或大范围 VPN 功能。默认情况下，无需许可证便可部署多个 GlobalProtect 门户和网关（无需进行 HIP 检查）。如果要使用高级 GlobalProtect 功能（HIP 检查和相关内容更新、GlobalProtect 移动应用程序、IPv6 连接或 GlobalProtect 无客户端 VPN），则需要为每个网关提供 GlobalProtect 许可证（订阅）。<br>• GlobalProtect 入门 |
| 虚拟系统 | 这是一种永久许可证，需要使用此许可证来启用对 PA-3200 系列防火墙上多个虚拟系统的支持。另外，如果要将虚拟系统数增加到超出在 PA-5200 系列和 PA-7000 系列防火墙上默认提供的基数（基数因平台不同而异），则必须购买虚拟系统许可证。PA-800 系列、PA-220 和 VM 系列防火墙不支持虚拟系统。<br>• 虚拟系统入门 |
| **Enterprise Data Loss Prevention (DLP)**（企业数据丢失防护 **(DLP)**） | 提供基于云的保护，防止未经授权访问、滥用、提取和共享敏感信息。企业 DLP 通过基于机器学习的数据分类，采用单个引擎实现静态和动态敏感数据的准确检测和一致的策略实施；通过正则表达式或关键字实现数百种数据模式的准确检测和一致的策略实施；以及通过布尔逻辑扫描集合类数据实现数据配置文件的准确检测和一致的策略实施。<br>• 企业数据丢失防护入门 |


© 2019 Palo Alto Networks, Inc.

# 激活订阅许可证

按照下列步骤，在防火墙上激活新的许可证。

某些加密功能，如解密镜像和解密代理要求您激活免费的许可证以解锁功能。对于这些功能，您应按照下列步骤以 激活免费许可证以使用解密功能。

STEP 1 | 找到您购买的许可证对应的激活代码。

购买订阅服务时，必须已收到 Palo Alto Networks 客户服务部门发送来一封列明了每个订阅服务相关的激活代码的电子邮件。如果找不到这封电子邮件，请联系客户支持部门以获取激活代码，然后再继续操作。

STEP 2 | 激活支持许可证。

如果您不具备有效的支持许可证，将无法更新 PAN-OS 软件。

1. 登录至 Web 界面，然后选择**Device**（设备）> **Support**（支持）。
2. 单击 **Activate support using authorization code**（使用授权代码激活支持）。
3. 输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。

STEP 3 | 激活购买的每个许可证。

选择 **Device**（设备）> **Licenses**（许可证），然后使用以下方式之一激活许可证及订阅：

- **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）— 如果您已在客户支持门户上激活您的许可证，则使用此选项。
- **Activate feature using authorization code**（使用授权代码激活功能）— 使用此选项，可使用以前尚未在支持门户上激活的许可证授权代码启用购买的订阅服务。系统提示时，输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。
- **Manually upload license key**（手动上载许可证密钥）— 如果您的防火墙无法连接到 Palo Alto Networks 客户支持门户，请使用此选项。在此情况下，必须在具有 Internet 连接的计算机上从支持站点下载许可证密钥文件，然后上载到该防火墙。

STEP 4 | 验证是否已成功激活许可证

在 **Device**（设备）> **Licenses**（许可证）页面上，验证是否已成功激活许可证。例如，在激活 WildFire 许可证后，应该会看到该许可证有效：




STEP 5 | （仅 WildFire 订阅）执行提交以完成 WildFire 订阅激活。

激活 WildFire 订阅后，防火墙需要进行提交以开始转发高级文件类型。您应当：

- 提交任何暂挂的更改。
- 检查 WildFire 分析配置文件规则是否包括 WildFire 订阅现在支持的高级文件类型。如果不需要对任何规则进行更改，请对规则说明进行小幅修改并执行提交。



© 2019 Palo Alto Networks, Inc.

# 许可证到期后会发生什么？

Palo Alto Networks 订阅为防火墙提供附加功能和/或访问 Palo Alto Networks 云交付设备的权限。许可证过期后，一些订阅仍继续以有限容量运行，而另一些则完全停止运行。下面介绍了每个订阅到期后会发生的事件。

| 订阅 | 到期行为 |
| --- | --- |
| 威胁防护 | 系统日志中出现警报，指示许可证已到期。<br>您仍能：<br>• 除非您已手动安装或是作为自动安排的一部分安装有一个仅适用于应用程序的新内容更新，否则，请使用在许可证到期时安装的签名。如果这样操作，更新将删除您现有的威胁签名，且您将再也无法获得对这些签名的保护。<br>• 使用并修改自定义 App-ID™ 和威胁签名。<br>您再也不能：<br>• 安装新签名。<br>• 将签名滚回到先前版本。 |
| DNS 安全 | 您仍能：<br>• 使用本地 DNS 签名，前提是您拥有有效的威胁防护许可证。<br>您再也不能：<br>• 获取新的 DNS 签名。 |
| URL 筛选 | 您仍能：<br>• 使用自定义 URL 类别实施策略。<br>• 使用许可证到期时已保存在本地缓存中的 PAN-DB 类别实施策略。<br>您再也不能：<br>• 获取缓存的 PAN-DB 类别更新。<br>• 获取未缓存的 URL 的 PAN-DB 类别。 |
| WildFire | 您仍能：<br>• 转发 PE 进行分析。<br>• 每隔 24-48 小时获取签名更新一次，前提是您拥有有效的威胁防护订阅。<br>您再也不能：<br>• 通过 WildFire 公共云和私有云每隔 5 分钟获取更新一次。<br>• 转发 APK、Flash 文件、PDF、Microsoft Office 文件、Java Applets、Java 文件（.jar 和 .class）以及 SMTP 和 POP3 电子邮件消息中包含的 HTTP/HTTPS 电子邮件链接等高级文件类型。<br>• 使用 WildFire API。<br>• 使用 WildFire 设备托管 WildFire 私有云或 WildFire 混合云。 |
| AutoFocus | 您仍能： |



© 2019 Palo Alto Networks, Inc.

| 订阅 | 到期行为 |
| --- | --- |
| | • 在三个月宽限期内将外部动态列表与 AutoFocus 数据一起使用。<br>您再也不能：<br>• 访问 AutoFocus 门户。<br>• 查看 AutoFocus 情报摘要以监控日志或 ACC 构件。 |
| Cortex Data Lake（Cortex 数据湖） | 您仍能：<br>• 在日志数据被删除后拥有 30 天的宽限期保存此数据。<br>• 在 30 天宽限期结束后转发日志到 Cortex 数据湖。 |
| GlobalProtect | 您仍能：<br>• 使用适用于运行 Windows 和 macOS 的端点的应用程序。<br>• 配置单个或多个内部/外部网关。<br>您再也不能：<br>• 访问适用于运行 iOS、Android、Chrome OS 和 Windows 10 UWP 的 Linux OS 应用程序和移动应用程序。<br>• 使用适用于外部网关的 IPv6。<br>• 运行 HIP 检查。<br>• 使用 无客户端 VPN。<br>• 启用拆分隧道。 |
| VM-SERIES | 您仍能：<br>• 配置和使用您在许可证到期时已配置的防火墙。 |
| 支持 | 您再也不能：<br>• 接收软件更新。<br>• 下载 VM 映像。<br>• 受益于技术支持。 |


© 2019 Palo Alto Networks, Inc.

# 增强 Palo Alto Networks 云服务的应用日志

防火墙可收集提高 Palo Alto Networks 应用程序和服务（例如，Cortex XDR）的网络活动可见性的数据。这些增强应用程序日志应严格用于 Palo Alto Networks 应用程序和服务的使用与处理；您无法在防火墙或 Panorama 上查看增强应用程序日志。只有将日志发送到 Cortex 数据湖的防火墙才能生成增强应用程序日志。

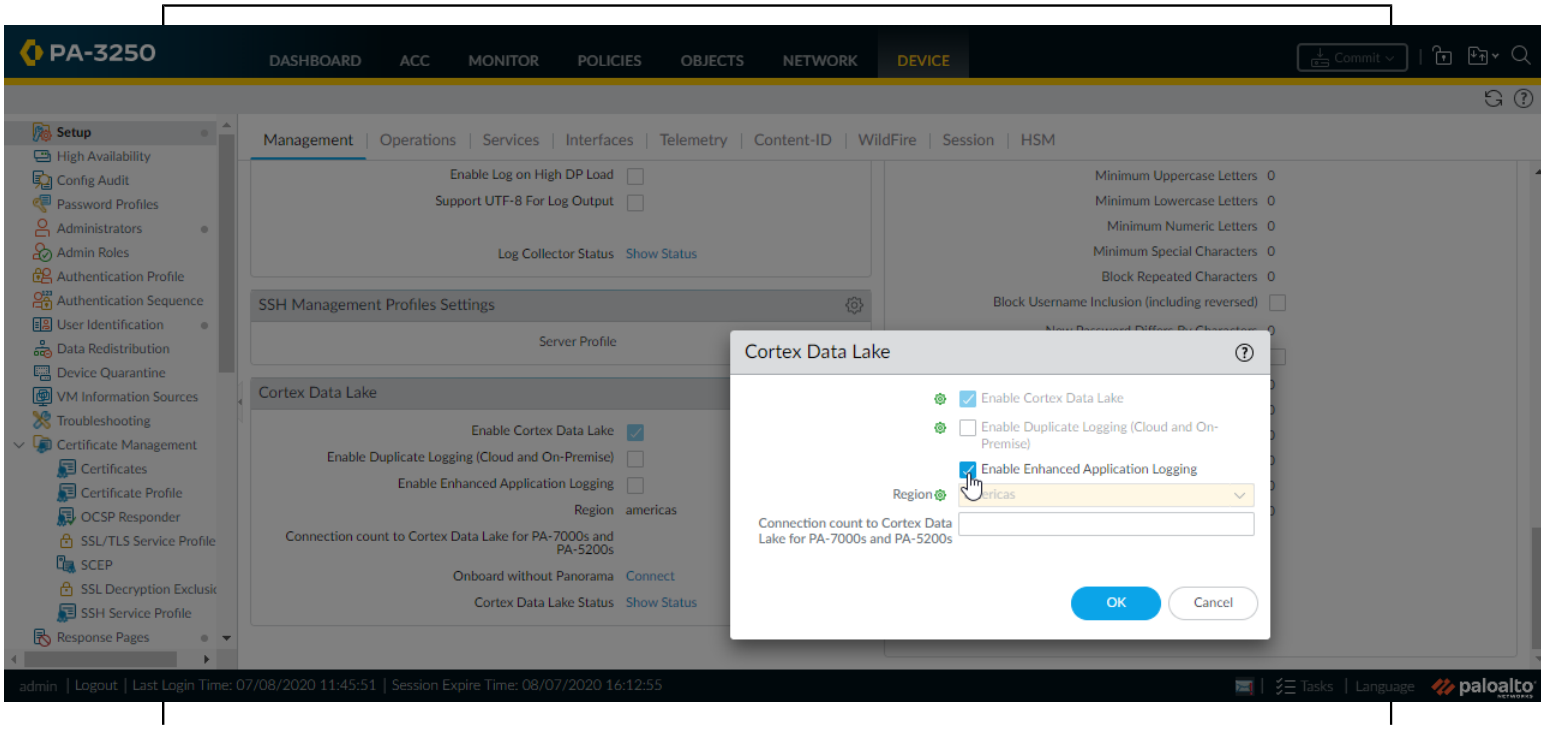
增强应用程序日志收集的数据类型示例包括 DNS 查询记录、以及用于指定访问 URL 和 DHCP 自动 IP 地址分配相关消息的 Web 浏览器或工具的 HTTP 标头用户代理字段。例如，借助于 DHCP 信息，Cortex XDR™ 就能根据主机名（而非 IP 地址）警告异常活动。这让安全分析师可以使用 Cortex XDR 有意义地评估用户活动是否位于其角色范围内，如果不在范围内，则应更快地采取行动阻止该活动。

要从最全面的增强应用程序日志集受益，还应启用 User-ID；基于 Windows 的 User-ID 代理和 PAN-OS 集成 User-ID 代理部署均收集一些未在防火墙 User-ID 日志中反映出、但却有助于将相关网络活动与特定用户相关联的数据。

要开始将增强应用程序日志转发至 Cortex 数据湖，请全局打开增强应用程序日志记录，然后基于每条安全规则进行启用（使用日志转发配置文件）。必须提供全局设置，以捕获非基于会话（例如，ARP 请求）的流量数据。强烈建议使用每安全策略规则。大部分增强应用程序日志从基于会话的流量中收集，而该流量由您的安全策略规则实施。

STEP 1 | 增强应用程序日志记录需要订阅 Cortex 数据湖，还建议使用 User-ID。以下是 Cortex 数据湖入门和启用 User-ID 的步骤。

STEP 2 | 要在防火墙上 **Enable Enhanced Application Logging**（启用增强应用程序日志记录），请选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Cortex Data Lak**（**Cortex** 数据湖），然后编辑 Cortex 数据湖设置。



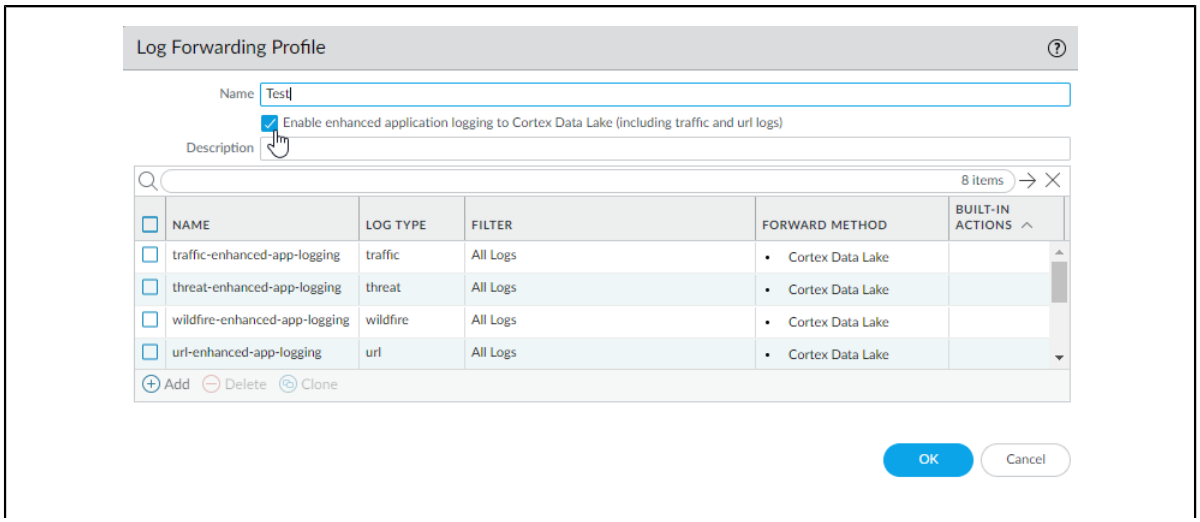

STEP 3 | 继续启用增强应用程序日志记录，以用于将流量控制到您希望扩展可见性的安全策略规则。

1. 选择 **Objects**（对象）> **Log Forwarding**（日志转发）并 **Add**（添加）或修改日志转发配置文件。



© 2019 Palo Alto Networks, Inc.

2. 更新配置文件以 **Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)**（启用对 **Cortex** 数据湖的增强型应用程序日志记录（包括流量和 **url** 日志）。




请注意，在日志转发配置文件中启用增强应用程序日志记录时，用于指定增强应用程序日志记录所需的日志类型的匹配列表将被自动添加到配置文件中。

3. 单击 **OK**（确定）以保存配置文件，并按需更新尽可能多的配置文件。
4. 必须将已更新的日志转发配置文件附加到安全策略规则，以触发与规则匹配的流量日志生成和转发。
   1. 选择 **Policies**（策略）> **Security**（安全）以查看已附加到每个安全策略规则的配置文件。
   2. 要更新已附加到规则的日志转发配置文件，请 **Add**（添加）或编辑规则，选择 **Policies**（策略）> **Security**（安全）> **Actions**（操作）> **Log Forwarding**（日志转发），然后选择与增强应用程序日志记录一起启用的日志转发配置文件。

# 软件和内容更新

PAN-OS 是运行所有 Palo Alto Networks 次世代防火墙的软件。Palo Alto Networks 也会频繁发布更新，为防火墙带来最新的安全功能。防火墙可实施基于内容更新提供的应用程序和威胁签名（等）策略，而无需更新防火墙配置。

成功下载并将 PAN-OS 软件更新安装到物理防火墙上后，一旦该物理防火墙作为软件安装流程的一部分重新启动后，即会验证该软件更新，以确保 PAN-OS 软件的完整性。这样可确保新运行的软件更新是已知良好的，且防火墙不会因远程或物理漏洞利用而受到威胁。

- PAN-OS 软件更新
- 动态内容更新
- 安装内容更新
- 应用程序和威胁内容更新
- 应用程序和威胁内容更新的最佳实践
- 内容交付网络基础架构

# PAN-OS 软件更新

PAN-OS 是运行所有 Palo Alto Networks 次世代防火墙的软件。防火墙运行的 PAN-OS 软件版本显示于防火墙 **Dashboard**（仪表板）上。

您可以在防火墙上直接检查是否有新的 PAN-OS 发布版本，或在 Palo Alto Networks 支持门户网站上查看。要将防火墙升级至 PAN-OS 的最新版本：

STEP 1 | 查看最新 PAN-OS 发行说明以了解有哪些新内容。还可以查看 PAN-OS 升级/降级注意事项以确保您了解所有 PAN-OS 发行版本可能带来的潜在更改。

STEP 2 | 检查是否有新的 PAN-OS 发行版本：

- **On the firewall**（在防火墙上）—选择 **Device**（设备）> **Software**（软件）和 **Check Now**（立即检查），让防火墙检查 Palo Alto Networks 升级服务器，查看是否有新的 PAN-OS 发行版本。
- **On the support portal**（在支持门户网站上）—前往 support.paloaltonetworks.com，然后在左边的菜单栏选择 **Updates**（更新）> **Software Updates**（软件更新）。下载并保存您想要用于升级防火墙的版本。

STEP 3 | 一旦您决定了您需要的发行版本，遵循完整的工作流程以 升级防火墙至新的 PAN-OS 版本。您将要采取的步骤可能取决于您当前运行的发行版本，您是否在使用 HA，以及您是否在通过 Panorama 管理防火墙。



© 2019 Palo Alto Networks, Inc.

# 动态内容更新

Palo Alto Networks 会经常发布防火墙可用于实施安全策略的更新，无需升级 PAN-OS 软件或更改防火墙配置。通过这些更新，防火墙可配备最新安全功能和威胁情报。

除任何防火墙都可以检索到的应用程序更新和一些防病毒更新外，根据订阅，您还可以使用动态内容更新。您可以为每个动态内容更新设置一个时间表，以定义防火墙检查、下载或安装新更新的频率（**Device**（设备）> **Dynamic Updates**（动态更新））。

| 动态内容更新 | 这个包里有什么？ |
| --- | --- |
| 反病毒 | 防病毒更新每 24 小时发布一次，包括：<br>• 用于新发现恶意软件的 WildFire 签名。要想每隔五分钟（而非每天）获取一次这些更新，您需要 WildFire 订阅。<br>• （需要威胁防护）自动生成的命令和控制 (C2) 签名，可检测 C2 流量中的某些模式。即使是 C2 主机未知或变化迅速，防火墙也能通过这些签名检测到 C2 活动。<br>• （需要威胁防护）用于内置外部动态列表的新的、经过更新的列表条目。这些列表包括恶意 IP 地址、高风险 IP 地址、防弹主机提供的 IP 地址，有助于保护您免遭恶意主机的攻击。<br>• （需要威胁防护）本地 DNS 签名集更新，可供防火墙用于标识已知的恶意域。如果已设置DNS sinkholing，则防火墙可以标识网络上尝试连接这些域的主机。要允许防火墙根据完整的 DNS 签名数据库检查域，请设置DNS 安全。 |
| 应用程序 | 应用程序更新可提供新建和修改过的应用程序签名，或 App-ID。此更新不需要任何额外订阅，但一定需要具备有效的维护/支持合约。新的应用程序更新仅在每月的第三个星期二发布，以便您可以提前做好任何必要的策略更新准备；App-ID 修改发布得更频繁。当新建和修改过的 App-ID 使防火墙能够以越来越高地精度执行您的安全策略时，发生的安全策略更改可能会影响应用程序的可用性。要充分利用应用程序更新，请遵照我们的提示以管理新建和修改过的 App-ID。 |
| 应用程序和威胁 | 包括新的和更新的应用程序和威胁签名。如果您已订阅威胁防护，则可以获得此更新（在这种情况下，您将获得此更新，而不是应用程序更新）。新的威胁更新会经常发布，有时每周发布几次，并附带更新的 App-ID。新建 App-ID 仅在每月的第三个星期二发布。防火墙仅需 30 分钟即可检索到最新威胁和应用程序更新。<br>有关如何最好启用应用程序和威胁更新以确保应用程序可用性，并防止最新威胁的指导，请查看应用程序和威胁内容更新的最佳实践。 |
| **GlobalProtect** 数据文件 | 包括供应商特定信息，用于定义和评估 GlobalProtect 应用程序返回的主机信息配置文件 (HIP) 数据。您必须订阅 GlobalProtect 网关才能获取这些更新。此外，您必须在 GlobalProtect 运行前为这些更新创建一个计划表。 |
| **GlobalProtect** 无客户端 **VPN** | 包含新的和更新的应用程序签名，使得无客户端 VPN 能够访问 GlobalProtect 门户的常见 Web 应用程序。您必须订阅 GlobalProtect 才能获取这些更新。此外，您必须在 GlobalProtect 无客户端 VPN 运行前为这些更新创建一个计划表。建议的最佳实践是始终为 GlobalProtect 无客户端 VPN 安装最新内容更新。 |
| **WildFire** | 提供实时访问 WildFire 公共云所生成的恶意软件和防病毒签名的权限。或者，您可以配置 PAN-OS 来检索 WildFire 签名更新包。您可以将防火墙设为每分钟检查一次新的更新，确保防火墙能够在一分钟内检索到最新 WildFire 签名。若未订阅 WildFire，您必须至少等待 24 小时才能获得防病毒更新中提供的签名。 |



© 2019 Palo Alto Networks, Inc.

| 动态内容更新 | 这个包里有什么？ |
| --- | --- |
| **WF** - 私有 | 由于 WildFire 设备执行了分析，从而能几乎实时地提供已创建的恶意软件和防病毒签名。要从 WildFire 设备获取内容更新，防火墙和设备必须同时运行 PAN-OS 6.1 或更高版本，且防火墙必须配置为可以转发文件和电子邮件链接到 WildFire 私有云。 |



© 2019 Palo Alto Networks, Inc.

# 安装内容更新

为了确保您始终不会受到最新威胁（包括尚未发现的威胁）的攻击，您必须确保防火墙始终具有 Palo Alto Networks 发布的最新更新内容及软件。您可用的动态内容更新取决于您拥有的订阅 。

按照以下步骤安装内容更新。此外，您还可以设置内容更新计划，以定义防火墙检索和安装更新的频率。

与其他更新类型相比，应用程序和威胁内容更新的工作方式略有不同 — 要充分利用最新应用程序知识和威胁防护措施，并根据指南以部署应用程序和威胁内容更新，而不是此处所述的步骤。

STEP 1 | 确保防火墙具备防火墙服务器访问权限。

1. 默认情况下，防火墙在 **updates.paloaltonetworks.com** 访问 **Update Server**（更新服务器），以便防火墙从适用于动态更新的内容交付网络基础架构中与其最接近的服务器接收内容更新。如果防火墙对互联网的访问受限，请将更新服务器地址设置为使用主机名 **staticupdates.paloaltonetworks.com**，而非从 CDN 架构中动态选择服务器。
2. （可选）单击 **Verify Update Server Identity**（确认更新服务器身份）进行额外验证，从而启用防火墙检查服务器的 SSL 证书是否由授信机构颁发。默认启用此选项。
3. （可选）如果防火墙需要使用代理服务器才能访问 Palo Alto Networks 更新服务，则请在 **Proxy Server**（代理服务器）窗口中输入：
   - **Server**（服务器）— 代理服务器的 IP 地址或主机名。
   - **Port**（端口）— 代理服务器的端口。范围：1-65535。
   - **User**（用户）— 用于访问此服务器的用户名。
   - **Password**（密码）— 用户用以访问该代理服务器的密码。在 **Confirm Password**（确认密码）中重新输入此密码。
4. （可选）连接失败时，最多可以配置 3 次重新连接尝试。使用 **debug set-content-download-retry attempts** 设置连接尝试次数。默认值为 0。

STEP 2 | 检查最新内容更新。

选择 **Device**（设备）> **Dynamic Updates**（动态更新）并单击 **Check Now**（立即检查）（位于窗口的左下角）以检查最新更新。**Action**（操作）列中的链接指示是否有更新可用：

- **Download**（下载）— 指示有新更新文件可用。单击该链接便可以开始将文件直接下载到防火墙。成功下载后，**Action**（操作）列中的链接将从**Download**（下载）更改为**Install**（安装）。




在安装应用程序和威胁更新之前，无法下载防病毒更新。

- **Revert**（还原）— 指示之前安装的内容版本或软件版本可用。您可以选择还原到之前安装的版本。

STEP 3 | 安装内容更新。

在 *PA-220* 防火墙上，最长需要 *10* 分钟来完成安装，而在 *PA-5200* 系列、*PA-7000* 系列或 *VM* 系列防火墙上，最长仅需两分钟即可完成。

单击 **Install**（安装）连接中的 **Action**（操作）列。安装完成时，将在 **Currently Installed**（当前已安装）列中显示复选标记。






© 2019 Palo Alto Networks, Inc.

STEP 4 | 调度每项内容更新。

为您要计划的每项更新重复执行此步骤。

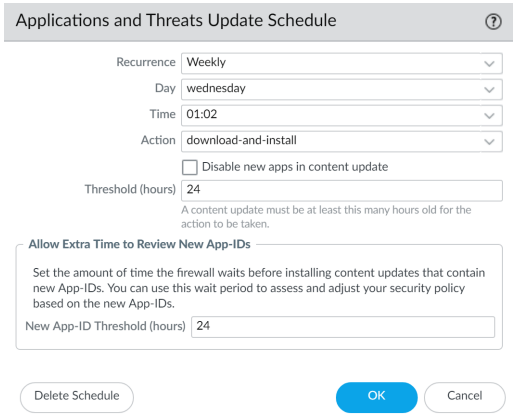
交错执行更新计划，因为防火墙每次只能下载一项更新。如果您计划以相同时间间隔下载这些更新，则只有第一项下载会成功。

1. 通过单击 **None**（无）链接设置每个更新类型的计划。




2. 通过从 **Recurrence**（重复）下拉列表中选择值来指定希望更新发生的频率。根据内容类型的不同，可用值会发生变化（WildFire 更新具有**Real-time**（实时）、**Every Minute**（每分钟）、**Every 15 Minutes**（每 15 分钟）、**Every 30 minutes**（每 30 分钟）或 **Every Hour**（每小时）选项，而应用程序及威胁更新可计划为 **Weekly**（每周）、**Daily**（每天）、**Hourly**（每小时）或 **Every 30 Minutes**（每 30 分钟），防病毒更新可计划为**Hourly**（每小时）、**Daily**（每天）或 **Weekly**（每周））。
3. 指定 **Time**（时间）（如果是 WildFire，则指定每小时后的分钟数），并且在适用情况下，根据选择的 **Recurrence**（重复）值指定希望更新发生在 **Day**（星期几）。
4. 指定是希望系统 **Download Only**（仅下载），还是 **Download And Install**（下载和安装）（最佳实践）更新。
5. 在 **Threshold (Hours)**（阈值（小时））字段输入发布后执行内容更新的等待时间。在极少数情况下，可能会发现内容更新中存在错误。为此，您可能希望延迟安装新更新，直到更新已经发布一定的时间后才安装。

   如果您的关键任务应用程序必须 *100#* 可用，请将“应用程序”或“应用程序和威胁”更新的阈值设置为至少 *24* 小时或更长时间，并遵循应用程序和威胁内容更新的最佳实践。此外，虽然计划内容更新是一次性或不常发生的任务，计划设置完毕后，您将需要继续管理新建和修改过的 App-ID（均包含在内容发布中），因为这些 *App-ID* 可以改变安全策略实施的方式。
6. （可选）输入 **New App-ID Thresholds**（新的 **App-ID** 阈值）（以小时为单位），以设置防火墙在安装包含新 App-ID 的内容更新之前等待的时间。




7. 单击 **OK**（确定）以保存计划设置。
8. 单击**Commit**（提交）以将设置保存到正在运行的配置中。

STEP 5 | 更新 PAN-OS。

始终在更新 *PAN-OS* 前更新内容。所有 *PAN-OS* 版本均具备最低支持内容发行版本。



© 2019 Palo Alto Networks, Inc.

1. 审核发行说明。
2. 更新 PAN-OS 软件。


© 2019 Palo Alto Networks, Inc.

# 应用程序和威胁内容更新

应用程序和威胁内容更新可为防火墙提供最新的应用程序和威胁签名。包内应用程序部分包括新的和修改过的 App-ID，无需许可证。完整的“应用程序和威胁”内容包也包含新的和修改过的威胁签名，需要“威胁防护”许可证。由于防火墙会根据自定义设置自动检索并安装最新的应用程序和威胁签名，因此可以基于最新的 App-ID 和威胁防护执行安全策略，无需任何其他配置。

新的和修改过的威胁签名以及修改过的 App-ID 应至少每周发布一次，通常频率应该更高。新 App-ID 在每个月的第三个星期二发布。由于新的 App-ID 可以更改安全策略实施流量的方式，因此更有限的 App-ID 新版本旨在为您提供可预测窗口，以准备和更新安全策略。此外，内容更新应是累积式的，即，最新内容更新应始终包含先前版本中发布的应用程序和威胁签名。

由于应用程序和威胁签名通过单个包提供（相同的解码器使应用程序签名能够识别应用程序，同时也使威胁签名能够检查流量），您需要考虑是否要一起或单独部署签名。您选择部署内容更新的方式取决于组织的网络安全和应用程序的可用性要求。首先，将您的组织标识为具有以下状态之一（或者两者都有，具体取决于防火墙的位置）：

- 奉行安全第一的组织会优先考虑使用最新威胁签名来进行防护，而非应用程序的可用性。您主要将防火墙用于实现威胁防护功能。其次，对影响安全策略实施应用程序流量的方式的 App-ID 做出的任何更改。
- 任务关键型网络优先考虑应用程序的可用性，而非使用最新威胁签名来进行防护。您的网络绝不容忍停机。防火墙在线部署以实施安全策略。如果您在安全策略中使用 App-ID，则引入任何影响 App-ID 的内容版本的更改都可能会导致停机。

您可以采取任务关键型或安全第一的方式来部署内容更新，或可以将这两种方法相结合来满足业务需求。查看并考虑 应用程序和威胁内容更新的最佳实践以决定您想要如何实施应用程序和威胁更新。然后：

- ❑ 部署应用程序和威胁内容更新。
- ❑ 遵守我们的 内容更新提示。



虽然计划内容更新是一次性或不常发生的任务，计划设置完毕后，您将需要继续管理新建和修改过的 App-ID（均包含在内容发布中），因为这些 *App-ID* 可以改变安全策略实施的方式。

## 部署应用程序和威胁内容更新

在采取步骤布置应用程序和威胁内容更新之前，请了解应用程序和威胁内容更新的工作原理，并确定想要如何实现应用程序和威胁内容更新的最佳实践。

此外，Panorama 可以让您能轻松快速地部署内容更新到防火墙。如果使用 Panorama 管理防火墙，请遵循部署内容更新的这些步骤，而不是下面的步骤。

STEP 1 | 要解锁完整的“应用程序和威胁”内容数据包，请获取“威胁防护”许可证，并在防火墙上激活许可证。

1. 选择**Device**（设备）> **Licenses**（许可证）。
2. 手动上传许可证密钥，或从 Palo Alto Networks 许可证服务器检索密钥。
3. 检验“威胁防护”许可证是否激活。

STEP 2 | 设置防火墙计划，以检索和安装内容更新。

完成以下步骤后，请务必考虑您的组织是任务关键型或安全第一型组织（或是两者兼而有之），并查看应用程序和威胁内容更新的最佳实践。

1. 选择**Device**（设备）> **Dynamic Updates**（动态更新）。
2. 选择“应用程序和威胁”内容更新 **Schedule**（计划）。
3. 设置防火墙检查 Palo Alto Networks 更新服务器新“应用程序和威胁”内容发布的频率（**Recurrence**（重复周期）），以及 **Day**（日期）和 **Time**（时间）。



© 2019 Palo Alto Networks, Inc.

4. 设置防火墙在发现和检索新内容发布时执行的 **Action**（操作）。
5. 设置内容发布的安装 **Threshold**（阈值）。在防火墙可以检索发布并执行在上一步配置的“操作”之前，Palo Alto Networks 更新服务器上的内容发布必须至少在这段时间内可用。
6. 如果使用任务关键型网络，即您对应用程序停机时间零容忍（应用程序的可用性甚至等同于最新威胁防护），则可以设置 **New App-ID Threshold**（新建 **App-ID** 阈值）。仅在新建 App-ID 在这段时间已可用之后，防火墙方检索包含这些新建 App-ID 的内容更新。
7. 单击 **OK**（确定）以保存“应用程序和威胁”内容更新计划，并 **Commit**（提交）。

STEP 3 | 设置日志转发，将 Palo Alto Networks 关键内容警告发送给您用于监控网络和防火墙活动的外部服务。为此，可以确保相应人员收到有关关键内容问题的通知，以便按需采取行动。关键内容警告将记录为带有以下“类型”和“事件”的系统日志条目：(subtype eq content) 及 (eventid eq palo-alto-networks-message)。

STEP 4 | 虽然计划内容更新是一次性或不常发生的任务，计划设置完毕后，您将需要继续管理新建和修改过的 App-ID（均包含在内容发布中），因为这些 App-ID 可以改变安全策略实施的方式。

## 内容更新提示

Palo Alto Networks 应用程序和威胁内容发布经过严格的性能和质量检查。但是，因为客户网络环境中可能存在诸多变量，因此在极少数情况下，会出现内容发布以意想不到的方式影响网络的事件。请执行以下提示来减轻或解决内容发布带来的问题，尽可能将对您网络的影响降至最低。

- 请执行应用程序和威胁内容更新的最佳实践。

  查看并执行 应用程序和威胁内容更新的最佳实践。您选择部署内容更新的方式取决于您的网络安全和应用程序的可用性要求。
- 确保您运行的是最新内容。

  如果尚未配置可以自动下载和安装的防火墙，请获取最新内容更新。

  防火墙将验证已下载的内容更新是否仍然是安装时 Palo Alto Networks 推荐的更新。默认情况下，当内容更新下载自 Palo Alto Networks 更新服务器（手动或按计划）或是在安装前进行下载，防火墙执行的这类检查都将非常有用。因为在极少情况下，会出现 Palo Alto Networks 从可用性中删除内容更新的情况，即便是防火墙已成功下载，但该选项仍可以防止防火墙安装 Palo Alto Networks 已经删除的内容更新。如果看到一条“您正在尝试安装的内容更新已不再有效”错误消息，请 **Check Now**（立即检查），获取最新内容更新，并安装该版本（**Device**（设备）> **Dynamic Updates**（动态更新））。
- 打开威胁情报遥测。

  打开防火墙发送给 Palo Alto Networks 的威胁情报遥测。我们使用遥测数据来标识和解决内容更新相关的问题。

  遥测数据有助于我们快速识别在 Palo Alto Networks 客户群中以意想不到的方式影响防火墙性能或安全策略实施的内容更新。越快识别问题，我们就能越快地帮助您避免问题，或减轻对您网络的影响。

  要启动防火墙和 Palo Alto Networks 一起收集和共享遥测数据：

  1. 选择**Device**（设备）> **Setup**（设置）> **Telemetry**（遥测）。
  2. 编辑 **Telemetry**（遥测）设置，并 **Select All**（选择所有）。
  3. 单击 **OK**（确定）和 **Commit**（提交），保存您的更改。
- 向相应人员转发 **Palo Alto Networks** 内容更新警报。

  启用 Palo Alto Networks 关键内容警报的日志转发，以便将内容发布问题相关的重要消息直接发送给相应的人员。

  现在，Palo Alto Networks 可以将内容更新问题相关的警报直接发送给防火墙 Web 接口，或是在您已启用日志转发功能时，发送给用于监控的外部服务。关键内容警报对问题进行描述，为此，您能够了解它对您的影响，且还包含必要时应采取的操作步骤。


© 2019 Palo Alto Networks, Inc.

在防火墙 Web 接口上，关键内容问题警报的显示方式类似于当日消息。当 Palo Alto Networks 发布内容更新相关的关键警报时，警报将会在您登陆至防火墙 Web 接口时默认显示。如果您已成功登陆到防火墙 Web 接口，您会发现，在 Web 接口底部菜单栏上消息图标上会出现一个感叹号，单击消息图标以显示警报。

关键内容更新警报还可以记录为类型为动态更新，事件为 **palo-alto-networks-message** 的系统日志条目。使用下列筛选器以查看这些日志条目：( subtype eq dynamic-updates) 和 ( eventid eq palo-alto-networks-message)。

- 必要时，使用 **Panorama** 回滚到较早的内容版本。

  在看到内容更新相关的问题后，您可以使用 Panorama 快速将受管防火墙恢复至最新内容更新版本，而不是手动为每个防火墙恢复内容版本：恢复受管防火墙上的内容更新。



© 2019 Palo Alto Networks, Inc.

# 应用程序和威胁内容更新的最佳实践

部署内容更新的最佳实践有助于确保策略的无缝实施，同时防火墙可以持续配置新的和修改过的应用程序和威胁签名。即使应用程序和威胁签名一起通过单个内容更新包提供（请阅读更多有关应用程序和威胁内容更新的信息），您也可以根据网络安全和可用性要求灵活地区别部署：

- 奉行安全第一的组织会优先考虑使用最新威胁签名来进行防护，而非应用程序的可用性。您主要将防火墙用于实现威胁防护功能。
- 任务关键型网络优先考虑应用程序的可用性，而非使用最新威胁签名来进行防护。您的网络绝不容忍停机。防火墙在线部署以实施安全策略。如果您在安全策略中使用 App-ID，则任何影响 App-ID 的内容的更改都可能会导致停机。

您可以采取任务关键型或安全第一的方式来部署内容更新，或可以将这两种方法相结合来满足业务需求。在应用下列最佳实践以最有效地利用新的和修改过的威胁和应用程序签名时，请考虑您自己的方法：

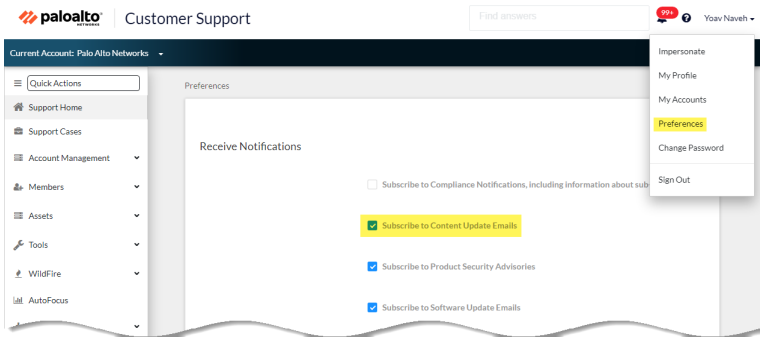
- 内容更新的最佳实践——任务关键型
- 内容更新的最佳实践 ——安全第一

## 内容更新的最佳实践——任务关键型

发布新应用程序和威胁签名时，应用程序和威胁内容更新的最佳实践有助于确保策略的无缝实施。当您对应用程序的停机时间零容忍时，请遵循这些最佳实践，在任务关键型网络中部署内容更新。

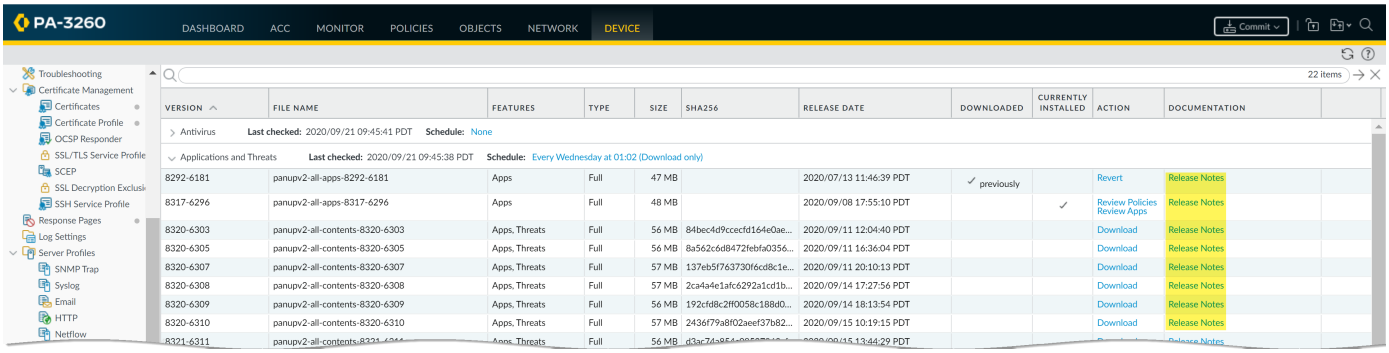
- 请始终查看“内容发布说明”，了解内容发布中引入的新识别和修改的应用程序和威胁签名列表。内容发布说明还对更新如何影响现有安全策略的实施进行说明，并提供有关如何修改安全策略以实现新功能的最佳利用的建议。

  要订阅获取新内容更新的通知，请访问客户支持门户，编辑您的 **Preferences**（首选项），然后选择 **Subscribe to Content Update Emails**（订阅内容更新电子邮件）。




  您还可以在 Palo Alto Networks 支持门户上查看应用程序和威胁内容发布说明，或是直接在防火墙 Web 界面查看：选择 **Device**（设备）> **Dynamic Updates**（动态更新），打开特定内容发布版本的 **Release Note**（发布说明）。

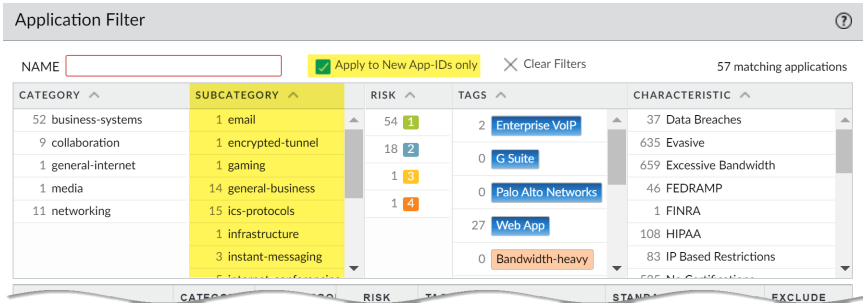

© 2019 Palo Alto Networks, Inc.



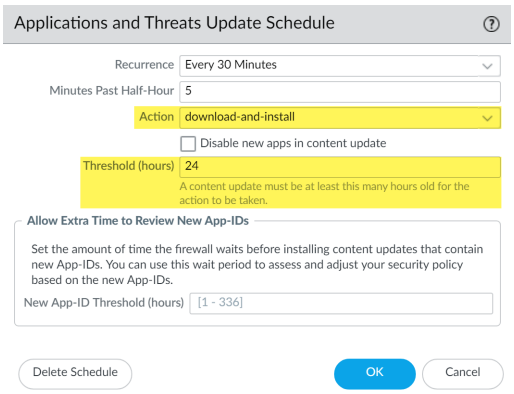

内容发布说明的“说明”部分着重强调 *Palo Alto Networks* 认为未来可能会对覆盖范围有重大影响的更新：例如，新的 *App-ID* 或解码器。检查这些未来更新，以便在发布之前解决策略带来的任何影响。

- 创建安全策略规则，始终允许某些类别的新建 App-ID，例如，关键业务功能所依赖的身份验证或软件开发应用程序。也就是说，当内容发布引入或更改重要业务应用程序的覆盖时，防火墙将继续无缝允许应用程序，无需更新安全策略。这就消除了关键类别中 App-ID 的任何潜在可用性影响，给您提供三十天的时间（新建 App-ID 应每月发布一次）调整安全策略，以允许任务关键型 App-ID。

  为此，创建用于关键类别中新 App-ID 的应用程序筛选器（**Objects > Application Filters**（对象> 应用程序筛选器））并添加应用程序筛选器至安全策略规则。




- 为了降低与启用新应用程序和威胁签名相关的安全策略实施的任何影响，可以交错使用新内容。在将新内容部署到具有更高业务风险的位置（例如具有关键应用程序的位置）之前，先将其提供给业务风险较低的位置（用户较少的卫星办公室）。在您的网络中部署之前，先将最新的内容更新部署到某些防火墙，这样便可更容易地解决出现的任何问题。您可以根据组织或位置使用 Panorama 将交错计划和安装阈值推送到防火墙和设备组（使用 Panorama 将更新部署至防火墙）。
- 安排内容更新，以自动**download-and-install**（下载并安装）然后，设置**Threshold**（阈值），确定防火墙在安装最新内容之前需要等待的时间量。在任务关键型网络中，安排的阈值最长为 48 小时。

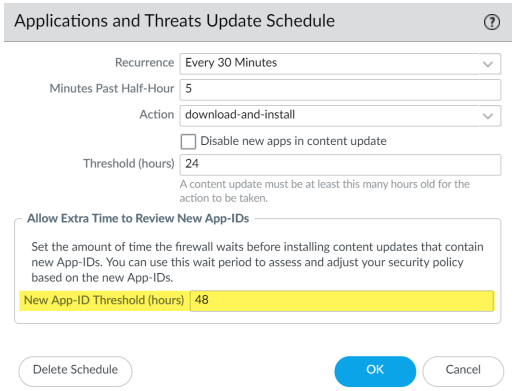




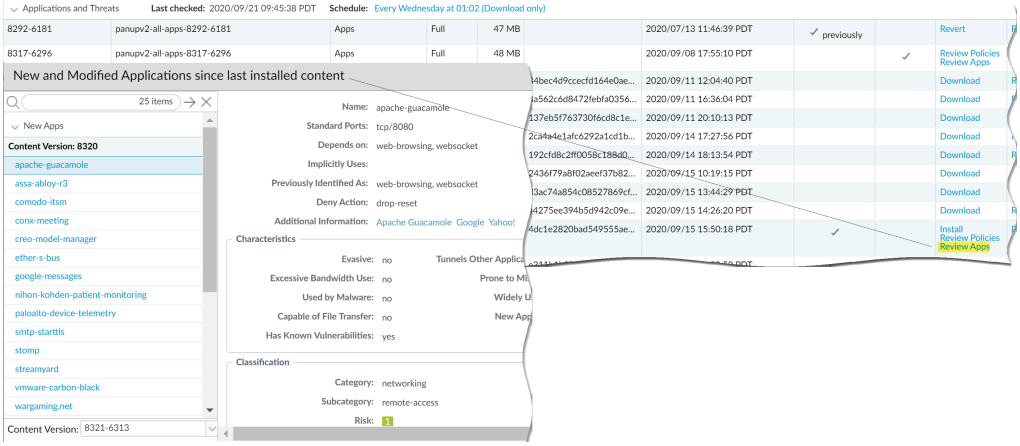

© 2019 Palo Alto Networks, Inc.

安装延迟，可确保防火墙在指定时间段内仅安装在客户环境中可用且功能正常的内容。要安排内容更新，请选择 **Device**（设备）> **Dynamic Updates**（动态更新）> **Schedule**（安排）。

- 在安装前，请给自己额外的时间根据新建 App-ID 调整您的安全策略。为此，设置仅适用于包含新建 App-ID 的内容更新的安装阈值。带新建 App-ID 的内容更新应每月仅发布一次，安装阈值应在此时触发。安排内容更新以配置 **New App-ID Threshold**（新建 **App-ID** 阈值）（**Device**（设备）> **Dynamic Updates**（动态更新）> **Schedule**（安排））。

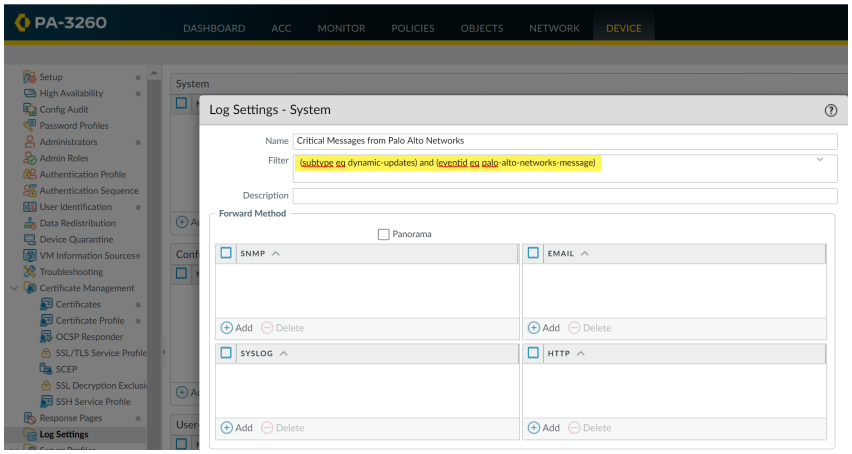



- 始终查看内容发布引入的新建和修改过的 App-ID，以评估更改可能会对安全策略产生的影响。以下主题介绍了您可以在安装新建 App-ID 前后用于更新安全策略的选项。管理新建和修改过的 App-ID。




- 设置日志转发，将 Palo Alto Networks 关键内容警告发送给您用于监控网络和防火墙活动的外部服务。为此，可以确保相应人员收到有关关键内容问题的通知，以便按需采取行动。关键内容警告将记录为带有以下“类型”和“事件”的系统日志条目：**`(subtype eq dynamic-updates)`** 及 **`(eventid eq palo-alto-networks-message)`**。


© 2019 Palo Alto Networks, Inc.




*PAN-OS 8.1.2* 将关键内容警告的日志类型从 ***general*** 更改为 ***dynamic-updates***。如果使用 *PAN-OS 8.1.0* 或 *PAN-OS 8.1.1*，则关键内容将记录为带有有以下类型和事件的系统日志条目，同时，应使用下列筛选器设置转发这些警告：***(subtype eq general)*** 和 ***(eventid eq palo-alto-networks-message)***。

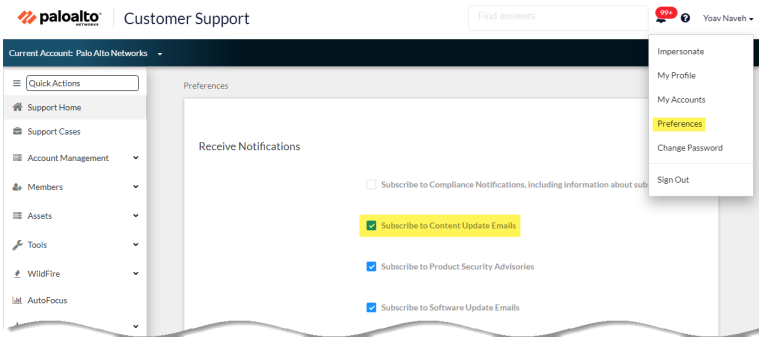
- 在专门的模拟环境中测试新应用程序和威胁内容更新，然后再在生产环境中启用。测试新应用程序和威胁的最简单方法是使用测试防火墙来接入生产流量。在测试防火墙上安装最新内容，并在处理从生产环境复制的流量时监控防火墙。您还可以使用测试客户端和测试防火墙或数据包捕获 (PCAP) 来模拟生产流量。使用 PCAP 可以很好地模拟各种部署的流量，其中防火墙安全策略因位置而异。

## 内容更新的最佳实践——安全第一

发布新应用程序和威胁签名时，应用程序和威胁内容更新的最佳实践有助于确保策略的无缝实施。当您主要使用防火墙实现威胁防护功能且您的首要任务是预防攻击时，请遵循这些最佳实践，在 *security-first network*（安全第一网络）中部署内容更新。

- 请始终查看“内容发布说明”，了解内容发布中引入的新识别和修改的应用程序和威胁签名列表。内容发布说明还对更新如何影响现有安全策略的实施进行说明，并提供有关如何修改安全策略以实现新功能的最佳利用的建议。

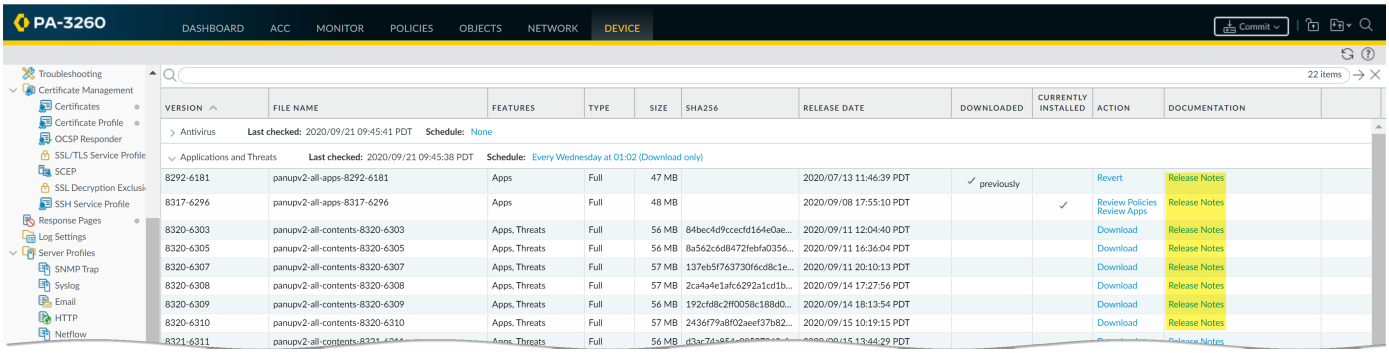
  要订阅获取新内容更新的通知，请访问客户支持门户，编辑您的 **Preferences**（首选项），然后选择 **Subscribe to Content Update Emails**（订阅内容更新电子邮件）。




  您还可以在 Palo Alto Networks 支持门户上查看应用程序和威胁内容发布说明，或是直接在防火墙 Web 界面查看：选择 **Device**（设备）> **Dynamic Updates**（动态更新），打开特定内容发布版本的 **Release Note**（发布说明）。

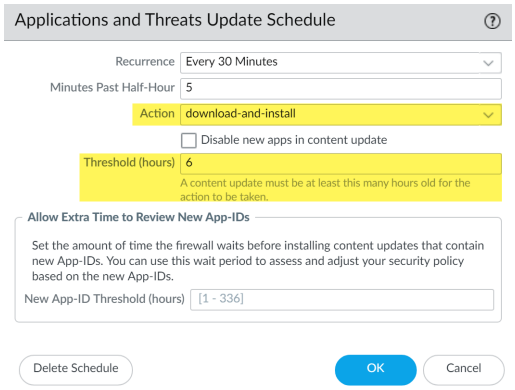


© 2019 Palo Alto Networks, Inc.




内容发布说明的“说明”部分着重强调 *Palo Alto Networks* 认为未来可能会对覆盖范围有重大影响的更新：例如，新的 *App-ID* 或解码器。检查这些未来更新，以便在发布之前解决策略带来的任何影响。

- 为了降低与启用新应用程序和威胁签名相关的安全策略实施的任何影响，可以交错使用新内容。在将新内容部署到具有更高业务风险的位置（例如具有关键应用程序的位置）之前，先将其提供给业务风险较低的位置（用户较少的卫星办公室）。在您的网络中部署之前，先将最新的内容更新部署到某些防火墙，这样便可更容易地解决出现的任何问题。您可以根据组织或位置使用 Panorama 将交错计划和安装阈值推送到防火墙和设备组（使用 Panorama 将更新部署至防火墙）。
- 安排内容更新，以自动**download-and-install**（下载并安装）然后，设置**Threshold**（阈值），确定防火墙在安装最新内容之前需要等待的时间量。在安全第一的网络中，安排 6 到 12 小时的阈值。

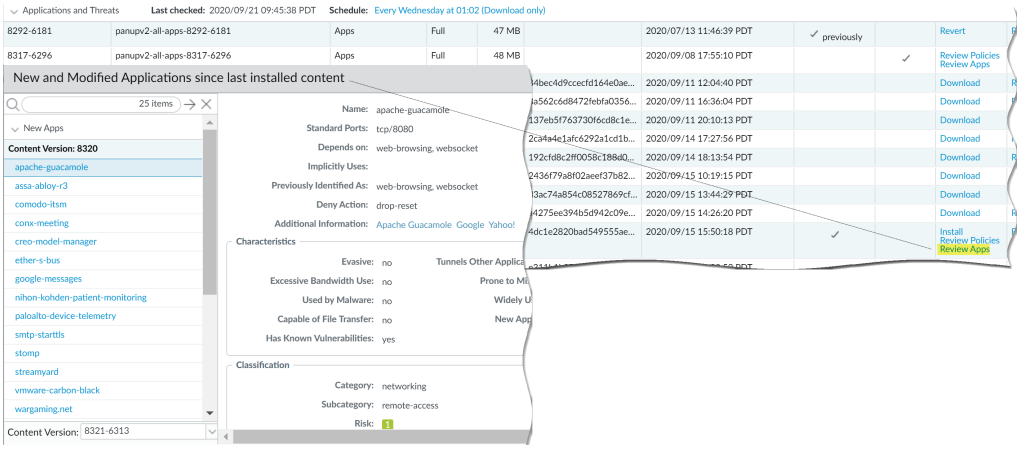



安装延迟，可确保防火墙在指定时间段内仅安装在客户环境中可用且功能正常的内容。要安排内容更新，请选择 **Device**（设备）> **Dynamic Updates**（动态更新）> **Schedule**（安排）。

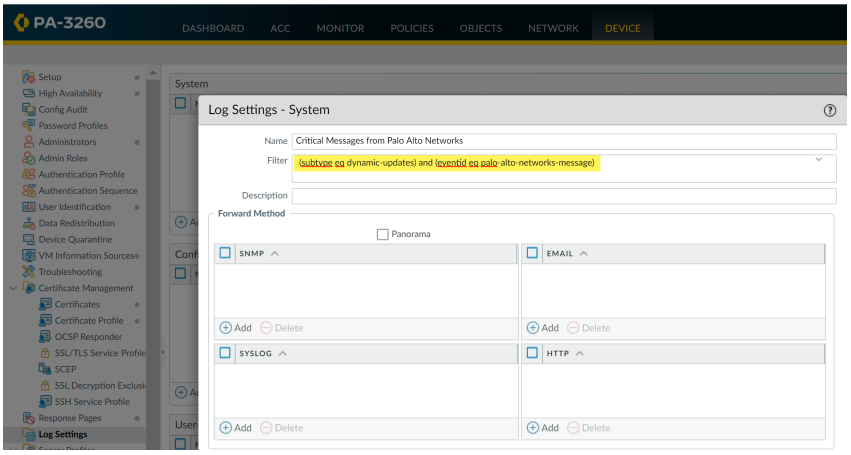
请勿安排 *New App-ID Threshold*（新建 *App-ID* 阈值）。此阈值给予任务关键型组织额外的时间来根据新建 *App-ID* 调整安全策略实施。但是，因为该阈值还会延迟最新威胁防护更新的交付，因此不建议奉行安全第一的组织使用。

- 查看内容发布引入的新建和修改过的 App-ID，以评估更改可能会对安全策略产生的影响。以下主题介绍了您可以在安装新建 App-ID 前后用于更新安全策略的选项。管理新建和修改过的 App-ID。


© 2019 Palo Alto Networks, Inc.




- 设置日志转发，将 Palo Alto Networks 关键内容警告发送给您用于监控网络和防火墙活动的外部服务。为此，可以确保相应人员收到有关关键内容问题的通知，以便按需采取行动。关键内容警告将记录为带有以下“类型”和“事件”的系统日志条目：(`subtype eq dynamic-updates`) 及 (`eventid eq palo-alto-networks-message`)。




*PAN-OS 8.1.2* 将关键内容警告的日志类型从 ***`general`*** 更改为 ***`dynamic-updates`***。如果使用 *PAN-OS 8.1.0* 或 *PAN-OS 8.1.1*，则关键内容将记录为带有有以下类型和事件的系统日志条目，同时，应使用下列筛选器设置转发这些警告：***`(subtype eq general)`*** 和 ***`(eventid eq palo-alto-networks-message)`***。



© 2019 Palo Alto Networks, Inc.

# 内容交付网络基础架构

Palo Alto Networks 维护了一个内容交付网络 (CDN) 基础架构，以便将内容更新交付到 Palo Alto Networks 防火墙。防火墙通过访问 CDN 中的 Web 资源来执行各种内容和应用程序标识功能。

下表列出了防火墙所访问的功能和应用的 Web 资源：

| 资源 | 网址 | 静态地址（如果需要静态服务器） |
|---|---|---|
| 应用程序数据库 | • updates.paloaltonetworks.com:443<br>• proditpdownloads.paloaltonetworks.com:443 | staticupdates.paloaltonetworks.com |
| 威胁/抗病毒数据库 | • updates.paloaltonetworks.com:443<br>• downloads.paloaltonetworks.com:443<br>• proditpdownloads.paloaltonetworks.com:443<br>最佳实践是设置更新服务器来访问 updates.paloaltonetworks.com。这样可以让 Palo Alto Networks 防火墙从 CDN 基础架构中与其最接近的服务器接收内容更新。 | staticupdates.paloaltonetworks.com |
| PAN-DB URL Filtering | *.urlcloud.paloaltonetworks.com<br>解析到主 URL s0000.urlcloud.paloaltonetworks.com，然后重定向到最近的区域服务器：<br>• s0100.urlcloud.paloaltonetworks.com<br>• s0200.urlcloud.paloaltonetworks.com<br>• s0300.urlcloud.paloaltonetworks.com<br>• s0500.urlcloud.paloaltonetworks.com | 不可使用静态 IP 地址。但是，您可以手动将 URL 解析到一个 IP 地址，并允许访问区域服务器 IP 地址。 |



© 2019 Palo Alto Networks, Inc.

# 防火墙管理

管理员可以使用 Web 界面、CLI 和 API 管理界面配置、管理和监控 Palo Alto Networks 防火墙。您可对基于管理角色的管理界面访问进行自定义，从而指定某些管理员的具体任务或权限。

- 管理接口
- 使用 Web 界面
- 管理配置备份
- 管理防火墙管理员
- 引用：Web 界面管理员访问
- 引用：端口码使用
- 将防火墙重置为出厂默认设置
- 自举防火墙

# 管理接口

您可使用以下用户界面来管理 Palo Alto Networks 防火墙：



请勿从 *Internet* 或企业安全边界内其他不信任区域启用管理访问。要确保正确保护防火墙的安全，请遵循确保管理员访问安全的最佳实践。

- 使用 Web 界面以更容易地执行配置和监控任务。此图形界面可让您使用 HTTPS（推荐）或 HTTP 访问防火墙，这是执行管理任务的最佳方法。
- 使用命令行界面 (CLI) 通过在 SSH（推荐）、Telnet 或控制台端口快速连续地输入命令来执行一系列任务。CLI 是一个简洁的界面，支持两种命令模式（操作和配置），且每种模式都拥有自己的命令和语句的层次结构。熟悉命令的嵌套结构和语法后，便可利用 CLI 作出快速响应，并实现高效的管理。
- 使用 XML API可让您简化操作并与现有内部开发的应用程序和存储库进行整合。XML API 是一种使用 HTTP/HTTPS 请求和响应执行的 Web 服务。
- 使用 Panorama 为多个防火墙执行基于 Web 的管理、报告和日志收集。Panorama Web 界面类似于防火墙 Web 界面，但具有用于集中管理的其他功能。



© 2019 Palo Alto Networks, Inc.

# 使用 Web 界面

以下主题对如何使用防火墙 Web 界面进行了介绍。有关 Web 界面上选项卡和字段的详细信息，请参阅《Web 界面参考指南》。

- 启动 Web 界面
- 配置横幅、当日消息及徽标
- 使用管理员登录活动指标检测帐户不当使用
- 管理和监控管理任务
- 提交、验证和预览防火墙配置更改
- 导出配置表格数据
- 利用全局查找搜索防火墙或 Panorama 管理服务器
- 管理配置更改限制锁

## 启动 Web 界面

支持使用以下 Web 浏览器访问防火墙 Web 界面：

- Internet Explorer 11 及更高版本
- Firefox 3.6 及更高版本
- Safari 5 及更高版本
- Chrome 11 及更高版本

执行以下任务以启动 Web 界面。

STEP 1 | 开启互联网浏览器，在 URL 字段输入防火墙的 IP 地址 (https://<IP address>)。



默认情况下，管理 *(MGT)* 界面仅允许 *HTTPS* 访问 *Web* 界面。要启用其他协议，请选择 *Device*（设备）> *Setup*（设置）> *Interfaces*（接口），并编辑 *Management*（管理）接口。

STEP 2 | 根据帐户使用的身份验证类型登录防火墙。如果首次登录防火墙，请使用默认值 **admin** 作为用户名和密码。

- **SAML** — 单击 **Use Single Sign-On**（使用单点登录）(SSO)。如果防火墙为管理员执行授权（角色分配），请输入您的 **Username**（用户名）并 **Continue**（继续）。如果 SAML 标识提供商 (IdP) 执行授权，直接 **Continue**（继续），无需输入 **Username**（用户名）。在这两种情况下，防火墙都将重定向到 IdP，提示您输入用户名和密码。对 IdP 进行身份验证后，将显示防火墙 Web 界面。
- 任何其他类型的身份验证 — 输入您的用户 **Name**（名称）和 **Password**（密码）。如果登录页面有横幅和复选框，请阅读登录横幅并选择 **I Accept and Acknowledge the Statement Below**（我接受并确认以下陈述）。然后单击 **Login**（登录）。

STEP 3 | 读取并 **Close**（关闭）当日消息。

## 配置横幅、当日消息及徽标

登录横幅指您可选择添加至登录页面的文本，以便管理员在登录前看到其必须知道的信息。例如，您可以添加信息以提醒用户关于未授权使用防火墙的限制。

您还可在 Web 界面的顶部（标头横幅）及底部（脚注横幅）添加突出叠加文本的色带，以确保管理员可看见防火墙管理分类级别等重要信息。



© 2019 Palo Alto Networks, Inc.

登录后将自动出现当日信息对话框。对话框将显示 Palo Alto Networks 的嵌入信息，主要为软件或内部发布等相关重要信息。您还可添加自定义信息，如即将进行的、可能对管理员任务产生影响的系统重启，以确保管理员能看见该信息。

您可以将出现在登录页面及 Web 界面标头的默认徽标替换成您组织的徽标。

STEP 1 | 配置登录横幅。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。
2. 输入 **Login Banner**（登录横幅）（最多 3,200 个字符）。
3. （可选）选择 **Force Admins to Acknowledge Login Banner**（强制管理员确认登录横幅）以强制管理员选择横幅文本上方的 **I Accept and Acknowledge the Statement Below**（我接受并确认以下陈述）复选框，激活 **Login**（登录）按钮。
4. 单击 **OK**（确定）。

STEP 2 | 设置当日消息。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑横幅和消息设置。
2. 启用 **Message of the Day**（当日消息）。
3. 输入 **Message of the Day**（当日消息）（最多 3,200 个字符）。

   输入消息并单击 *OK*（确认）后，后续登录的管理员和刷新其浏览器的管理员将立即看到新的或更新的消息，而无需进行提交操作。这可让您将即将执行、且可能影响其配置更改的提交操作告知其他管理员。根据您消息所规定的提交时间，管理员可确定是否完成、保存或撤销其更改。
4. （可选）选择 **Allow Do Not Display Again**（允许不再显示）（默认为禁用该选项），给予管理员在首次登录会话后取消显示消息的选项。管理员仅可取消显示其自身登录会话的消息。在当日消息对话框中，每条消息都有单独的取消显示选项。
5. （可选）输入当日消息对话框的标头 **Title**（标题）（默认为 `Message of the Day`）。

STEP 3 | 配置标头和脚注横幅。

明亮的背景颜色及对比鲜明的文本颜色能增加管理员注意到并读取横幅的可能性。您可以使用与您组织分类级别对应的颜色。

1. 输入 **Header Banner**（标头横幅）（最多 3,200 个字符）。
2. （可选）取消选中**Same Banner Header and Footer**（相同横幅标头及脚注）（默认为启用该选项）以使用不同的标头及脚注横幅。
3. 如果标头横幅与脚注横幅不同，输入 **Footer Banner**（脚注横幅）（最多 3,200 个字符）。
4. 单击 **OK**（确定）。

STEP 4 | 替换登录页面及标头中的徽标。

任何徽标图像的最大尺寸均为 *128KB*。支持的文件类型有 *png*、*gif* 和 *jpg*。防火墙不支持隔行扫描或包含 *Alpha* 通道的图像文件。

1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），然后单击 Miscellaneous（其他）部分的 **Custom Logos**（自定义徽标）。
2. 对 **Login Screen**（登录屏幕）徽标及 **Main UI**（主要 **UI**）（标头）徽标执行以下步骤：
   1. 单击上传 。
   2. 选择徽标图像并单击 **Open**（打开）。

      您可以单击放大镜图标，预览图像以查看 *PAN-OS* 如何进行裁剪以拟合。



© 2019 Palo Alto Networks, Inc.

3. 单击 **Close**（关闭）。
3. **Commit**（提交）更改。

STEP 5 | 确认横幅、当日消息及徽标按预期显示。

1. 退出并返回至显示您之前选择的新徽标的登录页面。
2. 输入您的登录凭证，查看横幅并选择 **I Accept and Acknowledge the Statement Below**（我接受并确认以下陈述）以启用 **Login**（登录）按钮，然后 **Login**（登录）。

   对话框将显示当日消息。Palo Alto Networks 嵌入的消息将显示于同一对话框的不同页面。如需导航该页面，请单击对话框两侧向右或向左箭头，或单击对话框底部周围的页面选择器（●○○○）。
3. （可选）您配置的消息及 Palo Alto Networks 嵌入的任何消息均可选择 **Do not show again**（不再显示）。
4. **Close**（关闭）当日消息对话框以进入 Web 界面。

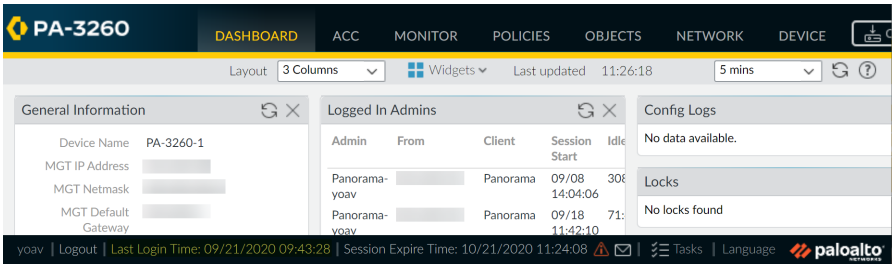
   标头及脚注横幅的文本及颜色将按配置显示在所有 Web 界面。您为 Web 界面选择的新图标将显示在标头横幅下方。

# 使用管理员登录活动指标检测帐户不当使用

上次的登录时间及失败登录尝试指标提供了一种检测 Palo Alto Networks 防火墙 Panorama 管理服务器上的管理员帐户不当使用的可视化方法。您可以根据上次的登录信息确定是否有他人利用您的登录凭证进行登录，您也可以通过失败登录次数来确定您的帐户是否成为了蛮力攻击的目标。

STEP 1 | 查看登录活动指数以监控最近的帐户活动。

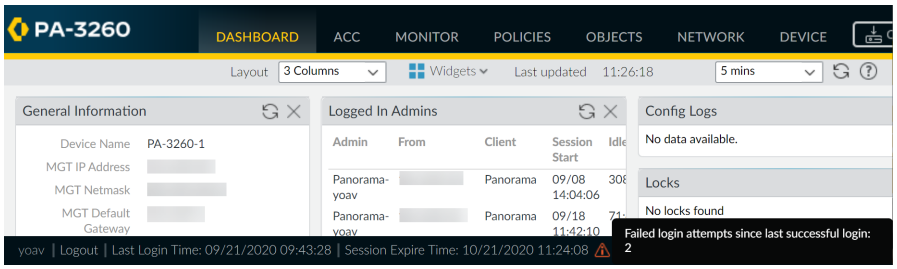
1. 登录您防火墙或 Panorama 管理服务器的 Web 界面，
2. 查看位于窗口左下角的最近登录详情，确认时间戳与上次登录时间一致。




3. 查看上次登录时间右边的警告图标，了解失败登录尝试次数。

   如果自上次成功登陆起，使用您帐户登录的失败尝试超过 1 次，将显示失败登录指标。

   1. 如果看到警告图标，将鼠标停在其上方，显示失败登录尝试次数。




   2. 单击警告图标查看失败登录尝试概览。包含管理帐户名称、登录失败原因、源 IP 地址、日期及时间等详细信息。



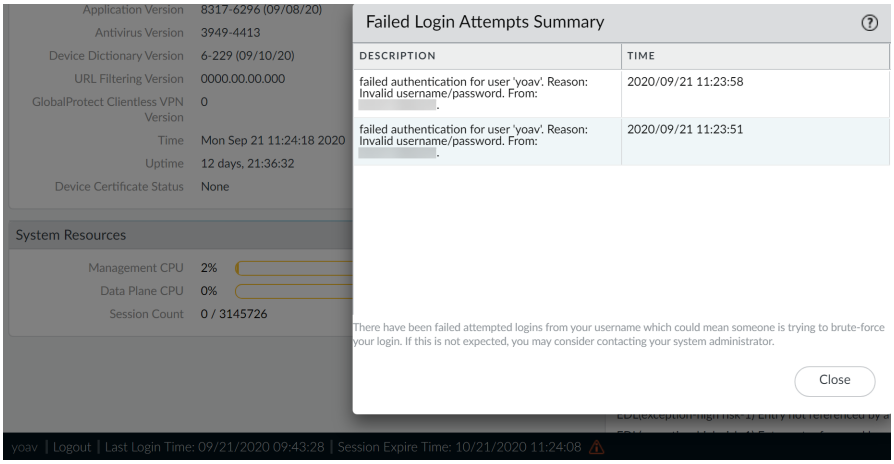
在您成功登录并退出后，失败登录计数器将重置为 *0*，因此您可在下次登录时查看新的失败登录详情（若有）。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 确定持续尝试登录您的防火墙或 Panorama 管理服务器的主机位置。

1. 单击失败登录警告图标查看失败登录尝试概览。
2. 定位并记录试图登录的主机的源 IP 地址。例如，以下数据显示了多次失败登录尝试。




3. 与网络管理员一起找到使用该 IP 地址的用户及主机。

   如果无法确定进行蛮力攻击的系统位置，请考虑重命名帐户以防止将来再次受到攻击。

STEP 3 | 如果检测到帐户窃取情况，请执行以下步骤。

1. 选择 **Monitor**（监控）> **Logs**（日志）> **Configuration**（配置），查看配置更改并提交历史记录，以确定您的帐户是否被用来做出您并不知情的更改。
2. 选择 **Device**（设备）> **Config Audit**（配置审核），对比当前配置与您怀疑已利用您的凭据做出更改的配置之前所运行的配置。您亦可使用 Panorama 进行上述操作。

   如果您的管理员帐户被用来创建新的帐户，执行配置审核以帮助您检测与任何未授权帐户有关的更改。

3. 如果您发现日志被清除，或难以确定是否帐户被用于进行不当更改，请将配置恢复到已知的正确配置。

   在恢复至先前配置前，请仔细审核以确保其包含正确的设置。例如，您恢复的配置可能不包含最近更改，因此您需要在还原至备份配置时应用那些更改。

   采用以下最佳实践，帮助阻挡对特权帐户的蛮力攻击。

   - 通过在身份验证配置文件或管理界面的身份验证设置（*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Authentication Settings*（身份验证设置））中设置失败尝试次数和锁定时间（分钟），限制防火墙锁定特权帐户之前允许的失败尝试次数。
   - 使用接口管理配置文件限制访问。
   - 对特权帐户实施复杂密码。

# 管理和监控管理任务

任务管理器会显示您及其他管理员发起的所有操作（如手动提交）详情，或自防火墙上次重启后，防火墙发起的所有操作详情（如生成预定报告）。您可以使用任务管理器解决失败操作，了解与已完成提交相关的警告，查看提交队列详情或取消暂挂提交。

您还可查看系统日志以监控防火墙上的系统事件或查看配置日志以监控防火墙配置更改。



© 2019 Palo Alto Networks, Inc.

STEP 1 | 单击 Web 界面底部的 **Tasks**（任务）。

STEP 2 | 仅 **Show**（显示）**Running**（正在运行)的任务（进展中）或显示 **All**（所有）任务（默认为该选项）。或者，按类型筛选任务：

- **Jobs**（作业）— 管理员发起的提交，防火墙发起的提交及软件或内容下载及安装。
- **Reports**（报告）— 预定生成的报告。
- **Log Requests**（日志请求）— 访问 **Dashboard**（仪表板）或 **Monitor**（监控）页面触发的日志查询。

STEP 3 | 执行以下任何操作：

- 显示或隐藏任务详细信息 — 默认情况下，任务管理器显示每个任务的类型、状态、开始时间和消息。要查看任务的结束时间及作业 ID，您必须手动配置任务管理器以显示这些列。要显示或隐藏某列，打开任何列标头的下拉菜单，选择 **Columns**（列），然后按需要选中或取消选中列名。
- 调查警告或故障 — 阅读 Messages（消息）列的条目了解任务详细信息。如果列显示 `Too many messages`（消息太多），单击 Type（类型）列中的相应条目，了解更多信息。
- 显示提交说明 — 如果管理员在配置提交时输入了说明，您可单击 Messages（消息）列中的 **Commit Description**（提交说明）以显示说明。
- 检查提交在队列中的位置 — Messages（消息）列指示了正在进行中的提交的队列位置。
- 取消暂挂提交 — 单击 **Clear Commit Queue**（清除提交队列）以取消所有暂挂提交（仅可用于已预定义的管理角色）。要取消单个提交，单击 Action（操作）列中该提交的 **x** 键（在防火墙将其从队列中清除前，该提交仍会保留在队列中）。您不能取消正在进行的提交。

# 提交、验证和预览防火墙配置更改

提交正在激活防火墙配置暂挂的更改。您可以按管理员或位置筛选暂挂的更改，然后仅预览、验证或提交这些更改。位置可以是特定虚拟系统、共享策略和对象，或共享设备和网络设置。

防火墙会将提交操作整理成队列，以便您可在之前的提交操作处于进行状态时，启动新的提交操作。防火墙按其启动顺序执行提交，但会优先执行防火墙触发的自动提交（如 FQDN 刷新）。但是，如果队列已有最大数量的管理员发起的提交，则必须等待防火墙完成暂挂提交的处理后才可启动新提交。要取消暂挂提交或查看处于任何状态的提交详情，请参阅管理和监控管理任务。

发起提交后，防火墙会在激活更改前检查其有效性。验证输出将显示阻止提交（出错），或须知的重要事项（警告）的条件。例如，验证可能指出一个需要修复才能提交成功的无效路径目标。验证过程能让您在提交之前查找和修复错误（不会对正在运行的配置进行任何更改）。如果您拥有固定提交窗口，并且希望确保提交将成功而没有出现错误，这将非常有用。

托管防火墙一旦被 Panorama™ 管理服务器启用和管理，就能从本地测试本地提交或是从 Panorama 推送的配置，以验证新更改不会中断 Panorama 与托管防火墙之间的连接。如果提交的配置中断 Panorama 与托管防火墙之间的连接，那么防火墙会自动使提交失败，且配置会恢复为先前运行的配置。此外，由 Panorama 管理服务器管理的防火墙每隔 60 分钟会检查一次它与 Panorama 的连接。如果托管防火墙检测到它再也无法成功连接到 Panorama，就会将配置恢复为先前运行的配置。



提交、验证、预览、保存和恢复操作仅适用于上次提交后所做的更改。要将配置还原到上次提交之前的状态，必须加载之前备份的配置。

要防止多个管理员在并行会话中进行配置更改，请参阅管理配置更改限制锁。

STEP 1 | 配置要提交、验证或预览的配置更改范围。

1. 单击 Web 界面顶部的 **Commit**（提交）。
2. 选择以下任一选项：

   - **Commit All Changes**（提交所有更改）（默认）-— 将提交应用于具有管理权限的所有更改。选择此选项时，不能手动筛选提交范围。而是分配给您用于登录的帐户的管理员角色确定提交范围。



© 2019 Palo Alto Networks, Inc.

- **Commit Changes Made By**（提交所做的更改）-— 使您能够通过管理员或位置筛选提交范围。分配给您用于登录的帐户的管理角色确定可以筛选的更改。



要提交其他管理员的更改，您用于登录的帐户必须分配给“超级用户”角色或管理角色配置文件，并启用 *Commit For Other Admins*（为其他管理员提交）权限。

3. （可选）要根据管理员筛选提交范围，请选择 **Commit Changes Made By**（提交所做的更改），单击相邻链接，选择管理员，然后单击 **OK**（确定）。
4. （可选）要根据位置筛选，请选择 **Commit Changes Made By**（提交所做的更改），并清除要从 Commit Scope（提交范围）中排除的任何更改。



如果您启用及禁用的配置更改间的相关性导致验证错误，请在启用所有更改的情况下进行提交。例如，在将更改提交到虚拟系统时，必须包括对该虚拟系统中的同一规则库加载、删除或重定位规则的所有管理员的更改。

STEP 2 | 预览提交将激活的更改。

预览在您忘记自己的更改或您不确定自己是否想要激活这些更改等情况下很有用处。

防火墙让您将“提交范围”中选择的配置与正在运行的配置进行比较。预览窗口并排显示配置，并使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。

**Preview Changes**（预览更改）并选择 **Lines of Context**（上下文行数），这是比较配置文件中的行数，以显示高亮差异之前和之后的信息。这些附加行数有助于使预览输出与 Web 界面设置相互关联。完成更改审核后，关闭预览窗口。



由于预览结果会在新浏览器窗口中显示，所以您的浏览器必须设置允许窗口弹出。如果预览窗口未打开，请参阅浏览器文档，了解允许窗口弹出的相关步骤。

STEP 3 | 预览您用于提交更改的各个设置。

如果您想了解有关更改的详细信息（例如设置类型和实施更改的人员），预览会很有用。

1. 单击 **Change Summary**（更改摘要）。
2. （可选）列名称**Group By**（分组方式）（例如，设置 **Type**（类型））。
3. 完成更改审核后，**Close**（关闭）“更改摘要”对话框。

STEP 4 | 提交前验证更改以确保成功提交。

1. **Validate Changes**（验证更改）。

   验证结果显示的所有错误及警告均与实际提交所显示的一致。
2. 解决验证结果找到的任何错误。

STEP 5 | Commit（提交）配置更改。

**Commit**（提交）更改以验证并激活。



要查看暂挂（仍可取消）、进行中、已完成或失败的提交，请参阅管理和监控管理任务。

# 导出配置表格数据

从 Panorama™ 和防火墙导出策略规则、配置对象和 IPS 签名，以证明外部审核员是否符合法规要求、定期查看防火墙配置、并生成防火墙策略报告。这样，审核员就可以在无需直接访问您的防火墙和设备、拍摄屏幕截图或访问 XML API 的情况下生成配置报告。在 Web 界面中，您可以采用 PDF 或 CSV 格式导出策略、



© 2019 Palo Alto Networks, Inc.

对象、网络、防火墙的配置表格数据、Panorama 配置，以及防病毒、防间谍和漏洞保护安全配置文件中的签名例外情况。

配置表的导出就像打印功能一样，即，不能将生成的文件导回到 Panorama 或防火墙。当以 PDF 格式导出数据且表格数据超过 50000 行时，数据将拆分为多个 PDF 文件（例如，<report-name>_part1.pdf 和 <report-name>_part2.pdf）。当以 CSV 格式导出数据时，则只有一个文件。这些导出格式允许您使用与报告条件匹配的筛选器，并在 PDF 报告中进行搜索，以快速查找特定数据。此外，在导出配置表格数据时，会生成系统日志以记录事件。

STEP 1 | 启动 Web 界面，并标识需要导出的配置数据。

STEP 2 | 必要时，使用筛选器以生成需要导出的配置数据，然后单击 **PDF/CSV**。



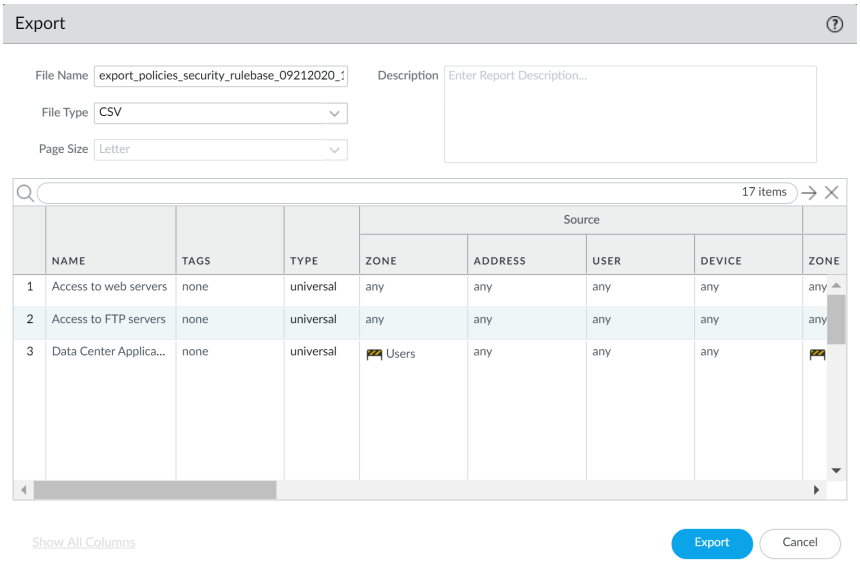

STEP 3 | 配置“配置表格导出”报告：

1. 输入 **File Name**（文件名称）。
2. 选择 **File Name Type**（文件类型）。
3. （可选）输入报告说明。
4. 确认配置表格数据是否与您应用的筛选器匹配。

选择 *Show All Columns*（显示所有列）以显示应用的所有筛选器。

STEP 4 | **Export**（导出）配置表格数据。

配置表的导出就像打印功能一样，即，不能将生成文件导回到 Panorama 或防火墙。




STEP 5 | 选择用于保存导出文件的位置。

# 利用全局查找搜索防火墙或 Panorama 管理服务器

全局查找可让您在防火墙或 Panorama 上搜索特定字符串的待选配置，如 IP 地址、对象名称、策略规则名称、威胁 ID、UUID 或应用程序名称。除了搜索配置对象和设置之外，还可以按作业 ID 或作业类型进行搜索，以便管理员执行或自动提交防火墙或 Panorama 执行的提交。搜索结果已按类别进行分组，并在 Web 界面上提供指向配置位置的链接，这样您可以轻松找到引用字符串的所有位置。搜索结果也有助于您标识依赖或引用此搜索项或字符串的其他对象。例如，弃用安全配置文件时，要在全局查找中输入配置文件名称



© 2019 Palo Alto Networks, Inc.

以找到此配置文件的所有实例，然后单击每个实例以导航至配置页面，并作出必要的更改。删除所有引用之后，才能删除配置文件。您可以为具有依赖关系的所有配置项执行此操作。

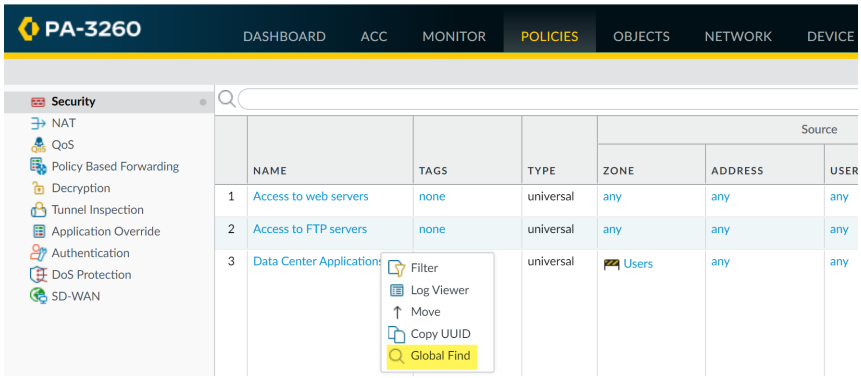
观看视频。

全局查找不会搜索动态内容（如日志、地址范围或已分配的 *DHCP* 地址）。在 *DHCP* 的情况下，您可以针对 *DHCP* 服务器属性（如 *DNS* 条目）进行搜索，但不能搜索分配给用户的单个地址。全局查找也不会搜索通过用户 *ID* 标识的单个用户或组名称，除非在策略中定义了用户/用户组。一般情况下，只能针对防火墙写入配置的内容进行搜索。

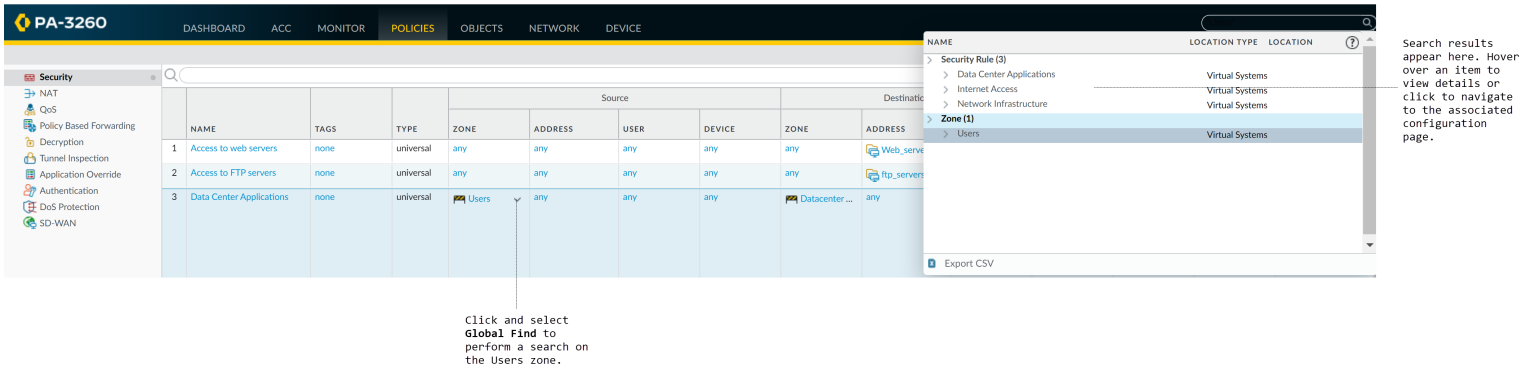
- 通过单击位于 Web 界面右上角的 **Search**（搜索）图标启动全局查找。




- 要从配置区域内访问全局查找功能，单击项目旁边的下拉列表，然后选择**Global Find**（全局查找）：




例如，单击名为 **Users**（用户）区域上的 **Global Find**（全局查找），会搜索引用区域的每个位置的待选配置。以下屏幕截图显示区域用户的搜索结果：




搜索提示：

- 如果您在已启用多个虚拟系统的防火墙上搜索或如果已定义定制管理员角色类型，则全局查找将只返回管理员在其中拥有权限的防火墙区域的结果。这同样适用于 Panorama 设备组。
- 搜索项目中的空格作为 AND 操作进行处理。例如，如果您针对公司政策进行搜索，则搜索结果包含公司和策略存在配置中的实例。
- 要查找一个精确短语，请给该短语加上引号。
- 要返回上一个搜索，单击 Web 界面右上角的搜索图标，随即会显示最后 20 个搜索的列表。单击列表中的项目可重新执行该搜索。搜索历史记录列表对于每个管理员帐户都是唯一。



© 2019 Palo Alto Networks, Inc.

- 要搜索 UUID，您必须复制并粘贴 UUID。

## 管理配置更改限制锁

可以使用配置锁来阻止其他管理员更改待选配置或提交配置更改，直到手动删除该锁或防火墙自动将其删除（提交后）。锁定确保管理员不会在并行登录会话中对同一设置或互相依赖的设置进行有冲突的更改。

防火墙将提交请求排成队列，并按照管理员发起提交的顺序进行提交。有关详细信息，请参阅提交、验证和预览防火墙配置更改。要查看列队提交的状态，请参阅管理和监控管理任务。

- 查看关于当前锁定的详情。

  例如，您可以查看其他管理员是否设置了锁定，阅读他们为了解释锁定原因而输入的备注。

  单击 Web 界面顶部的锁定 图标。相邻数字为当前锁定的个数。

- 锁定配置。
  1. 单击 Web 界面顶部的锁定图标。

     锁定图像根据当前锁定状态是 还是未设置 而异。
  2. **Take a Lock**（执行锁定），选择锁定 **Type**（类型）：
     - **Config**（配置）— 阻止其他管理员对待选配置进行更改。
     - **Commit**（提交）— 阻止其他管理员提交对待选配置进行的更改。
  3. （仅具备多个虚拟系统的防火墙）选择 **Location**（位置）或 **Shared**（共享）位置以锁定特定虚拟系统的配置。
  4. （可选）最佳实践是在锁定后输入 **Comment**（注释）以便其他管理员了解锁定原因。
  5. 单击 **OK**（确定）和 **Close**（关闭）。

- 解锁配置。

  只有超级用户或锁定配置的管理员可手动解锁。尽管如此，在完成提交操作后，防火墙会自动解除锁定。

  1. 单击 Web 界面顶部的锁定图标。
  2. 在列表中选择锁定条目。
  3. 单击 **Remove Lock**（删除锁定）、**OK**（确定）和 **Close**（关闭）。

- 配置防火墙在待选配置更改时自动应用提交锁定。此设置应用于所有管理员。
  1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。
  2. 选择 **Automatically Acquire Commit Lock**（自动获取提交锁定），然后单击 **OK**（确定），再单击 **Commit**（提交）。


© 2019 Palo Alto Networks, Inc.

# 管理配置备份

防火墙上的运行配置包含您已经提交且已激活的所有设置，如用于阻止或允许网络中各类流量的当前策略规则。待选配置是正在运行的配置的副本，包含您在上次提交后所做的任何未激活更改。保存运行中或待选配置的备份版本可以让您能够稍后恢复这些版本。例如，如果一个提交验证显示当前待选配置错误太多，不容易修复，您可以恢复之前的待选配置。您也可以还原到当前的运行配置，而无需先保存备份。如果需要导出配置的特定部分以进行内部审查或审核，则可以导出配置表格数据。

有关提交操作的详细信息，请参阅提交、验证和预览防火墙配置更改。

- 保存并导出防火墙配置
- 还原防火墙配置更改

## 保存并导出防火墙配置

将待选配置的备份保存到防火墙上的永久存储中，以备稍后还原该备份（请参阅还原防火墙配置更改）。这对于保留在系统事件或管理员操作导致防火墙重启时将会丢失的更改十分有用。重新启动后，PAN-OS 自动还原至当前运行的配置版本，防火墙将该版本存储于名为 running-config.xml 的文件中。如果要还原到比当前运行的配置更早的防火墙配置，则保存备份也很有用。防火墙不会自动将待选配置保存为永久存储。您必须手动将待选配置保存为默认快照文件 (.snapshot.xml) 或自定义命名快照文件。防火墙本地存储快照文件，但您可以将其导出到外部主机。

您不必保存配置备份以还原自上次提交或重新启动以来所做的更改；只需选择 *Config*（配置）> *Revert Changes*（恢复更改）即可完成（请参阅还原防火墙配置更改）。

完成设置编辑并单击 *OK*（确定）后，防火墙会更新待选配置但不会保存备份快照。

此外，保存更改不会激活它们。要激活更改，请执行提交（请参阅提交、验证和预览防火墙配置更改）。

*Palo Alto Networks* 建议您将任何重要配置备份到防火墙的外部主机。

STEP 1 | 如果待选配置包含您希望将其保存于防火墙重启事件的更改，您可保存待选配置的本地备份快照。

这些是您不准备提交的更改，如您不能在当前登录会话中完成的更改。

要替换带所有管理员所做的所有更改的默认快照文件 (.snapshot.xml)，请执行以下步骤之一：

- 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）并 **Save candidate configuration**（保存待选配置）。
- 使用已分配给超级用户角色或管理员角色配置文件的管理帐户登录防火墙，并启用 **Save For Other Admins**（为其他管理员保存）权限。然后在 Web 界面顶部选择 **Config**（配置）> **Save Changes**（保存更改），选择**Save All Changes**（保存所有更改），并 **Save**（保存）。

要创建包含所有管理员所做的所有更改的快照但不替换默认快照文件：

1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），单击 **Save named configuration snapshot**（保存已命名配置快照）。
2. 指定新的或现有配置文件的 **Name**（名称）。
3. 单击 **OK**（确定）和 **Close**（关闭）。

仅保存待选配置的特定更改，而不替换默认快照文件的任何部分：

1. 使用具有角色权限的管理帐户登录到防火墙，以保存所需更改。



© 2019 Palo Alto Networks, Inc.

2. 在 Web 界面顶部选择 **Config**（配置）> **Save Changes**（保存更改）。
3. 选择 **Save Changes Made By**（所作更改保存依据）。
4. 要按管理员筛选保存范围，请单击 **<administrator-name>**，选择管理员，然后单击 **OK**（确定）。
5. 要按位置筛选保存范围，请清除要排除的任何位置。位置可以是特定虚拟系统、共享策略和对象，或共享设备和网络设置。
6. 单击 **Save**（保存），指定新配置文件或现有配置文件的 **Name**（名称），然后单击 **OK**（确定）。

STEP 2 | 导出待选配置，正在运行中的配置或防火墙状态信息至防火墙的外部主机。

选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）并单击导出选项：

- **Export named configuration snapshot**（导出已命名配置快照）— 导出当前运行的配置、待选配置快照，或之前导入的配置（待选配置或正在运行的配置）。防火墙会将配置导出为带有您指定 **Name**（名称）的 XML 文件。
- **Export configuration version**（导出配置版本）— 选择运行中配置的 **Version**（版本），导出为 XML 文件。无论您何时提交配置更改，防火墙都会创建版本。
- **Export device state**（导出设备状态）— 将防火墙状态信息导出为状态包。除正在运行的配置之外，状态信息将包含从 Panorama 推送的设备组和模板设置。如果防火墙为 GlobalProtect 门户，则此状态信息包也会包含证书信息、卫星列表，以及卫星身份验证信息。如果您更换了防火墙或门户，您可通过导入状态包来还原更换时导出的信息。

# 还原防火墙配置更改

还原操作将当前待选配置中的设置替换为另一个配置的设置。当您想要撤销多个设置的更改以作为单个操作，而不是手动重新配置每个设置时，还原更改十分有用。

您可以还原自上次提交以来对防火墙配置所做的暂挂更改。防火墙提供按管理员或位置筛选暂挂更改的选项。位置可以是特定虚拟系统、共享策略和对象，或共享设备和网络设置。如果您已为比当前运行配置更早的待选配置保存快照文件（请参阅保存并导出防火墙配置），还可以还原到该快照。还原到快照可以还原在最后一次提交之前存在的候选配置。无论您何时提交更改，防火墙会自动保存运行中配置的新版本，您亦可随时还原至任一版本。

- 还原到当前运行的配置（文件名为 running-config.xml）。

  此操作将撤销自上次提交之后，对待选配置所作的更改。

  要还原所有管理员所做的所有更改，请执行以下步骤之一：

  - 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），**Revert to running configuration**（还原到正在运行的配置），然后单击 **Yes**（是）确认操作。
  - 使用已分配给超级用户角色或管理员角色配置文件的管理帐户登录防火墙，并启用 **Commit For Other Admins**（为其他管理员提交）权限。然后在 Web 界面顶部选择**Config**（配置）> **Revert Changes**（还原更改），选择 **Revert All Changes**（还原所有更改），并 **Revert**（还原）。

  要仅还原待选配置的特定更改：

  1. 使用具有角色权限的管理帐户登录到防火墙，以还原所需更改。

     控制提交操作的权限也可控制还原操作。

  2. 在 Web 界面顶部选择 **Config**（配置）> **Revert Changes**（还原更改）。
  3. 选择 **Revert Changes Made By**（所作更改还原依据）。
  4. 要按管理员筛选还原范围，请单击 **<administrator-name>**，选择管理员，然后单击 **OK**（确定）。
  5. 要按位置筛选还原范围，请清除要排除的任何位置。
  6. **Revert**（还原）更改。


© 2019 Palo Alto Networks, Inc.

- 还原到待选配置的默认快照。

  这是您单击 Web 界面顶部 **Config**（配置）> **Save Changes**（保存更改）时创建或替换的快照。

  1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）并 **Revert to last saved configuration**（还原到上次保存的配置）。
  2. 单击 **Yes**（是）以确认操作。
  3. （可选）单击 **Commit**（提交）以使用快照覆写正在运行的配置。

- 还原到存储在防火墙上运行配置的先前版本。

  无论您何时提交配置更改，防火墙都会创建版本。

  1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）并 **Load configuration version**（加载配置版本）。
  2. 选择一个配置 **Version**（版本），单击 **OK**（确定）。
  3. （可选）单击 **Commit**（提交）以使用您刚刚还原的版本覆写正在运行的配置。

- 还原到以下之一：

  - 您之前导入的当前运行配置的自命名版本
  - 自命名待选配置快照（而非默认快照）

  1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），并单击 **Load named configuration snapshot**（加载已命名配置快照）。
  2. 选择快照 **Name**（名称），单击 **OK**（确定）。
  3. （可选）单击 **Commit**（提交）以使用快照覆写正在运行的配置。

- 还原到之前导出至外部主机的运行中或待选配置。

  1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），并单击 **Import named configuration snapshot**（导入已命名配置快照），**Browse**（浏览）至位于外部主机的配置文件，单击 **OK**（确定）。
  2. 单击 **Load named configuration snapshot**（加载已命名配置快照），选择您导入的配置文件 **Name**（名称），单击 **OK**（确定）。
  3. （可选）单击 **Commit**（提交）以使用您刚刚导入的快照覆写正在运行的配置。

- 还原您从防火墙导出的状态信息。

  除正在运行的配置之外，状态信息将包含从 Panorama 推送的设备组和模板设置。如果防火墙为 GlobalProtect 门户，则此状态信息包也会包含证书信息、卫星列表，以及卫星身份验证信息。如果您更换了防火墙或门户，您可通过导入状态包来还原与此更换操作相关的信息。

  导入状态信息：

  1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），并单击 **Import device state**（导入设备状态），然后 **Browse**（浏览）至状态包，单击 **OK**（确定）。
  2. （可选）单击 **Commit**（提交）以应用导入状态信息至正在运行的配置。



© 2019 Palo Alto Networks, Inc.

# 管理防火墙管理员

管理帐户为 Palo Alto Networks 防火墙的管理员指定角色和身份验证方法。每个 Palo Alto Networks 防火墙都已预定义一个默认管理帐户 (admin)，该帐户具有对防火墙的完全读写权限（也称为超级用户权限）。



作为最佳实践，请为需要访问防火墙管理或报告功能的每个用户创建一个单独的管理帐户。这样可以更好地保护防火墙，防止未经授权即对其进行配置，并且可以记录每位管理员的操作。务必按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙和其他安全设备的管理访问权限。

- 管理角色类型
- 配置管理角色配置文件
- 管理身份验证
- 配置管理帐户和身份验证

## 管理角色类型

角色定义相关管理员对防火墙所具备的访问权限类型。管理员类型为：

- 基于角色 — 要对 Web 界面、CLI 和 XML API 的功能区域提供更精细的访问权限控制，您可以配置自定义角色。例如，可以为操作人员创建一个可访问 Web 界面的防火墙和网络配置区域的管理员角色配置文件，并为安全管理员另外创建一个可访问安全策略定义、日志和报告的配置文件。在具有多个虚拟系统的防火墙上，您可以选择将角色定义为所有虚拟系统或特定虚拟系统的访问。在产品增加新功能后，您必须更新拥有相应访问特权的角色：防火墙不会自动添加新功能至各自定义角色。有关可为自定义管理员角色配置的权限的详细信息，请参阅引用：Web 界面管理员访问。
- 动态 — 内置角色，可提供对防火墙的访问权限。添加新功能时，防火墙会自动更新动态角色的定义；您不需要手动更新这些角色。下表列出了与动态角色相关的访问权限。

| 动态角色 | 权限 |
|---|---|
| 超级用户 | 对防火墙有完全访问权，且可定义新管理员账户和虚拟系统。您必须拥有超级用户权限才能用其创建管理用户。 |
| 超级用户（只读） | 防火墙只读访问权限。 |
| 设备管理员 | 对所有防火墙有完全访问权，但无权定义新账户或虚拟系统。 |
| 设备管理员（只读） | 对所有防火墙设置有只读访问权，但不包括密码配置文件（无访问权）和管理员账户（仅登录账户可见）。 |
| 虚拟系统管理员 | 在防火墙上访问所选虚拟系统，以创建和管理虚拟系统的特定方面。虚拟系统管理员无法访问网络接口、VLAN、虚拟线路、虚拟路由器、IPSec 隧道、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。 |
| 虚拟系统管理员（只读） | 在防火墙上只读访问所选虚拟系统，以及虚拟系统的特定方面。只读权限的虚拟系统管理员无法访问网络接口、VLAN、虚拟线路、虚拟路由器、IPSec 隧道、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。 |



© 2019 Palo Alto Networks, Inc.

## 配置管理角色配置文件

管理员角色配置文件可用于定义粒度管理访问权限，以确保保护敏感企业信息和最终用户隐私。

最佳实践是创建 *Admin Role*（管理员角色）配置文件，从而仅允许管理员以执行作业的目的访问其需要访问的管理界面。

STEP 1 | 选择 **Device**（设备）> **Admin Roles**（管理角色），然后单击 **Add**（添加）。

STEP 2 | 输入 **Name**（名称）以标识角色。

STEP 3 | 对于 **Role**（角色）的范围，选择 **Device**（设备）或 **Virtual System**（虚拟系统）。

STEP 4 | 在 **Web UI** 和 **REST API** 选项卡上，单击每个功能区域的图标以切换到目标设置："启用"、"只读"或"禁用"。对于 **XML API** 选项卡，选项为"启用"或"禁用"。有关 **Web UI** 选项的详细信息，请参阅 Web 界面访问权限。

STEP 5 | 选择 **Command Line**（命令行）选项卡，然后选择 CLI 访问选项。**Role**（角色）范围控制以下可用选项：

- **Device**（设备）角色 — **superuser**（超级用户）、**superreader**（超级读者）、**deviceadmin**（设备管理员）、**devicereader**（设备读者）或 **None**（无）
- **Virtual System**（虚拟系统）角色 — **vsysadmin**（系统管理员）、**vsysreader**（系统读者）或 **None**（无）

STEP 6 | 单击 **OK**（确定）保存配置文件。

STEP 7 | 为管理员分配角色。请参阅配置防火墙管理员帐户。

## 管理身份验证

您可以为防火墙管理员配置以下类型的身份验证和授权（角色和访问域分配）：

| 身份验证方法 | 身份验证方法 | 说明 |
|---|---|---|
| 本地 | 本地 | 管理帐户凭证和身份验证机制对防火墙而言均属于本地。您可以定义属于防火墙本地的帐户（带或不带数据库）— 请参阅本地身份验证，以了解使用本地数据库的优缺点。您可以使用防火墙来管理角色分配，但不支持访问域。有关详细信息，请参阅为防火墙管理员配置本地或外部身份验证。 |
| SSH 密钥 | 本地 | 管理帐号对防火墙而言属于本地，但对 CLI 的身份验证却基于 SSH 密钥。您可以使用防火墙来管理角色分配，但不支持访问域。有关详细信息，请参阅配置基于 SSH 密钥的管理员 CLI 身份验证。 |
| 证书 | 本地 | 管理帐号对防火墙而言属于本地，但对 Web 界面的身份验证却基于客户端证书。您可以使用防火墙来管理角色分配，但不支持访问域。有关详细信息，请参阅配置基于证书的管理员 Web 界面身份验证。 |
| 外部服务 | 本地 | 防火墙本地定义的管理帐户作为外部多重因素身份验证、SAML、Kerberos、TACACS+、RADIUS 或 LDAP 服务器上的定义帐户引用。外部服务器执行身份验证。您可以使用防火墙来管理角色分配，但不 |



© 2019 Palo Alto Networks, Inc.

| 身份验证方法 | 身份验证方法 | 说明 |
| --- | --- | --- |
| | | 支持访问域。有关详细信息，请参阅为防火墙管理员配置本地或外部身份验证。 |
| 外部服务 | 外部服务 | 管理帐户在外部 SAML、TACACS+ 或 RADIUS 服务器上定义。服务器执行身份验证和授权。对于授权，您可以在 TACACS+ 或 RADIUS 服务器上定义供应商特定属性 (VSA)，或在 SAML 服务器上定义 SAML 属性。PAN-OS 将属性映射到在防火墙上定义的管理员角色、访问域、用户组和虚拟系统。有关详细信息，请参阅：<br>• 配置 SAML 身份验证<br>• 配置 TACACS+ 身份验证<br>• 配置 RADIUS 身份验证 |

# 配置管理帐户和身份验证

如果您已配置身份验证配置文件（请参阅配置身份验证配置文件和序列）或您不需要为身份验证管理员配置，则可以配置防火墙管理员帐户。或者，您可以执行以下列出的其中一项其他流程，配置管理账户已进行特定类型的身份验证。

- 配置防火墙管理员帐户
- 为防火墙管理员配置本地或外部身份验证
- 配置 Web 界面的基于证书的管理员身份验证
- 配置 CLI 的 SSH 基于密钥的管理员身份验证
- 配置 API 密钥生命周期

## 配置防火墙管理员帐户

管理帐户指定防火墙管理员角色和身份验证方法。用于分配角色和执行身份验证的服务决定是否在防火墙、外部服务器或两者上添加帐户（请参阅管理身份验证）。如果身份验证方法取决于本地防火墙数据库或外部服务，则必须在添加管理帐户之前配置身份验证配置文件（请参阅配置管理帐户和身份验证）。如果您已配置身份验证配置文件，或者您将使用不含防火墙数据库的本地身份验证，请执行以下步骤，在防火墙上添加管理帐户。

为需要访问防火墙管理或报告功能的每个用户创建一个单独的管理帐户。这样可以更好地保护防火墙，防止未经授权即对其进行配置，并且可以记录每位管理员的操作。

务必按照安全管理访问的最佳实践确保您以防止成功攻击的方式保护对防火墙和其他安全设备的管理访问权限。

STEP 1 | 选择 **Device**（设备）> **Administrators**（管理员），并 **Add**（添加）帐户。

STEP 2 | 输入用户 **Name**（名称）。

如果防火墙使用本地用户数据库来对帐户进行身份验证，请输入您为数据库中帐户指定的名称（请参阅将用户组添加到本地数据库。）

STEP 3 | 如果为管理员配置其中之一，请选择 **Authentication Profile**（身份验证配置文件）或序列。

如果防火墙对帐户使用不含本地用户数据库的本地身份验证，请选择 **None**（无）（默认），并输入 **Password**（密码）。

STEP 4 | 选择 **Administrator Type**（管理员类型）。



© 2019 Palo Alto Networks, Inc.

如果为用户配置了自定义角色，选择 **Role Based**（基于角色），并选择管理员角色 **Profile**（配置文件）。或者，选择 **Dynamic**（动态）（默认）并选择动态角色。如果动态角色为 **virtual system administrator**（虚拟系统管理员），添加一个或多个虚拟系统管理员有权管理的虚拟系统。

STEP 5 | （可选）为管理员选择 **Password Profile**（密码配置文件），以便防火墙在无本地用户数据库的情况下进行本地身份验证。有关详细信息，请参阅定义密码配置文件。

STEP 6 | 单击 **OK**（确定）和 **Commit**（提交）。

## 为防火墙管理员配置本地或外部身份验证

您可以使用本地身份验证和外部身份验证服务来对访问防火墙的管理员进行身份验证。这些身份验证方法提示管理员响应一个或多个身份验证质询，例如输入用户名和密码的登录页面。



如果您使用外部服务来管理身份验证和授权（角色和访问域分配），请参阅：

- 配置 SAML 身份验证
- 配置 TACACS+ 身份验证
- 配置 RADIUS 身份验证

要对没有质询-响应机制来对管理员进行身份验证，您可以配置基于证书的管理员 Web 界面身份验证和配置基于 SSH 密钥的管理员 CLI 身份验证。

STEP 1 | （仅限外部身份验证）将防火墙与外部服务器相连接，以对管理员身份进行验证。

配置服务器配置文件：

- 添加 RADIUS 服务器配置文件。

  如果防火墙通过 RADIUS 与多重因素身份验证 (MFA) 服务集成，则必须添加 RADIUS 服务器配置文件。在这种情况下，MFA 服务提供所有身份验证因素（质询）。如果防火墙通过供应商 API 与 MFA 服务集成，您仍然可以使用 RADIUS 服务器配置文件作为第一个因素，但还需要 MFA 服务器配置文件作为其他因素。
- 添加 MFA 服务器配置文件。
- 添加 TACACS+ 服务器配置文件。
- 添加 SAML IdP 服务器配置文件。您不能将 Kerberos 单点登录 (SSO) 与 SAML SSO 组合；您只能使用一种类型的 SSO 服务。
- 添加 Kerberos 服务器配置文件。
- 添加 LDAP 服务器配置文件。

STEP 2 | （仅限本地数据库身份验证）配置属于防火墙本地的用户数据库。

1. 将用户帐户添加到本地数据库。
2. （可选）将用户组添加到本地数据库。

STEP 3 | （仅限本地身份验证）定义密码复杂度和过期设置。

这些设置增加了攻击者得到密码的难度，从而有助于防止防火墙的未授权访问。

1. （确定所有本地管理员帐户的全局密码复杂性和过期设置。这些设置不适用于您指定密码哈希（而非密码）的本地数据库帐户（请参阅本地身份验证）。
   1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑最低密码复杂性设置。
   2. 选择 **Enabled**（启用）。
   3. 定义密码设置并单击 **OK**（确定）。
2. 定义密码配置文件。



© 2019 Palo Alto Networks, Inc.

将配置文件分配给要覆盖全局密码到期设置的管理员帐户。配置文件仅适用于与本地数据库不相关联的帐户（请参阅本地身份验证）。

1. 选择 **Device**（设备）> **Password Profiles**（密码配置文件），**Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 定义密码过期设置并单击 **OK**（确定）。

STEP 4 | （仅限 Kerberos SSO）创建 Kerberos 密钥表。

密钥表是包含防火墙的 Kerberos 帐户信息的文件。要支持 Kerberos SSO，您的网络必须具有 Kerberos 基础架构。

STEP 5 | 配置身份验证配置文件。



如果您的管理帐户存储在多种类型的服务器上，您可以为每种类型的服务器创建一个身份验证配置文件，并将所有配置文件添加到身份验证序列。

配置身份验证配置文件和序列。在身份验证配置文件中，指定身份验证服务的 **Type**（类型）和相关设置：

- 外部服务 — 选择外部服务器 **Type**（类型），然后选择您为其创建的 **Server Profile**（服务器配置文件）。
- 本地数据库身份验证 — 将 **Type**（类型）设置为 **Local Database**（本地数据库）。
- 无数据库的本地身份验证 — 将 **Type**（类型）设置为 **None**（无）。
- **Kerberos SSO** — 指定 **Kerberos Realm**（**Kerberos** 域）并 **Import**（导入）**Kerberos Keytab**（**Kerberos** 密钥表）。

STEP 6 | 分配身份验证配置文件或序列至管理员帐户。

1. 配置防火墙管理员帐户。
   - 分配您配置的 **Authentication Profile**（身份验证配置文件）或序列。
   - （仅限本地数据库身份验证）指定您添加到本地数据库的用户帐户 **Name**（名称）。
2. **Commit**（提交）更改。
3. （可选）测试身份验证服务器连接，验证防火墙是否可以使用身份验证配置文件来对管理员进行身份验证。

## 配置 *Web* 界面的基于证书的管理员身份验证

作为一种比基于密码的面向防火墙 Web 界面的身份验证更加安全的替代性方案，您可以为处于防火墙本地的管理员帐户配置基于认证的身份验证。基于证书的身份验证执行数字签名（而非密码）的交换和验证。



为任何管理员配置基于证书的身份验证都会禁用防火墙上所有管理员的用户名/密码登录；此后管理员需要使用证书进行登录。

STEP 1 | 在防火墙上生成证书颁发机构 (CA) 证书。

您将使用该 CA 证书对每个管理员的客户端证书进行签名。

创建自签名根 CA 证书。



或者，从企业 *CA* 或第三方 *CA* 导入证书和私钥 。

STEP 2 | 配置确保对 Web 界面进行安全访问所用的证书配置文件。



© 2019 Palo Alto Networks, Inc.

配置证书配置文件。

- 将 **Username Field**（用户名字段）设置为 **Subject**（对象）。
- 在 CA 证书部分，**Add**（添加）您刚刚创建或导入的 **CA Certificate**（**CA** 证书）。

STEP 3 | 配置防火墙，以便使用证书配置文件对管理员进行身份验证。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 Authentication Settings（身份验证设置）。
2. 选择您为身份验证管理员创建的 **Certificate Profile**（证书配置文件）并单击 **OK**（确定）。

STEP 4 | 配置管理员帐户使用客户端证书身份验证。

对于所有访问防火墙 Web 界面的管理员，配置防火墙管理员帐户，然后选择 **Use only client certificate authentication**（仅使用客户端证书身份验证）。

如果您已经部署了企业 CA 生成的客户端证书，请跳转至步骤 8。否则，请前往步骤 5。

STEP 5 | 为每个管理员生成客户端证书。

生成证书。在 **Signed By**（签名者）下拉菜单中，选择自签名根 CA 证书。

STEP 6 | 导出客户端证书。

1. 导出证书和私钥。
2. **Commit**（提交）更改。防火墙会重启并终止登录会话。此后，管理员只能从使用您生成的客户端证书的客户端系统对 Web 界面进行访问。

STEP 7 | 将客户端证书导入到要访问 Web 界面的每个管理员的客户端系统。

请参阅您的 Web 浏览器文档。

STEP 8 | 验证管理员是否可以对 Web 界面进行访问。

1. 在具备用户端证书的电脑浏览器中打开 IP 地址。
2. 收到提示时，选择您导入的证书，然后单击 **OK**（确定）。浏览器随即显示证书警告。
3. 将该证书添加到浏览器异常列表。
4. 单击 **Login**（登录）。会显示 Web 界面，不提示您输入用户名或密码。

## 配置 *CLI* 的 *SSH* 基于密钥的管理员身份验证

对于使用安全外壳 (SSH) 对 Palo Alto Networks 防火墙的 CLI 进行访问的管理员而言，SSH 密钥提供相较于密码更为安全的身份验证方法。SSH 密钥提供两要素身份验证（密钥和通行码）选项，且不通过网络发送密码，基本上排除了所有蛮力攻击风险。SSH 密钥还会启用自动化脚本对 CLI 进行访问。

STEP 1 | 使用 SSH 密钥生成工具在管理员的客户端系统上创建非对称密钥对。

支持的密钥格式为 IETF SECSH 和开放式 SSH。支持的算法为 DSA（1,024 位）和 RSA（768-4,096 位）。

关于生成密钥对所需的命令，请参阅您的 SSH 客户端文档。

公钥和私钥是两个分开的文件。将这两个文件保存到防火墙可以访问的位置。为了增强安全性，请输入加密私钥的口令。登录过程中，防火墙会提示管理员输入此口令。

STEP 2 | 配置管理员帐户使用公钥身份验证。

1. 配置防火墙管理员帐户。



© 2019 Palo Alto Networks, Inc.

- 如果 SSH 密钥身份验证失败，请配置要用来作为回退方法的身份验证方法。如果您已配置了管理员的 **Authentication Profile**（身份验证配置文件），请在下拉列表中选择此文件。如果您选择 **None**（无），则必须输入 **Password**（密码）并 **Confirm Password**（确认密码）。
- 选择 **Use Public Key Authentication (SSH)**（使用公钥身份验证 **(SSH)**），然后 **Import Key**（导入密钥），**Browse**（浏览）到您刚才生成的公钥，然后单击 **OK**（确定）。

2. **Commit**（提交）更改。

STEP 3 | 配置 SSH 客户端以使用私钥对防火墙进行身份验证。

在管理员的客户端系统上执行这项任务。关于步骤，请参阅您的 SSH 客户端文档。

STEP 4 | 验证管理员是否可以使用 SSH 密钥身份验证对防火墙 CLI 进行访问。

1. 使用管理员的用户端系统的浏览器前往防火墙 IP 地址。
2. 以管理员身份登录到防火墙的 CLI。输入用户名后，您会看到以下输出内容（以密钥值为例）：

```
Authenticating with public key “dsa-key-20130415”
```

3. 如果收到提示，请输入您在创建密钥时定义的密码。

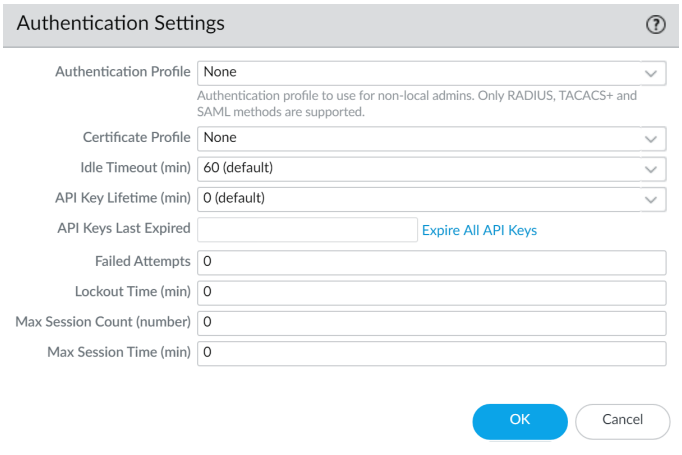
## 配置 *API* 密钥生命周期

防火墙和 Panorama 上的 API 密钥让您可以验证对 XML API 和 REST API 的 API 调用。由于这些密钥授予了对防火墙和 Panorama 访问权限，而该类权限是安全状态的关键元素，最好的做法是规定 API 密钥生命周期以实施密钥定期轮换。在规定密钥生命周期后，当您重新生成 API 密钥时，每个密钥都是唯一的。

除了设置提醒您定期重新生成密钥的密钥生命周期外，您也可以在一个或多个密钥泄露时，撤销当前有效的所有 API 密钥。撤销密钥将使当前的所有有效密钥失效。

STEP 1 | 选择**Device**（设备）> **Setup**（设置）> **Management**（管理）。

STEP 2 | 编辑验证设置以指定 **API Key Lifetime (min)**（**API** 密钥生命周期）（分钟）。




设置 API 密钥生命周期以提供泄露保护，并减少意外暴露的影响。默认情况下，API 密钥生命周期被设为 0，意味着该密钥永远不会过期。为了确保您的密钥频繁轮换，且在重新生成时每个密钥都是唯一的，您必须指定范围在 1-525600 分钟之间的有效期。请参考您企业的审计和合规政策，以确定您应如何指定 API 密钥有效生命周期。

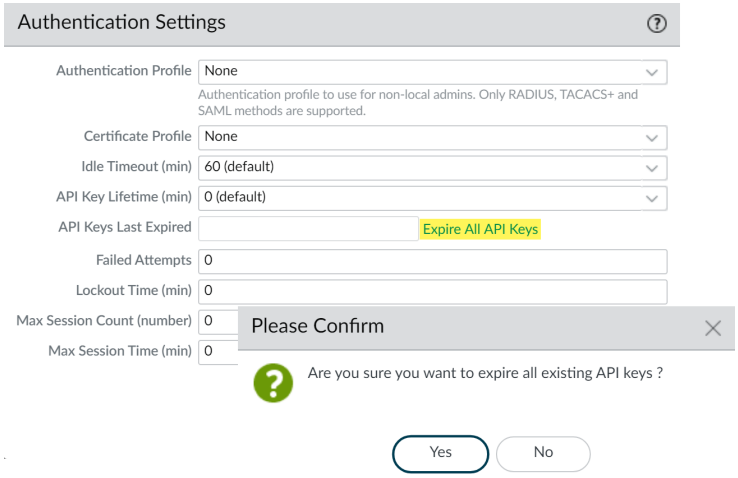
STEP 3 | **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

STEP 4 | （要撤销所有 API 密钥）选择 **Expire all API Keys**（让所有 **API** 密钥过期）以重置当前有效的 API 密钥。

如果您刚设置过密钥生命周期，并希望重置所有 API 密钥以符合新的条款，可以使所有现有密钥过期。




确认后，密钥将被撤销，您可以查看 **API Keys Last Expired**（最近过期的 **API** 密钥）的时间戳。



© 2019 Palo Alto Networks, Inc.

# 参考资料：Web 界面管理员访问

您可为整道防火墙或一个以上的虚拟系统（位于支持多个虚拟系统的平台）配置权限。在 **Device**（设备）或 **Virtual System**（虚拟系统）指定值中，您可以配置自定义管理员角色的权限，这些权限比动态管理员角色相关的已确定权限更精确。

对权限进行详细的配置可以确保低级管理员无法访问某些信息。您可以为防火墙管理员（请参阅配置防火墙管理员帐户）、Panorama 管理员或设备组以及模板管理员（请参阅《Panorama 管理员指南》）创建自定义角色。您可将管理员角色应用至您可分配一个或多个虚拟系统的基于角色的自定义管理员帐户。以下主题介绍了您可以为自定义管理员角色配置的权限。

- Web 界面访问权限
- Panorama Web 界面访问权限

## Web 界面访问权限

如果要阻止基于角色的管理员访问 Web 界面上的特定选项卡，可禁用选项卡，这样使得管理员在使用关联的基于角色的管理帐户登录后将看不到选项卡。例如，可以为操作人员创建只可用于访问 **Device**（设备）和 **Network**（网络）选项卡的管理角色配置文件，并为安全管理员另外创建可用于访问 **Object**（对象）、**Policy**（策略）和 **Monitor**（监控）选项卡的配置文件。

可在 **Device**（设备）或 **Virtual System**（虚拟系统）单选按钮所定义的 **Device**（设备）级别或 **Virtual System**（虚拟系统）级别应用管理员角色。如果选择 **Virtual System**（虚拟系统），则分配该配置文件的管理员只能访问为其分配的虚拟系统。此外，对该管理员而言，仅**Device**（设备）> **Setup**（设置）> **Services**（服务）> **Virtual Systems**（虚拟系统）选项卡可用，**Global**（全局）选项卡不可用。

以下主题描述如何为 Web 界面的不同部分设置管理员角色权限：

- 定义对 Web 界面选项卡的访问
- 提供对监控选项卡的粒度访问
- 提供对策略选项卡的粒度访问
- 提供对对象选项卡的粒度访问
- 提供对网络选项卡的粒度访问
- 提供对设备选项卡的粒度访问
- 定义管理角色配置文件中的用户隐私设置
- 限制管理员访问提交和验证功能
- 提供对全局设置的粒度访问
- 提供对 Panorama 选项卡的粒度访问控制

### 定义对 *Web* 界面选项卡的访问

下表介绍了可以分配给管理员角色配置文件的顶级访问权限（**Device**（设备）> **Admin Roles**（管理员角色））。您可以在 Web 界面的顶级选项卡上启用、禁用或定义只读访问权限。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| 仪表盘 | 控制访问 **Dashboard**（仪表板）选项卡。如果禁用此权限，管理员将看不到该选项卡，且将无法访问所有仪表盘小组件。 | 是 | 否 | 是 |
| ACC | 控制访问应用程序命令中心 (ACC)。如果禁用此权限，**ACC** 选项卡将不会显示在 Web 界面中。请记住，如果想要在仍能够访问 ACC 的同时保 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 护用户隐私，可以禁用 **Privacy**（隐私）> **Show Full IP Addresses**（显示完整 IP 地址）选项和/或 **Show User Names In Logs And Reports**（显示日志和报告中的用户名）选项。 | | | |
| 监视 | 控制访问 **Monitor**（监控）选项卡。如果禁用此权限，管理员将看不到 **Monitor**（监控）选项卡，且将无法访问任何日志、数据包捕获、会话信息、报告或 App Scope。要更精确地控制管理员可以看到的监控信息，保留启用 Monitor（监控）选项，然后启用或禁用选项卡上的特定节点，如提供对监控选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 数量 | 控制访问 **Policies**（策略）选项卡。如果禁用此权限，管理员将看不到 **Policies**（策略）选项卡，且将无法访问任何策略信息。要更精确地控制管理员可以看到的策略信息（如允许访问特定策略类型或只读访问策略信息），保留启用 **Policies**（策略）选项，然后启用或禁用选项卡上的特定节点，如提供对策略选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 对象 | 控制访问 **Objects**（对象）选项卡。如果禁用此权限，管理员将看不到 **Objects**（对象）选项卡，且将无法访问任何对象、安全配置文件、日志转发配置文件、解密配置文件或时间表。要更精确地控制管理员可以看到的对象信息，保留启用 **Objects**（对象）选项，然后启用或禁用选项卡上的特定节点，如提供对对象选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 网络 | 控制访问 **Network**（网络）选项卡。如果禁用此权限，管理员将看不到 **Network**（网络）选项卡，且将无法访问任何界面、区域、VLAN、Virtual Wire、虚拟路由器、IPsec 隧道、DHCP、DNS 代理、GlobalProtect、QoS 配置信息或网络配置文件。要更精确地控制管理员可以看到的对象信息，保留启用 **Network**（网络）选项，然后启用或禁用选项卡上的特定节点，如提供对网络选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 设备 | 控制访问 **Device**（设备）选项卡。如果禁用此权限，管理员将看不到**Device**（设备）选项卡，且将无法访问任何设备范围内配置信息，如 User-ID、高可用性、服务器配置文件或证书配置信息。要更精确地控制管理员可以看到的对象信息，保留启用 **Objects**（对象）选项，然后启用或禁用选项卡上的特定节点，如提供对设备选项卡的粒度访问中所述。<br><br>您无法允许基于角色的管理员访问 *Admin Roles*（管理角色）或 *Administrators*（管理员）节点， | 是 | 否 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 即使您能够完全访问 *Device*（设备）选项卡。 | | | |

## 提供对监控选项卡的粒度访问

在某些情况下，您可能希望允许管理员查看 **Monitor**（监控）选项卡的一部分但并非所有区域。例如，您可能想要限制管理员只能操作配置和系统日志，因为它们不包含敏感的用户数据。尽管本部分的管理员角色定义指定了管理员可以看到的 **Monitor**（监控）选项卡区域，但您也可以结合使用本部分的权限和隐私权限，如禁用查看日志和报告中的用户名的功能。但是，需要记住一点的是任何系统生成的报告仍将会显示用户名和 IP 地址，即使您已在角色中禁用该功能。由于此原因，如果您不想让管理员看到任何私人用户信息，则应按下表中的详细所述禁用访问特定报告。

下表列出了 **Monitor**（监控）选项卡访问权限级别以及可用的管理员角色。



设备组和模板角色只能看到分配给上述角色的位于访问域中的设备组的日志数据。

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- | --- |
| 监视 | 启用或禁用访问 **Monitor**（监控）选项卡。如果禁用此权限，管理员将看不到该选项卡或任何相关的日志或报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 日志 | 启用或禁用访问所有日志文件。也可以保留启用此权限，然后禁用您不想让管理员查看的特定日志。请记住，如果想要在仍然能够访问一个或多个日志的同时保护用户隐私，可以禁用 **Privacy**（隐私）> **Show Full IP Addresses**（显示完整 IP 地址）选项和/或 **Show User Names In Logs And Reports**（显示日志和报告中的用户名）选项。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 通信 | 指定管理员是否可以查看流量日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 威胁 | 指定管理员是否可以查看威胁日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| URL 筛选 | 指定管理员是否可以查看 URL 筛选日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| WildFire 提交内容 | 指定管理员是否可以查看 WildFire 日志。这些日志只有在拥有 WildFire 提交时才可用。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 数据筛选 | 指定管理员是否可以查看数据筛选日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| HIP 匹配 | 指定管理员是否可以查看 HIP 匹配日志。HIP 匹配日志只有在拥有 GlobalProtect 许可证（订阅）时才可用。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| GlobalProtect | 指定管理员是否可以查看 GlobalProtect 日志。这些日志只有在拥有 GlobalProtect 许可证（订阅）时才可用。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| User-ID | 指定管理员是否可以查看 User-ID 日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| GTP | 指定移动网络运营商是否可以查看 GTP 日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 隧道检测 | 指定管理员是否可以查看隧道检测日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| SCTP | 指定移动网络运营商是否可以查看流控制传输协议 (SCTP)日志。<br>  <br>您必须先在 *Panorama*（*Device*（设备）> *Setup*（设置）> *Management*（管理））上启用 *SCTP*，然后才能控制管理员访问 *SCTP* 日志、自定义报告或预定义报告以获取 *Panorama* 和设备组/模板。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 配置 | 指定管理员是否可以查看配置日志。 | 防火墙：是 | 是 | 否 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | | Panorama：是<br>设备组/模板：否 | | | |
| system | 指定管理员是否可以查看系统日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| 警报 | 指定管理员是否可以查看系统生成的警告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 身份验证 | 指定管理员是否可以查看身份验证日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| 自动关联引擎 | 启用或禁用访问关联对象和防火墙上生成的关联事件日志。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 关联对象 | 指定管理员是否可以查看和启用/禁用关联对象。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 关联事件 | 指定管理员权限 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 数据包捕获 | 指定管理员是否可以从 **Monitor**（监控）选项卡查看数据包捕获 (pcaps)。请记住，数据包捕获是原始流量数据，因此可能包含用户的 IP 地址。禁用 **Show Full IP Addresses**（显示完整 **IP** 地址）权限将不会混淆 pcap 中的 IP 地址，因此如果您担心用户隐私，则应禁用 Packet Capture（数据包捕获）权限。 | 防火墙：是<br>Panorama：否<br>设备组/模板：否 | 是 | 是 | 是 |
| 应用程序范围 | 指定管理员是否可以查看 App Scope 可见性和分析工具。启用 App Scope 可启用访问所有的 **App Scope** 图表。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 会话浏览器 | 指定管理员是否可以浏览和筛选当前正在防火墙上运行的会话。请记住，会话浏览器显示的是原始流量数据，因此可能包含用户的 IP 地址。禁用 | 防火墙：是<br>Panorama：否 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | **Show Full IP Addresses**（显示完整 IP 地址）权限将不会混淆会话浏览器中的 IP 地址，因此如果您担心用户隐私，则应禁用 **Session Browser**（会话浏览器）权限。 | 设备组/模板：否 | | | |
| 阻止 IP 列表 | 指定管理员是否可以查看阻止列表（启用或只读）并从列表中删除条目（启用）。如果禁用该设置，管理员将无法从阻止列表中查看或删除条目。 | 防火墙：是<br>Panorama: under Context Switch UI：是<br>模板：是 | 是 | 是 | 是 |
| Botnet | 指定管理员是否可以生成和查看 Botnet 分析报告或在只读模式下查看 Botnet 报告。禁用 **Show Full IP Addresses**（显示完整 IP 地址）权限将不会混淆调度的 Botnet 报告中的 IP 地址，因此如果您担心用户隐私，则应禁用 **Botnet** 权限。 | 防火墙：是<br>Panorama：否<br>设备组/模板：否 | 是 | 是 | 是 |
| PDF 报告 | 启用或禁用访问所有 PDF 报告。也可以保留启用此权限，然后禁用您不想让管理员查看的特定 PDF 报告。请记住，如果想要在仍然能够访问一个或多个报告的同时保护用户隐私，可以禁用 **Privacy**（隐私）> **Show Full IP Addresses**（显示完整 IP 地址）选项和/或 **Show User Names In Logs And Reports**（显示日志和报告中的用户名）选项。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 管理 PDF 摘要 | 指定管理员是否可以查看、添加或删除 PDF 摘要报告定义。凭借只读访问，管理员可以查看 PDF 摘要报告定义，但不能添加或删除。如果禁用此选项，管理员既不可以查看报告定义也不可以添加/删除。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| PDF 摘要报告 | 指定管理员是否可以在 **Monitor**（监控）> **Reports**（报告）中查看生成的 PDF 摘要报告。如果禁用此选项，**PDF Summary Reports**（**PDF** 摘要报告）类别将不会显示在 **Reports**（报告）节点中。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 用户活动报告 | 指定管理员是否可以查看、添加或删除用户活动报告定义和下载报告。凭借只读访问，管理员可以查看用户活动报告定义，但不能添加或删除。如果禁用此选项，管理员无法查看此类别的 PDF 报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| SaaS 应用程序使用情况报告 | 指定管理员是否可以查看、添加或删除 SaaS 应用程序使用报告。凭借只读访问，管理员可以查看 SaaS 应用程序使用报告定义，但不能添加或删除。如果禁用此选项，管理员既不可以查看报告定义也不可以添加/删除。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| 报告组 | 指定管理员是否可以查看、添加或删除报告组定义。凭借只读访问，管理员可以查看报告组定义，但不能添加或删除。如果禁用此选项，管理员无法查看此类别的 PDF 报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| 电子邮件计划程序 | 指定管理员是否可以为电子邮件调度报告组。因为通过接收电子邮件生成的报告可能包含通过禁用 **Privacy**（隐私）> **Show Full IP Addresses**（显示完整 IP 地址）选项和/或 **Show User Names In Logs And Reports**（显示日志和报告中的用户名）选项无法移除的敏感用户数据，并且因为它们可能也显示管理员无法访问的日志数据，因此如果您拥有用户隐私要求，则应禁用 **Email Scheduler**（电子邮件调度程序）选项。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| 管理自定义报告 | 启用或禁用访问所有自定义报告功能。也可以保留启用此权限，然后禁用您不想让管理员查看的特定自定义报告。请记住，如果想要在仍然能够访问一个或多个报告的同时保护用户隐私，可以禁用 **Privacy**（隐私）> **Show Full IP Addresses**（显示完整 IP 地址）选项和/或 **Show User Names In Logs And Reports**（显示日志和报告中的用户名）选项。<br>  <br>调度要运行的报告（而不是按需运行）将会显示 *IP* 地址和用户信息。在这种情况下，请确保限制访问相应的报告区域。此外，自定义报告功能不会限制生成包含日志数据的报告的功能，该日志数据包含在管理员角色排除的日志中。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| Application Statistics | 指定管理员是否可以创建包括应用程序统计数据库中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 数据筛选日志 | 指定管理员是否可以创建包括数据筛选日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 威胁日志 | 指定管理员是否可以创建包括威胁日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 威胁摘要 | 指定管理员是否可以创建包括威胁摘要数据库中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 流量日志 | 指定管理员是否可以创建包括流量日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 流量摘要 | 指定管理员是否可以创建包括流量摘要数据库中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| URL 日志 | 指定管理员是否可以创建包括 URL 筛选日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| HIP 匹配 | 指定管理员是否可以创建包括 HIP 匹配日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| GlobalProtect | 指定管理员是否可以创建包括 GlobalProtect 日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| WildFire 日志 | 指定管理员是否可以创建包括 WildFire 日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| GTP 日志 | 指定移动网络运营商是否可以创建包括 GTP 日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| GTP 摘要 | 指定移动网络运营商是否可以创建包括 GTP 日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 隧道日志 | 指定管理员是否可以创建包括隧道检测日志中数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 隧道摘要 | 指定管理员是否可以创建包括隧道摘要数据库中数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| SCTP 日志 | 指定移动网络运营商是否可以创建包括 SCTP 日志中数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| SCTP 摘要 | 指定移动网络运营商是否可以创建包括 SCTP 摘要数据库中数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 用户 ID | 指定管理员是否可以创建包括 User-ID 日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 身份验证 | 指定管理员是否可以创建包括身份验证日志中的数据的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 查看计划的自定义报告 | 指定管理员是否可以查看已计划生成的自定义报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 查看预定义的应用程序报告 | 指定管理员是否可以查看应用程序报告。隐私权限不会对在 **Monitor**（监控）> **Reports**（报告）节点上可用的报告产生影响，因此如果您拥有用户隐私要求，则应禁用访问报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| 查看预定义的威胁报告 | 指定管理员是否可以查看威胁报告。隐私权限不会对在 **Monitor**（监控）> **Reports**（报告）节点上可用的报告产生影响，因此如果您拥有用户隐私要求，则应禁用访问报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 查看预定义的 URL 筛选报告 | 指定管理员是否可以查看 URL 筛选报告。隐私权限不会对在 **Monitor**（监控）> **Reports**（报告）节点上可用的报告产生影响，因此如果您拥有用户隐私要求，则应禁用访问报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 查看预定义的流量报告 | 指定管理员是否可以查看流量报告。隐私权限不会对在 **Monitor**（监控）> **Reports**（报告）节点上可用的报告产生影响，因此如果您拥有用户隐私要求，则应禁用访问报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 查看预定义的 GTP 报告 | 指定移动网络运营商是否可以查看 GTP 报告。隐私权限不会对在 **Monitor**（监控）> **Reports**（报告）节点上可用的报告产生影响，因此如果您拥有用户隐私要求，则应禁用访问报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |
| 查看预定义的 SCTP 报告 | 指定移动网络运营商是否可以查看 SCTP 报告。隐私权限不会对在 **Monitor**（监控）> **Reports**（报告）节点上可用的报告产生影响，因此如果您拥有用户隐私要求，则应禁用访问报告。 | 防火墙：是<br>Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |

## 提供对策略选项卡的粒度访问

如果在管理员角色配置文件中启用 Policy（策略）选项卡，则可以在必要时为定义的管理员角色启用、禁用或提供对该选项卡内特定节点的只读访问。通过允许访问特定策略类型，可以启用查看、添加或删除策略规则的功能。通过允许只读访问特定策略，可以允许管理员查看相应的策略规则库，但不能添加或删除规则。禁用访问特定策略类型可防止管理员查看策略规则库。

因为基于特定用户（按用户名或 IP 地址）的策略必须明确定义，因此用来禁用查看完整 IP 地址或用户名的功能的隐私设置不适用于 Policy（策略）选项卡。因此，您应只允许用户隐私限制排除的管理员访问策略选项卡。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| 安全 | 启用此权限可让管理员查看、添加和/或删除安全策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看安全策略规则库，应禁用此权限。 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| NAT | 启用此权限可让管理员查看、添加和/或删除 NAT 策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看 NAT 策略规则库，应禁用此权限。 | 是 | 是 | 是 |
| QoS | 启用此权限可让管理员查看、添加和/或删除 QoS 策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看 QoS 策略规则库，应禁用此权限。 | 是 | 是 | 是 |
| 基于策略的转发 | 启用此权限可让管理员查看、添加和/或删除基于策略的转发 (PBF) 策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看 PBF 策略规则库，应禁用此权限。 | 是 | 是 | 是 |
| 解密 | 启用此权限可让管理员查看、添加和/或删除解密策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看解密策略规则库，应禁用此权限。 | 是 | 是 | 是 |
| 隧道检测 | 启用此权限可让管理员查看、添加和/或删除隧道检测规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看隧道检测规则库，应禁用此权限。 | 是 | 是 | 是 |
| 应用程序替代 | 启用此权限可让管理员查看、添加和/或删除应用程序替代策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看应用程序替代策略规则库，应禁用此权限。 | 是 | 是 | 是 |
| 身份验证 | 启用此权限可让管理员查看、添加和/或删除身份验证策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看身份验证规则库，应禁用此权限。 | 是 | 是 | 是 |
| DoS 保护 | 启用此权限可让管理员查看、添加和/或删除强制 DoS 保护策略规则。如果您希望管理员能够查看规则但不能修改，则应将此权限设置为只读。要防止管理员查看 DoS 保护策略规则库，应禁用此权限。 | 是 | 是 | 是 |

## 提供对对象选项卡的粒度访问

对象是一个容器，用来对特定策略筛选器值（如 IP 地址、URL、应用程序或服务）进行分组以简化规则定义。例如，地址对象可能包含 DMZ 区域的 Web 和应用程序服务器的特定 IP 地址定义。

当决定是否允许将 objects（对象）选项卡作为一个整体访问时，应确定管理员是否拥有策略定义责任。如果没有，则管理员可能不需要访问该选项卡。但是，如果管理员需要创建策略，您可以启用访问该选项卡，然后提供节点级别粒度访问权限。


© 2019 Palo Alto Networks, Inc.

通过启用访问特定节点，可向管理员授予权限以查看、添加和删除相应的对象类型。授予只读访问权限可让管理查看已经定义的对象，但不能创建或删除任何对象。禁用节点可防止管理员在 Web 界面中查看节点。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| 地址 | 指定管理员是否可以查看、添加或删除在安全策略中使用的地址对象。 | 是 | 是 | 是 |
| 地址组 | 指定管理员是否可以查看、添加或删除在安全策略中使用的地址组对象。 | 是 | 是 | 是 |
| 区域 | 指定管理员是否可以查看、添加或删除在安全、解密或 DoS 策略中使用的区域对象。 | 是 | 是 | 是 |
| 应用程序 | 指定管理员是否可以查看、添加或删除在策略中使用的应用程序对象。 | 是 | 是 | 是 |
| 应用程序组 | 指定管理员是否可以查看、添加或删除在策略中使用的应用程序组对象。 | 是 | 是 | 是 |
| 应用程序筛选器 | 指定管理员是否可以查看、添加或删除应用程序筛选器以简化重复搜索。 | 是 | 是 | 是 |
| 服务 | 指定管理员是否可以查看、添加或删除在创建策略时使用的服务对象，策略用于限制应用程序可以使用的端口号。 | 是 | 是 | 是 |
| 服务组 | 指定管理员是否可以查看、添加或删除在安全策略中使用的服务组对象。 | 是 | 是 | 是 |
| 标记 | 指定管理员是否可以查看、添加或删除已在防火墙上定义的标记。 | 是 | 是 | 是 |
| GlobalProtect | 指定管理员是否可以查看、添加或删除 HIP 对象和配置文件。您可以在 GlobalProtect 级别同时限制访问两种类型的对象，或通过启用 GlobalProtect 权限和限制 HIP 对象或 HIP 配置文件访问提供粒度控制。 | 是 | 否 | 是 |
| HIP 对象 | 指定管理员是否可以查看、添加或删除用于定义 HIP 配置文件的 HIP 对象。同样，HIP 对象也可用于生成 HIP 匹配日志。 | 是 | 是 | 是 |
| 无客户端应用 | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect VPN 无客户端应用程序。 | 是 | 是 | 是 |
| 无客户端应用组 | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect VPN 无客户端应用程序组。 | 是 | 是 | 是 |
| HIP 配置文件 | 指定管理员是否可以查看、添加或删除在安全策略中使用和/或用于生成 HIP 匹配日志的 HIP 配置文件。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 外部动态列表 | 指定管理员是否可以查看、添加或删除在安全策略中使用的外部动态列表。 | 是 | 是 | 是 |
| 自定义对象 | 指定管理员是否可以查看自定义间谍软件和漏洞签名。您可以限制访问启用或禁用访问此级别的所有自定义签名，或者通过启用自定义对象权限，然后限制访问每种类型的签名提供更精确的控制。 | 是 | 否 | 是 |
| 数据模式 | 指定管理员是否可以查看、添加或删除在创建自定义漏洞保护配置文件时使用的自定义数据模式签名。 | 是 | 是 | 是 |
| 间谍软件 | 指定管理员是否可以查看、添加或删除在创建自定义漏洞保护配置文件时使用的自定义间谍软件签名。 | 是 | 是 | 是 |
| 漏洞 | 指定管理员是否可以查看、添加或删除在创建自定义漏洞保护配置文件时使用的自定义漏洞签名。 | 是 | 是 | 是 |
| URL 类别 | 指定管理员是否可以查看、添加或删除在策略中使用的自定义 URL 类别。 | 是 | 是 | 是 |
| 安全配置文件 | 指定管理员是否可以查看安全配置文件。您可以限制访问启用或禁用访问此级别的所有自定义签名，或者通过启用安全配置文件权限，然后限制访问每种类型的配置文件提供更精确的控制。 | 是 | 否 | 是 |
| 反病毒 | 指定管理员是否可以查看、添加或删除防病毒配置文件。 | 是 | 是 | 是 |
| 防间谍软件 | 指定管理员是否可以查看、添加或删除防间谍软件配置文件。 | 是 | 是 | 是 |
| 漏洞保护 | 指定管理员是否可以查看、添加或删除漏洞保护配置文件。 | 是 | 是 | 是 |
| URL 筛选 | 指定管理员是否可以查看、添加或删除 URL 筛选配置文件。 | 是 | 是 | 是 |
| 文件传送阻止 | 指定管理员是否可以查看、添加或删除文件传送阻止配置文件。 | 是 | 是 | 是 |
| WildFire 分析 | 指定管理员是否可以查看、添加或删除 WildFire 分析配置文件。 | 是 | 是 | 是 |
| 数据筛选 | 指定管理员是否可以查看、添加或删除数据筛选配置文件。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| DoS 保护 | 指定管理员是否可以查看、添加或删除 DoS 保护配置文件。 | 是 | 是 | 是 |
| GTP 保护 | 指定移动网络运营商是否可以查看、添加或删除 GTP 保护配置文件。 | 是 | 是 | 是 |
| SCTP 保护 | 指定移动网络运营商是否可以查看、添加或删除流控制传输协议 (SCTP) 保护配置文件。 | 是 | 是 | 是 |
| 安全配置文件组 | 指定管理员是否可以查看、添加或删除安全配置文件组。 | 是 | 是 | 是 |
| 日志转发 | 指定管理员是否可以查看、添加或删除日志转发配置文件。 | 是 | 是 | 是 |
| 身份验证 | 指定管理员是否可以查看、添加或删除身份验证执行对象。 | 是 | 是 | 是 |
| 解密配置文件 | 指定管理员是否可以查看、添加或删除解密配置文件。 | 是 | 是 | 是 |
| 计划 | 指定管理员是否可以查看、添加或删除将安全策略限制为某个特定日期和/或时间范围的计划。 | 是 | 是 | 是 |

## 提供对网络选项卡的粒度访问

当决定是否允许将 **Network**（网络）选项卡作为一个整体访问时，应确定管理员是否拥有网络管理责任，包括 GlobalProtect 管理。如果没有，则管理员可能不需要访问该选项卡。

您也可以在节点级别定义访问 **Network**（网络）选项卡。通过启用访问特定节点，可向管理员授予权限以查看、添加和删除相应的网络配置。授予只读访问权限可让管理员查看已经定义的配置，但不能创建或删除任何配置。禁用节点可防止管理员在 Web 界面中查看节点。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 接口 | 指定管理员是否可以查看、添加或删除接口配置。 | 是 | 是 | 是 |
| 区域 | 指定管理员是否可以查看、添加或删除区域。 | 是 | 是 | 是 |
| VLAN | 指定管理员是否可以查看、添加或删除 VLAN。 | 是 | 是 | 是 |
| 虚拟线路 | 指定管理员是否可以查看、添加或删除 Virtual Wire。 | 是 | 是 | 是 |
| 虚拟路由器 | 指定管理员是否可以查看、添加、修改或删除虚拟路由器。 | 是 | 是 | 是 |
| IPSec 隧道 | 指定管理员是否可以查看、添加、修改或删除 IPSec 隧道配置。 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| GRE 隧道 | 指定管理员是否可以查看、添加、修改或删除 GRE 隧道配置。 | 是 | 是 | 是 |
| DHCP | 指定管理员是否可以查看、添加、修改或删除 DHCP 服务器和 DHCP 中继配置。 | 是 | 是 | 是 |
| DNS 代理 | 指定管理员是否可以查看、添加、修改或删除 DNS 代理配置。 | 是 | 是 | 是 |
| GlobalProtect | 指定管理员是否可以查看、添加或修改 GlobalProtect 门户和网关代理配置。可以禁用访问所有的 GlobalProtect 功能，或才可以启用 GlobalProtect 权限，然后将角色限制为门户或网关配置区域。 | 是 | 否 | 是 |
| 门户 | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect 门户配置。 | 是 | 是 | 是 |
| 网关 | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect 网关配置。 | 是 | 是 | 是 |
| MDM | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect MDM 服务器配置。 | 是 | 是 | 是 |
| 设备块列表 | 指定管理员是否可以查看、添加、修改或删除设备阻止列表。 | 是 | 是 | 是 |
| 无客户端应用 | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect 无客户端 VPN 应用程序。 | 是 | 是 | 是 |
| 无客户端应用组 | 指定管理员是否可以查看、添加、修改或删除 GlobalProtect 无客户端 VPN 应用程序组。 | 是 | 是 | 是 |
| QoS | 指定管理员是否可以查看、添加、修改或删除 QoS 配置。 | 是 | 是 | 是 |
| LLDP | 指定管理员是否可以查看、添加、修改或删除 LLDP 配置。 | 是 | 是 | 是 |
| 网络配置文件 | 将默认状态设置为启用或禁用下面所述的所有网络设置。 | 是 | 否 | 是 |
| GlobalProtect IPSec 加密 | 控制访问 **Network Profiles**（网络配置文件）> **GlobalProtect IPSec Crypto**（**GlobalProtect IPSec** 加密）节点。<br>如果禁用此权限，管理员将看不到此节点，或可以为 GlobalProtect 网关和客户端之间的 VPN 隧道中的身份验证和加密操作配置算法。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| | 如果将权限设置为只读，管理员可以查看当前 GlobalProtect IPSe 加密配置文件，但是不能添加或编辑。 | | | |
| IKE 网关 | 控制访问 **Network Profiles**（网络配置文件）> **IKE Gateways**（**IKE** 网关）节点。如果禁用此权限，管理员将看不到 **IKE Gateways**（**IKE** 网关）节点或定义网关，其中包括与对端网关执行 IKE 协议协商必需的配置信息。<br>如果将权限状态设置为只读，可以查看当前配置的 IKE 网关，但不能添加或编辑网关。 | 是 | 是 | 是 |
| IPSec 加密 | 控制访问 **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密）节点。如果禁用此权限，管理员将看不到 **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密）节点，或者指定根据 IPSec SA 协商在 VPN 隧道中用于标识、身份验证和加密的协议和算法。<br>如果将权限状态设置为只读，可以查看当前配置的 IPSec 加密配置，但不能添加或编辑配置。 | 是 | 是 | 是 |
| IKE 加密 | 控制设备如何交换信息以确保安全通信。指定根据 IPsec SA 协商 (IKEv1 Phase-1) 在 VPN 隧道中用于标识、身份验证和加密的协议和算法。 | 是 | 是 | 是 |
| 监视 | 控制访问 **Network Profiles**（网络配置文件）> **Monitor**（监控）节点。如果禁用此权限，管理员将看不到 **Network Profiles**（网络配置文件）> **Monitor**（监控）节点，或者能够创建或编辑用于监控 IPSec 隧道和监控基于策略的转发 (PBF) 规则的下一个跃点设备的监控配置文件。<br>如果将权限状态设置为只读，可以查看当前配置的监控配置文件配置，但不能添加或编辑配置。 | 是 | 是 | 是 |
| 接口管理 | 控制访问 **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理）节点。如果禁用此权限，管理员将看不到 **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理）节点或能够指定用于管理防火墙的协议。<br>如果将权限状态设置为只读，可以查看当前配置的接口管理配置文件配置，但不能添加或编辑配置。 | 是 | 是 | 是 |
| 区域保护 | 控制访问 **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）节点。如果禁用此权限，管理员将看不到**Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）节点，或能够配置用来确定防火墙如何响应来自指定安全区域的威胁的配置文件。 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 如果将权限状态设置为只读，可以查看当前配置的区域保护配置文件配置，但不能添加或编辑配置。 | | | |
| QoS 配置文件 | 控制访问 **Network Profiles**（网络配置文件）> **QoS** 节点。如果禁用此权限，管理员将看不到 **Network Profiles**（网络配置文件）> **QoS** 节点，或能够配置用来确定如何处理 QoS 流量类的 QoS 配置文件。<br>如果将权限状态设置为只读，可以查看当前配置的 QoS 配置文件配置，但不能添加或编辑配置。 | 是 | 是 | 是 |
| LLDP 配置文件 | 控制访问 **Network Profiles**（网络配置文件）> **LLDP** 节点。如果禁用此权限，管理员将看不到 **Network Profiles**（网络配置文件）> **LLDP** 节点，或能够配置用来控制防火墙上的接口是否可以参加链路层发现协议的 LLDP 配置文件。<br>如果将权限状态设置为只读，可以查看当前配置的 LLDP 配置文件配置，但不能添加或编辑配置。 | 是 | 是 | 是 |
| BFD 配置文件 | 控制访问 **Network Profiles**（网络配置文件）> **BFD Profile**（**BFD** 配置文件）节点。如果禁用此权限，管理员将看不到 **Network Profiles**（网络配置文件）> **BFD Profile**（**BFD** 配置文件）节点或无法创建 BFD 配置文件。通过双向转发检测 (BFD) 配置文件，您可以配置 BFD 设置以应用至一个或多个静态路由或路由协议。因此，BFD 可检测失败链接或 BFD 对等设置并允许超快的故障转移。<br>如果将权限状态设置为只读，可以查看当前配置的 BFD 配置文件配置，但不能添加或编辑 BFD 配置文件。 | 是 | 是 | 是 |

## 提供对设备选项卡的粒度访问

要定义 **Device**（设备）选项卡的粒度访问权限，在创建或编辑管理员角色配置文件（**Device**（设备）> **Admin Roles**（管理员角色））时，请向下滚动到 **WebUI** 选项卡上的 **Device**（设备）节点。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 设置 | 控制访问 **Setup**（设置）节点。如果禁用此权限，管理员将看不到 **Setup**（设置）节点，且将无法访问防火墙范围内的配置信息，如管理、操作、服务、Content-ID、WildFire 或会话设置信息。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| 管理 | 控制访问 **Management**（管理）节点。如果禁用该权限，管理员将无法配置主机名、域、时区、身份验证、记录和报告、Panorama 连接、横幅、消息、密码复杂性设置等设置。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |
| 操作 | 控制访问 **Operations**（操作）和 **Telemetry and Threat Intelligence**（遥测和威胁情报）节点。如禁用此权限，则管理员将不能：<br>• 加载防火墙配置。<br>• 保存或还原防火墙配置。<br>此权限仅适用于 *Device*（设备）> *Operations*（操作）选项。保存和提交权限控制管理员是否可以通过 *Config*（配置）> *Save*（保存）和 *Config*（配置）> *Revert*（还原）选项保存或还原配置。<br>• 创建客户徽标。<br>• 配置 SNMP 监控防火墙设置。<br>• 配置统计信息服务功能。<br>• 配置 **Telemetry and Threat Intelligence**（遥测和威胁情报）设置。<br>仅具有预定义超级用户角色的管理员才能导出或导入防火墙配置并关闭防火墙。<br>仅具有预定义超级用户或设备管理员角色的管理员才能重新启动防火墙或重新启动数据面板。<br>具有仅允许访问特定虚拟系统的角色的管理员无法通过 **Device**（设备）> **Operations**（操作）选项加载、保存或还原防火墙配置。 | 是 | 是 | 是 |
| 服务 | 控制访问 **Services**（服务）节点。如果禁用该权限，管理员将无法配置 DNS 服务器、更新服务器、代理服务器、NTP 服务器等服务，也无法设置服务路由。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |
| 内容 ID | 控制访问 **Content-ID**（内容 **ID**）节点。如果禁用该权限，管理员将不能配置 URL 筛选或 Content-ID。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| WildFire | 控制访问 **WildFire** 节点。如果禁用此权限，管理员将看不能配置 WildFire 设置。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |
| 会话 | 控制访问 **Session**（会话）节点。如果禁用该权限，管理员将无法配置 TCP、UDP 或 ICMP 的会话或超时设置，也无法配置解密或 VPN 会话设置。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |
| HSM | 控制访问 **HSM** 节点。如果禁用此权限，管理员将看不能配置硬件安全模块 (HSM)。<br>如果将权限状态设置为只读，可以查看当前配置，但不能进行任何更改。 | 是 | 是 | 是 |
| 高可用性 | 控制访问 **High Availability**（高可用性）节点。如果禁用此权限，管理员将看不到 **High Availability**（高可用性）节点或访问防火墙范围内的高可用性配置信息，如常规设置信息或链接和路径监控。<br>如果将此权限状态设置为只读，管理员可以查看防火墙的高可用性配置信息，但不允许执行任何配置程序。 | 是 | 是 | 是 |
| 配置审核 | 控制访问配置审核节点。如果禁用此权限，管理员将看不到 **Config Audit**（配置审核）节点或访问任何防火墙范围内的配置信息。 | 是 | 否 | 是 |
| 管理员 | 控制访问**Administrators**（管理员）节点。此功能只能允许只读访问。<br>如果禁用此权限，管理员将看不到 **Administrators**（管理员）节点或访问有关自己管理帐户的信息。<br>如果您将该权限设置为只读，管理员将可查看其管理员帐户的配置信息。他们将看不到有关在防火墙上配置的其他管理帐户的任何信息。 | 否 | 是 | 是 |
| 管理角色 | 控制访问 **Admin Roles**（管理员角色）节点。此功能只能允许只读访问。<br>如果禁用此权限，管理员将看不到 **Admin Roles**（管理员角色）节点或访问任何有关管理员角色配置文件配置的防火墙范围内信息。<br>如果您将该权限设置为只读，您将可以查看配置于防火墙的所有管理员角色配置信息。 | 否 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 身份验证配置文件 | 控制访问 **Authentication Profile**（身份验证配置文件）节点。如果禁用此权限，管理员将看不到 **Authentication Profile**（身份验证配置文件）节点，也不能创建或编辑身份验证配置文件，从而用来指定 RADIUS、TACACS+、LDAP、Kerberos、SAML、多重因素身份验证 (MFA) 或本地数据库身份验证设置。PAN-OS 使用身份验证配置文件来对防火墙管理员和身份验证门户或 GlobalProtect 最终用户进行身份验证。<br>如果将此权限状态设置为只读，管理员可以查看 **Authentication Profile**（身份验证配置文件）信息，但不能创建或编辑身份验证配置文件。 | 是 | 是 | 是 |
| 身份验证序列 | 控制访问身份验证序列节点。如果禁用此权限，管理员将看不到身份验证序列节点，也不能创建或编辑身份验证序列。<br>如果将此权限状态设置为只读，管理员可以查看 **Authentication Profile**（身份验证配置文件）信息，但不能创建或编辑身份验证序列。 | 是 | 是 | 是 |
| 虚拟系统 | 控制访问 **Virtual Systems**（虚拟系统）节点。如果禁用此权限，管理员将看不到也不能配置虚拟系统。<br>如果将权限状态设置为只读，可以查看当前配置的虚拟系统，但不能添加或编辑配置。 | 是 | 是 | 是 |
| 共享网关 | 控制访问 **Shared Gateways**（共享网关）节点。共享网关允许虚拟系统共享用于外部通信的通用接口。<br>如果禁用此权限，管理员将看不到也不能配置共享网关。<br>如果将权限状态设置为只读，可以查看当前配置的共享网关，但不能添加或编辑配置。 | 是 | 是 | 是 |
| 用户标识 | 控制访问 **User Identification**（用户标识）节点。如果禁用此权限，管理员将无法看到 **User Identification**（用户标识）节点或访问防火墙范围内的用户标识配置信息，如用户映射、连接安全、User-ID 代理、终端服务器代理、组映射设置或身份验证门户设置。<br>如果将此权限状态设置为只读，管理员可以查看防火墙配置信息，位不允许执行任何配置程序。 | 是 | 是 | 是 |
| VM 信息源 | 控制访问 **VM Information Source**（VM 信息源）节点，可让您配置防火墙/Windows User-ID 代理以自动收集 VM 库存。如果禁用此权限，管理员将看不到 **VM Information Source**（VM 信息源）节点。 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| | 如果将此权限状态设置为只读，管理员可以查看配置的 VM 信息源，但不能添加、编辑或删除任何源。<br>  设备组和模板管理员不能使用此权限。 | | | |
| 证书管理 | 将默认状态设置为启用或禁用下面所述的所有证书设置。 | 是 | 否 | 是 |
| 证书 | 控制访问**Certificates**（证书）节点。如果禁用此权限，管理员将看不到证书节点，也不能配置或访问有关设备**Certificates**（证书）或默认受信任的证书颁发机构的信息。<br>如果将此权限状态设置为只读，管理员可以查看证书配置信息，位不允许执行任何配置程序。 | 是 | 是 | 是 |
| 证书配置文件 | 控制访问**Certificate Profile**（证书配置）文件节点。如果禁用此权限，管理员将看不到**Certificate Profile**（证书配置）文件节点，也不能创建证书配置文件。<br>如果将此权限状态设置为只读，管理员可以查看当前配置的防火墙证书配置文件，但不允许创建或编辑证书配置文件。 | 是 | 是 | 是 |
| OCSP 响应者 | 控制访问 **OCSP Responder**（**OCSP** 响应）节点。如果禁用此权限，管理员将看不到 **OCSP Responder**（**OCSP** 响应者）节点，也不能定义将用来验证防火墙签发的证书的吊销状态的服务器。<br>如果将此权限状态设置为只读，管理员可以查看防火墙的 **OCSP Responder**（**OCSP** 响应者）配置，但不允许创建或编辑 OCSP 响应者配置。 | 是 | 是 | 是 |
| SSL/TLS 服务配置文件 | 控制访问 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）节点。<br>如果禁用此权限，管理员将看不到节点或不能对指定使用 SSL/TLS 的防火墙服务的证书和协议版本或版本范围的配置文件进行配置。<br>如果将权限设置为只读，管理员可以查看当前 SSL/TLS 服务配置文件，但是不能添加或编辑。 | 是 | 是 | 是 |
| Scep | 控制访问 **SCEP** 节点。如果禁用该权限，管理员将无法查看节点，也不能定义指定签发特殊设备证书所需要的简单证书注册协议 (SCEP) 的配置文件。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 如果您将此权限设置为只读，则管理员可以查看当前的 SCEP 配置文件但无法对其进行创建或编辑。 | | | |
| SSL 解密排除 | 控制访问 **SSL Decryption Exclusion**（**SSL** 解密排除）节点。如果禁用此权限，管理员将看不到节点，也不能查看 SSL 解密添加自定义排除。<br>如果您将此权限设置为只读，则管理员可以查看当前的 SSL 解密排除，但无法对其进行创建或编辑。 | 是 | 是 | 是 |
| 响应页 | 控制访问 **Response Pages**（响应页面）节点。如果禁用此权限，管理员将看不到 **Response Page**（响应页面）节点，也不能定义下载和显示的自定义 HTML 消息，而非请求的 Web 页面或文件。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Response Page**（响应页面）配置，但不允许创建或编辑响应页面配置。 | 是 | 是 | 是 |
| 日志设置 | 将默认状态设置为启用或禁用下面所述的所有日志设置。 | 是 | 否 | 是 |
| system | 控制访问 **Log Settings**（日志设置）> **System**（系统）节点。如果禁用此权限，管理员将看不到**Log Settings**（日志设置）> **System**（系统）节点或者指定防火墙转发到 Panorama 或外部服务（例如 Syslog 服务器）的系统日志。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **System**（系统）设置，但无法添加、编辑或删除设置。 | 是 | 是 | 是 |
| 配置 | 控制访问 **Log Settings**（日志设置）> **Configuration**（配置）节点。如果禁用此权限，管理员将看不到 **Log Settings**（日志设置）> **Configuration**（配置）节点或者指定防火墙转发到 Panorama 或外部服务（例如 Syslog 服务器）的配置日志。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **Configuration**（配置）设置，但无法添加、编辑或删除设置。 | 是 | 是 | 是 |
| User-ID | 控制访问 **Log Settings**（日志设置）> **User-ID** 节点。如果禁用此权限，管理员将看不到 **Log Settings**（日志设置）> **User-ID** 节点或者指定防火墙转发到 Panorama 或外部服务（例如 Syslog 服务器）的 User-ID 日志。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **User-ID** 设置，但无法添加、编辑或删除设置。 | | | |
| HIP 匹配 | 控制访问 **Log Settings**（日志设置）> **HIP Match**（**HIP** 匹配）节点。如果禁用此权限，管理员将看不到 **Log Settings**（日志设置）> **HIP Match**（**HIP** 匹配）节点或者指定防火墙转发到 Panorama 或外部服务（例如 Syslog 服务器）的主机信息配置文件 (HIP) 匹配日志。HIP 匹配日志提供适用于 GlobalProtect 端点的安全策略规则的信息。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **HIP** 设置，但无法添加、编辑或删除设置。 | 是 | 是 | 是 |
| GlobalProtect | 控制访问 **Log Settings**（日志设置）> **GlobalProtect**节点。如果禁用此权限，管理员将无法看到**Log Settings**（日志设置）> **GlobalProtect** 节点或指定防火墙转发到 Panorama 或外部服务（例如 Syslog 服务器）的 GlobalProtect 日志。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **GlobalProtect** 设置，但无法添加、编辑或删除设置。 | 是 | 是 | 是 |
| 关联 | 控制访问 **Log Settings**（日志设置）> **Correlation**（关联）节点。如果禁用此权限，管理员将看不到 **Log Settings**（日志设置）> **Correlation**（关联）节点或者添加、删除或修改关联日志转发设置或标记源或目标 IP 地址。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **Correlation**（关联）设置，但无法添加、编辑或删除设置。 | 是 | 是 | 是 |
| 警报设置 | 控制访问 **Log Settings**（日志设置）> **Alarm Settings**（警报设置）节点。如果禁用此权限，管理员将看不到 **Log Settings**（日志设置）> **Alarm Settings**（警报设置）节点或者在可配置的时间段内重复击中安全策略规则（或一组规则）时，配置防火墙生成的通知。<br>如果将此权限设置为只读，管理员可以查看防火墙的 **Log Settings**（日志设置）> **Alarm Settings**（警报设置）设置，但无法编辑设置。 | 是 | 是 | 是 |
| 管理日志 | 控制访问 **Log Settings**（日志设置）> **Manage Logs**（管理日志）节点。如果禁用此权限，管理员将看不到**Log Settings**（日志设置）> **Manage Logs**（管理日志）节点或清除指示日志。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 如果将此权限状态设置为只读，管理员可以查看 **Log Settings**（日志设置）> **Manage Logs**（管理日志）信息，但不能清除任何日志。 | | | |
| 服务器配置文件 | 将默认状态设置为启用或禁用下面所述的所有服务器配置文件设置。 | 是 | 否 | 是 |
| Snmp 陷阱 | 控制访问 **Server Profiles**（服务器配置文件）> **SNMP Trap**（SNMP 陷阱）节点。如果禁用此权限，管理员将看不到 **Server Profiles**（服务器配置文件）> **SNMP Trap**（SNMP 陷阱）节点，也不能指定一个或多个要用于系统日志条目的 SNMP 陷阱目标。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **SNMP Trap Logs**（SNMP 陷阱日志）信息，但不能指定 SNMP 陷阱目标。 | 是 | 是 | 是 |
| Syslog | 控制访问 **Server Profiles**（服务器配置文件）> **Syslog** 节点。如果禁用此权限，管理员将看不到**Server Profiles**（服务器配置文件）> **Syslog**节点，也不能指定一个或多个 Syslog 服务器。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **Syslog** 信息，但不能指定 Syslog 服务器。 | 是 | 是 | 是 |
| email | 控制访问 **Server Profiles**（服务器配置文件）> **Email**（电子邮件）节点。如果禁用此权限，管理员将看不到 **Server Profiles**（服务器配置文件）> **Email**（电子邮件）节点，也不能配置用来启用系统电子邮件通知和配置日志条目的电子邮件配置文件。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **Email**（电子邮件）信息，但不能配置电子邮件服务器配置文件。 | 是 | 是 | 是 |
| Http | 控制访问 **Server Profiles**（服务器配置文件）> **HTTP** 节点。如果禁用此权限，管理员将看不到 **Server Profiles**（服务器配置文件）> **HTTP** 节点，也不能配置用来启用日志转发到 HTTP 目标任何日志条目的 HTTP 服务器配置文件。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **HTTP** 信息，但不能配置 HTTP 服务器配置文件。 | 是 | 是 | 是 |
| Netflow | 控制访问 **Server Profiles**（服务器配置文件）> **Netflow** 节点。如果禁用此权限，管理员将看不到**Server Profiles**（服务器配置文件）> **Netflow**节点，也不能定义 NetFlow 服务器配置 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 文件，用于指定导出频率和将接收导出数据的 NetFlow 服务器。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **Netflow** 信息，但不能定义 Netflow 配置文件。 | | | |
| RADIUS | 控制访问 **Server Profiles**（服务器配置文件）> **RADIUS** 节点。如果禁用此权限，管理员将看不到**Server Profiles**（服务器配置文件）> **RADIUS** 节点，也不能配置在身份验证配置文件中确定的 RADIUS 服务器的设置。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **RADIUS** 信息，但不能配置 RADIUS 服务器的设置。 | 是 | 是 | 是 |
| TACACS+ | 控制访问 **Server Profiles**（服务器配置文件）> **TACACS+** 节点。<br>如果禁用此权限，管理员将看不到 此 节点，或配置对文件配置引用进行身份验证的 TACACS+ 服务器的设置。<br>如果将权限设置为只读，管理员可以查看当前 TACACS+ 服务器配置文件，但是不能添加或编辑。 | 是 | 是 | 是 |
| LDAP | 控制访问 **Server Profiles**（服务器配置文件）> **LDAP** 节点。如果禁用此权限，管理员将看不到 **Server Profiles**（服务器配置文件）> **LDAP**节点，也不能配置通过身份验证配置文件进行身份验证的 LDAP 服务器的设置。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **LDAP** 信息，但不能配置 LDAP 服务器的设置。 | 是 | 是 | 是 |
| Kerberos | 控制访问 **Server Profiles**（服务器配置文件）> **Kerberos** 节点。如果禁用此权限，管理员将看不到**Server Profiles**（服务器配置文件）> **Kerberos** 节点或配置允许用户对域控制器进行本地身份验证的 Kerberos 服务器。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **Kerberos** 信息，但不能配置 Kerberos 服务器的设置。 | 是 | 是 | 是 |
| SAML 标识提供商 | 控制访问 **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商）节点。如果您禁用此权限，则管理员不能查看节点或配置 SAML 标识提供商 (IdP) 服务器配置文件。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **SAML** | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | **Identity Provider**（**SAML** 标识提供商）信息，但不能配置 SAML IdP 服务器配置文件。 | | | |
| 多重因素身份验证 | 控制访问 **Server Profiles**（服务器配置文件）> **Multi Factor Authentication**（多重因素身份验证）节点。如果您禁用此权限，则管理员不能查看节点或配置多重因素身份验证 (MFA) 服务器配置文件。<br>如果将此权限状态设置为只读，管理员可以查看 **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商）信息，但不能配置 MFA 服务器配置文件。 | | | |
| 本地用户数据库 | 将默认状态设置为启用或禁用下面所述的所有本地用户数据库设置。 | 是 | 否 | 是 |
| 用户 | 控制访问 **Local User Database**（本地用户数据库）> **Users**（用户）节点。如果禁用此权限，管理员将看不到 **Local User Database**（本地用户数据库）> **Users**（用户）节点，或者在防火墙上设置本地数据库以存储远程访问用户、防火墙管理员和身份验证门户用户的身份验证信息。<br>如果将此权限状态设置为只读，管理员可以查看 **Local User Database**（本地用户数据库）> **Users**（用户）信息，但无法在防火墙上设置本地数据库以存储身份验证信息。 | 是 | 是 | 是 |
| 用户组 | 控制访问 **Local User Database**（本地用户数据库）> **Users**（用户）节点。如果禁用此权限，管理员将看不到 **Local User Database**（本地用户数据库）> **Users**（用户）节点，也不能将用户组信息添加到本地数据库。<br>如果将此权限状态设置为只读，管理员可以查看 **Local User Database**（本地用户数据库）> **Users**（用户）信息，但无法将用户组信息添加到本地数据库。 | 是 | 是 | 是 |
| 访问域 | 控制访问 **Access Domain**（访问域）节点。如果禁用此权限，管理员将无法看到 **Access Domain**（访问域）节点或创建或编辑访问域。<br>如果将此权限设置为只读，则管理员可以查看 **Access Domain**（访问域）信息，但不能创建或编辑访问域。 | 是 | 是 | 是 |
| 已计划的日志导出 | 控制访问 **Scheduled Log Export**（已计划的日志导出）节点。如果禁用此权限，管理员将无法看到 **Scheduled Log Export**（已计划的日志导出）节点，也不能计划以 CSV 格式导出日志并将其保存到文件传输协议 (FTP) 服务器，或使用安 | 是 | 否 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 全复制 (SCP) 在防火墙和远程主机之间安全地传输数据。<br>如果将此权限状态设置为只读，管理员可以查看 **Scheduled Log Export Profile**（已计划的日志导出配置文件）信息，但不能计划导出日志。 | | | |
| 软件 | 控制访问 **Software**（软件）节点。如果禁用此权限，管理员将看不到 **Software**（软件）节点或查看 Palo Alto Networks 提供的 PAN-OS 软件的最新版本，阅读每个版本的发行说明并选择要下载和安装的版本。<br>如果将此权限状态设置为只读，管理员可以查看 **Software**（软件）信息，但不能下载或安装软件。 | 是 | 是 | 是 |
| GlobalProtect 客户端 | 控制访问 **GlobalProtect Client**（**GlobalProtect** 客户端）节点。如果禁用此权限，管理员将看不到 **GlobalProtect Client**（**GlobalProtect** 客户端）节点或查看可用的 GlobalProtect 版本，下载代码或激活 GlobalProtect 应用。<br>如果将此权限状态设置为只读，管理员可以查看可用的 **GlobalProtect Client**（**GlobalProtect** 客户端）版本，但不能下载或安装应用软件。 | 是 | 是 | 是 |
| 动态更新 | 控制访问 **Dynamic Updates**（动态更新）节点。如果禁用此权限，管理员将看不到 **Dynamic Updates**（动态更新）节点，也不能查看最新的更新、阅读每个更新的发行说明或选择要上传和安装的更新。<br>如果将此权限状态设置为只读，管理员可以查看可用的 **Dynamic Updates**（动态更新）版本，阅读发行说明，但不能上传或安装软件。 | 是 | 是 | 是 |
| 许可证 | 控制访问 **Licenses**（许可证）节点。如果禁用此权限，管理员将看不到 **Licenses**（许可证）节点，也不能查看安装的许可证或激活许可证。<br>如果将此权限状态设置为只读，管理员可以查看安装的 **Licenses**（许可证），但不能执行许可证管理功能。 | 是 | 是 | 是 |
| 支持 | 控制访问 **Support**（支持）节点。如果禁用此权限，管理员将无法看到 **Support**（支持）节点、激活支持或访问 Palo Alto Networks 的产品和安全警报。<br>如果将此权限状态设置为只读，管理员可以查看 **Support**（支持）节点和访问产品和安全警报，但不能激活支持。 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 仅具有预定义超级用户角色的管理员才能使用 **Support**（支持）节点生成技术支持文件，或者生成和下载统计转储和核心文件。 | | | |
| 主密钥和诊断 | 控制访问 **Master Key and Diagnostics**（主密钥和诊断）节点。如果禁用此权限，管理员将看不到 **Master Key and Diagnostics**（主密钥和诊断）节点，也不能指定在防火墙上用来加密私钥的主密钥。<br>如果将此权限状态设置为只读，管理员可以查看 **Master Key and Diagnostics**（主密钥和诊断）节点和查看有关已指定的主密钥的信息，但不能添加或编辑新的主密钥配置。 | 是 | 是 | 是 |

## 定义管理角色配置文件中的用户隐私设置

要定义管理员可以访问的最终用户隐私数据，在创建或编辑管理员角色配置文件（**Device**（设备）> **Admin Roles**（管理员角色））时，请向下滚动到 **WebUI** 选项卡上的 **Privacy**（隐私）选项。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 隐私 | 将默认状态设置为启用或禁用下面所述的所有隐私设置。 | 是 | N/A | 是 |
| 显示完整 IP 地址 | 如果设置为禁用，则通过正在流经 Palo Alto Networks 防火墙的流量获得的完整 IP 地址不会显示在日志或报告中。在通常显示 IP 地址的位置，将显示相关的子网。<br>计划报告通过 *Monitor*（监控）> *Reports*（报告）显示在界面中，且通过计划电子邮件发送的报告仍将显示完整 *IP* 地址。由于这种异常，我们建议在 *Monitor*（监控）选项卡内将以下设置设置为禁用：自定义报告、应用程序报告、威胁报告、*URL* 过滤报告、流量报告和电子邮件调度程序。 | 是 | N/A | 是 |
| 显示日志和报告中的用户名 | 如果被禁用，则通过正在流经 Palo Alto Networks 防火墙的流量获得的用户名不会显示在日志或报告中。通常显示这些用户名的列为空。<br>计划报告通过 *Monitor*（监控）> *Reports*（报告）显示在界面中，或通过电子邮件调度程序发送的报告仍将显示用户名。由于这种异常，我们建议在 *Monitor*（监控）选项卡内将以下设置设置为禁用：自定义报告、应用程序报 | 是 | N/A | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 告、威胁报告、*URL* 过滤报告、流量报告和电子邮件调度程序。 | | | |
| 查看 PCAP 文件 | 如果设置为禁用，通常在流量、威胁和数据筛选日志内提供的数据包捕获文件将不会显示。 | 是 | N/A | 是 |

## 限制管理员访问提交和验证功能

要限制访问提交（和还原）、保存和验证功能，在创建或编辑管理员角色配置文件（**Device**（设备）> **Admin Roles**（管理员角色））时，请向下滚动到 **WebUI** 选项卡上的 **Commit**（提交）、**Save**（保存）和 **Validate**（验证）选项。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 提交 | 将默认状态设置为启用或禁用下面所述的所有提交和还原权限。 | 是 | N/A | 是 |
| 设备 | 禁用时，管理员无法提交或还原任何管理员进行的防火墙配置更改，包括他或她自己的更改。 | 是 | N/A | 是 |
| 为其他管理员提交 | 禁用时，管理员无法提交或还原其他管理员进行的防火墙配置更改。 | 是 | N/A | 是 |
| 保存 | 将默认状态设置为启用或禁用下面所述的所有保存操作权限。 | 是 | N/A | 是 |
| 部分保存 | 禁用时，管理员无法保存任何管理员进行的防火墙配置更改，包括他或她自己的更改。 | 是 | N/A | 是 |
| 为其他管理员保存 | 禁用时，管理员无法保存其他管理员进行的防火墙配置更改。 | 是 | N/A | 是 |
| 验证 | 如果设置为禁用，管理员无法验证配置。 | 是 | N/A | 是 |

## 提供对全局设置的粒度访问

要定义管理员可以访问的全局设置，在创建或编辑管理员角色配置文件（**Device**（设备）> **Admin Roles**（管理员角色））时，请向下滚动到**WebUI** 选项卡上的 **Global**（全局）选项。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| 全局 | 将默认状态设置为启用或禁用下面所述的所有全局设置。实际上，此时该设置仅适用于系统警报。 | 是 | N/A | 是 |
| 系统警报 | 如果设置为禁用，管理员无法将任何更查看或确认生成的警报。 | 是 | N/A | 是 |


© 2019 Palo Alto Networks, Inc.

## 提供对 *Panorama* 选项卡的粒度访问控制

下表列出了 **Panorama** 选项卡访问权限级别以及可用的自定义 Panorama 管理员角色。防火墙管理员不能访问这些权限。

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| 设置 | 指定管理员是否可以查看或编辑 Panorama 设置信息，包括 **Management**（管理）、**Operations**（操作）和 **Telemetry**（遥测）、**Services**（服务）、Content-ID、**WildFire**、Session（会话）或 **HSM**。<br>如果您将权限设置为：<br>• 只读，管理员可以看相关信息，但不能编辑。<br>• 禁用此权限，则管理员无法查看或编辑相关信息。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 高可用性 | 指定管理员是否可以查看和管理 Panorama 管理服务器的高可用性 (HA) 设置。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 管理服务器的高可用性配置信息，但不能管理该配置。<br>如果您禁用此权限，则管理员不能查看或管理 Panorama 管理服务器的高可用性配置设置。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 配置审核 | 指定管理员是否可以运行 Panorama 配置审核。如果您禁用此权限，则管理员不能运行 Panorama 配置审核。 | Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| 管理员 | 指定管理员是否可以查看 Panorama 管理员帐户详细信息。<br>您对此功能无法启用完全访问权限：只能启用只读访问权限。（只能具有动态角色的 Panorama 管理员可以添加、编辑或删除 Panorama 角色。）凭借只读访问权限，管理员可以查看与其自己的帐户相关的信息，但不能查看其他 Panorama 管理员帐户。<br>如果您禁用此权限，则管理员无法查看与任何 Panorama 管理员帐户相关的信息，包括其自有帐户的信息。 | Panorama：是<br>设备组/模板：否 | 否 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| 管理角色 | 指定管理员是否可以查看 Panorama 管理员角色。<br>您对此功能无法启用完全访问权限：只能启用只读访问权限。（只能具有动态角色的 Panorama 管理员可以添加、编辑或删除自定义 Panorama 角色。）凭借只读访问权限，管理员可以查看 Panorama 管理员角色配置，但不能对其进行管理。<br>如果您禁用此权限，则管理员不能查看或管理 Panorama 管理员角色。 | Panorama：是<br>设备组/模板：否 | 否 | 是 | 是 |
| 访问域 | 指定管理员是否可以查看、添加、编辑、删除或克隆 Panorama 管理员的访问域配置。（此权限控制只对访问域配置进行访问；不能访问分配给访问域的设备组、模板和防火墙的上下文。）<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 访问域配置，但不能对其进行管理。<br>如果您禁用此权限，则管理员不能查看或管理 Panorama 访问域配置。 | Panorama：是<br>设备组/模板：否<br>将访问域分配给设备组和模板管理员，这样他们就能访问分配给这些访问域的设备组、模板和防火墙的上下文中的配置和监控数据。 | 是 | 是 | 是 |
| 身份验证配置文件 | 指定管理员是否可以查看、添加、编辑、删除或克隆 Panorama 管理员的身份验证配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 身份验证配置文件，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 Panorama 身份验证配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 身份验证序列 | 指定管理员是否可以查看、添加、编辑、删除或克隆 Panorama 管理员的身份验证序列。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 身份验证序列，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 Panorama 身份验证序列。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| 用户标识 | 指定管理员是否可以配置 User-ID 连接安全性，并查看、添加、编辑或删除数据重新分发点（如 User-ID 代理）。<br>如果您将此权限设置为只读，则管理员可以查看 User-ID 连接安全性和重新分发点的设置，但不能管理该设置。<br>如果您禁用此权限，则管理员不能查看或管理 User-ID 连接安全性或重新分发点的设置。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 受管设备 | 指定管理员是否可以查看、添加、编辑或删除作为受管设备的防火墙，以及在其上安装软件或内容更新。<br>如果您将此权限设置为只读，则管理员可以查看受管防火墙，但不能添加、删除和标记防火墙，也不能在其上安装更新。<br>如果您禁用此权限，则管理员不能查看、添加、编辑、标记和删除受管防火墙，也不能在其上安装更新。<br>  具有设备部署权限的管理员仍然可以使用 *Panorama > Device Deployment*（设备部署）在受管防火墙上安装更新。 | Panorama：是<br>设备组/模板：是 | 是<br>（对于设备组和模板角色，为否） | 是 | 是 |
| 模板 | 指定管理员是否可以查看、编辑、添加或删除模板及模板堆栈。<br>如果您将此权限设置为只读，则管理员可以查看模板及堆栈配置，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理模板及堆栈配置。 | Panorama：是<br>设备组/模板：是<br>  设备组和模板管理员只能查看分配给上述管理员的位于访问域中的模板和堆栈。 | 是<br>（对于设备组和模板管理员，为否） | 是 | 是 |
| 设备组 | 指定管理员是否可以查看、编辑、添加或删除设备组。<br>如果您将此权限设置为只读，则管理员可以查看设备组配置，但不能对其进行管理。 | Panorama：是<br>设备组/模板：是<br>  设备组和模板管理员只能访问分配给上述管理 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 如果您禁用此权限，则管理员无法查看或管理设备组配置。 | 员的位于访问域中设备组。 | | | |
| 受管收集器 | 指定管理员是否可以查看、编辑、添加或删除受管收集器。<br>如果您将此权限设置为只读，则管理员可以查看受管收集器配置，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看、编辑、添加或删除受管收集器配置。<br>具有设备部署权限的管理员仍然可以使用 *Panorama > Device Deployment*（设备部署）选项在受管收集器上安装更新。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 收集器组 | 指定管理员是否可以查看、编辑、添加或删除收集器组。<br>如果您将此权限设置为只读，则管理员可以查看收集器组，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理收集器组。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| VMware 服务管理器 | 指定管理员是否可以查看和编辑 VMware 服务管理器设置。<br>如果您将此权限设置为只读，则管理员可以查看设置，但无法执行任何相关配置或操作步骤。<br>如果您禁用此权限，则管理员无法查看设置或执行任何相关配置或操作步骤。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 证书管理 | 为所有 Panorama 证书管理权限设置默认状态（启用或禁用）。 | Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| 证书 | 指定管理员是否可以查看、编辑、生成、删除、调用、更新或导出证书。此权限还指定管理员是否可以导入或导出高可用性密钥。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 证书，但无法管理该证书或高可用性密钥。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 如果您禁用此权限，则管理员不能查看或管理 Panorama 证书或高可用性密钥。 | | | | |
| 证书配置文件 | 指定管理员是否可以查看、添加、编辑、删除或克隆 Panorama 证书配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 证书配置文件，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 Panorama 证书配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| SSL/TLS 服务配置文件 | 指定管理员是否可以查看、添加、编辑、删除或克隆 SSL/TLS 服务配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 SSL/TLS 服务配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 SSL/TLS 服务配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 日志设置 | 为所有日志设置权限设置默认状态（启用或禁用）。 | Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| system | 指定管理员是否可以查看和配置对将系统日志转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看系统日志转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。<br>此权限仅适用于 *Panorama* 和日志收集器生成的系统日志。收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的系统日志的转发。*Device*（设备）> *Log Settings*（日志设置）> 系统 权限控制日志从防火墙 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 直接转发到外部服务（无需在日志收集器上聚合）。 | | | | |
| 配置 | 指定管理员是否可以查看和配置对将配置日志转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看配置日志转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。<br>此权限仅适用于 *Panorama* 和日志收集器所生成的配置日志。收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的配置日志的转发。*Device*（设备）> *Log Settings*（日志设置）> 配置权限控制日志从防火墙直接转发到外部服务（无需在日志收集器上聚合）。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| User-ID | 指定管理员是否可以查看和配置对将 User-ID 日志转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看配置日志转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。<br>此权限仅适用于 *Panorama* 生成的 *User-ID* 日志。收集器组权限（*Panorama* > *Collector Groups*（收集器 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 组））控制日志收集器从防火墙接收的 *User-ID* 日志的转发。*Device*（设备）> *Log Settings*（日志设置）> User-ID 权限控制日志从防火墙直接转发到外部服务（无需在日志收集器上聚合）。 | | | | |
| HIP 匹配 | 指定管理员是否可以查看和配置对将 HIP 匹配日志从传统模式的 Panorama 虚拟设备转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看 HIP 匹配日志的转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。<br>收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的 *HIP* 匹配日志的转发。*Device*（设备）> *Log Settings*（日志设置）> HIP 匹配权限控制日志从防火墙直接转发到外部服务（无需在日志收集器上聚合）。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| GlobalProtect | 指定管理员是否可以查看和配置对从传统模式的 Panorama 虚拟设备向外部服务转发 GlobalProtect 日志进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看 GlobalProtect 日志的转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| |  收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的 *GlobalProtect* 日志的转发。*Device*（设备）> *Log Settings*（日志设置）> *GlobalProtect* 权限控制从防火墙直接向外部服务转发日志（无需在日志收集器上聚合）。 | | | | |
| 关联 | 指定管理员是否可以查看和配置对将关联日志从传统模式的 Panorama 虚拟设备转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看关联日志转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。<br>  收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制在 *Panorama* 模式下从 *Panorama M* 系列设备或 *Panorama* 虚拟设置转发关联日志。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 通信 | 指定管理员是否可以查看和配置对将流量日志从传统模式的 Panorama 虚拟设备转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看流量日志的转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| |  收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的流量日志的转发。日志转发权限（*Objects*（对象）> *Log Forwarding*（日志转发））控制从防火墙直接转发到外部服务（无需在日志收集器上聚合）。 | | | | |
| 威胁 | 指定管理员是否可以查看和配置对将威胁日志从传统模式的 Panorama 虚拟设备转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看威胁日志的转发设置，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理该设置。<br>  收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的威胁日志的转发。日志转发权限（*Objects*（对象）> *Log Forwarding*（日志转发））控制从防火墙直接转发到外部服务（无需在日志收集器上聚合）。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| WildFire | 指定管理员是否可以查看和配置对将 WildFire日志从传统模式的 Panorama 虚拟设备转发到外部服务进行控制的设置（syslog、电子邮件、SNMP 陷阱或 HTTP 服务器）。<br>如果您将此权限设置为只读，则管理员可以查看 WildFire 日志的转发设置，但无法对其进行管理。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 如果您禁用此权限，则管理员无法查看或管理该设置。<br><br>收集器组权限（*Panorama* > *Collector Groups*（收集器组））控制日志收集器从防火墙接收的 *WildFire* 日志的转发。日志转发权限（*Objects*（对象）> *Log Forwarding*（日志转发））控制从防火墙直接转发到外部服务（无需在日志收集器上聚合）。 | | | | |
| 服务器配置文件 | 为所有服务器配置文件权限设置默认状态（启用或禁用）。<br><br>这些权限仅适用于从 *Panorama* 或日志收集器转发日志的服务器配置文件，以及用于验证 *Panorama* 管理员的服务器配置文件。*Device*（设备）> 服务器配置文件权限对用于直接从防火墙将日志转发到外部服务的服务器配置文件以及用于验证防火墙管理员的服务器配置文件的访问进行控制。 | Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| Snmp 陷阱 | 指定管理员是否可以查看和配置 SNMP 陷阱服务器配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 SNMP 陷阱服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员不能查看或管理 SNMP 陷阱服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| Syslog | 指定管理员是否可以查看和配置 Syslog 服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 如果您将此权限设置为只读，则管理员可以查看 Syslog 服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员不能查看或管理 Syslog 服务器配置文件。 | | | | |
| email | 指定管理员是否可以查看和配置电子邮件服务器配置文件。<br>如果您将此权限设置为只读，则管理员可以查看电子邮件服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理电子邮件服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| RADIUS | 指定管理员是否可以查看和配置用于验证 Panorama 管理员的 RADIUS 服务器配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 RADIUS 服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 RADIUS 服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| TACACS+ | 指定管理员是否可以查看和配置用于验证 Panorama 管理员的 TACACS+ 服务器配置文件。<br>如果禁用此权限，管理员将无法查看此节点，或配置对文件配置引用进行身份验证的 TACACS+ 服务器的设置。<br>如果将权限设置为只读，管理员可以查看当前 TACACS+ 服务器配置文件，但是无法添加或编辑。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| LDAP | 指定管理员是否可以查看和配置用于验证 Panorama 管理员的 LDAP 服务器配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 LDAP 服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 LDAP 服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| Kerberos | 指定管理员是否可以查看和配置用于验证 Panorama 管理员的 Kerberos 服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 如果您将此权限设置为只读，则管理员可以查看 Kerberos 服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 Kerberos 服务器配置文件。 | | | | |
| SAML 标识提供商 | 指定管理员是否可以查看和配置用于对 Panorama 管理员进行身份验证的 SAML 标识提供商 (IdP) 服务器配置文件。<br>如果您将此权限设置为只读，则管理员可以查看 SAML IdP 服务器配置文件，但无法对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理 SAML IdP 服务器配置文件。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 已计划的配置导出 | 指定管理员是否可以查看、添加、编辑、删除或克隆调度的 Panorama 配置导出。<br>如果您将此权限设置为只读，则管理员可以查看调度的导出，但不能对其进行管理。<br>如果您禁用此权限，则管理员无法查看或管理调度的导出。 | Panorama：是<br>设备组/模板：否 | 是 | 否 | 是 |
| 软件 | 指定管理员是否可以：查看与 Panorama 管理服务器上安装的软件更新相关的信息；下载、上传或安装更新；以及查看相关的发布说明。<br>如果您将此权限设置为只读，则管理员可以查看关于 Panorama 软件更新的信息和相关的发布说明，但不能执行任何相关的操作。<br>如果您禁用此权限，则管理员无法查看 Panorama 软件更新，也无法查看相关的发布说明或执行任何相关的操作。<br>*Panorama* > Device Deployment（设备部署）> 软件权限对在防火墙上部署的 *PAN-OS* 软件的访问权限以及在专用日志收集器上部署的 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | *Panorama* 软件的访问权限进行控制。 | | | | |
| 动态更新 | 指定管理员是否可以：查看与 Panorama 管理服务器上安装的内容更新相关的信息（例如 WildFire 更新）；下载、上传、安装或恢复更新；并查看相关的发布说明。<br>如果您将此权限设置为只读，则管理员可以查看关于 Panorama 内容更新的信息和相关的发布说明，但无法执行任何相关的操作。<br>如果您禁用此权限，则管理员无法查看 Panorama 内容更新，也无法查看相关的发布说明或执行任何相关的操作。<br>*Panorama* > 设备部署 > 动态更新权限对在防火墙和专用日志收集器上部署的内容更新的访问权限进行控制。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 支持 | 指定管理员是否可以：查看 Panorama 支持许可证信息、产品警报和安全警报；激活支持许可证和管理案例。只有超级用户管理员才能生成技术支持文件。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 支持信息、产品警报和安全警报，但无法激活支持许可证，也无法生成技术支持文件或管理案例。<br>如果您禁用此权限，则管理员无法：查看 Panorama 支持信息、产品警报或安全警报；激活支持许可证，生成技术支持文件或管理案例。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |
| 设备部署 | 为与防火墙和日志收集器部署许可证和软件或内容更新相关的所有权限设置启用或禁用的默认状态。<br>*Panorama* > 软件和 *Panorama* > 动态更新权限可对在 *Panorama* 管理服务 | Panorama：是<br>设备组/模板：是 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- | --- |
| | 器上安装的软件和内容更新进行控制。 | | | | |
| 软件 | 指定管理员是否可以：查看与防火墙和日志收集器上安装的软件更新相关的信息；下载、上传或安装更新；以及查看相关的发布说明。<br>如果您将此权限设置为只读，则管理员可以查看与软件更新相关的信息，还可以查看相关的发布说明，但无法将更新部署到防火墙或专用日志收集器。<br>如果您禁用此权限，则管理员无法查看与软件更新相关的信息，无法查看相关的发布说明，也无法将更新部署到防火墙或专用日志收集器。 | Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| GlobalProtect 客户端 | 指定管理员是否可以：查看与防火墙上的 GlobalProtect 应用程序软件更新相关的信息；下载、上传或激活更新；以及查看相关的发布说明。<br>如果您将此权限设置为只读，则管理员可以查看与 GlobalProtect 应用程序软件更新相关的信息，还可以查看相关的发布说明，但无法激活防火墙上的更新。<br>如果您禁用此权限，则管理员无法查看与 GlobalProtect 应用程序软件更新相关的信息，也无法查看相关的发布说明，或无法激活防火墙上的更新。 | Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| 动态更新 | 指定管理员是否可以：查看与防火墙和专用日志收集器上安装的内容更新（例如，应用程序更新）相关的信息；下载、上传或安装更新；以及查看相关的发布说明。<br>如果您将此权限设置为只读，则管理员可以查看与内容更新相关的信息，还可以查看相关的发布说明，但无法将更新部署到防火墙或专用日志收集器。<br>如果您禁用此权限，则管理员无法查看与内容更新相关的信息，无法查看相关的发布说明，也无法将更新部署到防火墙或专用日志收集器。 | Panorama：是<br>设备组/模板：是 | 是 | 是 | 是 |
| 许可证 | 指定管理员是否可以查看、刷新和激活防火墙许可证。 | Panorama：是 | 是 | 是 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 管理员角色可用性 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|---|
| | 如果您将此权限设置为只读，则管理员可以查看防火墙许可证，但无法刷新或激活这些许可证。<br>如果您禁用此权限，则管理员无法查看、刷新或激活防火墙许可证。 | 设备组/模板：是 | | | |
| 主密钥和诊断 | 指定管理员是否可以查看和配置主密钥，以在 Panorama 上加密私钥。<br>如果您将此权限设置为只读，则管理员可以查看 Panorama 主密钥配置，但无法对其进行更改。<br>如果您禁用此权限，则管理员无法查看或编辑 Panorama 主密钥配置。 | Panorama：是<br>设备组/模板：否 | 是 | 是 | 是 |

## Panorama Web 界面访问权限

通过自定义 Panorama 管理员角色，您可以定义对 Panorama 选项的访问权限，以及仅允许访问设备组和模板（**Policies**（策略）、**Objects**（对象）、**Network**（网络）和 **Device**（设备）选项卡）。

您可以创建的管理员角色包括 **Panorama** 以及设备组和模板。不能将 CLI 访问权限分配到 **Device Group and Template**（设备组和模板）管理员角色配置文件。如果您将 CLI 的超级用户权限分配到 **Panorama** 管理员角色，则具有该角色的管理员可以访问所有功能（不管您分配的 Web 界面权限为何）。

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| 仪表盘 | 控制访问 **Dashboard**（仪表板）选项卡。如果禁用此权限，管理员将看不到该选项卡，且将无法访问所有仪表盘小组件。 | 是 | 否 | 是 |
| ACC | 控制访问应用程序命令中心 (ACC)。如果禁用此权限，**ACC** 选项卡将不会显示在 Web 界面中。请记住，如果想要在仍能够访问 ACC 的同时保护用户隐私，可以禁用 **Privacy**（隐私）> **Show Full IP Addresses**（显示完整 IP 地址）选项和/或 **Show User Names In Logs And Reports**（显示日志和报告中的用户名）选项。 | 是 | 否 | 是 |
| 监视 | 控制访问 **Monitor**（监控）选项卡。如果禁用此权限，管理员将看不到 **Monitor**（监控）选项卡，且将无法访问任何日志、数据包捕获、会话信息、报告或 App Scope。要更精确地控制管理员可以看到的监控信息，保留启用 Monitor（监控）选项，然后启用或禁用选项卡上的特定节点，如提供对监控选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 数量 | 控制访问 **Policies**（策略）选项卡。如果禁用此权限，管理员将看不到 **Policies**（策略）选项卡，且将无法访问任何策略信息。要更精确地控制管理 | 是 | 否 | 是 |



© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
| --- | --- | --- | --- | --- |
| | 员可以看到的策略信息（如允许访问特定策略类型或只读访问策略信息），保留启用 **Policies**（策略）选项，然后启用或禁用选项卡上的特定节点，如提供对策略选项卡的粒度访问中所述。 | | | |
| 对象 | 控制访问 **Objects**（对象）选项卡。如果禁用此权限，管理员将看不到 **Objects**（对象）选项卡，且将无法访问任何对象、安全配置文件、日志转发配置文件、解密配置文件或时间表。要更精确地控制管理员可以看到的对象信息，保留启用 **Objects**（对象）选项，然后启用或禁用选项卡上的特定节点，如提供对对象选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 网络 | 控制访问 **Network**（网络）选项卡。如果禁用此权限，管理员将看不到 **Network**（网络）选项卡，且将无法访问任何界面、区域、VLAN、Virtual Wire、虚拟路由器、IPsec 隧道、DHCP、DNS 代理、GlobalProtect、QoS 配置信息或网络配置文件。要更精确地控制管理员可以看到的对象信息，保留启用 **Network**（网络）选项，然后启用或禁用选项卡上的特定节点，如提供对网络选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 设备 | 控制访问 **Device**（设备）选项卡。如果禁用此权限，管理员将看不到**Device**（设备）选项卡，且将无法访问任何设备范围内配置信息，如 User-ID、高可用性、服务器配置文件或证书配置信息。要更精确地控制管理员可以看到的对象信息，保留启用 **Device**（设备）选项，然后启用或禁用选项卡上的特定节点，如提供对设备选项卡的粒度访问中所述。<br><br>您无法允许基于角色的管理员访问 *Admin Roles*（管理员角色）或 *Administrators*（管理员）节点，即使您能够完全访问 *Device*（设备）选项卡。 | 是 | 否 | 是 |
| Panorama | 控制访问 **Panorama** 选项卡。如果您禁用此权限，则管理员无法查看 **Panorama** 选项卡，也没有权限访问任何 Panorama 级的配置信息，如受管设备、受管收集器或收集器组。<br><br>要更精确地控制管理员可以看到的对象信息，保留启用 **Panorama** 选项，然后启用或禁用选项卡上的特定节点，如提供对 Panorama 选项卡的粒度访问中所述。 | 是 | 否 | 是 |
| 隐私 | 控制访问定义管理员角色配置文件中的用户隐私设置中所述的隐私设置。 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

| 访问级别 | 说明 | 启用 | 只读 | 禁用 |
|---|---|---|---|---|
| 验证 | 如果设置为禁用，管理员无法验证配置。 | 是 | 否 | 是 |
| 保存 | 将下面描述的所有保存权限设置为默认状态（启用或禁用）（部分保存和为其他管理员保存）。 | 是 | 否 | 是 |
| • 部分保存 | 禁用时，管理员无法保存任何管理员对 Panorama 配置所做的更改。 | 是 | 否 | 是 |
| • 为其他管理员保存 | 禁用时，管理员无法保存其他管理员对 Panorama 配置所做的更改。 | 是 | 否 | 是 |
| 提交 | 将下面描述的所有提交、推送和还原权限设置为默认状态（启用或禁用）（Panorama、设备组、模板、强制模板值、收集器组、WildFire 设备集群）。 | 是 | 否 | 是 |
| • Panorama | 禁用时，管理员无法提交或还原任何管理员进行的配置更改，包括他或她自己的更改。 | 是 | 否 | 是 |
| • 为其他管理员提交 | 禁用时，管理员无法提交或还原其他管理员进行的配置更改。 | 是 | 否 | 是 |
| 设备组 | 禁用时，管理员无法将更改推送到设备组。 | 是 | 否 | 是 |
| 模板 | 禁用时，管理员无法将更改推送到模板。 | 是 | 否 | 是 |
| 强制模板值 | 该权限控制对推送范围选择对话框中 **Force Template Values**（强制模板值）选项的访问。<br>如果设置为禁用，则管理员无法将本地防火墙配置中的覆写设置替换为 Panorama 从模板中推动的设置。<br>如果在启用 *Force Template Values*（强制模板值）的情况下推送配置，则防火墙上的所有替代值将替换为模板中的值。在使用此选项之前，检查防火墙上的替代值，确保您的提交不会导致任何意外的网络中断，或是因替换这些替代值而产生问题。 | 是 | 否 | 是 |
| 收集器组 | 禁用时，管理员无法将更改推送到收集器组。 | 是 | 否 | 是 |
| WildFire 设备集群 | 禁用时，管理员无法将更改推送到 WildFire 设备集群。 | 是 | 否 | 是 |
| 任务 | 禁用时，管理员无法访问任务管理器。 | 是 | 否 | 是 |
| 全局 | 控制访问提供对全局设置的粒度访问中所述的全局设置（系统警告）。 | 是 | 否 | 是 |


© 2019 Palo Alto Networks, Inc.

# 参考资料：端口码使用

下表列出了防火墙和 Panorama 相互通信，或与网络上的其他服务进行通信所使用的端口。

- 用于管理功能的端口
- 用于 HA 的端口
- 用于 Panorama 的端口
- 用于 GlobalProtect 的端口
- 用于 User-ID 的端口

## 用于管理功能的端口

防火墙和 Panorama 使用以下端口执行管理功能。

| 目标端口 | 协议 | 说明 |
|---|---|---|
| 22 | TCP | 用于从客户端系统与防火墙 CLI 界面进行通信。 |
| 80 | TCP | 防火墙作为 OCSP 响应者侦听在线证书状态协议 (OCSP) 更新时所使用的端口。 |
| 123 | UDP | 防火墙用于 NTP 更新的端口。 |
| 443 | TCP | 用于从客户端系统与防火墙 Web 界面进行通信。启用 VM 监控以跟踪虚拟网络上的更改时，这也是防火墙和 User-ID 代理侦听更新的端口。<br>要监控 AWS 环境，这是可用的唯一端口。<br>要监控 VMware vCenter/ESXi 环境，默认的侦听端口是 443，但可自行配置。 |
| 162 | UDP | 防火墙、Panorama 或日志收集器用来转发 Traps 至 SNMP 管理器的端口。<br>此端口不需要在 *Palo Alto Networks* 防火墙上开放。您必须配置简单网络管理协议 *(SNMP)* 管理器来侦听此端口。有关详细信息，请参阅 *SNMP* 管理软件的文档。 |
| 161 | UDP | 防火墙从 SNMP 管理器侦听轮询请求（GET 消息）的端口。 |
| 514<br>514<br>6514 | TCP<br>UDP<br>SSL | 如果您配置 Syslog 监控，则是防火墙、Panorama 或日志收集器用来将日志发送到 Syslog 服务器的端口，以及 PAN-OS 集成的 User-ID 代理或基于 Windows User-ID 代理侦听身份验证 Syslog 消息的端口。 |
| 2055 | UDP | 如果您配置 NetFlow 导出，则是防火墙用来将 NetFlow 记录发送到 NetFlow 收集器的默认端口，但此端口可配置。 |
| 5008 | TCP | GlobalProtect Mobile Security Manager 从 GlobalProtect 网关侦听 HIP 请求的端口。<br>如果您使用的是第三方 MDM 系统，则可以根据 MDM 供应商的要去将网关配置为使用不同的端口。 |



© 2019 Palo Alto Networks, Inc.

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| 6081<br>6082 | TLS 1.2<br>TCP | 用于 User-ID™ 身份验证门户的端口：用于不带 SSL/TLS 服务器配置文件的身份验证门户的端口 6081 以及用于带 SSL/TLS 的身份验证门户的端口 6082。 |
| 10443 | SSL | 防火墙和 Panorama 用于提供有关威胁的上下文信息或将威胁调查无缝转移到威胁库和 AutoFocus 的端口。 |

## 用于 HA 的端口

配置为高可用性 (HA) 对端的防火墙必须能够相互通信才能维护状态信息（HA1 控制链接）和同步数据（HA2 数据链接）。在“主动/主动”高可用性部署中，对等防火墙也必须将数据包转发到拥有该会话的高可用性对等。HA3 链接是一个第 2 层 (MAC-in-MAC) 链接，不支持第 3 层寻址或加密。

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| 28769<br>28260 | TCP<br>TCP | 用于 HA1 控制链路，以便清除高可用性对等防火墙之间的文本通信。HA1 链接是一个第 3 层链接，需要 IP 地址。 |
| 28 | TCP | 用于高可用性对等防火墙之间加密通信 (SSH over TCP) 的 A1 控制链路。 |
| 28770 | TCP | 侦听 HA1 备份链接的端口。 |
| 28771 | TCP | 用于检测信号备份。如果对 HA1 或 HA1 备份链路使用带内端口，Palo Alto Networks 建议在 MGT 接口上启用检测信号备份。 |
| 99<br>29281 | IP<br>UDP | HA2 链接用于在 HA 对中的防火墙之间同步会话，转发表、IPSec 安全关联和 ARP 表。HA2 链接上的数据流始终是单向的（“HA2 保持活动状态”时除外）；它从主动防火墙（主动/被动）或主动主要防火墙（主动/主动）流动到被动防火墙（主动/被动）或主动辅助防火墙（主动/主动）。HA2 链接是第 2 层链接，它在默认情况下使用以太网类型 0x7261。<br>还可以将 HA 数据链路配置为使用 IP（协议号 99）或 UDP（端口 29281）进行传输，因此允许 HA 数据链路跨越子网。 |

## 用于 Panorama 的端口

Panorama 使用以下端口。

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| 22 | TCP | 用于从客户端系统与 Panorama CLI 界面进行通信。 |
| 443 | TCP | 用于从客户端系统与防火墙 Panorama 界面进行通信。 |
| 444 | TCP | 用于 Panorama 和 Cortex 数据湖之间的通讯。 |
| 3978 | TCP | 用于 Panorama 与受管防火墙和/或受管日志收集器之间的通信，以及如下收集器组中各受管收集器之间的通信： |



© 2019 Palo Alto Networks, Inc.

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| | | • 对于 Panorama 与防火墙之间的通信，这是双向连接，在这种情况下，防火墙可以将日志转发到 Panorama，Panorama 也可以将配置更改推送到防火墙。此外，也可以通过同一连接发送上下文切换命令。<br>• 日志收集器使用此目标端口来将日志转发到 Panorama。<br>• 用于在 Panorama 模式中与 M 系列设备上的默认日志收集器以及专用日志收集器之间进行通信。 |
| 28443 | TCP | 用于受管设备（防火墙和日志收集器）从 Panorama 检索软件和内容更新。<br><br>仅运行 *PAN-OS 8.x* 和更高版本的设备才能通过此端口从 *Panorama* 检索更新。对于运行早期版本的设备，*Panorama* 通过端口 *3978* 推送更新数据包。 |
| 28769（5.1 及更高版本）<br>28260（5.0 及更高版本）<br>49160（5.0 及更低版本） | TCP<br>TCP<br>TCP | 用于使用明文通信的高可用性对等之间的高可用性连接和同步。其中任一对等均可发起通信。 |
| 28 | TCP | 用于使用加密通信 (SSH over TCP) 的 Panorama 高可用性对等之间的高可用性对等连接和同步。其中任一对等均可发起通信。<br>用于收集器组中日志收集器之间的通信，以便进行日志分发。 |
| 28270（6.0 及更高版本）<br>49190（5.1 及更低版本） | TCP | 用于收集器组中日志收集器之间的通信，以便进行日志分发。 |
| 2049 | TCP | Panorama 虚拟设备用于将日志写入 NFS 数据存储位置。 |
| 10443 | SSL | Panorama 用于提供有关威胁的上下文信息或将威胁调查无缝转移到威胁库和 AutoFocus 的端口。 |
| 23000 到 23999 | TCP、UDP 或 SSL | 用于 Panorama 和陷阱 ESM 组件之间的 Syslog 通信。 |

## 用于 GlobalProtect 的端口

GlobalProtect 使用以下端口。

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| 443 | TCP | 用于 GlobalProtect 应用和门户之间的通信，或 GlobalProtect 应用和网关之间的通信，以及 SSL 隧道连接。 |


© 2019 Palo Alto Networks, Inc.

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| | | GlobalProtect 网关还使用此端口从 GlobalProtect 应用收集主机信息，并执行主机信息配置文件 (HIP) 检查。 |
| 4501 | UDP | 用于 GlobalProtect 应用和网关之间的 IPSec 隧道连接。 |

有关如何使用回环接口以通过不同端口和地址访问 GlobalProtect 的提示，请参阅能否将 GlobalProtect 门户页面配置为可通过任意端口进行访问？

## 用于 User-ID 的端口

User-ID 是一个在用户 IP 地址与用户名和组成员资格之间建立映射关系，从而对网络上的用户活动启用基于用户或基于组的策略以及可见性（例如，为了快速跟踪可能成为威胁受害者的用户）的一个功能。为执行这种映射关系，防火墙、User-ID 代理（安装在基于 Windows 的系统或在防火墙上运行的 PAN-OS 集成代理上）和/或终端服务器代理必须能够连接到网络上的目录服务，这样才能执行组映射和用户映射。此外，如果代理在防火墙外的系统上运行，则必须能够连接到防火墙以将用户名映射的 IP 地址告知防火墙。下表列出了 User-ID 的通信要求以及建立连接所需的端口号。

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| 389 | TCP | 防火墙用来连接 LDAP 服务器（明文或启动传输层安全）（启动 TLS）以便将用户映射到组的端口。 |
| 3268 | TCP | 防火墙用来连接 Active Directory 全局目录服务器（明文或启动 TLS）以便将用户映射到组的端口。 |
| 636 | TCP | 防火墙用来通过 SSL 将 LDAP 连接到 LDAP 服务器以便将用户映射到组的端口。 |
| 3269 | TCP | 防火墙用来通过 SSL 将 LDAP 连接到 Active Directory 全局目录服务器以便将用户映射到组的端口。 |
| 514<br>6514 | TCP<br>UDP<br>SSL | 配置 User-ID 以监控用户映射的 Syslog 发件人时，User-ID 代理用于侦听身份验证 syslog 消息的端口。端口取决于代理和协议的类型：<br>• PAN-OS 集成 User-ID 代理 — 端口 6514 用于 SSL，端口 514 用于 UDP。<br>• 基于 Windows 的 User-ID 代理 — 端口 514 用于 TCP 和 UDP。 |
| 5007 | TCP | 防火墙用于从 User-ID 或终端服务器代理侦听用户映射信息的端口。代理在发现新的或更新的映射时就会发送 IP 地址和用户名映射以及一个时间戳。此外，它还会非常频繁的链接到防火墙来刷新已知的映射。 |
| 5006 | TCP | User-ID 代理用于侦听 XML API 请求的端口。此通信的源通常是运行调用 API 的脚本的系统。 |
| 88 | UDP/TCP | User-ID 代理用于验证 Kerberos 服务器的端口。防火墙首先尝试 UDP，然后回退至 TCP。 |
| 1812 | UDP | User-ID 代理用于验证 RADIUS 服务器的端口。 |



© 2019 Palo Alto Networks, Inc.

| 目标端口 | 协议 | 说明 |
| --- | --- | --- |
| 49 | TCP | User-ID 代理用于验证 TACACS+ 服务器的端口。 |
| 135 | TCP | User-ID 代理用于与 Microsoft 远程过程调用 (RPC) 终结点映射程序建立基于 TCP 的 WMI 连接的端口。建立连接后，终结点映射程序会将代理随即分配到在 49152-65535 端口范围内分配的端口。该代理使用此链接对 Exchange Server 或 AD 服务器安全日志、会话表发起 RPC 查询。这也是用于访问终端服务器的端口。<br>User-ID 代理还使用此端口来连接客户端系统以执行 Windows Management Instrumentation (WMI) 探测。 |
| 139 | TCP | User-ID 代理用于与 AD 服务器建立基于 TCP 的 NetBIOS 连接，以便对安全日志和会话信息发送 RPC 查询的端口。<br>User-ID 代理还使用此端口来连接客户端系统以执行 NetBIOS 探测（仅在基于 Windows 的 User-ID 代理上受支持）。 |
| 445 | TCP | User-ID 代理使用基于 TCP 的 SMB 连接将 Active Directory (AD) 连接到 AD 服务器，以便访问用户登录信息（打印假脱机程序和 Net 登录）的端口。 |
| 5985 | Http | User-ID 代理使用以通过 HTTP 上 WinRM 协议监控日志和会话信息的端口。 |
| 5986 | HTTPS | User-ID 代理使用以通过 HTTPS 上 WinRM 协议监控日志和会话信息的端口。 |


© 2019 Palo Alto Networks, Inc.

# 将防火墙重置为出厂默认设置

将防火墙重置为出厂默认设置将导致所有配置设置和日志丢失。

STEP 1 | 设置防火墙的控制台连接。

1. 使用串行电缆将计算机连接到控制台端口，并使用终端模拟软件 (9600-8-N-1) 连接到防火墙。

   如果您的计算机没有 *9* 针串行端口，请使用 *USB* 转串行端口转换器。

2. 输入您的登录凭据。
3. 输入以下 CLI 命令：

   **debug system maintenance-mode**

   在维护模式下，防火墙将重新启动。

STEP 2 | 将防火墙重置为出厂默认设置。

1. 当防火墙重新启动时，按 **Enter** 键以继续打开维护模式菜单。
2. 选择 **Factory Reset**（恢复出厂设置）并按 **Enter** 键。
3. 选择 **Factory Reset**（恢复出厂设置）并再次按 **Enter** 键。

   防火墙将会在没有任何配置设置的情况下重新启动。登录防火墙的默认用户名和密码是 admin/admin。

   要在防火墙上执行初始配置和设置网络连接，请参阅将防火墙集成到管理网络。



© 2019 Palo Alto Networks, Inc.

# 自举防火墙

自举可加快防火墙配置及许可流程，使防火墙在联网或不联网情况下于网络运行。通过自举，您可以选择是否为防火墙配置基本配置文件 (init-cfg.txt)，从而使其连接至 Panorama 并获取完整配置或为防火墙全面配置基本配置及可选的 bootstrap.xml 文件。

- USB 闪存盘支持
- init-cfg.txt 样本文件
- 为防火墙自举准备 USB 闪存盘
- 使用 USB 闪存盘自举防火墙

## USB 闪存盘支持

对基于硬件的 Palo Alto Networks 防火墙进行自举的 USB 闪存盘必须支持下列中的一项：

- 文件分配表 32 (FAT32)
- 第 3 拓展文件系统 (ext3)

防火墙可通过以下具备 USB2.0 或 USB3.0 连接功能的闪存盘自举：

| 支持的 USB 闪存盘 |
| --- |
| Kingston<br>• Kingston SE9 8GB (2.0)<br>• Kingston SE9 16GB (3.0)<br>• Kingston SE9 32GB (3.0) |
| SanDisk<br>• SanDisk Cruzer Fit CZ33 8GB (2.0)<br>• SanDisk Cruzer Fit CZ33 16GB (2.0)<br>• SanDisk Cruzer CZ36 16GB (2.0)<br>• SanDisk Cruzer CZ36 32GB (2.0)<br>• SanDisk Extreme CZ80 32GB (3.0) |
| Silicon Power<br>• Silicon Power Jewel 32GB (3.0)<br>• Silicon Power Blaze 16GB (3.0) |
| PNY<br>• PNY Attache 16GB (2.0)<br>• PNY Turbo 32GB (3.0) |



© 2019 Palo Alto Networks, Inc.

# init-cfg.txt 样本文件

自举过程需要 init-cfg.txt 文件；该文件是您可使用文本编辑器创建的基本配置文件。要创建此文件，请参阅创建 init-cfg.txt 文件。以下 init-cfg.txt 样本文件显示了文件支持的参数；您必须提供的参数以粗体显示。

| init-cfg.txt 样本（静态 IP 地址） | init-cfg.txt 样本（DHCP 客户端） |
|---|---|
| **type=static**<br>**ip-address=10.5.107.19**<br>**default-gateway=10.5.107.1**<br>**netmask=255.255.255.0**<br>**ipv6-address=2001:400:f00::1/64**<br>**ipv6-default-gateway=2001:400:f00::2**<br>hostname=Ca-FW-DC1<br>panorama-server=10.5.107.20<br>panorama-server-2=10.5.107.21<br>tplname=FINANCE_TG4<br>dgname=finance_dg<br>dns-primary=10.5.6.6<br>dns-secondary=10.5.6.7<br>op-command-modes=multi-vsys,jumbo-frame<br><br>dhcp-send-hostname=no<br>dhcp-send-client-id=no<br>dhcp-accept-server-hostname=no<br>dhcp-accept-server-domain=no | **type=dhcp-client**<br>ip-address=<br>default-gateway=<br>netmask=<br>ipv6-address=<br>ipv6-default-gateway=<br>hostname=Ca-FW-DC1<br>panorama-server=10.5.107.20<br>panorama-server-2=10.5.107.21<br>tplname=FINANCE_TG4<br>dgname=finance_dg<br>dns-primary=10.5.6.6<br>dns-secondary=10.5.6.7<br>op-command-modes=multi-vsys,jumbo-frame<br>dhcp-send-hostname=yes<br>dhcp-send-client-id=yes<br>dhcp-accept-server-hostname=yes<br>dhcp-accept-server-domain=yes |

下表介绍了 init-cfg.txt 文件中的字段。类型为必选；如果类型为静态，即必需选择 IP 地址、默认网关及网络掩码，或选择 IPv6 地址及 IPv6 默认网关。

| 字段 | 说明 |
|---|---|
| 类型 | （必选）IP 地址管理类型：静态或 DHCP 客户端（显示用户地址信息）。 |
| IP 地址 | （IPv4 静态管理地址必选）IPv4 地址。如果类型为 dhcp-client，则防火墙会忽略该字段。 |
| default-gateway | （IPv4 静态管理地址必选）管理界面的 IPv4 默认网关。如果类型为 dhcp-client，则防火墙会忽略该字段。 |
| 网络掩码 | （IPv4 静态管理地址必选）IPv4 网络掩码。如果类型为 dhcp-client，则防火墙会忽略该字段。 |
| ipv6-address | （IPv6 静态管理地址必选）管理界面的 IPv6 地址及 /前缀长度。如果类型为 dhcp-client，则防火墙会忽略该字段。 |
| ipv6-default-gateway | （IPv6 静态管理地址必选）管理界面的 IPv6 默认网关。如果类型为 dhcp-client，则防火墙会忽略该字段。 |
| 主机名： | （可选）防火墙的主机名。 |



© 2019 Palo Alto Networks, Inc.

| 字段 | 说明 |
| --- | --- |
| panorama- | （推荐）Panorama 主服务器的 IPv4 或 IPv6 地址。 |
| panorama-server-2 | （可选）Panorama 辅助服务器的 IPv4 或 IPv6 地址。 |
| tplname | （推荐）Panorama 模板名。 |
| dgname | （推荐）Panorama 模板设备组名。 |
| dns-primary | （可选）DNS 主服务器的 IPv4 或 IPv6 地址。 |
| dns-secondary | （可选）DNS 辅助服务器的 IPv4 或 IPv6 地址。 |
| vm-auth-key | （仅 VM 系列防火墙）虚拟机器验证密钥。 |
| op-command-modes | （可选）输入 multi-vsys、jumbo-frame 或输入两者，中间加逗号。自举时启用多个虚拟系统及巨型帧。 |
| dhcp-send-hostname | （仅 DHCP 客户端类型）DHCP 服务器确定“是”或“否”值。如果为“是”，防火墙将发送主机名至 DHCP 服务器。 |
| dhcp-send-client-id | （仅 DHCP 客户端类型）DHCP 服务器确定“是”或“否”值。如果为“是”，防火墙将发送客户端 ID 至 DHCP 服务器。 |
| dhcp-accept-server-hostname | （仅 DHCP 客户端类型）DHCP 服务器确定“是”或“否”值。如果为“是”，防火墙将从 DHCP 服务器接受其主机名。 |
| dhcp-accept-server-domain | （仅 DHCP 客户端类型）DHCP 服务器确定“是”或“否”值。如果为“是”，防火墙将从 DHCP 服务器接受其 DNS 服务器。 |

## 为防火墙自举准备 USB 闪存盘

您可使用 USB 闪存盘进行防火墙自举。但是，要执行这一操作，必须运行 PAN-OS 7.1.0 或更高版本映像并将防火墙重置为出厂默认设置。出于安全考虑，您仅可在防火墙处于出厂默认设置或删除所有私人数据后进行防火墙自举。

STEP 1 | 从订单完成邮件中获取支持订阅的序列号 (S/Ns) 及验证码。

STEP 2 | 在客户支持门户上注册新防火墙的 S/Ns。

1. 转到 support.paloaltonetworks.com 并登录，然后选择 **Assets**（资产）> **Devices**（设备）> **Register New Device**（注册新设备）> **Register device using Serial Number or Authorization Code**（使用序列号或授权代码注册设备）。
2. 按步骤注册防火墙。
3. 单击 **Submit**（提交）。

STEP 3 | 在客户支持门户上激活验证码后会生成许可密钥。

1. 前往 support.paloaltonetworks.com 并登陆，然后在左侧导航窗格中选择 **Assets**（资产）> **Devices**（设备）。
2. 单击之前注册的所有设备 S/N 的 **Action**（操作）链接（铅笔图标）。
3. 在激活许可证上，选择 **Activate Auth-Code**（激活授权代码）。
4. 输入 **Authorization code**（授权代码），单击 **Agree**（同意）并 **Submit**（提交）。


© 2019 Palo Alto Networks, Inc.

STEP 4 | 在 Panorama 中添加 S/Ns。

完成《Panorama 管理员指南》将防火墙添加为未受管设备的第一步。

STEP 5 | 创建 init-cfg.txt 文件。

创建提供自举参数的 init-cfg.txt 文件（强制性文件）。字段如示例 init-cfg.txt 文件所述。

如果 *init-cfg.txt* 文件丢失，自举过程将失败且防火墙将按正常启动序列中的默认配置重启。

每个字段中的密钥和值之间无空格，请不要添加空格，因为这会导致管理服务器上解析失败。

您可以通过将 S/N 加入文件名来拥有多个 init-cfg.txt 文件 — 各远程站点分别拥有相应的 init-cfg.txt 文件。例如：

0008C200105-init-cfg.txt

0008C200107-init-cfg.txt

如果没有加入 S/N 的文件名，防火墙将使用 init-cfg.txt 文件进行自举。

STEP 6 | （可选）创建 bootstrap.xml 文件。

可选的 bootstrap.xml 文件是您可从现有生产防火墙中导出的完整防火墙配置。

1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）> **Export named configuration snapshot**（导出已命名配置快照）。
2. 选择已保存或正在运行中的配置 **Name**（名称）。
3. 单击 **OK**（确定）。
4. 将文件重命名为 **`bootstrap.xml`**。

STEP 7 | 在客户支持门户上创建并下载自举包。

对于物理防火墙，自举包仅要求 /license 和 /config 目录。

使用以下其中一个方法创建并下载自举包：

- 使用方法 **1** 创建远程站点的专门自举包（您仅有 1 个 init-cfg.txt 文件）。
- 使用方法 **2** 为多个站点创建 1 个自举包。

方法 **1**

1. 在本地系统上，前往 support.paloaltonetworks.com 并登录。
2. 选择 **Assets**（资产）。
3. 选择要自举的防火墙 S/N。
4. 选择 **Bootstrap Container**（自举容器）。
5. 单击 **Select**（选择）。
6. 上传并 **Open**（打开）您创建的 init-cfg.txt 文件。
7. （可选）选择您创建的 bootstrap.xml 文件并 **Upload Files**（上传文件）。

   您必须使用来自采用同一型号及 *PAN-OS* 版本的防火墙的 *bootstrap.xml* 文件。

8. 选择 **Bootstrap Container Download**（自举容器下载）以下载保存于本地系统且命名为**`bootstrap_<S/N>_<date>.tar.gz`** 的 tar.gz 文件。自举容器包含与防火墙 S/N 相关的许可证密钥。

方法 **2**



© 2019 Palo Alto Networks, Inc.

在本地系统创建具备两个顶级目录的 tar.gz 文件： /license and /config。包含所有许可证及所有 init-cfg.txt 文件，并将 S/N 加入文件名。

您从客户支持门户下载的许可证密钥文件的文件名中包含 S/N。在自举过程中，PAN-OS 将根据防火墙 S/N 检查文件名中的 S/N。

STEP 8 | 使用安全复制 (SCP) 或 TFTP 导入创建的 tar.gz 文件至运行 PAN-OS 7.1.0 或更高版本映像的防火墙。

访问 CLI，并输入下列中的一项命令：

- **tftp import bootstrap-bundle file <path and filename> from <host IP address>**

  例如：

  **tftp import bootstrap-bundle file /home/userx/bootstrap/devices/pa5000.tar.gz from 10.1.2.3**
- **scp import bootstrap-bundle from <<user>@<host>:<path to file>>**

  例如：

  **scp import bootstrap-bundle from userx@10.1.2.3:/home/userx/bootstrap/devices/pa200_bootstrap_bundle.tar.gz**

STEP 9 | 准备 USB 闪存盘。

1. 将 USB 闪存盘插入您在先前步骤中使用的防火墙。
2. 输入以下 CLI 操作指令，用您的 tar.gz 文件名替换 "**pa5000.tar.gz**"。该指令将格式化 USB 闪存盘、解压文件并验证 USB 闪存盘：

   **request system bootstrap-usb prepare from pa5000.tar.gz**
3. 按 **y** 键继续。USB 闪存盘准备好后，将显示以下信息：

   已成功完成 USB 准备。
4. 从防火墙上移除 USB 闪存盘。
5. 您可按需要准备多个 USB 闪存盘。

STEP 10 | 将 USB 闪存盘转发至远程站点。

如果您使用方法 2 创建自举包，您可以使用相同的 USB 闪存盘内容进行多个远程站点的防火墙自举。您可将该内容导入多个 USB 闪存盘或多次使用的单个 USB 闪存盘。

# 使用 USB 闪存盘自举防火墙

在收到包含自举文件的新 Palo Alto Networks 防火墙及 USB 闪存盘后，即可进行防火墙自举。

*Microsoft Windows* 和 *Apple Mac* 操作系统无法读取 *USB* 闪存盘，原因是闪存盘使用 *ext4* 文件系统的格式。您必须安装第三方软件或使用 *Linux* 系统读取 *USB* 闪存盘。

STEP 1 | 防火墙必须处于出厂默认设置或已将所有私人数据删除。

STEP 2 | 为确保防火墙与企业总部间的连接，请使用以太网电缆将管理界面 (MGT) 连接至以下其一：

- 上游调制解调器
- 转换器或路由器端口
- 防火墙中的以太网插口



© 2019 Palo Alto Networks, Inc.

STEP 3 | 将 USB 闪存盘插入防火墙及防火墙电源上的 USB 端口。处于出厂默认设置的防火墙将通过 USB 闪存盘自举。

在配置防火墙时，防火墙“状态”灯将由黄变绿；自动提交成功。

STEP 4 | 确认自举已完成。引导期间，您可在控制台上查看基本状态日志，并确认引导流程已完成。

1. 如果您已在 init-cfg.txt 文件中包含 Panorama 值（panorama-server、tplname 和 dgname），检查 Panorama 受管设备、设备组及模板名称。
2. 通过访问 Web 界面并选择 **Dashboard**（仪表板）> **Widgets**（小部件）> **System**（系统）或使用 CLI 操作指令 **`show system info`** 和 **`show config running`** 来确定常规系统设置及配置。
3. 选择 **Device**（设备）> **Licenses**（许可证）或使用 CLI 操作指令 **`request license info`** 来确定证书安装状态。
4. 如果您已配置 Panorama，则可通过 Panorama 管理内容及软件版本。如果您未配置 Panorama，则可使用 Web 界面管理内容及软件版本。

# 设备遥测

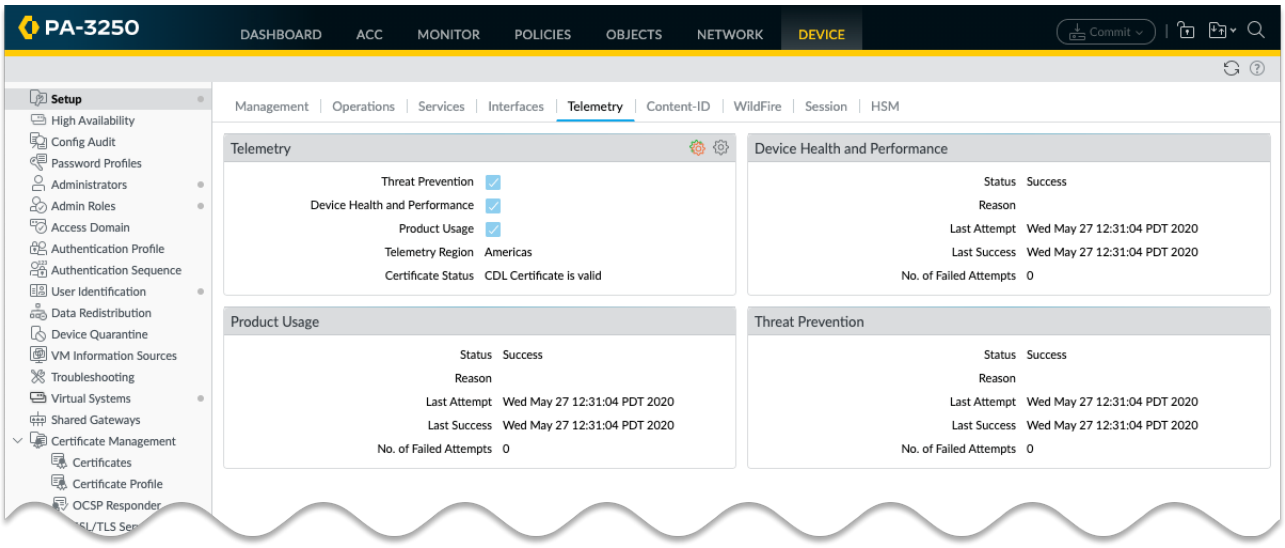
设备遥测将收集下一代防火墙或 Panorama 的相关数据，并通过将数据上传到 Cortex 数据湖，与 Palo Alto Networks 进行共享。该数据用于增强遥测应用程序，共享威胁情报。


> 设备遥测概述
> 设备遥测收集和传输间隔
> 管理设备遥测
> 监视设备遥测
> 采样设备遥测收集的数据

# 设备遥测概述

设备遥测将收集下一代防火墙或 Panorama 的相关数据，并通过将数据上传到 Cortex 数据湖，与 Palo Alto Networks 进行共享。这些数据用于为遥测应用程序提供支持，该应用程序基于云，可使您更轻松地监控和管理下一代防火墙和 Panorama。这些应用程序可提高设备运行状况、性能、容量规划和配置的可见性。通过这些应用程序，您可以最大限度地享受 Palo Alto Networks 所提供产品和服务带来的好处。

遥测数据还可用于共享威胁情报，提供增强的入侵防护、评估威胁签名，以及提高 PAN-DB URL 过滤、基于 DNS 的命令和控制 (C2) 签名和 WildFire 的恶意软件检测能力。




遥测数据将在有限的时间内收集并本地存储到您的设备上。仅当您为这些数据配置有目标区域时，才能与 Palo Alto Networks 共享。如果您的组织有 Cortex 数据湖许可证，那么，您只能将此数据发送到与您的 Cortex 数据湖实例所在位置相同的区域。如果您的组织没有 Cortex 数据湖许可证，那么，您必须安装设备证书才能共享这些数据。在这种情况下，您必须根据隐私和数据存储相关的所有适用的本地法律选择任何可用区域。

根据预定义收集间隔收集遥测数据，并与 Palo Alto Networks 共享。您可以通过启用/禁用数据类别来控制是否需要收集和共享数据。您还可以监控数据收集和传输的当前状态。

最后，您还可以针对防火墙出于遥测目的而收集的数据获取实时样本。有关可与 Palo Alto Networks 共享的所有遥测指标的完整说明（包括每个指标的隐私含义），请参阅 PAN-OS 设备遥测指标参考指南。



© 2019 Palo Alto Networks, Inc.

# 设备遥测收集和传输间隔

PAN-OS 将根据固定间隔收集并发送遥测数据。收集间隔的定义因指标而异，可以是下列之一：

- 每 20 分钟。
- 每 4 小时。
- 每周一次。

遥测数据将收集到数据包中。每个包都是截止到数据传输点收集到的所有数据的集合。这些包都存储在设备上，直至传输事件发生为止（每 4 小时传输一次）。一旦数据包被成功发送到 Palo Alto Networks，就可将其从设备上删除。

如果在将数据包发送到 Palo Alto Networks 时出现错误，防火墙将等待 10 分钟，然后重试。防火墙将继续尝试发送数据包，直至该包发送成功，或是需要释放存储空间以收集新的遥测数据。

按照固定的传输间隔，防火墙首先会发送为该事件安排的数据包。这些数据包成功发送后，防火墙将发送先前传输事件中存储的任何发送失败的数据包。



© 2019 Palo Alto Networks, Inc.

# 管理设备遥测

若要管理设备遥测，您可以：

- 启用设备遥测
- 禁用设备遥测
- 管理设备遥测收集的数据
- 管理历史设备遥测

## 启用设备遥测

设备默认不会与 Palo Alto Networks 共享数据。启用共享后，您可以通过下列操作停止共享所有设备遥测数据：**Device**（设备）> **Setup**（设置）> **Telemetry**（遥测），取消选中 **Enable Telemetry**（启用遥测）复选框，然后提交更改。

若要启用设备遥测以与 Palo Alto Networks 共享数据：

STEP 1 | 启用 Cortex 数据湖。

1. 如果您的组织没有 Cortex 数据湖许可证，请在设备上安装一个设备证书（如果还未安装）。

   如果您的组织有 Cortex 数据湖许可证，请务必将其激活。
2. 确保您的网络已正确配置 ，以便防火墙发送数据到 Cortex 数据湖。

STEP 2 | 导航至**Device**（设备）> **Setup**（设置）> **Telemetry**（遥测）

STEP 3 | 编辑 **Telemetry**（遥测）小部件。

STEP 4 | 在 **Telemetry Destination**（遥测目标）中，选择您所在的区域。如果您的组织正在使用 Cortex 数据湖，则必须使用 Cortex 数据湖被配置使用的区域。

STEP 5 | 单击 **OK**（确定）并提交更改。

## 禁用设备遥测

如果下一代防火墙配置为与 Palo Alto Networks 共享数据，则可通过下列操作禁用此共享：

STEP 1 | 导航至**Device**（设备）> **Setup**（设置）> **Telemetry**（遥测）

STEP 2 | 编辑 **Telemetry**（遥测）小部件。

STEP 3 | 取消选中 **Enable Telemetry**（启用遥测）复选框。

STEP 4 | 单击 **OK**（确定）并提交更改。

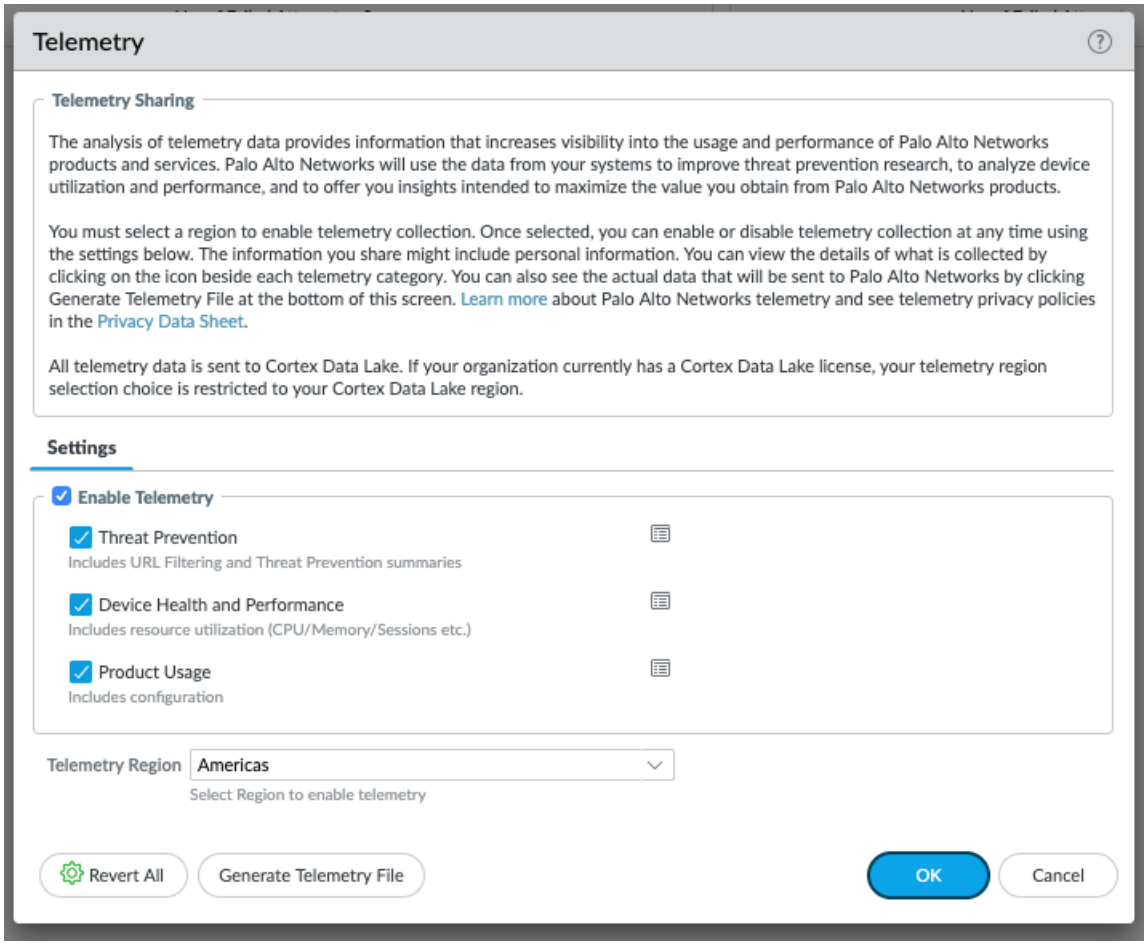
STEP 5 | 当前存储在 Cortex 数据湖中的任何遥测数据一旦被防火墙上传，将在一年后自动清除。或者，如果您不想数据在禁用遥测后的这段时间留存在 Cortex 数据湖中，请开立支持票证，并要求 Palo Alto Networks 清除您的遥测数据。

## 管理设备遥测收集的数据

选择 **Device**（设备）> **Setup**（设置）> **Telemetry**（遥测）以查看当前收集的遥测类别。若要更改这些类别，请编辑“遥测”小部件。取消选择您不希望防火墙收集的任何类别，单击 **OK**（确定），然后提交更改。



© 2019 Palo Alto Networks, Inc.




若要停止共享所有设备遥测，请取消选中 *Enable Telemetry*（启用遥测）复选框，然后提交更改。

# 管理历史设备遥测

PAN-OS 10.0 版本的设备遥测发生了显著变化。在 10.0 版本之前，遥测数据主要用于威胁情报。从 10.0 开始，威胁情报指标仍占设备收集数据的大头，但更多收集的则是设备运行状况、性能和配置相关的数据。

换句话说，PAN-OS 10.0 的设备遥测扩大了先前版本的数据收集范围。PAN-OS 10.0 还将遥测数据发送到与先前版本不同的云位置。但是，运行 PAN-OS 10.0 的下一代防火墙仍支持历史遥测。唯一区别在于 10.0 设备遥测的用户界面无法管理该历史数据收集功能。

如果有现存的下一代防火墙，且已启用任何历史遥测数据类别，那么，一旦升级到 PAN-OS 10.0，防火墙仍将继续收集并共享这些信息。如果想关闭此遥测数据共享，可使用以下 CLI 命令：

```
set deviceconfig system update-schedule statistics-service application-
reports no
set deviceconfig system update-schedule statistics-service threat-
prevention-reports no
set deviceconfig system update-schedule statistics-service threat-
prevention-information no
set deviceconfig system update-schedule statistics-service threat-
prevention-pcap no
set deviceconfig system update-schedule statistics-service passive-dns-
monitoring no
set deviceconfig system update-schedule statistics-service url-reports no
```


© 2019 Palo Alto Networks, Inc.

```
set deviceconfig system update-schedule statistics-service health-
performance-reports no
set deviceconfig system update-schedule statistics-service file-
identification-reports no
```

如果您安装有 10.0 版防火墙，且已关闭此遥测共享，但是您希望将此数据与 Palo Alto Networks 共享，那么您可以使用下列命令打开此遥测共享：

```
set deviceconfig system update-schedule statistics-service application-
reports yes
set deviceconfig system update-schedule statistics-service threat-
prevention-reports yes
set deviceconfig system update-schedule statistics-service threat-
prevention-information yes
set deviceconfig system update-schedule statistics-service threat-
prevention-pcap yes
set deviceconfig system update-schedule statistics-service passive-dns-
monitoring yes
set deviceconfig system update-schedule statistics-service url-reports yes
set deviceconfig system update-schedule statistics-service health-
performance-reports yes
set deviceconfig system update-schedule statistics-service file-
identification-reports yes
```

您可以使用以下 CLI 命令查看设备是否正在收集和共享此历史遥测数据：

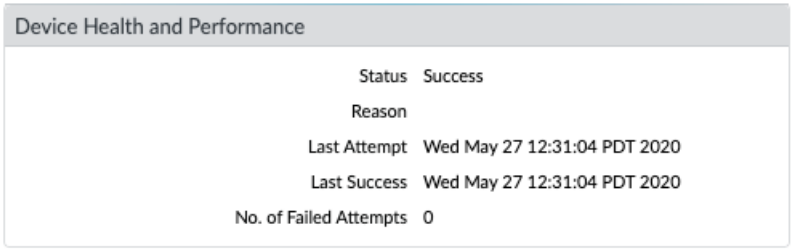
```
show deviceconfig system update-schedule statistics-service
```



© 2019 Palo Alto Networks, Inc.

# 监视设备遥测

PAN-OS 将向您显示每个遥测类别的共享状态。可通过 **Device**（设备）> **Setup**（设置）> **Telemetry**（遥测）查看每个指标类别的小部件。



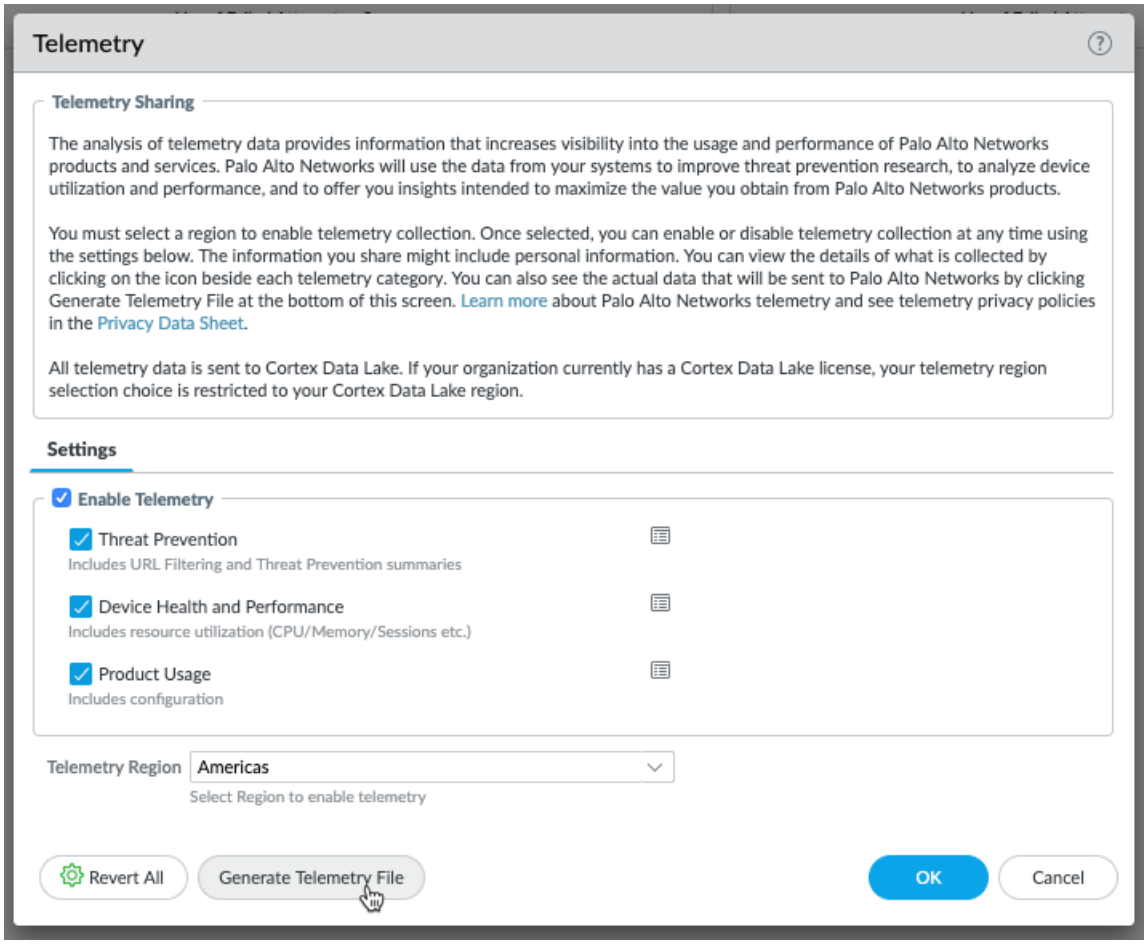

一旦失败，设备将在下一个传输时重新尝试发送。如果问题仍存在，请执行检查，确保设备已正确配置为发送数据到 Cortex 数据湖：

- 如果您的组织拥有 Cortex 数据湖许可证，请务必激活您的 Cortex 数据湖许可证，并确保您的防火墙已配置为使用 Cortex 数据湖。
- 如果您的组织没有 Cortex 数据湖许可证，请务必安装设备证书，并确保您的网络已配置为允许 Cortex 数据湖流量。


© 2019 Palo Alto Networks, Inc.

# 采样设备遥测收集的数据

您可以下载设备遥测收集并与 Palo Alto Networks 共享的数据的实例。为此，请前往 **Device**（设备）> **Setup**（设置）> **Telemetry**（遥测），然后编辑 **Telemetry**（遥测）小部件。然后单击 **Generate Telemetry File**（生成遥测文件）。




数据收集将需要几分钟，具体取决于防火墙的速度。该过程完成过后，单击 **Download Device Telemetry Data**（下载设备遥测数据）。遥测数据包会压缩成 tar 包，并置于默认浏览器下载目录中。

有关设备遥测收集并与 Palo Alto Networks 共享的每个指标的说明，请参阅 PAN-OS 设备遥测指标参考指南。

# 身份验证

身份验证是一种通过验证用户身份，从而仅允许合法用户访问，进而保护服务和应用程序的方法。有一些防火墙和 Panorama 功能需要身份验证。管理员进行身份验证以访问防火墙和 Panorama 的 Web 界面、CLI 或 XML API。最终用户通过身份验证门户或 GlobalProtect 进行身份验证，以访问各种服务和应用程序。有几种身份验证服务可供您选择，以保护您的网络并与您现有的安全基础设施相匹配，同时确保流畅的用户体验。

如果您拥有公钥基础设施，则可以部署证书以启用身份验证，而无需用户手动响应登录挑战（请参阅证书管理）。或者，除证书外，还可以执行交互式身份验证，即要求用户使用一种或多种方法进行身份验证。以下主题描述了如何实现、测试和排除不同类型的交互式身份验证故障：


> 身份验证类型
> 计划您的身份验证部署
> 配置多重因素身份验证
> 配置 SAML 身份验证
> 配置 Kerberos 单一登入
> 配置 Kerberos 服务器身份验证
> 配置 TACACS+ 身份验证
> 配置 RADIUS 身份验证
> 配置 LDAP 身份验证
> 身份验证服务器连接超时
> 配置本地数据库身份验证
> 配置身份验证配置文件和序列
> 测试身份验证服务器连接
> 身份验证策略
> 身份验证问题故障排除

# 身份验证类型


- 外部身份验证服务
- 多重因素身份验证
- SAML
- Kerberos
- TACACS+
- RADIUS
- LDAP
- 本地身份验证


## 外部身份验证服务

防火墙和 Panorama 可以使用外部服务器来控制对 Web 界面的管理访问，并通过身份验证门户和 GlobalProtect 来控制最终用户访问服务或应用程序。在这种情况下，对您的网络而言，无论是内部服务（如 Kerberos）还是外部服务（如 SAML 标识提供商），任何不属于防火墙或 Panorama 的本地身份验证服务都将被视为外部身份验证服务。防火墙和 Panorama 可以集成的服务器类型包括多重因素身份验证 (MFA)、SAML、Kerberos、TACACS+、RADIUS 和 LDAP。虽然您也可以使用防火墙和 Panorama 支持的本地身份验证服务，通常会优选外部服务，因为外部服务可提供以下功能：

- 对外部标识存储中的所有用户帐户进行集中管理。所有支持的外部服务都为最终用户和管理员提供此选项。
- 集中管理帐户授权（角色和访问域分配）。SAML、TACACS + 和 RADIUS 的管理员可以使用此选项。
- 单点登录 (SSO)，使用户对访问多个服务和应用程序仅执行一次身份验证。SAML 和 Kerberos 支持 SSO。
- 不同类型（因素）的多重身份验证挑战，以保护您最敏感的服务和应用程序。MFA 服务支持此选项。

通过外部服务的身份验证需要服务器配置文件以定义防火墙与服务相连接的方式。将服务器配置文件分配给身份验证配置文件，这些配置文件确定为每个应用程序和用户组自定义的设置。例如，您可以为访问 Web 界面的管理员配置一个身份验证配置文件，为访问 GlobalProtect 门户的最终用户配置另一个配置文件。有关详细信息，请参阅配置身份验证配置文件和序列。

## 多重因素身份验证

您可以配置多重因素身份验证 (MFA)，以确保每个用户在访问高敏感度的服务和应用程序时使用多种方法（因素）进行身份验证。例如，您可以强制用户输入登录密码，输入手机接收到的验证码，然后才允许访问重要的财务文档。这种方法有助于防止攻击者仅通过窃取密码来访问网络中的每个服务和应用程序。当然，并不是每个服务和应用程序都需要相同程度的保护，而且用户频繁访问的敏感度较低的服务和应用程序可能并不需要 MFA。为了适应各种安全需求，您可以根据具体的服务、应用程序和最终用户配置身份验证策略，以触发 MFA 或单一身份验证因素（例如登录凭据或证书）。

在选择要执行的身份认证因素的数量和类型时，了解策略评估对用户体验的影响至关重要。当用户请求服务或应用程序时，防火墙应首先评估身份验证策略。如果请求与已启用 MFA 的身份验证策略规则匹配，则防火墙将显示身份验证门户 Web 表单，以便用户可以对第一个因素进行身份验证。如果身份验证成功，防火墙会为每个其他因素显示一个 MFA 登录页面。一些 MFA 服务提示用户从两到四个因素中选择一个，这在某些因素不可用时非常有用。如果所有因素均通过身份验证，防火墙将评估所请求的服务或应用程序的安全策略。



为了减少中断用户工作流程的身份验证挑战的频率，您可以配置使用 Kerberos 或 SAML 单点登录 *(SSO)* 身份验证的第一个因素。

要实现 *GlobalProtect* 的 *MFA*，请参阅配置 GlobalProtect 以加快多重因素身份验证通知。



© 2019 Palo Alto Networks, Inc.

您不能在身份验证序列中使用 *MFA* 身份验证配置文件。

对于通过身份验证策略的最终用户身份验证，防火墙直接与多个 MFA 平台（Duo v2、Okta Adaptive、PingID 和 RSA SecurID）集成，并通过 RADIUS 或 SAML 集成到所有其他 MFA 平台。对于 GlobalProtect 门户和网关的远程用户身份验证以及 Panorama 和 PAN-OS Web 界面的管理员身份验证，防火墙仅使用 RADIUS 和 SAML 与 MFA 供应商集成。

防火墙支持以下 MFA 因素：

| 因素 | 说明 |
| --- | --- |
| 推送 | 端点设备（如手机或平板电脑）会提示用户允许或拒绝身份验证。 |
| 短信服务 (SMS) | 端点设备上的 SMS 消息提示用户允许或拒绝身份验证。在某些情况下，端点设备提供用户必须在 MFA 登录页面中输入的代码。 |
| 语音 | 自动化电话提醒提示用户通过按下手机上的键或在 MFA 登录页面中输入代码进行身份验证。 |
| 一次性密码 (OTP) | 端点设备提供自动生成的字母数字字符串，用户将其输入到 MFA 登录页面中以启用单个事务或会话的身份验证。 |

## SAML

您可以使用安全声明标记语言 (SAML) 2.0 来对访问防火墙或 Panorama Web 界面的管理员以及访问组织内部或外部 Web 应用程序的最终用户进行身份验证。在每位用户访问大量应用程序并为每位用户进行身份验证将阻碍用户生产力的环境中，您可以配置 SAML 单点登录 (SSO) 以便登录一次即可访问多个应用程序。同样，SAML 单点退出 (SLO) 使用户能够通过退出一个会话来结束多个应用程序的会话。访问 Web 界面的管理员和通过 GlobalProtect 或身份验证门户访问应用程序的最终用户可以使用 SSO。SLO 可供管理员和 GlobalProtect 最终用户使用，但身份验证门户最终用户不能使用。当您在防火墙上或在 Panorama 上配置 SAML 身份验证时，可以指定管理员授权的 SAML 属性。SAML 属性使您能够通过目录服务来快速更改管理员的角色、访问域和用户组，这通常比在防火墙或 Panorama 上重新配置设置更为容易。



管理员无法使用 *SAML* 对防火墙或 *Panorama CLI* 进行身份验证。

您不能在身份验证序列中使用 *SAML*身份验证配置文件。

SAML 身份验证需要一个控制访问应用程序的服务提供商（防火墙或 Panorama），以及一个对用户进行身份验证的标识提供商 (IdP)，例如 PingFederate。当用户请求服务或应用程序时，防火墙或 Panorama 会拦截请求，并将用户重定向到 IdP 进行身份验证。然后，IdP 对用户进行身份验证并返回一个 *SAML* 声明，表示身份验证成功或失败。针对身份验证门户最终用户的 SAML 身份验证对通过身份验证门户访问应用程序的最终用户进行 SAML 身份验证。



© 2019 Palo Alto Networks, Inc.

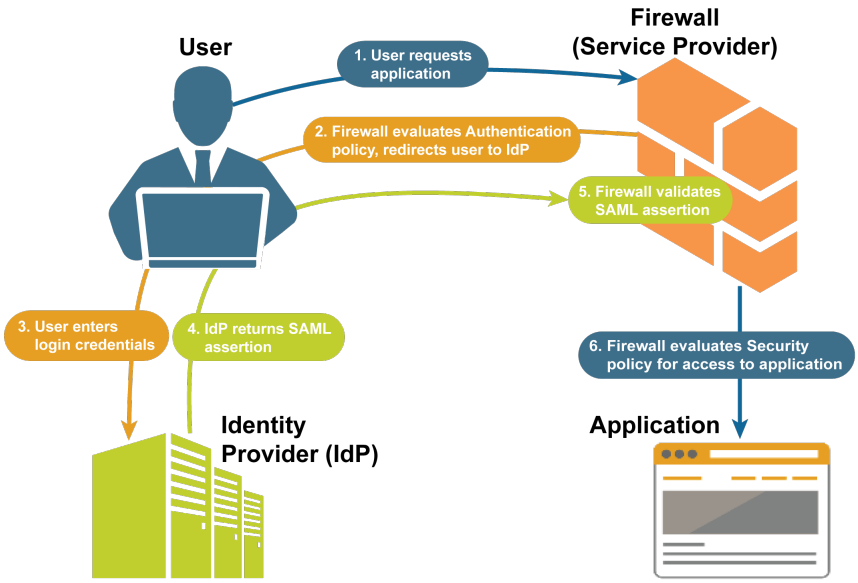



图 **1:** 针对身份验证门户最终用户的 **SAML** 身份验证

## Kerberos

Kerberos 是一种通过使用唯一密钥（称为票据）实现不安全网络上各方之间信息安全交换以标识各方的身份验证协议。防火墙和 Panorama 支持两种类型的管理员和最终用户 Kerberos 身份验证：

- **Kerberos server authentication**（**Kerberos** 服务器身份验证）— Kerberos 服务器配置文件使用户能够在本地对 Active Directory 域控制器或 Kerberos V5 兼容的身份验证服务器进行身份验证。这种身份验证方式为交互式，要求用户输入用户名和密码。有关配置步骤，请参阅配置 Kerberos 服务器身份验证。
- **Kerberos single sign-on (SSO)**（**Kerberos** 单点登录 **(SSO)**）— 支持 Kerberos V5 SSO 的网络仅在用户首次访问网络时提示用户登录（例如，登录 Microsoft Windows）。在此初始登录之后，用户便可以在网络中访问任何基于浏览器的服务（例如，防火墙 Web 界面），而不必重新登录，除非 SSO 会话过期。（您的 Kerberos 管理员负责设置 SSO 会话的持续时间。）如果您同时启用 Kerberos SSO 和外部身份验证服务（例如，TACACS+ 服务器），设备首先尝试 SSO，并且只有在失败的情况下才会返回到外部服务进行身份验证。要支持 Kerberos SSO，您的网络需要：
  - Kerberos 基础架构，包括密钥分发中心 (KDC)（含身份验证服务器 (AS) 和票据授予服务 (TGS)）。
  - 防火墙或 Panorama 的 Kerberos 帐户可对用户进行身份验证。该帐户需要创建 Kerberos Keytab，即包含防火墙或 Panorama 的主体名及哈希密码的文件。SSO 进程需要 keytab。

  有关配置步骤，请参阅配置 Kerberos 单点登录。

*Kerberos SSO* 仅适用于 *Kerberos* 环境内部的服务和应用程序。要使 *SSO* 用于外部服务和应用程序，请使用 SAML。

## TACACS+

增强型终端访问控制器访问控制系统 (TACACS+) 是一组通过集中式服务器进行身份验证和授权的协议。TACACS+ 加密用户名和密码，比仅加密密码的 RADIUS 更安全。因使用 TCP，TACACS+ 也更可靠，而 RADIUS 则使用 UDP。您可以为防火墙上的最终用户或管理员以及 Panorama 上的管理员配置 TACACS+ 身份验证。或者，您可以使用 TACACS+ 供应商特定属性 (VSA) 来管理管理员授权。TACACS+ VSA 使您能够通过目录服务（而不是重新配置防火墙和 Panorama 上的设置）来快速更改管理员的角色、访问域和用户组。

防火墙和 Panorama 支持以下 TACACS+ 属性和 VSA。有关在 TACACS+ 服务器上定义这些 VSA 的步骤，请参阅 TACACS+ 服务器文档。



© 2019 Palo Alto Networks, Inc.

| 姓名 | 值 |
| --- | --- |
| 服务 | 需要此属性来确定特定于 Palo Alto Networks 的 VSA。必须将值设置为 **`PaloAlto`**。 |
| 协议 | 需要此属性来确定特定于 Palo Alto Networks 设备的 VSA。必须将值设置为 **`firewall`**。 |
| PaloAlto-Admin-Role | 防火墙上的默认（动态）管理角色名称或定制管理角色名称。 |
| PaloAlto-Admin-Access-Domain | 防火墙管理员的访问域名（在 **Device**（设备）> **Access Domains**（访问域）页面设置）。如果防火墙具有多个虚拟系统，则定义此 VSA。 |
| PaloAlto-Panorama-Admin-Role | Panorama 上的默认（动态）管理角色名称或定制管理角色名称。 |
| PaloAlto-Panorama-Admin-Access-Domain | 设备组和模板管理员的访问域名（在 **Panorama** > **Access Domains**（访问域）页面设置）。 |
| PaloAlto-User-Group | 身份验证配置文件允许列表中的用户组的名称。 |

# RADIUS

远程身份验证拨入用户服务 (RADIUS) 是一种广受支持的网络协议，提供集中式身份验证和授权。您可以为防火墙上的最终用户或管理员以及 Panorama 上的管理员配置 RADIUS 身份验证。或者，您可以使用 RADIUS 供应商特定属性 (VSA) 来管理管理员授权。RADIUS VSA 使您能够通过目录服务（而不是重新配置防火墙和 Panorama 上的设置）来快速更改管理员的角色、访问域和用户组。您还可以将防火墙配置为使用 RADIUS 服务器以：

- 从 GlobalProtect 端点收集 VSA。
- 实施多重因素身份验证。

向 RADIUS 服务器发送身份验证请求时，防火墙和 Panorama 将身份验证配置文件名用作网络访问服务器 (NAS) 标识符，即便在配置文件已分配至启动身份验证流程的服务器的身份验证序列中（例如，对 Web 界面的管理访问）。

防火墙和 Panorama 支持以下 RADIUS VSA。要在 RADIUS 服务器上定义 VSAs，您必须指定供应商代码（Palo Alto Networks 防火墙或 Panorama 为 25461）及 VSA 名称及编码。某些 VSA 还需要一个值。有关定义这些 VSA 的步骤，请参阅 RADIUS 服务器文档。

或者，您可以下载 Palo Alto Networks RADIUS 字典。该字典定义 Palo Alto Networks 防火墙和 RADIUS 服务器用于相互进行通信的身份验证属性，然后将其安装在 RADIUS 服务器上，以便映射属性到 RADIUS 二进制数据中。

预定义服务器上用户的动态管理员角色时，使用小写字母指定角色（例如，输入 ***`superuser`***，而不是 ***`SuperUser`***）。

在思科安全访问控制服务器 *(ACS)* 上配置高级供应商选项时，必须将 *Vendor Length Field Size*（供应商长度字段大小）和 *Vendor Type Field Size*（供应商类型字段大小）同时设置为 ***`1`***。否则，身份验证将失败。


© 2019 Palo Alto Networks, Inc.

| 姓名 | 编码 | 值 |
| --- | --- | --- |
| 用于管理员帐户管理和身份验证的 VSA | | |
| PaloAlto-Admin-Role | 1 | 防火墙上的默认（动态）管理角色名称或定制管理角色名称。 |
| PaloAlto-Admin-Access-Domain | 2 | 防火墙管理员的访问域名（在 **Device**（设备）> **Access Domains**（访问域）页面设置）。如果防火墙具有多个虚拟系统，则定义此 VSA。 |
| PaloAlto-Panorama-Admin-Role | 3 | Panorama 上的默认（动态）管理角色名称或定制管理角色名称。 |
| PaloAlto-Panorama-Admin-Access-Domain | 4 | 设备组和模板管理员的访问域名（在 **Panorama** > **Access Domains**（访问域）页面设置）。 |
| PaloAlto-User-Group | 5 | 身份验证配置文件引用的用户组的名称。 |
| 从 GlobalProtect 端点转发到 RADIUS 服务器的 VSA | | |
| PaloAlto-User-Domain | 6 | 在定义这些 VSA 时，请勿指定值。 |
| PaloAlto-Client-Source-IP | 7 | |
| PaloAlto-Client-OS | 8 | |
| PaloAlto-Client-Hostname | 9 | |
| PaloAlto-GlobalProtect-Client-Version | 10 | |

# LDAP

轻型目录访问协议 (LDAP) 是用于访问信息目录的标准协议。您可以为最终用户和防火墙或 Panorama 管理员配置 LDAP 身份验证。

配置防火墙以连接到 LDAP 服务器还可以根据用户和用户组（而不仅是 IP 地址）来定义策略规则。有关步骤，请参阅将用户映射到组和启用基于用户和组的策略。

# 本地身份验证

虽然防火墙和 Panorama 为管理员和最终用户提供本地身份验证，但在大多数情况下，外部身份验证服务是可取的，因为它们提供帐户集中管理功能。但是，您可能需要不通过您的组织为常规帐户预留的目录服务器管理的特殊用户帐户。例如，您可以定义防火墙本地的超级用户帐户，以便在目录服务器关闭时访问防火墙。在这种情况下，您可以使用以下本地身份验证方法：

- （仅限防火墙）本地数据库身份验证 — 要配置本地数据库身份验证，应创建一个在防火墙上本地运行的数据库。该数据库包括用户帐户（用户名和密码或哈希密码）和用户组。在您只知道哈希密码（而不是明文密码）的情况下，此类身份验证对于创建重用现有 Unix 帐户凭据的用户帐户非常有用。由于本地数据库身份验证与身份验证配置文件相关联，您可以适应不同用户组需要不同身份验证设置的部署，例如 Kerberos 单点登录 (SSO) 或多重因素身份验证 (MFA)。（有关详细信息，请参阅配置身份验证配置文件和序列）。对于使用明文密码的帐户，您也可以定义密码复杂性和到期设置。访问防火墙（但不是



© 2019 Palo Alto Networks, Inc.

Panorama）的管理员以及通过身份验证门户或 GlobalProtect 访问服务和应用程序的最终用户都可以使用此身份验证方法。

- 无数据库的本地身份验证 — 您可以在未创建在防火墙或 Panorama 上本地运行的用户和用户组数据库的情况下配置防火墙管理帐户或 Panorama 管理帐户。由于此方法与身份验证配置文件无关，因此您无法将其与 Kerberos SSO 或 MFA 组合。但是，这是唯一允许密码配置文件的身份验证方法，可让您将各个帐户与不同于全局设置的密码过期设置相关联。（有关详细信息，请参阅定义密码复杂度和过期设置）


© 2019 Palo Alto Networks, Inc.

# 计划您的身份验证部署

在为访问防火墙的管理员和通过身份验证门户访问服务和应用程序的最终用户实施身份验证解决方案之前，需要考虑以下几个关键问题。

对于最终用户和管理员，请考虑：

- 如何利用您的现有安全基础设施？通常，将防火墙与现有基础设施集成比为防火墙服务单独设置一个新的解决方案要更快速、价格更便宜。防火墙可以与多重因素身份验证、SAML、Kerberos、TACACS+、RADIUS 和 LDAP 服务器集成。如果您的用户访问网络外部的服务和应用程序，则可以使用 SAML 将防火墙与控制访问外部和内部服务和应用程序的标识提供商 (IdP) 集成。
- 如何优化用户体验？如果不希望用户手动进行身份验证，并且您拥有公钥基础设施，则可以实施证书身份验证。另一个选择是实施 Kerberos 或 SAML 单点登录 (SSO)，这样用户只需登录一个服务和应用程序即可访问多个服务和应用程序。如果网络需要额外的安全性，可以将证书身份验证与交互式（质询-响应）身份验证相结合。
- 是否需要不通过您的组织为常规帐户预留的目录服务器管理的特殊用户帐户？例如，您可以定义防火墙本地的超级用户帐户，以便在目录服务器关闭时访问防火墙。您可以为这些专用帐户配置本地身份验证。



外部验证服务通常比本地验证服务更好，因为其可提供帐户集中管理、可靠的验证服务，以及常规的日志记录和故障排除功能。

仅对于最终用户，请考虑：

- 哪些服务和应用程序比其他服务和应用程序更敏感？例如，您可能需要对关键财务文档而不是搜索引擎进行严格的身份验证。为了保护最敏感的服务和应用程序，您可以配置多重因素身份验证 (MFA)，以确保每个用户在访问这些服务和应用程序时使用多种方法（因素）进行身份验证。为了适应各种安全需求，您可以根据具体的服务、应用程序和最终用户配置身份验证策略规则，以触发 MFA 或单一身份验证因素（例如登录凭据或证书）。其他用于减少攻击面的方法包括网络分段和用于应用程序的用户组。

仅对于管理员，请考虑：

- 您是否使用外部服务器集中管理所有管理帐户的授权？通过在外部服务器上定义供应商特定属性 (VSA)，您可以通过目录服务（而不是重新配置防火墙的设置）来快速更改管理员角色分配。VSA 还使您能为具有多个虚拟系统的防火墙的管理员指定访问域。SAML、TACACS+ 和 RADIUS 支持外部授权。



© 2019 Palo Alto Networks, Inc.

# 配置多重因素身份验证

要使用多重因素身份验证 (MFA) 来保护敏感的服务和应用程序，您必须配置身份验证门户以显示第一个身份验证因素的 Web 表单，并记录身份验证时间戳。防火墙使用时间戳来评估身份验证策略规则的超时。要启用其他身份验证因素，可以通过 RADIUS 或供应商 API 将防火墙与 MFA 供应商集成。评估身份验证策略后，防火墙将评估安全策略，因此必须为这两种策略配置规则。

*Palo Alto Networks* 通过应用程序内容更新为 MFA 供应商提供支持。这意味着如果您使用 *Panorama* 将设备组配置推送到防火墙，则必须在防火墙上安装相同的应用程序更新，如 *Panorama* 所示，以避免供应商支持的不匹配。

*MFA* 供应商 *API* 集成仅能通过身份验证策略对最终用户身份验证进行支持。对于 *GlobalProtect* 门户或网关的远程用户身份验证或 *PAN-OS* 或 *Panorama Web* 界面的管理员身份验证，您只能使用受 *RADIUS* 或 *SAML* 支持的 *MFA* 供应商； 这些用例不支持通过供应商 *API* 提供的 *MFA* 服务。

STEP 1 | 在 **Redirect**（重定向）模式下配置身份验证门户，以显示第一个身份验证因素的 Web 表单、记录身份验证时间戳，并更新用户映射。

STEP 2 | 配置以下服务器配置文件之一，以定义防火墙如何连接到为第一个身份验证因素的用户进行身份验证的服务。

- 添加 RADIUS 服务器配置文件。如果防火墙通过 RADIUS 与 MFA 供应商集成，则必须这样做。在这种情况下，MFA 供应商提供第一个和所有其他身份验证因素，因此可跳过下一步（配置 MFA 服务器配置文件）。如果防火墙通过 API 与 MFA 供应商集成，您仍然可以使用 RADIUS 服务器配置文件作为第一个因素，但还需要 MFA 服务器配置文件作为其他因素。
- 添加 SAML IdP 服务器配置文件。
- 添加 Kerberos 服务器配置文件。
- 添加 TACACS+ 服务器配置文件。
- 添加 LDAP 服务器配置文件。

在大多数情况下，推荐将外部服务用于第一个身份验证因素。但是，您可以配置配置本地数据库身份验证作为替代方案。

STEP 3 | 添加 MFA 服务器配置文件。

配置文件对防火墙如何连接到 MFA 服务器进行定义。在第一个因素之后，为每个身份验证因素添加单独的配置文件。防火墙通过供应商 API 与这些 MFA 服务集成。您最多可以指定三个其他因素。尽管一些供应商让用户从几个因素中选择一个，但每个 MFA 供应商只提供一个因素。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Multi Factor Authentication**（多重因素身份验证），并 **Add**（添加）配置文件。
2. 输入标识 MFA 服务器的 **Name**（名称）。
3. 在与 MFA 服务器建立安全连接时，请选择防火墙将用于验证 MFA 服务器证书的 **Certificate Profile**（证书配置文件）。
4. 选择部署的 **MFA Vendor**（**MFA** 供应商）。
5. 配置每个供应商属性的 **Value**（值）。

   属性对防火墙如何连接到 MFA 服务器进行定义。每个供应商 **Type**（类型）需要不同的属性和值；有关详细信息，请参阅供应商文档。
6. 单击 **OK**（确定）保存配置文件。

STEP 4 | 配置身份验证配置文件。



© 2019 Palo Alto Networks, Inc.

该配置文件定义了用户必须响应的身份验证因素的顺序。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识身份验证配置文件。
3. 选择第一个身份验证因素的 **Type**（类型），并选择相应的 **Server Profile**（服务器配置文件）。
4. 选择 **Factors**（因素），**Enable Additional Authentication Factors**（启用其他身份验证因素），并 **Add**（添加）您配置的 MFA 服务器配置文件。

   防火墙将按照列出的顺序从上到下调用每个 MFA 服务。
5. 单击 **OK**（确定）保存身份验证配置文件。

### STEP 5 | 配置身份验证执行对象。

该对象将每个身份验证配置文件与一个身份验证门户方法相关联。该方法确定第一个身份验证挑战（因素）是否透明，或是否需要用户响应。

选择您配置的 **Authentication Profile**（身份验证配置文件），然后输入 **Message**（消息），告知用户如何为第一个因素进行身份验证。该信息将显示在身份验证门户 Web 表单中。



如果将 *Authentication Method*（身份验证方法）设置为 *browser-challenge*（浏览器-质询），则身份验证门户 *Web* 表单仅在 *Kerberos SSO* 身份验证失败时才会显示。否则，第一个因素的身份验证会自动完成，用户将看不到 *Web* 表单。

### STEP 6 | 配置身份验证策略规则。

该规则必须与要保护的服务和应用程序以及必须进行身份验证的用户相匹配。

1. 选择 **Policies**（策略）> **Authentication**（身份验证），然后 **Add**（添加）规则。
2. 输入标识规则的 **Name**（名称）。
3. 选择 **Source**（源）并 **Add**（添加）特定区域和 IP 地址，或选择 **Any**（任何）区域或 IP 地址。

   该规则仅适用来自于指定 IP 地址或特定区域内接口的流量。
4. 选择 **User**（用户），然后选择或 **Add**（添加）规则所适用的源用户和用户组（默认为 **any**（任何））。
5. 选择 **Destination**（目标）并 **Add**（添加）特定区域和 IP 地址，或选择 **Any**（任何）区域或 IP 地址。

   IP 地址可以是您要控制访问权限的资源（如服务器）。
6. 选择 **Service/URL Category**（服务/URL 类别），然后选择或 **Add**（添加）规则控制访问的服务和服务组（默认为 **service-http**）。
7. 选择或 **Add**（添加）规则控制访问的 URL 类别（默认为 **any**（任何））。例如，您可以创建一个自定义 URL 类别，指定最敏感的内部站点。
8. 选择 **Actions**（操作），然后选择您创建的 **Authentication Enforcement**（身份验证执行）对象。
9. 指定 **Timeout**（超时）期限（分钟）（默认为 60 分钟），在此期间，防火墙会提示用户仅对服务和应用程序的重复访问进行一次身份验证。

   *Timeout*（超时）是更严格的安全（身份验证提示之间的时间更短）和用户体验（身份验证提示之间的时间更长）之间的权衡。访问关键系统和敏感区域（例如数据中心）时，进行更频繁的身份验证通常是很正确的选择。在网络外围设备以及对于用户体验为核心的业务，进行更少的身份验证往往是比较正确的选择。
10. 单击 **OK**（确定）保存规则。

### STEP 7 | 自定义 MFA 登录页面。

防火墙显示此页面，告诉用户如何对 MFA 因素进行身份验证，并指示身份验证状态（正在进行中、成功或失败）。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Device**（设备）> **Response Pages**（响应页面），然后选择 **MFA Login Page**（**MFA** 登录页面）。
2. 选择 **Predefined**（预先定义的）响应页面并 **Export**（导出）页面到您的客户端系统。
3. 在您的客户端系统上，使用 HTML 编辑器自定义下载的响应页面，并使用唯一文件名保存。
4. 返回到防火墙上的 MFA 登录页面对话框，**Import**（导入）您的自定义页面，**Browse**（浏览）以选择 **Import File**（导入文件），选择 **Destination**（目标）（虚拟系统或 **shared**（共享）位置），单击 **OK**（确定），然后再单击 **Close**（关闭）。

STEP 8 | 配置安全策略规则，允许用户访问需要身份验证的服务和应用程序。

1. 创建安全策略规则。
2. **Commit**（提交）更改。

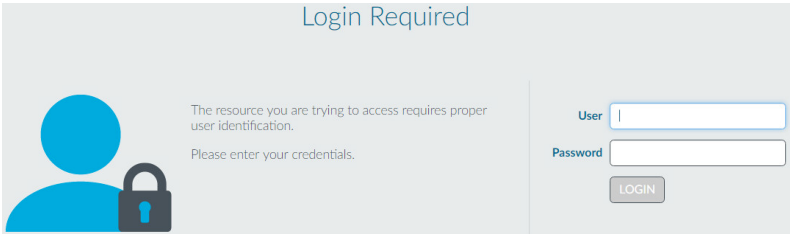


防火墙上的自动关联引擎使用多个关联对象来检测网络上可能会显示与 *MFA* 相关的凭据滥用事件。要查看事件，请选择 *Monitor*（监控）> *Automated Correlation Engine*（自动关联引擎）> *Correlated Events*（关联事件）。

STEP 9 | 验证防火墙是否执行 MFA。

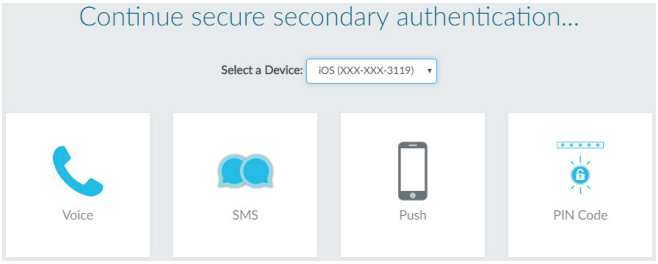
1. 作为身份验证规则中指定的源用户之一登录到您的网络。
2. 请求与规则中指定的服务或应用程序之一相匹配的服务或应用程序。

   防火墙显示第一个身份验证因素的身份验证门户 Web 表单。该页面包含您在身份验证执行对象中输入的消息。例如：




3. 输入您的用户凭据进行第一次身份验证质询。

   然后，防火墙会显示下一个身份验证因素的 MFA 登录页面。例如，MFA 服务可能会提示您选择语音、短信、推送或 PIN 码 (OTP) 身份验证方法。如果选择推送，您的手机会提示您同意身份验证。




4. 验证下一个因素。

   防火墙会显示身份验证成功或失败的消息。如果身份验证成功，防火墙会显示一个用于下一个身份验证因素的 MFA 登录页面（如有）。

   为每个 MFA 因素重复执行此步骤。对所有因素进行身份验证后，防火墙会评估安全策略以确定是否允许访问服务或应用程序。
5. 结束刚刚访问的服务或应用程序会话。
6. 为相同的服务或应用程序启动新的会话。确保在身份验证规则中配置的 **Timeout**（超时）期限内执行此步骤。

   防火墙允许访问无需重新进行身份验证。


© 2019 Palo Alto Networks, Inc.

7. 等待直到 **Timeout**（超时）期限到期，并请求相同的服务或应用程序。

   防火墙提示您重新进行身份验证。

# 在 RSA SecurID 和防火墙之间配置 MFA

多重因素身份验证允许您在允许用户访问网络资源之前使用多重因素检验其身份，从而保护公司资产。要在防火墙和“RSA SecurID 访问云身份验证服务”之间启用多重因素身份验证 (MFA)，则首先必须配置 RSA SecurID 服务，以便获得需要使用多重因素配置防火墙以检验用户身份的详细信息。在 RSA SecurID 访问控制台上执行完所需配置后，您可以配置防火墙，以便与 RSA SecurID 集成。

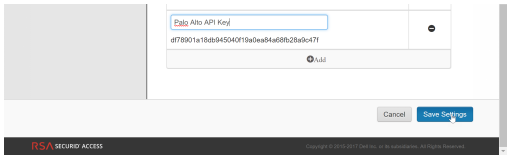
*Palo Alto Networks* 下一代防火墙与 *RSA SecurID* 访问云身份验证服务集成。与 *RSA SecurID* 的 *MFA API* 集成仅支持基于云的服务，不支持用于本地部署身份验证管理器的双重因素身份验证，前提是第二个因素使用供应商特定 *API*。此集成所需的最低内容版本是 *752* 和 *PAN-OS 8.0.2*。

- 获取 RSA SecurID 访问云身份验证服务详细信息
- 配置带 RSA SecurID 的 MFA 防火墙

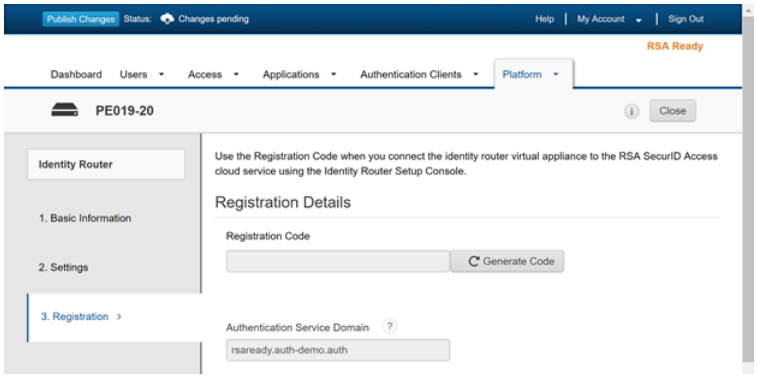
## 获取 *RSA SecurID* 访问云身份验证服务详细信息

要安全传递来往于防火墙和 RSA SecurID 访问云身份验证服务的用户身份验证请求，您首先必须转至 RSA SecurID 访问控制台配置 RSA 访问 ID、身份验证服务 URL、以及防火墙需要用于进行身份验证至服务且与服务进行交互的客户端 API 密钥。此外，防火墙还需要“访问策略 ID”，以使用 RSA Approve 或 RSA Tokencode 身份验证方法对身份源进行验证。

- 生成 **RSA SecurID API** 密钥— 登录至 RSA SecurID 访问控制台，并选择 **My Account**（我的帐户）> **Company Settings**（公司设置）> **Authentication API Keys**（身份验证 **API** 密钥）。**Add**（添加）新密钥，然后 **Save Settings**（保存设置），并 **Publish Changes**（发布更改）。



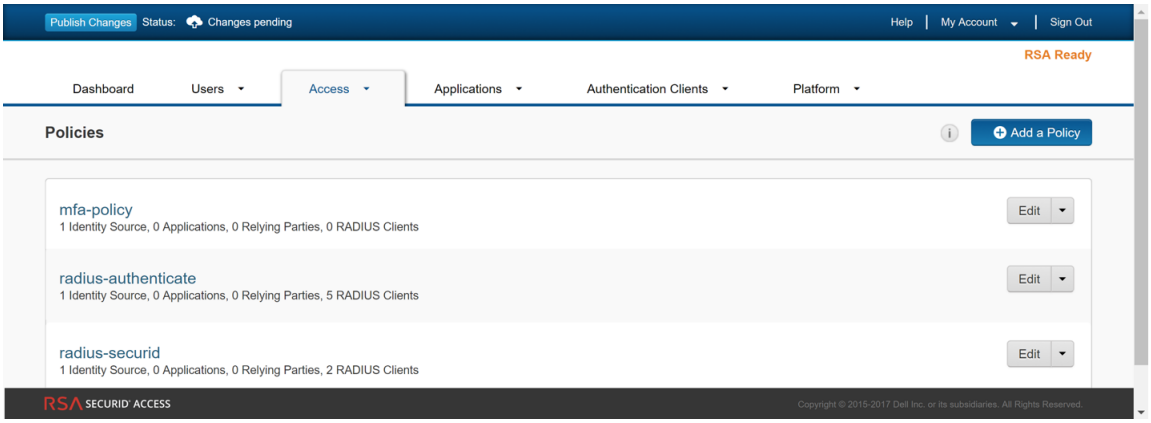

- 获取防火墙必须与其连接的 **RSA SecurID** 访问端点 **API**（身份验证服务域）— 选择 **Platform**（平台）> **Identity Routers**（身份路由器），选择要 **Edit**（编辑）的“身份路由器”，并记下 **Authentication Service Domain**（身份验证服务域）。在本例中，域为 https://rsaready.auth-demo.auth。






© 2019 Palo Alto Networks, Inc.

- 获取访问策略 **ID**— 选择 **Access**（访问）> **Policies**（策略），记下允许防火墙充当 RSA SecurID 服务的身份验证客户端的访问策略名称。策略必须配置为仅使用 RSA Approve 或 RSA Tokencode 身份验证方法。




## 配置带 *RSA SecurID* 的 *MFA* 防火墙

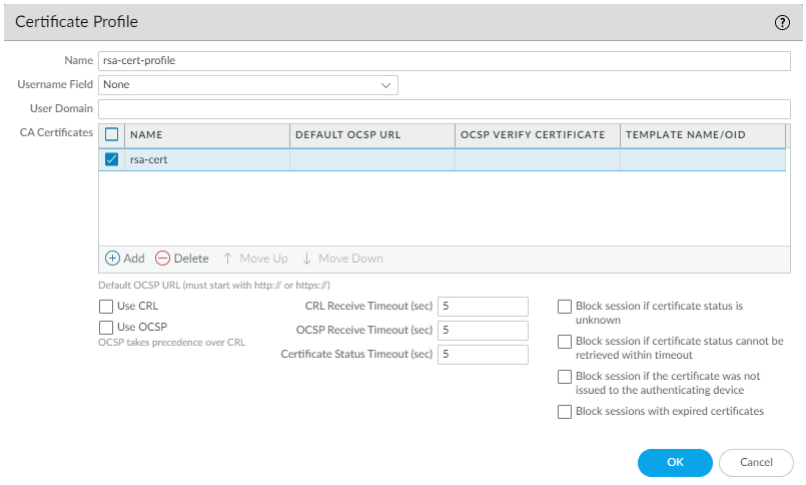
在获取 RSA SecurID 访问云身份验证服务详细信息后，可以将防火墙配置为在调用 MFA 时提示用户提供 RSA SecurID 令牌。

STEP 1 | 防火墙配置为信任 RSA SecurID 访问端点 API 提供的 SSL 证书。

1. 从 RSA SecurID 访问端点导出 SSL 证书，并将其导入防火墙。

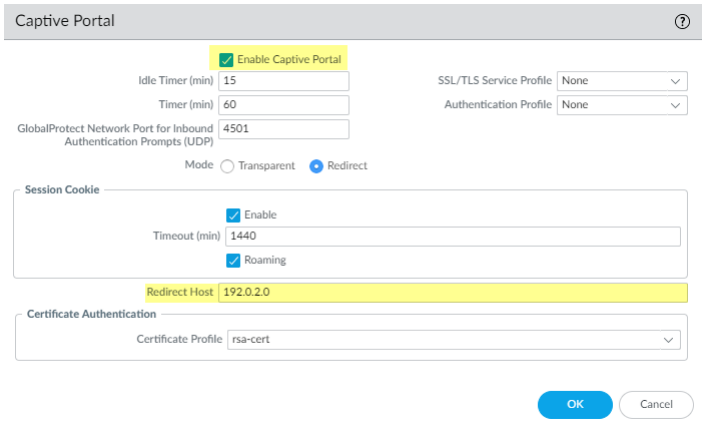
   要启用防火墙和 RSA SecurID 访问端点 API 之间的信任，必须导入自签名证书，或是证书签名时所使用的 CA 证书。

2. 配置证书配置文件（**Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后单击 **Add**（添加））。



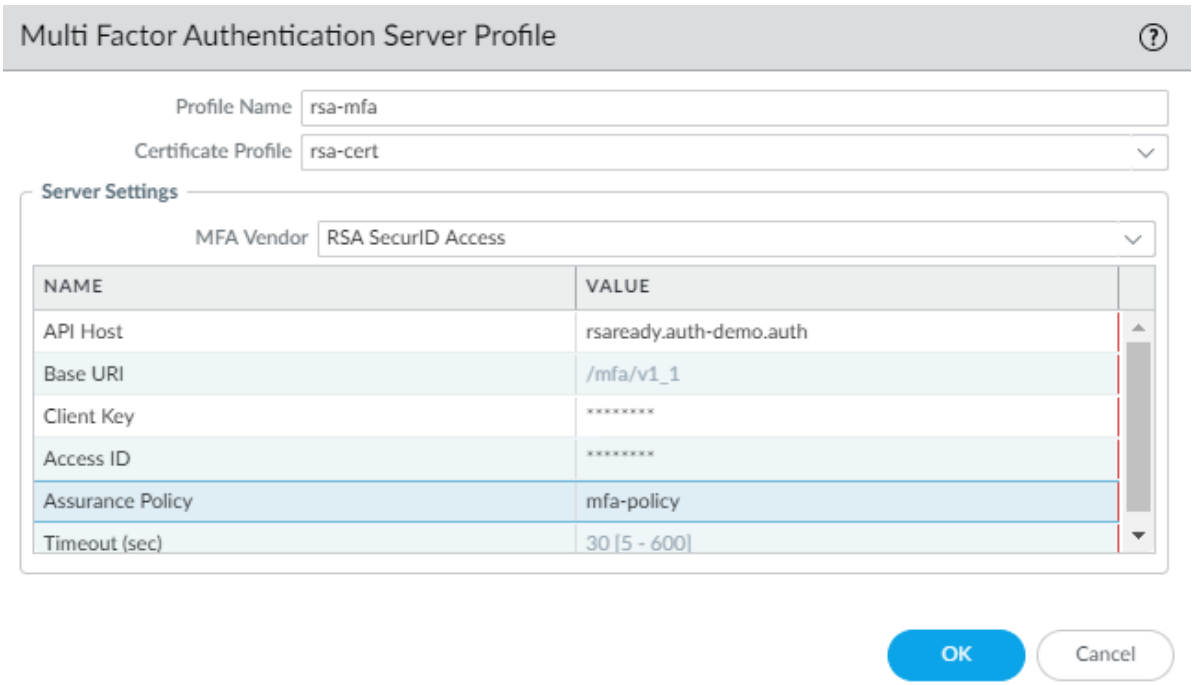

STEP 2 | 在 重定向模式下配置身份验证门户（**Device**（设备）> **User Identification**（用户标识）> **Authentication Portal Settings**（身份验证门户设置）），以显示用于验证 RSA SecurID 的 Web 表单。必须指定“重定向主机”为 IP 地址或是解析到第 3 层接口（防火墙重定向 Web 请求的目标接口）IP 地址的主机名（即名称中没有点的主机名）。


© 2019 Palo Alto Networks, Inc.




STEP 3 | 配置多重因素身份验证服务器配置文件以指定防火墙必须连接至 RSA SecurID 云服务的方式（**Device**（设备）> **Server Profiles**（服务器配置文件）> **Multi Factor Authentication**（多重因素身份验证），并单击 **Add**（添加））。

1. 输入标识 MFA 服务器配置文件的 **Name**（名称）。
2. 选择先前创建的 **Certificate Profile**（证书配置文件），此示例中为 rsa-cert-profile。防火墙将在与 RSA SecurID 云服务建立安全连接时使用此证书。
3. 在 **MFA Vendor**（**MFA** 供应商）下拉列表中，选择 **RSA SecurID Access**（**RSA SecurID** 访问）。
4. 为您在获取 RSA SecurID 访问云身份验证服务详细信息中记下的每个属性配置**Value**（值）：
   - **API Host**（**API** 主机）— 输入必须与防火墙连接的 RSA SecurID 访问 API 端点的主机名或 IP 地址，在此示例中为 rsaready.auth-demo.auth。
   - **Base URI**（基本 **URI**）— 不得修改默认值 (/mfa/v1_1)
   - **Client Key**（客户端密钥）— 输入 RSA SecurID 客户端密钥。
   - **Access ID**（访问 **Id**）— 输入 RSA SecurID 访问 ID。
   - **Assurance Policy**（保障策略）— 输入 RSA SecurID 访问策略名，在此示例中为 mfa-policy 。
   - **Timeout**（超时）— 默认超时为 30 秒。





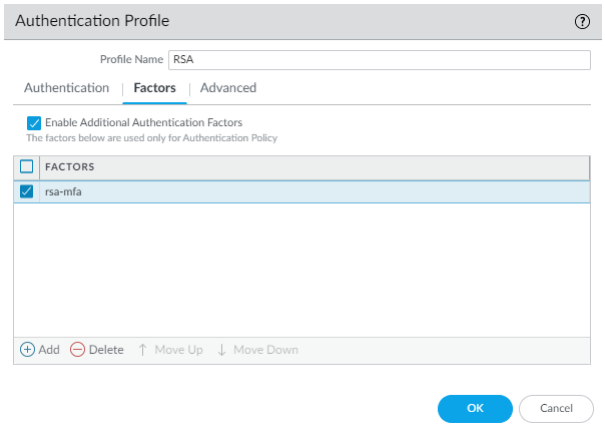

© 2019 Palo Alto Networks, Inc.

5. 保存配置文件。

STEP 4 | 配置身份验证配置文件（**Device**（设备）> **Authentication Profile**（身份验证配置文件），并单击 **Add**（添加））。

该配置文件定义了用户必须响应的身份验证因素的顺序。

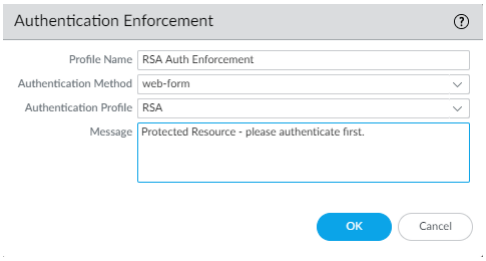
1. 选择第一个身份验证因素的 **Type**（类型），并选择相应的 **Server Profile**（服务器配置文件）。
2. 选择 **Factors**（因素），**Enable Additional Authentication Factors**（启用其他身份验证因素），并 **Add**（添加）您在此示例中先前创建的 rsa-mfa 配置文件。




3. 单击 **OK**（确定）保存身份验证配置文件。

STEP 5 | 配置身份验证执行对象。（**Objects**（对象）> **Authentication**（身份验证），然后单击 **Add**（添加））。

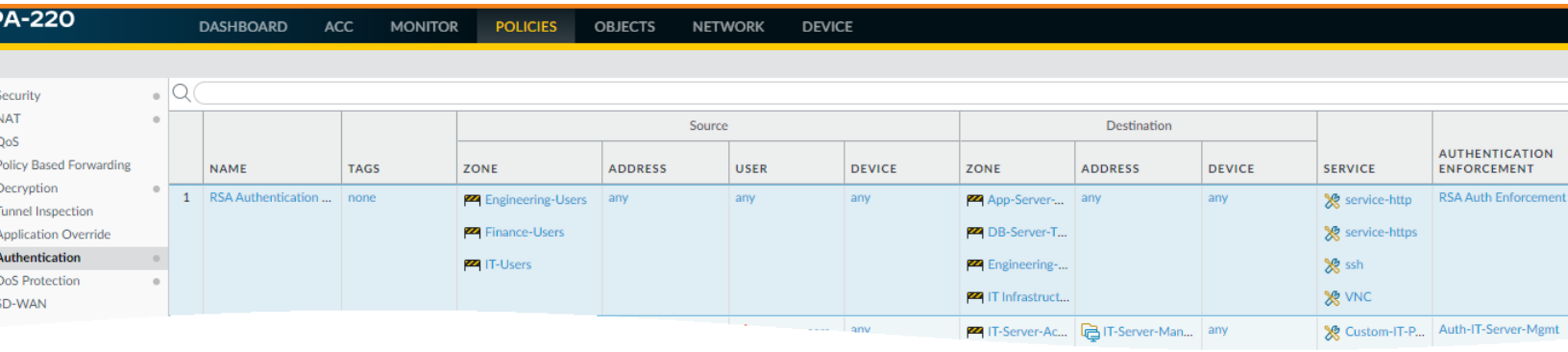
必须选择在此示例中刚定义的名为 RSA 的身份验证配置文件。




STEP 6 | 配置身份验证策略规则。（**Policies**（策略）> **Authentication**（身份验证），然后单击 **Add**（添加））

您的身份验证策略规则必须匹配想要保护的服务和应用程序，指定必须进行身份验证的用户，并包含触发身份验证配置文件的身份验证实施对象。在此示例中，RSA SecurID 使用名为 RSA 身份验证实施的身份验证实施对象一起对访问 HTTP、HTTPS、 SSH 和 VNC 通信的所有用户进行身份验证（在 **Actions**（操作）中，选择 **Authentication Enforcement**（身份验证实施）对象）。

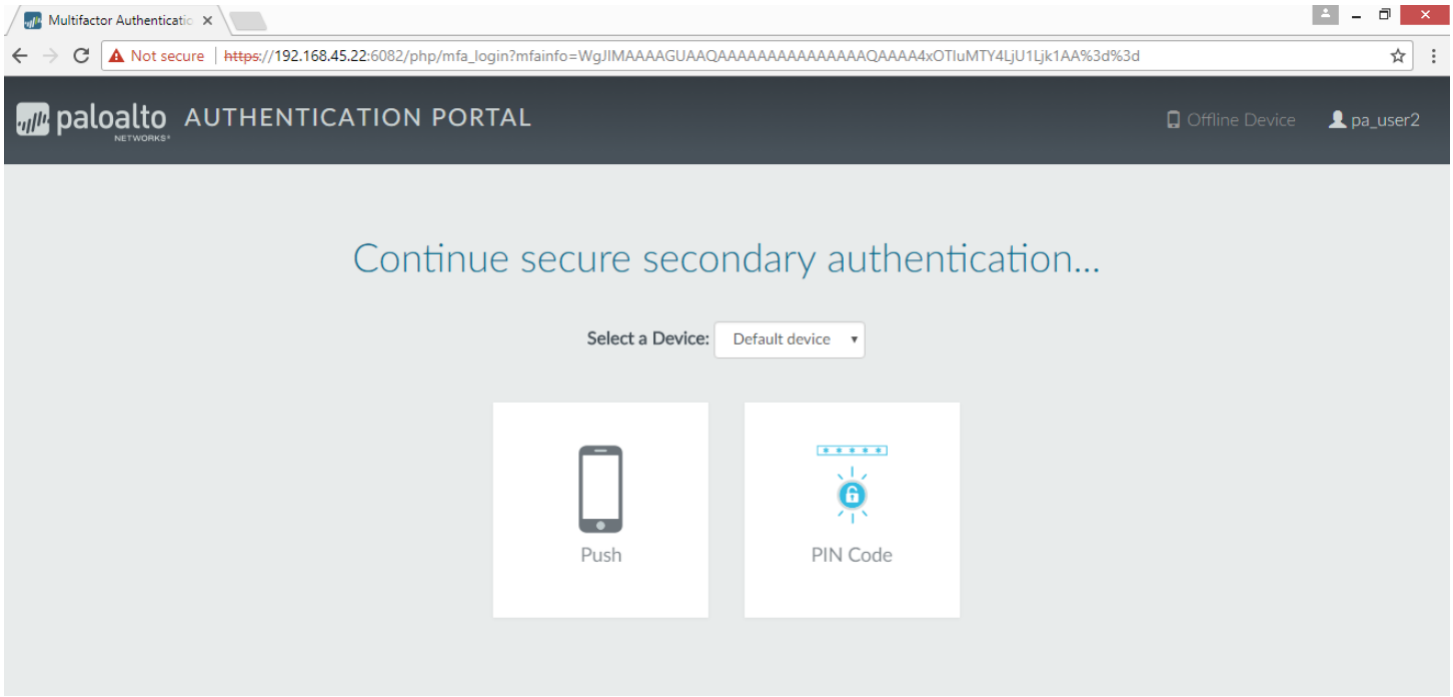

© 2019 Palo Alto Networks, Inc.




STEP 7 | 在防火墙上 **Commit**（提交）更改。

STEP 8 | 检验 RSA SecurID 是否正使用您启用的推送或 PIN 码身份验证方法保护您网络上用户的安全。

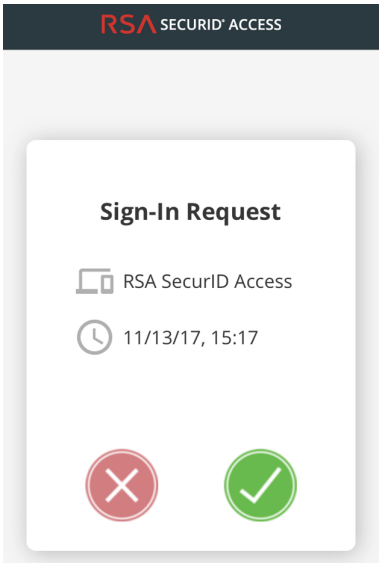
1. 推送身份验证
    1. 要求网络上的用户启动 Web 浏览器访问网络。应显示您早期定义的用于重定向主机的带 IP 地址或主机名的身份验证门户页面。
    2. 验证用户是否输入第一个身份验证因素的凭据，并继续输入第二个身份验证因素的凭据，然后选中 **Push**（推送）。




3. 检查用户移动设备上 RSA SecurID 访问应用程序中的 **Sign-In request**（签入请求）。
4. 要求用户 **Accept**（接受）移动设备上的“签入请求”，并等待数秒，以便防火墙接收身份验证成功的通知。用户应能够访问所请求的网站。

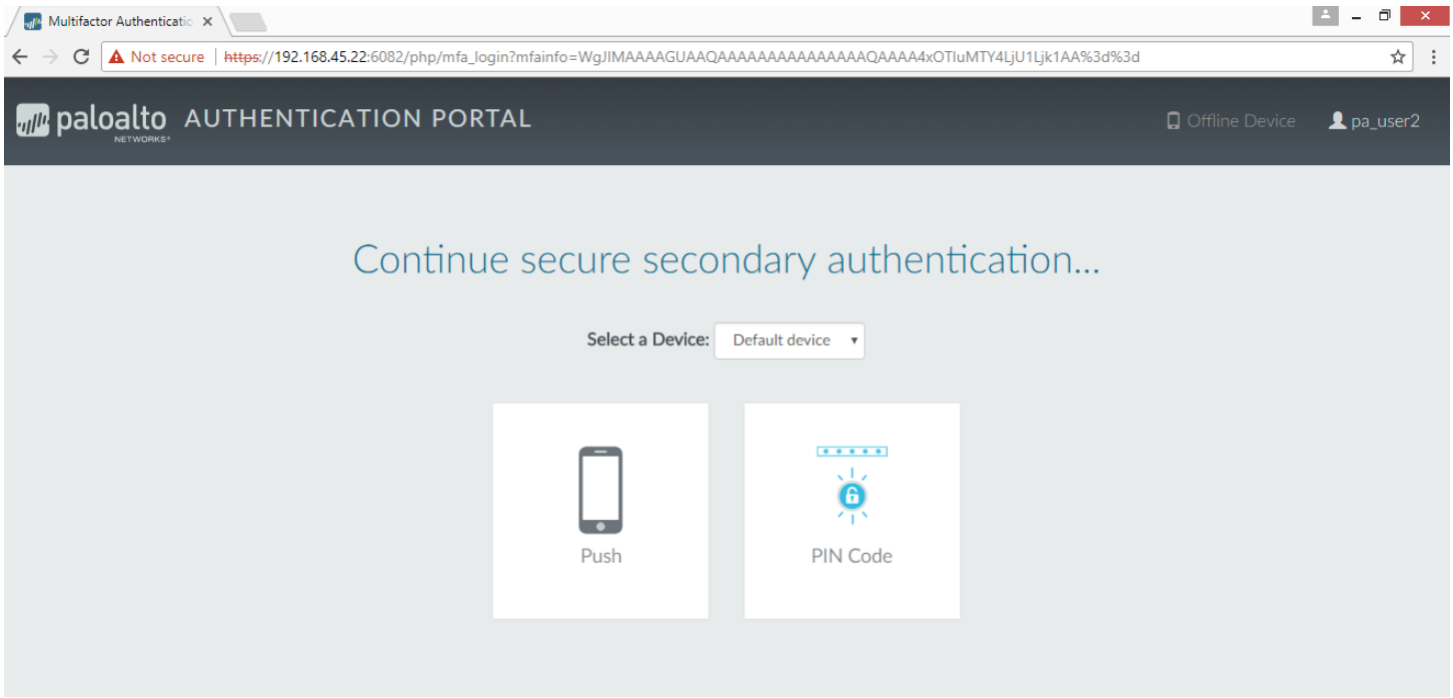


© 2019 Palo Alto Networks, Inc.



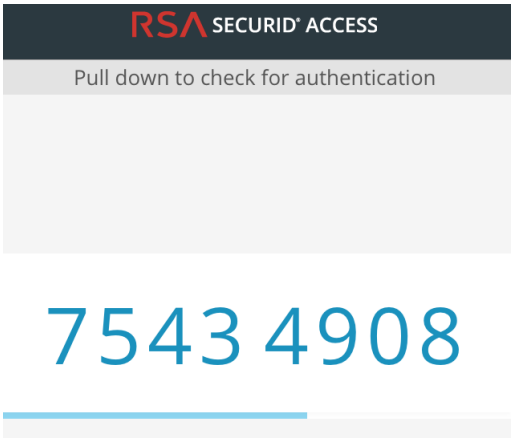

要测试失败的身份验证，请 *Decline*（拒绝）移动设备上的签入请求。

2. **PIN 码身份验证**
   1. 要求网络上的用户启动 Web 浏览器访问网络。应显示您早期定义的用于重定向主机的带 IP 地址或主机名的身份验证门户页面。
   2. 验证用户是否输入第一个身份验证因素的凭据，并继续输入第二个身份验证因素的凭据，然后选中 **PIN Code**（**PIN 码**）。




3. 检查用户移动设备上 RSA SecurID 访问应用程序中是否显示 **PIN Code**（**PIN 码**）。


© 2019 Palo Alto Networks, Inc.




4. 要求用户在 Web 浏览器提示 **Enter the PIN...**（输入 **PIN...**）中复制 PIN 码，然后单击 **Submit**（提交）。等待数秒，以便防火墙接收身份验证成功的通知。用户应能够访问所请求的网站。

# 在 Okta 和防火墙之间配置 MFA

多重因素身份验证允许您在允许用户访问网络资源之前使用多重因素检验其身份，从而保护公司资产。

要启用防火墙和 Okta 身份管理服务之间的多重因素身份验证：

- 配置 Okta
- 配置防火墙以便与 Okta 进行集成
- 采用 Okta 对 MFA 进行验证

## 配置 *Okta*

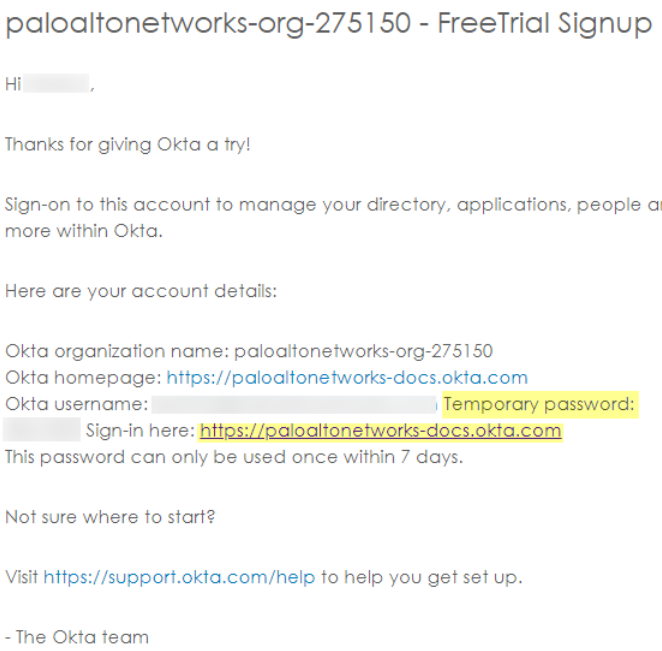
登录 Okta 管理门户以创建用户账户、定义 Okta MFA 策略，并获取在防火墙上使用 Okta 配置 MFA 所需的令牌信息。

STEP 1 | 创建 Okta 管理用户帐户。

1. 提交电子邮件地址和姓名，然后单击 **Get Started**（开始）。
2. 单击确认电子邮件内的链接，使用包含的临时密码登录到 Okta 管理门户。



© 2019 Palo Alto Networks, Inc.


paloaltonetworks-org-275150 - FreeTrial Signup

Hi ,

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: paloaltonetworks-org-275150
Okta homepage: https://paloaltonetworks-docs.okta.com
Okta username: Temporary password:
Sign-in here: https://paloaltonetworks-docs.okta.com
This password can only be used once within 7 days.

Not sure where to start?

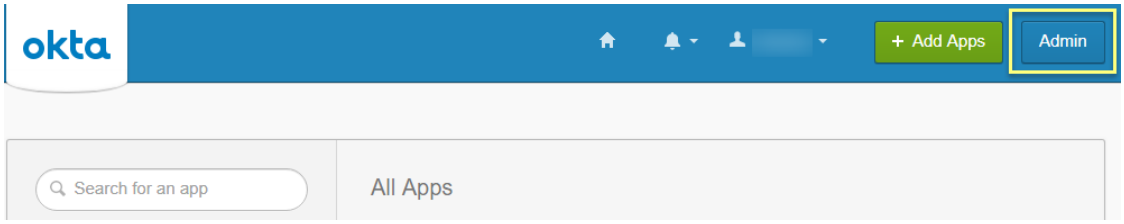
Visit https://support.okta.com/help to help you get set up.

- The Okta team

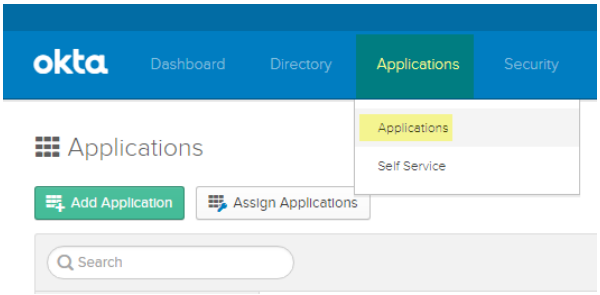
3. 创建一个至少包含 8 个字符（必须包含 1 个小写字母、1 个大写字母、1 个数字）的新密码，请勿包含用户名的任何部分。
4. 选择密码提醒问题，并输入答案。
5. 选择安全图像，然后 **Create My Account**（创建我的账户）。

STEP 2 | 配置您的 Okta 服务。

如果登陆后未被重定向到 *Okta* 管理门户，则选择右上角的 *Admin*（管理）。

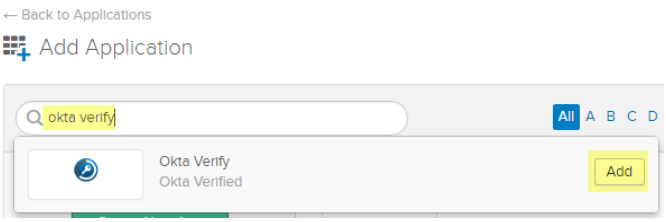



1. 在 Okta 仪表板，使用您的 Okta 管理凭据登录，然后选择 **Applications**（应用程序）> **Applications**（应用程序）。



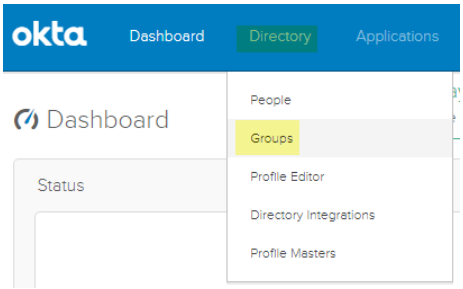

2. 选择 **Add Application**（添加应用程序）。
3. 搜索 **`Okta Verify`**。
4. 选择 **Add**（添加），然后 **Done**（完成）。


© 2019 Palo Alto Networks, Inc.

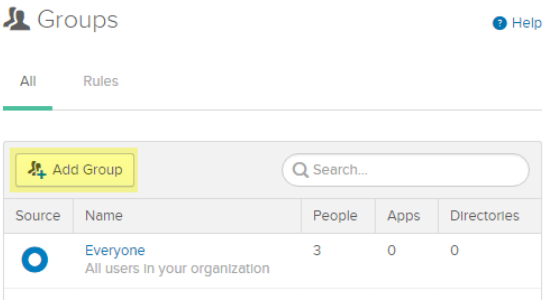



STEP 3 | 创建一个或多个用户组对您的用户进行分类（例如，按设备，按策略，或按部门），并分配 Okta 验证应用程序。

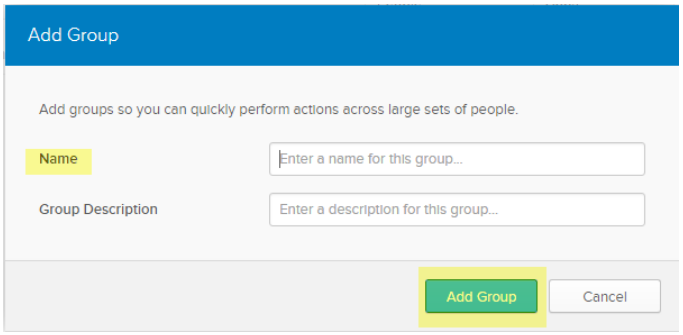
1. 选择 **Directory**（目录）> **Groups**（组）。




2. 单击 **Add Group**（添加组）。




3. 输入组 **Name**（名称）和 **Group Description**（组描述）（可选），然后 **Add Group**（添加组）。

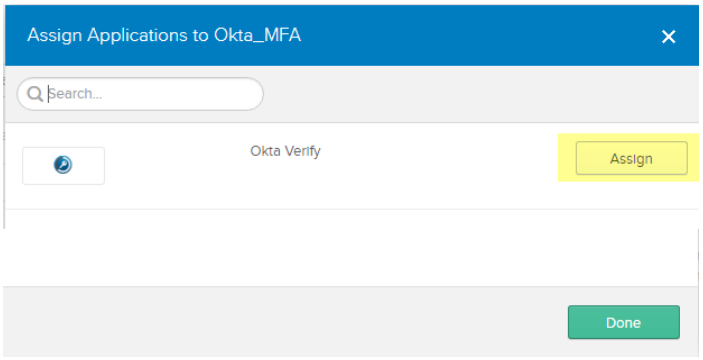



默认组 ***Everyone*** 包含在配置 Okta 第一步时为组织配置的所有用户。

4. 选择刚创建的组，然后选择 **Manage Apps**（管理应用程序）。
5. **Assign**（分配）您在第二步添加的 Okta 验证应用程序。



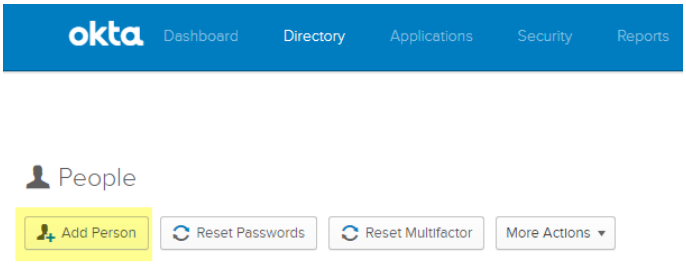
© 2019 Palo Alto Networks, Inc.



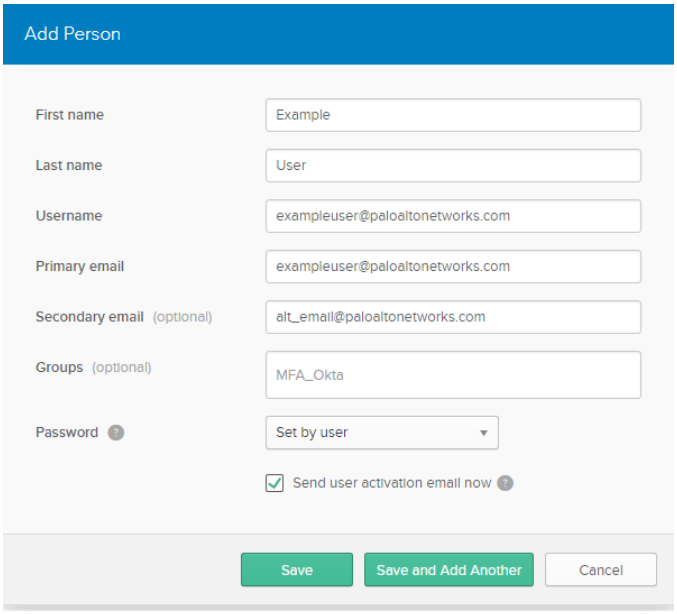

6. 应用程序 **Assigned**（分配）结束后，单击 **Done**（完成）。
7. 对于所有将为 MFA 使用 Okta 验证应用程序的组，请重复此过程。

STEP 4 | 添加用户，并将其分配给一个组。

1. 在 Okta 仪表板上选择 **Directory**（目录）> **People**（人员）> **Add Person**（添加人员）。




2. 输入用户的 **First Name**（名字）、**Last Name**（姓氏）和 **Username**（用户名）。用户名必须与自动填充的 **Primary email**（主要电子邮件）和防火墙上输入的用户名匹配。您可以为用户输入一个备用电子邮件地址作为 **Secondary Email**（次要电子邮件）。




3. 输入与此用户关联的一组或多 **Groups**（组）名称。开始输入时，组名可自动填充。
4. 选中 **Send user activation email now**（现在发送用户激活电子邮件），然后 **Save**（保存）以添加单个用户，或是 **Save and Add Another**（保存并添加另一个）以持续添加用户。

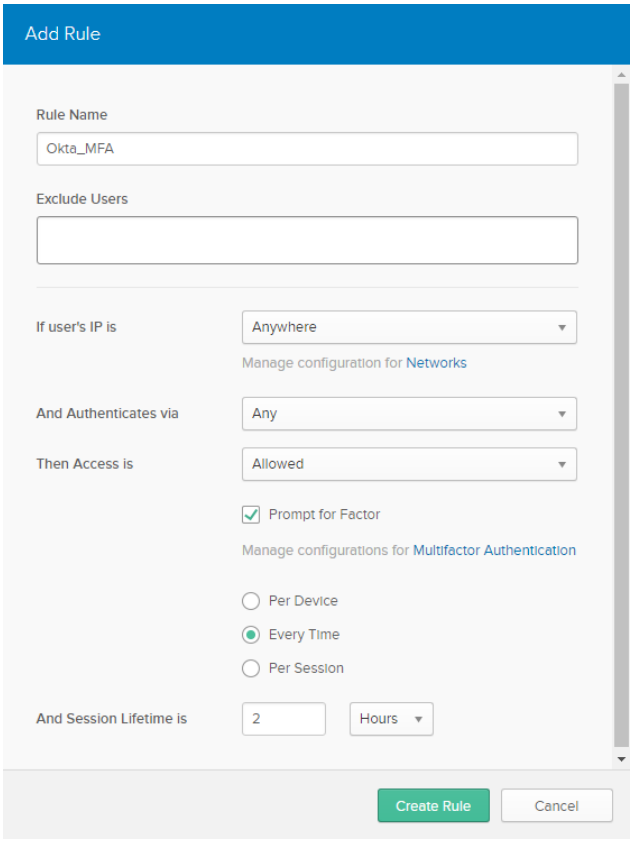
STEP 5 | 向用户分配测试策略。

1. 选择 **Security**（安全）> **Authentication**（身份验证）> **Sign On**（登录）。


© 2019 Palo Alto Networks, Inc.

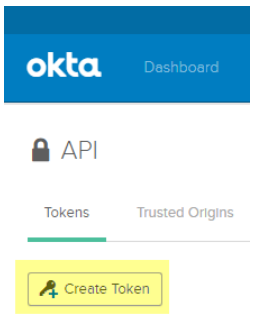
此处会出现一个带 **Default Rule**（默认规则）的 **Default Policy**（默认策略），不会提示用户使用 MFA 进行登录。

2. 输入 **Rule Name**（规则名称）并选中 **Prompt for Factor**（因素提示）以执行 MFA 提示，然后选择提示类型（**Per Device**（每设备）、**Every Time**（每次）或 **Per Session**（每个会话）），最后 **Create Rule**（创建规则）。




STEP 6 | 因为 Okta 身份验证令牌信息仅显示一次，请将其记录在安全的地方。

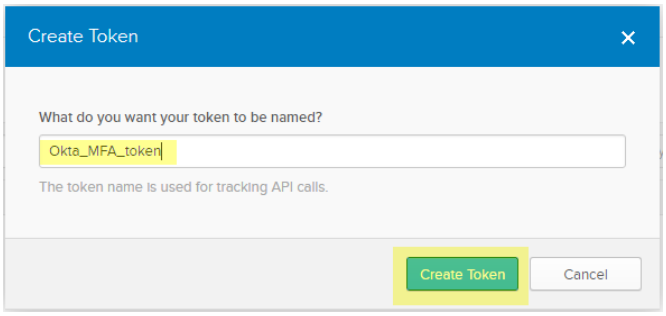
1. 选择**Security**（安全）> **API** > **Tokens**（令牌）。
2. 选择 **Create Token**（创建令牌）。



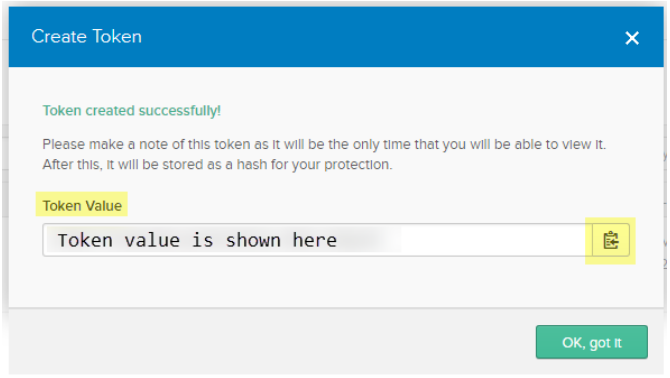

3. 输入令牌名，然后 **Create Token**（创建令牌）。



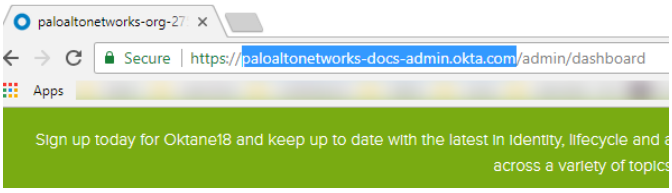
© 2019 Palo Alto Networks, Inc.



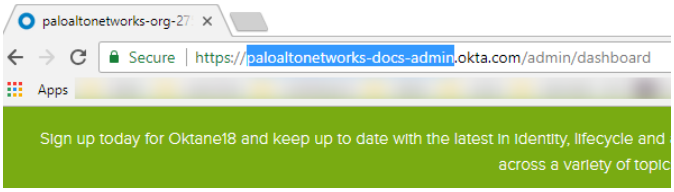

4. 复制 **Token Value**（令牌值）。
   可以单击 **Copy to clipboard**（复制到剪贴板）按钮以将令牌值复制到您的剪贴板。




5. 在用于 Okta 管理仪表板的 URL 中，复制 URL 中 **`https://`** 之后到 **`/admin`** 的部分，用作 **API host**（**API** 主机）。




6. 省略此 URL 中用作 **Organization**（组织）的 **`okta.com`** 域。




   例如，在上述 Okta 管理仪表板示例中，**`https://paloaltonetworks-doc-admin.okta.com/admin/dashboard`**：

   - API 主机名为 **`paloaltonetworks-doc-admin.okta.com`**。
   - 组织为 **`paloaltonetworks-doc-admin`**。

STEP 7 | 使用 Base-64 编码导出证书链中的所有证书：

1. 根据您的浏览器，使用以下方法之一导出证书链中的所有证书。
   - **Chrome** — 按下 **`F12`**，然后选择 **Security**（安全）> **View Certificate**（查看证书）> **Details**（详细信息）> **Copy to File**（复制到文件）。
   - **Firefox** — 选择 **Options**（选项）> **Privacy & Security**（隐私和安全）> **View Certificates**（查看证书）> **Export**（导出）。


© 2019 Palo Alto Networks, Inc.

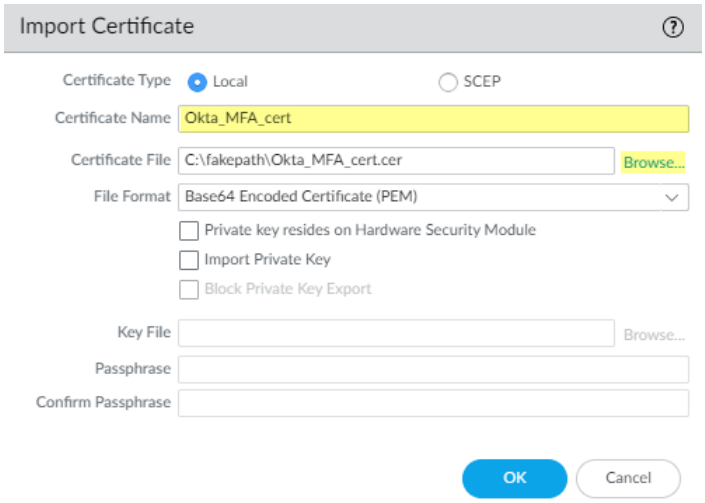
- **Internet Explorer** — 选择 **Settings**（设置）> **Internet Options**（互联网选项）> **Content**（内容）> **Certificates**（证书）> **Export**（导出）。

2. 使用证书导出向导导出证书链中的所有证书，然后选择格式 **Base-64 encoded X.509**。

## 配置防火墙以便与 *Okta* 进行集成

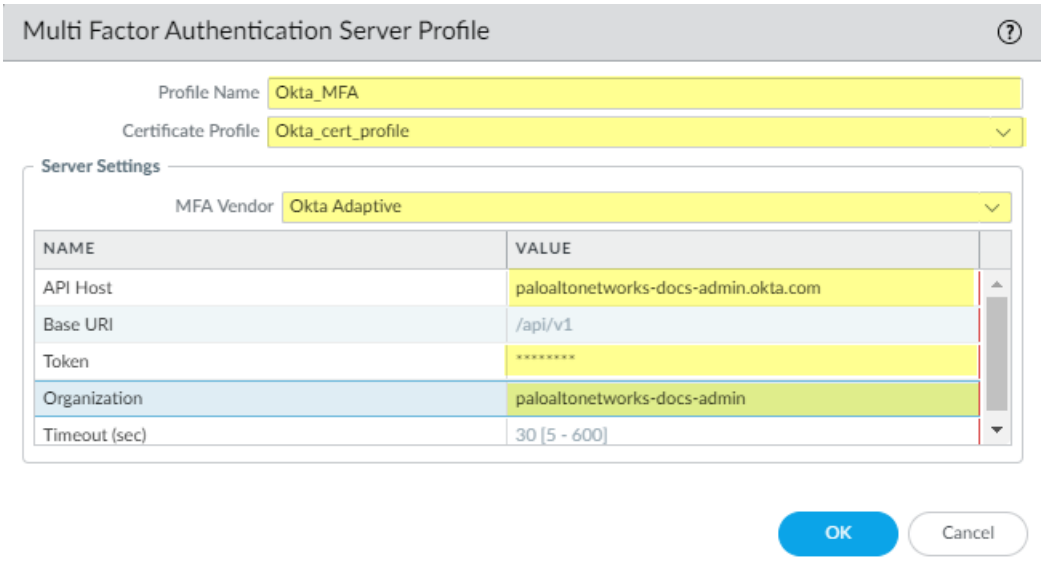
作为先决条件，您必须使用 Okta 对想要进行身份验证的所有用户进行映射。

STEP 1 | 导入防火墙上证书链中的所有证书，并将导入的 CA 证书（根证书和中间证书）添加到 Certificate Profile（证书配置文件）。




STEP 2 | 添加用于 Okta 的 **Multi Factor Authentication Server Profile**（多重因素身份验证服务器配置文件）。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Multi Factor Authentication**（多重因素身份验证）。
2. **Add**（添加）MFA 服务器配置文件。




3. 输入 **Profile Name**（配置文件名称）。
4. 选择您在配置防火墙以便与 Okta 进行集成 中第一步创建的 **Certificate Profile**（证书配置文件）。
5. 选择 **Okta Adaptive** 作为 **MFA Vendor**（MFA 供应商）。

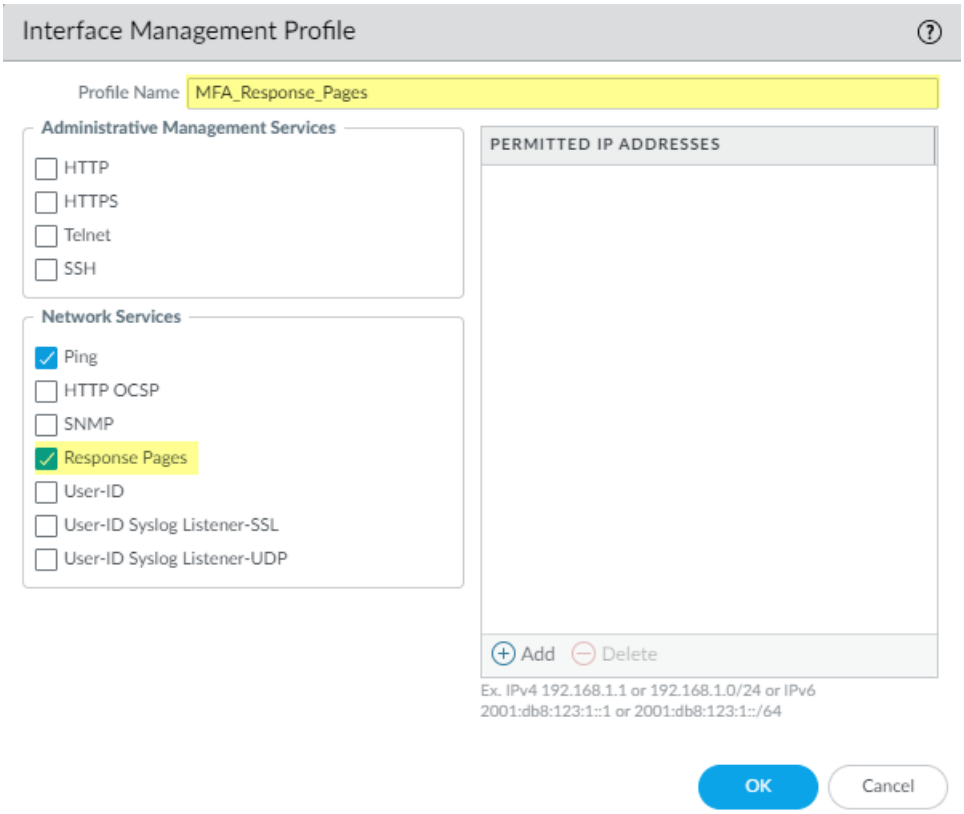


© 2019 Palo Alto Networks, Inc.

6. 输入在配置防火墙以便与 Okta 进行集成的第四步中的 **API Host**（**API** 主机）、**Token**（令牌）和 **Organization**（组织）。

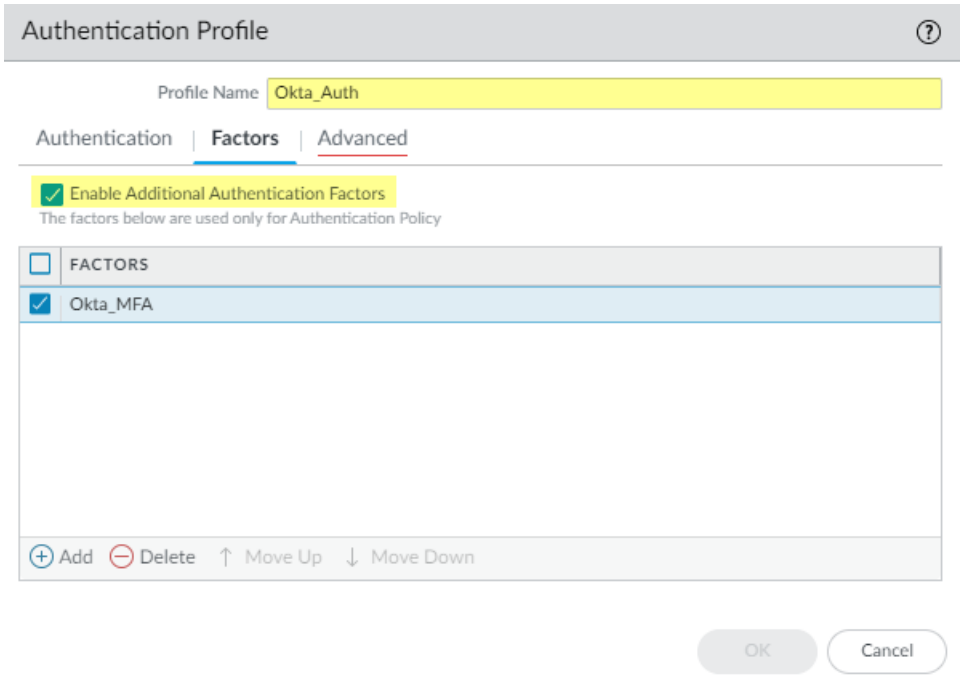
STEP 3 | 使用 **Redirect Mode**（重定向模式）配置身份验证门户，以将用户重定向到 MFA 供应商质询。

STEP 4 | 启用接口管理配置文件 上的响应页面，以将用户重定向到响应页面质询。




STEP 5 | 创建身份验证配置文件，并添加 MFA 供应商作为 **Factor**（因素）（请参阅第三步的配置多重因素身份验证。）


© 2019 Palo Alto Networks, Inc.




STEP 6 | 在源区域，Enable User-ID（启用 User-ID），要求标识用户使用您的 MFA 供应商对质询做出响应。

STEP 7 | 创建身份验证实施对象以使用 MFA 供应商，并创建身份验证策略规则（请参阅第四步和第五步中的配置身份验证策略）。

STEP 8 | **Commit**（提交）更改。

### 采用 *Okta* 对 *MFA* 进行验证

STEP 1 | 验证您的用户是否接收到其注册电子邮件，是否已激活其账户，是否已在其设备上下载 Okta 验证应用程序。

STEP 2 | 前往将提示响应页面质询的网站。

如果正在使用自签名证书（而非组织的 *PKI* 签名证书），则会出现一条安全警告，用户必须单击此警告才能访问质询。

STEP 3 | 使用您的 Okta 凭据登录响应页面。

STEP 4 | 确认设备是否接收到质询推送通知。

STEP 5 | 确认用户是否在通过接收其设备上推送通知的方式对质询进行身份验证后，能够成功访问此页面。

## 在 Duo 和防火墙之间配置 MFA

多重因素身份验证 (MFA) 允许您在允许用户访问网络资源之前使用多重因素检验其身份，从而保护公司资产。可通过多种方法将 Duo 身份管理服务用于对防火墙进行身份验证：



© 2019 Palo Alto Networks, Inc.

- 使用 GlobalProtect 网关和 RADIUS 服务配置文件对 VPN 登录进行双重因素身份验（受 PAN-OS 7.0 及更高版本支持）。
- 使用身份验证门户和 MFA 服务器配置文件进行基于 API 的集成（无须 Duo 身份验证代理或 SAML IdP — 受 PAN-OS 8.0 及更高版本支持）。
- 本地部署服务器的 SAML 集成（受 PAN-OS 8.0 及更高版本支持）。

要在防火墙和 Duo 之间启用 SAML MFA，以确保对防火墙的管理访问：

- 采用 Duo 访问网关为 SAML MFA 配置 Duo
- 配置防火墙以便与 Duo 进行集成
- 采用 Duo 对 MFA 进行验证

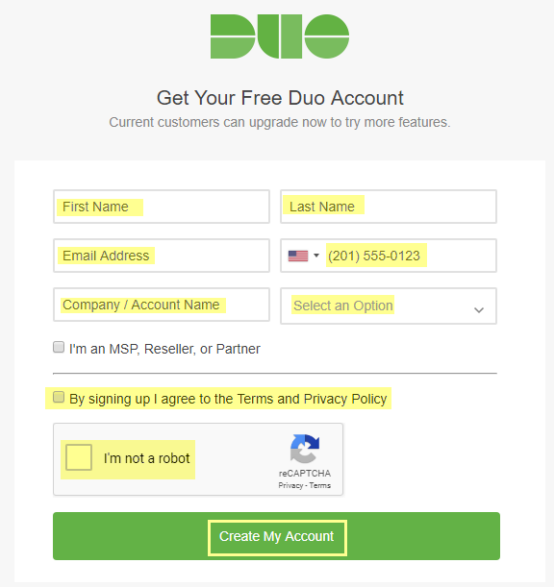
## 采用 *Duo* 访问网关为 *SAML MFA* 配置 *Duo*

开始之前，请检验您是否已在 DMZ 区域的本地部署服务器上成功部署 DuoAccessGateway (DAG)。

创建 Duo 管理员账户，并配置 Duo 访问网关，以便在用户访问资源前对其进行身份验证。

STEP 1 | 创建 Duo 管理员帐户。

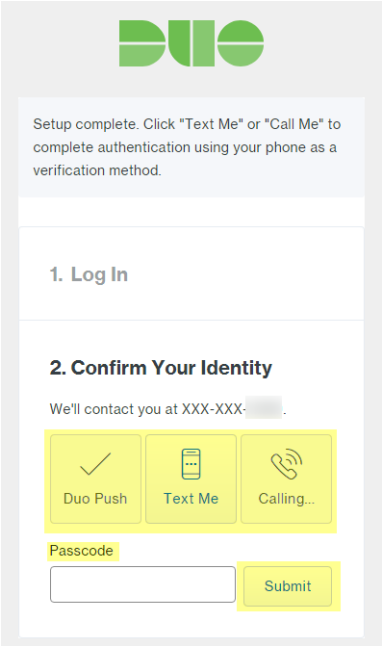
1. 在 Duo 账户创建页面上，输入您的 **First Name**（名字）、**Last Name**（姓氏）、**Email Address**（电子邮件地址）、**Cell Phone Number**（手机号码）、**Company / Account Name**）（公司/账号名称），并选择组织内员工人数。
2. 同意条款和隐私政策，并回复 reCAPTCHA 质询以 **Create My Account**（创建我的账户）。




STEP 2 | 验证 Duo 管理员帐户。

1. 选择身份验证检验方法（**Duo Push**（**Duo** 推送）、**Text Me**（发短信）或 **Calling...**（呼叫））。
2. 输入您接收到的 **Passcode**（密码），并 **Submit**（提交）密码以验证您的账户。

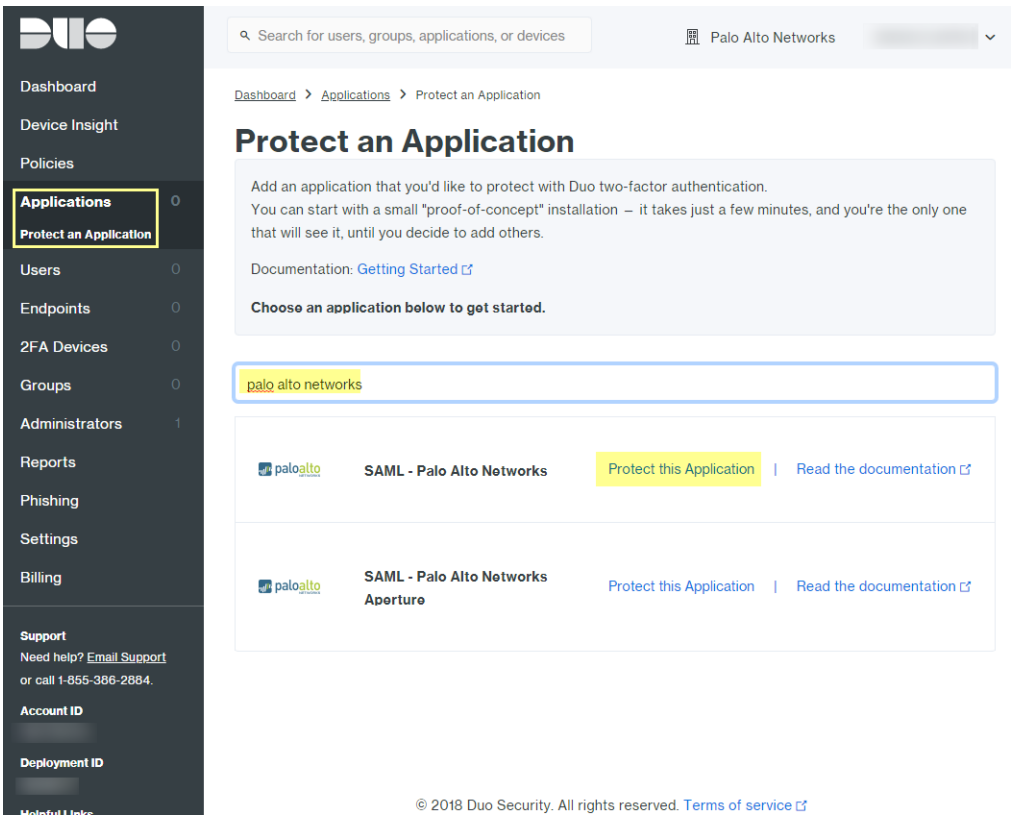

© 2019 Palo Alto Networks, Inc.




STEP 3 | 为 SAML 配置您的 Duo 服务。

配置创建成功后，请下载页面顶部的配置文件。

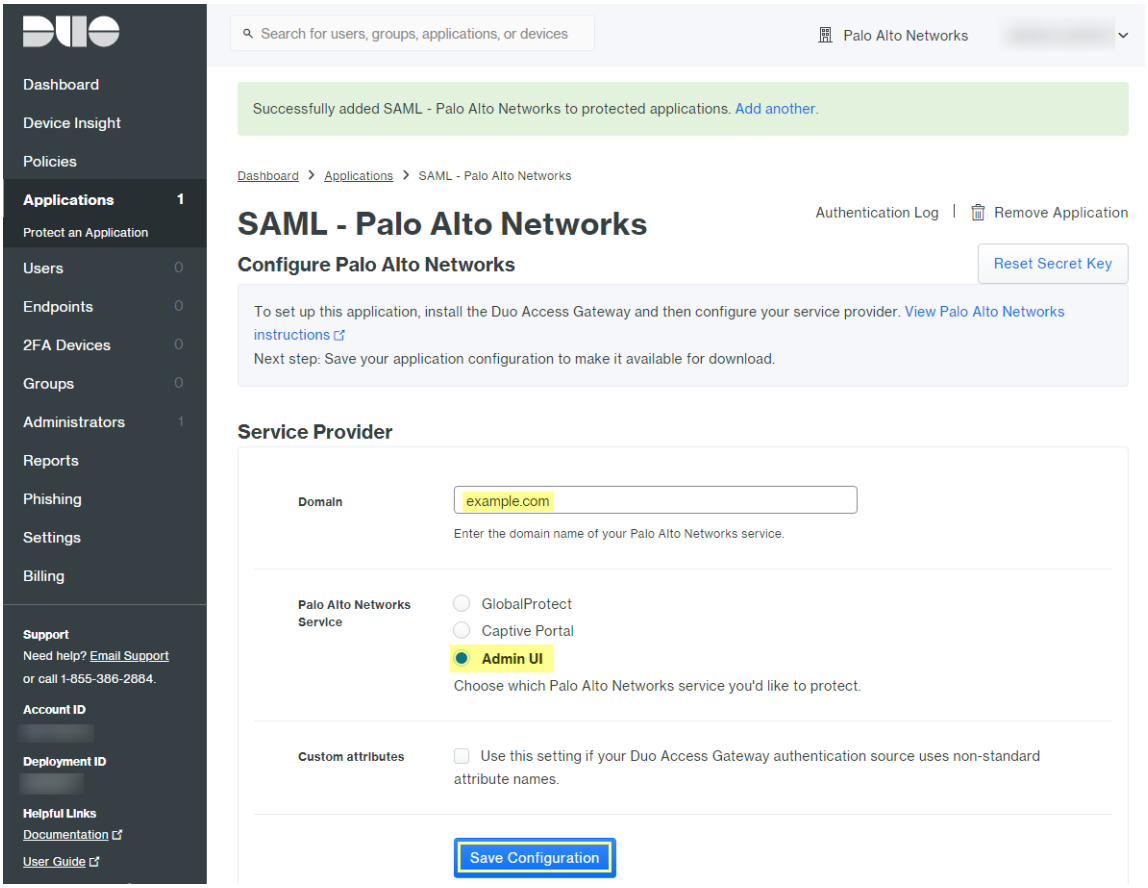
1. 在 Duo 管理面板上，选择 **Applications**（应用程序）> **Protect an Application**（保护应用程序）。
2. 输入 **`Palo Alto Networks`** 以搜索应用程序。
3. 在结果列表中找到 **SAML - Palo Alto Networks** ，然后 **Protect this Application**（保护此应用程序）。





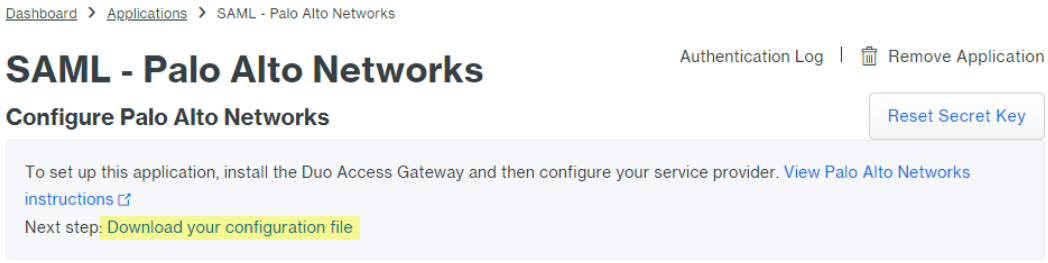

© 2019 Palo Alto Networks, Inc.

4. 输入 **Domain**（域）。
5. 选择 **Admin Ui**（管理 **UI**）作为 **Palo Alto Networks Service**。
6. 配置您的 **Policy**（策略）和其他 **Settings**（设置），并 **Save Configuration**（保存配置）。




7. **Download your configuration file**（下载您的配置文件）。

   下载文件的链接位于页面顶部。




STEP 4 | 上传配置文件到 Duo 访问网关 (DAG)。

1. 在 DAG 管理控制台中选择 **Applications**（应用程序）。
2. 单击 **Choose File**（选择文件），选择已下载的配置文件，然后 **Upload**（上传）。
3. 在 **Settings**（设置）> **Session Management**（会话管理）中，禁用 **User agent binding**（用户代理绑定），然后 **Save Settings**（保存设置）。

STEP 5 | 在 Duo 管理控制台中，配置您的 Active Directory 或 OpenLDAP 服务器作为身份验证源，并下载元数据文件。

1. 登录到 Duo 管理控制台。


© 2019 Palo Alto Networks, Inc.

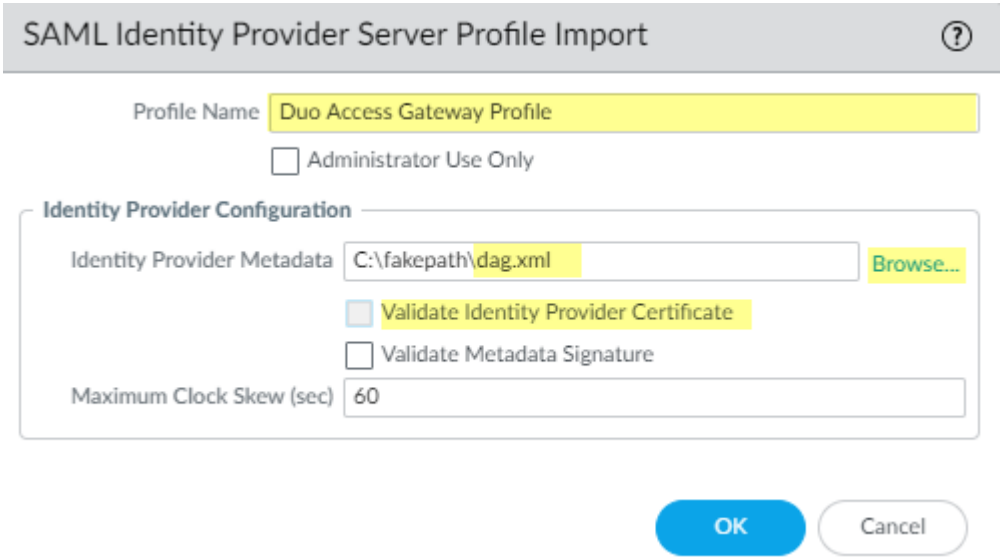
2. 在 **Authentication Source**（身份验证源）> **Set Active Source**（设置活动源）中，选择您的 **Source type**（源类型）（Active Directory 或 OpenLDAP），然后 **Set Active Source**（设置活动源）。
3. 在 **Configure Sources**（配置源）中输入 **Attributes**（属性）。
   - 对于 Active Directory，请输入 **`mail,sAMAccountName,userPrincipalName,objectGUID`**。
   - 对于 OpenLDAP，请输入 **`mail,uid`**。
   - 对于任何自定义属性，将其附加到列表的末尾，并用逗号将每个属性隔开。请勿删除任何现有属性。
4. **Save Settings**（保存设置）以保存配置。
5. 选择 **Applications**（应用程序）> **Metadata**（元数据），然后单击 **Download XML metadata**（下载 XML 元数据）以下载需要将其导入防火墙的 XML 元数据。

   文件名则为 dag.xml。因为此文件包含通过防火墙对您的 Duo 账户进行身份验证的敏感信息，因此，必须将其保存在安全位置，防止出现损害此信息的风险。

## 配置防火墙以便与 *Duo* 进行集成

STEP 1 | 导入 Duo 元数据。

1. 登录到防火墙 Web 界面。
2. 在防火墙上，选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（SAML 标识提供商）> **Import**（导入）。
3. 输入 **Profile Name**（配置文件名称）。
4. **Browse**（浏览）到 **Identity Provider Metadata**（标识提供商元数据）文件（**dag.xml**）。
5. 如果 Duo 访问网关提供自签名证书作为 IdP 的签名证书，则无法验证标识提供商证书。在这种情况下，请务必使用 PAN-OS 10.0 减少对 CVE-2020-2021的暴露。




STEP 2 | 添加身份验证配置文件。

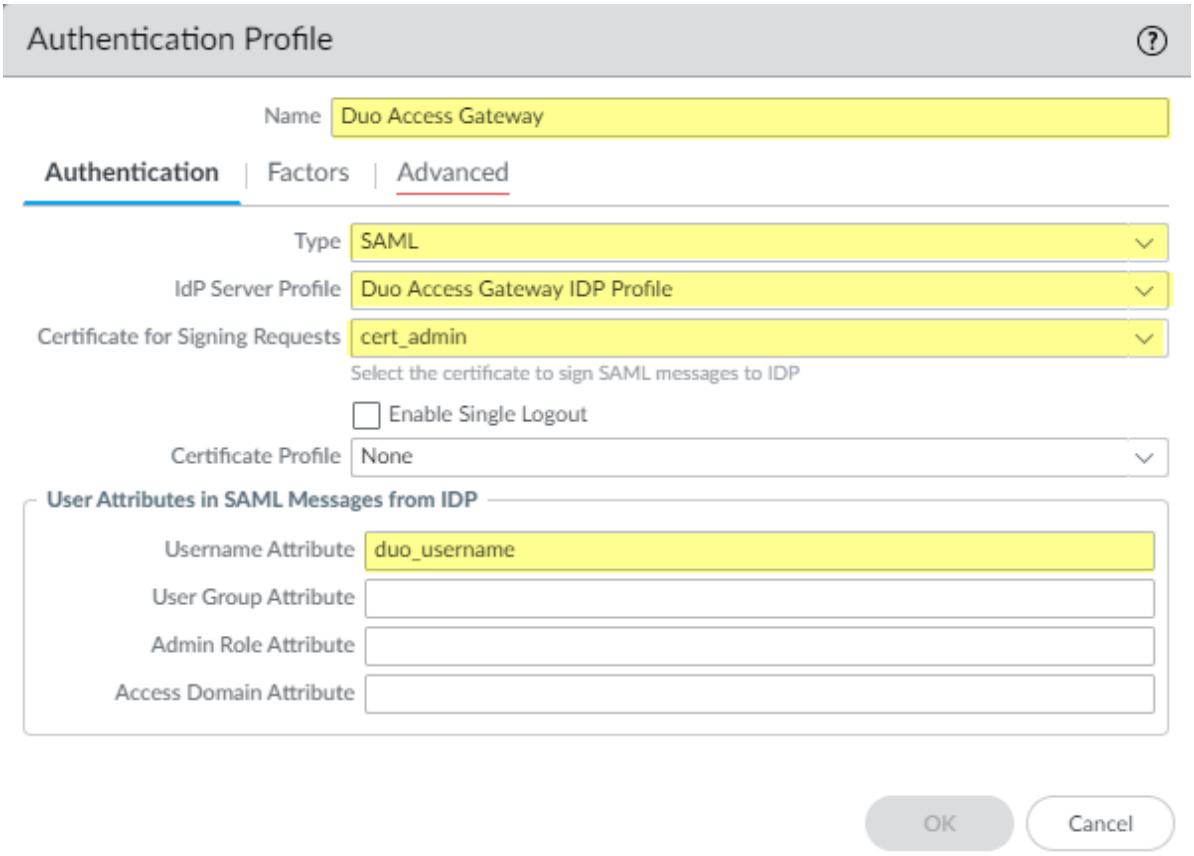
身份验证配置文件允许 Duo 作为验证管理员登录凭据的标识提供商。

1. **Add**（添加）**Authentication Profile**（身份验证配置文件）。
2. 输入配置文件 **Name**（名称）。
3. 选择 **SAML** 作为身份验证 **Type**（类型）。



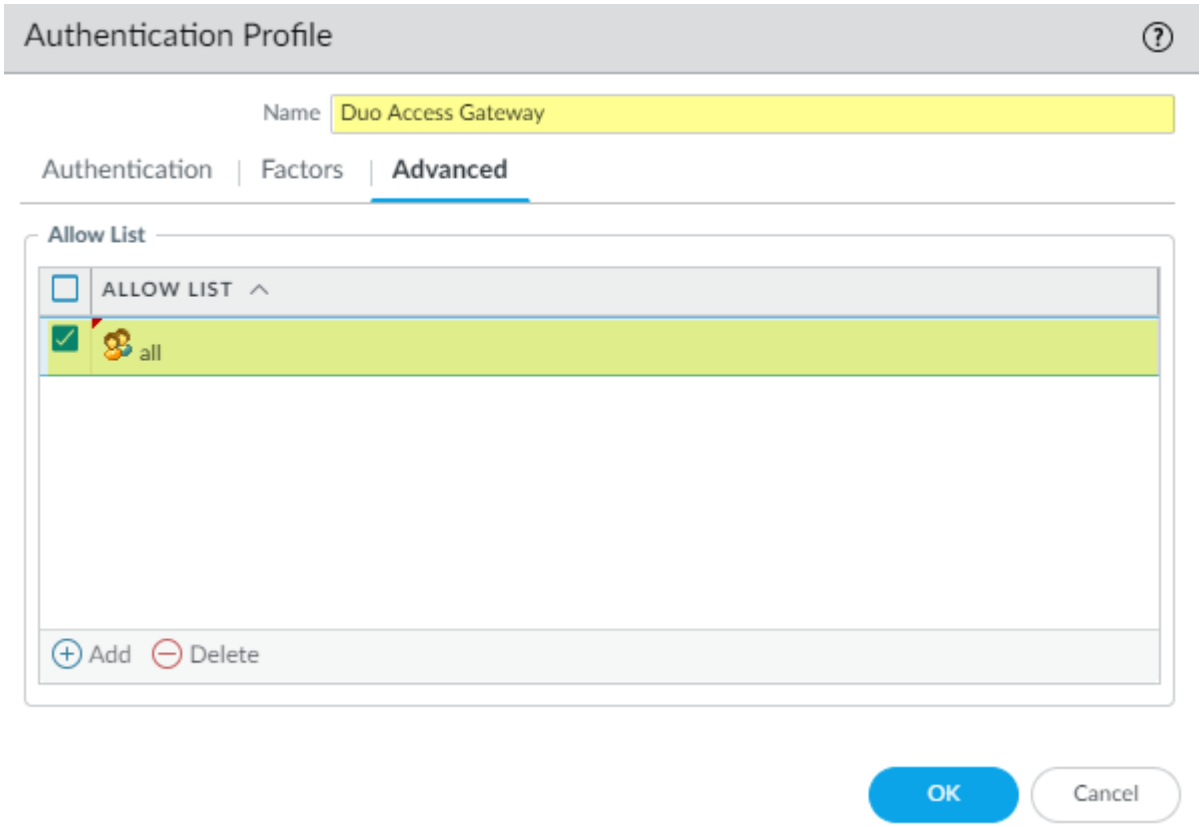
© 2019 Palo Alto Networks, Inc.

4. 选择 **Duo Access Gateway Profile**（**Duo** 访问网关配置文件）作为 **IdP Server Profile**（**IdP** 服务器配置文件）。
5. 选择想要用于与 Duo 访问网关进行 SAML 通信的证书，以获取 **Certificate for Signing Requests**（签名请求证书）。
6. 输入 **`user.username`** 作为 **Username Attribute**（用户名属性）。




7. 选择 **Advanced**（高级）以 **Add**（添加）允许列表。
8. 选择 **all**（全部），然后单击 **OK**（确定）。
9. **Commit**（提交）更改。


© 2019 Palo Alto Networks, Inc.

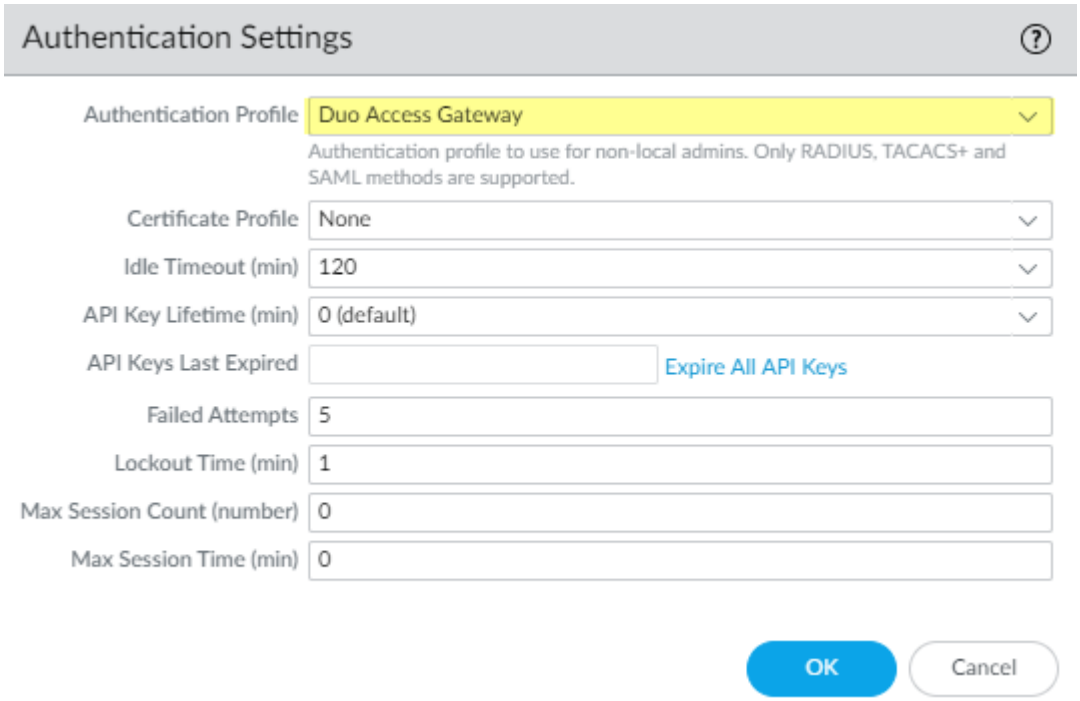



STEP 3 | 指定防火墙用于通过 Duo 实施 SAML 身份验证的身份验证设置。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 **Authentication Settings**（身份验证设置）。
2. 选择 **Duo Access Gateway**（**Duo** 访问网关）作为 **Authentication Profile**（身份验证配置文件），然后单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

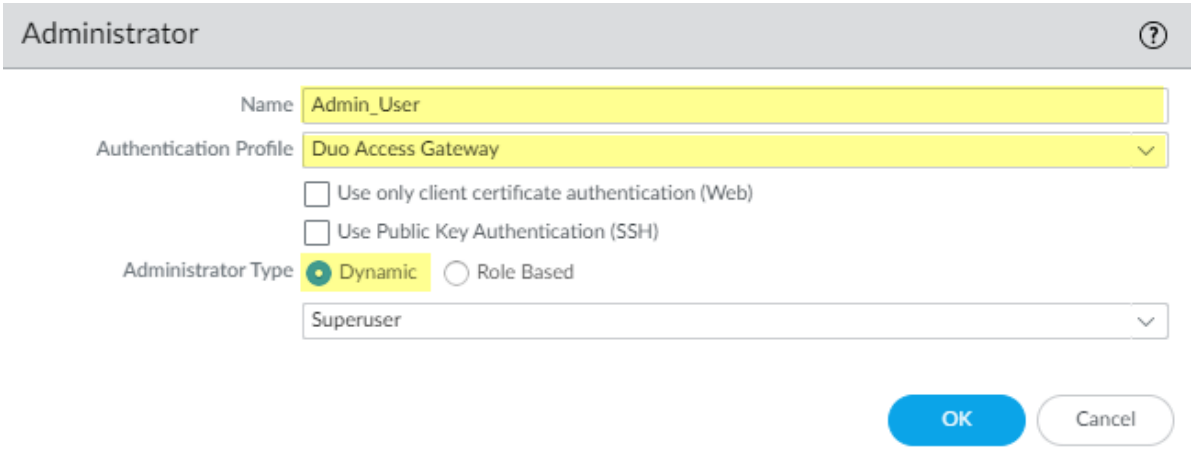



3. **Commit**（提交）更改。

STEP 4 | 为将通过 Duo 对防火墙进行身份验证的管理员添加账户。

1. 选择 **Device**（设备）> **Administrators**（管理员），并 **Add**（添加）帐户。
2. 输入用户 **Name**（名称）。
3. 选择 **Duo Access Gateway**（Duo 访问网关）作为 **Authentication Profile**（身份验证配置文件）。
4. 选择 **Administrator Type**（管理员类型），然后单击 **OK**（确定）。

   如果想为用户使用自定义角色，请选择 **Role Based**（基于角色）。否则，请选择 **Dynamic**（动态）。若要求管理员通过使用 Duo 的 SSO 进行登录，请将身份配置文件分配给所有当前管理员。




## 采用 *Duo* 对 *MFA* 进行验证

STEP 1 | 登录防火墙的 Web 界面。


© 2019 Palo Alto Networks, Inc.

STEP 2 | 选择 **Use Single Sign-On**（使用单点登录），并 **Continue**（继续）。

STEP 3 | 在 Duo 访问网关登录页面上输入您的登录凭据。

STEP 4 | 选择身份验证方法（推送通知、电话呼叫或密码输入）。

身份验证成功后，您将被重定向到防火墙 Web 界面。



© 2019 Palo Alto Networks, Inc.

# 配置 SAML 身份验证

要配置 SAML 单点登录 (SSO) 和单点退出 (SLO)，必须将防火墙和 IdP 相互注册，以实现相互之间的通信。如果 IdP 提供包含注册信息的元数据文件，可将其导入防火墙以注册 IdP 并创建 IdP 服务器配置文件。服务器配置文件定义如何连接到 IdP，并指定 IdP 用于签署 SAML 消息的证书。您还可以为防火墙使用证书来签署 SAML 消息。必须使用证书确保防火墙与 IdP 之间的通信安全。

Palo Alto Networks 需要 HTTPS （而非加密 SAML断言等其他方法）来确保所有 SAML 事务的机密性。要确保 SAML 事务中处理的所有消息的完整性，Palo Alto Networks 要求使用数字证书对所有消息进行加密签名。

以下步骤介绍如何为最终用户和防火墙管理员配置 SAML 身份验证。您还可以为 Panorama 管理员配置 SAML 身份验证。

*SSO* 可供管理员和 *GlobalProtect* 以及身份验证门户最终用户使用。*SLO* 可供管理员和 *GlobalProtect* 最终用户使用，但身份验证门户最终用户不能使用。

管理员可以使用 *SAML* 对防火墙 *Web* 界面进行身份验证，而不对 *CLI* 进行身份验证。

STEP 1 | 获取 IdP 和防火墙将用于签署 SAML 消息的证书。

如果证书没有指定密钥使用属性，默认情况下允许所有用法，包括签名消息。在这种情况下，可以通过任何方法获取证书。

如果证书明确指定密钥使用属性，则其中一个属性必须为数字签名，该属性在防火墙或 Panorama 上生成的证书不可用。在这种情况下，必须导入证书：

- 防火墙用于签署 **SAML** 消息的证书 — 从企业证书颁发机构 (CA) 或第三方 CA 导入证书。
- **IdP** 用于签署 **SAML** 消息的证书（所有部署均须执行）— 从 IdP 导入包含证书的元数据文件（请参阅下一步）。IdP 证书仅限于以下算法：

  公钥算法 — RSA（1,024 位或更大）和 ECDSA（所有大小）。FIPS/CC 模式下的防火墙支持 RSA（2,048 位或更大）和 ECDSA（所有大小）。

  签名算法 — SHA1、SHA256、SHA384 和 SHA512。FIPS/CC 模式下的防火墙支持 SHA256、SHA384 和 SHA512。

STEP 2 | 添加 SAML IdP 服务器配置文件。

服务器配置文件将 IdP 注册到防火墙，并定义连接方式。

在此示例中，从 IdP 导入 SAML 元数据文件，以便防火墙能够自动创建服务器配置文件并填充连接、注册和 IdP 证书信息。

如果 *IdP* 不提供元数据文件，请选择 *Device*（设备）> *Server Profiles*（服务器配置文件）> *SAML Identity Provider*（*SAML* 标识提供商），*Add*（添加）服务器配置文件，并手动输入信息（请咨询您的 *IdP* 管理员了解有关值的信息）。

1. 将 SAML 元数据文件从 IdP 导出到您可以通过其上传元数据到防火墙的客户端系统。

   文件中指定的证书必须符合上述步骤中列出的要求。有关导出文件的说明，请参阅您的 IdP 文档。
2. 选择 Panorama™ 上的**Device**（设备）> **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商）或**Panorama** > **Server Profiles**（服务器配置文件）> **SAML Identity Provider**（**SAML** 标识提供商），然后将元数据文件 **Import**（导入）到防火墙。
3. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
4. **Browse**（浏览）到 **Identity Provider Metadata**（标识提供商元数据）文件。



© 2019 Palo Alto Networks, Inc.

5. 选择 **Validate Identity Provider Certificate**（验证标识提供商证书）（默认），以验证信任链和 IdP 证书的吊销状态（可选）。

   要启用此选项，证书颁发机构 (CA) 必须为您签发 IdP 签名证书。您创建的证书配置文件必须包含颁发 IdP 签名证书的 CA。在 Authentication Profile（身份验证配置文件）中，选择 SAML 服务器配置文件和 Certificate Profile（证书配置文件）以验证 IdP 证书。

   如果您的 IdP 签名证书是一个自签名证书，则不存在信任链；因此，您无法启用此选项。无论是否启用 **Validate Identity Provider Certificate**（验证标识提供商证书）选项，防火墙始终都会根据您配置的标识提供商证书验证 SAML 响应或断言的签名。如果您的 IdP 提供自签名证书，请务必使用 PAN-OS 10.0 版本来降低 CVE-2020-2021 带来的风险。

   验证证书，确保证书未泄露，从而提高安全性。

6. 输入 **Maximum Clock Skew**（最大时钟偏差），这是防火墙验证 IdP 消息时，IdP 与防火墙的系统时间之间允许的差异（以秒为单位）（默认为 60；范围为 1 到 900）。如果差异超过该值，则身份验证失败。
7. 单击 **OK**（确定）保存服务器配置文件。
8. 单击服务器配置文件名称以显示配置文件设置。验证导入的信息是否正确，并在必要时进行编辑。
9. 无论是导入 IdP 元数据还是手动输入 IdP 信息，应始终确保您的 SAML 标识提供商的签名证书是您的服务器配置文件的 **Identity Provider Certificate**（标识提供商证书），且您的 IdP 发送的是经过签名的 SAML 响应、断言或两者。

STEP 3 | 配置身份验证配置文件。

配置文件定义了一组用户通用的身份验证设置。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 将 **Type**（类型）设置为 **SAML**。
4. 选择您配置的 **IdP Server Profile**（**IdP** 服务器配置文件）。
5. 选择 **Certificate for Signing Requests**（签名请求证书）。

   防火墙使用此证书对发送给 IdP 的消息进行签名。您可以导入企业 CA 生成的证书，也可以使用在防火墙或 Panorama 上生成的根 CA 生成证书。
6. （可选）**Enable Single Logout**（启用单点退出）（默认情况下禁用）。
7. 选择防火墙将用于验证 **Identity Provider Certificate**（标识提供商证书）的 **Certificate Profile**（证书配置文件）。
8. 输入 IdP 消息用于标识用户的 **Username Attribute**（用户名属性）（默认为 **`username`**（用户名））。

   预定义用户的动态管理员角色时，使用小写字母指定角色（例如，输入 ***`superreader`***，而不是 ***`SuperReader`***）。如果您管理 *IdP* 标识存储中的管理员授权，还请指定 *Admin Role Attribute*（管理员角色属性）和 *Access Domain Attribute*（访问域属性）。
9. 选择 **Advanced**（高级）并 **Add**（添加）可使用该身份验证配置文件进行身份验证的用户和用户组。
10. 单击 **OK**（确定）保存身份验证配置文件。

STEP 4 | 将身份验证配置文件分配给需要身份验证的防火墙应用程序。

1. 将身份验证配置文件分配给：
   - 您在防火墙上本地管理的管理员帐户。在此示例中，先配置防火墙管理员帐户，然后再验证此过程中的 SAML 配置。



© 2019 Palo Alto Networks, Inc.

- 您在 IdP 标识存储中外部管理的管理员帐户。选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），编辑身份验证设置，然后选择配置的 **Authentication Profile**（身份验证配置文件）。
- 验证用于保护最终用户通过身份验证门户访问的服务和应用程序的策略规则。请参阅配置身份验证策略。
- 最终用户访问的 GlobalProtect 门户和网关。

2. **Commit**（提交）更改。

   防火墙验证您分配给 SAML IdP 服务器配置文件的 **Identity Provider Certificate**（标识提供商证书）。

STEP 5 | 创建 SAML 元数据文件以在 IdP 上注册防火墙应用程序（管理访问、身份验证门户或 GlobalProtect）。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），并在配置的身份验证配置文件的身份验证列中单击 **Metadata**（元数据）。
2. 在 **Service**（服务）下拉列表中，选择要注册的应用程序：
   - **Management**（管理）（默认）— 对 Web 界面的管理访问。
   - **authentication-portal**（身份验证门户）— 最终用户通过身份验证门户访问服务和应用程序。
   - **Global-protect**（全局保护）— 最终用户通过 GlobalProtect 访问服务和应用程序。
3. （仅限身份验证门户或 GlobalProtect）对于 **Vsysname Combo**，选择在其中定义了身份验证门户设置或 GlobalProtect 门户的虚拟系统。
4. 根据您要注册的应用程序输入接口、IP 地址或主机名：
   - **Management**（管理）— 对于 **Management Choice**（管理选择），选择 **Interface**（接口）（默认），然后选择启用的接口以对 Web 界面进行管理访问。默认选择的是 MGT 接口的 IP 地址。
   - **authentication-portal**（身份验证门户）— 对于 **IP Hostname**（**IP** 主机名），输入 **Redirect Host**（重定向主机）的 IP 地址或主机名（请参阅 **Device**（设备）> **User Identification**（用户标识）> **Authentication Portal Settings**（身份验证门户设置））。
   - **global-protect**（全局保护）— 对于 **IP Hostname**（**IP** 主机名），输入 GlobalProtect 门户或网关的主机名或 IP 地址。
5. 单击 **OK**（确定），并将元数据文件保存到客户端系统。
6. 将元数据文件导入 IdP 服务器以注册防火墙应用程序。如需了解相关说明，请参阅 IdP 文档。

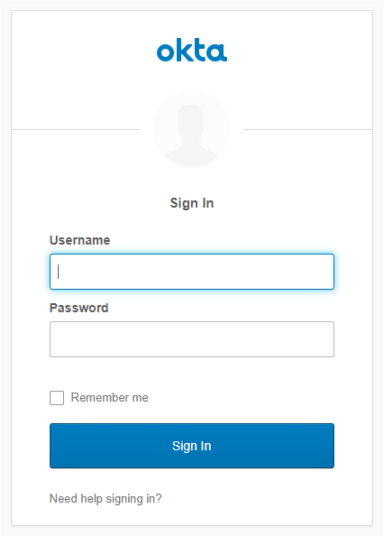
STEP 6 | 验证用户是否可以使用 SAML SSO 进行身份验证。

例如，要验证 SAML 是否正在使用本地管理员帐户访问 Web 界面：

1. 前往防火墙 Web 界面的 URL。
2. 单击 **Use Single Sign-On**（使用单点登录）。
3. 输入管理员的用户名。
4. 单击 **Continue**（继续）。

   防火墙将重定向，以便对显示登录页面的 IdP 进行身份验证。例如：


© 2019 Palo Alto Networks, Inc.




5. 使用您的 SSO 用户名和密码登录。

   在 IdP 上成功进行身份验证后，将重定向到显示 Web 界面的防火墙。
6. 使用您的防火墙管理员帐户请求访问另一个 SSO 应用程序。

   成功访问表示 SAML SSO 身份验证成功。



© 2019 Palo Alto Networks, Inc.

# 配置 Kerberos 单一登入

Palo Alto Networks 防火墙和 Panorama 支持 Kerberos V5 单一登入 (SSO)，其可对访问 Web 界面的管理员及访问身份验证门户的最终用户的身份进行验证。启用 Kerberos SSO 后，仅初次访问网络需要用户登录（例如登录到 Microsoft Windows）。在此初始登录之后，用户便可以在网络中访问任何基于浏览器的服务（例如，防火墙 Web 界面），而不必重新登录，除非 SSO 会话过期。

STEP 1 | 创建 Kerberos 密钥表。

密钥表是包含防火墙的主体名称和密码的文件，是 SSO 进程所必需的。当您在身份验证配置文件和序列中配置 Kerberos 时，防火墙会首先检查 Kerberos SSO 主机名。如果您提供一个主机名，防火墙将搜索密钥表查找与该主机名相匹配的服务主体名称，并仅使用该密钥表解密。如果您没有提供主机名，防火墙将在身份验证序列中逐个尝试密钥表，直至其可以成功通过 Kerberos 验证。



如果发送到防火墙的请求中包含 *Kerberos SSO* 主机名，则主机名必须与密钥表的服务主体名称匹配； 否则，不会发送 *Kerberos* 身份验证请求。

1. 登录到 Active Directory 服务器，打开命令提示符。
2. 输入以下命令注册 GlobalProtect 或身份验证门户的服务主体名称 (SPN)，其中，*<portal_fqdn>* 和 *<service_account_username>* 是变量。

   **setspn -s HTTP/*<portal_fqdn>* *<service_account_username>***
3. 为防火墙创建 Kerberos 帐户。请参阅您的 Kerberos 文档了解步骤。
4. 登录 KDC 并打开命令提示符。
5. 输入以下命令，其中，*<portal_fqdn>*, *<kerberos_realm>*、*<netbios_name>*、*<service_account_username>*、*<password>*、*<filename>* 和 *<algorithm>* 是变量。

   **ktpass /princ HTTP *<portal_fqdn>*@*<kerberos_realm>* /mapuser *<netbios_name>**<service_account_username>* /pass *<password>*/out *<filename>*.keytab /ptype KRB5_NT_PRINCIPAL /crypto *<algorithm>***



*<kerberos_realm>* 值内所有字符均必须为大写（例如，请输入 ***AD1.EXAMPLE.COM***，而不是 ***ad1.example.com***）。



如果防火墙处于 *FIPS/CC* 模式，则算法必须为 ***aes128-cts-hmac-sha1-96*** 或 ***aes256-cts-hmac-sha1-96***。否则，您也可以使用 ***des3-cbc-sha1*** 或 ***arcfour-hmac***。要使用高级加密标准 *(AES)* 算法，*KDC* 的功能级别必须是 *Windows Server 2012* 或更高版本，并且必须为防火墙帐户启用 *AES* 加密。

*keytab* 中的算法必须与 *TGS* 签发给客户的服务票据中的算法相匹配。*Kerberos* 管理员确定服务票据使用的算法。

STEP 2 | 配置身份验证配置文件和序列以定义 Kerberos 设置和一组用户通用的其他身份验证选项。

- 输入 **Kerberos Realm**（**Kerberos** 域）（通常是用户的 DNS 域，除非域为大写）。
- **Import**（导入）您为防火墙创建的 **Kerberos Keytab**（**Kerberos** 密钥表）。

STEP 3 | 将身份验证配置文件分配给需要身份验证的防火墙应用程序。

- 对 Web 界面的管理访问 — 配置防火墙管理员帐户并分配您配置的身份验证配置文件。
- 最终用户访问服务和应用程序 — 将配置的身份验证配置文件分配给身份验证执行对象。配置对象时，请将 **Authentication Method**（身份验证方法）设置为 **browser-challenge**（浏览器-质询）。将对象分配给身份验证策略规则。有关为最终用户配置身份验证的完整步骤，请参阅配置身份验证策略。



© 2019 Palo Alto Networks, Inc.

# 配置 Kerberos 服务器身份验证

您可以使用 Kerberos 将最终用户和防火墙或 Panorama 管理员进行本地身份验证，以访问 Active Directory 域控制器或与 Kerberos V5 兼容的身份验证服务器。这种身份验证方式为交互式，要求用户输入用户名和密码。

要使用 *Kerberos* 服务器进行身份验证，必须能够通过 *IPv4* 地址访问服务器。不支持 *IPv6* 地址。

STEP 1 | 添加 Kerberos 服务器配置文件。

配置文件定义防火墙如何连接到 Kerberos 服务器。

1. 在 Panorama™ 上选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Kerberos** 或**Panorama** > **Server Profiles**（服务器配置文件）> **Kerberos**，然后 **Add**（添加）服务器配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. **Add**（添加）每个服务器并指定 **Name**（名称）（以标识服务器）、IPv4 地址 或 **Kerberos Server**（**Kerberos** 服务器）的 FQDN 以及与服务器进行通信的可选 **Port**（端口）号（默认值为 88）。

   如果使用 *FQDN* 地址对象来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。
4. 单击 **OK**（确定）保存对配置文件所做的更改。

STEP 2 | 分配服务器配置文件至配置身份验证配置文件和序列。

身份验证配置文件定义了一组用户通用的身份验证设置。

STEP 3 | 将身份验证配置文件分配给需要身份验证的防火墙应用程序。

- 对 Web 界面的管理访问 — 配置防火墙管理员帐户并分配您配置的身份验证配置文件。
- 最终用户访问服务和应用程序 — 将配置的身份验证配置文件分配给身份验证执行对象，并将对象分配给身份验证策略规则。有关为最终用户配置身份验证的完整步骤，请参阅配置身份验证策略。

STEP 4 | 验证防火墙是否可以测试身份验证服务器连接，以对用户进行身份验证。



© 2019 Palo Alto Networks, Inc.

# 配置 TACACS+ 身份验证

您可以为最终用户和防火墙或 Panorama 管理员配置 TACACS+ 身份验证。您还可以通过定义供应商特定属性 (VSA) 使用 TACACS+ 来管理管理员授权（角色和访问域分配）。对于所有用户，必须配置 TACACS+ 服务器配置文件，以定义防火墙或 Panorama 如何连接到服务器。然后，将服务器配置文件分配给需要常用身份验证设置的每组用户的身份验证配置文件。身份验证配置文件的使用方式取决于 TACACS+ 服务器进行身份验证的用户：

- 最终用户 — 将身份验证配置文件分配给身份验证执行对象，并将对象分配给身份验证策略规则。有关完整步骤，请参阅配置身份验证策略。
- 具有防火墙或 **Panorama** 本地管理授权的管理帐户 — 将身份验证配置文件分配给防火墙管理员或 Panorama 管理员帐户。
- 具有 **TACACS+** 服务器管理授权的管理帐户 — 以下步骤介绍如何为防火墙管理员配置 TACACS+ 身份验证和授权。有关 Panorama 管理员的信息，请参阅为 Panorama 管理员配置 TACACS+ 身份验证。

STEP 1 | 添加 TACACS+ 服务器配置文件。

配置文件定义防火墙如何连接到 TACACS+ 服务器。

1. 在 Panorama™ 上选择**Device**（设备）> **Server Profiles**（服务器配置文件）> **TACACS+** 或**Panorama** > **Server Profiles**（服务器配置文件）> **TACAS+**，然后 **Add**（添加）配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. （可选）选择 **Administrator Use Only**（仅限管理员使用）以限制管理员访问权限。
4. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-20）。
5. 选择防火墙用于向 TACACS+ 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **CHAP**）。

   如果 *TACACS+* 服务器支持该协议，请选择 *CHAP*；该协议比 *PAP* 更安全。

6. **Add**（添加）每个 TACACS+ 服务器，并输入以下内容：
   - 输入标识服务器的 **Name**（名称）
   - **TACACS+ Server**（**TACACS+** 服务器）IP 地址或 FQDN。如果使用 FQDN 地址对象来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。
   - **Secret**（密钥）/**Confirm Secret**（确认密钥）（加密用户名和密码的密钥）
   - 用于身份验证请求的服务器 **Port**（端口）（默认为 49）
7. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | 将 TACACS+ 服务器配置文件分配到身份验证配置文件。

身份验证配置文件定义了一组用户通用的身份验证设置。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 将 **Type**（类型）设置为 **TACACS+**。
4. 选择您配置的 **Server Profile**（服务器配置文件）。
5. 选择 **Retrieve user group from TACACS+**（从 **TACACS+** 中检索用户组），以从 TACACS+ 服务器上定义的 VSA 收集用户组信息。

   防火墙与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的用户和组。
7. 单击 **OK**（确定）保存身份验证配置文件。


© 2019 Palo Alto Networks, Inc.

STEP 3 | 配置防火墙，以便为所有管理员使用身份验证配置文件。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 Authentication Settings（身份验证设置）。
2. 选择您配置的 **Authentication Profile**（身份验证配置文件），然后单击 **OK**（确定）。

STEP 4 | 配置为管理员定义授权设置的角色和访问域。

如果您已在 TACACS+ 服务器上定义 TACACS+ VSA，则为防火墙上的角色和访问域指定的名称必须与 VSA 值相匹配。

1. 如果管理员将使用自定义角色而不是预先定义（动态）角色，请配置管理角色配置文件。
2. 如果防火墙有多个虚拟系统，请配置访问域 — 选择 **Device**（设备）> **Access Domain**（访问域），**Add**（添加）访问域，输入 **Name**（名称）以标识访问域，并 **Add**（添加）管理员将访问的每个虚拟系统，然后单击 **OK**（确定）。

STEP 5 | **Commit**（提交）您的更改，以在防火墙上将其激活。

STEP 6 | 配置 TACACS+ 服务器对管理员进行身份验证和授权。

有关执行以下步骤的具体说明，请参阅 TACACS+ 服务器文档：

1. 添加作为 TACACS+ 客户端的防火墙 IP 地址或主机名。
2. 添加管理员帐户。

   如果您选择将 *CHAP* 指定为 *Authentication Protocol*（身份验证协议），则必须使用可逆加密密码定义帐户。否则，*CHAP* 身份验证将失败。
3. 为每个管理员的角色、访问域和用户组定义 TACACS+ VSA。

   预定义用户的动态管理员角色时，使用小写字母指定角色（例如，输入 ***superuser***，而不是 ***SuperUser***）。

STEP 7 | 验证 TACACS+ 服务器是否为管理员执行身份验证和授权。

1. 使用您添加到 TACACS+ 服务器的管理员帐户登录防火墙 Web 界面。
2. 验证您是否只能访问与管理员关联的角色允许的 Web 界面页面。
3. 在 **Monitor**（监控）、**Policies**（策略）和 **Objects**（对象）选项卡中，验证您是否只能访问与管理员关联的访问域允许的虚拟系统。



© 2019 Palo Alto Networks, Inc.

# 配置 RADIUS 身份验证

您可以为最终用户和防火墙或 Panorama 管理员配置 RADIUS 身份验证。对于管理员，您可以通过定义供应商特定属性 (VSA) 使用 RADIUS 来管理授权（角色和访问域分配）。您还可以使用 RADIUS 为管理员和最终用户实施多重因素身份验证 (MFA)。要启用 RADIUS 身份验证，必须配置 RADIUS 服务器配置文件，以定义防火墙或 Panorama 如何连接到服务器（请参阅以下步骤 1）。然后，将服务器配置文件分配给需要常用身份验证设置的每组用户的身份验证配置文件（请参阅以下步骤 5）。身份验证配置文件的使用方式取决于 RADIUS 服务器进行身份验证的用户：

- 最终用户 — 将身份验证配置文件分配给身份验证执行对象，并将对象分配给身份验证策略规则。有关完整步骤，请参阅配置身份验证策略。



您也可以通过将身份验证配置文件分配给 *GlobalProtect* 门户或网关，配置发送 *RADIUS* 供应商特定属性 VSA 的客户端系统到 *RADIUS* 服务器。然后，*RADIUS* 管理员根据这些 *VSA* 执行管理任务。

- 具有防火墙或 **Panorama** 本地管理授权的管理帐户 — 将身份验证配置文件分配给防火墙管理员或 Panorama 管理员帐户。
- 具有 **RADIUS** 服务器管理授权的管理帐户 — 以下步骤介绍如何为防火墙管理员配置 RADIUS 身份验证和授权。有关 Panorama 管理员的信息，请参阅为 Panorama 管理员配置 RADIUS 身份验证。

STEP 1 | 添加 RADIUS 服务器配置文件。

配置文件定义防火墙如何连接到 RADIUS 服务器。

1. 在 Panorama™ 上选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **RADIUS** 或**Panorama** > **Server Profiles**（服务器配置文件）> **RADIUS**，然后 **Add**（添加）配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. （可选）选择 **Administrator Use Only**（仅限管理员使用）以限制管理员访问权限。
4. 输入身份验证请求超时后以秒为单位的 **Timeout**（超时）（默认为 3；范围为 1-120）。



如果使用服务器配置文件将防火墙与 *MFA* 服务进行集成，请输入一个能够让用户拥有足够时间进行身份验证的间隔。例如，如果 *MFA* 服务提示输入一次性密码 *(OTP)*，则用户需要时间查看其端点设备上的 *OTP*，然后在 *MFA* 登录页面输入 *OTP*。

5. 输入 **Retries**（重试）次数。
6. 选择防火墙用于向 RADIUS 服务器进行身份验证的 **Authentication Protocol**（身份验证协议）（默认为 **PEAP-MSCHAPv2**）。

   根据您要在多重因素身份验证 (MFA) 环境中对用户进行身份验证的因素，选择相应的身份验证协议：

   - 用户名、密码和推送（自动触发的带外请求）：支持所有身份验证协议
   - 推送、密码、令牌和 **PIN**（当密码或令牌或 **PIN** 一起提供时）：支持 PAP、PEAP with GTC 和 EAP-TTLS with PAP
   - 用户名、密码、令牌、 **PIN** 和质询 - 响应（当密码或令牌或 **PIN** 一起提供时）:支持 PAP 和 PEAP with GTC

   如果选择 EAP 身份验证方法（PEAP-MSCHAPv2、PEAP with GTC 或 EAP-TTLS with PAP），请确认您的 RADIUS 服务器是否支持传输层安全 (TLS) 1.1 或更高版本，您的 RADIUS 服务器的根证书和中间证书颁发机构 (CA) 是否包含在与 RADIUS 服务器配置文件相关的证书配置文件中。如果选择 EAP 方法，且您未能将已配置的证书配置文件与 RADIUS 配置文件相关联，则身份验证失败。
7. **Add**（添加）每个 RADIUS 服务器，并输入以下内容：

   - 输入标识服务器的 **Name**（名称）
   - **RADIUS Server**（**RADIUS** 服务器）IP 地址或 FQDN。如果使用 FQDN 来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。



© 2019 Palo Alto Networks, Inc.

- **Secret**（密钥）/**Confirm Secret**（确认密钥）是加密密码的关键，最长不超过 64 个字符。
- 用于身份验证请求的服务器 **Port**（端口）（默认为 1812）

8. 单击 **OK**（确定）保存服务器配置文件。

对于冗余，请按照您想要防火墙使用的序列添加多个 RADIUS 服务器。如果您已选中 EAP 方法，请配置一个身份验证序列，确保用户将能够成功响应身份验证质询。EAP 没有备用的身份验证方法：如果用户的身份验证质询失败，且您尚未配置一个允许其他身份验证方法的身份验证序列，则身份验证失败。

STEP 2 | 如果您将 PEAP-MSCHAPv2 和 GlobalProtect 一起使用，请选择 **Allow users to change passwords after expiry**（允许用户在密码到期后进行更改），使 GlobalProtect 用户更改过期密码，以便登录。

STEP 3 | （仅 PEAP-MSCHAPv2、PEAP with GTC 或 EAP-TTLS with PAP）要在使用服务器进行身份验证之后，对创建的外部隧道中的用户身份进行匿名化处理，请选择 **Make Outer Identity Anonymous**（使外部身份匿名）。



您必须配置 *RADIUS* 服务器，以便整条链均允许匿名用户访问。某些 *RADIUS* 服务器配置可能不支持匿名外部标识，因此您可能需要清除该选项。清除时，*RADIUS* 服务器将以明文形式传输用户名。

STEP 4 | 如果选择 EAP 身份验证方法，则选中证书配置文件。

STEP 5 | 将 RADIUS 服务器配置文件分配到身份验证配置文件。

身份验证配置文件定义了一组用户通用的身份验证设置。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识身份验证配置文件。
3. 将 **Type**（类型）设置为 **RADIUS**。
4. 选择您配置的 **Server Profile**（服务器配置文件）。
5. 选择 **Retrieve user group from RADIUS**（从 **RADIUS** 中检索用户组），以从 RADIUS 服务器上定义的 VSA 收集用户组信息。

   防火墙与您在身份验证配置文件允许列表中指定的组在组信息方面进行匹配。
6. 选择 **Advanced**（高级），并在允许列表中 **Add**（添加）允许使用此身份验证配置文件进行身份验证的用户和组。
7. 单击 **OK**（确定）保存身份验证配置文件。

STEP 6 | 配置防火墙，以便为所有管理员使用身份验证配置文件。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 Authentication Settings（身份验证设置）。
2. 选择您配置的 **Authentication Profile**（身份验证配置文件），然后单击 **OK**（确定）。

STEP 7 | 配置为管理员定义授权设置的角色和访问域。

如果您已在 RADIUS 服务器上定义 RADIUS VSA，则为防火墙上的角色和访问域指定的名称必须与 VSA 值相匹配。

1. 如果管理员使用自定义角色而不是预先定义（动态）角色，请配置管理员角色配置文件。
2. 如果防火墙拥有多个虚拟系统，请配置访问域：
   1. 选择 **Device**（设备）> **Access Domain**（访问域），**Add**（添加）访问域，然后输入 **Name**（名称）以识别访问域。
   2. **Add**（添加）管理员将访问的每个虚拟系统，然后单击 **OK**（确定）。

STEP 8 | **Commit**（提交）您的更改，以在防火墙上将其激活。



© 2019 Palo Alto Networks, Inc.

STEP 9 | 配置 RADIUS 服务器对管理员进行身份验证和授权。

有关执行以下步骤的具体说明，请参阅 RADIUS 服务器文档：

1. 添加作为 RADIUS 客户端的防火墙 IP 地址或主机名。
2. 添加管理员帐户。

   如果 *RADIUS* 服务器配置文件将 *CHAP* 指定为 *Authentication Protocol*（身份验证协议），则必须使用可逆加密密码定义帐户。否则，*CHAP* 身份验证将失败。
3. 定义防火墙的供应商代码 (25461)，并为每个管理员的角色、访问域和用户组定义 RADIUS VSA。

   预定义用户的动态管理员角色时，使用小写字母指定角色（例如，输入 **`superuser`**，而不是 **`SuperUser`**）。

   在 *ACS* 上配置高级供应商选项时，必须将 *Vendor Length Field Size*（供应商长度字段大小）和 *Vendor Type Field Size*（供应商类型字段大小）同时设置为 ***1***。否则，身份验证将失败。
4. 如已选择 EAP 方法，则防火墙将对服务器，而不是客户端进行验证。要确保客户端的有效性，请按 IP 地址或子域限制客户端。

STEP 10 | 验证 RADIUS 服务器是否为管理员执行身份验证和授权。

1. 使用您添加到 RADIUS 服务器的管理员帐户登录防火墙 Web 界面。
2. 验证您是否只能访问与管理员关联的角色允许的 Web 界面页面。
3. 在 **Monitor**（监控）、**Policies**（策略）和 **Objects**（对象）选项卡中，验证您是否只能访问与管理员关联的访问域允许的虚拟系统。
4. 在 **Monitor**（监控）> **Authentication**（身份验证）中，检验 **Authentication Protocol**（身份验证协议）。
5. 使用以下 CLI 命令测试证书配置文件的连接和有效性：

```
admin@PA-220 > test authentication authentication-profile auth-profile
 username <username> password <password>
```


© 2019 Palo Alto Networks, Inc.

# 配置 LDAP 身份验证

您可以使用 LDAP 对通过身份验证门户访问应用程序或服务的最终用户进行身份验证，并对访问 Web 界面的防火墙或 Panorama 管理员进行身份验证。



您还可以连接到 *LDAP* 服务器，以根据用户组定义策略规则。有关详细信息，请参阅将用户映射到组。

STEP 1 | 添加 LDAP 服务器配置文件。

配置文件对防火墙如何连接到 LDAP 服务器进行定义。

1. 在 Panorama™ 上选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP** 或**Panorama** > **Server Profiles**（服务器配置文件）> **LDAP**，然后 **Add**（添加）服务器配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. （仅多 vsys）选择配置文件可用的 **Location**（位置）。
4. （可选）选择 **Administrator Use Only**（仅限管理员使用）以限制管理员访问权限。
5. **Add**（添加）LDAP 服务器（最多 4 个）。对于每个服务器，输入 **Name**（名称）（以标识服务器）、**LDAP Server**（**LDAP** 服务器）IP 地址或 FQDN 以及服务器 **Port**（端口）（默认为 389）。

   如果使用 *FQDN* 地址对象来标识服务器，并随后更改地址，则必须提交更改以使新服务器地址生效。
6. 选择服务器 **Type**（类型）。
7. 选择 **Base DN**（基本 **DN**）。

   要标识目录的基本 DN，请打开 **Active Directory Domains and Trusts**（活动目录域和信任）Microsoft 管理控制台控制单元，并使用顶级域的名称。
8. 输入 **Bind DN**（绑定 **DN**）和 **Password**（密码）以启用身份验证服务对防火墙进行身份验证。

   绑定 *DN* 账户必须有权读取 *LDAP* 目录。
9. 以秒为单位输入 **Bind Timeout**（绑定超时）和 **Search Timeout**（搜索超时）（默认均为 30）。
10. 输入 **Retry Interval**（重试时间间隔），以秒计（默认为 60）。
11. 启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项（默认已启用）。端点使用的协议取决于服务器端口：
    - 389（默认）— TLS（具体来说，设备使用 StartTLS 操作，这可以将初始明文连接升级至 TLS。）
    - 636 — SSL
    - 任何其他端口 — 设备首先尝试使用 TLS。如果目录服务器不支持 TLS，则设备回滚至 SSL。
12. （可选）如需额外的安全性，启用 **Verify Server Certificate for SSL sessions**（验证 **SSL** 会话的服务器证书）选项，使端点验证目录服务器为 SSL/TLS 连接出示的证书。要启用验证，还必须启用 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）选项。为了验证成功，证书必须符合以下条件之一：
    - 它位于设备证书列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。必要时，将证书导入设备。
    - 证书签发机构位于可信证书授权机构列表中：**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Default Trusted Certificate Authorities**（默认可信证书授权机构）。
13. 单击 **OK**（确定）保存服务器配置文件。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 分配服务器配置文件至 Configure an Authentication Profile and Sequence（配置身份验证配置文件和序列），以定义各种身份验证设置。

STEP 3 | 将身份验证配置文件分配给需要身份验证的防火墙应用程序。

- 对 **Web** 界面的管理访问 — 配置防火墙管理员帐户并分配您配置的身份验证配置文件。
- 最终用户访问服务和应用程序 — 有关为最终用户配置身份验证的完整步骤，请参阅配置身份验证策略。

STEP 4 | 验证防火墙是否可以测试身份验证服务器连接，以对用户进行身份验证。



© 2019 Palo Alto Networks, Inc.

# 身份验证服务器连接超时

您可以将防火墙配置为使用外部身份验证服务来对访问防火墙或 Panorama 的管理员以及通过身份验证门户访问服务或应用程序的最终用户进行身份验证。要确保防火墙不会通过持续尝试到达不可访问的身份验证服务器来浪费资源，可以设置超时间隔，以使防火墙在该间隔结束后停止尝试连接。您可以在服务器配置文件中设置超时，以定义防火墙连接到身份验证服务器的方式。选择超时值时，您的目标是在保护防火墙资源的需要和考虑影响身份验证服务器对防火墙的响应速度的正常网络延迟之间取得平衡。

- 设置身份验证服务器超时的原则
- 修改 PAN-OS Web 服务器超时
- 修改身份验证门户会话超时

## 设置身份验证服务器超时的原则

以下是一些有关超时设置的原则，以便防火墙尝试与外部身份验证服务相连接。

- 除了在特定服务器的服务器配置文件中设置的超时之外，防火墙还具有全局 PAN-OS Web 服务器超时。当防火墙连接到任何外部服务器以对防火墙 Web 界面或 PAN-OS XML API 的管理访问以及通过身份验证门户对应用程序或服务进行访问的最终用户进行身份验证时，全局超时适用。默认情况下，全局超时为 30 秒（范围为 3-125）。它必须等于或大于任何服务器配置文件允许连接尝试的总时间。服务器配置文件的总时间等于超时值乘以重试次数再乘以服务器数量。例如，如果 RADIUS 服务器配置文件指定 3 秒超时、3 次重试和 4 个服务器，则配置文件允许连接尝试的总时间为 36 秒 (3 x 3 x 4)。必要时修改 PAN-OS Web 服务器超时。

  除非发现身份验证失败，否则请勿更改 *PAN-OS Web* 服务器超时。将超时设置过高可能会降低防火墙的性能或导致其丢弃身份验证请求。您可以在身份验证日志中查看身份验证失败。
- 防火墙使用身份验证门户会话超时，该超时对最终用户响应身份验证门户 Web 表单中的身份验证挑战所花费的时间进行定义。当用户请求符合身份验证策略规则的服务或应用程序时，会显示 Web 表单。默认情况下，会话超时为 30 秒（范围为 1-1,599,999）。它必须等于或大于 PAN-OS Web 服务器超时。必要时修改身份验证门户会话超时。请记住，增加 PAN-OS Web 服务器和身份验证门户会话超时可能会降低防火墙的性能或导致其丢弃身份验证请求。

  身份验证门户会话超时与用于确定防火墙保留 *IP* 地址到用户名映射的时间的计时器无关。
- 超时是身份验证序列的累积结果。例如，考虑具有两个身份验证配置文件的身份验证序列的情况。一个身份验证配置文件指定 RADIUS 服务器配置文件具有 3 秒超时、3 次重试和 4 个服务器。另一个身份验证配置文件指定 TACACS+ 服务器配置文件具有 3 秒超时和 2 个服务器。防火墙可以尝试使用该身份验证顺序对用户进行身份验证的最长时间为 42 秒：RADIUS 服务器配置文件的 36 秒加上 TACACS+ 服务器配置文件的 6 秒。
- Kerberos 服务器配置文件中指定的每个服务器的 Kerberos 服务器超时为 17 秒，且不可配置。
- 要配置其他服务器类型的超时和相关设置，请参阅：
  - 添加 MFA 服务器配置文件。
  - 添加 SAML IdP 服务器配置文件。
  - 添加 TACACS+ 服务器配置文件。
  - 添加 RADIUS 服务器配置文件。
  - 添加 LDAP 服务器配置文件。



© 2019 Palo Alto Networks, Inc.

## 修改 PAN-OS Web 服务器超时

PAN-OS Web 服务器超时必须等于或大于任何身份验证服务器配置文件中的超时与该配置文件中的重试次数和服务器数量的乘积。

除非发现身份验证失败，否则请勿更改 *PAN-OS Web* 服务器超时。将超时设置过高可能会降低防火墙的性能或导致其丢弃身份验证请求。您可以在身份验证日志中查看身份验证失败。

STEP 1 | 访问防火墙 CLI。

STEP 2 | 通过输入以下命令设置 PAN-OS Web 服务器超时，其中 ***<value>*** 是秒数（默认为 30；范围为 3 到 125）。

```
> configure
# set deviceconfig setting l3-service timeout <value>
# commit
```

## 修改身份验证门户会话超时

身份验证门户会话超时必须大于等于 PAN-OS Web 服务器超时。有关详细信息，请参阅身份验证服务器连接超时。

您将 *PAN-OS Web* 服务器和身份验证门户会话超时值设置的越高，身份验证门户响应用户的速度就越慢。

STEP 1 | 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话超时。

STEP 2 | 以秒为单位输入新的 **Authentication Portal**（身份验证门户）值（默认值为 30；范围为 1 到 1,599,999），然后单击 **OK**（确定）。

STEP 3 | **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 配置本地数据库身份验证

您可以配置防火墙本地的用户数据库，以对访问防火墙 Web 界面的管理员以及通过身份验证门户或 GlobalProtect 访问应用程序的最终用户进行身份验证。执行以下步骤以使用本地数据库配置本地身份验证。



外部身份验证服务通常比本地身份验证更好，因为它们能对帐户进行集中式管理。

您还可以在没有数据库的情况下配置本地身份验证，但只能对防火墙或 Panorama 管理员进行身份验证。

STEP 1 | 将用户帐户添加到本地数据库。

1. 选择 **Device**（设备）> **Local User Database**（本地用户数据库）> **Users**（用户），然后单击 **Add**（添加）。
2. 输入管理员的用户 **Name**（名称）。
3. 输入 **Password**（密码）和 **Confirm Password**（确认密码）或 **Password Hash**（密码哈希）。
4. **Enable**（启用）帐户（默认为启动）并单击 **OK**（确定）。

STEP 2 | 将用户组添加到本地数据库。

如果您的用户需要群组关系，则需进行该操作。

1. 选择 **Device**（设备）> **Local User Database**（本地用户数据库）> **User Groups**（用户组），然后单击 **Add**（添加）。
2. 输入 **Name**（名称）以标识用户组。
3. **Add**（添加）该组的所有用户，单击 **OK**（确定）。

STEP 3 | 配置身份验证配置文件。

身份验证配置文件定义了一组用户通用的身份验证设置。设置 **Local Database**（本地数据库）的身份验证 **Type**（类型）。

STEP 4 | 将身份验证配置文件分配给管理员帐户或身份验证策略规则，以便最终用户使用。

- 管理员 — 配置防火墙管理员帐户：

  指定在该步骤之前定义的用户 **Name**（名称）。

  分配您为该帐户配置的 **Authentication Profile**（身份验证配置文件）。

- 最终用户 — 有关为最终用户配置身份验证的完整步骤，请参阅配置身份验证策略。

STEP 5 | 验证防火墙是否可以测试身份验证服务器连接，以对用户进行身份验证。



© 2019 Palo Alto Networks, Inc.

# 配置身份验证配置文件和序列

身份验证配置文件定义身份验证服务，对访问防火墙 Web 界面的管理员以及通过身份验证门户或 GlobalProtect 访问应用程序的最终用户的登录凭据进行验证。该服务可以是防火墙提供的本地身份验证，也可以是外部身份验证服务。身份验证配置文件还定义了 Kerberos 单点登录 (SSO) 等选项。

一些网络具有多个数据库（例如 TACACS+ 和 LDAP）以用于不同用户和用户组。要在这种情况下对用户进行身份验证，请配置身份验证序列 — 登录时防火墙与用户匹配的身份验证配置文件的排列次序。防火墙依次检查每个配置文件，直到成功验证用户的身份。只有序列中所有配置文件的身份验证都失败时，才会拒绝用户访问。序列可以指定基于防火墙支持的任何身份验证服务的身份验证配置文件，但多重因素身份验证 (MFA) 和 SAML 除外。

STEP 1 | （仅限外部服务）将防火墙与外部服务器相连接，以对用户身份进行验证：

1. 设置外部服务器。如需了解相关说明，请参阅服务器文档。
2. 为您使用的身份验证服务类型配置服务器配置文件。
   - 添加 RADIUS 服务器配置文件。

     如果防火墙通过 *RADIUS* 与 *MFA* 服务集成，则必须添加 *RADIUS* 服务器配置文件。在这种情况下，*MFA* 服务提供所有身份验证因素。如果防火墙通过供应商 *API* 与 *MFA* 服务集成，您仍然可以使用 *RADIUS* 服务器配置文件作为第一个因素，但还需要 *MFA* 服务器配置文件作为其他因素。

   - 添加 MFA 服务器配置文件。
   - 添加 SAML IdP 服务器配置文件。
   - 添加 Kerberos 服务器配置文件。
   - 添加 TACACS+ 服务器配置文件。
   - 添加 LDAP 服务器配置文件。

STEP 2 | （仅限本地数据库身份验证）配置属于防火墙本地的用户数据库。

对于要根据属于防火墙本地的用户身份存储来配置本地身份验证的每个用户和用户组，请执行以下步骤：

1. 将用户帐户添加到本地数据库。
2. （可选）将用户组添加到本地数据库。

STEP 3 | （仅限 Kerberos SSO）如果 Kerberos 单点登录 (SSO) 是主身份验证服务，请为防火墙创建 Kerberos 密钥表。

创建 Kerberos 密钥表。密钥表是包含防火墙的 Kerberos 帐户信息的文件。要支持 Kerberos SSO，您的网络必须具有 Kerberos 基础架构。

STEP 4 | 配置身份验证配置文件。

定义下列中的其一或两者：

- **Kerberos SSO** — 防火墙首先尝试 SSO 身份验证。如果失败，则返回到指定的身份验证 **Type**（类型）。
- 外部身份验证或本地数据库身份验证 — 防火墙提示用户输入登录凭据，并使用外部服务或本地数据库对用户进行身份验证。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件）并 **Add**（添加）身份验证文件。
2. 输入 **Name**（名称）以标识身份验证配置文件。
3. 选择身份验证服务 **Type**（类型）。


© 2019 Palo Alto Networks, Inc.

如果您使用多重因素身份验证，则所选类型仅适用于第一个身份验证因素。在 **Factors**（因素）选项卡中选择其他 MFA 因素的服务。

如果选择 **RADIUS**、**TACACS+**、**LDAP** 或 **Kerberos**，请选择 **Server Profile**（服务器配置文件）。

如果选择 **LDAP**，请选择 **Server Profile**（服务器配置文件）并定义 **Login Attribute**（登录属性）。对于 Active Directory，请输入 **sAMAccountName**（sAMAccountName）作为值。

如果选择**SAML**，请选择 **IdP Server Profile**（**IdP** 服务器配置文件）。

4. 如果您想要启用 Kerberos SSO，输入 **Kerberos Realm**（**Kerberos** 域）（通常是用户的 DNS 域，除非域为大写）并 **Import**（导入）您为防火墙或 Panorama 创建的 **Kerberos Keytab**。
5. （仅限 MFA），选择 **Factors**（因素），**Enable Additional Authentication Factors**（启用其他身份验证因素），并 **Add**（添加）您配置的 MFA 服务器配置文件。

   防火墙将按照列出的顺序从上到下调用每个 MFA 服务。
6. 选择 **Advanced**（高级）并 **Add**（添加）可使用该配置文件进行身份验证的用户和用户组。

   您可从本地数据库选择用户和用户组，或者，从基于 LDAP 的目录服务（如 Active Directory）将防火墙配置为将用户映射到组。默认情况下，此列表为空，意味着没有任何用户可以进行身份验证。

   您还可以选择在组映射配置中定义的自定义组。
7. （可选）要在防火墙向服务器发送身份验证请求之前修改用户信息，请配置 **Username Modifier**（用户名修饰符）。

   - **%USERDOMAIN%\%USERINPUT%** — 如果源不包含域（例如，使用 sAMAccountName 时），防火墙会在用户名之前添加您指定的 **User Domain**（用户域）。如果源包含域，则防火墙将该域替换为 **User Domain**（用户域）。如果 **User Domain**（用户域）为空，在防火墙发送请求到身份验证服务器之前，会将该域自防火墙从源接收的用户信息中删除。

     因为 *LDAP* 服务器不支持 *sAMAccountName* 中的反斜杠，因此，不得使用此选项对 *LDAP* 服务器进行身份验证。
   - **%USERINPUT%** —（默认）防火墙采用从源接收到的格式发送用户信息到身份验证服务器。
   - **%USERINPUT%@%USERDOMAIN%** — 如果防火墙不包含该域，则会在用户名后添加 **User Domain**（用户域）值。如果源包含域，则防火墙将该域替换为 **User Domain**（用户域）值。如果 **User Domain**（用户域）为空，防火墙在发送请求到身份验证服务器之前，会从防火墙从源接收的用户信息中删除该域。
   - 无 — 如果手动输入 **`None`**：
     - 对于 LDAP 和 Kerberos 服务器配置文件，防火墙使用从源接收的域选择合适的身份验证配置文件，然后在发送身份验证请求到服务器时删除该域。这样，您就可以在身份验证序列中包含 **User Domain**（用户域），但会在防火墙发送身份验证请求到服务器之前删除该域。例如，如果使用 LDAP 服务器配置文件和 samAccountName 充当属性，则使用此选项，这样，防火墙不会将该域发送至仅需要用户名而不需要域的身份验证服务器。
     - 对于 RADIUS 服务器配置文件：
       - 如果源以 **`domain\username`** 格式发送用户信息，则防火墙以相同格式发送用户信息到服务器。
       - 如果源以 **`username@domain`** 格式发送用户信息，在将其发送到服务器之前，防火墙将用户信息格式标准化为 **`domain\username`**。
       - 如果源仅发送用户名，在以 **`domain\username`** 格式发送信息到服务器之前，防火墙添加您指定的 **User Domain**（用户域）。
     - 对于本地数据库、TACACS+ 和 SAML，防火墙采用从源接收到的格式发送用户信息到身份验证服务器。
8. 单击 **OK**（确定）保存身份验证配置文件。



© 2019 Palo Alto Networks, Inc.

STEP 5 | 配置身份验证序列。

如果您希望防火墙尝试多个身份验证配置文件来对用户进行身份验证，则是必需的。防火墙按自上而下的顺序对配置文件进行评估，直到有一个配置文件成功实现用户身份验证。

1. 选择 **Device**（设备）> **Authentication Sequence**（身份验证序列）并 **Add**（添加）身份验证序列。
2. 输入 **Name**（名称）以标识身份验证序列。



为加速身份验证流程，*Use domain to determine authentication profile*（利用域确定身份验证配置文件）：防火墙将对用户在登录时输入的域名与序列中的身份验证配置文件的 *User Domain*（用户域）或 *Kerberos Realm*（*Kerberos* 域）进行匹配，然后利用配置文件来进行用户身份验证。如果防火墙找不到匹配项，或者您禁用了该选项，则防火墙按自上而下的顺序尝试配置文件。

3. **Add**（添加）每个身份验证配置文件。要更改配置文件的评估顺序，选择一个配置文件，然后 **Move Up**（上移）或 **Move Down**（下移）。
4. 单击 **OK**（确定）以保存身份验证序列。

STEP 6 | 将身份验证配置文件或序列分配给防火墙管理员的管理帐户或最终用户的身份验证策略。

- 管理员 — 根据管理员授权的方式分配身份验证配置文件：

  在防火墙上本地管理的授权 — 配置防火墙管理员帐户。

  在 SAML、TACACS+ 或 RADIUS 服务器上管理的授权 — 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），编辑身份验证设置，并选择 **Authentication Profile**（身份验证配置文件）。

- 最终用户 — 有关为最终用户配置身份验证的完整步骤，请参阅配置身份验证策略。

STEP 7 | 验证防火墙是否可以测试身份验证服务器连接，以对用户进行身份验证。



© 2019 Palo Alto Networks, Inc.

# 测试身份验证服务器连接

测试身份验证功能使您能够验证防火墙或 Panorama 是否可以与身份验证配置文件中指定的身份验证服务器进行通信，以及向特定用户提出的身份验证请求是否成功。您可以测试对访问 Web 界面的管理员或通过 GlobalProtect 或身份验证门户访问应用程序的最终用户进行身份验证的身份验证配置文件。您可以在待选配置中执行身份验证测试，以在提交前验证配置是否正确。

STEP 1 | 配置身份验证配置文件。无需在测试前提交身份验证配置文件或服务器配置文件配置。

STEP 2 | 登录至防火墙 CLI。

STEP 3 | （具有多个虚拟系统的防火墙）定义测试命令将访问的目标虚拟系统。

具有多个虚拟系统的防火墙需要此功能，以便测试身份验证命令可以找到要测试的用户。

通过输入以下命令定义目标虚拟系统：

```
admin@PA-325060> set system setting target-vsys <vsys-name>
```

例如，如果在 vsys2 中定义用户，请输入：

```
admin@PA-3250> set system setting target-vsys vsys2
```

***Target-vsys*** 选项基于登录会话，因此，防火墙在您退出后将清除该选项。

STEP 4 | 输入以下命令以测试身份验证配置文件：

```
admin@PA-3250> test authentication authentication-profile <authentication-
profile-name> 用户名 <username> 密码
```

例如，要为名为 **bsimpson** 的用户测试名为 **my-profile** 的身份验证配置文件，请输入：

```
admin@PA-3250> test authentication authentication-profile my-profile
 username bsimpson password
```

运行 ***test*** 命令时，身份验证配置文件和服务器配置文件的名称应区分大小写。此外，如果身份验证配置文件已经定义用户名修饰符，那么必须输入包含用户名的修饰符。例如，如果为名为 ***bsimpson*** 的用户添加用户名修饰符 ***%USERINPUT%@%USERDOMAIN%*** 并且域名是 ***mydomain.com***，则输入 ***bsimpson@mydomain.com*** 作为用户名。这样可以确保防火墙向身份验证服务器发送正确的凭据。在此示例中，*mydomain.com* 是您在身份验证配置文件的 *User Domain*（用户域）字段中定义的域。

STEP 5 | 查看测试输出。

如果正确配置了身份验证配置文件，则输出将显示 `Authentication succeeded`。如果存在配置问题，则输出显示的信息可帮助您排查配置问题。

根据正在使用的身份验证类型的多种相关因素以及问题类型，输出结果各有不同。例如，*RADIUS* 和 *TACACS+* 使用不同底层库，因此这两种类型存在的相同问题将产生不同错误。此外，如果存在网络问题（比如在身份验证服务器配置文件中使用了错误的端口或



© 2019 Palo Alto Networks, Inc.

*IP* 地址），则输出错误不具体。这是因为测试命令不能执行防火墙与身份验证服务器之间的初始握手来确定有关问题的详细信息。


© 2019 Palo Alto Networks, Inc.

# 身份验证策略

身份验证策略可让您在最终用户访问服务和应用程序之前验证他们的身份。每当用户请求服务或应用程序时（如访问网页时），防火墙都会评估身份验证策略。根据匹配身份验证策略规则，防火墙会提示用户使用登录和密码、语音、短信、推送或一次性密码 (OTP) 身份验证等一个或多个方法（因素）进行身份验证。对于第一个因素，用户通过身份验证门户 Web 表单进行身份验证。而对于任何其他因素，用户则通过多重因素身份验证 (MFA) 登录页面进行身份验证。



要实现 *GlobalProtect* 身份验证策略，请参阅配置 GlobalProtect 以加快多重因素身份验证通知。

在用户对所有因素进行身份验证后，防火墙会评估安全策略以确定是否允许访问服务或应用程序。

为了减少中断用户工作流的身份验证挑战的频率，您可以指定一个超时期限，在此期限内，用户仅对初次访问服务和应用程序进行身份验证，而不会对后续访问进行验证。身份验证策略与身份验证门户集成以记录用于评估超时的时间戳，并启用基于用户的策略和报告。

User-ID 会根据身份验证过程中防火墙收集到的用户信息来创建新的 IP 地址到用户名的映射，或在映射信息已更改后更新该用户的现有映射。防火墙生成 User-ID 日志以记录补充和更新。防火墙还会为与身份验证规则相匹配的每个请求生成身份验证日志。如果您喜欢集中式监控，则可以根据 User-ID 或身份验证日志配置报告，并将日志转发到 Panorama 或外部服务，就像其他日志类型一样。

- 身份验证时间戳
- 配置身份验证策略

## 身份验证时间戳

配置身份验证策略规则时，您可以指定一个超时期限，在此期限内，用户仅对初次访问服务和应用程序进行身份验证，而不会对后续访问进行验证。您的目标是指定一个超时时间，在保护服务和应用程序的需求以及最大限度减少用户工作流中断的需求之间达成平衡。用户进行身份验证时，防火墙会记录第一个身份验证挑战（因素）的时间戳和任何其他多重因素身份验证 (MFA) 因素的时间戳。当用户随后请求符合身份验证规则的服务和应用程序时，防火墙将对规则中指定的与每个时间戳相关的超时时间进行评估。也就是说，当超时到期时，防火墙会根据每个因素重新发布身份验证挑战。如果您重新分发用户映射和身份验证时间戳，所有防火墙将为所有用户强制执行一致的身份验证策略超时。



防火墙为每个 *MFA* 供应商记录一个单独的时间戳。例如，如果您使用 Duo v2 和 *PingID* 服务器来向 *MFA* 因素提出挑战，则防火墙会记录一个响应 *Duo* 因素的时间戳和一个响应 *PingID* 因素的时间戳。

在超时期限内，成功通过一个身份验证规则验证的用户可以访问受其他规则保护的服务或应用程序。但是，这种可移植性仅适用于触发相同身份验证因素的规则。例如，成功通过触发 TACACS+ 身份验证规则验证的用户，必须再次通过触发 SAML 身份验证规则的验证，即使访问请求均位于两个规则的超时期限内。

在评估每个身份验证规则的超时时间和身份验证门户设置中定义的全局计时器（请参阅配置身份验证门户）时，无论哪个时间先到，防火墙都会提示用户重新进行身份验证。重新进行身份验证时，防火墙会记录规则的新身份验证时间戳，并重新设置身份验证门户计时器的计时。因此，要为不同的身份验证规则启用不同的超时时间，请将身份验证门户计时器设置为与任何规则中的超时相同或更高的值。

## 配置身份验证策略

执行以下步骤，为通过身份验证门户访问服务的最终用户配置身份验证策略。在开始之前，请确保您的安全策略允许用户访问需要身份验证的服务和 URL 类别。



© 2019 Palo Alto Networks, Inc.

STEP 1 | 配置身份验证门户。如果您使用多重因素身份验证 (MFA) 服务对用户进行身份验证，则必须将 **Mode**（模式）设置为 **Redirect**（重定向）。

STEP 2 | 配置防火墙，使用以下一项服务对用户进行身份验证。

- 外部身份验证服务 — 配置服务器配置文件以定义防火墙与服务的连接方式。
- 本地数据库身份验证 — 将每个用户帐户添加到防火墙上的本地用户数据库。
- Kerberos 单点登录 (SSO) — 为防火墙创建 Kerberos 密钥表。或者，您可以将防火墙配置为使用 Kerberos SSO 作为主身份验证服务，并且如果 SSO 发生故障，则可以回退到外部服务或本地数据库身份验证。

STEP 3 | 为需要相同身份验证服务和设置的每组用户和身份验证策略规则配置身份验证配置文件和序列。

选择身份验证服务 **Type**（类型）和相关设置：

- 外部服务— 选择外部服务器 **Type**（类型），然后选择您为其创建的 **Server Profile**（服务器配置文件）。
- 本地数据库身份验证 — 将 **Type**（类型）设置为 **Local Database**（本地数据库）。在 **Advanced**（高级）设置中，**Add**（添加）您创建的身份验证门户用户和用户组。
- **Kerberos SSO** — 指定 **Kerberos Realm**（**Kerberos** 域）并 **Import**（导入）**Kerberos Keytab**（**Kerberos** 密钥表）。

STEP 4 | 配置身份验证执行对象。

该对象将每个身份验证配置文件与一个身份验证门户方法相关联。该方法确定第一个身份验证挑战（因素）是否透明，或是否需要用户响应。

1. 选择 **Objects**（对象）> **Authentication**（身份验证），并 **Add**（添加）对象。
2. 输入 **Name**（名称）以标识对象。
3. 为身份验证配置文件中指定的身份验证服务 **Type**（类型）选择 **Authentication Method**（身份验证方法）：
   - **Browser-challenge**（浏览器-质询）— 如果您希望客户端浏览器响应第一个身份验证因素，而不是让用户输入登录凭据，请选择此方法。对于此方法，必须在身份验证配置文件中配置 Kerberos SSO。如果浏览器质询失败，防火墙将回退到 **web-form**（**Web** 表单）方法。
   - **web-form**（**Web** 表单）— 如果您希望防火墙显示用户可输入登录凭据的身份验证门户 Web 表单，请选择此方法。
4. 选择您配置的 **Authentication Profile**（身份验证配置文件）。
5. 输入身份验证门户 Web 表单将显示的 **Message**（消息），告知用户如何验证第一个身份验证因素。
6. 单击 **OK**（确定）保存对象。

STEP 5 | 配置身份验证策略规则。

为需要相同身份验证服务和设置的每组用户、服务和 URL 类别创建规则。



如果您的身份验证策略使用默认身份验证实施对象（例如，*default-browser-challenge*），则防火墙不会应用身份验证门户超时。如果想要求用户在身份验证门户超时后重新进行身份验证，请克隆默认身份验证对象规则，并将该规则移到默认身份验证对象规则之前。

1. 选择 **Policies**（策略）> **Authentication**（身份验证），然后 **Add**（添加）规则。
2. 输入标识规则的 **Name**（名称）。
3. 选择 **Source**（源）并 **Add**（添加）特定区域和 IP 地址，或选择 **Any**（任何）区域或 IP 地址。

   该规则仅适用来自于指定 IP 地址或特定区域内接口的流量。


© 2019 Palo Alto Networks, Inc.

4. 选择 **User**（用户），然后选择或 **Add**（添加）规则所适用的源用户和用户组（默认为 **any**（任何））。
5. 选择或 **Add**（添加）规则所适用的主机信息配置文件（默认为 **any**（任何））。
6. 选择 **Destination**（目标）并 **Add**（添加）特定区域和 IP 地址，或选择 **Any**（任何）区域或 IP 地址。

   IP 地址可以是您要控制访问权限的资源（如服务器）。
7. 选择 **Service/URL Category**（服务/URL 类别），然后选择或 **Add**（添加）规则控制访问的服务和服务组（默认为 **service-http**）。
8. 选择或 **Add**（添加）规则控制访问的 URL 类别（默认为 **any**（任何））。例如，您可以创建一个自定义 URL 类别，指定最敏感的内部站点。
9. 选择 **Actions**（操作），然后选择您创建的 **Authentication Enforcement**（身份验证执行）对象。
10. 指定 **Timeout**（超时）期限（分钟）（默认为 60 分钟），在此期间，防火墙会提示用户仅对服务和应用程序的重复访问进行一次身份验证。

    *Timeout*（超时）是更严格的安全（身份验证提示之间的时间更短）和用户体验（身份验证提示之间的时间更长）之间的权衡。访问关键系统和敏感区域（例如数据中心）时，进行更频繁的身份验证通常是很正确的选择。在网络外围设备以及对于用户体验为核心的业务，进行更少的身份验证往往是比较正确的选择。
11. 单击 **OK**（确定）保存规则。

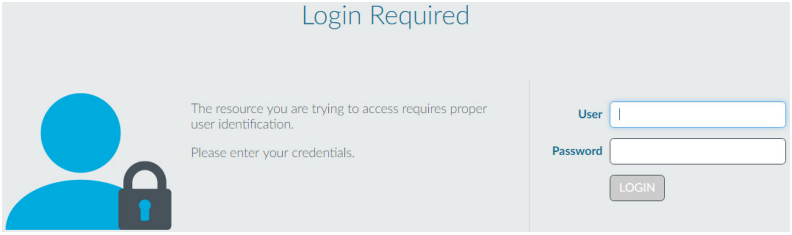
STEP 6 | （仅限 MFA）自定义 MFA 登录页面。

防火墙显示此页面，以便用户可以对任何其他 MFA 因素进行身份验证。

STEP 7 | 验证防火墙是否已执行身份验证策略。

1. 作为身份验证策略规则中指定的源用户之一登录到您的网络。
2. 请求与规则中指定的服务或 URL 类别匹配的服务或 URL 类别。

   防火墙显示第一个身份验证因素的身份验证门户 Web 表单。例如：




   如果您将防火墙配置为使用一个或多个 *MFA* 服务，请对其他身份验证因素进行身份验证。
3. 结束刚刚访问的服务或 URL 会话。
4. 为相同的服务或应用程序启动新的会话。确保在身份验证规则中配置的 **Timeout**（超时）期限内执行此步骤。

   防火墙允许访问无需重新进行身份验证。
5. 等待直到 **Timeout**（超时）期限到期，并请求相同的服务或应用程序。

   防火墙提示您重新进行身份验证。

STEP 8 | （可选）重新分发数据和身份验证时间戳到实施身份验证策略的其他防火墙，以确保对所有用户一致应用超时。


© 2019 Palo Alto Networks, Inc.

# 身份验证问题故障排除

当用户无法对 Palo Alto Networks 防火墙或 Panorama 进行身份验证，或身份验证流程所花时间长于预期时，对身份验证相关信息的分析能帮您确定失败或延时的原因：

- 用户行为 — 例如，在输入错误凭据或大量用户同时尝试访问之后锁定用户。
- 系统或网络问题 — 例如，身份验证服务器无法访问。
- 配置问题 — 例如，身份验证配置文件的允许列表未具备本应具有的所有用户。

以下 CLI 命令显示可帮助您对这些问题进行排查的信息：

| 任务 | 命令 |
| --- | --- |
| 显示与身份验证配置文件 (**auth-profile**)、身份验证序列 (**is-seq**) 或虚拟系统 (**vsys**)相关的锁定用户数。<br><br>要锁定用户，请使用以下操作指令：<br><br>**> request authentication [unlock-admin \| unlock-user]** | **PA-220> show authentication locked-users**<br>**{**<br>**vsys *<value>*** \|<br>auth-profile <value> \|<br>is-seq<br>{yes \| no}<br>{auth-profile \| vsys} <value><br>} |
| 使用 **debug authentication** 命令对身份验证事件进行故障排查。<br><br>使用 **show** 选项显示身份验证请求统计信息以及当前调试级别：<br>• **Show** 显示身份验证服务 (authd) 的当前调试级别。<br>• **Show-active-requests** 显示身份验证请求、允许列表、锁定的用户帐户以及多重因素身份验证 (MFA) 请求的活动检查次数。<br>• **Show-pending-requests** 显示身份验证请求、允许列表、锁定的用户帐户以及 MFA 请求的挂起检查次数。<br>• **Connection-show** 显示所有身份验证服务器或某个特定协议类型的身份验证请求和响应统计信息。<br><br>使用 **connection-debug** 选项来启用或禁用身份验证：<br>• 用 **on** 选项或 **off** 选项可启用或禁用 authd 的调试。<br>• 使用 **connection-debug-on** 选项或 **connection-debug-off** 选项可用启用或禁用所有身份验证服务器或某个特定协议类型的调试。 | **PA-220> debug authentication**<br>**{**<br>**on {debug \| dump \| error \| info \| warn} \|**<br>**show \|**<br>**show-active-requests \|**<br>**show-pending-requests \|**<br>**connection-show \|**<br>**{**<br>**connection-id \|**<br>**protocol-type**<br>**{**<br>**Kerberos connection-id *<value>*** \|<br>LDAP connection-id <value> \|<br>RADIUS connection-id <value> \|<br>TACACS+ connection-id <value> \|<br>}<br>connection-debug-on \|<br>{<br>connection-id \|<br>debug-prefix \|<br>protocol-type<br>{<br>Kerberos connection-id <value> \|<br>LDAP connection-id <value> \| |



© 2019 Palo Alto Networks, Inc.

| 任务 | 命令 |
| --- | --- |
| | RADIUS connection-id <value><br>\|<br>TACACS+ connection-id <value><br>\|<br>}<br>connection-debug-off \|<br>{<br>connection-id \|<br>protocol-type<br>{<br>Kerberos connection-id <value><br>\|<br>LDAP connection-id <value> \|<br>RADIUS connection-id <value><br>\|<br>TACACS+ connection-id <value><br>\|<br>}<br>connection-debug-on<br>} |
| 测试证书配置文件的连接和有效性。 | PA-220> test authentication<br>authentication-profile auth-profile<br>username *<username>*password *<password>* |
| 使用 **Monitor**（监控）> **Logs**（日志）> **Authentication**（身份验证）中显示的**Authentication ID**（身份验证 **ID**）对特定身份验证进行故障排除。 | PA-220> grep *<Authentication ID>* |

# 证书管理

以下主题介绍了 Palo Alto Networks® 防火墙和 Panorama 使用的不同密钥和证书，以及获取和管理它们的方法：


- 密钥和证书
- 默认可信证书颁发机构(CA)
- 证书撤消
- 证书部署
- 设置证书吊销状态验证
- 配置主密钥
- 主密钥加密
- 获取证书
- 导出证书和私钥
- 配置证书配置文件
- 配置 SSL/TLS 服务配置文件
- 配置 SSH 服务配置文件
- 入站流量管理之证书替换
- 配置 SSL 转发代理服务器证书的密钥大小
- 吊销和续订证书
- 安全密钥与硬件安全模块

# 密钥和证书

为了确保安全通信会话双方之间的信任，Palo Alto Networks 防火墙和 Panorama 会使用数字证书。每个证书都包含用来加密明文或解密密文的加密密钥。此外，每个证书还包括用来对颁发者的身份进行验证的数字签名。颁发者必须在验证方的受信任的证书颁发机构 (CA) 列表内。或者，验证方对颁发者的身份进行验证不会吊销证书（请参阅证书吊销）。

Palo Alto Networks 防火墙和 Panorama 会在以下应用程序中使用证书：

- 身份验证门户、多重因素身份验证 (MFA) 以及防火墙或 Panorama Web 界面访问的用户身份验证。
- Device authentication for GlobalProtect VPN（远程用户到端点或大规模部署）。
- Device authentication for IPSec 站点到站点 VPN 和互联网Key Exchange (IKE)。
- 外部动态列表 (EDL) 验证。
- User-ID 代理和 TS 代理访问。
- 解密入站和出站 SSL 流量。

  防火墙对流量进行解密，以应用策略和规则，然后在将流量转发到最终目的地之前再对其进行重新加密。对于出站流量，防火墙作为转发代理服务器，建立与目标服务器的 SSL/TLS 连接。为了确保自身和客户端之间的连接，防火墙使用签名证书自动生成目标服务器证书的副本。

下表介绍了 Palo Alto Networks 防火墙和 Panorama 使用的密钥和证书。作为最佳实践，可以对每一种用途使用不同的密钥和证书。

**表 1: Palo Alto Networks 设备密钥/证书**

| 密钥/证书用途 | 说明 |
|---|---|
| 管理访问 | 安全访问防火墙和 Panorama 管理界面（HTTPS 访问 Web 界面）需要适用于 MGT 接口（或数据平面上的指定接口，如果设备不使用 MGT 接口）的服务器证书，以及用来对管理员身份进行验证的证书（可选）。 |
| 身份验证门户 | 在身份验证策略标识访问 HTTPS 资源的用户的部署中，应为身份验证门户接口指定服务器证书。如果您将身份验证门户配置为使用证书标识用户（而不是交互式身份验证或除交互式身份验证外），也应部署客户端证书。有关身份验证门户的更多信息，请参阅使用身份验证门户将 IP 地址映射到用户名。 |
| 转发信任 | 对于出站 SSL/TLS 流量，如果将防火墙用作转发代理信任对目标服务器的证书进行签名的 CA，则防火墙使用转发信任 CA 证书生成目标服务器证书的副本，以提交给客户端。要设置私钥大小，请参阅配置 SSL 转发代理服务器证书的密钥大小。为了增加安全性，应将密钥存储在硬件安全模块（有关详细信息，请参阅安全密钥与硬件安全模块）。 |
| 转发不可信 | 对于出站 SSL/TLS 流量，如果将防火墙用作转发代理不信任对目标服务器的证书进行签名的 CA，则防火墙使用转发不信任 CA 证书生成目标服务器证书的副本，以提交给客户端。 |
| SSL 入站检查 | 密钥用于解密检查和策略执行的入站 SSL/TLS 流量。对于此应用程序，将导入防火墙的私钥用于每台服务器以符合 SSL/TLS 入站检查。请参阅配置 SSL 入站检查。<br><br>从 *PAN-OS 8.0* 开始，防火墙将使用椭圆曲线 *Diffie-Hellman Exchange (ECDHE)* 算法执行严格的证书检查。这意味着，如果防火墙使用中间证书，您必须在更新到 *PAN-OS 8.0* 或更高版本之后将证书从 *Web* 服务器重新导入到防火墙，并将服务器证书与中间证 |



© 2019 Palo Alto Networks, Inc.

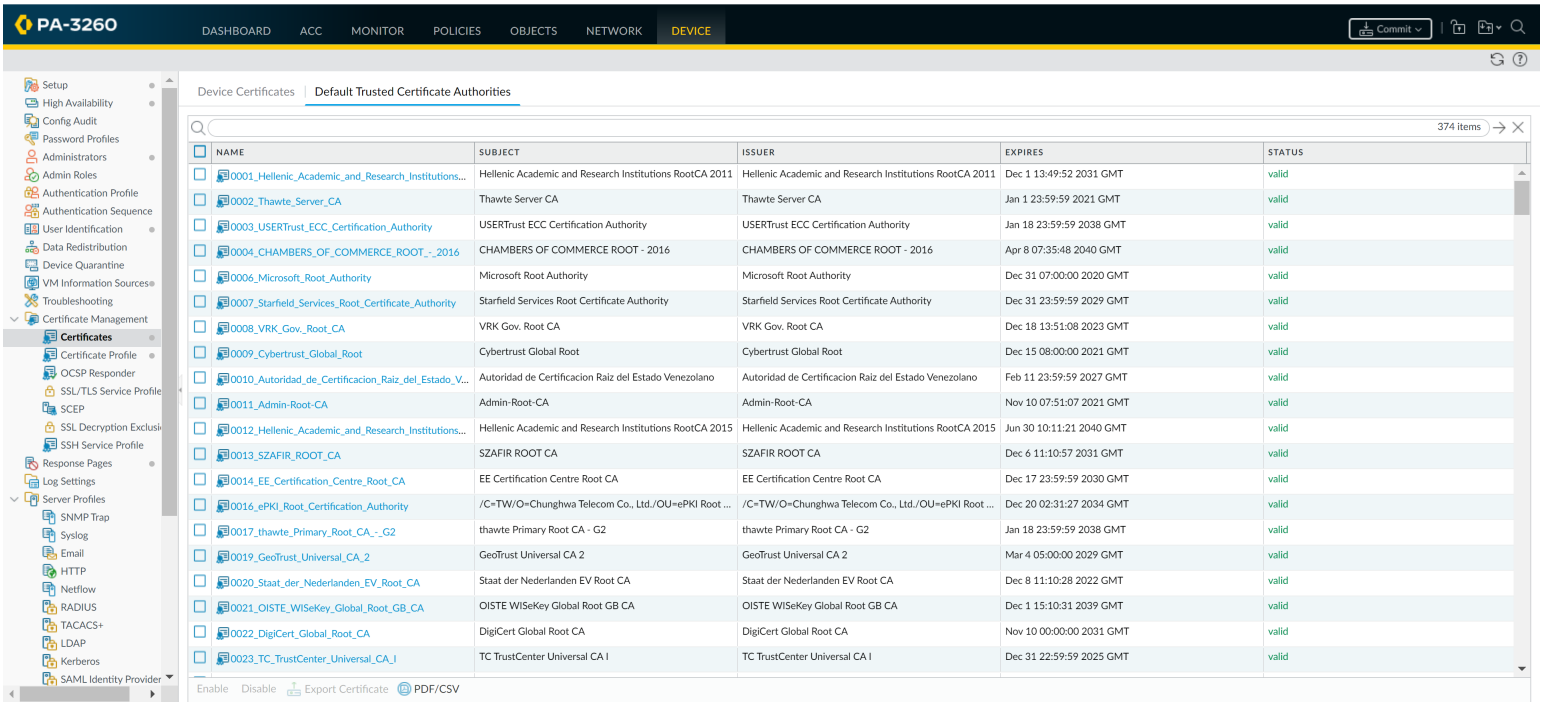
| 密钥/证书用途 | 说明 |
| --- | --- |
| | 书相结合（安装链式证书）。否则，链中拥有中间证书的 *SSL* 入站检查会话将失败。要安装链式证书：<br>1. 在文本编辑器（如记事本）中打开每个证书 *(.cer)* 文件。<br>2. 端到端地粘贴每个证书，服务器证书在上，下面包含每个签名者。<br>3. 将文件另存为文本 *(.txt)* 或证书 *(.cer)* 文件（文件名不能包含空格）。<br>4. 将组合（链式）证书导入到防火墙。 |
| SSL 排除证书 | 服务器排除 SSL/TLS 解密的证书。例如，如果您启用 SSL 解密，但网络包括防火墙不应为其解密流量的服务器（如人力资源系统的 Web 服务），可以将相应的证书导入防火墙并将它们配置为 SSL 排除证书。请参阅解密排除。 |
| GlobalProtect | GlobalProtect 组件之间的所有交互均通过 SSL/TLS 连接实现。因此，作为 GlobalProtect 部署的一部分，都会为所有 GlobalProtect 门户、网关和 Mobile Security Manager 部署服务器证书。（可选）同样也为身份验证用户部署证书。<br>*GlobalProtect 大规模 VPN (LSVPN) 功能需要 CA 签名证书。* |
| 站点到站点 VPN (IKE) | 在站点到站点 IPSec VPN 部署中，对等设备使用互联网Key Exchange (IKE) 网关建立安全通道。IKE 网关使用证书或预共享密钥对对等设备进行相互验证。您可以在防火墙上定义 IKE 网关时配置和指定证书或密钥。请参阅站点到站点 VPN 概述。 |
| 主密钥 | 防火墙使用主密钥来对所有私钥和密码进行加密。如果网络需要存储私钥的安全位置，可以使用存储在硬件安全模块 (HSM) 上的加密（包装）密钥对主密钥进行加密。有关详细信息，请参阅使用 HSM 加密主密钥。 |
| 安全系统日志 | 用于在防火墙和系统日志服务器之间建立安全连接的证书。请参阅自定义 Syslog 字段说明。 |
| 可信的根 CA | 指定防火墙信任的 CA 签发的根证书。防火墙可以使用自签名的根 CA 证书自动为其他应用程序签发证书（如 SSL 转发代理）。<br>此外，如果防火墙必须与其他防火墙建立安全连接，则为其签发证书的根 CA 必须在防火墙上受信任的根 CA 列表中。 |
| 设备间通信 | 默认情况下，Panorama、防火墙和日志收集器使用一组用于管理和日志转发的 SSL/TLS 连接的预定义证书。但是，您可以通过将自定义证书部署到部署中的设备来增强这些连接。这些证书也可用于保护 Panorama HA 对端设备之间的 SSL/TLS 连接。 |


© 2019 Palo Alto Networks, Inc.

# 默认可信证书颁发机构(CA)

默认情况下，防火墙信任最常见且最受信任的颁发机构 (CA)。这些受信证书提供程序负责发布防火墙安全连接至 internet 所需的证书。

若要查看并管理防火墙默认可信的 CA 列表，请选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Default Trusted Certificate Authorities**（默认可信证书颁发机构）：




您可以想要添加的唯一其他 CA 就是您组织所需的可信企业 CA —— 请参阅获取证书。



© 2019 Palo Alto Networks, Inc.

# 证书撤消

Palo Alto Networks 防火墙和 Panorama 使用数字证书确保安全通信会话双方之间的信任。为了增加安全性，可以配置防火墙或 Panorama 检查证书的吊销状态。提供已吊销证书的一方不值得信任。如果证书是关系链的一部分，则防火墙或 Panorama 会检查关系链中每个证书的状态，除了设备无法验证吊销状态的根 CA 证书。

有多种不同情况可能会使得证书在到期之前变成无效。例如，更改证书名称、更改主体和证书颁发机构之间的关联（如员工终止雇用）及泄露（已知或可疑）私钥。在这些情况下，签发证书的证书颁发机构必须吊销证书。

Palo Alto Networks 防火墙和 Panorama 支持使用以下两种方法来验证证书吊销状态。如果同时配置这两种方法，则防火墙和 Panorama 首先尝试使用 OCSP 方法；如果 OCSP 服务器不可用，设备使用 CRL 方法。

- 证书吊销列表 (CRL)
- 在线证书状态协议 (OCSP)

在 *PAN-OS* 中，证书吊销状态验证是一项可选功能。最佳实践是为证书配置文件启用该功能，用于为身份验证门户、*GlobalProtect*、站点到站点 *IPsec VPN* 和防火墙或 *Panorama Web* 界面访问定义用户和设备身份验证，以确认该证书尚未被撤销。

## 证书吊销列表 (CRL)

每个证书颁发机构 (CA) 会定期向公共储存库签发证书吊销列表 (CRL)。CRL 按序列号标识已吊销的证书。在 CA 吊销证书后，下一个 CRL 更新将包括该证书的序列号。

Palo Alto Networks 防火墙下载和缓存在防火墙的受信任 CA 列表中列出的每个 CA 最后签发的 CRL。缓存仅适用于已验证的证书；如果防火墙从未验证证书，则防火墙缓存不会存储签发 CA 的 CRL。此外，缓存仅存储 CRL，直到它过期。

该防火墙仅支持卓越编码规则 (DER) 格式的 CRL。如果该防火墙下载其他格式的 CRL（例如，增强的私人邮件 (PEM) 格式），则当用户执行触发该过程的活动时（例如，发送出站 SSL 数据），使用该 CRL 的任何撤消验证过程将会失败。该防火墙将生成验证失败的系统日志。如果是验证 SSL 证书，该防火墙也会向用户显示 SSL 证书错误通知响应页面。

如果您配置多个 *CRL* 分配点 *(CDP)* 且防火墙无法访问第一个 *CDP*，防火墙将无法检查剩余的 *CDP*。要重定向无效的 *CRL* 请求，可配置 DNS 代理作为备用服务器。

要使用 CRL 验证用于解密入站和出站 SSL/TLS 流量的证书的撤消状态，请参阅配置用于 SSL/TLS 解密的证书吊销状态验证。

要使用 CRL 验证用来对用户和设备进行验证的证书的吊销状态，可配置证书配置文件并将其分配给以下应用程序专用的接口：身份验证门户、GlobalProtect（远程用户到站点或大规模）、站点到站点 IPSec VPN 或 Palo Alto Network 防火墙或 Panorama Web 界面访问。有关详细信息，请参阅配置证书吊销状态验证。

## 在线证书状态协议 (OCSP)

当建立 SSL/TLS 会话后，客户端可以使用在线证书状态协议 (OCSP) 检查身份验证证书的吊销状态。验证客户端向 OCSP 响应者（服务器）发送包含证书序列号的请求。响应者搜索签发证书的证书颁发机构 (CA) 的数据库，并向客户端返回包含不同状态（良好、已吊销或未知）的响应。OCSP 方法的好处是它可以实时验证状态，而不是取决于 CRL 的签发频率（每小时、每天或每周）。

Palo Alto Networks 防火墙下载和缓存在防火墙的受信任 CA 列表中列出的每个 CA 的 OCSP 状态信息。缓存仅适用于已验证的证书；如果防火墙从未验证证书，则防火墙缓存不会存储签发 CA 的 OCSP 信息。如果企业拥有自己的公钥基础设施 (PKI)，则可以将防火墙配置为 OCSP 响应者（请参阅配置 OCSP 响应者）。


© 2019 Palo Alto Networks, Inc.

要在将防火墙用作 SSL 转发代理时使用 OCSP 验证证书的吊销状态，请执行配置用于 SSL/TLS 解密的证书吊销状态验证下的步骤。

以下应用程序使用证书对用户和/设备进行身份验证：身份验证门户、GlobalProtect（远程用户到站点或大规模）、站点到站点 IPSec VPN 以及 Palo Alto Network 防火墙或 Panorama Web 界面访问。要使用 OCSP 验证证书的吊销状态：

- 配置 OSCP 响应者（如果正在将防火墙配置为 OCSP 响应者）。
- 启用防火墙上的 HTTP OSCP 服务（如果正在将防火墙配置为 OCSP 响应者）。
- 创建或获取每个应用程序的证书。
- 配置每个应用程序的证书配置文件。
- 将证书配置文件分配给相关应用程序。

要涵盖 OCSP 响应者不可用的情况，可以配置 CRL 作为回顾方法。有关详细信息，请参阅配置证书吊销状态验证。



© 2019 Palo Alto Networks, Inc.

# 证书部署

Palo Alto Networks 防火墙或 Panorama 的基本部署方法包括：

- 从受信任的第三方 **CA** 获取证书 — 从受信任的第三方证书颁发机构 (CA)（如 VeriSign 或 GoDaddy）获取证书的好处是终端客户端已经信任该证书，因为常见浏览器在其受信任的根证书存储库中已包括著名 CA 的根 CA 证书。因此，对于需要终端客户端与 Palo Alto Network 防火墙或 Panorama 建立安全连接的应用程序，可以从终端客户端信任的 CA 购买证书，以避免将根 CA 证书预先部署到终端客户端。（此类应用程序包括 GlobalProtect 门户或 GlobalProtect Mobile Security Manager。）但是，大多数第三方 CA 不能签发签名证书。因此，这种类型的证书不适用于需要防火墙签发证书的应用程序（如 SSL/TLS 解密和大规模 VPN）。请参阅从外部 CA 获取证书。
- 从企业 **CA** 获取证书 — 拥有自己内部 CA 的企业可以用它来为防火墙应用程序签发证书，并将这些证书导入防火墙。好处是终端客户端可能已经信任企业 CA。您可以生成所需的证书并将它们导入防火墙，或者在防火墙上生成证书签名请求 (CSR) 并将该请求发送给企业 CA 进行签名。这种方法的好处是私钥不会离开防火墙。此外，企业 CA 也可以签发防火墙用来自动生成证书的签名证书（例如，用于 GlobalProtect 大规模 VPN 或需要 SSL/TLS 解密的站点）。请参阅导入证书和私钥。
- 生成自签名证书 — 您可以在防火墙上创建自签名根 CA 证书，并使用它来自动为其他防火墙应用程序签发证书。



如果使用此方法为需要终端客户端信任证书的应用程序生成证书，最终用户将会看到一个证书错误，因为根 *CA* 证书不在其受信任的根证书存储库中。要防止出现此错误，应将自签名根 *CA* 证书部署到所有最终用户系统。可以手动或使用集中式部署方法部署证书，如 *Active Directory* 组策略对象 *(GPO)*。



© 2019 Palo Alto Networks, Inc.

# 设置证书吊销状态验证

要验证证书吊销状态，防火墙可使用在线证书状态协议 (OCSP) 和/或证书吊销列表 (CRL)。有关这些方法的详细信息，请参阅证书吊销。如果同时配置这两种方法，则防火墙首先尝试使用 OCSP，并且只有在 OCSP 响应者不可用时返回来使用 CRL 方法。如果企业拥有自己的公钥基础设施 (PKI)，则可以将防火墙配置作为 OCSP 响应者。

以下主题介绍了配置防火墙验证证书吊销状态的方法：

- 配置 OCSP 响应者
- 配置证书吊销状态验证
- 配置用于 SSL/TLS 解密的证书吊销状态验证

## 配置 OCSP 响应者

要使用在线证书状态协议 (OCSP) 验证证书吊销状态，必须配置防火墙访问 OCSP 响应者（服务器）。管理 OCSP 响应者的实体可以是第三方证书颁发机构 (CA)。如果企业拥有自己的公钥基础设施 (PKI)，则可以使用外部 OCSP 响应者，或将防火墙配置为 OCSP 响应者。有关 OCSP 的详细信息，请参阅证书吊销。

STEP 1 | 定义外部 OCSP 响应者或将防火墙配置为 OCSP 响应者。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **OCSP Responder**（**OCSP** 响应者），然后单击 **Add**（添加）。
2. 输入 **Name**（名称）以标识响应者（最多 31 个字符）。名称区分大小写。它必须是唯一且只能使用字母、数字、空格、连字符和下划线。
3. 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。
4. 在 **Host Name**（主机名）字段中，输入主机名（建议）或 OCSP 响应者的 IP 地址。您可以输入 IPv4 或 IPv6 地址。根据此值，PAN-OS 自动派生一个 URL，并将其添加到正在验证的证书。

   如果将防火墙本身配置作为 OCSP 响应者，则主机名必须在防火墙用于 OCSP 服务的接口中解析 IP 地址。
5. 单击 **OK**（确定）。

STEP 2 | 如果想要防火墙使用管理接口作为 OCSP 响应者接口，请启用防火墙上的 OCSP 通信。否则，继续执行下一步以配置备用接口。

1. 选择**Device**（设备）> **Setup**（设置）> **Management**（管理）。
2. 在“管理接口设置”部分中，编辑以选中 **HTTP OCSP** 复选框，然后单击 **OK**（确定）。

STEP 3 | 要使用备用接口作为 OCSP 响应者接口，可将接口管理配置文件添加到 OCSP 服务使用的接口。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理）。
2. 单击 **Add**（添加）以创建新的配置文件，或单击现有配置文件的名称。
3. 选中 **HTTP OCSP** 复选框，然后单击 **OK**（确定）。
4. 选择 **Network**（网络）> **Interfaces**（接口），然后单击防火墙将用于 OCSP 服务的接口的名称。在步骤 1 中指定的 OCSP **Host Name**（主机名）必须在此接口中解析 IP 地址。
5. 选择 **Advanced**（高级）> **Other info**（其他信息），然后选择配置的“接口管理配置文件”。
6. 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 配置证书吊销状态验证

防火墙和 Panorama 使用证书来对某些应用程序的用户和设备进行身份验证，如身份验证门户、GlobalProtect、站点到站点 IPSec VPN 和防火墙/Panorama Web 界面访问。为了提高安全性，最佳实践是配置防火墙或 Panorama 验证用于设备/用户身份验证的证书的吊销状态。

STEP 1 | 为每个应用程序配置证书配置文件。

为配置文件指定一个或多个根 CA 证书，并选择防火墙验证证书吊销状态的方法。

有关不同应用程序使用证书的详细信息，请参阅密钥和证书。

STEP 2 | 将证书配置文件分配给相关应用程序。

分配证书配置文件的步骤，取决于需要证书配置文件的应用程序。

# 配置用于 SSL/TLS 解密的证书吊销状态验证

防火墙将解密入站和出站 SSL/TLS 流量，以检测流量中的威胁。在创建允许流量的安全策略规则，并将安全配置文件应用至规则时，请创建一个模拟解密策略规则以解密该流量。如果不解密该流量，防火墙将无法使用安全配置文件检测流量（您将无法监测您看不见的内容）。防火墙会先转发流量，然后对其进行重新加密。（请参阅 SSL 入站检查和 SSL 转发代理。）您可以按照如下所示步骤配置防火墙以验证用于解密的证书的吊销状态。

启用 *SSL/TLS* 解密证书的吊销状态验证将会增加建立会话过程的时间。如果在会话超时之前验证无法完成。则第一次尝试访问站点可能会失败。由于这些原因，默认禁用验证。

STEP 1 | 定义吊销状态请求的特定服务超时间隔。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后在“会话功能”部分中选择 **Decryption Certificate Revocation Settings**（解密证书吊销设置）。
2. 执行下述一个或两个步骤，具体取决于防火墙将使用在线证书状态协议 (OCSP) 还是证书吊销列表 (CRL) 方法验证证书吊销状态。如果防火墙同时使用两种方法，则它首先会尝试使用 OCSP；如果 OCSP 响应者不可用，则防火墙尝试使用 CRL 方法。
   - 在 CRL 部分中，选中 **Enable**（启用）复选框，然后输入 **Receive Timeout**（接收超时）。这是防火墙在过后停止等待 CRL 服务响应的时间间隔（1 至 60 秒）。
   - 在 OCSP 部分中，选中 **Enable**（启用）复选框，然后输入 **Receive Timeout**（接收超时）。这是防火墙在过后停止等待 OCSP 响应者响应的时间间隔（1 至 60 秒）。

   根据在步骤 2 中指定的 **Certificate Status Timeout**（证书状态超时）值，防火墙可能会在一个或两个 **Receive Timeout**（接收超时）间隔过去之前注册一个超时。

STEP 2 | 定义吊销状态请求的总超时间隔。

输入 **Certificate Status Timeout**（证书状态超时）。这是防火墙在停止等待任何证书状态服务响应并应用在步骤 3 中选择性定义的会话阻止逻辑的时间间隔（1 至 60 秒）。将 **Certificate Status Timeout**（证书状态超时）与 OCSP/CRL **Receive Timeout**（接收超时）进行关联，如下所示：

- 如果同时启用 OCSP 和 CRL — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或两个 **Receive Timeout**（接收超时）值的总和。
- 如果只启用 OCSP — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或 OCSP **Receive Timeout**（接收超时）值。
- 如果只启用 CRL — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或 CRL **Receive Timeout**（接收超时）值。

STEP 3 | 定义未知证书状态的阻塞行为或吊销状态请求超时。



© 2019 Palo Alto Networks, Inc.

如果您希望防火墙在 OCSP 或 CRL 服务返回未知证书吊销状态时阻塞 SSL/TLS 会话，请选中 **Block Session With Unknown Certificate Status**（如果证书状态未知，则阻止会话）复选框。否则，防火墙会继续进行会话。

如果您希望防火墙在注册请求超时后阻塞 SSL/TLS 会话，请选中 **Block Session On Certificate Status Check Timeout**（如果证书状态检查超时，则阻止会话）复选框。否则，防火墙会继续进行会话。

STEP 4 | 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 配置主密钥

每个防火墙和 Panorama 管理服务器都有一个默认主密钥，用于加密配置中的所有私钥和密码以进行保护（例如用于 SSL 转发代理解密的私钥）。



尽快更改默认主密钥，确保加密时使用的主密钥是唯一的。

在高可用性 (HA) 配置内，必须在对中的防火墙或 Panorama 上使用相同的主密钥。否则，HA 同步将无法正常工作。

另外，如果使用 Panorama 来管理防火墙，则必须在 Panorama 和所有受管防火墙上使用相同的主密钥，以便 Panorama 可以将配置推送到防火墙。

一定要将主密钥存储于安全位置。您无法恢复主密钥，恢复默认主密钥的唯一方法是将防火墙重置为出厂默认设置。

STEP 1 | 备份配置。

STEP 2 | （仅限 HA）禁用 HA。

在您部署新的主密钥至防火墙 HA 对前，需要执行此步骤。如果您在部署新的主密钥前未禁用 HA，Panorama 将失去与主要防火墙的连接。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑 Setup（设置）。
2. 禁用（取消选择）**Enable Ha**（启用 **HA**）设置，然后单击 **OK**（确定）。
3. **Commit**（提交）配置更改。

STEP 3 | 选择 **Device**（设备）> **Master Key and Diagnostics**（主密钥和诊断），然后编辑主密钥部分。

STEP 4 | 输入 **Current Master Key**（当前主密钥）（如果存在）。

STEP 5 | 定义新的 **New Master Key**（新主密钥），然后 **Confirm New Master Key**（确认新主密钥）。密钥必须只能包含 16 个字符。

STEP 6 | 要指定主密钥 **Lifetime**（生命周期），输入密钥在过后到期的 **Days**（天）数和/或 **Hours**（小时）数。

您必须在当前密钥过期之前配置新主密钥。如果主密钥过期，防火墙或 Panorama 在维护模式下自动重新启动。然后必须将防火墙重置为出厂默认设置。



根据设备执行加密的个数，将 *Lifetime*（生命周期）设为两年或更短。设备执行的加密次数越多，则应设置更短的生命周期。关键的考虑因素在于唯一性加密次数不会在更改主密钥之前用完。根据主密钥值和初始化向量 *(IV)* 值，每个主密钥最多可提供 $2^{32}$ 次唯一性加密。$2^{32}$ 次唯一性加密用完后，可重复加密（但不再是唯一的），这存在安全风险。

设置主密钥 *Time for Reminder*（提醒时间）值，并在出现提醒通知后，更改主密钥。

STEP 7 | 输入 **Time for Reminder**（提醒时间），指定在防火墙生成过期警报时主密钥过期之前的 **Days**（天）数和 **Hours**（小时）数。防火墙自动打开系统警报对话框以显示警报。



设置提醒，这样，在安排的维护时间窗口中提醒时间过期之前，您就有充足的时间配置新的主密钥。一旦达到提醒时间且防火墙或 *Panorama* 发送了通知日志，就立即更改主密



© 2019 Palo Alto Networks, Inc.

钥，不要等到生命周期过期。对于已分组设备，跟踪每个设备（例如，*Panorama* 管理的防火墙以及防火墙 *HA* 对），并在组内任何设备达到提醒时间时，更改主密钥。

要确保显示过期警报，请选择 *Device*（设备）> *Log Settings*（日志设置），然后编辑警报设置并 *Enable Alarms*（启用警报）。

STEP 8 | 启用 **Auto Renew Master Key**（自动更新主密钥）以配置防火墙自动更新主密钥。要配置 **Auto Renew With Same Master Key**（通过相同主密钥自动更新），指定 **Days**（天）和/或 **Hours**（小时）数以更新相同的主密钥。密钥扩展允许防火墙保留功能，并继续保护您的网络；如果现有主密钥生命周期即将结束，此方法不能作为配置新密钥的代替手段。

自动续订主密钥既存在好处，也存在风险。好处在于通过延长主密钥生命周期，可防止主密钥在该生命周期到期前更改失败。风险在于一旦设备通过主密钥执行的加密数超过主密钥可以生成的唯一性加密次数（$2^{32}$ 次唯一性加密），加密就会重复，并产生安全风险。

如果主密钥到期（您没有自动进行续订且没有及时更换），设备将进入维护模式。

如果启用 *Auto Renew Master Key*（自动续订主密钥），请进行设置，确保总时间（生命周期 + 自动续订时间）不会使设备用完唯一加密。例如，如果您认为设备将在两年半的时间内用完主密钥的唯一性加密次数，您可以将生命周期设为两年，将提醒时间设为 *60* 天，将自动续订主密钥设为 *60-90* 天，这样，您可以在生命周期到期前有额外的时间配置新的主密钥。但是，最佳做法仍是在生命周期到期前更改主密钥，确保设备不会重复使用加密。

在密钥生命周期结束后，配置主密钥以自动更新时，应考虑下次可用维护窗口之前的天数。

STEP 9 | （可选）为了增加安全，选择是否使用 **HSM** 对主密钥进行加密。有关详细信息，请参阅使用 HSM 加密主密钥。

STEP 10 | 单击 **OK**（确定）和 **Commit**（提交）。

STEP 11 | （仅限 HA）再次启用 HA。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑 Setup（设置）。
2. 选择 **Enable Ha**（启用 **HA**），并单击 **OK**（确定）。
3. **Commit**（提交）配置更改。



© 2019 Palo Alto Networks, Inc.

# 主密钥加密

在 Palo Alto Networks 物理和虚拟设备上，您可以配置主密钥以使用（PAN-OS 10.0 中引入的）AES-256-CBC 或 AES-256-GCM 加密算法，从而加密密钥和密码等数据。AES-256-GCM 提供的加密能力比 AES-256-CBC 更强，可提高您的安全状态。其还包括一项内置的完整性检查。主密钥使用配置的加密算法对存储在防火墙和 Panorama 上的敏感数据进行加密。如果使用的加密算法是 AES-256-GCM，您仍可以通过存储在 HSM上的加密密钥，使用 HSM 加密主密钥。

主密钥用于加密数据的默认加密算法是 AES-256-CBC —与主密钥在 PAN-OS 10.0 之前使用的算法相同。AES-256-CBC 是默认加密级别，因为当您使用 Panorama 管理防火墙时，受管防火墙可能位于不同的 PAN-OS 版本上，位于低于 PAN-OS 10.0 版本的 PAN-OS 上的防火墙不支持 AES-256-GCM。因此 Panorama 使用的加密级别必须低于受管设备使用的加密级别。例如，如果一些受管设备使用 PAN-OS 10.0，一些受管设备使用更低版本，则 Panorama 必须使用 AES-256-CBC。但是，如果所有受管设备均运行 PAN-OS 10.0 或更高版本，则 Panorama 及其所有受管设备都可以使用 AES-256-GCM。

在 *Panorama* 及其防火墙上使用相同的加密级别，并在防火墙对上使用相同的加密级别。升级设备以使用最强加密算法。如果 *Panorama* 管理的所有设备均运行 *PAN-OS 10.0*，则在所有设备上都使用 *AES-256-GCM*。使用不同加密级别的受管设备或配对设备的配置可能会不同步。

一旦将加密算法更改为 AES-256-GCM，设备将使用 AES-256-GCM（而不是 AES-256-CBC）来加密敏感数据。从一种算法更改为另一种算法后，您还可以指定是否要：

- 使用新算法重新加密现有加密数据。
- 保留使用旧加密算法加密的现有数据，仅将新算法用于新的（未来）加密。

默认情况下，一旦更改加密算法，设备将使用新算法重新加密现有加密数据，并加密新数据。如果使用 *Panorama* 管理设备，这些设备可能位于不同版本的 *PAN-OS* 上，可能不支持最新加密算法。在更改加密算法或重新加密已被加密的数据之前，请确保您已知悉 *Panorama* 及其受管设备支持的加密算法。

- 配置主密钥加密级别
- 防火墙 HA 对上主密钥加密
- 主密钥加密日志
- AES-256-GCM 唯一主密钥加密

## 配置主密钥加密级别

您可以配置主密钥加密算法级别，以及是否需要使用 CLI，以新的加密算法级别重新加密当前的所有已加密数据。您可以根据关键字顺序更改加密级别，或是您可以更改加密级别并指定是否需要对之前加密的数据重新加密。

通过以下可操作的 CLI 命令，您可以更改加密级别，并以指定的加密级别自动重新加密当前的所有已加密数据：

```
admin@PA-NGFW>request encryption-level level <0|1|2>
```

通过以下可操作的 CLI 命令，您可以更改加密级别，并指定是否需要以新的加密级别重新加密当前的所有已加密数据：

```
admin@PA-NGFW>request encryption-level re-encrypt <yes|no> level <0|1|2>
```


© 2019 Palo Alto Networks, Inc.

| 关键字 | 选项 |
| --- | --- |
| 级别 | **0** = 使用默认算法 (AES-256-CBC) 加密数据<br>**1** = 使用 AES-256-CBC 算法加密数据<br>**2** = 使用 AES-256-GCM 算法加密数据<br>防火墙使用指定算法重新加密当前的所有已加密数据，并加密新的敏感数据。如果不想使用新算法重新加密当前加密数据，请在命令字符串中指定**re-encrypt no**。这一操作可阻止防火墙自动加密防火墙已经加密的数据。<br>仅在 *Panorama* 和所有受管设备（或 *HA* 对中的两个设备）运行 *PAN-OS 10.0* 或更高版本时使用 *AES-256-GCM*，并配置所有设备使用 *AES-256-GCM*。使用不同加密级别的受管设备或配对设备可能无法同步。 |
| re-encrypt | **no** = 不重新加密当前已加密的数据。防火墙不会重新加密当前已加密的数据。当前已加密的数据仍使用防火墙最初用于加密数据的算法进行加密。防火墙仅在未来将指定算法用于加密敏感数据。<br>**yes** = 采用指定算法重新加密当前已加密的数据，并在将来使用此算法加密敏感数据。 |

使用可操作的 CLI 命令 **show system masterkey-properties** 确认设备当前所配置的加密算法（级别），例如：

```
admin@PA-NGFW>show system masterkey-properties
```

```
Master key expires at: unspecified
Reminders will begin at: unspecified
Master key on hsm: no
Automatically renew master key lifetime: 0
Encryption Level: 1
```

输出显示当前加密级别为 1，即 AES-256-CBC。

如果降级到更早版本的 PAN-OS，设备会自动将加密算法还原到降级的 PAN-OS 版本支持的级别，并自动以此级别重新加密已加密的数据，确保设备可以根据需要解密和使用这些数据。例如，如果设备运行 PAN-OS 10.0 并使用 AES-256-GCM 作为解密算法（更早版本的 PAN-OS 不支持此算法），且您降级到 PAN-OS 9.1，则设备将使用 PAN-OS 9.1 支持的 AES-256-CBC 算法重新加密已加密的数据。

## 防火墙 HA 对上主密钥加密

若要在防火墙高可用性 (HA) 对上使用加密级别 AES-256-GCM，两个防火墙均必须运行 PAN-OS 10.0，确保两个防火墙都可以支持 AES-256-GCM。如果 HA 对中有一个防火墙运行的版本低于 PAN-OS 10.0，则无法使用 AES-256-GCM。一旦两个防火墙都使用 PAN-OS 10.0，两个防火墙都可以解码 AES-256-CBC 或 AES-256-GCM 加密密钥，确保他们都可以使用这两个加密级别。但是，两个防火墙应使用相同的加密级别，以避免出现不同步。



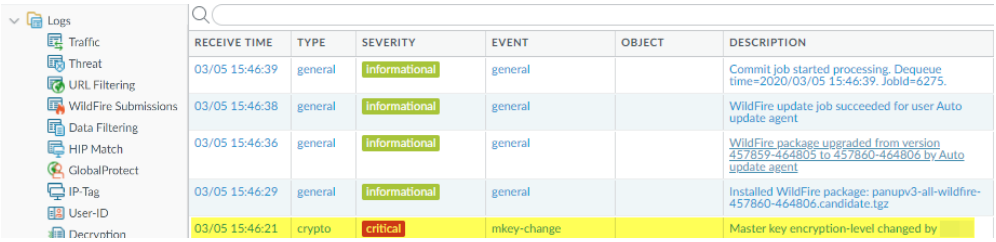
© 2019 Palo Alto Networks, Inc.

在 *HA* 对中两个防火墙上使用 *AES-256-GCM* 加密算法。无论是使用 *AES-256-GCM* 还是 *AES-256-CBC*，应在两个防火墙上使用相同的算法。

您无需禁用 HA 以更改其中两个防火墙都运行 PAN-OS 10.0 的 HA 对中的防火墙的加密级别。

## 主密钥加密日志

防火墙在更改主密钥加密算法（级别）时生成系统日志（**Monitor**（监控）> **Logs**（日志）> **System**（系统））。




若要查看主密钥加密的所有系统日志，请创建一个显示 **Type**（类型）为 crypto: **(subtype eq crypto)** 的所有日志的筛选器。

## AES-256-GCM 唯一主密钥加密

主密钥在用完唯一组合并必须重复加密之前，只能生成一定数量的唯一密钥。防火墙使用带初始化向量 (IV) 的 AES-256-GCM 加密算法创建唯一加密。IV 是随意指定的一个数字，只能在创建加密时使用一次，这样，才能确保每个加密的唯一性。

使用主密钥和 IV 的所有加密都应是唯一的，以防止伪造攻击。防火墙必须满足唯一性要求，即，在两个或更多不同的输入数据集上使用相同 IV 和相同密钥创建经过身份验证的加密的概率不得大于 $2^{32}$。

一旦 IV 的唯一值全部用完，IV 值将重复。一旦 IV 值重复，那么，使用相同主密钥和重复 IV 值来加密数据就意味着该加密与之前在其他数据上使用的加密相同。请在系统用完唯一加密之前更改主密钥，以防止防火墙在多个敏感数据上使用相同的加密（主密钥和 IV 值的组合）。唯一加密组合绝对不能重复或重复使用。

若要跟踪需要更改主密钥的时间，请在各个设备上设置主密钥的 **Lifetime**（生命周期）和 **Reminder**（提醒）值（**Device**（设备）> **Master Key and Diagnostics**（设备主密钥和诊断），然后编辑主密钥）。根据主密钥加密的预期数量保守地设置该值，确保所有加密都是唯一的，且不会出现加密组合重复或重复使用加密组合的现象。


© 2019 Palo Alto Networks, Inc.

# 获取证书


- 创建自签名根 CA 证书
- 生成证书
- 导入证书和私钥
- 从外部 CA 获取证书
- 安装设备证书
- 使用 SCEP 部署证书


## 创建自签名根 CA 证书

自签名根证书颁发机构 (CA) 证书是证书链中的最顶层证书。防火墙可以使用此证书自动签发证书以用于其他用途。例如，防火墙签发证书用于 SSL/TLS 解密和 GlobalProtect 大规模 VPN 中的卫星设备。

当与防火墙建立安全连接后，远程客户端必须信任签发证书的根 CA。否则，客户端浏览器会显示一个警告，提示证书无效且可能会（取决于安全设置）阻止连接。为了阻止出现这种情况，应在生成自签名根 CA 证书后将其导入客户端系统。

您可在 *Palo Alto Networks* 防火墙或 *Panorama* 中生成自签名证书，只要它们属于 *CA* 证书。

STEP 1 | 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

STEP 2 | 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 3 | 单击 **Generate**（生成）。

STEP 4 | 输入 **Certificate Name**（证书名称），例如 `GlobalProtect_CA`。证书名称区分大小写且在防火墙上最多可包含 63 个字符，或在 Panorama 上包含最多 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。

STEP 5 | 在 **Common Name**（公用名）字段中，输入您在其中配置服务使用此证书的接口的 FQDN（建议）或 IP 地址。

STEP 6 | 如果防火墙具备一个以上的虚拟系统，且您希望证书为所有虚拟系统所用，选择 **Shared**（共享）复选框。

STEP 7 | 将 **Signed By**（签名者）字段留空以便将证书指定为自签名。

STEP 8 | （必选）选中 **Certificate Authority**（证书颁发机构）复选框。

STEP 9 | 将 **OCSP Responder**（**OCSP** 响应者）字段留空；吊销状态验证不适用于根 CA 证书。

STEP 10 | 单击 **Generate**（生成）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 生成证书

Palo Alto Networks 防火墙和 Panorama 使用证书来对某些应用程序的客户端、服务器、用户和设备进行身份验证，如 SSL/TLS 解密、身份验证门户、GlobalProtect、站点到站点 IPSec VPN 和防火墙/Panorama Web 界面访问。为每一种用途生成证书：有关详细信息，请参阅密钥和证书。

要生成证书，必须先创建自签名根 CA 证书或导入证书（导入证书和私钥）进行签名。要使用在线证书状态协议 (OCSP) 验证证书吊销状态，应在生成证书之前配置 OCSP 响应者。

STEP 1 | 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

STEP 2 | 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 3 | 单击 **Generate**（生成）。

STEP 4 | 选择 **Local**（本地）（默认）作为 **Certificate Type**（证书类型），除非您希望 部署 SCEP 证书至 GlobalProtect 端点。

STEP 5 | 输入 **Certificate Name**（证书名称）。证书名称区分大小写且在防火墙上最多可包含 63 个字符，或在 Panorama 上包含最多 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。

STEP 6 | 在 **Common Name**（公用名）字段中，输入您在其中配置服务使用此证书的接口的 FQDN（建议）或 IP 地址。

STEP 7 | 如果防火墙具备一个以上的虚拟系统，且您希望证书为所有虚拟系统所用，选择 **Shared**（共享）复选框。

STEP 8 | 在 **Signed By**（签名者）字段中，选择将签发证书的根 CA 证书。

STEP 9 | （可选）选择 **OCSP Responder**（OCSP 响应者）。

STEP 10 | 对于密钥生成 **Algorithm**（算法），请选择 **RSA**（默认）或 **Elliptical Curve DSA**（椭圆曲线 **DSA**）(ECDSA)。对于受支持的客户端浏览器和操作系统，我们建议使用 ECDSA。

运行 *PAN-OS 6.1* 及之前版本的防火墙将会删除从 *Panorama™* 推送的所有 *ECDSA* 证书，并且在这些防火墙上由 *ECDSA* 证书授权机构 *(CA)* 签发的所有 *RSA* 证书都将无效。

不能使用硬件安全模块 (HSM) 存储用于 SSL 解密的 ECDSA 密钥。

STEP 11 | 选择 **Number of Bits**（位数）来定义证书的密钥长度。值越大越安全，但是需要的处理时间也越长。

STEP 12 | 选择 **Digest**（摘要）算法。从安全性最高到最低，可选择：**sha512**、**sha384**、**sha256** (默认)、**sha1**和**md5**。

在请求依赖 *TLSv1.2*（如管理员访问 *Web* 界面）的防火墙服务时使用的客户端证书不能将 *sha512* 作为摘要算法。客户端证书必须使用较低的摘要算法（如 *sha384*），或者必须在为防火墙服务配置 SSL/TLS 服务配置文件时将 *Max Version*（最高版本）限制为 *TLSv1.1*。

STEP 13 | 为 **Expiration**（过期）输入证书有效的天数（默认为 365)。



© 2019 Palo Alto Networks, Inc.

STEP 14 | （可选）**Add**（添加）**Certificate Attributes**（证书属性）以唯一标识防火墙和将使用证书的服务。



如果添加 *Host Name*（主机名）（*DNS* 名称）属性，最佳做法是与 *Common Name*（公用名）匹配，因为主机名会填充证书的主题备用名称 *(SAN)*字段，且一些浏览器会要求 *SAN* 指定证书保护的域；此外，对于 *GlobalProtect*，*Host Name*（主机名）必须与 *Common Name*（公用名）匹配。

STEP 15 | 单击 **Generate**（生成），然后在“设备证书”页面中单击证书名称。



不论处于哪个时区，防火墙所显示的证书生效及失效日期/时间始终为格林威治标准时间 *(GMT)*。

STEP 16 | 选中与证书在防火墙上的预期用途相对应的复选框。

例如，如果防火墙将使用此证书来将 syslog 安全地转发到外部 syslog 服务器，选中 **Certificate for Secure Syslog**（安全 **syslog** 证书）复选框。

STEP 17 | 单击 **OK**（确定）和 **Commit**（提交）。

## 导入证书和私钥

如果企业拥有自己的公钥基础设施 (PKI)，则可以将证书和私钥从企业证书颁发机构 (CA) 导入防火墙。企业 CA 证书（与从受信任的第三方 CA 购买的大多数证书不同）可以自动为某些应用程序（如 SSL/TLS 解密或大规模 VPN）签发 CA 证书。



您可在 *Palo Alto Networks* 防火墙或 *Panorama* 中导入自签名证书，只要它们属于 *CA* 证书。

相反，要将自签名根 *CA* 证书导入所有客户端系统，最佳实践是从企业 *CA* 导入证书，因为客户端已经与企业 *CA* 建立了信任关系，这简化了部署。

如果将要导入的证书是证书链的一部分，最佳实践是导入整个证书链。

STEP 1 | 从企业 CA 中，导出防火墙用于进行身份验证的证书和私钥。

在导出私钥后，必须输入密码对密钥进行加密传输。还务必要确保管理系统可以访问证书和密钥文件。在将密钥导入防火墙后，必须输入同一密码进行解密。

STEP 2 | 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

STEP 3 | 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 4 | 单击 **Import**（导入）并输入 **Certificate Name**（证书名称）。证书名称区分大小写且在防火墙上最多可包含 63 个字符，或在 Panorama 上包含最多 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。

STEP 5 | 要使证书适用于所有虚拟系统，请选中 **Shared**（共享）复选框。此复选框只有在防火墙支持多个虚拟系统时才会显示。

STEP 6 | 输入从 CA 收到的 **Certificate File**（证书文件）的路径和名称，或 **Browse**（浏览）以查找该文件。

STEP 7 | 选择 **File Format**（数据格式）：



© 2019 Palo Alto Networks, Inc.

- **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）— 这是默认和最常见的格式，其中密钥和证书在同一个容器（**Certificate File**（证书文件））中。如果硬件安全模块 (HSM) 存储此证书的私钥，请选中 **Private key resides on Hardware Security Module**（硬件安全模块上的私钥）复选框。
- **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 必须从证书单独导入密钥。如果硬件安全模块 (HSM) 存储此证书的私钥，请选中 **Private key resides on Hardware Security Module**（硬件安全模块上的私钥）复选框，然后跳过下一个步骤。否则，选中 **Import Private Key**（导入私钥）复选框，输入 **Key File**（密钥文件）或 **Browse**（浏览）到该文件，然后继续下一个步骤。

STEP 8 | 输入并重新输入（确认）用于加密私钥的 **Passphrase**（密码）。

STEP 9 | 单击 **OK**（确定）。设备证书页面将会显示导入的证书。

# 从外部 CA 获取证书

从外部证书颁发机构 (CA) 获取证书的好处是私钥不会离开防火墙。要从外部 CA 获取证书，应生成证书签名请求 (CSR) 并将其提交给 CA。在 CA 使用指定的属性签发证书后，将其导入防火墙。CA 可以是众所周知的公共 CA 或企业 CA。

要使用在线证书状态协议 (OCSP) 验证证书吊销状态，应在生成 CSR 之前配置 OCSP 响应者。

STEP 1 | 从外部 CA 索取证书。

1. 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。
2. 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。
3. 单击 **Generate**（生成）。
4. 输入 **Certificate Name**（证书名称）。证书名称区分大小写且在防火墙上最多可包含 63 个字符，或在 Panorama 上包含最多 31 个字符。它必须是唯一的，且只能使用字母、数字、连字符和下划线。
5. 在 **Common Name**（公用名）字段中，输入您在其中配置服务使用此证书的接口的 FQDN（建议）或 IP 地址。
6. 如果防火墙具备一个以上的虚拟系统，且您希望证书为所有虚拟系统所用，选择 **Shared**（共享）复选框。
7. 在 **Signed By**（签名者）字段中，选择 **External Authority (CSR)**（外部颁发机构 **(CSR)**）。
8. 如果适用，请选择 **OCSP Responder**（**OCSP** 响应者）。
9. （可选）**Add**（添加）**Certificate Attributes**（证书属性）以唯一标识防火墙和将使用证书的服务。

   如果添加 *Host Name*（主机名）属性，则将它与 *Common Name*（公用名）进行匹配（这是 *GlobalProtect* 的强制规定）。主机名填充证书的主题备用名称字段。
10. 单击 **Generate**（生成）。**Device Certificates**（设备证书）选项卡将会显示状态为 `pending` 的 CSR。

STEP 2 | 将 CSR 提交到 CA。

1. 选择 CSR 并单击 **Export**（导出），将 .csr 文件保存到本地计算机。
2. 将 .csr 文件上传到 CA。

STEP 3 | 导入证书。

1. 在 CA 发送签名的证书响应 CSR 后，返回到 **Device Certificates**（设备证书）选项卡，然后单击 **Import**（导入）。
2. 输入用于生成 CSR 的 **Certificate Name**（证书名称）。
3. 输入 CA 发送的 PEM **Certificate File**（证书文件）的路径和名称，或 **Browse**（浏览）到该文件。


© 2019 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。**Device Certificates**（设备证书）选项卡将会显示状态为 `valid` 的证书。

STEP 4 | 配置证书。

1. 单击证书 **Name**（名称）。
2. 选中与证书在防火墙上的预期用途相对应的复选框。例如，如果防火墙将使用此证书来将 syslog 安全地转发到外部 syslog 服务器，选中 **Certificate for Secure Syslog**（安全 **syslog** 证书）复选框。
3. 单击 **OK**（确定）和 **Commit**（提交）。

# 安装设备证书

下一代防火墙可以利用设备遥测和 IoT 等云服务。为此，必须安装设备证书以使用 Palo Alto Networks 客户支持门户 (CSP) 成功对防火墙执行身份验证，从而利用这些云服务。需要安装设备证书的情况因功能而异，因此，仅在功能设置文档要求您必须安装设备证书时才执行这一操作。

您只需要安装一次设备证书即可。每个使用设备证书的功能都将使用防火墙上已安装的证书（如有）。

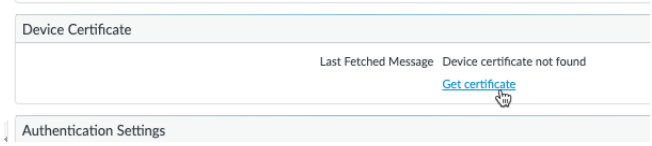
您可以将设备证书安装到由 Panorama 托管的防火墙上。如果您想将设备证书直接安装到单个下一代防火墙上（即，您不会使用 Panorama）：

STEP 1 | 生成一次性密码 (OTP)。

1. 登录到客户支持门户。
2. 选择 **Assets**（资产）> **Device Certificates**（设备证书）和 **Generate OTP**（生成 **OTP**）。
3. 对于 **Device Type**（设备类型），选择 **Generate OTP for Next-Gen Firewalls**（为下一代防火墙生成 **OTP**）。
4. 选择 **PAN OS Device**（**PAN OS** 设备）序列号。
5. **Generate OTP**（生成 **OTP**）并复制该 OTP。

STEP 2 | 以管理员用户身份登录到下一代防火墙。

STEP 3 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Device Certificate**（设备证书）并**Get certificate**（获取证书）。




STEP 4 | 粘贴您生成的 **One-time Password**（一次性密码），然后单击 **OK**（确定）。

STEP 5 | 您的下一代防火墙可成功检索并安装证书。

# 使用 SCEP 部署证书

如果您的企业 PKI 中包含简单证书注册协议 (SCEP)，则可以配置 SCEP 配置文件，以自动生成和分发唯一的客户端证书。SCEP 操作是动态的，因为当 SCEP 客户端提出请求时，企业 PKI 生成特定用户的证书并将其发送至 SCEP 客户端。然后，SCEP 客户端以透明方式将该证书部署至客户端设备。

您可以和 GlobalProtect 一起使用 SCEP 配置文件将特定用户的客户端证书分配给 GlobalProtect 用户。在此用例中，GlobalProtect 充当您企业 PKI 中 SCEP 服务器的 SCEP 客户端。此外，您可以使用 SCEP 配置文件将客户端证书分配给进行相互身份验证的 Palo Alto Networks 设备，以便 Palo Alto Networks 设备管理访问，实现设备间通信。

STEP 1 | 创建 SCEP 配置文件。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **SCEP**，然后 **Add**（添加）新配置文件。
2. 输入 **Name**（名称）以标识 SCEP 配置文件。
3. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。

STEP 2 | （可选）要让基于 SCEP 的证书生成更安全，可在公钥基础结构 (PKI) 与门户之间为各证书请求配置 SCEP 质询-响应机制。

配置此机制后，其操作不可见，您无需再进行任何输入操作。

为了符合《美国联邦处理标准》(FIPS)，采用 **Dynamic**（动态）SCEP 质询，并指定使用 HTTPS 的 **Server URL**（服务器 **URL**）。

选择以下任一选项：

- **None**（无）— （默认）SCEP 服务器不会在门户发布证书前对其进行质询。
- **Fixed**（固定）— 从 PKI 基础结构中的 SCEP 服务器获取注册质询密码，然后将该密码输入“密码”字段。
- **Dynamic**（动态）— 输入选中项的用户名和密码（可能是 PKI 管理员的凭据）以及门户-客户端提交这些凭据的 SCEP **Server URL**（服务器 URL）。每次提出证书请求后，使用这些凭据验证至 SCEP 服务器，而 SCEP 服务器会以透明方式生成门户 OTP 密码。（每次提出证书请求后，您可在 `The enrollment challengepassword is`（注册质询密码为）字段所在屏幕刷新后发现此 OTP 更改。）PKI 会以透明方式将各新密码传到门户，然后门户可将此密码用于其证书请求。

STEP 3 | 指定 SCEP 服务器与门户之间的连接设置，以便门户请求和接收客户端证书。

您可通过指定证书 **Subject**（主题）名称中的令牌纳入有关客户端设备或用户的其他信息。

门户将令牌值和主机 ID 纳入向 SCEP 服务器发送的 CSR 请求中。

1. 配置门户用于访问 PKI 中 SCEP 服务器的 **Server URL**（服务器 **URL**）（例如，`http://10.200.101.1/certsrv/mscep/`）。
2. 在 **CA-IDENT Name**（**CA-IDENT** 名称）字段中输入字符串（最长不超过 255 个字符）以标识 SCEP 服务器。
3. 输入在 SCEP 服务器生成的证书中使用的 **Subject**（主题）名称。该主题必须是格式为 <**attribute**>=<**value**> 的可分辨名称，且必须包含公用名属性 (CN=<**variable**>)。CN 支持以下动态令牌：
   - `$USERNAME` — 使用此令牌让门户为特定用户请求证书。要与 GlobalProtect 一起使用这个变量，必须启用组映射。用户输入的用户名必须与用户组映射表中的名称匹配。
   - `$EMAILADDRESS` — 使用此令牌请求与特定电子邮件地址相关联的证书。要使用此变量，必须启用组映射，并在服务器配置文件的邮件域部分配置 **Mail Attributes**（邮件属性）。如果 GlobalProtect 无法识别用户的电子邮件地址，则会生成唯一 ID 并使用该值填充 CN。
   - `$HOSTID` — 要仅为设备请求证书，请指定主机 ID 令牌。当用户尝试登录至门户时，端点将发送包含其主机 ID 值的标识信息。主机 ID 值视设备类型而定，为接口 (Mac) 的 GUID (Windows) MAC 地址、Android ID（Android 设备）、UDID（iOS 设备）或 GlobalProtect 分配的唯一名称 (Chrome)。
   - `$UDID` — 根据 GlobalProtect 客户端的设备 UDID 或 Palo Alto Networks 设备间进行相互身份验证的设备序列号，使用 UDID 公用名属性请求证书。

   当 GlobalProtect 门户将 SCEP 设置推送到代理时，将会使用证书所有者（例如 **O=acme,CN=johndoe**）的实际值（用户名、主机 ID 或电子邮箱地址）替换主题名称的公用名 (CN) 部分。
4. 选择 **Subject Alternative Name Type**（主题备用名称类型）。


© 2019 Palo Alto Networks, Inc.

使用用于主题备用名称类型的静态条目。防火墙不支持 ***$USERNAME*** 等动态令牌。

- **RFC 822 Name**（**RFC 822** 名称）— 输入证书主题或“主题备选名称”扩展中的电子邮件名称。
- **DNS Name**（**DNS** 名称）— 输入用于评估证书的 DNS 名称。
- **Uniform Resource Identifier**（统一资源标识符）— 输入客户端从其获取证书的资源名称。
- **None**（无）— 不指定证书属性。

STEP 4 | （可选）为证书配置加密设置。

- 选择证书的密钥长度（**Number of Bits**（位数））。

  如果防火墙为 FIPS-CC 模式且密钥生成算法为 RSA，则 RSA 密钥必须为 2,048 位或更大。
- 选择 **Digest for CSR**（**CSR** 摘要）以标识证书签名请求 (CSR) 的摘要算法：sha1、sha256 或 sha384。

STEP 5 | （可选）配置证书的允许用途：签名或加密。

- 要将证书用于签名，选中 **Use as digital signature**（用作数字签名）复选框。这可使端点能够使用证书中的密钥来验证数字签名。
- 要将证书用于加密，选中 **Use for key encipherment**（用于加密）复选框。这可使客户端能够使用证书中的密钥来加密通过 SCEP 服务器颁发的证书建立的 HTTPS 连接所交换的数据。

STEP 6 | （可选）为确保门户连接到正确的 SCEP 服务器，请输入 **CA Certificate Fingerprint**（**CA** 证书指纹）。该指纹可从 SCEP 服务器界面的“指纹”字段中获取。

1. 输入 SCEP 服务器管理 UI 的 URL（例如，`http://<hostname or IP>/CertSrv/mscep_admin/`）。
2. 复制指纹并将其输入 **CA Certificate Fingerprint**（**CA** 证书指纹）字段中。

STEP 7 | 启用 SCEP 服务器与防火墙之间的相互 SSL 身份验证。这必须符合《美国联邦信息处理标准》(FIPS)。

（*FIPS-CC* 操作已在防火墙登录页面及防火墙状态栏中予以指明。）

选择 SCEP 服务器的根 **CA Certificate**（**CA** 证书）。或者，您也可以通过选择 **Client Certificate**（客户端证书）在 SCEP 服务器和服务器之间启用相互 SSL 身份验证。

STEP 8 | 保存并提交配置。

1. 单击 **OK**（确定）以保存设置并关闭 SCEP 配置。
2. **Commit**（提交）配置。

门户尝试使用 SCEP 配置文件中的设置请求 CA 证书，并将其保存至承载门户的防火墙。如果成功，则 CA 证书显示在 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）中。

STEP 9 | （可选）如果门户在保存 SCEP 配置文件后未能获取证书，您可手动从门户生成证书签名请求 (CSR)。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
2. 输入 **Certificate Name**（证书名称）。该名称不得包含空格。
3. 选择用于提交 CSR 至企业 PKI 的 **SCEP Profile**（**SCEP** 配置文件）。
4. 单击 **OK**（确定）以提交请求和生成证书。



© 2019 Palo Alto Networks, Inc.

# 导出证书和私钥

Palo Alto Networks 建议您使用企业公钥基础设施 (PKI) 在组织中分配证书和私钥。但是，如果需要，您也可以从防火墙或 Panorama 导出证书和私钥。您可以在以下情况下使用导出的证书和私钥：

- 配置 Web 界面的基于证书的管理员身份验证
- 在 GlobalProtect LSVPN 组件之间启用 SSL，以将 GlobalProtect 代理/应用身份验证配置到门户和网关
- SSL 转发代理解密
- 从外部 CA 获取证书

STEP 1 | 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

STEP 2 | 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（特定 vsys 或 **Shared**（共享））。

STEP 3 | 选择证书，单击 **Export**（导出），然后选择 **File Format**（文件格式）：

- **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 这是默认格式，也是最常见的格式，并且具备互联网上的广播支持。如果您希望导出的文件包含私钥，请选中 **Export Private Key**（导出私钥）复选框。
- **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）— 这种格式比 PEM 更安全，但不常见或者不具备广播支持。导出的文件将自动包含私钥。
- **Binary Encoded Certificate (DER)**（二进制编码证书 **(DER)**）— 相较于其他格式而言，更多的操作系统类型支持这种格式。您可以只导出证书，不导出私钥：忽略 **Export Private Key**（导出私钥）复选框和密码字段。

STEP 4 | 如果 **File Format**（文件格式）为 PKCS12 或者 PEM，并且选中了 **Export Private Key**（导出私钥）复选框，输入 **Passphrase**（密码）和 **Confirm Passphrase**（确认密码）对私钥进行加密。将证书和私钥导入客户端系统时，将使用该密码。

STEP 5 | 单击 **OK**（确认），将证书/私钥文件保存到您的计算机中。



© 2019 Palo Alto Networks, Inc.

# 配置证书配置文件

证书配置文件定义用于下列各项的用户和设备身份验证：身份验证门户、多重因素身份验证(MFA)、GlobalProtect、站点到站点 IPSec VPN、外部动态列表(EDL)验证、动态 DNS (DDNS)、User-ID 代理和 TS 代理访问、以及对于 Palo Alto Networks 防火墙或 Panorama 的 Web 界面访问。配置文件用来指定要使用的证书、验证证书吊销状态的方法和状态限制访问的方式。配置每个应用程序的证书配置文件。



最佳实践是为证书配置文件启用在线证书状态协议 *(OCSP)* 和证书撤销列表 *(CRL)* 状态验证，以验证证书是否已撤销。启用 *OCSP* 和 *CRL*，这样，在 *OCSP* 服务器不可用时，防火墙可以使用 *CRL*。有关这些方法的详细信息，请参阅证书吊销。

STEP 1 | 获取将要分配的证书颁发机构 (CA) 证书。

执行下列步骤之一，获取将要分配到配置文件的 CA 证书。必须至少分配一个证书。

- 生成证书。
- 从企业 CA 导出证书，然后将其导入防火墙（请参阅3步骤）。

STEP 2 | 标识证书配置文件。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后单击 **Add**（添加）。
2. 输入 **Name**（名称）以标识配置文件。名称区分大小写，必须是唯一的，最多可以包含 63 个字符（防火墙）或 31 个字符 (Panorama)，只能包括字母、数字、空格、连字符和下划线。
3. 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 3 | 分配一个或多个证书。

为每个 CA 证书完成以下步骤：

1. 在 CA 证书表格中，单击 **Add**（添加）。
2. 选择 **CA Certificate**（**CA** 证书）。另外，要导入证书，单击 **Import**（导入），输入 **Certificate Name**（证书名称），**Browse**（浏览）到从企业 CA 中导出的 **Certificate File**（证书文件），然后单击 **OK**（确认）。
3. （可选）如果防火墙使用 OCSP 验证证书吊销状态，可配置以下字段覆盖默认行为。对于大多数部署，这些字段不适用。
   - 默认情况下，防火墙使用证书中的“颁发机构信息访问”(AIA) 提取 OCSP 响应者信息。要替代 AIA 信息，请输入 **Default OCSP URL**（默认 **OCSP URL**）（以 `http://` 或 `https://` 为开头）。
   - 默认情况下，防火墙使用在 **CA** 证书字段中选择的证书验证 OCSP 响应者。要使用不同的证书进行验证，可在 **OCSP** 验证 **CA** 证书字段中进行选择。
4. 单击 **OK**（确定）。“证书”表格将会显示分配的证书。

STEP 4 | 定义用来验证证书吊销状态和相关阻塞行为的方法。

1. 选择 **Use CRL**（使用 **CRL**）和/或 **Use OCSP**（使用 **OCSP**）。如果同时选择两种方法，则防火墙首先尝试使用 OCSP，并且只有在 OCSP 响应者不可用时返回来使用 CRL 方法。
2. 根据验证方法，输入 **CRL Receive Timeout**（**CRL** 接收超时）和/或 **OCSP Receive Timeout**（**OCSP** 接收超时）。这些是防火墙在过后停止等待 CRL/OCSP 服务响应的时间间隔（1 至 60 秒）。
3. 输入 **Certificate Status Timeout**（证书状态超时）。这是防火墙在过后停止等待任何证书状态服务响应和应用定义的任何会话阻塞逻辑的时间间隔（1 至 60 秒）。将 **Certificate Status Timeout**（证书状态超时）与 OCSP/CRL **Receive Timeout**（接收超时）进行关联，如下所示：



© 2019 Palo Alto Networks, Inc.

- 如果同时启用 OCSP 和 CRL — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或两个 **Receive Timeout**（接收超时）值的总和。
- 如果只启用 OCSP — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或 OCSP **Receive Timeout**（接收超时）值。
- 如果只启用 CRL — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或 CRL **Receive Timeout**（接收超时）值。

4. 如果您希望防火墙在 OCSP 或 CRL 服务返回未知证书吊销状态时阻止会话，请选中 **Block session if certificate status is unknown**（如果证书状态未知，则阻止会话）。否则，防火墙会允许会话。
5. 如果您希望防火墙在注册 OCSP 或 CRL 请求超时后阻止会话，请选中 **Block session if certificate status cannot be retrieved within timeout**（如果无法在超时时间内检索到证书状态，则阻止会话）。否则，防火墙会允许会话。
6. （仅限 **GlobalProtect**）如果您希望防火墙在客户端证书主题中包含的序列号属性与 GlobalProtect 应用为端点报告的主机 ID 不匹配时阻止会话，请选中 **Block sessions if the certificate was not issued to the authenticating device**（如果证书未发送至执行身份验证的设备，则阻止会话）。

STEP 5 | 单击 **OK**（确定）和 **Commit**（提交）。


© 2019 Palo Alto Networks, Inc.

# 配置 SSL/TLS 服务配置文件

Palo Alto Networks 防火墙和 Panorama 使用 SSL/TLS 服务配置文件指定证书及 SSL/TLS 服务的许可协议版本。防火墙和 Panorama 将 SSL/TLS 应用于身份验证门户、GlobalProtect 门户和网关、管理 (MGT) 界面入站流量、URL 管理替代功能及 User-ID™ Syslog 侦听服务。通过定义协议版本，您可以使用配置文件来限制与请求服务的客户端进行安全通信的密码套件。通过启用防火墙或 Panorama，该操作可避免 SSL/TLS 版本的已知缺陷，提升网络安全性。如果服务请求包含超出指定范围的协议版本，防火墙或 Panorama 会降级或升级以连接至支持版本。

在请求防火墙服务的客户端系统中，证书信任列表 *(CTL)* 必须包括颁发在 *SSL/TLS* 服务配置文件中指定的证书的证书颁发机构 *(CA)* 证书。否则，用户在请求防火墙服务时会看到证书出错。客户端浏览器默认提供大多数第三方 *CA* 证书。如果企业或防火墙生成的 *CA* 证书是颁发者，则必须将该 *CA* 证书部署到客户端浏览器中的 *CTL*。

STEP 1 | 对于每种所需的服务，在防火墙上生成或导入证书（请参阅获取证书）。

*SSL/TLS* 服务配置文件仅使用已签名的证书，而不使用 *CA* 证书。

STEP 2 | 选择 **Device**（设备）> **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

STEP 3 | 如果防火墙具备一个以上的虚拟系统 (vsys)，选择具备可用配置文件的 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 4 | 单击 **Add**（添加），然后输入 **Name**（名称）以标识配置文件。

STEP 5 | 选择您刚才获取的 **Certificate**（证书）。

STEP 6 | 定义服务可以使用的协议范围：

- 对于 **Min Version**（最小版本），选择允许的最新 TLS 版本：**TLSv1.0**（默认）、**TLSv1.1**、或 **TLSv1.2**。
- 对于 **Max Version**（最大版本），选择允许的最新 TLS 版本：**TLSv1.0**、**TLSv1.1**、**TLSv1.2** 或 **Max**（最大）（最新的可用版本）。默认版本为 **Max**（最大）。

最佳做法是设置 *Min Version*（最小版本）为 *TLSv1.2*，*Max Version*（最大版本）为 *Max*（最大）。

在运行 *PAN-OS 8.0* 或更高版本的 *FIPS/CC* 模式的防火墙上，*TLSv1.1* 是最早支持 *TLS* 的版本；请勿选择 *TLSv1.0*。

在请求依赖 *TLSv1.2* 的防火墙服务时使用的客户端证书不能将 *SHA512* 作为摘要算法。客户端证书必须使用较低的摘要算法（如 *SHA384*），或者您必须将防火墙服务的 *Max Version*（最高版本）限制为 *TLSv1.1*。

STEP 7 | 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 配置 SSH 服务配置文件

通过 SSH 服务配置文件，您可以自定义 SSH 参数以增强与 Palo Alto Networks 管理和高可用性 (HA) 设备的 SSH 连接的安全性和完整性。SSH 默认支持所有密码、密钥交换算法和消息认证码，这些都使您的连接易受攻击。通过 SSH 服务配置文件，您可以限制 SSH 服务器支持的算法。您还可以生成新的主机密钥，并指定用于重新生成和交换 SSH 会话密钥的数据量、时间和基于数据包的阈值。

根据 SSH 服务器实例配置管理或 HA SSH 服务配置文件。您可以通过防火墙或 Panorama™ Web 界面（适用于跨多个防火墙或设备的设置）或 CLI 对配置文件进行配置。

您最多可以配置 *4* 个管理和 *4* 个 *HA* 服务器配置文件。

要在收集器组内为每个专用日志收集器（日志收集器模式下的 *M* 系列或 *Panorama* 虚拟设备）使用相同的 *SSH* 连接，请从 *Panorama* 管理服务器配置 *SSH* 服务配置文件，并将更改 *Commit*（提交）到 *Panorama*，然后*Push*（推送）配置到日志收集器。您还可以使用命令 ***set log-collector-group <name> general-setting management ssh*** 从 *CLI* 执行这些步骤。

- 创建 SSH 管理配置文件
- 创建 SSH HA 配置文件

## 创建 SSH 管理配置文件

您可以创建 SSH 管理配置文件以自定义用于管理连接的 SSH 设置。

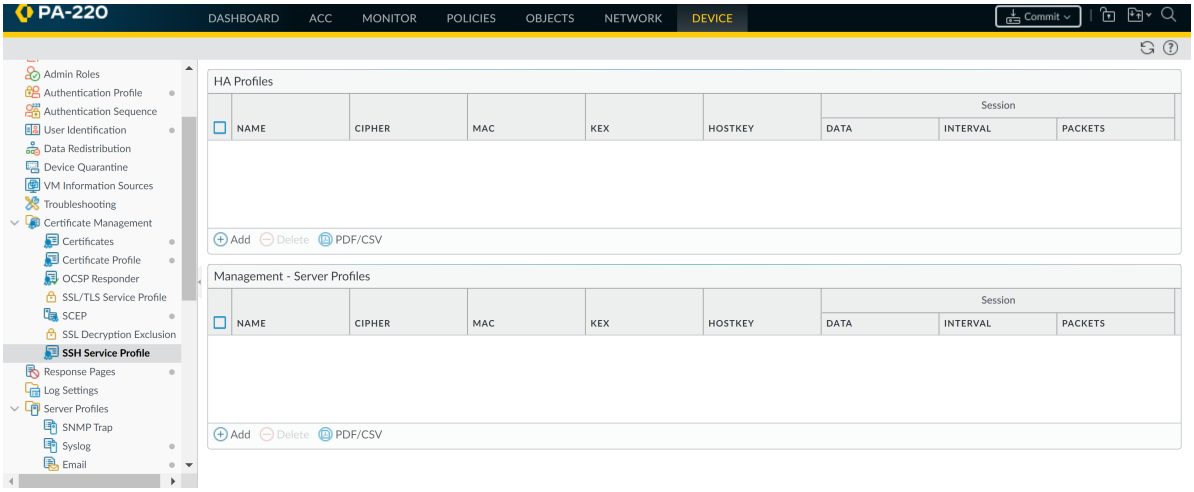
您可以从 *CLI* 配置或更新现有管理配置文件。

STEP 1 | 创建管理 - 服务器配置文件。

1. 选择 **Device**（设备）> **Certification Management**（证书管理）> **SSH Service Profile**（**SSH** 服务配置文件）。
2. **Add**（添加）管理 - 服务器配置文件。

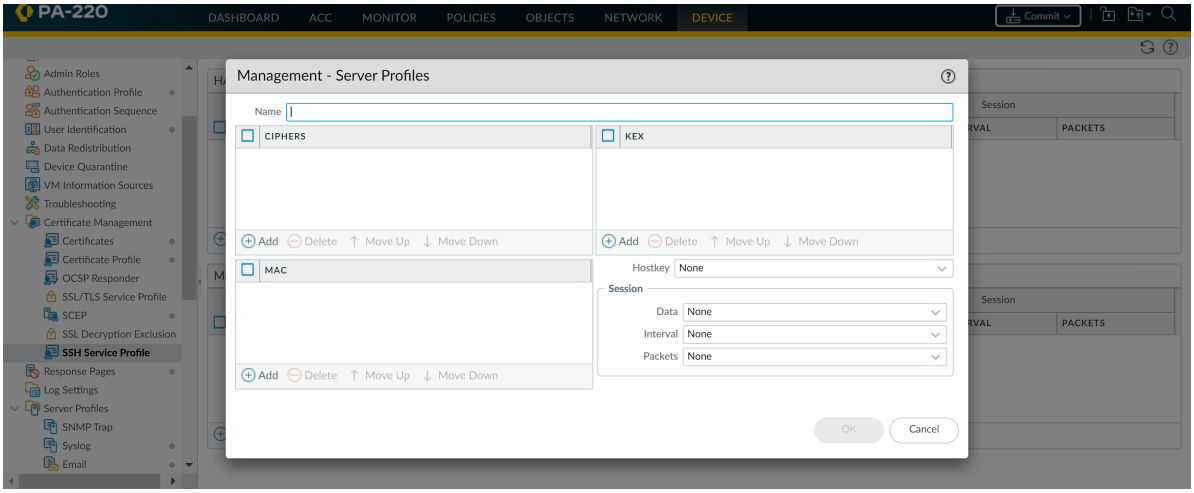


© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

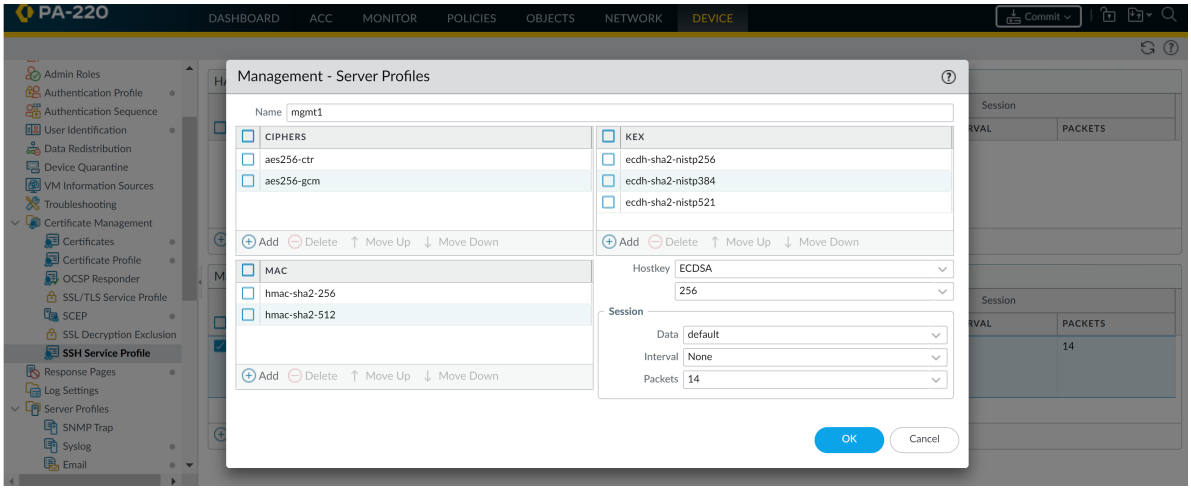





© 2019 Palo Alto Networks, Inc.

3. 输入 **Name**（名称）以标识配置文件。
4. （可选）**Add**（添加）配置文件将支持的密码、消息认证码或密钥交换算法。
5. （可选）选择 **Hostkey**（主机密钥）和密钥长度。
6. （可选）输入 SSH 会话密钥更新参数值：**Data**（数据）、**Interval**（间隔）和 **Packets**（数据包）。


© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

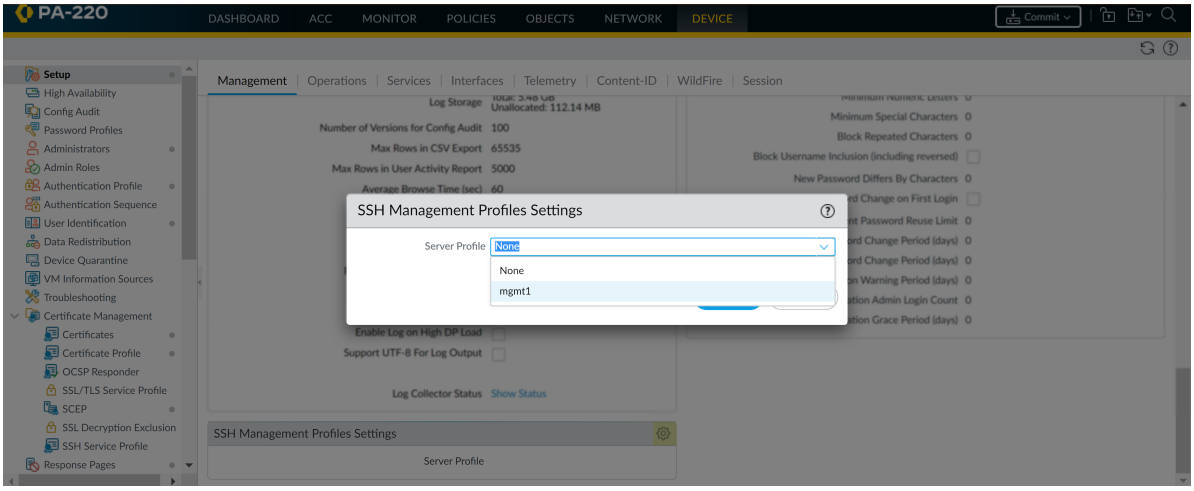
7. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 2 | 选择要应用的管理配置文件。

1. 选择**Device**（设备） > **Setup**（设置） > **Management**（管理）。在“SSH 管理配置文件”设置下，选择现有配置文件。



© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

2. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 3 | 从 CLI 重新启动管理 SSH 服务以应用配置文件。

每次应用新的配置文件或更改正在使用的配置文件时，必须重新启动连接；这将重新启动设备。新配置不会影响活动会话。此配置文件将应用到后续连接（或会话）。

1. admin@PA-3260> **set ssh service-restart mgmt**

# 创建 SSH HA 配置文件

为确保 HA 对中设备之间 SSH 通信的安全，应创建一个 SSH HA 配置文件。在创建配置文件之前，必须先在设备之间建立 HA 连接。如果尚未建立 HA 连接，您必须在控制链路连接上启用加密，将 HA 密钥导出到网络位置，并导入对等设备上的 HA 密钥。（请参阅配置主动/被动 HA 或配置主动/主动 HA。）



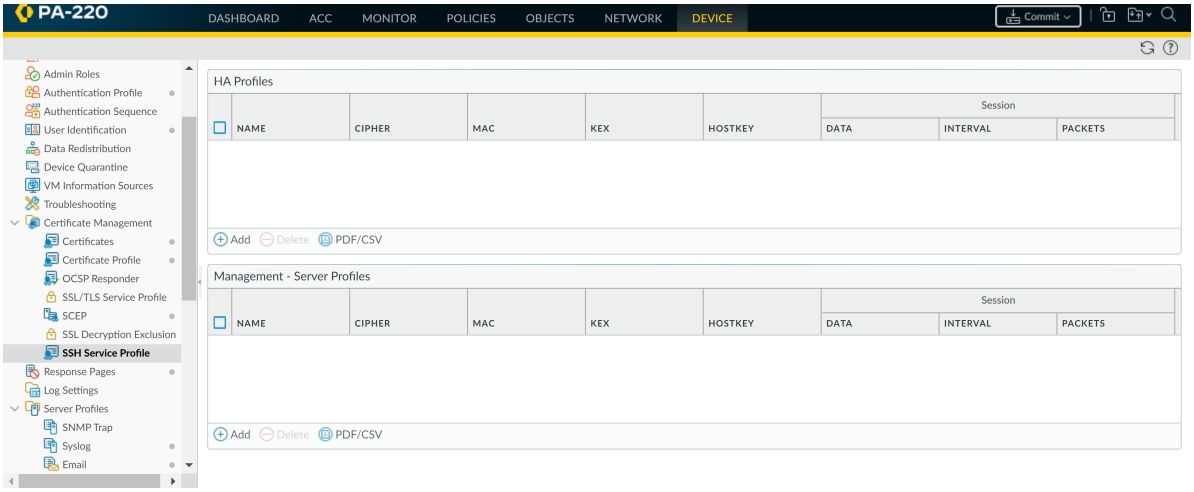
您可以从 *CLI* 配置或更新现有 HA 配置文件。

STEP 1 | 创建 HA 配置文件。

1. 选择 **Device**（设备）> **Certification Management**（证书管理）> **SSH Service Profile**（**SSH** 服务配置文件）。
2. **Add**（添加）HA 配置文件。

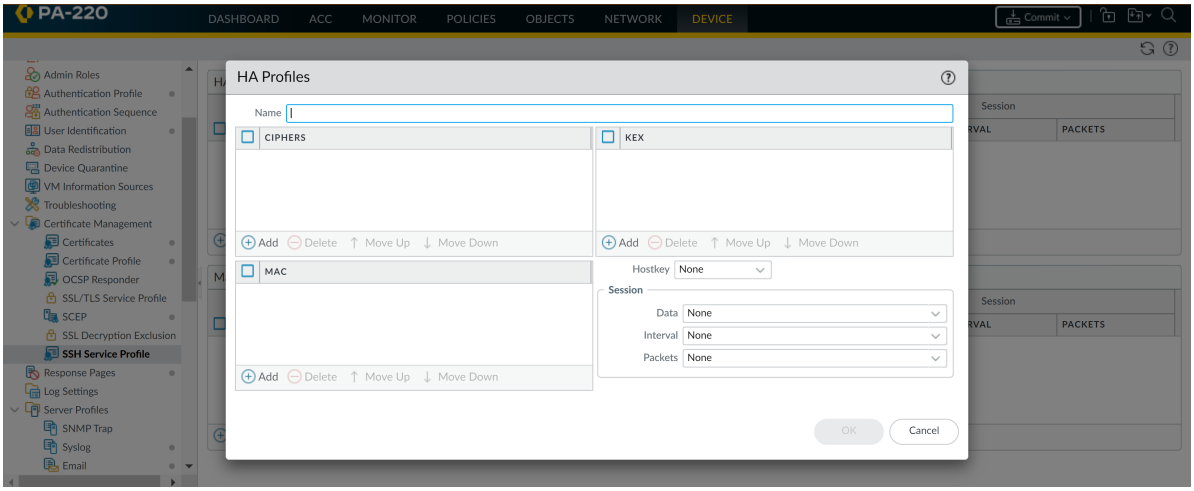


© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

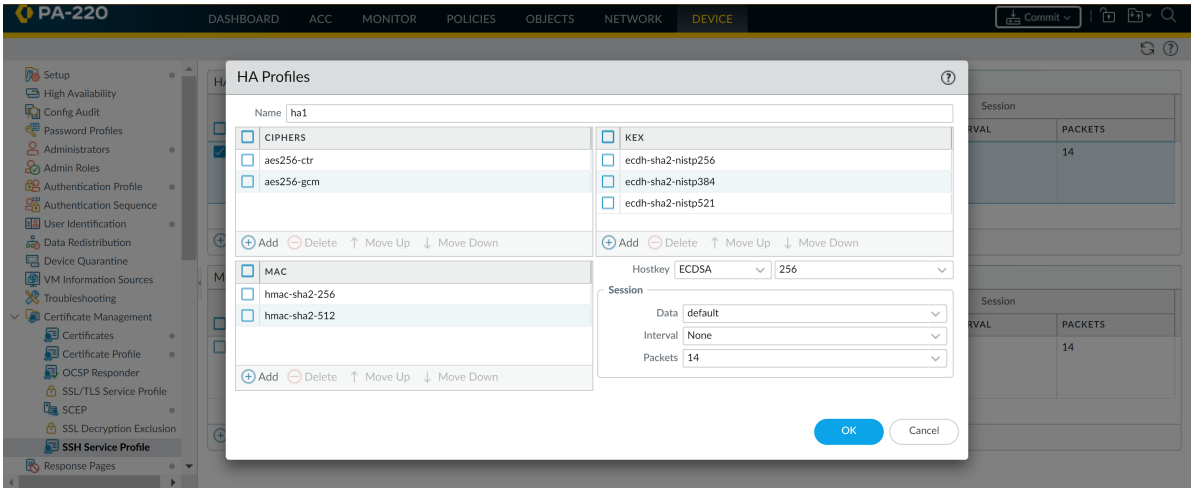





© 2019 Palo Alto Networks, Inc.

3. 输入 **Name**（名称）以标识配置文件。
4. （可选）**Add**（添加）配置文件将支持的密码、消息认证码或密钥交换算法。
5. （可选）选择 **Hostkey**（主机密钥）和密钥长度。
6. （可选）输入 SSH 会话密钥更新参数值：**Data**（数据）、**Interval**（间隔）和 **Packets**（数据包）。


© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

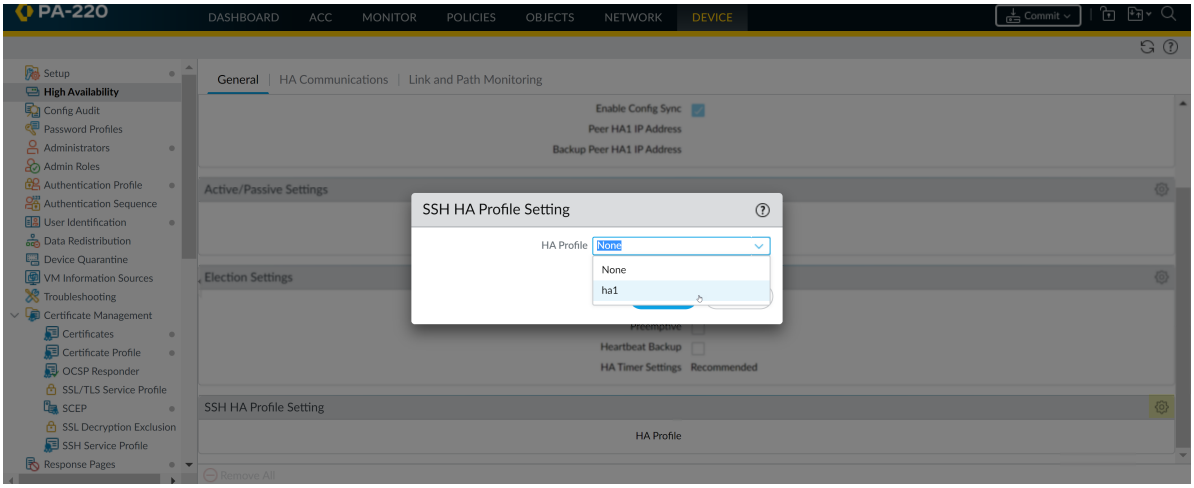
7. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 2 | 选择要应用的 HA 配置文件。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规）。在“SSH HA 配置文件”设置下，选择现有配置文件。



© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

2. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 3 | 从 CLI 重新启动 HA1 SSH 服务以应用配置文件。

每次应用新的配置文件或更改正在使用的配置文件时，必须重新启动连接；这将重新启动设备。新配置不会影响活动会话。此配置文件将应用到后续连接（或会话）。

1. admin@PA-3260> **set ssh service-restart ha**



如果 *HA* 对之间已建立连接，且您想减少 *SSH* 服务重新启动时的停机时间，则可以使用以下命令。如果尚未建立 *HA* 连接，必须重新启动 *SSH* 服务。

- （已配置 *HA1* 备份）*admin@PA-3260>* ***request high-availability session-reestablish***
- （未配置 *HA1* 备份或 *HA1* 备份链路已关闭）*admin@PA-3260>* ***request high-availability session-reestablish force***

  如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份后，使用 ***force*** 选项将不起作用。）



© 2019 Palo Alto Networks, Inc.

# 入站流量管理之证书替换

首次启动防火墙或 Panorama 时，会自动生成默认证书，允许 HTTPS 通过管理 (MGT) 界面及（仅防火墙）其他任何支持 HTTPS 流量管理的接口访问 Web 界面及 XML API（有关详细信息，请参阅使用接口管理概要文件限制访问）。要提高入站流量管理的安全性，您需要将默认证书替换为向您组织专门发放的证书。



您无法查看、修改或删除默认证书。

为了确保流量管理，还必须配置管理帐户和身份验证。

STEP 1 | 获取证书旨在向管理员的用户端系统验证防火墙或 Panorama。

您可以使用用户端系统已信任的证书来简化证书部署。因此，我们建议您从您企业的证书颁发机构 (CA) 导入证书和私钥或从外部 CA 获取证书；用户端受信任的根证书存储区可能已存在确保可信性的相关根 CA 证书。



如果您在防火墙或 *Panorama* 上生成证书，管理员会看到证书错误，原因是根 *CA* 证书不在用户端系统信任的根证书存储区内。要防止出现此错误，应将自签名根 *CA* 证书部署到所有最终用户端系统。



不论您以何种方式获取证书，为提高安全性起见，我们都推荐使用 *sha256Digest*（摘要）算法或更高级别的算法。

STEP 2 | 配置 SSL/TLS 服务配置文件。

选择您刚才获取的 **Certificate**（证书）。



为提高安全性，我们建议您将 *Min Version*（最小版本）（最先允许的 *TLS* 版本）设置为 *TLSv1.2*，管理入站流量。我们还建议您为每项防火墙或 *Panorama* 服务使用不同的 *SSL/TLS Service Profile*（*SSL/TLS* 服务配置文件），而非将同一配置文件应用于所有防火墙或 *Panorama* 服务。

STEP 3 | 应用 SSL/TLS Service Profile（SSL/TLS 服务配置文件）进行入站流量管理。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。
2. 选择刚刚完成配置的 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
3. 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 配置 SSL 转发代理服务器证书的密钥大小

当响应 SSL 转发代理会话中的客户端时，该防火墙会创建目标服务器向其提供的证书的副本，并用该副本来建立与客户端的连接。默认情况下，该防火墙会使用与目标服务器所提供的证书相同的密钥大小来生成证书。尽管如此，您可以更改防火墙生成证书的密钥大小，如下所示：

STEP 1 | 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后在“解密设置”部分单击 **SSL Forward Proxy Settings**（**SSL** 转发代理设置）。

STEP 2 | 选择 密钥大小：

- **Defined by destination host**（目标主机定义）— 防火墙根据目标服务器证书确定用于在自身与客户端之间建立 SSL 代理会话的证书的密钥大小和哈希算法。如果目标服务器使用 1,024 位 RSA 密钥，则防火墙会使用 1,024 位 RSA 密钥来生成证书。如果目标服务器使用大于 1,024 位（例如，2,048 位或 4,096 位）的密钥大小，则防火墙会使用 2,048 位 RSA 密钥来生成证书。如果目标服务器使用 SHA-1 哈希算法，则防火墙会使用该 SHA-1 哈希算法来生成证书。如果目标服务器使用强于 SHA-1 的哈希算法，则防火墙会使用 SHA-256 算法生成证书。这是默认设置。
- **1024-bit RSA**（**1,024** 位 **RSA**）— 不管目标服务器证书的密钥大小是什么，防火墙都会生成使用 1,024 位 RSA 密钥和 SHA-1 哈希算法的证书。自 2013 年 12 月 31 日起，公共证书授权机构 (CA) 和常用浏览器为所用密钥小于 2048 位的 X.509 证书提供有限支持。将来，当出现此类密钥时，浏览器将根据安全设置向用户发出警告或全面阻止 SSL/TLS 会话。
- **2048-bit RSA**（**2,048** 位 **RSA**）— 不管目标服务器证书的密钥大小是什么，防火墙都会生成使用 2,048 位 RSA 密钥和 SHA-256 哈希算法的证书。公共 CA 和常用浏览器支持 2,048 位密钥，此类密钥的安全性高于 1,024 位密钥。

更改密钥大小设置会清除当前证书缓存。

STEP 3 | 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 吊销和续订证书


- 吊销证书
- 续订证书


## 吊销证书

有多种不同情况可能会使得证书在到期之前变成无效。例如，更改证书名称、更改主体和证书颁发机构之间的关联（如员工终止雇用）及泄露（已知或可疑）私钥。在这些情况下，签发证书的证书颁发机构 (CA) 必须吊销证书。以下任务介绍了如何为是 CA 的防火墙吊销证书。

STEP 1 | 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

STEP 2 | 如果防火墙支持多个虚拟系统，该选项卡将会显示 **Location**（位置）下拉列表。选择证书所属的虚拟系统。

STEP 3 | 选择要吊销的证书。

STEP 4 | 单击 **Revoke**（吊销）。PAN-OS 立即将证书的状态设置为吊销，并将序列号添加到在线证书状态协议 (OCSP) 响应者缓存或证书吊销列表 (CRL)。无需执行提交。

## 续订证书

如果证书到期或即将到期，可以重新设置有效期。如果外部证书颁发机构 (CA) 签发证书，且防火墙使用在线证书状态协议 (OCSP) 验证证书吊销状态，则防火墙使用 OCSP 响应者信息更新证书状态（请参阅配置 OCSP 响应者）。如果防火墙是签发证书的 CA，则防火墙将它替换为拥有不同序列号的新证书，但属性与旧证书相同。

STEP 1 | 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

STEP 2 | 如果防火墙具备一个以上的虚拟系统 (vsys)，选择证书 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 3 | 选择要续订的证书并单击 **Renew**（续订）。

STEP 4 | 输入 **New Expiration Interval**（新的到期间隔）（天数）。

STEP 5 | 单击 **OK**（确定）和 **Commit**（提交）。




© 2019 Palo Alto Networks, Inc.

# 安全密钥与硬件安全模块

硬件安全模块 (HSM) 是一种用于管理数字密钥的物理设备。HSM 可提供安全存储和生成数字密钥。它可以同时提供防止未经授权和潜在对手使用这些材料的逻辑和物理保护。

HSM 客户端集成 Palo Alto Networks 防火墙和 Panorama 可增强在 SSL/TLS 解密中使用私钥的安全性（同时用于 SSL 转发代理和 SSL 入站检查）。此外，您也可以使用 HSM 对主密钥进行加密。

以下主题介绍了 HSM 集成 Palo Alto Networks 防火墙或 Panorama 的方法：

- 建立与 HSM 的连接
- 使用 HSM 加密主密钥
- 在 HSM 上存储私钥
- 管理 HSM 部署

## 建立与 HSM 的连接

HSM 客户端与 PA-3200 系列、PA-5200 系列、PA-7000 系列和 VM 系列防火墙以及 Panorama 管理服务器（虚拟设备和 M 系列设备）集成，可用于以下 HSM 供应商：

- **nCipher nShield Connect** — 受支持的客户端版本取决于 PAN-OS 发布版本：
  - PAN-OS 10.0 支持客户端版本 12.40.2（对于较旧的设备，最多向后兼容到版本 11.50）。
  - PAN-OS 9.1、9.0 和 8.1 支持客户端版本 12.30。
  - PAN-OS 8.0 和较低版本支持客户端版本 11.62。
- **SafeNet Network** — 受支持的客户端版本取决于 PAN-OS 发布版本：
  - PAN-OS 10.0 支持客户端版本 5.4.2 和 7.2。
  - PAN-OS 9.1 和 9.0 支持客户端版本 5.4.2 和 6.3。
  - PAN-OS 8.1 支持客户端版本 5.4.2 和 6.2.2。
  - PAN-OS 8.0.2 及 PAN-OS 8.0 更高版本（也包括 PAN-OS 7.1.10 及 PAN-OS 7.1 更高版本）支持客户端版本 5.2.1、5.4.2 和 6.2.2。

HSM 服务器版本必须与这些客户端版本兼容。请参阅 HSM 供应商文档，了解客户端-服务器版本兼容性矩阵。在防火墙或 Panorama 上，使用以下程序选择与 SafeNet HSM 服务器兼容的 SafeNet Network 客户端版本。

*HSM* 服务器升级后，可能无法降级。

- 建立与 SafeNet Network HSM 的连接
- 设置与 nCipher nshield Connect HSM 的连接

- 安装 SafeNet 客户端 RPM 数据包管理器。
  1. 选择 **Device**（设备）> **Setup**（设置）> **HSM**并**Select HSM Client Version**（选择 **HSM** 客户端版本）（硬件安全操作设置）。
  2. 选择适用于您的 HSM 服务器版本的 **Version 5.4.2**（版本 **5.4.2**）（默认）或 **7.2**。
  3. 单击 **OK**（确定）。
  4. （仅当您在防火墙上更改 HSM 版本时需要）如果版本更改成功，防火墙会提示您重启以更改为新的 HSM 版本。如果出现提示，请单击 **Yes**（是）。
  5. 如果主密钥不在防火墙上，则客户端版本更新失败。**Close**（关闭）消息，然后将主密钥本地设置给防火墙：


© 2019 Palo Alto Networks, Inc.

- 编辑硬件安全模块供应商，并禁用（清除） **Master Key Secured by HSM**（**HSM** 加密的主密钥）选项。
- 单击 **OK**（确定）。
- 选择 **Device**（设备） > **Master Key and Diagnostics**（主密钥和诊断），然后编辑主密钥。
- 输入 **Current Master Key**（当前主密钥）；然后，您可以输入相同的密钥作为 **New Master Key**（新主密钥），并 **Confirm New Master Key**（确认主密钥）。
- 单击 **OK**（确定）。
- 重复前四个步骤以 **Select HSM Client Version**（选择 **HSM** 客户端版本），并再次重新启动。

## 建立与 *SafeNet Network HSM* 的连接

要在 Palo Alto Networks 防火墙（HSM 客户端）与 SafeNet Network HSM 服务器之间建立连接，您必须指定服务器的 IP 地址，输入密码以便服务器对防火墙进行身份验证，然后向服务器注册防火墙。配置 HSM 客户端之前，请为 HSM 服务器上的防火墙创建一个分区，然后确认防火墙上的 SafeNet Network 客户端版本是否与您的 SafeNet Network HSM 服务器兼容（请参阅建立于 HSM 的连接）。

在 HSM 和防火墙连接之前，HSM 根据防火墙 IP 地址对防火墙进行身份验证。因此，您必须配置防火墙才能使用静态 IP 地址，而不是通过 DHCP 分配的动态地址。防火墙 IP 地址在运行期间发生更改时，HSM 上的操作将停止工作。

*HSM* 配置在高可用性 *(HA)* 防火墙对端设备之间无法同步。因此，必须在每个对端设备上单独配置 *HSM*。在主动/被动 *HA* 配置中，必须手动执行一次故障转移，以单独配置并对 *HSM* 的每个 *HA* 对端设备进行身份验证。初始手动故障转移后，正常的故障转移功能不需要用户进行互动。

STEP 1 | 定义每个 SafeNet Network HSM 的连接设置。

1. 登录到防火墙 Web 界面，然后选择 **Device**（设备） > **Setup**（设置） > **HSM**。
2. 编辑硬件安全模块供应商设置，并将 **Provider Configured**（配置的供应商）设置为 **SafeNet Network HSM**。
3. **Add**（添加）每个 HSM 服务器，如下所示。高可用性 (HA) HSM 配置至少需要两个服务器；您的集群中最多可拥有 16 个 HSM 服务器。集群中所有 HSM 服务器必须在相同的 SafeNet 版本上运行，且必须分开进行身份验证。若想要复制整个集群中的密钥，应仅使用 SafeNet 集群。或者，您可以最多添加 16 个独立运行的 SafeNet HSM 服务器。
   1. 输入 HSM 服务器的 **Module Name**（模块名称）（最多包含 31 个字符的 ASCII 字符串）。
   2. 输入 HSM **Server Address**（服务器地址）的 IPv4 地址。
4. （仅 HA）选择 **High Availability**（高可用性），指定 **Auto Recovery Retry**（自动恢复重试）值（在故障转移到 HSM HA 对端设备服务器之前 HSM 客户端尝试恢复其与 HSM 服务器连接的最大允许次数；范围为 0 - 500，默认为 0），然后输入 **High Availability Group Name**（高可用性组名称）（最多包含 31 个字符的 ASCII 字符串）。

   如果已配置两个或以上 *HSM* 服务器，最佳实践是启用 *High Availability*（高可用性）。否则，防火墙将不能使用其他 *HSM* 服务器。
5. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 2 | （可选）如果不希望防火墙通过管理接口（默认）进行连接，则配置服务路由以连接到 HSM。

如果为 *HSM* 配置服务路由，则运行 ***clear session all*** *CLI* 命令，这将清除所有现有的 *HSM* 会话，从而导致所有 *HSM* 状态关闭后又重新打开。在 *HSM* 恢复所需的几秒内，所有 *SSL/TLS* 操作均将失败。

1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）并单击 **Service Route Configuration**（服务路由配置）。



© 2019 Palo Alto Networks, Inc.

2. **Customize**（自定义）服务路由。默认情况下，**IPv4** 选项卡处于活动状态。
3. 单击服务列中的 **HSM**。
4. 选择 HSM 的 **Source Interface**（源接口）。
5. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 3 | 配置防火墙以验证 HSM。

1. 选择 **Device**（设备）> **Setup**（设置）**Setup Hardware Security Module**（设置硬件安全模块）。
2. 选择 HSM **Server Name**（服务器名称）。
3. 为身份验证选择 **Automatic**（自动）或**Manual**（手动），并信任证书。
4. 输入**Administrator Password**（管理员密码）以向防火墙验证 HSM。
5. 单击 **OK**（确定）。

   防火墙尝试对 HSM 进行身份验证并显示状态消息。
6. 再次单击 **OK**（确定）。

STEP 4 | 使用 HSM 服务器将防火墙注册为 HSM 客户端，并将防火墙分配给 HSM 服务器上的一个分区。



如果 *HSM* 已经具有已注册相同 *<cl-name>* 的防火墙，则必须首先运行 ***client delete -client <cl-name>*** 命令删除重复注册，其中 *<cl-name>* 是要删除的客户端（防火墙）注册的名称。

1. 从远程系统登录到 HSM。
2. 使用 **`client register -c <cl-name> -ip <fw-ip-addr>`** CLI 命令注册防火墙，其中 *<cl-name>* 是您分配给防火墙以在 HSM 上使用的名称，*<fw-ip-addr>* 是防火墙 IP 地址。
3. 使用 **`client assignpartition -c <cl-name> -p <partition-name>`** CLI 命令将分区分配给防火墙，其中 *<cl-name>* 是在 **`client register`** 命令中分配给防火墙的名称，*<partition-name>* 是您希望分配给防火墙的之前配置的分区的名称。

STEP 5 | 配置防火墙连接到 HSM 分区。

1. 选择 **Device**（设备）> **Setup**（设置）> **HSM** ，然后刷新（）显示。
2. **Setup HSM Partition**（设置 **HSM** 分区）（硬件安全操作设置）。
3. 输入**Partition Password**（分区密码）以向防火墙验证 HSM 上的分区。
4. 单击 **OK**（确定）。

STEP 6 | （仅 HA）重复上一次的身份验证、注册和分区连接步骤，将另一个 HSM 添加到现有 HA 组。



如果从配置中删除 *HSM*，请重复上一个分区连接步骤，从 *HA* 组中移除已删除的 *HSM*。

STEP 7 | 使用 HSM 验证防火墙连接和身份验证。

1. 选择 **Device**（设备）> **Setup**（设置）> **HSM**，并检查身份验证和连接状态：
   - 绿色 — 防火墙已成功通过身份验证并连接到 HSM。
   - 红色 — 防火墙无法对 HSM 进行身份验证，或 HSM 的网络连接失败。
2. 在“硬件安全模块状态”中查看以下列以确定身份验证状态：
   - **Serial Number**（序列号）— 如果防火墙已成功通过 HSM 身份验证，则显示此 HSM 分区的序列号。
   - 分区— 分配到防火墙的 HSM 上的分区名称。
   - **Module State**（模块状态）— HSM 连接的当前状态。如果硬件安全模块状态显示 HSM，该值始终为 `Authenticated`（已进行身份验证）。


© 2019 Palo Alto Networks, Inc.

## 设置与 *nCipher nshield Connect HSM* 的连接

您必须将远程文件系统 (RFS) 设置为中心，以便组织中使用 nCipher nShield Connect HSM 的所有防火墙（HSM 客户端）同步密钥数据。要确保防火墙上的 nShield Connect 客户端版本与 nShield Connect 服务器兼容，请参阅建立与 HSM 的连接。

在 HSM 和防火墙连接之前，HSM 根据防火墙 IP 地址对防火墙进行身份验证。因此，您必须配置防火墙才能使用静态 IP 地址，而不是通过 DHCP 分配的动态地址。（防火墙 IP 地址在运行期间发生更改时，HSM 上的操作将停止工作）。

*HSM* 配置在高可用性 *(HA)* 防火墙对端设备之间无法同步。因此，必须在每个对端设备上单独配置 *HSM*。在主动/被动 *HA* 配置中，必须手动执行一次故障转移，以单独配置并对 *HSM* 的每个 *HA* 对端设备进行身份验证。初始手动故障转移后，正常的故障转移功能不需要用户进行互动。

STEP 1 | 定义每个 nCipher nShield Connect HSM 的连接设置。

1. 登录到防火墙 Web 界面，然后选择 **Device**（设备）> **Setup**（设置）> **HSM**。
2. 编辑硬件安全模块供应商设置，并将 **Provider Configured**（配置的供应商）设置为 **nShield Connect**。
3. **Add**（添加）每个 HSM 服务器，如下所示。HA HSM 配置需要两台服务器。
   1. 输入 HSM 服务器的 **Module Name**（模块名称）。该名称可以是任意 ASCII 字符串，长度最多 31 个字符。
   2. 输入 HSM **Server Address**（服务器地址）的 IPv4 地址。
4. 输入 **Remote Filesystem Address**（远程文件系统地址）的 IPv4 地址。
5. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 2 | （可选）如果不希望防火墙通过管理接口（默认）进行连接，则配置服务路由以连接到 HSM。

如果为 *HSM* 配置服务路由，则运行 ***clear session all*** *CLI* 命令，这将清除所有现有的 *HSM* 会话，从而导致所有 *HSM* 状态关闭后又重新打开。在 *HSM* 恢复所需的几秒内，所有 *SSL/TLS* 操作均将失败。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务）并单击 **Service Route Configuration**（服务路由配置）。
2. **Customize**（自定义）服务路由。默认情况下，**IPv4** 选项卡处于活动状态。
3. 单击服务列中的 **HSM**。
4. 选择 HSM 的 **Source Interface**（源接口）。
5. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 3 | 将防火墙作为 HSM 客户端注册到 HSM 服务器。

此步骤简要介绍了使用 nShield Connect HSM 前面板接口的程序。有关详细信息，请参阅 nCipher 文档。

1. 登录到 nCipher nShield Connect HSM 的前面板显示屏。
2. 使用右侧导航按钮选择 **System**（系统）> **System configuration**（系统配置）> **Client config**（客户端配置）> **New client**（新客户端）。
3. 输入防火墙 IP 地址。
4. 选择 **System**（系统）> **System configuration**（系统配置）> **Client config**（客户端配置）> **Remote file system**（远程文件系统），然后输入设置 RFS 的客户端计算机的 IP 地址。

STEP 4 | 配置 RFS 以接受来自防火墙的连接。

1. 从 Linux 客户端登录到 RFS。



© 2019 Palo Alto Networks, Inc.

2. 通过运行 **anonkneti *<ip-address>*** CLI 命令获取电子序列号 (ESN) 和 $K_{NETI}$ 密钥的哈希，该密钥对客户端的 HSM 进行身份验证。其中，*<ip-address>* 是 HSM IP 地址。

   例如：

   ```
   anonkneti 192.0.2.1
   ```

   ```
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```

   在本例中，`B1E2-2D4C-E6A2` 是 ESN，`5a2e5107e70d525615a903f6391ad72b1c03352` 是 $K_{NETI}$ 密钥的哈希。
3. 通过超级用户帐户使用以下命令设置 RFS：

   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```

   *<Ip-address>* 是 HSM 的 IP 地址；*<ESN>* 是电子序列号；而 *<hash-Kneti-key>* 是 $K_{NETI}$ 密钥的哈希。

   下例使用在此步骤中获得的值：

   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2
    5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. 使用以下命令允许在 RFS 上提交 HSM 客户端：

   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```

   其中，*<FW-IPaddress>* 是防火墙 IP 地址。

STEP 5 | 对 HSM 的防火墙进行身份验证。

1. 从防火墙 Web 界面中，选择 **Device**（设备）> **Setup**（设置）> **HSM**，并 **Setup Hardware Security Module**（设置硬件安全模块）。
2. 单击 **OK**（确定）。

   防火墙尝试对 HSM 进行身份验证并显示状态消息。
3. 单击 **OK**（确定）。

STEP 6 | 将防火墙与 RFS 同步，方法是选择 **Device**（设备）> **Setup**（设置）> **HSM**，并 **Synchronize with Remote Filesystem**（与远程文件系统进行同步）。

STEP 7 | 使用 HSM 验证防火墙连接和身份验证。

1. 选择 **Device**（设备）> **Setup**（设置）> **HSM**，并检查身份验证和连接状态：
   - 绿色 — 防火墙已成功通过身份验证并连接到 HSM。
   - 红色 — 防火墙无法对 HSM 进行身份验证，或 HSM 的网络连接失败。
2. 检查硬件安全模块状态以确定身份验证状态。
   - **Name**（名称）— HSM 的名称。
   - **IP Address**（IP 地址）— HSM 的 IP 地址。
   - **Module State**（模块状态）— HSM 连接的当前状态：`Authenticated`（已验证）或 `NotAuthenticated`（未验证）。


© 2019 Palo Alto Networks, Inc.

# 使用 HSM 加密主密钥

主密钥对防火墙和 Panorama 上的所有私钥和密码进行加密处理。如果安全要求规定将私钥存储在安全位置，则可以使用存储在 HSM 上的加密密钥对主密钥进行加密。然后，防火墙或 Panorama 要求 HSM 在需要对防火墙上的密码或私钥进行解密时解密主密钥。通常，为了增加安全性，将 HSM 安装在与防火墙或 Panorama 隔开的高度安全位置。

HSM 使用包装密钥对主密钥进行加密。为保持安全，必须偶尔更改（刷新）此包装密钥。

在 *FIPS/CC* 模式下配置的防火墙不支持使用 *HSM* 加密主密钥。

以下主题介绍如何对主密钥进行初始加密以及如何刷新主密钥加密：

- 加密主密钥
- 刷新主密钥加密

## 加密主密钥

如果之前尚未在防火墙上对主密钥进行加密，请使用以下步骤进行加密。如果第一次对密钥进行加密，或者如果已经定义新密钥且想要对它进行加密，都可以使用此步骤。如果要刷新有关之前加密密钥的加密，请参阅刷新主密钥加密。

STEP 1 | 选择 **Device**（设备）> **Master Key and Diagnostics**（主密钥和诊断）。

STEP 2 | 在 **Master Key**（主密钥）字段中，指定当前用来对防火墙中所有私钥和密码进行加密的密钥。

STEP 3 | 如果更改主密钥，请输入新的主密钥并确认。

STEP 4 | 选中 **HSM** 复选框。

- **Life Time**（生命周期）— 指定主密钥过期之前的天数和小时数（范围为 1-730 天）。
- **Time for Reminder**（提醒时间）— 指定过期之前向用户通知即将过期的天数和小时数（范围为 1-365 天）。

STEP 5 | 单击 **OK**（确定）。

## 刷新主密钥加密

最佳实践是通过旋转为其加密的包装密钥来定期刷新主密钥加密。旋转的频率取决于应用程序。包装密钥位于您的 HSM 上。以下命令对于 SafeNet Network 和 nCipher nShield Connect HSM 均相同。

STEP 1 | 登录至防火墙 CLI。

STEP 2 | 使用以下 CLI 命令可在 HSM 上对主密钥的包装密钥进行循环位移：

```
> request hsm mkey-wrapping-key-rotation
```

如果已经在 HSM 上加密主密钥，则 CLI 命令将会在 HSM 上生成新的包装密钥，并使用它来对主密钥进行加密。

如果尚未在 HSM 上加密主密钥，则 CLI 命令将会在 HSM 上生成新的包装密钥供将来使用。

此命令不会删除旧的包装密钥。



© 2019 Palo Alto Networks, Inc.

# 在 HSM 上存储私钥

为了增强安全性,您可以使用 HSM 为以下程序确保 SSL/TLS 解密中使用的私钥的安全：

- SSL 转发代理 — HSM 可存储用来在 SSL/TLS 转发代理操作中签发证书的转发信任证书的私钥。然后，防火墙将在该操作期间生成的证书发送到 HSM 进行签名，随后再转发到客户端。
- SSL 入站检查 — HSM 可以存储用来执行 SSL/TLS 入站检查的内部服务器私钥。

如果使用 DHE 或 ECDHE 密钥交换算法来启用用于 SSL 解密的完全正向保密 (PFS)，则不能使用 HSM 来存储 SSL 入站检查的私钥。除非您正在使用 TLSv1.3，否则您还可以使用 HSM 存储用于 SSL 转发代理或 SSL 入站检查解密的 ECDSA 密钥。对于 TLSv1.3 流量， PAN-OS 仅支持 SSL 转发代理的 HSM。它不支持 SSL 入站检测的 HSM。

STEP 1 | 在 HSM 上导入或生成用于解密部署的证书和私钥。

有关在 HSM 上导入或生成证书和私钥的说明，请参阅 HSM 文档。

STEP 2 | （仅限 nCipher nShield Connect）将 nCipher nShield 远程文件系统的密钥数据同步至防火墙。



与 *SafeNet Network HSM* 的同步为自动完成。

1. 访问防火墙 Web 界面，然后选择 **Device**（设备）> **Setup**（设置）> **HSM**。
2. **Synchronize with Remote Filesystem**（与远程文件系统进行同步）（硬件安全操作设置）。

STEP 3 | 导入与存储在 HSM 的密钥对应的证书。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Import**（导入）。
2. 输入 **Certificate Name**（证书名称）。
3. **Browse**（浏览）到 HSM 上的 **Certificate File**（证书文件）。
4. 选择 **File Format**（数据格式）：
5. 选择 **Private Key resides on Hardware Security Module**（硬件安全模块上的私钥）。
6. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 4 | （仅限转发信任证书）启用在 SSL/TLS 转发代理中使用的证书。

1. 打开在步骤 3 中导入的证书进行编辑。
2. 选择 **Forward Trust Certificate**（转发信任证书）。
3. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 5 | 验证是否成功地将证书导入到防火墙。

找到在步骤 3 中导入的证书，然后在 Key（密钥）列中检查图标：

- 锁定图标 — 证书的私钥存储在 HSM 上。
- 错误图标 — 私钥未存储在 HSM 上或者未正确验证或连接 HSM。

# 管理 HSM 部署

您可以执行以下任务来管理 HSM 部署：

- 查看 HSM 配置设置。

  选择 **Device**（设备）> **Setup**（设置）> **HSM**。

- 显示详细的 HSM 信息。



© 2019 Palo Alto Networks, Inc.

从“硬件安全操作”部分中选择 **Show Detailed Information**（显示详细信息）。

将会显示有关 HSM 服务器、HSM 高可用性状态和 HSM 硬件的信息。

- 导出支持文件。

  从 Hardware Security Operations（硬件安全操作）部分中选择 **Export Support File**（导出支持文件）。

  将会创建测试文件帮助客户在使用防火墙的 HSM 配置解决问题时提供支持。

- 重置 HSM 配置。

  从“硬件安全操作”部分中选择 **Reset HSM Configuration**（重置 **HSM** 配置）。

  选择此选项将会删除所有 HSM 连接。在使用此选项后，必须重复所有身份验证步骤。

# 高可用性

高可用性 (HA) 是一种部署，在该部署中，两个防火墙结合成组或最多 16 个防火墙置于一个 HA 集群中，且其配置保持同步，从而防止网络上出现单点故障。防火墙对等端之间的检测信号连接可以确保当某个对等端关闭时提供无缝故障转移。设置 HA 可提供冗余，并且可以确保业务连续性。


> HA 概述
> HA 概念
> 设置主动/被动 HA
> 设置主动/主动 HA
> HA 集群概述
> HA 集群最佳实践和配置
> 配置 HA 集群
> 刷新 HA1 SSH 密钥和配置密钥选项
> HA 防火墙状态
> 引用：HA 同步
> CLI 速查表 - HA

# HA 概述

您可以将两个 Palo Alto Networks 防火墙配置为 HA 对，或是最多配置 16 个防火墙作为 HA 集群的对等成员。集群中的对等设备可以是 HA 对，也可以是独立防火墙。设置 HA 后，便可以确保在对等防火墙出现故障时有备用防火墙可用，从而最大程度地减少停机时间。HA 对中的防火墙或集群可使用防火墙上的专用或带内 HA 端口来同步数据（网络、对象和策略配置）并维护状态信息。管理端口 IP 地址或管理员配置文件等设备特定配置、HA 特定配置、日志数据和应用程序命令中心 (ACC) 信息不会在对等设备之间共享。

若要查看整个 HA 对的合并应用程序和日志视图，必须使用 Panorama，即 Palo Alto Networks 集中式管理系统。请查阅《Panorama 管理员指南》中的《环境切换—防护墙或 Panorama》。咨询 主动/被动 HA 的先决条件 和 主动/主动 HA 的先决条件。强烈建立您使用 Panorama 配置 HA 集群成员。咨询 HA 集群最佳实践和配置。

当 HA 对或 HA 集群中的一道防火墙出现故障，对等防火墙接管保护通信的任务时，该事件称为故障转移。触发故障转移的条件有：

- 监视的一个或多个接口发生故障。（链接监视）
- 无法到达防火墙上指定的一个或多个目标。（路径监视）
- 防火墙不响应检测信号轮询。（检测信号轮询和呼叫消息）
- 重要芯片或软件组件故障，被称为数据包路径健康监控。

Palo Alto Networks 防火墙支持状态主动/被动或主动/主动高可用性，同时支持会话和配置同步，但以下除外：

- Azure 上的 VM 系列防火墙 和 AWS 上的 VM 系列防火墙 仅支持主动/被动 HA。

  在 AWS 上，当您通过 Amazon 弹性负载均衡 (ELB) 服务部署防火墙时，不支持 HA（此情况下，ELB 服务提供故障转移功能）。
- Google 云平台上的 VM 系列防火墙不支持 HA。

如果要配置 HA 集群，请先了解 HA 概念和 HA 集群概述。



© 2019 Palo Alto Networks, Inc.

# HA 概念

以下主题介绍了 HA 如何在 Palo Alto Networks 防火墙运作的概念性信息：


- HA 模式
- HA 链路和备份链路
- 设备优先级和抢先
- 故障转移
- 主动/被动 HA 的 LACP 及 LLDP 预先协商
- 浮动 IP 地址和虚拟 MAC 地址
- ARP 加载共享
- 基于路由的冗余
- 高可用性计时器
- 会话所有者
- 会话设置
- 处于主动/主动模式的 NAT
- 处于主动/主动 HA 模式的 ECMP


## HA 模式

您可以按照以下两种模式来设置 HA 对中的防火墙：

- 主动/被动 — 一个防火墙主动管理通信，而另一个防火墙保持同步并随时准备在主动设备发生故障时转换为主动状态。在此配置中，两个防火墙共享相同的配置设置，一台主动管理通信，直到发生路径、链接、系统或网络故障。当主动防火墙发生故障时，被动设备将无缝接管并实施相同的策略，以维持网络的安全性。主动/被动高可用性在 Virtual Wire、第 2 层和第 3 层部署中受支持。
- 主动/主动 — HA 对中的两个防火墙都是主动设备，同时处理通信，并且同步处理会话设置和会话所有权。两个防火墙会分别获取会话表及路由表，并彼此进行同步。主动/主动高可用性在 Virtual Wire、第 2 层和第 3 层部署中受支持。

  处于主动/主动 HA 模式的防火墙不支持 DHCP 客户端。而且，仅主动-主要防火墙具备 DHCP 中继功能。主动-辅助防火墙会丢弃其收到的 DHCP 广播数据包。



主动/主动配置不会加载平衡通信。虽然可通过发送通信至对等加载共享，但不会发生负载平衡。可通过 *ECMP*、多个 *ISP* 及负载均衡器加载共享会话至两道防火墙。

在决定是使用主动/被动还是主动/主动模式时，请考虑以下差异：

- 主动/被动模式设计简单；该模式下，能更轻松地解决路由及通信流问题。主动/被动模式支持第 2 层部署；主动/主动模式不支持。
- 主动/主动模式需要能构建复杂性更高的网络的高级设计概念。根据实施主动/主动 HA 的方式，可能需要额外配置，如激活两道防火墙的联网协议、复制 NAT 池、部署浮动 IP 地址等，从而提供相应的故障转移。由于两个防火墙均在主动处理通信，防火墙使用会话所有者及会话设置概念执行第 7 层内容检查。如果防火墙分别需要各自的路由实例，且您需要防火墙始终输出完整、实时的冗余，则建议您使用主动/主动模式。主动/主动模式下，故障转移的速度更快，此外，两个防火墙均会主动处理流通信，因此，较之主动/被动模式，其能更好地处理最大通信流。



主动/主动模式下，*HA* 对可用于临时处理通信，且其处理的通信量较一个防火墙正常情况下处理的更大。但这并非绝对的，原因是如果一个防火墙发生故障，流量便会重定向流至 *HA* 对中的另一道防火墙。您的设计必须让另一个防火墙能够处理最大通信负载，同时启用内容检查。如果设计为另一个防火墙订阅的通信处理能力过大，则可能导致高延迟和/或应用程序故障。



© 2019 Palo Alto Networks, Inc.

有关在主动/被动模式中防火墙设置的信息，请参阅设置主动/被动 HA。有关在主动/主动模式中防火墙设置的信息，请参阅设置主动/主动 HA。

在 HA 集群中，所有成员均处于活跃状态，集群中没有被动防火墙这一说（HA 对除外），这样，可在将其添加到 HA 集群后，确保他们的主动/被动关系。

## HA 链路和备份链路

HA 对中的防火墙使用 HA 链接 同步数据和维护状态信息。某些型号的防火墙有专用 HA 端口：控制链路 (HA1) 和数据链路 (HA2)，而其他防火墙则要求使用带内端口作为 HA 链接。

- 对于具有专用 HA 端口的防火墙，请使用这些端口来管理防火墙之间的通信和同步。有关详细信息，请参阅 Palo Alto Networks 防火墙上的 HA 端口。
- 对于没有专用 HA 端口的防火墙，例如 PA-220 和 PA-220R 防火墙，最佳实践是使用 HA1 端口的管理端口，并将数据面板端口用作 HA1 备份。



对于没有专用 *HA* 端口的防火墙，请根据您的环境以及您了解的最不常使用和最不拥挤的端口来决定要用于 *HA1* 和 *HA1* 备份的端口。将 *HA1* 分配给最佳接口，将 *HA1* 备份分配给另一个接口。

集群中的 HA 对等可以是独立集群成员和 HA 对的组合。HA 集群成员使用 HA4 和 HA4 备份链路执行会话状态同步。非 HA 对的集群成员之间不支持 HA1（控制链路）、HA2（数据链路）和 HA3（数据包转发链路）。

| HA 链路和备份链路 | 说明 |
|---|---|
| 控制链接 | HA1 链接用于交换呼叫消息、检测信号和 HA 状态信息，以及路由和 User-ID 信息的管理面板同步。防火墙亦使用该链接与其对等设备同步配置更改。HA1 链接是一个第 3 层链接，需要 IP 地址。<br>ICMP 用于交换 HA 对等设备之间的检测信号。<br>HA1 使用端口 — 使用 TCP 端口 28769 和 28260 进行明文通信；使用端口 28 进行加密通信 (SSH over TCP)。<br>如果您在 HA1 链路上启用了加密，您也可以 刷新 HA1 SSH 密钥和配置密钥选项。 |
| 数据链路 | HA2 链接用于在 HA 对中的防火墙之间同步会话、转发表、IPSec 安全关联和 ARP 表。HA2 链接上的数据流始终是单向的（“HA2 保持活动状态”除外）；它从主动防火墙流动到被动防火墙。HA2 链接是第 2 层链接，它在默认情况下使用以太网类型 0x7261。<br>HA2 使用端口 — 可以将 HA 数据链路配置为使用 IP（协议号 99）或 UDP（端口 29281）进行传输，因此允许 HA 数据链路跨越子网。 |
| HA1 和 HA2 备份链路 | 为 HA1 和 HA2 链接提供冗余。当专用备份链接不可用时，带内端口可用于 HA1 和 HA2 连接的备份链接。当配置备份 HA 链接时，请注意以下原则：<br>• 主要和备份 HA 链接的 IP 地址不得互相重叠。<br>• HA 备份链接必须位于与主要 HA 链接不同的子网上。<br>• 必须在单独的物理端口上配置 HA1 备份和 HA2 备份端口。HA1 备份链路使用端口 28770 和 28260。<br>• PA-3200 系列防火墙不支持 HA1 备用链路的 IPv6 地址；请使用 IPv4 地址。 |



© 2019 Palo Alto Networks, Inc.

| HA 链路和备份链路 | 说明 |
| --- | --- |
| | 如果对 *HA1* 或 *HA1* 备份链路使用带内端口，*Palo Alto Networks* 建议启用检测信号备份（在 *MGT* 接口上使用端口 *28771*）。 |
| 数据包转发链路 | 除 HA1 和 HA2 链路外，主动/主动部署还需要专用的 HA3 链路。在会话设置及非对称通信流处理期间，防火墙使用 HA3 链路将数据包转发至对等设备。HA3 链路是一个第 2 层链路，使用 MAC 套 MAC 封装。它不支持第 3 层定址或加密。PA-7000 系列防火墙将一对一地同步 NPC 中的会话。在 PA-800 系列、PA-3200 系列和 PA-5200 系列防火墙上，您可将聚合接口配置为 HA3 链路。集成接口还可为 HA3 链路提供冗余，您不能为 HA3 链路配置备份链路。在 PA-3200 系列、PA-5200 系列和 PA-7000 系列防火墙上，专用 HSCI 端口支持 HA3 链路。防火墙会将专有数据包标头添加至正在穿越 HA3 链路的数据包，因此通过该链路的 MTU 必须大于所转发的最大数据包长度。 |
| HA4 链路和 HA4 备份链路 | HA4 链路和 HA4 备份链路针对具有相同集群 ID 的所有 HA 集群成员执行会话缓存同步。集群成员之间的 HA4 链路通过发送和接收第二层 keepalive 消息，检测集群成员之间发生的连接故障。查看防火墙仪表板上 HA4 和 HA4 备份链路的状态。 |

## *Palo Alto Networks* 防火墙上的 *HA* 端口

在高可用性 (HA) 配置中将两个 Palo Alto Networks® 防火墙进行连接时，我们建议您使用专用 HA 端口进行 HA 链接和备份链接。这些专用端口包括：用于 HA 控制和同步流量且标记为 HA1、HA1-A 和 HA1-B 的 HA 1 端口，HA2，以及用于 HA 会话建立流量的高速机箱互联 (HSCI) 端口。PA-5200 系列防火墙具有可用于配置 HA1 流量且标记为 AUX-1 和 AUX-2 的多用途辅助接口。

此外，您还可以为 HA 3 配置 HSCI 端口。该端口可用于在会话建立和对称通信流动期间将数据包转发至对等防火墙（仅限主动/主动 HA）。HSCI 端口可用于 HA2 流量、HA3 流量，或两者都可以。

*HA1* 和 *AUX* 链路可以使管理平面上的功能保持同步。相对于使用带内端口，使用管理面板上的专用 *HA* 端口进行管理的效率更高，因为不需要将同步数据包传递到数据面板。

如果防火墙没有专用 HA 端口，可以将数据端口配置为 HA 端口。如果防火墙有专用 HA 端口，但不具备专用 HA 备用端口，则还可以将数据端口配置为专用 HA 端口的备份。

只要有可能，请直接在 *HA* 对中将两道防火墙之间的 *HA* 端口直接连接（而不是通过交换机或路由器），以避免在发生网络问题时引发 *HA* 链路和通信问题。

使用下表了解专用 HA 端口以及如何连接 HA 链接和备份链接：

| 模型 | 前面板专用接口 |
| --- | --- |
| PA-800 系列防火墙 | • **HA1** 和 **HA2**— 在 HA 模式下用于 HA1 和 HA2 的以太网 10Mbps/100Mbps/1000Mbps 端口。<br>  • 对于 **HA1** 流量— 将该对中第一道防火墙的 HA1 端口直接连接到第二道防火墙的 HA1 端口，或者通过交换机或路由器将这些端口连接在一起。<br>  • 对于 **HA2** 流量— 将该对中第一道防火墙的 HA2 端口直接连接到第二道防火墙的 HA2 端口，或者通过交换机或路由器将这些端口连接在一起。 |


© 2019 Palo Alto Networks, Inc.

| 模型 | 前面板专用接口 |
| --- | --- |
| PA-3200 系列防火墙 | • **HA1-A and HA1-B**（**HA1-A** 和 **HA1-B**）—在 HA 模式下用于 HA1 流量的以太网 10Mbps/100Mbps/1000Mbps 端口。<br>  • 对于 **HA1** 流量— 将该对中第一道防火墙的 HA1-A 端口直接连接到第二道防火墙的 HA1-A 端口，或者通过交换机或路由器将这些端口连接在一起。<br>  • **For a backup to the HA1-A connection**（对于**HA1-A** 连接备份）—将该对中第一道防火墙的 HA1-B 端口直接连接到第二道防火墙的 HA1-B 端口，或者通过交换机或路由器将这些端口连接在一起。<br>   如果防火墙数据平面因故障而重启或经手动重启，*HA1-B* 链路也将随之重新启动。如果发生这种情况，且未连接和配置 *HA1-A* 链路，则会发生脑裂状况。因此，我们建议您连接并配置 *HA1-A* 端口和 *HA1-B* 端口以提供冗余，避免脑裂问题。<br>   您可以通过 *PAN-OS* 或 *Panorama* 将防火墙的 *SFP* 端口重新映射为 *HA1-A* 和 *HA1-B* 端口。<br>• **HSCI** — HSCI 端口是在 HA 配置中连接两个 PA-3200 系列防火墙的第一层 SFP+ 接口。将此端口用于 HA2 连接、HA3 连接或两者连接。<br>HSCI 端口上承载的流量是原始的第一层流量，不能路由，不能切换。因此，您必须将 HSCI 端口相互进行直接连接（从第一道防火墙的 HSCI 端口到第二道防火墙的 HSCI 端口）。 |
| PA-5200 系列防火墙 | • **HA1-A and HA1-B**（**HA1-A** 和 **HA1-B**）—在 HA 模式下用于 HA1 流量的以太网 10Mbps/100Mbps/1000Mbps 端口。<br>  • 对于 **HA1** 流量— 将该对中第一道防火墙的 HA1-A 端口直接连接到第二道防火墙的 HA1-A 端口，或者通过交换机或路由器将这些端口连接在一起。<br>  • **For a backup to the HA1-A connection**（对于**HA1-A** 连接备份）—将该对中第一道防火墙的 HA1-B 端口直接连接到第二道防火墙的 HA1-B 端口，或者通过交换机或路由器将这些端口连接在一起。<br>• **HSCI** — HSCI 端口是在 HA 配置中连接两个 PA-5200 系列防火墙的第一层接口。将此端口用于 HA2 连接、HA3 连接或两者连接。<br>   *PA-5220* 防火墙上的 *HSCI* 端口是 *QSFP+* 端口，而 *PA-5250*、*PA-5260* 和 *PA-5280* 防火墙上的端口是 *QSFP28* 端口。<br>HSCI 端口上承载的流量是原始的第一层流量，无法路由或切换。因此，您必须将 HSCI 端口相互进行直接连接（从第一道防火墙的 HSCI 端口到第二道防火墙的 HSCI 端口）。 |
| PA-5200 系列防火墙（续） | • **AUX-1** 和 **AUX-2** — 辅助 SFP+ 端口是多用途端口，既可以为 HA1 配置管理功能，又能将日志转发至 Panorama。当您需要其中某一个功能进行光纤连接时，请使用这些端口。<br>  • 对于 **HA1** 流量— 将该对中第一道防火墙的 AUX-1 端口直接连接到第二道防火墙的 AUX-1 端口，或者通过交换机或路由器将这些端口连接在一起。 |



© 2019 Palo Alto Networks, Inc.

| 模型 | 前面板专用接口 |
| --- | --- |
| | • **For a backup to the AUX-1 connection**（对于**AUX-1** 连接备份）—将该对中第一道防火墙的 AUX-2 端口直接连接到第二道防火墙的 AUX-2 端口，或者通过交换机或路由器将这些端口连接在一起。 |
| PA-7000 系列防火墙 | • **HA1-A and HA1-B**（**HA1-A** 和 **HA1-B**）—在 HA 模式下用于 HA1 流量的以太网 10Mbps/100Mbps/1000Mbps 端口。<br>  • 对于 **HA1** 流量— 将该对中第一道防火墙的 HA1-A 端口直接连接到第二道防火墙的 HA1-A 端口，或者通过交换机或路由器将这些端口连接在一起。<br>  • **For a backup to the HA1-A connection**（对于**HA1-A** 连接备份）—将该对中第一道防火墙的 HA1-B 端口直接连接到第二道防火墙的 HA1-B 端口，或者通过交换机或路由器将这些端口连接在一起。<br>  不能在 *NPC* 数据端口或管理 *(MGT)* 端口上配置 *HA1* 连接。<br>• **HSCI-A** 和 **HSCI-B**— HSCI 端口是在 HA 配置中连接两个 PA-7000 系列防火墙的第一层 SFP+ 接口。将这些端口用于 HA2 连接、HA3 连接或两者连接。<br>HSCI 端口上承载的流量是原始的第一层流量，不能路由，不能切换。因此，必须按照以下方式连接这些端口：<br>  • 对于 **HA2** 和 **HA 3** 流量— 将第一道防火墙上的 HSCI-A 端口直接与第二道防火墙上的 HSCI-A 端口相连接。<br>  对于 *HA2* 或 *HA2/HA3* 流量，*PA-7000* 系列防火墙将一对一地同步 *NPC* 中的会话。<br>  • 对于 **HSCI-A** 连接备份— 将第一道防火墙上的 HSCI-B 端口直接与第二道防火墙上的 HSCI-B 端口相连接。<br>*HA2* 和 *HA2* 备份链路可以配置为使用数据面板接口，而不是 *HSCI* 端口。但是，如果按照此种方式配置，*HA2* 和 *HA2* 备份链路都需要使用数据面板接口。*HA2* 或 *HA2* 备份混合使用数据面板端口和 *HSCI* 端口将导致提交失败。这适用于 *PA-7050-SMC*、*PA-7080-SMC*、*PA-7050-SMC-B* 和 *PA-7080-SMC-B*。 |

## 设备优先级和抢先

可以为主动-被动 HA 对中的防火墙分配设备优先级值，以指示优先选择哪道防火墙来承担主动角色或主动角色。如果您需要使用 HA 对中的特定防火墙来主动保护通信安全，则必须在两道防火墙上启用抢先行为，并为每道防火墙分配一道防火墙优先级值。具有较低数值，从而具有较高优先级的防火墙将被指定为主动。另一道防火墙则为被动设备。

这对于主动-主动同样适用；但是，设备 *ID* 将用于分配设备优先级值。类似地，设备 ID 中的较低数值对应较高优先级。具有较高优先级的防火墙变为主动-主要防火墙，配对防火墙变为主动-次要防火墙。

默认情况下，抢先在防火墙上是禁用的，并且必须在两道防火墙上同时启用。启用后，抢先行为将允许具有较高优先级（较低数值）的防火墙在从故障中修复后恢复为主动或主动-主要角色。当发生抢先行为时，该事件会记录在系统日志中。


© 2019 Palo Alto Networks, Inc.

# 故障转移

当一道防火墙发生故障，且 HA 对中的对等设备（或 HA 集群中的对等设备）接管保护流量的任务时，该事件称为故障转移。例如，当 HA 对中的防火墙监视的指标失败时，将触发故障转移。防火墙为检测防火墙故障而监控的指标有：

- 检测信号轮询和呼叫消息

  防火墙使用呼叫消息和检测信号来验证对等防火墙是否有响应和是否可操作。呼叫消息以配置的呼叫间隔从一个对等设备发送到另一个对等设备，以验证防火墙的状态。检测信号是通过控制链路对 HA 对等端进行的 ICMP ping 操作，对等端响应 ping 操作以确定该防火墙已连接并且有响应。默认情况下，检测信号的间隔是 1000 毫秒。每 1000 毫秒发送一次 ping，如果检测信号连续丢失三次，则发生故障转移。有关触发故障转移的高可用性计时器的详细信息，请参阅 HA 计时器。
- 链接监视

  您可以指定防火墙将要监控的一组物理接口（链路组），然后防火墙将监控组内各个链路的状态（上行链路或下行链路）。您可以确定链路组的故障条件：组内 **Any**（任何）下行链路或 **All**（所有）下行链路构成链路组失效（但不一定是故障转移）。

  您可以创建多个链路组。因此，您还可以确定一组链路组的故障条件：**Any**（任何）链路组失败或 **All**（所有）链路组失效（这决定了何时触发故障转移）。默认行为是，**Any**（任何）链路组中的 **Any**（任何）一个链路出现故障都会导致防火墙将 HA 状态更改为非运行（或在主动/主动模式下更改为试验状态），从而指示监视的对象出现故障。
- 路径监视

  您可以指定防火墙要监控的 IP 地址的目标 IP 组。防火墙使用 ICMP ping 监控从网络到任务关键型 IP 地址的所有路径，从而验证 IP 地址的可访问性。ping 操作的默认间隔是 200ms。一旦连续 10 次 ping 操作（默认值）都失败，则该 IP 地址被视为不可访问。您可以指定目标 IP 组中 IP 地址的故障条件：组内 **Any**（任何）IP 地址不可访问或是 **All**（所有）IP 地址不可访问。您可以为虚拟线路、VLAN 或虚拟路由器的路径组指定多个目标 IP 组；您可以指定路径组中目标 IP 组的故障条件：**Any**（任何）或 **All**（所有）（构成路径组失效）。您可以配置多个虚拟线路路径组、VLAN 路径组和虚拟路由器路径组。

  您还可以确定全局故障条件：**Any**（任何）路径组失效或 **All**（所有）路径组失效（这决定了何时触发故障转移）。默认行为是，**Any**（任何）虚拟线路、VLAN 或虚拟路由器路径组的 **Any**（任何）目标 IP组中的**Any**（任何）一个 IP 地址不可访问都会导致防火墙将 HA 状态更改为非运行（或在主动/主动模式下更改为试验状态），从而指示监视的对象出现故障。

除了以上列出的故障转移触发条件外，当管理员将设备置于挂起状态或者发生抢先时，也会发生故障转移。

在 PA-3200 系列、PA-5200 系列和 PA-7000 系列防火墙上，当内部健康检查失败时可能会发生故障转移。此健康检查不可配置，用于监控 FPGA、CPU 等重要组件。此外，常规健康检查会在引起故障转移的任何平台上进行。

以下描述了作为 HA 集群成员的 PA-7000 系列防火墙上的网络处理卡 (NPC) 发生故障时的情形：

- 一旦用于保留 HA 集群会话缓存（其他成员会话副本）的 NPC 出现故障，防火墙将无法正常运行。发生这种情况后，会话分发设备（例如，负载均衡器）必须检测防火墙是否关闭，并将会话负载分发给其他集群成员。
- 如果集群成员的 NPC 发生故障，且该 NPC 并未启用链路监视或路径监视，PA-7000 系列防火墙成员将保持正常运行，但容量会降低，原因是有一个 NPC 发生故障。
- 如果集群成员的 NPC 发生故障，且该 NPC 已启用链路监视或路径监视，PA-7000 系列防火墙将无法运行，且会话分发设备（例如，负载均衡器）必须检测防火墙是否关闭，并将会话负载分发给其他几圈成员。



© 2019 Palo Alto Networks, Inc.

## 主动/被动 HA 的 LACP 及 LLDP 预先协商

如果防火墙使用 LACP 或 LLDP 协议，这些协议在发生故障转移时的协商可次秒级故障转移。尽管如此，您可以启用被动防火墙上的接口，在故障转移前进行 LACP 和 LLCP 协商。因此，处于被动或非运行 HA 状态的防火墙可使用 LACP 或 LLDP 与相邻设备进行通信。此预先协商可加速故障转移过程。

除 VM 系列防火墙以外的所有防火墙型号都支持预协商配置，但这取决于以太网或 AE 端口是否为第 2 层、第 3 层或虚拟线路部署。HA 被动防火墙以以下两种方式中的一种处理 LACP 和 LLDP 数据包：

- 主动 — 防火墙已在端口配置 LACP 或 LLCP，并主动参与 LACP 或 LLCP 预先协商。
- 被动 — 端口未配置 LACP 或 LLDP，防火墙不参与协议，但允许防火墙任一端的对等分别预先协商 LACP 或 LLDP。

下表显示的是聚合以太网 (AE) 和以太网接口支持的部署。

| 接口部署 | AE 接口 | 以太网接口 |
|---|---|---|
| 第 2 层中的 LACP | 活跃 | 不支持 |
| 第 3 层中的 LACP | 活跃 | 不支持 |
| 虚拟线路中的 LACP | 不支持 | 被动 |
| 第 2 层中的 LLDP | 活跃 | 活跃 |
| 第 3 层中的 LLDP | 活跃 | 活跃 |
| 虚拟线路中的 LLDP | 活跃 | • 如果已配置 LLDP，则是主动。<br>• 如果未配置 LLDP，则是被动。 |

子接口和隧道接口不支持预先协商。

要配置 LACP 或 LLDP 预先协商，请参阅（可选）如果您的网络使用 LACP 或 LLDP，请启用主动/被动 HA 的 LACP 及 LLDP 预先协商，以实现超快的故障转移中的步骤。

## 浮动 IP 地址和虚拟 MAC 地址

在 HA 主动/主动模式的第 3 层部署中，如果出现链路或防火墙故障，您可以分配浮动 IP 地址，从一个 HA 防火墙移动至另一个防火墙。拥有该浮动 IP 地址的端口将使用虚拟 MAC 地址对 ARP 请求做出响应。

如果您需要虚拟路由器冗余协议 (VRRP) 等功能时，则建议使用浮动 IP 地址。浮动 IP 地址还可用于实施 VPN 及源 NAT，在提供这些服务的设备发生故障时仍然允许持久连接。

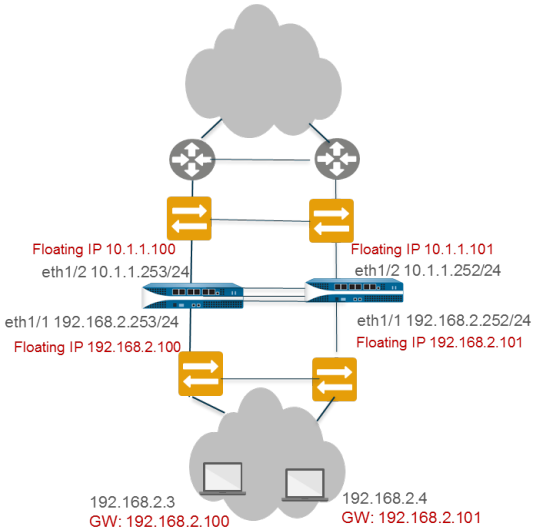
如下图所示，每个 HA 防火墙接口都拥有各自的 IP 地址及浮动 IP 地址。在防火墙出现故障时，防火墙的接口 IP 地址始终为本地，但浮动 IP 地址会在防火墙间移动。配置终端主机以将浮动 IP 地址用作其默认网关，以便加载均衡通信至两个 HA 对等。您亦可使用外部负载均衡器加载均衡通信。

如果链路或防火墙出现故障，或者路径监控事件导致故障转移，浮动 IP 地址和虚拟 MAC 地址会迁移至正常运行的防火墙。（如下表，每个防火墙均有两个浮动 IP 地址及虚拟 MAC 地址；它们均会在防火墙故障时发生迁移。）正常运行的防火墙将发送 Gratuitous ARP 以更新已连接交换机的 MAC 表，通知交换机浮动 IP 地址及 MAC 地址所有权的更改，从而重定向流量至自身。

在故障防火墙恢复运作后，默认情况下，浮动 IP 地址及虚拟 MAC 地址会根据浮动 IP 地址绑定的设备 ID [0 或 1] 迁移回该防火墙。更具体地说，恢复后的故障防火墙将重新运作。当前的主动防火墙会判定该防火墙恢复运行，并核对其处理的浮动 IP 是属于它自己还是其他防火墙。如果浮动 IP 地址最初与其他设备 ID 绑


© 2019 Palo Alto Networks, Inc.

定，则防火墙会将其返回至其他设备 ID。（了解该默认行为的备选操作，请查阅用例：配置具有绑定至主动-主要防火墙的浮动 IP 地址的主动/主动 HA。）




HA 对中的每个防火墙会为其具备浮动 IP 地址或 ARP 加载共享 IP 地址的所有接口创建 MAC 地址。

防火墙（除 PA-7000、PA-5200 和 PA-3200 系列防火墙）的虚拟 MAC 地址的格式为 00-1B-17-00-xx-yy，其中 00-1B-17 为供应商 ID（此处的供应商为 Palo Alto Networks），00 为固定的，xx 为下图所示的设备 ID 和组 ID，yy 为接口 ID：

| 7 | 6 | 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 |
|---|---|---|---|
| Device-ID | 0 | 群组 ID | 接口 ID |

PA-7000、PA-5200 和 PA-3200 系列防火墙的虚拟 MAC 地址的格式为 B4-0C-25-xx-xx-xx，其中 B4-0C-25 为供应商 ID（此处的供应商为 Palo Alto Networks），接下来的 24 位依次为设备 ID、组 ID 和接口 ID，如下所示：

| 7 6 5 | 4 | 3 2 1 0 7 6 | 5 4 3 2 | 1 0 7 6 5 4 3 2 1 0 |
|---|---|---|---|---|
| 111 | 设备 ID | 群组 ID | 0000 | 接口 ID |

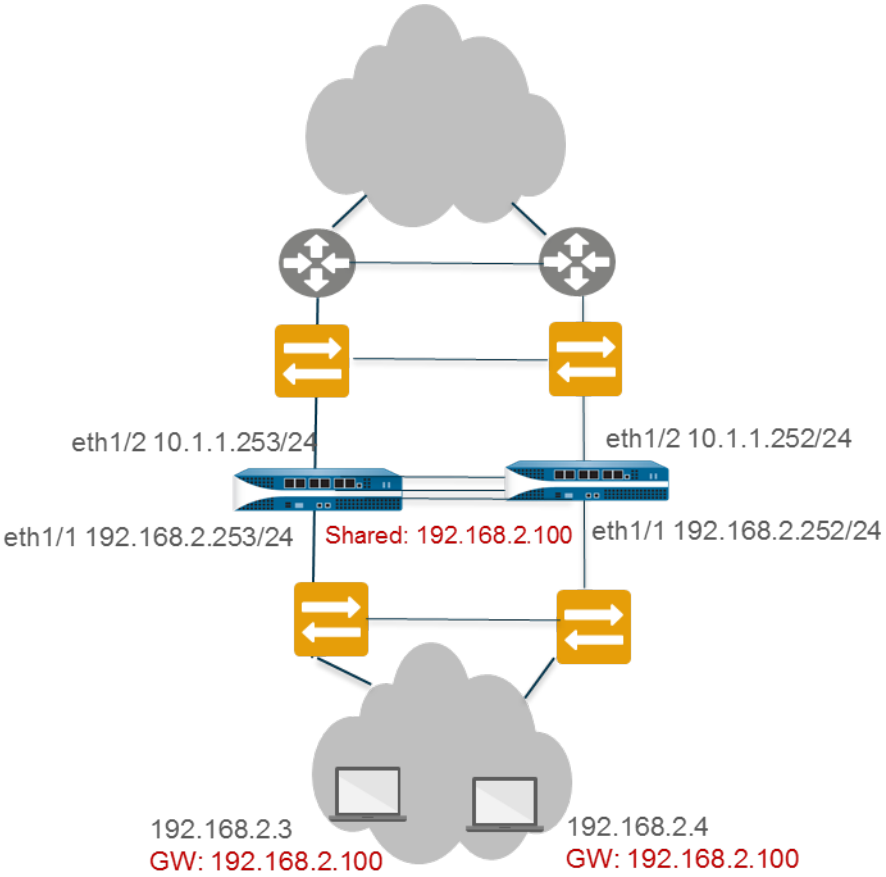
当新的主动设备接管时，会从每个已连接接口发送 Gratuitous ARP，以便向连接的第 2 层交换机通知虚拟 MAC 地址的新位置。要配置浮动 IP 地址，请查阅用例：配置具有浮动 IP 地址的主动/主动 HA。

## ARP 加载共享

在第 3 层接口部署及主动/主动 HA 配置中，ARP 加载共享允许防火墙共享 IP 地址并提供网关服务。仅在防火墙及终端主机间无第 3 层设备存在，即终端主机将防火墙用作其默认网关的情况下使用 ARP 加载共享。



© 2019 Palo Alto Networks, Inc.



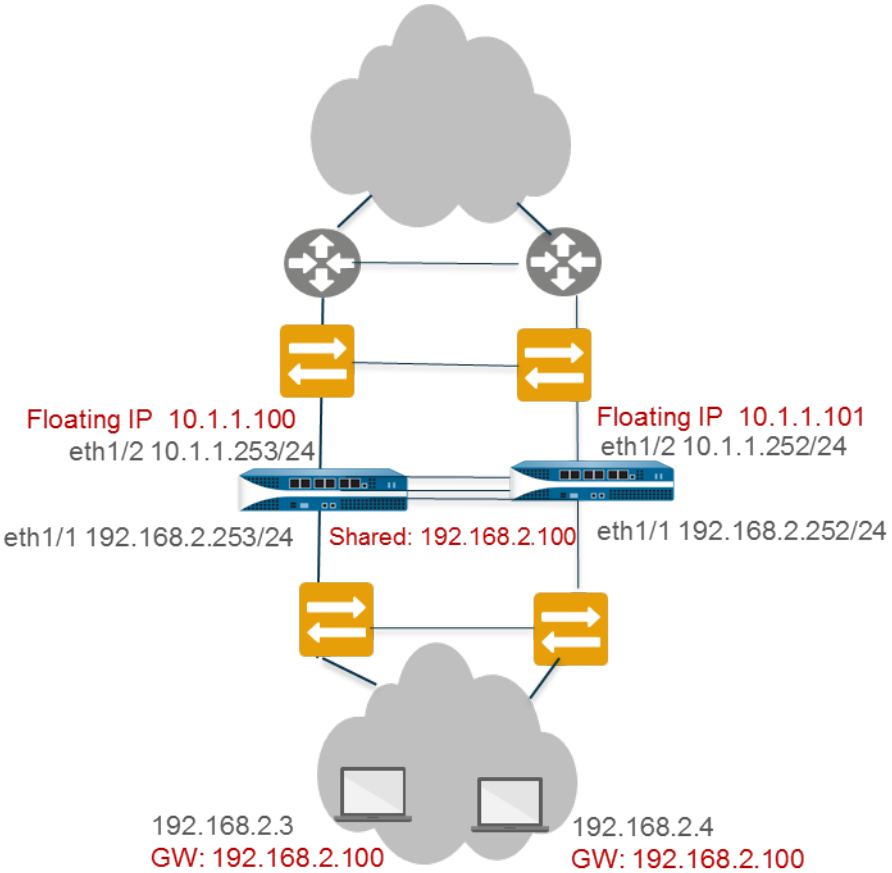

在此情况下，所有主机均配置使用一个网关 IP 地址。其中一个防火墙响应 ARP 请求，通过其虚拟 MAC 地址获取网关 IP 地址。每个防火墙都有一个为共享 IP 地址生成的虚拟 MAC 地址。您可用控制哪个防火墙将响应 ARP 请求的负载共享算法进行配置；可通过计算 ARP 请求源 IP 地址的哈希或模数确定哪个防火墙将进行响应。

从网关收到 ARP 响应后，终端主机会捕获 MAC 地址，所有来自主机的流量会通过响应虚拟 MAC 地址的防火墙进行路由，获取 ARP 缓存的生命周期。ARP 缓存的生命周期取决于终端主机的操作系统。

如果链路或防火墙出现故障，浮动 IP 地址和虚拟 MAC 地址会迁移至正常运行的防火墙。正常运行的防火墙将发送 Gratuitous ARP 以更新已连接交换机的 MAC 表，将流量从发生故障的防火墙重定向至自身。请参阅用例：配置主动/主动 HA 的 ARP 加载共享。

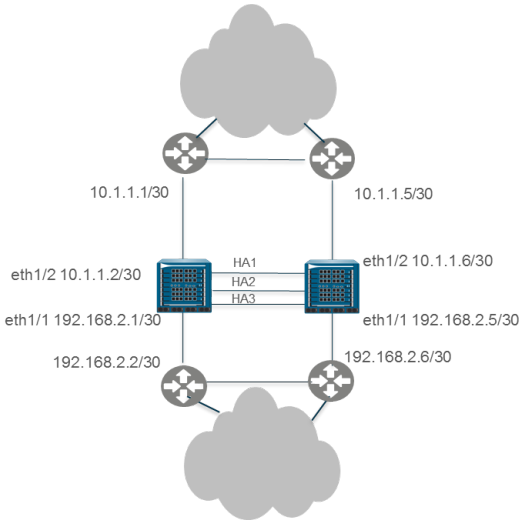
您可为 HA 防火墙 WAN 端的接口配置移动 IP 地址，为 HA 防火墙 LAN 端的接口配置共享 IP 地址，以进行 ARP 负载共享。例如，下图为上游 WAN 端路由器的浮动 IP 地址及 LAN 分段主机的 ARP 负载共享地址示例。


© 2019 Palo Alto Networks, Inc.




## 基于路由的冗余

处于第 3 层接口部署及主动/主动 HA 模式的防火墙连接路由器而非交换机。防火墙使用动态路由协议确定最佳路径（非对称路由）并在 HA 对间加载共享。该情形下，不需要浮动 IP 地址。如果链路、监控路径或防火墙出现故障，或者双向转发检测 (BFD) 检测到链路故障，路由协议（RIP、OSPF 或 BGP）会将重路由的通信发送至正常运行的防火墙。每个防火墙接口均配置有不同的 IP 地址。配置时，防护墙的 IP 地址始终为本地，在一个防火墙出现故障时，其不会在设备间迁移。请参阅用例：配置带有基于路由冗余的主动/主动 HA。






© 2019 Palo Alto Networks, Inc.

# 高可用性计时器

高可用性 (HA) 计时器用于加快检测防火墙故障和触发故障转移。若要降低配置 HA 对计时器的复杂性，您可以从以下三个配置文件中进行选择：**Recommended**（建议）、**Aggressive**（积极）和 **Advanced**（高级）。对于特定的防火墙平台，这些配置文件会自动填写最佳高可用性计时器值，从而更快地执行高可用性部署。

对于典型的故障转移计时器设置，使用 **Recommended**（建议）的配置文件；对于更快的故障转移计时器设置，使用 **Aggressive**（积极）的配置文件。**Advanced**（高级）配置文件可用于自定义适合您的网络需求的计时器值。

下表介绍了配置文件中包含的每个计时器，以及不同硬件模型的当前预设值（推荐/积极）；这些值仅供当前参考，在以后的版本中可能会发生变化。



影响 *HA* 集群成员的计时器如配置 HA 集群中所述。

| 计时器 | 说明 | PA-7000 系列<br>PA-5200 系列<br>PA-3200 系列 | PA-800 系列<br>PA-220<br>VM-SERIES | Panorama 虚拟设备<br>Panorama M 系列 |
|---|---|---|---|---|
| 监视失败保持运行时间（毫秒） | 防火墙在路径监视或链路监测失败之后将保持活动状态的时间间隔。建议使用此设置，以避免因邻近设备偶然翻动而导致 HA 故障转移。 | 0/0 | 0/0 | 0/0 |
| Preemption Hold Time (min) | 被动或主动辅助防火墙在接管主动或主动主要防火墙之前要等待的时间。 | 1/1 | 1/1 | 1/1 |
| 检测信号间隔（毫秒） | HA 对等以 ICMP Ping 的方式交换检测信号消息的频率。 | 1000/1000 | 2000/1000 | 2000/1000 |
| 提升保持时间（毫秒） | 被动防火墙（在主动/被动模式下）或主动辅助防火墙（在主动/主动模式下）在与 HA 对的通信丢失之后，作为主动防火墙或主动主要防火墙接管之前将等待的时间。发出对等失败声明后，此持有时间才会开始。 | 2000/500 | 2000/500 | 2000/500 |
| 其他主设备保持运行时间(毫秒) | 此时间间隔（以毫秒为单位）适用于与监视失败保持时间相同的事件（范围是 0-60,000，默认为 500）。其他时间间隔仅适用于主动/被动模式下的主动对等，以及主动/主动模式下的主动-主要对等。建议使用此计时器，以免两个防火 | 500/500 | 500/500 | 7000/5000 |



© 2019 Palo Alto Networks, Inc.

| 计时器 | 说明 | PA-7000 系列<br>PA-5200 系列<br>PA-3200 系列 | PA-800 系列<br>PA-220<br>VM-SERIES | Panorama 虚拟设备<br>Panorama M 系列 |
|---|---|---|---|---|
| | 墙在同时遇到相同链接/路径监控失败时，发生故障转移。 | | | |
| Hello Interval (ms) | 为验证另一个防火墙上的 HA 功能是否正常运行而发送的呼叫数据包之间相隔的毫秒数（范围为 8,000-60,000，默认为 8,000）。 | 8000/8000 | 8000/8000 | 8000/8000 |
| 最大翻动数 | 发生下列情况之一时，计算翻动数：<br>• 已启用抢先的防火墙在激活后 20 分钟内退出激活状态。<br>• 链路或路径在正常运行后的保持时间短于 10 分钟。<br>如果抢先失败或无法正常运行，此值表示在挂起防火墙之前允许的最大翻动数（范围为 0-16；默认为 3）。 | 3/3 | 3/3 | 不适用 |

## 会话所有者

处于 HA 主动/主动配置时，两个防火墙同时运作，这表明可在两者间分配数据包。此分配要求防火墙执行两项功能：会话所有权及会话设置。通常而言，HA 对中的每个防火墙分别执行其中一项功能，目的是避免非对称路由环境下可能出现的争用现象。

您可将会话的会话所有者配置为从终端主机处收到新会话的第一个数据包的防火墙或处于主动-主要状态的防火墙（主设备）。如果已配置主设备，但收到第一个数据包的防火墙不处于主动-主要状态，则防火墙会通过 HA 3 链路将数据包转发至对等防火墙（会话所有者）。

会话所有者执行所有第 7 层流程，如 App-ID、Content-ID 及会话的威胁扫描。所有会话流量日志均由会话所有者生成。

如果会话所有者出现故障，对等防火墙将成为会话所有者。现有会话故障将转移至正常运作的防火墙，且这些会话将无法执行第 7 层流程。默认情况下，修复故障后，防火墙在故障前所拥有的会话将恢复至原始防火墙，但第 7 层流程不会恢复。

如果将会话所有权配置为主设备，会话设置亦默认由主设备进行。

*Palo Alto Networks* 建议将会话所有者设置为第一个数据包，将会话设置设置为 *IP Modulo*，除非另有特殊用途说明。将会话所有者设为第一个数据包以减少 *HA3* 链路的流量，并帮助在对等设备之间分配数据平面负载。

将会话所有者及会话设置设置为主设备将导致主动-主要设备处理所有通信。您想要这样配置的原因如下：



© 2019 Palo Alto Networks, Inc.

- 您正在排除故障并捕获日志和 *pcap*，因此数据包处理未在防火墙间作区分。
- 您想要强制主动/主动 *HA* 对像主动/被动 *HA* 对那样运作。请参阅用例：配置具有绑定至主动-主要防火墙的浮动 IP 地址的主动/主动 HA。

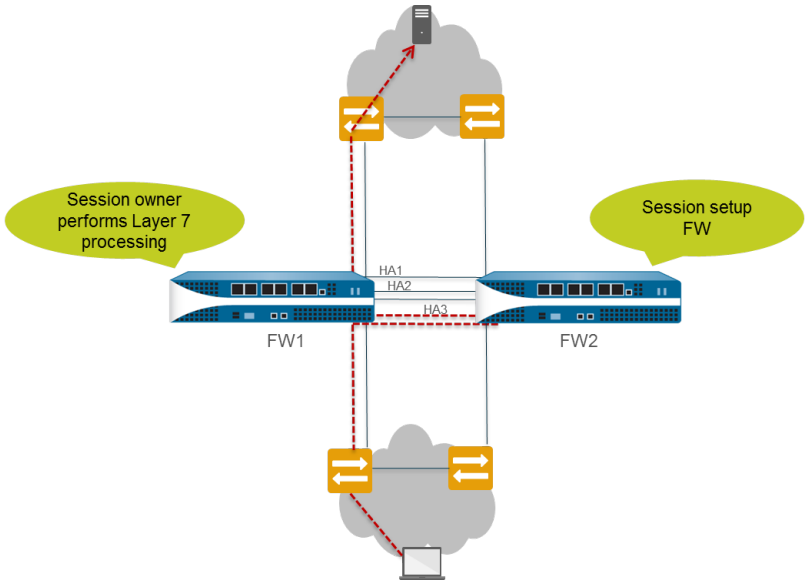
## 会话设置

会话设置防火墙执行第 2 层到第 4 层的必要流程，建立新对话。会话设置防火墙还使用会话所有者的 NAT 池执行 NAT。选中下列中的一个会话设置加载共享选项即可确定主动/主动配置中的会话设置防火墙。

| 会话设置选项 | 说明 |
|---|---|
| **IP 模** | 防火墙根据源 IP 地址的奇偶校验分布会话设置。这是共享会话设置的一种确定性方法。 |
| **IP 哈希** | 防火墙使用源和目标 IP 地址的哈希分配会话设置责任。 |
| 主设备 | 主动-主要防火墙始终负责设置会话；仅一个防火墙履行所有的会话设置责任。 |
| 第一个数据包 | 收到第一个会话数据包的防火墙执行会话设置。 |

- 如果您希望加载-共享会话所有者及会话设置责任，将会话所有者设为第一个数据包，将会话设置设置为 *IP modulo*。这些为推荐设置。
- 如果您想要排除故障或捕获日志或 *pcaps*，或者如果您想要主动/主动 *HA* 对像主动/被动 *HA* 对那样运作，则可将会话所有者及会话设置设置为主设备，以便主动-主要设备执行所有通信处理。请参阅用例：配置具有绑定至主动-主要防火墙的浮动 IP 地址的主动/主动 HA。

防火墙使用 HA3 链路发送数据包至对等以建立会话（如需要）。下图为防火墙 FW1 收到的新会话数据包路径，下文为相关介绍。红色虚线指通过 HA3 链路， FW1 转发数据包至 FW2，FW2 将数据包转回 FW1。

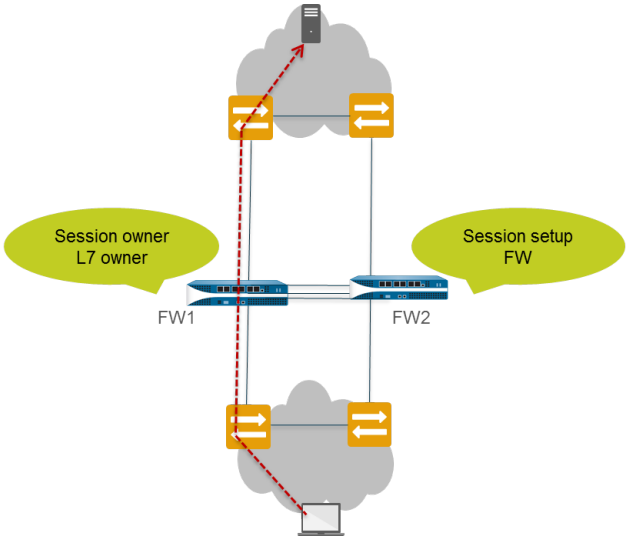



1. 终端主机发送数据包至 FW1。
2. 通过检查数据包内容，FW1 将其与现有会话进行匹配。如果没有会话与数据包匹配，FW1 则会判定这是其收到的新会话的第一个数据包，该数据包由此成为会话所有者（假定 **Session Owner Selection**（会话所有者选择）设置为 **First Packet**（第一个数据包））。


© 2019 Palo Alto Networks, Inc.

- FW1 使用已配置的会话设置加载-共享选项识别会话设置防火墙。该例中，FW2 被配置为执行会话设置。
- FW1 使用 HA3 链路发送第一个数据包至 FW2。
- FW2 设置会话并将数据包返回至 FW1，进行第 7 层处理。
- 然后，FW1 将数据包转出出口接口至目标。

下图为与现有会话匹配的数据包路径，下文为相关介绍：




- 终端主机发送数据包至 FW1。
- 通过检查数据包内容，FW1 将其与现有会话进行匹配。如果会话与现有会话匹配，FW1 则会对数据包进行处理，并将数据包转出出口接口至目标。

## 处于主动/主动模式的 NAT

在主动/主动 HA 配置中：

- 您必须将所有动态 IP (DIP) NAT 规则及动态 IP 和端口 (DIPP) 绑定至 Device ID 0 或 Device ID 1。
- 您必须将所有静态 NAT 规则绑定至 Device ID 0 或 Device ID 1 或两台设备或主动-主要防火墙。

因此，当其中一个防火墙创建新会话时，Device ID **0** 或 Device ID **1** 的绑定将确定哪一个 NAT 规则与防火墙匹配。设备绑定必须包含会话所有者防火墙以生成匹配。

会话设置防火墙执行 NAT 策略匹配，但 NAT 规则基于会话所有者被评估。即会话根据与会话所有者绑定的 NAT 规则转换该会话。在执行 NAT 策略匹配时，防火墙将跳过所有未绑定至会话所有者防火墙的 NAT 规则。

例如，假设带有 Device ID 1 的防火墙是会话所有者和会话设置防火墙。当带有 Device ID 1 的防火墙尝试将会话与 NAT 规则匹配时，它会忽略所有绑定到 Device ID 0 的规则。防火墙仅在会话所有者与及 NAT 规则中设备 ID 匹配的情况下执行 NAT 转换。

您通常在对等防火墙使用不同 IP 地址进行转换的情况下创建设备专用的 NAT 规则。

如果一个对等出现故障，则主动发那个火枪会继续为来自故障防火墙的同步会话处理通信，包括 NAT 转换等。在源 NAT 配置中，如果一个防火墙出现故障：

- 用作 NAT 规则转换 IP 地址的浮动 IP 地址转至未发生故障的防火墙。因此，发生故障转移的现有会话仍会使用该 IP 地址。
- 所有新会话将使用未发生故障防火墙本身拥有的专用 NAT 规则。也就是说，未发生故障的防火墙仅使用与其设备 ID 匹配的 NAT 规则即可转换新会话；它会忽略任何绑定至故障设备 ID 的 NAT 规则。

了解带有 NAT 的主动/主动 HA 实例，请查阅：


© 2019 Palo Alto Networks, Inc.

- 用例：配置具有使用浮动 IP 地址的源 DIPP NAT 的主动/主动 HA
- 用例：为主动/主动 HA 防火墙配置单独的源 NAT IP 地址池
- 用例：配置带有目标 NAT 的主动/主动 HA，进行ARP 加载共享
- 用例：在第三层中配置带有目标 NAT 的主动/主动 HA，进行 ARP 加载共享

# 处于主动/主动 HA 模式的 ECMP

当主动/主动 HA 对等发生故障时，其会话将转换至新的主动-主要防火墙，该防火墙将使用与故障防火墙相同的出口接口。如果防火墙在 ECMP 路径中找到该接口，则转移会话将使用相同的出口接口及路径。该行为的发生与使用的 ECMP 算法无关；适合使用相同接口。

主动-主要防火墙仅在无 ECMP 路径与原始接口出口匹配的情况下选择新的 ECMP 路径。

如果您未在主动/主动对等上配置相同接口，则主动-主要防火墙会在故障转移时从 FIB 表中选择最佳路径。因此，现有会话可能不会根据 ECMP 算法进行分配。


© 2019 Palo Alto Networks, Inc.

# 设置主动/被动 HA


- 主动/被动 HA 的先决条件
- 主动/被动 HA 的配置原则
- 配置主动/被动 HA
- 定义 HA 故障转移条件
- 验证故障转移


## 主动/被动 HA 的先决条件

若要在 Palo Alto Networks 防火墙上设置高可用性，您需要提供满足以下条件的一对防火墙：

- 相同的型号 — HA 对中的两个防火墙必须采用相同的硬件型号或虚拟机型号。
- 相同的 **PAN-OS** 版本 — 两个防火墙应该运行相同的 PAN-OS 版本，并且每一台设备的应用程序、URL 和威胁数据库都必须处于最新状态。
- 相同的多虚拟系统功能 — 两个防火墙必须启用或禁用 **Multi Virtual System Capability**（多虚拟系统功能）。启用后，每个防火墙均需要其自身的多虚拟系统许可证。
- 相同的接口类型 — 专用 HA 链路，或者管理端口和设置为 HA 接口类型的带内端口组合。
  - 确定 HA 对之间的 HA1（控制）连接的 IP 地址。如果两台对等设备直接连接在一起或连接到同一台交换机，则它们的 HA1 IP 地址必须在同一个子网上。

    对于没有专用 HA 端口的防火墙，可以使用管理端口用于控制连接。使用管理端口，将在两个防火墙的管理面板之间提供一个直接的通信链路。但是，由于管理端口不会在对之间直接连线，因此请确保建立在您的网络中连接这两个接口的路由。
  - 如果使用第 3 层作为 HA2（数据）连接的传输方法，请确定 HA2 链路的 IP 地址。仅当 HA2 连接必须通过路由网络进行通信时才应使用第 3 层。HA2 链路的 IP 子网不得与 HA1 链路的子网或与分配给防火墙上数据端口的任何其他子网重叠。
- 相同的许可证集合 — 许可证对于每个防火墙是唯一的，无法在防火墙之间进行共享。因此，必须以相同的方式许可两个防火墙。如果两个防火墙所拥有的许可证集合不同，则它们将无法同步配置信息和维持无缝故障转移所需的同等性。



最佳实践是，如果您已有防火墙，并且您希望添加新的防火墙来实现 *HA* 目的，而新的防火墙具有现有配置，则建议在新防火墙上将防火墙重置为默认出厂设置。这样可以确保新防火墙具有初始配置。高可用性配置完成后，您随后可以使用初始配置将主防火墙的配置同步到新引入的防火墙。

## 主动/被动 HA 的配置原则

要在 HA 中设置主动 (PeerA) 被动 (PeerB) 对，您必须在两个防火墙上以完全相同的方式配置某些选项，并在每个防火墙上独立（不匹配）配置一些选项。这些 HA 设置不会在防火墙之间同步。有关已同步/未同步内容的详细信息，请参阅参考资料：高可用性同步。

下表列出了必须在两个防火墙上以完全相同的方式配置的设置：

- 您必须在两个防火墙上启用 HA。
- 您必须在两个防火墙上配置相同的“组 ID”值。防火墙使用“组 ID”值为配置的所有接口创建虚拟 MAC 地址。有关虚拟 MAC 地址的信息，请参阅“浮动 IP 地址”和“虚拟 MAC 地址”。当新的主动防火墙接管时，会从每个已连接接口发送 Gratuitous ARP 信息，以便向连接的第 2 层交换机通知虚拟 MAC 地址的新位置。
- 如果使用带内端口作为 HA 链接，则必须将 HA1 和 HA2 链接接口设置为 HA 类型。
- 将两个防火墙上的 HA 模式设置为主动被动。
- 如果需要，请启用两个防火墙的抢先。但是，设备优先级值不得相同。



© 2019 Palo Alto Networks, Inc.

- 如有必要，必须在两个防火墙上配置 HA1 链路加密（用于 HA 对等端之间的通信）。
- 根据所使用 HA1 和 HA1 备份端口的组合，使用以下建议来决定是否应该启用检测信号备份：

  如果配置为 *DHCP* 寻址（*IP Type*（*IP* 类型）设置为 *DHCP Client*（*DHCP* 客户端）），则管理接口不支持 *HA* 功能（*HA1* 和 *HA1* 备份）。*AWS* 和 *Azure* 除外，其管理接口配置为 *DHCP* 客户端，支持 *HA1* 和 *HA1* 备份链接。

  - HA1：专用 HA1 端口

    HA1 备份：专用 HA1 端口

    建议：启用检测信号备份
  - HA1：专用 HA1 端口

    HA1 备份：带内端口

    建议：启用检测信号备份
  - HA1：专用 HA1 端口

    HA1 备份：管理端口

    建议：不启用检测信号备份
  - HA1：带内端口

    HA1 备份：带内端口

    建议：启用检测信号备份
  - HA1：管理端口

    HA1 备份：带内端口

    建议：不启用检测信号备份

下表列出了必须在两个防火墙上独立配置的设置。有关不会在对端之间自动同步的其他配置设置，请参阅参考资料：高可用性同步了解更多详情。

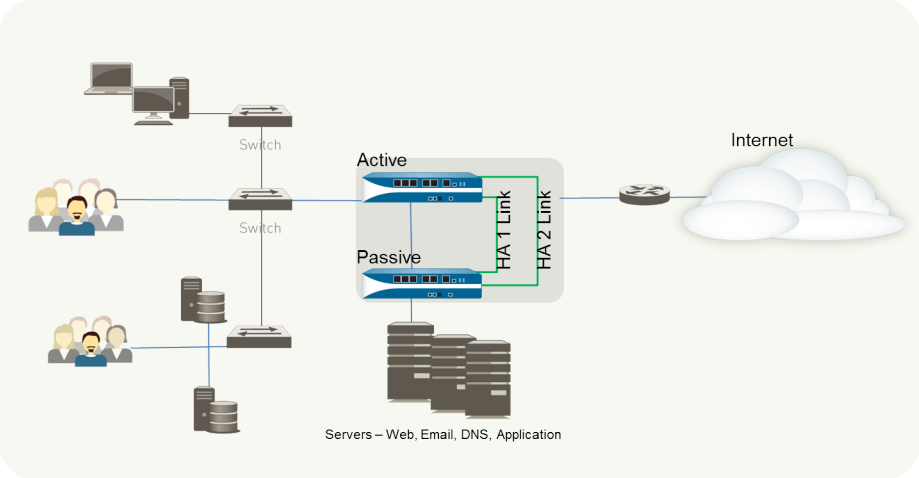
| 独立配置设置 | PeerA | PeerB |
|---|---|---|
| 控制链接 | 在此防火墙 (PeerA) 上配置的 HA1 链路的 IP 地址。 | 在此防火墙 (PeerB) 上配置的 HA1 链路的 IP 地址。 |
| | 对于没有专用 HA 端口的防火墙，为控制链路使用管理端口 IP 地址。 | |
| 数据链路<br>启用 HA 并且在防火墙备之间建立控制链路后，将在设备之间同步数据链路信息。 | 默认情况下，HA2 链路使用 Ethernet/第 2 层。<br>如果使用第 3 层连接，则需要在此防火墙 (PeerA) 上配置该数据链路的 IP 地址。 | 默认情况下，HA2 链路使用 Ethernet/第 2 层。<br>如果使用第 3 层连接，则需要在此防火墙 (PeerB) 上配置该数据链路的 IP 地址。 |
| 设备优先级（如果已启用抢先，则必须设置） | 与其对等端相比，您计划设置为主动的防火墙必须具有较低的数值。因此，如果 Peer A 将用作主动防火墙，请保留默认值 100 并增加 PeerB 上的值。<br>如果对等防火墙的设备优先级值相同，则使用 HA1 链路的 MAC 地址作为连接断路器。 | 如果 PeerB 是被动设备，请将设备优先级值设置为大于 PeerA 上的数字。例如，将该值设置为 110。 |


© 2019 Palo Alto Networks, Inc.

| 独立配置设置 | PeerA | PeerB |
| --- | --- | --- |
| 链路监视 — 监视在此防火墙上处理重要通信的一个或多个物理接口，并定义失败条件。 | 选择防火墙上要监视的物理接口，并定义触发故障转移的失败条件（全部或任何）。 | 在此防火墙上选择要监视的一组相似物理接口，并定义触发故障转移的失败条件（全部或任何）。 |
| 路径监视 — 监视防火墙可以使用 ICMP ping 来确定是否响应的一个或多个目标 IP 地址。 | 定义失败条件（全部或任何）、ping 间隔和 ping 计数。这对于监视其他互连网络设备的可用性尤为有用。例如，监视连接到服务器的路由器的可用性、与服务器本身的连接性或者处于通信流中的某些其他重要设备。<br>确保您要监视的节点/设备不可能无响应，尤其是其在负载情况下，因为这可能会导致路径监视失败并触发故障转移。 | 选取可监视的一组相似设备或目标 IP 地址，以便确定 PeerB 的故障转移触发。定义失败条件（全部或任何）、ping 间隔和 ping 计数。 |

# 配置主动/被动 HA

以下步骤介绍如何以主动/被动部署配置一对防火墙，如以下示例拓扑中所示。




要配置主动/被动 HA 对，请首先在第一个防火墙上完成以下工作流程，然后在第二个防火墙重复该步骤。

STEP 1 | 连接 HA 端口以在防火墙之间建立物理连接。

- 对于具备专用 HA 端口的防火墙，请使用 Ethernet 线缆连接设备对上的专用 HA1 端口和 HA2 端口。如果设备对直接互连，请使用交叉电缆。
- 对于没有专用 HA 端口的防火墙，请选择两个数据接口用于 HA2 链路和备用 HA1 链路。然后，使用 Ethernet 线缆连接两道防火墙上的这些带内 HA 接口。

使用管理端口用于 HA1 链路，并确保管理端口可以在您的网络中互连。

STEP 2 | 在管理端口上启用 ping。

启用 ping 可允许管理端口交换检测信号备份信息。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑管理接口设置。
2. 选择 **Ping** 作为允许在该接口上执行的服务。



© 2019 Palo Alto Networks, Inc.

STEP 3 | 如果防火墙没有专用 HA 端口，请设置数据端口用作 HA 端口。

对于具有专用 HA 端口的防火墙，请继续执行下一步。

1. 选择 **Network**（网络）> **Interfaces**（接口）。
2. 确保在希望使用的端口上已建立链路。
3. 选择接口并将 **Interface Type**（接口类型）设置为 **HA**。
4. 根据需要设置 **Link Speed**（链接速度）和 **Link Duplex**（链接双工设置）。

STEP 4 | 设置 HA 模式和组 ID。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置部分。
2. 设置 **Group ID**（组 **ID**），也可选择输入设备对 **Description**（说明）。网络中每个 HA 对的组 ID 均不同。如果您拥有多个共享相同广播域的 HA 对，您必须为每个 HA 对设置不同的组 ID。
3. 将模式设置为 **Active Passive**（主动被动）。

STEP 5 | 设置控制链路连接。

此示例显示了设置为 HA 接口类型的带内端口。

对于使用管理端口作为控制链路的防火墙，将自动预填充 IP 地址信息。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑控制链路 (HA1) 部分。
2. 选择您已连接并用作 HA1 链路的 **Port**（端口）。
3. 设置 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）及 **Netmask**（子网掩码）。

   如果 HA1 接口位于不同的子网上，输入 **Gateway**（网关）的 IP 地址。如果防火墙直接连接或位于相同的 VLAN 上，则不要添加网关地址。

STEP 6 | （可选）为控制链接连接启用加密。

这通常用于在两道防火墙未直接相连时（即端口连接到交换机或路由器时）保护链路的安全。

1. 从一道防火墙中导出 HA 密钥并将其导入对等防火墙。
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
   2. 选择 **Export HA key**（导出 **HA** 密钥）。将 HA 密钥保存到对等设备可以访问的网络位置。
   3. 在对等防火墙上，选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书），然后再选择 **Import HA key**（导入 **HA** 密钥）以浏览到您保存密钥的位置并将密钥导入对等设备。
   4. 在第二道防火墙上重复此过程，以在两个设备上交换 HA 密钥。
2. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），编辑控制链路 (HA1) 部分。
3. 选择 **Encryption Enabled**（启用加密）。

   如果启用加密，则在完成 *HA* 防火墙配置后，您可以刷新 HA1 SSH 密钥和配置密钥选项。

STEP 7 | 设置备份控制链路连接。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑控制链路（HA1 备份）部分。
2. 选择 HA1 备份接口并设置 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）和 **Netmask**（子网掩码）。

   *PA-3200* 系列防火墙不支持 *HA1* 备份控制链路的 *IPv6* 地址；请使用 *IPv4* 地址。


© 2019 Palo Alto Networks, Inc.

STEP 8 | 在防火墙之间设置数据链路连接 (HA2) 和备份 HA2 连接。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑数据链路 (HA2) 部分。
2. 选择用于数据链路连接的 **Port**（端口）。
3. 选择 **Transport**（传输）方法。默认设置是 **ethernet**，可以在 HA 对直接连接或通过交换机连接时使用该设置。如果需要通过网络路由数据链接通信，请选择 **IP** 或 **UDP** 作为传输模式。
4. 如果使用 IP 或 UDP 作为传输方法，请输入 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）和 **Netmask**（子网掩码）。
5. 确认已选中 **Enable Session Synchronization**（启用会话同步）。
6. 选中 **HA2 Keep-alive**（**HA2** 保持活动）状态以启用对 HA 对之间的 HA2 数据链接的监视。如果根据设置的阈值（默认值为 10000 毫秒）发生故障，将执行定义的操作。对于主动/被动配置，将在发生 HA2 保持活动状态故障时生成一条关键的系统日志消息。

   您可以在 *HA* 对的两道防火墙或仅在一台防火墙上配置“*HA2* 保持活动状态”选项。如果仅在一道防火墙上启用此选项，则仅该防火墙会发送保持活动状态消息。发生故障时另一道防火墙会收到通知。
7. 编辑 **Data Link (HA2 Backup)**（数据链路（**HA2** 备份））部分，选择接口，添加 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）和 **Netmask**（子网掩码）。

STEP 9 | 如果控制链接使用专用 HA 端口或带内端口，则需要启用检测信号备份。

如果您使用管理端口用于控制链路，则不需要启用检测信号备份。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 选择 **Heartbeat Backup**（检测信号备份）。

   若要允许在防火墙之间传输检测信号，必须确认两个对等端之间的管理端口可以路由到对方。

   启用检测信号备份还可让您防止裂脑情形。当 *HA1* 链接故障导致防火墙在正常运作的情况下错过检测信号时，即会发生裂脑。在该情形下，每个对等都认为另一个对等发生故障，并尝试启用正在运行的服务，从而导致裂脑。在启用检测信号备份链接后，裂脑将被阻止，原因是冗余检测信号及呼叫信心通过管理端口传送，

STEP 10 | 设置设备优先级并启用抢先。

仅当您希望确保特定防火墙为首选主动防火墙时才需要此设置。有关详细信息，请参阅设备优先级和抢先。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 在 **Device Priority**（设备优先级）中设置数值。确保在要分配较高优先级的防火墙上设置较低的数值。

   如果两个防火墙具有相同的设备优先级值，则在 *HA1* 控制链路上具有最低 *MAC* 地址的防火墙将变为主动防火墙。
3. 选择 **Preemptive**（抢先）。

   必须同时在主动和被动防火墙上启用抢先。

STEP 11 | （可选）修改 HA 计时器。

默认情况下，高可用性计时器配置文件设置为 **Recommended**（建议）配置文件，并且适用于最佳高可用性部署。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 为了更快触发故障转移，请选择 **Aggressive**（积极）配置文件；为了触发设置中的故障转移，请选择 **Advanced**（高级）以定义自定义值。



© 2019 Palo Alto Networks, Inc.

要查看配置文件内个别计时器的预设值，请选择高级并单击建议加载或积极加载。此屏幕上将显示硬件模型的预设值。

STEP 12 | (可选）在被动防火墙上修改 HA 端口的链路状态。

默认情况下，被动链接状态为 *shutdown*（断开）。在启用 *HA* 后，主动防火墙上 *HA* 端口的链接状态将变为绿色，而被动防火墙上的状态将变为断开并显示为红色。

将链接状态设置为 **Auto**（自动）可在发生故障转移时减少被动防火墙进行接管所需的时间量，并且允许您监视链接状态。

若要使被动防火墙的链接状态保持为已连接并反映物理接口上的连线状态，请执行下列步骤：

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑主动被动设置。
2. 将 **Passive Link State**（被动链接状态）设置为 **Auto**（自动）。

   自动选项可以减少在发生故障转移时被动防火墙进行接管所需的时间量。

   尽管该接口显示为绿色（已接线并已建立连接），但在触发故障转移之前，它将继续放弃所有通信。

   当您修改被动链接状态时，请确保邻近的设备不会仅根据防火墙的链接状态将通信转发到被动防火墙。

STEP 13 | 启用 HA。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置部分。
2. 选择 **Enable HA**（启用 **HA**）。
3. 选中 **Enable Config Sync**（启用配置同步）。此设置将启用主动和被动防火墙之间的配置设置同步。
4. 在 **Peer HA1 IP Address**（对等 **HA1 IP** 地址）中输入分配给对等设备的控制链路的 IP 地址。

   对于没有专用 HA 端口的防火墙，如果对等端使用管理端口用于 HA1 链接，请输入对等端的管理端口 IP 地址。
5. 输入 **Backup HA1 IP Address**（备份 **HA1 IP** 地址）。

STEP 14 | （可选）如果您的网络使用 LACP 或 LLDP，请启用主动/被动 HA 的 LACP 及 LLDP 预先协商），以实现更快的故障转移。

如果您希望在主动模式下使用预先协商功能，则需在配置 *HA* 协议预先协商前，启用 LACP 和 LLDP。

1. 确保在步骤12中将链接状态设置为 **Auto**（自动）。
2. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。
3. 启用 LACP 主动预先谈判：
   1. 在第 2 层或第 3 层部署中选择 AE 接口。
   2. 选择 **LACP** 选项卡。
   3. 选中**Enable in HA Passive State**（在 **HA** 被动状态中启用）。
   4. 单击 **OK**（确定）。

      您无法选择 *Same System MAC Address for Active-Passive HA*（对主动-被动 *HA* 系统相同的 *MAC* 地址），原因是预先谈判。
4. 启用 LACP 被动预先谈判：
   1. 在虚拟线路部署中选择以太网接口。


© 2019 Palo Alto Networks, Inc.

2. 选择 **Advanced**（高级）选项卡。
3. 选择 **LACP** 选项卡。
4. 选中**Enable in HA Passive State**（在 **HA** 被动状态中启用）。
5. 单击 **OK**（确定）。

5. 启用 LLDP 主动预先谈判：
   1. 在第 2 层、第 3 层或虚拟线路部署中选择以太网接口。
   2. 选择 **Advanced**（高级）选项卡。
   3. 选择 **LLDP** 选项卡。
   4. 选中**Enable in HA Passive State**（在 **HA** 被动状态中启用）。
   5. 单击 **OK**（确定）。



如果您想要允许虚拟线路部署的 *LLDP* 被动预先谈判，在不启用 *LLDP* 的情况下执行步骤14.e 。

STEP 15 | 保存配置更改。

单击 **Commit**（提交）。

STEP 16 | 在完成两个防火墙的配置后，验证防火墙是否已在主动/被动 HA 中配对。

1. 访问两个防火墙上的 **Dashboard**（仪表板），并查看高可用性小部件。
2. 在主动防火墙上，单击 **Sync to peer**（同步到对等）链接。
3. 确认防火墙已配对并同步，如下所示：
   - 在被动防火墙上：本地防火墙的状态应显示 **passive**（被动），并且运行配置应显示为 **synchronized**（已同步）。
   - 在主动防火墙上：本地防火墙的状态应显示 **active**（主动），并且运行配置应显示为 **synchronized**（已同步）。

# 定义 HA 故障转移条件

执行下列任务以使用链路监视或路径监视来定义故障转移条件，从而确定将导致 HA 对中防火墙故障转移的事件，此时，保护流量的任务从之前活动的防火墙传递到其 HA 对端。HA 概述介绍导致故障转移的条件。

您可以监视每个虚拟路由器、VLAN 或虚拟线路上的多个 IP 路径组。您可以为每个路径组启用一个或多个 IP 地址，并为每个路径组指定一个自己的对端故障条件。此外，您可以使用“任何”或“所有”故障检查设置路径组级别与更广泛的虚拟路由器或 VLAN 或虚拟线路组级别发生的这些失败条件，从而确定活动防火墙的状态。

一旦升级到 PAN-OS 10.0，防火墙会自动将您当前监视的目标 IP 地址传输到新创建的目标组，并为该组提供一个默认路径监视名称。新目标组将在路径组级别保留之前的故障转移条件。



在升级到 *PAN-OS 10.0* 之前，请务必删除主动/主动 *HA* 中所有的 *VLAN* 路径监视配置，因为 *VLAN* 路径监视与 *PAN-OS 10.0* 中的主动/主动 *HA* 不兼容；保留更早的主动/主动 *HA* 配置会导致自动提交失败。

启用路径监视之前，必须先设置您的虚拟路由器、VLAN 或虚拟线路，或是这些逻辑网络组件的组合。虚拟路由器和虚拟线路中的路径监视与主动/主动和主动/被动 HA 部署均兼容；但是，仅主动/被动对支持 VLAN 中的路径监视。

启用路径监视之前，还必须：

- 检查虚拟路由器中目标 IP 组的可访问性。
- 确保 VLAN（您打算启用路径监视的 VLAN）包含所配置的接口。
- 获取您将其用于从适当的目标 IP 地址接收 ping 的源 IP 地址。



© 2019 Palo Alto Networks, Inc.

如果您正在使用 *NMPv3* 监视防火墙，请注意，每个防火墙的 *SNMPv3* 引擎 *ID* 都是唯一的，并且此引擎 *ID* 在 *HA* 对之间不同步，因此，可让您单独监视 *HA* 对中的每个防火墙。有关设置 *SNMP* 的信息，请查阅转发 Traps 至 SNMP 管理器。由于使用防火墙序列号生成引擎 *ID*，因此，在 *VM-Series* 防火墙上，您必须申请一个有效许可证来获取每个防火墙的唯一引擎 *ID*。

STEP 1 | 要配置 HA 链路监视，请指定一组要监视的防火墙物理接口（上行链路或下行链路）。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Link and Path Monitoring**（链路和路径监视）。
2. 在“链路监视”部分中，按 **Name**（名称）**Add**（添加）链路组。
3. 选择 **Enabled**（已启用）以启用链路组。
4. 选择用于链路组中接口的 **Failure Condition**（失败条件）：**Any**（任何）（默认）或 **All**（全部）。
5. **Add**（添加）要监视的 **Interface**（接口）。
6. 单击 **OK**（确定）。

STEP 2 | （可选）修改已在防火墙上配置的一组链路组的失败条件。

默认情况下，防火墙将在所监视的任何链路组失败时触发故障转移。

1. 编辑 **Link Monitoring**（链路监视）部分。
2. 将 **Failure Condition**（失败条件）设为 **Any**（任何）（默认）或 **All**（全部）。
3. 单击 **OK**（确定）。

STEP 3 | 若要配置虚拟线路、VLAN 或虚拟路由器的 HA 路径监视，请指定防火墙将 ping 以验证网络连接性的目标 IP 地址。

1. 在“路径监视”部分，选择 **Add Virtual Wire Path**（添加虚拟线路路径）、**Add VLAN Path**（添加 **VLAN** 路径）或 **Add Virtual Router Path**（添加虚拟路由器路径）。
2. 输入虚拟线路、VLAN 或虚拟路由器路径组的 **Name**（名称）。
3. （仅限虚拟线路路径或 VLAN 路径）输入要用于 ping 经过虚拟线路或 VLAN 的目标 IP 地址的**Source IP**（源 **IP**）地址。
4. 选择 **Enabled**（已启用）以启用路径组。
5. 选择导致该路径组失败的 **Failure Condition**（失败条件）：**Any**（任何）（默认）将在该路径组中一个或多个目标 IP 组失败时报告故障，而 **All**（全部）则仅在该路径组所有目标 IP 组均失败时报告故障。
6. 输入以毫秒为单位的 **Ping Interval**（**Ping** 间隔）；即发送到目标 IP 地址的 ICMP 消息之间的间隔（范围为 200-60,000；默认为 200）。
7. 输入在声明失败前必须失败的 **Ping Count**（**Ping** 计数）（范围为 3-10；默认为 10）。
8. **Add**（添加）并输入 **Destination IP Group**（目标 **IP** 组）名称。
9. **Add**（添加）一个或多个要 ping 的 **Destination IP**（目标 **IP**）地址。
10. 选择 **Enabled**（已启用）以启用目标 IP 组的路径监视。
11. 选择导致该目标 IP 组出现故障的 **Failure Condition**（失败条件）：**Any**（任何）（默认）将在一个或多个列出的 IP 地址不可访问时报告故障，而 **All**（全部）则仅在所有列出的 IP 地址均不可访问时报告故障。
12. 单击 **OK**（确认）两次。
13. （仅限 Panorama）选择适当的 Panorama 模板以将路径监视配置推送到您的设备。

STEP 4 | （可选）修改已在防火墙上配置的一组路径组的失败条件。

默认情况下，防火墙将在监视的任何路径组失败时触发故障转移。

1. 编辑 **Path Monitoring**（路径监视）部分。
2. 选择 **Enabled**（已启用）以启用设备上的路径监视。


© 2019 Palo Alto Networks, Inc.

3. 将 **Failure Condition**（失败条件）设为**Any**（任何）（默认），这样，将在监视的一个或多个虚拟路由器、VLAN 或虚拟线路关闭时发出该防火墙的故障。选择 **All**（全部），这样，将在监视的所有虚拟路由器、VLAN 或虚拟线路关闭时发出该防火墙的故障。
4. 单击 **OK**（确定）。

STEP 5 | **Commit**（提交）。

## 验证故障转移

要测试您的高可用性配置是否工作正常，请触发手动故障转移并验证防火墙是否能够成功转换状态。

STEP 1 | 挂起主动防火墙。

选择 **Device**（设备）> **High Availability**（高可用性）> **Operational Commands**（操作指令），单击 **Suspend local device**（挂起本地设备）链接。

STEP 2 | 验证被动防火墙是否已接管为主动设备。

在 **Dashboard**（仪表板）上，验证高可用性小部件中的被动防护墙状态是否已更改为 **active**（主动）。

STEP 3 | 将挂起的对等防火墙还原为运行状态。等待几分钟时间，然后验证是否已发生抢先（如果已启用 **Preemptive**（抢先））。

1. 在之前挂起的防火墙上，选择 **Device**（设备）> **High Availability**（高可用性）> **Operational Commands**（操作指令），并单击 **Make local device functional**（使本地设备正常运行）链接。
2. 在 **Dashboard**（仪表板）高可用性小部件中，确认该防火墙已接管为主动防火墙，并且对等端现在已处于被动状态。



© 2019 Palo Alto Networks, Inc.

# 设置主动/主动 HA


- 主动/主动 HA 的先决条件
- 配置主动/主动 HA
- 确定主动/主动用例


## 主动/主动 HA 的先决条件

若要在防火墙上设置主动/主动 HA，您需要提供满足以下条件的一对防火墙：

- 相同的型号 — HA 对中的两个防火墙必须采用相同的硬件型号。
- 相同的 **PAN-OS** 版本 — 两个防火墙必须运行相同的 PAN-OS 版本，并且每一台设备的应用程序、URL 和威胁数据库都必须处于最新状态。
- 相同的多虚拟系统功能 — 两个防火墙必须启用或禁用 **Multi Virtual System Capability**（多虚拟系统功能）。启用后，每个防火墙均需要其自身的多虚拟系统许可证。
- 相同的接口类型 — 专用 HA 链路，或者管理端口和设置为 HA 接口类型的带内端口组合。
  - 必须为 HA 接口配置静态 IP 地址，而非从 DHCP 获得的 IP 地址（除 AWS 可使用 DHCP 地址外）。确定 HA 对之间的 HA1（控制）连接的 IP 地址。如果两台对等设备直接连接在一起或连接到同一台交换机，则它们的 HA1 IP 地址必须在同一个子网上。

    对于没有专用 HA 端口的防火墙，可以使用管理端口用于控制连接。使用管理端口，将在两个防火墙的管理面板之间提供一个直接的通信链路。但是，由于管理端口不会在对之间直接连线，因此请确保建立在您的网络中连接这两个接口的路由。
  - 如果使用第 3 层作为 HA2（数据）连接的传输方法，请确定 HA2 链路的 IP 地址。仅当 HA2 连接必须通过路由网络进行通信时才应使用第 3 层。HA2 链路的 IP 子网不得与 HA1 链路的子网或与分配给防火墙上数据端口的任何其他子网重叠。
  - 每个防火墙均需要 HA3 链接专用的接口。PA-7000 系列防火墙将 HSCI 端口用于 HA3。PA-5200 系列防火墙可以将 HSCI 端口用于 HA3，也可以在数据面板端口上配置用于 HA3 的聚合接口，以获得冗余。在其他平台上，您可将数据面板端口上的聚合接口配置为 HA3 链路以获得冗余。
- 相同的许可证集合 — 许可证对于每个防火墙是唯一的，无法在防火墙之间进行共享。因此，必须以相同的方式许可两个防火墙。如果两个防火墙所拥有的许可证集合不同，则它们将无法同步配置信息和维持无缝故障转移所需的同等性。

如果您已有防火墙，并且您希望添加新的防火墙来实现 *HA* 目的，而新的防火墙具有现有配置，则建议在新防火墙上将防火墙重置为默认出厂设置。这样可以确保新防火墙具有初始配置。高可用性配置完成后，您随后可以使用初始配置将主防火墙的配置同步到新引入的防火墙。您还需要配置本地 *IP* 地址。

## 配置主动/主动 HA

以下步骤介绍了在主动/主动配置中配置防火墙的基本工作流程。但是，在开始之前，请确定您的主动/主动用例，以为您的特定网络环境配置更为适合的示例。

如果 *HA* 防火墙之间装有交换机，连接 *HA3* 链路的交换机端口必须支持巨型帧，以处理与 *HA 3* 链接上的 *MAC* 套 *MAC* 封装有关的开销。

要配置主动/主动，首先在第一台对等设备上完成以下步骤，然后在第二台对等设备上完成，确保将设备 ID 设置为每个对等设备上不同的值（0 或 1）。

STEP 1 | 连接 HA 端口以在防火墙之间建立物理连接。



© 2019 Palo Alto Networks, Inc.

对于每个用例，防火墙可使用任意硬件模式；选择与您的模式对应的 *HA3* 步骤。

- 对于具备专用 HA 端口的防火墙，请使用 Ethernet 线缆连接设备对上的专用 HA1 端口和 HA2 端口。如果设备对直接互连，请使用交叉电缆。
- 对于没有专用 HA 端口的防火墙，请选择两个数据接口用于 HA2 链路和备用 HA1 链路。然后，使用 Ethernet 线缆连接两道防火墙上的这些带内 HA 接口。使用管理端口用于 HA1 链路，并确保管理端口可以在您的网络中互连。
- 对于 HA3：
  - 在 PA-7000 系列防火墙上，将第一个机箱上的高速机箱互联 (HSCI-A) 连接到第二个机箱上的 HSCI-A，并将第一个机箱上的 HSCI-B 也连接到第二个机箱上的 HSCI-B。
  - 在 PA-5200 系列防火墙（有一个 HSCI 端口）上，将第一个机箱上的 HSCI 端口连接到第二个机箱上的 HSCI 端口。您还可以在 PA-5200 系列防火墙上使用 HA3 数据端口。
  - 在 PA-3200 系列防火墙（有一个 HSCI 端口）上，将第一个机箱上的 HSCI 端口连接到第二个机箱上的 HSCI 端口。
  - 在任何其他硬件模式下，HA3 均使用数据面板接口。

STEP 2 | 在管理端口上启用 ping。

启用 ping 可允许管理端口交换检测信号备份信息。

1. 在 **Device**（设备）> **Setup**（设置）> **Management**（管理）中，编辑管理界面设置。
2. 选择 **Ping** 作为允许在该接口上执行的服务。

STEP 3 | 如果防火墙没有专用 HA 端口，请设置数据端口用作 HA 端口。

对于具有专用 HA 端口的防火墙，请继续执行下一步。

1. 选择 **Network**（网络）> **Interfaces**（接口）。
2. 确保在希望使用的端口上已建立链路。
3. 选择接口并将 **Interface Type**（接口类型）设置为 **HA**。
4. 根据需要设置 **Link Speed**（链接速度）和 **Link Duplex**（链接双工设置）。

STEP 4 | 启用主动/主动 HA 并设置组 ID。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置。
2. 选择 **Enable HA**（启用 **HA**）。
3. 输入**Group ID**（组 **ID**），两道防火墙的组 ID 必须一致。防火墙使用组 ID 计算虚拟 MAC 地址（范围为 1-63）。
4. （可选）输入 **Description**（说明）。
5. 对于 **Mode**（模式），选择 **Active Active**（主动/主动）。

STEP 5 | 设置设备 ID，启用同步，并在对等防火墙上识别控制链路

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置。
2. 选择 **Device Id**（设备 **ID**），如下所示：
   - 配置第一台对等设备时，请将 **Device ID**（设备 **ID**）设置为 **0**。
   - 配置第二台对等设备时，请将 **Device ID**（设备 **ID**）设置为 **1**。
3. 选中 **Enable Config Sync**（启用配置同步）。该设置用于同步两个防火墙的配置（默认为启用）。
4. 输入 **Peer HA1 IP Address**（对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
5. （可选）输入 **Backup Peer HA1 IP Address**（备份对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
6. 单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

STEP 6 | 确定具有较低设备 ID 的防火墙是否会在从故障中恢复后抢先主动-主要防火墙。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 选择 **Preemptive**（抢先），具有较低设备 ID 的防火墙将会在任一防火墙从故障中恢复后恢复主动-主要操作。两个防火墙必须选择 **Preemptive**（抢先）才能发生抢先。

   如果您希望在手动将从故障中恢复的防火墙设为主动-主要防火墙前，主动-主要角色仍由当前防火墙承担，则保留 **Preemptive**（抢先）为未选状态。

STEP 7 | 如果控制链接使用专用 HA 端口或带内端口，则需要启用检测信号备份。

如果您使用管理端口用于控制链路，则不需要启用检测信号备份。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 选择 **Heartbeat Backup**（检测信号备份）。

   若要允许在防火墙之间传输检测信号，必须确认两个对等端之间的管理端口可以路由到对方。



启用检测信号备份可让您防止裂脑情形。当 *HA1* 链接故障导致防火墙在正常运作的情况下错过检测信号时，即会发生裂脑。在该情形下，每个对等都认为另一个对等发生故障，并尝试启用正在运行的服务，从而导致裂脑。在启用检测信号备份链接后，裂脑将被阻止，原因是冗余检测信号及呼叫信息通过管理端口传送。

STEP 8 | （可选）修改 HA 计时器。

默认情况下，高可用性计时器配置文件设置为 **Recommended**（建议）配置文件，并且适用于最佳高可用性部署。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 选择 **Aggressive**（积极）以触发更快的故障转移。选择 **Advanced**（高级）以定义在设置中触发故障转移的自定义值。



要查看配置文件内个别计时器的预设值，请选择高级并单击建议加载或积极加载。此屏幕上将显示硬件模型的预设值。

STEP 9 | 设置控制链路连接。

此示例中使用了设置为 HA 接口类型的带内端口。

对于使用管理端口作为控制链路的防火墙，将自动预填充 IP 地址信息。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑控制链路 (HA1)。
2. 选择您已连接并用作 HA1 链路的 **Port**（端口）。
3. 设置 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）及 **Netmask**（子网掩码）。

   如果 HA1 接口位于不同的子网上，输入 **Gateway**（网关）的 IP 地址。如果防火墙直接连接，则不要添加网关地址。

STEP 10 | （可选）为控制链接连接启用加密。

这通常用于在两道防火墙未直接相连时（即端口连接到交换机或路由器时）保护链路的安全。

1. 从一道防火墙中导出 HA 密钥并将其导入对等防火墙。
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
   2. 选择 **Export HA key**（导出 **HA** 密钥）。将 HA 密钥保存到对等设备可以访问的网络位置。
   3. 在对等防火墙上，选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书），然后再选择 **Import HA key**（导入 **HA** 密钥）以浏览到您保存密钥的位置并将密钥导入对等设备。
2. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑控制链路 (HA1)。



© 2019 Palo Alto Networks, Inc.

3. 选择 **Encryption Enabled**（启用加密）。



如果启用加密，则在完成 *HA* 防火墙配置后，您可以刷新 HA1 SSH 密钥和配置密钥选项。

STEP 11 | 设置备份控制链路连接。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑控制链路 (HA1 备份)。
2. 选择 HA1 备份接口并设置 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）和 **Netmask**（子网掩码）。



*PA-3200* 系列防火墙不支持 *HA1* 备份控制链路的 *IPv6* 地址；请使用 *IPv4* 地址。

STEP 12 | 在防火墙之间设置数据链路连接 (HA2) 和备份 HA2 连接。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑数据链路 (HA2)。
2. 选择用于数据链路连接的 **Port**（端口）。
3. 选择 **Transport**（传输）方法。默认设置是 **ethernet**，可以在 HA 对直接连接或通过交换机连接时使用该设置。如果需要通过网络路由数据链接通信，请选择 **IP** 或 **UDP** 作为传输模式。
4. 如果使用 IP 或 UDP 作为传输方法，请输入 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）和 **Netmask**（子网掩码）。
5. 确认已选中 **Enable Session Synchronization**（启用会话同步）。
6. 选中 **HA2 Keep-alive**（**HA2** 保持活动）状态以启用对 HA 对之间的 HA2 数据链接的监视。如果根据设置的阈值（默认值为 10000 毫秒）发生故障，将执行定义的操作。当 HA2 保持活动状态发生故障时，系统会根据您的配置生成关键的系统日志消息，或生成拆分数据平面。



您可以在 *HA* 对的两道防火墙或仅在一道防火墙上配置 *HA2* 保持活动状态选项。如果仅在一道防火墙上启用此选项，则仅该防火墙会发送保持活动状态消息。发生故障时另一道防火墙会收到通知。



拆分数据平面导致两个对等的数据平面独立平行，同时将高可用性状态保持为主动主要和主动辅助。如果仅一道防火墙配置为拆分数据平面，则拆分数据平面也适用于其他设备。

7. 编辑 **Data Link (HA2 Backup)**（数据链路（**HA2** 备份））部分，选择接口，添加 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）和 **Netmask**（子网掩码）。
8. 单击 **OK**（确定）。

STEP 13 | 配置 HA3 链路进行数据包转发。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，编辑数据包转发。
2. 在 **HA3 Interface**（**HA3** 接口），选择要用于在主动/主动 HA 对等之间转发数据包的数据接口。它必须为能够进行第 2 层传输的专用接口，并设置为**Interface Type HA**（接口类型 **HA**）。
3. 选择 **VR Sync**（**VR** 同步）强制同步 HA 对等上配置的所有虚拟路由器。未对动态路径协议配置虚拟路由时，请使用此选项。两个对等必须通过交换式网络连接到相同的下一个跃点路由器，并且只能使用静态路由。
4. 选中 **QoS Sync**（**QoS** 同步），可将所有物理接口中的 QoS 配置文件选择同步。如果两个对等具有类似的链路速度，且在所有物理接口中均需使用相同的 QoS 配置文件，请使用此选项。此设置将影响网络选项卡中的 QoS 同步设置。无论此设置如何，QoS 策略都会同步。

STEP 14 | （可选）修改试验保持时间。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，编辑数据包转发。



© 2019 Palo Alto Networks, Inc.

2. 在 **Tentative Hold Time (sec)**（试验保持时间（秒））中，输入防火墙从故障恢复后试验状态的保持时间（范围为 10-600，默认为 60）。

STEP 15 | 配置会话所有者和会话设置。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，编辑数据包转发。
2. 在 **Session Owner Selection**（会话所有者选择），选择以下其一：
   - **First Packet**（第一个数据包）— 收到新会话的第一个数据包的防火墙为会话所有者（推荐设置）。该设置将通过 HA3 中的流量最小化，并在各对等中加载共享流量。
   - **Primary Device**（主设备）— 处于主动-主要状态的防火墙为会话所有者。
3. 在 **Session Setup**（会话设置），选择以下其一：
   - **IP Modulo**（IP 模）— 防火墙在在数据包的源和目标 IP 地址执行 XOR 操作，并根据结果，选择将设置会话的 HA 对等设备。
   - **Primary Device**（主要设备）— 主动-主要防火墙设置所有会话。
   - **First Packet**（第一个数据包）— 收到第一个新会话数据包的防火墙执行会话设置（推荐设置）。

     从会话所有者和会话设置的第一个数据包开始，然后可以根据负载分布更改为其他选项之一。
   - **IP Hash**（IP 哈希）— 防火墙使用源地址或目标 IP 地址或结合源与 IP 地址的哈希分配会话设置责任。
4. 单击 **OK**（确定）。

STEP 16 | 配置 HA 虚拟地址。

您需要一个虚拟地址才能使用浮动 IP 地址和虚拟 MAC 地址或 ARP 加载共享。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，**Add**（添加）虚拟地址。
2. 输入或选择 **Interface**（接口）。
3. 选择 **IPv4** 或 **IPv6** 选项卡并单击 **Add**（添加）。
4. 输入 **IPv4 Address**（IPv4 地址）或 **IPv6 Address**（IPv6 地址）。
5. 关于 **Type**（类型）：
   - 选择 **Floating**（浮动）以配置虚拟 IP 地址为浮动 IP 地址。
   - 选择 **ARP Load Sharing**（ARP 加载共享）以配置虚拟 IP 地址为共享 IP 地址，并跳至配置 ARP 加载共享。

STEP 17 | 配置浮动 IP 地址。

1. 不要选择 **Floating IP bound to the Active-Primary device**（绑定至主动-主要设备的浮动 IP），除非您希望主动/主动 HA 对像主动/被动 HA 对那样运作。
2. 对于 **Device 0 Priority**（**Device 0** 优先级）和 **Device 1 Priority**（**Device 1** 优先级），分别输入配置 Device ID 0 和 Device ID 1 的防火墙的优先级。相关优先级旨在确定哪个对等拥有您刚配置的浮动 IP 地址（范围为 0-255）。具有较低数值（具有较高优先级）的防火墙将拥有该浮动 IP 地址。
3. 选择 **Failover address if link state is down**（如果链接状态为失效，则对地址执行故障转移），让防火墙在接口上的链接状态为失败时使用故障转移地址。
4. 单击 **OK**（确定）。

STEP 18 | 配置 ARP 加载共享。

设备选择算法旨在确定哪个 HA 防火墙将响应 ARP 请求以提供加载共享。

1. 在 **Device Selection Algorithm**（设备选择算法），选择以下其一：


© 2019 Palo Alto Networks, Inc.

- **IP Modulo**（**IP** 模）— 防火墙根据 ARP 请求者 IP 地址的奇偶校验响应 ARP 请求。
- **IP Hash**（**IP** 哈希）— 防火墙根据 ARP 请求者 IP 地址的哈希响应 ARP 请求。

2. 单击 **OK**（确定）。

STEP 19 | 定义 HA 故障转移条件。

STEP 20 | **Commit**（提交）配置。

# 确定主动/主动用例

确定您已有的用例，然后选择相应流程配置主动/主动 HA。

如果您在使用基于路由的冗余、浮动 IP 地址和虚拟 MAC 地址或ARP 加载共享，选择相应流程：

- 用例：配置带有基于路由冗余的主动/主动 HA
- 用例：配置具有浮动 IP 地址的主动/主动 HA
- 用例：配置主动/主动 HA 的 ARP 加载共享

如果您想要像主动/被动部署那样运作的第 3 层主动/主动 HA 部署，选择以下流程：

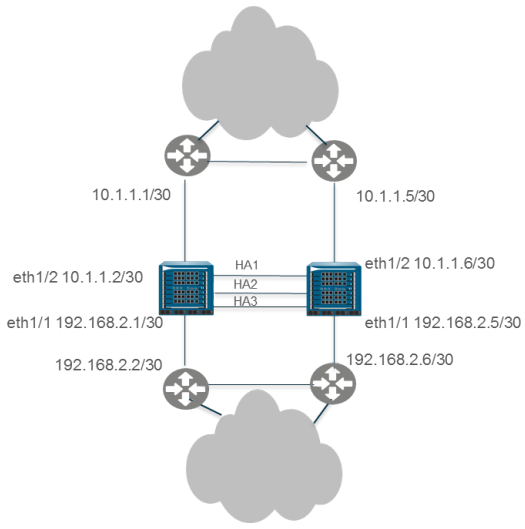
- 用例：配置具有绑定至主动-主要防火墙的浮动 IP 地址的主动/主动 HA

如果要配置处于主动/主动模式的 NAT，请查阅以下流程：

- 用例：配置具有使用浮动 IP 地址的源 DIPP NAT 的主动/主动 HA
- 用例：为主动/主动 HA 防火墙配置单独的源 NAT IP 地址池
- 用例：配置带有目标 NAT 的主动/主动 HA，进行ARP 加载共享
- 用例：在第三层中配置带有目标 NAT 的主动/主动 HA，进行 ARP 加载共享

## 用例：配置带有基于路由冗余的主动/主动 *HA*

以下第 3 层拓扑展示的是在主动/主动 HA 环境中使用基于路由的冗余的两个 PA-7050 防火墙。防火墙属于 OSPF 区域。如果链路或防火墙出现故障，OSPF 通过将流量重定向至正常运作的防火墙处理冗余。




STEP 1 | 配置主动/主动 HA。

执行步骤 1 到步骤 15。

STEP 2 | 配置 OSPF。



© 2019 Palo Alto Networks, Inc.

查阅 OSPF。

STEP 3 | 定义 HA 故障转移条件。

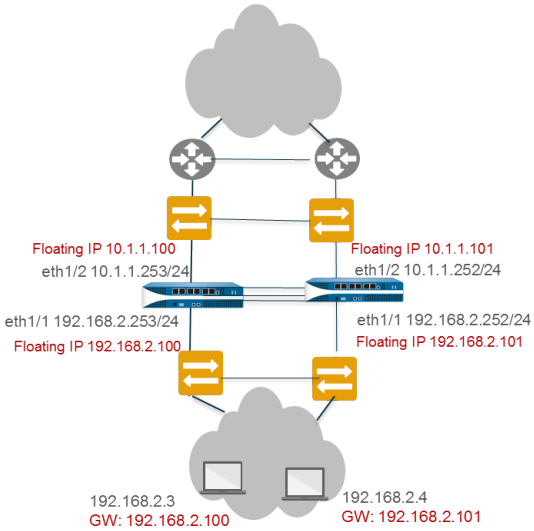
定义 HA 故障转移条件。

STEP 4 | **Commit**（提交）配置。

STEP 5 | 除步骤 5 外，以相同方式配置对等防火墙，如果您已为第一个防火墙选择 Device ID **0**，为对等防火墙选择 Device ID **1**。

## 用例：配置具有浮动 *IP* 地址的主动/主动 *HA*

在该第 3 层端口示例中，HA 防火墙连接至交换机，并使用浮动 IP 地址处理链接或防火墙故障。每个终端主机均配置有网关，即其中一个 HA 防火墙的浮动 IP 地址。请参阅浮动 IP 地址和虚拟 MAC 地址。




STEP 1 | 配置主动/主动 HA。

执行步骤 1 到步骤 15。

STEP 2 | 配置 HA 虚拟地址。

您需要一个虚拟地址才能使用浮动 IP 地址和虚拟 MAC 地址。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，**Add**（添加）虚拟地址。
2. 输入或选择 **Interface**（接口）。
3. 选择 **IPv4** 或 **IPv6** 选项卡并单击 **Add**（添加）。
4. 输入 **IPv4 Address**（IPv4 地址）或 **IPv6 Address**（IPv6 地址）。
5. 在 **Type**（类型）中，选择 **Floating**（浮动）以配置虚拟 IP 地址为浮动 IP 地址。

STEP 3 | 配置浮动 IP 地址。

1. 不要选择 **Floating IP bound to the Active-Primary device**（绑定至主动-主要设备的浮动 **IP**）。
2. 对于 **Device 0 Priority**（**Device 0** 优先级）和 **Device 1 Priority**（**Device 1** 优先级），分别输入配置 Device ID 0 和 Device ID 1 的防火墙的优先级。相关优先级旨在确定哪个对等拥有您刚配置的浮动 IP 地址（范围为 0-255）。具有较低数值（具有较高优先级）的防火墙将拥有该浮动 IP 地址。
3. 选择 **Failover address if link state is down**（如果链接状态为失效，则对地址执行故障转移），让防火墙在接口上的链接状态为失败时使用故障转移地址。


© 2019 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。

STEP 4 | 启用防火墙（除 PA-7000 系列防火墙）上的巨型帧。

执行配置主动/主动 HA 的步骤 19。

STEP 5 | 定义 HA 故障转移条件

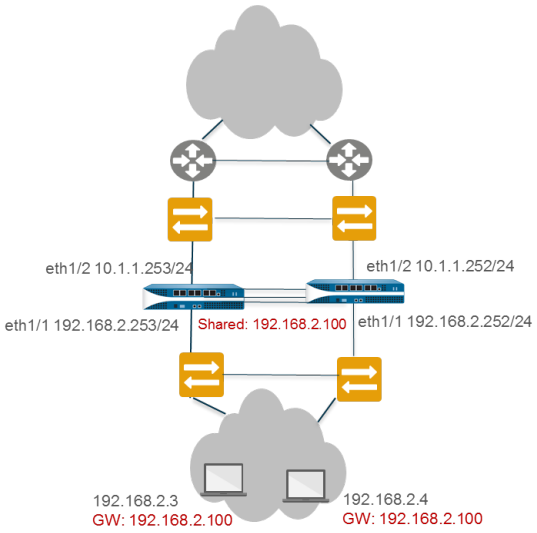
STEP 6 | **Commit**（提交）配置。

STEP 7 | 除选择不同的设备 ID 外，以相同方式配置对等防火墙。

例如，如果您已为第一个防火墙选择 Device ID **0**，为对等防火墙选择 Device ID **1**。

## 用例：配置主动/主动 *HA* 的 *ARP* 加载共享

该例中，第 3 层部署主机需要来自 HA 防火墙的网关服务。防火墙配置有一个共享 IP 地址，该地址允许 ARP 加载共享。每个终端主机均配置相同网关，即 HA 防火墙的共享 IP 地址。




STEP 1 | 执行配置主动/主动 HA 的步骤 1 至步骤 15。

STEP 2 | 配置 HA 虚拟地址。

虚拟地址为允许 ARP 加载共享的共享 IP 地址。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Virtual Address**（虚拟地址），然后单击 **Add**（添加）。
2. 输入或选择 **Interface**（接口）。
3. 选择 **IPv4** 或 **IPv6** 选项卡并单击 **Add**（添加）。
4. 输入 **IPv4 Address**（IPv4 地址）或 **IPv6 Address**（IPv6 地址）。
5. 对于 **Type**（类型），选择 **ARP Load Sharing**（ARP 加载共享）以允许两个对端使用虚拟 IP 地址进行 ARP 加载共享。

STEP 3 | 配置 ARP 加载共享。

设备选择算法旨在确定哪个 HA 防火墙将响应 ARP 请求以提供加载共享。

1. 在 **Device Selection Algorithm**（设备选择算法），选择以下其一：
   - **IP Modulo**（IP 模）— 防火墙根据 ARP 请求者 IP 地址的奇偶校验响应 ARP 请求。



© 2019 Palo Alto Networks, Inc.

- **IP Hash**（**IP** 哈希）— 防火墙根据 ARP 请求者 IP 地址的哈希响应 ARP 请求。

2. 单击 **OK**（确定）。

STEP 4 | 启用防火墙（除 PA-7000 系列防火墙）上的巨型帧。

STEP 5 | 定义 HA 故障转移条件

STEP 6 | **Commit**（提交）配置。

STEP 7 | 除选择不同的设备 ID 外，以相同方式配置对等防火墙。

例如，如果您已为第一个防火墙选择 Device ID **0**，为对等防火墙选择 Device ID **1**。

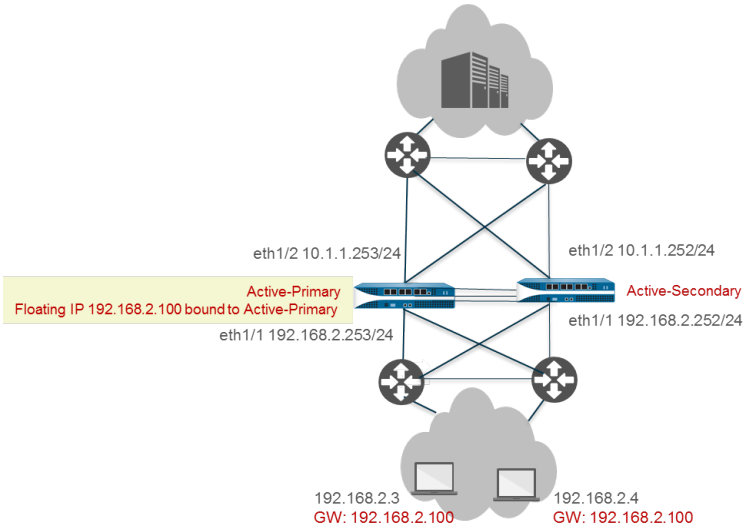
## 用例：配置具有绑定至主动-主要防火墙的浮动 *IP* 地址的主动/主动 *HA*

在关键任务数据中心，您可能想要两个第 3 层 HA 防火墙均参与路径监控，以便它们能够检测来自上游防火墙的路径失败。此外，您可能偏向于控制在防火墙恢复正常后返回至防火墙的浮动 IP 地址（如果返回），而非返回至其绑定的设备 ID 的浮动 IP 地址。（该默认行为在浮动 IP 地址和虚拟 MAC 地址进行描述。）

在该用例中，您在浮动 IP 地址及主动-主要角色返回至恢复正常运作的 HA 对等后进行控制。主动/主要 HA 防火墙共享绑定至任一处于主动-主要状态的防火墙的单一浮动 IP 地址。由于仅有 1 个浮动 IP 地址，网络通信主要流向 1 个防火墙，因此该主动/主动部署的运作与主动/被动部署相同。

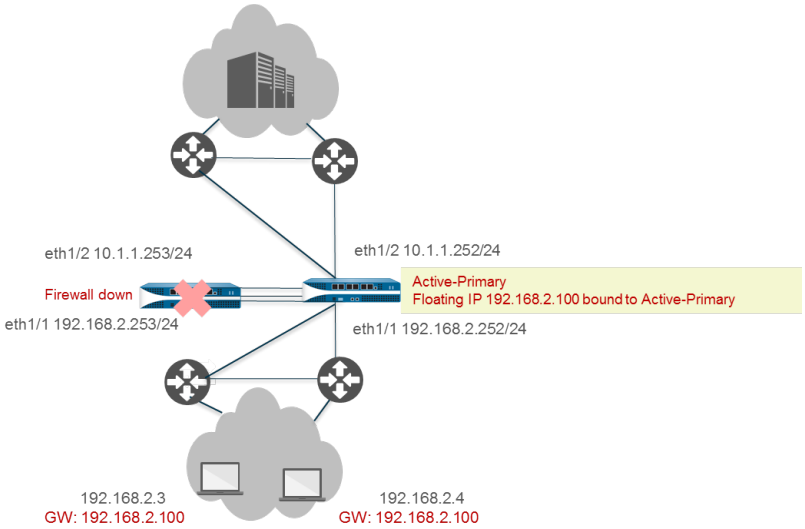
在该用例中，具备在第 3 层运行的虚拟 PortChannels (vPCs) 的 Cisco Nexus 7010 交换机与防护墙相连。您必须在防火墙的南端和北端配置第 3 层交换机（路由器对等），并将浮动 IP 地址设为路由偏好。也就是说，您必须设计网络，以便路由对等的路由表具备通往浮动 IP 地址的最佳路径。该例使用具备相应跃点数的静态路由，目的是让浮动 IP 地址路由使用较低跃点数（首选浮动 IP 地址路由）并接收通信。除使用静态路由外，您还可选择通过设计网络来重新分配浮动 IP 地址至 OSPF 路由协议（如果您在使用 OSPF）。

以下拓扑图示了绑定至主动-主要防火墙（最初为左边的防火墙对等 A）的浮动 IP 地址。




发生故障转移时，即主动-主要防火墙（对等 A）出现故障，主动-辅助防火墙（对等 B）接管为主动-主要对等时，浮动 IP 地址转至对等 B（如下图所示）。即便对等 A 恢复正常运作，对等 B 仍将作为主动-主要防火墙，通信亦继续流向该对等，而对等 A 则成为主动-辅助防火墙。是否以及何时将对等 A 恢复为主动-主要防火墙由您决定。


© 2019 Palo Alto Networks, Inc.




绑定浮动 IP 地址至主动-主要防火墙让您可更严密地管控在各 HA 防火墙状态中转换的防火墙确定浮动 IP 地址所有权的方式。具有以下好处：

- 您可获得主动/主动 HA 配置，从两个防火墙的外部进行路径监控，但防火墙的运作与主动/被动 HA 配置相同，原因是被定向至浮动 IP 地址的通信始终流向主动-主要防火墙。

在两个防火墙上禁用抢先后，您可得到下列好处：

- 如果主动-辅助防火墙上下翻动，则浮动 IP 地址不会在 HA 防火墙间来回移动。
- 在手动将通信定向至已恢复运作的防火墙前，您可核查该防火墙及相邻部件的功能，您可在中断期间方便时进行核查。
- 您可控制浮动 IP 地址为哪个防火墙所有，以使现有及新会话的所有通信流入主动-主要防火墙，从而最小化 HA3 链路的通信。

- 我们强烈建议您配置在支持浮动 *IP* 地址的接口上配置 *HA* 链接，以允许 *HA* 对等快速检测链接失败并将对等转移至对等。要正常运作，两个 *HA* 对等必须具备链接监控。
- 我们强烈建议您配置 *HA* 路径检测，从而在路径失败时通知 *HA* 对等，让防火墙将故障转移至其对等。由于浮动 *IP* 地址始终绑定至主动-主要防火墙，防护墙无法在路径失败或未启用路径监控的情况下自动将故障转移至对等。

您无法为绑定至主动-主要防火墙的浮动 *IP* 地址配置 *NAT*。

STEP 1 | 执行配置主动/主动 HA 的步骤 1 至步骤 5。

STEP 2 | （可选）禁用“抢先”。

禁用“抢先”可让您对从故障中恢复、并成为主动-主要防火墙的防火墙进行全面控制。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑选择设置。
2. 如果已启用“抢先”，需清除 **Preemptive**（抢先）。
3. 单击 **OK**（确定）。

STEP 3 | 执行配置主动/主动 HA 的步骤 7 至步骤 14。

STEP 4 | 配置会话所有者和会话设置。



© 2019 Palo Alto Networks, Inc.

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，编辑数据包转发。
2. 在 **Session Owner Selection**（会话所有者选择），我们推荐您选择 **Primary Device**（主设备）。处于主动-主要状态的防火墙为会话所有者。

   或者，您也在 **Session Owner Selection**（会话所有者选择）中选择 **First Packet**（第一个数据包），然后在 **Session Setup**（会话设置）中，选择 **Primary Device**（主要设备）或 **First Packet**（第一个数据包）。
3. 在 **Session Setup**（会话设置），选择**Primary Device**（主设备）— 主动-主要防火墙设置所有会话。如果您希望主动/主动配置像主动/被动配置那样运作，即所有活动均在主动-主要防火墙上进行，则推荐该设置。

   您还必须设计网络，排除非对称性通信流入 *HA* 对的可能。如果您未进行上述操作且通信流入主动-辅助防火墙，将 *Session Owner Selection*（会话所有者选择）及 *Session Setup*（会话设置）设置为 *Primary Device*（主设备），从而让通过 *HA3* 的通信流往主动-主要防火墙，拥有并设置会话。
4. 单击 **OK**（确定）。

STEP 5 | 配置 HA 虚拟地址。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Virtual Address**（虚拟地址），然后单击 **Add**（添加）。
2. 输入或选择 **Interface**（接口）。
3. 选择 **IPv4** 或 **IPv6** 选项卡并 **Add**（添加）**IPv4 Address**（**IPv4** 地址）或 **IPv6 Address**（**IPv6** 地址）。
4. 在 **Type**（类型）中，选择 **Floating**（浮动）以配置虚拟 IP 地址为浮动 IP 地址。
5. 单击 **OK**（确定）。

STEP 6 | 将 IP 地址绑定至主动-主要防火墙。

1. 选择 **Floating IP bound to the Active-Primary device**（绑定至主动-主要设备的浮动 **IP**）。
2. 选择 **Failover address if link state is down**（如果链接状态为失效，则对地址执行故障转移），让防火墙在接口上的链接状态为失败时使用故障转移地址。
3. 单击 **OK**（确定）。

STEP 7 | 启用防火墙（除 PA-7000 系列防火墙）上的巨型帧。

STEP 8 | **Commit**（提交）配置。

STEP 9 | 除选择不同的设备 ID 外，以相同方式配置对等防火墙。

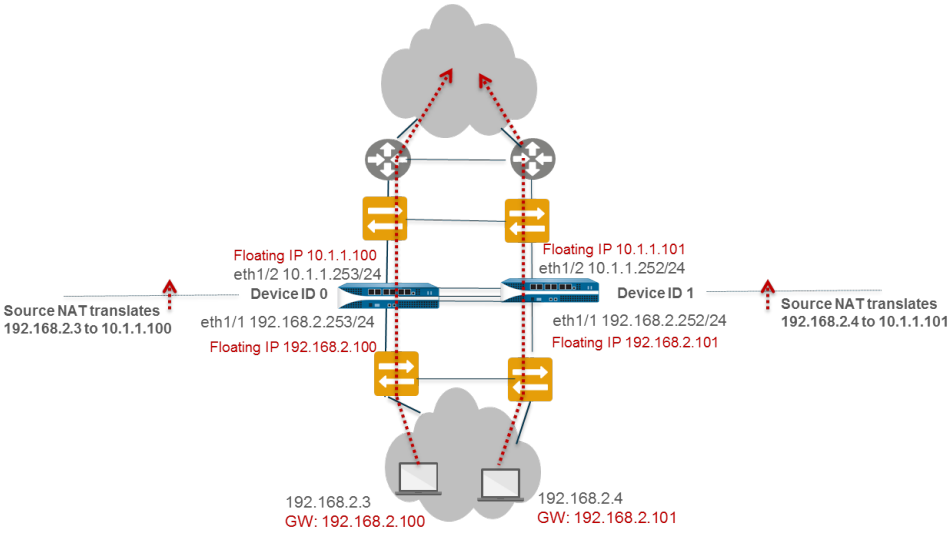
例如，如果您已为第一个防火墙选择 Device ID **0**，为对等防火墙选择 Device ID **1**。

## 用例：配置具有使用浮动 *IP* 地址的源 *DIPP NAT* 的主动/主动 *HA*

第 3 层接口示例使用主动/主动 HA 模式下的源 NAT。第 2 层交换机创建广播域以确保用户可触及防火墙北面和南面的一切。

PA-3050-1 具备 Device ID 0，而其 HA 对等 PA-3050-2 具备 Device ID 1。在该用例中，NAT 将源 IP 地址及端口号转换为配置于出口接口的浮动 IP 地址。每个主机均配备默认网关地址，即每个防火墙 Ethernet1/1 上的浮动 IP 地址。该配置需要两个源 NAT 规则，其中一个绑定至每个设备 ID，纵使您会在一个防火墙上配置上述两个 NAT 规则，且它们会同步至对等防火墙。


© 2019 Palo Alto Networks, Inc.




STEP 1 | 在 PA-3050-2（设备 ID 1）上，执行配置主动/主动 HA 的步骤 1 至步骤 3。

STEP 2 | 启用主动/主动 HA。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置。
2. 选择 **Enable HA**（启用 **HA**）。
3. 输入**Group ID**（组 **ID**），两道防火墙的组 ID 必须一致。防火墙使用组 ID 计算虚拟 MAC 地址（范围为 1-63）。
4. 对于 **Mode**（模式），选择 **Active Active**（主动/主动）。
5. 将 **Device ID**（设备 **ID**）设置为 **1**。
6. 选中 **Enable Config Sync**（启用配置同步）。该设置用于同步两个防火墙的配置（默认为启用）。
7. 输入 **Peer HA1 IP Address**（对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
8. （可选）输入 **Backup Peer HA1 IP Address**（备份对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
9. 单击 **OK**（确定）。

STEP 3 | 配置主动/主动 HA。

完成步骤 6 到步骤 14。

STEP 4 | 配置会话所有者和会话设置。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）中，编辑数据包转发。
2. 在 **Session Owner Selection**（会话所有者选择），选择 **First Packet**（第一个数据包）— 收到新会话的第一个数据包的防火墙为会话所有者。
3. 对于 **Session Setup**（会话设置），选择 **IP Modulo**（**IP** 模）— 防火墙根据源 IP 地址的奇偶校验分布会话设置负载。
4. 单击 **OK**（确定）。

STEP 5 | 配置 HA 虚拟地址。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Virtual Address**（虚拟地址），然后单击 **Add**（添加）。
2. 选择 **Interface**（接口）eth1/1。
3. 选择 **IPv4** 并 **Add**（添加）**IPv4 Address**（**IPv4** 地址）10.1.1.101。
4. 在 **Type**（类型）中，选择 **Floating**（浮动）以配置虚拟 IP 地址为浮动 IP 地址。



© 2019 Palo Alto Networks, Inc.

STEP 6 | 配置浮动 IP 地址。

1. 不要选择 **Floating IP bound to the Active-Primary device**（绑定至主动-主要设备的浮动 **IP**）。
2. 选择 **Failover address if link state is down**（如果链接状态为失效，则对地址执行故障转移），让防火墙在接口上的链接状态为失败时使用故障转移地址。
3. 单击 **OK**（确定）。

STEP 7 | 启用防火墙（除 PA-7000 系列防火墙）上的巨型帧。

STEP 8 | 定义 HA 故障转移条件。

STEP 9 | **Commit**（提交）配置。

STEP 10 | 使用相同设置配置对等防火墙 PA-3050-1，但以下更改除外：

- 选择 **Device ID 0**。
- 配置 HA 虚拟地址 10.1.1.100。
- 在 **Device 1 Priority**（**Device 1** 优先级）输入 255。在 **Device 0 Priority**（**Device 0** 优先级）输入 0。

在该示例中，Device ID 0 的优先级值较低（优先级更高）；因此，Device ID 0 防火墙 (PA-3050-1) 拥有浮动 IP 地址 10.1.1.100。

STEP 11 | 还是在 PA-3050-1 上，为 Device ID 0 创建源 NAT 规则。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 输入规则 **Name**（名称），该例中，名称将作为识别其为 Device ID 0 的源 NAT 规则的依据。
3. 在 **NAT Type**（**NAT** 类型），选择 **ipv4**（默认）。
4. 在 **Original Packet**（原始数据包），为 **Source Zone**（源区域）选择 **Any**（任意）。
5. 在 **Destination Zone**（目标区域），选择您为外部网络创建的区域。
6. 允许 **Destination Interface**（目标接口）、**Service**（服务）、**Source Address**（源地址）和 **Destination Address**（目标地址）继续设置为 **Any**（任意）。
7. 在 **Translated Packet**（转换数据包），选择 **Dynamic IP And Port**（动态 **IP** 和端口）为 **Translation Type**（转换类型）。
8. 选择 **Address Type**（地址类型）为 **Interface Address**（接口地址），选中该选项后，转换地址将成为接口的 IP 地址。选择 **Interface**（接口）（该例为 eth1/1）及浮动 IP 地址 10.1.1.100 的 **IP Address**（**IP** 地址）。
9. 在 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选项卡上，为 **Active/Active HA Binding**（主动/主动绑定）选择 **0** 以绑定 NAT 规则至 Device ID 0。
10. 单击 **OK**（确定）。

STEP 12 | 为 Device ID 1 创建源 NAT 规则。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 输入策略规则 **Name**（名称），该例中，名称将帮助识别其为 Device ID 1 的源 NAT 规则。
3. 在 **NAT Type**（**NAT** 类型），选择 **ipv4**（默认）。
4. 在 **Original Packet**（原始数据包），为 **Source Zone**（源区域）选择 **Any**（任意）。在 **Destination Zone**（目标区域），选择您为外部网络创建的区域。
5. 允许 **Destination Interface**（目标接口）、**Service**（服务）、**Source Address**（源地址）和 **Destination Address**（目标地址）继续设置为 **Any**（任意）。
6. 在 **Translated Packet**（转换数据包），选择 **Dynamic IP And Port**（动态 **IP** 和端口）为 **Translation Type**（转换类型）。
7. 选择 **Address Type**（地址类型）为 **Interface Address**（接口地址），选中该选项后，转换地址将成为接口的 IP 地址。选择 **Interface**（接口）（该例为 eth1/1）及浮动 IP 地址 10.1.1.101 的 **IP Address**（**IP** 地址）。


© 2019 Palo Alto Networks, Inc.

8. 在 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选项卡上，为 **Active/Active HA Binding**（主动/主动绑定）选择 **1** 以绑定 NAT 规则至 Device ID 1。
9. 单击 **OK**（确定）。

STEP 13 | **Commit**（提交）配置。

## 用例：为主动/主动 *HA* 防火墙配置单独的源 *NAT IP* 地址池

如果您想要使用源处于主动/主动模式的 NAT的 IP 地址池，则每个防火墙必须有自己的池，然后您才能将其绑定至 NAT 规则中的设备 ID。

（主动/被动及主动/主动模式下）地址对象和 NAT 规则会进行同步，因此仅需在 HA 对的其中一个防火墙上配置它们。

该例中配置的地址对象被命名为 Dyn-IP-Pool-dev0，包含 IP 地址池 10.1.1.140-10.1.1.150。该例中还配置了另一个命名为 Dyn-IP-Pool-dev1 的地址对象，其包含 IP 地址池 10.1.1.160-10.1.1.170。第一个地址对象绑定至 Device ID 0；第二个地址对象绑定至 Device ID 1。

STEP 1 | 在一个 HA 防火墙上，创建地址对象。

1. 选择 **Objects**（对象）> **Addresses**（地址）并 **Add**（添加）地址对象 **Name**（名称），该例中为 Dyn-IP-Pool-dev0。
2. 为 **Type**（类型）选择 **IP Range**（**IP** 范围）并输入范围 10.1.1.140-10.1.1.150。
3. 单击 **OK**（确定）。
4. 重复上述步骤，以配置命名为 Dyn-IP-Pool-dev1 的地址对象， **IP Range**（**IP** 范围）为 10.1.1.160-10.1.1.170。

STEP 2 | 为 Device ID 0 创建源 NAT 规则。

1. 选择 **Policies**（策略） > **NAT** 并 **Add**（添加）策略规则，该规则具有 **Name**（名称），如 Src-NAT-dev0。
2. 在 **Original Packet**（原始数据包），为 **Source Zone**（源区域）选择 **Any**（任意）。
3. 在 **Destination Zone**（目标区域），选择您想要转换源地址的目标区域，如 Untrust。
4. 在 **Translated Packet**（转换数据包），为 **Translation Type**（转换类型）选择 **Dynamic IP and Port**（动态 **IP** 和端口）。
5. 为**Translated Address**（转换地址）**Add**（添加）为设备 ID 0 Dyn-IP-Pool-dev1 的地址池创建的地址对象。
6. 为 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选择 **0** 以绑定 NAT 规则至 Device ID 0。
7. 单击 **OK**（确定）。

STEP 3 | 为 Device ID 1 创建源 NAT 规则。

1. 选择 **Policies**（策略） > **NAT** 并 **Add**（添加）策略规则，该规则具有 **Name**（名称），如 Src-NAT-dev1。
2. 在 **Original Packet**（原始数据包），为 **Source Zone**（源区域）选择 **Any**（任意）。
3. 在 **Destination Zone**（目标区域），选择您想要转换源地址的目标区域，如 Untrust。
4. 在 **Translated Packet**（转换数据包），为 **Translation Type**（转换类型）选择 **Dynamic IP and Port**（动态 **IP** 和端口）。
5. 为**Translated Address**（转换地址）**Add**（添加）为设备 ID 1：Dyn-IP-Pool-dev1 的地址池创建的地址对象。
6. 为 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选择 **1** 以绑定 NAT 规则至 Device ID 1。
7. 单击 **OK**（确定）。

STEP 4 | **Commit**（提交）配置。

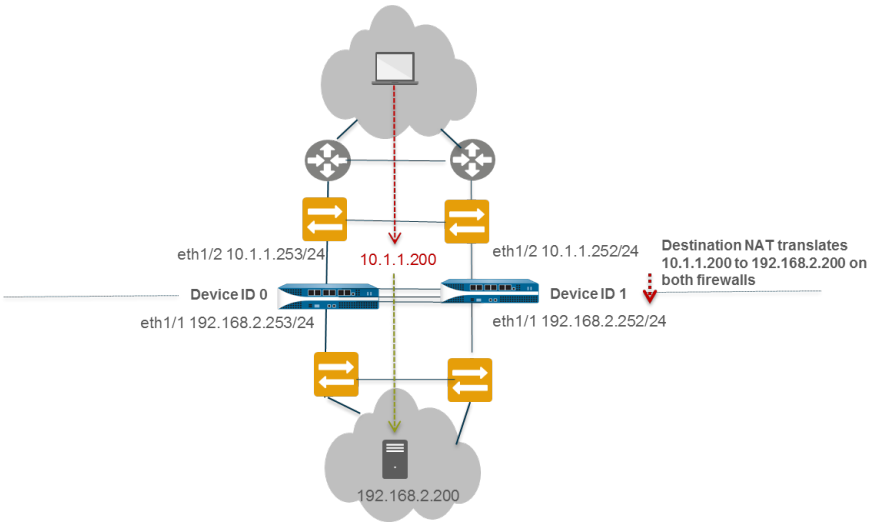


© 2019 Palo Alto Networks, Inc.

## 用例：配置带有目标 *NAT* 的主动/主动 *HA*，进行*ARP* 加载共享

第 3 层接口示例使用主动/主动 HA 模式下的 NAT，并在目标 NAT 上使用 ARP 加载共享。两个防火墙均通过入口接口 MAC 地址响应要求目标 NAT 地址的 ARP 请求。目标 NAT 将公共和共享 IP 地址（此例中为 10.1.1.200）转换为服务器的专有 IP 地址（此例中为 192.168.2.200）。

当 HA 防火墙收到目标 10.1.1.200 的通信后，两个防火墙都可能响应 ARP 请求，这会导致网络不稳定。为避免可能出现的问题，您可通过绑定目标 NAT 规则至主动-主要防火墙来配置处于主动-主要状态的防火墙，从而响应 ARP 请求。




STEP 1 | 在 PA-3050-2（设备 ID 1）上，执行配置主动/主动 HA 的步骤 1 至步骤 3。

STEP 2 | 启用主动/主动 HA。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置。
2. 选择 **Enable HA**（启用 **HA**）。
3. 输入**Group ID**（组 **ID**），两道防火墙的组 ID 必须一致。防火墙使用组 ID 计算虚拟 MAC 地址（范围为 1-63）。
4. （可选）输入 **Description**（说明）。
5. 对于 **Mode**（模式），选择 **Active Active**（主动/主动）。
6. **Device ID** 选择 **1**。
7. 选中 **Enable Config Sync**（启用配置同步）。该设置用于同步两个防火墙的配置（默认为启用）。
8. 输入 **Peer HA1 IP Address**（对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
9. （可选）输入 **Backup Peer HA1 IP Address**（备份对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
10. 单击 **OK**（确定）。

STEP 3 | 执行配置主动/主动 HA 的步骤 6 至步骤 15。

STEP 4 | 配置 HA 虚拟地址。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Virtual Address**（虚拟地址），然后单击 **Add**（添加）。
2. 选择 **Interface**（接口） eth1/1。
3. 选择 **IPv4** 并 **Add**（添加）**IPv4 Address**（**IPv4** 地址）10.1.1.200。
4. 对于 **Type**（类型），选择 **ARP Load Sharing**（**ARP** 加载共享），为两个对端设备配置用于 ARP 加载共享的虚拟 IP 地址。


© 2019 Palo Alto Networks, Inc.

STEP 5 | 配置 ARP 加载共享。

设备选择算法旨在确定哪个 HA 防火墙将响应 ARP 请求以提供加载共享。

1. 在 **Device Selection Algorithm**（设备选择算法），选择 **IP Modulo**（**IP** 模）。防火墙根据 ARP 请求者 IP 地址的奇偶校验响应 ARP 请求。
2. 单击 **OK**（确定）。

STEP 6 | 启用防火墙（除 PA-7000 系列防火墙）上的巨型帧。

STEP 7 | 定义 HA 故障转移条件。

STEP 8 | **Commit**（提交）配置。

STEP 9 | 使用相同设置配置对等防火墙 PA-3050-1 (Device ID 0)，在步骤 2 选择 **Device ID 0** 除外。

STEP 10 | 还是在 PA-3050-1（ Device ID 0）上，创建目标 NAT 规则，以便主动-主要防火墙响应 ARP 请求。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 输入规则 **Name**（名称），该例中，名称将作为识别其为第 2 层 ARP 的目标 NAT 规则的依据。
3. 在 **NAT Type**（**NAT** 类型），选择 **ipv4**（默认）。
4. 在 **Original Packet**（原始数据包），为 **Source Zone**（源区域）选择 **Any**（任意）。
5. 在 **Destination Zone**（目标区域），选择您为外部网络创建的 Untrust 区域。
6. 允许 **Destination Interface**（目标接口）、**Service**（服务）、**Source Address**（源地址）继续设置为 **Any**（任意）。
7. 设置 **Destination Address**（目标地址）为 10.1.1.200。
8. **Translated Packet**（转换数据包）的源地址转换依旧为 **None**（无）。
9. 在 **Destination Address Translation**（目标地址转换）输入目标服务其的专有 IP 地址，此例中为 192.168.1.200。
10. 在 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选项卡上，为 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选择 **primary**（主要）以绑定 NAT 规则至处于主动-主要状态的防火墙。
11. 单击 **OK**（确定）。

STEP 11 | **Commit**（提交）配置。

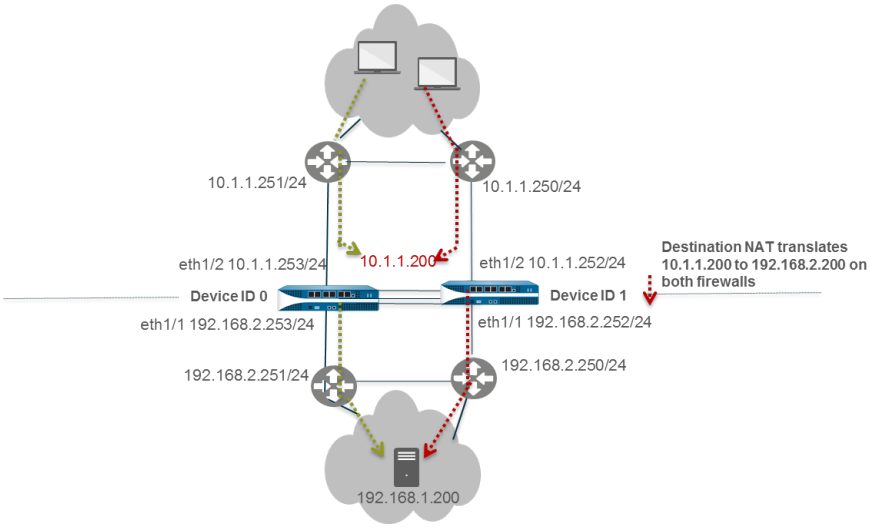
## 用例：在第三层中配置带有目标 *NAT* 的主动/主动 *HA*，进行 *ARP* 加载共享

第 3 层接口示例使用主动/主动 HA 模式下的 NAT 和 ARP 加载共享。PA-3050-1 具备 Device ID 0，而其 HA 对等 PA-3050-2 具备 Device ID 1。

在该用例中，两个 HA 防火墙必须响应 ARP 请求，获取目标 NAT 地址。通信可从 untrust 区域的任意 WAN 路由器到达任一防火墙。目标 NAT 将公共和共享 IP 地址转换为服务器的专有 IP 地址。该配置需要一个绑定至两个设备 ID 的目标 NAT 规则，以便防火墙响应 ARP 请求。



© 2019 Palo Alto Networks, Inc.




STEP 1 | 在 PA-3050-2（设备 ID 1）上，执行配置主动/主动 HA 的步骤 1 至步骤 3。

STEP 2 | 启用主动/主动 HA。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）> **Setup**（设置）并编辑。
2. 选择 **Enable HA**（启用 **HA**）。
3. 输入**Group ID**（组 **ID**），两道防火墙的组 ID 必须一致。防火墙使用组 ID 计算虚拟 MAC 地址（范围为 1-63）。
4. （可选）输入 **Description**（说明）。
5. 对于 **Mode**（模式），选择 **Active Active**（主动/主动）。
6. **Device ID** 选择 **1**。
7. 选中 **Enable Config Sync**（启用配置同步）。该设置用于同步两个防火墙的配置（默认为启用）。
8. 输入 **Peer HA1 IP Address**（对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
9. （可选）输入 **Backup Peer HA1 IP Address**（备份对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
10. 单击 **OK**（确定）。

STEP 3 | 配置主动/主动 HA。

执行步骤 6 到步骤 15。

STEP 4 | 配置 HA 虚拟地址。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Virtual Address**（虚拟地址），然后单击 **Add**（添加）。
2. 选择 **Interface**（接口）eth1/2。
3. 选择 **IPv4** 并 **Add**（添加）**IPv4 Address**（**IPv4** 地址）10.1.1.200。
4. 对于 **Type**（类型），选择 **ARP Load Sharing**（**ARP** 加载共享），为两个对端设备配置用于 ARP 加载共享的虚拟 IP 地址。

STEP 5 | 配置 ARP 加载共享。

设备选择算法旨在确定哪个 HA 防火墙将响应 ARP 请求以提供加载共享。

1. 在 **Device Selection Algorithm**（设备选择算法），选择以下其一：
   - **IP Modulo**（**IP** 模）— 防火墙根据 ARP 请求者 IP 地址的奇偶校验响应 ARP 请求。
   - **IP Hash**（**IP** 哈希）— 防火墙根据 ARP 请求者的源 IP 地址及目标 IP 地址的哈希响应 ARP 请求。
2. 单击 **OK**（确定）。


© 2019 Palo Alto Networks, Inc.

STEP 6 | 启用防火墙（除 PA-7000 系列防火墙）上的巨型帧。

STEP 7 | 定义 HA 故障转移条件。

STEP 8 | **Commit**（提交）配置。

STEP 9 | 使用相同设置配置对等防火墙 PA-3050-1（设备 ID 0），设置为 **0**（而不是 **1**）的 **Device ID** 除外。

STEP 10 | 还是在 PA-3050-1 （设备 ID 0）中，创建设备 ID 0 及设备 ID 1 的目标 NAT 规则。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 输入规则 **Name**（名称），该例中，名称将作为识别其为第 3 层 ARP 的目标 NAT 规则的依据。
3. 在 **NAT Type**（**NAT** 类型），选择 **ipv4**（默认）。
4. 在 **Original Packet**（原始数据包），为 **Source Zone**（源区域）选择 **Any**（任意）。
5. 在 **Destination Zone**（目标区域），选择您为外部网络创建的 Untrust 区域。
6. 允许 **Destination Interface**（目标接口）、**Service**（服务）、**Source Address**（源地址）继续设置为 **Any**（任意）。
7. 设置 **Destination Address**（目标地址）为 10.1.1.200。
8. **Translated Packet**（转换数据包）的源地址转换依旧为 None（无）。
9. 在 **Destination Address Translation**（目标地址转换）输入目标服务其的专有 IP 地址，此例中为 192.168.1.200。
10. 在 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选项卡上，为 **Active/Active HA Binding**（主动/主动 **HA** 绑定）选择 **both**（两者），绑定 NAT 规则至 Device ID 0 和 Device ID 1。
11. 单击 **OK**（确定）。

STEP 11 | **Commit**（提交）配置。

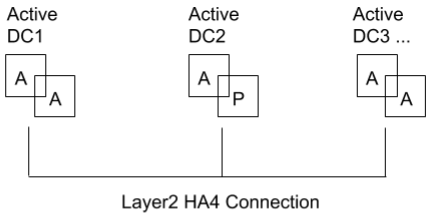


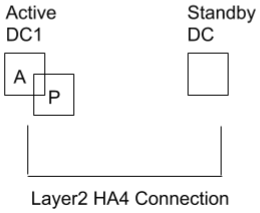
© 2019 Palo Alto Networks, Inc.

# HA 集群概述

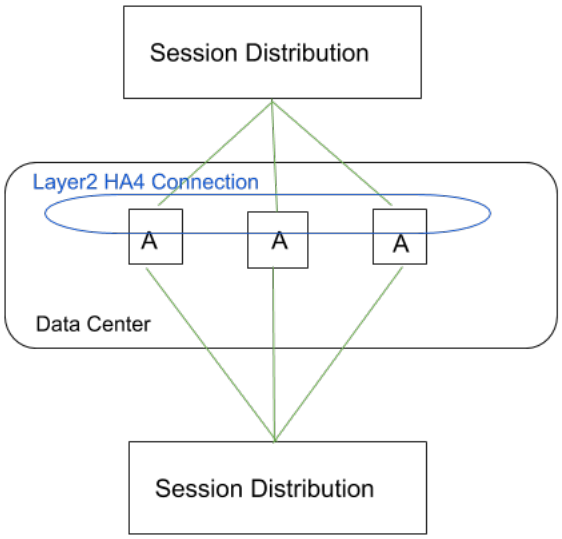
目前有很多 Palo Alto Networks® 防火墙型号都支持高可用性 (HA) 集群中最多 16 个防火墙之间的会话状态同步。HA 集群对等同步会话，以防止数据中心或带水平扩展防火墙的大型安全检查点出现故障。一旦网络中断或防火墙出现故障，会话会将故障转移到集群中的另一个防火墙。此类同步在下列用例中尤其有用。

第一个用例：如果 HA 对等分布在多个数据中心，那么，数据中心内部或之间不会出现单点故障。第二个是多数据中心用例，其中一个数据中心主用，另一个数据中心备用。




第三个用例是水平扩展的 HA 集群用例，其中，您将 HA 集群成员添加到单个数据中心，以扩展安全，确保会话生存能力。






© 2019 Palo Alto Networks, Inc.

HA 集群支持第三层或虚拟线路部署。集群中的 HA 对等可以是 HA 对和独立集群成员的组合。在 HA 集群中，所有成员均处于活跃状态，不存在被动防火墙的概念（HA 对除外），这样，可在将其添加到 HA 集群后，保持他们的主动/被动关系。

所有集群成员共享会话状态。一旦有新的防火墙加入到 HA 集群，就会触发集群中所有防火墙同步所有现有会话。HA4 和 HA4 备份连接是专用的集群链路，用于同步具有相同集群 ID 的所有集群成员的会话状态。集群成员之间的 HA4 链路用于检测集群成员之间的连接故障。非 HA 对的集群成员之间不支持 HA1（控制链路）、HA2（数据链路）和 HA3（数据包转发链路）。

对于尚未执行故障转移的正常会话，仅充当会话所有者的防火墙创建流量日志。对于已执行故障转移的会话，新的会话所有者（接收故障转移流量的防火墙）将创建流量日志。

支持 HA 集群的防火墙型号以及每个集群支持的最大成员数如下所示：

| 防火墙型号 | 每个集群支持的成员数 |
| --- | --- |
| PA-3200 系列 | 6 |
| PA-5200 系列 | 16 |
| 至少带有以下卡之一的 PA-7000 系列防火墙：PA-7000-100G-NPC、PA-7000-20GQXM-NPC、PA-7000-20GXM-NPC | PA-7080：4<br>PA-7050：6 |
| VM-300 | 6 |
| VM-500 | 6 |
| VM-700 | 16 |

请先考虑HA 集群最佳实践和配置，然后再开始配置 HA 集群。



© 2019 Palo Alto Networks, Inc.

# HA 集群最佳实践和配置

HA 集群配置要求和最佳实践如下所示。

- 配置要求和最佳实践
  - HA 集群成员必须是同型号的防火墙，并运行相同的 PAN-OS® 版本。

    在升级期间，防火墙成员将继续与不同版本的成员会话同步。
  - 强烈建议使用 Panorama 配置 HA 集群成员，使所有集群成员的所有配置和策略保持同步，这也是最佳做法。
  - HA 集群成员必须拥有相同组件的许可证，确保策略实施和内容检测功能的一致性。
  - 许可证应同时到期，防止出现许可证不匹配以及功能丧失等问题。
  - 所有集群成员都应运行相同版本的动态内容更新，确保安全实施的一致性。
  - HA 集群成员必须共享同一区域名称，使会话成功将故障转移到另一个集群成员。例如，假定进入名为 **`internal`** 的入口区域的会话因为链路下行而被丢弃。对于这些将故障转移到集群中 HA 防火墙对等设备的会话，该对等设备必须也有一个名为 **`internal`** 的区域。
  - 在正常（非故障）情况下，客户端到服务器流量和服务器到客户端流量必须返回到同一防火墙，以便对内容进行安全扫描。非对称流量不会被丢弃，但是，出于安全考虑，无法对其进行扫描。
- 会话同步最佳实践
  - 应在数据平面接口上使用专用的 HA 通信接口。HASI 接口不能用于 HA4。这会允许将 HA 对和集群会话同步分开，确保获得最大带宽和会话同步的可靠性。
  - 如果使用数据平面接口，HA4 的大小应合适。这可尽量确保集群成员之间会话状态的同步。
  - 最佳做法是为 HA4 通信链路设置一个专有集群网络，确保集群成员之间获得足够的带宽，从而实现不堵塞的低延迟连接。
  - 设计网络架构，执行流量工程以避免可能出现的争用情况，在这种情况下，网络会将流量从会话所有者引导至集群成员，然后即可成功实现防火墙之间会话的同步。第二层 HA4 连接必须具备足够的带宽和低延迟，允许 HA 成员之间的及时同步。HA4 延迟必须低于对等设备在集群成员之间切换流量时发生的延迟。
  - 设计网络架构以最大限度地减少不对称流量。会话设置需要一个集群成员来查看完整的 TCP 三向握手。
- 运行状态检查最佳实践
  - 在集群的 HA 对中，为 HA1、HA2 和 HA4 配置具有 HA 备份通信链路的主动/被动对。为 HA1、HA2、HA3 和 HA4 配置具有 HA 备份通信链路的主动/主动对。
  - 在所有集群成员上配置 HA4 备份链路。



© 2019 Palo Alto Networks, Inc.

# 配置 HA 集群

请先了解 HA 集群，再根据 HA 集群最佳实践和配置 将 HA 防火墙配置为集群成员。

STEP 1 | 建立可充当 HA 接口的接口（该接口之后会分配为 HA4 链路）。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并选择一个接口；例如，ethernet1/1。
2. 选择 **Interface Type**（接口类型）为**HA**。
3. 将接口分配到 **Security Zone**（安全区域）。
4. 单击 **OK**（确定）。
5. 重复此步骤以配置充当 HA4 备份链路的另一个接口。

STEP 2 | 启用 HA 集群。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后编辑集群设置。
2. **Enable Cluster Participation**（启用集群参与）。
3. 输入 **Cluster ID**（集群 **ID**），这是 HA 集群的唯一数字 ID，在此集群中，所有成员都可以共享会话状态，范围为 1-99。
4. 输入一个简短而有用的 **Cluster Description**（集群说明）。
5. （可选）更改 **Cluster Synchronization Timeout (min)**（集群同步超时（分钟）），这是本地防火墙在另一个集群成员（例如，处于未知状态时）阻止集群完全同步时，进入活动状态之前等待的最大分钟数；范围为 0-30；默认值为 0。
6. （可选）更改 **Monitor Fail Hold Down Time (min)**（监视失败抑制时间（分钟）），经过此时间后，将重新测试下行链路以查看该链路是否备份；范围为 1-60；默认值为 1。
7. 单击 **OK**（确定）。

STEP 3 | 配置 HA4 链路。

1. 选择 **HA Communications**（**HA** 通信），并在“集群链路”部分中编辑 HA4 部分。
2. 选择在第一步中配置的接口充当 HA4 链路**Port**（端口）的 **HA** 接口，例如， ethernet1/1。
3. 输入本地 HA 接口的 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）。
4. 输入 **Netmask**（网络掩码））。
5. （可选）更改 **HA4 Keep-alive Threshold (ms)**（**HA4 Keep-alive** 阈值（毫秒）），以指定防火墙必须从集群成员接收 keepalive 从而知晓集群成员是否正常运行的时间范围；范围为 5,000 - 60,000；默认值为 10,000。
6. 单击 **OK**（确定）。

STEP 4 | 配置 HA4 备份链路。

1. 编辑“HA4 备份”部分。
2. 选择在第一步中配置的其他接口充当 HA4 备份链路**Port**（端口）的 **HA** 接口。
3. 输入本地 HA 备份接口的 **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）。
4. 输入 **Netmask**（网络掩码））。
5. 单击 **OK**（确定）。

STEP 5 | 指定 HA 集群的所有成员，包括本地成员和任何 HA 对中的 HA 对等。

1. 选择 **Cluster Config**（集群配置）。
2. （在支持的防火墙上）**Add**（添加）对等成员的 **Device Serial Number**（设备序列号）。
3. （在 Panorama 上）**Add**（添加）并从下拉列表中选择 **Device**（设备），然后输入 **Device Name**（设备名称）。
4. 输入集群中 HA 对等的 **HA4 IP Address**（**HA4 IP** 地址）。



© 2019 Palo Alto Networks, Inc.

5. 输入集群中 HA 对等的 **HA4 Backup IP Address**（**HA4 备份 IP 地址**）。
6. 为所识别的对等启用 **Session Synchronization**（会话同步）。
7. （可选）输入有用的 **Description**（说明）。
8. 单击 **OK**（确定）。
9. 选择并 **Enable**（启用）设备。

STEP 6 | 为链路和路径监视 Define HA failover conditions（定义 HA 故障转移条件）。

STEP 7 | **Commit**（提交）。

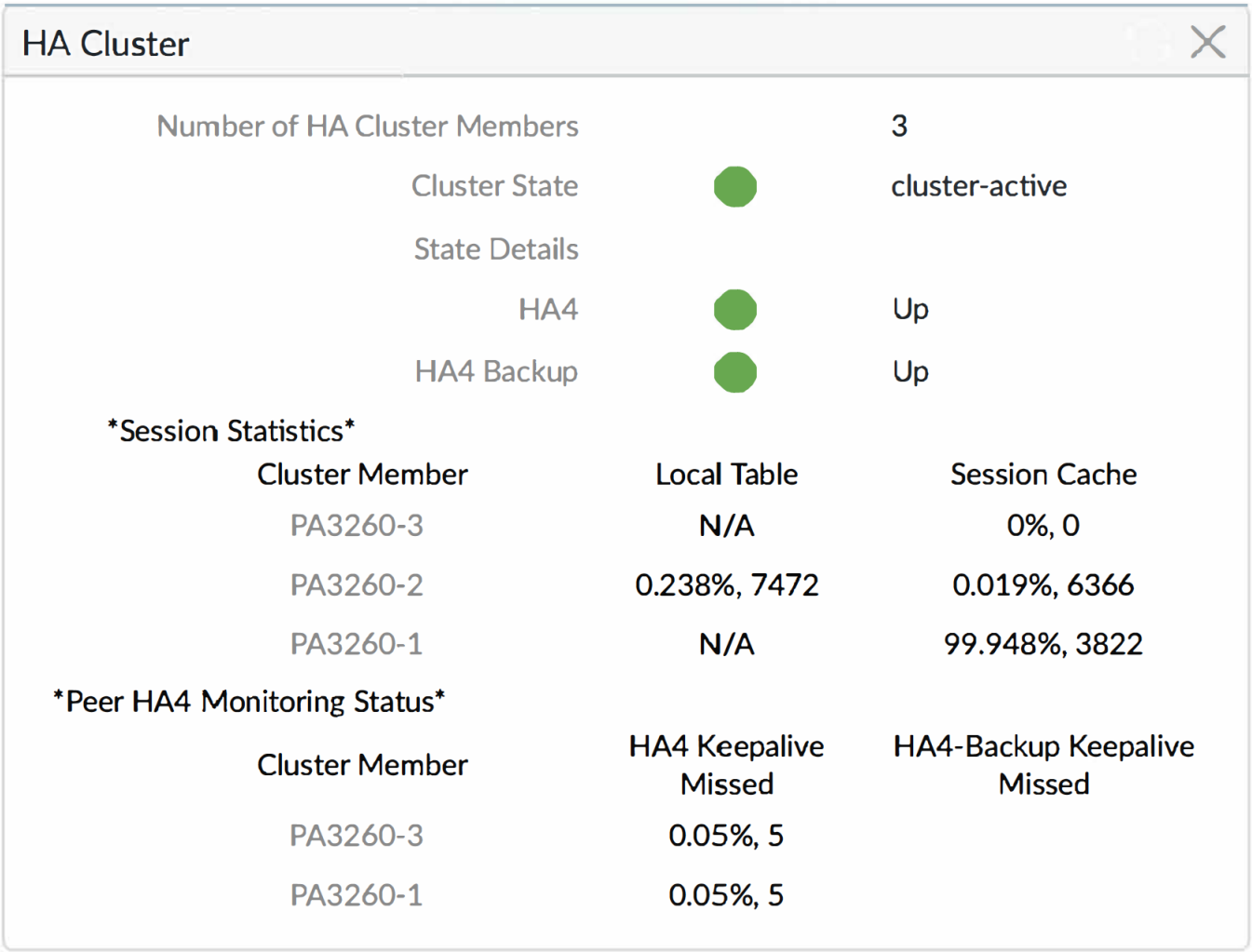
STEP 8 | （仅限 Panorama）刷新 HA 集群中的 HA 防火墙列表。

1. 在模板中，选择**Device**（设备）> **High Availability**（高可用性）> **Cluster Config**（将配置）。
2. 单击屏幕底部的 **Refresh**（刷新）。

STEP 9 | 在 UI 中查看 HA 集群信息。

1. 选择 **Dashboard**（仪表板）。
2. 查看 HA 集群字段。集群运行状态可通过顶部显示的集群状态和 HA4 连接进行了解。HA4 和 HA4 备份指示器将显示其中之一：绿色表示集群成员链路状态为上行。红色表示所有集群成员的链路状态均为下行。黄色表示一些集群成员的链路状态为上行，另一些集群成员的链路状态为下行。灰色表示未配置。中间部分显示的是本地会话表和会话缓存表的容量，这样，您可以监视表是否已满，并视情况计划防火墙的升级。底部显示的是 HA4 和 HA4 备份链路的通信故障，显示成员之间同步信息可能出现的错误。


© 2019 Palo Alto Networks, Inc.




STEP 10 | 访问 CLI 以查看 HA 集群和 HA4 链路信息，并执行其他 HA 集群任务。



© 2019 Palo Alto Networks, Inc.

# 刷新 HA1 SSH 密钥和配置密钥选项

所有 Palo Alto Networks 防火墙都预先配置有安全外壳 (SSH)，且高可用性(HA)防火墙可同时充当 SSH 服务器和 SSH 客户端。在配置主动/被动或主动/主动 HA 时，您可以为 HA 防火墙之间的 HA1（控制链路）连接启用加密。我们建议通过加密保护 HA 对等设备之间的 HA1 流量，尤其是防火墙不在同一站点时。在 HA1 控制链路上启用加密后，您可以使用 CLI 创建 SSH 服务配置文件，并保护 HA 防火墙之间的连接。

您可以通过 SSH 服务配置文件更改默认主机密钥类型，为 HA1 控制链路生成一对新的 SSH 主机公钥和私钥，并配置其他 SSH HA1 设置。您可以在无需重新启动 HA 对等设备的情况下，将新的主机密钥和配置的设置应用于防火墙。防火墙将与其对等设备重新建立 HA1 会话，以同步配置更改。此外，还可以为重新建立的 HA1 和 HA1 备份会话生成系统日志（子类型为 `ha`）。

以下示例显示的是如何在启用加密并访问 CLI 之后为 HA1 配置各种 SSH 设置。（有关 SSH 管理服务器配置文件示例的信息，请参阅刷新 SSH 密钥并配置用于管理接口连接的密钥选项。）

您必须启用加密，并且只有在此加密功能可以在 *HA* 对上正常运行后才能执行下列任务。

如果在 FIPS-CC 模式配置 *HA1* 控制链路，必须为会话密钥设置自动密钥更新参数。

要在收集器组内为每个专用日志收集器（日志收集器模式下的 *M* 系列或 *Panorama* 虚拟设备）使用相同的 *SSH* 连接，请从 *Panorama* 管理服务器配置 *SSH* 服务配置文件，并*Commit*（提交）*Panorama* 更改，然后*Push*（推送）配置到日志收集器。您还可以使用命令 ***set log-collector-group <name> general-setting management ssh***。

- 创建 SSH 服务配置文件，以更好地控制 HA 防火墙之间的 SSH 连接。

  本示例显示的是在未配置任何设置的情况下创建 HA 配置文件。

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>***
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. 若要验证是否已创建新配置文件，并查看任何现有配置文件的设置：

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles**

- （可选）设置 SSH 服务器为仅使用 HA1 会话的指定加密密码。

  默认情况下，HA1 SSH 允许用于 CLI HA 会话加密的所有受支持的密码。在设置一个或多个密码时，SSH 服务器仅在连接时通告这些密码。如果 SSH 客户端（HA 对等设备）尝试使用其他密码进行连接，则服务器会终止连接。

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ciphers ha-profiles *<name>* ciphers *<cipher>***

     **aes128-cbc** — 使用密码块链的 128 位 AES 密码

     **aes128-ctr** — 使用计数器模式的 128 位 AES 密码

     **aes128-gcm** — 使用 GCM (Galois/Counter Mode) 的 128 位 AES 密码

     **aes192-cbc** — 使用密码块链的 192 位 AES 密码



© 2019 Palo Alto Networks, Inc.

**aes192-ctr** — 使用计数器模式的 192 位 AES 密码

**aes256-cbc** — 使用密码块链的 256 位 AES 密码

**aes256-ctr** — 使用计数器模式的 256 位 AES 密码

**aes256-gcm** — 使用 GCM 的 256 位 AES 密码

3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
6. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**



如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份后，使用 *force* 选项将不起作用。）

7. 若要验证密码是否已更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles ciphers**

- （可选）设置默认主机密钥类型。

  如果在 HA1 控制链路上启用加密，除非您做出更改，否则，防火墙将使用默认主机密钥类型 RSA 2048。在与 HA 对等设备建立加密会话之前，HA1 SSH 连接仅使用默认主机密钥类型对 HA 对等设备进行身份验证。您可以更改默认主机密钥类型；选项包括 ECDSA 256、 384 或 521，或 RSA 2048、3072 或 4096。如果您偏向于更长的 RSA 密钥长度，或相比于 RSA 而言更喜欢 ECDSA，则更改默认主机密钥类型。在本示例中，默认主机密钥类型为 256 位的 ECDSA 密钥。此外，它还使用新的主机密钥在无需重启 HA 对等设备的情况下重新建立 HA1 连接。

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* default-hostkey key-type ECDSA key-length 256**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**



必须已在 *HA* 防火墙之间建立 *HA* 连接。如果防火墙尚未建立 *HA* 连接，您必须在控制链路连接上启用加密，将 *HA* 密钥导出到网络位置，并导入对等设备上的 *HA* 密钥。请参阅配置主动/被动 HA 或配置主动/主动 HA。

  6. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
  7. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**



如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使两台 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份后，使用 ***force*** 选项将不起作用。）

  8. 若要验证主机密钥是否已更新：

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* default-hostkey**

- （可选）从您选择用于 HA1 控制链路上 SSH 的一组密码中删除一个密码。



© 2019 Palo Alto Networks, Inc.

在本示例中，删除的是具有 128 位密钥的 AES CBC 密码。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **delete deviceconfig system ssh profiles ha-profiles *<name>* ciphers aes128-cbc**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
6. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**

   如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使两台 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份时，使用 ***force*** 选项将不起作用。）
7. 若要验证密码是否删除：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* ciphers**

- （可选）设置 HA1 SSH 服务器将支持的会话密钥交换算法。

默认情况下，SSH 服务器（HA 防火墙）向 SSH 客户端（HA 对等防火墙）通告所有密钥交换算法。



如果使用 *ECDSA* 默认密钥类型，最佳做法是使用 *ECDH* 密钥算法。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* kex *<value>***

   **diffie-hellman-group14-sha1** — 使用 SHA1 哈希的 Diffie-Hellman 组 14

   **Ecdh-sha2-nistp256**—使用 — 根据美国国家标准与技术研究院 (NIST) P-256 使用 SHA2-256 哈希的椭圆曲线 Diffie-Hellman

   **ecdh-sha2-nistp384** — NIST P-384 使用 SHA2-384 哈希的椭圆曲线 Diffie-Hellman

   **ecdh-sha2-nistp521** — NIST P-521 使用 SHA2-521 哈希的椭圆曲线 Diffie-Hellman
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
6. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**

   如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使两台 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份时，使用 ***force*** 选项将不起作用。）
7. 若要验证密钥交换算法是否更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

- （可选）设置 HA1 SSH 服务器将支持的消息认证码 (MAC)。


© 2019 Palo Alto Networks, Inc.

默认情况下，服务器向客户端通告所有 MAC 算法。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* mac *<value>***

   **hmac-sha1** — 使用 SHA1 加密哈希的 MAC

   **hmac-sha2-256** — 使用 SHA2-256 加密哈希的 MAC

   **hmac-sha2-512** — 使用 SHA2-512 加密哈希的 MAC
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
6. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**

   如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使两台 *HA* 对等设备之间出现短暂的裂脑情形。配置 *HA1* 备份时，使用 ***force*** 选项将不起作用。
7. 若要验证 MAC 算法是否更新：

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

- （可选）为 HA1 SSH 重新生成 ECDSA 或 RSA 主机密钥以替代现有密钥，并使用新密钥在 HA 对等设备之间重新建立 HA1 会话，在无需重启 HA 对等设备。

  HA 对等设备使用主机密钥相互验证身份。在本示例中，重新生成 ECDSA 256 默认主机密钥。

  重新生成主机密钥并不会更改您的默认主机密钥类型。要重新生成您正在使用的默认主机密钥，必须在重新生成时指定默认主机密钥类型和长度。重新生成非默认主机密钥类型的主机密钥时，只需重新生成一个您正在使用的密钥之外的密钥即可，因此，该密钥不起作用。

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh regenerate-hostkeys ha key-type ECDSA key-length 256**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

     必须已在 *HA* 防火墙之间建立 *HA* 连接。如果防火墙尚未建立 *HA* 连接，您必须在控制链路连接上启用加密，将 *HA* 密钥导出到网络位置，并导入对等设备上的 *HA* 密钥。请参阅配置主动/被动 HA 或配置主动/主动 HA。
  6. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
  7. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**

     如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使两台 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份后，使用 ***force*** 选项将不起作用。）



© 2019 Palo Alto Networks, Inc.

- （可选）通过设置密钥更新参数，确定 SSH 何时通过 HA1 控制链路对会话密钥自动执行密钥更新。

  会话密钥用于加密 HA 对等设备之间的流量。您设置的参数可以是数据量（MB）、时间间隔（秒）和数据包计数。一旦其中一个密钥更新参数达到其配置的值，SSH 将启动密钥交换。

  如果您不确定您配置的参数是否会在您想要密钥更新时立即达到其值，您可以配置第二个或第三个参数。第一个达到配置值的参数将提示进行密钥更新，然后，防火墙将重置所有密钥更新参数。

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey data 32**

     先前密钥更新结束后，若出现大量数据传输（以兆字节为单位），则会进行密钥更新。默认值基于您使用的密码，范围从 1GB 到 4GB；范围为 10MB - 4,000MB。或者，您可以使用命令 **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey data default**，从而将数据参数设为您正在使用的单个密码的默认值。
  3. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey interval 3600**

     先前密钥更新结束后，经过指定时间间隔（以秒为单位），则会发生密钥更新。默认情况下，禁用基于时间的密钥更新（设为无）。范围为 10 至 3,600。
  4. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey packets 27**

     先前密钥更新结束后，传输指定数量 ($2^n$) 的数据包后，则会进行密钥更新。例如，14 表示在密钥更新发生前最多可传输 $2^{14}$ 个数据包。默认值为 $2^{28}$。范围为 12 至 27（$2^{12}$ - $2^{27}$）。或者，您可以输入**set deviceconfig system ssh profiles ha-profiles *<name>* session-rekey packets default**，将数据包参数设为 $2^{28}$。

     根据您的流量类型和网络速度（以及对您适用的 *FIPS-CC* 要求）选择密钥更新参数。请勿将参数设置过低，否则，可能会影响 *SSH* 性能。
  5. admin@PA-3250# **commit**
  6. admin@PA-3250# **exit**
  7. （HA1 备份已配置）admin@PA-3250> **request high-availability session-reestablish**
  8. （HA1 备份未配置或 HA1 备份链路已关闭）admin@PA-3250> **request high-availability session-reestablish force**

     如果无 *HA1* 备份，您可以强制防火墙重新建立 *HA1* 会话，使两台 *HA* 对等设备之间出现短暂的裂脑情形。（配置 *HA1* 备份后，使用 ***force*** 选项将不起作用。）
  9. 若要验证更改：

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles *<name>* session-rekey**

- 通过选择配置文件并重新启动 HA1 SSH 服务激活配置文件。

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh ha ha-profile *<name>***
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **set ssh service-restart ha**
  6. 若要验证使用的配置文件是否正确：


© 2019 Palo Alto Networks, Inc.

admin@PA-3250> **configure**

admin@PA-3250# **show deviceconfig system ssh ha**



© 2019 Palo Alto Networks, Inc.

# HA 防火墙状态

HA 可能处于以下状态之一：

| HA 防火墙状态 | 发生于 | 说明 |
| --- | --- | --- |
| 初始 | A/P 或 A/A | 加入 HA 对后防火墙的过渡状态。在发现对等并开始协商前，启动后的防火墙将保持该状态。超时后，如果 HA 协商未开始，防火墙将变成主动。 |
| 活跃 | A/P | 在主动/主动 HA 配置中的主动防火墙状态。 |
| 被动 | A/P | 主动/被动配置中的被动防火墙状态。被动防火墙可在不干扰网络的情况下变为主动防火墙。尽管被动防火墙未在处理其他通信：<br>• 如果被动链接状态配置为“自动”，则被动防火墙将运行路由协议、监控链接及路径状态，且被动防火墙将预先协商 LACP 和 LLDP，如果 LACP 和 LLDP 预先协商已分别预先配置。<br>• 被动防火墙会同步流动状态、运行时对象及配置。<br>• 被动防火墙使用呼叫协议监控主动防火墙的状态。 |
| 主动主要 | A/A | 在主动/主动配置中，防火墙处于连接至 User-ID 代理、运行 DHCP 服务器及 DHCP 中继、匹配 NAT 和 PBF 规则与主动-主要防火墙设备 ID 的状态。处于该状态的防火墙可拥有并设置会话。 |
| 主动辅助 | A/A | 在主动/主动配置中，防火墙处于连接至 User-ID 代理、运行 DHCP 服务器、匹配 NAT 和 PBF 规则与主动-辅助防火墙设备 ID 的状态。处于主动-辅助状态的防火墙不支持 DHCP 中继。处于该状态的防火墙可拥有并设置会话。 |
| 暂定 | A/A | 由以下中的一项引起的防火墙状态（主动/主动配置中）：<br>• 防火墙故障。<br>• 被监控对象（链接或路径）故障。<br>• 防火墙处于挂起或不运行的状态。<br>处于试验状态的防火墙从对等同步会话和配置。<br>• 在虚拟线路部署中，因路径失败进入试验状态的防火墙会通过 HA3 链路将收到的数据包发送至对等防火墙进行处理。处理完该数据包后，对等防火墙会通过 HA3 链路将其返回，然后从入口接口发出。该行为将转发路径保存于虚拟线路部署。<br>• 在第 3 层部署中，处于试验状态的防火墙收到数据包后将通过 HA3 链路发送数据包至对等防火墙，让其拥有或建立会话。根据网络拓扑，该防火墙会将数据包发出至目标或将其发送回处于试验状态的对等防火墙以转发。<br>在路径或链接失败排除后，或当出现故障的防火墙从试验状态变成主动-辅助状态时，则会触发**Tentative Hold Time**（试验保持时间），出现路由收敛。防火墙将尝试构建路由邻接，并在处理任何数据包之前先填充其路由表。如果没有此计时器，恢复中的防火墙会立即进入主动二级状态，并且会因为没有必需的路由而使数据包被静默丢弃。<br>防火墙脱离挂起状态后，即会在链接启用并能处理流入的数据包后进入试验状态，持续时间被称为 **Tentative Hold Time**（试验保持时间）。 |



© 2019 Palo Alto Networks, Inc.

| HA 防火墙状态 | 发生于 | 说明 |
| --- | --- | --- |
| | | **Tentative Hold Time range**（试验保持时间，秒）可禁用（设置为 0 秒）或设为 10-600；默认为 60 秒。 |
| 不运作 | A/P 或 A/A | 由数据面板或配置不匹配，如仅配置一个防火墙用于数据包转发，VR 同步或 QoS 同步引起的错误状态。<br>在主动/主动模式中，所有可导致试验状态的原因可导致不运作状态。 |
| 挂起 | A/P 或 A/A | 设备被禁用，因此，无法传递数据流量。虽然仍会发生 HA 通信，但设备不会参与 HA 选择过程。没有用户干预，它无法转换至 HA 运行状态。 |


© 2019 Palo Alto Networks, Inc.

# 参考资料：高可用性同步

如果您已在 HA 对的对等设备启用配置同步，您在一个对等设备上配置的大部分配置设备将在提交后自动同步至另一个对等设备。要避免配置冲突，始终在主动（主动/被动）或主动-主要（主动/主动）对等设备上进行配置更改，等待其在做出任何其他配置更改前同步至对等设备。

仅已提交配置会在 *HA* 对等间同步。*HA* 同步时，提交队列中的任何配置不会被同步。

以下主题对您必须单独在每个防火墙上配置的配置设置（这些设置不会从 HA 对等同步）进行了说明。

- 哪些设置不会在主动/被动 HA 中同步？
- 哪些设置不会在主动/主动 HA 中同步？
- 系统运行时信息同步

## 哪些设置不会在主动/被动 HA 中同步？

您必须在处于主动/被动部署的 HA 对防护墙配置以下设置。这些设置不会从一个对等同步至另一个对等。

| 配置项 | 哪些设置不会在主动/被动中同步？ |
|---|---|
| 管理接口设置 | 所有管理配置设置必须在每个防火墙上单独配置，包括：<br>• **Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（常规设置）— 主机名、域、登录横幅、SSL/TLS 服务配置文件（和相关联证书）、时区、区域、日期、时间、纬度和经度。<br>• **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Management Interface Settings**（管理界面设置）— IP 类型、IP 地址、子网掩码、默认网关、IPv6 地址/前缀长度、默认 IPv6 网关、速度、MTU 和服务（HTTP、HTTP OCSP、HTTPS、Telnet、SSH、Ping、SNMP、User-ID、User-ID Syslog Listener-SSL 和 User-ID Syslog Listener-UDP） |
| Multi-vsys 功能 | 必须激活对中每个防火墙上的虚拟系统许可证，以增加超出 PA-3200 系列、PA-5200 系列和 PA-7000 系列防火墙提供的默认基本数量的虚拟系统数量。<br>您必须在每个防火墙上启用 **Multi Virtual System Capability**（多个虚拟系统功能）（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（常规设置））。 |
| Panorama 设置 | 在每个防火墙上设置以下 Panorama 设置（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Panorama Settings**（**Panorama** 设置））。<br>• **Panorama** 服务器<br>• **Disable Panorama Policy and Objects**（禁用 **Panorama** 策略及对象）和 **Disable Device and Network Template**（禁用设备和网络模板） |
| SNMP | **Device**（设备）> **Setup**（设置）> **Operations**（操作）> **SNMP Setup**（**SNMP** 设置） |
| 服务 | **Device**（设备）> **Setup**（设置）> **Services**（服务） |


© 2019 Palo Alto Networks, Inc.

| 配置项 | 哪些设置不会在主动/被动中同步？ |
| --- | --- |
| 全局服务路由 | **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Service Route Configuration**（服务路由配置） |
| 遥测和威胁情报设置 | **Device**（设备）> **Setup**（设置）> **Telemetry and Threat Intelligence**（遥测和威胁情报） |
| 数据保护 | **Device**（设备）> **Setup**（设置）> **Content-ID**（内容-ID）> **Manage Data Protection**（管理数据保护） |
| 巨型帧 | **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Session Settings**（会话设置）> **Enable Jumbo Frame**（启用巨型帧） |
| 数据包缓冲区保护 | **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Session Settings**（会话设置）> **Packet Buffer Protection**（数据包缓冲区保护）<br>**Network**（网络）> **Zones**（区域）> **Enable Packet Buffer Protection**（启用数据包缓冲区保护） |
| 转发代理服务器证书设置 | **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Decryption Settings**（加密设置）> **SSL Forward Proxy Settings**（SSL 转发代理设置） |
| HSM 加密的主密钥 | **Device**（设备）> **Setup**（设置）> **HSM** > **Hardware Security Module Provider**（硬件安全模块供应商）> **Master Key Secured by HSM**（HSM 加密的主密钥） |
| 日志导出设置 | **Device**（设备）> **Scheduled Log Export**（计划日志导出） |
| 软件更新 | 您可以单独在每个防火墙上下载和安装软件更新，或将其下载至一个对等，然后将该更新同步至另一个对等。您必须在每个对端设备上安装更新（**Device**（设备）> **Software**（软件））。 |
| GlobalProtect 代理包 | 您可以单独在每个防火墙上单独下载和安装 GlobalProtect 应用更新，或将其下载至一个对等，然后将该更新同步至另一个对等。您必须在每个对端设备上分别激活（**Device**（设备）> **GlobalProtect Client**（GlobalProtect 客户端））。 |
| 内容更新 | 您可以单独在每个防火墙上下载和安装内容更新，或将其下载至一个对等，然后将该更新同步至另一个对等。您必须在每个对端设备上安装更新（**Device**（设备）> **Dynamic Updates**（动态更新））。 |
| 许可证/订阅 | **Device**（设备）> **Licenses**（许可证） |
| 支持订阅 | **Device**（设备）> **Support**（支持） |
| 主密钥 | HA 对中每个防火墙的主密钥必须相同，但是您必须在每个防火墙上手动输入（**Device**（设备）> **Master Key and Diagnostics**（主密钥和诊断））。<br>在更改主密钥前，您必须禁用两个对端设备的配置同步（**Device**（设备）> **High Availability**（高可用性）> **General**（常规）> **Setup**（设置），并清除 **Enable Config Sync**（启用配置同步）复选框），然后在更改密钥后重新启用同步。 |
| 报告、日志和仪表板设置 | 日志数据、报告、仪表板数据和设置（列显示、部件）不在对等间同步。但报告配置设置会进行同步。 |


© 2019 Palo Alto Networks, Inc.

| 配置项 | 哪些设置不会在主动/被动中同步？ |
| --- | --- |
| HA 设置 | **Device**（设备）> **High Availability**（高可用性） |
| 规则使用数据 | 命中次数、创建日期和修改日期等规则使用数据不会在对等设备间同步。您需要登录到每个防火墙，以查看每个防火墙的策略规则命中次数数据，或使用 Panorama 查看 HA 防火墙对等设备上的信息。 |
| 仅通过 SSL 运行的设备管理证书和 Syslog 通信证书 | **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）<br>通过 SSL 运行的设备管理证书或 syslog 通信证书不与 HA 对等设备同步。 |
| 证书配置文件中的证书 | **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件） |
| 仅用于设备管理的 SSL/TLS 服务配置文件 | **Device**（设备）> **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）<br>用于设备管理的 SSL/TLS 服务配置文件不与 HA 对等设备同步。 |
| Device-ID 和 IoT Security | IP 地址到设备映射和策略规则建议不会与 HA 对等同步。 |

## 哪些设置不会在主动/主动 HA 中同步？

您必须在处于主动/主动部署的 HA 对防护墙配置以下设置。这些设置不会从一个对等同步至另一个对等。

| 配置项 | 哪些设置不会在主动/主动中同步？ |
| --- | --- |
| 管理接口设置 | 所有管理配置设置必须在每个防火墙上单独配置，包括：<br>• **Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（常规设置）— 主机名、域、登录横幅、SSL/TLS 服务配置文件（和相关联证书）、时区、区域、日期、时间、纬度和经度。<br>• **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Management Interface Settings**（管理界面设置）— IP 地址、子网掩码、默认网关、IPv6 地址/前缀长度、默认 IPv6 网关、速度、MTU 和服务（HTTP、HTTP OCSP、HTTPS、Telnet、SSH、Ping、SNMP、User-ID、User-ID Syslog Listener-SSL 和 User-ID Syslog Listener-UDP） |
| Multi-vsys 功能 | 必须激活对中每个防火墙上的虚拟系统许可证，以增加超出 PA-3200 系列、PA-5200 系列和 PA-7000 系列防火墙提供的默认基本数量的虚拟系统数量。<br>您必须在每个防火墙上启用 **Multi Virtual System Capability**（多个虚拟系统功能）（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（常规设置））。 |
| Panorama 设置 | 在每个防火墙上设置以下 Panorama 设置（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Panorama Settings**（**Panorama** 设置））。<br>• **Panorama** 服务器<br>• **Disable Panorama Policy and Objects**（禁用 **Panorama** 策略及对象）和 **Disable Device and Network Template**（禁用设备和网络模板） |


© 2019 Palo Alto Networks, Inc.

| 配置项 | 哪些设置不会在主动/主动中同步？ |
| --- | --- |
| SNMP | **Device**（设备）> **Setup**（设置）> **Operations**（操作）> **SNMP Setup**（SNMP 设置） |
| 服务 | **Device**（设备）> **Setup**（设置）> **Services**（服务） |
| 全局服务路由 | **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Service Route Configuration**（服务路由配置） |
| 遥测和威胁情报设置 | **Device**（设备）> **Setup**（设置）> **Telemetry and Threat Intelligence**（遥测和威胁情报） |
| 数据保护 | **Device**（设备）> **Setup**（设置）> **Content-ID**（内容-ID）> **Manage Data Protection**（管理数据保护） |
| 巨型帧 | **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Session Settings**（会话设置）> **Enable Jumbo Frame**（启用巨型帧） |
| 数据包缓冲区保护 | **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Session Settings**（会话设置）> **Packet Buffer Protection**（数据包缓冲区保护）<br>**Network**（网络）> **Zones**（区域）> **Enable Packet Buffer Protection**（启用数据包缓冲区保护） |
| 转发代理服务器证书设置 | **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Decryption Settings**（加密设置）> **SSL Forward Proxy Settings**（SSL 转发代理设置） |
| HSM 配置 | **Device**（设备）> **Setup**（设置）> **HSM** |
| 日志导出设置 | **Device**（设备）> **Scheduled Log Export**（计划日志导出） |
| 软件更新 | 您可以单独在每个防火墙上下载和安装软件更新，或将其下载至一个对等，然后将该更新同步至另一个对等。您必须在每个对端设备上安装更新（**Device**（设备）> **Software**（软件））。 |
| GlobalProtect 代理包 | 您可以单独在每个防火墙上单独下载和安装 GlobalProtect 应用更新，或将其下载至一个对等，然后将该更新同步至另一个对等。您必须在每个对端设备上分别激活（**Device**（设备）> **GlobalProtect Client**（GlobalProtect 客户端））。 |
| 内容更新 | 您可以单独在每个防火墙上下载和安装内容更新，或将其下载至一个对等，然后将该更新同步至另一个对等。您必须在每个对端设备上安装更新（**Device**（设备）> **Dynamic Updates**（动态更新））。 |
| 许可证/订阅 | **Device**（设备）> **Licenses**（许可证） |
| 支持订阅 | **Device**（设备）> **Support**（支持） |
| Ethernet 接口 IP 地址 | 所有以太网接口配置设置会同步，但 IP 地址除外（**Network**（网络）> **Interface**（接口）> **Ethernet**（以太网））。 |
| Loopback 接口 IP 地址 | 所有回环接口配置设置会同步，但 IP 地址除外（**Network**（网络）> **Interface**（接口）> **Loopback**（回环））。 |



© 2019 Palo Alto Networks, Inc.

| 配置项 | 哪些设置不会在主动/主动中同步？ |
| --- | --- |
| 隧道接口 IP 地址 | 所有隧道接口配置设置会同步，但 IP 地址除外（**Network**（网络）> **Interface**（接口）> **Tunnel**（隧道））。 |
| LACP 系统优先级 | 主动/主动部署中的每个对端设备必须具备独特的 LACP 系统 ID（**Network**（网络）> **Interface**（接口）> **Ethernet**（以太网）> **Add Aggregate Group**（添加集成组）> **System Priority**（系统优先级））。 |
| VLAN 接口 IP 地址 | 所有 VLAN 接口配置设置会同步，但 IP 地址除外（**Network**（网络）> **Interface**（接口）> **VLAN**）。 |
| 虚拟路由器 | 仅在启用 VR 同步时会进行虚拟路由器配置同步（**Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Packet Forwarding**（数据包转发））。是否启用同步取决于您的网络设计，包括您是否拥有非对称性路由。 |
| IPSec 隧道 | IPSec 隧道配置同步取决于您是否已配置使用浮动 IP 地址的虚拟地址（**Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Virtual Address**（虚拟地址））。如果您已配置浮动 IP 地址，这些设置会自动同步。否则，您必须在每个对等上单独配置这些设置。 |
| GlobalProtect 门户配置 | GlobalProtect 门户配置同步取决于您是否已配置使用浮动 IP 地址的虚拟地址（**Network**（网络）> **GlobalProtect** > **Portals**（门户））。如果您已配置浮动 IP 地址，GlobalProtect 门户配置设置会自动同步。否则，您必须在每个对等上单独配置这些门户设置。 |
| GlobalProtect 网关配置 | GlobalProtect 网关配置同步取决于您是否已配置使用浮动 IP 地址的虚拟地址（**Network**（网络）> **GlobalProtect** > **Gateways**（网关））。如果您已配置浮动 IP 地址，GlobalProtect 网关配置设置会自动同步。否则，您必须在每个对等上单独配置这些网关设置。 |
| QoS | 仅在启用 **QoS Sync**（**QoS** 同步）时会进行 QoS 配置同步（**Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）> **Packet Forwarding**（数据包转发））。您可能选择不同步 Qos 设置，例如，每个链接的带宽不同或您的服务提供商延迟不同。 |
| LLDP | 主动/主动配置中，LLDP 状态或单个防火墙数据不会同步（**Network**（网络）> **Network Profiles**（网络配置文件）> **LLDP**）。 |
| BFD | 主动/主动配置中，BFD 配置或 BFD 会话数据不会同步（**Network**（网络）> **Network Profiles**（网络配置文件）> **BFD Profile**（**BFD** 配置文件））。 |
| IKE 网关 | IKE 网关配置同步取决于您是否已配置使用浮动 IP 地址的虚拟地址（**Network**（网络）> **IKE Gateways**（**IKE** 网关））。如果您已配置浮动 IP 地址，IKE 网关配置设置会自动同步。否则，您必须在每个对等上单独配置 IKE 网关设置。 |
| 主密钥 | HA 对中每个防火墙的主密钥必须相同，但是您必须在每个防火墙上手动输入（**Device**（设备）> **Master Key and Diagnostics**（主密钥和诊断））。<br>在更改主密钥前，您必须禁用两个对端设备的配置同步（**Device**（设备）> **High Availability**（高可用性）> **General**（常规）> **Setup**（设置），并清除 **Enable Config Sync**（启用配置同步）复选框），然后在更改密钥后重新启用同步。 |


© 2019 Palo Alto Networks, Inc.

| 配置项 | 哪些设置不会在主动/主动中同步？ |
| --- | --- |
| 报告、日志和仪表板设置 | 日志数据、报告、仪表板数据和设置（列显示、部件）不在对等间同步。但报告配置设置会进行同步。 |
| HA 设置 | • **Device**（设备）> **High Availability**（高可用性）<br>• （例外为 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Configuration**（主动/主动配置）> **Virtual Addresses**（虚拟地址），不进行同步。） |
| 规则使用数据 | 命中次数、创建日期和修改日期等规则使用数据不会在对等设备间同步。您需要登录到每个防火墙，以查看每个防火墙的策略规则命中次数数据，或使用 Panorama 查看 HA 防火墙对等设备上的信息。 |
| 仅通过 SSL 运行的设备管理证书和 Syslog 通信证书 | **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）<br>通过 SSL 运行的设备管理证书或 syslog 通信证书不与 HA 对等设备同步。 |
| 证书配置文件中的证书 | **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件） |
| 仅用于设备管理的 SSL/TLS 服务配置文件 | **Device**（设备）> **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）<br>用于设备管理的 SSL/TLS 服务配置文件不与 HA 对等设备同步。 |
| Device-ID 和 IoT Security | IP 地址到设备映射和策略规则建议不会与 HA 对等同步。 |

## 系统运行时信息同步

下表对 HA 对端设备之间同步的系统运行时信息进行汇总。

| 运行时信息 | 配置已同步？ | | HA 链接 | 详细信息 |
| --- | --- | --- | --- | --- |
| | A/P | A/A | | |
| 管理层面 | | | | |
| 用户到组的映射 | 是 | 是 | HA1 | |
| 跨虚拟系统的用户映射 | 是 | 是 | HA1 | |
| 用户到 IP 地址映射 | 是 | 是 | HA1 | |
| DHCP 租赁（作为服务器） | 是 | 是 | HA1 | 如果 HA 对等设备上的 PAN-OS 版本不匹配，则 DHCP 租赁（作为服务器）配置信息将不会同步。 |
| DNS 缓存 | 否 | 否 | N/A | |


© 2019 Palo Alto Networks, Inc.

| 运行时信息 | 配置已同步？ | | HA 链接 | 详细信息 |
|---|---|---|---|---|
| | A/P | A/A | | |
| FQDN 刷新 | 否 | 否 | N/A | |
| IKE 密钥（阶段 2） | 是 | 是 | HA1 | |
| 转发信息库 (FIB) | 是 | 是 | HA1 | |
| PAN-DB URL 缓存 | 是 | 否 | HA1 | 这在数据数据库备份至磁盘（每 8 个小时 1 次，即 URL 数据库版本更新时）或防火墙重启时同步。 |
| 内容（手动同步） | 是 | 是 | HA1 | |
| PPPoE、PPPoE 租用 | 是 | 是 | HA1 | |
| DHCP 客户端设置及租赁 | 是 | 是 | HA1 | 如果 HA 对等设备上的 PAN-OS 版本不匹配，则 DHCP 客户端设置及租赁配置信息将不会同步。 |
| 记录于用户列表的 SSL VPN | 是 | 是 | HA1 | |
| 数据面板 | | | | |
| 会话表 | 是 | 是 | HA2 | • 主动/被动对等不同步 ICMP 或主机会话信息。<br>• 主动/主动对等不同步主机会话、多播路会话或 BFD 会话信息。<br>  主机会话是指终止在其中一个防火墙接口上的会话，例如对其中一个防火墙接口或 *GP* 隧道执行 *ping* 操作的 *ICMP* 会话。 |
| ARP 表 | 是 | 否 | HA2 | |
| 邻居发现 (ND) 表 | 是 | 否 | HA2 | |
| MAC 表 | 是 | 否 | HA2 | |


© 2019 Palo Alto Networks, Inc.

| 运行时信息 | 配置已同步？ | | HA 链接 | 详细信息 |
|---|---|---|---|---|
| | A/P | A/A | | |
| IPSec 序列号（反重放） | 是 | 是 | HA2 | |
| DoS 阻止列表条目 | 否 | 否 | N/A | |
| 虚拟 MAC | 是 | 是 | HA2 | |
| SCTP 关联 | 是 | 否 | HA2 | |

# 监控

为了预防可能出现的问题，并在需要时加快事件响应，防火墙使用可自定义报告和信息报告提供有关流量和用户模式的情报。利用仪表盘、应用程序命令中心 (ACC)、报告和防火墙日志，您可以监控网络上的活动。您可以使用预定义或自定义视图来监视日志并筛选日志信息以生成报告。例如，您可以使用预定义模板生成用户活动报告或分析报告和日志，以解释网络上的异常行为并生成通信模式的自定义报告。为了通过直观视觉方式呈现网络活动，仪表盘和 ACC 包括了小部件、图表和表格，您可与它们进行互动，以便查找您关注的信息。此外，您可以配置防火墙，以便将监控信息作为电子邮件通知、Syslog 消息、SNMP 陷阱和 NetFlow 记录发送到外部服务。


> 使用仪表板
> 使用应用程序命令中心
> 使用 App-Scope 报告
> 使用自动关联引擎
> 执行数据包捕获
> 监视应用程序和威胁
> 查看和管理日志
> 监控阻止列表
> 查看和管理报告
> 查看策略规则使用情况
> 使用外部服务进行监控
> 配置日志转发
> 配置电子邮件警报
> 使用 Syslog 进行监控
> SNMP 监控和陷阱
> 将日志转发到 HTTP(S) 目标
> NetFlow 监控

# 使用仪表板

**Dashboard**（仪表板）选项卡小部件显示一般防火墙信息，如软件版本、每个接口的运行状态、资源使用率以及威胁日志、配置日志和系统日志中的最多 10 个最新条目。默认情况下显示所有可用的小部件，但每个管理员可根据需要删除和添加各个小部件。单击刷新图标，更新仪表盘或单个小部件。要更改自动刷新间隔，请从下拉列表（**1 min**（**1** 分钟）、**2 mins**（**2** 分钟）、**5 mins**（**5** 分钟）或 **Manual**（手动））中选择间隔。要向仪表盘添加小部件，请单击小部件下拉列表，选择类型，然后选择小部件名称。要删除小部件，请在标题栏单击。下表介绍了仪表盘小部件。

| 仪表盘图表 | 说明 |
|---|---|
| 热门应用程序 | 显示会话最多的应用程序。块大小表示会话的相对数量（将鼠标置于块之上可查看数字），颜色表示安全风险 — 从绿色（最低）到红色（最高）。单击应用程序可查看其应用程序配置文件。 |
| 热门高风险应用程序 | 与热门应用程序类似，同时还显示会话最多、风险最高的应用程序。 |
| 常规信息 | 显示防火墙名称、型号、PAN-OS 软件版本、应用程序、威胁、URL 筛选定义版本、当前日期和时间以及距离上次重新启动的时间长度。 |
| 接口状态 | 表示每个接口的状态为开启（绿色）、关闭（红色）还是未知（灰色）。 |
| 威胁日志 | 显示威胁日志中最后 10 个条目的威胁 ID、应用程序以及日期和时间。威胁 ID 是违反 URL 过滤配置文件的恶意软件说明或 URL。 |
| 配置日志 | 显示配置日志中最后 10 个条目的管理员用户名、客户端（Web 或 CLI）以及日期和时间。 |
| 数据过滤日志 | 显示数据过滤日志中最后 60 分钟的说明以及日期和时间。 |
| URL 过滤日志 | 显示 URL 过滤日志中最后 60 分钟的说明以及日期和时间。 |
| 系统日志 | 显示系统日志中最后 10 个条目的说明以及日期和时间。<br>已安装配置条目表示配置更改提交成功。 |
| 系统资源 | 显示管理 CPU 使用率、数据面板使用率以及会话计数（将显示通过防火墙建立的会话数目）。 |
| 登录管理 | 显示当前登录的每个管理员的源 IP 地址、会话类型（Web 或 CLI）和会话开始时间。 |
| ACC 风险因素 | 显示过去一周处理的网络通信平均风险因子（1 到 5）。值越高表示风险越大。 |
| 高可用性 | 如果启用了高可用性 (HA)，则会指示本地和对等防火墙的 HA 状态 — 绿色（主动）、黄色（被动）或黑色（其他）。有关 HA 的详细信息，请参阅高可用性。 |
| 锁 | 显示管理员锁定的配置。 |



© 2019 Palo Alto Networks, Inc.

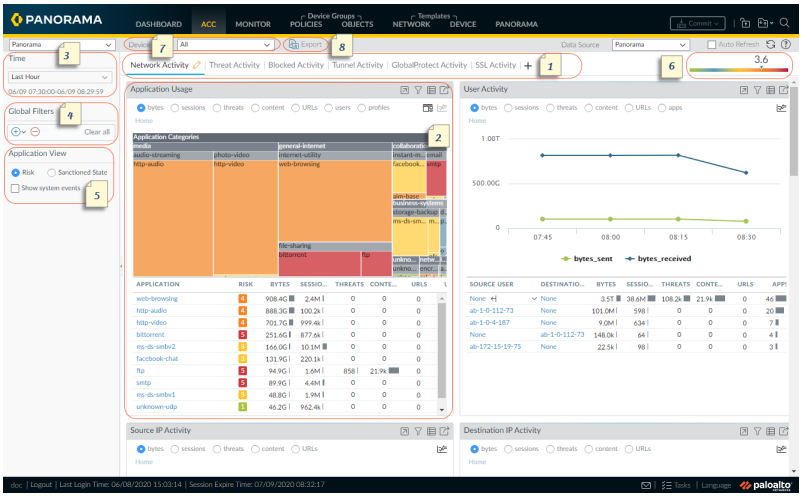
# 使用应用程序命令中心

应用程序命令中心 (ACC) 提供您的网络上的应用程序、用户、URL、威胁和内容的交互式图形概览。ACC 使用防火墙日志，让您查看流量模式，并且获取有关威胁的实用信息。ACC 布局包括网络活动、威胁活动、已阻止活动的选项卡视图，而且每个视图包括相关的小部件，以实现网络流量的更好可视化。通过图形表示，您能够与数据交互，查看网络上的事件之间的关系，以便发现异常情况，寻找增强网络安全规则的方法。对于网络的个性化视图而言，您还可以添加一个自定义选项卡，包括小部件，让您深入到对您而言最重要的信息。


- ACC—第一印象
- ACC 选项卡
- ACC 小部件（小部件说明）
- ACC 筛选器
- 与 ACC 交互
- 用例：ACC — 信息发现路径


## ACC—第一印象

快速概览 ACC。




| ACC—第一印象 | | |
|---|---|---|
| 1 | **Tabs**（选项卡） | ACC 包括三个预定义的选项卡，可在其中查看网络流量、威胁活动和阻止的活动。有关每个选项卡的信息，请参阅 ACC 选项卡。 |
| 2 | 小部件 | 每个选项卡都包括一组默认的小部件，这些小部件最能代表与选项卡相关联的事件和趋势。小部件可让您使用以下筛选器调查数据：<br>• 字节（传入和传出）<br>• 会话<br>• 内容（文件和数据）<br>• URL 类别<br>• 威胁（以及计数） |



© 2019 Palo Alto Networks, Inc.

| ACC—第一印象 | | |
|---|---|---|
| | | 有关每个小部件的信息，请参阅 ACC 小部件。 |
| 3 | 时间 | 每个小部件中的图表或图形提供摘要和历史视图。可以选择一个自定义范围，或者从最近 15 分钟最多至最近 90 天内（或最近 30 个日历日内）选择一个预定义的时间段。选定时间段应用于 ACC 中的所有选项卡。<br>默认情况下，用于展示数据的时间段为 **Last Hour**（最后一小时），间隔 15 分钟更新一次。会在屏幕上显示日期和时间间隔，例如在 11:40，时间范围为 01/12 10:30:00-01/12 11:29:59。 |
| 4 | 全局过滤器 | 全局筛选器可让您设置适用于所有小部件和选项卡的筛选器。图表/图形会在展示数据之前应用选定的筛选器。有关使用筛选器的信息，请参阅 ACC 筛选器。 |
| 5 | Application View（应用程序视图） | 应用程序视图可让您通过正在网络上使用的批准或未批准应用程序，或通过正在网络上使用的应用程序的风险级别对 ACC 视图进行筛选。绿色表示已批准的应用程序，蓝色表示未批准的应用程序，黄色表示部分批准的应用程序。部分批准的应用程序是指那些批准状态混淆的应用程序，也就是说，标记为“已批准”的应用程序不一致。例如，为多个虚拟系统启用的防火墙上或 Panorama 设备组中一个或多个防火墙之间的一个或多个虚拟系统上的应用程序可能会通过批准。 |
| 6 | **Risk factir**（风险系数） | 风险系数（最低为 1，最高为 5）指示网络上使用的应用程序的相对风险。风险系数使用各种因素来评估相关风险级别，例如应用程序是否能够共享文件、是否容易误用、是否试图避开防火墙，它还考虑到通过阻止的威胁的数量看到的威胁活动和恶意软件，以及指向恶意主机和域的受影响的主机或流量。 |
| 7 | 源 | 用于 ACC 显示的数据。选项可能会有所不同，具体取决于防火墙和 Panorama。<br>在防火墙中，如果为多个虚拟系统启用，则可以使用 **Virtual System**（虚拟系统）下拉列表更改 ACC 显示，以包括所有虚拟系统或者仅包括选定虚拟系统中的数据。<br>在 Panorama 上，您可以选择 **Device Group**（设备组）下拉菜单来更改 ACC 显示，以包括所有设备组或者仅包括选定设备组的数据。<br>此外，在 Panorama 上，您可将 **Data Source**（数据源）更改为 **Panorama** 数据或 **Remote Device Data**（远程设备数据）。**Remote Device Data**（远程设备数据）仅用于所有托管防火墙都在 PAN-OS 7.0.0 或更高版本上的情况。当您筛选特定设备组的显示时，**Panorama** 数据用作数据源 。 |
| 8 | 导出 | 可以将当前选定选项卡中显示的小部件导出为 PDF。PDF 文件可下载和保存至您计算机上与 Web 浏览器相关联的文件夹。 |


© 2019 Palo Alto Networks, Inc.

# ACC 选项卡

ACC 包括下列预定义选项卡，用于查看网络活动、威胁活动和阻止的活动。

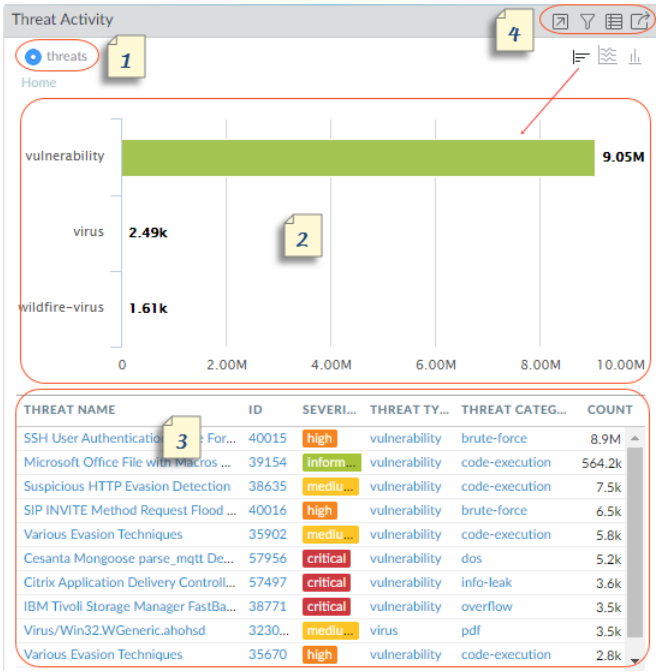
| 选项卡 | 说明 |
| --- | --- |
| **Network Activity**（网络活动） | 简要显示网络上的流量和用户活动，包括：<br>• 使用最多的应用程序<br>• 生成流量最多的用户（通过深入分析用户访问的字节、内容、威胁或 URL）<br>• 最常用的安全规则（针对发生的流量匹配）<br>此外，还可以按照源或目标区域、地区、IP 地址、入口和出口接口，以及主机信息（例如网络中最常用的设备的操作系统）来查看网络活动。 |
| **Threat Activity**（威胁活动） | 简要显示网络上的威胁，侧重于排名靠前的威胁：安全漏洞、间谍软件、病毒、访问恶意域或 URL 的主机、按文件类型和应用程序提交的顶级 WildFire，以及使用非标准端口的应用程序。此选项卡中的“受影响的主机”小部件（仅有一部分平台支持）使用更好的可视化技术对检测进行补充；它使用来自关联事件选项卡（**Automated Correlation Engine**（自动关联引擎）> **Correlated Events**（关联事件））信息，按照源用户或 IP 地址，提供网络中的受影响主机的数据的聚合视图，按严重性排序。 |
| **Blocked Activity**（阻止的活动） | 专门显示被阻止进入网络的流量。使用此选项卡中的小部件，您可以查看被以下因素拒绝的活动：应用程序名称、用户名、威胁名称、被阻止内容（被文件传送阻止配置文件阻止的文件和数据）。它还列出了用于匹配以阻止威胁、内容和 URL 的热门安全规则。 |
| **Tunnel Activity**（隧道活动） | 根据隧道检测策略显示防火墙检测的隧道流量活动。信息包括基于隧道 ID、监控标签、用户和隧道协议（如通用路由封装 (GRE)、用户数据 (GTP-U) 的通用分组无线服务 (GPRS) 隧道协议和非加密 IPSec）的隧道使用情况。 |
| **GlobalProtect Activity**（**GlobalProtect** 活动） | 显示 GlobalProtect 部署中的用户活动概述。信息包括用户数量、用户连接次数、用户连接的网关、连接失败数和失败原因、使用的身份验证方法和 GlobalProtect 应用程序版本的摘要以及被隔离的端点数量。<br>此外，此选项卡显示已被隔离的设备的图表视图摘要。使用图表顶部的切换键，根据导致 GlobalProtect 隔离设备的操作、GlobalProtect 隔离设备的原因、以及隔离设备的位置查看隔离设备。 |
| **SSL Activity**（**SSL** 活动） | 显示防火墙上的 TLS/SSL 解密活动概述。信息包括网络中成功和不成功的解密活动，协议、证书和版本等导致解密失败的问题，TLS 版本，密钥交换算法，以及解密和未解密流量的数量和类型。<br>使用 ACC 信息评估网络中解密运行的方式，然后使用解密日志深入了解详细信息。 |

您还可以与 ACC 交互创建包含自定义布局和小部件的自定义选项卡，满足您的网络监控需求，还可以导出选项卡与另一位管理员分享。


© 2019 Palo Alto Networks, Inc.

# ACC 小部件

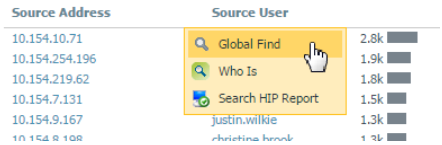
每个选项卡上的小部件都是交互式的。您可以设置 ACC 筛选器，并深入分析每个表格或图形的详细信息，或者自定义包括在选项卡中的小部件，以重点显示您需要的信息。有关每个小部件显示内容的详细信息，请参阅小部件说明。




| 小部件 | | |
|---|---|---|
| 1 | 查看 | 可以按照字节、会话、威胁、计数、内容、URL、恶意、良性、文件、应用程序、数据、配置文件、对象或用户来对数据进行排序。各个小部件的可用选项有所不同。 |
| 2 | 图形 | 图形显示选项有树状图、线形图、水平条形图、堆栈区域图形、堆栈条形图以及地图。各个小部件的可用选项有所不同，每个图形类型也会提供不同的交互体验。例如，使用非标准端口的应用程序的小部件可让您选择树状图和线形图。<br>要深入分析显示视图，可单击图形。单击的区域会成为筛选器，可让您放大所选的内容，并且查看关于该内容的更详细的信息。 |
| 3 | 表 | 在图形下方的表格中，会提供用于展示图形的数据的详细视图。您可通过多种方式与表格进行交互：<br>• 在表格中单击某种属性，并设置针对该属性的本地筛选器。图形将会更新，使用本地筛选器对表格进行排序。显示在图形和表格中的信息始终保持同步。<br>• 将鼠标悬停在表格中的属性上，使用下拉菜单中的可用选项。 |



© 2019 Palo Alto Networks, Inc.

| 小部件 | | |
|---|---|---|
| | |  |
|  | 操作 | 最大化视图 — 可让您放大小部件，从而在包含更多可视信息的更大屏幕空间中查看表格。<br>设置本地筛选器— 可让您添加 ACC 筛选器以调整小部件中显示的内容。使用这些筛选器自定义小部件；这些自定义项在多次登录时保留。<br>跳到日志— 可让您直接导航到日志（**Monitor**（监控）> **Logs**（日志）> **<log-type>**（<日志类型>）选项卡）。在展示图形的时间段内对日志进行过滤。<br>如果已设置本地筛选器和全局筛选器，则日志查询会合并时间段和筛选器，并且仅显示与合并的筛选器集合相匹配的日志。<br>**Export**（导出）— 可让您将图形导出为 PDF。PDF 文件将会下载并保存到您的计算机上。它将保存在与您的 Web 浏览器关联的 Downloads 文件夹中。 |

# 小部件说明

ACC 上的每个选项卡都包括一组不同的小部件。

| 小部件 | 说明 |
|---|---|
| **Network Activity**（网络活动）— 简要显示网络上的流量和用户活动。 | |
| **Application Usage**（应用程序使用） | 该表格显示您网络上使用最多的十大应用程序，网络上的所有其他应用程序都汇总显示为其他。图形按应用程序类别、子类别、应用程序来显示所有应用程序。使用此小部件可扫描正在网络上使用的应用程序，它让您知道使用带宽、会话计数、文件传输最多的主要应用程序，以及触发威胁最多和访问 URL 的应用程序。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：树状图、区域图、柱状图、折线图（图表可能变化，具体取决于按所选属性的排序） |
| **User Activity**（用户活动） | 显示网络上的十大活跃用户，他们产生的流量最多，为获取内容消耗的网络资源也最多。使用此小部件可以监控使用量最大的用户，按字节、会话、威胁、内容（文件和模式）、访问的 URL 进行排序。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：区域图、柱状图、折线图（图表可能变化，具体取决于按所选属性的排序） |


© 2019 Palo Alto Networks, Inc.

| 小部件 | 说明 |
| --- | --- |
| **Source IP Activity**（源 IP 活动） | 显示在您网络上启动活动最多的十大设备 IP 地址或主机名。其他所有设备都汇总显示为其他。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：区域图、柱状图、折线图（图表可能变化，具体取决于按所选属性的排序） |
| **Destination IP Activity**（目标 IP 活动） | 显示网络上用户访问最多的十大目标的 IP 地址或主机名。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：区域图、柱状图、折线图（图表可能变化，具体取决于按所选属性的排序） |
| **Source Regions**（源区域） | 显示在您网络上启动活动最多的全球十大地区（内置或自定义的区域）。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：地图、条形图 |
| **Destination Regions**（目标区域） | 显示在您网络上启动活动最多的全球十大目标地区（内置或自定义的区域）。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：地图、条形图 |
| **GlobalProtect Host Information**（GlobalProtect 主机信息） | 显示关于运行 GlobalProtect 代理的主机的状态的信息；主机系统是 GlobalProtect 端点。这些信息来自 HIP 匹配日志中的条目，这些日志是在 GlobalProtect 应用提交的数据与您在防火墙上定义的 HIP 对象或 HIP 配置文件相匹配时生成的。如果您没有 HIP 匹配日志，则此小部件为空。要了解如何创建 HIP 对象和 HIP 配置文件，并将其用作策略匹配条件，请参阅配置基于 HIP 的策略实施。<br>排序属性：配置文件、对象、操作系统<br>可用图表：条形图 |
| 规则使用情况 | 显示允许网络上的流量最多的十大规则。使用此小部件可查看最常用的规则、监控使用模式、评估规则是否能够有效地保护网络安全。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：折线图 |
| **Ingress Interfaces**（入口接口） | 显示流量进入网络使用最多的防火墙接口。<br>排序属性：字节、发送的字节、接收的字节<br>可用图表：折线图 |
| **Egress Interfaces**（出口接口） | 显示流量流出网络使用最多的防火墙接口。<br>排序属性：字节、发送的字节、接收的字节<br>可用图表：折线图 |
| **Source Zones**（源区域） | 显示流量进入网络使用最多的区域。<br>排序属性：字节、会话、威胁、内容、URL |


© 2019 Palo Alto Networks, Inc.

| 小部件 | 说明 |
| --- | --- |
| | 可用图表：折线图 |
| **Destination Zones**（目标区域） | 显示流量流出网络使用最多的区域。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：折线图 |
| **Threat Activity**（威胁活动）— 简要显示网络上的威胁。 | |
| **Compromised Hosts**（受影响的主机） | 显示网络上最可能受影响的主机。此小部件总结来自关联日志的事件。对于每个源用户/IP 地址，这些信息包括触发匹配的关联对象以及匹配数，这个匹配数来自从关联事件日志中核对的匹配证据汇总。有关详细信息，请参阅使用自动关联引擎。<br>在 PA-5200 系列、PA-7000 系列和 Panorama 上可用。<br>排序属性：严重性（默认情况下） |
| **Hosts Visiting Malicious URLs**（访问恶意 **URL** 的主机） | 显示网络上的主机（IP 地址/主机名）访问恶意 URL 的频率。根据 PAN-DB 中的分类，已知这些 URL 为恶意软件。<br>排序属性：计数<br>可用图表：折线图 |
| **Hosts Resolving Malicious Domains**（解析恶意域的主机） | 显示匹配 DNS 签名的顶级主机；网络上试图解析恶意 URL 的主机名或域的主机。这些信息通过对网络上的 DNS 活动进行分析来收集。该小部件利用了被动 DNS 监控、在网络上生成的 DNS 流量、在沙盒中观察到的活动（如果您在防火墙上配置了 DNS Sinkhole），以及提供给 Palo Alto Networks 客户的有关恶意 DNS 源的 DNS 报告。<br>排序属性：计数<br>可用图表：折线图 |
| **Threat Activity**（威胁活动） | 显示在网络上发现的威胁。这些信息基于抗病毒、防间谍软件、漏洞防护配置文件中的签名不匹配，以及 WildFire 报告的病毒。<br>排序属性：威胁<br>可用图表：条形图、区域图、柱状图 |
| 不同应用程序的 **WildFire** 活动 | 显示生成 WildFire 提交最多的应用程序。此小部件使用来自 WildFire 提交日志的恶意和良性裁决。<br>排序属性：恶意，良性<br>可用图表：条形图、折线图 |
| **WildFire Activity by File Type**（不同文件类型的 **WildFire** 活动） | 显示不同文件类型的威胁载体。此小部件显示生成 WildFire 提交最多的文件类型，并使用来自 WildFire 提交日志的恶意和良性裁决。如果此数据不可用，则小部件为空。<br>排序属性：恶意，良性<br>可用图表：条形图、折线图 |
| 使用非标准端口的应用程序 | 显示通过非标准端口进入网络的应用程序。如果您迁移了防火墙规则，不再使用基于端口的防火墙，请使用这些信息来创建策略规则，仅允许在应用程序中在默认端 |


© 2019 Palo Alto Networks, Inc.

| 小部件 | 说明 |
| --- | --- |
| | 口上传输流量。需要时，允许例外情形，在非标准端口上传输流利，或者创建定制应用程序。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：树状图、折线图 |
| **Rules Allowing Applications On Non Standard Ports**（允许应用程序使用非标准端口的规则） | 显示允许应用程序使用非标准端口的安全策略规则。图形显示所有规则，而表格则显示使用最多的十大规则，并将来自其他规则的数据汇总为其他。<br>此信息让您能够评估应用程序是否跳过端口或潜入网络，从而帮助您识别网络安全漏洞。例如，您可以验证一条允许应用程序使用除默认端口之外的任何端口传输流量的规则。举个例子，您有一条规则允许 DNS 流量通过 *application-default* 端口传输（端口 53 是 DNS 标准端口）。此小部件将显示允许 DNS 流量通过除端口 53 之外的任何端口进入网络的所有规则。<br>排序属性：字节、会话、威胁、内容、URL<br>可用图表：树状图、折线图 |
| **Blocked Activity**（阻止的活动）— 专门显示被阻止进入网络的流量 | |
| **Blocked Application Activity**（阻止的应用程序活动） | 显示被拒绝进入网络的应用程序，让您能够查看您禁止进入网络的威胁、内容和 URL。<br>排序属性：威胁、内容、URL<br>可用图表：树状图、区域图、柱状图 |
| **Blocked User Activity**（阻止的用户活动） | 显示按照附加到安全策略的抗病毒、防间谍软件、文件阻止或 URL 筛选配置文件进行的匹配阻止的用户请求。<br>排序属性：威胁、内容、URL<br>可用图表：条形图、区域图、柱状图 |
| **Blocked Threats**（阻止的威胁） | 显示网络上成功拒绝的威胁。这些威胁是按照抗病毒签名、漏洞签名和 DNS 签名匹配的，这些签名可通过防火墙上的动态内容更新获取。<br>排序属性：威胁<br>可用图表：条形图、区域图、柱状图 |
| **Blocked Content**（阻止的内容） | 显示被阻止进入网络的文件和数据。内容被阻止，原因是根据在文件阻止安全配置文件或数据筛选安全配置文件中定义的标准，安全策略拒绝了访问。<br>排序属性：文件、数据<br>可用图表：条形图、区域图、柱状图 |
| **Security Policies Blocking Activity**（安全策略阻止活动） | 显示阻止或限制流量进入网络的安全策略规则。由于此小部件显示被拒绝进入网络的威胁、内容和 URL，因此您可以使用它评估策略规则的有效性。此小部件不显示由于您在策略中定义的拒绝规则而被阻止的流量。<br>排序属性：威胁、内容、URL<br>可用图表：条形图、区域图、柱状图 |
| **GlobalProtect Activity**（**GlobalProtect** 活动）— 显示 GlobalProtect 部署中的用户活动信息。 | |



© 2019 Palo Alto Networks, Inc.

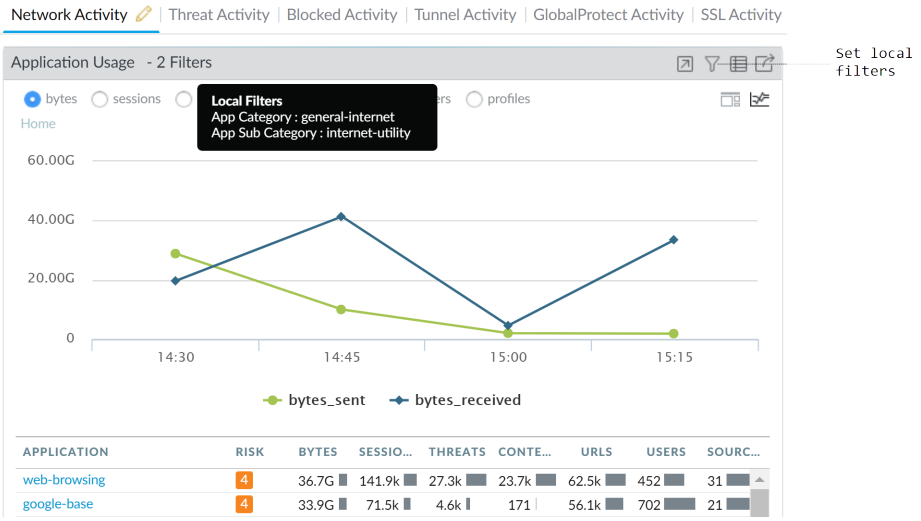
| 小部件 | 说明 |
| --- | --- |
| **Successful GlobalProtect Connection Activity**（**GlobalProtect** 连接活动成功） | 显示选定时段内 GlobalProtect 连接活动的图表视图。通过图表顶部的切换按钮，可按用户、门户和网关以及位置在连接统计数据之间切换。<br>排序属性：用户、门户/网关、位置<br>可用图表：条形图、折线图 |
| **Unsuccessful GlobalProtect Connection Activity**（**GlobalProtect** 连接活动失败） | 显示选定时段内 GlobalProtect 连接活动失败的图表视图。通过图表顶部的切换按钮，可按用户、门户和网关以及位置在连接统计数据之间切换。为了帮助您识别连接问题，并进行故障排除，您还可以查看原因图表或原因图。对于此图表，ACC 会指示错误、源用户、公共 IP 地址等信息，帮助您识别并快速解决问题。<br>排序属性：用户、门户/网关、原因、位置<br>可用图表：条形图、折线图 |
| **GlobalProtect Deployment Activity**（**GlobalProtect** 部署活动） | 显示部署的图表视图摘要。通过图表顶部的切换按钮，可按身份验证方法、GlobalProtect 应用程序版本以及操作系统版本查看用户分布。<br>排序属性：身份验证方法、GlobalProtect 应用程序版本、OS<br>可用图表：条形图、折线图 |
| **GlobalProtect Quarantine Activity**（**GlobalProtect** 隔离活动） | 显示已被隔离的设备的图表视图摘要。使用图表顶部的切换键，根据导致 GlobalProtect 隔离设备的操作、GlobalProtect 隔离设备的原因、以及隔离设备的位置查看隔离设备。<br>排序属性：操作、原因、位置<br>可用图表：条形图、折线图 |
| **SSL Activity**（**SSL** 活动）— 显示网络中 SSL/TLS 活动的相关信息。 | |
| **Traffic Activity**（流量活动） | 按会话总数或字节总数显示 SSL/TLS 活动与非 SSL/TLS 活动。 |
| **SSL/TLS Activity**（**SSL/TLS** 活动） | 按 TLS 版本和应用程序或 SNI 显示成功的 TLS 连接。通过该小部件，您可以知晓允许较弱 TLS 协议版本会给您带来的风险。通过识别使用弱协议的应用程序和 SNI，您可以分别进行评估，并决定是否允许出于业务原因对其进行访问。如果开展业务不需要使用该应用程序，您可以阻止而不是允许相应流量。单击应用程序或 SNI 以深入了解并查看详细的信息。 |
| **Decryption Failure Reasons**（解密失败原因） | 按 SNI 显示解密失败的原因，例如证书或协议问题。使用这些信息可以检测出因解密策略或配置文件配置错误，或是流量使用弱协议或算法而导致的问题。单击失败原因以深入了解并隔离每个 SNI 的会话数，或是单击 SNI 以查看该 SNI 出现的失败。 |
| **Successful TLS Version Activity**（成功的 **TLS** 版本活动） | 按会话或字节数显示已解密和未解密的流量。未解密的流量可能是因为策略、策略配置错误或被列入解密排除列表而无法解密（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））。 |
| **Successful Key Exchange Activity**（成功的密钥交换活动） | 按应用程序或 SNI 显示每个算法成功的密钥交换活动。单击密钥交换算法以仅查看该算法的活动，或是单击应用程序或 SNI 以查看该应用程序或 SNI 的密钥交换活动。 |


© 2019 Palo Alto Networks, Inc.

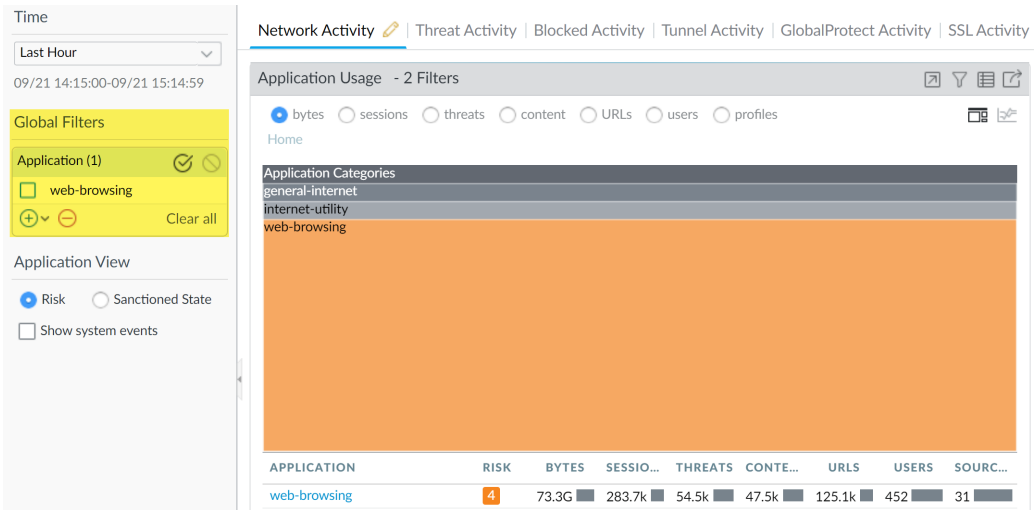
# ACC 筛选器

通过 ACC 小部件上的图形和表格，您可以使用筛选器来缩小显示的数据范围，以便能够隔离特定属性，更加详细地分析需要查看的信息。ACC 支持同时使用小部件和全局筛选器。

- 小部件筛选器 — 应用小部件筛选器，它是对于特定小部件而言属于本地的筛选器。小部件筛选器可让您与图形进行交互，并且自定义显示的内容，从而能够深入分析详细信息，以及访问要在特定小部件上监控的信息。要创建在重新启动之后仍然可以持续发挥作用的小部件筛选器，必须使用 **Set Local Filter**（设置本地筛选器）选项。




- 全局筛选器 — 在 ACC 中的所有选项卡上应用全局筛选器。全局筛选器可让您立即根据关注的详细信息来调整显示的内容，并且从当前显示中排除无关的信息。例如，要查看与特定用户和应用程序相关的所有事件，可以将用户名和应用程序应用为全局筛选器，从而通过 ACC 中的所有选项卡和小部件仅查看关于该用户和应用程序的信息。全局筛选器的效果不是永久性的。




您可以通过三种方式应用全局筛选器：

- 从表格设置全局筛选器 — 从任何小部件的表格中选择属性，然后将其应用为全局筛选器。
- 将小部件筛选器添加到全局筛选器 — 将鼠标悬停于属性上方，然后单击属性右侧的箭头图标。此选项可让您提升小部件中使用的本地筛选器，同时全局应用属性，以更新 ACC 上所有选项卡的显示内容。
- 定义全局筛选器 — 使用 ACC 上的 **Global Filters**（全局筛选器）窗格定义筛选器。

有关使用这些筛选器的详细信息，请参阅与 ACC 交互。



© 2019 Palo Alto Networks, Inc.

# 与 ACC 交互

要自定义和优化 ACC 显示，可以添加、删除、导出和导入选项卡，添加和删除小部件，设置本地和全局筛选器，以及与小部件进行交互。

- 添加选项卡。
  1. 选择 + 图标以及选项卡列表。
  2. 添加 **View Name**（视图名称）。此名称会用作选项卡的名称。最多可以添加 5 个选项卡。

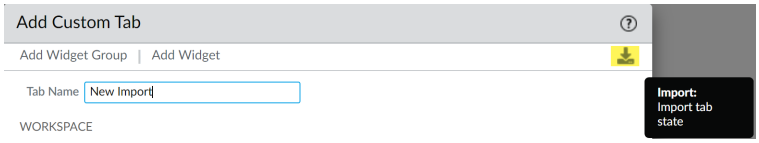
- 编辑选项卡。

  选择选项卡，然后单击选项卡名称旁边的铅笔图标以编辑选项卡。例如 Threat Activity 。

  通过编辑选项卡，您可以添加、删除或重置显示在选项卡中的小部件。还可以更改选项卡中的小部件布局。

  要将选项卡保存为默认选项卡，请选择 。

- 导出和导入选项卡。
  1. 选择选项卡，然后单击选项卡名称旁边的铅笔图标以编辑选项卡。
  2. 选择 图标，将当前选项卡以 .txt 文件格式导出。您可以与其他管理员共享此 .txt 文件。
  3. 要在另一个防火墙上将该选项卡作为新选项卡导入，请选择选项卡列表中的 + 图标，然后添加名称并单击导入图标，然后再浏览以选择 .txt 文件。




- 查看选项卡中包括哪些小部件。
  1. 选择选项卡，然后单击铅笔图标以编辑选项卡。
  2. 选择 **Add Widgets**（添加小部件）下拉列表，并确认已选中小部件的复选框。

- 添加小部件或小部件组。
  1. 添加新的选项卡，或者编辑预定义的选项卡。
  2. 选择 **Add Widgets**（添加小部件），然后选中要添加的小部件的复选框。最多可以添加 12 个小部件。
  3. （可选）如需创建双列布局，请选择 **Add Widget Group**（添加小部件组）。可以将小部件拖放到双列显示中。将小部件拖动到布局中时，会在放置小部件之处显示占位符。

     不能命名小部件组。

- 删除选项卡或小部件组/小部件。
  1. 要删除自定义选项卡，可选择选项卡并单击 X 图标。 Custom_threat_user_activity

     不能删除预定义的选项卡。

  2. 要删除小部件组/小部件，请在工作区部分中编辑选项卡，然后单击右侧的 [X] 图标。不能撤消删除。


© 2019 Palo Alto Networks, Inc.

- 重置选项卡中的默认小部件。

  在预定义的选项卡（例如 **Blocked Activity**（阻止的活动）选项卡）上，您可以删除一个或多个小部件。如果要重置布局以包括选项卡的默认小部件组，请编辑选项卡并单击 **Reset View**（重置视图）。

- 在区域图、柱状图或折线图中，放大显示详细信息。

  观察放大显示功能如何工作。

  单击并拖动图形中的某个区域可以放大显示。例如，当您放大显示一个拆线图时，它会触发重新查询，防火墙将会提取特定时间段的数据。它并非只是简单的放大。

- 使用表格下拉菜单可查找有关属性的更多信息。

  1. 将鼠标悬停在表格中的属性上可以看到下拉菜单。
  2. 单击下拉菜单可查看可用选项。

     - **Global Find**（全局查找）— 使用利用全局查找搜索防火墙或 Panorama 管理服务器 可查找对属性（用户名/IP 地址、对象名称、策略规则名称、威胁 ID、应用程序名称）的引用，包括待选配置的任何位置。
     - **Value**（值）— 显示威胁 ID、应用程序名称或地址对象的详细信息。
     - **Who Is** — 执行对 IP 地址的域名 (*WHOIS*) 查找。存储互联网资源的已注册用户或被分配者的查找查询数据库。
     - **Search HIP Report**（搜索 **HIP** 报名）— 使用用户名或 IP 地址，查找 HIP 匹配报告中的匹配。

- 设置小部件筛选器。

  还可以在图形下方的表格中单击某个属性，以将其应用为小部件筛选器。

  1. 选择小部件，然后单击 图标。
  2. 单击 图标添加要应用的筛选器。
  3. 单击应用。这些过滤器在重新启动之后仍然可以持续发挥作用。

     小部件名称旁边会指示激活的小部件筛选器。

- 对小部件筛选器进行求反

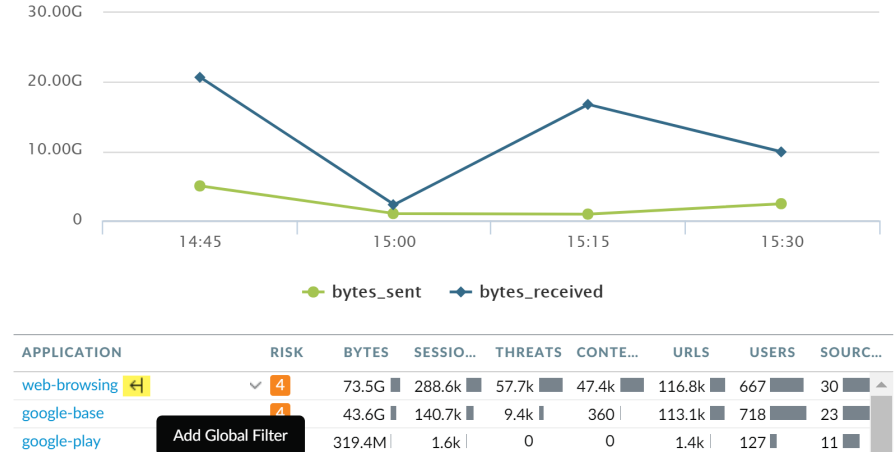
  1. 单击 图标可显示“设置本地筛选器”对话框。
  2. 添加筛选器，然后单击 求反图标。

- 从表格设置全局过滤器。

  将鼠标悬停于图表下方的表格中属性的上方，然后单击在此属性右侧的箭头图标。



© 2019 Palo Alto Networks, Inc.




- 使用全局筛选程序窗格设置全局筛选程序。

  观察正在运行的全局筛选器。

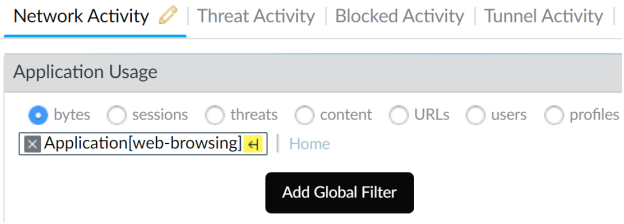
  1. 找到 ACC 左侧的 **Global Filters**（全局筛选器）窗格。

  2. 单击 图标可查看您可以应用的筛选器列表。

- 将本地筛选器升级为全局筛选器。

  1. 在小部件中的任意表格上，单击某个属性的链接。这样会将该属性设置为小部件筛选器。
  2. 要将筛选器升级为全局筛选器，请选择筛选器右侧的箭头。

- 删除过滤器。

  单击 图标可删除筛选器。

  - 对于全局筛选器：位于“全局筛选器”窗格中。
  - 对于小部件筛选器：单击 图标以显示“设置本地筛选器”对话框，然后选择筛选器并单击 图标。

- 清除所有筛选器。

  - 对于全局筛选器：单击“全局筛选器”下方的 **Clear All**（全部清除）按钮。
  - 对于小部件筛选器：选择小部件，然后单击 图标。然后单击“设置本地筛选器”对话框中的 **Clear All**（全部清除）按钮。

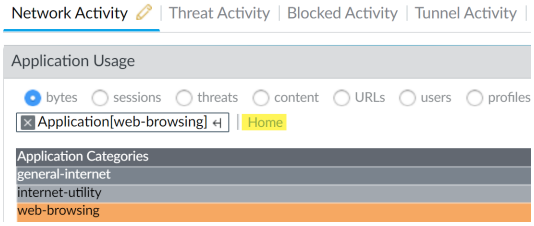
- 查看正在使用的筛选器。

  - 对于全局筛选器：应用的全局筛选器的数量显示在全局筛选器下方的左窗格中。


© 2019 Palo Alto Networks, Inc.

- 对于小部件筛选器：小部件名称旁边会显示在小部件中应用的小部件筛选器的数量。要查看筛选器，请单击 图标。

- 重置小部件上的显示。
  - 如果您要设置小部件筛选器或深入分析图形，请单击 **Home**（主页）链接以重置小部件上的显示。

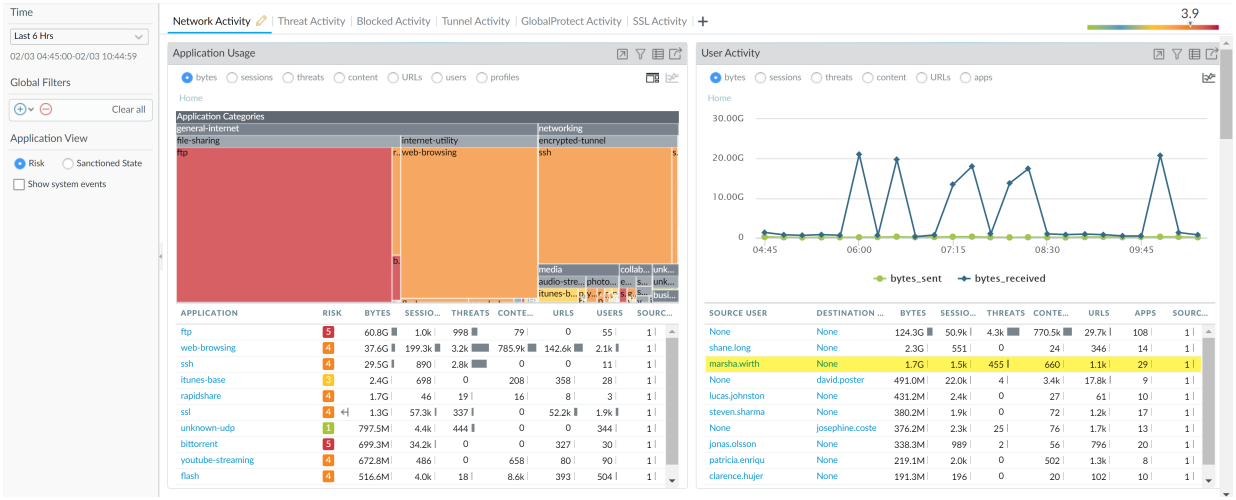



# 用例：ACC — 信息发现路径

ACC 提供丰富的信息，您可以通过这些信息分析网络流量。我们看一个使用 ACC 发现关注事件的示例。本示例说明了如何使用 ACC 确保合法用户对他们的操作负责、检测和跟踪未经授权的活动、检测和诊断受影响的主机以及网络上易受攻击的系统。

ACC 中的小部件和筛选器为您提供了基于您关注的事件来分析数据和筛选视图的功能。您可以跟踪引起您关注的事件、直接导出选项卡的 PDF 文件、访问原始日志、保存要跟踪的活动的个性化视图。利用这些功能，您可以监控活动并开发相应的策略和应对措施，从而增强针对恶意活动的网络防御。在本部分中，您将与不同选项卡上的 ACC 小部件交互与 ACC 交互，使用小部件筛选器进行深入分析，使用全局筛选器调整 ACC 视图，并导出 PDF 文件与事件响应或 IT 团队进行共享。

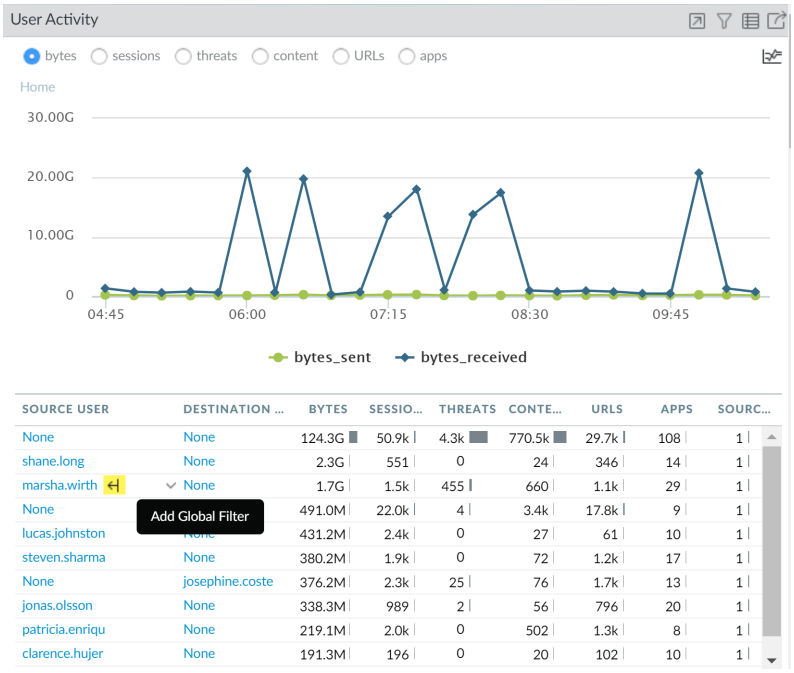
在 **ACC** > **Network Activity**（网络活动）选项卡中，您第一眼就能看到“应用程序使用情况”和“用户活动”小部件。“用户活动”小部件显示 Marsha Wirth 在前一小时内传输了 718 MB 数据。这个数据量超出了网络上其他所有用户的将近六倍。要查看过去几小时内的趋势，请将 **Time**（时间）长度延长为 **Last 6 Hrs**（最近 6 小时），现在可以看到 Marsha 的活动，她在 891 次会话中传输了 6.5 GB 数据，触发了 38 个威胁签名。




由于 Marsha 传输了大量数据，因此我们将她的用户名应用为全局筛选器 (ACC 筛选器)，并调整 ACC 中的所有视图，以重点显示 Marsha 的流量活动。



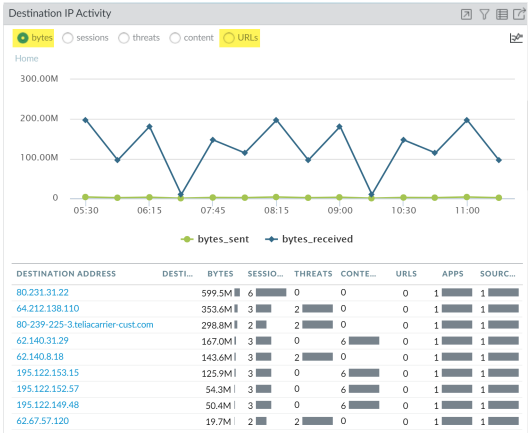
© 2019 Palo Alto Networks, Inc.




“应用程序使用情况”选项卡现在显示 Martha 使用最多的应用程序是 Rapidshare，这是瑞士的一个文件托管站点，属于文件共享 URL 类别。为了进行更深入调查，我们将 Rapidshare 添加为全局筛选器，并查看 Marsha 在 Rapidshare 的上下文中的活动。

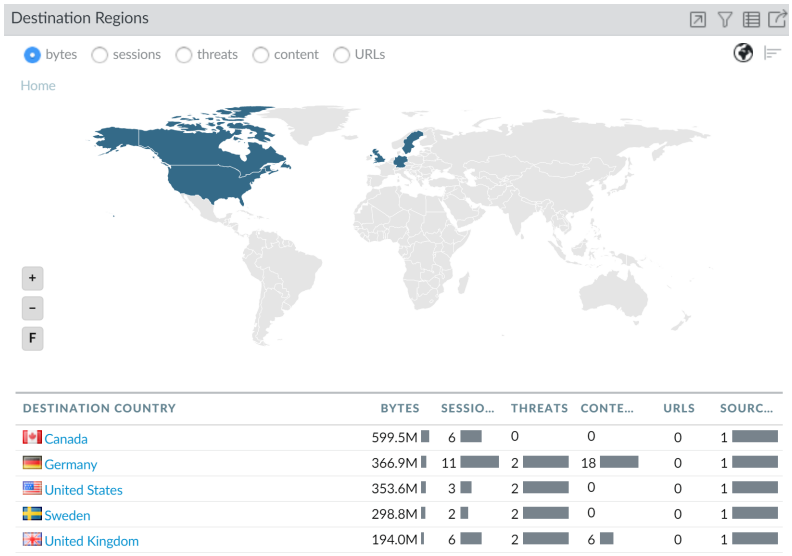
考虑是否批准在公司内部使用 *Rapidshare.*是否应该允许向该站点上传文件？是否需要 *QoS* 策略来限制带宽？

要查看 Marsha 曾与哪些 IP 地址进行通信，请选中 **Destination IP Activity**（目标 **IP** 活动）小部件，并按字节数和 URL 查看这些数据。



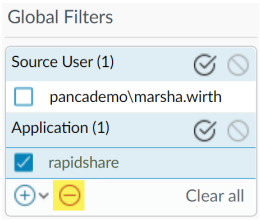

要找出 Marsha 曾与哪些国家/地区进行通信，请在 **Destination Regions**（目标区域）小部件中对 **sessions**（会话）进行排序。


© 2019 Palo Alto Networks, Inc.

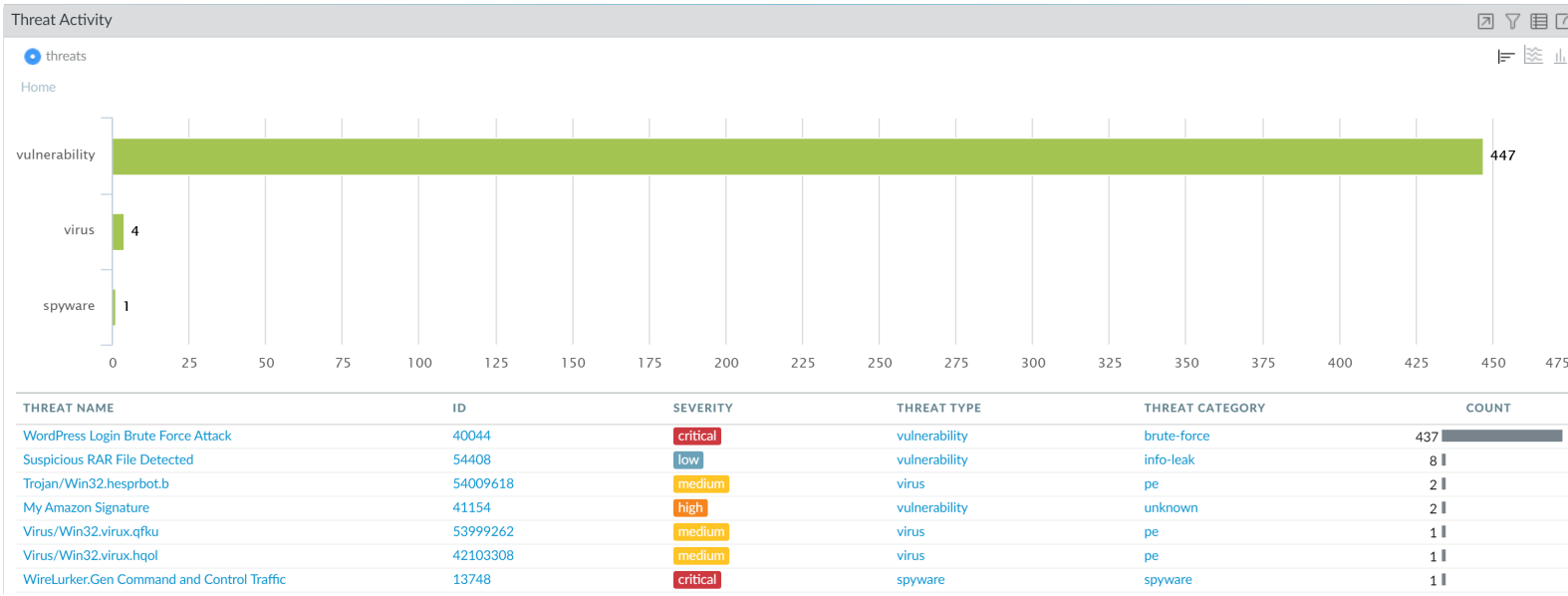



通过这些数据，您可以确认网络用户 Marsha 在韩国和欧盟建立了会话，在美国境内的会话中记录了 19 个威胁。

要从威胁视角查看 Marsha 的活动，请删除 Rapidshare 全局筛选器。




在 **Threat Activity**（威胁活动）选项卡上的 **Threat Activity**（威胁活动）小部件中查看威胁。此小部件显示她的活动触发了 26 个漏洞的匹配，这些漏洞分别属于溢出、DoS 和代码执行类别。其中几个漏洞属于高严重性的漏洞。



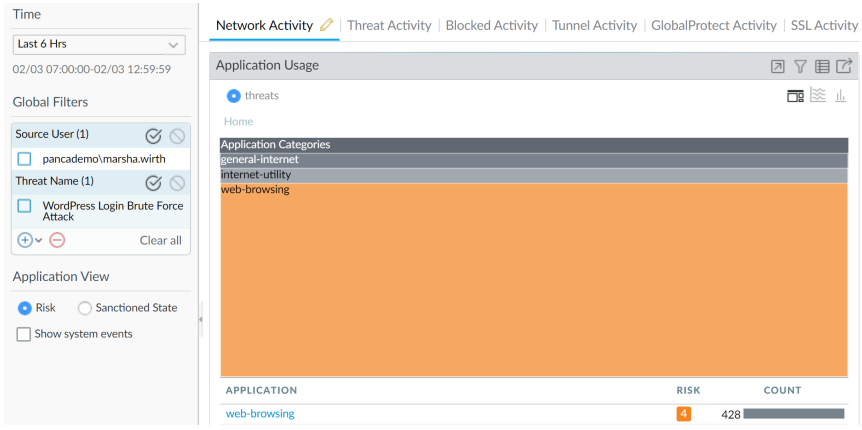

为了进一步深入分析每个漏洞，请单击图形，缩小调查的范围。每次单击都会在小部件上自动应用本地筛选器。



© 2019 Palo Alto Networks, Inc.




要按名称调查每种威胁，您可以创建全局筛选器，例如 **Microsoft Works File Converter Field Length Remote Code Execution Vulnerability**（**Microsoft** 工作文件转换器字段长度远程代码执行漏洞）。然后，在 **Network Activity**（网络活动）选项卡中查看 **User Activity widget**（用户活动小部件）。该选项卡进行自动筛选，以显示 Marsha 的威胁活动（请注意屏幕截图中的全局筛选器）。

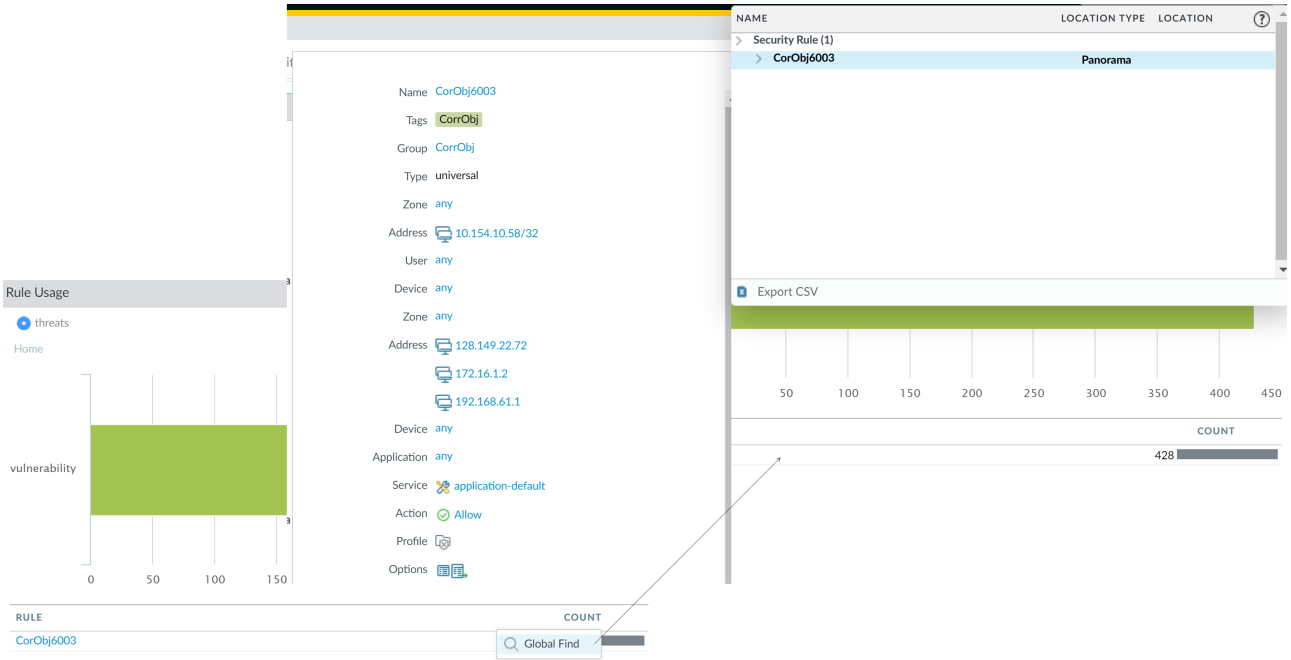



请注意，这个 Microsoft 代码执行漏洞是由 imap 应用程序通过电子邮件触发的。您现在可以确定 Martha 受到了 IE 漏洞和电子邮件附件漏洞的影响，她的计算机可能需要安装补丁。可以导航至 **Blocked Activity**（阻止的活动）选项卡中的 **Blocked Threats**（阻止的威胁）小部件，以确定其中多少漏洞被阻止。

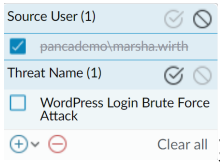
或者，也可以查看 **Network Activity**（网络活动）选项卡上的 **Rule Usage**（规则使用情况）小部件，以了解多少漏洞入侵了网络、哪些安全规则允许了这些流量，然后使用 **Global Find**（全局查找）功能，直接导航到安全规则。



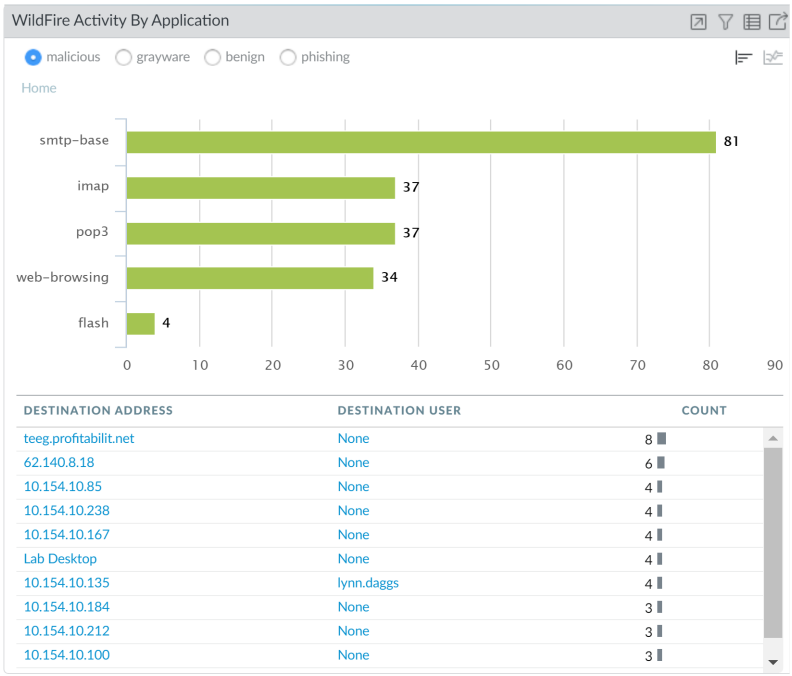
© 2019 Palo Alto Networks, Inc.




然后，深入分析为什么 imap 使用非标准端口 43206，而不是使用应用程序的默认端口 143。考虑修改安全策略规则，仅允许应用程序使用其默认端口，或者评估该端口是否应为网络上的例外情况。



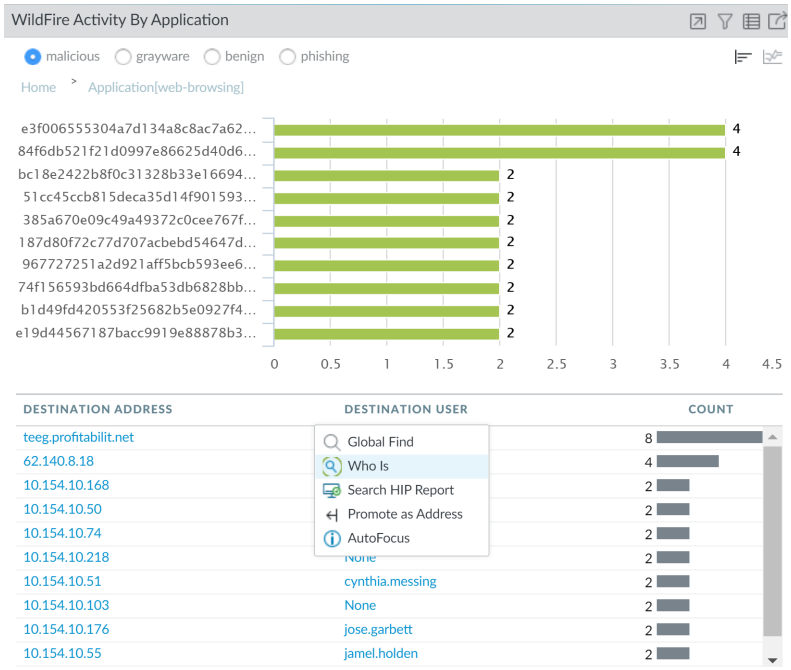

要查看在 imap 上是否已记录任何威胁，请在 **Threat Activity**（威胁活动）选项卡中的 **WildFire Activity by Application**（不同应用程序的 **WildFire** 活动）小部件中查看 Marsha 的活动。您可以确定 Marsha 没有恶意活动，但为了验证其他用户是否受到 imap 应用程序的影响，请将 Marsha 求反为全局筛选器，并查找通过 imap 触发威胁的其他用户。






© 2019 Palo Alto Networks, Inc.

在图形中单击 imap 的条形，深入分析与该应用程序相关的入站威胁。要查找 IP 地址注册到域名，请将鼠标悬停在攻击者 IP 地址上，并从下拉菜单中选择 **Who Is** 链接。




由于来自此 IP 地址的会话计数很高，请在与此 IP 地址相关的事件的 **Blocked Activity**（阻止的活动）选项卡中选中 **Blocked Content**（阻止的内容）和 **Blocked Threats**（阻止的威胁）小部件。通过 **Blocked Activity**（阻止的活动）选项卡，您可以验证当网络上的主机受到影响时，您的策略规则是否能够有效地阻止内容或威胁。

使用 ACC 的 **Export PDF**（导出 **PDF**）功能，您可以导出当前视图（创建数据的快照），并将其发送到事件响应团队。要直接从小部件查看威胁日志，您还可以单击 图标以跳转至日志；将会自动生成查询，仅在屏幕上显示相关的日志（例如在 **Monitor**（监控）> **Logs**（日志）> **Threat Logs**（威胁日志）中）。




您现在可以使用 ACC 查看网络数据/趋势，以了解哪些应用程序或用户生成的流量最多、多少应用程序导致了网络上的威胁。您能够识别哪些应用程序和用户生成了流量，确定应用程序是否通过默认端口传输数据，以及哪些策略规则允许流量进入网络，并确定威胁是否在网络上恣意扩散。还能够识别与网络上的主机进行通信的目标 IP 地址和地理位置。利用调查得出的结论，您可以创建面向目标的策略，为网络上的用户提供安全保护。


© 2019 Palo Alto Networks, Inc.

# 使用 App-Scope 报告

App Scope 报告可帮助深入了解，并提供分析工具，有助于指出有问题的行为，从而帮助您了解占用多数网络宽带的应用程序使用情况和用户活动、用户及应用程序中的变化，并识别网络威胁。

使用 App Scope 报告，可以快速查看是否有任何异常行为或意外情况。每个报告都提供一个进入网络的动态的、用户可自定义的窗口；将鼠标悬停于图表上的行或栏并单击该行或该栏，可打开特定应用程序、应用程序类别、用户或 ACC 显示的源的详细信息。**Monitor**（监控）> **App Scope**上的 App Scope 图表可让您：

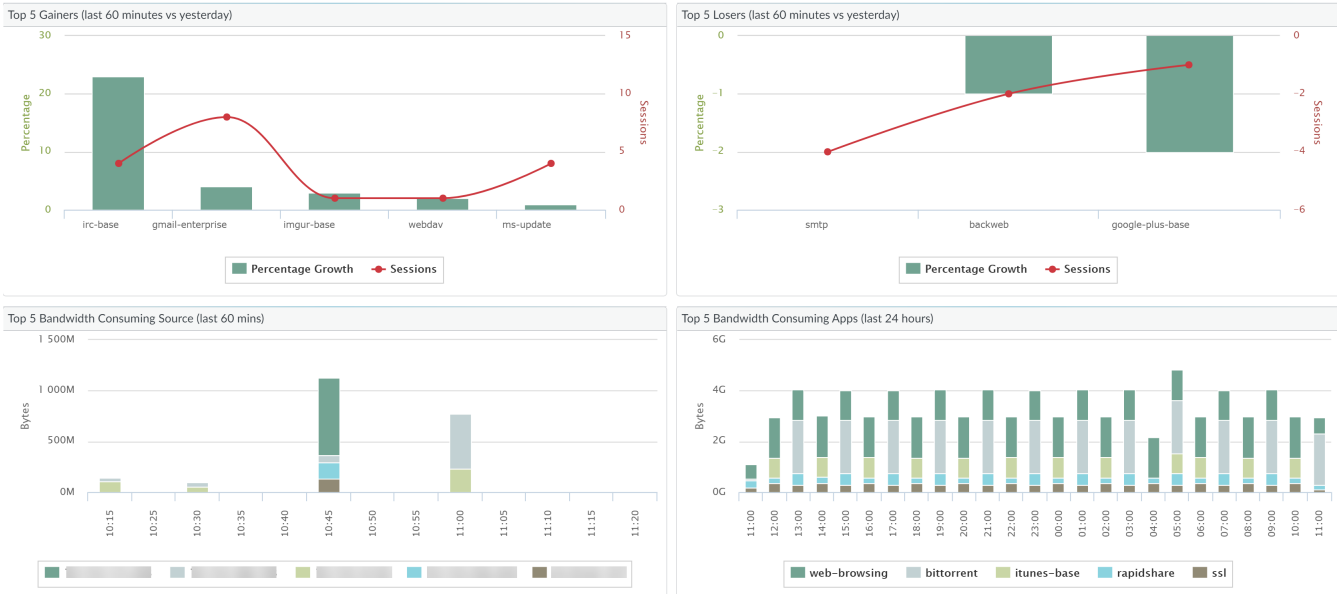
- 将图表中的属性切换为仅查看您希望查看的图表详细信息。包含或排除图表中的数据的功能可让您更改范围并更密切地查看详细信息。
- 单击条形图的属性，并深入分析 ACC 中的相关会话。单击任何条形图上的应用程序名称、应用程序类别、威胁名称、威胁类别、源 IP 地址或目标 IP 地址，以根据属性筛选，并查看 ACC 中的相关会话。
- 将图表或地图导出到 PDF 中，或导出为图像格式。出于便携性和方便离线查看的考虑，您可以将图表或地图导出为 PDF 或 PNG 图像。

可以使用以下 App Scope 报告：

- 摘要报告
- 异动监控报告
- 威胁监控报告
- 威胁地图报告
- 网络监控报告
- 通信地图报告

## 摘要报告

“App Scope 摘要”报告（**Monitor**（监控）> **App Scope** > **Summary**（监控））可显示前五个胜利者、失败者和带宽消耗应用程序、应用程序类别、用户和源的图表。

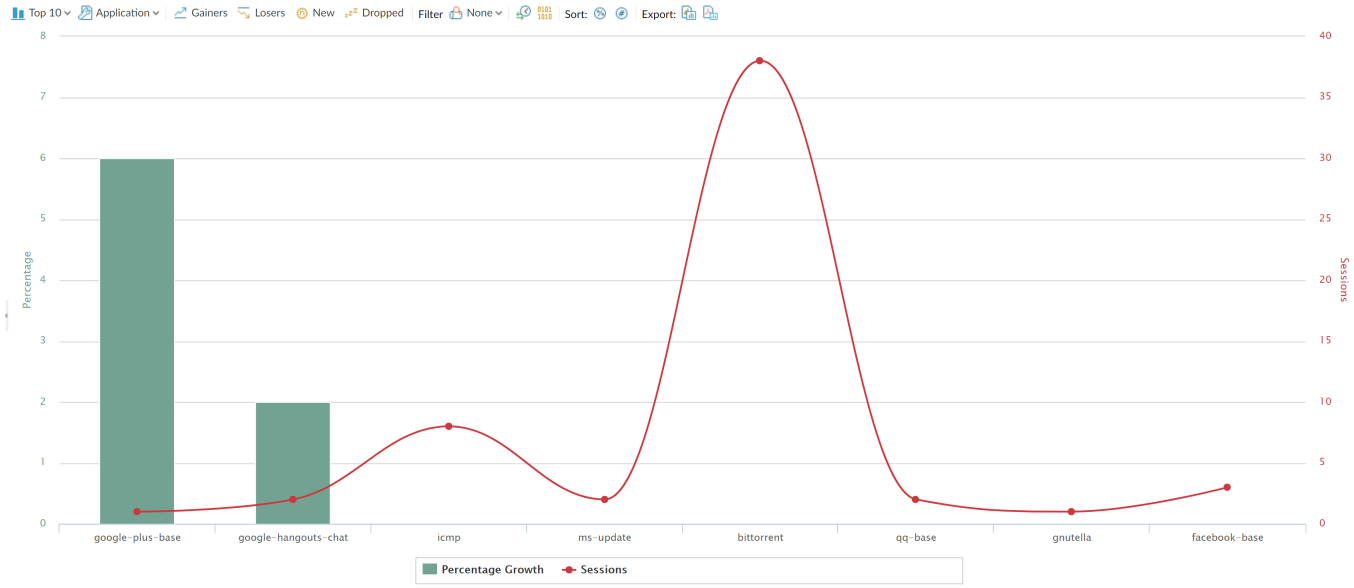





© 2019 Palo Alto Networks, Inc.

# 异动监控报告

“App Scope 异动监控”报告（**Monitor**（监控）> **App Scope** > **Change Monitor**（异动监控））显示指定时间段内的更改。例如，下表显示了在与过去 24 小时时段相比较的最后一小时内使用得最多的若干应用程序。排在前面的应用程序由会话数决定，并按百分比排序。




异动监控报告包含以下按钮和选项。

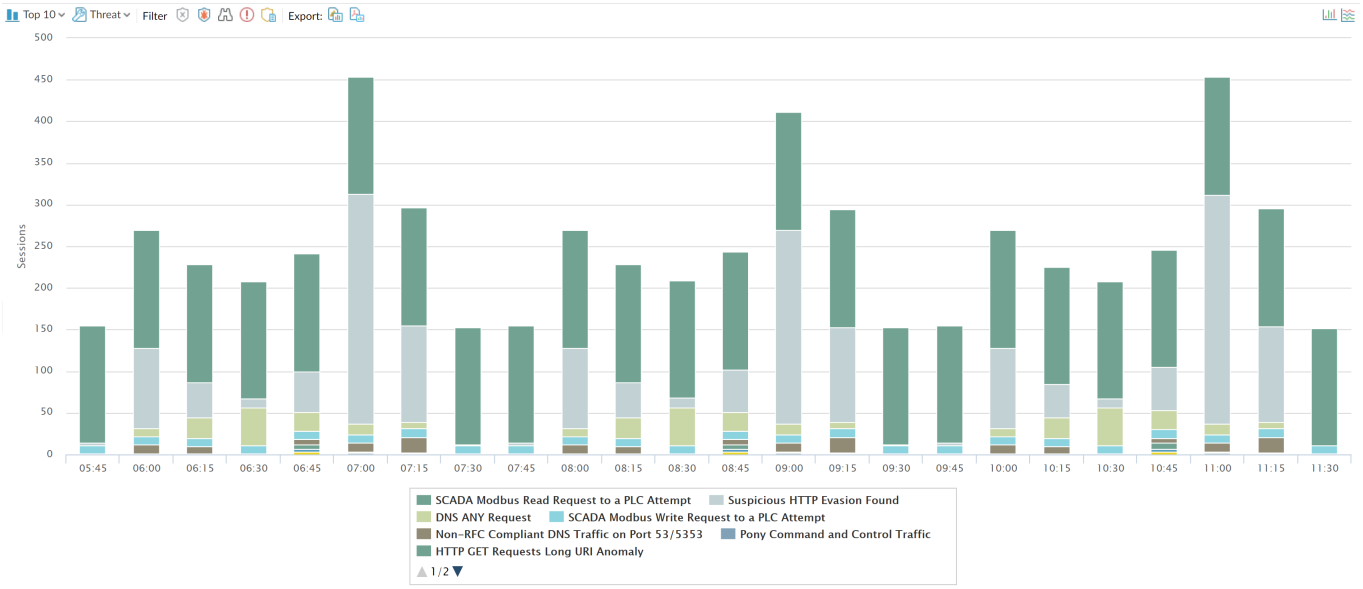
| 按钮 | 说明 |
|---|---|
| **Top 10** | 确定具有图表所包括的最高测量结果的记录数。 |
| 应用程序 | 确定报告的项目的类型：应用程序、应用程序类别、源或目标。 |
| **Gainers**（获得者） | 显示测量期间已增加的项目的测量结果。 |
| **Losers**（失败者） | 显示测量期间已减少的项目的测量结果。 |
| **New**（新增项） | 显示测量期间添加的项目的测量结果。 |
| **Dropped**（已丢弃） | 显示测量期间中断的项目的测量结果。 |
| **Filter**（筛选器） | 应用筛选器以仅显示所选项目。无显示所有条目。 |
|  | 确定是显示会话信息还是显示字节信息。 |
| **Sort**（排序） | 确定是按百分比还是按原始增长量对条目进行排序。 |
| 导出 | 导出图表作为 .png 图像或 PDF。 |
| 比较 | 指定执行更改测量的时间段。 |



© 2019 Palo Alto Networks, Inc.

# 威胁监控报告

App Scope 威胁监控报告（**Monitor**（监控）> **App Scope** > **Threat Monitor**（威胁监控））显示选定时间段内排在前面的威胁计数。例如，下图显示了过去 6 小时内排在前面的 10 种威胁类型。




每个威胁类型均用颜色进行标记，如图表下面的图例所示。威胁监控报告包含以下按钮和选项。

| 按钮 | 说明 |
|---|---|
| **Top 10** | 确定具有图表所包括的最高测量结果的记录数。 |
| 威胁 | 确定测量的项目的类型：威胁、威胁类别、源或目标。 |
| **Filter**（筛选器） | 应用筛选器以仅显示所选类型的项目。 |
|  | 确定是通过堆积柱形图还是通过堆积面积图来呈现信息。 |
| 导出 | 导出图表作为 .png 图像或 PDF。 |
|  | 指定执行测量的时间段。 |

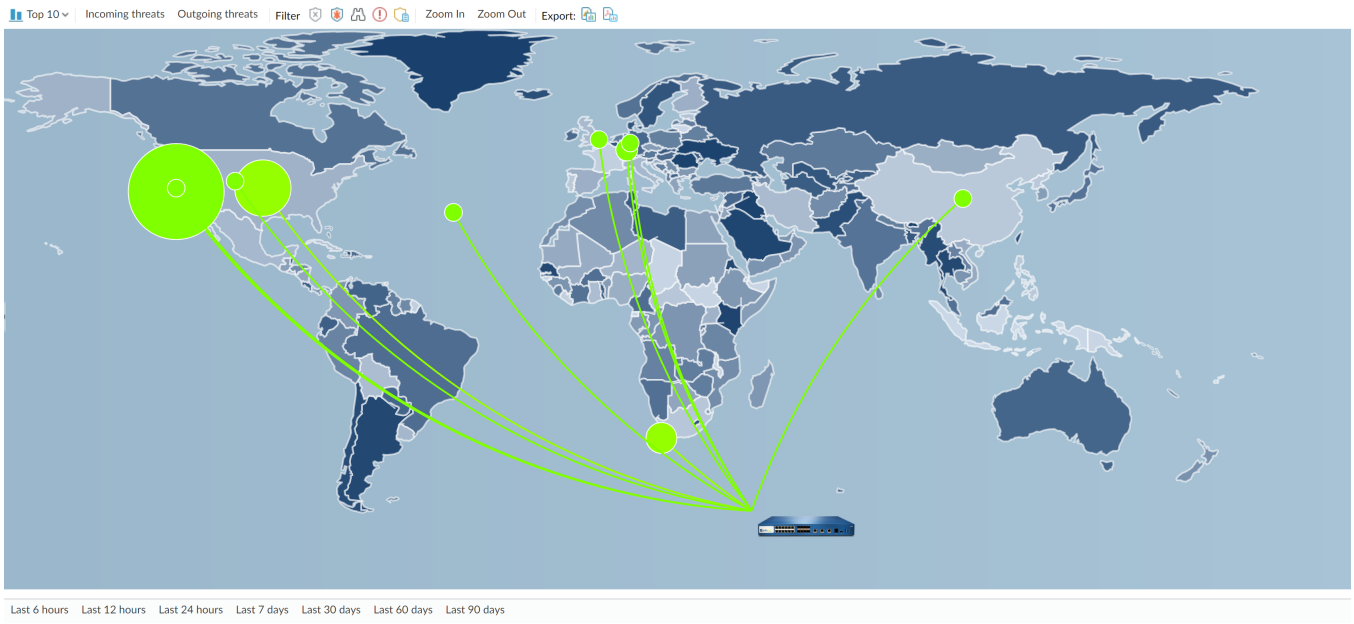
# 威胁地图报告

App Scope 威胁地图报告（**Monitor**（监控）> **App Scope** > **Threat Map**（威胁地图））显示威胁的地理视图，包括严重性。每个威胁类型均用颜色进行标记，如图表下面的图例所示。

防火墙使用地理定位创建威胁地图。如果您尚未指定防火墙上的地理定位坐标，则防火墙位于威胁地图屏幕的下方（常规设置部分中的 **Device**（设备）> **Setup**（设置）> **Management**（管理））。



© 2019 Palo Alto Networks, Inc.



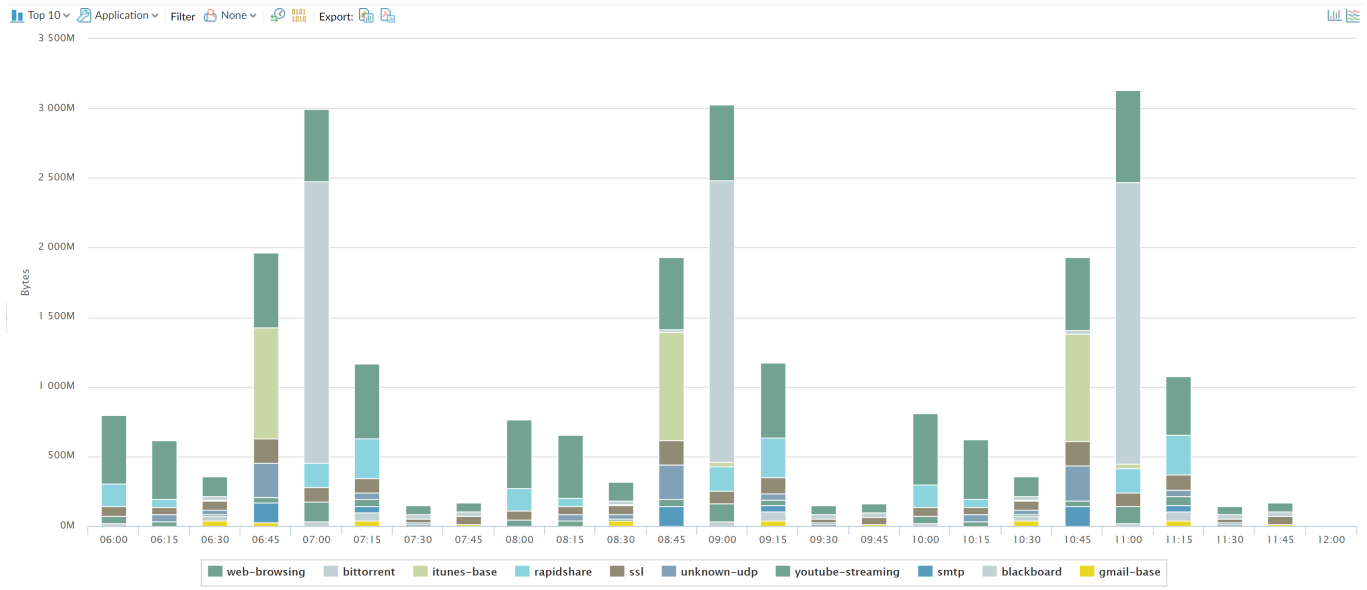

威胁地图报告包含以下按钮和选项。

| 按钮 | 说明 |
| --- | --- |
| **Top 10** | 确定具有图表所包括的最高测量结果的记录数。 |
| 传入威胁 | 显示传入威胁。 |
| 传出威胁 | 显示传出威胁。 |
| 筛选器 | 应用筛选器以仅显示所选类型的项目。 |
| 放大和缩小 | 放大和缩小地图。 |
| 导出 | 导出图表作为 .png 图像或 PDF。 |
| Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days | 表示执行测量的时间段。 |

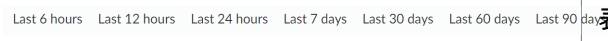
# 网络监控报告

App Scope 网络监控报告（**Monitor**（监控） > **App Scope** > **Network Monitor**（网络监控））显示指定时间段内专用于不同网络功能的带宽。每个网络功能均用颜色进行标记，如图表下面的图例所示。例如，下图显示了过去 7 天基于会话信息的应用程序带宽。


© 2019 Palo Alto Networks, Inc.




网络监控报告包含以下按钮和选项。

| 按钮 | 说明 |
| --- | --- |
| **Top 10** | 确定具有图表所包括的最高测量结果的记录数。 |
| 应用程序 | 确定报告的项目的类型：应用程序、应用程序类别、源或目标。 |
| **Filter**（筛选器） | 应用筛选器以仅显示所选项目。**None**（无）显示所有条目。 |
|  | 确定是显示会话信息还是显示字节信息。 |
| 导出 | 导出图表作为 .png 图像或 PDF。 |
|  | 确定是通过堆积柱形图还是通过堆积面积图来呈现信息。 |
|   | 表示执行更改测量的时间段。 |

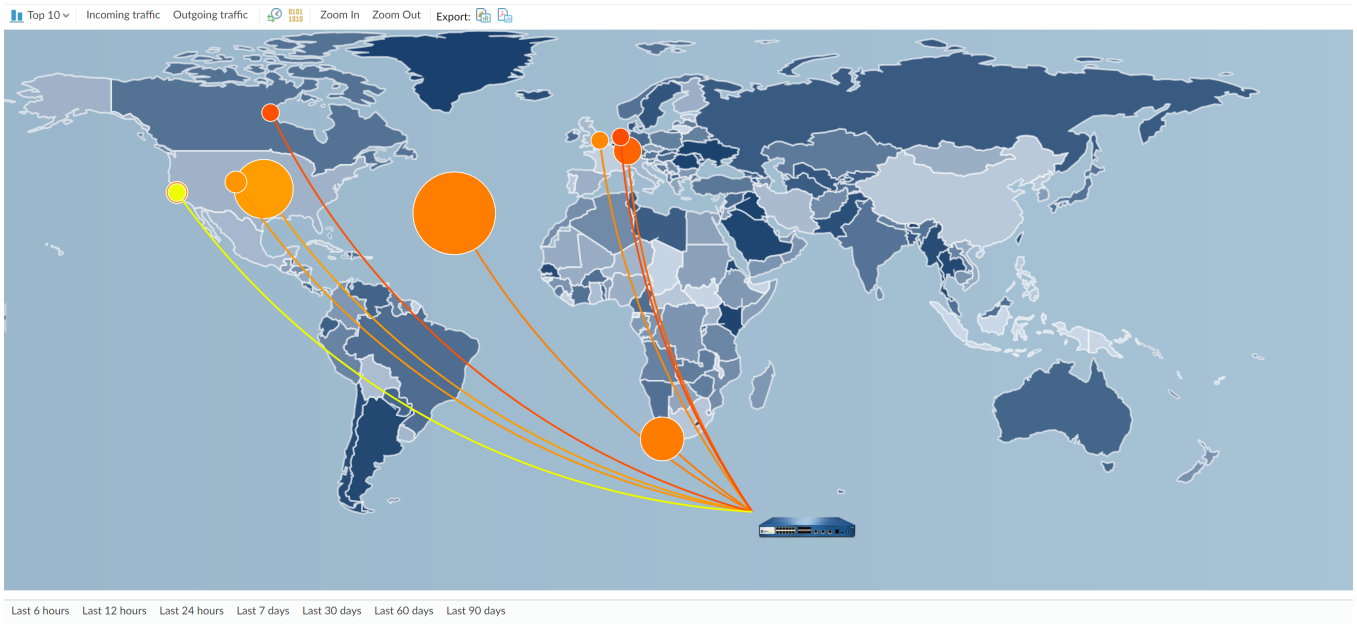
# 通信地图报告

App Scope 通信地图报告（**Monitor**（监控） > **App Scope** > **Traffic Map**（通信地图））按照会话数或流量显示通信流的地理视图。

防火墙使用地理定位创建流量地图。如果您尚未指定防火墙上的地理定位坐标，则防火墙位于流量地图屏幕的底部（常规设置部分中的 **Device**（设备） > **Setup**（设置） > **Management**（管理））。



© 2019 Palo Alto Networks, Inc.




每个通信类型均用颜色进行标记，如图表下面的图例所示。通信地图报告包含以下按钮和选项。

| 按钮 | 说明 |
| --- | --- |
| **Top 10** | 确定具有图表所包括的最高测量结果的记录数。 |
| 传入威胁 | 显示传入威胁。 |
| 传出威胁 | 显示传出威胁。 |
| | 确定是显示会话信息还是显示字节信息。 |
| 放大和缩小 | 放大和缩小地图。 |
| 导出 | 导出图表作为 .png 图像或 PDF。 |
| Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days | 表示执行更改测量的时间段。 |



© 2019 Palo Alto Networks, Inc.

# 使用自动关联引擎

自动关联引擎是一种分析工具，使用防火墙上的日志来检测网络上的应该采取行动的事件。该引擎可以关联一系列相关威胁事件，当综合分析这些事件时，我们很可能发现网络上的主机受到影响，或者受到其他更高级别的威胁。它会指出风险区域，例如网络上的受影响主机，从而让您能够评估风险，并采取行动防止网络资源被利用。自动关联引擎使用关联项目 来分析日志以获取其中的模式，当发生匹配时，它会生成关联事件。

以下型号支持自动关联引擎：

- *Panorama — M* 系列设备和虚拟设备
- *PA-7000* 系列防火墙
- *PA-5200* 系列防火墙
- *PA-3200* 系列防火墙


- 自动关联引擎概念
- 查看关联项目
- 解释关联事件
- 使用 ACC 中的“受影响主机”小部件


## 自动关联引擎概念

自动关联引擎使用关联项目 来分析日志以获取其中的模式，当发生匹配时，它会生成关联事件。


- 关联项目
- 关联事件


### 关联项目

关联项目是一种定义文件，它指定对照匹配的模式和用于执行查询的数据源，以及查找这些模式的时间段。模式是查询防火墙上的以下数据源（或日志）的条件的布尔结构：应用程序统计信息、流量、流量摘要、威胁摘要、威胁、数据筛选、URL 筛选。每个模式都有严重性分级和阈值（在指定的时间限制之内出现模式匹配的次数，达到该次数时才表明存在恶意行动）。达到匹配条件时，则会记录关联事件。

关联项目能够连接孤立的网络事件，并查找表示更严重事件的模式。这些对象能够识别可疑流量模式和网络异常情况，包括可疑 IP 活动、已知的命令与控制活动、已知的漏洞利用或 botnet 活动，当它们关联时，则表明网络上的主机很可能已受到影响。关联项目由 Palo Alto Networks 威胁研究团队定义和开发，提供对防火墙和 Panorama 的每周动态更新。为了获取新的关联项目，防火墙必须具有威胁防御许可证。Panorama 需要支持许可证才能获取更新。

在关联项目中定义的模式可以是静态或动态的。包括在 WildFire 中发现到的模式的相关对象是动态的，可以通过被网络上的恶意软件作为目标的主机启动的命令与控制活动或是 Panorama 上的陷阱保护端点发现的活动，关联由 WildFire 检测到的恶意软件模式。例如，当主机向 WildFire 云提交一个文件，而且判断为恶意时，则关联项目会查找网络上展现云中所见的相同行为的其他主机或客户端。如果恶意软件样本执行了 DNS 查询并浏览到恶意软件域，则关联项目将解析日志以查找类似事件。当主机上的活动与云中的分析相匹配时，则会记录高严重性的关联事件。

### 关联事件

当在关联项目中定义的模式和阈值与网络上的流量模式相匹配时，将会记录关联事件。要解释关联事件和查看事件的图形显示，请参阅使用 ACC 中的“受影响主机”小部件。



© 2019 Palo Alto Networks, Inc.

# 查看关联项目

可以查看防火墙当前可用的关联对象。

STEP 1 | 选择 **Monitor**（监控）> **Automated Correlation Engine**（自动关联引擎）> **Correlation Objects**（关联对象）。默认情况下，列表中的所有项目都启用。

| TITLE | CATEGORY | STATE | DESCRIPTION |
|---|---|---|---|
| Multiple User from One Endpoint MFA Credential Theft | credential-theft-abuse | active | This correlation object detects multiple account abuse from a possibly compromised endpoint |
| WildFire C2 | compromised-host | active | This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network. |
| WildFire and Traps ESM Correlated C2 | compromised-host | active | This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware. |
| Single Account and Endpoint MFA Credential Theft | credential-theft-abuse | active | This correlation object detects activity from a possibly compromised user account from a single endpoint |
| Compromise Activity Sequence | compromised-host | active | This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain. |
| Exploit Kit Activity | compromised-host | active | This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature. |
| Single Account 1 FA Multiple Endpoints Credential Timeouts | credential-theft-abuse | active | This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account |
| Beacon Detection | compromised-host | active | This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc. |
| Single Account and Endpoint MFA Credential Timeout | credential-theft-abuse | active | This correlation object detects timedout MFA authentication attempts from a single endpoint using single account |
| Multiple Endpoint MFA Credential Timeout Abuse | credential-theft-abuse | active | This correlation object detects timed out second factor authentications from multiple endpoints using a single user account |
| Multiple Endpoint MFA Credential Abuse | credential-theft-abuse | active | This correlation object detects activity from multiple endpoints using a single user account |
| Exploit Kit Delivering XOR obfuscated malware | compromised-host | active | This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities. |
| Single Account 1 FA Credential Abuse | credential-theft-abuse | active | This correlation object detects timed out first factor authentications from an endpoint using a single user account |

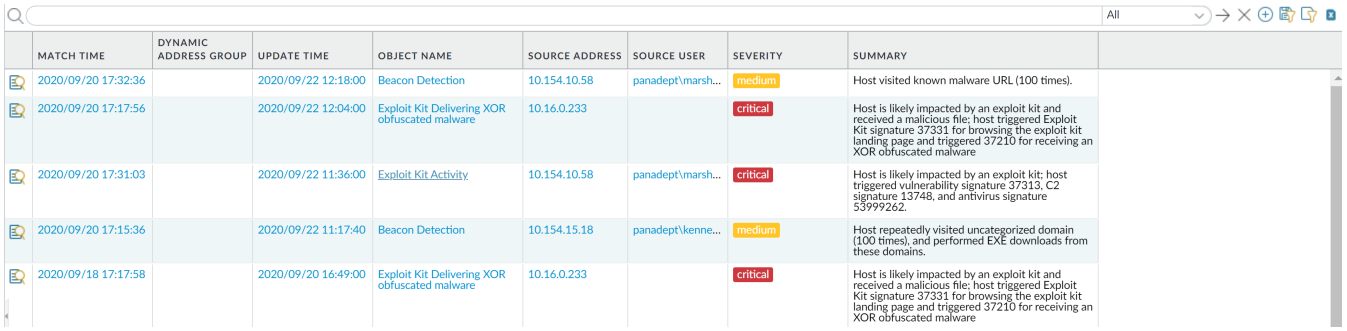
STEP 2 | 查看有关每个关联项目的详细信息。每个项目提供以下信息：

- **Name**（名称）和 **Title**（主题）— 名称和主题指示关联对象检测到的活动类型。默认情况下，名称列在视图中隐藏。要查看项目的定义，请取消隐藏该列，并单击名称链接。
- **ID** — 标识关联对象的唯一编号。默认情况下，此列也会隐藏。该 ID 属于 6000 系列。
- **Category**（类别）— 针对网络、用户或主机的威胁或危害的类型的分类。现在，所有项目都标识网络上的受影响主机。
- **State**（状态）— 表示关联对象的状态，即启用（活动）还是禁用（不活动）。默认情况下，列表中的所有项目都启用，因而处于状态。由于这些项目是基于威胁智能数据的，并且由 Palo Alto Networks 威胁研究团队定义，因此请保持项目的活动状态，以便跟踪和检测网络上的恶意活动。
- **Description**（说明）— 指定防火墙或 Panorama 分析日志的匹配条件。它说明了识别恶意活动或可疑主机行为的加快发展或升级的匹配条件序列。例如，**Compromise Lifecycle**（危害生命周期）对象可检测出涉入到整个攻击生命周期的主机，攻击分为三步升级，首先扫描或探测活动，然后实施攻击，最后将网络连接到已知恶意域。

有关详细信息，请参阅自动关联引擎概念和使用自动关联引擎。

# 解释关联事件

您可在 **Monitor**（监控）> **Automated Correlation Engine**（自动关联引擎）> **Correlated Events**（关联事件）选项卡中查看和分析为每个关联事件生成的日志。






© 2019 Palo Alto Networks, Inc.

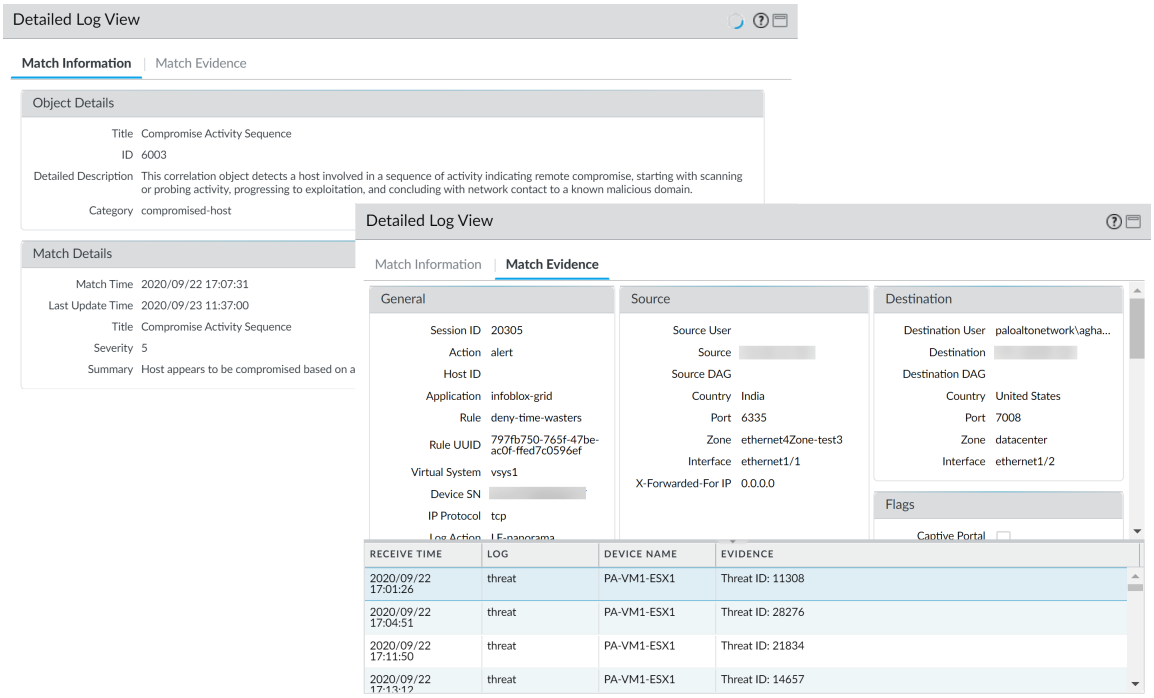
关联事件包括以下详细信息：

| 字段 | 说明 |
| --- | --- |
| **Match Time**（匹配时间） | 关联项目触发匹配项的时间。 |
| **Update Time**（更新时间） | 上一次通过匹配证据更新事件的时间。当防火墙收集到在关联项目中定义的模式或事件序列的证据时，关联事件日志上的时间戳将会更新。 |
| 项目名称 | 触发匹配项的关联项目的名称。 |
| **Source Address**（源地址） | 产生流量的网络用户/设备的 IP 地址。 |
| 源用户 | 目录服务器的用户和用户组信息（如果启用User-ID）。 |
| 严重性级别<br><br>要将防火墙或 *Panorama* 配置为使用电子邮件、*SNMP* 或 *syslog* 消息发送所需安全级别的警报，请参阅使用外部服务进行监控。 | 级别表示匹配的紧急程度和影响。严重性级别表示损害程度或升级模式，以及发生的频率。由于关联对象主要侧重于检测威胁，因此关联事件通常与确定网络上受影响的主机相关联，且严重性意味着以下级别：<br>• **Critical**（严重）— 根据表示升级模式的关联事件确认主机已受到影响。例如，当主机收到 WildFire 判定为恶意的文件时会记录重要事件，此事件呈现一些在该恶意文件的 WildFire 沙盒中观察到的命令和控制活动。<br>• **High**（高）— 根据多个威胁事件之间的关联表示主机很有可能受到影响，如在与从特定主机生成的命令和控制活动相匹配的网络中的任何位置检测到的恶意软件。<br>• **Medium**（中）— 根据检测到的一个或多个可疑事件表示主机可能受到影响，如重复访问已知的恶意 URL，以建议对命令和控制活动编写脚本。<br>• **Low**（低）— 根据检测到的一个或多个可疑事件表示主机可能受到影响，如访问恶意 URL 或动态 DNS 域。<br>• **Informational**（参考）— 检测到可以在聚合中用于确定可疑活动的事件；每个事件对于自己并不一定很重要。 |
| **Summary**（摘要） | 汇总收集的针对关联事件的证据的说明。 |

单击 图标可查看详细日志视图，其中包括匹配的所有证据：



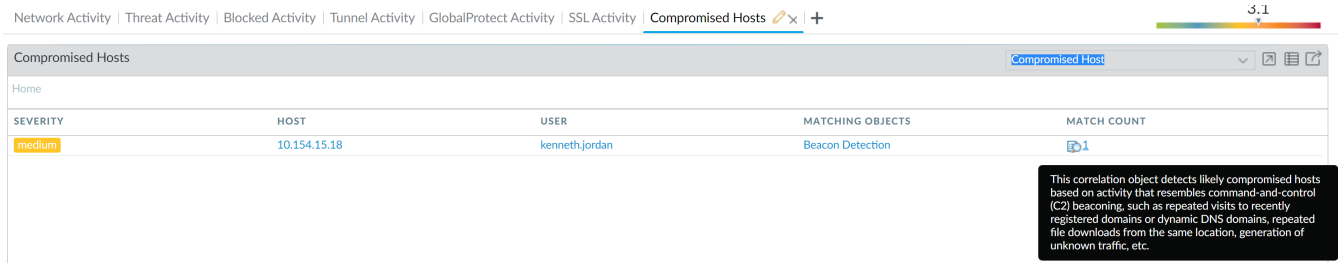
© 2019 Palo Alto Networks, Inc.




| 选项卡 | 说明 |
|---|---|
| **Match Information**（匹配信息） | 对象详细信息：提供触发匹配项的关联项目的信息。<br>Match Details（匹配详细信息）：匹配详细信息的摘要,包括匹配时间、匹配证据中的上一次更新时间、事件的严重性，以及事件摘要。 |
| **Match Evidence**（匹配证据） | 提供确认关联事件的所有证据。它列出为每个会话收集的证据的详细信息。 |

# 使用 ACC 中的“受影响主机”小部件

**ACC > Threat Activity**（威胁活动）上的“受影响主机”小部件可以汇总关联事件 ，并按严重性对它们进行排序。它显示触发事件的源 IP 地址/用户、匹配的关联项目、匹配项目的次数。使用匹配计数链接可跳转至匹配证据详细信息。




有关更多详细信息，请参阅使用自动关联引擎和使用应用程序命令中心。


© 2019 Palo Alto Networks, Inc.

# 执行数据包捕获

所有 Palo Alto Networks 防火墙都允许您对穿过防火墙上的管理接口和网络接口的流量执行数据包捕获 (pcaps)。在数据面上执行数据包捕获时，您可能需要 禁用硬件卸载，以确保防火墙捕获所有流量。

数据包捕获可能消耗大量 *CPU* 资源，并且降低防火墙性能。仅在必要时使用此功能，并且确保在收集到所需的数据包之后关闭此功能。


- 数据包捕获类型
- 禁用硬件卸载
- 执行自定义数据包捕获
- 执行威胁数据包捕获
- 执行应用程序数据包捕获
- 在管理接口上执行数据包捕获


## 数据包捕获类型

您可以启用不同类型的数据包捕获，具体取决于您需要执行的操作：

- 自定义数据包捕获 — 防火墙捕获所有流量的数据包，或者根据定义的筛选器捕获特定流量的数据包。例如，可以配置防火墙，以便仅捕获进出特定源和目标 IP 地址或端口的数据包。您可以使用数据包捕获来排除与网络相关的问题，或者收集应用程序属性，以便能够编写定制应用程序签名或从 Palo Alto Networks 请求应用程序签名。请参阅执行自定义数据包捕获。
- 威胁数据包捕获 — 当防火墙检测到病毒、间谍软件或漏洞时，它会捕获数据包。您可在防病毒、防间谍软件和漏洞防护安全配置文件中启用此功能。在威胁日志的第二列，将显示查看或导出数据包捕获结果的链接。这些数据包捕获提供关于威胁的上下文，可帮助您确定攻击是否成功，或者了解有关攻击者使用的方法的详细信息。如果您感觉出现了误报或漏报，也可将此类型的 pcap 提交到 Palo Alto Networks，对威胁进行重新分析。请参阅执行威胁数据包捕获。
- 应用程序数据包捕获 — 防火墙基于您定义的特定应用程序或筛选器来捕获数据包。在匹配数据包捕获规则的流量的流量日志的第二列，将显示查看或导出数据包捕获结果的链接。请参阅执行应用程序数据包捕获。
- 管理接口数据包捕获—防火墙在管理接口 (MGT) 上捕获数据包。对于穿过接口的服务，例如防火墙管理身份验证到外部身份验证服务、软件和内容更新、日志转发、与 SNMP 服务器通信、GlobalProtect 和身份验证门户的身份验证请求，数据包捕获在排除服务故障时非常有用。请参阅在管理接口上执行数据包捕获。
- **GTP** 事件数据包捕获—防火墙捕获单一 GTP 事件,如 GTP-in-GTP、最终用户 IP 欺骗和异常 GTP 消息，便于移动网络操作员轻松进行 GTP 故障排除。在移动网络保护配置文件中启用数据包捕获。

## 禁用硬件卸载

流经 Palo Alto Networks 上网络数据端口的流量被数据面板 CPU 执行数据包捕获。要捕获流经管理接口的流量，必须在管理接口上执行数据包捕获，在这种情况下，数据包捕获在管理层面执行。

当数据包捕获在数据面板上执行时，与防火墙、丢弃和出口捕获阶段相比，入口阶段的数据包捕获筛选器的使用方式将有所不同。入口阶段将使用数据包捕获筛选器以将符合筛选器的单个数据包复制到捕获文件中。未能通过数据包解析检查的数据包在捕获前就被丢弃。防火墙、丢弃和出口捕获阶段将使用相同的数据包捕获筛选器标记所有符合筛选器的新会话。因为每个会话都可以标识客户端到服务器以及服务器到客户端的连接（如会话表所示），在任何一个方向与标记会话匹配的任何流量都将被复制到防火墙阶段和传输阶段捕获文件中。相反，在任何一个方向与标记会话匹配的任何丢弃流量（接收后阶段）都将被复制到丢弃阶段捕获文件中。



© 2019 Palo Alto Networks, Inc.

在包含网络处理器的防火墙型号中，可以卸载符合 Palo Alto Networks 某些预定义标准的流量，以供网络处理器进行处理。这些卸载过的流量将不会到达数据面板 CPU，从而也不会被捕获。要捕获卸载流量，必须使用 CLI 关闭硬件卸载功能。

可以卸载的常见流量包括非加密 SSL 和 SSH 流量（加密后，在 SSL/SSH 会话初始设置之后无法进行检测）、网络协议（OSPF、BGP、RIP 等）以及匹配应用程序覆盖策略的流量。有些类型的流量永远不会卸载，例如 ARP、所有非 IP 流量、IPSec、和 VPN 会话。一旦被网络处理器标识，单个 SYN、FIN 和 RST，即使是已卸载的会话流量，也绝不会被卸载，且始终流至数据面板 CPU。

以下防火墙支持硬件卸载：*PA-3200* 系列、*PA-5200* 系列和 *PA-7000* 系列防火墙。

禁用硬件卸载会增加数据面 *CPU* 使用率。如果数据面 *CPU* 使用率已经很高，您可能希望在禁用硬件卸载之前计划一个维护窗口。

STEP 1 | 通过运行以下 CLI 命令来禁用硬件卸载：

```
admin@PA-7050>set session offload no
```

STEP 2 | 在防火墙捕获所需的流量之后，通过运行以下 CLI 命令来启用硬件卸载：

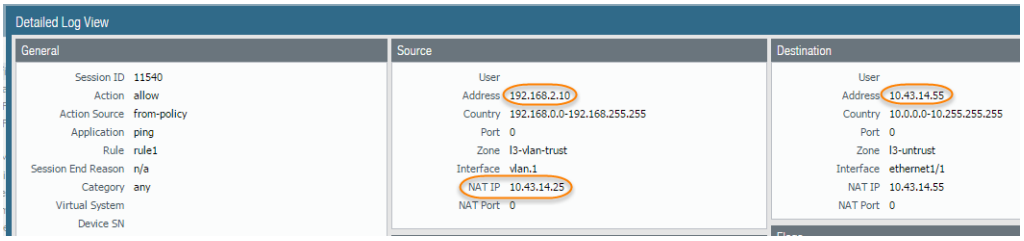
```
admin@PA-7050>set session offload yes
```

# 执行自定义数据包捕获

自定义数据包捕获允许您定义防火墙将捕获的流量。要确保捕获所有流量，您可能需要禁用硬件卸载。

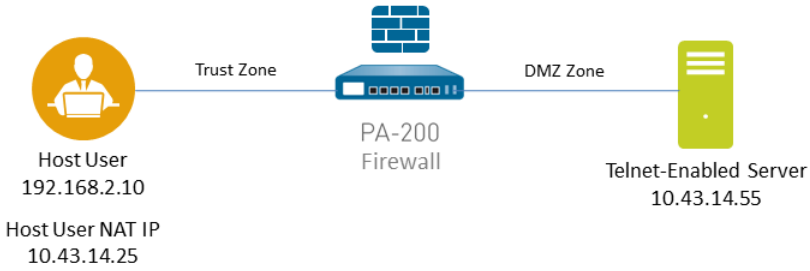
STEP 1 | 在启动数据包捕获之前，请确定要捕获的流量的属性。

例如，对于两个系统之间的流量，需要确定源 IP 地址、源 NAT IP 地址、目标 IP 地址，执行从源系统到目标系统的 Ping 命令。Ping 命令完成之后，转至 **Monitor**（监控）> **Traffic**（流量），找到两个系统的流量日志。单击位于日志第一列的 **Detailed Log View**（详细日志视图）图标，记下源地址、源 NAT IP 地址、目标地址。




以下示例显示了如何使用数据包捕获来解决从信任区域中的用户到 DMZ 区域中的服务器的 Telnet 连接问题。


© 2019 Palo Alto Networks, Inc.




STEP 2 | 设置数据包捕获筛选器，使得防火墙仅捕获您关注的流量。

筛选器让您更加轻松地查找在数据包捕获中需要的信息，并且减少防火墙执行数据包捕获所需的工作量。要捕获所有流量，请不要定义筛选器，而应将筛选器选项关闭。

例如，如果您在防火墙上配置了 NAT，则将需要应用两个筛选器。第一个筛选器用于筛选从 NAT 前源 IP 地址到目标 IP 地址的流量，第二个筛选器用于筛选从目标服务器到源 NAT IP 地址的流量。

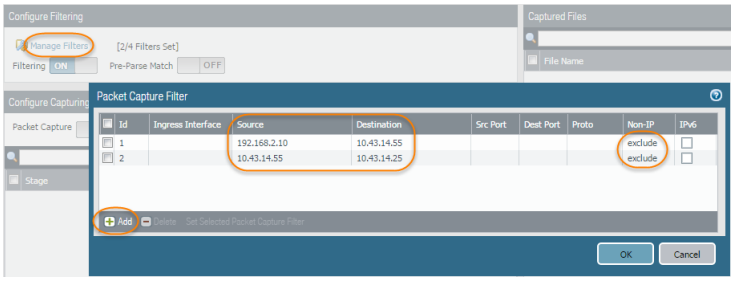
1. 选择**Monitor**（监控）> **Packet Capture**（数据包捕获）。
2. 单击窗口底部的 **Clear All Settings**（清除所有设置），以清除全部现有捕获设置。
3. 单击 **Manage Filters**（管理筛选器）并单击 **Add**（添加）。
4. 选择 **Id** 1，在 **Source**（源）字段中输入所需的源 IP 地址，在 **Destination**（目标）字段中输入目标 IP 地址。

   例如，输入源 IP 地址 `192.168.2.10` 和目标 IP 地址 `10.43.14.55`。要进一步筛选捕获，请将 **Non-IP**（非 **IP**）设置为 **exclude**（排除）非 IP 流量，例如广播流量。
5. **Add**（添加）第二个筛选器，并选择 **Id** 2。

   例如，在 **Source**（源）字段中输入 `10.43.14.55`，在 **Destination**（目标）字段中输入 `10.43.14.25`。在 **Non-IP**（非 **IP**）下拉菜单中选择 **exclude**（排除）。



© 2019 Palo Alto Networks, Inc.




6. 单击 **OK**（确定）。

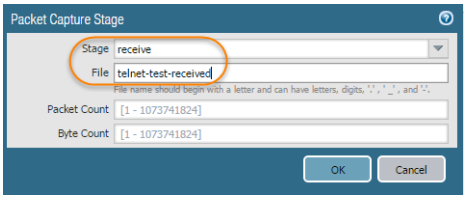
STEP 3 | 将 **Filtering**（筛选）设置为 **On**（开）。

STEP 4 | 指定触发数据包捕获的流量阶段，以及用于存储捕获内容的文件名。对于每个阶段的定义，请单击数据包捕获页面上的 **Help**（帮助）图标。

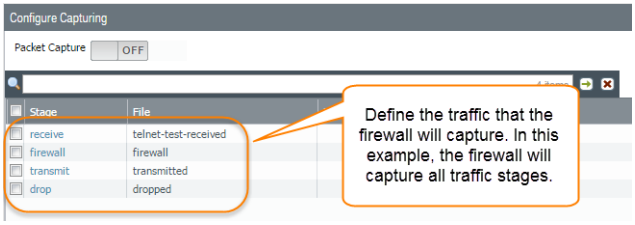
例如，要配置所有数据包捕获阶段，并为每个阶段定义文件名，请执行以下程序：

1. 为数据包捕获配置 **Add**（添加）一个 **Stage**（阶段），并为生成的数据包捕获定义 **File**（文件）名。

   例如，在 **Stage**（阶段）字段中选择 **receive**（接收），并将 **File**（文件）名设置为 telnet-test-received。



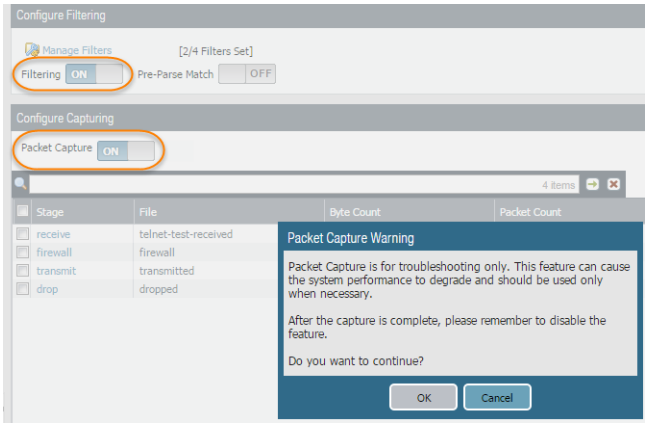

2. 继续 **Add**（添加）您要捕获的每个 **Stage**（阶段）（**receive**（接收）、**firewall**（防火墙）、**transmit**（传输）和 **drop**（丢弃）），并为每个阶段设置唯一的 **File**（文件）名。




STEP 5 | 将 **Packet Capture**（数据包捕获）设置为 **ON**（开）。

防火墙或设备警告您系统性能可能会降低；单击 **OK**（确定）确认警告。如果您定义了筛选器，则数据包捕获只对性能产生很小的影响，但在防火墙捕获了您希望分析的数据之后，应该始终 **Off**（关闭）数据包捕获。


© 2019 Palo Alto Networks, Inc.

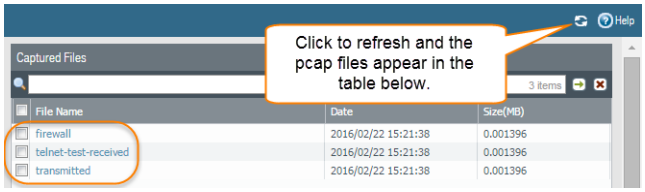



STEP 6 | 生成与您定义的筛选器匹配的流量。

在本示例中，我们通过从源系统 (192.168.2.10) 运行以下命令，生成从源系统到启用 Telnet 的服务器的流量：

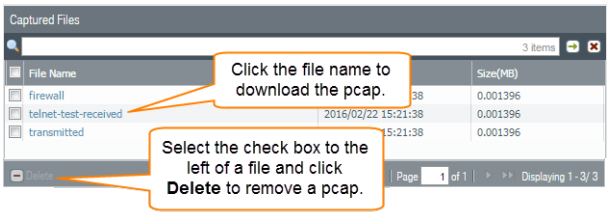
```
telnet 10.43.14.55
```

STEP 7 | **OFF**（关闭）数据包捕获，然后单击刷新按钮以查看数据包捕获文件。



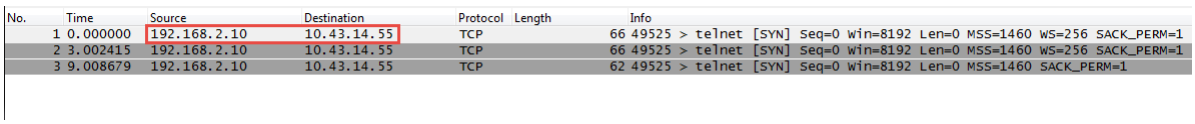

请注意，在本例中没有丢弃的数据包，因而防火墙不会为丢弃阶段创建文件。

STEP 8 | 单击“文件名”列中的文件名，下载数据包捕获。




STEP 9 | 使用网络数据包分析工具，查看数据包捕获文件。

在本例中，received.pcap 数据包捕获显示：从位于 192.168.2.10 的源系统至位于 10.43.14.55 的 Telnet 服务器的 Telnet 会话失败。源系统向服务器发出 Telnet 请求，但服务器没有响应。在本例中，服务器可能没有启用 Telnet，因此请检查服务器。




STEP 10 | 在目标服务器 (10.43.14.55) 上启用 Telnet 服务，并打开数据包捕获，以执行新的数据包捕获。

STEP 11 | 生成将触发数据包捕获的流量。



© 2019 Palo Alto Networks, Inc.

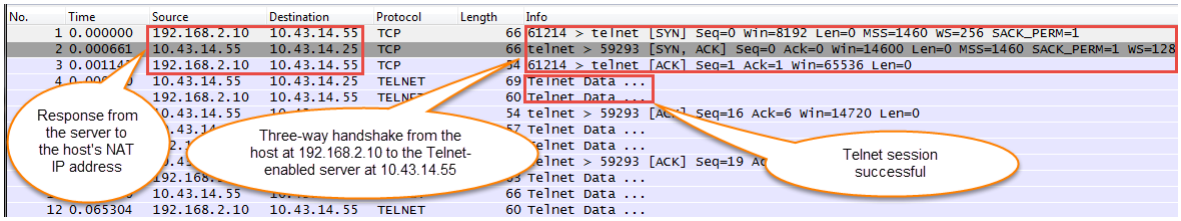
再次运行从源系统至启用 Telnet 的服务器的 Telnet 会话。

```
telnet 10.43.14.55
```

STEP 12 | 下载并打开 received.pcap 文件，并使用网络数据包分析工具查看该文件。

以下数据包捕获现在显示：从位于 192.168.2.10 的主机用户至位于 10.43.14.55 的 Telnet 服务器的 Telnet 会话成功。

您还会看到 *NAT* 地址 *10.43.14.25*。当服务器响应时，它也会响应 *NAT* 地址。您可以看到主机和服务器之间的三向握手，然后看到 *Telnet* 数据，这表明会话成功。




# 执行威胁数据包捕获

要将防火墙配置为在检测到威胁时执行数据包捕获 (pcap)，请在抗病毒、防间谍软件、漏洞防护安全配置文件上启用数据包捕获。

STEP 1 | 在安全配置文件中启用数据包捕获选项。

有些安全配置文件允许您定义单个数据包捕获或扩展捕获。如果您选择扩展捕获，请定义捕获长度。这样可以允许防火墙捕获更多数据包，以提供与威胁相关的更多上下文。

如果针对特定威胁的操作是允许，则防火墙不会触发威胁日志，也不会捕获数据包。如果操作是警报，则您可以将数据包捕获设为单个数据包捕获或扩展捕获。所有阻止操作（丢弃、阻止和重置操作）都能捕获单个数据包。默认操作取决于设备上的内容数据包。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件），并按照以下方式为支持的配置文件启用数据包捕获选项：
   - **Antivirus**（抗病毒）— 选择自定义搞病毒配置文件，并在 **Antivirus**（抗病毒）选项卡中选中 **Packet Capture**（数据包捕获）复选框。
   - **Anti-Spyware**（防间谍软件）— 选择自定义防间谍软件配置文件，单击 **DNS Signatures**（DNS 签名）选项卡，并在 **Packet Capture**（数据包捕获）下拉菜单中选择 **single-packet**（单数据包）或 **extended-capture**（扩展捕获）。
   - **Vulnerability Protection**（漏洞保护）—选择自定义漏洞保护配置文件，然后在 **Rules**（规则）选项卡中单击 **Add**（添加），以添加新规则或选择现有规则。将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单个数据包）或 **extended-capture**（扩展捕获）。

   如果配置文件已定义了签名例外，请单击 *Exceptions*（例外）选项卡，并在签名的 *Packet Capture*（数据包捕获）列中设置 *single-packet*（单个数据包）或 *extended-capture*（扩展捕获）。
2. （可选）如果您为任何配置文件选择了 **extended-capture**（扩展捕获），请定义扩展数据包捕获长度。
   1. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID**（内容-ID），并编辑 Content-ID（内容-ID）设置。
   2. 在 **Extended Packet Capture Length (packets)**（扩展数据包捕获长度（数据包））部分中，指定防火墙将捕获的数据包数量（范围为 1-50；默认值为 5）。


© 2019 Palo Alto Networks, Inc.

3. 单击 **OK**（确定）。

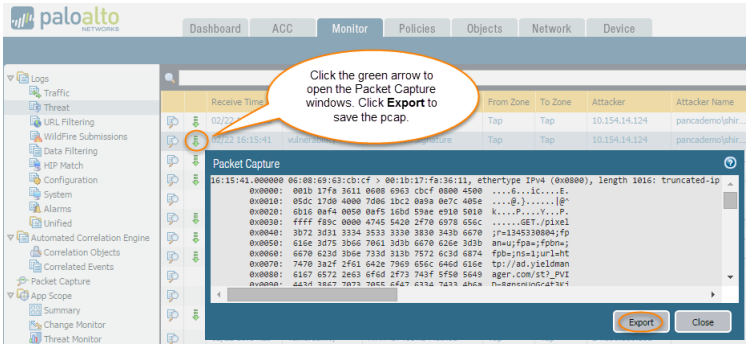
STEP 2 | 将安全配置文件（已启用数据包捕获）添加到安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全）并选择规则。
2. 选择 **Actions**（操作）选项卡。
3. 在“配置文件设置”部分中，选择启用了数据包捕获的配置文件。

   例如，单击 **Antivirus**（抗病毒）下拉菜单，并选择启用了数据包捕获的配置文件。

STEP 3 | 从威胁日志查看/导出数据包捕获。

1. 选择 **Monitor**（监视器）> **Logs**（日志）> **Threat**（威胁）。
2. 在您感兴趣的日志条目中，单击第二列中的绿色数据包捕获图标 。直接查看数据包捕获或将其 **Export**（导出）到您的系统。




# 执行应用程序数据包捕获

以下主题介绍配置防火墙以执行应用程序数据包捕获的两种方法：

- 执行针对未知应用程序的数据包捕获
- 执行定制应用程序数据包捕获

## 执行针对未知应用程序的数据包捕获

对于包含防火墙无法识别的应用程序的会话，Palo Alto Networks 防火墙可自动生成数据包捕获。通常，被分类为未知流量 — tcp、udp 或 non-syn-tcp — 的应用程序，都是尚未具有 App-ID 签名的商用应用程序、网络上的内部或定制应用程序，或存在潜在威胁的应用程序。您可以使用这些数据包捕获，来收集与未知应用程序相关的更多上下文，或使用信息来分析流量是否存在潜在威胁。您还可以管理自定义或未知应用程序，方式如下：通过安全策略进行控制，或者编写自定义应用程序签名并创建基于自定义签名的安全规则。如果应用程序是商用应用程序，您可将数据包捕获提交至 Palo Alto Networks，以便创建 App-ID 签名。

STEP 1 | 确认未知应用程序数据包捕获已启用（该选项默认启用）。

1. 要查看未知应用程序捕获设置，请运行以下 CLI 命令：

```
admin@PA-220>show running application setting | match “Unknown capture”
```

2. 如果未知捕获设置选项处于关闭状态，请启用该选项：

```
admin@PA-220>set application dump-unknown yes
```

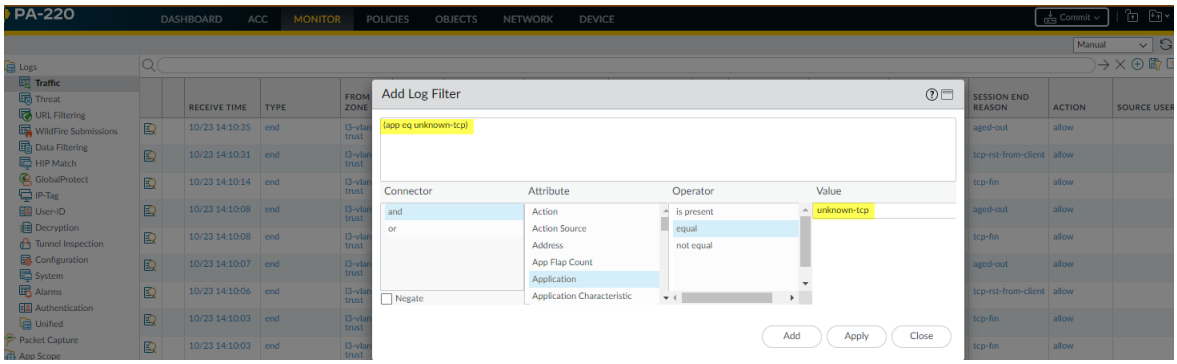
STEP 2 | 通过筛选流量日志，找到 TCP 和 UDP 应用程序。

1. 选择 **Monitor**（监视器）> **Logs**（日志）> **Traffic**（流量）.

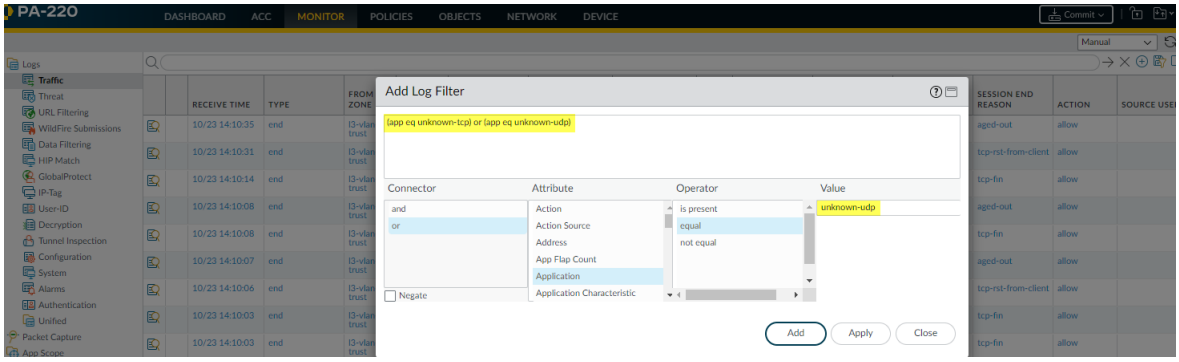


© 2019 Palo Alto Networks, Inc.

2. 单击 **Add Filter**（添加筛选器），创建筛选器的未知 TCP 部分（**Connector**（连接器）= “and”，**Attribute**（属性）= “Application”，**Operator**（运算符）= “equal”，并输入 “unknown-tcp” 作为 **Value**（值）），然后单击 **Add**（添加）以添加查询到筛选器。

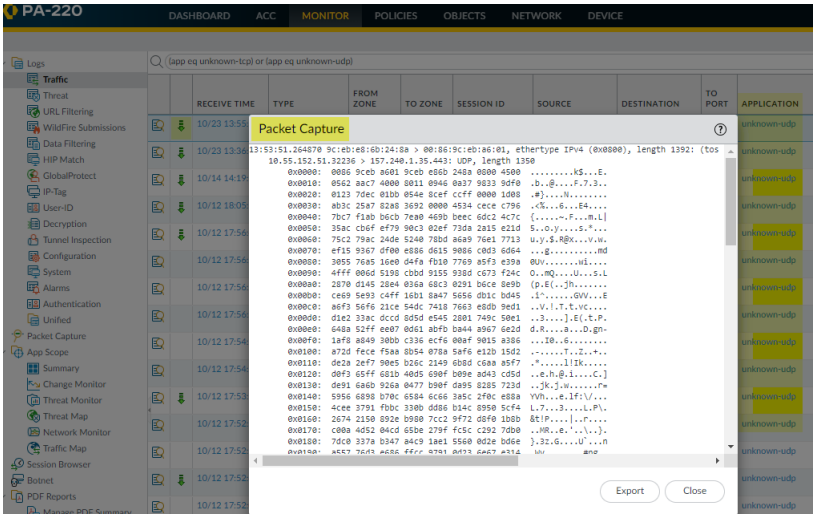



3. 创建筛选器的未知 UDP 部分（**Connector**（连接器）= “or”，**Attribute**（属性）= “Application”，**Operator**（运算符）= “equal”，并输入 “unknown-tcp” 作为 **Value**（值），然后单击 **Add**（添加）以添加查询到筛选器。




4. 单击 **Apply**（应用）将筛选器应用到日志屏幕查询字段。

STEP 3 | 单击查询字段旁边的 **Apply Filter**（应用筛选器）箭头，然后单击数据包捕获图标以查看数据包捕获或将其 **Export**（导出）到本地系统。




## 执行定制应用程序数据包捕获

您可以配置 Palo Alto Networks 防火墙，基于您定义的应用程序名称和筛选器来执行数据包捕获。然后，您可以利用数据包捕获，排除控制应用程序方面的问题。配置应用程序数据包捕获时，您必须使用在 App-



© 2019 Palo Alto Networks, Inc.

ID 数据库中定义的应用程序名称。可使用 Applipedia 查看所有 App-ID 应用程序的列表，也可在防火墙的 Web 界面上查看，位置是 **Objects**（对象）> **Applications**（应用程序）。

STEP 1 | 使用终端模拟器应用程序（如 PuTTY），启动与防火墙的 SSH 会话。

STEP 2 | 打开应用程序数据包捕获并定义筛选器。

```
admin@PA-220>set application dump on application <application-name> rule
 <rule-name>
```

例如，要为匹配名为社交网络应用程序的安全规则的 linkedin-base 应用程序捕获数据包，请运行以下 CLI 命令：

```
admin@PA-220>set application dump on application linkedin-base rule "Social
 Networking Apps"
```



也可以应用其他筛选器，例如源 *IP* 地址和目标 *IP* 地址。

STEP 3 | 查看数据包捕获输出，以确保应用了正确的筛选器。该输出将在启用数据包捕获后显示。

以下输出确认正在针对与社交网络应用程序规则匹配的流量，执行基于 linkedin-base 应用程序的应用程序捕获筛选。

```
Application setting:
Application cache            : yes
Supernode                    : yes
Heuristics                   : yes
Cache Threshold              : 16
Bypass when exceeds queue limit: no
Traceroute appid             : yes
Traceroute TTL threshold     : 30
Use cache for appid          : no
Use simple appsigs for ident : yes
Use AppID cache on SSL/SNI   : no
Unknown capture              : on
Max. unknown sessions        : 5000
Current unknown sessions     : 7
Application capture          : on
Max. application sessions    : 5000
Current application sessions : 0
Application filter setting:
    Rule                     : Social Networking Apps
    From                     : any
    To                       : any
    Source                   : any
    Destination              : any
    Protocol                 : any
    Source Port              : any
    Dest. Port               : any
    Application              : linkedin-base

Current APPID Signature
   Memory Usage              : 16768  KB (Actual 16440  KB)
      TCP 1 C2S              : regex 11898  states
      TCP 1 S2C              : regex 4549   states
      UDP 1 C2S              : regex 4234   states
      UDP 1 S2C              : regex 1605   states

Alternate APPID Signature
   Memory Usage              : 16768  KB (Actual 16425  KB)
      TCP 1 C2S              : regex 11878  states
      TCP 1 S2C              : regex 4549   states
      UDP 1 C2S              : regex 4233   states
      UDP 1 S2C              : regex 1604   states
```

STEP 4 | 从 Web 浏览器访问 linkedin.com，并执行 LinkedIn 任务以生成 LinkedIn 流量，然后运行下列 CLI 命令以关闭应用程序数据包捕获：

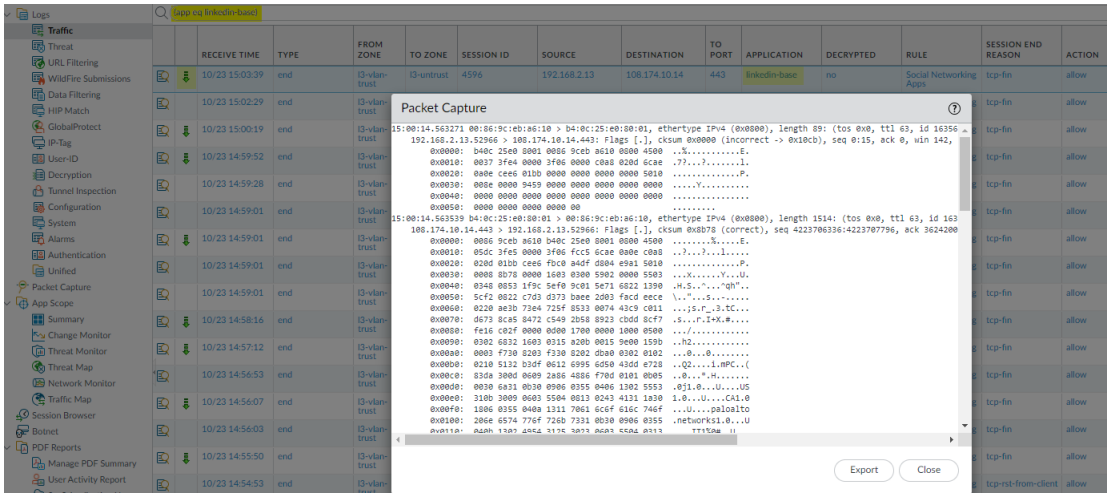
```
admin@PA-220>set application dump off
```

STEP 5 | 查看/导出数据包捕获。

1. 登录到防火墙的 Web 界面并选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）。
2. 在您感兴趣的日志条目中，单击绿色数据包捕获图标。
3. 直接查看数据包捕获或将其 **Export**（导出）到您的计算机。以下屏幕截图显示了 linkedin-base 数据包捕获。



© 2019 Palo Alto Networks, Inc.




# 在管理接口上执行数据包捕获

使用 **tcpdump** CLI 命令，您可以捕获穿过 Palo Alto Networks 防火墙上的管理接口 (MGT) 的数据包。

每个平台都设置了 ***tcpdump*** 捕获的默认字节数。*PA-220* 防火墙捕获每个数据包的 *68* 字节数据，超出的部分将会截取。*PA-7000* 系列防火墙和 *VM* 系列防火墙捕获每个数据包的 *96* 字节数据。要定义 ***tcpdump*** 捕获的数据包数量，请使用 ***snaplen***（*snap* 长度）选项（范围 *0-65535*）。将 ***snaplen*** 设置为 *0* 将导致防火墙使用捕获完整数据包所需的最大长度。

STEP 1 | 使用终端模拟器应用程序（如 PuTTY），启动与防火墙的 SSH 会话。

STEP 2 | 要在 MGT 接口上启动数据包捕获，请运行以下命令：

```
admin@PA-220>tcpdump filter “<filter-option> <IP-address>”snaplen length
```

例如，要捕获管理员使用 RADIUS 向防火墙进行身份验证时生成的流量，请按照 RADIUS 服务器的目标 IP 地址（在本例中为 10.5.104.99）进行筛选：

```
admin@PA-220>tcpdump filter “dst 10.5.104.99” snaplen 0
```

还可按 src（源 IP 地址）、host、net 进行筛选，您可以排除内容。例如，要按子网进行筛选，并排除所有 SCP、SFTP 和 SSH 流量（它们使用端口 22），请运行以下命令：

```
admin@PA-220>tcpdump filter “net 10.5.104.0/24 and not port 22” snaplen 0
```

每次 ***tcpdump*** 执行数据包捕获时，它将内容存储在名为 *mgmt.pcap* 的文件中。每次您运行 ***tcpdump*** 时，此文件会被覆盖。

STEP 3 | 在您感兴趣的流量穿过 MGT 接口后，请按 Ctrl + C 键停止捕获。

STEP 4 | 通过运行以下命令查看数据包捕获：

```
admin@PA-220> view-pcap mgmt-pcap mgmt.pcap
```

以下输出显示从 MGT 端口 (10.5.104.98) 到 RADIUS 服务器 (10.5.104.99) 的数据包捕获：


© 2019 Palo Alto Networks, Inc.

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, Access
 Request (1), id: 0x00 length: 89
 09:55:29.144354 arp reply 10.5.104.98 is-at 00:25:90:23:94:98 (oui
 Unknown)
 09:55:29.379290 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS, Access
 Request (1), id: 0x00 length: 70
 09:55:34.379262 arp who-has 10.5.104.99 tell 10.5.104.98
```

STEP 5 | （可选）使用 SCP（或 TFTP）从防火墙导出数据包捕获。例如，要使用 SCP 导出数据包捕获，请运行以下命令：

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to <username@host:path>
```

例如，要将 pcap 导出至位于 10.5.5.20 的启用 SCP 的服务器，保存在名为 temp-SCP 的临时文件夹中，请运行 CLI 命令：

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to admin@10.5.5.20:c:/temp-
SCP
```

输入 SCP 服务器上的登录名和密码，防火墙会将数据包捕获复制到启用 SCP 的服务器上的 c:\temp-SCP 文件夹中。

STEP 6 | 现在可以使用 Wireshark 等网络数据包分析工具，查看数据包捕获文件。

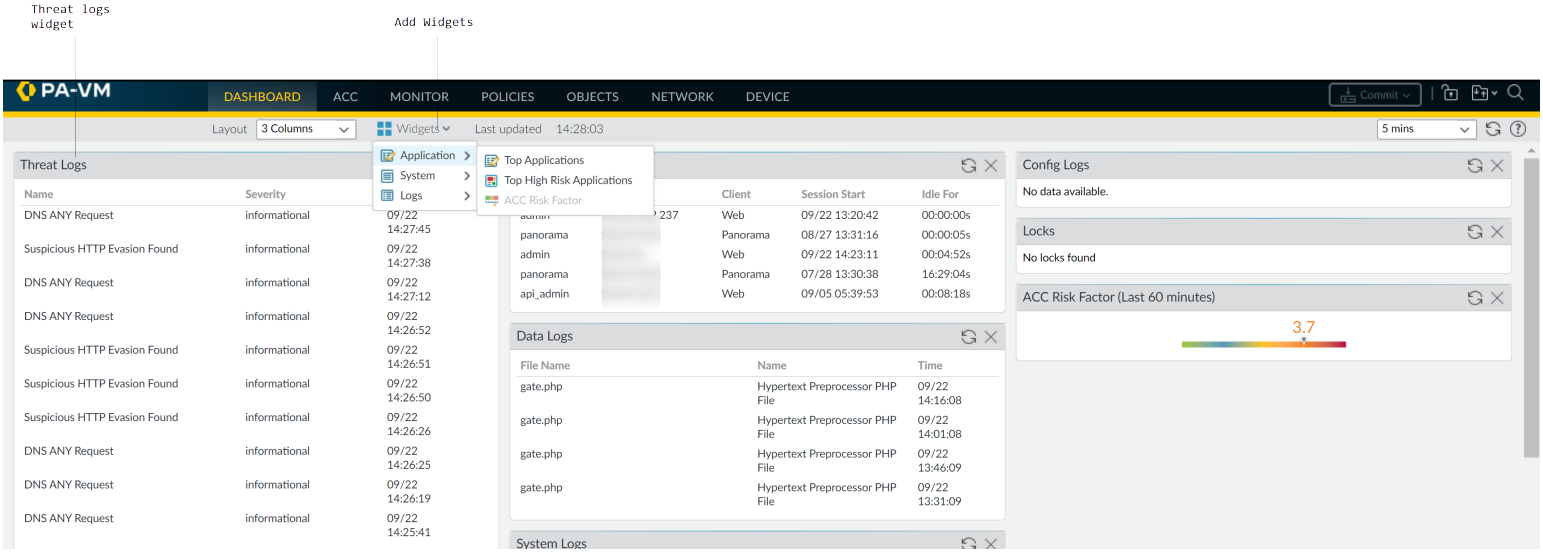


© 2019 Palo Alto Networks, Inc.

# 监视应用程序和威胁

所有的 Palo Alto Networks 下一代防火墙都配备有App-ID技术，它会识别遍历您的网络的应用程序，无论协议、加密或规避策略如何。然后可以使用应用程序命令中心监控应用程序。ACC 以图形方式汇总来自各个日志数据库的数据，从而突出显示穿过网络的应用程序、使用这些应用程序的用户及其潜在的安全影响。ACC 会使用 App-ID 执行的连续通信分类进行动态更新；如果某个应用程序更改端口或行为，则 App-ID 会继续查看通信，在 ACC 中显示结果。这项对 URL 类别、威胁和数据的额外展示可以完整且全面地了解网络活动。通过 ACC，可以非常迅速地了解有关遍历网络的通信的详细信息，然后将该信息转换为更全面的安全策略。

还可以使用仪表板监控网络。




内容交付网络基础架构以检查防火墙上记录的事件是否会构成安全风险。AutoFocus 情报摘要显示了全球范围内与您网络中的日志关联的属性、活动或行为的盛行以及链接到其上的 WildFire 判定和 AutoFocus 标记。使用活动 AutoFocus 订阅，可使用此信息创建自定义 AutoFocus 警报，以跟踪您网络上的特定威胁。



© 2019 Palo Alto Networks, Inc.

# 查看和管理日志

日志是一个自动生成并打上时间戳的文件，提供防火墙上的系统事件的审核记录或防火墙监控的网络流量事件。日志条目包含构件，这些构件即与记录事件关联的属性、活动或行为，例如应用程序类型或攻击者 IP 地址。每个日志类型都记录了一个单独事件类型的信息。例如，防火墙生成一个威胁日志，以记录与间谍软件、安全漏洞或病毒签名匹配的流量，或记录与为防火墙上的端口扫描或主机扫掠活动配置的阈值相匹配的 DoS 攻击。

- 日志类型和严重性级别
- 查看日志
- 筛选日志
- 导出日志
- 配置日志存储配额和过期期限
- 计划将日志导出至 SCP 或 FTP 服务器

## 日志类型和严重性级别

您可在 **Monitor**（监控）> **Logs**（日志）页面中查看以下日志类型。

- 流量日志
- 威胁日志
- URL 过滤日志
- WildFire 提交日志
- 数据过滤日志
- 关联日志
- 隧道检测日志
- 配置日志
- 系统日志
- HIP 匹配日志
- GlobalProtect 日志
- IP 标记日志
- User-ID 日志
- 解密日志
- 警报日志
- 身份验证日志
- 统一日志

### 流量日志

流量日志在每个会话的开始和结束显示一个条目。每个条目均包括以下信息：日期和时间；源和目标区域、源和目标动态地址组、地址和端口；应用程序名称；应用到流量的安全规则名称；规则操作（允许、拒绝或丢弃）；传入和传出接口；字节数；会话结束原因。

仅当与流量匹配的规则包括动态地址组时，才会显示动态地址组。如果 *IP* 地址出现在多个动态地址组中，那么，防火墙最多在日志中显示 *5* 个动态地址组以及源 *IP* 地址。

Type（类型）列显示条目是用于会话的开始还是结束。Action（操作）列显示防火墙已允许、拒绝还是丢弃了会话。丢弃表示阻止通信的安全规则指定了任意应用程序，而拒绝则表示规则标识了特定应用程序。如果在标识应用程序之前防火墙丢弃流量，例如当规则丢弃特定服务的所有流量时，Application（应用程序）列将显示为“not-applicable（不适用）”。



© 2019 Palo Alto Networks, Inc.

单击条目旁边的 可查看有关会话的其他详细信息，比如 ICMP 条目是否在相同源和目标之间聚合多个会话（这种情况下，Count（计数）列值将大于一）。

一旦禁用 *PAN-OS 10.0* 引用的解密日志，防火墙将 *HTTP/2* 日志作为流量日志发送。 但是，一旦启用解密日志，防火墙会将 *HTTP/2* 日志作为隧道检测日志发送（禁用解密日志后，*HTTP/2* 日志将作为流量日志发送），因此，必须检查隧道检测日志，而不是 *HTTP/2* 事件的流量日志。

## 威胁日志

当流量与某个附加到防火墙上的安全规则的安全配置文件匹配时，威胁日志显示条目。每个条目均包括以下信息：日期和时间；威胁类型（例如病毒或间谍软件）；威胁说明或 URL（名称列）；源和目标区域、地址、源和目标动态地址组、和端口；应用程序名称；警报操作（例如允许或阻止）；和严重性级别。

仅当与流量匹配的规则包括动态地址组时，才会显示动态地址组。如果 *IP* 地址出现在多个动态地址组中，那么，防火墙最多在日志中显示 *5* 个动态地址组以及源 *IP* 地址。

要查看有关各个威胁日志条目的更多详细信息：

- 单击威胁条目旁边的 可查看详细信息，例如条目是否在相同源和目标之间聚合相同类型的多个威胁（这种情况下，Count（计数）列值大于一）。
- 如果您将防火墙配置为执行数据包捕获，单击条目旁边的 以访问捕获的数据包。

下表概述了威胁严重性级别：

| 严重性级别 | 说明 |
|---|---|
| 关键 | 严重威胁，如对广泛部署的软件的默认安装产生影响的威胁，这些威胁会导致服务器的超级用户权限被窃取，使得攻击者有机会广泛窃用漏洞利用代码。攻击者通常不需要任何特别的身份验证凭据，或者无需知道各个受害人，也不需要操纵目标，即可执行所有特定功能。 |
| 高 | 能够演变为关键威胁但有抑制因素的威胁；例如，可能难以利用，不会导致攻击者的权限得到提升，或者受害者群体不会很大。<br>被判为恶意软件且操作设置为允许的 WildFire 提交日志条目将被记录为高。 |
| 中 | 影响力降到最低的小威胁，例如不会危害目标的 DoS 攻击或如下攻击：需要攻击者与受害者驻留在同一 LAN 中，仅会影响非标准配置或不知名应用程序，或者提供的访问权限有限。<br>• 根据现有的 WildFire 签名严重性，被判为恶意且操作设置阻止或警报的威胁日志条目被记录为严重性为“Medium（中）”的威胁。 |
| 低 | 警告级别的威胁，对组织的基础结构产生的影响非常小。它们通常需要本地或物理系统访问权限，并且可能经常会导致受害者隐私或 DoS 问题及信息遭到泄漏。<br>• 与 Data Filtering（数据筛选）配置文件匹配的情况会被记录为严重性为“Low（低）”的威胁。<br>• 被判为灰色软件且操作设置为任何的 WildFire 提交日志条目被记录为严重性为“Low（低）”的威胁。 |
| 参考 | 不会立即构成威胁，但是会被报告，以提醒相关人员注意可能存在更深层次问题的可疑事件。<br>• URL 过滤日志条目被记录为参考。<br>• 被判为良性且操作设置为任何的 WildFire 提交日志条目被记录为参考。<br>• 带有任何判定且操作设置为阻止和转发的 WildFire 提交日志条目被记录为参考。 |


© 2019 Palo Alto Networks, Inc.

| 严重性级别 | 说明 |
| --- | --- |
| | • 带有任何判定且操作设置为阻止的日志条目被记录为参考。 |

## URL 过滤日志

URL 筛选日志显示与附加到安全策略规则的 URL 筛选配置文件相匹配的流量条目。例如，如果某个规则阻止对特定网站和网站类别的访问，或如果配置某个规则以在用户访问网站时生成警报，则防火墙会生成一个日志。

## WildFire 提交日志

防火墙将样本（文件和电子邮件链接）转发给 WildFire 云，然后根据 WildFire 分析配置文件设置（**Objects**（对象）> **Security Profiles**（安全配置文件）> **WildFire Analysis**（**WildFire** 分析））进行分析。WildFire 完成样本的静态和动态分析后，防火墙为其转发的每个样本都生成 WildFire Submissions（WildFire 提交）日志条目。WildFire 提交日志条目包括防火墙对样本的操作（允许或阻止）、对提交样本的 WildFire 判定以及样本的严重性级别 。

下表概述了 WildFire 判定：

| 结论 | 说明 |
| --- | --- |
| **Benign**（良性） | 表示 WildFire 分析对条目的判定为良性。分类为良性的文件是安全的，没有展现恶意行为。 |
| 灰色软件 | 表示 WildFire 分析对条目的判定为件。分类为灰色软件的文件不会产生直接安全威胁，但可能展示冒失的行为。灰色软件可能包括广告软件、间谍软件、浏览器帮助程序对象 (BHO)。 |
| 网络仿冒 | 表示 WildFire 对链接的分析判定为网络钓鱼。网络钓鱼判定表明指向用户的链接的网站显示凭据网络钓鱼活动。 |
| 恶意软件 | 表示 WildFire 分析对条目的判定为恶意。被判定为恶意类的样本会构成安全威胁。我们可能遇及的恶意软件包括病毒、蠕虫、特洛伊木马、远程访问工具 (RAT)、Rootkit、Botnets 等等。对于被认定为恶意软件的样本，WildFire 云会生成并分发一个与之对应的签名，以免日后再受影响。 |

## 数据过滤日志

数据筛选日志显示有关安全规则的条目，帮助阻止敏感信息（例如信用卡号）流出受防火墙保护的区域。有关定义数据筛选配置文件的信息，请参阅数据筛选。

此日志类型还会显示文件阻止配置文件的信息。例如，如果某个规则阻止了 .exe 文件，则日志显示被阻止的文件。

## 关联日志

当在关联项目中定义的模式和阈值与网络上的流量模式相匹配时，防火墙将会记录关联事件。要解释关联事件和查看事件的图形显示，请参阅使用 ACC 中的“受影响主机”小部件。

下表概述了关联日志严重性级别：



© 2019 Palo Alto Networks, Inc.

| 严重性级别 | 说明 |
| --- | --- |
| 关键 | 根据表示升级模式的关联事件确认主机已受到影响。例如，当主机收到 WildFire 判定为恶意的文件时会记录重要事件，此事件呈现一些在该恶意文件的 WildFire 沙盒中观察到的命令和控制活动。 |
| 高 | 根据多个威胁事件之间的关联，表示主机很有可能受到影响，如在与从特定主机生成的命令和控制活动相匹配的网络中的任何位置检测到的恶意软件。 |
| 中 | 根据检测到的一个或多个可疑事件，表示主机可能受到影响，如重复访问已知的恶意 URL，以建议对命令和控制活动编写脚本。 |
| 低 | 根据检测到的一个或多个可疑事件，表示主机可能受到影响，如访问恶意 URL 或动态 DNS 域。 |
| 参考 | 检测到可以在聚合中用于确定可疑活动的事件；每个事件对于自己并不一定很重要。 |

## 隧道检测日志

隧道检测日志类似于隧道会话的流量日志，用于显示非加密隧道会话的条目。为了防止重复计数，防火墙只保存流量日志中的内部流，并将隧道会话发送至隧道检测日志。隧道检测日志条目包括接收时间（接收日志的日期和时间）、隧道 ID、监控标记、会话 ID、应用于隧道会话的安全规则、会话中的字节数、父会话 ID（用于隧道会话的会话 ID）、源地址、源用户和源区域、目标地址、目标用户和目标区域。

一旦启用 *PAN-OS 10.0* 中引入的解密日志，防火墙会将 *HTTP/2* 日志作为隧道检测日志发送（禁用解密日志后，*HTTP/2* 日志将作为流量日志发送），因此，必须检查隧道检测日志，而不是 *HTTP/2* 事件的流量日志。在这种情况下，还必须启用隧道内容检测以获取 *HTTP/2* 流量的 *App-ID*。

单击“详细日志”视图查看条目的详细信息，例如使用的隧道协议以及指示隧道内容是否被检测的标志。只有具有父会话的会话才会设置隧道已检测标志，意味着会话处于隧道与隧道之间（两级封装）。隧道的第一个外部标头将不会设置隧道已检测标志。

## 配置日志

配置日志显示防火墙配置的更改。每个条目均包括日期和时间、管理员用户名、从管理员进行更改的 IP 地址、客户端类型（Web、CLI 或 Panorama）、执行的命令类型、命令状态（成功还是失败）、配置路径以及更改前后的值。

## 系统日志

系统日志显示防火墙上各个系统事件的条目。每个条目均包括日期和时间、事件严重性和事件说明。下表概述了 Syslog 严重性级别：有关系统日志消息及其对应安全级别的部分列表，请参阅系统日志参考。

| 严重性级别 | 说明 |
| --- | --- |
| 关键 | 硬件故障，包括高可用性 (HA) 故障转移和链接故障。 |
| 高 | 严重问题，包括与外部设备（例如 LDAP 和 RADIUS 服务器）断开连接。 |
| 中 | 中级通知，例如抗病毒软件包升级。 |


© 2019 Palo Alto Networks, Inc.

| 严重性级别 | 说明 |
| --- | --- |
| 低 | 不太严重的通知，例如用户密码更改。 |
| 参考 | 登录/注销、管理员名称或密码更改、任何配置更改以及其他严重性级别未涵盖的所有其他事件。 |

## HIP 匹配日志

GlobalProtect 主机信息配置文件 (HIP) 匹配可让您收集有关访问您的网络的终端设备安全状态的信息（例如是否启用了磁盘加密）。防火墙可根据您定义的基于 HIP 的安全规则允许或拒绝对特定主机的访问。HIP 匹配日志显示与针对规则配置的 HIP 对象或 HIP 配置文件相匹配的流量。

## GlobalProtect 日志

GlobalProtect 日志显示以下与 GlobalProtect 相关的日志：

- GlobalProtect 系统日志。

  GlobalProtect 身份验证事件日志保留在 **Monitor**（监控）> **Logs**（日志）> **System**（系统）中，但是，GlobalProtect 日志的 **Auth Method**（身份验证方法）列显示登录时使用的身份验证方法。
- LSVPN/卫星事件。
- GlobalProtect 门户和网关日志。
- 无客户端 VPN 日志。

## IP 标记日志

IP 标记日志显示源 IP 地址在防火墙上注册或取消注册的方法和时间，以及防火墙应用到地址的标记类型。此外，各日志条目显示配置的超时（如已配置）和 IP 地址到标记映射信息的源，如 User-ID 代理 VM 信息源和自动标记。更多信息，请参阅如何动态注册 IP 地址和标记。

## User-ID 日志

User-ID日志显示 IP 地址到用户名映射的信息和 身份验证时间戳，如映射信息的来源和用户进行身份验证的时间。您可以使用这些信息帮助排除 User-ID 和身份验证问题。例如，如果防火墙为用户应用错误的策略规则，则您可以查看日志以验证是否已将该用户映射到正确的 IP 地址以及组关联是否正确。

## 解密日志

解密日志默认显示失败的 TLS 握手条目，也可以显示成功的 TLS 握手条目，但前提是您已在解密策略中启用此功能。如果启用成功握手条目，确保您具有该日志的系统资源（日志空间）。

解密日志包含的信息量很大，有助于您 排除故障并监视解密，然后解决问题。您可以在日志中启用 62 列不同类型的信息，您可以选择任何单个日志（，放大镜），然后在单独的详细信息视图中查看详细信息。您可以查看证书、密码套件和错误信息，包括：主题通用名称、颁发机构通用名称、根通用名称、根状态、证书密钥类型和大小、证书开始和结束日期、证书序列号、证书指纹、TLS 版本、密钥交换算法、加密算法、协商的 EC 曲线、身份验证算法、SNI、代理类型、错误信息（密码、HSM、资源、恢复、协议、功能、证书、版本）以及错误索引（通过查询以了解更多错误信息的代码）。

## 警报日志

警报是防火墙生成的消息，其中将指明超出事件类型所配置阈值的特定类型事件（如加密、解密故障等）发生的次数。要启动警报和配置警报阈值，选择 **Device**（设备）> **Log Settings**（日志设置），并编辑警报设置。



© 2019 Palo Alto Networks, Inc.

生成警报时，防火墙将创建警报日志，并打开系统警报对话框以显示警报。**Close**（关闭）此对话框后，您可随时通过单击 Web 界面底部的 **Alarms**（警报）( ) 将其重新打开。要防止防火墙自动打开针对特定警报的对话框，在“未确认的警报”列表中选择该警报，并 **Acknowledge**（确认）该警报。

## 身份验证日志

身份验证日志显示有关当最终用户尝试访问由身份验证策略规则控制访问的网络资源时发生的身份验证事件的信息。您可以使用此信息帮助排除访问问题，并根据需要调整身份验证策略。结合关联对象，您还可以使用身份验证日志识别网络中的可疑活动（如暴力攻击）。

或者，您可以将身份验证规则配置为日志超时事件。这些超时与用户只需要对资源进行一次身份验证但可以重复访问的时间段相关。查看有关超时的信息有助于您确定是否以及如何进行调整（有关详细信息，请参阅身份验证时间戳）。

系统日志记录与 *GlobalProtect* 以及管理员访问 *Web* 界面相关的身份验证事件。

## 统一日志

统一日志是单个视图中显示的“Traffic（流量）”、“Threat（威胁）”、“URL Filtering（URL 筛选）”、“WildFire Submissions（WildFire 提交）”和“Data Filtering（数据筛选）”日志中的条目。统一日志视图使您能够调查和筛选同一位置的不同日志类型中的最新条目，而不是单独通过各个日志类型进行搜索。单击筛选区域中的“Effective Queries（有效查询）”( )，以选择哪种日志类型将显示统一日志视图中的条目。

统一日志视图仅显示您有权查看的日志中的条目。例如，没有权限查看 WildFire Submissions（WildFire 提交）日志的管理员在查看统一日志时，将无法看见 WildFire Submissions（WildFire 提交）日志条目。管理角色类型定义这些权限。

当您在 *AutoFocus* 中设置远程搜索以在防火墙上执行针对性搜索时，搜索结果显示在统一日志视图中。

# 查看日志

可用列表方式查看防火墙上的不同日志类型。防火墙本地存储所有日志文件，并默认自动生成“Configuration and System（配置和系统）”日志。要了解有关可触发其他类型日志的条目创建的安全规则的更多信息，请参阅日志类型和严重性级别。

要配置防火墙以将日志作为 syslog 消息、电子邮件通知或简单网络管理协议 (SNMP) 陷阱转发，使用外部服务进行监控。

STEP 1 | 选择要查看的日志类型。

1. 选择 **Monitor**（监视器）> **Logs**（日志）。
2. 从列表中选择日志类型。

防火墙仅显示您有权查看的日志。例如，如果您的管理帐户没有权限查看“*WildFire Submissions*（*WildFire* 提交）”日志，当您访问日志页面时，防火墙不显示该日志类型。管理角色类型 定义权限。

STEP 2 | （可选）自定义日志列显示。

1. 单击任意列标题右侧的箭头，然后选择 **Columns**（列）。
2. 从列表中选择要显示的列。日志自动更新，以匹配您的选择。

STEP 3 | 查看有关日志条目的其他详细信息。

- 单击特定日志条目的小望远镜 ( )。详细日志视图包含更多有关会话的源和目标的信息，以及与该日志条目相关的会话列表的信息。


© 2019 Palo Alto Networks, Inc.

- （仅威胁日志）单击条目旁边的 访问威胁的本地数据包捕获。要启用本地数据包捕获，请参阅 执行数据包捕获。
- （流量、威胁、URL 筛选、WildFire 提交、数据筛选和统一日志）查看日志条目的 AutoFocus 威胁数据。
  1. 启用 AutoFocus 威胁情报。

     启用 *Panorama* 中的 *AutoFocus*，以查看所有 *Panorama* 日志条目的 *AutoFocus* 威胁数据，包括未连接到 *AutoFocus* 和/或运行 *PAN-OS 7.0* 及更早版本的防火墙中的威胁数据（*Panorama* > *Setup*（设置）> *Management*（管理）> *AutoFocus*）。
  2. 将鼠标悬停在 IP 地址、URL、用户代理、威胁名称（子类型：仅病毒和 WildFire 病毒）、文件名或 SHA-256 哈希上。
  3. 单击下拉列表 () 并选择 **AutoFocus**。
  4. 内容交付网络基础架构。

后续步骤...

- 筛选日志。
- 导出日志。
- 配置日志存储配额和过期期限。

# 筛选日志

每个日志均有一个筛选区域，可在其中设置日志条目显示的条件。筛选日志的能力有助于将重心放在防火墙上拥有特定属性或特性的事件。按与各个日志条目关联的构建筛选日志。

例如，通过规则 UUID 筛选，可更容易找到您想要定位的特定规则，即便是在许多名称类似的规则之中。如果您的规则集很大，并包含许多规则，可使用规则的 UUID 作为筛选器突出显示您需要找到的特殊规则，而无需在逐页浏览结果。



STEP 1 | （仅统一日志）选择要包括在统一日志显示中的日志类型。

1. 单击有效查询 ()。
2. 从列表中选择一个或多个日志类型（**traffic**（流量）、**threat**（威胁）、**url**、**data**（数据）和 **wildfire**）。
3. 单击 **OK**（确定）。统一日志更新，以仅显示所选日志类型中的条目。

STEP 2 | 将筛选器添加到筛选器字段中。

如果构件的值与运算符（如 *has* 或 *in* 等）相匹配，请将该值放入引号内，以免造成语法错误。例如，如果要按目标国家/地区进行筛选，且将 *IN* 用作指定 *INDIA*（印度）的值，请以 ***( dstloc eq "IN" )*** 形式输入筛选程序。

- 单击一个或多个构件（例如与流量和攻击者 IP 地址关联的应用程序类型）。例如，单击源 **10.0.0.25** 和日志条目的应用程序 **web-browsing**（**web** 浏览），以仅显示日志中包含这两个构件的条目（AND 搜索）。
- 要指定需添加到筛选器字段的构件，单击“Add Filter（添加筛选器）”()。
- 要添加之前保存的筛选器，单击 Load Filter（加载筛选器）()。

STEP 3 | 将筛选器应用于日志。

单击“Apply Filter（应用筛选器）”()。日志将刷新，以仅显示与当前筛选器匹配的日志条目。

STEP 4 | （可选）保存频繁使用的筛选器。



© 2019 Palo Alto Networks, Inc.

1. 单击“Save Filter（保存筛选器）”( )。
2. 输入筛选器的 **Name**（名称）。
3. 单击 **OK**（确定）。您可单击“Load Filter（加载筛选器）”( ) 以查看已保存的筛选器。

后续步骤...

- 查看日志。
- 导出日志。

## 导出日志

您可将一个日志类型的内容导出到逗号分隔值 (CSV) 格式的报告。默认情况下，该报告可最多包含 2,000 行日志条目。

STEP 1 | 设置行数，以在报告中显示。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑“日志记录和报告设置”。
2. 单击 **Log Export and Reporting**（日志导出和报告）选项卡。
3. 编辑 **Max Rows in CSV Export**（**CSV** 导出中的最大行数）（最多 1048576 行）。
4. 单击 **OK**（确定）。

STEP 2 | 下载日志。

1. 单击“Export to CSV（导出为 CSV）”( ).将出现一个显示下载状态的进度条。
2. 下载完成后，单击 **Download file**（下载文件）将日志副本保存到您的本地文件夹。有关已下载日志的列标题的说明，请参阅 Syslog 字段说明。

后续步骤...

计划将日志导出至 SCP 或 FTP 服务器。

## 配置日志存储配额和过期期限

防火墙会自动删除超过期限的日志。当防火墙到达日志类型的存储配额时，它会自动删除该类型的旧日志，从而腾出空间，即便您没有设置过期期限也是如此。



如果您希望手动删除日志，请选择 *Device*（设备）> *Log Settings*（日志设置），然后在“管理日志”部分中单击链接，按类型清除日志。

STEP 1 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑“日志记录和报告设置”。

STEP 2 | 选择 **Log Storage**（日志存储）并输入各个日志类型的 **Quota (%)**（配额 **(%)**）。当您更改百分比值时，对话框将会刷新，以显示相应的绝对值（配额 GB/MB 列）。

STEP 3 | 输入每种日志类型的 **Max Days**（最大天数）（过期期限），范围为 1-2,000。默认情况下，该字段留空，这意味着日志永不过期。



防火墙在高可用性 *(HA)* 对之间同步过期期限。因为只有主动的高可用性对才会生成日志，被动的对等设备没有可删除的日志，除非发生了故障转移，并且它开始生成日志。

STEP 4 | 单击 **OK**（确定）和 **Commit**（提交）。


© 2019 Palo Alto Networks, Inc.

# 计划将日志导出至 SCP 或 FTP 服务器

您可以计划将流量、威胁、URL 筛选、数据筛选、HIP 匹配和 WildFire 提交日志导出至 Secure Copy (SCP) 服务器或文件传输协议 (FTP) 服务器。应为要导出的每种日志类型执行以下操作。



您可以从 CLI 使用 Secure Copy (SCP) 命令，将完整的日志数据库导出至 *SCP* 服务器，再将其导入另一个防火墙。由于日志数据库过大，无法在以下平台上导出或导入，它们不支持以下选项：*PA-7000* 系列防火墙（所有 *PAN-OS* 版本）、运行 *Panorama 6.0* 或更新版本的 *Panorama* 虚拟设备，以及 *Panorama M* 系列设备（所有 *Panorama* 版本）。

STEP 1 | 选择 **Device**（设备）> **Scheduled Log Export**（计划日志导出），然后单击 **Add**（添加）。

STEP 2 | 输入计划日志导出的 **Name**（名称）并 **Enable**（启用）。

STEP 3 | 选择要导出的 **Log Type**（日志类型）。

STEP 4 | 选择每天 **Scheduled Export Start Time**（计划导出开始时间）。可以选择 24 小时制时间 (00:00 - 23:59)，增量为 15 分钟。

STEP 5 | 选择用于导出日志的 **Protocol**（协议）：**SCP**（安全）或 **FTP**。

STEP 6 | 输入服务器的 **Hostname**（主机名）或 IP 地址。

STEP 7 | 输入 **Port**（端口）号。默认情况下，FTP 使用端口 21，SCP 使用端口 22。

STEP 8 | 输入用于保存导出的日志的 **Path**（路径）或目录。

STEP 9 | 输入用于访问服务器的 **Username**（用户名）和 **Password**（密码）（并 **Confirm Password**（确认密码））。

STEP 10 | （仅适用于 FTP）如果您希望使用 FTP 被动模式（在该模式中，防火墙发起与 FTP 服务器的数据连接）请选中 **Enable FTP Passive Mode**（启用 **FTP** 被动模式）。默认情况下，防火墙使用 FTP 主动模式，由 FTP 服务器发起与防火墙的数据连接。请根据 FTP 服务器支持情况和网络要求来选择模式。

STEP 11 | （仅 SCP）单击 **Test SCP server connection**（测试 **SCP** 服务器连接）。在建立连接之前，防火墙必须接受 SCP 服务器的主机密钥。



如果使用 *Panorama* 模板配置日志导出计划，必须在将模板配置提交到防火墙后执行此步骤。在提交模板后，登录到每个防火墙，打开日志导出计划，然后单击 *Test SCP server connection*（测试 *SCP* 服务器连接）。

STEP 12 | 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 监控阻止列表

防火墙可以通过两种方式将 IP 地址放置于阻止列表中：

- 根据规则配置漏洞保护配置文件以阻止 IP 连接，将配置文件应用于区域中应用的安全策略。
- 使用保护操作和分类的 DoS 保护配置文件配置 DoS 保护策略规则，指定每秒允许的最大连接速率。当传入数据包与 DoS 保护策略匹配并超出最大速率时，如果您已指定阻止期限和分类的策略规则以包含源 IP 地址，则防火墙将违规的源 IP 地址放置于阻止列表中。

在上述情况下，在这些数据包使用 CPU 或数据包缓冲区资源之前，防火墙会自动阻止硬件中的流量。如果攻击流量超过硬件的阻止能力，则防火墙会使用软件中的 IP 阻止机制阻止流量。

防火墙根据漏洞保护配置文件或 DoS 保护策略规则自动创建一个硬件阻止列表条目；来自该规则的源地址是硬件阻止列表中的源 IP 地址。

在类型列表中指示硬件 (hw) 或软件 (sw) 是否阻止阻止列表中的条目。屏幕底部将显示：

- 防火墙支持的阻止 IP 地址数量中的 **Total Blocked IPs**（总阻止 **IP**）计数。
- 防火墙使用的阻止列表百分比。

要查看阻止列表上地址的详细信息，请将鼠标悬停在源 IP 地址上，然后单击向下箭头链接。点击 Who Is 链接，显示网络解决方案 Who Is 功能，提供有关地址的信息。

有关配置漏洞保护配置文件的更多信息，请参阅自定义暴力签名的操作和触发条件。有关阻止列表和 DoS 保护配置文件的更多信息，请参阅针对新会话的泛滥攻击配置 DoS 保护。



© 2019 Palo Alto Networks, Inc.

# 查看和管理报告

防火墙上的报告功能可用于保持网络上的脉冲，验证策略，以及集中精力维护网络安全以确保用户的安全和网络使用效率。


- 报告类型
- 查看报告
- 配置报告的过期期限和运行时间
- 禁用预定义的报告
- 自定义报告
- 生成定制报告
- 生成 Botnet 报告
- 生成 SaaS 应用程序使用情况报告
- 管理 PDF 摘要报告
- 生成用户/组活动报告
- 管理报告组
- 计划通过电子邮件传递的报告
- 管理报告存储容量


## 报告类型

防火墙可以包含可直接使用的预定义报告，您也可以创建符合指定数据和可执行的任务的需求的定制报告，或组合预定义和定制报告来编译您所需的信息。防火墙提供以下报告类型：

- 预定义报告 — 可让您快速查看网络上的通信的摘要。预定义报告分为四种类型 — 应用程序、通信、威胁和 URL 筛选。请参阅查看报告。
- 用户或组活动报告 — 可让您计划或创建特定用户或用户组的应用程序使用和 URL 活动的按需报告。此报告包括 URL 类别和针对单个用户计算的预计浏览时间。请参阅生成用户/组活动报告。
- 定制报告 — 通过筛选条件和要包括的列，创建和计划显示您想查看的确切信息的定制报告。您也可以包括查询生成器来更具体地展开报告数据。请参阅生成定制报告。
- **PDF** 摘要报告 — 可将威胁、应用程序、趋势、通信和 URL 筛选类别的最多 18 个预定义或定制报告/图表聚合到一个 PDF 文档中。请参阅管理 PDF 摘要报告。
- **Botnet** 报告可让您使用基于行为的机制来识别网络中可能感染 Botnet 的主机。请参阅生成 Botnet 报告。
- 报告组 — 可将自定义和预定义报告组合成报告组并编译成一个 PDF 文档，然后通过电子邮件将此文档发送给一个或多个收件人。请参阅管理报告组。

可以按照需求和重复计划生成报告，并计划通过电子邮件交付这些报告。

## 查看报告

防火墙提供它每天生成的超过 40 个预定义报告。您可以直接在防火墙上查看这些报告。还可以创建定制报告和摘要报告。

系统将分配大约 200 MB 的空间用于在防火墙上保存报告。此限值仅可重新配置用于 PA-7000 系列和 PA-5200 系列防火墙。对于其他防火墙型号，您可以配置报告的过期期限和运行时间运行防火墙在超过期限后删除报告。请记住，当防火墙到达其存储限制时，它会自动删除旧报告，从而腾出空间，即便您没有设置过期期限也是如此。节省防火墙上的系统资源的另一种方式是禁用预定义的报告。要长期保存报告，您可以导出报告（按照以下说明）或计划通过电子邮件传递的报告。



与其他报告不同，您不能将用户/组活动报告保存在防火墙上。您必须根据需求生成用户/组活动报告或计划通过电子邮件传送这些报告。



© 2019 Palo Alto Networks, Inc.

STEP 1 | (仅限 VM-50、VM-50 Lite 和 PA-200 防火墙）启用生成预定义报告。

*VM-50、VM-50 Lite* 和 *PA-200* 防火墙默认禁用预定义报告，以节省资源。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 **Logging and Reporting**（日志记录和报告）。
2. 选择 **Pre-Defined Reports**（预定义报告），然后启用（勾选）**Pre-Defined Reports**（预定义报告）。
3. 勾选（启用）您要生成的预定义报告，然后单击 **OK**（确定）
4. **Commit**（提交）配置更改。
5. 访问防火墙 CLI 以启用预定义报告。

   从 Panorama™ 管理服务器推送本地预定义报告和预定义报告需执行此步骤。

```
admin> debug predefined-default enable
```

STEP 2 | 选择 监视器 > 报告.

报告在页面右侧被分成以下几个部分（类型）：**Custom Reports**（定制报告）、**Application Reports**（应用程序报告）、**Traffic Reports**（流量报告）、**Threat Reports**（威胁报告）、**URL Filtering Reports**（URL 筛选报告）和 **PDF Summary Reports**（PDF 摘要报告）。

STEP 3 | 选择要查看的报告。然后报告页面显示前一天的报告。

要查看其它日期的报告，在页面底部的日历中选择一个日期，并选择一个报告。如果在另一个部分中选择报告，则选择的日期重置为当前日期。

STEP 4 | 要脱机查看报告，可以将报告导出为 PDF、CSV 或 XML 格式。单击页面底部的 **Export to PDF**（导出为 **PDF**）、**Export to CSV**（导出为 **CSV**）或 **Export to XML**（导出为 **XML**），然后打印或保存文件。

## 配置报告的过期期限和运行时间

过期期限和运行时间是全局设置，适用于所有报告类型。运行新报告后，防火墙会自动删除超过过期期限的报告。

STEP 1 | 请选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），编辑“日志记录和报告设置”，然后选择 **Log Export and Reporting**（日志导出和报告）选项卡。

STEP 2 | 将 **Report Runtime**（报告运行时间）设置为 24 小时制时间表中的一个小时（默认为 02:00；范围为 00:00 [午夜] 至 23:00）。

STEP 3 | 输入 **Report Expiration Period**（报告过期期限）天数，范围为 1-2,000。

您不能更改防火墙为保存报告分配的存储空间：预定义为大约 *200 MB*。请记住，当防火墙到达其存储限制时，它会自动删除旧报告，从而腾出空间，即便您没有设置 *Report Expiration Period*（报告过期期限）也是如此。

STEP 4 | 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

## 禁用预定义的报告

防火墙包含大约 40 份每天自动生成的预定义报告。如果您不使用部分或所有这些报告，可以在防火墙上禁用所选报告并节省系统资源。

请确保没有报告组或 PDF 摘要报告包括您将禁用的预定义报告。否则，防火墙将提供没有任何数据的 PDF 摘要报告或报告组。

STEP 1 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑“日志记录和报告设置”。

STEP 2 | 选择 **Pre-Defined Reports**（预定义报告）选项卡，并清除您要禁用的每种报告。要禁用所有预定义报告，请单击 **Deselect All**（取消全选）。

STEP 3 | 单击 **OK**（确定）和 **Commit**（提交）。

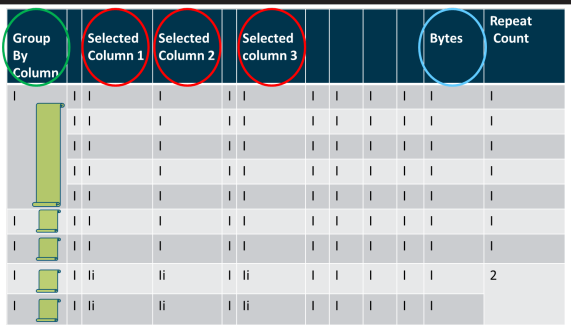
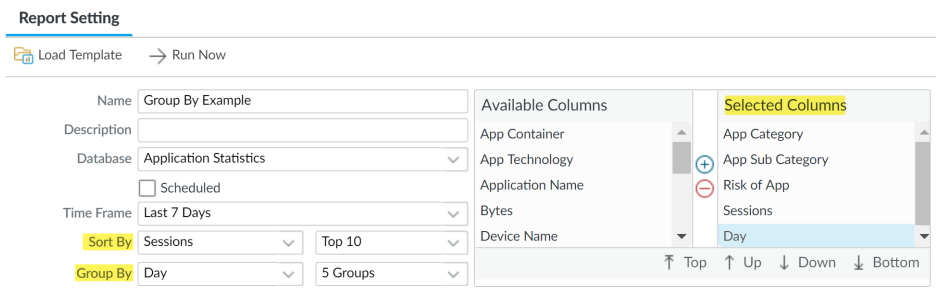
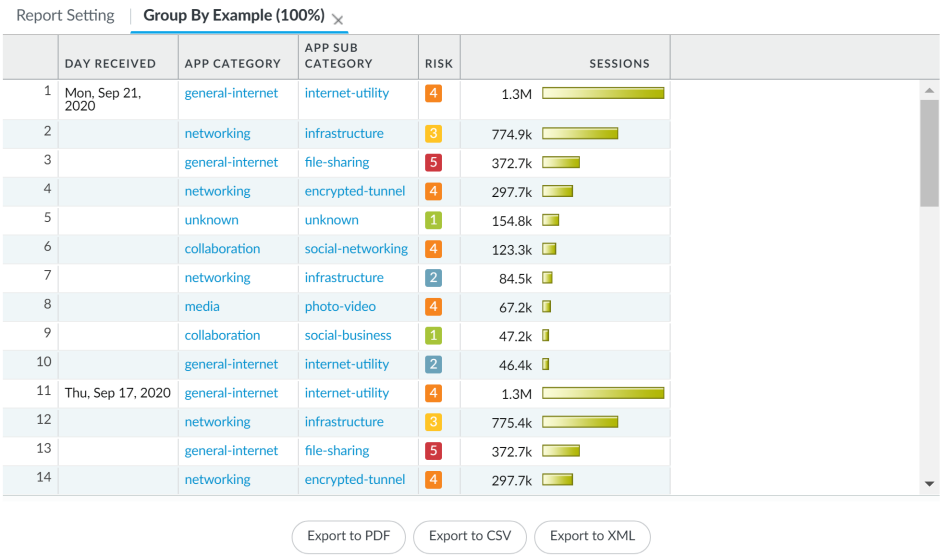
## 自定义报告

要创建所需自定义报告，您必须考虑要检索和分析的属性或关键信息（例如威胁）以及对信息进行分类的最佳方法（例如按规则 UUID 分组），以便于查看应用于每个威胁类型的规则。这种考虑将引导您在定制报告中作出以下选择：

| 选择 | 说明 |
| --- | --- |
| 数据库 | 您可以根据以下数据库类型之一准备报告：<br>• 摘要数据库 — 这些数据库可用于应用程序统计信息、流量、威胁、URL 筛选和隧道检测日志。防火墙每间隔 15 分钟聚合一次详细日志。为了在生成报告时启用更快的响应时间，防火墙会将数据进行聚合：重复会话将被分组并递增重复次数，并且一些属性（列）将从摘要中排除。<br>• 详细日志 — 这些数据库逐条列出日志并列出每个日志条目的所有属性（列）。<br>基于详细日志的报告需要花费更多的时间来运行，除非确实需要，否则不建议使用。 |
| 属性 | 是指要用作匹配条件的列。属性是指可在报告中选择的列。在 **Available Columns**（可用列）列表中，可以添加匹配数据和聚合详细信息的选择条件（**Selected Columns**（所选列））。 |
| 排序方式/分组方式 | **Sort By**（排序方式）和 **Group By**（分组方式）标准可让您对报告中的数据进行排序/分组；可用的排序和分组属性基于所选数据源的变化而变化。<br>“Sort By（排序方式）”选项指定用于聚合的属性。如果您未选择排序属性，报告则会返回前面 N 个结果，不进行任何聚合。<br>‘分组方式”选项可让您选择属性作为对数据进行分组的锚点；报告中的所有数据随后将显示于前 5 组、前 10 组、前 25 组或前 50 组数据集合中。例如，当您选择“小时”作为“分组”选项，并想要 24 小时时间段内的前 25 组，则报告的结果将在 24 小时内每小时生成。报告中的首列会显示小时，下一组列显示剩下的所选报告列。 |
| | 下例介绍生成报告时 **Selected Columns**（所选列）和 **Sort By**（排序方式）/**Group By**（分组方式）标准如何同时工作： |



© 2019 Palo Alto Networks, Inc.

| 选择 | 说明 |
| --- | --- |
| |  <br>带红色圆圈的列（如上）表示所选列，是指与用来生成报告相匹配的属性。分析数据源的每个日志条目，并将其与上述列相匹配。如果多个会话拥有与所选列相同的值，则会聚合这些会话，并递增重复次数（或会话）。<br>带蓝色圆圈的列表示所选的排序顺序。指定排序顺序（**Sort By**（排序方式））时，会根据所选属性对数据进行排序（和聚合）。<br>带绿色圆圈的列表示选择的 **Group By**（分组方式），将充当报告的锚点。**Group By**（分组方式）列将用作前 N 组数据的筛选匹配条件。然后，对于前 N 组数据中的每组数据，报告会枚举所有其他所选列的值。 |
| | 例如，如果报告包含以下选择：<br>  <br>输出显示如下：<br>  |



© 2019 Palo Alto Networks, Inc.

| 选择 | 说明 |
| --- | --- |
| | 根据 **Day**（天数）锚定报告，且根据 **Sessions**（会话）对报告进行排序。报告列出 **Last 7 Days**（过去 **7** 天）时间范围内流量最大的五天（**5 Groups**（5 组））的数据。通过所选列（**App Category**（应用程序类别）、**App Subcategory**（应用程序子类别）和 **Risk**（风险））每日的 **Top 5**（前 5 个）会话来枚举数据。 |
| **Time frame** | 是指要分析的数据的日期范围。您可以定义一个自定义范围或从过去 15 分钟至过去 30 天内选择一个时间期限。报告可以按需运行或按计划每日或每周运行。 |
| 查询生成器 | 查询生成器可让您定义指定查询以便进一步调整所选的属性。它可让您使用运算符 **and** 和 **or** 和匹配条件来查看报告中想要查看的数据，然后包含或排除与报告中的查询相匹配或相反的数据。查询让您能够在报告中生成信息的重点排序规则。 |

## 生成定制报告

您可以配置防火墙立即（按需）或按计划（每天晚上）生成的自定义报告。要了解可用于创建所需自定义报告的选项，请参阅自定义报告。

防火墙生成计划的自定义报告之后，如果您修改其配置以更改未来输出，则可能会使得该报告过去的结果无效。如果需要修改计划报告配置，最佳实践是创建一个新报告。

STEP 1 | 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告）。

STEP 2 | 单击 **Add**（添加），然后输入报告的 **Name**（名称）。

要使报告基于预定义模板，请单击 *Load Template*（加载模板）并选择模板。然后，可编辑所选模板并将其保存为定制报告。

STEP 3 | 选择用于报告的 **Database**（数据库）。

每次创建自定义报告时，都会自动创建一个日志查看报告。此报告将显示用于构建定制报告的日志。日志查看报告使用与定制报告相同的名称，但会附加短语（日志查看）到报告名称后。

创建报告组时，可以包含定制报告和日志查看报告。有关详细信息，请参阅管理报告组。

STEP 4 | 选中 **Scheduled**（已计划）复选框，可每晚运行报告。然后，可在侧边的 **Reports**（报告）列中查看报告。

STEP 5 | 定义筛选条件。选择 **Time Frame**（时间框架）、**Sort By**（排序）顺序、**Group By**（分组方式）首选项，然后选择报告中必须显示的列。

STEP 6 | （可选）如果希望进一步调整选择标准，请选择 **Query Builder**（查询生成器）属性。要构建报告查询，请指定以下项，并单击添加。根据需要重复操作以构造完整查询。

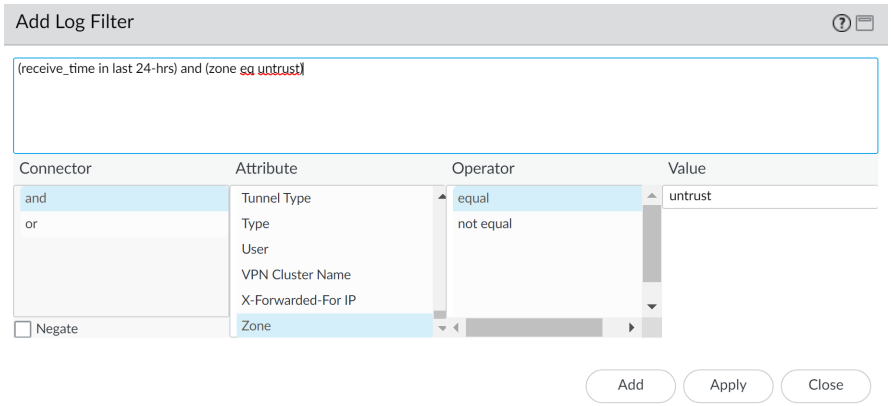
- **Connector**（连接器）— 选择要放在正在添加的表达式前面的连接符 (and/or)。
- **Negate**（求反）— 选中此复选框将查询解释为否定。例如，如果您选择匹配过去 24 小时内和/或源自不可信区域的条目，选中“求反”选项会导致匹配不是过去 24 小时内的和/或不是源自不可信区域的条目。
- 属性- 选择数据元素。可用选项取决于数据库的选择。
- 运算符- 选择用于确定属性是否应用的标准（比如 = ）。可用选项取决于数据库的选择。



© 2019 Palo Alto Networks, Inc.

- 值- 指定要匹配的属性值。

例如，下图（基于 `Traffic Log` 数据库）显示的查询将列出在过去 24 小时内收到并且来自不信任区域的通信日志条目。

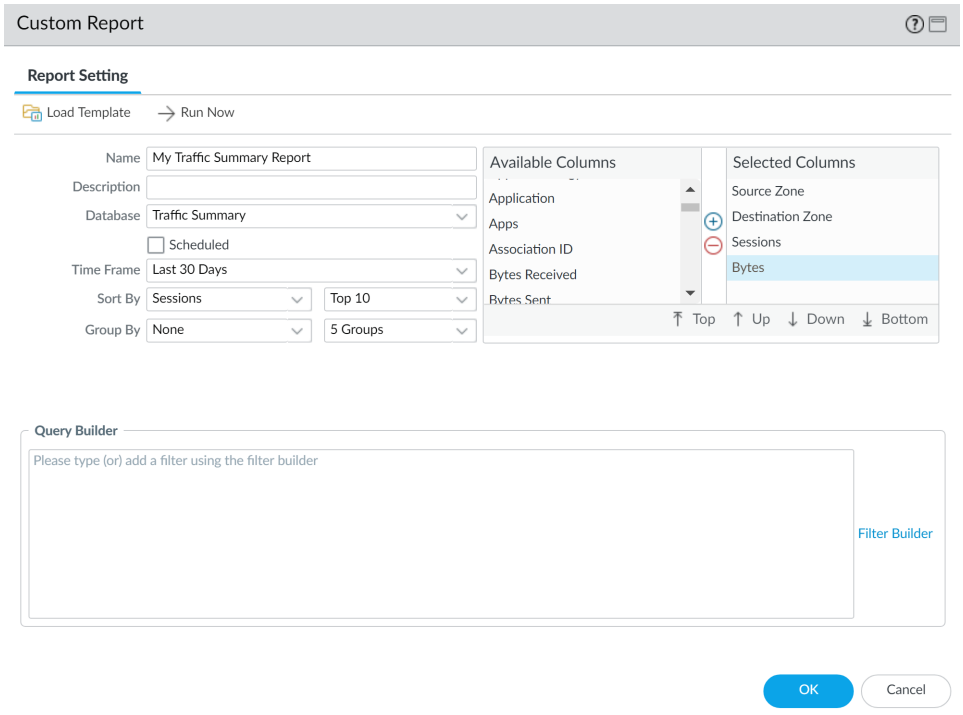



STEP 7 | 要测试报告设置，请选择 **Run Now**（立即运行）。根据需要修改设置，以更改报告中显示的信息。

STEP 8 | 单击 **OK**（确定）保存定制报告。

定制报告示例

如果设置一个简单报告并在其中使用过去 30 天的通信摘要数据库，然后按照前 10 个会话（这些会话按照星期几被分为 5 组）对数据进行排序。应将定制报告设置成：




并且，报告的 PDF 输出应显示如下：



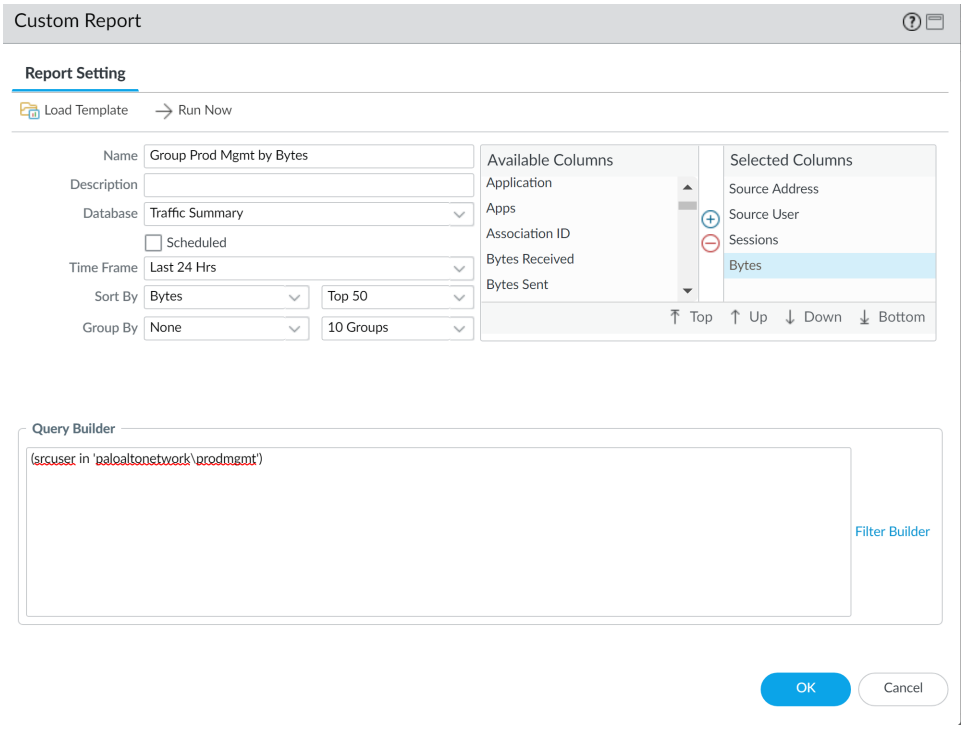
© 2019 Palo Alto Networks, Inc.

# My Traffic Summary Report

ca1demo.paloaltonetworks.com : 2016/01/25 10:34:39 - 2016/02/24 10:34:38

| Source Zone | Destination Zone | App Category | Application | Sessions | Bytes |
|---|---|---|---|---|---|
| Tap | Tap | general-internet | web-browsing | 74.54 M | 2.47 T |
| Tap | Tap | networking | dns | 52.03 M | 28.93 G |
| Tap | Tap | networking | ssl | 18.01 M | 678.13 G |
| Tap | Tap | general-internet | bittorrent | 9.80 M | 1.62 T |
| Tap | Tap | general-internet | google-base | 4.48 M | 168.99 G |
| Tap | Tap | unknown | insufficient-data | 4.45 M | 31.30 G |
| Tap | Tap | collaboration | facebook-base | 4.09 M | 99.14 G |
| Tap | Tap | networking | ntp | 4.07 M | 3.29 G |
| Tap | Tap | collaboration | blackboard | 2.84 M | 186 G |
| Tap | Tap | collaboration | smtp | 1.92 M | 172.57 G |
| Tap | Tap | networking | icmp | 1.36 M | 320.49 M |
| Tap | Tap | general-internet | gnutella | 1.17 M | 17.84 G |
| Tap | Tap | collaboration | myspace-base | 1.10 M | 35.22 G |
| Tap | Tap | general-internet | ping | 1.06 M | 86.21 M |
| Tap | Tap | general-internet | flash | 1.01 M | 168.14 G |

如果希望使用查询生成器来生成显示用户组中网络资源占用排名靠前的用户的定制报告，则应将报告设置成：




此自定义报告应显示产品管理用户组中排列靠前的用户（根据字节数进行排序）。

## 生成 Botnet 报告

Botnet 报告可让您使用启发式和基于行为的机制，识别网络中可能感染恶意软件或 Botnet 的主机。为了评估 Botnet 活动和受感染主机，防火墙将威胁、URL 和数据筛选日志中的用户和网络数据数据与 PAN-DB 中的恶意软件 URL、已知动态 DNS 域提供程序、最近 30 天内注册域的列表关联起来。您可以配置报告，以识别访问这些站点的主机，以及与中继聊天 (IRC) 服务器通信的主机，或使用了未知应用程序的主机。恶意软件通常使用动态 DNS 来避开 IP 阻止，而 IRC 服务器通常使用 Bot 实现自动功能。



© 2019 Palo Alto Networks, Inc.

防火墙需要威胁预防和 *URL* 筛选许可证，才能使用 *Botnet* 报告。您可以使用自动关联引擎，基于除 *Botnet* 报告使用的指标之外的其他指标来监控可疑活动。但是，*Botnet* 是唯一将新注册域作为指标的工具。

- 配置 Botnet 报告
- 解释 Botnet 报告输出

## 配置 *Botnet* 报告

您可以计划运行 Botnet 报告，也可按需要运行该报告。防火墙每隔 24 小时生成计划的 Botnet 报告，因为基于行为的检测需要在该时间范围内关联多个日志上的流量。

STEP 1 | 定义表示可能存在 Botnet 活动的流量类型。

1. 选择 **Monitor**（监控）> **Botnet**，并单击位于页面右侧的 **Configuration**（配置）。
2. **Enable**（启用）并定义报告将包括的每种类型的 HTTP 流量的 **Count**（计数）。

   **Count**（计数）值表示每种流量类型的事件必须发生的最小次数，只有达到这个次数，报告才会列出相关主机，它们具有较高的置信度评分（感染 Botnet 的可能性较高）。如果事件次数小于 **Count**（计数），报告将会显示较低的置信度评分，而对于某些流量类型，则不会显示主机的条目。例如，如果您将 **Malware URL Visit**（恶意软件 **URL** 访问）的 **Count**（计数）设置为 3，则访问已知恶意 URL 三次或更多的主机的评分将高于访问不足三次的主机。有关详细信息，请参阅解释 Botnet 报告输出。
3. 定义阈值，该值将决定报告是否包括与涉及未知 TCP 或未知 UDP 应用程序的流量相关的主机。
4. 选中 **IRC** 复选框可包括涉及 IRC 服务器的流量。
5. 单击 **OK**（确定）以保存报告配置。

STEP 2 | 计划运行报告或按需运行报告。

1. 单击页面右侧的 **Report Setting**（报告设置）。
2. 在 **Test Run Time Frame**（测试运行时间范围）下拉菜单中选择报告的时间间隔。
3. 选中 **No. of Rows**（行数）以将其包含于报告内。
4. （可选）**Add**（添加）到查询生成器可按属性（如源/目标 IP 地址、用户或区域）筛选报告输出。

   例如，如果预先知道从 IP 地址 10.3.3.15 发出的流量不包含潜在的 botnet 活动，添加 **`not (addr.src in 10.0.1.35)`** 作为查询，将该主机排除在报告输出范围之外。有关详细信息，请参阅解释 Botnet 报告输出。
5. 选择 **Scheduled**（计划）可每天运行报告，单击 **Run Now**（立即运行）可立即运行报告。
6. 单击 **OK**（确定）和 **Commit**（提交）。

## 解释 *Botnet* 报告输出

在 Botnet 报告中，对于与您在配置报告时定义为可疑的流量相关联的每台主机，都会显示一行。对于每台主机，该报告显示从 1 至 5 的置信度评分，表示发生 Botnet 感染的可能性，其中 5 表示最高可能性。该评分与威胁严重性级别相对应：1 是参考，2 是低，3 是中，4 是高，5 是危急。防火墙评分的依据为：

- 流量类型 — 某些 HTTP 流量类型涉及 Botnet 活动的可能性更高。例如，报告为访问已知恶意 URL 的主机分配的置信度要高于浏览 IP 域而非 URL 的主机，前提是假定您将这些活动都定义为可疑的。
- 事件次数 — 与次数更多的可疑事件相关联的主机将具有更高的置信度评分，这要基于您在配置 Botnet 报告时定义的阈值（**Count**（计数）值）。
- 可执行文件下载 — 对于下载可执行文件的主机，报告会分配更高的置信度评分。可执行文件导致很多感染，当与其他类型的可疑流量结合在一起时，它能够帮助您区分对受影响主机的调查的优先级。

查看报告输出时，您可能发现防火墙用于评估 Botnet 活动的源（例如 PAN-DB 中的恶意软件 URL 列表）存在缺漏。还可能发现这些源会识别您认为安全的流量。为了弥补这两种情况，您可在配置 Botnet 报告时添加查询筛选器。


© 2019 Palo Alto Networks, Inc.

# 生成 SaaS 应用程序使用情况报告

SaaS 应用程序使用情况报告（PDF 版）由两部分组成，允许您按风险和约束状态轻松搜索 SaaS 应用程序活动。约束应用程序是指您正式同意在您网络上使用的应用程序。SaaS 应用程序是 **Objects**（对象）> **Applications**（应用程序）下应用程序详细信息页面中具有特性“SaaS=yes”的应用程序，所有其他应用程序均被视为非 SaaS。要指示您已对某个 SaaS 或非 SaaS 应用程序执行约束操作，必须对其使用名为“约束”的预定义标记。防火墙和 Panorama 会将任何没有此预定义标记的应用程序视为其使用不受网络约束的应用程序。

- 报告第一部分展示的是报告期间在您网络上获得的 SaaS 应用程序的主要发现，对约束应用程序和未约束应用程序的比较结果，并按使用情况、合规性和数据传输基于约束状态列出顶级应用程序。为了帮助您识别和浏览高风险应用程序的使用范围，本报告中具有风险特征的应用程序部分列出了具有下列不利托管特征的 SaaS 应用程序：已获取证书、过去出现数据泄露、支持基于 IP 的限制、财务可行性以及服务条款。此外，还可以查看约束与未约束 Saas 应用程序在下列各个方面的对比：您网络上使用的应用程序总数、这些应用程序消耗的带宽、使用这些应用程序的用户数、使用最大数量的 Saas 应用程序的高级用户组、以及通过约束和未约束 Saas 应用程序来传输最大数据量的高级用户组。报告的这个第一部分还根据使用的最大应用程序数量、用户数量和各个应用程序子类别中传输的数据量，强调了按照顺序列示的热门 SaaS 应用程序子类别。
- 报告的第二部分主要讲述报告第一部分中列示的各个应用程序子类别的 SaaS 和非 SaaS 应用程序的详细浏览信息。对于子类别中的各个应用程序，它还包括有关传输数据最多的那批用户、被阻挡或警告最多的文件类型以及各个应用程序的热门威胁的相关信息。此外，报告的这一部分记录了防火墙提交的用于 WildFire 分析的各个应用程序样本，以及用于确定良性和恶意的样本数量。

使用此报告中的见解整合关键业务级的已批准 SaaS 应用程序列表，并实施策略以控制会构成不必要的恶意软件传播和数据泄露风险的非约束风险应用程序。

预定义 *SaaS* 应用程序使用情况报告仍作为每日查看报告，列示给定日期您的网络上运行最多的前 *100* 位 *SaaS* 应用程序（是指具有 *SaaS* 应用程序特征 *SaaS=yes* 的应用程序）。此报告无法查看已指定为约束的应用程序，但可以查看您网络上正在使用的所有 *SaaS* 应用程序。

STEP 1 | 将您批准在您的网络上使用的应用程序标记为“Sanctioned（约束）”。

要生成正确且可供参考的报告，您需要在带有多个虚拟系统防火墙中以及属于 *Panorama* 设备组的防火墙之间对受约束的应用程序进行统一标记。如果同一个应用程序在一个虚拟系统中标记为受约束，而未在其他虚拟系统中进行同样的标记，或在 *Panorama* 上，如果一个应用程序在父设备组中标记为未约束，而在子设备组中标记为约束（或反之），则 *SaaS* 应用程序使用报告将应用程序报告为部分约束，将会产生重叠的结果。

示例：如果 Box 在虚拟系统 1 上受约束，而 Google Drive 在虚拟系统 2 上受约束，则虚拟系统 1 中的 Google Drive 用户将被计为未约束 SaaS 应用程序的用户，而虚拟系统 2 中的 Box 用户将被计为未约束 SaaS 应用程序的用户。报告中的关键发现将突出显示，一共在含约束和未约束应用程序的网络上发现两个唯一的 SaaS 应用程序。

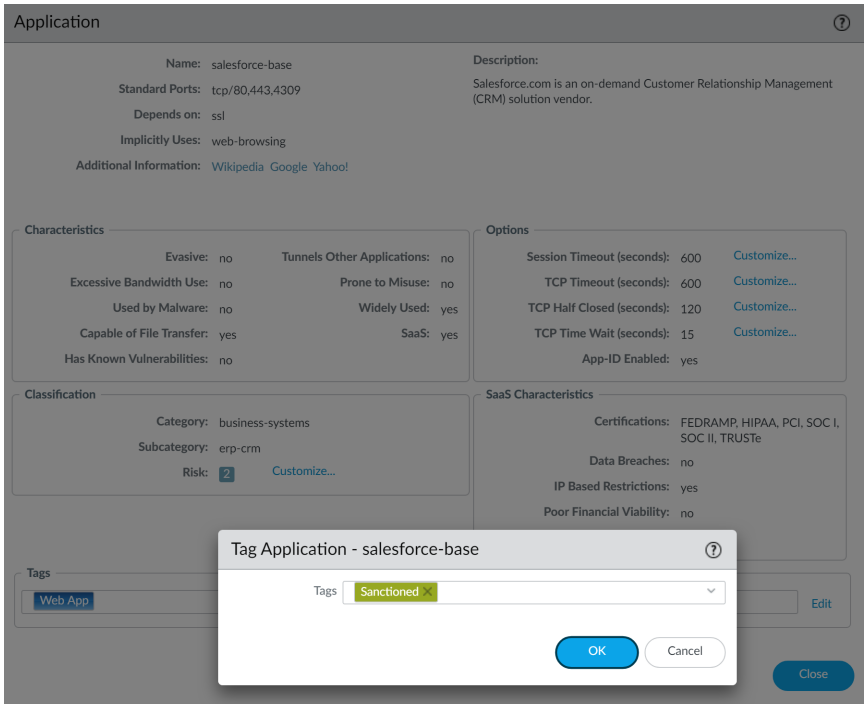
1. 选择**Objects**（对象）> **Applications**（应用程序）。
2. 单击应用程序的 **Name**（名称）编辑应用程序，并在“Tag（标记）”部分中选择 **Edit**（编辑）。
3. 从 **Tags**（标记）下拉列表中选择 **Sanctioned**（约束）。

   必须使用预定义 **Sanctioned**（约束）标记（ 

）。如果使用任何其他标记指示您约束了一个应用程序，防火墙将无法识别该标记，报告会不准确。



© 2019 Palo Alto Networks, Inc.




4. 单击 **OK**（确定）和 **Close**（关闭）以退出所有打开的对话框。

STEP 2 | 配置 SaaS 应用程序使用情况报告。

1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **SaaS Application Usage**（**SaaS** 应用程序使用）。
2. 单击 **Add**（添加），输入一个 **Name**（名称），并选择报告的 **Time Period**（时间段）（默认为 **Last 7 Days**（过去 7 天））。

   默认情况下，报告包括有关热门 *SaaS* 和非 *SaaS* 应用程序自子类别的详细信息，这些信息会使报告的页数和文件大小变大。如要减小文件大小并将页数限制为 *10* 页，清除 *Include detailed application category information in report*（在报告中包括详细的应用程序类别信息）复选框。
3. 选择是否要使报告 **Include logs from**（包含来自...的日志）：

   在 *PAN-OS 10.0.2* 以及更高版本中，根据 *Cortex* 数据湖中日志生成的报告仅支持包括 *Selected Zone*（选定区域）的日志。

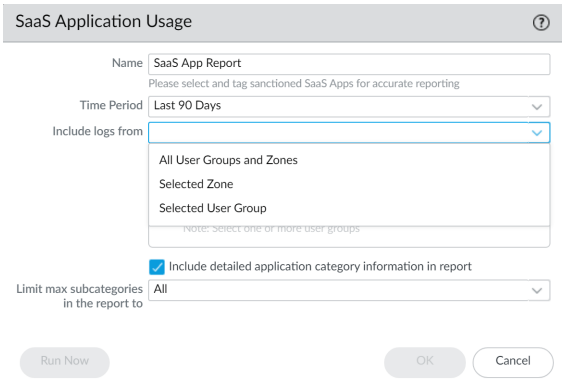
   - **All User Groups and Zones**（所有用户组和区域）— 报告包括有关日志中可用的所有安全区域和用户组的数据。

     如果要在报告中包括特定的用户组，请选择 **Include user group information in the report**（在报告中包括用户组信息），然后单击 **manage groups**（管理组）链接以选择要包括的组。添加范围必须介于 1 至 25，以便防火墙或 Panorama 可以筛选所选用户组的日志。如果已选择要包括的组，报告会将所有用户组聚合到一个名为“其他”的组中。
   - **Selected Zone**（选中区域）— 报告筛选指定安全区域的数据，并仅包括该区域的数据。

     如果要在报告中包括特定的用户组，请选择 **Include user group information in the report**（在报告中包括用户组信息），然后单击 **manage groups for selected zone**（选中区域管理组）链接以选择要包括在报告中的区域内的用户组。添加范围必须介于 1 至 25，以便防火墙或 Panorama 可以筛选安全区域内所选用户组的日志。如果已选择要包括的组，报告会将所有用户组聚合到一个名为“其他”的组中。


© 2019 Palo Alto Networks, Inc.

- **Selected User Group**（选中用户组）— 报告仅筛选指定用户组的数据，并且仅包括所选用户组的 SaaS 应用程序使用信息。




4. 选择是否要将报告中的所有应用程序子类别（默认值）或 **Limit the max subcategories in the report**（将报告中的最大子类别限制）为前 10、15、20 或 25 类（默认为所有子类别）。
5. 单击 **Run Now**（立即运行），生成最近 7 天和最后 30 天时间段内的按需报告。确保您的浏览器禁用弹出窗口屏蔽，因为报告会在新标签页中打开。
6. 单击 **OK**（确定）保存更改。

STEP 3 | 计划通过电子邮件传递的报告。

最近 90 天的报告必须安排通过电子邮件传递。

在 PA-220R 和 PA-800 系列防火墙中，SaaS 应用程序使用报告不会在电子邮件中以 PDF 附件的形式发送。而是通过电子邮件为您提供一个链接，您必须单击它以在 Web 浏览器中打开报告。

# 管理 PDF 摘要报告

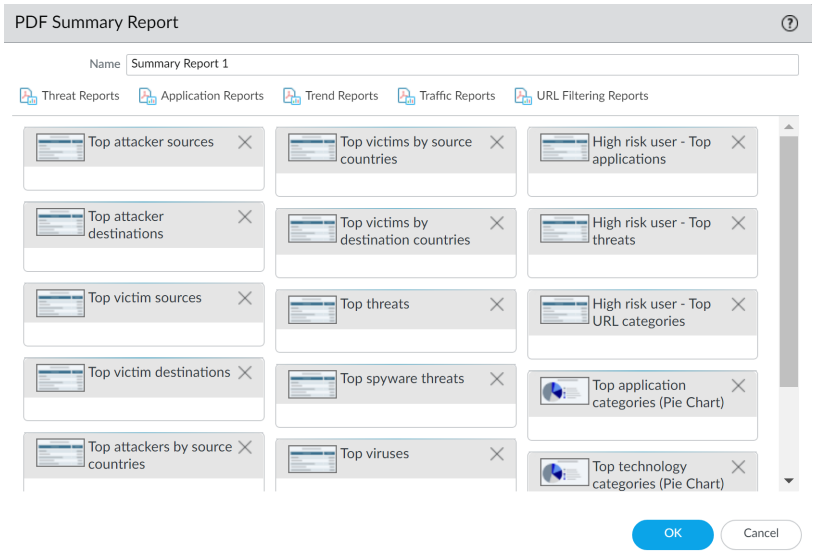
PDF 摘要报告包含根据现有报告编译的信息，此信息基于每个类别中前 5 条数据（而不是前 50 条数据）。它们还包含在其他报告中没有的趋势图表。

STEP 1 | 设置 **PDF Summary Report**（**PDF** 摘要报告）。

1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **Manage PDF Summary**（管理 **PDF** 摘要）。
2. 单击 **Add**（添加），然后输入报告的 **Name**（名称）。
3. 使用每个报告组的下拉列表，然后选择一个或多个元素以设计 PDF 摘要报告。最多可包括 18 个报告元素。



© 2019 Palo Alto Networks, Inc.




在 *PDF* 摘要报告的预定义小部件列中，选择 *Top Threats*（最高威胁）显示为 `top-attacks`。

- 要从报告中删除元素，请单击 **x** 图标或从相应报告组的下拉列表中清除此选择。
- 要重新排列报告，请将元素图标拖放至报告的其他区域。

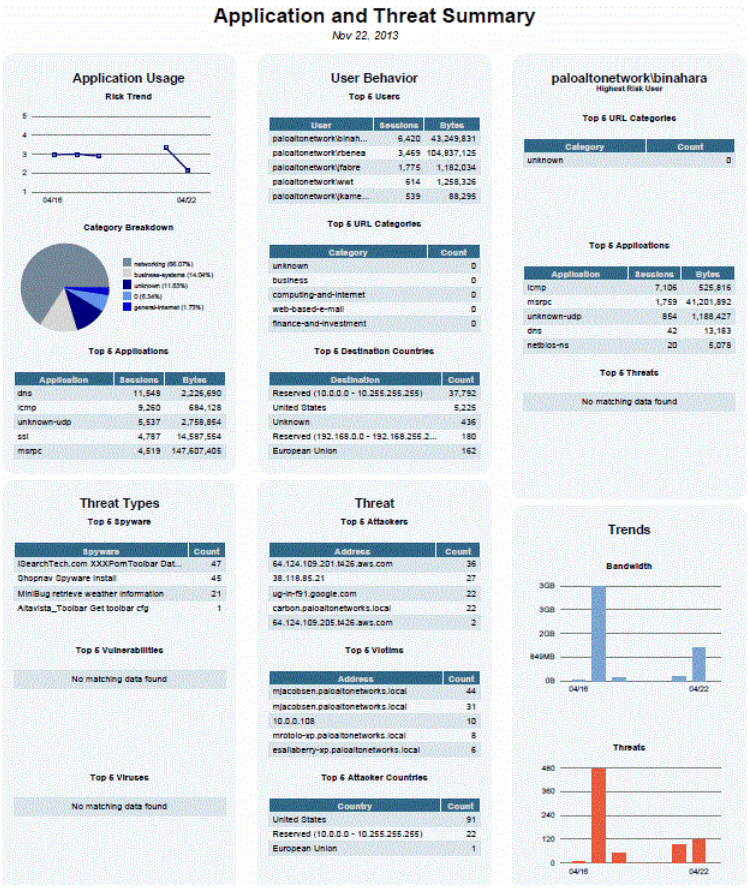
4. 单击 **OK**（确定）以保存报告。
5. **Commit**（提交）更改。

STEP 2 | 查看报告。

要下载并查看 PDF 摘要报告，请参阅查看报告。



© 2019 Palo Alto Networks, Inc.




下列摘要部分是指以下 *PDF* 摘要报告元素：

- ***Top 5 Attacks***（前 ***5*** 大攻击）— 是指 *Top threats*（最高威胁）元素。
- ***Top 5 Threats***（前 ***5*** 大威胁）— 是指 *High risk user - Top threats*（高风险用户 - 最高威胁）元素。
- 最高威胁报告 — 是指来自*Top threats*（最高威胁）元素的完整威胁列表。

# 生成用户/组活动报告

用户/组活动报告概括单个用户或用户组的 Web 活动。这两类报告所含信息相同，但有两个例外：**Browsing Summary by URL Category**（**URL** 类别的浏览摘要）和 **Browse time calculations**（浏览时间计算），它们仅包含在用户活动报告中。

您必须在防火墙上配置User-ID，以访问用户和用户组的列表。

STEP 1 | 为用户/组活动报告配置浏览时间和日志数。

仅在您希望更改默认值时才需要。

1. 请选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），编辑“日志记录和报告设置”，然后选择 **Log Export and Reporting**（日志导出和报告）选项卡。
2. 在 **Max Rows in User Activity Report**（用户活动报告中的最大行数）中，输入详细用户活动报告支持的最大行数（范围为 1-1048576，默认值为 5000）。它将决定报告分析的日志数。
3. 输入以秒为单位的 **Average Browse Time**（平均浏览时间），也就是您预测用户浏览某个网页应该花费的时间（范围为 0-300，默认值为 60）。平均浏览时间过后发出的任何请求将被视为新的浏览活动。计算使用仅记录用户访问页面（记录在 URL 筛选日志中）作为依据，并忽略在第一次请求时间



© 2019 Palo Alto Networks, Inc.

（开始时间）与平均浏览时间之间加载的任何新网页。例如，如果您将 **Average Browse Time**（平均浏览时间）设置为 2 分钟，那么用户打开一个网页并查看该页面 5 分钟，则此页面的浏览时间仍然为 2 分钟。由于防火墙无法确定用户查看给定页面的时间，因此系统将执行此操作。平均浏览时间计算将忽略类别为“Web 通告”和“内容分发网络”的两类站点。

4. 在 **Page Load Threshold**（页面加载阈值）中，输入预测在页面上加载页面元素所需的时间，以秒为单位（默认值为 20）。第一次页面加载和页面加载阈值之间发出的任何请求都会被假定为页面元素。在页面加载阈值之外发生的任何请求都会被假定为用户单击页面内链接的操作。
5. 单击 **OK**（确定）保存更改。

STEP 2 | 生成用户/组活动报告。

1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **User Activity Report**（用户活动报告）。
2. 单击 **Add**（添加），然后输入报告的 **Name**（名称）。
3. 创建此报告：
   - 用户活动报告 — 选择 **User**（用户）并输入用户的 **Username**（用户名）或 **IP address**（**IP** 地址）（IPv4 或 IPv6）。
   - 组活动报告 — 选择**Group**（组）并选择用户组的 **Group Name**（组名称）。
4. 选择报告的 **Time Period**（时间段）。
5. （可选）选中 **Include Detailed Browsing**（包括详细浏览）复选框（默认清除），在报告中包括详细的 URL 日志。

   详细的浏览活动信息可能包含所选用户或用户组的大量日志（成千上万条日志），从而使报告非常大。
6. 要按需运行报告，请单击 **Run Now**（立即运行）。
7. 要保存报告配置，请单击 **OK**（确定）。您可将用户/组活动报告的输出保存在防火墙上。要计划通过电子邮件传送报告，请参见计划通过电子邮件传递的报告。

# 管理报告组

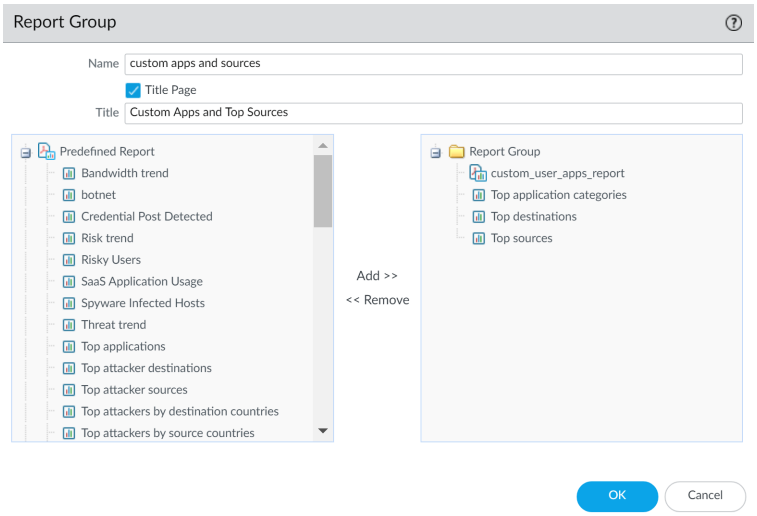
报告组允许您创建报告集合，系统可以对此集合进行编译并将其作为单个聚合 PDF 报告来发送，该报告中包含可选的标题页和所有成员报告。

设置报告组。

必须设置 **Report Group**（报告组）以通过电子邮件发送报告。

1. 创建电子邮件服务器配置文件。
2. 定义 **Report Group**（报告组）。报告组可将预定义报告、PDF 摘要报告、定制报告和日志查看报告编译成单个 PDF 报告。
   1. 选择 **Monitor**（监视器）> **Report Group**（报告组）。
   2. 单击 **Add**（添加），然后输入报告组的 **Name**（名称）。
   3. （可选）选择 **Title Page**（标题页面）并为 PDF 输出添加 **Title**（标题）。
   4. 在左列中选择报告并单击 **Add**（添加）可将每个报告移动到右侧的报告组。


© 2019 Palo Alto Networks, Inc.




**Log View**（日志查看）报告是每次创建自定义报告时自动创建的一种报告类型，它与此自定义报告使用相同的名称。此报告将显示用于构建此定制报告内容的日志。

要包含日志查看数据，请在创建报告组时，将自定义报告添加到 **Custom Reports**（定制报告）列表下，然后通过从 **Log View**（日志查看）列表中选择匹配的报告名称来添加日志查看报告。此报告将包含定制报告数据和用于创建定制报告的日志数据。

5. 单击 **OK**（确定）以保存设置。
6. 要使用报告组，请参阅计划通过电子邮件传递的报告。

# 计划通过电子邮件传递的报告

可计划每天或在每周的特定日期通过电子邮件传递报告。凌晨 2:00 开始执行已计划的报告，生成所有已计划的报告后，才能开始通过电子邮件传递报告。

STEP 1 | 选择 **Monitor**（监控）> **PDF Reports**（PDF 报告）> **Email Scheduler**（电子邮件计划程序）并单击 **Add**（添加）。

STEP 2 | 输入标识计划的 **Name**（名称）。

STEP 3 | 选择通过电子邮件传递的 **Report Group**（报告组）。要设置报告组，请参阅管理报告组。

STEP 4 | 对于 **Email Profile**（电子邮件配置文件），选择用于传递报告的电子邮件服务器配置文件，或单击 **Email Profile**（电子邮件配置文件）链接以创建电子邮件服务器配置文件。

STEP 5 | 在 **Recurrence**（重复）下列列表中选择生成和发送报告频率。

STEP 6 | **Override Email Addresses**（替代收件人电子邮件）字段可让您只将此报告发送给指定收件人。当您将收件人添加到该字段时，防火墙不会向电子邮件服务器配置文件中配置的收件人发送报告。出现下述情况时使用此选项：此报告只是为了引起某人的注意（此人不是管理员，也不是电子邮件服务器配置文件中定义的收件人）。

STEP 7 | 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 管理报告存储容量

默认情况下，防火墙包含 200MB 的专属存储空间，用于存储防火墙生成的报告。在某些实例中，尤其对于 PA-7000 系列和 PA-5200 系列防火墙，您可能需要可用的增加报告存储空间容量，以成功生成新报告。

STEP 1 | 访问防火墙 CLI。

STEP 2 | 确认防火墙当前的报告存储容量：

命令输出以字节显示报告存储空间大小。对于此程序，防火墙具有默认的 200MB 报告存储容量。

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

209715200
```

STEP 3 | 确认您在防火墙上有足够的存储空间，以分配用于不断扩大的报告存储容量：

```
admin> show system disk-space
```

```
admin@ISP-CONDOR-B(active)> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        12G  8.9G  2.0G  83% /
none            7.9G   52K  7.9G   1% /dev
/dev/sda5        16G  8.5G  5.9G  59% /opt/pancfg
/dev/sda6        12G  5.8G  5.0G  54% /opt/panrepo
tmpfs           7.9G  247M  7.6G   4% /dev/shm
/dev/sda8        22G  8.7G   12G  43% /opt/panlogs
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```

STEP 4 | 根据需要增加报告存储容量：

例如，我们将报告存储空间增加至 1 GB。

```
admin> request report-storage-size set size <0-4>
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size set size 1

cfg.report-storage-size-gb: 1
```

STEP 5 | 确认报告存储容量以增加至之前步骤中设定的容量：

```
admin> request report-storage-size show
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

1073741824
```



© 2019 Palo Alto Networks, Inc.

# 查看策略规则使用情况

因为您的环境和安全需求会随时间发生变化，因此，请查看安全、NAT、QoS、基于策略的转发 (PBF)、解密、隧道检测、应用程序覆盖、身份验证或 DoS 保护规则与流量匹配的次数，以帮助及时更新您的防火墙策略。要阻止攻击者利用过度配置访问，例如当服务器退役时，或您不再需要临时访问服务时，请使用策略规则命中次数数据以标识和删除未使用的规则。

您还可以借助策略规则使用数据来验证规则添加和规则更改功能，并在规则使用时监控时间框架。例如，当您将基于端口的规则迁移到基于应用的规则时，应在基于端口的规则上创建一个基于应用的规则，并检查与基于端口的规则相匹配的任何流量。迁移后，命中次数数据将帮助您确定基于端口的规则是否可以安全删除，方法是通过确认流量是否与基于应用的规则（而非基于端口的规则）相匹配。您可以通过策略规则命中次数确定规则是否对访问实施有效。

您可以重置规则点击数数据以验证现有规则，或衡量指定时间段内的规则使用情况。策略规则命中次数数据并非存储在防火墙或 Panorama 上，因此，您重置（清除）命中次数后，该数据不再可用。

筛选策略规则库后，管理员可以直接从策略优化器中执行删除、禁用、启用和标记策略规则等操作。例如，您可以筛选未使用的规则，然后进行标记以供检查，从而确定是否需要在规则库中安全删除这些规则，或是将其继续保留在规则库中。通过让管理员直接从策略优化器执行操作，您可以减少用于进一步协助简化规则生命周期管理工作的管理开销，确保您的防火墙不会过度配置。

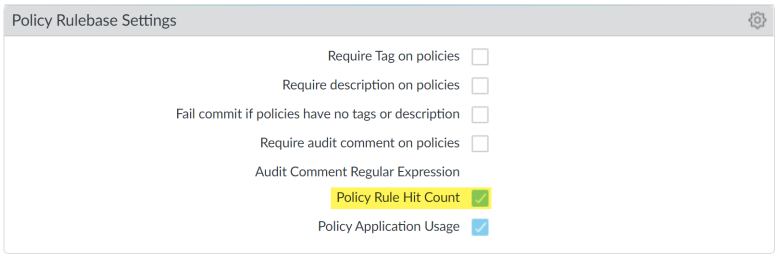
高可用性 *(HA)* 部署中防火墙上的规则命中次数数据并不会同步，因此，您需要登录每个防火墙以查看每个防火墙的策略规则命中次数数据，或使用 *Panorama* 查看 *HA* 防火墙对等设备上的信息。

使用安全策略规则优化确定首先迁移或清除的规则时，策略规则使用数据可能会很有用。

STEP 1 | 启动 Web 界面。

STEP 2 | 验证 **Policy Rule Hit Count**（策略规则命中次数）是否启用。

1. 导航至策略规则库设置（**Device**（设备）> **Setup**（设置）> **Management**（管理））。
2. 验证 **Policy Rule Hit Count**（策略规则命中次数）是否启用。




STEP 3 | 选择 **Policies**（策略）。

STEP 4 | 查看每个策略规则的策略规则使用情况：

- 点击数— 流量与策略规则中定义的标准匹配的次数。除非您手动重置或重命名规则，否则应通过重新启动、数据面板重启和升级来保留。
- 上一次点击— 流量与规则匹配的最新时间戳。
- 第一次点击— 流量与此规则匹配的第一个实例。
- 修改时间 — 最后一次修改策略规则的日期和时间。
- 创建时间 — 策略规则创建的日期和时间。



© 2019 Palo Alto Networks, Inc.

如果在 *Panorama* 运行 *PAN-OS 8.1* 且“策略规则命中次数”设置启用的情况下创建规则，则在升级到 *PAN-OS 9.0* 时，第一次命中的日期和时间将用作创建日期和时间。如果在禁用策略规则命中次数设置时在 *PAN-OS 8.1* 中创建规则，或在 *Panorama* 运行 *PAN-OS 8.0* 或更早版本时创建规则，则规则创建日期为 *Panorama* 成功升级到 *PAN-OS 9.0* 的日期和时间。

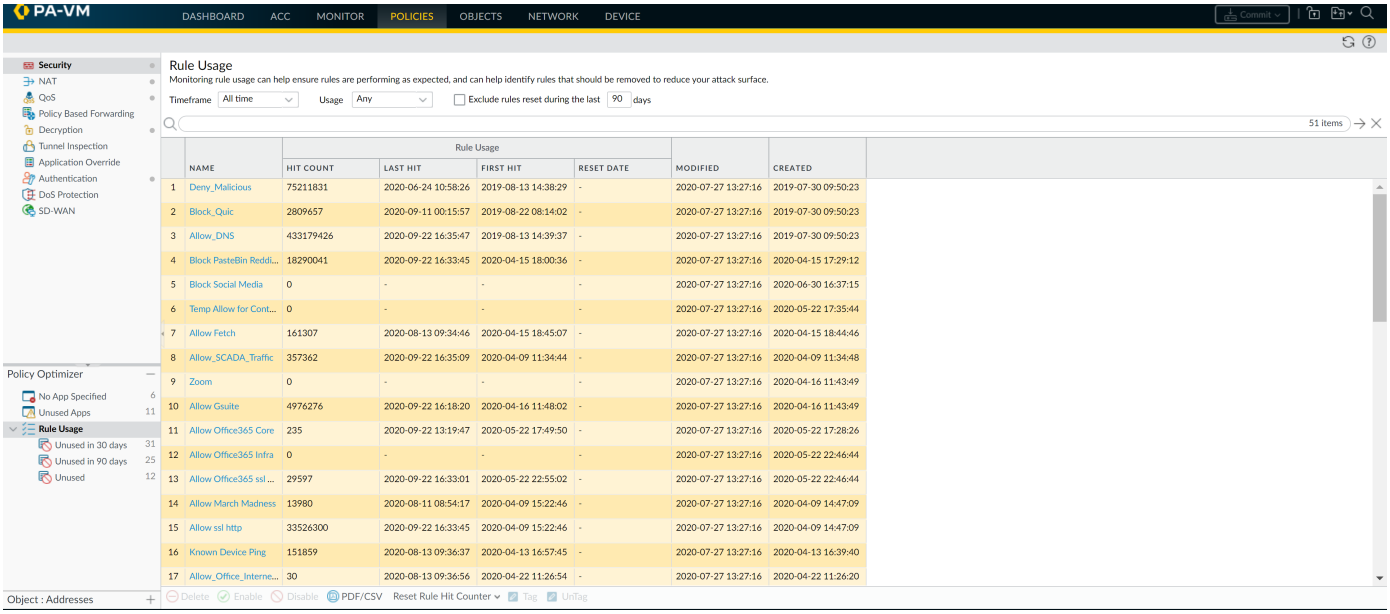
| NAME | T... | Source Z... | Source A... | Source U... | Rule Usage HIT COUNT | Rule Usage LAST HIT | Rule Usage FIRST HIT | MODIFIED | CREATED |
|---|---|---|---|---|---|---|---|---|---|
| Video | n... | a... | a... | a... | 2424328 | 2020-09-22 11:33:00 | 2019-07-30 10:12:57 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| Video Streaming | n... | a... | a... | a... | 14337228 | 2020-09-22 16:26:58 | 2019-07-30 10:12:57 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| cavenger | n... | a... | a... | a... | 321760616 | 2020-09-22 16:27:10 | 2019-07-30 10:12:57 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| Web Traffic | n... | a... | a... | a... | 1509584361 | 2020-09-22 16:27:10 | 2019-07-30 10:12:02 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |
| iperf | n... | a... | a... | a... | 5 | 2019-10-15 14:54:31 | 2019-10-11 13:08:28 | 2020-07-27 13:27:16 | 2019-07-30 09:50 |

STEP 5 | 在 Policy Optimizer（策略优化器）对话框中，查看 **Rule Usage**（规则使用情况）筛选器。

STEP 6 | 筛选选中规则库中的规则。

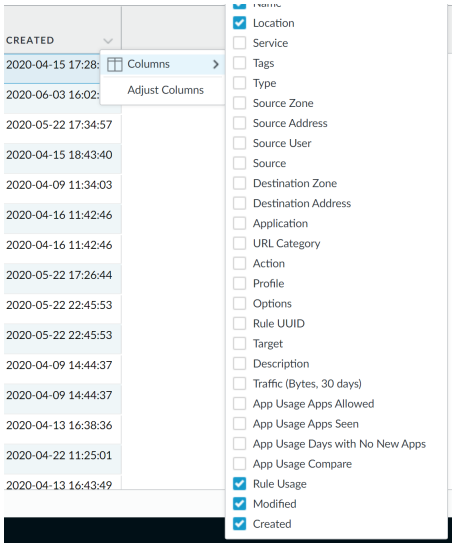
使用规则使用情况筛选器评估指定时间段内的规则使用情况。例如，筛选选定规则库中最近 *30* 天内未使用的规则。您还可以使用 *Created*（创建）和 *Modified*（修改）日期等其他规则属性评估规则使用情况，从而可以筛选出正确的规则组以供查看。使用此数据有助于您管理规则生命周期，并确定是否需要删除规则，以减小您的网络攻击面。

1. 选择想要筛选的 **Timeframe**（时间段），或指定 **Custom**（自定义）时间段。
2. 选择要筛选的规则 **Usage**（使用情况）。
3. （可选）如果已重置任何规则的规则使用情况数据，请检查排除最近 <*number of days*> 天内的规则重置，并决定何时根据规则重置以来指定的天数排除规则。筛选结果仅包含指定天数之前重置的规则。

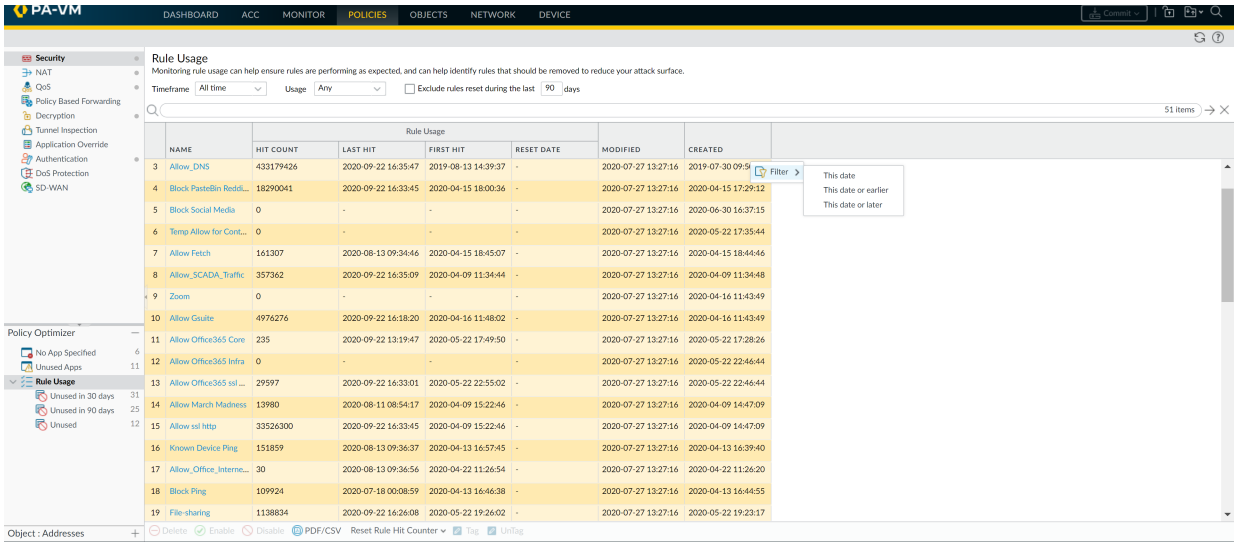



4. （可选）根据规则数据指定搜索筛选器
    1. 将光标悬停在列标题和 **Columns**（列）上。
    2. 添加想要显示或用于筛选的任何其他列。


© 2019 Palo Alto Networks, Inc.




3. 将光标悬停在想通过 **Filter**（筛选器）筛选的列数据。对于包含日期的数据，选择是否使用 **This date**（此日期）、**This date or earlier**（此日期或更早日期）或 **This date or later**（此日期或更晚日期）进行筛选。
4. **Apply Filter**（应用筛选器）()。




STEP 7 | 对一个或多个未使用的策略规则执行操作。

1. 选择一个或多个未使用的策略规则。
2. 然后执行以下操作之一：
   - **Delete**（删除）— 删除所选的一个或多个策略规则。
   - **Enable**（启用）— 启用所选的一个或多个策略规则（若已禁用）。
   - **Disable**（禁用）— 禁用所选的一个或多个策略规则（若已启用）。
   - **Tag**（标记）— 将一个或多个组标记应用于所选的一个或多个策略规则。若要标记策略规则，组标记必须已经存在。
   - **Untag**（取消标记）— 取消所选的一个或多个策略规则中的组标记。
3. **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 使用外部服务进行监控

使用外部服务监控防火墙，您能够收到有关重要事件的警报，利用专用长期存储将监控信息存档在系统上，并与第三方安全监控工具集成。以下是使用外部服务的一些常见场景：

- 有关重要系统事件或威胁的即时通知，您可以使用 SNMP 监控统计信息、将陷阱转发至 SNMP 管理器或配置电子邮件警报。
- 将基于 HTTP 的 API 请求直接发送到任何暴露 API 的第三方服务以自动执行工作流程或操作。例如，您可以转发符合定义条件的日志，以便在 ServiceNow 上创建事件票据，而不是依靠外部系统将 syslog 消息或 SNMP 陷阱转换为 HTTP 请求。您可以修改 HTTP 请求中的 URL、HTTP 标头、参数和负载，以根据防火墙日志中的属性触发操作。请参阅将日志转发到 HTTP(S) 目标。
- 要实现长期日志存储和集中式防火墙监控，您可以配置 Syslog 监控，以便将日志数据发送至 syslog 服务器。这样便可以集成第三方安全监控工具，例如 Splunk 或 ArcSight。
- 要监控穿过防火墙接口的 IP 流量的统计信息，您可以配置 NetFlow 导出，以便在 NetFlow 收集器中查看统计信息。

您可配置日志转发，将日志从防火墙直接转发至外部服务，或从防火墙转发至 Panorama，然后将 Panorama 配置为将日志转发至服务器。有关在决定将日志转发至何处时应该考虑的因素，请参阅日志转发选项。



您不能在 *Panorama* 上汇总 *NetFlow* 记录；您必须将它们直接从防火墙发送至 *NetFlow* 收集器。



© 2019 Palo Alto Networks, Inc.

# 配置日志转发

在使用多个防火墙来控制和分析网络流量的环境中，任何一个防火墙都只能为其所监控的流量显示日志和报告。因为登录到多个防火墙可使监控更加累赘，您可以将日志从所有防火墙转发到 Panorama 或外部服务，从而更有效地实现对网络活动的全局可见性。如果使用外部服务进行监控，防火墙会自动将日志转换为必要的格式：syslog 消息、SNMP 陷阱、电子邮件通知或 HTTP 有效负载，以将日志详细信息发送到 HTTP(S) 服务器。如果组织中某些团队可以通过仅监视与其操作相关的日志来提高效率，则可以根据任何日志属性（例如：威胁类型或源用户）创建转发筛选器。例如，调查恶意软件攻击的安全运营分析师可能只对类型属性设置为 WildFire 病毒的威胁日志感兴趣。



您可将日志从防火墙直接转发至外部服务，或从防火墙转发至 *Panorama*，然后将 Panorama 配置为将日志转发至服务器。有关在决定将日志转发至何处时应该考虑的因素，请参阅日志转发选项。

您可以从 CLI 使用 Secure Copy (SCP) 命令，将完整的日志数据库导出至 *SCP* 服务器，再将其导入另一个防火墙。由于日志数据库过大，无法在 *PA-7000* 系列防火墙上导出或导入，它们不支持这些选项。还可在所有平台上使用 *Web* 界面来查看和管理报告，但只能按每个日志类型，而不是整个日志数据库。

STEP 1 | 为将要接收日志信息的每种外部服务配置服务器配置文件。



您可以使用单独的配置文件，将按日志属性筛选的不同日志集发送到其他服务器。要提高可用性，请在单个配置文件中定义多个服务器。

配置以下一个或多个服务器配置文件：

- （对于 SMTP over TLS 为必要操作）如果尚未执行此操作，请为电子邮件服务器创建证书配置文件。
- 2要让 SNMP 管理器（陷阱服务器）能够解释防火墙陷阱，您必须将 Palo Alto Networks 支持的 MIB 加载至 SNMP 管理器，并在必要时进行编译。有关详细信息，请参阅 SNMP 管理软件文档。
- 如果 syslog 服务器使用客户端身份验证，则还必须5
- 配置 HTTP 服务器配置文件（请参阅将日志转发到 HTTP/S 目标）。

STEP 2 | 创建日志转发配置文件。

配置文件定义了流量、威胁、WildFire 提交、URL 筛选、数据筛选、隧道和身份验证日志的目标。

1. 选择 **Objects**（对象）> **Log Forwarding**（日志转发）并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。

   如果您希望防火墙自动为新的安全规则和区分配配置文件，请输入 **`default`**。如果您不需要默认配置文件，或者您希望覆盖现有默认配置文件，请输入一个 **Name**（名称），在将配置文件分配到安全规则和区域时，帮助您标识配置文件。

   如果不存在名为 ***`default`*** 的日志转发配置文件，则在新的安全规则（*Log Forwarding*（日志发转）字段）和新的安全区域（*Log Setting*（日志设置）字段中），配置文件选择设置为 *None*（无），但您可以更改这一选择。
3. **Add**（添加）一个或多个匹配列表配置文件。

   配置文件指定日志查询筛选器、转发目的地和自动操作（如标记）。对于每个匹配列表配置文件：

   1. 输入 **Name**（名称）以标识配置文件。
   2. 选择 **Log Type**（日志类型）。
   3. 在 **Filter**（筛选器）下拉列表中，选择 **Filter Builder**（筛选器构建器）。指定以下内容，然后 **Add**（添加）每个查询：



© 2019 Palo Alto Networks, Inc.

- **Connector**（连接器）逻辑（和/或）
- 日志 **Attribute**（属性）
- 定义包含或排除逻辑的 **Operator**（运算符）
- 用于查询匹配的属性 **Value**（值）

4. 如果想要将日志转发到日志收集器或 Panorama 管理服务器，则选中**Panorama**。
5. 对于您用于监控的每种类型的外部服务（SNMP、电子邮件、Syslog 和 HTTP），请 **Add**（添加）一个或多个服务器配置文件。

4. （可选，仅限 GlobalProtect）如果正在使用带安全策略的日志转发配置文件自动隔离使用 GlobalProtect 的设备，请选择 **Built-in Actions**（内置操作）区域中的 **Quarantine**（隔离）。
5. 单击 **OK**（确定）保存日志转发配置文件。

STEP 3 | 将日志转发配置文件分配给安全规则和网络区域。

安全、身份验证和 DoS 保护规则支持日志转发。在本示例中，将配置文件分配至安全规则。

针对想要触发日志转发的每种规则，执行以下步骤：

1. 选择 **Policies**（策略）> **Security**（安全）并编辑规则。
2. 选择 **Actions**（操作）选项卡，并选择您创建的 **Log Forwarding profile**（日志转发配置文件）。
3. 将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）或 **Group**（组），然后选择触发日志生成和转发所需的安全配置文件或 **Group Profile**（组配置文件）：
   - 威胁日志 — 流量必须匹配分配给规则的任何安全配置文件。
   - WildFire 提交日志 — 流量必须匹配分配给规则的 WildFire 分析配置文件。
4. 对于流量日志，选中 **Log At Session Start**（在会话开始时记录）和/或 **Log At Session End**（在会话结束时记录）。
5. 单击 **OK**（确定）保存规则。

STEP 4 | 配置系统、配置、关联、GlobalProtect、HIP 匹配和 User-ID 日志的目标。

*Panorama* 基于它收到的防火墙日志而非防火墙提供的聚合关联日志生成关联日志。

1. 选择**Device**（设备）> **Log Settings**（日志设置）。
2. 对于防火墙将转发的每个日志类型，请参阅步骤添加一个或多个匹配列表配置文件。

STEP 5 | （仅限 PA-7000 系列防火墙）配置日志卡接口以执行日志转发。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并单击 **Add Interface**（添加接口）。
2. 选择 **Slot**（插槽）和 **Interface Name**（接口名称）。
3. 将 **Interface Type**（接口类型）设置为 **Log Card**（日志卡）。
4. 输入 **IP Address**（IP 地址）、**Default Gateway**（默认网关）和（仅限 IPv4）**Netmask**（网络掩码）。
5. 选择 **Advanced**（高级），并指定 **Link Speed**（链接速度）、**Link Duplex**（链接双工）和 **Link State**（链接状态）。

   这些字段默认设置为 *auto*（自动），指示防火墙基于连接自动确定值。但是，针对任何连接推荐的最小 *Link Speed*（链接速度）为 *1000 (Mbps)*。

6. 单击 **OK**（确定）保存更改。

STEP 6 | 提交并验证您的更改。

1. **Commit**（提交）更改。


© 2019 Palo Alto Networks, Inc.

2. 确认您配置的日志目标收到了防火墙日志：
   - Panorama — 如果防火墙将日志转发至 Panorama 模式下的 Panorama 虚拟设备或 M 系列设备，则在 Panorama 收到日志之前，您必须配置收集器组。然后您可以验证日志转发。
   - 电子邮件服务器 — 确认指定收件人收到了以电子邮件通知形式发送的日志。
   - Syslog 服务器 — 请参阅 syslog 服务器的文档，以验证其是否能接收到 syslog 消息形式的日志。
   - SNMP 管理器 —使用 SNMP 管理器浏览 MIB 和对象 验证是否接收充当 SNMP 陷阱的日志。
   - HTTP 服务器 —将日志转发到 HTTP/S 目标。


© 2019 Palo Alto Networks, Inc.

# 配置电子邮件警报

您可为系统、配置、HIP 匹配、关联、威胁、WildFire 提交和流量日志配置电子邮件警报。您可以使用单独的配置文件，向不同服务器发送每种日志类型的电子邮件通知。要提高可用性，请在单个配置文件中定义多个服务器（最多 4 个）。



最佳做法是配置传输层安全 *(TLS)*，要求防火墙在将电子邮件中继到服务器之前采用电子邮件服务器进行身份验证。这有助于防止恶意活动，例如，可用于发送垃圾邮件或恶意软件的简单邮件传输协议 *(SMTP)* 以及可用于网络钓鱼攻击的电子邮件欺骗。

STEP 1 | （对于 SMTP over TLS 为必要操作）如果尚未执行此操作，请为电子邮件服务器创建证书配置文件。

STEP 2 | 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Email**（电子邮件）。

STEP 3 | **Add**（添加）电子邮件服务器配置文件，并输入 **Name**（名称）。

STEP 4 | 在显示的只读窗口中，**Add**（添加）电子邮件服务器，并输入 **Name**（名称）。

STEP 5 | 如果防火墙具有多个虚拟系统 (vsys)，请选择此配置文件可用的 **Location**（位置）（vsys 或 **Shared**（共享））。

STEP 6 | （可选）输入 **Email Display Name**（电子邮件显示名称）以指定电子邮件发件人字段显示的名称。

STEP 7 | 输入防火墙发送电子邮件的 **From**（发件人）电子邮件地址。

STEP 8 | 输入防火墙发送电子邮件的 **To**（收件人）电子邮件地址。

STEP 9 | （可选）如果要向第二个帐户发送电子邮件，请输入 **Additional Recipient**（其他收件人）地址。只能添加一个其他收件人。要添加多个收件人，请添加通讯组列表的电子邮件地址。

STEP 10 | 输入用于发送电子邮件的 **Email Gateway**（电子邮件网关）IP 地址或主机名。

STEP 11 | 选择用于连接到电子邮件服务器的协议 **Type**（类型）：

- **Unauthenticated SMTP**（未经身份验证的 **SMTP**）— 在未执行身份验证的情况下使用 SMTP 连接电子邮件服务器。默认 **Port**（端口）是 25，但是，您可以指定其他端口。此协议不能提供与 SMTP over TLS 相同的安全性，但是，如果选择此协议，将跳过下一步。
- **SMTP over TLS**—（推荐）使用 TLS 将要求通过身份验证才能连接到电子邮件服务器。继续进行下一步以配置 TLS 身份验证。

STEP 12 | （仅限 SMTP over TLS）将防火墙配置为使用 TLS 身份验证以连接到电子邮件服务器。

1. （可选）指定用于连接到电子邮件服务器的 **Port**（端口）（默认为 587）。
2. **TLS Version**（**TLS** 版本）— 指定 TLS 版本（**1.1** 或 **1.2**）。



*Palo Alto Networks* 强烈建议使用最新版 *TLS*。

3. 选择适用于防火墙和电子邮件服务器的 **Authentication Method**（身份验证方法）：
   - **Auto**（自动）— 允许防火墙和电子邮件服务器确定身份验证方法。
   - **Login**（登录）— 对用户名和密码使用 Base64 编码，并分别进行传输。



© 2019 Palo Alto Networks, Inc.

- **Plain**（普通）— 对用户名和密码使用 Base64 编码，并一起传输。

4. 选择电子邮件服务器执行身份验证时使用的 **Certificate Profile**（证书配置文件）。
5. 输入发送电子邮件的账户的 **Username**（用户名）和**Password**（密码），然后 **Confirm Password**（确认密码）。
6. （可选）要确认防火墙是否能成功通过电子邮件服务器进行身份验证，您可以 **Test Connection**（测试连接）。

STEP 13 | 单击 **OK**（确定）以保存电子邮件服务器配置文件。

STEP 14 | （可选）选择 **Custom Log Format**（自定义日志格式）选项卡，并自定义电子邮件的格式。有关如何为各个日志类型创建自定义格式的详细信息，请参阅常见事件格式配置指南。

STEP 15 | 为流量、威胁和 WildFire 提交日志配置电子邮件警报。

1. 请参阅创建日志转发配置文件。
    1. 选择 **Objects**（对象）> **Log Forwarding**（日志转发），单击 **Add**（添加），并输入标识配置文件的 **Name**（名称）。
    2. 针对每种日志类型及每种严重性级别或 WildFire 判定，选择电子邮件服务器配置文件并单击 **OK**（确定）。
2. 请参阅将日志转发配置文件分配给安全规则和网络区域。

STEP 16 | 为系统、配置、HIP 匹配和关联日志配置电子邮件警报。

1. 选择**Device**（设备）> **Log Settings**（日志设置）。
2. 对于系统和关联日志，请单击每种严重性级别，选择 **Email**（电子邮件）服务器配置文件，并单击 **OK**（确定）。
3. 对于配置和 HIP 匹配日志，请编辑此部分，选择 **Email**（电子邮件）服务器配置文件，并单击 **OK**（确定）。
4. 单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 使用 Syslog 进行监控

Syslog 是一个标准日志传输机制，它能够将不同供应商的不同网络设备（例如路由器、防火墙和打印机）中的日志数据聚合到中心存储库进行存档、分析和报告。Palo Alto Networks 防火墙可将它们生成的每种类型日志转发至外部 syslog 服务器。您可以使用 TCP 或 TLS（仅限 TLSv1.2）来实现安全可靠的日志转发，或者使用 UDP 进行非安全转发。

- 配置 Syslog 监控
- Syslog 字段说明

## 配置 Syslog 监控

要使用 Syslog 进行监控 Palo Alto Networks 防火墙，请创建 Syslog 服务器配置文件，并将其分配至每种日志类型的日志设置。或者，您可以配置在 syslog 消息中使用的标头格式，并启用通过 TLSv1.2 的 Syslog 客户端身份验证。

STEP 1 | 配置 Syslog 服务器配置文件。



您可以使用单独的配置文件，向不同服务器发送每种日志类型的 *syslog*。要提高可用性，请在单个配置文件中定义多个服务器（最多 *4* 个）。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Syslog**。
2. 单击 **Add**（添加），然后输入配置文件的 **Name**（名称）。
3. 如果防火墙具有多个虚拟系统 (vsys)，请选择此配置文件可用的 **Location**（位置）（vsys 或 **Shared**（共享））。
4. 对于每个 syslog 服务器，单击 **Add**（添加），并输入连接到防火墙所需的信息：
   - **Name**（名称）— 服务器配置文件的唯一名称。
   - **Syslog Server**（**Syslog** 服务器）- Syslog 服务器的 IP 地址或完全限定域名 (FQDN)。

     在已配置 *FQDN* 并使用 *UDP* 传输的情况下，如果防火墙不解析 *FQDN*，则防火墙使用 *FQDN* 的现有 *IP* 地址解析充当 *Syslog Server*（*Syslog* 服务器）地址。
   - **Transport**（传输）— 请选择**TCP**、**UDP** 或 **SSL** (TLS) 作为与 Syslog 服务器进行通信的方法。对于**SSL**，防火墙仅支持 TLSv1.2。
   - **Port**（端口）— 发送 Syslog 消息所使用的端口号（在端口 514 的默认值为 UDP）；必须在防火墙和 Syslog 服务器上使用同一端口号。
   - **Format**（格式）— 请选择要使用的 Syslog 消息格式：**BSD**（默认格式）或 **IETF**。通常来说，**BSD** 格式通过 UDP 端口发送，**IETF** 格式通过 TCP 或 SSL/TLS 发送。
   - **Facility**（工具）— 选择一个 Syslog 标准值（默认值为 **LOG_USER**），用于计算 Syslog 服务器实现中的优先级 (PRI) 字段。选择用于映射如何使用 PRI 字段管理 syslog 消息的值。
5. （可选）若要自定义防火墙发送的 Syslog 消息的格式，请选择 **Custom Log Format**（自定义日志格式）选项卡。有关如何为各个日志类型创建自定义格式的详细信息，请参阅常见事件格式配置指南。
6. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | 为流量、威胁和 WildFire 提交日志配置 syslog 转发。

1. 配置防火墙以转发日志。有关详细信息，请参阅步骤创建日志转发配置文件。
   1. 选择 **Objects**（对象）> **Log Forwarding**（日志转发），单击 **Add**（添加），并输入标识配置文件的 **Name**（名称）。
   2. 针对每种日志类型及每种严重性级别或 WildFire 判定，选择 **Syslog** 服务器配置文件并单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

2. 分配日志转发配置文件到安全策略，以触发日志生成和转发。有关详细信息，请参阅步骤将日志转发配置文件分配给安全规则和网络区域。

   1. 选择 **Policies**（策略）> **Security**（安全）并选择一条策略规则。
   2. 选择 **Actions**（操作）选项卡，并选择您创建的 **Log Forwarding profile**（日志转发配置文件）。
   3. 在 **Profile Type**（配置文件类型）下拉列表中，选择 **Profiles**（配置文件）或 **Group**（组），然后选择为触发日志生成和转发所需的安全配置文件或 **Group Profile**（组配置文件）。
   4. 对于流量日志，请选择 **Log at Session Start**（在会话开始时记录）和 **Log At Session End**（在会话结束时记录）复选框之一或两者，然后单击 **OK**（确定）。

   有关如何配置日志转发配置文件和分配配置文件到策略规则的详细信息，请参阅配置日志转发。

STEP 3 | 为系统、配置、HIP 匹配和关联日志配置 syslog 转发。

1. 选择**Device**（设备）> **Log Settings**（日志设置）。
2. 对于系统和关联日志，请单击每种严重性级别，选择 **Syslog** 服务器配置文件，并单击 **OK**（确定）。
3. 对于配置、HIP 匹配和关联日志，请编辑此部分，选择 **Syslog** 服务器配置文件，并单击 **OK**（确定）。

STEP 4 | （可选）配置 Syslog 消息的标头格式。

日志数据包括生成日志的防火墙的唯一标识符。选择标头格式可在筛选和报告日志数据时为一些安全信息和事件管理 (SIEM) 服务器提供很大的灵活性。

此设置是全局设置，适用于防火墙上配置的所有 syslog 服务器配置文件。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑“日志记录和报告设置”。
2. 选择 **Log Export and Reporting**（日志导出和报告）选项卡并选择 Syslog 主机名格式：
   - **FQDN**（默认）— 拼合在发送防火墙上定义的主机名和域名。
   - **Hostname**（主机名）— 可使用发送防火墙上定义的主机名。
   - **ipv4-address**（**ipv6** 地址）— 使用用于发送日志的防火墙接口的 IPv4 地址。默认情况下，此接口是 MGT 接口。
   - **ipv6-address**（**ipv6** 地址）— 使用用于发送日志的防火墙接口的 IPv6 地址。默认情况下，此接口是 MGT 接口。
   - **None**（无）— 可保留未在防火墙上进行配置的主机名字段。发送日志的防火墙无标识符。
3. 单击 **OK**（确定）保存更改。

STEP 5 | 创建证书以确保通过 TLSv1.2 的 syslog 通信安全

如果 syslog 服务器使用客户端身份验证，则它是必须的。Syslog 服务器会使用此证书验证防火墙是否获得授权与 Syslog 服务器通信。

请确保符合以下条件：

- 私匙在发送防火墙上必须可用；密匙不能位于硬件安全模块 (HSM) 上。
- 证书的使用者和颁发者不得是同一人。
- syslog 服务器和发送防火墙必须具有同一个受信任证书授权机构 (CA) 签署的证书。或者，您可以在防火墙上生成自签名证书，从防火墙导出此证书，并将其导入 Syslog 服务器。
- 只要信任链中的每个证书指定了这两个扩展中的一个或全部，则可以使用在线证书状态协议 (OCSP) 或证书吊销列表 (CRL) 使 TLS 上的 Syslog 服务器连接通过验证。但是，您无法绕过 OCSP或 CRL 故障，因此，您必须确保证书链有效，并使用 OCSP 或 CRL 验证每个证书。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
2. 输入证书的 **Name**（名称）。
3. 在 **Common Name**（公用名称）字段中，输入将日志发送到 Syslog 服务器的防火墙的 IP 地址。
4. 在 **Signed by**（签名者）中，选择 Syslog 服务器和发送防火墙都信任的受信任 CA 或自签名 CA。



© 2019 Palo Alto Networks, Inc.

证书不能是 **Certificate Authority**（证书颁发机构）或 **External Authority**（外部颁发机构）（证书签署请求 [CSR]）。

5. 单击 **Generate**（生成）。防火墙生成证书和密钥对。
6. 单击证书名称对其进行编辑，请选中 **Certificate for Secure Syslog**（安全 **Syslog** 的日志）复选框，然后单击 **OK**（确定）。

STEP 6 | 提交您的更改并查看 syslog 服务器上的日志。

1. 单击 **Commit**（提交）。
2. 要查看日志，请参阅 syslog 管理软件的文档。您还可以查看 Syslog 字段说明。

# Syslog 字段说明

以下主题列出了 Palo Alto Networks 防火墙可以转发至外部服务器的每种日志类型的标准字段，以及严重性级别、自定义格式和转义序列。为了便于解析，我们使用逗号作为分隔符；每个字段都是逗号分隔值 (CSV) 字符串。FUTURE_USE 标签适用于防火墙当前无法实施的字段。

*WildFire* 日志是威胁日志的子类型，使用相同的 *Syslog* 格式。

- 流量日志字段
- 威胁日志字段
- HIP 匹配日志字段
- IP 标记日志字段
- User-ID 日志字段
- 解密日志字段
- 隧道检测日志字段
- SCTP 日志字段
- 配置日志字段
- 身份验证日志字段
- 系统日志字段
- 关联事件日志字段
- GTP 日志字段
- 自定义日志/事件格式
- 转义序列

## 流量日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，源地址，目标地址，NAT 源 IP，NAT 目标 IP，规则名称，源用户，目标用户，应用程序，虚拟系统，源区域，目标区域，入站接口，出站接口，日志操作，FUTURE_USE，会话 ID，重复次数，源端口，目标端口，NAT 源端口，NAT 目标端口，标志，协议，操作，字节，发送的字节，接收的字节，数据包，启动时间，耗用时间，类别，FUTURE_USE，序列号，操作标志，源国家/地区，目标国家/地区，FUTURE_USE，发送的数据包，接收的数据包，会话结束原因，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，操作源，源 VM UUID，目标 VM UUID，隧道 ID/IMSI，监控标记/IMEI，父会话 ID，父启动时间，隧道类型，SCTP 关联 ID，SCTP 块，发送的 SCTP 块，接收的 SCTP 块，规则 UUID，HTTP/2 连接，链路更改次数，策略 ID，链路交换机，SD-WAN 集群，SD-WAN 设备类型，SD-WAN 集群类型，SD-WAN 站点，动态用户组名称，XFF 地址，源设备类别，源设备配置文件，源设备型号，源设备供应商，源设备操作系统系列，源设备操作系统版本，源主机，源 MAC 地址，目标设备类别，目标设备配置文件，目标设备型号，目标设备供应商，目标设备操作系统系列，目标设备操作系统版本，目标主机名，目标 MAC 地址，容器 ID，POD 命名空间，POD 名称，源外部动态列表，


© 2019 Palo Alto Networks, Inc.

目标外部动态列表，主机 ID，序列号，源动态地址组，目标动态地址组，会话所有者，高分辨率时间戳，A 切片服务类型，A 切片区分项

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 TRAFFIC。 |
| 威胁/内容类型 (subtype) | 通信日志的子类型；值为开始、结束、丢弃和拒绝。<br>• 开始 — 会话已开始<br>• 结束 — 会话已结束<br>• 丢弃 — 标识应用程序之前以及无规则允许执行会话时丢弃会话。<br>• 拒绝 — 标识应用程序之后，有规则阻止或无规则允许执行会话时丢弃会话。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 原始会话源 IP 地址。 |
| 目标地址 (dst) | 原始会话目标 IP 地址。 |
| NAT 源 IP (natsrc) | 如果执行源 NAT，则为 NAT 后源 IP 地址。 |
| NAT 目标 IP (natdst) | 如果执行目标 NAT，则为 NAT 后目标 IP 地址。 |
| 规则名称 (rule) | 与会话匹配的规则名称。 |
| 源用户 (srcuser) | 启动会话的用户的用户名。 |
| 目标用户 (dstuser) | 接收会话的用户的用户名。 |
| 应用程序 (app) | 与会话关联的应用程序。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源区域 (from) | 会话的源区域。 |
| 目标区域 (to) | 会话的目标区域。 |
| 入站接口 (inbound_if) | 会话的源接口。 |
| 出站接口 (outbound_if) | 会话的目标接口。 |
| 日志操作 (logset) | 适用于会话的日志转发配置文件。 |
| 会话 ID (sessionid) | 应用于每个会话的内部数字标识符。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和子类型的会话数量。 |
| 源端口 (sport) | 会话利用的源端口。 |
| 目标端口 (dport) | 会话利用的目标端口。 |
| NAT 源端口 (natsport) | NAT 后源端口。 |
| NAT 目标端口 (natdport) | NAT 后目标端口。 |
| 标志 (flags) | 提供会话详细信息的 32 位字段；该字段可使用这些值与日志记录值进行 AND 运算解码：<br>• 0x80000000 — 有数据包捕获的会话 (PCAP)<br>• 0x40000000 — 启用选项，允许客户端使用多个路径连接到目标主机<br>• 0x20000000 — 文件已提交至 WildFire 进行判定<br>• 0x10000000 — 检测到最终用户提交企业凭据<br>• 0x08000000 — 流量来源已列入允许列表，不受 recon 保护<br>• 0x02000000 — IPv6 会话<br>• 0x01000000 — SSL 会话已解密（SSL 代理）<br>• 0x00800000 — 已通过 URL 筛选拒绝会话<br>• 0x00400000 — 会话已执行 NAT 转换<br>• 0x00200000 — 通过身份验证门户捕获到会话的用户信息<br>• 0x00100000 — 应用程序流量位于非标准的目标端口上<br>• 0x00080000 — 源自代理的 X-Forwarded-For 值位于源用户字段中<br>• 0x00040000 — 日志与 http 代理会话中的事务 (Proxy Transaction) 相对应<br>• 0x00020000 — 客户端到服务器的流量将根据策略转发<br>• 0x00010000 — 服务器到客户端的流量将根据策略转发<br>• 0x00008000 — 会话是指访问容器页面（容器页面）<br>• 0x00002000 — 会话暂时与处理应用程序相关性的隐式规则相匹配。在 PAN-OS 5.0.0 及更高版本中可用。<br>• 0x00000800 — 对称返回，用于转发会话的通信<br>• 0x00000400 — 解密流量通过镜像端口以明文发送<br>• 0x00000100 — 正在检查外部隧道中的有效负载 |
| IP 协议 (proto) | 与会话关联的 IP 协议。 |
| 操作 (action) | 对会话执行操作；可能的值为：<br>• 允许 — 策略允许对会话执行操作<br>• 拒绝 — 策略阻止对会话执行操作<br>• 丢弃 — 会话被静默丢弃<br>• 丢弃 ICMP — 会话被静默丢弃，有一条关于 ICMP 无法到达的消息发送至主机或应用程序<br>• 重置二者 — 会话被终止，TCP 重置发送至连接两端<br>• 重置客户端 — 会话被终止，TCP 重置发送至客户端<br>• 重置服务器 — 会话被终止，TCP 重置发送至服务器 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 字节数 (bytes) | 会话的总字节数（传输和接收）。 |
| 已发送字节数 (bytes_sent) | 客户端到服务器方向的会话字节数。 |
| 已接收字节数 (bytes_received) | 从服务器到客户端方向的会话字节数。 |
| 数据包 (packets) | 会话的数据包总数（传输和接收）。 |
| 启动时间 (start) | 会话开始的时间。 |
| 耗用时间 (elapsed) | 会话的耗用时间。 |
| 类别 (category) | 与会话关联的 URL 类别（如果适用）。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 源国家/地区 (srcloc) | 源国家/地区或专用地址的内部区域；最长为 32 个字节。 |
| 目标国家/地区 (dstloc) | 目标国家/地区或专用地址的内部区域。最长为 32 个字节。 |
| 发送的数据包 (pkts_sent) | 从客户端到服务器的会话数据包数。 |
| 接收的数据包 (pkts_received) | 从服务器到客户端的会话数据包数。 |
| 会话结束原因 (session_end_reason) | 会话终止原因。如果导致终止的原因有多个，那么该字段只会显示优先级最高的原因。以下是按照优先级进行排序的可能会话结束原因值（第一个优先级最高）：<br>• 威胁 — 防火墙检测到与重置、丢弃或阻止（IP 地址）操作相关的威胁。<br>• 策略拒绝 — 会话与包含拒绝或丢弃操作的安全策略匹配。<br>• decrypt-cert-validation（解密证书验证）— 会话终止，因为您配置防火墙在此会话使用的客户端身份验证或当此会话使用的服务器证书处于以下任一情况时，阻挡 SSL 转发代理解密或 SSL 入站检查：已过期、不可信的颁发者、未知状态或状态验证超时。当服务器证书产生类型为 bad_certificate、unsupported_certificate、certificate_revoked、access_denied 或 no_certificate_RESERVED（仅针对 SSLv3）的致命错误警报时，也会显示此会话终止原因（仅 SSLv3 ）。<br>• decrypt-unsupport-param（解密不支持参数）— 会话终止，因为您配置防火墙在此会话使用不受支持的协议版本、密码或 SSH 算法时，阻挡 SSL 转发代理解密或 SSL 入站检查。当此会话产生类型为 unsupported_extension、unexpected_message 或 handshake_failure 的致命错误警报时，也会显示此会话终止原因。<br>• decrypt-error（解密错误）— 会话终止，因为您配置防火墙在防火墙资源或硬件安全模块 (HSM) 不可用时，阻挡 SSL 转发代理解密或 SSL 入站检查。当您配置防火墙在产生了 SSH 错误或任何除针对解密证书验证和解密不支持参数终止原因之外的致命错误时，阻挡 SSL 流量。<br>• tcp-rst-from-client — 客户端向服务器发送 TCP 重置。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • tcp-rst-from-server — 服务器向客户端发送 TCP 重置。<br>• resources-unavailable — 会话因系统资源限制而丢弃。例如，会话可能已超出每个流允许的失序数据包数或全局失序数据包队列。<br>• tcp-fin — 连接中的两个主机发送了用于关闭会话的 TCP FIN 消息。 |
| | • tcp-reuse — 有会话被重复使用，防火墙关闭了之前的会话。<br>• decoder — 解码器检测到使用协议（如 HTTP 代理）的新连接并结束了之前的连接。<br>• aged-out — 会话已老化。<br>• unknown — 此值适用于以下情况：<br>  • 上述原因未包含的会话终止（例如 `clear session all` 命令）。<br>  • 对于在不支持会话结束原因字段的 PAN-OS 版本（低于 PAN-OS 6.1 的版本）中生成的日志，在升级到当前 PAN-OS 版本或将日志加载到防火墙后，该值将变为 **unknown**。<br>  • 在 Panorama 中，如果日志接收自 PAN-OS 版本无法提供相应会话结束原因支持的防火墙，那么值为 **unknown**。<br>• n/a — 此值适用于流量日志类型不为 **end** 的情况。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 操作源 (action_source) | 指定是否执行操作以允许或阻止在应用程序或策略中定义的某个应用程序。对会话的操作可能是允许、拒绝、重置服务器、重置客户端、重置两者。 |
| 源 VM UUID (src_uuid) | 标识 VMware NSX 环境中来宾虚拟机的源通用唯一标识符。 |
| 目标 VM UUID (dst_uuid) | 标识 VMware NSX 环境中来宾虚拟机的目标通用唯一标识符。 |
| 隧道 ID/IMSI(tunnelid/imsi) | 国际移动订户标识 (IMSI)是分配给 GSM/UMTS/EPS 系统中每个移动订户的唯一号码。IMSI 仅由十进制数字（0 到 9）组成，允许的最大位数为 15。 |
| 监控标记/IMEI (monitortag/imei) | 国际移动订户标识 (IMSI)是分配给移动站每台设备的唯一的 15 或 16 位数字。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 父会话 ID (parent_session_id) | 隧道会话中的会话 ID。仅适用于内部隧道（如为两级隧道）或内部内容（如为一级隧道）。 |
| 父启动时间 (parent_start_time) | 父隧道会话开始的年/月/日小时:分钟:秒。 |
| 隧道类型 (tunnel) | 隧道类型，如 GRE 或 IPSec。 |
| SCTP 关联 ID (assoc_id) | 标识两个 SCTP 端点之间关联的所有连接的编号。 |
| SCTP 块 (chunks) | 发送至关联或从关联接收到的 SCTP 块总数。 |
| 发送的 SCTP 块 (chunks_sent) | 为关联发送的 SCTP 块数。 |
| 接收的 SCTP 块 (chunks_received) | 为关联接收的 SCTP 块数。 |
| 规则 UUID (rule_uuid) | 永久标识规则的 UUID。 |
| HTTP/2 连接 (http2_connection) | 通过显示以下值之一标识流量是否使用 HTTP/2 连接：<br>• 父会话 ID — HTTP/2 连接<br>• 0 — SSL 会话 |
| 链路更改次数 (link_change_count) | 会话期间链路翻动的次数。 |
| 策略 ID (policy_id) | SD-WAN 策略的名称。 |
| 链路交换机 (link_switches) | 最多包含四个链路翻动条目，每个条目都包括链路名称、链路标记、链路类型、物理接口、时间戳、读取的字节数、写入的字节数、链路运行状况和链路翻动原因。 |
| SD-WAN 集群 (sdwan_cluster) | SD-WAN 集群的名称。 |
| SD-WAN 设备类型 (sdwan_device_type) | 设备类型（中心或分支）。 |
| SD-WAN 集群类型 (sdwan_cluster_type) | 集群类型（网状或中心辐射式）。 |
| SD-WAN 站点 (sdwan_site) | SD-WAN 站点的名称。 |
| 动态用户组名称 (dynusergroup_name) | 包含发起会话的用户的动态用户组的名称。 |
| XFF 地址 (xff_ip) | 请求 Web 页面的用户的 IP 地址，或是靠近最后一个其请求已被遍历的设备的 IP 地址。如果请求经过一个或多个代理、负载平衡器或其他上游设备，则防火墙将显示最新设备的 IP 地址。 |
| 源设备类别 (src_category) | 被 Device-ID 标识为流量源的设备类别。 |
| 源设备配置文件 (src_profile) | 被 Device-ID 标识为流量源的设备的配置文件。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 源设备型号(src_model) | 被 Device-ID 标识为流量源的设备的型号。 |
| 源设备供应商 (src_vendor) | 被 Device-ID 标识为流量源的设备的供应商。 |
| 源设备 OS 系列 (src_osfamily) | 被 Device-ID 标识为流量源的设备的操作系统类型。 |
| 源设备 OS 版本 (src_osversion) | 被 Device-ID 标识为流量源的设备的操作系统版本。 |
| 源主机名 (src_host) | 被 Device-ID 标识为流量源的设备的主机名。 |
| 源 MAC 地址 (src_mac) | 被 Device-ID 标识为流量源的设备的 MAC 地址。 |
| 目标设备类别 (dst_category) | 被 Device-ID 标识为流量目标的设备的类别。 |
| 目标设备配置文件 (dst_profile) | 被 Device-ID 标识为流量目标的设备的配置文件。 |
| 目标设备型号 (dst_model) | 被 Device-ID 标识为流量目标的设备的型号。 |
| 目标设备供应商(dst_vendor) | 被 Device-ID 标识为流量目标的设备的供应商。 |
| 目标设备 OS 系列 (dst_osfamily) | 被 Device-ID 标识为流量目标的设备的操作系统类型。 |
| 目标设备 OS 版本 (dst_osversion) | 被 Device-ID 标识为流量目标的设备的操作系统版本。 |
| 目标主机名 (dst_host) | 被 Device-ID 标识为流量目标的设备的主机名。 |
| 目标 MAC 地址(dst_mac) | 设备 ID 将其标识为流量目标的设备的 MAC 地址。 |
| 容器 ID (container_id) | 已部署应用程序 POD 的 Kubernetes 节点上 PAN-NGFW pod 的容器 ID。 |
| POD 命名空间 (pod_namespace) | 受保护的应用程序 POD 的命名空间。 |
| POD 名称 (pod_name) | 受保护的应用程序 POD。 |
| 源外部动态列表(src_edl) | 包含流量源 IP 地址的外部动态列表名称。 |
| 目标外部动态列表 (dst_edl) | 包含流量目标 IP 地址的外部动态列表名称。 |
| 主机 ID (hostid) | GlobalProtect 分配用于标识主机的唯一 ID。 |
| 用户设备序列号 (serialnumber) | 用户计算机或设备的序列号。 |
| 源动态地址组 (src_dag) | 原始会话源动态地址组。 |
| 目标动态地址组 (dst_dag) | 原始目标源动态地址组。 |
| 会话所有者(session_owner) | 会话表数据在 HA 故障转移时同步的 HA 集群中的高可用性(HA)原始对等会话所有者。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 高分辨率时间戳 (high_res_timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00:000-8:00` 。 |
| 切片服务类型 (nsdsai_sst) | 网络切片 ID 的 A 切片服务类型。 |
| A 切片区分项 (nsdsai_sd) | 网络切片 ID 的 A 切片区分项。 |

## 威胁日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，源地址，目标地址，NAT 源 IP，NAT 目标 IP，规则名称，源用户，目标用户，应用程序，虚拟系统，源区域，目标区域，入站接口，出站接口，日志操作，FUTURE_USE，会话 ID，重复次数，源端口，目标端口，NAT 源端口，NAT 目标端口，标志，IP 协议，操作，URL/文件名，威胁 ID，类别，严重性，方向，序号，操作标志，源位置，目标位置，FUTURE_USE，内容类型，PCAP_ID，文件摘要，云，URL 索引，用户代理，文件类型，X-Forwarded-For，引用站点，发件人，主题，收件人，报告 ID，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，FUTURE_USE，源 VM UUID，目标 VM UUID，HTTP 方法，隧道 ID/IMSI，监控标记/IMEI，父会话 ID，父会话开始时间，隧道类型，威胁类别，内容版本，FUTURE_USE，SCTP 关联 ID，有效载荷协议 ID，HTTP 标头，URL 类别列表，规则 UUID，HTTP/2 连接，动态用户组名称，XFF 地址，源设备类别，源设备配置文件，源设备型号，源设备供应商，源设备操作系统系列，源设备操作系统版本，源主机，源 MAC 地址，目标设备类别，目标设备配置文件，目标设备型号，目标设备供应商，目标设备操作系统系列，目标设备操作系统版本，目标设备主机名，目标 MAC 地址，容器 ID，POD 命名空间，POD 名称，源外部动态列表，目标外部动态列表，主机 ID，序列号，域 EDL，源动态地址组，目标动态地址组，会话所有者，部分哈希，高分辨率时间戳，原因，理由，A 切片服务类型

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (Serial #) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 THREAT。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 威胁/内容类型 (subtype) | 威胁日志的子类型。值包括以下项目：<br>• 数据 — 与数据筛选配置文件匹配的数据模式。<br>• 文件 — 与文件传送阻止配置文件匹配的文件类型。<br>• 泛滥攻击 — 通过区域保护配置文件检测泛滥攻击。<br>• 数据包 — 由区域保护配置文件触发的基于数据包的攻击保护。<br>• 扫描 — 通过区域保护配置文件检测扫描。<br>• 间谍软件 — 通过防间谍软件配置文件检测间谍软件。<br>• url — URL 筛选日志。<br>• 病毒 — 通过防病毒软件配置文件检测病毒。<br>• 漏洞 — 通过漏洞保护配置文件检测漏洞利用。<br>• wildfire — 当防火墙每个 WildFire 分析配置文件和判定（恶意软件、网络钓鱼、灰色软件或良性软件，取决于记录的内容）都提交一个文件给 WildFire 时，生成的 WildFire 判定记录在 WildFire 提交日志中。<br>• WildFire 病毒 — 通过防病毒软件配置文件检测病毒。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 原始会话源 IP 地址。 |
| 目标地址 (dst) | 原始会话目标 IP 地址。 |
| NAT 源 IP (natsrc) | 如果执行源 NAT，则为 NAT 后源 IP 地址。 |
| NAT 目标 IP (natdst) | 如果执行目标 NAT，则为 NAT 后目标 IP 地址。 |
| 规则名称 (rule) | 与会话匹配的规则名称。 |
| 源用户 (srcuser) | 启动会话的用户的用户名。 |
| 目标用户 (dstuser) | 接收会话的用户的用户名。 |
| 应用程序 (app) | 与会话关联的应用程序。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源区域 (from) | 会话的源区域。 |
| 目标区域 (to) | 会话的目标区域。 |
| 入站接口 (inbound_if) | 会话的源接口。 |
| 出站接口 (outbound_if) | 会话的目标接口。 |
| 日志操作 (logset) | 适用于会话的日志转发配置文件。 |
| 会话 ID (sessionid) | 应用于每个会话的内部数字标识符。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和内容/威胁类型的会话数量。 |
| 源端口 (sport) | 会话利用的源端口。 |
| 目标端口 (dport) | 会话利用的目标端口。 |
| NAT 源端口 (natsport) | NAT 后源端口。 |
| NAT 目标端口 (natdport) | NAT 后目标端口。 |
| 标志 (flags) | 提供会话详细信息的 32 位字段；该字段可使用这些值与日志记录值进行 AND 运算解码：<br>• 0x80000000 — 有数据包捕获的会话 (PCAP)<br>• 0x40000000 — 启用选项，允许客户端使用多个路径连接到目标主机<br>• 0x20000000 — 文件已提交至 WildFire 进行判定<br>• 0x10000000 — 检测到最终用户提交企业凭据<br>• 0x08000000 — 流量来源已列入允许列表，不受 recon 保护<br>• 0x02000000 — IPv6 会话<br>• 0x01000000 — SSL 会话已解密（SSL 代理）<br>• 0x00800000 — 已通过 URL 筛选拒绝会话<br>• 0x00400000 — 会话已执行 NAT 转换<br>• 0x00200000 — 通过身份验证门户捕获到会话的用户信息<br>• 0x00100000 — 应用程序流量位于非标准的目标端口上<br>• 0x00080000 — 源自代理的 X-Forwarded-For 值位于源用户字段中<br>• 0x00040000 — 日志与 http 代理会话中的事务（代理事务）相对应<br>• 0x00020000 — 客户端到服务器的流量将根据策略转发<br>• 0x00010000 — 服务器到客户端的流量将根据策略转发<br>• 0x00008000 — 会话是指访问容器页面（容器页面）<br>• 0x00002000 — 会话暂时与处理应用程序相关性的隐式规则相匹配。在 PAN-OS 5.0.0 及更高版本中可用。<br>• 0x00000800 — 对称返回，用于转发此会话的流量<br>• 0x00000400 — 解密流量通过镜像端口以明文发送<br>• 0x00000010 — 正在检查外部隧道中的有效负载 |
| IP 协议 (proto) | 与会话关联的 IP 协议。 |
| 操作 (action) | 针对会话采取的操作；值为警报、允许、拒绝、丢弃、丢弃所有数据包、重置客户端、重置服务器、重置两者、阻止 URl。<br>• 警报 — 检测到威胁或 URL 但未阻止<br>• 允许 — 泛滥攻击检测报警<br>• 拒绝 — 激活淹没攻击检测机制并具有配置拒绝通信<br>• 丢弃 — 检测到威胁时丢弃关联会话<br>• 重置客户端 — 检测到威胁时发送 TCP RST 至客户端<br>• 重置服务器 — 检测到威胁时发送 TCP RST 至服务器<br>• 重置两者 — 检测到威胁时发送 TCP RST 至客户端和服务器<br>• 阻止 URL — URL 请求被阻止，因为它与已设置的要阻止的 URL 类型相匹配<br>• 阻止 IP — 检测到威胁，阻止客户端 IP |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • 随机丢弃 — 检测到泛滥攻击，随机丢弃数据包<br>• Sinkhole — DNS sinkhole 已激活<br>• Cookie 同步发送 — Cookie 同步警报<br>• 阻止 - 继续（仅限 URL 子类别）— HTTP 请求被阻止，并通过确认按钮被重定向至继续页面以继续<br>• 继续（仅限 URL 子类别）— 对阻止 - 继续 URL 继续页面的响应，表示阻止 - 继续请求被允许，以继续<br>• 阻止 - 覆盖（仅限 URL 子类别）— 阻止 HTTP 请求，并重定向至需要从防火墙管理员获取通行码以继续的管理替代页面<br>• 覆盖 - 锁定（仅限 URL 子类别）— 源 IP 的管理替代通行码尝试太多次且均以失败告终。现在，IP 被阻止关联阻止 - 覆盖重定向页面<br>• 覆盖（仅限 URL 子类别）— 响应阻止 - 覆盖页面，其中提供了正确的通行码，且允许请求<br>• 阻止（仅限 Wildfire）— 文件被防火墙阻止，并上传至 Wildfire |
| URL/文件名 (misc) | 长度可变的字段。文件名最多包含 63 个字符。URL 最多包含 1023 个字符<br>子类型是 url 时的实际 URI<br>子类型为文件时的文件名或文件类型<br>子类型为病毒时的文件名<br>子类型为 wildfire-virus 时的文件名<br>子类型为 wildfire 时的文件名<br>子类型为 vulnerability 时的 URL 或 文件名，如适用<br>威胁类别是 `domain-edl` 的 URL |
| 威胁/内容名称 (threatid) | 已知自定义威胁的 Palo Alto Networks 标识符。该标识是一个说明性字符串，后跟括号中含有某些子类型的 64 位数字标识符：<br>• 8000 – 8099 — 扫描检测<br>• 8500 – 8599 — 泛滥攻击检测<br>• 9999 — URL 筛选日志<br>• 10000 – 19999 — 防间谍软件回拨检测<br>• 20000 – 29999 — 防间谍软件下载检测<br>• 30000 – 44999 — 漏洞利用检测<br>• 52000 – 52999 — 文件类型检测<br>• 60000 – 69999 — 数据筛选检测<br>如果 域 EDL 字段已填充，那么该字段也使用相同的值填充。<br>病毒检测的威胁 *ID* 范围、*WildFire* 签名馈送，以及以前发布中使用的 *DNS C2* 签名已被永久替换为永久、全局唯一 ID。请参阅威胁/内容类型 *(subtype)* 和威胁类别 *(thr_category)* 字段名称，以创建更新过的报告，筛选威胁日志和 *ACC* 活动。 |
| 类别 (category) | 对于 URL 子类型，为 URL 类别；对于 WildFire 子类型，判定结论位于文件上，值为“恶意”、“网络钓鱼”、“灰色软件”或“良性”；对于其他子类型，值为“任意”。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 严重性 (severity) | 与威胁关联的严重性；值为 informational、low、medium、high、critical。 |
| 方向 (direction) | 表示攻击的方向，“客户端到服务器”或“服务器到客户端”。<br>• 0 — 威胁方向为客户端到服务器<br>• 1 — 威胁方向为服务器到客户端 |
| 序号 (seqno) | 递增的 64 位日志条目标识符。每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 源国家/地区 (srcloc) | 源国家/地区或专用地址的内部区域。最长为 32 个字节。 |
| 目标国家/地区 (dstloc) | 目标国家/地区或专用地址的内部区域。最长为 32 个字节。 |
| 内容类型 (contenttype) | 仅当子类型为 URL 时适用。<br>HTTP 响应数据的内容类型。最长为 32 个字节。 |
| PCAP ID (pcap_id) | 数据包捕获 (pcap) ID 是 64 位的无符号整数，用来标记含扩展 pcap（此通信流的组成部分）的关联威胁 pcap 文件的 ID。所有威胁日志都包含一个 0 的 pcap_id（无关联 pcap）或一个扩展 pcap 文件的 ID。 |
| 文件摘要 (filedigest) | 仅适用于 WildFire 子类型；所有其他类型不使用此字段<br>Filedigest 字符串显示发送后通过 WildFire 服务进行分析的文件的二进制哈希。 |
| 云 (cloud) | 仅适用于 WildFire 子类型；所有其他类型不使用此字段。<br>云字符串显示 WildFire 应用程序（专用）或从此处上传文件进行分析的 WildFire 云（公用）的 FQDN。 |
| URL 索引 (url_idx) | 在 URL 筛选和 WildFire 子类型中使用。<br>当应用程序使用 TCP keepalive 保持一定时间长度的连接时，该会话的所有日志条目都有单个会话 ID。在此类情况下，当单个威胁日志（和会话 ID）包括多个 URL 条目时，url_idx 就是计数器，让您能够关联单个会话内的每个日志条目的顺序。<br>例如，要获取防火墙转发至 WildFire 进行分析的某个文件的 URL，请在 WildFire 提交日志中找到会话 ID 和 url_idx，并在 URL 筛选日志中搜索相同的会话 ID 和 url_idx。会话 ID 和 url_idx 匹配的日志条目将包含提交至 WildFire 的文件的 URL。 |
| 用户代理 (user_agent) | 仅适用于 URL 筛选器子类型；所有其他类型不使用此字段。<br>用户代理字段可指定用户用于访问 URL 的 Web 浏览器，例如互联网Explorer。此信息在 HTTP 请求中发送到服务器。 |
| 文件类型 (filetype) | 仅适用于 WildFire 子类型；所有其他类型不使用此字段。<br>可指定防火墙为 WildFire 分析而转发的文件类型。 |
| X-Forwarded-For (xff) | 仅适用于 URL 筛选器子类型；所有其他类型不使用此字段。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | HTTP 标头中的 X-Forwarded-For 字段包含请求网页的用户的 IP 地址。允许您识别用户的 IP 地址，尤其是在您的网络上有代理服务器时相当有用，即可在数据包标头的源 IP 地址字段中使用其自己的地址代替用户 IP 地址。 |
| 引用站点 (referer) | 仅适用于 URL 筛选器子类型；所有其他类型不使用此字段。<br>HTTP 标头中的引用站点字段包含用户链接到其他网页的网页的 URL；它是用户重定向（引用）到所请求的网页的源。 |
| 发件人 (sender) | 指定电子邮件发件人姓名。 |
| 主题 (subject) | 指定电子邮件主题。 |
| 收件人 (recipient) | 指定电子邮件收件人姓名。 |
| 报告 ID (reportid) | 仅适用于 WildFire 子类型；所有其他类型不使用此字段。<br>识别 WildFire 云或 WildFire 设备上的分析请求。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 源 VM UUID (src_uuid) | 标识 VMware NSX 环境中来宾虚拟机的源通用唯一标识符。 |
| 目标 VM UUID (dst_uuid) | 标识 VMware NSX 环境中来宾虚拟机的目标通用唯一标识符。 |
| HTTP 方法 (http_method) | 仅在 URL 筛选日志中。描述 Web 请求中使用的 HTTP 方法。只记录以下方法：连接、删除、获取、标头、选项、发布、放置。 |
| 隧道 ID/IMSI (tunnel_id/imsi) | 国际移动订户标识 (IMSI)是分配给 GSM/UMTS/EPS 系统中每个移动订户的唯一号码。IMSI 仅由十进制数字（0 到 9）组成，允许的最大位数为 15。 |
| 监控标记/IMEI (monitortag/imei) | 国际移动订户标识 (IMSI)是分配给移动站每台设备的唯一的 15 或 16 位数字。 |
| 父会话 ID (parent_session_id) | 隧道会话中的会话 ID。仅适用于内部隧道（如为两级隧道）或内部内容（如为一级隧道）。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 父会话开始时间 (parent_start_time) | 父隧道会话开始的年/月/日小时:分钟:秒。 |
| 隧道类型 (tunnel) | 隧道类型，如 GRE 或 IPSec。 |
| 威胁类别 (thr_category) | 描述用于对不同类型的威胁签名进行分类的威胁类别。<br>如果域外部动态列表生成了日志，则会在该字段填入 `domain-edl`。 |
| 内容版本 (contentver) | 生成日志时，防火墙上的应用程序和威胁版本。 |
| SCTP 关联 ID (assoc_id) | 标识两个 SCTP 端点之间关联的所有连接的编号。 |
| 有效载荷协议 ID (ppid) | 数据块数据部分中用于有效载荷的协议 ID<br>。 |
| HTTP 标头 (http_headers) | 表示防火墙上 URL 日志条目中已插入的 HTTP 标头。 |
| URL 类别列表 (url_category_list) | 列出防火墙用于实施策略的 URL 过滤类别。 |
| 规则 UUID (rule_uuid) | 永久标识规则的 UUID。 |
| HTTP/2 连接 (http2_connection) | 通过显示以下值之一标识流量是否使用 HTTP/2 连接：<br>• TCP 连接会话 ID — 会话是 HTTP/2<br>• 0 — 会话不是 HTTP/2 |
| 动态用户组名称 (dynusergroup_name) | 包含发起会话的用户的动态用户组的名称。 |
| XFF 地址 (xff_ip) | 请求 Web 页面的用户的 IP 地址，或是靠近最后一个其请求已被遍历的设备的 IP 地址。如果请求经过一个或多个代理、负载平衡器或其他上游设备，则防火墙将显示最新设备的 IP 地址。 |
| 源设备类别 (src_category) | 被 Device-ID 标识为流量源的设备类别。 |
| 源设备配置文件 (src_profile) | 被 Device-ID 标识为流量源的设备的配置文件。 |
| 源设备型号(src_model) | 被 Device-ID 标识为流量源的设备的型号。 |
| 源设备供应商 (src_vendor) | 被 Device-ID 标识为流量源的设备的供应商。 |
| 源设备 OS 系列 (src_osfamily) | 被 Device-ID 标识为流量源的设备的操作系统类型。 |
| 源设备 OS 版本 (src_osversion) | 被 Device-ID 标识为流量源的设备的操作系统版本。 |
| 源主机名 (src_host) | 被 Device-ID 标识为流量源的设备的主机名。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 源 MAC 地址 (src_mac) | 被 Device-ID 标识为流量源的设备的 MAC 地址。 |
| 目标设备类别 (dst_category) | 被 Device-ID 标识为流量目标的设备的类别。 |
| 目标设备配置文件 (dst_profile) | 被 Device-ID 标识为流量目标的设备的配置文件。 |
| 目标设备型号 (dst_model) | 被 Device-ID 标识为流量目标的设备的型号。 |
| 目标设备供应商(dst_vendor) | 被 Device-ID 标识为流量目标的设备的供应商。 |
| 目标设备 OS 系列 (dst_osfamily) | 被 Device-ID 标识为流量目标的设备的操作系统类型。 |
| 目标设备 OS 版本 (dst_osversion) | 被 Device-ID 标识为流量目标的设备的操作系统版本。 |
| 目标主机名 (dst_host) | 被 Device-ID 标识为流量目标的设备的主机名。 |
| 目标 MAC 地址(dst_mac) | 设备 ID 将其标识为流量目标的设备的 MAC 地址。 |
| 容器 ID (container_id) | 已部署应用程序 POD 的 Kubernetes 节点上 PAN-NGFW pod 的容器 ID。 |
| POD 命名空间 (pod_namespace) | 受保护的应用程序 POD 的命名空间。 |
| POD 名称 (pod_name) | 受保护的应用程序 POD。 |
| 源外部动态列表(src_edl) | 包含流量源 IP 地址的外部动态列表名称。 |
| 目标外部动态列表 (dst_edl) | 包含流量目标 IP 地址的外部动态列表名称。 |
| 主机 ID (hostid) | GlobalProtect 分配用于标识主机的唯一 ID。 |
| 用户设备序列号 (serialnumber) | 用户计算机或设备的序列号。 |
| 域 EDL (domain_edl) | 包含流量域名的外部动态列表名称。 |
| 源动态地址组 (src_dag) | 原始会话源动态地址组。 |
| 目标动态地址组 (dst_dag) | 原始目标源动态地址组。 |
| 部分哈希 (partial_hash) | 机器学习部分哈希。 |
| 高分辨率时间戳 (high_res timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31） |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br><br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00.000-8:00` 。 |
| 原因 (reason) | 数据筛选操作的原因。 |
| 理由 (justification) | 数据筛选操作的理由。 |
| 切片服务类型 (nsdsai_sst) | 网络切片 ID 的 A 切片服务类型。 |

## *HIP* 匹配日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，源用户，虚拟系统，计算机名称，操作系统，源地址，HIP，重复次数，HIP 类型，FUTURE_USE，FUTURE_USE，序列号，操作标志，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，虚拟系统 ID，IPv6 源地址，主机 ID，用户设备序列号，设备 MAC 地址，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 HIP-MATCH。 |
| 威胁/内容类型 (subtype) | HIP 匹配日志的子类型；未使用。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源用户 (srcuser) | 启动会话的用户的用户名。 |
| 虚拟系统 (vsys) | 与 HIP 匹配日志关联的虚拟系统。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 计算机名称 (machinename) | 用户计算机的名称。 |
| 操作系统 (os) | 用户的计算机或设备（或客户端系统）上的安装的操作系统。 |
| 源地址 (src) | 源用户的 IP 地址。 |
| HIP (matchname) | HIP 对象或配置文件的名称。 |
| 重复次数 (repeatcnt) | HIP 配置文件匹配的次数。 |
| HIP 类型 (matchtype) | HIP 字段是代表 HIP 对象还是 HIP 配置文件。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 虚拟系统 ID (vsys_id) | Palo Alto Networks 防火墙上的虚拟系统的唯一标识符。 |
| IPv6 系统地址 (srcipv6) | 用户机器或设备的 IPv6 地址。 |
| 主机 ID (hostid) | GlobalProtect 分配用于标识主机的唯一 ID。 |
| 用户设备序列号 (serialnumber) | 用户计算机或设备的序列号。 |
| 设备 MAC 地址 (mac) | 用户机器或设备的 MAC 地址。 |
| 高分辨率时间戳 (high_res _timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31） |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br><br>从运行 *PAN-OS 10.0* 以及更高版本的受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00.000-8:00` 。 |

## GlobalProtect 日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，虚拟系统，事件 ID，阶段，身份验证方法，隧道类型，源用户，源区域，计算机名称，公用 IP，公用 IPv6，私有 IP，私有 IPv6，主机 ID，序列号，客户端版本，客户端操作系统，客户端操作系统版本，重复次数，原因，错误，说明，状态，位置，登录持续时间，连接方法，错误代码，门户，序列号，操作标志，高分辨率时间戳，选择类型，响应时间，优先级，尝试网关，网关

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 GLOBALPROTECT。 |
| 威胁/内容类型 (subtype) | 威胁日志的子类型。值包括以下项目：<br>• 数据 — 与数据筛选配置文件匹配的数据模式。<br>• 文件 — 与文件传送阻止配置文件匹配的文件类型。<br>• 泛滥攻击 — 通过区域保护配置文件检测泛滥攻击。<br>• 数据包 — 由区域保护配置文件触发的基于数据包的攻击保护。<br>• 扫描 — 通过区域保护配置文件检测扫描。<br>• 间谍软件 — 通过防间谍软件配置文件检测间谍软件。<br>• url — URL 筛选日志<br>• 病毒 — 通过防病毒软件配置文件检测病毒。<br>• 漏洞 — 通过漏洞保护配置文件检测漏洞利用。<br>• wildfire — 当防火墙每个 WildFire 分析配置文件和判定（恶意软件、网络钓鱼、灰色软件或良性软件，取决于记录的内容）都提交一个文件给 WildFire 时，生成的 WildFire 判定记录在 WildFire 提交日志中。<br>• WildFire 病毒 — 通过防病毒软件配置文件检测病毒。 |
| 生成时间 (time_generated) | 是指在数据面板上生成日志的时间。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 事件 ID (eventid) | 显示事件名称的字符串。 |
| 阶段 (stage) | 显示连接阶段的字符串（例如，before-login、login或 tunnel）。 |
| 身份验证方法 (auth_method) | 显示身份验证方法的字符串，例如，LDAP、RADIUS 或 SAML。 |
| 隧道类型 (tunnel_type) | 隧道的类型（SSLVPN 或 IPSec）。 |
| 源用户 (srcuser) | 发起会话的用户的用户名。 |
| 源区域 (srcregion) | 发起会话的用户的区域。 |
| 计算机名称 (machinename) | 用户计算机的名称。 |
| 公用 IP (public_ip) | 发起会话的用户的公用 IP 地址。 |
| 公用 IPv6 (public_ipv6) | 发起会话的用户的公用 IPv6 地址。 |
| 私有 IP (private_ip) | 发起会话的用户的私有 IP 地址。 |
| 私有 IPv6 (private_ipv6) | 发起会话的用户的私有 IPv6 地址。 |
| 主机 ID (hostid) | GlobalProtect 分配用于标识主机的唯一 ID。 |
| 序列号 (serialnumber) | 用户计算机或设备的序列号。 |
| 客户端版本 (client_ver) | 客户端使用的 GlobalProtect 应用程序版本。 |
| 客户端操作系统 (client_os) | 客户端设备使用的操作系统类型（例如，Windows 或 Linux）。 |
| 客户端操作系统版本 (client_os_ver) | 客户端设备使用的操作系统版本。 |
| 重复次数 (repeatcnt) | GlobalProtect 在最近 5 秒内检测到的、具有相同源 IP 地址、目标 IP 地址、应用程序和子类型的会话数。 |
| 原因 (reason) | 显示隔离原因的字符串。 |
| 错误 (error) | 显示任何事件中发生的错误的字符串。 |
| 说明 (opaque) | 已发生的任何事件的其他信息。 |
| 状态 (status) | 事件的状态（成功或失败）。 |
| 位置 (location) | 显示管理员定义的 GlobalProtect 门户或网关位置的字符串。 |
| 登录持续时间 (login_duration) | 用户在从登录到注销期间，与 GlobalProtect 网关保持连接的持续时间（以秒为单位）。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 连接方法 (connect_method) | 显示 GlobalProtect 应用程序如何连接到网关的字符串（例如，`on-demand` 或 `user-logon`）。 |
| 错误代码 (error_code) | 与发生的任何错误相关联的整数。 |
| 门户 (portal) | GlobalProtect 门户或网关的名称。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 网关选择方法 (selection_type) | 选择用于连接网关的连接方法。<br>• 手动 —您想 GlobalProtect 应用程序手动连接的网关。<br>• 首选 — 您想 GlobalProtect 应用程序连接的首选网关。<br>• 自动 — 根据分配给网关的优先级和响应时间自动连接到最佳可用网关。 |
| SSL 响应时间 (response_time) | 隧道设置期间，在端点上测量的所选网关的 SSL 响应时间（以毫秒为单位）。 |
| 网关优先级 (priority) | GlobalProtect 应用程序可以连接的网关的优先级顺序，划分为最高 (1)、高 (2)、中 (3)、低 (4) 或最低 (5)。 |
| 尝试网关 (attempted_gateways) | 使用网关名称、SSL 响应名称以及优先级为每个网关连接尝试收集的字段（请参阅多网关配置中的网关优先级）。每个字段条目都用逗号分开，例如 `g82-gateway,12,3`。每个网关条目都用分号分开，例如 `g83-gateway,10,2;g84-gateway,-1,1`。 |
| 网关名称 (gateway) | 门户配置上指定的网关名称。 |

## *IP* 标记日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，虚拟系统，源 IP，标记名称，事件 ID，重复计数，超时，数据源名称，数据源类型，数据源子类型，序号，操作标志，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，虚拟系统 ID，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 IPTAG。 |
| 威胁/内容类型 (subtype) | HIP 匹配日志的子类型；未使用。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 虚拟系统 (vsys) | 与 HIP 匹配日志关联的虚拟系统。 |
| 源 IP (src) | 源用户的 IP 地址。 |
| 标记名称 (tag_name) | 映射到源 IP 地址的标记。 |
| 事件 ID (event_id) | 显示事件名称的字符串。 |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和子类型的会话数量。 |
| 超时 (timeout) | 源 IP 地址的 IP 地址到标记映射的有效期。 |
| 数据源名称 (datasourcename) | 从中收集映射信息的源名称。 |
| 数据源类型 (datasource_type) | 从中收集映射信息的源。 |
| 数据源子类型 (datasource_subtype) | 用于识别数据源中 IP 地址到用户名映射的机制。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符。每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号，其中共享设备组（级别 0）除外，它未包含在此结构中。<br>如果日志值为 12、34、45 和 0，其表示日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 虚拟系统 ID (vsys_id) | Palo Alto Networks 防火墙上的虚拟系统的唯一标识符。 |
| 高分辨率时间戳 (high_res timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD： |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br><br>从运行 *PAN-OS 10.0* 以及更高版本的受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00:000-8:00` 。 |

## *User-ID* 日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，虚拟系统，源 IP，用户，数据源名称，事件 ID，重复次数，超时阈值，源端口，目标端口，数据源，数据源类型，序号，操作标志，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，虚拟系统 ID，因素类型，因素完成时间，因素编号，FUTURE_USE，FUTURE_USE，用户组标记，按源分类的用户，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 USERID。 |
| 威胁/内容类型 (subtype) | User-ID 日志的子类型；值为登录、注销、注册标记和取消注册标记。<br>• 登录 — 已登录用户。<br>• 注销 — 已注销用户。<br>• 注册标记 — 指示为用户注册的一个或多个标记。<br>• 取消注册标记 — 指示为用户取消注册的一个或多个标记。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 虚拟系统 (vsys) | 与配置日志关联的虚拟系统。 |
| 源 IP (ip) | 原始会话源 IP 地址。 |
| 用户 (user) | 标识最终用户。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 数据源名称 (datasourcename) | 发送 IP（端口）- 用户映射的 User-ID 源。 |
| 事件 ID (eventid) | 显示事件名称的字符串。 |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和子类型的会话数量。 |
| 超时阈值 (timeout) | 超时之后，IP/用户映射会被清除。 |
| 源端口 (beginport) | 会话利用的源端口。 |
| 目标端口 (endport) | 会话利用的目标端口。 |
| 数据源 (datasource) | 从中收集映射信息的来源。 |
| 数据源类型 (datasourcetype) | 用于识别数据源中 IP/用户映射的机制。 |
| 序号 (seqno) | 生成日志的防火墙的序列号。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API query：`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 虚拟系统 ID (vsys_id) | Palo Alto Networks 防火墙上的虚拟系统的唯一标识符。 |
| 因素类型 (factortype) | 供应商用于在多因素身份验证的情况下对用户进行身份验证。 |
| 因素完成时间 (factorcompletiontime) | 身份验证完成的时间。 |
| 因素编号 (factorno) | 指使用主要身份验证 (1) 或其他因素 (2, 3)。 |
| 用户组标记 (ugflags) | 显示该用户组是否在用户组映射时被发现。受支持的值包括：<br>• 发现的用户组 — 指示用户是否可以映射到组。<br>• 重复用户 — 指示是否在用户组内发现重复用户。如果未发现用户组，则显示 `N/A`。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 按用户分类的源 (userbysource) | 指示通过 IP 地址到用户名映射从源中接收到的用户名。 |
| 高分辨率时间戳 (high_res timestamp) | 在管理面板上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00:000-8:00` 。 |

## 解密日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，配置版本，生成时间，源地址，目标地址，NAT 源 IP，NAT 目标 IP，规则，源用户，目标用户，应用程序，虚拟系统，源区域，目标区域，入站接口，出站接口，日志操作，记录时间，会话 ID，重复计数，源端口，目标端口，NAT 源端口，NAT 目标端口，标志，IP 协议，操作，隧道，FUTURE_USE，FUTURE_USE，源 VM UUID，目标 VM UUID，规则 UUID，客户端到防火墙阶段，防火墙到客户端阶段，TLS 版本，密钥交换算法，加密算法，哈希算法，策略名称，椭圆曲线，错误索引，根状态，链状态，代理类型，证书序列号，指纹，证书开始日期，证书结束日期，证书版本，证书大小，通用名称长度，颁发机构通用名称长度，根通用名称长度，SNI 长度，证书标志，主题通用名称，颁发机构主题通用名称，根主题通用名称，服务器名称指示，错误，容器 ID，POD 命名空间，POD 名称，源外部动态列表，目标外部动态列表，源动态地址组，目标动态地址组，高分辨率时间戳，源设备类别，源设备配置文件，源设备型号，源设备供应商，源设备 OS 系列，源设备 OS 版本，源主机名，源 Mac 地址，目标设备类别，目标设备配置文件，目标设备型号，目标设备供应商，目标设备 OS 系列，目标设备 OS 版本，目标主机名，目标 Mac 地址，序列号，操作标志

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 DECRYPTION。 |
| 威胁/内容类型 (subtype) | 未在解密日志中使用。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 配置版本 (config_ver) | 软件版本。 |
| 生成时间 (time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 原始会话源 IP 地址。 |
| 目标地址 (dst) | 原始会话目标 IP 地址。 |
| NAT 源 IP (natsrc) | 如果执行源 NAT，则为 NAT 后源 IP 地址。 |
| NAT 目标 IP (natdst) | 如果执行目标 NAT，则为 NAT 后目标 IP 地址。 |
| 规则 (rule) | 用于控制会话流量的安全策略规则。 |
| 源用户 (srcuser) | 启动会话的用户的用户名。 |
| 目标用户 (dstuser) | 接收会话的用户的用户名。 |
| 应用程序 (app) | 与会话关联的应用程序。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源区域 (from) | 会话的源区域。 |
| 目标区域 (to) | 会话的目标区域。 |
| 入站接口 (inbound_if) | 会话的源接口。 |
| 出站接口 (outbound_if) | 会话的目标接口。 |
| 日志操作 (logset) | 适用于会话的日志转发配置文件。 |
| 记录时间 (time_received) | 接收日志的时间。 |
| 会话 ID (sessionid) | 应用于每个会话的内部数字标识符。 |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和内容/威胁类型的会话数量。 |
| 源端口 (sport) | 会话利用的源端口。 |
| 目标端口 (dport) | 会话利用的目标端口。 |
| NAT 源端口 (natsport) | NAT 后源端口。 |
| NAT 目标端口 (natdport) | NAT 后目标端口。 |
| 标志 (flags) | 提供会话详细信息的 32 位字段；该字段可使用这些值与日志记录值进行 AND 运算解码：<br>• 0x80000000 — 有数据包捕获的会话 (PCAP) |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • 0x40000000 — 启用选项，允许客户端使用多个路径连接到目标主机<br>• 0x20000000 — 文件已提交至 WildFire 进行判定<br>• 0x10000000 — 检测到最终用户提交企业凭据<br>• 0x08000000 — 流量来源已列入允许列表，不受 recon 保护<br>• 0x02000000 — IPv6 会话<br>• 0x01000000 — SSL 会话已解密（SSL 代理）<br>• 0x00800000 — 已通过 URL 过滤拒绝会话<br>• 0x00400000 — 会话已执行 NAT 转换<br>• 0x00200000 — 通过身份验证门户捕获到会话的用户信息<br>• 0x00100000 — 应用程序流量位于非标准的目标端口上<br>• 0x00080000 — 源自代理的 X-Forwarded-For 值位于源用户字段中<br>• 0x00040000 — 日志与 http 代理会话中的事务 (Proxy Transaction) 相对应<br>• 0x00020000 — 客户端到服务器的流量将根据策略转发<br>• 0x00010000 — 服务器到客户端的流量将根据策略转发<br>• 0x00008000 — 会话是指访问容器页面（容器页面）<br>• 0x00002000 — 会话暂时与处理应用程序相关性的隐式规则相匹配。在 PAN-OS 5.0.0 及更高版本中可用。<br>• 0x00000800 — 对称返回，用于转发会话的通信<br>• 0x00000400 — 解密流量通过镜像端口以明文发送<br>• 0x00000100 — 正在检查外部隧道中的有效负载 |
| IP 协议 (proto) | 与会话关联的 IP 协议。 |
| 操作 (action) | 对会话执行操作；可能的值为：<br>• 允许 — 策略允许对会话执行操作<br>• 拒绝 — 策略阻止对会话执行操作<br>• 丢弃 — 会话被静默丢弃<br>• 丢弃 ICMP — 会话被静默丢弃，有一条关于 ICMP 无法到达的消息发送至主机或应用程序<br>• 重置二者 — 会话被终止，TCP 重置发送至连接两端<br>• 重置客户端 — 会话被终止，TCP 重置发送至客户端<br>• 重置服务器 — 会话被终止，TCP 重置发送至服务器 |
| 隧道 (tunnel) | 隧道类型。 |
| 源 VM UUID (src_uuid) | VMware NSX 环境中来宾虚拟机的源通用唯一标识符。 |
| 目标 VM UUID (dst_uuid) | VMware NSX 环境中来宾虚拟机的目标通用唯一标识符。 |
| 规则 UUID (rule_uuid) | 永久标识规则的 UUID。 |
| 客户端到防火墙的阶段 (hs_stage_c2f) | TLS 握手从客户端到防火墙的阶段，例如，客户端 Hello、服务器 Hello、证书、客户端/服务器密钥交换等。 |
| 防火墙到客户端的阶段 (hs_stage_f2s) | TLS 握手从防火墙到服务器的阶段。 |
| TLS 版本 (tls_version) | 用于会话的 TLS 协议版本。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 密钥交换算法 (tls_keyxchg) | 用于会话的密钥交换算法。 |
| 加密算法 (tls_enc) | 用于加密会话数据的算法，例如 AES-128-CBC、 AES-256-GCM 等。 |
| 哈希算法 (tls_auth) | 用于会话的身份验证算法，例如，SHA、SHA256、SHA384 等。 |
| 策略名称 (policy_name) | 会话相关的解密策略的名称。 |
| 椭圆曲线 (ec_curve) | 客户端和服务器协商的椭圆加密曲线，用于使用 ECDHE 加密套件的连接。 |
| 错误索引 (err_index) | 发生的错误类型：密码、资源、恢复、版本、协议、证书、功能或 HSM。 |
| 根状态 (root_status) | 根证书的状态，例如，可信、不可信或未检查。 |
| 链状态 (chain_status) | 链是否可信。值为：<br>• 未检查<br>• 不可信<br>• 可信<br>• 不完整 |
| 代理类型 (proxy_type) | 解密代理类型，例如，转发代理的转发、入站检查的入站、未解密流量的不解密、解密代理、GlobalProtect 等。 |
| 证书序列号 (cert_serial) | 证书唯一标识符，由证书颁发机构生成。 |
| 证书指纹 (fingerprint) | 证书哈希，格式为二进制 x509。 |
| 证书开始日期 (notbefore) | 证书开始生效的日期（证书在此日期之前是无效的）。 |
| 证书结束日期 (notafter) | 证书到期的日期（证书在此日期之后将失效）。 |
| 证书版本 (cert_ver) | 证书的版本（V1、V2 或 V3）。 |
| 证书大小 (cert_size) | 证书密钥大小。 |
| 通用名称长度(cn_len) | 主题通用名称的长度。 |
| 颁发机构通用名称长度 (issuer_len) | 颁发机构通用名称的长度。 |
| 根通用名称长度 (rootcn_len) | 根通用名称的长度。 |
| SNI 长度 (sni_len) | 服务器名称指示（主机名）的长度。 |
| 证书标志 (cert_flags) | 证书标志可以返回 7 个值：<br>• 会话已恢复 (b_resume_session)<br>• 证书（主题）通用名称被截断 (b_cert_cn_truncated)<br>• 颁发机构通用名称被截断 (b_issuer_cn_truncated) |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • 根通用名称被截断 (b_root_cn_truncated)<br>• 服务器名称指示 (SNI) 被截断 (b_sni_truncated)<br>• 证书类型，RSA 或 ECDSA (b_cert_type)<br>• 未使用 (padding3) |
| 主题通用名称 (cn) | 域名（证书保护的服务器名称）。 |
| 颁发机构通用名称 (issuer_cn) | 用于验证证书内容的组织的名称。 |
| 根通用名称 (root_cn) | 根证书颁发机构名称。 |
| 服务器名称指示 (sni) | 客户端尝试连接的服务器的主机名。使用 SNI 可使服务器托管多个网站，并在同一 IP 地址和 TCP 端口上显示多个证书，因为每个网站的 SNI 都是唯一的。 |
| 错误 (error) | 显示事件中发生的错误的字符串。 |
| 容器 ID (container_id) | 防火墙在云容器中运行时用于标识容器的唯一字母数字字符串。 |
| POD 命名空间 (pod_namespace) | Kubernetes pod 命名空间的名称。 |
| POD 名称 (pod_name) | Kubernetes pod 的名称。 |
| 源外部动态列表 (src_edl) | 包含流量源 IP 地址的外部动态列表名称。 |
| 目标外部动态列表 (dst_edl) | 包含流量目标 IP 地址的外部动态列表名称。 |
| 源动态地址组 (src_dag) | 被 Device-ID 标识为流量源的动态地址组。 |
| 目标动态地址组 (dst_dag) | 被 Device-ID 标识为流量目标的动态地址组。 |
| 高分辨率时间戳 (high_res_timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-* |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | *OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 *1969-12-31T16:00:00:000-8:00* 。 |
| 源设备类别 (src_category) | 被 Device-ID 标识为流量源的设备的类别。 |
| 源设备配置文件 (src_profile) | 被 Device-ID 标识为流量源的设备的设备配置文件。 |
| 源设备型号(src_model) | 被 Device-ID 标识为流量源的设备的型号。 |
| 源设备供应商 (src_vendor) | 被 Device-ID 标识为流量源的设备的供应商。 |
| 源设备 OS 系列 (src_osfamily) | 被 Device-ID 标识为流量源的设备的操作系统类型。 |
| 源设备 OS 版本 (src_osversion) | 被 Device-ID 标识为流量源的设备的操作系统版本。 |
| 源主机名 (src_host) | 被 Device-ID 标识为流量源的设备的主机名。 |
| 源 MAC 地址 (src_mac) | 被 Device-ID 标识为流量源的设备的 MAC 地址。 |
| 目标设备类别 (dst_category) | 被 Device-ID 标识为流量目标的设备的类别。 |
| 目标设备配置文件 (dst_profile) | 被 Device-ID 标识为流量目标的设备的配置文件。 |
| 目标设备型号 (dst_model) | 被 Device-ID 标识为流量目标的设备的型号。 |
| 目标设备供应商(dst_vendor) | 被 Device-ID 标识为流量目标的设备的供应商。 |
| 目标设备 OS 系列 (dst_osfamily) | 被 Device-ID 标识为流量目标的设备的操作系统类型。 |
| 目标设备 OS 版本 (dst_osversion) | 被 Device-ID 标识为流量目标的设备的操作系统版本。 |
| 目标主机名 (dst_host) | 被 Device-ID 标识为流量目标的设备的主机名。 |
| 目标 MAC 地址(dst_mac) | 被 Device-ID 标识为流量目标的设备的 MAC 地址。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |


© 2019 Palo Alto Networks, Inc.

## 隧道检测日志字段

格式：FUTURE_USE，接收时间，序列号，类型，子类型，FUTURE_USE，生成时间，源地址，目标地址，NAT 源 IP，NAT 目标 IP，规则名称，源用户，目标用户，应用程序，虚拟系统，源区域，目标区域，入站接口，出站接口，日志操作，FUTURE_USE，会话 ID，重复次数，源端口，目标端口，NAT 源端口，NAT 目标端口，标志，协议，操作，严重性，序号，操作标志，源位置，目标位置，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，隧道 ID/IMSI，监控标记/IMEI，父会话 ID，父启动时间，隧道，字节数，已发送字节数，已接收字节数，数据包，发送的数据包，接收的数据包，最大封装，未知协议，严格检查，隧道分片，已创建会话，已关闭会话，会话结束原因，操作源，启动时间，耗用时间，隧道检测规则，远程用户 IP，远程用户 ID，规则 UUID，PCAP ID，动态用户组，源外部动态列表，目标外部动态列表，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的月、日和时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 与会话相关的日志类型：START 或 END。 |
| 威胁/内容类型 (subtype) | 通信日志的子类型；值为开始、结束、丢弃和拒绝<br>• 开始 — 会话已开始<br>• 结束 — 会话已结束<br>• 丢弃 — 标识应用程序之前以及无规则允许执行会话时丢弃会话。<br>• 拒绝 — 标识应用程序之后，有规则阻止或无规则允许执行会话时丢弃会话。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 会话中数据包的源 IP 地址。 |
| 目标地址 (dst) | 会话中数据包的目标 IP 地址。 |
| NAT 源 IP (natsrc) | 如果执行源 NAT，则为 NAT 后源 IP 地址。 |
| NAT 目标 IP (natdst) | 如果执行目标 NAT，则为 NAT 后目标 IP 地址。 |
| 规则名称 (rule) | 会话上生效的安全策略规则的名称。 |
| 源用户 (srcuser) | 会话中数据包的源用户 ID。 |
| 目标用户 (dstuser) | 会话中数据包的目标用户 ID。 |
| 应用程序 (app) | 会话中使用的隧道协议。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源区域 (from) | 会话中数据包的源区域。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 目标区域 (to) | 会话中数据包的目标区域。 |
| 入站接口 (inbound_if) | 会话的源接口。 |
| 出站接口 (outbound_if) | 会话的目标接口。 |
| 日志操作 (logset) | 适用于会话的日志转发配置文件。 |
| 会话 ID (sessionid) | 正在记录的会话的会话 ID。 |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和子类型的会话数量。 |
| 源端口 (sport) | 会话利用的源端口。 |
| 目标端口 (dport) | 会话利用的目标端口。 |
| NAT 源端口 (natsport) | NAT 后源端口。 |
| NAT 目标端口 (natdport) | NAT 后目标端口。 |
| 标志 (flags) | 提供会话详细信息的 32 位字段；该字段可使用这些值与日志记录值进行 AND 运算解码：<br>• 0x80000000 — 有数据包捕获的会话 (PCAP)<br>• 0x02000000 — IPv6 会话<br>• 0x01000000 — SSL 会话已解密（SSL 代理）<br>• 0x00800000 — 已通过 URL 筛选拒绝会话<br>• 0x00400000 — 会话已执行 NAT 转换 (NAT)<br>• 0x00200000 — 通过身份验证门户捕获到会话的用户信息<br>• 0x00080000 — 源自代理的 X-Forwarded-For 值位于源用户字段中<br>• 0x00040000 — 日志与 http 代理会话中的事务（代理事务）相对应<br>• 0x00008000 — 会话是指访问容器页面（容器页面）<br>• 0x00002000 — 会话暂时与处理应用程序相关性的隐式规则相匹配。在 PAN-OS 5.0.0 及更高版本中可用。<br>• 0x00000800 — 对称返回，用于转发会话的通信 |
| IP 协议 (proto) | 与会话关联的 IP 协议。 |
| 操作 (action) | 对会话执行操作；可能的值为：<br>• 允许 — 策略允许对会话执行操作<br>• 拒绝 — 策略阻止对会话执行操作<br>• 丢弃 — 会话被静默丢弃<br>• 丢弃 ICMP — 会话被静默丢弃，有一条关于 ICMP 无法到达的消息发送至主机或应用程序<br>• 重置二者 — 会话被终止，TCP 重置发送至连接两端<br>• 重置客户端 — 会话被终止，TCP 重置发送至客户端<br>• 重置服务器 — 会话被终止，TCP 重置发送至服务器 |
| 严重性 (severity) | 与事件关联的严重性；值为：informational、low、medium、high 和 critical。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。PA-7000 系列防火墙不支持此字段。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 源位置 (srcloc) | 源国家/地区或专用地址的内部区域；最长为 32 个字节。 |
| 目标位置 (dstloc) | 目标国家/地区或专用地址的内部区域。最长为 32 个字节。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 隧道 ID (tunnelid) | 被检测隧道的 ID 或移动用户的国际移动订户标识 (IMSI) ID。 |
| 监控标记 (monitortag) | 为移动设备的隧道检测策略规则或国际移动设备标识 (IMEI) ID 配置的监控名称。 |
| 父会话 ID (parent_session_id) | 隧道会话中的会话 ID。仅适用于内部隧道（如为两级隧道）或内部内容（如为一级隧道）。 |
| 父启动时间 (parent_start_time) | 父隧道会话开始的年/月/日小时:分钟:秒。 |
| 隧道类型 (tunnel) | 隧道类型，如 GRE 或 IPSec。 |
| 字节数 (bytes) | 会话中的字节数。 |
| 已发送字节数 (bytes_sent) | 客户端到服务器方向的会话字节数。 |
| 已接收字节数 (bytes_received) | 从服务器到客户端方向的会话字节数。 |
| 数据包 (packets) | 会话的数据包总数（传输和接收）。 |
| 发送的数据包 (pkts_sent) | 从客户端到服务器的会话数据包数。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 接收的数据包 (pkts_received) | 从服务器到客户端的会话数据包数。 |
| 最大封装 (max_encap) | 数据包超过隧道检测策略规则中配置的最大封装级数时，防火墙丢弃的数据包数（如果超过最大隧道检测级别，则丢弃数据包）。 |
| 未知协议 (unknown_proto) | 数据包包含隧道检测策略规则中启用的未知协议时，防火墙丢弃的数据包数（如果隧道内存在未知协议，则丢弃数据包）。 |
| 严格检查 (strict_check) | 数据包中的隧道协议标头不符合隧道检测策略规则中启用的隧道协议 RFC 时，防火墙丢弃的数据包数（**Drop packet if tunnel protocol fails strict header check**（如果隧道协议未通过严格的标头检查，则丢弃数据包））。 |
| 隧道分片 (tunnel_fragment) | 防火墙因分片错误而丢弃的数据包数。 |
| 已创建会话 (sessions_created) | 已创建的内部会话数。 |
| 已关闭会话 (sessions_closed) | 创建的已完成/已关闭会话数。 |
| 会话结束原因 (session_end_reason) | 会话终止原因。如果导致终止的原因有多个，那么该字段只会显示优先级最高的原因。以下是按照优先级进行排序的可能会话结束原因值（第一个优先级最高）：<br>• 威胁 — 防火墙检测到与重置、丢弃或阻止（IP 地址）操作相关的威胁。<br>• 策略拒绝 — 会话与包含拒绝或丢弃操作的安全策略匹配。<br>• decrypt-cert-validation（解密证书验证）— 会话终止，因为您配置防火墙在此会话使用的客户端身份验证或当此会话使用的服务器证书处于以下任一情况时，阻挡 SSL 转发代理解密或 SSL 入站检查：已过期、不可信的颁发者、未知状态或状态验证超时。当服务器证书产生类型为 bad_certificate、unsupported_certificate、certificate_revoked、access_denied 或 no_certificate_RESERVED（仅针对 SSLv3）的致命错误警报时，也会显示此会话终止原因。<br>• decrypt-unsupport-param（解密不支持参数）— 会话终止，因为您配置防火墙在此会话使用不受支持的协议版本、密码或 SSH 算法时，阻挡 SSL 转发代理解密或 SSL 入站检查。当此会话产生类型为 unsupported_extension、unexpected_message 或 handshake_failure 的致命错误警报时，也会显示此会话终止原因。<br>• decrypt-error（解密错误）— 会话终止，因为您配置防火墙在防火墙资源或硬件安全模块 (HSM) 不可用时，阻挡 SSL 转发代理解密或 SSL 入站检查。当您配置防火墙在产生了 SSH 错误或任何除针对解密证书验证和解密不支持参数终止原因之外的致命错误时，阻挡 SSL 流量。<br>• tcp-rst-from-client — 客户端向服务器发送 TCP 重置。<br>• tcp-rst-from-server — 服务器向客户端发送 TCP 重置。<br>• resources-unavailable — 会话因系统资源限制而丢弃。例如，会话可能已超出每个流允许的失序数据包数或全局失序数据包队列。<br>• tcp-fin — 连接中的一个或两个主机发送了用于关闭会话的 TCP FIN 消息。<br>• tcp-reuse — 有会话被重复使用，防火墙关闭了之前的会话。<br>• decoder — 解码器检测到使用协议（如 HTTP 代理）的新连接并结束了之前的连接。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • aged-out — 会话已老化。<br>• unknown — 此值适用于以下情况：<br>  • 上述原因未包含的会话终止（例如 `clear session all` 命令）。<br>  • 对于在不支持会话结束原因字段的 PAN-OS 版本（低于 PAN-OS 6.1 的版本）中生成的日志，在升级到当前 PAN-OS 版本或将日志加载到防火墙后，该值将变为 `unknown`。<br>  • 在 Panorama 中，如果日志接收自 PAN-OS 版本无法提供相应会话结束原因支持的防火墙，那么值为 `unknown`。<br>• n/a — 此值适用于流量日志类型不为 **end** 的情况。 |
| 操作源 (action_source) | 指定是否执行操作以允许或阻止在应用程序或策略中定义的某个应用程序。对会话的操作可能是允许、拒绝、重置服务器、重置客户端、重置两者。 |
| 启动时间 (start) | 会话开始的年/月/日小时:分钟:秒。 |
| 耗用时间 (elapsed) | 会话的耗用时间。 |
| 隧道检测规则 (tunnel_insp_rule) | 与明文隧道流量匹配的隧道检测规则的名称。 |
| 远程用户 IP (remote_user_ip) | 远程用户的 IPv4 或 IPv6 地址。 |
| 远程用户 ID (remote_user_id) | 远程用户的 IMSI 标识，如果可用，还有一个 IMEI 标识或一个 MSISDN 标识。 |
| 安全规则 UUID (rule_uuid) | 永久标识规则的 UUID。 |
| PCAP ID (pcap_id) | 用于定义防火墙上 pcap 文件位置的唯一数据包捕获 ID。 |
| 动态用户组名称 (dynusergroup_name) | 包含发起会话的用户的动态用户组的名称。 |
| 源外部动态列表 (src_edl) | 包含流量源 IP 地址的外部动态列表名称。 |
| 目标外部动态列表 (dst_edl) | 包含流量目标 IP 地址的外部动态列表名称。 |
| 高分辨率时间戳 (high_res timestamp) | 在管理面板上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br><br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 *1969-12-31T16:00:00:000-8:00* 。 |

## *SCTP* 日志字段

格式：FUTURE_USE，接收时间，序列号，类型，FUTURE_USE，FUTURE_USE，生成时间，源地址，目标地址，FUTURE_USE，FUTURE_USE，规则名称，FUTURE_USE，FUTURE_USE，FUTURE_USE，虚拟系统，源区域，目标区域，入站接口，出站接口，日志操作，FUTURE_USE，会话 ID，重复计数，源端口，目标端口，源端口，FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE，IP 协议，操作，设备组层次结构级别 1， 设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，序列号， FUTURE_USE，SCTP 关联 ID，有效载荷协议 ID，严重性，SCTP 块类型，FUTURE_USE，SCTP 验证标记 1， SCTP 验证标记 2，SCTP 原因代码，Diameter 命令代码，Diameter AVP 代码，SCTP 流 ID，SCTP 关联结束原因，操作代码，SCCP 主叫方 SSN，SCCP 主叫方全局标题，SCTP 筛选器，SCTP 块，发送的 SCTP 块，接收的 SCTP 块，数据包，发送的数据包，接收的数据包，规则 UUID，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 SCTP。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 原始会话源 IP 地址。 |
| 目标地址 (dst) | 原始会话目标 IP 地址。 |
| 规则名称 (rule) | 会话上生效的安全策略规则的名称。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源区域 (from) | 会话的源区域。 |
| 目标区域 (to) | 会话的目标区域。 |
| 入站接口 (inbound_if) | 会话的源接口。 |
| 出站接口 (outbound_if) | 会话的目标接口。 |
| 日志操作 (logset) | 适用于会话的日志转发配置文件。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 会话 ID (sessionid) | 应用于每个会话的内部数字标识符。 |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和子类型的会话数量。 |
| 源端口 (sport) | 会话利用的源端口。 |
| 目标端口 (dport) | 会话利用的目标端口。 |
| IP 协议 (proto) | 与会话关联的 IP 协议。 |
| 操作 (action) | 对会话执行操作；可能的值为：<br>• 允许 — 策略允许对会话执行操作<br>• 拒绝 — 策略阻止对会话执行操作 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| SCTP 关联 ID (assoc_id) | 应用于每个 SCTP 关联的内部 56 位数字逻辑标识符。 |
| 有效载荷协议 ID (ppid) | 标识触发此事件的数据块中的有效载荷协议 ID (PPID)。PPID 由互联网号码分配机构 (IANA) 分配。 |
| 严重性 (severity) | 与事件关联的严重性；值为：informational、low、medium、high 和 critical。 |
| SCTP 块类型 (sctp_chunk_type) | 描述块中所含信息的类型，例如控制或数据。 |
| SCTP 事件类型 (sctp_event_type) | 当 SCTP 保护配置文件应用于 SCTP 流量时，定义每个 SCTP 块或数据包触发的事件。也可由 SCTP 关联的开始或结束触发。 |
| SCTP 验证标记 1 (verif_tag_1) | 发起关联的 endpoint1 用于验证接收到的 SCTP 数据包是否属于当前 SCTP 关联，并对 endpoint2 进行验证。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| SCTP 验证标记 2 (verif_tag_2) | endpoint2 用于验证接收到的 SCTP 数据包是否属于当前 SCTP 关联，并对 endpoint1 进行验证。 |
| SCTP 原因代码 (sctp_cause_code) | 端点发送用于将错误条件的原因发送给相同 SCTP 关联的其他端点。 |
| Diameter 应用程序 ID (diam_app_id) | 触发事件的数据块中的 Diameter 应用程序。Diameter 应用程序 ID 由互联网号码分配机构 (IANA) 分配。 |
| Diameter 命令代码 (diam_cmd_code) | 触发事件的数据块中的 Diameter 命令代码。Diameter 命令代码由互联网号码分配机构 (IANA) 分配。 |
| Diameter AVP 代码 (diam_avp_code) | 触发事件的数据块中的 Diameter AVP 代码。 |
| SCTP 流 ID (stream_id) | 携带触发事件数据块的流 ID。 |
| SCTP 关联结束原因 (assoc_end_reason) | 关联终止的原因。如果有多个原因导致关联终止，则显示最高优先级的原因。会话可能结束原因按优先级递减的方式显示如下：<br>• shutdown-from-endpoint（最高优先级）— 端点发出 SHUTDOWN<br>• abort-from-endpoint — 端点发出 ABORT<br>• unknown（最低优先级）— 关联过期，或是关联是因为上述原因之外的因素终止（例如，clear session all 命令）。 |
| 操作代码 (op_code) | 在触发事件的数据块中标识 MAP 或 CAP 等应用层 SS7 协议的操作代码。 |
| SCCP 主叫方 SSN (sccp_calling_ssn) | 触发事件的数据块中信令连接控制部分 (SCCP) 主叫方子系统号码 (SSN)。 |
| SCCP 主叫方全局标题 (sccp_calling_gt) | 触发事件的数据块中信令连接控制部分 (SCCP) 主叫方全局标题 (GT)。 |
| SCTP 筛选器 (sctp_filter) | 与 SCTP 块匹配的筛选器名称。 |
| SCTP 块 (chunks) | 关联的总块数（传输和接收） |
| 发送的 SCTP 块 (chunks_sent) | 关联的 endpoint1（发起关联）-to-endpoint2 块数。 |
| 接收的 SCTP 块 (chunks_received) | 关联的 endpoint2-to-endpoint1（发起关联）块数。 |
| 数据包 (packets) | 会话的数据包总数（传输和接收）。 |
| 发送的数据包 (pkts_sent) | 从客户端到服务器的会话数据包数。 |
| 接收的数据包 (pkts_received) | 从服务器到客户端的会话数据包数。 |
| 规则 UUID (rule_uuid) | 永久标识规则的 UUID。 |
| 高分辨率时间戳 (high_res_timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD： |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | • **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>  从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00.000-8:00` 。 |

## 身份验证日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，虚拟系统，源 IP，用户，标准化用户，对象，身份验证策略，重复计数，身份验证 ID，供应商，日志操作，服务器配置文件，说明，客户端类型，事件类型，因素编号，序列号，操作标志，设备组层次结构 1，设备组层次结构 2，设备组层次结构 3，设备组层次结构 4，虚拟系统名称，设备名称，虚拟系统 ID，身份验证协议，规则 UUID，高分辨率时间戳，源设备类别，源设备配置文件，源设备型号，源设备供应商，源设备 OS 系列，源设备 OS 版本，源主机名，源 Mac 地址

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的设备的序列号。 |
| 类型 (type) | 指定日志类型；值为 AUTHENTICATION。 |
| 威胁/内容类型 (subtype) | 系统日志的子类型；指生成日志的系统守护程序；值为加密、dhcp、dnsproxy、dos、常规、全局保护、ha、hw、nat、ntpd、pbf、端口、pppoe、ras、路由、satd、sslmgr、sslvpn、用户 ID、url 筛选、vpn。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源 IP (ip) | 原始会话源 IP 地址。 |
| 用户 (user) | 进行身份验证的最终用户。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 标准化用户 (normalize_user) | 进行身份验证的标准化版本用户名（例如将域名附加到用户名）。 |
| 对象 (object) | 与系统事件关联的对象的名称。 |
| 身份验证策略 (authpolicy) | 在允许访问受保护资源之前调用以进行身份验证的策略。 |
| 重复次数 (repeatcnt) | 在 5 秒钟内显示相同源 IP、目标 IP、应用程序和子类型的会话数量。 |
| 身份验证 ID (authid) | 通过主要身份验证和其他（多重因素）身份验证提供的唯一 ID。 |
| 供应商 (vendor) | 提供其他多重因素身份验证的供应商。 |
| 日志操作 (logset) | 日志操作 (logset) |
| 服务器配置文件 (serverprofile) | 用于身份验证的身份验证服务器。 |
| 说明 (desc) | 其他身份验证信息。 |
| 客户端类型 (clienttype) | 用于完成身份验证的客户端类型（例如，身份验证门户）。 |
| 事件类型 (event) | 身份验证尝试的结果。 |
| 因素编号 (factorno) | 指使用主要身份验证 (1) 或其他因素 (2, 3)。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符。每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 虚拟系统 ID (vsys_id) | Palo Alto Networks 防火墙上的虚拟系统的唯一标识符。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 身份验证协议 (authproto) | 指服务器使用的身份验证协议。例如，PEAP with GTC。 |
| 规则 UUID (rule_uuid) | 永久标识规则的 UUID。 |
| 高分辨率时间戳 (high_res_timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00:000-8:00` 。 |
| 源设备类别 (src_category) | 被 Device-ID 标识为流量源的设备类别。 |
| 源设备配置文件 (src_profile) | 被 Device-ID 标识为流量源的设备的配置文件。 |
| 源设备型号(src_model) | 被 Device-ID 标识为流量源的设备的型号。 |
| 源设备供应商 (src_vendor) | 被 Device-ID 标识为流量源的设备的供应商。 |
| 源设备 OS 系列 (src_osfamily) | 被 Device-ID 标识为流量源的设备的操作系统类型。 |
| 源设备 OS 版本 (src_osversion) | 被 Device-ID 标识为流量源的设备的操作系统版本。 |
| 源主机名 (src_host) | 被 Device-ID 标识为流量源的设备的主机名。 |
| 源 MAC 地址 (src_mac) | 被 Device-ID 标识为流量源的设备的 MAC 地址。 |

## 配置日志字段

格式：FUTURE_USE，接收时间，序列号，类型，子类型，FUTURE_USE，生成时间，主机，虚拟系统，命令，管理员，客户端，结果，配置路径，更改详细信息前，更改详细信息后，序号，操作日志，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，设备组，审核注释



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的设备的序列号。 |
| 类型 (type) | 指定日志类型；值为 CONFIG。 |
| 威胁/内容类型 (subtype) | 配置日志的子类型；未使用。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 主机 (host) | 客户端计算机的主机名称或 IP 地址 |
| 虚拟系统 (vsys) | 与配置日志关联的虚拟系统 |
| 命令 (cmd) | 由管理员执行的命令，值为添加、复制、提交、删除、编辑、移动、重命名、设置。 |
| 管理员 (admin) | 执行配置的管理员的用户名 |
| 客户端 (client) | 管理员使用的客户端；值为 Web 和 CLI |
| 结果 (result) | 配置操作的结果；值为已提交配置、配置成功、配置失败和未授权配置 |
| 配置路径 (path) | 发出配置命令的路径；最长为 512 个字节 |
| 变更前详细信息 (before_change_detail) | 此字段仅位于自定义日志中；不在默认格式下。<br>配置变更前包含完整的 xpath。 |
| 变更后详细信息 (after_change_detail) | 此字段仅位于自定义日志中；不在默认格式下。<br>配置变更后包含完整的 xpath。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一： |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 设备组 (dg_id) | 防火墙所属的设备组（如果由 Panorama™ 管理服务器托管）。 |
| 审核注释 (comment) | 在策略规则配置更改中输入的审核注释。 |

## 系统日志字段

格式：FUTURE_USE，接收时间，序列号，类型，内容/威胁类型，FUTURE_USE，生成时间，虚拟系统，事件 ID，对象， FUTURE_USE，FUTURE_USE，模块，严重性，说明， 序号，操作标志，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，FUTURE_USE，FUTURE_USE，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 SYSTEM。 |
| 内容/威胁类型 (subtype) | 系统日志的子类型；指生成日志的系统守护程序；值为加密、dhcp、dnsproxy、dos、常规、全局保护、ha、hw、nat、ntpd、pbf、端口、pppoe、ras、路由、satd、sslmgr、sslvpn、用户 ID、url 筛选、vpn。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 虚拟系统 (vsys) | 与配置日志关联的虚拟系统。 |
| 事件 ID (eventid) | 显示事件名称的字符串。 |
| 对象 (object) | 与系统事件关联的对象的名称。 |
| 模块 (module) | 当子类型字段的值为常规时，该字段才有效。它提供与生成日志的子系统相关的其他信息；值为常规、管理、授权、ha、升级、机壳。 |
| 严重性 (severity) | 与事件关联的严重性；值为：informational、low、medium、high 和 critical。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 说明 (opaque) | 事件的详细说明；最长为 512 个字节。 |
| 序号 (seqno) | 递增的 64 位日志条目标识符；每个日志类型都有唯一的编号空间。 |
| 操作标志 (actionflags) | 指示日志是否已转发到 Panorama 的位字段。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 高分辨率时间戳 (high_res_timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>从运行 *PAN-OS 10.0* 以及更高版本受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 *1969-12-31T16:00:00:000-8:00* 。 |

## 关联事件日志字段

格式：FUTURE_USE，接收时间，序列号，类型，内容/威胁类型，FUTURE_USE，生成时间，源地址。源用户，虚拟系统，类别，严重性，设备组层次结构级别 1，设备组层次结构级别 2，设备组层次结构级别 3，设备组层次结构级别 4，虚拟系统名称，设备名称，虚拟系统 ID，对象名称，对象 ID，证据


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间。 |
| 序列号 (serial) | 生成日志的设备的序列号。 |
| 类型 (type) | 指定日志类型；值为 CORRELATION。 |
| 内容/威胁类型 (subtype) | 系统日志的子类型；指生成日志的系统守护程序；值为加密、dhcp、dnsproxy、dos、常规、全局保护、ha、hw、nat、ntpd、pbf、端口、pppoe、ras、路由、satd、sslmgr、sslvpn、用户 ID、url 筛选、vpn。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 启动事件的用户的 IP 地址。 |
| 源用户 (srcuser) | 启动事件的用户的用户名。 |
| 虚拟系统 (vsys) | 与配置日志关联的虚拟系统。 |
| 类别 (category) | 针对网络、用户或主机的威胁或伤害的类型的摘要。 |
| 严重性 (severity) | 与事件关联的严重性；值为：informational、low、medium、high 和 critical。 |
| 设备组层次结构（dg_hier_level_1 至 dg_hier_level_4） | 一系列标识号，表示设备组在设备组层次结构中的位置。生成日志的防火墙（或虚拟系统）包括每个父级在其设备组层次结构中的标识号。共享设备组（级别 0）不包括在此结构中。<br>如果日志值为 12、34、45、0，其含义是日志是由属于设备组 45 的防火墙（或虚拟系统）生成的，其父级为 34 和 12。要查看与值 12、34 或 45 对应的设备组名称，请使用以下方法之一：<br>API 查询：<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| 虚拟系统名称 (vsys_name) | 与会话关联的虚拟系统的名称；仅在为多个虚拟系统启用的防火墙上有效。 |
| 设备名称 (device_name) | 在其上记录会话的防火墙的主机名。 |
| 虚拟系统 ID (vsys_id) | Palo Alto Networks 防火墙上的虚拟系统的唯一标识符。 |
| 对象名称 (objectname) | 匹配的关联对象的名称。 |
| 对象 ID (object_id) | 与系统事件关联的对象的名称。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 证据 (evidence) | 一份摘要陈述，指示主机与关联对象中定义的条件相匹配的次数。例如，主机访问已知恶意软件 URL（19 次）。 |

## GTP 日志字段

格式：FUTURE_USE，接收时间，序列号，类型，威胁/内容类型，FUTURE_USE，生成时间，源地址，目标地址，FUTURE_USE，FUTURE_USE，规则名称，FUTURE_USE，FUTURE_USE，应用程序，虚拟系统，源区域，目标区域，入站接口，出站接口，日志操作，FUTURE_USE，会话 ID，FUTURE_USE，源端口，目标端口，FUTURE_USE，FUTURE_USE，FUTURE_USE，协议，操作，GTP 事件类型，MSISDN，访问点名称，无线访问技术，GTP 消息类型，最终用户 IP 地址，隧道端点标识符 1，隧道端点标识符 2，GTP 接口，GTP 原因，严重性，服务国家 MCC，服务网络 MNC，区域代码，单元 ID，GTP 事件代码，FUTURE_USE，FUTURE_USE，源位置，目标位置，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，隧道 ID/IMSI，监视器标签/
IMEI，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，FUTURE_USE，开始时间，耗用时间，隧道检测规则，远程用户 IP，远程用户 ID，规则 UUID，PCAP ID，高分辨率时间戳

| 字段名称 | 说明 |
| --- | --- |
| 接收时间 (receive_time 或 cef-formatted-receive_time) | 在管理面板上接收日志的时间（月，日，时）。 |
| 序列号 (serial) | 生成日志的防火墙的序列号。 |
| 类型 (type) | 指定日志类型；值为 GTP。 |
| 威胁/内容类型 (subtype) | 通信日志的子类型；值为开始、结束、丢弃和拒绝。<br>• 开始 — 会话已开始<br>• 结束 — 会话已结束<br>• 丢弃 — 标识应用程序之前以及无规则允许执行会话时丢弃会话。<br>• 拒绝 — 标识应用程序之后，有规则阻止或无规则允许执行会话时丢弃会话。 |
| 生成时间 (time_generated 或 cef-formatted-time_generated) | 是指在数据面板上生成日志的时间。 |
| 源地址 (src) | 会话中数据包的源 IP 地址。 |
| 目标地址 (dst) | 会话中数据包的目标 IP 地址。 |
| 规则名称 (rule) | 会话上生效的安全策略规则的名称。 |
| 应用程序 (app) | 会话中使用的隧道协议。 |
| 虚拟系统 (vsys) | 与会话关联的虚拟系统。 |
| 源区域 (from) | 会话中数据包的源区域。 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 目标区域 (to) | 会话中数据包的目标区域。 |
| 入站接口 (inbound_if) | 会话的源接口。 |
| 出站接口 (outbound_if) | 会话的目标接口。 |
| 日志操作 (logset) | 适用于会话的日志转发配置文件。 |
| 会话 ID (sessionid) | 正在记录的会话的会话 ID。 |
| 源端口 (sport) | 会话利用的源端口。 |
| 目标端口 (dport) | 会话利用的目标端口。 |
| IP 协议 (proto) | 与会话关联的 IP 协议。 |
| 操作 (action) | 对会话执行操作；可能的值为：<br>• 允许 — 策略允许对会话执行操作<br>• 拒绝 — 策略阻止对会话执行操作 |
| GTP 事件类型 (event_type) | 定义检查 GTP 保护配置文件时 GTP 消息触发的事件是否适用于 GTP 流量。启动或结束 GTP 会话也会触发。 |
| MSISDN (msisdn) | 与由国家代码、国家目的地代码和订户组成的移动订户相关联的服务标识。包含十进制数字 (0-9)，最多只能包含 15 位数字。 |
| 访问点名称 (apn) | 参考移动网络中的数据包数据网络数据网关 (PGW)/ 网关 GPRS 支持节点。由一个强制的 APN 网络标识符和一个可选的 APN 运算符标识符组成。 |
| 无线访问技术 (rat) | 用于无线访问的技术类型。例如，EUTRAN、WLAN、Virtual、HSPA Evolution、GAN 和 GERAN。 |
| GTP 消息类型 (msg_type) | 表示 GTP 消息类型。 |
| 结束 IP 地址 (end_ip_adr) | 由 PGW/GGSN 分配的移动订户 IP 地址。 |
| 隧道端点标识符 1 (teid1) | 标识网络节点中的 GTP 隧道。TEID1 是 GTP 消息中的第一个 TEID。 |
| 隧道端点标识符 2 (teid2) | 标识网络节点中的 GTP 隧道。TEID2 是 GTP 消息中的第二个 TEID。 |
| GTP 接口 (gtp_interface) | 接收 GTP 消息的 3GPP 接口。 |
| GTP 原因 (cause_code) | 日志中的 GTP 原因值响应提供有关接受或拒绝网络节点提出的 GTP 请求的信息的信息元素。 |
| 严重性 (severity) | 与事件关联的严重性；值为：informational、low、medium、high 和 critical。 |
| 服务网络 MCC (mcc) | 服务核心网络运营商的移动国家代码。 |



© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| 服务网络 MNC (mnc) | 服务核心网络运营商的移动网络代码。 |
| 区域代码 (area_code) | 公共陆地移动网 (PLMN) 内的区域。 |
| Cell ID (cell_id) | 区域代码内的基站。 |
| GTP 事件代码 (event_code) | 描述 GTP 事件的事件代码。 |
| 源位置 (srcloc) | 源国家/地区或专用地址的内部区域；最长为 32 个字节。 |
| 目标位置 (dstloc) | 目标国家/地区或专用地址的内部区域；最长为 32 个字节。 |
| 隧道 ID/IMSI (imsi) | 国际移动订户标识 (IMSI)是分配给 GSM/UMTS/EPS 系统中每个移动订户的唯一号码。IMSI 仅由十进制数字（0 到 9）组成，允许的最大位数为 15。 |
| 监控标记/IMEI (imei) | 国际移动订户标识 (IMSI)是分配给移动站每台设备的唯一的 15 或 16 位数字。 |
| 启动时间 (start) | 会话开始的时间。 |
| 耗用时间 (elapsed) | 会话的耗用时间。 |
| 隧道检测规则 (tunnel_insp_rule) | 与明文隧道流量匹配的隧道检测规则的名称 |
| 远程用户 IP (remote_user_ip) | 远程用户使用的 IPv4 或 IPv6 地址。 |
| 远程用户 ID (remote_user_id) | 远程用户的 IMSI 标识，如果可用，还有一个 IMEI 标识和/或一个 MSISDN 标识。 |
| 规则 UUID (rule_uuid) | 规则的通用唯一 ID。 |
| PCAP ID (pcap_id) | 用于查找保存在防火墙上 pcap 文件的唯一数据包捕获 ID。 |
| 高分辨率时间戳 (high_res_timestamp) | 在管理平面上接收日志的时间（以毫秒为单位）。<br>此新字段的格式为 YYYY-MM-DDThh:ss:sssTZD：<br>• **YYYY**— 四位数字年份<br>• **MM**— 两位数字月份<br>• **DD**— 两位数字日期（01 到 31）<br>• **T**— 指示时间戳开始的指示符<br>• **hh**— 使用 24 小时制的两位数字小时值（00 到 23）<br>• **mm**— 两位数字分钟值（00 到 59）<br>• **ss**— 两位数字分秒值（00 到 60）<br>• **sss**— 一位或多位数字毫秒值<br>• **TZD**— 时区指示符（+hh:mm 或 -hh:mm）<br>从运行 *PAN-OS 10.0* 以及更高版本的受管防火墙接收的日志支持高分辨率时间戳。无论什么时候接收日志，从运 |


© 2019 Palo Alto Networks, Inc.

| 字段名称 | 说明 |
| --- | --- |
| | 行 *PAN-OS 9.1* 以及更低版本受管防火墙接收的日志始终显示时间戳 `1969-12-31T16:00:00:000-8:00` 。 |

## *Syslog* 严重性

根据日志类型和内容设置 Syslog 严重性。

| 日志类型/严重性 | Syslog 严重性 |
| --- | --- |
| 通信 | 信息 |
| 配置 | 信息 |
| 威胁/系统 — 参考 | 信息 |
| 威胁/系统 — 低 | 通知 |
| 威胁/系统 — 中 | 警告 |
| 威胁/系统 — 高 | 警告 |
| 威胁/系统 — 严重 | 关键 |

## 自定义日志/事件格式

要通过外部日志解析系统促进集成，防火墙可让您自定义日志格式；还可让您添加自定义密匙：值属性对。可配置自定义消息格式，路径为：**Device**（设备）> **Server Profiles**（服务器配置文件）> **Syslog** > **Syslog Server Profile**（**Syslog** 服务器配置文件）> **Custom Log Format**（自定义日志格式）。

为了达到 ArcSight 常见事件格式 (CEF) 符合日志格式的目标，请参阅《CEF 配置指南》。

## 转义序列

含逗号或双引号的任何字段都必须加上双引号。此外，如果双引号出现在字段中，则必须在字段前加上其他双引号，对字段进行转义。要维护向后兼容性，则必须始终在威胁日志的杂项字段前添加双引号。



© 2019 Palo Alto Networks, Inc.

# SNMP 监控和陷阱

以下主题介绍 Palo Alto Networks 防火墙、Panorama 和 WF-500 设备如何实施 SNMP，以及配置 SNMP 监控和陷阱传送的程序。

- SNMP 支持
- 使用 SNMP 管理器浏览 MIB 和对象
- 为防火墙保护的网元启用 SNMP 服务
- 使用 SNMP 监控统计信息
- 将陷阱转发至 SNMP 管理器
- 支持的 MIB

## SNMP 支持

您可以使用 SNMP 管理器，来监控防火墙、Panorama 或 WF-500 设备的事件驱动警报和运行统计信息，以及它们处理的流量。统计信息和陷阱可以帮助您识别资源限制、系统更改或故障、恶意软件攻击。您可以通过将日志数据作为陷阱转发来配置警报，并能够在收到来自 SNMP 管理器的 GET 消息（请求）时发送统计信息作为响应。所有陷阱和统计信息都有对象标识符 (OID)。在您加载到 SNMP 管理器的管理信息库 (MIB) 内部，相关的 OID 以层次结构进行组织，以实现监控。

当某个事件触发了 *SNMP* 陷阱生成（例如，一个接口出现故障）时，防火墙、*Panorama* 虚拟设备、*M* 系列设备和 *WF-500* 设备通过更新对应的 *SNMP* 对象（例如，接口 *MIB*）来进行响应，而非等待所有对象每 *10* 秒钟进行的定期更新。这确保您的 *SNMP* 管理器在轮询对象确认事件时显示最新信息。

防火墙、Panorama 和 WF-500 设备支持 SNMP 2c 和 SNMP 3 这两个版本。请根据您网络上的其他设备支持的版本，以及您的网络安全要求，来决定使用哪个版本。SNMPv3 比 SNMPv2c 更加安全，而且实现了比后者更加精确的系统统计信息访问控制。下表总结了每种版本的安全功能。当您使用 SNMP 监控统计信息并将陷阱转发至 SNMP 管理器时，可以选择版本并配置安全功能。

| SNMP版本 | 身份验证 | 消息私密性 | 消息完整性 | MIB 访问粒度 |
|---|---|---|---|---|
| SNMPv2c | 社区字符串 | 否（明文） | 否 | 设备上的所有 MIB 的 SNMP 团体访问 |
| SNMPv3 | 引擎 ID、用户名和身份验证密码（密码的 SHA 哈希） | SNMP 消息的 AES 128 加密的隐私密码 | 是 | 基于包括或排除特定 OID 的视图的用户访问 |

在 SNMP 实施显示的部署中，防火墙将陷阱转发至 SNMP 管理器，同时还将日志转发至日志收集器。或者，您可以配置日志收集器，以便将防火墙陷阱转发至 SNMP 管理器。有关这些部署的详细信息，请参阅集中式日志记录和报告中的日志转发选项。在所有部署中，SNMP 管理器都直接从防火墙、Panorama 或 WF-500 设备获取统计信息。在本例中，单个 SNMP 管理器同时收集陷阱和统计信息，但如果单独的管理器更加适合您的网络，也可以使用单独的管理器。


© 2019 Palo Alto Networks, Inc.

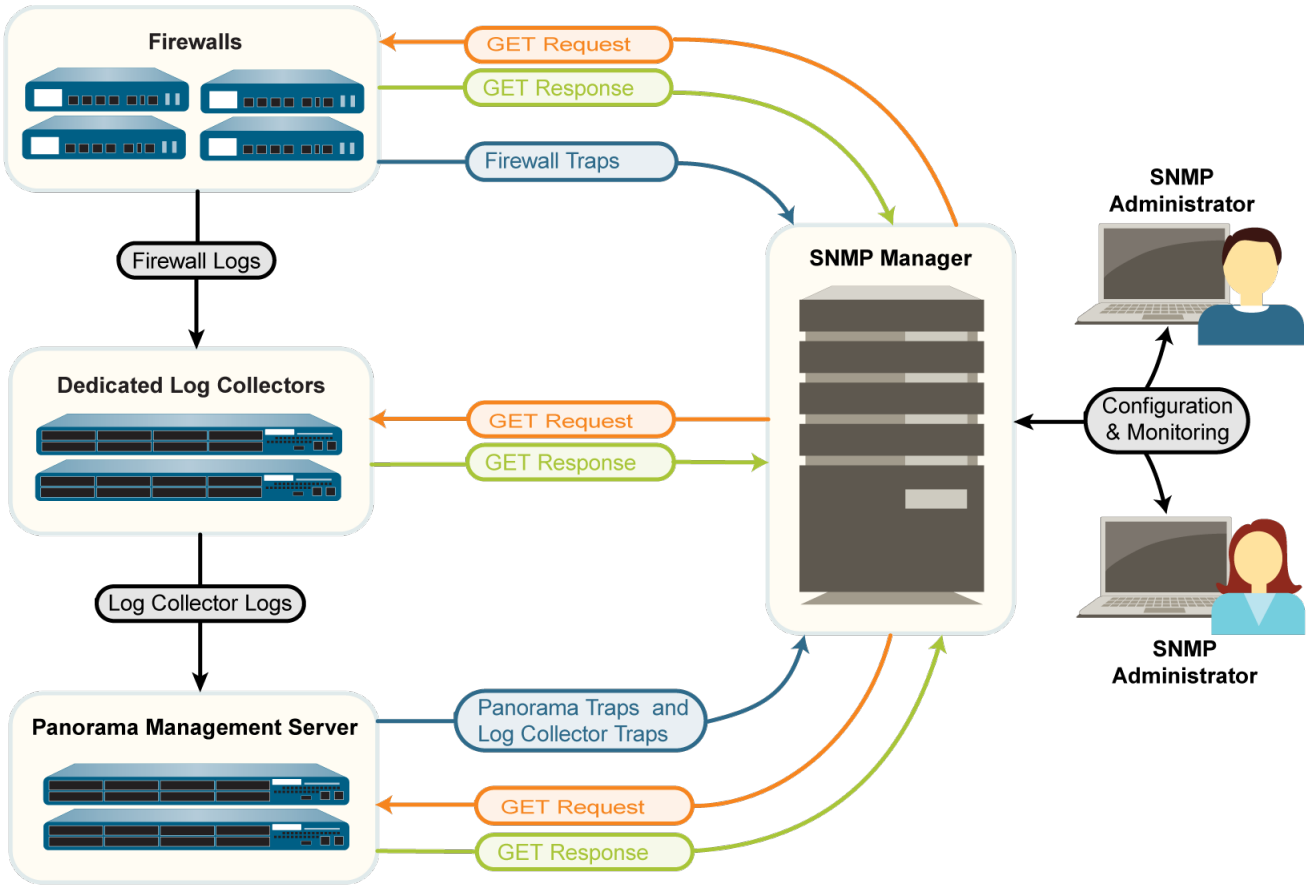



图 2: SNMP 实施

# 使用 SNMP 管理器浏览 MIB 和对象

要使用 SNMP 监控 Palo Alto Networks 防火墙、Panorama 或 WF-500 设备，您必须首先将支持的 MIB加载到 SNMP 管理器，并确定哪些对象标识符 (OID) 与您希望监控的系统统计信息和陷阱相对应。以下主题概述了如何在 SNMP 管理器中查找 OID 和 MIB。有关执行这些任务的具体步骤，请参阅 SNMP 管理软件。

- 识别包含已知 OID 的 MIB
- 对 MIB 执行 Walk
- 确定系统统计信息或陷阱的 OID

## 识别包含已知 *OID* 的 *MIB*

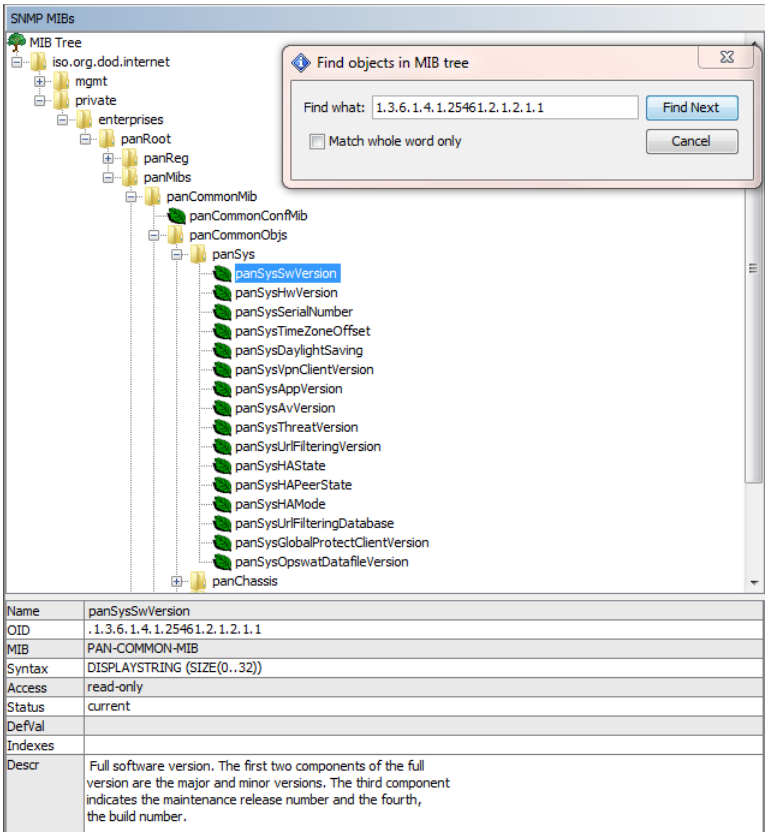
如果您已经知道了某个特定 SNMP 对象（统计信息或陷阱）的 OID，并希望知道类似对象的 OID，以便对其进行监控，您可以浏览包含已知 OID 的 MIB。

STEP 1 | 将所有支持的 MIB加载到 SNMP 管理器中。

STEP 2 | 在整个 MIB 树中搜索已知 OID。搜索结果显示 OID 的 MIB 路径，以及关于 OID 的信息（例如名称、状态和说明）。然后，您可在同一个 MIB 中搜索其他 OID，以查看关于它们的信息。



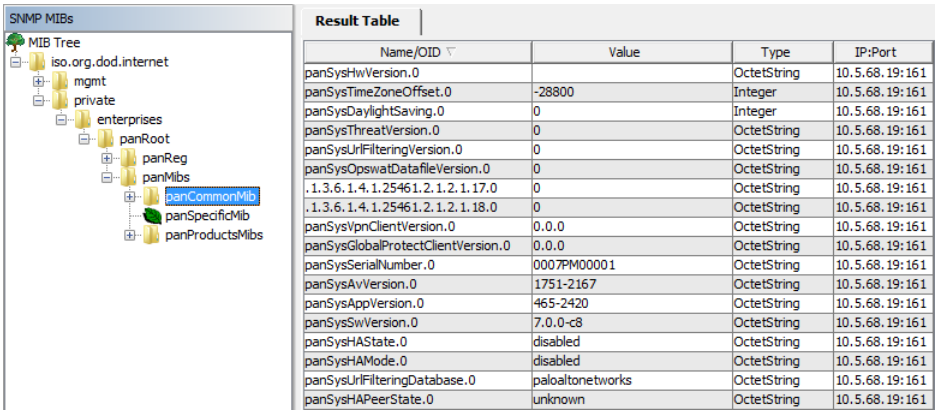
© 2019 Palo Alto Networks, Inc.




STEP 3 | （可选）对 MIB 执行 Walk以显示其所有对象。

## 对 *MIB* 执行 *Walk*

如果您希望查看哪些 SNMP 对象（统计信息和陷阱）可用于进行监控，那么显示特定 MIB 的所有对象可能是非常有用的。为此，请将支持的 MIB加载到您的 SNMP 管理器中，并对所需的 MIB 执行 *walk*。要列出 Palo Alto Networks 防火墙、Panorama 和 WF-500 设备的陷阱，请对 panCommonEventEventsV2 MIB 执行 Walk。在以下示例中，对PAN-COMMON-MIB.my执行 Walk 会显示 OID 列表，以及特定统计信息的 OID 值：




## 确定系统统计信息或陷阱的 *OID*

要使用 SNMP 管理器监控 Palo Alto Networks 防火墙、Panorama 或 WF-500 设备，您必须知道要监控的系统统计信息和陷阱的 OID。

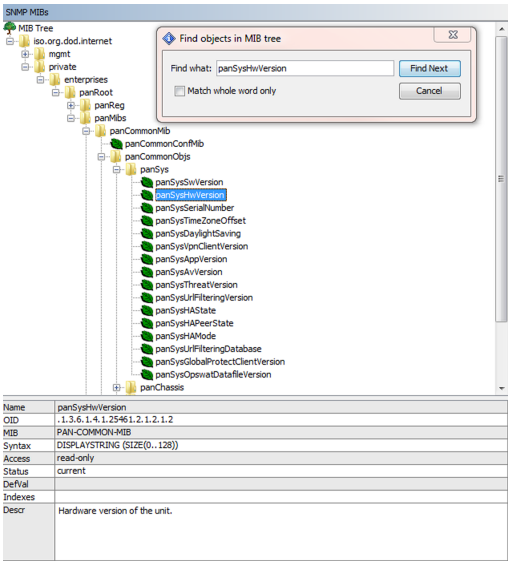

© 2019 Palo Alto Networks, Inc.

STEP 1 | 查看支持的 MIB 以确定哪个 MIB 包含您需要的统计信息类型。例如，PAN-COMMON-MIB.my 包含硬件版本信息。panCommonEventEventsV2 MIB 包含 Palo Alto Networks 防火墙、Panorama 和 WF-500 设备支持的所有陷阱。

STEP 2 | 在文本编辑器中打开 MIB 并执行关键字搜索。例如，使用 **Hardware version** 作为 PAN-COMMON-MIB 中的搜索字符串，可以确定 panSysHwVersion 对象：

```
panSysHwVersion OBJECT-TYPE
 SYNTAX DisplayString (SIZE(0..128))
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "Hardware version of the unit."
 ::= {panSys 2}
```

STEP 3 | 在 MIB 浏览器中，搜索 MIB 树以查找确定的对象名称，以便显示它的 OID。例如，panSysHwVersion 对象的 OID 是 1.3.6.1.4.1.25461.2.1.2.1.2。




# 为防火墙保护的网元启用 SNMP 服务

如果您要使用简单网络管理协议 (SNMP) 来监控或管理位于 Palo Alto Networks 防火墙安全区域内的网元（例如交换机或路由器），则必须创建一条安全规则，允许这些网元的 SNMP 服务。

您无需创建安全规则来启用 *Palo Alto Networks* 防火墙、*Panorama* 或 *WF-500* 设备的 *SNMP* 监控。有关详细信息，请参阅使用 SNMP 监控统计信息。

STEP 1 | 创建应用程序组。

1. 选择 **Objects**（对象）> **Application Group**（应用程序组），然后单击 **Add**（添加）。
2. 输入一个 **Name**（名称）来标识应用程序组。
3. 单击 **Add**（添加），键入 **snmp**，然后从下拉菜单中选择 **snmp** 和 **snmp-trap**。
4. 单击 **OK**（确定）以保存配置文件组。

STEP 2 | 创建安全规则以允许 SNMP 服务。

1. 选择 **Policies**（策略）> **Security**（安全），并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入网关的 **Name**（名称）。



© 2019 Palo Alto Networks, Inc.

3. 在 **Source**（源）和 **Destination**（目标）选项卡中，单击 **Add**（添加）并输入流量的 **Source Zone**（源区域）和 **Destination Zone**（目标区域）。
4. 在 **Applications**（应用程序）选项卡中，单击 **Add**（添加），键入刚创建的应用程序组对象的名称，然后从下拉列表中选择该名称。
5. 在 **Actions**（操作）选项卡中，确认 **Action**（操作）设置为 **Allow**（允许），然后单击 **OK**（确定）和 **Commit**（提交）。

# 使用 SNMP 监控统计信息

简单网络管理协议 (SNMP) 管理器从 Palo Alto Networks 防火墙收集到的统计信息有助于您了解网络的运行状况（系统和连接）、确定资源限制并监控流量或处理负载。统计信息包括接口状态（开启或关闭）、活动用户会话、并发会话、会话利用率、温度、系统正常运行时间等信息。

您可将 *SNMP* 管理器配置为控制 *Palo Alto Networks* 防火墙（使用 *SET* 消息），或仅从这些设备收集统计信息（使用 *GET* 消息）。有关如何为 *Palo Alto Networks* 防火墙实施 *SNMP* 的详细信息，请参阅 SNMP 支持 。

STEP 1 | 配置 SNMP 管理器以获取来自防火墙的统计信息。

以下步骤概述您在 SNMP 管理器上执行的任务。有关具体步骤，请参阅 SNMP 管理器的文档。

1. 若要启用 SNMP 管理器来解读防火墙统计信息，应加载 Palo Alto Networks 防火墙的配套 MIB，并在必要时编译它们。
2. 对于 SNMP 管理器将监控的每个防火墙，请定义防火墙的连接设置（IP 地址和端口）和身份验证设置（SNMPv2c 团体字符串或 SNMPv3 EngineID/用户/密码）。

   所有 *Palo Alto Networks* 防火墙都使用端口 *161*。

   对于多个防火墙，SNMP 管理器可以使用相同或不同的连接和身份验证设置。这些设置必须与您在防火墙上配置 SNMP 时定义的设置相匹配（请参阅步骤 3）。例如，如果使用 SNMPv2c，则您在配置防火墙时定义的团体字符串必须与您为 SNMP 管理器中为该防火墙定义的团体字符串相匹配。
3. 确定您要监控的统计信息的对象标识符 (OID)。例如，为了监控防火墙的会话利用率，MIB 浏览器显示此统计信息对应于 PAN-COMMON-MIB.my中的 OID 1.3.6.1.4.1.25461.2.1.2.3.1.0。有关详细信息，请参阅使用 SNMP 管理器浏览 MIB 和对象。
4. 配置 SNMP 管理器以监控所需的 OID。

STEP 2 | 支持防火墙接口上的 SNMP 流量。

这个接口将接收来自 SNMP 管理器的统计信息请求。

*PAN-OS* 不会同步高可用性 *(HA)* 配置中的防火墙的管理 *(MGT)* 接口设置。您必须为每个 *HA* 对配置接口。

在防火墙 Web 界面中执行此步骤。

- 要启动 MGT 接口上的 SNMP 流量，选择 **Device**（设备）> **Setup**（设置）> **Interfaces**（接口），编辑 **Management**（管理）设置，选择 **SNMP**，然后单击 **OK**（确定）和 **Commit**（提交）。
- 要启用任何其他接口上的 SNMP 流量，为 SNMP 服务创建一个接口管理配置文件，并将此配置文件分配给将接收 SNMP 请求的接口。接口类型必须为第 3 层以太网。

STEP 3 | 配置防火墙以响应来自 SNMP 管理器的统计信息请求。

*PAN-OS* 不会同步高可用性 *(HA)* 配置中的防火墙的 *SNMP* 响应设置。您必须为每个 *HA* 对配置这些设置。


© 2019 Palo Alto Networks, Inc.

1. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），并在其他部分中单击 **SNMP Setup**（**SNMP** 设置）。
2. 选择 SNMP **Version**（版本），并按照以下方式配置身份验证值。有关版本详细信息，请参阅 SNMP 支持。
   - **V2c** — 输入 **SNMP Community String**（**SNMP** 团体字符串），不但可用于识别 SNMP 管理器和监控设备的团体，并且还可用作密码，对团体成员彼此进行身份验证。

     作为最佳实践，不要使用默认团体字符串 ***public***；它是广为人知的，因此不太安全。
   - **V3** — 创建至少一个 SNMP 视图组和一个用户。当防火墙转发陷阱和 SNMP 管理器获取防火墙统计信息时，用户帐户和视图可提供身份验证、隐私和访问控制。
     - **Views**（视图）— 每个视图是一个配对的 OID 和位掩码：OID 指定 MIB，掩码（十六进制格式）指定可以在 MIB 内部（包括匹配）或外部（排除匹配）访问的对象。单击第一个列表中的 **Add**（添加），并输入视图组的 **Name**（名称）。对于组中的每个视图，单击 **Add**（添加）并配置视图 **Name**（名称）、**OID**、匹配 **Option**（选项）（**include**（包括）或 **exclude**（排除））以及 **Mask**（掩码）。
     - **Users**（用户）— 单击第二个列表中的 **Add**（添加），在 **Users**（用户）下输入用户名，从下拉菜单中选择 **View**（视图）组，输入用于向 SNMP 管理器进行身份验证的身份验证密码（**Auth Password**（身份验证密码）），并输入用于加密发往 SNMP 管理器的 SNMP 消息的隐私密码（**Priv Password**（隐私密码））。
3. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 4 | 在 SNMP 管理器中监控防火墙统计信息。

有关详细信息，请参阅 SNMP 管理器的文档。

监控与防火墙接口相关的统计信息时，必须将 *SNMP* 管理器中的接口索引与防火墙 *Web* 界面中的接口名称相匹配。有关详细信息，请参阅 SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符。

## 将陷阱转发至 SNMP 管理器

简单网络管理协议 (SNMP) 陷阱可向您发出警报，包括关于系统事件（Palo Alto Networks 防火墙的硬件或软件故障或更改）或威胁（与防火墙安全规则匹配的威胁）的警报，以引起您的即时关注。

要查看 *Palo Alto Networks* 防火墙支持的陷阱列表，请使用 *SNMP* 管理器访问 *panCommonEventEventsV2 MIB*。有关详细信息，请参阅使用 SNMP 管理器浏览 MIB 和对象。

有关 *Palo Alto Networks* 防火墙如何实施 *SNMP* 的详细信息，请参阅 SNMP 支持。

STEP 1 | 让 SNMP 管理器能够解释接收的陷阱。

加载 Palo Alto Networks 防火墙的支持的 MIB，并在必要时编译它们。有关具体步骤，请参阅 SNMP 管理器的文档。

STEP 2 | 配置 SNMP 陷阱服务器配置文件。

该配置文件定义防火墙如何访问 SNMP 管理器（陷阱服务器）。您最多只能为每个配置文件定义四个 SNMP 管理器。



© 2019 Palo Alto Networks, Inc.

或者，为不同的日志类型、严重性级别和 *WildFire* 判定配置单独的 *SNMP* 陷阱服务器配置文件。

1. 登录到防火墙 Web 界面。
2. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **SNMP Trap**（ **SNMP** 陷阱）。
3. 单击 **Add**（添加），然后输入配置文件的 **Name**（名称）。
4. 如果防火墙具有多个虚拟系统 (vsys)，请选择此配置文件可用的 **Location**（位置）（vsys 或 **Shared**（共享））。
5. 选择 SNMP **Version**（版本），并按照以下方式配置身份验证值。有关版本详细信息，请参阅 SNMP 支持。
   - **V2c** — 对于每台服务器，请单击 **Add**（添加）并输入服务器 **Name**（名称）、IP 地址（**SNMP Manager**（**SNMP** 管理器））以及 **Community String**（团体字符串）。团体字符串可用于识别 SNMP 管理器和监控设备的团体，并且还可用作密码，对团体成员彼此进行身份验证。

     作为最佳实践，不要使用默认团体字符串 ***public***；它是广为人知的，因此不太安全。
   - **V3** — 每台服务器，请单击 **Add**（添加）并输入服务器 **Name**（名称）、IP 地址（**SNMP Manager**（**SNMP** 管理器））、SNMP **User**（用户）帐户（必须与在 SNMP 管理器中定义的用户名相匹配）、用于唯一标识防火墙的 **EngineID**（可将此字段留空，以使用防火墙序列号）、用于向服务器进行身份验证的身份验证密码（**Auth Password**（身份验证密码））、用于加密发往服务器的 SNMP 消息的隐私密码（**Priv Password**（隐私密码））。
6. 单击 **OK**（确定）保存服务器配置文件。

STEP 3 | 配置日志转发。

1. 配置流量、威胁和 WildFire 陷阱的目标：
   1. 创建日志转发配置文件。对于每种日志类型和每种严重性级别或 WildFire 判定，请选择 **SNMP Trap**（**SNMP** 陷阱）服务器配置文件。
   2. 将日志转发配置文件分配给安全规则和网络区域。规则和区域将触发陷阱生成和转发。
2. 配置系统、配置、User-ID、HIP 匹配和关联日志的目标。对于每种日志（陷阱）类型和严重性级别，请选择 **SNMP Trap**（**SNMP** 陷阱）服务器配置文件。
3. 单击 **Commit**（提交）。

STEP 4 | 在 SNMP 管理器中监控陷阱。

请参阅 SNMP 管理器的文档。

监控与防火墙接口相关的陷阱时，必须将 *SNMP* 管理器中的接口索引与防火墙 *Web* 界面中的接口名称相匹配。有关详细信息，请参阅 SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符。

# 支持的 MIB

下表列出了 Palo Alto Networks 防火墙、Panorama 和 WF-500 设备支持的简单网络管理协议 (SNMP) 管理信息库 (MIB)。您必须将这些 MIB 加载到 SNMP 管理器中，才能监控在 MIB 中定义的对象（系统统计信息和陷阱）。有关详细信息，请参阅使用 SNMP 管理器浏览 MIB 和对象。


© 2019 Palo Alto Networks, Inc.

| MIB 类型 | 支持的 MIB |
| --- | --- |
| 标准 — 互联网工程任务组 (IETF) 维护大多数标准 MIB。您可从 IETF 网站下载 MIB。<br><br>*Palo Alto Networks 防火墙、Panorama 和 WF-500 设备并非支持所有这些 MIB 中的所有对象 (OID)。有关支持的 OID 的概述，请参阅支持的 MIB 链接。* | MIB-II<br>IF-MIB<br>HOST-RESOURCES-MIB<br>ENTITY-MIB<br>ENTITY-SENSOR-MIB<br>ENTITY-STATE-MIB<br>IEEE 802.3 LAG MIB<br>LLDP-V2-MIB.my<br>BFD-STD-MIB |
| 企业 — 您可从 Palo Alto Networks 技术文档门户下载企业 MIB。 | PAN-COMMON-MIB.my<br>PAN-GLOBAL-REG-MIB.my<br>PAN-GLOBAL-TC-MIB.my<br>PAN-LC-MIB.my<br>PAN-PRODUCT-MIB.my<br>PAN-ENTITY-EXT-MIB.my<br>PAN-TRAPS.my |

## MIB-II

MIB-II 为基于 TCP/IP 的网络中的网络管理协议提供对象标识符 (OID)。使用此 MIB 可监控关于系统和接口的常规信息。例如，您可以按接口类型（ifType 对象）来分析带宽使用率趋势，以确定防火墙是否需要更多该类型的接口，以适应流量的剧增。

Palo Alto Networks 防火墙、Panorama 和 WF-500 设备仅支持以下对象组：

| 对象组 | 说明 |
| --- | --- |
| 系统 | 提供系统信息，例如硬件型号、系统正常时间、FQDN 和物理位置。 |
| 接口 | 提供物理和逻辑接口的统计信息，例如类型、当前带宽（速度）、运行状态（例如开启或关闭）、丢弃的数据包。逻辑接口支持 VPN 隧道、聚合组、第 2 层子接口、第 3 层子接口、回环接口和 VLAN 接口。 |

RFC 1213 定义了这种 MIB。

## IF-MIB

IF-MIB 支持更多接口类型（物理和逻辑）和更大计数器 (64K)，超出在MIB-II中定义的接口和计数器。除了 MIB-II 提供的统计信息之外，使用此 MIB 可以监控更多接口统计信息。例如，要监控高速接口（大于 2.2Gps）的当前带宽，例如 PA-5200 系列防火墙的 10G 接口，您必须检查 IF-MIB 中的 ifHighSpeed 对象，而不是 MIB-II 中的 ifSpeed 对象。评估网络的容量时，IF-MIB 统计信息可能是非常有用的。



© 2019 Palo Alto Networks, Inc.

Palo Alto Networks 防火墙、Panorama 和 WF-500 设备仅支持 IF-MIB 中的 ifXTable，IF-MIB 提供大量接口信息，例如传送和接收的多播和广播数据包数量、接口是否处于混杂模式、接口是否有物理连接器。

RFC 2863 定义了这种 MIB。

## HOST-RESOURCES-MIB

HOST-RESOURCES-MIB 提供主计算机资源信息。使用此 MIB 可监控 CPU 和内存使用统计信息。例如，检查当前的 CPU 负载（hrProcessorLoad 对象）有助于您排除防火墙上的性能问题。

Palo Alto Networks 防火墙、Panorama 和 WF-500 设备仅支持以下部分对象组：

| 对象组 | 说明 |
| --- | --- |
| hrDevice | 提供 CPU 负载、存储容量、分区大小等信息。hrProcessorLoad OID 提供处理数据包的内核的平均数。<br>对于具备多个数据平面 (DP) 的 PA-7000 和 PA-5200 系列防火墙，您可以监控单个数据平面处理器的利用率。设置在利用率达到每个 DP 处理器特定阈值时发出的警报，以避免出现服务可用性问题。 |
| hrSystem | 提供系统正常运行时间、当前用户会话数、当前进程数等信息。 |
| hrStorage | 提供已使用的存储容量等信息。 |

RFC 2790 定义了这种 MIB。

## ENTITY-MIB

ENTITY-MIB 提供多个逻辑和物理组件的 OID。使用此 MIB 可确定哪些物理组件装载在系统上（例如风扇和温度传感器），并查看型号和序列号等相关信息。您还可以使用这些组件的索引号，在ENTITY-SENSOR-MIB和ENTITY-STATE-MIB中确定它们的运行状态。

Palo Alto Networks 防火墙、Panorama 和 WF-500 设备仅支持以下部分 entPhysicalTable 组：

| object | 说明 |
| --- | --- |
| entPhysicalIndex | 单个命名空间，包括磁盘插槽和磁盘驱动器。 |
| entPhysicalDescr | 组件说明。 |
| entPhysicalVendorType | 当它可用时，则为 sysObjectID（请参阅PAN-PRODUCT-MIB.my）（机箱和模块对象）。 |
| entPhysicalContainedIn | 包含此组件的组件的 entPhysicalIndex 值。 |
| entPhysicalClass | 机箱 (3)、插槽容器 (5)、电源 (6)、风扇 (7)、温度或其他环境传感器 (8)、线卡的模块 (9)。 |
| entPhysicalParentRelPos | 此子 组件在其同级 组件中的相对位置。同级组件定义为共享每个 entPhysicalContainedIn 和 entPhysicalClass 对象的相同实例的 entPhysicalEntry 组件。 |
| entPhysicalName | 只有当管理 (MGT) 接口允许命名线卡时才会支持。 |


© 2019 Palo Alto Networks, Inc.

| object | 说明 |
| --- | --- |
| entPhysicalHardwareRev | 组件的供应商特定硬件版本。 |
| entPhysicalFirwareRev | 组件的供应商特定固件版本。 |
| entPhysicalSoftwareRev | 组件的供应商特定软件版本。 |
| entPhysicalSerialNum | 组件的供应商特定序列号。 |
| entPhysicalMfgName | 组件的制造商名称。 |
| entPhysicalMfgDate | 组件的制造日期。 |
| entPhysicalModelName | 磁盘型号。 |
| entPhysicalAlias | 网络管理者为组件指定的别名。 |
| entPhysicalAssetID | 网络管理者为组件指定的用户分配资产跟踪标识符。 |
| entPhysicalIsFRU | 指示组件是否为现场可更换单元 (FRU)。 |
| entPhysicalUris | 组件的通用语言设备标识符 (CLEI) 编号（例如 URN:CLEI:CNME120ARA）。 |

RFC 4133 定义了这种 MIB。

## *ENTITY-SENSOR-MIB*

ENTITY-SENSOR-MIB 增加了对ENTITY-MIB定义之外的网络设备的物理传感器的支持。将此 MIB 与 ENTITY-MIB 结合使用可监控系统的物理组件（例如风扇和温度传感器）的运行状态。例如，要排除可能由于环境条件导致的问题，您可将 ENTITY-MIB 中的实体索引（entPhysicalDescr 对象）映射到 ENTITY-SENSOR-MIB 中的运行状态值（entPhysSensorOperStatus 对象）。在以下示例中，PA-3020 防火墙的所有风扇和温度传感器都在工作：

| Name/OID | Value |
| --- | --- |
| entPhysicalDescr.1 | PA-3020 |
| entPhysicalDescr.2 | Fan #1 RPM |
| entPhysicalDescr.3 | Fan #2 RPM |
| entPhysicalDescr.4 | Fan #3 RPM |
| entPhysicalDescr.5 | Fan #4 RPM |
| entPhysicalDescr.6 | Temperature @ Ocelot |
| entPhysicalDescr.7 | Temperature @ Switch |
| entPhysicalDescr.8 | Temperature @ Cavium |
| entPhysicalDescr.9 | Temperature @ Intel PHY |
| entPhysicalDescr.10 | Temperature @ Switch Core |
| entPhysicalDescr.11 | Temperature @ Cavium Core |
| entPhySensorOperStatus.2 | ok (1) |
| entPhySensorOperStatus.3 | ok (1) |
| entPhySensorOperStatus.4 | ok (1) |
| entPhySensorOperStatus.5 | ok (1) |
| entPhySensorOperStatus.6 | ok (1) |
| entPhySensorOperStatus.7 | ok (1) |
| entPhySensorOperStatus.8 | ok (1) |
| entPhySensorOperStatus.9 | ok (1) |
| entPhySensorOperStatus.10 | ok (1) |
| entPhySensorOperStatus.11 | ok (1) |

同一个 *OID* 可能表示不同平台上的不同传感器。使用目标平台的 *ENTITY-MIB*，将值与说明匹配。

Palo Alto Networks 防火墙、Panorama 和 WF-500 设备仅支持以下部分 entPhySensorTable 组。支持部分随平台而变化，并仅包括热传感器（温度，以摄氏度为单位）和风扇传感器（以 RPM 为单位）。

RFC 3433 定义了 ENTITY-SENSOR-MIB。



© 2019 Palo Alto Networks, Inc.

## ENTITY-STATE-MIB

ENTITY-STATE-MIB 提供ENTITY-MIB定义之外的关于物理组件状态的信息，包括基于机箱的平台中的组件的管理和运行状态。将此 MIB 与 ENTITY-MIB 结合使用可监控 PA-7000 系列防火墙的组件（例如线卡、风扇托架和电源）的运行状态。例如，要排除威胁日志的日志转发问题，您可将 ENTITY-MIB 中的日志处理卡 (LPC) 索引（entPhysicalDescr 对象）映射到 ENTITY-SENSOR-MIB 中的运行状态值（entStateOper 对象）。运行状态值使用数字来指示状态：1 表示未知，2 表示禁用，3 表示启用，4 表示测试。PA-7000 系列防火墙是唯一支持此 MIB 的 Palo Alto Networks 防火墙。

RFC 4268 定义了 ENTITY-STATE-MIB。

## IEEE 802.3 LAG MIB

使用 IEEE 802.3 LAG MIB 可监控启用了链接聚合控制协议 (ECMP) 的聚合组的状态。当防火墙记录 LACP 事件时，它还会生成对排除故障非常有帮助的陷阱。例如，陷阱可以告诉您防火墙和 LACP 对等之间是否出现了流量中断，这可能是由于连接丢失、接口速度和双工值不匹配导致的。

PAN-OS 实施了 LACP 的以下 SNMP 表。

*dot3adTablesLastChanged* 对象指示对 *dot3adAggTable*、*dot3adAggPortListTable* 和 *dot3adAggPortTable* 的最近一次更改的时间。

| 表 | 说明 |
|---|---|
| 聚合器配置表 (dot3adAggTable) | 本表包含关于与防火墙关联的每一个聚合组的信息。每个聚合组都有一个条目。<br>有些表对象受到限制，dot3adAggIndex 对此进行了说明。此索引是本地系统分配给聚合组的唯一标识符。它标识一个聚合组实例，涵盖了包含对象的从属受管对象。标识符是只读的。<br>*ifTable MIB*（接口条目列表）不支持逻辑接口，因此没有聚合组的条目。 |
| 聚合端口列表 (dot3adAggPortListTable) | 本表列出与防火墙中的每个聚合组相关的端口。每个聚合组都有一个条目。<br>dot3adAggPortListPorts 属性列出了与聚合组关联的整组端口。列表中设置的每个位代表一个端口成员。对于非机箱平台，它是一个 64 位值。对于机箱平台，该值是 8 个 64 位条目。 |
| 聚合端口表 (dot3adAggPortTable) | 本表包含与防火墙中的聚合组关联的每个端口的 LACP 配置信息。每个端口都有一个条目。对于与聚合组没有关联的端口，本表不包含任何相关条目。 |
| LACP 统计信息表 (dot3adAggPortStatsTable) | 本表包含与防火墙中的聚合组关联的每个端口的链接聚合信息。每个端口都有一行。对于与聚合组没有关联的端口，本表不包含任何相关条目。 |

IEEE 802.3 LAG MIB 包括以下与 LACP 相关的陷阱：

| 陷阱名称 | 说明 |
|---|---|
| panLACPLostConnectivityTrap | 对等丢失与防火墙的连接。 |
| panLACPUnresponsiveTrap | 对等未对防火墙做出响应。 |


© 2019 Palo Alto Networks, Inc.

| 陷阱名称 | 说明 |
| --- | --- |
| panLACPNegoFailTrap | 与对等的 LACP 协商失败。 |
| panLACPSpeedDuplexTrap | 防火墙和对等上的链路速度和双工设置不匹配。 |
| panLACPLinkDownTrap | 聚合组中的某个接口已关闭。 |
| panLACPLacpDownTrap | 已从聚合组中删除接口。 |
| panLACPLacpUpTrap | 已向聚合组添加接口。 |

有关 MIB 定义，请参阅 IEEE 802.3 LAG MIB。

## *LLDP-V2-MIB.my*

使用 LLDP-V2-MIB 可监控链路层发现协议 (LLDP) 事件。例如，您可以检查 lldpV2StatsRxPortFramesDiscardedTotal 对象，以查看出于任何原因丢弃的 LLDP 帧的数量。Palo Alto Networks 防火墙使用 LLDP 来发现相邻设备及其功能。LLDP 让故障排除变得更加简单，特别是对于 Virtual Wire 部署，ping 或 traceroute 实用工具在这些部署中无法检测到防火墙。

Palo Alto Networks 防火墙支持除以下对象之外的所有 LLDP-V2-MIB 对象：

- 以下 lldpV2Statistics 对象：
  - lldpV2StatsRemTablesLastChangeTime
  - lldpV2StatsRemTablesInserts
  - lldpV2StatsRemTablesDeletes
  - lldpV2StatsRemTablesDrops
  - lldpV2StatsRemTablesAgeouts
- 以下 lldpV2RemoteSystemsData 对象：
  - lldpV2RemOrgDefInfoTable 表
  - 在 lldpV2RemTable 表中： lldpV2RemTimeMark

RFC 4957 定义了这种 MIB。

## *BFD-STD-MIB*

使用双向转发检测 (BFD) MIB 监控和接收两个转发引擎（如接口、数据链路或实际转发引擎）之间的双向路径故障警报。例如，可检查 bfdSessState 对象，以查看转发引擎之间的 BFD 会话状态。在 Palo Alto Networks 实施中，一个转发引擎为防火墙接口，而另一个则为已配置 BFD 的相邻对等。

RFC 7331 定义了这种 MIB。

## *PAN-COMMON-MIB.my*

使用 PAN-COMMON-MIB 可监控 Palo Alto Networks 防火墙、Panorama 和 WF-500 设备的以下信息：

| 对象组 | 说明 |
| --- | --- |
| panSys | 包括系统软件/硬件版本、动态内容版本、序列号、HA 模式/状态和全局计数器等对象。 |



© 2019 Palo Alto Networks, Inc.

| 对象组 | 说明 |
| --- | --- |
| | 全局计数器包括与拒绝服务 (DoS)、IP 分片、TCP 状态、丢弃数据包相关的计数器。通过跟踪这些计数器，您能够监控由于 DoS 攻击、系统或连接故障、资源限制导致的流量不规则。PAN-COMMON-MIB 支持防火墙的全局计数器，但不支持 Panorama 的全局计数器。 |
| panChassis | 机箱类型和 M 系列设备模式（Panorama 或日志收集器）。 |
| panSession | 会话利用率信息。例如，防火墙或特定虚拟系统上的活动会话的总数。 |
| panMgmt | 防火墙至 Panorama 管理服务器的连接的状态： |
| panGlobalProtect | GlobalProtect 网关利用率（百分比）、允许的最大隧道数、活动隧道数。 |
| panLogCollector | 记录每个日志收集器的统计信息，包括日志记录速率、日志配额、磁盘使用率、保留期限、日志冗余（启用或禁用）、从防火墙到日志收集器的转发状态、从日志收集器到外部服务的转发状态，以及防火墙到日志收集器的连接状态。 |
| panDeviceLogging | 记录每个防火墙的统计信息，包括日志记录速率、磁盘使用率、保留期限、从单个防火墙到 Panorama 和外部服务器的转发状态，以及防火墙到日志收集器的连接状态。 |

## PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my 包含 Palo Alto Networks 企业 MIB 模块的不同子目录树的全局顶层 OID 定义。此 MIB 不包含您要监控的对象；只有在被其他 MIB 引用时，它才是必需的。

## PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my 定义 Palo Alto Networks 企业 MIB 模块中的对象文本值的约定（例如字符长度和允许字符数）。所有 Palo Alto Networks 产品都使用这些约定。此 MIB 不包含您要监控的对象；只有在被其他 MIB 引用时，它才是必需的。

## PAN-LC-MIB.my

PAN-LC-MIB.my 包含日志收集器（日志收集器模式的 M 系列设备）实施的受管对象的定义。使用此 MIB 可监控记录速率、日志数据库存储持续时间（以天为单位）、日志收集器上的每个逻辑磁盘（最多 4 个）的磁盘使用率（以 MB 为单位）。例如，您可以使用此信息来确定是否应该添加更多日志收集器或将日志转发至外部服务器（例如 syslog 服务器）进行存档。

## PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my 为所有 Palo Alto Networks 产品定义 sysObjectID OID。此 MIB 不包含您要监控的对象；只有在被其他 MIB 引用时，它才是必需的。

## PAN-ENTITY-EXT-MIB.my

将 PAN-ENTITY-EXT-MIB.my 和ENTITY-MIB结合使用，可监控 PA-7000 系列防火墙的物理组件（例如风扇托架和电源）的功率，该系列是唯一支持此 MIB 的 Palo Alto Networks 防火墙。例如，在排除日志转发问题时，您可能希望检查日志处理卡 (LPC) 的功率：您可将 ENTITY-MIB 中的 LPC 索引（entPhysicalDescr 对象）映射到 PAN-ENTITY-EXT-MIB 中的值（panEntryFRUModelPowerUsed 对象）。


© 2019 Palo Alto Networks, Inc.

## *PAN-TRAPS.my*

使用 PAN-TRAPS.my 可查看生成的所有陷阱的完整列表，以及关于这些陷阱的信息（例如说明）。有关 Palo Alto Networks 防火墙、Panorama 和 WF-500 设备支持的陷阱列表，请参阅PAN-COMMON-MIB.my **panCommonEvents** > **panCommonEventsEvents** > **panCommonEventEventsV2** 对象。



© 2019 Palo Alto Networks, Inc.

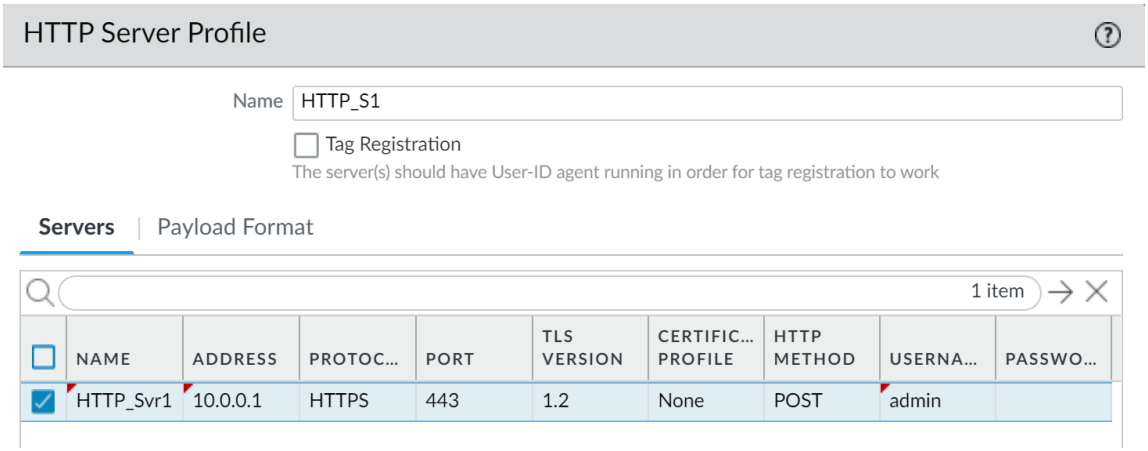
# 将日志转发到 HTTP/S 目标

防火墙和 Panorama™ 可以将日志转发到 HTTP/S 服务器。您可以选择转发所有日志或特定日志，以在事件发生时触发对外部基于 HTTP 的服务的操作。转发日志到 HTTP 服务器时，将防火墙配置为直接向第三方服务发送基于 HTTP 的 API 请求，以根据防火墙日志中的属性触发操作。您可以将防火墙配置为使用公开 API 的任何基于 HTTP 的服务，并修改 HTTP 请求中的 URL、HTTP 标头、参数和负载，以满足您的集成需求。

STEP 1 | 创建 HTTP 服务器配置文件以将日志转发到 HTTP/S 目标。

HTTP 服务器配置文件允许您指定访问服务器的方式，并定义将日志转发到 HTTP/S 目标的格式。默认情况下，防火墙使用管理端口转发这些日志。但是，您可以在 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Service Route Configuration**（服务路由配置）中分配不同的源接口和 IP 地址。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **HTTP**，并 **Add**（添加）新配置文件。
2. 指定服务器配置文件的 **Name**（名称），然后选择 **Location**（位置）。所有虚拟系统中的配置文件可以 **Shared**（共享），也可以属于特定虚拟系统。
3. **Add**（添加）各个服务器的详细信息。每个配置文件最多可包含 4 个服务器。
4. 输入 **Name**（名称）和 IP **Address**（地址）。
5. 选择 **Protocol**（协议）（**HTTP** 或 **HTTPS**）。默认 **Port**（端口）分别为 80 或 443；但是，您可以修改端口号以匹配 HTTP 服务器侦听的端口。
6. 选择服务器上受支持的 **TLS Version**（**TLS** 版本）：**1.0**、**1.1** 或 **1.2**（默认）。
7. 选择用于与服务器进行 TLS 连接的 **Certificate Profile**（证书配置文件）。
8. 选择第三方服务支持的 **HTTP Method**（**HTTP** 方法）— **DELETE**、**GET**、**POST**（默认）或 **PUT**。
9. （可选）如果需要，输入 **Username**（用户名）和 **Password**（密码）对服务器进行身份验证。
10. （可选）选择 **Test Server Connection**（测试服务器连接），以验证防火墙与 HTTP/S 服务器之间的网络连接。

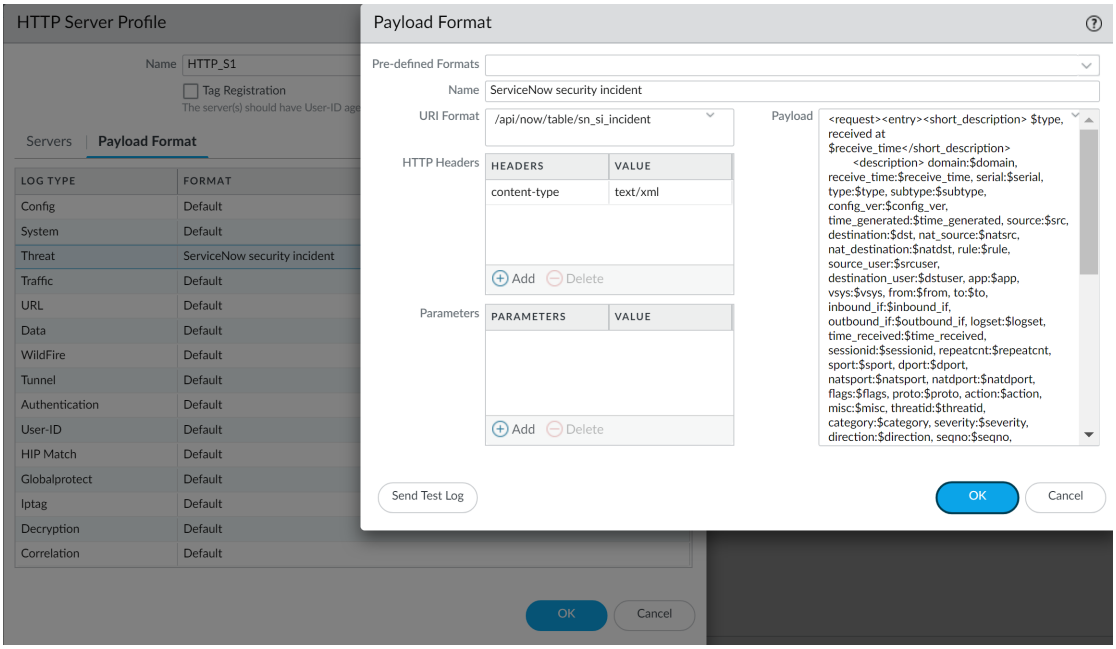



STEP 2 | 为 HTTP 请求选择 **Payload Format**（负载格式）。

1. 为要定义 HTTP 请求格式的每个日志类型选择 **Log Type**（日志类型）链接。
2. 选择 **Pre-defined Formats**（预定义格式）（通过内容更新可用）或创建自定义格式。

   如果创建自定义格式，则 **URI** 是 HTTP 服务的资源端点。防火墙将 URI 附加到之前定义的 IP 地址，以构建 HTTP 请求的 URL。确保 URI 和负载格式与第三方供应商所需的语法相匹配。您可以使用 HTTP 标头、参数、值对和请求负载中所选日志类型所支持的任何属性。


© 2019 Palo Alto Networks, Inc.



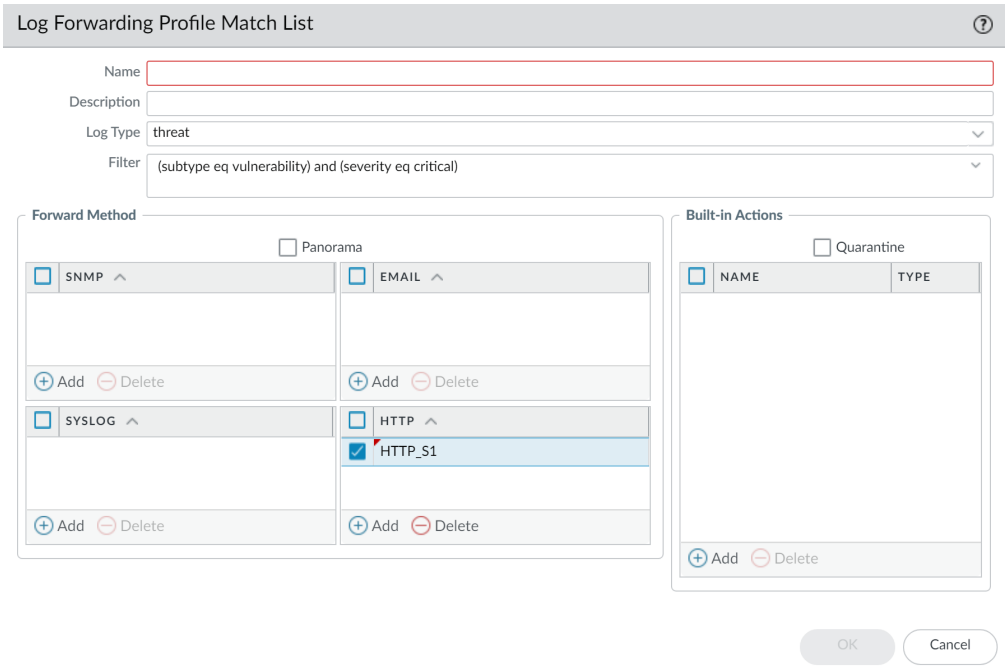

3. **Send Test Log**（发送测试日志）来验证 HTTP 服务器是否收到该请求。当您以交互方式发送测试日志时，防火墙将使用最初格式，并且不会使用防火墙日志中的值替换该变量。如果您的 HTTP 服务器发送 404 响应，请提供参数的值，以便服务器可以成功处理请求。

STEP 3 | 定义防火墙将日志转发到 HTTP 服务器的匹配条件，并附加要使用的 HTTP 服务器配置文件。

1. 选择要触发工作流程的日志类型：
   - 为与用户活动有关的日志（例如，流量、威胁或身份验证日志）添加日志转发配置文件（**Objects**（对象）> **Log Forwarding Profile**（日志转发配置文件））。
   - 为与系统事件相关的日志（例如配置或系统日志）选择 **Device**（设备）> **Log Settings**（日志设置）。
2. 选择日志类型并使用新的 **Filter Builder**（筛选器构建器）来定义匹配条件。
3. **Add**（添加）将日志转发到 HTTP 目标的 HTTP 服务器配置文件。



© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

# NetFlow 监控

NetFlow 是一项行业标准的协议，防火墙能够使用该协议导出其接口上 IP 流量的相关统计信息。防火墙将统计信息以 NetFlow 字段导出到 NetFlow 收集器中。NetFlow 收集器是一种出于安全、管理、核算和故障排除目的用于分析网络流量的服务器。所有 Palo Alto Networks 防火墙都支持 NetFlow 9 版。以上防火墙仅支持单向 NetFlow，而不支持双向 NetFlow。防火墙支持对接口上所有 IP 数据包执行 NetFlow 处理，不支持采样 NetFlow。可以为第 3 层、第 2 层、虚拟线路、旁接、VLAN、回环和隧道接口导出 NetFlow 记录。对于聚合以太网子接口，您可以导出组内数据流经的各个子接口的记录。要识别 NetFlow 收集器中的防火墙接口，请参阅SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符。防火墙支持 NetFlow 收集器用于解密 NetFlow 字段的标准和企业（特定于 PAN-OS）NetFlow 模板。

- 配置 NetFlow 导出
- NetFlow 模板

## 配置 NetFlow 导出

要使用 NetFlow 收集器分析防火墙接口上的网络流量，请执行以下步骤配置 NetFlow 记录导出。

STEP 1 | 创建 NetFlow 服务器配置文件。

配置文件定义接收导出记录并指定导出参数的 NetFlow 收集器。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **NetFlow** ，并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）以标识配置文件。
3. 根据 NetFlow 收集器的要求，指定防火墙刷新 NetFlow 模板的频率，以 **Minutes**（分钟）（默认为 30）和 **Packets**（数据包）（导出记录 — 默认为 20）为单位。在任一阈值过后，防火墙将刷新模板。
4. 指定 **Active Timeout**（主动超时），这是防火墙导出记录的频率（以分钟为单位，默认为 5）。
5. 选中 **PAN-OS Field Types**（**PAN-OS** 字段类型）（如果您希望防火墙导出 App-ID 及 User-ID 字段）。
6. **Add**（添加）将接收记录的每个 NetFlow 收集器（每个配置文件最多两个）。对于每个收集器，指定以下各项：
   - 用来标识收集器的 **Name**（名称）。
   - **NetFlow Server**（**NetFlow** 服务器）主机名或 IP 地址。
   - 访问 **Port**（端口）（默认为 2055）。
7. 单击 **OK**（确定）保存配置文件。

STEP 2 | 将 NetFlow 服务器配置文件分配给携带您希望分析的流量的防火墙接口。

在本示例中，将配置文件分配至现有的以太网接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后单击接口名称，以对其进行编辑。

   可以为第 *3* 层、第 *2* 层、虚拟线路、旁接、*VLAN*、回环和隧道接口导出 *NetFlow* 记录。对于聚合以太网接口，您可以导出聚合组的记录，但不能导出组内各个接口的记录。

2. 选择您配置的 NetFlow 服务器配置文件（**NetFlow Profile**（**NetFlow** 配置文件）），然后单击 **OK**（确定）。

STEP 3 | （**PA-7000** 系列和 **PA-5200** 系列防火墙所需）配置防火墙将用于发送 NetFlow 记录的接口的服务路由。



© 2019 Palo Alto Networks, Inc.

您不能使用管理 (MGT) 接口从 PA-7000 系列和 PA-5200 系列防火墙发送 NetFlow 记录。对于其他防火墙型号，服务路由为可选项。对于所有防火墙，发送 NetFlow 记录的接口不一定与防火墙收集记录的接口相同。

1. 选择**Device**（设备）> **Setup**（设置）> **Services**（服务）。
2. （具有多个虚拟系统的防火墙）选择以下选项之一：
   - **Global**（全局）— 如果服务路由适用于防火墙上的所有虚拟系统，请选择此选项。
   - **Virtual Systems**（虚拟系统）— 如果服务路由适用于特定的虚拟系统，请选择此选项。将 **Location**（位置）设置为虚拟系统。
3. 选择 **Service Route Configuration**（服务路由配置）并自定义。
4. 选择接口使用的协议（**IPv4** 或 **IPv6**）。如果需要，您可以配置两个协议的服务路由。
5. 单击服务列中的 **Netflow**。
6. 选择 **Source Interface**（源接口）。

   *Any*（任何）、*Use default*（使用默认）和 *MGT* 并不是从 *PA-7000* 系列或 *PA-5200* 系列防火墙发送 *NetFlow* 记录的有效接口选项。
7. 选择 **Source Address**（源地址）（IP 地址）。
8. 单击 **OK**（确定）两次以保存更改。

STEP 4 | **Commit**（提交）更改。

STEP 5 | 在 NetFlow 收集器中监控防火墙流量。

请参阅您的 NetFlow 收集器文档。

监控统计信息时，必须将 *NetFlow* 收集器中的接口索引与防火墙 *Web* 界面中的接口名称相匹配。有关详细信息，请参阅 SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符。

要解决 NetFlow 交付问题，请使用操作 CLI 命令 **`debug log-receiver netflow statistics`**。

# NetFlow 模板

NetFlow 收集器使用模板来破译防火墙导出的字段。防火墙根据导出的数据类型选择模板：IPv4 或 IPv6 流量、包含或不包含 NAT、标准或专用于企业（PAN-OS 特定）的字段。防火墙定期刷新模板，以重新评估使用哪一个模板（以防导出数据类型变化），并将所有更改应用于所选模板中的字段。配置 NetFlow 导出时，根据 NetFlow 收集器的要求，基于时间间隔和导出的记录数设置刷新率。在任一阈值过后，防火墙将刷新模板。

Palo Alto Networks 防火墙支持以下 NetFlow 模板：

| 模板 | ID |
|---|---|
| IPv4 标准版 | 256 |
| IPv4 企业版 | 257 |
| IPv6 标准版 | 258 |
| IPv6 企业版 | 259 |
| 含 NAT 的 IPv4 标准版 | 260 |


© 2019 Palo Alto Networks, Inc.

| 模板 | ID |
| --- | --- |
| 含 NAT 的 IPv4 企业版 | 261 |
| 含 NAT 的 IPv6 标准版 | 262 |
| 含 NAT 的 IPv6 企业版 | 263 |

下表列出了防火墙可发送的 NetFlow 字段，以及定义这些字段的模板：

| 值 | 字段 | 说明 | 模板 |
| --- | --- | --- | --- |
| 1 | IN_BYTES | 传入的计数器，长度为 N * 8 位，字节数与 IP 流相关。默认情况下，N 为 4。 | 所有模板 |
| 2 | IN_PKTS | 传入的计数器，长度为 N * 8 位，数据包数与 IP 流相关。默认情况下，N 为 4。 | 所有模板 |
| 4 | 协议 | IP 协议字节。 | 所有模板 |
| 5 | TOS | 输入传入的接口时服务字节设置的类型。 | 所有模板 |
| 6 | TCP_FLAGS | 此流中所有 TCP 标记总数。 | 所有模板 |
| 7 | L4_SRC_PORT | TCP/UDP 源端口数（例如 FTP、Telnet 或同等端口）。 | 所有模板 |
| 8 | IPV4_SRC_ADDR | IPv4 源地址。 | IPv4 标准版<br>IPv4 企业版<br>含 NAT 的 IPv4 标准版<br>含 NAT 的 IPv4 企业版 |
| 10 | INPUT_SNMP | 输入接口索引。默认情况下，值的长度为 2 个字节，但是也可能更多。有关 Palo Alto Networks 防火墙如何生成接口索引的详细信息，请参阅 SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符。 | 所有模板 |
| 11 | L4_DST_PORT | TCP/UDP 目标端口数（例如 FTP、Telnet 或同等端口）。 | 所有模板 |
| 12 | IPV4_DST_ADDR | IPv4 目标地址。 | IPv4 标准版<br>IPv4 企业版<br>含 NAT 的 IPv4 标准版<br>含 NAT 的 IPv4 企业版 |


© 2019 Palo Alto Networks, Inc.

| 值 | 字段 | 说明 | 模板 |
|---|---|---|---|
| 14 | OUTPUT_SNMP | 输出接口索引。默认情况下，值的长度为 2 个字节，但是也可能更多。有关 Palo Alto Networks 防火墙如何生成接口索引的详细信息，请参阅 SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符。 | 所有模板 |
| 21 | LAST_SWITCHED | 打开此流量的最后一个数据包时，系统的正常运行时间（以毫秒计）。 | 所有模板 |
| 22 | FIRST_SWITCHED | 打开此流量的第一个数据包时，系统的正常运行时间（以毫秒计）。 | 所有模板 |
| 27 | IPV6_SRC_ADDR | IPv6 源地址。 | IPv6 标准版<br>IPv6 企业版<br>含 NAT 的 IPv6 标准版<br>含 NAT 的 IPv6 企业版 |
| 28 | IPV6_DST_ADDR | IPv6 目标地址. | IPv6 标准版<br>IPv6 企业版<br>含 NAT 的 IPv6 标准版<br>含 NAT 的 IPv6 企业版 |
| 32 | ICMP_TYPE | 互联网控制消息协议 (ICMP) 数据包类型。这被报告为：<br>ICMP Type * 256 + ICMP code | 所有模板 |
| 61 | 方向 | 流方向：<br>• 0 = 入口<br>• 1 = 出口 | 所有模板 |
| 148 | flowId | 流的标识符，为观察域中的唯一标识。您可以使用此信息元素区分不同的流（如果未报告或已在单独的报告中报告 IP 地址等流密钥和端口数）。flowID 对应流量和威胁日志中的会话 ID 字段。 | 所有模板 |
| 233 | firewallEvent | 表示防火墙事件：<br>• 0 = 忽略（无效）— 未使用。<br>• 1 = 已创建流量 — NetFlow 数据记录用于新流量。<br>• 2 = 已创建流量 — NetFlow 数据记录用于结束流量。<br>• 3 = 已拒绝流量 — NetFlow 数据记录显示被防火墙策略拒绝的流量。<br>• 4 = 流量警报 — 未使用。 | 所有模板 |


© 2019 Palo Alto Networks, Inc.

| 值 | 字段 | 说明 | 模板 |
| --- | --- | --- | --- |
| | | • 5 = 流量更新 — NetFlow 数据记录发送用于持久流量，该流量比在 NetFlow 服务器配置文件中配置的 **Active Timeout**（主动超时）期限持续的时间更长。 | |
| 225 | postNATSourceIPv4Address | 此信息元素的定义和 sourceIPv4Address 的定义是一样的（例外情况是：在数据包穿过接口之后，它会报告防火墙在网络地址转换过程中生成的修改值）。 | 含 NAT 的 IPv4 标准版<br>含 NAT 的 IPv4 企业版 |
| 226 | postNATDestinationIPv4Address | 此信息元素的定义和 sourceIPv4Address 的定义是一样的（例外情况是：在数据包穿过接口之后，它会报告防火墙在网络地址转换过程中生成的修改值）。 | 含 NAT 的 IPv4 标准版<br>含 NAT 的 IPv4 企业版 |
| 227 | postNAPTSourceTransportPort | 此信息元素的定义和 sourceTransportPort 的定义是一样的（例外情况是：在数据包穿过接口之后，它会报告防火墙在网络地址转换过程中生成的修改值）。 | 含 NAT 的 IPv4 标准版<br>含 NAT 的 IPv4 企业版 |
| 228 | postNAPTDestinationTransportPort | 此信息元素的定义和 destinationTransportPort 的定义是一样的（例外情况是：在数据包穿过接口之后，它会报告防火墙在网络地址转换过程中生成的修改值）。 | 含 NAT 的 IPv4 标准版<br>含 NAT 的 IPv4 企业版 |
| 281 | postNATSourceIPv6Address | 此信息元素的定义和 sourceIPv6Address 信息元素的定义是一样的（例外情况是：在数据包穿过接口之后，它会报告防火墙在 NAT64 网络地址转换过程中生成的修改值）。有关 IPv6 标头中的源地址字段的定义，请参阅 RFC 2460。有关 NAT64 规范，请参阅 RFC 6146。 | 含 NAT 的 IPv6 标准版<br>含 NAT 的 IPv6 企业版 |
| 282 | postNATDestinationIPv6Address | 此信息元素的定义和 sourceIPv6Address 信息元素的定义是一样的（例外情况是：在数据包穿过接口之后，它会报告防火墙在 NAT64 网络地址转换过程中生成的修改值）。有关 IPv6 标头中的目标地址字段的定义，请参阅 RFC 2460。有关 NAT64 规范，请参阅 RFC 6146。 | 含 NAT 的 IPv6 标准版<br>含 NAT 的 IPv6 企业版 |
| 346 | privateEnterpriseNumber | 这是一个唯一可识别 Palo Alto Networks 的私人企业号：25461。 | IPv4 企业版<br>含 NAT 的 IPv4 企业版<br>IPv6 企业版<br>含 NAT 的 IPv6 企业版 |



© 2019 Palo Alto Networks, Inc.

| 值 | 字段 | 说明 | 模板 |
| --- | --- | --- | --- |
| 56701 | App-ID | App-ID 可识别的应用程序名称。名称最长可以为 32 个字节。 | IPv4 企业版<br>含 NAT 的 IPv4 企业版<br>IPv6 企业版<br>含 NAT 的 IPv6 企业版 |
| 56702 | User-ID | 用户 ID 可识别的用户名。名称最长可以为 64 个字节。 | IPv4 企业版<br>含 NAT 的 IPv4 企业版<br>IPv6 企业版<br>含 NAT 的 IPv6 企业版 |


© 2019 Palo Alto Networks, Inc.

# SNMP 管理器和 NetFlow 收集器中的防火墙接口标识符

当您使用 NetFlow 收集器（请参阅 NetFlow 监控）或 SNMP 管理器（请参阅 SNMP 监控和陷阱）监控 Palo Alto Networks 防火墙时，接口索引（SNMP ifindex 对象）可识别携带特定流的防火墙接口（请参阅 SNMP 管理器中的接口索引）。相反，防火墙 Web 界面使用接口名称（例如 ethernet1/1）而不是索引作为标识符。要了解您在 NetFlow 收集器或 SNMP 管理器中看到的哪些统计信息适用于哪种防火墙接口，您必须能够将接口索引与接口名称相匹配。

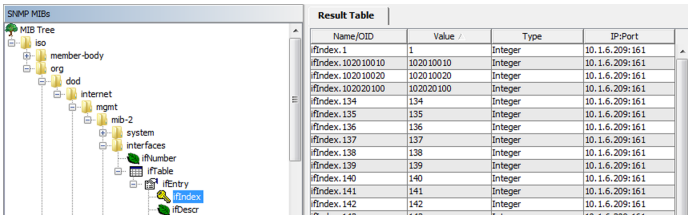



图 3: SNMP 管理器中的接口索引

您必须了解防火墙用于计算索引的公式，从而将索引与名称相匹配。该公式因平台和接口类型（物理或逻辑）而异。

物理接口索引的范围为 1-9999，防火墙对范围的计算如下：

| 防火墙平台 | 计算 | 示例接口索引 |
|---|---|---|
| VM-SERIES | 管理端口数 + 物理端口偏移<br>• **Number of management ports**（管理端口数）— 这是常量，即 1。<br>• **Physical port offset**（物理端口偏移）— 此为物理端口编号。 | VM-100 防火墙, Eth1/4 =<br>1（管理端口数）+ 4（物理端口）= **5** |
| PA-220、PA-220R、PA-800 系列 | 管理端口数 + 物理端口偏移<br>• **Number of management ports**（管理端口数）— 这是常量，即 5。<br>• **Physical port offset**（物理端口偏移）— 此为物理端口编号。 | PA-5200 系列防火墙，Eth1/4 =<br>5（管理端口数）+ 4（物理端口）= **9** |
| PA-3200 系列、PA-5200 系列 | 管理端口数 + 物理端口偏移<br>• **Number of management ports**（管理端口数）— 这是常量，即 4。<br>• **Physical port offset**（物理端口偏移）— 此为物理端口编号。 | PA-5200 系列防火墙，Eth1/4 =<br>4（管理端口数）+ 4（物理端口）= **8** |
| PA-7000 系列 | （最大端口数 * 插槽数）+ 物理端口偏移 + 管理端口数<br>• 最大端口数 — 这是常量，即 64。<br>• 插槽 — 这是网络接口卡的底盘插槽号。 | PA-7000 系列防火墙，Eth3/9 =<br>[64（最大端口数）* 3（插槽）] + 9（物理端口）+ 5（管理端口数）= **206** |



© 2019 Palo Alto Networks, Inc.

| 防火墙平台 | 计算 | 示例接口索引 |
| --- | --- | --- |
| | • **Physical port offset**（物理端口偏移）— 此为物理端口编号。<br>• **Number of management ports**（管理端口数）— 这是常量，即 5。 | |

所有平台的逻辑接口索引均为九个数字，防火墙的计算如下：

| 接口类型 | 范围 | 数字 9 | 数字 7-8 | 数字 5-6 | 数字 1-4 | 示例接口索引 |
| --- | --- | --- | --- | --- | --- | --- |
| 第 3 层子接口 | 101010001-199999999 | 类型：1 | 接口槽：1-9 (01-09) | 接口端口：1-9 (01-09) | 子接口：后缀 1-9999 (0001-9999) | Eth1/5.22 = 100000000（类型）+ 100000（插槽）+ 50000（端口）+ 22（后缀）= **101050022** |
| 第 2 层子接口 | 101010001-199999999 | 类型：1 | 接口槽：1-9 (01-09) | 接口端口：1-9 (01-09) | 子接口：后缀 1-9999 (0001-9999) | Eth2/3.6 = 100000000（类型）+ 200000（插槽）+ 30000（端口）+ 6（后缀）= **102030006** |
| Vwire 子接口 | 101010001-199999999 | 类型：1 | 接口槽：1-9 (01-09) | 接口端口：1-9 (01-09) | 子接口：后缀 1-9999 (0001-9999) | Eth4/2.312 = 100000000（类型）+ 400000（插槽）+ 20000（端口）+ 312（后缀）= **104020312** |
| vlan | 200000001-200009999 | 类型：2 | 00 | 00 | VLAN 后缀：1-9999 (0001-9999) | VLAN.55 = 200000000（类型）+ 55（后缀）= **200000055** |
| 回环 | 300000001-300009999 | 类型：3 | 00 | 00 | 回环后缀：1-9999 (0001-9999) | Loopback.55 = 300000000（类型）+ 55（后缀）= **300000055** |
| Tunnel | 400000001-400009999 | 类型：4 | 00 | 00 | 隧道后缀：1-9999 (0001-9999) | Tunnel.55 = 400000000 (type) + 55 (suffix) = **400000055** |
| 聚合组 | 500010001-500089999 | 类型：5 | 00 | AE 后缀：1-8 (01-08) | 子接口：后缀 1-9999 (0001-9999) | AE5.99 = 500000000（类型）+ 50000（AE 后缀）+ 99（后缀）= **500050099** |


© 2019 Palo Alto Networks, Inc.

# 监视收发器

您可以监视物理设备或设备中收发器的状态，以便于进行安装和故障排除。可以查看的诊断包括传输的偏置电流、发射功率、接收功率、收发器温度以及电源电压。以下列出了支持收发器监控的设备。

- PA-800 系列
- PA-3200 系列
- PA-5200 系列
- PA-7000 系列

使用命令行接口运行收发器监控。下表列出了所有可用 CLI 命令。



如果在不兼容的收发器上运行命令，对于任何不能读取的诊断信息，*CLI* 均返回“*n/a*”。

| CLI | 定义 |
| --- | --- |
| `show transceiver <interface name>` | 查看指定收发器以及各个诊断值的摘要。<br>示例：<br>`admin@PA-7080> show transceiver ethernet11/25`<br>CLI 将返回温度、电压、电流、发射功率和接收功率的值。 |
| `show transceiver-detail <interface name>` | 获取更多有关收发器规格的详细信息，包括供应商信息和链接长度。CLI 还将提供更多有关诊断的详细信息。 |
| `show transceiver all` | 查看所有活动收发器以及每个收发器诊断摘要的列表。 |
| `show transceiver-detail all` | 获取设备中各个收发器的全面详细信息。 |

# User-ID

与 IP 地址相反，用户标识是有效安全基础设施的一个组成部分。知道谁正在使用您网络上每个应用程序以及谁可能传送威胁或正在传输文件，都可以加强您的安全策略并减少事件响应时间。User-ID™ 是 Palo Alto Networks 防火墙的一项标准功能，可让您充分利用存储在各种存储库中的用户信息。以下主题提供有关 User-ID 以及如何配置 User-ID 的更多详细信息：

- User-ID 概述
- User-ID 概念
- 启用 User-ID
- 将用户映射到组
- 将 IP 地址映射到用户
- 启用基于用户和基于组的策略
- 为具有多个帐户的用户启用策略
- 验证用户标识配置
- 在大规模网络中部署 User-ID

# User-ID 概述

User-ID™ 使您能够使用各种技术识别网络上的所有用户，以确保您可以使用各种访问方法和操作系统（包括 Microsoft Windows、Apple iOS、Mac OS、Android 和 Linux®/UNIX）标识所有位置的用户。知道谁是您的用户，而不仅仅是其 IP 地址，使以下操作成为可能：

- 可视性 — 进一步了解用户的应用程序使用情况，为您提供一幅更相关的网络活动图。发现网络出现陌生或不熟悉的应用程序时，User-ID 的功能就变得很明显。通过 ACC 或日志查看器，您的安全团队可以识别应用程序的类型、用户、带宽和会话消耗、应用程序流量的来源和目标，以及任何相关的威胁。
- 策略控制 — 将用户信息绑定到安全策略规则可以提高启用遍历整个网络的应用程序的安全性，并确保仅有业务需求的用户才能访问。例如，一些应用程序，如软件即服务应用程序，可访问人力资源服务（如工作日或现时服务），仅能提供给网络上任何已知用户访问。然而，对于更敏感的应用程序，您可通过仅允许有需求的用户访问的方式减少您的攻击面。例如，虽然 IT 支持人员可能需要合法访问远程桌面应用程序，但您的大多数用户是不需要的。
- 日志记录、报告、取证 — 如果发生安全事件，基于用户信息而不仅仅是 IP 地址的取证分析和报告可以提供更全面的事件图像。例如，您可以使用预定义的用户/组活动来查看单个用户或用户组的 Web 活动摘要，或使用 SaaS 应用程序使用报告来查看哪些用户通过受约束的 SaaS 应用程序传输的数据最多。

为了实施基于用户和组的策略，防火墙必须具备将其收到的数据包中的 IP 地址映射到用户名的功能。User-ID 提供了很多机制来收集此用户映射信息。例如，User-ID 代理监控登录事件的服务器日志并侦听身份验证服务发出的 Syslog 消息。若要识别代理未进行映射的 IP 地址映射，您可以配置身份验证策略，将 HTTP 请求重定向至身份验证门户登录信息。您可以调整用户映射机制以适应您的环境，甚至在不同的站点使用不同的机制，以确保您可以在任何时间、任何地点为所有用户安全地访问应用程序。

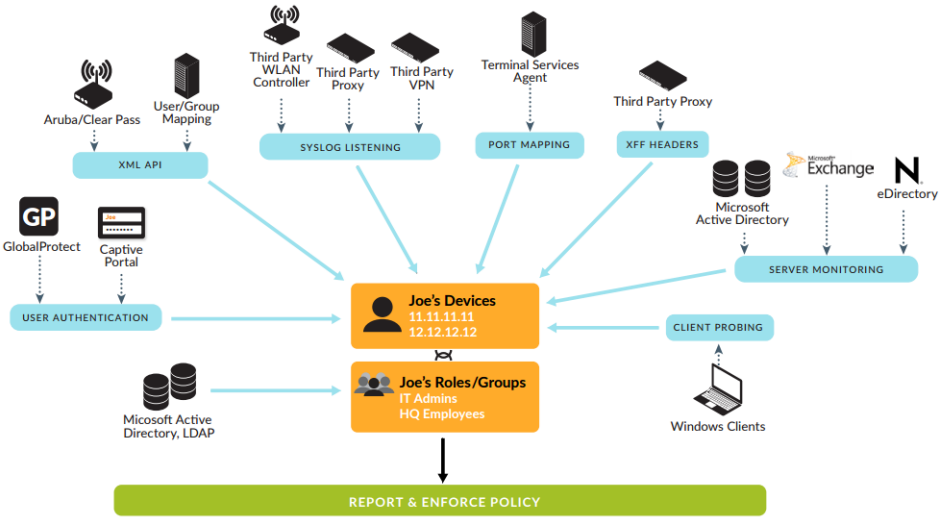



**图 4: User-ID**

要启用基于用户和组的策略实施，防火墙需要一个包含所有可用用户及其相应组成员的列表，以便在定义策略规则时可以选择组。防火墙通过直接连接到 LDAP 目录服务器或使用 XML API 与目录服务器集成来收集组映射信息。

有关 User-ID 的工作原理，请参阅User-ID 概念，有关设置 User-ID 的说明，请参阅启用 User-ID。

*User-ID* 在以下环境中不起作用：在防火墙将 *IP* 地址映射到用户名之前，用户的源 *IP* 地址不进行 *NAT* 转换。



© 2019 Palo Alto Networks, Inc.

# User-ID 概念


- 组映射
- 用户映射


## 组映射

要根据用户或组定义策略规则，您首先需要创建一个 LDAP 服务器配置文件，此配置文件定义防火墙连接目录服务器以及向目录服务器进行认证的方式。防火墙支持各种目录服务器，包括 Microsoft Active Directory (AD)、Novell eDirectory 和 Sun ONE Directory Server。服务器配置文件还定义防火墙如何搜索目录来检索组的列表以及对应的成员列表。如果防火墙本身不支持正在使用的目录服务器，则可以使用 XML API 集成组映射功能。然后，您可以创建组映射配置到将用户映射到组和启用基于用户和基于组的策略。

根据组成员资格（而不是个人用户）来定义策略规则将简化管理，因为这样避免了只要组中添加了新用户，您就必须更新规则的情况。配置组映射时，您可以限制将在策略规则中可用的组。您可以指定目录服务中已经存在的组或根据 LDAP 筛选器定义自定义组。较之于在 LDAP 服务器上创建新组或更改现有组，定义自定义组可能更迅速，并且不需要 LDAP 管理员干预。User-ID 将所有与筛选条件相符的 LDAP 目录用户映射到自定义组。例如，您可能希望某个安全策略允许市场营销部门的承包商访问社交网络站点。如果该部门不存在 Active Directory 组，那么您可以配置 LDAP 筛选器，用于匹配 LDAP 属性“部门”设置为“市场营销”的用户。基于用户组的日志查询和报告将包含自定义组。

## 用户映射

知道用户和组名称远远不够。防火墙还需要知道哪些 IP 地址映射到哪些用户，以便相应地实施安全规则。User-ID 概述介绍了用来标识网络上的用户和组的不同方法，并显示了用户映射和组映射如何共同协作以启用基于用户和组的安全策略实施和可见性。以下主题介绍进行用户映射的不同方法：

- 服务器监视
- 端口映射
- Syslog
- XFF 标头
- 用户名标头插入
- 身份验证策略和身份验证门户
- GlobalProtect
- XML API
- 客户端探测

### 服务器监视

利用服务器监控 User-ID 代理（无论是在您网络中域服务器上运行的基于 Windows 的代理，还是在防火墙上运行的集成于 PAN-OS 的 User-ID 代理），都可监控特定 Microsoft Exchange 服务器和域控制器的安全事件日志或 Novell eDirectory 服务器的登录事件。例如，在 AD 环境中，您可以配置 User-ID 代理来监视 Kerberos 票据授予和续订、Exchange Server 访问（如果已配置）以及文件和打印服务连接的安全日志。为了将这些事件记录在安全日志中，必须将 AD 域配置为记录成功的帐户登录事件。另外，由于用户可以登录域中的任何服务器，因此您必须为所有服务器设置服务器监视，以便捕获所有用户登录事件。有关详细信息，请参阅使用 Windows User-ID 代理配置用户映射或使用 PAN-OS 集成的 User-ID 代理来配置用户映射。

### 端口映射

在具有多用户系统的环境（如 Microsoft Terminal Server 或 Citrix 环境）中，许多用户共享同一 IP 地址。在这种情况下，用户至 IP 地址的映射过程要求知道每个客户端的源端口。若要执行这种类型的映射，必须在



© 2019 Palo Alto Networks, Inc.

Windows/Citrix 终端服务器上安装 Palo Alto Networks 终端服务器代理，以便为将源端口分配至各用户进程提供中介。对于不支持终端服务器代理的终端服务器（如 Linux 终端服务器），可以使用 XML API 将用户映射信息从登录和注销事件发送至 User-ID。有关配置的详细信息，请参阅为终端服务器用户配置用户映射。

## *XFF 标头*

如果您在您网络上的用户和防火墙之间部署了代理服务器，防火墙可能将代理服务器 IP 地址视为 HTTP/HTTPS 流量中代理转发的源 IP 地址而非请求内容的客户端的 IP 地址。在大多数情况下，代理服务器会在流量数据包中添加 X-Forwarded-For 标头，其中包含请求内容的客户端或请求来源的准确 IPv4 或 IPv6 地址。在这种情况下，您可以将防火墙配置为从 XFF 中提取最终用户 IP 地址，这样，User-ID 可以将该 IP 地址映射到用户名。这使您可以为策略使用 XFF 值并记录源用户日志，为此，您可以实施基于用户的策略，以便代理服务器后面的用户启用基于 Web 的安全访问。

## 用户名标头插入

当您使用 Palo Alto Networks 防火墙配置辅助实施设备以实施基于用户的策略时，此辅助设备可能不包含防火墙中的 IP 地址到用户名映射。传输用户标识到下游设备可能要求部署代理等其他设备，或是可能会对用户体验产生负面影响（例如，用户必须多次登录）。您可以动态添加域和用户名到用户传出流量的 HTTP 标头，从而允许与您的 Palo Alto Networks 防火墙一起使用的任何辅助设备接收用户信息和实施基于用户的策略。通过在流量标头中插入用户名和域来包含用户标识，这样可启用实施基于用户的策略，不会对用户体验或其他基础架构的部署产生负面影响。

## 身份验证策略和身份验证门户

在某些情况下，User-ID 代理无法使用服务器监控或其他方法将 IP 地址映射到用户名，例如在用户未登录或使用域服务器不支持的操作系统（如 Linux）的情况下。在其他情况下，无论 User-ID 代理采用何种方式执行用户映射，您可能希望用户在访问敏感应用程序时进行身份验证。就上述情况而言，您可以配置配置身份验证策略和使用身份验证门户将 IP 地址映射到用户名。与身份验证策略规则相匹配的任何 Web 流量（HTTP 或 HTTPS）都会提示用户通过身份验证门户进行身份验证。您可以使用以下身份验证门户身份验证方法：

- 浏览器质询 — 如果要减少用户必须响应的登录提示数量，请使用 Kerberos 单点登录。
- Web 表单 — 使用多重因素身份验证、SAML 单点登录、Kerberos、TACACS+、RADIUS、LDAP 或本地身份验证。
- 客户端证书身份验证。

## *Syslog*

您的环境中现有的网络服务可能需要对用户进行身份验证。这些服务包括无线控制器、802.1x 设备、Apple Open Directory 服务器、代理服务器和其他网络访问控制 (NAC) 机制。您可以将这些服务配置为发送包含有关登录和退出事件信息的 syslog 消息，并配置 User-ID 代理来解析这些消息。User-ID 代理解析登录事件以将 IP 地址映射到用户名，并解析退出事件以删除过期的映射。在 IP 地址分配经常会更改的环境中，删除过时的映射特别有用。

PAN-OS 集成的 User-ID 代理和基于 Windows 的 User-ID 代理都使用 Syslog 解析配置文件来解析 syslog 消息。在服务以不同格式发送消息的环境中，您可以为每种格式创建自定义配置文件，并将多个配置文件与每个 syslog 发件人相关联。如果您使用 PAN-OS 集成的 User-ID 代理，还可以使用 Palo Alto Networks 通过应用程序内容更新提供的预定义 Syslog 解析配置文件。

Syslog 消息必须符合以下条件 User-ID 代理才能进行解析：

- 每个消息都必须是单行文本字符串。新行(`\n`) 或回车加上新行(`\r\n`) 是允许的换行符分隔符。
- 单个消息的最大大小为 8,000 字节。
- 通过 UDP 传送的消息必须包含于单个数据包中；通过 SSL 传送的 Syslog 消息可跨多个数据包。单个数据包可能包含多个消息。

有关配置的详细信息，请参阅配置 User-ID 以监控用户映射的 Syslog 发件人。



© 2019 Palo Alto Networks, Inc.

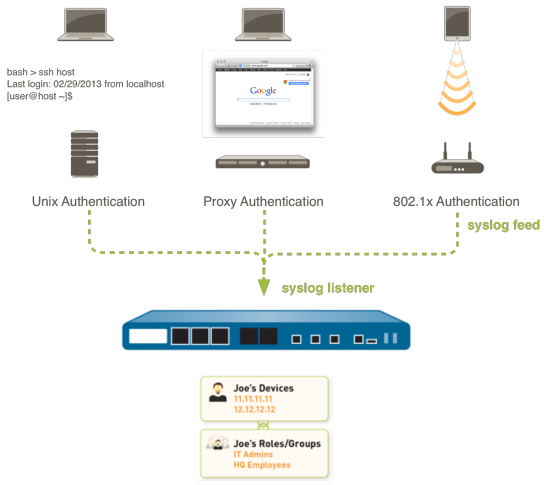



图 **5: Syslog** 的 **User-ID** 集成

## *GlobalProtect*

对于移动或漫游用户，GlobalProtect 端点直接向防火墙提供用户映射信息。在这种情况下，每个 GlobalProtect 用户都拥有一个在端点上运行的应用程序，该端点要求用户输入访问防火墙的 VPN 登录凭证。然后，将该登录信息添加到防火墙上的 User-ID 用户映射表，以查看和实施基于用户的安全策略。由于 GlobalProtect 用户必须通过身份验证才能获得网络访问权，因此必须确切知道 IP 地址到用户名映射。这是在敏感环境中可采用的最佳方案。在这些环境中，您必须是允许对应用程序或服务进行访问的用户。有关设置 GlobalProtect 的详细信息，请参阅《GlobalProtect 管理员指南》。

## *XML API*

身份验证门户和其他标准用户映射方法可能不适用于某些类型的用户访问。例如，标准方法无法为从第三方 VPN 解决方案连接的用户或连接到已启用 802.1x 的无线网络的用户添加用户映射。对于此类情况，可使用 PAN-OS XML API 来捕获登录事件，并将捕获到的事件发送给 PAN-OS 集成的 User-ID 代理。有关详细信息，请参阅 使用 XML API 将用户映射发送到 User-ID。

## 客户端探测

在 Microsoft Windows 环境中，您可以将 User-ID 代理配置为使用 Windows Management Instrumentation (WMI) 和/或 NetBIOS 探测定期探测客户端系统，以验证现有用户映射是否仍然有效，或用于获取尚未映射的 IP 地址的用户名。

仅基于 *Windows* 的 *User-ID* 代理支持 *NetBIOS* 探测；而 *PAN-OS* 集成的 *User-ID* 代理则不支持。

客户端探测专为大多数用户集中于内网 Windows 工作站的传统网络而设计，但并不是当今支持使用各种设备和操作系统的漫游和移动用户的更现代化网络的理想之选。此外，客户端探测可以生成大量的网络流量（基于映射 IP 地址的总数），并且在配置错误时可能会造成安全威胁。因此，不再推荐客户端探测用于用户映射。而是从多个孤立和可信的来源（如域控制器）以及通过与Syslog 或XML API集成来收集用户映射信息，这能够让您从任何设备类型或操作系统安全地捕获用户映射信息。如果敏感应用程序需要您准确知道用户是谁，请配置身份验证策略和身份验证门户以确保仅授权用户访问。

因为客户端探测信任从端点报告的数据，因此不推荐用于从高安全性网络中获取 *User-ID* 信息。如果您使用 *User-ID* 代理解析 *AD* 安全事件日志、*syslog* 消息或 *XML API* 以获取 *User-ID* 映射，*Palo Alto Networks* 建议禁用客户端探测。


© 2019 Palo Alto Networks, Inc.

> 如果您选择使用客户端探测，请勿在外部不可信接口上启用，因为这样会导致代理在网络外部发送包含敏感信息的客户端探测，如 *User-ID* 代理服务帐户的用户名、域名和密码哈希。攻击者可能会利用这些信息来渗透网络，以获得进一步的访问。

如果您选择在您的信任区域启用探测，代理会定期（默认情况下每 20 分钟一次，但可配置）探测每个获悉的 IP 地址，以验证同一用户仍处于登录状态。此外，如果遇到没有用户映射的 IP 地址，防火墙会将该地址发送至代理以立即进行探测。

有关详细信息，请参阅使用 Windows User-ID 代理配置用户映射或使用 PAN-OS 集成的 User-ID 代理来配置用户映射。



© 2019 Palo Alto Networks, Inc.

# 启用 User-ID

与 IP 地址相反，用户标识是有效安全基础设施的一个组成部分。知道谁正在使用您网络上的每个应用程序以及谁可能传送威胁或正在传输文件，都可以加强您的安全策略并减少事件响应时间。User-ID 使您能够利用存储在各种存储库中的用户信息，进行查看、基于用户和组的策略控制、改进日志记录、报告和取证：

STEP 1 | 启用源区域上的 User-ID，这些区域包括要发送要求控制用户访问的请求的用户。

仅在可信区域上启用 *User-ID*。如果在外部不可信区域（如互联网）上启用 *User-ID* 和客户端探测，则可以在受保护的网络之外发送探测，从而导致 *User-ID* 代理服务帐户名称、域名和加密密码哈希的信息披露，这可能会允许攻击者未经授权访问受保护的服务和应用程序。

1. 选择 **Network**（网络）> **Zones**（区域），然后单击区域 **Name**（名称）。
2. **Enable User Identification**（启用用户标识），然后单击 **OK**（确定）。

STEP 2 | 为 User-ID 代理创建专用服务帐户。

最佳实践是，创建一个服务帐户，具有支持您启用的 *User-ID* 选项所需的最低权限，以在服务帐户受到威胁时减少攻击面。

如果您计划使用基于 Windows 的 User-ID 代理或 PAN-OS 集成的 User-ID 代理来监控域控制器、Microsoft Exchange 服务器或 Windows 客户端以便用户登录和退出事件，则必须这样操作。

STEP 3 | 将用户映射到组。

这使防火墙能够连接到您的 LDAP 目录并检索组映射信息，以便您可以在创建策略时选择用户名和组名。

STEP 4 | 将 IP 地址映射到用户。

作为最佳实践，请勿在高安全性网络上启用客户端探测作为用户映射方法。客户端检测可以生成大量的网络流量，并且在配置错误时可能会造成网络威胁。

您的操作方式取决于用户所在的位置和正在使用的系统类型，以及正在网络上为用户收集登录和退出事件的系统。必须配置一个或多个 User-ID 代理以启用用户映射：

- 使用 Windows User-ID 代理配置用户映射。
- 使用 PAN-OS 集成的 User-ID 代理来配置用户映射 。
- 配置 User-ID 以监控用户映射的 Syslog 发件人。
- 为终端服务器用户配置用户映射。
- 使用 XML API 将用户映射发送到 User-ID。
- 在 HTTP 标头中插入用户名。

STEP 5 | 指定要在用户映射中包括和排除的网络。

作为最佳实践，请始终指定要在 *User-ID* 中包括和排除的网络。这样，您就可以确保仅探测受信资产，并且不会意外创建不需要的用户映射。

指定要包含和排除网络的方式取决于您使用的是基于 Windows 的 User-ID 代理还是 PAN-OS 集成的 User-ID 代理。



© 2019 Palo Alto Networks, Inc.

STEP 6 | 配置身份验证策略和身份验证门户。

防火墙在请求符合身份验证策略规则的服务、应用程序或 URL 类别时，使用身份验证门户来对最终用户进行身份验证。根据身份验证期间收集的用户信息，防火墙会创建新的用户映射或更新现有映射。身份验证期间收集的映射信息将覆盖通过其他 User-ID 方法收集的信息。

1. 配置身份验证门户。
2. 配置身份验证策略。

STEP 7 | 启用基于用户和基于组的策略执行。



如果可能，请基于组（而非用户）创建规则。当用户群发生变化时，这样做可以避免不得不长期更新规则（需要进行提交）。

配置 User-ID 后，在定义安全规则的源或目标时，可以选择用户名或组名：

1. 选择 **Policies**（策略）> **Security**（安全）并 **Add**（添加）新规则，或单击要编辑的现有规则名称。
2. 选择 **User**（用户）并采用下列其中一种方式来指定规则中要与哪些用户和组相匹配：
   - 如果要选择特定用户或组作为匹配条件，请单击“源用户”部分中的 **Add**（添加），以显示防火墙组映射功能发现的用户和组列表。选择要添加到规则的用户或组。
   - 若想要与已通过或未通过身份验证的任意用户都相匹配，且不需要知道特定用户或组名，请从 Source User（源用户）列表上的下拉列表中选择 **known-user**（已知用户）或 **unknown**（未知用户）。
3. 根据需要配置规则的其余部分，然后单击 **OK**（确定）以保存策略。有关安全规则中的其他字段的详细信息，请参阅设置基本安全策略。

STEP 8 | 创建安全策略规则，以安全地启用受信任区域内的 User-ID，并防止 User-ID 流量流出您的网络。

遵循最佳实践互联网网关安全策略，以确保您的代理（Windows 代理和 PAN-OS 集成代理）正在监控服务并分发映射到防火墙的区域仅允许 User-ID 应用程序 (`paloalto-userid-agent`)。重点：

- 代理所在区域与受监控服务器所在区域之间（或者，最好是在托管代理的特定系统与受监控服务器之间）允许 `paloalto-userid-agent` 应用程序。
- 代理与需要用户映射的防火墙之间，以及正在分发用户映射的防火墙与正在向其分发信息的防火墙之间允许 `paloalto-userid-agent` 应用程序。
- 拒绝将 `paloalto-userid-agent` 应用程序应用到任何外部区域，例如您的互联网区域。

STEP 9 | 配置防火墙以从 X-Forwarded-For (XFF) 标头获取用户 IP 地址。

当防火墙介于 Internet 和代理服务器之间时，防火墙查看到的数据包中的 IP 地址将用于代理服务器，而不是用户。相反，要查看 IP 地址，请将防火墙配置为使用 XFF 标头进行用户映射。启用此选项后，防火墙将 IP 地址与策略中引用的用户名进行匹配，以启用关联用户和组的控制和可见性。更多详细信息，请参阅识别通过代理服务器连接的用户。

1. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID**（内容-ID）并编辑 X-Forwarded-For 标头设置。
2. 选择 **X-Forwarded-For Header in User-ID**（在 **User-ID** 中使用 **X-Forwarded-For** 标头）。



选中 *Strip-X-Forwarded-For Header*（*Strip-X-Forwarded-For* 标头）不会禁止将 *XFF* 标头用于策略规则中的用户属性；防火墙只有在将 *XFF* 标头用于用户属性后才会将 *XFF* 值归零。

3. 单击 **OK**（确定）保存更改。

STEP 10 | 如果使用高可用性 (HA) 配置，请启用同步。



© 2019 Palo Alto Networks, Inc.

最佳实践是始终为 *HA* 配置启用 *Enable Config Sync*（启用配置同步）选项，以确保主动与被动防火墙之间的组映射和用户映射同步进行。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置部分。
2. 选择 **Enable HA**（启用 **HA**）。
3. 选中 **Enable Config Sync**（启用配置同步）。
4. 输入 **Peer HA1 IP Address**（对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
5. （可选）输入 **Backup Peer HA1 IP Address**（备份对等 **HA1 IP** 地址），即对等防火墙上 HA1 控制链路的 IP 地址。
6. 单击 **OK**（确定）。

STEP 11 | 提交更改。

**Commit**（提交）更改并激活。

STEP 12 | 验证 User-ID 配置。

配置用户映射和组映射后，请验证配置是否正常工作，并且是否可以安全地启用和监控用户和组对应用程序和服务的访问。



© 2019 Palo Alto Networks, Inc.

# 将用户映射到组

根据用户组成员资格（而不是个人用户）来定义策略规则将简化管理，因为这样避免了只要组成员资格发生更改，您就必须更新规则的情况。每个防火墙或 Panorama 在所有策略中可以引用的不同用户组数因型号而异。有关详细信息，请参阅兼容性矩阵。

使用以下过程可以使防火墙连接到 LDAP 目录并检索组映射信息。然后，您可以启用基于用户和基于组的策略。

以下是在 *Active Directory (AD)* 环境中进行组映射的最佳实践：

- 如果您具有单个域，则仅需要一个带 *LDAP* 服务器配置文件的组映射配置，此配置文件将防火墙连接到连接性最佳的域控制器。您最多可以将四个域控制器添加到 *LDAP* 服务器配置文件以实现冗余。请注意，通过为该域添加多个组映射配置，您不能为单个域增加四个以上的域控制器冗余。
- 如果您具有多个域和/或多个林，则必须创建一个带 *LDAP* 服务器配置文件的组映射配置，以将防火墙连接至每个域/林中的域服务器。执行相应步骤以确保单个林中用户名的唯一性。
- 如果您具有通用组，则创建一个 *LDAP* 服务器配置文件以与 *SSL* 端口 *3268* 或 *3269* 上的全局编录服务器的根域连接，然后创建另一个 *LDAP* 服务器配置文件以与端口 *389* 上的根域控制器连接。这有助于所有域和子域都能使用用户和组信息。
- 在使用组映射之前，请为基于用户的安全策略配置 *Primary Username*（主用户名），因为此属性将标识策略配置、日志和报告中的用户。

STEP 1 | 添加 LDAP 服务器配置文件。

配置文件定义防火墙如何连接到从中收集组映射信息的目录服务器。

如果创建多个使用相同的基本专有名称*(DN)*或 *LDAP* 服务器的组映射配置，那么，组映射配置不能包括重叠组（例如，一个组映射配置的包括列表不能包含已属于不同组映射配置的组）。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP**，并 **Add**（添加）服务器配置文件。
2. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。
3. **Add**（添加）LDAP 服务器。最多可以将四个服务器添加到配置文件，但这些服务器必须是相同 **Type**（类型）。对于每个服务器，输入 **Name**（名称）（以标识服务器）、**LDAP Server**（**LDAP** 服务器）IP 地址或 FQDN 以及服务器 **Port**（端口）（默认为 389）。
4. 选择服务器 **Type**（类型）。

   根据您的选择（例如 **active-directory**），防火墙自动在组映射设置中填充正确的 LDAP 属性。但是，如果您已自定义 LDAP 架构，则可能需要修改默认设置。
5. 对于 **Base DN**（基本 **DN**），输入您希望防火墙开始搜索用户和组信息的 LDAP 树位置的专有名称 (DN)。
6. 对于 **Bind DN**（绑定 **DN**）、**Password**（密码）和 **Confirm Password**（确认密码），请输入绑定到 LDAP 树的身份验证凭据。

   **Bind DN**（绑定 **DN**）可以是全限定 LDAP 名称（例如 `cn=administrator,cn=users,dc=acme,dc=local`）也可以是用户主体名称（例如 `administrator@acme.local`）。
7. 以秒为单位输入 **Bind Timeout**（绑定超时）和 **Search Timeout**（搜索超时）（默认均为 30）。
8. 单击 **OK**（确定）保存服务器配置文件。

STEP 2 | 确认组映射配置中的服务器设置。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）。
2. **Add**（添加）组映射配置。
3. 输入唯一的 **Name**（名称）以识别组映射配置。
4. 选择刚创建的 LDAP **Server Profile**（服务器配置文件）。
5. （可选）指定 **Update Interval**（更新间隔）（秒）。根据防火墙应检查 LDAP 源以获取组映射配置更新的频率，输入一个值（范围为 60—86400，默认为 3600）。如果 LDAP 源包括很多组，那么，太低的值可能不会提供足够的时间来映射所有组。
6. （可选）默认情况下，**User Domain**（用户域）字段为空：防火墙自动检测 Active Directory (AD) 服务器的域名。如果您输入一个值，则会替代防火墙从 LDAP 源检索到的任何域名。对于大多数配置，如果您需要输入一个值，则输入 NetBIOS 域名（例如，**`example`**，而非 **`example.com`**）。

   如果使用全局编录，输入一个值会替代来自此服务器的所有用户和组的域名，包括来自其他域的用户和组。
7. （可选）要筛选防火墙为组映射跟踪的组，请在组对象部分输入 **Search Filter**（搜索筛选器）（LDAP 查询）和 **Object Class**（对象类）（组定义）。
8. （可选）要筛选防火墙为组映射跟踪的用户，请在用户对象部分输入 **Search Filter**（搜索筛选器）（LDAP 查询）和 **Object Class**（对象类）（用户定义）。
9. 确保组映射配置 **Enabled**（已启用）（默认启用）。

STEP 3 | （可选）定义用户和组属性以收集用户和组映射。如果您想基于目录属性（而非域）映射用户，则必须执行此步骤。

1. 如果 User-ID 源仅发送用户名，且该用户名在整个组织内具有唯一性，请选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Setup**（设置），**Edit**（编辑）设置部分以 **Allow matching usernames without domains**（允许映射不带域的用户名），此时，防火墙可以检查在组映射时从 LDAP 服务器收集的唯一用户名是否与策略相关的用户相匹配，并避免覆盖您的源配置文件中的域。

   启用该选项前，请为包含可收集映射的 *User-ID* 源（GlobalProtect 或身份验证门户等）的 *LDAP* 组配置组映射。提交更改后，*User-ID* 源将使用不带域的用户名进行填充。只有在组映射期间收集的用户名才能在无域的情况下进行匹配。如果 *User-ID* 源以多种格式发送用户信息，且您已启用该选项，请验证防火墙收集的属性是否具有唯一的前缀。要确保启用此选项后正确标识用户，组映射的所有属性均必须具有唯一性。如果用户名不是唯一的，则防火墙在调试日志中记录错误。
2. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）> **Add**（添加）> **User and Group Attributes**（用户和组属性）> **User Attributes**（用户属性），输入想为用户标识收集的 **Directory Attribute**（目录属性）。指定 **Primary Username**（主用户名）以标识防火墙上的用户，并代表报告和日志中的用户，从而覆盖防火墙从 User-ID 源接收的任何其他格式。

   选择服务器配置文件 **Type**（类型）时，防火墙会自动填充用户和组属性值。根据 User-ID 源发送的用户信息，您可能需要正确配置下列属性：

   - 用户主体名称 **(UPN)**：**`userPrincipalName`**
   - **NetBios** 名称：**`sAMAccountName`**
   - 电子邮件 **ID**：此电子邮件的目录属性
   - **Multiple formats**（多种格式）：在启用 User-ID 源之前从用户目录检索用户映射属性。

   如果未指定主用户名，防火墙会为每个服务器配置文件类型使用下列默认值：

| 属性 | Active Directory | Novell eDirectory 或 Sun ONE Directory Server |
|---|---|---|
| 主用户名 | `sAMAccountName` | `uid` |


© 2019 Palo Alto Networks, Inc.

| 属性 | Active Directory | Novell eDirectory 或 Sun ONE Directory Server |
|---|---|---|
| 电子邮件 | `mail` | `mail` |
| 备用用户名 1 | `userPrincipalName` | 无。 |
| 组名称 | `name` | `cn` |
| 组成员 | `member` | `member` |

3. （可选）指定 **E-Mail**（电子邮件）地址格式，最多有三种 **Alternate Username**（备用用户名）格式。
4. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）> **Add**（添加）> **User and Group Attributes**（用户和组属性）> **Group Attributes**（组属性），指定 **Group Name**（组名称）、**Group Member**（组成员）和 **E-Mail**（电子邮件）地址格式。

   必须先进行提交，防火墙才能从 LDAP 服务器收集目录属性。

STEP 4 | 限制将在策略规则中可用的组。

仅当您希望将策略规则限制为特定组时才是必需的。**Group Include List**（组包括列表）和 **Custom Group**（自定义组）列表的最大组合数为每个组映射配置 640 个条目。每个条目可以是单个组，也可以是组列表。默认情况下，如果不指定组，那么所有组将在策略规则中可用。



您创建的任何自定义组也将在身份验证配置文件的允许列表中可用（配置身份验证配置文件和序列）。

1. 从目录服务添加现有组：
   1. 选择 **Group Include List**（组包括列表）。
   2. 选择要在策略规则中显示的可用组，并将其添加 (⊕) 到包括组中。
2. 如果要将策略规则基于不匹配现有用户组的用户属性，请创建基于 LDAP 筛选器的自定义组：
   1. 选择 **Custom Group**（自定义组）并 **Add**（添加）组。
   2. 输入组 **Name**（名称）（该名称在当前防火墙或虚拟系统的组映射配置中是唯一的）。

      如果 **Name**（名称）的值与现有 AD 组域的专有名称 (DN) 相同，则防火墙会将所有引用中使用自定义组用于该名称（例如，在策略和日志中）。
   3. 指定最长为 2,048 个 UTF-8 字符的 **LDAP Filter**（**LDAP** 筛选器），然后单击 **OK**（确定）。

      防火墙不会验证 LDAP 筛选器，因此您负责确保这些筛选器的精确性。

      为了最大限度地降低对 *LDAP* 目录服务器的性能影响，请在筛选器中仅使用建立了索引的属性。
3. 单击 **OK**（确定）保存更改。

   必须先进行提交，自定义组才能在策略和对象中可用。

STEP 5 | **Commit**（提交）更改。

必须先进行提交，您才能在策略和对象中使用自定义组，防火墙才能从 LDAP 服务器收集属性。



在将防火墙配置为从 *LDAP* 服务器检索组映射信息之后，但在基于所检索的组配置策略之前，最佳做法是等待防火墙刷新组映射缓存，或是手动刷新缓存。要验证当前可在策略中使用的组，请访问防火墙 CLI，然后运行 ***show user group*** 命令。要确定防火墙下一次刷新组映射缓存的时间，请运行 ***show user group-mapping statistics*** 命令，



© 2019 Palo Alto Networks, Inc.

并检查 *Next Action*。要手动刷新缓存，请运行 ***debug user-id refresh group-mapping all*** 命令。

STEP 6 | 检验用户和组映射是否已正确标识用户。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping**（组映射）> **Group Include List**（组包含列表）以确认防火墙是否已获取所有的组。
2. 要检验是否所有用户属性均已正确捕获，请使用以下 CLI 命令：

```
show user user-attributes user all
```

显示用于所有用户的用户主体名称 (UPN)、主用户名、电子邮件属性以及任何备用用户名的规范化格式：

```
admin@PA-VM-8.1> show user user-attributes user all
```

```
Primary: nam\sam-user    Email: sam-user@nam.com
```

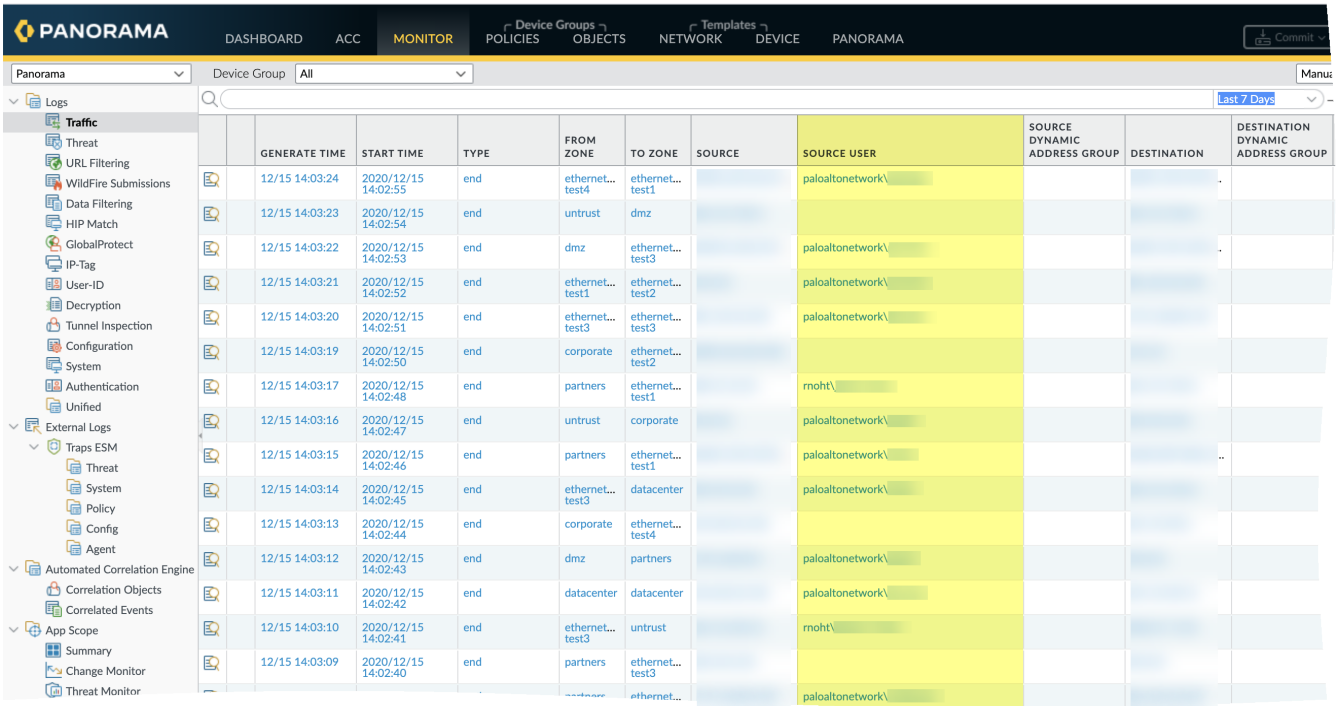
```
Alt User Names:1) nam.com\sam-user
```

```
2) nam\sam-user-upn
```

```
3) sam-user-upn@nam.local
```

```
4) sam-user@nam.com
```

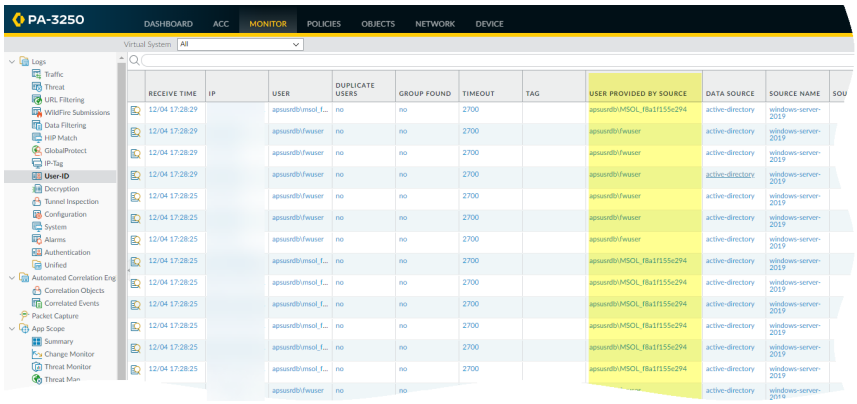
3. 检验用户名是否正确显示在 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）下的 **Source User**（源用户）列。






© 2019 Palo Alto Networks, Inc.

4. 检验用户是否已映射到 **Monitor**（监控）> **Logs**（日志）> **User-ID**（用户 **ID**）下的 **User Provided by Source**（按源提供的用户）列中的正确用户名。






© 2019 Palo Alto Networks, Inc.

# 将 IP 地址映射到用户

User-ID 提供许多不同的方法来将 IP 地址映射到用户名。在开始配置用户映射之前，请考虑用户登录的位置、访问的服务以及控制访问所需的应用程序和数据。这将通知您哪些类型的代理或集成最有助于您标识用户。

一旦确定计划，便可根据需要使用一种或多种以下方法开始配置用户映射，以实现基于用户的访问，并查看应用程序和资源：

- 如果您有用户使用未登录到域服务器的客户端系统，如运行尚未登录到域的 Linux 客户端的用户，您可以使用身份验证门户将 IP 地址映射到用户名。身份验证门户与身份验证策略组合使用，也可确保所有用户通过身份验证访问您最敏感的应用程序和数据。
- 当用户登录您的 Exchange 服务器、域控制器或 eDirectory 服务器 或 Windows 客户端，要映射用户，则必须配置 User-ID 代理：
  - 使用 PAN-OS 集成的 User-ID 代理来配置用户映射
  - 使用 Windows User-ID 代理配置用户映射
- 如果您的客户端在 Windows 环境中运行多用户系统，例如，Microsoft Terminal Server 或 Citrix Metaframe Presentation Server 或 XenApp，配置 Palo Alto Networks 终端服务器 (TS) 代理执行用户映射。对于不在 Windows 上运行的多用户系统，您可以使用 PAN-OS XML API 检索源自 Terminal Server 的用户映射。
- 要从认证用户的现有网络服务（如无线控制器、802.1x 设备、Apple Open Directory 服务器、代理服务器或其他网络访问控制 (NAC) 机制）中获取用户映射，请配置 User-ID 以监控用户映射的 Syslog 发件人。

  虽然您可以在防火墙上配置 *Windows* 代理或 *PAN-OS* 集成的 *User-ID* 代理，以侦听来自网络服务的身份验证 *syslog* 消息，但因为仅 *PAN-OS* 集成的代理支持 *TLS* 上的 *syslog* 侦听，所以其为首选配置。
- 要在传出流量标头中包含用户名和域以使网络中的其他设备能标识用户并实施基于用户的策略，您可以在 HTTP 标头中插入用户名。
- 要 共享跨虚拟系统的 User-ID 映射，您可以配置虚拟系统作为 User-ID 中心。
- 对于通过使用其他方法无法进行映射的其他客户端，您可以使用 XML API 将用户映射发送到 User-ID。
- 大规模网络可以有数百个防火墙可进行查询以便进行用户和组映射的信息源，并可以有无数个基于映射信息实施策略的防火墙。您可以通过在 User-ID 代理收集映射信息之前聚合信息，简化此类网络的 User-ID 管理。您还可以通过配置某些防火墙重新分发映射信息，减少防火墙和信息源在查询进程中使用的资源数量。有关详细信息，请参阅在大规模网络中部署 User-ID。

## 为 User-ID 代理创建专用服务帐户

要使用基于 Windows 的 User-ID 代理或 PAN-OS 集成的 User-ID 代理来映射登录到您的 Exchange 服务器、域控制器、eDirectory 服务器或 Windows 客户端的用户，则必须在代理将监控其中每个域的域控制器上为 User-ID 代理创建一个专用服务帐户。

User-ID 代理将根据安全事件日志映射用户。为确保 User-ID 代理成功映射用户，请确认映射源为审核登录、审核 Kerberos 身份验证服务、以及审核 Kerberos 服务票证操作事件生成了日志。源至少应为下列事件生成日志：

- 登录成功 (4624)
- 已授予身份验证票证 (4768)
- 已授予服务票证 (4769)
- 已续订所授予的票证 (4770)

服务帐户所需的权限取决于您计划使用的用户映射方法和设置。例如，如果正在使用 PAN-OS 集成 User-ID 代理，则服务账户需要服务器操作员权限以监视用户会话。如果正在使用基于 Windows 的 User-ID 代理，



© 2019 Palo Alto Networks, Inc.

则服务账户不需要服务器操作员权限来监视用户会话。为了降低 User-ID 服务帐户损害的风险，请始终使用代理运行所需的最低权限来配置该帐户。

- 如果在受支持的 Windows 服务器上安装基于 Windows 的 User-ID 代理，则为 Windows User-ID 代理配置服务帐户。
- 如果在防火墙上使用 集成有 PAN-OS 的 User-ID 代理，则为 集成有 PAN-OS 的 User-ID 代理配置服务帐户。

*User-ID* 提供许多安全收集用户映射信息的方法。一些传统功能专门设计用于仅需要将用户映射到连接至本地网络的 *Windows* 桌面的环境，需要特权服务帐户。如果特权服务帐户受到损害，则会打开您的网络进行攻击。最佳做法是，避免使用需要权限的传统功能（客户端探测和会话监控），否则一旦受到攻击，就会构成威胁。

## 为 *Windows User-ID* 代理创建服务帐户

为 Windows User-ID 代理创建专用 Active Directory (AD) 服务帐户以访问其将进行监视以便收集用户映射的服务和主机。您必须在代理将监控的每个域中创建一个服务帐户。启用服务帐户所需的权限后，使用 Windows User-ID 代理配置用户映射。

以下工作流程将详细说明所需的所有特权，并提供有关 *User-ID* 功能需要可能构成威胁的特权的指导，以便您可以决定如何在不影响整体安全状态的情况下最佳地标识用户。

STEP 1 | 为 User-ID 代理创建 AD 服务帐户。

您必须在代理将监控的每个域中创建一个服务帐户。

1. 登录到域控制器。
2. 右键单击 Windows 图标 (.)，**Search**（搜索）**`Active Directory Users and Computers`**（**`Active Directory`** 用户和计算机），然后启动应用程序。
3. 在导航窗格中，打开域树，右键单击 **Managed Service Accounts**（托管服务帐户），然后选择 **New**（新建）> **User**（用户）。
4. 输入用户的 **First Name**（名字）、**Last Name**（姓氏）和 **User logon name**（用户登录名），然后单击 **Next**（下一步）。
5. 输入 **Password**（密码）和 **Confirm Password**（确认密码），然后单击 **Next**（下一步）和 **Finish**（完成）。

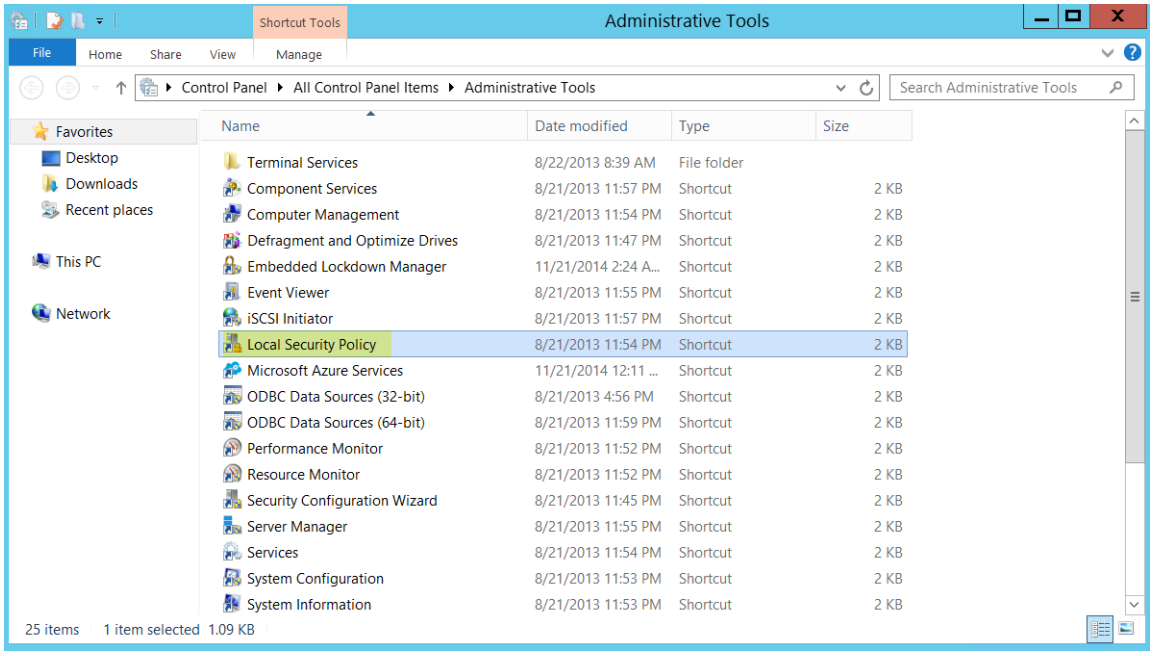
STEP 2 | 配置本地或组策略，以允许服务帐户作为服务登录。

以服务身份登录的权限仅在充当代理主机的 Windows 服务器上本地需要。

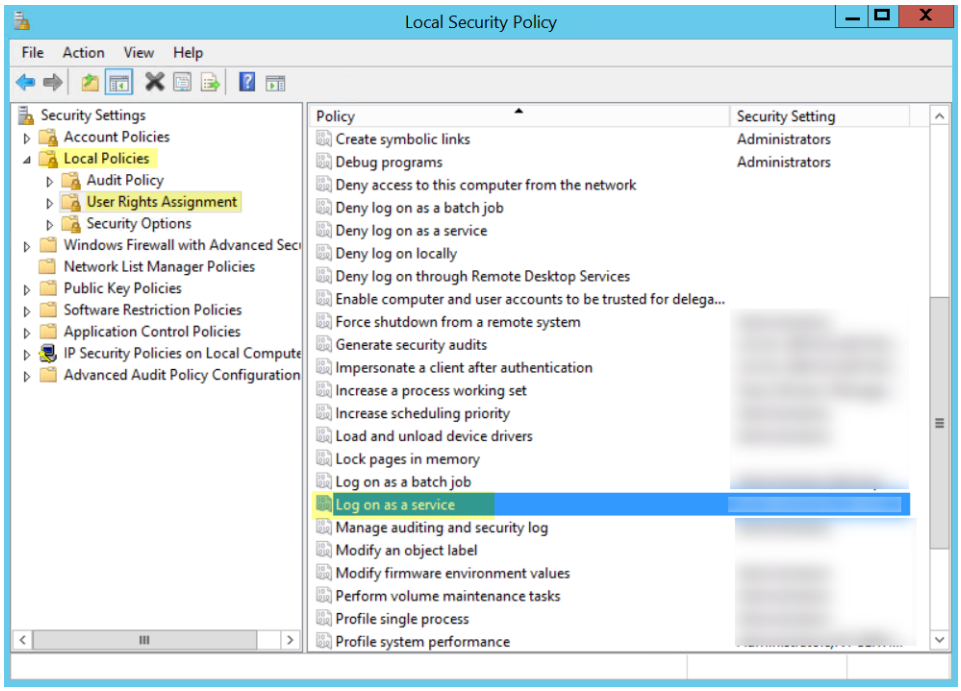
- 要本地分配权限：
  1. 请选择 **Control Panel**（控制面板）> **Administrative Tools**（管理工具）> **Local Security Policy**（本地安全策略）。



© 2019 Palo Alto Networks, Inc.

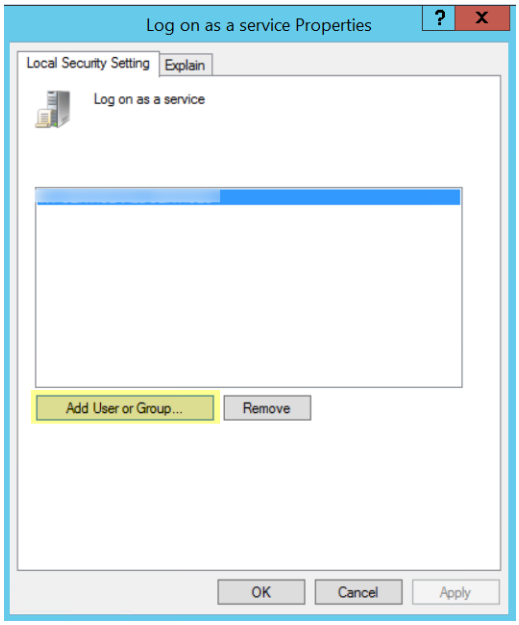
2. 


3. 选择 **Local Policies**（本地策略）> **User Rights Assignment**（用户权限分配）> **Log on as a service**（以服务身份登录）。

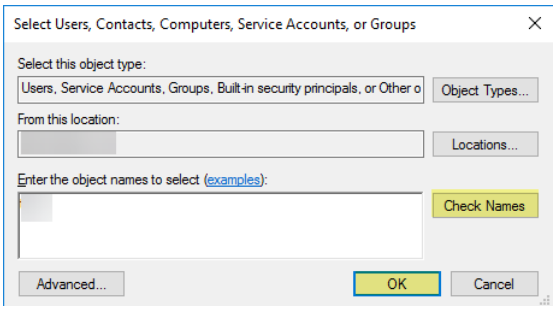



4. **Add User or Group**（添加用户或组）以添加服务账户。


© 2019 Palo Alto Networks, Inc.

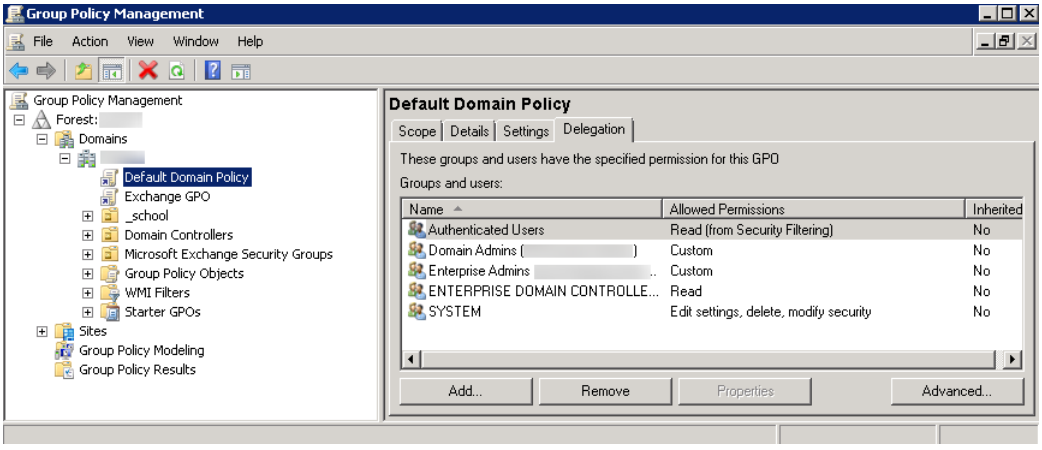



5. 以 **domain\username** 格式 **Enter the object names to select**（输入对象名称以选择）（服务帐户名称），然后单击 **OK**（确定）。




- 要在多个服务器上安装 Windows User-ID 代理的情况下配置组策略，请使用组策略管理编辑器。

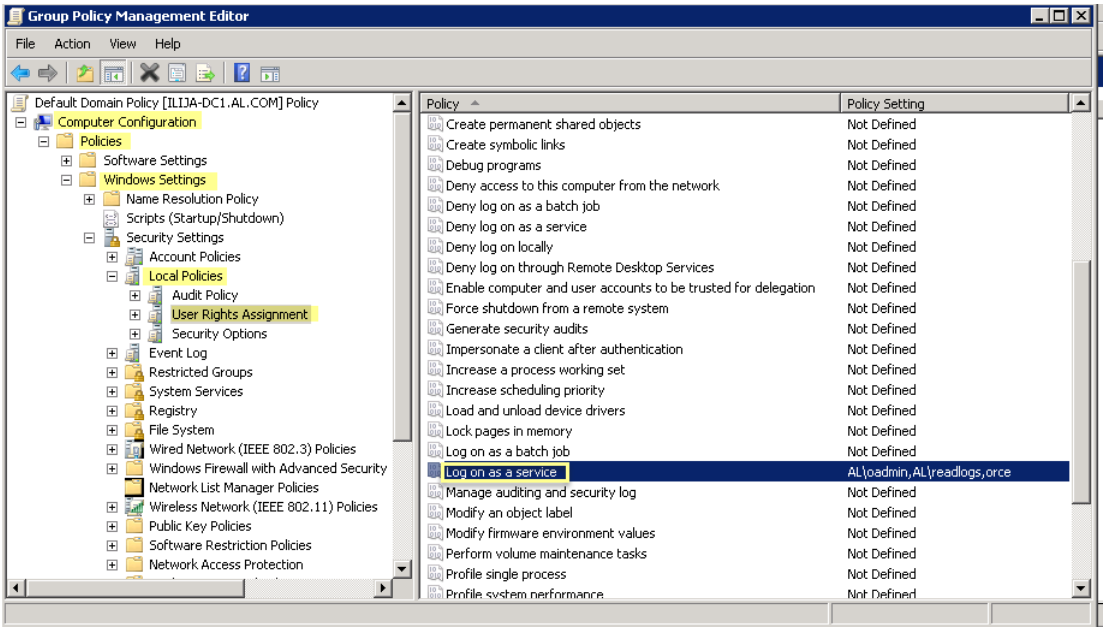
1. 为用作代理主机的 Windows 服务器选择 **Start**（启动）> **Group Policy Management**（组策略管理）> **<your domain>**（您的域名）> **Default Domain Policy**（默认域策略）> **Action**（操作）> **Edit**（编辑）。




2. 选择 **Computer Configuration**（计算机配置）> **Policies**（策略）> **Windows Settings**（Windows 设置）> **Security Settings**（安全设置）> **Local Policies**（本地策略）> **User Rights Assignment**（用户权限分配）。

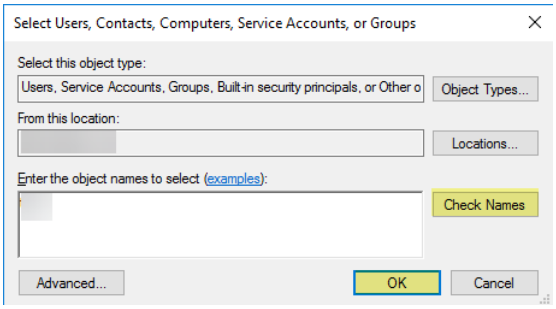


© 2019 Palo Alto Networks, Inc.




3. 右键单击 **Log on as a service**（以服务身份登录），然后选择 **Properties**（属性）。
4. **Add User or Group**（添加用户或组）以添加帐户用户名或 builtin 组，然后双击 **OK**（确定）。

管理员默认拥有此特权。




STEP 3 | 如果要使用WMI收集用户数据，分配 DCOM 权限给服务帐户，这样，就可以在受监控的服务器上使用 WMI 查询。

1. 选择 **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **<your domain>**（您的域）> **Builtin** > **Distributed COM Users**（分配的 **COM** 用户）。
2. 右键单击 **Properties**（属性）> **Members**（成员）> **Add**（添加），然后输入服务帐户名称。

STEP 4 | 如果计划使用 WMI 探测，请启用该帐户以读取待探测客户端系统上的 CIMV2 命名空间，并分配所需许可。

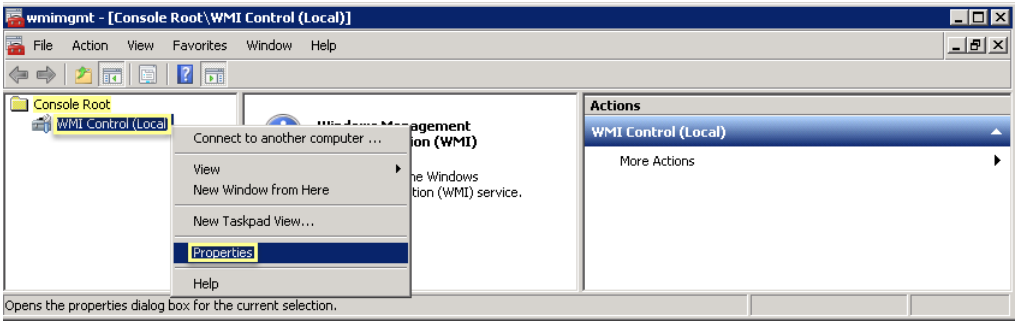
请不要在高安全性网络中启用客户端探测。客户端检测可以生成大量的网络流量，并且在配置错误时可能会造成网络威胁。而是从多个孤立和可信的来源（如域控制器）以及通过与 *Syslog* 或 *XML API* 集成来收集用户映射信息，这能够让您从任何设备类型或操作系统安全地捕获用户映射信息，而不只是从 *Windows* 客户端收集。

在 User-ID 代理将针对用户映射信息进行探测的每个客户端系统上执行此任务：

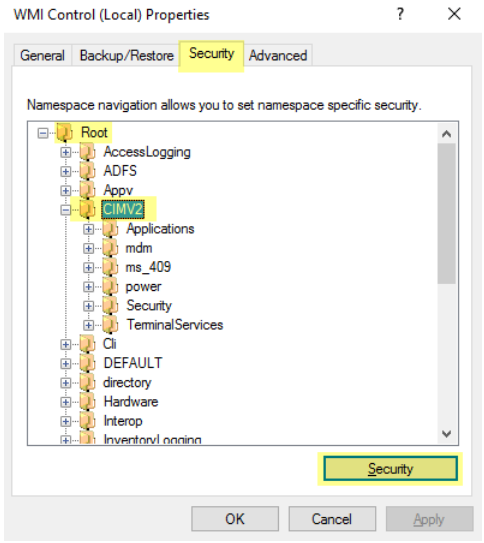
1. 右键单击 Windows 图标 (⊞)，**Search**（搜索）**`wmimgmt.msc`**，然后启动 WMI 管理控制台。


© 2019 Palo Alto Networks, Inc.

2. 在控制台树中，右键单击 **WMI Control**（**WMI 控制**），然后选择 **Properties**（**属性**）。




3. 选择 **Security**（**安全**）选项卡，然后选择 **Root**（**根**）> **CIMV2**，并单击 **Security**（**安全**）按钮。



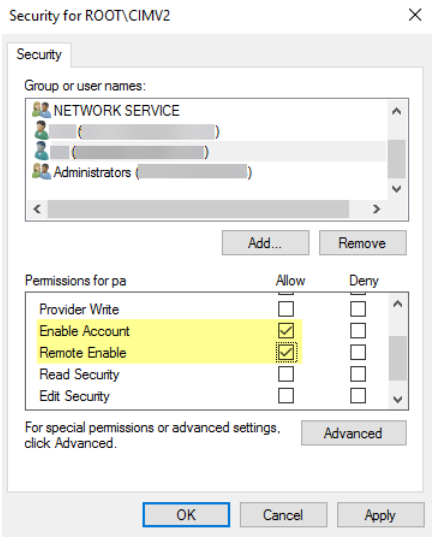

4. **Add**（**添加**）创建的服务帐户名称，**Check Names**（**检查名称**）以验证您的条目，然后单击 **OK**（**确定**）。

   您可能需要更改 *Locations*（*位置*）或单击 *Advanced*（*高级*）查询帐户名称。有关详细信息，请参阅对话框帮助。

5. 在 **<Username>** 部分的权限中，**Allow**（**允许**）**Enable Account**（**启用帐户**）和 **Remote Enable**（**远程启用**）权限。



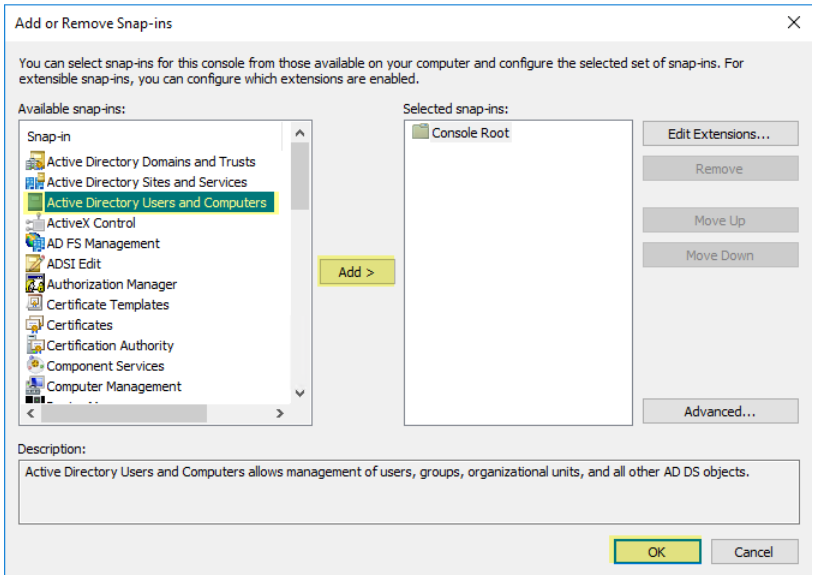
© 2019 Palo Alto Networks, Inc.




6. 双击 **OK**（确定）。
7. 使用本地用户和组 MMC 管理单元 (lusrmgr.msc) 将服务帐户添加到将要探测的系统本地分布式组件对象模型 (DCOM)用户和远程桌面用户组。

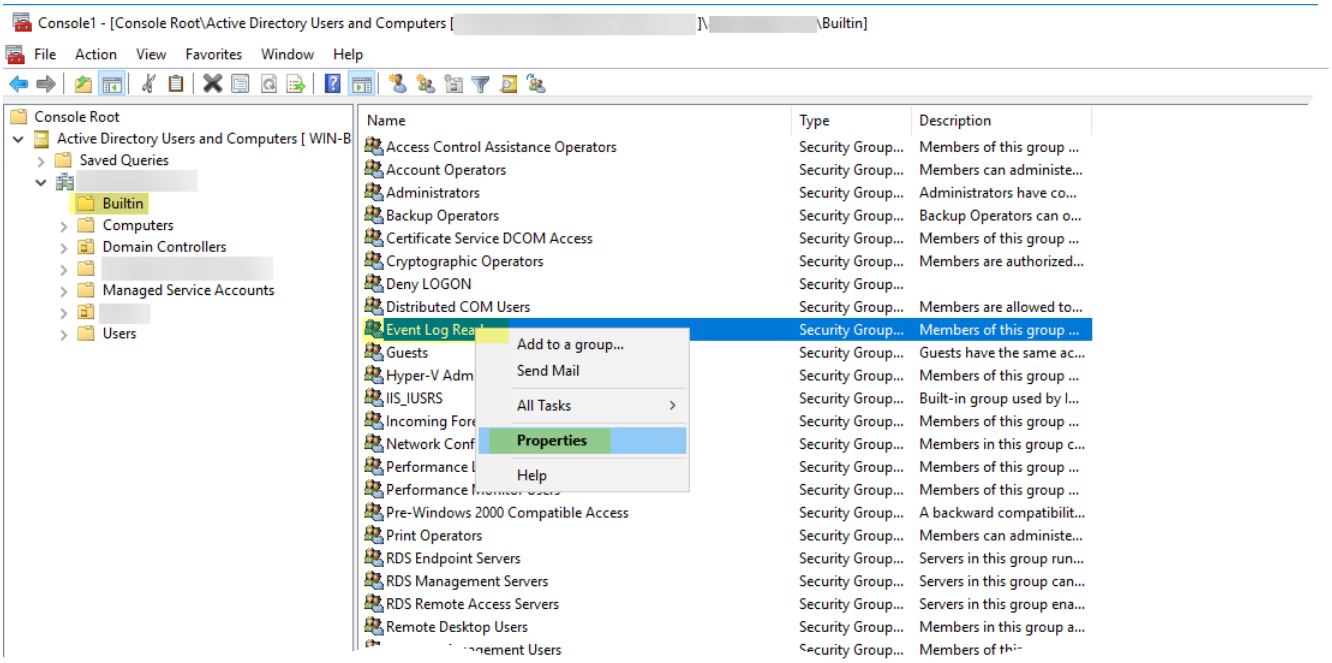
STEP 5 | 如果想要使用 服务器监视 以标识用户，则添加服务帐户至事件日志读取器 builtin 组，以允许服务帐户读取安全日志事件。

1. 在包含您想要 User-ID 代理读取的日志的域控制器或 Exchange 服务器，或在从 Windows 日志转发接收事件的成员服务器上，选择 **Start**（开始）> **Run**（运行），并输入 **MMC**。
2. 选择 **File**（文件）> **Add/Remove Snap-in**（添加/删除管理单元）> **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **Add**（添加），然后单击 **OK**（确定）以运行 MMC，并启动 Active Directory 用户和计算机管理单元。

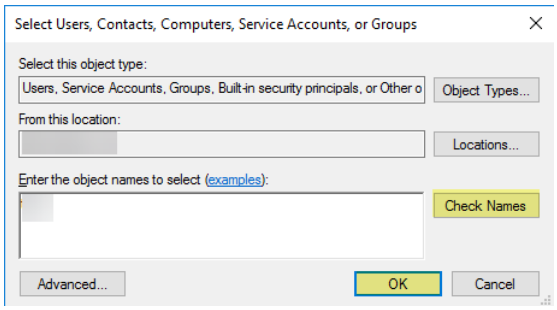



3. 导航至域的 Builtin 文件夹，右键单击 **Event Log Reader**（事件日志读取器）组，然后选择**Properties**（属性）> **Members**（成员）。


© 2019 Palo Alto Networks, Inc.




4. **Add**（添加）服务账户，然后单击 **Check Names**（检查名称）以验证您是否拥有正确的对象名称。




5. 单击 **OK**（确定）两次以保存设置。
6. 确认 Builtin 事件日志读取器组是否将服务账户列为成员（**Event Log Readers**（事件日志读取器）> **Properties**（属性）> **Members**（成员））。

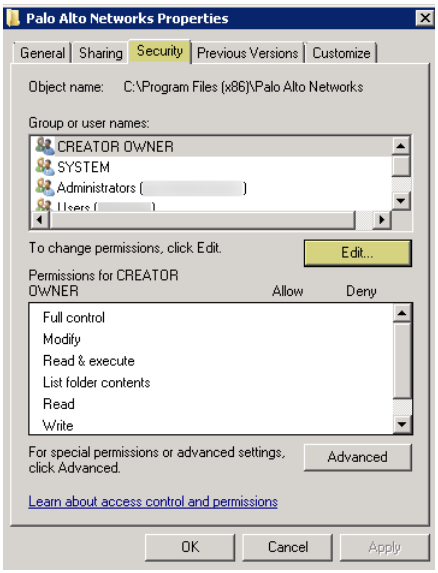
STEP 6 | 分配账户权限至安装文件夹，允许服务账户访问代理的安装文件件，从而读取配置，写入日志。

如果为 User-ID 代理配置的服务帐户不是域管理员，也不是 User-ID 代理服务器主机上的本地管理员，则只需执行此步骤。

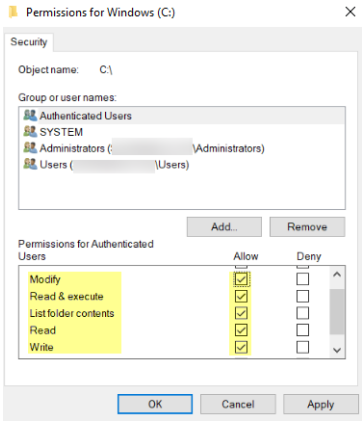
1. 从 Windows 资源管理器，导航至 `C:\Program Files(x86)\Palo Alto Networks`，右键单击文件夹，然后选择 **Properties**（属性）。
2. 在 **Security**（安全）选项卡上，单击 **Edit**（编辑）。



© 2019 Palo Alto Networks, Inc.




3. **Add**（添加）User-ID 代理服务帐户，并 **Allow**（允许） **Modify**（修改）、**Read & execute**（读取和执行）、**List folder contents**（列出文件夹内容）、**Read**（读取）和 **Write**（写入）权限，然后单击 **OK**（确定）以保存帐户设置。

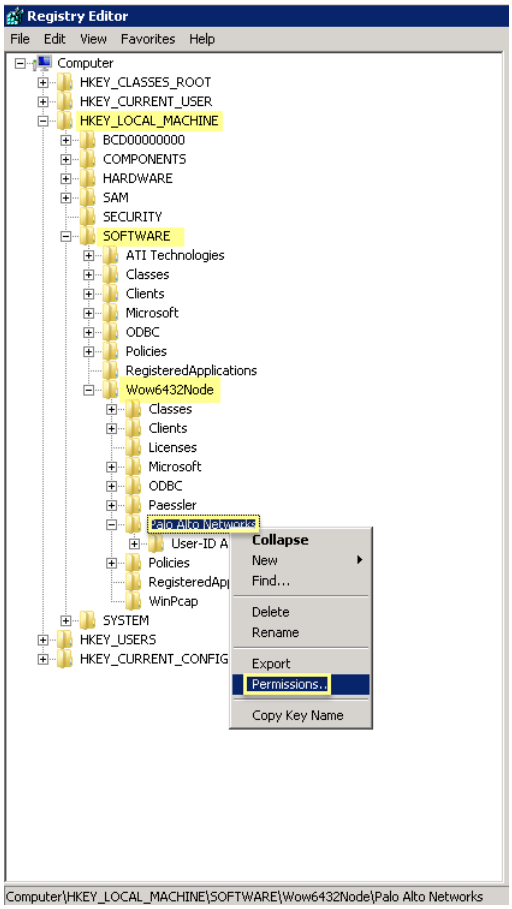



如果您不想配置单个权限，可以改为 *Allow*（允许）*Full Control*（完全控制）权限。

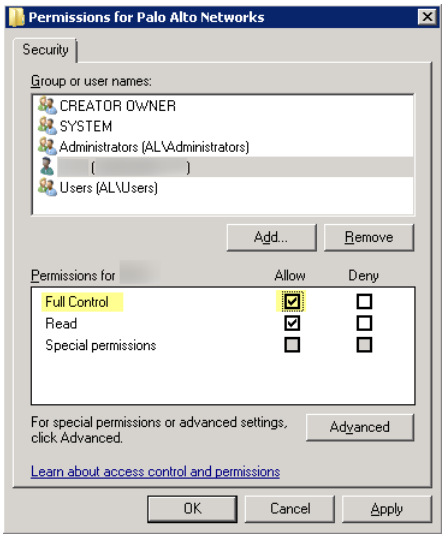
STEP 7 | 要允许代理更改配置（例如，如果选择不同的日志记录级别），为 User-ID 代理注册表的子目录树分配服务帐户权限。

1. 选择 **Start**（启动）> **Run**（运行），输入 **`regedt32`**，然后导航至下列位置之一中的 Palo Alto Networks 子目录树：
   - **32 位系统** — `HKEY_LOCAL_MACHINE\Software\ Palo Alto Networks`
   - **64 位系统** — `HKEY_LOCAL_MACHINE\Software\WOW6432Node\PaloAlto Networks`
2. 右键单击 **Palo Alto Networks** 节点，并选择 **Permissions**（权限）。


© 2019 Palo Alto Networks, Inc.




3. 为 User-ID 服务帐户分配 **Full Control**（完全控制）权限，然后单击 **OK**（确定）以保存设置。




STEP 8 | 禁用不需要的服务帐户权限。

确保 User-ID 服务帐户具有最低帐户权限，您可以减少帐户受到损害的攻击面。

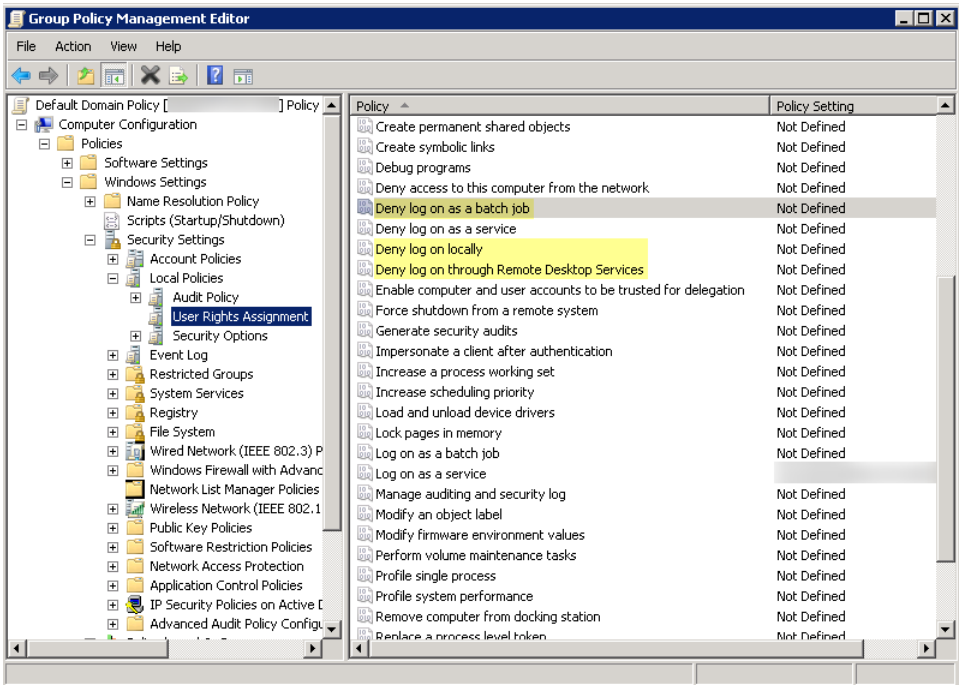
为确保 User-ID 帐户具有必要的最低权限，请拒绝该帐户的以下权限。



© 2019 Palo Alto Networks, Inc.

- 拒绝 **User-ID** 服务帐户的交互式登录 — 尽管 User-ID 服务帐户确实需要读取和解析 Active Directory 安全事件日志的权限，但无需以交互方式登录到服务器或域系统。您可以使用组策略或使用托管服务帐户来限制此权限（有关详细信息，请参阅 Microsoft TechNet）。

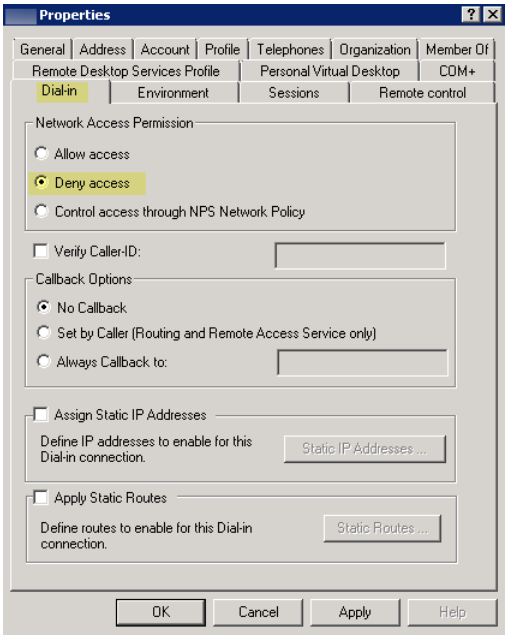
  1. 选择 **Group Policy Management Editor**（组策略管理编辑器）> **Default Domain Policy**（默认域策略）> **Computer Configuration**（计算机配置）> **Policies**（策略）> **Windows Settings**（Windows 设置）> **Security Settings**（安全设置）> **User Rights Assignment**（用户权限分配）。
  2. 对于**Deny log on as a batch job**（拒绝作为批处理作业登录）、**Deny log on locally**（拒绝本地登录）以及 **Deny log on through Remote Desktop Services**（拒绝通过远程桌面服务登录），右键单击 **Properties**（属性）。
  3. 选择 **Define these policy settings**（定义这些策略设置）> **Add User or Group**（添加用户或组）并添加服务帐户名称，然后单击 **OK**（确定）。




- 拒绝 **User-ID** 服务帐户的远程访问 — 这样可以防止攻击者使用该帐户从网络外部访问您的网络。

  1. 选择 **Start**（启动）> **Run**（运行），输入 **MMC**，然后选择 **File** > **Add/Remove Snap-in**（添加/删除管理单元）> **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **Users**（用户）。
  2. 右键单击服务帐户名称，然后选择 **Properties**（属性）。
  3. 选择 **Dial-in**（拨入），然后 **Deny**（拒绝）**Network Access Permission**（网络访问权限）。


© 2019 Palo Alto Networks, Inc.




STEP 9 | 下一步，使用 Windows User-ID 代理配置用户映射。

## 为 集成有 *PAN-OS* 的 *User-ID* 代理创建服务帐户

为 PAN-OS 集成 User-ID 代理创建专用 Active Directory (AD) 服务帐户，以访问其进行监视以收集用户映射的服务和主机。您必须在代理监视的每个域中创建服务帐户。启用服务帐户所需权限后，使用集成有 PAN-OS 的 User-ID 代理配置用户映射。

以下工作流程将详细说明所需的所有特权，并提供有关 *User-ID* 功能需要可能构成威胁的特权的指导，以便您可以决定如何在不影响整体安全状态的情况下最佳地标识用户。

STEP 1 | 为 User-ID 代理创建 AD 服务帐户。

您必须在代理将监控的每个域中创建一个服务帐户。

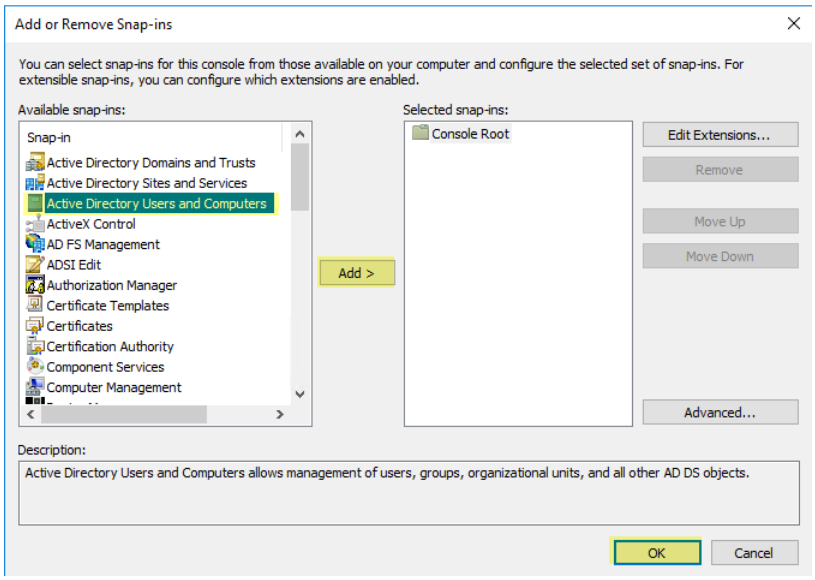
1. 登录到域控制器。
2. 右键单击 Windows 图标 (⊞)，**Search**（搜索）**`Active Directory Users and Computers`**（**`Active Directory`** 用户和计算机），然后启动应用程序。
3. 在导航窗格中，打开域树，右键单击 **Managed Service Accounts**（托管服务帐户），然后选择 **New**（新建）> **User**（用户）。
4. 输入用户的 **First Name**（名字）、**Last Name**（姓氏）和 **User logon name**（用户登录名），然后单击 **Next**（下一步）。
5. 输入 **Password**（密码）和 **Confirm Password**（确认密码），然后单击 **Next**（下一步）和 **Finish**（完成）。

STEP 2 | 如果想要使用 服务器监视 以标识用户，则添加服务帐户至事件日志读取器 builtin 组，以允许服务帐户读取安全日志事件。

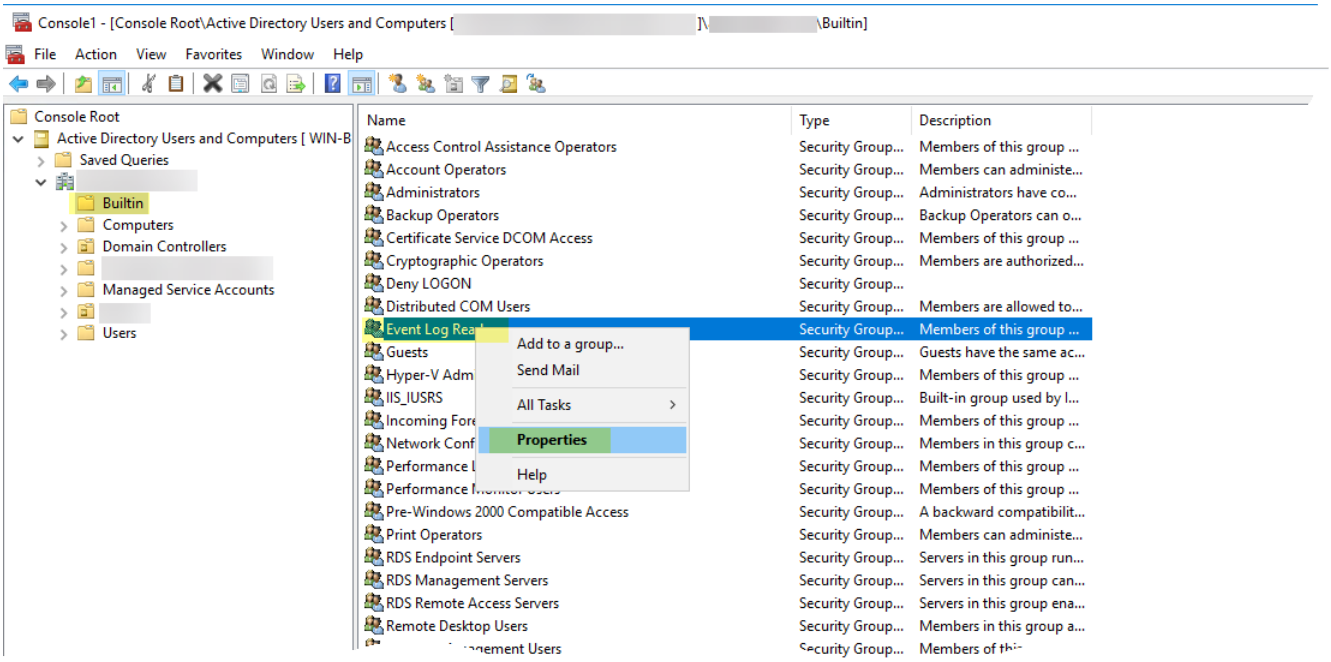
1. 在包含您想要 User-ID 代理读取的日志的域控制器或 Exchange 服务器，或在从 Windows 日志转发接收事件的成员服务器上，选择 **Start**（开始）> **Run**（运行），并输入 **`MMC`**。
2. 选择 **File**（文件）> **Add/Remove Snap-in**（添加/删除管理单元）> **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **Add**（添加），然后单击 **OK**（确定）以运行 MMC，并启动 Active Directory 用户和计算机管理单元。



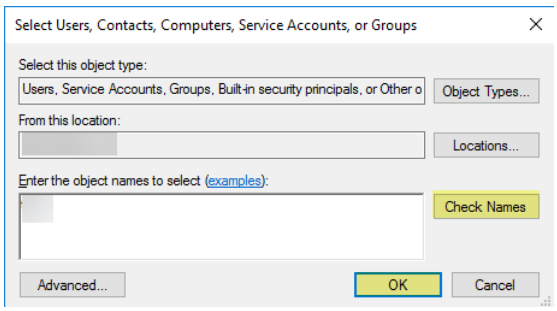
© 2019 Palo Alto Networks, Inc.




3. 导航至域的 Builtin 文件夹，右键单击 **Event Log Reader**（事件日志读取器）组，然后选择**Properties**（属性） > **Members**（成员）。




4. **Add**（添加）服务账户，然后单击 **Check Names**（检查名称）以验证您是否拥有正确的对象名称。




5. 单击 **OK**（确定）两次以保存设置。


© 2019 Palo Alto Networks, Inc.

6. 确认 Builtin 事件日志读取器组是否将服务账户列为成员（**Event Log Readers**（事件日志读取器）> **Properties**（属性）> **Members**（成员））。

STEP 3 | 如果要使用WMI收集用户数据，分配 DCOM 权限给服务帐户，这样，就可以在受监控的服务器上使用 WMI 查询。

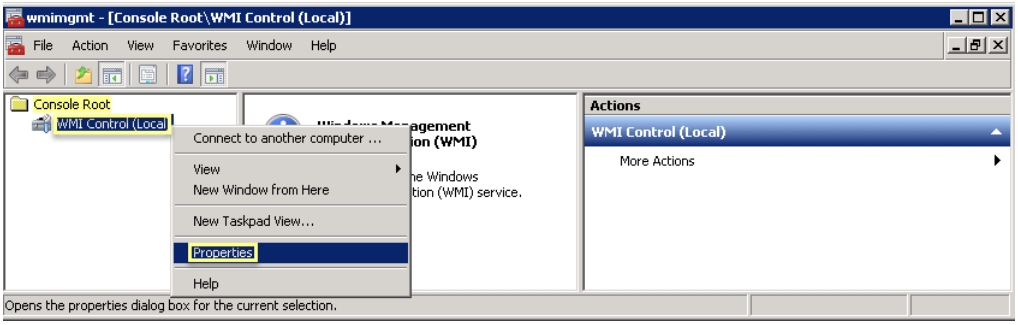
1. 选择 **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **<your domain>**（您的域）> **Builtin** > **Distributed COM Users**（分配的 **COM** 用户）。
2. 右键单击 **Properties**（属性）> **Members**（成员）> **Add**（添加），然后输入服务帐户名称。

STEP 4 | 如果计划使用WMI 探测，请启用此服务帐户以读取想要监视的域控制器上的 CIMV2 命名空间，并为待探测客户端系统分配所需许可。

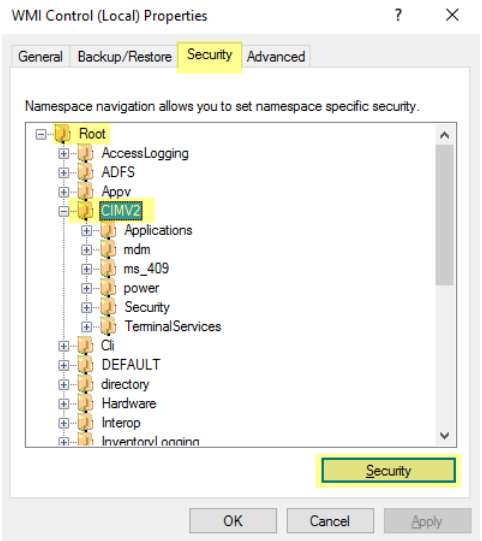
请不要在高安全性网络中启用客户端探测。客户端检测可以生成大量的网络流量，并且在配置错误时可能会造成网络威胁。而是从多个孤立和可信的来源（如域控制器）以及通过与 *Syslog* 或 *XML API* 集成来收集用户映射信息，这能够让您从任何设备类型或操作系统安全地捕获用户映射信息，而不只是从 *Windows* 客户端收集。

在 User-ID 代理将针对用户映射信息进行探测的每个客户端系统上执行此任务：

1. 右键单击 Windows 图标，**Search**（搜索）`wmimgmt.msc`，然后启动 WMI 管理控制台。
2. 在控制台树中，右键单击 **WMI Control**（**WMI** 控制），然后选择 **Properties**（属性）。




3. 选择 **Security**（安全）选项卡，然后选择 **Root**（根）> **CIMV2**，并单击 **Security**（安全）按钮。



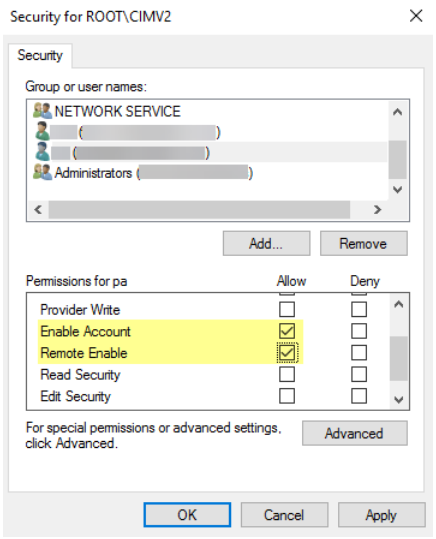

4. **Add**（添加）创建的服务帐户名称，**Check Names**（检查名称）以验证您的条目，然后单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

您可能需要更改 *Locations*（位置）或单击 *Advanced*（高级）查询帐户名称。有关详细信息，请参阅对话框帮助。

5. 在 **<Username>** 部分的权限中，**Allow**（允许）**Enable Account**（启用帐户）和 **Remote Enable**（远程启用）权限。




6. 双击 **OK**（确定）。
7. 使用本地用户和组 MMC 管理单元 (lusrmgr.msc) 将服务帐户添加到将要探测的系统本地分布式组件对象模型 (DCOM)用户和远程桌面用户组。

STEP 5 | （不推荐）要允许代理监视用户会话以轮询 Windows 服务器，从而获取用户映射信息，请为此服务帐户分配服务器操作员权限。

因为此组还具有关闭和重新启动服务器的权限，仅在监控的用户会话非常重要时才为该组分配该帐户。

1. 选择 **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **<your domain>**（您的域）> **Builtin** > **Server Operators Group**（服务器操作员组）。
2. 右键单击 **Properties**（属性）> **Members**（成员）> **Add**（添加），以添加服务帐户名称

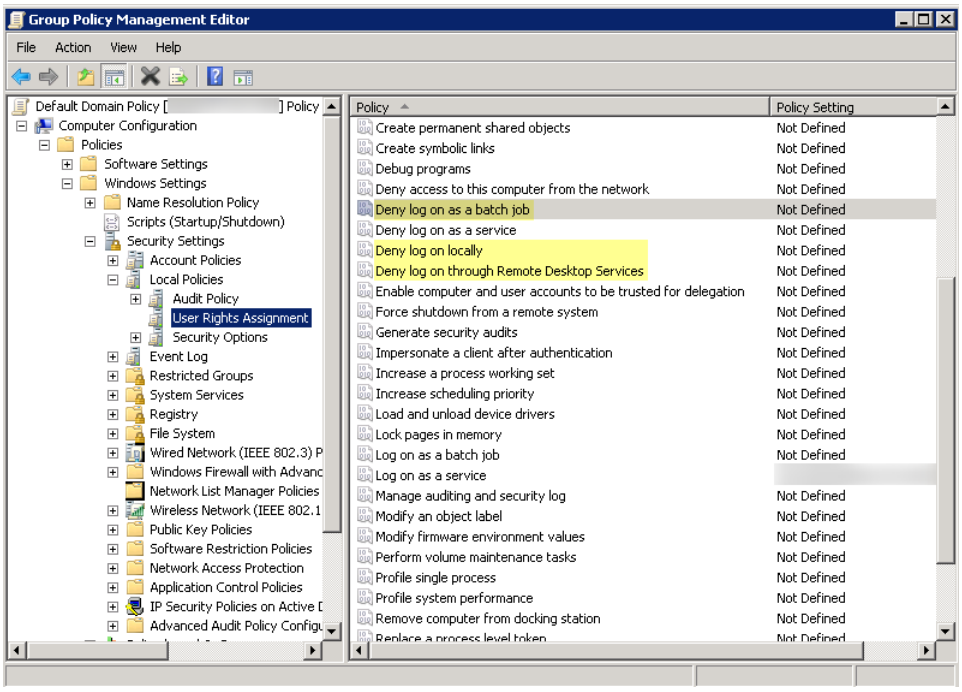
STEP 6 | 禁用不需要的服务帐户权限。

确保 User-ID 服务帐户具有最低帐户权限，您可以减少帐户受到损害的攻击面。

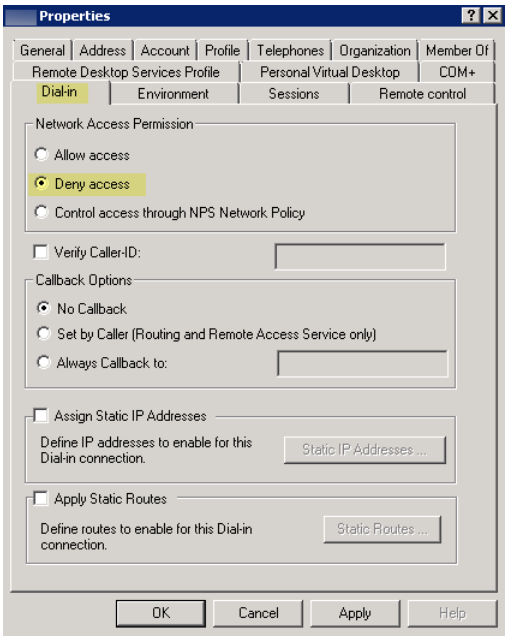
为确保 User-ID 帐户具有必要的最低权限，请拒绝该帐户的以下权限：

- 拒绝 **User-ID** 服务帐户的交互式登录 — 尽管 User-ID 服务帐户确实需要读取和解析 Active Directory 安全事件日志的权限，但无需以交互方式登录到服务器或域系统。您可以使用组策略或使用托管服务帐户来限制此权限（有关详细信息，请参阅 Microsoft TechNet）。
  1. 选择 **Group Policy Management Editor**（组策略管理编辑器）> **Default Domain Policy**（默认域策略）> **Computer Configuration**（计算机配置）> **Policies**（策略）> **Windows Settings**（**Windows** 设置）> **Security Settings**（安全设置）> **User Rights Assignment**（用户权限分配）。
  2. 对于 **Deny log on as a batch job**（拒绝作为批处理作业登录）、**Deny log on locally**（拒绝本地登录）以及 **Deny log on through Remote Desktop Services**（拒绝通过远程桌面服务登录），右键单击 **Properties**（属性），然后选择**Define these policy settings**（定义这些策略设置）> **Add User or Group**（添加用户或组），添加服务帐户名称，并单击 **OK**（确定）。


© 2019 Palo Alto Networks, Inc.




- 拒绝 **User-ID** 服务帐户的远程访问 — 这样可以防止攻击者使用该帐户从网络外部访问您的网络。
  1. **Start**（开始）> **Run**（运行），输入 **MMC**，并选择 **File** > **Add/Remove Snap-in**（添加/删除管理单元）> **Active Directory Users and Computers**（**Active Directory** 用户和计算机）> **Users**（用户）。
  2. 右键单击服务帐户名称，然后选择 **Properties**（属性）。
  3. 选择 **Dial-in**（拨入），然后 **Deny**（拒绝）**Network Access Permission**（网络访问权限）。




STEP 7 | 下一步，使用 集成有 PAN-OS 的 User-ID 代理配置用户映射。



© 2019 Palo Alto Networks, Inc.

# 使用 Windows User-ID 代理配置用户映射

在大多数情况下，大部分网络用户都将登录到您监视的域服务中。对于这些用户，Palo Alto Networks User-ID 代理监视登录事件的服务器，并执行 IP 地址到用户名的映射。配置 User-ID 代理所采用的方式取决于环境规模的大小和域服务器所在位置。最佳实践是，将 User-ID 代理安装于监控的服务器旁（即受监控服务器和 Windows User-ID 代理不应相互跨 WAN 链接）。这是因为用户映射的大多数通信都出现在代理与受监控服务器之间，只有少量的通信（上次更新后用户映射的增量）是从代理到防火墙。

以下主题介绍如何安装和配置 User-ID 代理，以及如何配置防火墙检索代理发出的用户映射信息：

- 安装基于 Windows 的 User-ID 代理
- 为用户映射配置 Windows User-ID 代理

## 安装基于 *Windows* 的 *User-ID* 代理

以下步骤介绍如何在域中的成员服务器上安装 User-ID 代理以及利用所需权限设置服务帐户。如果正在升级，安装程序将自动移除旧版本，但是，运行安装程序前，最好备份 config.xml 文件。

有关与安装基于 *Windows* 的 *User-ID* 代理的系统要求相关的信息以及有关受支持服务器 *OS* 版本的信息，请参阅User-ID 代理发行说明和Palo Alto Networks 兼容性矩阵。

STEP 1 | 为 User-ID 代理创建专用 Active Directory 服务帐户以访问其将进行监控以便收集用户映射的服务和主机。

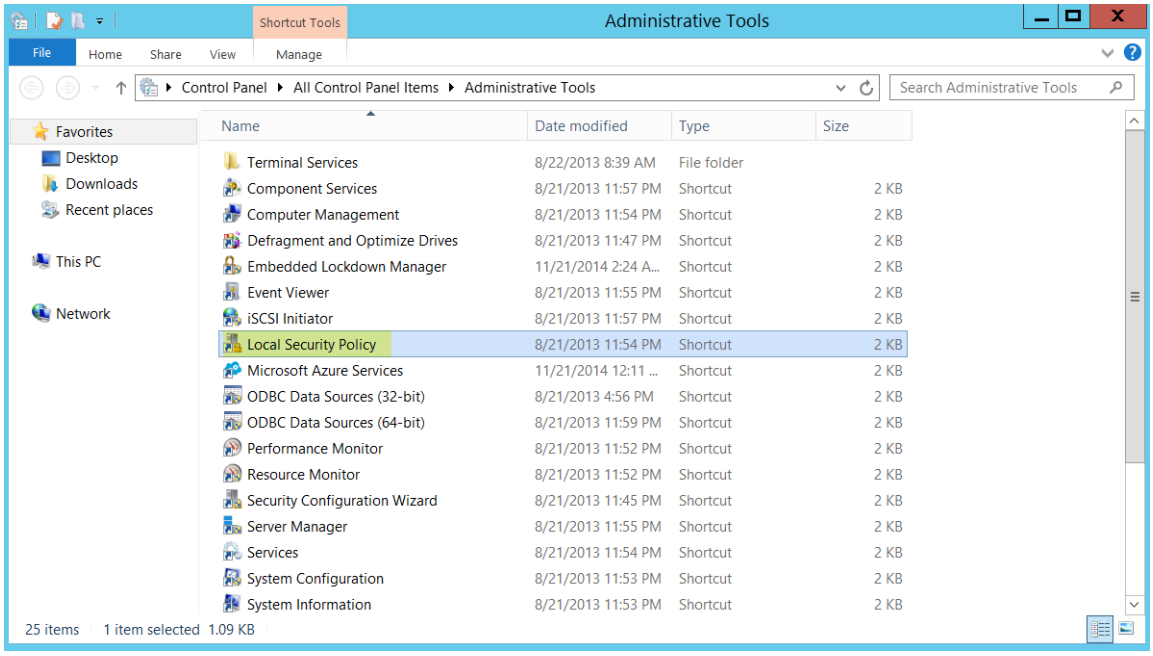
为 User-ID 代理创建专用服务帐户 ，并为 Windows User-ID 代理授予必要的权限。

1. 通过配置本地或组策略，使服务账号以服务身份登录。
    1. 如果在多个服务器上安装基于 Windows 的 User-ID 代理，则配置组策略，然后为充当代理主机的 Windows 服务器选择 **Group Policy Management**（组策略管理）> **Default Domain Policy**（默认域策略）> **Computer Configuration**（计算机配置）> **Policies**（策略）> **Windows Settings**（**Windows** 设置）> **Security Settings**（安全设置）> **Local Policies**（本地策略）> **User Rights Assignment**（用户权限分配）。
    2. 右键单击 **Log on as a service**（以服务身份登录），然后选择 **Properties**（属性）。
    3. 添加服务账户用户名或 builtin 组（默认情况下，管理员拥有此权限）。

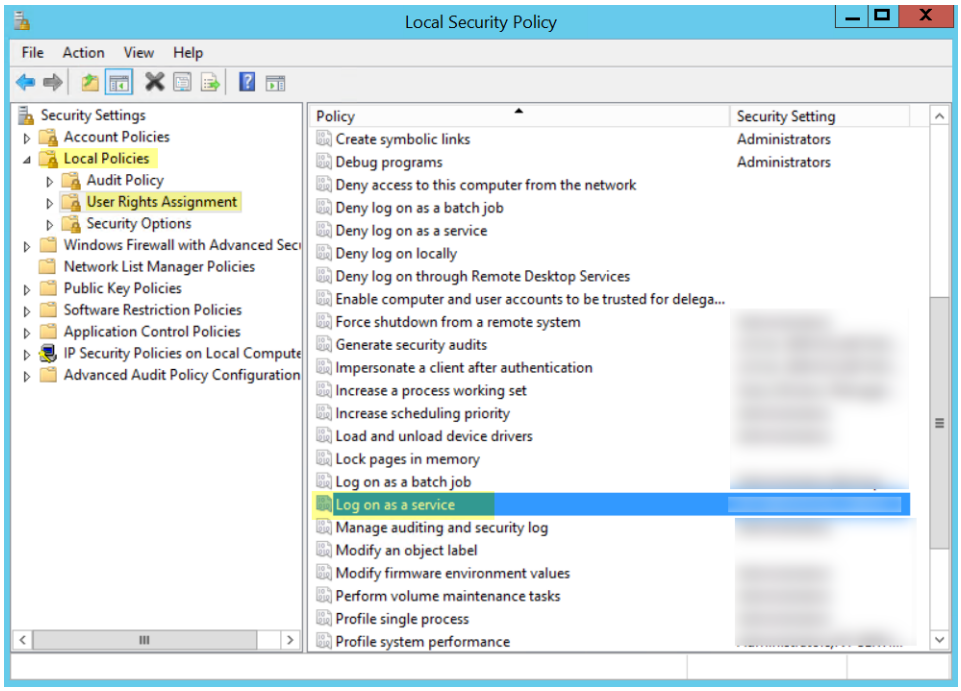
    以服务身份登录的权限仅在充当代理主机的 *Windows* 服务器上本地需要。如果仅使用一个 *User-ID* 代理，则可以使用以下说明本地授予代理主机上的权限。

    1. 要本地分配权限，请选择 **Control Panel**（控制面板）> **Administrative Tools**（管理工具）> **Local Security Policy**（本地安全策略）。


© 2019 Palo Alto Networks, Inc.



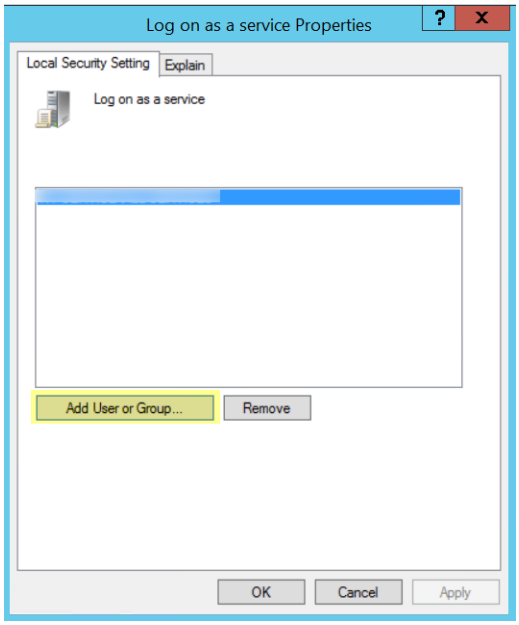

2. 选择 **Local Policies**（本地策略）> **User Rights Assignment**（用户权限分配）> **Log on as a service**（以服务身份登录）。



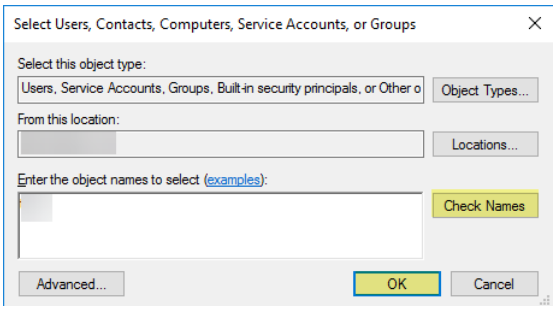

3. **Add User or Group**（添加用户或组）以添加服务账户。



© 2019 Palo Alto Networks, Inc.



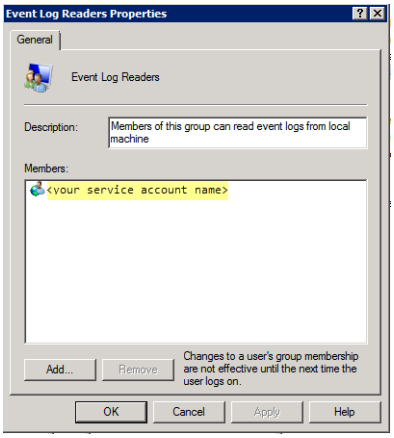

4. 在 **Enter the object names to select**（输入对象名称以进行选择）输入字段内输入 **domain\username** 格式的服务账户名称，然后单击 **OK**（确定）。




要确认服务账户名称是否有效，**Check Names**（检查名称）。

2. 如果想要使用服务器监控以标识用户，则添加服务账户至事件日志读取器 Builtin 组，以启用读取安全日志事件的权限。
   1. 在包含您想要 User-ID 代理读取的日志的域控制器或 Exchange 服务器，或在从 Windows 日志转发接收事件的成员服务器上，运行 MMC，并启动 Active Directory 用户和计算机管理单元。
   2. 导航至域的 Builtin 文件夹，右键单击 **Event Log Reader**（事件日志读取器），然后选择 **Add to Group**（添加到组）以打开属性对话框。
   3. 单击 **Add**（添加），输入配置 User-ID 服务要使用的服务帐户名称，然后单击 **Check Names**（检查名称）以验证对象名称是否正确。
   4. 单击 **OK**（确定）两次以保存设置。
   5. 确认 Builtin 事件日志读取器组是否将服务账户列为成员。

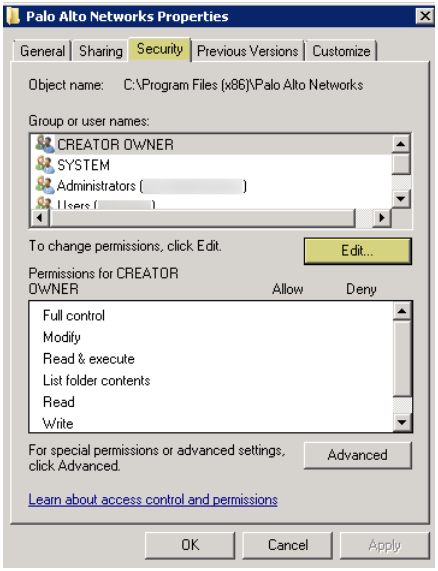

© 2019 Palo Alto Networks, Inc.




3. 分配账户权限至安装文件夹，允许服务账户访问代理的安装文件件，从而读取配置，写入日志。

   如果为 User-ID 代理配置的服务帐户不是域管理员，也不是 User-ID 代理服务器主机上的本地管理员，则只需执行此步骤。

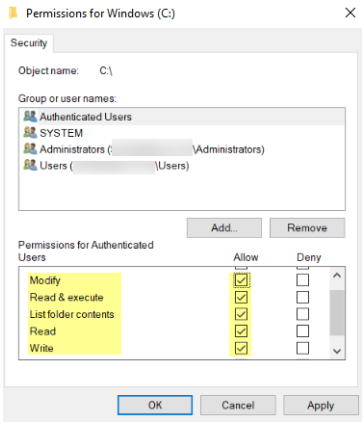
   1. 从 Windows 资源管理器，导航至 32 位系统的 **`C:\Program Files(x86)\Palo Alto Networks`**，右键单击文件夹，然后选择 **Properties**（属性）。
   2. 在 **Security**（安全）选项卡上，单击 **Edit**（编辑）。




   3. **Add**（添加）User-ID 代理服务帐户，并将其权限分配给 **Modify**（修改）、**Read & execute**（读取和执行）、**List folder contents**（列出文件夹内容）、**Read**（读取）和 **Write**（写入），然后单击 **OK**（确定）以保存帐户设置。



© 2019 Palo Alto Networks, Inc.




如果允许服务账户访问 *User-ID* 代理的注册表项，则 *Allow*（允许）*Full Control*（完全控制）权限。

4. 要为 User-ID 代理注册表的子目录树分配服务帐户权限：
   1. 运行 **regedt32**，并导航至下列位置之一中的 Palo Alto Networks 子目录树：`HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`。
   2. 右键单击 Palo Alto Networks 节点，并选择 **Permissions**（权限）。
   3. 为 User-ID 服务帐户分配 **Full Control**（完全控制）权限，然后单击 **OK**（确定）以保存设置。

STEP 2 | 决定安装 User-ID 代理的位置。

User-ID 代理使用 Microsoft 远程过程调用 (RPC) 查询域控制器和 Exchange 服务器日志。在最初连接期间，代理将最新的 50000 个事件从日志传输到映射用户。在后续的每个连接中，代理传输时间戳晚于上次与域控制器通信的事件。因此，请始终在具有要监视的服务器的每个站点上安装一个或多个 User-ID 代理。

- 您必须在运行支持的操作系统版本之一的系统上安装 User-ID 代理：请参阅 兼容性矩阵中的“操作系统 (OS) 兼容性 User-ID 代理”。系统还必须满足最低要求（请参阅 User-ID 代理发行说明）。
- 确保将要托管 User-ID 代理的系统与其将要监控的服务器属于同一个域。
- 最佳实践是，在要监视的服务器旁安装 User-ID 代理：User-ID 代理和监视的服务器之间的通信比 User-ID 代理和防火墙之间的通信更多，因此，在监视的服务器旁安装代理可优化带宽使用率。
- 要确保最全面的用户映射，必须监视用于处理您要映射的用户身份验证的所有域控制器。您可能需要安装多个 User-ID 代理，以便有效监控所有资源。
- 如果正在使用 User-ID 代理进行凭据检测，则必须将其安装在只读域控制器 (RODC) 上。最佳做法是部署用于此目的的单独代理。请勿使用 RODC 上安装的 User-ID 代理将 IP 地址映射到用户。用于凭据检测的 User-ID 代理安装程序名为 UaCredInstall64-x.x.x.msi。

STEP 3 | 下载 User-ID 代理安装程序。

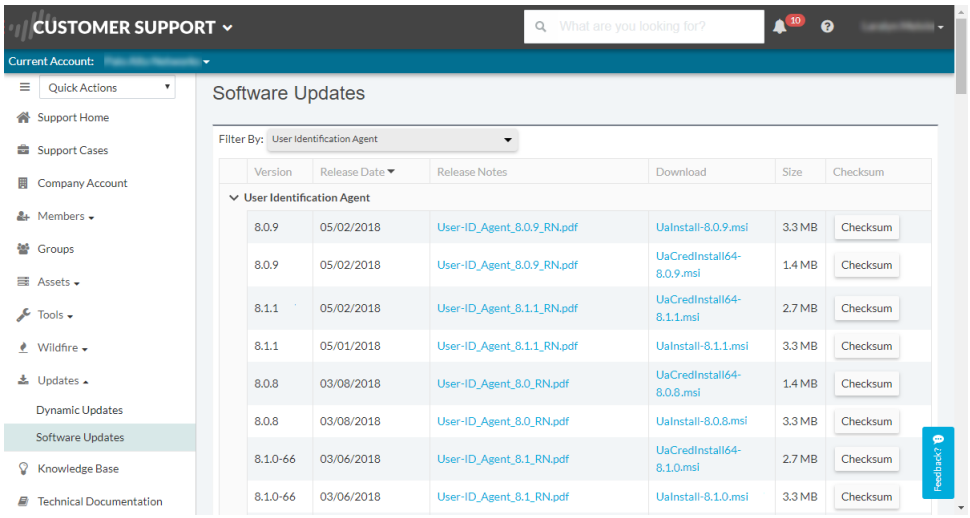
安装与防火墙上运行的 *PAN-OS* 版本相同的 *User-ID* 代理版本。如果没有与 *PAN-OS* 版本匹配的 *User-ID* 代理版本，请安装最接近于 *PAN-OS* 版本的最新版本。

1. 登录到 Palo Alto Networks 客户支持门户。
2. 选择 **Updates**（更新）> **Software Updates**（软件更新）。
3. 设置 **Filter By**（筛选方式）为 **User Identification Agent**（用户标识代理），并选择想要从相应的下载列中安装的 User-ID 代理版本。例如，要下载 User-ID 代理 9.0 版，则选择 **UaInstall-9.0.0-0.msi**。

   如果正在使用 User-ID 代理进行凭据检测，则必须下载名为 `UaInstall-x.x.x.msi` 的 `UaCredInstall64-x.x.x.msi` 文件，而非常规的 User-ID 安装文件。


© 2019 Palo Alto Networks, Inc.

4. 将 `UaCredInstall64-x.x.x-xx.msi` 或`UaInstall-x.x.x-xx.msi` 文件保存于计划安装代理的系统上（务必根据 Windows 系统是运行 32 位还是 64 位 OS 选择适用版本）。




STEP 4 | 以管理员身份运行安装程序。

1. 打开 Windows **Start**（开始）菜单，右击 **Command Prompt**（命令提示符）程序，然后选择 **Run as administrator**（以管理员身份运行）。
2. 从命令行，运行已下载的 .msi 文件。例如，如果文件 .msi 文件保存于桌面上，则需输入以下内容：

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```

3. 按照安装提示，使用默认设置安装代理。默认情况下，代理安装到 **`C:\Program Files(x86)\Palo Alto Networks`**（对于 32 位系统），但是您可以单击 **Browse**（浏览）以选择其他位置。
4. 完成安装后，请单击 **Close**（关闭）以关闭安装窗口。

STEP 5 | 以管理员身份启动 User-ID 代理应用程序。

打开 Windows **Start**（开始）菜单，右键单击 **User-ID Agent**（**User-ID** 代理）程序，然后选择 **Run as administrator**（以管理员身份运行）。

必须以管理员身份运行 *User-ID* 代理应用程序，以安装应用程序、提交配置更改，或卸载应用程序。

STEP 6 | （可选）更改 User-ID 代理用于登录的服务帐户。

默认情况下，代理使用用于安装 .msi 文件的管理员帐户。要将帐户更改为受限帐户：

1. 选择 **User Identification**（用户标识）> **Setup**（设置）并单击 **Edit**（编辑）。
2. 选择 **Authentication**（身份验证）选项卡，然后在 **User name for Active Directory**（**Active Directory** 的用户名称）字段中输入希望 User-ID 代理使用的服务帐户名称。
3. 输入指定帐户的 **Password**（密码）。
4. **Commit**（提交）对 User-ID 代理配置做出的更改，以使用服务帐户凭据重新启动服务。

STEP 7 | （可选）在 Windows User-ID 代理和防火墙之间分配自己的证书以进行相互身份验证。

1. 使用以下方法之一获取 Windows User-ID 代理证书。上传服务器证书（增强的私人邮件 (PEM) 格式）和服务器证书的加密密钥。
   - 生成证书并将其导出以上传到 Windows User-ID 代理。



© 2019 Palo Alto Networks, Inc.

- 从企业证书颁发机构 (CA) 导出证书，并将其上传到 Windows User-ID 代理。

2. 将服务器证书添加到 Windows User-ID 代理。
   1. 在 Windows User-ID 代理上，选择 **Server Certificate**（服务器证书），然后单击 **Add**（添加）。
   2. 输入从 CA 接收到的证书文件的路径和名称，或浏览到证书文件。
   3. 输入私钥密码。
   4. 单击 **OK**（确定），然后单击 **Commit**（提交）。
3. 将证书上传到防火墙以验证 Windows User-ID 代理的身份。
4. 配置客户端设备（防火墙或 Panorama）的证书配置文件。
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
   2. 配置证书配置文件。

      您只能为 *Windows User-ID* 代理和终端服务器 *(TS)* 代理分配一个证书配置文件。因此，您的证书配置文件必须包括颁发证书（上传到已连接的 *User-ID* 和 *TS* 代理）的所有证书颁发机构。
5. 分配防火墙上的证书配置文件。
   1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Connection Security**（连接安全），然后单击编辑按钮。
   2. 选择您在上一步中配置的 **User-ID Certificate Profile**（**User-ID** 证书配置文件）。
   3. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

STEP 8 | 使用基于 Windows 的 User-ID 代理配置凭据检测。

要使用基于 Windows 的 User-ID 代理检测凭据提交和阻止凭证网络钓鱼，必须在基于 Windows 的 User-ID 代理上安装 User-ID 凭据服务。您只能在只读域控制器 (RODC) 上安装此插件。

## 为用户映射配置 *Windows User-ID* 代理

Palo Alto Networks User-ID 代理是一种 Windows 服务，此服务连接到网络上的服务器（例如，Active Directory 服务器、Microsoft Exchange 服务器和 Novell eDirectory 服务器），并监视登录事件日志。此代理使用日志信息将 IP 地址映射到用户名。将 Palo Alto Networks 防火墙连接到 User-ID 代理，可检索用户映射信息，通过用户名（而非 IP 地址）监视用户活动，以及实施基于用户和组的安全策略。

有关 *User-ID* 代理支持的服务器 *OS* 版本相关信息，请参阅 User-ID 代理发布说明中的“操作系统 *(OS)* 兼容性 *User-ID* 代理”部分。

STEP 1 | 定义 User-ID 代理将监视的服务器，以便将 IP 地址收集到用户映射信息中。

User-ID 代理最多可以监控 100 个服务器，其中最多 50 个服务器可为 Syslog Sender。

为了收集需要的所有映射，*User-ID* 代理必须连接到您的用户登录的所有服务器，以便监视包含登录事件的所有服务器上的安全日志文件。

1. 打开 Windows **Start**（开始）菜单，然后选择 **User-ID Agent**（**User-ID** 代理）。
2. 选择 **User Identification**（用户标识）> **Discovery**（发现）。
3. 在屏幕的 **Servers**（服务器）部分中，单击 **Add**（添加）。
4. 输入要监视的服务器的 **Name**（名称）和 **Server Address**（服务器地址）。网络地址可以是 FQDN 或 IP 地址。
5. 选择 **Server Type**（服务器类型）（**Microsoft Active Directory**、**Microsoft Exchange**、**Novell eDirectory** 或 **Syslog Sender**），然后单击 **OK**（确定）以保存服务器条目。为每个要监视的服务器重复此步骤。


© 2019 Palo Alto Networks, Inc.

6. （可选）要让防火墙能够利用 DNS 查找功能自动发现网络上的域控制器，请单击 **Auto Discover**（自动发现）。

   自动发现功能只定位本地域中的域控制器；您必须手动添加 *Exchange* 服务器、*eDirectory* 服务器和 *syslog* 发件人。

7. （可选）要调整防火墙轮询已配置的服务器获取映射信息的频率，请选择 **User Identification**（用户标识）> **Setup**（设置）并 **Edit**（编辑）“设置”部分。在 **Server Monitor**（服务器监视）选项卡上，修改 **Server Log Monitor Frequency (seconds)**（服务器日志监视频率（秒））字段中的值。在较旧的域控制器或延迟性较高的链接的环境中，应当将此字段中的值增加到 5 秒。

   确保未选择 *Enable Server Session Read*（启用服务器会话读取）设置。此设置要求 *User-ID* 代理具有拥有服务器操作员权限的 *Active Directory* 帐户，以便它可以读取所有用户会话。相反，应使用 *Syslog* 或 *XML API* 集成来监控捕获所有设备类型和操作系统（而不仅仅是 *Windows* 操作系统）的登录和退出事件的来源，如无线控制器和网络访问控制器 *(NAC)*。

8. 单击 **OK**（确定）以保存设置。

STEP 2 | 指定 Windows User-ID 代理应包括的子网或 User-ID 应排除的子网。

默认情况下，User-ID 映射访问受监控服务器的所有用户。

最佳实践是始终指定 *User-ID* 应包括和排除的网络，以确保代理只与内部资源进行通信，并防止未经授权的用户被映射。您应仅在组织内部用户登录的子网上启用 *User-ID*。

1. 选择 **User Identification**（用户标识）> **Discovery**（发现）。
2. 在已配置网络的包括/排除列表中 **Add**（添加）一个条目，输入该条目的 **Name**（名称），并将该子网的 IP 地址范围作为 **Network Address**（网络地址）输入。
3. 选择是否包括或排除网络：
   - **Include specified network**（包括指定网络）— 如果要将用户映射限制到仅登录指定子网络的用户，请选择此选项。例如，如果包括 10.0.0.0/8，则代理将映射该子网上的用户，并排除所有其他用户。如果要代理在其他子网中映射用户，则必须重复这些步骤才能向列表中添加其他网络。
   - **Exclude specified network**（排除指定网络）— 仅当您要代理排除您添加用于包括的子网的子集时，才选择此选项。例如，如果包括 10.0.0.0/8 并排除 10.2.50.0/22，则代理将映射 10.0.0.0/8（10.2.50.0/22 除外）的所有子网上的用户，并将排除 10.0.0.0/8 之外的所有子网。

     如果添加排除配置文件而不添加任何包括配置文件，则 *User-ID* 代理会排除所有子网，而不只是已添加的子网。

4. 单击 **OK**（确定）。

STEP 3 | （可选）如果配置代理连接到 Novell eDirectory 服务器，则必须指定代理搜索目录的方式。

1. 选择 **User Identification**（用户标识）> **Setup**（设置）并单击窗口上“设置”部分中的 **Edit**（编辑）。
2. 选择 **eDirectory** 选项卡，然后填写以下字段：
   - **Search Base**（搜索库）— 代理查询的起始点或根上下文，例如：`dc=domain1,dc=example,dc=com`。
   - **Bind Distinguished Name**（绑定可辨别名称）— 用于绑定目录的帐户，例如：`cn=admin,ou=IT, dc=domain1, dc=example, dc=com`。
   - **Bind Password**（绑定密码）— 绑定帐户密码。代理将在配置文件中保存加密密码。
   - **Search Filter**（搜索筛选）— 用户条目的搜索查询（默认为 `objectClass=Person`）。
   - **Server Domain Prefix**（服务器域前缀）— 唯一标识用户的前缀。只在具有重叠命名空间（例如，不同用户在两个不同的目录中具有相同的名称）的情况下，才需要此前缀。
   - **Use SSL**（使用 SSL）— 选中此复选框可使用 SSL 进行 eDirectory 绑定。



© 2019 Palo Alto Networks, Inc.

- **Verify Server Certificate**（验证服务器证书）— 选中此复选框可在使用 SSL 时验证 eDirectory 服务器证书。

STEP 4 | （可选，不推荐）配置客户端探测。

请不要在高安全性网络中启用客户端探测。客户端检测可以生成大量的网络流量，并且在配置错误时可能会造成网络威胁。

1. 在 **Client Probing**（客户端探测）选项卡上，选中 **Enable WMI Probing**（启用 **WMI** 探测）复选框和/或 **Enable NetBIOS Probing**（启用 **NetBIOS** 探测）复选框。
2. 通过在 Windows 防火墙中针对每个被探测的客户端添加一个远程管理例外，以确保 Windows 防火墙允许客户端探测。

为使 *NetBIOS* 探测有效工作，每个被探测的客户端 *PC* 必须在 *Windows* 防火墙中允许端口 *139*，还必须启用文件和打印机共享服务。虽然不推荐客户端探测，如果打算启用，只要有可能，*WMI* 探测比 *NetBIOS* 更可取。

STEP 5 | 保存配置。

单击 **OK**（确定）以保存 User-ID 代理安装设置，然后单击 **Commit**（提交）以重启 User-ID 代理并加载新设置。

STEP 6 | （可选）定义一组无需提供 IP 地址到用户名映射的用户，例如 kiosk 帐户。

使用标题 `ignore_user_list` 将 `ignore-user` 列表保存为代理主机上的文本文档，并使用 .txt 文件扩展名将其保存到已安装有代理的域服务器上的 User-ID 代理文件夹中。

忽略用户帐户列表；可以将任意多个帐户添加到列表中，没有数量限制。每个用户帐户名必须单独占一行。例如：

```
SPAdmin
SPInstall
TFSReport
```

您可将星号用作通配符，以匹配多个用户名，但仅可用作该条目中的最后一个字符。例如，`corpdomain\it-admin*` 将匹配 `corpdomain` 域中用户名以字符串 `it-admin` 开头的所有管理员。您也可以使用 `ignore-user` 列表来标识要使用身份验证门户强制进行身份验证的用户。

添加条目到“忽略用户”列表后，必须停止并重新启动服务连接。

STEP 7 | 配置防火墙以连接到 User-ID 代理。

防火墙只能连接一个基于 *Windows* 的 *User-ID* 代理，该代理正在使用 *User-ID* 凭据服务插件来检测公司凭据提交。有关如何使用此服务进行凭据网络钓鱼防护的详细信息，请参阅使用基于 Windows 的 User-ID 代理配置凭据检测。

要连接到 User-ID 代理以接收用户映射，请在每个防火墙上完成以下步骤：

1. 选择 **Device**（设备）> **Data Redistribution**（数据重新分发）> **Agents**（代理），然后单击 **Add**（添加）。
2. 输入代理 **Name**（名称）。
3. **Add an Agent Using**（添加代理的方式）**Host and Port**（主机和端口）。
4. 输入安装有 User-ID 代理的 Windows **Host**（主机）的 IP 地址。


© 2019 Palo Alto Networks, Inc.

5. 输入代理将在其上侦听用户映射请求的端口的 **Port**（端口）号 (1-65535)。该值必须与在 User-ID 代理上配置的值相匹配。默认情况下，在防火墙和 User-ID 代理较新版本上，端口设置为 5007。但是，某些 User-ID 代理较旧版本默认使用端口 2010。
6. 选择 **IP User Mappings**（**IP** 用户映射）作为 **Data type**（数据类型）。
7. 确保配置设置为 **Enabled**（已启用），然后单击 **OK**（确定）。
8. **Commit**（提交）更改。
9. 验证 **Connected status**（连接状态）显示为“已连接”（绿灯）。

STEP 8 | 验证 User-ID 代理是否成功地将 IP 地址映射到用户名以及防火墙是否可连接到代理。

1. 启动 User-ID 代理，并选择 **User Identification**（用户标识）。
2. 验证代理状态是否显示为 **Agent is running**（代理正在运行）。如果代理未运行，请单击 **Start**（开始）。
3. 要验证 User-ID 代理是否可连接到被监视的服务器，请确保每个服务器的状态均为 **Connected**（已连接）。
4. 要验证防火墙是否可连接到 User-ID 代理，请确保已连接的每个设备的状态均为 **Connected**（已连接）。
5. 要验证 User-ID 代理是否将 IP 地址映射到用户名，请选择 **Monitoring**（监视）并确保填充映射表格。您也可以单击 **Search**（搜索）以从列表中搜索特定用户或单击 **Delete**（删除）以删除用户映射。

# 使用 PAN-OS 集成的 User-ID 代理来配置用户映射

下面的步骤介绍了如何在防火墙上配置集成于 PAN-OS® 的 User-ID™ 代理，以便执行 IP 地址到用户名的映射。除 NetBIOS 客户端探测（支持 WMI 探测）之外，集成的 User-ID 代理与基于 Windows 的代理执行的任务相同。

STEP 1 | 为 User-ID 代理创建 Active Directory 服务帐户，以访问防火墙将进行监控以便收集用户映射信息的服务和主机。

为 User-ID 代理创建专用服务帐户。

STEP 2 | 定义防火墙将监视的服务器，以收集用户映射信息。

在每个防火墙最多总共 100 个受监控服务器的限制内，您可以为任何单个虚拟系统定义不超过 50 个 Syslog Sender。



要收集需要的所有映射，防火墙必须连接到您的用户登录的所有服务器，以便防火墙可以监视所有服务器上包含登录事件的安全日志文件。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）。
2. **Add**（添加）服务器（Server Monitoring（服务器监视）部分）。
3. 输入标识服务器的 **Name**（名称）。
4. 选择服务器的 **Type**（类型）。
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - **Syslog** 发件人
5. （仅限 Microsoft Active Directory 和 Microsoft Exchange only）选择要用于监视服务器上安全日志和会话信息的 **Transport Protocol**（传输协议）。
   - **WMI** — 防火墙和受监控服务器使用 Windows Management Instrumentation (WMI) 进行通信。
   - **WinRM-HTTP** — 防火墙和受监控服务器使用 Kerberos 执行相互身份验证，受监控服务器使用协商的 Kerberos 会话密钥解密与防火墙的通信。



© 2019 Palo Alto Networks, Inc.

- **WinRM-HTTPS** — 防火墙和受监控服务器使用 HTTPS 进行通信，并使用基本身份验证或 Kerberos 执行相互身份验证。

如果选择 Windows 远程管理 (WinRM) 选项，则必须使用 WinRM 配置服务器监控。

6. （仅限 Microsoft Active Directory、Microsoft Exchange 和 Novell eDirectory）输入服务器的 **Network Address**（网络地址）。

   如果使用带 Kerberos 的 WinRM，必须输入完全限定域名 *(FQDN)*。如果想使用带基本身份验证的 WinRM，或使用 *WMI* 监控服务器，可以输入 *IP* 地址或 *FQDN*。

   要使用 *WMI* 监控服务器，请指定 *IP* 地址、服务帐户名称（如果所有服务器监控都在同一域中）或完全限定域名 *(FQDN)*。如果指定 *FQDN*，请使用下级登录名，格式为 *(DLN)\sAMAccountName*，而非 *FQDN\sAMAccountName*。例如，使用 ***example\user.services***，而不是 ***example.com\user.services***。如果指定 *FQDN*，防火墙将尝试使用不支持 *WMI* 的 *Kerberos* 进行身份验证。
7. （仅限 Syslog 发件人）如果选择 **Syslog Sender**（**Syslog** 发件人）作为服务器 **Type**（类型），将 PAN-OS 集成 User-ID 代理配置为 Syslog 侦听器。
8. （仅限 Novell eDirectory）确保 **Enabled**（已启用）您选择的 **Server Profile**（服务器配置文件），然后单击 **OK**（确定）。
9. （可选）配置防火墙，使其通过使用 DNS 查找自动 **Discover**（发现）网络上的域控制器。

   自动发现功能仅适用于域控制器；您必须手动添加任何要监视的 *Exchange Server* 或 *eDirectory* 服务器。

STEP 3 | （可选）指定防火墙将轮询 Windows 服务器以查找映射信息的频率。这是最后一条查询的结束与下一条查询开始之间的时间间隔。

如果域控制器正在处理多个请求，查询之间的延迟可能会大于指定值。

1. **Edit**（编辑）**Palo Alto Networks User ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）。
2. 选择 **Server Monitor**（服务器监视）选项卡，并指定 **Server Log Monitor Frequency**（服务器日志监视频率）（以秒计，范围为 1-3,600；默认为 2）。在较旧域控制器或高延迟链接的环境中，应将此频率设为最小值 5 秒。

   确保未启用 *Enable Session*（启用会话）选项。此选项要求 *User-ID* 代理具有拥有服务器操作员权限的 *Active Directory* 帐户，以便它可以读取所有用户会话。相反，应使用 *Syslog* 或 *XML API* 集成来监视捕获所有设备类型和操作系统（而不仅仅是 *Windows* 操作系统）的登录和注销事件的来源，如无线控制器和网络访问控制 *(NAC)* 设备。
3. 单击 **OK**（确定）保存更改。

STEP 4 | 指定 PAN-OS 集成的 User-ID 代理应包括的子网或用户映射应排除的子网。

默认情况下，User-ID 映射访问受监控服务器的所有用户。

最佳实践是始终指定 *User-ID* 应包括和（可选）排除的网络，以确保代理只与内部资源进行通信，并防止未经授权的用户被映射。您应仅在组织内部用户登录的子网上启用用户映射。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）。
2. **Add**（添加）条目到 **Include/Exclude Networks**（包括/排除网络），并输入条目 **Name**（名称）。确保条目 **Enabled**（已启用）。
3. 输入 **Network Address**（网络地址），然后选择将其包括还是排除：


© 2019 Palo Alto Networks, Inc.

- **Include**（包括）— 如果要将用户映射限制到仅登录指定子网络的用户，请选择此选项。例如，如果包括 10.0.0.0/8，则代理将映射该子网上的用户，并排除所有其他用户。如果要代理在其他子网中映射用户，则必须重复这些步骤才能向列表中添加其他网络。
- **Exclude**（排除）— 如果要配置代理以排除添加用于包括的子网的子集，请选择此选项。例如，如果包括 10.0.0.0/8 并排除 10.2.50.0/22，则代理将映射 10.0.0.0/8（10.2.50.0/22 除外）的所有子网上的用户，并将排除 10.0.0.0/8 之外的所有子网。



如果添加排除配置文件而不添加任何包括配置文件，则 *User-ID* 代理会排除所有子网，而不只是已添加的子网。

4. 单击 **OK**（确定）。

STEP 5 | 为防火墙将用于访问 Windows 资源的帐户设置域凭据。监视 Exchange Server 和域控制器以及进行 WMI 探测时均需要该凭据。

1. **Edit**（编辑）**Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）。
2. 选择 **Server Monitor Account**（服务器监控帐户）选项卡，然后输入将用于探测客户端和监视服务器的 User-ID 代理服务帐户的 **User Name**（用户名）和 **Password**（密码）。使用 **`domain\username`** 语法输入用户名。
3. 如果使用 WinRM 监控服务器，配置防火墙以对您正在监控的服务器进行身份验证。
   - 如果想使用带基本身份验证的 WinRM，在服务器上启用 WinRM，配置基本身份验证，并指定服务帐户**Domain's DNS Name**（域的 **DNS** 名称）。
   - 如果想使用带 Kerberos 的 WinRM，配置 Kerberos 服务器配置文件（如果尚未执行这一操作），然后选择 **Kerberos Server Profile**（**Kerberos** 服务器配置文件）。

STEP 6 | （可选，不推荐）配置 WMI 探测（PAN-OS 集成的 User-ID 代理不支持 NetBIOS 探测）。



请不要在高安全性网络中启用 *WMI* 探测。客户端检测可以生成大量的网络流量，并且在配置错误时可能会造成网络威胁。

1. 在 **Client Probing**（客户端探测）选项卡上，**Enable Probing**（启用探测）。
2. （可选）指定 **Probe Interval**（探测间隔）以定义在最后一条探测请求结束与下一个请求开始之间的时间间隔（以分钟为单位）。

   如有必要，请增加该值，确保 User-ID 代理拥有足够时间来探测获取的所有 IP 地址（范围为 1-1440；默认为 20）。



如果请求负载很高，则观察到的请求之间的延迟可能明显超出指定间隔。

3. 单击 **OK**（确定）。
4. 通过在 Windows 防火墙中针对每个被探测的客户端添加一个远程管理例外，以确保 Windows 防火墙允许客户端探测。

STEP 7 | （可选）定义一组无需提供 IP 地址到用户名映射的用户帐户，例如 kiosk 帐户。



在充当 *User-ID* 代理（而不是客户端）的防火墙上定义忽略用户列表。如果在客户端防火墙上定义忽略用户列表，在重新分发期间，列表中的用户仍会进行映射。

在 **Ignore User List**（忽略用户列表）选项卡中，**Add**（添加）要从用户映射中排除的各个用户名。您也可以使用忽略用户列表来标识要使用身份验证门户强制进行身份验证的用户。您可将星号用作通配符，以匹配多个用户名，但仅可用作该条目中的最后一个字符。例如，**`corpdomain\it-admin*`** 将匹配 `corpdomain` 域中用户名以字符串 `it-admin` 开头的所有管理员。您最多可添加 5,000 个条目，以从用户映射中进行排除。

STEP 8 | 激活配置更改。



© 2019 Palo Alto Networks, Inc.

单击 **OK**（确定）和 **Commit**（提交）。

STEP 9 | 验证配置。

1. 访问防火墙 CLI。
2. 输入以下操作命令：

```
> show user server-monitor state all
```

3. 在 Web 界面的 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）选项卡中，确认您为进行服务器监视配置的每个服务器的状态均为 `Connected`（已连接）。

# 使用 WinRM 配置服务器监控

您可以配置集成有 PAN-OS 的 User-ID 代理，以通过使用 Windows 远程管理 (WinRM) 监控服务器。在监控服务器事件以映射用户事件到 IP 地址时，使用 WinRM 协议可提高速度、效率和安全性。集成有 PAN-OS 的 User-ID 代理支持 Windows Server 2012 Active Directory 和 Microsoft Exchange Server 2012 或更高版本上的 WinRM 协议。

使用 WinRM 配置服务器监控有三种方式：

- 使用基本身份验证在 HTTPS 上配置 WinRM— 防火墙先使用 User-ID 代理的服务帐户用户名和密码对受监控服务器进行身份验证，然后，防火墙使用 User-ID 证书配置文件对受监控服务器进行身份验证。
- 使用 Kerberos 在 HTTP 上配置 WinRM— 防火墙和受监控服务器使用 Kerberos 执行相互身份验证，受监控服务器使用协商的 Kerberos 会话密钥解密与防火墙的通信。
- 使用 Kerberos 在 HTTPS 上配置 WinRM— 防火墙和受监控服务器使用 HTTPS 进行通信，并使用 Kerberos 执行相互身份验证。

## 使用基本身份验证在 *HTTPS* 上配置 *WinRM*

在使用基本身份验证配置 WinRM 以使用 HTTPS 时，防火墙将使用 SSL 在安全隧道中传输服务帐户凭据。

STEP 1 | 为您想要监控的服务器配置具有远程管理用户和 CIMV2 权限的服务帐户。

STEP 2 | 在监控的 Windows 服务器上，获取 Windows 服务器证书指纹，以通过 WinRM 使用并启用 WinRM。

用于在想要监控的服务器上配置 *WinRM* 的帐户必须具有管理员权限。

1. 验证本地计算机证书存储区是否安装有证书（**Certificates (Local Computer)**（证书（本地计算机））> **Personal**（个人）> **Certificates**（证书））。

   如果无法查看本地计算机证书存储区，则启动 Microsoft 管理控制台（**Start**（启动）> **Run**（运行）> **MMC**），并添加证书管理单元（**File**（文件）> **Add/Remove Snap-in**（添加/删除管理单元）> **Certificates**（证书）> **Add**（添加）> **Computer account**（计算机帐户）> **Next**（下一步）> **Finish**（完成））。
2. 打开证书，然后选择 **General**（常规）> **Details**（详细信息）> **Show: <All>**（显示：**<All>**）。
3. 选择 **Thumbprint**（指纹），然后复制指纹。
4. 要启用防火墙以使用 WinRM 连接到 Windows 服务器，输入以下命令：**`winrm quickconfig`**。
5. 输入 **`y`** 以确认更改，然后确认输出是否显示为 `WinRM service started`。

   如果 WinRM 已启用，则输出显示为 `WinRM service is already running on this machine`.系统将提示您确认任何其他所需的配置更改。
6. 要验证 WinRM 是否使用 HTTPS 进行通信，输入以下命令：**`winrm enumerate winrm/config/listener`**，并确认输出是否显示为 `Transport = HTTPS`。


© 2019 Palo Alto Networks, Inc.

WinRM/HTTPS 默认使用端口 5986。

7. 从 Windows 服务器命令提示符中，输入以下命令：**`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**，其中 *hostname* 是 Windows 服务器的主机名， *Certificate Thumbprint* 是从证书复制的值。

   使用命令提示符（而非 *Powershell*），删除证书指纹中的任何空格，以确保 *WinRM* 能够验证证书。

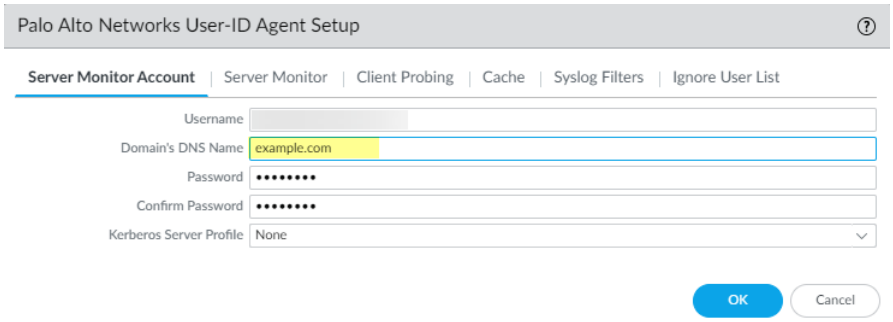
8. 从 Windows 服务器命令提示符中，输入以下命令：

```
c:\> winrm set winrm/config/client/auth @{Basic="true"}
```

9. 输入以下命令：**`winrm get winrm/config/service/Auth`**，并确认 `Basic = true`。

STEP 3 | 在 集成有 PAN-OS 的 User-ID 代理和受监控服务器之间启用基本身份验证。

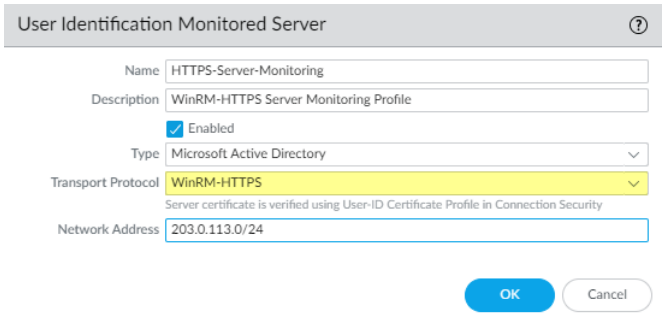
1. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Server Monitor Account**（服务器监控帐户）。
2. 以 **`domain\username`** 格式输入 User-ID 代理将用于监控服务器的服务帐户 **User Name**（用户名）。
3. 输入服务器监控帐户 **Domain's DNS Name**（域的 **DNS** 名称）。




4. 输入服务帐户**Password**（命名），并 **Confirm Password**（确认密码）。
5. 单击 **OK**（确定）

STEP 4 | 为 集成有 PAN-OS 的 User-ID 代理配置服务监控。

1. 选择 Microsoft 服务器 **Type**（类型）（**Microsoft Active Directory** 或 **Microsoft Exchange**）。
2. 选择 **Win-RM-HTTPS** 作为 **Transport Protocol**（传输协议），以通过 HTTPS 使用 Windows 远程管理 (WinRM) 监控服务器安全日志和会话信息。



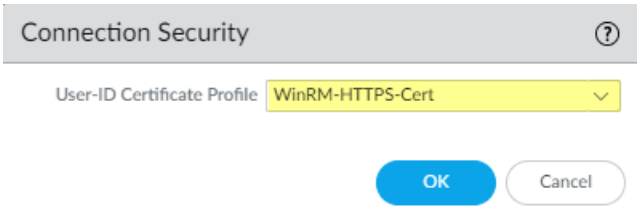

3. 输入服务器的 IP 地址或 FQDN **Network Address**（网络地址）。



© 2019 Palo Alto Networks, Inc.

STEP 5 | 要使集成有 PAN-OS 的 User-ID 代理能够使用 WinRM-HTTPS 与受监控服务器进行通信，请验证您是否已为 Windows 服务器用于 WinRM 的服务证书成功导入根证书到防火墙上，并将其与 User-ID 证书配置文件相关联。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Connection Security**（连接安全）。
2. 单击 **Edit**（编辑）。
3. 选择用于 **User-ID Certificate Profile**（**User-ID** 证书配置文件）的 Windows 服务器证书。




4. 单击 **OK**（确定）。

STEP 6 | **Commit**（提交）更改。

STEP 7 | 验证各个受监控服务器状态是否为已连接（**Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射））。

## 使用 *Kerberos* 在 *HTTP* 上配置 *WinRM*

使用 Kerberos 在 HTTP 上配置 WinRM 时，防火墙和受监控服务器使用 Kerberos 执行相互身份验证，受监控服务器使用协商的 Kerberos 会话密钥解密与防火墙的通信。

使用 *Kerberos* 的 *WinRM* 支持 *aes128-cts-hmac-sha1-96* 和 *aes256-cts-hmac-sha1-96* 密码。如果您想监控的服务器使用 *RC4*，则必须下载 *Windows* 更新，并在您想监控的服务器的注册表设置中为 *Kerberos*禁用 *RC4*。

STEP 1 | 为您想要监控的服务器配置具有远程管理用户和 CIMV2 权限的服务帐户。

STEP 2 | 确认已在您正监控的 Windows 服务器上启用 WinRM。

用于在想要监控的服务器上配置 *WinRM* 的帐户必须具有管理员权限。

1. 要启用防火墙以使用 WinRM 连接到 Windows 服务器，输入以下命令：**`winrm quickconfig`**。
2. 输入 **`y`** 以确认更改，然后确认输出是否显示为 `WinRM service started`。

   如果 WinRM 已启用，则输出显示为 `WinRM service is already running on this machine`.系统将提示您确认任何其他所需的配置更改。
3. 要验证 WinRM 是否使用 HTTPS 进行通信，输入以下命令：**`winrm enumerate winrm/config/listener`**，并确认输出是否显示为 `Transport = HTTPS`。

   WinRM/HTTP 默认使用端口 5985。
4. 输入以下命令：**`winrm get winrm/config/service/Auth`**，并确认 `Kerberos = true`。

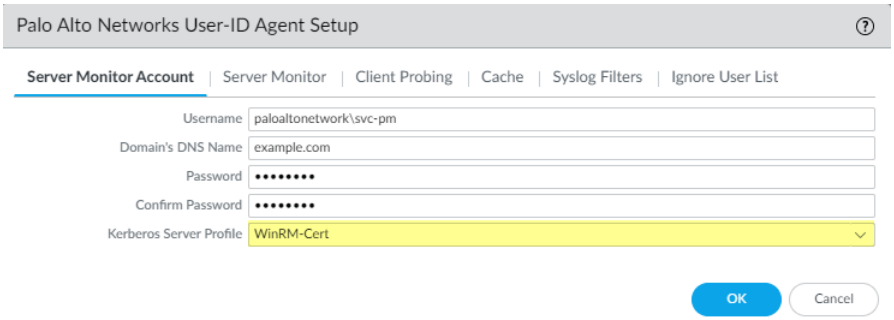
STEP 3 | 启用 集成有 PAN-OS 的 User-ID 代理和受监控服务器，以使用 Kerberos 进行身份验证。

1. 如果未在初始配置时执行这一操作，请配置日期和时间 (NTP) 设置，以确保成功执行 Kerberos 协商。
2. 在防火墙上配置 Kerberos 服务器配置文件，以与服务器进行身份验证，从而监控安全日志和会话信息。


© 2019 Palo Alto Networks, Inc.

3. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（Palo Alto Networks User-ID 代理设置）> **Server Monitor Account**（服务器监控帐户）。
4. 以 **domain\username** 格式输入 User-ID 代理将用于监控服务器的服务帐户 **User Name**（用户名）。
5. 输入服务器监控帐户 **Domain's DNS Name**（域的 **DNS** 名称）。

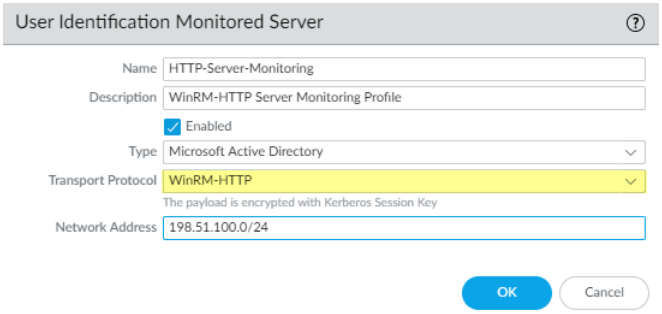
   Kerberos 使用域名查找服务帐户。
6. 输入服务帐户**Password**（命名），并 **Confirm Password**（确认密码）。
7. 选择您在步骤 3.2 中配置的 **Kerberos Server Profile**（**Kerberos** 服务器配置文件）。




8. 单击 **OK**（确定）。

STEP 4 | 为 集成有 PAN-OS 的 User-ID 代理配置服务监控。

1. 配置 Microsoft 服务器类型（**Microsoft Active Directory** 或 **Microsoft Exchange**）。
2. 选择 **WinRM-HTTP** 作为 **Transport Protocol**（传输协议），以通过 HTTP 使用 Windows 远程管理 (WinRM) 监控服务器安全日志和会话信息。




3. 输入服务器的 FQDN **Network Address**（网络地址）。

   如果使用 Kerberos，网络地址必须拥有完全限定域名 (FQDN)。

STEP 5 | **Commit**（提交）更改。

STEP 6 | 验证各个受监控服务器状态是否为已连接（**Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射））。

## 使用 *Kerberos* 在 *HTTPS* 上配置 *WinRM*

使用 Kerberos 在 HTTPS 上配置 WinRM 时，防火墙和受监控服务器使用 HTTPS 进行通信，并使用 Kerberos 执行相互身份验证。



© 2019 Palo Alto Networks, Inc.

使用 *Kerberos* 的 *WinRM* 支持 *aes128-cts-hmac-sha1-96* 和 *aes256-cts-hmac-sha1-96* 密码。如果您想监控的服务器使用 *RC4*，则必须下载 *Windows* 更新 ，并在您想监控的服务器的注册表设置中为 *Kerberos*禁用 *RC4*。

STEP 1 | 为您想要监控的服务器配置具有远程管理用户和 CIMV2 权限的服务帐户。

STEP 2 | 在监控的 Windows 服务器上，获取 Windows 服务器证书指纹，以通过 WinRM 使用并启用 WinRM。

用于在想要监控的服务器上配置 *WinRM* 的帐户必须具有管理员权限。

1. 验证本地计算机证书存储区是否安装有证书（**Certificates (Local Computer)**（证书（本地计算机））> **Personal**（个人）> **Certificates**（证书））。

   如果无法查看本地计算机证书存储区，则启动 Microsoft 管理控制台（**Start**（启动）> **Run**（运行）> **MMC**），并添加证书管理单元（**File**（文件）> **Add/Remove Snap-in**（添加/删除管理单元）> **Certificates**（证书）> **Add**（添加）> **Computer account**（计算机帐户）> **Next**（下一步）> **Finish**（完成））。
2. 打开证书，然后选择 **General**（常规）> **Details**（详细信息）> **Show: <All>**（显示：**<All>**）。
3. 选择 **Thumbprint**（指纹），然后复制指纹。
4. 要启用防火墙以使用 WinRM 连接到 Windows 服务器，输入以下命令：**`winrm quickconfig`**。
5. 输入 **`y`** 以确认更改，然后确认输出是否显示为 `WinRM service started`。

   如果 WinRM 已启用，则输出显示为 `WinRM service is already running on this machine`.系统将提示您确认任何其他所需的配置更改。
6. 要验证 WinRM 是否使用 HTTPS 进行通信，输入以下命令：**`winrm enumerate winrm/config/listener`**。然后确认输出是否显示为 `Transport = HTTPS`。

   WinRM/HTTPS 默认使用 5986。
7. 从 Windows 服务器命令提示符中，输入以下命令：**`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**，其中 *hostname* 是 Windows 服务器的主机名， *Certificate Thumbprint* 是从证书复制的值。

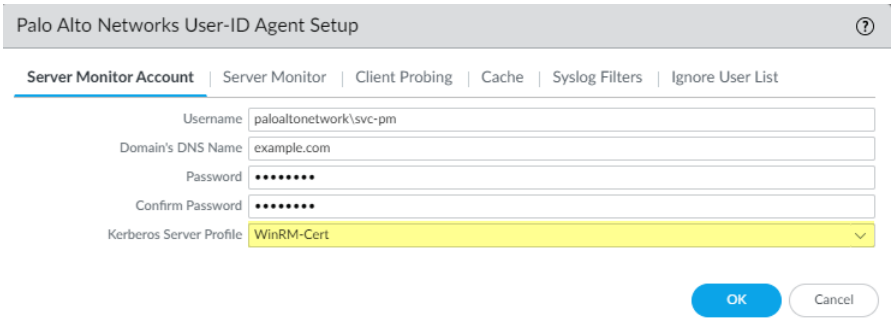
   使用命令提示符（而非 *Powershell*），删除证书指纹中的任何空格，以确保 *WinRM* 能够验证证书。
8. 输入以下命令：**`winrm get winrm/config/service/Auth`**，并确认 `Basic = false` and `Kerberos= true`。

STEP 3 | 启用 集成有 PAN-OS 的 User-ID 代理和受监控服务器，以使用 Kerberos 进行身份验证。

1. 如果未在初始配置时执行这一操作，请配置日期和时间 (NTP) 设置，以确保成功执行 Kerberos 协商。
2. 在防火墙上配置 Kerberos 服务器配置文件，以与服务器进行身份验证，从而监控安全日志和会话信息。
3. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Server Monitor Account**（服务器监控帐户）。
4. 以 **`domain\username`** 格式输入 User-ID 代理将用于监控服务器的服务帐户 **User Name**（用户名）。
5. 输入服务器监控帐户 **Domain's DNS Name**（域的 **DNS** 名称）。

   Kerberos 使用域名查找服务帐户。
6. 输入服务帐户**Password**（命名），并 **Confirm Password**（确认密码）。
7. 选择您在步骤 3.2 中创建的 **Kerberos Server Profile**（**Kerberos** 服务器配置文件）。

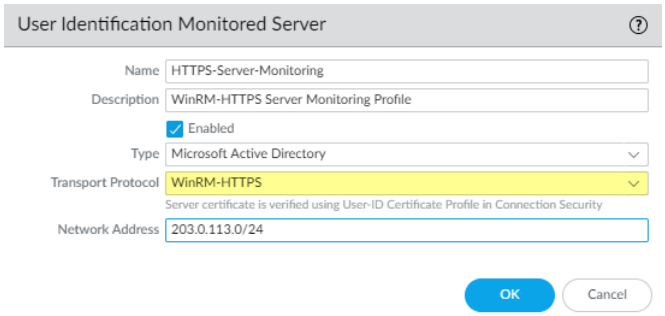

© 2019 Palo Alto Networks, Inc.




8. 单击 **OK**（确定）。

STEP 4 | 为 集成有 PAN-OS 的 User-ID 代理配置服务监控。

1. 配置 Microsoft 服务器类型（**Microsoft Active Directory** 或 **Microsoft Exchange**）。
2. 选择 **Win-RM-HTTPS** 作为 **Transport Protocol**（传输协议），以通过 HTTPS 使用 Windows 远程管理 (WinRM) 监控服务器安全日志和会话信息。



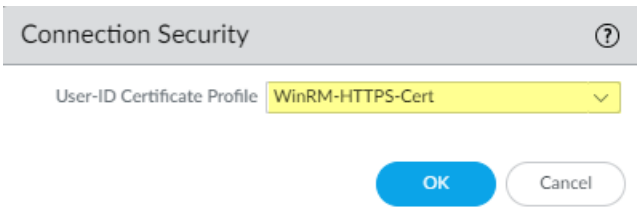

3. 输入服务器的 FQDN **Network Address**（网络地址）。

   如果使用 Kerberos，网络地址必须拥有完全限定域名 (FQDN)。

STEP 5 | 要使集成有 PAN-OS 的 User-ID 代理能够使用 WinRM-HTTPS 与受监控服务器进行通信，请验证您是否已为 Windows 服务器用于 WinRM 的服务证书成功导入根证书到防火墙上，并将其与 User-ID 证书配置文件相关联。

防火墙使用同一证书对所有受监控服务器进行身份验证。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Connection Security**（连接安全）。
2. 单击 **Edit**（编辑）。
3. 选择用于 **User-ID Certificate Profile**（**User-ID** 证书配置文件）的 Windows 服务器证书。




4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

STEP 6 | 验证各个受监控服务器状态是否为已连接（**Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射））。



© 2019 Palo Alto Networks, Inc.

# 配置 User-ID 以监控用户映射的 Syslog 发件人

要从对用户进行身份验证的现有网络服务获取 IP 地址到用户名映射，您可以配置 PAN-OS 集成的 User-ID 代理或基于 Windows 的 User-ID 代理来解析来自这些服务的Syslog消息。为保持最新的用户映射，您还可以配置 User-ID 代理来解析用于退出事件的 syslog 消息，以便防火墙自动删除过时映射。

- 将 PAN-OS 集成 User-ID 代理配置为 Syslog 侦听器
- 将 Windows User-ID 代理配置为 Syslog 侦听程序

## 将 *PAN-OS* 集成 *User-ID* 代理配置为 *Syslog* 侦听器

要配置 PAN-OS 集成 User-ID 代理以创建新的用户映射，并通过 syslog 监控删除过时映射，请先定义 Syslog 解析配置文件。User-ID 代理使用配置文件在 syslog 消息中查找登录和退出事件。在 *syslog* 发件人（对用户进行身份验证的网络服务）以不同格式传送 syslog 消息的环境中，为每个 syslog 格式配置配置文件。Syslog 消息必须符合某些条件 User-ID 代理才能进行解析（请参阅 Syslog）。此过程使用以下格式的示例：

- 登录事件 — `[Tue Jul 5 13:15:04 2016 CDT] Administratorauthentication success User:johndoe1 Source:192.168.3.212`
- 注销事件 — `[Tue Jul 5 13:18:05 2016CDT] User logout successful User:johndoe1 Source:192.168.3.212`

配置 Syslog 解析配置文件后，可以指定要监控的 User-ID 代理的 syslog 发件人。

STEP 1 | 确定您的特定 Syslog 发件人是否具有预定义的 Syslog 解析配置文件。

Palo Alto Networks 通过应用程序内容更新提供多个预定义的配置文件。预定义的配置文件会全局应用至整个防火墙，而自定义配置文件仅适用于单个虚拟系统。



给定内容版本中的任何新 *Syslog* 解析配置文件将与用于定义筛选器的特定正则表达式一起编档存储于相应的发布说明中。

1. 安装最新的应用程序或应用程序和威胁更新：
   1. 选择 **Device**（设备）> **Dynamic Updates**（动态更新）并 **Check Now**（立即检查）。
   2. **Download**（下载）并 **Install**（安装）任何新的更新。
2. 确定哪些预定义的 Syslog 解析配置文件可用：
   1. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射），然后单击服务器监控部分中的 **Add**（添加）。
   2. 将 **Type**（类型）设置为 **Syslog Sender**（**Syslog** 发件人），然后单击筛选器部分中的 **Add**（添加）。如果您需要的 Syslog 解析配置文件可用，请跳过定义自定义配置文件的步骤。

STEP 2 | 定义自定义 Syslog 解析配置文件以创建和删除用户映射。

每个配置文件都会筛选 syslog 消息以标识登录事件（创建用户映射）或退出事件（删除映射），但一个配置文件不可同时标识两种事件。

1. 查看 syslog 发件人生成的 syslog 消息，以标识登录和退出事件的语法。这使您能够在创建 Syslog 解析配置文件时定义匹配模式。

   查看 *syslog* 消息时，还要确定是否包含域名。如果不包含，并且您的用户映射需要域名，则在定义 *User-ID* 代理监控的 *syslog* 发件人（本过程稍后将进行说明）时，请输入 *Default Domain Name*（默认域名）。
2. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）并编辑 Palo Alto Networks User-ID 代理设置。
3. 选择 **Syslog Filters**（**Syslog** 筛选器）并 **Add**（添加）Syslog 解析配置文件。
4. 输入名称以标识 **Syslog Parse Profile**（**Syslog** 解析配置文件）。


© 2019 Palo Alto Networks, Inc.

5. 选择解析的 **Type**（类型）以在 syslog 消息中查找登录或退出事件：
   - **Regex Identifier**（正则表达式标识符）— 正则表达式。
   - **Field Identifier**（字段标识符）— 文本字符串。

   以下步骤描述如何配置这些解析类型。

STEP 3 | （仅限正则表达式标识符解析）定义正则表达式匹配模式。



如果 *Syslog* 消息中使用独立空格键或 *Tab* 键作为分隔符，则使用 **\s**（适用于空格键）和 **\t**（适用于 *Tab* 键）。

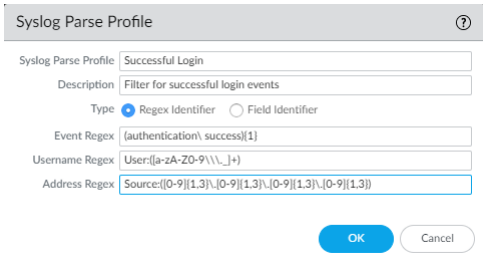
1. 为您要查找的事件类型输入 **Event Regex**（事件正则表达式）：
   - 登录事件 — 对于示例消息，正则表达式 **(authentication\ success){1}** 提取字符串 `authenticationsuccess` 的第一个 **{1}** 实例。
   - 注销事件 — 对于示例消息，正则表达式 **(logout\ successful){1}** 提取字符串 `logoutsuccessful` 的第一个 **{1}** 实例。

   空格之前的反斜杠 (\) 是标准的正则表达式转义符，表示正则表达式引擎不会将空格视为特殊字符。
2. 输入 **Username Regex**（用户名正则表达式）以标识用户名的开头。

   在示例消息中，正则表达式 **User:([a-zA-Z0-9\\\._]+)** 会匹配字符串 `User:johndoe1`，并将 `johndoe1` 标识为用户名。
3. 输入用于标识 syslog 消息的 IP 地址部分的 **Address Regex**（地址正则表达式）。

   在示例消息中，正则表达式 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** 应与 IPv4 地址 `Source:192.168.3.212` 相匹配。

   以下是使用正则表达式标识登录事件的 Syslog 解析配置文件的完整示例：




4. 单击 **OK**（确定）两次以保存配置文件。

STEP 4 | （仅限字段标识符解析）定义字符串匹配模式。

1. 输入 **Event String**（事件字符串）来标识要查找的事件类型。
   - 登录事件 — 对于示例消息，字符串 `authentication success` 标识登录事件。
   - 注销事件 — 对于示例消息，字符串 `logoutsuccessful` 标识注销事件。
2. 输入 **Username Prefix**（用户名前缀）来标识 syslog 消息中用户名字段的开头。该字段不支持正则表达式，如 \s（对于空格）或 \t（对于选项卡）。

   在示例消息中，`User:` 标识用户名字段的开始。
3. 输入表示 syslog 消息中用户名字段结束的 **Username Delimiter**（用户名分隔符）。使用 **\s** 标识独立空格（如示例消息中），使用 **\t** 表示选项卡。
4. 输入 **Address Prefix**（地址前缀）以标识 syslog 消息中 IP 地址字段的开始。该字段不支持正则表达式，如 \s（对于空格）或 \t（对于选项卡）。

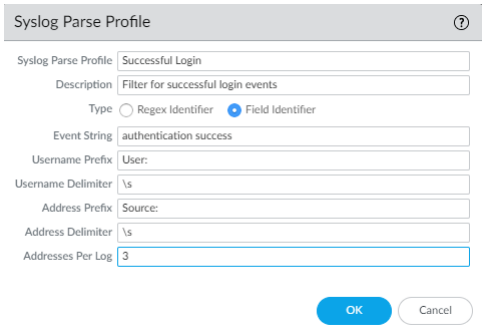
   在示例消息中，`Source:` 标识地址字段的开始。
5. 输入表示 syslog 消息中 IP 地址字段结束的 **Address Delimiter**（地址分隔符）。



© 2019 Palo Alto Networks, Inc.

例如，输入 **\n** 以表示分隔符为换行符。

以下是使用字符串匹配来标识登录事件的 Syslog 解析配置文件的完整示例：




6. 单击 **OK**（确定）两次以保存配置文件。

STEP 5 | 指定防火墙监控的 syslog 发件人。

在每个防火墙最多总共 100 个受监控服务器的限制内，您可以为任何单个虚拟系统定义不超过 50 个 Syslog Sender。

防火墙将丢弃不是该列表中的发件人发出的 Syslog 消息。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射），然后 **Add**（添加）条目到服务器监控列表。
2. 输入 **Name**（名称）以标识发件人。
3. 确保发件人配置文件 **Enabled**（已启用）（默认启用）。
4. 将 **Type**（类型）设置为 **Syslog Sender**（**Syslog** 发件人）。
5. 输入 syslog 发件人的 **Network Address**（网络地址）（IP 地址）。
6. 选择 **SSL**（默认）或 **UDP** 作为 **Connection Type**（连接类型）。



若要选择防火墙用于接收 *syslog* 消息的 *TLS* 证书，请选择 *Device*（设备）> *User Identification*（用户标识）> *User Mapping*（用户映射）> *Palo Alto Networks User-ID Agent Setup*（*Palo Alto Networks User-ID* 代理设置）。*Edit*（编辑）设置，选择 *Server Monitor*（服务器监视器），然后选择包含您希望防火墙用于接收 *syslog* 消息的 *Syslog Service Profile*（*Syslog* 服务配置文件）。



集成于 *PAN-OS* 的 *User-ID* 代理仅接受通过 *SSL* 和 *UDP* 传送的 *Syslog* 消息。但是，使用 *UDP* 接收 *syslog* 消息时必须谨慎，因为 *UDP* 协议不可靠，因此无法验证消息是否是从可信的 *syslog* 发件人发出的。尽管您可以将 *syslog* 消息限制为特定源 *IP* 地址，但攻击者仍可以欺骗 *IP* 地址，并可能会将未经授权的 *syslog* 消息注入到防火墙中。



因为流量被加密，因此，始终使用 *SSL* 侦听 *syslog* 消息（*UDP* 以明文形式发送流量）。如果您必须使用 *UDP*，请确保 *syslog* 发件人和客户端均在某个专用的安全网络上，以防止不可信主机向防火墙发送 *UDP* 流量。

当具有有效 SSL 连接时，使用 SSL 进行连接的 Syslog 发件人将仅显示已连接状态。使用 UDP 的 Syslog Sender 不会显示 Status（状态）值。

7. 对于发件人支持的每个 syslog 格式，将 Syslog 解析配置文件 **Add**（添加）到筛选器列表中。选择配置每个配置文件以进行标识的 **Event Type**（事件类型）：**login**（登录）(default)（默认）或**logout**（退出）。
8. （可选）如果 syslog 消息不包含域信息，并且用户映射需要域名，请输入 **Default Domain Name**（默认域名）以附加到映射。
9. 单击 **OK**（确定）以保存设置。


© 2019 Palo Alto Networks, Inc.

STEP 6 | 在防火墙用于收集用户映射的接口上启用 Syslog 侦听器服务。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理），然后 **Add**（添加）新配置文件。
2. 根据在"服务器监控"列表中为 syslog 发件人定义的协议，选择 **User-ID Syslog Listener-SSL** 或 **User-ID Syslog Listener-UDP**，或选择两者。

   不可配置侦听端口（*UDP* 为 *514*，*SSL* 为 *6514*），只能通过管理服务启用。

3. 单击 **OK**（确定）以保存接口管理配置文件。

   即使启用了接口上的 *User-ID Syslog* 侦听器服务，此接口也只接受在 *User-ID* 受监控的服务器配置中具有相应条目的发件人发出的 *Syslog* 连接。防火墙将丢弃不是该列表中的发件人发出的连接或消息。

4. 将接口管理配置文件分配给防火墙用于收集用户映射的接口：
   1. 选择 **Network**（网络）> **Interfaces**（接口）并编辑接口。
   2. 选择 **Advanced**（高级）> **Other info**（其他信息），选择刚添加的接口 **Management Profile**（管理配置文件），然后单击 **OK**（确定）。
5. **Commit**（提交）更改。

STEP 7 | 验证防火墙在用户登录和退出时是否添加和删除用户映射。

您可以使用 CLI 命令查看有关 *syslog* 发件人、*syslog* 消息和用户映射的其他信息。

1. 登录到受监控的 syslog 发件人生成登录和退出事件消息的客户端系统。
2. 登录至防火墙 CLI。
3. 验证防火墙是否将登录用户名映射到客户端 IP 地址：

```
> show user ip-user-mapping ip <ip-address>
IP address:     192.0.2.1 (vsys1)
User:           localdomain\username
From:           SYSLOG
```

4. 退出客户端系统。
5. 验证防火墙是否删除用户映射：

```
> show user ip-user-mapping ip <ip-address>
No matched record
```

## 将 *Windows User-ID* 代理配置为 *Syslog* 侦听程序

要配置基于 Windows 的 User-ID 代理以创建新的用户映射，并通过 syslog 监控删除过时映射，请先定义 Syslog 解析配置文件。User-ID 代理使用配置文件在 syslog 消息中查找登录和退出事件。在 *syslog* 发件人（对用户进行身份验证的网络服务）以不同格式传送 syslog 消息的环境中，为每个 syslog 格式配置配置文件。Syslog 消息必须符合某些条件 User-ID 代理才能进行解析（请参阅 Syslog）。此过程使用以下格式的示例：

- 登录事件 — `[Tue Jul 5 13:15:04 2016 CDT] Administrator authentication success User:johndoe1 Source:192.168.3.212`
- 退出事件 — `[Tue Jul 5 13:18:05 2016 CDT] User logout successful User:johndoe1 Source:192.168.3.212`



© 2019 Palo Alto Networks, Inc.

配置 Syslog 解析配置文件后，可以指定 User-ID 代理要监控的 syslog 发件人。

基于 *Windows* 的 *User-ID* 代理仅接受通过 *TCP* 和 *UDP* 传送的 *Syslog* 消息。但是，使用 *UDP* 接收 *syslog* 消息时必须谨慎，因为 *UDP* 协议不可靠，因此无法验证消息是否是从可信的 *syslog* 发件人发出的。尽管您可以将 *syslog* 消息限制为特定源 *IP* 地址，但攻击者仍可以欺骗 *IP* 地址，并可能会将未经授权的 *syslog* 消息注入到防火墙中。最佳实践是，使用 *TCP*，而非 *UDP*。在任一情况下，请确保 *syslog* 发件人和客户端均在某个专用的安全 *VLAN* 上，以防止不可信主机向 *User-ID* 代理发送 *syslog*。

STEP 1 | 如果尚未执行，请部署基于 Windows 的 User-ID 代理。

1. 安装基于 Windows 的 User-ID 代理。
2. 配置防火墙以连接到 User-ID 代理。

STEP 2 | 定义自定义 Syslog 解析配置文件以创建和删除用户映射。

每个配置文件都会筛选 syslog 消息以标识登录事件（创建用户映射）或退出事件（删除映射），但一个配置文件不可同时标识两种事件。

1. 查看 syslog 发件人生成的 syslog 消息，以标识登录和退出事件的语法。这使您能够在创建 Syslog 解析配置文件时定义匹配模式。

   查看 *syslog* 消息时，还要确定是否包含域名。如果不包含，并且您的用户映射需要域名，则在定义 *User-ID* 代理监控的 *syslog* 发件人（本过程稍后将进行说明）时，请输入 *Default Domain Name*（默认域名）。
2. 打开 Windows **Start**（开始）菜单，然后选择 **User-ID Agent**（**User-ID** 代理）。
3. 选择 **User Identification**（用户标识）> **Setup**（设置）并 **Edit**（编辑）设置。
4. 选择 **Syslog** 和 **Enable Syslog Service**（启用 **Syslog** 服务），并 **Add**（添加）Syslog 解析配置文件。
5. 输入 **Profile Name**（配置文件名称）和 **Description**（说明）。
6. 选择解析的 **Type**（类型）以在 syslog 消息中查找登录和退出事件：
   - **Regex**（正则表达式）— 正则表达式。
   - **Field**（字段）— 文本字符串。

   以下步骤描述如何配置这些解析类型。

STEP 3 | （仅限正则表达式解析）定义正则表达式匹配模式。

如果 Syslog 消息中使用独立空格键或 Tab 键作为分隔符，则使用 **\s**（适用于空格键）和 **\t**（适用于 Tab 键）。

1. 为您要查找的事件类型输入 **Event Regex**（事件正则表达式）：
   - 登录事件 — 对于示例消息，正则表达式 **(authentication\ success){1}** 提取字符串 `authentication success` 的第一个 **{1}** 实例。
   - 退出事件 — 对于示例消息，正则表达式 **(logout\ successful){1}** 提取字符串 `logout successful` 的第一个 **{1}** 实例。

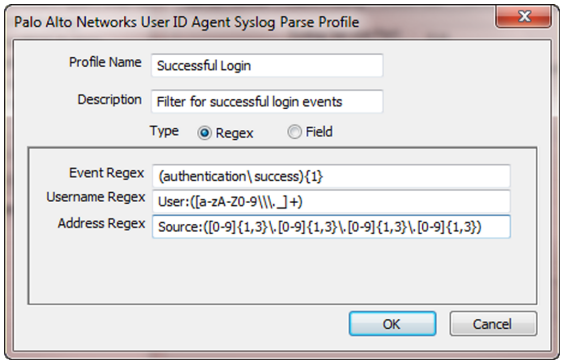
   空格之前的反斜杠是标准的正则表达式转义符，表示正则表达式引擎不会将空格视为特殊字符。
2. 输入 **Username Regex**（用户名正则表达式）以标识用户名的开头。

   在示例消息中，正则表达式 **User:([a-zA-Z0-9\\\._]+)** 会匹配字符串 `User:johndoe1`，并将 `johndoe1` 标识为用户名。
3. 输入用于标识 syslog 消息的 IP 地址部分的 **Address Regex**（地址正则表达式）。

   在示例消息中，正则表达式 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** 应与 IPv4 地址 `Source:192.168.3.212` 相匹配。

   以下是使用正则表达式标识登录事件的 Syslog 解析配置文件的完整示例：


© 2019 Palo Alto Networks, Inc.




4. 单击 **OK**（确定）两次以保存配置文件。

STEP 4 | （仅限字段标识符解析）定义字符串匹配模式。

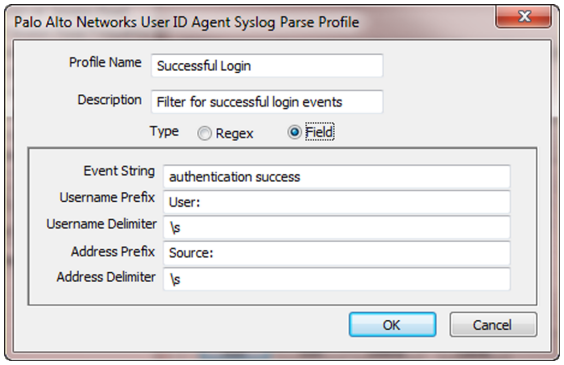
1. 输入 **Event String**（事件字符串）来标识要查找的事件类型。
   - 登录事件 — 对于示例消息，字符串 `authentication success` 标识登录事件。
   - 退出事件 — 对于示例消息，字符串 `logout successful` 标识退出事件。
2. 输入 **Username Prefix**（用户名前缀）来标识 syslog 消息中用户名字段的开头。该字段不支持正则表达式，如 \s（对于空格）或 \t（对于选项卡）。

   在示例消息中，`User:` 标识用户名字段的开始。
3. 输入表示 syslog 消息中用户名字段结束的 **Username Delimiter**（用户名分隔符）。使用 **`\s`** 标识独立空格（如示例消息中），使用 **`\t`** 表示选项卡。
4. 输入 **Address Prefix**（地址前缀）以标识 syslog 消息中 IP 地址字段的开始。该字段不支持正则表达式，如 \s（对于空格）或 \t（对于选项卡）。

   在示例消息中，`Source:` 标识地址字段的开始。
5. 输入表示 syslog 消息中 IP 地址字段结束的 **Address Delimiter**（地址分隔符）。

   例如，输入 **`\n`** 以表示分隔符为换行符。

   以下是使用字符串匹配来标识登录事件的 Syslog 解析配置文件的完整示例：




6. 单击 **OK**（确定）两次以保存配置文件。

STEP 5 | 指定 User-ID 代理监控的 syslog 发件人。

在 User-ID 代理最多总共可监控 100 个所有类型的服务器的限制内，最多 50 个服务器可作为 Syslog Sender。

User-ID 代理将丢弃不是该列表中的发件人发出的任何 Syslog 消息。

1. 选择 **User Identification**（用户标识）> **Discovery**（发现），然后 **Add**（添加）条目到服务器列表。
2. 输入 **Name**（名称）以标识发件人。



© 2019 Palo Alto Networks, Inc.

3. 输入 syslog 发件人的 **Server Address**（服务器地址）（IP 地址或 FQDN）。
4. 将 **Server Type**（服务器类型）设置为 **Syslog Sender**（**Syslog** 发件人）。
5. （可选）如果要在 syslog 消息的用户名中覆盖当前域，或是在 syslog 消息不包含域时将域预先加入用户名，请输入 **Default Domain Name**（默认域名）。
6. 对于发件人支持的每个 syslog 格式，将 Syslog 解析配置文件 **Add**（添加）到筛选器列表中。选择配置的每个配置文件的 **Event Type**（事件类型）以标识 **login**（登录）（默认）或 **logout**（退出），然后单击 **OK**（确定）。
7. 单击 **OK**（确定）以保存设置。
8. **Commit**（提交）您对 User-ID 代理配置的更改。

STEP 6 | 验证 User-ID 代理在用户登录和退出时是否添加和删除用户映射。



您可以使用 CLI 命令查看有关 *syslog* 发件人、*syslog* 消息和用户映射的其他信息。

1. 登录到受监控的 syslog 发件人生成登录和退出事件消息的客户端系统。
2. 验证 User-ID 代理是否将登录用户名映射到客户端 IP 地址：
   1. 在 User-ID 代理中，选择 **Monitoring**（监控）。
   2. 在筛选器字段中输入用户名或 IP 地址，**Search**（搜索）并确认该列表显示映射。
3. 验证防火墙是否能从 User-ID 代理接收到用户映射：
   1. 登录至防火墙 CLI。
   2. 运行以下命令：

```
> show user ip-user-mapping ip <ip-address>
```

   如果防火墙接收到用户映射，则输出类似于以下内容：

```
IP address:    192.0.2.1 (vsys1)
User:          localdomain\username
From:          SYSLOG
```

4. 退出客户端系统。
5. 验证 User-ID 代理是否已删除用户映射：
   1. 在 User-ID 代理中，选择 **Monitoring**（监控）。
   2. 在筛选器字段中输入用户名或 IP 地址，**Search**（搜索）并确认该列表不显示映射。
6. 验证防火墙是否删除用户映射：
   1. 访问防火墙 CLI。
   2. 运行以下命令：

```
> show user ip-user-mapping ip <ip-address>
```

   如果防火墙已删除用户映射，则输出类似于以下内容：

```
No matched record
```


© 2019 Palo Alto Networks, Inc.

# 使用身份验证门户将 IP 地址映射到用户名

当用户启动与身份验证策略规则匹配的 Web 流量（HTTP 或 HTTPS）时，防火墙会提示用户通过身份验证门户进行身份验证。这确保您能确切地知道正在访问最敏感应用程序和数据的用户是谁。防火墙会根据身份验证过程中收集到的用户信息来创建新的 IP 地址到用户名映射，或更新该用户的现有映射。这种用户映射方法在防火墙无法通过其他方法（如监控服务器）来了解映射信息的环境中十分有用。例如，您可能有尚未登录到受监控域服务器的用户，例如 Linux 客户端上的用户。

- 身份验证门户的身份验证方法
- 身份验证门户模式
- 配置身份验证门户

## 身份验证门户的身份验证方法

身份验证门户使用以下方法对 Web 请求与身份验证策略规则相匹配的用户进行身份验证：

| 身份验证方法 | 说明 |
| --- | --- |
| Kerberos SSO | 防火墙使用 Kerberos 单点登录 (SSO) 以透明方式从浏览器获取用户凭据。要使用此方法，您的网络需要 Kerberos 基础架构，包括密钥分发中心 (KDC)（含身份验证服务器 (AS) 和票据授予服务 (TGS)）。防火墙必须具有 Kerberos 帐户。<br>如果 Kerberos SSO 身份验证失败，防火墙会返回到 Web 表单或客户端证书身份验证，具体取决于您的身份验证策略和身份验证门户配置。 |
| Web 表单 | 防火墙会将 Web 请求重定向至 Web 表单进行身份验证。对于此方法，您可以配置身份验证策略以使用多重因素身份验证 (MFA)、SAML、Kerberos、TACACS+、RADIUS 或 LDAP 身份验证。虽然用户必须手动输入其登录凭据，但此方法适用于所有浏览器和操作系统。 |
| 客户端证书身份验证 | 防火墙提示浏览器显示有效的客户端证书，以对用户进行身份验证。如需使用此方法，必须在每个用户系统上提供客户端证书，并安装用于在防火墙上签发这些证书的可信任证书授权机构 (CA) 证书。 |

## 身份验证门户模式

身份验证门户模式定义防火墙如何捕获用于身份验证的 Web 请求：

| 模式 | 说明 |
| --- | --- |
| transparent | 防火墙按照身份验证策略规则拦截浏览器通信，并模仿原始目标 URL 发出 HTTP 401，以调用身份验证。但是，由于防火墙没有目标 URL 的真正证书，因此浏览器将向尝试访问安全站点的用户显示证书错误。因此，仅可在绝对必要时（例如第 2 层或虚拟线路部署）使用此模式。 |
| redirect | 防火墙拦截未知的 HTTP 或 HTTPS 会话，并使用 HTTP 302 重定向将它们重定向至防火墙上的第 3 层接口，以执行身份验证。这是首选模式，因为此模式能提供更好的最终用户体验（无证书错误）。但是，它却需要额外的第 3 层配置。重定向模式的另一个优势是用户可以使用会话 Cookie，这样用户在每次超时到期时可以继续浏览经过身份验证的站点，无需进行重新映射。这对从一个 IP 地址漫游到另一个地址（例如，从公司 LAN 到 |



© 2019 Palo Alto Networks, Inc.

| 模式 | 说明 |
| --- | --- |
| | 无线网络）的用户尤为有用，因为只要会话保持打开状态，用户就无需因 IP 地址变更重新进行身份验证。<br>如果使用 Kerberos SSO ，则必须使用重定向模式，因为浏览器将只向受信任的站点提供凭据。如果您使用多重因素身份验证验证身份验证门户用户的身份，也需要重定向模式。 |

## 配置身份验证门户

下列步骤介绍如何使用集成于 PAN-OS 的 User-ID 代理来配置身份验证门户身份验证，以便对与防火墙接口的身份验证策略规则相匹配的 Web 请求进行重定向（重定向主机）。

SSL 入站检测不支持身份验证门户重定向。若要使用身份验证门户重定向和解密，必须使用SSL 转发代理。

基于其敏感度，用户通过身份验证门户访问的应用程序需要不同的身份验证方法和设置。为了适应所有身份验证要求，您可以使用默认和自定义身份验证执行对象。每个对象将身份验证规则与身份验证配置文件和身份验证门户身份验证方法相关联。

- 默认身份验证执行对象 — 如果要将多个身份验证规则与相同的全局身份验证配置文件相关联，请使用默认对象。配置身份验证门户之前，您必须配置此身份验证配置文件，然后在身份验证门户设置中对其进行分配。对于需要多重因素身份验证 (MFA) 的身份验证规则，不得使用默认身份验证执行对象。
- 自定义身份验证执行对象 — 为需要与全局配置文件不同的身份验证配置文件的每个身份验证规则使用一个自定义对象。需要 MFA 的身份验证规则必须配置自定义对象。配置身份验证策略时，要使用自定义对象，创建身份验证配置文件，并在配置身份验证门户后将其分配给对象。

请记住，仅当用户通过身份验证门户 Web 表单或 Kerberos SSO 进行身份验证时，才需要身份验证配置文件。此外，除这些方法之外，以下过程还描述了如何实现客户端证书身份验证。

如果使用身份验证门户，而不使用其他 *User-ID* 功能（用户映射和组映射），则不需要配置 *User-ID* 代理。

STEP 1 | 配置某些接口，防火墙将这些接口用于入站 Web 请求、对用户进行身份验证以及与目录服务器通信以将用户名映射到 IP 地址。

当防火墙连接至身份验证服务器或用户 ID 代理时，默认使用管理接口。最佳做法是通过配置连接到身份验证服务器或用户 ID 代理的服务路由以隔离您的管理网络。

1. （仅限 MGT 接口）选择 **Device**（设备）> **Setup**（设置）> **Interfaces**（接口），编辑 **Management**（管理）接口，选中 **User ID**（用户标识），然后单击 **OK**（确定）。
2. （仅限非 MGT 接口）将接口管理配置文件分配给防火墙将用于入站 Web 请求和与目录服务器通信的第 3 层接口。您必须在接口管理配置文件中启用 **Response Pages**（响应页面）和 **User-ID**（用户标识）。
3. （仅限非 MGT 接口）针对防火墙将用对用户进行身份验证的接口，配置服务路由。如果防火墙具有多个虚拟系统 (vsys)，服务路由可以是全局，也可以是特定于 vsys。服务必须包含 **LDAP**，并且可能包含以下各项：
   - **Kerberos**、**RADIUS**、**TACACS+** 或 **Multi-Factor Authentication**（多重因素身份验证）— 为您使用的任何身份验证服务配置服务路由。
   - **UID** 代理— 仅在启用基于用户和基于组的策略时配置此服务。
4. （仅限重定向模式）创建 DNS 地址 (A) 记录，以将第 3 层接口上的 IP 地址映射到重定向主机。如果您将使用 Kerberos SSO，则必须添加 DNS 指针 (PTR) 记录，其执行相同映射。


© 2019 Palo Alto Networks, Inc.

如果您的网络不支持从任何防火墙接口访问目录服务器，则必须使用 Windows User-ID 代理配置用户映射。

STEP 2 | 请确保将域名系统 (DNS) 配置为可解析域控制器的地址。

若要验证解析是否正确，请 ping 服务器 FQDN。例如：

```
admin@PA-220> ping host dc1.acme.com
```

STEP 3 | 将客户端配置为信任身份验证门户证书。

重定向模式所必需 — 用于以透明方式重定向用户，而不显示证书错误。您可以生成自签名证书，也可以导入由外部证书颁发机构 (CA) 签名的证书。

若要使用自签名证书，请首先创建一个根 CA 证书，然后使用该 CA 证书来签名您将用于身份验证门户的证书：

1. 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。
2. 创建自签名根 CA 证书或导入 CA 证书（请参阅导入证书和私钥）。
3. 生成证书以用于身份验证门户。务必配置以下字段：
   - **Common Name**（通用名称）— 输入第 3 层接口的 Intranet 主机的 DNS 名称。
   - **Signed By**（签署者）— 选择您刚刚创建或导入的 CA 证书。
   - 证书属性 — 单击**Add**（添加），针对 **Type**（类型），选择 **IP**，针对 **Value**（值），输入防火墙将请求重定向到的第 3 层接口上的 IP 地址。
4. 配置 SSL/TLS 服务配置文件。将您刚刚创建的身份验证门户分配给配置文件。

   如果未分配 *SSL/TLS* 服务配置文件，防火墙默认使用 *TLS 1.2*。要使用不同的 *TLS* 版本，请为想要使用的 *TLS* 版本配置 *SSL/TLS* 服务配置文件。
5. 将客户端配置为信任证书：
   1. 导出 CA 证书（刚刚创建或导入的证书）。
   2. 通过手动配置浏览器，或者通过将证书添加到 Active Directory (AD) 组策略对象 (GPO) 的可信根中，将该证书作为可信的根 CA 导入到所有客户端浏览器。

STEP 4 | （可选）配置客户端证书身份验证。

不需要身份验证配置文件或序列来进行客户端证书身份验证。如果同时配置了身份验证配置文件/序列和证书身份验证，则用户必须同时使用这两者进行身份验证。

1. 使用根 CA 证书为每个将要通过身份验证门户进行身份验证的用户生成客户端证书。在这种情况下，CA 通常是您的企业 CA，而非是防火墙。
2. 以 PEM 格式导出 CA 证书至防火墙可访问的系统。
3. 将 CA 证书导入防火墙：请参阅导入证书和私钥。在导入后，单击导入的证书，选择 **Trusted Root CA**（可信根 **CA**），然后单击 **OK**（确定）。
4. 配置证书配置文件。
   - 在 **Username Field**（用户名字段）下拉列表中，选择包含用户身份信息的证书字段。
   - 在 **CA Certificates**（**CA** 证书）列表中，单击 **Add**（添加），并选择刚导入的 CA 证书。

STEP 5 | （可选）为 Apple Captive Network Assistant 配置身份验证门户。

仅在将身份验证门户与 Apple Captive Network Assistant (CNA) 配合使用时，才需执行此步骤。若要将身份验证门户与 CNA 配合使用，请执行以下步骤。



© 2019 Palo Alto Networks, Inc.

1. 验证是否为重定向主机指定 FQDN（而不仅仅是 IP 地址）。
2. 选择为指定 FQDN 使用公共签名证书的 SSL/TLS 服务配置文件。
3. 输入以下命令，调整支持身份验证门户的请求数：**set deviceconfig setting ctd cap-portal-ask-requests *<threshold-value>***

   默认情况下，防火墙为身份验证门户设定了速率限制阈值，以限制每两秒钟对一个请求发起的请求数。CNA 发送可能超出此限制的多个请求，这可能导致 TCP 重置、CNA 出错。推荐阈值为 5（默认为 1）。此值允许每两秒钟最多发起 5 个请求。您可以根据您的环境配置不同的值。如果当前值不足以处理该请求数，请增加该值。

STEP 6 | 配置身份验证门户设置。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Authentication Portal Settings**（身份验证门户设置），然后编辑设置。
2. **Enable Authentication Portal**（启用身份验证门户）（默认为启用）。
3. 指定 **Timer**（计时器），这是防火墙在用户通过身份验证门户进行身份验证后保留的 IP 地址到用户名映射的最长时间（默认为 60；范围为 1-1,440）。**Timer**（计时器）到期后，防火墙会删除用于评估身份验证策略规则中 **Timeout**（超时）的映射和任何关联的身份验证时间戳。

   在每个身份验证策略规则中评估身份验证门户 *Timer*（计时器）和 *Timeout*（超时）值时，无论哪一个设置先到期，防火墙均会提示用户重新进行身份验证。重新进行身份验证时，防火墙会重新设置身份验证门户 *Timer*（计时器）的时间计数，并为用户记录新的身份验证时间戳。因此，要为不同的身份验证规则启用不同的 *Timeout*（超时）时间，请将身份验证门户 *Timer*（定时器）设置为与任何规则中 *Timeout*（超时）一样或更高的值。
4. 选择您基于 TLS 的重定向请求创建的 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。请参阅配置 SSL/TLS 服务配置文件。
5. 选择 **Mode**（模式）（在此示例中为 **Redirect**（重定向））。
6. （仅限重定向模式）指定 **Redirect Host**（重定向主机），即解析到第 3 层接口（防火墙重定向 Web 请求的目标接口）IP 地址的 Intranet 主机名（即名称中没有点的主机名）。

   如果用户通过 Kerberos 单点登录 (SSO) 进行身份验证，则 **Redirect Host**（重定向主机）必须与在 Kerberos 密钥表中指定的主机名相同。
7. 选择要使用的故障回退身份验证方法：
   - 要使用客户端证书身份验证，请选择您创建的 **Certificate Profile**（证书配置文件）。
   - 要使用全局设置进行交互式或 SSO 身份验证，请选择您配置的 **Authentication Profile**（身份验证配置文件）。
   - 要使用身份验证策略规则特定设置进行交互式或 SSO 身份验证，请在配置身份验证策略时将身份验证配置文件分配给身份验证执行对象。
8. 单击 **OK**（确定），并 **Commit**（提交）身份验证门户配置。

STEP 7 | 后续步骤...

当用户请求服务或应用程序时，防火墙不会向用户显示身份验证门户 Web 表单，直到您的配置身份验证策略规则能触发身份验证。

# 为终端服务器用户配置用户映射

终端服务器的每个用户都使用同一个 IP 地址，因此，IP 地址到用户名映射不足以确定特定用户。为了在基于 Windows 的终端服务器上标识特定用户，Palo Alto Networks 终端服务器代理（TS 代理）将为每个用户分配端口范围。然后，TS 代理就已分配的端口范围通知已连接的每个防火墙，这些端口范围允许防火墙创建 IP 地址-端口-用户映射表，并启用基于用户和组的安全策略实施。对于非 Windows 终端服务器，请配置 PAN-OS XML API 以提取用户映射信息。以下值适用于两种方法：

- 默认端口范围：1025 到 65534


© 2019 Palo Alto Networks, Inc.

- 每个用户的块大小：200
- 多用户系统的最大数量：2，500

有关 TS 代理支持的终端服务器以及每个防火墙型号支持的 TS 代理数的信息，请参阅 Palo Alto Networks 兼容性矩阵和产品比较工具。

以下部分介绍如何为终端服务器用户配置用户映射：

- 配置 Palo Alto Networks 终端服务器 (TS) 代理执行用户映射
- 使用 PAN-OS XML API 检索源自 Terminal Server 的用户映射

## 配置 *Palo Alto Networks 终端服务器 (TS)* 代理执行用户映射

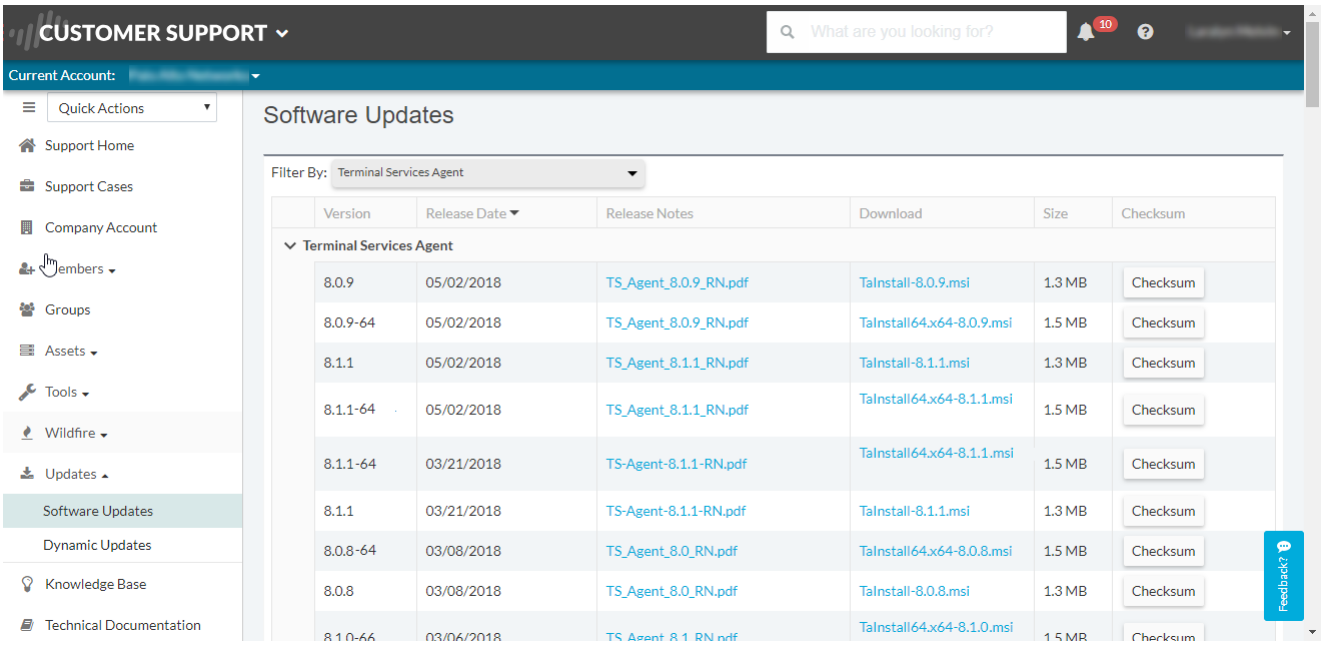
要在终端服务器上安装和配置 TS 代理，请执行以下操作。要映射所有用户，必须在用户登录的所有终端服务器上安装 TS 代理。

如果使用 *TS* 代理 *7.0* 或更高版本，则禁用 *TS* 代理主机上的任何 *Sophos* 防病毒软件。否则，防病毒软件将覆盖 *TS* 代理分配的源端口。

有关默认值、范围和其他规格的信息，请参阅为终端服务器用户配置用户映射。有关 *TS* 代理支持的终端服务器以及每个防火墙型号支持的 *TS* 代理数的信息，请参阅 Palo Alto Networks 兼容性矩阵。

STEP 1 | 下载 TS 代理安装程序。

1. 登录到 Palo Alto Networks 客户支持门户。
2. 选择**Updates**（更新）> **Software Updates**（软件更新）。
3. 设置 **Filter By**（筛选挑几件）为 **Terminal Services Agent**（终端服务代理），并从相应的下载列中选择想要安装的代理版本。例如，要下载 TS 代理 9.0，请选择 **TaInstall-9.0.msi**。
4. 将 `TaInstall.x64-x.x.x-xx.msi` 或 `TaInstall-x.x.x-xx.msi` 文件保存于计划安装代理的系统上；务必根据 Windows 系统是运行 32 位还是 64 位 OS 选择适用的版本。




STEP 2 | 以管理员身份运行安装程序。

1. 打开 Windows **Start**（开始）菜单，右击 **Command Prompt**（命令提示符）程序，然后选择 **Run as administrator**（以管理员身份运行）。



© 2019 Palo Alto Networks, Inc.

2. 从命令行，运行已下载的 .msi 文件。例如，如果文件 `TaInstall-9.0.msi` 保存于桌面上，则需输入以下内容：

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>TaInstall-9.0.0-1.msi
```

3. 按照安装提示，使用默认设置安装代理。安装程序将代理安装在 `C:\ProgramFiles (x86)\Palo Alto Networks\Terminal Server Agent` 中。

   为确保端口分配的正确性，必须使用默认的终端服务器代理安装文件夹位置。

4. 完成安装后，**Close**（关闭）安装窗口。

   如果正在升级为具有比现有安装的驱动程序更新的 *TS* 代理版本，则安装向导将在升级之后提示您重启系统。

STEP 3 | 为 TS 代理定义端口范围以分配给终端用户。

*System Source Port Allocation Range*（系统源端口分配范围）和 *System Reserved Source Ports*（系统保留源端口）可指定要分配给非用户会话的端口范围。确保这两个字段中的值不会与为用户通信指定的端口重叠。只能通过编辑相应的 *Windows* 注册表设置更改这些值。*TS* 代理分配用于会话 *0* 发出的网络流量的端口。

1. 打开 Windows **Start**（开始）菜单，然后选择 **Terminal Server Agent**（终端服务器代理）以启动终端服务器代理应用程序。
2. **Configure**（配置）（侧菜单）代理。
3. 输入 **Source Port Allocation Range**（源端口分配范围）（默认值为 20,000 - 39,999）。该值表示 TS 代理将为用户映射分配的端口数的全部范围。指定的端口范围不能与 **System Source Port Allocation Range**（系统源端口分配范围）重叠。
4. （可选）如果源端口分配包含不想 TS 代理分配给用户会话的端口或端口范围，请将它们指定为 **Reserved Source Ports**（保留源端口）。要包括多个范围，请使用不带空格的逗号（例如：`2000-3000,3500,4000-5000`）。
5. 登录终端服务器时，请指定分配给每个单独用户的端口数（**Port Allocation Start Size Per User**（每个用户的端口分配开始大小））；默认为 200。
6. 指定 **Port Allocation Maximum Size Per User**（每个用户的端口分配最大大小），该值表示终端服务器代理可分配给单个用户的最大端口数。
7. 如果用户用完已分配的端口，请指定是否继续处理来自用户的通信。默认情况下，启用 **Fail port binding when available ports are used up**（可用端口用完时无法绑定端口），此复选框表示当所有端口都用完时，应用程序将无法发送通信。要使用户在端口用完后能继续使用应用程序，请禁用（取消选中）此选项，但是一旦执行此操作，该通信可能无法使用 User-ID 进行标识。
8. 如果终端服务器在您尝试将其关闭时停止响应，则启用 **Detach agent driver at shutdown**（关闭时分离代理驱动程序）选项。

STEP 4 | （可选）为 TS 代理和防火墙之间的相互身份验证分配自己的证书。

1. 获取企业 PKI 的 TS 代理证书或在防火墙上生成一个证书。必须加密服务器证书的私钥，且证书必须以 PEM 文件格式上传。执行以下任务之一以上传证书：
   - 生成证书并将其导出。
   - 从企业证书颁发机构 (CA) 导出证书。
2. 将服务器证书添加到 TS 代理。
   1. 在 TS 代理上，选择 **Server Certificate**（服务器证书），然后 **Add**（添加）新证书。
   2. 输入从 CA 接收到的证书文件的路径和名称，或浏览到证书文件。


© 2019 Palo Alto Networks, Inc.

3. 输入私钥密码。
4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

*TS* 代理在端口 *5009* 上使用自签名证书，详细信息如下：*Issuer:CN=Terminal Server Agent, OU=Engineering, O=Palo Alto Networks, L=Santa Clara, S=California, C=USSubject:CN=Terminal Server Agent, OU=Engineering, O=Palo Alto Networks, L=Santa Clara, S=California, C=US*

3. 配置并分配防火墙的证书配置文件。
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）以配置证书配置文件。

      您只能为 *Windows User-ID* 代理和 *TS* 代理分配一个证书配置文件。因此，您的证书配置文件必须包括上传到已连接的 *Windows User-ID* 和 *TS* 代理的颁发证书的所有证书颁发机构。
   2. 选择 **Device**（设备）> **User Identification**（用户标识）> **Connection Security**（连接安全）。
   3. 编辑 (⚙)，并选择在上一步中配置的证书配置文件作为 **User-ID Certificate Profile**（**User-ID** 证书配置文件）。
   4. 单击 **OK**（确定）。
   5. **Commit**（提交）更改。

STEP 5 | 配置防火墙以连接到终端服务器代理。

要连接到终端服务器代理以接收用户映射，请在每个防火墙上执行以下步骤：

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Terminal Server Agents**（终端服务器代理），然后 **Add**（添加）新的 TS 代理。
2. 输入终端服务器代理的 **Name**（名称）。
3. 输入安装有终端服务器代理的 Windows **Host**（主机）的主机名或 IP 地址。

   主机名或 IP 地址可解析出一个静态 IP 地址。如果更改现有主机名，在提交更改以解析新主机名时，TS 代理会重置。如果主机名解析出多个 IP 地址，TS 代理使用列表中的第一个地址。
4. （可选）输入作为传出流量源 IP 地址显示的任何 **Alternative IP Addresses**（备用 **IP** 地址）的主机名或 IP 地址。

   主机名或 IP 地址可解析出一个静态 IP 地址。您最多可以输入 8 个 IP 地址或主机名。
5. 输入代理将在其上侦听用户映射请求的端口的 **Port**（端口）号。该值必须与在终端服务器代理上配置的值相匹配。默认情况下，端口在防火墙上和代理上都设置为 5009。如果在防火墙上更改该值，也必须将终端服务器代理 **Configure**（配置）对话框上的 **Listening Port**（侦听端口）更改为相同的端口。
6. 确保配置设置为 **Enabled**（已启用），然后单击 **OK**（确定）。
7. **Commit**（提交）更改。
8. 验证连接状态显示为 **Connected**（已连接）（绿灯）。

STEP 6 | 验证终端服务器代理是否成功将 IP 地址映射到用户名以及防火墙是否可连接到代理。

1. 打开 Windows **Start**（开始）菜单，然后选择 **Terminal Server Agent**（终端服务代理）。
2. 通过确保“连接列表”中的每台设备的 **Connection Status**（连接状态）都是 `Connected`（已连接）来验证防火墙可连接到代理。
3. 验证终端服务器代理成功将端口范围映射到用户名（在侧菜单中选择 **Monitor**（监视器）来），并确认映射表已填充。

STEP 7 | （仅限 Windows 2012 R2 服务器）在 Microsoft互联网Explore 中为每个使用浏览器的用户禁用增强保护模式。



© 2019 Palo Alto Networks, Inc.

对于 Google Chrome 或 Mozilla Firefox 等其他浏览器，不一定要执行此任务。



要为所有用户禁用增强保护模式，请使用本地安全策略。

在 Windows Server 上执行以下步骤：

1. 启动互联网Explorer。
2. 选择 **Settings**（设置）> **Internet options**（互联网选项）> **Advanced**（高级）并向下滚动至 Security（安全）部分。
3. 禁用（取消选中）**Enable Enhanced Protected Mode**（启用增强保护模式）选项。
4. 单击 **OK**（确定）。



在互联网*Explorer* 中，*Palo Alto Networks* 建议不要禁用保护模式，这与增强保护模式不同。

## 使用 *PAN-OS XML API* 检索源自 *Terminal Server* 的用户映射

PAN-OS XML API 使用标准的 HTTP 请求来发送和接收数据。API 调用可直接从命令行实用程序（如 cURL）发起，也可以使用任何支持 RESTful 服务的脚本或应用程序框架发起。

要使非 Windows 终端服务器能够将用户映射信息直接发送到防火墙，请创建提取用户登录和退出事件的脚本，并使用这些脚本来提取 PAN-OS XML API 请求格式输入。然后，定义利用 cURL 或 wget 将 XML API 请求提交到防火墙并提供防火墙的 API 密匙以确保通信安全的机制。利用以下 API 消息从多用户系统创建用户映射（例如终端服务器请求）：

- **<multiusersystem>** — 在防火墙上设置 XML API 多用户系统的配置。此消息可用来定义终端服务器的 IP 地址（该地址是指此终端服务器上的所有用户的源地址）。另外，**<multiusersystem>** 设置消息可用来指定分配以执行用户映射的源端口数的范围和登录时分配给每个单个用户的端口数（称为块大小）。如果想使用默认源端口分配范围 (1025-65534) 和块大小 (200)，则无需发送 **<multiusersystem>** 设置事件到防火墙。相反，接收到首个用户登录事件消息时，防火墙会使用默认设置自动生成 XML API 多用户系统配置。
- **<blockstart>** — 与 **<login>** 和 **<logout>** 消息一起使用，表示已分配给用户的源端口数。防火墙随后使用该块大小来确定映射到登录消息中的 IP 地址和用户名的端口数的范围。例如，如果 **<blockstart>** 值为 13200，且为多用户系统配置的块大小为 300，那么，分配给用户的实际源端口范围为 13200 至 13499。用户启用的每个连接都应使用已分配范围内的唯一源端口数，这样可使防火墙能够基于其 IP 地址-端口-用户映射确定用户，从而实施基于用户和组的安全规则。当用户用完已分配的所有端口时，终端服务器必须发送为用户分配新的端口范围新的 **<login>** 消息，以便防火墙更新 IP 地址-端口-用户映射。另外，单个用户名可同时拥有已映射的多个端口块。当接收到含 **<blockstart>** 参数的 **<logout>** 消息时，防火墙将从其映射表中移除相应的 IP 地址-端口-用户映射。当接收到含用户名和 IP 地址但不含 **<blockstart>** 的 **<logout>** 消息时，防火墙将从其映射表中移除用户。此外，当接收到只含 IP 地址的 **<logout>** 消息时，防火墙将从其映射表中移除多用户系统以及与之关联的所有映射。



终端服务器发送到防火墙的 *XML* 文件可包含多个消息类型，并且这些消息在文件中无需以特殊顺序排列。但是，当接收到含多个消息类型的 *XML* 文件时，防火墙将按照以下顺序进行处理：首先处理多用户系统请求，其次是登录事件，然后再是退出事件。

以下工作流程介绍了一个如何使用 PAN-OS XML API 将用户映射从非 Windows 终端服务器发送到防火墙的示例。

STEP 1 | 生成用于对防火墙和终端服务器之间的 API 通信进行身份验证的 API 密匙。要生成 API 密匙，则必须提供管理帐户的登录凭证；所有管理员都可使用 API（包括使用已启用的 XML API 权限的基于角色的管理员）。



© 2019 Palo Alto Networks, Inc.

密码中的任何特殊字符都必须是 *URL*/百分比编码。

从浏览器登录到防火墙。然后，要生成防火墙的 API 密匙，请打开一个新的浏览器窗口并输入以下 URL：

```
https://<Firewall-IPaddress>/api/?
type=keygen&user=<username>&password=<password>
```

其中，**<Firewall-IPaddress>** 是防火墙的 IP 地址或 FQDN，**<username>** 和 **<password>** 是防火墙上的管理用户帐户的凭证。例如：

```
https://10.1.2.5/api/?type=keygen&user=admin&password=admin
```

防火墙对含密匙的消息作出响应，例如：

```
<response status="success">
   <result>
      <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
   </result>
</response>
```

STEP 2 | （可选）生成终端服务器将发送来指定终端服务代理使用的每个用户的端口范围和端口块大小的设置消息。

如果终端服务代理未发送设置消息，防火墙会在收到首条登录消息时使用以下默认设置自动创建终端服务器代理配置：

- 默认端口范围：1025 到 65534
- 每个用户的块大小：200
- 多用户系统的最大数量：1，000

下面显示样本设置消息：

```
<uid-message>
  <payload>
<multiusersystem>
<entry ip="10.1.1.23" startport="20000"          endport="39999"
 blocksize="100/">
</multiusersystem>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

其中，`entry ip` 指定分配给终端服务器用户的 IP 地址，`startport` 和 `endport` 指定分配端口到单个用户时要使用的端口范围，`blocksize` 指定要分配给每个用户的端口数。块大小的最大值为 4000，每个多用户系统可分配最多 1000 个块。

切记，定义自定义块大小或端口范围时，必须配置分配给端口范围内的每个端口的值以及无缺口或未使用端口的值。例如，如果将端口范围设置为 1000-1499，则应将块大小设置为 100，而不是 200。这是因为如果设置为 200，端口范围的末端则会有未使用的端口。

STEP 3 | 创建用于提取登录事件的脚本，并创建要发送到防火墙的 XML 输入文件。



© 2019 Palo Alto Networks, Inc.

确保此脚本在固定边界强制分配端口数范围，且无任何窗口重叠。例如，如果端口范围为 1000-1999，块大小为 200，那么可接受的块起始值应为 1000、1200、1400、1600 或 1800。块起始值 1001、1300 或 1850 为不可接受值，因为端口范围内的某些端口号会处于未使用状态。



终端服务器发送到防火墙的登录事件负载可包含多个登录日志。

以下显示 PAN-OS XML 登录事件的输入文件格式：

```
<uid-message>
<payload>
<login>
<entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
<entry name="acme\jparker" ip="10.1.1.23" blockstart="20100">
<entry name="acme\ccrisp" ip="10.1.1.23" blockstart="21000">
</login>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

防火墙使用该信息填充其用户映射表。基于从上述示例中提取的映射，如果防火墙已接收含源地址和 10.1.1.23:20101 端口的数据包，则会将请求映射到用户 jparker 以实施策略。



每个多用户系统可分配最多 *1,000* 个端口块。

STEP 4 | 创建用于提取退出事件的脚本，并创建要发送到防火墙的 XML 输入文件。

当接收到含 `blockstart` 参数的 `logout` 事件消息时，防火墙将移除相应的 IP 地址-端口-用户映射。当接收到含用户名和 IP 地址但不含 `blockstart` 参数的 `logout` 消息时，防火墙将移除此用户的所有映射。此外，接收到只含 IP 地址的 `logout` 消息时，防火墙将移除多用户系统以及与之关联的所有映射。

以下显示 PAN-OS XML 退出事件的输入文件格式：

```
<uid-message>
<payload>
<logout>
<entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
<entry name="acme\ccrisp" ip="10.1.1.23">
<entry ip="10.2.5.4">
</logout>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```



您也可以使用以下 *CLI* 命令从防火墙上清除多用户系统条目：***clear xml-api multiusersystem***

STEP 5 | 确保创建的脚本包括一种动态实施方式，通过此方式可将使用 XML API 分配的端口块范围与分配给终端服务器上的用户的实际源端口进行匹配，以及在用户退出或端口分配发生变更时移除映射。



© 2019 Palo Alto Networks, Inc.

执行此操作的方式是使用 Netfilter NAT 规则将用户会话隐藏于通过基于 uid 的 XML API 分配的特定端口范围后。例如，要确保将带用户 ID jjaso 的用户映射到源网络地址转换 (SNAT) 值 10.1.1.23:20000-20099，创建的脚本则应包含：

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner jjaso -p
 tcp -j SNAT --to-source 10.1.1.23:20000-20099
```

同样地，当用户退出或端口分配发生变更时，所创建的脚本还应确保 IP 表路由配置动态移除 SNAT 映射：

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```

STEP 6 | 定义如何将含设置、登录和退出事件的 XML 输入文件打包到 wget 或 cURL 消息中以传送到防火墙。

要将文件应用到使用 **wget** 的防火墙：

```
> wget --post file <filename> “https://<Firewall-IPaddress>/api/?type=user-
id&key=<key>&file-name=<input_filename.xml>&client=wget&vsys=<VSYS_name>”
```

例如，用于将命名为 login.xml 的输入文件发送到使用 wget 密匙为 `k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg` 的位于 10.2.5.11 的防火墙的语法应显示如下：

```
> wget --post file login.xml “https://10.2.5.11/api/?type=user-
id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&file-
name=login.xml&client=wget&vsys=vsys1”
```

要将文件应用到使用 **cURL** 的防火墙：

```
> curl --form file=@<filename> https://<Firewall-IPaddress>/api/?
type=user-id&key=<key>&vsys=<VSYS_name>
```

例如，使用 cURL 的密匙 `k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg` 将名为 login.xml 的输入文件发送到位于 10.2.5.11 的防火墙的语法如下：

```
> curl --form file@login.xml “https://10.2.5.11/api/?type=user-
id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&vsys=vsys1”
```

STEP 7 | 验证防火墙是否正在成功地接收终端服务器发出的登录事件。

要验证配置，请打开连接到防火墙的 SSH 连接并运行以下 CLI 命令：

要验证终端服务器是否通过 **XML** 连接到防火墙：

```
admin@PA-5250> show user xml-api multiusersystem
Host            Vsys    Users   Blocks
-----------------------------------------
10.5.204.43   vsys1      5         2
```

要验证防火墙是否通过 **XML** 接收终端服务器发出的映射：

```
admin@PA-5250> show user ip-port-user-mapping all

Global max host index 1, host hash count 1
```



© 2019 Palo Alto Networks, Inc.

```
XML API Multi-user System 10.5.204.43
Vsys 1, Flag 3
Port range: 20000 - 39999
Port size: start 200; max 2000
Block count 100, port count 20000
20000-20199: acme\administrator

Total host: 1
```

# 使用 XML API 将用户映射发送到 User-ID

User-ID 提供多种开箱即用的方式来获取用户映射信息。然而，您可能拥有用于捕获用户信息的应用程序或设备，但在本机无法与 User-ID 整合。例如，您可能拥有内部开发的自定义应用程序或设备，但它们不支持标准的用户映射方法。在这种情况下，可使用 PAN-OS XML API 创建可将信息发送到 PAN-OS 集成的 User-ID 代理或直接发送到防火墙的自定义脚本。PAN-OS XML API 使用标准的 HTTP 请求来发送和接收数据。API 调用可直接从命令行实用程序（如 cURL）发起，也可以使用任何支持 POST 和 GET 请求的脚本或应用程序框架发起。

要使外部系统能够将用户映射信息发送到 PAN-OS 集成的 User-ID 代理，可创建用于提取用户登录和退出事件的脚本，并将这些事件用作为 PAN-OS XML API 请求的输入。然后，定义将 XML API 请求提交到防火墙的机制（利用 cURL 或 wget），并使用防火墙的 API 密匙以确保通信安全。有关更多详细信息，请参阅《PAN-OS XML API 使用指南》。


© 2019 Palo Alto Networks, Inc.

# 启用基于用户和基于组的策略

启用 User-ID 后，将可以配置适用于特定用户和组的安全策略。基于用户的策略控制还可包括应用程序信息（包括其所属的类别和子类别、底层技术或应用程序特性）。定义策略规则，以便在出站或入站方向安全启用基于用户或用户组的应用程序。

基于用户的策略示例包括：

- 仅允许 IT 部门在标准端口上使用诸如 SSH、telnet 和 FTP 等工具。
- 允许帮助台服务组使用 Slack。
- 允许所有用户阅读 Facebook，但阻止使用 Facebook 应用程序，并限制向员工发布营销信息。



© 2019 Palo Alto Networks, Inc.

# 为具有多个帐户的用户启用策略

如果您的组织中的某个用户有多项职责，则该用户可能具有多个用户名（帐户），每个包含不同特权以访问一组特定服务，但包含全部用户名，这些用户名分享相同 IP 地址（用户的客户端系统）。但是，User-ID 代理将任何一个 IP 地址（或者终端服务器用户的 IP 地址和端口范围）只能映射到一个用户名来实施策略，并且无法预测代理将预测哪个用户名。要控制某一用户的所有用户名的访问权，您必须对规则、用户组和 User-ID 代理进行调整。

例如，假设防火墙有一个规则是允许用户名 corp_user 访问电子邮件，并且还有一个规则是允许用户名 admin_user 访问 MySQL Server。服务器从同一个客户端 IP 地址使用任一用户名登录。如果 User-ID 代理将 IP 地址映射到 corp_user，则无论用户是以 corp_user 身份还是 admin_user 身份登录，防火墙都会将该用户识别为 corp_user 并允许访问电子邮件，但不允许访问 MySQL Server。另一方面，如果 User-ID 代理将 IP 地址映射到 admin_user，则防火墙始终将该用户识别为 admin_user，无论登录名如何，并且允许访问 MySQL Server，但不允许访问电子邮件。以下步骤描述本示例如何同时实现这两个规则。

STEP 1 | 为需要不同访问特权的每个服务配置用户组。

在此示例中，每个组面向单个服务（电子邮件或 MySQL Server）。但是，通常是为一组需要相同特权的服务配置每个组（例如，一个面向所有基本用户服务的组和一个面向所有管理服务的组）。

如果您的组织的用户组已经可以访问用户需要的服务，则只需要将用于限制性更少的服务的用户名添加到这些组。在此示例中，电子邮件服务器需要的访问权的限定性低于 MySQL Server 并且用于访问电子邮件的用户名是 corp_user。因此，您将 corp_user 添加到可以访问电子邮件的组 (corp_employees) 并添加到可访问 MySQL Server 的组 (network_services)。

如果将某个用户名添加到特定现有组会违反您的组织惯例，则可以根据 LDAP 筛选器创建自定义组。对于本示例，假设 network_services 是自定义组，您可以按如下所示配置此组：

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置），然后单击 **Add**（添加）以添加具有唯一 **Name**（名称）的组映射配置。
2. 选择 LDAP **Server Profile**（服务器配置文件）并确保启用了 **Enabled**（已启用）复选框。
3. 选择 **Custom Group**（自定义组）选项卡，然后选择 **Add**（添加）以添加自定义组，并且以 network_services 作为 **Name**（名称）。
4. 指定与 corp_user 的 LDAP 熟悉相匹配的 **LDAP Filter**（**LDAP** 筛选器）并单击 **OK**（确定）。
5. 单击 **OK**（确定）和 **Commit**（提交）。



之后，如果有其他用户位于限制性更低的服务的组中，并且这些用户被授予了访问限制性更高的服务的其他用户名，则可以将这些用户名添加到限制性更高的服务的组中。这种情况比相反情况更常见；可以访问限制性更高的服务的用户通常已经能够访问限制性更低的服务。

STEP 2 | 配置规则以根据您刚刚配置的组来控制用户访问权。

更多信息，请参阅启用基于用户和基于组的策略执行。

1. 配置安全规则以允许 corp_employees 组访问电子邮件。
2. 配置安全规则以允许 network_services 组访问 MySQL Server。

STEP 3 | 配置 User-ID 代理的忽略列表。

这确保 User-ID 代理将客户端 IP 地址仅映射到的用户名是属于分配了您刚刚配置的规则的组。忽略列表必须包含不是这些组成员的用户的用户名。

在此示例中，您将 admin_user 添加到基于 Windows 的 User-ID 代理的忽略列表，以确保其将客户端 IP 地址映射到 corp_user。这保证了无论用户是以 corp_user 身份还是 admin_user 身份登录，防火墙都会将该用户识别为 corp_user 并应用您配置的两个规则，因为 corp_user 是规则所引用的组的成员。



© 2019 Palo Alto Networks, Inc.

1. 创建 `ignore_user_list.txt` 文件。
2. 打开此文件并添加 admin_user。

   如果您稍后添加了更多用户名，则每个用户名必须在单独一行中。
3. 将文件保存到安装了代理的域服务器上的 User-ID 代理文件夹中。



如果使用 *PAN-OS* 集成的 *User-ID* 代理，请参阅使用 PAN-OS 集成的 User-ID 代理来配置用户映射了解有关如何配置忽略列表的说明。

STEP 4 | 为受限制的服务配置端点身份验证。

这使端点可以验证用户的凭据并保留了为具有多个用户名的用户启用访问权的功能。

在此示例中，您已配置了防火墙规则，以允许 corp_user（network_services 组的成员）将服务请求发送到 MySQL Server。您现在必须配置 MySQL Server 以响应任何未经授权的用户名（如 corp_user）：通过提示用户输入授权用户名 (admin_user) 的登录凭据。



如果用户以 *admin_user* 身份登录网络，则用户随后可以访问 *MySQL Server*，而不会提示用户再次输入 *admin_user* 凭据。

在此示例中，corp_user 和 admin_user 都具有电子邮件帐户，因此电子邮件服务器将不会提示用户输入其他凭据，无论用户在登录网络时输入了哪个用户名。

防火墙现在准备好为具有多个用户名的用户实施规则。



© 2019 Palo Alto Networks, Inc.

# 验证用户标识配置

配置好用户和组映射，启用安全策略上的 User-ID，并配置好身份验证策略后，必须验证 User-ID 是否正常运行。

STEP 1 | 访问防火墙 CLI。

STEP 2 | 验证组映射是否可以正常运行：

在 CLI 中，输入以下操作命令：

```
> show user group-mapping statistics
```

STEP 3 | 验证用户映射是否可以正常运行：

若使用 PAN-OS 集成 User-ID 代理，则可以使用下列命令从 CLI 对其进行验证：

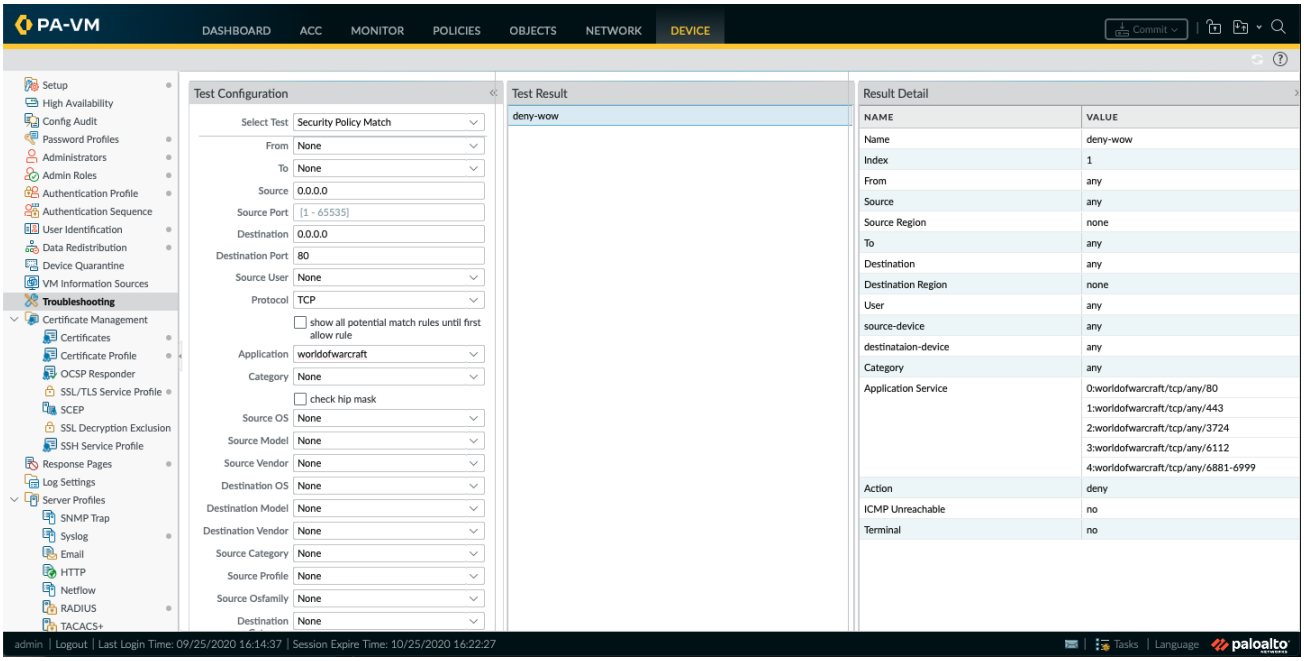
```
> show user ip-user-mapping-mp all
IP              Vsys  From  User          Timeout (sec)
------------------------------------------------------
192.168.201.1   vsys1 UIA   acme\george            210
192.168.201.11  vsys1 UIA   acme\duane             210
192.168.201.50  vsys1 UIA   acme\betsy             210
192.168.201.10  vsys1 UIA   acme\administrator     210
192.168.201.100 vsys1 AD    acme\administrator     748
Total: 5 users
*: WMI probe succeeded
```

STEP 4 | 测试您的安全策略规则。

- 从启用了 User-ID 的区域中的某台计算机开始，尝试访问站点和应用程序，以测试在策略中定义的规则，并确保按照需求允许和拒绝通信。
- 您还可以对运行中的配置执行故障排除，以确定策略是否配置正确。例如，假设您已经有一个阻止用户玩 World of Warcraft 的规则，则可以按照如下所示测试策略：

1. 选择 **Device**（设备）> **Troubleshooting**（故障排除），并从选择测试下拉列表中选择 **Security Policy Match**（安全策略匹配）。
2. 输入 `0.0.0.0`，作为源和目标 IP 地址。这将针对所有源和目标 IP 地址执行策略匹配测试。
3. 输入目标端口。
4. 输入协议。
5. **Execute**（执行）安全策略匹配测试。


© 2019 Palo Alto Networks, Inc.




STEP 5 | 测试您的身份验证策略和身份验证门户配置。

1. 在同一个区域中，转到非您的目录成员的计算机，例如 Mac OS 系统，然后 ping 到区域外部的系统。ping 操作应该可以正常工作，无需进行身份验证。
2. 在同一台计算机中，打开浏览器并导航到与您定义的身份验证规则相匹配的目标区域中的网站。身份验证门户 Web 表单应显示并提醒您提供登录凭据。
3. 使用正确的凭据登录并确认重定向到请求的页面。
4. 还可以使用以下 **`test authentication-policy-match`** 操作命令来测试身份验证策略：

```
> test authentication-policy-match from corporate to internet source
 192.168.201.10 destination 8.8.8.8
Matched rule: 'authentication portal' action: web-form
```

STEP 6 | 验证日志文件显示用户名。

选择一个日志页面（例如 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量））并验证源用户列是否显示用户名。

STEP 7 | 验用证报告显示户名。

1. 选择 监视器 > 报告.
2. 选择一个包括用户名的报告类型。例如，在被拒绝的应用程序报告中，“Source User（源用户）”列应显示尝试访问应用程序的用户列表。



© 2019 Palo Alto Networks, Inc.

# 在大规模网络中部署 User-ID

大规模网络可以有数百个防火墙可进行查询以便将 IP 地址映射到用户名或将用户名映射到用户组的信息源。您可以通过在 User-ID 代理收集用户映射和组映射信息之前聚合信息，简化此类网络的 User-ID 管理，从而减少所需的代理数量。

大规模网络还可以有无数个使用映射信息实施策略的防火墙。您还可以通过配置某些防火墙通过重新分发而非直接查询来获取映射信息，减少防火墙和信息源在查询进程中使用的资源数量。当用户依赖于本地来源进行身份验证（例如区域目录服务），但需要访问远程服务和应用程序（如全局数据中心应用程序）时，重新分发还能使防火墙实施基于用户的策略。

如果您配置身份验证策略，您的防火墙还必须将与用户对身份验证挑战的响应相关联的身份验证时间戳进行重新分发。防火墙使用时间戳来评估身份验证策略规则的超时。超时允许身份验证成功的用户在稍后请求服务和应用程序，而无需在超时时段内再次进行身份验证。即使最初允许用户访问的防火墙与以后控制该用户访问的防火墙不同，重新分发时间戳也能让您为每个用户执行一致超时。

如果您配置了多个虚拟系统，您可以通过选择虚拟系统作为 User-ID 中心，在多个虚拟系统之间共享 IP 地址到用户名映射信息。

- 为大量映射信息源部署 User-ID
- 重新分发数据和身份验证时间戳
- 共享跨虚拟系统的 User-ID 映射

## 为大量映射信息源部署 User-ID

您可以使用 Windows 日志转发和全局目录服务器简化大规模网络的 Microsoft Active Directory (AD) 域控制器或 Exchange 服务器中的用户映射和组映射。这些方法通过在 User-ID 代理收集映射信息之前聚合信息，简化此类网络的 User-ID 管理，从而减少所需的代理数量。

- Windows 日志转发和全局目录服务器
- 计划大规模 User-ID 部署
- 配置 Windows 日志转发
- 为大量映射信息源配置 User-ID

### *Windows* 日志转发和全局目录服务器

由于每个 User-ID 代理最多可以监控 100 个服务器，因此防火墙需要多个 User-ID 代理来监控数百个 AD 域控制器或 Exchange 服务器的网络。创建和管理多个 User-ID 代理涉及到相当多的管理开销，特别是关于扩展难以跟踪新域控制器的网络。Windows 日志转发可降低要监控的服务器数量，从而降低要管理的 User-ID 代理数量，从而使您可以最大程度减少管理开销。配置 Windows 日志转发时，多个域控制器将其登录事件导出到单个域成员（User-ID 代理将从该域成员中收集用户映射信息）。



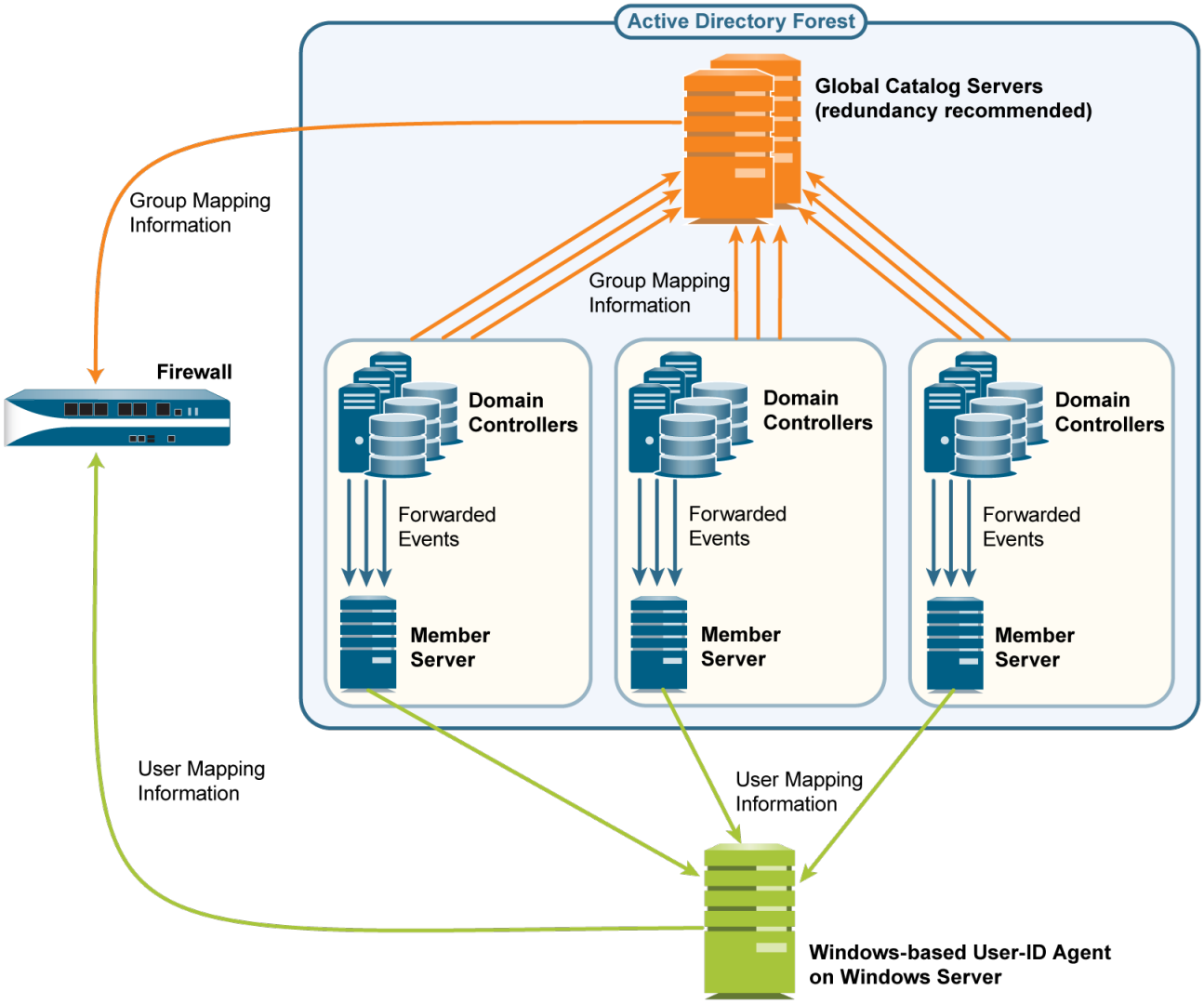
您可以为 *Windows Server* 版本 *2012* 和 *2012 R2* 配置 *Windows* 日志转发。非 *Microsoft* 服务器无法使用 *Windows* 日志转发。

要在大规模网络中收集组映射信息，您可以配置防火墙以查询从域控制器中接收帐户信息的全局目录服务器。

下图说明了在防火墙使用基于 Windows 的 User-ID 代理的大规模网络的用户映射和组映射。请参阅 计划大规模 User-ID 部署 以确定此部署是否适合您的网络。



© 2019 Palo Alto Networks, Inc.




## 计划大规模 *User-ID* 部署

决定是否对 User-ID 实施使用 Windows 日志转发和全局目录服务器时，请咨询您的系统管理员以确定：

- 域控制器将登录事件转发到成员服务器所需要的带宽。带宽是域控制器的登录率（每分钟登录次数）域每个登录事件的字节大小的乘积。

  域控制器不会转发其整个安全日志；域控制器仅转发用户映射流程每次登录所需要的事件：对于 Windows Server 2012 和 MS Exchange，为四个事件。
- 以下网络元素是否支持所需带宽：
  - **Domain controllers**（域控制器）— 必须支持与转发事件相关联的处理负载。
  - **Member Servers**（成员服务器）— 必须支持与接收事件相关联的处理负载。
  - **Connections**（连接）— 域控制器、成员服务器和全局目录服务器的地理分部（本地还是远程）是一项因素。通常，远程分发支持更低带宽。

## 配置 *Windows* 日志转发

要配置 Windows 日志转发，您需要有管理特权以在 Windows 服务器上配置组策略。在所有 *Windows Event Collectors*（*Windows* 事件收集器）上配置 Windows 日志转发 —— 从域控制器收集登录事件的成员服务器。以下是任务的概述；请参阅 Windows 服务器文档以了解具体步骤。



© 2019 Palo Alto Networks, Inc.

STEP 1 | 在每个成员服务器上，启用事件收集，添加域控制器作为事件源并配置事件收集查询（订阅）。您在订阅中指定的活动根据域控制器平台而异：

- **Windows Server 2012**（包括 **R2**）和 **2016** 或 **MS Exchange** — 必需事件的事件 ID 为 4768（授予了身份验证票据）、4769（授予了服务票据）、4770（续订了授予的票据）和 4624（登录成功）。



要尽快转发事件，请在配置订阅时 *Minimize Latency*（最大限度减少延迟）。

User-ID 代理监视 Windows 事件收集器上的安全日志，而不是默认的已转发事件位置。要将事件日志记录路径更改为安全日志，请对每个 Windows 事件收集器执行以下步骤。

1. 打开“事件查看器”。
2. 右键单击 **Security**（安全）日志，然后选择 **Properties**（属性）。
3. 复制 **Log path**（日志路径）（默认为 `%SystemRoot%\System32\Winevt\Logs\security.evtx`），然后单击 **OK**（确定）。
4. 右键单击 **Forwarded Events**（已转发事件）文件夹，然后选择 **Properties**（属性）。
5. 通过粘贴 **Security**（安全）日志中的值来替换默认 **Log path**（日志路径）(`%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx`)，然后单击 **OK**（确定）。

STEP 2 | 配置组策略以在域控制器上启用 Windows 远程管理 (WinRM)。

STEP 3 | 配置组策略以在域控制器上启用 Windows 事件转发。

## 为大量映射信息源配置 *User-ID*

STEP 1 | 在将要收集登录事件的成员服务器上配置 Window 日志转发。

配置 Windows 日志转发。步骤需要管理特权以在 Windows 服务器上配置组策略。

STEP 2 | 安装基于 Windows 的 User-ID 代理。

在可以访问成员服务器的 Windows 服务器上安装基于 Windows 的 User-ID 代理。确保将要托管 User-ID 代理的系统与其将要监控的服务器属于同一个域。

STEP 3 | 配置 User-ID 代理以从成员服务器收集用户映射信息。

1. 启动基于 Windows 的 User-ID 代理。
2. 选择 **User Identification**（用户标识）> **Discovery**（发现）并针对将要从域控制器中接收事件的每个成员服务器执行以下步骤：
   1. 在“服务器”部分中，单击 **Add**（添加）并输入 **Name**(名称)以标识成员服务器。
   2. 在 **Server Address**（服务器地址）字段中，输入成员服务器的 FQDN 或 IP 地址。
   3. 对于 **Server Type**（服务器类型），选择 **Microsoft Active Directory**。
   4. 单击 **OK**（确定）以保存服务器条目。
3. 配置剩余的 User-ID 代理设置（请参阅为用户映射配置基于 Windows 的 User-ID 代理）。
4. 如果 User-ID 源提供多种格式的用户名，则在将用户映射到组时指定 **Primary Username**（主用户名）的格式。

   主用户名是指用于标识防火墙上用户的用户名，无论 User-ID 源提供的格式是什么，都可代表报告和日志中的用户。

STEP 4 | 配置 LDAP 服务器配置文件以指定防火墙如何连接到全局目录服务器（最多四个）来获取组映射信息。



© 2019 Palo Alto Networks, Inc.

为提高可用性，请至少使用两个全局目录服务器以实现冗余性。

您只能对通用组收集组映射信息，不能对本地域组（子域）收集。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **LDAP**，然后单击 **Add**（添加）并输入配置文件 **Name**（名称）。
2. 在“服务器”部分中，对于每个全局目录，单击 **Add**（添加），然后输入服务器的 **Name**（名称）、IP 地址（**LDAP Server**（**LDAP** 服务器））和 **Port**（端口）。对于纯文本或启动传输层安全（启动 TLS）连接，请对 **Port**（端口）使用 3268。对于基于 SSL 连接的 LDAP，请对 **Port**（端口）使用 3269。如果连接将使用“启动基于 SSL 的 TLS 或 LDAP”，并选中 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）复选框。
3. 在 **Base Dn**（基础 **Dn**）字段字段中，输入防火墙将要开始搜索组映射信息的全局目录服务器（例如 `DC=acbdomain,DC=com`）。
4. 对于 **Type**（类型），选择 **active-directory**。

STEP 5 | 配置 LDAP 服务器配置文件以指定防火墙如何连接到包含域映射信息的服务器（最多四个）。

User-ID 使用此信息将 DNS 域名称映射到 NetBios 域名。映射确保策略规则中的域/用户名引用。

为提高可用性，请至少使用两个服务器以实现冗余性。

这些步骤与您在上一步中为全局目录创建 LDAP 服务器配置文件的步骤相同，但以下字段除外：

- **LDAP Server**（**LDAP** 服务器）— 输入包含域映射信息的域控制器的 IP 地址。
- **Port**（端口）— 对于纯文本或启动 TLS 连接，请使用 **Port**（端口）389。对于基于 SSL 连接的 LDAP，请对 **Port**（端口）使用 636。如果连接将使用“启动基于 SSL 的 TLS 或 LDAP”，并选中 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）复选框。
- **Base Dn**（基础 **DN**）— 选择防火墙将开始搜索域映射信息的域控制器中的起始 DN。值必须以下列字符串开头：`cn=partitions,cn=configuration`（例如 `cn=partitions,cn=configuration,DC=acbdomain,DC=com`）。

STEP 6 | 为您创建的每个 LDAP 服务器配置文件创建组映射配置。

1. 选择 **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）。
2. 单击 **Add**（添加）并输入 **Name**（名称）以标识组映射配置。
3. 选择 LDAP **Server Profile**（服务器配置文件）并确保选中了 **Enabled**（已启用）复选框。

   如果全局目录和域映射服务器引用了比安全规则需要的更多组，请配置 *Group Include List*（组包括列表）和/或 *Custom Group*（自定义组列表以限制 *User-ID* 执行映射的组。
4. 单击 **OK**（确定）和 **Commit**（提交）。

# 在 HTTP 标头中插入用户名

当您使用 Palo Alto Networks 防火墙配置辅助实施设备以实施基于用户的策略时，此辅助设备可能不包含防火墙中 IP 地址到用户名的映射。传输用户信息到下游设备可能要求部署代理等其他设备，或是可能会对用户体验产生负面影响（例如，用户必须多次登录）。通过在 HTTP 标头中共享用户标识，可以在不影响用户体验或是无需部署其他基础设施的情况下实施基于用户的策略。

配置此功能时，应用 URL 配置文件到您的安全策略，并提交您的更改，之后，防火墙将：

1. 以源用户组映射中主用户名的格式填充用户和域值。



© 2019 Palo Alto Networks, Inc.

2. 使用 Base64 对这些信息进行编码。
3. 添加 Base64 编码的标头到负载中。
4. 路由流量到下游设备。

如果只想在用户访问特定域时包含用户名和域，请配置一个域列表，这样，防火墙仅在列表中的域与 HTTP 请求的主机标头匹配时才会插入标头。

要与下游设备共享用户信息，必须先启用 User-ID，并配置组映射。

要在标头中包含用户名和域，防火墙需要用户的 *IP* 地址到用户名的映射。如果未映射用户，防火墙将为标头中的域和用户名插入 *Base64* 编码的未知内容。

要在 HTTP 流量标头中包含用户名和域，必须先创建一个解密配置文件以解密 HTTPS 流量。

此功能支持转发代理解密流量。

STEP 1 | 创建或编辑 **URL** 筛选配置文件。

如果 *URL* 筛选配置文件的操作是阻止域，则防火墙不会插入标头。

STEP 2 | 使用预定义类型创建或编辑 HTTP 标头插入条目。

您最多可为每个配置文件定义 5 个标头。

STEP 3 | 选择 **Dynamic Fields**（动态字段）作为标头 **Type**（类型）。

STEP 4 | **Add**（添加）想要插入标头的 **Domains**（域）。用户访问列表中的域时，防火墙将插入特定标头。

STEP 5 | **Add**（添加）新 **Header**（标头）或是选择 **X-Authenticated-User** 进行编辑。

STEP 6 | 选择标头 **Value**（值）格式（`($domain)\($user)` 或 `WinNT://($domain)/($user)`），或使用 `($domain)` 和 `($user)` 动态令牌（例如，用于 UserPrincipalName 的 `($user)@($domain)`）输入自己的格式。

每个值只能使用相同的动态令牌（***`($user)`*** 或 ***`($domain)`***）一次。

每个值最多可包含 512 个字符。防火墙使用组映射配置文件中的主用户名填充动态令牌 `($user)` 和 `($domain)`。例如：

- 如果主用户名是 sAMAccountName，则 `($user)` 的值为 sAMAccountName，`($domain)` 的值为 NetBios domain name。
- 如果主用户名是 UserPrincipalName，则 `($user)` 是用户账户名称（前缀），`($domain)` 是域名系统 (DNS) 名称。

STEP 7 | （可选）选择 **Log**（日志）以启用标头插入日志记录。

STEP 8 | 将 URL 筛选配置文件应用到 HTTP 或 HTTPS 流量的安全策略规则。

STEP 9 | 选择 **OK**（确定）两次，以确认 HTTP 标头配置。

STEP 10 | **Commit**（提交）更改。


© 2019 Palo Alto Networks, Inc.

STEP 11 | 验证防火墙是否在 HTTP 标头中包含用户名和域。

- 使用 **show user user-ids all** 命令验证组映射是否正确。
- 使用 **show counter global name ctd_header_insert** 命令查看防火墙插入的 HTTP 标头数。
- 如果已在步骤 7 中配置日志记录，请检查插入的 Base64 编码负载的日志（例如，**corpexample \testuser** 应在日志中显示为 **Y29ycGV4YW1wbGVcdGVzdHVzZXI=**）。

# 重新分发数据和身份验证时间戳

在大型网络中，您可以配置一些防火墙通过重新分发来收集映射信息，而不是配置所有防火墙直接查询映射信息源，从而简化资源使用。

如果您配置身份验证策略，防火墙还必须重新分发在用户进行身份验证以访问应用程序和服务时生成的身份验证时间戳。防火墙使用时间戳来评估身份验证策略规则的超时。超时允许身份验证成功的用户在稍后请求服务和应用程序，而无需在超时时段内再次进行身份验证。重新分发时间戳使您能够在网络中的所有防火墙上执行一致的超时。

防火墙将数据和身份验证时间戳作为同一重新分发流程的一部分进行共享；而不必单独配置每种信息类型的重新分发。

- 防火墙有关数据重新分发的部署
- 配置数据重新分发

## 防火墙有关数据重新分发的部署

在大型网络中，您可以配置一些防火墙通过重新分发来收集数据，而不是配置所有防火墙直接查询数据源，从而简化资源使用。数据重新分发还可以提供粒度，允许您仅将指定类型的信息重新分发给所选的设备。此外，您还可以使用子网和范围筛选 IP 用户映射或 IP 标记映射，确保防火墙仅收集需要实施策略的映射。

数据重新分发既可以是单向（代理将数据提供给客户端），也可以是双向（代理和客户端可以同时发送和接收数据）。

若要重新分发数据，可以使用下列架构类型：

- 适用于单个区域的中心辐射型架构：

  要在防火墙之间重新分发数据，最佳做法是采用中心辐射型架构。在这种配置中，中心防火墙从 Windows User-ID 代理、Syslog 服务器、域控制器或其他防火墙等源收集数据。配置重新分发客户端防火墙以从中心防火墙收集数据。

  例如，中心（由一对 VM-50 构成，以实现复原能力）可以连接到 User-ID 源以进行用户映射。随后，中心可以在使用用户映射强制实施策略的客户端防火墙连接到中心以检索数据时，重新分发用户映射。
- 适用于多个区域的多中心辐射型架构：

  如果已在多个区域部署防火墙，且希望将数据分发给所有这些区域的防火墙，以便能实现策略实施的一致性，而不会受用户登录位置的影响，那么，您可以针对多个区域使用多中心辐射型架构。

  首先，在各个区域配置防火墙以从源收集数据。此防火墙将充当重新分发的本地中心，从该区域内的所有源收集数据，并将这些数据重新分发给客户端防火墙。接下来，配置客户端防火墙以连接到该区域以及其他所有区域的重新分发中心，这样，客户端防火墙就拥有所有中心的所有数据。

  最佳做法是在防火墙需要发送和接收数据时，启用区域内的双向重新分发。例如，如果防火墙既充当远程用户的 GlobalProtect 网关，又充当本地用户的分支防火墙，那么，防火墙必须将为远程用户收集的用户映射发送给中心防火墙，并从中心防火墙接收本地用户的用户映射。
- 层级式架构：

  要重新分发数据，您还可以使用层级式架构。例如，要重新分发 User-ID 信息等数据，请分层组织重新分发序列，其中，每一层都有一个或多个防火墙。在底层，在防火墙上运行的 PAN-OS 集成的 User-ID 代理和在 Windows 服务器上运行的基于 Windows 的 User-ID 代理将 IP 地址映射到用户名。每个上面的层



© 2019 Palo Alto Networks, Inc.

都有防火墙来接收来自其下面的层中多达 100 个重新分发点的映射消息和身份验证时间戳。顶层防火墙汇总来自所有层的映射信息和时间戳。此部署提供为所有用户配置策略（在顶层防火墙中）和为相应域中的部分用户配置特定区域或功能策略（在底层防火墙中）的选择。

在这种情况下，三层防火墙将来自本地办公室的映射和时间戳重新分发至区域办公室，然后再重新分发至全局数据中心。用于汇总所有信息的数据中心防火墙将与其他数据中心防火墙共享此信息，以便它们能够全部执行策略，并为整个网络上的用户生成报告。只有底层防火墙才使用 User-ID 代理查询目录服务器。

User-ID 代理查询的信息源不计入序列中的最多 10 个跃点中。然而，用于将映射信息转发至防火墙的基于 Windows 的 User-ID 代理计入在内。同时在本示例中，顶层有两个跃点：一个用于在一个数据中心防火墙中汇总信息，另一个用于与其他数据中心防火墙共享此信息。

## 配置数据重新分发

配置数据重新分发前，请

- ❑ 计划重新分发架构。要考虑的一些因素是：
  - 哪些防火墙将为所有数据类型实施策略？哪些防火墙将为数据子集执行特定区域或功能策略？
  - 重新分发序列需要多少个跃点来汇总所有数据？用户映射的最大允许跃点数为 10，IP 地址到用户映射和 IP 地址到标记映射的最大允许跃点数均为 1。
  - 如何最大程度减少用于查询用户映射信息源的防火墙的数量？查询防火墙的数量越少，防火墙和信息源上的处理负载就越少。
- ❑ 配置重新分发代理将从中获取数据以重新分发给客户端的数据源：
  - 通过 PAN-OS 集成 User-ID 代理或基于 Windows 的 User-ID 代理配置的用户映射
  - 动态地址组的 IP 地址到标记映射
  - 动态用户组的用户名到标记映射
  - 用于实现 基于 HIP 的策略实施的 GlobalProtect
  - 设备隔离数据（仅限 Panorama）
- ❑ 配置身份验证策略。

数据重新分发包括：

- 提供信息的重新分发代理
- 接收信息的重新分发代理

在数据重新分发序列中的防火墙上执行以下步骤。

STEP 1 | 在重新分发客户端防火墙上，配置防火墙、Panorama 或 Windows User-ID 代理作为数据重新分发代理。

1. 选择 **Device**（设备）> **Data Redistribution**（数据重新分发）> **Agents**（代理）。
2. **Add**（添加）重新分发代理，并输入 **Name**（名称）。
3. 确认代理 **Enabled**（已启用）。

STEP 2 | 使用代理 **Serial Number**（序列号）或 **Host and Port**（主机和端口）添加代理。

- 若要使用序列号添加代理，请选择要用作重新分发代理的防火墙的**Serial Number**（序列号）。
- 若要使用代理主机和端口信息添加代理，请：
  1. 输入**Host**（主机）信息。
  2. 选择主机是否为 **LDAP Proxy**（**LDAP** 代理）。
  3. 输入 **Port**（端口）（默认为 5007，范围为 1—65535）。
  4. （仅限多个虚拟系统）输入 **Collector Name**（收集器名称）以标识要用作重新分发代理的虚拟系统。


© 2019 Palo Alto Networks, Inc.

5. （仅限多个虚拟系统）输入并确认要用作重新分发代理的虚拟系统的 **Collector Pre-Shared Key**（收集器预先分享密钥）。

STEP 3 | 选择一个或多个要进行重新分发的代理的 **Data Type**（数据类型）。

- **IP User Mappings**（**IP** 用户映射）— User-ID 的 IP 地址到用户名映射。
- **IP Tags**（**IP** 标记）— 动态地址组的 IP 地址到标记映射。
- **User Tags**（用户标记）— 动态用户组的用户名到标记映射。
- **HIP**— GlobalProtect 的主机信息配置文件(HIP)，包括 HIP 对象和配置文件。
- **Quarantine List**（隔离列表）— 被GlobalProtect 标识为“已隔离”的设备。

STEP 4 | （仅限多个虚拟系统）将虚拟系统配置为可用于重新分发数据的收集器。

如果防火墙接收到数据但未重新分发，请跳过此步骤。



您可以在不同防火墙上或同一个防火墙上的虚拟系统之间重新分发信息。无论哪种情况，每个虚拟系统都将被视为重新分发序列中的一个跃点。

1. 选择 **Device**（设备）> **Data Redistribution**（数据重新分发）> **Collector Settings**（收集器设置）。
2. 编辑 **Data Redistribution Agent Setup**（数据重新分发代理设置）。
3. 输入将该防火墙或虚拟系统标识为 User-ID 代理的 **Collector Name**（收集器名称）和 **Pre-Shared Key**（预共享密钥）。
4. 单击 **OK**（确定）保存更改。

STEP 5 | （可选，但建议这样做）配置数据重新分发要包括和排除的网络。

重新分发 IP 地址到标记映射或 IP 地址到用户名映射时，您可以包括或排除网络和子网。



最佳做法是始终指定要包括和排除的网络，确保代理仅与内部资源进行通信。

1. 选择 **Device**（设备）> **Data Redistribution**（数据重新分发）> **Include/Exclude Networks**（包括/排除网络）。
2. **Add**（添加）条目并输入 **Name**（名称）。
3. 确保条目 **Enabled**（已启用）。
4. 选择要 **Include**（包括）或 **Exclude**（排除）条目。
5. 输入条目的 **Network Address**（网络地址）。
6. 单击 **OK**（确定）。

STEP 6 | 配置防火墙用于查询其他防火墙的 User-ID 信息的服务路由。

如果防火墙仅从基于 Windows 的 User-ID 代理或直接从信息源（例如目录服务器）而非其他防火墙接收用户映射信息，请跳过此步骤。

1. 选择**Device**（设备）> **Setup**（设置）> **Services**（服务）。
2. （仅限具有多个虚拟系统的防火墙）选择 **Global**（全局）（对于防火墙范围内的服务路由 ）或 **Virtual Systems**（虚拟系统）（对于虚拟系统特定服务路由），然后配置服务路由。
3. 单击 **Service Route Configuration**（服务路由配置），选择 **Customize**（自定义），然后根据网络协议选择 **IPv4** 或 **IPv6**。如果网络使用这两种协议，为这两种协议配置服务路由。
4. 选择 **UID Agent**（**UID** 代理），然后选择 **Source Interface**（源接口）和 **Source Address**（源地址）。
5. 单击 **OK**（确定）两次，以保存服务路由。

STEP 7 | 启用防火墙以在其他防火墙查询要重新分发的数据时进行响应。



© 2019 Palo Alto Networks, Inc.

如果防火墙接收到数据但未重新分发，请跳过此步骤。

配置接口管理配置文件（**User-ID** 服务已启用），并将配置文件分配给防火墙接口。

STEP 8 | （可选，但建议这样做）使用企业 PKI 中的自定义证书来建立重新分发客户端与重新分发代理之间的唯一信任链。

1. 在重新分发客户端防火墙上，创建一个适用于传出连接的自定义 SSL certificate profile（SSL 证书配置文件）。
2. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Secure Communication Settings**（安全通信设置）。
3. **Edit**（编辑）设置。
4. 选择 **Customize Secure Server Communication**（自定义安全服务器通信）选项。
5. 选择您在子步骤 1 中创建的 **Certificate Profile**（证书配置文件）。
6. 单击 **OK**（确定）。
7. 为 **Data Redistribution**（数据重新分发）**Customize Communication**（自定义通信）。
8. **Commit**（提交）更改。
9. 输入以下 CLI 命令以确认证书配置文件（`SSL` 配置）是否使用 自定义证书：**`show redistribution agent state <agent-name>`**（其中，*<agent-name>*是重新分发代理或 User-ID 代理的名称）。

STEP 9 | （可选，但建议这样做）使用企业 PKI 中的自定义证书来建立重新分发代理与重新分发客户端之间的唯一信任链。

1. 在重新分发代理防火墙上，为防火墙创建一个用于传入连接的自定义 SSL/TLS 服务配置文件。
2. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Secure Communication Settings**（安全通信设置）。
3. **Edit**（编辑）设置。
4. 选择 **Customize Secure Server Communication**（自定义安全服务器通信）选项。
5. 选择在步骤 1 中创建的 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
6. 单击 **OK**（确定）。
7. **Commit**（提交）更改。
8. 输入以下 CLI 命令以确认证书配置文件（`SSL` 配置）是否使用 自定义证书：**`show redistribution service status`**。

STEP 10 | 验证代理是否正确将数据重新分发给客户端。

1. 查看代理统计信息（**Device**（设备）> **Data Redistribution**（数据重新分发）> **Agents**（代理）），然后选择 **Status**（状态）以查看重新分发代理的活动摘要，例如客户端防火墙已收到的映射数。
2. 确认 **Connected**（已连接）状态为 **yes**（是）。
3. 在代理上，访问 CLI，并输入以下 CLI 命令以检查重新分发状态：**`show redistribution service status`**。
4. 在代理上，输入以下 CLI 命令以查看重新分发客户端：**`show redistribution service client all`**。
5. 在客户端上，输入以下 CLI 命令以检查重新分发状态：**`show redistribution service client all`**。
6. 确认 User-ID 日志中的 **Source Name**（源名称）（**Monitor**（监控）> **Logs**（日志）> **User-ID**），以验证防火墙是否能从重新分发代理接收映射。
7. 在客户端上，查看 IP 标记日志（**Monitor**（监控）> **Logs**（日志）> **IP-Tag**（**IP** 标记））以确认客户端防火墙可以接收数据。
8. 在客户端上，输入以下 CLI 命令，并检验防火墙接收映射的源是否为 `REDIST`：**`show user ip-user-mapping all`**。

STEP 11 | （可选）要对数据重新分发执行故障排除，请启用 traceroute 选项。



© 2019 Palo Alto Networks, Inc.

一旦启用 traceroute 选项，接收数据的防火墙会将其 IP 地址附加到 <route> 字段，该字段是一个已对数据进行遍历的所有防火墙 IP 地址列表。此选项要求重新分发路由中的所有 PAN-OS 设备均使用 PAN-OS 10.0 版。如果重新分发路由中使用的 PAN-OS 设备是 PAN-OS 9.1 或更早版本，则 traceroute 信息将在该设备处终止。

1. 在提供了源的重新分发代理上，输入以下 CLI 命令：**debug user-id test cp-login traceroute yes ip-address *<ip-address>* user *<username>*** ( 其中，***<ip-address>*** 是您要验证的 IP 地址到用户名映射的 IP 地址，***<username>***是您要验证的 IP 地址到用户名映射的用户名 ) 。
2. 在配置 traceroute 的防火墙客户端上，通过输入以下 CLI 命令确认防火墙是否重新分发数据：**show user ip-user-mapping all**。

   防火墙将显示映射创建的时间戳 ( SeqNumber ) 以及用户是否具有 GlobalProtect ( GP 用户 ) 。

```
admin > show user ip-user-mapping-mp ip 192.0.2.0

IP address:  192.0.2.0 (vsys1)
User:    jimdoe
From:   REDIST
Timeout:  889s
Created:  11s ago
Origin:   198.51.100.0
SeqNumber:  15895329682-67831262
GP User:  No
Local HIP:  No
Route Node 0: 198.51.100.0 (vsys1)
Route Node 1: 198.51.100.1 (vsys1)
```

# 共享跨虚拟系统的 User-ID 映射

当您有多个虚拟系统而想要简化 User-ID™ 源配置时，您可以在单个虚拟系统上配置 User-ID 源，以与防火墙上的所有其他虚拟系统共享 IP 地址到用户名映射。

将单个虚拟系统配置为 *User-ID* 中心，可通过消除在多个虚拟系统上配置源的需要，从而简化用户映射，尤其是当用户流量通过多个虚拟系统 ( 该系统基于用户尝试访问的资源 ) 时 ( 例如，在学术网络环境中，学生尝试访问不同系别，而该系别由不同的虚拟系统管理 ) 。

要映射用户，防火墙使用本地虚拟系统上的映射表，并为该用户应用策略。如果防火墙在用户流量流出的虚拟系统上未找到用户映射，该防火墙将查询中心以获得该用户的 IP 地址到用户名信息。如果防火墙定位了 User-ID 中心和本地虚拟系统上的映射，防火墙使用其在本地学习的映射。

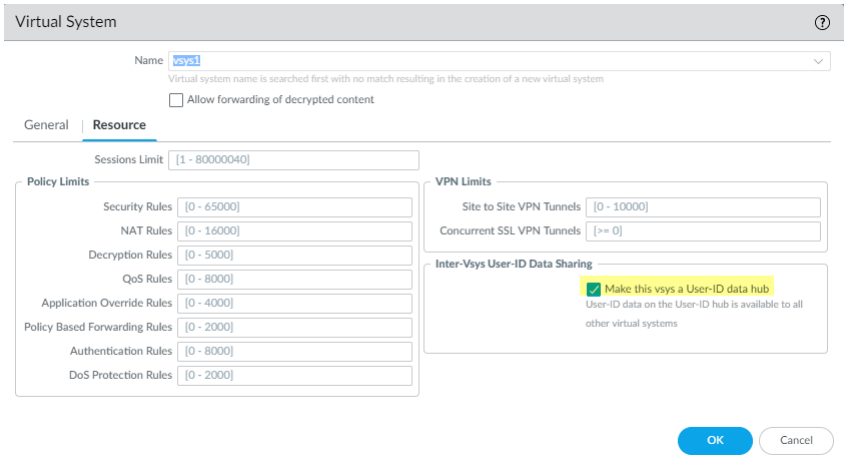
在您配置了 User-ID 中心后，当虚拟系统需要识别用户以进行基于用户的策略实施，或在日志或报告中显示用户名但源在本地不可用时，虚拟系统可以使用 User-ID 中心上的映射表。当您选择中心时，防火墙在其他虚拟系统上保留映射，因此我们建议在中心上整合 User-ID 源。但是，如果您不想要从某个特定源共享映射，您可以配置单个虚拟系统执行用户映射。

STEP 1 | 将虚拟系统作为 User-ID 中心分配。

1. 选择 **Device** ( 设备 ) > **Virtual Systems** ( 虚拟系统 ) ，然后选择您整合了您的 User-ID 源的虚拟系统。
2. 在 **Resource** ( 资源 ) 选项卡上，**Make this vsys a User-ID data hub** ( 将此 **vsys** 设为 **User-ID** 数据中心 ) ，单击 **Yes** ( 是 ) 以确认。然后单击 **OK** ( 确定 ) 。



© 2019 Palo Alto Networks, Inc.




STEP 2 | 整合您的 User-ID 源并迁移至您希望作为 User-ID 中心使用的虚拟系统。

此步骤将整合 User-ID 配置以实现操作的简化。通过配置中心至监控器服务器，并连接至之前由其他虚拟系统监控的代理，中心将收集用户映射信息，而不是让每个虚拟系统独立进行收集。如果您不想共享来自特定虚拟系统的映射，在未被用作中心的虚拟系统上配置此类映射。

1. 移除任何不必要或过期的源。
2. 通过 XML API 标识用于您的 基于 Windows 的或集成代理以及发送用户映射的源的所有配置，并将这些配置复制到您想要用作 User-ID 中心的虚拟系统。

   在中心上，您可以配置任何当前在虚拟系统上配置的任何 *User-ID* 源。然而，来自终端服务器代理和组映射的 *IP* 地址和端口到用户名映射信息不会在 *User-ID* 中心和连接的虚拟系统之间共享。
3. 指定 User-ID 应包括在映射中的子网或 User-ID 应从映射中排除的子网。
4. 定义 **Ignore User List**（忽略用户列表）。
5. 在所有其他虚拟系统上，移除 User-ID 中心上的任何源。

STEP 3 | **Commit**（提交）更改以启用 User-ID 中心，并开始为整合的源收集映射。

STEP 4 | 确认 User-ID 中心正在映射用户。

1. 使用 **`show user ip-user-mapping all`** 命令显示 IP 地址到用户名映射，以及哪个虚拟系统提供该等映射。
2. 使用 **`show user user-id-agent statistics`** 命令以限制哪个虚拟系统正在作为 User-ID 中心使用。


© 2019 Palo Alto Networks, Inc.

# App-ID

要在网络中安全启用应用程序，Palo Alto Networks 下一代防火墙可同时提供应用程序和 Web 透视图，即 App-ID 和 URL 筛选，从而防止出现各种法律、法规、工作效率和资源利用率风险。

App-ID 能够让您深入了解网络上的应用程序，以便掌握它们的工作原理、行为特征及其相对风险。这些应用程序知识可让您创建和强制执行安全策略规则，以启用、检查和设计所需的应用程序，以及阻止不需要的应用程序。当您定义策略规则以允许流量时，App-ID 开始对流量进行分类，而无需使用任何其他配置。

新建和修改过的 App-ID 作为应用程序和威胁内容更新的组成部分进行发布——遵循应用程序和威胁内容更新的最佳实践，以实现应用程序和威胁签名的无缝最新。


> App-ID 概述
> 简化 App-ID 策略规则
> 应用程序 ID 和 HTTP/2 检查
> 管理自定义应用程序或未知应用程序
> 管理新建和修改过的 App-ID
> 在策略中使用应用程序对象
> 在默认端口上安全启用应用程序
> 应用程序与隐式支持
> 安全策略规则优化
> 应用层网关
> 禁用 SIP 应用层网关 (ALG)
> 使用 HTTP 标头管理 SaaS 应用程序访问
> 保留遗留应用程序的自定义超时

# App-ID 概述

App-ID 是一个已获专利的流量分类系统，仅在 Palo Alto Networks 防火墙中提供，用于确定应用程序的内容，而不考虑应用程序所使用的端口、协议、加密（SSH 或 SSL）或任何其他规避策略。它采用多种分类机制对您的网络流量流进行应用程序签名、应用程序协议解码和启发以准确识别应用程序。

以下是 App-ID 识别遍历网络的应用程序的方式：

- 根据安全策略匹配流量以检查在网络中是否允许它。
- 然后，对允许的流量应用签名，以根据独特的应用程序属性和相关的事务特征识别应用程序。此外，签名也可用来确定应用程序是使用其默认端口还是使用非标准端口。如果安全策略允许流量，则会对流量进行扫描和进一步分析，以便更详细地识别应用程序。
- 如果 App-ID 确定正在使用加密（SSL 或 SSH）并且正确部署了解密策略规则，则会对会话进行解密并在解密流程中再次应用应用程序签名。
- 然后，使用协议已知的解码器来应用其他基于上下文的签名，检测可能为协议内隧道的其他应用程序（如通过 HTTP 使用的 Yahoo!Instant Messenger）。此外，还可以使用解码器来验证流量是否符合协议规范，并为应用程序的 NAT 遍历和开放式动态针孔提供支持，如 SIP 和 FTP。
- 对于特别规避和通过高级签名和协议分析无法识别的应用程序，可以使用启发或行为分析来确定应用程序的身份。

在识别应用程序后，可以使用安全策略检查确定处理应用程序的方式，如阻止或允许和扫描威胁，以及使用 QoS 检查是否有未经授权的文件传输和数据模式或形状。



© 2019 Palo Alto Networks, Inc.

# 简化 App-ID 策略规则

使用单个策略规则安全启用具有共同属性的广泛应用程序集（例如，为您的用户提供访问基于 Web 的应用程序或安全启用所有企业 VoIP 应用程序的广泛权限）。Palo Alto Networks 负责研究具有共同属性的应用程序，并通过动态内容更新中的标记传输这些信息。这会：

- 减少错误，节省时间。
- 帮助您创建可自动更新的策略，以处理新发布的应用程序。
- 帮助您通过策略优化器简化向基于 App-ID 的规则集的转换。

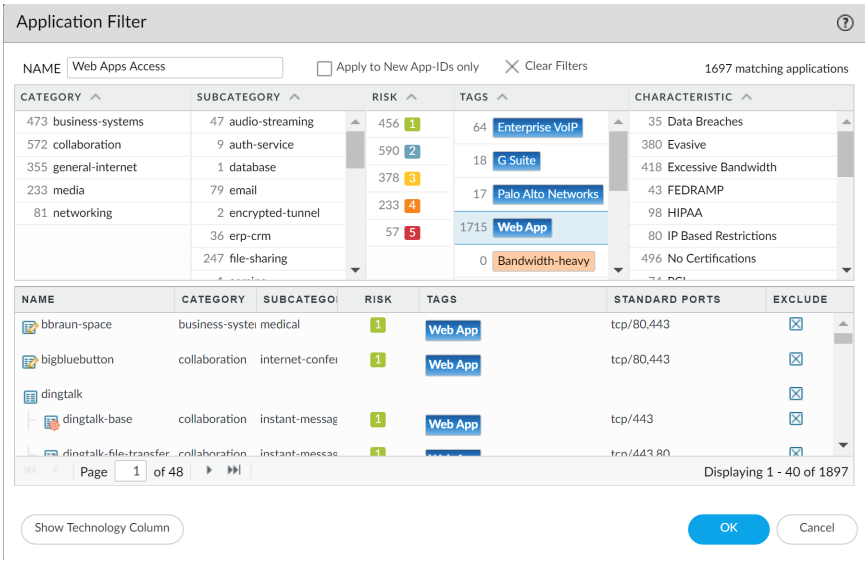
然后，防火墙可以使用基于标记的应用程序筛选器自动实施新的和更新过的 App-ID，无需您在添加新应用程序时查看或更新策略规则。如果选择将应用程序从特定标记中排除，则新的内容更新将遵循这些排除。您还可以使用自己的标记，根据策略要求定义应用程序类型。

- 使用标签创建应用程序筛选器
- 创建基于自定义标签的应用程序过滤器

## 使用标签创建应用程序筛选器

STEP 1 | 使用一个或多个标签创建应用程序筛选器。

如果选择多个标签，应用程序必须与待包含在筛选器中的两个标签均匹配。




STEP 2 | 创建安全策略规则，在 **Application**（应用程序）选项卡上 **Add**（添加）新的应用程序筛选器。

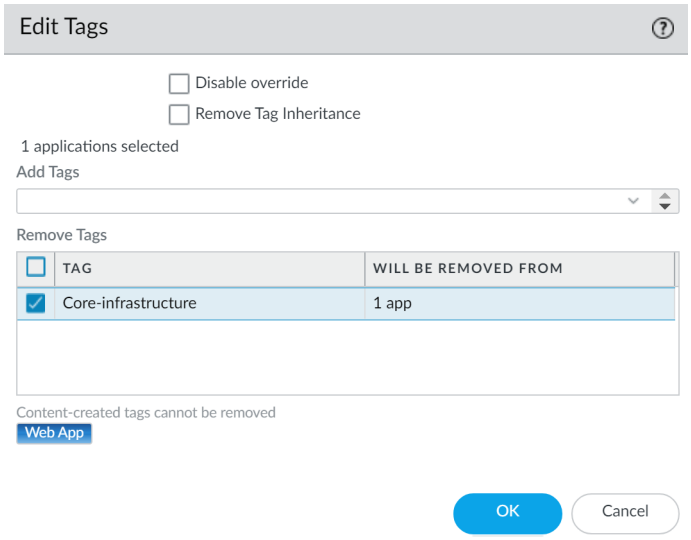
STEP 3 | **Commit**（提交）更改。

## 创建基于自定义标签的应用程序过滤器

STEP 1 | 创建自定义标签 并应用至 App-ID。

1. （可选）删除应用程序标签。
2. 筛选或搜索应用程序，然后选择具体的应用程序，以删除标签。
3. 编辑标签，然后选择要删除的标签。

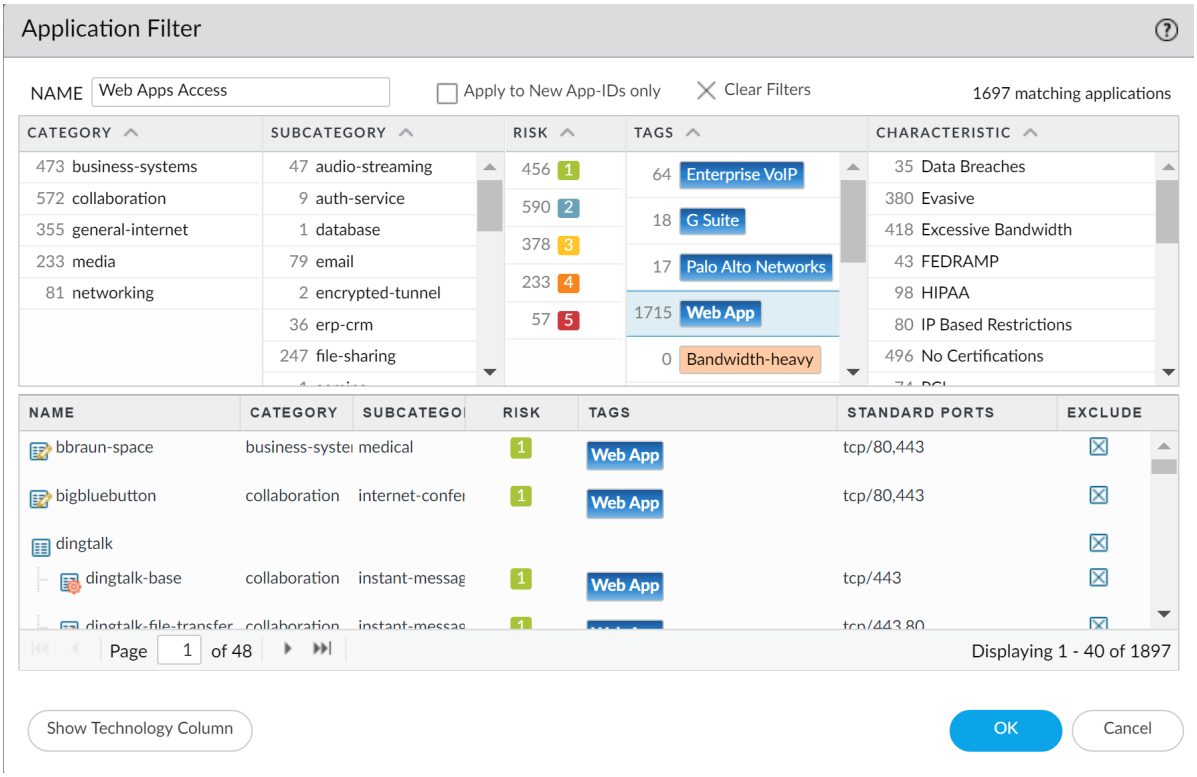

© 2019 Palo Alto Networks, Inc.




4. 单击 **OK**（确定）。

STEP 2 | 使用一个或多个标签创建应用程序筛选器。

如果选择多个标签，应用程序必须与待包含在筛选器中的两个标签均匹配。




STEP 3 | 创建安全策略规则，在 **Application**（应用程序）选项卡上 **Add**（添加）新的应用程序筛选器。

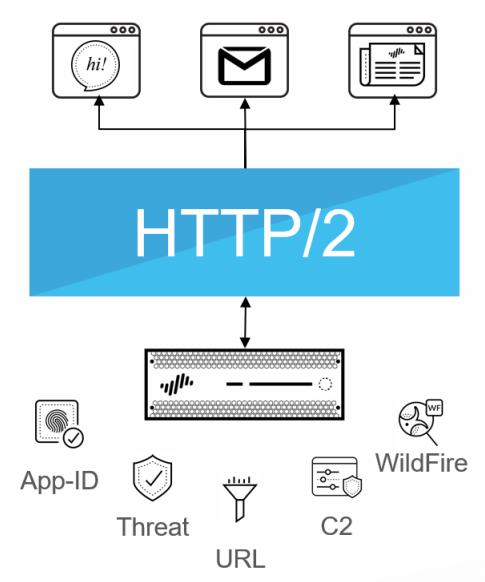
STEP 4 | **Commit**（提交）更改。



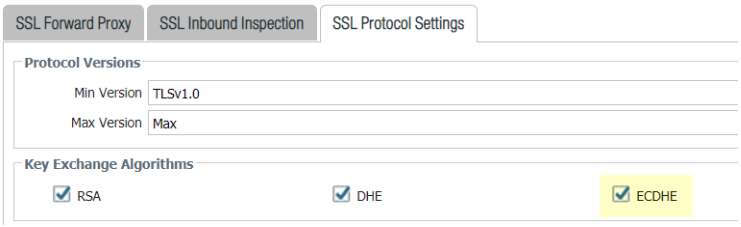
© 2019 Palo Alto Networks, Inc.

# 应用程序 ID 和 HTTP/2 检查

您现在可以在 HTTP/2 上安全启用应用程序，而无需在防火墙上进行任何额外配置。随着更多的网站继续采用 HTTP/2，防火墙可以逐个流地实施安全策略和所有威胁检测和防护功能。对 HTTP/2 流量的观察让您可以保证在 HTTP/2 上提供服务的 Web 服务器的安全，并让您的用户从 HTTP/2 提供的速度和资源效率增益中获益。




当 SSL 解密启用时，防火墙默认处理并检查 HTTP/2 流量。为了让 HTTP/2 检查正常运行，必须启用防火墙以使用 ECDHE（椭圆曲线 Diffie-Hellman）作为 SSL 会话的密钥交换算法。ECDHE 默认为启用，但您可以通过选择 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（SSL 解密）> **SSL Protocol Settings**（SSL 协议设置）确认其是否已启用。



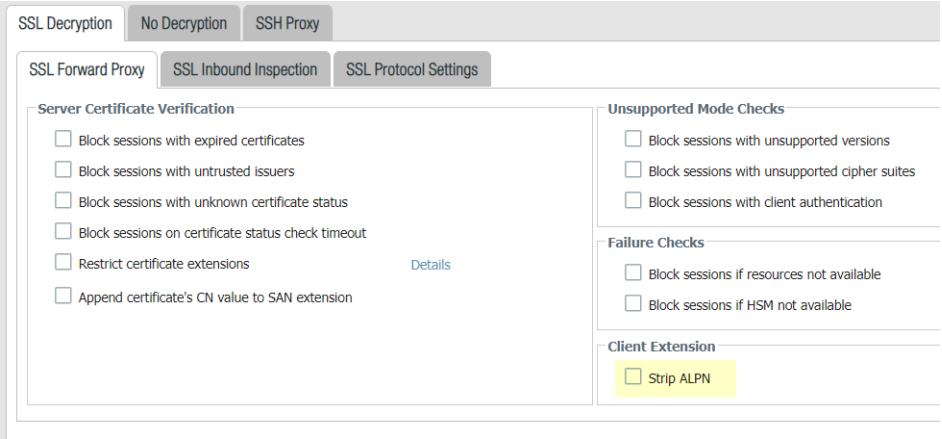

一旦启用 *PAN-OS 10.0* 中引入的解密日志，就必须启用 隧道内容检测以获取 *HTTP/2* 流量的 *App-ID*。

您可以为目标流量或全局禁用 HTTP/2 检查：

- 为目标流量禁用 HTTP/2 检查。

  您需要指定防火墙以删除应用层协议协商 (ALPN) TLS 扩展中包含的任何值。ALPN 用于确保 HTTP/2 连接安全，因此，当没有为该 TLS 扩展指定值时，防火墙会将 HTTP/2 流量降级为 HTTP/1.1，或将其分类为未知 TCP 流量。


© 2019 Palo Alto Networks, Inc.




1. 选择 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 转发代理），然后选择 **Strip ALPN**（删除 **ALPN**）。
2. 将解密配置文件附加到解密策略（**Policies**（策略）> **Decryption**（解密））以关闭与策略匹配的流量的 HTTP/2 检查。
3. **Commit**（提交）更改。

- 全局禁用 HTTP/2 检查。

  使用 CLI 命令：`set deviceconfig setting http2 enable no` 并 **Commit**（提交）您的更改。防火墙将把 HTTP/2 流量分类为未知 TCP 流量。



© 2019 Palo Alto Networks, Inc.

# 管理自定义应用程序或未知应用程序

Palo Alto Networks 可以每周提供用于识别新 App-ID 签名的应用程序更新。默认情况下，在防火墙上始终启用 App-ID，且无需启用一系列签名识别众所周知的应用程序。通常，在 ACC 和流量日志中仅被分类为未知流量（tcp、udp 或 non-syn-tcp）的应用程序都是尚未添加到 App-ID 的商用应用程序，网络上的内部或定制应用程序，或存在潜在威胁的应用程序。

有时，防火墙可能会因以下原因将应用程序报告为未知应用程序：

- 数据不完整 — 握手已发生，但在超时之前没有发送数据包。
- 数据不允许 — 握手已发生，后跟一个或多个数据包；但是，没有交换足够数据包来识别应用程序。

可以使用下列选项来处理未知应用程序：

- 创建安全策略，从而通过未知 TCP、未知 UDP 或通过由源区域、目标区域和 IP 地址的组合来控制未知应用程序。
- 从 Palo Alto Networks 索取 App-ID — 如果想要检查和控制遍历网络的应用程序，对于任何未知流量，都可以记录数据包捕获。如果数据包捕获表明应用程序是商业应用程序，则可以将此数据包捕获提交给 Palo Alto Networks 用于开发 App-ID。如果应用程序是内部应用程序，则可以创建自定义 App-ID 和/或定义应用程序覆盖策略。
- 创建定制应用程序使用签名并将它附加到安全策略，或者创建自定义应用程序和定义应用程序覆盖策略。自定义应用程序可让您定制内部应用程序的定义 — 其特征、类别和子类别、风险、端口、超时 — 以及实施粒度策略控制，以最大限度减少网络上无法识别的流量范围。此外，创建自定义应用程序还可让您正确识别 **ACC** 和流量日志中的应用程序，并用于审核/报告网络中的应用程序。对于定制应用程序，您可以指定签名和模式来唯一识别应用程序，并将它附加到安全策略以允许或拒绝应用程序。

  或者，如果您想防火墙使用快速路径（第四层检查，而不是使用 App-ID 的第七层检查）处理定制应用程序，可以在应用程序覆盖策略规则中引用定制应用程序。包含定制应用程序的应用程序覆盖可阻止 App-ID 引擎（即第七层检查）处理会话。相反，它会强制防火墙作为常规状态检查防火墙在第四层处理会话，从而节省应用程序处理时间。

  例如，如果您在主机标头 *www.mywebsite.com* 上创建用于触发器的定制应用程序，并且将数据包首先识别为 *Web* 浏览，然后匹配作为定制应用程序（其父应用程序为 Web 浏览）。由于父应用程序为 Web 浏览，因此在第七层对定制应用程序进行检查，并扫描内容和漏洞。

  如果定义应用程序覆盖，防火墙会在第四层停止处理。将定制应用程序名称分配给会话有助于识别流量日志中的应用程序，而不会扫描流量的威胁。



© 2019 Palo Alto Networks, Inc.

# 管理新建和修改过的 App-ID

新建和修改过的 App-ID 作为应用程序和威胁内容更新的组成部分向防火墙提供。当新建和修改过的 App-ID 使防火墙能够以越来越高地精度执行您的安全策略时，安装内容更新发布时发生的安全策略更改可能会影响应用程序的可用性。为此，您需要思考应如何实现内容更新的最佳部署，以便您能获取可用的最新威胁预防，同时调整您的安全策略，以更好地利用新建和修改过的 App-ID。

以下选项使您可以评估新 App-ID 对现有策略实施的影响，禁用（和启用）App-ID，以及无缝更新策略规则以保护和实施新识别的应用程序：

- 最佳工作流程包含新的和修改过的 App-ID
- 请参阅内容发布中新建和修改过的 App-ID
- 请参阅新的和修改过的 App-ID 如何影响您的安全策略
- 确保允许新的关键 App-ID
- 监控新的 App-ID
- 禁用或启用 App-ID

您还可以利用 简化 App-ID 策略规则 来使用内容更新中提供的应用程序标记。

## 最佳工作流程包含新的和修改过的 App-ID

请参阅此主要工作流程以首先设置“应用程序和威胁”内容更新，然后将新建和修改过的 App-ID 以最佳方式插入到您的安全策略中。此处列出了部署内容更新所需的一切信息参考。

STEP 1 | 您的业务需求应与部署“应用程序和威胁”内容更新的方法保持一致。

了解应用程序和威胁内容更新的工作方式，然后将您的组织标识为任务关键型或安全第一型。知道对您业务最为关键的点将有助于您确定如何部署内容更新，并使用最佳实践以满足您的业务需求。您可能会发现，您也许需要混合使用这两种方法，具体根据防火墙部署（数据中心或周边）或办公地点（远程或总部）而定。

STEP 2 | 根据您组织的网路安全和应用程序可用性要求，请查看并应用应用程序和威胁内容更新的最佳实践。

STEP 3 | 配置安全策略规则为始终允许可能会产生全网范围内影响的新建 App-ID，例如，身份验证或软件开发应用程序。

新建 App-ID 特性只能与最新内容发布中引入的 App-ID 相匹配。在安全策略中使用时，您可以有一个月的时间根据新建 App-ID 来对您的安全策略进行微调，同时确保划入关键类别的 App-ID 的持续可用性（确保允许新的关键 App-ID）。

STEP 4 | 设置部署应用程序和威胁内容更新时间表；这包括延迟新建 App-ID 安装，直至您有时间进行必要的安全策略更新的选项（使用 **New App-ID Threshold**（新建 **App-ID** 阈值））。

STEP 5 | 内容更新安装计划设置完毕后，需要定期检入，并请参阅内容发布中新建和修改过的 App-ID。

STEP 6 | 随后，请参阅新的和修改过的 App-ID 如何影响您的安全策略，并按需对您的安全策略做出调整。

STEP 7 | 监控新的 App-ID，查看网络上新建 App-ID 的活动，以便您做好准备进行最有效的安全策略更新。



© 2019 Palo Alto Networks, Inc.

# 请参阅内容发布中新建和修改过的 App-ID

对于已下载和已安装的内容更新，您可以查看更新中所包含的新建和修改过的 App-ID 列表。已提供完整的应用程序详细信息，重要的是，已突出显示具有全网影响（LDAP 或 IKE 等）且推荐用于策略审核的应用程序更新。对于修改过的 App-ID，应用程序详细信息还会描述覆盖范围现在会如何扩展或如何变得更精细。

STEP 1 | 选择 **Device**（设备）> **Dynamic Updates**（动态更新），然后选择 **Check Now**（立即检查）以刷新可用内容更新的列表。

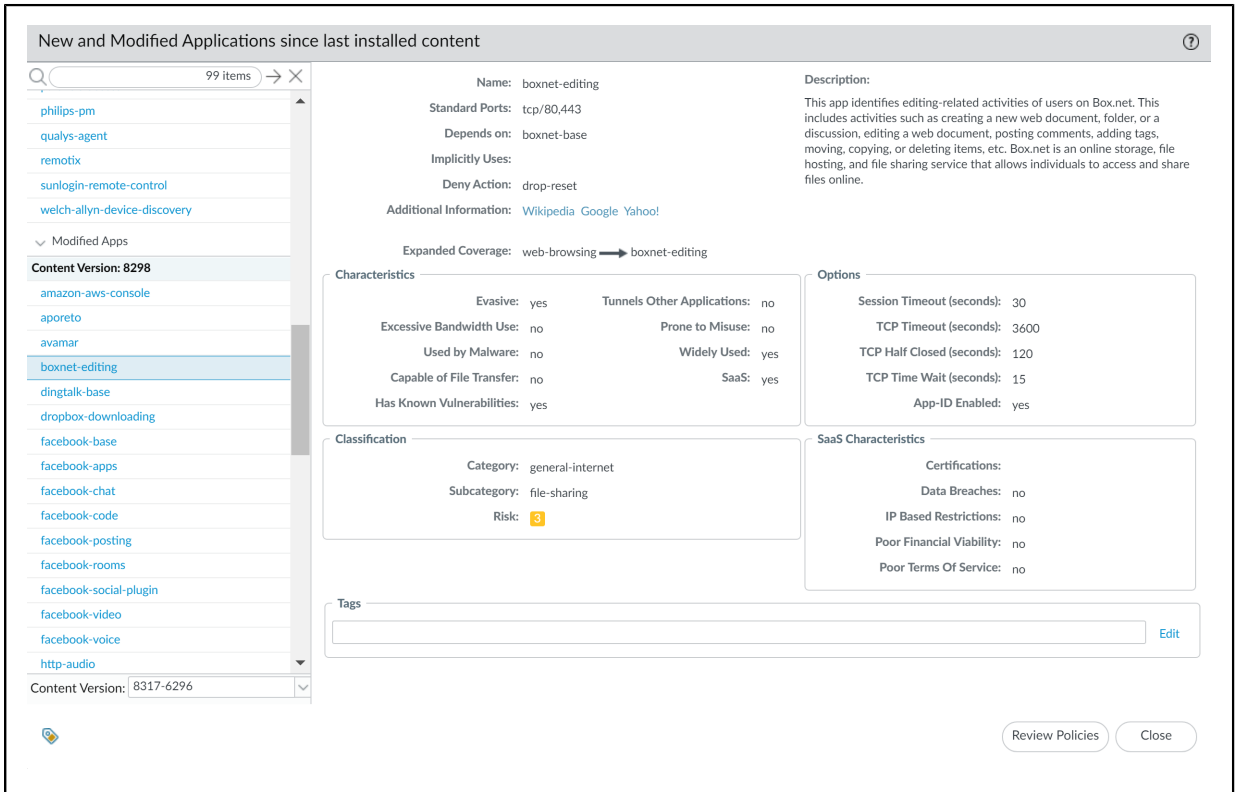
STEP 2 | 对于已下载或当前已安装的内容发布，单击 **Actions**（操作）列中的 **Review Apps**（查看应用程序）链接，以查看此发布中新标识和修改过的应用程序的详细信息：

Applications and Threats  **Last checked:** 2020/09/23 01:02:02 PDT  **Schedule:** Every Wednesday at 01:02 (Download only)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8292-6181 | panupv2-all-apps-8292-6181 | Apps | Full | 47 MB | | 2020/07/13 11:46:39 PDT | ✓ previously | | Revert | Release Notes |
| 8317-6296 | panupv2-all-apps-8317-6296 | Apps | Full | 48 MB | | 2020/09/08 17:55:10 PDT | | ✓ | Review Policies Review Apps | Release Notes |
| 8320-6309 | panupv2-all-contents-8320-6309 | Apps, Threats | Full | 56 MB | 192cfd8c2ff0058c188d0... | 2020/09/14 18:13:54 PDT | | | Download | Release Notes |
| 8320-6310 | panupv2-all-contents-8320-6310 | Apps, Threats | Full | 57 MB | 2436f79a8f02aeef37b82... | 2020/09/15 10:19:15 PDT | | | Download | Release Notes |
| 8321-6311 | panupv2-all-contents-8321-6311 | Apps, Threats | Full | 56 MB | d3ac74a854c08527869cf... | 2020/09/15 13:44:29 PDT | | | Download | Release Notes |
| 8321-6312 | panupv2-all-contents-8321-6312 | Apps, Threats | Full | 57 MB | a4275ee394b5d942c09e... | 2020/09/15 14:26:20 PDT | | | Download | Release Notes |

STEP 3 | 查看自上一个内容版本以来，此内容发布引入或修改过的 App-ID。

新建和修改过的 App-ID 应单独列出。已为每个应用程序提供完整的详细信息，并突出显示 Palo Alto Networks 预示其具有全网影响且推荐用于策略审核的 App-ID。




可用来评估对策略实施可能产生影响的新建 App-ID 详细信息包括：

- **Depends on**（依赖于）— 列出此 App-ID 唯一标识应用程序时所依赖的应用程序签名。如果 **Depends On**（依赖于）字段中列出的某个应用程序签名被禁用，那么还将禁用从属 App-ID。
- **Previously Identified As**（先前标识为）— 列出与新 App-ID 安装前用于唯一标识应用程序的应用程序相匹配的 App-ID。



© 2019 Palo Alto Networks, Inc.

- **App-ID Enabled**（启用 **App-ID** 功能）— 在下载内容发布后，所有 App-ID 显示为已启用，除非您在安装内容更新之前选择手动禁用 App-ID 签名。

对于修改过的 App-ID，详细信息包含如下信息：**Expanded Coverage**（扩展覆盖范围）、**Remove False Positive**（删除误报）、以及应用程序元数据更改。扩展覆盖范围和删除误报字段均指出应用程序覆盖范围是如何发生更改（范围更广或更窄），时钟图标则表示元数据的更改，其中已对某些应用程序详细信息进行更新。

STEP 4 | 根据您的发现，单击 **Review Policies**（审核策略）以查看新建和修改过的 App-ID 如何影响安全策略实施：请参阅新的和修改过的 App-ID 如何影响您的安全策略。

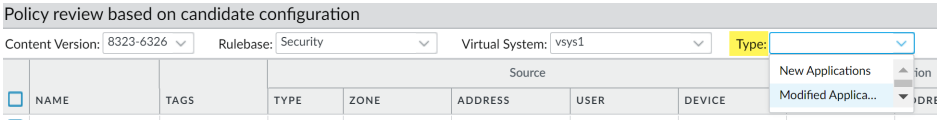
## 请参阅新的和修改过的 App-ID 如何影响您的安全策略

新分类和修改过的 App-ID 可能会更改防火墙实施流量的方式。执行内容更新策略审核，查看新的修改过的 App-ID 如何影响您的安全策略，并轻松进行必要的调整。您可以对已下载且安装完毕的内容执行内容更新策略审核。

STEP 1 | 选择 **Device**（设备）> **Dynamic Updates**（动态更新）。

STEP 2 | 要了解更多内容发布中引入或修改的每个 App-ID，请参阅内容发布中新建和修改过的 App-ID。

STEP 3 | 对于已下载或当前安装完毕的内容发布，请单击操作列中的 **Review Policies**（审核策略）。**Policy review based on candidate configuration**（基于待选配置的策略审核）对话框可用于按照 **Content Version**（内容版本）进行筛选，并可查看某个特定版本中引入的新建或修改过的 App-ID（还可以根据 **Rulebase**（规则库）、**Virtual System**（虚拟系统）和 **Application**（应用程序）来筛选新建 App-ID 的策略影响）。




STEP 4 | 从 **Application**（应用程序）下拉菜单中选择一个 App-ID 以查看当前对应用程序实施的策略规则。显示的规则是基于新 App-ID 安装前与应用程序匹配的 App-ID（查看应用程序详细信息以查看某个应用程序在新 App-ID 之前 **Previously Identified As**（先前标识为）应用程序签名的列表）。

STEP 5 | 使用策略查看中提供的详细信息来计划策略规则更新，以便在安装 App-ID 时生效，或是如果当前已安装包含 App-ID 的内容发布版本，则您做出的更改将立即生效。

您可以 **Add app to selected policies**（添加应用程序至选中策略）或 **Remove app from selected policies**（从选中策略中删除应用程序）。

## 确保允许新的关键 App-ID

新的 App-ID 可能会导致新标识为属于某个应用程序的流量策略实施发生更改。要降低对安全策略实施的影响，您可以在安全策略规则中使用 **New App-ID**（新 **App-ID**）特性，以便规则始终实施最新引进的 App-ID，不会要求您在安装新的 App-ID 时配置更改。新 App-ID 特性应始终只能与最新安装的内容发布中的新 App-ID 相匹配。安装新的内容发布时，新的 App-ID 特性将自动开始只与该内容发布版本中的新 App-ID 匹配。

您可以选择实施所有新的 App-ID，或是指定安全策略规则以实施某些可能会对全网产生影响，或是会产生关键影响的新 App-ID 类型（例如，仅实施身份验证或软件开发应用程序）。将安全策略规则设置为


© 2019 Palo Alto Networks, Inc.

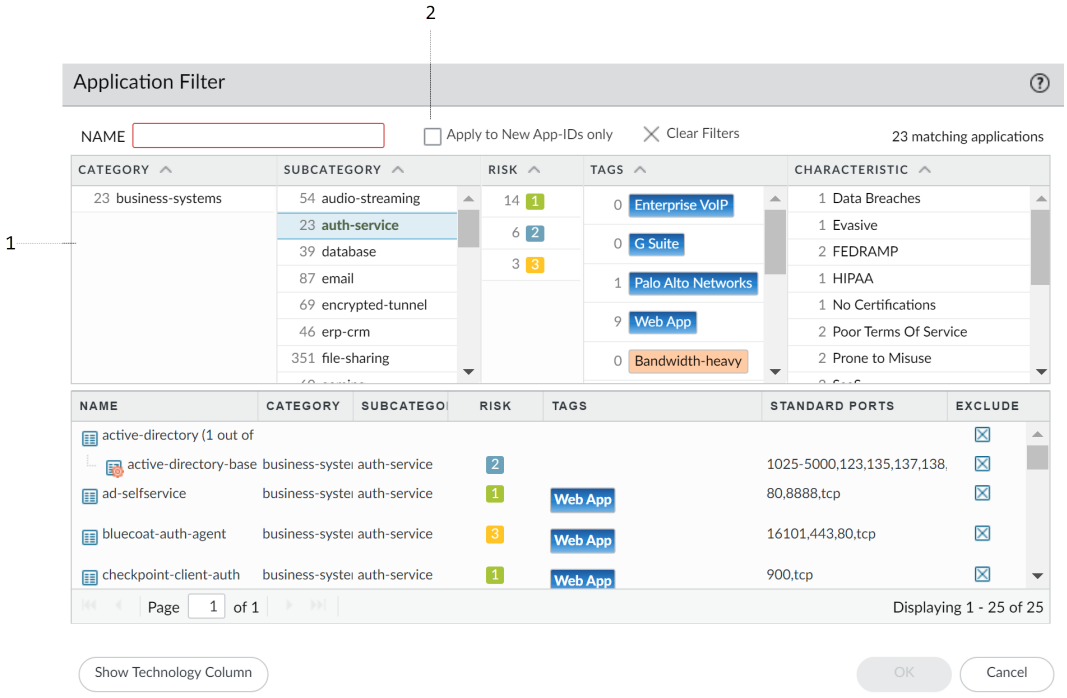
**Allow**（允许），确保即使是 App-ID 发布为关键应用程序引入已扩展或更精确的覆盖，防火墙也会继续允许这些操作。

新 App-ID 每月发布一次，因此，允许最新 App-ID 的策略规则为您提供一个月的时间（或是，如果防火墙未按计划安装内容更新，直至下次您手动安装更新）来对新分类应用程序可能会对安全策略实施产生的影响进行评估，并进行必要的调整。

STEP 1 | 选择 **Object**（对象）> **Application Filters**（应用程序筛选器）并 **Add**（添加）新的应用程序筛选器。

STEP 2 | 根据子类别或特征定义想要确保其持续可用性的新应用程序类型。例如，选择 “auth-service”，确保任何新安装的已知可执行或支持身份验证的应用程序获得许可。

STEP 3 | 只有在缩小想要安装时立即允许的新应用程序类型范围后，才能选择 **Apply to New App-IDs only**（仅应用于新 **App-ID**）。




STEP 4 | 选择 **Policies**（策略）> **Security**（安全），然后添加或编辑配置以允许匹配流量的安全策略规则。

STEP 5 | 选择 **Application**（应用程序），然后添加新的 **Application Filter**（应用程序筛选器）至策略规则中作为匹配条件。

STEP 6 | 单击 **OK**（确定）和 **Commit**（提交），保存您的更改。

STEP 7 | 要继续调整安全策略以考虑新 App-ID 引入的任何实施更改：

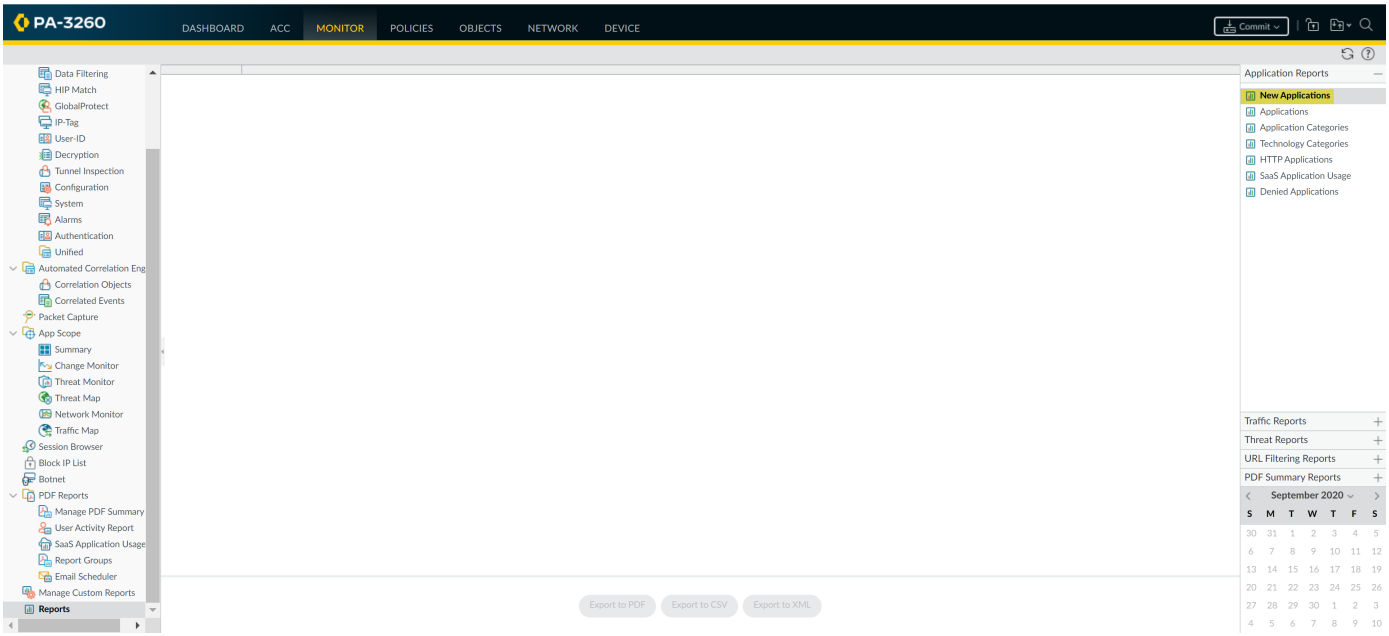
- 监控新的 App-ID — 监控并获取新 App-ID 活动有关的报告。
- 请参阅内容发布中新建和修改过的 App-ID — 请参阅新安装 App-ID 是如何影响现有安全策略规则。


© 2019 Palo Alto Networks, Inc.

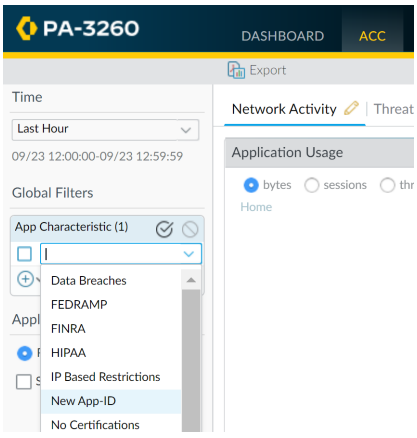
# 监控新的 App-ID

**New App-ID**（新建 **App-ID**）特性使您能够监控网络上的新应用程序，以便更好地对可能想要执行的安全策略更新进行评估。使用 ACC 上新建 App-ID 特性，查看网络上的新应用程序，生成对新分类应用程序活动进行详细说明的报告。a您所掌握的内容将有助于您做出有关如何更新您的安全策略以实施最新分类的 App-ID 的正确决策。无论您是在 ACC 上使用 App-ID，或是使用 App-ID 生成报告（或是确保允许新的关键 App-ID），新建 App-ID 特性将始终仅与最新安装的内容发布中的新建 App-ID 匹配。安装新的内容发布时，新的 App-ID 特性将自动开始只与该内容发布版本中的新 App-ID 匹配。

- 生成一份专门针对新应用程序进行详细说明的报告（仅在最新内容发布中引入应用程序）。




- 使用 ACC 监控新应用程序的活动：选择 **ACC**，并在 **Global Filters**（全局筛选器）中选择 **Application**（应用程序）> **Application Characteristics**（应用程序特性）> **New App-ID**（新建 **App-ID**）。




# 禁用或启用 App-ID

如果要立即从最新威胁防护中受益，且计划稍后启用 App-ID，则可以禁用内容发布中引入的所有 App-ID，然后，您可以禁用特定应用程序的 App-ID。



© 2019 Palo Alto Networks, Inc.

引用了 App-ID 的策略规则仅根据已启用的 App-ID 来匹配和实施流量。

某些 App-ID 无法禁用，并且仅允许启用状态。无法禁用的 App-ID 包括其他 App-ID（如 unknown-tcp）隐式使用的应用程序签名。禁用基础 App-ID 可能会导致依赖于基础 App-ID 的 App-ID 也被禁用。例如，禁用 facebook-base 将禁用所有其他 Facebook App-ID。

- 禁用某个内容发布中的所有 App-ID 或者为计划的内容更新禁用所有 App-ID。

  虽然此选项可让您稍后有机会启用 App-ID 以保护您免受威胁，但 Palo Alto Networks 建议您不要定期禁用 App-ID，而应该配置安全策略规则以暂时允许新建 App-ID。此规则将始终允许仅在最新内容发布中引入新建 App-ID。因为包含新建 App-ID 的内容更新每月只发布一次，因此您就有时间评估新建 App-ID，并根据需要调整安全策略以涵盖新建 App-ID，同时确保关键应用程序的可用性不会受到影响。

  - 要禁用某个内容发布中引入的所有新 App-ID，请选择 **Device**（设备）> **Dynamic Updates**（动态更新）并 **Install**（安装）应用程序和威胁内容发布。系统提示时，选择 **Disable new apps in content update**（在内容更新中禁用新应用程序）。选中该复选框以禁用应用程序并继续安装内容更新。
  - 在 **Device**（设备）> **Dynamic Updates**（动态更新）页面上，选择 **Schedule**（计划）。选择 **Disable new apps in content update**（在内容更新中禁用新应用程序）以下载和安装内容发布。

- 对一个或多个应用程序一次性禁用 App-ID。

  - 要快速禁用单个应用程序或者同时禁用多个应用程序，请单击 **Objects**（对象）> **Applications**（应用程序）。选中一个或多个应用程序的复选框，然后单击 **Disable**（禁用）。
  - 要查看单个应用程序的详细信息并随后禁用该应用程序的 App-ID，请选择 **Objects**（对象）> **Applications**（应用程序）并 **Disable App-ID**（禁用 **App-ID**）。可以使用此步骤来禁用挂起的 App-ID（表示包含 App-ID 的内容发布已下载到防火墙但没有安装）或安装的 App-ID。

- 启用 App-ID。

  通过选择 **Objects**（对象）> **Applications**（应用程序）来启用先前禁用的 App-ID。选中一个或多个应用程序的复选框，然后单击 **Enable**（启用）或打开特定应用程序的详细信息，然后单击 **Enable App-ID**（启用 **App-ID**）。


© 2019 Palo Alto Networks, Inc.

# 在策略中使用应用程序对象

使用应用程序对象定义安全策略处理应用程序的方式。

- 创建应用程序组
- 创建应用程序筛选器
- 创建定制应用程序
- 解析应用程序相关性

## 创建应用程序组

应用程序组是一个对象，其中包含您要策略中以类似方式处理的应用程序。应用程序组用于访问您明确批准的应用程序，以便在您的组织中使用。对批准的应用程序进行分组可简化对规则库的管理。您可以仅更新受影响的应用程序组，而不必在支持的应用程序中发生更改时更新个别策略规则。

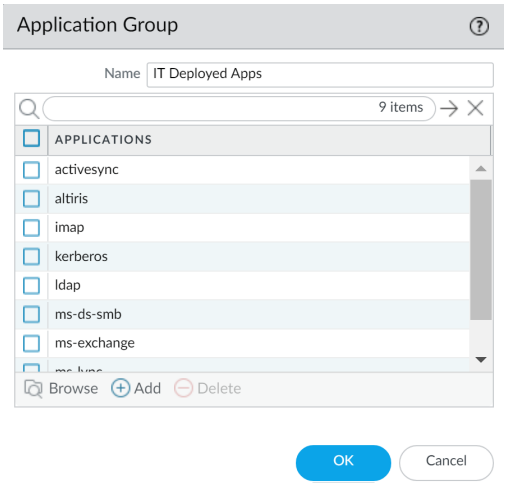
在决定对应用程序分组时，请考虑如何规划实施对已批准的应用程序的访问和创建与每个策略目标一致的应用程序组。例如，对于您的某些应用程序，您将仅允许 IT 管理员访问，而对于其他应用程序，您希望可供组织中的所有已知用户使用。在这种情况下，您将为所有这些策略目标创建单独的应用程序组。尽管您通常希望仅在默认端口上启用应用程序的访问，但您可能希望对此端口的例外应用程序进行分组，并在单独规则中实施对这些应用程序的访问。

STEP 1 | 选择**Objects**（对象）> **Applications**（应用程序）。

STEP 2 | **Add**（添加）一个分组并为其提供一个描述性 **Name**（名称）。

STEP 3 | （可选）选择 **Shared**（共享）以在共享位置创建对象，作为 Panorama 中的共享对象以进行访问，或在多个虚拟系统防火墙中跨所有虚拟系统进行使用。

STEP 4 | **Add**（添加）您希望在组中的应用程序，然后单击 **OK**（确定）。




STEP 5 | **Commit**（提交）配置。

## 创建应用程序筛选器

应用程序筛选器是一个根据您定义的应用程序属性（包括类别、子类别、技术、风险因素和特征）来动态对应用程序分组的对象。如果您希望安全地启用对未明确批准的应用程序的访问，但您希望用户能够访问，那么此操作会很有用。例如，您可能希望让员工能够选择自己的业务用办公程序（如 Evernote、Google Docs



© 2019 Palo Alto Networks, Inc.

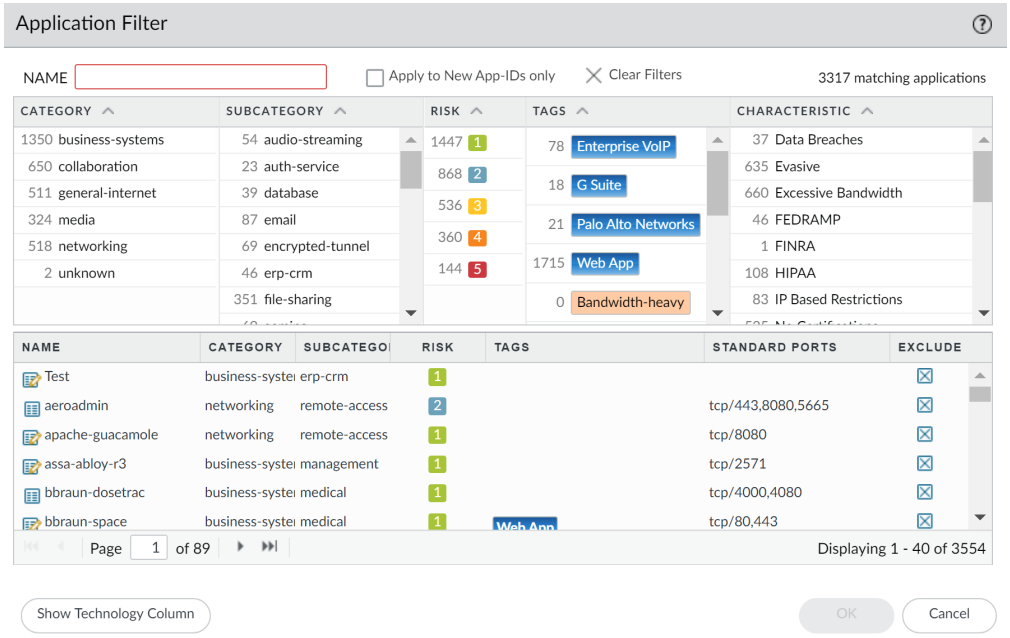
或 Microsoft Office 365）。要安全地启用这些类型的应用程序，您可以创建一个与类别 **business-systems** 和子类别 **office-programs** 相匹配的应用程序筛选器。在新应用程序办公程序出现并创建新 App-ID 后，这些新应用程序将自动匹配您已定义的筛选器；您不必对策略规则库进行任何其他更改便可安全启用与针对筛选器定义的属性相匹配的任何应用程序。

STEP 1 | 选择**Objects**（对象）> **Application Filters**（应用程序过滤器）。

STEP 2 | **Add**（添加）一个筛选器并为其提供一个描述性 **Name**（名称）。

STEP 3 | （可选）选择 **Shared**（共享）以在共享位置创建对象，作为 Panorama 中的共享对象以进行访问，或在多个虚拟系统防火墙中跨所有虚拟系统进行使用。

STEP 4 | 通过从“类别”、“子类别”、“技术”、“风险”和“特征”部分中选择属性值来定义筛选器。在您选择值时，请注意对话框顶部的匹配应用程序列表范围变窄。调整了筛选器属性以匹配要安全启用的应用程序类型后，单击 **OK**（确定）。




STEP 5 | **Commit**（提交）配置。

# 创建定制应用程序

要安全启用应用程序，必须对所有时间内、所有端口上的所有流量进行归类。通过 App-ID，在 ACC 和流量日志中仅被分类为未知流量（tcp、udp 或 non-syn-tcp）的应用程序都是尚未添加到 App-ID 的商用应用程序，网络上的内部或定制应用程序，或存在潜在威胁的应用程序。



如果您看到尚未具备 *App-ID* 的商业应用程序的未知流量，则可以在以下网址中提交新 *App-ID* 的申请：http://researchcenter.paloaltonetworks.com/submit-an-application/。

为确保您的内部定制应用程序不会显示为未知流量，请创建一个定制应用程序。然后您可以对这些应用程序实施粒度策略控制，以最大限度减小网络上无法识别流量的范围，从而减少攻击面。此外，创建定制应用程序还可让您正确识别 ACC 和流量日志中的应用程序，这使您可以审核/报告网络中的应用程序。

要创建定制应用程序，必须定义应用程序属性：其特征、其类别和子类别、风险、端口和超时。此外，还必须定义可供防火墙用于匹配流量流自身的模式或值（即签名）。最后，可以将定制应用程序附加到用于允许


© 2019 Palo Alto Networks, Inc.

或拒绝应用程序的安全策略（或者将其添加到应用程序组或将其与应用程序筛选器匹配）。还可以创建定制应用程序以标识包含热门话题的临时应用程序，如世界杯或疯狂三月的 ESPN3-Video。

为了收集正确的数据创建定制应用程序签名，您需要深入了解数据包捕获和形成数据报的方式。如果创建的签名过于宽泛，您可能会在无意中包括其他类似流量；如果定义过于狭窄，流量可以逃避检测（如果不根据模式进行严格匹配）。

定制应用程序存储在防火墙的单独数据库中，并且该数据库不会受每周的 *App-ID* 更新影响。

支持的应用协议解码器使防火墙能够检测可能在协议内部隧道的应用程序，包括内容发布版本 *609* 中的以下内容：*FTP*、*HTTP*、*MAP*、*POP3*、*SMB* 和 *SMTP*。

以下是如何创建定制应用程序的基本示例。

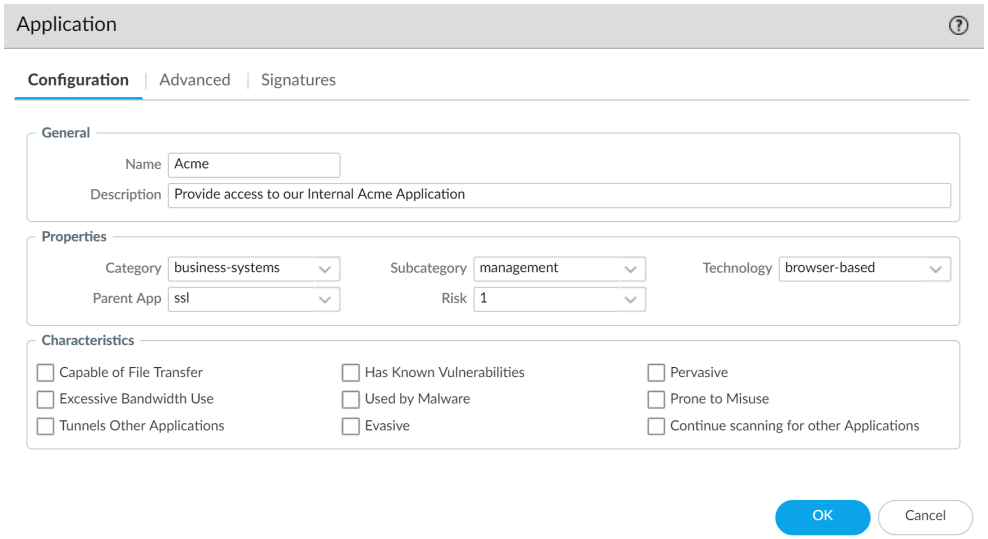
STEP 1 | 收集将能够用于编写定制签名的应用程序的信息。

为此，必须了解应用程序并了解您希望如何控制对应用程序的访问。例如，您可能希望限制用户可在应用程序中执行的操作（比如上传、下载或实时串流）。或者您可能希望允许应用程序，但实施 QoS 策略。

- 捕获应用程序数据包，以便您可以查找有关要作为定制应用程序签名的基础的应用程序的唯一特征。执行此操作的一种方法是在客户端系统上运行协议分析器（如 Wireshark）以捕获客户端与服务器之间的数据包。在应用程序中执行不同操作（比如上传和下载），以便您能够在生成的数据包捕获 (PCAP) 查找每种类型的会话。
- 因为在默认情况下防火墙对所有未知流量采用数据包捕获，如果防火墙在客户端与服务器之间，则您可以直接从流量日志中查看未知流量的数据包捕获。
- 使用数据包捕获来查找数据包 *contexts* 中的模式或值，可将其用于创建将唯一匹配应用程序流量的签名。例如，在 HTTP 响应或请求标头、URI 路径或主机名中查找字符串模式。有关可用来创建应用程序签名的不同字符串以及可以在数据包中查找对应值的位置的信息，请参阅创建定制威胁签名。

STEP 2 | 添加定制应用程序。

1. 选择 **Objects**（对象）> **Applications**（应用程序），然后单击 **Add**（添加）。
2. 在 **Configuration**（配置）选项卡上，输入定制应用程序的 **Name**（名称）和 **Description**（说明），这将帮助其他管理员了解您创建应用程序的原因。
3. （可选）选择 **Shared**（共享）以在共享位置创建对象，作为 Panorama 中的共享对象以进行访问，或在多个虚拟系统防火墙中跨所有虚拟系统进行使用。
4. 定义应用程序属性和特征。





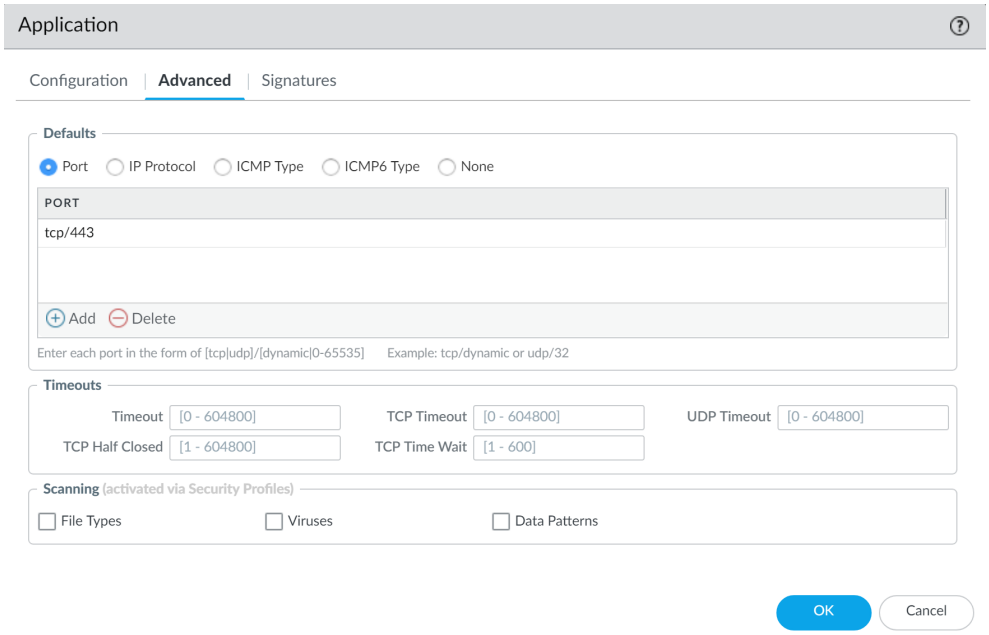

© 2019 Palo Alto Networks, Inc.

STEP 3 | 定义有关应用程序的详细信息，比如底层协议、运行应用程序的端口号、超时值以及您希望对流量执行的任何类型的扫描。

在 **Advanced**（高级）选项卡上，定义将允许防火墙用于标识应用程序协议的设置：

- 指定应用程序使用的默认端口或协议。
- 指定会话超时值。如果不指定超时值，那么将使用默认超时值。
- 表示您计划对应用程序流量执行的任何类型的附加扫描。

例如，要创建通过 SSL 运行但使用端口 4443（而不是 SSL 的默认端口 443）的定制基于 TCP 程序，您需指定端口号。通过为定制应用程序添加端口号，您可以创建策略规则（对应用程序使用默认端口），而不必在防火墙上打开其他端口。这将提高您的安全态势。



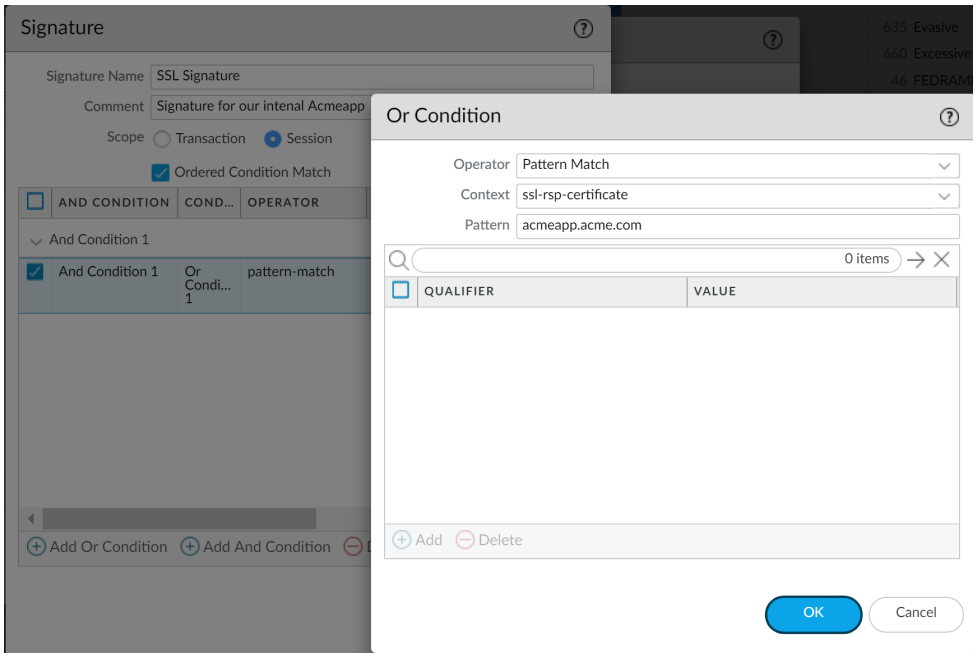

STEP 4 | 定义防火墙用来将流量与新应用程序进行匹配的条件。

您将使用从数据包捕获收集的信息来指定唯一字符串上下文值，防火墙可使用这些值来匹配应用程序流量中的模式。

1. 在 **Signatures**（签名）选项卡上，单击 **Add**（添加），然后定义 **Signature Name**（签名名称），然后可以选择定义 **Comment**（注释）以提供有关您计划如何使用此签名的信息。
2. 指定签名的 **Scope**（范围）：是与完整 **Session**（会话）还是单个 **Transaction**（事务）匹配。
3. 通过单击 **Add And Condition**（添加 **AND** 条件）或 **Add Or Condition**（添加 **OR** 条件）来指定用于定义签名的条件。
4. 选择 **Operator**（运算符）以定义将使用的匹配条件的类型：**Pattern Match**（模式匹配）或 **Equal To**（等于）。
   - 如果选择了 **Pattern Match**（模式匹配），选择 **Context**（上下文），然后使用正则表达式来定义 **Pattern**（模式）以匹配所选上下文。（可选）单击 **Add**（添加）以定义限定符/值对。**Qualifier**（限定符）列表特定于您选择的 **Context**（上下文）。
   - 如果选择了 **Equal To**（等于），选择 **Context**（上下文），然后使用正则表达式来定义数据包标头中用于匹配所选上下文的字节的 **Position**（位置）。选择 **first-4bytes**（第一个 **4** 字节）或 **second-4bytes**（第二个 **4** 字节）。定义 **Mask**（掩码）的 4 字节十六进制（例如 0xffffff00）和 **Value**（值）（例如 0xaabbccdd）。


© 2019 Palo Alto Networks, Inc.

例如，如果您为某个内部应用程序创建定制应用程序，则可以使用 **ssl-rsp-certificate Context**（**ssl-rsp-certificate** 上下文）来定义与服务器的 SSL 协商的证书响应消息的模式匹配，然后创建 **Pattern**（模式）以匹配消息中服务器的通用名称，如下所示：




5. 对每个匹配条件重复步骤 4.c 和 4.d。
6. 如果防火墙尝试匹配签名定义的顺序很重要，请务必选中 **Ordered Condition Match**（排序条件匹配）复选框，并且随后对条件进行排序，以便按照适当顺序对条件进行求值。选择一个条件或组，然后单击 **Move Up**（上移）或 **Move Down**（下移）。无法将条件从一个组移动到另一个组。
7. 单击 **OK**（确定）以保存签名定义。

STEP 5 | 保存应用程序。

1. 单击 **OK**（确定）以保存定制应用程序定义。
2. 单击 **Commit**（提交）。

STEP 6 | 验证流量是否如期匹配定制应用程序。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）安全策略规则以允许新应用程序。
2. 从位于防火墙和应用程序之间的客户端系统中运行应用程序，然后查看流量日志（**Monitor**（监控）> **Traffic**（流量））以确保您看到与新应用程序匹配的流量（并且正在根据您的策略规则进行处理）。

# 解析应用程序相关性

您可以在创建新的安全策略规则以及执行提交时看到应用程序相关性。当策略未包含所有应用程序相关性时，您可以直接访问关联的安全策略规则，以添加所需应用程序。

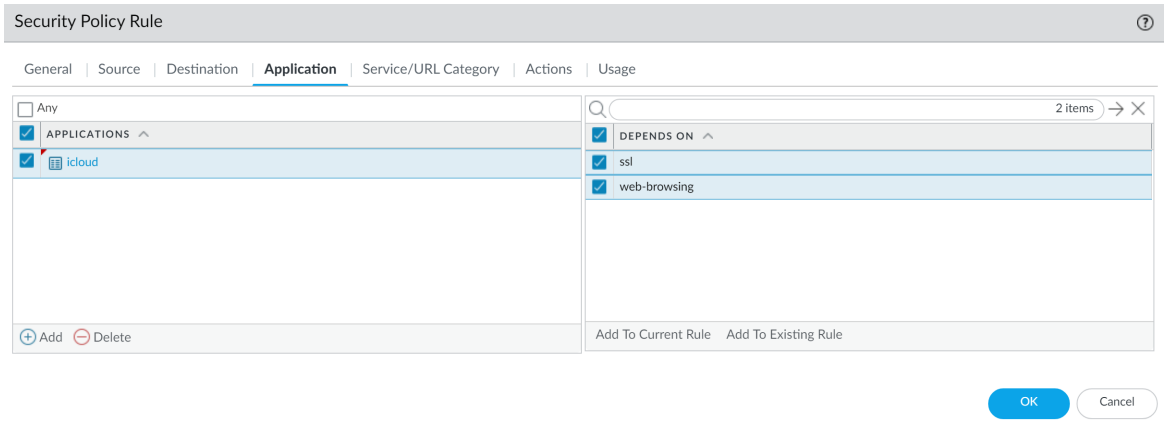
STEP 1 | 创建安全策略规则。

STEP 2 | 指定规则将允许或阻止的应用程序。

1. 在 **Applications**（应用程序）选项卡中，**Add**（添加）想要安全启用的 **Application**（应用程序）。您可以选择多个应用程序，或者使用应用程序组或应用程序筛选程序。
2. 查看选中应用程序的相关性，并 **Add To Current Rule**（添加到当前规则）或 **Add To Existing Rule**（添加到现有规则）。



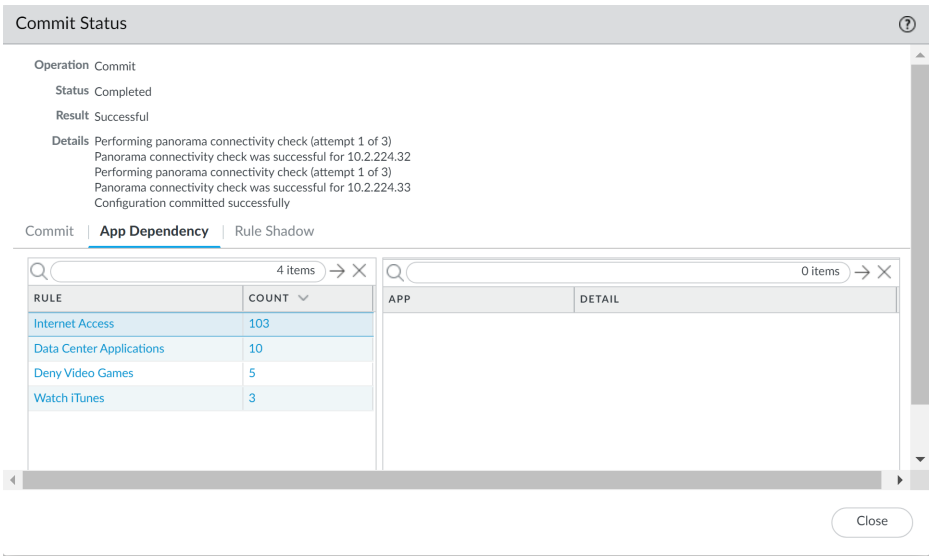
© 2019 Palo Alto Networks, Inc.




3. 如果添加到现有规则，请 **Select Rule**（选择规则）并单击 **OK**（确定）。

STEP 3 | 单击 **OK**（确定）并 **Commit**（提交）更改。

1. 查看 **App Dependency**（应用程序相关性）选项卡中的任何提交警告。




2. 选择 **Count**（计数）以查看未包含的应用程序相关性。
3. 选择 **Rule**（规则）名称以打开策略，并添加相关性。

解析任何应用程序相关性，否则，他们将继续在提交时生成警告。

4. 单击 **OK**（确定）并 **Commit**（提交）更改。


© 2019 Palo Alto Networks, Inc.

# 在默认端口上安全启用应用程序

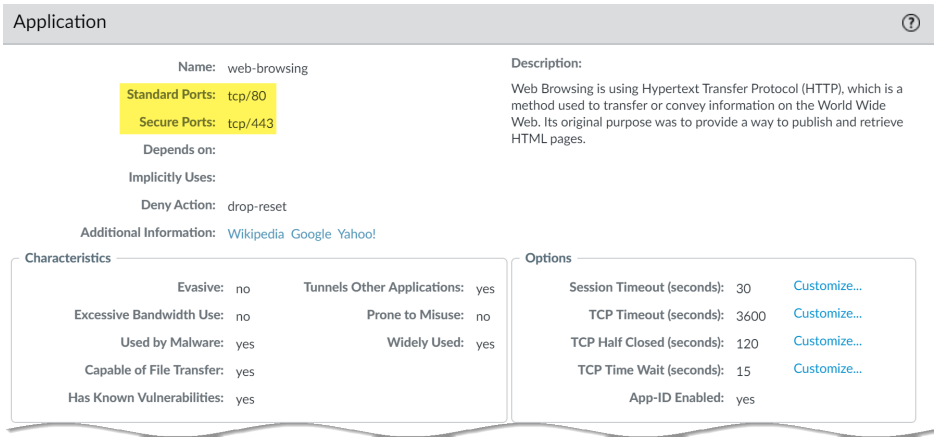
在异常端口上运行的应用程序可指示出尝试规避传统基于端口的保护机制的攻击者。Application-default 是 Palo Alto Networks 防火墙的一项功能，为您提供防止此类规避的建议方法，并在其最常用端口上启用应用程序。application-default 是基于应用程序的安全策略的最佳做法 — 其可降低管理开销，并修补基于端口的策略所带来的安全漏洞：

- **Less overhead**（更少开销）— 基于您的业务需要编写简单的、基于应用程序的安全规则，而非搜索和保持应用程序-端口映射。我们为所有带 App-ID 的应用程序定义了默认端口。
- **Stronger security**（更强的安全性）— 启用应用程序以仅在其默认端口上运行是安全性方面的最佳做法。application-default 可帮助您确保在应用程序行为异常时关键应用程序保持可用，而不会对安全造成影响。

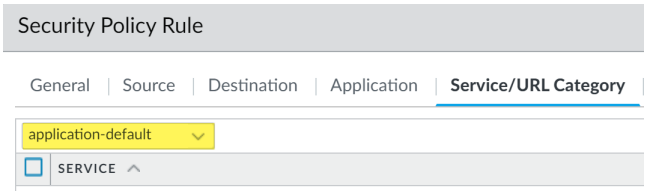
  此外，应用程序使用的默认端口有时取决于应用程序处于加密还是明文状态。基于端口的策略要求您打开应用程序可能用到的所有默认端口，以进行加密。打开端口会导致出现安全漏洞，攻击者可以利用该漏洞绕过您的安全策略。但是，application-default 会区分加密和明文应用程序流量。这意味着，其可以实施应用程序的默认端口，而无论其是否加密。

  例如，没有 application-default 功能时，您需要打开端口 80 和 443 以启用 web 浏览流量 — 您将允许两个端口上的明文和加密 web 浏览流量。application-default 功能开启后，防火墙严格实施明文 web 浏览流量（仅限端口 80），且仅在端口 443 上实施 SSL-隧道流量。

要查看应用程序默认使用的端口，您可以访问 Applipedia 或选择 **Objects**（对象）> **Applications**（应用程序）。应用程序详细信息包括应用程序的标准端口 — 明文状态下最常用的端口。对于 web 浏览，SMTP、FTP、LDAP、POP3 和 IMAP 详细信息也包含了应用程序的安全端口 — 即加密状态下应用程序使用的端口。




选择 **Policy**（策略）> **Security**（安全），并添加或修改规则，以仅在默认端口上执行应用程序：






将 *application-default* 作为基于应用程序的安全策略一部分，并与 *SSL* 一同使用，是最佳的做法。此外，如果您有控制 *web* 浏览流量的现有安全策略规则，且 *Service*（服务）被设为 *service-http* 和 *service-https*，您应更新这些规则以使用应用程序-默认代替。



© 2019 Palo Alto Networks, Inc.

# 应用程序与隐式支持

当创建安全策略以允许特定的应用程序时，您还必须确保根据应用程序允许任何其他应用程序。在许多情况下，您无需显式允许访问相关应用程序以便让流量通过，因为防火墙能够确定它们的依赖关系并隐式允许。这种隐式支持也适用于基于 HTTP、SSL、MS-RPC 或 RTSP 的定制应用程序。对于防火墙无法及时确定依赖性应用程序的应用程序，将会要求您在定义安全策略时显式允许依赖性应用程序。您可以采用下列其中一种方法，从基于应用程序的安全策略工作流中确定应用程序依赖性：

- 策略优化器
- 使用标签创建应用程序筛选器
- 创建基于自定义标签的应用程序过滤器
- 解析应用程序相关性

Applipedia 在必要时也可用。

下表列出了防火墙对其具有隐式支持的应用程序（截止至内容更新 595）。

| 应用程序 | 隐式支持 |
|---|---|
| 360-safeguard-update | http |
| apple-update | http |
| apt-get | http |
| as2 | http |
| avg-update | http |
| avira-antivir-update | http, ssl |
| blokus | rtmp |
| bugzilla | http |
| clubcooee | http |
| corba | http |
| cubby | http, ssl |
| dropbox | ssl |
| esignal | http |
| evernote | http, ssl |
| ezhelp | http |
| facebook | http, ssl |
| facebook-chat | jabber |


© 2019 Palo Alto Networks, Inc.

| 应用程序 | 隐式支持 |
| --- | --- |
| facebook-social-plugin | http |
| fastviewer | http, ssl |
| forticlient-update | http |
| good-for-enterprise | http, ssl |
| google-cloud-print | http, ssl, jabber |
| google-desktop | http |
| google-talk | jabber |
| google-update | http |
| gotomypc-desktop-sharing | citrix-jedi |
| gotomypc-file-transfer | citrix-jedi |
| gotomypc-printing | citrix-jedi |
| hipchat | http |
| iheartradio | ssl, http, rtmp |
| infront | http |
| instagram | http, ssl |
| issuu | http, ssl |
| java-update | http |
| jepptech-updates | http |
| kerberos | rpc |
| kik | http, ssl |
| lastpass | http, ssl |
| logmein | http, ssl |
| mcafee-update | http |
| megaupload | http |
| metatrader | http |
| mocha-rdp | t_120 |



© 2019 Palo Alto Networks, Inc.

| 应用程序 | 隐式支持 |
| --- | --- |
| mount | rpc |
| ms-frs | msrpc |
| ms-rdp | t_120 |
| ms-scheduler | msrpc |
| ms-service-controller | msrpc |
| nfs | rpc |
| oovoo | http, ssl |
| paloalto-updates | ssl |
| panos-global-protect | http |
| panos-web-interface | http |
| pastebin | http |
| pastebin-posting | http |
| pinterest | http, ssl |
| portmapper | rpc |
| prezi | http, ssl |
| rdp2tcp | t_120 |
| renren-im | jabber |
| roboform | http, ssl |
| salesforce | http |
| stumbleupon | http |
| supremo | http |
| symantec-av-update | http |
| trendmicro | http |
| trillian | http, ssl |
| twitter | http |
| whatsapp | http, ssl |


© 2019 Palo Alto Networks, Inc.

| 应用程序 | 隐式支持 |
| --- | --- |
| xm-radio | rtsp |



© 2019 Palo Alto Networks, Inc.

# 安全策略规则优化

策略优化器提供简单的工作流程以迁移您的传统安全策略规则库至基于 App-ID 的规则库，从而通过减少攻击表面和获得应用程序内的可见性，提高安全性，以便您可以安全启用。策略优化器识别基于端口的规则，以便您将其转为基于应用程序的允许规则，或从基于端口的规则添加应用程序至现有的基于应用程序的规则，而不对应用程序可用性造成影响。其还可识别过度配置的，基于 App-ID 的规则（配置有未使用应用程序的 App-ID 规则）。策略优化器帮助您优先那些需要先迁移的，基于端口的规则，识别基于应用程序的规则（允许您不适用的应用程序），并分析规则使用特征，如命中次数。

将基于端口的规则转为基于应用程序的规则可改善您的安全状态，因为您可以选择您想允许的应用程序，同时拒绝其他所有应用程序，从而消除您网络中不需要的和潜在的恶意流量。通过结合限制默认端口的应用程序流量（将服务设为 **application-default**），转换至基于应用程序的规则也可以防止规避应用程序在非标准端口上运行。

您可以将此功能用于：

- 运行 PAN-OS 9.0 版并启用了 App-ID 的防火墙。
- 运行 PAN-OS 9.0 版的 Panorama。您无需升级防火墙，Panorama 可以使用 **Policy Optimizer**（策略优化器）的功能。但是，要使用 **Rule Usage**（规则使用）功能（监控策略规则使用），管理的防火墙必须运行 PAN-OS 8.1 或更高版本。如果管理的防火墙连接至日志收集器，这些日志收集器也必须运行 PAN-OS 9.0 版本。具有日志处理卡 (LPC) 的托管 PA-7000 系列防火墙还可运行 PAN-OS 8.1（及更高版本）。

*PA-7000* 系列防火墙支持两种日志记录卡，*PA-7000* 系列防火墙日志处理卡 *(LPC)* 和高性能 *PA-7000* 系列防火墙日志转发卡 *(LFC)*。与 *LPC* 不同，*LFC* 没有进行日志本地储存的磁盘空间。取而代之的是，*LFC* 将所有日志转发至一个或多个日志记录系统，如 *Panorama* 或系统日志服务器。如果您使用 *LFC*，策略优化器的应用程序使用信息不会显示在防火墙上，因为流量日志并非本地储存。如果您使用 *LPC*，流量日志将本地存储到防火墙上，因此，策略优化器的应用程序使用信息会显示在防火墙上。

使用此功能：

- 迁移基于端口的规则至基于应用程序的规则—与结合流量日志和手动映射应用程序至基于端口的规则不同，使用策略优化器以识别基于端口的规则，并列出与各规则相匹配的应用程序，从而让您可以选择您想要允许的应用程序，并将其安全启用。将您的传统基于端口规则转换为基于应用程序的允许规则，以支持您的业务应用程序并让您可以阻止与恶意活动相关的任何应用程序。
- 识别过度配置的，基于应用程序的规则—较广泛的规则允许将不使用的应用程序留在网络上，从而增加了攻击面和恶意流量的危险。

将未使用的应用程序从安全策略规则中移除，以减少攻击面并保持规则库的整洁。不得让无人使用的应用程序存在于您的网络上。

要将配置从传统防火墙迁移到 *Palo Alto Networks* 设备，请参阅最佳实践之迁移到基于应用程序的策略。

您无法在 **Security**（安全）> **Policies**（策略）中分类安全策略规则，因为分类可能更改规则库内的规则顺序。然而，在 **Polices**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）下，策略优化器可提供不影响规则顺序的分类选项，以帮助您优先需要先转换或清除的规则。您可以对过去 30 天的规则按流量分类、按规则上的应用程序数量分类、按没有新应用程序的天数分类，以及按照允许的应用程序数量（针对过度配置规则）。

您也可以以其他方式使用策略优化器，包括验证预生产规则和对现有规则的故障排除。注意策略优化器仅遵循 **Log at Session End**（在会话结束时记录）并忽略 **Log at Session Start**（在会话开始时记录）以避免计算规则上的瞬时应用程序。


© 2019 Palo Alto Networks, Inc.

由于资源的限制，*VM-50 Lite* 虚拟防火墙不支持策略优化器。


- 策略优化器概念
- 从基于端口迁移至基于 App-ID 安全策略规则
- 规则克隆迁移用例：Web 浏览和 SSL 流量
- 添加应用程序至现有规则
- 通过未使用的应用程序识别安全策略规则
- 应用程序使用统计信息的高可用性
- 如何禁用策略优化器


# 策略优化器概念

更多有关此功能支持的信息，请查看以下主题：


- 排序和筛选安全策略规则
- 清除应用程序使用数据


## 排序和筛选安全策略规则

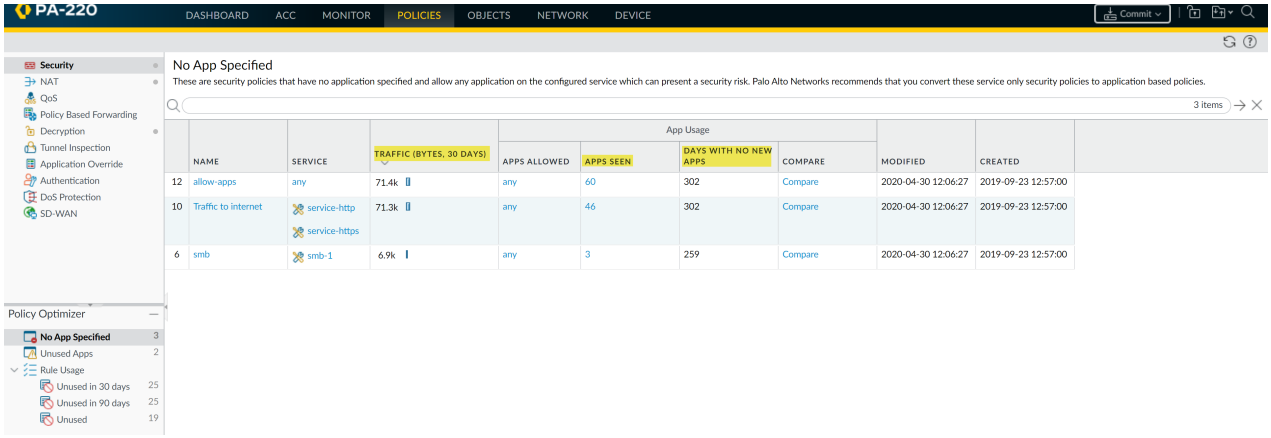
您可以通过筛选安全策略规则查看未配置有应用程序的所有基于端口的规则（**Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序））。此外，还可以查看已配置有应用程序但流量尚未到达所有应用程序的所有规则（**Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Unused Apps**（未使用的应用程序））。您可以根据不同类型的统计信息对筛选的策略规则进行排序，这有助于确定优先将哪些基于端口的规则迁移到基于应用程序的规则或首先清理的规则。

您不能在 *Policies*（策略）> *Security*（安全）中筛选或排序规则，因为这会更改策略规则在规则库中的顺序。筛选并排序 *Policies*（策略）> *Security*（安全）> *Policy Optimizer*（策略优化器）> *No App Specified*（未指定应用程序）和 *Policies*（策略）> *Security*（安全）> *Policy Optimizer*（策略优化器）> *Unused Apps*（未使用的应用程序）不会更改规则在规则库中的顺序。

您可以单击多个列标题，根据应用程序使用统计信息排序基于端口的规则（**No App Specified**（未指定应用程序））和带未使用应用程序的规则（**Unused Apps**（未使用的应用程序））。此外，还可以 查看策略规则使用情况 以协助识别并删除未使用的规则，从而降低安全风险，保持策略规则库的有序性。跟踪规则使用情况还可以快速验证新规则的添加和规则的更改情况，以及监控操作和故障排除任务的规则使用情况。



© 2019 Palo Alto Networks, Inc.




- **Traffic (Bytes, 30 days)**（流量（字节，30 天））— 过去 30 天在规则上显示的流量。默认情况下，在 30 天窗口中，会将当前与大多数流量匹配的规则置于列表顶部（时间范围越大，重点就越会放在仍保留在列表顶部的旧规则，因为这些规则具有较大的累计总数，即使这些规则可能再也查看不了太多的流量）。单击以反向排序。
- **Apps Seen**（显示的应用程序）— 将显示的应用程序最多或最少的规则置顶。防火墙永远不会自动清除应用程序数据。

  防火墙会大约每小时更新一次 *Apps Seen*（显示的应用程序）。但是，如果应用程序流量较大或规则较多，则更新时间可能超过一个小时。添加应用程序到规则后，请等待至少一个小时，然后再运行流量日志，以查看应用程序的日志信息。
- **Days with No New Apps**（没有新应用程序的天数）— 将自上一个新应用程序匹配规则以来具有最多或最少天数的规则置顶。
- （仅限Unused Apps（未使用的应用程序））**Apps Allowed**（允许的应用程序）— 将配置有最多或最少应用程序的规则置顶。

应用程序使用统计信息仅计算满足下列条件的规则中的应用程序数：

- 规则的操作必须为 **Allow**（允许）。
- 规则的日志设置必须为 **Log at Session End**（在会话结束时记录）（这是默认日志设置）。忽略 **Log at Session Start**（在会话开始时记录）的规则可用于防止瞬态应用程序计数。
- 有效流量必须与该规则匹配。例如，如果会话在有足够的流量通过防火墙以标识应用程序时结束，则不会对其进行计数。下列流量类型无效，因此，不会用作策略优化器统计信息：


© 2019 Palo Alto Networks, Inc.

- Insufficient-data
- Not-applicable
- Non-syn-tcp
- Incomplete

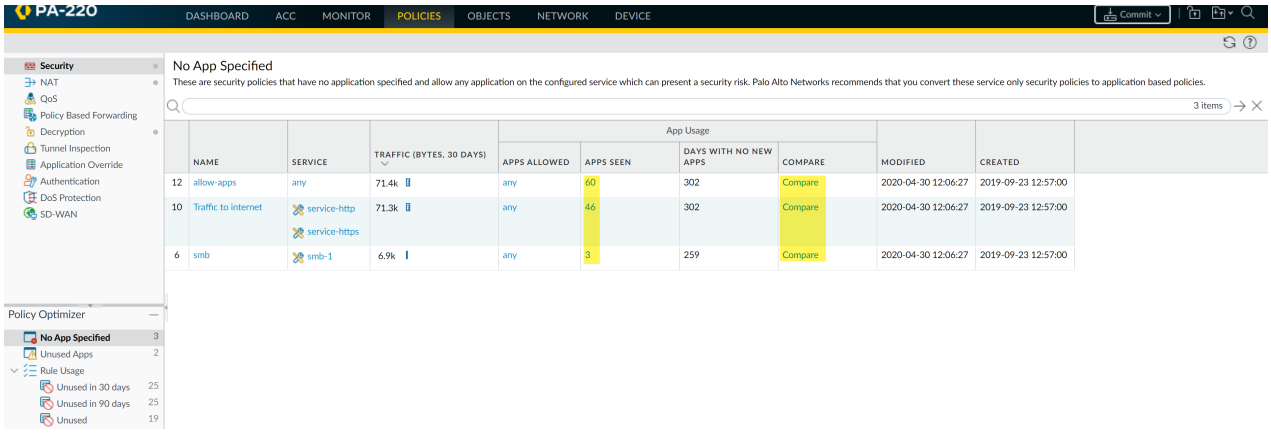
  您可以筛选流量日志（**Monitor**（监控）> **Logs**（日志）> **Traffic**（流量））以查看标识为这些类型之一的流量。例如，要查看所有标识为 incomplete 的所有流量，请使用筛选器 **(app eq incomplete)**。

如果不满足这些条件，应用程序不会用作 **Apps Seen**（显示的应用程序）等统计信息，不会影响 **Days with No New Apps**（没有新应用程序的天数）等统计信息，也不会出现在应用程序列表中。

防火墙不会跟踪区域间默认和区域内默认安全策略规则的应用程序使用统计信息。

如果规则 *UUID* 发生更改，因为 *UUID* 更改会使防火墙将该规则视为不同的（新的）规则，因此，应重置用于该规则的应用程序使用统计信息。

要查看并排序规则上显示的应用程序，在规则行中，单击 **Compare**（比较）或单击 **Apps Seen**（显示的应用程序）中的数字。

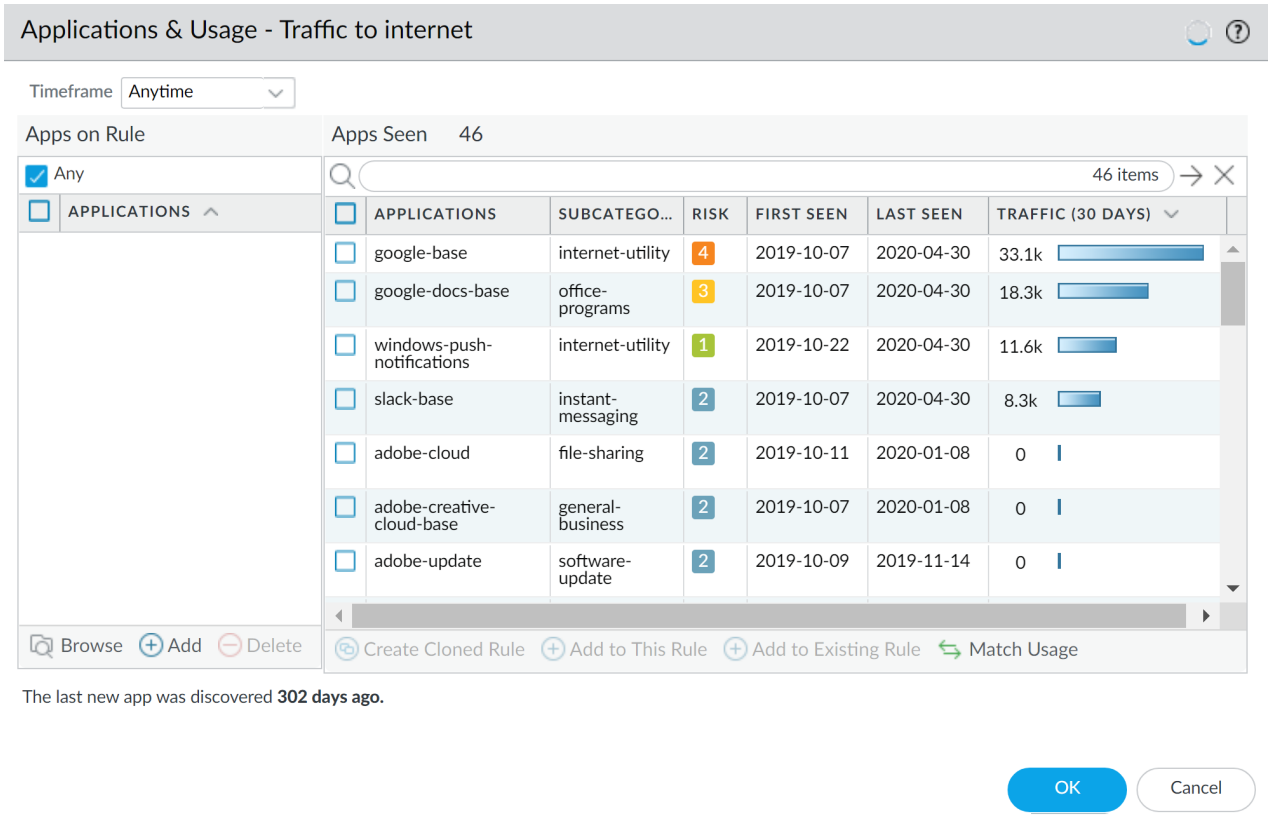



对于在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）和 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Unused**



© 2019 Palo Alto Networks, Inc.

**Apps**（未使用的应用程序）中显示的规则，单击 **Compare**（比较）或 **Apps Seen**（显示的应用程序）数字就会显示 **Applications & Usage**（应用程序和使用情况），从而可以查看规则上显示的应用程序，并对其进行排序。此外，在 **Applications & Usage**（应用程序和使用情况）中，您还可以从基于端口迁移至基于 App-ID 安全策略规则，并删除规则中的未使用应用程序。




您可以通过所有六个 **Apps Seen**（显示的应用程序）统计信息将规则上显示的应用程序排序（**Apps Seen**（显示的应用程序）不会实时更新，需要一个小时或更长时间来完成更新，具体视流量容量和规则数而定）。

- **Applications**（应用程序）— 按应用程序名称的字母顺序。如果您为规则服务（服务不能是 **any**（任何））配置特定端口或端口范围，应用程序有标准端口，且配置端口与 application-default 端口不匹配，则会在应用程序旁边出现一个三角形的黄色警告图标。
- **Subcategory**（子类别）— 按应用程序子类别的字母顺序，派生于应用程序内容元数据。
- **Risk**（风险）— 根据应用程序的风险等级。
- **First Seen**（首次显示）— 应用程序在规则上第一次被显示的日期。时间戳分辨率仅为当天（不是每小时）。
- **Last Seen**（上次显示）— 应用程序在规则上最近一次被显示的日期。时间戳分辨率仅为当天（不是每小时）。
- **Traffic (30 days)**（流量（30 天））— 过去 30 天与规则匹配的流量（以字节为单位）是默认排序方式。

设置 **Timeframe**（时间段）以显示特定时间段内的统计信息 — **Anytime**（任何时间）、**Past 7 days**（过去 7 天）、**Past 15 days**（过去 15 天）、或 **Past 30 days**（过去 30 天）。


© 2019 Palo Alto Networks, Inc.

*Traffic (30 days)*（流量（*30* 天））始终仅显示最近 *30* 天的流量（以字节为单位）。更改 *Timeframe*（时间段）不会影响 *Traffic (30 days)*（流量（*30* 天））字节测量的持续时间。

单击列标题对显示结果进行排序，再次单击列可反向排序。例如，单击 **Risk**（风险）以按从低风险到高风险的顺序对应用程序排序。再次单击 **Risk**（风险）可按从高风险到低风险的顺序对应用程序排序。

防火墙不会在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）、**Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Unused Apps**（未使用的应用程序）或 **Applications & Usage**（应用程序和使用情况）中实时报告应用程序使用情况的统计信息，因此，该功能不能替代报告运行。

- 防火墙大约每小时更新一次 **Apps Allowed**（允许的应用程序）、**Apps Seen**（显示的应用程序）和 **Applications & Usage**（应用程序和使用情况）中列出的应用程序，而不是实时更新。但是，如果流量较大或规则较多，更新时间可能更长。添加应用程序到规则后，请等待至少一个小时，然后再运行流量日志，以查看应用程序的日志信息。

  防火墙会大约每小时更新一次 **Apps Seen**（显示的应用程序）。但是，如果应用程序流量较大或规则较多，则更新时间可能超过一个小时。添加应用程序到规则后，请等待至少一个小时，然后再运行流量日志，以查看应用程序的日志信息。
- 防火墙每天在午夜设备时间更新一次 **Days with No New Apps**（没有新应用程序的天数）以及 **Applications & Usage**（应用程序和使用情况）上的 **First Seen**（首次查看）和 **Last Seen**（上次查看）。
- 对于带有大量显示应用程序的规则，用于处理应用程序使用情况统计信息的时间可能更长。
- 若安全策略规则库带有大量具有许多应用程序的规则，用于处理应用程序使用情况统计信息的时间可能更长。
- 对于由 Panorama 管理的防火墙，应用程序使用数据仅对 Panorama 推送到防火墙的规则可见，而对于每个防火墙上本地配置的规则不可见。

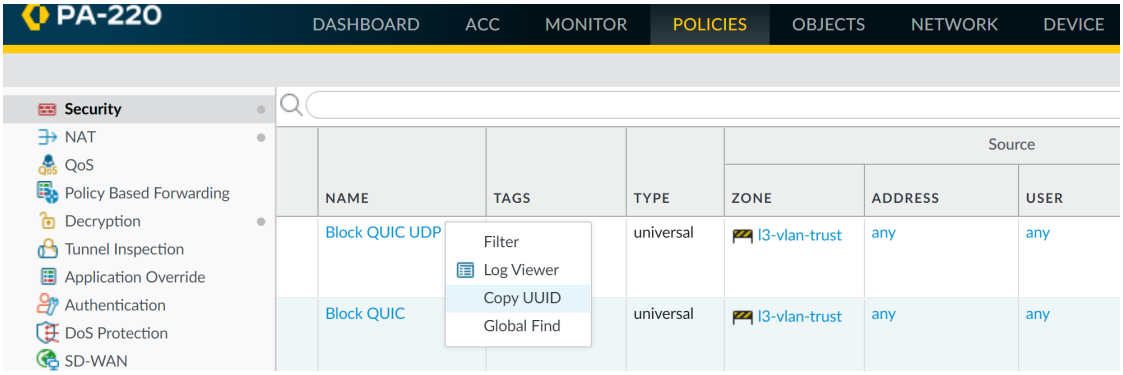
## 清除应用程序使用数据

您可以使用 CLI 命令以清除单个安全策略规则的应用程序使用数据，并重置 **Apps Seen**（显示的应用程序）和其他应用程序使用数据。

STEP 1 | 找到您想要清除应用程序使用数据的安全策略规则 UUID。

可以通过两种方法在 UI 中找到 UUID：

- 在 **Policies**（策略）> **Security**（安全）中，从 **Rule UUID**（规则 **UUID**）列复制 UUID。
- 在 **Policies**（策略）> **Security**（安全）中，选择 **Name**（名称）下拉菜单中的 **Copy UUID**（复制 **UUID**）。




STEP 2 | 从 UI 切换至 CLI。

使用您在 UI 中捕获的 UUID 以清除规则的应用程序使用数据：

```
admin@PA-VM>clear policy-app-usage-data ruleuuid <uuid-value>
```



© 2019 Palo Alto Networks, Inc.

粘贴或输入规则的 UUID 作为值，并执行命令以清除规则的应用程序使用数据。

# 从基于端口迁移至基于 App-ID 安全策略规则

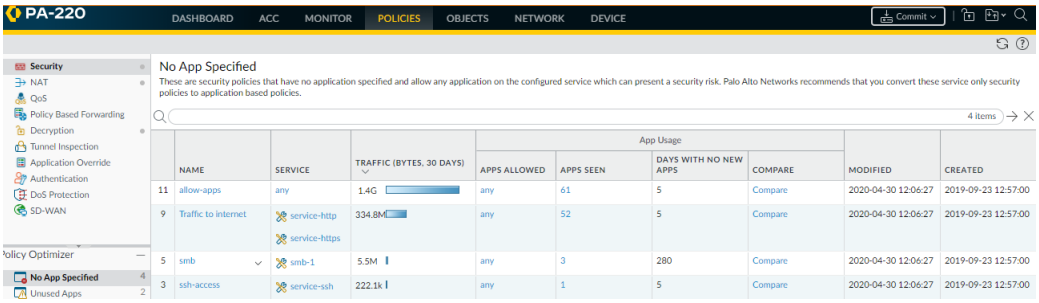
从传统防火墙转换到 Palo Alto Networks 下一代防火墙时，您会继承大量允许端口上任何应用程序的端口规则。由于任何应用程序都可使用开放端口，因此会增大攻击面。通过策略优化器，可以标识任何基于端口的传统安全策略规则上显示的所有应用程序，并提供一个可用于选择您要允许其出现在该规则上的应用程序的简单工作流程。迁移基于端口的规则到基于应用程序的规则后，可以减小攻击面，从而在您的网络上安全地启用应用程序。通过策略优化器，可在添加新应用程序时维护规则库。

一次只能迁移少量基于端口的规则到基于应用程序的规则，并按优先级排定迁移顺序。相较于一次迁移一个大型规则库而言，逐步转换更安全，并且更容易确保基于应用程序的新规则可以管控必要的应用程序。使用 *Policy Optimizer*（策略优化器）确定规则转换的优先级。

要将配置从传统防火墙迁移到 *Palo Alto Networks* 设备，请参阅最佳实践之迁移到基于应用程序的策略。

STEP 1 | 标识基于端口的规则。

基于端口的规则未配置有（不允许）应用程序。**Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）显示所有基于端口的规则（**Apps Allowed**（允许的应用程序）设为 **any**（任何））。




STEP 2 | 确定转换基于端口的规则的优先级。

通过 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序），您可以将规则排序，而不会影响其在规则库中的顺序，并为您提供其他信息，这有助于您根据业务目标和风险承受能力确定规则转换的优先级。

- **Traffic (Bytes, 30 days)**（流量（字节，30 天））— （单击以进行排序）。 当前匹配最多流量的规则显示在列表的顶部。这是默认的排序顺序。
- **Apps Seen**（显示的应用程序）— （单击以进行排序）。 出现大量与基于端口的规则匹配的合法应用程序可能表示，您应将该规则替换为可严格定义应用程序、用户、以及源和目标的多个基于应用程序的规则。例如，如果基于端口的规则控制不同设备组上用于不同用户组的多个应用程序，则创建可将应用程序与其合法用户和设备进行配对的单个规则，从而减小攻击面，提高可见性。（单击 **Apps Seen**（显示的应用程序）数或 **Compare**（比较）后，可显示与该规则匹配的应用程序。）

  防火墙会大约每小时更新一次 *Apps Seen*（显示的应用程序）。但是，如果应用程序流量较大或规则较多，则更新时间可能超过一个小时。添加应用程序到规则后，请等待至少一个小时，然后再运行流量日志，以查看应用程序的日志信息。
- **Days with No New Apps**（没有新应用程序的天数）— （单击以进行排序）。 一旦基于端口的规则上显示的应用程序数保持稳定，您可以更确信该规则是成熟的，转换不会意外排除合法应用程序，且不会再有新应用程序会与该规则匹配。**Created**（创建日期）和 **Modified**（修改日期）可帮助您评估规则的稳定性，因为近期未进行修改的旧规则可能会更稳定。

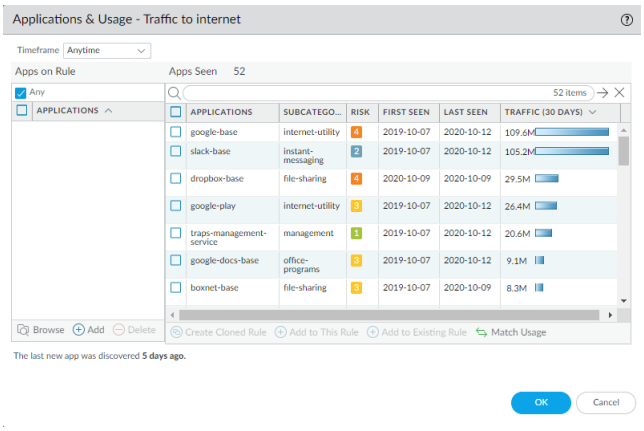

© 2019 Palo Alto Networks, Inc.

- **Hit Count**（命中次数）— 显示所选时间范围内具有最多匹配次数的规则。通过重置命中计数器，指定以天为单位的排除时间段，可以排除规则。因为您不知道计数器已重置，因此，排除最近进行过命中计数器重置操作的规则可防止对显示命中次数比预期少的规则产生误解。

此外，您还可以使用 *Hit Count*（命中次数）执行查看策略规则使用情况，以帮助标识和删除未使用的规则，从而降低安全风险，保持规则库的有序性。

STEP 3 | 检查基于端口的规则 **Apps Seen**（显示的应用程序），从具有最高优先级的规则开始。

在 **No Apps Specified**（未指定应用程序）上，单击 **Compare**（比较）或 **Apps Seen**（显示的应用程序）数以打开 **Applications & Usage**（应用程序和使用情况），其中列出了指定 **Timeframe**（时间段）内与基于端口的规则匹配的应用程序、每个应用程序的 **Risk**（风险）、**First Seen**（首次查看）应用程序的日期、**Last Seen**（上次查看）应用程序的日期、以及过去 30 天的流量。




您可以检查过去 7 天、15 天或 30 天，或规则生命周期内（**Anytime**（任何时间））基于端口的规则 **Applications seen**（显示的应用程序）。对于迁移规则，**Anytime**（任何时间）可对与规则匹配的应用程序提供最完整的评估。

您可以搜索并筛选 **Apps Seen**（显示的应用程序），但请注意，更新 **Apps Seen**（显示的应用程序）可能需要一小时或更长时间。此外，您还可以通过单击列标题对 **Apps Seen**（显示的应用程序）进行排序。例如，单击 **Traffic (30 days)**（流量（30 天））可将具有最新流量的应用程序排至列表顶部，或单击 **Subcategory**（子类别）以根据子类别对应用程序进行排序。

*First Seen*（首次查看）和 *Last Seen*（上次查看）数据的测量粒度都是一天，因此，在您定义规则的当天，这两列的日期是相同的。第二天，防火墙会查看应用程序上的流量，您会发现日期有差异。

STEP 4 | 克隆或添加应用程序到规则，以指定想要允许其在规则上运行的应用程序。

在 **Applications & Usage**（应用程序和使用情况）上，通过以下两种方式将基于端口的规则转换到基于应用程序的规则：

- **Clone the rule**（克隆规则）— 保留基于端口的原始规则，直接在规则库中原始规则的前面克隆基于应用程序的规则。
- **Add Applications to the Rule**（添加应用程序到规则）— 将基于端口的原始规则替换为基于应用程序的新规则，并删除原始规则。

如果您已有基于应用程序的规则，并且要将应用程序从基于端口的规则迁移到这些规则，您可以添加应用程序至现有规则，而不是克隆新规则，或是通过添加应用程序到该规则来转换基于端口的规则。



© 2019 Palo Alto Networks, Inc.

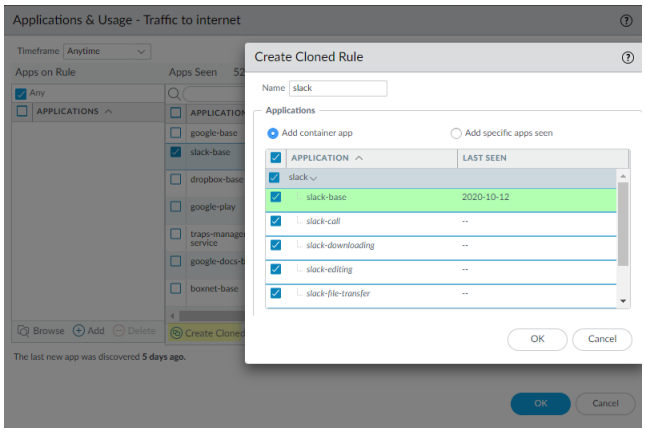
某些应用程序以一定的间隔时间出现在网络上，例如每季度季度或每年一次。如果历史记录的时间长度不足以捕获其最新活动，这些应用程序可能不会出现在 *Applications & Usage*（应用程序和使用情况）屏幕上。

在克隆规则或添加应用程序到规则时，除原始规则外，其他都不会发生更改。除用于添加到规则的应用程序的规则外，原始规则的配置将保持不变。例如，如果原始规则的服务允许 *Any*（任何）应用程序或指定特定服务，您需要将服务更改为 *Application-Default*，以将允许的应用程序限制到新规则上的对应默认端口。

克隆是一种安全的规则迁移方式，尤其是当 **Applications & Usage**（应用程序和使用情况）显示多个与该规则匹配的知名应用程序时（规则克隆迁移用例：Web 浏览和 SSL 流量提供此类示例）。克隆可保留基于端口的原始规则，并将其置于基于应用程序的克隆规则后面，从而消除了因流量与流至端口规则的克隆规则不匹配而导致应用程序可用性丢失的风险。当合法应用程序的流量未在合理时间段到达基于端口的规则时，您可以将其删除，以完成该规则的迁移。

要克隆基于端口的规则：

1. 在 **Apps Seen**（显示的应用程序）中，单击克隆规则中您想要运行的每个应用程序旁边的复选框。请注意，更新 **Apps Seen**（显示的应用程序）可能需要一小时或更长时间。
2. 单击 **Create Cloned Rule**（创建克隆规则）。在 **Create Cloned Rule**（创建克隆规则）对话框中，确定克隆规则的 **Name**（名称）（在本示例中为“slack”），并根据需要在同一容器和应用程序依赖关系中添加其他应用程序。例如，要通过选择基于 slack 的应用程序来可克隆规则：




   绿色文本是选中进行克隆的应用程序。容器应用程序（**slack**）位于灰色行中。斜体列出的应用程序未出现在规则中，但位于与选中应用程序相同的容器中。规则上显示的各个应用程序均为普通字体。默认情况下，所有应用程序均应包含在克隆规则中（默认选中可在容器内添加所有应用程序的 **Add Container App**（添加容器应用程序）选项），以帮助防止规则在将来发生中断。
3. 如果想要允许容器内所有应用程序，请让 **Add container app**（添加容器应用程序）保持选中状态。这也是规则能够“适应未来需求”，因为，在添加应用程序到容器应用程序中时，可自动将其添加到规则。

   如果想要限制对容器内某些单独应用程序的访问，可取消选中您不想用户访问的每个应用程序旁边的复选框。这也会取消选中容器应用程序，因此，如果想要稍后允许容器内的新应用程序，您必须单独添加这些应用程序。

   如果取消选中容器应用程序，则会取消选中所有应用程序，您必须手动选择想要包含在克隆规则中的应用程序。
4. 如果在应用程序下面的方框内列出应用程序相关性（此示例中没有），请勾选。选中的应用程序需要运行这些应用程序相关性。常见的相关性包括 **ssl** 和 **web-browsing**。
5. 单击 **OK**（确定），直接在规则库中基于端口的规则前面添加基于应用程序的新规则。
6. **Commit**（提交）配置。


© 2019 Palo Alto Networks, Inc.

克隆规则并 **Commit**（提交）配置时，您选中用于克隆规则的应用程序将从基于端口的原始规则的 **Apps Seen**（显示的应用程序）列表中删除。例如，如果基于端口的规则有 16 个 **Apps Seen**（显示的应用程序），且您选中 2 个单独应用程序和 1 个相依应用程序用于克隆规则，在克隆后，基于端口的规则将显示 13 个**Apps Seen**（显示的应用程序），原因是有 3 个选中的应用程序从基于端口的规则中删除 (16 - 3 = 13)。克隆规则在 **Apps on Rule**（规则上的应用程序）中显示三个已添加的应用程序。

使用容器应用程序创建克隆规则的方式略有不同。例如，基于端口的规则有 16 个 **Apps Seen**（显示的应用程序），且您选中 1 个单独应用程序和 1 个容器应用程序用于克隆规则。容器应用程序有 5 个单独应用程序和 1 个相依应用程序。克隆后，克隆规则显示 7 个 **Apps on Rule**（规则上的应用程序），包括 1 个单独应用程序、5 个在容器应用程序中的单独应用程序、以及 1 个用于容器应用程序的相依应用程序。但是，在基于端口的原始规则中，因为仅 1 个单独应用程序、1 个容器应用程序、和 1 个容器应用程序的相依应用程序从基于端口的规则中删除，因此，**Apps Seen**（显示的应用程序）中显示有 13 个应用程序。

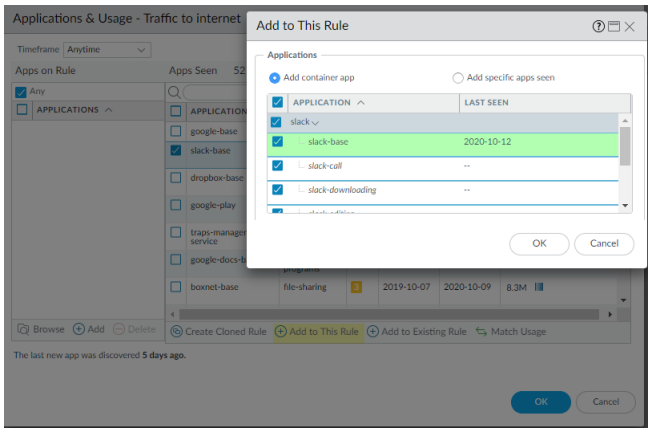
与克隆相比，添加应用程序到基于端口的规则可替换生成的基于应用程序的规则。添加应用程序到规则比克隆更简单，但风险更大，因为您可能会无意错过应出现在规则上的应用程序，且基于端口的原始规则不再出现在规则库中以捕获意外遗漏。但是，添加应用程序到仅适用于少数知名应用程序的基于端口的规则可快速将规则迁移到基于应用程序的规则。例如，对于仅控制 TCP 端口 22 流量的基于端口的规则，唯一合法的应用程序是 SSH，因此，添加应用程序到规则就很安全。

使用传统安全策略规则的 *Application*（应用程序）选项卡添加应用程序不会更改 *Apps Seen*（显示的应用程序）或 *Apps on Rule*（规则上的应用程序）。要保留准确的应用程序使用信息，在将基于端口的规则替换为基于应用程序的规则时，需在 *Apps Seen*（显示的应用程序）中使用 *Add to This Rule*（添加到此规则）或 *Match Usage*（匹配使用情况）添加应用程序，或创建克隆规则，或添加应用程序到现有基于应用程序的规则。

通过添加应用程序，有三种方法可将基于端口的规则替换为基于应用程序的规则（**Apps Seen**（显示的应用程序）中的 **Add to This Rule**（添加到此规则）和 **Match Usage**（匹配使用情况），以及 **Apps on Rule**（规则上的应用程序）中的 **Add**（添加））：

- 从 **Apps Seen**（显示的应用程序）中，将应用程序 **Add to This Rule**（添加到此规则）（匹配规则的应用程序）。请注意，更新 **Apps Seen**（显示的应用程序）可能需要一小时或更长时间。

  1. 从规则上 **Apps Seen**（显示的应用程序）中选择应用程序。
  2. 单击 **Add to This Rule**（添加到此规则）。在 **Add to This Rule**（添加到此规则）对话框中，根据需要添加相同容器应用程序和应用程序相关性中的其他应用程序。例如，要添加 slack-base 到规则：




与 **Create Cloned Rule**（创建克隆规则）对话框类似，**Add to This Rule**（添加到此规则）中的绿色文本是选中要添加到此规则的应用程序。容器应用程序（**slack**）位于灰色行中。斜体列出的应用程序未出现在规则中，但位于与选中应用程序相同的容器中。规则上显示的各个应用程序均为普



© 2019 Palo Alto Networks, Inc.

通字体。默认情况下，所有应用程序均应包含在克隆规则中（默认选中可在容器内添加所有应用程序的 **Add Container App**（添加容器应用程序）选项），以帮助防止规则在将来发生中断。

3. 如果想要允许容器内所有应用程序，请让 **Add container app**（添加容器应用程序）保持选中状态。这也是规则能够"适应未来需求"，因为，在添加应用程序到容器应用程序中时，可自动将其添加到规则。

   如果想要限制对容器内某些单独应用程序的访问，可取消选中您不想用户访问的每个应用程序旁边的复选框。这也会取消选中容器应用程序，因此，如果想要稍后允许容器内的新应用程序，您必须单独添加这些应用程序。

   如果取消选中容器应用程序，则会取消选中所有应用程序，您必须手动选择想要包含在克隆规则中的应用程序。
4. 如果在应用程序下面的方框内列出应用程序相关性（此示例中没有），请勾选。选中的应用程序需要运行这些应用程序相关性。
5. 单击 **OK**（确定）将基于端口的规则替换为基于应用程序的新规则。

在 **Add to This Rule**（添加到此规则）并 **Commit**（提交）配置时，未添加的应用程序将从 **Apps Seen**（显示的应用程序）中删除，原因是基于应用程序的新规则不允许它们再继续存在。例如，如果规则有 16 个 **Apps Seen**（显示的应用程序），且您将 3 个应用程序 **Add to This Rule**（添加到此规则），则生成的新规则仅在 **Apps Seen**（显示的应用程序）中显示这 3 个应用程序。

使用容器应用程序**Add to This Rule**（添加到此规则）的方式略有不同。例如，基于端口的规则有 16 个 **Apps Seen**（显示的应用程序），且您选中 1 个单独应用程序和 1 个容器应用程序添加到新规则。容器应用程序有 5 个单独应用程序和 1 个相依应用程序。添加应用程序到规则后，新规则显示 7 个**Apps on Rule**（规则上的应用程序），包括 1 个单个应用程序、5 个在容器应用程序中的单个应用程序、以及 1 个用于容器应用程序的相依应用程序。但是，因为有 1 个单独应用程序、1 个容器应用程序、和 1 个容器应用程序的相依应用程序从该列表中删除，因此，**Apps Seen**（显示的应用程序）显示有 13 个应用程序。

- 只需单击一次，即可将规则上所有 **Apps Seen**（显示的应用程序）一次性添加到规则中（**Match Usage**（匹配使用情况））。

  基于端口的规则允许任何应用程序，因此，*Apps Seen*（显示的应用程序）可能包括不需要或不安全的应用程序。仅当规则查看少量具有合法业务目的的知名应用程序时，才能使用 *Match Usage*（匹配使用情况）转换规则。*TCP* 端口 *22* 就是一个很好的示例。该端口仅允许 *SSH* 流量，因此，如果 *SSH* 是可以打开端口 *22* 的基于端口的规则上显示的唯一应用程序时，您可以安全启用 *Match Usage*（匹配使用情况）。

  1. 在 **Apps Seen**（显示的应用程序）中，单击 **Match Usage**（匹配使用情况）。请注意，更新 **Apps Seen**（显示的应用程序）可能需要一小时或更长时间。**Apps Seen**（显示的应用程序）中的所有应用程序都将复制到 **Apps on Rule**（规则上的应用程序）。
  2. 单击 **OK**（确定）可创建基于应用程序的规则，并替换基于端口的规则。
- 如果您知道想要在规则上运行的应用程序，您可以在 **Apps on Rule**（规则上的应用程序）中手动 **Add**（添加）应用程序。但是，该方法等同于使用传统安全策略规则的 **Application**（应用程序）选项卡，不会更改 **Apps Seen**（显示的应用程序）或 **Apps on Rule**（规则上的应用程序）。若要保留准确的应用程序使用信息，请在 **Apps Seen**（显示的应用程序）中使用 **Add to This Rule**（添加到此规则）、**Create Cloned Rule**（创建克隆规则）或 **Match Usage**（匹配使用情况）转换规则。

  1. 在 **Apps on Rule**（规则上的应用程序）中，**Add**（添加）（或**Browse**（浏览））并选中要添加到规则的应用程序。这等同于在 **Application**（应用程序）选项卡中添加应用程序。
  2. 单击 **OK**（确定）以添加应用程序到规则，并将基于端口的规则替换为基于应用程序的新规则。

  因为该方法等同于使用 *Application*（应用程序）选项卡添加应用程序，因此，不会弹出添加应用程序依赖关系的对话框。

STEP 5 | 对于每个基于应用程序的规则，设置 **Service**（服务）为 **application-default**。


© 2019 Palo Alto Networks, Inc.

如果出于业务需求，您需要允许在特定客户端和服务器之间的非标准端口上运行应用程序（例如，内部自定义应用程序），则将例外限制为必要的应用程序、源和目标。考虑重写自定义应用程序，这样，就可以使用应用程序默认端口。

STEP 6 | **Commit**（提交）配置。

STEP 7 | 监控规则。

- 克隆规则 — 监控基于端口的原始规则，确保基于应用程序的规则与所需流量匹配。如果您想要允许的应用程序与基于端口的规则匹配，请将其添加到基于应用程序的规则，或为其克隆基于应用程序的其他规则。若在合理时间段内，只有您不希望在您网络上运行的应用程序与基于端口的规则匹配时，则克隆规则是稳健的（与您想控制的所有应用程序流量相匹配），您可以安全地删除它。
- 使用添加应用程序的规则 — 因为您只将具有少数知名应用程序的基于端口的规则直接转换为基于应用程序的规则，因此，在大多数情况下，该规则从一开始就是可靠的。监控转换规则，检查预期流量是否与规则匹配；如果流量比预期少，则规则可能不会允许所有必要的应用程序。如果流量超出预期，则规则可能会允许不需要的流量。倾听用户反馈 — 如果用户无法访问其业务需要的应用程序，则该规则（或其他规则）可能太严格。

# 规则克隆迁移用例：Web 浏览和 SSL 流量

允许在 TCP 端口 80（HTTP Web 浏览）和 443 (HTTPS SSL) 进行 Web 访问的基于端口的规则无法控制哪些应用程序可以使用这些开放端口。Web 应用程序有很多，因此，允许 Web 流量的一般规则可允许成千上万的应用程序，其中有很多都是您不想在网络上运行的。

本用例展示的是如何将允许所有 Web 应用程序的基于端口的策略迁移到仅允许您想运行的应用程序的基于应用程序的策略，这样，您就可以安全地启用您选择允许的应用程序。对于可以查看大量应用程序的规则，克隆基于端口的原始规则比添加应用程序到规则更安全，原因是添加会替代基于端口的规则。因此，如果您不小心忘记添加关键应用程序，则应用程序的可用性就会受到影响。并且，如果您采用 **Match Usage**（匹配使用情况），这一操作也会替代基于端口的规则，并允许规则显示的所有应用程序，这样做是很危险的，尤其对于 Web 浏览流量。

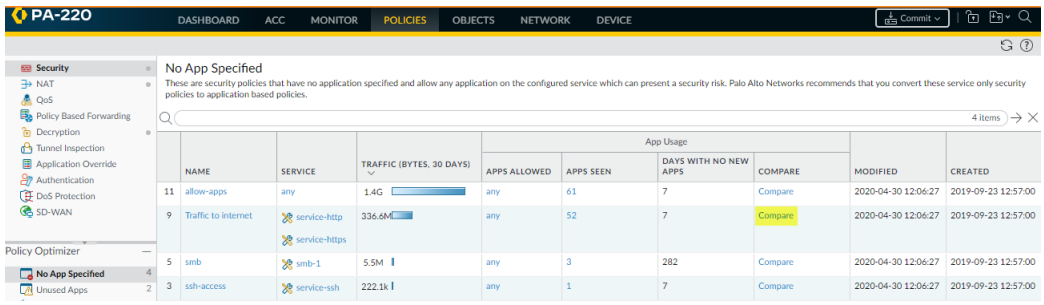
克隆规则可保留基于端口的原始规则，并将克隆规则直接置于规则库中基于端口的规则前面，这样，您就可以监控规则。此外，通过克隆，您还能将可以查看大量不同应用程序的规则（例如，基于端口的 Web 流量规则）拆分为多个基于应用程序的规则，这样，您可以区别对待不同的应用程序组。一旦您确定要允许克隆规则（或规则）中需要允许的所有应用程序，则可以删除基于端口的规则。

在本示例中，通过克隆基于端口的 Web 流量规则，可以为基于 Web 的文件共享流量创建一个基于应用程序的规则（在基于端口的规则中显示的应用程序流量子集）。

STEP 1 | 导航至 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）以查看基于端口的规则。

STEP 2 | 对您想要迁移的规则单击 **Compare**（比较）。

在本示例中，允许 Web 访问的基于端口的规则名为 Internet 流量。



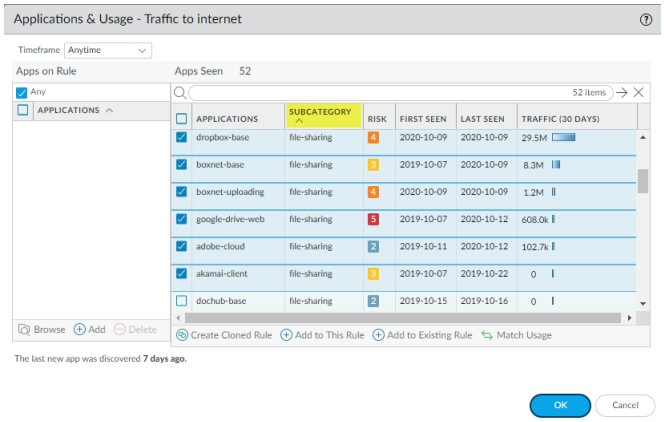



© 2019 Palo Alto Networks, Inc.

STEP 3 | 使用排序选项从 **Apps Seen**（显示的应用程序）中查看并选择您要允许的应用程序。

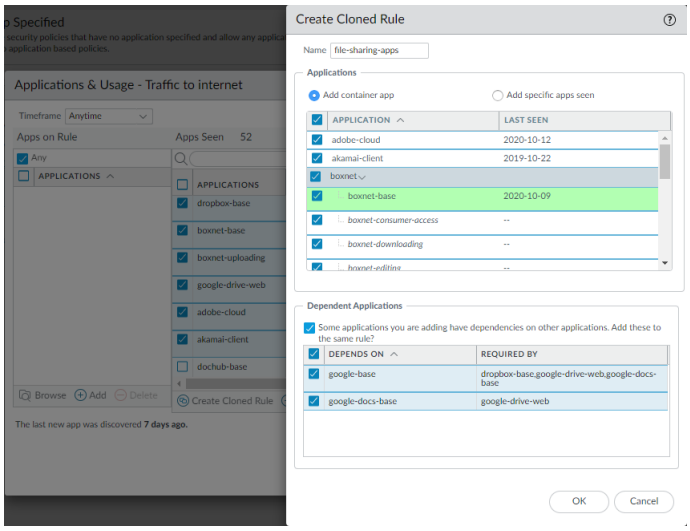
*Apps Seen*（显示的应用程序）数大约每小时更新一次，因此，如果您未看到预计数量的应用程序，请在一小时后再次查看。考虑到防火墙的负载，这些字段的更新可能需要一个小时以上。

例如，单击 **Subcategory**（子类别）以排序应用程序，滚动至文件共享子类别，然后选择想要允许的应用程序。或者，您可以筛选（搜索）文件共享应用程序。




STEP 4 | 单击 **Create Cloned Rule**（创建克隆规则）并 **Name**（命名）克隆规则（本示例中为文件共享应用程序）。

**Create Cloned Rule**（创建克隆规则）可显示选中应用程序（绿色阴影显示）、容器应用程序（灰色阴影显示）、容器中未显示在规则中的各个应用程序（斜体显示）、以及显示在规则中的各个应用程序（普通文本字体显示）。滚动 **Applications**（应用程序）可显示所有容器应用程序及其各自的应用程序。




此外，**Create Cloned Rule**（创建克隆规则）还可显示所选应用程序的相关应用程序。在本例中，一些选中应用程序需要（**Required By**（必须））运行 google-base和 google-docs-base 应用程序。

STEP 5 | 选择想要出现在克隆规则中的应用程序。

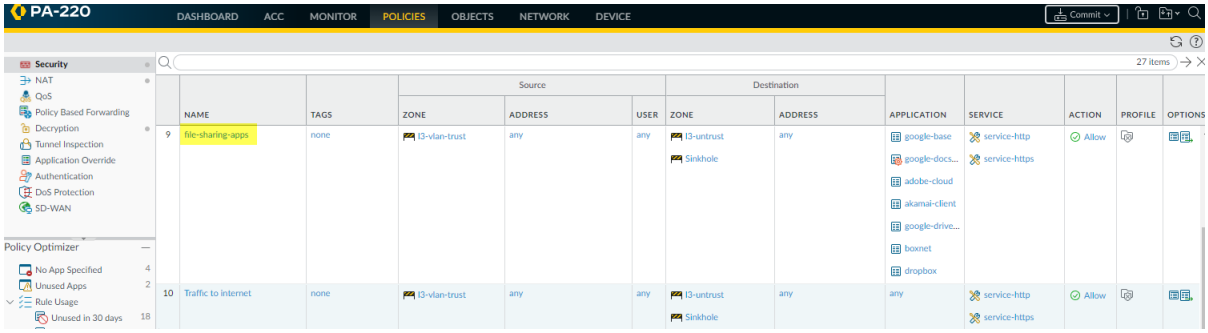
对于不要包含在内的应用程序，取消勾选相应的框，这一操作也会取消勾选容器应用程序。如果不想包含容器应用程序，当新应用程序添加到容器后，无法将这些应用程序自动添加到规则。


© 2019 Palo Alto Networks, Inc.

如果取消勾选容器应用程序，则会取消勾选容器内的所有单个应用程序，然后，您必须选择想要手动添加的应用程序。

STEP 6 | 单击 **OK**（确定）以创建克隆规则。

STEP 7 | 在 **Policies**（策略）> **Security**（安全）中，将克隆规则（文件共享应用程序）插入到规则库中基于端口的原始规则（Internet 流量）的前面。




STEP 8 | 单击规则名称以编辑克隆规则，此克隆规则会继承基于端口的原始规则的属性。

STEP 9 | 在 **Service/URL Category**（服务/URL 类别）选项卡中，从 **Service**（服务）中删除 service-http 和 service-https。

这会将 **Service**（服务）更改为 **application-default**，从而阻止应用程序使用非标准端口，进一步减小攻击面。

如果出于业务需求，您需要允许在特定客户端和服务器之间的非标准端口上运行应用程序（例如，内部自定义应用程序），则将例外限制为必要的应用程序、源和目标。考虑重写自定义应用程序，这样，就可以使用应用程序默认端口。

STEP 10 | 在 **Source**（源）、**User**（用户）和 **Destination**（目标）选项卡中，严格限制规则，将其仅应用于正确位置（区域、子网）出现的正确客户。

例如，您可能决定仅让出于业务目的需要共享 Web 文件的用户组使用 Web 文件共享活动。

STEP 11 | 单击 **OK**（确定）。

STEP 12 | **Commit**（提交）配置。

STEP 13 | 针对基于端口的 Web 访问规则中的其他应用程序类别重复执行此过程，直到基于应用程序的规则仅允许您想要其在您网络上运行的应用程序。

当您想允许的流量在很长一段时间内停止流到基于端口的原始规则，从而可确保不再需要基于端口的规则时，您可以从规则库中删除基于端口的规则。

## 添加应用程序至现有规则

某些情况下，您可能想要添加在基于端口规则上学习（发现的）应用程序至已存在的规则。例如，管理员可能从允许互联网访问（端口 80/443 规则）的基于端口的规则，为常规业务 Web 应用程序创建了一个克隆的、基于应用程序的规则。随后，该管理员注意到基于端口的互联网访问规则发现了更多的常规业务应用程序，并想要将部分或全部应用程序添加至克隆的、基于应用程序的规则（为相同类型的应用程序克隆另一个基于应用程序的规则会创建不必要的规则，并导致规则库复杂化）。

本示例假定用于控制常规业务流量的基于应用程序的安全策略规则已存在，或是已从基于端口的互联网访问规则进行克隆，类似于规则克隆迁移用例：Web 浏览和 SSL 流量。在该示例中，我们从基于端口的互联网



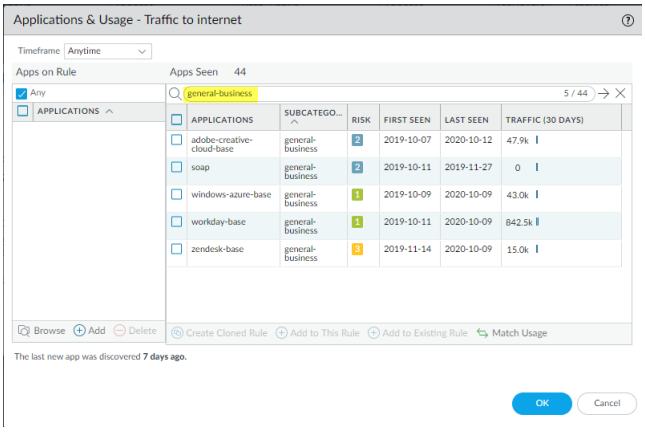
© 2019 Palo Alto Networks, Inc.

访问规则克隆了基于应用程序的规则，并将新规则的服务更改为 application-default（应用程序默认），以防止基于 Web 的应用程序使用非标准端口。

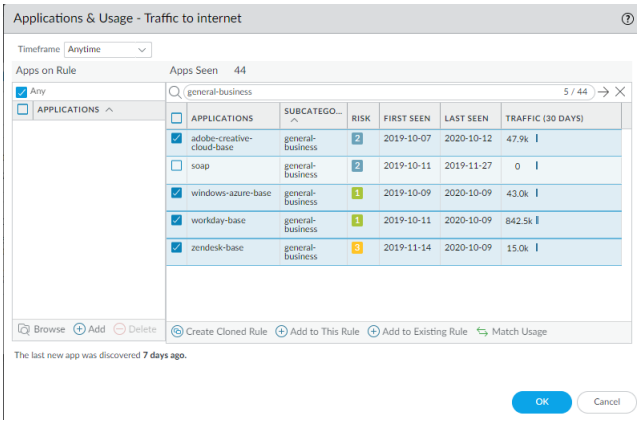


您不仅可以将应用程序添加到现有的基于应用程序的规则，还可将其添加到现有的基于端口的规则。这会使添加到规则的应用程序从基于端口的规则转换为基于应用程序的规则。如果执行此操作，请前往规则，并将服务更改为 *application-default*，以防止应用程序使用非标准端口（此外，规则上配置的服务可能与应用程序不匹配）。

STEP 1 | 检查基于端口的互联网访问规则，发现该规则已看到常规业务应用程序，且需要您允许其中一些应用程序用于业务目的。

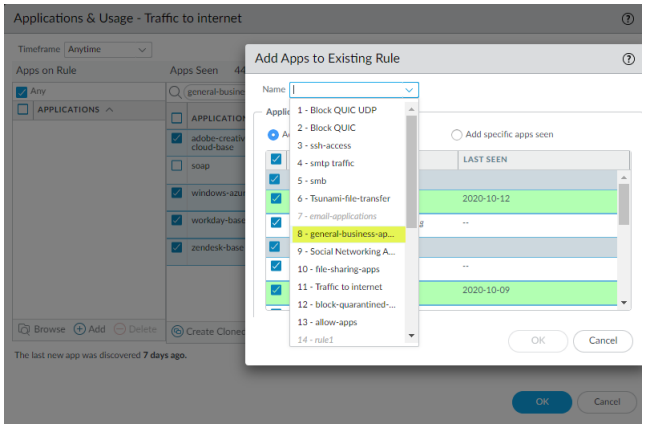



STEP 2 | 选择您想要添加至现有规则的常规业务应用程序。




STEP 3 | 点击 **Add to Existing Rule**（添加至现有规则）并选择您想添加到应用程序的规则 **Name**（名称），此例中，名称为 **general-business-applications**。

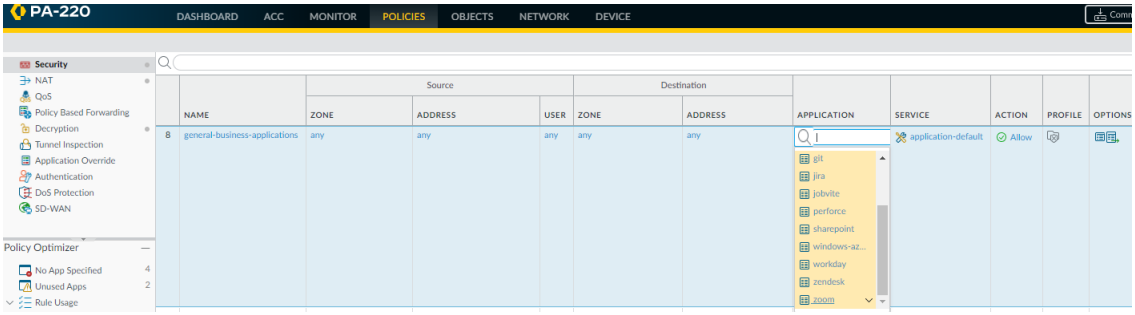

© 2019 Palo Alto Networks, Inc.




STEP 4 | 单击 **Add Apps to Existing Rule**（添加应用程序到现有规则）中的 **OK**（确定），以将选中的应用程序添加到 **general-business-applications**规则中。

STEP 5 | 单击 **Applications & Usage**（应用程序和使用情况）中的 **OK**（确定）。

STEP 6 | 更新后的规则现在将控制规则中原有的应用程序和您刚才添加的应用程序。




# 通过未使用的应用程序识别安全策略规则

如果基于应用程序的安全策略规则允许大量应用程序，您可以删除未使用应用程序（从未出现在规则上的应用程序），以严格管理这些规则，从而仅允许与规则匹配的流量中实际显示的应用程序。最佳做法是标识并删除安全策略规则中的未使用应用程序，这样，可以减小攻击面，从而加强您的安全状态。

STEP 1 | 标识带未使用应用程序的安全策略规则。

**Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Unused Apps**（未使用应用程序）显示采用与规则不匹配（未出现在规则上）的应用程序配置的所有基于应用程序的规则。这意味着这些规则将允许网络上未使用的应用程序（或者，有其他规则将该规则遮盖，使您希望与此规则匹配的流量与规则库中较早规则进行匹配）。

*Apps Allowed*（允许的应用程序）和 *Apps Seen*（显示的应用程序）数大约每小时更新一次，因此，如果您为规则配置了应用程序，且无法查看到预计数量的 *Apps Allowed*（允许的应用程序），请在一小时后再次查看。考虑到防火墙的负载，这些字段的更新可能需要一个小时以上。

STEP 2 | 确定修改带未使用应用程序的规则的优先级。

通过 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Unused Apps**（未使用的应用程序），您可以排序规则（不会影响其在规则库中的顺序），并为您提供其他信息，这有助于您根据业务目标和风险承受能力确定规则清理的优先级。



© 2019 Palo Alto Networks, Inc.

- **Apps Allowed**（允许的应用程序）（允许里诶包上的应用程序数）和 **Apps Seen**（显示的应用程序）（规则上实际显示的允许的应用程序数）之间的差值代表每个规则上配置（而不是实际显示在规则上）的应用程序数，这代表规则过度配置的程度。单击 **Apps Allowed**（允许的应用程序）可根据规则允许的应用程序数进行排序，单击 **Apps Seen**（显示的应用程序）可根据规则上实际显示的应用程序数进行排序。
- **Days with No New Apps**（没有新应用程序的天数）（单击以进行排序）显示自上次新应用程序匹配规则后的天数。这代表规则的成熟度，且不会看到任何尚未显示的应用程序。**Days with No New Apps**（没有新应用程序的天数）越长，新应用程序越不可能匹配规则，您越有可能知道规则允许的所有应用程序。
- 此外，通过 **Created**（创建）和 **Modified**（修改）日期，可以帮助确定规则是否足够成熟，从而了解规则上未显示的应用程序是否可能会在以后显示，或规则是否能够发现预计与规则匹配的所有应用程序。规则被 **Modified**（修改）的时间越长，规则就可能越成熟。（如果 **Created**（创建）和 **Modified**（修改）日期一致，规则就未经过修改。）
- **Hit Count**（命中次数）— 显示所选时间范围内具有最多匹配次数的规则。通过重置命中计数器，指定以天为单位的排除时间段，可以排除规则。因为您不知道计数器已重置，因此，排除最近进行过命中计数器重置操作的规则可防止对显示命中次数比预期少的规则产生误解。

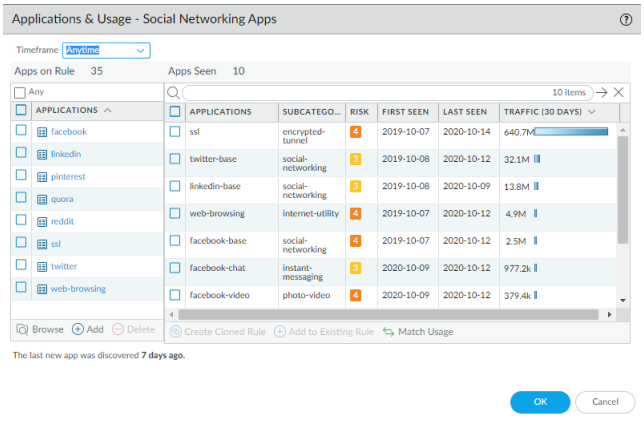


此外，您还可以使用 *Hit Count*（命中次数）以查看策略规则使用情况。

您还可以单击 **Traffic (Bytes, 30 days)**（流量（字节，30 天）），根据过去 30 天内规则发现的流量容量进行排序。使用此信息确定规则修改的优先级。例如，您可以优先考虑 **Apps Allowed**（允许的应用程序）和 **Apps Seen**（显示的应用程序）差值最大的规则，以及具有最长 **Days with No New Apps**（没有新应用程序的天数）的规则，因为这些规则具有最多数量的未使用应用程序，也是最成熟的。

STEP 3 | 查看规则上 **Apps Seen**（显示的应用程序）。

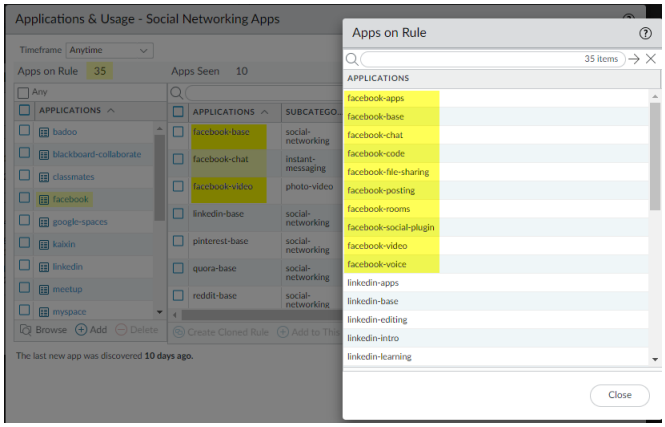
在 **Unused Apps**（未使用的应用程序）上，单击 **Compare**（比较）或 **Apps Seen**（显示的应用程序）列上的数字以打开 **Applications & Usage**（应用程序和使用情况）。其中，显示的是为规则配置的应用程序（**Apps on Rule**（规则上的应用程序））以及规则上 **Apps Seen**（显示的应用程序）。




- **Apps Seen**（显示的应用程序）旁边的数字（在本示例中，为 10）是与规则匹配的应用程序数。请注意，防火墙更新 **Apps Seen**（显示的应用程序）至少需要一小时。
- **Apps on Rule**（规则上的应用程序）旁边的数字（在本示例中，为 35）是指规则上配置的应用程序数，这一结果通过计数容器应用程序中所有应用程序得出（但不是容器应用程序本身 — 如果在规则上配置容器应用程序，则规则允许容器应用程序的各个应用程序）。因为**Applications**（应用程序）列表仅显示为规则手动配置的应用程序，因此，当您在规则上配置容器应用程序时，**Applications**（应用程序）仅显示容器应用程序，而不显示容器内的各个应用程序（除非您还手动为规则配置了单独的应用程序）。因此，**Apps on Rule**（规则上的应用程序）数可能与 **Applications**（应用程序）列表内的应用程序数不一致。
- 单击 **Apps on Rule**（规则上的应用程序）旁边的数字，以查看规则上所有单独应用程序。


© 2019 Palo Alto Networks, Inc.

在本例中，规则有 10 个 **Apps Seen**（显示的应用程序）（与规则匹配的应用程序），但允许 35 个 **Apps on Rule**（规则上的应用程序）。在规则上配置了 **facebook** 容器应用程序，此规则可以查看 facebook-base、facebook-chat 和 facebook-video（**Apps Seen**（显示的应用程序））等单独应用程序的流量。单击 **Apps on Rule**（规则上的应用程序）数字后，**Apps on Rule**（规则上的应用程序）对话框将显示允许的单独应用程序，但不会显示容器应用程序本身。




您无法通过弹出对话框执行应用程序的添加或删除操作。

将规则上 **Apps Seen**（显示的应用程序）与 **Apps on Rule**（规则上的应用程序）进行比较。如果不使用规则上的应用程序（您看不到应用程序，或是您在 **Apps Seen**（显示的应用程序）中的允许容器内看不到应用程序），可考虑删除规则上的应用程序，以缩小攻击范围。考虑到定期使用的应用程序（例如，季度或年度事件），如果在相当长的时间段内未对其执行检查，可能会看起来是未使用的。通过 **Timeframe**（时间段），您可以为规则上**Apps Seen**（显示的应用程序）选择时间段。选择 **Anytime**（任何时间）可查看规则生命周期中显示的每个应用程序。根据在 **No App Specified**（未指定应用程序）对话框中的 **Created**（创建）或 **Modified**（修改）日期以及定期事件的时间间隔，规则在防火墙上出现的时间可能不长，不足以查看所有定期使用的应用程序。

STEP 4 | 删除规则中的未使用应用程序。

通过 **Delete**（删除）（或 **Add**（添加））**Apps on Rule**（规则上的应用程序）中的应用程序，可手动删除（或添加）应用程序；或通过 **Match Usage**（匹配使用情况）添加规则上 **Apps Seen**（显示的应用程序），并删除单击后规则上未出现匹配流量的应用程序。

要手动删除规则中的应用程序，从 **Apps on Rule**（规则上的应用程序）中选择应用程序，并将其 **Delete**（删除）。确保在将应用程序从规则中删除之前，定期事件不会需要此类应用程序。（您还可以通过安全策略规则的 **Application**（应用程序）选项卡删除应用程序。）

通过 **Match Usage**（匹配使用情况），可将规则上 **Apps Seen**（显示的应用程序）移至 **Apps on Rule**（规则上的应用程序），并删除规则中所有未使用的应用程序。

您可以将规则从 *Policies*（策略）> *Security*（安全）和 *No App Specified*（未指定应用程序）克隆到从基于端口迁移至基于 App-ID 安全策略规则。您无法从 *Unused Apps*（未使用的应用程序）开始克隆规则。

STEP 5 | **Commit**（提交）配置。

STEP 6 | 监控更新规则，倾听用户反馈，确保更新规则允许您想要允许的应用程序，且不会无意间阻止定期使用的应用程序。

*Apps Allowed*（允许的应用程序）数和 *Apps Seen*（显示的应用程序）数大约每一小时更新一次。从规则中删除所有未使用的应用程序后，在防火墙更新显示之前，规则会一直出现在 *Policies*（策略）> *Security*（安全）> *Policy Optimzer*（策略优化器）> *Unused*



© 2019 Palo Alto Networks, Inc.

*Apps*（未使用的应用程序）中。当防火墙更新显示，且 *Apps Allowed*（允许的应用程序）数与 *Apps Seen*（显示的应用程序）数一致时，规则不再出现在 *Unused Apps*（未使用应用程序）屏幕中。但是，考虑到防火墙的负载，更新这些字段的可能需要一个小时以上。

## 应用程序使用统计信息的高可用性

当您配置两个防火墙作为高可用性 (HA) 对时，可在生成应用程序流量日志的防火墙上本地查看应用程序使用统计信息。您查看应用程序使用统计信息的位置也部分取决于 HA 配置：

- 主动/被动 — 主动设备生成应用程序使用统计信息。如果被动设备未发现用户流量，则仅主动设备显示应用程序使用统计信息。如果被动设备发现了流量，则被动设备仅显示其所发现流量的应用程序使用统计信息。

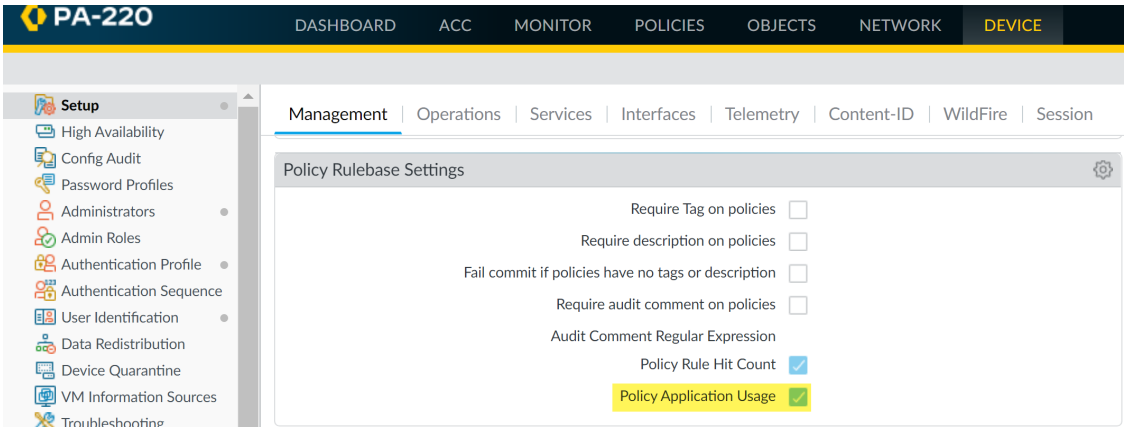
  在故障转移时，应用程序使用统计信息仅基于新的主动设备上生成的流量日志（故障转移之前为被动状态的设备）。
- 主动/主动 — 拥有会话的设备针对该会话生成流量日志，因此，会话的应用程序使用统计信息仅在拥有该会话的设备上可用。如果主动设备拥有一个会话，其他主动设备不会显示该会话的应用程序使用统计信息。

## 如何禁用策略优化器

策略优化器默认启用。策略优化器提供多种功能，以轻松从基于端口迁移至基于 App-ID 安全策略规则和 通过未使用的应用程序识别安全策略规则，以及从规则中移除未使用的应用程序，但您也可以根据需要禁用此功能。

STEP 1 | 导航至 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Policy Rulebase Settings**（策略规则库设置）。

STEP 2 | 勾选 **Policy Application Usage**（策略应用程序使用情况）方框以启用此功能，取消选择方框以禁用此功能。





© 2019 Palo Alto Networks, Inc.

# 应用层网关

Palo Alto Networks 防火墙不按端口和协议对流量进行分类；相反，它根据独特属性和事务特征使用 App-ID 技术识别应用程序。但是，有些应用程序需要防火墙动态打开针孔建立连接、确定会话的参数并协商用于将用于传输数据的端口；这些应用程序使用应用层负载在应用程序打开数据连接的动态 TCP 或 UDP 端口上进行通信。对于这些应用程序，会将防火墙用作应用层网关 (ALG)，并且打开针孔用于限制时间和专门用于传输数据或控制流量。此外，防火墙还会在必要时执行负载的 NAT 重写。

- *H.323*（*H.225* 和 *H.248*）网守路由模式不支持 *ALG*。
- 当将防火墙用作会话发起协议 *(SIP)* 的应用层网关时，它默认对负载执行 *NAT* 重写并为媒体端口打开动态针孔。在某些情况下，根据在环境中使用的 *SIP* 应用程序，*SIP* 端点在其客户端拥有嵌入的 *NAT* 智能。在这种情况下，您可能需要禁用 *SIP ALG* 功能，以防止防火墙修改信令会话。在禁用 *SIP ALG* 后，如果 *App-ID* 确定会话为 *SIP*，则不会转换负载，同时也不会打开动态针孔。请参阅禁用 SIP 应用层网关 (ALG)。

使用动态 *IP* 和端口 *(DIPP) NAT* 时，*Palo Alto Networks* 防火墙 *ALG* 解码器需要 *IP* 和端口（*Sent-by* 地址和 *Sent-by* 端口）在 *SIP* 标头（*Contact* 字段和 *Via* 字段）下组合使用，以便能够转换此标头，并基于此打开预测会话。

下表列出了 IPv4、NAT、IPv6、NPTv6 和 NAT64 ALG，并用复选标记表示 ALG 是否支持各个协议（如 SIP）。

| App-ID | IPv4 | NAT | IPv6 | NPTv6 | NAT64 |
|---|---|---|---|---|---|
| SIP | ✓ | ✓ | ✓ | — | — |
| SCCP | ✓ | ✓ | ✓ | — | — |
| MGCP | ✓ | ✓ | — | — | — |
| FTP | ✓ | ✓ | ✓ | ✓ | — |
| RTSP | ✓ | ✓ | ✓ | ✓ | — |
| MySQL | ✓ | ✓ | — | — | — |
| Oracle/SQLNet/TNS | ✓ | ✓ | ✓ | ✓ | — |
| RPC | ✓ | ✓ | — | — | — |
| RSH | ✓ | ✓ | — | — | — |
| UNIStim | ✓ | ✓ | — | — | — |
| H.225 | ✓ | ✓ | — | — | — |



© 2019 Palo Alto Networks, Inc.

| App-ID | IPv4 | NAT | IPv6 | NPTv6 | NAT64 |
|---|---|---|---|---|---|
| H.248 | ✓ | ✓ | — | — | — |


© 2019 Palo Alto Networks, Inc.

# 禁用 SIP 应用层网关 (ALG)

Palo Alto Networks 防火墙使用会话发起协议 (SIP) 应用层网关 (ALG) 打开启用 NAT 的防火墙中的动态针孔。但是，一些应用程序（如 VoIP）在客户端应用程序中拥有嵌入的 NAT 智能。在这些情况下，防火墙中的 SIP ALG 可能会受到信令会话的影响，并导致客户端应用程序停止运行。

解决此问题的一种解决办法是为 SIP 定义应用程序覆盖策略，但使用这种方法会禁用 App-ID 和威胁检测功能。更好的解决办法是禁用 SIP ALG，这样就不会禁用 App-ID 或威胁检测功能。

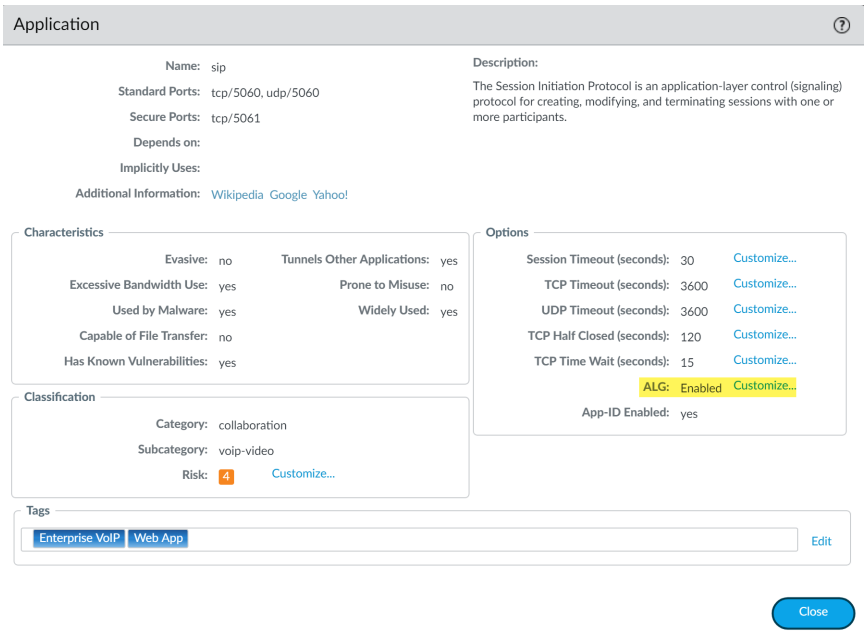
以下步骤介绍了禁用 SIP ALG 的方法。

STEP 1 | 选择**Objects**（对象）> **Applications**（应用程序）。

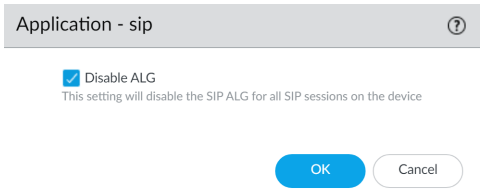
STEP 2 | 选择 **sip** 应用程序。

可以在 **Search**（搜索）框中输入 **sip** 以帮助查找 sip 应用程序。

STEP 3 | 在“应用程序”对话框的“选项”部分中，为 **ALG** 选择 **Customize...**（自定义...）。




STEP 4 | 选中“应用程序 - sip”对话框中的 **Disable ALG**（禁用 **ALG**）复选框，然后单击 **OK**（确定）。




STEP 5 | **Close**（关闭）“应用程序”对话框，然后 **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 使用 HTTP 标头管理 SaaS 应用程序访问

可以使用未约束 SaaS 应用程序实现网络以外敏感信息的传输，通常是通过访问客户版应用程序来完成。但是，如果需要允许特定的个人或组织访问企业版应用程序，则不能完全阻止 SaaS 应用程序。

您可以在允许特定企业帐户时使用自定义 HTTP 标头禁用 SaaS 客户帐户。许多 SaaS 应用程序均基于特定 HTTP 标头中的信息来允许或禁用对应用程序的访问。您可以使用预定义类型创建 HTTP 标头插入条目，以管理对 Google G Suite 和 Microsoft Office 365 等流行的 SaaS 应用程序的访问。Palo Alto Networks® 使用内容更新来维持特定于这些应用程序的预定义规则集，并添加新的预定义规则集。

如果想要管理对使用 HTTP 标头限制服务访问的 SaaS 应用程序的访问，您还可以创建自定义 HTTP 标头插入条目，对此，Palo Alto Networks 未提供预定义规则集。

请注意，商业版 SaaS 应用程序始终使用 SSL，因此，必须进行解密以执行 HTTP 标头插入。如果上游防火墙尚未对流量进行解密，则可以将防火墙配置为使用 SSL 转发代理解密来解密流量。

使用此功能时，无需提供 *URL* 筛选许可证。

要了解如何使用 HTTP 标头管理 SaaS 应用程序，请参阅以下内容：

- 了解 SaaS 自定义标头
- 预定义 SaaS 应用程序类型使用的域
- 使用预定义类型创建 HTTP 标头插入条目
- 创建自定义 HTTP 标头插入条目

## 了解 SaaS 自定义标头

开始之前，您必须了解用于正在管理的 SaaS 应用程序的自定义 HTTP 标头。您需要了解使用这些标头可以完成的操作以及完成目标需要的特定信息。

请注意，使用自定义标头的 SaaS 应用程序并非总是使用这些标头来控制对帐户类型的访问。例如，Palo Alto Networks® 为确定网络用户是否能够访问限制内容的 YouTube 自定义标头提供预定义支持。

此外，您还应读取想要控制对其进行访问的 SaaS 应用程序的文件，这样，您才能了解需要用于该应用程序的标头。

以下限制适用于 *HTTP* 标头插入：

- 标头名称字符长度：*100* 显示动态组定义的两个示例。
- 标头值字符长度：*512*。

请注意，一些 *SaaS* 应用程序可能会定义自定义标头名称，或向这些自定义标头分配一些超出这些限制的值。这种情况很少见，但是，如果 *SaaS* 应用程序超出这些字符长度限制的其中一个或所有，那么您的新一代防火墙将无法成功管理对此 *SaaS* 应用程序的访问。

下表列出了用于 Palo Alto Networks® 为其提供预定义支持的 SaaS 应用程序的标头列表，此外，每个标头还包含一个获取特定标头更多信息的链接。

| 应用程序 | 标头 | 有关详细信息 |
| --- | --- | --- |
| **Dropbox** | `X-Dropbox-allowed-Team-Ids` | www.dropbox.com/help/business/network-control<br>您可以允许访问约束企业版 Dropbox 帐户。该标头的值是企业帐户的团队 Id，您可以从 Dropbox 管理控制 |


© 2019 Palo Alto Networks, Inc.

| 应用程序 | 标头 | 有关详细信息 |
| --- | --- | --- |
| | | 台的网络控制部分获取。此外，您还必须在相同位置启用该功能。<br><br>有关管理该标头以及如何启用 Dropbox 客户端以解密其流量的详细信息，请联系您的 Dropbox 帐户代表。 |
| **Google G Suite** | `X-GooGApps-Allowed-Domains` | support.google.com/a/answer/1668854?hl=en<br><br>您可以从您的域访问特定的 Google 帐户。您赋予该标头的值是您的域和子域。<br><br>为成功插入 Google 应用程序的标头，还必须：<br><br>1. 创建一个包括以下类别和 URL 的 SSL 解密配置文件：<br>• business-and-economy<br>• computer-and-internet-info<br>• content-delivery-networks<br>• internet-communications-and-telephony<br>• low-risk<br>• online-storage-and-backup<br>• search-engine<br>• web-based-email<br>• drive.google.com<br>• *.google.com<br>• *.googleusercontent.com<br>• *.gstatic.com<br>2. HTTP/2 当前不支持 HTTP 标头插入。若要插入标头，请使用相应解密配置文件中的 **Strip ALPN**（剥离 **ALPN**）功能将 HTTP/2 连接降级为 HTTP/1.1。有关详细信息，请参阅应用程序 ID 和 HTTP/2 检查。<br>3. 创建规则以阻止快速 UDP 互联网连接(QUIC) App-ID，并将其置于安全策略的顶部，因为防火墙不支持该协议的标头插入。完成此操作后，应用程序将恢复为使用防火墙在上一步中处理的 HTTP/2 over TLS。 |
| **Microsoft Office 365** | `Restrict-Access-To-Tenants`<br><br>`Restrict-Access-Context` | docs.microsoft.com/en-us/azure/active-directory/active-directory-tenant-restrictions<br><br>您提供的`Restrict-Access-To-Tenants`包含一个想要您的用户进行访问的租户列表。您可以使用注册有租户的任何域以识别该列表中的租户。<br><br>您提供的`Restrict-Access-Context` 包含一个正在设置租户限制的目录 ID。您可以在 Azure 门户中找到您的目录 ID。以管理员身份登录，选择**Azure Active Directory**（**Azure** 活动目录），然后选择**Properties**（属性）。 |
| **YouTube** | `YouTube-Restrict` | support.google.com/a/answer/6214622?hl=en |



© 2019 Palo Alto Networks, Inc.

| 应用程序 | 标头 | 有关详细信息 |
| --- | --- | --- |
| | | 您提供的标头包含想要您的用户进行查看的视频类型的信息。您可以指定设置为**Strict**（严格）或**Moderate**（中等）。有关这些不同设置的详细信息，请参阅 support.google.com/a/answer/6212415。 |

## 预定义 SaaS 应用程序类型使用的域

SaaS 应用程序使用 HTTPS，因此，要将自定义标头插入该流量，必须解密自定义标头。如果使用防火墙提供的转发代理解密来解密自定义标头，则必须首先识别与流量相关的域，然后识别想要解密的特定 HTTPS 流量。下表列出了 Palo Alto Networks® 已为其提供预定义规则的每个 SaaS 应用程序的相关域。

| 应用程序 | 域 |
| --- | --- |
| **Dropbox** | `*.dropbox.com` |
| **G Suite** | `*.google.com`<br>`gmail.com` |
| **Microsoft Office 365** | `login.microsoftonline.com`<br>`login.microsoft.com`<br>`login.windows.net` |
| **YouTube** | `www.youtube.com`<br>`m.youtube.com`<br>`youtubei.googleapis.com`<br>`youtube.googleapis.com`<br>`www.youtube-nocookie.com` |

## 使用预定义类型创建 HTTP 标头插入条目

STEP 1 | 如果无上游设备完成对 HTTPS 流量的解密，请使用配置 SSL 转发代理配置解密。



如果您正在为 *Dropbox* 配置 *SSL* 解密，则您还必须配置 *Dropbox* 客户端，以允许 *SSL* 流量。这些程序专为 *Dropbox* 而设。要获取这些程序，请联系您的 *Dropbox* 帐户代表。

1. 为您正在管理的 SaaS 应用程序**Add**（添加）自定义 URL 类别（**Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别））。
2. 指定类别的 **Name**（名称）。
3. **Add**（添加）特定于您正在管理的 SaaS 应用程序的域，或是特定于想要在标头中插入用户名和域的 SaaS 应用程序的域。要获取用于每个预定义 SaaS 应用程序的域列表，请参阅预定义 SaaS 应用程序类型使用的域。有关配置防火墙以在 HTTP 标头中包含用户名和域的更多信息，请参阅 在 HTTP 标头中插入用户名。

   每个域名最多可包含 254 个字符，每个条目最多可标识 50 个域。域列表支持通配符（例如，**`*.example.com`**）。最佳实践是不要嵌套通配符（例如，**`*.*.*`**），也不要在同一 URL 配置文件中重叠域。



© 2019 Palo Alto Networks, Inc.

4. 对于SaaS 应用程序管理，请创建解密策略规则，然后根据此步骤进行如下配置：
   - 在 **Service/URL Category**（服务/URL 类别）选项卡上， **Add**（添加）您在上一步创建的**URL Category**（URL 类别）。
   - 在 **Options**（选项）选项卡上，务必将 **Action**（操作）设置为 **Decrypt**（解密），将 **Type**（类型）设置为 **SSL Forward Proxy**（SSL 转发代理）。

STEP 2 | 编辑或添加 URL 筛选配置文件。

STEP 3 | 在**URL Filtering Profile**（URL 筛选配置文件）对话框中选择**HTTP Header Insertion**（HTTP 标头插入）。

STEP 4 | **Add**（添加）条目。

1. 指定此条目的 **Name**（名称）（最多 100 个字符）。
2. 选择预定义 **Type**（类型）。

   这可以填充**Domains**（域）和 **Headers**（标头） 列表。
3. 对于每个**Header**（标头），请输入**Value**（值）。
4. （可选）选择**Log**（日志）以启用标头插入活动的日志记录。

   未记录允许流量，因此，允许流量的标头插入情况也不会被记录。
5. 单击 **OK**（确定）保存更改。

STEP 5 | **Add**（添加）或编辑安全策略规则（**Policies**（策略）> **Security**（安全））以将 HTTP 标头插入到 URL 筛选配置文件中。

- 对于 SaaS 应用程序管理，允许用户访问您正在为其配置标头插入规则的 SaaS 应用程序。
- 要将用户名和域包含在 HTTP 标头中，应用 URL 筛选配置文件到 HTTP 或 HTTPS 流量安全策略规则。

1. 选择在步骤 2 编辑或创建的 URL 筛选配置文件（**Actions**（操作）> **URL Filtering**（URL 筛选））。
2. 单击 **OK**（确定）保存，然后 **Commit**（提交）更改。

STEP 6 | 验证防火墙是否正确插入标头。

- 对于 Saas 应用程序管理，从端点开始，确认 Saas 应用程序的访问是否达到您的预期。
  1. 尝试访问您希望能够访问的账户或内容。如果您无法访问 SaaS 账户或内容，则配置无效。
  2. 尝试访问您希望被阻止的账户或内容。如果您能访问 SaaS 账户或内容，则配置无效。
  3. 如果上述两步均如您所愿，您可以查看日志。如果您已在步骤 4.4 配置有日志记录，则可以看到记录的 HTTP 标头插入活动。

## 创建自定义 HTTP 标头插入条目

STEP 1 | 如果无上游设备完成对 HTTPS 流量的解密，请使用配置 SSL 转发代理解密配置解密。

1. 为您正在管理的 SaaS 应用程序**Add**（添加）自定义 URL 类别（**Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（URL 类别））。
2. 指定类别的 **Name**（名称）。
3. 为您正在管理的特定 SaaS 应用程序**Add**（添加）域。
4. 创建解密策略规则，然后根据此过程进行如下配置：
   - 在 **Service/URL Category**（服务/URL 类别）选项卡上， **Add**（添加）您在上一步创建的**URL Category**（URL 类别）。
   - 在 **Options**（选项）选项卡上，务必将 **Action**（操作）设置为 **Decrypt**（解密），将 **Type**（类型）设置为 **SSL Forward Proxy**（SSL 转发代理）。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 编辑或创建 URL 筛选配置文件。

STEP 3 | 在**URL Filtering Profile**（**URL** 筛选配置文件）对话框中选择**HTTP Header Insertion**（**HTTP** 标头插入）。

STEP 4 | **Add**（添加）条目。

1. 指定该条目的 **Name**（名称）。
2. 选择 **Custom**（自定义）作为 **Type**（类型）。
3. **Add**（添加）域到 **Domains**（域）列表。

   您最多可以添加 50 个域，每个域名最多可包含 256 个字符，可以使用通配符（例如：*.example.com）。

   当此列表中的域与 *HTTP* 请求的主机标头的域相匹配时，会发生 *HTTP* 标头插入。

4. **Add**（添加）标头到 **Header**（标头）列表。

   您最多可以添加 5 个标头，每个标头最多可包含 100 个字符，但不能包含任何空格。
5. 对于每个标头r **Value**（值）。
6. （可选）选择**Log**（日志）以启用标头插入活动的日志记录。
7. 单击 **OK**（确定）保存更改。

STEP 5 | **Add**（添加）或编辑允许用户访问您正在为其配置标头插入规则的 SaaS 应用程序的安全策略规则（**Policies**（策略）> **Security**（安全））和安全策略。

1. 选择在步骤 2 编辑或创建的 URL 筛选配置文件（**Actions**（操作）> **URL Filtering**（**URL** 筛选））。
2. 单击 **OK**（确定）保存，然后 **Commit**（提交）更改。

STEP 6 | 验证 SaaS 应用程序的访问方式是否如您所愿。从连接至您网络的端点开始：

1. 尝试访问您希望能够访问的账户或内容。如果您无法访问 SaaS 账户或内容，则配置无效。
2. 尝试访问您希望被阻止的账户或内容。如果您能访问 SaaS 账户或内容，则配置无效。
3. 如果上述两步均如您所愿，您可以查看日志。如果您已在步骤 4.6 配置有日志记录，则可以看到记录的 HTTP 标头插入活动。

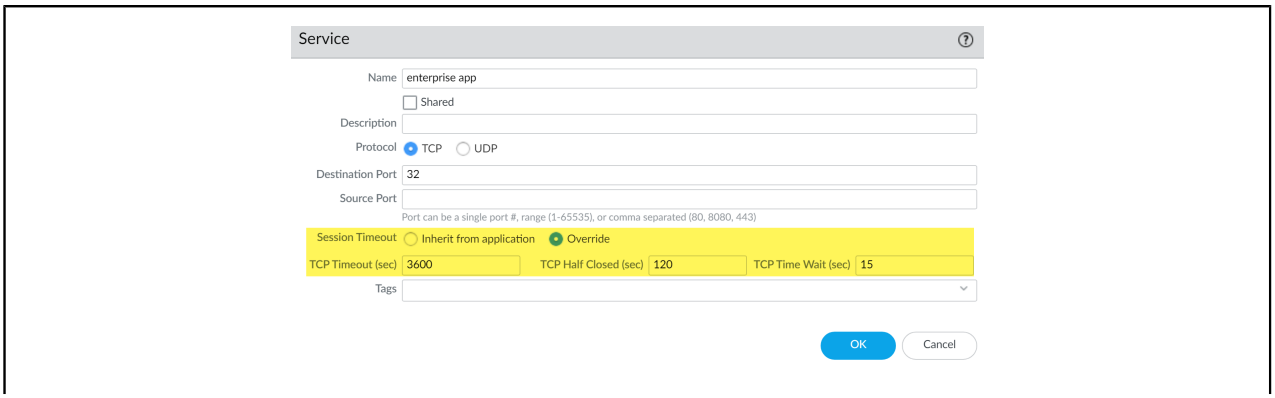


© 2019 Palo Alto Networks, Inc.

# 保留数据中心应用程序的自定义超时

当您从基于端口的策略转移到基于应用程序的策略时，可以轻松保留应用程序的自定义超时。使用此方法以保留自定义超时，而非覆盖 App-ID（丢失应用程序可见性），或创建自定义 App-ID（浪费时间和研究）。

首先，请将自定义超时设置配置为服务对象的组成部分：




然后，在策略规则中添加服务对象以将自定义超时应用至规则适用的应用程序。

以下步骤是关于如何将自定义超时应用至应用程序的描述。要将自定义超时应用至用户组，您可以采用相同的步骤，但必须将服务对象添加至安全策略规则中，该规则适用于您想要应用超时的用户。

STEP 1 | 选择 **Objects**（对象）> **Services**（服务）以添加或修改服务对象。

此外，您还可以在定义安全策略规则的匹配条件时创建服务对象：选择 **Policies**（策略）> **Security**（安全）> **Service/URL Category**（服务/URL 类别），并 **Add**（添加）新的服务对象，以运用至受规则管理的应用程序流量。

STEP 2 | 选择服务需要使用的协议（TCP 或 UDP）。

STEP 3 | 输入服务使用的目标端口号或端口号范围。

STEP 4 | 定义服务的会话超时：

- **Inherit from application**（从应用程序继承）（默认）— 不应用基于服务的超时，而应用应用程序超时。
- **Override**（替代）— 定义服务的自定义会话超时。

STEP 5 | 如果选择覆盖应用程序超时并定义自定义会话超时，请继续：

- 输入 **TCP Timeout**（TCP 超时）值，以设置数据传输开始后 TCP 会话可保持打开的最长时间（以秒为单位）。如果该时间到期，会话将关闭。值范围为 1-604800，默认为 3600 秒。
- 输入 **TCP Half Closed**（TCP 半闭合）值，以设置（在接收第一个 FIN 数据包和接收第二个 FIN 数据包或 RST 数据包之间）会话保持在会话表中范围内的最大时间长度（以秒为单位）。如果计时器到期，会话将关闭。值范围为 1-604800，默认为 120 秒。
- 输入 **TCP Wait Time**（TCP 等待时间）值，以设置（在接收第二个 FIN 数据包或 RST 数据包之后）会话保持在会话表中范围内的最大时间长度（以秒为单位）。如果计时器到期，会话将关闭。值范围为 1-600，默认为 15 秒。

STEP 6 | 单击 **OK**（确定）保存服务对象。

STEP 7 | 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）或修改策略规则，以管理想要控制的应用程序。



© 2019 Palo Alto Networks, Inc.

STEP 8 | 选择 **Service/URL Category**（服务/**URL** 类别），然后 **Add**（添加）您刚刚创建至安全策略规则的服务对象。

STEP 9 | 单击 **OK**（确定）并 **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 设备 *ID*


> Device-ID 概述
> 准备部署 Device-ID
> 配置设备 ID
> 管理设备 ID
> 设备 ID 的 CLI 命令

# Device-ID 概述

无论您的环境是否支持“自带设备”(BYOD)，您的网络中都可能已存在大量设备，甚至数量可能超出您的预期。随着网络上用户及其随附设备数量的增加，对可扩展性的需求也会增加，更不用说不断增长的物联网(IoT) 基础架构，因此，恶意用户利用漏洞的几率会增加，从而形成一个不断增长的风险区域。此外，一旦标识这些设备，您又如何确保这些设备不会因操作软件过时等漏洞而遭受攻击？通过使用防火墙上的 Device-ID™ 或推送来自 Panorama 的策略，您可以获得网络上事件的设备上下文，获取这些设备的策略规则建议，根据设备写入策略，以及根据建议执行安全策略。

与 User-ID 提供基于用户的策略以及 App-ID 提供基于应用程序的策略相似，Device-ID 采用相似方式提供基于设备的策略规则，与其 IP 地址或位置更改无关。通过提供设备的可追溯性以及将网络事件与特定设备相关联，Device-ID 允许您获取事件如何与设备关联的上下文，并写入与设备（而不是会随时间发生变化的用户、位置或 IP 地址）关联的策略。您可以在安全性、解密、服务质量 (QoS) 和身份验证策略中使用 Device-ID。

*Device-ID* 需要 *IoT Security* 证书、*Cortex* 数据湖 *(CDL)* 许可证以及设备证书。

如果防火墙运行的是 PAN-OS 8.1.0 到 PAN-OS 9.1.x 版本，则 IoT Security 许可证可为设备提供设备分类、行为分析和威胁分析。如果使用的是 PAN-OS 10.0 或更高版本，您可以使用 Device-ID 获取 IP 地址到设备映射以查看设备的网络事件上下文，使用 IoT Security 以获取这些设备的策略规则建议，并在报告和 ACC 中获得设备的可见性。

您可以在运行 *PAN-OS* 版本 *10.0* 或更高版本的任何 *Panorama* 或防火墙上创建基于设备的安全策略。若要要实施安全策略，设备必须拥有有效的 *IoT Security* 许可证。

若要标识并分类设备，IoT Security 应用程序应使用防火墙上日志、网络协议和会话的元数据。这不包括与设备标识无关的私人或敏感信息或数据。元数据还可作为确定设备预期行为的依据，然后，基于这种行为可建立用于定义设备允许的流量和协议的策略规则建议标准。

IoT Security 使用网络中存在的 Palo Alto Networks 防火墙标识并分类网络中的设备后，您无需部署新的设备或第三方解决方案，Device-ID 可以利用此数据将设备与策略规则匹配，并提供网络事件的设备上下文。通过防火墙或 Panorama 提供的流量、应用程序、用户、设备和威胁可见性，您可以立即将网络事件追溯到单个设备，并获取用于保护这些设备的安全策略规则建议。

所有支持 *PAN-OS 10.0* 的防火墙平台均支持 *Device-ID* 和 *IoT Security* 应用程序，但 *VM-50* 系列、*VM-200*、*CN* 系列和 *Prisma Access* 除外。

设备有六级分类（也称为属性）：

| 属性 | 示例 |
| --- | --- |
| 类别 | ATM 机；3D 打印机 |
| 配置文件 | Palo Alto Networks 设备 |
| 模型 | iPad |
| 操作系统版本 | iOS 9.9.3 |
| OS 系列 | Android; iOS |



© 2019 Palo Alto Networks, Inc.

| 属性 | 示例 |
| --- | --- |
| 供应商 | ASUS；Philips |

为获取网络中设备的策略规则建议，防火墙会观察流量，从而生成增强应用程序日志 (EAL)。随后，防火墙将 EAL 转发至 Cortex 数据湖 (CDL) 进行处理。中心上的 IoT Security 应用程序接收来自 CDL 的日志进行分析，提供 IP 地址到设备映射，并为您的设备生成最新策略规则建议。通过 IoT Security 应用程序，您可以查看这些策略规则建议，并为这些设备创建安全策略。激活 IoT Security 应用程序中的策略规则后，将这些规则导入防火墙或 Panorama，并提交您的安全策略。

防火墙必须能够观测网络上的 DHCP 广播和单播流量以标识设备。防火墙观测的流量越多，为设备提供的策略规则建议就越准确，就能更快、更准确地为设备提供 IP 地址到设备映射。一旦设备发送 DHCP 流量以获取 IP 地址，防火墙就会观察此类请求，并生成可发送到 Cortex 数据湖以供 IoT Security 进行处理和分析的 EAL。



若要观测 *L2* 接口上的流量，必须为该接口配置 *VLAN*。通过允许防火墙将该接口作为 *DHCP* 中继的 *L3* 接口进行处理，就可以在不影响流量或性能的情况下观测 *DHCP* 广播流量。

由于防火墙需要根据流量检测设备，然后为这些设备实施安全策略，因此，防火墙既充当用于收集设备元数据的传感器，又充当为设置实施安全策略的执行器。IoT Security 应用程序将在新设备发送 DHCP 流量时自动对其进行检测，在第一周内就可标识 95% 的设备。

每个应用程序通常都有一个可导入到防火墙或 Panorama 的单独建议。导入建议时，防火墙或 Panorama 至少会从建议创建两个用于定义设备行为的对象：

- 在流量来源处标识设备的源设备对象
- 一个或多个用于标识所允许流量目标的目标对象，这可以是设备、IP 地址或完全限定域名 (FQDN)

如果防火墙或 Panorama 已经存在任何设备对象，则防火墙或 Panorama 将更新设备对象，而不是新建一个设备对象。您可以在安全、身份验证、解密和服务质量 (QoS) 策略中使用这些设备对象。

防火墙还将用于标识源设备的标记与充当 IoT Security 策略规则建议的规则相关联。



一旦标记不同步，要恢复映射，只能将标记与规则关联，因此，切勿编辑或删除标记。

为了实现 Device-ID 的最佳部署和操作，我们建议执行以下最佳实践：

- 将 Device-ID 部署到位于网络中心的防火墙上。例如，如果您的环境规模较大，可以将 Device-ID 部署到 IP 地址管理 (IPAM) 设备上游的防火墙上。如果您的环境规模较小，可将 Device-ID 部署到充当 DHCP 服务器的防火墙上。
- 在初始部署期间，应允许 Device-ID 至少可在 14 天内从您的网络中收集元数据。如果设备不是每天都活动，标识过程可能会更长。
- 按最关键到最不关键设备的顺序写入基于设备的策略。按如下类别优先排序：
  1. 类别（首先是安全网络设备）
  2. 关键设备（例如，服务器或 MRI 机器）
  3. 特定于环境的设备（例如，火灾报警器和胸卡读卡器）
  4. 面向消费者的 IoT 设备（例如，智能手表或智能音箱）
- 按区域启用 Device-ID（仅针对内部区域）。


© 2019 Palo Alto Networks, Inc.

# 准备部署 Device-ID

要准备用于 Device-ID 部署的网络，请完成下列预部署任务，使防火墙生成并发送增强应用程序日志 (EAL) 到 Cortex 数据湖，以供用于生成策略规则建议的 IoT Security 进行处理和分析。

STEP 1 | 如果尚未执行此操作，请在防火墙或 Panorama 上安装设备证书。

STEP 2 | 激活 Cortex 数据湖 (CDL) 实例，并将防火墙与该实例连接。

1. 激活 Cortex 数据湖实例。
2. 将防火墙与 Cortex 数据湖连接。

STEP 3 | （仅限 L2 接口）为每个 L2 接口创建一个 VLAN 接口，这样，防火墙就可以观测 DHCP 广播流量。

STEP 4 | （可选）配置服务路由以允许 Device-ID 和 IoT Security 的必要流量。

默认情况下，防火墙使用管理接口。若要使用其他接口，请执行以下步骤。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后选择 **Service Route Configuration**（服务路由配置）。
2. **Customize**（自定义）服务路由。
3. 选择 **IPv4** 协议。



*Device-ID* 和 *IoT Security*不支持 *IPv6*。

4. 在服务列中选择 **Data Services**（数据服务）。
5. 选择 **Source Interface**（源接口）和 **Source Address**（源地址）。
6. 双击 **OK**（确定）。

STEP 5 | 使用 App-ID 以允许 Device-ID 和 IoT Security 的必要流量。

- 使用 **paloalto-iot-security** App-ID 以允许 IoT Security 应用程序与防火墙或 Panorama 之间的流量。



如果防火墙通过与 *CDL* 和 *IoT Security* 位于同一区域的数据接口发送来自管理接口的流量，则不需要此 *App-ID*。仅当流量横跨多个安全区域时，才需要使用此 *App-ID*。

- 使用 **paloalto-logging-service** App-ID 以允许所有 EAL 和所有会话日志的流量。
- 使用 **paloalto-updates** App-ID 以允许检索 IoT Security 动态更新和设备目录更新。
- 使用 **paloalto-iot-security** App-ID 以允许检索策略规则建议。



如果防火墙之间存在一个使用 *Device-ID* 和互联网的非 *Palo Alto Networks* 防火墙，请验证此非 *Palo Alto Networks* 防火墙是否能够访问 *iot.services-edge.paloaltonetworks.com:443*。

STEP 6 | 将防火墙配置为观察并生成 DHCP 流量日志，然后转发日志以供 IoT Security 进行处理和分析。

- 如果防火墙充当 DHCP 服务器：
  1. 启用增强应用程序日志记录。
  2. 创建 日志转发配置文件以将日志转发到 CDL 进行处理。
  3. 启用 **DHCP Broadcast Session**（**DHCP** 广播会话）选项（**Device**（设备）> **Setup**（设置）> **Session**（会话）> **Session Settings**（会话设置））。
  4. 创建安全策略规则以允许 **Application**（应用程序）类型 **dhcp**。



© 2019 Palo Alto Networks, Inc.

- 如果防火墙不是 DHCP 服务器，请配置一个充当DHCP 中继代理的接口，这样，防火墙可为从客户端接收的 DHCP 流量生成 EAL。
- 如果 DHCP 服务器与防火墙接口位于同一网段，请在 DHCP 服务器之前部署一个虚拟线路接口，确保防火墙可在首次 DHCP 交换时为所有数据包生成 EAL，且对性能的影响最小。

  1. 配置相应区域的虚拟线路接口，并启用 **Multicast Firewalling**（多播防火墙）选项（**Network**（网络）> **Virtual Wires**（虚拟线路）> **Add**（添加））。
  2. 配置规则以允许往返于虚拟线路区域之间 DHCP 服务器的 DHCP 流量。该策略必须允许服务器当前观测到的所有现存流量，并使用同一日志转发配置文件充当剩余规则。
  3. 若要允许 DHCP 服务器检查 IP 地址是否在将其作为租借分配给新请求之前就已激活，请配置规则以允许从 DHCP 服务器到剩余子网执行 ping。
  4. 配置规则以允许不会转发日志进行流量匹配的 DHCP 服务器之间的所有其他流量。
  5. 配置 DHCP 服务器主机以使用第一个虚拟线路接口，并配置网络交换机以使用第二个虚拟线路接口。为最大限度地减少接线，您可以在交换基础结构中使用隔离的 VLAN，而不是将 DHCP 服务器主机直接与防火墙连接。
- 如果要使用旁接接口来获得对防火墙通常因当前配置或网路拓扑结构无法观察到的 DHCP 流量的可见性，最佳做法是使用以下配置。

  1. 配置 旁接接口和相应区域。
  2. 配置规则以匹配使用同一日志转发配置文件充当剩余规则的 DHCP 流量。
  3. 为减少防火墙上的会话负载，请配置规则以丢弃所有其他流量。
  4. 将旁接接口与网络交换机上的端口镜像连接。

STEP 7 | 添加会话日志类型到日志转发配置文件。

如果日志转发配置文件中没有现存条目，请选择**Enable enhanced application logging to Cortex Data Lake (including traffic and url logs)**（启用对 **Cortex** 数据湖的增强应用程序日志记录（包括流量和 **url** 日志））选项以添加所有日志条目。

1. **Add**（添加）新配置文件，并输入名称。
2. 选择 **traffic**（流量）作为 **Log type**（日志类型）。
3. 选择 **All logs**（所有日志）作为 **Filter**（筛选器）。
4. 选择 **Cortex Data Lake**（**Cortex** 数据湖）选项。
5. 单击 **OK**（确定）。
6. 对 **threat**（威胁）重复子步骤 1-5，如果您有订阅，请选择 **wildfire** 日志类型。


© 2019 Palo Alto Networks, Inc.

# 配置设备 ID

完成以下任务，将 IP 地址到设备映射和策略规则建议从 IoT Security 导入到防火墙或 Panorama。

STEP 1 | 在中心激活 IoT Security 许可证。

1. 根据电子邮件中的说明激活您的 IoT Security 许可证。
2. 初始化 IoT Security 应用程序。有关详细信息，请参阅 IoT Security 入门和 IoT Security 最佳实践。
3. 将许可证应用于想要将其用于执行 IoT 安全策略的防火墙。
4. 刷新防火墙或 Panorama 上的许可证。

STEP 2 | 定义 IoT Security 应用程序上的 IoT 安全策略。

1. 在IoT Security 应用程序上，选择源设备对象。
2. 为源设备对象**Create**（创建）一组新的策略规则。

   有关 IoT Security 的详细信息，请参阅 IoT Security 入门。
3. **Activate**（激活）策略规则以确认更改。

STEP 3 | 将 IP 地址到设备映射和策略规则建议导入防火墙或 Panorama。

1. 导入策略规则建议。
   - 在防火墙上，选择 **Device**（设备）> **Policy Recommendation**（策略建议）。
   - 在 Panorama 上，选择 **Panorama** > **Policy Recommendation**（策略建议），然后将策略规则推送到 Panorama 管理的策略规则。

   推送策略到防火墙后，必须在防火墙上执行同步策略规则，以创建策略规则建议到策略规则映射。

   选择策略建议后，防火墙或 Panorama 将与 IoT Security 进行通信，以获得最新的策略规则建议。策略规则建议不会缓存在防火墙或 Panorama 上。

   由于 *IoT Security* 利用设备可信行为创建策略规则建议，因此，规则默认操作为“允许”。
2. 选择 **Source Device Profile**（源设备配置文件）。
3. 确认 **Destination Device Profile**（目标设备配置文件）以及允许的 **Applications**（设备）是否正确。
4. 选择 **Import Policy Rules**（导入策略规则）以导入策略规则。
5. （仅限 Panorama）选择想要导入策略规则的设备组的 **Location**（位置）。
6. 输入策略规则的 **Name**（名称）。
7. （仅限 Panorama）选择 **Destination Type**（目标类型）（**Pre-Rulebase**（前导规则库）或 **Post-Rulebase**（后继规则库））。
8. 选择用于定义规则库中规则位置的 **After Rule**（后继规则）。
   - **No Rule Selection**（不选择规则）— 将规则置于规则库顶部。
   - **Default One**（默认一个）— 将规则置于所列规则之后。

   在安全策略中，设备 *ID* 必须位于应用于设备的任何现有规则之前。
9. 针对每个策略规则建议重复此过程，以创建规则，从而允许各个设备对象访问相应目标。
10. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 4 | 启用想要使用设备 ID 的所有区域中的设备 ID，以检测设备，实施安全策略。

设备 ID 默认映射启用设备 ID 的区域内所有子网。您可以在 **Include List**（包括列表）和 **Exclude List**（排除列表）中修改设备 ID 要映射的子网。



© 2019 Palo Alto Networks, Inc.

最佳做法是在源区域启用设备 *ID* 以检测设备，实施安全策略。您只能为内部区域启用设备 *ID*。

1. 选择**Network**（网络）> **Zones**（区域）。
2. 选择想要启用设备 ID 的区域。
3. **Enable Device Identification**（启用设备标识），然后单击 **OK**（确定）。

STEP 5 | **Commit**（提交）更改。

STEP 6 | 检验安全策略是否正确。

1. 选择 **Policies**（策略），然后选择从策略规则建议创建的规则。

   IoT Security 分配的 **Description**（说明）中包括源设备对象和用于标识源设备对象的 **Tags**（标记），并说明了此规则是 IoT Security 的建议。

   设备对象名称必须是唯一的。

2. 选择 **Source**（源）选项卡，然后验证 **Source Device Profile**（源设备配置文件）。
3. 选择 **Destination**（目标）选项卡，然后验证 **Destination Device Profile**（目标设备配置文件）。
4. 选择 **Application**（应用程序）选项卡，然后验证 **Applications**（应用程序）。
5. 选择 **Actions**（操作）选项卡，然后验证 **Action**（操作）（默认为 **Allow**（允许））。
6. 使用 Explore（探索）确认 CDL 是否收到您的日志，然后查看 CDL 接收到的日志。

STEP 7 | 为任何尚未拥有 IoT Security 策略规则建议的设备创建自定义设备对象。

例如，如果您无法通过安全策略建议确保笔记本电脑和智能手机等设备的安全，则必须为这些设备类型手动创建可以在您安全策略中使用的设备对象。有关自定义设备对象的详细信息，请参阅管理设备 ID。

STEP 8 | 使用设备对象实施策略规则，监控并标识潜在问题。

下表包含设备对象用例的一些示例。

- 在安全、身份验证、QoS 和解密策略中使用源设备对象和目标设备对象。
- 使用解密日志标识故障，并标识对解密最关键的资产。
- 在 ACC 中查看设备对象活动以跟踪新设备和设备行为。
- 使用设备对象创建自定义报告（例如，用于事件报告或审核）。


© 2019 Palo Alto Networks, Inc.

# 管理设备 ID

根据需要执行下列任务，确保策略规则建议和设备对象保持最新，或恢复策略规则建议映射。

STEP 1 | 每当建议的 **New Updates Available**（新更新可用）列显示为 **Yes**（是），更新策略规则建议。

随着设备获得新的功能，IoT Security 会更新策略规则建议，从而建议防火墙或 Panorama 应允许的其他流量或协议。每日检查 IoT Security 以获取更新，并尽快更新策略规则建议。

1. 在 IoT Security 应用程序上，**Edit**（编辑）策略规则，然后单击 **Next**（下一步）。
2. 选择新建议，并单击 **Next**（下一步）。
3. **Save**（保存）更改。
4. 在防火墙或 Panorama 上，单击 **Import Policy Rules**（导入策略规则），然后单击 **Yes**（是）以确认您要替换当前规则。

   此操作将替换规则的建议，而不是规则本身。
5. （仅限 Panorama）为所有设备组重复上一步。
6. **Commit**（提交）更改。

STEP 2 | 查看、更新并维护设备目录中的设备对象。

您必须为任何尚未拥有 *IoT Security* 策略规则建议的设备创建设备对象。例如，您无法通过 *IoT Security* 策略规则建议确保笔记本电脑和智能手机等设备的安全，您必须为这些类型的设备创建设备对象，并在安全策略中使用这些对象，以确保这些设备的安全。

1. 选择 **Objects**（对象）> **Devices**（设备）
2. **Add**（添加）设备对象。
3. **Browse**（浏览）列表或使用关键字 **Search**（搜索）。

   搜索结果包括多种类型的设备对象属性（例如，**Category**（类别）和 **Profile**（配置文件））。
4. 若要添加自定义设备对象，请输入该设备对象的 **Name**（名称）和 **Description**（说明）（可选）。

   必须为每个设备对象使用唯一名称。切勿从策略规则建议中更改设备对象说明的标记。
5. （仅限 Panorama）选择 **Shared**（已共享）选项，使该设备对象可用于其他设备组。
6. 选择设备对象属性（**Category**（类别）、 **OS**、**Profile**（配置文件）、**Osfamily**、 **Model**（型号）和 **Vendor**（供应商））。
7. 单击 **OK**（确定）以确认您的更改。

STEP 3 | 在某些情况下（例如，如果您恢复之前的配置），策略规则建议到策略规则映射可能不同步。您还必须在将策略规则从 Panorama 推送到 Panorama 管理的防火墙之后，同步各个防火墙上的映射。要同步映射，请执行以下操作：

- 在防火墙上，选择 **Device**（设备）> **Policy Recommendation**（策略建议）> **Sync Policy Rules**（同步策略规则）
- 在 Panorama 上，选择 **Panorama** > **Policy Recommendation**（策略建议）> **Sync Policy Rules**（同步策略规则）。

防火墙或 Panorama 扫描规则库内所有规则以检查将规则标识为 IoT Security 策略规则建议的标记，获取源设备对象信息，并重新填充本地策略规则建议数据库。



© 2019 Palo Alto Networks, Inc.

STEP 4 | 删除任何不再需要的策略规则建议。

如果不再使用策略规则建议，您可以删除策略规则建议。您还必须删除策略规则建议中的规则以实施更新后的安全策略。

1. 在 IoT Security 应用程序上，选择 **Delete**（删除）。
2. 单击**Mark as Removed**（标记为已删除）以选择此建议进行删除。
3. 删除映射。
   - 在防火墙上，选择 **Device**（设备）> **Policy Recommendation**（策略建议）> **Remove Policy Mapping**（删除策略映射）。
   - 在 Panorama 上，选择 **Device**（设备）> **Policy Recommendation**（策略建议）> **Remove Policy Mapping**（删除策略映射），然后选择您想从中删除映射的 **Location**（位置）。
4. 单击 **Yes**（是）以确认删除映射。
5. 选择 **Policies**（策略）> **Security**（安全）。在 Panorama 中，选择**Policies**（政策）> **Security**（安全）> **Pre-Rules/Post-Rules**（前导规则/后继规则）。
6. 选择您想删除的策略规则建议中的规则，然后选择 **Delete**（删除）。
7. **Commit**（提交）更改。

STEP 5 | 使用 CLI 命令对防火墙和 IoT Security 之间的任何问题进行故障排除。



© 2019 Palo Alto Networks, Inc.

# 设备 ID 的 CLI 命令

使用以下 CLI 命令查看有关对防火墙和 IoT Security 之间的任何问题进行故障排除的信息。通常，包含 **eal** 的 CLI 命令显示传出数据计数器，而包含 **icd** 的 CLI 命令显示传入数据计数器。

| 示例 | 命令 |
| --- | --- |
| 查看增强型应用程序日志记录 (EAL) 计数器，例如防火墙和 Cortex 数据湖之间的连接数以及日志量。 | **show iot eal all** |
| 查看更多有关防火墙与 Cortex 数据湖之间连接的详细信息。 | **show iot eal conn** |
| 按平面（数据平面或管理平面）查看 EAL 计数器摘要，例如 PAN-OS 版本和序列号。 | **show iot eal dpi-eal** |
| 按平面（数据平面或管理平面）以及按协议查看 EAL 计数器。 | **show iot eal dpi-stats all** |
| 按协议查看 EAL 计数器。 | **show iot eal dpi-stats subtype dhcp\|http** |
| 查看主机信息配置文件 (HIP) 匹配报告计数器摘要。 | **show iot eal hipreport-eal** |
| 查看 EAL 日志响应时间计数器。 | **show iot eal response-time** |
| 查看防火墙和 IoT Security 应用程序之间边缘服务连接的详细运行状况信息，以及 IP 地址到设备映射和策略规则建议计数器。 | **show iot icd statistics all** |
| 查看边缘服务连接计数器。 | **show iot icd statistics conn** |
| 查看 IP 地址到设备映射计数器。 | **show iot icd statistics verdict** |
| 查看防火墙上所有 IP 地址到设备映射。 | **show iot ip-device-mapping-mp all** |
| 查看特定 IP 地址的 IP 地址到设备映射。 | **show iot ip-device-mapping-mp ip *IP-address*** |
| 查看数据平面上 IP 地址到设备映射列表。 | **show iot ip-device-mapping all** |
| 清除管理平面上 IP 地址到设备映射。 | **debug iot clear-all type device** |
| 清除数据平面上 IP 地址到设备的映射。 | **clear user-cache all** |

# 威胁防护

Palo Alto Networks® 下一代防火墙可防止和阻止您的网络免遭商品威胁和高级持续性威胁 (APT)。防火墙的多管齐下的检测机制包括基于签名（IPS/命令和控制/抗病毒）的方法、基于启发式（Bot 检测）的方法、基于沙箱 (WildFire) 的方法和基于第 7 层协议分析 (App-ID) 的方法。

商品威胁攻击不是太复杂，可以在防火墙上结合使用抗病毒、防间谍软件、漏洞防护功能以及 URL 筛选和应用识别功能很容易地检测和阻止。

高级威胁是有组织的网络攻击者利用复杂的攻击向量以您的网络为攻击目标进行攻击，最常见的高级威胁为知识产权盗窃和财务数据盗窃。这些威胁非常具有逃避性，因此需要智能监控机制来获取有关恶意软件的详细的主机和网络取证。Palo Alto Networks 下一代防火墙与 WildFire™ 和 Panorama™ 一起提供用于拦截和破坏攻击链的综合解决方案，并且能够让您深入了解如何在网络基础设施（包括移动和虚拟化）上防止安全侵犯。



实施威胁防护配置后，导出配置表格数据，为您的配置创建 *PDF* 或 *CSV* 格式的报告，以用于内部审核或审核。

- 防止网络免遭第 4 层和第 7 层逃避的最佳实践
- 设置防病毒威胁、防间谍软件和漏洞保护
- DNS 安全
- 使用 DNS 查询来确定网络上受感染的主机
- 设置数据筛选
- 预定义的数据筛选模式
- 创建数据筛选配置文件
- WildFire Inline ML
- 设置文件阻止
- 防止暴力攻击
- 自定义暴力签名的操作和触发条件
- 启用规避签名
- 监控阻止 IP 列表
- 威胁签名类别
- 创建威胁异常
- 自定义签名
- 进一步了解和评估威胁
- 与 Palo Alto Networks 共享威胁情报
- 威胁阻止资源

# 防止网络免遭第 4 层和第 7 层逃避的最佳实践

要监控和防止网络免遭大多数第 4 层和第 7 层攻击，以下是一些建议。

- 升级到最新的 PAN-OS 软件版本和内容版本，以确保您拥有最新的安全更新。请参阅安装内容和软件更新。
- 启用 DNS 安全（需要威胁防护和 DNS 安全订阅许可证）来 sinkhole 恶意 DNS 请求。Palo Alto Networks 建议在防间谍软件配置文件中使用下列 DNS 安全类别配置设置：

| SIGNATURE SOURCE | LOG SEVERITY | POLICY ACTION | PACKET CAPTURE |
|---|---|---|---|
| : Palo Alto Networks Content | | | |
| default-paloalto-dns | | sinkhole | extended-capture |
| : DNS Security | | | |
| Command and Control Domains | critical | sinkhole | extended-capture |
| Dynamic DNS Hosted Domains | medium | sinkhole | disable |
| Grayware Domains | high | sinkhole | disable |
| Malware Domains | high | sinkhole | disable |
| Parked Domains | medium | sinkhole | disable |
| Phishing Domains | high | sinkhole | disable |
| Newly Registered Domains | medium | sinkhole | disable |

  - 对于日志严重性设置，请使用以下设置：
    - 将命令和控制域设为关键。
    - 将灰色软件域、恶意软件域和网络钓鱼域设为“高”。
    - 将动态 DNS 托管域、新注册的域以及寄放域设为“中”。
  - 对于策略操作，将所有签名源设为 **sinkhole**。
  - 对于数据包捕获，将命令和控制域设为扩展捕获。将所有其他类别保留为默认设置。

  更多有关防间谍设置的信息，请参阅最佳实践 Internet 网关防间谍配置文件。
- 设置防火墙充当代理并启用规避签名：

  *DSN* 代理不属于防火墙安全策略引擎；相反，它会在保持域到 *IP* 映射的同时引导防火墙解析 *DNS* 主机名，这对于防止 *TLS/HTTP* 规避至关重要。

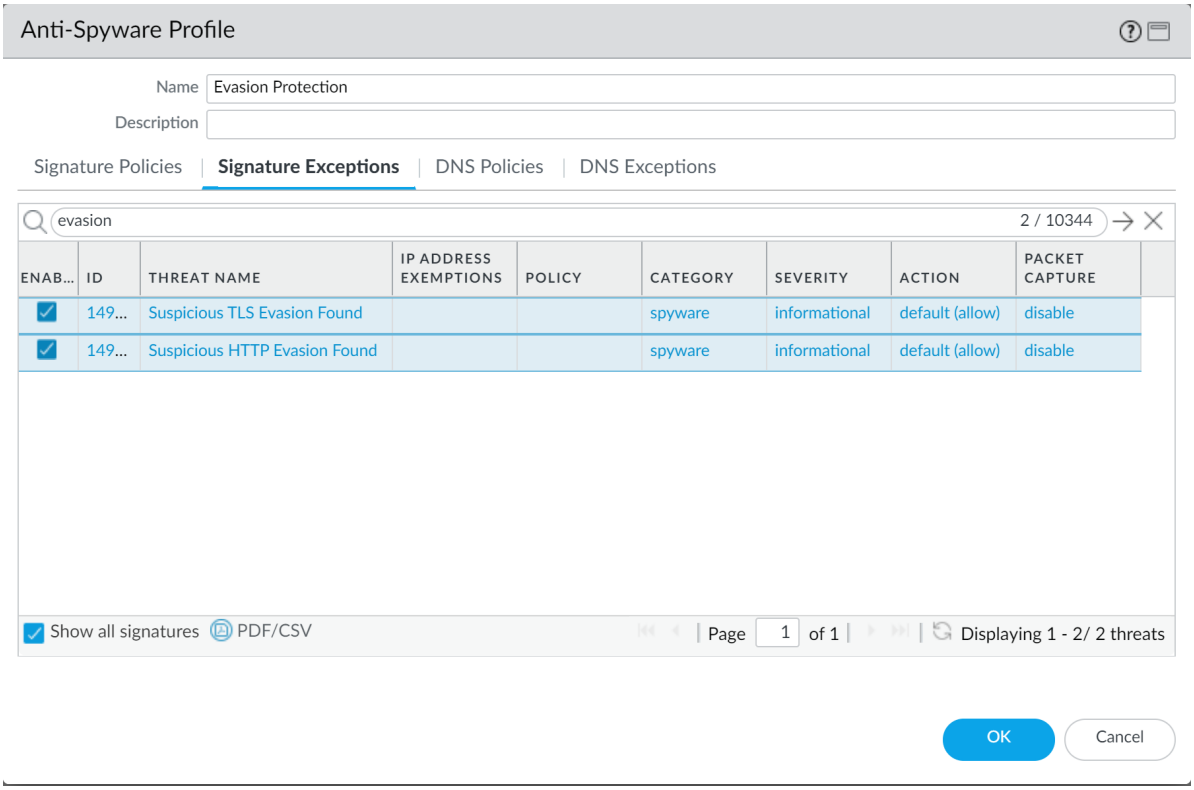
  - 配置 DNS 代理对象。

    作为 DNS 代理，防火墙解析 DNS 请求并缓存主机名到 IP 地址的映射，以便快速高效地解析将来的 DNS 查询。
  - 启用规避签名

    当客户端连接到非源 DNS 请求中指定的域时，用于检测创建的 HTTP 或 TLS 请求的规避签名将发出警报。启用规避签名之前，请务必配置 DNS 代理。若无 DNS 代理，当 DNS 负载均衡配置中的 DNS 服务器向防火墙和客户端返回不同的 IP 地址（用于承载相同资源的服务器）来响应同一 DNS 请求时，可触发规避签名。

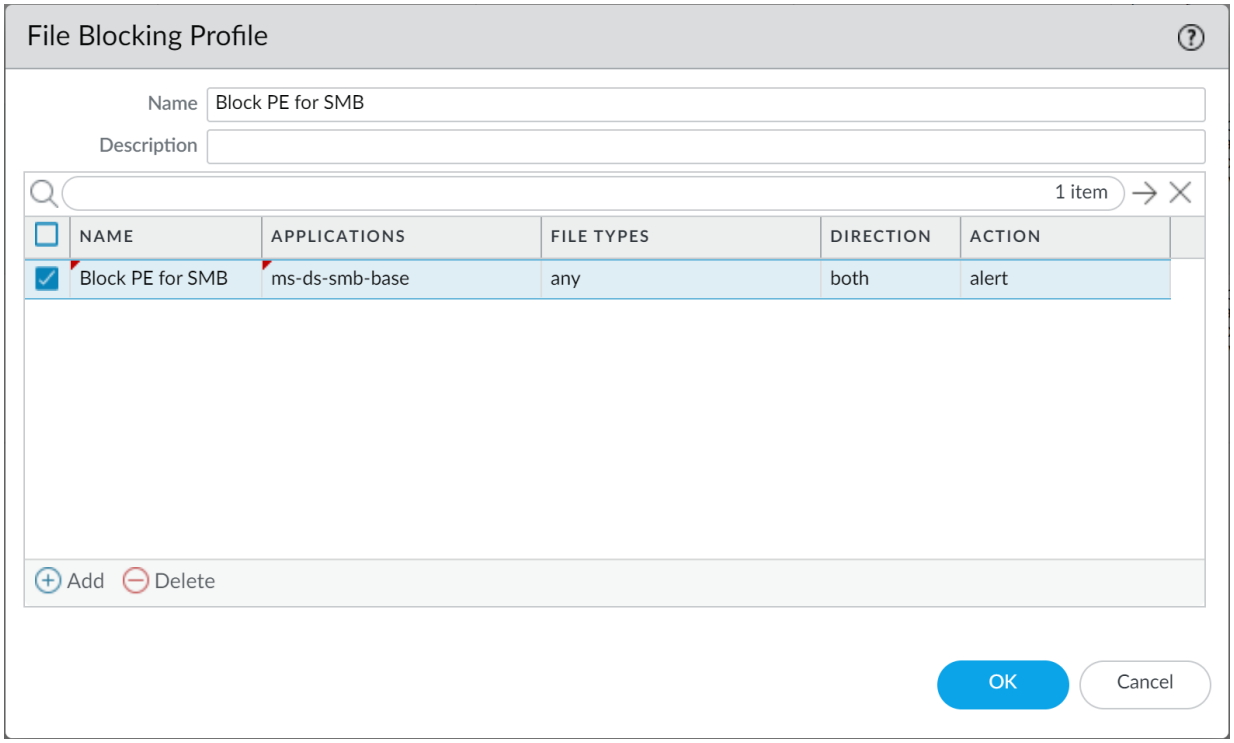


© 2019 Palo Alto Networks, Inc.



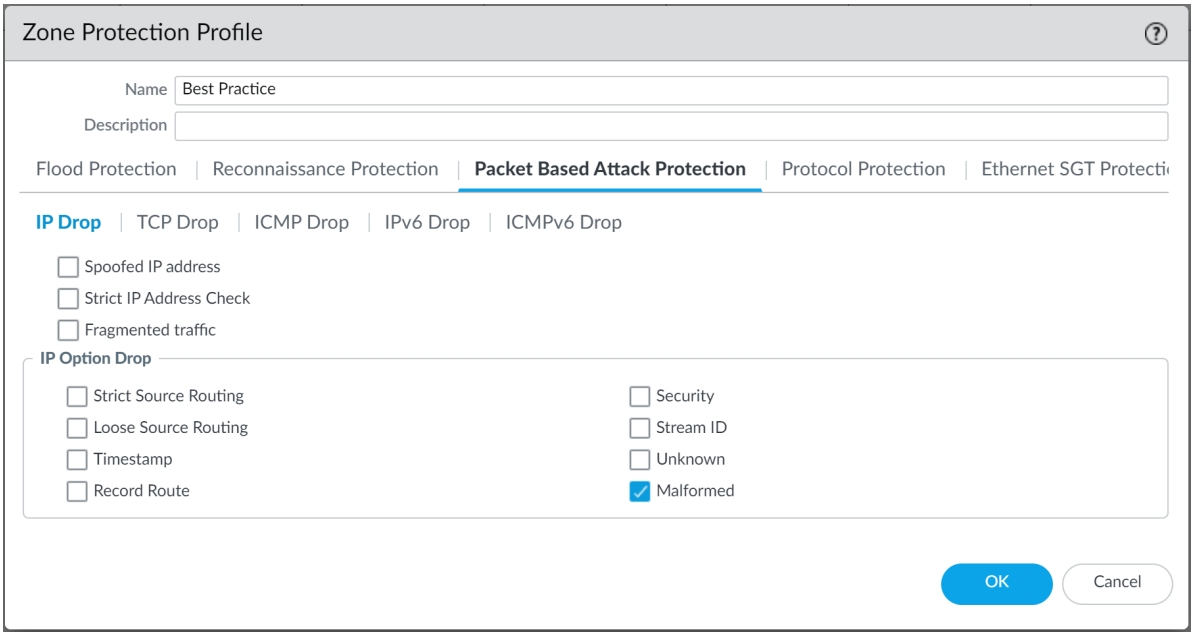

- 对于服务器，创建安全策略规则以仅允许您在每个服务器上批准的应用程序。验证用于应用程序的标准端口与服务器上的侦听端口匹配。例如，为了确保您的电子邮件服务器仅允许 SMTP 通信，将 Application（应用程序）设置为 **smtp** 并将 Service（服务）设置为 **application-default**（应用程序-默认）。如果服务器仅使用一部分标准端口（例如，如果您的 SMTP 服务器仅使用端口 587，同时 SMTP 应用程序有被定义为 25 和 587 的标准端口），应创建仅包括端口 587 的新的自定义服务，并在安全策略规则中使用此新服务，而不是使用 application-default（应用程序-默认）。此外，确保对特定源和目标区域与 IP 地址集的访问受限。
- 使用安全策略阻止所有未知应用程序和流量。通常，分类为未知流量的唯一应用程序是您网络上的内部或自定义应用程序或潜在威胁。未知流量可能是不合规的应用程序或不正常或异常的协议，或者是使用非标准端口的已知应用程序，因此应将这两种应用程序阻止。请参阅管理自定义应用程序或未知应用程序。
- 创建文件传送阻止以阻止基于互联网的服务器消息块 (SMB) 流量的可移植可执行 (PE) 文件类型，该流量从信任区域流向不信任区域（ms-ds-smb 应用程序）。


© 2019 Palo Alto Networks, Inc.




- 实时阻止可移植可执行文件(PE)和 PowerShell 脚本的恶意变体。启用WildFire Inline ML后，您可以通过防火墙上的机器学习动态分析文件。防病毒保护这一附加层是基于 WildFire 的签名的补充，可扩展至尚不存在签名的文件。
- 创建配置的区域保护配置文件，以防范基于数据包的攻击（**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护））：
  - 选择此选项以丢弃 **Malformed**（格式错误）的 IP 数据包（**Packet Based Attack Protection**（基于数据包的攻击保护）> **IP Drop**（**IP** 丢弃））。


© 2019 Palo Alto Networks, Inc.



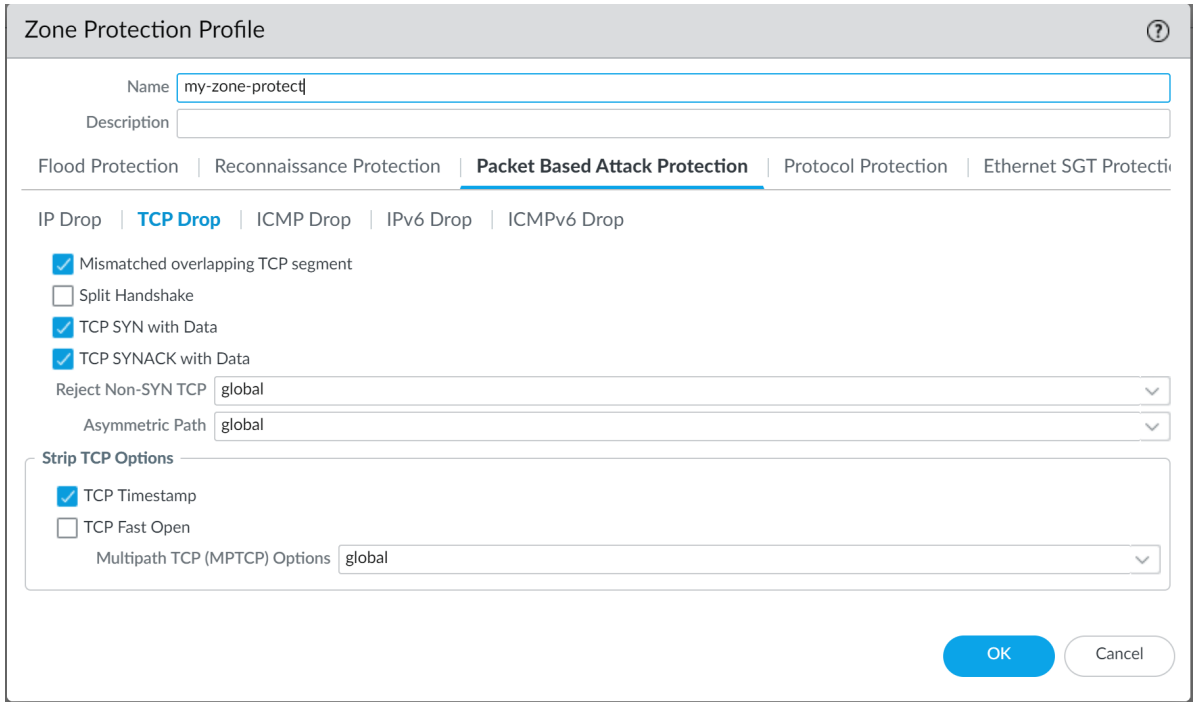

- 启用丢弃 **Mismatched overlapping TCP segment**（不匹配的重叠 TCP 分段）选项（**Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP Drop**（TCP 丢弃））。

  通过故意建立与重叠的连接，但其中的数据不同，可以尝试导致攻击者误解连接的意图，故意诱发误报或漏报。攻击者还可使用 IP 欺骗和序列号预测来拦截用户的连接并插入自己的数据。选择 **Mismatched overlapping TCP segment**（不匹配的重叠 TCP 分段）选项，指定 PAN-OS 丢弃具有不匹配的重叠数据的帧。当接收到的分段包含在另一个分段中、与另一个分段部分重叠，或包含另一个完整的分段时，应将其丢弃。
- 启用丢弃 **TCP SYN with Data**（带数据的 TCP SYN）和丢弃 **TCP SYNACK with Data**（带数据的 TCP SYNACK）选项（**Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP Drop**（TCP 丢弃））。

  在三向握手期间，丢弃负载中包含数据的 SYN 和 SYN-ACK 数据包，阻止负载所包含的恶意软件并防止其在 TCP 握手完成之前提取未授权的数据，以增加安全性。
- 在防火墙转发数据包之前，将 TCP 时间戳从 SYN 数据包中删除（**Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP Drop**（TCP 丢弃））。

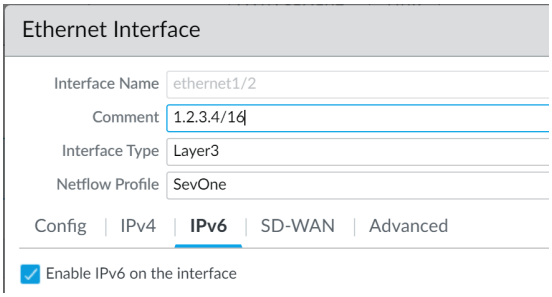
  当您启用 **Strip TCP Options - TCP Timestamp**（删除 TCP 选项 — TCP 时间戳）选项时，TCP 连接两端的 TCP 堆栈都不会支持 TCP 时间戳。这可以防止攻击同一序列号多个数据包上使用的不同时间戳。


© 2019 Palo Alto Networks, Inc.




- 如果您在网络主机上配置 IPv6 地址，在务必在尚未启用时启用 IPv6 支持（**Network**（网络）> **Interfaces**（接口）> **Ethernet** > **IPv6**）。

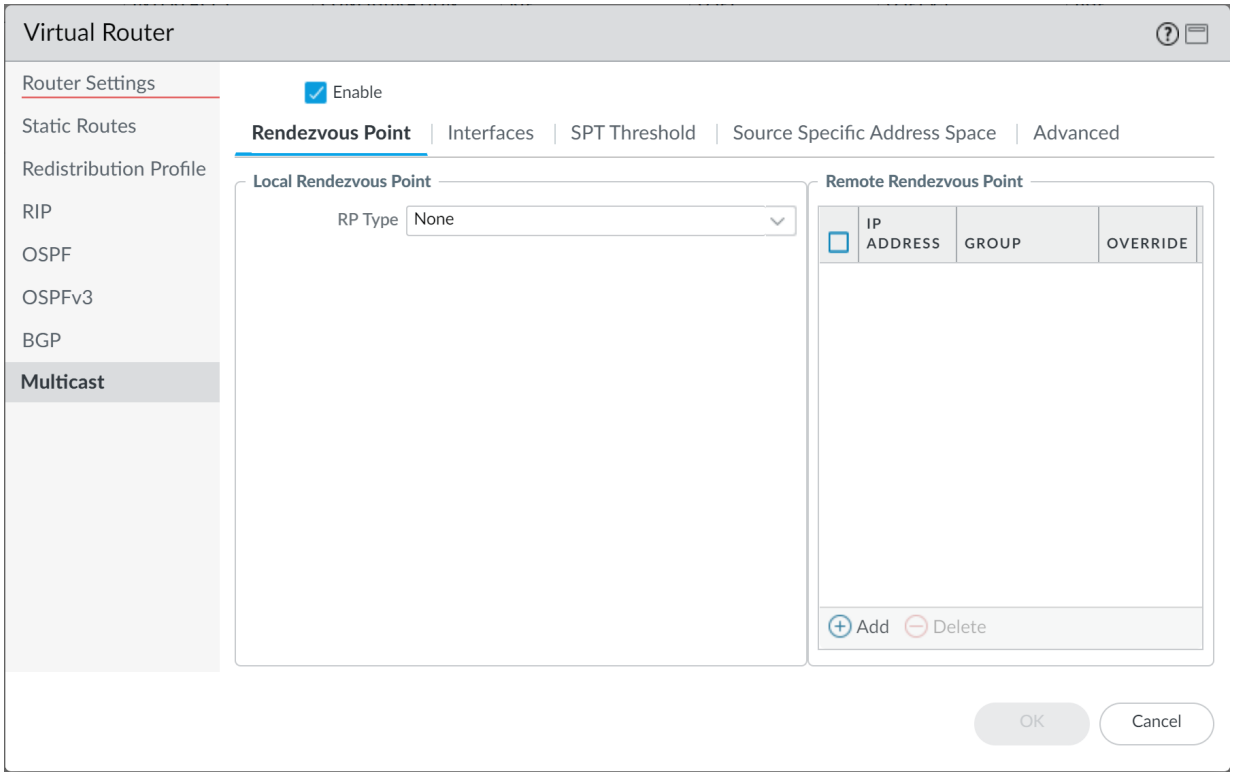
  启用 IPv6 支持可以访问 IPv6 主机，还允许筛选封装在 IPv4 数据包中的 IPv6 数据包，从而阻止 IPv6 利用 IPv4 多播地址进行网络侦查检测。




- 启用多播流量支持，使防火墙可以对多播流量执行策略（**Network**（网络）> **Virtual Router**（虚拟路由器）> **Multicast**（多播））。



© 2019 Palo Alto Networks, Inc.



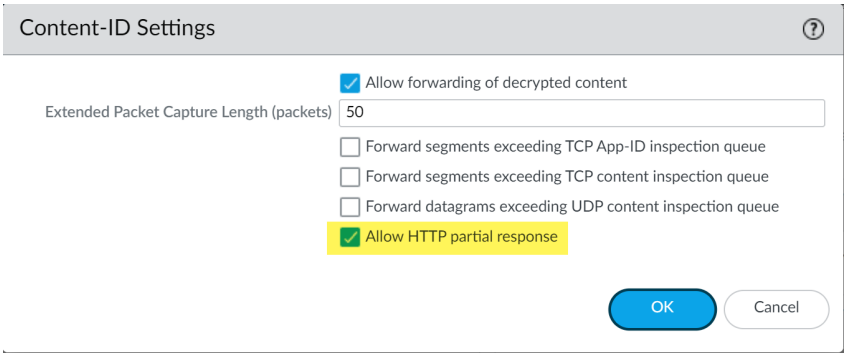

- 禁用 **Forward datagrams exceeding UDP content inspection queue**（转发超过 **UDP** 内容检查队列的数据报）和 **Forward segments exceeding TCP content inspection queue**（转发超过 **TCP** 内容检查队列的分段）选项（**Device**（设备）> **Setup**（设置）> **Content-ID** > **Content-ID Settings**（**Content-ID** 设置））。

  默认情况下，当 TCP 或 UDP 内容检查队列被填满时，防火墙将跳过对超过 64 个队列限制的 TCP 分段或 UDP 数据报的 Content-ID 检查。禁用此选项可确保对防火墙允许的所有 TCP 和 UDP 数据报执行内容检查。仅在特定情况下，例如，如果防火墙平台的规模未进行适当调整，不符合用例要求，则禁用此设置可能会影响性能。
- 禁用 **Allow HTTP partial response**（允许 **HTTP** 部分响应）（**Device**（设备）> **Setup**（设置）> **Content-ID** > **Content-ID Settings**（**Content-ID** 设置））。

  HTTP 部分响应选项可让客户端提取文件的任何部分。传输路径中的下一代防火墙识别并丢弃恶意文件后，它将终止与 RST 数据包的 TCP 会话。如果 Web 浏览器实施了 HTTP 标头范围选项，则将启动新会话，以便仅获取该文件的剩余部分。这可防止防火墙因缺乏上下文而触发相同的签名到初始会话，同时也可防止允许 Web 浏览器重组文件并发送恶意内容。禁用此选项将防止发生此情况。

  禁用此选项不会影响设备性能，但可能会影响 *HTTP* 文件传输的中断恢复。此外，禁用此选项也可能会影响流媒体服务，如 *Netflix*、*Windows Server* 更新服务 *(WSUS)* 和 *Palo Alto Networks* 内容更新。


© 2019 Palo Alto Networks, Inc.




- 创建可用以阻止协议异常以及所有低严重性和高严重性漏洞的漏洞防护配置文件。

  当协议行为偏离标准和合规使用时，就会发生协议异常。例如，格式错误的数据包、写入不当的应用程序、或在非标准端口上运行的应用程序等，都将被视为协议异常，并可用作规避工具。

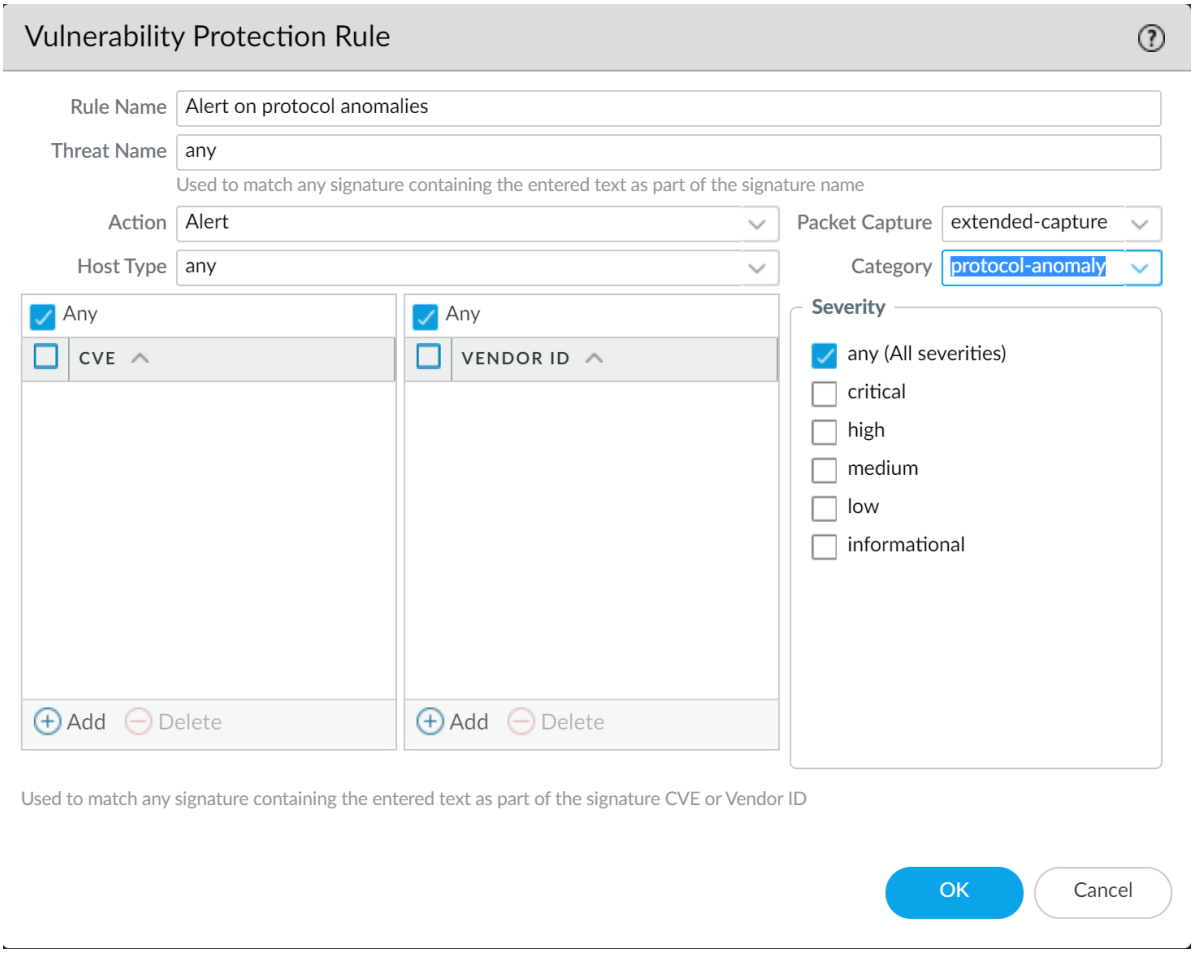
  如果是任务关键型网络，业务的最高优先级应是应用程序的可用性，您应在协议出现异常的一段时间内发出警报，以确保没有关键内部应用程序正在以非标准方式使用已建立的协议。如果您发现某些关键应用程序触发协议异常签名，则可将这些应用程序从协议异常执行中排除。为此，请在漏洞防护配置文件中添加另一个规则，允许协议异常，并将配置文件附加到执行关键应用程序往来流量的安全策略规则。

  确保允许关键内部应用程序协议异常的漏洞防护配置文件规则和安全策略规则均列在阻止协议异常的规则之上。流量根据安全策略规则和相关的漏洞保护配置文件规则从上到下进行评估，并基于第一个匹配规则执行。

  - 从协议异常发出警报开始：

    创建漏洞保护配置文件规则，将 **Action**（操作）设置为警报，将 **Category**（类别）设置为协议异常，将 **Severity**（严重性）设置为任意。监控流量，以确定任何关键内部应用程序是否正在以非标准方式使用已建立的协议。一旦发现，请继续允许这些应用程序的协议异常，然后阻止所有其他应用程序的协议异常。

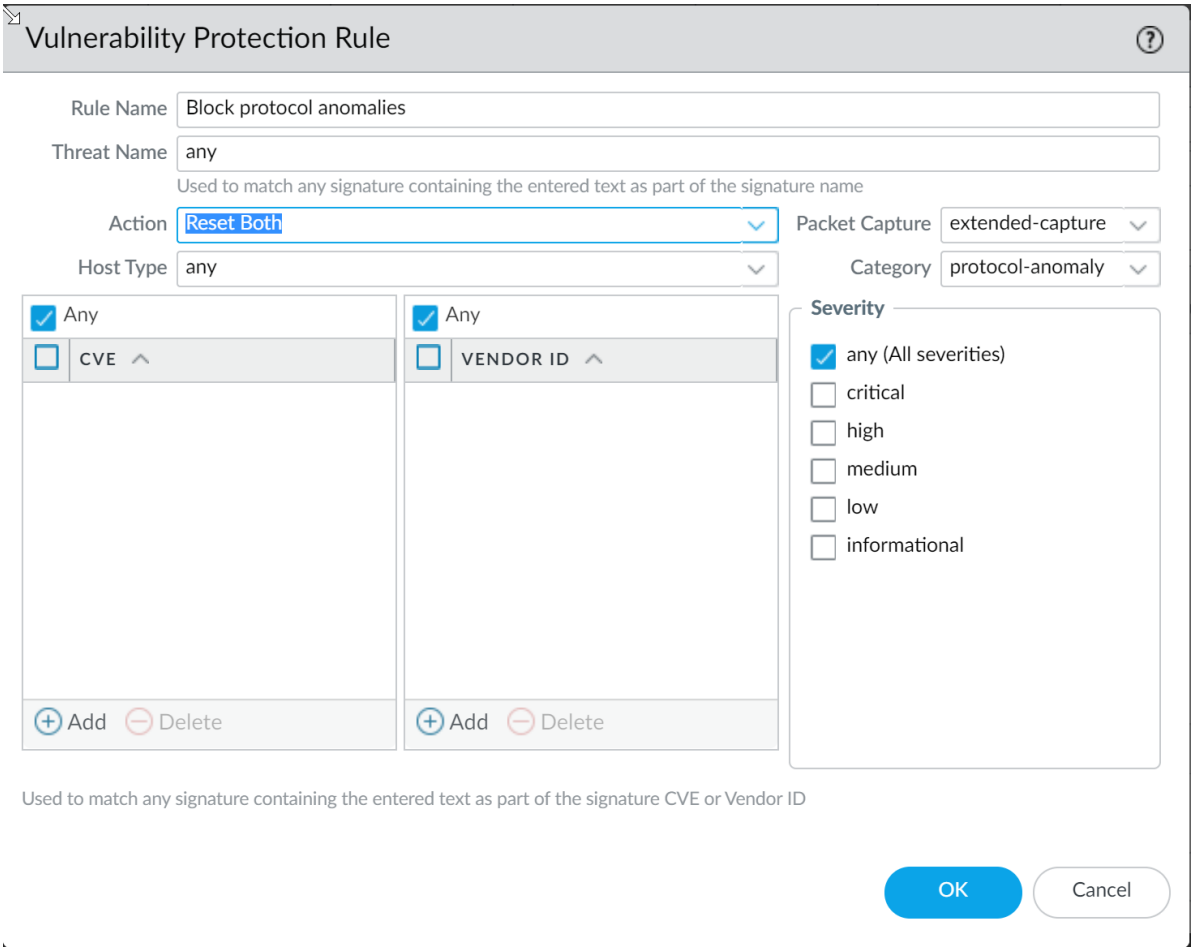

© 2019 Palo Alto Networks, Inc.




- 阻止协议异常：

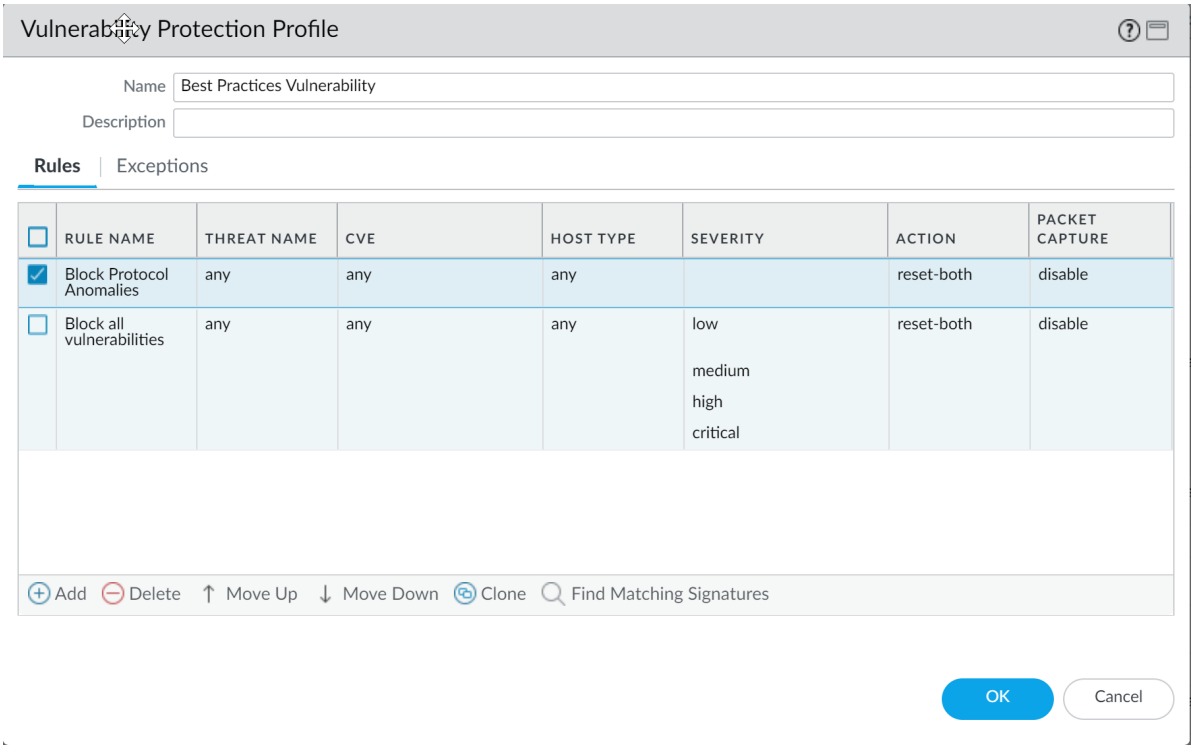
  创建漏洞保护配置文件规则，将 **Category**（类别）设置为协议异常，将规则 **Action**（操作）设置为重置二者，将 **Severity**（严重性）设置为任意。


© 2019 Palo Alto Networks, Inc.




- 可选择允许以非标准方式使用已建立协议的关键应用程序的协议异常。为此，请创建允许协议异常的漏洞保护配置文件规则：将规则 **Action**（操作）设置为允许，将 **Category**（类别）设置为协议异常，将 **Severity**（严重性）设置为任意。将漏洞保护配置文件规则附加到执行重要应用程序往来流量的安全策略规则。
- 向用以阻止所有低严重性和高严重性漏洞的漏洞防护配置文件附加另一条规则。此规则必须显示在阻止协议异常的规则后。


© 2019 Palo Alto Networks, Inc.




- 继续将以下安全配置文件附加到安全策略规则以提供基于签名的保护：
  - 用以阻止严重性偏低和偏高的所有间谍软件的防间谍软件配置文件。
  - 用以阻止与防病毒签名匹配的所有内容的防病毒配置文件。


© 2019 Palo Alto Networks, Inc.

# 设置防病毒威胁、防间谍软件和漏洞保护

每个 Palo Alto Networks 下一代防火墙均配置有可附加到安全策略规则的预定义防病毒、防间谍软件和漏洞保护配置文件。系统有一个预定义的防病毒配置文件，即 **default**（默认）配置文件，该配置文件对各种协议使用默认操作（阻止 HTTP、FTP 和 SMB 流量，并警告 SMTP、IMAP 和 POP3 流量）。系统有两个预定义的防间谍软件和漏洞保护配置文件：

- **default**（默认）— 对所有客户端和服务器的关键、高和中等严重性间谍软件/安全漏洞保护事件应用默认操作。它不检测低严重性和信息类事件。
- **strict**（严格）— 对所有客户端和服务器的关键、高和中等严重性间谍软件/安全漏洞保护事件应用阻止响应，并对低严重性和信息类事件使用默认操作。

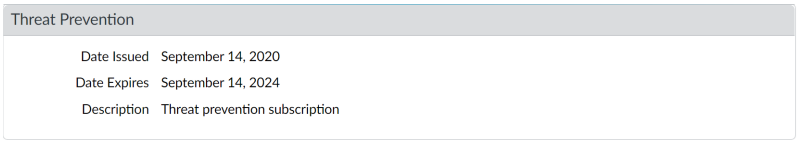
为了确保进入您网络的流量不含任何威胁，请将预定义的配置文件附加到您的基本 Web 访问策略。当监视网络上的通信和扩展策略规则库时，随后可以设计多个更为精细的配置文件来处理特定安全需求。

使用以下工作流程设置默认防病毒、防间谍软件和漏洞保护安全配置文件。

*Palo Alto Networks* 定义所有反间谍软件和漏洞保护签名的默认操作。要查看默认操作，请选择 *Objects*（对象）> *Security Profiles*（安全配置文件）> *Anti-Spyware*（防间谍软件）或 *Objects*（对象）> *Security Profiles*（安全配置文件）> *Vulnerability Protection*（漏洞保护），然后选择一个配置文件。单击 *Exceptions*（例外）选项卡，然后单击 *Show all signatures*（显示所有签名），以查看签名列表和相应的默认 *Action*（操作）。要更改默认操作，请创建一个新的配置文件，并在配置文件中指定一个 *Action*（操作）和/或将个别签名异常添加到 *Exceptions*（异常）。

STEP 1 | 验证您是否具有威胁阻止订阅。

威胁阻止订阅将抗病毒、防间谍软件和漏洞保护功能绑定在一个许可证中。要验证是否具有有效的威胁防御订阅，选择 **Device**（设备）> **Licenses**（许可证），并验证 **Threat Prevention**（威胁阻止）过期日期是否设置为将来。




STEP 2 | 下载最新内容。

1. 选择 **Device**（设备）> **Dynamic Updates**（动态更新），然后单击页面底部的 **Check Now**（立即检查）以检索最新签名。
2. 在 **Actions**（操作）列中，单击 **Download**（下载）安装最新的防病毒更新，然后下载，并 **Install**（安装）最新的应用程序和威胁更新。

STEP 3 | 安排内容更新。

有关部署更新的重要信息，请查阅应用程序和威胁内容更新的最佳实践。

1. 选择 **Device**（设备）> **Dynamic Updates**（动态更新），然后单击 **Schedule**（计划），以自动检索 **Antivirus**（防病毒）和 **Applications and Threats**（应用程序和威胁）的签名更新。
2. 指定更新的频率和时间：
   - **download-only**（仅下载）— 防火墙根据您定义的计划自动下载最新更新，但必须手动 **Install**（安装）。
   - **download-and-install**（下载并安装）— 防火墙根据您定义的计划自动下载并安装更新。



© 2019 Palo Alto Networks, Inc.

3. 单击 **OK**（确定）以保存更新计划；无需提交。
4. （可选）定义 **Threshold**（阈值），以指示在防火墙下载之前更新可用的最短小时数。例如，将 **Threshold**（阈值）设置为 **10**，表示防火墙在至少 10 小时内不会下载更新，而不考虑计划如何。
5. （仅 HA）决定是否 **Sync To Peer**（同步到对端设备），使对端设备在下载和安装后能够同步内容更新（更新计划不会在对端设备之间同步；您必须手动配置两个对端设备的计划）。

   根据您的 HA 部署，决定是否及如何 **Sync To Peer**（同步到对端设备）时还需考虑其他注意事项：

   - 主动/被动 **HA** — 如果防火墙正在使用 MGT 端口进行内容更新，则请安排两个防火墙来单独下载和安装更新。但是，如果防火墙正在使用数据端口进行内容更新，则被动防火墙将不会下载或安装更新，除非变为活动状态。为了在使用数据端口进行更新时保持两个防火墙上的计划同步，请在两个防火墙上安排更新，然后启用 **Sync To Peer**（同步到对端设备），以便确定进行主动下载和安装更新，并将更新推送到被动防火墙。
   - 主动/主动 **HA** — 如果防火墙正在使用 MGT 接口进行内容更新，请在两个防火墙上选择 **download-and-install**（下载并安装），但都不启用 **Sync To Peer**（同步到对端设备）。但是，如果防火墙正在使用数据端口，请在两个防火墙上选择 **download-and-install**（下载并安装），然后启用 **Sync To Peer**（同步到对端设备），以便在一个防火墙进入主动-辅助状态时，主动-主要防火墙将下载并安装更新，并将其推送到主动-辅助防火墙。

STEP 4 | （可选）创建防病毒、防间谍软件和漏洞保护的自定义安全配置文件。

或者，您可以使用预定义的默认或严格配置文件。



安全传输 到最佳实践安全配置文件以实现最佳安全状态。

- 要创建自定义的防病毒配置文件，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）并 **Add**（添加）新配置文件。使用防病毒配置文件传输步骤安全实现您的目标。
- 要创建自定义的防间谍软件配置文件，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）并 **Add**（添加）新配置文件。使用防间谍软件配置文件传输步骤安全实现您的目标。
- 要创建自定义的漏洞保护配置文件，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Vulnerability Protection**（漏洞保护）并 **Add**（添加）新配置文件。使用漏洞保护配置文件传输步骤安全实现您的目标。

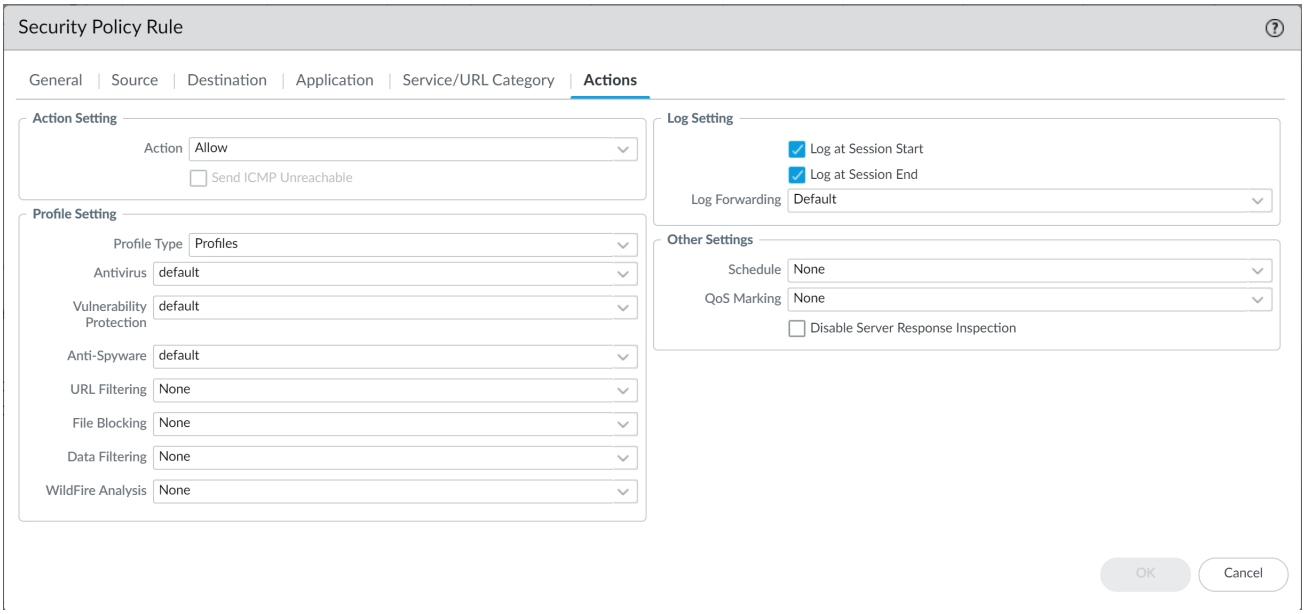
STEP 5 | 将安全配置文件附加到安全策略规则。



使用安全策略规则配置防火墙时，防火墙会使用漏洞保护配置文件来阻止连接，因此防火墙将自动阻止硬件中的流量（请参阅监控已阻止的 IP 地址）。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择要修改的规则。
2. 在 **Actions**（操作）选项卡上，选择 **Profiles**（配置文件）作为 **Profile Type**（配置文件类型）。
3. 选择您为 **Antivirus**（防病毒）、**Anti-Spyware**（防间谍软件）和 **Vulnerability Protection**（漏洞保护）创建的安全配置文件。


© 2019 Palo Alto Networks, Inc.




STEP 6 | 提交更改。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# DNS 安全

DNS 安全是一种持续进化的威胁防护服务，设计用于保护您的网络，防御使用 DNS 的高级威胁。通过利用高级机器学习和预测分析，服务提供实时的 DNS 请求分析，并允许生成和分配 DNS 签名，这些签名专门设计用于防御使用 C2 的 DNS 和数据窃取的恶意软件。通过与可扩展的云架构结合，其提供了对可扩展的威胁情报系统的访问，以便让您的网络保护保持更新。

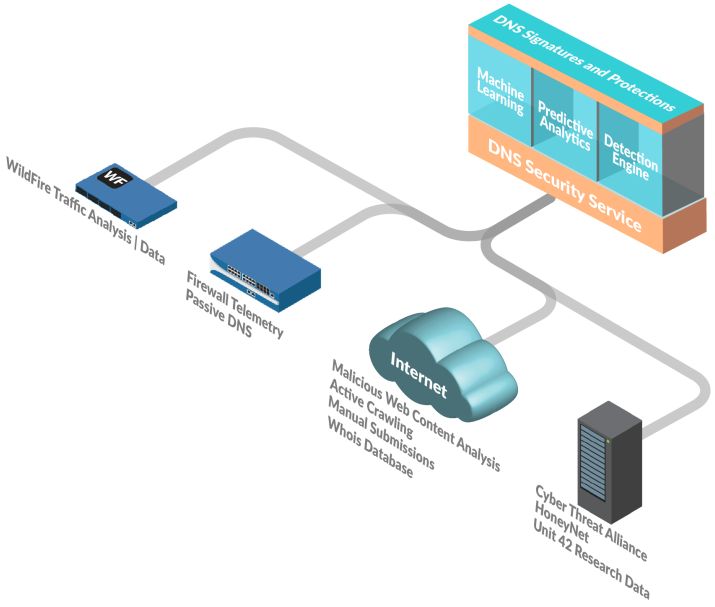
- 关于 DNS 安全
- 云 DNS 签名和保护
- DNS 安全分析
- 启用 DNS 安全

## 关于 DNS 安全

通过主动威胁防护许可证，客户可以配置其防火墙以通过 Palo Alto Networks 生成的域列表 sinkhole DNS 请求。这些本地访问的自定义 DNS 签名列表与 防病毒程序以及 WildFire 更新一同打包，并涵盖了在发布时与策略实施和保护关联性最高的威胁。为通过 DNS 获得对威胁的更全面涵盖，DNS 安全订阅让用户可以通过高级预测分析，访问实时保护。通过诸如 DGA/DNS 隧道检车和机器学习之类的技术，DNS 流量中隐藏的威胁可被主动识别，并通过无限扩展的云服务进行共享。由于 DNS 签名和保护储存在基于云的架构中，您可以访问不断扩展的完整签名数据库，这些签名是通过众多数据源而生产的。这允许您通过 DNS 实时防御各种威胁，以及新生成的恶意域。要对抗以后的威胁，可通过新内容的发布，实现对 DNS 安全服务分析、检测和预防能力的更新。

要访问 DNS 安全服务，您必须拥有有效的威胁保护和 DNS 安全许可证。

下面的工作流程描述了 DNS 安全服务如何使用各种数据源以生成 DNS 签名：

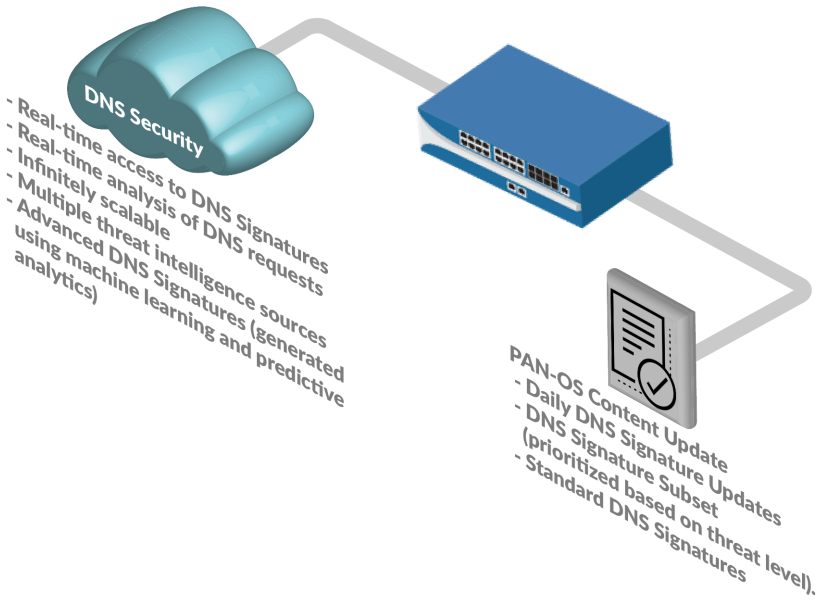



## 云 DNS 签名和保护

作为基于云的服务，DNS 安全允许您访问可无限扩展的 DNS 签名和保护源，以免让您的公司受到恶意域的攻击。Palo Alto Networks 生成的域签名和保护从多个源衍生而来，包括 WildFire 流量分析、被动 DNS、主动 Web 抓取和恶意 Web 内容分析、URL 沙箱分析、蜜网、DGA 反向工程、遥测数据、whois、Unit 42 研究组织和第三方数据源，如 网络威胁联盟。此按需云数据库为用户提供了对完整 Palo Alto Network 的 DNS


© 2019 Palo Alto Networks, Inc.

签名集的访问，包括使用高级分析技术生成的签名，以及实时的 DNS 请求分析。本地可用的可下载 DNS 签名集（与防病毒程序以及 WildFire 更新打包）配有 100k 签名的硬编码容量限制，且不包含通过高级分析生成的签名。为了更好的接收日常生成的新 DNS 签名流入，基于云的签名数据库为用户提供了对新添加 DNS 签名的即时访问，而无需下载更新。如果网络连接出现故障或不可用，防火墙使用指定的 DNS 签名集。




## DNS 安全分析

DNS 安全服务通过对多个 DNS 数据源使用预测分析和机器学习来执行实时 DNS 请求分析。该服务用于针对基于 DNS 的威胁提供防护，可通过配置附加到安全策略规则的防间谍软件安全配置文件来实时访问。每个 DNS 威胁类别（DNS 签名源）都允许您定义单独的策略操作，记录特定签名类型的严重性级别。这样，您就可以按照网络安全协议，根据威胁性质创建特定的安全策略。Palo Alto Networks 还会根据 PAN-DB 和 Alexa 指标生成并保留明确允许的域列表。可以经常访问这些允许域列表，且该列表已知没有恶意内容。DNS 安全类别和允许列表可通过 PAN-OS 内容版本进行更新和扩展。

您可以使用 AutoFocus 查看 DNS 安全云服务生成的组织的 DNS 统计信息数据。这可以提供快速直观的评估，其中根据可用的 DNS 类别描述了通过网络的 DNS 请求的详细信息。或者，您可以使用 **`test dns-proxy dns-signature fqdn <domain>`** 命令检索域信息和事务详细信息，例如延迟和 TTL。

一旦升级到 *PAN-OS 10.0* 以及更高版本，*DNS* 安全源将被重新定义为新的类别，以提供扩展的粒度控制，这样，新类别就将替代先前定义的操作，并获取默认设置。必须对新定义的 *DNS* 安全类别重新应用任何 *sinkhole*、日志严重性和相应的数据包捕获设置。

DNS 安全服务目前支持检测下列 DNS 威胁类别：

- **Command and Control Domains**（命令和控制域）— C2 包括恶意软件和/或受影响系统用于暗中与攻击者远程服务器进行通信，从而接收恶意命令和泄漏数据的 URL 和域（这包括 DNS 隧道检测和 DGA 检测）。
  - **DNS Tunnel Detection**（**DNS** 隧道检测）— DNS 隧道可被攻击者用于在 DNS 查询和响应中，对非 DNS 程序和协议的数据进行编码。其为攻击者提供了开放的反向隧道，攻击者可通过该隧道传输文件或远程访问系统。DNS 隧道检测使用机器学习以分析 DNS 查询的行为质量，包括域、熵、查询率和模式的 n-gram 频率分析，以确定查询是否与基于隧道的 DNS 攻击一致。通过与防火墙的自动化策略操作结合，其允许您快速检测隐藏在 DNS 隧道内的 C2 或数据窃取，并根据您定义的策略规则自动阻挡。



© 2019 Palo Alto Networks, Inc.

- **DGA Detection**（**DGA** 检测）—域生成算法 (DGA) 用于自动生成域，特别是在建立恶意命令和控制 (C2) 通讯隧道时会生成大量域。基于 DGA 的恶意软件（如 Pushdo、BankPatch 和 CryptoLocker）会通过在大量的可疑内容中隐藏其主动 C2 服务器位置来限制被阻止的域数量，而且可基于多种因素（如时间、加密密钥或其他唯一值）通过算法生成。DGA 生成的大部分域并不会解析为有效域，其必须全部被识别，以提供对给定威胁的全面抵御。DGA 分析可确定域是否由机器生成而非人工生成，其方法是通过反向工程和分析在 DGA 中发现的其他频繁使用的技术。而后，Palo Alto Networks 使用这些特征实时识别和阻挡之前未知的、基于 DGA 的威胁。

- **Dynamic DNS Hosted Domains**（动态 **DNS** 托管域）— 动态 DNS (DDNS) 服务提供主机名和 IP 地址之间近乎实时的映射，从而在静态 IP 不可用时，使不断变化的 IP 地址保持与特定域的链接。这让攻击者有机会通过使用 DDNS 服务更改用于托管命令和控制服务器的 IP 地址，从而入侵网络。恶意软件活动和漏洞利用工具包将 DDNS 服务作为其有效载荷分发策略的组成部分加以利用。攻击者将 DDNS 域作为其主机名基础结构的组成部分加以利用，就能更改与特定 DNS 记录关联的 IP 地址，这样就能更容易避开检测。DNS 安全通过筛选和交叉引用来自各种源的 DNS 数据，生成随后可被进一步验证以提高准确性的待选列表，从而检测有漏洞的 DDNS 服务。
- **Malware Domains**（恶意软件域）— 恶意软件域用于托管和分发恶意软件，可能包括尝试安装各种威胁（如可执行文件、脚本、病毒、隐蔽强迫式下载）的网站。恶意软件域与 C2 的区别在于，恶意软件域通过外部源将恶意有效载荷传输到您的网络，而对于 C2，受影响的端点通常会尝试连接到远程服务器，以检索其他指令或其他恶意内容。
- **Newly Registered Domains**（新注册域）— 新注册域是指由 TLD 运营商或实体最近添加、从未注册过的新域。虽然可以根据法律要求创建新的域，但是，绝大多数域通常都是用于协助执行恶意活动，例如作为 C2 服务器运行或是用于分发恶意软件、垃圾邮件、PUP/广告软件。Palo Alto Networks 通过监控特定馈送（域注册表和注册器），并使用区域文件、被动 DNS、WHOIS 数据来检测注册活动，从而检测新注册域。
- **Phishing Domains**（网络钓鱼域）— 网络钓鱼域尝试通过网络钓鱼或网络欺骗伪装成合法网站，诱使用户提交个人信息或用户凭据等敏感数据。这些恶意活动可通过社会工程活动（凭借看似可信的源，操纵用户通过电子邮件或其他形式的电子通信提交个人信息）或 Web 流量重定向（将用户定向到看似合法的欺诈站点）进行。
- **Grayware Domains**（灰色软件域）—（安装有 PAN-OS 内容版本 8290 以及更高版本时可用）。灰色软件域通常不会直接构成安全威胁，但是，他们会协助攻击媒介，产生各种不良行为，或是可能只包含可疑/攻击性内容。这包括尝试诱骗用户授予远程访问权限的网站，包含广告软件和其他未经请求的应用程序（例如，挖矿软件、劫持程序和 PUP [潜在有害程序]）的网站，以及使用快速通量技术、误植域名域以及各种协助执行非法活动或诈骗的站点部署域标识隐藏操作的网站。
- **Parked Domains**（寄放域）—（安装有 PAN-OS 内容版本 8318 以及更高版本时可用）寄放域通常是指用于托管有限内容的非活动网站，通常以点阅广告的形式出现，可为主题实体带来收益，但其中包含的内容通常对最终用户没用。尽管他们通常充当合法占位符或是仅起到良性妨碍的作用，但是，他们还可用作分发恶意软件的潜在媒介。
- **Proxy Avoidance and Anoymizers**（代理规避和匿名程序）—（安装有 PAN-OS 内容版本 8340 以及更高版本时可用）代理规避和匿名者是指用于绕过内容过滤策略的服务流量。尝试通过匿名程序代理服务绕过组织内容过滤策略的用户在 DNS 级别会被阻止。

# 启用 DNS 安全

若要通过使用 DNS 安全为 DNS sinkhole 启用域查询，您必须激活 DNS 安全订阅,创建（或修改）防间谍软件策略以引用 DNS 安全服务，配置各个 DNS 签名类别的日志严重性和策略设置，然后将配置文件附加到安全策略规则。

STEP 1 | 激活订阅许可证。

STEP 2 | 配置 DNS 签名策略设置，以发送恶意软件 DNS 查询到定义的 sinkhole。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）。
2. 创建或修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 确定配置文件的**Name**（名称），或者提供描述。
4. 选择 **DNS Policies**（**DNS** 策略）选项卡。

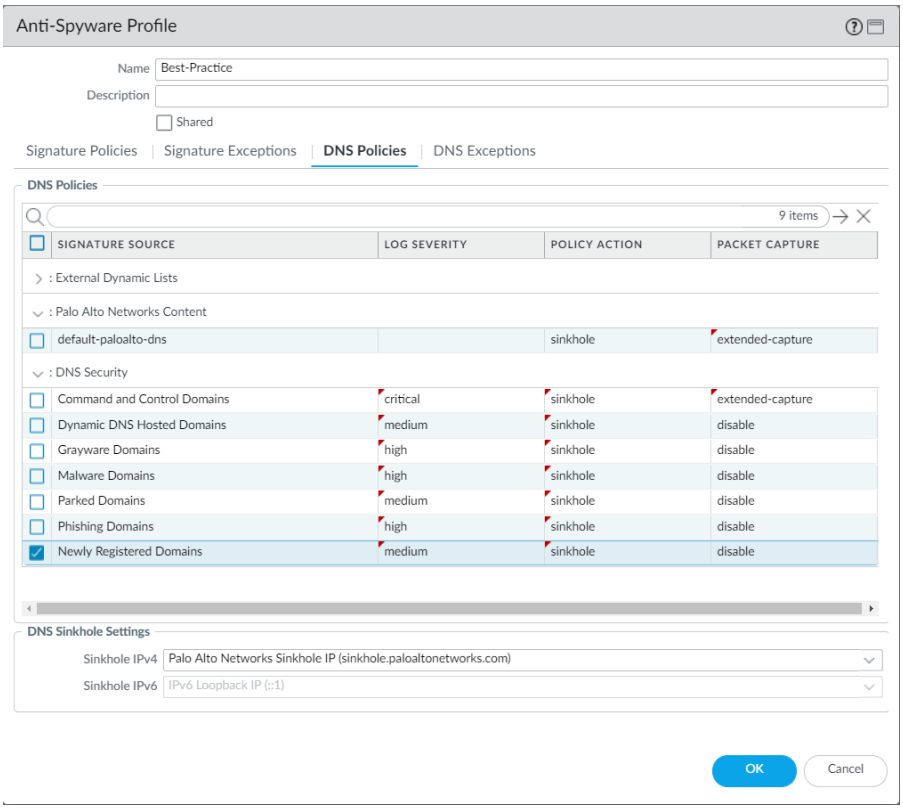

© 2019 Palo Alto Networks, Inc.

5. 在“DNS 安全”标题下的 **Signature Source**（签名源）列中，存在可单独配置的 DNS 签名源，您可以通过该签名源定义单独的策略操作和日志严重性级别。

   *Palo Alto Networks* 建议更改签名源的默认 *DNS* 策略设置以确保最佳覆盖范围，并协助事件响应和修复。请遵循防止网络免遭第 4 层和第 7 层逃避的最佳实践中概述的 *DNS* 安全设置配置最佳实践。

   - 指定防火墙检测到与 DNS 签名匹配的域时记录的日志严重性级别。更多有关各种日志严重性级别的信息，请参阅威胁严重性级别。
   - 选择为 DNS 安全签名源的已知恶意软件站点执行 DNS 查找时采取的操作。可选操作为警报、允许、阻止或 sinkhole。验证操作是否设为 sinkhole。
   - 在 **Packet Capture**（数据包捕获）下拉列表中，选择 **single-packet**（单个数据包）以捕获会话的第一个数据包，或选择 **extended-capture**（扩展捕获）以设置为 1-50 个数据包之间的值。然后您可使用数据包捕获进行进一步分析。
6. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 设置）部分中，验证是否已启用 **Sinkhole**。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole 地址 (sinkhole.paloaltonetworks.com)。Palo Alto Networks 可通过内容更新自动刷新此地址。

   如果想要修改到网络上的本地服务器或回环地址的 **Sinkhole Ipv4** 或 **Sinkhole Ipv6** 地址，请参阅将 Sinkholing IP 地址配置为网络上的本地服务器。
7. 单击 **OK**（确定）以保存防间谍软件配置文件。




STEP 3 | 将防间谍软件配置文件附加至安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全）。
2. 选择或创建 **Security Policy Rule**（安全策略规则）。
3. 在 **Actions**（操作）选项卡上，选中 **Log at Session End**（在会话结束时记录）复选框以启用日志记录。



© 2019 Palo Alto Networks, Inc.

4. 在配置设置部分中，单击 **Profile Type**（配置类型）下拉列表以查看所有 **Profiles**（配置文件）。在 **Anti-Spyware**（防间谍软件）下拉列表中选择新的或修改过的配置文件。
5. 单击 **OK**（确定）以保存策略规则。

STEP 4 | 测试是否实施了策略操作。

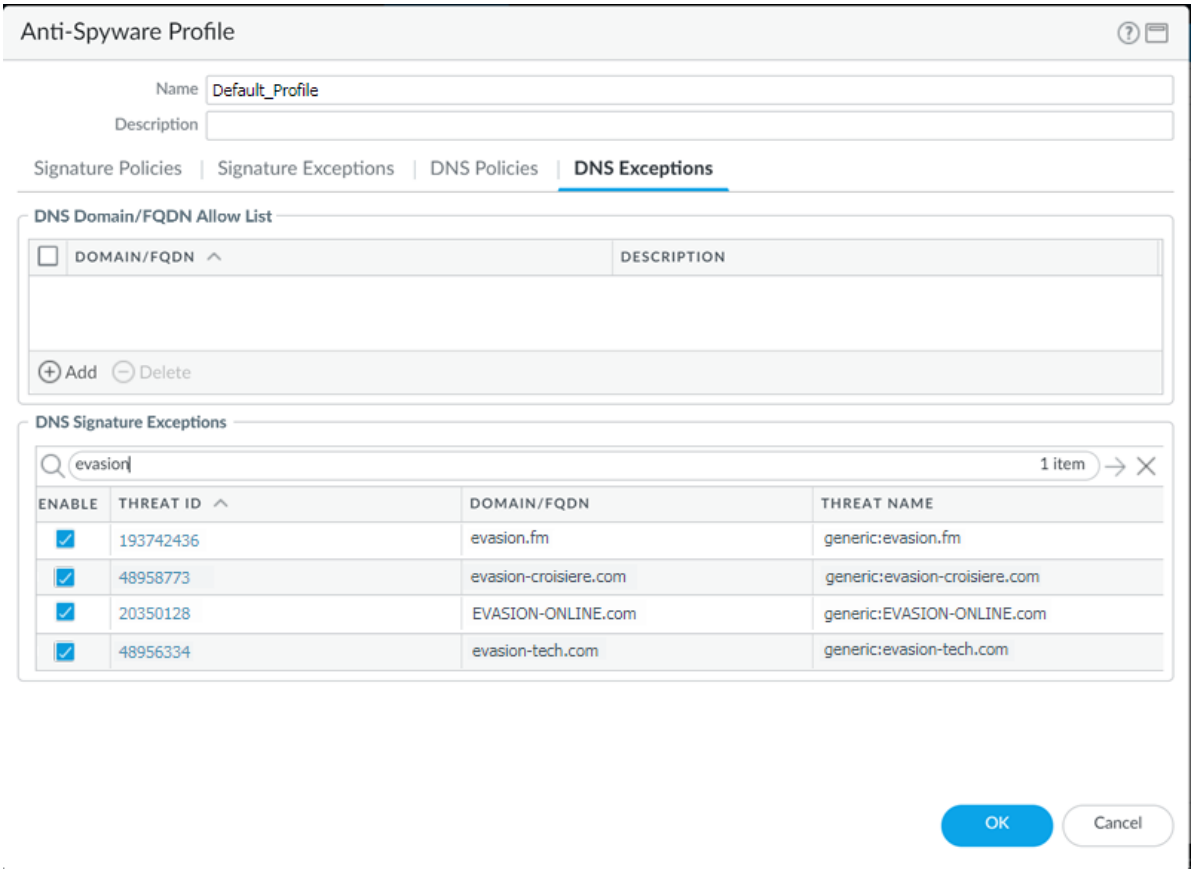
1. 访问以下测试域，以验证是否针对给定威胁类型实施了策略操作：
   - C2 — test-c2.testpanw.com
   - DNS 隧道 — test-dnstun.testpanw.com
   - DGA — test-dga.testpanw.com
   - 动态 DNS — test-ddns.testpanw.com
   - 恶意软件 — test-malware.testpanw.com
   - 新注册域 — test-nrd.testpanw.com
   - 网络钓鱼 — test-phishing.testpanw.com
   - 灰色软件 — test-grayware.testpanw.com
   - 寄放域 — test-parked.testpanw.com
   - 代理规避和匿名程序 — test-proxy.testpanw.com
2. 监控防火墙上的活动：
   1. 选择 **ACC** 并添加 URL 域作为查看访问域的威胁活动和阻止的活动的全局筛选器。
   2. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），并通过 `(action eq sinkhole)` 筛选以查看被 Sinkhole 的域上的日志。

STEP 5 | 在流量日志中识别受感染的流量主机

STEP 6 | （可选）在发生误报时添加域签名例外。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）。
2. 选择要修改的配置文件。
3. **Add**（添加）或修改要从中排除威胁签名的防间谍软件配置文件，然后选择 **DNS Exceptions**（DNS 例外）。
4. 通过输入名称或 FQDN 搜索要排除的 DNS 签名。
5. 选中要从执行中排除的 DNS 签名的各个 **Threat ID**（威胁 ID）复选框。
6. 单击 **OK**（确定）以保存新的或修改过的反间谍软件配置文件。


© 2019 Palo Alto Networks, Inc.




STEP 7 | （可选）添加允许列表以指定明确允许的 DNS 域/FQDN 列表。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 选择要修改的配置文件。
3. **Add**（添加）或修改要从中排除威胁签名的防间谍软件配置文件，然后选择 **DNS Exceptions**（**DNS** 例外）。
4. 若要**Add**（添加）新的**FQDN Allow List**（**FQDN** 允许列表），请提供 DNS 域或 FQDN 位置和说明。
5. 单击 **OK**（确定）以保存新的或修改过的反间谍软件配置文件。

STEP 8 | （可选）验证防火墙与 DNS 安全服务的连接性。如果无法访问该服务，请验证以下域是否被阻止：dns.service.paloaltonetworks.com。

对防火墙使用下列 CLI 命令，验证防火墙与 DNS 安全服务的连接可用性。

```
show dns-proxy dns-signature info
```

例如：

```
show dns-proxy dns-signture info

Cloud URL: dns.service.paloaltonetworks.com:443

Telemetry URL: io.dns.service.paloaltonetworks.com:443
```



© 2019 Palo Alto Networks, Inc.

```
Last Result: None

Last Server Address:

Parameter Exchange: Interval 300 sec

Allow List Refresh: Interval 43200 sec

Request Waiting Transmission: 0

Request Pending Response: 0

Cache Size: 0
```

STEP 9 | （可选）检索指定域的交易详细信息，例如延迟、TTL 和签名类别。

在防火墙上使用以下 CLI 命令查看列表的详细信息。

```
test dns-proxy dns-signature fqdn
```

例如：

```
test dns-proxy dns-signature fqdn www.yahoo.com

DNS Signature Query [ www.yahoo.com ]

Completed in 178 ms

DNS Signature Response

Entries: 2

Domain                              Category        GTID                TTL
-------------------------------------------------------------------------------------
*.yahoo.com                         Benign          0
 86400
  www.yahoo.com                     Benign          0                   3600
```

STEP 10 | （可选）配置 DNS 签名查找超时设置。如果防火墙因连接问题无法在指定时间内检索到签名裁决，则包含所有后续 DNS 响应在内的请求都将通过。您可以通过检查平均延迟时间来验证这些请求是否都在配置时段内。如果平均延迟时间超出配置时段，请考虑更新设置，设置一个比平均延迟时间更大的值，从而阻止请求超时。

1. 在 CLI 中，发出以下命令以查看平均延迟时间。

   ```
   show dns-proxy dns-signature
   counters
   ```

   默认超时为 100 毫秒。
2. 向下滚动输出到签名请求 API 标题下的延迟部分，验证平均延迟时间是否在定义的超时时段内。此延迟时间表示 DNS 安全服务检索签名裁决所花费的平均时间量。关于各延迟时段的其他延迟统计数据可能低于平均值。

   ```
   Signature query API:
     .
     .
   ```

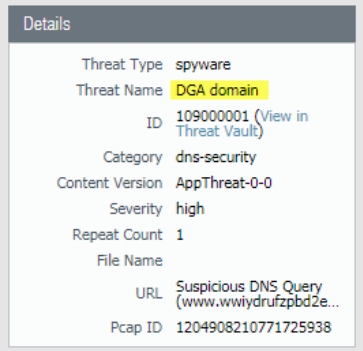


© 2019 Palo Alto Networks, Inc.

```
.
   [latency    ] :
      max     1870 (ms)   min     16(ms)   avg     27(ms)
        50 or less : 47246
        100 or less : 113
        200 or less : 25
        400 or less : 15
               else : 21
```

3. 如果平均延迟时间一律高于默认超时值，您可以增加设置，使请求位于规定时段内。选择 **Device**（设置）> **Content-ID**，并更新 **Realtime Signature Lookup**（实时签名查询）设置。
4. 提交更改。

若要查看 sinkholed DNS 查询，请查阅防火墙威胁日志（**Monitor**（监控）> **Logs**（日志），然后从列表选择日志类型）：






© 2019 Palo Alto Networks, Inc.

# 使用 DNS 查询来确定网络上受感染的主机

防间谍软件配置文件中的 DNS Sinkhole 操作可让防火墙对已知恶意域或自定义域的 DNS 查询伪造响应，以便您能够在网络上识别已被恶意软件感染的主机。受影响的主机可能通过命令和控制 (C2) 服务器启动通讯—一旦实现连接，攻击者可远程控制受感染的主机，从而进一步渗透网络或外泄数据。

对 Palo Alto Networks DNS 签名列表中包括的任何域的 DNS 查询将被 sinkhole 到 Palo Alto Networks 服务器 IP 地址。

防火墙有两个 DNS 签名源，可用于识别恶意和 C2 域：

- （需要威胁保护）本地 DNS 签名—这是一个有限的 DNS 签名指定集，防火墙可将其用于识别恶意域。防火墙获得新 DNS 签名作为日常防病毒更新的一部分。
- （需要 DNS 安全）DNS 安全签名 — 防火墙访问 Palo Alto Networks DNS 安全云服务，以检查是否有针对 DNS 签名完整数据库的恶意域。特定签名—仅由 DNS 安全提供—可专门检测使用机器学习技术的 C2 攻击，比如域生成算法 (DGA) 和 DNS 隧道。

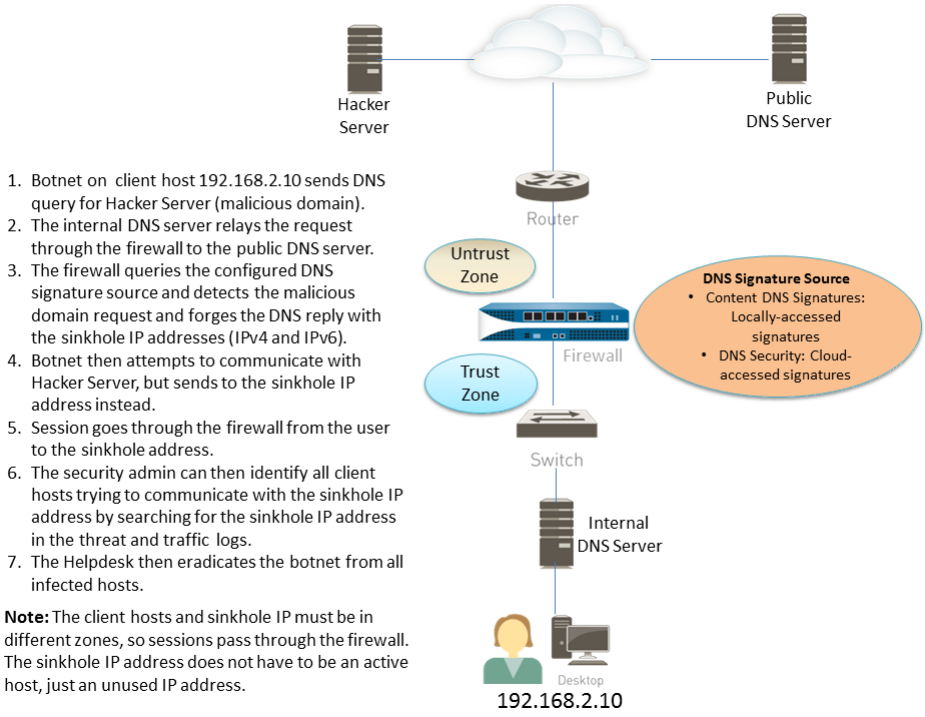
本地 DNS 签名集或 DNS 安全签名集内域的 DNS 查询被导向至 Palo Alto Networks 服务器，而主机无法访问恶意域。下列主题提供了有关如何启用 DNS Sinkholing 以便您识别受感染的主机的详细信息。

- 了解 DNS Sinkholing 的工作原理。
- 配置 DNS Sinkholing。
- 为自定义域列表配置 DNS Sinkholing。
- 启用 DNS 安全至 sinkhole C2 域。
- 将 Sinkholing IP 地址配置为网络上的本地服务器。
- 查看试图连接到恶意域的受感染主机。

## DNS Sinkholing 的工作原理

DNS Sinkholing 可帮助您在防火墙无法看到受感染的 DNS 查询的情况下识别受使用 DNS 流量的网络保护的感染主机（即防火墙无法看到 DNS 查询的始发者）。在防火墙在本地 DNS 服务器中检测不到任何内容的典型部署中，威胁日志将确定本地 DNS 解析器作为流量的来源，而不是实际受感染的主机。Sinkholing 恶意 DNS 查询通过伪造对恶意域中定向客户端主机查询的响应解决这种可见性问题，以便客户端试图连接到恶意域（如对于命令和控制），而不是试图连接到默认的 Palo Alto Networks Sinkhole IP 地址（或当您选择为自定义域列表配置 DNS Sinkholing 时定义的 IP 地址）。可在流量日志中轻松识别受感染的主机。


© 2019 Palo Alto Networks, Inc.




1. Botnet on client host 192.168.2.10 sends DNS query for Hacker Server (malicious domain).
2. The internal DNS server relays the request through the firewall to the public DNS server.
3. The firewall queries the configured DNS signature source and detects the malicious domain request and forges the DNS reply with the sinkhole IP addresses (IPv4 and IPv6).
4. Botnet then attempts to communicate with Hacker Server, but sends to the sinkhole IP address instead.
5. Session goes through the firewall from the user to the sinkhole address.
6. The security admin can then identify all client hosts trying to communicate with the sinkhole IP address by searching for the sinkhole IP address in the threat and traffic logs.
7. The Helpdesk then eradicates the botnet from all infected hosts.

**Note:** The client hosts and sinkhole IP must be in different zones, so sessions pass through the firewall. The sinkhole IP address does not have to be an active host, just an unused IP address.

# 配置 DNS Sinkholing

要启用 DNS Sinkholing，将默认防间谍软件配置文件附加到安全策略规则（请参见设置防病毒、防间谍软件和漏洞保护）。对 Palo Alto Networks DNS 签名源中包括的任何域的 DNS 查询将被解析到默认的 Palo Alto Networks Sinkhole IP 地址。IP 地址当前为 IPv4 — sinkhole.paloaltonetworks.com，回环地址当前为 Ipv6 地址 — ::1。这些地址可能出现变更，可随内容更新而更新。

STEP 1 | 为外部动态列表中的自定义域列表启用 DNS Sinkholing。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）。
2. 修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 为配置文件 **Name**（命名），然后选择 **DNS Policies**（**DNS** 策略）选项卡。
4. 确认 **Signature Source**（签名源）中是否存在 **default-paloalto-dns**。
5. （可选）在 **Packet Capture**（数据包捕获）下拉列表中，选择 **single-packet**（单个数据包）以捕获会话的第一个数据包，或选择 **extended-capture**（扩展捕获）以设置为 1-50 个数据包之间的值。然后您可使用数据包捕获进行进一步分析。

STEP 2 | 验证防间谍软件配置文件中的启用 Sinkholing 设置。

1. 在 **DNS Policies**（**DNS** 策略）选项卡中，确认 DNS 查询的 **Policy Action**（策略操作）是否为 **Sinkhole**。
2. 在“DNS Sinkhole 设置”部分中，确认是否已启用 **Sinkhole**。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole IP 地址。Palo Alto Networks 可通过内容更新自动刷新此 IP 地址。

   如果想要修改到网络上的本地服务器或回环地址的 **Sinkhole Ipv4** 或 **Sinkhole Ipv6** 地址，请参阅将 Sinkholing IP 地址配置为网络上的本地服务器。
3. 单击 **OK**（确定）以保存防间谍软件配置文件。

STEP 3 | 将防间谍软件配置文件附加至安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择安全策略规则。
2. 在 **Actions**（操作）选项卡上，选中 **Log at Session Start**（在会话开始时记录）复选框以启用日志记录。



© 2019 Palo Alto Networks, Inc.

3. 在配置设置部分中，单击 **Profile Type**（配置类型）下拉列表以查看所有 **Profiles**（配置文件）。在 **Anti-Spyware**（防间谍软件）下拉列表中选择新的配置文件。
4. 单击 **OK**（确定）以保存策略规则。

STEP 4 | 通过监控防火墙上的活动，测试策略操作是否已实施。

1. 选择 **ACC** 并添加 URL 域作为查看访问域的威胁活动和阻止的活动的全局筛选器。
2. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），并通过 `(action eq sinkhole)` 筛选以查看被 Sinkhole 的域上的日志。

# 为自定义域列表配置 DNS Sinkholing

要为自定义域列表启用 DNS Sinkholing，必须创建包括域的外部动态列表，在防间谍软件配置文件中启用 Sinkhole 操作，并将配置文件附加到安全策略规则。当客户端尝试访问列表中的某个恶意域时，防火墙会将数据包中的目标 IP 地址伪造为默认的 Palo Alto Networks 服务器或用户针对 Sinkholing 定义的 IP 地址。

对于外部动态列表中包括的每个自定义域，防火墙将生成基于 DNS 的防间谍软件签名。签名将被命名为 Custom Malicious DNS Query <domain name>，属于中等严重性类型的间谍软件；每个签名为域名的 24 字节哈希值。

每个防火墙模式支持一个或多个外部动态列表中最多 50,000 个域名，但对任何列表没有最大限制。

STEP 1 | 为外部动态列表中的自定义域列表启用 DNS Sinkholing。

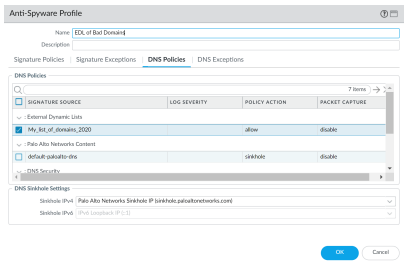
1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）。
2. 修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 为配置文件 **Name**（命名），然后选择 **DNS Policies**（**DNS** 策略）选项卡。
4. 从 **External Dynamic Lists**（外部动态列表）签名源中选择 EDL。

   如果您已创建*Domain List*（域列表）类型的外部动态列表，您可以从此处选择。此列表不显示您可能创建的 *URL* 或 *IP* 地址类型的外部动态列表。
5. 从防间谍软件配置文件配置外部动态列表（请参阅将防火墙配置为访问外部动态列表）。**Type**（类型）预设为 **Domain List**（域列表）。
6. （可选）在 **Packet Capture**（数据包捕获）下拉列表中，选择 **single-packet**（单个数据包）以捕获会话的第一个数据包，或选择 **extended-capture**（扩展捕获）以设置为 1-50 个数据包之间的值。然后您可使用数据包捕获进行进一步分析。

STEP 2 | 验证防间谍软件配置文件中的启用 Sinkholing 设置。

1. 在 **DNS Policies**（**DNS** 策略）选项卡中，确认 DNS 查询的 **Policy Action**（策略操作）是否为 **Sinkhole**。
2. 在“DNS Sinkhole 设置”部分中，确认是否已启用 **Sinkhole**。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole IP 地址。Palo Alto Networks 可通过内容更新自动刷新此 IP 地址。

   如果想要修改到网络上的本地服务器或回环地址的 **Sinkhole Ipv4** 或 **Sinkhole Ipv6** 地址，请参阅将 Sinkhole IP 地址配置为网络上的本地服务器。




3. 单击 **OK**（确定）以保存防间谍软件配置文件。


© 2019 Palo Alto Networks, Inc.

STEP 3 | 将防间谍软件配置文件附加至安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择安全策略规则。
2. 在 **Actions**（操作）选项卡上，选中 **Log at Session Start**（在会话开始时记录）复选框以启用日志记录。
3. 在配置设置部分中，单击 **Profile Type**（配置类型）下拉列表以查看所有 **Profiles**（配置文件）。在 **Anti-Spyware**（防间谍软件）下拉列表中选择新的配置文件。
4. 单击 **OK**（确定）以保存策略规则。

STEP 4 | 测试是否实施了策略操作。

1. 查看外部动态列表条目（该条目属于域列表），并从列表中访问域。
2. 监控防火墙上的活动：
   1. 选择 **ACC** 并添加 URL 域作为查看访问域的威胁活动和阻止的活动的全局筛选器。
   2. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），并通过 `(action eq sinkhole)` 筛选以查看被 Sinkhole 的域上的日志。

STEP 5 | 验证外部动态列表中的条目已忽略或跳过。

在防火墙上使用以下 CLI 命令查看列表的详细信息。

```
request system external-list show type domain name <list_name>
```

例如：

```
request system external-list show type domain name
My_List_of_Domains_2015
vsys1/EBLDomain:
Next update at : Thu May 21 10:15:39 2015
Source : https://1.2.3.4/My_List_of_Domains_2015
Referenced : Yes
Valid : Yes
Number of entries : 3
domains:www.example.com
baddomain.com
qqq.abcedfg.com
```

STEP 6 | （可选）按需检索外部动态列表。

要强制防火墙按需检索更新后的列表，而不是在下一次刷新时间间隔后进行检索（您为外部动态列表定义的 **Repeat**（重复）频率），使用以下 CLI 命令：

```
request system external-list refresh type domain name  <list_name>
```

或者，您可以使用防火墙接口从 Web 服务器检索外部动态列表。

# 将 Sinkholing IP 地址配置为网络上的本地服务器

默认情况下，将为所有 Palo Alto Networks DNS 签名启用 Sinkholing，且将设置访问 Palo Alto Networks 服务器的默认 Sinkhole IP 地址。如果想要将 Sinkhole IP 地址设置为网络上的本地服务器，请使用本部分中的说明。



© 2019 Palo Alto Networks, Inc.

必须获取要用作为 Sinkhole IP 地址的 IPv4 和 IPv6 地址，因为恶意软件可能使用这两种协议中的一种，也可能同时使用两种来执行 DNS 查询。DNS Sinkhole 地址必须位于与客户端主机所在区域不同的区域中，从而确保当受感染的主机尝试启动与 Sinkhole IP 地址的会话时，可通过防火墙进行路由。

该 *Sinkhole* 地址必须保留用于此目的，并且不需要分配给物理主机。您可以选择性地使用诱惑服务器作为物理主机，以进一步分析恶意流量。

要遵循的配置步骤使用以下示例 *DNS Sinkhole* 地址：

*IPv4 DNS Sinkhole* 地址—*10.15.0.20*

*IPv6 DNS Sinkhole* 地址—*fd97:3dec:4d27:e37c:5:5:5:5*

STEP 1 | 配置 Sinkhole 接口和区域

必须将客户端主机所在区域的流量转发到定义 Sinkhole IP 地址的区域，因此必须记录流量。

请为 *Sinkhole* 流量使用专用区域，因为受感染的主机会将流量发送到此区域。

1. 选择 **Network**（网络）> **Interfaces**（接口）并选择一个要配置为 Sinkhole 接口的接口。
2. 在 **Interface Type**（接口类型）下拉列表中，选择 **Layer3**（第 3 层）。
3. 要添加 IPv4 地址，请选择 **Ipv4** 选项卡，再选择 **Static**（静态），然后单击 **Add**（添加）。在本例中，请将 10.15.0.20 添加为 IPv4 DNS Sinkhole 地址。
4. 选择 **Ipv6** 选项卡并单击 **Static**（静态），然后单击 **Add**（添加）并输入 IPv6 地址和子网掩码。在本例中，请输入 fd97:3dec:4d27:e37c::/64 作为 IPv6 Sinkhole 地址。
5. 单击 **OK**（确定）以保存。
6. 要为 Sinkhole 添加一个区域，请选择 **Network**（网络）> **Zones**（区域）并单击 **Add**（添加）。
7. 输入区域 **Name**（名称）。
8. 在 **Type**（类型）下拉列表中，选择 **Layer3**（第 3 层）。
9. 在 **Interfaces**（接口）部分，单击 **Add**（添加）并添加您刚才配置的接口。
10. 单击 **OK**（确定）。

STEP 2 | 启用 DNS Sinkholing。

默认情况下，将为所有 Palo Alto Networks DNS 签名启用 Sinkholing。要将 sinkhole 地址更改为本地服务器，请参阅为自定义域列表配置 DNS Sinkholing 中的步骤验证防间谍软件配置文件中的 Sinkholing 设置。

STEP 3 | 请编辑安全策略，以允许信任区域中客户端主机的流量流向非信任区域，从而包括 Sinkhole 区域作为目标，并附加防间谍软件配置文件。

编辑安全策略规则，以允许信任区域中的客户端主机的流量流向非信任区域，从而确保标识来自受感染主机的流量。通过将 Sinkhole 区域添加为规则中的目标，您可以让受感染的客户端向 DNS Sinkhole 发送伪造的 DNS 查询。

1. 选择 **Policies**（策略）> **Security**（安全）。
2. 选择允许客户端主机区域的流量流向非信任区域的现有策略。
3. 在 **Destination**（目标）选项卡上，**Add**（添加）Sinkhole 区域。这允许客户端主机流量流向 Sinkhole 区域。
4. 在 **Actions**（操作）选项卡上，选中 **Log at Session Start**（在会话开始时记录）复选框以启用日志记录。这样可以确保在访问非信任或 Sinkhole 区域时，来自信任区域的客户端主机的流量可以得到记录。
5. 在 **Profile Setting**（配置文件设置）部分，选择您启用 DNS Sinkholing 的 **Anti-Spyware**（防间谍软件）配置文件。
6. 单击 **OK**（确定）以保存安全策略，然后单击 **Commit**（提交）。


© 2019 Palo Alto Networks, Inc.

STEP 4 | 为了确认您可以识别受感染的主机，请验证从信任区域的客户端主机流向新的 Sinkhole 区域的流量得到了记录。

在本示例中，受感染的客户端主机是 192.168.2.10，而 Sinkhole IPv4 地址为 10.15.0.20。

1. 在信任区域的客户端主机中，打开命令提示窗口并运行以下命令：

```
C:\>ping <sinkhole address>
```

以下示例显示了对 DNS Sinkhole 地址 10.15.0.2 执行 Ping 请求所产生的输出，结果显示 `Request timed out`，这是因为在示例中，Sinkhole IP 地址未分配给物理主机：

```
C:\>ping 10.15.0.20
Pinging 10.15.0.20 with 32 bytes of data:
Request timed out.
Request timed out.
Ping statistics for 10.15.0.20:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

2. 在防火墙上，选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）并找到源为 192.168.2.10 且目标为 10.15.0.20 的日志条目。这将确认 Sinkhole IP 地址的流量正在流向防火墙区域。



您可以搜索和/或筛选日志，使其仅显示目标为 *10.15.0.20* 的日志。为此，请在 *Destination*（目标）列中单击 *IP* 地址 *(10.15.0.20)*，这会将筛选条件 *(addr.dst in 10.15.0.20)* 添加到搜索字段。单击位于搜索字段右侧的“应用筛选器”图标以应用筛选条件。

STEP 5 | 测试 DNS Sinkholing 是否正确配置。

您正在模拟当恶意应用程序尝试调用主页时受感染的应用程序将执行的操作。

1. 找到防火墙的当前防病毒签名数据库中包括的一个恶意域以测试 Sinkholing。
   1. 选择 **Device**（设备）> **Dynamic**（动态）**Updates**（更新）并在 **Antivirus**（防病毒）部分单击当前安装的防病毒数据库的 **Release Notes**（发布说明）链接。您还可以在 Palo Alto Networks 支持站点上的动态更新下找到列出增量签名更新的防病毒发布说明。
   2. 在发布说明的第二列，找到带有域扩展名的一行项目（例如，com、edu 或 net）。左列将显示域名。例如，在防病毒版本 1117-1560 中，左列包括一个名为“tbsbana”的项目，且右列为“net”。

      下面显示了这一行在发布说明中的内容：

```
conficker:tbsbana 1
variants: net
```

2. 在客户端主机上打开命令提示窗口。
3. 对您识别为恶意域的 URL 执行 NSLOOKUP。

   例如，使用 URL `track.bidtrk.com`：

```
C:\>nslookup
 track.bidtrk.com
 Server: my-local-dns.local
 Address: 10.0.0.222
 Non-authoritative answer:
 Name: track.bidtrk.com.org
 Addresses: fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
```



© 2019 Palo Alto Networks, Inc.

在输出中，请注意恶意域的 NSLOOKUP 已使用配置的 Sinkhole IP 地址 (10.15.0.20) 进行伪造。由于该域与一个恶意 DNS 签名匹配，因此会执行 Sinkhole 操作。

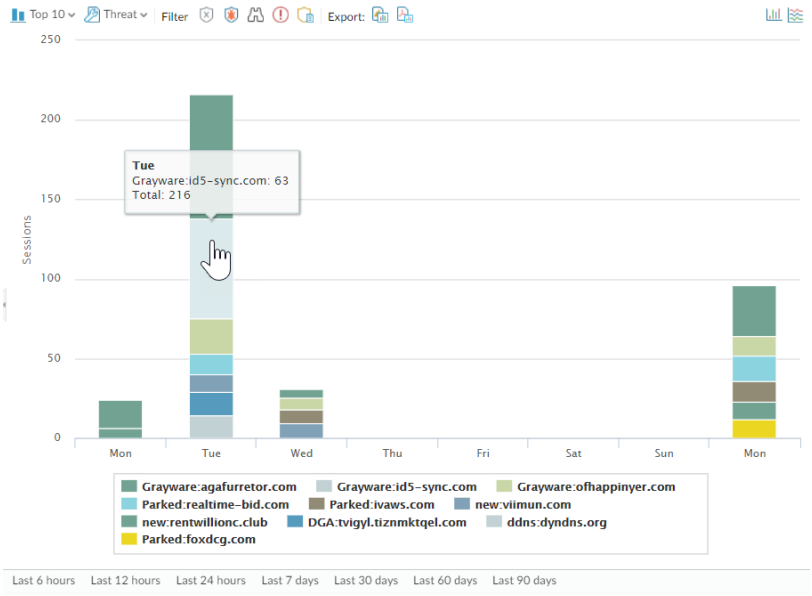
4. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁）并找到相应的日志条目，从而验证对 NSLOOKUP 请求执行了正确的操作。
5. 对 **`track.bidtrk.com`** 执行 Ping，这将产生到 Sinkhole 地址的网络流量。

# 查看试图连接到恶意域的受感染主机

在您配置 DNS Sinkholing 并验证恶意域的流量流向 Sinkhole 地址后，您应定期监控流向该 Sinkhole 地址的流量，从而跟踪受感染的主机并消灭威胁。

- 使用 App Scope 识别受感染的客户端主机。
  1. 选择 **Monitor**（监控）> **App Scope**并选择 **Threat Monitor**（威胁监控）。
  2. 单击显示页面顶部的 **Show spyware**（显示间谍软件）按钮。
  3. 选择一个时间范围。

     以下屏幕截图显示了可以 DNS 查询的三个实例，均为测试客户端主机在已知恶意域上执行 NSLOOKUP 时产生。单击图表可查看关于事件的更多详细信息。




- 对自定义报告进行配置，从而识别将流量发送到 Sinkhole IP 地址的所有客户端主机，本例中为 10.15.0.20。

  转发到 *SNMP* 管理器、*Syslog* 服务器和/或 *Panorama* 以对这些事件发出警报。

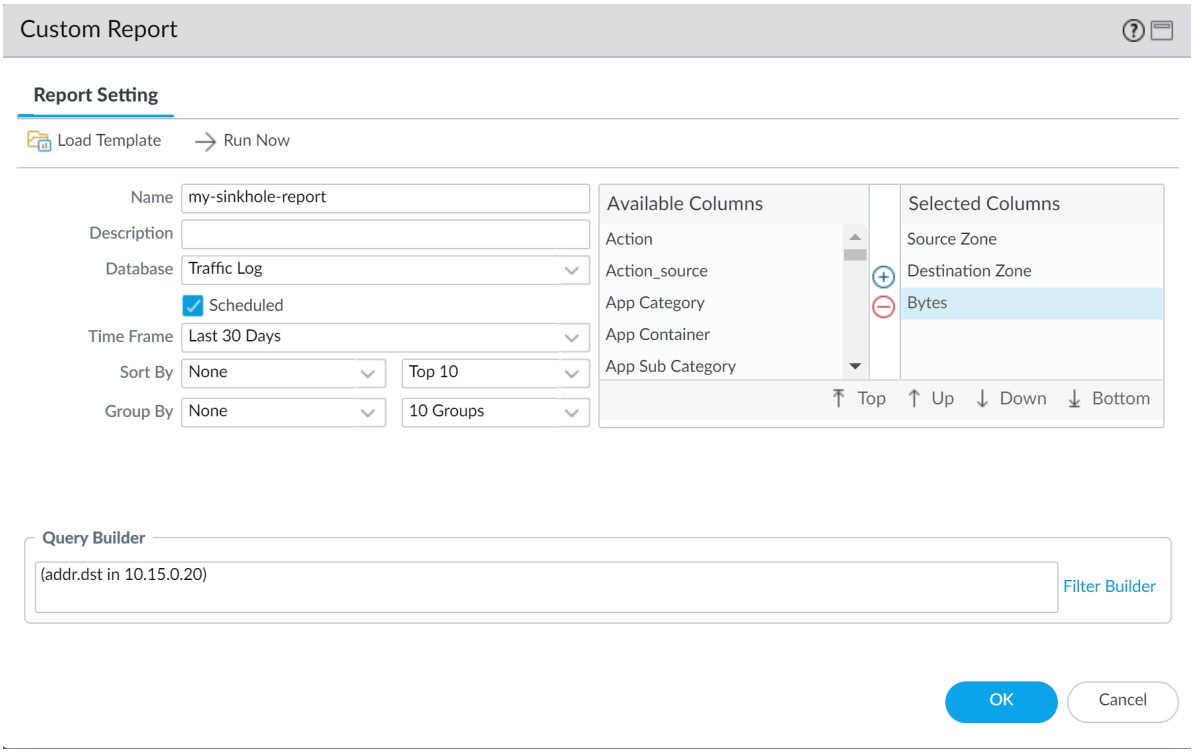
  在本例中，受感染的客户端主机对列于 Palo Alto Networks DNS 签名数据库中的已知恶意域执行了 NSLOOKUP。发生此事件时，系统会将查询发送到本地 DNS 服务器，该服务器随后通过防火墙将请求转发到外部 DNS 服务器。具有所配置的防间谍软件配置文件的防火墙安全策略将查询与 DNS 签名数据库进行匹配，然后使用 Sinkhole 地址 10.15.0.20 和 fd97:3dec:4d27:e37c:5:5:5:5 伪造回复。客户端尝试启动会话，而流量日志则会记录活动的源主机和目标地址，这将重定向到伪造的 Sinkhole 地址。

  查看防火墙上的流量日志可让您识别将流量发送到 Sinkhole 地址的任何客户端主机。在本例中，日志显示发送恶意 DNS 查询的源地址为 192.168.2.10。该主机随后将被找到并进行清理。如果没有 DNS


© 2019 Palo Alto Networks, Inc.

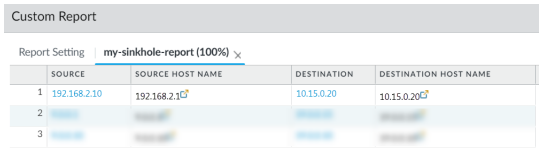
Sinkhole 选项，管理员可能只会将本地 DNS 服务器看做执行查询的系统，并且不会发现受感染的客户端主机。如果您尝试使用操作“Sinkhole”对威胁日志运行报告，该日志可能会显示本地 DNS 服务器而不是受感染的主机。

1. 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告）。
2. 单击 **Add**（添加）并 **Name**（命名）报告。
3. 定义一个自定义报告，用于捕获 Sinkhole 地址的流量，如下：
   - **Database**（数据库）— 选择 **Traffic Log**（流量日志）。
   - **Scheduled**（已计划）— 启用 **Scheduled**（已计划），报告将每晚运行。
   - **Time Frame**（时间范围）— 30 天
   - **Selected Columns**（所选列）— 选择 **Source address**（源地址）或 **Source User**（源用户）（如果您已配置 User-ID），这将识别出报告中受感染的客户端主机；并且选择 **Destination address**（目标地址），这就是 Sinkhole 地址。
   - 在该屏幕底部的部分，为 Sinkhole 地址（本例中为 10.15.0.20）的流量创建一条自定义查询。您可以在 **Query Builder**（查询生成器）窗口中输入目标地址 (**addr.dst in 10.15.0.20**)，也可以在每列中选择以下地址并单击 **Add**（添加）：Connector = and, Attribute = Destination Address, Operator = in, and Value = 10.15.0.20.单击 **Add**（添加）以添加查询。




4. 单击 **Run Now**（立即运行）以运行报告。该报告将显示所有将流量发送到 Sinkhole 地址的客户端主机，即表示这些主机很可能已经被感染。现在您可以跟踪这些主机并检查其中是否有恶意软件了。


© 2019 Palo Alto Networks, Inc.




5. 要查看已运行的已计划报告，请选择 **Monitor**（监控） > **Reports**（报告）。


© 2019 Palo Alto Networks, Inc.

# 数据筛选

使用数据筛选配置文件来防止您网络上的敏感、机密和专有信息传出。预定义模式、内置设置和可自定义的选项让您可以轻松保护包含特定文件属性（如文档标题或作者）、信用卡号、不同国家监管信息（如社保号码）和第三方数据丢失保护 (DLP) 标签的文件。

- 预定义数据模式—轻松筛选常见模式，包括信用卡号。预定义数据筛选模式还可以识别来自不同国家的特定（监管）信息，如社保号码（美国）、INSEE 识别号（法国）以及新西兰税务部门识别号。许多预定义数据筛选模式都启用了对标准（如 HIPAA、GDPR、金融现代化法案）的合规性。
- 对 **Azure** 信息保护和 **Titus** 数据分级的内置支持—预定义的文件属性允许您基于 Azure 信息保护和 Titus 标签筛选内容。Azure 信息保护标签储存在元数据中，因此务必确保您知道您想要防火墙筛选的 Azure 信息保护标签的 GUID。
- 数据丢失保护 **(DLP)** 解决方案的自定义数据模式—如果您正在使用填充文件属性的第三方端点 DLP 解决方案，以表示敏感内容，您可以创建自定义数据模式，以识别您的 DLP 解决方案标记的文件属性和值，然后基于该模式，记录或阻挡您的数据筛选配置文件检测到的文件。

## 创建数据筛选配置文件

数据筛选配置文件可防止敏感信息离开您的网络。

首先，您应创建一个可指定信息类型的数据模式以及您希望防火墙进行筛选的字段。然后，将此模式附加到数据筛选配置文件中，该配置文件指定了您希望如何实施防火墙筛选出的内容。添加数据筛选配置文件到安全策略规则，使筛选流量与此规则开始进行匹配。

STEP 1 | 定义一个新的数据模式对象，以检测要筛选的信息。

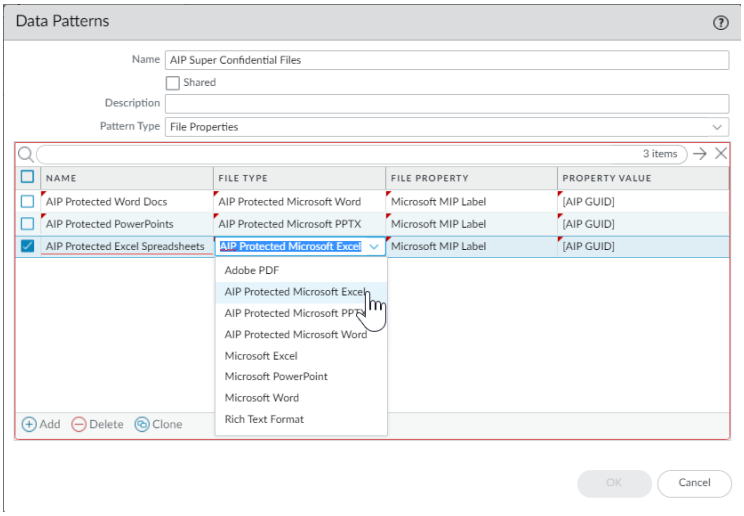
1. 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **Data Patterns**（数据模式）并 **Add**（添加）新对象。
2. 为新对象提供一个描述性 **Name**（名称）。
3. （可选）如果要使数据模式用于以下情况，请选择 **Shared**（共享）：
   - **Every virtual system (vsys) on a multi-vsys firewall**（多虚拟系统防火墙上的每个虚拟系统 **(vsys)**）— 如果取消选中（禁用），该数据模式仅对 **Objects**（对象）选项卡中选择的虚拟系统可用。
   - **Every device group on Panorama**（**Panorama** 上的每个设备组）— 如果取消选中（禁用），该数据模式仅对 **Objects**（对象）选项卡中选择的设备组可用。
4. （可选 — 仅限 Panorama）选择 **Disable override**（禁用覆盖）可阻止管理员替代设备组中继承对象的数据模式对象设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
5. （可选 — 仅限 Panorama）选择 **Data Capture**（数据捕获）以自动收集被筛选器阻止的数据。

   在设置页面上为管理数据保护指定密码，以查看捕获的数据（*Device*（设备）> *Setup*（设置）> *Content-ID* > *Manage Data Protection*（管理数据保护））。
6. 将 **Pattern Type**（模式类型）设置为以下之一：
   - **Predefined Pattern**（预定义模式）— 根据 HIPAA、GDPR、《金融服务现代化法案》等多个合规标准筛选信用卡、社会保险号和个人身份信息。
   - **Regular Expression**（正则表达式）— 用于自定义数据模式的筛选器。
   - **File Properties**（文件属性）— 基于文件属性和关联值的筛选器。
7. 将新规则 **Add**（添加）至数据模式对象。
8. 根据您为此对象选择的 **Pattern Type**（模式类型）指定数据模式：
   - 预定义 — 选择 **Name**（名称），然后选择要进行筛选的预定义数据模式。



© 2019 Palo Alto Networks, Inc.

- 正则表达式 — 指定描述性 **Name**（名称），选择要扫描的**File Type**（文件类型）（或类型），然后输入您希望防火墙检测的特定 **Data Pattern**（数据模式）。
- **File Properties**（文件属性）— 指定描述性 **Name**（名称），选择要扫描的 **File Type**（文件类型）和 **File Property**（文件属性），然后输入您希望防火墙检测的特定 **Property Value**（属性值）。
  - 要筛选 **Titus** 分类文件：选择其中一种非 AIP 保护文件类型，并将 **File Property**（文件属性）设置为 TITUS GUID。输入 Titus 标签 GUID 充当 **Property Value**（属性值）。
  - 对于 **Azure** 信息保护标签文件：选择除富文本格式之外的任何 **File Type**（文件类型）。对于选中的文件类型，将 **File Property**（文件属性）设为 Microsoft MIP 标签，并输入 Azure 信息保护标签 GUID 充当 **Property Value**（属性值）。




9. 单击 **OK**（确定）以保存数据模式。

STEP 2 | 将数据模式对象添加到数据筛选配置文件。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Data Filtering**（数据筛选），并 **Add**（添加）或修改数据筛选配置文件。
2. 为新配置文件提供一个描述性 **Name**（名称）。
3. **Add**（添加）新的配置文件规则，然后选择您在步骤中创建的数据模式。
4. 根据数据模式指定您要筛选的 **Applications**（应用程序）、**File Types**（文件类型）以及流量的 **Direction**（方向）（上传或下载）。

   您选择的文件类型必须与您之前为数据模式定义的文件类型相同，或者必须是包含数据模式文件类型的文件类型。例如，您可以同时定义数据模式对象和数据筛选配置文件，以扫描所有 *Microsoft Office* 文档。或者，您可以将数据模式对象定义为仅匹配 *Microsoft PowerPoint* 演示文稿，而数据筛选配置文件则扫描所有 *Microsoft Office* 文档。

   如果数据模式对象附加到数据筛选配置文件，并且配置的文件类型在两者之间不对齐，则配置文件将不会正确筛选与数据模式对象匹配的文档。
5. 设置 **Alert Threshold**（警报阈值）以指定在文件中检测到数据模式以触发警报的次数。
6. 设置 **Block Threshold**（阻止阈值）以阻止文件中至少包含数据模式的多个实例。
7. 设置与此规则匹配的文件记录的 **Log Severity**（日志严重性）。
8. 单击 **OK**（确定）以保存数据筛选配置文件。

STEP 3 | 将数据筛选设置应用于流量。

1. 选择 **Policies**（策略）> **Security**（安全），并 **Add**（添加）或修改安全策略规则。


© 2019 Palo Alto Networks, Inc.

2. 选择 **Actions**（操作）并将 Profile Type（配置文件类型）设置为 **Profiles**（配置文件）。
3. 将在步骤 2 中创建的数据筛选配置文件附加到安全策略规则。
4. 单击 **OK**（确定）。

STEP 4 | （推荐）防止 Web 浏览器恢复防火墙已终止的会话。

此选项确保在防火墙检测并丢弃敏感文件时，*Web* 浏览器无法恢复会话以尝试检索该文件。

1. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID**，并编辑 Content-ID 设置。
2. 清除 **Allow HTTP partial response**（允许 **HTTP** 部分响应）。
3. 单击 **OK**（确定）。

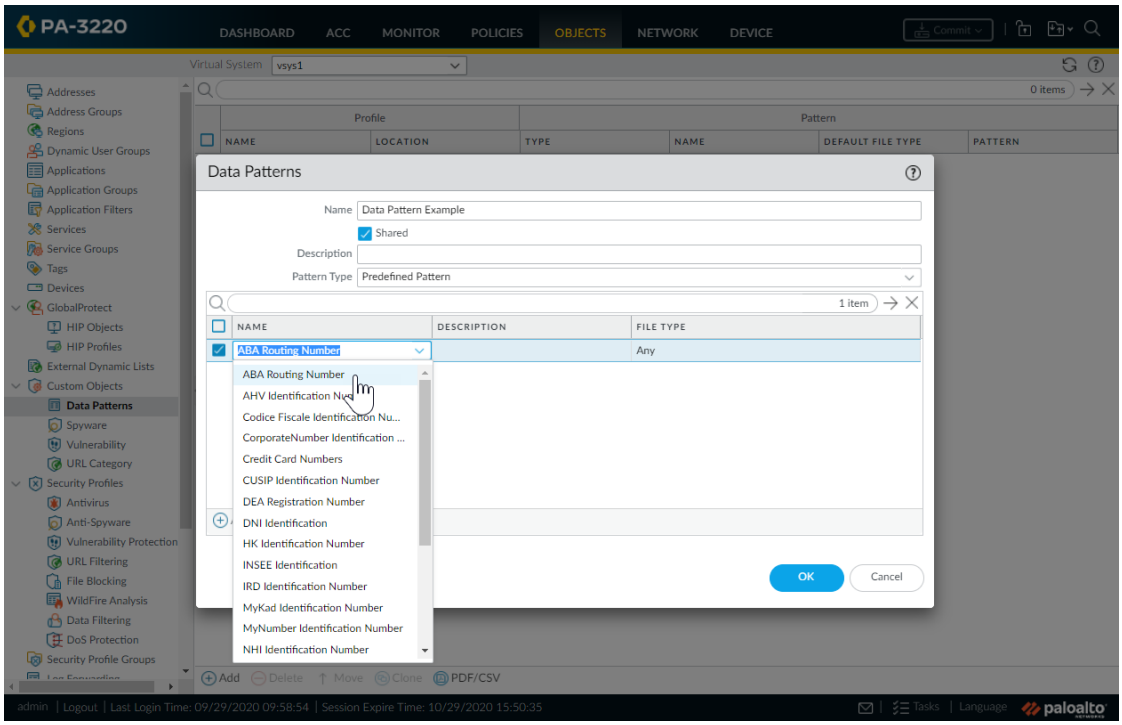
STEP 5 | 监控防火墙正在筛选的文件。

选择 **Monitor**（监控）> **Data Filtering**（数据筛选）以根据数据筛选设置查看防火墙检测到和阻止的文件。

## 预定义的数据筛选模式

要满足 HIPAA、GDPR 和《金融服务现代化法案》等标准，防火墙应提供预定义数据模式。您可以使用这些模式防止信用卡和社会保险号等常见类型的敏感信息离开您的网络。

您可以查找预定义数据模式，方法如下：选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **Data Patterns**（数据模式），然后单击 **Add**（添加）新对象。然后，设置 **Pattern Type**（模式类型）为 **Predefined Pattern**（预定义模式），并 **Add**（添加）新规则到数据模式对象。从 **Name**（名称）下显示的列表中选择数据模式。




如果想要保护的信息类型不包含在预定义模式列表内，可以使用正则表达式创建自定义模式。

以下是可用的数据模式列表：



© 2019 Palo Alto Networks, Inc.

| 模式 | 说明 |
| --- | --- |
| 信用卡号 | 16 位信用卡号 |
| 社会保险号 | 带破折号的 9 位社会保险号 |
| 社会保险号（不带破折号分隔符） | 不带破折号的 9 位社会保险号 |
| ABA 银行代号 | 美国银行协会银行代号 |
| AHV 识别号 | Swiss Alters und Hinterlassenenversicherungsnummer |
| Codice Fiscale 识别号 | 意大利财政税务号卡识别号码 |
| 公司编号识别号 | 日本国税厅公司编号 |
| CUSIP 识别号 | 统一安全标识程序委员会识别号码 |
| DEA 注册号 | 美国缉毒局注册号 |
| DNI 识别号 | Spanish Documento nacional de identidad Identification Number number |
| HK 识别号 | 香港居民身份证号码 |
| INSEE 识别号 | 法国国家统计与经济研究所识别号 |
| IRD 识别号 | 新西兰税务局识别号 |
| MyKad 识别号 | 马来西亚公民身份证识别号码 |
| MyNumber 识别号 | 日本社会保障・税番号制度识别号码 |
| NHI 识别号 | 新西兰国家健康指数编号 |
| NIF 识别号 | 西班牙纳税识别号码 |
| NIN 识别号 | 台湾身份证号码 |
| NRIC 识别号 | 新加坡国民身份证识别号码 |
| 永久帐户识别号 | 印度国民使用的印度永久帐户号码 |
| PRC 识别号 | 中华人民共和国居民身份证号码 |
| PRN 识别号 | 韩国居民登记号码 |
| 韩国居民登记 | 韩国居民登记号码 |


© 2019 Palo Alto Networks, Inc.

# WildFire Inline ML

通过防病毒配置文件中的 WildFire inline ML 选项，防火墙数据面板可在可移植可执行文件 (PE) 和 PowerShell 脚本上实时使用机器算法。这一层防病毒保护是对基于 WildFire 的签名的补充，可扩展至尚不存在签名的文件。各个 inline ML 模型通过评估文件详细信息（包括解码器字段和模式），动态检测特定类型的恶意文件，从而形成文件的高概率分类。这种保护可扩展至当前已知以及未来可能会发生变化的、与 Palo Alto Networks 标识为恶意的特征相匹配的威胁。为了跟上威胁形势的最新变化，可以通过内容发布添加或更新 inline ML 模式。启用 WildFire inline ML 前，必须要拥有有效的 WildFire 订阅。

作为 URL 过滤配置的一部分，还可启用基于 Inline ML 的保护以实时检测恶意 URL。有关详细信息，请参阅：URL 过滤 Inline ML

*VM-50* 或 *VM50L* 虚拟设备不支持 *WildFire inline ML*。

## 配置 WildFire Inline ML

若要启用 WildFire inline ML 配置，需将使用 inline ML 设置配置的防病毒配置文件附加到安全策略规则（请参阅设置防病毒威胁、防间谍软件和漏洞防护）。

*VM-50* 或 *VM50L* 虚拟设备当前不支持 *WildFire inline ML*。

STEP 1 | 若要利用 WildFire inline ML，必须具有一个可用于分析 Windows 可执行文件的有效 WildFire 订阅。

确认您是否具有 WildFire 订阅。若要确认您当前拥有许可证是何种订阅，请选择 **Device**（设备）> **Licenses**（许可证），确认是否显示相应的许可证，许可证是否已过期。

WildFire License

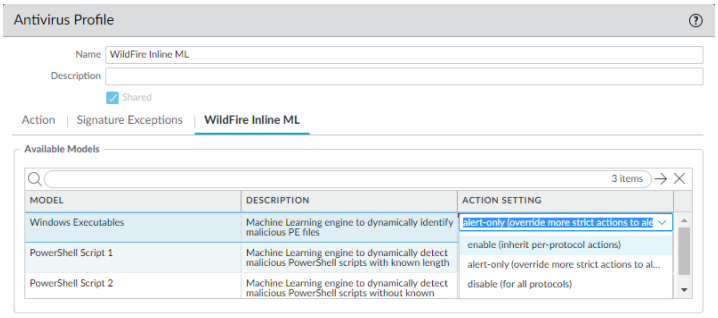
| | |
|---|---|
| Date Issued | July 25, 2019 |
| Date Expires | July 25, 2020 |
| Description | WildFire signature feed, integrated WildFire logs, WildFire API |

STEP 2 | 创建新的防病毒安全配置文件，或是更新现有防病毒安全配置文件以使用实时 WildFire inline ML 模式。

1. 选择现有 **Antivirus Profile**（防病毒配置文件）或新建一个（选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）并 **Add**（添加）新配置文件）。
2. 配置防病毒配置文件。
3. 选择 **WildFire Inline ML**选项卡，并为每个 WildFire Inline ML 模式使用 **Action Setting**（操作设置）。这会强制针对每种模式为所有协议配置 WildFire Inline ML 操作设置。目前提供三种分类引擎：Windows 可执行文件、PowerShell 脚本 1 和 PowerShell 脚本 2。



© 2019 Palo Alto Networks, Inc.



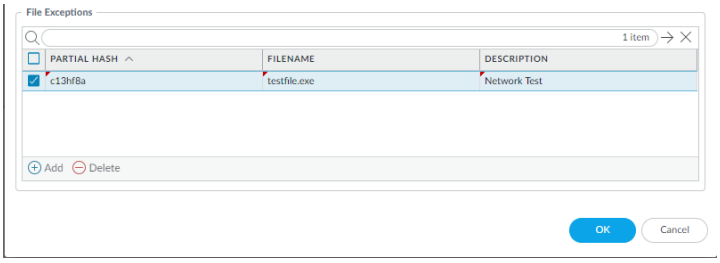

- **enable (inherit per-protocol actions)**（启用（继承每个协议操作））— WildFire 根据您在 **Action**（操作）选项卡“解码器”部分“WildFire Inline ML 操作”列中的选择检查流量。
- **alert-only (override more strict actions to alert)**（仅警报（替代更严格的警报操作））— WildFire 根据您在 **Action**（操作）选项卡“解码器”部分“WildFire Inline ML 操作”列中的选择检查流量，并以高于警报（丢弃、重置客户端、重置服务器、重置两者）的严重性级别替代任何操作，警报允许流量通过，同时仍能生成警报并保存到威胁日志中。
- **disable (for all protocols)**（禁用（对于所有协议））— WildFire 允许流量通过，无需任何策略操作。

4. 单击 **OK**（确定）从防病毒配置文件的配置窗口退出，并 **Commit**（提交）新设置。

STEP 3 | （可选）如果遇到误报，添加例外文件到您的防病毒安全配置文件。您可以直接将例外文件详细信息添加到例外列表，或是通过指定威胁日志中的文件添加例外文件详细信息。

- 直接将例外文件添加到例外列表。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）。
2. 选择想要排除特定文件的防病毒配置文件，然后选择 **WildFire Inline ML**。
3. 添加要从实施中排除的文件的哈希、文件名和说明。




4. 单击 **OK**（确定）以保存防病毒配置文件，然后 **Commit**（提交）更新。

- 从威胁日志条目中添加例外文件。

1. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），然后在日志中筛选 **ml-virus** 威胁类型。为要创建例外的文件选择威胁日志。
2. 前往 **Detailed Log View**（详细日志视图），然后向下滚动至 **Details**（详细信息）窗格，选择 **Create Exception**（创建例外）。




3. 添加 **Description**（说明），然后单击 **OK**（确定）以添加例外文件。
4. 可在 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）> **WildFire Inline ML**下的 **File Exceptions**（例外文件）列表中找到新的例外文件。

STEP 4 | （可选）检查防火墙与 Inline ML 云服务的连接状态。

在防火墙上使用以下 CLI 命令查看连接状态。


© 2019 Palo Alto Networks, Inc.

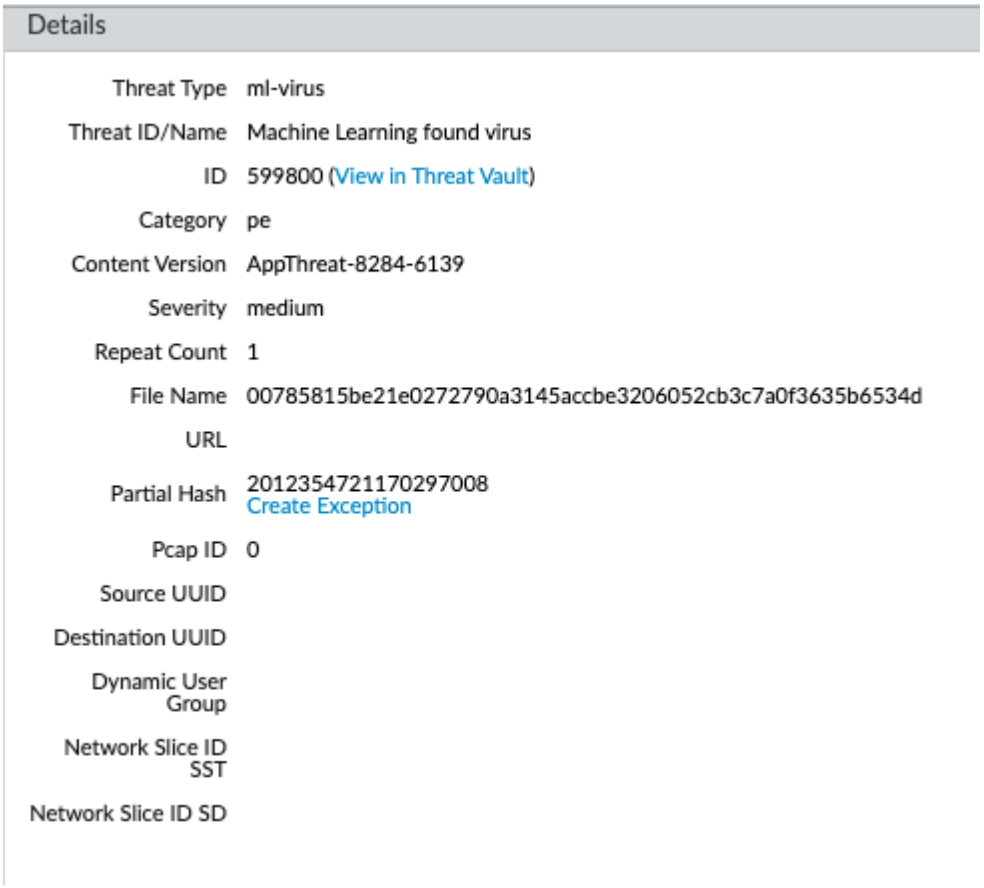
```
show mlav cloud-status
```

例如：

```
show mlav cloud-status

MLAV cloud
Current cloud server:          ml.service.paloaltonetworks.com
Cloud connection:              connected
```

如果无法连接到 Inline ML 云服务，请检验以下域是否被阻止：ml.service.paloaltonetworks.com。

若要查看 WildFire Inline ML 检测到的文件信息，请检查威胁日志（**Monitor**（监控）**> Logs**（日志）**> Threat**（威胁），然后从列表中选择日志类型）。使用 WildFire inline ML 分析过的文件将被标记为威胁类型 **ml-virus**：






© 2019 Palo Alto Networks, Inc.

# 设置文件阻止

文件阻止配置文件可用来识别要阻止或监视的特定文件类型。对于大多数流量（包括内网流量），已知具有威胁或无实际上传/下载应用价值的阻止文件。目前，这些包括批处理文件、DLLs、Java 类文件、帮助文件、Windows 快捷方式 (.lnk) 及 BitTorrent 文件。此外，为防止隐藏下载，您可允许下载/上传执行及档案文件（.zip 和 .rar），但需强制用户确认其在传输文件，以便用户注意到浏览器正在尝试下载他们没有注意到的内容。对于允许常规 Web 浏览的策略规则，文件阻止设置应更为严密，原因是其所面临的用户在未察觉情况下下载恶意软件的风险更高。针对此类流量，添加更为严格的文件传送阻止配置文件，该配置文件同时亦可阻止可移植可执行 (PE) 文件。

您可以定义自己的自定义文件阻止配置文件，或者在将文件阻止应用于安全策略规则时，选择以下预定义配置文件之一。您可以克隆并编辑在内容发行版本 653 及更高版本中可用的预定义配置文件，然后在传输到文件阻止最佳实践设置时，按照文件阻止配置文件安全传输步骤保留应用程序可用性：

- **basic file blocking**（基本文件阻止）— 将此配置文件附加到安全策略规则，允许流量往来于较不敏感的应用程序，以阻止通常包含在恶意软件攻击活动中的文件，或是没有上传/下载的真正用例。此配置文件阻止 PE 文件 (.scr, .cpl, .dll, .ocx, .pif, .exe)、Java 文件 (.class, .jar)、帮助文件 (.chm, .hlp) 以及其他潜在的恶意文件类型 (.vbe, .hta, .wsf, .torrent, .7z, .rar, .bat) 的上传和下载。此外，它提示用户确认何时尝试下载加密的 rar 或加密的 zip 文件。此规则会对所有其他文件类型发出警报，以便您全面了解进出网络的所有文件类型。
- **strict file blocking**（严格文件阻止）— 在安全策略规则中使用更严格的配置文件，允许访问最敏感的应用程序。此配置文件阻止与其他配置文件相同的文件类型，另外阻止 Flash、.tar、多级编码、.cab、.msi、加密的 rar 和加密的 zip 文件。

这些预定义配置文件旨在为您提供最安全的网络状态。但是，如果您的业务关键型应用程序依赖某些在这些默认配置文件中被阻止的应用程序，则可以根据需要复制配置文件并进行修改。确保您只对需要上传和/或下载危险文件类型的用户使用修改的配置文件。另外，为了减少攻击面，请确保您正在使用其他安全措施来确保用户上传和下载的文件不会对您的组织构成威胁。例如，如果必须允许下载 PE 文件，请确保您将所有未知的 PE 文件发送到 WildFire 进行分析。另外，保持严格的 URL 筛选策略，以确保用户无法从已知承载有恶意内容的网站下载内容。

STEP 1 | 创建文件阻止配置文件。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **File Blocking**（文件阻止）并 **Add**（添加）配置文件。
2. 输入文件阻止配置文件的 **Name**（名称），例如 **`Block_EXE`**。
3. （可选）输入 **Description**（说明），例如 **`Block users from downloading exe files from websites`**。
4. （可选）指定配置文件与以下内容 **Shared**（共享）：
   - **Every virtual system (vsys) on a multi-vsys firewall**（多虚拟系统防火墙上的每个虚拟系统 (vsys)）— 如果取消选中（禁用），该配置文件仅对 **Objects**（对象）选项卡中选择的虚拟系统可用。
   - **Every device group on Panorama**（Panorama 上的每个设备组）— 如果取消选中（禁用），该配置文件仅对 **Objects**（对象）选项卡中选择的设备组可用。
5. （可选 — 仅限 Panorama）选择 **Disable override**（禁用覆盖）可阻止管理员替代设备组中继承配置文件的文件阻止配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。

STEP 2 | 配置文件传送阻止选项。

1. **Add**（添加）并定义配置文件规则。
2. 输入规则 **Name**（名称），例如 **`BlockEXE`**。
3. 选择 **Any**（任何）或指定一个或多个特定的 **Applications**（应用程序）进行筛选，例如 **web-browsing**（**Web** 浏览）。


© 2019 Palo Alto Networks, Inc.

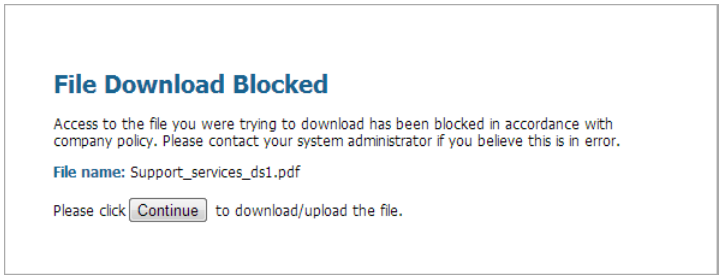
只有 *Web* 浏览器可以显示响应页面（继续提示），允许用户确认其在阻止流量中选择用于这些应用程序的任何其他应用程序结果，因为没有提示显示允许用户继续。

4. 选择 **Any**（任何）或指定一个或多个特定的 **File Types**（文件类型），例如 **exe**。
5. 指定 **Direction**（方向），例如 **download**（下载）。
6. 指定 **Action**（操作）（**alert**（警报）、**block**（阻止）或 **continue**（继续））。例如，在允许下载可执行文件 (.exe) 之前，请选择 **continue**（继续）提示用户进行确认。或者，您可以 **block**（阻止）指定的文件，或者当用户下载可执行文件时，您可以将防火墙配置为仅触发 **alert**（警报）。
7. 单击 **OK**（确定）保存配置文件。

STEP 3 | 将文件阻止配置文件应用于安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择一项现有策略规则或 **Add**（添加）一项新策略规则，如设置基本安全策略中所述。
2. 在 **Actions**（操作）选项卡上，选择您在上一步中配置的文件阻止配置文件。在此示例中，配置文件名称为 **`Block_EXE`**。
3. **Commit**（提交）配置。

STEP 4 | 为了测试文件阻止配置，请访问防火墙信任区域中的端点 PC，并尝试从不可信区域的网站中下载可执行文件；应显示响应页面。单击 **Continue**（继续）确认您可以下载该文件。也可以设置其他操作，如 **alert**（警报）或 **block**（阻止），这些操作不提供用户继续下载的选项。。下面显示了文件传送阻止的默认响应页面：




STEP 5 | （可选）定义自定义文件阻止响应页面（**Device**（设备）> **Response Pages**（响应页面））。这允许您在响应页面中向用户提供详细信息。您可以包含诸如公司政策信息和技术支持人员的联系信息。

当您使用 *continue*（继续）操作创建文件阻止配置文件时，您只能选择 *web-browsing*（*Web* 浏览）应用程序。如果选择任何其他应用程序，则由于不存在提示用户继续操作的选项，因此匹配安全策略的通信不会流经防火墙。此外，您需要配置和启用 *HTTPS* 网站的解密策略。

检查日志以确定测试此功能时使用的应用程序。例如，如果使用 *Microsoft SharePoint* 下载文件，则即使使用 *web-browser* 来访问站点，应用程序实际上是 *`sharepoint-base`* 或 *`sharepoint-document`*。（有助于将应用程序类型设置为 *Any*（任何）以进行测试。）



© 2019 Palo Alto Networks, Inc.

# 防止暴力攻击

暴力攻击使用来自同一源或目标 IP 地址的大量请求/响应攻击系统。攻击者采用反复试验法猜出对挑战或请求的响应。

防火墙上的漏洞防护配置文件包括可用来防止暴力攻击的签名。每个签名都拥有 ID、威胁名称、严重性且在记录模式时触发。模式指定将流量识别为暴力攻击的条件和时间间隔；一些签名与另一个严重性较低的子签名关联，并用于指定要匹配的模式。当模式与签名或子签名匹配时，它会触发签名的默认操作。

要加强保护：

- 将漏洞保护配置文件附加至安全策略规则。请参阅设置抗病毒、防间谍软件和漏洞保护。
- 安装包含新签名的内容更新以防止新出现的威胁。请参阅安装内容和软件更新。



© 2019 Palo Alto Networks, Inc.

# 自定义暴力签名的操作和触发条件

防火墙包括两种类型的预定义暴力签名：父签名和子签名。子签名是与签名匹配的流量模式的一个单一事件。父签名与子签名关联，并在指定时间间隔内发生多个事件且与在子签名中定义的流量模式匹配时触发。

通常，子签名的默认操作为允许，因为单个事件并不代表攻击。这样可确保不会阻止合法流量，并且也不会为不值得关注的事件生成威胁日志。Palo Alto Networks 建议您在更改默认操作前应仔细考虑。

在大多数情况下，暴力签名是一个值得关注的事件，因为它会频繁发生。如果需要，可以执行以下操作之一来自定义暴力签名的操作：

- 创建规则以修改暴力类别中所有签名的默认操作。可以选择允许、警报、阻止、重置或丢弃流量。
- 定义特定签名的例外。例如，可以搜索 CVE 并为其定义例外。

对于父签名，可以同时修改触发条件和操作；对于子签名，只能修改操作。



要有效地减轻攻击，请指定 *block-ip* 地址操作，而不是丢弃或重置大多数暴力签名的操作。

STEP 1 | 创建新的漏洞防护配置文件。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Vulnerability Protection**（漏洞保护）并 **Add**（添加）配置文件。
2. 输入漏洞保护配置文件的 **Name**（名称）。
3. （可选）输入 **Description**（说明）。
4. （可选）指定配置文件与以下内容 **Shared**（共享）：
   - **Every virtual system (vsys) on a multi-vsys firewall**（多虚拟系统防火墙上的每个虚拟系统 **(vsys)**）— 如果取消选中（禁用），该配置文件仅对 **Objects**（对象）选项卡中选择的虚拟系统可用。
   - **Every device group on Panorama**（**Panorama** 上的每个设备组）— 如果取消选中（禁用），该配置文件仅对 **Objects**（对象）选项卡中选择的设备组可用。
5. （可选 — 仅限 Panorama）选择 **Disable override**（禁用覆盖）可阻止管理员替代设备组中继承配置文件的漏洞防护配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。

STEP 2 | 创建规则用于定义类别中所有签名的操作。

1. 在 **Rules**（规则）选项卡上，**Add**（添加）并输入新规则的 **Rule Name**（规则名称）。
2. （可选）指定特定的威胁名称（默认为 **any**（任何））。
3. 设置 **Action**（操作）。在本例中，将其设置为 **Block IP**（阻止 **IP**）。

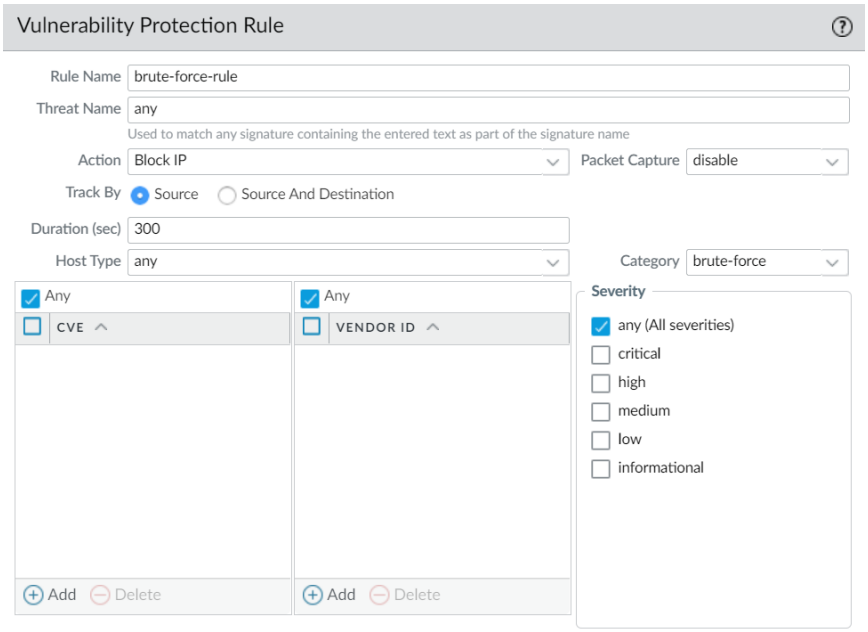


如果将漏洞保护配置文件设置为阻止 *IP*，则防火墙首先使用硬件来阻止 *IP* 地址。如果攻击流量超过硬件的阻止能力，则防火墙会使用软件阻止机制来阻止剩余的 *IP* 地址。

4. 将 **Category**（类别）设置为 **brute-force**（暴力）。
5. （可选）如果阻止，请指定要阻止的 **Host Type**（主机类型）：**server**（服务器）或 **client**（客户端）（默认为**any**（任何））。
6. 请参阅步骤 3 以自定义特定签名的操作。
7. 请参阅步骤 4 以自定义父签名的触发阈值。



© 2019 Palo Alto Networks, Inc.

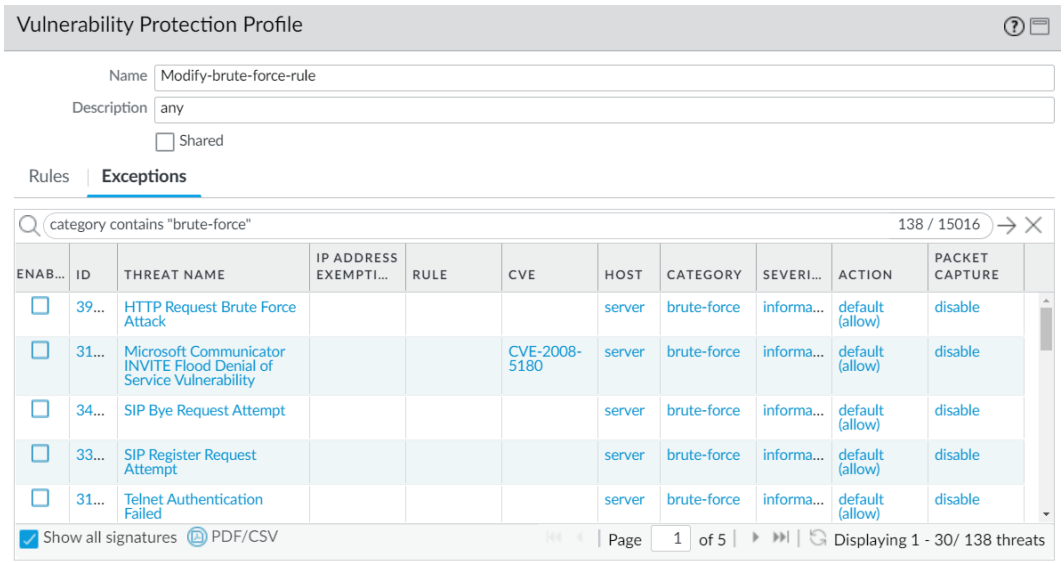



8. 单击 **OK**（确定）以保存规则和配置文件。

STEP 3 | （可选）自定义特定签名的操作。

1. 在 **Exceptions**（例外）选项卡上，**Show all signatures**（显示所有签名）以查找要修改的签名。

   要查看暴力类别中的所有签名，搜索 `category contains 'brute-force'`（包含"`brute-force`"的类别）。
2. 要编辑特定签名，单击 Action（操作）列中的预定义默认操作。




3. 设置操作：**Allow**（允许）、 **Alert**（警报）、**Block Ip**（阻止 Ip）或 **Drop**（丢弃）。如果选择 **Block Ip**（阻止 Ip），请完成以下额外任务：
   1. 指定在之后触发操作的 **Time**（时间）段（以秒为单位）。
   2. 指定是否使用 **IP source**（IP 源）或 **IP source and destination**（IP 源和目标）**Track By**（跟踪标准）并阻止 IP 地址。
4. 单击 **OK**（确定）。
5. 对于每一个修改的签名，选中 **Enable**（启用）列中的复选框。


© 2019 Palo Alto Networks, Inc.

6. 单击 **OK**（确定）。

STEP 4 | 自定义父签名的触发条件。

可以编辑的父签名使用此图标标记：。

在本例中，搜索条件为暴力类别和 CVE-2008-1447。

1. 编辑 () 签名的时间属性和聚合条件。
2. 要修改触发阈值，请指定每 **seconds**（秒）的 **Number of Hits**（击中数）。
3. 指定是否按 **source**（源）、**destination**（目标）或 **source-and-destination**（源到目标）汇总击中数（**Aggregation Criteria**（聚合标准））。
4. 单击 **OK**（确定）。

STEP 5 | 将新配置文件附加到安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），并 **Add**（添加）或修改安全策略规则。
2. 在 **Actions**（操作）选项卡上，选择 **Profiles**（配置文件）作为配置文件设置的 **Profile Type**（配置文件类型）。
3. 选择您的 **Vulnerability Protection**（漏洞保护）配置文件。
4. 单击 **OK**（确定）。

STEP 6 | 提交更改。

1. 单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 启用规避签名

Palo Alto Networks 规避签名检测创建的 HTTP 或 TLS 请求，并且可以向客户端连接到除 DNS 查询中指定域之外的域的实例提供警报。只有在防火墙还能够充当 DNS 代理并解析域名查询时，规避签名才有效。最佳实践是采取以下步骤启用规避签名。

STEP 1 | 启用客户端和服务器的防火墙中介，以充当 DNS 代理。

配置 DNS 代理对象，包括：

- 指定想要防火墙侦听 DNS 查询的接口。
- 定义防火墙将与其通信以解析 DNS 请求的 DNS 服务器。
- 设置防火墙无需联系 DNS 服务器即可在本地解析的静态 FQDN 到 IP 地址条目。
- 为已解析的主机名到 IP 地址映射启用缓存。

STEP 2 | 获取最新的应用程序和威胁内容版本（至少为内容版本 579 或更高版本）。

1. 选择**Device**（设备）> **Dynamic Updates**（动态更新）。
2. **Check Now**（立即检查）以获取最新的应用程序和威胁内容更新。
3. 下载并安装应用程序和威胁内容版本 579（或更高版本）。

STEP 3 | 定义防火墙如何执行与规避签名相匹配的流量。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件），然后 **Add**（添加）或修改防间谍软件配置文件。
2. 选择 **Exceptions**（例外），然后选择 **Show all signatures**（显示所有签名）。
3. 基于关键字 `evasion`（规避）筛选签名。
4. 对于所有规避签名，将 **Action**（操作）设置为除允许或默认操作之外的任何设置（对于规避签名，默认操作为允许）。例如，将签名 ID 14978 和 14984 的 **Action**（操作）设置为 **alert**（警报）或 **drop**（丢弃）。
5. 单击 **OK**（确定）以保存更新后的防间谍软件配置文件。
6. 将防间谍软件配置文件附加至安全策略规则：选择 **Policies**（策略）> **Security**（安全），再选择要修改的目标策略，最后单击 **Actions**（操作）选项卡。在“配置文件设置”中，单击 **Anti-Spyware**（防间谍软件）旁边的下拉列表，然后选择刚修改的防间谍软件配置文件以执行规避签名。

STEP 4 | 提交更改。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 监控阻止 IP 列表

防火墙维护其阻止的源 IP 地址阻止列表。当防火墙阻止源 IP 地址时，例如当您配置以下任一策略规则时，防火墙在这些数据包使用 CPU 或数据包缓冲区资源之前阻止硬件流量：

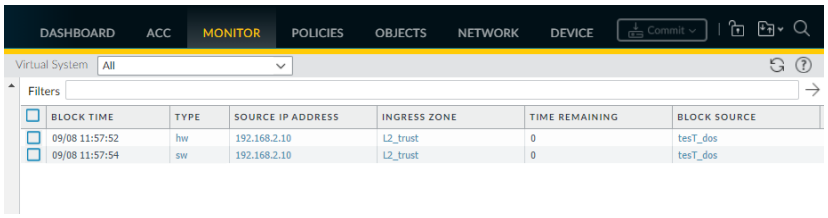
- 分类的 DoS 保护策略规则，具有 **Protect**（保护）操作（分类的 DoS 保护策略指定传入连接匹配源 IP 地址、目标 IP 地址或源和目标 IP 地址对，并与分类的 DoS 保护配置文件相关联，如针对新会话的泛滥攻击配置 DoS 保护中所述）。
- 使用漏洞保护配置文件的安全策略规则

PA-3200 防火墙、PA-5200 系列和 PA-7000 系列防火墙支持阻止硬件 IP 地址。

您可以查看阻止列表，获取有关阻止列表中 IP 地址的详细信息，或查看硬件和软件正在阻止的地址数。如果认为不应该阻止，可以从列表中删除 IP 地址。您可以更改列表中地址详细信息的来源。您还可以更改硬件阻止 IP 地址的时长。

- 查看阻止列表条目。
  1. 选择 **Monitor**（监控）> **Block IP List**（阻止 **IP** 列表）。

     在类型列表中指示硬件 (hw) 或软件 (sw) 是否阻止阻止列表中的条目。
  2. 在屏幕底部查看：
     - 防火墙支持的阻止 IP 地址数量中的 **Total Blocked IPs**（总阻止 **IP**）计数。
     - 防火墙使用的阻止列表百分比。
  3. 要筛选显示的条目，请在列中选择一个值（在 **Filters**（筛选器）字段中创建一个筛选器），并应用筛选器 ()。否则，防火墙将显示前 1,000 个条目。
  4. 输入 **Page**（页面）编号，或单击屏幕底部的箭头，以向前滚动条目页。
  5. 要查看阻止列表上地址的详细信息，请将鼠标悬停在源 IP 地址上，然后单击向下箭头链接。点击 **Who Is** 链接，显示有关地址的网络解决方案 Who Is 信息。




- 删除阻止列表条目。

  如果确定不应该阻止 *IP* 地址，则删除该条目。然后，应修改导致防火墙阻止地址的策略规则。

  1. 选择 **Monitor**（监控）> **Block IP List**（阻止 **IP** 列表）。
  2. 选择一个或多个条目，然后单击 **Delete**（删除）。
  3. （可选）选择 **Clear All**（清除所有）以从列表中删除所有条目。

- 禁用或重新启用硬件 IP 地址阻止以进行排除故障。

  禁用硬件 *IP* 地址阻止，防火墙仍执行您配置的任何软件 *IP* 地址阻止。

```
> set system setting hardware-acl-blocking [enable | disable]
```



© 2019 Palo Alto Networks, Inc.



为节省 *CPU* 和数据包缓冲区资源，并将硬件 *IP* 地址阻止保持启用的状态，除非 *Palo Alto Networks* 的技术支持要求您禁用，例如，正在调试流量时。

- 调整硬件阻止的 IP 地址保留在阻止列表中的秒数（范围为1-3,600；默认为 1）。

```
> set system setting hardware-acl-blocking duration <seconds>
```



硬件阻止列表条目的保留时间短于软件阻止列表条目，以减少超出硬件阻止能力的事件发生。

- 更改默认网站，从网络解决方案 Who Is 到不同的网站查找更多有关 IP 地址的消息。

```
# set deviceconfig system ip-address-lookup-url <url>
```

- 查看硬件和软件阻止的源 IP 地址数量，例如查看攻击速率。

  查看硬件阻止表和阻止列表上的 IP 地址条目总和（被硬件和软件阻止）：

```
> show counter global name flow_dos_blk_num_entries
```

  查看硬件阻止表上被硬件阻止的 IP 地址条目数：

```
> show counter global name flow_dos_blk_hw_entries
```

  查看阻止列表上被软件阻止的 IP 地址条目数：

```
> show counter global name flow_dos_blk_sw_entries
```

- 查看 PA-7000 系列防火墙上每个插槽的阻止列表信息。

```
> show dos-block-table software filter slot <slot-number>
```



© 2019 Palo Alto Networks, Inc.

# 威胁签名类别

有三种均用于在防火墙扫描网络流量时检测不同威胁类型的 Palo Alto Networks 威胁签名类型：

- 防病毒签名 — 检测可执行文件和文件类型中发现的病毒和恶意软件。
- 防间谍软件签名 — 检测命令和控制 (C2) 活动，受感染客户端上的间谍软件将通过这些活动，在未经用户同意的情况下收集数据和/或与远程攻击者通信。
- 漏洞签名 — 检测攻击者有可能会试图利用的系统缺陷。

签名的严重性表明检测到事件的风险。签名的默认操作（例如，阻止或警告）正是 Palo Alto Networks 推荐您实施匹配流量的方式。

您必须设置防病毒、防间谍软件和漏洞保护，以告知防火墙在检测到威胁时应该如何操作，同时，您也能轻松使用默认的安全配置文件，根据 Palo Alto Networks 建议开始阻止威胁。对于每种签名类型、类别，甚至是特定签名，您都可以继续修改或创建新的配置文件，以便更精细地执行潜在威胁。

下表按类别（防病毒、间谍软件和漏洞）列出了所有可能的签名类别，并包含每个类别中提供签名的内容更新（应用程序和威胁、防病毒或 WildFire）。此外，还可以前往 Palo Alto Networks 威胁库以进一步了解威胁签名。

| 威胁类别 | 提供这些签名的内容更新 | 说明 |
|---|---|---|
| 防病毒签名 | | |
| apk | 反病毒<br>WildFire 或 WildFire Private | 恶意安卓应用程序 (APK) 文件。 |
| dmg | 反病毒<br>WildFire 或 WildFire Private | 与 Mac OS X 一起使用的恶意 Apple 磁盘映像 (DMG) 文件。 |
| flash | 反病毒<br>Wildfire 或 WildFire Private | 嵌入网页的 Adobe Flash 小程序和 Flash 内容。 |
| java-class | 反病毒 | Java applet（JAR/Class 文件类型）。 |
| macho | 反病毒<br>Wildfire 或 WildFire Private | Mach 对象文件 (Mach-O) 是 Mac OS X 原生的可执行文件、库和对象代码。 |
| 办事处 | 反病毒<br>Wildfire 或 WildFire Private | Microsoft Office 文件，包括文档（DOC、DOCX、RTF）、工作簿（XLS、XLSX）和 PowerPoint（PPT、PPTX）。 |
| openoffice | 反病毒<br>Wildfire 或 WildFire Private | Office Open XML (OOXML) 2007+ 文档。 |



© 2019 Palo Alto Networks, Inc.

| 威胁类别 | 提供这些签名的内容更新 | 说明 |
| --- | --- | --- |
| pdf | 反病毒<br>Wildfire 或 WildFire Private | 可移植文档格式 (PDF) 文件。 |
| pe | 反病毒<br>Wildfire 或 WildFire Private | 可移植可执行 (PE) 文件可以在 Microsoft Windows 系统上自动执行，并且仅在获得授权时才被允许。这些文件类别包括：<br>• 对象代码。<br>• 字体 (FON)。<br>• 系统文件(SYS)。<br>• 驱动程序文件 (DRV)。<br>• Windows 控制面板项目 (CPL)。<br>• 动态链接库 (DLL)。<br>• 用于 OLE 自定义控件或 ActiveX 控件的库 (OCX)。<br>• 可用于执行其他文件的脚本 (SCR)。<br>• 在 OS 和固件之间运行，以便于设备更新和引导操作的可扩展固件接口 (EFI)。<br>• 程序信息文件 (PIF)。 |
| pkg | 反病毒<br>Wildfire 或 WildFire Private | 与 Mac OS X 一起使用的 Apple 软件安装程序包 (PKG)。 |
| 间谍软件签名 | | |
| 通告 | 应用程序和威胁 | 监测可能会显示不需要的广告的程序。一些广告软件会修改浏览器以突出显示并超链接 Web 页面上最常搜索的关键字 — 这些链接将用户重定向到广告网站。此外，广告软件还会从命令和控制 (C2) 服务器检索更新，并将这些更新安装到浏览器或客户端系统上。<br>此类别的新发布保护工具很少见。 |
| autogen | 反病毒 | 这些基于有效负载的签名可以检测命令和控制 (C2) 流量，并自动生成。重要的是，即使是 C2 主机未知或变化迅速，自动生成的签名也能检测到 C2 流量。 |
| 后门 | 应用程序和威胁 | 检测允许攻击者未经授权远程访问系统的程序。 |
| Botnet | 应用程序和威胁 | 显示 botnet 活动。Botnet 是被攻击者控制的受恶意软件感染的计算机（“机器人”）网络。攻击者可以集中命令 botnet 中的每台计算机，并同时执行协调操作（例如，启动 DoS 攻击等）。 |
| 浏览器劫持 | 应用程序和威胁 | 检测正在修改浏览器设置的插件或软件。浏览器劫持者可能会接管自动搜过或跟踪用户的 Web 活动，并将此信息发送给 C2 服务器。<br>此类别的新发布保护工具很少见。 |


© 2019 Palo Alto Networks, Inc.

| 威胁类别 | 提供这些签名的内容更新 | 说明 |
| --- | --- | --- |
| 挖矿程序 | 应用程序和威胁 | （有时也称为加密攻击或挖掘程序）检测利用计算资源在用户不知情的情况下挖掘加密货币的恶意程序的下载尝试或产生的网络流量。挖矿程序的二进制文件通常由尝试确定系统基础架构的 Shell 脚本下载器传输，会杀死系统上的其他挖掘程序进程。一些挖掘程序进程在其他进程中执行，例如呈现恶意 Web 页面的 Web 浏览器。 |
| 数据窃取 | 应用程序和威胁 | 检测向已知 C2 服务器发送信息的系统。<br>此类别的新发布保护工具很少见。 |
| dns | 反病毒 | 检测连接到恶意域的 DNS 请求。<br>Dns 和 dns-wildfire 签名检测相同的恶意域；但是，dns 签名包含在日常的防病毒内容更新中，dns-wildfire 签名包含在每 5 分钟发布保护措施的 Wildfire 更新中。 |
| dns-security | 反病毒 | 检测连接到恶意域的 DNS 请求。<br>除 DNS 安全服务生成的唯一签名外，dns-security 还包括来自 dns 和 dns-wildfire 的签名。 |
| dns-wildfire | Wildfire 或 WildFire Private | 检测连接到恶意域的 DNS 请求。<br>Dns 和 dns-wildfire 签名检测相同的恶意域；但是，dns 签名包含在日常的防病毒内容更新中，dns-wildfire 签名包含在每 5 分钟发布保护措施的 Wildfire 更新中。 |
| 下载程序 | 应用程序和威胁 | （也被称为植入程序、stager 或加载程序）检测利用互联网连接到远程服务器以在受影响系统上下载并执行恶意软件的程序。最常见的用例是在网络攻击第一阶段的最高点部署的下载程序，其中，执行下载程序所获取的有效载荷被视为第二阶段。常见的下载程序类型包括 Shell 脚本（Bash，PowerShell 等）、特洛伊木马、以及 PDF 和 Word 文件等恶意诱惑文档（也称为 maldos）。 |
| 欺诈 | 应用程序和威胁 | （包括表单劫持、网络钓鱼和诈骗）检测对已确定会被注入恶意 JavaScript 代码以收集用户敏感信息的受影响网站的访问（例如，从电子商务网站结账页面捕获的付款信息中的名称、地址、电子邮件、信用卡号、CVV、到期日期等）。 |
| 黑客工具 | 应用程序和威胁 | 检测被恶意操作者用于执行侦听、攻击或访问易受攻击系统、泄漏数据，或创建命令和控制渠道，以在未经授权的情况下暗中控制计算机系统的软件工具生成的流量。这些程序与恶意软件和网络攻击强烈关联。黑客工具可能会以善意方式部署用于红队和蓝组运作、渗透测试和研发。使用或拥有这些工具在某些国家或地区是违法的，这与工具用途无关。 |
| 密钥日志记录程序 | 应用程序和威胁 | 通过记录按键和捕获屏幕截图检测允许攻击者秘密跟踪用户活动的程序。 |


© 2019 Palo Alto Networks, Inc.

| 威胁类别 | 提供这些签名的内容更新 | 说明 |
| --- | --- | --- |
| | | 按键记录程序使用各种 C2 方法定期将日志和报告发送到预定义的电子邮件地址或 C2 服务器。通过按键记录程序监管，攻击者可以检索能够启用网络访问的凭据。 |
| networm | 应用程序和威胁 | 检测能实施系统间自我复制和传播的程序。网络蠕虫可能会使用共享资源或利用安全故障访问目标系统。 |
| 网络钓鱼工具包 | 应用程序和威胁 | 在用户尝试连接到网络钓鱼工具包登录页面时进行检测（可能是在接收到包含连接到恶意站点的链接的电子邮件后）。网络钓鱼网站诱使用户提交攻击者可以窃取的凭据，以便登录到网络。<br><br>除了阻止登录到网络钓鱼工具包登录页面，还可以启用多重因素身份验证和凭据网络钓鱼防护以阻止所有阶段发生的网络钓鱼攻击。 |
| 利用后 | 应用程序和威胁 | 检测指示攻击利用后阶段的活动，此时，攻击者尝试对受攻击系统的价值进行评估。这可能包括评估存储在系统上的数据敏感性，以及系统在进一步危害网络方面的有用性。 |
| webshell | 应用程序和威胁 | 检测 Web 外壳和 Web 外壳流量，包括植入检测以及命令和控制交互。Web 外壳必须首先由恶意操作者植入到受影响的主机中，通常针对的是 Web 服务器或框架。随后与 Web 外壳文件进行的通信经常使恶意操作者在系统中建立立足点，执行服务和网络枚举、泄漏数据，并在 Web 服务器用户上下文中实施远程代码执行。PHP、.NET 和 Perl 标记脚本是最常见的 Web 外壳类型。攻击者还会使用受到 Web 外壳影响的服务器（Web 服务器可以是面向互联网的系统，也可以是内部系统）攻击其他内部系统。 |
| 间谍软件 | 应用程序和威胁 | 检测出站 C2 通信。这些签名可以自动生成，或是通过 Palo Alto Networks 研究人员手动创建。<br><br>间谍软件和自动生成签名都可以检测出站 *C2* 通信；但是自动生成签名是基于有效负载的，可唯一用于检测与位置或变化迅速的 *C2* 主机之间的 *C2* 通信。 |
| 漏洞签名 | | |
| 暴力破解 | 应用程序和威胁 | 暴力破解签名检测特定时间范围内多次出现的情况。虽然孤立的活动可能是良性的，但暴力破解签名可以表明发生可疑活动时的频率和速率。例如，单个 FTP 登录失败不会显示恶意活动。但是，短时间内 FTP 多次登录失败可能表示攻击者正尝试通过密码组合来访问 FTP 服务器。<br><br>您可以针对暴力破解签名调整活动和触发条件。 |
| 代码执行 | 应用程序和威胁 | 检测代码执行漏洞（攻击者可利用此漏洞，使用已登录用户的权限在系统上运行代码）。 |
| 代码混淆 | 应用程序和威胁 | 检测已转换（以隐藏某些数据）但同时又保留了功能的代码。混淆的代码很难或者无法被读取，因此就不知道代码正在执行哪些 |


© 2019 Palo Alto Networks, Inc.

| 威胁类别 | 提供这些签名的内容更新 | 说明 |
| --- | --- | --- |
| | | 命令，或是代码想要与哪个程序进行交互。最常见的是，恶意操作者会混淆代码以隐藏恶意软件。更为罕见的是，合法的开发人员可能会混淆代码以保护隐私、知识产品或提高用户体验。例如，某些类别的混淆（例如缩小）会减少文件大小，从而减少网站加载时间和带宽使用。 |
| dos | 应用程序和威胁 | 检测拒绝服务 (DoS) 攻击，此时，攻击者尝试使目标系统不可用，暂时中断系统和相关的应用程序和服务。要执行 DoS 攻击，攻击者可能会使目标系统泛滥，或是发送导致其失败的信息。DoS 攻击会使合法用户（员工、成员和账户持有者等）失去其希望访问的服务或资源。 |
| 漏洞利用工具包 | 应用程序和威胁 | 检测漏洞利用工具包登录页面。漏洞利用工具包登录页面常常包含多个浏览器和插件中针对一个或多个常见漏洞和暴露 (CVE) 的多个漏洞利用。因为目标 CVE 更改速度快，因此，漏洞利用工具包签名可基于漏洞利用数据包登录页面（而非 CVE）触发。<br>当用户访问带漏洞利用工具包的网站时，漏洞利用工具包就会扫描目标 CVE，并尝试以静默的方式发送恶意有效负载到受害者的计算机。 |
| 信息泄露 | 应用程序和威胁 | 检测攻击者可以用于窃取敏感信息或专有信息的软件漏洞。通常，因为不存在全面的检查来保护数据，因此信息泄露可能存在，攻击者可以通过发送创建的请求来利用信息泄露。 |
| insecure-credentials | 应用程序和威胁 | 检测是否为软件、网络设备和 IoT 设备使用了弱密码、已泄漏的密码和制造商默认的密码。 |
| 溢出 | 应用程序和威胁 | 检测溢出漏洞（攻击者可以利用未对请求进行适当检查的情况）。成功的攻击可能会导致使用应用程序、服务器或操作系统权限执行远程代码。 |
| 网络仿冒 | 应用程序和威胁 | 在用户尝试连接到网络钓鱼工具包登录页面时进行检测（可能是在接收到包含连接到恶意站点的链接的电子邮件后）。网络钓鱼网站诱使用户提交攻击者可以窃取的凭据，以便登录到网络。<br>除了阻止登录到网络钓鱼工具包登录页面，还可以启用多重因素身份验证和凭据网络钓鱼防护以阻止所有阶段发生的网络钓鱼攻击。 |
| 协议异常 | 应用程序和威胁 | 检测协议行为偏离标准和合规使用时的协议异常。例如，格式错误的数据包、写入不当的应用程序、或在非标准端口上运行的应用程序等，都将被视为协议异常，并可用作规避工具。最佳实践是阻止任何严重性的协议异常。 |
| Sql 注入 | 应用程序和威胁 | 检测一种常见的黑客技术，此时，攻击者将 SQL 查询插入到应用程序的请求中，以便从数据库读取或是修改数据库。这种类型的技术通常用于未全面清理用户输入的网站。 |


© 2019 Palo Alto Networks, Inc.

# 创建威胁异常

Palo Alto Networks 对威胁签名的建议默认操作（如阻止或警报）进行定义。您可以使用威胁 ID 来排除执行威胁签名或修改防火墙对该威胁签名执行的操作。例如，您可以修改在网络上触发误报的威胁签名的操作。

配置防病毒、漏洞、间谍软件和 DNS 签名等的威胁异常，以更改防火墙对威胁的执行。但是，在开始之前，请确保防火墙根据默认签名设置检测并处理威胁：

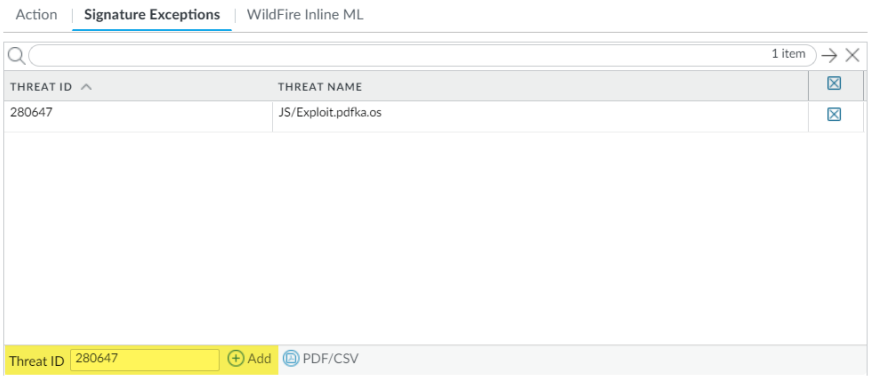
- 获取最新的防病毒、威胁和应用程序，以及 WildFire 签名更新。
- 设置防病毒、防间谍软件和漏洞保护，并将这些安全配置文件应用于您的安全策略。

STEP 1 | 从执行中排除防病毒签名。



虽然您可以使用防病毒配置文件将防病毒签名从执行中排除，但无法更改防火墙对特定防病毒签名执行的操作。但是，您可以通过编辑解码器（*Objects*（对象）> *Security Profiles*（安全配置文件）> *Antivirus*（防病毒）> *<antivirus-profile>* > *Antivirus*）来定义防火墙的操作，以处理不同类型流量中的病毒。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）。
2. **Add**（添加）或修改要从中排除威胁签名的现有防病毒配置文件，然后选择 **Signature Exception**（签名例外）。
3. **Add**（添加）要从执行中排除的威胁签名的 **Threat Id**（威胁 **ID**）。

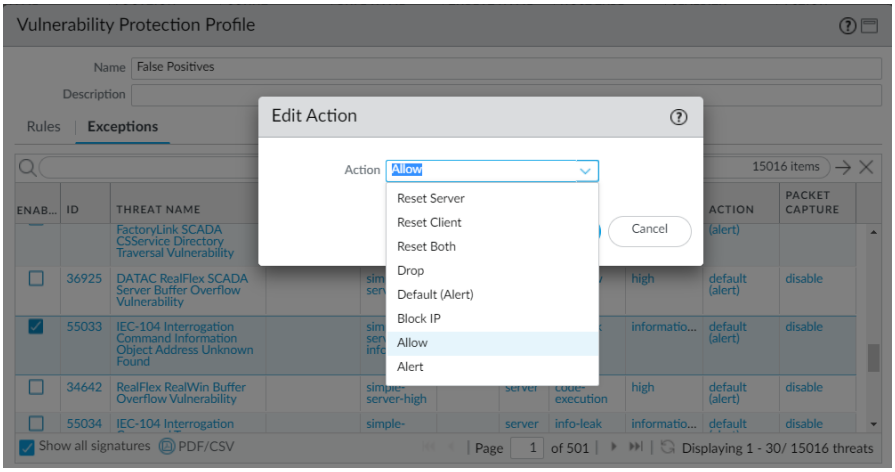



4. 单击 **OK**（确定）以保存防病毒配置文件。

STEP 2 | 修改对漏洞和间谍软件签名的执行（DNS 签名除外；跳到下一个选项以修改 DNS 签名的执行，这是一种间谍软件签名）。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）或 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Vulnerability Protection**（漏洞保护）。
2. **Add**（添加）或修改要排除威胁签名的现有防间谍软件或漏洞防护配置文件，然后选择 **Signature Exceptions**（签名例外）（对于防间谍保护配置文件）或 **Exceptions**（例外）（对于漏洞防护配置文件）。
3. **Show all signatures**（显示所有签名），然后筛选以选择要修改其执行规则的签名。
4. 对于您想要修改其实施的签名，勾选 **Enable**（启用）列下的复选框。
5. 选择让防火墙处理该威胁签名的 **Action**（操作）。


© 2019 Palo Alto Networks, Inc.



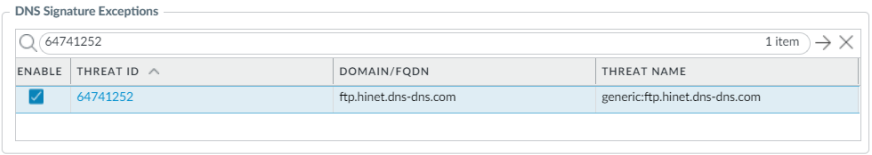

对于要从执行中排除的签名，因为这些签名会触发误报，请将 **Action**（操作）设置为 **Allow**（允许）。

6. 单击 **OK**（确定）以保存新的或修改过的反间谍软件或漏洞保护配置文件。

STEP 3 | 修改 DNS 签名的执行。

默认情况下，对侦测到 DNS 签名的恶意主机名的 DNS 查找将被 sinkhole。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）。
2. **Add**（添加）或修改要从中排除威胁签名的防间谍软件配置文件，然后选择 **DNS Exceptions**（DNS 例外）。
3. 搜索要从执行中排除的 DNS 签名的 DNS 威胁 ID，然后选择相应签名的方框：




4. 单击 **OK**（确定）以保存新的或修改过的反间谍软件配置文件。



© 2019 Palo Alto Networks, Inc.

# 自定义签名

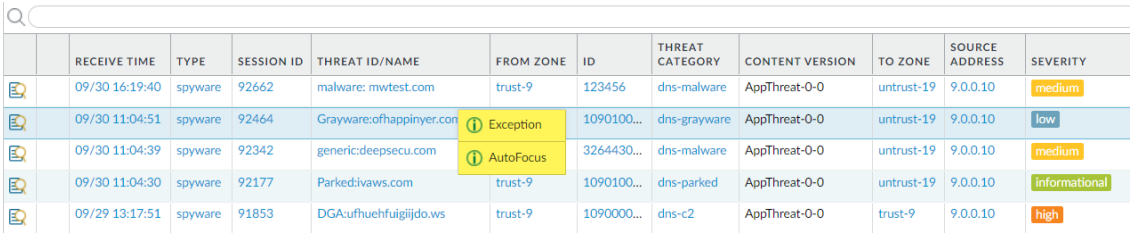
您可以创建自定义威胁签名来检测和阻止特定流量。当防火墙由 Panorama 管理服务器管理时，ThreatID 将映射到防火墙上相应的自定义威胁，使防火墙生成已填充有自定义 ThreatID 的威胁日志。更多信息，请访问我们的自定义设备和威胁签名指南。



© 2019 Palo Alto Networks, Inc.

# 监控并获取威胁报告

威胁库和 AutoFocus 等功能集成到防火墙后，可以查看防火墙检测到的威胁的性质，并提供一张关于构件如何适用于您组织的网络流量的完整图像（构件是属性、活动，或与文件、电子邮件链接或会话相关联的行为）。您可以立即获得关于威胁的上下文信息，或将威胁调查从防火墙无缝转移到威胁库和 AutoFocus。



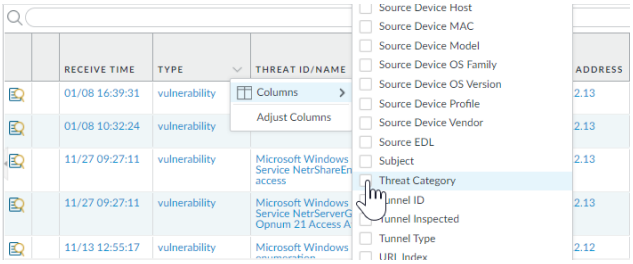

此外，您可以使用威胁签名类别（用于将威胁事件类型分类）将您的视图缩小到某种类型的威胁活动或构建自定义报告。

- 监控活动并根据威胁类别创建自定义报告
- 进一步了解威胁签名
- AutoFocus 网络流量威胁情报

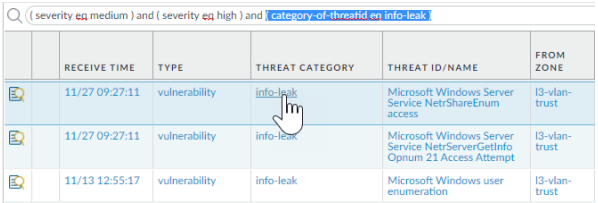
## 监控活动并根据威胁类别创建自定义报告

威胁类别将不同类型的威胁签名进行分类，以帮助您了解和划出事件威胁签名检测之间的连接。威胁类别是更广泛的威胁签名类型的子集：间谍软件、漏洞、防病毒和 DNS 签名。威胁日志条目显示每个已记录事件的 **Threat Category**（威胁类别）。

- 按威胁类别筛选威胁日志。
  1. 选择 **Monitor**（监视器）> **Logs**（日志）> **Threat**（威胁）。
  2. 添加威胁类别列，以查看每个日志条目的威胁类别：




  3. 要根据威胁类别筛选：
     - 使用日志查询构建器添加具有 **Attribute**（属性）威胁类别的筛选器，并在 **Value**（值）字段中输入威胁类别。
     - 选择任何日志条目的威胁类别，并将该类别添加到筛选器：

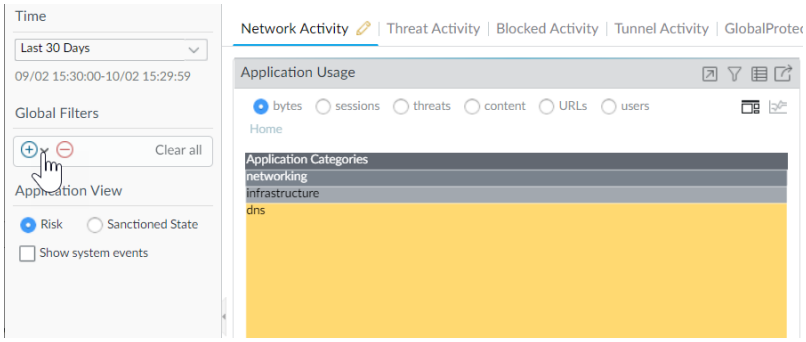



- 按威胁类别筛选 ACC 活动。

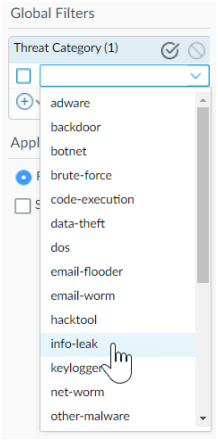


© 2019 Palo Alto Networks, Inc.

1. 选择 **ACC** 并添加威胁类别作为全局筛选器：




2. 选择威胁类别以筛选所有 ACC 选项卡。




- 根据威胁类别创建自定义报告，以接收防火墙检测到的特定威胁类型相关的信息。
  1. 选择 **Monitor**（监控）> **Manage Custom**（管理自定义）报告以添加新的自定义报告或修改现有报告。
  2. 选择 **Database**（数据库）作为自定义报告的来源； 在这种情况下，从两种类型的数据库源（摘要数据库和详细日志）中选择 **Threat**（威胁）。精简摘要数据库数据，以便在生成报告时获取更快的响应时间。详细日志需要更长的生成时间，但为每个日志条目提供一个逐项和完整的数据集。
  3. 在查询构建器中，添加带有属性 **Threat Category**（威胁类别）的报告筛选器，然后在“值”字段中，根据您的报告选择一个威胁类别。
  4. 要测试新报告设置，请选择 **Run Now**（立即运行）。
  5. 单击 **OK**（确定）以保存报告。

# 进一步了解威胁签名

防火墙威胁日志记录防火墙根据威胁签名检测到的所有威胁（设置防病毒、防间谍软件和漏洞保护），而 ACC 显示网络上最高威胁的概述。防火墙记录的每个事件都包括标识相关威胁签名的 ID。

您可以使用威胁日志或 ACC 条目找到威胁 ID，以便：

- 轻松检查是否已将威胁签名配置为安全策略的异常（创建威胁异常）。
- 查找有关特定威胁的最新威胁库信息。因为威胁库与防火墙集成，可让您在防火墙的上下文中直接查看有关威胁签名的详细信息，或者在新的浏览器窗口中为防火墙记录的威胁启动威胁库搜索。



如果签名已禁用，则签名 *UTID* 可能会重新用于新签名。


© 2019 Palo Alto Networks, Inc.

查看内容更新发行说明，了解新签名和禁用签名相关的通知。签名在以下情况下可能被禁用：签名检测到的活动由于攻击者的攻击而停用，签名产生了重大的误报，或是签名与其他类似签名合并为单个签名（签名优化）。

STEP 1 | 确认防火墙已连接到威胁库。

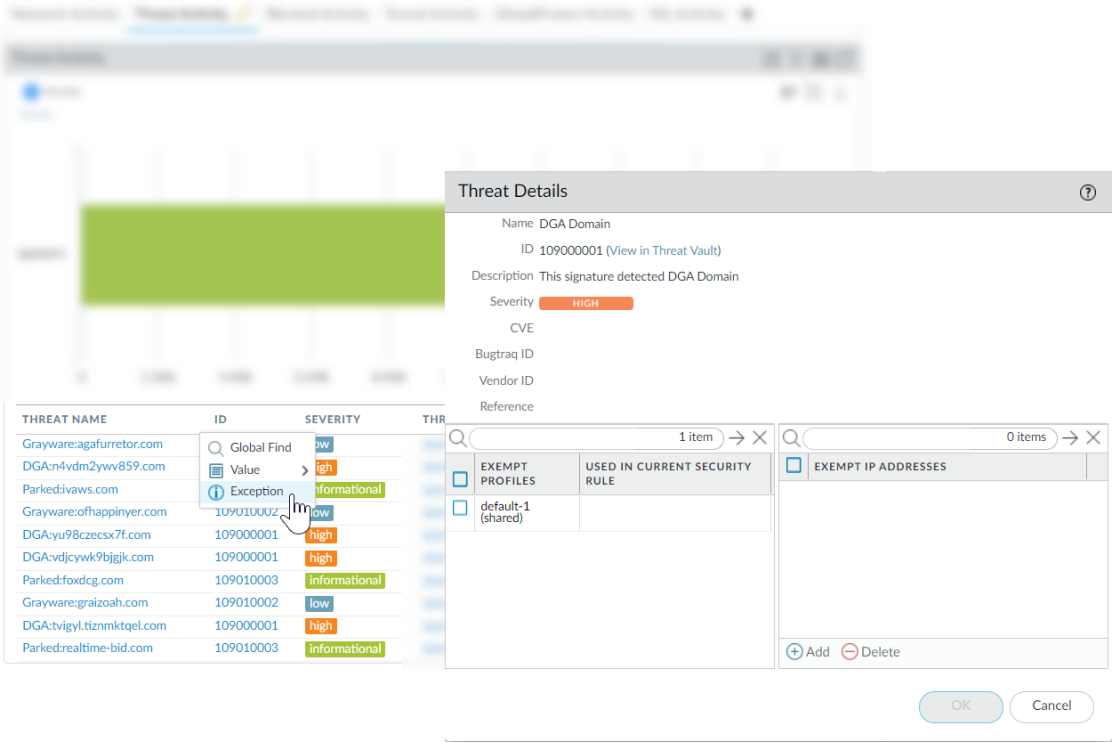
选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）并编辑 **Logging and Reporting**（日志记录和报告）设置为 **Enable Threat Vault Access**（启用威胁库访问）。默认情况下启用威胁库访问。

STEP 2 | 查找防火墙检测到的威胁的威胁 ID。

- 要查看防火墙根据威胁签名检测到的每个威胁事件，请选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁）。可以在 ID 列中找到威胁条目的 ID，或选择日志条目以查看日志详细信息，包括威胁 ID。
- 要查看网络上最高威胁的概述，请选择 **ACC** > **Threat Activity**（威胁活动），并查看“威胁活动”小部件。ID 列显示每个已显示威胁的威胁 ID。
- 要查看可将其配置为威胁异常的威胁的详细信息（即，防火墙执行的威胁与为威胁签名定义的默认操作不同），请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware/Vulnerability Protection**（防间谍软件/漏洞保护）。**Add**（添加）或修改配置文件，然后单击 **Exceptions**（异常）选项卡来查看已配置的异常。如果没有配置异常，可筛选威胁签名，或选择 **Show all signatures**（显示所有签名）。

STEP 3 | 悬停在 **Threat Name**（威胁名称）或威胁 **ID** 上打开下拉列表，然后单击 **Exception**（异常）查看威胁详细信息以及如何配置防火墙以执行威胁。

例如，进一步了解有关 ACC 的最高威胁：




STEP 4 | 查看威胁的最新 **Threat Details**（威胁详细信息），并根据威胁 ID 启动威胁库搜索。

- 显示的威胁详细信息包括威胁的最新威胁库信息、可用于进一步了解威胁的资源以及与威胁相关联的 CVE。



© 2019 Palo Alto Networks, Inc.

- 选择 **View in Threat Vault**（在威胁库中查看）以在新窗口中打开威胁库搜索，并查找 Palo Alto Networks 威胁数据库具有的针对该威胁签名的最新信息。

STEP 5 | 检查是否已将威胁签名配置为安全策略的异常。

- 如果 **Used in current security rule**（在当前安全规则中使用）列已清除，防火墙将根据建议的默认签名操作（例如，阻止或警报）实施该威胁。
- 在 **Used in current security rule**（在当前安全规则中使用）列中任何位置使用的复选标记均表示安全策略规则已配置为基于相关联的 **Exempt Profiles**（免除配置文件）设置对威胁执行非默认操作（例如，允许）。



仅当安全策略规则已配置威胁异常时 *Used in security rule column*（在当前安全规则中使用）才不会指示安全策略规则是否已启用。选择 *Policies*（策略）> *Security*（安全），以检查是否启用指定的安全策略规则。

STEP 6 | **Add**（添加）IP 地址，在其上筛选威胁异常或查看现有 **Exempt IP Addresses**（免除 **IP** 地址）。

仅有当关联的会话具有匹配的源 IP 地址或目标 IP 地址时，才配置免除 IP 地址来执行威胁异常；对于所有其他会话，将基于默认签名操作来执行威胁。

# AutoFocus 网络流量威胁情报

通过有效的 AutoFocus 订阅，您可以使用 AutoFocus 门户上最新的威胁数据对比网络活动。连接防火墙及 AutoFocus，解锁以下功能：

- 查看 AutoFocus 情报摘要，了解记录于防火墙日志的会话构件。
- 打开 AutoFocus 搜索，查找防火墙的日志构件。

AutoFocus 情报概览可显示构件在您的网络及全局网络中的普遍性。WildFire 判定及构件的 AutoFocus 标签列表可指明构件是否存在安全风险。

- AutoFocus 情报摘要
- 启用 AutoFocus 威胁情报
- 查看并处理 AutoFocus 情报摘要数据



您也可以根据 *AutoFocus* 的结果实施策略：

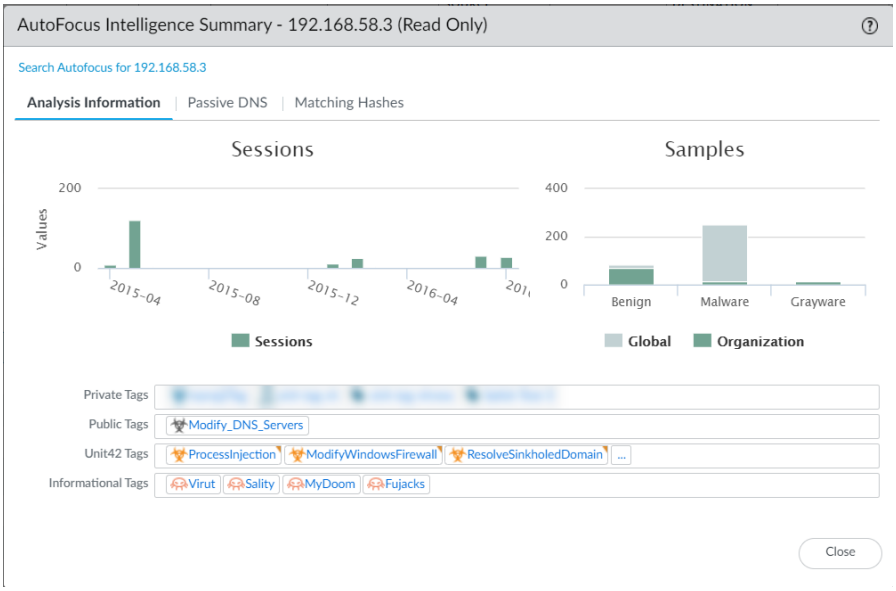
- 导出 AutoFocus 构件（IP 地址、URL 和域）并将其用于外部动态列表。
- 使用 AutoFocus 挖掘程序作为外部动态列表源。

## *AutoFocus* 情报摘要

AutoFocus 情报摘要提供与构件信息相关的集中视图，该构件是 AutoFocus 从其他 AutoFocus 用户、WildFire、PAN-DB URL 筛选数据库、Unit 42 和开源情报收集的威胁情报中提取所得。



© 2019 Palo Alto Networks, Inc.




| AutoFocus 情报摘要 | |
|---|---|
| 分析信息 | “分析信息”选项卡显示以下信息：<br>• 会话 — 防火墙中记录的会话数，防火墙检测到与该构件相关联的样本。<br>• 样本 — 与构件相关的组织和全球样本比较，并按 WildFire 判定（良性软件、恶意软件或灰色软件）分组。全局是指所有 WildFire 提交的样本，而组织仅指贵组织提交到 WildFire 的样本。<br>• 匹配标记 — 与构件相匹配的 AutoFocus 标记。AutoFocus 标记指示构件是否链接到恶意软件或针对性攻击。 |
| 被动 DNS | “被动 DNS”选项卡显示包含该构件的被动 DNS 历史记录。此被动 DNS 历史记录基于 AutoFocus 的全局 DNS 情报，但不限于您网络中的 DNS 活动。被动 DNS 历史记录包括：<br>• 域请求<br>• DNS 请求类型<br>• DNS 请求解析的 IP 地址或域（不显示私有 IP 地址）<br>• 执行请求的次数<br>• 第一次和最后一次看到请求的日期和时间 |
| 匹配哈希 | “匹配哈希”选项卡显示最近检测到的 5 个匹配样本。收集的样本包括：<br>• 样本的 SHA256 哈希<br>• 样本文件类型<br>• WildFire 分析样本并为其分配 WildFire 判定的日期和时间<br>• WildFire 对样本的判定结果<br>• WildFire 更新样本的 WildFire 判定的日期和时间（如适用） |

## 启用 *AutoFocus* 威胁情报

激活 AutoFocus 许可证，并启用防火墙以与 AutoFocus 通信。设置完成后，您将可以查看日志或 ACC 构件的 AutoFocus 情报摘要，以在您的网络和任何相关威胁中评估其普遍性。



© 2019 Palo Alto Networks, Inc.

STEP 1 | 验证 AutoFocus 许可证是否已在在防火墙上激活。

1. 选择 **Device**（设备）> **Licenses**（许可证）以确认 AutoFocus 设备许可证已安装及其有效性（检查失效日期）。
2. 如果防火墙未显示许可证，激活订阅许可证。

STEP 2 | 连接防火墙与 AutoFocus。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）并编辑 AutoFocus 设置。
2. 输入 **AutoFocus URL**：

   `https://autofocus.paloaltonetworks.com:10443`
3. 使用 **Query Timeout**（查询超时）字段设置防火墙查阅 AutoFocus 以获取威胁情报数据的持续时间。如果 AutoFocus 门户在指定期限结束前未作出响应，防火墙将关闭连接。

   最佳实践是将“查询超时”设置为默认值：*15* 秒。最好在该期间完成 *AutoFocus* 查阅。
4. 选择 **Enabled**（启用）以允许防火墙与 AutoFocus 的连接。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改以在重启时保留 AutoFocus 设置。

STEP 3 | 连接 AutoFocus 至防火墙。

1. 登录至 AutoFocus 门户：https://autofocus.paloaltonetworks.com
2. 选择 **Settings**（设置）。
3. **Add new**（添加新）远程系统。
4. 输入描述性 **Name**（名称）以标识防火墙。
5. 选择 **PanOS** 作为“系统类型”。
6. 输入防火墙 IP **Address**（地址）。
7. 单击 **Save changes**（保存修改）以添加远程系统。
8. 再次单击设置页面的 **Save changes**（保存更改），确认防火墙已成功添加。

STEP 4 | 检测防火墙与 AutoFocus 之间的连接。

1. 在防火墙上，选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）。
2. 验证您是否可以 通过 AutoFocus 评估防火墙构件。

## 查看并处理 *AutoFocus* 情报摘要数据

与 AutoFocus 情报摘要交互以显示构件相关的更多信息，或者将构件研究扩展到 AutoFocus。AutoFocus 标记可以显示构件是否与特定类型的恶意软件或恶意行为相关联。

STEP 1 | 确认防火墙已经连接上 AutoFocus。

在防火墙上启用 AutoFocus 威胁情报（需要有效的 AutoFocus 订阅）。

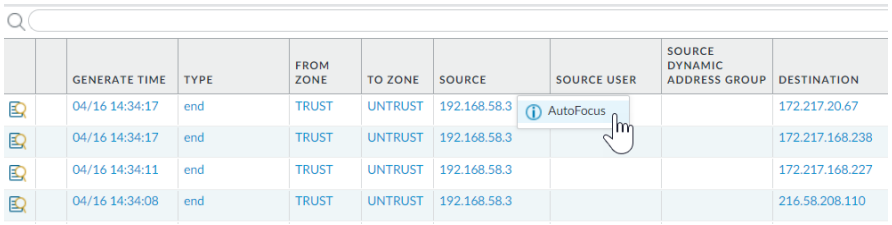
STEP 2 | 找到要调查的构件。

在以下情况下，可以查看构件的 AutoFocus 情报摘要：

- 查看日志（仅限流量、威胁、URL 筛选、WildFire 提交、数据筛选和统一日志）。
- 查看外部动态列表条目。

STEP 3 | 将鼠标悬停在构件上方以打开下拉列表，然后单击 **AutoFocus**。


© 2019 Palo Alto Networks, Inc.




AutoFocus 情报摘要仅适用于以下类型的构件：

IP 地址

网址

域

用户代理

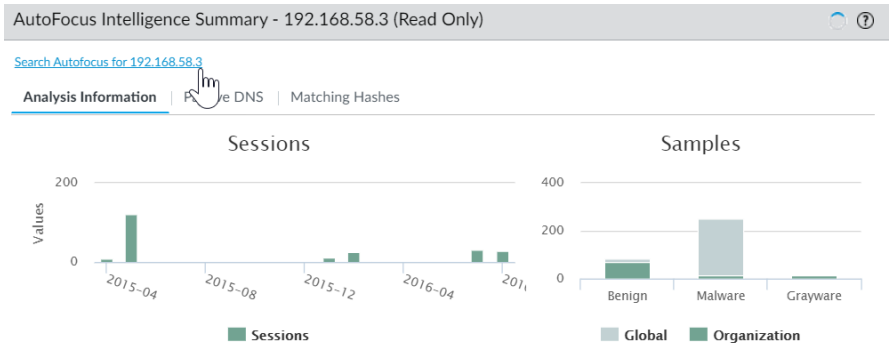
威胁名称（仅对于子类型病毒和 WildFire 病毒的威胁）

文件名

SHA-256 哈希

STEP 4 | 启动 AutoFocus 以搜索用于打开 AutoFocus 情报摘要的构件。

单击 AutoFocus 情报摘要窗口顶部的 **Search AutoFocus for...**（搜索 **AutoFocus** 以...）链接。搜索结果包括与构件相关的所有样本。在 **My Samples**（我的样本）和 **All Samples**（所有样本）选项卡之间进行切换，并比较样本数量以确定组织中构件的普遍性。




STEP 5 | 启动 AutoFocus 以搜索 AutoFocus 情报摘要中的其他构件。

单击以下构件以确定其在您组织中的普遍性：

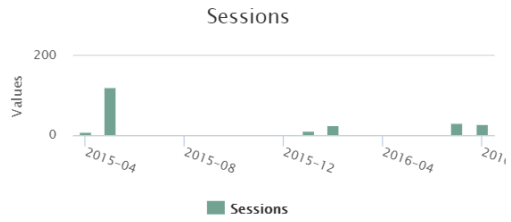
- 分析信息选项卡中的 WildFire 判定
- 被动 DNS 选项卡中的 URL 和 IP 地址
- 匹配哈希选项卡中的 SHA256 哈希值

STEP 6 | 查看每个月组织中与构件关联的会话数。

将鼠标悬停在会话栏上。

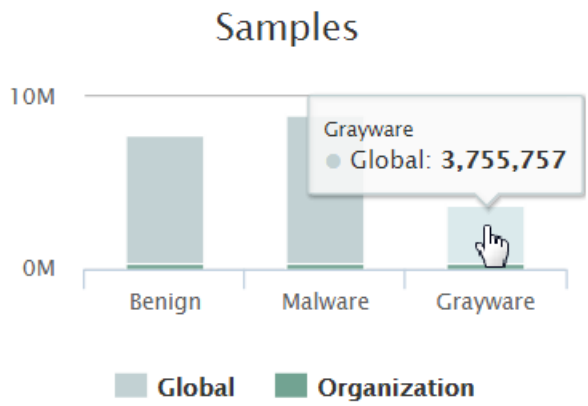


© 2019 Palo Alto Networks, Inc.



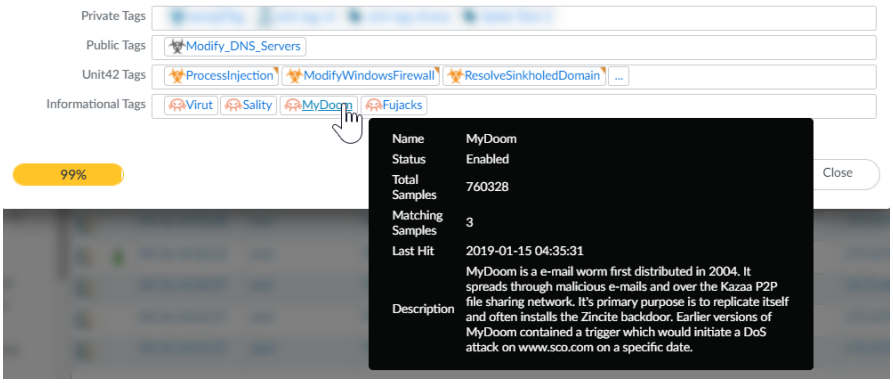

STEP 7 | 通过范围和 WildFire 判定来查看与构件关联的样本数。

将鼠标悬停在样本栏上。




STEP 8 | 查看有关匹配 AutoFocus 标记的更多详细信息。

将鼠标悬停在匹配标记上方以查看标记说明和其他标记详细信息。




STEP 9 | 查看与匹配标签关联的其他样本。

单击匹配标记以启动 AutoFocus 搜索该标记。搜索结果包括与标记匹配的所有样本。

Unit 42 标记用于标识构成直接安全风险的威胁和活动。单击 Unit 42 匹配标记，查看网络中有多少个样本与标记标识的威胁相关联。

STEP 10 | 查看构件的更多匹配标记。

单击省略号（...）以启动 AutoFocus 搜索构件。搜索结果中的标记列显示构件的更多匹配标记，可让您了解其他恶意软件、恶意行为、威胁因素、漏洞或通常检测到构件的活动。



© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

# 与 Palo Alto Networks 共享威胁情报

遥测是收集和传输数据进行分析的过程。在防火墙上启用遥测后，防火墙会定期收集并将信息（包括有关应用程序、威胁、设备运行状况等）发送至 Palo Alto Networks。共享威胁情报可提供以下好处：

- 增强向您和全球其他客户提供漏洞和间谍软件签名。例如，当威胁事件触发漏洞或间谍软件签名时，防火墙会与 Palo Alto Networks 威胁研究团队共享与威胁相关联的 URL，以便将该 URL 正确分类为恶意软件。
- 快速测试和评估对您网络没有影响的实验威胁签名，从而更快地将关键威胁阻止签名发布到所有 Palo Alto Networks 客户。
- 提高 PAN-DB URL 筛选、基于 DNS 的命令和控制 (C2) 签名以及 WildFire 的准确性和恶意软件检测能力。

Palo Alto Networks 使用从遥测中提取的威胁情报为您和其他 Palo Alto Networks 用户提供这些优势。所有 Palo Alto Networks 用户都能从每位用户共享的遥测数据中获益，从而使得遥测成为一种社区推动的预防威胁的方法。Palo Alto Networks 不会与其他客户或第三方组织共享您的遥测数据。

若要了解更多有关遥测的信息，包括它的优势、使用情况和配置，请参阅设备遥测。



© 2019 Palo Alto Networks, Inc.

# 威胁阻止资源

有关威胁阻止最佳实践的详细信息，请参阅以下资源：

- 创建自定义威胁签名
- 防止网络免遭第 4 层和第 7 层逃避的最佳实践
- URL 筛选最佳实践
- 零信任最佳实践
- DoS 和区域保护最佳实践

要查看 Palo Alto Networks 产品可以识别的威胁和应用程序的列表，请使用以下链接：

- Applipedia — 提供有关 Palo Alto Networks 可识别的应用程序的详细信息。
- Threat Vault — 列出 Palo Alto Networks 产品可识别的威胁。您可以按漏洞、间谍软件或病毒进行搜索。单击 ID 号旁边的详细信息图标可获取有关威胁的详细信息。

# 解密

Palo Alto Networks 防火墙可以解密和检查流量，以便查看威胁，从而对协议、证书验证和故障处理进行控制。解密可对解密流量执行策略，这样，防火墙可以根据您配置的安全设置处理加密流量。解密流量，防止恶意加密内容进入您的网络，敏感内容以加密流量的方式隐藏，从而离开您的网络。启用解密可包括准备解密所需的密钥和证书，创建解密策略和策略，并配置解密端口镜像。


> 解密概述
> 解密概念
> 准备部署解密
> 确定解密流量
> 配置 SSL 转发代理
> 配置 SSL 入站检查
> 配置 SSH 代理
> 为未加密流量配置服务器证书验证
> 解密排除
> 阻止私钥导出
> 让用户选择停用 SSL 解密
> 暂时禁用 SSL 解密
> 配置解密端口镜像
> 验证解密
> 排除故障并监视解密
> 解密代理
> 激活免费许可证以使用解密功能

# 解密概述

安全套接字套 (SSL) 和安全外壳 (SSH) 加密协议是用来保护 Web 服务器和客户端两个实体之间的流量。SSL 和 SSH 封装流量和加密数据，这样使得除客户端和服务器以外的实体使用证书确认设备之间的信任和解密数据的密钥变得毫无意义。解密 SSL 和 SSH 流量以：

- 防止隐藏为加密流量的恶意软件进入您的网络。例如，攻击者破坏使用 SSL 加密的站点。员工访问此站点，并在不知情的情况下下载漏洞或恶意软件。然后，恶意软件使用受感染的员工端点在网络中横向移动，并危害其他系统。
- 防止网络泄露敏感信息。
- 确保在安全网络上运行适当的应用程序。
- 选择性地解密流量；例如，创建解密策略和配置文件，以便从解密中排除金融或健康站点的流量。

Palo Alto Networks 防火墙解密基于策略，并且可用来解密、检查以及控制入站和出站 SSL 和 SSH 连接。您可以使用解密策略按目标、源或 URL 类别指定解密的流量，并根据关联解密配置文件中的安全设置阻止、限制或转发指定流量。解密配置文件控制 SSL 协议、证书验证和故障检查，阻止使用弱算法或不受支持模式的流量访问网络。防火墙使用证书和密钥将流量解密成明文，然后对明文流量强制执行 App-ID 和安全设置，包括解密、防病毒、漏洞、防间谍软件、URL 过滤、Wildfire 和文件传送阻止配置文件。解密并检查流量后，在退出防火墙时，防火墙会对明文流量进行重新加密以确保隐私和安全。

防火墙提供三种类型的解密策略规则：用户控制出站 SSL 流量的 SSL 转发代理、用于控制入站 SSL 流量的 SSL 入站检查、以及用于控制隧道 SSH 流量的 SSH 代理。可以将解密配置文件附加到策略规则，以便将细粒度访问设置应用于流量，例如，检查服务器证书、不受支持模式和故障。

SSL 解密（转发协议和入站检查）需要证书将防火墙建立为可信任第三方，并在客户端和服务器之间建立信任，确保 SSL/TLS 连接的安全。此外，还可以在因为技术原因从 SSL 解密中排除服务器时使用证书（站点出于证书固定、不受支持密码或相互身份验等原因破解解密）。SSH 解密不需要证书。



使用解密最佳做法清单来计划、执行和维护您的解密部署。

您可以集成硬件安全模块 (HSM) 和防火墙，在 SSL 转发代理和 SSL 入站检查解密中启用私钥的增强的安全性。要了解有关使用 HSM 存储和生成密钥以及将 HSM 集成防火墙的更多信息，请参阅安全密钥与硬件安全模块。

还可以使用解密镜像将解密流量作为明文转发给第三方解决方案，以进行其他分析和存档。



如果启用解密镜像，请了解与可以解密的流量以及可以存储流量的地点和方式相关的本地法律和法规，因为包括敏感信息在内的所有镜像流量都以明文形式转发。



© 2019 Palo Alto Networks, Inc.

# 解密概念

更多有关解密功能和支持的信息，请查看以下主题：

- 适用于解密策略的密钥和证书
- SSL 转发代理
- SSL 转发代理解密配置文件
- SSL 入站检查
- SSL 入站检查解密配置文件
- SSL 协议设置解密配置文件
- SSH 代理
- SSH 代理解密配置文件
- SSL 不解密配置文件
- 用于椭圆曲线加密法 (ECC) 证书的 SSL 解密
- 用于 SSL 解密的完全正向保密 (PFS)
- SSL 解密和主题备用名称(SAN)
- TLSv1.3 解密
- 解密会话的高可用性支持
- 正在解密镜像
- 解密代理

## 适用于解密策略的密钥和证书

密钥是数字组成的字符串，通常使用涉及随机数和大素数的数学运算生成。密钥将密码和共享密钥等字符串从未加密明文转换为加密密文，并从加密密文转换为未加密明文。并且，密码可能是对称（同一密钥用于加密和解密）或不对称（一个密钥用于加密和数学上相关的密钥用于解密）。任何系统都可以生成密钥。

X.509 证书用于在客户端和服务器之间建立信任，从而建立 SSL 连接。客户端尝试验证服务器（或服务器验证客户端）了解 X.509 证书的结构，以此了解如何从证书内的字段中提取有关服务器的标识信息，如 FQDN 或 IP 地址（在证书内称为公用名或 *CN*），或向其签发证书的企业、部门或用户的名称。证书颁发机构 (CA) 必须颁发所有证书。在 CA 验证客户端或服务器后，CA 签发证书并使用私钥进行签名。



如果您拥有两个具有相同主题和密钥的 *CA*（*Device*（设备）> *Certificate Management*（证书管理）> *Device Certificates*（设备证书））且其中一个 *CA* 已过期，请删除（自定义）或禁用（预定义）过期 *CA*。如果未删除或禁用过期 *CA*，则防火墙可在过期 *CA* 在受信任链中启用而产生阻止页面时建立一个过期 *CA* 链。

将解密策略应用于流量后，只有防火墙信任签发服务器证书的 CA 时才能在客户端和服务器之间进行会话。为了建立信任，防火墙必须在其证书信任列表 (CTL) 中拥有服务器的根 CA 证书，并使用该根 CA 证书中包含的公钥来验证签名。然后，防火墙提交由客户端的转发信任证书签名的服务器证书的副本进行验证。您也可以配置防火墙使用企业 CA 作为 SSL 转发代理的转发信任证书。如果防火墙在其 CTL 中没有服务器的根 CA 证书，则会将由转发不可信证书签名的服务器证书的副本提交给客户端。转发不可信证书可确保当尝试使用不受信任的证书访问服务器托管的站点时，系统为客户端提供证书警告。

有关证书的详细信息，请参阅证书管理。



要控制防火墙信任的受信任 *CA*，请使用防火墙 *Web* 接口上的 *Device*（设备）> *Certificate Management*（证书管理）> *Certificates*（证书）> *Default Trusted Certificate Authorities*（默认受信任的证书颁发机构）。

下表介绍了 Palo Alto Networks 防火墙进行解密时使用的不同证书。



© 2019 Palo Alto Networks, Inc.

| 与解密一起使用的证书 | 说明 |
| --- | --- |
| 转发信任（用于 SSL 转发代理解密） | 如果客户端尝试连接到拥有由防火墙信任的 CA 签名的证书的站点，则防火墙在解密过程中将证书提交给客户端。在服务器证书由受信 CA 签署后，要为防火墙配置提供给客户端的转发信任证书，请参阅配置 SSL 转发代理。<br>默认情况下，防火墙根据目标服务器的密钥大小，确定用于客户端证书的密钥大小。但是，可以为 SSL 代理服务器证书配置密钥大小。为了增加安全性，请考虑请将与转发信任证书相关联的私钥存储在硬件安全模块上（请参阅在 HSM 上存储私钥）。<br>在安全存储库中备份与防火墙转发信任 *CA* 证书相关联的私钥（而非防火墙主密钥），这样，如果防火墙出现故障，您仍可以访问转发信任 *CA* 证书。为了增加安全性，请考虑请将与转发信任证书相关联的私钥存储在硬件安全模块上（请参阅在 HSM 上存储私钥）。 |
| 转发不可信（用于 SSL 转发代理解密） | 如果客户端尝试连接到拥有由防火墙不信任的 CA 签名的证书的站点，则防火墙在解密过程中将证书提交给客户端。要在防火墙上配置转发不受信任证书，请参阅配置 SSL 转发代理。 |
| SSL 入站检查 | 网络上想用于执行发往这些服务器的流量的 SSL 入站检查的服务器证书。将服务器证书导入防火墙。<br>从 *PAN-OS 8.0* 开始，防火墙将使用椭圆曲线 *Diffie-Hellman Exchange (ECDHE)* 算法执行严格的证书检查。这意味着，如果防火墙使用中间证书，您必须在更新到 *PAN-OS 8.0* 或更高版本之后将证书从 *Web* 服务器重新导入到防火墙，并将服务器证书与中间证书相结合（安装链式证书）。否则，链中拥有中间证书的 *SSL* 入站检查会话将失败。要安装链式证书：<br>1. 在文本编辑器（如记事本）中打开每个证书 *(.cer)* 文件。<br>2. 端到端地粘贴每个证书，服务器证书在上，下面包含每个签名者。<br>3. 将文件另存为文本 *(.txt)* 或证书 *(.cer)* 文件（文件名不能包含空格）。<br>4. 将组合（链式）证书导入到防火墙。 |

# SSL 转发代理

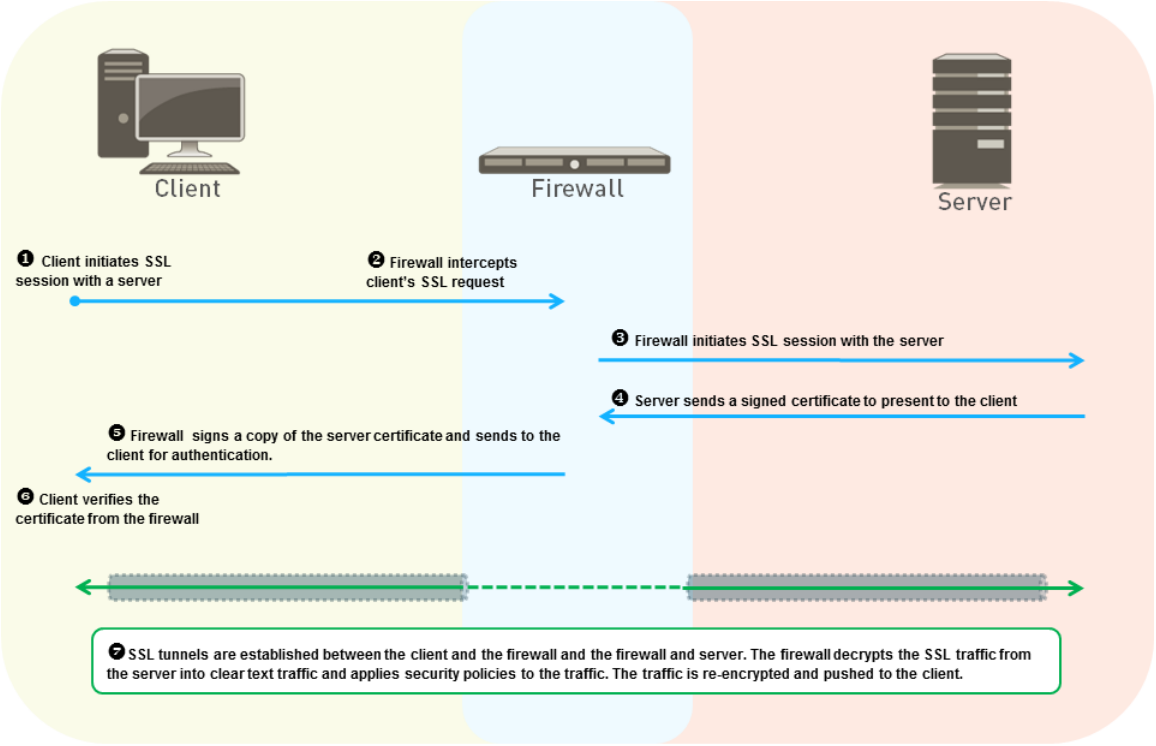
配置防火墙以解密前往外部站点的 SSL 流量时，防火墙将充当 SSL 转发代理。使用 SSL 转发代理解密策略进行解密，并检查从内部用户到 Web 的 SSL/TLS 流量。SSL 转发代理解密通过解密流量的方式阻止隐藏为 SSL 加密流量的恶意软件进入您的企业网络，这样，防火墙可以将解密配置文件以及安全策略和配置文件应用于流量。

在 SSL 转发代理解密中，防火墙是内部客户端和外部服务器之间的中间人。防火墙使用证书向服务器透明地显示客户端，并向客户端透明地显示服务器，这样，客户端会认为它正在与服务器直接通信（即使客户端会话与防火墙一起），服务器也认为它正在与客户端直接通信（即使服务器会话与防火墙一起）。防火墙使用证书使自身成为客户端与服务器之间会话的受信任第三方（中间人）（有关证书的详细信息，请参阅适用于解密策略的密钥和证书）。

下图显示此过程的详细信息。有关配置 SSL 转发代理的详细信息，请参阅配置 SSL 转发代理。



© 2019 Palo Alto Networks, Inc.

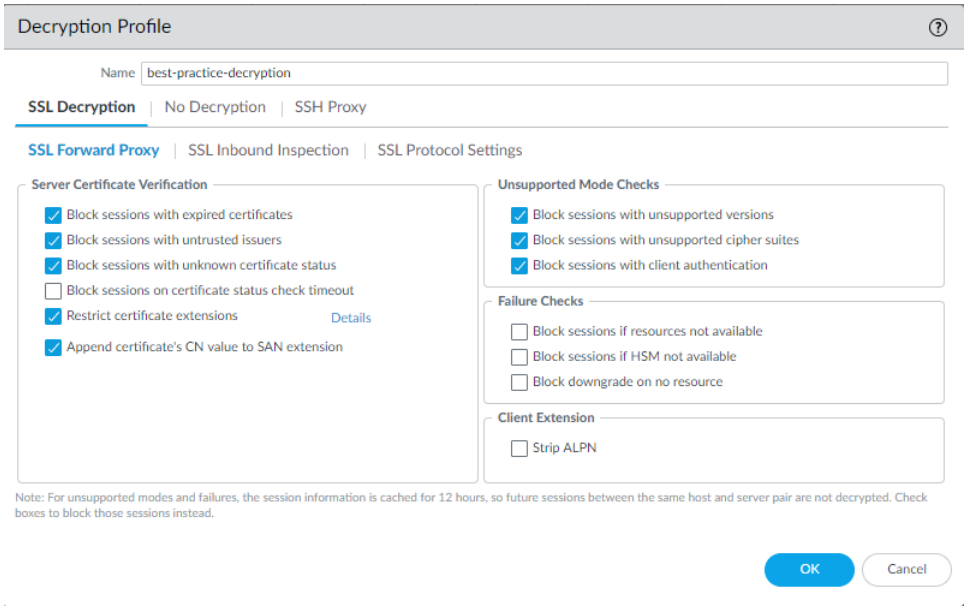



1. 网络上的内部客户端尝试启动与外部服务器的 TLS 会话。
2. 防火墙拦截客户端的 SSL 证书请求。对于客户端，防火墙充当外部服务器，即使正在建立的安全会话使用了防火墙（而非实际服务器）。
3. 随后，防火墙转发客户端的 SSL 证书请求到服务器，以启动与服务器的单独会话。对于服务器，防火墙看起来像客户端，服务器不知道有一个中间人，服务器对证书进行验证。
4. 服务器向防火墙发送一个用于客户端的签名证书。
5. 防火墙对服务器证书进行分析。如果服务器证书由防火墙信任的 CA 签名，且符合您配置的策略和配置文件要求，则防火墙生成一个服务器证书的 SSL 转发信任副本，并将其发送给客户端。如果服务器证书由防火墙不信任的 CA 签名，则防火墙生成一个服务器证书的 SSL 转发不可信副本，并将其发送给客户端。防火墙生成并发送给客户端的证书副本中包含原服务器证书的扩展名，称为 *impersonation* 证书，因为它不是服务器的实际证书。如果防火墙不信任此服务器，则客户端会收到它们正在尝试连接到不受信任站点的阻止页面警告，并且如果让用户选择停用 SSL 解密，则客户端可以选择继续或终止会话。
6. 客户端验证防火墙的模拟证书。然后，客户端启动与服务器的会话密钥交换，而防火墙则充当代理，这与充当代理的方式一致。防火墙转发客户端密钥至服务器，并为客户端制作服务器密钥的模拟副本，这样，防火墙仍充当“隐形”代理，客户端和服务器相信，他们的会话就是相互之间的会话，但仍有两个单独的会话，一个在客户端和防火墙之间进行，另一个在防火墙和服务器之间进行。现在，所有各方都拥有所需的证书和密钥，防火墙可以解密流量。
7. 所有 SSL 会话流量透明地穿过客户端和服务器之间的防火墙。防火墙解密 SSL 流量，将安全策略和配置文件以及解密配置文件应用于流量，重新加密流量，然后转发。

# SSL 转发代理解密配置文件

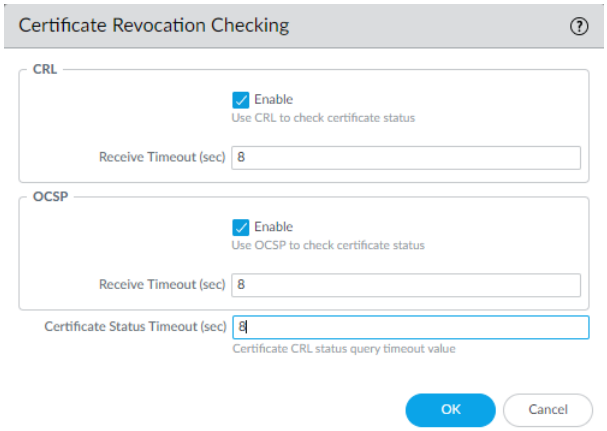
SSL 转发代理解密配置文件（**Objects**（对象）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 转发代理））对用于您附加配置文件的转发代理解密策略中定义的 SSL/TLS 出站流量的服务器验证、会话模式检查和失败检查进行控制。下图显示的是用于转发代理解密配置文件设置的最佳实践一般建议，但您使用的设置取决于公司的安全合规规则和当地法律法规。此外，还为外围互联网网关解密配置文件和数据中心解密配置文件提供特定的最佳实践。


© 2019 Palo Alto Networks, Inc.




服务器证书验证：

- 阻止过期证书会话 — 始终检查此框，阻止拥有过期证书服务器的会话，并阻止访问潜在不安全站点。如果不检查此框，则用户可能会与潜在恶意站点连接，并进行交易，并在尝试连接时查看警告消息，但此时连接不会受阻。
- 阻止不可信颁发者会话 — 始终检查此框，阻止拥有不可信证书颁发者服务器的会话。不可信颁发者可能是指中间人攻击、重放攻击或其他攻击。
- 阻止带未知证书状态的会话 — 当服务器的证书吊销状态返回成“未知”状态时，阻止 SSL/TLS 会话。因为证书状态可能由于多种原因而未知，因此，对于一般解密安全，检查此框通常会过多地加强安全性。但是，在诸如数据中心之类的网络中高安全性区域，检查此框就很有意义。
- 阻止证书状态检查超时上的会话 — 若证书检查超时，是否需要阻止会话，这取决于您公司的安全合规性立场，因为这是更严格的安全性和更好的用户体验的权衡。证书状态验证可以检查吊销服务器上的证书吊销列表 (CRL)，或使用在线证书状态协议 (OCSP) 查看颁发的 CA 是否已吊销，且证书不受信。但是，吊销服务器响应速度很慢，导致会话超时，即使是证书有效，防火墙也会阻止会话。如果 **Block sessions on certificate status check timeout**（阻止证书状态检查超时上的会话）且吊销服务器响应速度很慢，则可以使用 **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Decryption Settings**（解密设置），然后单击 **Certificate Revocation Checking**（证书吊销检查）将默认超时值 5 秒更改为其他值。例如，您可以将超时值增至 8 秒，如下图所示。因为服务器证书可能包含 CRL 分发点 (CDP) 扩展中的 CRL URL 以及颁发机构信息访问 (AIA) 证书扩展中的 OCSP URL，则启用 CRL 和 OCSP 证书吊销检查。






© 2019 Palo Alto Networks, Inc.

- 限制证书扩展 — 选中此框，将服务器证书中的证书扩展限制为密钥用法和扩展密钥用法，并阻止带其他扩展的证书。但是，在某些部署中，可能需要其他一些证书扩展，因此，如果您的部署不需要其他证书扩展，则仅选中此框。
- 附加证书 **CN** 值到 **SAN** 扩展 — 选中此框，确保当浏览器要求服务器证书使用主题备用名称 (SAN) 且不支持基于公用名 (CN) 的证书匹配时，如果证书不具有 SAN 扩展，用户仍可以访问请求的 Web 资源，因为防火墙会将 SAN 扩展（基于 CN）添加到模拟证书。

不受支持模式检查。如果您不阻止带不受支持模式的会话，一旦与潜在不安全服务器连接，用户将接收警告消息，他们可以单击此消息，访问可能存在危险的站点。阻止这些会话可以保护您免受使用较弱且有风险的协议版本和算法的服务器的影响：

- 阻止带不受支持版本的会话 — 配置 SSL 协议设置解密配置文件时，可以指定网络上允许的最低版本的 SSL 协议，从而通过阻止较弱的协议来减少攻击面。始终选中此框以阻止您选择不予支持且带较弱 SSL/TLS 协议版本的会话。
- **Block sessions with unsupported cipher suites**（阻止带不受支持密码套件的会话）— 如果防火墙不支持握手中指定的密码套件，则始终选中此框以阻止会话。您可以在解密配置文件的 **SSL Protocol Settings**（**SSL** 协议设置）选项卡上配置防火墙支持的算法。
- 阻止带客户端身份验证的会话 — 如果您没有需要进行客户端身份验证的关键应用程序，则阻止此会话，因为防火墙不会解密需要进行客户端身份验证的会话。防火墙需要客户端和服务器证书以执行双向解密，但是，通过客户端身份验证，防火墙仅知道服务器证书。这会对用于客户端身份验证会话的解密进行破解。选中此框后，防火墙会阻止除SSL 解密排除列表上站点会话以外的所有带客户端身份验证的会话（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））。

  如果您不 **Block sessions with client authentication**（阻止带客户端身份验证的会话），当防火墙尝试解密使用客户端身份验证的会话时，防火墙允许此会话，并将包含服务器 URL/IP 地址、应用程序和解密配置文件的条目添加到本地解密排除缓存。

  您可能需要允许来自使用客户端身份验证的站点以及不属于 *SSL* 解密排除列表中预定义站点的站点的网络上的流量。创建一个根据客户端身份验证允许会话的解密配置文件。将其添加到仅用于托管应用程序的服务器的解密策略。为了进一步提高安全性，您可能需要多重因素身份验证来完成用户登录过程。

失败检查：

- **Block sessions if resources not available**（如果资源不可用，则阻止会话）— 如果在无可用的防火墙处理资源时阻止会话，则防火墙将在没有用于解密流量的资源时丢弃流量。如果您没有在防火墙因为缺少资源而无法处理解密时阻止会话，那么，您要解密的流量会进入网络并保持加密状态，因此，不会被检测。但是，在资源不可用时阻止会话会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及用户体验的依赖性，这与更严格的安全性相关。或者，考虑使用处理能力更强的防火墙型号，这样，您可以解密更多的流量。
- **HSM** 不可用时阻止会话 — 如果使用硬件安全模块 (HSM) 存储私钥，是否需要使用私钥将取决于您在以下方面的合规性规则：私钥必须来自何处，以及如果处理 HSM 不可用时的加密流量。例如，如果您的公司要求使用用于私钥签名的 HSM，则在 HSM 不可用时阻止会话。但是，如果您的公司对此不那么严格，则您可以考虑在 HSM 不可用时不阻止会话。（如果 HSM 关闭，则防火墙可以处理缓存有来自 HSM 响应的站点的解密，但不会处理其他站点的解密。）在这种情况下，最佳做法是根据您公司的政策行事。如果 HSM 对您的业务至关重要，则在高可用性 (HA) 对中运行 HSM（PAN-OS 8.1 支持 HSM HA 对中的两个成员）。
- **Block downgrade on no resource**（在无资源时阻止降级）— 如果防火墙没有适用于 TLSv1.3 的处理资源，则阻止将防火墙从 TLSv1.3 降级到 TLSv1.2。如果阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会丢弃使用 TLSv1.3 的流量，而不是降级到 TLSv1.2。如果不阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会降级到 TLSv1.2。但是，在资源不可用时阻止降级会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及用户体验的依赖性，这与更严格的安全性相关。您可能希望创建一个单独的解密策略和配置文件，以管理您不想降级 TLS 版本的敏感流量的解密。


© 2019 Palo Alto Networks, Inc.

# SSL 入站检查

使用 SSL 入站检查可解密和检查从客户端到目标网络服务器（拥有其证书且可将该证书导入防火墙的任何服务器）之间的入站 SSL/TLS 流量。例如，如果员工远程连接到 Web 服务器托管的公司网络，并试图将限制的内部文档添加到其 Dropbox 文件夹（使用 SSL 进行数据传输），则 SSL 入站检查可通过阻止或限制会话确保公司安全网络不会泄露敏感数据。

在防火墙上，您必须为想要执行 SSL 入站检查的每个服务器安装证书和私钥。此外，还必须在执行 SSL 入站检查的每个防火墙上安装公钥证书和私钥。防火墙执行 SSL 入站检查的方式取决于协商密钥的类型、Rivest、Shamir、Adleman (RSA) 或完全正向保密 (PFS)

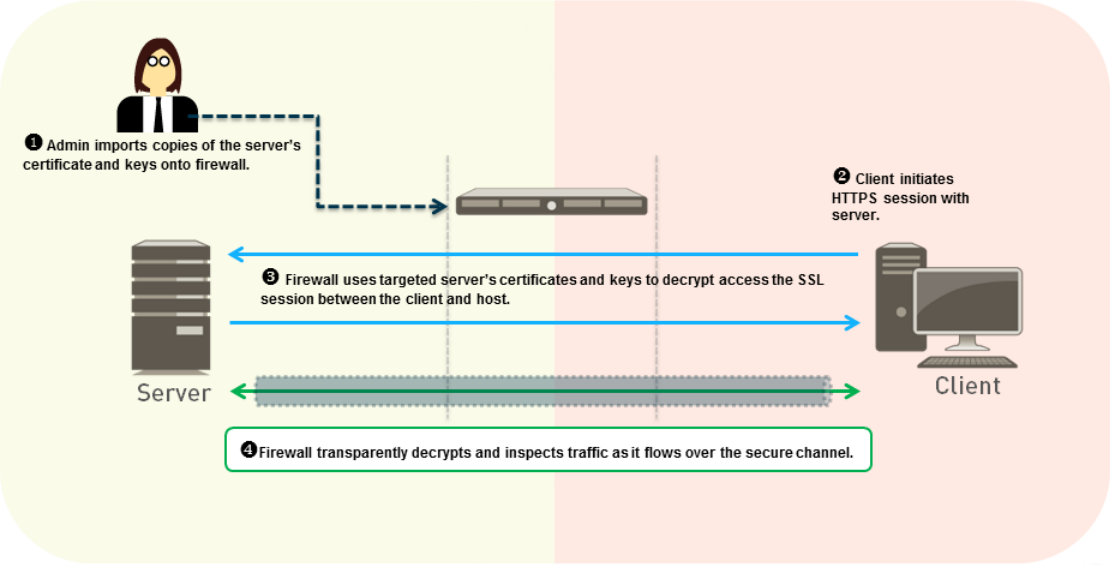
对于 RSA 密钥，防火墙可在不终止连接的情况下执行 SSL 入站检查。当加密会话流量流经防火墙时，防火墙会透明地进行复制，并对其进行解密，这样，防火墙可以将适当的策略应用于流量。

配置用于 *SSL* 入站检查流量的 SSL 协议设置解密配置文件时，为具有不同安全功能的服务器的创建单独的配置文件。例如，如果某一组的服务器仅支持 *RSA*，则 *SSL* 协议设置仅需支持 *RSA* 即可。但是，支持 *PFS* 的 *SSL* 协议设置应支持 *PFS*。配置受服务器支持的最高安全水平的 *SSL* 协议设置，但对性能进行检查，确保防火墙资源可以处理高安全协议和算法所需的高处理负载。

对于使用 Diffie-Hellman exchange (DHE) 或椭圆曲线 Diffie-Hellman exchange (ECDHE) 的 PFS 密钥，防火墙充当外部客户端和内部服务器之间的中间人代理。由于 PFS 会在每个会话中生成新的密钥，防火墙无法在入站 SSL 流量通过时简单地对其进行复制和解密，因此防火墙必须充当代理设备。

下图显示了当密钥交换算法为 RSA 时，SSL 入站检查的工作原理。当密钥交换算法是 PFS 时，防火墙充当代理（在客户端和防火墙之间创建一个安全会话，在防火墙和服务器之间创建另一个安全会话），必须为每个安全会话生成新的会话密钥。

有关启用此功能的详细信息，请参阅配置 SSL 入站检查。

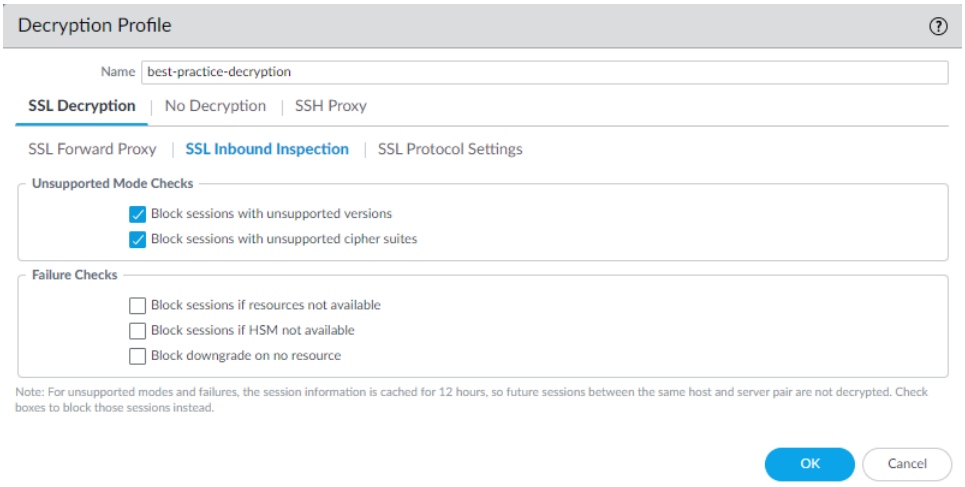



# SSL 入站检查解密配置文件

SSL 入站检查解密配置文件（**Objects**（对象）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（**SSL** 解密）> **SSL Inbound Inspection**（**SSL** 入站检查））对用于您附加配置文件的入站检查解密策略中定义的 SSL/TLS 入站流量的会话模式检查和失败检查进行控制。下图显示的是用于入站检查解密配置文件设置的最佳实践一般建议，但您使用的设置取决于公司的安全合规规则和当地法律法规。



© 2019 Palo Alto Networks, Inc.




不受支持模式检查。如果您不阻止带不受支持模式的会话，一旦与潜在不安全服务器连接，用户将接收警告消息，他们可以单击此消息，访问可能存在危险的站点。阻止这些会话可以保护您免受使用较弱且有风险的协议版本和算法的服务器的影响：

1. **Block sessions with unsupported versions**（阻止带不受支持版本的会话）— 配置SSL 协议设置解密配置文件时，可以指定网络上允许的最低版本的 TLS 协议，从而通过阻止较弱的协议来减少攻击面。始终选中此框以阻止您选择不予支持且带较弱 SSL 和 TLS 协议版本的会话。
2. **Block sessions with unsupported cipher suites**（阻止带不受支持密码套件的会话）— 如果防火墙不支持握手中指定的密码套件，则始终选中此框以阻止会话。您可以在解密配置文件的 **SSL Protocol Settings**（**SSL** 协议设置）选项卡上配置防火墙支持的算法。

失败检查：

- **Block sessions if resources not available**（如果资源不可用，则阻止会话）— 如果在无可用的防火墙处理资源时阻止会话，则防火墙将在没有用于解密流量的资源时丢弃流量。如果您没有在防火墙因为缺少资源而无法处理解密时阻止会话，那么，您要解密的流量会进入网络并保持加密状态，因此，不会被检测。但是，在资源不可用时阻止会话会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及用户体验的依赖性，这与更严格的安全性相关。或者，考虑使用处理能力更强的防火墙型号，这样，您可以解密更多的流量。
- **HSM** 不可用时阻止会话 — 如果使用硬件安全模块 (HSM) 存储私钥，是否需要使用私钥将取决于您在以下方面的合规性规则：私钥必须来自何处，以及如果处理 HSM 不可用时的加密流量。例如，如果您的公司要求使用用于私钥签名的 HSM，则在 HSM 不可用时阻止会话。但是，如果您的公司对此不那么严格，则您可以考虑在 HSM 不可用时不阻止会话。（如果 HSM 关闭，则防火墙可以处理缓存有来自 HSM 响应的站点的解密，但不会处理其他站点的解密。）在这种情况下，最佳做法是根据您公司的政策行事。如果 HSM 对您的业务至关重要，则在高可用性 (HA) 对中运行 HSM（PAN-OS 8.1 支持 HSM HA 对中的两个成员）。
- **Block downgrade on no resource**（在无资源时阻止降级）— 如果防火墙没有适用于 TLSv1.3 的处理资源，则阻止将防火墙从 TLSv1.3 降级到 TLSv1.2。如果阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会丢弃使用 TLSv1.3 的流量，而不是降级到 TLSv1.2。如果不阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会降级到 TLSv1.2。但是，在资源不可用时阻止降级会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及用户体验的依赖性，这与更严格的安全性相关。您可能希望创建一个单独的解密策略和配置文件，以管理您不想降级 TLS 版本的敏感流量的解密。

# SSL 协议设置解密配置文件

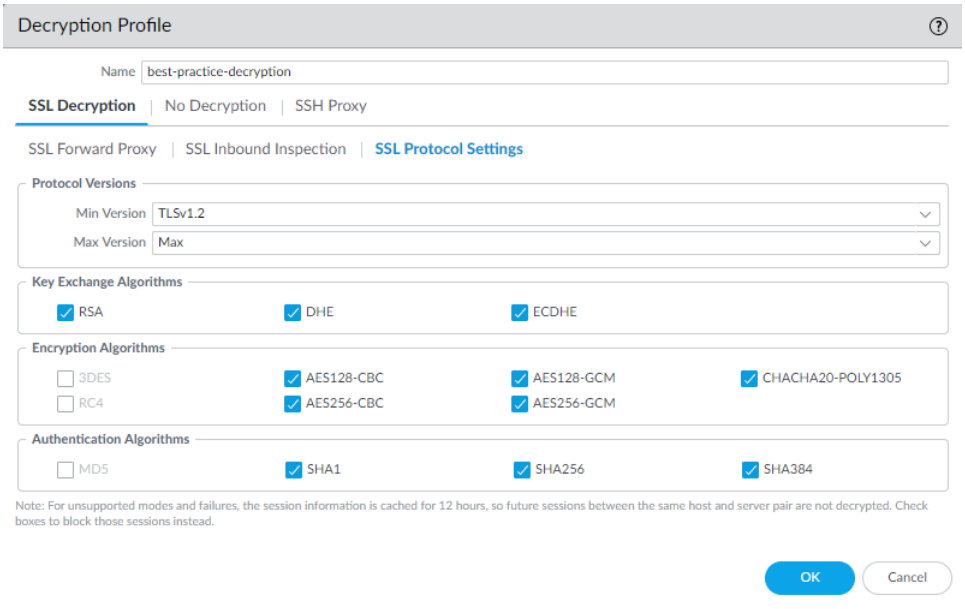
SSL 协议设置（**Objects**（对象）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 协议设置））对是否允许易受攻击的 SSL/TLS 协议版本、弱加密算法和弱身份


© 2019 Palo Alto Networks, Inc.

验证算法进行控制。SSL 协议设置应用于出站 SSL 转发代理和入站 SSL 入站检查流量。这些设置不会应用于 SSH 代理流量或您不会解密的流量。

下图显示的是用于 SSL 协议设置的最佳实践一般建议。此外，还为外围互联网网关解密配置文件和数据中心解密配置文件提供特定的最佳实践。

配置用于 *SSL* 入站检查流量的 *SSL* 协议设置时，为具有不同安全功能的服务器的创建单独的配置文件。例如，如果某一组的服务器仅支持 *RSA*，则 *SSL* 协议设置仅需支持 *RSA* 即可。但是，支持 *PFS* 的 *SSL* 协议设置应支持 *PFS*。配置受您要保护的目标服务器支持的最高安全水平的 *SSL* 协议设置，但对性能进行检查，确保防火墙资源可以处理高安全协议和算法所需的高处理负载。




协议版本：

- 设置 **Min Version**（最小版本）为 **TLSv1.2** 以提供重视安全支持 TLSv1.2 的最强安全业务站点。如果站点（或站点类别）仅支持较弱的密码，请查看该站点，并确定其是否包含有合法的业务应用程序。如果包含，则通过以下方式将此站设为例外：配置与站点支持的最强密码匹配的带 **Min Version**（最小版本）的解密配置文件，然后将配置文件用于解密策略规则，以限制允许弱密码仅用于此站点或涉及的多个站点。如果站点不包含合法的业务应用程序，则不得削弱您的安全状态来支持此站点 — 弱协议（和密码）包含攻击者可以利用的已知漏洞。

  如果站点属于开展业务不需要使用的站点类型，则使用 URL 过滤阻止对整个类别的访问。请勿支持弱加密或身份验证算法，除非您必须这样做以支持重要的历史站点，当您创建例外时，请单独创建一个仅允许用于这些站点的较弱协议的解密配置文件。请勿降级仅应用于 TLSv1.1 大多数站点的主要解密配置文件，以适应较弱站点。

  *Qualys SSL Labs* SSL Pulse *Web* 页面提供了世界上 *150000* 个最受欢迎站点使用的具有不同密码和协议百分比的最新统计数据，因此，您可以了解趋势，知道全球范围内对更安全的密码和协议的需求有多广。
- 设置 **Max Version**（最大版本）为 **Max**（最大），而不是特定版本，这样防火墙会随协议的改善自动支持最新和最佳协议。无论您是想将解密配置文件附加到管理入站（SSL 入站检查）或出站（SSL 转发代理）流量的解密策略规则，请避免允许弱算法。

  如果解密策略支持移动应用程序，且其中有很多都使用固定证书，请将 *Max Version*（最高版本）设为 *TLSv1.2*。因为 *TLSv1.3* 会对在之前 *TLS* 版本中未加密的证书信息进行加密，防火墙无法根据证书信息自动添加解密排除项，这会影响某些移动应用程序。因此，


© 2019 Palo Alto Networks, Inc.

一旦启用 *TLSv1.3*，除非您已为该流量创建不解密策略，否则，防火墙可能会丢弃某些移动应用程序流量。

如果您知晓用于开展业务的移动应用程序，则考虑为这些应用程序创建单独的解密策略和配置文件，以便能够为所有其他流量启用 *TLSv1.3*。

密钥交换算法：将所有三个方框均保持选中状态（默认），以支持 RSA 和 PFS（DHE 和 ECDHE）密钥交换，但最低版本设为 TLSv1.3 时除外，因为它只支持 ECDHE。



要支持 *HTTP/2* 流量，您必须勾选 *ECDHE* 框。

加密算法：设置协议最低版本为 TLSv1.2 后，将自动取消选中（阻止）较老、较弱的 3DES 和 RC4 算法。一旦将协议最低版本设为 TLSv1.3，就会自动阻止 3DES、RC4、AES128-CBC 和 AES256-CBC 算法。对于必须允许较弱 TLS 协议的任何流量，创建一个单独的解密配置文件，并将其仅应用于此站点的流量，然后取消选中相应的方框以允许算法。允许使用 3DES 或 RC4 算法的流量会使您的网络面临巨大风险。如果阻止 3DES 或 RC4 会阻止您访问业务所需的站点，则为此站点创建一个单独的解密配置文件和测量。请勿弱化任何其他站点的解密。

身份验证算法：防火墙自动阻止较老、较弱的 MD5 算法。如果将最低版本设为 TLSv1.3，防火墙还会阻止 SHA1。请勿允许您网络上的经过身份验证的 MD5 流量，SHA1 是您应该允许的最弱身份验证算法。如果站点均不必使用 SHA1，则阻止 SHA1 流量以进一步减少攻击面。

## SSH 代理

在 SSH 代理配置中，防火墙驻留在客户端和服务器之间。防火墙通过 SSH 代理解密对入站和出站 SSH 连接进行解密，确保攻击者无法使用 SSH 来挖掘不需要的应用程序和内容。SSH 解密不需要证书，防火墙在其启动时会自动生成用于 SSH 解密的密钥。在防火墙启动过程中，它会检查是否有现有的密钥。如果没有，防火墙会产生一个密钥。防火墙使用密钥对防火墙上配置的所有虚拟系统的 SSH 会话和所有 SSH v2 会话进行解密。

SSH 允许隧道，以便隐藏恶意流量，防止对其进行解密。防火墙可以解密 SSH 隧道内的流量。可以通过为其 **Action**（操作）设置为 **Deny**（拒绝）的应用程序 **ssh-tunnel**（**SSH** 隧道）配置安全策略规则（以及允许来自 **ssh** 应用程序流量的安全策略规则）的方式阻止所有 SSH 隧道流量。

SSH 隧道会话可以挖掘 X11 Windows 数据包和 TCP 数据包。一个 SSH 连接可能包含多个通道。将 SSH 解密配置文件应用于流量时，对于连接中的每个通道而言，防火墙会检查流量 App-ID，标识通道类型。通道类型可以是：

- 会话
- X11
- 转发的 tcpip
- 直接的 tcpip

当通道类型是会话时，防火墙将流量标识为允许的 SSH 流量，例如 SFTP 或 SCP。当通道类型是 X11、forwarded-tcpip 或 direct-tcpip 时，防火墙将流量标识为 SSH 隧道流量，并加以阻止。

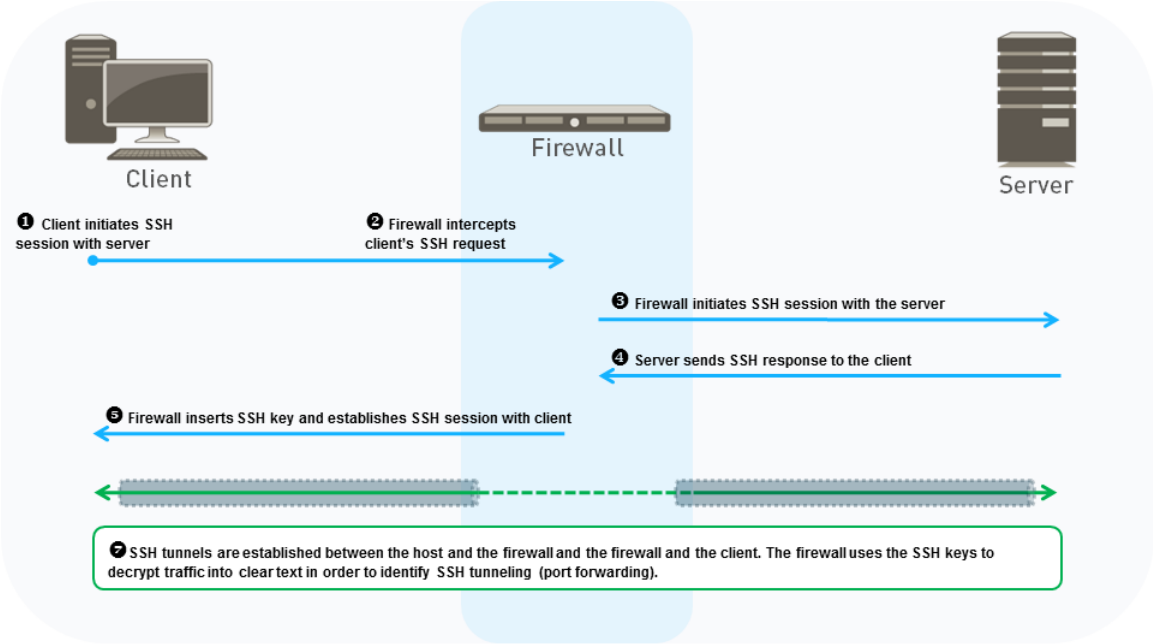


将 *SSH* 使用限制为需要管理网络设备、记录所有 *SSH* 流量、且考虑配置多重因素身份验证的管理员，确保只有合法用户可以使用 *SSH* 访问设备，从而减少攻击面。

下图显示 SSH 代理解密的工作原理。有关如何启用 SSH 代理解密的信息，请参阅配置 SSH 代理。



© 2019 Palo Alto Networks, Inc.




当客户端将 SSH 请求发送到服务器以启动会话时，防火墙会拦截此请求并将其转发到服务器。随后，防火墙拦截服务器响应并将其转发到客户端。这将建立两个单独的 SSH 隧道：一条隧道位于防火墙和客户端之间，另一条位于防火墙和服务器之间，而防火墙则充当代理。当流量在客户端和服务器之间流动时，防火墙会检查 SSH 流是正常路由还是使用 SSH 隧道（端口转发）。防火墙不会对 SSH 隧道执行内容和威胁检查，但是，如果防火墙识别出 SSH 隧道，则会阻止 SSH 隧道流量，并根据配置的安全策略加以限制。

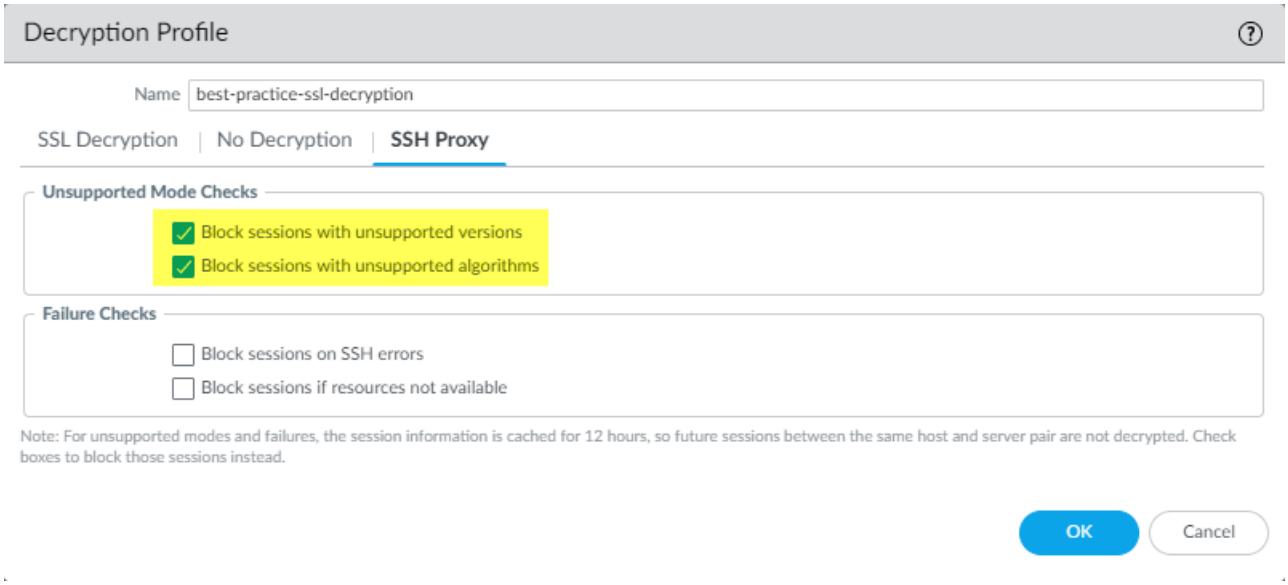
## SSH 代理解密配置文件

SSH 代理解密配置文件（**Objects**（对象）> **Decryption Profile**（解密配置文件）> **SSH Proxy**（**SSH** 代理））对用于您附加配置文件的 SSH 代理解密配置文件策略中定义的 SSH 流量的会话模式检查和失败检查进行控制。下图显示的是用于 SSH 代理解密配置文件设置的最佳实践一般建议，但您使用的设置取决于公司的安全合规规则和当地法律法规。

防火墙不会对 *SSH* 隧道执行内容和威胁检查（端口转发）。但是，防火墙会区分 *SSH* 应用程序和 *SSH* 隧道应用程序。如果防火墙识别出 *SSH* 隧道，则会根据配置的安全策略阻止 *SSH* 隧道流量，并限制流量。



© 2019 Palo Alto Networks, Inc.




不受支持模式检查。防火墙支持 SSHv2。如果您不阻止带不受支持模式的会话，一旦与潜在不安全服务器连接，用户将接收警告消息，他们可以单击此消息，访问可能存在危险的站点。阻止这些会话可以保护您免受使用较弱且有风险的协议版本和算法的服务器的影响：

1. 阻止带不受支持版本的会话 — 防火墙具有一组预定义受支持版本。选中此框会阻止较弱版本的流量。始终选中此框以阻止带较弱协议版本的会话，从而减少攻击面。
2. 阻止带不受支持算法的会话 — 防火墙具有一组预定义受支持算法。选中此框会阻止带较弱算法的流量。始终选中此框以阻止带不受支持算法的会话，从而减少攻击面。

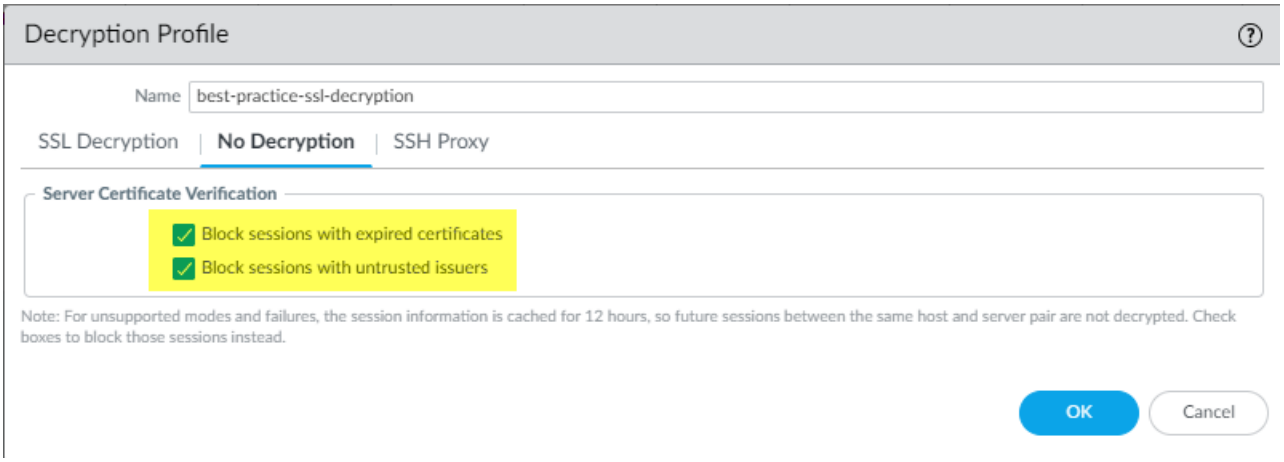
失败检查：

- 阻止 **SSH** 错误中的会话 — 如果 SSH 发生错误，则选中此框终止会话。
- 资源不可用时阻止会话 — 如果您不想在防火墙处理资源不可用时阻止会话，则想要解密的加密流量仍以加密的形式进入网络，从而导致潜在危险连接。但是，在防火墙处理资源不可用时阻止会话会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及您的业务对用户体验的依赖性，这与更严格的安全性相关。或者，考虑使用处理能力更强的防火墙型号，这样，您可以解密更多的流量。

# 不解密配置文件

“不解密”配置文件（**Objects**（对象）> **Decryption Profile**（解密配置文件）> **No Decryption**（不解密））将对您选择不解密的流量执行服务器验证检查。您可以将“不解密”配置文件附加到“不解密”解密策略（用于定义从解密中排除的流量）。（请勿使用策略来排除不能解密的流量，因为网站可能会因固定证书或策略要求的相互身份验证等技术原因破解解密。相反，应将主机名添加到解密排除列表。）下图显示的是用于无解密配置文件设置的最佳实践一般建议，但您使用的设置取决于公司的安全合规规则和当地法律法规。


© 2019 Palo Alto Networks, Inc.




- 阻止过期证书会话 — 检查此框，阻止拥有过期证书服务器的会话，并阻止访问潜在不安全站点。如果不检查此框，则用户可能会与潜在恶意站点连接，并进行交易，并在尝试连接时查看警告消息，但此时连接不会受阻。
- 阻止不可信颁发机构会话 — 检查此框，阻止拥有不可信证书颁发机构服务器的会话。不可信颁发者可能是指中间人攻击、重放攻击或其他攻击。

请勿将不解密配置文件附加到用于您不解密的 *TLSv1.3* 流量的解密策略。与之前的版本不同，*TLSv1.3* 将加密证书信息，这样，防火墙就无法查看证书数据，也不会阻止过期证书会话或不可信颁发机构会话，因此，配置文件就会无效。（防火墙可对 *TLSv1.2* 以及更低版本执行证书检查，因为这些协议不会加密证书信息，您应对这些流量应用“不解密”配置文件。）但是，应为未解密的 *TLSv1.3* 流量创建解密策略，因为除非此解密策略可以控制该流量，否则，防火墙将不会记录未解密的流量。

（适用于 *TLSv1.2* 以及更早版本）如果选择允许不可信颁发者会话（不建议），且仅*Block sessions with expired certificates*（阻止过期证书会话），在某些情况下，可能会无意阻止可信的过期颁发者会话。如果防火墙证书存储区包含有效的自签名可信 *CA*，且服务器在证书链中发送过期 *CA*，则防火墙不会检查其证书存储区。相反，防火墙会在发现可信的有效替代信任锚点时阻止基于过期 *CA* 的会话，并允许基于可信任的自签名证书的会话。

为避免这种情况，除了 *Block sessions with expired certificates*（阻止过期证书会话），还应启用 *Block sessions with untrusted issuers*（阻止不可信颁发者会话）。这样，防火墙就必须检查其证书存储区，查找自签名可信 *CA*，并允许会话。

## 用于椭圆曲线加密法 (ECC) 证书的 SSL 解密

防火墙使用 ECC 证书自动解密来自网站和应用程序的 SSL 流量，包括椭圆曲线数字签名算法 (ECDSA) 证书。鉴于组织转向使用 ECC 证书从强大的密钥和小型证书大小中受益，因此您可以继续查看并安全启用 ECC 安全应用程序和网站流量。

使用 *ECC* 证书的网站和应用程序的解密不支持镜像到防火墙的流量；使用 *ECC* 证书的加密流量必须直接通过防火墙以便防火墙对其进行解密。

您可以使用硬件安全模块 (HSM) 存储与 *ECDSA* 证书相关联的私钥。对于 *TLSv1.3* 流量，*PAN-OS* 仅支持 *SSL* 转发代理的 *HSM*。它不支持 *SSL* 入站检测的 *HSM*。

## 用于 SSL 解密的完全正向保密 (PFS)

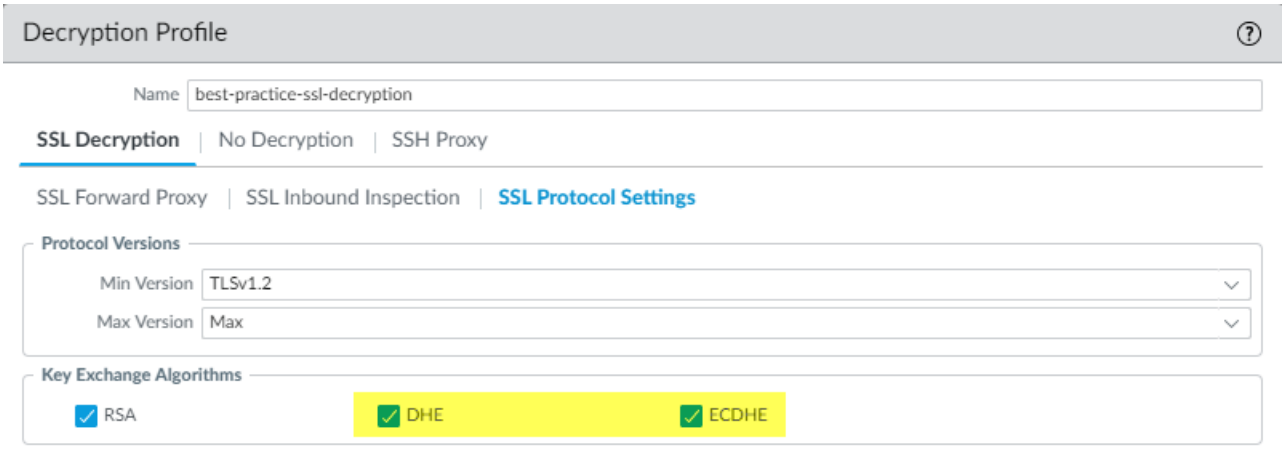
PFS 是一种防止攻陷一个加密会话从而攻陷多个加密会话的安全通信协议。服务器通过 PFS 为与客户端建立的每个安全会话生成唯一私钥。如果服务器私钥被攻陷，则只有使用该密钥建立的单个会话才会遭受攻击，


© 2019 Palo Alto Networks, Inc.

而攻击者无法从过去和将来会话中检索数据，因为服务器建立的每个会话均带有生成的唯一密钥。防火墙解密使用 PFS 密钥交换算法建立的 SSL 会话，并保留过去和未来会话的 PFS 保护。

默认启用支持基于 Diffie-Hellman (DHE) 的 PFS 和椭圆曲线基于 Diffie-Hellman (ECDHE) 的 PFS（**Objects**（对象）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 协议设置）。

如果使用 *DHE* 或 *ECDHE* 密钥交换算法来启用支持 *SSL* 解密的 *PFS*，则可以使用硬件安全模块 (HSM) 来存储 *SSL* 入站检查的私钥。

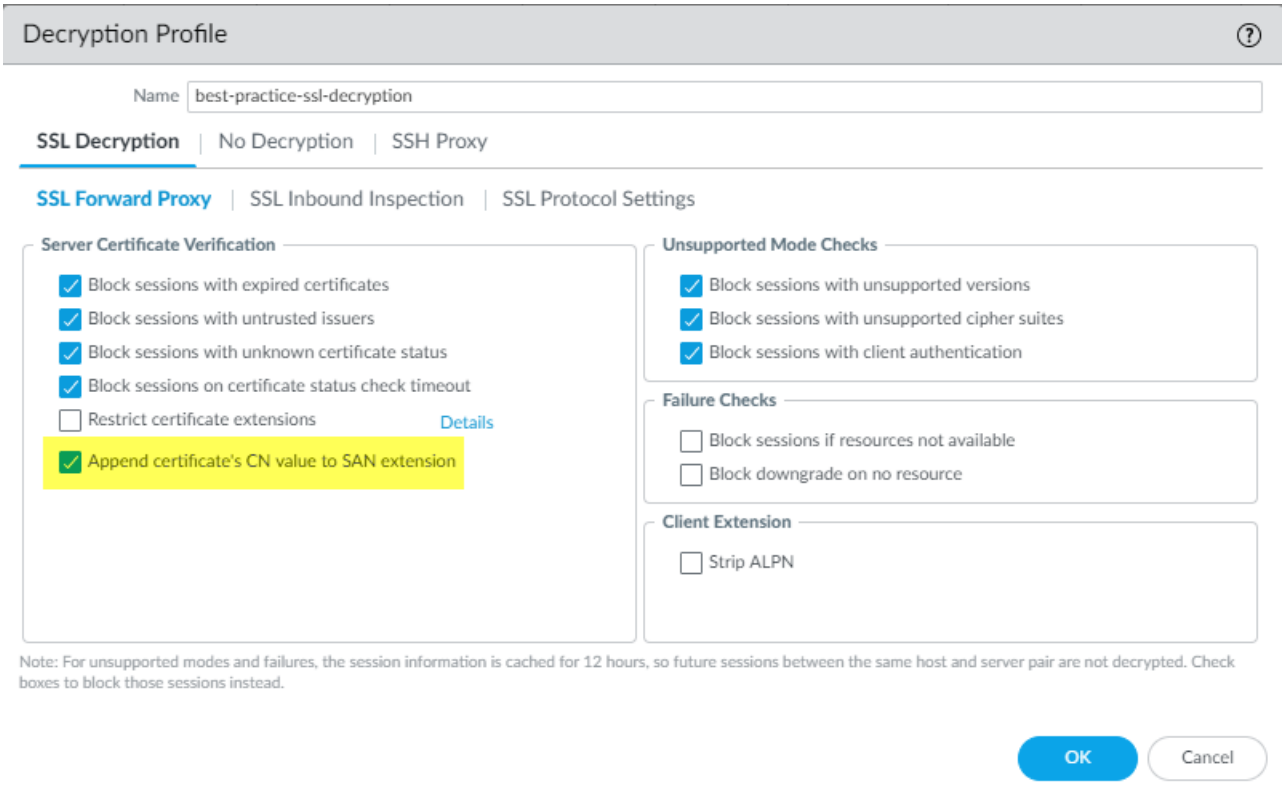



# SSL 解密和主题备用名称(SAN)

一些浏览器需要服务器证书使用“主题备用名称”(SAN) 以指定证书保护的域，且不再支持基于服务器证书公用名 (CN) 的证书匹配。SAN 使单个服务器证书保护多个名称；CN 的定义不及 SAN，只能保护单个域或是域中所有第一级子域。但是，如果服务器证书仅包含一个 CN，则需要 SAN 的浏览器将不会允许最终用户连接至请求的 Web 资源。防火墙可以将 SAN 添加到生成的模拟证书，并在 SSL 解密期间将自己创建为受信任的第三方。当服务器证书仅包含一个 CN，则执行 SSL 解密的防火墙将服务器证书 CN 复制到模拟证书 SAN。防火墙将带有 SAN 的模拟证书提供给客户端，然后，浏览器才能支持链接。最终用户可以继续访问其所需的资源，防火墙可以解密会话。

要启用支持解密 SSL 流量的 SAN，请更新附加到相关解密策略的解密配置文件：选择 **Objects**（对象）> **Decryption Profile**（解密配置文件）> **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 转发代理）> **Append certificate's CN value to SAN extension**（将证书 **CN** 值附加到 **SAN** 扩展））。


© 2019 Palo Alto Networks, Inc.




# TLSv1.3 解密

您可以解密 TLSv1.3 流量，全面了解 TLSv1.3 流量，并阻止 TLSv1.3 流量中的已知和未知威胁。TLSv1.3 是最新版 TLS 协议，可提供应用程序安全性和性能提升。当您将关联的解密配置文件配置为使用 TLSv1.3 作为最低协议版本或使用 TLSv1.3 或最新可用版本作为最高协议版本时，就可将现有解密策略与 TLSv1.3 一起使用。防火墙支持 TLSv1.3 转发代理解密、入站检查、解密代理和解密端口映射。

若要使用 TLSv1.3，客户端和服务器必须能够协商 TLSv1.3 密码。对于不支持 TLSv1.3 的网站，防火墙将选择服务器支持的较旧版本的 TLS 协议。

防火墙支持的 TLSv1.3 解密算法如下：

- TLS13-AES-128-GCM-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

如果应用至解密流量的解密配置文件将协议的**Max Version**（最高版本）指定为 **Max**（最大值），那么，该配置文件将支持 TLSv1.3，并自动将 TLSv1.3 与支持 TLSv1.3 的站点一起使用。否则，若要支持 TLSv1.3，需将 **Max Version**（最高版本）设为 **Max**（最大）。升级到 PAN-OS 10.0 后，**Max Version**（最高版本）设为 **Max**（最大）的所有解密配置文件均将重置为 **TLSv1.2**，以便自动支持使用固定证书并阻止丢弃该流量的移动应用程序。

并不是所有应用程序都支持 TLSv1.3 协议。根据解密最佳实践，请将 TLS 协议的 **Min Version**（最低版本）设为 **TLSv1.2**，然后将 **Max Version**（最高版本）设置保留为 **Max**（最大）。如果出于业务目的需要允许较弱的 TLS 协议，请单独创建一个具有允许较弱协议的 **Min Version**（最低版本）的 SSL 解密配置文件，并将该配置文件附加到用于定义您需要使用较弱 TLS 协议允许的流量的解密策略中。

如果解密策略支持移动应用程序，且其中有很多都使用固定证书，请将 **Max Version**（最高版本）设为 **TLSv1.2**。因为 TLSv1.3 会对在之前 TLS 版本中未加密的证书信息进行加密，防火墙无法根据证书信息自动添加解密排除项，这会影响某些移动应用程序。因此，一旦启用 TLSv1.3，除非您已为该流量创建不解密策


© 2019 Palo Alto Networks, Inc.

略，否则，防火墙可能会丢弃某些移动应用程序流量。如果您出于业务目的而使用的移动应用程序是已知的，则考虑为这些应用程序创建单独的解密策略和配置文件，这样，您可以为所有其他流量启用 TLSv1.3。



请勿将不解密配置文件附加到用于您不解密的 *TLSv1.3* 流量的解密策略。与之前的 *TLS* 版本相比，变化在于，*TLSv1.3* 加密证书信息，这样，防火墙就再次无法查看证书数据，也不会阻止与过期证书或不可信颁发机构的会话，因此，配置文件将无效。（防火墙可对 *TLSv1.2* 以及更低版本执行证书检查，因为这些协议不会加密证书信息，您应对这些流量应用“不解密”配置文件。）但是，应为未解密的 *TLSv1.3* 流量创建解密策略，因为除非此解密策略可以控制该流量，否则，防火墙将不会记录未解密的流量。

一旦您在SSL 协议设置解密配置文件中允许不受支持的模式，防火墙会自动添加流量到 本地解密排除缓存。防火墙仍会解密并检查从 TLSv1.3 降级到 TLSv1.2 的流量，且在缓存中将服务器添加到缓存的**Reason**（原因）显示为 TLS13_UNSUPPORTED。

如果从 PAN-OS 10.0 降级到之前的版本，那么，将 TLSv1.3 指定为 **Min Version**（最低版本）或 **Max Version**（最高版本）的任何解密配置文件都将切换到最高的受支持版本。例如，从 PAN-OS 10.0 降级到 PAN-OS 9.1 后，TLSv1.3 将被替换为 TLSv1.2。如果运行 PAN-OS 10.0 的 Panorama 设备将配置推送到运行较低版本 PAN-OS 的设备，那么，将 TLSv1.3 指定为 **Min Version**（最低版本）或 **Max Version**（最高版本）的任何解密配置文件也都将切换到最高的受支持版本。



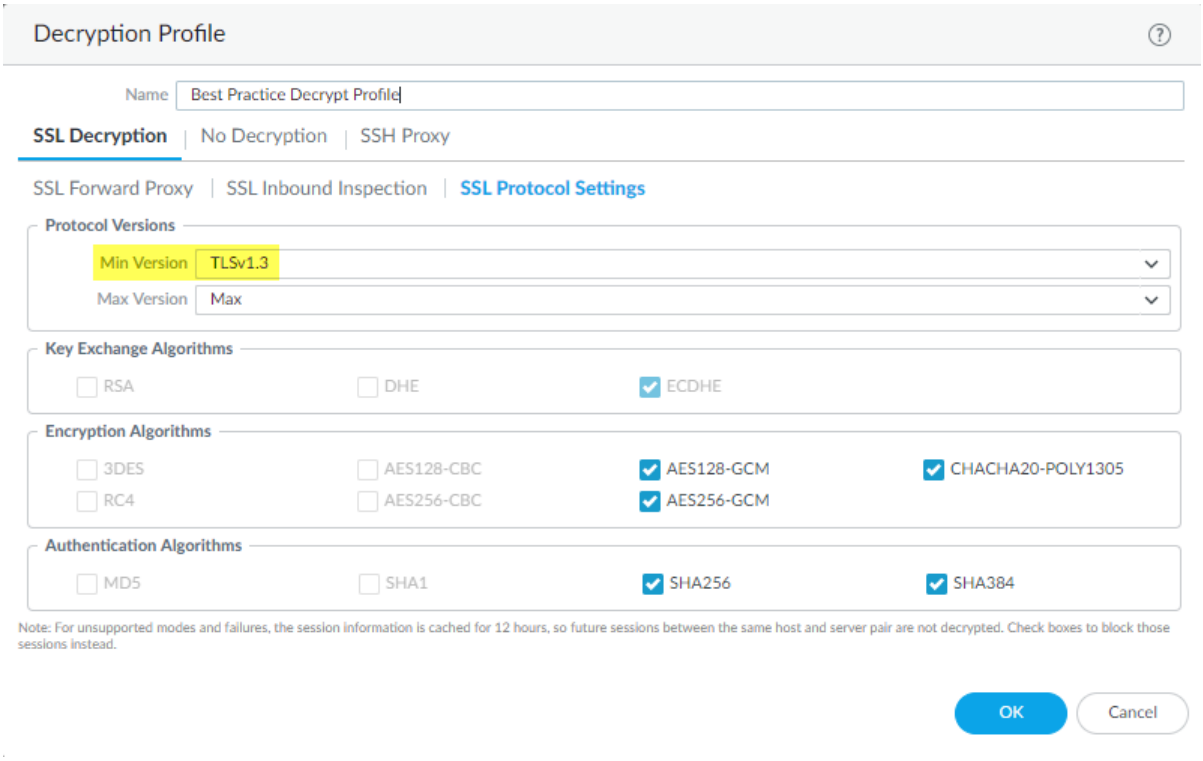
对于 *TLSv1.3* 流量，*PAN-OS* 仅支持 *SSL* 转发代理的硬件安全模块*(HSM)*。它不支持 *SSL* 入站检测的 *HSM*。

您可以配置将 TLSv1.3 设为最低允许协议版本的 SSL 解密配置文件，以获得最佳安全性。但是，有些应用程序不支持 TLSv1.3，且如果 TLSv1.3 不是允许的最低协议版本，这些应用程序可能就不会运行。仅将 TLSv1.3 设为最低版本的配置文件应用到仅支持 TLSv1.3 的应用程序流量。

1. 创建一个新的 SSL 解密配置文件或编辑现有配置文件（**Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件））。

   如果配置文件是新的，请指定配置文件 **Name**（名称）。
2. 选择 **SSL Protocol Settings**（**SSL** 协议设置）。
3. 将 **Min Version**（最低版本）更改为 **TLSv1.3**。


© 2019 Palo Alto Networks, Inc.




为 **Max Version**（最高版本）选择 **Max**（最大），确保配置文件控制的流量可以使用最强的可用协议版本。**Min Version**（最低版本）用于设置流量可以使用的最弱协议版本。将最低版本设为 **TLSv1.3** 意味着流量必须使用 TLSv1.3（或更高版本），且较弱协议版本将被阻止。（解密策略规则定义了配置文件控制的流量。）

一旦将 TLSv1.3 配置为 **Min Version**（最低版本），就必须使用 Perfect Forward Secrecy (PFS)（完全正向保密 (PFS)），且较弱的密钥交换、加密和身份验证算法都将不可用。

4. 配置您需要设置或更改的任何其他解密配置文件设置。
5. 单击 **OK**（确定）保存配置文件。
6. 将配置文件附加到相应的解密策略规则，以将其应用到相应的流量。

# 解密会话的高可用性支持

只有当解密的入站 SSL 会话通过非 PFS 密钥交换算法创建时，防火墙才会支持这些会话的高可用性 (HA) 同步。防火墙不支持任何其他解密流量的 HA 同步。防火墙根据解密策略解密故障转移之后开始的新会话。

下表显示了在故障转移之后加密会话的 HA 同步支持：

| 会话类型 | PFS 密钥交换 | 非 PFS 密钥交换 |
|---|---|---|
| SSL 入站会话（入站检查解密） | 无 HA 同步，防火墙丢弃会话 | 有 HA 同步，防火墙允许会话，但不加密会话 |
| SSL 出站会话（SSL 转发代理解密） | 无 HA 同步，防火墙丢弃会话 | 无 HA 同步，防火墙丢弃会话 |


© 2019 Palo Alto Networks, Inc.

# 正在解密镜像

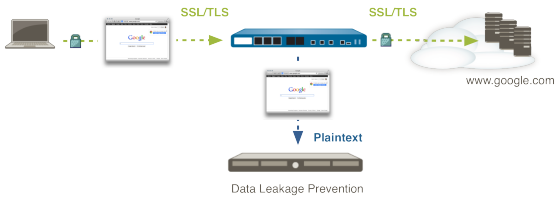
解密镜像可以创建来自防火墙的已解密流量的副本，并将其发送到能够接收原始数据包捕获的流量收集工具（如 NetWitness 或 Solera）以用于存档和分析。对于因取证和历史研究目的或因数据遗失防护 (DLP) 目的而需要全面数据捕获的企业而言，可以安装一个免费许可证来启用此功能。

许可证安装完成后，将流量收集工具直接与防火墙上的以太网接口相连接，并将 **Interface Type**（接口类型）设为 **Decrypt Mirror**（解密镜像）。防火墙使用收集工具模拟 TCP 握手，然后通过此接口发送每个以明文形式解密的数据包。

*VM* 系列没有适用于公共云平台（*AWS*、*Azure*、*Google Cloud Platform*）和 *VMware NSX* 的解密端口镜像功能。

请记住，在某些国家/地区限制解密、存储、检查和/或使用 SSL 流量，并且只有在征得用户同意后才能使用解密镜像功能。此外，使用此功能可能会使得对防火墙拥有管理访问权限的恶意用户盗取用户名、密码、社会安全号码、信用卡号码或使用加密通道提交的其他敏感信息。Palo Alto Networks 建议您在生产环境中激活和使用此功能之前咨询您的企业顾问。

下图显示镜像解密流量的工作过程，配置解密端口镜像部分介绍如何授权许可和启用此功能。





© 2019 Palo Alto Networks, Inc.

# 准备部署解密

部署解密最耗时的部分不是配置解密策略和配置文件，而是部署准备：与利益相关者一起决定解密的流量和不解密的流量，培训用户群有关网站访问变更的信息，开发公钥基础设施 (PKI)，以及计划分阶段的优先部署。

设置解密目标并查看解密规划最佳实践列表，确保您了解推荐的最佳实践。最佳实践的目标是解密防火墙资源允许的流量，并首先解密最重要的流量。



创建和部署解密策略规则前，把基于端口的安全策略规则迁移到基于应用程序的安全策略规则。如果您创建解密规则基于出口安全策略迁移到基于应用程序的安全政策,改变可能导致解密规则阻止流量,您计划让因为安全策略规则使用应用程序默认端口,以防止应用程序流量使用非标准端口。例如，被标识为 *web* 浏览应用程序流量*(*默认端口 *80)*的流量可能具有具有不同默认端口的基础应用程序，例如 *HTTPS* 流量*(*默认端口 *443)*。应用程序默认规则阻止 *HTTPS* 流量，因为使用非标准端口（*443* 而不是 *80*）的解密流量。在部署解密之前迁移到基于 *APP-ID* 的规则意味着当您在 *POC* 中测试您的解密部署时，您将发现安全策略配置错误，并在将其向一般用户群推出之前予以修复。

要准备部署解密：

- 与利益相关者联合制定解密部署策略
- 制定 PKI 推出计划
- 调整防火墙解密部署规模
- 规划分阶段的优先部署

## 与利益相关者联合制定解密部署策略

与法律、财务、HR、管理人员、安全和 IT/支持等利益相关者合作，制定解密部署策略。首先，应获得解密流量所需的批准，以保护公司安全。解密流量包括了解法律法规和业务是如何影响您可以和不可以解密的流量。

标识想要解密的流量，并确定其优先级。最佳做法是尽可能多地解密流量，以便了解加密流量中的潜在威胁，并阻止这些威胁。如果防火墙规模不正确导致您无法解密想要解密的所有流量，则确定最关键服务器、最高风险流量类别、不太可信的分段和 IP 子网的优先级。为了有助于确定优先级，请问自己一些问题，例如“如果此服务器受到攻击，会发生什么？”以及“对于我想要达到的性能水平，我能承受多大的风险？”。

接下来，标识不能解密的流量，因为流量会出于固定证书、不完整的证书链、不受支持密码或相互身份验证等技术原因无法解密。解密技术上无法解密的站点会导致阻止该流量。对技术上无法解密的网站进行评估，并自我提问，您是否需要出于业务原因访问这些站点。如果您无需访问这些站点，则允许解密以进行阻止。如果出于业务目的，您需要访问其中任何一个站点，则将其添加到 SSL 解密排除列表，以便将其从解密中排除。SSL 解密排除列表专用于技术上无法解密的站点。

标识您出于法律、法规、个人或其他原因而选择不进行解密的敏感流量，例如，金融、健康、或政府流量，或是某些高管的流量。这不是技术上无法解密的流量，因此，您无需使用 SSL 解密排除列表将此流量从解密中排除。相反，您可以创建与策略的解密排除以标识和控制您选择不进行解密的流量，并将无解密的解密配置文件应用于策略，从而防止证书有问题的服务器访问网络。基于策略的解密排除仅用于排除您选择不进行解密的流量。

在规划解密策略时，请考虑您公司的安全合规性规则、计算机使用策略和您的业务目标。极度严格的控制会阻止用户访问过去经常访问的非商业站点，从而影响用户体验。但对于政府或金融机构而言，控制就需极度严格。在可用性、管理开销和安全方面始终存在权衡。解密策略越严格，网站无法访问的可能性就越大，从而可能会导致用户投诉，并修改规则库。



© 2019 Palo Alto Networks, Inc.

虽然严格的解密策略在最初可能会导致一些用户投诉，但这些投诉会引起您对未约束或不受欢迎站点的关注，因为这些站点是由于使用了弱算法或拥有证书问题而被阻止。将投诉作为更好地了解网络上流量的工具。

不同的用户组，甚至是个人用户，都可能会需要不同的解密策略，或是您可能想要将相同的解密策略应用于所有用户。例如，管理人员可能免于使用适用于其他员工的解密策略。您可以想要对员工组、承包商、合作伙伴和来宾使用不同的解密策略。准备更新的法律和 HR 计算机使用策略，分发给所有员工、承包商、合作伙伴、客人和任何其他网络用户，以便在您解密时，用户能够理解他们的数据可以解密和扫描以便发现威胁。

处理来宾用户的方式取决于他们所需的访问权限。将来宾放置在单独的 *VLAN* 和单独的 *SSID* 上进行无线访问，这样，就可以将来宾与网络上的其他用户隔离。如果来宾无需访问您的企业网络，则不让他们访问，也就无需解密他们的流量。如果来宾需要访问您的企业网络，则解密其流量：

- 企业不会控制来宾设备。解密来宾流量，并让其遵守您的来宾安全策略，这样，防火墙就可以检测流量，阻止威胁。为此，可以通过捕获门户重定向用户，指导他们如何下载和安装 *CA* 证书，并清楚地通知来宾他们的流量将被解密。将此过程包括在公司的隐私和计算机使用策略中。
- 创建单独的解密策略规则和安全策略规则，以严格控制来宾访问，这样，客户只能访问其需要访问的网络区域。

与不同的用户组类似，确定要解密的设备和要解密的应用程序。当今的网络不仅支持企业设备，还支持 BYOD、移动设备、远程用户设备和其他设备，包括承包商、合作伙伴和来宾设备。现在，用户尝试访问许多约束和未约束的站点，然后，您应该决定想要解密的通信量。

企业不控制 *BYOD* 设备。如果允许网络上的 *BYOD* 设备，则解密其流量，并让其遵守您应用于其他网络流量的相同的安全策略，这样，防火墙可以检测流量，阻止威胁。为此，可以通过捕获门户重定向 *BYOD* 用户，指导他们如何下载和安装 *CA* 证书，并清楚地通知用户他们的流量将被解密。培训 *BYOD* 用户有关这个过程，并将其纳入公司的隐私和计算机使用政策。

确定想要记录的流量，并调查可以记录的流量。请注意有关您可以记录和存储的数据类型，以及您可以记录和存储数据的位置相关的当地法律。例如，当地法律可能会阻止记录和存储健康和财务数据等个人信息。

决定如何处理恶意证书。例如，您是阻止还是允许证书状态未知的会话？了解想要如何处理恶意证书的方式可确定您如何配置您附加到解密策略以根据服务器证书验证状态允许哪种会话的解密配置文件。

## 制定 PKI 推出计划

计划如何推出您的公钥基础设施 (PKI)。网络设备需要 SSL 转发信任 CA 证书（可信站点）和 SSL 转发不可信 CA 证书（不可信站点）。生成单独的转发信任和转发不可信证书（因为想要使用不可信证书警告正在尝试访问潜在危险站点的用户，因此，请勿签署具有企业根 CA 的转发不可信证书）。Palo Alto Networks 下一代防火墙拥有两种生成用于 SSL 解密的 CA 证书的方法。

- 从企业根 **CA** 生成充当从属证书的 **SSL CA** 证书 — 如果已有企业 PKI，这将是最佳做法。因为网络设备已经信任企业根 CA，因此，从您的企业根 CA 生成从属证书使得推出更容易、更顺畅，从而避免在开始部署阶段时出现任何证书问题。如果您没有 Enterprise Root CA，可以考虑获得一个。
- 在防火墙上生成自签名根 **CA** 证书，并在此防火墙上创建从属 **CA** 证书 — 如果没有企业根 CA，可通过此方法获得自签名根 CA 证书以及从属转发信任和不可信 CA 证书。此方法要求您必须在所有网络设备上安装自签名证书，这样，这些设备才能识别防火墙的自签名证书。因为防火墙必须部署到所有设备，因此，相较于大型部署而言，此方法更适用于小型部署和概念验证 (POC) 试验。

不得将转发不可信证书导出到网络设备上的证书信任列表中。因为在信任列表中安装不可信证书将会导致防火墙无法信任设备信任网站，因此，这一点至关重要。此外，用户将看不到不可


© 2019 Palo Alto Networks, Inc.

信站点的证书警告，这样，就不知道这些站点是不受信的，可能会访问这些站点，从而导致网络遭受威胁。



无论您是从企业根 *CA* 生成转发信任证书，还是使用防火墙上生成的自签名证书，均应为每个防火墙生成从属转发信任 *CA*。使用单个从属 *CA* 比较灵活，您可以在设备（或设备组）退役时吊销一个证书，不会对其余部署产生影响，同时也能减少在必须要吊销证书的情况下所产生的任何影响。因为用户看到的 *CA* 错误消息包含有关流量正在遍历的防火墙信息，因此，每个防火墙上的单个转发信任 *CA* 也有助于解决问题。如果在每个防火墙上使用相同的转发信任 *CA*，则会失去该信息的粒度。

在不同的防火墙上使用不同的转发不可信证书毫无益处，因此，可以在所有防火墙上使用相同的转发不可信证书。如果您的私钥需要额外的安全性，请考虑将它们存储在 HSM 。

您可能需要为来宾用户做出专门调整。如果来宾用户无需访问您的企业网络，请勿让其访问，然后，您也无须解密其流量或创建基础架构以支持来宾访问。如果您需要支持来宾用户，请与法务部门讨论是否可以解密来宾流量。

如果您可以解密来宾流量，则以对待 BYOD 设备的方式对待来宾。解密来宾流量，并使其服从与应用于其他网络通信量相同的安全策略。为此，可以通过身份验证门户重定向来宾用户，指导他们如何下载和安装 CA 证书，并清楚地通知用户他们的流量将被解密。将此过程包括在公司的隐私和计算机使用策略中。此外，将来宾流量限制为仅来宾需要访问的区域。

如果您由于法律原因不能解密来宾流量，隔离来宾流量并防止其在您的网络中横向移动：

- 为来宾创建隔离区域，并限制访客对该区域的访问。要防止横向移动，不得允许来宾访问其他区域。
- 仅允许受约束的应用程序，使用 URL 过滤以防止对危险 URL 类别的访问，并应用 最佳实践安全配置文件。
- 应用无解密解密政策和配置文件，以防止来宾使用未知或过期 CA 访问网站。

所有员工、承包商、合作伙伴和其他用户应使用您的常规企业基础架构，且您应解密并检查其流量。

## 调整防火墙解密部署规模

解密加密流量消耗防火墙 CPU 资源，且可能会影响吞吐量。通常，安全级别越高（解密的流量越多，协议设置越严格），解密消耗的防火墙资源就越多。与您的 Palo Alto Networks SE/CE 一起调整防火墙部署的大小，避免调整错误。影响解密资源消耗的因素以及防火墙可以解密的流量数包括：

- 要解密的 SSL 流量。这因网络而异。例如，一些应用程序必须进行解密，以防止恶意软件或漏洞进入网络或是未经授权的数据传输；一些应用程序因为当地法律法规或业务原因而无法解密；而其他应用程序则是明文（未加密），无需解密。想要解密的流量越多，需要的资源就越多。
- TLS 协议版本。版本越高，越安全，但会消耗更多的资源。尽量使用最高的 TLS 协议版本，以最大限度地提高安全性。
- 密钥大小。密钥越大，安全性越高，但密钥处理时消耗的资源也越多。
- 密钥交换算法。Diffie-Hellman Ephemeral (DHE) 椭圆曲线 Diffie-Hellman Exchange (ECDHE) 等完全正向保密 (PFS) 临时密钥交换算法在处理时比 Rivest-Shamir-Adleman (RSA) 算法消耗更多的资源。因为防火墙必须为每个会话生成新的密钥，但生成新的密钥会消耗防火墙更多的资源，因此，PFS 密钥交换算法比 RSA 密钥交换算法提供的安全性更高。但是，如果攻击者破坏了会话密钥，PFS 会阻止攻击者使用此密钥来解密相同客户端和服务器之间的任何其他会话，但 RSA 做不到这一点。
- 加密算法。密钥交换算法确定加密算法是 PFS 还是 RSA。
- 证书验证方法。RSA（而非 RSA 密钥交换算法）比椭圆曲线数字签名算法 (ECDSA) 消耗的资源更少，但 ECDSA 更安全。



密钥交换算法和证书验证方法的结合会影响吞吐量性能，如 *RSA* 和 *ECDSA* 基准测试中所示。*PFS* 的性能成本与 *PFS* 实现的高安全性相抵，但并不是所有类别的流量都需要 *PFS*。通过将 *RSA* 用于要解密，并检查其是否存在威胁但不敏感的流量的流量可以节省防火墙 *CPU* 周期。



© 2019 Palo Alto Networks, Inc.

- 平均事务大小。例如，若平均事务较小，解密时需要更多的处理能力。测量所有流量的平均事务大小，然后测量端口 443 的流量的平均交易大小（HTTPS 加密流量的默认端口），了解加密流量相对于总流量和平均交易大小进入防火墙的比例。消除异常大事务等异常值，以便对平均事务大小进行更真实的测量。
- 防火墙模型和资源。较新防火墙型号的处理能力优于较旧防火墙型号。

这些因素的组合决定了解密如何消耗防火墙处理的资源。为了更好地利用防火墙的资源，请理解您正在保护的数据的风险。如果防火墙资源有问题，对较高优先级的流量使用更强的解密，并使用更少的处理器密集型解密来解密和检查低优先级的流量，直到您可以增加可用的资源。例如，您可以使用 RSA（而非 ECDHE 和 ECDSA）用于不敏感或高优先级流量，并通过为高优先级的敏感流量使用基于 PFS 的解密来保留防火墙资源。（您仍在解密和检查较低优先级流量，但若使用安全性不如 PFS 的算法，则会消耗更少的计算资源。）关键是要了解不同流量类型的风险，并区别对待。

测量防火墙性能以了解当前可用资源，这有助于您了解是否需要更多的防火墙资源来解密想要解密的流量。测量防火墙性能还能在部署解密后为性能比较设置基准。

调整防火墙部署规模时，不仅应考虑您当前的需要，还应考虑您未来的需求。包含增加解密流量的空间，因为据 Gartner 预测，到 2019 年，80% 以上的企业网络流量将被加密，超过 50% 的新恶意软件活动将使用各种形式的加密。与您的 Palo Alto Networks 代表合作，充分利用他们在调整防火墙规模方面的经验，帮助您调整您的防火墙部署规模。

## 规划分阶段的优先部署

计划以受控方式逐个推出解密。请勿一次性推出整个解密部署。测试并确保解密按计划进行，用户了解您正在做什么以及您这样做的原因。以这种方式推出解密可在任何事超出预期时使故障排除更加容易，同时有助于用户进行调整，适应更改。

因为解密设置可能会改变利益相关者、员工以及承包商和合作伙伴等其他用户访问某些网站的能力，因此请对这些人员进行培训。用户应知道如何应对之前可以访问的网站变得不能访问等情况，也知道应向技术支持提供哪些信息。支持人员应了解推出的内容，推出的时间，以及为如何遭遇问题的用户提供帮助。向一般人群推出解密之前：

- 确定可帮助支持解密且能在全面推出期间可以帮助其他有问题员工的早期采用者。寻求部门经理的帮助，帮助他们了解解密流量的益处。
- 与了解解密流量重要性的早期采用者和其他员工一起在每个部分设置概念验证 (POC) 试验。向 POC 参与者介绍这些变化以及如何在遇到问题时联系技术支持。这样，解密 POC 就成为与技术支持一起针对如何支持解密并为支持一般推出提供最轻松方法进行 POC 的机会。POC 用户和技术支持之间的交互还允许您对策略进行微调，知道如何与用户进行沟通。

  通过 POC，您可以体验优先解密的内容，这样，当您在一般人群中进行分阶段解密时，您的 POC 经验可帮助您了解如何分阶段解密不同的 URL 类别。测量解密影响防火墙 CPU 和内存利用率的方式，以帮助了解防火墙规模是否合适或您是否需要升级。此外，POC 还可以揭示技术上（解密并阻挡其流量）无法解密且需要添加到解密排除列表的应用程序。

  设置 POC 时，还可以设置一个用户组，在一般推出之前对运行就绪情况和程序进行验证。
- 在一般推出之前对用户群进行培训，并在新用户加入公司时对其进行培训。因为部署有可能会影响用户先前访问但不安全的网站，因此，这是部署解密的关键阶段，这样，这些站点将再也不能访问。POC 经验有助于确定要通信的最重要的点。
- 解密阶段。您可以通过几种方式完成。您可以首先解密具有最高优先级的流量（例如，最有可能包含恶意流量的 URL 类别，例如游戏），然后在获取更多的经验后解密更多。或者，您可以采取更保守的方式解密不会对您的业务产生影响的 URL 类别（因此，即使出现问题，也不会出现影响业务的问题），例如，新闻递送。在所有情况下，分阶段解密的最佳做法是解密一些 URL 类别、考虑用户反馈、运行报告，确保解密按期进行，然后逐步解密更多的 URL 类别，并进行验证等。如果您出于技术原因或是因为您选择不对其进行解密而导致无法解密，则计划实施解密排除，从解密中排除站点。

  如果让用户选择停用 SSL 解密（用户看到一个响应页面，允许其停用解密并在无需前往站点的情况下结束会话，或是前往站点并同意对流量进行解密），则对用户就内容、查看原因和选项等进行培训。


© 2019 Palo Alto Networks, Inc.

- 创建实际可行的部署计划表，以便有时间对推出的各个阶段进行评估。



将防火墙放置在可以查看所有网络流量的位置，这样，加密流量不会无意访问您的网络，因为他们会绕过防火墙。



© 2019 Palo Alto Networks, Inc.

# 确定解密流量

解密策略规则允许您定义想要防火墙解密的流量，定义您出于私人原因或本地法规等原因选择从解密中排除的流量。

附加解密配置文件到每个解密策略规则，视配置文件启用证书检查、会话模式检查、故障检查、以及协议和算法检查。这些检查可防止有风险的连接，例如，不可信证书颁发者会话，弱协议、密码和算法，以及证书有问题的服务器。

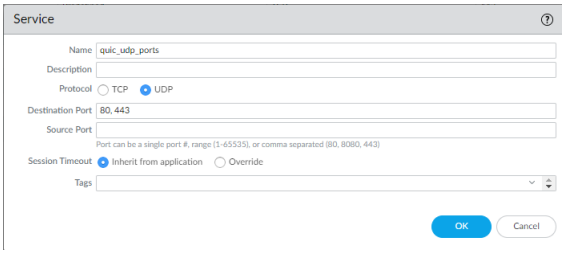
查看解密部署最佳实践列表，确保您了解推荐的最佳实践。

阻止已知危险的 URL 过滤类别，例如恶意软件、网络钓鱼、动态 DNS、未知、命令和控制、代理规避和匿名者、版权侵犯、极端主义、新注册域、灰色软件和寄放。如果因为业务原因必须允许任何这些类别，请解密，并对流量应用严格的安全配置文件。

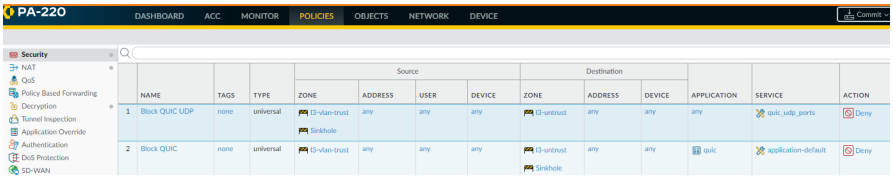
如果允许，应始终解密的 URL 类别：在线存储和备份、基于 Web 的电子邮件、Web 托管、个人网站和博客以及内容交付网络。

在安全策略中，阻止快速 *UDP* 互联网连接 *(QUIC)* 协议，除非出于业务原因希望允许加密浏览器流量。*Chrome* 和其他一些浏览器使用 *QUIC* 而非 *TLS* 建立会话，但 *QUIC* 使用的是防火墙无法解密的专有加密，因此潜在危险流量可能以加密流量的形式进入网络。阻止 *QUIC* 会强制浏览器退回到 *TLS*，使防火墙解密流量。

创建安全策略规则以阻止其 *UDP* 服务端口（*80* 和 *443*）上的 *QUIC*，并创建单独的规则以阻止 *QUIC* 应用程序。对于用于阻止 *UDP* 端口 *80* 和 *443* 的规则，请创建一个包括 *UDP* 端口 *80* 和 *443* 的服务（*Objects*（对象）> *Services*（服务））：




使用此服务指定用于阻止 *QUIC* 的 *UDP* 端口。在第二条规则中，阻止 *QUIC* 应用程序：




- 创建解密配置文件
- 创建解密策略规则

## 创建解密配置文件

通过解密配置文件，您可对解密流量及您选择从解密中排除的 SSL 流量进行检查。（如果服务器由于证书固定或其他原因从技术上破解 SSL 解密，则添加此服务器到解密排除列表。）根据您的需求创建解密配置文件以：


© 2019 Palo Alto Networks, Inc.

- 根据证书状态阻止会话，包含阻止具有过期证书、不可信颁发者、未知证书状态、证书状态检查超时和证书扩展的会话。
- 阻止具有不受支持版本和密码套件的会话，以及需要使用客户端身份验证的会话。
- 阻止以下情形下的会话，包括无法获得执行解密的资源或缺失硬件安全模块导致无法签署证书。
- 在 SSL 协议设置中定义允许用于 SSL 转发代理和 SSL 入站检查流量的协议版本和密钥交换、加密和身份验证算法。

请勿削弱应用于大多数站点的主要解密配置文件，以适应较弱站点。相反，应为需要支持，但不需要支持强密码和算法的站点创建一个或多个单独的解密配置文件。此外，您还可以为不同的 URL 类别创建不同的解密配置文件，以便对未包含敏感材料的流量的安全和性能进行微调，您应始终根据您的能力解密和检查所有流量。

在创建解密配置文件后，将其附加至解密策略规则，然后防火墙会在与解密策略规则匹配的流量上执行解密配置文件设置。

Palo Alto Networks 防火墙包含默认的解密配置文件，您可使用该文件实施为解密通信推荐的基础协议版本和密码套件。但是，最佳实践是启用更严格的解密控制，如SSL 转发代理解密配置文件、SSL 入站检查解密配置文件和 SSL 协议设置解密配置文件中所述。



避免支持弱协议或算法，因为这些协议或算法包含攻击者可以利用的已知漏洞。如果必须允许较弱协议或算法来支持使用带较弱协议的传统协议的关键合作伙伴或承包商，则为该例外创建单独的解密配置文件，并将其附加到仅将配置文件应用于相关流量的解密策略（例如，合作伙伴的源 *IP* 地址）。不得将弱协议用于所有流量。

STEP 1 | 创建新解密配置文件。

选择 **Objects**（对象）> **Decryption Profile**（解密配置文件），**Add**（添加）或修改解密配置文件规则，然后为该规则提供一个描述性的 **Name**（名称）。

STEP 2 | （可选）允许防火墙或所有 Panorama 设备组的所有虚拟系统 **Shared**（共享）配置文件规则。

STEP 3 | （仅解密镜像）启用以太网接口，以便防火墙使用其复制和转发解密通信。

与此任务分开，请执行配置解密端口镜像。请注意可能会禁止镜像的当地隐私法规，或是控制您可以镜像的流量类型。解密端口镜像要求解密端口镜像许可证。

STEP 4 | （可选）阻止和控制 SSL 隧道和/或入站流量：



尽管可以选择将解密配置文件用于解密流量，但最佳做法是始终将解密配置文件应用于策略规则，以保护您的网络，免遭加密威胁。您无法保护自己免受看不到的威胁。

选择 **SSL Decryption**（**SSL** 解密）：

- 选择 **SSL Forward Proxy**（**SSL** 转发代理）配置设置以验证证书，实施协议版本和密码套件，并对 SSL 解密流量进行失败检查。这些设置仅在该配置文件被加至配置为实施 SSL 转发代理解密的解密策略规则时有效。
- 选择 **SSL Inbound Inspection**（**SSL** 入站检查）配置设置，以实施协议版本和密码套件，并对 SSL 入站流量进行失败检查。这些设置仅在该配置文件被加至实施 SSL 入站检查的解密策略规则时有效。
- 选择 **SSL Protocol Settings**（**SSL** 协议设置）配置设置，从而对解密 SSL 流量上实施的最低和最高协议版本、密钥交换、加密及身份验证算法进行控制。这些设置仅在该配置文件被加至旨在实施 SSL Forward Proxy（SSL 转发代理）解密或 SSL Inbound Inspection（SSL 入站检查）的解密策略规则时有效。

STEP 5 | （可选）对您选择用于创建基于策略的解密排除的流量（如某个 URL 类别）进行阻止和控制。



© 2019 Palo Alto Networks, Inc.

尽管可以选择将解密配置文件用于您选择不进行解密的流量，但最佳做法是始终将解密配置文件应用于策略规则，以保护您的网络，免遭具有过期证书或不可信颁发者的会话。

选择 **No Decryption**（无解密）以配置不解密配置文件，并选中 **Block sessions with expired certificates**（阻止过期证书会话）和 **Block sessions with untrusted issuers**（阻止不可信颁发者会话）框，从而验证从解密中排除的流量的证书。创建仅用于您选择不进行加密的流量的基于策略的排除。如果服务器由于结束原因破解解密，则不得创建基于策略的排除，并将服务器添加到 SSL 解密排除列表（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））。

这些设置仅在该配置文件被加至旨在禁用某些流量解密的解密策略规则时有效。

STEP 6 | （可选）阻止和控制解密的 SSH 流量。

选择 **SSH Proxy**（**SSH** 代理）以配置 SSH 代理解密配置文件，并配置设置以在系统资源不可用于执行解密时实施受支持的协议版本并阻止会话。

这些设置仅在解密配置文件规则被加至解密 SSH 流量的解密策略规则时有效。

STEP 7 | 在创建解密策略规则时添加解密配置文件。

防火墙将解密配置文件应用于匹配解密策略规则的流量的配置文件设置，并予以设施。

STEP 8 | **Commit**（提交）配置。

## 创建解密策略规则

创建解密策略规则旨在确定通过防火墙解密的流量类型以及您希望防火墙采用的解密类型：SSL 转发代理、SSL 入站检查或 SSH 代理解密。您还可使用解密策略规则确定解密镜像。

STEP 1 | 添加新解密策略规则。

选择 **Policies**（策略）> **Decryption**（解密），**Add**（添加）新解密策略规则，并给策略规则一个描述性的 **Name**（名称）。

STEP 2 | 根据网络及 策略对象配置匹配流量的解密规则：

- **Firewall security zones**（防火墙安全区）— 选择 **Source**（源）和/或 **Destination**（目标）并根据 **Source Zone**（源区）和/或 **Destination Zone**（目标区）匹配流量。
- **IP addresses, address objects, and/or address groups**（**IP** 地址、地址对象和/或地址组）— 选择 **Source**（源）和/或 **Destination**（目标）并根据 **Source Address**（源地址）和/或 **Destination Address**（目标地址）匹配流量。或者，您还可以选择 **Negate**（求反）以排除源地址列表的解密。
- **Users**（用户）— 选择 **Source**（源），然后设置待解密流量的 **Source User**（源用户）。您可以解密特定用户或群组流量，或解密某些类型用户的流量，如未知用户或已登录用户（已连接 GlobalProtect 但未登录的用户）。
- **Ports and protocols**（端口和协议）— 选择 **Service/URL Category**（服务/**URL** 类别）设置基于服务匹配流量的规则。默认情况下，策略规则设置为解密 TCP 或 UDP 端口的 **Any**（任何）流量。您可以 **Add**（添加）服务或服务组，或者视需要将规则设置为 **application-default**，从而仅在应用程序默认端口匹配应用程序。

应用程序默认设置在创建基于策略的解密排除是非常有用。您可以排除对任何运行于其默认端口的应用程序的解密，同时继续解密在非标准端口上检测到的相同应用程序。

- **URLs and URL categories**（**URL** 和 **URL** 类别）— 选择 Service/URL Category（服务/URL 类别），并根据以下列表解密流量：


© 2019 Palo Alto Networks, Inc.

- 防火墙实施策略时检索的外部托管 URL 列表（请参阅 **Objects**（对象）> **External Dynamic Lists**（外部动态列表））。
- Palo Alto Networks 预定义 URL 类别，可轻松解密所有类别的允许流量。因为您可以按类别（而非单独地）排除敏感站点，因此此选项在您创建基于策略的解密排除时也非常有用。例如，虽然您可以创建自定义 URL 类别来对您不想要解密的网站进行分组，也可以根据预定义 Palo Alto Networks URL 类别排除对金融或医疗保健相关网站的解密。此外，您可以阻止有风险的 URL 类别，并创建舒适页面以通知站点被阻的原因，或是让用户停用 SSL 解密。

  您可以使用高风险和中等风险的预定义 URL 类别来创建可解密所有高风险和中等风险的 URL 流量的解密策略规则。将规则作为安全网置于规则库的底部（所有解密例外均必须置于此规则的前面，这样才不会解密敏感信息），确保您能解密并检测所有有风险的流量。但是，如果您允许访问的高风险或中等风险站点包含个人身份信息 (PII) 或其他您不想解密的敏感信息，请阻止这些站点，以免允许有风险的加密流量并避免隐私问题，或是创建无解密规则来处理敏感流量。
- 自定义 URL 类别（请参阅 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别））。例如，可以创建自定义 URL 类别以指定需要出于业务目的进行访问，但不支持安全协议和算法的一组站点，然后应用自定义解密配置文件，允许将更宽松的协议和算法仅用于这些站点（这样，您无需将大多数站点的解密配置文件降级，从而降低安全性）。

STEP 3 | 将规则设置为解密匹配流量或排除解密匹配流量。

选择 **Options**（选项）并设置策略规则 **Action**（操作）：

要解密匹配流量：

1. 将 **Action**（操作）设置为 **Decrypt**（解密）。
2. 设置防火墙对匹配流量执行的解密 **Type**（类型）：
   - SSL 转发代理
   - SSL 入站检查。如果您想要启用 SSL 入站检查，同样选择 SSL 入站流量的内部目标服务器 **Certificate**（证书）。
   - SSH 代理

要排除解密匹配流量：

将 **Action**（操作）设置为 **No Decrypt**（不解密）。

STEP 4 | （可选）选择 **Decryption Profile**（解密配置文件）以对与策略规则匹配的流量执行其他检查。



尽管可以选择将解密配置文件用于解密流量，但最佳做法是始终将解密配置文件应用于策略规则，以保护您的网络，免遭加密威胁。您无法保护自己免受看不到的威胁。

例如，将解密配置文件附加到策略规则，确保服务器证书的有效性，并使用不受支持协议或密码阻止会话。要创建解密配置文件，请选择 **Objects**（对象）> **Decryption Profile**（解密配置文件）。

1. 创建解密策略规则，或打开现有规则进行修改。
2. 选择 **Options**（选项），然后选择 **Decryption Profile**（解密配置文件），以全面阻止和控制符合该规则的流量。

   防火墙将该配置文件规则设置按策略规则 **Action**（操作）（解密或不解密）及策略规则 **Type**（类型）（SSL 转发代理、SSL 入站检查或 SSH 代理）应用于匹配流量。这样，您可以使用适用于不同类型流量和用户的不同类型的解密策略规则的不同解密配置文件。
3. 单击 **OK**（确定）。

STEP 5 | 配置解密日志记录（配置是否需要同时记录成功的和失败的 TLS 握手，然后配置解密日志转发）。

STEP 6 | 单击 **OK**（确定）以保存策略。



© 2019 Palo Alto Networks, Inc.

STEP 7 | 选择下一步以完全启用防火墙解密流量...

- 配置 SSL 转发代理
- 配置 SSL 入站检查
- 配置 SSH 代理
- 为您选择不想解密的的流量创建基于策略的解密排除，并将出于固定证书或相互身份验证等技术原因而无法解密的站点添加到 SSL 解密排除列表。


© 2019 Palo Alto Networks, Inc.

# 配置 SSL 转发代理

要启用防火墙进行 SSL 转发代理解密，您必须设置所需证书以让防火墙作为受信第三方（代理）参与客户端与服务器之间的会话。防火墙可使用企业证书颁发机构 (CA) 签署的证书或防火墙上生成的自签名证书作为转发信任证书，从而验证与客户端之间的 SSL 会话。

- （推荐的最佳实践）企业 **CA** 签名证书 —企业 CA 可签发签名证书，防火墙可用来为需要 SSL 解密的站点签名证书。在防火墙信任签署目标服务器证书的 CA 后，防火墙便可向用户端发送由企业 CA 签署的目标服务器证书副本。这是最佳实践，因为通常所有网络设备都已信任企业 CA（通常已在设备的 CA 信任存储中安装就绪），因此，您无需在端点上部署证书，部署过程也更加顺利。
- 自签名证书 — 防火墙可以充当 CA，并生成自签名证书，防火墙可用来为需要 SSL 解密的站点签名证书。防火墙可以签署服务器证书副本提供给客户端，并建立 SSL 会话。此方法要求您必须在所有网络设备上安装自签名证书，这样，这些设备才能识别防火墙的自签名证书。因为防火墙必须部署到所有设备，因此，相较于大型部署而言，此方法更适用于小型部署和概念验证 (POC) 试验。

此外，如果服务器证书由防火墙不信任的 CA 签署，则为防火墙设置向用户端提供的转发不信任证书。这可确保当尝试使用不受信任的证书访问站点时，系统为客户端提供证书警告。



无论您是从企业根 *CA* 生成转发信任证书，还是使用防火墙上生成的自签名证书，均应为每个防火墙生成从属转发信任 *CA*。使用单个从属 *CA* 比较灵活，您可以在设备（或设备组）退役时吊销一个证书，不会对其余部署产生影响，同时也能减少在必须要吊销证书的情况下所产生的任何影响。因为用户看到的 *CA* 错误消息包含有关流量正在遍历的防火墙信息，因此，每个防火墙上的单个转发信任 *CA* 也有助于解决问题。如果在每个防火墙上使用相同的转发信任 *CA*，则会失去该信息的粒度。

SSL 转发代理解密所需的转发信任和转发不信任证书设置结束后，创建一个解密策略规则定义您想要防火墙进行解密的流量，然后创建一个解密配置文件将 SSL 控制和检查用于此流量。解密策略将与规则匹配的 SSL 隧道流量解密为明文流量。防火墙根据解密策略附带的解密配置文件和防火墙安全策略阻止并限制流量。在退出防火墙时，防火墙会对流量进行重新加密。

STEP 1 | 确保将相应的接口配置为 Virtual Wire、第 2 层或第 3 层接口。

查看 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）选项卡上的配置接口。**Interface Type**（接口类型）列显示是将接口配置为 **Virtual Wire**（虚拟线路）或 **Layer 2**（第 **2** 层）还是 **Layer 3**（第 **3** 层）接口。可以选择接口以修改其配置，包括接口的类型。

STEP 2 | 在服务器证书由受信 CA 签署后，为防火墙配置提供给用户端的转发信任证书。您可以使用企业 CA 签发证书或自签名证书作为转发信任证书。

（推荐的最佳实践）使用企业 CA 签署证书作为转发信任证书。在每个防火墙上创建唯一命名的转发信任证书。

1. 生成企业 CA 的证书签名请求 (CSR) 以进行签名和验证。
    1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书），然后单击 **Generate**（生成）。
    2. 输入 **Certificate Name**（证书名称）。为每个防火墙使用唯一名称。
    3. 在 **Signed By**（签名者）下拉列表中，选择 **External Authority (CSR)**（外部颁发机构 **(CSR)**）。
    4. （可选）如果企业 CA 需要，则添加 **Certificate Attributes**（证书属性）以进一步确定防火墙的详细信息，如国家/地区或部门。
    5. 单击 **Generate**（生成）以保存 CSR。挂起证书现在显示在 **Device Certificates**（设备证书）选项卡上。
2. 导出 CSR：
    1. 选择在 **Device Certificates**（设备证书）选项卡上显示的挂起证书。



© 2019 Palo Alto Networks, Inc.

2. 单击 **Export**（导出）以下载和保存证书文件。

   取消选择 *Export private key*（导出私钥）以确保私钥在防火墙上仍保持安全。

3. 单击 **OK**（确定）。

3. 将证书文件提供给企业 CA。从企业 CA 处收到企业 CA 签名证书后，保存企业 CA 签名证书以便导入防火墙。
4. 将企业 CA 签署的证书导入防火墙：
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书），然后单击 **Import**（导入）。
   2. 准确输入暂挂的 **Certificate Name**（证书名称）。输入的 **Certificate Name**（证书名称）必须与挂起证书名称完全匹配才能激活挂起证书。
   3. 选择从企业 CA 收到的签名 **Certificate File**（证书文件）。
   4. 单击 **OK**（确定）。证书将显示为有效，且已选中“密钥”和“CA”复选框。
5. 选择验证的证书，以启用该证书作为 **Forward Trust Certificate**（转发信任证书）以用于 SSL 转发代理解密。
6. 单击 **OK**（确定）以保存企业 CA 签发的转发信任证书。

将自签名证书用作转发信任证书：

1. 创建自签名根 CA 证书。
2. 单击自签名根 CA 证书（**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书））以打开 **Certificate information**（证书信息），然后单击 **Trusted Root CA**（可信根 **CA**）复选框。
3. 单击 **OK**（确定）。
4. 为每个防火墙生成新的从属 CA 证书：
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
   2. 单击窗口底部的 **Generate**（生成）。
   3. 输入 **Certificate Name**（证书名称）。
   4. 输入 **Common Name**（公用名），如 192.168.2.1。这应该是将出现中证书中的 IP 地址或 FQDN。在本例中，我们使用信任接口的 IP 地址。避免在此字段中使用空格。
   5. 在 **Signed By**（签名者）字段中，选择您创建的自签名根 CA 证书。
   6. 单击 **Certificate Authority**（证书颁发机构）复选框以启用防火墙签发证书。选中此复选框将在防火墙上创建将被导入客户端浏览器的证书授权机构 (CA)，以便客户端信任防火墙作为 CA。
   7. **Generate**（生成）证书。
5. 单击新证书进行修改，然后单击 **Forward Trust Certificate**（转发信任证书）复选框，将证书配置为转发信任证书。
6. 单击 **OK**（确定）以保存自签名转发信任证书。
7. 要在每个防火墙上生成唯一的从属 CA 证书，重复此步骤。

STEP 3 | 分发转发信任证书至用户端系统的证书存储区。

如果您在将企业 CA 签署的证书用作 SSL 转发代理解密的转发信任证书，且用户端系统已将企业 CA 安装至本地受信根 CA 列表，则可以跳过该步骤。（因为企业可信根 CA 已对您在防火墙上生成的从属 CA 证书进行签名，因此客户端系统将其视为可信。）



如果您未在用户端系统安装转发信任证书，用户将会看到他们访问的每个 *SSL* 站点的证书警告。

在配置为 GlobalProtect 门户的防火墙上：



© 2019 Palo Alto Networks, Inc.

该选项支持 *Windows* 及 *Mac* 用户端 *OS* 版本，同时要求用户端系统安装 *GlobalProtect agent 3.0.0* 或更高版本。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户），然后选择现有门户配置或 **Add**（添加）新配置。
2. 选择 **Agent**（代理），然后选择现有代理配置或 **Add**（添加）新配置。
3. **Add**（添加）自签名的防火墙可信根 CA 证书到可信根 CA 部分。GlobalProtect 将防火墙的可信根 CA 证书分发给客户端系统后，因为客户端信任防火墙的根 CA 证书，因此，客户端系统将信任防火墙的从属 CA 证书。
4. **Install in Local Root Certificate Store**（安装于本地根证书存储区）以便 GlobalProtect 门户自动配发证书并将其安装于 GlobalProtect 用户端系统的证书存储区。
5. 双击 **OK**（确定）。

无 GlobalProtect：

导出防火墙可信根 CA 证书，这样，可以将其导入客户端系统。突出显示证书，然后单击窗口底部的 **Export**（导出）。选择 PEM 格式。

请勿选择 *Export private key*（导出私钥）复选框#私钥应保留在防火墙上，不应导出到客户端系统。

将防火墙的可信根 CA 证书导入到客户端系统上的浏览器上的可信根 CA 列表，以便客户端信任它。在将证书导入客户端浏览器时，确保已将证书添加到受信任的根证书颁发机构证书库。在 Windows 系统中，默认的导入位置为个人证书存储。还可以通过使用集中式部署选项简化此过程，如 Active Directory 组策略对象 (GPO)。

STEP 4 | 配置转发不可信证书（为所有防火墙使用相同的转发不可信证书）。

1. 单击证书页面底部的 **Generate**（生成）。
2. 输入 **Certificate Name**（证书名称），例如 my-ssl-fwd-untrust。
3. 设置 **Common Name**（常见名称），例如 192.168.2.1。将 **Signed By**（签名者）留空。
4. 单击 **Certificate Authority**（证书颁发机构）复选框以启用防火墙签发证书。
5. 单击 **Generate**（生成）以生成证书。
6. 单击 **OK**（确定）以保存。
7. 单击新证书 my-ssl-fwd-untrust 以进行修改并启用 **Forward Untrust Certificate**（转发不可信证书）选项。

   不得将转发不可信证书导出到网络设备上的证书信任列表中。不得在客户端系统上安装转发不可信证书。因为在信任列表中安装不可信证书将会导致防火墙无法信任设备信任网站，因此，这一点至关重要。此外，用户将看不到不可信站点的证书警告，这样，就不知道这些站点是不受信的，可能会访问这些站点，从而导致网络遭受威胁。
8. 单击 **OK**（确定）以保存。

STEP 5 | （可选）配置 SSL 转发代理服务器证书的密钥大小，以便防火墙向客户端显示。默认情况下，防火墙根据目标服务器证书的密钥大小，确定要使用的密钥大小。

STEP 6 | 创建解密策略规则以定义防火墙进行解密的流量，并创建解密配置文件以将 SSL 控制用于流量。

尽管解密配置文件为可选项，但最佳做法是在每个解密策略规则中包含一个解密配置文件，以阻止脆弱且易受攻击的协议和算法允许您网络上的可疑流量。

1. 选择 **Policies**（策略）> **Decryption**（解密），添加或修改现有规则，然后确定待解密流量。



© 2019 Palo Alto Networks, Inc.

2. 选择 **Options**（选项）并：
   - 将规则 **Action**（操作）设置为 **Decrypt**（解密）匹配流量。
   - 将规则 **Type**（类型）设置为 **SSL Forward Proxy**（**SSL** 转发代理）。
   - （可选，但属最佳做法）配置或选择现有 **Decryption Profile**（解密配置文件）以全面阻挡并控制已解密流量（例如，创建解密配置文件来执行证书检查并实施强大的密码套件和协议版本）。
3. 单击 **OK**（确定）以保存。

STEP 7 | 启用防火墙转发解密后的 SSL 通信进行 WildFire 分析。



此选项需要一个活动的 *WildFire* 许可证，也是 WildFire 最佳实践。

STEP 8 | **Commit**（提交）配置。

STEP 9 | 选择您的下一步：

- 让用户选择停用 SSL 解密。
- 配置解密排除以禁用特定类型流量的解密。



© 2019 Palo Alto Networks, Inc.

# 配置 SSL 入站检查

使用 SSL 入站检查解密并检查传往网络服务器的入站 SSL 流量（如防火墙加载有服务器证书，则可对所有服务器进行 SSL 入站检查）。在启用 SSL 入站检查解密策略后，防火墙将策略识别到的所有 SSL 流量解密为明文流量并进行检查。防火墙根据策略附带的解密配置文件和应用于流量的安全策略阻止、限制或允许流量，包括任何已配置的防病毒配置文件、漏洞防护配置文件、防间谍配置文件、URL 筛选配置文件和文件阻止配置文件。最佳做法是启用防火墙转发解密后的 SSL 通信进行 WildFire 分析并生成签名。

配置 SSL 入站检查，包括在防火墙上安装目标服务器的证书，创建 SSL 入站检查解密策略，以及将解密配置文件应用于策略。

*SSL* 入站检查不支持身份验证门户重定向。若要使用身份验证门户重定向和解密，必须使用SSL 转发代理。

STEP 1 | 确保将相应的接口配置为 Tap、Virtual Wire、第 2 层或第 3 层接口。

如果协商密码包括 *PFS* 密钥交换算法（*DHE* 和 *ECDHE*），则不能使用 *Tap* 模式接口进行 *SSL* 入站检查。

查看 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）选项卡上的配置接口。**Interface Type**（接口类型）列显示是将接口配置为 **Virtual Wire**（虚拟线路）或 **Layer 2**（第 2 层）还是 **Layer 3**（第 3 层）接口。可以选择接口以修改其配置，包括接口类型。

STEP 2 | 确保已在防火墙上安装目标服务器的证书。

在 Web 界面上，选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）可查看在防火墙上安装的证书。

要将目标服务器证书导入防火墙：

1. 在 **Device Certificates**（设备证书）选项卡上，选择 **Import**（导入）。
2. 输入描述性 **Certificate Name**（证书名称）。
3. 浏览并选择目标服务器的 **Certificate File**（证书文件）。
4. 单击 **OK**（确定）。

STEP 3 | 创建解密策略规则以定义防火墙进行解密的流量，并创建解密配置文件以将 SSL 控制用于流量。

尽管解密配置文件为可选项，但最佳做法是在每个解密策略规则中包含一个解密配置文件，以阻止脆弱且易受攻击的协议和算法允许您网络上的可疑流量。

1. 选择 **Policies**（策略）> **Decryption**（解密），**Add**（添加）或修改现有规则，然后确定待解密流量。
2. 选择 **Options**（选项）并：
   - 将规则 **Action**（操作）设置为 **Decrypt**（解密）匹配流量。
   - 将规则**Type**（类型）设置为 **SSL Inbound Inspection**（**SSL** 入站管理）。
   - 选择内部服务器的 **Certificate**（证书），该服务器是入站 SSL 流量的目的地。
   - （可选，但属最佳做法）配置或选择现有 **Decryption Profile**（解密配置文件）以全面阻止和控制加密流量（例如，创建解密配置文件来终止不受支持算法且带有不受支持密码套件的会话）。

     配置用于 *SSL* 入站检查流量的#unique_568时，为具有不同安全功能的服务器创建单独的配置文件。例如，如果某一组的服务器仅支持 *RSA*，则 *SSL* 协议设置仅需支



© 2019 Palo Alto Networks, Inc.

持 *RSA* 即可。但是，支持 *PFS* 的 *SSL* 协议设置应支持 *PFS*。配置受服务器支持的最高安全水平的 *SSL* 协议设置，但对性能进行检查，确保防火墙资源可以处理高安全协议和算法所需的高处理负载。

3. 单击 **OK**（确定）以保存。

STEP 4 | 启用防火墙转发解密后的 SSL 通信进行 WildFire 分析。



此选项需要一个活动的 *WildFire* 许可证，也是 WildFire 最佳实践。

STEP 5 | **Commit**（提交）配置。

STEP 6 | 选择您的下一步...

- 让用户选择停用 SSL 解密。
- 配置解密排除以禁用特定类型流量的解密。



© 2019 Palo Alto Networks, Inc.

# 配置 SSH 代理

配置 SSH 代理不需要使用证书和密钥解密在防火墙启动时自动生成的 SSH 会话。启用 SSH 解密后，防火墙会解密 SSH 流量，并根据您的解密策略和解密配置文件设置阻止和/或限制 SSH 流量。在退出防火墙时会对流量进行重新加密。

STEP 1 | 确保将相应的接口配置为 Virtual Wire、第 2 层或第 3 层接口。只能在虚拟线路、第 2 层或第 3 层接口上执行解密。

查看 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）选项卡上的配置接口。**Interface Type**（接口类型）列显示是将接口配置为 **Virtual Wire**（虚拟线路）或 **Layer 2**（第 2 层）还是 **Layer 3**（第 3 层）接口。可以选择接口以修改其配置，包括接口的类型。

STEP 2 | 创建解密策略规则以定义防火墙进行解密的流量，并创建解密配置文件以将检查应用于 SSH 流量。



尽管解密配置文件为可选项，但最佳做法是在每个解密策略规则中包含一个解密配置文件，以阻止脆弱且易受攻击的协议和算法允许您网络上的可疑流量。

1. 选择 **Policies**（策略）> **Decryption**（解密），添加或修改现有规则，然后确定待解密流量。
2. 选择 **Options**（选项）并：
   - 将规则 **Action**（操作）设置为 **Decrypt**（解密）匹配流量。
   - 将规则**Type**（类型）设置为 **SSH Proxy**（SSH 代理）。
   - （可选项，但属最佳做法）配置或选择现有 **Decryption Profile**（解密配置文件）以全面阻止和控制加密流量（例如，创建解密配置文件来终止不受支持版本且带有不受支持算法的会话）。
3. 单击 **OK**（确定）以保存。

STEP 3 | **Commit**（提交）配置。

STEP 4 | （可选）继续解密排除以禁用特定类型流量的解密。



© 2019 Palo Alto Networks, Inc.

# 为未加密流量配置服务器证书验证

因为流量具有私人性、敏感性，或是考虑到当地法律法规的原因，可以为您选择不进行解密的流量创建不解密策略。例如，您可以选择不解密某些管理人员的流量，或是金融用户和包含个人信息的财务服务器之间的流量。（请勿排除不能解密的流量，因为网站可能会因固定证书或策略要求的相互身份验证等技术原因中断解密。相反，应将主机名添加到解密排除列表。）

但是，仅仅因为您没有解密流量，并不代表可以允许和放任网络上所有和任何未解密的流量。最佳做法是将不解密配置文件应用至未解密流量，从而阻止过期证书会话和不可信颁发者。

STEP 1 | 创建解密策略规则，标识未解密流量，创建解密配置文件，阻止错误会话。

1. 选择 **Policies**（策略）> **Decryption**（解密），添加或修改现有规则，以标识未解密流量。
2. 选择 **Options**（选项）并：
   - 设置 **Action**（操作）规则为 **No Decrypt**（无解密），这样，防火墙就不会解密与规则匹配的流量。
   - 因为流量未解密，请忽略规则 **Type**（类型）。
   - （可选，但属最佳做法）配置或选择现有未解密流量的解密配置文件，以阻止过期证书回话和不可信证书颁发者。



切勿为未解密的 *TLSv1.3* 流量的解密策略附加“不解密”配置文件，因为防火墙无法读取加密证书信息，从而无法执行证书检查。但是，应为未解密的 *TLSv1.3* 流量创建解密策略，因为除非此解密策略可以控制该流量，否则，将不会记录未解密的流量。

STEP 2 | **Commit**（提交）配置。

STEP 3 | 选择您的下一步：

- 让用户选择停用 SSL 解密。
- 配置解密排除以禁用特定类型流量的解密。



© 2019 Palo Alto Networks, Inc.

# 解密排除

您可以从解密中排除两种类型的流量：

- 流量由于技术原因终止解密，如通过使用固定证书、不完整的证书链、不受支持的密码或相互身份验证（出于阻止流量的原因而尝试解密流量）。Palo Alto Networks 提供预定义 SSL 解密排除列表（**Device**（设备）> **Certificate management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除）），默认情况下，将装有已知技术上终止解密的应用程序和服务的主机从 SSL 解密中排除。如果遇到技术上终止解密且不在 SSL 解密排除列表中的站点，可以按服务器主机名将其手动添加至列表。防火墙阻止应用程序和服务在技术上无法解密的站点，除非您已将这些站点添加到 SSL 解密排除列表。

  如果解密配置文件允许 **Unsupported Modes**（不受支持的模式）（具有客户端身份验证、不受支持的版本、或不受支持的密码套件的会话），防火墙会自动将使用允许的不受支持模式的服务器和应用程序添加到本地 SSL 解密排除缓存中（ **Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除）> **Show Local Exclusion Cache**（显示本地排除缓存））。阻止不受支持的模式时，您可以提高安全性，但也会阻止与使用这些模式的应用程序进行通信。
- 出于业务、法规、个人或其他原因您选择不进行解密的流量，例如，金融服务、健康医疗或政府流量。您可以根据源、目标、URL 类别和服务排除流量。

您可以使用星号 (*) 作为通配符来创建用于多个与域相关联的主机名的解密排除。星号与插入符号 (^) 在用于 URL 类别异常时的行为方式相同 — 每个星号控制主机名中一个变量子域（标签）。这样，您既可以创建非常具体的排除，也可以创建非常笼统的排除。例如：

- mail.*.com 与 mail.company.com 匹配，但不与 mail.company.sso.com 匹配。
- *.company.com 与 tools.company.com 匹配，但不与 eng.tools.company.com 匹配。
- *.*.company.com 与 eng.tools.company.com 匹配，但不与 eng.company.com 匹配。
- *.*.*.company.com 与 corp.exec.mail.company.com 匹配，但不与 corp.mail.company.com 匹配。
- mail.google.* 与 mail.google.com 匹配，但不与 mail.google.uk.com 匹配。
- mail.google.*.* 与 mail.google.co.uk 匹配，但不与 mail.google.com 匹配。

例如，要使用通配符从解密中排除 video-stats.video.google.com，而不是从解密中排除 video.google.com，请排除 *.*.google.com。



不管主机名之前的星号通配符数量是多少（主机名之前没有非通配符标签），主机名必须与条目匹配。例如，**.google.com*、**.*.google.com* 和 **.*.*.google.com* 全部都与 *google.com* 匹配。但是，**.dev.*.google.com* 不与 *google.com* 匹配，原因在于有一个标签 *(dev)* 不是通配符。

要想提高流量的可见性，并尽可能地减少攻击面，除非您必须这样做，否则请勿执行解密例外。

- Palo Alto Networks 预定义解密排除
- 出于技术原因从解密中排除服务器
- 本地解密排除缓存
- 创建基于策略的解密排除

## Palo Alto Networks 预定义解密排除

防火墙提供预定义 SSL 解密排除列表，以便排除由于固定证书和相互身份验证等技术原因而对解密进行破解的解密常用站点。作为应用程序和威胁内容更新（或者应用程序内容更新，如果没有威胁阻止许可证时）的一部分，预定义解密排除默认启动，Palo Alto Networks 会向防火墙提供新的和更新过的预定义解密排除。防火墙不会解密与预定义排除匹配的流量，并允许基于管理此流量的安全策略的加密流量。但是，防火墙无法检测加密流量，会对其执行安全策略。

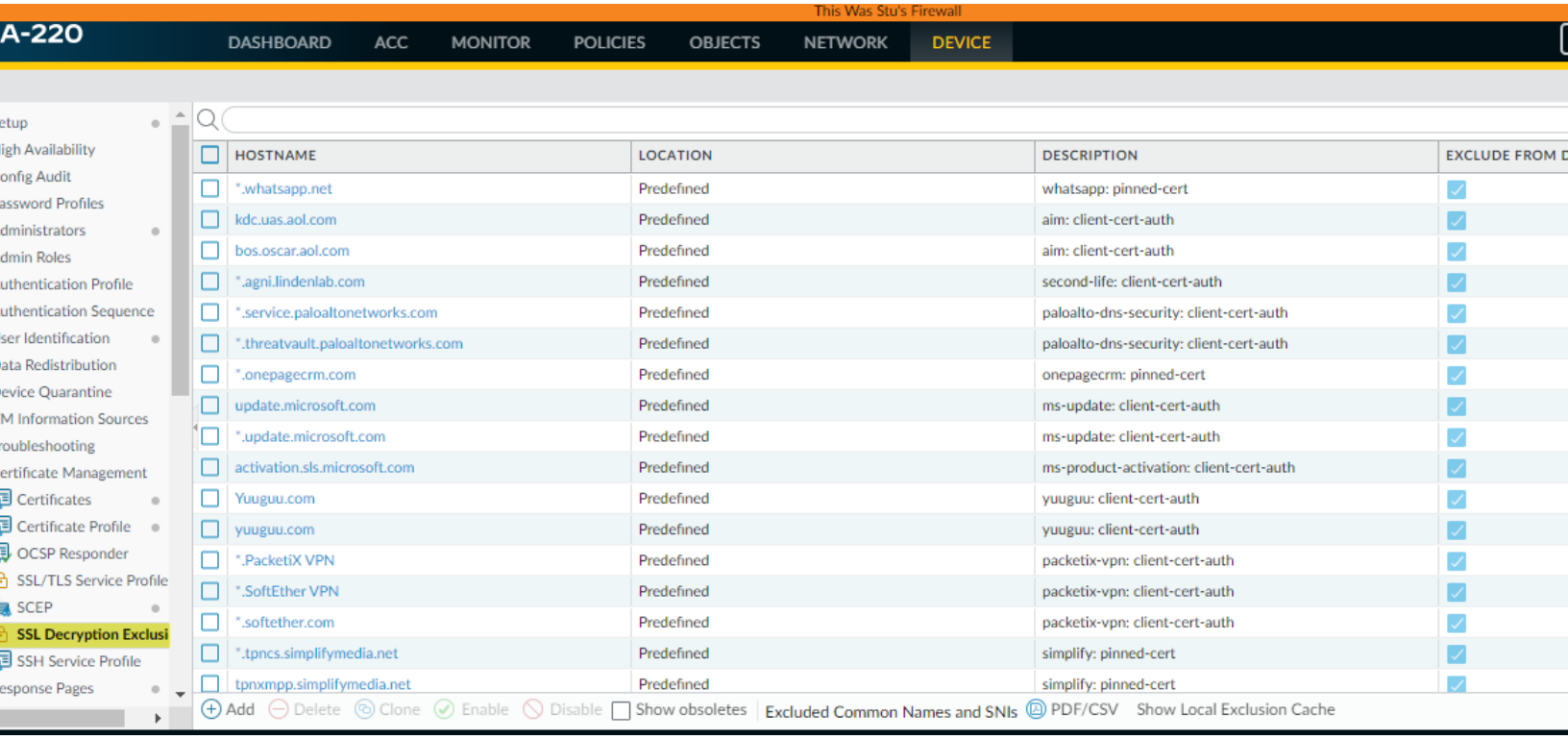


© 2019 Palo Alto Networks, Inc.

*SSL* 解密排除列表不能用于出于法律、法规、业务、隐私或其他意志原因选择不进行解密的站点，而仅用于技术上无法解密的站点（解密这些站点阻止其流量）。对于您选择不进行解密的流量，如 *IP* 地址、用户、*URL* 类别、服务，甚至是整个区域），创建基于策略的解密排除。

因为 SSL 解密排除列表上站点流量仍是加密的，因此，防火墙不会对其进行检测，或是提供进一步的安全措施。您可以禁用预定义排除。例如，您可以选择禁用预定义排除以实施严格的安全策略。此安全策略仅允许防火墙能够进行检查且防火墙可以对其实施安全策略的应用程序和服务。但是，如果 SSL 解密排除列表未启用其应用程序和服务可从技术上破解解密的站点，则防火墙将阻止此站点。

您可以直接在防火墙上查看和管理所有 Palo Alto Networks 预定义 SSL 解密排除（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusions**（**SSL** 解密排除））。




**Hostname**（主机名）显示托管能从技术上进行破解的应用程序或服务的主机名。如果主机不在预定义列表中，则还可以 **Add**（添加）主机以出于技术原因从解密中排除服务器。

**Description**（说明）显示防火墙不能对站点流量进行解密的原因，例如，**pinned-cert**（固定证书）或 **client-cert-auth**（客户端证书验证）。

当预定义 SSL 解密排除变得过时时，防火墙会自动从列表中删除已启用的预定义 SSL 解密排除（当应用程序变得支持解密时，防火墙删除由于之前解密而导致破解的应用程序）。**Show Obsoletes**（显示过时）检查列表上是否存在任何禁用的预定义排除，且这些排除是否不再需要。防火墙不会自动从列表中删除禁用的预定义解密排除，但您可以选择并 **Delete**（删除）过时条目。

您可以选择主机名的复选框，然后单击 **Disable**（禁用）以便从列表中删除预定义站点。SSL 解密排除列表仅用于出于技术原因破解解密的站点，请勿将其用于您选择不进行解密的站点。

## 出于技术原因从解密中排除服务器

如果解密从技术上能将重要的应用程序或服务破解（解密对齐进行阻挡的流量），则可以将托管到应用程序或服务的站点主机名添加到 Palo Alto Networks 预定义 SSL 解密排除列表，以创建自定义解密例外。因为流量仍是加密的，所以，防火墙不会对 SSL 解密排除列表允许的流量上的安全策略进行解密、检查和实施。因


© 2019 Palo Alto Networks, Inc.

此，确保添加到列表的站点确实是包含业务所需的应用程序或服务的站点。例如，某些业务关键型内部自定义应用程序可能会无法解密，您可以将其添加到列表，这样，防火墙便会允许加密的自定义应用程序流量。

*SSL* 解密排除列表不能用于出于法律、法规、业务、隐私或其他意志原因选择不进行解密的站点，而仅用于技术上无法解密的站点。对于您选择不进行解密的流量（*IP* 地址、用户、*URL* 类别、服务，甚至是整个区域），创建基于策略的解密排除。

站点在技术上无法解密的原因包括固定证书、客户端身份验证、不完整的证书链以及不受支持密码。对于 HTTP 公钥固定 (HPKP)，只要您在客户端上安装了企业 CA 证书（或证书链），使用 HPKP 的大部分浏览器将允许转发代理解密。

如果将站点从解密排除的技术原因是不完整的证书链，则下一代防火墙不会像浏览器一样自动修复链。如果需要添加站点到 *SSL* 解密排除列表，请手动查看此站点，确保这是一个合法的业务站点，然后下载丢失的子 *CA* 证书，并在防火墙上加载和部署。

将服务器添加到 SSL 解密排除列表后，防火墙将对您用于定义解密排除的服务器主机名与服务器提供的证书的公用名 (CN) 进行比较。如果单个服务器采用不同的证书托管多个网站，则防火墙将主机名与客户端提供的服务器名称指示 (SNI) 进行比较，以指示想要连接的服务器。

STEP 1 | 选择 **Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusions**（**SSL** 解密排除）。

STEP 2 | **Add**（添加）新的解密排除，或选择现有的自定义条目进行修改。

STEP 3 | 输入要排除解密的网站或应用程序的 **hostname**（主机名）。

主机名区分大小写。

您可以使用通配符排除多个与域关联的主机名。防火墙将会从解密中排除服务器提供与域匹配的 CN 的所有会话。

确保每个自定义条目的主机名字段的唯一性。如果预定义的排除匹配自定义条目，则自定义条目优先。

STEP 4 | （可选）选择 **Shared**（共享）可在多个虚拟系统防火墙中的所有虚拟系统之间共享排除。

STEP 5 | **Exclude**（排除）解密应用程序。或者，如果要修改现有的解密排除，您可以清除此复选框来开始解密先前从解密中排除的条目。

STEP 6 | 单击 **OK**（确定）以保存新的排除条目。

## 本地解密排除缓存

防火墙可将服务器添加到“本地解密排除”缓存（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除）> **Show Local Exclusion Cache**（显示本地排除缓存）），并在流量出于固定证书或不受支持证书等技术原因破解解密时，自动在 12 小时内将流量从解密中排除。一旦解密配置文件允许不受支持模式（客户端身份验证会话、不受支持版本或不受支持密码套件），且允许的流量使用不受支持的模式时，设备会自动将服务器添加到本地排除缓存，并绕过解密。防火墙不会对本地解密排除缓存允许的流量进行解密、检测以及执行安全策略，因为流量仍保持加密状态。务必确保您（通过应用允许不受支持模式的解密配置文件）从解密中排除的站点是具有业务所需应用程序或服务的站点。

阻止不受支持模式后，与使用这些模式来提高安全性的应用程序之间的通信也会被阻止。将应用程序从解密中排除的常见原因是客户端身份验证，因此，最佳做法是阻止不受支持版本和不受支持密码，允许解密配置文件中的客户端身份验证。如果解密配置文件允许客户端身份验证，那么，一旦客户端启动与要求客户端进



© 2019 Palo Alto Networks, Inc.

行身份验证的服务器之间的会话时，防火墙将应用程序和服务器添加到本地排除缓存，并允许流量，而不是因为防火墙不能进行解密而阻止该流量。



如果允许来自使用客户端身份验证的站点以及不属于 SSL 解密排除列表中预定义站点的流量，请创建一个允许客户端身份验证会话的解密配置文件。将此配置文件添加到仅用于包含应用程序的服务器的解密策略规则。为了进一步提高安全性，您可能需要多重因素身份验证来完成用户登录过程。或者，您可以将站点添加到 *SSL* 解密排除列表，以在不使用显式解密策略的情况下跳过解密。

防火墙基于用于控制应用程序流量的解密策略和配置文件添加 SSL 解密排除缓存条目。如果不阻止解密配置文件中的 **Unsupported Mode Checks**（不受支持模式检查），一旦出现下列情况，防火墙将添加条目到“本地 SSL 解密排除”缓存：

- 客户端仅支持 TLSv1.2，服务器仅支持 TLSv1.3。在本地缓存中，显示的排除原因是 SSL_UNSUPPORTED。
- 客户端支持 TLSv1.3 和 TLSv1.2，服务器仅支持 TLSv1.2。在这种情况下，**Reason**（原因）列显示 TLS13_UNSUPPORTED。

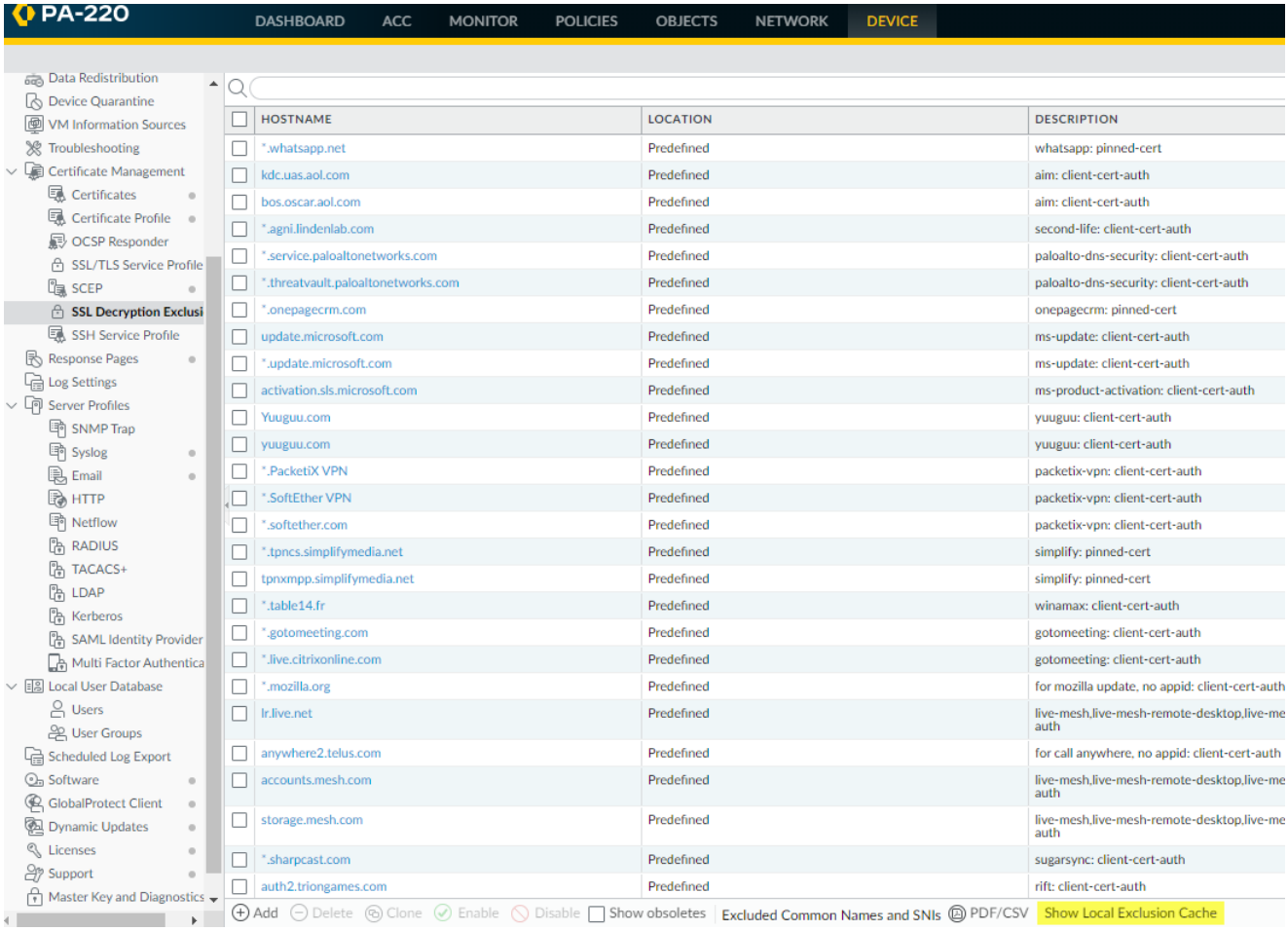
  

  一旦添加服务器到“本地 *SSL* 解密排除”缓存的 *Reason*（原因）是 *TLS13_UNSUPPORTED*，防火墙将协议降级到 *TLSv1.2*，且防火墙解密并检测流量。
- 客户端通告服务器不支持的特定密码。
- 客户端通告服务器不支持的特定曲线。

本地缓存中最多可包括 1,024 个条目。您不能将本地排除项手动添加到“本地 SSL 解密排除”缓存（但是，您可以将解密排除项手动添加到“SSL 解密排除”列表）。

要查看“本地 SSL 解密排除”缓存，您必须具有超级用户或证书管理管理员权限。若要查看该缓存，请导航至 **Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除），然后单击屏幕底部旁边的 **Show Local Exclusion Cache**（显示本地排除缓存）。本地排除缓存显示应用程序、服务器、包括在缓存中的原因、控制流量的解密配置文件以及每个条目的更多信息。您可以手动选择并删除本地缓存中的条目。


© 2019 Palo Alto Networks, Inc.




您还可以使用 CLI 删除缓存条目：

```
clear ssl-decrypt exclude-cache [server <value>] [application <value>]
```

如果有人尝试在本地缓存条目过期（12 小时）之前访问同一服务器，防火墙会将会话与缓存条目进行匹配，绕过解密，并允许流量。如果更改解密策略或配置文件，则防火墙将刷新本地排除缓存，因为这些更新可能会影响会话分类。如果缓存已满，则防火墙会在新条目到达时清除最旧的条目。

# 创建基于策略的解密排除

基于策略的解密排除用于排除您选择不进行解密的流量。您可以基于流量的源、目标、服务或 URL 类别的任意组合创建基于策略的解密排除。可以选择不进行解密的流量示例包括：

- 因包含个人身份信息(PII)或其他敏感信息（例如，URL 筛选类别 金融服务、健康和医疗、以及政府）而不得解密的流量。
- 源自或传往其流量不应进行解密的管理人员或其他用户的流量。
- 财务服务器等某些设备可能需要从解密中排除。
- 视业务不同，一些公司可能会重视隐私和用户体验，而不仅仅是某些应用程序的安全。
- 阻止解密某些流量的法律或地方法规。

  根据法规和法律合规性要求不能解密流量的示例是欧盟 (EU) 通用数据保护条例 (GDPR)。EU GDPR 要求对所有个人的私人数据进行强力保护。GDPR 对所有公司都有影响，包括需要收集或处理 EU 居民个人资料的外国公司。



© 2019 Palo Alto Networks, Inc.

不同的法规和合规性规则可能意味着您对不同国家或地区的相同数据采用不同的处理方法。企业通常可以在其公司数据中心解密个人信息，因为企业对这些信息具有拥有权。最佳做法是尽可能多地解密流量，这样，您才能查看并对其执行安全保护。

您可以使用预定义 URL 类别排除解密中的整个网站类别，可以创建自定义 URL 类别来定义您不想进行解密的自定义 URL 里列表，或是创建外部动态列表 (EDL) 以定义您不想进行解密的自定义 URL 列表。

在诸如 Office 365 等具有动态更改 IP 地址的环境，或是您需要对想要从解密中排除的 URL 列表进行频繁更改的环境中，通常最好是使用 EDL（而非 URL 类别）来指定排除的 URL。因为编辑 EDL 会在不执行 **Commit**（提交）的状态下动态改变 URL 类别，因此，在动态环境中使用 EDL 的破坏性较小，而编辑自定义 URL 类别则需要 **Commit**（提交）才能生效。



创建 *EDL* 或包含您选择不进行解密的所有类别的自定义 *URL* 类别，这样，解密策略规则就可以管控您选择允许的解密流量。将无解密配置文件应用于规则。通过添加类别到 *EDL* 或自定义 *URL* 类别，可以轻松排除解密中的流量，且有助于保持规则库的有序性。



与安全策略规则类似，防火墙将传入流量与策略规则库序列中的解密策略规则进行对比。将解密排除规则置于规则库的顶部，以避免无意中解密敏感流量或法律和法规要求不得解密的流量。

如果创建基于策略的解密排除，最佳做法是根据如下顺序将下列排除规则放置在解密规则库的顶部：

1. 用于敏感目标服务器的基于 IP 地址的例外。
2. 用于管理人员和其他用户或组的基于源用户的例外。
3. 用于目标 URL 的基于自定义 URL 或 EDL 的例外。
4. 用于金融服务、健康和医疗、政府等整个类别的目标 URL 的基于预定义 URL 类别的敏感例外。

将解密流量的规则放置在解密规则库中这些规则的后面。

STEP 1 | 根据匹配标准排除解密流量。

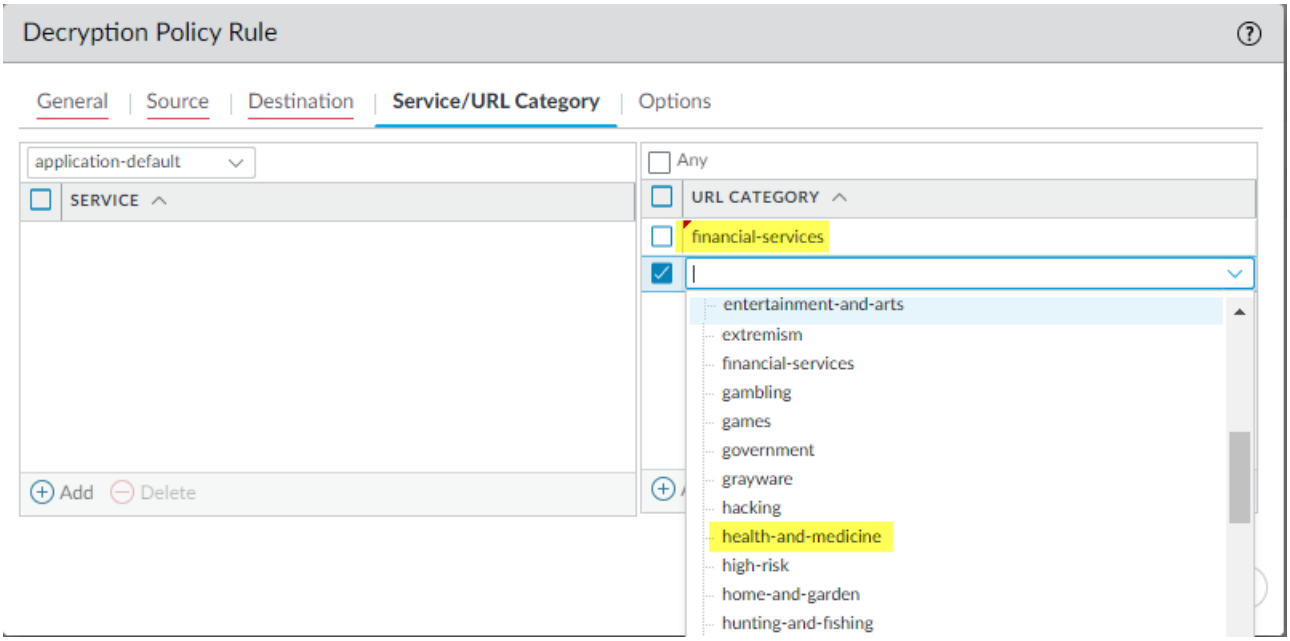
本例显示了如何根据 SSL 转发代理解密策略排除分类为金融或医疗保健相关的流量。

1. 选择 **Policies**（策略）> **Decryption**（解密），并 **Add**（添加）或修改解密策略规则。
2. 确定您希望排除解密的流量。

   在该举例中：

   1. 指定规则的描述性 **Name**（名称），如 No-Decrypt-Finance-Health。
   2. 将 **Source**（源）和 **Destination**（目标）设置为 **Any**（任何），以向所有传往外部服务器的 SSL 流量应用 No-Decrypt-Finance-Health 规则。
   3. 选择 **URL Category**（**URL** 类别）并 **Add**（添加）URL 类别 financial-services 和 health-and-medicine。


© 2019 Palo Alto Networks, Inc.




3. 选择 **Options**（选项）并设置规则为 **No Decrypt**（不解密）。
4. （可选，但属最佳做法）创建并附加未解密配置文件到规则，以对防火墙未解密的会话证书进行验证。将此配置文件设置为 **Block sessions with expired certificates**（阻止过期证书会话）和 **Block sessions with untrusted issuers**（阻止不可信颁发机构会话）。

   例外：切勿为未解密的 *TLSv1.3* 流量的解密策略附加“不解密”配置文件，因为防火墙无法读取加密证书信息，从而无法执行证书检查。但是，应为未解密的 *TLSv1.3* 流量创建解密策略，因为除非此解密策略可以控制该流量，否则，将不会记录未解密的流量。
5. 单击 **OK**（确定）以保存 No-Decrypt-Finance-Health 解密规则。

STEP 2 | 将解密排除规则置于解密策略规则库的顶部。

防火墙对规则库序列中的传入流量实施解密规则，并实施与流量匹配的第一个规则。

选择 **No-Decrypt-Finance-Health** 策略（**Decryption**（解密）> **Policies**（策略）），然后单击 **Move Up**（向上移动），直到它出现在列表顶部，或拖放此规则。

STEP 3 | 保存配置。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 阻止私钥导出

在 PAN-OS 或 Panorama 中生成证书私钥，或是将证书私钥导入到 PAN-OS 或 Panorama 中时，可以永久阻止该私钥的导出。通过阻止从 PAN-OS 设备中导出私钥，可防止恶意管理员或其他不良操作者滥用密钥，从而增强您的安全状态。具有证书管理角色的管理员可以阻止私钥导出。您不能阻止设备上已存在的密钥；您只能在 PAN-OS 中生成密钥时将其阻止，或是在将密钥导入 PAN-OS 时进行阻止。

一旦某个管理员阻止私钥导出，任何管理员都将无法导出该密钥，即使是超级用户管理员也不能导出。如果需要从 PAN-OS 设备导出私钥，请重新生成证书和密钥，但不要选择阻止私钥导出的选项。

要降级到更低版本的 PAN-OS，必须先删除私钥已被阻止的证书。如果您在尝试降级之前并未删除私钥已被阻止的证书，会出现一条错误消息，要求您删除这些证书。必须先删除，然后才能降级。降级后，如果需要使用这些被删除的证书，请重新导入或重新生成。

如果使用企业公钥基础设施 *(PKI)* 生成证书和私钥，请阻止私钥导出，原因在于您可以将它们从企业证书颁发机构 *(CA)* 安装到新的防火墙和 *Panorama* 上，因此没有理由将它们从 *PAN-OS* 导出。

如果在防火墙或 *Panorama* 上生成自签名证书，且使用“阻止私钥导出”选项，则无法将证书和密钥导出到其他 *PAN-OS* 设备。

即使您已阻止私钥导出，您仍可以导出和导入设备状态（**Device**（设备）> **Setup**（设置）> **Operations**（操作））。我们已将私钥纳入到设备状态导入和导出，但是，管理员无权读取或解码这些私钥。

如果两个防火墙采用相同的主密钥，则可以在一个防火墙上导入或加载另一个防火墙的配置。如果防火墙使用的主密钥不一致，就无法执行导入或加载配置这一操作，且在读取证书时，会提交失败。

- 生成私钥并阻止它
- 导入和阻止私钥
- 导入和阻止 IKE 网关私钥
- 验证私钥阻止

## 生成私钥并阻止它

阻止私钥导出，以防止私钥在证书生成后被滥用。

STEP 1 | 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

如果有一个以上的虚拟系统，请选择证书 **Location**（位置）或 **Shared**（共享））。

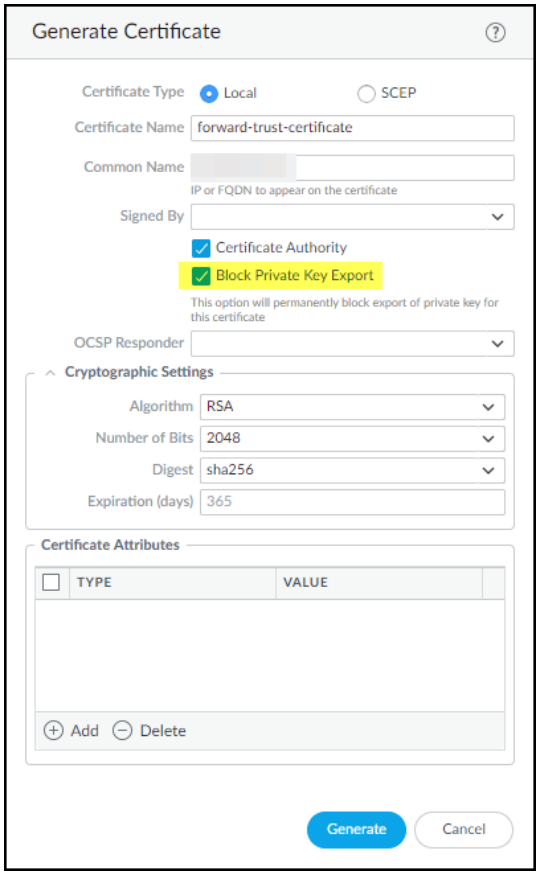
STEP 2 | **Generate**（生成）证书。

STEP 3 | 选择 **Block Private Key Export**（阻止私钥导出）以防止任何人导出证书。

有关其他证书字段的信息，请参阅生成证书。



© 2019 Palo Alto Networks, Inc.




STEP 4 | 单击 **Generate**（生成）以生成新的证书。

您可以通过可操作的 *CLI* 命令生成证书，并阻止证书私钥被导出：

```
admin@pa-220> request certificate generate block-private-keys yes
```

前述 *CLI* 命令还包括证书和其他未显示的参数。

## 导入和阻止私钥

阻止私钥导出，以防止私钥在导入证书后被滥用。

STEP 1 | 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。

如果有一个以上的虚拟系统，请选择证书 **Location**（位置）或 **Shared**（共享））。

STEP 2 | **Import**（导入）证书。

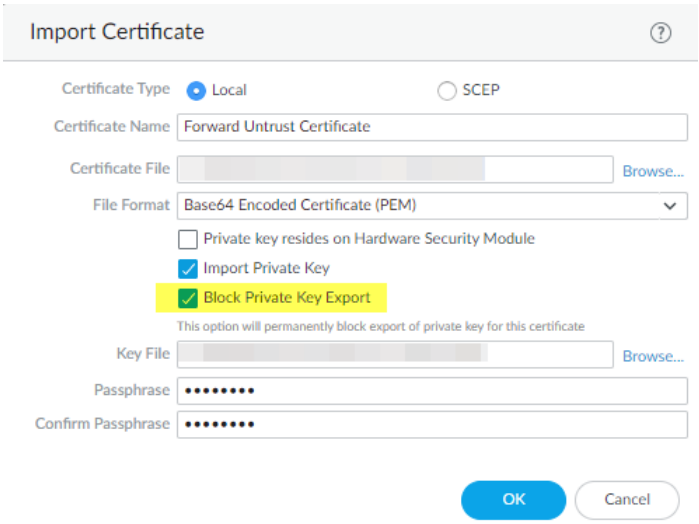
STEP 3 | 选择 **Import Private Key**（导入私钥）以激活阻止私钥导出这一选项。

STEP 4 | 选择 **Block Private Key Export**（阻止私钥导出）以防止任何人导出证书。

有关其他证书导入字段的信息，请参阅导入证书和私钥。



© 2019 Palo Alto Networks, Inc.




STEP 5 | 单击 **OK**（确定）以导入证书。

如果使用 *SCP* 可操作的 *CLI* 命令导入证书或导入证书私钥，您仍可以阻止导出私钥：

- ***admin@pa-220> scp import private-key block-private-key ...***

前面的每个 *CLI* 命令都还包括用于指定源、证书名称以及其他未显示参数的关键字。

若使用 *SCP* 可操作的 *CLI* 命令导出证书，并包括证书私钥 (***scp export certificate passphrase <phrase> remote-port <1-65536> to <destination> certificate-name <name> include-key <yes | no> format <der | pem | pkcs10 | pkcs12>***)，如果证书私钥被阻止，命令将失败，并返回错误消息，因为您无法导出已被阻止的私钥。

## 导入和阻止 IKE 网关私钥

阻止私钥导出，以防止私钥在用于 IKE 网关身份验证的证书生成后被滥用。

STEP 1 | 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Gateways**（**IKE** 网关）。

STEP 2 | **Add**（添加）新的 IKE 网关。

STEP 3 | 在 **General**（常规）选项卡中，对于 **Authentication**（身份验证），请选择 **Certificate**（证书）。

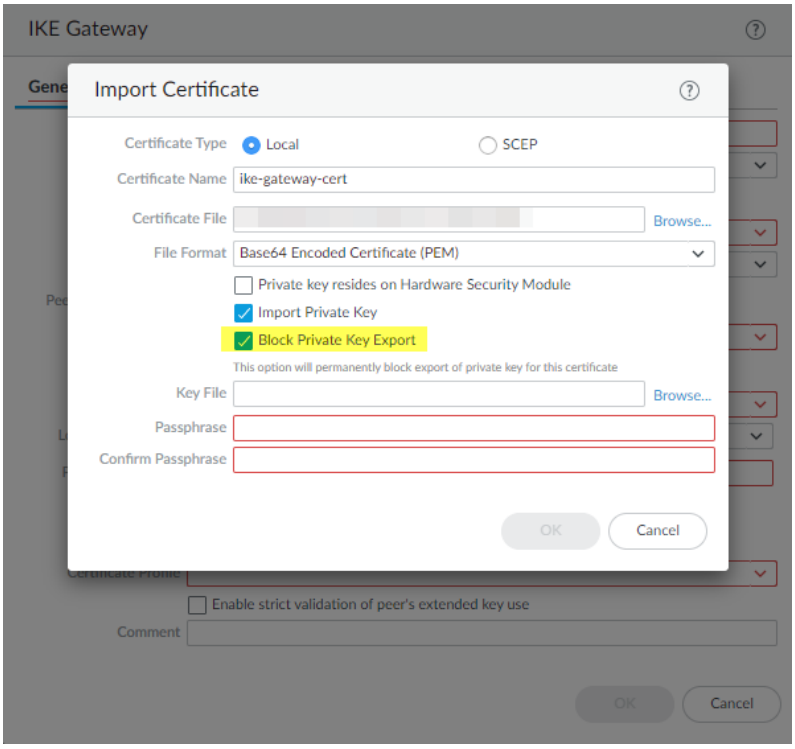
STEP 4 | 对于 **Local Certificate**（本地证书），根据您是要 导入现有证书还是要创建证书，选择 **Import**（导入）或 **Generate**（生成）。

STEP 5 | 输入证书信息。导入证书时，请选择 **Import Private Key**（导入私钥）以激活 **Block Private Key Export**（阻止私钥导出）复选框。

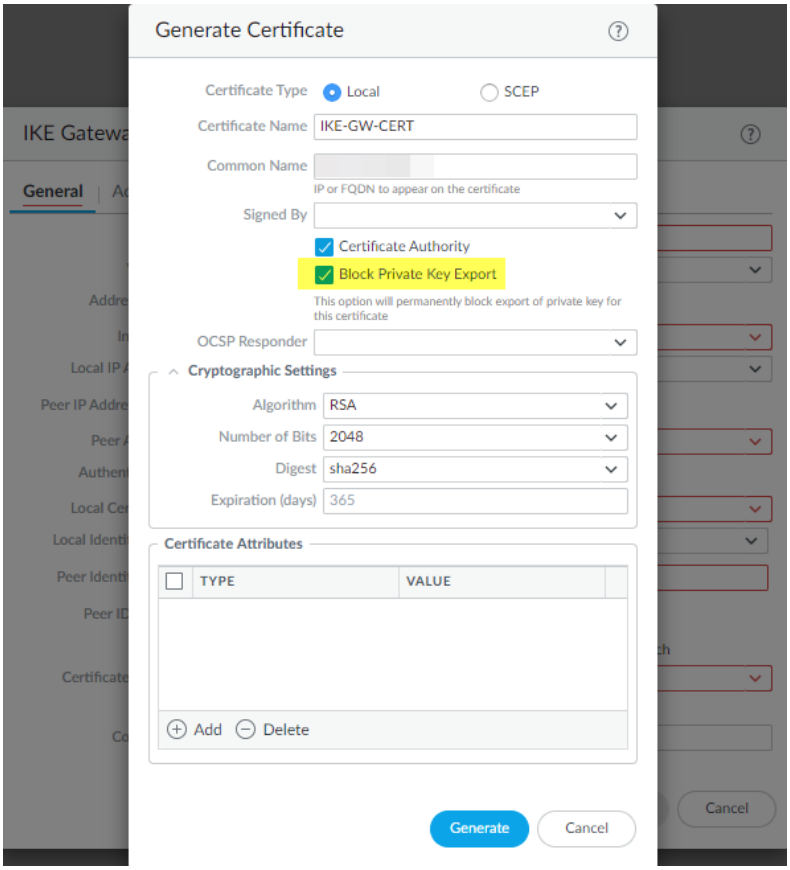
STEP 6 | 选择 **Block Private Key Export**（阻止私钥导出）以防止任何人导出密钥。

要导入证书，请输入并确认 **Passphrase**（密码），然后单击 **OK**（确定）


© 2019 Palo Alto Networks, Inc.




若要生成证书，请单击 **Generate**（生成）。




STEP 7 | 输入并确认 **Passphrase**（密码），然后单击 **OK**（确定）。



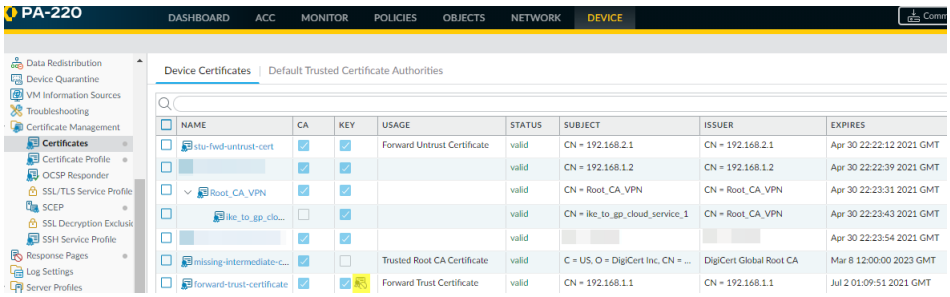
© 2019 Palo Alto Networks, Inc.

# 验证私钥阻止

您可以通过多种方式验证私钥是否被阻止导出。

- 检查 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）中的**Key**（密钥）列。

  在本例中，forward-trust-certificate 被阻止：




- 当您尝试导出一个其私钥已被阻止导出的证书时，**Export Private Key**（导出私钥）复选框将不可用，此时您无法导出该密钥，只能导出证书。

- 使用下列可操作的 CLI 命令列出设备上所有证书，尤其是私钥已被阻止导出的特定 Vsys 上的所有证书。

```
admin@pa-220> request certificate show-blocked <shared | vsys>
```

- 使用下列可操作的 CLI 命令检查特定证书的私钥是否已被阻止导出：

```
admin@pa-220> request certificate is-blocked certificate-name <name>
```

  如果证书被阻止导出，则命令返回为 **yes**（是）；如果证书未被阻止，则命令返回为 **no**（否）。


© 2019 Palo Alto Networks, Inc.

# 让用户选择停用 SSL 解密

在隐私敏感的情况下，可能需要提醒您的用户防火墙正在解密某些 Web 流量，并让他们知道其流量已解密以继续访问此站点，或是终止会话且阻止进入此站点。（没有前往站点的选项，同时也避免解密。）

用户首次尝试浏览与您的解密策略匹配的 HTTPS 网站或应用程序时，防火墙会显示一个响应页面来通知用户该会话将被解密。用户可以单击 **Yes**（是）来允许解密并继续打开该网站，也可以选择单击 **No**（否）来停用解密并终止会话。选择允许解密应用于用户在接下来的 24 小时内尝试访问的所有 HTTPS 网站，此后防火墙将重新显示响应页面。用户选择停用 SSL 解密的一分钟后，将无法进入所请求的 Web 页面或任何其他 HTTPS 网站。一分钟后，在用户下次尝试访问 HTTPS 网站时，防火墙将重新显示响应页面。

该防火墙包括您可以启用的预定义 SSL 解密退出页面。您可以选择性地使用您自己的文字和/或图像自定义该页面。但是，最佳做法是不允许用户停用解密。



大于最大支持大小的自定义响应页面不会被解密或向用户显示。在 *PAN-OS 8.1.2* 及更高版本 *PAN-OS 8.1* 发布中，解密站点上的自定义响应页面不会超过 *8191* 字节；在 *PAN-OS 8.1.3* 及更高版本中，最大大小增至 *17999* 字节。

STEP 1 | （可选）自定义 SSL 解密退出页面。

1. 选择 **Device**（设备）> **Response Pages**（响应页面）。
2. 选择 **SSL Decryption Opt-out Page**（SSL 解密退出页面）链接。
3. 选择 **Predefined**（预定义）页面并单击 **Export**（导出）。
4. 使用所选 HTML 文本编辑器编辑该页面。
5. 如果要添加图像，请将图像上传到可从最终用户系统访问的 Web 服务器上。
6. 在 HTML 文件中添加一行指向该图像的内容。例如：

```
<img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?1382722588"/>
```

7. 用新文件名保存编辑后的页面。确保该页面保持其 UTF-8 编码。
8. 返回防火墙，然后选择 **Device**（设备）> **Response Pages**（响应页面）。
9. 选择 **SSL Decryption Opt-out Page**（SSL 解密退出页面）链接。
10. 单击 **Import**（导入），然后在 **Import File**（导入文件）字段中输入路径和文件名，或 **Browse**（浏览）以定位文件。
11. （可选）从 **Destination**（目标）下拉列表中选择将在其上使用该登录页面的虚拟系统，或选择共享以使其可供所有虚拟系统使用。
12. 单击 **OK**（确定）以导入文件。
13. 选择刚才导入的响应页面，然后单击 **Close**（关闭）。

STEP 2 | 启用“SSL 解密退出”。

1. 在 **Device**（设备）> **Response Pages**（响应页面）页面上，单击 **Disabled**（禁用）链接。
2. 选择 **Enable SSL Opt-out Page**（启用 SSL 退出页面），然后单击 **OK**（确定）。
3. **Commit**（提交）更改。

STEP 3 | 验证在您尝试浏览网站时显示的“退出”页。

在浏览器中，转到与您的解密策略匹配的加密网站。

验证显示的 SSL 解密退出响应页。



© 2019 Palo Alto Networks, Inc.





© 2019 Palo Alto Networks, Inc.

# 暂时禁用 SSL 解密

在某些情况下，您可能希望暂时禁用 SSL 解密。例如，如果部署的 SSL 解密过于仓促，且有些部分无法正常运行，但您又不确定问题出在哪里，而您又有很多的规则需要检查，因此，您可以使用 CLI 暂时关闭解密，让自己有时间分析并解决问题。问题解决后，您可以使用 CLI 重新打开 SSL 解密。因为使用 CLI 实施暂时禁用，然后重新启用解密无需提交操作，因此可在不中断网络流量的情况下进行操作。

以下 CLI 命令可暂时禁用 SSL 解密和重新启用解密，均无需提交。



重启后，禁用 *SSL* 解密的命令不会在配置中保留。如果暂时关闭解密，然后重启防火墙，无论问题是否修复，解密都将再次打开。

- 禁用 SSL 解密

```
set system setting
ssl-decrypt skip-ssl-decrypt yes
```

- 重新启用 SSL 解密

```
set system setting
ssl-decrypt skip-ssl-decrypt no
```



© 2019 Palo Alto Networks, Inc.

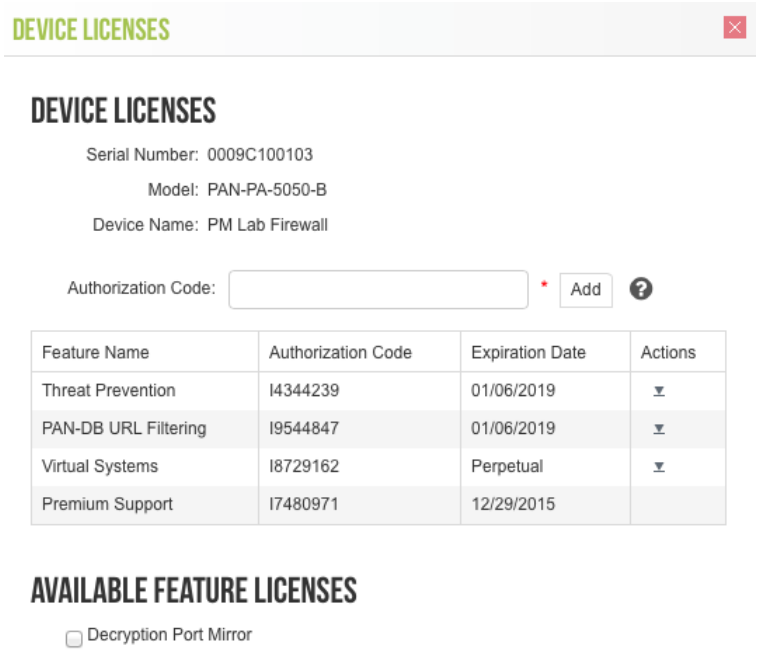
# 配置解密端口镜像

在可以启用解密镜像之前，必须获取并安装解密端口镜像许可证。许可证免费提供，并且可通过以下步骤所述的支持门户进行激活。在安装解密端口镜像许可证和重启防火墙后，可以启用解密端口镜像。

请记住，在某些国家/地区限制解密、存储、检查和/或使用 SSL 流量，并且只有在征得用户同意后才能使用解密镜像功能。此外，使用此功能可能会使得对防火墙拥有管理访问权限的恶意用户盗取用户名、密码、社会安全号码、信用卡号码或使用加密通道提交的其他敏感信息。Palo Alto Networks 建议您在生产环境中激活和使用此功能之前咨询您的企业顾问。

STEP 1 | 索取想要在其中启用解密端口镜像的每台防火墙的许可证。

1. 登录到 Palo Alto Networks 客户支持网站并导航到 **Assets**（资源）选项卡。
2. 选择要许可的防火墙名称，然后选择 **Actions**（操作）。
3. 选择 **Decryption Port Mirror**（解密端口镜像）。将会显示法律公告。
4. 如果您在明确潜在的法律含义和要求后仍想设置解密端口镜像，单击 **I understand and wish to proceed**（我了解并希望继续）。
5. 单击 **Activate**（激活）。




STEP 2 | 在防火墙上安装解密端口镜像许可证。

1. 从防火墙 Web 界面中，选择 **Device**（设备）> **Licenses**（许可证）。
2. 单击 **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）。
3. 验证在防火墙上是否已激活许可证。




4. 重启防火墙（**Device**（设备）> **Setup**（设置）> **Operations**（操作））。在 PAN-OS 重新加载前，此功能不适用于配置。


© 2019 Palo Alto Networks, Inc.

STEP 3 | 启用防火墙来转发加密流量。只有具备超级用户权限才能执行此步骤。

在安装一个虚拟系统的防火墙上：

1. 选择 **Device**（设备）> **Setup**（设置）> **Content - ID**（内容 **ID**）。
2. 选中 **Allow forwarding of decrypted content**（允许转发加密的内容）复选框。
3. 单击 **OK**（确定）以保存。

在安装多个虚拟系统的防火墙上：

1. 选择 **Device**（设备）> **Virtual System**（虚拟系统）。
2. 通过选择 **Add**（添加）以选择要编辑的虚拟系统或创建新的虚拟系统。
3. 选中 **Allow forwarding of decrypted content**（允许转发加密的内容）复选框。
4. 单击 **OK**（确定）以保存。

STEP 4 | 启用要用于解密镜像的 Ethernet 接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。
2. 选择要为解密端口镜像配置的以太网接口。
3. 选择 **Decrypt Mirror**（解密镜像）作为 **Interface Type**（接口类型）。

   此接口类型将只有在安装解密端口镜像许可证后才会显示。
4. 单击 **OK**（确定）以保存。

STEP 5 | 启用解密的流量的镜像。

1. 选择 **Objects**（对象）> **Decryption Profile**（解密配置文件）。
2. 选择 **Interface**（接口）以用于 **Decryption Mirroring**（解密镜像）。

   **Interface**（接口）下拉列表包含已定义类型的所有以太网接口：**Decrypt Mirror**（解密镜像）。
3. 指定在策略执行之前或之后是否镜像解密的流量。

   默认情况下，防火墙会在安全策略查询之前将所有解密的流量镜像到接口，这可让您重播事件和分析生成威胁或触发丢弃操作的流量。如果只想在安全策略执行之后镜像解密的流量，请选中 **Forwarded Only**（仅已转发）复选框。使用此选项，只镜像通过防火墙转发的流量。如果将解密的流量转发到其他威胁检测设备（如 DLP 设备或其他入侵防御系统 (IPS)），可以使用此选项。
4. 单击 **OK**（确定）以保存解密配置文件。

STEP 6 | 将解密配置文件规则（使用已启用的解密端口镜像）附加到解密策略规则。根据策略规则镜像所有解密的流量。

1. 选择 **Policies**（策略）> **Decryption**（解密）。
2. 单击 **Add**（添加）以配置解密策略或选择要编辑的现有解密策略。
3. 在 **Options**（选项）选项卡中，选择 **Decrypt**（解密）和步骤 4 中创建的 **Decryption Profile**（解密配置文件）。
4. 单击 **OK**（确定）以保存策略。

STEP 7 | 保存配置。

单击 **Commit**（提交）。



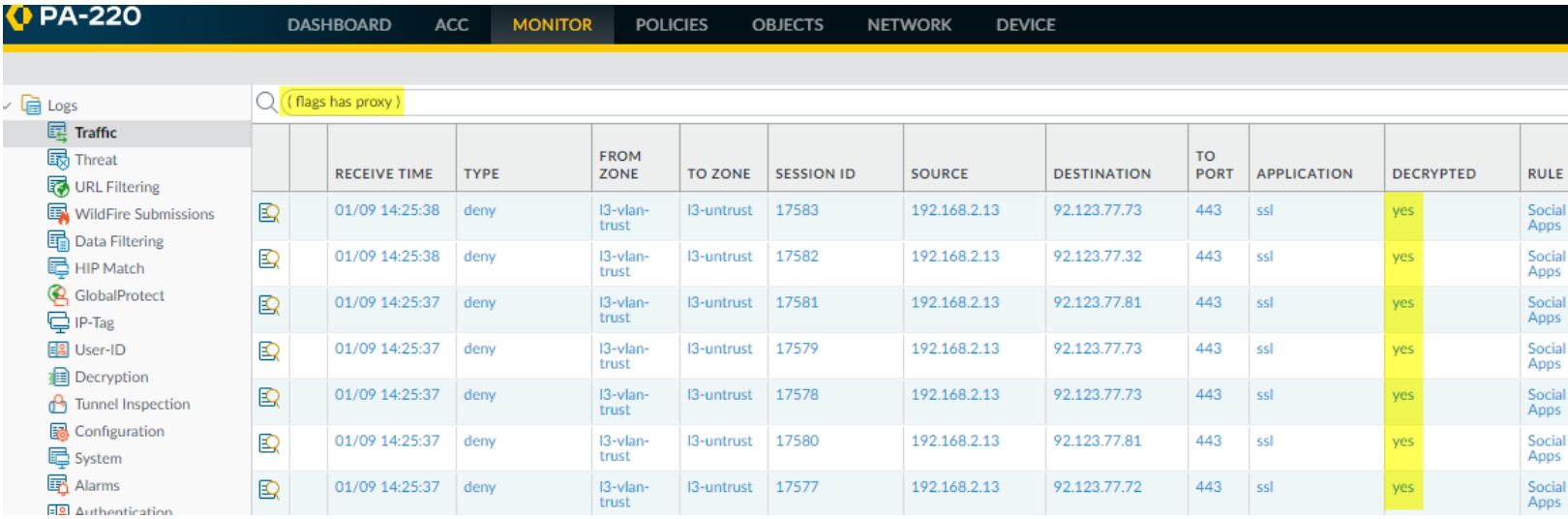
© 2019 Palo Alto Networks, Inc.

# 验证解密

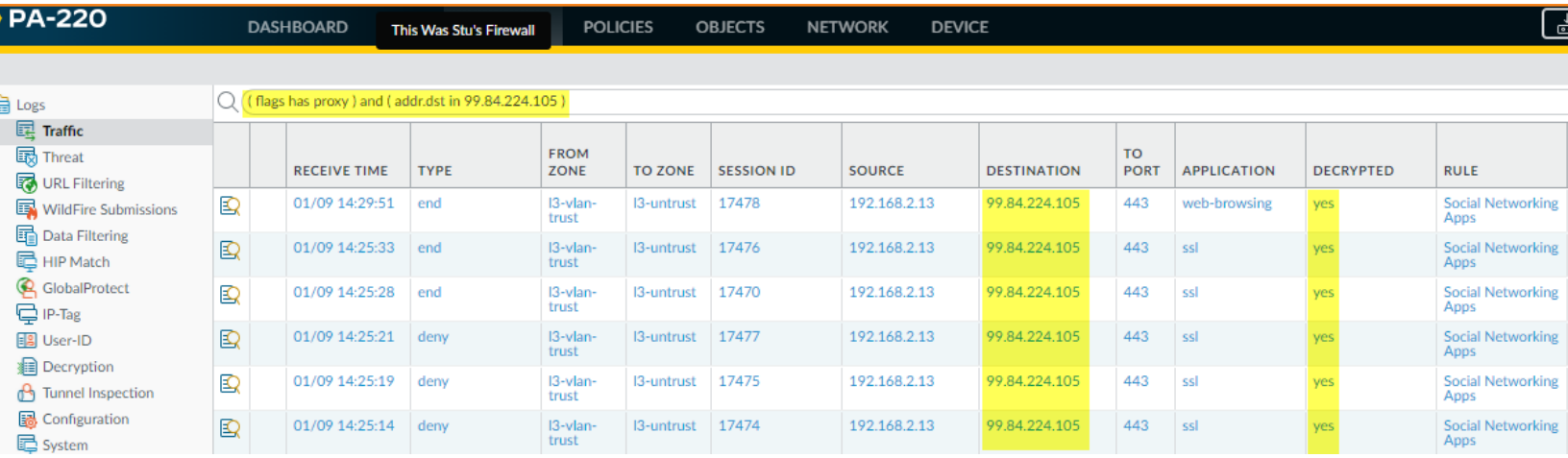
配置最佳实践解密配置文件并将其用于流量后，您可以检查（PAN-OS 10.0 中引入的）解密日志和流量日志，以验证防火墙是否正在解密您想要解密的流量，而没有解密您不想解密的流量。本主题介绍了如何使用流量日志检查解密。此外，还应遵循部署后解密最佳实践以维护部署。

- 查看已解密流量会话 — 使用筛选程序（`flags has proxy`）筛选流量日志（**Monitor**（监控）> **Logs**（日志）> **Traffic**（流量））。

  此筛选程序仅显示 SSL 代理标记所在的日志，即仅解密流量 — 每个日志条目在 **Decrypted**（已解密）列中的值均为 yes。




您可以通过向筛选程序添加更多词语的方式更精细地筛选流量。例如，您可以通过添加筛选程序（`addr.dst in 99.84.224.105`）筛选仅前往目标 IP 地址 99.84.224.105 的已解密流量。

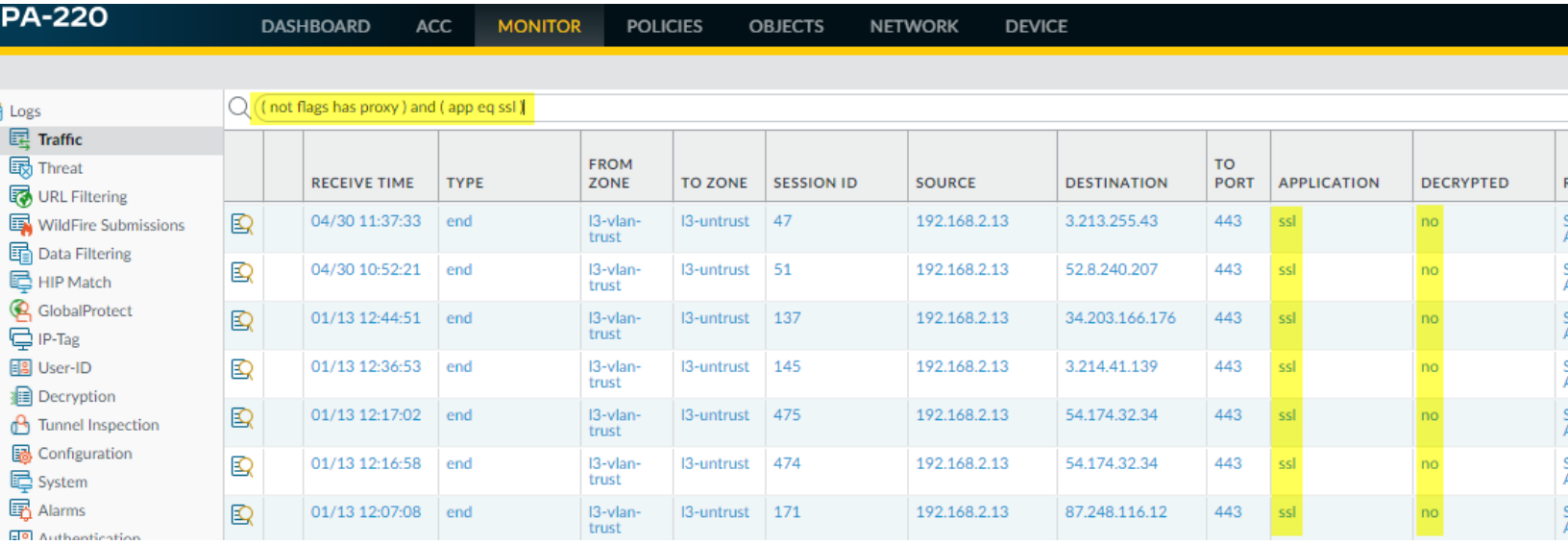



- 查看未解密的 SSL 流量会话 — 使用筛选程序（`not flags has proxy ) and ( app eq ssl`）筛选流量日志（**Monitor**（监控）> **Logs**（日志）> **Traffic**（流量））。

  此筛选程序仅显示 SSL 代理标记不在的日志（即仅加密流量）且流量是 SSL 流量；每个日志条目在 **Decrypted**（已解密）列中的值均为 **no**（否），在 **Application**（应用程序）列中的值为 **ssl**。



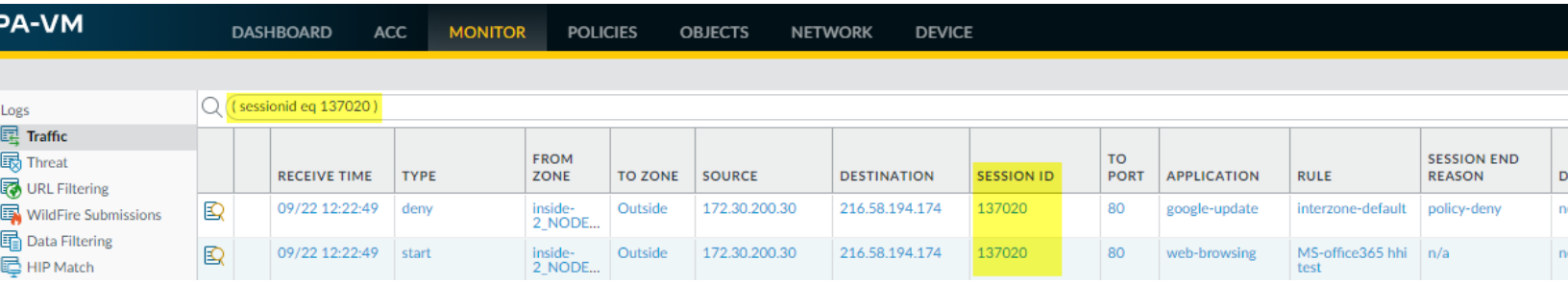
© 2019 Palo Alto Networks, Inc.



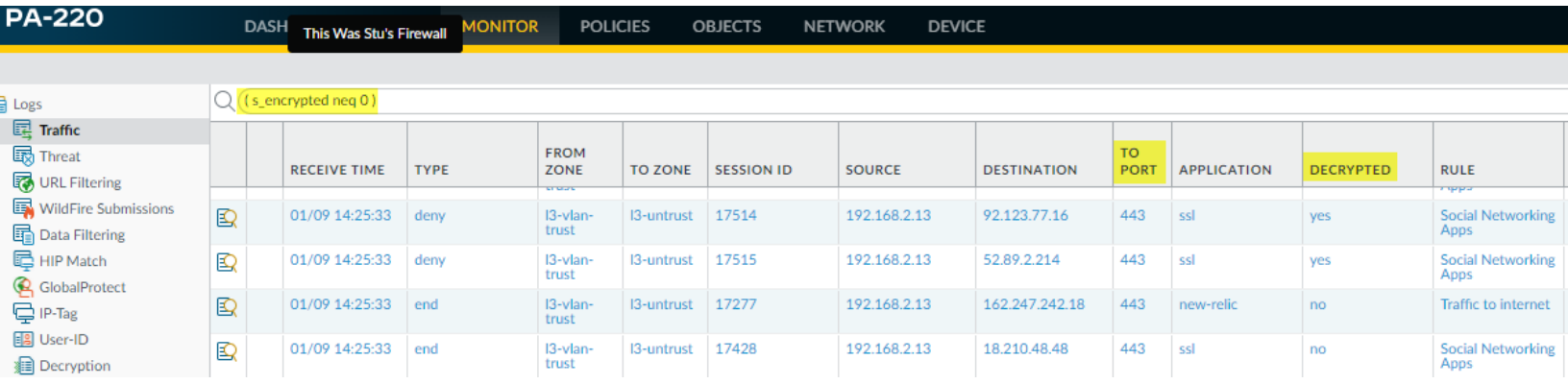

与查看已解密流量日志的示例类似，您可以添加词语到您不想以更精细方式解密的流量。

- 查看特定会话的日志 — 若要查看特定会话的流量日志，请筛选会话 ID。

  例如，要查看 ID 为 137020 的会话日志，则使用词语 `( sessionid eq 137020)` 进行筛选。您可以在日志输出的会话 ID 列中找到 ID 编号，如前面的屏幕所示。如果不显示会话 ID 列，则添加列到输出。



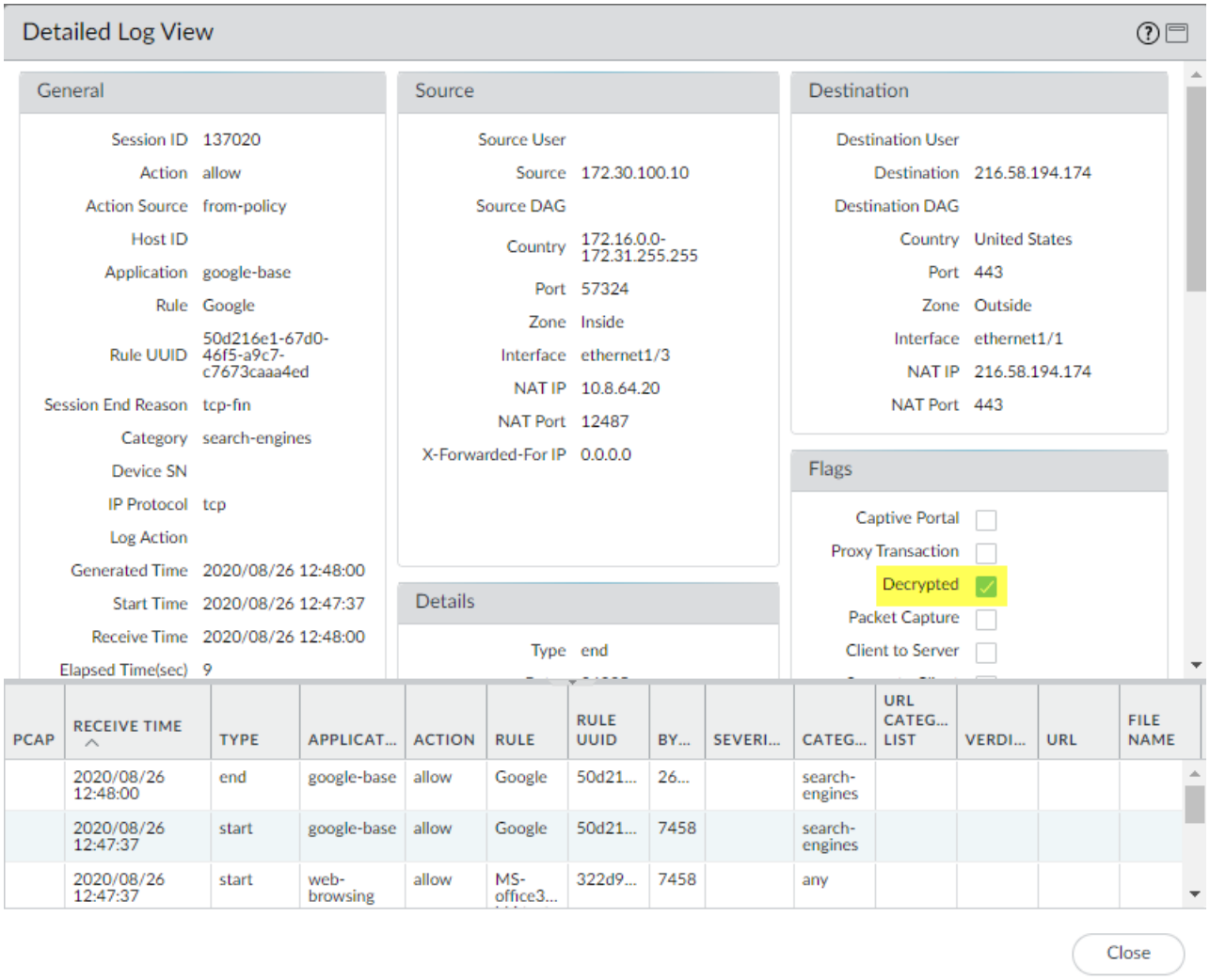

- 查看所有 **TLS** 和 **SSH** 流量— 筛选流量日志（**Monitor**（监控）> **Logs**（日志）> **Traffic**（流量））以查看已解密的和未解密的 TLS 和 SSH 流量，并使用筛选程序 `(s_encrypted neq 0 )`：




- 深入查看详细信息 — 要查看特定日志条目的更多信息，单击放大镜以查看更详细的日志视图。例如，对于会话 ID 137020（如上一个要点所示），详细的日志如下所示：



© 2019 Palo Alto Networks, Inc.




**Decrypted**（已解密）标记的框提供了用于验证流量是否已解密的第二种方法。

此外，您还可以获取已解密流量的上游和下游数据包捕获以查看防火墙如何处理 SSL 流量，如何处理数据包，或如何执行深度数据包检查。



© 2019 Palo Alto Networks, Inc.

# 排除故障并监视解密

故障排除工具可提高 TLS 流量的可见性，便于您监控您的解密部署。通过该工具，您可以快速轻松地诊断并解决解密问题，消除解密部署的薄弱点，修复解密问题，从而改善安全状况。例如，您可以：

- 通过服务名称标识 (SNI) 和应用程序识别导致解密失败的流量。
- 识别使用弱协议和算法的流量。
- 检查网络中成功和失败的解密活动。
- 查看各会话的相关详细信息。
- 配置文件解密使用情况和模式。
- 监控详细的解密统计信息以及与应用、失败、版本、算法等相关的信息。

以下工具可提供 TLS 握手的可见性，帮助您对解密部署进行故障排除，并监控解密部署：

- **ACC** > **SSL Activity**（**ACC SSL** 活动）— 此选项卡（PAN-OS 10.0 中引入）上的 5 个 ACC 小部件提供了网络中成功和失败的解密活动的详细信息，包括解密失败、TLS 版本、密钥交换、以及解密和未解密流量的数量和类型。
- **Monitor**（监控）> **Logs**（日志）> **Decryption**（解密）— 解密日志（PAN-OS 10.0 中引入）提供了与解密日志匹配的各个会话的详细信息，以及 GlobalProtect 会话（已在 GlobalProtect 门户或 GlobalProtect 网关配置中启用解密日志记录时）的详细信息。选择可以显示的列，以查看应用程序、SNI、解密策略名称、错误索引、TLS 版本、密钥交换版本、加密算法、证书密钥类型等许多其他特征方面的信息。筛选各列中的信息，以识别使用特定 TLS 版本和算法的流量、特定错误，或您想调查的任何其他特征。解密策略默认仅记录失败的 TLS 握手。根据可用的日志存储，您可以将解密策略配置为还记录成功的 TLS 握手。
- **Local Decryption Exclusion Cache**（本地解密排除缓存）— 存在两种因客户端身份验证或固定证书等技术原因破解解密，从而需要从解密中排除的站点结构：SSL 解密排除列表和本地解密排除缓存。SSL 解密排除列表包括 Palo Alto Networks 已识别的、出于技术原因破解解密的站点。该列表通过内容更新保持最新，以便您可以手动添加站点到该列表。“本地解密排除缓存”将自动添加本地用户遇到的、因技术原因破解解密的站点，并将这些站点从解密中排除，但前提是对流量应用的解密配置文件允许不受支持的模式（如果不受支持的模式被阻止，则流量也会被阻止，而不是添加到本地缓存）。
- **Custom Report Templates for Decryption**（解密自定义报告模板）— 您可以使用用于汇总解密活动的 4 个预定义模板（PAN-OS 10.0 引入）创建自定义报告（**Monitor**（监控）> **Manage Custom Reports**（管理自定义报告））。

常见的故障排除方法是使用新的 ACC 小部件标识引发解密问题的流量，然后使用新的解密日志和自定义报告模板深入了解详细信息，获取有关该流量的上下文，以便能准确诊断出问题，这种方法比过去的方法更容易。通过了解解密问题及其原因，您可以选择正确的方式来解决各个问题，例如：

- 修改解密策略规则（策略规则用于定义受规则影响的流量、对该流量采取的操作、日志设置，以及应用到该流量的解密配置文件）
- 修改解密配置文件（解密策略规则针对该流量定义的可接受的协议和算法，以及故障检查、不受支持的模式检查（检查不受支持的密码和版本等）、证书检查等）
- 将出于技术原因破解解密的站点添加到 SSL 解密排除列表
- 评估关于以下方面的安全决策：您的员工、客户和合作伙伴确实需要访问的站点，以及在站点使用弱解密协议或算法时您可以阻止的站点

目标应为解密您可以解密的所有流量（解密最佳实践），以便于您不仅可以监控流量，还能正确处理不能解密的流量。

升级到 PAN-OS 10.0 后，设备占用 1% 的日志空间，并将其分配给解密日志。配置解密日志记录中的步骤 3显示了如何通过修改日志空间分配，从而为解密日志分配更多的空间。

如果从 PAN-OS 10.0 或更高版本降级到 PAN-OS 9.1 或更低版本，PAN-OS 10.0 中引入的功能（解密日志、ACC 中的 SSL 活动小部件、自定义报告解密模板）将从 UI 中移除。对解密日志的引用也将从日志转发



© 2019 Palo Alto Networks, Inc.

配置文件中移除。此外，本地解密排除缓存也将只能通过 PAN-OS 9.1 以及更低版本中的 CLI 查看（PAN-OS 10.0 已将本地缓存添加到 UI）。

如果将配置从 PAN-OS 10.0 或更高版本推送到运行 PAN-OS 9.1 或更低版本的设备，Panorama 将移除 PAN-OS 10.0 中引入的功能。


- 解密应用程序命令中心小部件
- 解密日志
- 自定义解密报告模板
- 解密故障排除工作流程示例


# 解密应用程序命令中心小部件

PAN-OS 10.0 中引入的适用于解密的应用程序命令中心 (ACC) 小部件（**ACC** > **SSL Activity**（**ACC SSL** 活动））可与解密日志一起帮助您快速轻松地诊断并解决解密问题。使用 **SSL Activity**（**SSL** 活动）小部件查看并分析网络解密活动，包括解密和未解密的会话数，有多少流量使用了不同的 TLS 协议版本，导致解密失败的最常见的原因，以及使用弱密码和弱算法的应用程序和服务器名称标识 (SNI)。接下来，使用解密日志深入分析会话，然后诊断确切问题，以便您采取适当的操作。

PAN-OS 10.0 引入了 5 个新的解密小部件。使用小部件提供的信息标识配置错误的解密策略和配置文件，并就允许和阻止哪些流量做出明智的决策：

- **Traffic Activity**（流量活动）— 按会话总数或通信量（以字节为单位）显示 SSL/TLS 活动与非 SSL/TLS 活动。
- **SSL/TLS Traffic**（**SSL/TLS** 流量）— 按会话总数或通信量（以字节为单位）显示解密和未解密流量。流量未解密的原因包括：
  - 此流量适用于“不解密”策略。
  - 解密策略有意使流量免于解密（例如，使用“不解密”策略）。
  - 解密策略配置错误，流量本该解密，但却没有。
  - 站点列入到 SSL 解密排除列表（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））。该列表中包含的是 Palo Alto Networks 已确定会因为固定证书或客户端身份验证等技术原因破坏解密的站点。对于这些站点，防火墙将绕过解密。
  - 站点列入到 本地解密排除缓存。该缓存中包含的是用户遇到的、出于技术原因而阻止解密的站点。

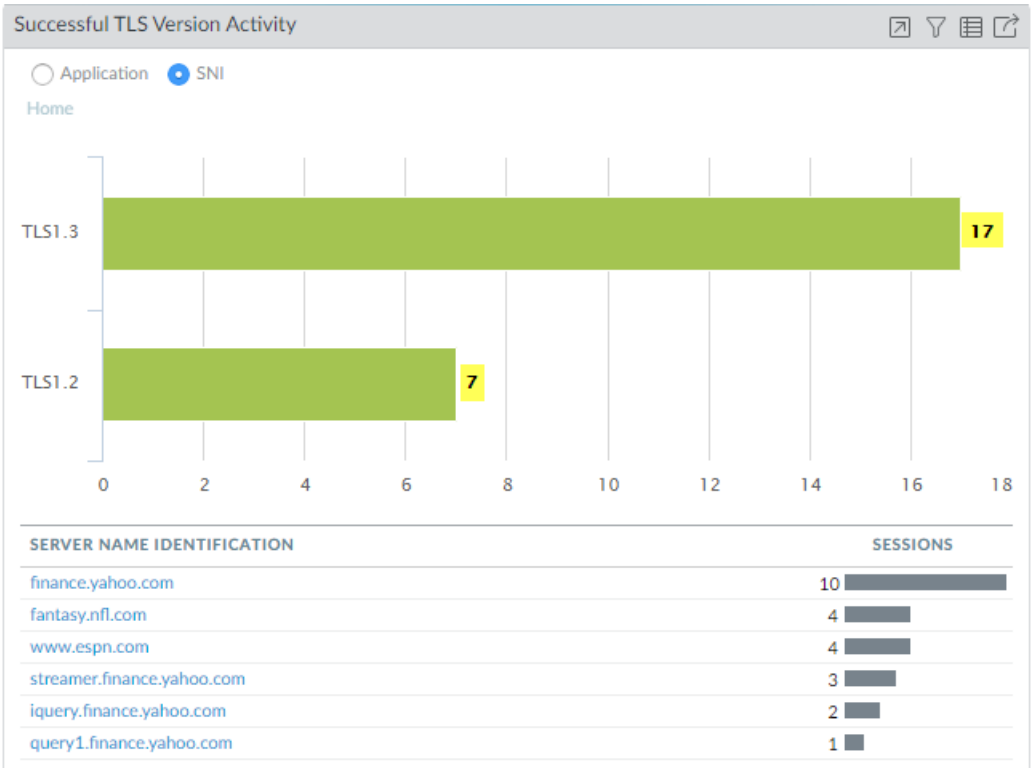
ACC 仅使用解密策略控制的流量的数据填充接下来三个小部件。如果未对流量应用解密策略，则该流量不会填充这些小部件。

- **Decryption Failure Reasons**（解密失败原因）— 显示导致解密失败的原因：协议、证书、版本、密码、HSM、资源、恢复或功能问题、SNI 等。使用这些信息可以检测出因解密策略或配置文件配置错误，或是流量使用不受支持的弱协议或算法而导致的问题。单击失败原因以深入了解经历过失败的每个 SNI 的会话数并进行隔离，或是单击 SNI 以查看该 SNI 出现的所有解密失败事件。
- **Successful TLS Version Activity**（成功的 **TLS** 版本活动）— 按应用程序 TLS 版本或 SNI（SNI 仅用于转发代理）显示成功的 TLS 连接，这样，您就可以评估因允许较弱的 TLS 协议版本而承受的风险。通过标识使用弱协议的应用程序和 SNI，您可以分别进行评估，并决定是否允许出于业务原因对其进行访问。如果开展业务不需要使用该应用程序，您可以阻止该流量（而不是允许该流量）以降低风险。单击 TLS 版本了解详细信息，并查看使用该 TLS 版本的 SNI 或应用程序。单击应用程序或 SNI 了解详细信息，并查看这些应用程序或 SNI 会话使用各个 TLS 版本的数量是多少。
- **Successful Key Exchange Activity**（成功的密钥交换活动）— 按算法显示应用程序或 SNI（SNI 仅用于转发代理）的成功密钥交换活动。单击密钥交换算法以仅查看该算法的活动，或是单击应用程序或 SNI 以查看该应用程序或 SNI 的密钥交换算法活动。

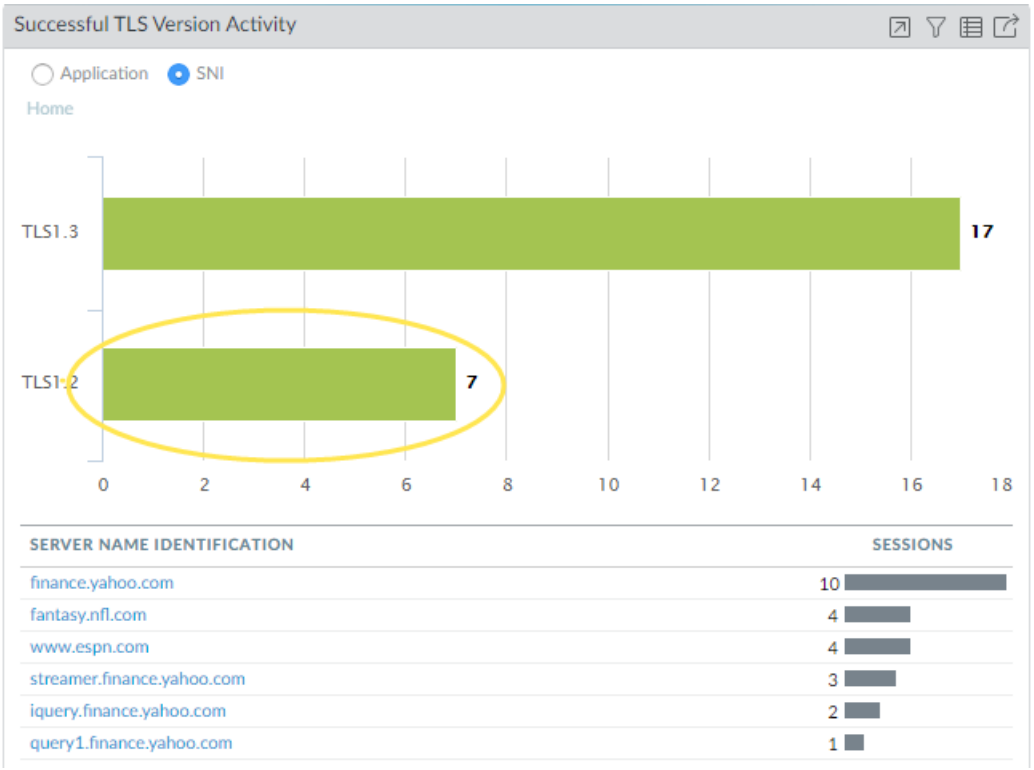
以下是深入分析 ACC 数据的示例，展示了如何检查成功的 TLS 版本活动：

1. **Successful TLS Version Activity**（成功的 **TLS** 版本活动）小部件显示，有 17 个会话使用 TLSv1.3，有 7 个会话使用 TLSv1.2。SNI 列表显示目标 SNI 和每个 SNI 的会话数。


© 2019 Palo Alto Networks, Inc.



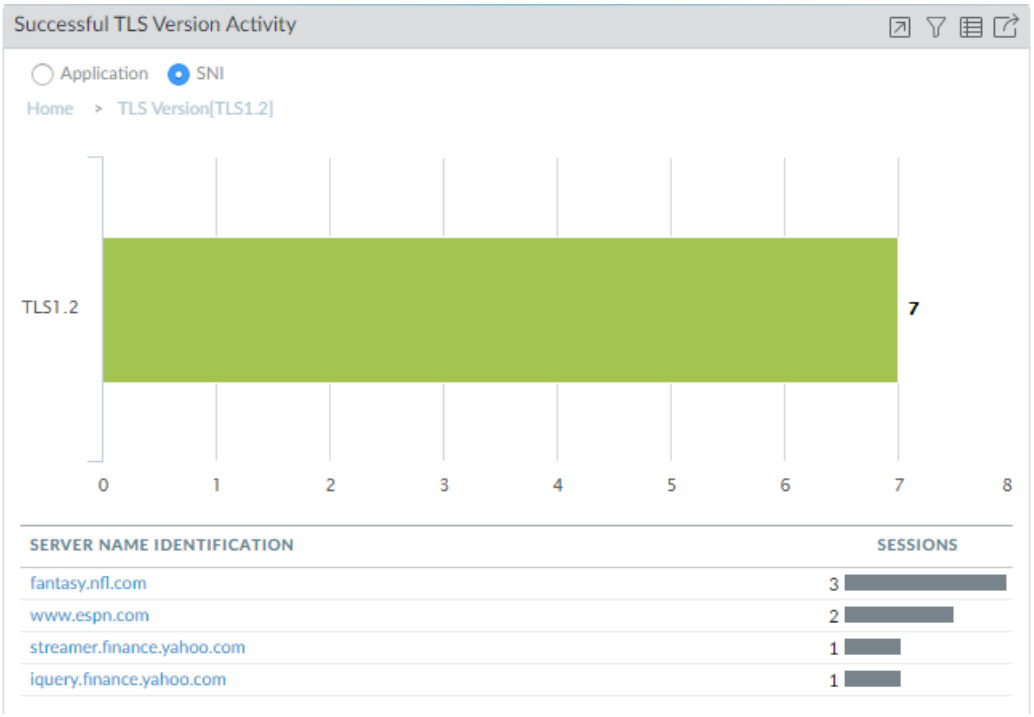

2. 若要查看哪个 SNI 使用 TLSv1.2，请单击带 TLS1.2 标记的绿条。



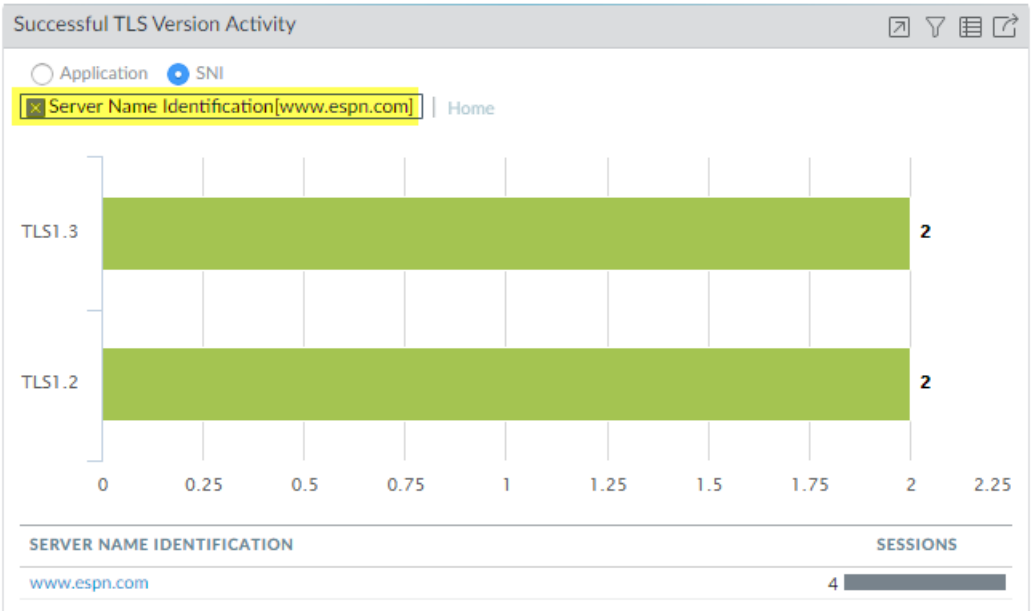

3. 现在，您可以看到，这 7 个 TLSv1.2 会话分布在 4 个服务器。



© 2019 Palo Alto Networks, Inc.




4. 单击 **Home**（主页）返回到主屏幕。现在，单击 www.espn.com SNI，将显示其使用的 TLS 版本。我们可以看到，有 4 个会话使用 TLSv1.3，有 2 个会话使用 TLSv1.2。




对于任何解密小部件，都可通过单击“跳转到日志”图标，直接跳转到与 ACC 中数据相对应的解密日志：




在前面的示例中，在调查的任何阶段，您都可以跳转到解密日志，以深入了解数据。例如，您可以检查使用 TLSv1.2 的单个会话的日志，以了解其为什么不使用 TLSv1.3。

解密 ACC 小部件将根据 Palo Alto Networks App-ID 显示所解密的应用程序名称。填充 ACC 时，防火墙仅标识具有 Palo Alto Networks App-ID 的应用程序；防火墙不会将自定义应用程序或没有 App-ID 的应用程序填入 ACC。内容更新功能会定期更新 App-ID。应用程序显示为不完整或未知的其他原因包括：


© 2019 Palo Alto Networks, Inc.

- 防火墙在标识应用程序之前就已删除会话。
- 解密日志依据流量日志填充解密日志中的应用程序字段。但是，如果流量日志不能在 60 秒或更短时间内完成，则流量日志不会填充解密日志中的应用程序字段，且应用程序会显示为不完整或未知。

# 解密日志

解密日志（**Monitor**（监控）> **Logs**（日志）> **Decryption**（解密））提供了与解密策略匹配的会话相关的全面信息，帮助您获取该流量的上下文信息，从而轻松准确地诊断并解决解密问题。防火墙无法记录与解密策略不匹配的流量。如果想记录不解密的流量，请创建基于策略的解密排除，并对于管理 TLSv1.2 和更早流量的策略，将"不解密"配置文件应用到该流量。

PAN-OS 支持适用于下列流量类型的解密日志：

- 转发代理 — 几个字段仅显示转发代理流量的信息，包括根 CA（仅适用于可信证书）和服务器名称指示 (SNI)。
- 入站检查。
- 不解密（解密策略从解密中排除的流量）。

  因为会话仍保持加密状态，因此，防火墙显示的信息较少。对于未解密的 *TLSv1.3* 流量，由于 *TLSv1.3* 加密了证书信息，因此不会显示证书信息。
- GlobalProtect — 包括 GlobalProtect 网关、GlobalProtect 门户以及 GlobalProtect 无客户端 VPN（仅限客户端到防火墙）。

  *GlobalProtect* 不支持 *TLSv1.3*。
- 解密镜像
- 解密代理（在 **Proxy Type**（代理类型）列中显示为转发代理）。

并非所有类型的流量都支持每个参数。按代理类型和 TLS 版本划分的不受支持的参数针对每种类型的解密流量提供了完整的不受支持参数列表。

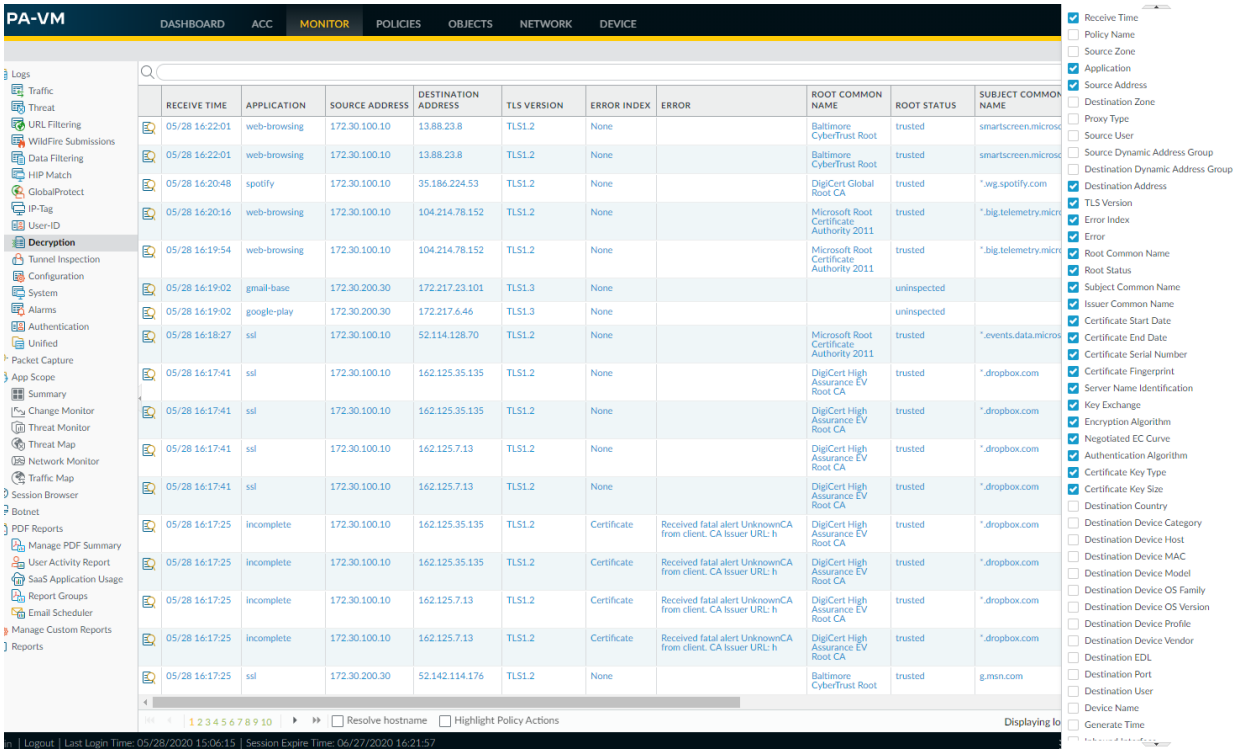
转发代理流量的数据取决于 TLS 握手是否成功。对于失败的 TLS 握手，防火墙将发送导致错误出现的事务支路的错误数据，即客户端到防火墙或防火墙到服务器。对于成功的 TLS 握手，发送的数据则是来自首先成功完成的支路，通常是客户端到防火墙。

解密日志不支持 *SSH* 代理流量。此外，证书信息也不可用于会话恢复日志。

防火墙默认记录所有失败的 TLS 握手流量。您还可以选择记录成功的 TLS 握手流量。您最多可以查看 62 列日志信息，例如，应用程序、SNI、解密策略名称、错误索引、TLS 版本、密钥交换版本、加密算法、证书密钥类型等许多其他特征：



© 2019 Palo Alto Networks, Inc.




单击放大镜图标 (🔍) 以查看会话的详细日志视图。

解密日志从流量日志中学习每个会话的 *App-ID*，因此，要在解密日志中查看 *App-ID*，必须先启用流量日志。如果流量日志被禁用，*App-ID* 将显示为 *incomplete*（不完整）。例如，大部分 *GlobalProtect* 流量都是区域内流量（不可信区域到不可信区域），但是，默认区域内策略不会启用流量日志。若要查看 *GlobalProtect* 区域内流量的 *App-ID*，必须启用区域内流量的流量日志。

对于长会话，防火墙可能会在流量日志完成前生成解密日志（流量日志通常在会话结束时生成），这也会导致 *App-ID* 显示为 *incomplete*（不完整）。在这些情况下，*App-ID* 不可用于解密日志。此外，一旦 *TLS* 握手失败并生成错误日志，该失败将使会话在防火墙确定 *App-ID* 之前终止，从而使 *App-ID* 不可用。在这些情况下，应用程序可能会显示为 *ssl* 或 *incomplete*（不完整）。

要解决问题，请使用解密 ACC 小部件（**ACC** > **SSL Activity**（**SSL** 活动））标识导致解密问题的流量，然后使用解密日志和自定义解密报告模板深入了解详细信息。

转发解密日志进行存储时，因为解密日志包含敏感信息，请务必安全地传输和存储日志。

一旦启用解密日志，防火墙会将 *HTTP/2* 日志作为隧道检测日志发送（禁用解密日志后，*HTTP/2* 日志将作为流量日志发送），因此，必须检查隧道检测日志，而不是 *HTTP/2* 事件的流量日志。此外，还必须启用隧道内容检测以获取 *HTTP/2* 流量的 *App-ID*。

- 配置解密日志记录
- 修复不完整的证书链
- 解密日志错误、错误索引和位掩码

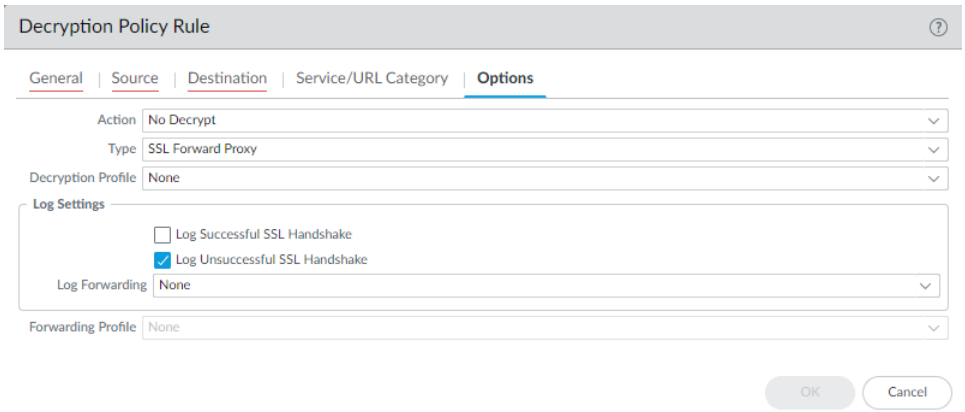
## 配置解密日志记录

防火墙生成用于受解密策略管控的会话的解密日志，包括带“不解密”策略的会话。在用于控制您想记录的流量的解密策略中配置解密日志记录。


© 2019 Palo Alto Networks, Inc.

STEP 1 | 配置要登录到解密策略的解密流量（**Policies**（策略）> **Decryption**（解密））。

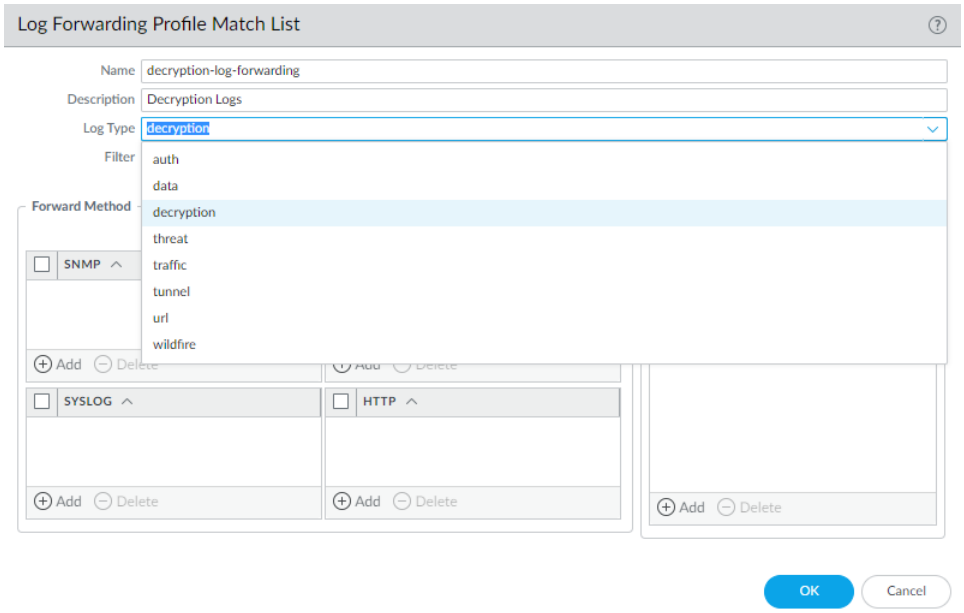
防火墙默认只记录失败的 TLS 握手：




通过记录成功握手和失败握手，可尽可能多地查看设备可用资源允许的解密流量（不要解密私有或敏感流量；遵循解密最佳实践并尽可能多地解密流量）。

STEP 2 | 创建日志转发配置文件以将解密日志转发到日志收集器、其他存储设备或特定管理员，然后在解密策略 **Options**（选项）选项卡的 **Log Forwarding**（日志转发）字段中指定配置文件。

若要转发解密日志，必须配置日志转发配置文件（**Objects**（对象）> **Log Forwarding**（日志转发））以指定解密 **Log Type**（日志类型）和 日志转发方法。



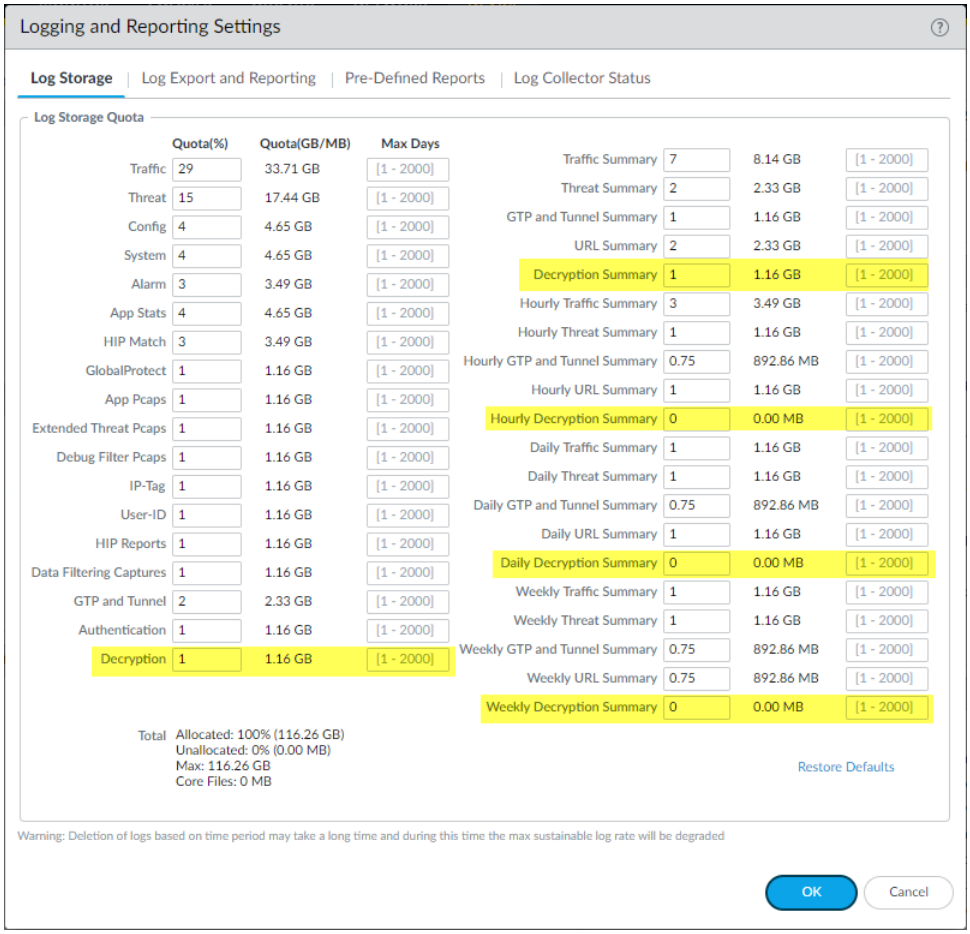

如果想转发解密日志，必须安全存储这些日志，因为其中包含敏感信息。

STEP 3 | 如果您不仅记录了成功的 TLS 握手，还记录了失败的 TLS 握手，请为防火墙的解密日志配置一个更大的日志存储空间配额（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（记录和报告设置）> **Log Storage**（日志存储））。

默认配额（分配）是设备日志存储容量的 1%（针对解密日志），常规解密摘要的 1%。没有分配默认的每小时、每天或每周解密摘要值。



© 2019 Palo Alto Networks, Inc.




解密日志所需的存储量由多种因素决定，而这又取决于您的部署。例如，请考虑以下因素：

- 通过防火墙的 TLS 流量。
- 解密的 TLS 流量。
- 其他日志的使用情况（评估应将哪个日志容量分配给解密日志）。
- 如果同时记录成功的和失败的 TLS 握手，那么，需要的容量可能就比只记录失败的 TLS 握手时所需的容量大很多。根据所解密的流量，解密日志占用的容量可能与流量日志或威胁日志需要的容量差不多，且在设备容量已完全订阅的情况下，可能需要进行权衡。

所分配的日志配额总和不能超过防火墙可用日志资源的 *100%*。

您可能需要进行试验，尝试找出适用于特定部署中各个日志类别的正确配额。如果只记录失败的握手，可以从默认值开始，或是将分配值提高两三个百分点。如果需要同时记录成功和失败的握手，可能需要将分配给流量日志的容量分大约一半给解密日志。可以根据流量、业务以及监控要求来确定您希望将其容量分配给解密日志的日志类型。

## 解密日志错误、错误索引和位掩码

解密日志中的 **Error Index**（错误索引）列和 **Error**（错误）列分别提供了解密错误类别和详细信息相关的信息。您还可以在详细日志视图下的握手详细信息部分查看错误和错误索引信息（单击以查看任何日志条目）。解密日志 **Error Index**（错误索引）指示 8 个错误类别中的其中一个：


© 2019 Palo Alto Networks, Inc.

| 错误索引 | 错误（错误索引可能显示的错误） |
| --- | --- |
| 证书 | 错误包括证书无效、证书过期、客户端证书不受支持、OCSP/CRL 检查吊销和失败、颁发机构 CA 不可信（不可信根签名的会话，其中包括不完整的证书链）以及其他证书错误。<br><br>如果防火墙因为站点未发送完整的证书链而缺少中间证书，您可以查找丢失的证书，并将其安装到 修复不完整的证书链。 |
| 密码 | 在下列情况下，会出现不受支持密码错误：<br>• 客户端尝试协商一个受防火墙支持的密码，但是流量不支持使用解密配置文件的密码。<br>• 客户端尝试协商一个防火墙不支持的密码。<br>• （罕见）已启用入站检查，且服务器功能与解密配置文件设置中的不匹配。<br>该错误消息包括不受支持的客户端密码位掩码值和不受支持的解密配置文件密码位掩码值。使用位掩码值标识客户端尝试使用的密码，并列出解密配置文件支持的密码值，具体在后文中详述。 |
| 功能 | 错误包括 TLS 握手过大或握手未知、证书链过大（超过 5 个证书）以及其他不受支持的功能。 |
| **HSM** | 硬件存储模块 (HSM) 错误包括未知请求、未在配置中找到项目、请求超时以及其他 HSM 错误和故障。 |
| 协议 | 错误包括 TLS 握手失败、私钥和公钥不匹配、Heartbleed 错误、TLS 密钥更换失败以及其他 TLS 协议错误。一旦服务器不支持客户端支持的协议、服务器使用防火墙不支持的证书类型，以及出现常见的 TLS 协议错误，就会出现协议错误。 |
| 资源 | 错误包括缺少足够的内存。 |
| 恢复 | 与恢复会话 ID 和票证、恢复防火墙缓存中会话条目相关的会话恢复错误，以及其他会话恢复错误。 |
| 版本 | 错误包括客户端和解密配置文件版本不匹配以及客户端和服务器版本不匹配。<br>错误消息包括用于标识受支持客户端和解密配置文件版本的位掩码值。使用位掩码值标识客户端尝试使用的密码，并列出解密配置文件支持的密码值，具体在后文中详述。 |

如果错误不存在合适的错误说明类别，则默认消息为 *General TLS protocol error*（常见的 *TLS* 协议错误）。

版本和密码日志错误包括您使用可操作的 CLI 命令将其转换至实际值的位掩码值：

- 版本错误位掩码值用于标识客户端和服务器使用的 TLS 协议版本之间的不一致，以及客户端与应用到流量的解密配置文件之间的 TLS 协议不匹配。用于转换版本错误位掩码的 CLI 命令为：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version <bitmask-value>
```

  该命令可传回与与位掩码匹配的 TLS 版本。
- 密码错误位掩码值用于标识加密以及客户端与应用到流量的解密配置文件之间的其他不匹配。



© 2019 Palo Alto Networks, Inc.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher <bitmask-value>
```

该命令可使密码返回到与位掩码匹配的版本。

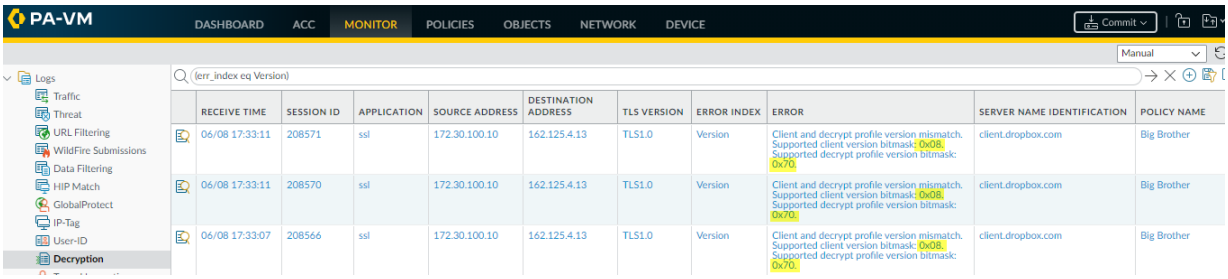
筛选解密日志以查找版本和密码错误，将带错误的会话位掩码值插入到适当的 CLI 命令中，获取导致错误的协议版本或密码值，并使用该信息更新您想允许访问相关站点的解密策略或配置文件。

- 版本错误
- 密码错误
- 根状态“未检查”

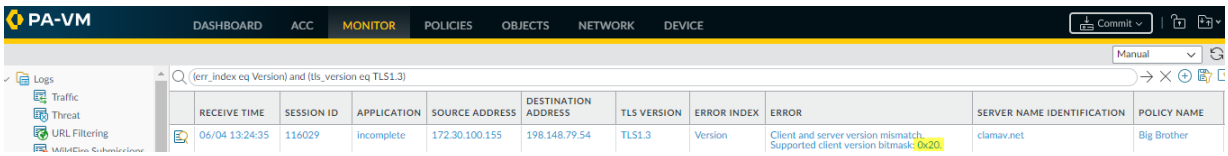
版本错误

要标识并修复版本不匹配错误，请：

1. 使用筛选器 **(err_index eq Version)** 筛选解密日志以标识版本错误。高亮显示的值是位掩码值：




您可以通过多种方式筛选解密日志。例如，若要只查看 TLSv1.3 版本错误，请使用筛选器 **(err_index eq Version)** 和 **(tls_version eq TLS1.3)**：




2. 登录到 CLI 并查找位掩码值。第一个屏幕截图中的版本错误（所有三个会话出现的错误相同）显示客户端与解密配置文件不匹配 — 受支持的客户端版本位掩码是 0x08，而受支持的解密配置文件版本位掩码是 0x70：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

此输出显示，客户端仅支持 TLSv1.0。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```



© 2019 Palo Alto Networks, Inc.

```
TLSv1.3
```

此输出显示，解密配置文件支持 TLSv1.1、TLSv1.2 和 TLSv1.3，但不支持 TLSv1.0。现在您已经知道引起错误的问题是：客户端仅支持非常老旧的 TLS 协议版本，而附加到用于控制流量的解密策略规则的解密配置文件不允许 TLSv1.0 流量。

接下来要做的就是确定采取哪些操作。您可以更新客户端，这样，客户端就能接受更安全的 TLS 版本。如果客户端出于某些原因需要使用 TLSv1.0，那么，您可以让防火墙继续阻止流量，或是您可以更新解密配置文件以允许所有 TLSv1.0 流量（不建议），或是您可以创建允许 TLSv1.0 的解密策略和配置文件，并将其仅用于必须使用 TLSv1.0 但又不支持更安全协议的客户端设备（允许流量的最安全选项）。

第二个屏幕截图中显示的是另一种错误，即客户端和服务端版本不匹配。错误显示，受支持的客户端位掩码是 0x20：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x20
```

```
TLSv1.2
```

输出显示，客户端仅支持 TLSv1.2。因为服务器不支持 TLSv1.2，可能只支持 TLSv1.3 或只支持 TLSv1.1 或更低版本（安全性较低的协议）。您可以使用 Wireshark 或其他数据包分析工具找出服务器支持的 TLS 版本。根据服务器支持的版本，您可以执行以下操作：

- 如果服务器只支持 TLSv1.3，您可以编辑解密配置文件，使其支持 TLSv1.3。
- 如果服务器只支持 TLSv1.1 或更低版本，请评估您出于业务原因是否需要访问此服务器。如果不需要，请阻止流量，提高安全性。如果您出于业务原因需要访问此服务器，请创建或添加服务器到仅会应用于您出于业务原因而需要访问的服务器和站点的解密策略；不得允许访问使用安全性更低的 TLS 版本的所有服务器。

3. 要找到用于控制会话流量的解密策略，请勾选日志中的 **Policy Name**（策略名称）列（或是单击解密日志旁边的放大镜图标以查看“详细日志视图”的“常规”部分中的信息）。在上面的示例中，解密策略名称为 Big Brother。为找到解密策略和配置文件，请前往 **Policies**（策略）> **Decryption**（解密），选择名为 Big Brother 的策略，然后选择 **Options**（选项）选项卡。**Decryption profile**（解密配置文件）中显示解密配置文件的名称。

   前往 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件），选择相应的解密配置文件，并进行编辑以解决版本问题。

密码错误

使用解密日志查找密码错误的方式类似版本错误 — 通过筛选日志查找错误，获取错误位掩码。然后，您可以前往 CLI，将位掩码转换为错误值，再采取适当的操作解决此问题。例如：

1. 使用筛选器 **(err_index eq Cipher)** 筛选解密日志以标识密码错误。例如，让我们来检查一个错误消息为“密码不受支持”的密码错误。受支持的客户端密码位掩码为：0x80000000。受支持的解密配置文件密码位掩码为 0x60f79980。
2. 登录到 CLI 并查找位掩码值：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher 0x80000000
```

```
CHACHA_PLY1305_SHA256
```

此输出显示，客户端尝试协商一个防火墙支持的密码（如果位掩码全部为零 (0x0000000)，那么，客户端将尝试协商一个防火墙不支持的密码）：



© 2019 Palo Alto Networks, Inc.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher 0x80000000
```

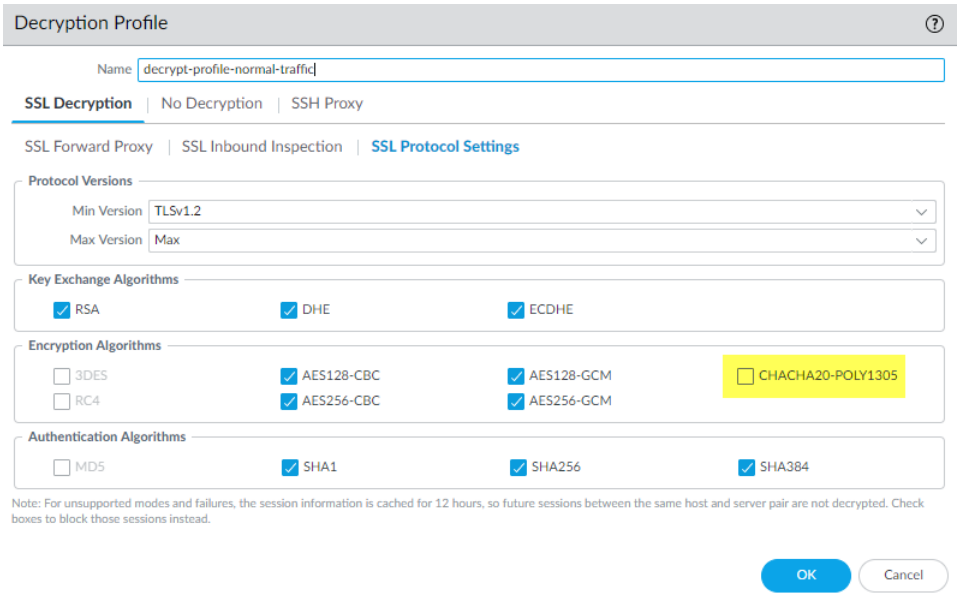
```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS13_WITH_AES_256_GCM_SHA384
TLS13_WITH_AES_128_GCM_SHA256
```

此输出显示，用于控制流量的解密配置文件支持很多密码，但不支持客户端尝试使用的密码。

为解决此问题以便防火墙允许和解密流量，您需要在解密配置文件中添加对缺失密码的支持。

3. 检查解密日志或详细日志视图 **Policy Name**（策略名称）以获取用于控制流量的解密策略的名称。前往 **Policies**（策略）> **Decryption**（解密），然后选择策略。在 **Options**（选项）选项卡上，查找解密配置文件的名称。接下来，前往 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件），选择相应的解密配置文件，并进行编辑以解决版本问题。

   在此例中，解密配置文件不支持密码 TLS13_WITH_CHACHA_POLY1305_SHA256，因此，客户端无法连接：




   为解决这一问题，请选择 **CHACHA20-POLY1305**加密算法选项（ **Max**（最大值）的**Max Version**（最高版本）设置表明，配置文件已支持 TLSv1.3，且身份验证算法设置已包括 SHA256，因此，仅加密算法支持缺失），然后 **Commit**（提交）配置。提交配置后，解密配置文件将支持缺失密码，流量解密会话也会成功。

   如果防火墙不支持密码套件，而您出于业务目的需要允许流量，请创建仅应用到该流量的解密策略和配置文件。在解密配置文件中，禁用 *Block sessions with unsupported cipher suites*（阻止具有不受支持加密套件的会话）选项


© 2019 Palo Alto Networks, Inc.

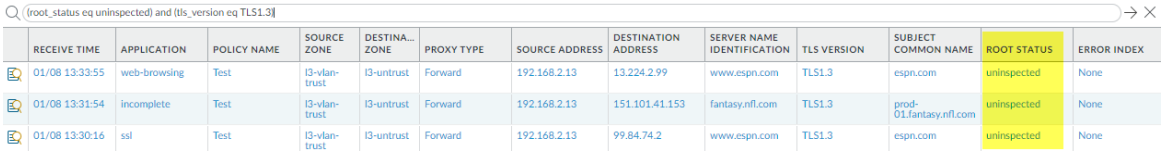
。

根状态“未检查”

在某些情况下，**Root Status**（根状态）列会显示值 **uninspected**（未检查）。防火墙无法检查根状态的原因有很多，包括：

- 会话恢复。
- 由于流量受“不解密”策略控制而不进行解密，因此，防火墙不会解密流量。
- 在防火墙可以检查服务器证书之前发生解密失败。

筛选解密日志 **(root_status eq uninspected) and (tls_version eq TLS1.3)** 以查看根状态未检查的解密会话：




## 修复不完整的证书链

并不是所有网站都会发送完整的证书链，即使是 RFC 5246 TLSv1.2 标准，也会要求经过身份验证的服务器提供一个指向可接受证书颁发机构的有效证书链。一旦启用解密，并在解密策略中应用可启用 **Block sessions with untrusted issuers**（阻止不可信颁发机构会话）的转发代理解密配置文件，如果网站服务器向防火墙提交的证书列表中缺少中间证书，则防火墙无法构建顶部（根）证书的证书链。在这些情况下，因为防火墙无法构建根证书链，且缺少中间证书，无法建立信任，因此，防火墙向客户端呈现的是不可信的转发证书。

防火墙仅在其默认可信证书颁发机构存储中有根证书。

如果您出于业务目的而需要通信的网站有一个或多个中间证书缺失，且解密配置文件阻止不可信颁发机构会话，那么，您可以找到并下载缺失的中间证书，并将其作为可信根 CA 安装在防火墙上，这样，防火墙就可以信任网站的服务器。（或者，您可以联系网站所有者，要求他们配置器服务器，这样，就可在握手时发送中间证书。）

如果在解密配置文件中允许不可信颁发机构会话，即使颁发机构不可信，防火墙也会建立会话；但是，最佳做法是阻止不可信颁发机构会话，以提高安全性。

STEP 1 | 查找导致不完整证书链错误的网站。

1. 筛选解密日志以标识因为不完整证书链导致失败的解密会话。

   在筛选器字段，输入查询 **(err_index eq Certificate) and (error contains 'http')**。该查询筛选包含字符串“http”的证书错误日志，这会查找所有包含 CA 颁发机构 URL（通常称为 URI）的错误条目。CA 颁发机构 URL 提供 CA 颁发机构的授权信息访问 (AIA) 信息。

2. 单击 **Error**（错误）列中以“Received fatal alert UnknownCA from client.CA Issuer URL:”（从客户端接收致命警报 UnknownCA。CA 颁发机构 URL：）开头且后跟 URI 的条目。

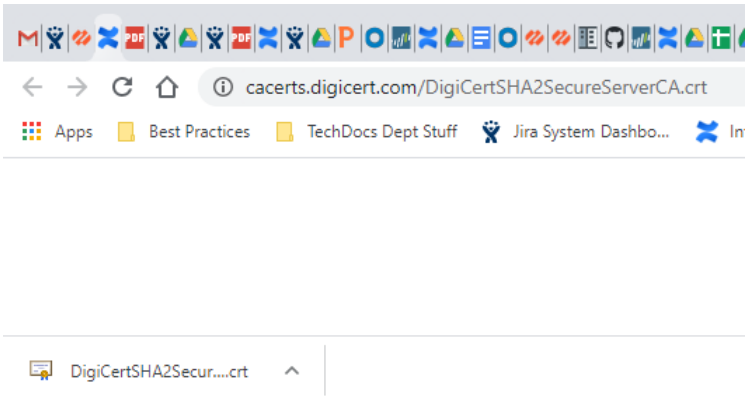
   
   

   防火墙自动将选择的错误添加到查询，并显示完整的 URI 路径（完整的 URI 在 **Error**（错误）列中被截断）。

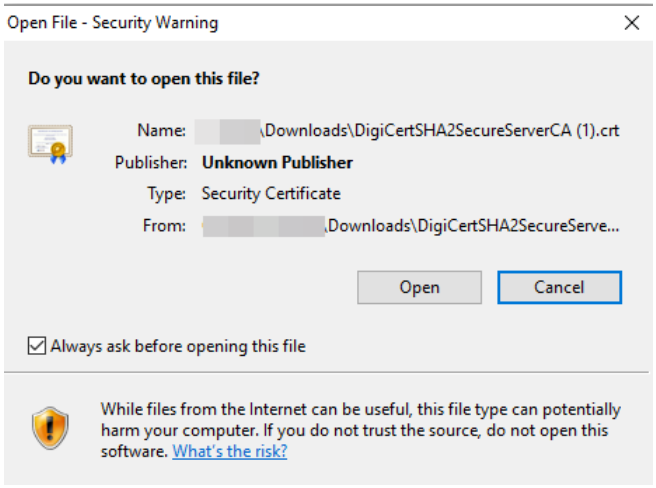
STEP 2 | 复制并粘贴 URI 到您的浏览器，然后按 Enter 键以下载缺失的中间证书。



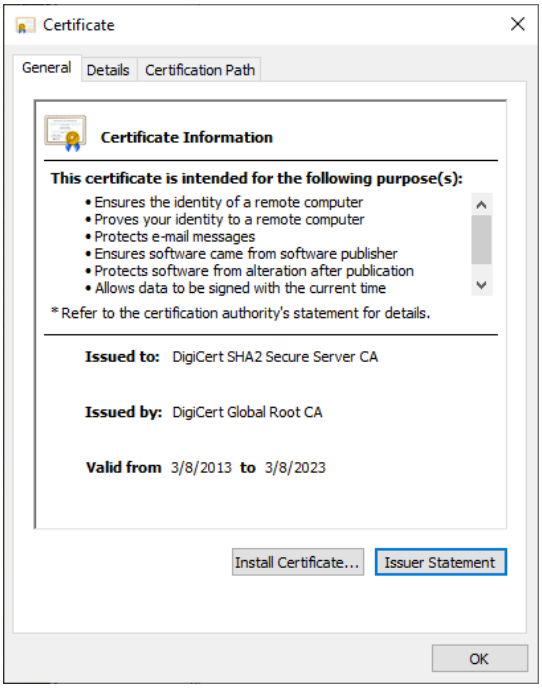
© 2019 Palo Alto Networks, Inc.




STEP 3 | 单击证书以打开对话框。



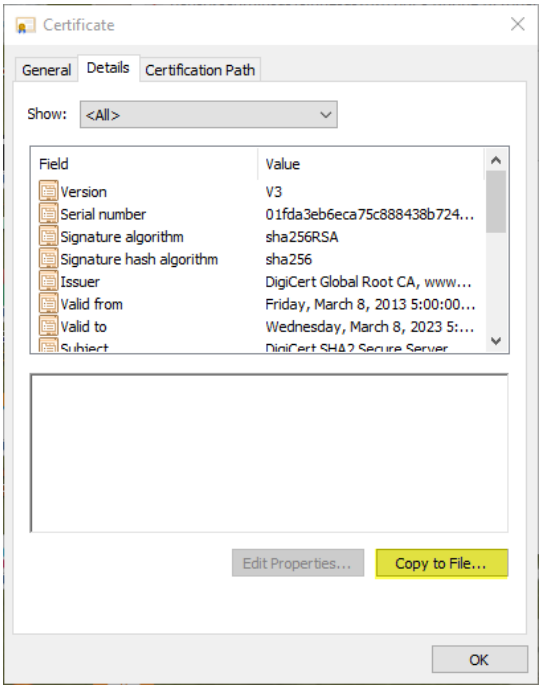

STEP 4 | 单击 **Open**（打开）以打开证书文件。





© 2019 Palo Alto Networks, Inc.

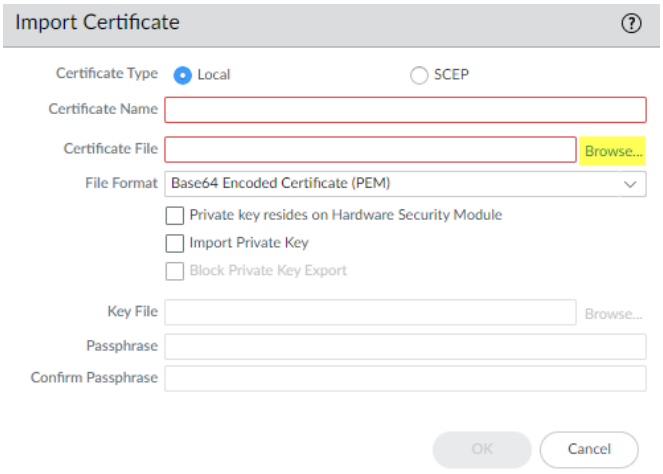
STEP 5 | 选择 **Details**（详细信息）选项卡，然后单击 **Copy to File...**（复制到文件...）。




按照导出说明操作。证书随后将复制到您指定作为默认下载文件夹的文件夹。

STEP 6 | 将证书导入到防火墙。

1. 导航至 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书），然后选择 **Import**（导入）。
2. **Browse**（浏览）至您存储缺失的中间证书的文件夹，然后选择该文件夹。将 **File Format**（文件格式）保留为 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）。



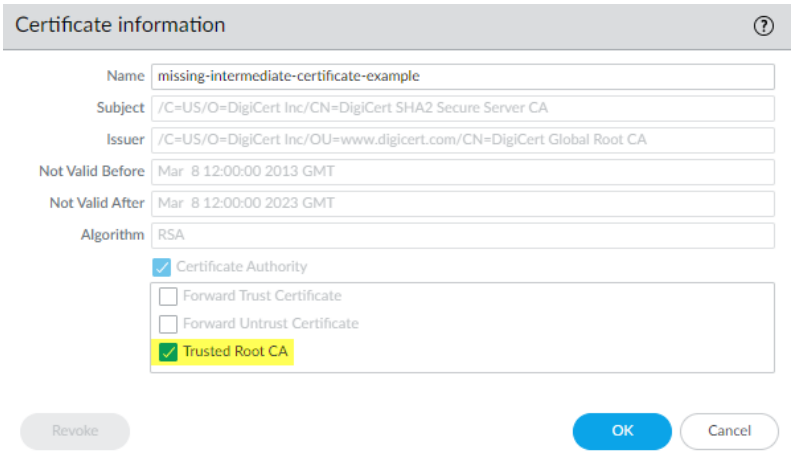

3. 给证书命名，然后指定您想使用的其他任何选项，并单击**OK**（确定）。

STEP 7 | 导入证书时，从 **Device Certificates**（设备证书）列表中选择证书以打开证书信息对话框。

STEP 8 | 选择 **Trusted Root CA**（可信根 **CA**）以将防火墙上的证书标记为可信根 CA，然后单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.




在**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）中，导入的证书此时将出现在证书列表中。检查 **Usage**（使用情况）列，以确认状态为 **Trusted Root CA Certificate**（可信根 CA 证书），从而验证防火墙是否将该证书视为可信根 CA。

STEP 9 | **Commit**（提交）配置。

STEP 10 | 您现在可以修复损坏的证书链。

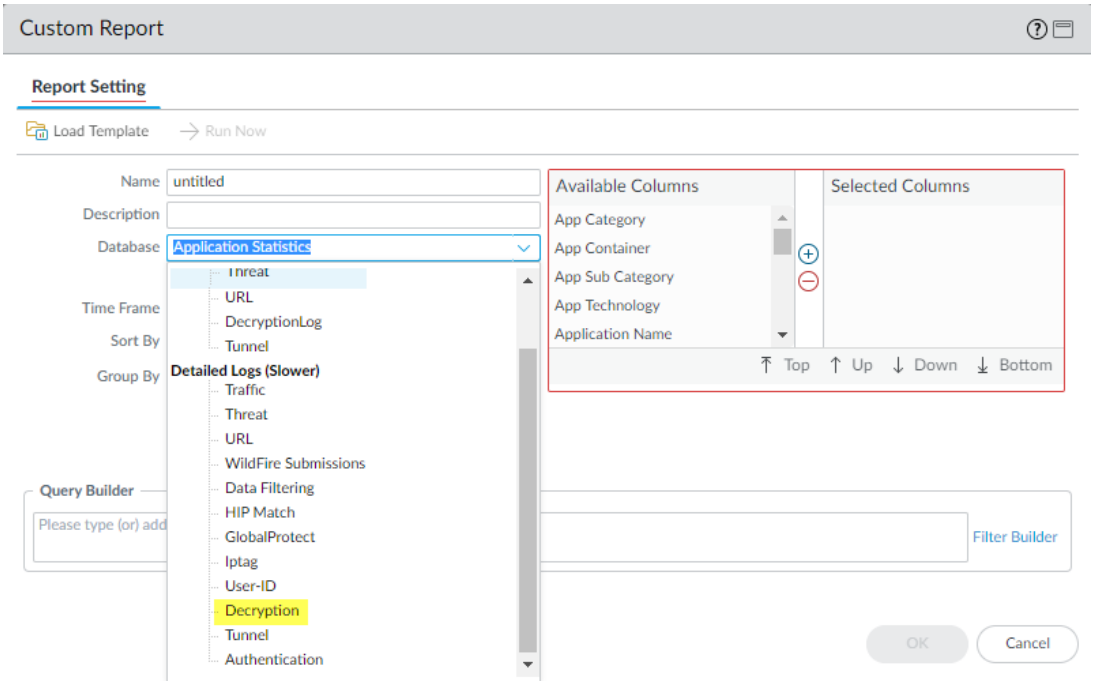
由于该 CA 颁发机构已可信，因此，防火墙不会阻止流量。对所有缺失的中间证书重复此过程，以修复他们的证书链。

# 自定义解密报告模板

您可以根据解密日志中的字段和自定义模板创建自定义报告，并为解密事件生成自定义报告。选择包含在自定义报告中的日志字段，并选择用于细化日志查询的模板：

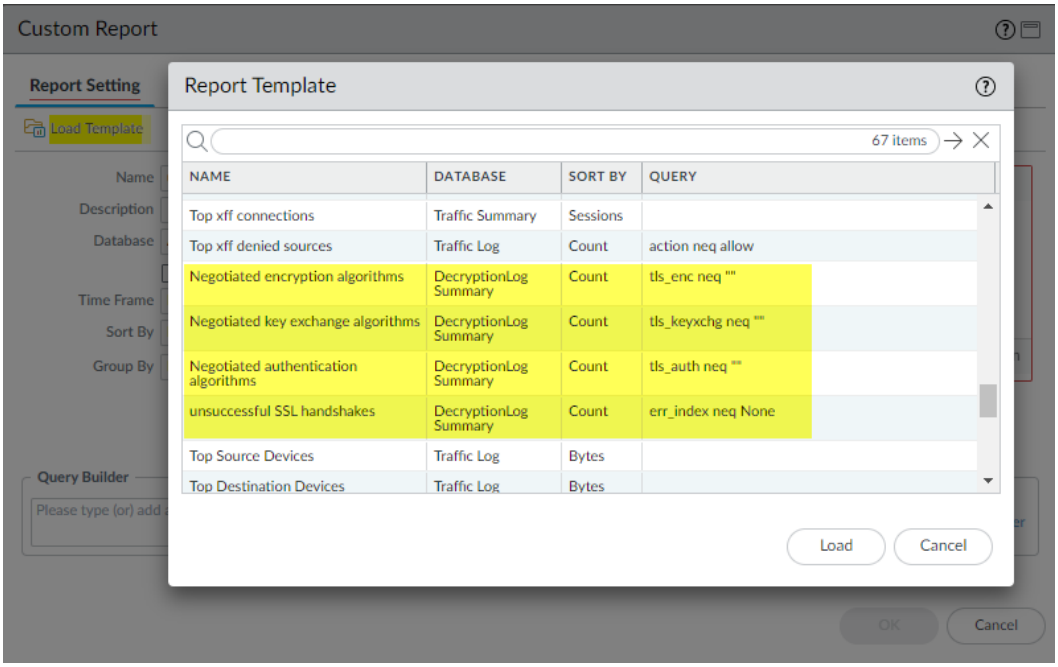
1. **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告）。
2. **Add**（添加）自定义报告。
3. 若要配置用于自定义报告的解密日志字段，请选择 **Decryption**（解密）作为**Database**（数据库）。


© 2019 Palo Alto Networks, Inc.




更改 **Available Columns**（可用列）列表，以便与解密日志中可用的列匹配。选择并添加您想包含在自定义报告中的列（信息）。如果不想进一步细化自定义报告，请单击 **OK**（确定）以生成报告。

4. 如果需要进一步细化，请使用查询生成器和 PAN-OS 10.0 中引入的 4 个模板完善自定义揭秘报告的输出。若要选择用于筛选报告输出的模板，请单击 **Load Template**（加载模板），并从 4 个解密模板中进行选择：




**Query**（查询）列显示各个模板呈现的筛选查询。**Load**（加载）所需查询，然后单击**OK**（确定）以生成自定义报告。



© 2019 Palo Alto Networks, Inc.

## 按代理类型和 TLS 版本划分的不受支持的参数

解密日志字段显示各个解密代理类型的解密会话参数。但是，考虑到版本支持、TLS 握手加密部分、信息可用性等原因，一些参数可能不能用于所有代理类型或 TLS 版本。下表显示的是按代理类型和 TLS 版本划分的不受支持的解密日志参数。

| 代理类型 | 不受支持的参数 | TLS 版本 |
|---|---|---|
| 转发代理 | 协商的 EC 曲线 | TLSv1.3 |
| 入站检查 | 服务器名称指示<br>根通用名称 | 全部 |
| | 协商的 EC 曲线 | TLSv1.3 |
| 不解密（解密策略规则中的 **No Decrypt** 操作） | 协商的 EC 曲线<br>服务器名称指示 | TLSv1.2 |
| | 协商的 EC 曲线<br>服务器名称指示<br>证书信息（所有证书信息字段，例如，证书开始日期、证书结束日期、证书密钥类型等） | TLSv1.3 |
| 解密代理 | 协商的 EC 曲线 | TLSv1.3 |
| GlobalProtect 网络门户 | 服务器名称指示<br>根通用名称<br>解密策略名称<br>App-ID | 全部 |
| GlobalProtect 网关 | 服务器名称指示<br>解密策略名称<br>App-ID | 全部 |
| 无客户端 SSLVPN | 服务器名称指示 | 全部 |
| SSH | 不支持解密日志 | |
| 明文 | 不支持解密日志 | |

## 解密故障排除工作流程示例

应用程序命令中心 (ACC) 的解密日志和 “SSL 活动”小部件提供的解密故障排除工具功能强大，既可独立运行，又可组合运行。一旦您掌握了这些工具的使用方法，就能调查并解决各种解密问题。

以下示例显示的是如何使用故障排除工具标识、调查并解决解密问题。利用这些工具对您在解密部署时遇到的任何问题执行故障排除。

- 调查解密失败原因



© 2019 Palo Alto Networks, Inc.

- 对不受支持的密码套件进行故障排除
- 识别弱协议和密码套件
- 标识不可信的 CA 证书
- 对过期证书进行故障排除
- 对证书吊销问题进行故障排除
- 对固定证书进行故障排除

## 调查解密失败原因

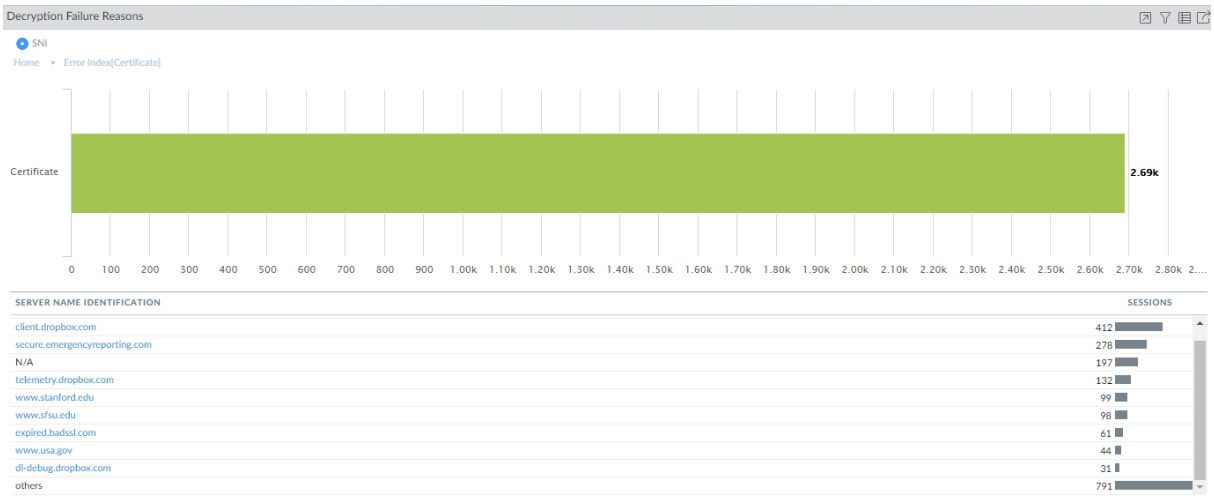
解密失败的最常见原因包括 TLS 协议错误、密码版本错误（客户端和服务器版本不匹配，且客户端和解密配置文件版本不匹配）和证书错误。要调查解密错误，首先使用应用程序命令中心 (ACC) 标识失败，然后前往解密日志，深入了解详细信息。

STEP 1 | 从 **ACC** > **SSL Activity**（**ACC SSL** 活动）中开始您的调查，并查找“解密失败原因”小部件。




在本例中，我们调查证书错误。您可以采用相同的过程来调查版本和协议错误。

STEP 2 | 单击 **Certificate**（证书）旁边的绿条，以查看发生过证书错误的主机 (SNI) 以及发生过大量证书错误的主机列表。




STEP 3 | 前往 **Monitor**（监控）> **Logs**（日志）> **Decryption**（解密）以深入了解日志。

使用查询 **(err_index eq Certificate)** 以筛选解密日志，从而查看发生过证书错误的所有解密会话。

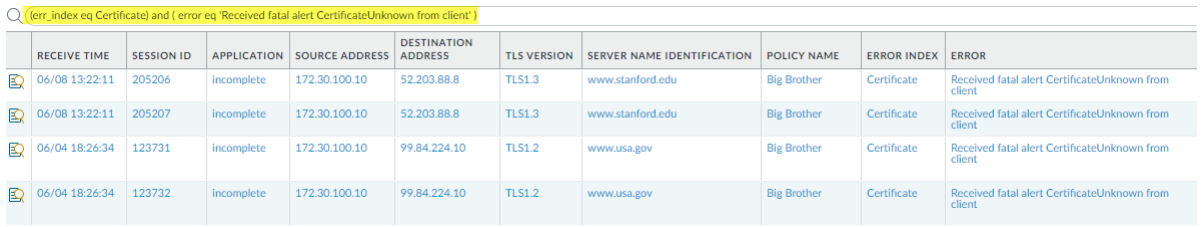


© 2019 Palo Alto Networks, Inc.


(err_index eq Certificate)

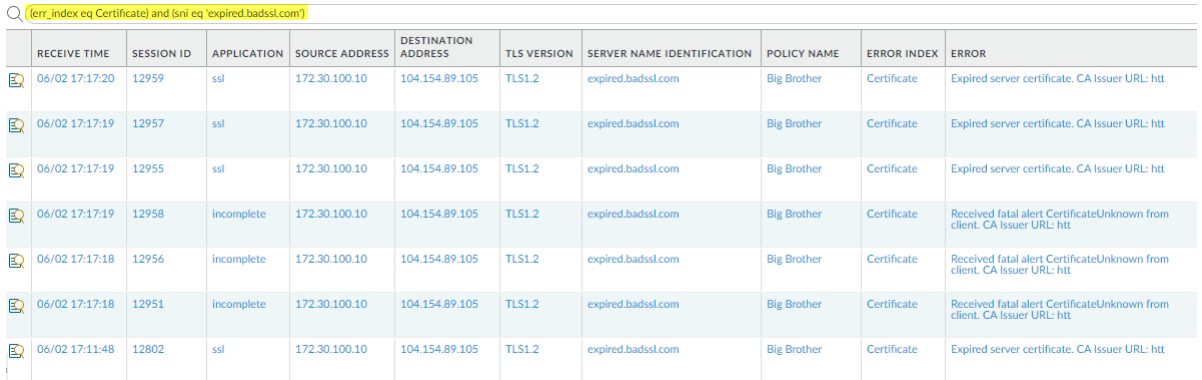
| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 13:22:11 | 205207 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/08 11:17:14 | 203671 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Expired server certificate. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:14 | 203669 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:11 | 203666 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:11 | 203663 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:16:18 | 203598 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:16:18 | 203576 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked |
| 06/08 11:16:18 | 203575 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked |
| 06/04 18:26:34 | 123731 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |

**Error**（错误）列显示证书错误原因。若要筛选曾出现过相同错误的所有解密会话，请单击错误消息，将其添加到查询，然后执行查询。例如，若要根据从客户端接收的致命警报查找所有错误，通过单击错误可生成查询 **(err_index eq Certificate) and (error eq 'Received fatal alert CertificateUnknown from client')**：


(err_index eq Certificate) and ( error eq 'Received fatal alert CertificateUnknown from client' )

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 13:22:11 | 205206 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/08 13:22:11 | 205207 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/04 18:26:34 | 123731 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/04 18:26:34 | 123732 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |

若要筛选特定主机接收到的证书错误，请添加该 SNI 到查询，而不是添加错误消息文本。例如，要查找 expired.badssl.comm 的所有证书错误，请使用查询 **(err_index eq Certificate) and (sni eq 'expired.badssl.com')**：


(err_index eq Certificate) and (sni eq 'expired.badssl.com')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/02 17:17:20 | 12959 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12957 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12955 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12958 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:17:18 | 12956 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:17:18 | 12951 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:11:48 | 12802 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |

**Error**（错误）列显示的是与 expired.badssl.com 关联的各个证书错误的具体原因。

一旦知晓导致解密失败的证书问题原因，就可以解决这一问题。例如，如果证书链不完整，您可以修复不完整的证书链。如果证书到期，您可以通知站点管理员，或是在您需要访问站点时创建基于策略的例外。

## 对不受支持的密码套件进行故障排除

在解密日志中识别并解决不受支持密码套件的问题是版本错误调查的一个方面，值得单独研究。

STEP 1 | 在解密日志中（**Monitor**（监控）> **Logs**（日志）> **Decryption**（解密））， 使用查询 **(error contains 'Client and decrypt profile mismatch'** 识别所有密码套件版本不匹配问题。



© 2019 Palo Alto Networks, Inc.

通过在日志筛选这些不匹配项，可以找出客户端和解密配置文件密码套件支持的版本不匹配的所有实例。

(error contains 'Client and decrypt profile version mismatch')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|
| 06/16 09:41:22 | 99445 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:22 | 99444 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99441 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99440 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |

若要找出曾出现过相同错误的所有解密会话，请单击错误消息，将其添加到查询，然后移除原始查询，例如：

( error eq 'Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. ' )

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|
| 06/16 09:41:22 | 99445 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:22 | 99444 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99441 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99440 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:51 | 99251 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:51 | 99250 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:46 | 99249 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:46 | 99248 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 08:41:21 | 98685 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |

采用十六进制代码识别客户端支持的具体版本和解密配置文件支持的具体版本。

STEP 2 | 登录到 CLI 并查找位掩码值。

该错误显示的是客户端和解密配置文件不匹配问题。受支持的客户端位掩码是 0x08，受支持的解密配置文件位掩码是 0x70：

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

此输出显示，客户端仅支持 TLSv1.0。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```



© 2019 Palo Alto Networks, Inc.

```
TLSv1.3
```

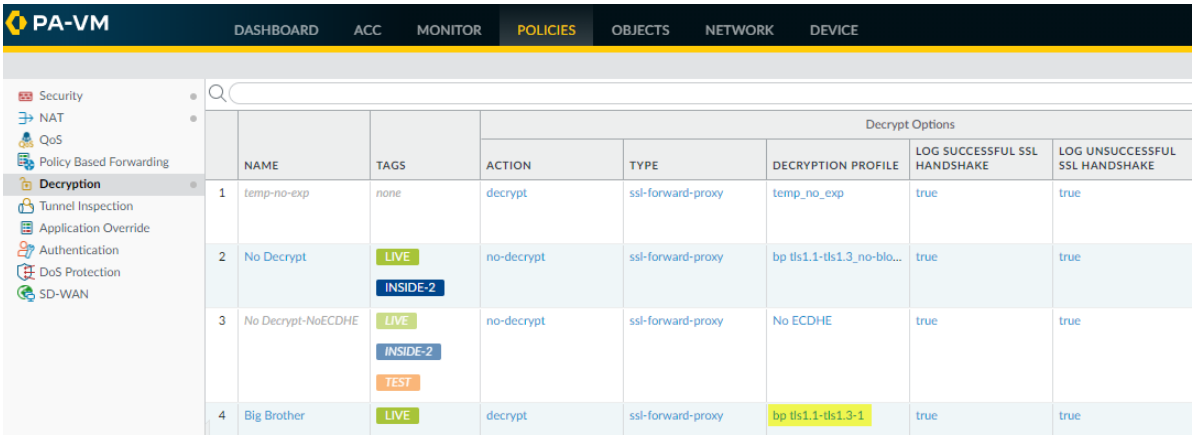
此输出显示，解密配置文件支持 TLSv1.1、TLSv1.2 和 TLSv1.3，但不支持 TLSv1.0。现在您已经知道客户端仅支持旧的 TLS 协议版本，而附加到用于控制流量的解密策略规则的解密配置文件不允许该版本。

STEP 3 | 确定要采取的操作。

您可以更新客户端，这样，客户端就能接受更安全的 TLS 版本。如果客户端出于某些原因需要使用 TLSv1.0，那么，您可以让防火墙继续阻止流量，或是您可以更新解密配置文件以允许所有 TLSv1.0 流量（不建议），或是您可以创建允许 TLSv1.0 的解密策略和配置文件，并将其仅用于必须使用 TLSv1.0 但又不支持更安全协议的客户端设备（允许流量的最安全选项）。

STEP 4 | 如果选择编辑解密配置文件，那么，要找到用于控制会话流量的解密策略，请勾选日志中的 **Policy Name**（策略名称）列（或是单击解密日志旁边的放大镜图标以查看“详细日志视图”的“常规”部分中的信息）。

1. 在此例中，解密策略名称为 Big Brother；要找出解密配置文件，请前往**Policies**（策略）> **Decryption**（解密），并检查 **Decryption Profile**（解密配置文件）列。



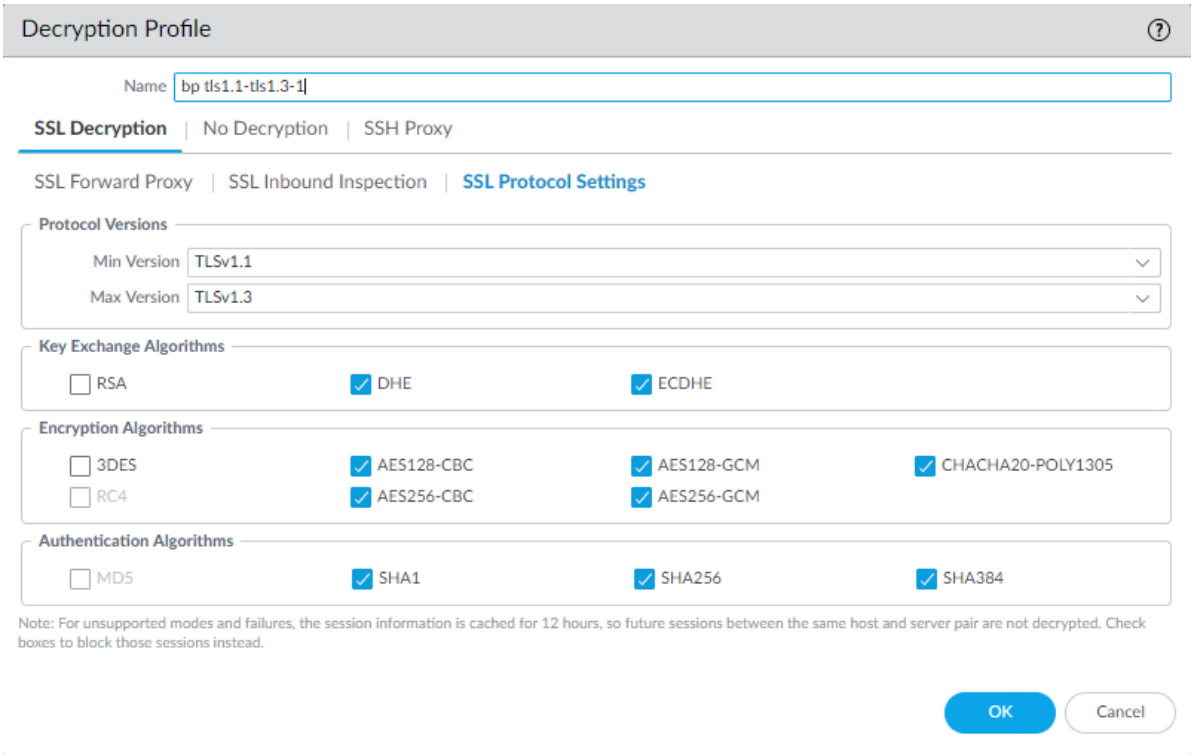

解密配置文件的名称为 **bp tls1.1-tls1.3-1**。您还可以选择 Big Brother 策略，然后选择 **Options**（选项）选项卡以查看解密配置文件的名称。

前往 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件），选择相应的解密配置文件，并进行编辑以解决版本问题。

2. 前往 **Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件）。

选择解密配置文件 **bp tls1.1-tls1.3-1**，然后单击 **SSL Protocol Settings**（**SSL** 协议设置）选项卡。


© 2019 Palo Alto Networks, Inc.




配置文件支持的最低 TLS 协议版本（**Min Version**（最低版本））是 TLSv1.1。若要允许因版本不匹配而阻止的流量，您可以将 **Min Version**（最低版本）更改为 TLSv1.0。但是，更安全的做法是更新客户端，使其使用最新的 TLS 协议版本。如果无法更新客户端，可以创建一个仅应用于该用户、设备或源地址（以及任何类似用户、设备或源地址）的解密策略和配置文件（这样，一个策略和配置文件就可以控制此类所有流量），而不是使用允许 TLSv1.0 流量的通用解密策略。

## 识别弱协议和密码套件

弱 TLS 协议以及弱加密套件（加密算法、身份验证算法、密钥交换算法和协商的 EC 曲线）会削弱您的安全状态，比强 TLS 协议和强加密套件更容易被不良操作者实施漏洞利用。

解密日志条目中的 5 个字段用于显示解密会话的协议和密码套件：

| TLS VERSION | ENCRYPTION ALGORITHM | KEY EXCHANGE | AUTHENTICATI... ALGORITHM | NEGOTIATED EC CURVE |
|---|---|---|---|---|
| TLS1.2 | AES_128_GCM | ECDHE | SHA256 | secp256r1 |
| TLS1.2 | AES_256_GCM | ECDHE | SHA384 | secp256r1 |

跟踪易受攻击的旧 TLS 版本和密码套件，这样，您就能针对是否允许与可能损害您的安全状态的服务器和应用程序进行连接做出明智的决策。

此主题的示例展示了如何：

- 识别使用安全性较低的 TLS 协议版本的流量。
- 识别使用特定密钥交换算法的流量。
- 识别使用特定身份验证算法的流量。
- 识别使用特定加密算法的流量。

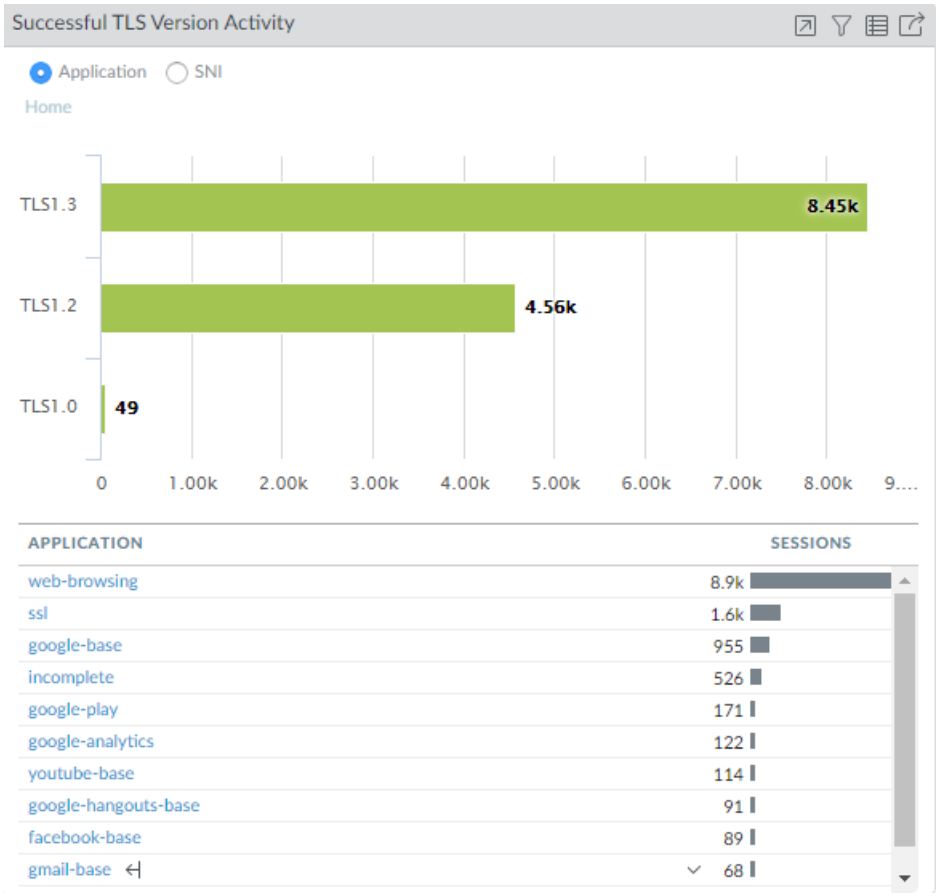
这些示例展示了如何通过各种方式使用解密故障排除工具，帮助您了解如何将这些工具用于对所遇到的任何解密问题执行故障排除。



© 2019 Palo Alto Networks, Inc.

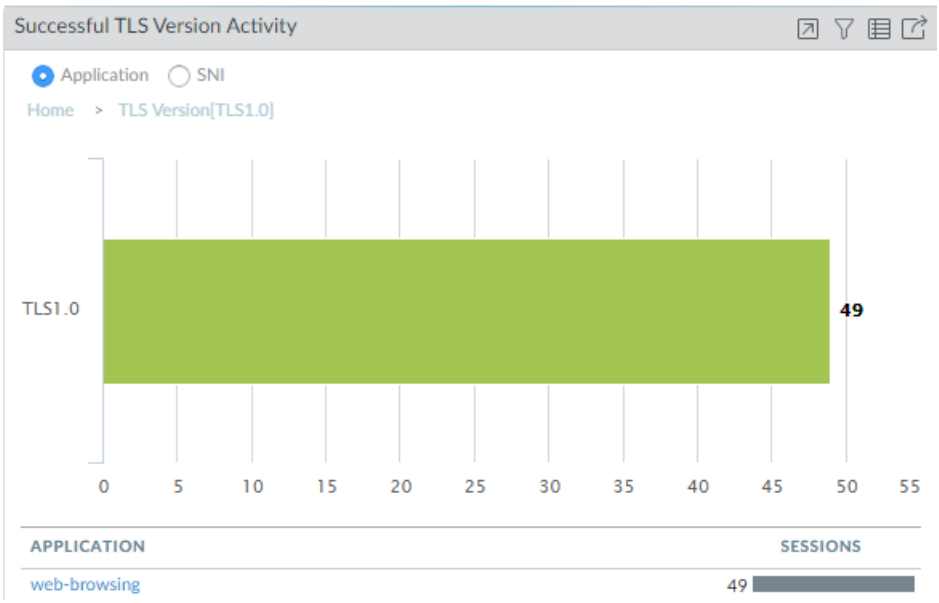
您可以使用 *Wireshark* 或其他数据包分析器仔细检查客户端或服务器是否引发问题、*TLS* 客户端和服务器版本以及其他密码套件信息。这有助于分析版本不匹配等问题。

- **TLS Protocols**（**TLS** 协议）— 识别使用较旧、安全性较低的 TLS 协议版本的流量，便于您评估是否允许访问使用弱协议的服务器和应用程序。
  1. 首先，请检查应用程序命令中心 (ACC)，查看防火墙是否允许弱协议（**ACC** > **SSL Activity**（**SSL** 活动）> **Successful TLS Version Activity**（成功的 **TLS** 版本活动）），并全面了解活动。




在本例中，大多数成功的 TLS 活动都是 TLSv1.2 和 TLSv1.3 活动。但是，也有一些允许 TLSv1.0 流量的实例。通过单击数字 **49** 深入了解 TLSv1.0 活动，并查看可以成功实现 TLSv1.0 连接的应用程序：


© 2019 Palo Alto Networks, Inc.

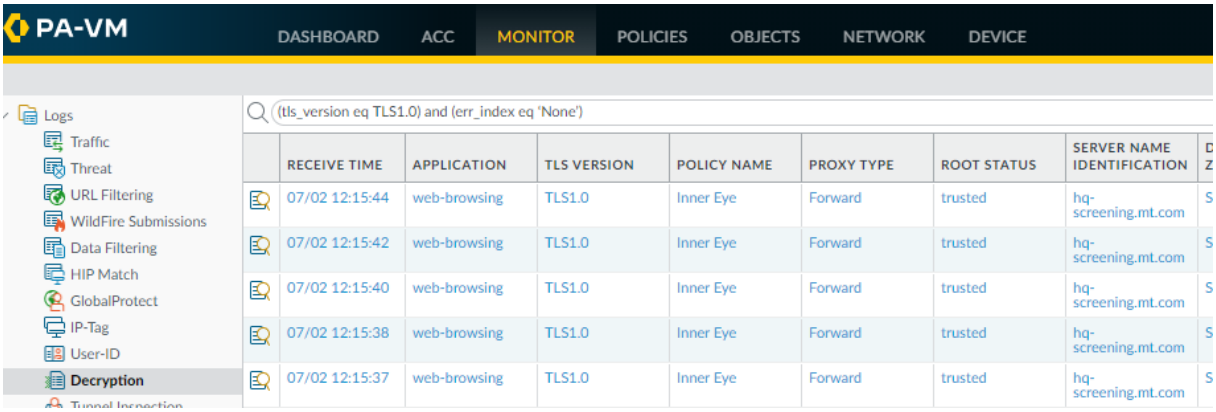



我们发现，防火墙允许标识为 Web 浏览流量的流量。为进一步了解什么是 TLSv1.0 Web 浏览流量以及为什么要允许此流量，我们接下来将转到解密日志。

2. 筛选解密日志以查看 TLSv1.0 活动详细信息。

   使用查询 **(tls_version eq TLS1.0) and (err_index eq 'None')** 以显示成功的 TLSv1.0 解密会话。

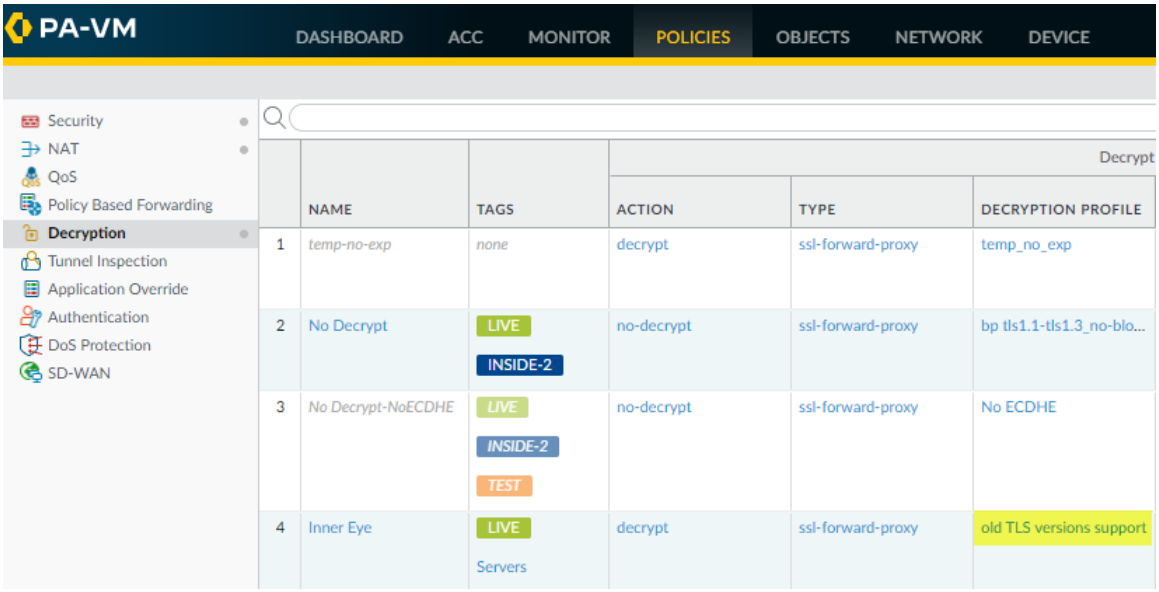
   仅当您在解密策略中启用了当配置解密日志记录时记录成功 *TLS* 握手的情况下，解密日志才会显示成功的 *TLS* 活动。如果禁用"记录成功的 *TLS* 握手"，您将无法查看此信息。



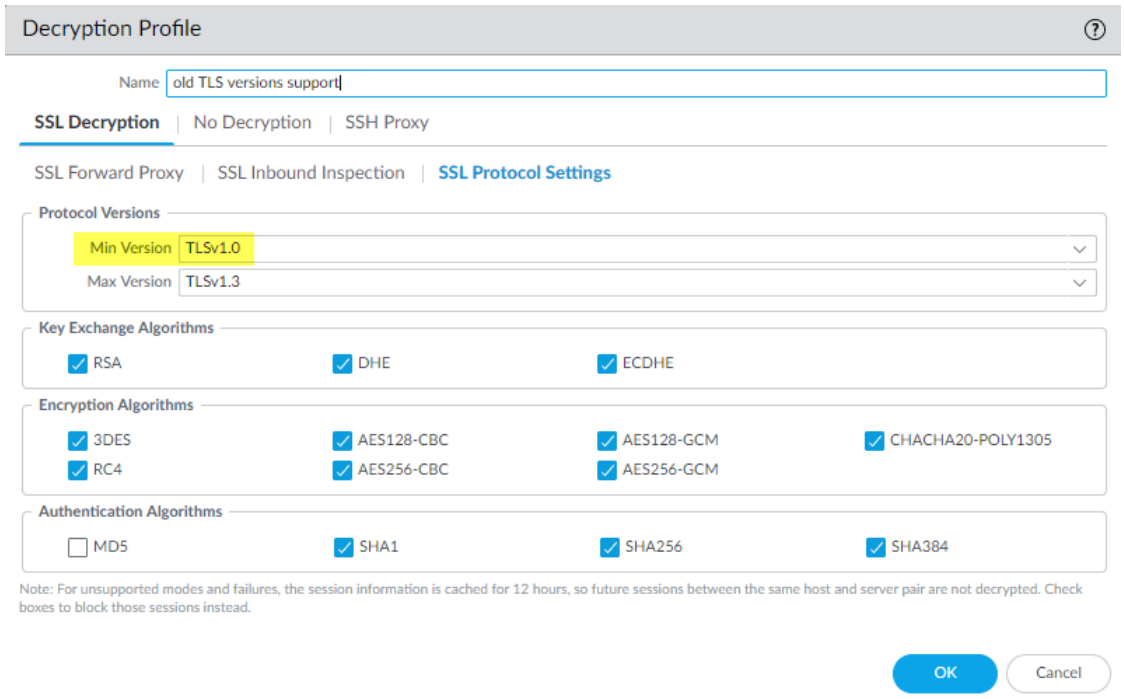

解密日志中显示，用于控制流量的解密策略名为 **Inner Eye**，主机名为 **hq-screening.mt.com**。知道使用 TLSv1.0 的站点后，我们可以检查解密策略（**Policies**（策略）> **Decryption**（解密）），找出用于控制流量的解密配置文件，并了解为什么该流量被允许：



© 2019 Palo Alto Networks, Inc.




我们发现，与策略关联的解密配置文件是 **old TLS versions support**（支持旧的 **TLS** 版本）。检查配置文件（**Objects**（对象）> **Decryption**（解密）> **Decryption Profile**（解密配置文件）），然后查看 SSL 协议设置以准确找出该配置文件允许的流量：




配置文件允许 TLSv1.0 流量。接下来要决定是要允许访问此站点（出于业务需要是否需要访问？）或者是否要阻止它。

另一种导致防火墙允许使用安全性较低协议的流量的常见情况是流量未解密。筛选 TLSv1.0 流量的解密日志时，如果**Proxy Type**（代理类型）列包含值 **No Decrypt**（不解密），那么，“不解密”策略就会控制该流量，这样，防火墙就不会解密或检测此流量。如果不想允许弱协议，请修改解密配置文件，以阻止 TLSv1.0 流量。

您可以通过多种方式筛选解密日志，从而找出使用弱协议的应用程序和站点，例如：

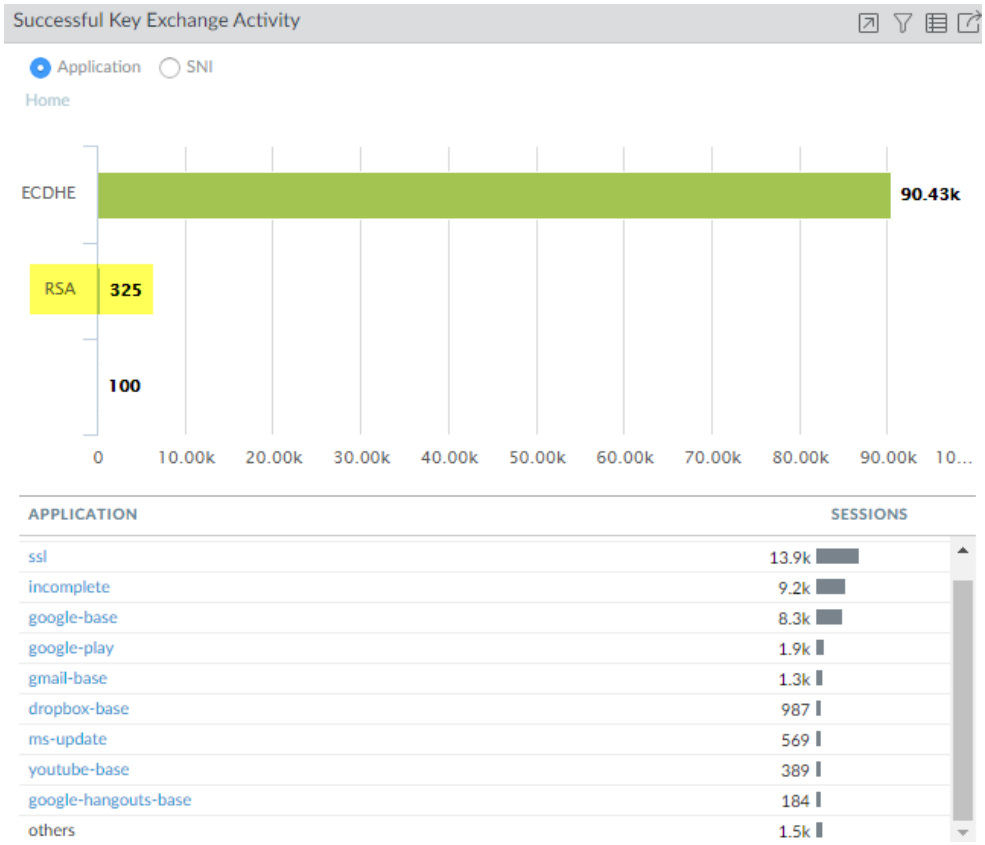

© 2019 Palo Alto Networks, Inc.

- 使用查询 **(tls_version eq TLS1.0)** 筛选成功和失败的 TLSv1.0 握手，而不仅是筛选成功的 TLSv1.0 握手。
- 使用查询 **(tls_version eq TLS1.0) and (err_index neq 'None')** 仅筛选成功的 TLSv1.0 握手。
- 使用查询 **(tls_version leq tls1.1)** 筛选所有安全性较低的协议（TLSv1.1 以及更高版本）。

如果想筛选其他 TLS 版本的日志，请将 **TLS1.0** 或 **TLS1.1** 更换为其他 TLS 版本。

3. 决定针对使用弱 TLS 协议的站点采取的操作。
   - 如果开展业务不需要访问该站点，最安全的做法通过编辑用于控制流量的解密策略和解密配置文件，阻止访问该站点。解密日志 **Policy Name**（策略名称）列显示了策略名称，人"解密策略"显示附加的解密配置文件（**Options**（选项）选项卡）。
   - 如果出于业务目的需要访问站点，请考虑创建仅应用于该站点（或应用于该站点和其他类似站点）的解密策略和解密配置文件，并阻止其他所有使用安全性较低的协议的流量。

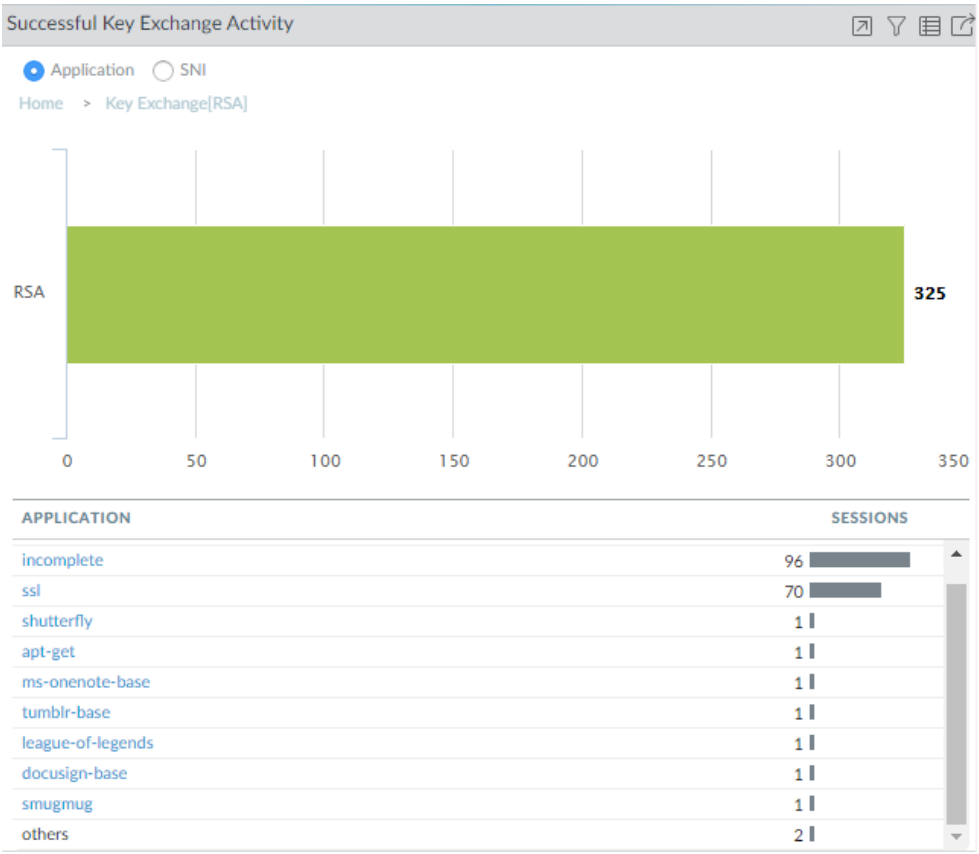
- **Key Exchange**（密钥交换）— 标识使用安全性较低的密钥交换算法的流量。
  1. 首先，请检查应用程序命令中心 (ACC)，查看防火墙允许的密钥交换算法（**ACC** > **SSL Activity**（**SSL** 活动）> **Successful Key Exchange Activity**（成功的密钥交换活动）），并全面了解活动。




大多数密钥交换都使用安全的 ECDHE 密钥交换算法。但是，有一些密钥交换会话也会使用安全性较低的 RSA 算法，而另一些会使用另一种密钥算法。例如，要开始调查使用 RSA 密钥交换的流量，请单击数字 **325** 以深入了解该数据。

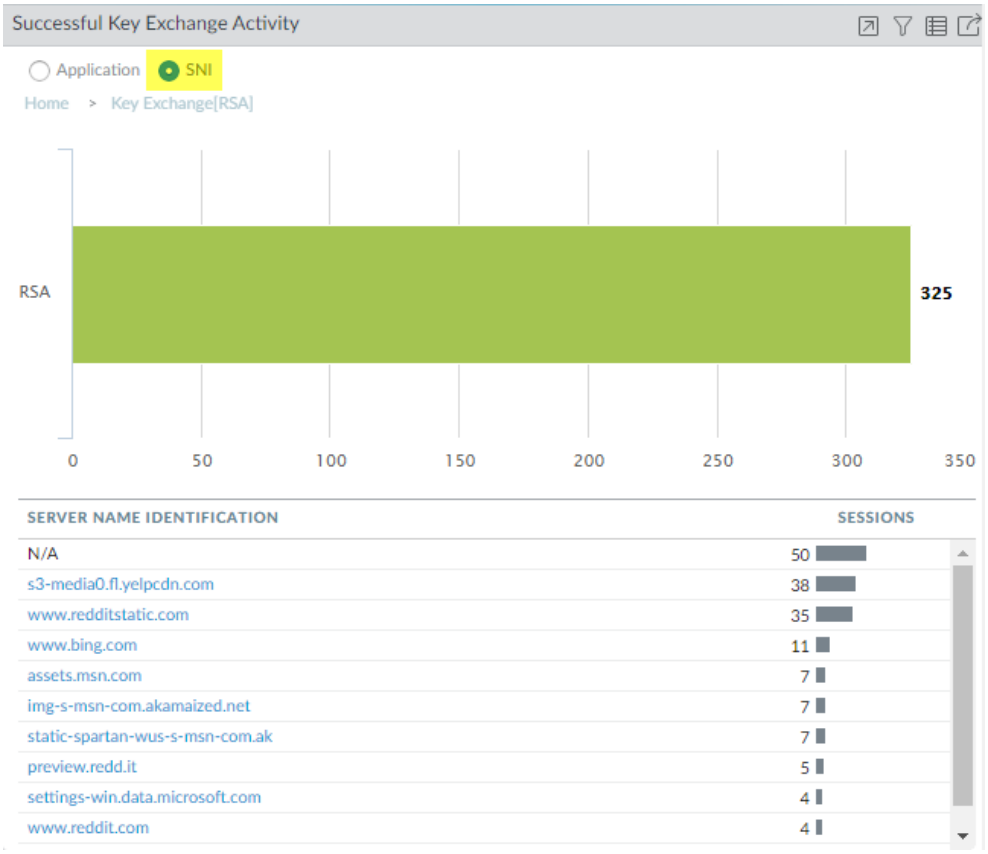


© 2019 Palo Alto Networks, Inc.




通过深入了解，将显示使用 RSA 密钥交换的应用程序。我们还可通过单击 **SNI** 单选按钮，按 SNI 查看 RSA 密钥交换：


© 2019 Palo Alto Networks, Inc.




有了这些信息，我们就可以转到日志，获取更多有关 RSA 密钥交换使用情况的上下文。

2. 前往解密日志（**Monitor**（监视）> **Logs**（日志）> **Decryption**（解密）），并使用查询 **(tls_keyxchg eq RSA)** 进行筛选，找出使用 RSA 密钥交换的解密会话：

(tls_keyxchg eq RSA)

| | RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|---|
| | 06/04 09:29:50 | 92884 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:50 | 92887 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:44 | 92998 | ssl | 172.30.200.30 | 74.120.19.22 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:24 | 92882 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:24 | 92880 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:23 | 92874 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:23 | 92873 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/03 22:30:11 | 36522 | vudu | 172.30.100.155 | 208.79.221.210 | TLS1.2 | None | | Big Brother |
| | 06/03 20:08:57 | 16896 | ssl | 172.30.200.30 | 66.117.28.86 | TLS1.2 | None | | No Decrypt |
| | 06/03 20:08:22 | 16947 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |

我们从日志的 **Policy Name**（策略名称）列可以看到，**No Decrypt**（不解密）解密策略控制大部分使用 RSA 密钥交换的流量，并且可以推断出，防火墙不会解密该流量，也不会在未经检测的情况下允许该流量。因为流量未解密，因此，防火墙无法标识应用程序，也无法将其列为 **ssl**。如果不想允许使用 RSA 密钥交换的流量，请修改附加到用于控制流量的解密策略的解密配置文件。



© 2019 Palo Alto Networks, Inc.

您可以添加到查询中，以进一步筛选您在 ACC 或第一个解密日志查询中看到的特定 SNI 或应用程序结果。

3. 决定要针对使用安全性较低的密钥交换算法的流量采取的操作。

   阻止访问使用安全性较低的密钥交换协议的站点，出于业务目的而需要访问时除外。对于这些站点，请考虑创建仅应用于该站点（或应用于该站点和其他类似站点）的解密策略和解密配置文件，并阻止其他所有使用安全性较低的密钥交换算法的流量。

- 使用解密日志标识较旧的、安全性较低的身份验证算法。

  使用解密日志筛选较旧的、安全性较低的身份验证算法。

  例如，要识别所有使用 SHA1 算法的会话，请使用查询 **(tls_auth eq SHA)**：

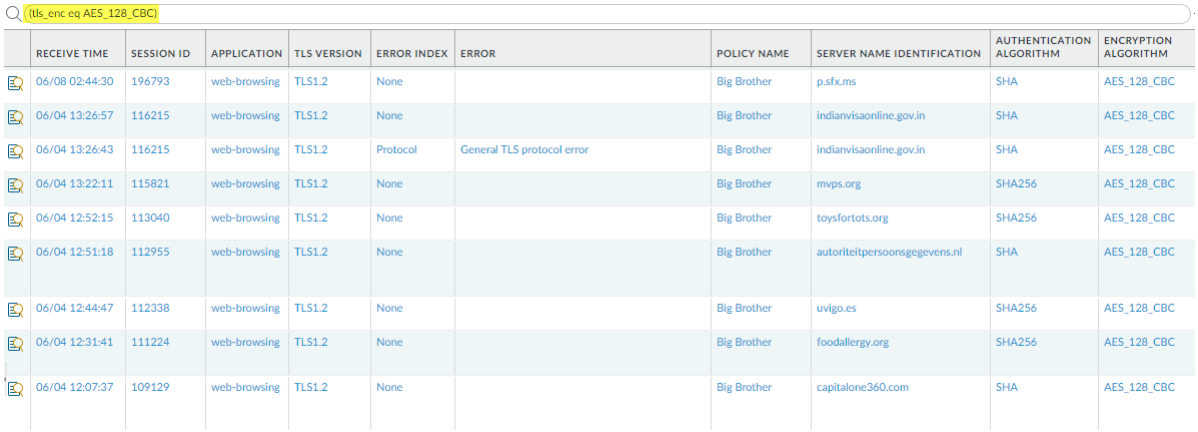

(tls_auth eq SHA)

| RECEIVE TIME | SESSION ID | APPLICATION | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION | AUTHENTICATION ALGORITHM |
|---|---|---|---|---|---|---|---|---|
| 06/08 23:12:02 | 213635 | ssl | TLS1.2 | None | | No Decrypt | | SHA |
| 06/08 11:16:02 | 203438 | incomplete | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| 06/08 11:16:02 | 203439 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| 06/08 11:15:01 | 203437 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| 06/08 02:45:32 | 196795 | incomplete | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| 06/08 02:44:30 | 196794 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| 06/08 02:44:30 | 196793 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
| 06/04 13:38:36 | 117329 | web-browsing | TLS1.2 | None | | Big Brother | inegi.org.mx | SHA |
| 06/04 13:35:01 | 116980 | web-browsing | TLS1.2 | None | | Big Brother | rupress.org | SHA |

  您可以添加到查询，以进一步深入了解结果。例如，您可以添加您在解密日志列看到的特定 SNI、密钥交换版本（例如，筛选还使用 RSA 密钥交换的 SHA1 会话）、TLS 版本或任何其他指标。

- 利用解密日志识别使用特定加密算法的会话。

  例如，要识别所有使用 AES-128-CBC 加密算法的会话，请使用查询 **(tls_enc eq AES_128_CBC)**：


(tls_enc eq AES_128_CBC)

| RECEIVE TIME | SESSION ID | APPLICATION | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION | AUTHENTICATION ALGORITHM | ENCRYPTION ALGORITHM |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 02:44:30 | 196793 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA | AES_128_CBC |
| 06/04 13:26:57 | 116215 | web-browsing | TLS1.2 | None | | Big Brother | indianvisaonline.gov.in | SHA | AES_128_CBC |
| 06/04 13:26:43 | 116215 | web-browsing | TLS1.2 | Protocol | General TLS protocol error | Big Brother | indianvisaonline.gov.in | SHA | AES_128_CBC |
| 06/04 13:22:11 | 115821 | web-browsing | TLS1.2 | None | | Big Brother | mvps.org | SHA256 | AES_128_CBC |
| 06/04 12:52:15 | 113040 | web-browsing | TLS1.2 | None | | Big Brother | toysfortots.org | SHA256 | AES_128_CBC |
| 06/04 12:51:18 | 112955 | web-browsing | TLS1.2 | None | | Big Brother | autoriteitpersoonsgegevens.nl | SHA | AES_128_CBC |
| 06/04 12:44:47 | 112338 | web-browsing | TLS1.2 | None | | Big Brother | uvigo.es | SHA256 | AES_128_CBC |
| 06/04 12:31:41 | 111224 | web-browsing | TLS1.2 | None | | Big Brother | foodallergy.org | SHA256 | AES_128_CBC |
| 06/04 12:07:37 | 109129 | web-browsing | TLS1.2 | None | | Big Brother | capitalone360.com | SHA | AES_128_CBC |

  您可以添加到查询，以进一步深入了解结果。

  用于查找其他较旧加密算法的查询示例包括：**(tls_enc eq DES_CBC)**、**(tls_enc eq 3DES_EDE_CBC)** 和 **(tls_enc eq DES40_CBC)**。

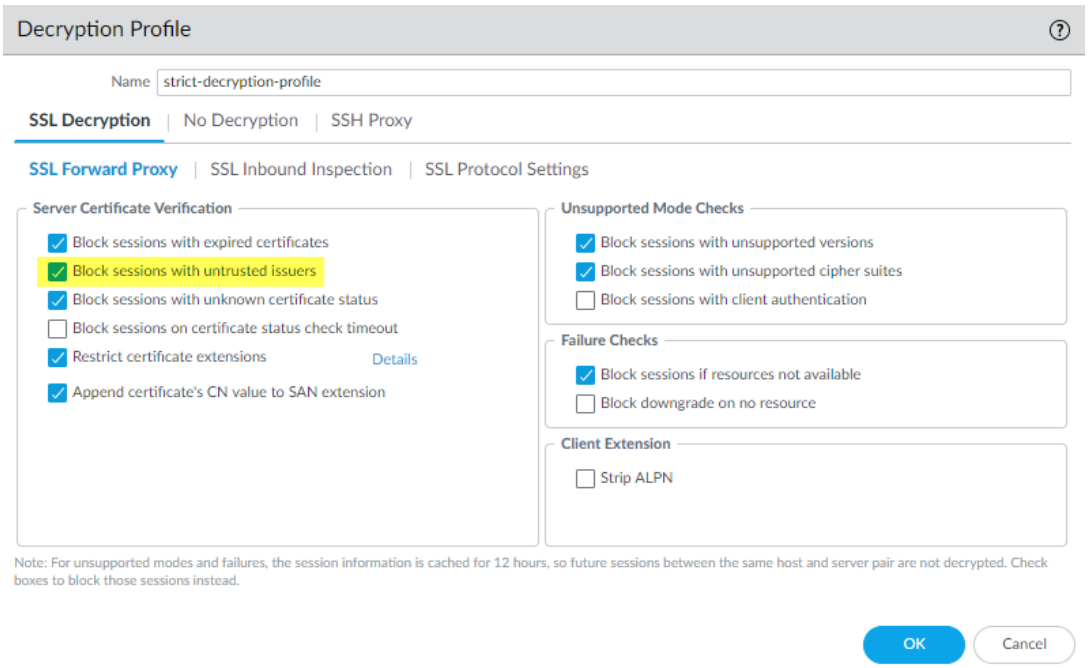
- 使用此方法和日志筛选器构建器创建查询，以调查协商的 ECC 曲线以及您在解密日志中发现的任何其他信息。


© 2019 Palo Alto Networks, Inc.

## 标识不可信的 CA 证书

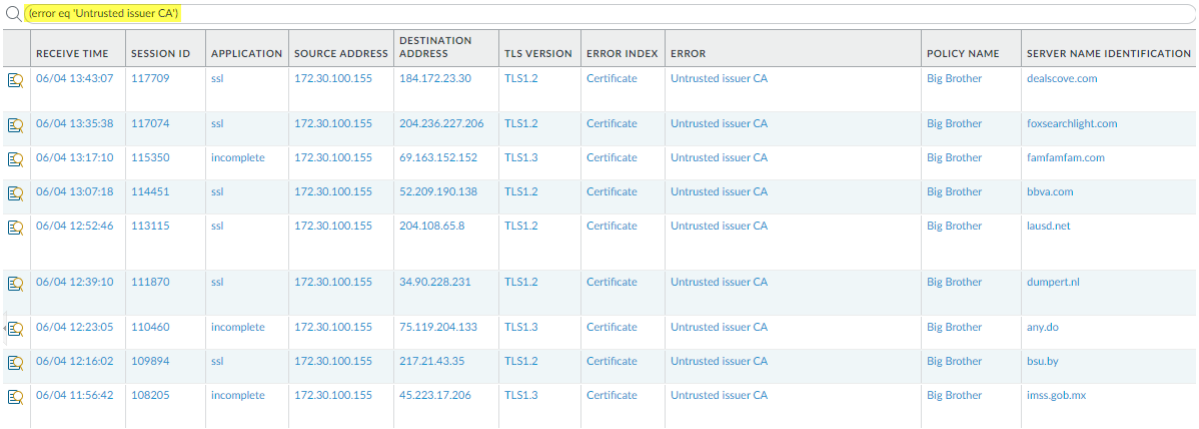
具有不可信 CA 的站点可能包含中间人攻击、重播攻击或其他恶意活动，因此，最佳做法是阻止访问带不可信 CA 以及由其他不可信根 CA 自签发的证书的站点。

STEP 1 | 请务必在转发代理解密配置文件中启用 **Block sessions with untrusted issuers**（阻止不可信颁发机构会话）（**Objects**（对象）> **Decryption**（解密）> **Decryption Profiles**（解密配置文件））以阻止具有不可信 CA 的站点。




一旦在解密配置文件中阻止不可信颁发机构会话，解密日志（**Monitor**（监视）> **Logs**（日志）> **Decryption**（解密））就会记录错误。

STEP 2 | 筛选日志以标识因使用查询导致证书吊销的失败会话 (`error eq 'Untrusted issuer CA'`)。


(error eq 'Untrusted issuer CA')

| | RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION |
|---|---|---|---|---|---|---|---|---|---|---|
| | 06/04 13:43:07 | 117709 | ssl | 172.30.100.155 | 184.172.23.30 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | dealscove.com |
| | 06/04 13:35:38 | 117074 | ssl | 172.30.100.155 | 204.236.227.206 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | foxsearchlight.com |
| | 06/04 13:17:10 | 115350 | incomplete | 172.30.100.155 | 69.163.152.152 | TLS1.3 | Certificate | Untrusted issuer CA | Big Brother | famfamfam.com |
| | 06/04 13:07:18 | 114451 | ssl | 172.30.100.155 | 52.209.190.138 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | bbva.com |
| | 06/04 12:52:46 | 113115 | ssl | 172.30.100.155 | 204.108.65.8 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | lausd.net |
| | 06/04 12:39:10 | 111870 | ssl | 172.30.100.155 | 34.90.228.231 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | dumpert.nl |
| | 06/04 12:23:05 | 110460 | incomplete | 172.30.100.155 | 75.119.204.133 | TLS1.3 | Certificate | Untrusted issuer CA | Big Brother | any.do |
| | 06/04 12:16:02 | 109894 | ssl | 172.30.100.155 | 217.21.43.35 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | bsu.by |
| | 06/04 11:56:42 | 108205 | incomplete | 172.30.100.155 | 45.223.17.206 | TLS1.3 | Certificate | Untrusted issuer CA | Big Brother | imss.gob.mx |

STEP 3 | （可选）双击 Qualys SSL 实验室站点上的证书过期日期。

在**Hostname**（主机名）字段输入服务器主机名（解密日志的**Server Name Identification**（服务器名称标识）列）并将其 **Submit**（提交）以查看主机的证书信息。



© 2019 Palo Alto Networks, Inc.

# 对过期证书进行故障排除

如果遵循解密最佳实践以及“转发代理解密”配置文件或“不解密”配置文件中的 **Block sessions with expired certificates**（阻止具有过期证书的会话），一旦服务器显示过期证书，防火墙就会阻止会话。但是，如果您出于业务目的需要访问的站点允许证书过期，那么，与该站点的连接将被阻止，且您可能都不知道原因。

您可以使用解密日志查看过期证书以及即将过期的证书，以便自己能知晓具体情况，并采取适当的操作。

STEP 1 | 使用查询 **(error eq 'Expired server certificate')** 筛选解密日志中的过期证书。

(error eq 'Expired server certificate')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | SERVER NAME IDENTIFICATION | POLICY NAME |
|---|---|---|---|---|---|---|---|---|---|
| 06/04 16:19:49 | 121352 | incomplete | 172.30.100.10 | 34.225.62.221 | TLS1.3 | Certificate | Expired server certificate | www.stanford.edu | Big Brother |
| 06/04 13:43:26 | 117747 | incomplete | 172.30.100.155 | 104.197.149.89 | TLS1.3 | Certificate | Expired server certificate | phone.com | Big Brother |
| 06/04 13:41:03 | 117572 | incomplete | 172.30.100.155 | 208.117.9.16 | TLS1.3 | Certificate | Expired server certificate | netcarshow.com | Big Brother |
| 06/04 13:38:51 | 117379 | ssl | 172.30.100.155 | 69.172.200.184 | TLS1.2 | Certificate | Expired server certificate | royal.gov.uk | Big Brother |
| 06/04 13:36:27 | 117150 | ssl | 172.30.100.155 | 107.21.104.61 | TLS1.2 | Certificate | Expired server certificate | www.uthscsa.edu | Big Brother |
| 06/04 13:34:53 | 117004 | incomplete | 172.30.100.155 | 66.115.56.251 | TLS1.3 | Certificate | Expired server certificate | gunsamerica.com | Big Brother |
| 06/04 13:33:17 | 116853 | incomplete | 172.30.100.155 | 34.107.140.234 | TLS1.3 | Certificate | Expired server certificate | skiplagged.com | Big Brother |
| 06/04 13:32:45 | 116798 | ssl | 172.30.100.155 | 104.236.4.58 | TLS1.2 | Certificate | Expired server certificate | uploading.com | Big Brother |
| 06/04 13:31:28 | 116655 | incomplete | 172.30.100.155 | 35.186.201.59 | TLS1.3 | Certificate | Expired server certificate | shared.com | Big Brother |
| 06/04 13:29:32 | 116507 | ssl | 172.30.100.155 | 147.139.136.53 | TLS1.2 | Certificate | Expired server certificate | beautynesia.id | Big Brother |
| 06/04 13:28:56 | 116426 | incomplete | 172.30.100.155 | 45.55.105.190 | TLS1.3 | Certificate | Expired server certificate | designbundles.net | Big Brother |

该查询可识别产生 `Expired server certificate`（服务器证书过期）错误的服务器。防火墙将因证书过期而阻止这些服务器。

STEP 2 | （可选）双击 Qualys SSL 实验室站点上的证书过期日期。

在**Hostname**（主机名）字段输入服务器主机名（解密日志的**Server Name Identification**（服务器名称指示）列）并将其 **Submit**（提交）以查看主机的证书信息。

STEP 3 | 使用可识别将达到的证书截止日期的查询筛选解密日志中即将到期的证书（**Monitor**（监控）> **Logs**（日志）> **Decryption**（解密））。

例如，如果今天是 2020 年 2 月 1 日，且您想给自己预留 2 个月的时间用于在站点不更新证书时执行评估和准备操作，则请查询解密日志中将在 2020 年 4 月 1 日或之前到期的证书 (**notafter leq '2020/4/01'**)：

(notafter leq '2020/4/01')

| RECEIVE TIME | APPLICATION | POLICY NAME | PROXY TYPE | SERVER NAME IDENTIFICATION | ROOT STATUS | TLS VERSION | CERTIFICATE START DATE | CERTIFICATE END DATE |
|---|---|---|---|---|---|---|---|---|
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a4.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a2.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a3.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| 01/09 14:25:38 | incomplete | Test 2 | Forward | a.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |

**Certificate End Date**（证书截止日期）列显示的是证书的具体到期日期。



© 2019 Palo Alto Networks, Inc.

STEP 4 | 确定对证书过期的站点采取的操作。

- 如果开展业务无需访问该站点，最安全的做法是继续阻止访问该站点。
- 如果出于业务目的需要访问该站点，请执行以下操作之一：
  - 联系具有过期证书的站点的管理员，通知他们需要更新或续订证书。
  - 创建一个解密策略并仅将其应用于您出于业务目的需要访问但具有过期证书的站点，以及一个允许证书过期的站点的解密配置文件。不得将该策略应用于任何您开展业务不需要访问的站点。一旦站点更新其证书，请将其从策略中移除。

## 对证书吊销问题进行故障排除

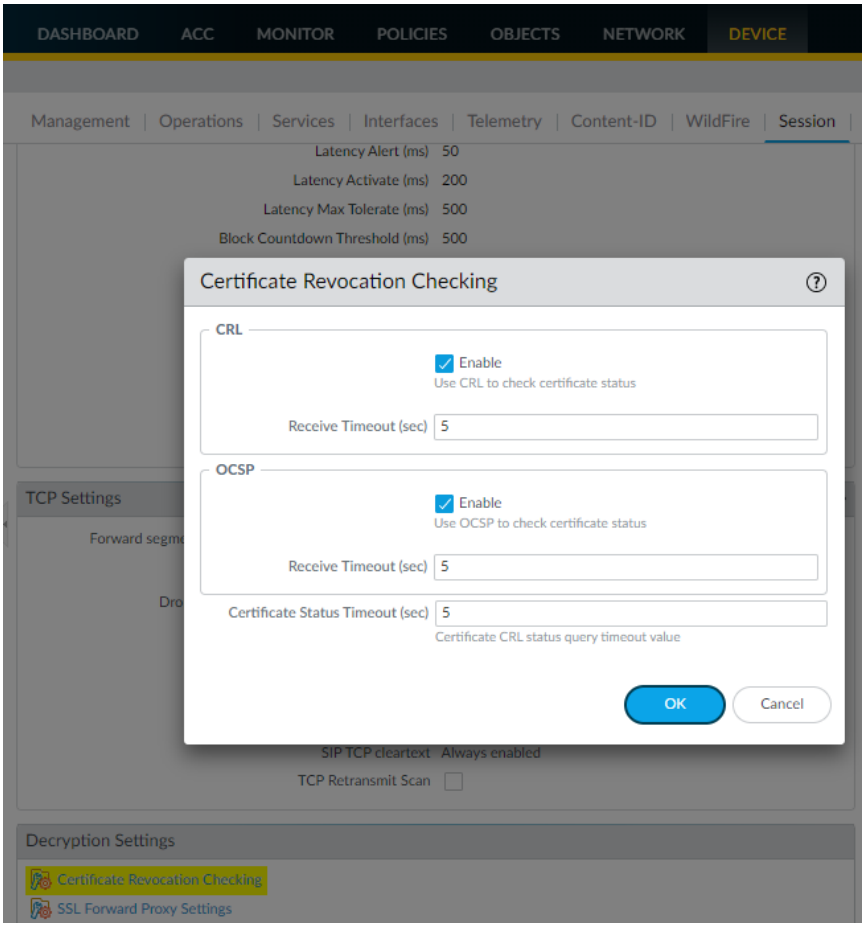
被吊销的证书将不再有效。即使证书被吊销的原因可能是良性的，但是，也可能表明站点出现安全问题，且证书不可信。

请勿信任被吊销的证书；启用证书吊销检查，以拒绝访问证书被吊销的站点。

要丢弃具有已吊销证书的会话，并对被吊销的证书执行故障排除，必须启用证书吊销检查。如果不启用证书吊销检查，防火墙就不会执行吊销证书检查，您就不知道该站点是否具有被吊销的证书。

STEP 1 | 请在尚未启用证书吊销检查时启用此检查。

1. 前往 **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Decryption Settings**（解密设置）。
2. 启用 OCSP 和 CRL 证书检查。

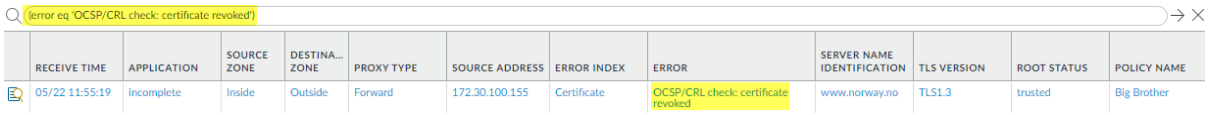





© 2019 Palo Alto Networks, Inc.

如果在“转发代理解密”配置文件中 **Block sessions on certificate status check timeout**（阻止证书状态检查超时的会话），且您担心 5 秒不够，进而导致大量会话因超时而被阻止，请将 **Receive Timeout (sec)**（接收超时（秒））设成为更长的时间。

STEP 2 | 使用查询 **(error eq 'OCSP/CRL check: certificate revoked')** 筛选解密日志（**Monitor**（监控）> **Logs**（日志）> **Decryption**（解密））以查找证书吊销错误。




STEP 3 | （可选）双击 Qualys SSL 实验室站点上的证书过期日期。

在**Hostname**（主机名）字段输入服务器主机名（解密日志的**Server Name Identification**（服务器名称指示）列）并将其 **Submit**（提交）以查看主机的证书信息。

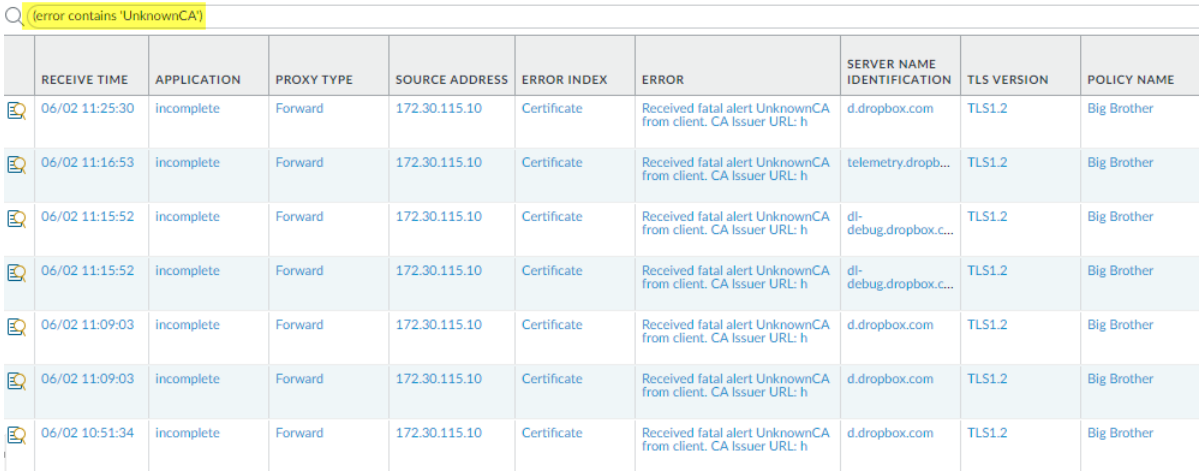
## 对固定证书进行故障排除

通过证书固定，客户端应用程序可以验证服务器的证书是否存在任何已知副本，从而确保该证书确实来自服务器。固定证书旨在阻止中间人 (MITM) 攻击，即客户端和服务器之间的设备将服务器证书替换为另一个证书。

尽管这可以防止恶意操作员拦截和操纵连接，但是，因为防火墙向客户端呈现的是其创建的模拟证书，而不是服务器证书，这也会阻止转发代理解密。转发代理会创建两个会话，一个是客户端和防火墙之间的会话，一个是防火墙和服务器之间的会话，而不是创建一个将客户端和服务器直接连接的会话。这会与客户端建立信任，使防火墙可以解密并检测流量。

但是，证书固定后，因为客户端不接受防火墙的模拟证书 — 客户端仅接受固定到应用程序的证书，因此，防火墙将无法解密流量。

STEP 1 | 使用查询 **(error contains 'UnknownCA')** 筛选解密日志（**Monitor**（监控）> **Logs**（日志）> **Decryption**（解密）），以查找固定证书。




一旦验证服务器证书失败，应用程序就会产生 TLS 错误代码（警报）。不同的应用程序可能会使用不同的错误代码来指示固定证书。固定证书最常用的错误指示符是 UnknownCA 和 BadCertificate。运行查询 **(error contains 'UnknownCA')** 后，再运行查询 **(error contains 'BadCertificate')**，以获取更多的固定证书错误。

您可以使用 *Wireshark* 等其他数据包分析器仔细检查错误。请在 *TLS* 握手后立即查看连接已断开的客户端，以确认出现的是固定证书问题。


© 2019 Palo Alto Networks, Inc.

STEP 2 | 确定如何处理固定证书。

如果开展业务无需访问，您可以允许防火墙继续阻止访问。如果需要访问，那么，您可以通过将其添加到 SSL 解密排除列表（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））的方式允许出于技术原因从解密中排除服务器。

防火墙绕过 SSL 解密排除列表中站点的解密。防火墙无法检测流量，但是，该流量是被允许的。



© 2019 Palo Alto Networks, Inc.

# 解密代理

解密代理允许您将 SSL 解密卸载到 Palo Alto Networks 下一代防火墙，且仅对流量进行一次解密。作为解密代理的防火墙将明文流量转发至安全链（第三方在线设备集），以进行其他实施。

为此，您可以在防火墙上整合安全功能，简化您的网络安全部署：解密代理无需第三方 SLL 解密解决方案，可让您减少使用执行流量分析和实施的第三方设备的数量。对于没有专用 SSL 解密设备的网络，因为流量只解密一次，因此，解密代理可以减少延迟。

解密代理支持 PA-7000 系列、PA-5200 系列、PA-3200 系列设备以及 VM-300、VM-500 和 VM-700 型号。当防火墙创建作为会话流量的受信第三方（或中间人）时，需要启用“SSL 转发代理解密”。

防火墙接口不能同时作为解密代理和 *GRE* 隧道端点。


- 解密代理的工作方式
- 解密代理概念
- 第三层安全链指南
- 配置具有一个或多个第三层安全链的解密代理
- 透明桥接安全链指南
- 配置具有单一透明桥接安全链的解密代理
- 配置具有多个透明桥接安全链的解密代理


## 解密代理的工作方式

配置用于执行 SSL 转发代理解密的防火墙可以充当解密代理而被启用。解密代理使用专有解密转发接口与安全链（第三方安全设备集）相连接。防火墙和安全链可一起用作专有分析网络。

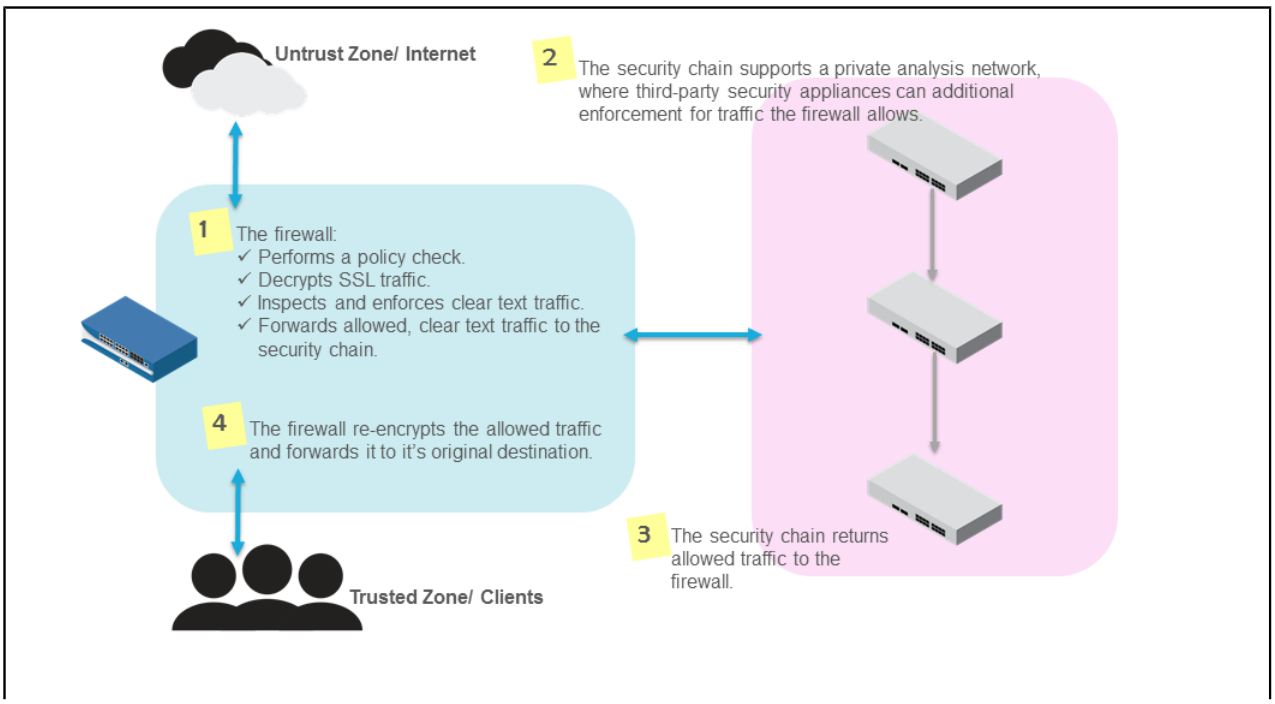
解密并检测 SSL 流量后，防火墙仅将允许的明文流量发送至安全链进行其他分析和实施。因为解密 SSL 流量的防火墙容量超出安全设备处理速度，因此您可以启用该防火墙以在多个安全链中分发解密 SSL 会话，避免任何一个链出现超额订购。安全链中的第一个设备将接收并实施明文流量，然后将允许的流量转发至安全链中下一个在线设备。安全链中最后一个设备将剩余的允许流量返回给防火墙。防火墙重新加密流量，并转发至其原始目的地。

支持两种类型的安全链部署：第三层安全链和透明桥接安全链。您可以根据构成您安全链的设备选择想要进行设置的部署类型（就像您正在使用无状态或有状态设备一样）。在两种安全链部署中，您可以根据分析所需让防火墙以单向或双向的方式引导流量通过安全链（请参阅解密代理：更多有关何时使用单向或双向流的信息，请参阅安全链会话流）。

下图显示了解密代理的工作方式。



© 2019 Palo Alto Networks, Inc.




# 解密代理概念

充当解密代理的防火墙使用专用解密转发接口发送解密流量至安全链，即第三方在线安全设备集，以进行其他分析。解密代理支持两种类型的安全链网络（第三层安全链和透明桥接安全链），此外，您还可以通过单向或双向方式引导流量通过安全链。单个防火墙最多可以在 64 个安全链中分发解密会话，并对安全链进行监控，确保能有效地处理流量。

更多有关解密代理支持和功能的信息，请查看以下主题。

- 解密代理：转发接口
- 解密代理：第三层安全链
- 解密代理：透明桥接安全链
- 解密代理：安全链会话流
- 解密代理：多个安全链
- 解密代理：安全链健康检查

## 解密代理：转发接口

作为解密代理启用的防火墙将使用一对专用的第三层接口来转发解密流量至安全链，以进行检测。解密转发接口必须分配给一个全新的虚拟路由器（尚未配置用于传递数据面板流量的路由或其他接口的虚拟路由器），这可确保防火墙转发至安全链进行其他分析的明文会话可以完全从数据面板流量中分割出来。

在部署带第三层安全链的解密代理时，一对解密转发接口（2 个）可最多支持 64 个安全链。

一对解密转发接口支持一个透明桥接安全链；但是，您可以配置多个解密转发接口对以支持多个透明桥接安全链。

## 解密代理：第三层安全链

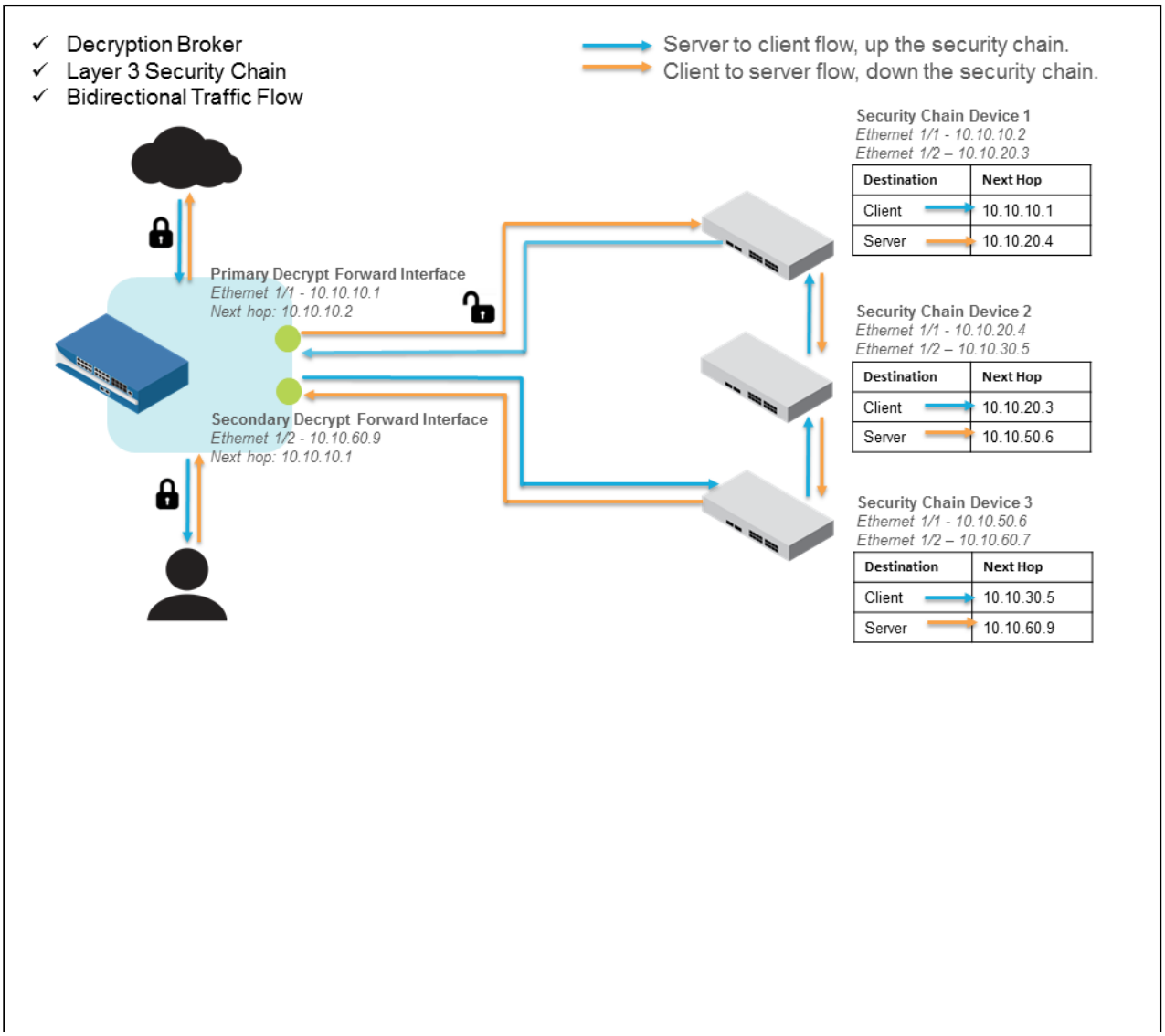
在第三层安全链网络中，安全链设备使用第 3 层接口连接到安全链网络，且每个接口必须具有分配的 IP 地址和子网掩码。安全链设备必须配置有静态路由，以将入站和出站通信引导到安全链中的下一个设备并返回到防火墙。



© 2019 Palo Alto Networks, Inc.

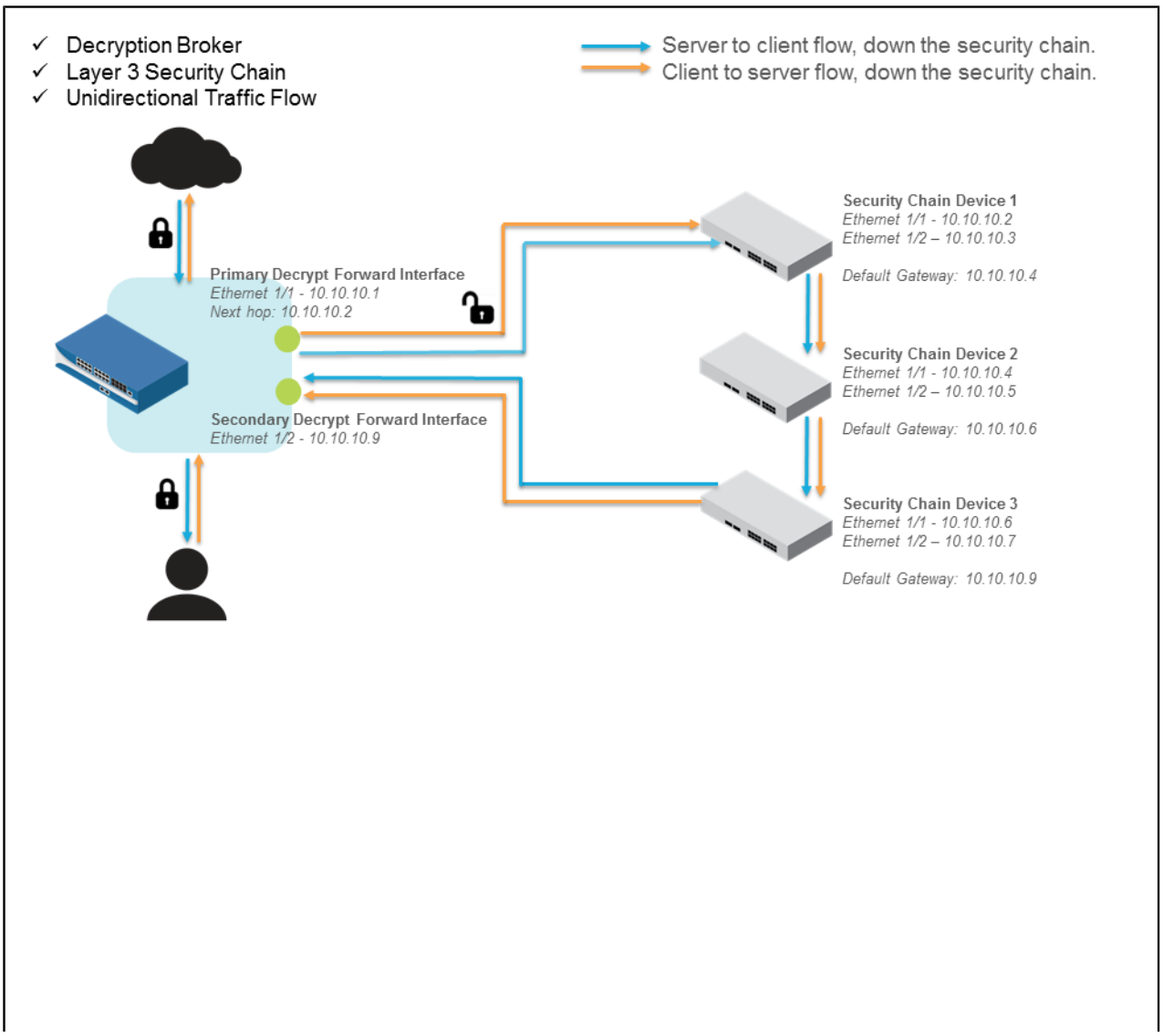
根据您选择的安全链会话流（单向或双向），入站和出站解密会话以相同或相反的方向通过安全链。

下图显示了防火墙用作解密代理将允许的明文流量双向引导通过第三层安全链。防火墙配置有静态路由和默认路由，前者用于将入站会话引导至客户端所在的内部受信区域（例如，员工），而后者则将出站会话引导至外部不受信区域（Internet）。对于出站会话，防火墙使用解密转发专用“主接口”将入站会话转发至安全链的第一个设备。安全链中的设备使用静态路由将流量引导至下一个在线设备；安全链中每个设备的下一跃点都是后续设备的入口端口 IP 地址。安全链中的最后一个设备的下一个跃点是防火墙中解密转发专用的辅助接口。（入站会话流正好相反）。




或者，下图显示的是用作将解密流量引导通过第三层安全链的解密代理的相同防火墙；但是，在此示例中，防火墙引导所有回话单向通过安全链。防火墙使用解密转发专用“主接口”将入站和出站会话转发至安全链的第一个设备。安全链中最后一个设备将入站和出站会话返回给防火墙。


© 2019 Palo Alto Networks, Inc.



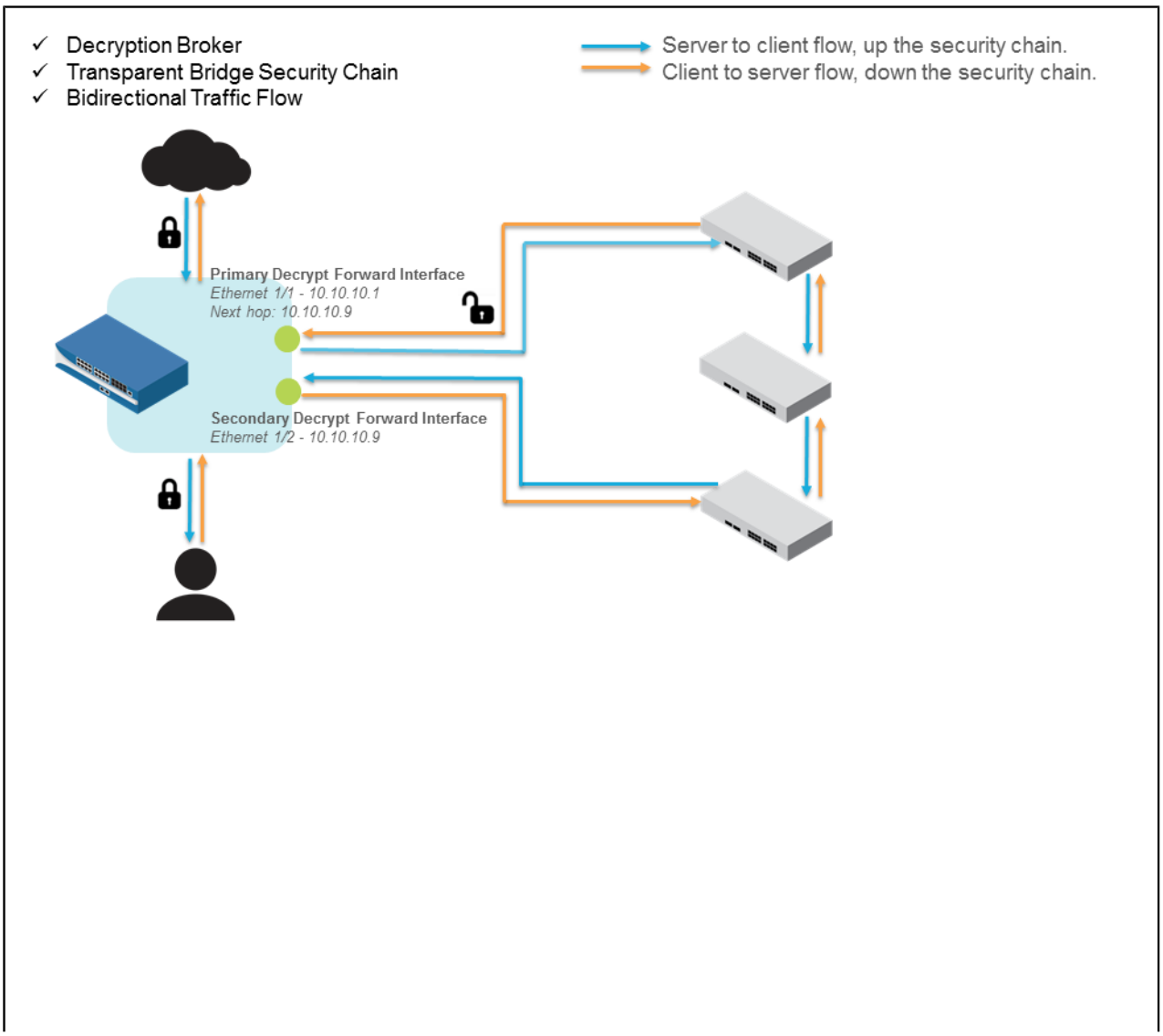

在第三层安全链所有部署（单向和双向）中，防火墙重新加密安全链返回的流量，并继续将其转发至相应的目的地。要开始其中一个部署，请配置具有一个或多个第三层安全链的解密代理。

## 解密代理：透明桥接安全链

在透明桥接安全链网络中，所有安全链设备均配置有两个连接到安全链网络的接口。这两个接口均配置为透明桥接模式；它们不具有分配的 IP 地址、子网掩码、默认网关和本地路由表。透明桥接模式下的安全链设备是逐个串联在一起的。它们在一个接口上接收流量，然后进行分析和实施。流量从另一个接口流出，然后传递给安全链中下一个在线设备。下面的第一张图显示的是具有双向会话流的透明桥接安全链，第二张图显示的是具有单向会话流的透明桥接安全链。要开始其中一个部署，请配置具有单一透明桥接安全链的解密代理。

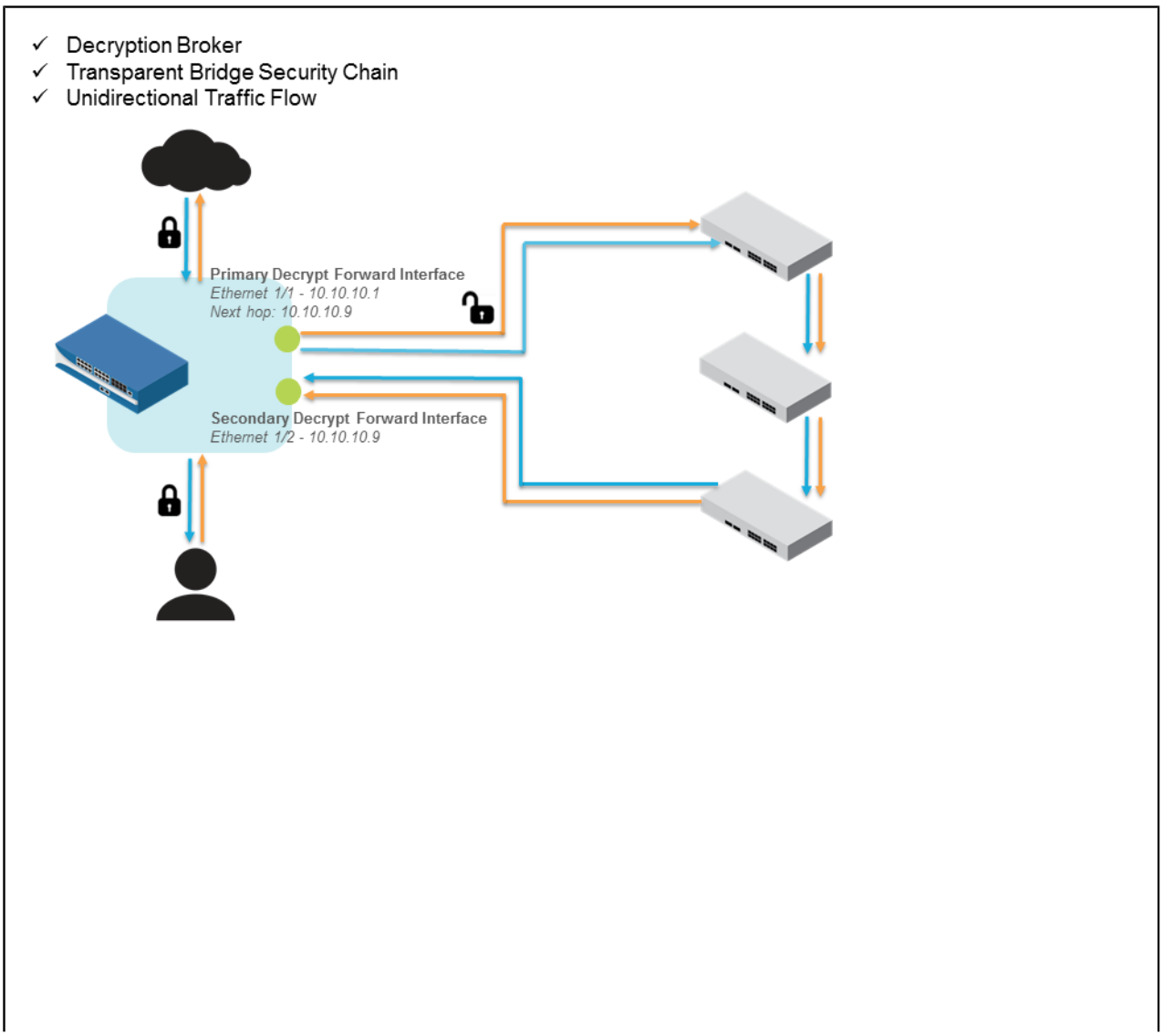


© 2019 Palo Alto Networks, Inc.





© 2019 Palo Alto Networks, Inc.




## 解密代理：安全链会话流

您可以选择防火墙引导入站和出站解密会话以相同的方向（单向）或想法的方向（双向）通过安全链的方式。例如，如果安全链中存在数据包记录器等无状态设备，则可以让流量单向流经安全链，这样，入站和出站流量会以相同的方向穿过设备。数据包记录器可接收相同端口上的入站和出站流量，随后检查来自会话两侧的数据包捕获，以检测数据表标头值是否发生更改。或者，如果安全链包含能够对流量实施有状态检测的数据丢失保护 (DLP) 解决方案等设备，则可以允许流量双向通过安全链。

## 解密代理：多个安全链

充当解密代理的防火墙支持转发至多个安全链（第三层、透明桥接或两者混合），以便提供冗余，平衡分析负载，从而避免安全链或安全链某个设备出现超额订阅。因为防火墙进行解密和转发流量的容量可能超过安全链中设备处理流量的容量，因此，您可以配置防火墙以将明文会话分发给多个安全链网络进行检测。防火墙可以在两种类型的安全链网络中分发会话，这样，安全链就能共享检测负载。但是，启用会话分发的方法会有所不同，具体取决于您是使用第三层安全链，还是使用透明桥接安全链。用于转发至多个第三层安全链的解密代理可以通过下列四种方法之一分发会话以进行检测：

- IP 模 — 防火墙根据源和目标 IP 地址的模块哈希分配会话。
- IP 哈希 — 防火墙根据源和目标 IP 地址的 IP 哈希及端口号分配会话。



© 2019 Palo Alto Networks, Inc.

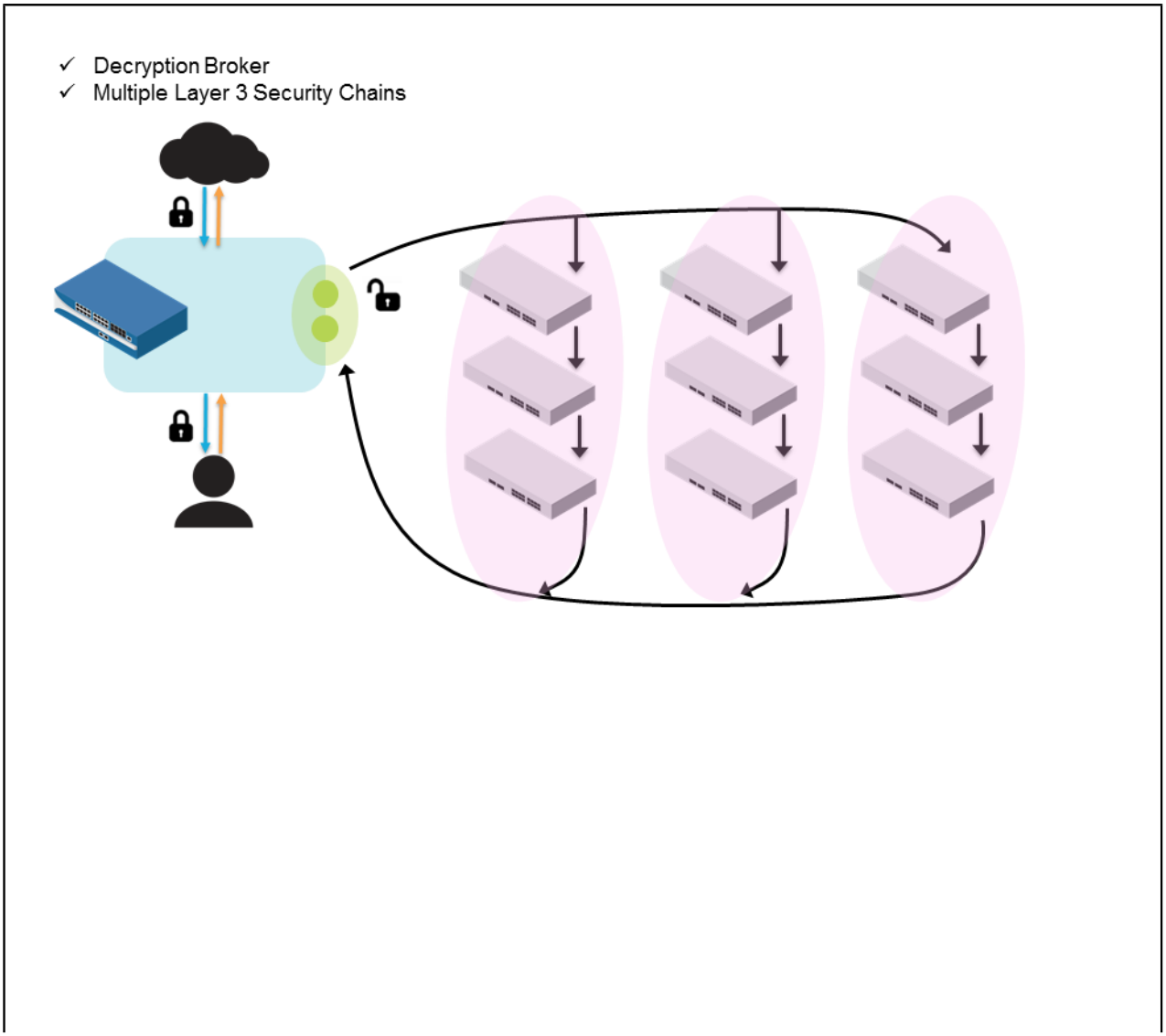
- 循环 — 防火墙在安全链中均匀分配会话。
- 最低延迟 — 防火墙以最低延迟向安全链分配更多会话。

必须配置用于转发至多个透明桥接安全链的解密代理，以执行基于策略的会话分发；符合策略规则的流量仅转发给与该规则相关联的安全链。例如，为每个解密策略指定一个不同的源地址，以便将单个透明桥接安全链专用于分析和实施源自特定 IP 地址范围的流量。

配置多个安全链时，必须部署足够的安全链，以便在安全链失败时提供额外的容量。如果您启用防火墙执行安全链健康检查，而安全链未能通过该检查，则防火墙将继续在健康的安全链之间分发解密会话。如果没有足够的健康链来覆盖额外的负载，因为剩余的健康安全链超额订购，因此单个安全链的失败可能会导致级联故障。

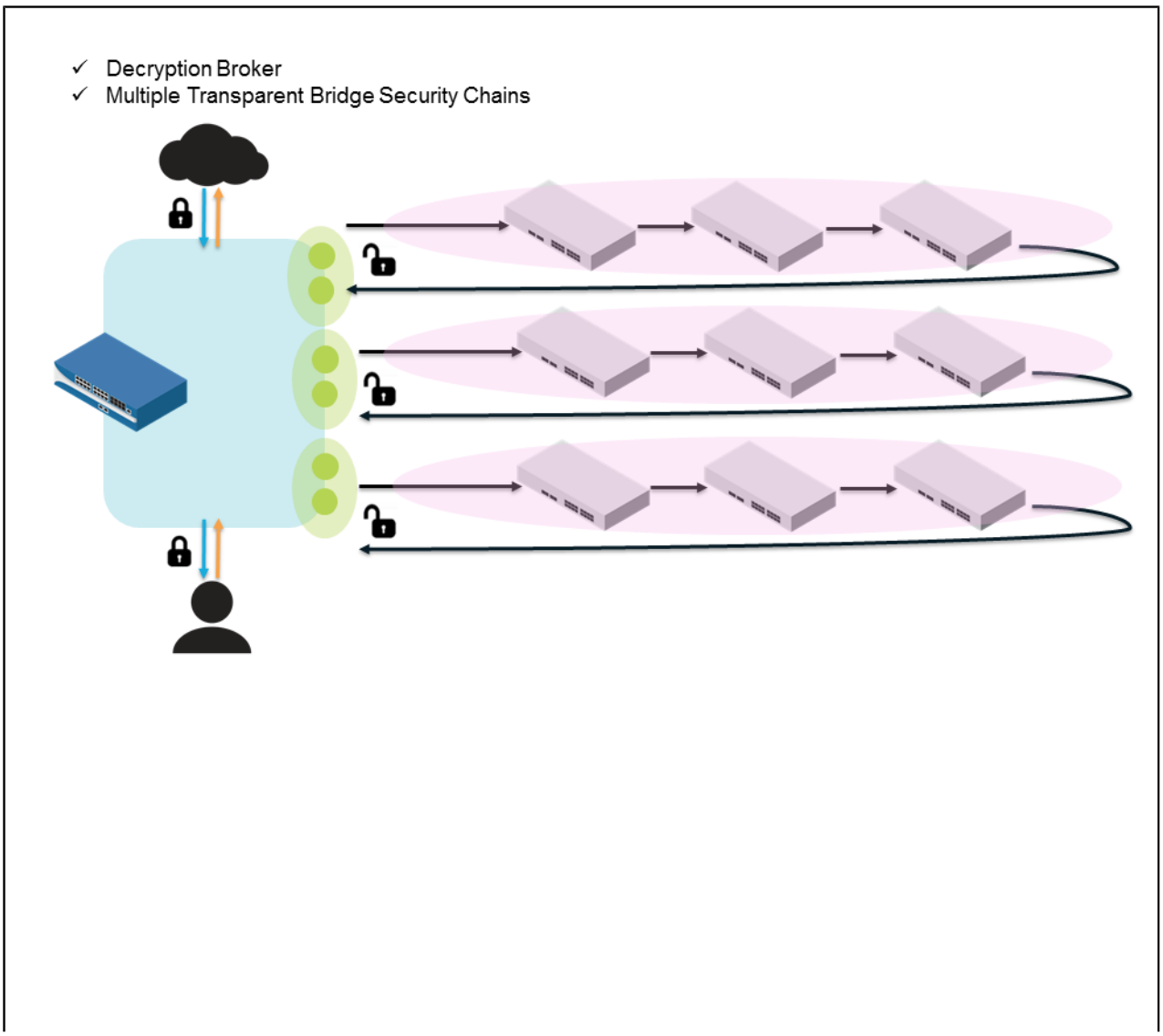
下面的第一张图显示的是具有多个第三层安全链的解密代理部署。请注意，一对解密转发接口可以将解密流量转发给多个第三层安全链（最多 64 个）。

下面的第二张图显示的是具有多个透明桥接安全链的解密代理部署。需要一对专门的解密转发接口来将流量转发给每个单独的透明桥接安全链。





© 2019 Palo Alto Networks, Inc.




## 解密代理：安全链健康检查

解密代理可以监控安全链的状态，确保其能有效地处理解密流量。定期进行安全检查，以监控：

- 安全设备的连接性（路径监控）
- 安全设备的处理速度和效率（HTTP 延迟监控）
- 安全设备的 HTTP 检查功能（HTTP 监控）

对于您启用的每种监控类型，必须定义想要触发未通过运行状况检查的条件。当安全链未通过安全检查，防火墙可以：

- 阻止分配给失败安全链的现有 SSL 会话。若安全链通过后续的运行状况检查，则防火墙将仅开始转发新的解密会话至该安全链，以进行分析。通信流必须通过允许访问 Internet 的防火墙安全策略检查和安全链检查。
- （仅限第三层安全链）允许流量绕过失败的安全链。请记住，绕过安全链的流量仍需经过防火墙解密和安全策略实施，但却不用经过安全链分析。该选项仅支持第三层安全链。因为透明桥接安全链会话分发基于策略进行，而符合策略规则的流量则已分配给特定链进行检查，因此流量无法绕过失败的安全链。

当安全链失败时，您可以根据组织的合规性以及可用性需求，选择防火墙阻止会话或是绕过安全链。



© 2019 Palo Alto Networks, Inc.

配置多个安全链时，最佳做法是部署足够的安全链，以便在安全链失败时提供额外的容量。如果您启用防火墙执行安全链健康检查，而安全链未能通过该检查，则防火墙将继续在健康的安全链之间分发解密会话。如果没有足够的健康链来覆盖额外的负载，因为剩余的健康安全链超额订购，因此单个安全链的失败可能会导致级联故障。

## 第三层安全链指南

请遵循以下指南来设置第三层安全链设备，以支持解密代理。

- 配置安全链设备第三层接口，以连接至安全链网络。这些第三层接口必须具有分配的 IP 地址和子网掩码。
- 请勿在安全链中包含用于修改 IP 或 TCP 标头的设备，或是必须禁用执行这些功能的任何特征。如果安全链使用修改过的 IP 或 TCP 标头将会话返回至防火墙，由于此会话无法与原始的预解密会话匹配，因此将被防火墙丢弃。
- 为安全链设备设置默认网关：
  - 对于安全链中除最后一个设备之外的所有其他设备，请将默认网关配置为下一个在线设备的 IP 地址。
  - 对于安全链中最后一个设备，请将默认网关配置为防火墙的辅助接口 IP 地址。这能确保最后一个设备可将通信流返回至防火墙。（配置解密转发配置文件时，您将其中一个解密转发接口分配作为解密代理的辅助接口。请参阅 Objects（对象）> Decryption（解密）> Forwarding Profile（转发配置文件）> Secondary Interface（辅助接口），然后使用此接口的 IP 地址）。
  - 如果将防火墙配置为引导会话单向通过安全链，则还必须将安全链中第一个设备的默认网关设置为防火墙的主接口 IP 地址（配置解密转发配置文件时，您将其中一个解密转发接口分配作为解密代理的主接口。请参阅 Objects（对象）> Decryption（解密）> Forwarding Profile（转发配置文件）> Primary Interface（主接口），然后使用此接口的 IP 地址）。
- 确认防火墙和安全链是否能有效地通信：检查用于引导防火墙和安全链之间通信的路由器是否配置正确；安全链设备是否配置有静态路由，以正确引导通信。
- 安全链设备不应将通信发送到安全链以外的网络。防火墙阻止与原始预解密会话不匹配的流量。但是，如果安全链设备需要 Internet 访问以接收更新，则设备必须能够访问独立的网络（例如，通过设备的管理端口）以加快这些更新。
- 配置多个安全链时，最佳做法是部署足够的安全链，以便在安全链失败时提供额外的容量。如果您启用防火墙执行安全链健康检查，而安全链未能通过该检查，则防火墙将继续在健康的安全链之间分发解密会话。如果没有足够的健康链来覆盖额外的负载，因为剩余的健康安全链超额订购，因此单个安全链的失败可能会导致级联故障。

## 配置具有一个或多个第三层安全链的解密代理

执行以下步骤，使防火墙充当解密代理，以便将流量分发至第三层安全链进行其他分析和实施。使防火墙充当解密代理的操作包括：

- 设置遵守第三层安全链指南的第三层安全链。
- 激活免费的解密代理许可证（解密许可证）。这包括转至 Palo Alto Networks 客户支持门户激活许可证，然后在防火墙上安装许可证。
- 至少启用两个防火墙接口作为解密转发接口。一对解密转发接口可以最多支持 64 个安全链。
- 配置“解密转发”配置文件，使防火墙将解密会话转发至一个或多个安全链，在多个安全链中分发这些会话，并监控安全链的健康状况。

STEP 1 | 遵循第三层安全链指南，确保您设置的安全链可以支持解密代理。

STEP 2 | 激活免费的解密代理许可证（请参阅解密许可证）。

STEP 3 | 确认防火墙是否已启用以执行 SSL 转发代理解密。


© 2019 Palo Alto Networks, Inc.

选择 **Policies**（策略）> **Decryption**（解密）来添加或修改解密策略规则。此外，您还可以将解密配置文件附加到解密策略规则中，以执行证书检查，验证 SSL 协议。例如，解密配置文件允许您使用不受支持协议或密码套件根据证书状态阻止会话，或是在执行解密的资源不可用时阻止会话。

STEP 4 | 启用一对第三层接口以转发解密流量。

1. 查看 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）选项卡上的配置接口。如果接口配置为第三层接口，则显示接口类型列。选择第三层接口，并为想要启用作为解密转发对的两个第三层接口完成下列步骤。
2. 选择配置选项卡，并将接口分配给未配置用于传递数据面板流量的路由或接口的虚拟路由器。虚拟路由器必须专用于解密转发接口，确保防火墙转发用于其他分析的明文会话实现与数据面板流量的完整分割。
3. 继续将接口分配到安全区域。（将两个接口都分配给相同的安全区域）。
4. 在高级选项卡上，选择“解密转发”。
5. 单击确定以保存接口设置。
6. 对偶数个接口重复这些步骤，然后在转发时实施配对。
7. 确保用于转发解密流量的接口不会被用于传递任何其他类型的流量。

STEP 5 | 创建解密转发配置文件，定义防火墙设置，以便将解密流量转发至第三层安全链。

1. 选择 **Objects**（对象）> **Decryption**（解密）> **Forwarding Profile**（转发配置文件），添加新的解密转发配置文件，再为其输入描述性名称。
2. 在常规选项卡上，设置安全链类型为路由（第三层），以配置防火墙将解密流量转发至带第三层设备的安全链。
3. 设置防火墙转发的解密流量的流方向：单向或双向。
4. 选择防火墙用于与安全链进行通信的主接口和辅助接口。

   主接口和辅助接口共同构成一对解密转发接口。仅显示您启用为解密转发接口的接口。您的安全链类型（第三层或透明桥接）和通信流方向（单向或双向）将确定允许两个接口转发中的哪一个、安全链的明文流量、以及哪一个接口可以在进行过其他实施后从安全链流回的流量。
5. 单击确定以保存解密配置文件。

STEP 6 | 将防火墙连接到安全链。

1. 选择“安全链”选项卡，并添加安全链。
2. 命名并启用安全链。
3. 在安全链中输入第一个设备和最后一个设备的详细信息。

   提供设备的描述性名称，然后在安全链中选择第一个设备的 IPv4 地址。或者，您可以定义个新的地址对象，以便轻松引用该设备。
4. 单击确定以保存安全链，然后继续重复这些步骤以添加另一个安全链。或者，如果您仅添加一个安全链，请继续后面的操作。

STEP 7 | （仅多个安全链）继续实施安全链选项卡中的其他操作，选择防火墙用户在安全链间分发解密会话的会话分发方法。

根据 IP 模、IP 哈希、循环调度或最低延迟选择会话分发。最低延迟会话分发方法还要求您启用防火墙，以在安全链上执行 HTTP 延迟监控和 HTP 监控。

STEP 8 | 选择健康监控器选项卡，使防火墙在安全链上执行安全链运行状况检查。

如果安全链未能执行运行状况检查，则防火墙随后可以阻止流量，直至安全链通过后续的运行状况检查且有能力进行处理，或是防火墙可以允许流量绕过失败的安全链。

1. 在“未通过运行状况检查”上，选择绕过安全链或阻止会话的防火墙。
2. 将未通过运行状况检查条件定义为符合任何运行状况监控条件（OR 条件）或符号所有条件（AND 条件）的事件。



© 2019 Palo Alto Networks, Inc.

3. 启用路径监控、HTTP 延迟监控和/或 HTTP 监控 。对于想要启用的每种监控类型，定义想要触发未通过运行状况检查的时间段和/或计数。

   若要有效支持最低延迟会话分发，则需要延迟和 HTTP 监控（**Objects**（对象）> **Decryption**（解密）> **Forwarding Profile**（转发配置文件）> **Security Chains Session Distribution Method**（安全链会话分发方法））。

STEP 9 | 保存转发配置文件。

STEP 10 | 将转发配置文件附加到解密策略规则。

防火墙解密并检测符合规则的流量，然后将明文流量转发至安全链，以进行进一步的检测和实施。

1. 选择 **Policies**（策略）> **Decryption**（解密），并选择解密策略规则。
2. 选择“选项”。
3. 将操作设置为解密并转发。
4. 选择您创建的转发配置文件。
5. 单击确定以保存策略规则，然后提交更改。

STEP 11 | 监控防火墙转发用于其他检测的解密流量。

1. 选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）然后添加筛选器：（标记带有解密转发）。
2. 检查流量日志条目的详细信息，并查找解密转发标志。

# 透明桥接安全链指南

配置透明桥接安全链设备时，请遵循以下指南来支持解密代理：

- 在透明桥接模式下，安全链上每个设备均必须配置有两个将设备连接至安全链网络的接口。安全链设备并不会使用本地路由表，而透明桥接接口却没有分配的 IP 地址、子网掩码和默认网关。
- 请勿在安全链中包含用于修改 IP 或 TCP 标头的设备，或是必须禁用执行这些功能的任何特征。如果安全链使用修改过的 IP 或 TCP 标头将会话返回至防火墙，由于此会话无法与原始的客户端到服务器或服务器到客户端会话匹配，因此将被防火墙丢弃。
- 配置多个安全链时，最佳做法是部署足够的安全链，以便在安全链失败时提供额外的容量。如果您启用防火墙执行安全链健康检查，而安全链未能通过该检查，则防火墙将继续在健康的安全链之间分发解密会话。如果没有足够的健康链来覆盖额外的负载，因为剩余的健康安全链超额订购，因此单个安全链的失败可能会导致级联故障。

# 配置具有单一透明桥接安全链的解密代理

执行以下步骤，使防火墙充当解密代理，以便将流量分发至透明桥接安全链进行其他分析和实施。使防火墙充当解密代理的操作包括：

- 设置遵守透明桥接安全链指南的透明桥接安全链。
- 激活免费的解密代理许可证（解密许可证）。这包括转至 Palo Alto Networks 客户支持门户激活许可证，然后在防火墙上安装许可证。
- 启用一对第三层防火墙接口作为解密转发接口。每对解密转发接口支持一个透明桥接安全链；您需要创建多个解密转发接口对以支持多个透明桥接安全链。
- 配置“解密转发”配置文件，使防火墙将解密会话转发至透明桥接安全链，并监控安全链的性能。

即使您计划启用带多个透明桥接安全链的解密代理，也必须首先执行以下步骤。

STEP 1 | 设置遵守透明桥接安全链指南的透明桥接安全链。

STEP 2 | 激活免费的解密代理许可证（请参阅解密许可证）。


© 2019 Palo Alto Networks, Inc.

STEP 3 | 确认防火墙是否已启用以执行 SSL 转发代理解密。

选择 **Policies**（策略）> **Decryption**（解密）来 **Add**（添加）或修改解密策略规则。此外，您还可以将解密配置文件附加到解密策略规则中，以执行证书检查，验证 SSL 协议。例如，解密配置文件允许您使用不受支持协议或密码套件根据证书状态阻止会话，或是在执行解密的资源不可用时阻止会话。

STEP 4 | 启用一对第三层接口以转发解密流量。

1. 查看 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）选项卡上的配置接口。

   如果接口配置为第三层接口，则显示接口类型列。选择第三层接口，并为想要启用作为解密转发对的两个第三层接口完成下列步骤。
2. 选择 **Config**（配置）选项卡，并将接口分配给未配置用于传递数据面板流量的路由或接口的 **Virtual Router**（虚拟路由器）。

   虚拟路由器必须专用于解密转发接口，确保防火墙转发用于其他分析的明文会话实现与数据面板流量的完整分割。
3. 继续将接口分配到 **Security Zone**（安全区域）。（将两个接口都分配给相同的安全区域）。
4. 在 **Advanced**（高级）选项卡上，选择 **Decrypt Forward**（解密转发）。
5. 单击**OK**（确定）以保存接口设置。
6. 重复这些步骤，启用至少两个接口转发解密流量。

   一对解密转发接口（两个）支持单个透明桥接安全链。如果想要防火墙在多个透明桥接安全链中分发解密会话，请继续为每个您想要支持的安全链启用一对解密转发接口。确保启用以转发解密流量的接口不会被用于传递任何其他类型的流量。

STEP 5 | 创建解密转发配置文件，定义防火墙设置，以便将解密流量转发至透明桥接安全链。

1. 选择 **Objects**（对象）> **Decryption**（解密）> **Forwarding Profile**（转发配置文件），**Add**（添加）新的解密转发配置文件，再为其输入描述性名称**Name**（名称）。
2. 在 **General**（常规）选项卡上，设置 **Security Chain Type**（安全链类型）为 **Transparent Bridge**（透明桥接），以配置防火墙将解密流量转发至带透明桥接设备的安全链。
3. 设置防火墙转发的解密流量的 **Flow Direction**（流方向）：**Unidirectional**（单向）或 **Bidirectional**（双向）。
4. 选择防火墙用于将流量转发至安全链的 **Primary Interface**（主接口）和 **Secondary Interface**（辅助接口）。

   主接口和辅助接口共同构成一对解密转发接口。仅显示您启用为解密转发接口的接口。

STEP 6 | 选择 **Health Monitor**（健康监控器）选项卡，使防火墙在透明桥接安全链上执行运行状况检查。

1. 如果想要在运行状况检查成功后丢弃流量，请将 **On Health Check Failure**（未通过运行状况检查）设为 **Block Session**（阻止会话），或是将其设为 **Bypass Security Chain**（绕过安全链）以转发不通过安全链的流量。

   透明桥接安全链会话分发基于策略进行，而与策略规则匹配的流量已分配给特定链进行检查，因此流量无法绕过不同的安全链（就像第 3 层模式中那样）。
2. 将 **Health Check Failed Condition**（未通过运行状况检查条件）定义为符合任何运行状况监控条件（**OR Condition**（**OR** 条件））或符号所有条件（**AND Condition**（**AND** 条件））的事件。
3. 启用 **Path Monitoring**（路径监控）、**HTTP Latency Monitoring**（**HTTP** 延迟监控）和/或 **HTTP Monitoring**（**HTTP** 监控）。对于想要启用的每种监控类型，定义想要触发未通过运行状况检查的时间段和/或计数。

   若要有效支持最低延迟会话方法，则需要延迟和 HTTP 监控（**Objects**（对象）> **Decryption**（解密）> **Forwarding Profile**（转发配置文件）> **Security Chains**（安全链）> **Session Distribution Method**（会话分发方法））。

STEP 7 | 保存转发配置文件。



© 2019 Palo Alto Networks, Inc.

STEP 8 | 将转发配置文件附加到解密策略规则。

防火墙解密并检测符合规则的流量，然后将明文流量转发至安全链，以进行进一步的检测和实施。

1. 选择 **Policies**（策略）> **Decryption**（解密），并选择解密策略规则。
2. 使用策略规则选项卡定义想要转发至相关透明桥接安全链的流量。

   例如，选择 **Source**（源）并 **Add**（添加）**Source Address**（源地址）范围，或单击 **New Address**（新地址）以创建可以识别给源自定 IP 地址范围内流量的地址对象。策略规则将仅执行来自该来源的流量。
3. 选择**Options**（选项）。
4. 将**Action**（操作）设置为 **Decrypt and Forward**（解密并转发）。
5. 选择 **Transparent Bridge Forwarding Profile**（透明桥接转发配置文件）。
6. 单击**OK**（确定）以保存策略规则，然后 **Commit**（提交）更改。

STEP 9 | （选项）继续配置具有多个透明桥接安全链的解密代理。

STEP 10 | 监控防火墙转发用于其他检测的解密流量。

- 选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）然后添加筛选器：（标记带有解密转发）。
- 检查流量日志条目的详细信息，并查找解密转发标志。

# 配置具有多个透明桥接安全链的解密代理

您可以将防火墙配置为在多个“多个安全链”之间分发会话，此时，安全链处于透明桥接模式。对于想要支持的每个透明桥接安全链，必须完成以下配置：

- 用于仅将流量转发至单个透明桥接安全链的一对解密转发接口。
- 用于仅为单个透明桥接安全链指定设置的解密转发配置文件。
- 仅指定用于某些待转发至单个透明桥接安全链的解密流量的解密策略规则。这允许您基于流量来源在多个透明桥接安全链中更加均匀地分发会话，避免任何单个安全链出现超额订阅。

STEP 1 | 首先，请遵循配置具有单一透明桥接安全链的解密代理的步骤。对于想要支持的每个透明桥接安全链，这包括：

- 在防火墙上，启用一对第三层接口以支持转发解密流量。
- 创建解密转发配置文件，定义防火墙设置，以便将解密流量转发至透明桥接安全链。

STEP 2 | 将每个透明桥接解密转发配置文件附加到单独的解密策略规则。

除了将解密转发设置运用至匹配流量，将透明桥接解密转发配置文件附加到解密策略规则后，您可以在透明桥接安全链中分发会话。为每个策略规则指定一个不同的源地址，以便将单个透明桥接安全链专用于分析和实施该范围内的流量。

1. 选择 **Policies**（策略）> **Decryption**（解密），并选择解密策略规则。
2. 选择 **Source**（源）并 **Add**（添加）Source Address（源地址）范围，或单击 **New Address**（新地址）以创建可以识别源自给定 IP 地址范围内流量的新地址对象。仅来自该 IP 地址范围的流量被转发至相关的透明桥接安全链进行分析。
3. 选择**Options**（选项）。
4. 将**Action**（操作）设置为 **Decrypt and Forward**（解密并转发）。
5. 选择 **Transparent Bridge Forwarding Profile**（透明桥接转发配置文件）以附加至策略规则。
6. 单击**OK**（确定）以保存策略规则，然后 **Commit**（提交）更改。

STEP 3 | 为您想要支持的尽可能多的安全链继续重复这些步骤 — 将一个透明桥接解密转发配置文件与一个解密策略相关联。



© 2019 Palo Alto Networks, Inc.

# 激活免费许可证以使用解密功能

解密 SSH 流量 和 SSL 流量（ SSL internet 流量 或 传往内部服务器的 SSL 流量 ）时无需提供许可证。

但是，您必须激活免费许可证，以启用解密代理和解密镜像。免费许可证要求确保了，仅在授权人员有目的地激活这些相关许可证后，方可使用这些功能。

要激活解密代理或解密镜像功能许可证，请遵循 Palo Alto Networks 客户支持门户上这些步骤。

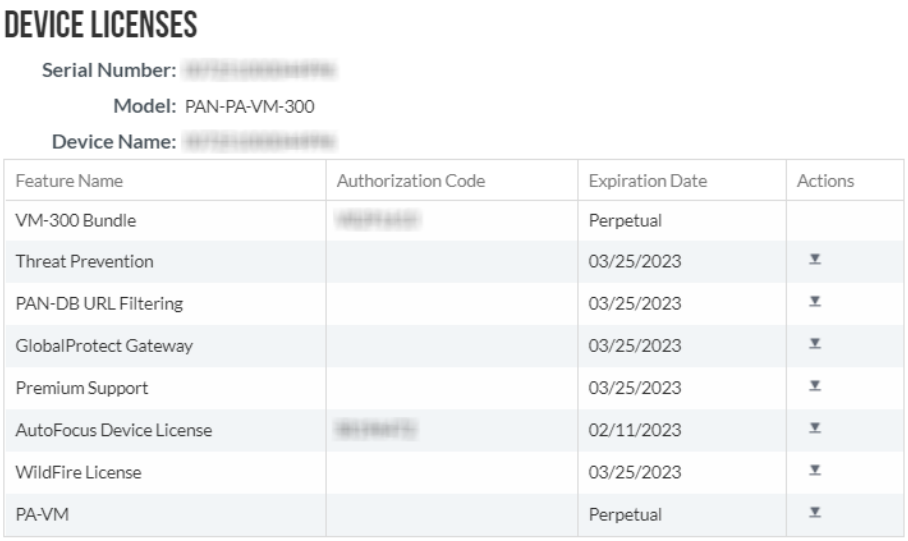
STEP 1 | 登录到客户支持门户。

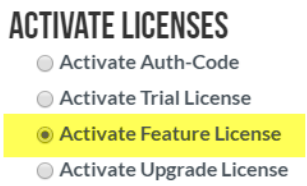
STEP 2 | 在左侧导航窗格中选择**Assets**（资产）> **Devices**（设备）。

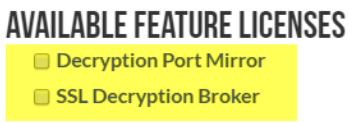
STEP 3 | 找到要启用解密代理或解密端口镜像的设备，并选择 **Actions**（操作）（铅笔图标）。

STEP 4 | 在“激活许可证”上，选择 **Activate Feature License**（激活功能许可证）。

STEP 5 | 选择想要激活免费许可证的功能：**Decryption Port Mirror**（解密端口镜像）或 **SSL Decryption Broker**（SSL 解密代理）。






© 2019 Palo Alto Networks, Inc.

STEP 6 | **Agree**（同意）并 **Submit**（提交）。

STEP 7 | 在防火墙上安装解密代理或解密端口镜像许可证。

1. 选择**Device**（设备）> **Licenses**（许可证）。
2. 单击 **Retrieve license keys from the license server**（从许可证服务器检索许可证密钥）。
3. 检验防火墙上的 **SSL Decryption Broker**（**SSL** 解密代理）或 **Decryption Port Mirror**（解密端口镜像）显示是否已激活。
4. 重启防火墙（**Device**（设备）> **Setup**（设置）> **Operations**（操作））。在防火墙重新加载前，无法配置解密端口镜像和解密代理。


© 2019 Palo Alto Networks, Inc.

# URL 筛选

Palo Alto Networks URL 筛选可让您监视和控制用户可访问的站点，通过控制用户可提交有效公司凭据的站点来防止网络钓鱼攻击，并为像 Google 和 Bing 之类的搜索引擎执行安全搜索。


> 关于 URL 筛选
> URL 筛选工作原理
> URL 过滤 Inline ML
> URL 筛选用例
> URL 分类
> 规划您的 URL 过滤部署
> URL 筛选最佳实践
> 启用 PAN-DB
> 配置 URL 筛选
> 配置 URL 过滤 Inline ML
> 监控 Web 活动
> 仅记录用户访问页面
> 创建自定义 URL 类别
> URL 类别异常
> 使用 URL 筛选配置文件中的外部动态列表
> 允许密码访问某些站点
> 预防凭证网络钓鱼
> 安全搜索执行
> URL 筛选响应页面
> 自定义 URL 筛选响应页面
> HTTP 标头日志记录
> 请求更改 URL 类别
> 对 URL 筛选进行故障排除
> PAN-DB 私有云

# 关于 URL 筛选

Palo Alto Networks URL 筛选通过向您提供安全启用 Web 访问权限，并控制您的用户与在线内容互动的方式，提供基于 Web 威胁的保护。

启用 URL 过滤后，任何端口上的所有 Web 流量（HTTP 和 HTTPS）：

- 都会与 URL 过滤数据库进行比较，该数据库中包含一个列表，其中列出了已进行分类的数百万个网站。您还可以使用这些 URL 类别作为匹配条件，实施安全策略。您还可以将 URL 过滤功能用于为用户执行安全搜索设置，并根据 URL 类别阻止凭据被盗。
- 使用 inline 机器学习 (ML)（这是一种基于防火墙的分析解决方案，可以实时阻止未知的恶意网络）检测网络钓鱼和恶意 JavaScript。

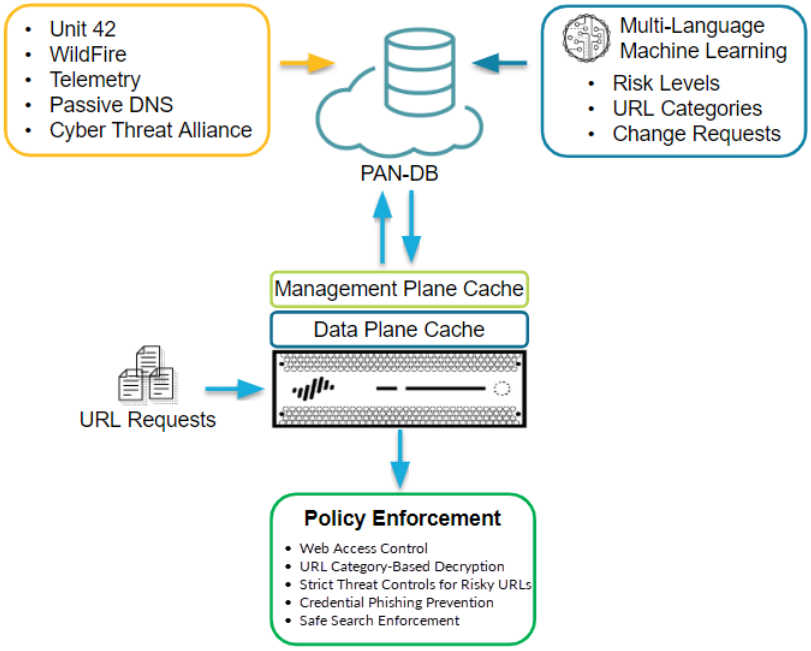
虽然有 Palo Alto Networks URL 过滤解决方案，但 PAN-DB 允许您在 *PAN-DB* 公共云和 *PAN-DB* 私有云之间进行选择。如果您网络上的 Palo Alto Networks 新一代防火墙可以直接访问 Internet，请使用公共云解决方案。如果您企业的网络安全要求禁止防火墙直接访问互联网，您可以在充当网络 PAN-DB 服务器的一台或多台 M-600 设备上部署 PAN-DB 私有云。



© 2019 Palo Alto Networks, Inc.

# URL 筛选工作原理

PAN-DB—URL 筛选云数据库—基于网站内容、功能和安全性进行网站分级。一个 URL 最多可有 4 个 URL 类别，包括指示站点将您置于危险的可能性的风险类别（高、中和低）。随着 PAN-DB 进行网站分类，启用了 URL 筛选的防火墙可通过该知识实时强制执行安全策略。




用户访问未缓存的 URL 时，防火墙将查看 PAN-DB 中站点的类别，并予以保存。防火墙保存新条目时，会将用户最近未访问的 URL 删除，这样，就能准确反映您网络中的流量。

此外，检查内置 PAN-DB 云查询，确保防火墙能够接收最新的 URL 分类信息。

在数据面板上将防火墙配置为使用机器学习实时分析 URL 后，可提供另一层安全保护，防止网络钓鱼网站攻击和 JavaScript 漏洞利用。用于识别这些基于 URL 的威胁的 inline ML 模式扩展至当前未知以及未来可能会出现的威胁（与 Palo Alto Networks 标识为恶意的特征相匹配）变体。为了跟上威胁形势的最新变化，可以通过内容发布添加或更新 inline ML 模式。

防火墙检查 PAN-DB 中的 URL 时，还会查找关键更新，例如之前被视为良性但现在被视为恶意的 URL。

如果您认为 PAN-DB 对站点进行了错误分类，您可以在您的浏览器中通过 Test A Site（测试站点）或直接从防火墙日 提交 URL 类别更改请求。



您知道吗？

从技术上而言，防火墙会将 *URL* 缓存在管理平面和数据平面上。

- *PAN-OS 9.0* 及后续版本不会下载 *PAN-DB* 种子数据库。相反，防火墙会在 *URL* 筛选许可证激活后，在执行 *URL* 查询时填充缓存。
- 管理平面会保留更多 *URL*，并直接与 *PAN-DB* 通信。一旦防火墙无法在缓存中找到 *URL* 类别，并在 *PAN-DB* 中执行查找时，就可以在管理平面上缓存检索到的类别信息。管理平面将此信息发送到数据平面，从而将其缓存，并用于实施策略。
- 数据平面保留的 *URL* 较少，可从管理平面接收信息。防火墙检查完 *URL* 的 URL 类别异常列表和自定义 URL 类别后，接着检查数据平面。只有当防火墙在数据平面中找不到 *URL* 类别时，才会检查管理平面，且如果管理平面也没有类别信息，则检查 *PAN-DB*。



© 2019 Palo Alto Networks, Inc.

# URL 过滤 Inline ML

通过 URL 过滤 inline ML，防火墙数据平面可以在网页上使用机器学习，以在检测到网络钓鱼变体时警告用户，同时防止 JavaScript 漏洞利用的恶意变体进入您的网站。inline ML 使用一系列 ML 模型评估各种网页的详细信息，从而动态分析并检测恶意内容。各个 inline ML 模型通过评估文件详细信息（包括解码器字段和模式），检测恶意内容，从而形成高概率分类和判定，然后将其用作更大型 Web 安全策略的组成部分。被 inline ML 划分到恶意类的 URL 将被转发到 PAN-DB 进行其他分析和判定。为了跟上威胁形势的最新变化，可以通过内容发布定期更新并添加 inline ML 模型。URL 过滤 inline ML 模型通过 URL 过滤配置文件进行配置，需要使用 PAN-DB URL 过滤许可证。此外，您还可以指定 URL 例外，以排除可能遇到的任何误报。这样，您就可以为配置文件创建更精细的规则，以满足特定安全需求。

作为配置防病毒配置文件的一部分，还可启用基于 Inline ML 的保护以实时检测恶意 PE 文件和 PowerShell 脚本。有关详细信息，请参阅：WildFire Inline ML

*VM-50* 或 *VM50L* 虚拟设备不支持 *URL* 过滤 *inline ML*。



© 2019 Palo Alto Networks, Inc.

# URL 筛选用例

除了仅阻止和允许某些站点外，还有很多使用 URL 筛选的方法。例如，针对每个 URL 使用多个类别，以允许用户访问站点，但是阻止提交公司凭据或下载文件等某些特定功能。此外，还可使用 URL 类别实施不同类型的策略，例如，身份验证、解密、QoS 和安全策略。

请继续阅读以了解更多有关使用 URL 筛选的不同方法。

### 基于 URL 类别控制 Web 访问

您可以创建 URL 筛选配置文件以指定 URL 类别的操作，并将该配置文件附加到策略规则中。防火墙根据配置文件中的设置对流量实施策略。例如，要阻止所有游戏网站，您可以在 URL 配置文件中为 URL 类别 *games* 设置阻止操作，并将该配置文件附加到允许 Web 访问的安全策略规则中。

### 多类别 URL 筛选

每个 URL 最多可有 4 个类别，包括指示站点将您置于危险的可能性的 risk 类别。通过对 URL 更精细的分类，您可以超越基本的“阻止或允许”方法进行 Web 访问。相反，您可以控制用户与业务所需的、但更有可能被用作网络攻击组成部分的在线内容的交互。

例如，您可能认为某些 URL 类别对您的组织有害，但是，这些类别能提供有价值的资源或服务（例如，云存储服务或博客），因此，对于是否阻止他们，您很犹豫。现在，您可以允许用户访问属于这些类型 URL 类别的站点，同时，还能通过解密和检测流量并执行内容仅读访问保护您的网络。

对于想要严格控制的 URL 类别，在执行 配置 URL 筛选 步骤时，将 URL 筛选配置文件操作设为警报。然后，继续执行 URL 筛选最佳实践：解密 URL 类别、阻止危险文件下载、并打开凭据网络钓鱼防护。

### 阻止或允许基于 URL 类别的公司凭据提交

预防凭证网络钓鱼通过启用防火墙检测站点的公司凭据提交，然后基于 URL 类别控制这些提交。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据，以及明确允许用户向公司和经批准的站点提交凭据。

### 实施安全搜索设置

很多搜索引擎都有安全搜索设置，用以筛选搜索结果中的成人图像和视频。如果最终用户未使用最严格的安全搜索设置，您可以启用防火墙来阻止搜索结果，还可以透明地启用用户安全搜索。防火墙可以针对以下搜索提供商执行安全搜索：Google、Yahoo、Bing、Yandex 和 YouTube。请参阅如何开始使用 安全搜索执行。

### 对某些站点实施密码访问权限

您可以阻止大多数用户访问站点，同时允许某些用户访问此站点。请参阅如何 允许密码访问某些站点。

### 阻止某些 URL 类别的高风险文件下载

您可以通过创建带文件阻止配置文件的安全策略阻止特定 URL 类别的高风险文件下载。

### 基于 URL 类别实施安全、解密、身份验证和 QoS 策略

您可以基于 URL 类别实施不同类型的防火墙策略。例如，假定您已启用 解密，但想排除某些个人信息被解密。在这种情况下，您可以创建解密策略规则，从解密中将与 URL 类别 *financial-services* 和 *health-and-medicine* 匹配的网站排除。又如，您可以在 QoS 策略中使用 URL 类 别*streaming-media*，以便对属于此类别的网站应用带宽控制。

下表介绍了接受 URL 类别作为匹配条件的策略：



© 2019 Palo Alto Networks, Inc.

| 策略类型 | 说明 |
| --- | --- |
| 解密 | 您还可以使用 URL 类别逐步实施解密，从解密中排除可能包含敏感信息或个人信息的 URL 类别（例如，financial-services 和 health-and-medicine）。<br>计划先对最危险的流量进行解密（URL 类别最有可能包含恶意流量，如赌博或高风险），然后在获得经验时进行解密。或者，先解密不影响业务的 URL 类别（如果出现错误，也不会影响业务），例如，新闻推送。考虑用户反馈，在这两种情况下，解密一些 URL 类别，运行报告，确保解密按预期进行，然后，逐步解密更多的 URL 类别等等。如果由于技术原因或因为选择不解密而不能对站点进行解密，则计划排除解密，将站点排除在解密之外。<br>  *URL* 筛选和解密的最佳实践是基于 *URL* 类别解密流量。 |
| 身份验证 | 要确保在允许用户访问特定类别之前对其进行身份验证，可以附加 URL 类别作为身份验证策略规则的匹配条件。 |
| **QoS** | 使用 QoS 策略来分配特定网站类别的吞吐量水平。例如，您可能想要允许 *streaming-media* 类别，但通过添加 URL 类别到 QoS 策略规则可以限制吞吐量。 |
| 安全 | 在安全策略规则中，可通过两种方式使用 URL 类别：<br>• 通过将规则选择为匹配条件，基于 URL 类别实施策略。<br>• 附加一个指定各个类别策略操作的 URL 筛选配置文件。<br>例如，贵公司的 IT 安全组需要访问 *hacking* 类别，但要拒绝其他所有用户访问此类别，您必须创建以下规则：<br>• 允许 IT 安全组访问分类为 *hacking* 的内容的安全策略规则。此安全策略规则引用 **Services/URL Category**（服务/**URL** 类别）选项卡中的 *hacking* 类别和 **Users**（用户）选项卡中的 IT 安全组。<br>• 另一个允许用户进行常规 Web 访问的安全策略规则。将用于阻止 *hacking* 类别的 URL 筛选配置文件附加到此规则。<br>在策略阻止 *hacking* 之前，必须列出允许访问 *hacking* 的策略。这是因为防火墙会对安全策略规则进行从上到下评估，因此当属于安全组的用户尝试访问 *hacking* 站点时，防火墙会先评估允许访问的策略规则，从而允许用户访问。防火墙会针对阻止访问 *hacking* 站点的常规 Web 访问规则评估其他所有组中的用户。 |



© 2019 Palo Alto Networks, Inc.

# URL 分类

PAN-DB 根据站点内容、功能和安全对网站进行分类。一个 URL 最多可以包含四个类别，包括用于表明站点让您暴露于威胁的程序的风险类别（高、中和低）。

访问测试站点以查看 PAN-DB 如何对 URL 进行分类，并了解所有可用的 URL 类别。此外，您还可以通过测试站点提交 URL 类别更改请求，或是，在防火墙中直接提交请求，方式如下：选择 **Monitor**（监控）> **Logs**（日志），然后打开日志条目详细信息。在 URL 类别下，您将看到用于提交更改请求的选项。

继续阅读以了解更多关于 URL 类别的信息：

- URL 筛选用例
- 以安全为中心的 URL 类别
- 恶意 URL 类别
- 经过验证的 URL 类别
- 可基于 URL 类别采取的策略操作

## 以安全为中心的 URL 类别

通过以安全为中心的 URL 类别，针对具有不同风险级别但尚未确认为恶意的站点，可采用具有针对性的解密和实施，从而帮助您减少攻击面。只有当网站满足该类别的标准时，才能归类到安全相关的类别。随着站点内容的变化，策略实施也会动态发生变化。您不能为以安全为中心的 URL 类别提交更改请求。

| 以安全为中心的 URL 类别 | |
|---|---|
| 高风险 | 高风险站点包括：<br>• 先前被确认为恶意软件、网络钓鱼或 C2 站点的站点。这些站点仍将保留在该类别中至少 30 天。<br>• 只有当 PAN-DB 完成站点分析和分类后，未知域才能被分类为高风险。<br>• 与已确认恶意活动相关联的站点。例如，如果同一域中存在恶意主机，则页面可能存在高风险，即使该页面本身不包含任何恶意内容。<br>• 防弹 ISP 托管站点<br>• 因存在活跃的动态 DNS 配置而被分类为 DDNS 的域。<br>• 源于已知允许恶意内容的 ASN 的 IP 托管站点。<br>默认和推荐策略操作：警报 |
| 中等风险 | 中等风险站点包括：<br>• 所有云存储站点（URL 类别为 **online-storage-and-backup**（在线存储和备用））<br>• 先前已被确认为恶意和网络钓鱼的站点，或至少 30 天仅显示良性活动的 C2 站点。这些站点将在该类别中再保留 60 天。<br>• 只有当 PAN-DB 完成站点分析和分类后，未知 IP 地址才能被分类为中等风险。<br>默认和推荐策略操作：警报 |
| 低风险 | 非中等风险或高风险的站点被视为低风险。这些站点至少 90 天显示良性活动。 |


© 2019 Palo Alto Networks, Inc.

| 以安全为中心的 URL 类别 | |
|---|---|
| | 默认和推荐策略操作：允许 |
| 新注册域 | 标识在过去 32 天内注册的站点。新域通常用作恶意活动中的工具。<br>默认策略操作：警报<br>推荐策略操作：阻止<br>新注册域通常是有目的地生成，或是通过域生成算法生成，专用于恶意活动。它是阻止此 *URL* 类别的最佳做法。 |

## 恶意 URL 类别

我们强烈建议您阻止标识有恶意或破坏性内容的 URL 类别。开始时，您可以克隆默认阻止恶意软件、网络钓鱼和命令和控制 URL 类别的默认 URL 筛选配置文件。此外，默认 URL 筛选配置文件还可以阻止滥用药物、成人、赌博、黑客、可疑的和武器类 URL 类别。是否阻止这些 URL 类别取决于您的业务要求。例如，大学可能不希望学生们访问大部分的这些网站，原因是可用性很重要，但是，视安全第一的企业可能会阻止某些或所有站点。

- **Command-and-control**（命令和控制）—— 恶意软件和/或受影响的系统使用命令和控制 URL 及域名与攻击者的远程服务器暗中交流，以接收恶意软件指令或泄露数据。
- **Malware**（恶意软件）— 已知有恶意软件或用于命令和控制 (C2) 流量的站点。也可能显示有渗透代码工具包。
- **Phishing**（钓鱼）— 已知有认证钓鱼页面，或钓鱼获取个人身份信息。
- **grayware**（灰色软件）— 不符合病毒定义，不构成直接安全威胁，但表现出干扰行为，且影响用户授予远程访问权限或执行其他未经授权操作的网站和服务。灰色软件包括诈骗、非法活动、犯罪活动、快速致富站点、广告软件以及其他不需要或未经批准的应用程序，例如，更改浏览器元素的嵌入式挖矿程序或劫持程序。没有显示恶意行为，且不属于目标域的误植域名将被归类到灰色软件。在内容发布版本 8206 之前，防火墙将灰色软件列入到恶意软件或可疑 URL 类别中。如果您不确定是否阻止灰色软件，请先发出灰色软件警报，然后调查警报，最后决定是阻止灰色软件还是继续发出灰色软件警报。
- **Dynamic-dns**（动态 **DNS**）— 动态指定 IP 地址的系统主机和域名，常常被用来传送恶意负荷或 C2 流量。而且动态 DNS 域名不会像由信誉良好的域名注册公司注册的域名那样通过审批流程，因此也不那么值得信赖。
- **Unknown**（未知）— PAN-DB 尚未标识的站点。如果可用性对您的业务至关重要，您必须允许流量、对未知站点发出警报、针对流量应用最佳实践安全配置文件，并对警报进行调查。

  *PAN-DB* 实时更新可在首次尝试访问未知站点后了解该未知站点，这样，就可快速标识未知 *URL*，并将未知 *URL* 变为已知 *URL*，以便防火墙在以后可根据实际的 *URL* 类别对其进行处理。
- **Newly-registered-domains**（新注册域）— 新注册域通常是有目的地生成，或是通过域生成算法生成，专用于恶意活动。
- **copyright-infringement(版权侵权)**— 具有非法内容的域名，例如允许非法下载可带来潜在责任风险的软件或其他知识产权的内容。介绍此类别以遵守教育领域要求的儿童保护法，及要求互联网提供商预防用户通过其服务共享受版权保护的资料的国家的法律。
- **extremism**（极端主义）— 宣扬恐怖主义、种族主义、法西斯主义或歧视不同种族背景、宗教或其他信仰的个人或群体的其他极端主义观点。介绍此类别旨在遵守教育行业要求的儿童保护法。在某些地区，法律和法规可能会禁止访问极端主义站点，允许访问这些站点可能会带来责任风险。
- **Proxy-avoidance-and-anonymizers**（回避代理和匿名者可疑的）— 常用来绕开内容筛选产品的 URL 和服务。
- **questionable**（可疑）— 包含针对特定个人或人群的恶趣味和攻击性内容的网站。


© 2019 Palo Alto Networks, Inc.

- **Parked**（寄放的）— 由个人注册的域名，后来常常会发现用作认证钓鱼。这些域名可能与合法域名很相似，如 pal0alto0netw0rks.com，就试图钓鱼获取认证或个人身份信息。或者可能是个人购买，希望有一天会有价值的域名，如 panw.net。

对于您决定发出警报，而非阻止的类别，可以非常严格地控制用户与站点内容的交互方式。例如，允许用户访问他们需要的资源（例如，出于研究目的访问开发人员博客或云存储服务），但采取以下预防措施降低暴露于基于 Web 的威胁：

- 遵循防间谍软件、漏洞保护、和文件阻止最佳实践。采取的保护措施应能阻止下载危险文件类型，并能阻止您发出警报的站点使用混淆的 JavaScript。
- 基于 URL 类别的目标解密。解密高风险和中等风险站点就是一个良好的开端。
- 在用户访问高风险和中等风险站点时向其显示响应页面。警告用户，他们试图访问的站点可能存在恶意，并在其决定继续访问站点时建议用户如何采取预防措施。
- 通过阻止用户向包括高风险和中等风险站点在内的站点提交其公司凭据，可防止凭据被盗。

## 经过验证的 URL 类别

已通过 Palo Alto Networks 验证，并纳入到特定类别组的 URL 不具有相关风险级别；风险级别仅适用于未经过验证的 URL。某些类别中经过验证的 URL（如下所示）被认为具有恶意，且默认被阻止，因为访问这些 URL 所带来的风险超过大多数环境中可接受的水平。专用 IP 地址（和主机）在主机环境中是唯一的，对 PAN-DB 不可见；因此，不会产生风险评级。

| 类别 | 默认操作 |
|---|---|
| 恶意软件 | 阻止 |
| 网络仿冒 | |
| 命令和控件 | |
| 灰色软件 | |
| 专用 **IP** 地址 | 已允许（无默认操作） |

有关当前 *URL* 类别的更多信息，请参阅：PAN-DB URL 过滤类别的完整列表

## 可基于 URL 类别采取的策略操作

在防火墙上，您可以使用 URL 筛选配置文件指定您想要实施 URL 类别的方式。默认情况下，创建新的 URL 筛选配置文件时，可将所有 URL 类别的站点访问设置为允许。这意味着，用户能够自由浏览所有站点且不会记录流量。通过确定您想要针对每个类别实施的 **Site Access**（站点访问权限），自定义 URL 筛选配置文件。为了防止凭据网络钓鱼，您还可以根据 URL 类别允许或禁用 **User Credential Submissions**（用户凭据提交）（例如，您可以阻止中风险和高风险站点的用户凭据提交）。用户仍可以访问这些站点，但不能向这些站点提交公司凭据。

开始实施您在 URL 筛选中定义的操作时，您需要将配置文件附加到安全策略规则中。防火墙会对匹配安全策略规则的流量实施配置文件操作（有关详细信息，请参阅配置 URL 筛选）。

进一步了解配置最佳实践 URL 筛选配置文件的相关信息，以避免 *URL* 受到出现的托管恶意软件或破坏性内容的攻击。


© 2019 Palo Alto Networks, Inc.

| 操作 | 说明 |
| --- | --- |
| 站点访问 | |
| 警报 | 允许网站且在 URL 筛选日志中生成日志条目。<br>  设置 *alert*（警报）作为您不会阻止记录的流量类别的操作，并提供流量的可见性。 |
| 允许 | 允许网站且不生成任何日志条目。<br>  因为您无法查看未记录的流量，因此，请勿将 *allow*（允许）设置作为您不会阻止的流量类别的操作。相反，应设置 *alert*（警报）作为您不会阻止记录的流量类别的操作，并提供流量的可见性。 |
| **block** | 阻止网站，用户将会看到响应页面且无法继续访问网站。同时会在 URL 筛选日志中生成日志条目。<br>阻止 URL 类别的站点访问也会为该 URL 类别设置用户凭据提交，以进行阻止。 |
| 继续 | 系统会为用户提示表明因公司政策已阻止该网站的响应页面，但会提示用户选择继续访问网站。**continue**（继续）操作通常用于被视为良性的类别，并可在他们觉得此站点的分类不正确时，为其提供继续选项来提升用户体验。可以自定义响应页面消息以包含特定于贵公司的详细信息。同时会在 URL 筛选日志中生成日志条目。<br>  继续页面不会正常显示在配置为使用代理服务器的客户端系统上。 |
| 替代 | 用户将会看到一个响应页面，表明允许访问指定类别中的网站需要密码。使用此选项，安全管理员或技术支持人员会提供密码，以授予指定类别中所有网站的临时访问权。同时会在 URL 筛选日志中生成日志条目。请参阅允许密码访问某些站点。<br>在早期发行版本中，URL 筛选类别替代可优先于自定义 URL 类别进行实施。升级到 PAN-OS 9.0 后，URL 类别替代项将转换为自定义 URL 类别，但不再优先于其他自定义 URL 类别实施。新的自定义 URL 类别采用最严格的 URL 筛选配置文件操作（而非在先前发行版本中为类别替代定义的操作）通过安全策略规则实施。可能的 URL 筛选配置文件操作从最严格到最不严格排序为：阻止、替代、继续、警报和允许。<br>这意味着，如果您的 URL 类别替代操作为允许，在 PAN-OS 9.0 中转换为自定义 URL 类别后，替代项可能会被阻止。<br>  替代页面不会正常显示在配置为使用代理服务器的客户端系统上。 |
| 无 | **none**（无）操作仅适用于自定义 URL 类别。选择 **none**（无）的目的是确保自定义类别将不会对其他配置文件产生任何影响（如果存在多个 URL 配置文件）。例如，如果您有两个 URL 配置文件，且一个配置文件中的自定义 URL 类别设置为 **block**（阻止），如果您不想阻止操作应用于另一个配置文件，您必须将此操作设置为 **none**（无）。<br>另外，要删除自定义 URL 类别，必须在使用该类别的任意配置文件中将其设置为 **none**（无）。 |


© 2019 Palo Alto Networks, Inc.

| 操作 | 说明 |
| --- | --- |
| 用户凭据权限 | |
|  这些设置需要您首先设置凭据网络钓鱼防护。 | |
| 警报 | 允许用户向此 URL 类别的站点提交公司凭据，但在每次发生时都会生成 URL 筛选警报日志。 |
| allow（允许）（默认） | 允许用户向此 URL 类别的网站提交公司凭据。 |
| block | 阻止用户向此 URL 类别的网站提交公司凭据。当用户访问阻止公司凭据提交的站点时，将向用户显示默认反网络钓鱼响应页面。您可以选择创建自定义阻止页面进行显示。 |
| 继续 | 向用户显示响应页面，提示他们选择继续以访问站点。默认情况下，当用户访问不鼓励凭据提交的站点时，将向用户显示反网络钓鱼继续页面。您还可以选择创建自定义响应页面进行显示 — 例如，如果要警告用户不要尝试进行网络钓鱼或在其他网站上重用其凭据时。 |


© 2019 Palo Alto Networks, Inc.

# 规划您的 URL 过滤部署

要首先在网络中部署 URL 过滤，我们建议您从基本设置开始，这样，您可以在阻止已确认恶意内容时查看 Web 活动模式：

- 从对大多数类别发出警报的（大多数）被动 URL 过滤配置文件开始。这样，您可以看到用户正在访问的站点，从而决定您想要允许、限制和阻止的内容。
- 阻止我们已知为恶意的 URL 类别：恶意软件、C2 和网络钓鱼。

因为向所有 Web 活动发出警报可能会创建大量日志文件，因此，您可能会决定只在您最初部署 URL 过滤时才这样做。

此时，您也可以通过启用 *URL* 过滤配置文件中的 *Log container page only*（仅日志容器页面）选项减少 *URL* 过滤日志，这样就只会记录与类别匹配的主页面，而非可能已在容器页面中加载的后续页面/类别。

STEP 1 | 您可以随时使用 Test A Site（测试站点）来查看 PAN-DB（URL 过滤云数据库）如何对特定 URL 进行分类，并了解所有可能的 URL 类别。

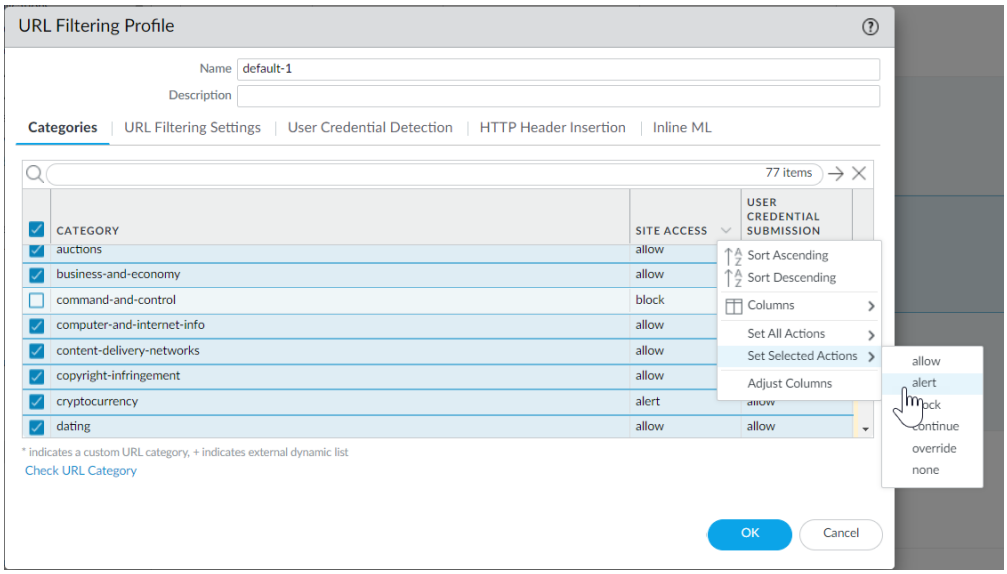
如果您不同意特定 URL 的分类方式，还可以使用 Test A Site（测试站点）提交更改请求。

STEP 2 | 创建一个可对所有类别发出警报以使您能够查看网络流量的被动 URL 过滤配置文件。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）**>URL Filtering**（**URL** 过滤）。
2. 选择默认配置文件，然后单击 **Clone**（复制）。新的配置文件将命名为 **default-1**。
3. 选择 **default-1** 配置文件并重命名。例如，将其重命名为 URL-Monitoring。

STEP 3 | 除应保持阻止状态的恶意软件、命令和控制、以及网络钓鱼外，请将所有类别的操作配置为 **alert**（警报）。

1. 在列出所有 URL 类别的部分，选择所有类别，然后取消选择恶意软件、命令和控制以及网络钓鱼。
2. 在操作列标题右侧，鼠标悬停在上方并选择向下箭头，然后依次选择 **Set Selected Actions**（设置选定操作）和 **alert**（警报）。




3. **Block**（阻止）访问已知的危险 URL 类别。



© 2019 Palo Alto Networks, Inc.

阻止访问恶意软件、网络钓鱼、动态 *DNS*、未知、命令和控制、极端主义、版权侵犯、回避代理和匿名者、新注册域、灰色软件以及寄放等 *URL* 类别。

4. 单击 **OK**（确定）保存配置文件。

STEP 4 | 将 URL 过滤配置文件应用到安全策略规则以允许用户的 Web 流量。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择相应的安全策略以进行修改。
2. 选择 **Actions**（操作）选择卡，然后在 **Profile Setting**（配置文件设置）部分中，单击 **URL Filtering**（**URL** 过滤）下拉列表，并选择新的配置文件。
3. 单击 **OK**（确定）以保存。

STEP 5 | 保存配置。

单击 **Commit**（提交）。

STEP 6 | 查看 URL 过滤日志以查看用户访问的所有网站类别。此外还会记录您已设为阻止的类别。

有关查看日志和生成报告的信息，请参阅监控 Web 活动。

选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 过滤）。将会为 URL 过滤数据库中存在的所有网站创建日志条目，该数据库属于设置为任何操作（非 **allow**（允许））的类别。您可以通过 URL 过滤报告查看 24 小时内的 Web 活动。（**Monitor**（监控）> **Reports**（报告））。

STEP 7 | 后续步骤：

- PAN-DB 最多可将每个 URL 分为四个类别，且每个 URL 都存在一个风险类别（高、中、低）。虽然高风险和中风险站点未被证实是恶意的，但他们与恶意站点密切关联。例如，他们可能与恶意站点位于同一域中，或可能直到最近他们才托管有恶意内容。对于您不允许或阻止的任何事件，可以使用风险类别，根据网站安全性写入简单的策略。

  您可以采取预防措施限制高风险的用户交互站点，尤其是在您想授予用户访问存在安全隐患的站点之权限的某些情况下（例如，您可能想让开发人员使用开发者微博进行研究，但是，已知微博通常是托管恶意软件的类别。）
- URL 过滤与 User-ID 配对后，可对基于组织或部门的 Web 访问进行控制，并阻止将公司凭据提交至未经批准的站点：
  - URL 过滤根据站点类别检测公司凭据提交到站点的情况，从而防止凭据被盗。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据、并明确允许用户向公司站点提交凭据。
  - 使用被动 URL 过滤配置文件添加或更新安全策略规则，以便将其应用到市场部或工程部等部门用户组（**Policies**（策略）> **Security**（安全）> **User**（用户））。监视部门活动，获得部门成员反馈，从而了解对部门工作必不可少的 Web 资源。
- 始终考虑使用 URL 过滤来减少您的攻击面，控制 Web 使用情况。例如，如果在学校内，您可以使用 URL 过滤执行严格的安全搜索设置，这样，搜索引擎就会将搜索结果中的成人图像和视频筛除。或者，如果是在安全运营中心，您可以向威胁分析人员提供进入受影响或危险站点进行搜索所需的密码访问权限，这样，就不会向整个组织或团队开放这些站点。
- 请遵守 URL 筛选最佳实践。


© 2019 Palo Alto Networks, Inc.

# URL 筛选最佳实践

Palo Alto Networks URL 筛选可保护您免遭基于 Web 的威胁，并为您提供一种监视和控制 Web 活动的简单方法。若要最大化地利用 URL 过滤，您应先为您开展业务所需的应用程序创建一个允许列表。然后，查看划分为恶意和攻击性内容的 URL 类别，我们建议您阻止这些类别。接下来，对其他方面而言，此最佳实践可指导您如何在不限制用户访问所需 Web 内容的情况下减少暴露于基于 Web 的威胁。

- 在您开始执行 URL 过滤之前，请标识您想允许的应用程序，然后创建应用程序允许规则，将其作为最佳实践互联网网关安全策略的组成部分。

  允许的应用程序不仅包括您出于业务和基础结构目的而提供和管理的应用程序，还包括您的用户为完成工作所需的其他应用程序，以及您允许用于个人目的的应用程序。

  标识完这些经过批准的应用程序后，您可以使用 URL 过滤控制和保护未列入到允许列表中的所有 Web 活动。
- 深入了解用户的 Web 活动，这样，您可以为您的组织规划出最有效的 URL 筛选策略，并使其顺利运行。这包括：
  - 使用 Test A Site（测试站点）查看 PAN-DB（URL 筛选云数据库）如何对特定 URL 进行分类，并了解所有可能的 URL 类别。
  - 从发出 URL 类别警报的（大多数）被动 URL 筛选配置文件开始。这样，您可以看到用户正在访问的站点，从而决定您想要允许、限制和阻止的内容。
  - 监控 Web 活动以评估用户正在访问的站点，并查看这些站点如何与您的业务需求保持一致。
- 阻止被划分为恶意和攻击性 Web 内容的 URL 类别。虽然我们知道这些类别很危险，但是请始终记住，您可能需要根据您的业务需求确定要阻止的 URL 类别。
- 使用 URL 类别逐步实施解密，从解密中排除敏感信息或个人信息（例如，financial-services 和 health-and-medicine）。

  计划先对最危险的流量进行解密（URL 类别最有可能包含恶意流量，如赌博或高风险），然后在获得经验时进行解密。或者，先解密不影响业务的 URL 类别（如果出现错误，也不会影响业务），例如，新闻推送。考虑用户反馈，在这两种情况下，解密一些 URL 类别，运行报告，确保解密按预期进行，然后，逐步解密更多的 URL 类别等等。如果由于技术原因或因为选择不解密而不能对站点进行解密，则计划排除解密，将站点排除在解密之外。

  根据 *URL* 类别进行有针对性的解密也是一种解密最佳实践。
- 通过启用防火墙检测站点的公司凭据提交情况阻止凭据被盗，然后基于 URL 类别控制这些提交。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据，以及明确允许用户向公司和经批准的站点提交凭据。
- 实时阻止 JavaScript 漏洞利用和网络钓鱼攻击的恶意变体。启用URL 过滤 Inline ML后，您可以通过防火墙上的机器学习动态分析 Web 页面。
- 解密、检查并严格限制用户与高风险和中风险内容（如果您出于业务原因不阻止任何恶意 URL 类别，您应严格限制用户与这些类别的交互）的交互。

  您批准的 Web 内容和您完全阻止的恶意 URL 类别都只是您整个 Web 流量的一部分。用户访问的其他内容包括良性内容（低风险）和风险内容（高风险和中风险）。高风险和中风险内容未被证实是恶意的，但他们与恶意站点密切关联。例如，高风险 URL 可能与恶意站点处于同一域中，或是过去可能托管过恶意内容。

  但是，很多对您组织构成风险的站点还能为您的用户提供有价值的资源和服务（云存储服务就是其中一个很好的示例）。尽管这些资源和服务是业务所必需的，但是，他们也很容易成为网络攻击的一部分。以下介绍了如何在确保用户良好体验的同时控制用户与这些存在潜在危险内容进行交互的方式：



© 2019 Palo Alto Networks, Inc.

- 在 URL 筛选配置文件中，设置高风险和中风险类别，以继续显示响应页面，从而警告用户，他们正在访问存在潜在危险的站点。如果用户决定继续前往该站点，请告知他们如何采取预防措施。如果您不想通过响应页面提示用户，可发出高风险和中风险类别警报。
- Decrypt（解密）解密高风险和中风险站点。
- 遵循高风险和中风险站点的防间谍软件、漏洞保护和文件阻止最佳实践。采取的保护措施应能阻止下载危险文件类型，并能阻止混淆的 JavaScript。
- 通过阻止用户向高风险和中风险站点提交其公司凭据，可防止凭据被盗。

- 学校或教育机构应使用安全搜索，确保搜索引擎将搜索结果中的成人图像和视频筛除。您甚至可以透明地启用用户安全搜索。
- 启用防火墙，使其在通过 PAN-DB 查找网站 URL 类别时保留初始 Web 请求。

  用户访问网站时，防火墙可通过启用 URL 筛选检查其 URL 类别的本地缓存，从而对网站进行分类。如果防火墙未在缓存中找到 URL 类别，将在 Palo Alto Networks URL 数据库 (PAN-DB) 中进行查找。默认情况下，防火墙在执行该云查找时允许用户发出 Web 请求，并在服务器响应时实施策略。

  但是，一旦您选择保留 Web 请求，除非防火墙找到 URL 类别或是超时，否则，防火墙将阻止该请求。如果查找超时，则防火墙认为 URL 类别是未解析的。

  1. 在**Device**（设备）> **Setup**（设置）> **Content-ID** 中，选中以下复选框

     **Hold client request for category lookup**（保持客户端类别查找请求）。


© 2019 Palo Alto Networks, Inc.

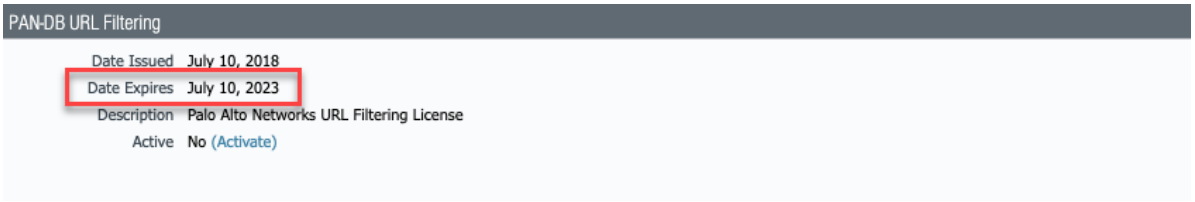
# 启用 PAN-DB

PAN-DB 是一种基于 Palo Alto Networks 开发出的 URL 筛选数据库，可提供高性能本地高速缓存，使 URL 查询获得最大内联性能，同时能覆盖恶意 URL 和 IP 地址。在 WildFire 识别未知的恶意软件、零日漏洞和高级持续性威胁 (APT) 时，PAN-DB 数据库会更新恶意 URL 的信息，使您能够阻止恶意软件下载，同时禁用命令和控制 (C2) 通信来保护您的网络免受网络威胁的侵害。识别确认的恶意内容（恶意软件、钓鱼和 C2）的 URL 类别每五分钟更新一次，以确保您可以在分类的数分钟内，管理对这些站点的访问。

STEP 1 | 获取和安装 PAN-DB URL 筛选许可证，并确认已安装。

如果许可证过期，防火墙将停止执行 *PAN-DB URL* 筛选；在安装有效许可证之前，*URL* 类别实施、*URL* 云查询以及其他基于云的更新也将无法运行。

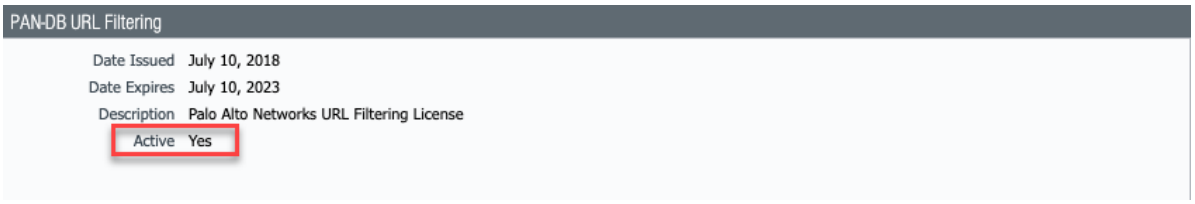
1. 选择 **Device**（设备）> **Licenses**（许可证），然后在“许可证管理”部分中选择许可证安装方法：
   - **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）
   - **Activate feature using authorization code**（使用授权代码激活功能）
   - **Manually upload license key**（手动上载许可证密钥）
2. 安装好许可证之后，确认 PAN-DB URL 筛选部分的 **Date Expires**（到期日期）字段是否显示有效日期。




STEP 2 | 激活 PAN-DB URL 筛选。

*PAN-OS 9.0* 及后续版本不会下载 *PAN-DB* 种子数据库。相反，防火墙会在 *URL* 筛选许可证激活后，在执行 *URL* 查询时填充缓存。

1. 单击 **Activate**（激活）。“激活”字段中的值更改为“是”。




STEP 3 | 为防火墙制定应用程序和威胁的相关动态更新下载计划。

接收内容更新需要威胁防御许可证，其中涵盖抗病毒以及应用程序和威胁。

1. 选择**Device**（设备）> **Dynamic Updates**（动态更新）。



© 2019 Palo Alto Networks, Inc.

2. 在“应用程序和威胁”部分的“计划”字段中，单击 **None**（无）链接以计划定期更新。

   如果防火墙拥有直接互联网访问权限，那么您只能计划动态更新。如果已在某个部分中计划过更新，那么链接文本会显示计划设置。

   应用程序和威胁更新有时包含与安全搜索执行相关的 URL 筛选更新。



© 2019 Palo Alto Networks, Inc.

# 配置 URL 筛选

在确定 URL 筛选策略要求后，您应该能够基本了解用户访问的网站类型和网站类别。使用这些信息创建自定义 URL 筛选配置文件，并将其附加到用于允许 Web 访问的安全策略规则。除了通过 URL 筛选配置文件管理 Web 访问之外，如果已配置 User-ID™，可以管理用户可向其提交公司凭据的站点。

STEP 1 | 创建 URL 筛选配置文件。



如果尚未执行该操作，请配置最佳实践 URL 筛选配置文件，以确保 *URL* 不受托管恶意软件或破坏性内容的攻击。

选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选），并 **Add**（添加）URL 筛选配置文件。

STEP 2 | 为每个 URL 类别定义站点访问。

选择 **Categories**（类别），并为每个 URL 类别设置站点访问：

- **allow**（允许）发往该 URL 类别的流量；允许流量未被记录。
- 选择 **alert**（警报）以查看用户访问的网站。允许与此类别匹配的流量，但应生成 URL 筛选日志以记录用户访问此类别中站点的时间。
- 选择 **block**（阻止）以拒绝访问与此类别匹配的流量，并启用已阻止流量的日志记录。
- 选择 **continue**（继续）可以向带有警告的用户显示一个页面，并要求他们单击 **Continue**（继续）以继续进入此类别的站点。
- 如仅允许在用户有提供配置密码的情况下进行访问，请选择 **override**（替代）。更多详细信息，请参阅允许密码访问某些站点。

STEP 3 | 配置 URL 筛选配置文件以检测提供给允许的 URL 类别的网站的公司凭据。



即使启用相应类别中的检查，防火墙仍会自动跳过检查与从未出现托管恶意软件或破坏性内容的站点相关的任何 *App-ID*™ 凭据提交情况，以确保最佳性能和低误报率。防火墙跳过凭据检查的站点列表通过应用程序和威胁内容更新自动更新。

1. 选择 **User Credential Detection**（用户凭据检测）。
2. 从 **User Credential Detection**（用户凭据检测）下拉列表的网页中选择其中一个检查公司凭据提交方法：
   - **Use IP User Mapping**（使用 **IP** 用户映射）— 检查有效的公司用户名提交，并验证用户名是否与登录至会话源 IP 地址的用户相匹配。要使用该方法，防火墙根据其 IP 地址到用户名的映射表匹配提交的用户名。要使用该方法，您可使用IP 地址映射到用户中描述的任何用户映射方法。
   - **Use Domain Credential Filter**（使用域凭据筛选器）— 检查有效的公司用户名和密码提交，并验证用户名是否映射到用户登录的 IP 地址。有关如何设置 User-ID 以启用此方法的说明，请参阅使用 Windows User-ID 代理配置用户映射。
   - **Use Group Mapping**（使用组映射）— 当防火墙配置为将用户映射到组时，根据用户到组映射表检查有效的用户名提交。

     使用组映射，您可以将凭据检测应用于目录的任何部分或特定组，例如可以访问最敏感应用程序的 IT 组。

     在用户名结构不是唯一的环境中，这种方法容易产生误报，因此，应仅使用此方法保护高价值用户账户。
3. 设置防火墙用于记录公司凭据提交检测的 **Valid Username Detected Log Severity**（有效用户名检测到的日志严重性）（默认为中等）。



© 2019 Palo Alto Networks, Inc.

STEP 4 | 配置“URL 过滤”配置文件，以使用URL 过滤 Inline ML实时检测网络钓鱼和恶意 JavaScript。

STEP 5 | 允许或阻止用户根据 URL 类别将公司凭据提交到站点，以便阻止凭据网络钓鱼。



即使启用相应类别中的检查，防火墙仍会自动跳过检查与从未出现托管恶意软件或破坏性内容的站点相关的 *App-ID* 凭据提交情况，以确保最佳性能和低误报率。防火墙跳过凭据检查的站点列表通过应用程序和威胁内容更新自动更新。

1. 对于允许 **Site Access**（站点访问）的每个 URL 类别，选择要处理 **User Credential Submissions**（用户凭据提交）的方法：
   - **alert**（警报）— 允许用户向站点提交凭据，但每次用户在该 URL 类别中向站点提交凭据时生成 URL 筛选警报日志。
   - **allow**（允许）（默认）— 允许用户向网站提交凭据。
   - **block**（阻止）— 显示防钓鱼阻止页面以阻止用户将凭据提交到网站。
   - **continue**（继续）— 显示防钓鱼继续页面，要求用户单击 **Continue**（继续）以访问该网站。
2. 配置 URL 筛选配置文件以检测提交给允许 URL 类别中网站的公司凭据。

STEP 6 | 定义 URL 类别异常列表，以指定始终应阻止或允许的网站，而不考虑 URL 类别。

例如，要减少“URL 过滤”日志，您可能想将公司网站加入到允许列表中，这样，这些站点就不会生产任何日志；或者，如果某个与工作无关的网站使用极度频繁，您可以将此站点添加到阻止列表。

无论相关类别的操作怎样，都将始终阻止阻止列表中的网站流量，始终允许允许列表中的 URL 流量。

有关正确格式和通配符使用的更多信息，请参阅 URL 类别异常列表。

1. 选择 **Overrides**（覆盖），并在 **Block List**（阻止列表）中输入 URL 或 IP 地址，然后选择一种操作：
   - **block**（阻止）— 阻止 URL。
   - **continue**（继续）— 提示用户单击 **Continue**（继续）以继续访问 Web 页面。
   - **override**（覆盖）— 提示用户输入密码以继续访问网站。
   - **alert**（警报）— 允许用户访问网站并在 URL 日志中添加警报日志条目。
2. 对于 **Allow**（允许）列表，输入应始终允许的 IP 地址或 URL。每一行必须用换行分隔。

STEP 7 | 启用安全搜索执行。

STEP 8 | 仅记录 URL 筛选事件日志容器页面。

1. 选择 **URL Filtering Settings**（**URL** 筛选设置）。**Log container page only**（仅记录容器页面）选项默认会启用，以便防火墙只记录与此类别匹配的主页面，而非已在容器页面中加载的后续页面或类别。
2. 要为所有页面和类别启用日志记录，请禁用 **Log container page only**（仅记录容器页面）选项。

STEP 9 | 为一个或多个受支持 HTTP 标头字段启用 HTTP 标头日志记录。

选择 **URL Filtering Settings**（**URL** 筛选设置），然后选择一个或多个以下字段进行记录：

- **User-Agent**（用户代理）
- **Referer**（推荐人）
- **X-Forwarded-For**

STEP 10 | 保存 URL 筛选配置文件并提交更改。

1. 单击 **OK**（确定）。
2. 单击 **Commit**（提交）。



要测试 *URL* 筛选配置，请访问设置为阻止的类别中的网站，或继续查看防火墙是否执行相应的操作。



© 2019 Palo Alto Networks, Inc.

STEP 11 | 在防火墙执行 URL 类别查找时，启用 **Hold client request for category lookup**（保持客户端类别查找请求）以阻止客户端请求。

1. 选择 **Device**（设备）> **Setup**（设置）> **Content - ID**（内容 ID）。
2. 选择 **Hold client request for category lookup**（保持客户端类别查找请求）。
3. Commit（提交）更改。



启用此功能作为 URL 筛选最佳实践。

STEP 12 | 设置 URL 类别查找超时之前的时间量，以秒计。

1. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID** > **gear icon**（齿轮图标）。
2. 输入 **Category lookup timeout (sec)**（类别查找超时（秒））时间量。
3. 单击 **OK**（确定）。
4. Commit（提交）更改。



© 2019 Palo Alto Networks, Inc.

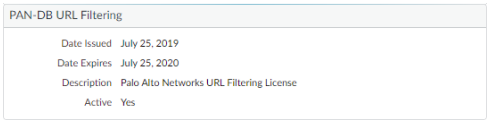
# 配置 URL 过滤 Inline ML

要启用 URL 过滤 inline ML，请将使用 inline ML 设置配置的“URL 过滤”配置文件附加到安全策略规则（请参阅 设置基本安全策略）。

*VM-50* 或 *VM50L* 虚拟设备当前不支持 *URL* 过滤 *inline ML*。

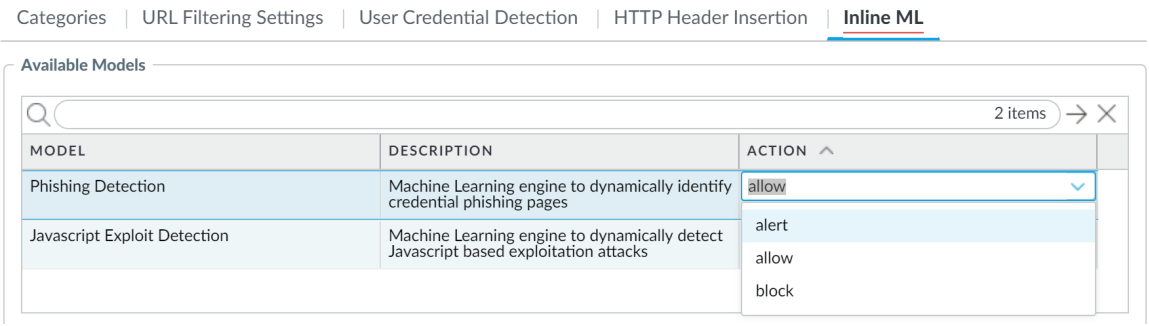
STEP 1 | 若要利用 URL 过滤 inline ML，必须具有有效的 PAN-DB“URL 过滤”订阅才能分析网页中的 JavaScript 和网络钓鱼威胁。

确认您是否具有 PAN-DB URL 过滤订阅。若要检查您是否拥有当前有效的许可证订阅，请选择 **Device**（设备）> **Licenses**（许可证），确认是否显示相应的许可证，许可证是否已过期。




STEP 2 | 创建新的 URL 过滤安全配置文件，或是更新现有 URL 过滤安全配置文件以使用 URL 过滤 inline ML。

1. 选择现有 **URL Filtering Profile**（**URL** 过滤配置文件）或是 **Add**（添加）新的配置文件（**Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 过滤））。
2. 选择 **Inline ML**，并定义每个 URL 过滤 inline ML 模式的策略 **Action**（操作）。这样，就可根据每个模式，实施所选的策略操作。目前提供两种分类引擎：**Phishing**（网络钓鱼）和 **JavaScript Exploit**（**JavaScript** 利用），各对应一种类型的恶意网页内容。
   - **Block**（阻止）— 防火墙检测网页上的网络钓鱼内容时，会生成 URL 过滤日志条目。
   - **Alert**（警报）— 防火墙允许访问网站，但还是会生成 URL 过滤日志条目。
   - **Allow**（允许）— 防火墙允许访问网站，但不会生成 URL 过滤日志条目。




3. 单击 **OK**（确定）以退出 URL 过滤配置文件配置对话框，然后 **Commit**（提交）更改。

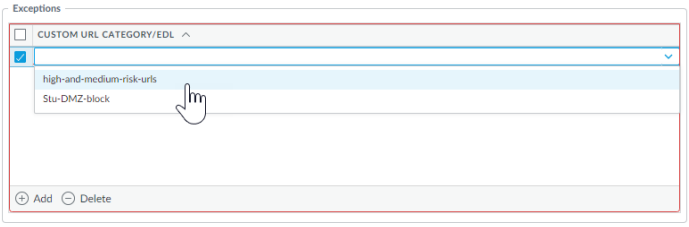
STEP 3 | （可选）如果遇到误报，则添加 URL 异常到您的 URL 过滤安全配置文件。您还可通过从 URL 过滤配置文件指定 EDL，或是从 URL 过滤日志添加网页条目来添加异常。

- 添加 EDL URL 异常列表。
  1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 过滤）。
  2. 选择想要排除特定 URL 的 URL 过滤配置文件，然后选择 **Inline ML**。



© 2019 Palo Alto Networks, Inc.

3. 单击 **Add**（添加）以选择一个预先存在的基于 URL 的外部动态列表。如果没有可用列表，请创建一个新的外部动态列表。




4. 单击 **OK**（确定）以保存 URL 过滤配置文件，并 **Commit**（提交）更改。

- 从 URL 过滤日志条目添加文件异常。

1. 选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 过滤），并使用 Inline ML 判定 **malicious-javascript**（恶意 **javascript**）或 **phishing**（网络钓鱼）筛选日志中的URL 条目。为要创建异常的 URL 选择一个 URL 过滤日志。
2. 前往 **Detailed Log View**（详细日志视图），然后向下滚动至 **Details**（详细信息）窗格，并选择 **Inline ML Verdict**（**Inline ML** 判定）旁边的 **Create Exception**（创建异常）。




3. 选择自定义 URL 异常类别，然后单击 **OK**（确定）。
4. 新的 URL 异常将添加到 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别）下的列表中。

STEP 4 | （可选）检验防火墙与 inline ML 云服务的连接状态。

在防火墙上使用以下 CLI 命令查看连接状态。

```
show mlav cloud-status
```

例如：

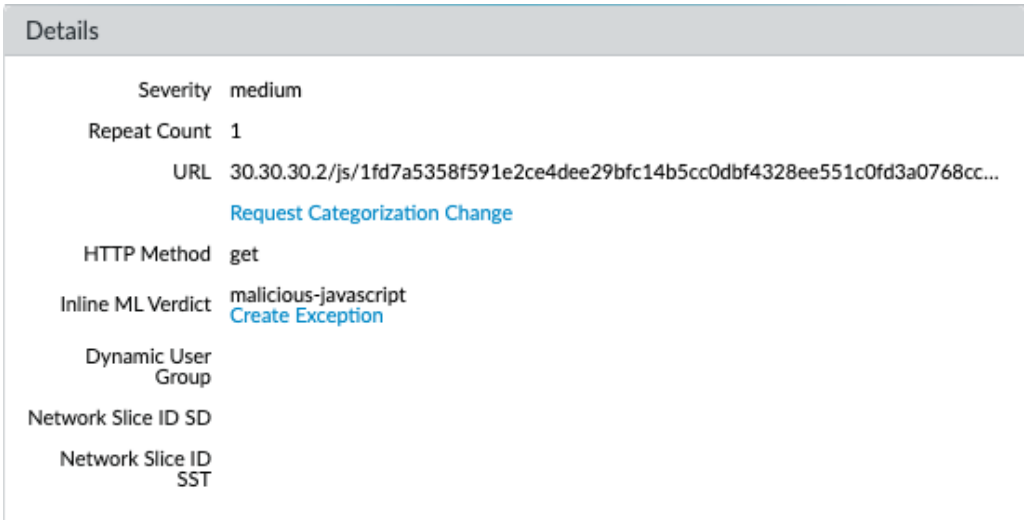
```
show mlav cloud-status

MLAV cloud
Current cloud server:          ml.service.paloaltonetworks.com
Cloud connection:              connected
```

如果无法连接到 inline ML 云服务，请检查以下域是否被阻止：ml.service.paloaltonetworks.com。

若要查看已使用 URL 过滤 inline ML 处理过的网页相关信息，请根据 **Inline ML Verdict**（**Inline ML** 判定）筛选日志（**Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 过滤））。已判定为包含危险的网页将按 **phishing**（网络钓鱼）或 **malicious-javascript**（恶意 **javascript**）判定进行分类。例如：



© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

# 监控 Web 活动

ACC、URL 筛选日志和报告可显示设置为 **alert**（警报）、**block**（阻止）、**continue**（继续）或 **override**（替代）的 URL 类别的所有用户 Web 活动。通过监控日志，可以更好地了解用户群的 Web 活动以确定 Web 访问策略。

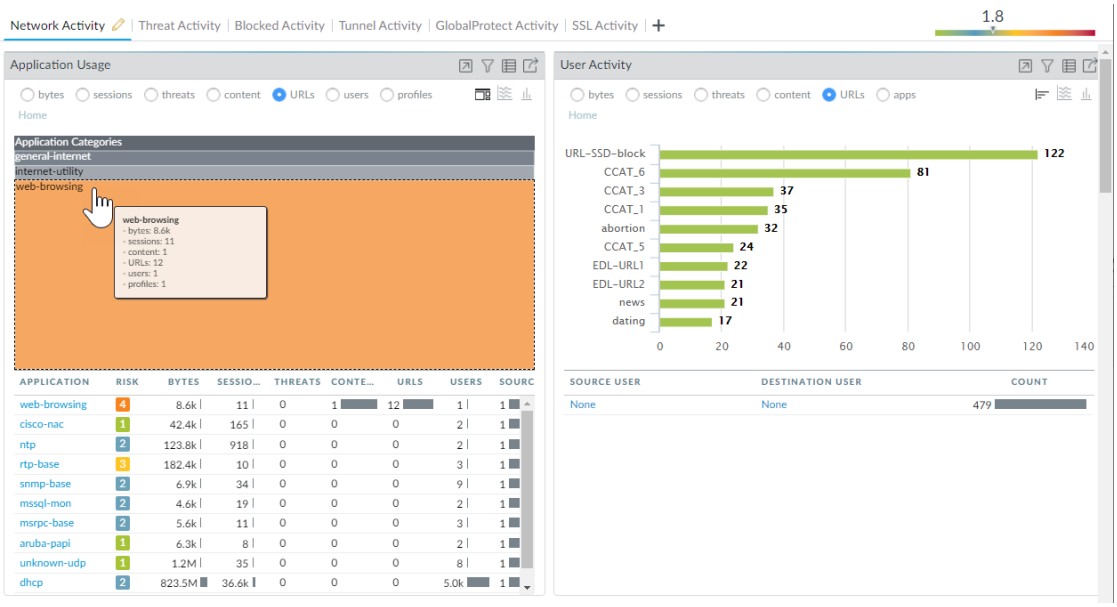
以下主题介绍如何监控 Web 活动：

- 监控网络用户的 Web 活动
- 查看用户活动报告
- 配置自定义 URL 筛选报告

## 监控网络用户的 Web 活动

您可以使用 ACC、URL 筛选报告以及防火墙上生成的日志来追踪用户活动。

- 要快速查看环境中最常见的类别用户访问，请选中 **ACC** 小部件。**Network Activity**（网络活动）选项卡中大部分小部件允许您对 URL 进行排序。例如，在“应用程序使用”小部件中，您可以看到网络类别是最常访问的类别，随后是加密隧道和 SSL。您还可以查看按照 URL 排序的 **Threat Activity**（威胁活动）和 **Blocked Activity**（阻止的活动）列表。




查看日志并配置日志选项：

- 可以从 ACC 直接跳转到日志 (🗒) 或选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 筛选）。

  每个条目的日志操作取决于您为相应类别定义的站点访问设置：

  - **Alert log**（警报日志）— 在此示例中，computer-and-internet-info 类别设置为警报。




  - **Block log**（阻止日志）— 在此示例中，insufficient-content 类别设置为继续。相反，如果该类别被设置为阻止，则日志操作将是 block-url。



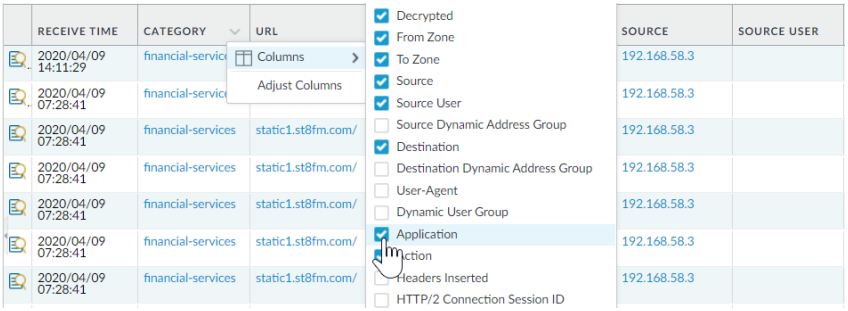
© 2019 Palo Alto Networks, Inc.

| | RECEIVE TIME | CATEGORY | URL | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|
| | 2020/04/08 18:47:49 | insufficient-content | munchkin.mark... | pm wifi | UNTRUST | | | | ssl | block-continue |

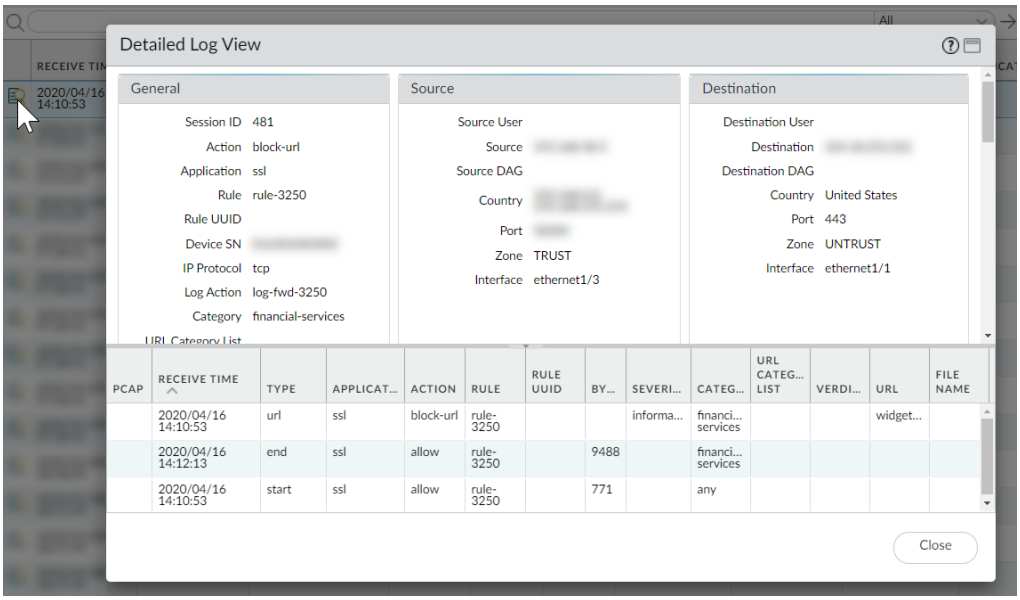
- **Alert log on encrypted website**（加密网站上的警报日志）— 在此示例中，类别是 private-ip-addresses，应用程序是 web-browsing。该日志还显示防火墙已解密此流量。

| | RECEIVE TIME | CATEGORY | URL | DECRYPTED | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2020/04/09 14:11:29 | private-ip-addresses | /Updates/Updat... | yes | TRUST | UNTRUST | 192.168.58.3 | | | web-browsing | alert |

- 也可以将多个其他列添加到 URL 筛选日志视图，如到区域和从区域、内容类型、以及是否执行数据包捕获。要修改显示的列，单击任何一列中的向下箭头，然后选择要显示的属性。



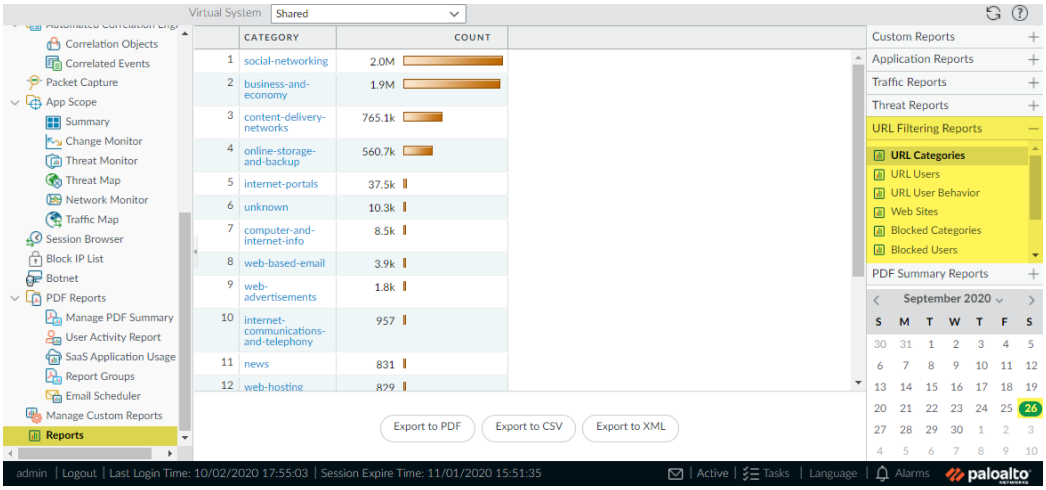

- 要查看完整的日志详细信息和/或请求访问的指定 URL 的类别更改，单击日志的第一列中的日志详细信息图标。




- 生成关于 URL 类别、URL 用户、访问的网站、已阻止类别等的预定义 URL 筛选报告。

  选择 **Monitor**（监控）> **Reports**（报告）并在 **URL Filtering Reports**（**URL** 筛选报告）部分下，选择其中一个报告。报告涵盖您在日历上选择的日期的 24 小时时段。也可以将报告导出为 PDF、CSV 或 XML 格式。


© 2019 Palo Alto Networks, Inc.



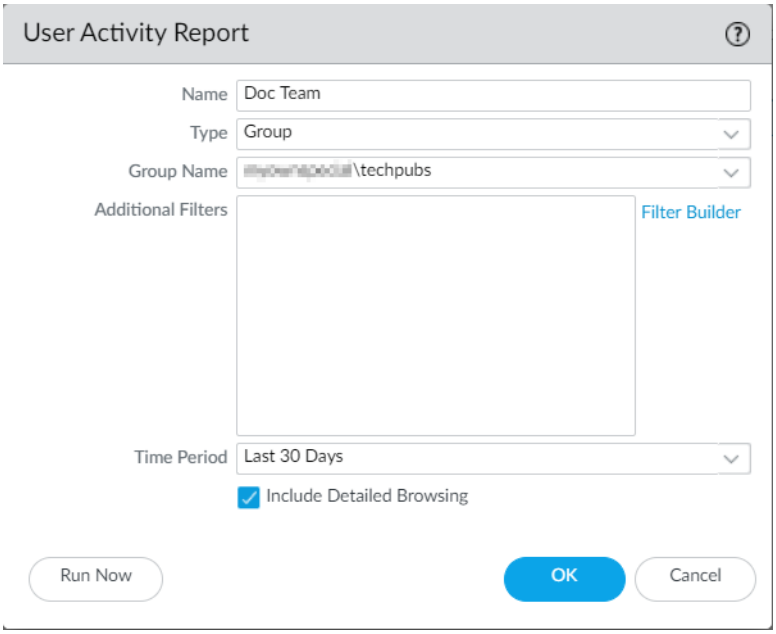

# 查看用户活动报告

此报告提供了查看用户或组活动的快速方法，并且也提供了用于查看浏览时间活动的选项。

STEP 1 | **配置用户活动报告。**

1. 选择 **Monitor**（监控）> **PDF Reports**（**PDF** 报告）> **User Activity Report**（用户活动报告）。
2. **Add**（添加）报告，然后输入报告的 **Name**（名称）。
3. 选择报告 **Type**（类型）：
   - 选择 **User**（用户）为其中一名用户生成报告。
   - 为一组用户选择 **Group**（组）。

   您必须启用 User-ID，才能选择用户名或组名。如果没有配置 *User-ID*，可选择类型 *User*（用户），然后输入用户计算机的 *IP* 地址。
4. 输入用户报告的 **Username/IP Address**（用户名/**IP** 地址），或输入用户组报告的组名。
5. 选择时段。可以选择现有时段，或选择 **Custom**（自定义）。
6. 选中 **Include Detailed Browsing**（包括详细浏览）复选框，这样可在报告中包括浏览信息。

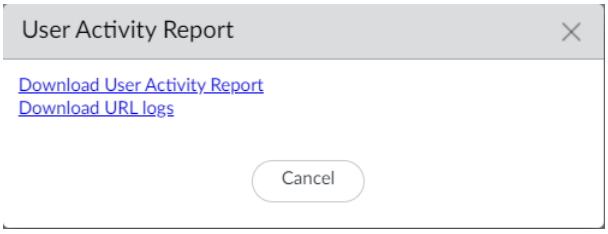





© 2019 Palo Alto Networks, Inc.

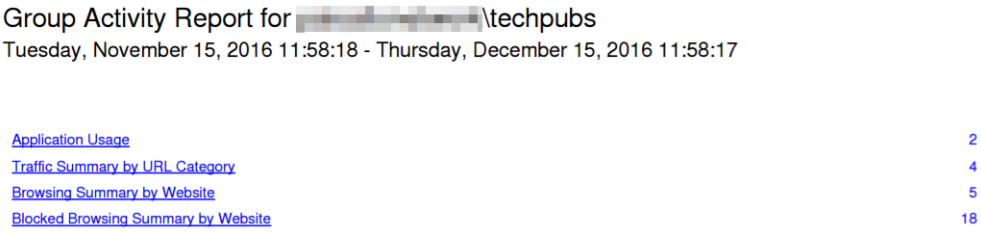
STEP 2 | 运行报告。

1. 单击 **Run Now**（立即运行）。
2. 防火墙完成生成报告时，单击其中一个链接下载报告：
   - 单击 **Download User Activity Report**（下载用户活动报告）可下载 PDF 版本的分析报告。
   - 单击 **Download URL Logs**（下载 **URL** 日志）可下载相应日志条目的 CSV 文件。

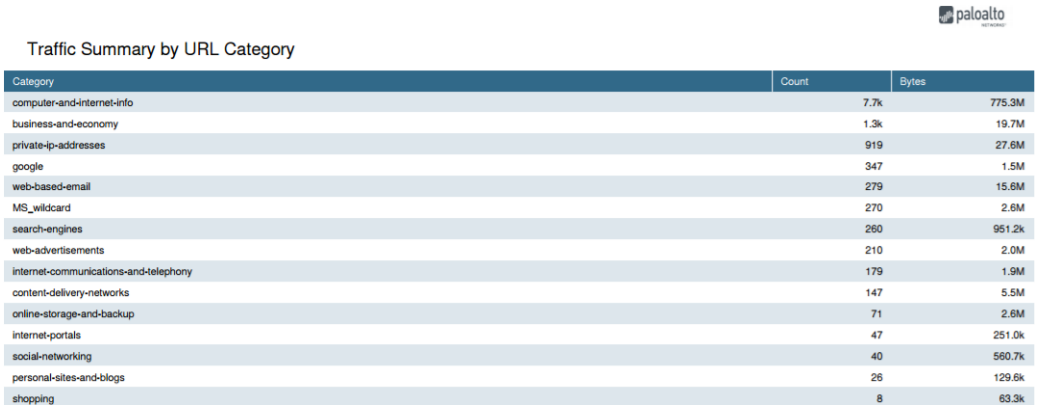



3. 下载报告后，单击 **Cancel**（取消）。
4. 如果要保存用户活动报告设置，以便稍后再次运行相同的报告，请单击 **OK**（确定）；否则请单击 **Cancel**（取消）。

STEP 3 | 通过打开下载的文件查看用户活动报告。PDF 版本的报告显示您基于报告的用户或组、报告时间框架和目录：




STEP 4 | 单击目录中的项目以查看报告详细信息。例如，单击 **Traffic Summary by URL Category**（按 **URL** 类别的流量摘要）可查看选定用户或组的统计信息。




| Category | Count | Bytes |
|---|---|---|
| computer-and-internet-info | 7.7k | 775.3M |
| business-and-economy | 1.3k | 19.7M |
| private-ip-addresses | 919 | 27.6M |
| google | 347 | 1.5M |
| web-based-email | 279 | 15.6M |
| MS_wildcard | 270 | 2.6M |
| search-engines | 260 | 951.2k |
| web-advertisements | 210 | 2.0M |
| internet-communications-and-telephony | 179 | 1.9M |
| content-delivery-networks | 147 | 5.5M |
| online-storage-and-backup | 71 | 2.6M |
| internet-portals | 47 | 251.0k |
| social-networking | 40 | 560.7k |
| personal-sites-and-blogs | 26 | 129.6k |
| shopping | 8 | 63.3k |

# 配置自定义 URL 筛选报告

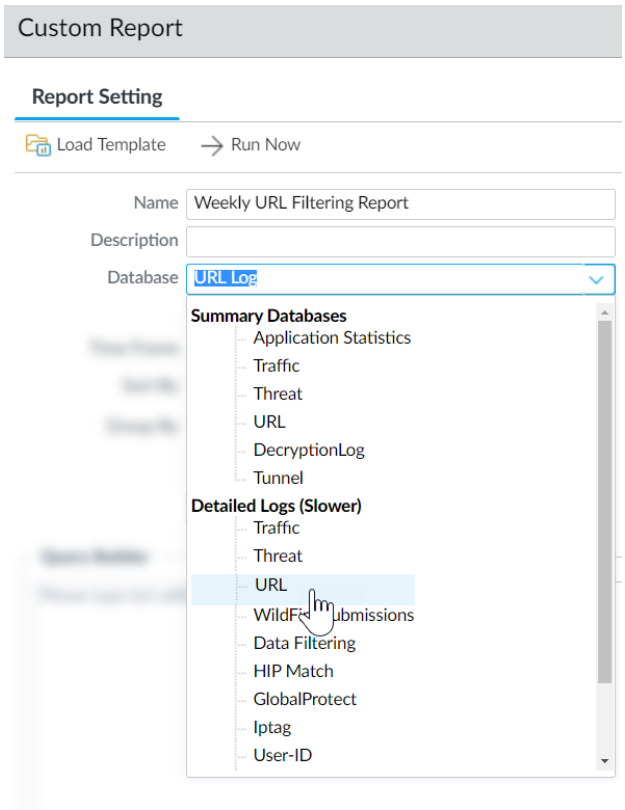
要生成可以定期运行的详细报告，请配置自定义 URL 筛选报告。您可以选择基于报告的 URL 筛选日志字段的任意组合。

STEP 1 | 添加新的自定义报告。

1. 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告），然后 **Add**（添加）报告。
2. 给予报告一个唯一的 **Name**（名称）和 **Description**（说明）（可选）。

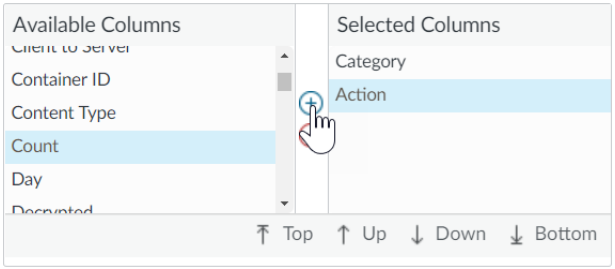

© 2019 Palo Alto Networks, Inc.

3. 选择用于生成报告的 **Database**（数据库）。要生成详细的 URL 筛选报告，请从“详细日志”部分中选择 **URL**：




STEP 2 | 配置报告选项。

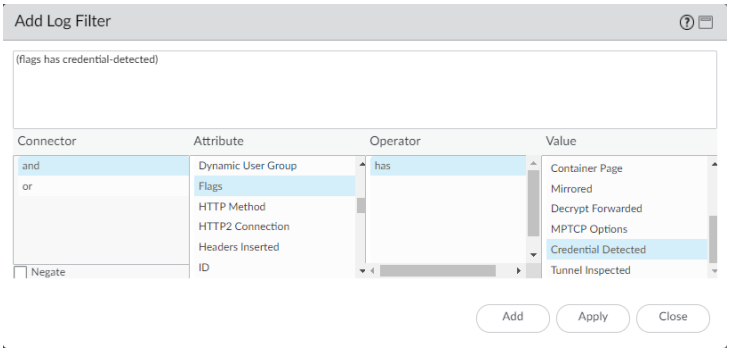
1. 选择预先定义的 **Time Frame**（时间框架）或选择 **Custom**（自定义）。
2. 从“可用列”列表中选择要包含在报告中的日志列，将其 (⊞) 添加到“选定列”中。例如，对于 URL 筛选报告，您可以选择：
   - 操作
   - 应用程序类别
   - 类别
   - 目标国家/地区
   - 源用户
   - 网址



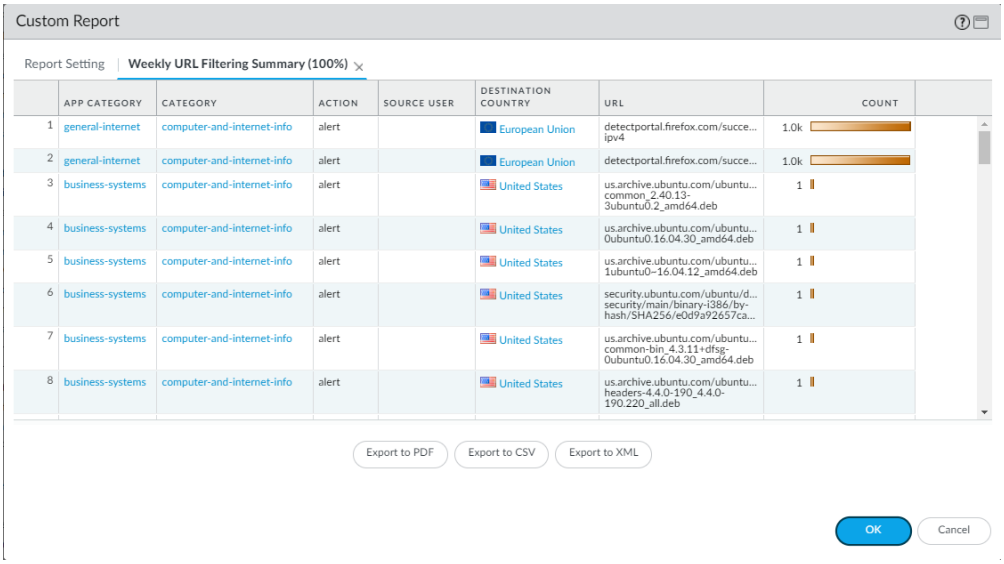

3. 如果防火墙启用阻止凭据网络钓鱼，请选择属性 **Flags**（标志），操作员 **has**（拥有）和值 **Credential Detected**（检测到的凭据），还应包括用户向站点提交有效公司凭据时在报告中记录的事件。



© 2019 Palo Alto Networks, Inc.




4. （可选）选择 **Sort By**（排序方式）选项，以设置用于汇总报告详细信息的属性。如果您未选择排序属性，报告则会返回前面 N 个结果，不进行任何聚合。选择 **Group By**（分组方式）属性，以用作分组数据的锚点。以下示例显示了将 **Group By**（分组方式）设置成 **App Category**（应用程序类别），将 **Sort By**（排序方式）设置成 **Top 5**（前 5 组）**Count**（计数）的一份报告。




STEP 3 | 运行报告。

1. 单击 **Run Now**（立即运行）图标可立即生成报告，该报告将在新选项卡中打开。
2. 完成报告审查后，返回 **Report Setting**（报告设置）选项卡，然后调整设置并再次运行报告，或继续下一步来安排报告。
3. 选择 **Schedule**（时间表）复选框以每天运行一次报告。这将生成每日报告，其中详细记录了过去 24 小时的 Web 活动。

STEP 4 | **Commit**（提交）配置。

STEP 5 | 查看自定义报告。

1. 选择 监视器 > 报告.
2. 展开右列的 **Custom Reports**（自定义报告）窗格，然后选择要查看的报告。最新报告会自动显示。
3. 要查看以前日期的报告，请从日历中选择日期。也可以将报告导出为 PDF、CSV 或 XML 格式。


© 2019 Palo Alto Networks, Inc.

# 仅记录用户访问页面

容器页面是用户在访问网站时访问的主页，但在此主页内可以加载其他页面。如果在 URL 筛选配置文件中启用 **Log Container page only**（仅记录容器页面）（**Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选））选项，则只会记录主容器页面，而非可能已在容器页面内加载的后续页面。因为 URL 筛选可能会生成大量的日志条目，且您可能想要启用此选项，因此日志条目将只包含请求页面文件名与特定 MIME 类型匹配时的 URI。默认设置包括以下 MIME 类型：

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml



如果已启用 *Log container page only*（仅记录容器页面）选项，抗病毒或漏洞防护可能并不能总是检测到威胁的相关 *URL* 日志条目。



© 2019 Palo Alto Networks, Inc.

# 创建自定义 URL 类别

您可以创建自定义 URL 筛选对象，指定 URL 类别实施的例外情况，并基于多个 URL 类别创建自定义 URL 类别：

- 对 **URL** 类别实施定义例外—创建 URL 的自定义列表，以便将其作为安全策略规则内的匹配条件使用。这特别适用于指定 URL 类别例外，让您可以实施特定 URL，而无视这些 URL 所属的 URL 类别。
- 基于多个 **PAN-DB** 类别定义自定义 **URL** 类别 — 让您可以针对符合类别集的网站指定实施。网站或网页必须与所有被定义为自定义类别的类别相符。

按照下列步骤创建自定义 URL 类别，定义您打算如何让防火墙实施自定义 URL 类别：

STEP 1 | 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别）。

STEP 2 | **Add**（添加）或修改自定义 URL 类别，并为类别提供描述性 **Name**（名称）。

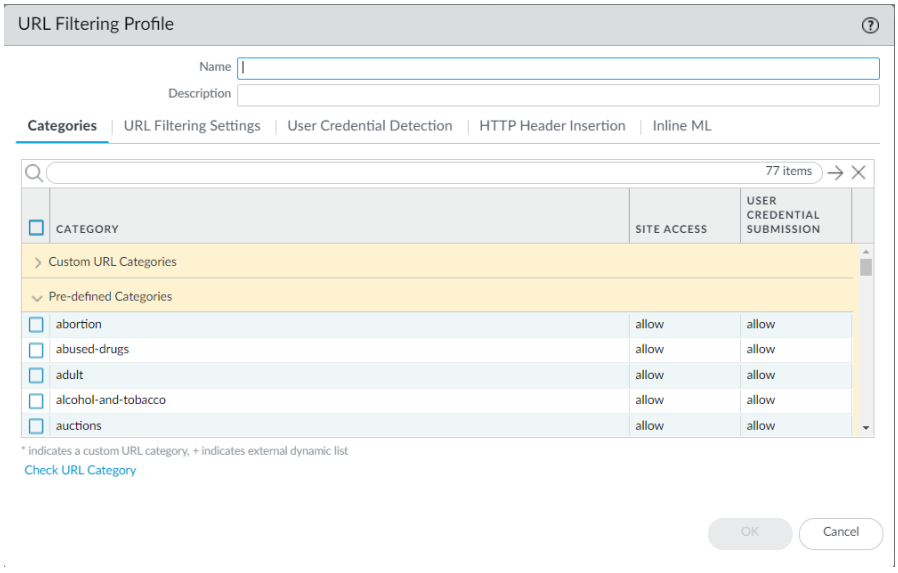
STEP 3 | 将类别 **Type**（类型）设置为 **Category Match**（类别匹配）或 **URL List**（**URL** 列表）：

- **URL List**（**URL** 列表）— 添加您想要实施且与其所属 URL 类别不同的 URL。使用此列表类型以定义 URL 类别实施的例外情况，或定义属于自定义类别的 URL 列表。关于如何填充此列表的详细信息，例如通配符使用指南，请参见 URL 类别异常。
- **Category Match**（类别匹配）— 针对符合类别集的网站实施。网站或网页必须与所有被定义为自定义类别的类别相符。

STEP 4 | 选择 **OK**（确定）以保存自定义 URL 类别对象。

STEP 5 | 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选），并 **Add**（添加）或修改 URL 筛选配置文件。

您的新自定义类别将在 **Custom URL Categories**（自定义 **URL** 类别）下拉列表中列出：




STEP 6 | 决定您如何为自定义 URL 类别实施 **Site Access**（站点访问）和 **User Credential Submissions**（用户凭据提交）。（要控制用户可提交企业凭据的站点，请参见预防凭证网络钓鱼）。

STEP 7 | 将 URL 筛选配置文件附加到安全策略规则，以实施与该规则相符的流量。



© 2019 Palo Alto Networks, Inc.

选择 **Policies**（策略）> **Security**（安全）> **Actions**（操作）并制定安全策略规则，以根据您刚刚更新的 URL 筛选配置文件实施流量。确保 **Commit**（提交）您的更改。



您也可以使用自定义 *URL* 类别作为安全策略匹配条件。这种情况下，您无需定义类别应如何作为 *URL* 筛选配置文件的一部分而被实施。在设置自定义类别后，直接前往您希望添加自定义 *URL* 类别的安全策略规则（*Policies*（策略）> *Security*（安全））。选择 *Service/URL Category*（服务/*URL* 类别）以使用自定义 *URL* 类别作为规则的匹配条件。



© 2019 Palo Alto Networks, Inc.

# URL 类别异常

您可以从 URL 类别实施中排除特定网站，务必阻止或允许这些网站，而不管其相关的 URL 类别。例如，您可以阻止 URL 类别，但选择允许某些已属于该类别的网站。要为 URL 类别实施创建这些类别的例外：

- 通过创建创建自定义 URL 类别列表添加您想要明确阻止或允许的站点 IP 地址或 URL（**Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别））。
- 使用 URL 筛选配置文件中的外部动态列表。使用“外部动态列表”指定您想要从 URL 类别中单独实施站点的好处在于，您可以无需在防火墙上更改配置或提交的前提下更新“外部动态列表”。

以下指南介绍了如何填充 URL 类别阻止和允许列表，或填充您正用作 URL 外部动态列表源的文本文件：

- URL 类别异常列表的基本指南
- URL 类别异常列表的通配符指南
- URL 类别异常列表 — 通配符示例

## URL 类别异常列表的基本指南

- 输入想要从相关 URL 类别单独实施的网站 IP 地址或 URL。
- 列表中的条目必须为完全匹配，并且不区分大小写。
- 输入与想要控制访问的网站（和可能的特定子域）完全匹配的字符串，或是使用通配符允许条目与有多个网站的子域匹配。有关使用通配符的详细信息，请参看 URL 类别异常列表的通配符指南。
- 忽略 URL 条目中的 `http` 和 `https`。
- 每个 URL 条目的最大长度为 255 个字符。

## URL 类别异常列表的通配符指南

您可以使用 URL 类别异常列表中的通配符来轻松配置与多个网站子域和页面匹配的单个条目，无需指定确切的子域和页面。

创建通配符条目时，请遵循这些指南：

- 以下字符将视为令牌分隔符：. / ? & = ; +

  由一个或两个这种字符分隔的每个字符串就是一个令牌。使用通配符作为令牌占位符，表明特定令牌可以包含任何值。
- 您可以使用星号 (*) 或插入符号 (^) 代替令牌，以指示通配符值。
- 通配符必须是令牌中唯一的字符，但是，条目可以包含多个通配符。

如何使用星号 **(*)** 和插入符号 **(^)** 通配符

| | |
|---|---|
| * | 用于指示一个或多个变量子域。如果使用 *，则条目将与 URL 开头或结尾处的所有其他子域匹配。如果您不想与超出该位置的所有其他子域匹配，请在条目结尾处使用正斜杠。<br>例如：<br>• **`*.paloaltonetworks.com`** 与 www.paloaltonetworks.com 和 www.paloaltonetworks.com.uk 匹配。<br>• **`*.paloaltonetworks.com/`** 与 www.paloaltonetworks.com 匹配，但不与 www.paloaltonetworks.com.uk 匹配。 |


© 2019 Palo Alto Networks, Inc.

| | |
|---|---|
| ^ | 用于指示一个变量子域。<br>例如：<br>**mail.^.com** 与 mail.company.com 匹配，但不与 mail.company.sso.com 匹配。 |

不要创建带有连续星号 ***(*)*** 通配符或九个以上连续插入符号 ***(^)*** 通配符的条目，因为这些条目可能会对防火墙性能产生影响。

例如，请勿添加诸如 ***mail.*.*.com***之类的条目，而应该根据想要控制其访问的网站范围，输入***mail.*.com*** 或 ***mail.^.^.com***。与 ***mail.*.com*** 等条目匹配的站点数显著多于与 ***mail.^.^.com*** 匹配的站点数；与 ***mail.*.com*** 匹配的站点包含任意数量的子域，而与 ***mail.^.^.com*** 匹配的站点仅包含两个子域。

## URL 类别异常列表 — 通配符示例

下表列出了使用通配符的 URL 异常列表中条目示例，以及与这些条目相匹配的站点示例。

| URL 异常列表条目 | 匹配网站 |
|---|---|
| **示例集 1** | |
| *.company.com | eng.tools.company.com<br>support.tools.company.com<br>tools.company.com<br>docs.company.com |
| ^.company.com | tools.company.com<br>docs.company.com |
| ^.^.company.com | eng.tools.company.com<br>support.tools.company.com |
| **示例集 2** | |
| mail.google.* | mail.google.com<br>mail.google.co.uk |
| mail.google.^ | mail.google.com |
| mail.google.^.^ | mail.google.co.uk |



© 2019 Palo Alto Networks, Inc.

# 使用 URL 筛选配置文件中的外部动态列表

为保护您的网络免遭新发现的威胁和恶意软件的威胁，您可以使用 URL 筛选配置文件中的 External Dynamic Lists（外部动态列表）。通过外部动态列表，您可以在不更改配置或不在防火墙上提交的情况下更新列表。外部动态列表是一个托管在外部 Web 服务器上的文本文件。您可使用此列表导入 URL 并对这些 URL 实施策略。更新 web 服务器上的列表时，防火墙检索更改，并对修改过的列表实施策略，而无需在防火墙上进行提交。

防火墙会以配置的间隔动态导入列表，并为列表中的 URL（IP 地址或域将被忽略）实施策略。有关 URL 格式化指南，请参见URL 类别异常。

相关详细信息，请参阅外部动态列表。

STEP 1 | 将防火墙配置为访问外部动态列表。

- 确保此列表不包括 IP 地址或域名；防火墙跳过非 URL 条目。
- 验证列表格式（请参阅）。
- 从类型下拉列表中选择 **URL List**（**URL** 列表）。

STEP 2 | 使用 URL Filtering（URL 筛选）配置文件中的外部动态列表。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）。
2. **Add**（添加）或修改现有的 URL Filtering（URL 筛选）配置文件。
3. **Name**（命名）配置文件，并在 **Categories**（类别）选项卡中从“Category（类别）”列表中选择外部动态列表。
4. 单击“Action（操作）”，为外部动态列表中的 URL 选择更精细的操作。

   如果包括在外部动态列表中的某个 *URL* 还包括在自定义 *URL* 类别或阻止和允许列表中，则此自定义类别中指定的操作或阻止和允许列表将优先于外部动态列表。
5. 单击 **OK**（确定）。
6. 将 URL 筛选配置文件附加至安全策略规则。
   1. 选择 **Policies**（策略）> **Security**（安全）。
   2. 选择 **Actions**（操作）选项卡，并在“Profile Setting（配置文件设置）”部分中，从 **URL Filtering**（**URL** 筛选）下拉列表中选择新的配置文件。
   3. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 3 | 测试是否实施了策略操作。

1. 查看外部动态列表条目以获取 URL 列表，并尝试从列表中访问 URL。
2. 验证您定义的操作在浏览器中实施。
3. 监控防火墙上的活动：
   1. 选择 **ACC** 并添加 URL 域作为查看访问 URL 的 Network Activity（网络活动）和 Blocked Activity（阻止的活动）的全局筛选器。
   2. 选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 筛选）访问详细的日志视图。

STEP 4 | 验证外部动态列表中的条目已忽略或跳过。

在 URL 类型的列表中，防火墙跳过非 URL 的无效条目，并忽视超过防火墙型号最大限制的条目。

要检查是否已达到外部动态列表类型的限制，请选择 *Objects*（对象）> *External Dynamic Lists*（外部动态列表），然后单击 *List Capacities*（列表容量）。

在防火墙上使用以下 CLI 命令查看列表的详细信息。



© 2019 Palo Alto Networks, Inc.

```
request system external-list show type url name <list_name>
```

例如：

```
request system external-list show type url name My_URL_List
vsys5/My_URL_List:
Next update at: Tue Jan 3 14:00:00 2017
Source: http://example.com/My_URL_List.txt
Referenced: Yes
Valid: Yes
Auth-Valid: Yes

Total valid entries: 3
Total invalid entries: 0
Valid urls:
www.URL1.com
www.URL2.com
www.URL3.com
```



© 2019 Palo Alto Networks, Inc.

# 允许密码访问某些站点

在某些情况下，可能存在想要阻止但又允许某些个人偶尔浏览的 URL 类别。在这种情况下，您应将类别操作设置为 **override**（替代），并在防火墙 Content-ID 配置中定义 URL 管理替代密码。当用户尝试浏览该类别时，他们需要先提供替代密码，然后才能访问站点。请按照以下过程配置 URL 管理替代：

STEP 1 | 设置 URL 管理替代密码。

1. 选择 **Device**（设备）> **Setup**（设置）> **Content - ID**（内容 **ID**）。
2. 在 **URL Admin Override**（**URL** 管理替代）部分中，单击 **Add**（添加）。
3. 在 **Location**（位置）字段中，选择要应用该密码的虚拟系统。
4. 输入 **Password**（密码）和 **Confirm Password**（确认密码）。
5. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。如果替代站点为 HTTPS 站点，配置文件会指定防火墙要向用户展示的证书。有关详细信息，请参阅配置 SSL/TLS 服务配置文件。
6. 选择用户密码提示 **Mode**（模式）：
   - **Transparent**（透明）— 防火墙会拦截发往设置为替代的 URL 类别内站点的浏览器流量并模仿原始目标 URL，以便发出 HTTP 302 提示输入适用于每个 vsys 级别的密码。

     如果客户端浏览器不信任证书，将会显示证书错误。
   - **Redirect**（重定向）— 防火墙会拦截指向设置为替代的 URL 类别的 HTTP 或 HTTPS 流量，并使用 HTTP 302 重定向将请求重定向到防火墙上的第 3 层接口，以便提示输入替代密码。如果选择该选项，那么您必须提供要将流量重定向至的 **Address**（地址）（IP 地址或 DNS 主机名）。
7. 单击 **OK**（确定）。

STEP 2 | （可选）设置自定义替代期。

1. 编辑 URL 筛选部分。
2. 对于已为其成功输入替代密码的类别中的站点，若要更改用户可以浏览该站点的时间量，请在 **URL Admin Override Timeout**（**URL** 管理替代超时）字段中输入新的值。默认情况下，如果不重新输入密码，那么用户可以访问该类别中的站点 15 分钟。
3. 对于在三次尝试输入替代密码失败后将设置为替代的站点，若要更改阻止用户访问该站点的时间量，请在 **URL Admin Lockout Timeout**（**URL** 管理锁定超时）字段中输入新值。默认情况下，将阻止用户 30 分钟。
4. 单击 **OK**（确定）。

STEP 3 | （仅重定向模式）创建要将针对替代配置类别中站点的 Web 请求重定向至的第 3 层接口。

1. 创建管理配置文件，以启用接口显示“URL 筛选继续和替代页面”响应页面：
   1. 选择 **Network**（网络）> **Interface Mgmt**（接口管理），然后单击 **Add**（添加）。
   2. 输入配置文件的 **Name**（名称），选择 **Response Pages**（响应页），然后单击 **OK**（确定）。
2. 创建第 3 层接口。确保附加您刚创建的管理配置文件（在“Ethernet 接口”对话框的 **Advanced**（高级）> **Other Info**（其他信息）选项卡上）。

STEP 4 | （仅重定向模式）若要透明地重定向用户而不显示证书错误，请安装与您要将针对替代配置 URL 类别中站点的 Web 请求重定向至的接口的 IP 地址匹配的证书。您可以生成自签名证书，也可以导入外部 CA 签名的证书。

若要使用自签名证书，必须先创建一个根 CA 证书，然后使用该 CA 签名您将用于 URL 管理替代的证书，步骤如下：

1. 若要创建根 CA 证书，请选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。输入



© 2019 Palo Alto Networks, Inc.

**Certificate Name**（证书名称），例如 RootCA。不要选择 **Signed By**（签名者）字段中的值（此值表示自签名）。请确保选中 **Certificate Authority**（证书授权机构）复选框，然后单击 **Generate**（生成）证书。

2. 若要创建用于 URL 管理替代的证书，请单击 **Generate**（生成）。输入 **Certificate Name**（证书名称），并输入接口的 DNS 名称或 IP 地址作为 **Common Name**（通用名）。在 **Signed By**（签名者）字段中，选择您在上一步中创建的 CA。添加 IP 地址属性，并指定您要将针对拥有替代操作的 URL 类别的 Web 请求重定向至的第 3 层接口的 IP 地址。
3. **Generate**（生成）证书。
4. 要配置客户端信任该证书，请在 **Device Certificates**（设备证书）选项卡上选择 CA 证书，然后单击 **Export**（导出）。然后，必须通过手动配置浏览器，或者通过将证书添加到 Active Directory 组策略对象 (GPO) 的可信根中，将该证书作为可信的根 CA 导入到所有客户端浏览器。

STEP 5 | 指定需要替代密码才能启用访问权限的 URL 类别。

1. 选择 **Objects**（对象）> **URL Filtering**（**URL** 筛选），然后选择现有 URL 筛选配置文件或 **Add**（添加）新配置文件。
2. 在 **Categories**（类别）选项卡上，针对需要密码的各个类别将“操作”设置为 **override**（替代）。
3. 完成 URL 筛选配置文件中的所有剩余部分，然后单击 **OK**（确定）保存该配置文件。

STEP 6 | 将 URL 筛选配置文件应用到安全策略规则，以允许访问需要进行密码替代才能访问的站点。

1. 选择 **Policies**（策略）> **Security**（安全），然后选择相应的安全策略以进行修改。
2. 选择 **Actions**（操作）选择卡，然后在 **Profile Setting**（配置文件设置）部分中，单击 **URL Filtering**（**URL** 筛选）下拉列表，并选择该配置文件。
3. 单击 **OK**（确定）以保存。

STEP 7 | 保存配置。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 预防凭证网络钓鱼

网络钓鱼站点是攻击者伪装成合法网站的站点，目的是窃取用户信息，尤其是可访问您网络的凭据。当网络钓鱼电子邮件进入网络时，只需单个用户单击链接并输入凭据来设置违规行为。您可以通过控制用户根据站点的 URL 类别提交公司凭据的站点，来检测和阻止进行中的网络钓鱼攻击，从而放置凭据被盗。此操作可让您阻止用户将凭据提交给不可信站点，同时允许用户继续向公司和受约束站点提交凭据。

通过扫描提交给网站的用户名和密码，并将这些提交内容与有效的公司凭据进行比较，以阻止凭据网络钓鱼。可以根据网站的 URL 类别选择要允许或阻止公司凭据提交的网站。当防火墙检测到用户尝试向已受限制的类别中的站点提交凭据时，会显示一个阻止用户提交凭据的阻止响应页面，或者显示一个继续页面，警告用户不要将凭据提交给某些 URL 类别中已分类的站点，但仍允许继续提交凭据。您可以自定义这些阻止页面，以教育用户反复使用公司凭据，即使在合法的非网络钓鱼站点上也是如此。

要启用凭据网络钓鱼阻止功能，您必须同时配置 User-ID 和 URL 筛选。前者用于监测用户将有效公司凭据（不是私人凭据）提交给站点的时间，后者用于指定要阻止用户输入其公司凭据的 URL 类别。以下主题描述可用于检测凭据提交的不同方法，并提供配置凭据网络钓鱼保护的说明。

- 检查公司凭据提交的方法
- 使用基于 Windows 的 User-ID 代理配置凭据检测
- 设置凭据网络钓鱼防护

## 检查公司凭据提交的方法

在您设置凭据网络钓鱼防护之前，请确定防火墙使用哪种方法来检查提交给网页的公司凭据是否有效。

| 检查已提交凭据的方法 | User-ID 配置要求 | 该方法将如何检测用户提交给网站的公司用户名和/或密码？ |
|---|---|---|
| 组映射 | 防火墙上的组映射 | 防火墙通过检查确定用户提交至受限站点的用户名是否匹配任何有效的公司用户名。<br>为此，防火墙将提交的用户名与其用户到组映射表中的用户名列表相匹配，以在用户向受限类别中的站点提交公司用户名时进行检测。<br>该方法仅根据 LDAP 组成员身份检查公司用户名提交，让配置更简单，但是更容易发生误报。 |
| IP 用户映射 | 通过用户映射、GlobalProtect 或身份验证策略和身份验证门户识别的 IP 地址到用户名映射。 | 防火墙通过检查确定用户提交至受限站点的用户名是否映射到登录用户名的 IP 地址。<br>为此，防火墙将登录用户名的 IP 地址和提交给网站的用户名与其 IP 地址到用户映射表相匹配，以在用户将公司用户名提交给受限类别中的站点时进行检测。<br>因为这种方法将与会话相关联的登录用户名的 IP 地址与 IP 地址到用户名映射表相匹配，因此它是检测公司用户名提交的有效方法，但不会检测公司密码提交。如果要检测公司用户名和密码提交，则必须使用域凭据筛选器方法。 |
| 域凭据筛选器 | 已配置 User-ID 凭据服务插件的 Windows User-ID 代理 | 防火墙通过检查确定用户提交的用户名和密码是否与同一用户的公司用户名和密码相匹配。 |


© 2019 Palo Alto Networks, Inc.

| 检查已提交凭据的方法 | User-ID 配置要求 | 该方法将如何检测用户提交给网站的公司用户名和/或密码？ |
| --- | --- | --- |
| | - 和 -<br>通过用户映射、GlobalProtect 或身份验证策略和身份验证门户识别的 IP 地址到用户名映射。 | 为此，防火墙必须能够将凭据提交与有效的公司用户名和密码相匹配，并验证提交的用户名是否映射至登录用户名的 IP 地址，如下所示：<br>• 要检测公司用户名和密码 — 防火墙从配备有 User-ID 凭据服务插件的 Windows User-ID 代理中检索一个名为 *bloom* 筛选器的安全位掩码。该插件服务扫描您的目录以获取用户名和密码哈希，将其解构为安全位掩码（即 bloom 筛选器），并将其传递到 Windows User-ID 代理。防火墙定期从 Windows User-ID 代理中检索bloom 筛选器。只要检测到用户将凭据提交到受限类别，就会重建 bloom 筛选器并查找匹配的用户名和密码哈希。防火墙只能连接一个正在运行 User-ID 凭据服务插件的 Windows User-ID 代理。<br>• 要验证凭据是否属于登录用户名 — 防火墙在其 IP 地址到用户名映射表中查找登录用户名的 IP 地址与检测到的用户名之间的映射关系。<br>要了解更多关于域凭据方法的工作原理以及启用此类检测的要求，请参阅使用基于 Windows 的 User-ID 代理配置凭据检测。 |

# 使用 Windows User-ID 代理配置凭据检测

域凭据筛选器检测使防火墙能够检测提交至 Web 页面的密码。该凭据检测方法需要 Windows User-ID 代理和 User-ID 凭据服务（User-ID 代理的一种插件，安装在只读域控制器 *(RODC)* 上）。

*Windows User-ID* 代理仅支持域凭据筛选检测方法。您不能使用 集成有 *PAN-OS* 的 *User-ID* 代理来配置此凭据检测方法。

RODC 是一个 Microsoft Windows 服务器，用于维护域控制器托管的 Active Directory 数据库的只读副本。例如，当域控制器位于公司总部时，RODC 可以部署在远程网络位置，以提供本地身份验证服务。在 RODC 上安装 User-ID 代理可能有用，原因如下：不需要访问域控制器目录来启用凭据检测，并且可支持有限的或有针对性的一组用户的凭据检测。因为 RODC 托管的目录为只读，因此，目录内容的安全性在域控制器上可得到保证。

因为您必须在 *RODC* 上安装 *Windows User-ID* 代理以进行凭据检测，因此最佳做法是为此目的部署单独的代理。请勿使用 *RODC* 上安装的 *User-ID* 代理将 *IP* 地址映射到用户。

在 RODC 上安装 User-ID 代理后，User-ID 凭据服务将在后台运行并扫描目录，找出 RODC 密码复制策略 (PRP) 中列出的组成员的用户名和密码哈希。您可以定义您在该列表中的角色。然后，User-ID 凭据服务将获取收集到的用户名和密码哈希，并将数据解构为一种名为 *bloom* 筛选器的位掩码。Bloom 筛选器的数据结构紧凑，提供一种检查元素（用户名或密码哈希）是否是元素集（您已批准用于复制到 RODC 的凭据集）成员的安全方法。User-ID 凭据服务将 bloom 筛选器转发给 Windows User-ID 代理；防火墙定期从 User-ID 代理中检索最新的 bloom 筛选器，并用其来检测用户名和密码哈希提交。然后，防火墙根据您的设置阻止、提醒或允许向 Web 页面提交有效的密码，或向用户显示响应页面，警告他们网络钓鱼的危险，但允许其继续提交。

在此过程中，User-ID 代理不会存储或公开任何密码哈希，也不会将密码哈希转发给防火墙。一旦密码哈希被解构成一个 bloom 筛选器，就无法再次恢复。

STEP 1 | 使用 Windows User-ID 代理配置用户映射。



© 2019 Palo Alto Networks, Inc.

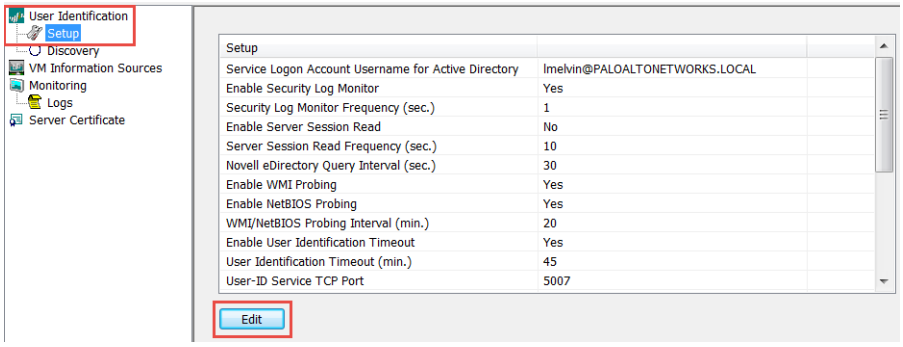
要启用凭据检测，必须在 *RODC* 上安装 *Windows User-ID* 代理。有关受支持的服务器列表，请参阅兼容性矩阵。为此，请安装单独的 *User-ID* 代理。

设置 User-ID 以启用域凭据筛选器检测时要记住的重要事项：

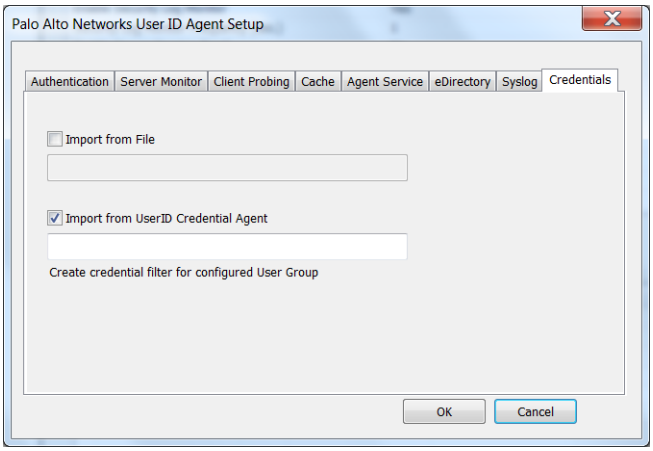
- 因为凭据网络钓鱼检测的有效性取决于您的 RODC 设置，请确保您还查看了RODC 管理的最佳实践和建议。
- 下载 User-ID 软件更新 ：
  - User-ID 代理 Windows 安装程序 — UaInstall-x.x.x-x.msi。
  - User-ID 代理凭据服务 Windows 安装程序 — UaCredInstall64-x.x.x-x.msi。
- 使用具有通过 LDAP 读取 Active Directory 之权限的帐户（User-ID 代理也需要此权限），在 RODC 上安装 User-ID 代理和用户代理凭据服务。
  - User-ID 代理凭据服务需要使用本地系统帐户进行登录的权限。有关详细信息，请参阅为 User-ID 代理创建专用服务帐户。
  - 服务帐户必须是 RODC 上本地管理员组成员。有关详细信息，请参阅以下链接。

STEP 2 | 启用 User-ID 代理和用户代理凭据服务（在后台运行以扫描允许使用的凭据）以共享信息。

1. 在 RODC 服务器上，启动 User-ID 代理。
2. 选择 **Setup**（设置），然后编辑设置部分。




3. 选择 **Credentials**（凭据）选项卡。仅在您已经安装 User-ID 代理凭据服务时，才会显示此选项卡。




4. 选择 **Import from User-ID Credential Agent**（从 **User-ID** 凭据代理导入）。这使得 User-ID 代理可以导入 User-ID 凭据代理创建的 bloom 筛选器来呈现用户和相应的密码哈希。
5. 单击 **OK**（确定），**Save**（保存）您的设置，并 **Commit**（提交）。

STEP 3 | 在 RODC 目录中，定义要为其支持凭据提交检测的用户组。

- 确认将应接收凭据提交执行的组添加到“允许的 RODC 密码复制组”。


© 2019 Palo Alto Networks, Inc.

- 检查在默认情况下，“允许的 RODC 密码复制组”中的任何组都不在“拒绝的 RODC 密码复制组”中。两者中列出的组均不会受到凭据网络钓鱼执行的影响。

STEP 4 | 继续下一个任务。

在防火墙上设置凭据网络钓鱼防护。

# 设置凭据网络钓鱼防护

在决定使用检查公司凭据提交的方法后，请执行以下步骤以使防火墙能够检测用户向 Web 页面提交公司凭据并在此操作上发出警报、阻止凭证提交，或要求用户在继续提交凭据之前确认网络钓鱼危险的时间。

STEP 1 | 如果尚未这样操作，请启用 User-ID。

任何一种检查公司凭据提交的方法均需要使用不同的 User-ID 配置来检查公司凭据提交：

- 如果您计划使用组映射方法，该方法是检测用户是否提交有效的公司用户名的方法，请将用户映射到组。
- IP 用户映射方法检测用户是否正提交有效的公司用户名，以及该用户名是否与登录用户名一致，如果您计划使用此方法，请将 IP 地址映射到用户。
- 域凭据筛选器方法检测用户是否正提交有效的用户名和密码，以及这些凭据是否属于登录用户，如果您计划使用此方法，请使用基于 Windows 的 User-ID 代理配置凭据检测并将 IP 地址映射到用户。

STEP 2 | 如果尚未执行该操作，请配置最佳实践 URL 筛选配置文件，以确保 URL 不受出现的托管恶意软件或破坏性内容的攻击。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选），并 **Add**（添加）或修改 URL 筛选配置文件。
2. 阻止访问所有已知的危险 URL 类别：恶意软件、网络钓鱼、动态 DNS、未知、命令和控制、极端主义、版权侵犯、回避代理和匿名者、新注册域、灰色软件以及寄放。

STEP 3 | Add（添加）解密策略规则，以解密您想要用于监控用户凭据提交的流量。

STEP 4 | 配置 URL 筛选配置文件以检测提供给允许的 URL 类别的网站的公司凭据。



防火墙不会检查可信站点的凭据提交，即使是您为了获得最佳性能启用对这些站点的 *URL* 类别检查。可信站点是指 *Palo Alto Networks* 尚未观察到任何恶意攻击或网络钓鱼攻击的站点。此可信站点列表的更新通过应用程序和威胁内容更新提供。有关免受凭据检测的 *App-ID* 列表，请参阅 live.paloaltonetworks.com 上的跳过凭据提交检测的可信 App-ID。

1. 选择 **User Credential Detection**（用户凭据检测）。
2. 从 **User Credential Detection**（用户凭据检测）下拉列表的网页中选择其中一个检查公司凭据提交方法：



确定主用户名的格式与 *User-ID* 源提供的用户名格式一致。

- **Use IP User Mapping**（使用 **IP** 用户映射）— 检查有效的公司用户名提交，并验证用户名是否已映射到会话的源 IP 地址。为此，防火墙根据其 IP 地址到用户名的映射表匹配提交的用户名和会话的源 IP 地址。要使用该方法，您可使用将 IP 地址映射到用户中描述的任何用户映射方法。
- **Use Domain Credential Filter**（使用域凭据筛选器）— 检查有效的公司用户名和密码提交，并验证用户名是否映射到用户登录的 IP 地址。有关如何设置 User-ID 以启用此方法的说明，请参阅使用基于 Windows 的 User-ID 代理配置凭据检测。
- **Use Group Mapping**（使用组映射）— 当防火墙配置为将用户映射到组时，根据用户到组映射表检查有效的用户名提交。



© 2019 Palo Alto Networks, Inc.

使用组映射，您可以将凭据检测应用于目录的任何部分，或可以访问最敏感应用程序的特定组，例如 IT 组。



该方法在没有唯一结构化用户名的环境中容易出现误报。因此，您只能使用此方法来保护您的高价值用户帐户。

3. 设置防火墙用于记录公司凭据提交检测的 **Valid Username Detected Log Severity**（有效用户名检测到的日志严重性）。默认情况下，防火墙将这些事件记录为中等严重性。

STEP 5 | 阻止（或警报）允许站点的凭据提交。

1. 选择 **Categories**（类别）。
2. 对于允许 **Site Access**（站点访问）的每个类别，选择要处理 **User Credential Submissions**（用户凭据提交）的方式方法：
   - **alert**（警报）— 允许用户向网站提交凭据，但是每次用户在该 URL 类别中向站点提交凭据时生成 URL 筛选日志。
   - **allow**（允许）—（默认）允许用户向网站提交凭据。
   - **block**（阻止）— 阻止用户向网站提交凭证。当用户尝试提交凭据时，防火墙会显示防钓鱼阻止页面，从而阻止凭据提交。
   - **continue**（继续）— 当用户尝试提交凭据时显示的防钓鱼继续页面响应页面。用户必须在响应页面上选择“继续”以继续提交。
3. 选择 **OK**（确定）以保存 URL 筛选配置文件。

STEP 6 | 将设置有凭据检测功能的 URL 筛选配置文件应用于您的安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全），并 **Add**（添加）或修改安全策略规则。
2. 在 **Actions**（操作）选项卡中，将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）。
3. 选择新的或已更新的 **URL Filtering**（**URL** 筛选）配置文件，将其附加到安全策略规则。
4. 选择 **OK**（确定）以保存安全策略规则。

STEP 7 | **Commit**（提交）配置。

STEP 8 | 监控防火墙检测到的凭据提交。



选择 *ACC* > *Hosts Visiting Malicious URLs*（访问恶意 *URL* 的主机）可查看访问过恶意软件和网络钓鱼站点的用户数。

选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 筛选）。

新的 **Credential Detected**（检测到的凭据）列显示防火墙检测到包含有效凭据的 HTTP 发布请求的事件：

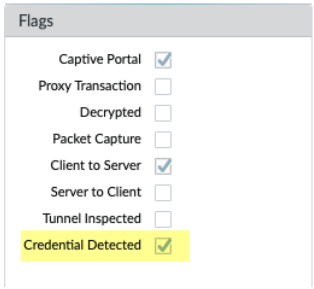
| | CATEGORY | APPLICATION | ACTION | CREDENTIAL DETECTED |
|---|---|---|---|---|
| | streaming-media | | block-url | yes |
| | streaming-media | | block-url | yes |
| | streaming-media | | block-url | yes |
| | streaming-media | | block-url | yes |
| | streaming-media | | block-url | yes |

要显示此列，将鼠标悬停在任何列标题上，然后单击箭头以选择要显示的列。

日志条目详细信息还显示凭据提交：



© 2019 Palo Alto Networks, Inc.




STEP 9 | 验证和解决凭据提交检测问题。

- 使用以下 CLI 命令查看凭据检测统计信息：

```
> show user credential-filter statistics
```

该命令的输出可能会有所不同，取决于为防火墙配置的用于检测凭据提交的方法。例如，如果在任何 URL 筛选配置文件中配置域凭据筛选器，则会显示将 bloom 筛选器转发到防火墙的 User-ID 代理列表，以及包含在 bloom 筛选器的凭据数。

- （仅限组映射法）使用以下 CLI 命令查看组映射信息，包括启用组映射凭据检测的 URL 筛选配置文件数，以及已尝试将凭据提交到受限站点的组成员的用户名。

```
> show user group-mapping statistics
```

- （仅限域凭据筛选器法）使用以下 CLI 命令查看正在向防火墙发送映射信息的所有基于 Windows 的 User-ID 代理：

```
> show user user-id-agent state all
```

命令输出现在显示 bloom 筛选器计数情况，包括防火墙从每个代理接收到的 bloom 筛选器更新次数，以及自上次 bloom 筛选器更新以来过去的时间长度（以秒计算）（前提是任何 bloom 筛选器更新失败）。

- （仅限域凭据筛选器法）基于 Windows 的 User-ID 代理显示引用 BF（bloom 筛选器）推送到防火墙的日志消息。在 User-ID 代理接口中，选择 **Monitoring**（监控）> **Logs**（日志）。



© 2019 Palo Alto Networks, Inc.

# 安全搜索执行

很多搜索引擎都有安全搜索设置，用以筛选搜索查询返回流量中的成人图像和视频。如果最终用户未使用最严格的安全搜索设置，您可以启用防火墙来阻止搜索结果，还可以透明地启用用户安全搜索。防火墙可以针对以下搜索提供商执行安全搜索：Google、Yahoo、Bing、Yandex 和 YouTube。考虑到安全搜索是一项尽力而为的设置，服务提供商并不保证它适用于每个网站，搜索提供商将网站分类为安全或不安全（不是 Palo Alto Networks）。

要使用此功能，您必须在 URL 筛选配置文件中启用 **Safe Search Enforcement**（安全搜索执行）选项并将其附加到安全策略规则。然后，防火墙将阻止任何没有使用最严格安全搜索设置的匹配搜索查询返回流量。执行安全搜索的方法有两种：

- 阻止未启用严格安全搜索时的搜索结果 — 如果最终用户在未先启用最严格安全搜索设置的情况下尝试执行搜索，那么防火墙会阻止搜索查询结果并显示 URL 筛选安全搜索阻止页面。默认情况下，该页面将提供一个用于配置安全搜索的搜索提供商设置的 URL。
- 透明启用用户安全搜索 — 如果最终用户在未先启用严格安全搜索设置的情况下尝试执行搜索，那么防火墙会阻止状态代码为 HTTP 503 的搜索结果，并将搜索查询重定向至包含安全搜索参数的 URL。您可以通过以下方式启用该功能：导入包含用于重写搜索 URL 的 Javascript 的新 URL 过滤安全搜索阻止页面，以将严格安全搜索参数包含在内。在该配置中，用户不会使用阻止页面，但会自动重定向至执行最严格安全搜索选项的搜索查询。Google、Yahoo 和 Bing 搜索支持这种安全搜索执行方法。

鉴于搜索提供商提供的安全搜索设置不同，请先查看不同的安全搜索执行。然后，您可以通过两种方式实施安全搜索：可以阻止禁用安全搜索时的搜索结果，也可以透明启用用户安全搜索：

- 搜索提供商的安全搜索设置
- 阻止未启用严格安全搜索时的搜索结果
- 透明启用用户安全搜索

## 搜索提供商的安全搜索设置

每个搜索提供商的安全搜索设置各不相同，请查看以下设置了解详情。

| 搜索提供商 | 安全搜索设置说明 |
|---|---|
| Google/YouTube | 通过 Google 安全搜索虚拟 IP 地址在各台计算机上或整个网络中提供安全搜索：<br>针对个人计算机上的 **Google** 搜索的安全搜索执行<br>在 Google 搜索设置中，**Filter explicit results**（筛选显式结果）设置可启用安全搜索功能。启用后，该设置会以 `FF=` 的形式存储在浏览器 Cookie 中，并会在每次用户执行 Google 搜索时传递到服务器。<br>将 **`safe=active`** 附加到 Google 搜索查询 URL 还会启用最严格安全搜索设置。<br>针对使用虚拟 **IP** 地址的 **Google** 和 **YouTube** 搜索的安全搜索执行<br>Google 会在每个 Google 和 YouTube 搜索中为服务器提供锁定安全搜索 (forcesafesearch.google.com) 设置。通过为 **`www.google.com`** 和 **`www.youtube.com`**（以及其他相关 Google 和 YouTube 国家/地区子域）添加 DNS 条目以将指向 **`forcesafesearch.google.com`** 的 CNAME 记录包含在您的 DNS 服务器配置中，您可以确保网络上的所有用户在每次执行 Google 或 TouTube 搜索时都会使用严格的安全搜索设置。但请记住，此解决方案与防火墙上的安全搜索执行不兼容。因此，如果您正在使用此选项在 Google 上执行安全搜索，最佳实践是通过创建自定义 URL 类别并将其添加到 URL 筛选配置文件中的阻止列表来阻止访问防火墙上的其他搜索引擎。 |


© 2019 Palo Alto Networks, Inc.

| 搜索提供商 | 安全搜索设置说明 |
| --- | --- |
| | • *PAN-OS* 支持通过 *HTTP* 标头插入实施 *YouTube* 安全搜索。*HTTP/2* 当前不支持 *HTTP* 标头插入。要实施 *YouTube* 安全搜索，应用程序 ID 和 HTTP/2 检查 请使用适当解密配置文件中的 *Strip ALPN*（剥离 *ALPN*）功能将 *HTTP/2* 连接降级为 *HTTP/1.1*。<br>• 如果您计划使用 *Google Lock SafeSearch* 解决方案，请考虑配置 *DNS* 代理（*Network*（网络）> *DNS Proxy*（*DNS* 代理））并将继承源设置为第 *3* 层接口，防火墙会在该接口上通过 *DHCP* 从服务提供商处接收 *DNS* 设置。您应使用 *www.google.com* 和 *www.youtube.com* 的 *Static Entries*（静态条目）配置 *DNS* 代理，以便为 *forcesafesearch.google.com* 服务器使用本地 *IP* 地址。 |
| Yahoo | 仅在各台计算机上提供安全搜索。Yahoo 搜索首选项包含三个安全搜索设置：**Strict**（严格）、**Moderate**（中等）或 **Off**（关闭）。启用后，该设置会以 `vm=` 的形式存储在浏览器 Cookie 中，并会在每次用户执行 Yahoo 搜索时传递到服务器。<br>将 `vm=r` 附加到 Yahoo 搜索查询 URL 还会启用最严格安全搜索设置。<br>如果在登录 *Yahoo* 帐户后在 *Yahoo Japan* (***yahoo.co.jp***) 执行搜索，终端用户还必须启用 *SafeSearch*（安全搜索）*Lock*（锁定）选项。 |
| Bing | 在各台计算机上或通过其 Bing in the Classroom 程序提供安全搜索。Bing 设置包含三个安全搜索设置：**Strict**（严格）、**Moderate**（中等）或 **Off**（关闭）。启用后，该设置会以 `adtl=` 的形式存储在浏览器 Cookie 中，并会在每次用户执行 Bing 搜索时传递到服务器。<br>将 **`adlt=strict`** 附加到 Bing 搜索查询 URL 还会启用最严格安全搜索设置。<br>Bing SSL 搜索引擎不会执行安全搜索 URL 参数，因此您应该考虑阻止基于 SSL 的 Bing，以实现全面安全搜索执行。 |

# 阻止未启用严格安全搜索时的搜索结果

默认情况下，在您启用安全搜索执行后，如果用户在未使用最严格安全搜索设置的情况下尝试执行搜索，那么防火墙会阻止搜索查询结果并显示 URL 筛选安全搜索阻止页面。该页面会提供一个指向相应搜索提供商的搜索设置页面的链接，以便终端用户能够启用安全搜索设置。如果计划使用该默认方法来执行安全搜索，那么您应该在部署该策略之前与终端用户进行相应沟通。有关各个搜索提供商的安全搜索实施方式的详细信息，请参阅。默认 URL 筛选安全搜索阻止页面会提供一个指向相应搜索提供商的搜索设置的链接。您可以选择自定义 URL 筛选响应页面。

另外，要启用安全搜索执行以对终端用户保持透明，请将防火墙配置为透明启用用户安全搜索。

STEP 1 | 在 URL 筛选配置文件中启用安全搜索执行。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）。
2. 选择要修改的现有配置文件，或克隆默认配置文件以创建新配置文件。
3. 在 **Settings**（设置）选项卡上，选中 **Safe Search Enforcement**（安全搜索执行）复选框以加以启用。
4. （可选）限制用户使用特定搜索引擎：
   1. 在 **Categories**（类别）选项卡中，将 **search-engines**（搜索引擎）类别设置为 **block**（阻止）。
   2. 针对希望终端用户能够访问的各个搜索引擎，在 **Allow List**（允许列表）文本框中输入 Web 地址。例如，为了只允许用户访问 Google 和 Bing 搜索，您要输入以下内容：

      **`www.google.com`**



© 2019 Palo Alto Networks, Inc.

```
www.bing.com
```

5. 根据需要配置其他设置，以便：
   - 为每个 URL 类别定义站点访问。
   - 定义阻止和允许列表，以指定始终应阻止或允许的网站，而不考虑 URL 类别。
6. 单击 **OK**（确定）保存配置文件。

STEP 2 | 将 URL 筛选配置文件添加到安全策略规则中，以允许来自互联网信任区域内客户端的流量。

1. 选择 **Policies**（策略）> **Security**（安全）并选择要将您刚启用安全搜索执行的 URL 筛选配置文件应用于的规则。
2. 在 **Actions**（操作）选项卡上，选择 **URL Filtering**（**URL** 筛选）配置文件。
3. 单击 **OK**（确定）以保存安全策略规则。

STEP 3 | 启用 SSL 转发代理解密。

由于大多数搜索引擎都会对其搜索结果进行加密，因此您必须启用 SSL 转发代理解密，以便防火墙能够检查搜索流量并检测安全搜索设置。

1. 为搜索站点添加自定义 URL 类别：
   1. 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类型）并 **Add**（添加）自定义类别。
   2. 输入类别 **Name**（名称），如 SearchEngineDecryption。
   3. 将以下内容 **Add**（添加）到站点列表中：

      ```
      www.bing.*
      ```

      ```
      www.google.*
      ```

      ```
      search.yahoo.*
      ```
   4. 单击 **OK**（确定）以保存自定义 URL 类别对象。
2. 按步骤配置 SSL 转发代理。
3. 在解密策略规则的 **Service/URL Category**（服务/**URL** 类别）选项卡中，**Add**（添加）您刚刚创建的自定义 URL 类别，然后单击 **OK**（确定）。

STEP 4 | （推荐）阻止在 SSL 上运行的 Bing 搜索流量。

由于 Bing SSL 搜索引擎并不遵循安全搜索设置，因此为了实现全面安全搜索执行，您必须拒绝在 SSL 上运行的所有 Bing 会话。

1. 为 Bing 添加自定义 URL 类别：
   1. 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类型）并 **Add**（添加）自定义类别。
   2. 输入类别 **Name**（名称），如 EnableBingSafeSearch。
   3. 将以下内容 **Add**（添加）到站点列表中：

      ```
      www.bing.com/images/*
      ```

      ```
      www.bing.com/videos/*
      ```
   4. 单击 **OK**（确定）以保存自定义 URL 类别对象。
2. 创建另一个 URL 筛选配置文件以阻止您刚创建的自定义类别：
   1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）。
   2. **Add**（添加）新配置文件并为其指定描述性 **Name**（名称）。
   3. 在类别列表中找到自定义类别并将其设置为 **block**（阻止）。
   4. 单击 **OK**（确定）以保存 URL 筛选配置文件。
3. 添加安全策略规则以阻止 Bing SSL 流量：


© 2019 Palo Alto Networks, Inc.

1. 选择 **Policies**（策略）> **Security**（安全）并 **Add**（添加）策略规则以允许来自 Internet 信任区域的流量。
2. 在 **Actions**（操作）选项卡上，附加您刚创建的 URL 筛选配置文件以阻止自定义 Bing 类别。
3. 在 **Service/URL Category**（服务/URL 类别）选项卡上，**Add**（添加）**New Service**（新服务）并为其指定描述性 **Name**（名称），如 bingssl。
4. 选择 **TCP** 作为 **Protocol**（协议）并将 **Destination Port**（目标端口）设置为 `443`。
5. 单击 **OK**（确定）保存规则。
6. 使用 **Move**（移动）选项，以确保该规则位于具有已启用安全搜索执行的 URL 筛选配置文件的规则之下。

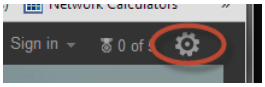
STEP 5 | 保存配置。

单击 **Commit**（提交）。

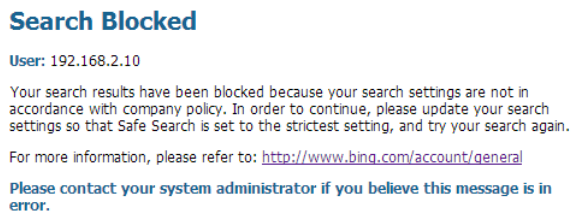
STEP 6 | 验证安全搜索执行配置。

仅当您正使用阻止页面执行安全搜索时，该验证步骤才会执行。如果您正使用透明安全搜索执行，防火墙阻止页面将调用使用查询字符串中安全搜索参数的 URL 重写。

1. 从防火墙的后台计算机中，为某一受支持搜索提供商禁用严格搜索设置。例如，在 bing.com 中，单击 Bing 菜单栏中的 **Preferences**（首选项）图标。




2. 将 **SafeSearch**（安全搜索）选项设置为 **Moderate**（中等）或 **Off**（关闭），然后单击 **Save**（保存）。
3. 执行 Bing 搜索，并验证 URL 筛选安全搜索阻止页面有否显示，而非验证搜索结果：




4. 使用阻止页面中的链接转至搜索提供商的搜索设置，并将安全搜索设置重新设置为最严格设置（对于 Bing，设置为 **Strict**（严格）），然后单击 **Save**（保存）。
5. 再次从 Bing 执行搜索，并验证经过筛选的搜索结果，而非验证阻止页面。

# 透明启用用户安全搜索

如果想要使用最严格的安全搜索筛选器来执行搜索查询结果筛选，但又不希望终端用户必须手动配置设置，那么您可以按照以下步骤启用透明安全搜索执行。该功能仅受 Google、Yahoo 和 Bing 搜索引擎支持，且需要使用 Content Release V475 或更高版本。

STEP 1 | 确保防火墙正在运行 Content Release V475 或更高版本。

1. 选择 **Device**（设备）> **Dynamic Updates**（动态更新）。
2. 检查 **Applications and Threats**（应用程序和威胁）部分以确定当前正在运行的更新。
3. 如果防火墙并未运行所需更新或更高版本，请单击 **Check Now**（立即检查）以检索可用更新列表。
4. 找到所需更新并单击 **Download**（下载）。
5. 下载完成后，单击 **Install**（安装）。

STEP 2 | 在 URL 筛选配置文件中启用安全搜索执行。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（URL 筛选）。



© 2019 Palo Alto Networks, Inc.

2. 选择要修改的现有配置文件，或克隆默认配置文件以创建新配置文件。
3. 在 **Settings**（设置）选项卡上，选中 **Safe Search Enforcement**（安全搜索执行）复选框以加以启用。
4. （可选）只允许访问特定搜索引擎：
   1. 在 **Categories**（类别）选项卡中，将 **search-engines**（搜索引擎）类别设置为 **block**（阻止）。
   2. 针对希望终端用户能够访问的各个搜索引擎，在 **Allow List**（允许列表）文本框中输入 Web 地址。例如，为了只允许用户访问 Google 和 Bing 搜索，您要输入以下内容：

      ```
      www.google.com
      ```

      ```
      www.bing.com
      ```
5. 根据需要配置其他设置，以便：
   - 为每个 URL 类别定义站点访问。
   - 定义阻止和允许列表，以指定始终应阻止或允许的网站，而不考虑 URL 类别。
6. 单击 **OK**（确定）保存配置文件。

STEP 3 | 将 URL 筛选配置文件添加到安全策略规则中，以允许来自互联网信任区域内客户端的流量。

1. 选择 **Policies**（策略）> **Security**（安全）并选择要将您刚启用安全搜索执行的 URL 筛选配置文件应用于的规则。
2. 在 **Actions**（操作）选项卡上，选择 **URL Filtering**（**URL** 筛选）配置文件。
3. 单击 **OK**（确定）以保存安全策略规则。

STEP 4 | （推荐）阻止在 SSL 上运行的 Bing 搜索流量。

由于 Bing SSL 搜索引擎并不遵循安全搜索设置，因此为了实现全面安全搜索执行，您必须拒绝在 SSL 上运行的所有 Bing 会话。

1. 为 Bing 添加自定义 URL 类别：
   1. 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类型）并 **Add**（添加）自定义类别。
   2. 输入类别 **Name**（名称），如 EnableBingSafeSearch。
   3. 将以下内容 **Add**（添加）到站点列表中：

      ```
      www.bing.com/images/*
      ```

      ```
      www.bing.com/videos/*
      ```
   4. 单击 **OK**（确定）以保存自定义 URL 类别对象。
2. 创建另一个 URL 筛选配置文件以阻止您刚创建的自定义类别：
   1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）。
   2. **Add**（添加）新配置文件并为其指定描述性 **Name**（名称）。
   3. 在类别列表中找到您刚创建的自定义类别并将其设置为 **block**（阻止）。
   4. 单击 **OK**（确定）以保存 URL 筛选配置文件。
3. **Add**（添加）安全策略规则以阻止 Bing SSL 流量：
   1. 选择 **Policies**（策略）> **Security**（安全）并 **Add**（添加）策略规则以允许来自 Internet 信任区域的流量。
   2. 在 **Actions**（操作）选项卡上，附加您刚创建的 URL 筛选配置文件以阻止自定义 Bing 类别。
   3. 在 **Service/URL Category**（服务/**URL** 类别）选项卡上，**Add**（添加）**New Service**（新服务）并为其指定描述性 **Name**（名称），如 bingssl。
   4. 选择 **TCP** 作为 **Protocol**（协议），将 **Destination Port**（目标端口）设置为 **443**。
   5. 单击 **OK**（确定）保存规则。
   6. 使用 **Move**（移动）选项，以确保该规则位于具有已启用安全搜索执行的 URL 筛选配置文件的规则之下。


© 2019 Palo Alto Networks, Inc.

STEP 5 | 编辑 URL 过滤安全搜索阻止页面，将现有代码替换为用于重写搜索查询 URL 以透明地执行安全搜索的 JavaScript。

1. 选择 **Device**（设备）> **Response Pages**（响应页面）> **URL Filtering Safe Search Block Page**（**URL** 筛选安全搜索阻止页面）。
2. 选择 **Predefined**（预定义），然后单击 **Export**（导出）以将文件保存在本地。
3. 使用 HTML 编辑器，并将所有现有阻止页面文本替换为以下文本，然后保存文件。

```
<html>
  <head>
    <title>Search Blocked</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta http-equiv="pragma" content="no-cache">
    <meta name="viewport" content="initial-scale=1.0">
    <style>
      #content {
      border:3px solid#aaa;
      background-color:#fff;
      margin:1.5em;
      padding:1.5em;
      font-family:Tahoma,Helvetica,Arial,sans-serif;
      font-size:1em;
      }
      h1 {
      font-size:1.3em;
      font-weight:bold;
      color:#196390;
      }
      b {
      font-weight:normal;
      color:#196390;
      }
    </style>
  </head>
  <body bgcolor="#e7e8e9">
    <div id="content">
      <h1>Search Blocked</h1>
      <p>
        <b>User:</b>
        <user/>
      </p>
      <p>Your search results have been blocked because your search
 settings are not in accordance with company policy.  In order to
 continue, please update your search settings so that Safe Search is
 set to the strictest setting. If you are currently logged into your
 account, please also lock Safe Search and try your search again.</p>
      <p>
        For more information, please refer to:
        <a href="<ssurl/>">
          <ssurl/>
        </a>
      </p>
      <p id="java_off"> Please enable JavaScript in your browser.<br></
p>
      <p><b>Please contact your system administrator if you believe this
 message is in error.</b></p>
    </div>
  </body>
  <script>
```



© 2019 Palo Alto Networks, Inc.

```
    // Grab the URL that's in the browser.
    var s_u = location.href;
    //bing
    // Matches the forward slashes in the beginning, anything, then
".bing." then anything followed by a non greedy slash. Hopefully the
first forward slash.
    var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u);
    if (b_a) {
       s_u = s_u + "&adlt=strict";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You are being
redirected to a safer search!';
    }
    //google
    // Matches the forward slashes in the beginning, anything, then
".google." then anything followed by a non greedy slash. Hopefully the
first forward slash.
    var g_a = /^.*\/\/(.+\.google\..+?)\//.exec(s_u);
    if (g_a) {
        s_u = s_u.replace(/&safe=off/ig,"");
        s_u = s_u + "&safe=active";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You are being
redirected to a safer search!';    }
    //yahoo
    // Matches the forward slashes in the beginning, anything, then
".yahoo."" then anything followed by a non greedy slash. Hopefully the
first forward slash.
    var y_a = /^.*\/\/(.+\.yahoo\..+?)\//.exec(s_u);
    if (y_a) {
        s_u = s_u.replace(/&vm=p/ig,"");
        s_u = s_u + "&vm=r";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You are being
redirected to a safer search!';
    }
    document.getElementById("java_off").innerHTML = ' ';
  </script>
</html>
```

STEP 6 | 将经过编辑的 URL 筛选安全搜索阻止页面导入到防火墙上。

1. 要导入经过编辑的阻止页面，请选择 **Device**（设备）> **Response Pages**（响应页面）> **URL Filtering Safe Search Block Page**（URL 筛选安全搜索阻止页面）。
2. 单击 **Import**（导入），然后在 **Import File**（导入文件）字段中输入路径和文件名，或 **Browse**（浏览）以定位文件。
3. （可选）从 **Destination**（目标）下拉列表中选择将在其上使用该登录页面的虚拟系统，或选择 **shared**（共享）以使其可供所有虚拟系统使用。
4. 单击 **OK**（确定）以导入文件。

STEP 7 | 启用 SSL 转发代理解密。

由于大多数搜索引擎都会对其搜索结果进行加密，因此您必须启用 SSL 转发代理解密，以便防火墙能够检查搜索流量并检测安全搜索设置。

1. 为搜索站点添加自定义 URL 类别：
    1. 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（URL 类型）并 **Add**（添加）自定义类别。


© 2019 Palo Alto Networks, Inc.

2. 输入类别 **Name**（名称），如 SearchEngineDecryption。
3. 将以下内容 **Add**（添加）到站点列表中：

   ```
   www.bing.*
   ```

   ```
   www.google.*
   ```

   ```
   search.yahoo.*
   ```
4. 单击 **OK**（确定）以保存自定义 URL 类别对象。

2. 按步骤配置 SSL 转发代理。
3. 在解密策略规则的 **Service/URL Category**（服务/**URL** 类别）选项卡中，**Add**（添加）您刚刚创建的自定义 URL 类别，然后单击 **OK**（确定）。

STEP 8 | 保存配置。

单击 **Commit**（提交）。

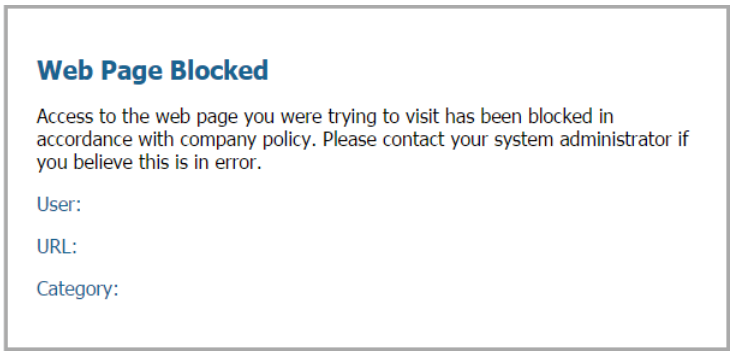


© 2019 Palo Alto Networks, Inc.

# URL 筛选响应页面

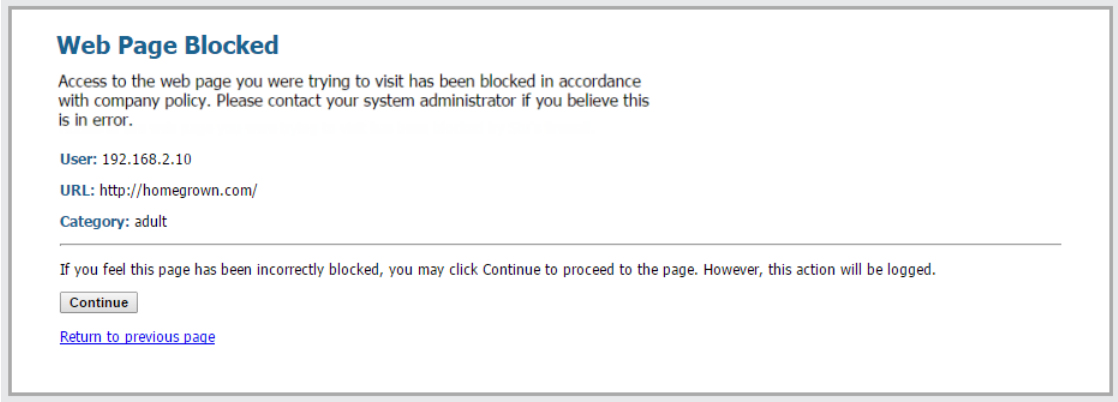
防火墙会提供三个预定义响应页面，当用户尝试浏览的站点属于配置有 URL 筛选配置文件中的任一阻止操作（阻止、继续或覆盖）的类别时，或是当 Container Pages（容器页面）已启用时，这些页面默认显示：

- **URL** 过滤和类别匹配阻止页面




- **URL** 过滤继续和替代页面

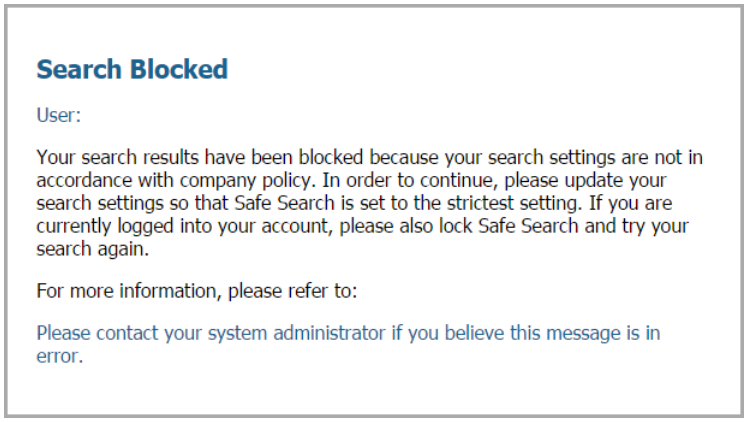
  包含可使用户通过单击 **Continue**（继续）以绕过阻止的初始阻止策略的页面。如果启用 URL 管理替代（允许密码访问某些站点），单击 **Continue**（继续）后，用户必须提供密码才能替代阻止此 URL 的策略。




- **URL** 筛选安全搜索块页

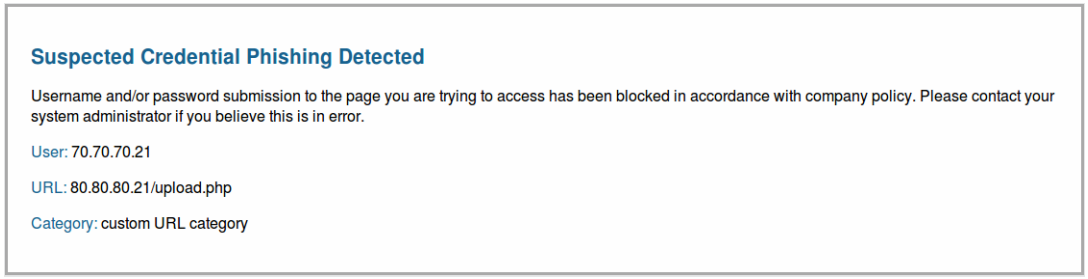
  安全策略规则阻止访问，该策略中的 URL 筛选配置文件已启用安全搜索执行选项（请参阅安全搜索执行）。如果使用 Google、Bing、Yahoo 或 Yandex 执行搜索，且其浏览器或搜索引擎帐户的安全搜索设置未设置为严格，则用户将看到此页面。


© 2019 Palo Alto Networks, Inc.



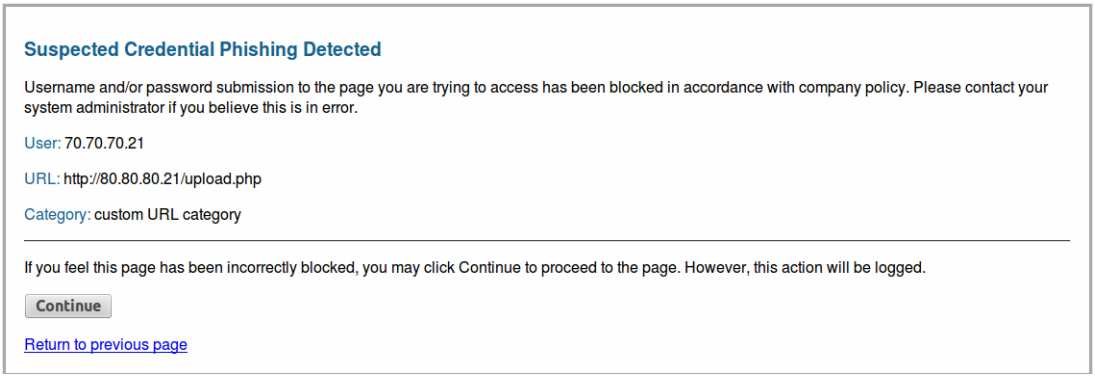

- 防钓鱼阻止页面

  当用户尝试在阻止凭据提交的类别中的网页上输入公司凭据（用户名或密码）时，向用户显示该页面。用户可以继续访问该站点，但仍然无法向任何关联的网络表单提交有效的公司凭据。要控制用户可以提交公司凭据的站点，防火墙必须配置 User-ID，并根据 URL 类别启用以便阻止凭据网络钓鱼。




- 防钓鱼继续页面

  此页面警告用户不要将凭据（用户名和密码）提交到网站。警告用户不要提交凭据可以帮助阻止他们重复使用公司凭据，并向他们讲解有关可能的网络钓鱼尝试的风险。他们必须选择继续才能在站点上输入凭据。要控制用户可以提交公司凭据的站点，防火墙必须配置 User-ID，并根据 URL 类别启用以便阻止凭据网络钓鱼。




您可以使用预定义页面，也可以自定义 URL 筛选响应页面，以便就您的特定可接受使用策略和/或公司品牌进行交流。另外，您还可以使用 URL 筛选响应页面变量在出现阻止事件时进行替换，或将任一受支持响应页面引用添加到外部图像、声音或样式表。



© 2019 Palo Alto Networks, Inc.

表 2: URL 筛选响应页面变量

| 变量 | 使用情况 |
| --- | --- |
| <user/> | 在显示响应页面时，防火墙会使用用户的用户名（如果可以通过 User-ID 加以使用）或 IP 地址来代替该变量。 |
| <url/> | 在显示响应页面时，防火墙会使用所请求的 URL 来代替该变量。 |
| <category/> | 防火墙会使用被阻止请求的 URL 筛选类别来代替该变量。 |
| <pan_form/> | 用于在“URL 筛选继续和替代”页面上显示 **Continue**（继续）按钮的 HTML 代码。 |

您还可以添加代码，以触发防火墙根据用户尝试访问的 URL 类别来显示不同的消息。例如，响应页面中的以下代码片段可指定在 URL 类别为 games 时显示消息 1，在类别为 travel 时显示消息 2，或在类别为 kids 时显示消息 3：

```
var cat = "<category/>";
switch(cat)
{
 case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break;
 case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break;
 case 'kids':
 document.getElementById("warningText").innerHTML = "Message 3";
 break;
}
```

对于每个阻止页面类型，只能为每个虚拟系统加载一个 HTML 页面。但是，当浏览器中显示响应页面时，可以从其他服务器加载其他资源，如图像、声音和级联样式表（CSS 文件）。所有引用都必须包含完全限定 URL。

表 3: 响应页面引用

| 引用类型 | 示例 HTML 代码 |
| --- | --- |
| 图像 | `<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">` |
| 声音 | `<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">` |
| 样式表 | `<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />` |


© 2019 Palo Alto Networks, Inc.

| 引用类型 | 示例 HTML 代码 |
| --- | --- |
| **超链接** | `<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">View Corporate Policy</a>` |



© 2019 Palo Alto Networks, Inc.

# 自定义 URL 筛选响应页面

防火墙提供预定义的URL 筛选响应页面，默认情况下，当用户执行以下操作时显示：

- 用户尝试浏览到具有受限访问的类别中的站点。
- 用户向启用凭据检测的站点提交有效的公司凭据（根据 URL 类别预防凭证网络钓鱼）。
- 仅记录用户访问页面阻止搜索尝试。

但是，您可以使用公司品牌、可接受的使用策略和指向内部资源的链接来创建自己的自定义响应页面。



大于最大支持大小的自定义响应页面不会被解密或向用户显示。在 *PAN-OS 8.1.2* 及更高版本 *PAN-OS 8.1* 发布中，解密站点上的自定义响应页面不会超过 *8191* 字节；在 *PAN-OS 8.1.3* 及更高版本中，最大大小增至 *17999* 字节。

STEP 1 | 导出默认响应页面。

1. 选择 **Device**（设备）> **Response Pages**（响应页面）。
2. 选择想要修改的 URL 筛选响应页面的链接。
3. 单击响应页面（预定义或共享），然后单击 **Export**（导出）链接，并将文件保存到桌面。

STEP 2 | 编辑导出的页面。

1. 使用所选 HTML 文本编辑器编辑该页面：
   - 如果希望响应页面显示与已阻止的特定用户、URL 或类别相关的自定义信息，请添加一个或多个受支持表 2: URL 筛选响应页面变量。
   - 如果想要包含自定义图像（如公司徽标）、声音、样式表或其他 URL 链接（如详细记录可接受 Web 使用策略的文档），请包含一个或多个受支持表 3: 响应页面引用。
2. 用新文件名保存编辑后的页面。确保该页面保持其 UTF-8 编码。例如，在“记事本”的“另存为”对话框中，从 **Encoding**（编码）下拉列表中选择 **UTF-8**。

STEP 3 | 导入自定义响应页面。

1. 选择 **Device**（设备）> **Response Pages**（响应页面）。
2. 选择与所编辑 URL 筛选响应页面对应的链接。
3. 单击 **Import**（导入），然后在 **Import File**（导入文件）字段中输入路径和文件名，或 **Browse**（浏览）以定位文件。
4. （可选）从 **Destination**（目标）下拉列表中选择将在其上使用该登录页面的虚拟系统，或选择 **shared**（共享）以使其可供所有虚拟系统使用。
5. 单击 **OK**（确定）以导入文件。

STEP 4 | 保存新的响应页面。

**Commit**（提交）更改。

STEP 5 | 验证新的响应页面是否有显示。

从浏览器中，转至将触发该响应页面的 URL。例如，要查看已修改的 URL 筛选和类别匹配响应页面，请浏览至您的 URL 筛选策略设置为阻止的 URL。

防火墙使用以下端口显示 URL 过滤响应页面：

- **HTTP**—6080
- **Default TLS with firewall certificate**（带防火墙证书的默认 **TLS**）—6081
- **Custom SSL/TLS profile**（自定义 **SSL/TLS** 配置文件）—6082



© 2019 Palo Alto Networks, Inc.

# HTTP 标头日志记录

URL 筛选提供监视和控制网络上的 Web 通信的功能。为了改善 Web 内容的可见性，您可以将 URL 筛选配置文件配置为记录 Web 请求中所含的 HTTP 标头属性。当客户端请求 Web 页面时，HTTP 标头会包含用户代理、推荐人和 x-forwarded-for 字段作为属性值对并将其转发给 Web 服务器。启用 HTTP 标头日志记录后，防火墙会在 URL 筛选日志中记录以下属性值对。



此外，您还可以使用 *HTTP* 标头管理对 *SaaS* 应用程序的访问。要执行此操作，无需获取 *URL* 筛选许可证，但必须使用 *URL* 筛选配置文件打开此功能。

| 属性 | 说明 |
|---|---|
| User-Agent（用户代理） | 用户用于访问 URL 的 Web 浏览器，如互联网Explorer。此信息在 HTTP 请求中发送到服务器。 |
| Referer（推荐人） | 用户链接到其他网页的网页的 URL；它是用户重定向（引用）到所请求的网页的源。 |
| X-Forwarded-For (XFF) | 用于保留请求此网页的用户 IP 地址的 HTTP 请求标头字段中的选项。如果您的网络上有代理服务器，XFF 能让您识别请求此内容的用户的 IP 地址，而不是仅将代理服务器的 IP 地址记录为请求此网页的源 IP 地址。 |
| 已插入标头 | 防火墙插入的标头类型和标头文本。 |



© 2019 Palo Alto Networks, Inc.

# 请求更改 URL 类别

如果您认为 URL 分类错误，您可以向我们发出请求，对其另行分类。直接在防火墙内，或是通过使用 Test A Site（测试站点）提交更改请求。更改请求触发 PAN-DB（URL 筛选云）立即对您建议执行类别更改的 URL 进行分析。如果 PAN-DB 确认新类别建议是正确的，就会批准更改请求。如果 PAN-DB 认为新类别建议不正确，则由来自 Palo Alto Networks 威胁研究和数据科学团队的人工编辑对更改请求进行审核。

提交更改请求后，您将收到我们发送的一封电子邮件，确认我们已收到您的请求。完成调查后，我们将向您发送另一封电子邮件，与您确认调查结果。

您无法请求更改 URL 接收到的风险类别（**high risk**（高风险）、**medium risk**（中风险）或 **low risk**（低风险）），也无法请求将 URL 分类为 **insufficient content**（内容不足）或 **newly-registered domains**（新注册域）。

- 在线提交更改请求
- 提交批量更改请求
- 从防火墙提交更改请求

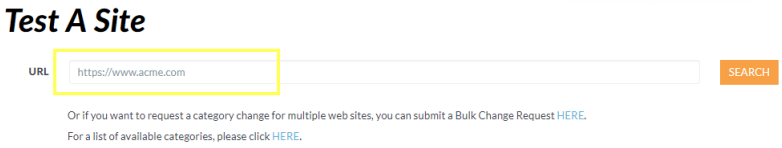
## 在线提交更改请求

要在线提交更改请求，请访问 Palo Alto Networks URL Filtering（URL 筛选）Test A Site（测试站点）。

STEP 1 | 前往 Test A Site（测试站点）。

虽然您需要在更改请求表中填入您的电子邮箱地址，但是，提交更改请求时，您无需登入。如果您决定不登入，需要进行 CAPTCHA 测试，以确认您是一个人（登入可避免 CAPTCHA 测试）。

STEP 2 | 输入 URL，检查其类别：




STEP 3 | 查看 URL 类别，如果您认为类别错误，请选择 **Request Change**（请求更改）。

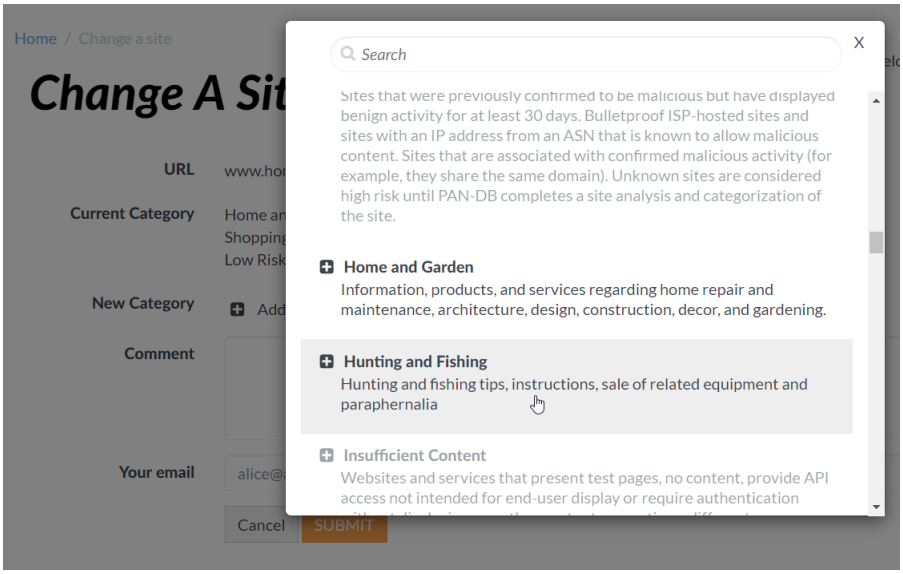



STEP 4 | 继续填写，然后提交更改请求表。

至少包括一条（最多两条）新类别建议，并进行评论（可选），告知我们更多有关您建议的信息。



© 2019 Palo Alto Networks, Inc.



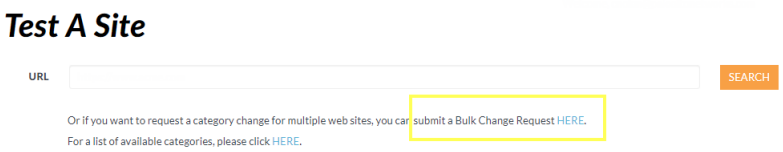

# 提交批量更改请求

如果您想一次性提交多个 URL 的更改请求，您还可以使用 Test A Site（测试站点）提交批量更改请求。

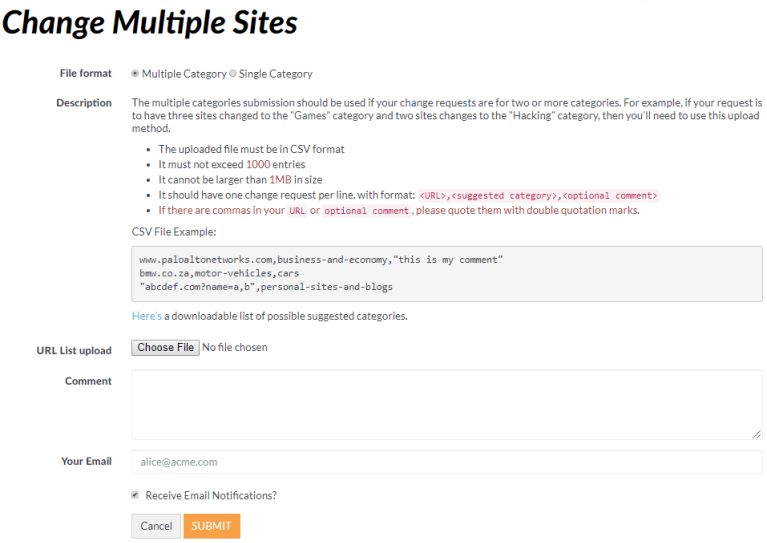
STEP 1 | 前往 Test A Site（测试站点）。

提交更改请求时，您无需登入；但是您需要在更改请求表中填入您的电子邮箱地址。如果您决定不登入，需要进行 CAPTCHA 测试，以确认您是一个人（登入可避免 CAPTCHA 测试）。

STEP 2 | 选择此选项以提交批量更改请求：




STEP 3 | 填写完成后，提交批量更改请求表。

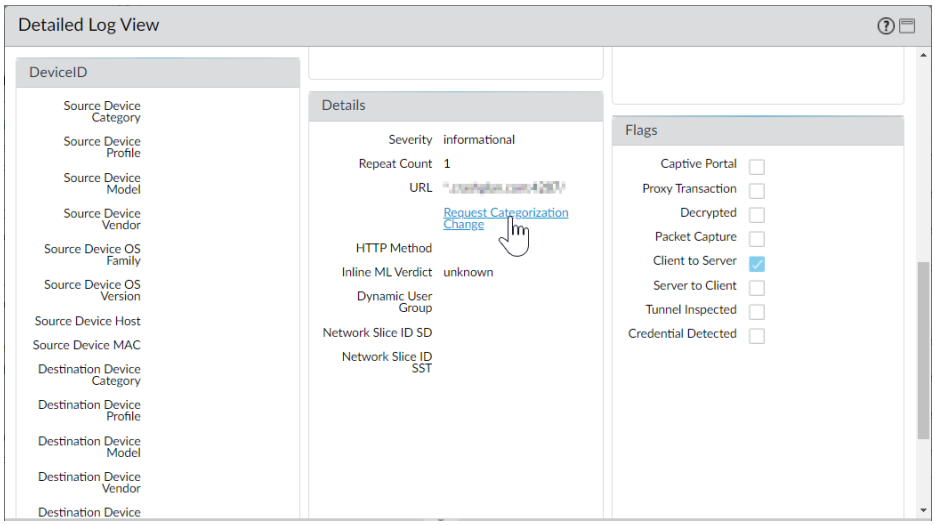




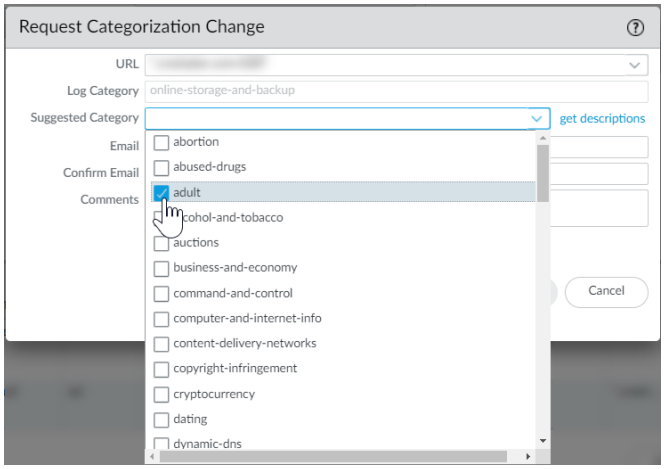

© 2019 Palo Alto Networks, Inc.

# 从防火墙提交更改请求

您还可以直接从防火墙提交 URL 类别更改请求。在 URL 筛选日志中，每个日志条目的详细信息都包含 **Request Categorization Change**（请求类别更改）（**Monitor**（监视器）> **Logs**（日志）> **URL Filtering**（**URL** 筛选））选项。




您可以在此处填写和提交请求表。






© 2019 Palo Alto Networks, Inc.

# 对 URL 筛选进行故障排除

以下主题提供了诊断和解决常见的 URL 筛选问题的故障排除指南。

- 激活 PAN-DB 问题
- PAN-DB 云连接问题
- 将 URL 分类为未解析
- 分类不正确

## 激活 PAN-DB 问题

使用以下工作流程来解决 PAN-DB 激活问题。

STEP 1 | 访问 PAN-OS CLI。

STEP 2 | 通过运行以下命令验证 PAN-DB 是否已激活：

```
show system setting url-database
```

如果响应为 `paloaltonetworks`，则 PAN-DB 为激活供应商。

STEP 3 | 通过运行以下命令验证防火墙是否已获得有效 PAN-DB 许可证：

```
request license info
```

应该能够看到许可证条目 `Feature：PAN-DB URL 筛选`。如果未安装许可证，将需要获取并安装许可证。请参阅配置 URL 筛选。

STEP 4 | 检查 PAN-DB 云连接状态。

## PAN-DB 云连接问题

要检查防火墙和 PAN-DB 云之间的连接：

```
show url-cloud status
```

如果云可访问，则预期响应类似如下：

```
show url-cloud status
PAN-DB URL Filtering
License :                              valid
Current cloud server :                 serverlist.urlcloud.paloaltonetworks.com
Cloud connection :                     connected
Cloud mode :                           public
URL database version - device :        20200624.20296
URL database version - cloud :         20200624.20296  ( last update time
 2020/06/24 12:39:19 )
URL database status :                  good
URL protocol version - device :        pan/2.0.0
URL protocol version - cloud :         pan/2.0.0
Protocol compatibility status :        compatible
```

如果云不可访问，则预期响应类似如下：



© 2019 Palo Alto Networks, Inc.

```
show url-cloud status
PAN-DB URL Filtering
License :                          valid
Cloud connection :                 not connected
URL database version - device :    0000.00.00.000
URL protocol version - device :    pan/0.0.2
```

使用以下清单来识别和解决连接问题：

- PAN-DB URL 筛选许可证字段是否显示为无效？获取并安装有效的 PAN-DB 许可证。
- URL 协议版本是否显示为不兼容？将 PAN-OS 升级到最新版本。
- 您是否可以从防火墙 ping PAN-DB 云服务器？运行以下命令以检查：

```
ping source <ip-address> host serverlist.urlcloud.paloaltonetworks.com <
```

例如，如果管理接口 IP 地址为 10.1.1.5，请运行以下命令：

```
ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
```

- 防火墙是否在 HA 配置中？验证防火墙的 HA 状态是处于主动、主动-主要或主动-辅助状态。如果防火墙处于不同的状态，将阻止对 PAN-DB 云的访问。在对中每个防火墙上运行以下命令以查看状态：

```
show high-availability state
```

如果防火墙和 PAN-DB 云之间仍存在连接问题，请联系 Palo Alto Networks 获得支持。

## 将 URL 分类为未解析

使用以下工作流程来进行故障排除：PAN-DB 所识别的部分或所有 URL 被分类为未解析的原因：

STEP 1 | 通过运行以下命令检查 PAN-DB 云连接：

```
show url-cloud status
```

Cloud connection: 字段应显示 `connected`。如果看到的不是 `connected`，那么未出现在管理面板缓存中的所有 URL 都将被分类为 `not-resolved`。要解决这一问题，请参阅 PAN-DB 云连接问题。

STEP 2 | 如果云连接状态显示 **connected**，请检查防火墙的当前利用率。如果防火墙的利用率突然上升，URL 请求可能会被丢弃（可能无法到达管理面板），并被分类为 **not-resolved**。

要查看系统资源，请运行运行以下命令并查看 `%CPU` 和 `%MEM` 列：

```
show system resources
```

您还可以在 Web 界面的 **Dashboard**（仪表板）上的 “系统资源”小部件上查看系统资源。

STEP 3 | 如果问题仍然存在，请联系 Palo Alto Networks 技术支持人员。

## 分类不正确

有时可能会遇到您认为分类不正确的网址。使用以下工作流程来确定站点的 URL 分类，并在适当时请求类别更改。

STEP 1 | 通过运行以下命令验证数据面板中的类别：



© 2019 Palo Alto Networks, Inc.

```
show running url <URL>
```

例如，要查看 Palo Alto Networks 网站的类别，请运行以下命令：

```
show running url paloaltonetworks.com
```

如果对存储在数据面板缓存中的 URL 分类正确（在本例中为“计算机和互联网信息”），则分类正确且无需执行进一步操作。如果类别不正确，请继续执行下一步。

STEP 2 | 通过运行以下命令验证管理面板中的类别是否正确：

```
test url-info-host <URL>
```

例如：

```
test url-info-host paloaltonetworks.com
```

如果对存储在管理面板缓存中的 URL 分类正确，请通过运行以下命令从数据面板缓存中移除该 URL：

```
clear url-cache url <URL>
```

下一次防火墙请求此 URL 的类别时，请求将会转发到管理面板。这样应该可以解决问题，且无需执行进一步操作。如果这样都无法解决问题，请转到下一步检查云系统中的 URL 类别。

STEP 3 | 通过运行以下命令验证云中的类别：

```
test url-info-cloud <URL>
```

STEP 4 | 如果对存储在云中的 URL 分类正确，请从数据面板和管理面板缓存中移除该 URL。

运行以下命令以从数据面板缓存中删除 URL：

```
clear url-cache url <URL>
```

运行以下命令以从管理面板缓存中删除 URL：

```
delete url-database url <URL>
```

下一次防火墙请求给定 URL 的类别时，请求将会转发到管理面板，然后再转发到云。这样应该可以解决类别查询问题。如果问题仍然存在，请参阅下一步提交分类更改请求。

STEP 5 | 要从 Web 界面提交更改请求，请转到 URL 日志，然后选择想要更改的 URL 的日志条目。

STEP 6 | 单击 **Request Categorization**（请求分类）更改链接，然后按照以下说明进行操作。通过搜索 URL，然后单击 **Request Change**（请求更改）图标，也可以从 Palo Alto Networks 测试站点网站请求类别更改。要查看包含所有可用类别和各类别描述的列表，请参阅 https://urlfiltering.paloaltonetworks.com/CategoryList.aspx。



© 2019 Palo Alto Networks, Inc.

如果更新请求获批，您将收到电子邮件通知。然后，您可以通过两种方式确保 URL 类别在防火墙上得到更新：

- 等到缓存中的 URL 过期，然后当有用户再访问该 URL 时，新分类更新就会进入缓存。
- 运行以下命令强制更新进入缓存：

```
request url-filtering update url <URL>
```


© 2019 Palo Alto Networks, Inc.

# PAN-DB 私有云

PAN-DB 私有云是本地解决方案，用于限制使用云服务的组织。通过该本地解决方案，您可以部署一台或多台 M-600 设备作为您网络或数据中心的 PAN-DB 服务器。防火墙将查询 PAN-DB 私有云来执行 URL 查询，而不是访问 PAN-DB 公共云。

网络上的防火墙在私有云和公共云上执行 URL 查询的过程是相同的。默认情况下，防火墙配置为访问公共 PAN-DB 云。如果您部署 PAN-DB 私有云，则必须为防火墙配置 IP 地址或 FQDN 列表来访问私有云中的服务器。



运行 *PAN-OS 5.0* 或更高版本的防火墙可以与 *PAN-DB* 私有云通信。

当设置 PAN-DB 私有云时，您可以将 M-600 设备配置为拥有直接互联网访问权，或保持设备完全脱机。因为 M-600 设备需要使用数据库和内容更新来执行 URL 查询，因此，如果设备没有活动的互联网连接，您必须手动将更新下载到您网络上的服务器，然后使用 SCP 将更新导入 PAN-DB 私有云中的各台 M-600 设备。此外，该设备必须能够为其服务的防火墙获取种子数据库和其他任何正常或关键内容更新。

为了对连接到 PAN-DB 私有云的防火墙进行身份验证，随设备一起打包了一组默认服务器证书，您不能导入或使用其他服务器证书对防火墙进行身份验证。如果您更改 M-600 设备上的主机名，设备将自动生成一组新的证书来对防火墙进行身份验证。

- 用于 PAN-DB 私有云的 M-600 设备
- 设置 PAN-DB 私有云

## 用于 PAN-DB 私有云的 M-600 设备

要部署 PAN-DB 私有云，您需要一台或多台 M-600 设备。M-600 设备以 Panorama 模式提供，要将其部署为 PAN-DB 私有云，必须将其设置为在 PAN-URL-DB 模式下操作。在 PAN-URL-DB 模式中，此设备为不想使用 PAN-DB 公共云的企业提供 URL 分类服务。

M-600 设备部署为 PAN-DB 私有云时，可使用两个端口 — MGT (Eth0) 和 Eth1，不能使用 Eth2。管理端口用于对设备的管理访问权以及从 PAN-DB 公共云或网络上的服务器获取最新内容更新。对于 PAN-DB 私有云和网络上的防火墙之间的通信，您可以使用 MGT 端口或 Eth1。



*M-200* 设备不能部署为 *PAN-DB* 私有云。

PAN-URL-DB 模式下的 M-600 设备：

- 没有 Web 接口，只支持命令行接口 (CLI)。
- 不能由 Panorama 管理。
- 不能部署在高可用性对中。
- 不需要使用 URL 筛选许可证。防火墙必须有有效的 PAN-DB URL Filtering 许可证才能连接到 PAN-DB 私有云并在其中进行查询。
- 随一组默认服务器证书一起提供，这组证书用于对要连接到 PAN-DB 私有云的防火墙进行身份验证。您不能导入或使用其他服务器证书对防火墙进行身份验证。如果您更改 M-600 设备上的主机名，设备将自动生成一组新的证书来对其服务的防火墙进行身份验证。
- 只能重置为 Panorama 模式。如果您想将此设备部署为专用日志收集器，请切换到 Panorama 模式，然后在日志收集器模式中对其进行设置。



© 2019 Palo Alto Networks, Inc.

表 4: **PAN-DB** 公共云和 **PAN-DB** 私有云之间的差别

| 差别 | PAN-DB 公共云 | PAN-DB 私有云 |
|---|---|---|
| 内容更新和数据库更新 | 内容（常规和关键）更新和完整数据库更新在一天内多次发布。PAN-DB 公共云每五分钟更新一次 URL 类别恶意软件和网络钓鱼。只要防火墙查询云服务器进行 URL 查找就会检查关键更新。 | 工作日的某一天可一次性获取内容更新和完整 URL 数据库更新。 |
| **URL** 分类请求 | 使用以下选项提交 URL 分类更改请求：<br>• Palo Alto Networks 测试站点网站。<br>• 防火墙上的 URL 筛选配置文件设置页面。<br>• 防火墙上的 URL 筛选日志。 | 只使用 Palo Alto Networks 测试站点网站提交 URL 分类更改请求。 |
| 未解析的 **URL** 查询 | 如果防火墙不能解析 URL 查询，该请求将发送到公共云中的服务器。 | 如果防火墙不能解析查询，该请求将发送到 PAN-DB 私有云中的 M-600 设备。如果此 URL 没有匹配项，PAN-DB 私有云会向防火墙发送类别未知响应；该请求不会发送到公共云，除非您已将 M-600 设备配置为访问 PAN-DB 公共云。<br>如果构成您 PAN-DB 私有云的 M-600 设备配置为完全脱机，则设备不会向公共云发送任何数据和分析。 |

# 设置 PAN-DB 私有云

要在网络或数据中心内部署一台或多台 M-600 设备作为 PAN-DB 私有云，必须完成以下任务：

- 配置 PAN-DB 私有云
- 将防火墙配置为访问 PAN-DB 私有云
- 在 PAN-DB 私有云上使用自定义证书配置身份验证

## 配置 *PAN-DB* 私有云

STEP 1 | 机架式安装 M-600 设备。

有关说明，请参阅《M-600 硬件参考指南》。

STEP 2 | 注册 M-600 设备。

有关注册 M-600 设备的说明，请参阅注册防火墙。

STEP 3 | 执行 M-600 设备的初始配置。

*PAN-DB* 模式下的 *M-600* 设备使用两个端口 — *MGT (Eth0)* 和 *Eth1*；*PAN-DB* 模式下不使用 *Eth2*。管理端口用于对设备的管理访问权以及从 *PAN-DB* 公共云获取最新内容更新。对于设备（*PAN-DB* 服务器）和网络上的防火墙之间的通信，您可以使用 *MGT* 端口或 *Eth1*。

1. 按以下方式之一连接到 M-600 设备：


© 2019 Palo Alto Networks, Inc.

- 使用串行电缆将计算机连接到 M-600 设备上的控制台端口，并使用终端模拟软件 (9600-8-N-1) 进行连接。
- 使用 RJ-45 以太网电缆从计算机连接到 M-600 设备上的 MGT 端口。从浏览器中访问 https://192.168.1.1。访问此 URL 可能需要将计算机的 IP 地址更改为 192.168.1.0 网络中的地址（如 192.168.1.2）。

2. 收到提示时，登录到设备。使用默认用户名和密码 (admin/admin) 登录。设备将开始初始化。
3. 配置 MGT 接口的网络访问设置（包括 IP 地址）。

```
set deviceconfig system ip-address  <server-IP> netmask <netmask> default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

其中，<*server-IP*>是您想要分配给服务器的管理接口的 IP 地址，<*netmask*> 是子网掩码，<*gateway-IP*> 是网关的 IP 地址，<*DNS-IP*> 是主 DNS 服务器的 IP 地址。

4. 配置 Eth1 接口的网络访问设置（包括 IP 地址）。

```
set deviceconfig system eth1 ip-address  <server-IP> netmask <netmask>
 default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

其中，<*server-IP*> 是您想要分配给服务器的数据接口的 IP 地址，<*netmask*> 是子网掩码，<*gateway-IP*> 是网关的 IP 地址，<*DNS-IP*> 是主 DNS 服务器的 IP 地址。

5. 将您的更改保存到 PAN-DB 服务器。

   提交

STEP 4 | 切换到 PAN-DB 私有云模式。

1. 要切换到 PAN-DB 模式，请使用 CLI 命令：

```
request system system-mode pan-url-db
```



您可以在 *Panorama* 模式和 *PAN-DB* 模式之间以及Panorama 模式和日志收集器模式之间来回切换。不支持 *PAN-DB* 模式和日志收集器模式之间的直接切换。在切换操作模式时，会触发数据重置。除了管理访问设置外，所有现有配置和日志将在重新启动时删除。

2. 使用以下命令验证该模式是否已更改：

```
show pan-url-cloud-status
hostname: M-600
ip-address: 1.2.3.4
netmask: 255.255.255.0
default-gateway: 1.2.3.1
ipv6-address: unknown
ipv6-link-local-address: fe80:00/64
ipv6-default-gateway:
mac-address: 00:56:90:e7:f6:8e
time: Mon Apr 27 13:43:59 2015
uptime: 10 days, 1:51:28
family: m
model: M-600
serial: 0073010000xxx
sw-version: 7.0.0
app-version: 492-2638
app-release-date: 2015/03/19  20:05:33
av-version: 0
```



© 2019 Palo Alto Networks, Inc.

```
av-release-date: unknown
wf-private-version: 0
wf-private-release-date: unknown
logdb-version: 7.0.9
platform-family: m
pan-url-db: 20150417-220
system-mode: Pan-URL-DB
operational-mode: normal
```

3. 使用以下命令查看设备上云数据库的版本：

```
show pan-url-cloud-status
Cloud status:            Up
URL database version:    20150417-220
```

STEP 5 | 安装内容和数据库更新。



设备只存储当前运行的内容版本和前一版本。

选取下列其中一种安装内容和数据库更新的方法：

- 如果 PAN-DB 服务器拥有直接互联网访问权，请使用以下命令：
  1. 检查是否有新版本可用：

     **request pan-url-db upgrade check**
  2. 检查服务器上当前安装的版本：

     **request pan-url-db upgrade info**
  3. 下载和安装最新版本：
     - **request pan-url-db upgrade download latest**
     - **request pan-url-db upgrade install** *<version latest | file>*
  4. 为 M-600 设备设置时间表，使其自动检查更新：

     **set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week** *<day of week>* at *<hr:min>*
- 如果 PAN-DB 服务器处于脱机状态，请访问 Palo Alto Networks 客户支持网站将内容更新下载并保存到您网络上的 SCP 服务器上。然后，您可以使用以下命令导入并安装这些更新：
  - **scp import pan-url-db remote-port** *<port-number>* from username@host:path
  - **request pan-url-db upgrade install file** *<filename>*

STEP 6 | 设置对 PAN-DB 私有云的管理访问



设备有一个默认 *admin* 帐户。您创建的其他任何管理用户可以是超级用户（具有完全访问权）或拥有只读访问权的超级用户。

PAN-DB 私有云不支持使用 RADIUS VSA。如果防火墙或 Panorama 上使用的 VSA 用于支持访问 PAN-DB 私有云，将出现身份验证失败。



© 2019 Palo Alto Networks, Inc.

- 在 PAN-DB 服务器上设置本地管理用户：
  1. 配置
  2. ```
     set mgt-config users  <username> permissions  role-based <superreader |
      superuser> yes
     ```
  3. ```
     set mgt-config users <username> password
     ```
  4. **Enter password:xxxxx**
  5. **Confirm password:xxxxx**
  6. 提交
- 通过 RADIUS 身份验证设置管理用户：
  1. 创建 RADIUS 配置文件。

     ```
     set shared server-profile radius  <server_profile_name>
      server <server_name> ip-address <ip_address> port <port_no>
      secret <shared_password>
     ```
  2. 创建身份验证配置文件

     ```
     set shared authentication-profile  <auth_profile_name> user-
     domain <domain_name_for_authentication> allow-list <all> method radius
      server-profile <server_profile_name>
     ```
  3. 将身份验证配置文件附加到用户。

     ```
     set mgt-config users  <username> authentication-
     profile <auth_profile_name>
     ```
  4. 提交更改。

     提交
- 查看用户列表：

```
show mgt-config users
users {
admin {
phash fnRL/G5lXVMug;
permissions {
role-based {
superuser yes;
}
}
}
admin_user_2 {
permissions {
role-based {
superreader yes;
}
}
authentication-profile RADIUS;
}
}
```

STEP 7 | 将防火墙配置为访问 PAN-DB 私有云。



© 2019 Palo Alto Networks, Inc.

## 将防火墙配置为访问 *PAN-DB* 私有云

在使用 PAN-DB 公共云时，各防火墙访问 AWS 云中的 PAN-DB 服务器来下载合格服务器列表，防火墙可连接这些服务器进行 URL 查询。使用 PAN-DB 私有云，您必须使用将用于 URL 查询的（静态）PAN-DB 私有云服务器列表来配置防火墙。此列表最多可包含 20 个条目，支持 IPv4 地址、IPv6 地址和 FQDN。列表中的每个条目（IP 地址或 FQDN）必须分配到 PAN-DB 服务器的管理接口和/或 eth1。

STEP 1 | 根据防火墙上的 PAN-OS 版本选择以下选项之一。

- 对于运行 PAN-OS 7.0 的防火墙，访问 PAN-OS CLI 或防火墙上的 Web 接口。

  使用以下 CLI 命令配置对私有云的访问：

  ```
  set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
   enable
  ```

  或者，在每个防火墙的 Web 界面中，选择 **Device**（设备）> **Setup**（设置）> **Content-ID**（内容 **ID**），编辑 URL 筛选部分并输入 **PAN-DB Server**（**PAN-DB** 服务器）IP 地址或 FQDN。该列表必须以逗号分隔。
- 对于运行 PAN-OS 5.0、6.0 或 6.1 的防火墙，请使用以下 CLI 命令配置对私有云的访问：

  ```
  debug device-server pan-url-db cloud-static-list-enable <IP addresses> 启用
  ```

  要删除私有 *PAN-DB* 服务器的条目，并允许防火墙连接到 *PAN-DB* 公共云，请使用以下命令：

  ```
  set deviceconfig setting pan-url-db cloud-static-list <IP addresses> 禁用
  ```

  在您删除私有 PAN-DB 服务器的列表时，会在防火墙上触发重选过程。防火墙会先检查 PAN-DB 私有云服务器列表，找到一个条目时，防火墙会访问 AWS 云中的 PAN-DB 服务器来下载它可以连接的合格服务器列表。

STEP 2 | **Commit**（提交）更改。

STEP 3 | 要验证更改是否生效，请在防火墙上使用以下 CLI 命令：

```
show url-cloud-status
Cloud status:            Up
URL database version:    20150417-220
```

## 在 *PAN-DB* 私有云上使用自定义证书配置身份验证

默认情况下，PAN-DB 服务器使用预定义证书进行相互身份验证，以建立用于管理访问和设备间通信的 SSL 连接。但是，您可以使用自定义证书配置身份验证。自定义证书允许您建立唯一的信任链，以确保您的 PAN-DB 服务器和防火墙之间的相互身份验证。对于 PAN-DB 专有云，防火墙充当客户端，PAN-DB 服务器充当服务器。

STEP 1 | 获取密钥对和证书颁发机构 (CA) 颁发的用于 PAN-DB 服务器和防火墙的证书。

STEP 2 | 导入 CA 证书以验证防火墙证书。

1. 登录到 PAN-DB 服务器上的 CLI，并进入配置模式。


© 2019 Palo Alto Networks, Inc.

```
admin@M-600> configure
```

2. 使用 TFTP 或 SCP 导入 CA 证书。

```
admin@M-600# {tftp | scp} import certificate from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-name <value>
 passphrase <value> format {pkcs12 | pem}
```

STEP 3 | 使用 TFTP 或 SCP 导入包含用于 PAN-DB M-600 设备的服务器证书和私钥的密钥对。

```
admin@M-600# {tftp | scp} import keypair from <value> file <value> remote-
port <1-65535> source-ip <ip/netmask> certificate-name <value> passphrase
 <value> format {pkcs12 | pem}
```

STEP 4 | 配置包含根 CA 和中间 CA 的证书配置文件。此证书定义 PAN-DB 服务器和防火墙之间的设备身份验证。

1. 从 PAN-DB 服务器上的 CLI 进入配置模式。

```
admin@M-600> configure
```

2. 命名证书配置文件。

```
admin@M-600# set shared certificate-profile <name>
```

3. （可选）设置用户域。

```
admin@M-600# set shared certificate-profile <name> 域 <value>
```

4. 配置 CA。

*Default-ocsp-url and ocsp-verify-cert are optional parameters.*

admin@M-600# 设置共享证书配置文件 *<name>* CA *<name>*

```
admin@M-600# set shared certificate-profile <name> CA <name> [default-
ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name> [ocsp-verify-
cert <value>]
```

STEP 5 | 配置用于 PAN-DB M-600 设备的 SSL/TLS 配置文件。该配置文件定义 PAN-DB 设备和客户端设备用于 SSL/TLS 服务的证书和协议范围。

1. 标识 SSL/TLS 配置文件。

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. 选择证书。



© 2019 Palo Alto Networks, Inc.

```
admin@M-600# set shared ssl-tls-service-profile <name> certificate <value>
```

3. 定义 SSL/TLS 范围。

   *PAN-OS 8.0* 或以上版本仅支持 *TLS1.2* 和更高版本的 *TLS* 版本。您必须将最高版本设置为 *TLS 1.2* 或 *max*（更高版本）。

```
admin@M-600# set shared ssl-tls-service-profile <name> protocol-settings
 min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name> protocol-settings
 max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | 在 PAN-DB上配置安全服务器通信。

1. 设置 SSL/TLS 配置文件。该 SSL/TLS 服务配置文件适用于 PAN-DB 和防火墙之间的所有 SSL 连接。

```
admin@M-600# set deviceconfig setting management secure-conn-server ssl-
tls-service-profile <ssltls-profile>
```

2. 设置证书配置文件。

```
admin@M-600# set deviceconfig setting management secure-conn-server
 certificate-profile <certificate-profile>
```

3. 设置 PAN-DB 断开和重新连接至防火墙之前应等待的断开等待时间（以分钟计）（范围为 0 - 44640）。

```
admin@M-600# set deviceconfig setting management secure-conn-server
 disconnect-wait-time <0-44640
```

STEP 7 | 导入 CA 证书以验证 PAN-DB M-600 设备证书。

1. 登录到防火墙 Web 界面。
2. 导入 CA 证书。

STEP 8 | 配置防火墙的本地或 SCEP 证书。

1. 如果是本地证书，则导入防火墙密钥对。
2. 如果防火墙使用 SCEP 证书，请配置 SCEP 配置文件。

STEP 9 | 配置防火墙的证书配置文件。您可以单独在每个防火墙上配置此配置，或者您可以将此配置从 Panorama 推送到防火墙作为模板的一部分。

1. 选择防火墙的 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）或 Panorama 的 **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 10 | 在每个防火墙上部署自定义证书。您可以从 Panorama 集中部署证书，也可以在每个防火墙上手动配置。

1. 登录到防火墙 Web 界面。


© 2019 Palo Alto Networks, Inc.

2. 选择防火墙的 **Device**（设备）> **Setup**（设置）> **Management**（管理）或 Panorama 的 **Panorama** > **Setup**（设置）> **Management**（管理），并 **Edit**（编辑）“安全通信”
3. 从相应的下拉列表中选择 **Certificate Type**（证书类型）、**Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
4. 从“自定义通信”设置中选择 **PAN-DB Communication**（**PAN-DB 配置**）。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

提交更改后，直到 **Disconnect Wait Time**（断开连接等待时间）结束后，防火墙才会终止与 PAN-DB 服务器的当前会话。断开连接等待时间将在您于下一步骤中，使用自定义证书后开始倒计时。

STEP 11 | 在所有防火墙上部署自定义证书后，执行自定义证书身份验证。

1. 登录到 PAN-DB 服务器上的 CLI，并进入配置模式。

```
admin@M-600> configure
```

2. 使用自定义证书。

```
admin@M-600# set deviceconfig setting management secure-conn-server
 disable-pre-defined-cert yes
```

提交更改后，断开连接等待时间开始倒计时（如果您已在 PAN-DB 上完成设置的配置）。等待时间结束后，PAN-DB 及其防火墙仅使用已配置证书进行连接。

STEP 12 | 您可以通过两种方式将新的防火墙或 Panorama 添加至您的 PAN-DB 专有云部署。

- 如果不能启用 **Custom Certificates Only**（仅自定义证书），则可以添加新防火墙至 PAN-DB 专有云，然后按照上述方法部署自定义证书。
- 如果在 PAN-DB 专有云上启用 **Custom Certificates Only**（仅自定义证书），则必须在将其连接至 PAN-DB 专有云之前在防火墙上部署自定义证书。

# 服务质量

服务质量 (QoS) 是一组在网络中应用的技术，用于保证能够在有限的网络容量下可靠地运行高优先级的应用程序和流量。为实现这一目的，QoS 技术为网络流量中的特定流提供了不同的处理方式和容量。这样使网络管理员可以分配处理流量的顺序，以及为流量提供的带宽量。

Palo Alto Networks 应用程序服务质量 (QoS) 提供应用到网络的基本 QoS，然后在此基础上进一步为应用程序和用户提供 QoS。

通过下列主题了解和配置 Palo Alto Networks 基于应用程序的 QoS：

- QoS 概述
- QoS 概念
- 配置 QoS
- 为虚拟系统配置 QoS
- 基于 DSCP 分类实施 QoS
- QoS 用例

使用 Palo Alto Networks 产品比较工具查看您的防火墙型号支持的 QoS 功能。选择两个或更多产品型号并单击 **Compare Now**（现在比较）来查看每个型号支持的 QoS 功能（例如，您可以检查您的防火墙型号是否支持子接口上的 QoS，如果支持，您还能查看子接口上能够启用的 QoS 最大数目。）

运行 PAN-OS 7.0 或更高版本的 PA-7000 系列、PA-5200 系列和 PA-3200 系列防火墙均支持聚合以太网 (AE) 接口上的 QoS。

# QoS 概述

使用 QoS 确定网络流量的各个质量方面的优先级，并且对其进行调整。您可以指派处理数据包和分配带宽的顺序，从而确保优先处理所选的流量、应用程序和用户，并且保证其达到最佳效果。

根据带宽（最大传输率）、吞吐量（实际传输率）、延迟（延迟时间）和抖动（延迟中的差异）来测量 QoS 实现的服务质量。由于能够加工和控制这些服务质量测量，因此对于对延迟和抖动高度敏感的高带宽实时流量（例如 IP 语音 (VoIP)、视频会议和视频点播）而言，QoS 特别重要。此外，使用 QoS 会带来以下结果：

- 确定网络和应用程序流量的优先级、保证重要的流量具有较高的优先级，或者限制不重要的流量。
- 使网络中的不同子网、类或用户共享相等的带宽。
- 在外部和/或内部分配带宽、将 QoS 同时应用到上传和下载流量，或者将 QoS 应用到上传或下载流量之一。
- 在企业环境中，确保对客户和可创收的流量的延迟较低。
- 分析应用程序的流量配置，以保证高效地利用带宽。

Palo Alto Networks 防火墙上的 QoS 实现始于三个支持完整 QoS 解决方案的主要配置组件：QoS 配置文件、QoS 策略以及 QoS 出口接口的设置。在 QoS 配置任务中，这三个选项都有助于扩展流量的处理流程，从而根据可配置的参数来优化通信流、确定通信流的优先级，以及分配和保证带宽。

图 QoS 通信流显示流量的处理流程：流量首先从源流入，接着通过启用 QoS 的防火墙对流量进行加工，然后确定流量的优先级并将其传输到目标。

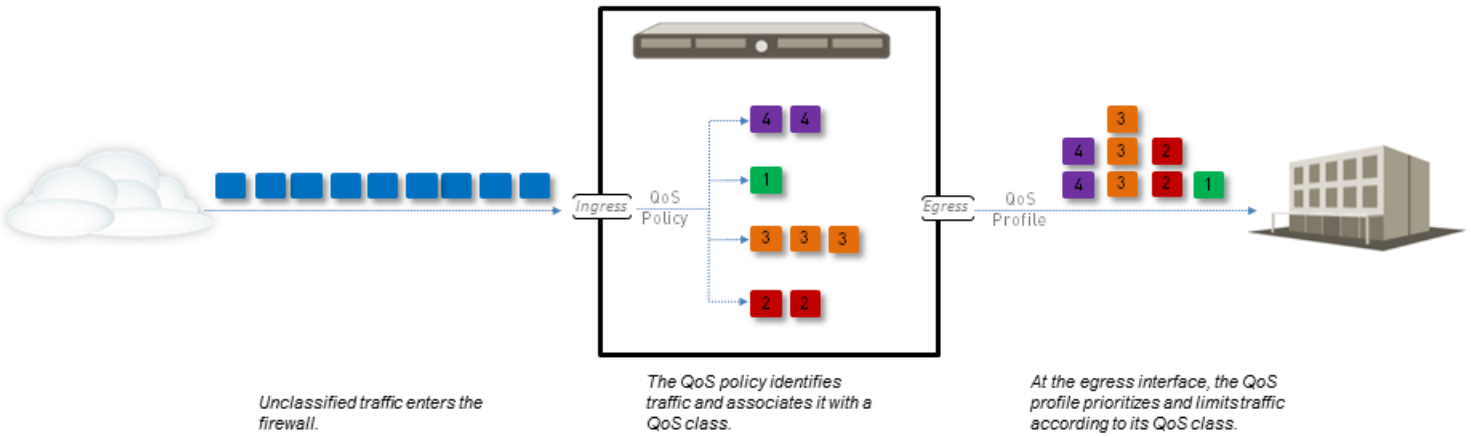



图 **7: QoS** 通信流

可通过 QoS 配置选项控制通信流，并且在流中的不同点对其进行定义。图 QoS 通信流指明可配置的选项在何处定义通信流。QoS 策略规则让您能够定义想要接收 QoS 处理的流量并为此流量分配一个 QoS 类。然后，当匹配流量流出物理接口时，将基于 QoS 配置文件类设置对匹配流量进行加工。

每一种 QoS 配置选项组件相互影响，可以使用 QoS 配置选项来创建完整且精细的 QoS 实施，而且管理员只需要少量操作就可以使用 QoS 配置选项。

每个防火墙型号支持的可以配置 QoS 的最大端口数。请参阅您防火墙型号的规格表或使用产品比较工具在单个页面上查看两个或多个防火墙的 QoS 功能支持。



© 2019 Palo Alto Networks, Inc.

# QoS 概念

通过以下主题来了解 Palo Alto Networks 防火墙上的 QoS 配置的不同组件和机制：

- 用于应用程序和用户的 QoS
- QoS 策略
- QoS 配置文件
- QoS 类
- QoS 优先级队列
- QoS 带宽管理
- QoS 出口接口
- 针对明文与隧道通信的 QoS

## 用于应用程序和用户的 QoS

Palo Alto Networks 防火墙提供基本的 QoS，用于根据网络或子网控制离开防火墙的流量，同时增强 QoS 的功能，以根据应用程序和用户对流量进行分类和加工。为了实现此功能，Palo Alto Networks 防火墙将App-ID和User-ID功能集成到 QoS 配置中。现在可以在 QoS 配置中使用用于在网络中识别特定应用程序和用户的 App-ID 和 User-ID 条目，从而轻松地指定要管理和/或保证其带宽的应用程序和用户。

## QoS 策略

使用 QoS 策略规则定义接受 QoS 处理的流量（无论是优先处理还是流量限制）并为该流量分配服务的 QoS 类。

基于以下条件定义匹配流量的 QoS 策略规则：

- 应用程序和应用程序组。
- 源区域、源地址和源用户。
- 目标区域和目标地址。
- 限制到特定 TCP 和/或 UDP 端口号的服务和服务组。
- URL 类别，包括自定义 URL 类别。
- 差分服务代码点（DSCP）和服务类型（ToS）的值用来指示流量所请求服务的级别，例如高优先级或尽可能地分发。

设置多个 QoS 策略规则（**Policies**（策略）> **QoS**）将不同类型的流量与不同服务的 QoS 类 相关联。

因为流量在传出防火墙时执行 QoS，因此，您可以在防火墙执行完所有其他安全策略规则（包括网络地址转换 (NAT) 规则）后将您的 QoS 策略规则应用到流量。如果想根据源对流量执行 QoS，确保在 QoS 策略规则中指定 NAT 后源地址（不得使用 NAT 前源地址）。

## QoS 配置文件

使用 QoS 配置文件规则定义包含在单个配置文件规则中的 QoS 类（最多 8 个）的值。

使用 QoS 配置文件规则，您可以为 QoS 类定义 QoS 优先级队列和 QoS 带宽管理。每个 QoS 配置文件规则让您能够为最多 8 个 QoS 类配置各个带宽和优先级设置，以及为 8 个类组合配置总带宽。将 QoS 配置文件规则（或多个 QoS 配置文件规则）附加到物理接口以将定义的优先级和带宽设置应用于流出此接口的流量。

可以在防火墙中使用默认的 QoS 配置文件规则。默认配置文件规则和在配置文件中定义的类没有预定义的最大带宽限制或保证带宽限制。

要定义 QoS 类的优先级和带宽设置，请参阅添加 QoS 配置文件规则中的步骤。

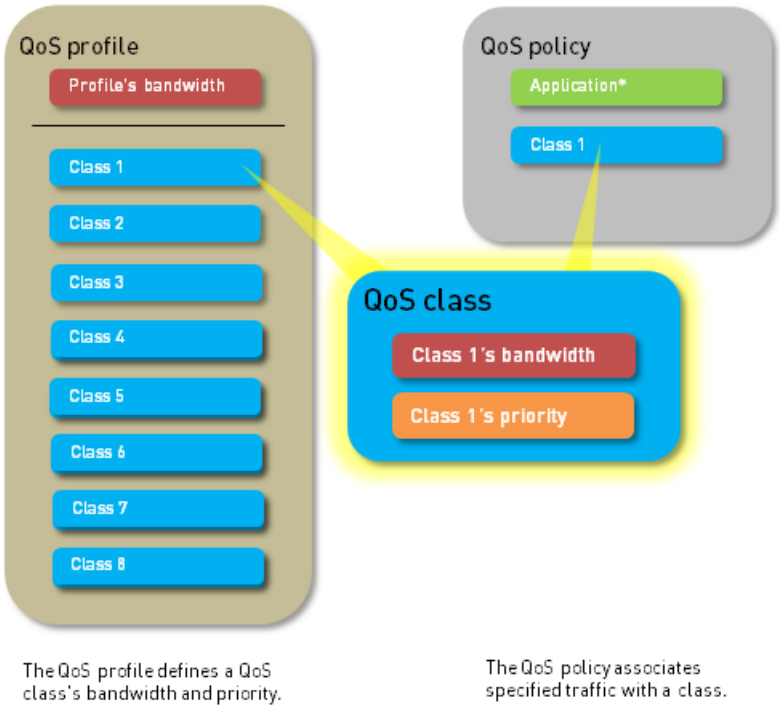


© 2019 Palo Alto Networks, Inc.

# QoS 类

QoS 类确定与 QoS 策略规则匹配的流量的优先级和带宽。您可以使用 QoS 配置文件规则定义 QoS 类。单个 QoS 配置文件中最多可包含 8 个可定义的 QoS 类。除非另行配置，否则会为与 QoS 类不匹配的流量分配类 4。

在 QoS 类定义中配置 QoS 优先级队列和 QoS 带宽管理，以及 QoS 配置的基本机制（请参阅添加 QoS 配置文件规则中的步骤）。对于每个 QoS 类，您可以设置匹配流量的优先级（实时、高、中和低）、最大带宽和保证带宽。QoS 优先级队列和带宽管理确定流量的顺序，以及如何处理进入或离开网络的流量。




# QoS 优先级队列

可以为 QoS 类实施四个优先级之一：实时、高、中和低。与某个 QoS 策略规则匹配的流量将被分配给与此规则关联的 QoS 类，同时防火墙将基于 QoS 类优先级处理匹配流量。将基于传出通信流中的数据包的优先级对其进行排队，直至网络准备好处理这些数据包。优先级排队可以确保重要的流量、应用程序和用户能够得到优先处理。实时优先级通常用于对延迟特别敏感的应用程序（例如语音和视频应用程序）。

# QoS 带宽管理

QoS 带宽管理让您能够控制网络上的通信流，这样流量不会超过网络容量（导致网络拥挤），还能够为特定类型的流量以及应用程序和用户分配带宽。使用 QoS，您可以为流量实施窄宽带或宽宽带。QoS 配置文件规则让您能够为各个 QoS 类设置带宽限制以及为所有 8 个 QoS 类设置总综合带宽。作为配置 QoS 步骤的一部分，您可以将 QoS 配置文件规则附加到某个物理接口以在流出此接口的流量上实施带宽设置：为匹配 QoS 类的流量（QoS 类被分配给符合 QoS 策略规则的流量）实施各个 QoS 类设置，可以将配置文件的总带宽限制应用于所有明文通信、从源接口和源子网发起的特定明文通信、所有隧道通信和各个隧道接口。您可以将多个配置文件规则附加到单个 QoS 接口，以将不同的带宽设置应用于流出此接口的流量。

以下字段支持 QoS 带宽设置：



© 2019 Palo Alto Networks, Inc.

- **Egress Guaranteed**（出口保证）—为匹配流量保证的带宽量。如果超过保证的出口带宽，防火墙会尽量让流量通过。保证带宽如不使用，将继续对所有流量保持可用状态。根据 QoS 配置，您可以为单个 QoS 类、全部或部分明文通信以及全部或部分隧道通信保证带宽。

  示例：

  类 1 流量有 5 Gbps 的保证出口带宽，这意味着类 1 流量有 5 Gbps 可用，但并非为其保留 5 Gbps。如果类 1 流量没有使用或仅使用了部分保证带宽，剩余带宽将可供其他流量类使用。然而，在高流量时段，绝对有 5 Gbps 的带宽可供类 1 流量使用。在拥堵时段，任何超过 5 Gbps 的类 1 流量都会得到尽可能地处理。
- **Egress Max**（最大出口）— 匹配流量的总带宽分配。防火墙将丢弃超过您设置的最大出口限制的流量。根据 QoS 配置，您可以为 QoS 类、所有或部分明文通信、所有或部分隧道通信或所有流出 QoS 接口的通信设置最大带宽。

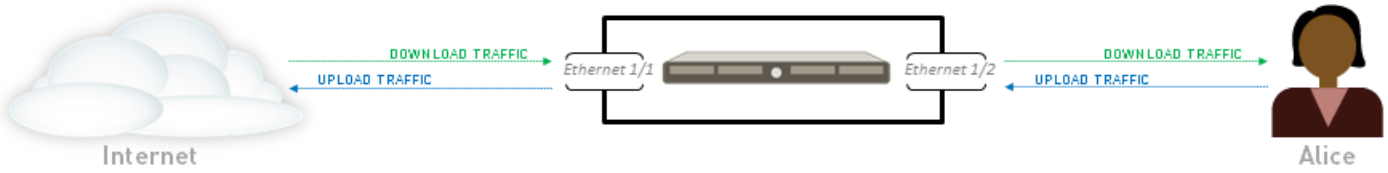
针对附加到接口的 *QoS* 配置文件规则的累计保证带宽不得超过分配给接口的总带宽。

要定义 QoS 类的带宽设置，请参阅添加 QoS 配置文件规则中的步骤。然后将这些带宽设置应用于明文和隧道流量，并设置 QoS 接口的总带宽限制，请参阅在物理接口上启用 QoS 中的步骤。

## QoS 出口接口

在标识为 QoS 处理的流量的出口接口上启用 QoS 配置文件规则即可完成 QoS 配置。QoS 流量的入口接口就是流量进入防火墙的接口。QoS 流量的出口接口则是流量离开防火墙的接口。将始终在通信流的出口接口上启用和实施 QoS。QoS 配置中的出口接口可以是防火墙的面向外部的接口或面向内部的接口，这取决于流量接收 QoS 处理的流。

例如，在企业网络中，如果限制员工从特定网站下载流量，则 QoS 配置中的出口接口是防火墙的内部接口，这是因为通信流来自 Internet，并且通过防火墙进入公司网络。另外，如果限制员工将流量上传到相同的网站，那么 QoS 配置中的出口接口是防火墙的外部接口，这是因为正在限制的流量来自公司网络，并且通过防火墙进入 Internet。




- The egress interface for Alice's download traffic is Ethernet 1/2. To prioritize or limit her download traffic, Alice enables QoS on Ethernet 1/2.
- The egress interface for Alice's upload traffic is Ethernet 1/1. To prioritize or limit her upload traffic, Alice enables QoS on Ethernet 1/1.

因为流量在传出防火墙时执行 QoS，因此，您可以在防火墙执行完所有其他安全策略规则（包括网络地址转换 (NAT) 规则）后将您的 QoS 策略规则应用到流量。如果想根据源对流量执行 QoS，则必须在 QoS 策略规则中指定 NAT 后源地址（不得使用 NAT 前源地址）。

了解更多有关如何标识需要接受 QoS 处理的应用程序的传出接口。

## 针对明文与隧道通信的 QoS

要启用 QoS 接口，您至少需要选择默认的 QoS 配置文件规则，它为流出接口的明文通信定义了宽带和优先级设置。但是，如果您要设置或修改 QoS 接口，您可以将精细的 QoS 设置应用于外传明文通信和隧道通信。QoS 优先处理和带宽限制可以实施于独立的隧道通信和/或来自不同源接口和源子网的明文通信。对 Palo Alto Networks 防火墙来说，隧道流量指的是隧道接口流量，特别是隧道模式的 IPSec 流量。


© 2019 Palo Alto Networks, Inc.

# 配置 QoS

请遵循以下步骤配置服务质量（QoS），这包括创建 QoS 配置文件、创建 QoS 策略和在接口上启用 QoS。

STEP 1 | 标识需要使用 QoS 管理的流量。

该示例说明如何使用 QoS 来限制 Web 浏览。

选择 **ACC** 来查看 **Application Command Center**（应用程序命令中心）页面。使用 **ACC** 页面上的设置和图表查看与应用程序、URL 筛选、Threat Prevention、数据筛选和 HIP 匹配相关的动态和流量。

单击任何应用程序名称来显示详细的应用程序信息。

STEP 2 | 标识需要接收 QoS 处理的应用程序的出口接口。

流量的出口接口取决于通信流。如果正在加工传入流量，则出口接口是面向内部的接口。如果正在加工传出流量，那么出口接口是面向外部的接口。

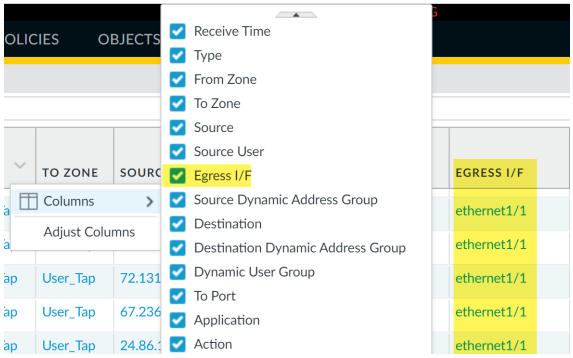
选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）来查看流量日志。

要筛选并且仅显示特定应用程序的日志：

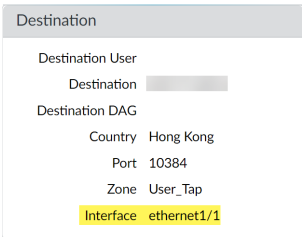
- 如果为应用程序显示条目，则单击“应用程序”列中带下划线的链接，然后单击“提交”图标 。
- 如果没有为应用程序显示条目，则单击“添加日志”图标，并且搜索应用程序 。

流量日志中的 **Egress I/F**（出口 **I/F**）显示每个应用程序的出口接口。要显示在默认情况下不显示的 **Egress I/F**（出口 **I/F**）列：

- 单击任何列标题以将列添加到日志：




- 单击任意条目左侧的小望远镜图标以显示详细的日志，该日志的“目标”部分中会列出应用程序的出口接口：




STEP 3 | 添加 QoS 策略规则。

QoS 策略规定义接收 QoS 处理的流量。防火墙将 QoS 服务类分配给与策略规则匹配的流量。



© 2019 Palo Alto Networks, Inc.

因为流量在传出防火墙时执行 *QoS*，因此，您可以在防火墙执行完所有其他安全策略规则（包括网络地址转换 *(NAT)* 规则）后将您的 *QoS* 策略规则应用到流量。如果想根据源对流量执行 *QoS*，则必须在 *QoS* 策略规则中指定 *NAT* 后源地址（不得使用 *NAT* 前源地址）。

1. 选择 **Policies**（策略）> **QoS**并 **Add**（添加）新的策略规则。
2. 在 **General**（常规）选项卡中，为 QoS 策略规则提供描述性的 **Name**（名称）。
3. 基于 **Source**（源）、**Destination**（目标）、**Application**（应用程序）、**Service/URL Category**（服务/**URL** 类别）和 **DSCP/ToS** 值（**DSCP/ToS** 设置允许您基于 DSCP 分类实施 QoS）指定要接收 QoS 处理的流量。

   例如，选择 **Application**（应用程序），单击 **Add**（添加），然后选择 **web-browsing**（**Web** 浏览），以将 QoS 应用于 Web 浏览流量。
4. （可选）继续定义其他参数。例如，选择 **Source**（源）并 **Add**（添加）**Source User**（源用户），以为特定用户的 Web 流量提供 QoS。
5. 选择 **Other Settings**（其他设置）并将 **QoS Class**（**QoS** 类）分配给匹配策略规则的流量。例如，将类 2 分配给 user1 的 Web 流量。
6. 单击 **OK**（确定）。

STEP 4 | 添加 QoS 配置文件规则。

QoS 配置文件规则让您能够定义流量可接收的包括优先级在内的 8 种服务类，并能够执行 QoS 带宽管理。

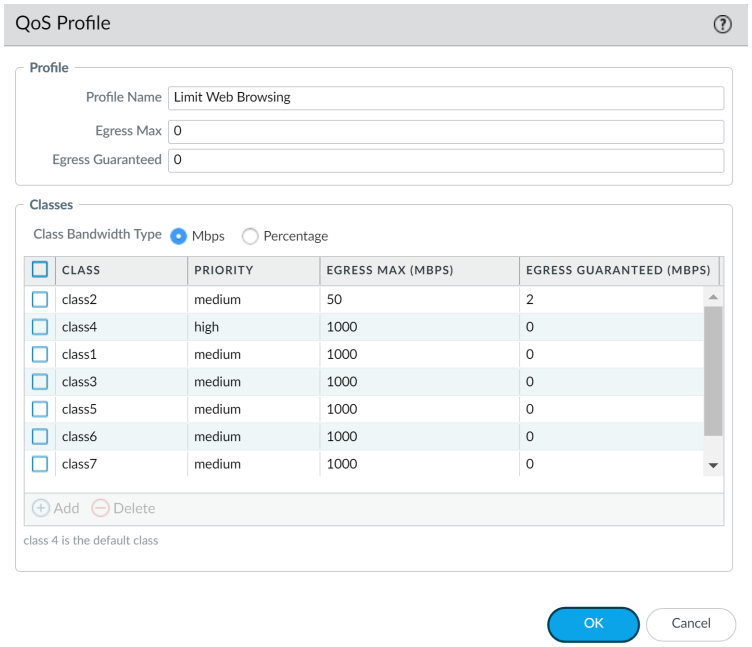
您可以通过单击 QoS 配置文件名称来编辑任何现有的 QoS 配置文件，包括默认的配置文件。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **QoS Profile**（**QoS** 配置文件）并 **Add**（添加）新的配置文件。
2. 输入描述性的 **Profile Name**（配置文件名称）。
3. 为配置文件规则设置 QoS 总宽带限制：
   - 输入**Egress Max**（最大出口）值来为 QoS 配置文件规则设置总体带宽分配。
   - 输入 **Egress Guaranteed**（出口保证）值来为 QoS 配置文件设置保证带宽。

   任何超过出口保证值的流量都会得到尽可能地处理，但是并不保证效果。保证带宽如不使用，将继续对所有流量保持可用状态。
4. 在类部分中，指定如何处理单独的 QoS 类（最多 8 个）：
   1. 将类 **Add**（添加）到 QoS 配置文件。
   2. 为类选择 **Priority**（优先级）：实时、高、中或低。
   3. 为分配给每个 QoS 类的流量输入 **Egress Max**（最大出口）和 **Egress Guaranteed**（出口保证）带宽。
5. 单击 **OK**（确定）。

在下列示例中，QoS 配置文件“限制 Web 浏览”将类 2 流量的流量的最大带宽限制为 50 Mbps，并且将其保证带宽限制为 2 Mbps。


© 2019 Palo Alto Networks, Inc.




STEP 5 | 在物理接口上启用 QoS。

此步骤部分包括为唯一的 QoS 处理选择明文通信和隧道通信的选项。

检查您正在使用的防火墙型号是否支持在子接口上启用 *QoS*，方法是查看产品规格的摘要。

1. 选择 **Network**（网络）> **QoS** 并 **Add**（添加）QoS 接口。
2. 选择 **Physical Interface**（物理接口）并选择要启用 QoS 的接口的 **Interface Name**（接口名称）。

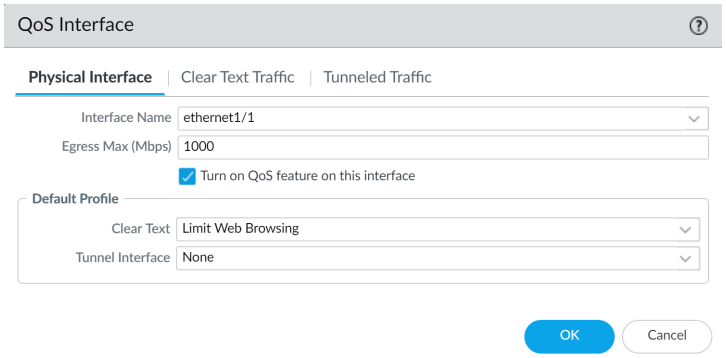
   在本示例中，Web 浏览流量的出口接口是 Ethernet 1/1（请参阅步骤 2）。
3. 为流出此接口的所有流量设置 **Egress Max**（最大出口）带宽。

   最佳实践是始终为 *QoS* 接口定义最大出口值。确保针对附加到接口的 *QoS* 配置文件规则的累计保证带宽不会超过分配给接口的总带宽。
4. 选择 **Turn on QoS feature on this interface**（为此接口启用 **QoS** 功能）。
5. 在“默认配置文件”部分中，选择 QoS 配置文件规则以应用于流出物理接口的所有 **Clear Text**（明文）通信。
6. （可选）选择默认的 QoS 配置文件规则以应用于流出接口的所有隧道通信。

例如，在 Ethernet 1/1 上启用 QoS，应用为 QoS 配置文件“限制 Web 浏览”（步骤 4）定义的带宽和优先级设置，以作为明文出口通信的默认设置。



© 2019 Palo Alto Networks, Inc.




1. （可选）继续定义更精细的设置，提供针对明文与隧道通信的 QoS。在 **Clear Text Traffic**（明文通信）选项卡和 **Tunneled Traffic**（隧道通信）选项卡上配置的设置将自动覆盖“物理接口”选项卡上的针对明文通信和隧道通信的默认配置文件设置。
   - 选择 **Clear Text Traffic**（明文通信），然后：
     - 为明文流量设置 **Egress Guaranteed**（出口保证）和 **Egress Max**（最大出口）带宽。
     - 单击 **Add**（添加）并应用 QoS 配置文件规则以基于源接口和源子网实施明文通信。
   - 选择 **Tunneled Traffic**（隧道通信），然后：
     - 为隧道流量设置 **Egress Guaranteed**（出口保证）和 **Egress Max**（最大出口）带宽。
     - 单击 **Add**（添加）并附加 QoS 配置文件规则到单一隧道接口。
2. 单击 **OK**（确定）。

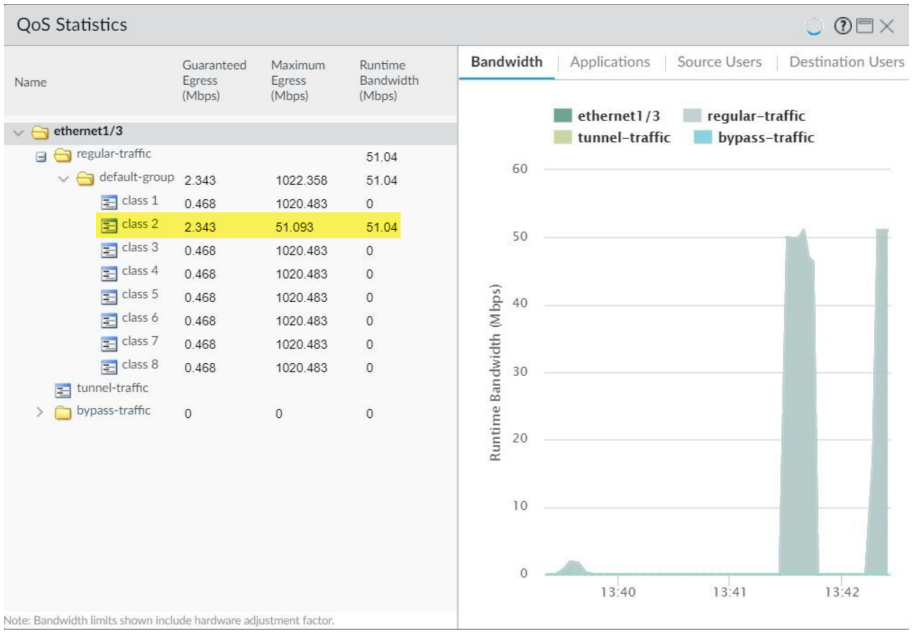
STEP 6 | 提交更改。

单击 **Commit**（提交）。

STEP 7 | 验证 QoS 配置。

选择 **Network**（网络）> **QoS**，然后选择 **Statistics**（统计信息）以查看 QoS 带宽、所选 QoS 类的活动会话和所选 QoS 类的活动应用程序。

例如，可查看启用 QoS 的 Ethernet 1/3 的统计信息：






© 2019 Palo Alto Networks, Inc.

类 2 流量的保证带宽限制为 2.343 Mbps，最大带宽限制为 51.093 Mbps。

继续单击选项卡，以显示有关应用程序、源用户、目标用户、安全规则以及 QoS 规则的更多信息。



*QoS Statistics*（*QoS* 统计信息）窗口上会显示带宽限制，其中包括硬件调整因素。



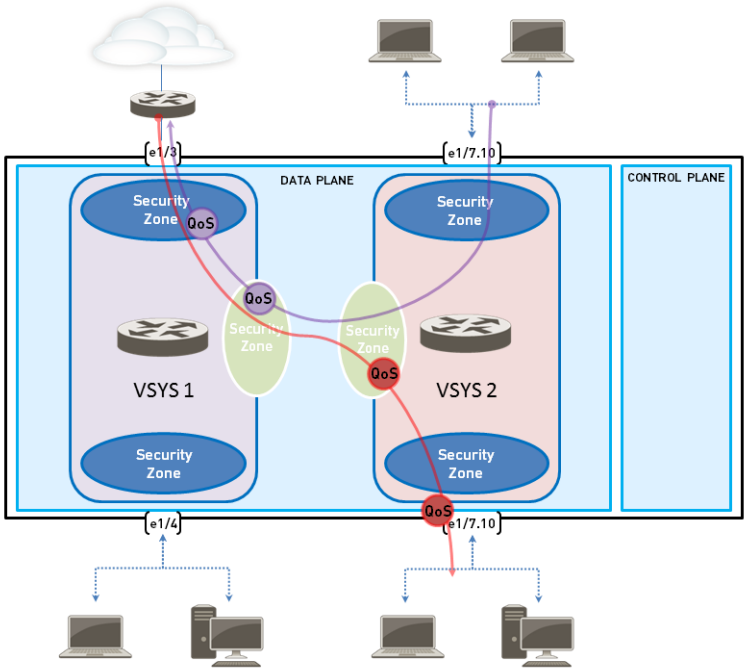
© 2019 Palo Alto Networks, Inc.

# 为虚拟系统配置 QoS

可以为单个或多个配置在 Palo Alto Networks 防火墙上的虚拟系统配置 QoS。因为虚拟系统是独立的防火墙，所以必须单独为单个虚拟系统配置 QoS。

为虚拟系统配置 QoS 类似于在物理防火墙上配置 QoS，不同之处是为虚拟系统配置 QoS 需要指定流量的源和目标。由于虚拟系统可以脱离物理边界存在，并且虚拟环境中的流量可以跨越多个虚拟系统，因此为单一虚拟系统控制和加工流量必须要求为流量指定源和目标区域和接口。

下列示例展示在防火墙中配置的两个虚拟系统。VSYS 1（紫色）和 VSYS 2（红色）都配置了 QoS 以确定两个不同的通信流的优先级，或者对这两个通信流进行限制，这通过相应的紫色 (VSYS 1) 和红色 (VSYS 2) 行表示。QoS 节点指示了流量中匹配 QoS 策略并分配了 QoS 服务类的点，随后指示了当流量出口防火墙时被加工的点。




有关虚拟系统以及配置方式的信息，请参阅虚拟系统。

STEP 1 | 配置与每个虚拟系统相关联的适当接口、虚拟路由器和安全区域。

- 要查看配置的接口，可选择 **Network**（网络）> **Interface**（接口）。
- 要查看配置的区域，可选择 **Network**（网络）> **Zones**（区域）。
- 要查看有关定义的虚拟路由器的信息，可选择 **Network**（网络）> **Virtual Routers**（虚拟路由器）。

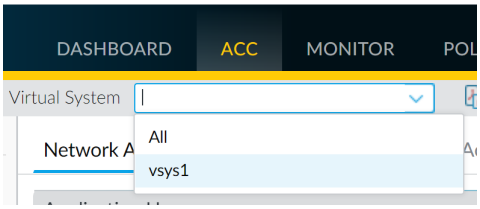
STEP 2 | 识别要应用 QoS 的流量。

选择 **ACC** 来查看 **Application Command Center**（应用程序命令中心）页面。使用 **ACC** 页面上的设置和图表查看与应用程序、URL 筛选、Threat Prevention、数据筛选和 HIP 匹配相关的动态和流量。

要为指定的虚拟系统查看信息，从 **Virtual System**（虚拟系统）下拉中选择该虚拟系统：



© 2019 Palo Alto Networks, Inc.




单击任何应用程序名称来显示详细的应用程序信息。

STEP 3 | 标识已经识别为需要 QoS 处理的应用程序的出口接口。

在虚拟系统环境中，QoS 会应用到虚拟系统上的流量的出口点上的流量。根据虚拟系统的配置和 QoS策略，QoS 流量的出口点可以与物理接口关联或可以是一个区域。

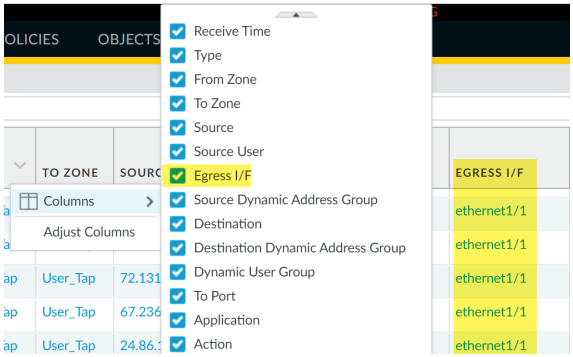
该示例说明如何限制 vsys 1 上的 Web 浏览流量。

选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）来查看流量日志。每个条目都可以显示包含在虚拟系统环境中配置 QoS 所必需的信息的列：

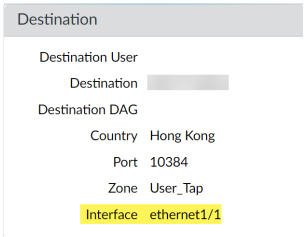
- 虚拟系统
- 出口接口
- 入口接口
- 源区域
- 目标区域

要显示在默认情况下不显示的列：

- 单击任何列标题以将列添加到日志：




- 单击任意条目左侧的小望远镜图标以显示详细的日志，该日志的 **Source**（源）和 **Destination**（目标）部分中会列出应用程序的出口接口，以及源区域和目标区域：




例如，对于来自 VSYS 1 的 Web 浏览流量，入口接口为 Ethernet 1/2，出口接口为 Ethernet 1/1，源区域为信任，目标区域为不信任。

STEP 4 | 创建 QoS 配置文件。

可以通过单击配置文件名称来编辑任何现有的 QoS 配置文件，包括默认的配置文件。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **QoS Profile**（**QoS** 配置文件），然后单击 **Add**（添加）以打开“QoS 配置文件”对话框。
2. 输入描述性的 **Profile Name**（配置文件名称）。
3. 输入 **Egress Max**（最大出口）来为 QoS 配置文件设置总体带宽分配。
4. 输入 **Egress Guaranteed**（出口保证）来为 QoS 配置文件设置保证带宽。

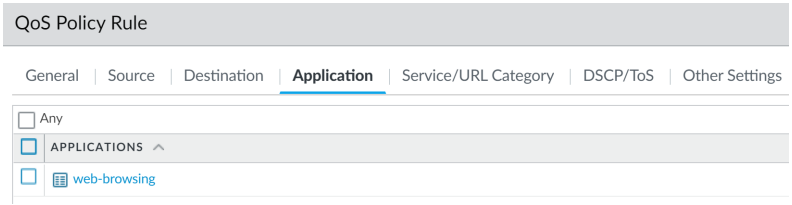
   任何超过 *QoS* 配置文件的出口保证限制的流量都会得到尽可能地处理，但是并不保证效果。
5. 在 **QoS Profile**（**QoS** 配置文件）的“类”部分中，指定如何处理单独的 QoS 类（最多 8 个）：
   1. 单击 **Add**（添加）来将类添加到 QoS 配置文件。
   2. 选择类的 **Priority**（优先级）。
   3. 为类输入 **Egress Max**（最大出口）来为这个单独的类设置总体带宽限制。
   4. 为类输入 **Egress Guaranteed**（出口保证）来为这个单独的类设置保证带宽。
6. 单击 **OK**（确定）以保存 QoS 配置文件。

STEP 5 | 创建 QoS 策略。

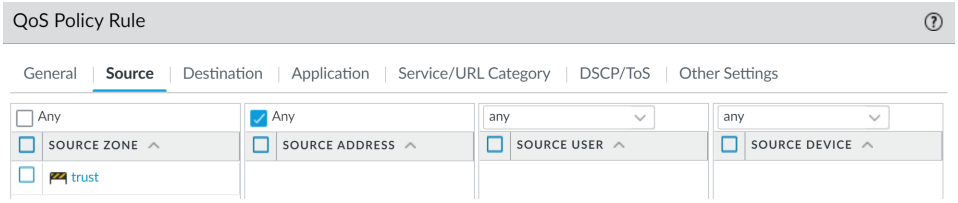
在多虚拟系统环境下，流量跨越多个虚拟系统。正因如此，如果您为一个虚拟系统启用 QoS，您必须基于源和目标区域定义接受 QoS 处理的流量。此操作确保仅为该虚拟系统确定流量优先级和进行流量加工（但不包括其他流量可能流经的虚拟系统）。

1. 选择 **Policies**（策略）> **QoS**并 **Add**（添加）QoS 策略规则。
2. 选择 **General**（常规），为 QoS 策略规则提供描述性的 **Name**（名称）。
3. 指定要应用 QoS 策略规则的流量。使用 **Source**（源）、**Destination**（目标）、**Application**（应用程序）和 **Service/URL Category**（服务/URL 类别）选项卡来定义用于识别流量的匹配参数。

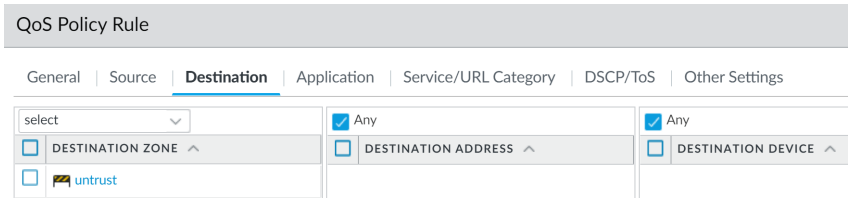
   例如，选择 **Application**（应用程序）并单击 **Add**（添加）Web 浏览，以将 QoS 策略规则应用到该应用程序：




4. 选择 **Source**（源）并 **Add**（添加）vsys 1 网络浏览流量的源区域。

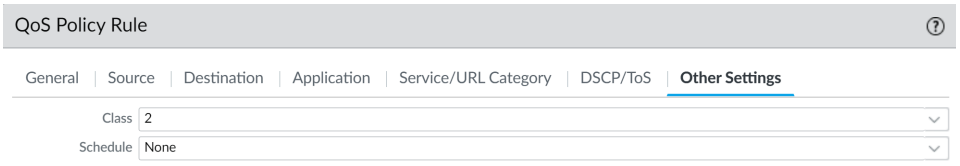



5. 选择 **Destination**（目标）并 **Add**（添加）vsys 1 网络浏览流量的目标区域。




6. 在 **Other Settings**（其他设置）选项卡中，选择要分配给 QoS 策略规则的 **QoS Class**（**QoS** 类）。例如，将类 2 分配给 vsys 1 上的 Web 浏览流量：


© 2019 Palo Alto Networks, Inc.



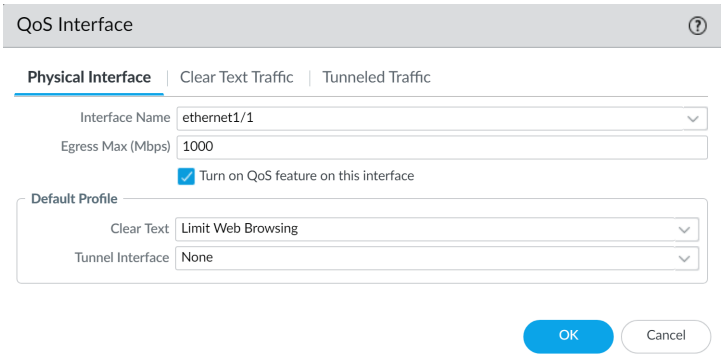

7. 单击 **OK**（确定）以保存 QoS 策略规则。

STEP 6 | 在物理接口上启用 QoS 配置文件。

最佳实践是始终为 *QoS* 接口定义 *Egress Max*（最大出口）值。

1. 选择 **Network**（网络）> **QoS**，然后单击 **Add**（添加）来打开“QoS 接口”对话框。
2. 在物理接口上启用 QoS：
   1. 在 **Physical Interface**（物理接口）选项卡中，选择要应用 QoS 配置文件的接口的 **Interface Name**（接口名称）。

      在本示例中，vsys 1 上的 Web 浏览流量的入口接口是 Ethernet 1/1（请参阅步骤 2）。




   2. 选择 **Turn on QoS feature on this interface**（为此接口启用 **QoS** 功能）。
3. 在 **Physical Interface**（物理接口）选项卡中，选择应用到所有 **Clear Text**（明文）流量的默认 QoS 配置文件。

   （可选）使用 **Tunnel Interface**（隧道接口）字段将默认 QoS 配置文件应用到所有隧道流量。
4. （可选）在 **Clear Text Traffic**（明文流量）选项卡中，为明文流量配置其他 QoS 设置：
   - 为明文流量设置 **Egress Guaranteed**（出口保证）和 **Egress Max**（最大出口）带宽。
   - 单击 **Add**（添加）将 QoS 配置文件应用到所选的明文流量，然后根据源接口和源子网为 QoS 处理选择流量（创建 QoS 节点）。
5. （可选）在 **Tunneled Traffic**（隧道流量）选项卡上，为隧道接口配置其他 QoS 设置：
   - 为隧道流量设置 **Egress Guaranteed**（出口保证）和 **Egress Max**（最大出口）带宽。
   - 单击 **Add**（添加）将所选隧道接口与 QoS 配置文件相关联。
6. 单击 **OK**（确定）以保存更改。
7. **Commit**（提交）更改。

STEP 7 | 验证 QoS 配置。

- 选择 **Network**（网络）> **QoS** 来查看“QoS 策略”页面。**QoS Policies**（**QoS** 策略）页面验证是否启用 QoS，并且包括 **Statistics**（统计信息）链接。单击统计信息链接查看 QoS 带宽、所选 QoS 节点或类的活动会话，以及所选 QoS 节点或类的活动应用程序。



© 2019 Palo Alto Networks, Inc.

- 在多 VSYS 环境中，会话不能跨越多个系统。如果流量通过多个虚拟系统，那么可以为一个通信流创建多个会话。要浏览在防火墙上运行的会话，以及查看应用的 QoS 规则和 QoS 类，可选择 **Monitor**（监控）> **Session Browser**（会话浏览器）。


© 2019 Palo Alto Networks, Inc.

# 基于 DSCP 分类实施 QoS

差分服务代码点 (DSCP) 是一个可用于为通信请求（例如）高优先级或尽可能地分发的数据包标头值。基于会话的 DSCP 分类让您能够确定传入流量的 DSCP 值，并让您能够在会话流量流出防火墙时用 DSCP 值标记会话。这让所有会话入站和出站流量流经您的网络时，都可以接受连续的 QoS 处理。例如，现在可以用防火墙基于其在会话开始时检测到 DSCP 值初始为入站流实施的 QoS 优先级来处理来自外部服务器的入站返回流量。防火墙与终端用户之间的网络设备也可以用相同的优先级处理返回流量（以及该会话的任意出站和入站流量）。

不同类型的 DSCP 标记表示不同层次的服务：

完成此步骤，使得防火墙能够用会话开始时监测到的同一 DSCP 值标记流量（在此示例中，防火墙将用 DSCP AF11 值标记返回流量）。配置 QoS 可让您在流量 egress 防火墙时对其进行加工，同时，在安全规则中启用该选项可让其他网络设备充当防火墙和客户端之间的媒介，以继续实施为 DSCP 标记流量设定的优先级。

- **Expedited Forwarding (EF)**（加速转发 **(EF)**）：可以用来为流量请求低泄露、低延迟并保证带宽。带有 EF 代码点值的数据包通常保证获得最高优先级分发。
- **Assured Forwarding (AF)**（确保转发 **(AF)**）：可以用来为应用程序提供可靠的分发。带有 AF 代码点的数据包表示流量请求接受比尽可能服务提供的优先级更高级别的处理（虽然带有 EF 代码点的数据包将仍然优先于带有 AF 代码点的数据包）。
- **Class Selector (CS)**（类选择器 **(CS)**）：可以用来为使用 IP 优先级字段标记优先流量的网络设备提供向后兼容性。
- **IP Precedence (ToS)**（**IP** 优先级 **(ToS)**）：可以为传统网络设备标记优先流量（IP 优先级标题字段用来为 DSCP 分类介绍之前的数据包表示优先级）。
- **Custom Codepoint**（自定义代码点）：通过输入 **Codepoint Name**（代码点名称）和 **Binary Value**（二进制值）来创建自定义代码点，以匹配到流量。

例如，选择 **Assured Forwarding (AF)**（确保转发 **(AF)**）确保由 AF 代码点值标记的流量在标记接收低优先级的应用程序上拥有较高优先级来得到可靠分发。使用以下步骤实现基于会话的 DSCP 分类。从配置在会话开始时侦测到的基于 DSCP 标记的 QoS 开始。接下来，使用与为初始出站流实施 QoS 相同的 DSCP 值，您可以继续为会话启用防火墙标记返回流。

STEP 1 | 执行配置 QoS 的初步步骤。

STEP 2 | 定义流量以基于 DSCP 值接受 QoS 处理。

1. 选择 **Policies**（策略）> **QoS** 并 **Add**（添加）或修改现有 QoS 规则，填充必填字段。
2. 选择 **DSCP/ToS** 并选择 **Codepoints**（代码点）。
3. **Add**（添加）为其要实施 QoS 的 DSCP/ToS 代码点。
4. 为 QoS 规则选择 DSCP/ToS 标记 **Type**（类型）以匹配流量：

   最佳实践是使用单个 *DSCP* 类型来管理和确定网络流量的优先级。

5. 通过指定 **Codepoint**（代码点）值在更精细的范围内将 QoS 策略匹配到流量。例如，为策略匹配选择确保转发 (AF) 作为 DSCP 值的 **Type**（类型），进一步指定 AF **Codepoint**（代码点）值，例如 AF11。

   如果选择加速转发 *(EF)* 作为 *DSCP* 标记的 *Type*（类型），不能指定精细的 *Codepoint*（代码点）值。*QoS* 策略规则将匹配至用任意 *EF* 代码点值标记的流量。

6. 选择 **Other Settings**（其他设置），然后将 **QoS Class**（**QoS** 类）分配给匹配 QoS 规则的流量。在本示例中，如果会话中的第一个数据包监测到值为 AF11 的 DSCP 标记，将类 1 分配给该会话。
7. 单击 **OK**（确定）以保存 QoS 规则。



© 2019 Palo Alto Networks, Inc.

STEP 3 | QoS 规则基于会话开始时监测到的 DSCP 标记，如果流量与之匹配，则为该流量定义接收的 QoS 优先级。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **QoS Profile**（**QoS** 配置文件）并 **Add**（添加）或修改现有 QoS 配置文件。关于配置文件设置选项和流量带宽的详细信息，请参阅 QoS 概念和配置 QoS。
2. **Add**（添加）或修改配置文件类。例如，由于步骤 2 展示了将 AF11 流量分类为类 1 流量的步骤，您可以添加或修改 **class1** 条目。
3. 为流量的类选择 **Priority**（优先级），例如 **high**（高）。
4. 单击 **OK**（确定）以保存 QoS 配置文件。

STEP 4 | 在接口上启用 QoS。

选择 **Network**（网络）> **QoS**并 **Add**（添加）或修改现有接口，然后 **Turn on QoS feature on this interface**（为此接口启用 **QoS** 功能）。

在此示例中，带有 AF11 DSCP 标记的流量与 QoS 规则匹配并分配到类 1。当类 1 流量流出防火墙时，此接口上启用的 QoS 配置文件实施高优先级处理（会话出站流量）。

STEP 5 | 启用 DSCP 标记。

用 DSCP 值标记返回流量，使得会话的入站流能够被标记为出站流监测到的同一 DSCP 值。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）或修改安全策略。
2. 选择 **Actions**（操作），在 **QoS Marking**（**QoS** 标记）下拉列表中选择 **Follow-Client-to-Server-Flow**（跟踪客户端至服务器的流）。
3. 单击 **OK**（确定）保存更改。

完成此步骤，使得防火墙能够用会话开始时监测到的同一 DSCP 值标记流量（在此示例中，防火墙将用 DSCP AF11 值标记返回流量）。配置 QoS 可让您在流量 egress 防火墙时对其进行加工，同时，在安全规则中启用该选项可让其他网络设备充当防火墙和客户端之间的媒介，以继续实施为 DSCP 标记流量设定的优先级。

STEP 6 | 提交配置。

**Commit**（提交）更改。


© 2019 Palo Alto Networks, Inc.

# QoS 用例

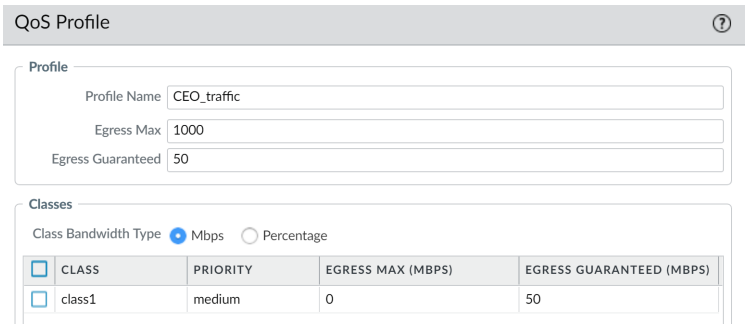
以下用例说明如何在常见情况下使用 QoS：

- 用例：单个用户的 QoS
- 用例：语音和视频应用程序的 QoS

## 用例：单个用户的 QoS

CEO 发现在网络用量较高时，无法访问有效响应关键业务通信的企业应用程序。IT 管理员希望确保相对于其他员工流量而言，所有进出 CEO 的流量都能得到优先处理，从而保证 CEO 能够访问并高效处理关键网络资源。

STEP 1 | 管理员创建 QoS 配置文件 ***CEO_traffic***，以定义由 CEO 发出的流量在公司网络之外流动时，如何对其进行处理和加工：

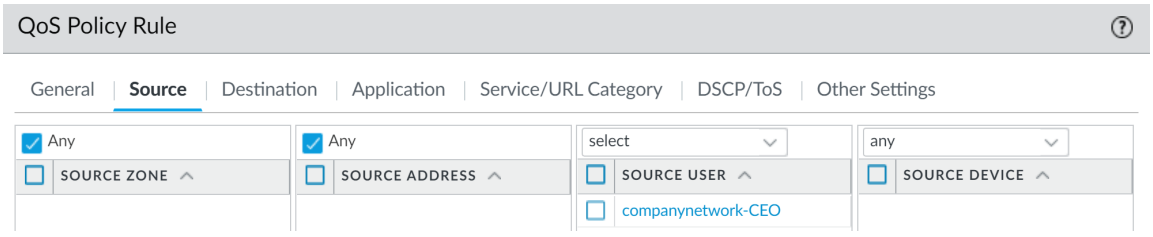



管理员分配 50 Mbps 的保证带宽（**Egress Guaranteed**（出口保证）），以确保 CEO 始终具有保证为其分配的带宽量（超过其需要的带宽量），而不用考虑网络拥挤。

管理员继续将类 1 流量指定为高优先级，并且将配置文件的最大带宽用量（**Egress Max**（最大出口））设置为 1000 Mbps，并且为管理员将要启用 QoS 的接口设置相同的最大带宽。管理员在任何情况下都不会限制 CEO 的带宽用量。

最佳实践是填充 *QoS* 配置文件的 *Egress Max*（最大出口）字段，即使配置文件的最大带宽与接口的最大带宽相匹配。*QoS* 配置文件的最大带宽始终不应该超过计划启用 *QoS* 的接口的最大带宽。

STEP 2 | 管理员创建 QoS 策略以识别 CEO 的流量（**Policies**（策略）> **QoS**），并为其分配在 QoS 配置文件中定义的类（请参阅上一步操作）。因为已配置 User-ID，所以管理员使用 QoS 策略中的 **Source**（源）选项卡来通过 CEO 的公司网络用户名单独识别 CEO 的流量。（如果未配置 User-ID，则管理员可以在 **Source Address**（源地址）之下 **Add**（添加）CEO 的 IP 地址。请参阅 User-ID。）：




管理员将 CEO 的流量与类 1 相关联（**Other Settings**（其他设置）选项卡），然后继续填充剩余的所需策略字段；管理员为策略提供描述性的 **Name**（名称）（**General**（常规）选项卡），并且为 **Source**

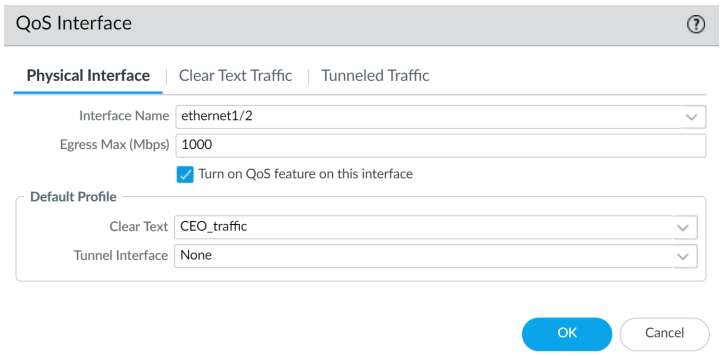


© 2019 Palo Alto Networks, Inc.

**Zone**（源）区域（**Source**（源）选项卡）和 **Destination Zone**（目标）区域（**Destination**（目标）选项卡）选择 **Any**（任意）：

| | NAME | TAGS | Source | | | | Destination | | | APPLICATION | SERVICE | DSCP/TOS | CLASS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | | |
| 1 | HTTPS | none | trust | any | any | any | untrust | any | any | web-browsing | any | any | 2 |
| 2 | Voice-Video | none | any | any | any | any | any | any | any | voip-video-l... | any | any | 1 |
| 3 | Guarantee CEO bandwidth | none | any | any | companynet... | any | any | any | any | any | any | any | 1 |

STEP 3 | 现在类 1 与 CEO 的流量相关联，管理员可以启用 QoS，方法是选中 **Turn on QoS feature on interface**（为接口启用 **QoS** 功能）并且选择通信流的出口接口。CEO 的通信流的出口接口是面向外部的接口，在本示例中为 Ethernet 1/2：



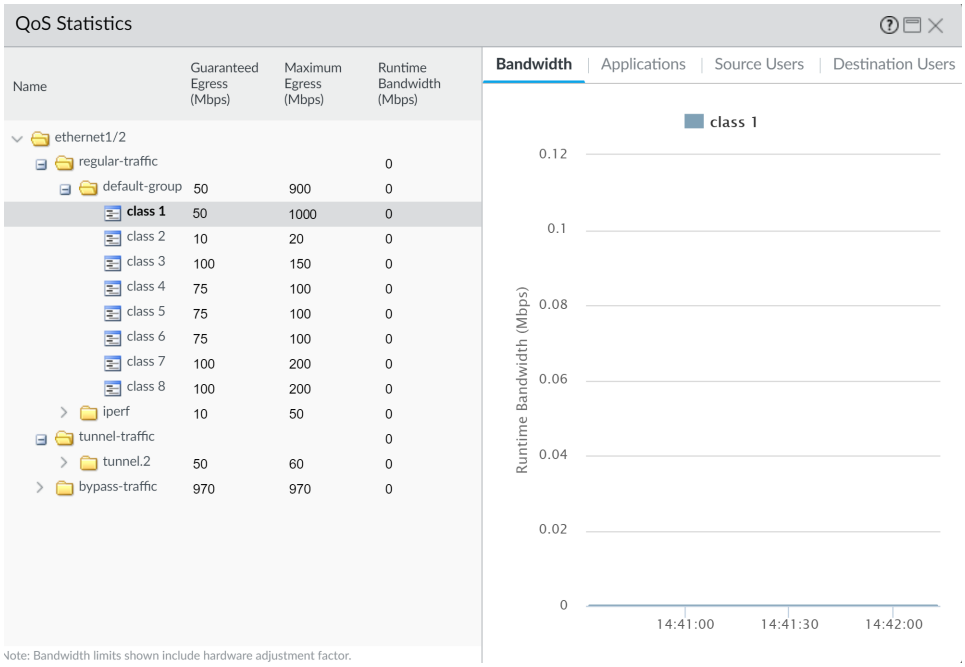

因为管理员希望通过自己创建的 QoS 配置文件及其关联的 QoS 策略来保证所有来自 CEO 的流量，所以选择将 *CEO_traffic* 应用到来自 Ethernet 1/2 的 **Clear Text**（明文）流量。

STEP 4 | 提交 QoS 配置之后，管理员会导航到 **Network**（网络）> **QoS** 页面，以确认是否已在面向外部的接口（即 ethernet 1/2）上启用 QoS 配置文件 CEO_traffic：

| NAME | GUARANTEED EGRESS (MBPS) | MAXIMUM EGRESS (MBPS) | PROFILE | ENABLED | |
|---|---|---|---|---|---|
| ethernet1/2 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 50.000 | | CEO_traffic | | |

STEP 5 | 单击 **Statistics**（统计信息），以查看当源自 CEO（类 1）的流量从 Ethernet 1/2 流出时，如何对其进行加工：


© 2019 Palo Alto Networks, Inc.




本示例说明如何将 *QoS* 应用到源自单个源用户的流量。但是，如果要保证或加工目标用户的流量，则可以进行类似的 *QoS* 设置。相反（或者除了该工作流程之外），可以创建 *QoS* 策略，以在 *Policies*（策略）> *QoS* 页面上将用户的 *IP* 地址指定为 *Destination Address*（目标地址）（而不是指定用户的源信息），然后在 *Network*（网络）> *QoS* 页面上对网络的面向内部的接口启用 *QoS*（而不是对面向外部的接口启用）。

## 用例：语音和视频应用程序的 QoS

语音和视频流量对由 QoS 功能加工和控制的测量（尤其是延迟和抖动）特别敏感。为了以语音方式清晰地传输语音和视频，必须采用一致的方式来丢弃、延迟或交付语音和视频数据包。除了保证带宽之外，对于语音和视频应用程序的最佳处理方法是保证语音和视频流量的优先级。

在本示例中，公司分支机构的员工难以使用视频会议和 IP 语音 (VoIP) 技术来与其他分支机构、合作伙伴和客户进行业务通信，而且对此种方式并不信任。IT 管理员尝试实施 QoS 来处理这些问题，并且确保分支机构的员工的业务通信有效且可靠。因为管理员希望同时保证传入和传出网络通信的 QoS，所以需要同时在防火墙的面向内部和面向外部的接口上启用 QoS。

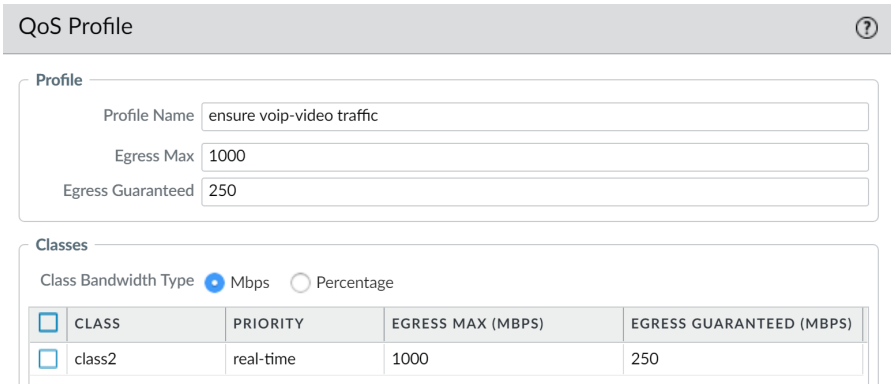
STEP 1 | 管理员创建 QoS 配置文件，并且定义类 2，这样类 2 流量将接收到实时优先级，并且在具有 1000 Mbps 的最大带宽的接口上，始终保证带宽为 250 Mbps，包括网络用量的峰值期。

通常建议受延迟影响的应用程序使用实时优先级，此优先级在保证语音和视频应用程序的效果和质量时特别有用。

在防火墙 Web 界面上，管理员选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Qos Profile**（**QoS** 配置文件）页面，单击 **Add**（添加），输入 **Profile Name**（配置文件名称） ensure voip-video traffic，并定义类 2 流量。

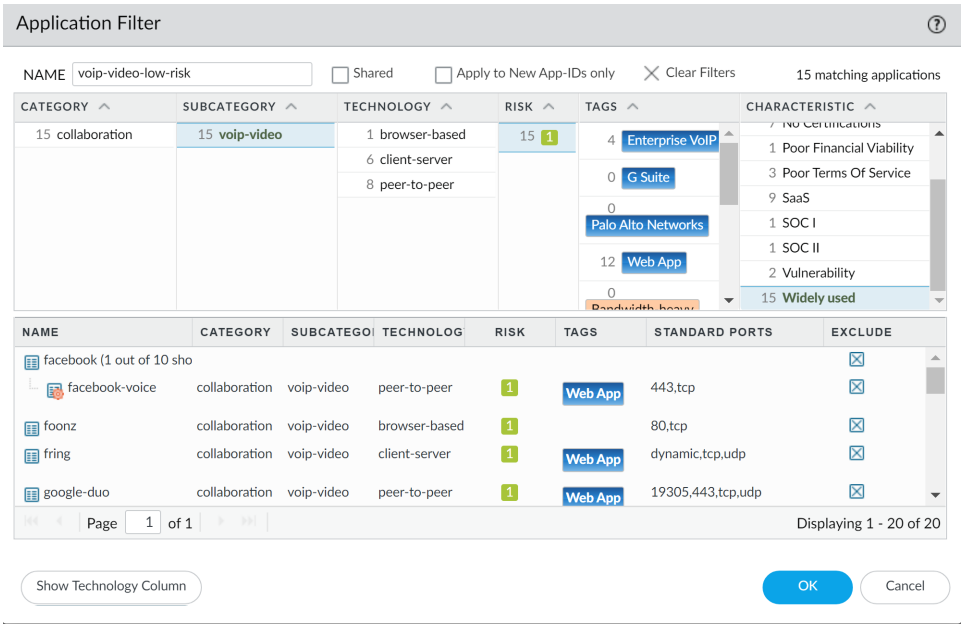


© 2019 Palo Alto Networks, Inc.

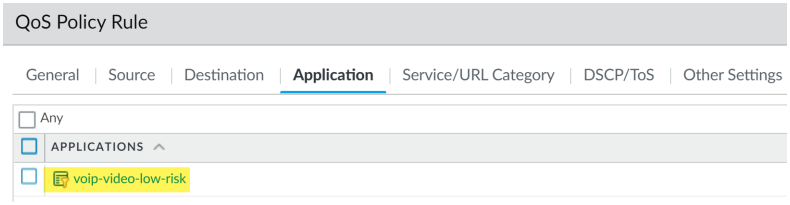



STEP 2 | 管理员创建 QoS 策略以识别语音和视频流量。因为公司没有一个标准的语音和视频应用程序，所以管理员希望确保将 QoS 应用到一些特定的应用程序（员工会定期地广泛使用这些应用程序与其他办公室、合作伙伴以及客户通信）。在 **Policies**（策略）> **QoS** > **QoS Policy Rule**（**QoS** 策略规则）> **Applications**（应用程序）选项卡上，管理员单击 **Add**（添加），并打开 **Application Filter**（应用程序筛选器）窗口。管理员继续选择筛选要应用 QoS 的应用程序的条件、选择子类别 voip-video，并且通过仅指定风险低、使用广泛的网络视频应用程序来缩小筛选的范围。

应用程序筛选器是动态工具，在用于筛选 QoS 策略中的应用程序时，可以在任何特定时间将 QoS 应用到所有满足 voip-video、low risk 和 widely used 条件的应用程序。




管理员将 **Application Filter**（应用程序筛选器）命名为 voip-video-low-risk，并且将其包含在 QoS 策略中：





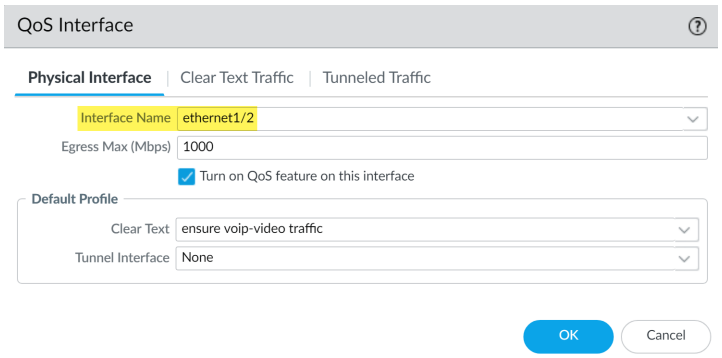
© 2019 Palo Alto Networks, Inc.

管理员将 QoS 策略命名为 Voice-Video，并选择“Other Settings（其他设置）”以分配所有匹配策略类 2 的流量。接下来他会将 Voice-Video QoS 策略用于传入和传出 QoS 流量，因此将 **Source**（源）和 **Destination**（目标）信息设置为 **Any**（任意）：

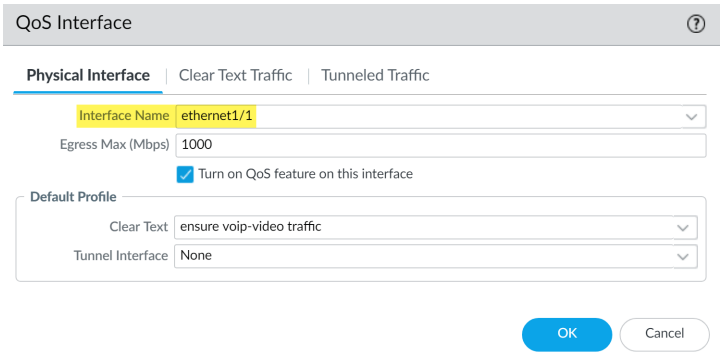
| | NAME | TAGS | Source | | | | Destination | | | APPLICATION | SERVICE | DSCP/TOS | CLASS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | | |
| 1 | HTTPS | none | trust | any | any | any | untrust | any | any | web-browsing | any | any | 2 |
| 2 | Voice-Video | none | any | any | any | any | any | any | any | voip-video-l... | any | any | 1 |

STEP 3 | 因为管理员希望确保将 QoS 用于传入和传出的语音和视频通信，所以将 QoS 应用到网络的面向外部的接口（将 QoS 应用到传出通信）以及面向内部的接口（将 QoS 应用到传入通信）。

管理员首先在面向外部的接口（本示例中为 ethernet 1/2）上启用创建的 QoS 配置文件 ensure voice-video traffic（该配置文件中的类 2 与策略 Voice-Video 相关联）。




然后在另一个接口即面向内部的接口（本示例中为 Ethernet 1/1）上启用相同的 QoS 配置文件 ensure voip-video traffic。




STEP 4 | 管理员选择 **Network**（网络）> **QoS** 以确认是否为传入和传出的语音和视频流量启用 QoS：

| NAME | GUARANTEED EGRESS (MBPS) | MAXIMUM EGRESS (MBPS) | PROFILE | ENABLED | |
|---|---|---|---|---|---|
| ethernet1/1 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 250.000 | | ensure voip-video traffic | | |
| ethernet1/2 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 250.000 | | ensure voip-video traffic | | |

管理员已成功在网络的面向内部和面向外部的接口上启用 QoS。现在可以确保为流入和流出网络的语音和视频应用程序流量启用实时优先级，从而确保可以可靠且有效地使用这些对延迟和抖动特别敏感的通信，以执行内部和外部业务通信。

# VPN

通过虚拟专用网络 (VPN) 创建隧道可让用户/系统在公共网络上安全地进行连接，如同在局域网 (LAN) 上进行连接。要建立 VPN 隧道，需要两台可以相互进行身份验证的设备，并且能够加密它们之间的信息流。此类设备可以是两个 Palo Alto Networks 防火墙，或是一个 Palo Alto Networks 防火墙和一个其他供应商提供的具备 VPN 功能的设备。


> VPN 部署
> 站点到站点 VPN 概述
> 站点到站点 VPN 概念
> 设置站点到站点 VPN
> 站点到站点 VPN 快速配置

# VPN 部署

Palo Alto Networks 防火墙支持以下 VPN 部署：

- 站点到站点 **VPN** — 连接中心站点和远程站点的简单 VPN，或者连接中心站点和多个远程站点的星型 VPN。防火墙使用 IP 安全 (IPSec) 协议组为两个站点之间的流量建立安全隧道。请参阅站点到站点 VPN 概述。
- 远程用户到站点 **VPN** — 使用 GlobalProtect 代理允许远程用户通过防火墙建立安全连接的解决方案。此解决方案使用 SSL 和 IPSec 在用户和站点之间建立安全连接。请参阅《GlobalProtect 管理员指南》。
- 大规模 **VPN** — Palo Alto Networks GlobalProtect 大规模 VPN (LSVPN) 提供了在最多 1,024 个卫星办公室部署可扩展星型 VPN 的简化机制。该解决方案需要在每个中心和每个星型拓扑中对 Palo Alto Networks 防火墙进行解密。它使用证书对设备进行身份验证、使用 SSL 在所有组件之间进行安全通信并使用 IPSec 保护数据。请参阅大规模 VPN (LSVPN)。

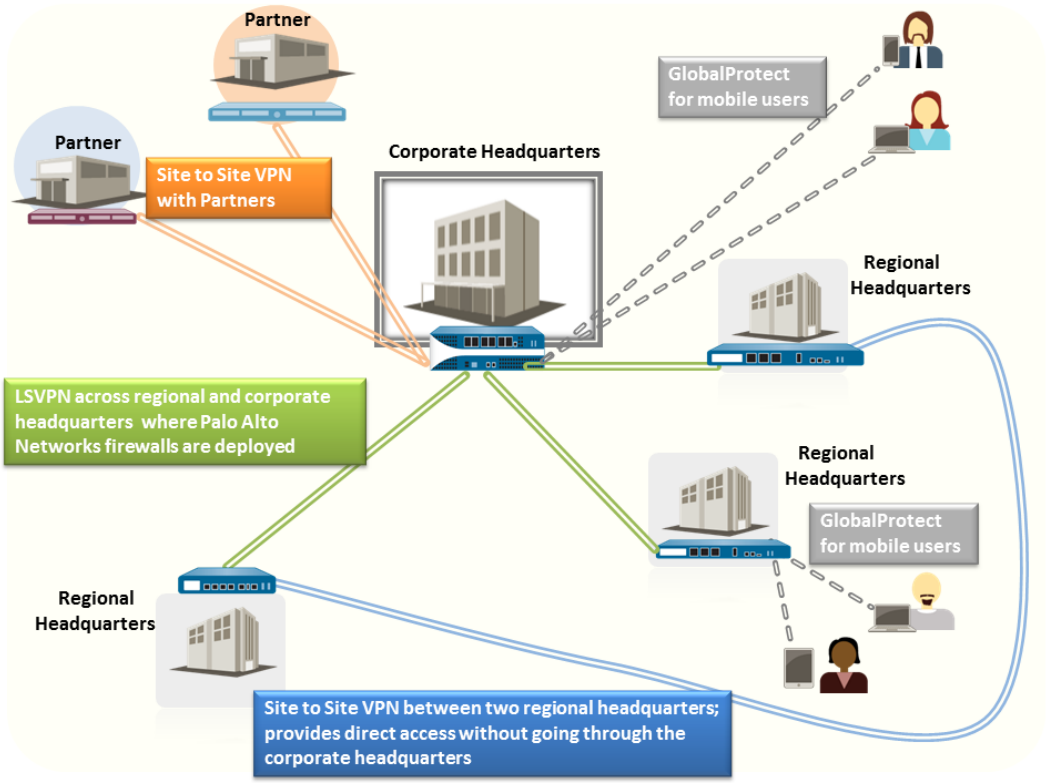



图 8: VPN 部署



© 2019 Palo Alto Networks, Inc.

# 站点到站点 VPN 概述

可让您连接两个局域网 (LAN) 的 VPN 连接称为站点到站点 VPN。您可以配置基于路由的 VPN，以连接位于两个站点的 Palo Alto Networks 防火墙，或者将 Palo Alto Networks 防火墙与其他位置的第三方安全设备进行连接。防火墙还可以与基于第三方的 VPN 设备进行互操作；Palo Alto Networks 防火墙支持基于路由的 VPN。

Palo Alto Networks 防火墙可建立基于路由的 VPN，其中防火墙可根据目标 IP 地址做出路由决策。如果通过 VPN 隧道将流量路由到特定目标，则会将该流量作为 VPN 流量进行处理。

可以使用 IP 安全 (IPSec) 协议组为 VPN 流量建立安全隧道，并保护 TCP/IP 数据包中的信息（如果隧道类型为 ESP，则加密）。在其他 IP 负载中嵌入 IP 数据包（标头和负载），并应用新标头，然后通过 IPSec 隧道发送。新标头中的源 IP 地址是本地 VPN 对等设备的源 IP 地址，目标 IP 地址是隧道远端 VPN 对等设备的目标 IP 地址。当数据包到达远程 VPN 对等设备（隧道远端的防火墙）后，将会移除外部标头，并将原始数据包发送到其目的地。

要建立 VPN 隧道，首先需要对对等设备进行身份验证。在身份验证成功后，对等设备协商加密机制和算法来保护通信。Internet 密钥交换 (IKE) 过程用来对 VPN 对等设备进行身份验证，并在隧道的每一端定义 IPSec 安全关联 (SA) 保护 VPN 通信。IKE 使用数字证书或预共享密钥，以及 Diffie Hellman 密钥为 IPSec 隧道建立 SA。SA 指定安全传输所需的所有参数 — 包括安全参数索引 (SPI)、安全协议、加密密钥和目标 IP 地址 — 加密、数据身份验证、数据完整性和端点身份验证。

下图显示了两个站点之间的 VPN 隧道。如果受 VPN 对等设备 A 保护的客户端需要位于其他站点的服务器的内容，则 VPN 对等设备 A 向 VPN 对等设备 B 发起连接请求。如果安全策略允许进行连接，VPN 对等设备 A 使用 IKE 加密配置文件参数（IKE 阶段 1）建立安全连接，并对 VPN 对等设备 B 进行身份验证。然后，VPN 对等设备 A 使用 IPSec 加密配置文件建立 VPN 隧道，该配置文件用来定义 IKE 阶段 2 参数以允许在两个站点之间安全传输数据。




图 **9:** 站点到站点 **VPN**


© 2019 Palo Alto Networks, Inc.

# 站点到站点 VPN 概念

VPN 连接可提供两个或多个站点之间的信息的安全访问。要提供资源和可靠连接的安全访问，VPN 连接需要以下组件：

- IKE 网关
- 隧道接口
- 隧道监控
- VPN 的 Internet 密钥交换 (IKE)
- IKEv2

## IKE 网关

在两个网络之间发起和终止 VPN 连接的 Palo Alto Networks 防火墙或防火墙和其他安全设备称为 IKE 网关。要建立 VPN 隧道并在 IKE 网关之间发送流量，每个对等设备必须拥有 IP 地址（静态或动态）或 FQDN。VPN 对等设备使用预共享密钥或证书进行相互身份验证。

对等设备还必须在 IKE 阶段 1 中协商用于建立 VPN 隧道的主模式或主动模式和 SA 生命周期。主模式保护对等设备的身份且更安全，因为在建立隧道时会交换多个数据包。主模式是为 IKE 协商推荐的模式，如果两个对等设备都支持该模式。主动模式使用少量数据包建立 VPN 隧道，因此速度较快，但用来建立 VPN 隧道的安全性较低。

有关配置的详细信息，请参阅设置 IKE 网关。

## 隧道接口

要建立 VPN 隧道，每个端点的第 3 层接口都必须拥有逻辑隧道接口用来连接到防火墙并建立 VPN 隧道。隧道接口是用来在两个端点之间传输流量的逻辑（虚拟）接口。如果配置任何代理 ID，代理 ID 将计入任何 IPSec 隧道容量。

隧道接口必须属于安全区域才能应用策略，并且必须将其分配给虚拟路由器才能使用现有路由基础设施。务必确保将隧道接口和物理接口分配给同一虚拟路由器，这样防火墙才可执行路由查找并确定要使用的相应隧道。

通常，连接到隧道接口的第 3 层接口属于外部区域，如不信任区域。尽管隧道接口可以位于与物理接口相同的安全区域，但为了增加安全性和更好地了解，可以为隧道接口创建单独区域。如果为隧道接口创建单独区域（即 VPN 区域），则需创建安全策略以便使得流量能够在 VPN 区域和信任区域之间流动。

要在站点之间路由流量，隧道接口不需要 IP 地址。如果要启用隧道监控，或者使用动态路由协议在隧道之间路由流量，则只需要 IP 地址。使用动态路由，可将隧道 IP 地址用作路由到 VPN 隧道的流量的下一个跃点 IP 地址。

如果使用 VPN 对等设备配置 Palo Alto Networks 防火墙执行基于策略的 VPN，则必须在建立 IPSec 隧道时配置本地和远程代理 ID。每个对等设备与实际在数据包中收到的内容进行配置的代理 ID 比较，以允许成功的 IKE 阶段 2 协商。如果需要多个隧道，可以为每个隧道接口配置唯一的代理 ID；一个隧道接口最多可以拥有 250 个代理 ID。每个代理 ID 对于防火墙的 IPSec VPN 隧道容量非常重要，并且隧道容量根据防火墙型号而有所不同。

有关配置的详细信息，请参阅建立 IPSec 隧道。

## 隧道监控

对于 VPN 隧道，可以检查整个隧道的目标 IP 地址连接。防火墙上的网络监控配置文件可让您验证目标 IP 地址连接（使用 ICMP）或指定轮询间隔的下一个跃点，并指定在发生故障后访问监控的 IP 地址要采取的操作。



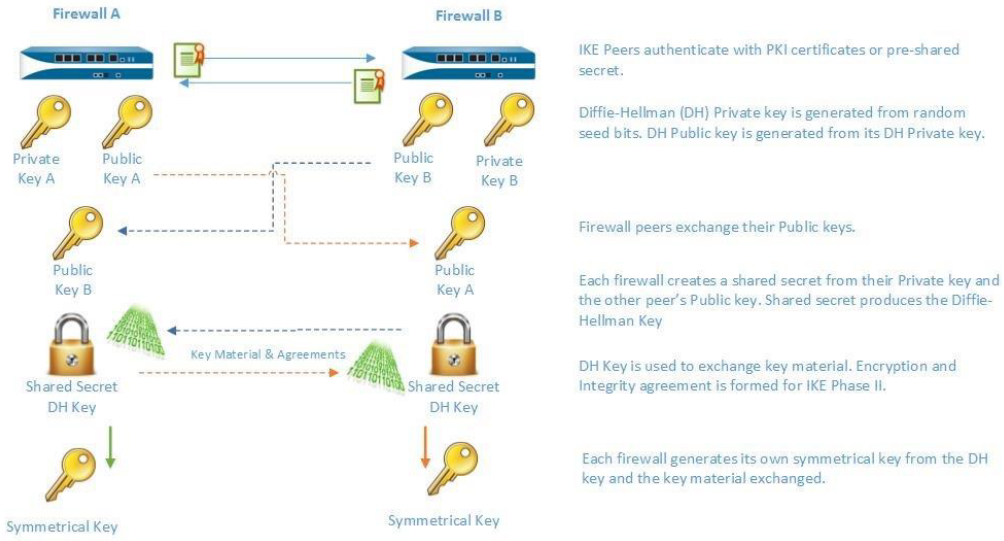
© 2019 Palo Alto Networks, Inc.

如果无法访问目标 IP 地址，可以配置防火墙等待隧道恢复或配置自动故障转换至另一个隧道。在这两种情况下，防火墙生成系统日志提醒您隧道发生故障，并重新协商 IPSec 密钥加快恢复。

有关配置的详细信息，请参阅设置隧道监控。

# VPN 的 Internet 密钥交换 (IKE)

IKE 过程允许位于隧道两端的 VPN 对等设备使用双方商定的加密的密钥或证书和方法对数据包进行加密和解密。IKE 过程在两个阶段会出现：IKE 阶段 1 和 IKE 阶段 2。每个阶段都可使用利用加密配置文件（即 IKE 加密配置文件和 IPSec 加密配置文件）定义的密钥和加密算法，并且 IKE 协商的结果为安全关联 (SA)。SA 是一组双方商定的密钥和算法，VPN 对等设备用来允许在 VPN 隧道之间传输数据。下图显示了建立 VPN 隧道的密钥交换过程：




## *IKE 阶段 1*

在本阶段中，防火墙使用在 IKE 网关配置和 IKE 加密配置文件中定义的参数相互进行身份验证，并建立安全控制通道。IKE 阶段支持使用预共享密钥或数字证书（使用公钥基础设施 (PKI)）对对等设备进行相互身份验证。预共享密钥是用于保护小型网络的简单解决方案，因为它们不需要支持 PKI 基础设施。数字证书需要更强的身份验证安全，因此保护大型网络或实施起来更方便。

使用证书时，请确保两个网关对等设备信任 CA 签发的证书，并且证书链中证书的最大长度为 5 或更少。在启用 IKE 碎片后，防火墙可以最多使用证书链中的 5 个证书重编 IKE 消息，并成功建立 VPN 隧道。

IKE 加密配置文件用于定义在 IKE SA 协商中使用的以下选项：

- Diffie-Hellman (DH) 组为 IKE 生成对称密钥。

  Diffie-Hellman 算法使用一方的私钥和另一方的公钥创建共享机密，即两个 VPN 隧道对等设备共享的加密密钥。在防火墙上支持的 DH 组为：组 1—768 位、组 2—1024 位（默认）、组 5—1536 位、组 14—2048 位、组 19—256 位椭圆曲线组和组 20—384 位椭圆曲线组。
- 身份验证算法 — sha1、sha 256、sha 384、sha 512 或 md5
- 加密算法 — 3des、aes-128-cbc、aes-192-cbc、aes-256-cbc 或 des

## *IKE 阶段 2*

在保护和验证隧道后，在阶段 2 中，通道可用来进一步保护在网络之间传输数据。IKE 阶段 2 使用在该过程的阶段 1 和 IPSec 加密配置文件中创建的密钥，定义在 IKE 阶段 2 的 SA 中使用的 IPSec 协议和密钥。

IPSEC 使用以下协议实现安全通信：


© 2019 Palo Alto Networks, Inc.

- 封装安全负载 (ESP) — 可让您对整个 IP 数据包进行加密，对数据包源进行身份验证并验证数据完整性。虽然 ESP 需要您对数据包进行加密和身份验证，但可以选择通过将加密选项设置为 Null 只加密或只进行身份验证；使用加密不会影响身份验证。
- 身份验证头 (AH) — 对数据包源进行身份验证和验证数据完整性。AH 不会对数据负载进行加密，且不适合用于数据隐私非常重要的部署。AH 常用于验证对等设备的合法性，并且不需要数据隐私。

表 **5: IPSEC** 身份验证和加密支持的算法

| ESP | AH |
|---|---|
| 支持的 Diffie Hellman (DH) 交换选项 | |
| • 组 1 — 768 位<br>• 组 2 — 1024 位（默认）<br>• 组 5 — 1536 位<br>• 组 14 — 2048 位。<br>• 组 19 — 256 位椭圆曲线组<br>• 组 20 —384 位椭圆曲线组<br>• no-pfs — 默认情况下，完全正向保密 (PFS) 处于启用状态，这表示 IKE 阶段 2 会使用上述所列组之一生成新 DH 密钥。该密钥独立于 IKE 阶段 1 中交换的密钥，可提供更好的数据传输安全。如果您选择 no-pf，则不会续订在阶段 1 中创建的 DH 密钥，且 IPSec SA 协商只需使用一个密钥。必须同时为 PFS 启用或禁用两个 VPN 对等设备。 | |
| 支持的加密算法 | |
| • 3des | 安全强度为 112 位的三重数据加密标准 (3DES) |
| • aes-128-cbc | 使用密码块链 (CBC) 的高级加密标准 (AES)，安全强度为 128 位 |
| • aes-192-cbc | 使用密码强度为 192 位的 CBC 的 AES |
| • aes-256-cbc | 使用密码强度为 256 位的 CBC 的 AES |
| • aes-128-ccm | 使用密码强度为 128 位的 Counter with CBC-MAC (CCM) 的 AES |
| • aes-128-gcm | 使用密码强度为 128 位的 Galois/Counter Mode (GCM) 的 AES |
| • aes-256-gcm | 使用密码强度为 256 位的 GCM 的 AES |
| • des | 安全强度为 56 位的数据加密标准 (DES) |
| 支持的身份验证算法 | |
| • md5 | • md5 |
| • sha 1 | • sha 1 |
| • sha 256 | • sha 256 |
| • sha 384 | • sha 384 |
| • sha512 | • sha 512 |



© 2019 Palo Alto Networks, Inc.

## 保护 *IPSec VPN* 隧道的方法（*IKE* 阶段 *2*）

可以使用手动密钥和自动密钥保护 IPSec VPN 隧道。此外，IPSec 配置选项包括密钥协议的 Diffie-Hellman 组，和/或加密算法和消息身份验证的哈希算法。

- 手动密钥 — 如果 Palo Alto Networks 防火墙使用旧设备建立 VPN 隧道，或者如果想要减少生成会话密钥的开销，通常使用手动密钥。如果使用手动密钥，必须在两个对等设备上配置同一密钥。

  不建议使用手动密钥建立 VPN 隧道，因为在中断对等设备之间的密钥信息时可能会影响会话密钥；如果该密钥受到影响，则数据传输不再安全。
- 自动密钥 — 自动密钥可让您根据在 IPSec 加密配置文件中定义的算法自动生成用于建立和维护 IPSec 隧道的密钥。

## IKEv2

IPSec VPN 网关使用 IKEv1 或 IKEv2 协商 IKE 安全关联 (SA) 和 IPSec 隧道。IKEv2 在 RFC 5996 内定义。

与使用阶段 1 SA 和阶段 2 SA 的 IKEv1 不同，IKEv2 使用封装式安全措施负载 (ESP) 或身份验证标头 (AH) 的子 SA，该 SA 与 IKE SA 一起设置。

如果位于两个网关之间的设备上出现 NAT，您需要在两个网关上启用 NAT 遍历 (NAT-T)。一个网关只能查看 NAT 设备的公共（全局可路由）IP 地址。

与 IKEv1 相比，IKEv2 具备以下优势：

- 隧道端点交换较少的消息即可建立隧道。IKEv2 使用四个消息；IKEv1 使用九个消息（在主要模式下）或六个消息（在主动模式下）。
- 内置 NAT-T 功能提升了供应商之间的兼容性。
- 如果隧道关闭，内置运行状况检查可自动重建隧道。活性检查取代了 IKEv1 中使用的失效对等设备检测。
- 支持流量选择器（每个交换一个）。流量选择器用在 IKE 协商中，用于控制哪些流量可以访问此隧道。
- 支持哈希和 URL 证书交换来减少碎片。
- 通过提高对等设备验证来抵御 Dos 攻击。超过半开 SA 数量可以触发 Cookie 验证。

在配置 IKEv2 之前，您应该先熟悉以下概念：

- 活性检查
- Cookie 激活阈值和严格 Cookie 验证
- 流量选择器
- 哈希和 URL 证书交换
- SA 密钥生命周期和重新验证间隔

在设置 IKE 网关后，如果您选择 IKEv2，请根据环境需要执行下列与 IKEv2 相关的可选任务：

- 导出对端设备的证书以使用哈希和 URL 进行访问
- 导入证书以进行 IKEv2 网关验证
- 更改 IKEv2 的密钥生命周期或身份验证间隔
- 更改 IKEv2 的 Cookie 激活阈值
- 配置 IKEv2 流量选择器

## 活性检查

IKEv2 的活性检查类似于失效对等设备检测 (DPD)，IKEv1 使用此检测作为确定对等设备是否仍可用的方式。

在 IKEv2 中，网关以可配置的时间间隔（默认为 5 秒）向对等设备发送任意 IKEv2 包传输或空的参考消息来实现活性检查。如果需要，发送者会尝试重新传输，最多尝试 10 次。如果得不到响应，发送方会关闭并删除 IKE_SA 和对应的 CHILD_SA。发送方会发出另一个 IKE_SA_INIT 消息来从头开始。


© 2019 Palo Alto Networks, Inc.

## *Cookie* 激活阈值和严格 *Cookie* 验证

始终为 IKEv2 启用 Cookie 验证；这有助于防御半开 SA DoS 攻击。您可以配置将触发 Cookie 验证的半开 SA 全局阈值数。您还可以配置各 IKE 网关来为每个新 IKEv2 SA 执行 Cookie 验证。

- **Cookie Activation Threshold**（**Cookie** 激活阈值）是全局 VPN 会话设置，用于限制同步半开 IKE SA（默认为 500）的数量。如果半开 IKE SA 数量超过 **Cookie Activation Threshold**（**Cookie** 激活阈值），响应者将会请求 Cookie，且发起者必须使用包含 Cookie 的 IKE_SA_INIT 进行响应以对此连接进行验证。如果 Cookie 验证成功，可以启动其他 SA。值为 0 表示 Cookie 验证应始终开启。

  发起者返回 Cookie 之前，响应者不会维护发起者的状态，也不会执行 Diffie-Hellman 密钥交换。IKEv2 Cookie 验证可减少试图保留大量连接半开放的攻击。

  **Cookie Activation Threshold**（**Cookie** 激活阈值）必须低于 **Maximum Half Opened SA**（最大半开 **SA**）设置。如果您更改 IKEv2 的 Cookie 激活阈值为非常高的数量（例如，65534），而 **Maximum Half Opened SA**（最大半开 **SA**）设置保留默认值 65535，基本上会禁用 cookie 验证。
- 如果无论全局阈值如何，您都想为网关收到的每个新 IKEv2 SA 执行 Cookie 验证，您可以启用 **Strict Cookie Validation**（严格 **Cookie** 验证）。**Strict Cookie Validation**（严格 **Cookie** 验证）只影响要配置的 IKE 网关，默认情况下处于禁用状态。禁用 **Strict Cookie Validation**（严格 **Cookie** 验证）时，系统将使用 **Cookie Activation Threshold**（**Cookie** 激活阈值）确定是否需要 Cookie。

## 流量选择器

在 IKEv1 中，具备基于路由的 VPN 的防火墙需要使用本地和远程代理 ID 才能设置 IPSec 隧道。每个对等设备需要将其代理 ID 与其在数据包中接收的代理 ID 进行比较才能成功协商 IKE 阶段 2。IKE 阶段 2 说的是协商 SA 来设置 IPSec 隧道。（有关代理 ID 的详细信息，请参阅隧道接口。）

在 IKEv2 中，您可以配置 IKEv2 流量选择器，此选择器是 IKE 协商期间使用的网络流量的组件。流量选择器在 CHILD_SA（隧道创建）阶段 2 期间用以设置隧道和确定允许哪些流量通过此隧道。这两个 IKE 网关对等设备必须协商并在流量选择器上达成一致；否则，其中一侧对等设备会缩小地址范围来达成一致。一个 IKE 连接可以有多个隧道；例如，您可以为各部门分配不同的隧道来隔离流量。流量分离还允许实施 QoS 之类的功能。

IPv4 和 IPv6 流量选择器有：

- 源 **IP** 地址 — 网络前缀、地址范围、特定主机或通配符。
- 目标 **IP** 地址 — 网络前缀、地址范围、特定主机或通配符。
- 协议 — 传输协议，如 TCP 或 UDP。
- 源端口 — 产生此数据包的端口。
- 目标端口 — 数据包的目标端口。

在 IKE 协商期间，不同的网络和协议可以有多个流量选择器。例如，发起者可能指示要通过隧道将 TCP 数据包从 172.168.0.0/16 发送到其对等设备，目标为 198.5.0.0/16。同时希望通过同一隧道将 UDP 数据包从 172.17.0.0/16 发送到同一网关，目标为 0.0.0.0（任意网络）。对等设备网关必须与这些流量选择器保持一致才能知道会发生什么操作。

有可能一个网关将使用流量选择器（比其它网关的 IP 地址更加具体的 IP 地址）开始协商。

- 例如，网关 A 提供源 IP 地址 172.16.0.0/16 和目标 IP 地址 192.16.0.0/16。但是网关 B 配置为使用 0.0.0.0（任意源）作为源地址，使用 0.0.0.0（任意目标）作为目标 IP 地址。因此，网关 B 会将其源 IP 地址缩小到 192.16.0.0/16，将目标地址缩小到 172.16.0.0/16。因此，缩小将适应网关 A 的地址，并且这两个网关的流量选择器将一致。
- 如果网关 B（配置了源 IP 地址 0.0.0.0）是发起者，而不是响应者，网关 A 将使用其更为具体的 IP 地址进行响应，网关 B 将缩小其地址以达成一致。



© 2019 Palo Alto Networks, Inc.

## 哈希和 *URL* 证书交换

IKEv2 支持在 SA 的 IKEv2 协商期间使用的哈希和 URL 证书交换。将证书存储在由 URL 指定的 HTTP 服务器上。对等设备从接收指向服务器的 URL 的服务器获取证书。哈希用于检查证书的内容是否有效。因此，这两个对等设备会与 HTTP CA 交换证书，而不是互相交换证书。

哈希和 URL 的哈希部分可减少消息大小，因此哈希和 URL 是一种在 IKE 阶段减少数据包碎片的方法。对端设备收到所需的证书和哈希，说明 IKE 阶段 1 已对对端设备进行验证。减少碎片发生有助于防御 DoS 攻击。

在配置 IKE 网关时，通过选择 **HTTP Certificate Exchange**（**HTTP** 证书交换）并输入 **Certificate URL**（证书 **URL**）可以启用哈希和 URL 证书交换。对端设备也必须使用哈希和 URL 证书交换才能使交换成功。如果对端设备不能使用哈希和 URL，将以在 IKEv1 中交换哈希和 URL 证书的类似方式交换 X.509 证书。

如果您启用哈希和 URL 证书交换，如果证书服务器中尚无此证书，必须将此证书导出到证书服务器。在您导出证书时，文件格式应为 **Binary Encoded Certificate (DER)**（二进制编码证书 **(DER)**）。请参阅导出对端设备的证书以使用哈希和 URL 进行访问。

## *SA* 密钥生命周期和重新验证间隔

在 IKEv2 中，有两个 IKE 加密配置文件值 **Key Lifetime**（密钥生命周期）和 **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数）来控制 IKEv2 IKE SA 的建立。密钥生命周期是协商 IKE SA 密钥保持有效的时间长度。在密钥的生命周期到期之前，必须重新为 SA 生成密钥；否则，一旦到期，SA 必须开始新的 IKEv2 IKE SA 密钥更新。默认值为 8 小时。

重新身份验证间隔等于 **Key Lifetime**（密钥生命周期）乘以 **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数）。验证倍数默认为 0，表示禁用重新验证功能。

身份验证倍数范围为 0-50。因此，例如您将身份验证倍数设置为 20，则系统会每隔 20 次密钥更新执行一次重新验证，即每 160 个小时执行一次。这表示须向 IKE 进行重新验证以从头重建 IKE SA 之前，网关有 160 小时的时间执行子 SA 创建。

在 IKEv2 中，发起者和响应者网关都有自己的密钥生命周期，而密钥生命周期较短的网关是要求更新 SA 密钥的网关。


© 2019 Palo Alto Networks, Inc.

# 设置站点到站点 VPN

要设置站点到站点 VPN：

- 请确保以太网接口、虚拟路由器和区域均已正确配置。有关更多信息，请参阅配置接口和区域。
- 创建隧道接口。理想的情况是，将隧道接口放在一个单独区域，以便隧道流量可以使用不同的策略。
- 设置静态路由或指定路由协议，以将流量重定向到 VPN 隧道。要支持动态路由协议（支持 OSPF、BGP、RIP），必须为隧道接口分配 IP 地址。
- 定义 IKE 网关在 VPN 隧道各端的对等设备之间建立通信；还定义加密配置文件指定用于标识、身份验证和加密的协议和算法，用来在 IKEv1 阶段 1 中建立 VPN 隧道。请参阅设置 IKE 网关和定义 IKE 加密配置文件。
- 配置建立 IPSec 连接在整个 VPN 隧道传输数据所需的参数；请参阅设置 IPSec 隧道。对于 IKEv1 阶段 2，请参阅定义 IPSec 加密配置文件。
- （可选）指定防火墙监控 IPSec 隧道的方式。请参阅设置隧道监控。
- 定义筛选和检查流量的安全策略。



如果安全规则库的结尾是拒绝规则，则除非另行允许，否则阻止区域内通信。必须在拒绝规则上方显式包括允许 *IKE* 和 *IPSec* 应用程序的规则。



如果您的 *VPN* 流量通过（不是始发或终止）*PA-7000* 系列或 *PA-5200* 系列防火墙，请配置双向安全策略规则以允许 *ESP* 或 *AH* 流量在两个方向流动。

完成这些任务后，便可使用隧道。发往在策略中定义的区域/地址的流量根据路由表中的目标路径自动正常路由，并作为 VPN 流量进行处理。有关站点到站点 VPN 的几个示例，请参阅站点到站点 VPN 快速配置。

为了排除故障，您可以启用/禁用，刷新或重新启动 IKE 网关或 IPSec 隧道。

## 设置 IKE 网关

要建立 VPN 隧道，VPN 对等设备或网关必须使用预共享密钥或数字证书进行相互身份验证，并在其中建立安全通道以协商用于保护各端主机之间流量的 IPSec 安全关联 (SA)。

STEP 1 | 定义 IKE 网关。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Gateways**（**IKE** 网关），**Add**（添加）网关，然后输入网关 **Name**（名称）（**General**（常规）选项卡）。
2. 设置 **Version**（版本）为 **IKEv1 only mode**（仅 **IKEv1** 模式）、**IKEv2 only mode**（仅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式）。IKE 网关将在此处指定的模式下开始与对等设备的协商。如果您选择 **IKEv2 preferred mode**（**IKEv2** 首选模式），这两个对端设备将使用 IKEv2，但远程对端设备要支持 IKEv2，否则它们将使用 IKEv1。

   选中的 **Version**（版本）还决定了您可以使用 **Advanced Options**（高级选项）选项卡上的哪些选项。

STEP 2 | 建立隧道（网关）的本地端点。

1. 选择 **Address Type**（地址类型）：**IPv4** 或 **IPv6**。
2. 在本地网关所在的防火墙上选择物理出站 **Interface**（接口）。
3. 从 **Local IP Address**（本地 **IP** 地址）列表中选择 VPN 连接将用作端点的 IP 地址；这是面向外部的接口，且具有防火墙上公开路由 IP 地址。

STEP 3 | 在隧道（网关）远端建立对等设备。

从 **Peer IP Address Type**（对端 **IP** 地址类型）选择以下其中一个并输入对端的相应信息：

- **IP** — 输入 **Peer Address**（对端地址）作为 IPv4 或 IPv6 地址，或输入 IPv4 或 IPv6 地址的地址对象。



© 2019 Palo Alto Networks, Inc.

- **FQDN** — 输入 **Peer Address**（对端地址）作为 FQDN 字符串或是使用 FQDN 字符串的地址对象。如果 FQDN 或 FQDN 地址对象解析为多个 IP 地址，则防火墙将从与 IKE 网关的地址类型（IPv4 或 IPv6）匹配的一组地址中选择首选地址，如下所示：
  - 如果未协商 IKE 安全关联 (SA)，则首选地址为具有最小值的 IP 地址。
  - 如果 IKE 网关使用返回地址集中的地址，则防火墙选择此地址（无论其是否是集中最小的地址）。
  - 如果 IKE 网关使用非返回地址集中的地址，则防火墙选择一个新地址，这是集中最小的地址。
- **Dynamic**（动态）— 如果对端设备 IP 地址或 FQDN 值未知，请选择 **Dynamic**（动态），此后，对端设备将启动协商。



使用 *FQDN* 或 *FQDN* 地址对象可以减少对端受动态 *IP* 地址变更影响的环境中的问题（否则，需要您重新配置此 *IKE* 网关对端地址）。

STEP 4 | 指定验证对端设备的方式：

选择 **Authentication**（身份验证）方法：**Pre-Shared Key**（预共享密钥）或 **Certificate**（证书）。如果您选择预共享密钥，请前进至下一步。如果选择证书，请跳到步骤 6 配置基于证书的身份验证。

STEP 5 | 配置预共享密钥。

1. 输入一个 **Pre-shared Key**（预共享密钥）作为整个隧道内身份验证的安全密钥。重新将此值输入到 **Confirm Pre-shared Key**（确认预共享密钥）。最多使用 255 个 ASCII 或非 ASCII 字符。



生成一个字典式攻击很难破解的密钥；如有必要，请使用预共享密钥生成器。

2. 对于 **Local Identification**（本地标识），请从以下类型中进行选择，然后输入您确定的值：**FQDN (hostname)**（主机名）、**IP address**（IP 地址）、**KEYID (binary format ID string in HEX)**（以十六进制表示的二进制格式 ID 字符串）、和**User FQDN (email address)**（用户 FQDN（电子邮件地址））。本地标识用于定义本地网关的格式和标识。如果没有指定值，则将使用本地 IP 地址作为本地标识值。
3. 对于 **Peer Identification**（对端标识），请从以下类型中进行选择，然后输入您确定的值：**FQDN (hostname)**（主机名）、**IP address**（IP 地址）、**KEYID (binary format ID string in HEX)**（以十六进制表示的二进制格式 ID 字符串）、和**User FQDN (email address)**（用户 FQDN（电子邮件地址））。对等设备标识用于定义对等设备网关的格式和标识。如果没有指定值，则将使用对端 IP 地址作为对端设备标识值。
4. 执行步骤 7（配置网关的高级选项）。

STEP 6 | 配置基于证书的身份验证。

如果您选择 **Certificate**（证书）作为对隧道另一端对端设备网关进行身份验证的方法，请执行此过程的剩余步骤。

1. 选择防火墙上已存在的 **Local Certificate**（本地证书），**Import**（导入）证书，或 **Generate**（生成）新证书。
   - 如果您需要 **Import**（导入）证书，则首先请导入证书以对 IKEv2 网关进行身份验证，然后返回到此任务。
   - 如果您想 **Generate**（生成）新证书，则首先请在防火墙上生成证书，然后返回到此任务。
2. （可选）启用（选择）**HTTP Certificate Exchange**（**HTTP** 证书交换）以配置哈希和 URL（仅限 IKEv2）。对于 HTTP 证书交换，请输入 **Certificate URL**（证书 **URL**）。有关更多信息，请参阅哈希和 URL 证书交换。
3. 选择 **Local Identification**（本地身标识）类型 — **Distinguished Name (Subject) FQDN (hostname)**（可分辨名称（主题）**FQDN**（主机名）、**IP address**（IP 地址）或 **User FQDN (email address)**（用户 **FQDN**（电子邮件地址）），然后输入值。本地标识用于定义本地网关的格式和标识。


© 2019 Palo Alto Networks, Inc.

4. 选择 **Peer Identification**（对端设备标识）类型 — **Distinguished Name (Subject) FQDN (hostname)**（可分辨名称（主题）**FQDN**（主机名）、**IP address**（**IP** 地址）或 **User FQDN (email address)**（用户 **FQDN**（电子邮件地址）），然后输入值。对等设备标识用于定义对等设备网关的格式和标识。
5. 选择 **Peer ID Check**（对端设备 **ID** 检查）类型：
   - **Exact**（精确）— 确保本地设置和对端设备 IKE ID 有效内容精确匹配。
   - **Wildcard**（通配符）— 允许对端设备标识只匹配通配符 (*) 之前的每个字符。通配符后面的字符不需要匹配。
6. （可选）即使对端设备标识与证书中的对端设备标识不匹配，IKE SA 仍成功，请单击 **Permit peer identification and certificate payload identification mismatch**（允许对等设备标识和证书有效内容标识不匹配）。
7. 创建 **Certificate Profile**（证书配置文件）。证书配置文件包含有关如何验证对等设备网关的信息。
8. （可选）要严格控制密钥的使用方式，请单击 **Enable strict validation of peer's extended key use**（启用对端设备扩展密钥使用的严格验证）。

STEP 7 | 配置网关的高级选项。

1. （可选）在公共选项（**Advanced Options**（高级选项））中**Enable Passive Mode**（启用被动模式），以指定防火墙仅响应 IKE 连接请求，但不启用。
2. 如果您的设备在网关之间执行 NAT，请 **Enable NAT Traversal**（启用 **NAT** 遍历），以在 IKE 和 UDP 协议中使用 UDP 封装，从而使这些协议直接通过中间 NAT 设备。
3. 如果已在步骤 1 中配置 **IKEv1 only mode**（仅 **IKEv1** 模式），请在 IKEv1 选项卡上进行以下配置：
   - 选择 **Exchange Mode**（交换模式）：**auto**（自动）、**aggressive**（主动）或**main**（主要）。将防火墙设置为使用 **auto**（自动）交换模式时，可以接受 **main**（主要）模式和 **aggressive**（主动）模式的协商请求；但是，只要有可能，该防火墙便会在 **main**（主要）模式进行交换。

     如果交换模式没有设置为 *auto*（自动），则必须使用同一交换模式配置两个对端设备，以允许每个对端设备接受协商请求。

   - 选择现有配置文件或保留 **IKE Crypto Profile**（**IKE** 加密配置文件）列表中的默认配置文件。必要时，您可以定义 IKE 加密配置文件。
   - （只有当使用基于证书的身份验证且尚未将交换模式设置为主动模式时）单击 **Enable Fragmentation**（启用碎片）以便使防火墙能够使用 IKE 碎片。
   - 单击 **Dead Peer Detection**（失效对端设备检测），然后输入 **Interval**（间隔）（范围为 2-100 秒）。对于 **Retry**（重试），请定义尝试重新检查有效性之前拖延的时间（范围为 2-100 秒）。失效对等设备检测通过将 IKE 阶段 1 通知负载发送到对等设备并等待确认来确定处于非活动状态或不可用的 IKE 对等设备。
4. 如果在步骤 1 中已配置 **IKEv2 only mode**（仅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式），请在 IKEv2 选项卡上进行以下配置：
   - 选择 **IKE Crypto Profile**（**IKE** 加密配置文件），此配置文件可配置 IKE 阶段 1 选项，如 DH 组、哈希算法和 ESP 身份验证。有关 IKE 加密配置文件的信息，请参阅 IKE 阶段 1。
   - （可选）启用 **Strict Cookie Validation**（严格 **Cookie** 验证）Cookie 激活阈值和严格 Cookie 验证。
   - （可选）如果您希望网关向其网关对端设备发送消息请求以请求响应，请单击 **Enable Liveness Check**（启用活性检查）并输入 **Interval (sec)**（间隔（秒））（默认为 5 秒）。如果需要，发起者最多会尝试 10 次活性检查。如果得不到响应，发起者会关闭并删除 IKE_SA 和 CHILD_SA。发起者会发出另一个 IKE_SA_INIT 消息来从头开始。

STEP 8 | 单击 **OK**（确定）并 **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

## 导出对端设备的证书以使用哈希和 *URL* 进行访问

IKEv2 支持哈希和 URL 证书交换作为隧道远端的对端设备从已导入此证书的服务器获取证书的方法。执行此任务以将证书导出到该服务器。您必须已使用 **Device**（设备）> **Certificate Management**（证书管理）创建证书。

STEP 1 | 选择 **Device**（设备）> **Certificates**（证书），并且如果您的平台支持多虚拟系统，您可以为 **Location**（位置）选择相应的虚拟系统。

STEP 2 | 在 **Device Certificates**（设备证书）选项卡上，选择要 **Export**（导出）到服务器的证书。

证书的状态应为有效，并且未到期。防火墙不会阻止您导出无效证书。

STEP 3 | 对于 **File Format**（文件格式），请选择 **Binary Encoded Certificate (DER)**（二进制编码证书 **(DER)**）。

STEP 4 | 保留 **Export private key**（导出私钥）的未选中状态。无需为哈希和 URL 导出私钥。

STEP 5 | 单击 **OK**（确定）。

## 导入证书以进行 *IKEv2* 网关验证

如果您要对 IKEv2 网关的对等设备进行身份验证，并且防火墙上没有使用过本地证书，或者您想从其他位置导入证书，请执行此任务。

此任务假设您已选择 **Network**（网络）> **IKE Gateways**（**IKE** 网关），已添加网关，并已为 **Local Certificate**（本地证书）单击 **Import**（导入）。

STEP 1 | 导入证书。

1. 选择 **Network**（网络）> **IKE Gateways**（**IKE** 网关），**Add**（添加）网关，然后在 **General**（常规）选项卡上为 **Authentication**（身份验证）选择 **Certificate**（证书）。对于 **Local Certificate**（本地证书），请单击 **Import**（导入）。
2. 在“导入证书”窗口中，为您要导入的证书输入 **Certificate Name**（证书名称）。
3. 如果要在多个虚拟系统间共享该证书，请选择 **Shared**（共享）。
4. 对于 **Certificate File**（证书文件），请单击 **Browse**（浏览）找到此证书文件。单击文件名并单击 **Open**（打开），此操作可填充 **Certificate File**（证书文件）字段。
5. 对于 **File Format**（文件格式），请选择下列其中一种：
   - **Base64** 编码证书 **(PEM)** — 包含证书，但不含密钥。这是明文。
   - 加密私钥和证书 **(PKCS12)** — 包含证书和密钥。
6. 如果密钥所在文件与证书文件不是同一文件，请选择 **Import private key**（导入私钥）。密钥可选，但以下情况例外：
   - 如果将 **File Format**（文件格式）设置为 **PEM**，您必须导入密钥。通过单击 **Browse**（浏览）并浏览到要导入的密钥文件来输入 **Key file**（密钥文件）。
   - 输入 **Passphrase**（密码）和 **Confirm Passphrase**（确认密码）。
7. 单击 **OK**（确定）。

STEP 2 | 继续下一个任务。

步骤配置基于证书的身份验证。


© 2019 Palo Alto Networks, Inc.

## 更改 *IKEv2* 的密钥生命周期或身份验证间隔

此任务为可选任务，IKEv2 IKE SA 密钥更新生命周期的默认设置为 8 小时。IKEv2 身份验证倍数的默认设置为 0，表示禁用重新验证功能。有关详细信息，请参阅 SA 密钥生命周期和重新验证间隔。

要更改默认值，请执行以下任务。先决条件是已存在 IKE 加密配置文件。

STEP 1 | 更改 IKE 加密配置文件的 SA 密钥生命周期或身份验证间隔

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Crypto**（**IKE** 加密），然后选择适用于本地网关的 IKE 加密配置文件。
2. 对于 **Key Lifetime**（密钥生命周期），请选择单位（**Seconds**（秒）、**Minutes**（分钟）、**Hours**（小时）或 **Days**（天））并输入值。最小值为 3 分钟。
3. 对于 **IKE Authentication Multiple**（**IKE** 身份验证倍数），请输入一个值，此值乘以生命周期可确定重新验证间隔。

STEP 2 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

## 更改 *IKEv2* 的 *Cookie* 激活阈值

如果需要 Cookie 验证前，您希望防火墙的阈值不同于 500 半开 SA 会话数的默认设置，请执行以下任务。有关 Cookie 验证的详细信息，请参阅 Cookie 激活阈值和严格 Cookie 验证。

STEP 1 | 更改 Cookie 激活阈值。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑 VPN 会话设置。对于 **Cookie Activation Threshold**（**Cookie** 激活阈值），请输入响应者从发起者请求 Cookie 之前允许的最大半开 SA 数量（范围为 0-65,535，默认为 500）。
2. 单击 **OK**（确定）。

STEP 2 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

## 配置 *IKEv2* 流量选择器

在 IKEv2 中，您可以配置流量选择器，这是 IKE 协商期间使用的网络流量的组件。流量选择器在 CHILD_SA（隧道创建）阶段 2 期间用以设置隧道和确定允许哪些流量通过此隧道。这两个 IKE 网关对等设备必须协商并在流量选择器上达成一致；否则，其中一侧对等设备会缩小地址范围来达成一致。一个 IKE 连接可以有多个隧道；例如，您可以为各部门分配不同的隧道来隔离流量。流量分离还允许实施 QoS 之类的功能。使用以下工作流可配置流量选择器。

STEP 1 | 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）> **Proxy IDs**（代理 **ID**）。

STEP 2 | 选择 **IPv4** 或 **Ipv6** 选项卡。

STEP 3 | 单击 **Add**（添加），然后在 **Proxy ID**（代理 **ID**）字段中输入 **Name**（名称）。

STEP 4 | 在 **Local**（本地）字段中，输入 **Source IP Address**（源 **IP** 地址）。

STEP 5 | 在 **Remote**（远程）字段中输入 **Destination IP Address**（目标 **IP** 地址）。

STEP 6 | 在 **Protocol**（协议）字段中，选择传输协议（**TCP** 或 **UDP**）。

STEP 7 | 单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

# 定义加密配置文件

加密配置文件指定用于在两个 IKE 对等设备之间进行身份验证和/或加密的密码，以及密钥的生命周期。每个再协商之间的时间段称为生命周期；当指定的时间段到期后，防火墙重新协商一组新的密钥。

为了保护 VPN 隧道之间的通信，防火墙需要 IKE 和 IPSec 加密配置文件来分别完成 IKE 阶段 1 和阶段 2 协商。防火墙包含现成的默认 IKE 加密配置文件和默认 IPSec 加密配置文件。

- 定义 IKE 加密配置文件
- 定义 IPSec 加密配置文件

## 定义 *IKE* 加密配置文件

IKE 加密配置文件用来设置在 IKE 阶段 1 的密钥交换过程中使用的加密和身份验证算法，密钥的生命周期指定了密钥的有效时间长度。要调用配置文件，必须将其附加到 IKE 网关配置。



一旦 *IKE* 网关的 *Peer IP Address Type*（对等 *IP* 地址类型）配置为 *Dynamic*（动态），且 *IKEv1* 主模式或 *IKEv2* 已被应用，那么，同一接口或本地 *IP* 地址上配置的所有 *IKE* 网关均必须使用相同的加密配置文件。

STEP 1 | 创建新的 IKE 配置文件。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Crypto**（**IKE** 加密），然后选择 **Add**（添加）。
2. 输入新配置文件的 **Name**（名称）。

STEP 2 | 指定密钥交换的 DH (Diffie–Hellman) 组，并指定身份验证和加密算法。

在对应的部分（DH 组、身份验证和加密）中单击 **Add**（添加），然后从菜单中进行选择。

如果您不确定 VPN 对等设备的支持内容，请按照安全性从高到低的顺序添加多个组或算法；对等设备会与最受支持的组或算法进行协商来建立隧道。

- DH 组 —
  - **group20**
  - **group19**
  - **group14**
  - **group5**
  - **group2**
  - **group1**
- 身份验证 —
  - **sha512**
  - **sha384**
  - **sha256**
  - **sha1**
  - **md5**
  - （PAN-OS 10.0.3 以及 10.0 的更新版本）**none**（无）



如果选择 *AES-GCM* 算法进行加密，必须选择身份验证设置 *none*（无），否则，提交将失败。哈希会根据所选 *DH* 组自动选择。*DH* 组 *19* 及以下使用*sha256*；*DH* 组 *20* 使用 *sha384*。

- 加密 ——
  - （PAN-OS 10.0.3 以及 10.0 的更新版本）**aes-256-gcm**（要求使用 IKEv2；DH 组应设为**group20**（组 **20**））



© 2019 Palo Alto Networks, Inc.

- （PAN-OS 10.0.3 以及 10.0 的更新版本）**aes-128-gcm**（要求使用 IKEv2 且 DH 组设为**group19**（组 **19**））
- **aes-256-cbc**
- **aes-192-cbc**
- **aes-128-cbc**
- **3des**
- **des**

选择对等设备支持的最强身份验证和加密算法。对于身份验证算法，请使用 *SHA-256* 或更高版本（对于长时间事务，首选为 *SHA-384* 或更高版本）。请勿使用 *SHA-1* 或 *MD5*。对于加密算法，请使用 *AES*； *DES* 和 *3DES* 很脆弱且易受攻击。带有 *Galois/*计数器模式 *(AES-GCM)* 的 *AES* 提供的安全性最高，且内置有身份验证功能，因此，如果选择 *aes-256-gcm* 或 *aes-128-gcm*加密，则必须将身份验证设为 *none*（无）。

STEP 3 | 指定密码有效的持续时间和重新进行身份验证的时间间隔。

有关详细信息，请参阅 SA 密钥生命周期和重新身份验证间隔。

1. 在 **Key Lifetime**（密钥生命周期）字段内，指定密钥的有效时段（以秒、分、小时或天为单位），范围为 3 分钟到 365 天；默认为 8 小时。密钥到期时，防火墙会重新协商新密钥。声明周期指的是每次重新协商之间的时段。
2. 对于 **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数），请指定 **Key Lifetime**（密钥生命周期）的乘数值（范围为 0-50；默认为 0）以确定身份验证计数。默认值 0 会禁用重新验证身份功能。

STEP 4 | 提交 IKE 加密配置文件。

单击 **OK**（确定）和 **Commit**（提交）。

STEP 5 | 将 IKE 加密配置文件附加到 IKE 网关配置。

请参阅配置网关的高级选项。

## 定义 *IPSec* 加密配置文件

IPSec 加密配置文件在 IKE 阶段 2 中被调用。它指定了当使用自动密钥 IKE 自动为 IKE SA 生成密钥时如何保护隧道内的数据。

STEP 1 | 创建新的 IPSec 配置文件。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密），然后选择 **Add**（添加）。
2. 输入新配置文件的 **Name**（名称）。
3. 选择想要应用以保护遍历整个隧道的数据的 **IPSec Protocol**（**IPSec** 协议）— ESP 或 AH。

   因为 *ESP* 提供连接机密性和身份验证，而 *AH* 仅提供身份验证，因此最佳做法是，选择通过 *AH*（身份验证标头）的 *ESP*（封装式安全措施负载）。
4. 单击 **Add**（添加），并为 ESP 选择 **Authentication**（身份验证）和 **Encryption**（加密）算法，然后为 AH 选择 **Authentication**（身份验证）算法，这样 IKE 对端设备可以协商用于在整个隧道内安全传输数据的密钥。

   如果您不确定 IKE 对等设备的支持内容，请按照安全性从高到低的顺序添加多个算法；对等设备会与最受支持的算法进行协商来建立隧道：

   - 加密 — **aes-256-gcm**、**aes-256-cbc**、**aes-192-cbc**、**aes-128-gcm**、**aes-128-ccm**（VM 系列防火墙不支持此选项）、**aes-128-cbc**、 **3des**、**des**



© 2019 Palo Alto Networks, Inc.

最佳做法是，选择对等设备支持的最强身份验证和加密算法。对于身份验证算法，请使用 *SHA-256* 或更高版本（对于长时间事务，首选为 *SHA-384* 或更高版本）。不得使用 *SHA-1*、*MD5* 或无。对于加密算法，请使用 *AES*； *DES* 和 *3DES* 很脆弱且易受攻击。

- 身份验证 — **sha512** 、**sha384**、**sha256**、**sha1** 和 **md5**。

STEP 2 | 选择 DH 组在 IKE 阶段 2 中用于 IPSec SA 协商。

从 **DH Group**（**DH 组**）中选择您想要使用的键强度：**group1**、**group2**、**group5**、**group14**、**group19**或 **group20**。要获得最高安全级别，请选择编号最大的组。

如果不想续订防火墙在 IKE 阶段 1 中创建的密钥，请选择 **no-pfs**（不进行完全向前保密）：防火墙会重复使用当前密钥进行 IPSec 安全关联 (SA) 协商。

STEP 3 | 指定密钥的持续时间 — 时间和流量容量。

使用时间和流量容量的组合可让您确保数据的安全性。

为有效密钥选择 **Lifetime**（生命周期）或时段，以秒、分钟、小时或天为单位（范围为 3 分钟到 365 天）。当指定的时间到期后，防火墙将重新协商一组新的密钥。

选择在其过后密钥必须重新协商的 **Lifesize**（生存期）或数据量。

STEP 4 | 提交 IPSec 配置文件。

单击 **OK**（确定）和 **Commit**（提交）。

STEP 5 | 将 IPSec 配置文件附加到 IPSec 隧道配置。

请参阅设置密钥交换。

# 建立 IPSec 隧道

IPSec 隧道配置可让您对遍历隧道的数据（IP 数据包）进行身份验证和/或加密。

如果设置防火墙使用支持基于策略的 VPN 的对等设备，必须定义代理 ID。支持基于策略的 VPN 的设备使用特定安全规则/策略或访问列表（源地址、目标地址和端口），允许感兴趣的流量通过 IPSec 隧道。在快速模式/IKE 阶段 2 协商过程中会引用这些规则，并且在该过程的第一或第二条消息中将其作为代理 ID 进行交换。因此，如果配置防火墙使用基于策略的 VPN 对等设备，对于成功的阶段 2 协商，必须定义代理 ID，以便使两个对等设备上的设置相同。如果尚未配置代理 ID，由于防火墙支持基于策略的 VPN，因此用作代理 ID 的默认值为源 IP 地址：0.0.0.0/0，目标 IP 地址：0.0.0.0/0，应用领域：任何领域；并且，当与对端设备交换这些值时，它会导致无法建立 VPN 连接。

STEP 1 | 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec 隧道**），然后 **Add**（添加）新隧道配置。

STEP 2 | 在 **General**（常规）选项卡上，输入隧道的 **Name**（名称）。

STEP 3 | 选择将用来建立 IPSec 隧道的 **Tunnel interface**（隧道接口）。

要创建新的隧道接口：

1. 选择 **Tunnel Interface**（隧道接口）> **New Tunnel Interface**（新建隧道接口）。（您还可以选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），并单击**Add**（添加）。）
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.2**。
3. 在 **Config**（配置）选项卡中，按下列方法选择 **Security Zone**（安全区域）列表以定义区域：

将信任区域用作隧道的终止点 — 请选择该区域。将隧道接口与在防火墙上为其输入数据包的面向外部接口相同的区域（和虚拟路由器）进行关联，减少创建区域间路由的需求。


© 2019 Palo Alto Networks, Inc.

或者，

为 **VPN** 隧道终止创建一个单独的区域（推荐）— 选择 **New Zone**（新区域），为新区域定义 **Name**（名称）（例如 vpn-corp），然后单击 **OK**（确定）。

1. 对于 **Virtual Router**（虚拟路由器），选择 **default**（默认）。
2. （可选）如果要为隧道接口分配 IPv4 地址，请选择 **IPv4**选项卡，**Add**（添加）IP 地址和子网掩码，如 10.31.32.1/32。
3. 单击 **OK**（确定）。

STEP 4 | （可选）在隧道接口上启用 IPv6。

1. 在 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道）> **IPv6** 上，选择 IPv6 选项卡。
2. 选择 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。

   此选项可允许通过 IPv4 IPSec 隧道路由 IPv6 流量，并在 IPv6 网络间提供加密。IPv6 流量先由 IPv4，然后由 ESP 加以封装。要将 IPv6 流量路由到隧道，可以使用静态路由到隧道、或使用 OSPFv3 或使用基于策略的转发 (PBF) 规则。
3. 以十六进制格式输入 64 位扩展唯一 **Interface Id**（接口 **ID**），如 00:26:08:FF:FE:DE:4E:29。默认情况下，防火墙将会使用从物理接口的 MAC 地址生成的 EUI-64。
4. 要将 IPv6 **Address**（地址）分配给隧道接口，请 **Add**（添加）IPv6 地址和前缀长度，如 2001:400:f00::1/64。如果未选择前缀，则需在地址文本框中完全指定分配给该接口的 IPv6 地址。
   1. 选择 **Use interface ID as host portion**（将接口 **ID** 作为主机部分使用）时，可将 IPv6 地址分配给将自身 ID 用作该地址的主机部分的接口。
   2. 选择 **Anycast**（任意播）以包括通过最近节点的路由。

STEP 5 | 设置密钥交换。

在 **General**（常规）选项卡中，配置以下类型的密钥交换之一：

设置自动密钥交换

1. 选择 IKE 网关。要设置 IKE 网关，请参阅设置 IKE 网关。
2. （可选）选择默认 IPSec 加密配置文件。要创建新的 IPSec 配置文件，请参阅定义 IPSec 加密配置文件。

设置手动密钥交换

1. 为本地防火墙指定 **Local SPI**（本地 **SPI**）。SPI 是一个 32 位十六进制指数，可将其添加到 IPSec 隧道的标头以帮助区分 IPSec 流量流；它用于创建建立 VPN 隧道所需的 SA。
2. 选择将成为隧道端点的 **Interface**（接口），且也可选择成为隧道端点的本地接口的 IP 地址。
3. 选择要使用的协议 — **AH**（AH）或 **ESP**（ESP）。
4. 对于 AH，选择 **Authentication**（身份验证）方法，并输入 **Key**（密钥）和 **Confirm Key**（确认密钥）。
5. 对于 ESP，选择 **Authentication**（身份验证）方法，并输入 **Key**（密钥）和 **Confirm Key**（确认密钥）。然后，选择 **Encryption**（加密）方法，并输入 **Key**（密钥）和 **Confirm Key**（确认密钥）（如需要）。
6. 指定远程对端设备的 **Remote SPI**（远程 **SPI**）。
7. 输入 **Remote Address**（远程地址），即远程对端设备的 IP 地址。

STEP 6 | 防止重放攻击。

当数据包被恶意拦截且拦截器重新传输时就会发生重放攻击。

在常规选项卡中，选中 **Show Advanced Options**（显示高级选项）复选框，然后选择 **Enable Replay Protection**（启用重放保护）以检测和消除重放攻击。



© 2019 Palo Alto Networks, Inc.

STEP 7 | （可选）保留服务类型标头以便优先考虑或处理 IP 数据包。

在 Show Advanced Options（显示高级选项）部分中，选择 **Copy TOS Header**（复制 **TOS** 标头）。这会将（服务类型）TOS 标头从封装数据包的内部 IP 标头复制到外部 IP 标头，以保留原始 TOS 信息。



如果隧道内有多个会话（每个会话使用不同的 *TOS* 值），复制 *TOS* 标头会导致 *IPSec* 数据包在送达时处于失序状态。

STEP 8 | （可选）选择 **Add GRE Encapsulation**（添加 **GRE** 封装）以通过 IPSec 启用 GRE。

当远程端点要求在 IPSec 启用流量前将该流量封装在 GRE 隧道中时，添加 GRE 封装。例如，某些实施要求在 IPSec 对多播流量加密之前，封装多播流量。当封装到 IPSec 中的 GRE 数据包具有与封装 IPSec 隧道相同的源 IP 地址和目标 IP 地址时，添加 GRE 封装。

STEP 9 | 启用隧道监控。



您必须向隧道接口分配一个 *IP* 地址才能进行监控。

选择此选项以便在隧道出现故障时向设备管理员发出警报并自动故障转移到另一个接口：

1. 选择 **Tunnel Monitor**（隧道监控）。
2. 在隧道的另一端指定 **Destination IP**（目标 **IP**）地址以确定此隧道是否正常工作。
3. 选择 **Profile**（配置文件）以确定在隧道出现故障后要采取的操作。要创建新的配置文件，请参阅定义隧道监控配置文件。

STEP 10 | 创建代理 ID 以标识 VPN 对等设备。

只有当 VPN 对等设备使用基于策略的 VPN 时才需要执行该步骤。

1. 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道），然后单击 **Add**（添加）。
2. 选择 **Proxy IDs**（代理 **ID**）选项卡。
3. 选择 **IPv4** 或 **Ipv6** 选项卡。
4. 单击 **Add**（添加），然后输入 **Proxy ID**（代理 **ID**）名称。
5. 输入 VPN 网关的 **Local**（本地）IP 地址或子网。
6. 输入 VPN 网关的 **Remote**（远程）IP 地址。
7. 选择 **Protocol**（协议）：
   - **Number** — 指定协议号（用于与第三方设备进行互操作）。
   - **Any**（任何）— 允许 TCP 和/或 UDP 流量。
   - **TCP** — 指定本地端口和远程端口号。
   - **UDP** — 指定本地端口和远程端口号。
8. 单击 **OK**（确定）。

STEP 11 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

# 设置隧道监控

要提供不间断的 VPN 服务，可以在防火墙上使用失效对等设备检测功能和隧道监控功能。还可以监控隧道的状态。这些监控任务在下面几个部分进行介绍：

- 定义隧道监控配置文件
- 查看隧道状态



© 2019 Palo Alto Networks, Inc.

## 定义隧道监控配置文件

隧道监控配置文件可让您验证 VPN 对等设备之间的连接；您可以配置隧道接口以指定的时间间隔 Ping 目标 IP 地址，并指定隧道之间通信中断后要采取的操作。

STEP 1 | 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Monitor**（监控）。可以使用默认隧道监控配置文件。

STEP 2 | 单击 **Add**（添加），然后输入配置文件的 **Name**（名称）。

STEP 3 | 选择无法访问目标 IP 地址时应采取的 **Action**（操作）。

- **Wait Recover**（等待恢复）— 防火墙等待隧道恢复。隧道将继续在路由决策中使用隧道接口，就像隧道仍处于活动状态。
- **Fail Over**（故障转移）— 强制流量转移到备份路径（如可用）。防火墙禁用隧道接口，从而禁用路由表中的任何路由使用接口。

在这两种情况下，防火墙尝试通过协商新的 IPSec 密钥加快恢复。

STEP 4 | 指定触发指定操作的 **Interval (sec)**（间隔（秒））和 **Threshold**（阈值）。

- **Threshold**（阈值）指定在执行指定操作之前等待的检测信号数（范围为 2-100；默认为 5）。
- **Interval (sec)**（间隔（秒））指定检测信号之间的时间（范围为 2-10，默认为 3）。

STEP 5 | 将监控配置文件附加到 IPSec 隧道配置。请参阅启用隧道监控。

## 查看隧道状态

隧道状态可让您知道是否已建立有效的 IKE 阶段 1 和阶段 2 SA，以及隧道接口是否已启用且是否可用于传递流量。

由于隧道接口是逻辑接口，因此它不能表示物理链路状态。因此，必须启用隧道监控，使隧道接口可以验证到 IP 地址的连接，并确定路径是否仍然可用。如果 IP 地址无法访问，防火墙将等待隧道恢复或故障转移。当执行故障转移时，现有的隧道断开，并触发路由更改建立新的隧道和重定向流量。

STEP 1 | 选择**Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）。

STEP 2 | 查看 **Tunnel Status**（隧道状态）。

- 绿色表示 IPSec SA 隧道有效。
- 红色表示 IPSec SA 不可用或已过期。

STEP 3 | 查看 **IKE Gateway Status**（**IKE** 网关状态）。

- 绿色表示 IKE 阶段 1 SA 有效。
- 红色表示该 IKE 阶段 1 SA 不可用或已过期。

STEP 4 | 查看 **Tunnel Interface Status**（隧道接口状态）。

- 绿色表示隧道接口已打开。
- 红色表示隧道接口已关闭，因为隧道监控已启用且状态为 DOWN。

要对尚未启动的 VPN 隧道进行故障排除，请参阅解释 VPN 错误消息。

# 启用/禁用，刷新或重新启动 IKE 网关或 IPSec 隧道

您可以启用、禁用、刷新或重新启动 IKE 网关或 VPN 隧道来简化故障诊断。



© 2019 Palo Alto Networks, Inc.

- 启用或禁用 IKE 网关或 IPSec 隧道
- 刷新和重新启动行为
- 刷新或重新启动 IKE 网关或 IPSec 隧道


## 启用或禁用 *IKE* 网关或 *IPSec* 隧道

您可以启用或禁用 IKE 网关或 IPSec 隧道来简化故障诊断。

- 启用或禁用 IKE 网关。
  1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Gateways**（**IKE** 网关），然后选择您要启用或禁用的网关。
  2. 在屏幕底部单击 **Enable**（启用）或 **Disable**（禁用）。

- 启用或禁用 IPSec 隧道。
  1. 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道），然后选择您要启用或禁用的隧道。
  2. 在屏幕底部单击 **Enable**（启用）或 **Disable**（禁用）。

## 刷新和重新启动行为

您可以刷新或重新启动 IKE 网关或 IPSec 隧道。IKE 网关和 IPSec 隧道的刷新和重新启动行为如下所示：

| 阶段 | 刷新 | 重新启动 |
|---|---|---|
| IKE 网关（IKE 阶段 1） | 为所选 IKE 网关更新屏幕上的统计信息。<br>等同于在 CLI 中发送第二个 `show` 命令（在初始 `show` 命令之后）。 | 重新启动所选 IKE 网关。<br>**IKEv2**：同时重新启动所有关联的子 IPSec 安全关联 (SA)。<br>**IKEv1**：不重新启动关联的 IPSec SA。<br>重新启动会干扰所有现有会话。<br>等同于在 CLI 中发送 **`clear`**、**`test`**、 **`show`** 命令序列。 |
| IPSec 隧道（IKE 阶段 2） | 为所选 IPSec 隧道更新屏幕上的统计信息。<br>等同于在 CLI 中发送第二个 `show` 命令（在初始 `show` 命令之后）。 | 重新启动 IPSec 隧道。<br>重新启动会干扰所有现有会话。<br>等同于在 CLI 中发送 **`clear`**、**`test`**、 **`show`** 命令序列。 |

## 刷新或重新启动 *IKE* 网关或 *IPSec* 隧道

请注意，重新启动 IKE 网关的结果取决于它是 IKEv1 还是 IKEv2。请参阅 IKE 网关（IKEv1 和 IKEv2）和 IPSec 隧道的刷新和重新启动行为。

- 刷新或重新启动 IKE 网关。
  1. 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道），然后为您要刷新或重新启动的网关选择隧道。
  2. 在针对该隧道的行内，在“状态”列中单击 **IKE Info**（**IKE** 信息）。
  3. 在 IKE 信息屏幕的底部，单击您想执行的操作：
     - **Refresh**（刷新）— 更新屏幕上的统计信息。


© 2019 Palo Alto Networks, Inc.

- **Restart**（重新启动）— 清除 SA，因此 IKE 协商重新开始和隧道重新创建前会丢弃流量。

- 刷新或重新启动 IPSec 隧道。

  因为使用隧道监视器监控隧道状态，或使用外部网络监视器监控通过 IPSec 隧道的网络连接，因此您可以确定隧道需要刷新或重新启动。

  1. 选择 **Network**（网络）> **IPSec TunnelsIPSec** 隧道），然后选择您要刷新或重新启动的隧道。
  2. 在针对该隧道的行内，在"状态"列中单击 **Tunnel Info**（隧道信息）。
  3. 在隧道信息屏幕的底部，单击您想执行的操作：
     - **Refresh**（刷新）— 更新屏幕上的统计信息。
     - **Restart**（重新启动）— 清除 SA，因此 IKE 协商重新开始和隧道重新创建前会丢弃流量。

# 测试 VPN 连接

执行此任务以测试 VPN 连接。

STEP 1 | 通过 Ping 隧道间的某台主机或使用以下 CLI 命令启动 IKE 阶段 1：

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | 输入以下命令测试 IKE 阶段 1 是否已设置：

```
show vpn ike-sa gateway <gateway_name>
```

检查输出框中是否显示安全关联。如果没有显示，请查看系统日志消息以解释失败的原因。

STEP 3 | 通过 Ping 隧道间的某台主机或使用以下 CLI 命令启动 IKE 阶段 2：

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | 输入以下命令测试 IKE 阶段 2 是否已设置：

```
show vpn ipsec-sa tunnel <tunnel_name>
```

检查输出框中是否显示安全关联。如果没有显示，请查看系统日志消息以解释失败的原因。

STEP 5 | 要查看 VPN 流量流信息，请使用以下命令：

```
show vpn flow
total tunnels configured:               1
filter - type IPSec, state any

total IPSec tunnel configured:        1
total IPSec tunnel shown:                1

name                     id      state      local-ip       peer-ip
       tunnel-i/f
------------------------------------------------------------------------------------
vpn-to-siteB       5       active    100.1.1.1     200.1.1.1     tunnel.41
```



© 2019 Palo Alto Networks, Inc.

# 解释 VPN 错误消息

下表列出了系统日志中记录的一部分常见的 VPN 错误消息。

**表 6: VPN 问题的 Syslog 错误消息**

| 如果错误如下： | 请尝试以下操作： |
| --- | --- |
| `IKE phase-1 negotiation is failed as initiator, main mode.Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`<br>**或者**<br>`IKE phase 1 negotiation is failed.Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]` | • 确认 IKE 网关配置中每个 VPN 对等设备的公共 IP 地址准确。<br>• 确认可以 ping IP 地址且路由问题不会导致连接出现故障。 |
| `Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...`<br>**或者**<br>`IKE phase-1 negotiation is failed.Unable to process peer's SA payload.` | 检查 IKE 加密配置文件配置，确认两端都建议进行常用加密、身份验证和 DH 组建议。 |
| `pfs group mismatched:my:2peer:0`<br>**或者**<br>`IKE phase-2 negotiation failed when processing SA payload.No suitable proposal found in peer's SA payload.` | 检查 IPSec 加密配置文件配置以确认：<br>• 在两个 VPN 对等设备上已启用或禁用 pfs<br>• 每个对等设备建议的 DH 组至少拥有一个共同的 DH 组 |
| `IKE phase-2 negotiation failed when processing Proxy ID.Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.` | 位于其中一端的 VPN 对等设备使用基于策略的 VPN。必须在 Palo Alto Networks 防火墙上配置代理 ID。请参阅创建代理 ID 以标识 VPN 对端设备。 |


© 2019 Palo Alto Networks, Inc.

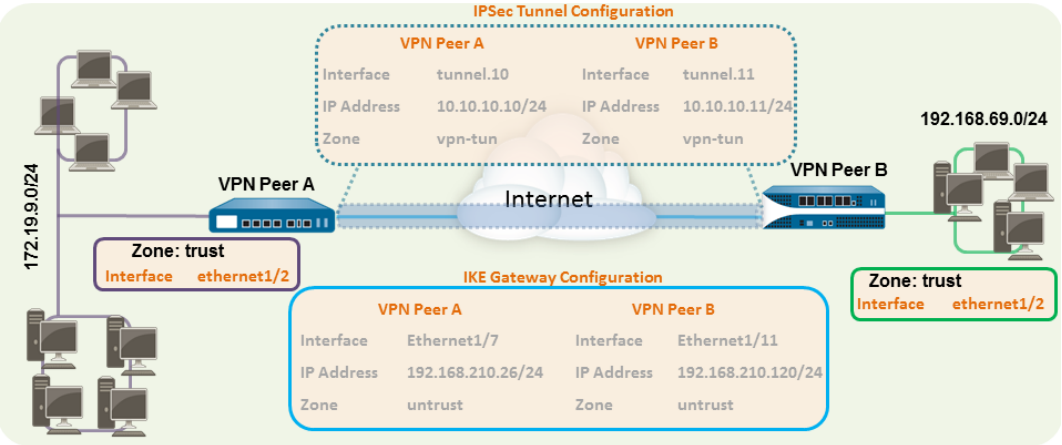
# 站点到站点 VPN 快速配置

以下部分提供了配置一些常见 VPN 部署的说明：

- 使用静态路由的站点到站点 VPN
- 使用 OSPF 的站点与站点 VPN
- 使用静态和动态路由的站点到站点 VPN

## 使用静态路由的站点到站点 VPN

下例显示了使用静态路由的两个站点之间的 VPN 连接。不使用动态路由，VPN 对等设备 A 和 VPN 对等设备 B 上的隧道接口不需要 IP 地址，因为防火墙自动将隧道接口用作在站点之间路由流量的下一个跃点。但是，要启用隧道监控，要为每个隧道接口分配一个静态 IP 地址。




STEP 1 | 配置第 3 层接口。

此接口用于 IKE 阶段 1 隧道。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择要为 VPN 配置的接口。
2. 从 **Interface Type**（接口类型）中选择 **Layer3**（第三层）。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (添加)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.210.26/24。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 192.168.210.26/24

   VPN 对等设备 B 配置如下：



© 2019 Palo Alto Networks, Inc.

- **Interface**（接口）— ethernet1/11
- **Security Zone**（安全区域）— 不可信
- **Virtual Router**（虚拟路由器）— 默认
- **IPv4** — 192.168.210.120/24

STEP 2 | 创建隧道接口，并将其附加到虚拟路由器和安全区域。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.1**。
3. 在 **Config**（配置）选项卡中，按下列方法展开 **Security Zone**（安全区域）以定义区域：
   - 要将信任区域用作隧道的终止点，请选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 *vpn-tun*），然后单击 **OK**（确定）。
4. 选择 **Virtual Router**（虚拟路由器）。
5. （可选）要向隧道接口分配 IP 地址，选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码。

   使用静态路由，隧道接口不需要 IP 地址。对于发往指定子网/IP 地址的流量，隧道接口将自动成为下一个跃点。如果要启用隧道监控，请考虑添加 IP 地址。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— tunnel.10
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 172.19.9.2/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— tunnel.11
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 192.168.69.2/24

STEP 3 | 在虚拟路由器上，将静态路由配置为目标子网。

1. 选择 **Network**（网络）> **Virtual Router**（虚拟路由器）并单击在上述步骤中定义的路由器。
2. 选择 **Static Route**（静态路由），并单击 **Add**（添加），然后输入新路由以访问子网（位于隧道的另一端）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Destination**（目标）— 192.168.69.0/24
   - **Interface**（接口）— tunnel.10

   VPN 对等设备 B 配置如下：
   - **Destination**（目标）— 172.19.9.0/24
   - **Interface**（接口）— tunnel.11

STEP 4 | 设置加密配置文件（IKE 加密配置文件用于阶段 1 和 IPSec 加密配置文件用于阶段 2）。

在两个对等设备上完成此任务，并确保设置相同的值。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Crypto**（**IKE** 加密）。在本例中，我们使用默认配置文件。


© 2019 Palo Alto Networks, Inc.

2. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密）。在本例中，我们使用默认配置文件。

STEP 5 | 设置 IKE 网关。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Gateway**（**IKE** 网关）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Local IP address**（本地 **IP** 地址）— 192.168.210.26/24
   - **Peer IP type/address**（对端设备 **IP** 类型/地址）— static/192.168.210.120
   - **Preshared keys**（预共享密钥）— 输入一个值
   - **Local identification**（本地标识）— 无；这意味着将使用本地 IP 地址作为本地标识值。
   - VPN 对等设备 B 配置如下：
   - **Interface**（接口）— ethernet1/11
   - **Local IP address**（本地 **IP** 地址）— 192.168.210.120/24
   - **Peer IP type/address**（对端设备 **IP** 类型/地址）— 静态/192.168.210.26
   - **Preshared keys**（预共享密钥）— 输入与对端设备 A 相同的值
   - **Local identification**（本地标识）— 无
3. 选择 **Advanced Phase 1 Options**（高级阶段 **1** 选项），然后选择先前创建用于 IKE 阶段 1 的 IKE 加密配置文件。

STEP 6 | 建立 IPSec 隧道。

1. 选择**Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Tunnel Interface**（隧道接口）— tunnel.10
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在步骤 4 中定义的 IPSec 加密配置文件。

   VPN 对等设备 B 配置如下：

   - **Tunnel Interface**（隧道接口）— tunnel.11
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在步骤 4 中定义的 IPSec 加密。
3. （可选）选择 **Show Advanced Options**（显示高级选项），并选择 **Tunnel Monitor**（隧道监控），然后指定为验证连接要 ping 的目标 IP 地址。通常，使用 VPN 对等设备的隧道接口 IP 地址。
4. （可选）要定义在建立连接失败后要采取的操作，请参阅定义隧道监控配置文件。

STEP 7 | 创建策略以允许站点（子网）之间的流量。

1. 选择 **Policies**（策略）> **Security**（安全）。
2. 创建规则以允许不可信区域与 vpn-tun 区域，以及 vpn-tun 区域与不可信区域之间的流量，流量来源于指定的源和目标 IP 地址。

STEP 8 | 提交任何挂起的配置更改。

单击 **Commit**（提交）。

STEP 9 | 测试 VPN 连接。

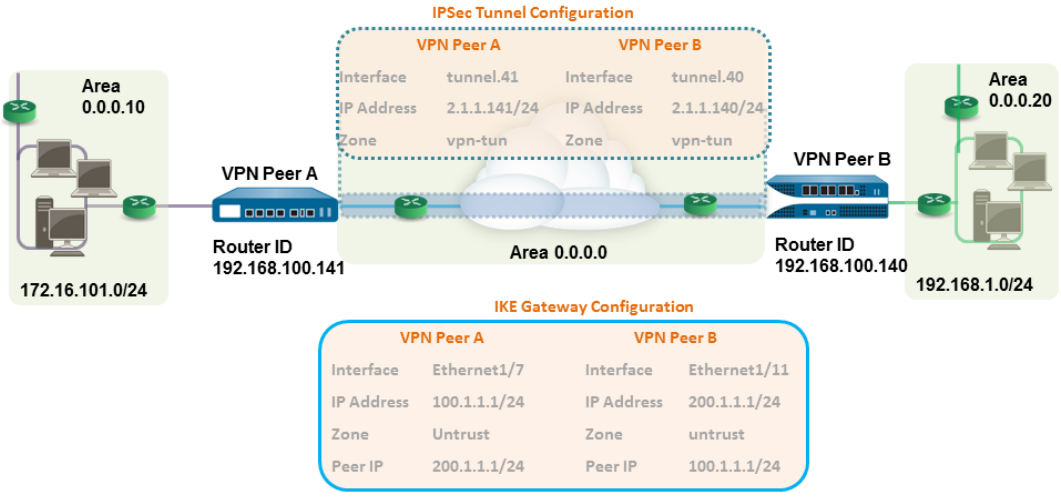


© 2019 Palo Alto Networks, Inc.

另请参阅查看隧道状态。

# 使用 OSPF 的站点与站点 VPN

在本例中，每个站点都使用 OSPF 动态路由流量。静态分配每个 VPN 对等设备的隧道 IP 地址，并用作在两个站点之间路由流量的下一个跃点。




STEP 1 | 在每个防火墙上配置第 3 层接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择要为 VPN 配置的接口。
2. 从 **Interface Type**（接口类型）列表中选择 **Layer3**（第三层）。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）列表中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (添加)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.210.26/24。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 100.1.1.1/24

   VPN 对等设备 B 配置如下：

   - **Interface**（接口）— ethernet1/11
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 200.1.1.1/24

STEP 2 | 创建隧道接口，并将其附加到虚拟路由器和安全区域。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），并单击 **Add**（添加）。


© 2019 Palo Alto Networks, Inc.

2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.11**。
3. 在 **Config**（配置）选项卡中，按下列方法展开 **Security Zone**（安全区域）以定义区域：
   - 要将信任区域用作隧道的终止点，请选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 vpn-tun），然后单击 **OK**（确定）。
4. 选择 **Virtual Router**（虚拟路由器）。
5. 要向隧道接口分配 IP 地址，请选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码/前缀，如 172.19.9.2/24。

   使用此 IP 地址作为将流量路由到隧道的下一个跃点 IP 地址，且也可用于监控隧道的状态。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— tunnel.41
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **Ipv4** — 2.1.1.141/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）—tunnel.40
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4**（IPv4）— 2.1.1.140/24

STEP 3 | 设置加密配置文件（IKE 加密配置文件用于阶段 1 和 IPSec 加密配置文件用于阶段 2）。

在两个对等设备上完成此任务，并确保设置相同的值。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Crypto**（**IKE** 加密）。在本例中，我们使用默认配置文件。
2. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密）。在本例中，我们使用默认配置文件。

STEP 4 | 在虚拟路由器上设置 OSPF 配置，并将 OSPF 区域连接到防火墙的相应接口。

有关防火墙上可用 OSPF 选项的详细信息，请参阅配置 OSPF。

当两个以上的 OSPF 路由器需要交换路由信息时，可将广播用作链路类型。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择默认路由器或添加新路由器。
2. 选择 **OSPF**（对于 IPv4）或 **OSPFv3**（对于 Ipv6），然后选择 **Enable**（启用）。
3. 在本例中，VPN 对等设备 A 的 OSPF 配置如下：
   - **Router ID**（路由器 **ID**）：192.168.100.141
   - **Area ID**（区域 **ID**）：0.0.0.0，分配给 tunnel.1 接口，链路类型：p2p
   - **Area ID**（区域 **ID**）：0.0.0.10，分配给接口 Ethernet1/1，链路类型：广播

   VPN 对等设备 B 的 OSPF 配置如下：
   - **Router ID**（路由器 **ID**）：192.168.100.140
   - **Area ID**（区域 **ID**）：0.0.0.0，分配给 tunnel.1 接口，链路类型：p2p
   - **Area ID**（区域 **ID**）：0.0.0.20，分配给接口 Ethernet1/15，链路类型：广播

STEP 5 | 设置 IKE 网关。



© 2019 Palo Alto Networks, Inc.

本示例对于两个 VPN 对等设备使用静态 IP 地址。通常，企业办公室使用静态配置的 IP 地址，分支机构使用的 IP 地址可以是动态 IP 地址；动态 IP 地址最不适合用于配置稳定服务，如 VPN。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Gateway**（**IKE** 网关）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Local IP address**（本地 **IP** 地址）— 100.1.1.1/24
   - **Peer IP address**（对端设备 IP 地址）— 200.1.1.1/24
   - **Preshared keys**（预共享密钥）— 输入一个值

   VPN 对等设备 B 配置如下：

   - **Interface**（接口）— ethernet1/11
   - **Local IP address**（本地 **IP** 地址）— 200.1.1.1/24
   - **Peer IP address**（对端设备 **IP** 地址）— 100.1.1.1/24
   - **Preshared keys**（预共享密钥）— 输入与对端设备 A 相同的值
3. 选择先前创建用于 IKE 阶段 1 的 IKE 加密配置文件。

STEP 6 | 建立 IPSec 隧道。

1. 选择**Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Tunnel Interface**（隧道接口）—tunnel.41
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。

   VPN 对等设备 B 配置如下：

   - 隧道接口 — tunnel.40
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。
3. 选择 **Show Advanced Options**（显示高级选项），并选择 **Tunnel Monitor**（隧道监控），然后指定为验证连接要 ping 的目标 IP 地址。
4. 要定义在建立连接失败后要采取的操作，请参阅定义隧道监控配置文件。

STEP 7 | 创建策略以允许站点（子网）之间的流量。

1. 选择 **Policies**（策略）> **Security**（安全）。
2. 创建规则以允许不可信区域与 vpn-tun 区域，以及 vpn-tun 区域与不可信区域之间的流量，流量来源于指定的源和目标 IP 地址。

STEP 8 | 验证 OSPF 邻接并从 CLI 路由。

验证两个防火墙可以相互看作完整状态的邻居。同时确认 VPN 对等设备的隧道接口的 IP 地址和 OSPF 路由器 ID。在每个 VPN 对等设备上使用以下 CLI 命令。

- `show routing protocol ospf neighbor`


© 2019 Palo Alto Networks, Inc.

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination              nexthop              metric flags      age   interface          next-AS
2.1.1.0/24               0.0.0.0                  10   Oi       6760  tunnel.41
172.16.101.0/24          0.0.0.0                  10   Oi       6854  ethernet1/1
192.168.1.0/24           2.1.1.140                20 A Oo       6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination              nexthop              metric flags      age   interface
2.1.1.0/24               0.0.0.0              10       Oi       20033 tunnel.40
172.16.101.0/24          2.1.1.141            20     AOo        6896  tunnel.40
192.168.1.0/24           0.0.0.0              10       Oi       8058  ethernet1/15
total routes shown: 3
```

STEP 9 | 测试 VPN 连接。

请参阅设置隧道监控和查看隧道状态。

# 使用静态和动态路由的站点到站点 VPN

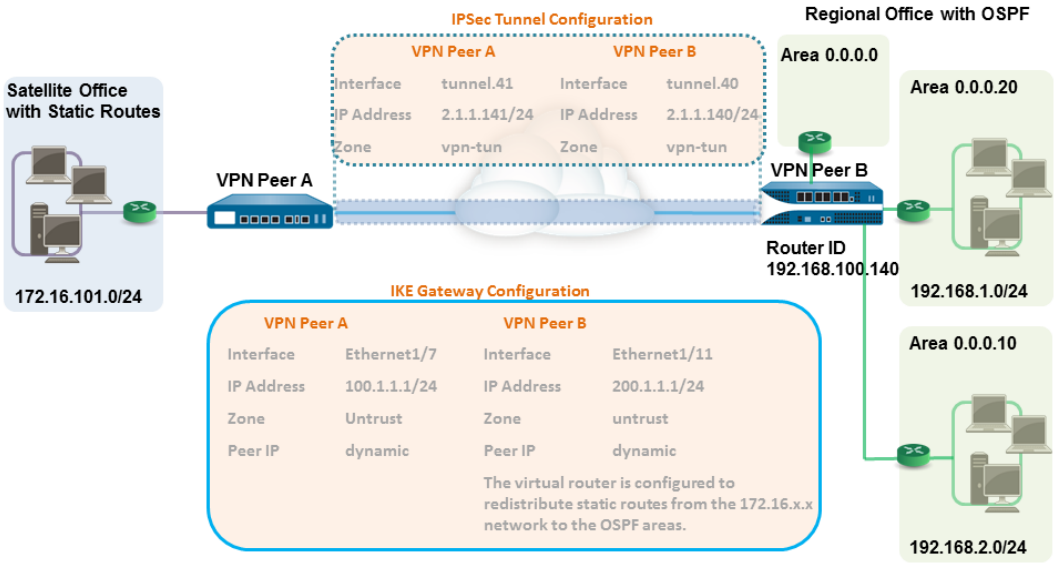
在本例中，一个站点使用静态路由，另一个站点使用 OSPF。当两个位置之间的路由协议不相同时，必须使用静态 IP 地址配置每个防火墙上的隧道接口。然后，要允许交换路由信息，必须使用重新分发配置文件配



© 2019 Palo Alto Networks, Inc.

置同时参与静态和动态路由过程的防火墙。配置重新分发配置文件，启用虚拟路由器重新分发和筛选协议之间的路由 — 静态路由、连接路由和主机 — 从静态自治系统到 OSPF 自治系统。如果不配置此重新分发配置文件，则其拥有各项协议功能，并且不会与在同一虚拟路由器上运行的其他协议交换任何路由信息。

在本例中，卫星办公室拥有静态路由，且会将发往 192.168.x.x 网络的所有流量路由到 tunnel.41。VPN 对端设备 B 上的虚拟路由器同时参与静态和动态路由过程，并使用重新分发配置文件进行配置，以将静态路由传播（导出）到 OSPF 自治系统。




STEP 1 | 在每个防火墙上配置第 3 层接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择要为 VPN 配置的接口。
2. 从 **Interface Type**（接口类型）中选择 **Layer3**（第三层）。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (添加)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.210.26/24。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 100.1.1.1/24

   VPN 对等设备 B 配置如下：

   - **Interface**（接口）— ethernet1/11
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 200.1.1.1/24


© 2019 Palo Alto Networks, Inc.

STEP 2 | 设置加密配置文件（IKE 加密配置文件用于阶段 1 和 IPSec 加密配置文件用于阶段 2）。

在两个对等设备上完成此任务，并确保设置相同的值。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Crypto**（**IKE** 加密）。在本例中，我们使用默认配置文件。
2. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密）。在本例中，我们使用默认配置文件。

STEP 3 | 设置 IKE 网关。

使用预共享密钥，要在建立 IKE 阶段 1 隧道时添加身份验证检查，可以设置本地和对等设备标识属性，以及在 IKE 协商过程中匹配的相应值。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IKE Gateway**（**IKE** 网关）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Local IP address**（本地 **IP** 地址）— 100.1.1.1/24
   - **Peer IP type**（对端设备 **IP** 类型）— 动态
   - **Preshared keys**（预共享密钥）— 输入一个值
   - **Local identification**（本地标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对端设备 A 的值。
   - **Peer identification**（对端设备标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对端设备 B 的值。

   VPN 对等设备 B 配置如下：

   - **Interface**（接口）— ethernet1/11
   - **Local IP address**（本地 **IP** 地址）— 200.1.1.1/24
   - **Peer IP address**（对端设备 **IP** 地址）— 动态
   - **Preshared keys**（预共享密钥）— 输入与对端设备 A 相同的值
   - **Local identification**（本地标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对端设备 B 的值
   - **Peer identification**（对端设备标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对端设备 A 的值
3. 选择先前创建用于 IKE 阶段 1 的 IKE 加密配置文件。

STEP 4 | 创建隧道接口，并将其附加到虚拟路由器和安全区域。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀，如 **.41**。
3. 在 **Config**（配置）选项卡中，按下列方法展开 **Security Zone**（安全区域）以定义区域：
   - 要将信任区域用作隧道的终止点，请选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 *vpn-tun*），然后单击 **OK**（确定）。
4. 选择 **Virtual Router**（虚拟路由器）。
5. 要向隧道接口分配 IP 地址，请选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码/前缀，如 172.19.9.2/24。

   使用此 IP 地址将流量路由到隧道，并监控隧道的状态。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— tunnel.41



© 2019 Palo Alto Networks, Inc.

- **Security Zone**（安全区域）— vpn_tun
- **Virtual Router**（虚拟路由器）— 默认
- **Ipv4** — 2.1.1.141/24

VPN 对等设备 B 配置如下：

- **Interface**（接口）— tunnel.42
- **Security Zone**（安全区域）— vpn_tun
- **Virtual Router**（虚拟路由器）— 默认
- **IPv4**（IPv4）— 2.1.1.140/24

STEP 5 | 指定在 192.168.x.x 网络中将流量路由到目标的接口。

1. 在 VPN 对等设备 A 上，选择虚拟路由器。
2. 选择 **Static Routes**（静态路由），然后 **Add**（添加）tunnel.41 作为在 192.168.x.x 网络中将流量路由到 **Destination**（目标）的**Interface**（接口）。

STEP 6 | 在虚拟路由器上设置静态路由和 OSPF 配置，并将 OSPF 区域连接到防火墙的相应接口。

1. 在 VPN 对端设备 B 上，选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择默认路由器或添加新路由器。
2. 选择 **Static Routes**（静态路由），然后 **Add**（添加）隧道 IP 地址作为在 172.168.x.x. 网络中路由流量的下一个跃点。

   分配所需的路由跃点数；使用较低的值，使得转发表中的路由选择具有更高的优先级。
3. 选择 **OSPF**（对于 IPv4）或 **OSPFv3**（对于 Ipv6），然后选择 **Enable**（启用）。
4. 在本例中，VPN 对等设备 B 的 OSPF 配置如下：
   - 路由器 ID：192.168.100.140
   - 区域 ID：0.0.0.0，分配给接口接口 Ethernet 1/12，链路类型：广播
   - 区域 ID：0.0.0.10，分配给接口 Ethernet1/1，链路类型：广播
   - 区域 ID：0.0.0.20，分配给接口 Ethernet1/15，链路类型：广播

STEP 7 | 创建重新分发配置文件以便将静态路由插入 OSPF 自治系统。

1. 在 VPN 对等设备 B 上创建重新分发配置文件。
   1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择上面使用的路由器。
   2. 选择 **Redistribution Profiles**（重新分发配置文件），然后单击 **Add**（添加）。
   3. 输入配置文件的名称，并选择 **Redist**（重新分发），然后指定 **Priority**（优先级）值。如果已配置多个配置文件，则首先匹配优先级值最低的配置文件。
   4. 将 **Source Type**（源类型）设置为 **static**（静态），然后单击 **OK**（确定）。在步骤 6 中定义的静态路由将用于重新分发。
2. 将静态路由插入 OSPF 系统。
   1. 选择 **OSPF** > **Export Rules**（导出规则）（对于 IPv4）或 **OSPFv3** > **Export Rules**（导出规则）（对于 IPv6）。
   2. 单击 **Add**（添加），然后选择刚创建的重新分发配置文件。
   3. 选择将外部路由插入 OSPF 系统的方式。默认选项 **Ext2** 仅使用外部跃点数计算路由的总成本。要同时使用内部和外部 OSPF 跃点数，请使用 **Ext1**。
   4. 为插入 OSPF 系统的路由分配 **Metric**（跃点数）（成本值）。此选项可让您在将路由插入 OSPF 系统时更改跃点数。
   5. 单击 **OK**（确定）。

STEP 8 | 建立 IPSec 隧道。

1. 选择**Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。


© 2019 Palo Alto Networks, Inc.

在本例中，VPN 对等设备 A 配置如下：

- **Tunnel Interface**（隧道接口）—tunnel.41
- **Type**（类型）— 自动密钥
- **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
- **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。

VPN 对等设备 B 配置如下：

- 隧道接口 — tunnel.40
- **Type**（类型）— 自动密钥
- **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
- **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。

3. 选择 **Show Advanced Options**（显示高级选项），并选择 **Tunnel Monitor**（隧道监控），然后指定为验证连接要 ping 的目标 IP 地址。
4. 要定义在建立连接失败后要采取的操作，请参阅定义隧道监控配置文件。

STEP 9 | 创建策略以允许站点（子网）之间的流量。

1. 选择 **Policies**（策略）> **Security**（安全）。
2. 创建规则以允许不可信区域与 vpn-tun 区域，以及 vpn-tun 区域与不可信区域之间的流量，流量来源于指定的源和目标 IP 地址。

STEP 10 | 验证 OSPF 邻接并从 CLI 路由。

验证两个防火墙可以相互看作完整状态的邻居。同时确认 VPN 对等设备的隧道接口的 IP 地址和 OSPF 路由器 ID。在每个 VPN 对等设备上使用以下 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**



© 2019 Palo Alto Networks, Inc.

以下是每个 VPN 对等设备上的输出示例。

```
VPN PeerA

destination            next hop        metric  flags   age     interface       next-AS
192.168.1.0/24         2.1.1.141       20      A S             tunnel.41
192.168.2.0/24         2.1.1.141       20      A S             tunnel.41
172.16.101.0/24        0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24           2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination            next hop        metric  flags   age     interface       next-AS
192.168.1.0/24         0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24         0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24        2.1.1.140       20      A H             tunnel.40
2.1.1.141/24           2.1.1.140       10      A C             tunnel.40
```

## STEP 11 | 测试 VPN 连接。

请参阅设置隧道监控和查看隧道状态。



© 2019 Palo Alto Networks, Inc.

# 大规模 *VPN (LSVPN)*

Palo Alto Networks 上的 GlobalProtect 大规模 VPN（LSVPN）特点在于简化了传统集线器和和星形 VPNs的配置，使你只需要配置远程卫星所需的最少配置，快速部署几个分公司之间的企业网络 .此解决方案使用证书对防火墙进行验证和使用 IPSec 保护数据。

LSVPN 用来启用 Palo Alto Networks 防火墙之间的站点到站点 VPN。要设置 Palo Alto Networks 防火墙和其他设备之间的站点到站点 VPN，请参阅VPN 。

以下主题介绍了 LSVPN 组件以及设置它们启用 Palo Alto Networks 防火墙之间站点到站点 VPN 服务的方法：

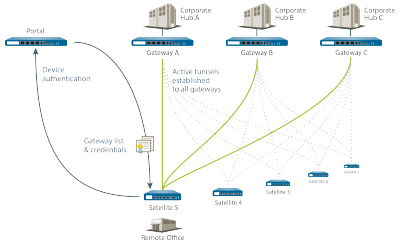
- LSVPN 概述
- 为 LSVPN 创建接口和区域
- 在 GlobalProtect LSVPN 组件之间启用 SSL
- 配置门户以验证卫星
- 为 LSVPN 配置 GlobalProtect 网关
- 为 LSVPN 配置 GlobalProtect 门户
- 准备卫星加入 LSVPN
- 验证 LSVPN 配置
- LSVPN 快速配置

# LSVPN 概述

GlobalProtect 提供了用于管理从远程站点安全访问企业资源的完整基础架构。该基础架构包含下列组件：

- **GlobalProtect** 门户 — 提供针对 GlobalProtect LSVPN 基础架构的管理功能。组成 GlobalProtect LSVPN 的每颗卫星都会收到门户的配置信息，包括用来将卫星（星型）连接到网关（中心）的配置信息。您可以在 Palo Alto Networks 任意下一代防火墙的接口上配置该门户。
- **GlobalProtect** 网关 — 为卫星连接提供隧道终结点的 Palo Alto Networks 防火墙。卫星访问的资源在网关上受到安全策略保护。它不需要单独的门户和网关；可以将一个防火墙同时用作门户和网关。
- **GlobalProtect** 卫星 — 远程站点的 Palo Alto Networks 防火墙，用来与公司办公室的网关建立 IPSec 隧道以便安全访问集中资源。卫星防火墙只需进行最少配置便可在添加新站点时快速轻松扩展 VPN。

下图说明了 GlobalProtect LSVPN 组件一起工作的原理。






© 2019 Palo Alto Networks, Inc.

# 为 LSVPN 创建接口和区域

您必须为 LSVPN 基础架构配置下列接口和区域：

- **GlobalProtect portal**（**GlobalProtect** 门户）— 需要 GlobalProtect 卫星连接的第 3 层接口。如果门户和网关位于同一防火墙，则可使用同一接口。门户必须位于可从分支机构访问的区域内。
- **GlobalProtect gateways**（**GlobalProtect** 网关）— 需要三个接口：区域中可通过远程卫星访问的第 3 层接口，信任区域中用于连接到受保护资源的内部接口和用于终止与卫星的 VPN 隧道的逻辑隧道接口。与其他站点到站点 VPN 解决方案不同，GlobalProtect 网关只需要一个隧道接口用来与所有远程卫星建立隧道连接（点对多点）。如果计划使用动态路由，则必须为隧道接口分配 IP 地址。GlobalProtect 支持隧道接口的 IPv6 和 IPv4 寻址。
- **GlobalProtect satellites**（**GlobalProtect** 卫星）— 需要一个隧道接口用来与远程网关（最多 25 个网关）建立 VPN。如果计划使用动态路由，则必须为隧道接口分配 IP 地址。GlobalProtect 支持隧道接口的 IPv6 和 IPv4 寻址。

有关门户、网关和卫星的详细信息，请参阅 LSVPN 概述。

STEP 1 | 配置第 3 层接口。

门户、每个网关和卫星都需要第 3 层接口在站点之间路由流量。

如果网关和门户位于同一防火墙，则可以同时为两个组件使用一个接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择要为 GlobalProtect LSVPN 配置的接口。
2. 从 **Interface Type**（接口类型）下列列表中选择 **Layer3**（第 3 层）。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）下拉列表中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 为接口分配一个 IP 地址：
   - 对于 IPv4 地址，选择 **IPv4**，**Add**（添加）IP 地址和子网掩码并分配给接口，例如 203.0.11.100/24。
   - 对于 IPv6 地址，选择 **IPv6**，**Enable IPv6 on the interface**（在接口上启用 **IPv6**），**Add**（添加）IP 地址和子网掩码并分配给接口，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 要保存接口配置，请单击 **OK**（确定）。

STEP 2 | 在承载 GlobalProtect 网关的防火墙上，配置用于终止 GlobalProtect 卫星所建立 VPN 隧道的逻辑隧道接口。

除非您计划使用动态路由，否则无需为隧道接口分配 *IP* 地址。但是，为隧道接口分配 *IP* 地址有助于对连通性问题进行故障排除。

确保在 *VPN* 隧道终止的区域内启用用户标识。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.2**。
3. 在 **Config**（配置）选项卡上，按下列方法展开 **Security Zone**（安全区域）下拉列表以定义区域：


© 2019 Palo Alto Networks, Inc.

- 要将信任区域用作隧道的终止点，请从下拉列表中选择该区域。
- （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 *lsvpn-tun*），选中 **Enable User Identification**（启用用户标识）复选框，然后单击 **OK**（确定）。

4. 选择 **Virtual Router**（虚拟路由器）。
5. （可选）要为隧道接口分配 IP 地址：
   - 对于 IPv4 地址，选择 **IPv4**，**Add**（添加）IP 地址和子网掩码并分配给接口，例如 203.0.11.100/24。
   - 对于 IPv6 地址，选择 **IPv6**，**Enable IPv6 on the interface**（在接口上启用 **IPv6**），**Add**（添加）IP 地址和子网掩码并分配给接口，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 要保存接口配置，请单击 **OK**（确定）。

STEP 3 | 如果已为 VPN 连接的隧道终止单独创建区域，则需创建安全策略以便在 VPN 区域和信任区域间启用通信流。

例如，策略规则可在 *lsvpn-tun* 域和 *L3-Trust* 域之间启用流量。

STEP 4 | 提交更改。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 在 GlobalProtect LSVPN 组件之间启用 SSL

GlobalProtect 组件间的所有交互均通过 SSL/TLS 连接实现。因此，在配置每个组件前须生成并/或安装必要的证书，以便在每个组件的配置中引用相应的证书和/或证书配置文件。下列章节描述了针对各类 GlobalProtect 证书所支持的证书部署方法、描述和最佳实践准则，同时提供了生成和部署必要证书的相关指导：

- 关于证书部署
- 将服务器证书部署到 GlobalProtect LSVPN 组件
- 通过 SCEP 部署客户端证书到 GlobalProtect 卫星

## 关于证书部署

可以通过两种基本方法为 GlobalProtect LSVPN 部署证书：

- **Enterprise Certificate Authority**（企业证书颁发机构）— 如果拥有自己的企业证书颁发机构，可以使用此内部 CA 为 GlobalProtect 门户签发中间 CA 证书，然后用来为 GlobalProtect 网关和卫星签发证书。您也可以将 GlobalProtect 门户配置为简单证书注册协议 (SCEP) 客户端，为 GlobalProtect 卫星颁发客户端证书。
- **Self-Signed Certificates**（自签名证书）— 可以在防火墙上生成自签名根 CA 证书，并将其用来为门户、网关和卫星签发服务器证书。当使用自签名根 CA 证书时，作为最佳实践，在门户上创建自签名根 CA 证书，并将其用来为网关和卫星签服务器证书。这样，可以将用于证书签名的私钥保存在门户。

## 将服务器证书部署到 GlobalProtect LSVPN 组件

GlobalProtect LSVPN 组件使用 SSL/TLS 进行相互身份验证。在部署 LSVPN 之前,您必须为各个门户和网关分配 SSL/TLS 服务配置文件.配置文件指定服务器证书和被允许的 TLS 版本，用于与卫星之间的通信。由于门户会在第一次与卫星进行连接时为每个卫星颁发服务器证书，作为卫星注册流程的一部分，所以你不需要创建卫星的 SSL/TLS 服务配置文件。

此外，必须将用来签发服务器证书的根证书颁发机构 (CA) 证书导入计划作为网关或卫星承载的每个防火墙。最后，在组成 LSVPN 的每个网关和卫星上，必须使用相互身份验证配置证书配置文件建立 SSL/TLS 连接。

下列工作流描述了将 SSL 证书部署至 GlobalProtect LSVPN 组件的最佳操作步骤：

STEP 1 | 在承载 GlobalProtect 门户的防火墙上，创建用于向 GlobalProtect 组件签发证书的根 CA 证书。

创建自签名根 CA 证书：

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
2. 输入 **Certificate Name**（证书名称），如 **LSVPN_CA**。
3. 不要选择 **Signed By**（签名者）字段中的值（此值表示自签名）。
4. 选中 **Certificate Authority**（证书颁发机构）复选框，然后单击 **OK**（确定）以生成证书。

STEP 2 | 为 GlobalProtect 门户和网关创建 SL/TLS 服务配置文件。

对于门户和各个网关，您必须分配引用唯一自签名服务器证书的 SSL/TLS 服务配置文件。



最佳实践是在门户上签发所需的全部证书，从而无需导出签名证书（和私钥）。



© 2019 Palo Alto Networks, Inc.

如果 *GlobalProtect* 门户和网关位于同一防火墙接口，可以同时为两个组件使用同一服务器证书。

1. 在门户上使用根 CA 为将要部署的每个网关生成证书：
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
   2. 输入 **Certificate Name**（证书名称）。
   3. 在 **Common Name**（公用名）字段中输入计划在其上配置网关的接口的 FQDN（推荐）或 IP 地址。
   4. 在 **Signed By**（签名者）字段中，选择您刚刚创建的 **LSVPN_CA**。
   5. 在“证书属性”部分，单击 **Add**（添加）并定义用于唯一标识网关的属性。如果添加**Host Name**（主机名称）属性（将填充证书 SAN 字段），则该属性须与已定义 **Common Name**（公用名）的值匹配。
   6. **Generate**（生成）证书。
2. 为门户和每个网关配置 SSL/TLS 服务配置文件：
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件），单击 **Add**（添加）。
   2. 输入 **Name**（名称）来标识配置文件并为门户或网关选择您刚刚创建的服务器 **Certificate**（证书）。
   3. 定义允许与卫星通信的 TLS 版本的范围（**Min Version**（最低版本）到 **Max Version**（最高版本）），并单击 **OK**（确定）。

STEP 3 | 将自签名服务器证书部署到网关。

最佳实践：

- 从门户导出由根 CA 签发的自签名服务器证书，并将其导入网关。
- 请确保为每个网关发布唯一的服务器证书。
- 证书的公用名 (CN)和主题备用名称 (SAN)字段（如果适用）必须与在其上配置网关的接口的 IP 地址或完全限定域名 (FQDN) 匹配。

1. 在门户上，选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Export**（导出）。
2. 从 **File Format**（文件格式）下拉列表中选择 **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）。
3. 输入（并重新输入）**Passphrase**（密码）以加密与证书关联的私钥，然后单击 **OK**（确定）以将 PKCS12 文件下载至计算机。
4. 在网关上，选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Import**（导入）。
5. 输入 **Certificate Name**（证书名称）。
6. 输入从门户上所下载 **Certificate File**（证书文件）的路径和名称，或 **Browse**（浏览）以查找该文件。
7. 选择 **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）作为 **File Format**（文件格式）。
8. 在 **Key File**（密钥文件）字段中输入 PKCS12 文件的路径和名称，或单击 **Browse**（浏览）以找到该文件。
9. 输入和重新输入在从门户导出时用于加密私钥的 **Passphrase**（密码），然后单击 **OK**（确定）以导入证书和密钥。



© 2019 Palo Alto Networks, Inc.

STEP 4 | 导入用来为 LSVPN 组件签发服务器证书的根 CA 证书。

必须将根 CA 证书导入所有网关和卫星。为安全起见，请确保仅导出证书，且不要导出关联私钥。

1. 从门户下载根 CA 证书。
    1. 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。
    2. 选择用来为 LSVPN 组件签发证书的根 CA 证书，然后单击 **Export**（导出）。
    3. 从 **File Format**（文件格式）下拉列表中选择 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**），然后单击 **OK**（确定）以下载证书。（请不要导出私钥。）
2. 在承载网关和卫星的防火墙上，导入根 CA 证书。
    1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Import**（导入）。
    2. 输入 **Certificate Name**（证书名称），该名称可将证书标识为您的客户端 CA 证书。
    3. **Browse**（浏览）到从 CA 下载的 **Certificate File**（证书文件）。
    4. 选择 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）作为 **File Format**（文件格式），然后单击 **OK**（确定）。
    5. 选择刚刚在 **Device Certificates**（设备证书）选项卡上导入的证书，然后将其打开。
    6. 选择 **Trusted Root CA**（可信根 **CA**），然后单击 **OK**（确定）。
    7. **Commit**（提交）更改。

STEP 5 | 创建证书配置文件。

GlobalProtect LSVPN 门户和每个网关都需要证书配置文件指定用于对卫星进行验证的证书。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件），然后单击 **Add**（添加）并输入配置文件 **Name**（名称）。
2. 确保将 **Username Field**（用户名字段）设置为 **None**（无）。
3. 在 **CA Certificates**（**CA** 证书）字段中，单击 **Add**（添加），然后选择在之前步骤中导入的可信根 CA 证书。
4. （推荐）允许使用 CRL 和/或 OCSP 来启用证书状态验证。
5. 单击 **OK**（确定）保存配置文件。

STEP 6 | 提交更改。

单击 **Commit**（提交）。

# 通过 SCEP 部署客户端证书到 GlobalProtect 卫星

你也可以将 GlobalProtect 门户配置为你的企业 PKI 中的 SCEP 服务器的简单证书注册协议 (SCEP) 客户端，作为向卫星部署客户端证书的备选方案。其中 SCEP 操作是动态的，当门户发出请求时，企业 PKI 生成证书并发送到门户。

当卫星设备请求连接到门户或网关时，序列号包含在连接请求中。门户通过 SCEP 配置文件中的设置向 SCEP 服务器提交 CSR，并在客户端证书主题中自动包含设备序列号。门户从企业 PKI 接收到客户端证书后，清晰地将客户端证书部署到卫星设备。然后卫星设备向门户或网关展示客户端证书，进行验证。

STEP 1 | 创建 SCEP 配置文件。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **SCEP**，然后 **Add**（添加）新配置文件。
2. 输入 **Name**（名称）以标识 SCEP 配置文件。
3. 如果此配置文件用于具有多重虚拟系统功能的防火墙，选择一个虚拟系统，或者 **Shared**（共享）为有此配置文件的 **Location**（位置）。


© 2019 Palo Alto Networks, Inc.

STEP 2 | （可选）要让基于 SCEP 的证书生成更安全，可在公钥基础结构 (PKI) 与门户之间为各证书请求配置 SCEP 质询-响应机制。

配置此机制后，其操作不可见，您无需再进行任何输入操作。

为了符合《美国联邦信息处理标准》(FIPS)，请使用 **Dynamic**（动态）SCEP Challenge（SCEP 质询）并指定使用 HTTPS 的 **Server URL**（服务器 **URL**）（请参阅步骤 7）。

选择以下任一选项：

- **None**（无）— （默认）SCEP 服务器不会在门户发布证书前对其进行质询。
- **Fixed**（固定）— 在 PKI 架构中，从 SCEP 服务器获取注册质询密码（如`http://10.200.101.1/CertSrv/mscep_admin/`），然后拷贝或输入到密码字段。
- **Dynamic**（动态）— 输入门户-客户端提交凭证的 SCEP **Server URL**（服务器 **URL**）（如`http://10.200.101.1/CertSrv/mscep_admin/`）、用户名和你选择的 OTP。用户名和密码可以作为 PKI 管理员的凭证。

STEP 3 | 指定 SCEP 服务器与门户之间的连接设置，以便门户请求和接收客户端证书。

为了识别卫星，门户在对 SCEP 服务器的 CSR 请求中自动包含设备序列号。由于 SCEP 需要**Subject**（主题）字段中有值，你可以保留默认的 `$USERNAME`令牌，即使该值不会在 LSVPN 客户端证书中使用。

1. 配置门户用于访问 PKI 中 SCEP 服务器的 **Server URL**（服务器 **URL**）（例如，`http://10.200.101.1/certsrv/mscep/`）。
2. 在 **CA-IDENT Name**（**CA-IDENT** 名称）字段中输入字符串（最长不超过 255 个字符）以标识 SCEP 服务器。
3. 选择 **Subject Alternative Name Type**（主题备用名称类型）。
   - **RFC 822 Name**（**RFC 822** 名称）— 输入证书主题或“主题备选名称”扩展中的电子邮件名称。
   - **DNS Name**（**DNS** 名称）— 输入用于评估证书的 DNS 名称。
   - **Uniform Resource Identifier**（统一资源标识符）— 输入客户端从其获取证书的资源名称。
   - **None**（无）— 不指定证书属性。

STEP 4 | （可选）为证书配置加密设置。

- 选择证书的密钥长度（**Number of Bits**（位数））。如果防火墙为 FIPS-CC 模式且密钥生成算法为 RSA，则 RSA 密钥必须为 2，048 位或更大。
- 选择 **Digest for CSR**（**CSR** 摘要），表示证书签名请求 (CSR) 的摘要算法：SHA1、SHA256、SHA384 或 SHA512。

STEP 5 | （可选）配置证书的允许用途：签名或加密。

- 要将证书用于签名，选中 **Use as digital signature**（用作数字签名）复选框。这可使端点能够使用证书中的密钥来验证数字签名。
- 要将证书用于加密，选中 **Use for key encipherment**（用于加密）复选框。这可使客户端能够使用证书中的密钥来加密通过 SCEP 服务器颁发的证书建立的 HTTPS 连接所交换的数据。

STEP 6 | （可选）为确保门户连接到正确的 SCEP 服务器，请输入 **CA Certificate Fingerprint**（**CA** 证书指纹）。该指纹可从 SCEP 服务器界面的“指纹”字段中获取。

1. 输入 SCEP 服务器管理 UI 的 URL（例如，`http://<hostname or IP>/CertSrv/mscep_admin/`）。
2. 复制指纹并将其输入 **CA Certificate Fingerprint**（**CA** 证书指纹）字段中。

STEP 7 | 启用 SCEP 服务器与 GlobalProtect 门户之间的相互 SSL 身份验证。这必须符合《美国联邦信息处理标准》(FIPS)。



© 2019 Palo Alto Networks, Inc.

（*FIPS-CC* 操作已在防火墙登录页面及防火墙状态栏中予以指明。）

选择 SCEP 服务器的根 **CA Certificate**（**CA** 证书）。或者，您也可以通过选择 **Client Certificate**（客户端证书）在 SCEP 服务器和 GlobalProtect 门户之间启用相互 SSL 身份验证。

STEP 8 | 保存并提交配置。

1. 单击 **OK**（确定）以保存设置并关闭 SCEP 配置。
2. **Commit**（提交）配置。

门户尝试使用 SCEP 配置文件中的设置请求 CA 证书，并将其保存至承载门户的防火墙。如果成功，则 CA 证书显示在 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）中。

STEP 9 | （可选）如果门户在保存 SCEP 配置文件后未能获取证书，您可手动从门户生成证书签名请求 (CSR)。

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Generate**（生成）。
2. 输入 **Certificate Name**（证书名称）。该名称不得包含空格。
3. 选择用于提交 CSR 至企业 PKI 的 **SCEP Profile**（**SCEP** 配置文件）。
4. 单击 **OK**（确定）以提交请求和生成证书。

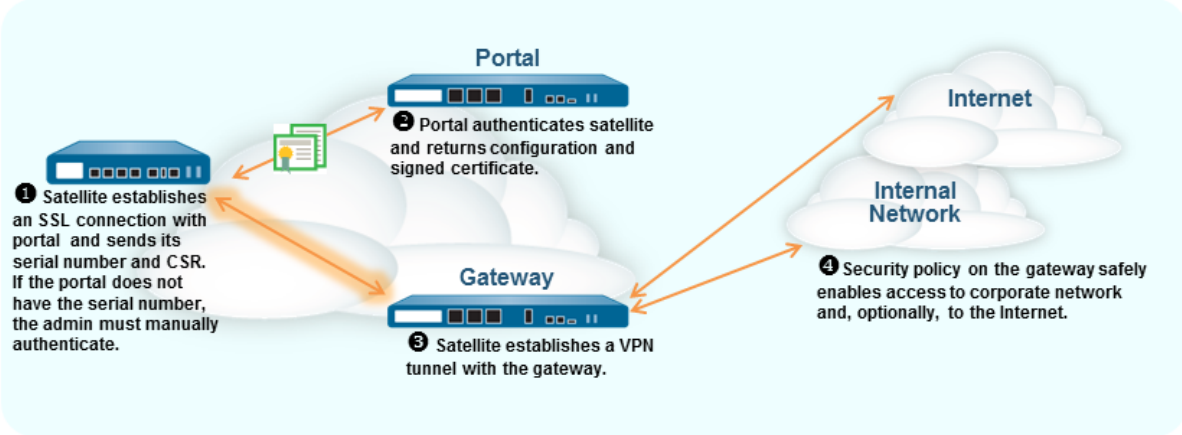

© 2019 Palo Alto Networks, Inc.

# 配置门户以验证卫星

要注册 LSVPN，每颗卫星均必须与门户建立 SSL/TLS 连接。在建立连接后，门户会对卫星进行验证以确保授权加入 LSVPN。在验证卫星成功后，门户会为卫星签发服务器证书并推送 LSVPN 配置，指定卫星可以连接的网关和与网关建立 SSL 连接所需的根 CA 证书。

在初始连接期间，卫星可以通过两种方法对门户进行验证：

- **Serial number**（序列号）— 可以使用已授权加入 LSVPN 的卫星防火墙的序列号配置门户。在卫星初始连接到门户期间，卫星会将其序列号提交到门户，如果门户在其配置中拥有该序列号，则对卫星验证将会成功。在配置门户完成后，可添加已授权卫星的序列号。请参阅配置门户。
- 用户名和密码 — 如果要在没有手动将卫星序列号输入到门户配置时配置卫星，可要求卫星管理员在与门户建立初始连接时进行验证。尽管门户始终会在卫星的初始请求中查找序列号，但如果它无法识别该序列号，则卫星管理员必须提供用户名和密码对门户进行验证。因为门户始终会回滚到这种形式的身份验证，因此必须创建验证配置文件以提交门户配置。这就要求为门户 LSVPN 配置设置验证配置文件，即使计划使用序列号对卫星进行验证。




下列工作流介绍了如何设置门户根据现有身份验证服务对卫星进行验证。GlobalProtect LSVPN 使用本地数据库、LDAP（包括 Active Directory）、Kerberos、TACACS+ 或 RADIUS 支持外部身份验证。

STEP 1 | （仅限外部身份验证）在门户上创建服务器配置文件。

服务器配置文件定义防火墙如何连接到外部身份验证服务，以验证卫星管理员输入的身份验证凭证。

如果使用本地身份验证，则跳过此步骤，为卫星管理员添加一个本地用户：请查阅将用户帐户添加到本地数据库。

为身份验证服务类型配置服务器配置文件：

- 添加 RADIUS 服务器配置文件。

您可以使用 *RADIUS* 与多重因素身份验证服务集成。

- 添加 TACACS+ 服务器配置文件。
- 添加 SAML IdP 服务器配置文件。
- 添加 Kerberos 服务器配置文件。
- 添加 LDAP 服务器配置文件。如果使用 LDAP 连接至 Active Directory (AD)，则须为每个 AD 域分别创建 LDAP 服务器配置文件。



© 2019 Palo Alto Networks, Inc.

### STEP 2 | 配置身份验证配置文件。

身份验证配置文件定义用来验证卫星的服务器配置文件。

1. 选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件），然后单击 **Add**（添加）。
2. 输入配置文件的 **Name**（名称），然后选择身份验证 **Type**（类型）。如果 **Type**（类型）为外部服务，请选择您在上一步中创建的 **Server Profile**（服务器配置文件）。如果您已添加本地用户，请将 **Type**（类型）设置为 **Local Database**（本地数据库）。
3. 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 为 LSVPN 配置 GlobalProtect 网关

因为门户传递至卫星的 GlobalProtect 配置包括卫星可连接的网关列表，因此建议在配置门户前配置网关。

完成下列任务后方可配置 GlobalProtect 网关：

- 为 LSVPN 创建接口和区域在您将配置各个网关的接口上。必须同时配置物理接口和虚拟隧道接口。
- 在 GlobalProtect LSVPN 组件之间启用 SSL通过配置建立 GlobalProtect 卫星和网关之间的双向 SSL/TLS 连接所需的网关服务器证书、SSL/TLS 服务器配置文件和证书配置文件。

配置组成 LSVPN 的每个 GlobalProtect 网关，如下所示：

STEP 1 | 添加网关。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）并单击 **Add**（添加）。
2. 在 **General**（常规）屏幕上，输入网关的 **Name**（名称）。网关名称不得包含空格，且最佳实践是在名称中包括有助用户和其他管理员标识网关的位置或其他描述性信息。
3. （可选）从 **Location**（位置）字段中选择该网关所属的虚拟系统。

STEP 2 | 指定使卫星设备能够连接至网关的网络信息。

如果尚未为网关创建网络接口，请参阅为 LSVPN 创建接口和区域以了解相关操作说明。

1. 选择卫星用于入口访问至网关的 **Interface**（接口）。
2. 指定网关访问的 **IP Address Type**（IP 地址类型）和 **IP address**（IP 地址）：
   - IP 地址类型可以是 **Ipv4**（仅 IPv4 ）、**IPv6**（仅 IPv6）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 地址必须与 IP 地址类型兼容。例如，`172.16.1/0`（对于 IPv4 地址）或 `21DA:D3:0:2F3B`（对于 IPv6 地址）。对于双栈配置，请输入 IPv4 和 IPv6 地址。
3. 单击 **OK**（确定）以保存更改。

STEP 3 | 指定网关认证卫星如何尝试建立隧道。如果尚未为网关创建 SSL/TLS 服务配置文件，请参阅将服务器证书部署到 GlobalProtect LSVPN 组件。

如果尚未建立身份验证配置文件或证书配置文件，请参阅配置门户以验证卫星以了解相关操作说明。

如果尚未设置证书配置文件，请参阅在 GlobalProtect LSVPN 组件之间启用 SSL以了解说明。

在 GlobalProtect 网关配置对话框中选择认证，然后配置以下内容：

- 如要确保网关和卫星之间的通信，则选择网关的**SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。
- 如要指定认证文件来认证卫星，则**Add**（添加）客户端认证。然后输入**Name**（名称）识别配置，选择**OS**：**Satellite**（卫星），将配置应用到所有卫星，并指定**Authentication Profile**（认证配置文件）来认证卫星。你也可以选择网关的**Certificate Profile**（证书配置文件）来认证尝试建立隧道的卫星设备。

STEP 4 | 配置隧道参数并启用隧道。

1. 在 GlobalProtect 网关配置对话框中，选择 **Satellite**（卫星）> **Tunnel Settings**（隧道设置）。
2. 选中 **Tunnel Configuration**（隧道配置）复选框以启用隧道。
3. 选择您定义的**Tunnel Interface**（隧道接口），以便在执行任务到为 LSVPN 创建接口和区域时终止 GlobalProtect 卫星建立的 VPN 隧道。
4. （可选）如果想要保留封装数据包中的服务类型 (ToS) 信息，选中**Copy TOS**（复制 **TOS**）。



如果隧道内有多个会话（每个会话使用不同的 *TOS* 值），复制 *TOS* 标头会导致 *IPSec* 数据包在送达时处于失序状态。



© 2019 Palo Alto Networks, Inc.

STEP 5 | （可选）启用隧道监控。

隧道监控能使卫星监控其网关隧道连接，以允许它在连接失败时故障转移至备份网关。故障转移至其他网关是使用 LSVPN 支持的隧道监控配置文件的唯一类型。

1. 选中 **Tunnel Monitoring**（隧道监控）复选框。
2. 指定卫星用于确定网关是否处于活动状态的 **Destination IP Address**（目标 **IP** 地址）。您可以指定 **IPv4** 地址和 **IPv6** 地址，或二者皆可。或者，如果已配置隧道接口的 IP 地址，可以将此字段留空，并且隧道监视器将改用隧道接口确定连接是否处于活动状态。
3. 从 **Tunnel Monitor Profile**（隧道监视器配置文件）下拉列表中选择 **Failover**（故障转移）（这是 LSVPN 唯一支持的隧道监视器配置文件）。

STEP 6 | 选择在建立隧道连接时要使用的 IPSec 加密配置文件。

配置文件用于指定 IPSec 加密类型和保护通过隧道的数据的验证方法。因为 LSVPN 中的两个隧道终结点是组织内受信任的防火墙，因此通常可以使用默认（预定义）配置文件，该配置文件使用 ESP 作为 IPSec 协议、DH group2、AES-128-CBC 加密和 SHA-1 进行身份验证。

在 **IPSec Crypto Profile**（**IPSec** 加密配置文件）下拉列表中，选择 **default**（默认）以使用预定义配置文件或选择 **New IPSec Crypto Profile**（新建 **IPSec** 加密配置文件）来定义新配置文件。有关身份验证和加密选项的详细信息，请参阅定义 IPSec 加密配置文件。

STEP 7 | 在建立 IPSec 隧道时配置网络设置以指定卫星。



还可以通过在承载卫星的防火墙上配置 *DHCP* 服务器来配置卫星将 *DNS* 设置推送到其本地客户端。在此配置中，卫星会将从网关获得的 *DNS* 设置推送到 *DHCP* 客户端。

1. 在 GlobalProtect 网关配置对话框中，选择 **Satellite**（卫星）> **Network Settings**（网络设置）。
2. （可选）如果卫星的本地客户端需要解析公司网络的 FQDN，可以通过以下方法之一配置网关将 DNS 设置推送到卫星：
   - 如果将网关的某一接口配置为 DHCP 客户端，则可将 **Inheritance Source**（继承源）设置为该接口，同时将 DHCP 客户端收到的相同设置分配给 GlobalProtect 卫星。可继承来自继承源的 DNS 后缀。
   - 手动定义要推送到卫星的 **Primary DNS**（主 **DNS**）、**Secondary DNS**（辅助 **DNS**）和 **DNS Suffix**（**DNS** 后缀）设置。
3. 要指定在建立 VPN 时分配给卫星隧道接口的地址的 **IP Pool**（**IP** 池），单击 **Add**（添加），然后指定要使用的 IP 地址范围。
4. 要定义需通过隧道路由至的目标子网，请在 **Access Route**（访问路由）区域内单击 **Add**（添加），然后按下列方法输入路由：
   - 如果要通过隧道路由卫星的所有流量，将该字段留空。

     在这种情况下，除一定流向本地子网的流量外，所有流量都会通过隧道流向网关。

   - 要仅通过网关路由一些流量（称为拆分隧道），指定必须建立隧道的目标子网。在这种情况下，卫星将使用自己的路由表路由不是发往指定访问路由的流量。例如，可以选择仅将隧道流量发往公司网络，并使用本地卫星安全启用互联网访问。
   - 如果要在卫星之间启用路由，输入受每颗卫星保护的网络的汇总路由。

STEP 8 | （可选）定义网关将接受来自卫星的路由（如果有）。

默认情况下，卫星将不会向其路由表添加任何卫星路由通告。如果不想网关接受来自卫星的路由，则不需要完成此步骤。



© 2019 Palo Alto Networks, Inc.

1. 要启用网关接受卫星通告的路由，选择 **Satellite**（卫星）> **Route Filter**（路由筛选器）。
2. 选中 **Accept published routes**（接受发布的路由）复选框。
3. 要筛选卫星通告的路由以添加到网关路由表，单击 **Add**（添加），然后定义要包含的子网。例如，如果在 LAN 端使用子网 192.168.x.0/24 配置所有卫星，可以将许可路由配置为 192.168.0.0/16 启用网关仅接受来自卫星的路由（如果该卫星位于 192.168.0.0/16 子网）。

STEP 9 | 保存网关配置。

1. 单击 **OK**（确定）以保存设置并关闭“GlobalProtect 网关配置”对话框。
2. **Commit**（提交）配置。



© 2019 Palo Alto Networks, Inc.

# 为 LSVPN 配置 GlobalProtect 门户

GlobalProtect 门户提供了针对 GlobalProtect LSVPN 基础架构的管理功能。组成 LSVPN 的每个卫星系统都会从门户收到配置信息，包括有关可用网关和连接到网关所需证书的信息。

下列章节提供了门户的设置过程：

- GlobalProtect 门户的 LSVPN 前提任务
- 配置门户
- 定义卫星配置

## GlobalProtect 门户的 LSVPN 前提任务

完成下列任务后方可配置 GlobalProtect 门户：

- ❑ 为 LSVPN 创建接口和区域在您将配置门户的接口上。
- ❑ 在 GlobalProtect LSVPN 组件之间启用 SSL 通过为门户服务器证书创建 SSL/TLS 服务器配置文件，发布网关服务器证书，以及配置门户发布 GlobalProtect 卫星的服务器配置文件。
- ❑ 配置门户以验证卫星通过定义门户将用于对卫星进行身份验证的身份验证配置文件（如果无法获取序列号）。
- ❑ 为 LSVPN 配置 GlobalProtect 网关。

## 配置门户

完成 GlobalProtect 门户的 LSVPN 前提任务后，请按下列方法配置 GlobalProtect 门户：

STEP 1 | 添加门户。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入门户的 **Name**（名称）。门户名称不得包含空格。
3. （可选）从 **Location**（位置）字段中选择该门户所属的虚拟系统。

STEP 2 | 指定网络信息以允许卫星连接至门户。

如果尚未为门户创建网络接口，有关说明请参阅 为 LSVPN 创建接口和区域。

1. 选择卫星用于入口访问门户的 **Interface**（接口）。
2. 指定门户访问的 **IP Address Type**（**IP** 地址类型）和 **IP address**（**IP** 地址）。
   - IP 地址类型可以是 **IPv4**（仅限 IPv4 流量）、**IPv6**（仅限 IPv6 流量）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。
   - IP 地址必须与 IP 地址类型兼容。例如，`172.16.1/0`（对于 IPv4 地址）或 `21DA:D3:0:2F3B`（对于 IPv6 地址）。对于双栈配置，请输入 IPv4 和 IPv6 地址。
3. 单击 **OK**（确定）以保存更改。

STEP 3 | 指定 SSL/TLS 服务配置文件，使卫星能够建立到门户的 SSL/TLS 连接。

如果尚未为门户网站创建 SSL/TLS 服务配置文件并发出网关证书，请参阅将服务器证书部署到 GlobalProtect LSVPN 组件。

1. 在 GlobalProtect 门户配置对话框中选择**Authentication**（认证）。
2. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

STEP 4 | 为认证卫星指定认证配置文件和可选的证书配置文件。



© 2019 Palo Alto Networks, Inc.

如果门户不能证实连接卫星的序列号，就会回到认证配置文件。因此，在能保存门户配置之前（单击 *OK*（确定）），必须配置身份验证配置文件。

**Add**（添加）一个客户端认证，然后输入 **Name**（名称）标识配置，选择**OS**：**Satellite**（卫星），将配置应用到所有卫星，并指定 **Authentication Profile**（认证配置文件）来认证卫星设备。你也可以为门户指定一个 **Certificate Profile**（证书配置文件）用来认证卫星设备。

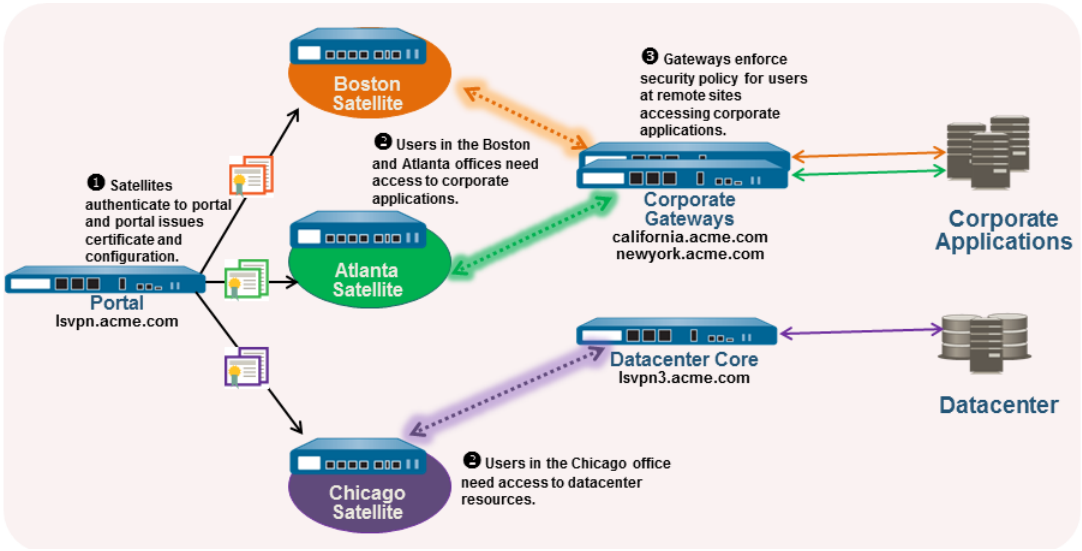
STEP 5 | 继续定义要推送到卫星的配置，或如果已经创建卫星配置，可保存门户配置。

单击 **OK**（确定）以保存门户配置或继续定义卫星配置。

# 定义卫星配置

当连接 GlobalProtect 卫星并成功验证 GlobalProtect 门户后，门户会提供卫星配置来指定卫星可以连接到的网关。如果所有卫星都将使用相同的网关和证书配置，可以创建一个可在成功验证后提交给所有卫星的卫星配置。但是，如果需要不同的卫星配置（例如，如果要将一组卫星连接到一个网关并将另一组卫星连接到不同网关），可以为每个卫星创建单独的卫星配置。然后，门户将使用注册用户名/组名或卫星序列号确定要部署的卫星配置。与安全规则评估相同，门户从列表的顶部开始查找匹配项。在其找到匹配项后，会将对应的配置提交给卫星。

例如，下图显示了其中一些分支机构需要 VPN 访问受外围防火墙保护的公司应用程序和其他站点需要 VPN 访问数据中心的网络。




使用下列步骤创建一个或多个卫星配置。

STEP 1 | 添加卫星配置。

卫星配置指定了用于部署至连接卫星的 GlobalProtect LSVPN 配置设置。至少必须定义一个卫星配置。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）并选择要为其添加卫星配置的门户配置，然后选择 **Satellite**（卫星）选项卡。
2. 在卫星部分中，单击 **Add**（添加）。
3. 为该配置输入 **Name**（名称）。

   如果计划创建多个配置，则应确保为每个配置定义的名称包含足够的描述性信息，以便对其进行区分。
4. 如要修改卫星检查端口进行更新的频率，在 **Configuration Refresh Interval (hours)**（配置刷新间隔（小时））字段中指定一个值，（范围为 1-48；默认为 24）。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 指定部署此配置的卫星。

门户使用 **Enrollment User/User Group**（注册用户/用户组）设置和/或 **Devices**（设备）序列号将卫星与配置进行匹配。因此，如果有多个配置，必须确保对其进行正确排序。一旦找到匹配项，门户便会传递配置。因此，较为具体的配置必须先于较为常规的配置。有关对卫星配置列表进行排序的说明，请参阅步骤 5。

指定卫星配置的匹配条件，如下所示：

- 要使用特定序列号限制卫星的此配置，选择 **Devices**（设备）选项卡，单击 **Add**（添加），然后输入序列号（无需输入卫星主机名；在卫星连接时将自动添加）。对于要接收此配置的每颗卫星，请重复此步骤。
- 选择 **Enrollment User/User Group**（注册用户/用户组）选项卡，单击**Add**（添加），然后输入要接收此配置的用户或组。需要对序列号不匹配的卫星进行验证，如同用户在此处所指定（个人用户或组成员）。

在将配置限定于特定组之前，必须将用户映射到组。

STEP 3 | 指定卫星使用此配置可与其建立 VPN 隧道的网关。

在卫星上安装网关发布的路由作为静态路由。静态路由的跳数为 *10* 乘以路由优先级。如果拥有多个网关，请确保同时设置路由优先级，确保备份网关通告的路由拥有比主网关通告的同一路由更高的跳数。例如，如果将主网关和备份网关的路由优先级分别设置为 *1* 和 *10*，则卫星将使用 *10* 作为主网关的跳数，并使用 *100* 作为备份网关的跳数。

1. 在 **Gateways**（网关）选项卡上，单击 **Add**（添加）。
2. 为网关输入描述性 **Name**（名称）。此处所输入的名称应与配置网关时所定义的名称匹配，同时还应包含足够的描述性信息以确定网关的位置。
3. 在网关字段中，输入在其上配置网关的接口的 FQDN 或 IP 地址。指定的地址必须与网关服务器证书中的公用名 (CN) 完全匹配。
4. （可选）如果要将两个或多个网关添加到配置，**Routing Priority**（路由优先级）有助于卫星选择首选网关。输入一个介于 1-25 范围内的值，数字越小优先级越高（即卫星可以连接到网关，如果所有网关可用）。卫星将路由优先级乘以 10 来确定路由跳数。

STEP 4 | 保存卫星配置。

1. 单击 **OK**（确定）以保存卫星配置。
2. 如果要添加其他卫星配置，请重复执行之前的步骤。

STEP 5 | 分配卫星配置以便将正确的配置部署至每颗卫星。

- 要在配置列表中上移卫星配置，请选择该配置并单击 **Move Up**（上移）。
- 要在配置列表中下移卫星配置，请选择该配置并单击 **Move Down**（下移）。

STEP 6 | 指定允许卫星组成 LSVPN 所需的证书。

1. 在 **Trusted Root CA**（可信根 **CA**）字段中，单击 **Add**（添加），然后选择用于签发网关服务器证书的 CA 证书。作为配置的一部分，门户将在此处所添加的根 CA 证书部署至所有卫星，以便使卫星与网关建立 SSL 连接。最佳实践是，所有网关均使用同一颁发者。
2. 选择 **Client Certificate**（客户端证书）发行的途径：
   - 在门户上存储客户端证书 —成功验证卫星后从**Issuing Certificate**（签发证书）下拉列表中选择**Local**（本地），然后选择门户用来向卫星签发客户端的根 CA 证书。


© 2019 Palo Alto Networks, Inc.



如果用于签发网关服务器证书的根 *CA* 证书不在门户上，则可立即将其 *Import*（导入）。有关如何导入根 *CA* 证书的详细信息，请参阅在 GlobalProtect LSVPN 组件之间启用 SSL。

- 门户作为 **SCEP** 客户端，能动态请求和签发客户端证书 — 选择 **SCEP**，然后选择用来生成到 SCEP 服务器的 CSRs 的**SCEP** 配置文件。



如果你还没将门户设置为 *SCEP* 客户端，那你现在可以添加一个 *New*（新的）*SCEP* 配置文件。有关详细信息，请参阅将客户端证书部署到使用 SCEP 的 GlobalProtect 卫星。

STEP 7 | 保存门户配置。

1. 单击 **OK**（确定）以保存设置并关闭“GlobalProtect 门户配置”对话框。
2. **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 准备卫星加入 LSVPN

要参与到 LSVPN，需要对卫星进行最少配置。因为执行的配置最少，因此在将卫星装运到分支机构进行安装前可进行预配置。

STEP 1 | 配置第 3 层接口（请参见第 3 层接口）。

这是卫星将用来连接到门户和网关的物理接口。此接口必须位于允许从本地信任网络之外进行访问的区域。作为最佳实践，为 VPN 连接创建专用区域以便更好了解和控制发往公司网关的流量。

STEP 2 | 配置隧道的逻辑隧道接口用来与 GlobalProtect 网关建立 VPN 隧道。



除非您计划使用动态路由，否则无需为隧道接口分配 *IP* 地址。但是，为隧道接口分配 *IP* 地址有助于对连通性问题进行故障排除。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.2**。
3. 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表，然后选择现有的区域，或者通过单击 **New Zone**（新建区域）和定义新区域的 **Name**（名称）（如 *lsvpnsat*）为 VPN 隧道流量创建单独的区域。
4. 在 **Virtual Router**（虚拟路由器）下拉列表中，选择 **default**（默认）。
5. （可选）要为隧道接口分配 IP 地址：
   - 对于 IPv4 地址，选择 **IPv4**，**Add**（添加）IP 地址和子网掩码并分配给接口，例如 203.0.11.100/24。
   - 对于 IPv6 地址，选择 **IPv6**，**Enable IPv6 on the interface**（在接口上启用 **IPv6**），**Add**（添加）IP 地址和子网掩码并分配给接口，例如 2001:1890:12f2:11::10.1.8.160/80。
6. 要保存接口配置，请单击 **OK**（确定）。

STEP 3 | 如果使用不受卫星信任的根 CA 生成门户服务器证书（例如，如果使用自签名证书），则导入所使用的根 CA 证书来签发门户服务器证书。

允许卫星与门户建立初始连接以获取 LSVPN 配置需要根 CA 证书。

1. 下载用来生成门户服务器证书的 CA 证书。如果使用自签名证书，可从门户导出根 CA 证书，如下所示：
   1. 选择**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）。
   2. 选择 CA 证书，并单击 **Export**（导出）。
   3. 从 **File Format**（文件格式）下拉列表中选择 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**），然后单击 **OK**（确定）以下载证书。（您无需导出私钥。）
2. 将刚导出的根 CA 证书导入每颗卫星，如下所示。
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书），然后单击 **Import**（导入）。
   2. 输入 **Certificate Name**（证书名称），该名称可将证书标识为您的客户端 CA 证书。
   3. **Browse**（浏览）到从 CA 下载的 **Certificate File**（证书文件）。
   4. 选择 **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）作为 **File Format**（文件格式），然后单击 **OK**（确定）。
   5. 选择刚刚在 **Device Certificates**（设备证书）选项卡上导入的证书，然后将其打开。
   6. 选择 **Trusted Root CA**（可信根 **CA**），然后单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

STEP 4 | 配置 IPSec 隧道配置。

1. 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道），然后单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入 IPSec 配置的描述性 **Name**（名称）。
3. 选择为卫星创建的 **Tunnel Interface**（隧道接口）。
4. 选择 **GlobalProtect Satellite**（**GlobalProtect** 卫星）作为 **Type**（类型）。
5. 输入门户的 IP 地址或 FQDN 作为 **Portal Address**（门户地址）。
6. 选择为卫星配置的第 3 层 **Interface**（接口）。
7. 选择要在选定接口上使用的 **IP Address**（**IP** 地址）。您可以选择 **IPv4** 地址和 **IPv6** 地址，或 IPv4 地址和 IPv6 地址。如需 **IPv6 preferred for portal registration**（**IPv6** 优于门户注册），请指定。

STEP 5 | （可选）配置卫星将本地路由发布到网关。

将路由推送到网关以允许本地子网的流量通过网关传递到卫星。但是，如为 LSVPN 配置 GlobalProtect 网关中详述，您还必须配置网关来接受路由。

1. 要允许卫星将路由推送到网关，在 **Advanced**（高级）选项卡上，选择 **Publish all static and connected routes to Gateway**（将所有静态和连接路由发布到网关）。

   如果您选中此复选框，防火墙会将所有静态和连接路由从卫星转发到网关。但是，为了阻止路由回环的形成，防火墙将应用一些路由筛选器，如以下所示：

   - 默认路由
   - 与隧道接口关联的虚拟路由器之外的虚拟路由器、内的路由
   - 使用隧道接口的路由
   - 使用的物理接口与隧道接口关联的路由
2. （可选）如果只推送特定子网的路由（而非所有路由），在“子网”部分中单击 **Add**（添加），并指定要发布的子网路由。

STEP 6 | 保存卫星配置。

1. 单击 **OK**（确定）以保存 IPSec 隧道设置。
2. 单击 **Commit**（提交）。

STEP 7 | 如果需要，可提供凭证以允许卫星对门户进行验证。

只有当门户无法在其配置中找到匹配的序列号或序列号无效时才需要执行此步骤。在这种情况下，卫星将无法与网关建立隧道。

1. 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道），然后单击为 LSVPN 创建的隧道配置 Status（状态）列中的 **Gateway Info**（网关信息）链接。
2. 单击 **Portal Status**（门户状态）字段中的 **enter credentials**（输入凭证）链接，然后输入卫星验证门户所需的用户名和密码。

   在卫星验证门户成功后，它将收到其签名的证书和配置，然后将用来连接到网关。您应该会看到隧道建立状态，且 **Status**（状态）更改为 **Active**（活动）。



© 2019 Palo Alto Networks, Inc.

# 验证 LSVPN 配置

在配置门户、网关和卫星后，验证卫星是否能够连接到门户和网关并与网关建立 VPN 隧道。

STEP 1 | 验证卫星与门户的连接。

在承载门户的防火墙上，通过选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户），然后单击门户配置条目的“信息”列中的 **Satellite Info**（卫星信息）验证卫星连接是否成功。

STEP 2 | 验证卫星与网关的连接。

在承载网关的每个防火墙上，通过选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关），然后单击网关配置条目的“信息”列中的 **Satellite Info**（卫星信息），验证卫星是否能建立 VPN 隧道。卫星与网关成功建立的隧道将会显示在 **Active Satellites**（活动卫星）选项卡上。

STEP 3 | 验证卫星的 LSVPN 隧道状态。

在承载卫星的每个防火墙上，通过选择 **Network**（网络）> **IPSec Tunnels**（IPSec 隧道），验证隧道状态，并验证由绿色图标表示的活动状态。



© 2019 Palo Alto Networks, Inc.

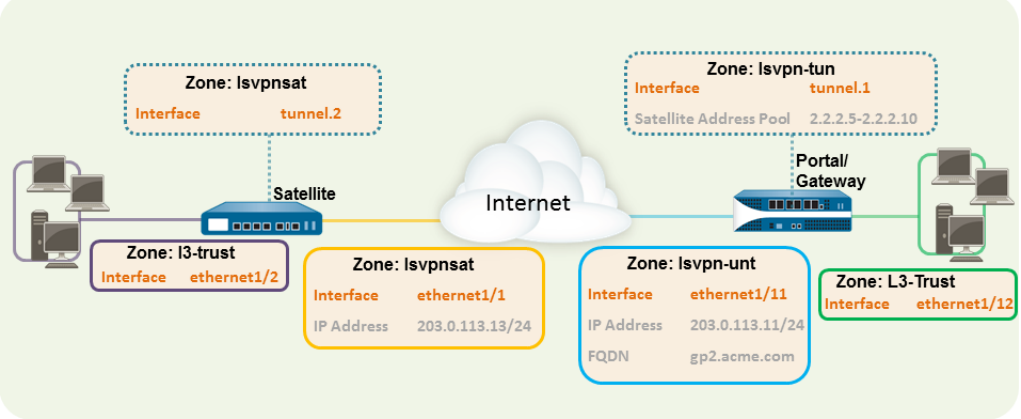
# LSVPN 快速配置

以下部分提供了有关配置部分常见 GlobalProtect LSVPN 部署的分步说明：

- 基本 LSVPN 配置和静态路由
- 高级 LSVPN 配置和动态路由
- 使用 iBGP 进行高级 LSVPN 配置

## 基本 LSVPN 配置和静态路由

此快速配置显示了启动和运行 LSVPN 的最快方法。在本例中，将公司总部站点的一个防火墙同时配置为门户和网关。通过最少配置快速轻松地部署卫星以优化可扩展性。




以下工作流显示了设置此基本配置的步骤：

### STEP 1 | 配置第 3 层接口。

在本例中，需要对门户/网关上的第 3 层接口进行以下配置：

- **Interface**（接口）— ethernet1/11
- **Security Zone**（安全区域）— lsvpn-tun
- **IPv4** — 203.0.113.11/24

### STEP 2 | 在承载 GlobalProtect 网关的防火墙上，配置用于终止 GlobalProtect 卫星所建立 VPN 隧道的逻辑隧道接口。

要更好地了解通过 *VPN* 连接的用户和组，在 *VPN* 隧道终止的区域中启用 *User-ID*。

在本例中，需要对门户/网关上的隧道接口进行以下配置：

- **Interface**（接口）— tunnel.1
- **Security Zone**（安全区域）— lsvpn-tun

### STEP 3 | 创建安全策略规则以允许流量在隧道终止的 VPN 区域 (lsvpn-tun) 和公司应用程序驻留的信任区域 (L3-Trust) 之间流动。

请参阅创建安全策略规则。

### STEP 4 | 将门户/网关分配 SSL/TLS 服务配置文件。配置文件必须引用自签名服务器证书。



© 2019 Palo Alto Networks, Inc.

证书主题名称必须与您为门户/网关创建的第 3 层接口的 FQDN 或 IP 地址匹配。

1. 在承载 GlobalProtect 门户的防火墙上，创建用于向 GlobalProtect 组件签发证书的根 CA 证书。在本例中，根 CA 证书 **lsvpn-CA** 将用来为门户/网关签发服务器证书。此外，门户将使用此根 CA 证书对来自卫星的 CSR 进行签名。
2. 为 GlobalProtect 门户和网关创建 SL/TLS 服务配置文件。

   因为本例中门户和网关位于同一接口，因此可以共享使用相同服务器证书的 SSL/TLS 服务配置文件。在本例中，配置文件名为 **lsvpnserver**。

STEP 5 | 创建证书配置文件。

在本例中，证书配置文件 **lsvpn-profile** 引用根 CA 证书 **lsvpn-CA**。网关将使用此证书配置文件对试图建立 VPN 隧道的卫星进行验证。

STEP 6 | 如果卫星序列号不可用，请为门户配置身份验证配置文件。

1. 在门户上创建一种类型的服务器配置文件：
   - 添加 RADIUS 服务器配置文件。

     您可以使用 *RADIUS* 与多重因素身份验证服务集成。
   - 添加 TACACS+ 服务器配置文件。
   - 添加 SAML IdP 服务器配置文件。
   - 添加 Kerberos 服务器配置文件。
   - 添加 LDAP 服务器配置文件。如果使用 LDAP 连接至 Active Directory (AD)，则须为每个 AD 域分别创建 LDAP 服务器配置文件。
2. 配置身份验证配置文件。在本例中，配置文件 **lsvpn-sat** 用来验证卫星。

STEP 7 | 为 LSVPN 配置 GlobalProtect 网关。

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）并 **Add**（添加）配置。本例需要进行以下网关配置：

- **Interface**（接口）— ethernet1/11
- **IP Address**（IP 地址）— 203.0.113.11/24
- **SSL/TLS Server Profile**（SSL/TLS 服务器配置文件）— lsvpnserver
- **Certificate Profile**（证书配置文件）— lsvpn-profile
- **Tunnel Interface**（隧道接口）— tunnel.1
- **Primary DNS**（主 DNS）/**Secondary DNS**（辅助 DNS）— 4.2.2.1/4.2.2.2
- **IP Pool**（IP 池）— 2.2.2.111-2.2.2.120
- **Access Route**（访问路由）— 10.2.10.0/24

STEP 8 | 配置门户。

选择 **Network**（网络）> **GlobalProtect** > **Portal**（门户）并 **Add**（添加）配置。本例需要进行以下门户配置：

- **Interface**（接口）— ethernet1/11
- **IP Address**（IP 地址）— 203.0.113.11/24
- **SSL/TLS Server Profile**（SSL/TLS 服务器配置文件）— lsvpnserver
- **Authentication Profile**（身份验证配置文件）— lsvpn-sat

STEP 9 | 定义卫星配置。


© 2019 Palo Alto Networks, Inc.

在门户配置的 **Satellite**（卫星）选项卡上，**Add**（添加）卫星配置和受信任的根 CA，并指定门户将用来为卫星签发证书的 CA。在本例中需要进行如下设置：

- **Gateway**（网关）— 203.0.113.11
- **Issuing Certificate**（签发证书）— lsvpn-CA
- **Trusted Root CA**（受信任的 **CA**）— lsvpn-CA

STEP 10 | 准备卫星加入 LSVPN。

需要对本例中的卫星配置进行如下设置：

接口配置

- 第 3 层接口 — ethernet1/1，203.0.113.13/24
- 隧道接口 — tunnel.2
- 区域 — lsvpnsat

门户的根 CA 证书

- lsvpn-CA

IPSec 隧道配置

- **Tunnel Interface**（隧道接口）— tunnel.2
- **Portal Address**（门户地址）— 203.0.113.11
- **Interface**（接口）— ethernet1/1
- **Local IP Address**（本地 **IP** 地址）— 203.0.113.13/24
- **Publish all static and connected routes to Gateway**（将所有静态路由和连接路由发布到网关）— enabled

# 高级 LSVPN 配置和动态路由

在拥有多个网关和多颗卫星的较大型 LSVPN 部署中，在初始配置中花费多一点时间设置动态路由可简化网关配置的维护，因为访问路由会动态更新。下面的示例配置显示了如何扩展基本 LSVPN 配置，以便配置 OSPF 作为动态路由协议。

设置 LSVPN 以便将 OSPF 用于动态路由需要在网关和卫星上执行以下额外步骤：

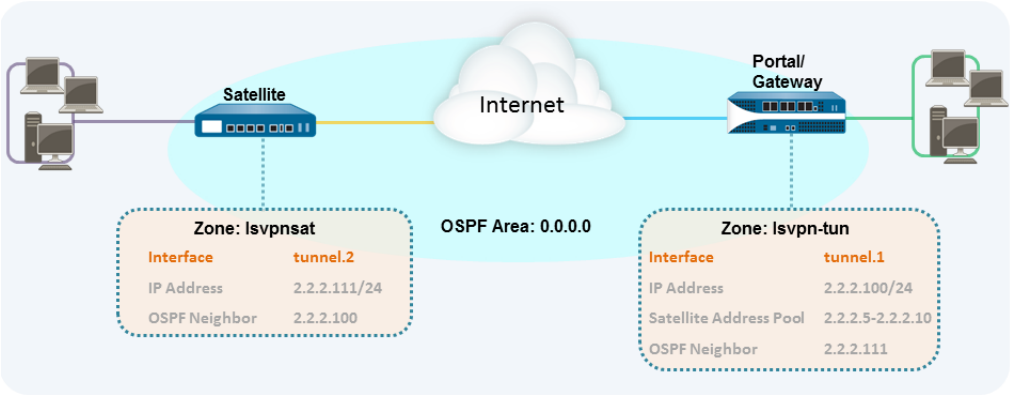
- 手动将 IP 地址分配到所有网关和卫星上的隧道接口。
- 配置所有网关和卫星上虚拟路由器的 OSPF 点对多点 (P2MP)。此外，作为每个网关上 OSPF 配置的一部分，必须手动定义每个卫星的隧道 IP 地址作为 OSPF 邻居。同样，在每颗卫星上，必须手动定义每个网关的隧道 IP 地址作为 OSPF 邻居。

尽管在 LSVPN 的初始配置过程中动态路由需要执行额外设置，但它减少了当网络上的拓扑发生变化时与保持路由最新相关的维护工作。

下图显示了 LSVPN 动态路由配置。本例显示了如何配置 OSPF 作为 VPN 的动态路由协议。



© 2019 Palo Alto Networks, Inc.




有关 LSVPN 的基本设置，请执行基本 LSVPN 配置和静态路由中的步骤。然后，完成以下工作流中的步骤扩展配置使用动态路由（而非静态路由）。

STEP 1 | 将 IP 地址添加到每个网关和每颗卫星上的隧道接口配置。

在每个网关和每颗卫星上完成以下步骤：

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道），然后选择为 LSVPN 创建的隧道配置以打开“隧道接口”对话框。

   如果尚未创建隧道接口，请参阅为 LSVPN 创建接口和区域中的步骤 2。
2. 在 **IPv4** 选项卡上，单击 **Add**（添加），然后输入 IP 地址和子网掩码。例如，要添加网关隧道接口的 IP 地址，请输入 2.2.2.100/24。
3. 单击 **OK**（确定）保存配置。

STEP 2 | 配置网关的动态路由协议。

要配置网关的 OSPF：

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择与 VPN 接口关联的虚拟路由器。
2. 在 **Areas**（区域）选项卡上，单击 **Add**（添加）以创建中枢区域，或者如果已经配置，单击区域 ID 以对其进行编辑。
3. 如果正在创建新的区域，请在 **Type**（类型）选项卡上输入 **Area ID**（区域 **ID**）。
4. 在 **Interface**（接口）选项卡上，单击 **Add**（添加），然后选择为 LSVPN 创建的隧道 **Interface**（接口）。
5. 选择 **p2mp** 作为 **Link Type**（链接类型）。
6. 单击“邻居”部分中的 **Add**（添加），然后输入每个卫星设备的隧道接口的 IP 地址，如 2.2.2.111。
7. 单击 **OK**（确定）两次以保存虚拟路由器配置，然后 **Commit**（提交）对网关的更改。
8. 每次将新的卫星添加到 LSVPN，请重复此步骤。

STEP 3 | 配置卫星的动态路由协议。

要配置卫星的 OSPF：

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择与 VPN 接口关联的虚拟路由器。
2. 在 **Areas**（区域）选项卡上，单击 **Add**（添加）以创建中枢区域，或者如果已经配置，单击区域 ID 以对其进行编辑。
3. 如果正在创建新的区域，请在 **Type**（类型）选项卡上输入 **Area ID**（区域 **ID**）。
4. 在 **Interface**（接口）选项卡上，单击 **Add**（添加），然后选择为 LSVPN 创建的隧道 **Interface**（接口）。
5. 选择 **p2mp** 作为 **Link Type**（链接类型）。


© 2019 Palo Alto Networks, Inc.

6. 单击“邻居”部分中的**Add**（添加），然后输入每个 GlobalProtect 网关的隧道接口的 IP 地址，如 2.2.2.100。
7. 单击 **OK**（确定）两次以保存虚拟路由器配置，然后 **Commit**（提交）对网关的更改。
8. 每次添加新的网关，请重复此步骤。

STEP 4 | 验证网关和卫星是否能够形成路由器邻接。

- 在每颗卫星和每个网关上，确认已形成对等设备邻接且为对等设备创建路由表条目（即卫星拥有到网关的路由和网关拥有到卫星的路由）。选择 **Network**（网络）> **Virtual Router**（虚拟路由器），然后单击用于 LSVPN 的虚拟路由器的 **More Runtime Stats**（更多运行时统计数据）链接。在 Routing（路由）选项卡上，验证 LSVPN 对端设备是否拥有路由。
- 在 **OSPF** > **Interface**（接口）选项卡上，验证 **Type**（类型）是否为 **p2mp**。
- 在 **OSPF** > **Neighbor**（邻居）选项卡上，验证承载网关的防火墙是否已与承载卫星的防火墙建立路由器邻接，反之亦然。同样，验证**Status**（状态）是否为**Full**（完全），这表明已经建立完全邻接。

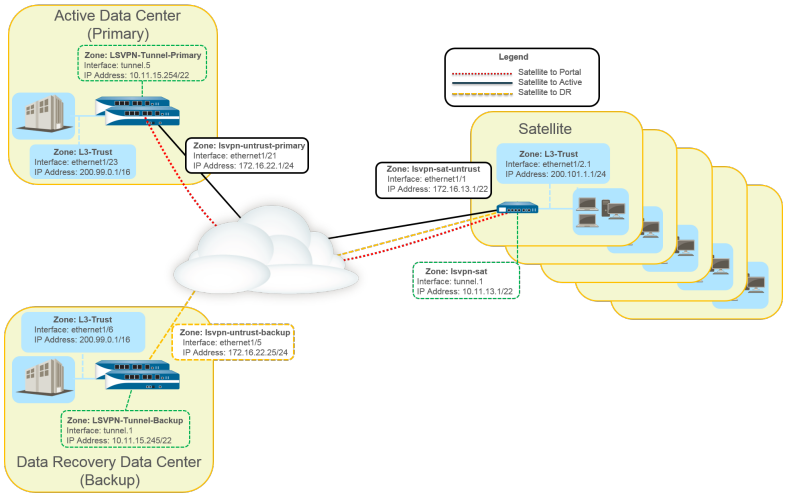
# 使用 iBGP 进行高级 LSVPN 配置

本用例对 GlobalProtect LSVPN 如何将分布式办公室位置与容纳用户关键应用程序的主数据中心和灾难恢复数据中心建立安全连接，以及内部边界网关协议 (iBGP) 如何简化部署和维护进行说明。使用此方法，您可以扩展至最多 500 个已连接到单个网关的卫星办公室。

BGP 是一种高度可扩展的动态路由协议，非常适合 LSVPN 等星型部署。作为一种动态路由协议，易于部署更多的卫星防火墙，以消除与访问路由（静态路由）相关的大量开销。BGP 拥有多种可调计时器、路由惩罚和路由刷新等路由筛选功能和特征，比其他路由协议（如 RIP 和 OSPF）具有更多的路由前缀数量和更高的稳定性。在 iBGP 的情况下，包括 LSVPN 部署中所有卫星和网关的对端组将在隧道端点上建立邻接。然后，该协议便可隐式控制路由通告、更新和收敛。

在该示例配置中，PA-5200 防火墙的主动/被动 HA 对部署在主（主动）数据中心，并充当门户和主网关。灾难恢复数据中心还具有两个作为备用 LSVPN 网关的 PA-5200 主动/被动 HA 对。门户和网关在分支机构中为部署为 LSVPN 卫星的 500 台 PA-220 服务。

这两个数据中心站点都会通告路由，但指标不一致。因此，卫星更喜欢安装主动数据中心的路由。但是，备份路由也存在于本地路由信息库 (RIB) 中。如果主动数据中心发生故障，则删除该数据中心通告的路由，并将其替换为灾难恢复数据中心的路由。故障转移时间取决于 iBGP 时间的选择以及与 iBGP 关联的路由收敛。




以下工作流显示了配置此部署的步骤：

STEP 1 | 为 LSVPN 创建接口和区域。

门户和主网关：



© 2019 Palo Alto Networks, Inc.

- 区域：LSVPN-Untrust-Primary
- 接口：ethernet1/21
- IPv4:172.16.22.1/24
- 区域：l3-信任
- 接口：ethernet1/23
- **IPv4**:200.99.0.1/16

备份网关：

- 区域：LSVPN-Untrust-Primary
- 接口：ethernet1/5
- **IPv4**:172.16.22.25/24
- 区域：l3-信任
- 接口：ethernet1/6
- **IPv4**:200.99.0.1/16

卫星：

- 区域：LSVPN-Sat-Untrust
- 接口：ethernet1/1
- **IPv4**:172.16.13.1/22
- 区域：l3-信任
- 接口：ethernet1/2.1
- **IPv4**:200.101.1.1/24



配置每个卫星设备的区域、接口和 *IP* 地址。每个卫星设备的接口和本地 *IP* 地址各不相同。该接口用于将 *VPN* 连接到门户和网关。

### STEP 2 | 在承载 GlobalProtect 网关的防火墙上，配置用于终止 GlobalProtect 卫星所建立 VPN 隧道的逻辑隧道接口。

主网关：

- 接口：tunnel.5
- **IPv4**:10.11.15.254/22
- 区域：LSVPN-Tunnel-Primary

备份网关：

- 接口：tunnel.1
- **IPv4**:10.11.15.245/22
- 区域：LSVPN-Tunnel-Backup

### STEP 3 | 在 GlobalProtect LSVPN 组件之间启用 SSL。

网关使用自签名根证书颁发机构 (CA) 为 GlobalProtect LSVPN 中的卫星颁发证书。因为一个防火墙包括门户和主网关，所以使用单个证书来验证卫星。相同的 CA 可以为备份网关生成一个证书。CA 生成的证书从门户推送到卫星设备，然后卫星用其对网关进行身份验证。

您还必须从相同的 CA 为备份网关生成证书，允许其与卫星进行身份验证。

1. 在承载 GlobalProtect 门户的防火墙上，创建用于向 GlobalProtect 组件签发证书的根 CA 证书。在此例中，根 CA 证书为 CA-cert。



© 2019 Palo Alto Networks, Inc.

2. 为 GlobalProtect 门户和网关创建 SL/TLS 服务配置文件。由于 GlobalProtect 门户和主网关位于同一防火墙接口，可以同时为两个组件使用同一服务器证书。
   - 根 **CA** 证书：CA-Cert
   - 证书名称：LSVPN-Scale
3. 将自签名服务器证书部署到网关。
4. 导入用来为 LSVPN 组件签发服务器证书的根 CA 证书。
5. 创建证书配置文件。
6. 使用以下设置在备份网关上重复步骤 2 到 5：
   - 根 **CA** 证书：CA-Cert
   - 证书名称：LSVPN-back-GW-cert

STEP 4 | 为 LSVPN 配置 GlobalProtect 网关。

1. 选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，命名主网关 **`LSVPN-Scale`**。
3. 在 **Network Settings**（网络设置）下，选择 **`ethernet1/21`** 作为主网关接口，然后输入 **`172.16.22.1/24`** 作为 IP 地址。
4. 在 **Authentication**（身份验证）选项卡中，选择在3中创建的 LSVPN-Scale 证书。
5. 选择 **Satellite**（卫星）> **Tunnel Settings**（隧道设置），然后选择 **Tunnel Configuration**（隧道配置）。将 **Tunnel Interface**（隧道接口）设置为 tunnel.5。该用例中的所有卫星均连接到单个网关，因此只需一个卫星配置。卫星将根据其序列号进行匹配，无需卫星作为用户进行身份验证。
6. 在 **Satellite**（卫星）> **Network Settings**（网络设置）上，一旦建立 VPN 连接，就应定义分配给卫星隧道接口的 IP 地址池。由于此用例使用动态路由，因此“访问路由”设置留空。
7. 使用以下设置在备份网关上重复步骤 1 到 5：
   - 名称：LSVPN-backup
   - 网关接口：ethernet1/5
   - 网关 **IP**：172.16.22.25/24
   - 服务器证书：LSVPN-backup-GW-cert
   - 隧道接口：tunnel.1

STEP 5 | 配置主网关和备用网关上的 iBGP，添加重新分发配置文件，以便卫星将本地路由插回到网关。

每个卫星办公室负责管理自己的网络和防火墙，因此重新分发配置文件 ToAllSat 配置为可将本地路由重新分发回 GlobalProtect 网关。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后 **Add**（添加）虚拟路由器。
2. 在 **Router Settings**（路由器设置）下，添加虚拟路由器的 **Name**（名称）和 **Interface**（接口）。
3. 选择 **Redistribution Profile**（重新分发配置文件），然后选择 **Add**（添加）。
   1. 命名重新分发配置文件 **`ToAllSat`**，并将 **Priority**（优先级）设置为 1。
   2. 将“重新分发”设置为 **Redist**。
   3. 从“接口”下拉列表中 **Add**（添加）**`ethernet1/23`**。
   4. 单击 **OK**（确定）。
4. 在“虚拟路由器”上选择 **BGP**，以配置 BGP。
   1. 在 **BGP** > **General**（常规）下，选择 **Enable**（启用）。
   2. 输入网关 IP 地址作为 **Router ID**（路由器 ID）(**`172.16.22.1`**)，输入 **`1000`** 作为 **AS Number**（AS 编号）。
   3. 在“选项”部分中，选择 **Install Route**（安装路由）。
   4. 在 **BGP** > **Peer Group**（对端组）下，单击 **Add**（添加）一个将所有卫星连接到网关的对端组。
   5. 在 **BGP** > **Redist Rules**（重新分发规则）下，**Add**（添加）之前创建的重新分发配置文件 **`ToAllSat`**。



© 2019 Palo Alto Networks, Inc.

5. 单击 **OK**（确定）。
6. 使用 **ethernet1/6** 在备份网关上为重新分发配置文件重复步骤 1 到 5。

## STEP 6 | 准备卫星加入 LSVPN。

所示的配置是单个卫星的示例。

每次将新的卫星添加到 LSVPN 部署时，请重复此配置。

1. 将隧道接口配置为 VPN 连接到网关的隧道端点。
2. 将 IPSec 隧道类型设置为 GlobalProtect 卫星，并输入 GlobalProtect 门户的 IP 地址。
3. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后 **Add**（添加）虚拟路由器。
4. 在 **Router Settings**（路由器设置）下，添加虚拟路由器的 **Name**（名称）和 **Interface**（接口）。
5. 选择 **Virtual Router**（虚拟路由器）> **Redistribution Profile**（重新分发配置文件），并使用以下设置 **Add**（添加）配置文件。
   1. 命名重新分发配置文件 **ToLSVPNGW**，并将 **Priority**（优先级）设置为 1。
   2. **Add**（添加）一个 **Interface**（接口）**ethernet1/2.1**。
   3. 单击 **OK**（确定）。
6. 选择 **BGP** > **General**（常规），**Enable**（启用）BGP 并配置协议如下：
   1. 输入网关 IP 地址作为 **Router ID**（路由器 **ID**）(**172.16.22.1**)，输入 **1000** 作为 **AS Number**（**AS** 编号）。
   2. 在“选项”部分中，选择 **Install Route**（安装路由）。
   3. 在 **BGP** > **Peer Group**（对端组）下，**Add**（添加）一个将所有卫星连接到网关的对端组。
   4. 在 **BGP** > **Redist Rules**（重新分发规则）下，**Add**（添加）之前创建的重新分发配置文件 **ToLSVPNGW**。
7. 单击 **OK**（确定）。

## STEP 7 | 为 LSVPN 配置 GlobalProtect 门户。

两个数据中心都会通告其路由，但具有不同的路由优先级，以确保主动数据中心为首选网关。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）并单击 **Add**（添加）。
2. 在 **General**（常规）中，输入 **LSVPN-Portal** 作为门户名称。
3. 在 **Network Settings**（网络设置）中，选择 **ethernet1/21** 作为 **Interface**（接口），然后选择 **172.16.22.1/24** 作为 **IP Address**（**IP** 地址）。
4. 在 **Authentication**（身份验证）选项卡下，从 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）下拉菜单中选择之前创建的主网关 SSL/TLS 配置文件 **LSVPN-Scale**。
5. 在 **Satellite**（卫星）选项卡下，**Add**（添加）一个卫星设备，并将其 **Name**（命名）为 **sat-config-1**。
6. 将 **Configuration Refresh Interval**（配置刷新间隔）设置为 **12**。
7. 在 **GlobalProtect Satellite**（**GlobalProtect** 卫星）> **Devices**（设备）下，在 LSVPN 中添加每个卫星设备的序列号和主机名。
8. 在 **GlobalProtect Satellite**（**GlobalProtect** 卫星）> **Gateways**（网关）下，添加每个网关的名称和 IP 地址。将主网关的路由优先级设置为 1，将备份网关的优先级设置为 10，以确保主动数据中心为首选网关。

## STEP 8 | 验证 LSVPN 配置。

## STEP 9 | （可选）向 LSVPN 部署添加新站点。

1. 选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）> **GlobalProtect Portal**（**GlobalProtect** 门户）> **Satellite Configuration**（卫星配置）> **GlobalProtect Satellite**（**GlobalProtect** 卫星）> **Devices**（设备），将新卫星的序列号添加到 GlobalProtect 门户。
2. 使用 GlobalProtect 门户 IP 地址配置卫星上的 IPSec 隧道。


© 2019 Palo Alto Networks, Inc.

3. 选择 **Network**（网络）> **Virtual Router**（虚拟路由器）> **BGP** > **Peer Group**（对端组），将卫星添加到每个网关上的 BGP 对端组配置。
4. 选择 **Network**（网络）> **Virtual Router**（虚拟路由器）> **BGP** > **Peer Group**（对端组），将网关添加到新卫星上的 BGP 对端组配置。

# Networking（网络）

所有 Palo Alto Networks® 下一代防火墙都提供了灵活的网络架构，包括支持动态路由、交换和 VPN 连接，让您几乎可将防火墙部署到任何网络环境中。在防火墙上配置 以太网端口时，可以选择 Virtual Wire、第 2 层或第 3 层接口部署。另外，为了集成到各种网段中，可以在不同的端口上配置不同类型的接口。网络接口配置完成后，可以以 PDF 或 CSV 格式导出配置数据表格，以进行内部审核或审核。

下列主题介绍了一些网络概念和将 Palo Alto Networks 下一代防火墙集成到网络的方法。


- 配置接口
- 虚拟路由器
- 服务路由
- 静态路由
- RIP
- OSPF
- BGP
- IP 多播
- 路由重新分发
- GRE 隧道
- DHCP
- DNS
- 动态 DNS 概述
- 为防火墙接口配置动态 DNS
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP
- BFD
- 会话设置和超时
- 隧道内容检测

# 配置接口

Palo Alto Networks 下一代防火墙一次可以运行多个部署，因为这些部署都是接口级部署。例如，您可以为第 3 层接口配置一些接口，将防火墙集成到动态路由环境中，同时配置其他接口以集成到第 2 层交换网络中。以下主题描述了每种接口类型的部署以及如何配置相应的接口类型：

- 旁接接口
- 虚拟线路接口
- 第 2 层接口
- 第 3 层接口
- 配置聚合接口组
- 使用接口管理概要文件限制访问

## 旁接接口

网络旁接是一种可让您访问计算机网络中数据流的设备。旁接模式部署可让您通过交换 SPAN 或镜像端口被动地监控网络中的通信流量。

SPAN 或镜像端口允许从交换机上的其他端口复制通信。通过将防火墙上的端口专用为旁接模式接口并将它与交换 SPAN 端口连接，交换 SPAN 端口就可向防火墙提供镜像通信。这样无需处于网络通信流量中即可提供网络中应用程序的可见性。

通过在旁接模式中部署防火墙，您可以查看您网络中运行的应用程序，而无需对网络设计进行任何更改。此外，当在旁接模式中时，防火墙也可以识别您网络上的威胁。但是请记住，由于在旁接模式下时，流量未经过防火墙，因此其无法对流量进行任何操作，如阻挡带有威胁的流量或引用 QoS 流量控制。

要配置旁接几口并开始监控您网络上的设备和威胁：

STEP 1 | 决定您想要将哪个端口作为您的旁接接口使用，并将其连接至配置有 SPAN/RSPAN 或端口镜像的交换机。

您将从 SPAN 目标端口，通过防火墙发送您的网络流量，从而可以查看您网络上的应用程序和威胁。

STEP 2 | 从防火墙 Web 接口，配置您想要作为网络旁接接口使用的接口。

1. 请选择 **Network**（网络）> **Interfaces**（接口），然后选择您刚刚使用电缆连接到相应端口的接口。
2. 选择 **Tap**（旁接）作为 **Interface Type**（接口类型）。
3. 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）并选择 **New Zone**（新建区域）。
4. 在 Zone（区域）对话框中，定义新区域的 **Name**（名称），例如TapZone，然后单击 **OK**（确定）。

STEP 3 | （可选）创建您想要使用的任何转发配置文件。

- 配置日志转发配置文件
- 配置 Syslog 监控

STEP 4 | 创建 安全配置文件以扫描您的网络流量是否具有威胁：

1. 选择**Objects**（对象）> **Security Profiles**（安全配置文件）。
2. 对于每种安全配置类型，**Add**（添加）一个新的配置文件，并将操作设为 **alert**（警报）。

   由于防火墙未与流量内联，您无法使用任何阻挡或重置操作。通过设置操作为警报，您将可以看到防火墙在日志和 ACC 中检测到的任何威胁。

STEP 5 | 创建一个安全策略规则，允许通过旁接接口的流量。

当为旁接模式创建安全策略规则时，源区域和目标区域必须一致。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Policies**（策略）> **Security**（安全），并单击 **Add**（添加）。
2. 在 **Source**（源）选项卡中，将 **Source Zone**（源区域）设为您刚创建的 TapZone。
3. 在 **Destination**（目标）选项卡中，将 **Destination Zone**（目标区）也设置为 TapZone。
4. 将所有规则匹配条件（**Applications**（应用程序）、**User**（用户）、**Service**（服务）、**Address**（地址）设置为 **any**（任意）。
5. 在 **Actions**（操作）选项卡中，将 **Action Setting**（操作设置）设置为 **Allow**（允许）。
6. 将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）并选择您创建的每个安全配置文件以提供威胁警报。
7. 确认 **Log at Session End**（会话端日志）已启用。
8. 单击 **OK**（确定）。
9. 将规则放置在您规则库的顶部。

STEP 6 | **Commit**（提交）配置。

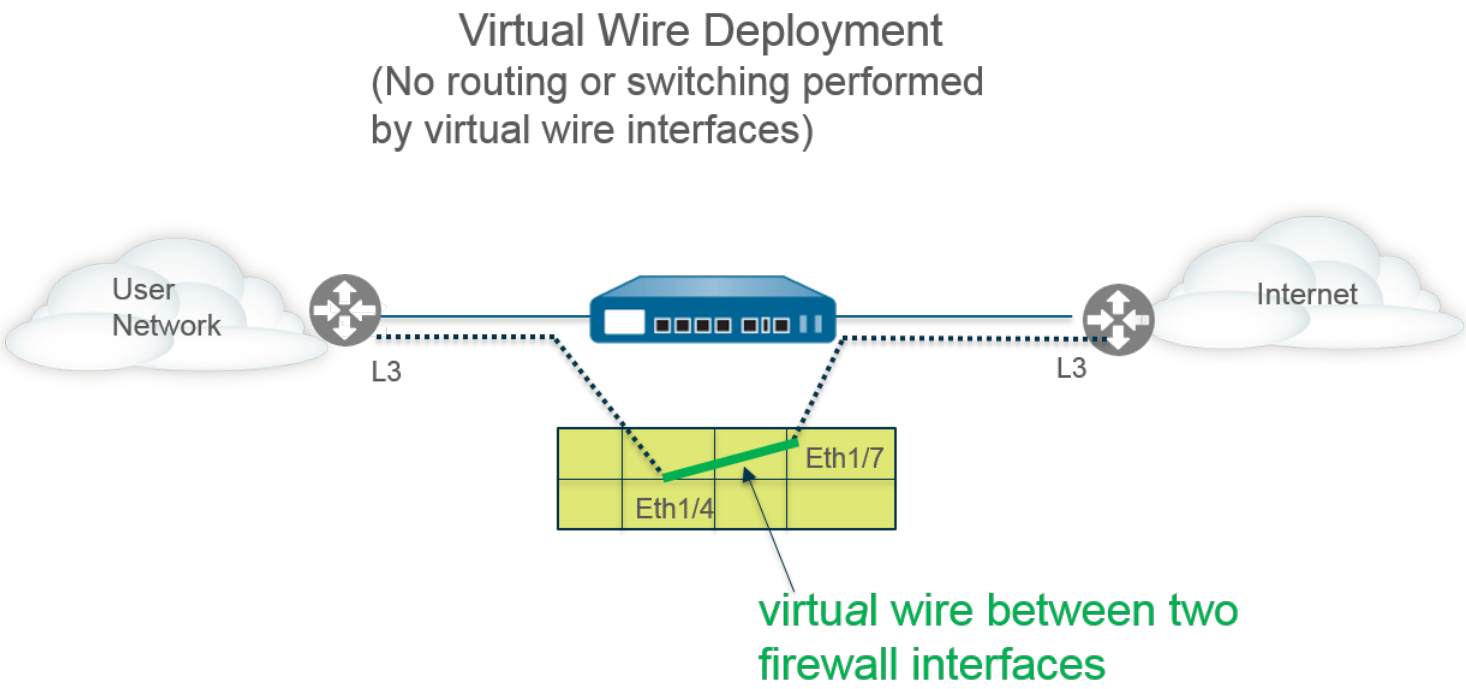
STEP 7 | 监控防火墙日志（**Monitor**（监控）> **Logs**（日志））和 **ACC** 以查看您网络上的应用程序和威胁。

## 虚拟线路接口

在虚拟线路部署中，通过将两个端口（接口）绑定在一起，将防火墙透明地安装在网段中。虚拟线路可实现两个接口的逻辑连接；因此，虚拟线路位于防火墙内部。

仅在要将防火墙无缝集成到拓扑中，并且防火墙上的两个已连接接口不需要进行任何交换或路由时，才能使用虚拟线路部署。防火墙将这个两个接口视为线路中的凸块。

虚拟线路部署使安装和配置防火墙更加简便，因为您可以将防火墙插入到现有拓扑中，而无需将 MAC 或 IP 地址分配给接口、重新设计网络或重新配置周边网络设备。除支持安全策略规则、App-ID、Content-ID、User-ID、解密、LLDP、主动/被动 HA 和主动/主动 HA、QoS、区域保护（有一些例外）、非 IP 协议保护、DoS 保护、数据包缓冲区保护、隧道内容检测和 NAT 之外，虚拟线路还支持阻止或允许基于虚拟 LAN (VLAN) 标记的流量。





© 2019 Palo Alto Networks, Inc.

每个虚拟线路接口都直接连接到第 2 层或第 3 层网络设备或主机。虚拟线路接口没有第 2 层或第 3 层地址。当其中一个虚拟线路接口接收到帧或数据包时，为了交换或路由目的，它会忽略任何第 2 层或第 3 层地址，但会在将允许的帧或数据包通过虚拟线路传送到第二个接口和与之相连接的网络设备之前应用您的安全或 NAT 策略规则。

对于需要支持交换、VPN 隧道或路由的接口，您不会使用虚拟线路部署，因为它们需要第 2 层或第 3 层地址。虚拟线路接口不使用能够提供控制 HTTP 和 ping 等服务的接口管理配置文件，因此要求接口具有 IP 地址。

所有出厂的防火墙都有两个预先配置为虚拟线路接口的以太网端口（端口 1 和 2），这些接口允许所有未标记的流量。



如果您在 *Cisco Trustsec* 网络内使用安全组标记 *(SGT)*，最好在第 *2* 层或虚拟线路模式下部署在线防火墙。第 *2* 层或虚拟线路模式下的防火墙可检查并提供标记流量的威胁阻止。



如果您不打算使用预配置的虚拟线路，则必须删除该配置，以防其与您在防火墙上配置的其他设置相干扰。请参阅设置外部服务的网络访问权。


- 虚拟线路上的第 2 层和第 3 层数据包
- 虚拟线路接口的端口速度
- 虚拟线路上的 LLDP
- 虚拟线路的聚合接口
- 虚拟线路支持高可用性
- 虚拟线路接口的区域保护
- VLAN 标记的流量
- Virtual Wire 子接口
- 配置虚拟线路


## 虚拟线路上的第 *2* 层和第 *3* 层数据包

只要应用于区域或接口的策略允许流量，虚拟线路接口将允许来自连接设备的第 2 层和第 3 层数据包透明地传递。虚拟线路接口本身不参与路由或交换。

例如，防火墙不会在通过虚拟链路的跟踪路由数据包中递减 TTL，因为该链路是透明的，并不会作为跃点计数。例如，操作、管理和维护 (OAM) 协议数据单元 (PDU) 等数据包不会在防火墙终止。因此，虚拟线路允许防火墙保持作为直通链路的透明状态，同时仍提供安全性、NAT 和 QoS 服务。

为了桥接协议数据单元 (BPDU) 和其他第 2 层控制数据包（通常未标记）通过虚拟线路，接口必须附加到允许未标记流量的虚拟线路对象，此为默认值。如果虚拟线路对象 **Tag Allowed**（允许的标记）字段为空，则虚拟线路允许未标记的流量。（安全策略规则不适用于第 2 层数据包。）

为了使路由（第 3 层）控制数据包通过虚拟线路，您必须应用允许流量通过的安全策略规则。例如，应用允许应用程序（如 BGP 或 OSPF）的安全策略规则。

如果要将安全策略规则应用于到达防火墙上虚拟线路接口的 IPv6 流量的区域，请启用 IPv6 防火墙。否则，IPv6 流量将通过线路透明地转发。

如果为虚拟线路对象启用多播防火墙，并将其应用于虚拟线路接口，则防火墙将根据安全策略规则检查多播流量并进行转发。如果不启用多播防火墙，则防火墙只能透明地转发多播流量。

虚拟线路上的分片与其他接口部署模式相同。

## 虚拟线路接口的端口速度

防火墙型号不同，提供的铜和光纤端口数量也各异，因此运行速度也不同。虚拟线路可以将相同类型（均为铜或均为光纤）的两个以太网端口绑定在一起，或将一个铜端口和一个光纤端口绑定在一起。防火墙上铜端口的 **Link Speed**（链接速度）默认设置为 **auto**（自动），这意味着防火墙会自动协商其速度和传输模



© 2019 Palo Alto Networks, Inc.

式（**Link Duplex**（链接双工））。配置虚拟线路时，您还可以选择特定的 **Link Speed**（链接速度）和 **Link Duplex**（链接双工），但任何单个虚拟线路上两个端口的这些设置的值均必须相同。

## 虚拟线路上的 *LLDP*

虚拟线路接口可以使用 LLDP 来发现相邻设备及其功能，而 LLDP 允许相邻设备检测网络中防火墙的存在。LLDP 简化了故障排除工作（尤其是在虚拟线路上），穿过虚拟线路的 ping 或 traceroute 通常无法检测到防火墙。LLDP 为其他设备提供了一种检测网络中防火墙的方法。没有 LLDP，网络管理系统几乎不可能通过虚拟链路来检测防火墙的存在。

## 虚拟线路的聚合接口

您可以为虚拟线路端口配置聚合接口组，但虚拟线路不得使用 LACP。如果在将防火墙连接至其他网络的设备上配置 LACP，则虚拟线路将以透明方式通过 LACP 数据包，而不执行 LACP 功能。



为了使聚合接口组正常运行，应确保将虚拟线路同侧相同 *LACP* 组的所有链路分配到同一个区域。

## 虚拟线路支持高可用性

如果使用虚拟线路路径组配置防火墙对高可用性进行路径监控，则防火墙会尝试通过在两个虚拟线路接口上发送 ARP 数据包来解析已配置目标 IP 地址的 ARP。正在监控的目标 IP 地址必须与虚拟线路周围的其中一台设备位于相同的子网上。

虚拟线路接口支持主动/被动和主动/主动 HA。对于具有虚拟线路的主动/主动 HA 部署，已扫描的数据包必须返回到接收防火墙中，以保留转发路径。因此，如果防火墙接收到的数据包属于对端 HA 防火墙拥有的会话，则会通过 HA3 链路将数据包发送给对端设备。

对于 PAN-OS 7.1 和更高版本，您可以配置 HA 对中的被动防火墙，以便在发生 HA 故障转移之前，允许防火墙任一侧的对端设备通过虚拟线路预先协商 LLDP 和 LACP。用于主动/被动 HA 的 LACP 及 LLDP 预先协商的这种配置加快了 HA 故障转移的速度。

## 虚拟线路接口的区域保护

您可以将区域保护应用到虚拟线路接口，但由于虚拟线路接口不执行路由，因此不能将基于数据包的攻击保护应用于带有欺诈 IP 地址的数据包，也不能抑制 ICMP TTL 过期错误数据包或 ICMP 碎片需要数据包。

虚拟线路接口默认转发所有接收到的非 IP 流量。但是，您可以使用具有协议保护功能的区域保护配置文件，阻止或允许虚拟线路上安全区域之间的某些非 IP 协议数据包。

## *VLAN* 标记的流量

虚拟线路接口默认允许所有未标记的流量。但是，您可以使用虚拟线路连接两个接口，并将其中一个接口配置为根据虚拟 LAN (VLAN) 标记阻止或允许通信的接口。VLAN 标记 0 表示未标记的流量。

您也可以创建多个子接口，将它们添加到不同区域，并根据 VLAN 标记或 VLAN 标记与 IP 分类器（地址、范围或子网）的组合对通信进行分类，以便应用特定 VLAN 标记的精细策略控制或从特定源 IP 地址、范围或子网应用 VLAN 标记的精细策略控制。

## *Virtual Wire* 子接口

虚拟线路部署可以使用虚拟线路子接口将流量隔离到区域内。当您需要管理多个客户网络的通信时，Virtual Wire 子接口使强制执行不同策略更加灵活。这些子接口可让您根据以下条件将通信隔离分类到不同区域（如有必要，这些区域可以分别属于独立的虚拟系统）：

- **VLAN** 标记 — 子接口的虚拟线路部署（仅适用于 VLAN 标记）中的示例显示 ISP 使用有 VLAN 标记的虚拟线路子接口对两个不同用户的通信进行隔离。


© 2019 Palo Alto Networks, Inc.

- **VLAN** 标记与 **IP** 分类器（地址、范围或子网）组合 — 下述示例显示 ISP 使用防火墙上的两个独立虚拟系统管理两个不同客户的通信。示例介绍了如何在每个虚拟系统上使用有 VLAN 标记和 IP 分类器的 Virtual Wire 子接口将通信分类到各个独立区域并从每个子网针对用户应用相关策略。

## Virtual Wire 子接口工作流程

- 配置两个 Virtual Wire 类型的以太网接口，并将其分别分配给一个 Virtual Wire。
- 在父级 Virtual Wire 上创建子接口来隔离 CustomerA 和 CustomerB 的通信。确保配置的 Virtual Wire 类型的每对子接口上定义的 VLAN 标记相同。这样做很有必要，因为 Virtual Wire 无法切换 VLAN 标记。
- 创建新的子接口，并定义 IP 分类器。您可以选择执行此任务，且仅当您希望添加带 IP 分类器的其他子接口以便根据 VLAN 标记和特定源 IP 地址、范围或子网的组合来进一步管理用户的通信时才需要执行此操作。

您也可以使用 IP 分类器来管理无标记通信。要执行此操作，您必须创建一个带 vlan 标记“0”的子接口，并使用 IP 分类器定义子接口，以便使用 IP 分类器来管理未标记的通信。

*IP* 分类只能在与 *Virtual Wire* 的一端关联的子接口上使用。*Virtual Wire* 的相应端上定义的各个子接口必须使用相同的 *VLAN* 标记，但不得包含 *IP* 分类器。

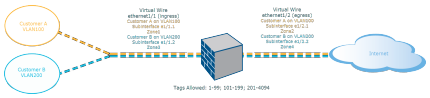


图 **10:** 子接口的 **Virtual Wire** 部署（仅适用于 **VLAN** 标记）

子接口的虚拟线路部署（仅适用于 VLAN 标记）图解显示了 CustomerA 和 CustomerB 通过第一个物理接口 ethernet1/1（配置为虚拟线路且为入口接口）连接到防火墙。第二个物理接口 ethernet1/2 也属于此虚拟线路，可用作出口接口以提供对 Internet 的访问。

对于 CustomerA，您也可以配置子接口 ethernet1/1.1（入口）和 ethernet1/2.1（出口）。对于 CustomerB，您可以配置子接口 ethernet1/1.2（入口）和 ethernet1/2.2（出口）。在配置子接口时，您必须分配合适的 VLAN 和区域以便为每个用户应用策略。在此示例中，CustomerA 的策略在区域 1 和区域 2 之间创建，CustomerB 的策略在区域 3 和区域 4 之间创建。

当通信从 CustomerA 或 CustomerB 进入防火墙时，传入数据包中的 VLAN 标记首先与入口接口上定义的 VLAN 标记相匹配。在此示例中，单个子接口与传入数据包中的 VLAN 标记相匹配，因此选择了此子接口。数据包从相应子接口离开之前，系统会评估和应用定义的区域策略。

不得在父级 *Virtual Wire* 接口和子接口上定义相同的 *VLAN* 标记。验证父级虚拟线路接口（*Network*（网络）> *Virtual Wires*（虚拟线路））的“允许的标记”列表中定义的 *VLAN* 标记不包含在子接口中。

子接口的虚拟线路部署（适用于 VLAN 标记和 IP 分类器）图解显示，除了默认虚拟系统 (vsys1) 之外，CustomerA 和 CustomerB 还连接到具有两个虚拟系统 (vsys) 的一个物理防火墙。每个虚拟系统都是针对每个用户分别进行管理的一个独立虚拟防火墙。每个虚拟系统都连接到独立管理的接口/子接口和安全区域。



© 2019 Palo Alto Networks, Inc.

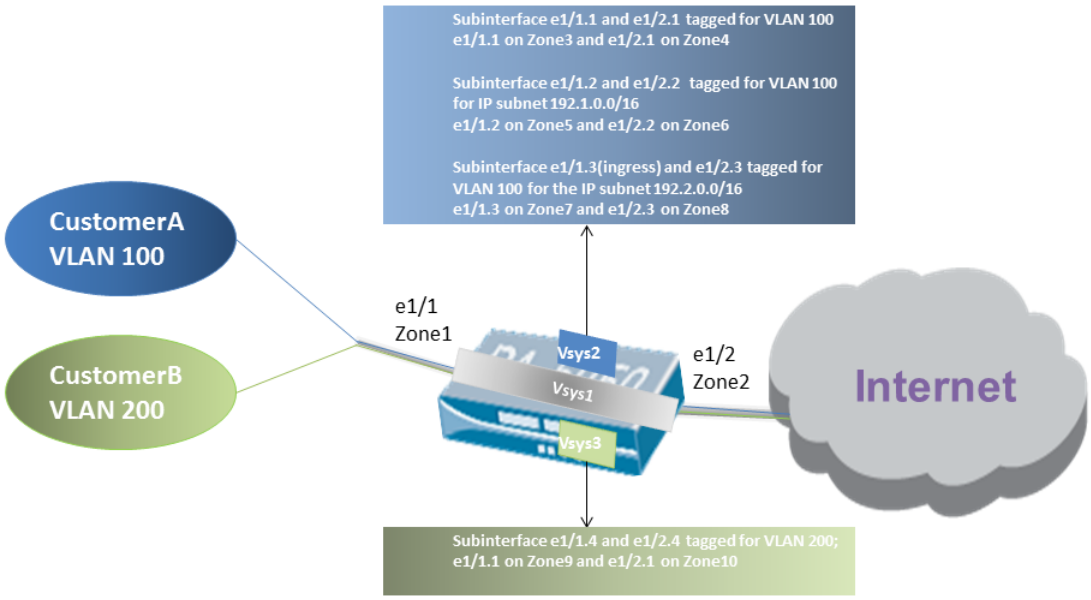



图 **11:** 子接口的 **Virtual Wire** 部署（适用于 **VLAN** 标记和 **IP** 分类器）

将 Vsys1 设置成使用物理接口 ethernet1/1 和 ethernet1/2 作为 Virtual Wire；ethernet1/1 用作接收接口，ethernet1/2 用作提供 Internet 访问的出口接口。将此 Virtual Wire 配置为接受除分配给子接口的 VLAN 标记 100 和 200 之外的所有已标记和无标记通信。

在 vsys2 中对 CustomerA 进行管理，在 vsys3 中对 CustomerB 进行管理。在 vsys2 和 vsys3 中，使用相应的 VLAN 标记和区域创建以下 vwire，以便强制执行各项策略。

| 用户 | Vsys | Vwire 子接口 | 区域 | VLAN 标记 | IP 分类器 |
|---|---|---|---|---|---|
| A | 2 | e1/1.1（入口）<br>e1/2.1（出口） | 区域 3<br>区域 4 | 100<br>100 | None |
| | 2 | e1/1.2（入口）<br>e1/2.2（出口） | 区域 5<br>区域 6 | 100<br>100 | IP 子网<br>192.1.0.0/16 |
| | 2 | e1/1.3（入口）<br>e1/2.3（出口） | 区域 7<br>区域 8 | 100<br>100 | IP 子网<br>192.2.0.0/16 |
| B | 3 | e1/1.4（入口）<br>e1/2.4（出口） | 区域 9<br>Zone10 | 200<br>200 | None |


© 2019 Palo Alto Networks, Inc.

当通信从 CustomerA 或 CustomerB 进入防火墙时，传入数据包中的 VLAN 标记首先与入口接口上定义的 VLAN 标记相匹配。在这种情况下，为 CustomerA 部署了多个使用相同 VLAN 标记的子接口。因此，防火墙首先要根据传入数据包中的源 IP 地址将通信分类缩窄到一个子接口。数据包从相应子接口离开之前，系统会评估和应用定义的区域策略。

对于返回路径通信，当在为用户部署的子接口上的 IP 分类器中定义 IP 地址时，防火墙将比较目标 IP 地址，并选择相应的 Virtual Wire 通过准确的子接口路由通信。

不得在父级 *Virtual Wire* 接口和子接口上定义相同的 *VLAN* 标记。验证父级虚拟线路接口（*Network*（网络）> *Virtual Wires*（虚拟线路））的“允许的标记”列表中定义的 *VLAN* 标记不包含在子接口中。

## 配置虚拟线路

以下任务说明如何配置两个虚拟线路接口来（在此示例中为 Ethernet 1/3 和 Ethernet 1/4）创建虚拟线路。两个接口必须具有相同的**Link Speed**（链接速度）和传输模式（**Link Duplex**（链接双工））。例如，全双工 1000 Mbps 铜端口匹配全双工 1 Gbps 光纤端口。

STEP 1 | 创建第一个虚拟线路接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择已启用的接口（在此示例中为 **ethernet1/3**）。
2. 将接口 **Interface Type**（接口类型）设置为 **Virtual Wire**（虚拟线路）。

STEP 2 | 将接口连接到虚拟线路对象。

1. 虽然仍在同一个以太网接口上，但在 **Config**（配置）选项卡上，选择 **Virtual Wire**（虚拟线路），并单击 **New Virtual Wire**（新建虚拟线路）。
2. 输入虚拟线路的 **Name**（名称）。
3. 对于 **Interface1**，选择刚配置的接口 (**ethernet1/3**)。（列表中仅显示配置为虚拟线路接口的接口。）
4. 对于 **Tag Allowed**（允许的标记），输入 **0** 表明允许未标记流量（如 BPDU 和其他第 2 层控制流量）。没有标记意味着标记为 0。输入其他允许的标记整数或标记范围，用逗号分隔（默认为 0；范围是 0 - 4094）。
5. 如希望将安全策略规则应用于通过虚拟线路的多播流量，请选择 **Multicast Firewalling**（多播防火墙）。否则，多播流量将以透明方式通过虚拟线路转发。
6. 选择 **Link State Pass Through**（链接状态传递），以便防火墙能够透明地运行。当防火墙检测到虚拟线路的链接呈链接断开状态时，就会导致虚拟线路对中的另一个接口掉线。因此，防火墙两侧设备的链接状态应一致，就好像它们之间没有防火墙一样。如果不选择此选项，链接状态不会传播到整个虚拟线路。
7. 单击 **OK**（确定）以保存虚拟线路对象。

STEP 3 | 确定虚拟线路接口的链接速度。

1. 虽然仍在同一个以太网接口上，但请选择 **Advanced**（高级），并注明或更改 **Link Speed**（链接速度）。端口类型确定列表中可用的速度设置。默认情况下，铜端口设置为 **auto**（自动）协商链接速度。两个虚拟线路接口均必须具有相同的链接速度。
2. 单击 **OK**（确定）以保存以太网接口。

STEP 4 | 通过重复上述步骤配置第二个虚拟线路接口（在本示例中为 **ethernet1/4**）。

选择创建的 **Virtual Wire**（虚拟线路）对象后，防火墙会自动将第二个虚拟线路接口添加为 **Interface2**。

STEP 5 | 为每个虚拟线路接口创建一个单独的安全区域。

1. 选择 **Network**（网络）> **Zones**（区域）并 **Add**（添加）区域。
2. 输入区域 **Name**（名称），例如 **`internet`**。
3. 对于 **Location**（位置），请选择区域应用的虚拟系统。



© 2019 Palo Alto Networks, Inc.

4. 对于 **Type**（类型），请选择 **Virtual Wire**（虚拟线路）。
5. **Add**（添加）属于该区域的 **Interface**（接口）。
6. 单击 **OK**（确定）。

STEP 6 | （可选）创建安全策略规则，允许第 3 层流量通过。

要允许第 3 层流量通过虚拟线路，请创建安全策略规则以允许流量从用户区域流到互联网区域，并选择要允许的应用程序（如 BGP 或 OSPF），允许流量从互联网区域流到用户区域。

STEP 7 | （可选）启用 IPv6 防火墙。

如果要将安全策略规则应用于到达虚拟线路接口的 IPv6 流量，请启用 IPv6 防火墙。否则，IPv6 流量会以透明方式转发。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 选择 **Enable IPv6 Firewalling**（启用 **IPv6** 防火墙）。
3. 单击 **OK**（确定）。

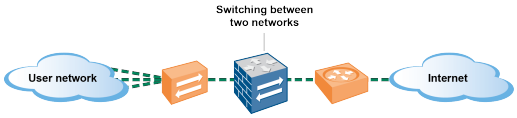
STEP 8 | **Commit**（提交）更改。

STEP 9 | （可选）配置 LLDP 配置文件并将其应用于虚拟线路接口（请参阅 配置 LLDP）。

STEP 10 | （可选）将非 IP 协议控制应用于虚拟线路区域（请参阅 配置协议保护）。否则，所有非 IP 流量都将通过虚拟线路转发。

# 第 2 层接口

在第 2 层的部署中，防火墙提供了两个或更多网络之间的交换。设备连接到第 2 层分段；防火墙将帧转发到正确的端口，该端口与帧中标识的 MAC 地址相关联。需要交换时配置第 2 层接口。




如果您在 *Cisco TrustSec* 网络内使用安全组标记 *(SGT)*，最好在第 *2* 层或虚拟线路模式下部署在线防火墙。第 *2* 层或虚拟线路模式下的防火墙可检查并提供标记流量的威胁阻止。

以下主题描述了您可以为所需的每种类型配置不同类型的第 2 层接口，其中包括使用虚拟 LAN (VLAN) 分离组间流量和策略有关的详细信息。另一个主题描述的是防火墙如何重写 Cisco 每个 VLAN 生成树 (PVST+) 或快速 PVST+ 桥接协议数据单元 (BPDU) 的入站端口 VLAN ID 号。

- 不带 VLAN 的第 2 层接口
- 带 VLAN 的第 2 层接口
- 配置第 2 层接口
- 配置第 2 层接口、子接口和 VLAN
- 管理每个 VLAN 生成树 (PVST+) BPDU 重写

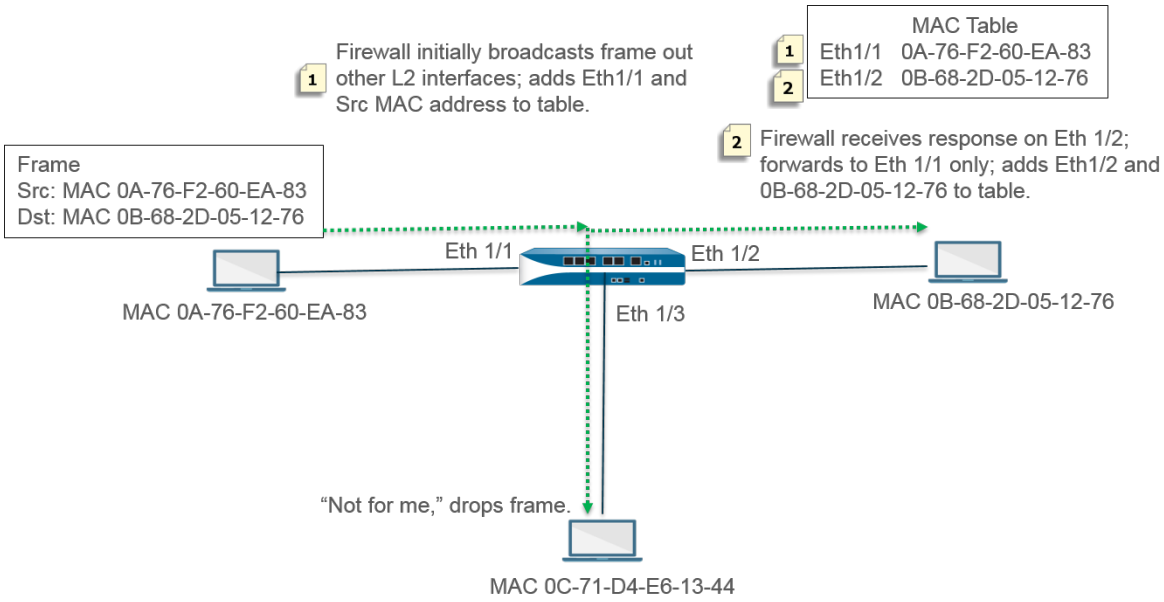
## 不带 *VLAN* 的第 *2* 层接口

配置第 2 层接口，以便其可以充当第 2 层网络中的交换机（不在网络边缘）。第 2 层主机可能在地理上彼此靠近，属于单个广播域。当您将接口分配给安全区域并将安全规则应用于该区域时，防火墙在第 2 层主机之间提供安全性。


© 2019 Palo Alto Networks, Inc.

主机通过帧交换在 OSI 模型的第 2 层与防火墙以及彼此之间进行通信。帧包含以太网标头，包括源和目标介质访问控制 (MAC) 地址，该地址是物理硬件地址。MAC 地址是 48 位十六进制数字，已格式化为六个八位字节，由冒号或连字符隔开（例如，00-85-7E-46-F1-B2）。

下图是具有三个第 2 层接口的防火墙，每个接口都以一对一的映射方式连接到第 2 层主机。




防火墙以空的 MAC 表开始。当源地址为 0A-76-F2-60-EA-83 的主机向防火墙发送帧时，防火墙的 MAC 表中没有目标地址 0B-68-2D-05-12-76，因此不知道向哪个接口转发帧；它将该帧广播到其所有第 2 层接口。防火墙将源地址为 0A-76-F2-60-EA-83 和相关联的 Eth1/1 放入其 MAC 表中。

地址为 0C-71-D4-E6-13-44 的主机接收广播，但目标 MAC 地址不是自己的 MAC 地址，所以将帧丢弃。

接收接口 Ethernet 1/2 将帧转发到其主机。当主机 0B-68-2D-05-12-76 响应时，会使用目标地址 0A-76-F2-60-EA-83，防火墙将 MAC 表 Ethernet 1/2 作为接口访问 0B-68-2D-05-12-76。

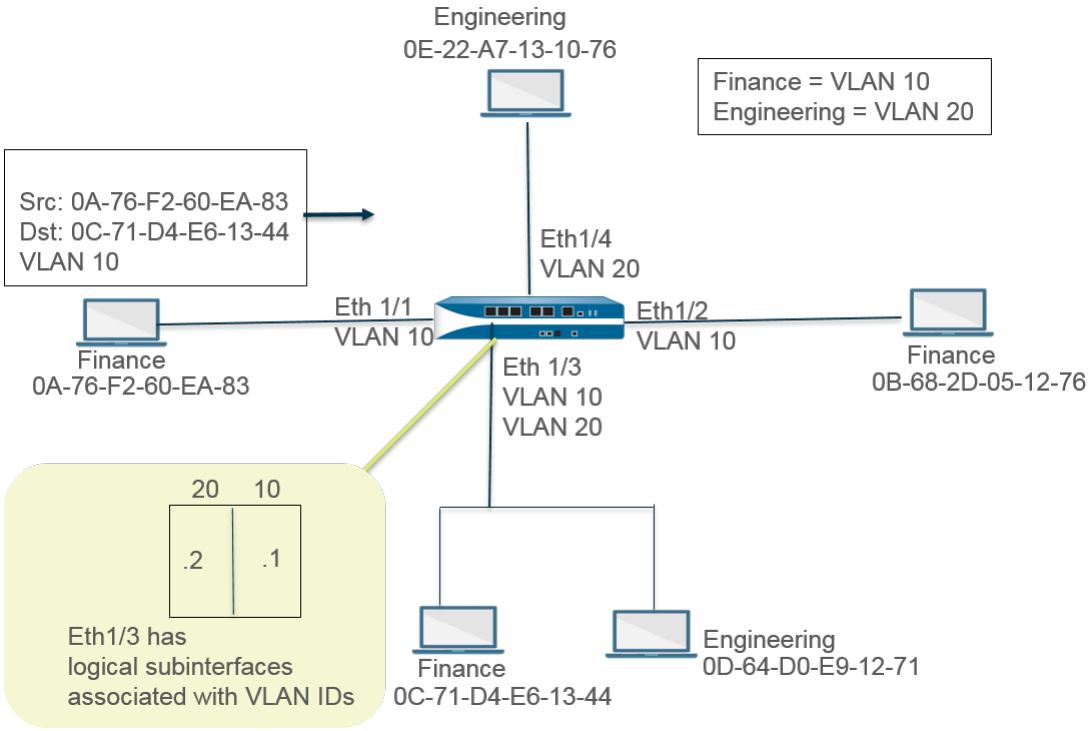
## 带 *VLAN* 的第 *2* 层接口

当您的组织想将 LAN 划分为单独的虚拟 LAN (VLAN)，以分离不同部门的流量和策略时，可以将第 2 层主机逻辑分组为 VLAN，从而将第 2 层网段划分为广播域。例如，您可以为财务部和工程部创建 VLAN。为此，配置第 2 层接口、子接口和 VLAN。

防火墙充当交换机，使用包含 VLAN ID 的以太网标头转发帧，并且目标接口必须具有该 VLAN ID 的子接口，以便接收该帧并将其转发给主机。在防火墙上配置第 2 层接口，并为接口配置一个或多个逻辑子接口，每个接口都带有 VLAN 标记 (ID)。

在下图中，防火墙有四个第 2 层接口，均连接到属于组织内不同部门的第 2 层主机。以太网接口 1/3 已配置子接口 .1（标记为 VLAN 10）和子接口 .2（标记为 VLAN 20），因此该段有两个广播域。VLAN 10 中的主机属于财务部；VLAN 20 中的主机属于工程部。


© 2019 Palo Alto Networks, Inc.




本例中，MAC 地址为 0A-76-F2-60-EA-83 的主机向防火墙发送 VLAN ID 为 10 的帧，防火墙向其另外的 L2 接口广播。以太网接口 1/3 接受该帧，因为它连接到目标为 0C-71-D4-E6-13-44 的主机，其子接口 .1 是已分配的 VLAN 10。以太网接口 1/3 将帧转发到财务部主机。

## 配置第 *2* 层接口

如果要进行第 2 层交换，并且不需要在 VLAN 间分隔通信，则配置不带 VLAN 的第 2 层接口 。

STEP 1 | 配置第 2 层接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并选择一个接口。**Interface Name**（接口名称）已固定，如 ethernet1/1。
2. 对于 **Interface Type**（接口类型），请选择 **Layer2**（第 2 层）。
3. 选择 **Config**（配置）选项卡，并将接口分配到 **Security Zone**（安全区域），或创建一个 **New Zone**（新区域）。
4. 在与第 2 层主机相连接的防火墙上配置其他第 2 层接口。

STEP 2 | 提交。

单击 **OK**（确定）和 **Commit**（提交）。

## 配置第 *2* 层接口、子接口和 *VLAN*

如果要进行第 2 层交换，并且需要在 VLAN 间分隔通信，则配置带 VLAN 的第 2 层接口。您可以控制第 2 层接口上安全区域之间的非 IP 协议，也可以控制第 2 层 VLAN 上单个区域内接口之间的非 IP 协议。

STEP 1 | 配置第 2 层接口和子接口，并分配 VLAN ID。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并选择一个接口。**Interface Name**（接口名称）已固定，如 ethernet1/1。
2. 对于 **Interface Type**（接口类型），请选择 **Layer2**（第 2 层）。
3. 选择 **Config**（配置）选项卡。
4. 对于 **VLAN**，请将设置保留为 **None**（无）。


© 2019 Palo Alto Networks, Inc.

5. 将接口分配到 **Security Zone**（安全区域）或创建一个 **New Zone**（新区域）。
6. 单击 **OK**（确定）。
7. 突出显示以太网接口，单击 **Add Subinterface**（添加子接口）。
8. **Interface Name**（接口名称）保持固定。之后，输入子接口号，范围为 1-9,999。
9. 输入 VLAN **Tag**（标记）ID，范围为 1-4,094。
10. 将子接口分配到 **Security Zone**（安全区域）。
11. 单击 **OK**（确定）。

STEP 2 | 提交。

单击 **Commit**（提交）。

STEP 3 | （可选）应用具有协议保护功能的区域保护配置文件，以控制第 2 层区域之间（或第 2 层区域内接口之间）的非 IP 协议数据包。

配置协议保护。

## 管理每个 *VLAN* 生成树 *(PVST+) BPDU* 重写

在防火墙上为第 2 层部署配置接口时，防火墙重写 Cisco 每个 VLAN 生成树 (PVST+) 或快速 PVST+ 桥接协议数据单元 (BPDU) 的入站端口 VLAN ID (PVID) 号至适当的出站 VLAN ID 号，并将 BPDU 转发出。这种默认行为从 PAN-OS 7.1 开始，允许防火墙正确标记位于防火墙各侧 VLAN 中 Cicso 交换机之间的 Cicso 专有 PVST+ 和快速 PVST+ 帧，这样，使用 Cisco PVST+ 和快速 PVST+ 执行的生成树回环检测就能正常运行。防火墙未参与生成树协议 (STP) 选择过程，因此，对于其他类型的生成树而言，没有行为更改。

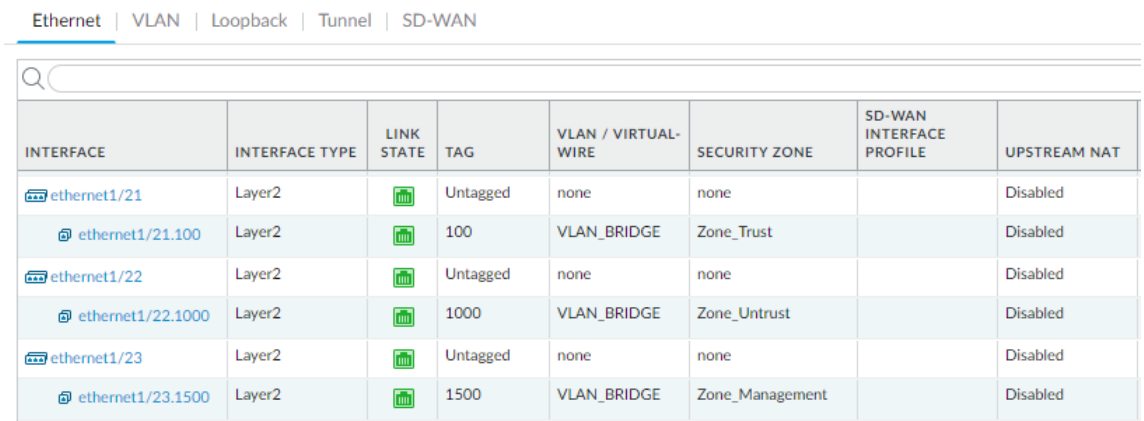
*Cisco* 交换机必须禁用回环保护，从而在防火墙上顺利进行 *PVST+* 或快速 *PVST+ BPDU* 重写。

只有第 2 层以太网和聚合以太网 (AE) 接口支持此功能。防火墙支持的 PVID 范围为 1-4,094，本征 VLAN ID 为 1，以便与 Cicso 本征 VLAN 实施兼容。

为支持 PVST+ BPDU 重写功能，PAN-OS 支持 PVST+ 本征 VLAN 概念。发送至和接收自本征 VLAN 的帧已被取消标记，且 PVID 等同于本征 VLAN。位于相同第 2 层部署中的所有交换机和防火墙必须拥有相同的本征 VLAN，以使 PVST+ 正常运行。虽然 Cicso 本征 VLAN 默认为 vlan1，但是，VLAN ID 也可以是除 1 之外的编号。

例如，防火墙配置有用于描述属于交换机或广播域的接口和子接口的 VLAN 对象（名为 VLAN_BRIDGE）。在此示例中，VLAN 包括三个子接口：标记为 100 的 ethernet1/21.100、标记为 1000 的 ethernet1/22.1000、以及标记为 1500 的 ethernet1/23.1500。

属于 VLAN_BRIDGE 的子接口如下所示：

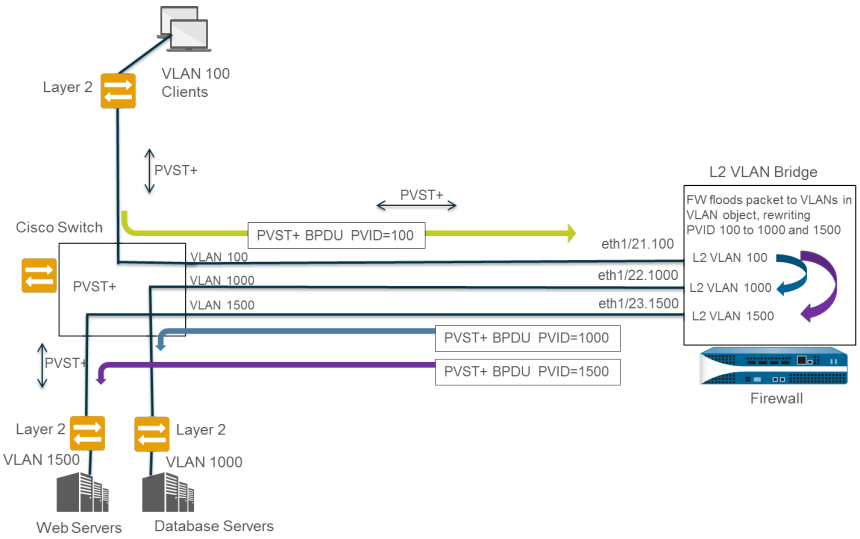



| INTERFACE | INTERFACE TYPE | LINK STATE | TAG | VLAN / VIRTUAL-WIRE | SECURITY ZONE | SD-WAN INTERFACE PROFILE | UPSTREAM NAT |
|---|---|---|---|---|---|---|---|
| ethernet1/21 | Layer2 | | Untagged | none | none | | Disabled |
| ethernet1/21.100 | Layer2 | | 100 | VLAN_BRIDGE | Zone_Trust | | Disabled |
| ethernet1/22 | Layer2 | | Untagged | none | none | | Disabled |
| ethernet1/22.1000 | Layer2 | | 1000 | VLAN_BRIDGE | Zone_Untrust | | Disabled |
| ethernet1/23 | Layer2 | | Untagged | none | none | | Disabled |
| ethernet1/23.1500 | Layer2 | | 1500 | VLAN_BRIDGE | Zone_Management | | Disabled |



© 2019 Palo Alto Networks, Inc.

防火墙自动重写 PVST+ BPDU 的序列通过下图和描述进行显示：




1. 属于 VLAN 100 的 Cicso 交换机端口发送 PVST+ BPDU（带 PVID，且 802.1Q VLAN 标记为 100）至防火墙。
2. 防火墙接口和子接口配置为第 2 层接口类型。防火墙上的入口子接口标记为 VLAN 100，这与 PVID 和传入 BPDU 的 VLAN 标记匹配，因此，防火墙接受此 BPDU。防火墙将 PVST+ BPDU 洪泛到属于同一 VLAN 对象的所有其他接口（在此示例中，为 ethernet1/22.1000 和 ethernet1/23.1500）。如果 VLAN 标记不匹配，则防火墙会丢弃 BPDU。
3. 当防火墙将 BPDU 洪泛至属于同一 VLAN 对象的其他接口时，防火墙会重写 PVID 和任何与出口接口 VLAN 标记相匹配的 802.1Q VLAN 标记。在此示例中，当 BPDU 遍历防火墙上的第 2 层桥接时，防火墙重写 CPDU PVID，一个子接口为 100-1000，第二个子接口为 100-1500。
4. 每个 Cicso 交换机都会接收传入 BPDU 上的正确 PVID 和 VLAN 标记，并处理 PVST+ 数据包以检测网络中可能存在的回环。

您可以通过以下 CLI 操作命令管理 PVST+ 和快速 PVST+ BPDU。

- 全局禁用或重新启用 PVID 的 PVST+ 和快速 PVST+ BPDU 重写（默认为启用）。

  **set session rewrite-pvst-pvid <yes|no>**

- 设置用于防火墙的本征 VLAN ID（范围为 1-4,094；默认为 1）。

  如果交换机上的本征 *VLAN ID* 值不是 *1*，则必须将防火墙上的本征 *VLAN ID* 设为相同值，否则，防火墙将丢弃具有该 *VLAN ID* 的数据包。这也适用于中继和非中继接口。

  **set session pvst-native-vlan-id <*vid*>**

- 丢弃所有 STP BPDU 数据包。

  **set session drop-stp-packet <yes|no>**

  为何想要丢弃所有 STP BPDU 数据包的示例：

  - 如果防火墙各侧只有一个交换机，且交换机之间不存在导致回环的任何其他连接，那么，就不需要 STP，且可以在交换机上禁用 STP，或是防火墙会阻止 STP。
  - 如果因 STP 交换机行为不当导致不正常的 BPDU 洪泛，则可以在防火墙上停止 STP 数据包，从而停止 BPDU 洪泛。


© 2019 Palo Alto Networks, Inc.

- 验证 PVST+BPDU 重写是否启用，查看 PVST 本征 VLAN ID，并确定防火墙是否正在丢弃所有 STP BPDU 数据包。

  **show vlan all**

  ```
  pvst+ tag rewrite: disabled
  pvst native vlan id:    5
  drop stp:                disabled
  total vlans shown:      1
  name      interface           virtual interface
  bridge    ethernet1/1
            ethernet1/2
            ethernet1/1.1
            ethernet1/2.1
  ```

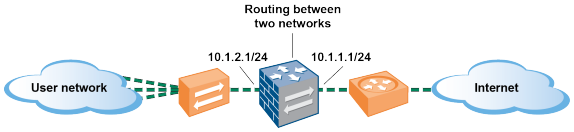
- 对 PVST+ BPDU 错误执行故障排除。

  **show counter global**

  查看 `flow_pvid_inconsistent` 计数器。该计数器计算 PVST+ BPDU 数据包中 802.1Q 标记和 PVID 字段不匹配的次数。

# 第 3 层接口

在第 3 层部署中，防火墙在多个端口之间进行路由通信。在配置第 3 层接口之前，必须配置要防火墙用于路由每个第 3 层接口流量的虚拟路由器。




如果您在 *Cisco TrustSec* 网络内使用安全组标记 *(SGT)*，最好在第 *2* 层或虚拟线路模式下部署在线防火墙。但是，如果您需要在 *Cisco TrustSec* 网络中使用第 *3* 层防火墙，您应在两个 *SGT* 交换协议 *(SXP)* 对等设备之间部署第 *3* 层防火墙，并配置防火墙以允许 *SXP* 对等设备之间的流量。

以下主题介绍如何配置第 3 层接口，以及如何使用邻居发现协议 (NDP) 配置 IPv6 主机，并查看链接本地网络上设备的 IPv6 地址，以便快速定位设备。

- 配置第 3 层接口
- 使用 NDP 管理 IPv6 主机

## 配置第 3 层接口

使用 IPv4 或 IPv6 地址配置第 3 层接口（以太网、VLAN、回环和隧道接口）需要执行以下步骤，以使防火墙能够在这些接口上进行路由。如果隧道用于路由或隧道监控功能打开，则隧道需要 IP 地址。执行以下任务之前，请定义一个或多个虚拟路由器。

通常，您可以使用以下步骤来配置连接到互联网的外部接口和内网接口。您可以在单个接口上配置 IPv4 和 IPv6 地址。



© 2019 Palo Alto Networks, Inc.

*PAN-OS* 防火墙模式最多支持 *16,000* 个分配给物理或第 *3* 层虚拟接口的 *IP* 地址；此最大值包括 *IPv4* 和 *IPv6* 地址。

如果使用 IPv6 路由，则可以配置防火墙以为 DNS 配置提供 IPv6 路由器通告。防火墙配置具有递归 DNS 服务器 (RDNS) 地址和 DNS 搜索列表的 IPv6 DNS 客户端，以便客户端可以解析其 IPv6 DNS 请求。因此，防火墙对您而言就像一个 DHCPv6 服务器。

STEP 1 | 选择一个接口并配置一个安全区域。

1. 选择 **Network**（网络）> **Interfaces**（接口）以及 **Ethernet**（以太网）、**VLAN**、**loopback**（回环）或 **Tunnel**（隧道），具体取决于所需的接口类型。
2. 选择要配置的接口。
3. 选择 **Interface Type**（接口类型）— **Layer3**（第 **3** 层）。
4. 在 **Config**（配置）选项卡上，对于 **Virtual Router**（虚拟路由器），选择正在配置的虚拟路由器，例如 **default**（默认）。
5. 对于 **Virtual System**（虚拟系统），如果是多虚拟系统防火墙，请选择正在配置的虚拟系统。
6. 对于 **Security Zone**（安全区域），选择接口所属的区域或创建 **New Zone**（新区域）。
7. 单击 **OK**（确定）。

STEP 2 | 配置 IPv4 地址的接口。

您可以通过以下三种方式之一为第 3 层接口分配 IPv4 地址：

- 静态
- DHCP 客户端 -— 防火墙接口充当 DHCP 客户端，并接收动态分配的 IP 地址。防火墙还可以将 DHCP 客户端接口收到的设置传播到在防火墙上运行的 DHCP 服务器中。这点最常用于将 DNS 服务器设置从互联网服务提供商传播到在受防火墙保护的网络上运行的客户端计算机中。
- PPPoE — 将接口配置为以太网上的点对点协议 (PPPoE) 终止点，以支持在数字用户线路 (DSL) 环境中进行连接，该环境中有 DSL 调制解调器，但没有其他 PPPoE 设备可终止连接。

1. 选择 **Network**（网络）> **Interfaces**（接口）以及 **Ethernet**（以太网）、**VLAN**、**loopback**（回环）或 **Tunnel**（隧道），具体取决于所需的接口类型。
2. 选择要配置的接口。
3. 要使用静态 IPv4 地址配置接口，请在 **IPv4** 选项卡上将 **Type**（类型）设置为 **Static**（静态）。
4. **Add**（添加）地址的 **Name**（名称）和 **Description**（说明）（可选）。
5. 对于 **Type**（类型），请选择以下选项之一：
   - **IP Netmask**（**IP** 子网掩码）— 输入要分配给接口的 IP 地址和子网掩码，例如 208.80.56.100/24。

     如果您为第 *3* 层接口地址使用 */31* 子网掩码，则接口必须配置有 *.1/31* 地址，以便 *ping* 等实用程序正常运行。

     如果配置的回环接口使用 *IPv4* 地址，该接口必须有一个 */32* 子网掩码；例如，*192.168.2.1/32*。
   - **IP Range**（**IP** 范围）— 输入 IP 地址范围，例如 192.168.2.1-192.168.2.4。
   - **FQDN** — 输入完全限定域名。
6. 选择要应用该地址的 **Tags**（标签）。
7. 单击 **OK**（确定）。

STEP 3 | 使用以太网上的点对点协议 (PPPoE) 配置接口。请参阅第 3 层接口。

*PPPoE* 在 *HA* 主动/主动模式下不受支持。


© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **Interfaces**（接口）以及 **Ethernet**（以太网）、**VLAN**、**loopback**（回环）或 **Tunnel**（隧道）。
2. 选择要配置的接口。
3. 在 **IPv4** 标签中，将 **Type**（类型）设置为 **PPPoE**。
4. 在 **General**（常规）选项卡上，选择 **Enable**（启用）激活 PPPoE 终止界面。
5. 输入用于点对点连接的 **Username**（用户名）。
6. 输入用户名的 **Password**（密码）和 **Confirm Password**（确认密码）。
7. 单击 **OK**（确定）。

STEP 4 | 将接口配置为 DHCP 客户端这样，就可接收动态分配的 IPv4 地址。



*DHCP* 客户端在 *HA* 主动/主动模式下不受支持。

STEP 5 | 配置带静态 IPv6 地址的接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）以及 **Ethernet**（以太网）、**VLAN**、**loopback**（回环）或 **Tunnel**（隧道）。
2. 选择要配置的接口。
3. 在 **IPv6** 选项卡上，选择接口上的 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）在接口上启用 IPv6 寻址。
4. 对于 **Interface ID**（接口 **ID**），请以十六进制格式输入 64 位扩展唯一标识符 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果将此字段留空，则防火墙使用根据物理接口的 MAC 地址生成的 EUI-64。如果在添加地址时启用 **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）选项，则防火墙使用接口 ID 作为该地址的主机部分。
5. **Add**（添加）IPv6 **Address**（地址）或选择一个地址组。
6. 选择 **Enable address on interface**（在接口上启用地址）在接口上启用此 IPv6 地址。
7. 选择 **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）将接口 ID 用作 IPv6 地址的主机部分。
8. （可选）选择 **Anycast**（任意播）使 IPv6 地址（路由）为任意播地址（路由），这意味着多个位置可以通告相同的前缀，然后 IPv6 发送任意播流量到它认为最接近的节点，取决于路由协议成本和其他因素。
9. （仅限以太网接口）选择 **Send Router Advertisement**（发送路由器通告）(RA)，使防火墙能够在路由器通告中发送该地址，在这种情况下，您还必须在接口上启用全局 **Enable Router Advertisement**（启用路由器通告）（下一步）。
10. （仅限以太网接口）以秒输入防火墙认为该地址有效的 **Valid Lifetime (sec)**（有效生存时间（秒））。有效生命周期必须等于或超过 **Preferred Lifetime(sec)**（首选生存时间（秒））（默认为 2,592,000）。
11. （仅限以太网接口）以秒输入有效地址首选的 **Preferred Lifetime(sec)**（首选生存时间（秒）），这意味着防火墙可以使用它来发送和接收流量。在首选生存时间到期后，防火墙不能使用此地址来建立新的连接，但在 **Valid Lifetime**（有效生存时间）到期（默认为 604,800）之前，任何现有的连接都是有效的。
12. （仅限以太网接口）如果能在不使用路由器的情况下访问前缀中包含地址的系统，请选择 **On-link**（在链路上）。
13. （仅限以太网接口）如果系统可以通过结合使用通告前缀和接口 IP 来独立创建 IP 地址，请选择 **Autonomous**（自治）。
14. 单击 **OK**（确定）。

STEP 6 | （仅使用 IPv6 地址的以太网或 VLAN 接口）启用防火墙从接口发送 IPv6 路由器通告 (RA)，并调整 RA 参数（可选）。



© 2019 Palo Alto Networks, Inc.

出于以下任一原因，调整 *RA* 参数：与使用不同值的路由器/主机进行互操作。为了在存在多个网关时实现快速收敛。例如，设置较低的 *Min Interval*（最小间隔）、*Max Interval*（最大间隔）和 *Router Lifetime*（路由器生存时间）值，以便 *IPv6* 客户端/主机可以在主网关出现故障后快速更改默认网关，并开始转发到网络中的另一个默认网关。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择要配置的接口。
3. 选择 **IPv6**。
4. 选择 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。
5. 在 **Router Advertisement**（路由器通告）选项卡上，选择 **Enable Router Advertisement**（启用路由器通告）（默认为禁用）。
6. （可选）设置防火墙发送 RA 之间的 **Min Interval (sec)**（最小间隔（秒）），即最小间隔，单位为秒（范围为 3-1,350；默认为 200）。防火墙将会以您配置的最小值和最大值之间的随机间隔发送路由器通告。
7. （可选）设置防火墙发送 RA 之间的 **Max Interval (sec)**（最大间隔（秒）），即最大间隔，单位为秒（范围为 4-1,800；默认值为 600）。防火墙将会以您配置的最小值和最大值之间的随机间隔发送路由器通告。
8. （可选）设置适用于发送数据包的客户端的 **Hop Limit**（跃点限制）（范围为 1-255，默认为 64）。输入 0 表示没有跃点限制。
9. （可选）设置 **Link MTU**（链路 **MTU**），用于客户端的链路最大传输单元 (MTU)（范围为 1,280-9,192；默认为 **unspecified**（未指定））。选择 **unspecified**（未指定），用于无链路 MTU。
10. （可选）设置 **Reachable Time (ms)**（可访问时间（毫秒）），该时间是客户端用于在收到可访问性确认消息后假定可以访问相邻设备的时间。选择 **unspecified**（未指定）表示没有可访问时间值（范围为 0 至 3,600,000，默认为**unspecified**（未指定））。
11. （可选）设置 **Retrans Time (ms)**（重传时间（毫秒）），客户端将使用重传计时器确定在重传邻居请求消息之前需要等待的时间（毫秒）。选择 **unspecified**（未指定）表示没有重传时间（范围为 0 至 4,294,967,295，默认为**unspecified**（未指定））。
12. （可选）设置 **Router Lifetime (sec)**（路由器生存时间（秒）），用于指定客户端将使用防火墙作为默认网关的时间（范围为 0-9,000；默认为 1,800）。零用于指定防火墙不是默认网关。当生存时间到期后，客户端会从其默认路由器列表删除防火墙条目，并将另一个路由器用作默认网关。
13. 设置 **Router Preference**（路由器首选项），客户端在网段具有多个 IPv6 路由器时用于选择首选路由器。**High**（高）、**Medium**（中）（默认）或 **Low**（低）是 RA 通告的优先级，表示与分段上其他路由器相关的防火墙虚拟路由器的相关优先级。
14. 选择 **Managed Configuration**（管理配置）以向客户端指示可通过 DHCPv6 使用该地址。
15. 选择 **Other Configuration**（其他配置）可向客户端表明可通过 DHCPv6 使用其他地址信息（例如，DNS 相关设置）。
16. 选择 **Consistency Check**（一致性检查）使防火墙验证从其他路由器发送的 RA 在链路上通告的消息是否一致。防火墙会记录任何不一致。
17. 单击 **OK**（确定）。

STEP 7 | （仅使用 IPv6 地址的以太网或 VLAN 接口）指定防火墙将在该接口的 ND 路由器通告中通告的递归 DNS 服务器地址和 DNS 搜索列表。

RDNS 服务器和 DNS 搜索列表是 DNS 客户端的 DNS 配置的一部分，以便客户端可以解析 IPv6 DNS 请求。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择正在配置的接口。
3. 选择**IPv6** > **DNS Support**（**DNS** 支持）。
4. **Include DNS information in Router Advertisement**（在路由器通告中包含 **DNS** 信息）可以使防火墙发送 IPv6 DNS 信息。


© 2019 Palo Alto Networks, Inc.

5. 对于 DNS **Server**（服务器），**Add**（添加）递归 DNS 服务器的 IPv6 地址。**Add**（添加）最多八个递归 DNS 服务器。防火墙按照从上到下的顺序发送 ICMPv6 路由器通告中的服务器地址。
6. 以秒为单位指定 **Lifetime**（生存时间），这是客户端可以使用特定 RDNS 服务器解析域名的最长秒数。
   - **Lifetime**（生存时间）范围是等于或介于 **Max Interval**（最大间隔）（在 **Router Advertisement**（路由器通告）选项卡上配置）和 **Max Interval**（最大间隔）的两倍之间的任何值。例如，如果您的最大间隔为 600 秒，则生存时间范围为 600-1,200 秒。
   - 默认 **Lifetime**（生存时间）为 1,200 秒。
7. 对于 DNS 后缀，**Add**（添加）**DNS Suffix**（**DNS** 后缀）（域名最多为 255 个字节）。**Add**（添加）最多八个 DNS 后缀。防火墙按照从上到下的顺序在 ICMPv6 路由器通告中发送后缀。
8. 以秒为单位指定 **Lifetime**（生存时间），这是客户端可以使用后缀的最长秒数。生命周期具有与 **Server**（服务器）相同的范围和默认值。
9. 单击 **OK**（确定）。

STEP 8 | （以太网或 VLAN 接口）指定静态 ARP 条目。静态 ARP 条目减少 ARP 处理。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择正在配置的接口。
3. 选择 **Advanced**（高级）> **ARP Entries**（**ARP** 条目）。
4. **Add**（添加）**IP Address**（**IP** 地址）及其对应的 **MAC Address**（**MAC** 地址）（硬件或介质访问控制地址）。对于 VLAN 接口，还必须选中 **Interface**（接口）。

   静态 *ARP* 条目不会超时。默认情况下，缓存中自动获取的 *ARP* 条目超时 *1800* 秒；您可以自定义 *ARP* 缓存超时；请参阅配置会话超时。
5. 单击 **OK**（确定）。

STEP 9 | （以太网或 VLAN 接口）指定静态邻居发现协议 (NDP) 条目。IPv6 的 NDP 执行的功能类似于 IPv4 的 ARP 提供的功能。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择正在配置的接口。
3. 选择 **Advanced**（高级）> **ND Entries**（**ND** 条目）。
4. **Add**（添加）**IPv6 Address**（**IPv6** 地址）及其相应的 **MAC Address**（**MAC** 地址）。
5. 单击 **OK**（确定）。

STEP 10 | （可选）启用接口上的服务。

1. 要在接口上启用服务，请选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择正在配置的接口。
3. 选择 **Advanced**（高级）> **Other Info**（其他信息）。
4. 展开 **Management Profile**（管理配置文件）列表，然后选择配置文件或 **New Management Profile**（新建管理配置文件）。
5. 输入配置文件的 **Name**（名称）。
6. 对于 **Permitted Services**（允许的服务），选择服务，例如 **Ping**，然后单击 **OK**（确定）。

STEP 11 | **Commit**（提交）更改。

STEP 12 | 连接接口。

使用直通线缆将已配置的接口连接到每个网段上的相应交换机或路由器。

STEP 13 | 验证接口是否处于活动状态。



© 2019 Palo Alto Networks, Inc.

从 Web 界面中，选择 **Network**（网络）> **Interfaces**（接口），然后验证“链接状态”列中的图标是否为绿色。还可以从 **Dashboard**（仪表盘）上的 **Interfaces**（接口）小部件监视链接状态。

STEP 14 | 配置静态路由和/或动态路由协议（RIP、OSPF 或 BGP），使虚拟路由器能够路由流量。

- 配置静态路由
- RIP
- OSPF
- BGP

STEP 15 | 配置默认路由。

配置静态路由并将其设置为默认。

## 使用 *NDP* 管理 *IPv6* 主机

本主题介绍如何使用 NDP 配置 IPv6 主机；因此，无需单独的 DHCPv6 服务器来执行这一操作。该主题还解释了如何使用 NDP 来监控 IPv6 地址，从而允许快速跟踪设备和违反安全规则的相关用户的 IPv6 地址和 MAC 地址。

- 用于 DNS 配置的 IPv6 路由器通告
- 配置用于 IPv6 路由器通告的 RDNS 服务器和 DNS 搜索列表
- NDP 监控
- 启用 NDP 监控

### 用于 **DNS** 配置的 **IPv6** 路由器通告

防火墙增强邻居发现 (ND) 的实施，以便您可以根据 RFC 6106，用于 DNS 配置的 IPv6 路由器通告为 IPv6 主机提供 DNS 递归服务器 (RDNSS) 选项和 DNS 搜索列表 (DNSSL) 选项。配置第 3 层接口时，您可以在防火墙上配置这些 DNS 选项，以便防火墙可以配置您的 IPv6 主机；因此，无需单独的 DHCPv6 服务器来配置主机。防火墙将包含这些选项的 IPv6 路由器通告 (RA) 发送到 IPv6 主机，作为其 DNS 配置的一部分，以便将其全面配置以访问 Internet 服务。因此，您的 IPv6 主机可配置：

- 可以解析 DNS 查询的 RDNS 服务器地址。
- 在将域名输入 DNS 查询之前，DNS 客户端（一次一个）将其添加到一个非限定域名的域名列表（后缀）。

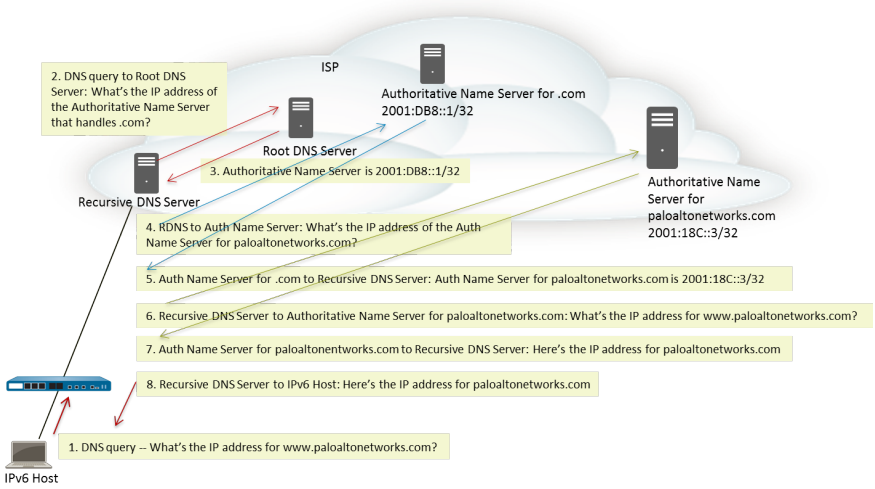
所有 PAN-OS 平台上的以太网接口、子接口、聚合以太网接口和第 3 层 VLAN 接口都支持用于 DNS 配置的 IPv6 路由器通告。



防火墙发送 *IPv6 RA* 用于 *DNS* 配置的功能允许防火墙执行类似于 *DHCP* 的角色，并与作为 *DNS* 代理、*DNS* 客户端或 *DNS* 服务器的防火墙无关。

使用 RDNS 服务器地址配置防火墙后，防火墙将使用这些地址配置 IPv6 主机（DNS 客户端）。IPv6 主机使用这些地址中的一个或多个来访问 RDNS 服务器。DNS 递归指的是 RDNS 服务器发起的一系列 DNS 请求，如下图中的三对查询和响应所示。例如，当用户尝试访问 www.paloaltonetworks.com 时，本地浏览器会发现不仅缓存中没有该域名的 IP 地址，客户端操作系统中也没有。客户端操作系统向属于本地 ISP 的 DNS 递归服务器启动 DNS 查询。


© 2019 Palo Alto Networks, Inc.




IPv6 路由器通告可以包含多个具有相同或不同生命周期的 DNS 递归服务器地址选项。只要地址具有相同的生命周期，单个 DNS 递归服务器地址选项可以包含多个 DNS 递归服务器地址。

DNS 搜索列表是防火墙通告 DNS 客户端的域名（后缀）列表。因此，防火墙配置 DNS 客户端在其非限定 DNS 查询中使用后缀。DNS 客户端在将名称输入 DNS 查询之前，将后缀（每次一个）附加到非限定域名，从而在 DNS 查询中使用完全限定域名 (FQDN)。例如，如果正被配置的 DNS 客户端的用户尝试为不带后缀的名称“quality”提交 DNS 查询，则路由器会将一段时间和 DNS 搜索列表中的第一个 DNS 后缀附加到名称中，并发送 DNS 查询。如果该列表中的第一个 DNS 后缀是“company.com”，则路由器生成的 DNS 查询为完全限定域名 (FQDN)“quality.company.com”。

如果 DNS 查询失败，客户端会将该列表中的第二个 DNS 后缀附加到非限定域名中，并发送新的 DNS 查询。客户端使用 DNS 后缀，直到 DNS 查找成功（忽略剩余后缀）或直到路由器已尝试列表中的所有后缀。

您可以使用 ND DNSSL 选项中要提供给 DNS 客户端路由器的后缀配置防火墙；接收 DNS 搜索列表选项的 DNS 客户端配置为在其非限定 DNS 查询中使用后缀。

要指定 RDNS 服务器和 DNS 搜索列表，配置用于 IPv6 路由器通告的 RDNS 服务器和 DNS 搜索列表。

配置用于 **IPv6** 路由器通告的 **RDNS** 服务器和 **DNS** 搜索列表

执行此任务以配置 IPv6 主机的用于 DNS 配置的 IPv6 路由器通告。

STEP 1 | 启用防火墙以从接口发送 IPv6 路由器通告。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择要配置的接口。
3. 在 **IPv6** 选项卡上，选择 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。
4. 在 **Router Advertisement**（路由器通告）选项卡上，选择 **Enable Router Advertisement**（启用路由器通告）。
5. 单击 **OK**（确定）。

STEP 2 | 指定防火墙将在该接口的 ND 路由器通告中通告的递归 DNS 服务器地址和 DNS 搜索列表。

RDNS 服务器和 DNS 搜索列表是 DNS 客户端的 DNS 配置的一部分，以便客户端可以解析 IPv6 DNS 请求。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择正在配置的接口。
3. 选择**IPv6** > **DNS Support**（**DNS** 支持）。
4. **Include DNS information in Router Advertisement**（在路由器通告中包含 **DNS** 信息）可以使防火墙发送 IPv6 DNS 信息。



© 2019 Palo Alto Networks, Inc.

5. 对于 DNS **Server**（服务器），**Add**（添加）递归 DNS 服务器的 IPv6 地址。**Add**（添加）最多八个递归 DNS 服务器。防火墙按照从上到下的顺序发送 ICMPv6 路由器通告中的服务器地址。
6. 以秒为单位指定 **Lifetime**（生存时间），这是客户端可以使用特定 RDNS 服务器解析域名的最长秒数。
   - **Lifetime**（生存时间）范围是等于或介于 **Max Interval**（最大间隔）（在 **Router Advertisement**（路由器通告）选项卡上配置）和 **Max Interval**（最大间隔）的两倍之间的任何值。例如，如果您的最大间隔为 600 秒，则生存时间范围为 600-1,200 秒。
   - 默认 **Lifetime**（生存时间）为 1,200 秒。
7. 对于 DNS 后缀，**Add**（添加）**DNS Suffix**（**DNS** 后缀）（域名最多为 255 个字节）。**Add**（添加）最多八个 DNS 后缀。防火墙按照从上到下的顺序在 ICMPv6 路由器通告中发送后缀。
8. 以秒为单位指定 **Lifetime**（生存时间），这是客户端可以使用后缀的最长秒数。生命周期具有与 **Server**（服务器）相同的范围和默认值。
9. 单击 **OK**（确定）。

STEP 3 | 提交更改。

单击 **Commit**（提交）。

**NDP 监控**

用于 IPv6 的邻居发现协议 (NDP) (RFC 4861) 执行的功能与 IPv4 的 ARP 功能相似。防火墙默认运行 NDP，其使用 ICMPv6 数据包来发现和跟踪连接链路上的链路层地址和邻居状态。

启用 NDP 监控因此您可以查看链路本地网络上设备的 IPv6 地址、其 MAC 地址、User-ID 的相关用户名（如果该设备用户使用目录服务登录）、地址的可访问性状态，以及 NDP 监控从该 IPv6 地址接收到路由器通告的日期和时间。用户名处于最佳情况；无用户名的网络上可以有许多 IPv6 设备，如打印机、传真机、服务器等。

如果要快速跟踪违反安全规则的设备和用户，非常有用的方法是将 IPv6 地址、MAC 地址和用户名显示在同一个位置。您需要对应于 IPv6 地址的 MAC 地址，以便跟踪 MAC 地址返回物理交换机或访问点。

*NDP* 监控不能保证发现所有设备，因为用于筛选 *NDP* 或重复地址检测 *(DAD)* 消息的防火墙和客户端之间可能会有其他网络设备。防火墙只能监控接口上发现的设备。

NDP 监控还监控来自客户端和邻居的重复地址检测 (DAD) 数据包。您还可以监控 IPv6 ND 日志，以便更容易排除故障。

所有 PAN-OS 型号上的以太网接口、子接口、聚合以太网接口和 VLAN 接口都支持用于 NDP 监控。

**启用 NDP 监控**

执行此任务为接口启用 NDP 监控。

STEP 1 | 启用 NDP 监控。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 选择正在配置的接口。
3. 选择 **IPv6**。
4. 选择 **Address Resolution**（地址解析）。
5. 选择 **Enable NDP Monitoring**（启用 **NDP** 监控）。

   启用或禁用 *NDP* 监控后，必须在 *NDP* 监控可以启动或停止之前 *Commit*（提交）。
6. 单击 **OK**（确定）。

STEP 2 | 提交更改。


© 2019 Palo Alto Networks, Inc.

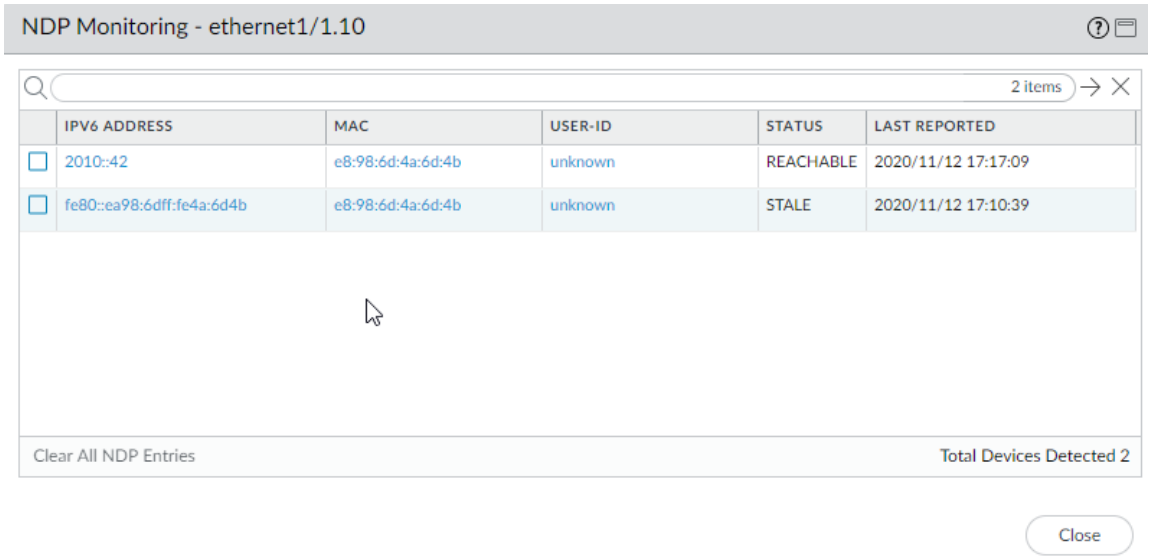
单击 **Commit**（提交）。

STEP 3 | 监控来自客户端和邻居的 NDP 和 DAD 数据包。

1. 选择 **Network**（网络）> **Interfaces**（接口）和 **Ethernet**（以太网）或 **VLAN**。
2. 对于启用了 NDP 监控的接口，在“功能”列中，将鼠标悬停在  NDP 监控图标上。

   如果启用 RA，接口的 NDP 监控摘要显示接口在路由通告 (RA) 中发送的 IPv6 **Prefixes**（前缀）列表（它们是接口本身的 IPv6 前缀）。

   摘要还指出是否启用 DAD、路由器通告和 DNS 支持；配置的任何 DNS 递归服务器的 IP 地址；以及 DNS 搜索列表中配置的任何 DNS 后缀。
3. 单击 NDP 监控图标以显示详细信息。




   接口的详细 NDP 监控表的每一行显示防火墙发现的邻居 IPv6 地址、相应的 MAC 地址、相应的用户 ID（最佳情况）、地址状态的可访问性、上次报告日期以及该 NDP 监控从 IP 地址接收 RA 的时间。打印机或其他非基于用户的主机不会显示用户 ID。如果 IP 地址状态为“失效”，根据 RFC 4861，无法知道可以访问邻居。

   右下角是链接本地网络上 **Total Devices Detected**（检测到的总设备）数量。

   - 在筛选器字段中输入 IPv6 地址，搜索要显示的地址。
   - 选中复选框以显示或不显示 IPv6 地址。
   - 单击数字、向右或向左箭头或垂直滚动条，可前进多个条目。
   - 单击 **Clear All NDP Entries**（清除所有 **NDP** 条目）以清除整个表。

STEP 4 | 监控 ND 日志以进行报告。

1. 选择 **Monitor**（监视器）> **Logs**（日志）> **System**（系统）。
2. 在“类型”列中，查看 **ipv6nd** 日志和相应的说明。

   例如，`inconsistent router advertisementreceived`（收到的不一致的路由器通告）表示防火墙接收到的 RA 不同于要发送的 RA。



© 2019 Palo Alto Networks, Inc.

# 配置聚合接口组

聚合接口组使用 IEEE 802.1AX 链路聚合将多个 Ethernet 接口组合到单个虚拟接口，该虚拟接口可将此防火墙连接到其他网络设备或防火墙。聚合接口组将通过平衡各组合接口中的负载流量来增加对等之间的带宽。同时，该接口也会提供冗余；当一个接口故障时，其他接口将继续支持通信。

在默认情况下，接口故障检测将仅在直接连接的对等之间的物理层上自动进行。然而，如果启用了链接聚合控制协议 (LACP)，则接口故障检测将在物理层和数据链路层自动进行，不论对等是否直接连接。LACP 还能在配置热后备的情况下，使故障自动转移到备用接口。除 VM 系列型号外的所有 Palo Alto Networks 防火墙均支持聚合组。 产品选型工具指示每个防火墙支持的聚合组数。每个聚合组最多可有 8 个接口。

*PAN-OS* 防火墙模式最多支持 *16,000* 个分配给物理或第 *3* 层虚拟接口的 *IP* 地址；此最大值包括 *IPv4* 和 *IPv6* 地址。

仅前 8 个聚合组支持 QoS。

配置聚合组之前，必须配置其接口。在分配给任何特定聚合组的接口中，硬件介质可以不同（例如，您可以混合光纤和铜线），但带宽和接口类型必须相同。带宽和接口类型选项如下：

- 带宽 — 1Gbps、10Gbps、40Gbps 或 100Gbps。
- 接口类型 — HA3、虚拟线路、第 2 层或第 3 层。

此流程仅为 *Palo Alto Networks* 防火墙的配置步骤。您还必须配置对等设备的聚合组。请参考该设备的文件了解其说明。

STEP 1 | 配置通用接口组参数。

1. 选择 **Network(网络)** > **Interfaces(接口)** > **Ethernet(以太网)** 并 **Add Aggregate**（添加聚合组）。
2. 在只读的 **Interface Name**（接口名称）的相邻字段中，输入一个数字 (1-8) 以标识该组。
3. 对于 **Interface Type**（接口类型），请选择 **HA**、**Virtual Wire**（虚拟线路）、**Layer2**（第 **2** 层）或 **Layer3**（第 **3** 层）。
4. 为您选择的 **Interface Type**（接口类型）配置剩下的参数。

STEP 2 | 配置 LACP 设置。

只有您想为聚合组启用 LACP 时才执行此步骤。

您不能为 *Virtual Wire* 接口启用 *LACP*。

1. 在 **LACP** 选项卡上，选择 **Enable LACP**（启用 **LACP**）。
2. 设置 LACP 状态查询 **Mode**（模式）设置为 **Passive**（被动）（防火墙回应 — 默认设置）或者 **Active**（主动）（防火墙查询对等设备）。

   最佳实践是：将一个 *LACP* 对等设备设置为主动模式，而另外一个设为被动模式。如果两个对端均为被动模式，则 *LACP* 无法正常运行。防火墙无法检测其对等设备的模式。
3. 为 LACP 查询和响应交换将 **Transmission Rate**（传输速率）设置为 **Slow**（缓慢）（每 30 秒 — 默认设置）或者 **Fast**（快速）（每秒）。根据用于处理网络的 LACP 的支持情况以及设备应有的接口故障检测和解决速度来设置传输速率。
4. 如果要在一秒钟之内启用故障转移至备用接口，请选择 **Fast Failover**（快速故障转移）。在默认情况下，禁用该选项，防火墙为故障转移处理使用 IEEE 802.1ax 标准，这将需要至少三秒。

   最佳实践是，在关键数据可能会在标准故障转移间隔期间丢失的部署中，使用 *Fast Failover*（快速故障转移）选项。


© 2019 Palo Alto Networks, Inc.

5. 输入在聚合组中活动 (1–8) 的 **Max Ports**（最大端口数）（接口数量）。如果分配给该组的接口数超过 **Max Ports**（最大端口数），其余接口将处于待机模式。防火墙会使用分配给（步骤 3）各个接口的 **LACP Port Priority**（**LACP** 端口优先级）来确定一开始就处于活动状态的接口，并确定待机接口在故障转移时变为活动状态的顺序。如果 LACP 对等有不匹配的端口优先级值，具有较低 **System Priority**（系统优先级）数（默认为 32,768；范围为 1–65,535）将覆盖其他对等。
6. （可选）仅对于主动/被动防火墙，如果要为被动防火墙启用 LACP 预先谈判，请选择 **Enable in HA Passive State**（启用 **HA** 被动状态）。LACP 预先协商可以更快地将故障转移到被动防火墙（有关详细信息，请参阅主动/被动 HA 的 LACP 及 LLDP 预先协商）。

   如果选择此选项，则不能选择 *Same System MAC Address for Active-Passive HA*（主动-被动 *HA* 的相同系统 *MAC* 地址）；预先谈判需要每个 *HA* 防火墙上都有独特的接口 *MAC* 地址。
7. （可选）仅对于主动/被动防火墙，选择 **Same System MAC Address for Active-Passive HA**（主动-被动 **HA** 的相同系统 **MAC** 地址）并且为两个 HA 防火墙指定一个单一的 **MAC Address**（**MAC** 地址）。如果虚拟化 LACP 对等（网络显示为单一设备），此选项可以尽可能减少故障转移延迟。默认情况下禁用此选项，HA 对中的两个防火墙各自拥有唯一的 MAC 地址。

   如果 *LACP* 对等未虚拟化，使用唯一的 *MAC* 地址可最大限度减少故障转移延迟。

STEP 3 | 为聚合组分配接口。

请针对聚合组中的各个接口 (1-8) 执行以下步骤。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后单击接口名称，以对其进行编辑。
2. 将 **Interface Type**（接口类型）设置为 **Aggregate Ethernet**（聚合 **Ethernet**）。
3. 选择刚才定义的 **Aggregate Group**（聚合组）。
4. 选择 **Link Speed**（链接速度）、**Link Duplex**（链接双工）和 **Link State**（链接状态）。

   最好为该组中的每个接口设置相同的链接速度和双工值。对于非匹配值，防火墙默认为更高的速度和全双工。
5. （可选）如果启用聚合组 LACP，输入一个 **LACP Port Priority**（**LACP** 端口优先级）（默认为 32,768；范围为 1–65,535）。如果您分配的接口数超过您为该组的 **Max Ports**（最大端口数）值，那么端口优先级将决定哪些接口处于活动状态，哪些接口处于待机状态。较低数（较高优先级）的接口将激活。
6. 单击 **OK**（确定）。

STEP 4 | 如果防火墙具有主动/主动配置，而且您在聚合 HA3 接口，请为聚合组启用数据包转发。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）并编辑“数据包转发”部分。
2. 选择为 **HA3 Interface**（**HA3** 接口）配置的聚合组，然后单击 **OK**（确定）。

STEP 5 | 提交更改并且确认聚合组状态。

1. 单击 **Commit**（提交）。
2. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。
3. 验证“链接状态”列是否有为聚合组显示绿色图标，该图标表示所有成员接口都已打开。如果图标呈黄色，就表示至少有一个（并非所有）成员处于关闭状态。如果图标呈红色，就表示所有成员都处于关闭状态。
4. 如果配置 LACP，验证 Features（功能）列是否有为聚合组显示 LACP 启用图标。



© 2019 Palo Alto Networks, Inc.

# 用于网络分段的 Bonjour Reflector

Apple Bonjour 也称为零配置网络，可自动发现本地网络上的设备和服务。例如，您可以通过 Bonjour，在未手动配置打印机 IP 地址的情况下，连接到打印机。Bonjour 使用多播 DNS (mDNS) 将名称转换为本地网络上的地址。Bonjour 针对其流量使用私有多播范围。该范围不允许进行流量路由，从而阻止在出于安全考虑或管理目的使用网络分段的环境中使用（例如，服务器和客户端位于不同的子网中）。

要在使用分段路由流量的网络环境中支持 Apple Bonjour，您可以在所指定的第 3 层 (L3) 以太网或聚合以太网 (AE) 接口或子接口之间转发 Bonjour IPv4 流量。通过 Bonjour Reflector，您可以将多播 Bonjour 广告和查询转发到 L3 以太网和 AE 接口或子接口，确保用户对服务的访问和设备可发现性，且不受在线时间 (TTL) 值或跃点限制的影响。

*PA-220*、*PA-800* 和 *PA-3200* 支持转发 *Bonjour* 流量。

启用此选项后，防火墙将 Bonjour 流量重定向到已启用此选项的 L3 和 AE 接口和子接口。必须启用想要管理 Bonjour 流量的所有支持接口上的此选项。例如，如果希望特定 L3 接口将 Bonjour 流量转发到 AE 接口，必须同时在这两个接口上启用此选项。您最多可在 16 个接口上启用此选项。

为防止形成循环，防火墙会将源 *MAC* 地址修改为防火墙传出接口 *MAC* 地址。为帮助阻止泛滥攻击，一旦防火墙每秒接收到的数据包数超过下表中所列的值，防火墙将丢弃数据包以保护防火墙和网络。

| 系列 | 速率限制（每秒） |
|---|---|
| *PA-220* | *100* |
| *PA-800* | *200* |
| *PA-3200* | *500* |

STEP 1 | 选择 **Network**（网络）> **Interfaces**（接口）。

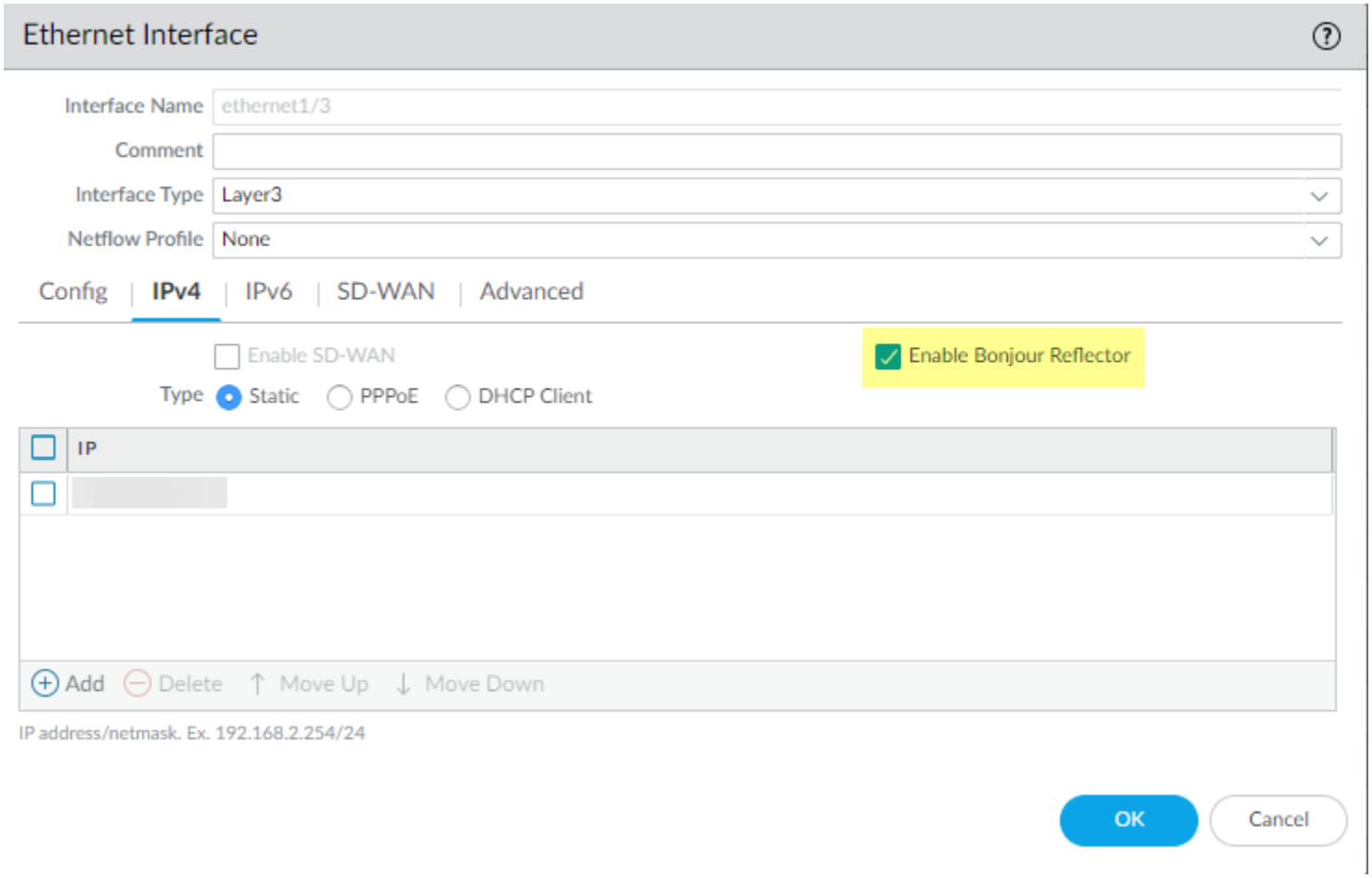
STEP 2 | 选择或 **Add**（添加）L3 以太网或子接口或 AE 接口。

如果添加子接口，必须使用 *0* 以外的 *Tag*（标记）。

STEP 3 | 选择 **IPv4**，然后选择 **Enable Bonjour Reflector**（启用 **Bonjour Reflector**）选项。



© 2019 Palo Alto Networks, Inc.




STEP 4 | 单击 **OK**（确定）。

STEP 5 | 针对想要转发 Bonjour 流量的所有 L3 或 AE 接口和子接口，重复步骤 1-4。

您最多可以在 *16* 个不同的接口或子接口上启用此选项。

STEP 6 | **Commit**（提交）更改。

STEP 7 | 确认启用 Bonjour Reflector 选项的一个或多个接口的 **Features**（功能）列均显示 **`Bonjour Reflector:yes`**（ ）。

STEP 8 | 使用 CLI 命令 **`show bonjour interface`**显示防火墙会转发 Bonjour 流量的所有接口以及计数器列表。**`rx`** 表示接口接收的 Bonjour 数据包总数。**`tx`** 表示接口传输的 Bonjour 数据包总数。**`drop`** 表示接口丢弃的数据包数。

```
admin> show bonjour interface

name                    rx          tx          drop
-------------------------------------------------------------
ethernet1/4             1           1           0
ethernet1/7             0           0           0
```



© 2019 Palo Alto Networks, Inc.

```
ethernet1/7.10          0           0           0
ethernet1/7.20          4           4           0
ae15                    0           0           0
ae16                    0           0           0
ae16.30                 0           2           0
ae16.40                 0           0           0
```

# 使用接口管理概要文件限制访问

接口管理配置文件可防止通过定义防火墙接口允许管理流量的协议、服务和 IP 地址，对防火墙进行未授权访问。例如，如果要防止用户通过 Ethernet1/1 接口访问防火墙 Web 界面，但是允许接口接受来自网络监控系统的 SNMP 查询。在这种情况下，则可以在一个接口管理配置文件中启用 SNMP 和禁用 HTTP/HTTPS，并且分配配置文件至 ethernet1/1。

您可将接口管理配置文件分配到第 3 层 Ethernet 接口（包括子接口），以及逻辑接口（聚合组、VLAN、回环和隧道接口）。如果没有分配一个接口管理配置文件至一个接口，它在默认情况下拒绝访问所有的 IP 地址、协议和服务。

管理 *(MGT)* 界面不会要求接口管理配置文件。对防火墙执行初始配置时，会限制 *MGT* 接口的协议、服务和 *IP* 地址。在 *MGT* 界面出现故障时，允许管理访问另外一个界面，从而可以继续管理防火墙。

使用接口管理配置文件启用对防火墙接口的访问时，请不要从 *Internet* 或企业安全边界内其他不信任区域启用管理访问（*HTTP*、*HTTPS*、*SSH* 或 *Telnet*），且永远不要启用 *HTTP* 或 *Telnet* 访问，因为这些协议会以明文形式传输。要确保正确保护防火墙管理访问的安全，请遵循确保管理员访问安全的最佳实践。

STEP 1 | 配置接口管理配置文件。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理），然后单击 **Add**（添加）。
2. 选择接口允许管理流量的协议：**Ping**、**Telnet**、**SSH**、**HTTP**、**HTTP OCSP**、**HTTPS** 或 **SNMP**。

   请勿启用 *HTTP*或 *Telnet*，因为这些协议会以明文形式传输，不安全。

3. 选择接口允许管理流量的服务：
   - **Response Pages**（响应页面）— 用于启用以下各项的响应页面：
     - **Authentication Portal**（身份验证门户）— 为提供身份验证门户响应页面，防火墙会将第 3 层接口上的端口保留为开放状态：6081 用于透明模式下的身份验证门户，6082 用于重定向模式下的身份验证门户。有关详细信息，请参阅配置身份验证门户。
     - **URL Admin Override**（URL 管理替代）— 有关详细信息，请参阅允许密码访问某些站点。
   - **User-ID**— 用于 重新分发数据和身份验证时间戳。
   - **User-ID Syslog Listener-SSL**（用户标识系统日志监听程序 **SSL**）或 **User-ID Syslog Listener-UDP**（用户标识系统日志监听程序 **UDP**）— 用于通过 SSL 或 UDP 配置 User-ID 以监控用户映射的 Syslog 发件人。
4. （可选）**Add**（添加）可以访问接口的允许 IP 地址。如果不将项目添加至清单，接口则没有 IP 地址限制。
5. 单击 **OK**（确定）。

STEP 2 | 为接口分配一个接口管理配置文件。

1. 选择 **Network**（网络）> **Interfaces**（接口），选择接口类型（**Ethernet**（以太网）、**VLAN**、**Loopback**（回环）或 **Tunnel**（隧道）），并选择接口。


© 2019 Palo Alto Networks, Inc.

2. 选择 **Advanced**（高级）> **Other info**（其他信息），然后选择添加的接口 **Management Profile**（管理配置文件）。
3. 单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 虚拟路由器

虚拟路由器是防火墙参与第三层路由的一种功能。防火墙使用虚拟路由器通过手动定义静态路由或参与一个或多个第 3 层路由协议（动态路由）来获取其他子网的路由。防火墙通过这些方法获取的路由填充防火墙的 IP 路由信息库 (RIB)。当数据包的目标子网不同于其所到达的子网时，虚拟路由器从 RIB 中获取最佳路由，将其放在转发信息库 (FIB) 中，并将数据包转发到 FIB 定义的下一个跃点路由器。防火墙使用 Ethernet 交换来连接同一 IP 子网上的其他设备。（如果正在使用 ECMP，一个例外是其中一个最佳路由进入 FIB，在这种情况下，所有等成本路由都将进入 FIB。）

在防火墙上定义的以太网、VLAN 和隧道接口可接收和转发第 3 层数据包。防火墙根据转发条件从传出接口中派生出目标区域，并参考策略规则来确定应用于每个数据包的安全策略。除路由到其他网络设备以外，如果指定下一个跃点指向其他虚拟路由器，则虚拟路由器可路由到同一防火墙内的其他虚拟路由器中。

您可以在虚拟路由器上配置第 3 层接口来参与动态路由协议（BGP、OSPF、OSPFv3 或 RIP），也可以添加静态路由。您还可以创建多个虚拟路由器，每个都用于维护不在虚拟路由器之间共享的一组单独路由，从而可以为不同的接口配置不同的路由行为。

在防火墙上定义的每个第 3 层以太网、回环、VLAN 和隧道接口都必须与虚拟路由器关联。虽然每个接口仅可属于一个虚拟路由器，但是可以为虚拟路由器配置多个路由协议和静态路由。无论是否为虚拟路由器配置静态路由和动态路由协议，都需要对其进行常规配置。

STEP 1 | 从网络管理员处收集必要的信息。

- 要执行路由的防火墙上的接口。
- 静态路由、OSPF 内部路由、OSPF 外部路由、IBGP、EBGP 和 RIP 路由的管理距离。

STEP 2 | 创建虚拟路由器并将接口应用到该路由器。

防火墙带有一个名为 **default**（默认）的虚拟路由器。您可以编辑 **default**（默认）虚拟路由器或添加一个新的虚拟路由器。

1. 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。
2. 选择一个虚拟路由器（名为 **default**（默认）的虚拟路由器或不同的虚拟路由器）或 **Add**（添加）新虚拟路由器的 **Name**（名称）。
3. 选择 **Router Settings**（路由器设置）> **General**（常规）。
4. 在 **Interfaces**（接口）框中单击 **Add**（添加），然后选择已定义接口。

   如果您想要将所有接口添加到此虚拟服务器，请重复此步骤。
5. 单击 **OK**（确定）。

STEP 3 | 设置静态和动态路由的管理距离。

根据您的网络需要设置各种类型的路由的管理距离。当虚拟路由器有两个或两个以上前往同一目标的路由时，可使用管理距离从不同的路由协议和静态路由中选择最佳路径，优先选择较短的距离。

- **Static**（静态）— 范围为 10-240，默认为 10。
- **OSPF Internal**（**OSPF** 内部）— 范围为 10-240，默认为 30。
- **OSPF External**（**OSPF** 外部）— 范围为 10-240，默认为 110。
- **IBGP** — 范围为 10-240，默认为 200。
- **EBGP** — 范围为 10-240，默认为 20。
- **RIP**— 范围为 10-240，默认为 120。



如果您想利用多个等成本路径进行转发，请参阅 ECMP。

STEP 4 | 提交虚拟路由器常规设置。



© 2019 Palo Alto Networks, Inc.

单击 **OK**（确定）和 **Commit**（提交）。

STEP 5 | 根据需要配置以太网、VLAN、回环和隧道接口。

配置第 3 层接口。



© 2019 Palo Alto Networks, Inc.

# 服务路由

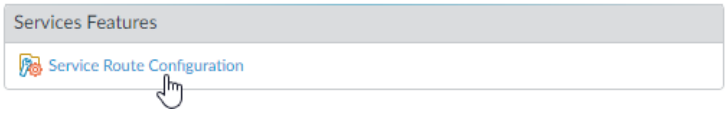
默认情况下，防火墙使用管理 (MGT) 接口来访问外部服务（如 DNS 服务器和外部身份验证服务器）和 Palo Alto Networks 服务（如软件、URL 更新、许可证和 AutoFocus）。使用 MGT 接口的备用方法是配置数据端口（常规接口）以访问这些服务。在服务器上，从该接口到服务的路径称为服务路由。服务数据包在分配给外部服务的端口上退出防火墙，服务器将其响应发送到配置的源端口和源 IP 地址。

您可以在为多个虚拟系统启用的防火墙上全局配置服务路由（如以下任务所示）或自定义虚拟系统的服务路由，以灵活地使用与虚拟系统相关联的接口。任何没有对特定服务配置服务路由的虚拟系统都会继承为该服务设置的接口和 IP 地址。

以下过程使您可以更改防火墙用于将请求发送到外部服务的接口。

STEP 1 | 自定义服务路由。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Global**（全局）（在没有多个虚拟系统的防火墙上省略全局功能），然后在服务功能部分中单击 **Service Route Configuration**（服务路由配置）。




2. 选择 **Customize**（自定义），然后执行以下操作之一创建服务路由：
   - 对于预定义服务：
     - 选择 **IPv4** 或 **IPv6**，然后单击要自定义服务路由的服务链接。

       要轻松使用多个服务的相同源地址，请选中服务的复选框，单击 *Set Selected Routes*（设置所选路由），然后继续执行下一步。
     - 要限制源地址的列表，请选择 **Source Interface**（源接口），然后选择 **Source Address**（源地址）（来自该接口）作为服务路由。选择 **Any**（任何）源接口，以确保您从中选择地址的源地址列表中的所有接口上的所有 IP 地址可用。选择 **Use default**（使用默认）使防火墙使用服务路由的管理接口，除非数据包目标 IP 地址与配置的目标 IP 地址匹配，在这种情况下，源 IP 地址设置为配置用于 **Destination**（目标）的 **Source Address**（源地址）。就任何目标服务路由而言，选择 **MGT** 均可使防火墙使用 MGT 接口作为服务路由。
     - 单击 **OK**（确定）以保存设置。
     - 如果要同时指定服务的 IPv4 和 IPv6 地址，请重复此步骤。
   - 对于目标服务路由：
     - 选择 **Destination**（目标）并 **Add**（添加）**Destination**（目标）IP 地址。在这种情况下，如果数据包到达与已配置的 **Destination**（目标）地址匹配的目标 IP 地址，则数据包的源 IP 地址将被设置为在下一步中配置的 **Source Address**（源地址）。
     - 要限制源地址的列表，请选择 **Source Interface**（源接口），然后选择 **Source Address**（源地址）（来自该接口）作为服务路由。选择 **Any**（任何）源接口，以确保您从中选择地址的源地址列表中的所有接口上的所有 IP 地址可用。选择 **MGT**可使防火墙使用 MGT 接口作为服务路由。
     - 单击 **OK**（确定）以保存设置。
3. 为要自定义的每个服务路由重复上述步骤。
4. 单击 **OK**（确定）以保存服务路由配置。

STEP 2 | 提交。

单击 **Commit**（提交）。


© 2019 Palo Alto Networks, Inc.

# 静态路由

静态路由通常与动态路由协议一起使用。您可以为动态路由协议无法到达的位置配置静态路由。静态路由需要在网络中的每个路由器上手动配置，而非防火墙在其路由表中输入动态路由；即使静态路由需要在所有路由器上进行配置，但可能更适用于小型网络而非配置路由协议。


- 静态路由概述
- 基于路径监控删除静态路由
- 配置静态路由
- 为静态路由配置路径监控


## 静态路由概述

如果确定要特定的第 3 层流量采取某种不参与 IP 路由协议的路由，则可以使用 IPv4 和 IPv6 路由配置静态路由。

默认路由是一个特定的静态路由。如果不使用动态路由获取虚拟路由器的默认路由，则必须配置静态默认路由。当虚拟路由器具有传入数据包，并且在其路由表中找不到数据包目标的匹配项时，虚拟路由器将数据包发送到默认路由。默认 IPv4 路由为 0.0.0.0/0；默认 IPv6 路由为 ::/0。您可以配置 IPv4 和 IPv6 默认路由。

静态路由本身不会发生改变或适应网络环境中的变化，因此如果沿着路由与定义端点静态发生故障，通常不会重新路由流量。但是，如果出现问题，您可以选择备份静态路由：

- 您可以使用双向转发检测 (BFD) 配置文件配置静态路由，且防火墙和 BFD 对等设备之间的 BFD 会话失败时，防火墙从 RIB 和 FIB 表删除失败的静态路由，并且允许较低优先级的替代路由接管。
- 您可以为静态路由配置路径监控以使防火墙使用替代路由。

默认情况下，静态路由的管理距离为 10。当防火墙有两个或多个通往同一目标的路由时，将使用管理距离最短的路由。将静态路由的管理距离增加至高于动态路由的值后，如果动态路由不可用，则可以使用静态路由作为备份路由。

配置静态路由时，可以指定防火墙是否在单播或多播路由表 (RIB) 或单播和多播路由表中安装 IPv4 静态路由，也可以根本不安装该路由。例如，您只能在多播路由表中安装 IPv4 静态路由，因为您只想多播流量使用该路由。此选项可让您更好地控制流量所需的路由。您可以指定防火墙是否在单播路由表中安装 IPv6 静态路由。

## 基于路径监控删除静态路由

当您为静态路由配置路径监控时，防火墙使用路径监控来检测一个或多个被监控目标的路径关闭的时间。然后，防火墙可以使用替代路由重新路由流量。防火墙对静态路由进行路径监控，就像 HA 的路径监控或基于策略的转发 (PBF) 一样，如下所示：

- 防火墙将 ICMP ping 消息（检测信号消息）发送到一个或多个已确定具有稳健性并能反映静态路由可用性的受监控目标。
- 如果对任何或所有受监控的 ping 失败，则防火墙也会考虑关闭静态路由，并将其从路由信息库 (RIB) 和转发信息库 (FIB) 中删除。RIB 是防火墙配置的静态路由表以及从路由协议获取的动态路由表。FIB 是防火墙用于转发数据包的路由转发表。防火墙从 RIB 中选择前往同一目标（基于具有最低跃点数的路由）的替代静态路由，并将其放置在 FIB 中。
- 防火墙继续监控故障路由。当路由恢复时，（根据 **Any**（任何）或 **All**（所有）故障条件），路径监控返回激活状态，抢占保持计时器开始计时。在保持计时器的持续时间内，路径监控必须保持激活状态；然后防火墙会认为静态路由是稳定的，并将其恢复到 RIB 中。然后，防火墙将路由的跃点数与同一目标的进行比较，以确定哪条路由前往 FIB。

路径监视是避免以下路由发生静默丢弃的理想机制：

- 静态或默认路由。



© 2019 Palo Alto Networks, Inc.

- 已重新分发到路由协议的静态或默认路由。
- 其中一个对端不支持 BFD 时的静态或默认路由。（最佳实践是请勿在单个接口上同时启用 BFD 和路径监控。）
- 不使用 PBF 路径监控的静态或默认路由，不会从 RIB、FIB 或重新分发策略中删除发生故障的静态路由。



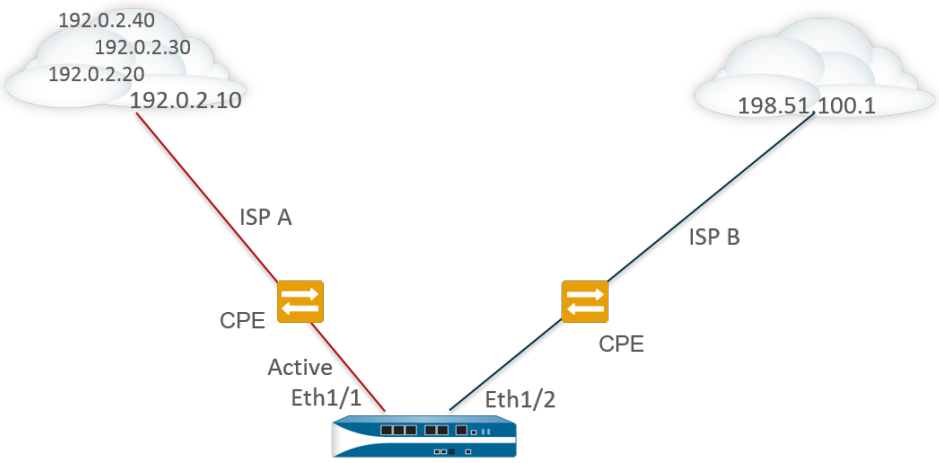
路径监控不适用于虚拟路由器之间配置的静态路由。

下图中，防火墙连接到两个 ISP，用于将冗余路由到互联网。主要默认路由 0.0.0.0（跃点数 10）使用下一个跃点 192.0.2.10；辅助默认路由 0.0.0.0（跃点数 50）使用下一个跃点 198.51.100.1。ISP A 的客户场所设备 (CPE) 保持激活主要物理链路，即使互联网连接已断开。在人为激活链路时，防火墙无法检测到链路是否已关闭，并且是否应在其 RIB 中将故障路由替换为辅助路由。

为了避免静默丢弃流量流向故障链路，请配置 192.0.2.20、192.0.2.30 和 192.0.2.40 的路径监视。如果这些目标的所有（或任何）路径出现故障，则防火墙假定下一个跃点 192.0.2.10 的路径也已关闭，应从其 RIB 中移除（使用下一个跃点 192.0.2.10 的）静态路由 0.0.0.0，并将静态路由替换为辅助路由前往（使用下一个跃点 198.51.100.1 的）同一目标 0.0.0.0，同时也访问互联网。



© 2019 Palo Alto Networks, Inc.




Route Table

| Destination | Next Hop | Metric | Interface | |
|---|---|---|---|---|
| 0.0.0.0/0 | 192.0.2.10 | 10 | ethernet1/1 | X Pings to 192.0.2.20, 192.0.2.30, and 192.0.2.40 fail, so static route removed |
| 0.0.0.0/0 | 198.51.100.1 | 50 | ethernet1/2 | |

当您配置静态路由时，其中一个必填字段是该目标的下一个跃点。您配置的下一个跃点类型决定防火墙在路径监控期间采取的操作，如下所示：

| 如果静态路由中的下一个跃点类型为： | ICMP Ping 的防火墙操作 |
|---|---|
| **IP** 地址 | 防火墙使用静态路由的源 IP 地址和出口接口作为 ICMP ping 的源地址和出口接口。它使用受监控目标已配置的目标 IP 地址作为 ping 的目标地址。它使用静态路由的下一个跃点地址作为 ping 的下一个跃点地址。 |



© 2019 Palo Alto Networks, Inc.

| 如果静态路由中的下一个跃点类型为： | ICMP Ping 的防火墙操作 |
|---|---|
| 下一个 **VR** | 防火墙使用静态路由的源 IP 地址作为 ICMP ping 的源地址。出口接口基于下一个跃点的虚拟路由器的查找结果。受监控目标已配置的目标 IP 地址是 ping 的目标地址。 |
| **None** | 防火墙使用路径监控的目标 IP 地址作为下一个跃点，并将 ICMP ping 发送到静态路由中的指定接口。 |

当静态或默认路由的路径监控发生故障时，防火墙会记录一个关键事件（路径监控故障）。当静态或默认路由恢复时，防火墙记录另一个关键事件（路径监控恢复）。

防火墙与主动/被动 HA 部署的路径监控配置进行同步，但防火墙阻止被动 HA 对端设备上的出口 ICMP ping 数据包，因为它不是主动处理流量。防火墙不会同步主动/主动 HA 部署的路径监控配置。

# 配置静态路由

执行以下任务，为防火墙上的虚拟路由器配置静态路由或默认路由。

STEP 1 | 配置静态路由。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择正在配置的虚拟路由器，例如 **default**（默认）。
2. 选择 **Static Routes**（静态路由器）选项卡。
3. 根据您要配置的静态路由类型，选择 **IPv4** 或 **IPv6**。
4. **Add**（添加）路由的 **Name**（名称）。
5. 对于 **Destination**（目标），输入路由和子网掩码（例如，192.168.2.2/24 用于 IPv4 地址或 2001:db8:123:1::1/64 用于 IPv6 地址）。如果要创建默认路由，请输入默认路由（0.0.0.0/0 用于 IPv4 地址或 ::/0 用于 IPv6 地址）。或者，可创建 IP 网络掩码类型的地址对象。
6. （可选）对于 **Interface**（接口），请指定要用于下一个跃点的数据包的出站接口。使用此接口来严格控制防火墙使用的接口，而不是路由表中用于此路由下一个跃点的接口。
7. 对于 **Next Hop**（下一个跃点），请选择以下选项之一：
   - **IP Address**（**IP** 地址）— 当您要路由到特定的下一个跃点时，输入 IP 地址（例如，192.168.56.1 或 2001:db8:49e:1::1）。您必须 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）（配置第 3 层接口时）才能使用 IPv6 下一个跃点地址。如果要创建默认路由，对于 **Next Hop**（下一个跃点），必须选择 **IP Address**（**IP** 地址）并输入 Internet 网关的 IP 地址（例如，192.168.56.1 或 2001:db8:49e:1::1）。或者，可创建 IP 网络掩码类型的地址对象。该地址对象必须具有 /32 (IPv4) 或 /128 (IPv6) 的网络掩码。
   - **Next VR**（下一个 **VR**）— 如需要内部路由到防火墙上的其他虚拟路由器，选择此选项，然后选择一个虚拟路由器。
   - **FQDN** — 输入 FQDN，或选择使用 FQDN 的地址对象，或是创建使用类型 FQDN 的新地址对象。

     如果使用 *FQDN* 充当静态路由下一个跃点，此 *FQDN* 必须解析出一个属于与您为静态路由配置的接口相同子网的 *IP* 地址，否则，防火墙拒绝解析，*FQDN* 仍保持为未解析。

     防火墙仅使用从 *FQDN* 的 *DNS* 解析出的一个 *IP* 地址（来自每个 *IPv4* 或 *IPv6* 系列类型）。如果 *DNS* 解析出多个地址，则防火墙会使用与配置用于下一个跃点的 *IP* 系列类型（*IPv4* 或 *IPv6*）匹配的首选 *IP* 地址。此首选 *IP* 地址是 *DNS* 服务器在其初始响应中返回的第一个地址。只要地址在后续响应中出现，无论其顺序如何，防火墙都会将该地址视为首选地址。
   - **Discard**（丢弃）— 选择是否要丢弃发往此目标的数据包。


© 2019 Palo Alto Networks, Inc.

- 无- 如果路由没有下一个跃点，请选择此项。例如，因为数据包仅有一种前往的方式，因此点对点连接不需要下一个跃点。

8. 为路由输入 **Admin Distance**（管理距离），以覆盖此虚拟路由器为静态路由设置的默认管理距离（范围为 10-240；默认值为 10）。
9. 输入路由 **Metric**（跃点数）（范围为 1-65,535）。

STEP 2 | 选择安装路由的位置。

选择您希望防火墙在其中安装静态路由的 **Route Table**（路由表）(RIB)：

- **Unicast**（单播）— 将路由安装到单播路由表。如果您希望路由仅用于单播通信，请选择此选项。
- **Multicast**（多播）— 将路由安装到多播路由表（仅适用于 IPv4 路由）。如果您希望路由仅用于多播通信，请选择此选项。
- **Both**（单播和多播）— 将路由安装到单播和多播路由表（仅适用于 IPv4 路由）。如果您希望单播或多播通信使用路由，请选择此选项。
- **No Install**（无安装）— 不在任一路由表中安装该路由。

STEP 3 | （可选）如果您的防火墙型号支持 BFD，则可以将 **BFD Profile**（**BFD** 配置文件）应用于静态路由，以便在静态路由失败时，防火墙可从 RIB 和 FIB 中删除路由，并使用替代路由。默认为 **None**（无）。

STEP 4 | 双击 **OK**（确定）。

STEP 5 | **Commit**（提交）配置。

## 为静态路由配置路径监控

使用以下步骤配置基于路径监控删除静态路由。

STEP 1 | 启用静态路由的路径监控。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **Static Routes**（静态路由），选择 **IPv4** 或 **IPv6**，然后选择要监控的静态路由。最多可监控 128 个静态路由。
3. 选择 **Path Monitoring**（路径监控）以启用路由的路径监控。

STEP 2 | 配置静态路由的受监控目标。

1. 按 **Name**（名称）**Add**（添加）受监控目标。每个静态路由最多可添加 8 个受监控目标。
2. 选择 **Enable**（启用）以监控目标。
3. 对于 **Source IP**（源 **IP**），选择防火墙在 ICMP ping 中用于受监控目标的 IP 地址：
   - 如果接口有多个 IP 地址，请选择一个。
   - 如果选择接口，防火墙默认使用分配给接口的第一个 IP 地址。
   - 如果选择 **DHCP (Use DHCP Client address)**（**DHCP**（使用 **DHCP** 客户端地址）），则防火墙会使用 DHCP 分配给接口的地址。要查看 DHCP 地址，请选择**Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），并在以太网接口行中单击 **Dynamic DHCP Client**（动态 **DHCP** 客户端）。IP 地址将显示在 Dynamic IP Interface Status（动态 IP 接口状态）窗口中。
4. 对于 **Destination Ip**（目标 **IP**），输入防火墙用于监控路径的 IP 地址或地址对象。受监控目标和静态路由目标使用的地址系列必须相同（IPv4 或 IPv6）。

   目标 *IP* 地址应属于可靠的端点；您不希望对本身不稳定或不可靠的设备进行路径监控。
5. （可选）指定 ICMP **Ping Interval (sec)**（**Ping** 间隔（秒））（以秒为单位），以确定防火墙监控路径的频率（范围为 1-60；默认为 3）。



© 2019 Palo Alto Networks, Inc.

6. （可选）在防火墙认为静态路由出现故障并将其从 RIB 和 FIB 中删除之前，指定不从目标返回的数据包的 ICMP **Ping Interval (sec)**（**Ping** 间隔（秒））（范围为 3-10；默认为 5）。
7. 单击 **OK**（确定）。

STEP 3 | 确定静态路由的路径监控是否基于一个或所有被监控目标，并设置抢占保持时间。

1. 选择 **Failure Condition**（故障条件），如果 ICMP 不能访问静态路由的 **Any**（任何）或 **All**（所有）受监控目标，则防火墙会从 RIB 和 FIB 删除此静态路由，并向 FIB 添加具有下一个最低跃点数且路由至同一目标的静态路由。

   选择 *All*（所有）可避免任何单个受监控目标在离线维护时发送路由失败的信号。

2. （可选）指定 **Preemptive Hold Time (min)**（抢占保持时间（分钟）），这是在防火墙将静态路由重新安装到 RIB 之前，停用的路径监控必须保持在激活状态的分钟数。路径监控评估静态路由的所有监控目标，并根据 **Any**（任何）或 **All**（所有）故障条件显示。如果链接在保持时间内断开或翻动，当链路恢复时，路径监控便可恢复；并且计时器会在路径监控返回激活状态时重启。

   如果 **Preemptive Hold Time**（抢占保持时间）为零，则防火墙会在路径监控激活时将路由立即重新安装到 RIB 中。范围为 0-1,440；默认为 2。
3. 单击 **OK**（确定）。

STEP 4 | 提交。

单击 **Commit**（提交）。

STEP 5 | 验证静态路由上的路径监控。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），再在所需虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
2. 从 **Routing**（路由）选项卡，选择 **Static Route Monitoring**（静态路由监控）。
3. 对于静态路由（目标），查看路径监控是启用还是禁用。状态列将显示路由是打开、关闭还是禁用。静态路由的标志为：A—激活，S—静态，E—ECMP。
4. 定期选择 **Refresh**（刷新），以查看路径监控的最新状态（健康检查）。
5. 将鼠标悬停在路由状态上，查看发送到该路由受监控目标的 ping 的受监控 IP 地址和结果。例如，3/5 表示 ping 间隔为 3 秒，ping 计数为 5 次连续缺失 ping（防火墙在过去 15 秒没有收到 ping），则表示路径监控检测到链路故障。根据 **Any**（任何）或 **All**（所有）故障条件，如果路径监控处于故障状态，并且防火墙在 15 秒后接收到 ping，则该路径被认为已激活，可启动 **Preemptive Hold Time**（抢占保持时间）。

   状态指示最近监控的 ping 结果：成功或失败。失败表示 ping 数据包系列（ping 间隔乘以 ping 计数）不成功。单个 ping 数据包故障不能反映出失败的 ping 状态。

STEP 6 | 查看 RIB 和 FIB 以验证静态路由是否被删除。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），再在所需虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
2. 从 **Routing**（路由）选项卡中，选择 **Route Table**（路由表）(RIB)，然后选择 **Forwarding Table**（转发表）(FIB) 以依次查看。
3. 选择 **Unicast**（单播）或 **Multicast**（多播）可查看相应的路由表。
4. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）、**IPv4 Only**（仅 **IPv4**）或 **IPv6 Only**（仅 **IPv6**）。
5. （可选）在筛选器字段中，输入正在搜索的路由，然后选择箭头，或使用滚动条在路由页面之间来回查看。
6. 看看路由是否被移除或是否存在。
7. 定期选择 **Refresh**（刷新），以查看路径监控的最新状态（健康检查）。


© 2019 Palo Alto Networks, Inc.



要查看为路径监控记录的事件，请选择 *Monitor*（监控）> *Logs*（日志）> *System*（系统）。查看 *path-monitor-failure* 的条目，表示静态路由目标的路径监控失败，因此路由已删除。查看 *path-monitor-recovery* 的条目，表示静态路由目标的路径监控已恢复，因此路由已恢复。



© 2019 Palo Alto Networks, Inc.

# RIP

路由信息协议 (RIP) 是为小型 IP 网络设计的内部网关协议 (IGP)。RIP 依赖跃点计数来确定路由；最佳路由具有最少的跃点数。RIP 基于 UDP 并使用端口 520 来进行路由更新。通过将路由限制为最多有 15 个跃点，该协议有助于防止形成路由回环，但同时也限制了支持的网络大小。如果需要 15 个以上的跃点，则无法路由通信。RIP 用于会聚的时间也会比 OSPF 和其他路由协议更长。防火墙支持 RIP v2。

请执行以下步骤以配置 RIP。

STEP 1 | 配置虚拟路由的常规配置设置。

有关详细信息，请参阅虚拟路由器。

STEP 2 | 配置 RIP 的常规配置设置。

1. 选择 **RIP** 选项卡。
2. 选中 **Enable**（启用）可启用 RIP 协议。
3. 如果您不想通过 RIP 获得任何默认路由，请选中 **Reject Default Route**（拒绝默认路由）。这是建议采用的默认设置。

   如果要允许通过 RIP 重新分发默认路由，请取消选中 **Reject Default Route**（拒绝默认路由）。

STEP 3 | 配置 RIP 接口。

1. 在 **Interfaces**（接口）选项卡中，从接口配置部分中选择一个接口。
2. 选择已定义接口。
3. 选择 **Enable**（启用）。
4. 选择 **Advertise**（通告）可将默认路由通告到具有指定跃点数值的 RIP 对等。
5. （可选）您也可以从 **Auth Profile**（身份验证配置文件）列表中选择一个配置文件。
6. 从 **Mode**（模式）列表中选择正常、被动或仅发送模式。
7. 单击 **OK**（确定）。

STEP 4 | 配置 RIP 计时器。

1. 在 **Timers**（计时器）选项卡上的 **Interval Seconds (sec)**（间隔秒数（秒））中输入一个值。此设置定义了以下 RIP 计时器的间隔（范围为 1-60；默认为 1）。
2. 指定 **Update Intervals**（更新间隔），以定义发布路由更新通知之间的间隔时长（范围为 1-3,600；默认为 30）。
3. 指定 **Delete Intervals**（删除间隔），以定义路由到期到删除路由之间的间隔时长（范围为 1-3,600，默认为 180）。
4. 指定 **Expire Intervals**（过期间隔），以定义最后一次更新路由到路由到期之间的间隔时长（范围为 1-3600，默认为 120）。

STEP 5 | （可选）配置身份验证配置文件。

默认情况下，防火墙无法使用 RIP 身份验证在 RIP 邻居之间进行交换。您也可以通过简单密码或使用 MD5 身份验证来配置 RIP 邻居之间 RIP 身份验证。推荐使用 MD5 身份验证，该身份验证比简单密码更加安全。

**RIP 简单密码身份验证**

1. 选择 **Auth Profiles**（身份验证配置文件），并 **Add**（添加）身份验证配置文件的名称以对 RIP 消息进行身份验证。
2. 选择 **Simple Password**（简单密码）作为 **Password Type**（密码类型）。
3. 输入一个简单密码并确定。

**MD5 RIP 身份验证**



© 2019 Palo Alto Networks, Inc.

1. 选择 **Auth Profiles**（身份验证配置文件），并 **Add**（添加）身份验证配置文件的名称以对 RIP 消息进行身份验证。
2. 选择 **MD5** 作为 **Password Type**（密码类型）。
3. **Add**（添加）一个或多个密码条目，包括：
   - 密匙 ID（范围 0-255）
   - 密钥
4. （可选）选择 **Preferred**（首选）状态。
5. 单击 **OK**（确定）以指定用来对传出消息进行身份验证的密匙。
6. 再次单击 Virtual Router - RIP Auth Profile（虚拟路由器 - RIP 身份验证配置文件）对话框中的 **OK**（确定）。

STEP 6 | **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# OSPF

开放式最短路径优先 (OSPF) 是一种内部网关协议 (IGP)，最常用来动态管理大型企业网络中的网络路由。OSPF 通过从其他路由器获取信息并以链接状态通告 (LSA) 的方式将路由通告到其他路由器，从而动态地确定路由。从 LSA 收集到的信息用于构建网络的拓扑图。此拓扑地图在网络中的路由器之间共享，并用来填充含可用路由的 IP 路由表。

动态检测网络拓扑中发生的变化，并使用这些变化瞬间生成新的拓扑图。单独计算每个路由的最短路径树。每个路由接口关联的指标用于估算最佳路由。这些可能包括距离、网络吞吐量、链路可用性等。此外，可以静态配置这些指标以直接获取 OSPF 拓扑图的结果。

实现 OSPF 的 Palo Alto Networks 可全面支持以下 RFC：

- RFC 2328（对于 IPv4）
- RFC 5340（对于 IPv6）

下列主题介绍 OSPF 以及在防火墙上配置 OSPF 所需步骤的详细信息：

- OSPF 概念
- 配置 OSPF
- 配置 OSPFv3
- 配置 OSPF 平稳重启
- 确认 OSPF 运行

## OSPF 概念

下列主题介绍您需要了解的 OSPF 概念，以便配置防火墙参与 OSPF 网络：

- OSPFv3
- OSPF 邻居
- OSPF 区域
- OSPF 路由器类型

### *OSPFv3*

OSPFv3 支持 IPv6 网络中的 OSPF 路由协议。例如，支持 IPv6 地址和前缀。保留执行了次要更改的 OSPFv2（对于 IPv4）中的大多数结构和功能。下面介绍 OSPFv3 的一些新增功能和更改：

- 支持每个链接上多个实例 — 使用 OSPFv3，您可以在单个链接上运行 OSPF 协议的多个实例。这通过分配一个 OSPFv3 实例 ID 号即可实现。分配给实例 ID 的接口会丢弃含不同 ID 的数据包。
- 协议处理每个链接 — OSPFv3 对每个链接进行操作，而不是像在 OSPFv2 上一样对每个 IP 子网进行操作。
- 寻址更改 — 除链接状态更新数据包中的 LSA 有效负载外，IPv6 地址并不在 OSPFv3 数据包中。通过路由器 ID 确定相邻路由器。
- 身份验证更改 — OSPFv3 未包含任何身份验证功能。在防火墙上配置 OSPFv3 需要指定封装式安全措施负载 (ESP) 或 IPv6 身份验证标头 (AH) 的身份验证配置文件。RFC 4552 中指定的密匙更换程序在本版本中不受支持。
- 支持每个链接上的多个实例 — 每个实例与 OSPFv3 数据包头中所含的实例 ID 相对应。
- **LSA** 新类型 — OSPFv3 支持两种 LSA 新类型：链接 LSA 和区域内前缀 LSA。

所有其他更改在 RFC 5340 中进行详细介绍。


© 2019 Palo Alto Networks, Inc.

## OSPF 邻居

通过公用网络连接在一起的两个启用了 OSPF 的路由器在同一 OSPF 区域形成的关系即称为 OSPF 邻居。可以通过一个公用广播域或点对点连接来连接相邻路由器。通过交换 OSPF 呼叫协议数据包可建立此连接。这些相邻关系用来在路由器之间交换路由更新。

## OSPF 区域

OSPF 在单个自治系统 (AS) 中工作。但是，此单个 AS 中的网络可划分为多个区域。默认情况下，将创建区域 0。区域 0 可以单独发挥功能，也可以充当大量区域的 OSPF 骨干区域。每个 OSPF 区域均采用 32 位标识符进行命名，大多数情况下以同一用点分隔的十进制地址作为 IP4 地址。例如，区域 0 通常记为 0.0.0.0。

区域的拓扑在其链接状态数据库中进行维护，而在其他区域中会隐藏，这样就减少了 OSPF 所需的路由通信量。然后，通过一个连接路由器在区域之间以汇总格式共享拓扑。

| OSPF 区域类型 | 说明 |
| --- | --- |
| 骨干区域 | 骨干区域（区域 0）是 OSPF 网络的核心。所有其他区域都必须连接到此区域，并且区域之间的所有通信必须遍历此区域。可通过骨干区域分配区域之间的所有路由。虽然所有其他 OSPF 区域都必须连接到骨干区域，但是不需要进行直接连接，可以通过虚拟链接进行连接。 |
| 正常 OSPF 区域 | 正常 OSPF 区域不存在任何限制；此区域可以承载所有类型的路由。 |
| 存根 OSPF 区域 | 存根区域不接收源自其他自治系统的路由。Stub 区域的路由通过骨干区域的默认路由执行。 |
| NSSA 区域 | 非纯末节区域 (NSSA) 是存根区域的一种类型，可以通过某些受限例外导入外部路由。 |

## OSPF 路由器类型

在 OSPF 区域中，路由器可划分为以下类别。

- 内部路由器 — 是指仅与同一区域内的设备具有 OSPF 邻居关系的路由器。
- 区域边界路由器 **(ABR)** — 与多个 OSPF 区域内的设备具有 OSPF 邻居关系的路由器。ABR 可从其连接的区域收集拓扑信息，并将收集到的信息分发给骨干区域。
- 骨干路由器 — 骨干路由器是运行 OSPF 的路由器，且至少有一个接口连接到 OSPF 骨干区域。由于 ABR 始终连接到骨干区域，因此始终将其归类为骨干路由器。
- 自治系统边界路由器 **(ASBR)** — 是指连接到一个以上路由协议并在这些路由协议之间交换路由信息的路由器。

# 配置 OSPF

通过从其他路由器获取信息并以链接状态通告 (LSA) 的方式将路由通告到其他路由器，OSPF 动态地确定路由。路由器保存它和目标之间的链接信息，并可高效地作出路由决策。成本会分配到每个路由器接口，在对所有遇到的出站路由接口和接收 LSA 的接口进行总计之后，确定最佳路由是那些具有最低路由成本的路由。

层次结构技术用于限制必须通告的路由数和关联的 LSA。由于 OSPF 动态地处理大量路由信息，因此它的处理器和内存需求高于 RIP。

STEP 1 | 配置虚拟路由的常规配置设置。

有关详细信息，请参阅虚拟路由器。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 启用 OSPF。

1. 选择 **OSPF**选项卡。
2. 选中 **Enable**（启用）可启用 OSPF 协议。
3. 输入 **Router ID**（路由器 **ID**）。
4. 如果不想通过 OSPF 获得任何默认路由，请选中 **Reject Default Route**（拒绝默认路由）。这是建议采用的默认设置。

   如果要允许通过 OSPF 重新分发默认路由，请取消选中 **Reject Default Route**（拒绝默认路由）。

STEP 3 | 配置 OSPF 协议的区域类型。

1. 在 **Areas**（区域）选项卡上，以 *x.x.x.x* 格式为区域 **Add**（添加）**Area Id**（区域 **ID**）。这是每个邻居必须接受才能成为同一区域成员的标识符。
2. 在 **Type**（类型）选项卡上，从区域 **Type**（类型）列表中选择以下某一项：
   - 正常— 没有限制；区域可以承载所有类型的路由。
   - 存根— 区域没有出口。要访问区域外的目标，必须通过连接到其他区域的边界。如果选择此选项，请配置以下设置：
     - **Accept Summary**（接受摘要）— 从其他区域接受链接状态通告 (LSA)。如果禁用 Stub 区域'93;区域边界路由器'94;(ABR) 接口的接受摘要选项，则 OSPF 区域将相当于'93;完全末节区域'94;(TSA)，且 ABR 将不会传播任何摘要 LSA。
     - **Advertise Default Route**（通告默认路由）— 默认路由 LSA 和已配置范围 1-255 内配置的跃点数值一起包含于向存根区域发布的通告中：
   - **NSSA**（非纯末节区域）— 防火墙仅可通过除 OSPF 路由之外的其他路由退出此区域。如果选择 NSSA，请选择 **Accept Summary**（接受摘要）和 **Advertise Default Route**（通告默认路由），如 **Stub** 中所述。如果选择此选项，请配置以下设置：
     - **Type**（类型）— 选择 **Ext 1**（扩展 **1**）或 **Ext 2**（扩展 **2**）路由类型来通告默认 LSA。
     - **Ext Ranges**（扩展范围）— **Add**（添加）要 **Advertise**（通告）或要 **Suppress**（禁止）通告的外部路由范围。
3. 单击 **OK**（确定）。

STEP 4 | 配置 OSPF 协议的区域范围

1. 在 **Range**（范围）选项卡上，**Add**（添加）以将区域中的 LSA 目标地址聚合到子网中。
2. **Advertise**（通告）或 **Suppress**（禁止）通告与子网匹配的 LSA，然后单击 **OK**（确定）。重复该过程以添加其他范围。

STEP 5 | 配置 OSPF 协议的区域接口

1. 在 **Interface**（接口）选项卡上，**Add**（添加）并为每个要包含在区域中的接口输入以下信息：
   - **Interface**（接口）— 选择接口。
   - **Enable**（启用）— 选择此选项可使 OSPF 接口设置生效。
   - **Passive**（被动）— 如果不想让 OSPF 接口发送或接收 OSPF 数据包，请选中此选项。如果您选择此选项，虽然不会发送或接收 OSPF 数据包，但接口仍然包含在 LSA 数据库中。
   - 链接类型 — 如果希望多播 OSPF 呼叫消息自动发现所有能够通过接口访问的邻居（如 Ethernet 接口），请选择广播。选择 **p2p**（点对点）以自动发现邻居。必须手动定义邻居时，选择 **p2mp**（点对多点），并通过该接口 **Add**（添加）可访问所有邻居的邻居 IP 地址。
   - **Metric**（跃点数）— 输入此接口的 OSPF 跃点数（范围为 0-65,535，默认为 10）。
   - **Priority**（优先级）— 输入此接口的 OSPF 优先级。这是指要选为指定路由器 (DR) 或备份 DR (BDR) 的路由器的优先级（范围为 0-255，默认为 1）。值配置为零时，路由器不会被选为 DR 或 BDR。
   - 身份验证配置文件— 选择先前定义的身份验证配置文件。
   - **Timing**（计时）— 如果需要，修改计时设置（不推荐）。有关这些设置的详细信息，请参阅联机帮助。


© 2019 Palo Alto Networks, Inc.

2. 单击 **OK**（确定）。

STEP 6 | 配置区域虚拟链接。

1. 在 **Virtual Link**（虚拟链接）选项卡上，为每个要包含在骨干区域中的虚拟链接 **Add**（添加）以下信息：
   - 名称— 输入虚拟链接的名称。
   - 启用— 选择该项可启用虚拟链接。
   - 邻居 **ID**— 输入虚拟链接另一端的路由器（邻居）的路由器 ID。
   - 中转区域— 输入实际包含虚拟链接的中转区域的区域 ID。
   - 计时 — 建议保留默认计时设置。
   - 身份验证配置文件— 选择先前定义的身份验证配置文件。
2. 单击 **OK**（确定），保存虚拟链接。
3. 单击 **OK**（确定），保存区域。

STEP 7 | （可选）配置身份验证配置文件。

默认情况下，防火墙无法使用 OSPF 身份验证在 OSPF 邻居之间进行交换。您也可以通过简单密码或使用 MD5 身份验证配置 OSPF 邻居之间的 OSPF 身份验证。推荐使用 MD5 身份验证，该身份验证比简单密码更加安全。

简单密码 **OSPF** 身份验证

1. 选择 **Auth Profiles**（身份验证配置文件）选项卡，并 **Add**（添加）身份验证配置文件的名称以对 OSPF 消息进行身份验证。
2. 选择 **Simple Password**（简单密码）作为 **Password Type**（密码类型）。
3. 输入一个简单密码并确定。

**MD5 OSPF** 身份验证

1. 选择 **Auth Profiles**（身份验证配置文件）选项卡，并 **Add**（添加）身份验证配置文件的名称以对 OSPF 消息进行身份验证。
2. 选择 **MD5** 作为 **Password Type**（密码类型），并 **Add**（添加）一个或多个密码条目，包括：
   - 密匙 ID（范围 0-255）
   - 密钥
   - 选择 **Preferred**（首选）选项以指定使用该密钥对传出消息进行身份验证。
3. 单击 **OK**（确定）。

STEP 8 | 配置 OSPF 高级选项。

1. 在 **Advanced**（高级）选项卡上，选中 **RFC 1583 Compatibility**（**RFC 1583** 兼容）以确保与 RFC 1583 兼容。
2. 指定 **SPF Calculation Delay (sec)**（**SPF** 计算延迟（秒））计时器的值 — 可让您调整在接收新拓扑信息和执行 SPF 计算之间的延迟。值越低 OSPF 重新收敛速度越快。与防火墙对等的路由器应使用相同的延迟值来优化收敛时间。
3. 指定 **LSA Interval (sec) time**（**LSA** 间隔时间（秒））计时器的值 — 同一个 LSA（相同路由器、相同类型、相同 LSA ID）的两个实例间传输的最短时间。这等同于 RFC 2328 中的 MinLSInterval。可使用较低的值，以减少发生拓扑更改时进行重新收敛的时间。
4. 单击 **OK**（确定）。

STEP 9 | **Commit**（提交）更改。

# 配置 OSPFv3

OSPF 支持 IPv4 和 IPv6。如果使用 IPv6，则必须使用 OSPFv3。



© 2019 Palo Alto Networks, Inc.

STEP 1 | 配置虚拟路由的常规配置设置。

有关详细信息，请参阅虚拟路由器。

STEP 2 | 配置 OSPFv3 的常规配置设置。

1. 选择 **OSPFv3** 选项卡。
2. 选中 **Enable**（启用）可启用 OSPF 协议。
3. 输入 **Router ID**（路由器 **ID**）。
4. 如果不想通过 OSPFv3 获得任何默认路由，请选中 **Reject Default Route**（拒绝默认路由）。这是建议采用的默认设置。

   如果要允许通过 OSPFv3 重新分发默认路由，请取消选中 **Reject Default Route**（拒绝默认路由）。

STEP 3 | 配置 OSPFv3 协议的身份验证配置文件。

OSPFv3 不包括任何自带的身份验证功能，它完全依赖 IPSec 来确保邻居之间的通信安全。

配置身份验证配置文件时，必须使用封装式安全措施负载 (ESP)（推荐）或 IPv6 身份验证标头 (AH)。

**OSPFv3 的 ESP 身份验证**

1. 在 **Auth Profiles**（身份验证配置文件）选项卡上，**Add**（添加）身份验证配置文件的名称以对 OSPFv3 消息进行身份验证。
2. 指定安全策略索引 (**SPI**)（十进制值，范围从 00000000 到 FFFFFFFF）。OSPFv3 邻接的两端必须具有相匹配的 SPI 值。
3. 对 **Protocol**（协议）选择 **ESP**。
4. 选择 **Crypto Algorithm**（加密算法）。

   您可以选择 **None**（无）或以下算法之一：**SHA1**、**SHA256**、**SHA384**、**SHA512** 或 **MD5**。
5. 如果选择了 **Crypto Algorithm**（加密算法）而不是选择的“无”，请输入 **Key**（密匙）值并确认。

**OSPFv3 的 AH 身份验证**

1. 在 **Auth Profiles**（身份验证配置文件）选项卡上，**Add**（添加）身份验证配置文件的名称以对 OSPFv3 消息进行身份验证。
2. 指定安全策略索引 (**SPI**)。OSPFv3 邻居两端之间的 SPI 必须匹配。SPI 数量必须是介于 00000000 与 FFFFFFFF 之间的十六进制值。
3. 对 **Protocol**（协议）选择 **AH**。
4. 选择 **Crypto Algorithm**（加密算法）。

   您可以输入以下算法之一：**SHA1**、**SHA256**、**SHA384**、**SHA512** 或 **MD5**。
5. 输入 **Key**（密匙）值并确认。
6. 单击 **OK**（确定）。
7. 再次单击“虚拟路由器 - OSPF 身份验证配置文件”对话框中的 **OK**（确定）。

STEP 4 | 配置 OSPFv3 协议的区域类型。

1. 在 **Areas**（区域）选项卡上，**Add**（添加）**Area Id**（区域 **ID**）。这是每个邻居必须接受才能成为同一区域成员的标识符。
2. 在 **General**（常规）选项卡上，从区域 **Type**（类型）列表中选择以下某一项：
   - 正常— 没有限制；区域可以承载所有类型的路由。
   - 存根— 区域没有出口。要访问区域外的目标，必须通过连接到其他区域的边界。如果选择此选项，请配置以下设置：
     - **Accept Summary**（接受摘要）— 从其他区域接受链接状态通告 (LSA)。如果禁用 Stub 区域'93;区域边界路由器'94;(ABR) 接口的接受摘要选项，则 OSPF 区域将相当于'93;完全末节区域'94;(TSA)，且 ABR 将不会传播任何摘要 LSA。



© 2019 Palo Alto Networks, Inc.

- **Advertise Default Route**（通告默认路由）— 默认路由 LSA 和已配置范围 1-255 内配置的跃点数值一起包含于向存根区域发布的通告中：

- **NSSA**（非纯末节区域）— 防火墙仅可通过除 OSPF 路由之外的其他路由退出此区域。如果选择此选项，请配置 **Accept Summary**（接受摘要）和 **Advertise Default Route**（通告默认路由），如 **Stub** 中所述。如果选择此选项，请配置以下设置：
  - **Type**（类型）— 选择 **Ext 1**（扩展 **1**）或 **Ext 2**（扩展 **2**）路由类型来通告默认 LSA。
  - **Ext Ranges**（扩展范围）— **Add**（添加）您希望为其启用或禁止通告的外部路由的范围。

STEP 5 | 将 OSPFv3 身份验证配置文件关联到区域或接口。

关联到区域

1. 在 **Areas**（区域）选项卡上，从表中选择一个现有区域。
2. 在 **General**（常规）选项卡上，从 **Authentication**（身份验证）列表中选择一个已定义的 **Authentication Profile**（身份验证配置文件）。
3. 单击 **OK**（确定）。

关联到接口

1. 在 **Areas**（区域）选项卡上，从表中选择一个现有区域。
2. 选择 **Interface**（接口）选项卡，并从 **Auth Profile**（身份验证配置文件）列表中 **Add**（添加）要与 OSPF 接口关联的身份验证配置文件。
3. 单击 **OK**（确定）。

STEP 6 | 再次单击 **OK**（确定）以保存区域设置。

STEP 7 | （可选）配置导出规则。

1. 在 **Export Rules**（导出规则）选项卡上，选中 **Allow Redistribute Default Route**（允许重新分发默认路由）以允许通过 OSPFv3 重新分发默认路由。
2. 单击添加。
3. 输入 **Name**（名称）；值必须是有效的 IPv6 子网或有效的重新分发配置文件名称。
4. 选择 **New Path Type**（新路径类型），**Ext 1** 或 **Ext 2**。
5. 为匹配路由指定具有 32 位值（点分十进制）的 **New Tag**（新标记）。
6. 为新规则分配 **Metric**（跃点数）（范围为 1 - 16,777,215）。
7. 单击 **OK**（确定）。

STEP 8 | 配置高级 OSPFv3 选项。

1. 如果想要防火墙参与 OSPF 拓扑分发且不用于转发中转通信，请在 **Advanced**（高级）选项卡上选中 **Disable Transit Routing for SPF Calculation**（禁用 **SPF** 计算的中转路由）。
2. 指定 **SPF Calculation Delay (sec)**（**SPF** 计算延迟（秒））计时器的值 — 可让您调整在接收新拓扑信息和执行 SPF 计算之间的延迟。值越低 OSPF 重新收敛速度越快。与防火墙对等的路由器应使用相同的延迟值来优化收敛时间。
3. 指定 **LSA Interval (sec) time**（**LSA** 间隔时间（秒））计时器的值，同一个 LSA（相同路由器、相同类型、相同 LSA ID）的两个实例间传输的最短时间（秒）。这等同于 RFC 2328 中的 MinLSInterval。可使用较低的值，以减少发生拓扑更改时进行重新收敛的时间。
4. （可选）配置 OSPF 平稳重启。
5. 单击 **OK**（确定）。

STEP 9 | **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 配置 OSPF 平稳重启

发生故障时，OSPF 平稳重启通过防火墙在短时转换期间内指导 OSPF 邻居继续使用路由器。这么做可以通过降低路由表重新配置和短时故障期间发生相关路由翻动的频率，从而增强网络的稳定性。

对于 Palo Alto Networks 防火墙，OSPF 平稳重启需要执行以下操作：

- 防火墙充当重启设备 — 当防火墙发生短时故障或短时间内不可用时，它会向其 OSPF 邻居发送宽限 LSA。必须将邻居配置为在平稳重启帮助程序模式下运行。在帮助程序模式中，邻居会接收到告知它防火墙将在定义为 **Grace Period**（宽限期）的指定时段内执行平稳重启的宽限 LSA。在宽限期期间，OSPF 邻居继续通过防火墙转发路由，并发送用于通知路由的 LSA。如果防火墙在宽限期过期之前恢复操作，则会像之前未发生网络故障时一样继续转发通信。如果防火墙在宽限期过期后仍无法恢复操作，OSPF 邻居则会退出帮助程序模式并恢复正常操作，这样就需要重新配置路由表以绕过防火墙。
- 防火墙充当平稳重启帮助程序 — 当邻居路由器可能发生短时故障的情况时，可以将防火墙配置为在平稳重启帮助程序模式中进行操作。在这种情况下，防火墙将采用 **Max Neighbor Restart Time**（最长邻近重新启动时间）。当防火墙接收到 OSPF 邻居发出的宽限 LSA 时，在宽限期或最长邻近重新启动时间过期之前，它会继续将通信路由给此邻居并通过此邻居通告路由。如果此邻居恢复服务时宽限期或邻居的最长重启时间未过期，则会像发生网络故障之前一样继续转发通信。如果此邻居在宽限期或最长邻近重新启动时间过期后仍未恢复服务，防火墙则会退出帮助程序模式并恢复正常操作，这样就需要重新配置路由表以绕过此邻居。

STEP 1 | 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择要配置的虚拟路由器。

STEP 2 | 选择 **OSPF** > **Advanced**（高级）或 **OSPFv3** > **Advanced**（高级）。

STEP 3 | 验证以下复选框是否已选中（默认启用）：

- **Enable Graceful Restart**（启用正常重启）
- **Enable Helper Mode**（启用帮助程序模式）
- **Enable Strict LSA checking**（启用严格的 **LSA** 检查）

除非拓扑有要求，否则始终选中上述复选框。

STEP 4 | 配置 **Grace Period**（宽限期），以秒计。

STEP 5 | 配置 **Max Neighbor Restart Time**（最长邻近重新启动时间），以秒计。

# 确认 OSPF 运行

提交 OSPF 配置后，可以通过以下任何操作确认 OSPF 是否正在运行：

- 查看路由表
- 确认 OSPF 邻居
- 确认建立了 OSPF 连接

## 查看路由表

通过查看路由表，可以了解是否已建立 OSPF 路由。可以通过 Web 界面或 CLI 查看路由表。如果正在使用 CLI，请使用以下命令：

- `show routing route`
- `show routing fib`

如果使用 Web 界面查看路由表，请使用以下工作流程：

STEP 1 | 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），再在所需虚拟路由器的同一行中，单击 **More Runtime Stats**（更多运行时统计数据）链接。


© 2019 Palo Alto Networks, Inc.

STEP 2 | 选择 **Routing**（路由）> **Route Table**（路由表），并检查通过 OSPF 记录的路由器路由表的 **Flags**（标记）列。

## 确认 *OSPF* 邻居

使用以下工作流程来确认 OSPF 邻接已建立：

STEP 1 | 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），再在所需虚拟路由器的同一行中，单击 **More Runtime Stats**（更多运行时统计数据）链接。

STEP 2 | 选择 **OSPF** > **Neighbor**（邻居），并检查 **Status**（状态）栏，以确定是否已建立 OSPF 邻接。

## 确认建立了 *OSPF* 连接

查看系统日志以确认防火墙已建立 OSPF 连接。

STEP 1 | 选择 **Monitor**（监控）> **System**（系统）并查找用于确认 OSPF 邻接已建立的消息。

STEP 2 | 选择 **OSPF** > **Neighbor**（邻居），并检查 **Status**（状态）栏，以确定是否已建立 OSPF 邻接（已满）。



© 2019 Palo Alto Networks, Inc.

# BGP

边界网关协议 (BGP) 是主互联网路由协议。BGP 根据自治系统 (AS) 内提供的 IP 前缀确定网络可访问性，其中 AS 是网络供应商指定为单个路由策略组成部分的一组 IP 前缀。


- BGP 概述
- MP-BGP
- 配置 BGP
- 为 IPv4 或 IPv 6 单播配置带 MP-BGP 的 BGP 对等设备
- 为 IPv4 多播配置带 MP-BGP 的 BGP 对等设备
- BGP 联合


## BGP 概述

BGP 在自治系统之间（外部 BGP 或 eBGP）或 AS 内部（内部 BGP 或 iBGP）发挥作用，以便与 BGP 演讲者交换路由和可访问性信息。防火墙提供包括以下功能的完整 BGP 实现：

- 关于每个虚拟路由器一个 BGP 路由实例的规范。
- 每个虚拟路由器的 BGP 设置，包括基本参数（如本地路由 ID 和本地 AS）和高级选项（如路径选择、路由反射器、BGP 联合、路由翻动惩罚和平稳重启）。
- 对等组和邻居设置，包括邻居地址、远程 AS 和高级选项（如邻居属性和连接）。
- 用于控制路由导入、导出和通告的路由策略，基于前缀的筛选以及地址聚合。
- IGP-BGP 交互，通过使用重新分发配置文件将路由注入 BGP。
- 身份验证配置文件，指定用于 BGP 连接的 MD5 身份验证密钥。身份验证有助于防止路由泄漏和成功的 DoS 攻击。
- 多协议 BGP (MP-BGP) 允许 BGP 对等设备在更新数据包中携带 IPv6 单播路由和 IPv4 多播路由，并允许防火墙和 BGP 对等设备使用 IPv6 地址进行通信。

## MP-BGP

BGP 支持 IPv4 单播前缀，但使用 IPv4 多播路由或 IPv6 单播前缀的 BGP 网络需要多协议 BGP (MP-BGP) 才能交换 IPv4 单播以外的地址类型的路由。MP-BGP 允许 BGP 对端设备在更新数据包中携带 IPv4 多播路由和 IPv6 单播路由，以及 BGP 对端设备在不启用 MP-BGP 的情况下携带的 IPv4 单播路由。

这样，MP-BGP 可以为您使用本地 IPv6 或双栈 IPv4 和 IPv6 的 BGP 网络提供 IPv6 连接。服务提供商可以向客户提供 IPv6 服务，企业可以使用服务提供商的 IPv6 服务。防火墙和 BGP 对端设备可以使用 IPv6 地址进行相互通信。

为使 BGP 支持多个网络层协议（除用于 IPv4 的 BGP 外），BGP-4 多协议扩展 (RFC 4760) 使用防火墙在 BGP 更新数据包中发送和接收的多协议可达性 NLRI 属性中的网络层可达性信息 (NLR)。该属性包含有关目标前缀的信息，包括两个标识符：

- 地址系列编号中 IANA 定义的地址系列标识符 (AFI)，表示目标前缀是 IPv4 或 IPv6 地址。（PAN-OS 支持 IPv4 和 IPv6 AFI。）
- PAN-OS 中的随后地址系列标识符 (SAFI)，表示目标前缀是单播或多播地址（如果 AFI 为 IPv4），或者目标前缀为单播地址（如果 AFI 为 IPv6）。PAN-OS 不支持 IPv6 多播。

如果为 IPv4 多播启用 MP-BGP，或者配置多播静态路由，则防火墙支持静态路由的单独单播和多播路由表。您可能希望将前往同一目标的单播和多播流量分开。多播流量可以采取与单播流量不同的路径，因为（举例来说），您的多播流量非常重要，因此您需要通过使其花费更少的跃点或经历更少的延迟才能更有效。

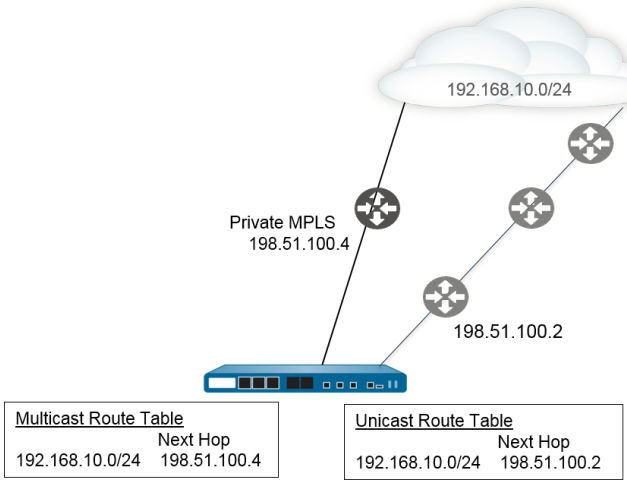
当 BGP 导入或导出路由，发送条件通告或执行路由重新分发或路由聚合时，还可以通过配置 BGP 仅使用单播或多播路由表（或两者）路由来更好地控制 BGP 的功能。



© 2019 Palo Alto Networks, Inc.

您可以通过启用 MP-BGP 并选择 IPv4 地址系列和多播随后地址系列，或通过在多播路由表中安装 IPv4 静态路由来决定使用专用多播 RIB（路由表）。采用上述任一种方法使用多播 RIB 后，防火墙将多播 RIB 用于所有多播路由和反向路径转发 (RPF)。如果您喜欢将单播 RIB 用于所有路由（单播和多播），则不应通过任一方法启用多播 RIB。

下图中，单播路由表中已安装 192.168.10.0/24 的静态路由，下一个跃点为 198.51.100.2。然而，多播流量可以采取与 MPLS 私有云不同的路径；在具有不同的下一个跃点 (198.51.100.4) 的多播路由表中安装相同的静态路由，以使其路径不同。




使用单独的单播和多播路由表可以在配置这些 BGP 功能时提供更多的灵活性和控制：

- 如上例所述，将 IPv4 静态路由安装到单播或多播路由表或单播和多播路由表。（只能在单播路由表中安装 IPv6 静态路由）。
- 创建导入规则，使匹配条件的任何前缀都将导入到单播或多播路由表，或导入单播和多播路由表中。
- 创建导出规则，使匹配条件的前缀从单播或多播路由表或单播和多播路由表中导出（发送到对端设备）。
- 使用非现有筛选器配置条件通告，以便防火墙搜索单播或多播路由表（或单播和多播路由表），以确保该表中不存在该路由，因此防火墙通告不同的路由。
- 使用通告筛选器配置条件通告，以便防火墙通过单播或多播路由表或单播和多播路由表通告符合条件的路由。
- 重新分发出现在单播或多播路由表中的路由，或单播和多播路由表中的路由。
- 使用通告筛选器配置路由聚合，以便通告来自单播或多播路由表或单播和多播路由表的聚合路由。
- 相反，使用禁止筛选器配置路由聚合，以便禁止（未通告）来自单播或多播路由表或单播和多播路由表的聚合路由。

使用 IPv6 地址系列配置带 MP-BGP 的对端设备时，可以在导入规则、导出规则、条件通告（通告筛选器和非现有筛选器）以及聚合规则（通告筛选器、禁止筛选器和聚合路由属性）的“地址前缀”和“下一个跃点”字段中使用 IPv6 地址。

# 配置 BGP

请执行以下任务以配置 BGP。

STEP 1 | 配置虚拟路由的常规配置设置。

有关详细信息，请参阅 虚拟路由器。

STEP 2 | 启用虚拟路由器的 BGP、分配路由器 ID，并将虚拟路由器分配给 AS。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。



© 2019 Palo Alto Networks, Inc.

2. 选择 **BGP**。
3. 为此虚拟路由器启用 BGP。
4. 为虚拟路由器的 BGP 分配一个 **Router ID**（路由器 **ID**），通常为 IPv4 地址，以确保路由器 ID 的唯一性。
5. 分配 **AS Number**（**AS** 编号），即虚拟路由器所属的、以路由器 ID 为基础的 AS 的编号（范围为 1-4,294,967,295）。
6. 单击 **OK**（确定）。

STEP 3 | 配置常规 BGP 配置设备。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **BGP** > **General**（常规）。
3. 选中 **Reject Default Route**（拒绝默认路由）以忽略由 BGP 对等通告的任何默认路由。
4. 选中 **Install Route**（安装路由）可在全局路由表中安装 BGP 路由。
5. 选择 **Aggregate MED**（聚合 **MED**）以启用路由聚合，即使路由有不同的多出口鉴别 (MED) 值也如此。
6. 指定 **Default Local Preference**（默认本地首选项），可使用该值在不同路径之间确定首选路径。
7. 选择 **AS Format**（**AS** 格式）以实现互操作性：
   - **2 Byte**（**2** 字节）（默认）
   - **4 Byte**（**4** 字节）

   运行时统计数据根据 RFC 5396，使用 *asplain* 表示法显示 *BGP 4* 字节 *AS* 编号。
8. 启用或禁用 **Path Selection**（路径选择）的下列每个设置：
   - **Always Compare MED**（始终比较 **MED**）— 启用此比较，从不同自治系统中的邻居处选择路径。
   - **Deterministic MED Comparison**（确定的 **MED** 比较）— 启用此比较，以在 IBGP 对端设备（同一自治系统中的 BGP 对端设备）通告的路由之间进行选择。
9. 对于 **Auth Profiles**（身份验证配置文件），**Add**（添加）身份验证配置文件：
   - **Profile Name**（配置文件名称）— 输入名称以标识配置文件。
   - **Secret/Confirm Secret**（密钥/确认密钥）— 输入并确认用于 BGP 对等通信的口令。该密钥被用作 MD5 身份验证的密钥。
10. 双击 **OK**（确定）。

STEP 4 | （可选）配置 BGP 设置。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **BGP** > **Advanced**（高级）。
3. 如果您已配置 ECMP 并希望通过多个 BGP 自治系统运行 ECMP，请选择 **ECMP Multiple AS Support**（**ECMP** 多个 **AS** 支持）。
4. 默认启用 **Enforce First AS for EBGP**（为 **EBGP** 执行第一个 **AS**）后，促使防火墙丢弃来自 eBGP 对端的传入更新数据包，而 eBGP 对端未列出自己的 AS 编号作为 AS_PATH 属性中的第一个 AS 编号。
5. 选择 **Graceful Restart**（平稳重启）并配置以下计时器：
   - **Stale Route Time (sec)**（路由停滞时长（秒））— 指定路由可保持停滞状态的时长（以秒计，范围为 1-3,600，默认为 120）。
   - **Local Restart Time (sec)**（本地重启时长（秒））— 指定本地设备重启所需时长（以秒计）。该值将被通告到对端（范围为 1-3,600，默认为 120）。
   - **Max Peer Restart Time (sec)**（最长对端重启时间（秒））— 指定本地设备接受的对端设备最长平滑重启时间（以秒计，范围是 1-3,600，默认为 120）。
6. 对于 **Reflector Cluster ID**（反射器集群 **ID**），指定代表反射器集群的 IPv4 标识符。
7. 对于 **Confederation Member AS**（联合成员 **As**），请指定仅在 BGP 联合内可见的自治系统编号标识符（也称为子自治系统编号）。有关详细信息，请参阅BGP 联合。


© 2019 Palo Alto Networks, Inc.

8. 为每个想要配置的惩罚配置文件 **Add**（添加）以下信息，选择 **Enable**（启用），然后单击 **OK**（确定）：
   - **Profile Name**（配置文件名称）— 输入名称以标识配置文件。
   - **Cutoff**（截断）— 指定路由撤销阈值，高于该值的路由通告将会被抑制（范围为 0.0-1,000.0，默认为 1.25）。
   - **Reuse**（重用）— 指定路由撤销阈值，低于该值的被抑制路由将会再次使用（范围为 0.0-1,000.0，默认为 5）。
   - **Max Hold Time (sec)**（最长保持时间（秒））— 指定路由可被抑制的最长时间，不论其如何不稳定（以秒计，范围为 0-3,600，默认为 900）。
   - **Decay Half Life Reachable (sec)**（可达半衰期（秒））— 指定一段时间，超过该时间后，如果认为路由可达，则路由的稳定性跃点数将会减半（以秒计，范围为 0-3,600，默认为 300）。
   - **Decay Half Life Unreachable (sec)**（不可达半衰期（秒））— 指定一段时间，超过该时间后，如果认为路由不可达，则路由的稳定性跃点数将会减半（以秒计，范围为 0-3,600，默认为 300）。
9. 双击 **OK**（确定）。

STEP 5 | 配置 BGP 对端组。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **BGP** > **Peer Group**（对端组），**Add**（添加）对端组 **Name**（名称），然后 **Enable**（启用）它。
3. 选中 **Aggregated Confed AS Path**（聚合 **Confed AS** 路径）以包含配置的聚合联合 AS 的路径。
4. 选中 **Soft Reset with Stored Info**（带存储信息的软重置），以便在更新对等端设置后执行防火墙的软重置。
5. 选择对端组 **Type**（类型）：
   - **IBGP — Export Next Hop**（导出下一个跃点）：选择 **Original**（原始跃点）或 **Use self**（使用自身）。
   - **EBGP Confed — Export Next Hop**（导出下一个跃点）：选择 **Original**（原始跃点）或 **Use self**（使用自身）。
   - **EBGP Confed — Export Next Hop**（导出下一个跃点）：选择 **Original**（原始跃点）或 **Use self**（使用自身）。
   - **EBGP — Import Next Hop**（导入下一个跃点）：选择 **Original**（原始跃点）或 **Use self**（使用自身）；并 **Export Next Hop**（导出下一个跃点）：指定 **Resolve**（解析跃点）或 **Use self**（使用自身）。如果要强制 BGP 从更新（防火墙发送给另一个 AS 的对等设备）的 AS_PATH 属性中删除私有 AS 编号，请选择 **Remove Private AS**（删除私有 **AS**）。
6. 单击 **OK**（确定）。

STEP 6 | 配置属于对端组的 BGP 对等设备，并指定其寻址。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **BGP** > **Peer Group**（对端组），并选择创建的对端组。
3. 对于对等设备，按 **Name**（名称）**Add**（添加）对端。
4. **Enable**（启用）对端。
5. 输入对端所属的 **Peer As**（对端 **AS**）。
6. 选择 **Addressing**（寻址）。
7. 对于 **Local Address**（本地地址），请选择正在配置 BGP 的 **Interface**（接口）。如果接口有多个 **IP** 地址，请输入该接口的 IP 地址作为 BGP 对端。
8. 对于**Peer Address**（对等地址），请选择 **IP**并输入 IP 地址，或选择或创建一个地址对象，或是选择 **FQDN** 并输入类别 FQDN 的 FQDN 或地址对象。

   防火墙仅使用从 *FQDN* 的 *DNS* 解析出的一个 *IP* 地址（来自每个 *IPv4* 或 *IPv6* 系列类型）。如果 *DNS* 解析出多个地址，则防火墙会使用与配置用于 *BGP* 对等设备的 *IP* 系列类型（*IPv4* 或 *IPv6*）匹配的首选 *IP* 地址。此首选 *IP* 地址是 *DNS* 服务器在其初始响



© 2019 Palo Alto Networks, Inc.

应中返回的第一个地址。只要地址在后续响应中出现，无论其顺序如何，防火墙都会将该地址视为首选地址。

9. 单击 **OK**（确定）。

STEP 7 | 配置 BGP 对端的连接设置。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **BGP** > **Peer Group**（对端组），并选择创建的对端组。
3. 选择您配置的 **Peer**（对端）。
4. 选择 **Connection Options**（连接选项）。
5. 选择对端的 **Auth Profile**（身份验证配置文件）。
6. 设置 **Keep Alive Interval(sec)**（保持活动状态间隔（秒））— 指定一个时间间隔，在该时间间隔之后，将根据保持时间设置抑制来自对端的路由（以秒计，范围为 0-1,200，默认为 30）。
7. 设置 **Multi Hop**（多个跃点）— 设置 IP 标头中的生存时间 (TTL) 值（范围为 0-255，默认为 0）。默认为 0 表示 1 代表 eBGP。默认为 0 表示 255 代表 iBGP。
8. 设置 **Open Delay Time (sec)**（打开延迟时间（秒））— TCP 握手和防火墙发送第一个 BGP 打开消息以建立 BGP 连接之间的延迟时间（以秒计，范围为 0-240，默认为 0）。
9. 设置 **Hold Time (sec)**（保持时间（秒））— 在关闭对端连接之前，从对端发出连续的 Keepalive 或 Update 消息之间所经历的时间（以秒计，范围为 3-3,600，默认为 90）。
10. 设置 **Idle Hold Time (sec)**（空闲保持时间（秒））— 在重试与对端连接之前等待的时间（以秒计，范围为 1-3,600，默认为 15）。
11. 设置 **Min Route Advertisement Interval (sec)**（最小路由通告间隔（秒））— 即 BGP 发言者（防火墙）发送给通告路由或撤销路由的 BGP 对端的两条连续 Update 消息之间的最短时间（以秒计，范围为 1 至 600，默认为 30）。
12. 对于 **Incoming Connections**（传入连接），输入 **Remote Port**（远程端口），并选择 **Allow**（允许）以允许流量流进该端口。
13. 对于 **Outgoing Connections**（传出连接），输入 **Local Port**（本地端口），并选择 **Allow**（允许）以允许流量流出该端口。
14. 单击 **OK**（确定）。

STEP 8 | 配置用于路由反射器客户端、对等类型、最大前缀数和双向转发检测 (BFD) 的 BGP 对端设置。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **BGP** > **Peer Group**（对端组），并选择创建的对端组。
3. 选择您配置的 **Peer**（对端）。
4. 选择 **Advanced**（高级）。
5. 对于 **Reflector Client**（反射器客户端），请选择以下选项之一：
   - **non-client**（非客户端）（默认）— 对端不是路由反射器客户端。
   - **client**（客户端）— 对端是路由反射器客户端。
   - 网状客户端
6. 对于 **Peering Type**（对等类型），请选择以下选项之一：
   - **Bilateral**（双边）— 两个 BGP 对端建立一个对等连接。
   - **Unspecified**（不指定）（默认）。
7. 对于 **Max Prefixes**（最大前缀数），输入受支持 IP 前缀的最大数量（范围为 1-100,000），或选择 **unlimited**（无限制）。
8. 如需为对端启用 **BFD**（只要 BFD 未在虚拟路由器级别上对 BGP 禁用，则将因此而覆盖 BGP 的 BFD 设置），请在以下各项中选择一项：
   - **Default**（默认）— 对端仅使用默认 BFD 设置。
   - **Inherit-vr-global-setting**（继承 **Vr** 全局设置）（默认设置）— 对端继承为虚拟路由器的 BGP 全域选择的 BFD 配置文件。
   - 您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。


© 2019 Palo Alto Networks, Inc.

选择 *Disable BFD*（禁用 *BFD*）可对 *BGP* 对端禁用 *BFD*。

9. 单击 **OK**（确定）。

STEP 9 | 配置导入和导出规则。

导入和导出规则用于进出其他路由器的导入和导出路由（例如，从互联网服务提供商导入默认路由）。

1. 选择 **Import**（导入），在 **Rules**（规则）字段中 **Add**（添加）名称，然后 **Enable**（启用）导入规则。
2. **Add**（添加）路由器要从中导入的 **Peer Group**（对端组）。
3. 单击 **Match**（匹配），并定义用于筛选路由信息的选项。您也可以定义路由器的多出口鉴别 (MED) 值和下一个跃点值来筛选路由。MED 选项是一个外部跃点，它会告知邻居 AS 的首选路径。较低的值比较高的值优先。
4. 单击 **Action**（操作），并定义基于 **Match**（匹配）选项卡中定义的筛选选项应该执行的操作（允许或拒绝）。如果选择 **Deny**（拒绝），则无需另外定义选项。如果选择 **Allow**（允许），则定义其他属性。
5. 选择 **Export**（导出）并定义导出属性，这些属性与 **Import**（导入）设置相似，但用于控制从防火墙导出到邻居的路由信息。
6. 单击 **OK**（确定）。

STEP 10 | 配置条件通告，可以控制当在本地 BGP 路由表 (LocRIB) 中有个别路由不可用时，由哪个路由发出通告，以指示对等操作或可访问性问题。

在尝试强制通过一个 AS 路由到另一个 AS 的情况下，如通过多个 ISP 链接到互联网且希望将通信路由到某个提供商而非另一个（除非与首选提供商断开连接），此功能特别有用。

1. 选择 **Conditional Adv**（条件通告），并 **Add**（添加）**Policy**（策略）名称。
2. **Enable**（启用）条件通告。
3. 在 **Used By**（使用者）部分，**Add**（添加）将使用条件通告策略的对端组。
4. 选择 **Non Exist Filter**（非现有筛选器），并定义首选路由的网络前缀。这可指定要通告的路由（如果此路由在本地 BGP 路由表中可用）。如果要通告的前缀与非现有筛选程序匹配，则通告将被禁止。
5. 选择 **Advertise Filters**（通告筛选器），并定义本地 RIB 路由表中的路由前缀。当非现有筛选器中的路由在本地路由表中不可用时，应通告此前缀。如果要通告的前缀与非现有筛选程序不匹配，将发生通告。
6. 单击 **OK**（确定）。

STEP 11 | 在 BGP 配置中配置摘要路径的聚合选项。

BGP 路径聚合用于控制 BGP 聚合地址的方式。表中每个条目都会创建一个聚合地址。当探测到至少一个指定路由与指定地址相匹配时，这样就会在路由表中生成聚合条目。

1. 选择 **Aggregate**（聚合），**Add**（添加）聚合地址的名称。
2. 输入要作为已聚合前缀的主前缀的网络 **Prefix**（前缀）。
3. 选择 **Suppress Filters**（抑制筛选器），并定义用于抑制相匹配的路由的属性。
4. 选择 **Advertise Filters**（通告筛选器），并定义用于始终将相匹配的路由通告给对端的属性。
5. 单击 **OK**（确定）。

STEP 12 | 配置重新分发规则。

此规则用于重新分发主路由和不位于对端路由器的本地 RIB 上的未知路由。

1. 选择 **Redist Rules**（重新分发规则），**Add**（添加）新的重新分发规则。
2. 输入 IP 子网 **Name**（名称）或选择重新分发配置文件。如有必要，您也可以配置新的重新分发配置文件。
3. **Enable**（启用）规则。



© 2019 Palo Alto Networks, Inc.

4. 输入要用于此规则的路由 **Metric**（跃点数）。
5. 在 **Set Origin**（设置起点）列表中，选择 **incomplete**（未完成）、**igp** 或 **egp**。
6. （可选）设置 MED、本地参数、AS 路径限值和社区值。
7. 单击 **OK**（确定）。

STEP 13 | **Commit**（提交）更改。

# 为 IPv4 或 IPv 6 单播配置带 MP-BGP 的 BGP 对等设备

配置 BGP 后，出于以下任意原因，应为 IPv4 或 IPv6 单播配置带 MP-BGP 的 BGP 对等设备：

- 要使 BGP 对等设备携带 IPv6 单播路由，请配置具有 **Ipv6** 地址系列类型和 **Unicast**（单播）随后地址系列的 MP-BGP，以便对等设备可以发送包含 IPv6 单播路由在内的 BGP 更新。BGP 对端操作（本地地址和对端地址）仍可以是 IPv4 地址，也可以均为 IPv6 地址。
- 要使用 IPv6 地址执行 BGP 对端操作（**Local Address**（本地地址）和 **Peer Address**（对端地址）应使用 IPv6 地址）。

以下任务说明如何启用带 MP-BGP 的 BGP 对等设备，以携带 IPv6 单播路由，因此可使用 IPv6 地址进行对端操作。

该任务还显示了如何查看单播或多播路由表，以及如何查看转发表、BGP 本地 RIB 和 BGP RIB 输出（发送给邻居的路由），以查看单播或多播路由表或特定地址系列（IPv4 或 IPv6）中的路由。

STEP 1 | 为对等设备启用 MP-BGP 扩展。

完成以下配置，使 BGP 对等设备的更新数据包中携带 IPv4 或 IPv6 单播路由，防火墙可以使用 IPv4 或 IPv6 地址与其对等设备进行通信。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择正在配置的虚拟路由器。
2. 选择 **BGP**。
3. 选择 **Peer Group**（对等组），并选择对等组。
4. 选择 BGP 对等设备（路由器）。
5. 选择 **Addressing**（寻址）。
6. 选择对等设备的 **Enable MP-BGP Extensions**（启用 **MP-BGP** 扩展）。
7. 对于 **Address Family Type**（地址系列类型），请选择 **IPv4** 或 **IPv6**。例如，选择 IPv6。
8. 对于 **Subsequent Address Family**（随后地址系列），请选择 **Unicast**（单播）。如果您为地址系列选择 **IPv4**，则也可以选择 **Multicast**（多播）。
9. 对于 **Local Address**（本地地址），选择 **Interface**（接口），还可以选择 **IP** 地址，例如 2001:DB8:55::/32
10. 对于 **Peer Address**（对端地址），使用与本地地址相同的地址系列（IPv4 或 IPv6）输入对等设备的 **IP** 地址，例如 2001:DB8:58::/32。
11. 选择 **Advanced**（高级）。
12. （可选）**Enable Sender Side Loop Detection**（启用发送端循环检测）。启用发送端循环检测后，防火墙在更新中发送路由之前检查其 FIB 中路由的 AS_PATH 属性，以确保对端 AS 编号不在 AS_PATH 列表中。如果对端 AS 编号在 AS_PATH 列表中，则防火墙会将其删除以防止循环
13. 单击 **OK**（确定）。

STEP 2 | （可选）创建静态路由并将其安装在单播路由表中，因为您希望该路由仅用于单播。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择正在配置的虚拟路由器。
2. 选择 **Static Routes**（静态路由），选择 **IPv4** 或 **IPv6**，并 **Add**（添加）路由。
3. 输入静态路由的 **Name**（名称）。
4. 基于您的选择（IPv4 或 IPv6）输入 IPv4 或 IPv6 **Destination**（目标）前缀和子网掩码。
5. 选择出口 **Interface**（接口）。


© 2019 Palo Alto Networks, Inc.

6. 选择 **Next Hop**（下一个跃点）作为 **IPv6 Address**（**IPv6** 地址）（或在选择 IPv4 时作为 **IP Address**（**IP** 地址）），并输入要向此静态路由直接传递多播通信的下一个跃点的地址。
7. 输入 **Admin Distance**（管理距离）。
8. 输入 **Metric**（指标）。
9. 对于 **Route Table**（路由表），请选择 **Unicast**（单播）。
10. 单击 **OK**（确定）。

STEP 3 | 提交配置。

单击 **Commit**（提交）。

STEP 4 | 查看单播或多播路由表。

1. 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。
2. 在虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
3. 选择 **Routing**（路由）> **Route Table**（路由表）。
4. 对于 **Route Table**（路由表），请选择 **Unicast**（单播）或 **Multicast**（多播），仅显示那些路由。
5. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 Only**（仅 **IPv4**）、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），仅显示该地址系列中的路由。



不支持选择 *IPv6 Only*（仅 *IPv6*）的 *Multicast*（多播）。

STEP 5 | 查看转发表。

1. 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。
2. 在虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
3. 选择 **Routing**（路由）> **Forwarding Table**（转发表）。
4. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 Only**（仅 **IPv4**）、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），仅显示该地址系列中的路由。

STEP 6 | 查看 BGP RIB 表。

1. 查看 BGP 本地 RIB，其中显示了防火墙用于路由 BGP 数据包的 BGP 路由。
    1. 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。
    2. 在虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
    3. 选择 **BGP** > **Local RIB**（本地 **RIB**）。
    4. 对于 **Route Table**（路由表），请选择 **Unicast**（单播）或 **Multicast**（多播），仅显示那些路由。
    5. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 Only**（仅 **IPv4**）、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），仅显示该地址系列中的路由。

    不支持选择 *IPv6 Only*（仅 *IPv6*）的 *Multicast*（多播）。
2. 查看 BGP RIB 输出表，其中显示了防火墙发送给 BGP 邻居的路由。
    1. 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。
    2. 在虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
    3. 选择 **BGP** > **RIB Out**（**RIB** 输出）。
    4. 对于 **Route Table**（路由表），请选择 **Unicast**（单播）或 **Multicast**（多播），仅显示那些路由。
    5. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 Only**（仅 **IPv4**）、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），仅显示该地址系列中的路由。



© 2019 Palo Alto Networks, Inc.

不支持选择 *IPv6 Only*（仅 *IPv6*）的 *Multicast*（多播）。

## 为 IPv4 多播配置带 MP-BGP 的 BGP 对等设备

如果您希望 BGP 对等设备能够在 BGP 更新中了解和传递 IPv4 多播路由，则在配置 BGP 后，为 IPv4 多播配置带 MP-BGP 的 BGP 对等设备。您可以将单播与多播通信分开，或者采用 MP-BGP 中列出的功能，仅使用单播或多播路由表中的路由或两个表中的路由。

若想仅支持多播通信，则必须使用筛选器来消除单播通信。

防火墙不支持多播通信的 ECMP。

STEP 1 | 启用 MP-BGP 扩展，使 BGP 对等设备可以与 IPv4 多播路由交换。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择正在配置的虚拟路由器。
2. 选择 **BGP**。
3. 选择 **Peer Group**（对等组），选择对等组和 BGP 对等设备。
4. 选择 **Addressing**（寻址）。
5. 选择 **Enable MP-BGP Extensions**（启用 **MP-BGP** 扩展）。
6. 对于 **Address Family Type**（地址系列类型），请选择 **IPv4**。
7. 对于 **Subsequent Address Family**（随后地址系列），选择 **Unicast**（单播），然后再选择 **Multicast**（多播）。
8. 单击 **OK**（确定）。

STEP 2 | （可选）创建 IPv4 静态路由，并将其仅安装在多播路由表中。

您可以将 BGP 对等设备的多播通信直接传递到特定的下一个跃点，如 MP-BGP 中的拓扑结构所示。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择正在配置的虚拟路由器。
2. 选择 **Static Routes**（静态路由）> **IPv4**，并为该路由 **Add**（添加）一个 **Name**（名称）。
3. 输入 IPv4 **Destination**（目标）前缀和子网掩码。
4. 选择出口 **Interface**（接口）。
5. 选择 **Next Hop**（下一个跃点）作为 **IP Address**（**IP** 地址），并输入要向此静态路由直接传递多播通信的下一个跃点的 IP 地址。
6. 输入 **Admin Distance**（管理距离）。
7. 输入 **Metric**（指标）。
8. 对于 **Route Table**（路由表），请选择 **Multicast**（多播）。
9. 单击 **OK**（确定）。

STEP 3 | 提交配置。

单击 **Commit**（提交）。

STEP 4 | 查看路由表。

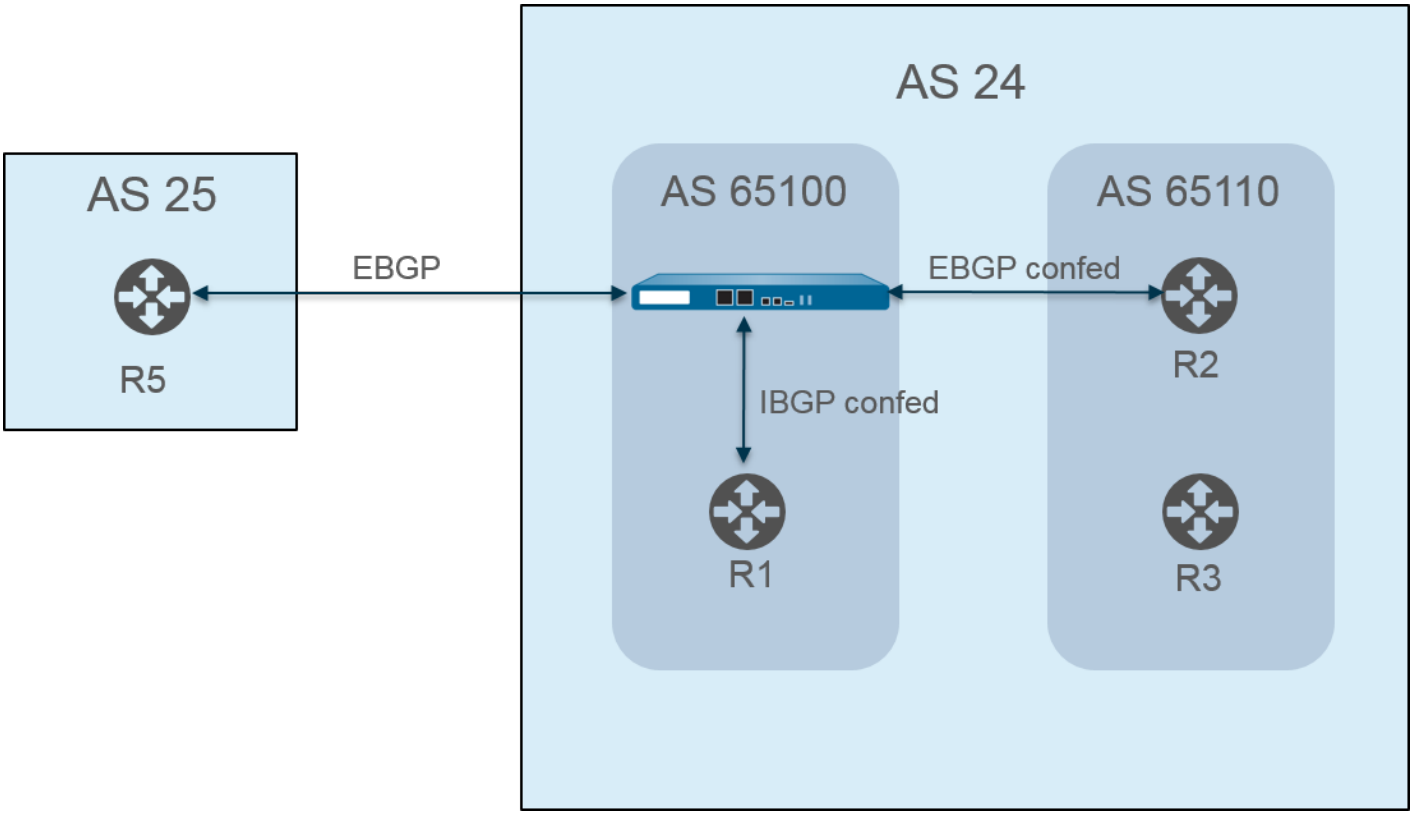
1. 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。
2. 在虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
3. 选择 **Routing**（路由）> **Route Table**（路由表）。
4. 对于 **Route Table**（路由表），请选择 **Unicast**（单播）或 **Multicast**（多播），仅显示那些路由。
5. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 Only**（仅 **IPv4**）、**IPv6 Only**（仅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），仅显示该地址系列中的路由。

STEP 5 | 要查看转发表、BGP 本地 RIB 或 BGP RIB 输出表，请参阅为 IPv4 或 IPv6 单播配置带 MP-BGP 的 BGP 对等设备。


© 2019 Palo Alto Networks, Inc.

# BGP 联合

BGP 联合提供了一种将自治系统 (AS) 划分为两个或多个子自治系统 (sub-AS)，以减轻 IBGP 全网状结构要求造成的负担。子自治系统内的防火墙（或其他路由设备）仍必须拥有一个带相同子自治系统内其他防火墙的 iBGP 全网状结构。您需要实现子自治系统之间的 BGP 对等操作，以便在主 AS 内进行完整的连接。子自治系统内彼此对等的防火墙形成 IBGP 联合对等。与不同子自治系统内防火墙对等的一个子自治系统内的防火墙形成 IBGP 联合对等。来自已连接的不同自治系统的两个防火墙形成 EBGP 对等体。




自治系统使用公共（全局分配的）AS 编号进行标识，例如上图中的 AS24 和 AS25。在 PAN-OS 环境中，您可以为每个子自治系统分配一个唯一的“联合会员 AS”编号，这也是仅在 AS 内可见的专用编号。在该图中，联合编号为 AS 65100 和 AS 65110。（自治系统 (AS) RFC6996 保留以供专用，表示 IANA 将 AS 编号 64512-65534 保留供专用。）

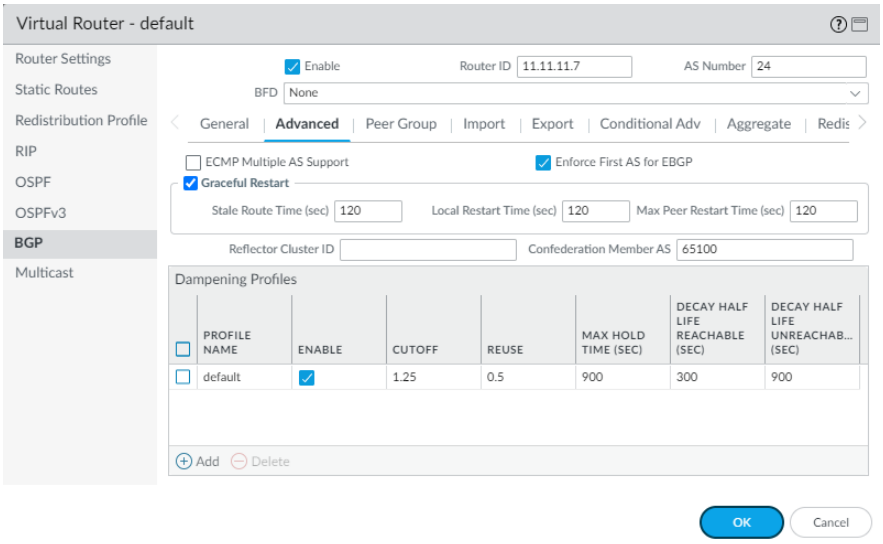
子自治系统联合在 AS 内看起来就像互为完整的自治系统。但是，当防火墙发送 AS 路径至 EBGP 对等体后，仅 AS 公用编号出现在 AS 路径中，不会包含子自治系统（联合成员 AS）专用编号。

BGP 对等操作发生在防火墙和 R2 之间。图中的防火墙具有以下相关配置设置：

- AS 编号—24
- 联合成员 AS — 65100
- 对等类型 —EBGP 联合
- 对等 AS — 65110



© 2019 Palo Alto Networks, Inc.




AS 65110 中的路由器 2 (R2) 配置如下：

- AS 编号—24
- 联合成员 AS—65110
- 对等类型 —EBGP 联合
- 对等 AS—65100

BGP 对等操作也出现在防火墙和 R1 之间。防火墙具有以下额外配置：

- AS 编号—24
- 联合成员 AS — 65100
- 对等类型 —IBGP 联合
- 对等 AS — 65110

R1 配置如下：

- AS 编号—24
- 联合成员 AS—65110
- 对等类型 —IBGP 联合
- 对等 AS—65100

BGP 对等操作出现在防火墙和 R5 之间。防火墙具有以下额外配置：

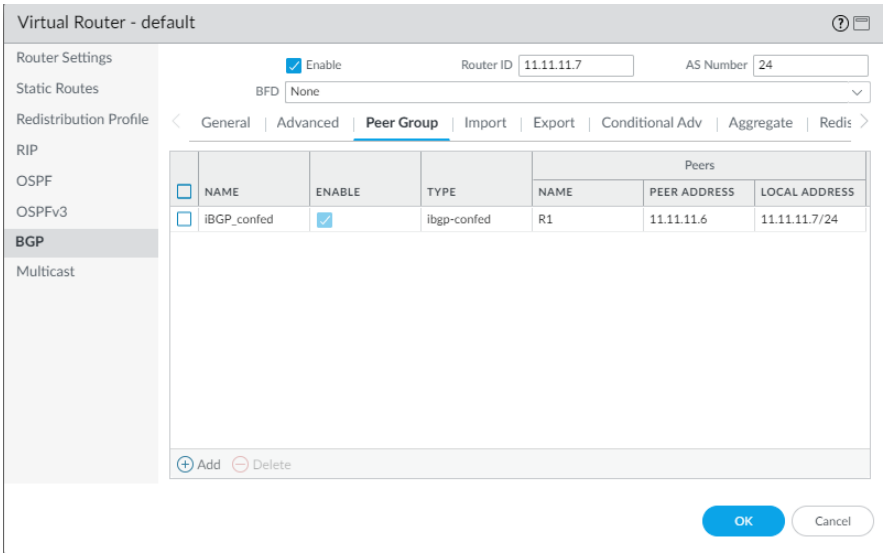
- AS 编号—24
- 联合成员 AS — 65100
- 对等类型 —EBGP
- 对等 AS — 25

R5 配置如下：

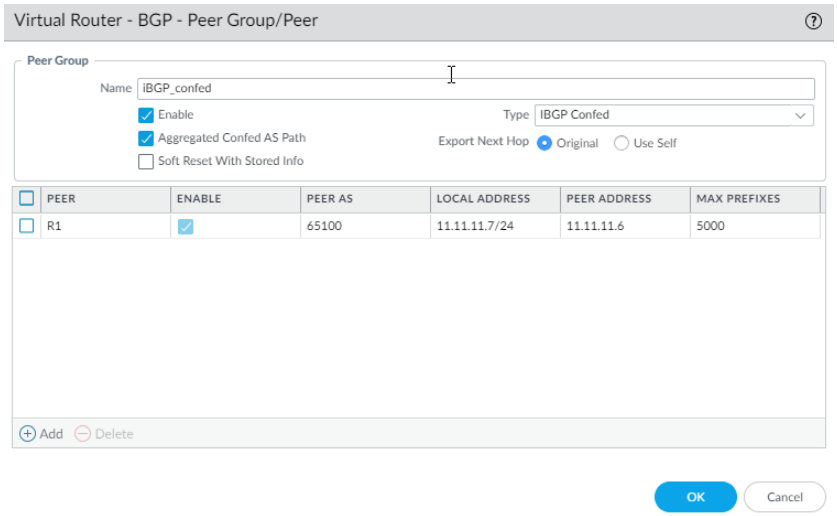
- AS — 25
- 对等类型 —EBGP
- 对等 AS — 24

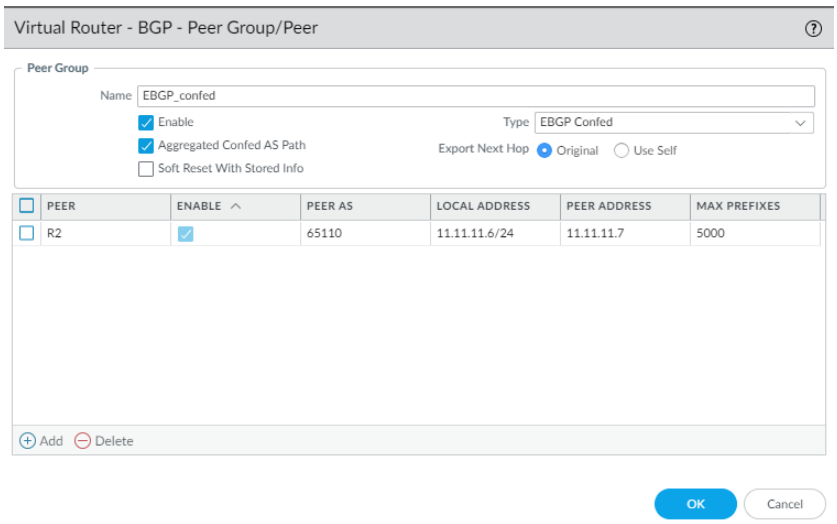
防火墙配置为与 R1、R2 和 R5 对等后，其对等体出现在 **Peer Group**（对等组）选项卡上：


© 2019 Palo Alto Networks, Inc.



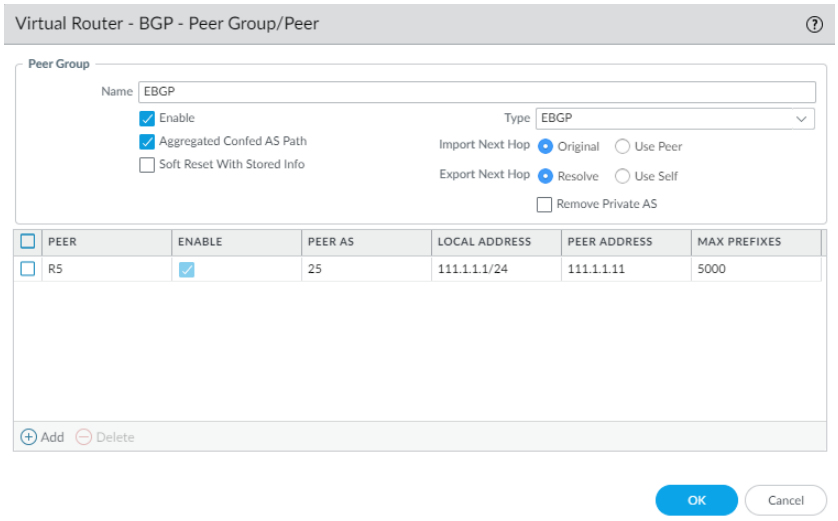

防火墙显示 R1、R2 和 R5 对等体：



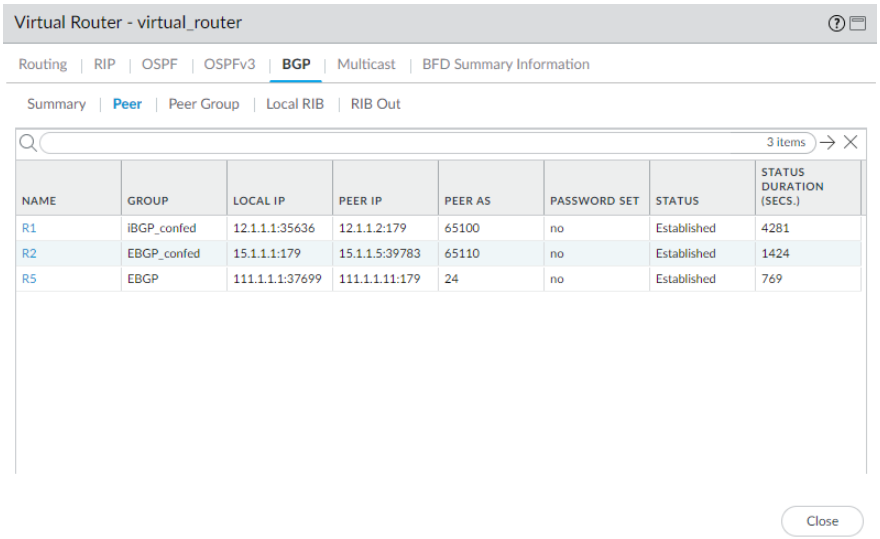






© 2019 Palo Alto Networks, Inc.

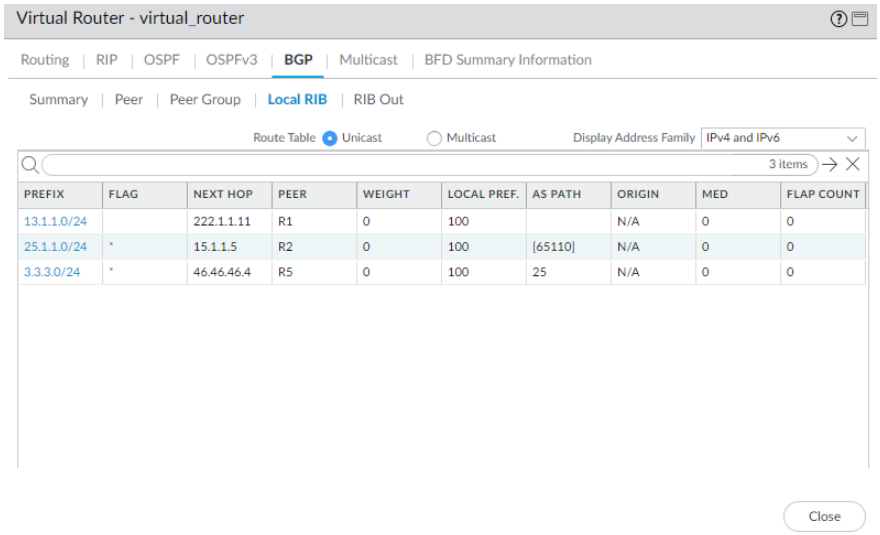



要验证是否已建立从防火墙到对等体的路由，请在虚拟路由器屏幕上选择 **More Runtime Stats**（更多运行时统计数据），然后选择 **Peer**（对等设备）选项卡。

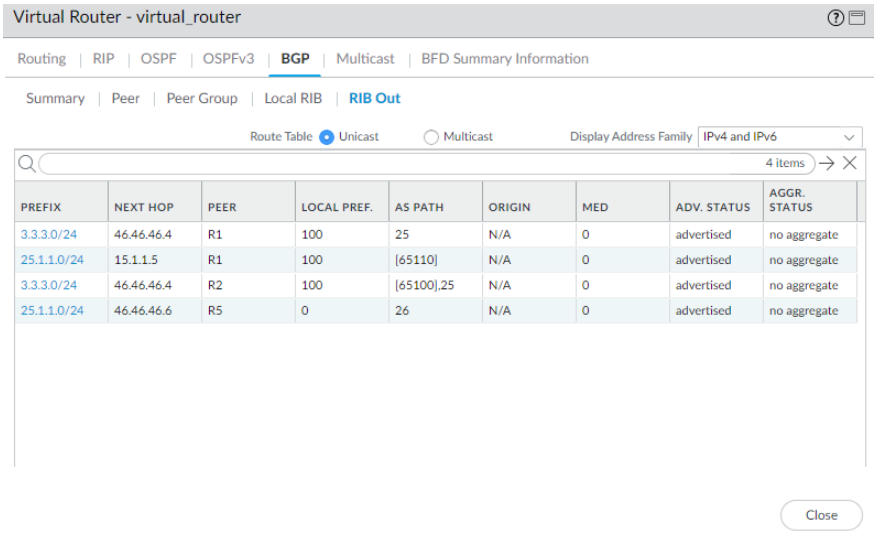



选择 **Local RIB**（本地 **RIB**）选项卡以查看有关路由信息库 (RIB) 中存储的路由信息。


© 2019 Palo Alto Networks, Inc.




然后选择 **RIB Out**（**RIB** 输出）选项卡。






© 2019 Palo Alto Networks, Inc.

# IP 多播

IP 多播是一组协议，网络设备使用这组协议通过一次传输（而非单播流量到多个接收器）的方式发送多个 IP 数据报到一组相关接收器，从而节省带宽。IP 多播适用于从一个或多个源到多个接收器之间的通信，例如音频或视频流、IPTV、视频会议、以及新闻和财务报告等其他通信分发。

多播地址标识了一组想要接收前往该地址流量的接收器。不得使用为特殊用途保留的多播地址，例如，从 224.0.0.0 到 224.0.0.255 或从 239.0.0.0 到 239.255.255.255。多播流量使用 UDP（不会重新发送丢失的数据包）。

Palo Alto Networks® 防火墙支持在防火墙上配置用于虚拟路由器的第三层接口上的 IP 多播和协议无关组播 (PIM)。

对于多播路由，第三层接口类型可以是以太网、聚合以太网 (AE)、VLAN、回环或隧道。接口组允许您使用相同的 Internet 组管理协议 (IGMP) 和 PIM 参数一次性配置具有相同组权限的多个防火墙接口（多播组允许接收任何源或仅接收特定源的流量）。一个接口只能属于一个接口组。

防火墙支持 IPv4 多播，但不支持 IPv6 多播。此外，防火墙也不支持 PIM 密集模式 (PIM-DM)、IGMP 代理、IGMP 静态加入、Anycast RP、GRE、或第二层或虚拟线路接口类型的多播配置。但是，虚拟线路接口可以传递多播数据包。此外，第二层接口可以切换不同 VLAN 之间的第三层 IPv4 多播数据包，防火墙将使用出口接口的 VLAN ID 重新标记 VLAN ID。

必须为虚拟路由器使用多播，为入口和出口接口启用 PIM，以便接口接收或转发多播数据包。除 PIM 外，还必须在面向接收器的出口接口上启用 IGMP。必须配置安全策略规则，允许 IP 多播流量前往名为 **multicast**（多播）的预定义第三层目标区域，或是 **any**（任何）目标区域。

- IGMP
- PIM
- 配置 IP 多播
- 查看 IP 多播信息

## IGMP

Internet 组管理协议(IGMP)是一种 IPv4 协议。多播接收器可使用该协议与 Palo Alto Networks® 防火墙上的接口通信，防火墙可使用该协议跟踪多播组的成员关系。当主机想要接收多播流量时，实施 IGMP 可发送 IGMP 成员关系报告消息，反过来，接收路由器发送 PIM 加入消息至主机想要加入的组的多播组地址。然后，在同一物理接口上的启动了 IGMP 的路由器（以太网分段等）使用 PIM 与其他启用了 IGMP 的路由器通信，以确定从源到相应接收器的路径。

仅启用面向多播接收器的接口上的 IGMP。接收器只能是远离虚拟路由器的一个第三层跃点。IGMP 消息是一端拥有 TTL 值的第二层消息，因此，不能通过 LAN 发出。

配置 IP 多播时，指定接口是否使用 IGMP 版本 1、IGMP 版本 2 或 IGMP 版本 3。您可以实施 IP 路由器警报选项 RFC 2113，这样，使用 IGMPv2 或 IGMPv3 的传入的 IGMP 数据包都具有 IP 路由器警报选项。

默认情况下，接口接收所有多播组的 IGMP 成员关系报告。可以配置多播组权限，以控制虚拟路由器从任何源（任何源多播或 ASM）接收成员关系报告的组，通常是 PIM 稀疏模式 (PIM-SM)。还可以指定虚拟路由器从特定源接收成员关系报告的组（PIM 特定源多播 [PIM-SSM]）。如果为 ASM 或 SSM 组指定权限，虚拟路由器拒绝来自其他组的成员关系报告。接口必须使用 IGMPv3 以传递 PIM-SSM 流量。

您可以指定 IGMP 可同时为接口处理的最大源数和最大多播组数。

虚拟路由器定期将 IGMP 查询多播至多播组的所有接收器。通过用于确定接收器的 IGMP 成员关系报告对 IGMP 查询做出响应的接收器仍想接收该组的多播流量。虚拟路由器仍保留一个包含接收器的多播组列表；只有当接收器关闭了与该组连接的多播分发树后，虚拟路由器才会将接口外的多播数据包转发至下一个跃点。虚拟路由器不会准确跟踪加入组的接收器。子网上只有一个路由器对 IGMP 查询做出响应，即 IGMP 查询器 — 具有最低 IP 地址的路由器。


© 2019 Palo Alto Networks, Inc.

可以配置具有 IGMP 查询间隔的接口，以及防火墙对查询做出响应的时间量（最大查询响应时间）。防火墙接收来自接收器的 IGMP 离开消息以离开组时，虚拟路由器检查接收离开消息的接口是否已通过立即离开选项配置。若没有立即离开选项，虚拟路由器发送一个查询，以确定是否仍存在该组的接收器成员。最后成员查询间隔指定该组用于响应并确认其是否仍想要该组的多播流量的任何剩余接收器所允许的秒数。

接口支持 IGMP 稳健性变量。可对此变量进行调整，以便防火墙随后对组成员关系间隔、其他查询器存在间隔、启动查询计数和最后成员查询计数进行调整。较高的稳健性变量可以容纳可能会丢弃数据包的子网。

查看 IP 多播信息以查看启动了 IGMP 的接口、IGMP 版本、查询器地址、稳健性设置、多播组数和源数限制、以及接口是否配置为立即离开。还可以查看接口所属的多播组以及其他 IGMP 成员关系信息。

# PIM

IP 多播使用路由器之间的协议无关组播 (PIM) 路由协议确定多播数据包从源到接收器（多播组成员）之间的分发树上的路径。Palo Alto Networks® 防火墙支持 PIM 稀疏模式 (PIM-SM) (RFC 4601)、PIM 任何源多播 (ASM)（有时也称为 PIM 稀疏模式）、以及 PIM 特定源多播 (SSM)。在 PIM-SM 中，源不会转发多播流量，直至属于多播组的接收器（用户）要求源发送流量。当主机想要接收多播流量时，实施 IGMP 可发送 IGMP 成员关系报告消息，然后，接收路由器发送 PIM 加入消息至其想要加入的组的多播组地址。

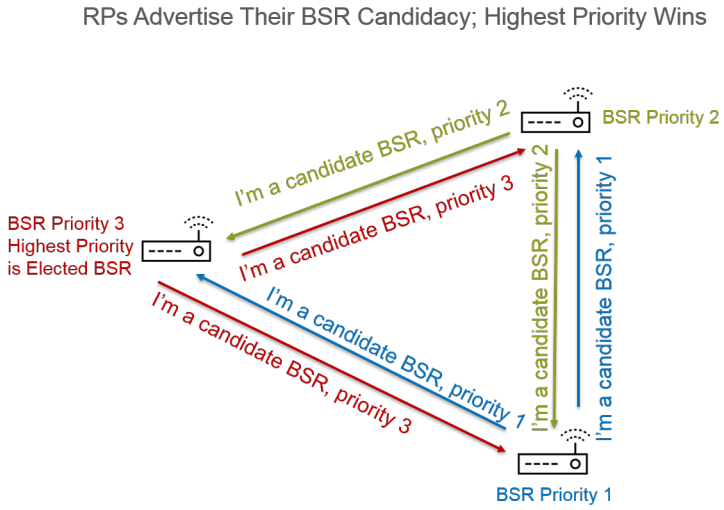
- 在 **ASM** 中，接收器使用 IGMP 请求多播组地址的流量；任何源都可能产生此流量。因此，接收器不一定非要知道发件人，接收器可以接收其不感兴趣的多播流量。
- 在 **SSM** (RFC 4607)中，接收器使用 IGMP 请求一个或多个特定源的流量到多播组地址。接收器知道收件人的 IP 地址，仅接收其想要接收的多播流量。SSM 要求 IGMPv3。您可以覆盖默认的 SSM 地址空间，即 232.0.0.0/8。

在 Palo Alto Networks® 防火墙上配置 IP 多播时，即使是在面向接收器的接口，也必须启用接口的 PIM 以转发多播流量。这与仅在面向接收器的接口上启用的 IGMP 不同。

ASM 要求集合点 (RP)，这是一个位于共享分发树连接点或根部的路由器。多播域的 RP 可充当所有多播组成员发送其加入消息的单个点。这一行为可降低路由回环的可能性，否则，如果组成员发送其加入消息至多个路由器，则会发生路由回环。（因为特定源多播使用最短路径树，因此，SSM 无需 RP，进而不需要 RP。）

在 ASM 环境中，虚拟路由器可采用两种方式确定哪一个路由器是多播组的 RP：

- 静态 **RP** 到组映射 — 在防火墙上配置充当多播组 RP 的虚拟路由器。您可以通过配置静态 RP 地址配置本地 RP，也可以通过指定本地 RP 是待选 RP，并基于最低优先级值动态选择 RP 的方式进行配置。此外，还可以为本地 RP 未覆盖的不同组地址范围静态配置一个或多个外部 RP，这有助于您实现多播流量的负载均衡，确保没有一个 RP 过载。
- 自举路由器 **(BSR)** — (RFC 5059) — 定义 BSR 角色。首先，BSR 待选相互宣传其优先级，然后具有最高优先级的待选被选为 BSR，如下图所示：

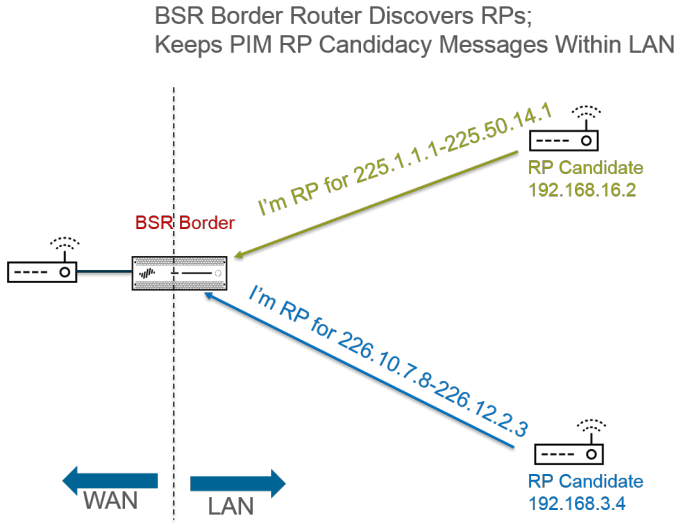





© 2019 Palo Alto Networks, Inc.

接下来，当待选 RP 周期性地将 BSR 消息单播到包含其 IP 地址的 BSR 以及将充当 RP 的多播组范围时，BSR 发现 RP。您可以将本地虚拟路由器配置为待选 RP，在这种情况下，虚拟路由器会宣布其用于特定多播组或组的 RP 待选。BSR 发送 RP 信息到 PIM 域中其他 RP。

为接口配置 PIM 时，可以在防火墙上的接口位于远离企业网络的企业边界时选择 BSR 边界。BSR 边界设置阻止防火墙在 LAN 之外发送 RP 待选 BSR 消息。在下图中，为面向 LAN 的接口启用 BSR 边界，并且此接口拥有最高优先级。如果虚拟路由器拥有静态 RP 和动态 RP（从 BSR 获取），则可以指定在配置本地静态 RP 时，静态 RP 是否可以覆盖为组获取的 RP。




为了便于 PIM 稀疏模式通知 RP 其拥有发送至共享树的流量，RP 必须知道源。当指定路由器 (DR)在 PIM 注册消息中封装来自主机的第一个数据包，并将此数据包单播到期本地网络的 RP 时，主机通知 RP 它正在发送流量到多播组地址。DR 还会将剪枝消息从接收器转发到 RP。RP 保留正发往多播组的源 IP 地址列表，此 RP 可从源转发多播数据包。

为什么 PIM 域中的路由器需要 DR？当路由器发送 PIM 加入消息到交换机时，两个路由器可以接收此消息，并将其转发到同一个 RP，从而导致冗余流量和带宽浪费。要阻止不必要的流量，PIM 路由器选择 DR（具有最高 IP 地址的路由器），只有 DR 转发加入消息到 RP。或者，可以分配 DR 优先级给接口组，该优先级优先于 IP 地址比较。请注意，DR 正在转发（单播）PIM 消息；而不是多播 IP 多播数据包。

您可以指定接口组将运行用于与虚拟路由器对等的 PIM 邻居（路由器）的 IP 地址。默认情况下，启动了 PIM 的路由器可以是 PIM 邻居，但限制邻居的选项可提供保护 PIM 环境中虚拟路由器的一步。

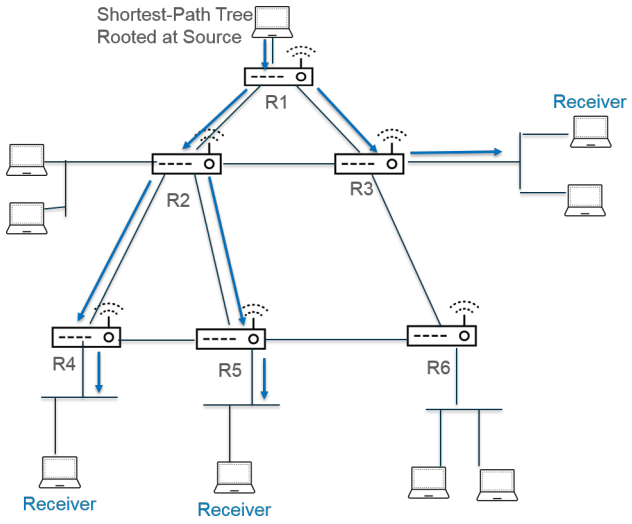
- 最短路径树 (SPT) 和共享树
- PIM 断言机制
- 反向路径转发

## 最短路径树 *(SPT)* 和共享树

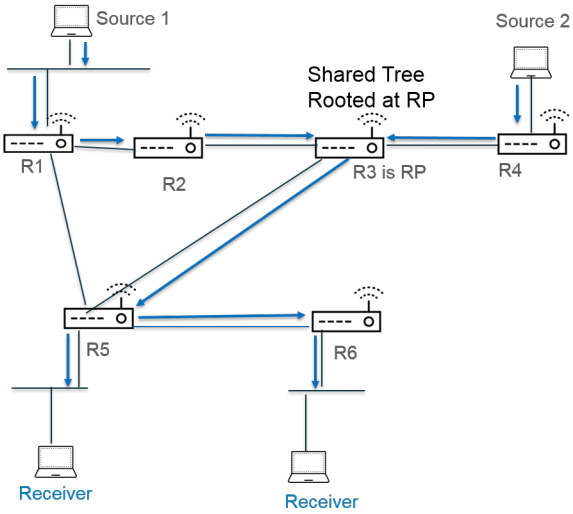
接收器加入多播组后，多路访问网络中的路由器构建发送至组内每个接收器所需的路由路径。每个发送至多播组的 IP 数据包均被分发（转发）给所有成员。路由路径构成一种用于多播数据包的分发树类型。多播分发树的目的是在当数据包到达路径分散点且路由器必须通过多个路径将数据包发送至所有组成员时，用于路由器复制多播数据包，但分发树必须避免通过其中没有所需接收器存在的路径发送数据包。分发树分以下几种：

- 源树 — 通过网络从多播源（树根）到多播组内接收器的一条路径。源树是多播数据包从源到接收器采用的最短路径，因此，也称为最短路径树 **(SPT)**。发送方和接收方注释为源和多播组对，缩写为 (S, G)；例如 (192.168.1.1, 225.9.2.6)。下图说明了从源到三个接收器的三个最短路径树。


© 2019 Palo Alto Networks, Inc.




- 共享树 — 以 RP，而非多播源为根的一条路径。共享树也称为 RP 树或 RPT。路由器将来自各种源的多播数据包转发至 RP，然后 RP 将此数据包转发到共享树。因为属于多播组的所有源均共享来自 RP 相同的分发树，因此，共享树注释为 (*, G)，使用通配符作为源。共享树注释的一个示例是 (*, 226.3.1.5)。下图说明了从 RP 根到接收器的共享树。




Source-Specific Multicast（特定源多播）(SSM) 使用源树分发。当您配置 IP 多播以使用任何源多播 (ASM) 时，您可以通过设定该组的 SPT 阈值来指定 Palo Alto Networks® 防火墙上虚拟路由器使用的分发树，以便将多播数据包传递到组：

- 默认情况下，虚拟路由器在接收到组或前缀的第一个多播数据包时，将多播路由从共享树切换到 SPT（**SPT Threshold**（**SPT** 阈值）设置为 0）。
- 当在任何时间段内通过任何接口到达指定多播组或前缀的数据包内的千比特总数达到配置数量时，则可以配置虚拟路由器以切换到 SPT。
- 可以将虚拟路由器配置为永不会切换至组或前缀的 SPT（它将持续使用共享树）。

SPT 需要更多内存，因此，请根据组的多播流量级别选择您的设置。如果虚拟路由器切换至 SPT，则数据包将从源（而不是 RP）到达，然后虚拟路由器发送剪枝消息到 RP。源通过最短路径树为该组发送随后多播数据包。



© 2019 Palo Alto Networks, Inc.

## *PIM* 断言机制

要防止多路访问网络上的路由器转发相同的多播流量到相同的下一个跃点（可能会导致冗余流量和带宽浪费），PIM 使用断言机制选择用于多路访问网络的单个 PIM 转发器。

如果虚拟路由器从虚拟路由器已关联为数据包中所标识相同 (S,G) 对的传出接口的接口源中接收多播数据包，则意味着这是一个重复的数据包。因此，虚拟路由器发送包含其指标的断言消息到多路访问网络上其他路由器。然后，路由器以这种方式选择 PIM 转发器：

1. PIM 转发器是与多播源管理距离最短的路由器。
2. 如果出现同等最短管理距离，则 PIM 转发器是具有到源的最佳单播路由指标的路由器。
3. 如果出现同等最短管理距离，则 PIM 转发器是具有最高 IP 地址的路由器。

未选中作为 PIM 转发器的路由器将停止向 (S,G) 对中标识的多播组转发流量。

配置 IP 多播时，可以配置虚拟路由器从接口发送 PIM 断言消息的间隔（断言间隔）。查看 IP 多播信息时，**PIM Interface**（**PIM** 接口）选项卡显示接口的断言间隔。

## 反向路径转发

PIM 通过使用虚拟路由器上的路由表将逆向路径转发 (RPF) 用于阻止多播路由回环。虚拟路由器接收到多播数据包时，会在其单播路由表中查找多播数据包的源，并检查与此源 IP 地址相关联的传出接口是否就是数据包到达的接口。如果接口匹配，则虚拟路由器复制此数据包，并将其从接口转发至组内的多播接收器。如果接口不匹配，则虚拟路由器丢弃此数据包。单播路由表基于底层静态路由或您网络使用的内部网关协议 (IGP)，例如 OSPF。

PIM 还使用 RPF 构建到源的最短路径树，一次一个 PIM 路由器跃点。虚拟路由器具有多播源地址，因此，虚拟路由器选择其可能用于转发单播数据包到源的上游 PIM 邻居作为其返回源的下一个跃点。下一个跃点路由器执行同样的操作。

RPF 成功且虚拟路由器在其多播路由信息库 (mRIB) 中具有路由条目后，虚拟路由器在其多播转发信息库（多播转表发或 mFIB）中保留基于源的树条目 (S,G) 和共享树条目 (*,G)。每个条目均包含源 IP 地址、多播组、传入接口（RPF 接口）和传出接口列表。因为最短路径树可以在路由器进行分支，因此一个条目可以使用多个传出接口。路由器必须通过多个接口将数据包转发至不同路径中放置的组接收器。当虚拟路由器使用 mFIB 转发多播数据包时，在尝试匹配 (*,G) 条目之前，必须与 (S,G) 条目匹配。

如果正在将多播源前缀通告给 BGP（使用 IPv4 地址系列和多播随后地址系列配置MP-BGP），则防火墙始终对防火墙在多播随后地址系列中接收到的 BGP 路由执行 RPF 检查。

有关如何查看 mFIB 和 mRIB 条目，请查看 IP 多播信息。请记住，多播路由表 (mRIB) 是一个与单播路由表 (RIB) 完全不同的表。

# 配置 IP 多播

在 Palo Alto Networks® 防火墙上配置虚拟路由器接口后，可接收和转发IP 多播数据包。必须为虚拟路由器启用 IP 多播，在入口和出口接口上配置协议无关多播 (PIM)，并在面向接收器的接口上配置 Internet 组管理协议 (IGMP)。

STEP 1 | 为虚拟路由器启用 IP 多播。

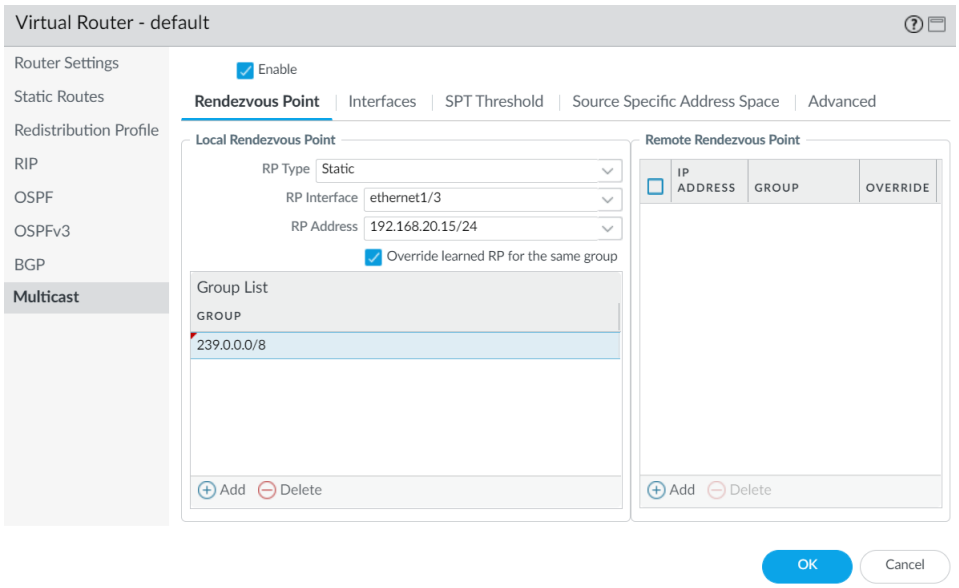
1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **Multicast**（多播），并 **Enable**（启用）IP 多播。

STEP 2 | （仅 ASM）如果虚拟路由器所在的多播域使用任意源多播 (ASM)，则为多播组标识并配置本地和远程集合点 (RP)。

1. 选择 **Rendezvous Point**（集合点）。
2. 选择可以确定如何选择 RP 的本地 **RP Type**（**RP** 类型）（选项包括：**Static**（静态）、**Candidate**（待选）或 **None**（无））：


© 2019 Palo Alto Networks, Inc.

- **Static**（静态）— 建立从 RP 到多播组的静态映射。配置静态 RP 需要在 PIM 域内其他 PIM 路由器上明确配置相同的 RP。
  - 选择 **RP Interface**（**RP** 接口）。有效的接口类型包括第三层、虚拟线路、回环、VLAN、聚合以太网 (AE) 和隧道。
  - 选择 **RP Address**（**RP** 地址）。列表显示的是选中的 RP 接口的 IP 地址。
  - 选择 **Override learned RP for the same group**（覆盖同一组内获取的 **RP**），这样，此静态 RP 将作为 RP，而非选中用于组列表中各组的 RP。
  - **Add**（添加）一个或多个其 RP 充当 RP 的 **Groups**（组）。




- **Candidate**（待选）— 根据优先级建立从 RP 到多播组的动态映射，这样，PIM 域内的各个路由器才能自动选择相同的 RP。
  - 选择待选 RP 的 **RP Interface**（**RP** 接口）。有效的接口类型包括第三层、回环、VLAN、聚合以太网 (AE) 和隧道。
  - 选择待选 RP 的 **RP Address**（**RP** 地址）。列表显示的是选中的 RP 接口的 IP 地址。
  - （可选）更改待选 RP 的 **Priority**（优先级）。防火墙将待选 RP 的优先级与其他待选 RP 的优先级进行比较，以确定哪一个作为指定组的 RP。防火墙选择优先级值最低的待选 RP（范围为 1 到 255；默认为 192）。
  - （可选）更改 **Advertisement Interval (sec)**（通告间隔（秒））（范围为 1 到 26214；默认为 60）。
  - 输入可与 RP 进行通信的多播组的 **Group List**（组列表）。
- **None**（无）— 选择此虚拟路由器是否是一个 RP。

3. **Add**（添加）远程集合点，并输入此远程（外部）RP 的 **IP Address**（**IP** 地址）。
4. **Add**（添加）其指定远程 RP 地址充当 RP 的多播 **Group Addresses**（组地址）。
5. 选择 **Override learned RP for the same group**（覆盖同一组内获取的 **RP**），这样，您静态配置的外部 RP 将作为 RP，而非动态获取（选中）用于组地址列表中各组的 RP。
6. 单击 **OK**（确定）。

STEP 3 | 指定一组共享多播配置的接口（IGMP、PIM 和组权限）。

1. 在 **Interfaces**（接口）选项卡上，**Add**（添加）接口组 **Name**（名称）。
2. 输入 **Description**（说明）。
3. **Add**（添加） **Interface**（接口），并选择属于接口组的一个或多个第三层接口。

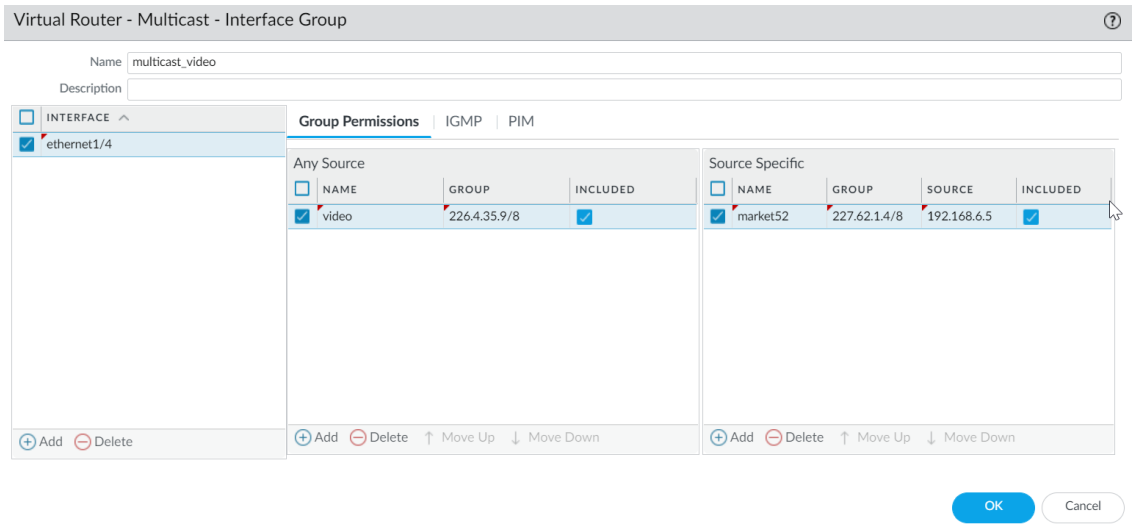


© 2019 Palo Alto Networks, Inc.

STEP 4 | （可选）配置接口组的多播组权限。默认情况下，接口组接受来自各组的 IGMP 成员关系报告和 PIM 加入消息。

1. 选择 **Group Permissions**（组权限）。
2. 要配置此接口组的任何源多播 (ASM)，在任何源窗口中 **Add**（添加）一个 **Name**（名称），以标识可接受来自任何源的 IGMP 成员关系报告和 PIM 加入消息的多播组。
3. 输入可以接收来自这些接口上任何源的多播数据包的多播 **Group**（组）地址或组地址和/或前缀。
4. 选择 **Included**（已包含）以包含接口组内 ASM **Group**（组）地址（默认）。取消选择 **Included**（已包含），以便在测试时从接口组将 ASM 组轻松排除。
5. **Add**（添加）想要从任何源接收多播数据包的其他多播 **Groups**（组）（对于接口组）。
6. 要在此接口组内配置特定源多播 (SSM) 组，在特定源窗口中 **Add**（添加）一个可用于标识多播组和源地址对的 **Name**（名称）。请勿使用已用于任何源多播的名称。（必须使用 IGMPv3 配置 SSM。）
7. 输入想要仅从特定源接收多播数据包（并能接收这些接口上的数据包）的多播 **Group**（组）地址或组地址和/或组前缀。

   指定权限的特定源组是指虚拟路由器必须视为特定于源的组。配置包含已为其配置权限的特定源组的 *Source Specific Address Space*（特定源地址空间）（步骤 9）。
8. 输入多播组可从中接收多播数据包的 **Source**（源）IP 地址。
9. 选择 **Included**（已包含）以包含接口组内的 SSM 组和源地址对（默认）。取消选择 **Included**（已包含），以便在测试时轻松将此对从接口组中排除。
10. **Add**（添加）仅从特定源接收多播数据包的其他多播 **Groups**（组）（对于接口组）。




STEP 5 | 如果接口面向多播接收器，则为接口组配置 IGMP，此时，必须使用 IGMP 加入一个组。

1. 在 **IGMP** 选项卡上 **Enable**（启用）IGMP（默认）。
2. 指定用于接口组内接口的 IGMP 参数：
   - **IGMP Version**（**IGMP** 版本）— **1**、**2** 或**3**（默认）。
   - **Enforce Router-Alert IP Option**（实施路由器警报 **IP** 选项）（默认情况下禁用）— 如果需要使用 IGMPv2 或 IGMPv3 的 IGMP 传入数据包以具有 IP 路由器警报选项，RFC 2113，则选择此选项。
   - **Robustness**（稳健性）— 防火墙用于调整组成员资格间隔、其他查询器存在间隔、启动查询计数以及最后成员查询计数的变量（范围为 1 到 7；默认为 2）。如果此防火墙所在的子网容易丢失数据包，则增加该值。
   - **Max Sources**（最大源数）— IGMP 可以为接口同步处理的最大源数（范围为 1 到 65535；默认为 **unlimited**（无限制））。
   - **Max Groups**（最大组数）— IGMP 可以为接口同步处理的最大组数（范围为 1 到 65535；默认为 **unlimited**（无限制））。


© 2019 Palo Alto Networks, Inc.

- **Query Interval**（查询间隔）— 虚拟路由器发送给接收器以确定该接收器是否仍想要为组接收多播数据包的 IGMP 成员资格查询之间的秒数（范围为 1 到 31744；默认为 125）。
- **Max Query Response Time (sec)**（最大查询响应时间（秒））— 在虚拟路由器决定此接收器不再想要为该组接收多播数据包之前，允许接收器向 IGMP 成员资格查询消息做出响应的最大秒数（范围为 0 到 3714.4；默认为 10）。
- **Last Member Query Interval (sec)**（最后成员查询间隔（秒））— 在接收器发送离开组消息后，允许接收器向虚拟路由器发送的特定于组的查询做出响应的秒数（范围为 0.1 到 3174.4；默认为 1）。
- **Immediate Leave**（立即离开）（默认情况下禁用）— 当多播组内仅有一位成员，且虚拟路由器接收到该组的 IGMP 离开消息时，立即离开设置将导致虚拟路由器立即将多播路由信息库 (mRIB) 和多播转发信息库 (mFIB) 内该组和传出接口删除，而非等待最后成员查询间隔到期。立即离开设置可节省网络资源。如果接口组使用 IGMPv1，则不能选择“立即离开”。

STEP 6 | 为接口组配置 PIM 稀疏模式 (PIM-SM)。

1. 在 **PIM** 选项卡上 **Enable**（启用）PIM （默认启用）。
2. 指定用于接口组内接口的 PIM 参数：
   - **Assert Interval**（断言间隔）— 虚拟路由器在多路访问网络上其他 PIM 路由器选择 PIM 转发器时向其发送的 PIM 断言消息之间的秒数（范围为 0 到 65534；默认为 177）。
   - **Hello Interval**（**Hello** 间隔）— 虚拟路由器从接口组内各个接口向其 PIM 邻居发送的 PIM Hello 消息之间的秒数（范围为 0 到 18000；默认为 30）。
   - **Join Prune Interval**（加入剪枝间隔）— 虚拟路由器向上游发送多播源的 PIM 加入消息（和 PIM 剪枝消息）之间的秒数（范围为 0 到 18000；默认为 60）。
   - **DR Priority**（**DR** 优先级）— 指定路由器 (DR) 优先级用于控制多路访问网络中哪一个路由器将 PIM 加入和剪枝消息转发给 RP（范围为 0 到 429467295；默认为 1）。DR 优先级优先于 IP 地址比较，以选择 DR。
   - **BSR Border**（**BSR** 边界）— 如果接口组内的接口均位于企业级 LAN 边界处布置的 BSR 上的虚拟路由器内，则选择此选项。这将防止 RP 待选 BSR 消息从 LAN 离开。
3. 指定虚拟路由器可从中接受多播数据包的每个路由器的 **IP Address**（**IP** 地址），从而 **Add**（添加）一个或多个 **Permitted PIM Neighbors**（允许的 **PIM** 邻居）。

STEP 7 | 单击 **OK**（确定）以保存接口组设置。

STEP 8 | （可选）根据最短路径树 (SPT) 和共享树更改最短路径树 (SPT) 阈值。

1. 选择 **SPT Threshold**（**SPT** 阈值），并 **Add**（添加）**Multicast Group/Prefix**（多播组/前缀），这是您正在为其指定分发树的多播组或前缀。
2. 指定 **Threshold (kb)**（阈值(kb)）— 路由至从共享树（源自 RP）切换到 SPT 分发的指定多播组或前缀的点：
   - **0 (switch on first data packet)**（**0**（在第一个数据包上切换））（默认）— 当虚拟路由器接收到该组或前缀的第一个数据包时，将为该组或前缀从共享树切换到 SPT。
   - **never (do not switch to spt)**（从不（不会切换到 **spt**））— 虚拟路由器持续使用共享树将数据包转发至该组或前缀。
   - 输入在任何接口和任何时间段内到达用于多播组或前缀的多播数据包的千比特总数，此时，虚拟路由器将更改为此多播组或前缀的 SPT 分发。

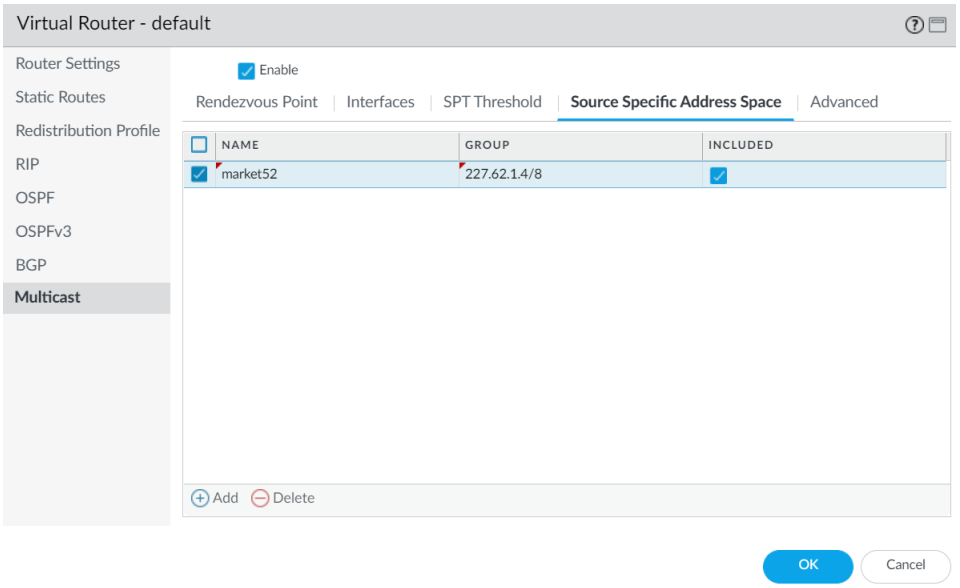
STEP 9 | 标识仅接受特定源的多播数据包的多播组或组和前缀。

1. 选择 **Source Specific Address Space**（特定源地址空间），并 **Add**（添加）空间 **Name**（名称）。
2. 输入带前缀长度的多播 **Group**（组），以标识从特定源接收多播数据包的地址空间。如果虚拟路由器接收用于 SSM 组的多播数据包，但该组未被 **Source Specific Address Space**（特定源地址空间）覆盖，则虚拟路由器丢弃该数据包。
3. 选择 **Included**（已包含）以包含用作多播组地址范围的特定源地址空间，虚拟路由器将从此范围接受源自允许特定源的多播数据包。取消选择 **Included**（已包含）以轻松排除测试用的组地址空间。



© 2019 Palo Alto Networks, Inc.

4. 添加其他特定源地址空间，以包含为其指定 SSM 组权限的所有这些组。




STEP 10 | （可选）在多播组和源之间的会话结束后，更改多播路由仍在 mRIB 中停留的时间长度。

1. 选择 **Advanced**（高级）选项卡。
2. 指定 **Multicast Route Age Out Time (sec)**（多播路由年龄超时（秒））（范围为 210 到 7200；默认为 210）。

STEP 11 | 单击 **OK**（确定）以保存多播配置。

STEP 12 | 创建一个安全策略规则，允许来自目标区域的多播流量。

1. 创建安全策略规则，并在 **Destination**（目标）选项卡上选择 **Destination Zone**（目标区域）为 **multicast**（多播）或 **any**（任何）。**multicast**（多播）区域是符合所有多播流量的预定义第三层区域。**Destination Address**（目标地址）可以是多播组地址。
2. 配置安全策略规则的其余部分。

STEP 13 | （可选）设置路由前启用多播数据包缓存。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 启用 **Multicast Route Setup Buffering**（多播路由设置缓存）（默认为禁用）。如果多播转发表 (mFIB) 中尚不存在相应多播组的条目，则防火墙可以保留多播流中的第一个数据包。**Buffer Size**（缓存大小）控制防火墙从流中缓存的数据包数。在 MFIB 中安装完路由后，防火墙自动将缓存过的第一个数据包转发至接收器。（如果内容服务器可直接连接到防火墙，且多播应用程序无法承担被丢弃流中的第一个数据包，则您仅需启用多播路由设置缓存即可解决问题。）
3. （可选）更改 **Buffer Size**（缓存大小）。缓存大小是指防火墙可以缓存，且直至 mFIB 条目设置后每多播流的数据包数（范围为 1 到 2000；默认为 1000）。防火墙可最多缓存 5000 个数据包（对于所有流）。
4. 单击 **OK**（确定）。

STEP 14 | **Commit**（提交）更改。

STEP 15 | 查看 IP 多播信息 可查看 mRIB 和 mFIB 条目、IGMP 接口设置、IGMP 组成员关系、PIM ASM 和 SSM 模式、到 RP 的组映射、DR 地址、PIM 设置、PIM 邻居等。

STEP 16 | 如果为多播流量配置静态路由，则只能在多播路由表（而非单播路由表）中安装路由，这样，路由才能仅用于多播流量。

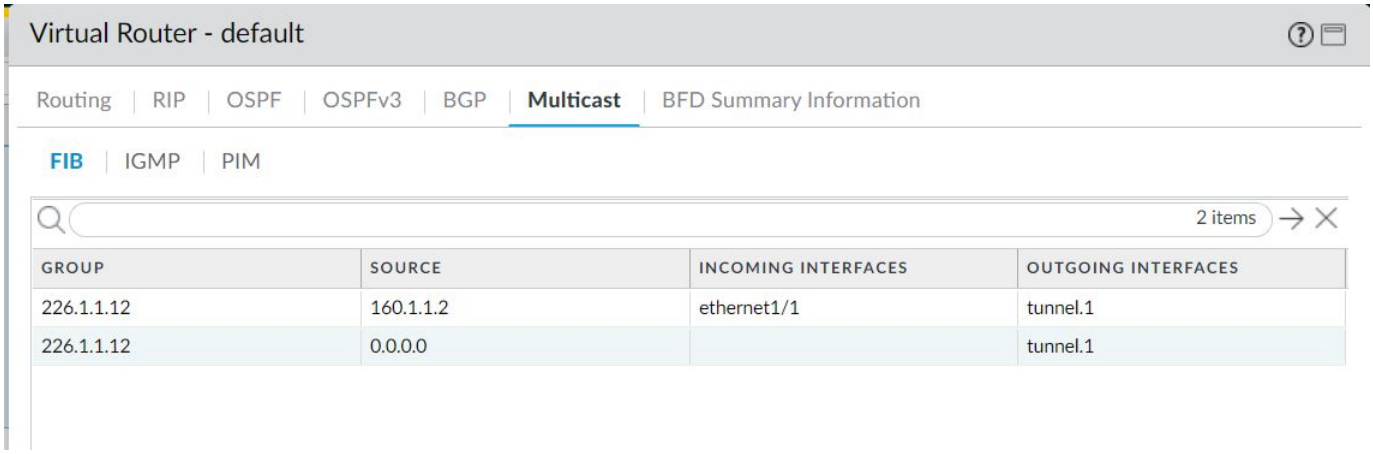

© 2019 Palo Alto Networks, Inc.

STEP 17 | 如果启用 IP 多播，除非您具有一个与逻辑单播拓扑分离的逻辑多播拓扑，否则无须使用 MP-BGP 为 IPv4 多播配置 BGP。只有当您想要在多播随后地址系列中间多播源前缀通告给 BGP 时，才能使用 IPv4 地址系列和多播随后地址系列配置 MP-BGP 扩展。

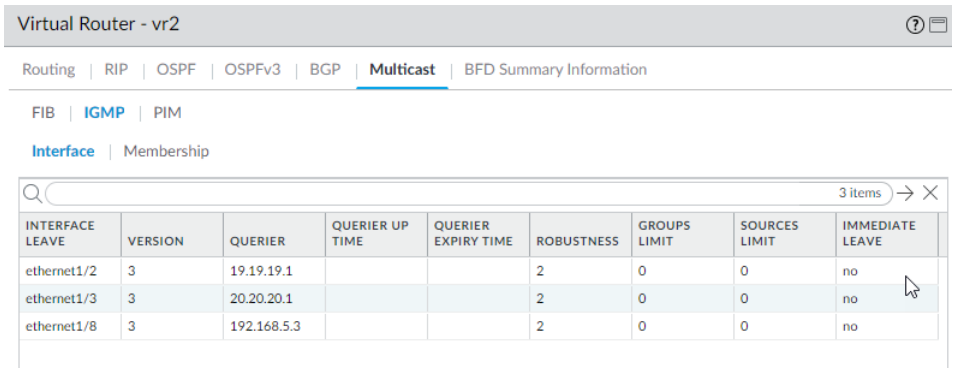
# 查看 IP 多播信息

配置 IP 多播路由后，可查看多播路由、转发条目以及与 IGMP 和 PIM 接口相关的信息。

- 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），再在配置的虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
  1. 选择 **Routing**（路由）> **Route Table**（路由表），然后选择 **Multicast**（多播）单选按钮，以便仅显示多播路由（目标 IP 多播组、指向该组的下一个跃点以及传出接口）。此信息来自 mRIB。
  2. 选择 **Multicast**（多播）> **FIB** 以查看源自 mFIB 的多播路由信息：虚拟路由器所属的多播组、相应的源、传入接口以及指向接收器的传出接口。



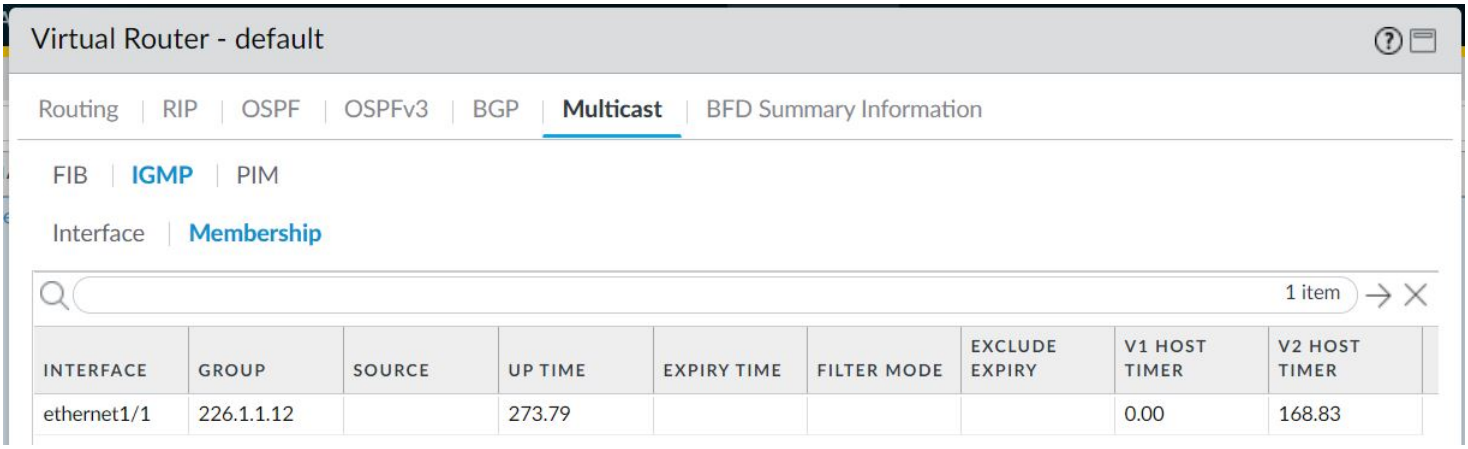

3. 选择 **Multicast**（多播）> **IGMP** > **Interface**（接口）以查看启用了 IGMP 的接口、关联的 IGMP 版本、IGMP 查询器的 IP 地址、查询器启动时间和过期时间、稳健性设置、多播组和源的数量限制、以及接口是否配置为立即离开。



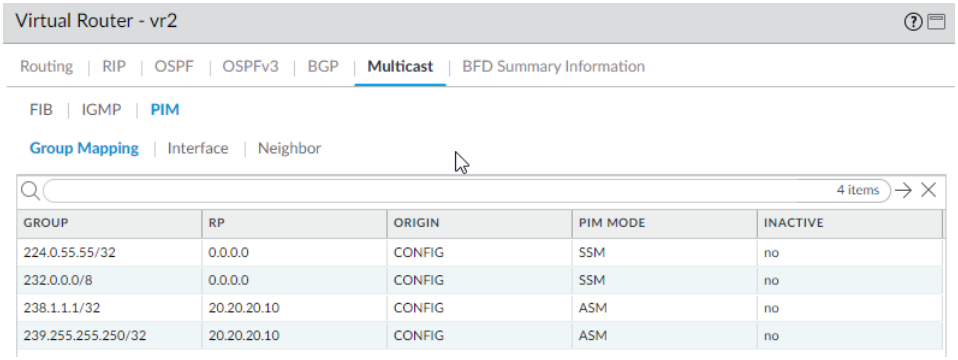

4. 选择 **Multicast**（多播）> **IGMP** > **Membership**（成员关系）以查看基于 IGMP 的接口和其所属的多播组、源以及其他 IGMP 信息。



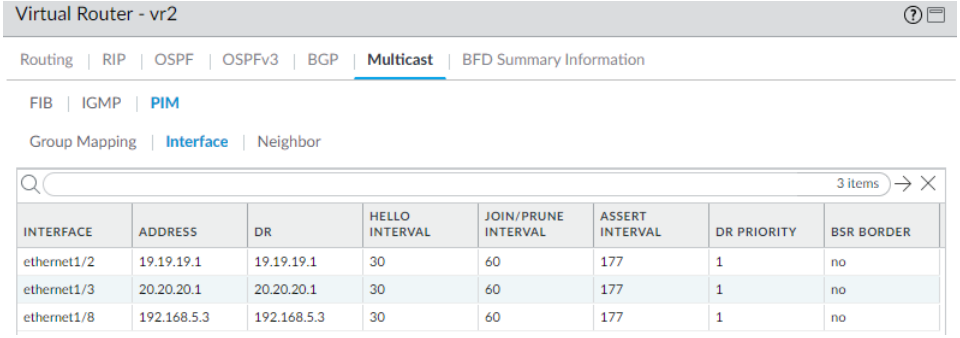
© 2019 Palo Alto Networks, Inc.




5. 选择 **Multicast**（多播）> **PIM** > **Group Mapping**（组映射）以查看映射到 RP 的多播组、RP 映射的来源、组的 PIM 模式（ASM 或 SSM）以及组是否未激活。SSM 模式下的组不会使用 RP，因此，RP 地址显示为 0.0.0.0。默认 SSM 组为 232.0.0.0/8。

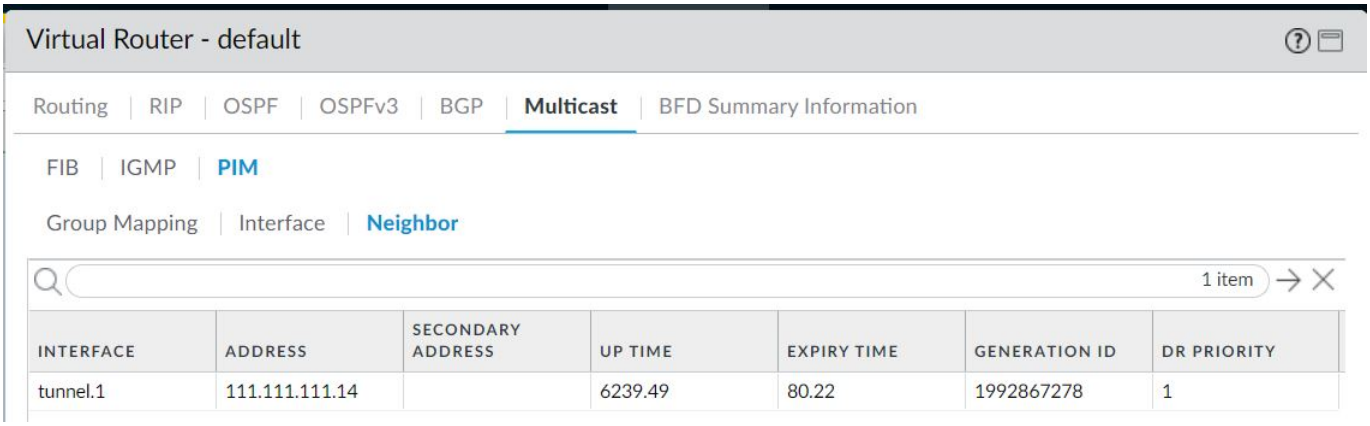



6. 选择 **Multicast**（多播）> **PIM** > **Interface**（接口）以查看接口 DR 的 IP 地址； DR 优先级；呼叫、加入/剪枝和断言间隔；以及接口是否是自举路由器 (BSR)。




7. 选择 **Multicast**（多播）> **PIM** > **Neighbor**（邻居）以查看作为虚拟路由器 PIM 邻居的路由器相关的信息。


© 2019 Palo Alto Networks, Inc.






© 2019 Palo Alto Networks, Inc.

# 路由重新分发

防火墙上的路由重新分发是将防火墙从一个路由协议（或静态或连接路由）获取的路由用于不同路由协议，从而增加网络流量可访问性的过程。若无路由重新分发功能，路由器或虚拟路由器仅与运行相同路由协议的其他路由器通告和共享路由。您可以将 IPv4 或 IPv6 BGP、连接或静态路由重新分发到 OSPF RIB 中，并将 OSPFv3、连接或静态路由重新分发到 BGP RIB 中。

这意味着，例如，您可以将曾经仅用于特定路由器上手动配置的静态路由的特定网络用于 BGP 自治系统或 OSPF 区域。您还可以将本地连接的路由（如私人实验室网络的路由）通告到 BGP 自治系统或 OSPF 区域。

您可能希望让内部 OSPFv3 网络上的用户访问 BGP，以使其能够访问互联网上的设备。在这种情况下，您将 BGP 路由重新分发到 OSPFv3 RIB。

相反，您可能希望让外部用户访问内部网络的某些部分，这样便可通过将 OSPFv3 路由重新分发到 BGP RIB 中，使内部 OSPFv3 网络可用。

STEP 1 | 创建重新分发配置文件。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **Redistribution Profile**（重新分发配置文件）和 **IPv4** 或 **IPv6**，并 **Add**（添加）配置文件。
3. 输入配置文件的 **Name**（名称），以字母数字字符开头，并包含零个或多个下划线 (_)、连字符 (-)、点 (.) 和空格（最多 16 个字符）。
4. 输入配置文件 **Priority**（优先级），范围为 1 - 255。防火墙将路由与配置文件进行匹配，以首先使用具有最高优先级（最低优先级值）的配置文件。优先级较高的规则优于优先级较低的规则。
5. 对于 **Redistribute**（重新分发），请选择以下选项之一：
   - **Redist**（重新分发）— 选择重新分发与此筛选器匹配的路由。
   - **No Redist**（无重新分发）— 选择重新分发与重新分发配置文件匹配的路由，但匹配此筛选器的路由除外。此选项将该配置文件视为指定不会选择用于重新分发的路由的阻止列表。例如，如果有多个用于 BGP 的重新分发配置文件，则可以创建一个 **No Redist**（无重新分发）配置文件，以排除多个前缀，然后排除优先级较低（较高优先级值）的常规重新分发配置文件。两个配置文件组合，优先级较高的配置文件优先。不能仅有 **No Redist**（无重新分发）配置文件；始终需要至少一个 **Redist**（重新分发）配置文件以重新分发路由。
6. 在 **General Filter**（常规筛选器）选项卡上，对于源类型，选择要重新分发的一种或多种类型的路由：
   - **bgp** — 重新分发与配置文件匹配的 BGP 路由。
   - **connect**（连接）— 重新分发与配置文件匹配的连接路由。
   - **ospf**（仅 IPv4）— 重新分发与配置文件匹配的 OSPF 路由。
   - **rip**（仅 IPv4）— 重新分发与配置文件匹配的 RIP 路由。
   - **ospfv3**（仅 IPv6）— 重新分发与配置文件匹配的 OSPFv3 路由。
   - **static**（静态）— 重新分发与配置文件匹配的静态路由。
7. （可选）对于 **Interface**（接口），请 **Add**（添加）一个或多个关联路由的出口接口以匹配重新分发。要删除条目，请单击 **Delete**（删除）。
8. （可选）对于 **Destination**（目标），请 **Add**（添加）一个或多个路由的 IPv4 或 IPv6 目标以匹配重新分发。要删除条目，请单击 **Delete**（删除）。
9. （可选）对于 **Next Hop**（下一个跃点），请 **Add**（添加）一个或多个路由的下一个跃点 IPv4 或 IPv6 地址以匹配重新分发。要删除条目，请单击 **Delete**（删除）。
10. 单击 **OK**（确定）。

STEP 2 | （可选 — 常规筛选器包含 ospf 或 ospfv3 时）创建 OSPF 筛选器，进一步指定要重新分发的 OSPF 或 OSPFv3 路由。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择虚拟路由器。
2. 选择 **Redistribution Profile**（重新分发配置文件）和 **Ipv4** 或 **Ipv6**，然后选择创建的配置文件。


© 2019 Palo Alto Networks, Inc.

3. 选择 **OSPF Filter**（**OSPF** 筛选器）。
4. 对于路径类型，选择一个或多个以下类型的 OSPF 路径以重新分发：**ext-1**、**ext-2**、**inter-area**或**intra-area**。
5. 要指定从中重新分发 OSPF 或 OSPFv3 路由的 **Area**（区域），请以 IP 地址格式 **Add**（添加）区域。
6. 要指定 **Tag**（标记），请以 IP 地址格式 **Add**（添加）标记。
7. 单击 **OK**（确定）。

STEP 3 | （可选 — 常规筛选器包含 bgp 时）创建 bgp 筛选器，进一步指定要重新分发的 bgp 路由。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择虚拟路由器。
2. 选择 **Redistribution Profile**（重新分发配置文件）和 **Ipv4** 或 **Ipv6** ，然后选择创建的配置文件。
3. 选择 **BGP Filter**（**BGP** 筛选器）。
4. 对于 **Community**（社区），**Add**（添加）以从社区列表中选择，例如众所周知的社区：**local-as**、**no-advertise**、**no-export**或**nopeer**。您还可以输入 32 位值，格式为十进制或十六进制或 AS:VAL，其中 AS 和 VAL 的范围为 0 - 65535。最多输入 10 个条目。
5. 对于 **Extended Community**（扩展社区），**Add**（添加）一个 64 位值的扩展社区，格式为十六进制或 TYPE:AS:VAL 或 TYPE:IP:VAL。TYPE 为 16 位；AS 或 IP 为 16 位；VAL 为 32 位。最多输入 5 个条目。
6. 单击 **OK**（确定）。

STEP 4 | 选择要重新分发路由的协议，并设置这些路由的属性。

此任务说明将路由重新分发到 BGP。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择虚拟路由器。
2. 选择 **BGP** > **Redist Rules**（重新分发规则）。
3. 选择 **Allow Redistribute Default Route**（允许重新分发默认路由）以允许防火墙重新分发默认路由。
4. 单击添加。
5. 选择 **Address Family Type**（地址系列类型）：指定放置重新分发路由的路由表的 **IPv4** 或 **IPv6**。
6. 选择创建的重新分发配置文件 **Name**（名称），该配置文件选择要重新分发的路由。
7. **Enable**（启用）重新分发规则。
8. （可选）输入以下防火墙应用于正在重新分发的路由的任何值：
   - **Metric**（跃点数），范围为 1 - 65535。
   - **Set Origin**（设置起点）— 路由的起点：**igp**、**egp**或**incomplete**（未完成）。
   - **Set MED**（设置 **MED**）— MED 值，范围为 0 - 4,294,967,295。
   - **Set Local Preference**（设置本地首选项）— 本地首选项的值，范围为 0 - 4,294,967,295。
   - **Set AS Path Limit**（设置 **AS** 路径限制）— AS_PATH 中自治系统的最大数量，范围为 1 - 255。
   - **Set Community**（设置社区）— 选择或输入格式为十进制或十六进制的 32 位值，或输入格式为 AS:VAL 的值，其中 AS 和 VAL 的范围为 0 - 65525 之间。最多输入 10 个条目。
   - **Set Extended Community**（选择扩展社区）— 选择或输入一个 64 位值的扩展社区，格式为十六进制或 TYPE:AS:VAL 或 TYPE:IP:VAL。TYPE 为 16 位；AS 或 IP 为 16 位；VAL 为 32 位。最多输入 5 个条目。
9. 单击 **OK**（确定）。

STEP 5 | **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# GRE 隧道

通用路由封装 (GRE) 隧道协议是用于封装负载协议的运载协议。GRE 数据包本身被封装在传输协议中（IPv4 或 IPv6）。

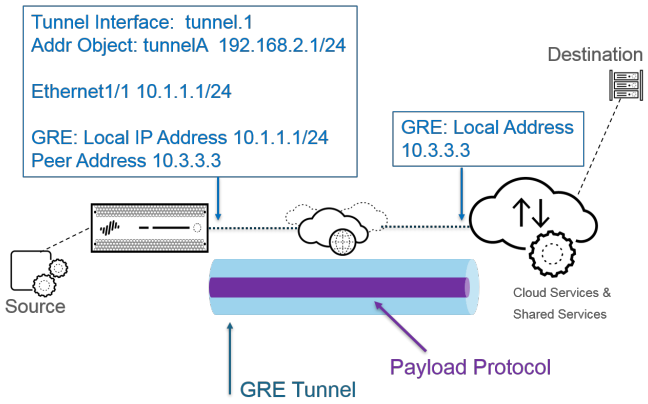
- GRE 隧道概述
- 创建 GRE 隧道

## GRE 隧道概述

通用路由封装 (GRE) 隧道在点对点逻辑链接中连接两个端点（防火墙和另一台设备）。防火墙可终止 GRE 隧道；您可以传送或转发数据包至 GRE 隧道。GRE 隧道易于使用，且通常是点对点连接的隧道协议选项，尤其是在连接云端的服务或合作伙伴网络时。

当您想要将发往某个 IP 地址的数据包导向点对点路径，如基于云的代理或合作伙伴网络时，可创建一个 GRE 隧道。通过此 GRE 隧道的数据包将在发往其目标地址时传输到云服务（通过传输网络，如互联网）。因此，云服务会对数据包实施其服务或策略。

下图是 GRE 隧道在互联网上将防火墙连接至云服务的示例。




为实现更好的性能和避免单点故障，在多个 *GRE* 隧道内分出多个与防火墙的连接，而不是使用单一隧道。每个 *GRE* 隧道需要一个隧道接口。

当防火墙允许数据包通过（根据策略匹配情况）且数据包流出至 GRE 隧道接口时，防火墙会添加 GRE 封装；其不会生成会话。防火墙不会对 GRE 封装流量实施安全策略规则查找；因此，您无需为防火墙封装的 GRE 流量配置安全策略规则。但是，当防火墙接收 GRE 流量时，其将生成会话并将所有策略应用至 GRE IP 标头和封装流量。防火墙将接收的 GRE 数据包按照其他数据包一样处理。因此：

- 如果防火墙在某个接口上接收 GRE 数据包时，该接口具有与隧道接口相关 GRE 隧道相同的区域（例如，隧道 1），则源区域与目标区域一致。默认情况下，允许在一个区域内存在流量（区域内流量），因此也默认允许传入 GRE 流量。
- 然而，如果配置自己的区域内安全策略规则以拒绝此流量，则必须明确允许 GRE 流量。
- 类似的，如果隧道接口相关 GRE 隧道（例如，隧道 1）区域与流入接口区域不同，您必须配置安全策略规则以允许 GRE 流量。

由于防火墙将隧道数据包封装在 GRE 数据包内，GRE 标头的另外 24 个字节自动产生更小的最大分段大小 (MSS)最大传输单元 (MTU)。如果不更改接口的 IPv4 MSS 调整大小，默认情况下，防火墙将使 MTU 减小 64 个字节（IP 标头 40 个字节 + GRE 标头 24 个字节）。这意味着如果默认 MTU 是 1500 个字节，则 MSS 将为 1436 个字节 (1500 - 40 - 24 = 1436)。例如，如果您配置 300 个字节的 MSS 调整大小，则 MSS 仅为 1176 个字节 (1500 - 300 - 24 = 1176)。


© 2019 Palo Alto Networks, Inc.

防火墙不支持将 GRE 或 IPSec 隧道路由到 GRE 隧道，但是，您可以将 GRE 隧道路由到 IPSec 隧道。此外：

- GRE 隧道不支持 QoS。
- 防火墙不支持将单接口同时作为 GRE 隧道端点和解密代理使用。
- GRE 隧道不支持 GRE 隧道端点之间的 NAT。

如果您需要连接其他供应商的网络，我们建议您建立 IPSec 隧道，而不是 *GRE* 隧道；只有当 *GRE* 隧道是此供应商唯一支持的点对点隧道机制时，才能使用 *GRE* 隧道。当远程端点要求 *Add GRE Encapsulation*（添加 *GRE* 封装）时，还可以启用 *GRE over IPSec*。当远程端点要求在 *IPSec* 启用流量前将该流量封装在 *GRE* 隧道中时，添加 *GRE* 封装。例如，某些实施要求在 *IPSec* 对多播流量加密之前，封装多播流量。如果您的环境有此要求，且 *GRE* 隧道和 *IPSec* 隧道共用相同的 *IP* 地址，在设置 *IPSec* 隧道时 *Add GRE Encapsulation*（添加 *GRE* 封装）。

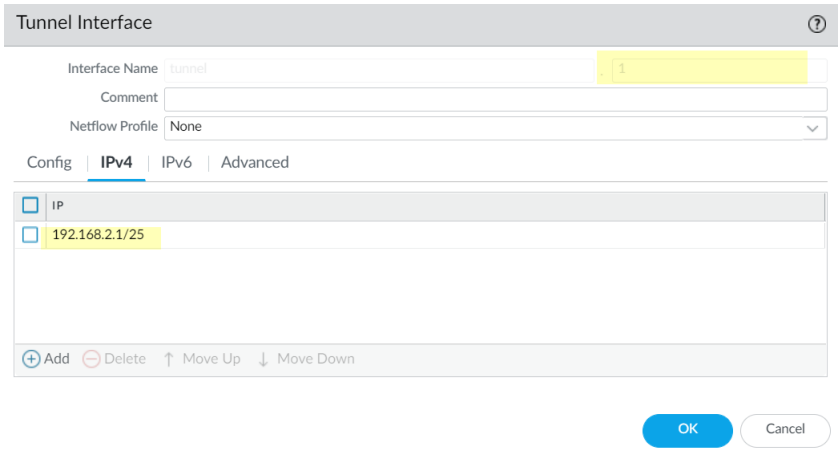
如果您不打算终止防火墙上的 *GRE* 隧道，但想要检查和控制在 *GRE* 隧道内通过防火墙的流量，则不要创建 *GRE* 隧道，而是执行 *GRE* 流量的 隧道内容检测。通过检查隧道内容，您可以对经过防火墙的 *GRE* 流量进行检查并实施策略，而不是创建一个点对点的逻辑链路以引导流量。

# 创建 GRE 隧道

创建通用路由封装 (GRE) 隧道以在点对点逻辑链接中连接两个端点。

STEP 1 | 创建隧道接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道）。
2. **Add**（添加）隧道，并输入隧道 **Interface Name**（接口名称），后跟一个句点和数字（范围为 1-9,999）。例如，`tunnel.1`。
3. 在 **Config**（配置）选项卡上，将隧道接口分配给 **Virtual Router**（虚拟路由器）。
4. 如果防火墙支持多个虚拟系统，将隧道接口分配给 **Virtual System**（虚拟系统）。
5. 将隧道接口分配到 **Security Zone**（安全区域）。




6. 为隧道接口分配一个 IP 地址。（如果想要路由到该隧道或监控隧道端点，必须分配一个 IP 地址。）选择 **IPv4** 或 **IPv6**，或配置两者。

   因为是点对点逻辑链接，因此，该地址和对端设备隧道接口的相应地址应在同一子网上。

   - （IPv4 only（仅限 IPv4））在 **IPv4**选项卡中，**Add**（添加）IPv4 地址，选择一个地址对象，或单击 **New Address**（新地址），然后指定地址 **Type**（类型）并将其输入。例如，输入 `192.168.2.1/25`。



© 2019 Palo Alto Networks, Inc.

- （IPv6 only（仅限 IPv6））在 **IPv6** 选项卡上，选择 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。
  1. 对于 **Interface ID**（接口 **ID**），选择 **EUI-64 (default 64-bit Extended Unique Identifier)**（**(EUI-64)** 默认 64 位扩展唯一标识符）。
  2. **Add**（添加）新 **Address**（地址），选择 IPv6 地址对象，或单击 **New Address**（新地址），并指定地址 **Name**（名称）。选择 **Enable address on interface**（在接口上启用地址），然后单击 **OK**（确定）。
  3. 选择地址 **Type**（类型）并输入 IPv6 地址或 FQDN，然后单击 **OK**（确定）以保存新地址。
  4. 选择 **Enable address on interface**（在接口上启用地址），然后单击 **OK**（确定）。

7. 单击 **OK**（确定）。

STEP 2 | 创建 GRE 隧道以强制数据包遍历特定点对点路径。

1. 选择 **Network**（网络）> **GRE Tunnels**（**GRE** 隧道）并按 **Name**（名称）**Add**（添加）隧道。
2. 选择用作本地 GRE 隧道端点的 **Interface**（接口）（源接口），该接口是以太网接口或子接口、聚合以太网 (AE) 接口、回环接口或 VLAN 接口。
3. 选择成为 **IP** 的 **Local Address**（本地地址），并选择您刚选择的接口 IP 地址。
4. 输入 **Peer Address**（对等地址），即 GRE 隧道对应端点的 IP 地址。
5. 选择您在步骤 1 中创建的 **Tunnel Interface**（隧道接口）。（该接口将标识作为路由出口 **Interface**（接口）的隧道。）
6. 输入封装在 GRE 数据包中的 IP 数据包的 **TTL**（范围为 1 - 255；默认为 64）。
7. 选择 **Copy ToS Header**（复制 **ToS** 标头），将封装数据包的内部 IP 标头中的服务类型 (ToS) 字段复制到其外部 IP 标头中，以保留原始 ToS 信息。如果您的网络使用 QoS 且根据 ToS 位实施 QoS 策略，请选择此选项。




STEP 3 | （最佳实践）为 GRE 隧道启用“保持活动状态”功能。

如果启用 *Keep Alive*（保持活动状态），默认情况下，*GRE* 隧道在 *10* 秒间隔内需要三个无返回的 *keepalive* 数据包（重试）进行关闭，且在 *10* 秒间隔内需要 *5* 个保留计时器间隔进行恢复。

1. 选择 **Keep Alive**（保持活动状态），从而为 GRE 隧道启用 keepalive 功能（默认为禁用）。
2. （可选）设置 GRE 隧道本地端发送至隧道对等的 keepalive 数据包之间的 **Interval (sec)**（间隔（秒））（以秒为单位）。此间隔即为：防火墙在 GRE 隧道恢复之前必须查看到成功的 keepalive 数据包的时间长度乘以 **Hold Timer**（保持计时器）的值（范围为 1 - 50；默认为 10）。若间隔设置过短，会导致很多不需要的 keepalive 数据包出现的您的环境中，这会需要额外的带宽和处理。若间隔设置过长，可能会导致故障延迟，原因是不能立即标识错误情况。


© 2019 Palo Alto Networks, Inc.

3. （可选）输入 **Retry**（重试）设置，这是在防火墙视隧道对端关闭之前，keepalive 数据包尚未返回的间隔数（范围为 1 - 255；默认为 3）。隧道关闭后，防火墙从转发表中删除与隧道关联的路由。配置重试设置有助于避免对尚未真正关闭的隧道采取措施。
4. （可选）设置 **Hold Timer**（保持计时器），这是在防火墙重新与隧道对端建立通信之前，keepalive 数据包成功的 **Intervals**（间隔）数（范围为 1 - 64；默认为 5）。

STEP 4 | 单击 **OK**（确定）。

STEP 5 | 配置路由协议或静态路由，以通过 GRE 隧道路由流量到目标。例如，配置静态路由到目标服务器网络，并指定成为本地隧道端点的出口 **Interface**（接口）(tunnel.1)。配置成为对端隧道上 IP 地址的下一个跃点。例如：192.168.2.3。

STEP 6 | **Commit**（提交）更改。

STEP 7 | 为隧道对端配置公共 IP 地址、其本地和对等 IP 地址（分别对应于防火墙 GRE 隧道行的对等和本地 IP 地址）以及其路由协议或静态路由。

STEP 8 | 验证防火墙是否可以通过 GRE 隧道与对等隧道通信。

1. 访问 CLI。
2. `> ping source 192.168.2.1 host 192.168.2.3`



© 2019 Palo Alto Networks, Inc.

# DHCP

本部分将介绍动态主机配置协议 (DHCP) 以及在 Palo Alto Networks 防火墙上配置接口以充当 DHCP 服务器、客户端或中继代理时需要执行的任务。通过将这些角色分配给不同的接口，防火墙可以扮演多个角色。


- DHCP 概述
- 防火墙作为 DHCP 服务器和客户端
- DHCP 消息
- DHCP 寻址
- DHCP 选项
- 将接口配置为 DHCP 服务器
- 将接口配置为 DHCP 客户端
- 将管理接口配置为 DHCP 客户端
- 将接口配置为 DHCP 中继代理
- 对 DHCP 进行监控和故障排除


## DHCP 概述

DHCP 是 RFC 2131 中定义的标准化协议，即动态主机配置协议。DHCP 的主要目的有两个：提供 TCP/IP 和链接层配置参数，为 TCP/IP 网络上的动态配置主机提供网络地址。

DHCP 使用“客户端-服务器”通信模型。该模型由设备可以扮演的三个角色构成：DHCP 客户端、DHCP 服务器和 DHCP 中继代理。

- 充当 DHCP 客户端（主机）的设备可以从 DHCP 服务器请求 IP 地址和其他配置设置。客户端设备上的用户可保存配置时间和作业，并且不需要了解网络的寻址计划或是继承自 DHCP 服务器的其他资源和选项。
- 充当 DHCP 服务器的设备可以为客户端提供服务。通过使用三种DHCP 寻址机制中的任一种机制，网络管理员可以保存配置时间，并能在客户端不再需要网络连接时重复使用有限数量的 IP 地址。服务器可以进行 IP 寻址并向多个客户端提供多个 DHCP 选项。
- 充当 DHCP 中继代理的设备可以在 DHCP 客户端和服务器间传输 DHCP 消息。

DHCP 使用用户数据报协议 (UDP) (RFC 768) 作为其传输协议。客户端发送到服务器的 DHCP 消息将发送到众所周知的端口 67（UDP — Bootstrap 协议和 DHCP）。DHCP 消息服务器发送到客户端的 将发送到端口 68。

Palo Alto Networks 防火墙上的接口可以充当 DHCP 服务器、客户端或中继代理。DHCP 服务器或中继代理的接口必须为第 3 层 Ethernet、聚合以太网或第 3 层 VLAN 接口。您可以使用任意角色组合的相应设置来配置防火墙的接口。防火墙作为 DHCP 服务器和客户端中汇总了各个角色的行为。

该防火墙支持 DHCPv4 服务器和 DHCPv6 中继。但是，单个接口不能同时支持 DHCPv4 服务器和 DHCPv6 中继。

Palo Alto Networks 的 DHCP 服务器和 DHCP 客户端实施仅支持 IPv4 地址。其 DHCP 中继实施支持 IPv4 和 IPv6。DHCP 客户端在高可用性主动/主动模式下不受支持。

## 防火墙作为 DHCP 服务器和客户端

防火墙可以充当 DHCP 服务器和 DHCP 客户端。动态主机配置协议 - DHCP，RFC 2131 旨在为 IPv4 和 IPv6 地址提供支持。DHCP 服务器的 Palo Alto Networks 实施仅支持 IPv4 地址。

防火墙 DHCP 服务器以以下方式工作：



© 2019 Palo Alto Networks, Inc.

- 当 DHCP 服务器收到发送自客户端的 DHCPDISCOVER 消息时，服务器会回复包含所有预定义和用户定义选项的 DHCPOFFER 消息，这些选项的顺序就是在配置中显示的顺序。客户端会选择它需要的选项并使用 DHCPREQUEST 消息响应。
- 当服务器收到来自客户端的 DHCPREQUEST 消息时，服务器会回复只包含请求内指定的选项的 DHCPACK 消息。

防火墙 DHCP 客户端的操作方式如下：

- 当 DHCP 客户端收到发送自服务器的 DHCPOFFER 时，无论 DHCPREQUEST 中发送了哪些选项，客户端都会自动缓存所提供所有选项以供将来使用。
- 默认情况下，为了节省内存消耗，如果客户端收到代码的多个值，客户端只会缓存各个选项代码的第一个值。
- DHCP 消息没有最大长度，除非 DHCP 客户端在 DHCPDISCOVER 或 DHCPREQUEST 消息中的选项 57 中指定最大值。

## DHCP 消息

DHCP 使用的标准消息类型共有八种，会在 DHCP 消息中以选项类型编号标识。例如，当客户端想要查找 DHCP 服务器时，它会在本地物理子网中广播 DHCPDISCOVER 消息。如果子网中没有 DHCP 服务器，而且 DHCP 帮助程序或 DHCP 中继的配置正确，那么此消息将转发到另一物理子网中的 DHCP 服务器。否则，此消息将止步于其源子网。一个或多个 DHCP 服务器将通过包含可用网络地址和其他配置参数的 DHCPOFFER 消息来进行响应。

当客户端需要 IP 地址时，它会向一个或多个服务器发送 DHCPREQUEST。当然，如果客户端正在请求 IP 地址,就表示它还没有 IP 地址，所以 RFC 2131 要求客户端发出的广播消息要在其 IP 标头中包含源地址 0。

当客户端从某个服务器请求配置参数时，它可能会收到来自多个服务器的响应。如果客户端收到其 IP 地址，即表示该客户端至少有一个 IP 地址，可能还有与其绑定的其他配置参数。DHCP 服务器会管理针对客户端的此类配置参数绑定。

下表中列有各个 DHCP 消息。

| DHCP 消息 | 说明 |
|---|---|
| DHCPDISCOVER | 用于查找可用 DHCP 服务器的客户端广播。 |
| DHCPOFFER | 服务器针对客户端的 DHCPDISCOVER 做出的响应，用于提供配置参数。 |
| DHCPREQUEST | 针对一个或多个服务器发出的客户端消息，用于执行以下任一任务：<br>• 从一个服务器请求参数，并隐式拒绝其他服务器提供的参数。<br>• 确认先前分配的地址是否正确（例如，在系统重启之后）。<br>• 延长网络地址的租借。 |
| DHCPACK | 从服务器发到客户端的确认消息，包含配置参数，还包括已确认的网络地址。 |
| DHCPNAK | 从服务器发到客户端的否定确认，用于表明客户端认为网络地址不正确（例如，如果客户端已移到新的子网中），或表明客户端的租借已过期。 |
| DHCPDECLINE | 从客户端发到服务器的消息，用于表明网络地址已被占用。 |
| DHCPRELEASE | 从客户端发到服务器的消息，用于放弃用户所用的网络地址并取消剩余的租借时间。 |



© 2019 Palo Alto Networks, Inc.

| DHCP 消息 | 说明 |
| --- | --- |
| DHCPINFORM | 从客户端发到服务器的消息，只用于请求本地配置参数；客户端拥有外部配置的网络地址。 |

# DHCP 寻址

- DHCP 地址分配方法
- DHCP 租借

## *DHCP 地址分配方法*

DHCP 服务器可以通过三种方式向客户端分配或发送 IP 地址：

- 自动分配 — DHCP 服务器将其 **IP** 池中的永久性 IP 地址分配给客户端。在防火墙上，将租借指定为无限制意味着分配是永久性的。
- 动态分配 — DHCP 服务器将地址 **IP** 池中的可复用 IP 地址分配给客户端，以便让其使用最长的一段时间，称为租借。如果客户的 IP 地址数量有限，这种地址分配方式就非常有用；可以将这些地址分配给只需临时访问网络的客户端。请参阅 DHCP 租借部分。
- 静态分配 — 网络管理员选择要分配给客户端的 IP 地址，然后由 DHCP 服务器将其发至客户端。静态 DHCP 分配是永久性的；将通过以下方式来完成：配置 DHCP 服务器并选择与客户端设备的 **MAC Address**（**MAC** 地址）相对应的 **Reserved Address**（保留地址）。即使客户端出现注销、重启、断电等情况，DHCP 分配也将保持就绪状态。

  IP 地址的静态分配非常有用，例如，当 LAN 中有打印机而您不希望其 IP 地址不断变化（因为它会通过 DNS 与打印机名称关联）时。又例如，客户端设备被用于执行某些关键任务，即使该设备出现关机、拔下插头、重启或断电等情况时，也必须保持相同的 IP 地址。

  在配置 **Reserved Address**（保留地址）时，请记住以下几点：

  - 它是 **IP** 池中的某个地址。您可以配置多个保留地址。
  - 如果未配置保留地址，那么服务器的客户端会在租借过期或执行重启等操作后收到来自该池中的新 DHCP 分配（除非将租借指定为无限制）。
  - 如果将 **IP Pools**（**IP** 池）中的所有地址都分配为 **Reserved Address**（保留地址），就意味着无法为下一个请求地址的 DHCP 客户端分配可用的动态地址。
  - 您可以分配保留地址，但不分配 **MAC** 地址。在这种情况下，DHCP 服务器不会向任何设备分配 **Reserved Address**（保留地址）。您可以保留池中的小部分地址，并在不使用 DHCP 的情况下对其进行静态分配，例如分配给传真机和打印机。

## *DHCP 租借*

租借被定义为：某个网络地址在一段时间内被 DHCP 服务器分配给某个客户端。租借可以通过后续请求延长（续订）。如果客户端不再需要该地址，则可在租借结束前将该地址重新释放到服务器。然后，服务器可以在未分配地址已用完时自由地将该地址分配给另一客户端。

为 DHCP 服务器所配置的租借期将应用于单个 DHCP 服务器（接口）动态分配给其客户端的所有地址。也就是说，该接口的所有动态分配地址都具有 **Unlimited**（无限制）的持续时间，或具有相同的 **Timeout**（超时）值。防火墙所配置的其他 DHCP 服务器的客户端可能具有不同的租借期。**Reserved Address**（保留地址）是一种静态地址分配，没有租借期。

根据 DHCP 标准 RFC 2131，DHCP 客户端不会等到租借过期，因为它会面临新地址分配风险。当 DHCP 客户端的租借期过半时，它会尝试延长租借，以便保留同一 IP 地址。因此，租借持续时间就好像是一个滑动窗口。


© 2019 Palo Alto Networks, Inc.

通常，如果已为设备分配 IP 地址，那么该设备随后会脱离网络，其租借不会延期，DHCP 服务器会让租借过期。因为客户端会脱离网络且不再需要该地址，所以服务器中的租借持续时间会耗尽，租借会处于“过期”状态。

防火墙有一个保留计时器，可避免过期 IP 地址立即被重新分配。这么做可以为该设备暂时保留该地址，以防该设备重新进入网络。但是，如果地址池中的地址已用完，服务器就会在保留计时器过期前重新分配该过期地址。过期地址会在系统需要更多地址时或在被保留计时器释放后自动清除。

可在 CLI 中使用 **show dhcp server lease** 操作命令查看已分配 IP 地址的租借信息。如果不想等待过期租借自动释放，则可以使用 **clear dhcp lease interface *<interface>* expired-only** 命令清除过期租借，以便让这些地址重新成为池中的可用地址。您可以使用 **clear dhcp lease interface *<interface>* ip *<ip_address>*** 命令释放特定 IP 地址。使用 **clear dhcp lease interface *<interface>* mac *<mac_address>*** 命令可以释放特定 MAC 地址。

# DHCP 选项

DHCP 和 DHCP 选项的历史记录可以追溯到 Bootstrap 协议 (BOOTP)。BOOTP 可供主机用于在其引导过程中进行自我动态配置。主机可能会收到来自某个服务器的 IP 地址以及要从中下载引导程序的文件，还会收到该服务器的地址以及互联网网关的地址。

BOOTP 数据包中所含的是一个供应商信息字段，其中可能包含一些含有各类信息（如子网掩码、BOOTP 文件大小及很多其他值）的标记字段。RFC 1497 对 BOOTP 供应商信息扩展进行了介绍。DHCP 将代替 BOOTP；BOOTP 在防火墙上不受支持。

这些扩展最终通过使用 DHCP 和 DHCP 主机配置参数（也称为“选项”）实现了扩展。和供应商扩展类似，DHCP 选项也是标记数据项，用于向 DHCP 客户端提供信息。这些选项将通过 DHCP 消息尾部的变长字段来发送。例如，DHCP 消息类型为选项 53，值 1 表示 DHCPDISCOVER 消息。RFC 2132，DHCP 选项和 BOOTP 供应商扩展对 DHCP 选项进行了定义。

DHCP 客户端可以与服务器协商，以限制服务器只发送客户端所请求的选项。

- 预定义 DHCP 选项
- DHCP 选项的多个值
- DHCP 选项 43、55 和 60 以及其他自定义选项

## 预定义 *DHCP* 选项

Palo Alto Networks 防火墙支持 DHCP 服务器实施中用户定义和预定义的 DHCP 选项。此类选项会在 DHCP 服务器上进行配置，并会发送到向服务器发送了 DHCPREQUEST 的客户端。客户端会继承并实施被编程为接受的选项。

该防火墙支持 DHCP 服务器上预先定义的以下选项（按照 **DHCP Server**（**DHCP** 服务器）配置屏幕上的显示顺序显示）：

| DHCP 选项 | DHCP 选项名称 |
|---|---|
| 51 | 租借持续时间 |
| 3 | 网关 |
| 1 | IP 池子网（掩码） |
| 6 | 域名系统 (DNS) 服务器地址（主和辅助） |
| 44 | Windows互联网名称服务 (WINS) 服务器地址（主和辅助） |



© 2019 Palo Alto Networks, Inc.

| DHCP 选项 | DHCP 选项名称 |
|---|---|
| 41 | 网络信息服务 (NIS) 服务器地址（主和辅助） |
| 42 | 网络时间协议 (NTP) 服务器地址（主和辅助） |
| 70 | 邮局协议版本 3 (POP3) 服务器地址 |
| 69 | 简单邮件传输协议 (SMTP) 服务器地址 |
| 15 | DNS 后缀 |

如前所述，您还可以配置供应商特定和自定义选项，这些选项支持各种办公设备，如 IP 电话和无线基础架构设备。每个选项代码支持多种值，这些值可以是 IP 地址、ASCII 或十六进制格式。通过防火墙增强的 DCHP 选项支持，分支机构无需购买和管理他们自己的 DHCP 服务器便能为 DHCP 客户端提供客户端特定和自定义选项。

## *DHCP 选项的多个值*

您可以为具有相同 **Option Name**（选项名称）的 **Option Code**（选项代码）输入多个选项值，但是特定代码和名称组合的所有值必须是同一类型（IP 地址、ASCII 或十六进制）。如果已继承或输入一种类型，而稍后为同一代码和名称组合输入了不同的类型，第二种类型将覆盖第一种类型。

通过使用不同的 **Option Name**（选项名称），您可以多次输入 **Option Code**（选项代码）。这种情况下，选项代码的 **Option Type**（选项类型）因选项名称不同而异。例如，如果选项 Coastal Server（选项代码 6）配置为 IP 地址类型，那么也允许选项服务器 XYZ（选项代码 6）带有 ASCII 类型。

防火墙会将选项（串在一起）的多个值按照从顶部到底部的顺序发送到客户端。因此，在为选项输入多个值时，请按照首选项顺序输入值，或者移动选项以实现列表中的优先顺序。防火墙配置中选项的顺序决定着这些选项在 DHCPOFFER 和 DHCPACK 消息中显示的顺序。

您可以输入已作为预定义选项代码存在的选项代码，而自定义选项将覆盖预定义选项；防火墙将发出警告。

## *DHCP 选项 43、55 和 60 以及其他自定义选项*

下表对 RFC 2132 中介绍的各种选项的选项行为进行了说明。

| 选项代码 | 选项名称 | 选项说明/行为 |
|---|---|---|
| 43 | 供应商特定信息 | 从服务器发送到客户端。DHCP 服务器已配置的提供给客户端的供应商特定信息。如果服务器在其表中有与客户端的 DHCPREQUEST 匹配的 Vendor Class Identifier（供应商类别标识符，VCI），则此信息只会发送到客户端。<br>选项 43 数据包可以包含多项供应商特定信息。还可以包含封装的供应商特定扩展数据。 |
| 55 | 参数请求列表 | 从客户端发送到服务器。DHCP 客户机正在请求的配置参数（选项代码）列表，可能是按照客户端的首选项顺序。服务器尝试以相同顺序的选项进行响应。 |


© 2019 Palo Alto Networks, Inc.

| 选项代码 | 选项名称 | 选项说明/行为 |
| --- | --- | --- |
| 60 | Vendor Class Identifier（供应商类别标识符-VCI) | 从客户端发送到服务器。DHCP 客户端的供应商类型和配置DHCP 客户端将 DHCPREQUEST 中的选项代码 60 发送到 DHCP 服务器。当服务器收到选项 60 时，会看到此 VCI 并查找自己表中匹配的 VCI，然后返回带有此值（与 VCI 对应）的选项 43，从而将供应商特定信息中继到正确的客户端。客户端和服务器都熟知 VCI。 |

您可以发送 RFC 2132 中未定义的自定义供应商特定选项代码。这些选项代码的范围为 1-254，可以是固定长度或可变长度

自定义 *DHCP* 选项未经 *DHCP* 服务器验证，因此必须确保为您所创建的选项输入正确的值。

对于 ASCII 和十六进制 DHCP 选项类型，选项值最大可以为 255 个八进制数。

## 将接口配置为 DHCP 服务器

该任务的先决条件如下：

- 配置第 3 层以太网或第 3 层 VLAN 接口。
- 将此接口分配给虚拟路由器和区域。
- 通过自己的网络计划确定有效的 IP 地址池，其中的地址可被指定为由 DHCP 服务器分配给客户端。
- 收集您计划配置的 DHCP 选项、值和 Vendor Class Identifiers（供应商类别标识符-VCI）。

容量如下：

- 对于除 PA-5200 系列和 PA-7000 系列防火墙之外的防火墙型号，请参阅 Product Selection tool（产品选型工具）。
- 对于 PA-5220 防火墙，最多可以配置 500 个 DHCP 服务器和最多 2,048 减去已配置的 DHCP 服务器数量的 DHCP 中继代理。例如，如果配置 500 个 DHCP 服务器，则可以配置 1,548 个 DHCP 中继代理。
- 对于 PA-5250、PA-5260 和 PA-7000 系列防火墙，最多可以配置 500 个 DHCP 服务器和最多 4096 减去已配置的 DHCP 服务器数量的 DHCP 中继代理。例如，如果配置 500 个 DHCP 服务器，则可以配置 3596 个 DHCP 中继代理。

请执行以下任务，以将防火墙上的接口配置为 DHCP 服务器。

STEP 1 | 选择要成为 DHCP 服务器的接口。

1. 选择 **Network**（网络）> **DHCP** > **DHCP Server**（**DHCP** 服务器）并 **Add**（添加）**Interface**（接口）名称，或选择一个名称。
2. 关于 **Mode**（模式），请选择 **enabled**（已启用）或 **auto**（自动）模式。自动模式会启用服务器，而且该服务器会在检测到网络中存在另一 DHCP 服务器时被禁用。**disabled**（禁用）设置会禁用该服务器。
3. （可选）如果希望服务器在将 IP 地址分配给其客户端之前对该地址执行 ping 操作，请单击 **Ping IP when allocating new IP**（在分配新 **IP** 时 **Ping IP**）。

   如果 *Ping* 收到响应，这意味着另一设备已拥有该地址，因此该地址不可用。服务器会转而分配池中的下一个地址。这一行为类似于针对 IPv6 的乐观重复地址检测 (DAD) (RFC 4429)。

   设置好选项并回到 *DHCP* 服务器选项卡后，接口的 *Probe IP*（探测 *IP*）列会指明 *Ping IP when allocating new IP*（分配新的 *IP* 时 *Ping IP*）是否已选中。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 配置服务器要发送到客户端的预定义 DHCP 选项。

- 在“选项”部分中，选择 **Lease**（租借）类型：
- **Unlimited**（无限制）可让服务器从 **IP Pools**（**IP** 池）中动态选择 IP 地址并将其永久分配给客户端。
- **Timeout**（超时）可决定租借的持续时长。输入 **Days**（天）数和 **Hours**（小时）数，并（可选）输入 **Minutes**（分钟）数。
- **Inheritance Source**（继承源）— 保留 **None**（无）或选择源 DHCP 客户端接口或 PPPoE 客户端接口，以便将各种服务器设置传播到 DHCP 服务器。如果指定了继承源，请选择想要从此源继承的一个或多个选项。

指定继承源使防火墙可快速添加来自 DHCP 客户端收到的上游服务器的 DHCP 选项。如果源更改了选项，客户端的选项也能得到更新。例如，如果源更换了其 NTP 服务器（已被标识为 **Primary NTP**（主 **NTP**）服务器），那么客户端会将该新地址自动继承为其 **Primary NTP**（主 **NTP**）服务器。

在继承包含多个 *IP* 地址的 *DHCP* 选项时，防火墙只会使用选项中包含的第一个 *IP* 地址来保存高速缓存。如果您需要为单个选项使用多个 *IP* 地址，请直接在此防火墙上配置 *DHCP* 选项，而不是配置继承选项。

- **Check inheritance source status**（检测继承源状态）— 如果已选择 **Inheritance Source**（继承源），那么单击此链接可打开 **Dynamic IP Interface Status**（动态 **IP** 接口状态）窗口，该窗口会显示继承自 DHCP 客户端的选项。
- **Gateway**（网关）— 用于访问和此 DHCP 服务器不在同一 LAN 中的任何设备的网络网关（防火墙上的接口）的 IP 地址。
- **Subnet Mask**（子网掩码）— 用于 **IP Pools**（**IP** 池）中地址的网络掩码。

请针对以下字段单击向下箭头并选择 **None**（无）或 **inherited**（继承），或者输入您的 DHCP 服务器将发送到客户端以用于访问该设备的远程服务器 IP 地址。如果选择 **inherited**（继承），DHCP 服务器会从被指定为 **Inheritance Source**（继承源）的源 DHCP 客户端继承值。

- 主 **DNS**、辅助 **DNS** — 首选和备用域名系统 (DNS) 服务器的 IP 地址。
- **Primary WINS**（主 **WINS**）、**Secondary WINS**（辅助 **WINS**）— 首选和备用 Windows Internet 命名服务 (WINS) 服务器的 IP 地址。
- **Primary NIS**（主 **NIS**）、**Secondary NIS**（辅助 **NIS**）— 首选和备用网络信息服务 (NIS) 服务器的 IP 地址。
- **Primary NTP**（主 **NTP**）、**Secondary NTP**（辅助 **NTP**）— 可用的网络时间协议服务器的 IP 地址。
- **POP3 Server**（**POP3** 服务器）— 邮局协议 (POP3) 服务器的 IP 地址。
- **SMTP Server**（**SMTP** 服务器）— 简单邮件传输协议 (SMTP) 服务器的 IP 地址。
- **DNS Suffix**（**DNS** 后缀）— 客户端无法解析所输入的非限定主机名时要在本地使用的后缀。

STEP 3 | （可选）配置 DHCP 服务器发送到其客户端的供应商特定选项或自定义 DHCP 选项。

1. 在自定义 DHCP 选项部分中，**Add**（添加）描述性 **Name**（名称）以标识 DHCP 选项。
2. 请输入您要配置的服务器能提供的 **Option Code**（选项代码）（范围为 1-254）。（有关选项代码，请参阅 RFC 2132）。
3. 如果 **Option Code**（选项代码）为 **43**，则会出现 **Vendor Class Identifier**（供应商类别标识符-**VCI**）字段。输入 VCI，该 VCI 是一个字符串或十六进制值（带有 0x 前缀），用作来自客户端请求（包含选项 60）的值的匹配项。服务器会在其表中查找传入 VCI，找到此 VCI 后返回选项 43 和对应的选项值。
4. **Inherit from DHCP server inheritance source**（从 **DHCP** 服务器继承源继承）— 只有为 DHCP 服务器预先定义的以下选项指定一个 **Inheritance Source**（继承源），并且希望供应商指定和自定义选项也从此源继承时，才选择该选项。
5. **Check inheritance source status**（检测继承源状态）— 如果已选择 **Inheritance Source**（继承源），那么单击此链接可打开 动态 **IP** 接口状态（**Dynamic IP Interface Status**），该窗口会显示继承自 DHCP 客户端的选项。


© 2019 Palo Alto Networks, Inc.

6. 如果你没有选择 **Inherit from DHCP server inheritance source**（从 **DHCP** 服务器继承源继承），请选择一个 **Option Type**（选项类型）：**IP Address**（**IP** 地址）、**ASCII** 或 **Hexadecimal**（十六进制）。十六进制值必须以 0x 前缀开头。
7. 输入您希望服务器为该 **Option Code**（选项代码）提供的 **Option Value**（选项值）。您可以在单独行上输入多个值。
8. 单击 **OK**（确定）。

STEP 4 | （可选）添加其他供应商特定选项或自定义 DHCP 选项。

1. 重复先前步骤以输入其他自定义 DHCP 选项。
   - 您可以为具有相同 **Option Name**（选项名称）的 **Option Code**（选项代码）输入多个选项值，但是 **Option Code**（选项代码）的所有值必须是同一类型（**IP Address**（**IP** 地址）、**ASCII** 或 **Hexadecimal**（十六进制））。如果已继承或输入一种类型，而稍后为同一 **Option Code**（选项代码）和同一 **Option Name**（选项名称）输入了不同的类型，则第二种类型会覆盖第一种类型。

     在为选项输入多个值时，请按照首选项顺序输入值，或者移动自定义 DHCP 选项以实现列表中的优先顺序。选择一个选项，然后单击 **Move Up**（上移）或 **Move Down**（下移）。
   - 通过使用不同的 **Option Name**（选项名称），您可以多次输入 **Option Code**（选项代码）。这种情况下，选项代码的 **Option Type**（选项类型）因选项名称不同而异。
2. 单击 **OK**（确定）。

STEP 5 | 确定有状态的 IP 地址池，DHCP 服务器将从中选择地址并将其分配给 DHCP 客户端。

如果您不是所用网络的网络管理员，请让网络管理员查看网络计划以获取有效的 *IP* 地址池，其中的地址可被指定为由 *DHCP* 服务器来分配。

1. 在 **IP Pools**（**IP** 池）字段中，**Add**（添加）IP 地址范围，该服务器会将该范围中的地址分配给客户端。输入 IP 子网和子网掩码（例如 192.168.1.0/24）或 IP 地址的范围（例如 192.168.1.10-192.168.1.20）。
   - 对于动态 IP 地址分配而言，IP 池或 **Reserved Address**（保留地址）是强制要求。
   - IP 池对于静态 IP 地址分配是可选的，只要你分配的 IP 地址属于防火墙接口服务的子网。
2. （可选）重复此步骤以指定另一 IP 地址池。

STEP 6 | （可选）指定 IP 池中的非动态分配 IP 地址。如果还指定了 **MAC Address**（**MAC** 地址），那么当设备通过 DHCP 请求 IP 地址时，**Reserved Address**（保留地址）会被分配给该设备。

有关 *Reserved Address*（保留地址）的分配说明，请参阅 DHCP 寻址部分。

1. 在 **Reserved Address**（保留地址）字段中，单击 **Add**（添加）。
2. 输入 **IP Pools**（**IP** 池）中不希望由 DHCP 服务器动态分配的 IP 地址（格式为 *x.x.x.x*）。
3. （可选）指定要为其永久分配您所指定 IP 地址的设备的 **MAC Address**（**MAC** 地址）（格式为 *xx:xx:xx:xx:xx:xx*）。
4. （可选）重复前两个步骤以保留另一地址。

STEP 7 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

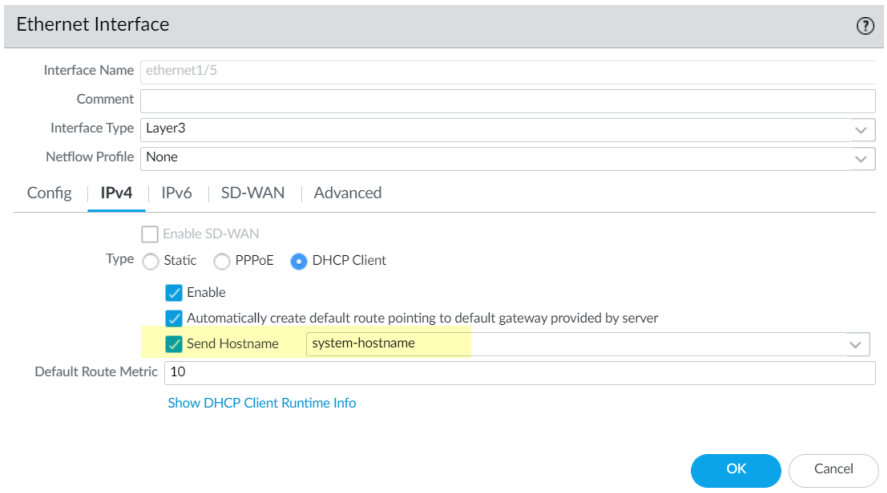
# 将接口配置为 DHCP 客户端

在将防火墙接口配置为 DHCP 客户端之前，请确保您已配置第 3 层接口（Ethernet、Ethernet 子接口、VLAN、VLAN 子接口、聚合或聚合子接口），并确保已将该接口分配给某个虚拟路由器和区域。如果需要使用 DHCP 为接口请求 IPv4 地址，请将接口配置为 DHCP 客户端。

您还可以将管理接口配置为 DHCP 客户端。

STEP 1 | 将接口配置为 DHCP 客户端。

1. 选择 **Network**（网络）> **Interfaces**（接口）。
2. 在 **Ethernet**（以太网）选项卡或 **VLAN** 选项卡上，**Add**（添加）第 3 层接口，或选择已配置的第 3 层接口，以使其成为 DHCP 客户端。
3. 单击 **IPv4** 选项卡；对于 **Type**（类型），选择 **DHCP Client**（**DHCP** 客户端）。
4. 选择 **Enable**（启用）。
5. （可选）启用此选项后，可自动创建指向服务器所提供的默认网关的默认路由（此选项默认启用）。启用此选项后，防火墙就会针对默认网关创建静态路由，当客户端尝试访问不需要在防火墙的路由表中进行路由维护的多个目标时，该静态路由非常有用。
6. （可选）启用此选项以 **Send Hostname**（发送主机名）后，就可分配主机名至 DHCP 客户端接口并发送该主机名（选项 12）至 DHCP 服务器，后者可通过 DNS 服务器注册该主机名。之后，DNS 服务器可自动管理主机名至动态 IP 地址解析。外部主机可通过其主机名识别接口。默认值表示 **system-hostname**（系统-主机名），这是您在 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（一般设置）中设定的防火墙主机名。或者，也可以输入接口主机名，最多可以是 64 个字符，包括大小写字母、数字、英文句号 (.)、连字符 (-) 和下划线 (_)。




7. （可选）输入防火墙和 DHCP 服务器间路由的 **Default Route Metric**（默认路由跃点数）（优先级级别）：范围为 1-65,535，10 个默认跃点数。数值越小的路由，在路由选择期间的优先级越高。例如，相对于跃点数为 100 的路由，会先使用跃点数为 10 的路由。

防火墙和 *DHCP* 服务器间路由的 *Default Route Metric*（默认路由跃点数）的默认值为 *10*。如果静态默认路由 *0.0.0.0/0* 使用 *DHCP* 接口作为其传出接口，则该路由的默认*Metric*（跃点数）仍为 *10*。因此，有两个路由的跃点数均为 *10*，这样，防火墙每次可随机选择其中一个路由，下次可选择另一个路由。

假定您启用此选项来自动创建指向服务器所提供的默认网关的默认路由，选择一个虚拟路由器，添加第 *3* 层接口静态路由，将*Metric*（跃点数）（默认为 *10*）设为一个大于 *10* 的值（例如，*100*），并提交您的更改。在路由表中，路由的跃点数不会显示为 *100*。相反，会如预期所示，显示默认值 *10*，这是因为 *10* 的优先级高于配置值 *100*。


© 2019 Palo Alto Networks, Inc.

但是，如果将静态路由的 *Metric*（跃点数）更改为小于 *10* 的值（例如，*6*），则路由表中路由的跃点数会更新，显示为配置值 *6*。

8. （可选）启用此选项以 **Show DHCP Client Runtime Info**（显示 **DHCP** 客户端运行时信息）后，就可以查看客户端已从其 DHCP 服务器继承的所有设置。

STEP 2 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

现在，以太网接口应当在 **Ethernet**（以太网）选项卡的 **IP Address**（**IP** 地址）中指明 **Dynamic-DHCP Client**（动态 **DHCP** 客户端）。

STEP 3 | （可选）查看防火墙上的哪个接口已被配置为 DHCP 客户端。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并检查 **IP Address**（**IP** 地址），看看哪些接口指明 DHCP 客户端。
2. 选择 **Network**（网络）> **Interfaces**（接口）> **VLAN**并检查 **IP Address**（**IP** 地址），看看哪些接口指明 DHCP 客户端。

# 将管理接口配置为 DHCP 客户端

防火墙上的管理接口支持 IPv4 的 DHCP 用户端，从而允许管理接口接受来自 DHCP 服务器的 IPv4 地址。管理接口还支持 DHCP 选项 12 和选项 61，从而允许防火墙分别发送其主机名和客户端识别符至 DHCP 服务器。

在默认情况下，在 AWS 和 Azure™ 部署的 VM 系列防火墙使用管理接口作为 DHCP 客户端，以获取其 IP 地址，而不是静态 IP 地址，因为云端部署需要此功能所提供的自动化。在默认情况下，关闭 VM 系列防火墙（AWS 和 Azure 中的 VM 系列防火墙除外）的管理接口上的 DHCP。WildFire 和 Panorama 型号上的管理接口不支持此 DHCP 功能。

- 对于基于硬件的防火墙型号（而非 *VM* 系列），在可能的时候，使用静态 *IP* 地址配置管理接口。
- 如果防火墙通过 *DHCP* 获得管理接口地址，在服务防火墙的 *DHCP* 服务器分配一个 *MAC* 地址预留。预留可确保防火墙在重启之后保留其管理 *IP* 地址。如果 *DHCP* 服务器是一个 *Palo Alto Networks* 防火墙，请参阅将接口配置为 DHCP 服务器中的第 *6* 步预约地址。

如果配置管理接口为 DHCP 客户端，则可应用以下限制：

- 您不能在 HA 配置中使用管理接口用于控制链路（HA1 或 HA1 备份）、数据链路（HA2 或 HA2 备份），或者数据包转发 (HA3) 通信。
- 当您自定义服务器路由时，您不能选择 **MGT**（管理）作为源接口（**Device**（设备）> **Setup**（设置）> **Services**（服务）> **Service Route Configuration**（服务路由配置）> **Customize**（自定义））。然而，您可以选择 **Use default**（使用默认设置）通过管理接口路由数据库。
- 您不能使用管理界面的动态 IP 地址连接到硬件安全模块 (HSM)。HSM 客户端防火墙上的 IP 地址必须是静态 IP 地址，因为 HSM 使用 IP 地址对防火墙进行身份验证。如果 IP 地址在运行时更改，HSM 上的操作将停止工作。

此任务的先决条件是，管理接口必须能够连接至 DHCP 服务器。

STEP 1 | 将管理接口配置为 DHCP 客户端，从而它可以从 DHCP 服务器接收其 IP 地址 (IPv4)、子网掩码 (IPv4) 和来自 DHCP 服务器的默认网关。

（可选）如果使用的协调系统接受此信息，还可以发送管理接口的主机名称和客户端标识符至 DHCP 服务器。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑管理界面设置部分。
2. 对于 **IP Type**（**IP** 类型），选择 **DHCP Client**（**DHCP** 客户端）。
3. （可选）选择防火墙的一个或两个选项在 DHCP 发现或请求消息中发送至 DHCP 服务器。



© 2019 Palo Alto Networks, Inc.

- **Send Hostname**（发送主机名）— 发送 **Hostname**（主机名）作为 DHCP 选项 12 的一部分（如在 **Device**（设备）> **Setup**（设置）> **Management**（管理）中所定义）。
- **Send Client ID**（发送客户端 **ID**）— 发送其客户端标识符，以作为 DHCP Option 61 的一部分。客户端标识符可以唯一识别 DHCP 客户端，而 DHCP 服务器使用它来指出其配置参数数据库。

4. 单击 **OK**（确定）。

STEP 2 | （可选）配置防火墙以接受来自 DHCP 服务器的主机名和域。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。
2. 选择一个或两个选项：
   - **Accept DHCP server provided Hostname**（接受 **DHCP** 服务器所提供的主机名）— 允许防火墙接受来自 DHCP 服务器的主机名称（如有效）。启用时，来自 DHCP 服务器的主机名覆盖 **Device**（设备）> **Setup**（设置）> **Management**（管理）中指定的现有 **Hostname**（主机名）。如果要手动配置主机名，请勿选择此选项。
   - **Accept DHCP server provided Domain**（接受 **DHCP** 服务器所提供的域）— 允许防火墙接受 DHCP 服务器所提供的域。来自 DHCP 服务器的域（DNS 后缀）覆盖 **Device**（设备）> **Setup**（设置）> **Management**（管理）中指定的现有 **Domain**（域）。如果要手动配置域，请勿选择此选项。
3. 单击 **OK**（确定）。

STEP 3 | 提交更改。

单击 **Commit**（提交）。

STEP 4 | 查看 DHCP 客户端信息。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）和管理界面设置。
2. 单击 **Show DHCP Client Runtime Info**（显示 **DHCP** 客户端运行时信息）。

STEP 5 | （可选）使用 DHCP 服务器续订 DHCP 版本，与租借期无关。

如果在测试或排除网络问题故障，此选项较为方便。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑管理界面设置部分。
2. 单击 **Show DHCP Client Runtime Info**（显示 **DHCP** 客户端运行时信息）。
3. 单击 **Renew**（续订）。

STEP 6 | （可选）解除来自 DHCP 服务器的以下 DHCP 选项：

- IP 地址
- 子网掩码
- 默认网关
- DNS 服务器（主要和辅助）
- NTP 服务器（主要和辅助）
- 域（DNS 后缀）

解除 *IP* 地址，也就是在没有配置其他接口用于管理访问时，断开网络连接和提供无法管理的防火墙。

使用 CLI 操作命令 **`request dhcp client management-interface release`**。

# 将接口配置为 DHCP 中继代理

要启用防火墙接口，以传输客户端和服务器之间的 DHCP 消息，则必须配置防火墙作为 DHCP 中继代理。接口最多可转发消息到 8 个外部 IPv4 DHCP 服务器和 8 个 IPv6 DHCP 服务器。客户端 DHCPDISCOVER


© 2019 Palo Alto Networks, Inc.

消息会发送至所有已配置的服务器，而第一个做出响应的服务器的 DHCPOFFER 消息会重新中继到发出请求的客户端。

容量如下：

- 您可以在除 PA-5200 系列和 PA-7000 系列防火墙外的所有防火墙型号上最多配置 500 个 DHCP 服务器(IPv4)和 DHCP 中继代理（IPv4 和 IPv6）
- 对于 PA-5220 防火墙，最多可以配置 500 个 DHCP 服务器和最多 2,048 减去已配置的 DHCP 服务器数量的 DHCP 中继代理。例如，如果配置 500 个 DHCP 服务器，则可以配置 1,548 个 DHCP 中继代理。
- 对于 PA-5250、PA-5260 和 PA-7000 系列防火墙，最多可以配置 500 个 DHCP 服务器和最多 4096 减去已配置的 DHCP 服务器数量的 DHCP 中继代理。例如，如果配置 500 个 DHCP 服务器，则可以配置 3596 个 DHCP 中继代理。

在配置 DHCP 中继代理之前，请确保您已配置第 3 层 Ethernet 或第 3 层 VLAN 接口，并确保已将该接口分配给某个虚拟路由器和区域。

STEP 1 | 选择 DHCP 中继。

选择 **Network**（网络）> **DHCP** > **DHCP Relay**（**DHCP** 中继）。

STEP 2 | 指定 DHCP 中继代理将要通信的各个 DHCP 服务器的 IP 地址。

1. 在 **Interface**（接口）字段中，选择希望其成为 DHCP 中继代理的接口。
2. 选择 **IPv4** 或 **IPv6**，以指明您将指定的 DHCP 服务器地址的类型。
3. 如果您已检查 **IPv4**，在 **DHCP Server IP Address**（**DHCP** 服务器 **IP** 地址）字段，**Add**（添加）将收发中继 DHCP 消息的 DHCP 服务器的地址。
4. 如果您已检查 **IPv6**，在 **DHCP Server IPv6 Address**（**DHCP** 服务器 **IPv6** 地址）字段，**Add**（添加）将收发中继 DHCP 消息的 DHCP 服务器的地址。如果指定了多播地址，请同时指定传出 **Interface**（接口）。
5. （可选）重复前三个步骤，为每个 IP 地址系列输入最多八个 DHCP 服务器地址。

STEP 3 | 提交配置。

单击 **OK**（确定）和 **Commit**（提交）。

# 对 DHCP 进行监控和故障排除

您可以查看 DHCP 服务器已分配的或已通过从 CLI 发出命令为 DHCP 客户端分配的动态地址租借的状态。您还可在租借时间结束并自动释放之前清除这些租借。

- 查看 DHCP 服务器信息
- 清除 DHCP 租借
- 查看 DHCP 客户端信息
- 收集 DHCP 的相关调试输出

## 查看 *DHCP* 服务器信息

执行此操作可以查看 DHCP 池统计信息、DHCP 服务器已分配的 IP 地址、相应的 MAC 地址、租借的状态和持续时间以及租借的开始时间。如果地址已配置为 **Reserved Address**（保留地址），`state` 列将显示 `reserved`，且不会有 `duration` 或 `lease_time`。如果租借已被配置为 **Unlimited**（无限制），`duration` 列会显示值 `0`。

- 查看 DHCP 池统计信息、DHCP 服务器分配的 IP 地址、MAC 地址、租借状态和持续时间以及租借开始时间。

```
admin@PA-220> show dhcp server lease interface all
```



© 2019 Palo Alto Networks, Inc.

```
interface: "ethernet1/2"
Allocated IPs: 1, Total number of IPs in pool: 5. 20.0000% used
ip              mac                state      duration    lease_time
192.168.3.11    f0:2f:af:42:70:cf  committed  0           Wed Jul  2
 08:10:56 2014
admin@PA-220>
```

- 查看 DHCP 服务器已分配给客户端的选项。

```
admin@PA-220> show dhcp server settings all
```

```
Interface    GW           DNS1        DNS2       DNS-Suffix Inherit source
------------------------------------------------------------------------
ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10             ethernet1/3
admin@PA-220>
```

## 清除 *DHCP* 租借

有几个清除 DHCP 租借的选项供您选择。

- 在保持计时器自动释放之前，先释放接口（服务器）的 DHCP 租借，例如 ethernet1/2。这些地址将重新成为 IP 池中的可用地址。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

- 释放特定 IP 地址的租借，例如 192.168.3.1。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

- 释放特定 MAC 地址的租借，例如 f0:2c:ae:29:71:34。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac f0:2c:ae:29:71:34
```

## 查看 *DHCP* 客户端信息

要查看在充当 DHCP 客户端时发送到防火墙的 IP 地址租借的状态，请使用其中一个 CLI 命令。

- **admin@PA-220>show dhcp client state *<interface_name>***
- **admin@PA-220> show dhcp client state all**

```
Interface       State        IP              Gateway          Leased-until
-------------------------------------------------------------------------
ethernet1/1     Bound        10.43.14.80     10.43.14.1       70315
admin@PA-220>
```


© 2019 Palo Alto Networks, Inc.

## 收集 *DHCP* 的相关调试输出

要收集 DHCP 的相关调试输出，请使用以下任一命令：

- **admin@PA-220> debug dhcpd**
- **admin@PA-220> debug management-server dhcpd**



© 2019 Palo Alto Networks, Inc.

# DNS

域名系统 (DNS) 是一种将用户友好型域名（例如 www.paloaltonetworks.com）转换成（解析到）IP 地址的协议，以便用户可以访问互联网或专用网络上的计算机、网站、服务或其他资源。


- DNS 概述
- DNS 代理对象
- DNS 服务器配置文件
- 多租户 DNS 部署
- 配置 DNS 代理对象
- 配置 DNS 服务器配置文件
- 用例 1：防火墙要求执行 DNS 解析
- 用例 2：ISP 租户使用 DNS 代理在其虚拟系统中对安全策略、报告和服务执行 DNS 解析。
- 用例 3：防火墙充当客户端和服务器之间的 DNS 代理
- DNS 代理规则和 FQDN 匹配


## DNS 概述

DNS 在实现用户对网络资源的访问方面起着至关重要的作用，因此用户无需记住 IP 地址，个人计算机也不需要存储大量映射到 IP 地址的域名。DNS 采用客户端/服务器模型；DNS 服务器通过查找其缓存中的域来为 DNS 客户端解析查询，并在必要时向其他服务器发送查询，直到可以使用相应的 IP 地址响应客户端。

域名的 DNS 结构具有层次性；域名中的顶级域名 (TLD) 可以是通用 TLD (gTLD)（如 com、edu、gov、int、mil、net 或 org（gov 和 mil 仅适用于美国））或国家/地区代码 (ccTLD)，例如 au（澳大利亚）或 us（美国）。ccTLD 通常保留用于国家和附属地区。

完全限定域名 (FQDN) 至少包括主机名、二级域和 TLD，以完全指定主机在 DNS 结构中的位置。例如，www.paloaltonetworks.com 是一个 FQDN。

但凡 Palo Alto Networks 防火墙在用户界面或 CLI 中使用 FQDN，防火墙必须使用 DNS 解析该 FQDN。根据 FQDN 查询的起源位置，防火墙会确定要用于解析查询的 DNS 设置。

FQDN 的 DNS 记录包括一个生存时间 (TTL) 值，默认情况下，防火墙将根据该 DNS 服务器提供的单独 TTL 在缓存内刷新每个 FQDN，前提是 TTL 大于或等于您在防火墙上配置的最短 FQDN 刷新时间，如未配置，则默认为 30 秒。基于 TTL 值刷新 FQDN 对于保证云端平台服务访问尤为关键，其通常需要频繁的 FQDN 刷新以确保服务的高度可用性。例如，支持自动扩展的云端环境取决于对动态服务扩展的 FQDN 解析，而 FQDN 的快速解析是此时间敏感环境下的关键要素。

通过配置最短 FQDN 刷新时间，您可以限制防火墙需要遵循的 TTL 值。如果您的 IP 地址不会经常更改，您可能需要设置较大的最短 FQDN 刷新时间，以免防火墙进行不必要的条目刷新。防火墙使用以下二者中的较大者：DNS TTL 时间和所配置的最短 FQDN 刷新时间。

例如，两个 FQDN 的 TTL 值如下。最短 FQDN 刷新时间代替较小（更快的）TTL 值。

| | TTL | 如果最短 FQDN 刷新时间 = 26 | 实际刷新时间 |
|---|---|---|---|
| FQDN A | 20 | | 26 |
| FQDN B | 30 | | 30 |

FQDN 刷新计时器在防火墙收到 DNS 服务器或解析 FQDN 的 DNS 代理对象的 DNS 响应时启动。



© 2019 Palo Alto Networks, Inc.

此外，您可以设置 失效超时以配置当无法访问 DNS 服务器时，防火墙继续使用失效（超时）FQDN 解析的时间。若在失效超时时间结束时，如果仍无法访问 DNS 服务器，失效 FQDN 条目将变为未解析（防火墙移除失效 FQDN 条目）。

以下防火墙任务与 DNS 有关：

- 使用至少一个 DNS 服务器配置防火墙，以便解析主机名。配置 DNS 主服务器或 DNS 辅助服务器或指定此类服务器的 DNS 代理对象，如用例 1：防火墙要求执行 DNS 解析中所示。
- 自定义防火墙如何处理每个虚拟系统的安全策略规则、报告和管理服务（如电子邮件、Kerberos、SNMP、syslog 等）发起的 DNS 解析，如用例 2：ISP 租户使用 DNS 代理在其虚拟系统中对安全策略、报告和服务执行 DNS 解析所示。
- 配置防火墙作为客户端的 DNS 服务器，如用例 3：防火墙充当客户端和服务器之间的 DNS 代理所示。
- 配置反间谍软件配置文件以使用 DNS 查询来确定网络上受感染的主机。
- 启用规避签名，然后启用规避签名以进行威胁防护。
- 将接口配置为 DHCP 服务器。为此，防火墙能够充当 DHCP 服务器，并将 DNS 信息发送到其 DHCP 客户端，这样所配置的 DHCP 客户端便可访问各自的 DNS 服务器。

# DNS 代理对象

配置为 DNS 代理时，防火墙是 DNS 客户端和服务器之间的中介；它通过解析来自其 DNS 代理缓存的查询来充当 DNS 服务器。如果在 DNS 代理缓存中找不到域名，则防火墙会在特定 DNS 代理对象（位于 DNS 查询到达的接口上）的条目中搜索域名的匹配项。防火墙根据匹配结果将查询转发到相应的 DNS 服务器。如果找不到匹配，防火墙将使用默认 DNS 服务器。

在 DNS 代理对象上，可配置确定防火墙以何种方式充当 DNS 代理的相应设置。您可以将 DNS 代理对象分配给单个虚拟系统，或者让所有虚拟系统共享一个 DNS 代理。

- 如果为虚拟系统配置了 DNS 代理对象，您可以指定DNS 服务器配置文件，该文件指定了主辅 DNS 服务器地址，以及其他信息。DNS 服务器配置文件可以简化配置。
- 如果共享 DNS 代理对象，则必须至少指定 DNS 服务器的主地址。



当通过 *DNS* 服务配置多个租户（*ISP* 订户）时，每个租户应拥有已定义的专用 *DNS* 代理，用于区分该租户的 *DNS* 服务与其他租户的服务。

在代理对象中，指定防火墙为其充当 DNS 代理的接口。该接口的 DNS 代理不使用服务路由；始终将对 DNS 请求作出的响应发送到分配给 DNS 请求到达的虚拟路由器的接口。

当您配置 DNS 代理对象时，可以为 DNS 代理提供静态的 FQDN 到地址的映射。您还可以创建 DNS 代理规则，以控制域名查询（与代理规则相匹配）定向到的 DNS 服务器。在防火墙上最多可以配置 256 个 DNS 代理对象。如果此 DNS 代理对象被分配给 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **DNS** 或**Device**（设备）> **Virtual Systems**（虚拟系统）> **vsys** > **General**（常规）> **DNS Proxy**（**DNS** 代理），则必须启用 **Cache**（缓存）和 **Cache EDNS Responses**（缓存 EDNS 响应）（在**Network**（网络）> **DNS Proxy**（**DNS** 代理）> **Advanced**（高级）下）。此外，如果此 DNS 代理对象配置有 **DNS proxy rules**（**DNS** 代理规则），那么这些规则还需启用缓存（打开此映射解析出的域缓存）。

当防火墙接收到 FQDN 查询（并且域名不在 DNS 代理缓存中）时，防火墙将从 FQDN 查询中获得域名与 DNS 代理对象的 DNS 代理规则中的域名进行比较。如果在单个 DNS 代理规则中指定多个域名，只要查询与规则中任何一个域名相匹配，则说明查询与规则匹配。DNS 代理规则和 FQDN 匹配描述防火墙如何确定 FQDN 是否与 DNS 代理规则中的域名相匹配。将与规则匹配的 DNS 查询发送到配置用于待解析的代理对象的 DNS 主服务器。

# DNS 服务器配置文件

要简化虚拟系统配置，DNS 服务器配置文件允许指定要配置的虚拟系统，继承源或 DNS 服务器的主辅 IP 地址，以及将在已发送到 DNS 服务器的数据包中使用的源接口和源地址（服务路由）。源接口确定虚拟路由器，该路由器具有路由表。在分配了源接口的虚拟路由器的路由表中查询目标 IP 地址。目标 IP egress 接口



© 2019 Palo Alto Networks, Inc.

的查询结果可能会与源接口的不同。数据包会离开通过路由表查询确定的目标 IP Ingress 接口，但是源 IP 地址会是配置的地址。源地址可用作 DNS 服务器回复的目标地址。

如果为虚拟系统指定了 DNS 服务器，虚拟系统报告和虚拟系统服务器配置文件会向该服务器发送查询。（在 **Device**（设备）> **Virtual Systems**（虚拟系统）> **General**（常规）> **DNS Proxy**（**DNS** 代理）中定义已使用的 DNS 服务器。）如果没有为虚拟系统指定 DNS 服务器，则会查询为防火墙指定的 DNS 服务器。

配置 DNS 服务器配置文件仅适用于虚拟系统；不适用于全局共享位置。

## 多租户 DNS 部署

防火墙会根据申请起源确定如何处理 DNS 请求。ISP 在防火墙上有多个租户的环境称为多租户。多租户 DNS 部署具有以下三种用例：

- 全局管理 **DNS** 解析 — 出于自身目的，防火墙需要 DNS 解析，例如，使用来自管理面板的请求为管理事件（如软件更新服务）解析 FQDN。防火墙使用服务路由连接到 DNS 服务器，因为特定虚拟路由器上并没有传入 DNS 请求。
- 虚拟系统的策略和报告 **FQDN** 解析 — 对于来自安全策略、报告或服务中的 DNS 查询，您可以指定一套特定于虚拟系统（租户）的 DNS 服务器，或者默认为全局 DNS 服务器。如果您的用例需要每个虚拟系统使用不同的 DNS 服务器集，则必须配置 DNS 代理对象。解析特定于分配了 DNS 代理的虚拟系统。如果没有适用于该虚拟系统的特定 DNS 服务器，防火墙则使用全局 DNS 设置。
- 虚拟系统的数据面板 **DNS** 解析 — 这种方法也称为 DNS 解析的网络请求。可以配置租户的虚拟系统，这样就可以在专用网络中的租户的 DNS 服务器上解析特定域名。这种方法支持拆分 *DNS*，意思是对于在其服务器上未解析的剩余 DNS 查询，租户也可以使用专用 ISP DNS 服务器。DNS 代理对象规则控制拆分 DNS；租户的域将 DNS 请求重定向到其专用 DNS 服务器（在 DNS 服务器配置文件中配置这些服务器）。DNS 服务器配置文件指定主辅 DNS 服务器，也指定适用于 IPv4 和 IPv6 的 DNS 服务路由，这样会覆盖默认的 DNS 设置。

下表对 DNS 解析类型进行了汇总。绑定位置确定用于解析的 DNS 代理对象。为了进行说明，用例显示了服务提供商可能如何配置 DNS 设置以提供防火墙以及租户（订户）虚拟系统所需的用于解析 DNS 查询的 DNS 服务。

| 解析类型 | 位置:共享 | 位置:特定 Vsys |
|---|---|---|
| 防火墙 DNS 解析 — 通过管理面板执行此任务 | 绑定：全局<br>如用例 1 所示 | N/A |
| 安全配置文件，报告和服务器配置文件解析 — 通过管理面板执行 | 绑定：全局<br>与用例 1 的行为相同 | 绑定：特定 vsys<br>如用例 2 所示 |
| 连接到防火墙上的接口的 DNS 客户端主机的 DNS 代理解析，经由防火墙连接到 DNS 服务器 — 通过数据面板执行 | 绑定：接口<br>服务路由：接收到 DNS 请求的接口和 IP 地址。<br>如用例 3 所示 | |

- 用例 1：防火墙要求执行 DNS 解析
- 用例 2：ISP 租户使用 DNS 代理在其虚拟系统中对安全策略、报告和服务执行 DNS 解析
- 用例 3：防火墙充当客户端和服务器之间的 DNS 代理

## 配置 DNS 代理对象

如果防火墙要充当虚拟系统的 DNS 代理，请执行此任务来配置 DNS 代理对象。既可以在所有虚拟系统中共享代理对象，也可以将代理对象应用到特定虚拟系统。


© 2019 Palo Alto Networks, Inc.

如果防火墙启用为 *DNS* 代理时，当客户端连接到非源 *DNS* 请求中指定的域时，用于检测创建的 *HTTP* 或 *TLS* 请求的规避签名将发出警报。最佳做法是，在配置 *DNS* 代理后启用规避签名，以在检测到创建的请求时触发警报。

STEP 1 | 配置 DNS 代理对象的基本设置。

1. 选择 **Network**（网络）> **DNS Proxy**（**DNS** 代理），然后 **Add**（添加）一个新对象。
2. 确认已选中 **Enable**（启用）。
3. 输入对象的 **Name**（名称）。
4. 对于 **Location**（位置），请选择对象要应用到的虚拟系统。如果您选择 **Shared**（共享），则必须至少指定 **Primary**（主）DNS 服务器地址和 **Secondary**（辅助）地址（可选）。
5. 如果您选择了虚拟系统，对于 **Server Profile**（服务器配置文件），请选择 DNS 服务器配置文件或单击 **DNS Server Profile**（**DNS** 服务器配置文件）以配置新的配置文件。请参阅配置 DNS 服务器配置文件。
6. 对于继承源，选择要从中继承默认 DNS 服务器设置的源。默认值是 **None**（无）。
7. 对于 **Interface**（接口），单击 **Add**（添加），然后指定 DNS 代理对象要应用到的接口。
   - 如果您使用 DNS 代理对象来执行 DNS 查找，则需要指定接口。防火墙会侦听该接口上的 DNS 请求，然后代理这些请求。
   - 如果您使用服务路由的 DNS 代理对象，该接口为可选接口。

STEP 2 | （可选）指定 DNS 代理规则。

1. 在 **DNS Proxy Rules**（**DNS** 代理规则）选项卡上，**Add**（添加）规则的 **Name**（名称）。
2. 如果想要防火墙缓存已解析的域，请 **Turn on caching of domains resolved by this mapping**（为此映射解析的域启用缓存）。
3. 对于 **Domain Name**（域名），**Add**（添加）一个或多个域，每行一个条目，以便防火墙对 FQDN 查询进行比较。如果查询与规则中的一个域匹配，则查询将发送到以下服务器之一进行解析（具体取决于在先前步骤中配置的内容）：
   - 直接为此代理对象指定的 **Primary**（主）或 **Secondary**（辅助）DNS 服务器。
   - 直接为此代理对象的 DNS 服务器配置文件指定的 **Primary**（主）或 **Secondary**（辅助）DNS 服务器。

   DNS 代理规则和 FQDN 匹配描述了防火墙如何将 FQDN 中的域名与 DNS 代理规则进行匹配。如果找不到匹配，则默认 DNS 服务器解析查询。
4. 执行以下操作之一，具体取决于您的 **Location**（位置）的设置：
   - 如果您选择虚拟系统，则选择 **DNS Server profile**（**DNS** 服务器配置文件）。
   - 如果您选择 **Shared**（共享），则输入 **Primary**（主）地址和 **Secondary**（辅助）地址（可选）。
5. 单击 **OK**（确定）。

STEP 3 | （可选）可以为 DNS 代理提供静态的 FQDN 到地址的条目。静态 DNS 条目允许防火墙在未发送查询到 DNS 服务器的情况下将 FQDN 解析为 IP 地址。

1. 在 **Static Entries**（静态条目）选项卡上，**Add**（添加）**Name**（名称）。
2. 输入完全限定域名 (**FQDN**)。
3. 对于 **Address**（地址），**Add**（添加）FQDN 应映射到的 IP 地址。

   您可以为条目提供其他 IP 地址。防火墙将在其 DNS 响应中提供所有 IP 地址，客户端则选择要使用的地址。
4. 单击 **OK**（确定）。

STEP 4 | 启用高速缓存，并配置 DNS 代理的其他高级设置。

1. 在 **Advanced**（高级）选项卡上，选中 **TCP Queries**（**TCP** 查询）可启用使用 TCP 的 DNS 查询。



© 2019 Palo Alto Networks, Inc.

- **Max Pending Requests**（最大挂起请求数）— 输入防火墙将支持的并发暂挂 TCP DNS 请求数的上限（范围为 64 至 256，默认为 64）。

2. 对于 **UDP Queries Retries**（**UDP** 查询重试），请输入：
   - **Interval(sec)**（间隔，秒）— 在未收到任何响应的情况下再次发送请求的间隔秒数（范围为 1-30，默认为 2）。
   - **Attempts**（尝试）— 在查询下一个 DNS 服务器之前的 UDP 最大查询次数（不包括第一次尝试）（范围为 1-30，默认为 5。）
3. 选择 **Cache**（缓存），启用防火墙来缓存其发现的 FQDN 到地址映射。如果此 DNS 代理对象用于防火墙生成的查询（即在**Device**（设备）> **Setup**（设置）> **Services**（服务）> **DNS**或在**Device**（设备）> **Virtual Systems**（虚拟系统）下），默认必须启用**Cache**（缓存），并选择一个虚拟系统和 **General** > **DNS Proxy**（通用 **DNS** 代理）。
   - 选择 **Enable TTL**（启用 **TTL**）— 限制防火墙缓存代理对象的 DNS 解析条目的时间长度。默认情况下禁用。
     - 输入 **Time to Live (sec)**（生存时间，秒），在该秒数后将删除代理对象的所有缓存条目。条目删除后，必须解析新的 DNS 请求并再次缓存。范围为 60-86,400。未设置默认 TTL；条目一直保留，直到防火墙用完缓存内存。
   - **Cache EDNS Responses**（缓存 **EDNS** 响应）— 如果此 DNS 代理对象用于防火墙生成的查询（即在 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **DNS**或在**Device**（设备）> **Virtual Systems**（虚拟系统）下），必须启用此设置，并选择一个虚拟系统和 **General** > **DNS Proxy**（通用 **DNS** 代理）。

STEP 5 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

# 配置 DNS 服务器配置文件

配置 DNS 服务器配置文件，以简化虚拟系统配置。**Primary DNS**（主 **DNS**）或 **Secondary DNS**（辅助 **DNS**）地址用于创建虚拟系统发送至 DNS 服务器的 DNS 请求。

STEP 1 | 指定 DNS 服务器配置文件的名称，请选择其要应用到的虚拟系统，然后指定主辅 DNS 服务器地址。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **DNS**，并 **Add**（添加）DNS 服务器配置文件的 **Name**（名称）。
2. 对于 **Location**（位置），请选择配置文件要应用到的虚拟系统。
3. 对于 **Inheritance Source**（继承源），如果未继承 DNS 服务器地址，请选择 **None**（无）。否则，指定配置文件应从中继承设置的 DNS 服务器。如果选择 DNS 服务器，请单击 **Check inheritance source status**（检查继承源状态）以查看相关信息。
4. 指定 **Primary DNS**（主 **DNS**）服务器的 IP 地址，或将其保留为 **inherited**（已继承）（如果选择 **Inheritance Source**（继承源））。

   请记住，如果您指定 *FQDN* 而非 *IP* 地址，则会在 *Device*（设备）> *Virtual Systems*（虚拟系统）> *DNS Proxy*（*DNS* 代理）中解析该 *FQDN* 的 *DNS*。
5. 指定 **Secondary DNS**（辅助 **DNS**）服务器的 IP 地址，或将其保留为 **inherited**（已继承）（如果选择 **Inheritance Source**（继承源））。

STEP 2 | 根据目标 DNS 服务器是否具有 IP 地址类型（IPv4 或 IPv6），配置防火墙自动使用的服务路由。

1. 单击 **Service Route IPv4**（服务路由 **IPv4**）启用要用来充当服务路由的后续接口和 IPv4 地址（如果目标 DNS 地址是 IPv4 地址）。


© 2019 Palo Alto Networks, Inc.

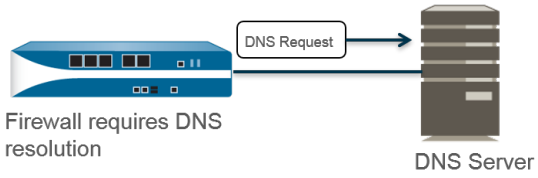
2. 指定 **Source Interface**（源接口），以便选择服务路由将使用的 DNS 服务器的源 IP 地址。防火墙确定分配给该接口的虚拟路由器，然后在虚拟路由器路由表中执行路由查找，以连接到目标网络（根据 **Primary DNS**（主 **DNS**）地址）。
3. 指定将数据包转发到的 DNS 服务器用作源地址的 IPv4 **Source Address**（源地址）。
4. 单击 **Service Route IPv6**（服务路由 **IPv6**）启用要用来充当服务路由的后续接口和 IPv6 地址（如果目标 DNS 地址是 IPv6 地址）。
5. 指定 **Source Interface**（源接口），以便选择服务路由将使用的 DNS 服务器的源 IP 地址。防火墙确定分配给该接口的虚拟路由器，然后在虚拟路由器路由表中执行路由查找，以连接到目标网络（根据 **Primary DNS**（主 **DNS**）地址）。
6. 指定将数据包转发到的 DNS 服务器用作源地址的 IPv6 **Source Address**（源地址）。
7. 单击 **OK**（确定）。

STEP 3 | 提交配置。

单击 **OK**（确定）和 **Commit**（提交）。

# 用例 1：防火墙要求执行 DNS 解析

此用例下，防火墙作为客户端，请求 FQDN 的 DNS 解析度，用于安全策略规则、报告、管理服务（如电子邮件、Kerberos、SNMP、系统日志等），以及管理时间，如软件更新服务、动态软件更新和 WildFire。在动态环境下，FQDN 更改更加频繁；准确的 DNS 解析允许防火墙执行精准的策略，提供报告和管理服务，并处理管理事件。共享的全局 DNS 服务执行管理面板功能的 DNS 解析。




STEP 1 | 配置防火墙要用于其 DNS 解析的主辅 DNS 服务器。

必须在防火墙上手动配置至少一个 *DNS* 服务器，否则无法解析主机名；防火墙不会使用其他来源（如 *ISP*）上的 *DNS* 服务器设置。

1. 编辑服务设置（**Device**（设备）> **Setup**（设置）> **Services**（服务）> **Global**（全局）用于支持多个虚拟系统的防火墙；**Device**（设备）> **Setup**（设置）> **Services**（服务）用于不支持多个虚拟系统的防火墙）。
2. 在 **Services**（服务）选项卡上，对于 **DNS**，选择 **Servers**（服务器），然后输入 **Primary DNS Server**（主 **DNS** 服务器）地址和 **Secondary DNS Server**（辅助 **DNS** 服务器）地址。
3. 继续步骤 3。

STEP 2 | 或者，如果您要配置高级 DNS 功能，如拆分 DNS、DNS 代理覆盖、DNS 代理规则、静态条目或 DNS 继承，可以配置 DNS 代理对象。

1. 编辑服务设置（**Device**（设备）> **Setup**（设置）> **Services**（服务）> **Global**（全局）用于支持多个虚拟系统的防火墙；**Device**（设备）> **Setup**（设置）> **Services**（服务）用于不支持多个虚拟系统的防火墙）。
2. 在 **Services**（服务）选项卡上，对于 **DNS**，请单击 **DNS Proxy Object**（**DNS** 代理对象）。
3. 从 **DNS Proxy**（**DNS** 代理）列表中，选择要用于配置全局 DNS 服务的 DNS 代理，或选择 **DNS Proxy**（**DNS** 代理）来配置新的 DNS 代理对象，如下所示：

    1. **Enable**（启用），然后输入 DNS 代理对象的 **Name**（名称）。



© 2019 Palo Alto Networks, Inc.

2. 在支持多个虚拟系统的防火墙上，对于 **Location**（位置），请选择 **Shared**（共享）以用于全局防火墙范围的 DNS 代理服务。

   共享的 *DNS* 代理对象不使用 *DNS* 服务器配置文件，因为他们不需要属于租户虚拟系统的特定服务路由。

3. 输入 **Primary**（主）DNS 服务器 IP 地址。（可选）输入 **Secondary**（辅助）DNS 服务器 IP 地址。
4. 选择 **Advanced**（高级）选项卡。确保 **Cache**（缓存）和 **Cache EDNS Responses**（缓存 **EDNS** 响应）均已启用（两者均默认启用）。
5. 单击 **OK**（确定）以保存 DNS 代理对象。

STEP 3 | （可选）设置 **Minimum FQDN Refresh Time (sec)**（最短 **FQDN** 刷新时间）（秒）以限制防火墙刷新 FQDN 缓存条目的频率。

默认状态下，防火墙基于单个 TTL，根据 DNS 记录内的 FQDN，在各 FQDN 缓存内刷新 FQDN，前提是 TTL 大于或等于最小的 FQDN 刷新设置（或前提是 TTL 大于或等于 30 秒的默认设置，如果您没有配置最短 FQDN 刷新时间）。要设置最短 FQDN 刷新时间，输入以秒为单位的数值（范围为 0 至 14,400；默认为 30）。设置为 0 表示防火墙将根据 DNS 记录中的 TTL 值刷新 FQDN；防火墙不会强制执行最短 FQDN 刷新时间。防火墙使用较大的 DNS TTL 时间和最短 FQDN 刷新时间。

如果 *DNS* 中 *FQDN* 的 *TTL* 较短，但 *FQDN* 解析不会随 *TTL* 时间段那样频繁更改，导致无需更快的更新，则您必须设置最短 *FQDN* 刷新时间，以避免不必要的 *FQDN* 刷新尝试。

STEP 4 | （可选）指定 **FQDN Stale Entry Timeout**（**FQDN** 失效条目超时）**(min)**（分钟），该时间是当无法访问 DNS 服务器时，防火墙可持续使用失效 FQDN 解析的分钟数（范围为 0 至 10,080；默认为 1,440）。

设置为 0 意味着防火墙不会继续使用失效 FQDN 条目。

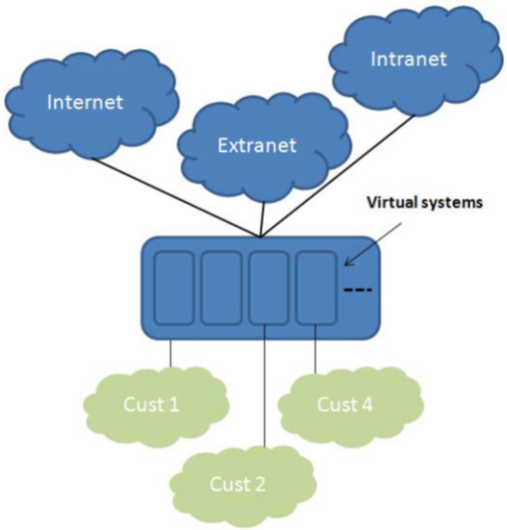
确保 *FQDN Stale Entry Timeout*（*FQDN* 失效条目超时）足够短，不会允许错误的流量转发（这会带来安全风险），但又足够长，以允许流量连续移动，不会导致计划外的网络中断。

STEP 5 | 单击 **OK**（确定）和 **Commit**（提交）。

## 用例 2：ISP 租户使用 DNS 代理在其虚拟系统中对安全策略、报告和服务执行 DNS 解析。

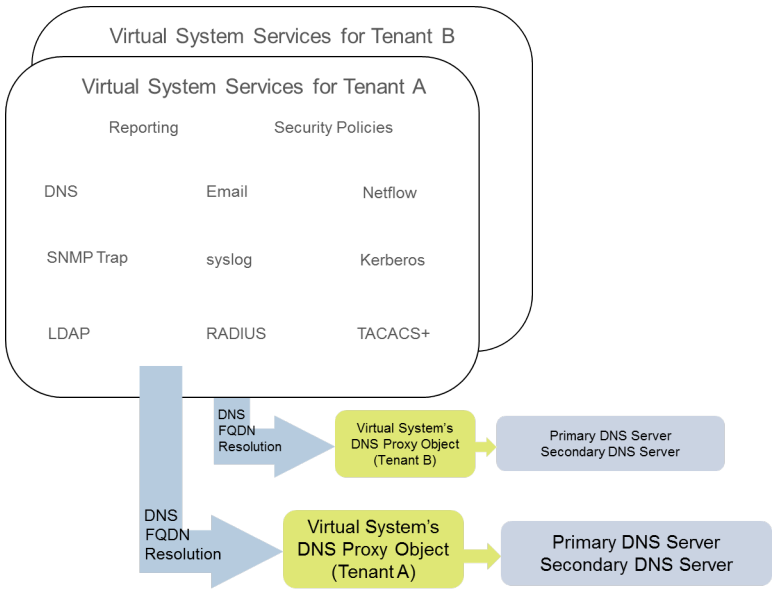
在此用例中，在防火墙上定义多个租户（ISP 订户），并将每个租户分配给独立的虚拟系统 (vsys) 虚拟路由器，以便为其服务和管理域分配网段。下图说明了防火墙中配置的多个虚拟系统。


© 2019 Palo Alto Networks, Inc.




对于在其专用网络中定义的安全策略规则、报告和管理服务（如电子邮件、Kerberos、SNMP、syslog 以及其他服务），每个租户都有专用服务器配置文件。

针对通过上述服务发起的 DNS 解析，为每个虚拟系统都已配置专用DNS 代理对象，允许每个租户自定义在其虚拟系统中执行 DNS 解析的方式。包含 **Location**（位置）的所有服务都会使用为虚拟系统配置的 DNS 代理对象，用于确定解析 FQDN 的主（或辅助）DNS 服务器，如下图所示。




STEP 1 | 针对每个虚拟系统，请指定要使用的 DNS 代理。

1. 选择 **Device**（设备）> **Virtual Systems**（虚拟系统）并 **Add**（添加）虚拟系统的 **ID**（范围是 1-255）和可选 **Name**（名称），在本例中为 Corp1 Corporation。
2. 在 **General**（常规）选项卡上，选择 **DNS Proxy**（**DNS** 代理）或创建一个新代理。在此实例中，选择 Corp1 DNS 代理作为 Corp1 公司的虚拟系统的代理。
3. 对于 **Interfaces**（接口），单击 **Add**（添加）。在此实例中，Ethernet1/20 专用于该租户。
4. 对于 **Virtual Routers**（虚拟路由器），单击 **Add**（添加）。将命名为 Corp1 VR 的虚拟路由器分配给虚拟系统，以划分路由功能。
5. 单击 **OK**（确定）。

STEP 2 | 配置 DNS 代理和服务器配置文件来支持虚拟系统的 DNS 解析。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **DNS Proxy**（**DNS** 代理），然后单击 **Add**（添加）。
2. 单击 **Enable**（启用），然后输入 DNS 代理的 **Name**（名称）。
3. 对于 **Location**（位置），请选择租户的虚拟系统（在此实例中为 Corp1 公司 (vsys6)）。（您也可以选择 **Shared**（共享）DNS 代理资源。）
4. 对于 **Server Profile**（服务器配置文件），请选择或创建配置文件来自定义要用来对该租户的安全策略、报告和服务器配置文件服务执行 DNS 解析的 DNS 服务器。

   如果尚未配置配置文件，在 **Server Profile**（服务器配置文件）字段中，单击 **DNS Server Profile**（**DNS** 服务器配置文件）以 配置 DNS 服务器配置文件。

   DNS 服务器配置文件会识别要用于管理该虚拟系统的 DNS 解析的主辅 DNS 服务器的 IP 地址。
5. 对于该服务器配置文件，也可配置 **Service Route IPv4**（服务路由 **IPv4**）和/或 **Service Route IPv6**（服务路由 **IPv6**）来指示要在其 DNS 请求中使用 **Source Interface**（源接口）的防火墙。如果此接口具有多个 IP 地址，还要配置 **Source Address**（源地址）。
6. 选择 **Advanced**（高级）选项卡。确保 **Cache**（缓存）和 **Cache EDNS Responses**（缓存 **EDNS** 响应）均已启用（两者均默认启用）。只要在**Device**（设备）> **Virtual Systems**（虚拟系统）> **vsys** > **General**（常规）> **DNS Proxy**（**DNS** 代理）下使用 DNS 代理对象，就必须执行此操作。
7. 单击 **OK**（确定）。
8. 单击 **OK**（确定）和 **Commit**（提交）。

   可选高级功能，例如可以使用 *DNS Proxy Rules*（*DNS* 代理规则）配置拆分 *DNS*。如果需要，可以使用单独的 *DNS* 服务器配置文件重定向将 *DNS Proxy Rule*（*DNS* 代理规则）中的 *Domain Name*（域名）与其他 *DNS* 服务器组进行匹配的 *DNS* 解析。用例 *3* 介绍了拆分 *DNS*。

   如果您在同一 DNS 代理对象中使用两个独立的 DNS 服务器配置文件，一个用于 DNS 代理，一个用于 DNS 代理规则，则会出现以下行为：

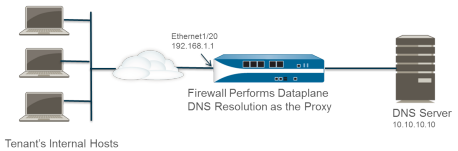
   - 如果在 DNS 代理使用的 DNS 服务器配置文件中定义服务路由，则会优先使用该服务路由。
   - 如果在 DNS 代理规则中使用的 DNS 服务器配置文件中定义服务路由，则不会使用该服务路由。如果服务路由与 DNS 代理使用的 DNS 服务器配置文件中定义的不同，在 **Commit**（提交）过程中会显示如下警告信息：

```
Warning: The DNS service route defined in the DNS proxy object is
 different from the DNS proxy rule's service route. Using the DNS proxy
 object's service route.
```

   - 如果在任何 DNS 服务器配置文件中都没定义服务路由，如果需要，则使用全局服务路由。

## 用例 3：防火墙充当客户端和服务器之间的 DNS 代理

在此用例中，防火墙位于 DNS 客户端和 DNS 服务器之间。配置防火墙上的 DNS 代理充当连接到防火墙接口的租户网络上驻留的主机的 DNS 服务器。在这种情况下，防火墙会在其数据面板上执行 DNS 解析。




这种情况会使用拆分 *DNS* 配置，即根据域名匹配配置 DNS 代理规则以将 DNS 请求重定向到 DNS 服务器组。如果没有匹配，服务器配置文件确定向其发送请求的 DNS 服务器，因此具有上述两种拆分 DNS 解析方法。


© 2019 Palo Alto Networks, Inc.

对于数据面板 *DNS* 解析，将 *PAN-OS* 中的 *DNS* 代理连接到外部 *DNS* 服务器的源 *IP* 地址会是代理的 *IP* 地址（源请求的目标 *IP*）。不使用在 *DNS* 服务器配置文件中定义的任何服务路由。例如，如果将请求从主机 *172.16.1.1* 发送到位于 *192.168.1.1* 的 *DNS* 代理，则发送到 *DNS* 服务器（位于 *10.10.10.10*）的请求会使用 *192.168.1.1* 的来源和 *10.10.10.10* 的目的地。

STEP 1 | 选择 **Network**（网络）> **DNS Proxy**（**DNS** 代理），然后单击 **Add**（添加）。

STEP 2 | 单击 **Enable**（启用），然后输入 DNS 代理的 **Name**（名称）。

STEP 3 | 对于 **Location**（位置），请选择租户的虚拟系统（在此实例中为 Corp1 公司 (vsys6)）。

STEP 4 | 对于 **Interface**（接口），选择将从租户主机（在此实例中为 Ethernet1/20）接收 DNS 请求的接口。

STEP 5 | 选择或创建 **Server Profile**（服务器配置文件）以自定义 DNS 服务器，用于解析该租户的 DNS 请求。

STEP 6 | 在 **DNS Proxy Rules**（**DNS** 代理规则）选项卡上，**Add**（添加）规则的 **Name**（名称）。

STEP 7 | （可选）选择 **Turn on caching of domains resolved by this mapping**（为此映射解析的域启用缓存）。

STEP 8 | **Add**（添加）一个或多个 **Domain Name**（域名），每行一个条目。DNS 代理规则和 FQDN 匹配描述了防火墙如何将 FQDN 与 DNS 代理规则中的域名进行匹配。

STEP 9 | 对于 **DNS Server profile**（**DNS** 服务器配置文件），选择一个配置文件。防火墙会将 DNS 请求中的域名与 **DNS Proxy Rules**（**DNS** 代理规则）中定义的域名进行对比。如果有匹配，会使用规则中定义的 **DNS Server profile**（**DNS** 服务器配置文件）确定 DNS 服务器。

STEP 10 | 在此实例中，如果请求中的域与 myweb.corp1.com 相匹配，则使用在 myweb DNS 服务器配置文件中定义的 DNS 服务器。如果没有匹配，则使用在 **Server Profile**（服务器配置文件）（Corp1 DNS 服务器配置文件）中定义的 DNS 服务器。

STEP 11 | 双击 **OK**（确定）。

## DNS 代理规则和 FQDN 匹配

当您通过使用 DNS 代理规则的 DNS 代理对象配置防火墙时，防火墙将 DNS 查询中的 FQDN 与 DNS 代理规则的域名进行比较。防火墙的比较工作如下：

| FQDN 与 DNS 代理规则的比较 | 例如 |
|---|---|
| 首先，防火墙在 DNS 代理规则中标记 FQDN 和域名。在域名中，由英文句点 (.) 分隔的字符串是一个标记。 | **`*.boat.fish.com`** 由四个标记组成：**`[*][boat][fish][com]`** |
| 匹配过程是在规则中的 FQDN 和域名之间进行标记精确匹配的过程；部分字符串不匹配。 | 规则：**`fishing`**<br>FQDN：**`fish`** — 不匹配 |
| 精确匹配要求的例外情况是使用通配符（星号 *）。* 匹配一个或多个标记。 | 规则：**`*.boat.com`** |



© 2019 Palo Alto Networks, Inc.

| FQDN 与 DNS 代理规则的比较 | 例如 |
| --- | --- |
| 这意味着仅通配符 (*) 组成的规则与任何带有一个或多个标记的 FQDN 匹配。 | FQDN：**www.boat.com** — 匹配<br>FQDN：**www.blue.boat.com** — 匹配<br>FQDN：**boat.com** — 不匹配 |
| | 规则：*****<br>FQDN：**boat** — 匹配<br>FQDN：**boat.com** — 匹配<br>FQDN：**www.boat.com** — 匹配 |
| 您可以在任何位置使用 *：头部标记、中间标记或尾部标记（但不可用于一个标记中的其他字符）。 | 规则：**www.*.com**<br>FQDN：**www.boat.com** — 匹配<br>FQDN：**www.blue.boat.com** — 匹配 |
| | 规则：**www.boat.***<br>FQDN：**www.boat.com** — 匹配<br>FQDN：**www.boat.fish.com** — 匹配 |
| | 规则：**www.boat*.com** — 无效 |
| 多个通配符 (*) 可以出现在域名的任何位置：头部标记、中间标记或尾部标记。每个非连续 * 匹配一个或多个标记。 | 规则：**a.*.d.*.com**<br>FQDN：**a.b.d.e.com** — 匹配<br>FQDN：**a.b.c.d.e.f.com** — 匹配<br>FQDN：**a.d.d.e.f.com** — 匹配（第一个 ***** 与 **d** 匹配；第二个 ***** 与 **e** 和 **f** 匹配）<br>FQDN：**a.d.e.f.com** — 不匹配（第一个 ***** 与 **d** 匹配；规则中随后的 **d** 不匹配） |
| 在连续标记中使用通配符时，第一个 * 匹配一个或多个标记；第二个 * 匹配一个标记。<br>这意味着仅 *.* 组成的规则匹配任何具有两个或多个标记的 FQDN。 | 头部标记的连续通配符：<br>规则：***.*.boat.com**<br>FQDN：**www.blue.boat.com** — 匹配<br>FQDN：**www.blue.sail.boat.com** — 匹配 |
| | 标记之间的连续通配符：<br>规则：**www.*.*.boat.com**<br>FQDN：**www.blue.sail.boat.com** — 匹配<br>FQDN：**www.big.blue.sail.boat.com** — 匹配 |
| | 尾部标记的连续通配符：<br>规则：**www.boat.*.***<br>FQDN：**www.boat.fish.com** — 匹配<br>FQDN：**www.boat.fish.ocean.com** — 匹配 |


© 2019 Palo Alto Networks, Inc.

| FQDN 与 DNS 代理规则的比较 | 例如 |
| --- | --- |
| | 仅连续通配符：<br>规则：*.*<br>FQDN：**boat** — 不匹配<br>FQDN：**boat.com** — 匹配<br>FQDN：**www.boat.com** — 匹配 |
| 连续和非连续通配符可以出现在同一规则中。 | 规则：**a.*.d.*.*.com**<br>FQDN：**a.b.c.d.e.f.com** — 匹配（第一个 * 与 **b** 和 **c** 匹配，第二个 * 与 **e** 匹配，第三个 * 与 **f** 匹配） <br>FQDN：**a.b.c.d.e.com** — 不匹配（第一个 * 与 **b** 和 **c** 匹配；第二个 * 与 **e** 匹配；第三个 * 不匹配） |
| 隐式尾部匹配行为提供一种额外的速记法：<br>只要规则的最后一个标记不是 *，如果规则中所有标记都与 FQDN 匹配，即使 FQDN 还有规则不具有的其他尾部标记，比较结果仍会是匹配。 | 规则：**www.boat.fish**<br>FQDN：**www.boat.fish.com** — 匹配<br>FQDN：**www.boat.fish.ocean.com** — 匹配<br>FQDN：**www.boat.fish** — 匹配 |
| 此规则以 * 结尾，因此隐式尾部匹配规则不适用。* 表现如下：与一个或多个标记相匹配。 | 规则：**www.boat.fish.***<br>FQDN：**www.boat.fish.com** — 匹配<br>FQDN：**www.boat.fish.ocean.com** — 匹配<br>FQDN：**www.boat.fish** — 不匹配（此 FQDN 没有与规则中的 * 相匹配的标记。） |
| 当 FQDN 与多个规则相匹配时，分裂算法选择最特定（最长）的规则；也就是说，该算法有利于具有较多标记和较少通配符 (*) 的规则。 | 规则1：***.fish.com** — 匹配<br>规则2：***.com** — 匹配<br>规则3：**boat.fish.com** — 匹配和平局<br>FQDN：**boat.fish.com**<br>FQDN 与三个规则全部匹配；防火墙是最特定的，因此使用规则 3。 |
| | 规则1：***.fish.com** — 不匹配<br>规则2：***.com** — 匹配<br>规则3：**boat.fish.com** — 不匹配<br>FQDN：**fish.com**<br>FQDN 与规则 1 不匹配，因为 * 没有匹配的标记。 |
| | 规则1：***.fish.com** — 匹配和平局<br>规则2：***.com** — 匹配<br>规则3：**boat.fish.com** — 不匹配<br>FQDN：**blue.boat.fish.com** |



© 2019 Palo Alto Networks, Inc.

| FQDN 与 DNS 代理规则的比较 | 例如 |
| --- | --- |
| | FQDN 与规则 1 和规则 2 匹配（因为 * 匹配一个或多个标记）。防火墙是最特定的，因此使用规则 1。 |
| 当使用通配符 (*) 和隐式尾部匹配规则时，可能会出现 FQDN 匹配多个规则的情况，并且分裂算法会对规则进行平等地权衡。<br>为避免歧义，如果具有隐式尾部匹配或通配符 (*) 的规则可以重叠，则通过指定尾部标记来替换隐式尾部匹配规则。 | 将：<br>规则：**www.boat**<br>替换为：<br>规则：**www.boat.com** |
| 最佳实践是创建 DNS 代理规则以避免歧义，获得出人意料的结果 | |
| 包含域名城中的顶级域名，以免调用可能使 FQDN 与多个规则匹配的隐式尾部匹配。 | **boat.com** |
| 如果使用通配符 (*)，请仅将其用作最左侧的标记。<br>这种做法遵循对通配符 DNS 记录和 DNS 层次性质的普遍理解。 | ***.boat.com** |
| 在规则中只使用一个 *。 | |
| 使用 * 建立与 DNS 服务器相关联的基本规则，并使用具有更多标记的规则来创建与不同服务器关联的规则的例外。<br>分裂算法将根据匹配的标记数量选择最特定的匹配。 | 规则：***.corporation.com** — DNS 服务器 A<br>规则：**www.corporation.com** — DNS 服务器 B<br>规则：***.internal.corporation.com** — DNS 服务器 C<br>规则：**www.internal.corporation.com** — DNS 服务器 D<br>FQDN：**mail.internal.corporation.com** — 与 DNS 服务器 C 匹配<br>FQDN：**mail.corporation.com** — 与 DNS 服务器 A 匹配 |


© 2019 Palo Alto Networks, Inc.

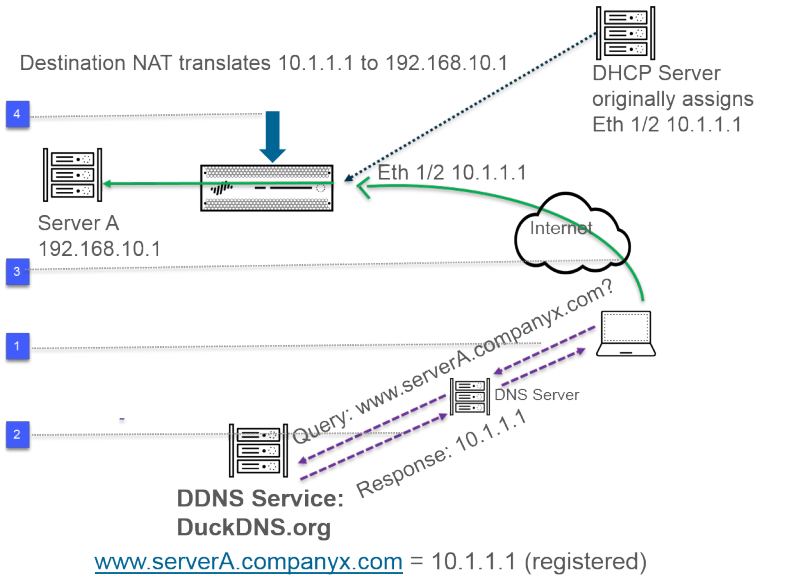
# 动态 DNS 概述

当您在防火墙后托管服务，并在防火墙上使用目标 NAT 策略访问这些服务，或者您需要提供对防火墙的远程访问时，您可以为通过动态 DNS (DDNS) 服务供应商为接口注册 IPv4 地址更改（接口为接收动态地址或具有静态地址的 DHCP 客户端）或 IPv6 地址更改（仅限静态地址）。DDNS 服务自动更新域名至 IP 地址映射，以向 DNS 客户端提供准确的 IP 地址，从而访问防火墙和防火墙后的服务。DDNS 通常用于托管服务的分支部署。防火墙接口没有了 DDNS 支持后，您需要外部部件以向客户端提供准确的 IP 地址。

防火墙支持以下 DDNS 服务供应商：DuckDNS、DynDNS、FreeDNS Afraid.org Dynamic API、FreeDNS Afraid.org 和 No-IP。单独的 DDNS 服务供应商决定其提供的服务，如支持一个主机名下有多少个 IP 地址，以及是否支持 IPv6 地址。Palo Alto Networks 利用内容更新来添加新 DDNS 服务供应商，并对其服务提供更新。

对于高可用性 *(HA)* 配置，确保 *HA* 防火墙对等设备（主动/被动或主动/主动）上的内容版本同步，因为防火墙基于当前 *Palo Alto Networks* 内容发布版本保持 *DDNS* 配置。*Palo Alto Networks* 可通过内容发布，从而更改或弃用现有 *DDNS* 服务。此外，*DDNS* 服务供应商可更改其提供的服务。*HA* 对等设备之间的内容版本不匹配可导致其使用 *DDNS* 服务的能力出现问题。

在下面的例子中，防火墙是 DDNS 服务供应商的 DDNS 客户端。最初，DHCP 服务器分配 IP 地址 10.1.1.1 至 Ethernet 1/2 接口。目标 NAT 策略将公共地址 10.1.1.1 转换为防火墙后服务器 A 的真实地址 (192.168.10.1)。

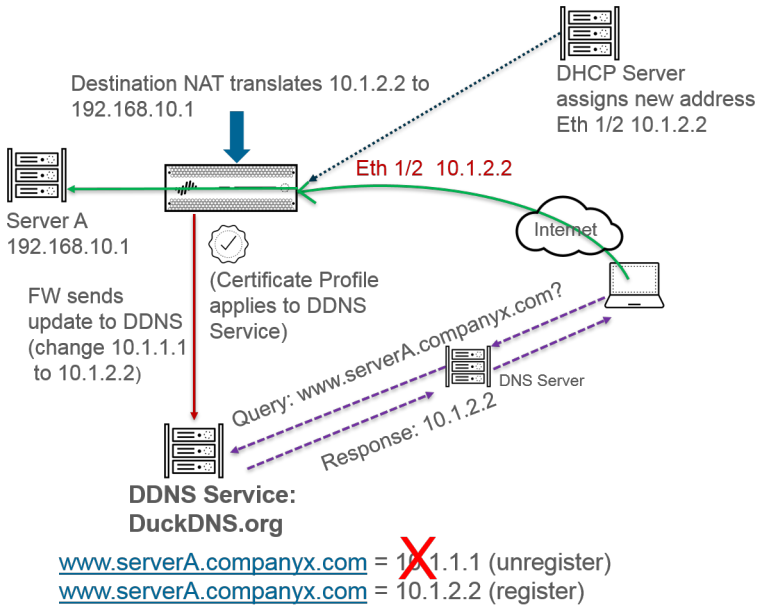



1. 当用户尝试联系 www.serverA.companyx.com 时，用户将查询该 IP 地址的本地 DNS 服务器。www.serverA.companyx.com（例如被设为 duckdns.org 记录：serverA.companyx.duckdns.org 的 CNAME）是属于 DDNS 供应商的域名（此例中为 DuckDNS）。DNS 服务器与 DDNS 提供商一同检查记录以解决查询。
2. DNS 服务器以 10.1.1.1 响应用户，这是 www.serverA.companyx.com 的 IP 地址。
3. 目标为 10.1.1.1 的用户数据包前往防火墙接口 Ethernet 1/2。
4. 此例中，防火墙执行目标 NAT 并在将数据包发送至目标之前，将 10.1.1.1 转换为 192.168.10.1。

一段时间后，DHCP 分配新的 IP 地址至防火墙接口，触发 DDNS 更新，如下所示：



© 2019 Palo Alto Networks, Inc.




1. DHCP 服务器分配新 IP 地址 (10.1.2.2) 至 Ethernet 1/2。
2. 当防火墙收到新地址时，其将带有 ww.serverA.companyx.com 新地址的更新发送至 DDNS 服务，随后由 DDNS 服务注册该新地址。（防火墙也会根据您所配置的更新间隔发送定期更新。防火墙通过 HTTPS 端口 443 发送 DDNS 更新。）

因此，在下次客户端查询 DNS 服务器以获取 www.serverA.companyx.com 的 IP 地址以及 DNS 服务器检查 DDNS 服务时，DDNS 服务将发送更新的地址 (10.1.2.2)。因此，用户将通过防火墙接口，以更新的接口地址成功访问服务或应用程序。

如果您的防火墙针对 *HA* 的主动/被动模式进行了配置，应注意该防火墙将在两个 *HA* 防火墙状态聚合时发送 *DDNS* 更新至 *DDNS* 服务。在 *HA* 状态聚合后，*DDNS* 会在被动防火墙上禁用。例如，当两个 *HA* 防火墙首次启动时，二者都将发送 *DDNS* 更新直至其确定是处于 *HA* 主动或被动模式。此间隔过程中，您仍可在系统日志内看到 *DDNS* 更新。在 *HA* 状态会聚且各防火墙通知其客户端防火墙的主动或被动状态后，被动防火墙不再发送 *DDNS* 更新。（在 *HA* 主动/主动模式下，各防火墙具有独立的 *DDNS* 配置，且不会同步该 *DDNS* 配置。）


© 2019 Palo Alto Networks, Inc.

# 为防火墙接口配置动态 DNS

在为防火墙接口配置 DDNS 之前：

- 确定您通过 DDNS 提供商注册的主机名。
- 从 DDNS 服务获得公共的 SSL 证书，并将其导入防火墙。
- （如果您使用 FreeDNS Afraid.org v1 或 FreeDNS Afraid.org Dynamic API v1）在 DDNS 服务器上，动态 DNS 服务选项卡包含下列选项：是否将相同 **IP** 的更新关联到一起？当此选项被启用时，DDNS 服务更新所有 DNS 记录内的主机名，该 DNS 记录包含了更改的旧 IP 地址，而不仅仅是单个主机名和 IP 地址的 DNS 记录。为避免更新您不希望更新的 DNS 记录，应禁用 **Link updates of the same IP together?**（是否将相同 **IP** 的更新关联到一起？）选项，从而让 DDNS 服务器仅更新包含特定主机名的 DNS 记录（带有新 IP 地址，且位于 DDNS 更新中）。

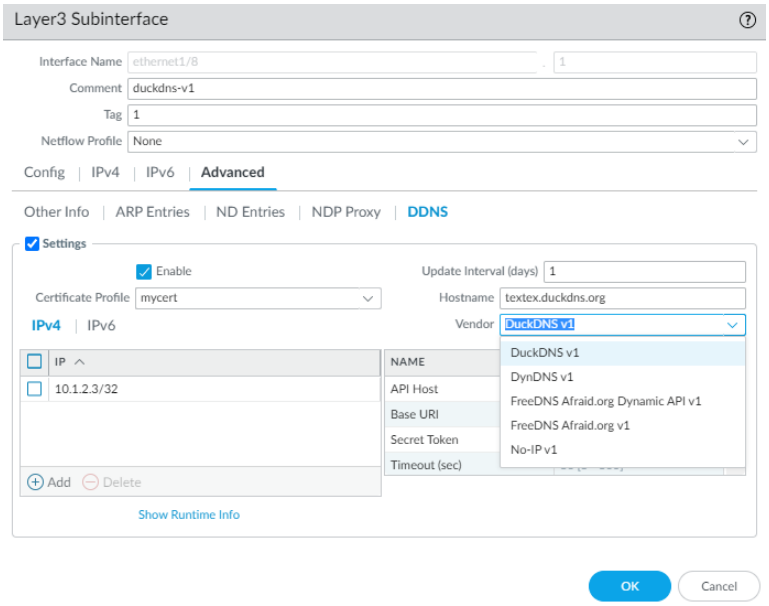
STEP 1 | 配置 DDNS。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并选择 3 层接口、子接口或聚合以太网 (AE) 接口；或选择 **Network**（网络）> **Interfaces**（接口）> **VLAN** 并选择一个接口或子接口。
2. 选择 **Advanced**（高级）> **DDNS** 并选择 **Settings**（设置）。
3. **Enable**（启用）DDNS。您必须首先启用 DDNS 进行配置。（如果您的 DDNS 配置尚未完成，您可以在不启用的情况下进行保存，这样，就不会丢失部分配置。）
4. 输入 **Update Interval (days)**（间隔时间（天）），即防火墙发送至 DDNS 服务以更新映射到 FQDN 的 IP 地址的更新间隔天数（默认为 1；范围为 1 至 30）。根据 IP 地址的更改频率选择间隔时间。（防火墙以固定间隔时间发送的更新，是除了防火墙接收到地址更改之后发送的更新之外的更新。依固定间隔发送更新是为了确保比如每次地址更改时的更新不会丢失。）
5. 输入通过 DDNS 服务注册的接口 **Hostname**（主机名）（例如，www.serverA.companyx.com 或 serverA）。

   确保此主机名与您通过 *DDNS* 服务注册的主机名相符。您应为主机名输入一个 *FQDN*；除了确认语法是否仅使用 *DNS* 允许的域名有效字符外，防火墙不会验证主机名。
6. 选择 **Ipv4** 并选择一个或多个被分配到接口的 Ipv4 地址，或 **Add**（添加）一个 Ipv4 地址与主机名关联（例如 10.1.1.1）。您只能选择 DDNS 服务允许的 IPv4 地址数。所有选中的 IPv4 地址都通过 DDNS 服务注册。选择至少一个 IPv4 或 IPv6 地址。
7. 选择 **IPv6** 并选择一个或多个被分配到接口的 IPv6 地址，或 **Add**（添加）一个 IPv6 地址与主机名关联。您只能选择 DDNS 服务允许的 IPv6 地址数。所有选中的 IPv6 地址都通过 DDNS 服务注册。选择至少一个 IPv4 或 IPv6 地址。
8. 使用从 DDNS 服务导入的 SSL 证书，选择或 创建一个新的证书配置文件（**Certificate Profile**（证书配置文件）），以便在防火墙首次连接 DDNS 服务以注册 IP 地址以及在每次更新时，验证 DDNS 服务的 SSL 证书。当防火墙连接 DDNS 服务以发送更新时，DDNS 服务为防火墙提供一个由证书颁发机构 (CA) 签名的 SSL 证书，以便防火墙验证 DDNS 服务。
9. 选择您为 DDNS 服务使用的 **Vendor**（供应商）（和版本号）。



© 2019 Palo Alto Networks, Inc.




*Palo Alto Networks* 可能通过内容更新更改支持的 *DDNS* 服务供应商。

10. 供应商的选择决定了供应商字段下方的供应商特定 **Name**（名称）和 **Value**（值）。有些值字段为只读，用于告知您防火墙用于连接到 DDNS 服务的参数。配置其他值字段，例如，DDNS 服务为您提供的密码以及防火墙在未接收到 DDNS 服务更新时使用的超时。
11. 单击 **OK**（确定）。

STEP 2 | （可选）如果您想要防火墙通过接口而非管理接口与 DDNS 服务通讯，可以为 DDNS 配置一个服务路径（为外部服务设置网络访问）。

STEP 3 | **Commit**（提交）更改。

STEP 4 | 查看接口的 DDNS 信息。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）或 **Network**（网络）> **Interfaces**（接口）> **VLAN**，然后选择您配置的接口。（配置了 DDNS 的接口在 — — 功能字段内显示 DDNS 图标。）
2. 选择 **Advanced**（高级）> **DDNS** 和 **Settings**（设置）。
3. **Show Runtime Info**（显示运行时信息）以查看接口的 DDNS 信息，包括最后返回代码（最后一次 FQDN 更新的结果）和 DDNS 服务最后一次接收到 FQDN 更新（日期和时间）。


© 2019 Palo Alto Networks, Inc.

# NAT

本部分将介绍网络地址转换 (NAT) 以及如何配置 NAT 防火墙。NAT 可将私有的不可路由 IPv4 地址转换为一个或多个全球可路由 IPv4 地址，从而节省组织的可路由 IP 地址。NAT 用于保密需要访问公共地址的主机的真实 IP 地址，通过端口转发管理流量。可以使用 NAT 解决网络社交挑战，使用相同的 IP 子网启用网络，从而进行相互通信。防火墙支持第 3 层和虚拟网线接口上的 NAT。

NAT64 选项会在 IPv6 和 IPv4 地址间转换，以使用不同的 IP 寻址方案来建立网络连接，并提供 IPv6 寻址迁移路径。IPv6-to-IPv6 Network Prefix Translation（IPv6 到 IPv6 网络前缀转换）(NPTv6) 可将一个 IPv6 前缀转换为另一个 IPv6 前缀。PAN-OS 支持所有这些功能。

如果在内部网络中使用私有 IP 地址，那么必须使用 NAT 将私有地址转换为可在外部网络上路由的公共地址。在 PAN-OS 中，您可以创建 NAT 策略规则，以向防火墙指明需要转换的数据包地址和端口，以及转换后的地址和端口。

- NAT 策略规则
- 源 NAT 和目标 NAT
- DNS 重写目标 NAT 用例
- NAT 规则容量
- 动态 IP 和端口 NAT 超额订阅
- 数据面板 NAT 内存统计信息
- 配置 NAT
- NAT 配置示例

## NAT 策略规则

- NAT 策略概述
- 已被标识为地址对象的 NAT 地址池
- NAT 地址池的代理 ARP

### *NAT* 策略概述

您至少可以配置 NAT 规则以匹配数据报的源区域和目标区域。除了区域之外，您还可以根据数据包的目标接口、源和目标地址以及服务来配置匹配条件。您可以配置多个 NAT 规则。防火墙会按照顺序自上而下地评估各个规则。如果数据包满足某个 NAT 规则的条件，那么该数据包不会采用其他 NAT 规则。因此，您的 NAT 规则列表应该按照从最具体到最不具体的顺序来排列，以让数据包采用为其创建的最具体规则。

静态 NAT 规则并不优先于其他形式的 NAT。因此，要使 NAT 工作，静态 NAT 规则必须位于防火墙上列表中其他 NAT 规则的上面。

NAT 规则提供地址转换，与安全策略规则不同，此转换允许或拒绝数据包。要了解防火墙在应用 NAT 规则和安全策略规则时所遵循的流逻辑，以便根据已定义的区域确定您所需的规则，这一点非常重要。您必须配置安全策略规则，从而允许 NAT 流量。

防火墙会进行传入数据包检查和路由查找，以确定传出接口和区域。之后，防火墙会确定数据包是否与根据源和/或目标区域定义的任一 NAT 规则相匹配。然后，防火墙会根据原始（NAT 前）的源和目标地址（而非 NAT 后区域）评估和应用与数据包匹配的所有安全策略。最后，防火墙会针对匹配的 NAT 规则对源和/或目标地址及端口号进行出口转换。

请记住，在数据包离开防火墙之前，不会对 IP 地址和端口进行转换。NAT 规则和安全策略将应用于原始 IP 地址（NAT 前地址）。NAT 规则是根据与 NAT 前 IP 地址相关的区域来配置的。

安全策略有别于 NAT 规则，因为安全策略会检查 NAT 前区域以确定数据包是否被允许。由于 NAT 的最根本目的是要修改源或目标 IP 地址（可能会导致数据包的传出接口和区域被修改），因此安全策略会被强制应用于 NAT 后区域。

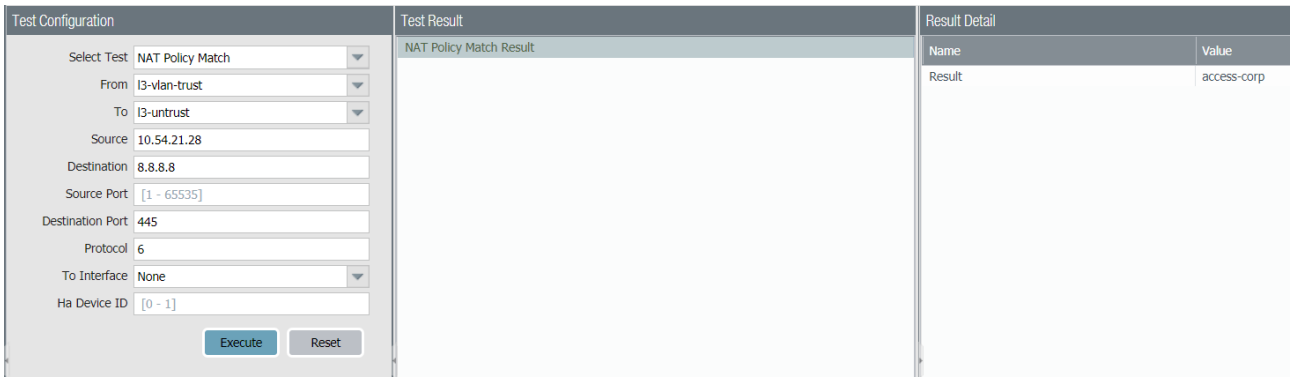


© 2019 Palo Alto Networks, Inc.

*SIP* 呼叫在经过防火墙时，有时候会出现单声道音频，因为请求管理器代表电话发送 *SIP* 消息，以建立连接。当来自请求管理器的消息抵达防火墙时，*SIP ALG* 必须将电话的 *IP* 地址通过 *NAT*。如果请求管理器和电话不在相同的安全区域，则 *NAT* 使用请求管理器区域查找电话 *IP* 地址。*NAT* 策略应该考虑这一点。

非 NAT 规则被配置为允许将随后在 NAT 策略中定义的 NAT 规则范围内所定义的 IP 地址排除。要定义非 NAT 策略，请指定所有匹配条件，并在源转换列中选择无源转换。

您可以通过选择 **Device**（设备）> **Troubleshooting**（故障排除）并测试流量是否符合 NAT 规则，以确认处理的 NAT 规则。例如：



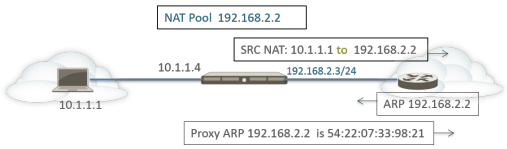

## 已被标识为地址对象的 *NAT* 地址池

在 NAT 策略规则中，在 NAT 策略规则中配置 **Dynamic IP**（动态 **IP**）或 **Dynamic IP and Port**（动态 **IP** 与端口）NAT 地址池时，通常使用地址目标配置转换后的地址池。每个地址目标可以是主机 IP 地址、IP 地址范围或 IP 子网。

由于 *NAT* 规则和安全策略规则都会使用地址对象，因此最好在命名 *NAT* 所使用的地址对象时加上前缀（如“*NAT*-名称”），以便区分这两者。

## *NAT* 地址池的代理 *ARP*

NAT 地址池未绑定到任何接口。下图演示了防火墙在为 NAT 地址池中的地址执行代理 ARP 时的行为。

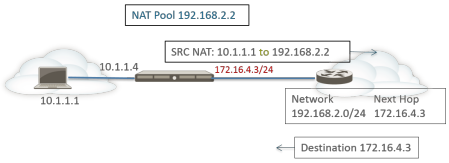



防火墙为客户端执行源 NAT，将源地址 10.1.1.1 转换为地址池中的地址 192.168.2.2。已转换数据包将发送到路由器。

对于返回流量，路由器不知道如何访问 192.168.2.2（因为此 IP 地址只是 NAT 地址池中的地址），因此它会将 ARP 请求数据包发送到防火墙。

- 如果地址池 (192.168.2.2) 与 egress/ingress 接口 IP 地址 (192.168.2.3/24) 在相同的子网内，则防火墙可以发送一个代理 ARP 回复至路由器，展示上图所示的 IP 地址的第 2 层 MAC 地址。
- 如果地址池 (192.168.2.2) 不是防火墙上接口的子网，防火墙将不会向路由器发送代理 ARP 回复。这意味着，必须使用必要的路由来配置路由器，以了解发往 192.168.2.2 数据的目的地，从而确保返回流量路由回防火墙，如下图所示。


© 2019 Palo Alto Networks, Inc.




# 源 NAT 和目标 NAT

防火墙支持源地址和/或端口转换与目标地址和/或端口转换。

- 源 NAT
- 目标 NAT

## 源 *NAT*

源 NAT 常被内部用户用于访问 Internet；源地址会被转换并保持私有状态。源 NAT 共有三类：

- 动态 **IP** 和端口 **(DIPP)** — 可将多个主机的源 IP 地址转换成带有不同端口号的相同公共 IP 地址。动态转换针对的是 NAT 地址池中的下一个可用地址，您会将其配置为 **Translated Address**（已转换地址）池中的 IP 地址、地址范围、子网或以上各项的组合。

  DIPP 可代替 NAT 地址池中的下一个地址，以让您指定 **Interface**（接口）的自有地址。在 NAT 中指定接口的好处在于：NAT 规则会自动更新为使用该接口后续获取的所有地址。DIPP 有时可以称为基于接口的 NAT 或网络地址端口转换 (NAPT)。

  DIPP 有默认的 NAT 超额订阅率，即可以同时使用同一转换后 IP 地址和端口对的次数。有关详细信息，请参阅动态 IP 和端口 NAT 超额订阅和修改 DIPP NAT 的超额订阅率。

  （仅影响未使用第二代 *PA-7050-SMC-B* 或 *PA-7080-SMC-B* 交换机管理卡的 *PA-7000* 系列防火墙）当您将点对点隧道协议*(PPTP)*与 *DIPP NAT* 一起使用时，防火墙仅对一个连接使用转换后的 *IP* 地址和端口对，且防火墙不支持 *DIPP NAT*。解决方法是更新 *PA-7000* 系列防火墙以使用第二代 *SMC-B* 卡。
- 动态 **IP** — 只会将源 IP 地址一对一地动态转换为 NAT 地址池中的下一个可用地址。NAT 池的大小应该等于需要地址转换的内部主机的数量。在默认情况下，如果源地址池大于 NAT 地址池，而且所有 NAT 地址最后都已被分配，那么需要进行地址转换的新连接将被丢弃。要覆盖此默认行为，请使用 **Advanced (Dynamic IP/Port Fallback)**（高级（动态 **IP**/端口回退））以在必要时使用 DIPP 地址。当会话终止时，或当池中的地址变为可用地址时，它们都可被分配用于转换新连接。

  动态 IP NAT 支持 保留动态 IP NAT 地址 的选项。
- 静态 **IP** — 可对源 IP 地址进行一对一的静态转换，但源端口将保持不变。静态 IP 转换常用于必须可供互联网使用的内部服务器。

## 目标 *NAT*

当防火墙将目标地址转换为不同的目标地址时，会对传入数据包执行目标 NAT。例如，将公共目标地址转换为私有目标地址时。目标 NAT 还提供执行端口转发或端口转换的选项。

目标 NAT 允许静态和动态转换：

- 静态 **IP** — 可使用多种格式配置的一种一对一的静态转换。只要已转换数据包格式相同且指定相同数量的 IP 地址，您可以指定原始数据包具有单个目标 IP 地址、IP 地址范围或 IP 网络掩码。防火墙每次都将原始目标地址静态转换成相同的已转换目标地址。也就是说，如果存在多个目标地址，则防火墙将为原始数据包配置的第一个目标地址转换成已转换数据包配置的第一个目标地址，并将配置的第二个原始目标地址转换成已配置的第二个已转换目标地址，以此类推，始终使用相同的转换。

  如果使用目标 NAT 转换静态 IPv4 地址，您还可以在防火墙一侧使用 DNS 服务解析另一侧上客户端的 FQDN。当采用包含 IPv4 地址的 DNS 相应遍历防火墙时，DNS 服务器会为外部设备提供一个内部 IP 地址，反之亦然。从 PAN-OS 9.0.2 以及之后的 9.0 版本，您可以将防火墙配置为在 DNS 响应（与规则匹



© 2019 Palo Alto Networks, Inc.

配）中重写 IP 地址，以便客户端接收访问目标服务所需的适当地址。通过适当的DNS 重写用例，可以确定此类重写的配置方式。

- 动态 **IP**（带会话分发）— 通过目标 NAT，您可以将原始目标地址转换为具有动态 IP 地址的目标主机或服务器，例如，使用 IP 网络掩码、IP 范围或 FQDN 的地址组或地址对象，其中任何一个都可以从 DNS 返回多个地址。动态 IP（带会话分发）仅支持 IPv4 地址。使用动态 IP 地址的目标 NAT 在使用动态 IP 寻址的云部署中尤其有用。

  如果转换后的目标地址可解析出多个地址，则防火墙会在多个地址之间分发传入 NAT 会话，以提供改进过的会话分发。分发基于以下几种方法之一：轮循机制（默认方法）、源 IP 哈希、IP 模、IP 哈希或最少会话。如果 DNS 服务器为 FQDN 返回的 IPv4 地址超过 32 个，则防火墙将在数据包中使用前 32 个地址。

  如果转换后的地址是仅可解析出 *IPv6* 地址的 *FQDN* 类型的地址对象，则目标 *NAT* 策略规则可视 *FQDN* 为未解析。

  使用 **Dynamic IP (with session distribution)**（动态 **IP**（带会话分发））允许您将多个前导 NAT 目标 IP 地址(*M*)转换为多个后导 NAT 目标 IP 地址(*N*)。多对多转换是指使用单个 NAT 规则会有*M* x *N*个目标 NAT 转换。

对于目标 *NAT*，最佳实践是：

- 对静态 *IP* 地址使用 *Static IP*（静态 *IP*）地址转换，这样，防火墙就可以检查并确保原始目标 *IP* 地址数与转换的目标 *IP* 地址数相同。
- 对基于 *FQDN* 的动态地址仅使用 *Dynamic IP*（动态 *IP*）（带会话分发）地址转换（防火墙无法检查 *IP* 地址数）。

以下是防火墙允许的目标 NAT 转换的常见示例：

| 转换类型 | 原始数据包的目标地址 | 映射到已转换数据包的目标地址 | 注意 |
|---|---|---|---|
| 静态 **Ip** | 192.168.1.1 | 2.2.2.2 | 每个原始数据包和已转换数据包都有一个可能的目标地址。 |
| | 192.168.1.1-192.168.1.4 | 2.2.2.1-2.2.2.4 | 每个原始数据包和已转换数据包都有四个可能的目标地址：<br>192.168.1.1 始终映射到 2.2.2.1<br>192.168.1.2 始终映射到 2.2.2.2<br>192.168.1.3 始终映射到 2.2.2.3<br>192.168.1.4 始终映射到 2.2.2.4 |
| | 192.168.1.1/30 | 2.2.2.1/30 | 每个原始数据包和已转换数据包都有四个可能的目标地址：<br>192.168.1.1 始终映射到 2.2.2.1<br>192.168.1.2 始终映射到 2.2.2.2<br>192.168.1.3 始终映射到 2.2.2.3<br>192.168.1.4 始终映射到 2.2.2.4 |
| 动态 **IP**（带会话分发） | 192.168.1.1/30 | domainname.com | 原始数据包有四个目标地址。例如，如果转换目标地址中的 FQDN |


© 2019 Palo Alto Networks, Inc.

| 转换类型 | 原始数据包的目标地址 | 映射到已转换数据包的目标地址 | 注意 |
| --- | --- | --- | --- |
| | | | 解析为 5 个 IP 地址，则单个 NAT 规则中可能有 20 个目标 NAT 转换。 |

目标 NAT 常用于配置若干 NAT 规则，以将单个公共目标地址映射到已分配给服务器或服务的若干私有目标主机地址。这种情况下，目标端口号用于识别目标主机。例如：

- 端口转发 — 可以将公共目标地址和端口号转换成私有目标地址，但会留用同一端口号。
- 端口转换 — 可以将公共目标地址和端口号转换成私有目标地址和另一端口号，以使真正的端口号保持私有状态。端口转换可通过以下方式来配置：在 NAT 策略规则的 **Translated Packet**（转换后的数据包）选项卡中输入 **Translated Port**（转换后的端口）。请参阅带有端口转换示例的目标 NAT。

## *DNS* 重写目标 *NAT* 用例

当您使用目标 NAT 执行从一个 IPv4 地址向不同 IPv4 地址的静态转换时，您也可使用防火墙一侧的 DNS 服务为客户端解析 FQDN。当包含 IP 地址的 DNS 响应穿过防火墙前往客户端时，防火墙不在该 IP 地址上执行 NAT，因此 DNS 服务器提供内部 IP 地址至外部设备（反之亦然），从而导致 DNS 客户端无法连接至目标服务。

为避免发生此问题，您可以根据为 NAT 策略规则配置的转换 IP 地址，配置防火墙以重写 DNS 响应中的 IP 地址（从 A 记录）。防火墙在 DNS 响应内的 IPv4 地址上（FQDN 解析）执行 NAT，之后将响应转发至客户端；由此，客户端接收适当的地址以访问目标服务。单 NAT 策略规则导致防火墙在与规则匹配的数据包上执行 NAT，还导致防火墙对 DNS 响应内的 IP 地址执行 NAT，且其与规则内的原始目标地址或转换目标地址匹配。

DNS 重写发生在全局级别；防火墙将“原始数据包”选项卡上的目标地址映射到“已转换数据包”选项卡上的目标地址。“原始数据包”选项卡上的所有其他字段都将被忽略。一旦 DNS 响应数据包到达，防火墙将根据如下所示的方向，检查该响应是否包含任何与映射的目标地址之一匹配的任何 A 记录。

您必须规定防火墙在 DNS 响应中的 IP 地址上，相对于 NAT 规则执行 NAT 的方式：**reverse**（反向）或 **forward**（正向）：

- **reverse**（反向）—如果数据包是与规则中 **Translated**（转换后）目标地址匹配的 DNS 响应，则使用该规则所用的反向转换进行 DNS 响应的转换。例如，若规则将 IP 地址 **1.1.1.10** 转换为 **192.168.1.10**，则防火墙会将 DNS 响应从**192.168.1.10** 重写为 **1.1.1.10** 。
- **forward**（正向）— 如果数据包是与规则中 **Original**（原始）目标地址匹配的 DNS 响应，则使用该规则所用的相同转换方式进行 DNS 响应的转换。例如，若规则将 IP 地址 **1.1.1.10** 转换为 **192.168.1.10**，则防火墙会将 DNS 响应从**1.1.1.10** 重写为 **192.168.1.10** 。

如果您有重叠的 *NAT* 规则，且 *DNS* 重写被禁用，而在其下的 *NAT* 规则 *DNS* 重写启用并被包含在重叠内，则防火墙会根据重叠 *NAT* 规则（以 *reverse*（反向）或 *forward*（正向）设置）重写 *DNS* 响应。重写具有优先级，*NAT* 规则顺序将被忽略。

考虑配置 DNS 重写的用例：

- DNS 反向重写目标 NAT 用例
- DNS 正向重写目标 NAT 用例

### DNS 反向重写目标 NAT 用例

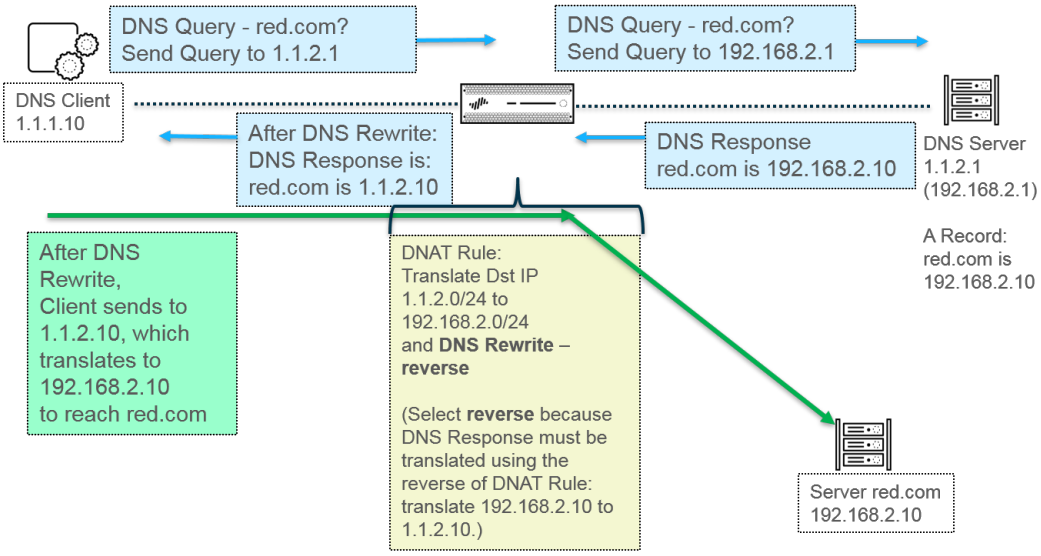
下面的用例展示了目标 NAT 带 DNS 重写（反向重写启用）的情况。这两种使用情况的差别在于 DNS 客户端、DNS 服务器和目标服务器是位于防火墙的公共侧还是内侧。以上任一情况下，DNS 客户端都位于最终目标服务器的防火墙相对侧。（如果您的 DNS 客户端及其最终目标服务器位于防火墙的同一侧，考虑DNS 正向重写目标 NAT 用例 3 和 4。）



© 2019 Palo Alto Networks, Inc.

用例 1 展示了防火墙公共侧上的 DNS 客户端，而 DNS 服务器和最终目标服务器均位于内侧。此情况要求 DNS 在相反方向上重写。DNS 客户端查询 red.com 的 IP 地址。基于 NAT 规则，防火墙将查询（最初前往公共地址 1.1.2.1）转换至内部地址 192.168.2.1。DNS 服务器响应 red.com 的 IP 地址为 192.168.2.10。规则包括启用 **DNS** 重写 - 反向且 192.168.2.10 的 DNS 响应在规则内与 192.168.2.0/24 的目标转换地址相匹配，由此防火墙可通过该规则所用的反向转换进行 DNS 响应的转换。规则要求转换 1.1.2.0/24 至 192.168.2.0/24，由此防火墙重写 192.168.2.10 至 1.1.2.10 的 DNS 响应。DNS 客户端接收响应并发送至 1.1.2.10，规则将其转换至 192.168.2.10 以达到服务器 red.com。

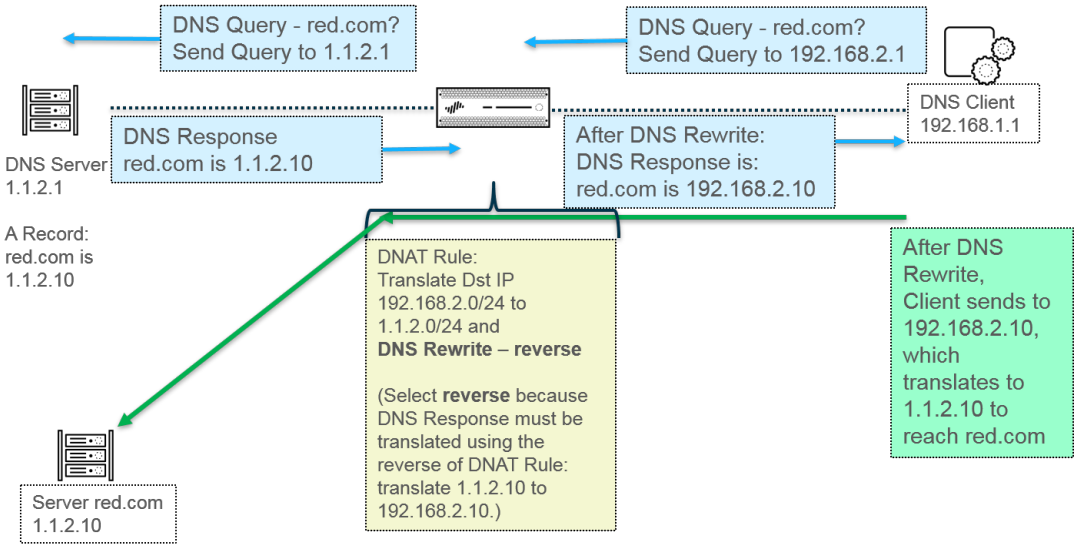
用例 1 摘要：DNS 客户端和目标服务器位于防火墙的相对侧。DNS 服务器提供 NAT 规则内与转换目标位置相匹配的地址，从而通过 NAT 规则的反向转换进行 DNS 响应的转换。




用例 2 展示了防火墙内侧上的 DNS 客户端，而 DNS 服务器和最终目标服务器均位于公共侧。此情况要求 DNS 在相反方向上重写。DNS 客户端查询 red.com 的 IP 地址。基于 NAT 规则，防火墙将查询（最初前往内部地址 192.168.2.1）转换至公共地址 1.1.2.1。DNS 服务器响应 red.com 的 IP 地址为 1.1.2.10。规则包括启用 **DNS** 重写 - 反向且 1.1.2.10 的 DNS 响应在规则内与 1.1.2.0/24 的目标转换地址相匹配，由此防火墙可通过该规则所用的反向转换进行 DNS 响应的转换。规则要求转换 192.168.2.0/24 至 1.1.2.0/24，由此防火墙重写 1.1.2.10 至 192.168.2.10 的 DNS 响应。DNS 客户端接收响应并发送至 192.168.2.10，规则将其转换至 1.1.2.10 以达到服务器 red.com。

用例 2 的摘要与用例 1 相同：DNS 客户端和目标服务器位于防火墙的相对侧。DNS 服务器提供 NAT 规则内与转换目标位置相匹配的地址，从而通过 NAT 规则的反向转换进行 DNS 响应的转换。


© 2019 Palo Alto Networks, Inc.



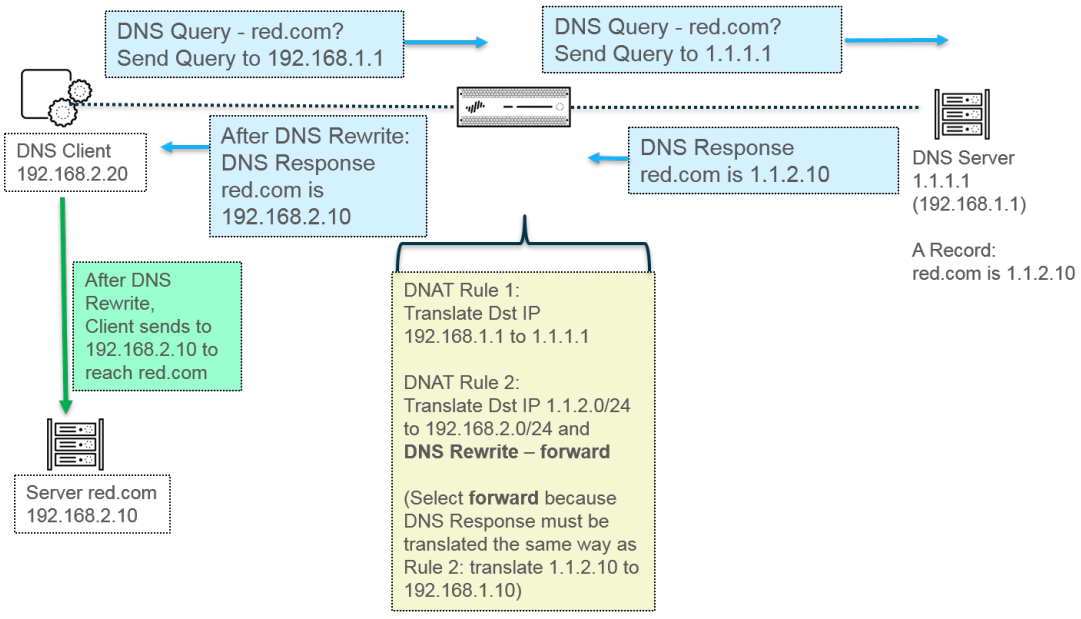

要执行 DNS 重写，配置 DNS 重写目标 NAT。

**DNS 正向重写目标 NAT 用例**

下面的使用情况展示了目标 NAT 带 DNS 重写（正向重写启用）的情况。这两种使用情况的差别在于 DNS 客户端、DNS 服务器和目标服务器是位于防火墙的公共侧还是内侧。以上任一情况下，DNS 客户端都位于最终目标服务器的防火墙相同侧。（如果您的 DNS 客户端及其最终目标服务器位于防火墙的相对侧，考虑DNS 反向重写目标 NAT 用例 1 和 2。）

用例 3 展示了均位于防火墙内侧的 DNS 客户端和终极目标服务器，而 DNS 服务器则位于公共侧。此情况要求 DNS 在正向方向上重写。DNS 客户端查询 red.com 的 IP 地址。基于规则 1，防火墙将查询（最初前往内部地址 192.168.1.1）转换至 1.1.1.1。DNS 服务器响应 red.com 的 IP 地址为 1.1.2.10。规则 2 包括启用 **DNS** 重写 - 正向且 1.1.2.10 的 DNS 响应在规则 2 内与 1.1.2.0/24 的原始目标地址相匹配，由此防火墙可通过该规则所用的正向转换进行 DNS 响应的转换。规则 2 要求转换 1.1.2.0/24 至 192.168.2.0/24，由此防火墙重写 1.1.2.10 至 192.168.2.10 的 DNS 响应。DNS 客户端接收响应并发送至 192.168.2.10 以达到服务器 red.com。

用例 3 摘要：DNS 客户端和目标服务器位于防火墙的相同侧。DNS 服务器提供 NAT 规则内与原始目标位置相匹配的地址，从而通过 NAT 规则的相同（正向）转换进行 DNS 响应的转换。

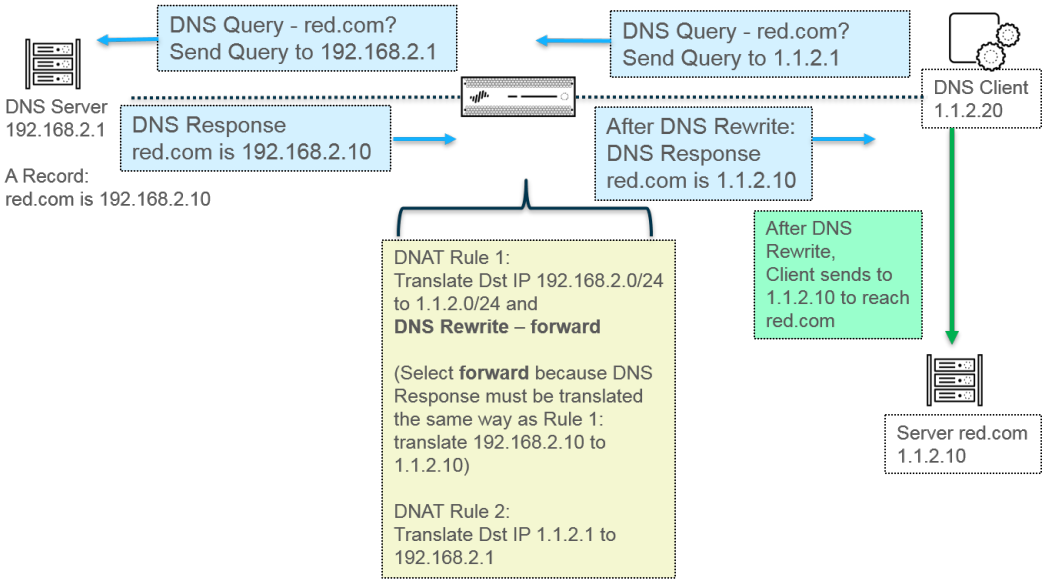





© 2019 Palo Alto Networks, Inc.

用例 4 展示了均位于防火墙公共侧的 DNS 客户端和终极目标服务器，而 DNS 服务器则位于内侧。此情况要求 DNS 在正向方向上重写。DNS 客户端查询 red.com 的 IP 地址。基于规则 2，防火墙将查询（最初前往公共目标 1.1.2.1）转换至 192.168.2.1。DNS 服务器响应 red.com 的 IP 地址为 192.168.2.10。规则 1 包括 **Enable DNS Rewrite - forward**（启用 **DNS** 重写 - 正向）且 192.168.2.10 的 DNS 响应在规则 1 内与 192.168.2.0/24 的原始目标地址相匹配，由此防火墙可通过该规则所用的正向转换进行 DNS 响应的转换。规则 1 要求转换 192.168.2.0/24 至 1.1.2.0/24，由此防火墙重写 192.168.2.10 至 1.1.2.10 的 DNS 响应。DNS 客户端接收响应并发送至 1.1.2.10 以达到服务器 red.com。

用例 4 的摘要与用例 3 相同：DNS 客户端和目标服务器位于防火墙的相同侧。DNS 服务器提供 NAT 规则内与原始目标位置相匹配的地址，从而通过 NAT 规则的相同（正向）转换进行 DNS 响应的转换。




要执行 DNS 重写，配置 DNS 重写目标 NAT。

## NAT 规则容量

允许的 NAT 规则数取决于防火墙型号。可以为静态、动态 IP (DIP) 以及动态 IP 和端口 (DIPP) NAT 设置各自的规则限值。用于这些 NAT 类型的规则总数不能超过总 NAT 规则容量。对于 DIPP，规则限值取决于防火墙的超额订阅设置（8、4、2 或 1）以及“每个规则只有一个转换后 IP 地址”这一假设。要查看特定于型号的 NAT 规则限制和已转换 IP 地址限制，请使用比较防火墙工具。

使用 NAT 规则时，请考虑以下事项：

- 如果池资源已用完，那么即使还未达到型号的最大规则计数，也将无法创建更多的 NAT 规则。
- 如果合并 NAT 规则，那么日志和报告也将合并。统计信息将按规则提供，而不会按规则中的所有地址来提供。如果需要精细的日志和报告，请不要合并规则。

## 动态 IP 和端口 NAT 超额订阅

动态 IP 和端口 (DIPP) NAT 可让您在并发会话中多次（8、4 或 2 次）使用每一个转换后 IP 地址和端口对。IP 地址和端口的这种可复用性（称为超额订阅）可为拥有少量公共 IP 地址的客户提供可扩展性。该设计基于以下假设：主机与不同目标相连，会话可以唯一标识，且不会发生冲突。实际上，超额订阅率会乘以地址/端口池的原始大小，以使大小变为原来的 8、4 或 2 倍。例如，如果允许的并发会话的默认限值为 64K 个，那么在乘以超额订阅率 8 后允许的并发会话就是 512K 个。

允许的超额订阅率因型号而异。超额订阅率全局适用；它会应用于防火墙。默认情况下，即使有足够的公共 IP 地址可供使用，因而无需进行超额订阅，该超额订阅率仍会设置并会占用内存。您可以将该比率从默认设置降为更小的设置，甚至降到 1（意味着不进行超额订阅）。通过配置更低的比率，您可以减小可执行的源


© 2019 Palo Alto Networks, Inc.

设备转换的数量，但提高 DIP 和 DIPP NAT 规则容量。要更改默认比率，请参阅修改 DIPP NAT 的超额订阅率。

如果选择 **Platform Default**（平台默认值），超额订阅的显式配置将被关闭并会应用平台的默认超额订阅率（如下图所示）。如果使用 **Platform Default**（平台默认值）设置，软件版本可以升级或降级。

下表列有各个型号的默认（最高）超额订阅率。

| 模型 | 默认超额订阅率 |
|---|---|
| PA-220 | 2 |
| PA-820 | 2 |
| PA-850 | 2 |
| PA-3220 | 4 |
| PA-3250 | 4 |
| PA-3260 | 4 |
| PA-5220 | 4 |
| PA-5250 | 8 |
| PA-5260 | 8 |
| PA-5280 | 8 |
| PA-7050 | 8 |
| PA-7080 | 8 |
| VM-50 | 2 |
| VM-100 | 1 |
| VM-200 | 1 |
| VM-300 | 2 |
| VM-500 | 8 |
| VM-700 | 8 |
| VM-1000-HV | 2 |

本防火墙的每一个 NAT 规则最多可支持 256 个转换后 IP 地址，每个型号可支持最大数量的转换后 IP 地址（所有 NAT 规则合并后）。如果超额订阅后会超出每个规则的最大转换后地址数 (256)，那么防火墙会自动降低超额订阅比率，以便成功地进行提交。但是，如果 NAT 规则会导致转换超出型号的最大转换后地址数，那么提交将以失败告终。



© 2019 Palo Alto Networks, Inc.

# 数据面板 NAT 内存统计信息

**show running global-ippool** 命令可显示与池的 NAT 内存占用情况相关的统计信息。“大小”列显示资源池所用内存的字节数。“比率”列显示超额订阅率（仅适用于 DIPP 池）。以下样本输出可以说明池和内存统计信息中的各行：

```
admin@PA-7050-HA-0 (active-primary)> show running global-ippool

Idx  Type            From                  To          Num   Ref.Cnt  Size      Ratio
1    Dynamic IP      201.0.0.0-201.0.255.255  210.0.0.0   4096  2        657072    N/A
2    Dynamic IP      202.0.0.0-202.0.0.255    220.0.0.0   256   1        41232     N/A
3    Dynamic IP/Port 200.0.2.100-200.0.2.100  200.0.3.11  1     1        68720        8

Usable NAT DIP/DIPP shared memory size: 58490064      ← Total physical NAT memory (bytes)
Used NAT DIP/DIPP shared memory size: 767024 (1.3%)   ← Bytes and % of usable NAT memory
Dynamic IP NAT Pool: 2 (1.19%)                        ← Number of DIP pools in use and % of total usable memory that all DIP pools use
Dynamic IP/Port NAT Pool: 1 (0.12%)                   ← Number of DIPP pools in use and % of total usable memory that all DIPP pools use
```

对于虚拟系统的 NAT 池统计信息，**show running ippool** 命令可以显示相应列，以指明各 NAT 规则所占用的内存大小以及所使用的超额订阅率（适用于 DIPP 规则）。下面是此命令的样本输出。

```
admin@PA-7050-HA-0 vsys1 (active-primary)> show running ippool

VSYS 1 has 4 NAT rules, DIP and DIPP rules:
Rule        Type            Used     Available    Mem Size     Ratio
------------ --------------- -------  ------------ ------------ -------
nat1        Dynamic IP      0        4096          788144        0
nat2        Dynamic IP      0        256            49424        0
nat3        Dynamic IP/Port 0        638976        100976        4
nat11       Dynamic IP      0        4096          788144        0
```

**show running nat-rule-ippool rule** 命令的输出字段会显示各 NAT 规则所占用的内容（以字节为单位）。下面是此命令的样本输出，圈示的内容是规则的内存使用情况。

```
admin@PA-7050-HA-0 (active-primary)> show running nat-rule-ippool rule nat1

VSYS 1 Rule nat1:
Rule: nat1, Pool index: 1,  memory usage: 788144
-----------------------------------------------------------
Reserve IP: no
201.0.0.0-201.0.255.255  =>
          210.0.0.0-210.0.15.255

Source          Xlat-Source     Ref.Cnt (F)     TTL(s)

Total IPs in use: 0
Total entries in time-reserve cache: 0
Total freelist left: 4096
```

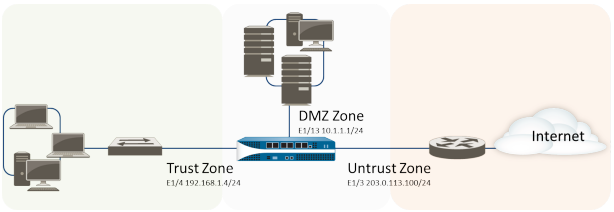
# 配置 NAT

请执行以下任务以配置 NAT 的各个方面。除了以下示例，NAT 配置示例部分中还有一些示例。

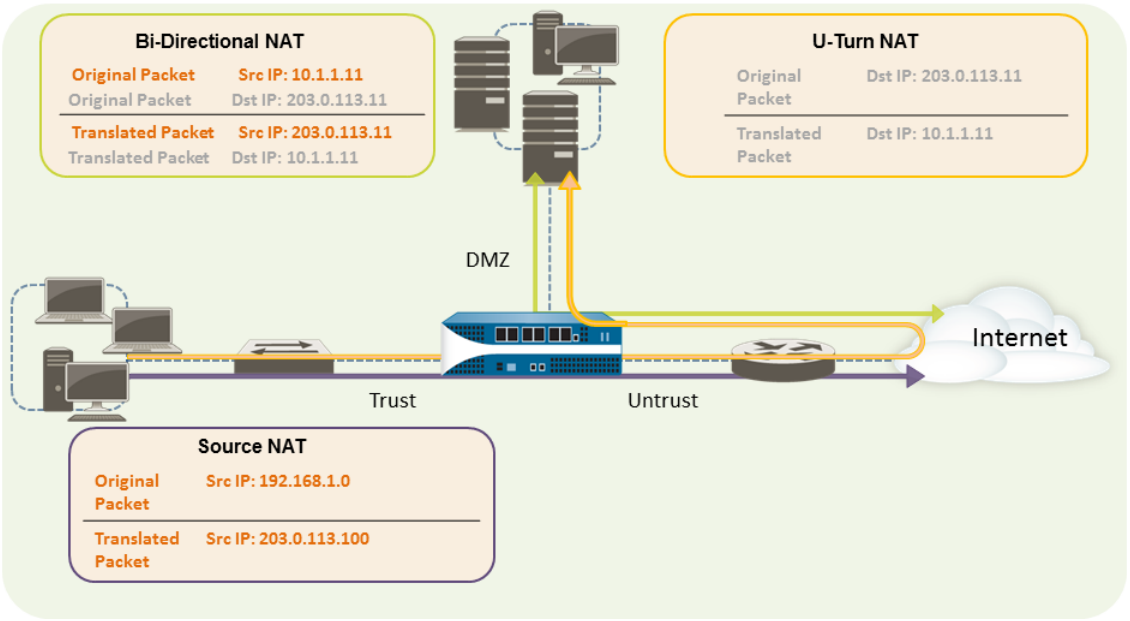
- 将内部客户端 IP 地址转换为公共 IP 地址（源 DIPP NAT）
- 使内部网络上的客户端能够访问公共服务器（目标 U-Turn NAT）
- 为面向公众的服务器启用双向地址转换（静态源 NAT）
- 配置 DNS 重写目标 NAT
- 使用动态 IP 地址配置目标 NAT
- 修改 DIPP NAT 的超额订阅率
- 保留动态 IP NAT 地址
- 为特定主机或接口禁用 NAT


© 2019 Palo Alto Networks, Inc.

本节中前三个 NAT 示例基于以下拓扑：




根据此拓扑，我们需要创建以下三种 NAT 策略：




- 若要让内部网络上的客户端能够访问互联网上的资源，需要将内部的 192.168.1.0 地址转换为可公开路由的地址。在此示例中，我们将配置源 NAT（紫色机柜和向上箭头），使用传出接口地址 203.0.113.100 作为从内部区域离开防火墙的所有数据包的源地址。有关说明，请参阅将内部客户端 IP 地址转换为公共 IP 地址（源 DIPP NAT）。
- 若要让内部网络上的客户端能够访问 DMZ 区域中的公共 Web 服务器，我们必须配置一个 NAT 规则，让该规则将来自外部网络的数据包（原始路由表查找将根据数据包中的目标地址 203.0.113.11 确定它的去向）重定向到 DMZ 网络 10.1.1.11 上的 Web 服务器的实际地址。为此，必须创建一个从信任区域（数据包中的源地址所在的区域）到不信任区域（原始目标地址所在的区域）的 NAT 规则，以便将目标地址转换为 DMZ 区域中的地址。此类型的目标 NAT 称为 *U-Turn NAT*（黄色机柜和向上箭头）。有关说明，请参阅使内部网络上的客户端能够访问公共服务器（目标 U-Turn NAT）。
- 若要让 Web 服务器（同时包含 DMZ 网络上的私有 IP 地址和供外部用户访问的面向公众的地址）能够发送和接收请求，防火墙必须将来自公共 IP 地址的传入数据包转换为私有 IP 地址，将来自私有 IP 地址的传出数据包转换为公共 IP 地址。在防火墙上，可以使用单个双向静态源 NAT 策略（绿色机柜和向上箭头）来实现此操作。请参阅为面向公众的服务器启用双向地址转换（静态源 NAT）。

## 将内部客户端 *IP* 地址转换为公共 *IP* 地址（源 *DIPP NAT*）

当内部网络上的客户端发送请求时，数据包中的源地址将包含客户端在内部网络上的 IP 地址。如果在内部使用私有 IP 地址范围，则在互联网上将无法路由来自客户端的数据包，除非您将离开网络的数据包中的源 IP 地址转换为可公开路由的地址。

在防火墙上，可以通过配置将源地址（和端口（可选））转换为公共地址的源 NAT 策略来执行此操作。执行此操作的一种方式是将所有数据包的源地址转换为防火墙上的传出接口，如以下过程所示。

STEP 1 | 为计划使用的外部 IP 地址创建一个地址对象。



© 2019 Palo Alto Networks, Inc.

1. 为对象选择 **Objects**（对象）> **Addresses**（地址），**Add**（添加）**Name**（名称）和 **Description**（说明）（可选）。
2. 从 **Type**（类型）中选择 **IP Netmask**（**IP** 网络掩码），然后输入防火墙上的外部接口的 IP 地址，在此示例中为 203.0.113.100。
3. 单击 **OK**（确定）。



尽管您不是必须在策略中使用地址对象，但这是最佳实践，因为它让您可以在一个地方进行更新，而不必更新引用该地址的每个策略，从而会简化管理。

STEP 2 | 创建 NAT 策略。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，为策略输入描述性名称。
3. （可选）输入一个标记，此标记是允许您对策略进行排序或筛选的关键字或短语。
4. 在 **NAT Type**（**NAT** 类型），选择 **ipv4**（默认）。
5. 在 **Original Packet**（原始数据包）选项卡上，在 **Source Zone**（源区域）部分中选择您为内部网络创建的区域（单击 **Add**（添加），然后选择区域），并从 **Destination Zone**（目标区域）列表中选择您为外部网络创建的区域。
6. 在 **Translated Packet**（已转换数据包）选项卡上，从屏幕的源地址转换部分内的 **Translation Type**（转换类型）列表中选择 **Dynamic IP And Port**（动态 **IP** 和端口）。
7. 对于 **Address Type**（地址类型），有两种选择。可以选择 **Translated Address**（转换后的地址），然后单击 **Add**（添加）。选择刚创建的地址对象。

   另外一种 **Address Type**（地址类型）为 **Interface Address**（接口地址），选中该选项后，转换地址将成为接口的 IP 地址。对于该选择，您会选择一个 **Interface**（接口），如果接口有一个以上 IP 地址，可随意选择一个 **IP Address**（**IP** 地址）。
8. 单击 **OK**（确定）。

STEP 3 | 提交更改。

单击 **Commit**（提交）。

STEP 4 | （可选）访问 CLI 来验证转换。

1. 使用 **`show session all`** 命令查看会话表，您可以在此表中验证源 IP 地址和端口以及相应的转换 IP 地址和端口。
2. 使用 *show session id <id_number>* 查看有关会话的更多详情。
3. 如果您配置了动态 IP NAT，请使用 **`show counter global filter aspect session severity drop | match nat`** 命令查看是否有任何会话因 NAT IP 分配而失败。如果转换新连接时动态 IP NAT 池中的所有地址都已被分配，将丢弃此数据包。

## 使内部网络上的客户端能够访问公共服务器（目标 *U-Turn NAT*）

当内部网络上的用户发送对 DMZ 中的公司 Web 服务器的访问请求时，DNS 服务器会将其解析为公共 IP 地址。在处理该请求时，防火墙将使用数据包中的原始目标（公共 IP 地址）并将该数据包路由到不信任区域的传出接口。在防火墙接收信任区域上用户的请求时，为了让防火墙知道它必须将 Web 服务器的公共 IP 地址转换为 DMZ 网络上的地址，您必须创建目标 NAT 规则，从而支持防火墙将该请求发送到 DMZ 区域的传出接口，如下所示。

STEP 1 | 为 Web 服务器创建地址对象。

1. 为地址对象选择 **Objects**（对象）> **Addresses**（地址），**Add**（添加）**Name**（名称）和 **Description**（说明）（可选）。
2. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并输入 Web 服务器的公共 IP 地址，在本例中为 203.0.113.11。



© 2019 Palo Alto Networks, Inc.

您可以通过单击 **Resolve**（解析）将地址对象类型从 **IP Netmask**（**IP** 网络掩码）切换到 **FQDN**，并在出现 FQDN 时单击 **Use this FQDN**（使用此 **FQDN**）。或者，对于 **Type**（类型），选择**FQDN**，并输入用于地址对象的 FQDN。如果输入 FQDN 并单击 **Resolve**（解析），则字段中将显示 FQDN 解析的 IP 地址。要将使用此 IP 地址的地址对象 **Type**（类型）从 FQDN 切换到 IP 网络掩码，请单击 **Use this address**（使用此地址），**Type**（类型）将切换到带该字段中显示的 IP 地址的 **IP Netmask**（**IP** 网络掩码）。

3. 单击 **OK**（确定）。

STEP 2 | 创建 NAT 策略。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，为 NAT 规则输入描述性 **Name(名称)**。
3. 在 **Original Packet**（原始数据包）选项卡上，在 **Source Zone**（源区域）部分中选择您为内部网络创建的区域（单击 **Add**（添加），然后选择区域），并从 **Destination Zone**（目标区域）列表中选择您为外部网络创建的区域。
4. 在 **Source Address**（源地址）部分中，**Add**（添加）您为公共 Web 服务器地址创建的地址对象。
5. 在 **Translated Packet**（转换后的数据包）选项卡上，对于目标地址转换，在 **Translation Type**（转换类型）中，选择 **Static Ip**（静态 **IP**），然后输入分配给 DMZ 网络上 Web 服务器接口的 IP 地址，在此示例中为 10.1.1.11。或者，可以选择 **Translation Type**（转换类型）为 **Dynamic IP (with session distribution)**（动态 **Ip**（带会话分发），然后输入 **Translated Address**（转换后的地址）至使用 IP 掩码、IP 范围或 FQDN 的“地址对象”或“地址组”。以上任何项都可以从 DNS 返回多个地址。如果转换目标地址解析出一个以上的地址，防火墙将根据您可以选择的若干方法之一，在多个地址之间分配传入的 NAT 会话：**Round Robin**（循环调度）（默认方法）、**Source IP Hash**（源 **IP** 哈希）、**IP Modulo**（**IP** 模）、**IP Hash**（**IP** 哈希）或 **Least Sessions**（最少会话）。
6. 单击 **OK**（确定）。

STEP 3 | 单击 **Commit**（提交）。

## 为面向公众的服务器启用双向地址转换（静态源 *NAT*）

当面向公众的服务器在它们所在的物理网段上分配有私有 IP 地址时，您将需要一个源 NAT 规则，以在 egress 时将服务器的源地址转换为外部地址。您可以创建一个静态 NAT 规则，以将内部源地址 10.1.1.11 转换为外部 Web 服务器地址，在此示例中为 203.0.113.11。

但是，面向公众的服务器必须能收发数据包。您需要一个相反的策略，用于将公共地址（来自互联网用户的传入数据包中的目标 IP 地址）转换为私有地址，以使防火墙能够将该数据包路由到您的 DMZ 网络。您可以创建一个双向静态 NAT 规则，如以下过程所述。双向转换选项仅适用于静态 NAT。

STEP 1 | 为 Web 服务器的内部 IP 地址创建地址对象。

1. 为对象选择 **Objects**（对象）> **Addresses**（地址），**Add**（添加）**Name**（名称）和 **Description**（说明）（可选）。
2. 从 **Type**（类型）列表中选择 **IP Netmask**（**IP** 网络掩码），然后输入 DMZ 网络上的 Web 服务器的 IP 地址，在此示例中为 10.1.1.11。
3. 单击 **OK**（确定）。



如果您尚未针对您的 *Web* 服务器的公共地址创建地址对象，那么现在就应该创建该对象。

STEP 2 | 创建 NAT 策略。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，为 NAT 规则输入描述性 **Name(名称)**。
3. 在 **Original Packet**（原始数据包）选项卡上，在 **Source Zone**（源区域）部分中选择您为 DMZ 创建的区域（单击 **Add**（添加），然后选择区域），并从 **Destination Zone**（目标区域）列表中选择您为外部网络创建的区域。



© 2019 Palo Alto Networks, Inc.

4. 在 **Source Address**（源地址）部分中，**Add**（添加）您为内部 Web 服务器地址创建的地址对象。
5. 在 **Translated Packet**（转换后的数据包）选项卡上，从 **Translation Type**（源地址转换）部分的 **Source Address Translation**（转换类型）列表中选择 **Static IP**（静态 **IP**），然后从 **Translated Address**（转换后的地址）列表中选择您为外部 Web 服务器地址创建的地址对象。
6. 在 **Bi-directional**（双向）字段中选择 **Yes**（是）。
7. 单击 **OK**（确定）。

STEP 3 | 提交。

单击 **Commit**（提交）。

## 配置 *DNS* 重写目标 *NAT*

当您配置用于执行 IPv4 地址静态转换的目标 NAT 策略规则时，您也可以启用 DNS 重写，以便防火墙根据规则配置的原始目标 IP 地址或转换目标 IP 地址，在 DNS 响应中重写 IPv4 地址。防火墙在 DNS 响应（与规则相匹配）内的 Ipv4 地址上（FQDN 解析）执行 NAT，之后将响应转发至客户端；由此，客户端接收适当的地址以访问目标服务。

查看 DNS 重写用例了解 DNS 重写，并可帮助您确定是否指定在 **reverse**（反向）或 **forward**（正向）方向中进行重写。

您无法在启用 *DNS* 重写的相同 *NAT* 规则中启用 *Bi-directional*（双向）源地址转换。

STEP 1 | 创建目标 NAT 策略规则，指定防火墙执行与规则相匹配的 IPv4 地址静态转换，同时指定当 IPv4 地址（来自 A 记录）与 NAT 规则中的原始目标地址相匹配时，防火墙在 DNS 响应中重写 IP 地址。

1. 选择 **Policies**（策略）> **NAT**并 **Add**（添加）NAT 策略规则。
2. （可选）在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称）。
3. 对于 **NAT Type**（**NAT** 类型），请选择 **ipv4**。
4. 在 **Original Packet**（原始数据包）选项卡中，**Add**（添加） **Destination Address**（目标地址）。

   此外，您还必须选择一个源区域或*Any*（任何）源区域，但是，将在全局层级进行 *DNS* 重写；仅“原始数据包”选项卡中的“目标地址”会进行匹配。*DNS* 重写将忽略“原始数据包”选项卡中的所有其他字段。
5. 在 **Translated Packet**（转换的数据包）选项卡上，为目标地址转换选择 **Translation Type**（转换类型）为 **Static IP**（静态 **IP**）。
6. 选择 **Translated Address**（转换地址） 或输入一个新地址。
7. **Enable DNS Rewrite**（启用 **DNS** 重写）并选择 **Direction**（方向）：
   - 当 DNS 响应中的 IP 地址需要 NAT 规则指定的反向转换时，选择 **reverse**（反向）（默认）。如果 DNS 响应与规则中的**Translated**（转换）目标地址匹配，则使用该规则所用的反向转换进行 DNS 响应的转换。例如，若规则将 IP 地址 1.1.1.10 转换为 192.168.1.10，则防火墙会将 DNS 响应从 192.168.1.10 重写为 1.1.1.10。
   - 当 DNS 响应中的 IP 地址需要进行 NAT 规则指定的相同转换时，选择 **forward**（正向）。如果 DNS 响应与规则中的**Original**（原始）目标地址匹配，则使用该规则所用的相同转换方式进行 DNS 响应的转换。例如，若规则将 IP 地址 1.1.1.10 转换为 192.168.1.10，则防火墙会将 DNS 响应从 1.1.1.10 重写为 192.168.1.10。
8. 单击 **OK**（确定）。

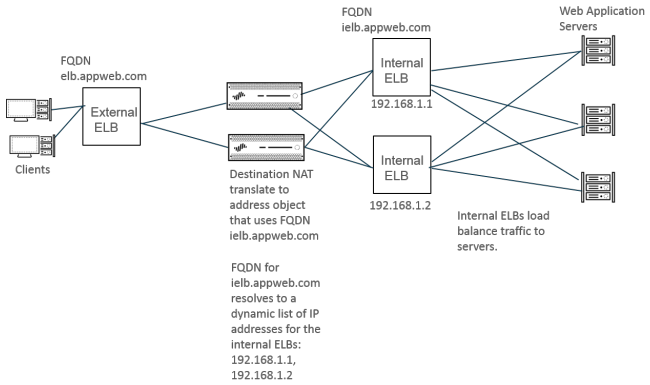
STEP 2 | **Commit**（提交）更改。


© 2019 Palo Alto Networks, Inc.

# 使用动态 *IP* 地址配置目标 *NAT*

用于目标 NAT将原目标地址转换为拥有动态 IP 地址且使用 FQDN 的目标主机或服务器。使用动态 IP 地址的目标 NAT 在云部署中尤其有用，通常使用动态 IP 寻址。当云中的主机或服务器有新的（动态）IP 地址时，不必通过持续查询 DNS 服务器手动更新 NAT 策略规则，也无需使用单独的外部组件通过最新 FQDN 到 IP 地址映射来更新 DNS 服务器。

在以下示例拓扑中，客户端想要访问在云中托管 Web 应用程序的服务器。外部“弹性负载均衡”(ELB) 连接至防火墙，防火墙连接至内部 ELB，内部 ELB 连接至服务器。例如，随着时间的推移，Amazon Web Services (AWS) 会根据服务需求为内部 ELB 添加（或删除）FQDN 分配的 IP 地址。因为更新是动态的，因此，可以灵活地将 NAT 的 FQDN 用于内部 ELB，有助于策略解决不同时间发生的不同 IP 地址问题，使目标 NAT 更易于使用。




STEP 1 | 使用服务器的 FQDN 创建地址对象，该服务器是要将地址进行转换的服务器。（地址对象也可以是 IP 网络掩码或 IP 范围。）

1. 选择 **Objects**（对象）> **Addresses**（地址），按 **Name**（名称）**Add**（添加）地址对象，例如 **`post-NAT-Internal-ELB`**。
2. 选择 **FQDN** 作为 **Type**（类型），然后输入 FQDN。在本示例中，FQDN 是 **`ielb.appweb.com`**。
3. 单击 **OK**（确定）。

STEP 2 | 创建目标 NAT 策略。

1. 在 **General**（常规）选项卡上，选择 **Policies**（策略）> **NAT**，并按 **Name**（名称）**Add**（添加）NAT 策略规则。
2. 选择 **ipv4** 作为 **NAT Type**（NAT 类型）。
3. 在 **Original Packet**（原始数据包）选项卡上，**Add**（添加）**Source Zone**（源区域）和 **Destination Zone**（目标区域）。
4. 在“目标地址转换”部分的 **Translated Packet**（转换后的数据包）选项卡上，选择 **Dynamic IP (with session distribution)**（动态 **IP**（带会话分发））作为 **Translation Type**（转换类型）。
5. 对于 **Translated Address**（转换后的地址），选择您为 FQDN、IP 网络掩码或 IP 范围创建的地址对象。在本示例中，FQDN 是 **`post-NAT-Internal-ELB`**。
6. 对于 **Session Distribution Method**（会话分发方法），选择以下其一：
   - **Round Robin**（循环调度）（默认）— 按轮流顺序分配新会话到 IP 地址。除非您有更改分发方法的理由，否则，循环调度法就比较合适。
   - **Source IP Hash**（源 **IP** 哈希）—根据源 IP 地址哈希分配新会话。如果您有来自某个单独源 IP 地址的传入流量，不得选择源 IP 哈希；请选择与之不同的方法。
   - **IP Modulo**（**IP** 模）— 防火墙考虑来自传入数据包的源和目标 IP 地址；防火墙执行 XOR 操作和模操作；结果可确定防火墙分配新会话的 IP 地址。
   - **IP Hash**（**IP** 哈希）— 根据源和目标 IP 地址的哈希分配新会话。
   - **Least Sessions**（最少会话）— 将新会话分配给具有最小并发会话的 IP 地址。如果您有大量短暂会话，**Least Sessions**（最少会话）将为您提供更均衡的会话分布。



© 2019 Palo Alto Networks, Inc.

防火墙在多个 *IP* 地址之间分发会话之前，不会从目标 *IP* 地址列表中删除重复的 *IP* 地址。防火墙分发会话到重复地址的方式与分发到非重复地址的方式一样。（例如，如果转换后的地址是地址对象的地址组，且一个地址对象是可解析出 *IP* 地址的 *FQDN*，另一个地址对象是包含同一 *IP* 地址的范围，则转换池中会出现重复地址。）

7. 单击 **OK**（确定）。

STEP 3 | **Commit**（提交）更改。

STEP 4 | （可选）您可以在防火墙刷新 FQDN 时配置频率（用例 1：防火墙要求执行 DNS 解析）。

## 修改 *DIPP NAT* 的超额订阅率

如果您有足够的公共 IP 地址，因而无需使用 DIPP NAT 超额订阅，那么您可以降低超额订阅率，从而增加允许的 DIP 和 DIPP NAT 规则。

STEP 1 | 查看 DIPP NAT 超额订阅率。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话）> **Session Settings**（会话设置）。查看 **NAT Oversubscription Rate**（**NAT** 超额订阅率）设置。

STEP 2 | 设置 DIPP NAT 超额订阅率。

1. 编辑 Session Settings（会话设置）部分。
2. 在 **NAT Oversubscription Rate**（**NAT** 超额订阅率）列表中，选择 **1x**、**2x**、**4x** 或 **8x**，这取决于您所需的比率。

   *Platform Default*（平台默认）设置将应用于型号的默认超额订阅设置。如果不想超额订阅，请选择 *1x*。

3. 单击 **OK**（确定）并 **Commit**（提交）更改。

## 保留动态 *IP NAT* 地址

还可以保留动态 IP NAT 地址（对于可配置的时间段），以防止它们作为转换后地址被分配至不同的需要转换的 IP 地址。在配置时，此保留将应用于进行中的所有转换动态 IP 地址和所有新转换。

对于进行中的转换和新转换，当源 IP 地址转换为可用的转换 IP 地址时，即使与该特定源 IP 相关的所有会话都过期后，此配对仍会保留。每个源 IP 地址的保留计时器从使用此源 IP 地址转换的所有会话到期时开始。动态 IP NAT 是一种一对一转换；一个动源 IP 地址转换为从配置池中可用的地址中动态选择的转换 IP 地址。因此，保留到期之前，保留的转换 IP 地址不可用于其他任何源 IP 地址，因为新会话尚未启动。每次源 IP/转换 IP 映射的新会话开始后，没有活动会话一段时间后，计时器会重置。

默认情况下，不会保留任何地址。您可以为防火墙或虚拟系统保留动态 IP NAT 地址。

- 为防火墙保留动态 IP NAT 地址。

  输入以下命令：

```
admin@PA-3250# set setting nat reserve-ip yes
```

```
admin@PA-3250# set setting nat reserve-time <1-604800 secs>
```

- 为虚拟系统保留动态 IP NAT 地址。

  输入以下命令：


© 2019 Palo Alto Networks, Inc.

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-ip yes
```

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800 secs>
```

例如，假如有 30 个地址的动态 IP NAT 池，**nat reserve-time** 设置为 28800 秒（8 小时）时，有 20 个转换在进行中。现在会保留这 20 个转换，以便使用各个源 IP/转换 IP 映射的最后一个会话（任何应用程序）到期时，只会为该源 IP 地址保留转换 IP 地址 8 小时，以防源 IP 地址需要再次转换。此外，因为剩余的 10 个转换地址已经分配，因此将分别为它们的源 IP 地址保留这些转换地址，每个都带有一个计时器，该计时器会在该源 IP 地址的最后一个会话到期时开始计时。

通过这种方式，每个源 IP 地址可以从池中重复转换至其相同的 NAT 地址；另外一个主机将不会分配至来自池的保留转换后 IP 地址，即使该转换地址没有活动会话。

假设源 IP/转换 IP 映射的所有会话都已到期，且为期 8 小时的保留计时器已开始。该转换的新会话开始后，计时器将停止，且会话将继续，直至全部结束，此时保留计时器将再次开始对保留转换地址进行计时。

保留计时器在动态 IP NAT 池中持续有效，直到您通过输入 **set setting nat reserve-ip no** 命令或者更改 **nat reserve-time**（**NAT** 保留时间）为不同的值进行禁用。

保留的 CLI 命令不会影响动态 IP 和端口 (DIPP) 或静态 IP NAT 池。

## 为特定主机或接口禁用 *NAT*

可对源 NAT 和目标 NAT 规则进行配置，以在禁用转换。在某些例外情况下，您可能不希望对子网中的某个主机或是退出特定接口的通信执行 NAT。以下步骤将介绍如何为主机禁用源 NAT。

STEP 1 | 创建 NAT 策略。

1. 选择 **Policies**（策略）> **NAT**，然后单击 **Add**（添加）策略的描述性 **Name**（名称）。
2. 在 **Original Packet**（原始数据包）选项卡上，在 **Source Zone**（源区域）部分中选择您为内部网络创建的区域（单击 **Add**（添加），然后选择区域），并从 **Destination Zone**（目标区域）列表中选择您为外部网络创建的区域。
3. 针对 **Source Address**（源地址），请单击 **Add**（添加）并输入主机地址。单击 **OK**（确定）。
4. 在 **Translated Packet**（转换后的数据包）选项卡上，从屏幕的源地址转换部分内的 **Translation Type**（转换类型）列表中选择 **None**（无）。
5. 单击 **OK**（确定）。

STEP 2 | 提交更改。

单击 **Commit**（提交）。

*NAT* 规则按照从顶部到底部的顺序处理，因此应用其他 *NAT* 策略之前要先应用 *NAT* 免除策略，以确保在要免除的源发生地址转换前先处理此策略。

# NAT 配置示例

- 目标 NAT 示例 — 一对一映射
- 带有端口转换示例的目标 NAT
- 目标 NAT 示例 — 一对多映射
- 源和目标 NAT 示例
- Virtual Wire 源 NAT 示例
- Virtual Wire 静态 NAT 示例
- Virtual Wire 目标 NAT 示例



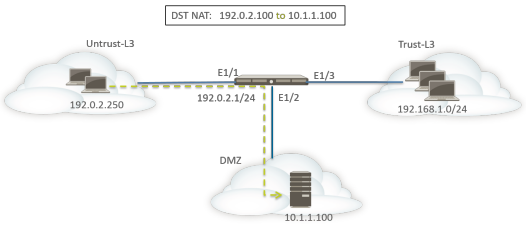
© 2019 Palo Alto Networks, Inc.

# 目标 *NAT* 示例 — 一对一映射

配置 NAT 和安全规则时最常见的错误是对区和地址对象的引用。目标 NAT 规则中使用的地址始终引用数据包中的原始 IP 地址（即前导转换地址）。NAT 规则中的目标区在原始数据包（即前导 NAT 目标 IP 地址）内目标 IP 地址的路由查找结束后确定。

安全策略中的地址还会引用原始数据包中的 IP 地址（即前导 NAT 地址）。但是，目标区是终端主机物理连接到的区。也就是说，安全规则中的目标区在后导 NAT 目标 IP 地址的路由查找结束后确定。

在以下一对一目标 NAT 映射中，来自名为 Untrust-L3 区域的用户访问名为 DMZ 区域中的服务器 10.1.1.100，使用 IP 地址 192.0.2.100。




在配置 NAT 规则之前，请考虑此情况的事件顺序。

- 主机 192.0.2.250 会为地址 192.0.2.100（目标服务器的公共地址）发送 ARP 请求。
- 防火墙将在 Ethernet1/1 接口上接收目标 192.0.2.100 的 ARP 请求数据包并对此请求进行处理。因为配置了目标 NAT 规则，防火墙会使用自己的 MAC 地址响应此 ARP 请求。
- 将针对匹配项评估 NAT 规则。对于要转换的目标 IP 地址，必须创建从 Untrust-L3 区域至 Untrust-L3 区域的目标 NAT 规则，以转换 192.0.2.100 的目标 IP 至 10.1.1.100。
- 确定转换地址后，防火墙将为目标 10.1.1.100 执行路由查找来确定传出接口。在此例中，DMZ 区域中的 egress 接口是 Ethernet1/2。
- 防火墙执行安全策略查找，以确认是否允许从 Untrust-L3 区域传输流量至 DMZ。

策略的方向与接收区和服务器物理所在的区匹配。

安全策略引用原始数据包中的 *IP* 地址，此数据包的目标地址为 *192.0.2.100*。

- 防火墙会将数据包转发到服务器外的传出接口 Ethernet1/2。目标地址将在数据包离开防火墙时更改为 10.1.1.100。

在本例中，为专用 Web 服务器 (10.1.1.100) 和公共 Web 服务器 (192.0.2.100) 配置地址对象。配置后的 NAT 规则将类似于下图：

| NAME | TAGS | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|
| | | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| Dst NAT-webserver | none | Untrust-L3 | Untrust-L3 | any | any | Webserver-public | any | none | destination-translation<br>address: webserver-private |

NAT 规则的方向基于路由查找的结果。

配置的安全策略可以从 Untrust-L3 访问服务器，如下所示：

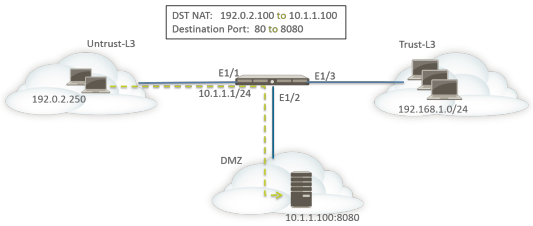
| NAME | Source | | Destination | | APPLICATION | SERVICE | ACTION | PROFILE | OPTIONS |
|---|---|---|---|---|---|---|---|---|---|
| | ZONE | ADDRESS | ZONE | ADDRESS | | | | | |
| Webserver access | Untrust-L3 | any | DMZ | Webserver-pu... | web-browsing | any | Allow | none | |



© 2019 Palo Alto Networks, Inc.

## 带有端口转换示例的目标 *NAT*

在此示例中，Web 服务器配置为侦听端口 8080 上的 HTTP 流量。客户端访问使用 IP 地址 192.0.2.100 和 TCP 端口 80 的 Web 服务器。目标 NAT 规则配置为将 IP 地址和端口转换为 10.1.1.100 和 TCP 端口 8080。为专用 Web 服务器 (10.1.1.100) 和公共 Web 服务器 (192.0.2.100) 配置地址对象。




必须在防火墙上配置以下 NAT 和安全规则：

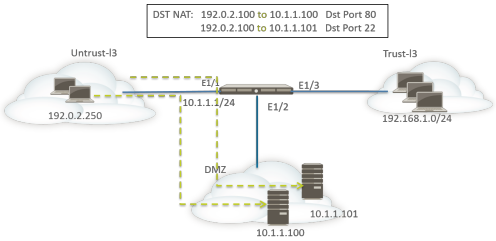
| NAME | TAGS | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|
| | | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| Dst NAT-webserver | none | Untrust-L3 | Untrust-L3 | any | any | Servers-public | any | none | destination-translation<br>address: webserver-private<br>port: 8080 |

| NAME | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| Webserver access | none | universal | Untrust-L3 | any | any | any | DMZ | Servers-public | any | web-browsing | any | Allow |

使用 **`show session all`** CLI 命令验证转换。

## 目标 *NAT* 示例 — 一对多映射

在此示例中，一个 IP 地址映射为两个不同的内部主机。防火墙使用应用程序识别防火墙转发流量的目标内部主机。




所有 HTTP 流量都发送到主机 10.1.1.100，SSH 流量发送到服务器 10.1.1.101。需要以下地址对象：

- 用于服务器的一个前导转换 IP 地址的地址对象
- 用于 SSH 服务器的实际 IP 地址的地址对象
- 用于 Web 服务器的实际 IP 地址的地址对象

创建了相应的地址对象：

- 公共服务器：192.0.2.100
- SSH 服务器：10.1.1.101
- 专用 Web 服务器：10.1.1.100

NAT 规则类似于下图：



© 2019 Palo Alto Networks, Inc.

| NAME | TAGS | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|
| | | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| Dst NAT-webserver | none | Untrust-L3 | Untrust-L3 | any | any | Servers-public | service-http | none | destination-translation<br>address: webserver-private |
| Dst NAT-SSH | none | Untrust-L3 | Untrust-L3 | any | any | Servers-public | custom-ssh | none | destination-translation<br>address: SSH-server |

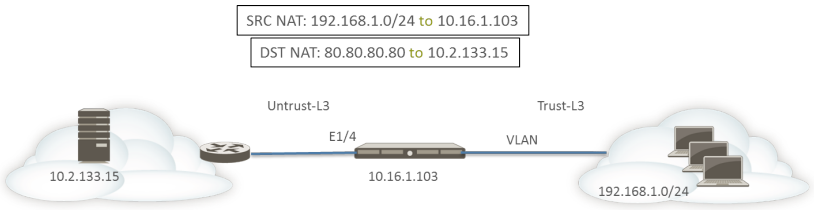
安全规则类似于下图：

| NAME | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| Webserver access | none | universal | Untrust-L3 | any | any | any | DMZ | Servers-public | any | web-browsing | any | Allow |
| SSH access | none | universal | Untrust-L3 | any | any | any | DMZ | Servers-public | any | ssh | any | Allow |

## 源和目标 *NAT* 示例

在此示例中，NAT 规则在客户端和服务器之间转换数据包的源和目标 IP 地址。

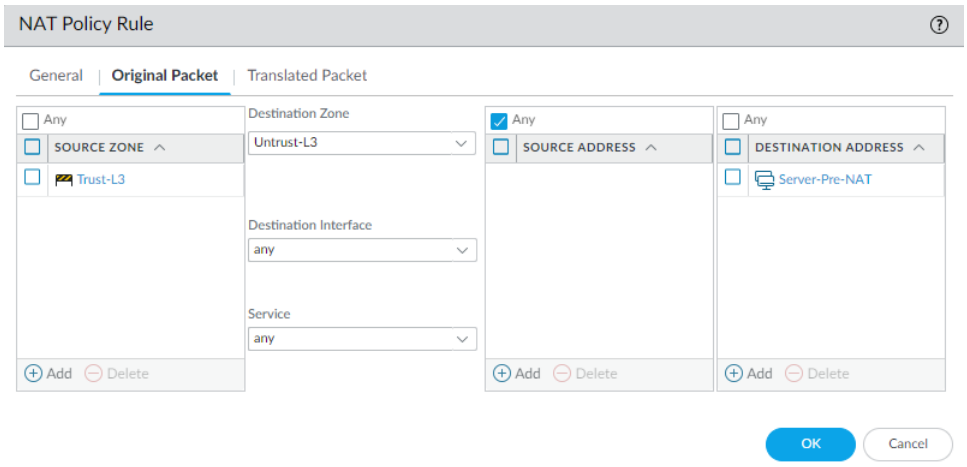
- 源 NAT — 从 Trust-L3 区域的客户端到 Untrust-L3 区域的服务器的数据包中的源地址将从 192.168.1.0/24 网络中的专用地址转换到防火墙 (10.16.1.103) 上出口端口的 IP 地址。动态 IP 和端口转换还会引起端口号转换。
- 目标 NAT — 从客户端到服务器的数据包中的目标地址将从服务器的公共地址 (80.80.80.80) 转换为服务器的专用地址 (10.2.133.15)。




为目标 NAT 创建了以下地址对象。

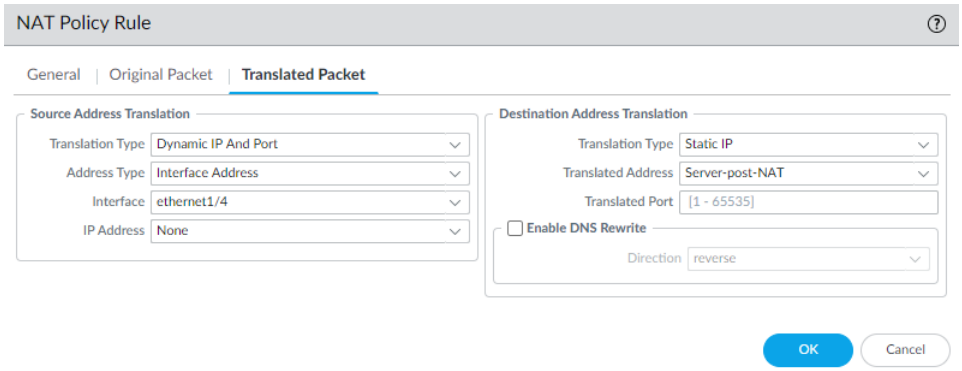
- 服务器前导 NAT：80.80.80.80
- 服务器后导 NAT：10.2.133.15

以下屏幕截图演示了如何为此示例配置源和目标 NAT 策略。





© 2019 Palo Alto Networks, Inc.




要验证转换，请使用 CLI 命令 **`show session all filter destination 80.80.80.80`**。客户端地址 192.168.1.11 及其端口号将转换至 10.16.1.103 和端口号。目标地址 80.80.80.80 将转换为 10.2.133.15。

## *Virtual Wire 源 NAT 示例*

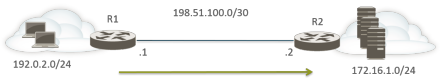
Palo Alto Networks 防火墙的 Virtual Wire 部署包括以透明方式为终端设备提供安全保障的优势。可以为 Virtual Wire 中配置的接口配置 NAT。允许所有 NAT 类型：源 NAT（动态 IP、动态 IP 和端口、静态）和目标 NAT。

因为 Virtual Wire 中的接口没有分配 IP 地址，因此无法将 IP 地址转换为接口 IP 地址。您必须配置 IP 地址池。

在虚拟线路接口上执行 NAT 时，建议将源地址转换为与相邻设备进行通信的子网不同的子网。防火墙将不会为 NAT 地址执行代理 ARP。必须在上游和下游路由器上配置相应的路由才能在 Virtual Wire 模式下转换数据包。相邻设备将只能解析对虚拟线路另一端设备接口上 IP 地址的 ARP 请求。有关代理 ARP 的更多说明，请参阅 NAT 地址池的代理 ARP。

在以下源 NAT 示例中，安全策略（未显示）将从名为 vw-trust 的虚拟线路区域配置为名为 vw-untrust 的区域。

在以下拓扑中，配置了两个路由器来提供子网 192.0.2.0/24 和 172.16.1.0/24 之间的连接。子网 198.51.100.0/30 中配置了路由器之间的链接。两个路由器上均配置了静态路由以在网络之间建立连接。在环境中部署防火墙之前，拓扑和各路由器的路由表类似于下图：




R1 上的路由：

| 目标 | 下一个跃点 |
|---|---|
| 172.16.1.0/24 | 198.51.100.2 |

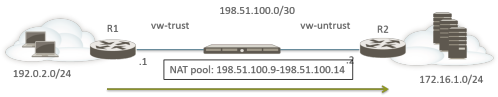
R2 上的路由：

| 目标 | 下一个跃点 |
|---|---|
| 192.0.2.0/24 | 198.51.100.1 |



© 2019 Palo Alto Networks, Inc.

现在，防火墙部署在两个第三层设备之间的 Virtual Wire 模式中。防火墙上配置了 198.51.100.9 - 198.51.100.14 范围的 NAT IP 地址池。子网 192.0.2.0/24 中的客户端访问网络 172.16.1.0/24 中的服务器的所有通信都将在到达 R2 时转换为 198.51.100.9 - 198.51.100.14 范围内的源地址。来自服务器的响应将定向到这些地址。



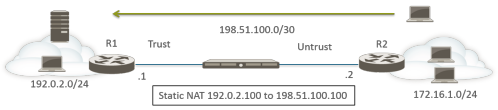

为了使得源 NAT 能够起作用，必须在 R2 配置适当的路由，从而不会丢弃发向其他地址的数据包。下面的路由表显示了 R2 上修改过的路由表；路由确保了传至目标 198.51.100.9 - 198.51.100.14（即子网 198.51.100.8/29 上的主机）的流量可以通过防火墙发回 R1。

R2 上的路由：

| 目标 | 下一个跃点 |
|---|---|
| 198.51.100.8/29 | 198.51.100.1 |

## Virtual Wire 静态 NAT 示例

在本例中，安全策略从名为 Trust 的虚拟线路配置为名为 Untrust 的虚拟线路。主机 192.0.2.100 静态转换为地址 198.51.100.100。启用 **Bi-directional**（双向）选项后，防火墙启用从 Untrust 区域至 Trust 区域的 NAT 策略。Untrust 区域上的客户端访问使用 IP 地址为 198.51.100.100 的服务器，防火墙转换为 198.0.2.100。由 192.0.2.100 中的服务器发起的任何连接都会转换为源 IP 地址 198.51.100.100。



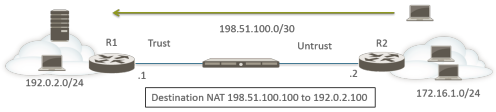

R2 上的路由：

| 目标 | 下一个跃点 |
|---|---|
| 198.51.100.100/32 | 198.51.100.1 |

| | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|
| NAME | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| Static NAT | Trust | Untrust | any | webserver-private | any | any | static-ip<br>webserver-public<br>bi-directional: yes | none |

## Virtual Wire 目标 NAT 示例

Untrust 区域的客户端访问使用 IP 地址为 198.51.100.100 的服务器，防火墙转换为 192.0.2.100。NAT 和安全策略都必须配置为从 Untrust 区域至 Trust 区域。




R2 上的路由：


© 2019 Palo Alto Networks, Inc.

| 目标 | 下一个跃点 |
| --- | --- |
| 198.51.100.100/32 | 198.51.100.1 |

| NAME | Original Packet | | | | | | Translated Packet | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| DST NAT | Untrust | Trust | any | any | webserver-public | any | none | destination-translation<br>address: webserver-private |



© 2019 Palo Alto Networks, Inc.

# NPTv6

IPv6-to-IPv6 Network Prefix Translation（IPv6 到 IPv6 网络前缀转换-NPTv6）用于执行一个 IPv6 前缀到另一个 IPv6 前缀的无状态静态转换（端口号不会更改）。NPTv6 有四大主要优势：

- 您可以阻止因从多个数据中心通告与提供商无关的地址而导致的非对称路由问题。
- NPTv6 允许通告更多特定路由，使返回流量可以到达传送此流量的同一防火墙。
- 专用地址和公共地址是独立的；可以在互不影响的情况下更改其中一个地址。
- 您可以将唯一本地地址转换为可全球路由地址。

此主题建立在对 NAT 的基本了解之上。在开始配置 NPTv6 之前，应确保您熟悉 NAT 概念。

- NPTv6 概述
- NPTv6 的运作方式
- NDP 代理
- NPTv6 和 NDP 代理示例
- 创建 NPTv6 策略

## NPTv6 概述

此部分介绍 IPv6-to-IPv6 Network Prefix Translation（IPv6 到 IPv6 网络前缀转换）(NPTv6) 以及如何对其进行配置。NPTv6 在 RFC 6296 内定义。Palo Alto Networks 不会实施 RFC 中定义的所有功能，但与已实施 RFC 功能兼容。

NPTv6 可执行一个 IPv6 前缀到另一个 IPv6 前缀的无状态转换。无状态表示它不会跟踪已转换地址上的端口或会话。NPTv6 与 NAT66 不同，它是有状态的。Palo Alto Networks 支持 NPTv6 RFC 6296 前缀转换；不支持 NAT66。

若使用 IPv4 空间中的受限地址，要求 NAT 将专用、不可路由 IPv4 地址转换为一个或多个可全局路由 IPv4 地址。

对于使用 IPv6 寻址的组织，由于 IPv6 地址的充足性，无需将 IPv6 地址转换为 IPv6 地址。但是，存在使用 NPTv6 的理由转换防火墙上的 IPv6 前缀。

NPTv6 转换 IPv6 地址的前缀部分,而不是主机部分或应用程序端口号.主机部分只是简单的复制，因此与防火墙的另一端相同。主机部分在数据包标头中仍然可见。

- NPTv6 不提供安全保障
- 针对 NPTv6 的型号支持
- 唯一本地地址
- 使用 NPTv6 的理由

### *NPTv6* 不提供安全保障

请务必了解 NPTv6 不支持安全性。通常，无状态网络地址转换不提供任何安全性，只是提供地址转换功能。NPTv6 不会隐藏或转换端口号。您必须正确设置各个方向的防火墙安全策略才能确保按照期望控制流量。

### 针对 *NPTv6* 的型号支持

以下型号支持 NPTv6（NPTv6 带有硬件查找，但数据包经过 CPU）：PA-7000 系列、PA-5200 系列、PA-800 防火墙和 PA-220 防火墙。VM 系列型号受支持，但不具备让硬件执行会话查找的能力。


© 2019 Palo Alto Networks, Inc.

## 唯一本地地址

RFC 4193 唯一本地 IPv6 单播地址定义了唯一本地地址 (ULA)，这些地址是 IPv6 单播地址。这些地址可视为 RFC 1918 专用 Private Internet 的地址分配中识别的专用 IPv4 地址的 IPv6 对等地址，这些地址不能全球路由。

ULA 在全球唯一，但并不是全球可路由。ULA 用于本地通信，且在有限区域（如站点或少数站点之间）内可路由。Palo Alto Networks 建议您不要分配 ULA，但配置有 NPTv6 的防火墙将转换发送到此防火墙的前缀，包括 ULA。

## 使用 *NPTv6* 的理由

尽管并不缺乏公共的可全局路由 IPv6 地址，但您可能会出于某些原因想要转换 IPv6 地址。NPTv6：

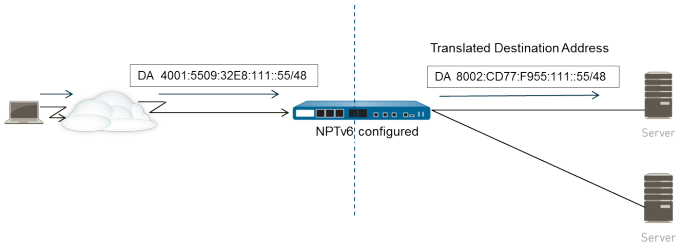
- 阻止非对称路由 — 如果与提供商无关的地址空间（例如，/48）由多个数据中心通告到全球 Internet，可能会出现非对称路由。通过使用 NPTv6，您可以从区域防火墙通告更多特定路由，返回流量将传至转换程序用于转换源 IP 地址的同一防火墙。
- 提供地址独立 — 如果全球前缀发生更改（例如，由 ISP 更改或因组织合并更改），您不需要更改本地网络中使用的 IPv6 前缀。反之，您可以更改内部地址，无需破坏用于访问互联网中专用网络内的服务的地址。无论是哪种情况，请更新 NAT 规则，而不是重新分配网络地址。
- 转换 **ULA** 以进行路由 — 您的专用网络中可以分配唯一本地地址，并可以让防火墙将其转换为可全局路由地址。因此，您可以便捷的使用地址寻址和转换的可路由功能。
- 降低 **IPv6** 前缀的暴露 — 如果您没有转换过网络前缀，IPv6 前缀的暴露会降低，但 NPTv6 并不是一种安全措施。各 IPv6 地址的接口标识符部分不会转换；此标识符在防火墙两端仍然一样，且对可看见此数据包标头的任何用户都可视。此外，这些前缀并不安全，它们可以由其他用户确定。

# NPTv6 的运作方式

在为 NPTv6 配置策略时，Palo Alto Networks 防火墙会在两个方向执行静态一对一 IPv6 转换。此转换基于 RFC 6296 中介绍的算法。

在一种使用案例中，执行 NPTv6 的防火墙位于内部网络和使用可全局路由前缀的外部网络（如 Internet）之间。当数据报流进出站方向时，内部源前缀将替换为外部前缀，称为源转换。

在另一种使用案例中，当数据报流进入站方向时，目标前缀将替换为内部前缀（称为目标转换）。下图演示了目标转换和 NPTv6 的特征：只会转换 IPv6 地址的前缀部分。不会转换地址的主机部分，此部分仍与防火墙的另一端相同。在下图中，主机标识符在防火墙的两端均为 111::55。




请务必了解 NPTv6 不支持安全性。在您计划 NPTv6 NAT 策略时，请记住一同配置各个方向的安全策略。

NAT 或 NPTv6 策略规则的源地址和转换地址不能同时设置为“任意”。

在您希望进行 IPv6 前缀转换的环境中，三个防火墙功能协同工作。NPTv6 NAT 策略、安全策略和 NDP 代理。

防火墙不会转换以下内容：

- 防火墙在临近对象发现 (ND) 高速缓存中的地址。
- 子网 0xFFFF（根据 RFC 6296 附录 B）。
- IP 多播地址。



© 2019 Palo Alto Networks, Inc.

- 前缀长度为 /31 或更短的 IPv6 地址。
- 本地链接地址。如果防火墙在 Virtual Wire 模式下运行，则没有 IP 地址需要转换，且防火墙不会转换本地链接地址。
- 使用 TCP 身份验证选项 (RFC 5925) 进行对等设备验证的 TCP 会话的地址。

在使用 NPTv6 时，快速路径流量的性能将受到影响，因为 NPTv6 在慢速路径内执行。

如果防火墙在隧道起源和终止，NPTv6 只会与 IPSec IPv6 一起使用。IPSec 流量中转将失败，因为源和/或目标 IPv6 地址会修改。可封装数据包的 NAT 遍历技术允许 IPSec IPv6 与 NPTv6 一起使用。

- 校验和中性映射
- 双向转换
- 应用于特定服务的 NPTv6

## 校验和中性映射

防火墙执行的 NPTv6 映射转换为校验和中性，表示“...他们将生成 IP 标头，当使用标准 Internet 校验和算法 [RFC 1071] 计算校验和时，这些 IP 标头将生成相同的 IPv6 伪标头校验和。” 有关校验和中性映射的详细信息，请参阅 RFC 6296 中的 2.6 小节。

如果使用 NPTv6 执行目标 NAT，您可以在 **`test nptv6`** CLI 命令的语法中提供防火墙接口的内部 IPv6 地址和外部前缀/前缀长度。CLI 会响应校验和中性，以及要在 NPTv6 配置中用来访问该目标的公共 IPv6 地址。

## 双向转换

当您 创建 NPTv6 策略 时，**Translated Packet**（已转换数据包）选项卡中的 **Bi-directional**（双向）选项提供一种方便的方法，从而可以让防火墙创建相应的 NAT 或 NPTv6 转换，方向与您配置的转换相反。默认情况下，禁用 **Bi-directional**（双向）转换。

如果启用 *Bi-directional*（双向转换），确保正确使用安全策略双向控制流量很重要。如果不使用这种策略，*Bi-directional*（双向）功能将允许数据包自动双向转换，您可能不希望这样。

## 应用于特定服务的 *NPTv6*

NPTv6 的 Palo Alto Networks 实施提供了筛选数据包的功能，用以限制要进行转换的数据包。请记住，NPTv6 不执行端口转换。不存在动态 IP 和端口 (DIPP) 转换的概念，因为 NPTv6 只转换 IPv6 前缀。但是，您可以指定只有特定服务端口的数据包可进行 NPTv6 转换。要执行此操作，请创建 NPTv6 策略，该策略在原始数据包中指定 **Service**（服务）。

# NDP 代理

IPv6 的邻近对象发现协议 (NDP) 执行的功能类似于 IPv4 的地址解析协议 (ARP) 提供的功能。RFC 4861 定义了 IPv6 的邻近对象发现。主机、路由器和防火墙使用 NDP 确定已连接链路上的邻居的链路层地址，以跟踪哪些邻居可以访问，并更新已发生更改的邻居的链路层地址。对等设备会通告它们自己的 MAC 地址和 IPv6 地址，同时会从对等设备征求地址。

当节点包含可以代表此节点转发数据包的邻居设备时，NDP 还支持代理概念。设备（防火墙）会执行 NDP 代理的角色。

Palo Alto Networks 防火墙在它们的接口上支持 NDP 和 NDP 代理。如果将防火墙配置为充当地址的 NDP 代理，将允许防火墙发送邻近对象发现 (ND) 通告，并响应来自对等设备（请求分配给防火墙后的设备的以 IPv6 为前缀的 MAC 地址）的 ND 征求。您也可以为防火墙不会响应其代理请求的设备配置地址（求反地址）。

实际上，默认情况下已启用 NDP，出于以下原因，您需要在配置 NPTv6 时配置 NDP 代理：


© 2019 Palo Alto Networks, Inc.

- NPTv6 的无状态特性需要一种方法来构造防火墙，使其响应发送给指定 NDP 代理地址的 ND 数据包，而不响应求反 NDP 代理地址。

  建议您对 *NDP* 代理配置中的邻居地址进行求反，因为 *NDP* 代理指示防火墙将访问防火墙后的这些地址，但是这些邻居不在防火墙后。

- NDP 会使防火墙将邻居的 MAC 地址和 IPv6 地址保存在其 ND 高速缓存中。（请参阅NPTv6 和 NDP 代理示例中的图片。）防火墙不会为在其 ND 高速缓存中找到地址执行 NPTv6 转换，因为这样做会引入冲突。如果高速缓存中地址的主机部分正好与邻居地址的主机部分重叠，且高速缓存中的前缀转换为与该邻居相同的前缀（因为防火墙上的传出接口与邻居属于同一子网），那么您将有一个与邻居的合法 IPv6 地址完全相同的转换地址，并会发生冲突。（如果在 ND 高速缓存中的地址上尝试执行 NPTv6 转换，信息性 syslog 消息将记录以下事件：`NPTv6 Translation Failed.`）

当启用 NDP 代理的接口收到为 IPv6 地址请求 MAC 地址的 ND 请求时，将执行以下序列：

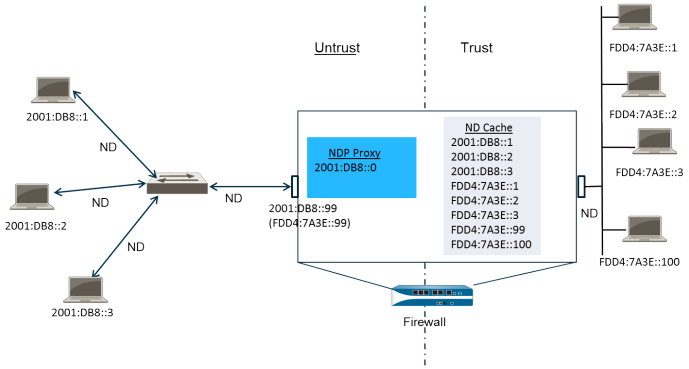
- 防火墙搜索 ND 高速缓存以确保其中不存在请求的 IPv6 地址。如果存在，防火墙将忽略 ND 请求。
- 如果源 IPv6 地址为 0，表示数据包为重复地址检测数据包，防火墙将忽略 ND 请求。
- 防火墙执行 NDP 代理地址的最长前缀匹配搜索并查找请求中地址的最佳匹配项。如果选中此匹配项的求反字段（在 NDP 代理列表中），防火墙将丢弃 ND 请求。
- 只有与最长前缀匹配搜索结果匹配，且匹配地址不是求反地址，NDP 代理才会响应 ND 请求。防火墙会使用 ND 数据包进行响应，提供自己的 MAC 地址作为至查询目标的下一个跃点的 MAC 地址。

为了成功的支持 NDP，防火墙不会为以下各项执行 NDP 代理：

- 重复地址检测 (DAD)。
- ND 高速缓存中的地址（因为此类地址不属于防火墙；它们属于已发现的邻居）。

# NPTv6 和 NDP 代理示例

下图演示了 NPTv6 和 NDP 代理如何协同运作。




- NPTv6 示例中的 ND 高速缓存
- NPTv6 示例中的 NDP 代理
- NPTv6 示例中的 NPTv6 转换
- 不会转换 ND 高速缓存中的邻居

## *NPTv6 示例中的 ND 高速缓存*

在上方的示例中，多个对等设备通过一个交换机连接到防火墙，在对等设备和交换机之间，交换机和防火墙之间以及防火墙和可信站点上的设置之间发生 ND。

防火墙认识对等设备时，会将这些设备的地址保存到其 ND 高速缓存中。可信对等设备 FDDA:7A3E::1、FDDA:7A3E::2 和 FDDA:7A3E::3 连接到可信站点上的防火墙。FDDA:7A3E::99 是防火墙自身的未转换地址，防火墙面向公众的地址为 2001:DB8::99。不可信站点上的对等设备地址已被发现并显示在 ND 高速缓存中：2001:DB8::1、2001:DB8::2 和 2001:DB8::3。



© 2019 Palo Alto Networks, Inc.

### *NPTv6 示例中的 NDP 代理*

在我们方案中，我们想要防火墙充当防火墙后的设备前缀的 NDP 代理。如果防火墙作为一组指定地址/范围/前缀的 NDP 代理，且能在 ND 请求或通告中看到此范围内的地址，那么只要具有此特定地址的设备不先响应，该地址不在 NDP 代理配置中进行求反，且该地址不在 ND 高速缓存中，防火墙都会进行响应。防火墙会执行前缀转换（如下所述）并将数据包发送到可信站点，该站点的地址可能已分配到设备，也可能未分配到设备。

在此示例中，ND 代理表包含网络地址 2001:DB8::0。当接口看到 2001:DB8::100 的 ND 时，L2 交换机上没有其他设备会认领此数据包，因此代理范围会让防火墙认领此数据包，在转换为 FDD4:7A3E::100 后，防火墙会将其发出到可信站点。

### *NPTv6 示例中的 NPTv6 转换*

在此示例中，**Original Packet**（原始数据包）的 **Source Address**（源地址）配置为 FDD4:7A3E::0，**Destination**（目标）配置为 **Any**（任意）。**Translated Packet**（已转换数据包）的 **Translated Address**（已转换地址）配置为 2001:DB8::0。

因此，带有源 FDD4:7A3E::0 的传出数据包将转换为 2001:DB8::0。在网络 2001:DB8::0 中带有目标前缀的传入数据包将转换为 FDD4:7A3E::0。

### 不会转换 *ND* 高速缓存中的邻居

在我们的示例中，防火墙后存在带有主机标识符 :1、:2 和 :3 的主机。如果这些主机的前缀转换为防火墙范围外的前缀，且这些设备也具有主机标识符 :1、:2 和 :3，因为地址的主机标识符部分保留不变，因此生成的转换地址将属于现有设备，从而出现寻址冲突。为了避免与重叠的主机标识符发生冲突，NPTv6 不会转换在其 ND 高速缓存中找到的地址。

## 创建 NPTv6 策略

如果您想要将 NAT NPTv6 策略配置为将一个 IPv6 前缀转换为另一个 IPv6 前缀，请执行此任务。该任务的先决条件如下：

- 启用 IPv6。选择 **Device**（设备）> **Setup**（设置）> **Session**（会话）。单击 **Edit**（编辑）并选择 **IPv6 Firewalling**（**IPv6** 防火墙）。
- 使用有效的 IPv6 地址并在启用 IPv6 的情况下配置第 3 层以太网接口。选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择一个接口并在 **IPv6** 选项卡上选择 **Enable IPv6 on the interface**（在此接口上启用 **IPv6**）。
- 请创建网络安全规则，因为 NPTv6 不提供安全保障。
- 决定您是想要源转换、目标转换还是两者都要。
- 标识要应用此 NPTv6 策略的区。
- 识别原始 IPv6 前缀和已转换 IPv6 前缀。

STEP 1 | 创建新的 NPTv6 策略。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，为 NPTv6 策略规则输入描述性 **Name**（名称）。
3. （可选）输入 **Description**（说明）和 **Tag**（标签）。
4. 对于 **NAT Type**（**NAT** 类型），请选择 **NPTv6**。

STEP 2 | 指定传入数据包的匹配条件；匹配所有条件的数据包将进行 NPTv6 转换。

两种转换类型都需要使用区。

1. 在 **Original Packet**（原始数据包）选项卡中，对于 **Source Zone**（源区域），请保留 **Any**（任何）或 **Add**（添加）将应用此策略的源区域。
2. 输入将应用此策略的 **Destination Zone**（目标区）。


© 2019 Palo Alto Networks, Inc.

3. （可选）选择一个 **Destination Interface**（目标接口）。
4. （可选）选择一个 **Service**（服务）来限制所转换的数据包类型。
5. 如果您正在执行源转换，请输入 **Source Address**（源地址）或选择 **Any**（任意）。该地址可以是一个地址对象。以下约束应用于 **Source Address**（源地址）和 **Destination Address**（目标地址）：
   - 尽管前缀中的前导 0 可以省略，但 **Original Packet**（原始数据包）和 **Translated Packet**（已转换数据包）的 **Source Address**（源地址）和 **Destination Address**（目标地址）的前缀必须是 xxxx:xxxx::/yy 格式。
   - IPv6 地址不能定义接口标识符（主机）部分。
   - 支持的前缀长度范围为 /32 - /64。
   - **Source Address**（源地址）和 **Destination Address**（目标地址）不能同时设置为 **Any**（任意）。
6. 如果您正在执行源转换，可以选择性地输入 **Destination Address**（目标地址）。如果您正在执行目标转换，则必须输入 **Destination Address**（目标地址）。目标地址（允许的地址对象）必须是子网掩码，而不仅仅是 IPv6 地址，也不是范围。前缀长度必须是 /32 到 /64（含）的值。本例中为 2001:db8::2/32。

STEP 3 | 指定已转换数据包。

1. 在 **Translated Packet**（已转换数据包）选项卡上，如果您想执行源转换，请为源地址转换部分中的 **Translation Type**（转换类型）中选择 **Static IP**（静态 IP）。如果您不想执行源转换，请选择 **None**（无）。
2. 如果您选择 **Static IP**（静态 IP），将显示 **Translated Address**（已转换地址）字段。输入已转换 IPv6 前缀或地址对象。请参阅之前步骤中列出的约束。

   最佳实践是将您的 *Translated Address*（已转换地址）配置为防火墙的不可信接口地址的前缀。例如，如果您的不可信接口地址为 *2001:1a:1b:1::99/64*，请将您的 *Translated Address*（已转换地址）配置为 *2001:1a:1b:1::0/64*。
3. （可选）如果想要防火墙按所配置转换的相反方向创建相应的 NPTv6，则选择 **Bi-directional**（双向）。

   如果启用 *Bi-directional*（双向）转换，确保正确使用安全策略规则双向控制流量很重要。如果不使用这种策略规则，*Bi-directional*（双向）转换将允许数据包自动双向转换，您可能不希望这样。
4. 如果您想要执行目标转换，请选择 **Destination Address Translation**（目标地址转换）。在 **Translated Address**（已转换地址）字段中，选择一个地址对象或输入您的内部目标地址。
5. 单击 **OK**（确定）。

STEP 4 | 配置 NDP 代理。

如果将防火墙配置为充当地址的 NDP 代理，将允许防火墙发送邻近对象发现 (ND) 通告，并响应来自对等设备（请求分配给防火墙后的设备的以 IPv6 为前缀的 MAC 地址）的 ND 征求。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）并选择一个接口。
2. 在 **Advanced**（高级）> **NDP Proxy**（**NDP** 代理）选项卡上，选择 **Enable NDP Proxy**（启用 **NDP** 代理）并单击 **Add**（添加）。
3. 为启用了 NDP 代理的设备输入 **IP Address(es)**（**IP** 地址）。可以是一个地址、一定范围内的地址或前缀和前缀长度。IP 地址的顺序无关紧要。这些地址最好与您在 NPTv6 策略中配置的已转换地址相同。

   如果地址为子网，*NDP* 代理会响应子网中的所有地址，因此您应该按照下一步所述，列出选择了 *Negate*（求反）的子网内的邻居。
4. （可选）为不想启用 NDP 代理的设备输入一个或更多地址，然后选择 **Negate**（求反）。例如，从前一步中配置的 IP 地址范围或前缀范围中，您可以对较小的地址子网进行求反。建议对防火墙邻居的地址进行求反。



© 2019 Palo Alto Networks, Inc.

STEP 5 | 提交配置。

单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# NAT64

NAT64 提供一种转换到 IPv6 的方法，同时还需要与 IPv4 网络进行通信。当您需要仅从 IPv6 网络到 Ipv4 网络进行通信时，可使用 NAT64 将源地址和目标地址从 IPv6 转换为 IPv4，反之亦然。NAT64 允许 IPv6 客户端访问 IPv4 服务器，并允许 IPv4 客户端访问 IPv6 服务器。配置 NAT64 之前，您应对 NAT 有所了解。


- NAT64 概况
- 嵌入 IPv4 的 IPv6 地址
- DNS64 服务器
- 路径 MTU 发现
- IPv6 启动的通信
- 为 IPv6 启动的通信配置 NAT64
- 为 IPv4 启动的通信配置 NAT64
- 通过端口转换为 IPv4 启动的通信配置 NAT64


## NAT64 概况

您可以在 Palo Alto Networks 防火墙上配置两种类型的 NAT64 转换；每种均可在两个 IP 地址系列之间进行双向转换：

- 防火墙支持IPv6 启动的通信的状态 NAT64，即，将多个 IPv6 地址映射到一个 IPv4 地址，从而保留 IPv4 地址。（不支持无状态 NAT64，即，将一个 IPv6 地址映射到一个 IPv4 地址，因此不保留 IPv4 地址。）为 IPv6 启动的通信配置 NAT64。
- 防火墙支持 IPv4 启动的与静态绑定的通信，将 IPv4 地址和端口号映射到 IPv6 地址。为 IPv4 启动的通信配置 NAT64。还支持端口重写，即，通过将 IPv4 地址和端口号转换为具有多个端口号的 IPv6 地址，从而保留更多的 IPv4 地址。通过端口转换为 IPv4 启动的通信配置 NAT64。

单个 IPv4 地址可用于 NAT44 和 NAT64；不会保留 NAT64 的 IPv4 地址池。

NAT64 在第 3 层接口、子接口和隧道接口上运行。要在 Palo Alto Networks 防火墙上使用 NAT64 进行 IPv6 启动的通信，必须具有第三方DNS64 服务器或解决方案，以将 DNS 查询功能与 NAT 功能分离。DNS64 服务器通过将从公共 DNS 服务器接收到的 IPv4 地址编码到 IPv6 主机的 IPv6 地址，实现 IPv6 主机和 IPv4 DNS 服务器之间的转换。

Palo Alto Networks 支持以下 NAT64 功能：

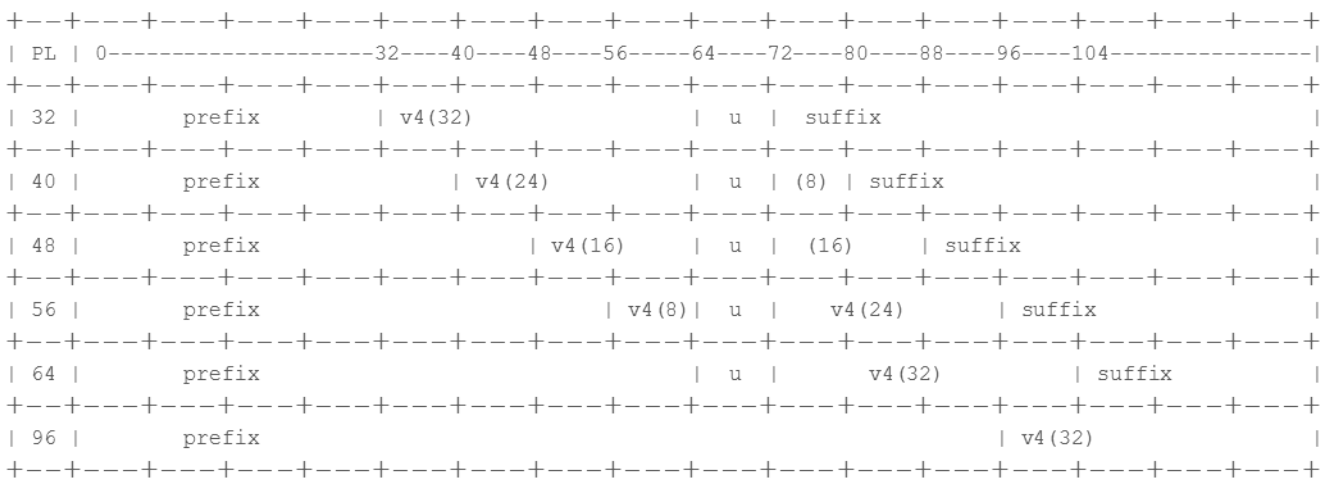
- 发夹 (NAT U-Turn)；此外，NAT64 通过丢弃具有源前缀 64::/n 的所有传入 IPv6 数据包来防止发夹回环攻击。
- 根据 RFC 6146 转换 TCP/UDP/ICMP 数据包，防火墙尽力转换不使用应用级网关 (ALG) 的其他协议。例如，防火墙可以转换 GRE 数据包。该转换具有与 NAT44 相同的限制：如果您没有可以使用单独控制和数据通道的协议 ALG，则防火墙可能无法了解返回流量。
- 根据 RFC 4884，在原始数据包字段 ICMP 长度属性中 IPv4 和 IPv6 之间的转换。

## 嵌入 IPv4 的 IPv6 地址

NAT64 使用嵌入 IPv4 的 IPv6 地址，如 RFC 6052、IPv4/Pv6 转换器的 IPv6 地址所述。嵌入 IPv4 的 IPv6 地址是一个 IPv6 地址，其中 32 位有一个已编码 IPv4 地址。IPv6 前缀长度（图中的 PL）确定 IPv6 地址中已编码的 IPv4 地址位置，如下所示：



© 2019 Palo Alto Networks, Inc.




防火墙支持转换使用这些前缀的 /32、/40、/48、/56、/64 和 /96 子网。单个防火墙支持多个前缀；每个 NAT64 规则使用一个前缀。该前缀可以是众所周知的前缀 (64:FF9B::/96)，也可以是对于控制地址转换器（DNS64 设备）的组织唯一的网络特定前缀 (NSP)。NSP 通常是组织的 IPv6 前缀内的网络。DNS64 设备通常将 u 字段和后缀设置为零；防火墙则忽略这些字段。

## DNS64 服务器

如果要使用 DNS 并通过 IPv6 启动的通信执行 NAT 64 转换，则必须使用第三方 DNS64 服务器或其他使用众所周知的前缀或您的 NSP 设置的 DNS64 解决方案。当 IPv6 主机尝试访问互联网上的 IPv4 主机或域时，DNS64 服务器会向授权 DNS 服务器查询映射到该主机名的 IPv4 地址。DNS 服务器将一个地址记录（A 记录）返回给包含主机名 IPv4 地址的 DNS64 服务器。

DNS64 服务器反过来又将 IPv4 地址转换为十六进制，并根据前缀长度将其编码为设置使用的 IPv6 前缀的适当的八位字节（众所周知的前缀或您的 NSP），从而导致嵌入 IPv4 的 IPv6 地址。DNS64 服务器向 IPv6 主机发送 AAAA 记录，将 IPv4 嵌入的 IPv6 地址映射到 IPv4 主机名。

## 路径 MTU 发现

IPv6 不会对数据包进行分片，因此防火墙采用两种方法来降低数据包分片需求：

- 当防火墙转换 DF（不分片）位为零的 IPv4 数据包时，表示发件人希望防火墙对太大的数据包进行分片，但防火墙不会对 IPv6 网络的数据包进行分片（转换之后），因为 IPv6 不会分片数据包。相反，您可以配置防火墙在转换之前分片 IPv4 数据包的最小规模。该设置为 **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小网络 **MTU**），符合 RFC 6145，IP/ICMP 转换算法。您可以将 **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小网络 **MTU**）设置为其最大值（**Device**（设备）> **Setup**（设置）> **Session**（会话）），这将使防火墙将 IPv4 数据包分片成 IPv6 的最小规模，然后再将其转换为 IPv6。（**NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小网络 **MTU**）不会更改接口 MTU。）
- 防火墙用来减少分片的另一种方法是路径 MTU 发现 (PMTUD)。在 IPv4 启动的通信中，如果待转换的 IPv4 数据包设置为 DF 位，出口接口的 MTU 小于数据包，则防火墙使用 PMTUD 丢弃数据包，并返回 ICMP“目标无法访问 — 需要进行分片”消息给源。源降低了该目标的路径 MTU，并重新发送数据包，直到连续减少路径 MTU 以允许传送数据包为止。

## IPv6 启动的通信

IPv6 向防火墙启动的通信类似于 IPv4 拓扑的源 NAT。当 IPv6 主机需要与 IPv4 服务器进行通信时，为 IPv6 启动的通信配置 NAT64。


© 2019 Palo Alto Networks, Inc.

在 NAT64 策略规则中，将原始源配置为 IPv6 主机地址或“任何”。将目标 IPv6 地址配置为众所周知的前缀或 DNS64 服务器使用的 NSP。（不用在规则中配置完整的 IPv6 目标地址。）

如果需要使用 DNS，则需要使用 DNS64 服务器将 IPv4 DNS “A” 结果转换为与 NAT64 前缀合并的“AAAA”结果。如果不使用 DNS，则需要按照 RFC 6052 规则使用防火墙上配置的 IPv4 目标地址和 NAT64 前缀创建地址。

对于使用 DNS 的环境，下面的示例拓扑说明了与 DNS64 服务器的通信。DNS64 服务器必须设置为使用众所周知的前缀 64:FF9B::/96 或您的网络特定前缀，该前缀必须符合 RFC 6052（/32、/40、/48、/56、/64 或 /96）。

在防火墙的已转换侧，为了实现状态 NAT64，转换类型必须是动态 IP 和端口。您将源转换地址配置为防火墙上出口接口的 IPv4 地址。您不用配置目标转换字段；防火墙首先通过查找规则的原始目标地址中的前缀长度，然后根据前缀，从传入数据包中的原始目标 IPv6 地址中提取已编码的 IPv4 地址，进而转换地址。

在防火墙查看 NAT64 规则之前，防火墙必须进行路由查找，以找到传入数据包的目标安全区域。防火墙无法路由到 NAT64 前缀，因此必须确保通过目标区域分配可以访问 NAT64 前缀。防火墙可能会将 NAT64 前缀分配给默认路由，或因没有其路由而删除 NAT64 前缀。因为 NAT64 前缀不在其路由表中，防火墙不会找到与出口接口和区域相关联的目标区域。

您还必须配置隧道接口（没有终止点）。您将 NAT64 前缀应用到隧道并应用适当的区域，以确保带 NAT64 前缀的 IPv6 通信分配到适当的目标区域。如果 IPv6 流量与 NAT64 规则不匹配，隧道还具有使用 NAT64 前缀丢弃该流量的优势。您在防火墙上配置的路由协议可用于查找其路由表中的 IPv6 前缀，从而找到目标区域，然后查看 NAT64 规则。

下图说明了 DNS64 服务器在名称解析过程中的作用。在此示例中，DNS64 服务器配置为使用众所周知的前缀 64:FF9B::/96。

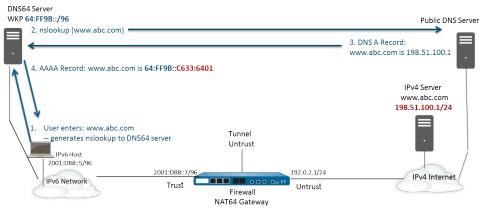
1 显示动态组定义的两个示例。IPv6 主机的用户输入 URL www.abc.com，为 DNS64 服务器生成名称服务器查找 (nslookup)。

2.DNS64 服务器向 www.abc.com 的公共 DNS 服务器发送一个 nslookup，请求其 IPv4 地址。

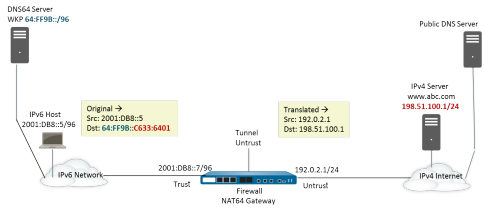
3.DNS 服务器返回一个向 DNS64 服务器提供 IPv4 地址的 A 记录。

4.DNS64 服务器向 IPv6 用户发送一条 AAAA 记录，将 IPv4 点分十进制地址 198.51.100.1 转换为十六进制数 C633:6401，并将其嵌入到自己的 IPv6 前缀 64:FF9B::/96 中。[198 = C6 hex; 51 = 33 hex; 100 = 64 hex; 1 = 01 hex.] The result is IPv4-Embedded IPv6 Address 64:FF9B::C633:6401.

请记住，在 /96 前缀中，IPv4 地址是 IPv6 地址中已编码的最后四个八位字节。如果 DNS64 服务器使用 /32、/40、/48、/56 或 /64 前缀，则 IPv4 地址按 RFC 6052 所示进行编码。




进行透明名称解析时，IPv6 主机向防火墙发送包含其 IPv6 源地址和 IPv6 目标地址 64:FF9B::C633:6401 的数据包，由 DNS64 服务器确定。防火墙根据您的 NAT64 规则执行 NAT64 转换。






© 2019 Palo Alto Networks, Inc.

# 为 IPv6 启动的通信配置 NAT64

该配置任务及其地址对应于 IPv6 启动的通信中的数字。

STEP 1 | 启用 IPv6 以在防火墙上运行。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 选择 **Enable IPv6 Firewalling**（启用 **IPv6** 防火墙）。
3. 单击 **OK**（确定）。

STEP 2 | 为 IPv6 目标地址创建一个地址对象（预转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64-IPv4 服务器。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并输入与 RFC 6052（/32、/40、/48、/56、/64 或 /96）兼容的子网掩码的 IPv6 前缀。这是 DNS64 服务器上配置的众所周知的前缀或是特定于网络的前缀。

   对于本示例，请输入 64:FF9B::/96。

   源和目标必须具有相同的子网掩码（前缀长度）。

   （无需输入完整的目标地址，因为根据前缀长度，防火墙会从传入数据包的原始目标 IPv6 地址中提取已编码的 IPv4 地址。在此示例中，传入数据包的前缀使用十六进制为 C633:6401 进行编码，这也是 IPv4 目标地址 198.51.100.1。）
4. 单击 **OK**（确定）。

STEP 3 | （可选）为 IPv6 源地址创建一个地址对象（预转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称）。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码）并输入 IPv6 主机的地址，在本例中为 2001:DB8::5/96。
4. 单击 **OK**（确定）。

STEP 4 | （可选）为 IPv4 源地址创建一个地址对象（已转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称）。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并输入防火墙出口接口的 IPv4 地址，在本例中为 192.0.2.1。
4. 单击 **OK**（确定）。

STEP 5 | 创建 NAT64 规则。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入 NAT64 规则的 **Name**（名称），例如 nat64_ipv6_init。
3. （可选）输入 **Description**（说明）。
4. 对于 **NAT Type**（**NAT** 类型），请选择 **nat64**。

STEP 6 | 指定原始的源信息和目标信息。

1. 对于 **Original Packet**（原始数据包），**Add**（添加）**Source Zone**（源区域），这可能是一个信任区域。
2. 选择 **Destination Zone**（目标区域），在本示例中为不信任区域。
3. （可选）选择 **Destination Interface**（目标接口）或默认（**any**（任何））。


© 2019 Palo Alto Networks, Inc.

4. 对于 **Source Address**（源地址），选择 **Any**（任何）或 **Add**（添加）您为 IPv6 主机创建的地址对象。
5. 对于 **Destination Address**（目标地址），**Add**（添加）您为 IPv6 目标地址创建的地址对象，在本例中为 nat64-IPv4 Server。
6. （可选）对于 **Service**（服务），请选择 **any**（任何）。

STEP 7 | 指定已转换的数据包信息。

1. 对于 **Translated Packet**（已转换数据包），在 **Source Address Translation**（源地址转换）的 **Translation Type**（转换类型）中，选择 **Dynamic IP and Port**（动态 IP 和端口）。
2. 对于 **Address Type**（地址类型），请执行以下操作之一：
   - 选择 **Translated Address**（已转换地址）并 **Add**（添加）您为 IPv4 源地址创建的地址对象。
   - 选择 **Interface Address**（接口地址），在这种情况下，已转换的源地址是防火墙出口接口的 IP 地址和子网掩码。对于该选择，请选择一个 **Interface**（接口），如果接口有一个以上 IP 地址，可随意选择一个 **IP Address**（IP 地址）。
3. 取消选择 **Destination Address Translation**（目标地址转换）。（防火墙根据 NAT64 规则中原始目标所指定的前缀长度，从传入数据包的 IPv6 前缀中提取 IPv4 地址。）
4. 单击 **OK**（确定）以保存 NAT64 策略规则。

STEP 8 | 配置隧道接口，以模拟具有除 128 以外的子网掩码的回环接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道）并 **Add**（添加）隧道。
2. 对于 **Interface Name**（接口名称），输入数字后缀，例如 .2。
3. 在 **Config**（配置）选项卡上，选择正在配置 NAT64 的 **Virtual Router**（虚拟路由器）。
4. 对于 **Security Zone**（安全区域），选择与 IPv4 服务器目标（信任区域）相关联的目标区域。
5. 在 **IPv6** 选项卡上，选择 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。
6. 单击 **Add**（添加），然后对于 **Address**（地址），选择 **New Address**（新建地址）。
7. 输入地址的 **Name**（名称）。
8. （可选）输入隧道地址的 **Description**（说明）。
9. 对于 **Type**（类型），选择 **IP Netmask**（IP 子网掩码）并输入 IPv6 前缀和前缀长度，在本例中为 64:FF9B::/96。
10. 单击 **OK**（确定）。
11. 选择 **Enable address on interface**（在接口上启用地址），然后单击 **OK**（确定）。
12. 单击 **OK**（确定）。
13. 单击 **OK**（确定）以保存隧道。

STEP 9 | 创建一个安全策略，允许来自信任区域的 NAT 流量。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）规则 **Name**（名称）。
2. 选择 **Source**（源）并 **Add**（添加）**Source Zone**（源区域）；选择 **trust**（信任）。
3. 对于 **Source Address**（源地址），选择 **Any**（任何）。
4. 选择 **Destination**（目标）并 **Add**（添加）**Destination Zone**（目标区域），选择 **Untrust**（不信任）。
5. 对于 **Application**（应用程序），选择 **Any**（任何）。
6. 对于 **Actions**（操作），选择 **Allow**（允许）。
7. 单击 **OK**（确定）。

STEP 10 | 提交更改。

单击 **Commit**（提交）。

STEP 11 | 排除 NAT64 会话故障或查看 NAT64 会话。



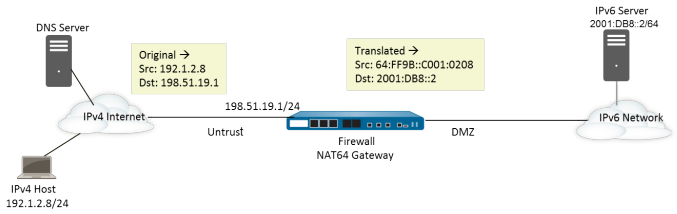
© 2019 Palo Alto Networks, Inc.

```
> show session id <session-id>
```

# 为 IPv4 启动的通信配置 NAT64

IPv6 服务器的 IPv4 启动的通信类似于 IPv4 拓扑中的目标 NAT。目标 IPv4 地址通过一对一的静态 IP 转换（而不是多对一的转换）映射到目标 IPv6 地址。

防火墙将源 IPv4 地址编码为众所周知的前缀 64:FF9B::/96，如 RFC 6052 中所述。转换的目标地址是实际 IPv6 地址。IPv4 启动的通信的常见用例发生在组织向组织 DMZ 区域中的 IPv6 服务器提供从公共不信任区域的访问时。此拓扑不使用 DNS64 服务器。




STEP 1 | 启用 IPv6 以在防火墙上运行。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 选择 **Enable IPv6 Firewalling**（启用 **IPv6** 防火墙）。
3. 单击 **OK**（确定）。

STEP 2 | （可选）当 IPv4 数据包的 DF 位设置为零（并且因为 IPv6 数据包不分片）时，请确保转换的 IPv6 数据包不超过目标 IPv6 网络的路径 MTU。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 对于 **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小网络 **MTU**），输入防火墙将 IPv4 数据包分片转换为 IPv6 的最小字节数（范围为 1280-9216，默认值为 1280）。

   如果您不希望防火墙在转换之前对 *IPv4* 数据包进行分片，请将 *MTU* 设置为 *9216*。如果转换后的 *IPv6* 数据包仍然超过该值，则防火墙丢弃该数据包，发出 *ICMP* 数据包，表明目标无法访问，需进行分片。
3. 单击 **OK**（确定）。

STEP 3 | 为 IPv4 目标地址创建一个地址对象（预转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64_ip4server。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并在不信任区域中输入防火墙接口的 IPv4 地址。此地址不得包含子网掩码，或只能包含子网掩码 /32。本例使用 198.51.19.1/32。
4. 单击 **OK**（确定）。

STEP 4 | 为 IPv6 源地址创建一个地址对象（已转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64_ip6source。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并输入与 RFC 6052（/32、/40、/48、/56、/64 或 /96）兼容的子网掩码的 NAT64 IPv6 地址。

   对于本示例，请输入 64:FF9B::/96。

   （防火墙使用十六进制为 C001:0208 的 IPv4 源地址 192.1.2.8 编码前缀）。
4. 单击 **OK**（确定）。


© 2019 Palo Alto Networks, Inc.

STEP 5 | 为 IPv6 目标地址创建一个地址对象（已转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64_server_2。
3. 对于 **Type**（类型），选择 **IP Netmask**（IP 子网掩码）并输入 IPv6 服务器（目标）的 IPv6 地址。此地址不得包含子网掩码，或只能包含子网掩码 /128。本例使用 2001:DB8::2/128。
4. 单击 **OK**（确定）。

STEP 6 | 创建 NAT64 规则。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入 NAT64 规则的 **Name**（名称），例如 nat64_ipv4_init。
3. 对于 **NAT Type**（NAT 类型），请选择 **nat64**。

STEP 7 | 指定原始的源信息和目标信息。

1. 对于 **Original Packet**（原始数据包），**Add**（添加）**Source Zone**（源区域），这可能是一个不信任区域。
2. 选择 **Destination Zone**（目标区域），这可能是一个信任区域或 DMZ 区域。
3. 对于 **Source Address**（源地址），选择 **Any**（任何）或 **Add**（添加）IPv4 主机的地址对象。
4. 对于 **Destination Address**（目标地址），**Add**（添加）IPv4 目标的地址对象，在本示例中为 nat64_ip4server。
5. 对于 **Service**（服务），请选择 **any**（任何）。

STEP 8 | 指定已转换的数据包信息。

1. 对于 **Translated Packet**（已转换数据包），在 **Source Address Translation**（源地址转换）的 **Translation Type**（转换类型）中，选择 **Static Ip**（静态 **IP**）。
2. 对于 **Translated Address**（已转换地址），选择您创建的源转换地址对象 nat64_ip6source。
3. 对于 **Destination Address Translation**（目标地址转换），对于 **Translated Address**（已转换地址），请指定单个 IPv6 地址（本例中为地址对象 nat64_server_2 或服务器的 IPv6 地址）。
4. 单击 **OK**（确定）。

STEP 9 | 创建一个安全策略，允许来自不信任区域的 NAT 流量。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）规则 **Name**（名称）。
2. 选择 **Source**（源）并 **Add**（添加）**Source Zone**（源区域）；选择 **Untrust**（不信任）。
3. 对于 **Source Address**（源地址），选择 **Any**（任何）。
4. 选择 **Destination**（目标）并 **Add**（添加）**Destination Zone**（目标区域），选择 **DMZ**。
5. 对于 **Actions**（操作），选择 **Allow**（允许）。
6. 单击 **OK**（确定）。

STEP 10 | 提交更改。

单击 **Commit**（提交）。

STEP 11 | 排除 NAT64 会话故障或查看 NAT64 会话。

```
> show session id <session-id>
```

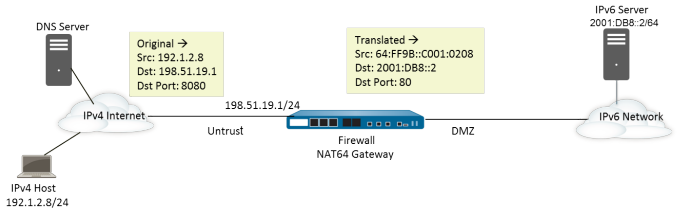
# 通过端口转换为 IPv4 启动的通信配置 NAT64

该任务建立在为 IPv4 启动的通信配置 NAT64分配的任务的基础之上，但是，控制 IPv6 网络的组织更愿意将公共目标端口号转换为内部目标端口号，从而使其不被防火墙 IPv4 不信任侧的用户看到。在此示例中，



© 2019 Palo Alto Networks, Inc.

端口 8080 转换为端口 80。为此，在 NAT64 策略规则的原始数据包中，创建一个指定目标端口为 8080 的新服务。对于已转换数据包，转换端口为 80。




STEP 1 | 启用 IPv6 以在防火墙上运行。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 选择 **Enable IPv6 Firewalling**（启用 **IPv6** 防火墙）。
3. 单击 **OK**（确定）。

STEP 2 | （可选）当 IPv4 数据包的 DF 位设置为零（并且因为 IPv6 数据包不分片）时，请确保转换的 IPv6 数据包不超过目标 IPv6 网络的路径 MTU。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 对于 **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小网络 **MTU**），输入防火墙将 IPv4 数据包分片转换为 IPv6 的最小字节数（范围为 1280-9216，默认值为 1280）。

   如果您不希望防火墙在转换之前对 *IPv4* 数据包进行分片，请将 *MTU* 设置为 *9216*。如果转换后的 *IPv6* 数据包仍然超过该值，则防火墙丢弃该数据包，发出 *ICMP* 数据包，表明目标无法访问，需进行分片。
3. 单击 **OK**（确定）。

STEP 3 | 为 IPv4 目标地址创建一个地址对象（预转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64_ip4server。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并在不信任区域中输入防火墙接口的 IPv4 地址和子网掩码。本例使用 198.51.19.1/24。
4. 单击 **OK**（确定）。

STEP 4 | 为 IPv6 源地址创建一个地址对象（已转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64_ip6source。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码），并输入与 RFC 6052（/32、/40、/48、/56、/64 或 /96）兼容的子网掩码的 NAT64 IPv6 地址。

   对于本示例，请输入 64:FF9B::/96。

   （防火墙使用十六进制为 C001:0208 的 IPv4 源地址 192.1.2.8 编码前缀）。
4. 单击 **OK**（确定）。

STEP 5 | 为 IPv6 目标地址创建一个地址对象（已转换）。

1. 选择 **Objects**（对象）> **Addresses**（地址），然后单击 **Add**（添加）。
2. 输入对象的 **Name**（名称），例如 nat64_server_2。
3. 对于 **Type**（类型），选择 **IP Netmask**（**IP** 子网掩码）并输入 IPv6 服务器（目标）的 IPv6 地址。本例使用 2001:DB8::2/64。

   源和目标必须具有相同的子网掩码（前缀长度）。


© 2019 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。

STEP 6 | 创建 NAT64 规则。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡上，输入 NAT64 规则的 **Name**（名称），例如 nat64_ipv4_init。
3. 对于 **NAT Type**（NAT 类型），请选择 **nat64**。

STEP 7 | 指定原始的源信息和目标信息，并创建一个服务以将转换限制为单个入口端口号。

1. 对于 **Original Packet**（原始数据包），**Add**（添加）**Source Zone**（源区域），这可能是一个不信任区域。
2. 选择 **Destination Zone**（目标区域），这可能是一个信任区域或 DMZ 区域。
3. 对于 **Service**（服务），选择新建 **Service**（服务）。
4. 输入服务 **Name**（名称），例如 Port_8080。
5. 选择 **TCP** 作为 **Protocol**（协议）。
6. 对于 **Destination Port**（目标端口），请输入 8080。
7. 单击 **OK**（确定）以保存服务。
8. 对于 **Source Address**（源地址），选择 **Any**（任何）或 **Add**（添加）IPv4 主机的地址对象。
9. 对于 **Destination Address**（目标地址），**Add**（添加）IPv4 目标的地址对象，在本示例中为 nat64_ip4server。

STEP 8 | 指定已转换的数据包信息。

1. 对于 **Translated Packet**（已转换数据包），在 **Source Address Translation**（源地址转换）的 **Translation Type**（转换类型）中，选择 **Static Ip**（静态 **IP**）。
2. 对于 **Translated Address**（已转换地址），选择您创建的源转换地址对象 nat64_ip6source。
3. 对于 **Destination Address Translation**（目标地址转换），对于 **Translated Address**（已转换地址），请指定单个 IPv6 地址（本例中为地址对象 nat64_server_2 或服务器的 IPv6 地址）。
4. 指定防火墙转换公共目标端口号的私有目标 **Translated Port**（已转换端口）号，在本示例中为 80。
5. 单击 **OK**（确定）。

STEP 9 | 创建一个安全策略，允许来自不信任区域的 NAT 流量。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）规则 **Name**（名称）。
2. 选择 **Source**（源）并 **Add**（添加）**Source Zone**（源区域）；选择 **Untrust**（不信任）。
3. 对于 **Source Address**（源地址），选择 **Any**（任何）。
4. 选择 **Destination**（目标）并 **Add**（添加）**Destination Zone**（目标区域），选择 **DMZ**。
5. 对于 **Actions**（操作），选择 **Allow**（允许）。
6. 单击 **OK**（确定）。

STEP 10 | 提交更改。

单击 **Commit**（提交）。

STEP 11 | 排除 NAT64 会话故障或查看 NAT64 会话。

```
> show session id <session-id>
```



© 2019 Palo Alto Networks, Inc.

# ECMP

等成本多路径 (ECMP) 处理是一个网络功能，它能让防火墙最多使用至同一目标的四条等成本路由。不使用此功能时，如果至同一目标存在多条等成本路由，那么虚拟路由器会从路由表中选择其中的一条路由，并将该路由添加到其转发表中；它不会使用任何其他路由，除非所选路由中断。

在虚拟路由器上启用 ECMP 功能后，对于一个目标，防火墙在其转发表中最多能有四条等成本路径，这使得防火墙能够：

- 通过多个等成本链路将平衡流（会话）加载到同一目标。
- 充分利用链路上至同一目标的可用带宽，不会让某些链路处于未使用状态。
- 如果某个链路出现故障，流量会动态转移到至同一目标的另一个 ECMP 成员上，而不必等待路由协议或 RIB 表选定替代路径/路由。这有助于缩短链路出现故障时的中断时间。

有关 HA 对等设备出现故障时如何选择 ECMP 路径的相关信息，请参阅处于主动/主动 HA 模式的 ECMP。

以下各节介绍 ECMP 以及如何对其进行配置：

- ECMP 负载均衡算法
- ECMP 型号、接口和 IP 路由支持
- 在虚拟路由器上配置 ECMP
- 为多个 BGP 自治系统启用 ECMP
- 验证 ECMP

## ECMP 负载均衡算法

让我们假设防火墙的路由信息库 (RIB) 有多个指向单个目标的等成本路径。等成本路径的最大数量默认为 2。ECMP 会从 RIB 中选择两个最好的等成本路径复制到转发信息库 (FIB)。然后，ECMP 会根据均衡负载方法来确定会话期间防火墙会对目标使用 FIB 中两个路径中的哪一个路径。

ECMP 负载均衡在会话层完成，而不是在数据包层完成 — 新会话在防火墙 (ECMP) 选择等成本路径时开始。单个目标的等成本路径被视为 ECMP 路径成员或 ECMP 组成员。ECMP 将根据您设置的均衡负载算法，来确定将为 ECMP 流使用 FIB 中多个目标路径中的哪一个路径。一个虚拟路由器只能使用一个负载均衡算法。



启用、禁用或更改现有虚拟路由器上的 *ECMP* 可使系统重启虚拟路由器，进而导致现有会话终止。

这四种算法选项分别着重于不同的优先级，具体如下所示：

- 基于哈希的算法优先处理会话粘连—**IP Modulo**（**IP** 模）和 **IP Hash**（**IP** 哈希）算法根据数据包标头中的信息（如源和目标地址）使用算法。因为给定会话内各个流的标头包含相同的源和目标信息，这些选项将优先处理会话粘连。如果选择 **IP Hash**（**IP** 哈希）算法，哈希可以基于源地址和目标地址，或者哈希可以仅基于源地址（在 PAN-OS 8.0.3 及更高版本中）。仅基于源地址使用 IP 哈希会使属于相同源 IP 地址的所有会话始终从可用的多个路径中获得相同的路径。因此，该路径更具粘性，需要时更容易进行故障排除。如果您有大量会话指向同一目标，且这些会话不能通过 ECMP 链接平均分布时，您可以选择设置 **Hash Seed**（哈希种子）值来进一步实现负载均衡的随机化。
- 均衡算法优先处理负载均衡—**Balanced Round**（均衡循环调度）算法可在链接之间等量地分布传入会话，负载均衡的优先级高于会话粘连。（循环调度指示选择最近选择最少的项的顺序。）此外，如果从 ECMP 组中添加或移除新路由（例如，如果组中的路径关闭），虚拟路由器将重新均衡组内链接间的会话。另外，如果会话中的流由于中断而必须切换路由，那么当与此会话关联的路由再次可用后，虚拟路由器再次重新均衡负载时，会话中的流将恢复为原始路由。
- 加权算法优先处理链接容量和/或速度 — 作为 ECMP 协议标准的扩展，Palo Alto Networks 实施提供了 **Weighted Round Robin**（加权循环调度）负载均衡选项，此选项会考虑防火墙传出接口上的不同链接容量和速度。使用此选项，您可以使用链接容量、速度和延迟等因素根据链接性能为接口分配 **ECMP**


© 2019 Palo Alto Networks, Inc.

**Weights**（**ECMP** 权重）（范围为 1-255，默认为 100），以确保负载均衡，进而保证充分利用可用链接。

例如，假设防火墙有指向 ISP: ethernet1/1 (100 Mbps) 和 ethernet1/8 (200 Mbps) 的冗余链接。尽管这些是等成本路径，但通过 ethernet1/8 的链接能提供更好的带宽，因此可以比 ethernet1/1 链接承受更多的负载。因此，为了确保负载均衡功能可以顾及链接容量和速度，您可以为 ethernet1/8 分配权重 200，为 ethernet1/1 分配权重 100。权重比率为 2:1 时，会使虚拟路由器向 ethernet1/8 发送两倍于 ethernet1/1 的会话数量。但是，因为 ECMP 协议本身基于会话，所以当使用 **Weighted Round Robin**（加权循环调度）算法时，防火墙只能尽最大努力均衡 ECMP 链接间的负载。

请记住，为接口分配 ECMP 权重是为了确定负载均衡（影响要选择哪个等成本路径），而不是为了选择路由（从可以具有不同成本的路由中选择路由）。

为较低的权重分配较低的速度和容量。为较高的权重分配较高的速度和容量。通过这种方式，防火墙可以根据这些比率分布会话，而不是覆盖等成本路径之一的低容量链接。

## ECMP 型号、接口和 IP 路由支持

所有 Palo Alto Networks 防火墙型号都支持 ECMP，PA-7000 系列、PA-5200 系列和 PA-3200 系列都支持硬件转发。VM 系列防火墙仅通过软件支持 ECMP。性能受不能卸载硬件的会话的影响。

第 3 层、第 3 层子接口、VLAN、隧道和聚合以太网接口上支持 ECMP。

可以为静态路由和防火墙支持的任何动态路由协议配置 ECMP。

因为容量基于路径数量，ECMP 会影响路由表容量，因此带有四个路径的 ECMP 路由会使用四条路由表容量。ECMP 实施可能会略微降低路由表容量，因为基于会话的标记要使用更多内存将通信流映射到特定接口。

使用静态路由的虚拟路由器到虚拟路由器路由不支持 ECMP。

## 在虚拟路由器上配置 ECMP

使用以下过程可在虚拟路由器上启用 ECMP。先决条件如下：

- 指定属于虚拟路由器的接口（**Network**（网络）> **Virtual Routers**（虚拟路由器）> **Router Settings**（路由器设置）> **General**（常规））。
- 指定 IP 路由协议。

启用、禁用或更改现有虚拟路由器的 ECMP 会导致系统重新启动虚拟路由器，这可能会导致会话终止。

STEP 1 | 为虚拟路由器启用 ECMP。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择要在其上启用 ECMP 的虚拟路由器。
2. 选择 **Router Settings**（路由器设置）> **ECMP**，然后选择 **Enable**（启用）。

STEP 2 | （可选）启用服务器到客户端之间的数据包对称返回。

选择 **Symmetric Return**（对称返回）可使返回数据包从关联入口数据包抵达时所通过的同一接口离开。也就是说，防火墙将使用接收接口来发送返回数据包，而不是使用 ECMP 接口。**Symmetric Return**（对称返回）设置将覆盖负载均衡。该行为仅适用于从服务器到客户端的通信流。

STEP 3 | 启用 **Strict Source Path**（严格源路径），确保源自防火墙的 IKE 和 IPSec 流量从 IPSec 隧道源 IP 地址所属的物理接口传出。

启用 ECMP 后，源自防火墙的 IKE 和 IPSec 流量默认从 ECMP 负载均衡法确定的接口传出。或者，您可以通过启用严格源路径，使源自防火墙的 IKE 和 IPSec 流量始终从 IPSec 隧道源 IP 地址所属的物理接口传出。只要防火墙有多个 ISP 向同一目标提供等价路径，就可以启用此功能。ISP 通常会执行反向路径转



© 2019 Palo Alto Networks, Inc.

发 (RPF) 检查（或者不同的检查以防止 IP 地址欺骗），以确保流量的传入和传出接口一致。由于 ECMP 会根据所配置的 ECMP 方法选择传出接口（而不是选择源接口充当传出接口），而这不符合 ISP 的期望，因此，ISP 可能会阻止合法的回传流量。在这种情况下，请启用严格源路径，这样，防火墙就能使用 IPSec 隧道源 IP 地址所属的接口作为传出接口，且 ISP 允许回传流量。

STEP 4 | 指定可以从路由信息库 (RIB) 复制到转发信息库 (FIB) 的等成本路径（到目标网络）的最大数量。

对于允许的 **Max Path**（最大路径数），请输入 **2**、**3** 或 **4**。默认：2.

STEP 5 | 为虚拟路由器选择负载均衡算法。有关负载均衡方法及其区别的详细信息，请参阅 ECMP 负载均衡算法。

对于 **Load Balance**（负载均衡），请从 **Method**（方法）列表中选择下列选项之一：

- **IP Modulo**（**IP** 模）（默认）— 使用数据包标头中的源和目标 IP 地址的哈希来确定要使用的 ECMP 路由。
- **IP Hash**（**IP** 哈希）— 有两种 IP 哈希方法可以确定要使用的 ECMP 路由（在步骤 5 中选择哈希选项）：
  - 使用源地址的哈希（在 PAN-OS 8.0.3 及更高版本中可用）。
  - 使用源和目标 IP 地址的哈希（默认 IP 哈希方法）。
- **Balanced Round Robin**（平衡循环调度）— 在 ECMP 路径之间使用循环调度并在路径数量发生更改时重新均衡路径。
- **Weighted Round Robin**（加权循环调度）— 使用循环调度和相关权重从 ECMP 路径间进行选择。在下方的步骤 6 中指定权重。

STEP 6 | （仅 IP 哈希）配置 IP 哈希选项。

如果您选择 **IP Hash**（**IP** 散列）作为 **Method**（方法）：

1. 如果要确保属于同一源 IP 地址的所有会话始终与可用的多个路径保持相同的路径，请选择 **Use Source Address Only**（仅使用源地址）（仅在 PAN-OS 8.0.3 及更高版本中可用）。此 IP 哈希选项提供路径粘连并简化故障排除。如果您不选择此选项，或者您使用 PAN-OS 8.0.3 之前的版本，则 IP 哈希将基于源和目标 IP 地址（默认 IP 哈希方法）。

   如果选择 *Use Source Address Only*（仅使用源地址），则不应将配置从 *Panorama* 推送到运行 *PAN-OS 8.0.2*、*8.0.1* 或 *8.0.0* 的防火墙。
2. 如果要在 **IP Hash**（**IP** 哈希）计算中使用源和目标端口数，请选择 **Use Source/Destination Ports**（使用源/目标端口）。

   启用 *Use Source Address Only*（仅使用源地址）这一选项，即使对于属于相同源 *IP* 地址的会话，也会随机选择路径。
3. 输入一个 **Hash Seed**（哈希种子）值（最大九位数的整数）。指定 **Hash Seed**（哈希种子）值以进一步实现负载均衡。如果您有大量带有相同元组信息的会话，那么指定哈希种子将非常有用。

STEP 7 | （仅限加权循环调度）为 ECMP 组中的各个接口定义权重。

如果您选择 **Weighted Round Robin**（加权循环调度）作为 **Method**（方法），请为各个接口（要路由到相同目标的流量的传出点，即属于 ECMP 组的接口，如为您的 ISP 提供冗余链接的接口或公司网络上指向核心业务应用程序的接口）定义权重。

权重越高，该等成本路径将越常被选中用于新会话。

应为快速链路指定高于慢速链路的权重，以使更多的 *ECMP* 通信使用快速链路。


© 2019 Palo Alto Networks, Inc.

1. 通过单击 **Add**（添加），然后选择 **Interface**（接口）来创建 ECMP 组。
2. 在 ECMP 组中 **Add**（添加）其他接口。
3. 单击 **Weight**（权重）并为各个接口指定相关权重（范围为 1-255，默认为 100）。

STEP 8 | 保存配置。

1. 单击 **OK**（确定）。
2. 在 ECMP Configuration Change（ECMP 配置更改）提示框中，单击 **Yes**（是）重启虚拟路由器。重新启动虚拟路由器可能会导致现有会话终止。

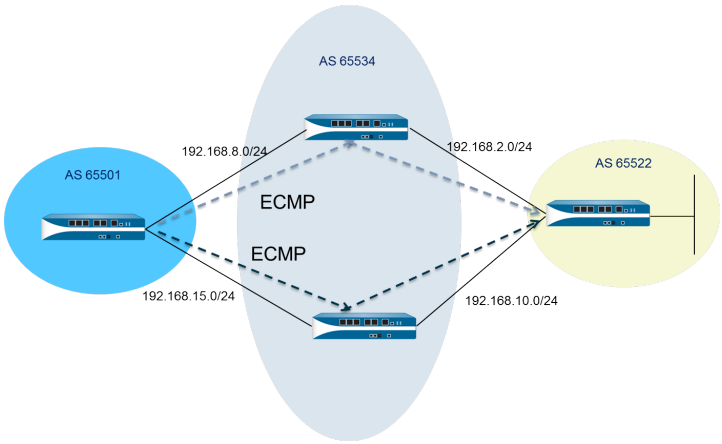
只有在修改带有 *ECMP* 的现有虚拟路由器时才会显示此消息。

STEP 9 | 提交更改。

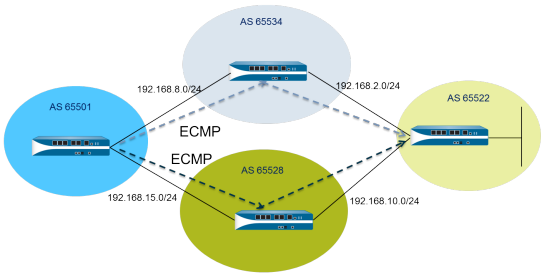
**Commit**（提交）配置。

# 为多个 BGP 自治系统启用 ECMP

如果您已配置 BGP，并希望在多个自治系统上启用 ECMP，请执行以下任务。此任务假定已配置 BGP。在下图中，目标的两个 ECMP 路径经过属于单个 BGP 自治系统内单个 ISP 的两个防火墙。




在下图中，目标的两个 ECMP 路径经过属于不同 BGP 自治系统内的两个不同 ISP 的两个防火墙。




STEP 1 | 配置 ECMP。

请参阅在虚拟路由器上配置 ECMP。

STEP 2 | 对于 BGP 路由，请在多个自治系统间启用 ECMP。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择要在其上为多个 BGP 自治系统启用 ECMP 的虚拟路由器。
2. 选择 **BGP** > **Advanced**（高级），并选择 **ECMP Multiple AS Support**（**ECMP** 多个 **AS** 支持）。

STEP 3 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

## 验证 ECMP

为 ECMP 配置的虚拟路由器指示转发信息库 (FIB) 表中哪些路由是 ECMP 路由。路由的 ECMP 标志 (E) 指示该路由组成传出接口到该路由的下一个跃点的 ECMP。要验证 ECMP，请使用以下步骤查看 FIB 并确认某些路由为等成本多路径。

STEP 1 | 选择**Network**（网络）> **Virtual Routers**（虚拟路由器）。

STEP 2 | 在启用 ECMP 的虚拟路由器的行中，单击 **More Runtime Stats**（详细运行时统计信息）。

STEP 3 | 选择 **Routing**（路由）> **Forwarding Table**（转发表）以查看 FIB。



在此表中，请注意同一目标的多个路由（指向不同接口）带有“*E*”标志。星号 *(*)* 表示是 *ECMP* 组的首选路径。


© 2019 Palo Alto Networks, Inc.

# LLDP

Palo Alto Networks 防火墙支持链路层发现协议 (LLDP)，此协议在链路层的功能是发现邻居设备及其功能。LLDP 允许防火墙和其他网络设备收发邻居的 LLDP 数据单元。接收设备会将信息存储在 MIB 中，这些信息可通过简单网络管理协议 (SNMP) 来访问。LLDP 简化了故障排除工作，尤其是对 virtual wire 部署，在此部署中，ping 或 traceroute 通常检测不到网络拓扑中的防火墙。


- LLDP 概述
- LLDP 内支持的 TLV
- LLDP Syslog 消息和 SNMP 陷阱
- 配置 LLDP
- 查看 LLDP 设置和状态
- 清除 LLDP 统计信息


## LLDP 概述

LLDP 在使用 MAC 地址的 OSI 模型的第 2 层运作。LLDPDU 是封装在以太帧中的类型长度值 (TLV) 元素的顺序。IEEE 802.1AB 标准为 LLDPDU 定义了三个 MAC 地址：01-80-C2-00-00-0E、01-80-C2-00-00-03 和 01-80-C2-00-00-00。

Palo Alto Networks 防火墙只支持传输一个 MAC 地址和接收 LLDP 数据单元：01-80-C2-00-00-0E。在传输时，防火墙使用 01-80-C2-00-00-0E 作为目标 MAC 地址。在接收时，防火墙处理使用 01-80-C2-00-00-0E 作为目标 MAC 地址的数据报。如果防火墙在其接口上接收 LLDPDU 的其他两个 MAC 地址中的任何一个，防火墙会执行此功能之前所执行的同一转发操作，具体如下所示：

- 如果接口类型为 vwire，防火墙会将数据报转发到其他端口。
- 如果接口类型为 L2，防火墙会在 VLAN 的剩余部分中填满数据报。
- 如果接口类型为 L3，防火墙会丢弃数据报。

不支持 Panorama 和 WildFire 设备。

不支持 LLDP 的接口类型有 TAP、高可用性 (HA)、解密镜像、virtual wire/vlan/L3 子接口和 PA-7000 系列日志处理卡 (LPC) 接口。

LLDP 以太帧具有以下格式：

| Preamble | Destination MAC | Source MAC | Ethertype | Chassis ID TLV | Port ID TLV | Time To Live TLV | Optional TLVs | End of LLDPDU TLV | Frame Check Sequence |
|---|---|---|---|---|---|---|---|---|---|
| | 01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00 | Station's Address | 0x88CC | Type=1 | Type=2 | Type=3 | Zero or more complete TLVs | Type=0, Length=0 | |

在 LLDP 以太帧中，TLV 结构具有以下格式：

| TLV Type | TLV Information String Length | TLV Information String |
|---|---|---|
| 7 bits | 9 bits | 0-511 octets |



© 2019 Palo Alto Networks, Inc.

# LLDP 内支持的 TLV

LLDPDU 包括强制和可选 TLV。下表列出了防火墙支持的必需 TLV：

| 必需 TLV | TLV 类型 | 说明 |
|---|---|---|
| 机箱 ID TLV | 1 | 标识防火墙机箱。每个防火墙只能有一个唯一机箱 ID。Palo Alto Networks 型号上的机箱 ID 子类型为 4（MAC 地址）时，将使用 MAC 地址 Eth0 来确保唯一性。 |
| 端口 ID TLV | 2 | 标识发送此 LLDPDU 的端口。每个防火墙为每个传输的 LLDPDU 消息使用一个端口 ID。端口 ID 子类型为 5（接口名称），可唯一地标识传输端口。防火墙使用接口的 ifname 作为端口 ID。 |
| 生存时间 (TTL) TLV | 3 | 指定接收自对等设备的 LLDPDU 信息在本地防火墙内保留有效的时长（以秒计，范围为 0-65,535）。该值是 LLDP 保持时间乘数的倍数。当 TTL 值为 0 时，与此设备关联的信息将不再有效，且防火墙将从 MIB 中移除此条目。 |
| LLDPDU TLV 结尾 | 0 | 指示 LLDP 以太帧中 TLV 的结尾。 |

下表列出了 Palo Alto Networks 防火墙支持的可选 TLV：

| 可选 TLV | TLV 类型 | 有关防火墙实施的用途和说明 |
|---|---|---|
| 端口说明 TLV | 4 | 介绍字母数字格式的防火墙的端口。将使用 ifAlias 对象。 |
| 系统名称 TLV | 5 | 配置字母数字格式的防火墙的名称。将使用 sysName 对象。 |
| 系统说明 TLV | 6 | 介绍字母数字格式的防火墙。将使用 sysDescr 对象。 |
| 系统功能 | 7 | 介绍接口的部署模式，具体如下所示：<br>• L3 接口通过路由器（位 6）功能和另一个位（位 1）通告。<br>• L2 接口通过 MAC 网桥（位 3）功能和另一个位（位 1）通告。<br>• virtual wire 接口通过中继器（位 2）功能和另一个位（位 1）通告。 |
| 管理地址 | 8 | 一个或多个 IP 地址用于防火墙管理，如下所示：<br>• 管理 (MGT) 接口的 IP 地址<br>• 接口的 IPv4 和/或 IPv6 地址<br>• 回环地址<br>• 在管理地址字段中输入的用户定义的地址<br>如果未提供管理 IP 地址，会默认使用传输接口的 MAC 地址。<br>其中包括所指定管理地址的接口号。另外还包括指定了管理地址的硬件接口的 OID（如果适用）。<br>如果指定了多个管理地址，将按照指定顺序从列表顶部开始发送这些地址。最多支持四个管理地址。<br>此为可选参数，可以保持禁用状态。 |


© 2019 Palo Alto Networks, Inc.

## LLDP Syslog 消息和 SNMP 陷阱

防火墙会将 LLDP 信息存储在 MIB 中，SNMP 管理器可以对此 MIB 进行监控。如果您想让防火墙发送有关 LLDP 事件的 SNMP 陷阱通知和 syslog 消息，必须在 LLDP 配置文件中启用 **SNMP Syslog Notification**（**SNMP Syslog** 通知）。

根据 RFC 5424 Syslog 协议和 RFC 1157 简单网络管理协议，LLDP 会在 MIB 发生更改时发送 syslog 和 SNMP 陷阱消息。这些消息受 **Notification Interval**（通知间隔）的频率限制，此间隔为 LLDP 全局设置，默认为 5 秒，可以自行配置。

因为 LLDP syslog 和 SNMP 陷阱消息受比率限制，因此提供给这些过程的某些 LLDP 信息可能与您在查看 LLDP 状态信息时看到的当前 LLDP 统计信息不匹配。这是正常的预期行为。

每个接口（以太网或 AE）最多可以接收 5 个 MIB。每个不同的源有一个 MIB。如果超过此限制，会触发错误消息 `tooManyNeighbors`。

## 配置 LLDP

要配置 LLDP 并创建 LLDP 配置文件，您必须是超级用户或设备管理员 (deviceadmin)。防火墙接口最多支持五个 LLDP 对等设备。

STEP 1 | 在防火墙上启用 LLDP 通信。

选择 **Network**（网络）> **LLDP**，并编辑 LLDP General（LLDP 常规）部分，选择 **Enable**（启用）。

STEP 2 | （可选）更改 LLDP 全局设置。

1. 对于 **Transmit Interval (sec)**（传输间隔（秒）），请指定 LLDPDU 的传输间隔（以秒计）。默认：30 秒。范围：1-3600 秒。
2. 对于 **Transmit Delay (sec)**（传输延迟（秒）），请指定在 TLV 元素更改和 LLDP 传输发送之间相隔的延迟时间（以秒计）。如果大量的网络更改导致 LLDP 更改数量猛增，或是接口出现翻动，则延迟有助于防止段中的 LLDPDU 泛滥。**Transmit Delay**（传输延迟）必须小于 **Transmit Interval**（传输间隔）。默认：2 秒。范围：1-600 秒。
3. 对于 **Hold Time Multiple**（保持时间倍数），请指定一个值，该值乘以 **Transmit Interval**（传输间隔）即可确定 TTL 保持总时间。默认：4。范围：1-100。无论乘数值是多少，最大的 TTL 保持时间都为 65535 秒。
4. 对于 **Notification Interval**（通知间隔），请指定 MIB 发生更改时 LLDP Syslog 消息和 SNMP 陷阱的传输间隔（以秒计）。默认：5 秒。范围：1-3600 秒。
5. 单击 **OK**（确定）。

STEP 3 | 创建 LLDP 配置文件。

有关可选 TLV 的说明，请参阅 LLDP 内支持的 TLV。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **LLDP Profile**（**LLDP** 配置文件）并 **Add**（添加）LLDP 配置文件的 **Name**（名称）。
2. 对于 **Mode**（模式），请选择 **transmit-receive**（传输接收）（默认）、**transmit-only**（仅传输）或 **receive-only**（仅接收）。
3. 选择 **SNMP Syslog Notification**（**SNMP Syslog** 通知）启用 SNMP 通知和 Syslog 消息。如果启用，将使用全局 **Notification Interval**（通知间隔）。防火墙将按照 **Device**（设备）> **Log Settings**（日志设置）> **System**（系统）> **SNMP Trap Profile**（**SNMP** 陷阱配置文件）和 **Syslog Profile**（**Syslog** 配置文件）中的配置来发送 SNMP 陷阱和 syslog 事件。
4. 对于可选 TLV，请选择您要传输的 TLV：
   - 端口说明
   - 系统名称
   - 系统说明



© 2019 Palo Alto Networks, Inc.

- 系统功能

5. （可选）选择 **Management Address**（管理地址）添加一个或多个管理地址，并且 **Add**（添加）一个 **Name**（名称）。
6. 选择从其中获取管理地址的 **Interface**（接口）。如果启用了 **Management Address**（管理地址）TLV，那么至少需要一个管理地址。如果未配置管理 IP 地址，则系统会使用传输接口的 MAC 地址作为管理地址 TLV。
7. 选择 **IPv4** 或 **IPv6**，然后在相邻字段内从列表（其中列出了所选接口上配置的地址）中选择 IP 地址，或输入一个地址。
8. 单击 **OK**（确定）。
9. 最多允许四个管理地址。如果您指定多个 **Management Address**（管理地址），将按照指定顺序从列表顶部开始发送这些地址。要更改地址顺序，请选择一个地址并使用 **Move Up**（向上移）或 **Move Down**（向下移）按钮。
10. 单击 **OK**（确定）。

STEP 4 | 为接口分配一个 LLDP 配置文件。

1. 选择 **Network**（网络）> **Interfaces**（接口），然后选择要分配 LLDP 配置文件的接口。
2. 选择 **Advanced**（高级）> **LLDP**。
3. 选择 **Enable LLDP**（启用 **LLDP**）来分配一个 LLDP 配置文件至接口。
4. 对于 **Profile**（配置文件），请选择您创建的配置文件。选择 **None**（无）可启用带有基本功能的 LLDP：发送这三个必需 TLV 并启用 **transmit-receive**（传输接收）模式。

   如果您要创建新的配置文件，请单击 **LLDP Profile**（**LLDP** 配置文件），并遵循上述步骤的说明操作。
5. 单击 **OK**（确定）。

STEP 5 | 提交更改。

单击 **Commit**（提交）。

## 查看 LLDP 设置和状态

执行以下过程以查看 LLDP 设置和状态。

STEP 1 | 查看 LLDP 全局设置。

选择 **Network**（网络）> **LLDP**。

在 LLDP General（LLDP 常规）屏幕中，**Enable**（启用）指示是否已启用 LLDP。

- 如果启用了 LLDP，将显示已配置的全局设置（传输间隔、传输延迟、保持时间倍数和通知间隔）。
- 如果没有启用 LLDP，将显示全局设置的默认值。

有关这些值的说明，请参阅配置 LLDP 中的第二步。

STEP 2 | 查看 LLDP 状态信息。

1. 选择 **Status**（状态）选项卡。
2. （可选）输入筛选器以限制要显示的信息。

   接口信息：

   - **Interface**（接口）— 已分配 LLDP 配置文件的接口的名称。
   - **LLDP**— LLDP 状态：启用或禁用。
   - **Mode**（模式）— 接口的 LLDP 模式：Tx/Rx、仅 Tx 或仅 Rx。
   - **Profile**（配置文件）— 已分配给接口的配置文件的名称。

   传输信息：

   - **Total Transmitted**（传输的总数）— 已传出接口的 LLDPDU 的计数。


© 2019 Palo Alto Networks, Inc.

- **Dropped Transmit**（丢弃的传输）— 因存在错误而未传出接口的 LLDPDU 的计数。例如，当系统在构建要传输的 LLDPDU 时会出现长度错误。

已收到的信息：

- **Total Received**（接收的总数）— 接口已收到的 LLDP 帧的计数。
- **Dropped TLV**（丢弃的 **TLV**）— 在收到后被放弃的 LLDP 帧的计数。
- **Errors**（错误数）—接口已收到且包含错误的 TLV 的计数。TLV 错误的类型包括：缺少一个或多个必需的 TLV，顺序错误，包含范围以外的信息，或是存在长度错误。
- **Unrecognized**（未识别）— LLDP 本地代理不识别的接口上收到的 TLV 的计数。例如，TLV 类型位于保留的 TLV 范围内。
- **Aged Out**（过期）— 因相应 TTL 到期而从接收 MIB 中删除的项目的计数。

STEP 3 | 查看接口上看到的各个邻居的摘要 LLDP 信息。

1. 选择 **Peers**（对等设备）选项卡。
2. （可选）输入筛选器限制正在显示的信息。

本地接口 — 防火墙上检测到邻居设备的接口。

远程机箱 **ID** — 对端设备的机箱 ID。将使用 MAC 地址。

端口 **ID** — 对端的端口 ID。

名称 — 对端设备的名称。

详细信息 — 提供以下远程对端的详细信息，这些信息取决于必需和可选 TLV：

- 机箱类别：MAC 地址。
- MAC 地址：对端的 MAC 地址。
- 系统名称：对等的名称。
- 系统说明：对端的说明。
- 端口说明：对端的端口说明。
- 端口类型：接口名称。
- 端口 ID：防火墙使用接口的 ifname。
- 系统功能：系统的功能。O = 其他，P = 中继器，B = 网桥，W = 无线 LAN，R = 路由器，T = 电话
- 启用的功能：对端上已启用的功能。
- 管理地址：对端的管理地址。

# 清除 LLDP 统计信息

您可以清除特定接口的 LLDP 统计信息。

清除特定接口的 LLDP 统计信息。

1. 选择 **Network**（网络）> **LLDP** > **Status**（状态），然后在左侧列中选择要清除 LLDP 统计信息的一个或多个接口。
2. 单击屏幕底部的 **Clear LLDP Statistics**（清除 **LLDP** 统计信息）。



© 2019 Palo Alto Networks, Inc.

# BFD

防火墙支持双向转发检测 (BFD) (RFC 5880)，该协议可以识别两台路由对等设备之间的双向路径故障。BFD 检测故障极快，可实现比链路监控或频繁动态路由健康检查（如呼叫数据包或检测信号）更快的故障转移。需要高可用性和极快故障转移的关键任务数据中心和网络需要 BFD，BFD 能够快速检测故障。

- BFD 概述
- 配置 BFD
- 引用：BFD 详细信息

## BFD 概述

启用 BFD 时，BFD 建立一个会话，从一个端点（防火墙）至使用三向握手链路端点的 BFD 对等设备。控制数据包执行握手，并且协商 BFD 配置文件中所配置的参数，包括对等设备可以发送和接收控制数据包的最小间隔。IPv4 和 IPv6 的 BFD 控制数据包通过 UDP 端口 3784 传输。多跳 BFD 控制数据包通过 UDP 端口 4784 传输。通过任一端口传输 BFD 控制数据包都在 UDP 数据包封装。

建立 BFD 会话之后，BFD 的 Palo Alto Networks 执行以异步模式操作，意味着两个端点以协商的间隔为对方发送控制数据包（就像呼叫数据包）。如果对等生没有在检测时间内接收到控制数据包（协商发送间隔乘以检测时间乘数），对等设备则认为会话关闭。（防火墙不支持按需模式，在该模式下，控制数据包只有在必要的情况下发送，而不是周期性发送。）

当启用 BFD 静态路径，且防火墙和 BFD 对等设备之间的 BFD 会话失败时，防火墙从 RIB 和 FIB 表删除失败的路由，并且允许较低优先级的备用路径接管。启用路由协议的 BFD 时，BFD 会通知路由协议切换至对等备用路径。因此，防火墙和 BFD 对等设备在新的路径重新会聚。

通过 BFD 配置文件，您可以配置 BFD 设置，并且将它们应用于一个或多个路由协议或防火墙上的静态路由。如果在没有配置文件的情况下启用了 BFD，则防火墙使用其默认 BFD 配置文件（所有的默认设置）。您不能更改默认的 BFD 配置文件。

当一个接口运行多个使用不同 BFD 配置文件的协议时，BFD 使用具有最低理想最短发送间隔的配置文件。请参阅 BFD 用于静态路由协议。

主动/被动高可用性对等设备同步 BFD 配置和会话；主动/主动高可用性对等设备不会。

BFD 在 RFC 5880 中标准化。PAN-OS 并不支持所有的 RFC 5880 部件；请参阅 BFD 不支持的 RFC 部件 。

PAN-OS 还支持 RFC 5881, http://www.rfc-editor.org/rfc/rfc5881.txt。在这种情况下，BFD 跟踪使用 IPv4 或 IPv6 的两个系统之间的单一跃点，从而两个系统直接相互连接。BFD 还跟踪有 BGP 连接的对等设备上的多个跃点。PAN-OS 遵守 BFD 封装要求，如 RFC 5883，https://www.rfc-editor.org/rfc/rfc5883.txt所述。然而，PAN-OS 不支持身份验证。

- BFD 模式、接口和客户端支持
- BFD 不支持的 RFC 部件
- 用于静态路由的 BFD
- BFD 用于静态路由协议

### *BFD* 模式、接口和客户端支持

以下防火墙模式不支持 BFD：PA-800 系列、PA-220 和 VM-50 防火墙。如在产品选择工具中所列，不支持 BFD 的模式支持最大数目的 BFD 会话。

BFD 在物理 Ethernet、聚合 Ethernet (AE)、VLAN 和隧道接口（站点到站点 VPN 和 LSVPN），以及第 3 层子接口上运行。

所支持的 BFD 客户端包括：

- 静态路由（IPv4 和 IPv6）包括单一跃点


© 2019 Palo Alto Networks, Inc.

- OSPFv2 和 OSPFv3（接口类型包括广播、点对点和点对多点）
- BGP IPv4 和 IPv6（IBGP、EBGP）包括单一跃点和多个跃点
- RIP（单一跃点）

## *BFD* 不支持的 *RFC* 部件

- 按需模式
- 身份验证
- 发送或接收 Echo（回显）数据包，然而，防火墙将传递到达虚拟线路或旁接接口的 Echo（回显）数据包。（BFD 回显数据包对于源和目标都有相同的 IP 地址。）
- 轮询序列
- 拥堵控制

## 用于静态路由的 *BFD*

要在静态路由上使用 BFD，静态路由相反端上的防火墙和对等设备都必须支持 BFD 会话。只有 **Next Hop**（下一个跃点）类型是 **IP Address**（**IP** 地址）时，静态路由才可以有一个 BFD 配置文件。

如果一个接口配置为一个以上静态路由对一个对等设备（BFD 会话具有相同的源 IP 地址和相同的目标 IP 地址）单一的 BFD 会话将自动处理多个静态路由。此行为会减少 BFD 会话。如果静态路由具有不同的 BFD 配置文件，具有最小 **Desired Minimum Tx Interval**（理想最短发送间隔）的配置文件起作用。

在要为 DHCP 或 PPPoE 客户端接口上的静态路由配置 BFD 时，必须执行两次提交。为静态路由启用 BFD 时，**Next Hop**（下一跃点）类型必须为 **IP Address**（**IP** 地址）。但是在 DHCP 或 PPPoE 接口提交时，接口 IP 地址和下一个跃点 IP 地址（默认的网关）。

您必须首先启用接口的 DHCP 或 PPPoE 客户端，执行提交，并且等待 DHCP 或 PPPoE 服务器向防火墙发送客户端 IP 地址和默认网关 IP 地址。然后您可以配置静态路由（使用 DHCP 或 PPPoE 客户端作为下一跃点），启用 BFD，并且执行第二次提交。

## *BFD* 用于静态路由协议

BFD 除了可以用于静态路由，防火墙还支持 BFD 用于 BGP、OSPF 和 RIP 路由协议。

多跃点 *BFD* 的 *Palo Alto Networks* 执行遵循 RFC 5883 的封装部分，多跃点路径的双向转发检测 (BFD)，但是不支持身份验证。其中一个解决方法是在 *BGP* 的 *VPN* 隧道中配置 *BFD*。*VPN* 隧道可以提供身份验证，而无需复制 *BFD* 身份验证。

当您为 OSPFv2 或 OSPFv3 广播接口启用 BFD 时，OSPF 仅使用其指定路由器 (DR) 和备用指定路由器 (BDR) 建立 BFD 会话。在点对点接口上，OSPF 与直接邻居建立一个 BFD 会话。在点对多点接口上，OSPF 与每个对等设备建立一个 BFD 会话。

防火墙不支持 OSPF 或 OSPFv3 虚拟链路上的 BFD。

每个路由协议在一个接口上可以有一个独立的 BFD 会话。或者，两个或多个路由协议（BGP、OSPF 和 RIP）可以为一个接口共享一个通用 BFD 会话。

当您为相同接口上的多个协议启用 BFD 时，而协议的源 IP 地址和目标 IP 地址也是相同的，协议共享单一的 BFD 会话，因此可以同时减少数据平面开销 (CPU) 和接口的流量负载。如果为这些协议配置不同的 BFD 配置文件，则只使用一个 BFD 配置文件：也就是具有最低 **Desired Minimum Tx Interval**（理想最短传输间隔时间）的配置文件。如果配置文件具有相同的 **Desired Minimum Tx Interval**（理想最短传输间隔时间），第一个创建会话所使用的配置文件起作用。在这种情况下，静态路由和 OSPF 共享相同的会话，因为在提交后立即创建静态会话，而 OSPF 等待邻居运行后，静态路由的配置文件起作用。

在这些情况下，使用单一 BFD 会话的优势在于，这种行为能更加有效利用资源。防火墙可以使用保存的资源来支持不同接口上的更多资源，或者支持不同源 IP 和目标 IP 地址对的 BFD。

相同接口上的 IPv4 和 IPv6 始终创建不同的 BFD 会话，即使它们使用相同的 BFD 配置文件。



© 2019 Palo Alto Networks, Inc.

如果同时实现 *BFD* 用于 *BGP* 和 *HA* 路径监控，*Palo Alto Networks* 建议您不要执行 *BGP* 平稳重启。当 *BFD* 对等设备接口出现故障并且路径监控失败时，*BFD* 可以删除路由表中受影响的路由，并将此更改同步到被动 *HA* 防火墙，然后“平稳重启”方可生效。如果决定实施 *BFD* 用于 *BGP*、*BGP* 的平稳重启和 *HA* 路径监控，则应将 *BFD* 配置为比默认值更大的“理想最短传输时间间隔”和更大的“检测时间乘数”。

# 配置 BFD

阅读完包含防火墙型号和支持接口的 BFD 概述后，请在配置 BFD 之前执行以下操作：

- 配置一个或多个虚拟路由器。
- 如果应用 BFD 至静态路由，配置一个或多个静态路由。
- 如果应用 BFD 至路由协议，配置一个路由协议（BGP、OSPF、OSPFv3 或 RIP）。

您的 *BFD* 实施取决于多个因素，例如流量负载、网络条件、*BFD* 设置的积极性，以及数据平面的忙碌性。

STEP 1 | 创建一个 BFD 配置文件。

如果在 *BFD* 配置文件中更改设置，在该配置文件中在使用现有 *BFD* 会话，而您提交该更改，在防火墙删除 *BFD* 会话并且使用新的设置重新创建时，防火墙发送一个 *BFD* 数据包，本地状态设置为 `admin down`（管理关闭）。对等设备可能会或者不会翻动路由协议或静态路由，具体取决于对等设备的实施 RFC 5882，第 *3.2* 节。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **BFD Profile**（**BFD** 配置文件）并 **Add**（添加）BFD 配置文件的 **Name**（名称）。名称区分大小写，且必须在防火墙上具有唯一性。仅可使用字母、数字、空格、连字符和下划线。
2. 选择 BFD 运行的 **Mode**（模式）：
   - **Active**（主动）— BFD 发起控制数据包的发送（默认）。BFD 对端设备中至少有一个要为主动；两个对端设备可同时为主动。
   - **Passive**（被动）— BFD 等待对端发送控制数据包，并在必要时作出响应。

STEP 2 | 配置 BFD 间隔。

1. 输入 **Desired Minimum Tx Interval (ms)**（理想最短传输间隔时间（毫秒））。这是您希望 BFD 协议（简称为 BFD）发送 BFD 控制数据包的最短间隔时间（毫秒）；因此您与对端设备协商传输间隔。PA-7000 和 PA-5200 系列防火墙的最短时间为 50；VM 系列防火墙的最短时间为 200。最大为 2,000；默认为 1,000。

   建议将 *PA-7000* 系列防火墙上的 *Desired Minimum Tx Interval*（理想最短传输间隔时间）设置为 *100* 或更高；小于 *100* 时可能会导致 *BFD* 翻动的风险。

   如果有多个路由协议使用同一个接口上的不同 *BFD*，请为 *BFD* 配置文件配置相同的 *Desired Minimum Tx Interval*（理想最小传输间隔时间）。
2. 输入 **Required Minimum Tx Interval (ms)**（要求的最短传输间隔时间（毫秒））。这是 BFD 能够接收 BFD 控制数据包的最短间隔时间（毫秒）。PA-7000 和 PA-5200 系列防火墙的最短时间为 50；VM 系列防火墙的最短时间为 200。最大为 2,000；默认为 1,000。

   建议将 *PA-7000* 系列防火墙上的 *Required Minimum Rx Interval*（要求的最短接收间隔时间）设置为 *100* 或更高；小于 *100* 时可能会导致 *BFD* 翻动的风险。

STEP 3 | 配置 BFD 检测时间乘数。


© 2019 Palo Alto Networks, Inc.

输入 **Detection Time Multiplier**（检测时间乘数）。本地系统计算检测时间的方式如下：用从远程系统接获取的 **Detection Time Multiplier**（检测时间乘数）乘以远程系统的约定传输间隔（**Required Minimum Rx Interval**（所需最小 **Rx** 间隔时间）越大，获得 **Desired Minimum Tx Interval**（理想最小 **Tx** 间隔时间）越晚。）。如果在检测时间耗尽前，BFD 未从其对等接收到 BFD 控制数据包，则会出现故障。范围为 2 至 50，默认为 3。

例如，传输间隔 300 ms x 3（检测时间乘数）= 900 ms 检测时间。

配置 *BFD* 配置文件，要考虑防火墙是一个基于会话的设备，通常位于网络或数据中心的边缘，链路可能比专用路由器要慢。因此，与所允许的最快设置相比，防火墙很可能需要更长的时间间隔，更大的乘数。如果检测时间太短，可能会引起错误的故障检测，而实际问题只是流量拥堵。

STEP 4 | 配置 BFD 保持时间。

输入 **Hold Time (ms)**（保持时间（毫秒））。BFD 传输 BFD 控制数据包之前，链路启用后的延迟时间（毫秒）。**Hold Time**（保持时间）仅适用于 BFD Active（BFD 活动）模式。如果 BFD 在 **Hold Time**（保持时间）内收到 BFD 控制数据包，则它会忽略这些数据包。范围为 0 - 120000。默认设置为 0 表示，不会应用传输 **Hold Time**（保持时间）；BFD 将在链路建立后，即刻收发 BFD 控制数据包。

STEP 5 | （可选 — 仅适用于 BGP IPv4 实施）为 BFD 配置文件配置与跃点相关的设置。

1. 选择 **Multihop**（多跃点）通过 BGP 启用 BFD 多跃点。
2. 输入 **Minimum Rx TTL**（最短接收 **TTL**）。这是 BFD 会在支持多跃点 BFD 时在 BFD 控制数据包中接受（接收）的最小生存时间 (TTL) 值（跃点数）。（范围为 1-254；没有默认设置）。

   如果防火墙收到比配置的 **Minimum Rx TTL**（最短接收 **TTL**）更小的 TTL，它会丢弃数据包。例如，如果对等设备距离有 5 个跃点，而对等设备传输一个 TTL 为 100 的 BFD 数据包至防火墙，而如果防火墙的 **Minimum Rx TTL**（最短接收 **TTL**）设置为 96 或更高，则防火墙丢弃该数据包。

STEP 6 | 保存 BFD 配置文件。

单击 **OK**（确定）。

STEP 7 | （可选）为静态路由启用 BFD。

静态路由相反端上的防火墙和对等都必须支持 BFD 会话。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并且选择配置静态路由的虚拟路由器。
2. 选择 **Static Routes**（静态路由器）选项卡。
3. 选择 **IPv4** 或 **Ipv6** 选项卡。
4. 选择要应用 BFD 时的静态路由。
5. 选择一个 **Interface**（接口）（即使正在使用 DHCP 地址）。**Interface**（接口）设置不能为 **None**（无）。
6. 对于 **Next Hop**（下一个跃点），选择 **IP Address**（**IP** 地址）并输入 IP 地址（如果未指定）。
7. 对于 **BFD Profile**（**BFD** 配置文件），选择以下选项之一：
   - **default**（默认）— 仅使用默认设置。
   - 您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。
   - **New BFD Profile**（新建 **BFD** 配置文件）— 允许您创建 BFD 配置文件。

   选择 *None (Disable BFD)*（无（禁用 *BFD*））可对此静态路由禁用 *BFD*。
8. 单击 **OK**（确定）。

**IPv4** 或 **IPv6** 选项卡上的 BFD 列指示为静态路由配置的 BFD 配置文件。



© 2019 Palo Alto Networks, Inc.

STEP 8 | （可选）为所有的 BGP 接口或单一 BGP 对等设备启用 BFD。

如果全局启用或禁用 *BFD*，所有运行 *BGP* 的接口将关闭，然后通过 *BFD* 功能打开。这可能会破坏所有 *BGP* 通信。在接口上启用 *BFD* 后，防火墙会对接口上对等到程序 *BFD* 的 *BGP* 连接进行阻止。对等设备将发现 *BGP* 连接丢弃，这可导致重新收敛。在重新收敛的非高峰期间启用 *BFP* 接口上的 *BFD* 不会影响生产流量。

如果同时实现 *BFD* 用于 *BGP* 和 *HA* 路径监控，*Palo Alto Networks* 建议您不要执行 *BGP* 平稳重启。当 *BFD* 对等设备接口出现故障并且路径监控失败时，*BFD* 可以删除路由表中受影响的路由，并将此更改同步到被动 *HA* 防火墙，然后“平稳重启”方可生效。如果决定实施 *BFD* 用于 *BGP*、*BGP* 的平稳重启和 *HA* 路径监控，则应将 *BFD* 配置为比默认值更大的“理想最短传输时间间隔”和更大的“检测时间乘数”。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择要配置 BGP 的虚拟路由器。
2. 选择 **BGP** 选项卡。
3. （可选）应用 BFD 至所有虚拟路由器上的 BGP 接口，在 **BFD** 列表中，选择以下选项之一并单击 **OK**（确认）：
   - **default**（默认）— 仅使用默认设置。
   - 您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。
   - **New BFD Profile**（新建 **BFD** 配置文件）— 允许您创建 BFD 配置文件。

   选择 *None (Disable BFD)*（无（禁用 *BFD*））可对虚拟路由器上的所有 *BGP* 接口禁用 *BFD*；无法对单个 *BGP* 接口启用 *BFD*。
4. （可选）启用 BFD 获取单一 BGP 对等接口（只要没有启用，替代 BGP 的 **BFD** 设置），执行以下任务：
   1. 选择 **Peer Group**（对等组）选项卡。
   2. 选择一个对等地址组。
   3. 选择一个对等。
   4. 在 **BFD** 列表中选择以下选项之一：

      **default**（默认）— 仅使用默认设置。

      **Inherit-vr-global-setting**（继承 **Vr** 全局设置）（默认设置）— BGP 对等继承为虚拟路由器的 BGP 全域选择的 BFD 配置文件。

      您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。

      选择 *Disable BFD*（禁用 *BFD*）可对 *BGP* 对等禁用 *BFD*。
5. 单击 **OK**（确定）。
6. 单击 **OK**（确定）。

BGP - Peer Group/Peer（BGP - 对等组/对等）列表上的 BFD 列指示为接口配置的 BFD 配置文件。

STEP 9 | （可选）为 OSPF 或 OSPFv3，或者为 OSPF 接口全局启用 BFD。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择要配置 OSPF 或 OSPFv3 的虚拟路由器。
2. 选择 **OSPF** 或 **OSPFv3** 选项卡。
3. （可选）在 **BFD** 列表中，选择以下选项之一为所有 OSPF 或 OSPFv3 接口启用 BFD，然后单击 **OK**（确定）：
   - **default**（默认）— 仅使用默认设置。
   - 您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。
   - **New BFD Profile**（新建 **BFD** 配置文件）— 允许您创建 BFD 配置文件。


© 2019 Palo Alto Networks, Inc.

选择 *None (Disable BFD)*（无（禁用 *BFD*））可对虚拟路由器上的所有 *OSPF* 接口禁用 *BFD*；无法对单个 *OSPF* 接口启用 *BFD*。

4. （可选）在单一 OSPF 对等接口启用 BFD（只要没有禁用，替代 OSPF 的 **BFD** 设置），执行以下任务：
   1. 选择 **Areas**（区域）选项卡并选择一个区域。
   2. 在 **Interface**（接口）选项卡上，选择一个接口。
   3. 在 **BFD** 列表中，选择以下选项之一为特定的 OSPF 对等配置 BFD：

      **default**（默认）— 仅使用默认设置。

      **Inherit-vr-global-setting**（继承 **vr** 全局设置）（默认设置）— OSPF 对等继承虚拟路由器的 OSPF 或 OSPFv3 的 **BFD** 设置。

      您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。

      选择 *Disable BFD*（禁用 *BFD*）可对 *OSPF* 或 *OSPFv3* 接口禁用 *BFD*。
   4. 单击 **OK**（确定）。
5. 单击 **OK**（确定）。

OSPF **Interface**（接口）选项卡上的 BFD 列说明为接口配置的 BFD 配置文件。

STEP 10 | （可选）为 RIP 或单一 RIP 接口全局启用 BFD。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），并选择要配置 RIP 的虚拟路由器。
2. 选择 **RIP** 选项卡。
3. （可选）在 **BFD** 列表中，选择以下选项之一为虚拟路由器上的所有 RIP 接口启用 BFD，然后单击 **OK**（确定）：
   - **default**（默认）— 仅使用默认设置。
   - 您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。
   - **New BFD Profile**（新建 **BFD** 配置文件）— 允许您创建 BFD 配置文件。

   选择 *None (Disable BFD)*（无（禁用 *BFD*））可对虚拟路由器上的所有 *RIP* 接口禁用 *BFD*；无法对单个 *RIP* 接口启用 *BFD*。
4. （可选）要为单一 RIP 接口启用 BFD（只要没有禁用，替代 RIP 的 **BFD** 设置），执行以下任务：
   1. 选择 **Interfaces**（接口）选项卡，然后选择一个接口。
   2. 在 **BFD** 列表中选择以下选项之一：

      **default**（默认）— 仅使用默认设置）。

      **Inherit-vr-global-setting**（继承 **vr** 全局设置）（默认设置）— RIP 接口继承您为虚拟路由器的 RIP 全局选择的 BFD 配置文件。

      您配置的 BFD 配置文件 — 请参阅创建 BFD 配置文件。

      选择 *None (Disable BFD)*（无（禁用 *BFD*））可对 *RIP* 接口禁用 *BFD*。
   3. 单击 **OK**（确定）。
5. 单击 **OK**（确定）。

**Interface**（接口）选项卡说明为接口配置的 BFD 配置文件。

STEP 11 | 提交配置。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

STEP 12 | 查看 BFD 摘要和详细信息。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），找到所需的虚拟路由器，然后单击 **More Runtime Stats**（更多运行时统计数据）。
2. 选择 **BFD Summary Information**（**BFD** 摘要信息）选项卡，查看摘要信息，例如 BFD 状态和运行时间统计数据。
3. （可选）在需要查看接口的行中，选择 **details**（详细信息），即可查看引用：BFD 详细信息。

STEP 13 | 监控由路由配置、监控 BFD 统计数据、状态所引用的 BFD 配置文件。

使用以下 CLI 操作命令：

- **show routing bfd active-profile [***<name>***]**
- **show routing bfd details [interface***<name>***][local-ip***<ip>***][multihop][peer-ip** *<ip>***][session-id][virtual-router***<name>***]**
- **show routing bfd drop-counters session-id** *<session-id>*
- **show counter global | match bfd**

STEP 14 | （可选）清除 BFD 传输、接收和丢弃计数器。

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | （可选）清除调试 BFD 会话。

```
clear routing bfd session-state session-id all | <1-1024>
```

## 参考资料：URL 详细信息

要查看虚拟路由器的以下 BFD 信息，请参阅查看 BFD 摘要和详细信息中的步骤。

| 姓名 | 值（示例） | 说明 |
|---|---|---|
| 会话 ID | 1 | BFD 会话的 ID 号。 |
| 接口 | ethernet1/12 | BFD 运行时所选的接口。 |
| 协议 | STATIC(IPV4) OSPF | 静态路由（静态路由 IP 地址系列）和/或在接口上运行 BFD 的动态路由协议。 |
| 本地 IP 地址 | 10.55.55.2 | 接口的 IP 地址。 |
| 邻居 IP 地址 | 10.55.55.1 | BFD 邻居的 IP 地址。 |
| BFD 配置文件 | 默认设置*（此 BFD 会话有多个 BFD 配置文件。最低的“理想最小 Tx 间隔时间 (ms) 用于选择有效的配置文件。） | 应用至接口的 BFD 配置文件名称。<br>由于样本接口具有静态路由和 OSPF 运行 BFD，带不同的配置文件，则防火墙使用具有最低 **Desired Minimum Tx Interval**（理想最小 **Tx** 间隔时间）的配置文件。在本例中，使用的配置文件是默认配置文件。 |


© 2019 Palo Alto Networks, Inc.

| 姓名 | 值（示例） | 说明 |
| --- | --- | --- |
| 状态（本地/远程） | 运行/运行 | 本地和远程 BFD 对等设备的状态。可能的状态包括 admin down（管理故障）、down（故障）、init（初始化）和 up（运行）。 |
| 运行时间 | 2 小时 36 分 21 秒 419 毫秒 | BFD 已经启动的时间长度（小时、分钟、秒和毫秒）。 |
| 鉴别（本地/远程） | 1391591427/1 | 本地和远程 BFD 对等设备的鉴别。 |
| 模式 | 活跃 | 在接口上配置 BFD 的模式：主动或被动 |
| 按需模式 | 禁用 | PAN-OS 不支持 BFD 按需模式，因此始终处于禁用状态。 |
| 多跃点 | 禁用 | BFD 多跃点：启用或禁用。 |
| 多跃点 TTL | | 多跃点 TTL；范围为 1-254。如果禁用 Multihop（多跃点），则字段为空。 |
| 本地诊断代码 | 0（无诊断） | 诊断代码指示本地系统最后改变状态的原因：<br>0—无诊断<br>1—控制检测时间耗尽<br>2—回显功能故障<br>3—邻居信号显示会话关闭<br>4—转发面板重置<br>5—路径关闭<br>6—连接路径关闭<br>7—管理关闭<br>8—反向连接路径关闭 |
| 最后接收远程诊断代码 | 0（无诊断） | 最后从 BFD 对等设备接收的诊断代码。 |
| 传输保持时间 | 0 毫秒 | BFD 发送 BFD 控制数据包之前，链路启用后的保持时间（毫秒）。0 毫秒保持时间是指马上发送。范围为 0-120000 毫秒。 |
| 最短接收间隔 | 1000 毫秒 | 从对等设备接收的最短接收间隔；BFD 对等设备接收控制数据包的间隔。最长为 2000 毫秒。 |
| 协商的传输间隔 | 1000 毫秒 | BFD 对等设备同意互相发送 BFD 控制数据包的传输间隔（毫秒为单位）。最长为 2000 毫秒。 |
| 接收的乘数 | 3 | 来自 BFD 对等设备的检测时间乘数值。发送时间乘以乘数等于检测时间。如果在检测时间耗尽前，BFD 未从其对等接收到 BFD 控制数据包，则会出现故障。范围为 2 - 50。 |


© 2019 Palo Alto Networks, Inc.

| 姓名 | 值（示例） | 说明 |
| --- | --- | --- |
| 检测时间（已超出） | 3000ms (0) | 超过了计算的检测时间（协商的传输间隔乘以乘数）和检测时间所超过的毫秒数。 |
| 传输控制数据包（最后） | 9383（420 毫秒之前） | BFD 所传输的控制数据包数量（以及自 BFD 传输最近控制数据包起的时间长）。 |
| 接收控制数据包（最后） | 9384（407 毫秒之前） | BFD 所接收的控制数据包数量（以及自 BFD 接收最近控制数据包起的时间长）。 |
| 代理数据面板 | 插槽 1 - DP 0 | 在 PA-7000 系列防火墙上，已分配数据面板 CPU，以处理此 BFD 会话的数据包。 |
| 错误 | 0 | BFD 错误数。 |
| 引起状态更改的最后数据包 | | |
| 版本 | 1 | BFD 版本。 |
| 轮询位 | 0 | BFD 轮询位；0 表示未设置。 |
| 理想的最短传输间隔 | 1000 毫秒 | 引起状态更改的最后一个数据包的理想最短传输间隔。 |
| 要求的最短接收间隔时间 | 1000 毫秒 | 引起状态更改的最后一个数据包的要求最短传输间隔时间。 |
| 检测乘数 | 3 | 引起状态更改的最后一个数据包的检测乘数。 |
| 我的鉴别器 | 1 | 远程鉴别器鉴别是对端用于区分它们之间多个 BFD 会话的独特非零值。 |
| 您的鉴别器 | 1391591427 | 本地鉴别器鉴别是对端用于区分它们之间多个 BFD 会话的独特非零值。 |
| 诊断代码 | 0（无诊断） | 引起状态更改的最后一个数据包的诊断代码。 |
| 长度 | 24 | BFD 控制数据包的长度（以字节为单位）。 |
| 按需位 | 0 | PAN-OS 不支持 BFD 按需模式，因此按需位始终设置为 0（禁用）。 |
| 最后位 | 0 | PAN-OS 不支持轮询序列，因此最后位始终设置为 0（禁用）。 |
| 多点位 | 0 | 此位预留用于将来 BFD 的点对多点扩展。它在传播和接收时都必须为零。 |
| 控制面板独立位 | 1 | • 如果设置为 1，传输系统的 BFD 实施不与其控制面板共享命运（也就是说，BFD 在转发面板实施，即使控制面板发生故障也可以继续正常运转）。在 PAN-OS 中，此位始终设置为 1。 |


© 2019 Palo Alto Networks, Inc.

| 姓名 | 值（示例） | 说明 |
| --- | --- | --- |
| | | • 如果设置为 0，传输系统的 BFD 实施与其控制面板共享命运。 |
| 身份验证呈现位 | 0 | PAN-OS 不支持 BFD 身份验证，因此身份验证呈现位始终设置为 0。 |
| 要求的最短回显接收间隔时间 | 0 毫秒 | PAN-OS 不支持 BFD 回显功能，因此始终为 0ms。 |



© 2019 Palo Alto Networks, Inc.

# 会话设置和超时

本部分介绍会影响 TCP、UDP 和 ICMPv6 会话的全局设置（除 IPv6、NAT64、NAT 超额订阅、jumbo frame 大小、MTU、加速老化和身份验证门户身份验证之外）。您还可以通过一个设置（重新匹配会话）将新配置的安全策略应用于已在进行的会话。

下列主题中的前几个主题将对 OSI 模型的传输层、TCP、UDP 和 ICMP 进行简单介绍。有关这些协议的详细信息，请参阅相应的 RFC。其余主题将介绍会话超时和设置。

- 传输层会话
- TCP
- UDP
- ICMP
- 控制特定 ICMP 或 ICMPv6 类型和代码
- 配置会话超时
- 会话分发策略
- 配置会话设置
- 阻止 TCP 分离握手会话建立

## 传输层会话

网络会话是在两个或更多通信设备间进行的消息交换，会持续一段时间。会话会建立，并会在结束后断开。OSI 模型的三个层（传输层、会话层和应用层）中出现的会话类型各不相同。

传输层位于 OSI 模型的第 4 层，可针对数据提供可靠或不可靠的端到端交付和流控制。用于在传输层实施会话的互联网协议包括传输控制协议 (TCP) 和用户数据报协议 (UDP)。

## TCP

传输控制协议 (TCP) (RFC 793) 是 Internet 协议 (IP) 集中的主要协议之一，常和 IP 统称为 *TCP/IP*。TCP 被视为可靠的传输协议，因为它会在传输和接收段时进行错误检查，会确认收到的段，并会对送达时顺序错误的段进行重新排序。TCP 还会针对丢弃段请求并进行重新传输。TCP 有状态且面向连接，表示会在会话期间在发送方和接收方之间建立连接。TCP 会针对数据包进行流控制，以应对网络拥挤。

TCP 会在会话设置期间执行握手，以便发起并确认会话。数据传输完成后，会话将按顺序关闭，两端会传输 FIN 数据包并通过 ACK 数据包进行确认。发起 TCP 会话的握手通常是发起程序和侦听程序之间的三向握手（交换三个消息），或者可以是其他形式，如四向或五向分离握手或同步开放式。TCP 分离握手丢弃说明了如何阻止 TCP 分离握手会话建立。

使用 TCP 作为传输协议的应用包括超文本传输协议 (HTTP)、安全 HTTP (HTTPS)、文件传输协议 (FTP)、简单邮件传输协议 (SMTP)、Telnet、邮局协议版本 3 (POP3)、Internet 消息访问协议 (IMAP) 和安全外壳 (SSH)。

下列主题详细介绍了 TCP 的 PAN-OS 实施。

- “TCP 半闭合”和“TCP 等待时间”计时器
- “未验证的 RST”计时器
- TCP 分离握手丢弃
- 最大分段大小 (MSS)

您可以使用防火墙上的区域保护配置文件以配置基于数据包的攻击保护，从而丢弃具有不良特性的 IP、TCP 和 IPv6 数据包，或者在允许数据包进入区域之前，从数据包中删除不需要的选项。您还可以配置泛滥攻击保护，指定触发警报、导致防火墙随机丢弃 SYN 数据包或使用 SYN cookie、使防火墙丢弃超过最大速率的 SYN 数据包的每秒 SYN 连接速率（不匹配现有会话）。

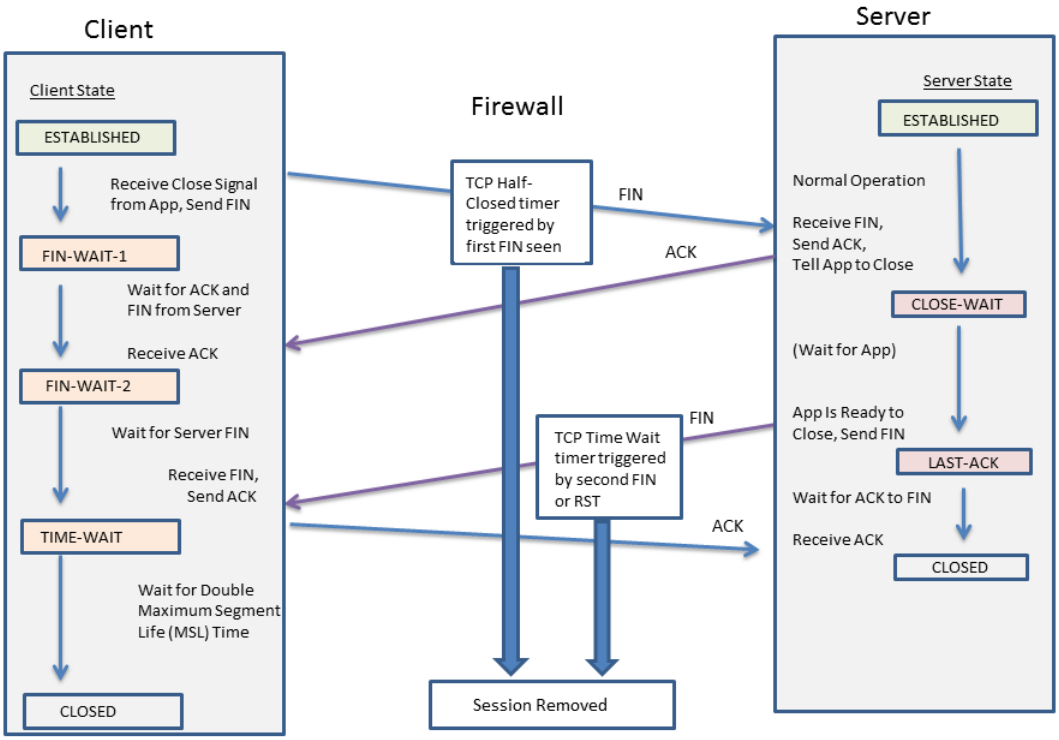

© 2019 Palo Alto Networks, Inc.

## “TCP 半闭合”和“TCP 等待时间”计时器

TCP 连接终止过程会使用“TCP 半闭合”计时器，该计时器由防火墙针对会话检测到的第一个 FIN 来触发。该计时器名为“TCP 半闭合”，因为 FIN 只会由连接的一端发出。第二个计时器，即“TCP 等待时间”，则由第二个 FIN 或由 RST 来触发。

如果防火墙只让第一个 FIN 触发一个计时器，那么过短的设置会导致半闭合会话过早关闭。反之，过长的设置会导致会话表过量增长，还可能会占用所有的会话。您可以利用两个计时器来设置一个相对较长的“TCP 半闭合”计时器和一个较短的“TCP 等待时间”计时器，以使全闭合会话快速老化并控制会话表的大小。

下图显示了防火墙的两个计时器在 TCP 连接终止过程中被触发的情况。




由于以下原因，“TCP 等待时间”计时器应设置为小于“TCP 半闭合”计时器的值：

- 如果在检测到第一个 FIN 后所留的时间较长，那么用于完全关闭会话的连接时间则较短。
- 等待时间较短是因为，在检测到第二个 FIN 或检测到 RST 后，会话无需长时间保持打开状态。较短的等待时间能够更早地释放资源，还能留出时间让防火墙检测最终 ACK 并重新传输其他数据报（如有需要）。

如果将“TCP 等待时间”计时器配置为大于“TCP 半闭合”计时器的值，提交会被接受，但实际上“TCP 等待时间”计时器不会超过“TCP 半闭合”值。

可以针对全局或针对各个应用设置这两个计时器。默认情况下，全局设置将用于所有应用。如果对“TCP 等待”计时器进行应用级配置，那么全局设置将被覆盖。

## “未验证的 RST”计时器

如果防火墙收到无法验证的重置 (RST) 数据包（因为该数据包在 TCP 窗口中的序列号并非预期值，或是该数据包来自非对称路径），那么“未验证的 RST”计时器将对会话进行老化控制。默认为 30 秒，范围为 1-600 秒。“未验证的 RST”计时器提供了额外的安全措施，下面的第二个要点对此进行了说明。



© 2019 Palo Alto Networks, Inc.

RST 数据包有三种可能的处理结果：

- 未进入 TCP 窗口的 RST 数据包将被丢弃。
- 进入 TCP 窗口但没有正确的预期序列号的 RST 数据包不会进行验证，但会采用“未验证的 RST”计时器设置。这么做有助于防止拒绝服务 (DoS) 攻击，这类攻击会向防火墙发送随机 RST 数据包以尝试中断现有会话。
- 进入 TCP 窗口并有正确的预期序列号的 RST 数据包会采用“TCP 等待时间”计时器设置。

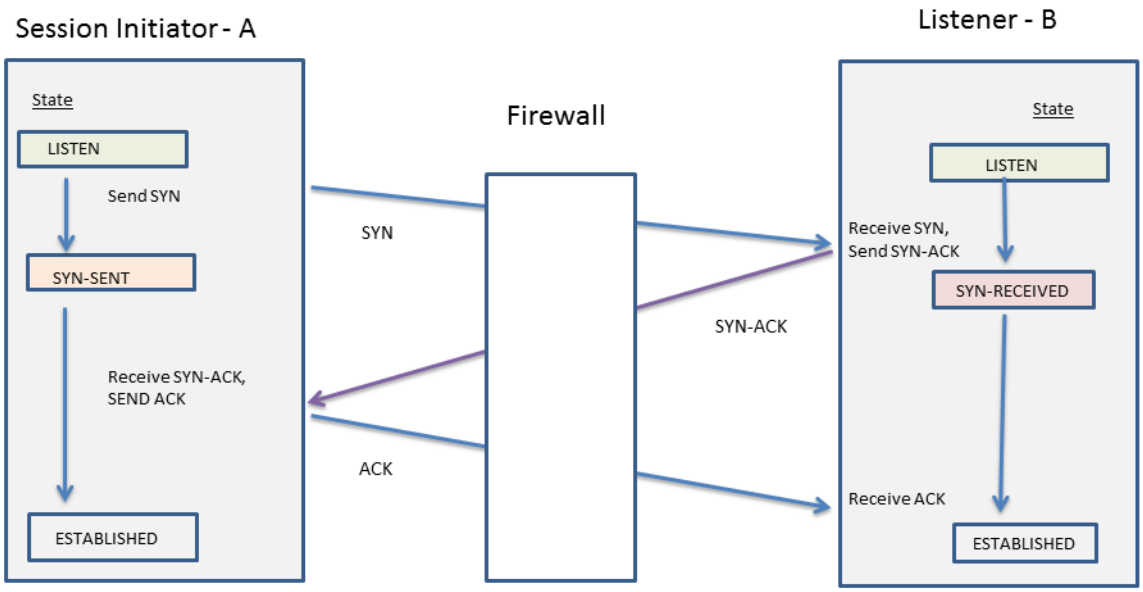
## TCP 分离握手丢弃

如果 TCP 会话建立过程中不使用众所周知的三向握手，而使用其他形式（如，四向或五向分离握手或同步开放式），区域保护配置文件中的 **Split Handshake**（分离握手）选项将阻止此 TCP 会话的建立。

Palo Alto Networks 下一代防火墙能在不启用 **Split Handshake**（分离握手）选项的情况下正确地处理会话以及所有适用于分离握手和同步开放式会话建立的第 7 层流程。但是，仍会提供 **Split Handshake**（分离握手）选项（会导致 TCP 分离握手丢弃）。如果为区域保护配置文件配置 **Split Handshake**（分离握手），而且该配置文件被应用于某个区域，那么必须使用标准的三向握手为该区域中的接口建立 TCP 会话；不允许使用变体。

**Split Handshake**（分离握手）在默认情况下禁用。

下图演示了用于通过 PAN-OS 防火墙在发起程序（通常是客户端）和侦听程序（通常是服务器）之间建立 TCP 会话的标准三向握手。




为分配给区的区保护配置文件配置了 **Split Handshake**（分离握手）选项。属于此区的接口将丢弃发送自服务器的所有同步 (SYN) 数据包，以阻止以下形式的握手。该图中的字母 A 表示会话发起程序，字母 B 表示侦听程序。握手的每个编号段都有一个箭头，用以指示从发送程序到接收程序的段方向，且每个段都指示了控制位设置。


© 2019 Palo Alto Networks, Inc.

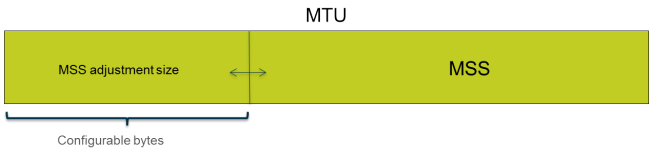
| 4-Way Split Handshake (Version 1) | 4-Way Split Handshake (Version 2) | Simultaneous Open | 5-Way Split Handshake |
|---|---|---|---|
| 1. A → B SYN<br>2. A ← B ACK<br>3. A ← B SYN<br>4. A → B ACK | 1. A → B SYN<br>2. A ← B SYN<br>3. A → B SYN-ACK<br>4. A ← B ACK | 1. A → B SYN<br>2. A ← B SYN<br>3. A → B SYN-ACK<br>4. A ← B SYN-ACK | 1. A → B SYN<br>2. A ← B ACK<br>3. A ← B SYN<br>4. A → B SYN-ACK<br>5. A ← B ACK |

可以阻止 TCP 分离握手会话建立。

## 最大分段大小 *(MSS)*

最大传输单元 (MTU) 是可以在单个 TCP 数据包传输的最大字节数。MTU 包括标头长度，因此 MTU 减去标头的字节数等于最大分段大小 (MSS)，也就是可以在单个数据包中传输的最大字节数。

MSS 的大小可配置（见上文），因此你的防火墙可以穿过具有比默认设置所允许更长标头的流量。Encapsulation（封装）功能可增长标头，这将有助于配置 MSS 调整大小，以允许 MPLS 标头或带 VLAN 标记的隧道通信等的字节。




如果设置不分片 (DF) 位集合的数据包，更大的 MSS 调整大小和更小的 MSS 会特别有帮助，从而较长的标头不会导致数据包长度超过所允许的 MTU。如果设置了 DF 位数据包，并且超过了 MTU，会丢弃较大的数据包。



您可以全局配置防火墙，以对超出出口接口 *MTU* 的 *IPv4* 数据包进行分段，即使是在数据包中已设置 *DF* 位的情况下。使用 *CLI* 命令 ***debug dataplane set ip4-df-ignore yes*** 启用第 *3* 层物理接口和 *IPSec* 隧道接口。使用 *CLI* 命令 ***debug dataplane set ipv4-df-ignore no*** 将防火墙恢复为默认行为。

防火墙支持在以下第 3 层接口类型的 IPv4 和 IPv6 地址可配置 MSS 调整大小：以太网、子接口、聚合以太网 (AE)、VLAN 和回环。IPv6 MSS 调整大小仅适用于在接口上启用 IPv6 的情况。



如果在接口上启用 *IPv4* 和 *IPv6*，*MSS* 调整大小在两个 *IP* 地址格式之间不同，与 *IP* 类型对应的适当 *MSS* 值用于 *TCP* 流量。

对于 IPv4 和 IPv6 地址，防火墙可以适应比预期更大的 TCP 标头长度。如果 TCP 数据包标头长度比计划的长，防火墙选择以下两个值中较大的 MSS 调整大小：

- 配置的 MSS 调整大小
- TCP 标头长度 (20) + TCP SYN 的 IP 标头长度总和

此操作意味着，如有必要，防火墙覆盖 MSS 调整大小。例如，如果你配置 MSS 调整大小为 42，你希望 MSS 等于 1458（默认 MTU 大小减去调整值 [1500 - 42]）。然而，TCP 数据包在标头有额外的 4 字节 IP 选项，因此 MSS 调整大小 (20+20+4) 等于 44，大于配置的 MSS 调整大小 42。得出的 MSS 为 1500-44=1456 字节，比预期的要小。



© 2019 Palo Alto Networks, Inc.

若要配置 MSS 调整大小，请参阅配置会话设置。

## UDP

用户数据报协议 (UDP) (RFC 768) 是 IP 集中的另一个主要协议，可代替 TCP。UDP 无状态且无连接，设置会话时不会握手，也不会在发送方和接收方之间建立连接；会通过不同路由向单个目标传送数据包。UDP 被视为不可靠的协议，因为它不会针对数据报进行确认、错误检测、重新传输或重新排序。由于无需提供这些功能，因此 UDP 的延迟较少并快于 TCP。UDP 被称为尽力而为的协议，因为它没有可确保数据送达目标的机制或保证。

UDP 数据包封装在 IP 数据包中。虽然 UDP 会使用校验和来验证数据完整性，但它不会执行网络接口级错误检查。错误检查被假设为无需执行，或由应用程序（而非 UDP 本身）来执行。UDP 没有数据包流控制处理机制。

UDP 通常用于需要更快速度的应用程序以及对时间敏感的实时交付，如 IP 语音 (VoIP)、流音频和视频以及线上游戏。UDP 面向事务，因此也用于需要响应来自多个客户端的小型查询的应用程序，如域名系统 (DNS) 和普通文件传输协议 (TFTP)。

您还可以在防火墙上使用区域保护配置文件配置泛滥攻击保护，从而指定触发警报、触发防火墙随机丢弃 UDP 数据包、使防火墙丢弃超过最大速率的 UDP 数据包的每秒 UDP 连接速率（不匹配现有会话）。（虽然 UDP 无连接，但是防火墙会基于会话跟踪 IP 数据包中的 UDP 数据报；因此，如果 UDP 数据包与现有会话不匹配，则被视为新会话，并作为与阈值的连接进行计数。）

## ICMP

Internet 控制消息协议 (ICMP) (RFC 792) 是 Internet 协议集中的另一个主要协议，用于 OSI 模型的网络层。ICMP 用于诊断和控制目的，以发送与 IP 操作相关的错误消息，或是发送与所请求服务或与主机或路由器可访问性相关的消息。网络使用程序（如 traceroute 和 ping）将通过各种 ICMP 消息来实施。

ICMP 是一种无连接协议，不会打开或维护实际会话。但是，可以将两个设备间的 ICMP 消息视为会话。

Palo Alto Networks 防火墙支持 ICMPv4 和 ICMPv6。您可以通过以下几种方式控制 ICMPv4 和 ICMPv6 数据包：

- 在规则中创建基于 ICMP 和 ICMPv6 数据包的安全策略规则并选择 **icmp** 或 **ipv6-icmp** 应用程序。
- 当您配置会话设置时控制ICMPv6 速率限制。
- 使用区域保护配置文件配置泛滥攻击保护，指定触发警报、触发防火墙随机丢弃 ICMP 或 ICMPv6 数据包、使防火墙丢弃超过最大速率的 ICMP 或 ICMPv6 数据包的每秒 ICMP 或 ICMPv6 连接速率（不匹配现有会话）。
- 使用区域保护配置文件配置基于数据包的攻击保护：
  - 对于 ICMP，您可以丢弃某些类型的数据包，或抑制某些数据包的发送。
  - 对于 ICMPv6 数据包（类型 1、2、3、4 和 137），您可以指定防火墙使用 ICMP 会话密钥来匹配安全策略规则，以确定是否允许 ICMPv6 数据包。（防火墙使用安全策略规则，覆盖使用嵌入式数据包的默认行为来确定会话匹配。）当防火墙丢弃符合安全策略规则的 ICMPv6 数据包时，防火墙会在流量日志中记录详细信息。

### 基于 *ICMP* 和 *ICMPv6* 数据包的安全策略规则

只有当安全策略规则允许会话时，防火墙才会转发 ICMP 或 ICMPv6 数据包（就像防火墙转发其他数据包类型一样）。防火墙依据其中一种方式来确定会话匹配，即该数据包是否是 ICMP 或 ICMPv6 错误数据包，或是与 ICMP 或 ICMPv6 信息数据包相反的重定向数据包：

- **ICMP** 类型 **3**、**5**、**11** 和 **12** 以及 **ICMPv6** 类型 **1**、**2**、**3**、**4** 和 **137** — 默认情况下，防火墙会从导致错误的原始数据包（调用数据包）中查找嵌入式 IP 数据包的字节数。如果嵌入式数据包与现有会话相匹配，则防火墙会根据与该会话相匹配的安全策略规则中指定的操作进行转发或丢弃 ICMP 或 ICMPv6 数据包。（您可以使用带基于数据包攻击保护功能的区域保护配置文件来替换 ICMPv6 类型的默认行为。）


© 2019 Palo Alto Networks, Inc.

- 剩余 **ICMP** 或 **ICMPv6** 数据包类型 — 防火墙将 ICMP 或 ICMPv6 数据包视为新会话处理。如果安全策略规则与数据包（防火墙标识为 **icmp** 或 **ipv6-icmp** 会话）匹配，则防火墙将根据安全策略规则操作转发或丢弃该数据包。安全策略计数器和流量日志反映了这些操作。

  如果不存在与数据包匹配的安全策略规则，则防火墙应用其默认安全策略规则，允许区域内流量并阻止区域间流量（默认情况下将为这些规则禁用日志记录）。

  虽然您可以替换默认规则以启用日志记录或更改默认操作，但我们不建议您更改特定案例的默认行为，因为这样做会对受默认规则影响的所有流量产生影响。相反，应创建安全策略规则来明确控制和记录 *ICMP* 或 *ICMPv6* 数据包。

  有两种方法可以创建明确的安全策略规则，以处理不是错误数据包或重定向数据包的 ICMP 或 ICMPv6 数据包：

  - 创建一个安全策略规则，以允许（或拒绝）所有 **ICMP** 或 **ICMPv6** 数据包 — 在安全策略规则中，指定应用程序 **icmp** 或 **ipv6-icmp**；防火墙将分别允许（或拒绝）与 ICMP 协议号 (1) 或 ICMPv6 协议号 (58) 匹配的所有 IP 数据包通过防火墙。
  - 创建自定义应用程序和安全策略规则以允许（或拒绝）来自或应用于该应用程序的数据包 — 这种方法更精细，允许您使用控制特定 ICMP 或 ICMPv6 类型和代码。

## *ICMPv6* 速率限制

ICMPv6 速率限制是一种节流机制，可以防止泛滥攻击和 DDoS 尝试。可通过实施来应用错误数据包速率和令牌桶，以协同实现节流并确保 ICMP 数据包不会对有防火墙保护的网段进行泛滥攻击。

首先，全局 **ICMPv6 Error Packet Rate (per sec)**（**ICMPv6** 错误数据包速率（每秒））可以控制允许通过防火墙的 ICMPv6 错误数据包的速率；默认为每秒 100 个数据包；范围为每秒 10 到 65535 个数据包。如果防火墙达到 ICMPv6 错误数据包速率，那么令牌桶就会生效并进行节流（如下所示）。

“逻辑令牌桶”这一概念将控制可用于传输 ICMP 消息的速率。桶中的令牌数可以配置，每个令牌都代表一条可以发送的 ICMPv6 消息。每发送一条 ICMPv6 消息，令牌计数就会递减；当桶中的令牌数为零时，便不能再发送 ICMPv6 消息，除非在桶中添加额外的令牌。令牌桶的默认大小为 100 个令牌（数据包）；范围为 10 到 65535 个令牌。

要更改默认令牌桶大小或错误数据包速率，请参阅 配置会话设置部分。

# 控制特定 ICMP 或 ICMPv6 类型和代码

使用此任务创建自定义 ICMP 或 ICMPv6 应用程序，然后创建安全策略规则以允许或拒绝该应用程序。

STEP 1 | 为 ICMP 或 ICMPv6 消息类型和代码创建自定义应用程序。

1. 选择 **Object**（对象）> **Applications**（应用程序）并 **Add**（添加）自定义应用程序。
2. 在 **Configuration**（配置）选项卡上，输入自定义应用程序的 **Name**（名称）和 **Description**（说明）。例如，输入名称 ping6。
3. 对于 **Category**（类别），请选择 **networking**（联网）。
4. 对于 **Subcategory**（子类别），请选择 **ip-protocol**。
5. 对于 **Technology**（技术），请选择 **network-protocol**。
6. 单击 **OK**（确定）。
7. 在 **Advanced**（高级）选项卡上，选择 **ICMP Type**（**ICMP** 类型）或 **ICMPv6 Type**（**ICMPv6** 类型）。
8. 对于 **Type**（类型），输入指定要允许或拒绝的 ICMP 或 ICMPv6 消息类型的数字（范围为 0-255）。例如，Echo Request 消息 (ping) 为 128。
9. 如果类型包含代码，请输入适用于要允许或拒绝的 **Type**（类型）值的 **Code**（代码）编号（范围为 0-255）。某些 **Type**（类型）值仅包含代码 0。
10. 单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 创建允许或拒绝您创建的自定义应用程序的安全策略规则。

创建安全策略规则。在 **Application**（应用程序）选项卡上，指定刚创建的自定义应用程序的名称。

STEP 3 | 提交更改。

单击 **Commit**（提交）。

# 配置会话超时

会话超时将定义 PAN-OS 在会话进入非活动状态后在防火墙上进行会话维护的持续时间。默认情况下，协议的会话超时到期时，PAN-OS 会关闭会话。您可以定义 TCP、UDP、尤其是 ICMP 会话的超时数值。默认超时值将应用于所有其他类型的会话。这些超时值都是全局性的，这意味着它们将应用于防火墙上的所有此类会话。

您还可以配置全局 ARP 缓存超时设置，以控制防火墙在其缓存中保留 ARP 条目（IP 地址到硬件地址映射）的时长。

除了全局设置以外，您还可以在 **Objects**（对象）> **Applications**（应用程序）选项卡中定义单个应用程序的超时值。防火墙会将应用程序超时值应用于处于已建立状态的应用程序。配置完成后，应用程序的超时值将替代全局 TCP 或 UDP 会话超时值。



如果在应用层更改 *TCP* 或 *UDP* 计时器，则将在所有虚拟系统中实施预定义应用程序和共享自定义应用程序中使用的这些计时器。如果需要应用程序计时器不同于虚拟系统，则必须创建自定义应用程序，为其分配独有的计时器，然后将自定义应用程序分配给唯一的虚拟系统。

如果需要为 TCP、UDP、ICMP、身份验证门户身份验证或其他类型的会话更改全局会话超时设置的默认值，请执行以下任务。所有值都以秒为单位。



默认值是最佳值。但是，您可以根据网络需求对其进行修改。将值设置得太低可能会导致对轻微的网络延迟过于敏感,还可能会导致无法与防火墙建立连接。将值设置得太高可能会导致故障检测延迟。

STEP 1 | 访问会话超时。

选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话超时。

STEP 2 | （可选）更改其他超时。

- **Default**（默认值）— 非 TCP/UDP 或非 ICMP 会话能在没有响应的情况下处于打开状态的最长时间（范围为 1 - 15,999,999，默认为 30）。
- **Discard Default**（丢弃默认值）— 在 PAN-OS 根据防火墙上配置的安全策略拒绝会话后非 TCP/UDP 会话将处于打开状态的最长时间（范围为 1 - 15,999,999，默认为 60）。
- **Scan**（扫描）— 任意会话在被视为处于非活动状态后将处于打开状态的最长时间（范围为 5 - 30，默认为 10）；当应用程序超出为其定义的应用程序滴滤阈值时，该应用程序将被视为处于非活动状态。
- **Authentication Portal**（身份验证门户）— 身份验证门户 Web 表单的身份验证会话超时。用户必须在此表单内输入验证凭证并验证成功才能访问请求的内容（范围为 1 - 15,999,999，默认为 30）。
- 要定义其他身份验证门户超时，如空闲计时器以及到期时间（在经过此时间之后，必须重新对用户进行身份验证），请选择 **Device**（设备）> **User Identification**（用户标识）> **Authentication Portal Settings**（身份验证门户设置）。请参阅配置身份验证门户。

STEP 3 | （可选）更改 TCP 超时。

- **Discard TCP**（丢弃 **TCP**）— TCP 会话在根据防火墙上配置的安全策略被拒后将处于打开状态的最长时间。默认：90。范围：1 - 15,999,999。
- **TCP** — TCP 会话在进入已建立状态后（即在握手完成和/或数据传输开始后）且没有响应的情况下保持打开状态的最长时间。默认： 3,600。范围：1 - 15,999,999。



© 2019 Palo Alto Networks, Inc.

- **TCP Handshake**（**TCP** 握手）— 从接收 SYN-ACK 及后续 ACK 开始到完全建立会话之间，允许经过的最长时间。默认：10。范围：1 - 60。
- **TCP init** — 从接收 SYN 和 SYN-ACK 开始到启动 TCP 握手计时器之前，允许经过的最长时间。默认：5.范围：1 - 60。
- **TCP Half Closed**（**TCP** 半闭合）— 接收第一个 FIN 和接收第二个 FIN 或接收 RST 之间相隔的最长时间。默认：120。范围： 1 - 604,800。
- **TCP Time Wait**（**TCP** 等待时间）— 接收第二个 FIN 或接收 RST 之后经历的最长时间。默认：15。范围：1 - 600。
- **Unverified RST**（未验证的 **RST**）— 接收无法验证的 RST（RST 在 TCP 窗口中，但其序列号并非预期值，或是 RST 来自非对称路径）之后经历的最长时间。默认：30。范围：1 - 600。
- 另请参阅（可选）更改其他超时部分中的 **Scan**（扫描）超时。

STEP 4 | （可选）更改 UDP 超时。

- **Discard UDP**（丢弃 **UDP**）— UDP 会话在根据防火墙上配置的安全策略被拒后将处于打开状态的最长时间。默认：60。范围：1 - 15,999,999。
- **UDP** — UDP 会话能在没有 UDP 响应的情况下保持打开状态的最长时间。默认：30。范围：1 - 15,999,999。
- 另请参阅（可选）更改其他超时部分中的 **Scan**（扫描）超时。

STEP 5 | （可选）更改 ICMP 超时。

- **ICMP** — ICMP 会话能在没有响应的情况下处于打开状态的最长时间。默认：6。范围：1 - 15,999,999。
- 另请参阅（可选）更改其他超时部分中的 **Discard Default**（丢弃默认值）和 **Scan**（扫描）超时。

STEP 6 | 单击 **OK**（确定）和 **Commit**（提交）。

STEP 7 | （可选）更改 ARP 缓存超时。

1. 访问 CLI 并指定防火墙在其缓存中保留 ARP 条目的时长（秒）。使用操作命令 **`set system setting arp-cache-timeout`** <*value*>，其中范围为 60 到 65535；默认为 1800。

   如果减少超时且缓存中现有条目的 TTL 大于新超时，则防火墙将删除这些条目并刷新 ARP 缓存。如果增加超时且现有条目的 TTL 小于新超时，根据 TTL，他们将会过期，并且防火墙会使用较大的超时值缓存新的条目。
2. 使用 CLI 操作命令 **`show system setting arp-cache-timeout`** 查看 ARP 缓存超时设置。

# 配置会话设置

本主题将介绍会话的各个设置，而非超时值。如果需要更改默认设置，请执行以下任务。

STEP 1 | 更改会话设置。

选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。

STEP 2 | 指定是否要应用新配置的安全策略规则至进行中的会话。

选择 **Rematch all sessions on config policy change**（重新匹配配置策略更改的所有会话）使防火墙将新配置的安全策略规则应用于已在进行的会话。该功能在默认情况下已启用。如果要清除此复选框，执行的所有策略规则仅适用于提交策略更改之后启动的会话。

例如，如果在将关联策略规则配置为允许 Telnet 后启动了一个 Telnet 会话，随后您又提交了策略更改以拒绝 Telnet，那么防火墙会将这个经过修订的策略应用于当前会话并阻止该对话。

STEP 3 | 配置 IPv6 设置。



© 2019 Palo Alto Networks, Inc.

- **ICMPv6 Token Bucket Size**（**ICMPv6** 令牌桶大小）— 默认：100 个令牌。请参阅 ICMPv6 速率限制部分。
- **ICMPv6 Error Packet Rate (per sec)**（**ICMPv6** 错误数据包速率（每秒））— 默认：100 显示动态组定义的两个示例。请参阅 ICMPv6 速率限制部分。
- **Enable IPv6 Firewalling**（启用 **IPv6** 防火墙）— 为 IPv6 启用防火墙功能。如果未启用 IPv6，则忽略所有基于 IPv6 的配置。即使为接口启用了 IPv6，为了让 IPv6 正常工作，仍需启用 **IPv6 Firewalling**（**IPv6** 防火墙）设置。

STEP 4 | 启用 Jumbo Frame 并设置 MTU。

1. 选择 **Enable Jumbo Frame**（启用 **Jumbo Frame**）— 启用 Ethernet 接口上的 Jumbo Frame。Jumbo frame 的最大传输单元 (MTU) 为 9,216 字节，仅某些型号的设备可使用此功能。
2. 取决于是否启用 Jumbo frame，设置 **Global MTU**（全局 **MTU**）：
   - 如果没有启用 Jumbo Frame，**Global MTU**（全局 **MTU**）默认为 1,500 字节；范围为 576 到 1,500 字节。
   - 如果启用 Jumbo Frame，**Global MTU**（全局 **MTU**）默认为 9,192 字节；范围为 9,192 到 9,216 字节。

   *Jumbo Frames* 所占内存最多为正常数据包的五倍，可将可用数据包缓冲区的数据减少 *20%*。这样，可减少专用于乱序、应用程序标识以及其他此类数据包处理任务的队列大小。如果您从 *PAN-OS 8.1* 开始启用 *Jumbo* 帧全局 *MTU* 配置，并重启您的防火墙，则将重新分发数据包缓冲区，以更有效地处理 *Jumbo* 帧。

   如果启用了 jumbo frame 并存在 MTU 未经专门配置的接口，那么这些接口将自动继承该 jumbo frame 大小。因此，在启用 Jumbo Frame 之前，如果存在不希望其包含 Jumbo Frame 的任何接口，您必须将该接口的 MTU 设置为 1500 字节或其他值。

STEP 5 | 调节 NAT 会话设置。

- **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小网络 **MTU**）— 设置 IPv6 转换流量的全局 MTU。默认值 1,280 字节基于 IPv6 通信的标准最小 MTU。
- **NAT Oversubscription Rate**（**NAT** 超额订阅率）— 如果将 NAT 配置为动态 IP 和端口 (DIPP) 转换，那么就可以将超额订阅率配置为乘以可以同时使用同一转换 IP 地址和端口对的次数。该比率为 1、2、4 或 8。默认设置取决于防火墙型号。
- 比率 1 意味着不能进行超额订阅；每个已转换 IP 地址和端口对每次都只能使用一次。
- 如果设置为 **Platform Default**（平台默认值），那么用户配置的比率将被禁用，并会应用型号的默认超额订阅率。

降低超额订阅率会减少源设备转换次数，但能提高 NAT 规则容量。

STEP 6 | 调节加速老化设置。

选择 **Accelerated Aging**（加速老化）可加快空闲会话的老化。你还可以更改阈值 (%) 和换算系数：

- **Accelerated Aging Threshold**（加速老化阈值）— 加速老化开始时的会话表全百分比。默认值为 80%。会话表一旦达到该阈值（全百分比），PAN-OS 就会在所有会话的老化计算中应用加速老化换算系数。
- 加速老化换算系数 — 加速老化计算中所用的换算系数。默认换算系数为 2，意外着将以两倍于所配置空闲时间的速率加速老化。将所配置空闲时间除以 2 就能得到比该时间快一半的超时值。为了执行会话加速老化计算，PAN-OS 会将所配置空闲时间（针对此类会话）除以换算系数，以确定更短的超时值。

例如，如果换算系数为 10，则通常在 3600 秒后超时的会话将以快 10 倍速度（该时间的 1/10）超时，即在 360 秒后超时。

STEP 7 | 启用数据包缓冲区保护。


© 2019 Palo Alto Networks, Inc.

1. 选择 **Packet Buffer Protection**（数据包缓冲区保护），使防火墙能够对可能攻陷其数据包缓冲区的会话采取行动，并导致合法流量被丢弃；默认被启用。
2. 如果启用数据包缓冲区保护，可以调整阈值和计时器，以指示防火墙如何响应数据包缓冲区滥用。
   - **Alert (%)**（警报 (%)）：当数据包缓冲区使用率超过此阈值时，防火墙会创建一个日志事件。默认情况下，阈值设置为 50%，范围为 0%-99%。如果该值设置为 0%，则表示防火墙不能创建日志事件。
   - **Activate (%)**（激活 (%)）：当数据包缓冲区使用率超过此阈值时，防火墙会对滥用会话应用随机早期丢弃 (RED)。默认情况下，阈值设置为 80%，范围为 0%-99%。如果该值设置为 0%，则表示防火墙不能应用 RED。

   警报事件记录在系统日志中。已丢弃的流量、已丢弃的会话和已阻止的 *IP* 地址等事件记录在威胁日志中。

   - **Block Hold Time (sec)**（阻止保持时间（秒））：在会话丢弃之前允许 RED 减轻会话持续的时间量。默认情况下，阻止保持时间是 60 秒。范围为 0 - 65,535 秒。如果该值设置为 0，则表示防火墙不能根据数据包缓冲区保护丢弃会话。
   - **Block Duration (sec)**（阻止期限（秒））：此设置定义会话保持丢弃状态或 IP 地址保持阻止状态的时长。默认为 3,600 秒，范围为 0 - 15,999,999 秒。如果此值设置为 0，则表示防火墙不能根据数据包缓冲区保护丢弃会话或阻止 IP 地址。

STEP 8 | 启用多播路由设置数据包的缓存。

1. 选中 **Multicast Route Setup Buffering**（多播路由设置缓存），以使防火墙能在多播路由或转发信息库 (FIB) 尚不存在的情况下，为相应的多播路由组保留多播会话中的第一个数据包。默认情况下，防火墙不会缓存新会话中的第一个多播数据包，而是会使用此数据包来设置多播路由。此为多播通信的预期行为。如果内容服务器可直接连接到防火墙，且自定义应用程序无法承担被丢弃会话中的第一个数据包，则您仅需启用多播路由设置缓存即可解决问题。该选项在默认情况下已禁用。
2. 如果启用了缓存，还可以调节 **Buffer Size**（缓存大小），指定每个流的缓存大小。防火墙可最多缓存 5,000 个数据包。

   您还可以通过配置虚拟路由器上的多播设置（设置虚拟路由器配置中的 *Multicast*（多播）> *Advanced*（高级）选项卡上的 *Multicast Route Age Out Time (sec)*（多播路由年龄超时（秒））），来调整多播路由在会话结束后可在防火墙的路由表中保留的时长（以秒为单位）。

STEP 9 | 保存会话设置。

单击 **OK**（确定）。

STEP 10 | 微调第 3 层接口的最大分段大小 (MSS) 调整大小设置。

1. 选择 **Network**（网络）> **Interfaces**（接口），选择 **Ethernet**（以太网）、 **VLAN** 或 **Loopback**（回环），并且选择第 3 层接口。
2. 选择 **Advanced**（高级）> **Other Info**（其他信息）。
3. 选择 **Adjust TCP MSS**（调整 **TCP MSS**）并输入以下值中的其一或两者：
   - **IPv4 MSS Adjustment Size**（**IPv4 MSS** 调整大小）（范围为 40 - 300 字节，默认为 40 字节）。
   - **IPv6 MSS Adjustment Size**（**IPv4 MSS** 调整大小）（范围为 60 - 300 字节，默认为 60 字节）。
4. 单击 **OK**（确定）。

STEP 11 | 提交更改。

单击 **Commit**（提交）。

STEP 12 | 更改巨型帧配置后，重新启动防火墙。



© 2019 Palo Alto Networks, Inc.

1. 选择**Device**（设备）> **Setup**（设置）> **Operations**（操作）。
2. 单击 **Reboot Device**（重新启动设备）。

# 会话分发策略

会话分发策略定义了 PA-5200 和 PA-7000 系列防火墙如何在防火墙数据平面处理器 (DP) 中分发安全处理（App-ID、Content-ID、URL 筛选、SSL 解密和 IPSec）。每个策略针对特定类型的网络环境和防火墙配置而设计，以确保防火墙以最大效率分发会话。例如，哈希会话分发策略最适合使用大规模源 NAT 的环境。

防火墙上的 DP 数量取决于防火墙型号：

| 防火墙型号 | 数据平面处理器 |
|---|---|
| PA-7000 系列 | 取决于已安装的网络处理卡 (NPC) 的数量。每个 NPC 都有多个数据平面处理器 (DP)，您可以在防火墙中安装多个 NPC。 |
| PA-5220 防火墙 | 1<br>  *PA-5220* 防火墙只有一个 *DP*，所以会话分发策略不起作用。将策略设置为默认值（轮循机制）。 |
| PA-5250 防火墙 | 2 |
| PA-5260 和 PA-5280 防火墙 | 3 |

以下主题提供有关可用的会话分发策略、如何更改活动策略以及如何查看会话分发统计信息的信息。

- 会话分发策略说明
- 更改会话分发策略和查看统计信息

## 会话分发策略说明

下表提供会话分发策略相关的信息，以帮助您确定哪种策略最适合您的环境和防火墙配置。

| 会话分发策略 | 说明 |
|---|---|
| 已修复 | 允许您指定防火墙将用于安全处理的数据平面处理器 (DP)。<br>使用此策略进行调试。 |
| 哈希 | 防火墙根据源地址和目标地址的哈希分发会话。基于哈希的分发通过避免潜在的 IP 地址或端口冲突来提高 NAT 地址资源管理的效率，并减少 NAT 会话设置的延迟。<br>将此策略用于以下环境：将大规模源 NAT 与动态 IP 转换或动态 IP 结合使用，以及使用端口转换或者两者。使用动态 IP 转换时，选择 **`source`** 地址选项。使用动态 IP 和端口转换时，选择 **`destination`** 地址选项。 |
| 入口插槽（PA-7000 系列防火墙默认值） | （仅限 PA-7000 系列防火墙）新会话将分配到同一 NPC 上的 DP，即会话第一个数据包到达的位置。DP 基于会话加载算法做出选择，但在这种情况下，会话仅限于入口 NPC 上的 DP。 |


© 2019 Palo Alto Networks, Inc.

| 会话分发策略 | 说明 |
| --- | --- |
| | 根据流量和网络拓扑，此策略通常会降低流量需要遍历交换结构的几率。<br>如果入口和出口都在相同的 NPC 上，则使用此策略来减少延迟。如果防火墙是混合 NPC（例如 PA-7000 20G 和 PA-7000 20GXM），则该策略可以将增加的容量与相应的 NPC 隔离，有助于隔离 NPC 故障的影响。 |
| 随机 | 防火墙随机选择一个 DP 进行会话处理。 |
| 轮循机制（PA-5200 系列防火墙默认值） | 防火墙根据活动数据平面之间的轮循机制算法选择数据平面处理器，以便在所有数据平面之间共享输入/输出和安全处理功能。<br>在低到中等需求环境中使用此策略，其中简单且可预测的负载均衡算法就已足够。<br>在高需求环境中，我们建议您使用会话加载算法。 |
| 会话加载 | 该策略类似于轮循机制策略，但使用基于加权的算法来确定如何分配会话以实现 DP 之间的平衡。由于会话生命周期的变化，DP 可能并不总是经历相同的负载。例如，如果防火墙具有三个 DP，DP0 的容量为 25%，DP1 为 25%，DP2 为 50%，则新的会话分配将以较低的容量对 DP 进行加权。随着时间的推移，这有助于改善负载均衡。<br>将此策略用于以下环境：在多个 NPC 插槽之间分发会话（如在插槽间聚合接口组中）或拥有非对称转发。如果防火墙是具有不同会话容量的 NPC 的组合（例如 PA-7000 20G 和 PA-7000 20GXM NPC 的组合），也可以使用此策略或入口插槽策略。 |
| 对称哈希 | （运行 PAN-OS 8.0 或更高版本的 PA-5200 系列和 PA-7000 系列防火墙）防火墙通过排序的源和目标 IP 地址的哈希来选择 DP。此策略为服务器到客户端 (s2c) 和客户端到服务器 (c2s) 的流量提供相同的结果（假设防火墙不使用 NAT）。<br>在高需求 IPSec 或 GTP 部署中使用此策略。<br>使用这些协议时，每个方向都被视为单向流，其中流元组不能彼此导出。该策略通过确保将两个方向的流量分配给相同的 DP 来提高性能并减少延迟，从而消除了对 DP 间通信的需要。 |

## 更改会话分发策略和查看统计信息

下表介绍了如何查看和更改活动会话分发策略，并介绍如何查看防火墙中每个数据平面处理器 (DP) 的会话统计信息。

| 任务 | 命令 |
| --- | --- |
| 显示活动会话分发策略。 | 使用 **show session distribution policy** 命令查看活动会话分发策略。<br>下面的输出显示了利用 ingress-slot 分发策略安装四个 NPC（插槽 2、10、11 和 12）的 PA-7080 防火墙。 |



© 2019 Palo Alto Networks, Inc.

| 任务 | 命令 |
| --- | --- |
| | > **show session distribution policy**<br><br>Ownership Distribution Policy: ingress-slot<br><br>Flow Enabled Line Cards: [2, 10, 11, 12]Packet Processing Enabled Line Cards: [2, 10, 11, 12] |
| 更改活动会话分发策略。 | 使用 **set session distribution-policy *<policy>*** 命令更改活动会话分发策略。<br>例如，要选择会话加载策略，请输入以下命令：<br><br>> **set session distribution-policy session-load** |
| 查看会话分发统计信息。 | 使用 **show session distribution statistics** 命令查看防火墙上数据平面处理器 (DP) 和每个活动 DP 上的会话数。<br>以下输出来自 PA-7080 防火墙：<br><br>> **show session distribution statistics**<br>DP Active Dispatched Dispatched/sec<br>----------<br>s1dp0 78698 7829818 1473<br>s1dp1 78775 7831384 1535<br>s3dp0 7796 736639 1488<br>s3dp1 7707 737026 1442<br><br>DP Active column 列出已安装 NPC 上的每个数据平面。前两个字符表示插槽号，最后三个字符表示数据平面数。例如，s1dp0 为安装在插槽 1 中 NPC 上的数据平面 0，s1dp1 为安装在插槽 1 中 NPC 上的数据平面 1。<br><br>Dispatched 列显示了自上次重新启动防火墙以来处理的数据平面的会话总数。<br><br>Dispatched/sec 列表示调度率。如果将 Dispatched 列中的数字相加，则总和为防火墙上的活动会话数。您还可以通过运行 **show session info CLI** 命令查看活动会话的总数。<br><br>*PA-5200 系列防火墙输出看起来类似，但 DP 数取决于型号，且只有一个 NPC 插槽 (s1)。* |

# 阻止 TCP 分离握手会话建立

您可以在区域保护配置文件中配置 TCP 分离握手丢弃，以阻止 TCP 会话的建立，除非该会话使用标准三向握手。此任务假设你为接口分配安全区域，从而防止 TCP 分离握手建立会话。

STEP 1 | 配置区保护配置文件以阻止不使用标准三向握手的 TCP 会话建立会话。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），然后 **Add**（添加）新配置文件（或选择现有配置文件）。
2. 如果要创建新配置文件，请为配置文件输入 **Name**（名称）和 **Description**（说明）（可选）。


© 2019 Palo Alto Networks, Inc.

3. 选择 **Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP Drop**（**TCP** 丢弃）并选择 **Split Handshake**（分离握手）。
4. 单击 **OK**（确定）。

STEP 2 | 将此配置文件应用于一个或多个安全区。

1. 选择 **Network**（网络）> **Zones**（区域），然后选择要将区域保护配置文件分配到的区域。
2. 在区域窗口中，从 **Zone Protection Profile**（区域保护配置文件）列表中选择您在上一步中配置的配置文件。

   或者，您可以在此处单击 **Zone Protection Profile**（区保护配置文件）开始创建新配置文件，这种情况下您可以相应地继续。
3. 单击 **OK**（确定）。
4. （可选）重复步骤 1-3 以将配置文件应用于其他区。

STEP 3 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 隧道内容检测

防火墙可在不终止隧道的情况下对明文隧道协议的流量内容进行检测：

- 通用路由封装 (GRE) (RFC 2784)
- 非加密 IPSec 流量 [IPSec 的 NULL 加密算法 (RFC 2410) 和传输模式 AH IPSec]
- 用户数据 (GTP-U) 的通用分组无线业务 (GPRS) 隧道协议
- 虚拟可扩展局域网 (VXLAN) (RFC 7348)



隧道内容检查用于明文隧道，不适用于携带加密流量的 *VPN* 或 *LSVPN* 隧道。

您可以使用隧道内容检测，对以上类型隧道中的流量和其他明文隧道中嵌套的流量（例如 GRE 隧道中的 Null 加密 IPSec 隧道）执行安全、DoS 保护和 QoS 策略。您可以在 ACC 中查看隧道检测日志和隧道活动，以验证隧道流量是否符合公司的安全和使用策略。

所有防火墙型号均支持 GRE、非加密 IPSec 和 VXLAN 协议的隧道内容检测。仅 支持 GTP 安全的防火墙支持 GTP-U 隧道内容检查—请参阅兼容性矩阵中根据型号支持 GTP 和 SCTP 安全的 PAN-OS 发布版本。

受支持的防火墙默认执行隧道加速，以提高经过 GRE 隧道、VXLAN 隧道和 GTP-U 隧道的流量性能和吞吐量。隧道加速提供的硬件卸载功能可缩短流量查找时间，从而根据内部流量更有效地分发隧道流量。但是，您可以 禁用隧道加速执行故障排除。

- 隧道内容检测概述
- 配置隧道内容检测
- 查看已检测的隧道活动
- 查看日志中的隧道信息
- 基于标记的隧道流量创建自定义报告
- 禁用隧道加速

## 隧道内容检测概述

防火墙可让您在无法首先终止隧道的网络上的任何位置对隧道内容进行检测。只要处于 GRE、非加密 IPSec、GTP-U 或 VXLAN 隧道的路径中，防火墙就可以检测隧道内容。

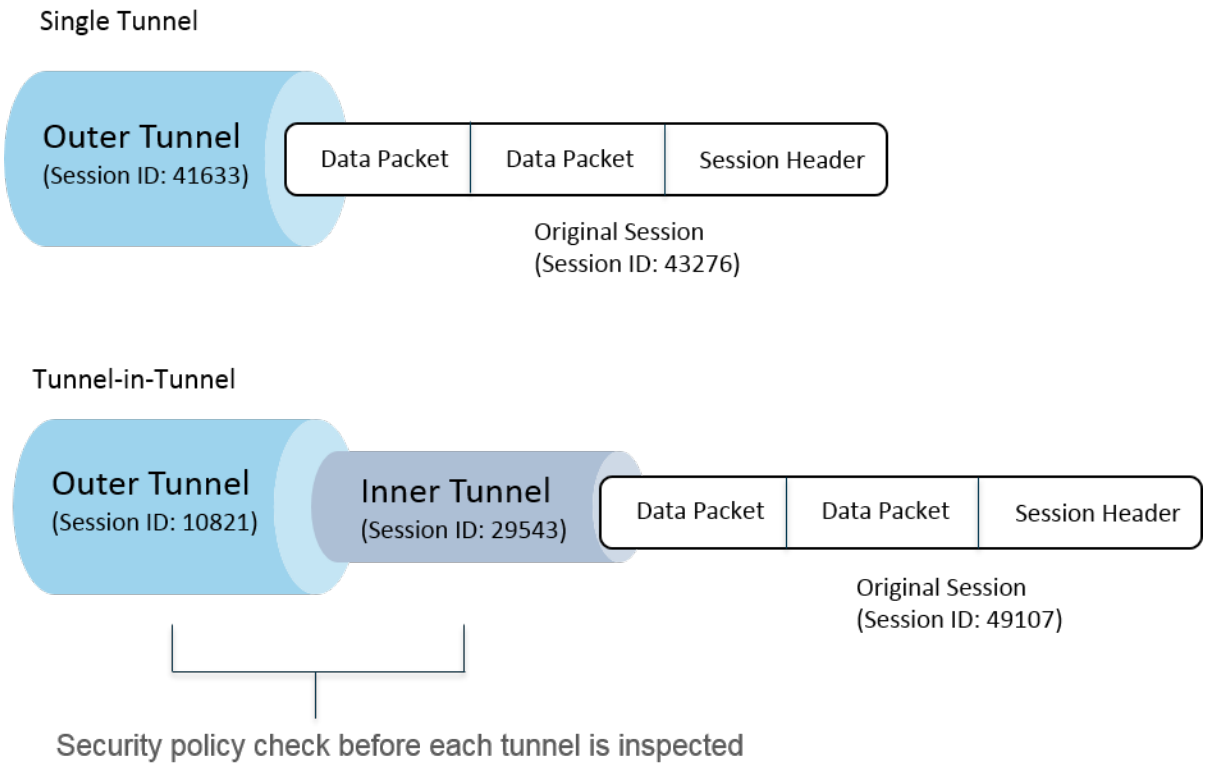
- 希望进行隧道内容检测的企业客户可以使用 GRE、VXLAN 或非加密 IPSec 隧道传输防火墙上的部分或全部流量。出于安全、QoS 和报告的考虑，您可能需要检测隧道内的流量。
- 服务提供商的客户使用 GTP-U 来传输来自移动设备的数据流量。您想在无需终止隧道协议的情况下检测内部内容，并且您想要记录来自用户的用户数据。

防火墙支持对以太网接口、子接口、AE 接口、VLAN 接口以及 VPN 和 LSVPN 隧道接口执行隧道内容检测。（防火墙检测的明文隧道可以位于防火墙终止的 VPN 或 LSVPN 隧道内，因此可以是 VPN 或 LSVPN 隧道接口。换句话说，当防火墙是 VPN 或 LSVPN 端点时，防火墙可以对隧道内容检测支持的任何非加密隧道协议的流量执行检测。）

第 3 层、第 2 层、虚拟线路和旁接部署均支持隧道内容监测。对共享网关和虚拟系统到虚拟系统的通信也可执行隧道内容检测。



© 2019 Palo Alto Networks, Inc.




上图显示，防火墙可以执行两级隧道检测。当已配置隧道检测策略规则的防火墙接收到数据包时：

- 防火墙首先执行安全策略检查，以确定数据包中的隧道协议（应用程序）是被允许还是拒绝。（隧道内协议支持 IPv4 和 IPv6 数据包。）
- 如果安全策略允许该数据包，则防火墙会根据源区域、源地址、源用户、目标区域和目标地址将数据包与隧道检测策略规则进行匹配。隧道检测策略规则确定防火墙检测的隧道协议、允许的最大封装级别（隧道中的单个隧道或隧道）、是否允许包含隧道协议（根据 RFC 2780，不能通过严格的标头检测）的数据包、以及是否允许包含未知协议的数据包。
- 如果数据包通过隧道检测策略规则的匹配条件，则防火墙将根据您的安全策略（必须）和您指定的选项策略检测内部内容。（原始会话支持的策略类型如下表所示）。
- 如果防火墙发现另一个隧道，则防火墙会以递归方式解析第二个标头的数据包，现处于第二级封装，所以与隧道区域匹配的第二个隧道检测策略规则必须允许最高级别的隧道检测（总共两级），以便防火墙继续处理数据包。
    - 如果您的规则允许进行两个级别的检测，防火墙将在此内部隧道执行安全策略检查，然后执行隧道检测策略检查。您在内部隧道中使用的隧道协议可能与您在外部隧道中使用的隧道协议有差别。
    - 如果您的规则不允许进行两个级别的检测，则防火墙基于您是否配置来丢弃具有比您配置的最高级别的隧道检测的封装级别更高的数据包。

默认情况下，封装在隧道中的内容属于与隧道相同的安全区域，并受到保护该区域的安全策略规则的约束。但是，您可以配置隧道区域，使您可以灵活地为内部内容配置与隧道安全策略规则各异的安全策略规则。如果对隧道区域使用不同的隧道检测策略，则必须始终具有最高级别的隧道检测（总共两级），因为根据定义，防火墙正在查看第二级封装。

防火墙不支持与在防火墙上终止的隧道流量相匹配的隧道检测策略规则；防火墙将丢弃与内部隧道会话匹配的数据包。例如，当 IPSec 隧道在防火墙上终止时，请勿创建与您终止的隧道相匹配的隧道检测策略规则。防火墙已对内部隧道流量进行检测，因此不需要隧道检测策略规则。

虽然隧道内容检测在共享网关和虚拟系统到虚拟系统通信上执行，但是您不能将隧道区域分配给共享网关或虚拟系统到虚拟系统通信；它们受到与其所属区域相同的安全策略规则的约束。



© 2019 Palo Alto Networks, Inc.

内部隧道会话和外部隧道会话对防火墙型号的最大会话容量进行计数。

下表用复选标记显示可以应用于外部隧道会话、内部隧道会话和内部原始会话的策略类型：

| 策略类型 | 外部隧道会话 | 内部隧道会话 | 内部原始会话 |
|---|---|---|---|
| App-Override | ✓ 仅限 VXLAN | — | ✓ |
| DoS 保护 | ✓ | ✓ | ✓ |
| NAT | ✓ | — | — |
| 基于策略的转发 (PBF) 和对称返回 | ✓ | — | — |
| QoS | — | — | ✓ |
| 安全（必须） | ✓ | ✓ | ✓ |
| User-ID | ✓ | ✓ | ✓ |
| 区域保护 | ✓ | ✓ | ✓ |

VXLAN 不同于其他协议。防火墙可以使用两组不同的会话密钥中的任一组来为 VXLAN 创建外部隧道会话。

- VXLAN UDP 会话 — 六元组密钥（区域、源 IP、目标 IP、协议、源端口和目标端口）创建 VXLAN UDP 会话。
- VNI 会话 — 包括隧道 ID（VXLAN 网络标识符或 VNI）的五元组密钥，并使用区域、源 IP、目标 IP、协议和隧道 ID (VNI) 创建 VNI 会话。

您可以在 ACC 上查看已检测的隧道活动，或是查看日志中的隧道信息。为了快速查看，请配置监控标记，以便您可以监控隧道活动并根据该标记筛选日志结果。

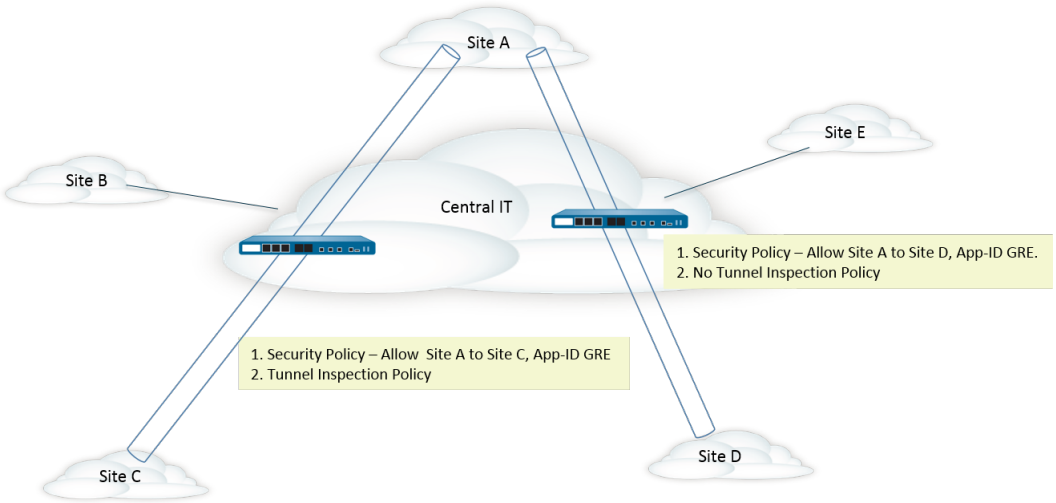
ACC 隧道活动在各种视图中提供数据。对于隧道 ID 使用情况、隧道监控标记和隧道应用使用，**bytes**（字节）、**sessions**（会话）、**threats**（威胁）、**content**（内容）和 **URL** 的数据均来自流量摘要数据库。对于隧道用户、隧道源 IP 和隧道目标 IP 活动，**bytes**（字节）和 **sessions**（会话）的数据来自流量摘要数据库，**threats**（威胁）的数据来自威胁摘要，**URL** 的数据来自 URL 摘要，而 **contents**（内容）的数据来自数据数据库，该数据库是威胁日志的一个子集。

如果在接口上启用 NetFlow，NetFlow 将只捕获外部隧道的统计信息，以避免重复计数（计算外部和外部流的字节）。

有关防火墙型号的隧道检测策略规则和隧道区域容量，请参见产品选择工具。

下图展示的是一家包含多个部门，且使用不同安全策略和隧道检测策略的公司。IT 中心团队提供区域之间的连接。一个隧道将站点 A 连接到站点 C；另一个隧道将站点 A 连接到站点 D。IT 中心团队将防火墙放置在每个隧道的路径中；站点 A 和 C 之间的隧道中的防火墙进行隧道检测；站点 A 和 D 之间的隧道中的防火墙流量非常敏感，因此无隧道检测策略。


© 2019 Palo Alto Networks, Inc.




# 配置隧道内容检测

执行此任务隧道允许的隧道协议配置隧道内容检测。

STEP 1 | 创建安全策略规则，允许数据包通过从源区域到目标区域的隧道使用特定应用程序（如 GRE 应用程序）。

创建安全策略规则

防火墙可以在会话开始或结束时，或开始和结束时均创建隧道检测日志。为安全策略规则指定 *Actions*（操作）时，请为长时间的隧道会话（如 *GRE* 会话）选择 *Log at Session Start*（在会话开始时记录）。

STEP 2 | 创建隧道检测策略规则。

1. 选择 **Policies**（策略）> **Tunnel Inspection**（隧道检测）并 **Add**（添加）策略规则。
2. 在 **General**（常规）选项卡上，输入隧道检测策略规则 **Name**（名称），以字母数字字符开头，并包含零个或多个字母数字、下划线 、连字符 、点 和空格字符。
3. （可选）输入 **Description**（说明）。
4. （可选）指定用于标识受隧道检测策略规则限制的数据包的 **Tag**（标记），以进行报告和日志记录。

STEP 3 | 指定确定隧道检测策略规则应用的数据包源的条件。

1. 选择 **Source**（源）选项卡。
2. 从区域列表中 **Add**（添加）**Source Zone**（源区域）（默认为**Any**（任意））。
3. （可选）**Add**（添加）**Source Address**（源地址）。您可以输入 IPv4 或 IPv6 地址、地址组或 Geo Region 地址对象（**Any**（任意））。
4. （可选）选择 **Negate**（求反）可选择除指定地址以外的任何地址。
5. （可选）**Add**（添加） **Source User**（源用户）（默认为 **any**（任意））。**Known-user**（已知用户）是经过身份验证的用户；**Unknown**（未知用户）未进行身份验证。

STEP 4 | 指定确定隧道检测策略规则应用的数据包目标的条件。

1. 选择 **Destination**（目标）选项卡。
2. 从区域列表中 **Add**（添加）**Destination Zone**（目标区域）（默认为**Any**（任意））。
3. （可选）**Add**（添加）**Destination Address**（目标地址）。您可以输入 IPv4 或 IPv6 地址、地址组或 Geo Region 地址对象（默认为**Any**（任意））。

   您还可以配置新的地址或地址组。



© 2019 Palo Alto Networks, Inc.

4. （可选）选择 **Negate**（求反）可选择除指定地址以外的任何地址。

STEP 5 | 指定防火墙将检测此规则的隧道协议。

1. 选择 **Inspection**（检测）选项卡。
2. **Add**（添加）希望防火墙检测的一个或多个 **Tunnel Protocol**（隧道协议）：
   - **GRE** — 防火墙检测隧道中使用通用路由封装(GRE)的数据包。
   - **GTP-U** — 防火墙检测隧道中使用用户数据 (GTP-U) 的通用分组无线业务 (GPRS) 隧道协议的数据包。
   - **Non-encrypted IPSec**（非加密 **IPSec**）— 防火墙检测隧道中使用非加密 IPSec（空加密 IPSec 或传输模式 AH IPSec）的数据包。
   - **VXLAN** — 防火墙检测用于隧道内虚拟可扩展局域网 (VXLAN) 隧道协议的数据包。

STEP 6 | 指定防火墙检测的封装级别数和防火墙丢弃数据包的条件。

1. 选择 **Inspect Options**（检测选项）。
2. 选择防火墙将检测的 **Maximum Tunnel Inspection Levels**（最大隧道检测级别）：
   - **One Level**（一级）（默认）— 防火墙仅检测外部隧道中的内容。

     对于 VXLAN，防火墙通过检测 VXLAN 有效负载来发现隧道内的封装内容或应用程序。因为仅在外部隧道进行 VXLAN 检测，因此，必须选择 **One Level**（一个级别）。
   - **Two Levels (Tunnel In Tunnel)**（二级（隧道中的隧道））— 防火墙检测外部隧道中的内容和内部隧道中的内容。
3. 选择以下任意、所有或无内容以指定防火墙是否在各种条件下丢弃数据包：
   - **Drop packet if over maximum tunnel inspection level**（如果超过最大隧道检测级别，则丢弃数据包）— 防火墙丢弃包含比 **Maximum Tunnel Inspection Levels**（最大隧道检测级别）配置的封装级别更多的数据包。
   - **Drop packet if tunnel protocol fails strict header check**（如果隧道协议不符合标头严格检测标准，则丢弃数据包）— 防火墙丢弃包含使用与该协议的 RFC 不符的标头的隧道协议的数据包。不符标头可能表示可疑的数据包。此选项可以促使防火墙根据 RFC 2890 验证 GRE 标头。

     如果防火墙正在使用比 RFC 2890 更早版本的 *GRE* 设备进行隧道传输，则不应启用选项 *Drop packet if tunnel protocol fails strict header check*（如果隧道协议不符合标头严格检测标准，则丢弃数据包）。
   - **Drop packet if unknown protocol inside tunnel**（如果隧道内存在未知协议，则丢弃数据包）— 防火墙丢弃隧道内包含的防火墙无法标识的协议的数据包。

     例如，如果选择此选项，则防火墙会丢弃与隧道检测策略规则匹配的加密 IPSec 数据包，因为防火墙无法读取这些数据包。因此，您可以允许 IPSec 数据包，防火墙将只允许加密的 IPSec 和 AH IPSec 数据包。
   - **Return scanned VXLAN tunnel to source**（将扫描的 **VXLAN** 隧道返回到源）— 当流量重定向到（转至）防火墙时，VXLAN 会封装该数据包。流量转向通常发生在公共云环境中。启用 **Return scanned VXLAN tunnel to source**（将扫描的 **VXLAN** 隧道返回到源），从而将封装数据包返回到原始的 VXLAN 隧道端点(VTEP)。此选项仅在第 3 层、第 3 层子接口、第 3 层聚合接口以及 VLAN 上得到支持。
4. 单击 **OK**（确定）。

STEP 7 | 管理隧道检测策略规则。

使用以下方式管理隧道检测策略规则：

- （筛选器字段）-— 仅显示筛选器字段中命名的隧道策略规则。
- **Delete**（删除）— 删除所选的隧道策略规则。
- **Clone**（复制）— **Add**（添加）按钮的替代方法；用新名称复制所选规则，然后可进行修改。


© 2019 Palo Alto Networks, Inc.

- **Enable**（启用）— 启用所选的隧道策略规则。
- **Disable**（禁用）— 禁用所选的隧道策略规则。
- **Move**（移动）— 在列表中上下移动所选的隧道策略规则；根据规则按照从上到下的顺序对数据包进行评估。
- **Highlight Unused Rules**（突出显示未使用的规则— 突出显示自上次重新启动防火墙以来没有数据包匹配的隧道策略规则。

STEP 8 | （可选）为隧道内容创建隧道源区域和隧道目标区域，并为每个区域配置安全策略规则。



最佳实践是为隧道流量创建隧道区域。因此，防火墙为具有相同五元组（源 *IP* 地址和端口、目标 *IP* 地址和端口，以及协议）的隧道和非隧道数据包创建单独的会话。



为 *PA-5200* 系列防火墙上的隧道流量分配隧道区域，使防火墙在软件中进行隧道检测；隧道检测没有被卸载到硬件。

1. 如果要隧道内容受到与不同于外部隧道区域的安全策略规则（先前配置）的安全策略规则的限制，请选择 **Network**（网络）> **Zones**（区域）并 **Add**（添加）隧道源区域的 **Name**（名称）。
2. 对于 **Location**（位置），选择虚拟系统。
3. 对于 **Type**（类型），请选择 **Tunnel**（隧道）。
4. 单击 **OK**（确定）。
5. 重复这些子步骤以创建隧道目标区域。
6. 为隧道源区域配置安全策略规则。

   因为您可能不知道隧道流量的始发者或流量的流向，并且您不想无意中禁用通过隧道的应用程序的流量，因此请将两个隧道区域都指定为 *Source Zone*（源区域），并在安全策略规则中将两个隧道区域都指定为 *Destination Zone*（目标区域），或者为源区域和目标区域选择 *Any*（任何），然后指定 *Applications*（应用程序）。
7. 为隧道目标区域配置安全策略规则。在上一步中配置隧道源区域的安全策略规则的提示也适用于隧道目标区域。

STEP 9 | （可选）为内部内容指定隧道源区域和隧道目标区域。

1. 指定刚刚添加的隧道源区域和隧道目标区域作为内部内容的区域。选择 **Policies**（策略）> **Tunnel Inspection**（隧道检测），在 **General**（常规）选项卡上，选择您创建的隧道检测策略规则的 **Name**（名称）。
2. 选择 **Inspection**（检测）。
3. 选择 **Security Options**（安全选项）。
4. **Enable Security Options**（启用安全选项）（默认禁用）使内部内容来源属于您指定的 **Tunnel Source Zone**（隧道源区域），并使内部内容目标属于您指定的 **Tunnel Destination Zone**（隧道目标区域）。

   如果不 **Enable Security Options**（启用安全选项），则内部内容来源属于与外部隧道来源相同的源区域，且内部内容目标属于与外部隧道目标相同的目标区域。这就意味着它们受到适用于这些外部区域的相同安全策略规则的约束。
5. 对于 **Tunnel Source Zone**（隧道源区域），在上一步骤中创建适当的隧道区域，以便将与该区域相关联的策略应用到隧道源区域。否则，内部内容来源默认使用与外部隧道中相同的源区域，且外部隧道源区域的策略同样适用于内部内容源区域。
6. 对于 **Tunnel Destinatio Zone**（隧道目标区域），在上一步骤中创建适当的隧道区域，以便将与该区域相关联的策略应用到隧道目标区域。否则，内部内容来源默认使用与外部隧道中相同的目标区域，且外部隧道源区域的策略同样适用于内部内容目标区域。

   如果为隧道检测策略规则配置 *Tunnel Source Zone*（隧道源区域）和 *Tunnel Destination Zone*（隧道目标区域），则应配置符合隧道检测策略规则中匹配条件的特定 *Source Zone*（源区域）（在步骤3中）和特定 *Destination Zone*（目标区域）（在



© 2019 Palo Alto Networks, Inc.

步骤4中），而不是指定 *Source Zone*（源区域）为 *Any*（任何），*Destination Zone*（目标区域）为 *Any*（任何）。该提示确保区域重新分配的区域方向正确对应于父区域。

在 *PA-5200* 系列或 *PA-7080* 防火墙上，如果在检测 *VXLAN* 时使用多播底层，则内部会话可在多个数据平面上出现重复，且可能会发生争用现象。为避免丢弃某些数据包，应遵守下列要求：

- 必须配置单独的隧道内容检测规则，以匹配发往每个 *VXLAN* 隧道端点 *(VTEP)* 的外部 *VXLAN* 数据包。
- 在单独规则中，您可以分配隧道区域。使用不同的隧道区域可使用于每个端点的内部会话各不相同。争用现象不会发生，也不会有任何数据包被丢弃。

7. 单击 **OK**（确定）。

STEP 10 | 为与隧道检测策略规则匹配的流量设置监控选项。

1. 选择 **Policies**（策略）> **Tunnel Inspection**（隧道检测），然后选择您创建的隧道检测策略规则。
2. 选择 **Inspection**（检测）> **Monitor Options**（监控选项）。
3. 输入 **Monitor Name**（监控名称），将类似流量分组在一起，以进行日志记录和报告。
4. 输入 **Monitor Tag (number)**（监控标记（编号）），将类似流量分组在一起，以进行日志记录和报告（范围为 1 至 16,777,215）。标记编号是全局定义的。

此字段不适用于 *VXLAN* 协议。*VXLAN* 日志自动使用 *VXLAN* 标头中的 *VNI ID*。

如果标记隧道流量，则可以稍后筛选隧道检测日志中的监控标记，并使用 *ACC* 查看基于监控标记的隧道活动。

5. **Override Security Rule Log Setting**（覆盖安全规则日志设置），以便为符合所选隧道检测策略规则的会话启用日志记录和日志转发选项。如果未选择此设置，则隧道日志生成和日志转发由适用于隧道流量的安全策略规则的日志设置确定。您可以覆盖控制流量日志的安全策略规则中的日志转发设置，具体做法是通过配置隧道检测日志设置来将隧道日志和流量日志分开储存。隧道检测日志储存外部隧道（GRE、非加密 IPSec、VXLAN 或 GTP-U）会话，而流量日志则储存内部流量。
6. 选择 **Log at Session Start**（在会话开始时记录）以在会话开始时记录流量。

因为隧道可以长时间保持运行状态，因此，最佳做法是在会话开始和结束时记录“隧道日志”。例如，*GRE* 隧道可能会在路由器启动时出现，并且直到路由器重新启动才会终止。如果您未能在会话开始时记录，则无法在 *ACC* 中看到活动的 *GRE* 隧道。

7. 选择 **Log at Session End**（在会话结束时记录）以在会话结束时记录流量。
8. 选择 **Log Forwarding**（日志转发）配置文件，以确定防火墙为符合隧道检测规则的会话转发隧道日志的位置。或者，您可以在配置日志转发的情况下创建新的日志转发配置文件。
9. 单击 **OK**（确定）。

STEP 11 | （可选，仅限 VXLAN）配置 **VXLAN ID (VNI)**。默认检测所有 VXLAN 网络接口 (VNI)。如果配置一个或多个 VXLAN ID，则策略仅检测这些 VNI。

在 *VXLAN* 协议上，使用隧道 *ID* 选项卡以指定 *VNI*。

1. 选择 **Tunnel ID**（隧道 **ID**）选项卡，单击 **Add**（添加）。
2. 分配 **Name**（名称）。名称是为了方便起见，不是日志记录、监控或报道的一个因素。
3. 在 **VXLAN ID (VNI)** 字段，输入单个 VNI、以逗号分隔的 VNI 列表、VNI 的范围（用连字符分隔）或这些的组合。例如，您可指定：

```
1677002,1677003,1677011-1677038,1024
```


© 2019 Palo Alto Networks, Inc.

STEP 12 | （可选）如果启用 **Rematch Sessions**（重新匹配会话）（**Device**（设备）> **Setup**（设置）> **Session**（会话）），请确保在创建或修改隧道检测策略时防火墙不会删除现有会话，方法是禁用控制隧道安全策略规则的区域的 **Reject Non-SYN TCP**（拒绝非 **SYN TCP**）。

在以下情况下，防火墙会显示以下警告：

- 创建隧道检测策略规则。
- 通过添加 **Protocol**（协议）或将 **Maximum Tunnel Inspection Levels**（最大隧道检测级别）从 **One Level**（一级）增加至 **Two Levels**（二级）来编辑隧道检测策略规则。
- 通过添加新区域或将一个区域更改为另一个区域，在 **Security Options**（安全选项）选项卡中 **Enable Security Options**（启用安全选项）。



警告:启用现有隧道会话上的隧道检测策略将使隧道内的现有 *TCP* 会话被视为 *non-syn-tcp* 流量。为确保启用隧道检测策略时不会丢弃现有会话，请使用区域保护配置文件将用于区域的 *Reject Non-SYN TCP*（拒绝非 *SYN TCP*）设置设为 *no*（否），并将其应用于控制隧道安全策略的区域。一旦防火墙识别了现有会话，便可以重新启用 *Reject Non-SYN TCP*（拒绝非 *SYN TCP*）设置，方法是将其设置为 *yes*（是）或 *global*（全局）。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），并 **Add**（添加）配置文件。
2. 输入配置文件的 **Name**（名称）。
3. 选择 **Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP Drop**（TCP 丢弃）。
4. 对于 **Reject Non-SYN TCP**（拒绝非 **SYN TCP**），请选择 **no**（否）。
5. 单击 **OK**（确定）。
6. 选择 **Network**（网络）> **Zones**（区域），然后选择控制隧道安全策略规则的区域。
7. 对于 **Zone Protection Profile**（区域保护配置文件），请选择刚创建的区域保护配置文件。
8. 单击 **OK**（确定）。
9. 重复本节中的前三个子步骤（12.f、12.g和12.h），将区域保护配置文件应用于控制隧道安全策略规则的其他区域。
10. 在防火墙识别现有会话后，便可以重新启用 **Reject Non-SYN TCP**（拒绝非 **SYN TCP**）设置，方法是将其设置为 **yes**（是）或 **global**（全局）。

STEP 13 | （可选）限制隧道中流量碎片。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），并按 **Name**（名称）**Add**（添加）配置文件
2. 输入 **Description**（说明）。
3. 选择 **Packet Based Attack Protection**（基于数据包的攻击保护）> **IP Drop**（IP 丢弃）> **Fragmented traffic**（碎片通信）。
4. 单击 **OK**（确定）。
5. 选择 **Network**（网络）> **Zones**（区域），然后选择要限制碎片的隧道区域。
6. 对于 **Zone Protection Profile**（区域保护配置文件），请选择刚创建的配置文件，将区域保护配置文件应用于隧道区域。
7. 单击 **OK**（确定）。

STEP 14 | **Commit**（提交）更改。

## 查看已检测的隧道活动

执行以下任务来查看已检测的隧道活动。

STEP 1 | 选择 **ACC**，并选择 **Virtual System**（虚拟系统）或 **All**（全部）虚拟系统。

STEP 2 | 选择隧道活动。



© 2019 Palo Alto Networks, Inc.

STEP 3 | 选择要查看的时间段，例如“过去 24 小时”或“过去 30 天”。

STEP 4 | 对于全局筛选器，单击 + 或 - 按钮以在隧道活动上使用 ACC 筛选器。

STEP 5 | 查看已检测的隧道活动；可以按照 **bytes**（字节）、**sessions**（会话）、**threats**（威胁）、**content**（内容）或 **URL** 在每个窗口中显示数据，并对数据进行排序。每个窗口以图形和表格形式显示隧道数据的不同方面：

- **Tunnel ID Usage**（隧道 **ID** 使用情况）— 每个隧道协议列出使用该协议的隧道的隧道 ID。表格提供协议的字节、会话、威胁、内容和 URL 的总计。将鼠标悬停在隧道 ID 上即可获得每个隧道 ID 的详细信息。
- **Tunnel Monitor Tag**（隧道监控标记）— 每个隧道协议列出使用该标记的隧道的隧道监控标记。表格提供该标记和协议的字节、会话、威胁、内容和 URL 的总计。将鼠标悬停在隧道监控标记上即可获得每个标记的详细信息。
- **Tunneled Application Usage**（隧道应用程序使用情况）— 应用程序类别以图形方式显示分组到介质、常规兴趣、协作和联网的应用程序类型，并按其风险进行颜色编码。应用程序表还包括每个应用程序的用户数。
- **Tunneled User Activity**（隧道用户活动）— 显示已发送和已接收字节的图形，例如，沿着日期和时间的 x 轴。将鼠标悬停在图上的某个点上即可查看该点处的数据。源用户和目标用户表为每个用户提供数据。
- **Tunneled Source IP Activity**（隧道源 **IP** 活动）— 显示字节、会话和威胁的图形和表格，例如，来自 IP 地址的攻击者。将鼠标悬停在图上的某个点上即可查看该点处的数据。
- **Tunneled Destination IP Activity**（隧道目标 **IP** 活动）— 根据目标 IP 地址显示图形和表格。例如，查看 IP 地址上每个受害者的威胁。将鼠标悬停在图上的某个点上即可查看该点处的数据。

## 查看日志中的隧道信息

您可以查看隧道检测日志，也可以在其他类型的日志中查看隧道检测信息。

**GRE**、非加密 **IPSec** 和 **GTP-U** 协议

- 当存在 TCI 流量规则匹配时，GRE、IPSec 和 GTP-U 协议通过隧道日志类型、匹配的协议以及配置的监控名称和监控标记（数字）而被记录在隧道检查日志中。
- 当不存在 TCI 规则匹配时，所有协议被记录在流量日志中。

**VXLAN** 协议

- 当存在 TCI 流量规则匹配时，VXLAN 协议通过隧道 (VXLAN) 日志类型、配置的监控名称和隧道 ID (VNI) 被记录在隧道检查日志中。

  在内部会话的流量日志中，隧道已检查标记表示一个 VNI 会话。父会话为内部会话创建时活跃的会话，因此 ID 可能与当前会话 ID 不相符。
- 当不存在 TCI 规则匹配时，VNI 会话被记录在带有 UDP 协议、源端口 0 和目标端口 4789（默认）的流量日志中。

- 查看隧道检测日志。
  1. 选择 **Monitor**（监控）> **Logs**（日志）> **Tunnel Inspection**（隧道检测）并查看日志数据以识别您的流量中使用的隧道 **Applications**（应用程序），以及未能通过标头严格检查的任何数量较高的数据包。
  2. 单击“详细日志视图”以查看日志相关的详细信息。

- 查看其他日志以获取隧道检测信息。
  1. 选择 **Monitor**（监视器）> **Logs**（日志）。
  2. 选择 **Traffic**（流量）、**Threat**（威胁）、**URL Filtering**（**URL** 筛选）、**WildFire Submissions**（**WildFire** 提交）、**Data Filtering**（数据筛选）或 **Unified**（统一）。


© 2019 Palo Alto Networks, Inc.

3. 对于日志条目，请单击详细日志视图 。
4. 在标志窗口中，查看是否选中 **Tunnel Inspected**（隧道已检测）标志。隧道已检测标志表示防火墙使用隧道检测策略规则对内部内容或内部隧道进行检测。父会话信息涉及外部隧道（相对于内部隧道）或内部隧道（相对于内部内容）。

   在 **Traffic**（流量）、**Threat**（威胁）、**URL Filtering**（**URL** 筛选）、**WildFire Submissions**（**WildFire** 提交）、**Data Filtering**（数据筛选）日志上，内部会话日志的详细日志视图仅显示直接父信息，不显示隧道日志信息。如果已配置两个级别的隧道检测，则可以选择此直接父级的父级会话以查看第二个父级日志。（必须监控 **Tunnel Inspection**（隧道检测）日志以查看隧道日志信息，如上一步所示。）
5. 如果正在查看已对其执行隧道检测的内部会话日志，请单击常规部分中的 **View Parent Session**（查看父会话）链接以查看外部会话信息。

## 基于标记的隧道流量创建自定义报告

您可以根据应用于隧道流量的标记创建报告以收集信息。

STEP 1 | 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告），然后单击 **Add**（添加）。

STEP 2 | 对于数据库，选择流量、威胁、URL、数据筛选或 WildFire 提交日志。

STEP 3 | 对于可用列，选择标记和监控标记，以及报告中所需的其他数据。

您也可以生成自定义报告。

## 禁用隧道加速

受支持的防火墙默认执行隧道加速，以提高性能和通过 GRE 隧道、VXLAN 隧道和 GTP-U 隧道的流量吞吐量。隧道加速提供的硬件卸载功能可缩短执行流量查找的时间，从而实现根据内部流量更高效地分发隧道流量。

PA-3200 系列防火墙、PA-7000 系列防火墙，以及PA-7000-100G-NPC-A 和 PA-7050-SMC-B 或 PA-7080-SMC-B 均支持 GRE 和 VXLAN 隧道加速。您可以禁用隧道加速以进行故障排除。一旦禁用隧道加速，就会同时禁用 GRE、VXLA 和 GTP-U 隧道。

STEP 1 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。

STEP 2 | 取消选择 **Tunnel Acceleration**（隧道加速）即可将其禁用。

STEP 3 | 单击 **OK**（确定）。

STEP 4 | **Commit**（提交）。

STEP 5 | 重启防火墙。

STEP 6 | （可选）查看隧道加速的状态。

1. 访问 CLI。
2. > **show tunnel-acceleration**

   系统输出 `Enabled`（已启用）或 `Disabled`（已禁用）。其他状态和原因（仅限 GTP-U）：

   - 已禁用— 防火墙型号不支持 GTP-U 隧道加速，或是 GTP 安全已禁用。
   - 错误（`TCL 带意外配置的 GTP-U`））— 启用隧道加速时配置了带 GTP-U 协议的 TCI。
   - 已启用— 隧道加速已启用；GTP-U 隧道加速尚未运行。GTP 安全已启用，但尚未重新启动。
   - 已安装— GTP-U 隧道加速正在运行。

# 策略

通过使用策略，可以强制执行规则并采取行动。在防火墙上可以创建以下不同类型的策略规则：安全、NAT、服务质量 (QoS)、基于策略的转发 (PBF)、解密、应用程序替代、身份验证、拒绝服务 (DoS) 和区域保护策略。所有这些不同的策略共同根据需要来允许、拒绝、优先排列、转发、加密、解密、例外处理、身份验证访问及重置连接，以便为您的网络提供保护。以下主题介绍如何使用策略：

- 策略类型
- 安全策略
- 策略对象
- 安全配置文件
- 跟踪规则库内规则
- 实施策略规则描述、标记和审核注释
- 将策略规则或对象移动或克隆到不同的虚拟系统
- 使用地址对象表示 IP 地址
- 使用标记分组并以可视方式区分对象
- 在策略中使用外部动态列表
- 动态注册 IP 地址和标记
- 在策略中使用动态用户组
- 使用自动标记实现安全操作自动化
- 监控虚拟环境中的变化
- 动态 IP 地址和标记的 CLI 命令
- 识别通过代理服务器连接的用户
- 基于策略的转发
- 测试策略规则

# 策略类型

Palo Alto Networks 下一代防火墙支持联合作用的各种策略类型，以安全地在您的网络上启用应用程序。

对于所有策略类型，当您 实施策略规则描述、标记和审核注释时，您可以使用审计注释存档以查看策略规则是如何随时间变化的。包含审计注释历史记录和配置日志的存档，让您可以比对配置版本并查看创建人、修改人以及创建和修改的理由。

| 策略类型 | 说明 |
| --- | --- |
| 安全 | 根据通信属性（例如源和目标安全区域、源和目标 IP 地址、应用程序、用户和服务）确定是阻止还是允许某个会话。有关更多详细信息，请参阅安全策略。 |
| NAT | 告知防火墙哪些数据包需要转换以及如何进行转换。防火墙支持源地址和/或端口转换与目标地址和/或端口转换。有关更多详细信息，请参阅 NAT。 |
| QoS | 使用一个或多个定义的参数识别需要 QoS 处理的流量（优先处理或带宽限制），并为其分配类。有关更多详细信息，请参阅服务质量。 |
| 基于策略的转发 | 确定所使用的传出接口应当不同于通常根据路由表使用的传出接口的流量。有关更多详细信息，请参阅基于策略的转发。 |
| 解密 | 确定您要检查可见性、控制和细化安全性的加密流量。有关更多详细信息，请参阅解密。 |
| 应用程序替代 | 确定您不希望 App-ID 引擎处理的会话，该会话为第七层检查。匹配应用程序替代策略的流量强制防火墙将会话作为第 4 层的常规状态检测防火墙处理。有关更多详细信息，请参阅管理自定义或未知应用程序。 |
| 身份验证 | 确定需要用户进行身份验证的流量。有关更多详细信息，请参阅身份验证策略。 |
| DoS 保护 | 确定潜在拒绝服务 (DoS) 攻击并针对规则匹配采取保护措施。有关更多详细信息，请参阅DoS 保护配置文件。 |



© 2019 Palo Alto Networks, Inc.

# 安全策略

安全策略可以防止网络资产遭受威胁和破坏，而且有助于优化网络资源分配，从而提高业务流程的生产力和效率。在 Palo Alto Networks 防火墙上，各个安全策略规则根据通信属性（例如源和目标安全区域、源和目标 IP 地址、应用程序、用户和服务）确定是阻止还是允许某个会话。



要确保最终用户在尝试访问您的网络资源时接受身份验证，防火墙需要在评估安全策略之前先评估身份验证策略。

通过防火墙的所有流量与会话匹配，每个会话与安全策略规则匹配。发生会话匹配时，防火墙在该会话中将匹配安全策略规则应用至双向流量（客户端至服务器和服务器至客户端）。对于与任何预定义的规则不匹配的流量，将应用默认规则。在安全规则库底部显示的默认规则是预定义的规则，用于允许所有区域内（在区域内部）流量和拒绝所有区域间（在区域之间）流量。虽然这些规则是预定义配置的一部分且默认为只读，但您可以覆盖它们并更改有限数量的设置，包括标记、操作（允许或阻止）、日志设置和安全配置文件。

从左至右以及从上到下对安全策略规则进行全面评估。将数据包与满足定义条件的第一个规则相匹配；触发匹配后，将不评估后面的规则。因此，较具体的规则必须放在较通用的规则前面，以实施最佳匹配条件。在会话结束时，与某个规则匹配的通信将在通信日志中生成日志条目（如果已启用此规则的日志记录）。每个规则的日志记录选项都是可配置的，例如，配置为在会话开始时进行记录，取代（或同时）在会话结束时记录。

在管理员配置规则后，您可以查看策略规则使用情况，以确定流量与安全策略规则匹配的时间和次数，从而确定其有效性。随着规则库的发展，更改和审计信息将会随时间丢失，除非在此规则创建或修改的时候对此信息进行存档。您可以 实施策略规则描述、标记和审核注释 以确保所有管理员输入审计注释，以便您查看审计注释存档、检查注释和配置日志记录，以及对所选规则进行规则配置版本的比较。您现在可以更进一步的查看和控制规则库。

- 安全策略的组件规则
- 安全策略操作
- 创建安全策略规则

## 安全策略的组件规则

安全策略规则构造允许组合必填和可选字段，如以下表格中所详述：

| 必填/可选 | 字段 | 说明 |
|---|---|---|
| 必需 | 姓名 | 用来标识规则的标签，最多 63 个字符。 |
| | **UUID** | 通用唯一标识符 (UUID) 是一个由 32 个字符组成的独特字符串，可永久标识规则，以便无论规则发生任何更改（例如，名称），都可以进行跟踪。 |
| | 规则类型: | 指定将规则应用于区域内部、区域之间还是两者的流量：<br>• 通用（默认）- 将规则应用于指定源和目标区域中的所有匹配区域间和区域内流量。例如，如果您使用源区域 A 和 B 及目标区域 A 和 B 创建通用规则，则该规则将适用于区域 A 内部的所有流量、区域 B 内部的所有流量、从区域 A 至区域 B 以及从区域 B 至区域 A 的所有流量。<br>• 区域内 — 将规则应用于指定源区域内部的所有匹配流量（您不能为区域内规则指定目标区域）。例如，如果您将源区域设置为 A 和 B，则规则将适用于区域 A 和区域 B 内部的所有流量，但不适用于区域 A 和 B 之间的流量。 |



© 2019 Palo Alto Networks, Inc.

| 必填/可选 | 字段 | 说明 |
| --- | --- | --- |
| | | • 区域间 — 将规则应用于指定源区域和目标区域之间的所有匹配流量。例如，如果您将源区域设置为 A、B 和 C，并将目标区域设置为 A 和 B，则该规则将适用于从区域 A 至区域 B、从区域 B 至区域 A、从区域 C 至区域 A 以及从区域 C 至区域 B 的流量，但不适用于区域 A、B 或 C 内部的流量。 |
| | **Source Zone**（源区域） | 发起通信的区域。 |
| | 目标区域 | 通信终止的区域。如果使用 NAT，请确保始终引用 NAT 后区域。 |
| | 应用程序 | 您要控制的应用程序。防火墙使用 App-ID（通信分类技术）识别网络上的通信。在创建阻止未知应用程序的安全策略，以及在启用、检查和塑造允许的安全策略时，App-ID 提供应用程序控制和可见性。 |
| | 操作 | 根据您在规则中定义的条件，为通信指定允许或拒绝操作。如果您将防火墙配置为拒绝通信，它将重新设置连接，或者静默地丢弃数据包。为了提供更好的用户体验，您可以不采用静默丢弃数据包的方式，而通过配置细化选项来拒绝流量，这将导致一些应用程序中断并表现为对用户停止响应。有关更多详细信息，请参阅安全策略操作。 |
| 可选 | 标记 | 可让您筛选安全规则的关键字或短语。如果已经定义了许多规则，随后想要查看这些使用特定关键字（如 *IT* 限制应用程序或高风险应用程序）标记的规则，则会很方便。 |
| | 说明 | 一个最多支持 1024 个字符的文本字段，用于描述规则。 |
| | **Source Address**（源地址） | 定义主机 IP 地址、子网、（类型 IP 子网掩码、IP 范围、FQDN 或 IP 通配符掩码的）地址对象、地址组或基于国家/地区的实施。如果您使用 NAT，请确保始终引用数据包中的原始 IP 地址（即 NAT 前 IP 地址）。 |
| | 目标地址 | 数据包的位置或目标。定义 IP 地址、子网、（类型 IP 子网掩码、IP 范围、FQDN、或 IP 通配符掩码的）地址对象、地址组或基于国家/地区的实施。如果您使用 NAT，请确保始终引用数据包中的原始 IP 地址（即 NAT 前 IP 地址）。 |
| | 用户 | 策略所应用到的用户或用户组。您必须在区域中启用 User-ID。若要启用 User-ID，请参阅 User-ID 概述。 |
| | **URL** 类别 | 利用 URL 类别作为匹配条件，可以根据每种 URL 类别自定义安全配置文件（防病毒威胁、防间谍软件、漏洞保护、文件传送阻止、数据筛选和 DoS）。例如，可以对高风险 URL 类别阻止 .exe 文件下载/上载，但是对其他类别则允许。启用此功能后，还可以将计划附加到特定 URL 类别（午餐期间及之后时段内使用社交媒体网站），使用 QoS（金融、医疗和商业）来标记特定 URL 类别，以及根据每种 URL 类别选择不同的日志转发配置文件。<br>尽管可以在防火墙上手动配置 URL 类别，但若要利用 Palo Alto Networks 防火墙上可用的动态 URL 类别更新，则必须购买 URL 过滤许可证。<br>要根据 *URL* 类别阻止或允许流量，必须对安全策略规则应用 *URL* 筛选配置文件。将 *URL* 类别定义为“任意”，然后将 *URL* |



© 2019 Palo Alto Networks, Inc.

| 必填/可选 | 字段 | 说明 |
| --- | --- | --- |
| | | 筛选配置文件附加到安全策略。有关在安全策略中使用默认配置文件的信息，请参阅设置基本安全策略。 |
| | 服务 | 可让您为应用程序选择第 4 层（TCP 或 UDP）端口。可以选择任意、指定端口，或使用应用程序-默认，来启用应用程序的标准端口。例如，对于使用众所周知的端口号的应用程序（如 DNS），应用程序-默认 选项将只与 TCP 端口 53 上的 DNS 通信相匹配。您也可以添加定制应用程序并定义应用程序可以使用的端口。<br>  对于入站规则（例如，从不可信区域到可信区域），使用“应用程序-默认”选项来阻止应用程序在异常端口及协议上运行。应用程序-默认是一个默认选项；使用此配置，即使防火墙仍会检查在所有端口上运行的所有应用程序，但只允许在其标准端口/协议上运行应用程序。 |
| | 安全配置文件 | 提供其他防范威胁、漏洞和数据泄露的保护措施。仅针对具有允许操作的规则评估安全配置文件。 |
| | **HIP Profile**（**HIP** 配置文件）（适用于 GlobalProtect） | 可让您识别具有主机信息配置文件 (HIP) 的客户端，然后实施访问权限。 |
| | 选项 | 可让您定义会话的日志记录、日志转发设置，更改与规则匹配的数据包的服务质量 (QoS) 标记，以及计划安全规则的生效时间（日期和时间）。 |

## 安全策略操作

对于与安全策略内定义的属性匹配的流量，您可以应用以下操作：

| 操作 | 说明 |
| --- | --- |
| **Allow**（允许）（默认） | 允许流量。 |
| **Deny**（拒绝） | 阻止流量，并强制执行为被拒应用程序定义的默认拒绝操作。要查看为应用程序默认定义的拒绝操作，请通过 **Objects**（对象）> **Applications**（应用程序）查看应用程序详细信息，或者在 Applipedia 中查看应用程序详细信息。 |
| **Drop**（丢弃） | 静默丢弃流量；对于应用程序，会覆盖默认拒绝操作。TCP 重置消息未发送到主机/应用程序。<br>对于第 3 层接口，要选择性地向客户端发送 ICMP 无法访问响应，请设置以下操作：**Drop**（丢弃）并启用 **Send ICMP Unreachable**（发送 **ICMP** 无法访问）复选框。启用此复选框时，防火墙将发送 ICMP 代码 *communication with the destination is administratively prohibited*—ICMPv4：类型 3、代码 13、ICMPv6：类型 1、代码 1。 |


© 2019 Palo Alto Networks, Inc.

| 操作 | 说明 |
| --- | --- |
| **Reset client**（重置客户端） | 向客户端设备发送 TCP 重置消息。 |
| **Reset server**（重置服务器） | 向服务器端设备发送 TCP 重置消息。 |
| **Reset both**（重置二者） | 向客户端和服务器端设备发送 TCP 重置消息。 |

只会在会话形成后发送重置消息。如果会话在 *3* 向握手完成前被阻止，防火墙将不会发送重置消息。

对于带有重置操作的 TCP 会话，防火墙不会发送 ICMP 无法访问响应。

对于带有丢弃或重置操作的 UDP 会话，如果选中 **ICMP Unreachable**（**ICMP** 不可访问）复选框，防火墙会向客户端发送 ICMP 消息。

## 创建安全策略规则

STEP 1 | （可选）删除默认安全策略规则。

默认情况下，防火墙包含一个名为 *rule1* 的安全规则，它允许从 Trust 区域到 Untrust 区域的所有通信。您可以删除该规则，或修改该规则以反映您的区域命名约定。

STEP 2 | 添加规则。

1. 选择 **Policies**（策略）> **Security**（安全），然后 **Add**（添加）新规则。
2. 在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称）。
3. 选择 **Rule Type**（规则类型）。

STEP 3 | 为数据包中的源字段定义匹配条件。

1. 在 **Source**（源）选项卡中，选择 **Source Zone**（源区域）。
2. 指定 **Source IP Address**（源 **IP** 地址）或将此值的设置保留为 **any**（任何）。

   如果您决定将某个区域作为 *Source Address*（源地址）*Negate*（求反），确保所有包含私有 *IP* 地址的区域都已添加到 *Source Address*（源地址）中，从而避免私有 *IP* 地址之间的连接丢失。
3. 指定源 **User**（名称）或将此值的设置保留为 **any**（任何）。

STEP 4 | 为数据包中的目标字段定义匹配条件。

1. 在 **Destination**（目标）选项卡中设置 **Destination Zone**（目标区域）。
2. 指定 **Destination IP Address**（目标 **IP** 地址）或将此值的设置保留为 **any**（任何）。

   如果您决定将某个区域作为 *Destination Address*（目标地址）*Negate*（求反），确保所有包含私有 *IP* 地址的区域都已添加到 *Destination Address*（目标地址）中，从而避免私有 *IP* 地址之间的连接丢失。

   最佳实践是，使用地址对象作为 *Destination Address*（目标地址），以便仅能够访问特定服务器或服务器组，尤其是对于 *DNS* 和 *SMTP* 等经常被利用的服务。通过仅限用户



© 2019 Palo Alto Networks, Inc.

访问特定目标服务器地址，您可以防止数据泄露以及通过 *DNS* 隧道等技术建立通信的命令和控制流量。

STEP 5 | 指定规则将允许或阻止的应用程序。



最佳实践是，始终使用基于应用程序的安全策略规则而不是基于端口的规则，并始终将“*Service*（服务）”设置为“*application-default*（应用程序-默认）”，除非您要为应用程序使用比标准端口更为严格的端口列表。

1. 在 **Applications**（应用程序）选项卡中，**Add**（添加）想要安全启用的 **Application**（应用程序）。您可以选择多个应用程序，或者使用应用程序组或应用程序筛选程序。
2. 在 **Service/URL Category**（服务/**URL** 类别）选项卡中，将服务保留设置为 **application-default**（应用程序-默认）以确保规则允许的任何应用程序仅允许在其标准端口上运行。

STEP 6 | （可选）将 URL 类别指定为规则匹配条件。

在 **Service/URL Category**（服务/**URL** 类别）选项卡中，选择 **URL Category**（**URL** 类别）。

如果您选择了一个 URL 类别，将只有 Web 流量匹配规则，并且只有流量到特定类目。

STEP 7 | 指定防火墙要对匹配规则的流量执行何种操作。

在**Actions**（操作）选项卡中，选择**Action**（操作）。有关各个操作的说明，请参阅安全策略操作。

STEP 8 | 配置日志设置。

- 默认情况下，规则将设置为 **Log at Session End**（在会话结束时记录）。如果您不需要在流量匹配此规则时生成任何日志，您可以禁用此设置，或者选择 **Log at Session Start**（在会话开始时记录）以获得更详细的日志记录。
- 选择 **Log Forwarding**（日志转发）配置文件。



最佳做法是，请不要选中 *Disable Server Response Inspection*（禁用服务器响应检查）*(DSRI)* 复选框。选择此选项将阻止防火墙检查从服务器到客户端的数据包。防火墙必须检查客户端到服务器流和服务器到客户端流，以检测和防止威胁，从而获取最佳安全状态。

STEP 9 | 附加安全配置文件以使防火墙能够扫描所有允许的流量是否带有威胁。



必须创建最佳实践安全配置文件，以帮助保护您的网络免受已知和未知威胁的侵害。

在 **Actions**（操作）选项卡中，从 **Profile Type**（配置文件类型）下拉列表中选择 **Profiles**（配置文件），然后选择要附加到规则的各个安全配置文件。

或者，从 **Profile Type**（配置文件类型）下拉列表中选择 **Group**（组），然后选择要附加的安全 **Group Profile**（组配置文件）。

STEP 10 | 单击 **Commit**（提交）以将策略规则保存到防火墙上正在运行的配置中。

STEP 11 | 为了验证是否已有效设置基本策略，请测试是否正在评估安全策略规则，并确定哪项安全策略规则适用于通信流。

输出将显示与 CLI 命令中指定的源和目标 IP 地址相匹配的最佳规则。

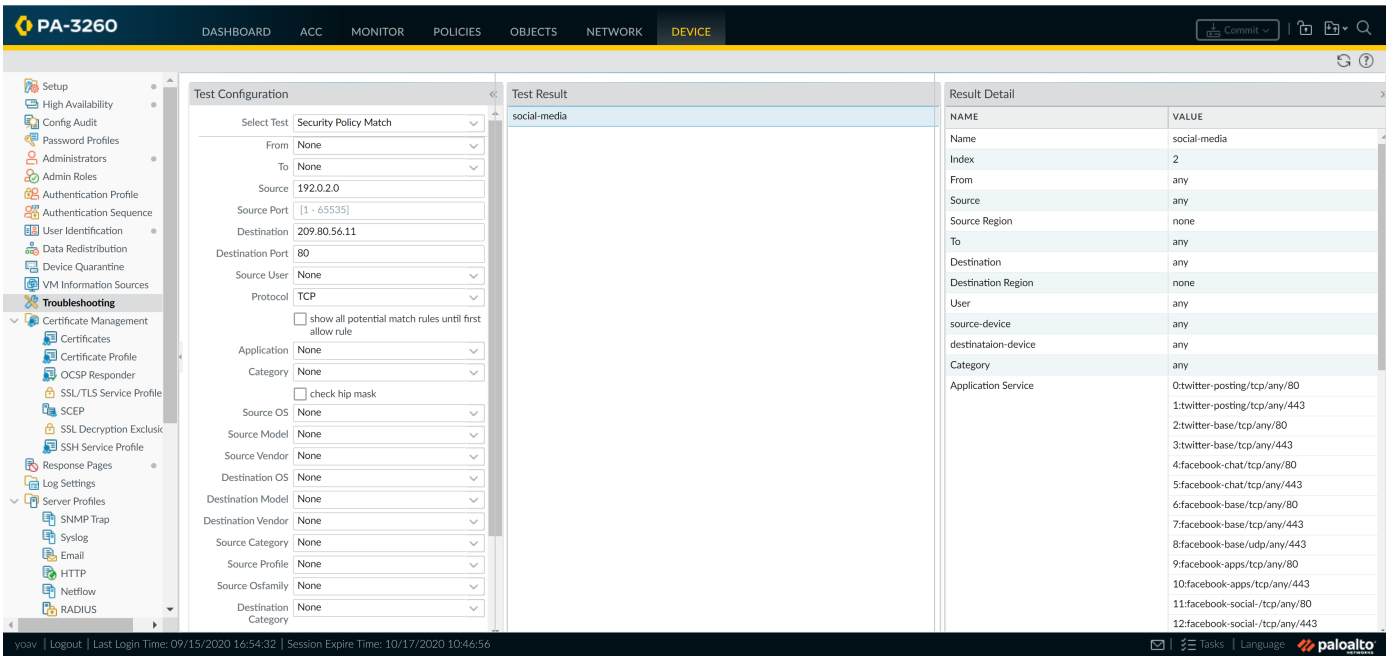
例如，若要验证数据中心中具有 IP 地址 208.90.56.11 的服务器访问 Microsoft 更新服务器时将应用的策略规则：

1. 选择 **Device**（设备）> **Troubleshooting**（故障排除），并从选择测试下拉列表中选择 **Security Policy Match**（安全策略匹配）。



© 2019 Palo Alto Networks, Inc.

2. 输入源和目标 IP 地址。
3. 输入协议。
4. **Execute**（执行）安全策略匹配测试。




STEP 12 | 在等待足够长时间允许流量通过防火墙后，查看策略规则使用情况以监控策略规则的使用状态，并确定策略规则的有效性。



© 2019 Palo Alto Networks, Inc.

# 策略对象

策略对象是将离散的个体标识（如 IP 地址、URL、应用程序或用户）集合在一起的单个对象或集合单元。有了集合单元形式的策略对象，您就可以在安全策略中引用该对象，而无需一次一个地手动选择多个对象。一般来说，在创建策略对象时，会将策略中需要相似权限的对象分为一组。例如，如果您的组织使用一组服务器 IP 地址对用户进行身份验证，则可将这组服务器 IP 地址分组为地址组策略对象，并在安全策略中引用此地址组。通过分组对象，可以显著降低创建策略所需的管理开销。



如果需要导出配置的特定部分以进行内部审查或审核，则可以以 *PDF* 或 *CSV* 文件格式导出配置表格数据。

您可以在防火墙上创建以下策略对象：

| 策略对象 | 说明 |
| --- | --- |
| 地址/地址组、地区 | 允许您将具有相同策略实施要求的特定源或目标地址分为一组。地址对象可以包括 IPv4 或 IPv6 地址（单个 IP、范围、子网）、IP 通配符地址（IPv4 地址/通配符掩码）或 FQDN。另外，可以使用经纬度坐标定义某个地区，也可以选择国家/地区并定义 IP 地址或 IP 范围。然后，可以对地址对象集合进行分组，以创建地址组对象。<br>您也可以使用动态地址组来动态更新主机 IP 地址频繁变更环境中的 IP 地址。<br>  <br>防火墙上预定义的外埠动态列表 *(EDLs)* 可记录防火墙型号支持的地址对象最大数量。 |
| 用户/用户组 | 允许您根据本地数据库、外部数据库或匹配条件创建用户列表，然后对它们进行分组。 |
| 应用程序组和应用程序筛选器 | 应用程序筛选器允许您动态筛选应用程序。通过应用程序筛选器，可以使用在防火墙的应用程序数据库中定义的属性筛选和保存一组应用程序。例如，您可以通过一个或多个属性来创建应用程序筛选器 — 类别、子类别、技术、风险、特征。利用应用程序筛选器，当出现内容更新时，任何与您的筛选器条件匹配的新应用程序都将自动添加到您已保存的应用程序筛选器。<br>如果您想为一组用户或者一项特定的服务，或为了达到特定的策略目标将特定的应用程序进行分组，应用程序组允许您为它们创建特定应用程序统计组。请参阅创建应用程序组。 |
| 服务/服务组 | 允许您指定服务可以使用的源和目标端口以及协议。该防火墙包括两个预定义服务，service-http 和 service-https，HTTP 使用 TCP 端口 80 和 8080，HTTPS 使用 TCP 端口 443。但是，您可以在自己选择的任何 TCP/UDP 端口上创建任何自定义服务，以便将应用程序的使用限制到网络上的特定端口（也就是说，可以为应用程序定义默认端口）。<br>  <br>若要查看某个应用程序使用的标准端口，请在 *Objects*（对象）> *Applications*（应用程序）中搜索该应用程序，然后单击链接。随即会显示简单的描述。 |



© 2019 Palo Alto Networks, Inc.

# 安全配置文件

通过安全策略规则，您可以允许或者阻止网络上的流量，安全配置文件将帮助您定义允许但扫描规则，该规则将扫描被允许的应用程序是否带有诸如病毒、恶意软件、间谍软件和 DDOS 攻击等威胁。当通信与安全策略中定义的允许规则相匹配时，将应用附加到此规则的安全配置文件以作为进一步内容检查的规则，如抗病毒检查和数据筛选。



安全配置文件不在通信流的匹配条件中使用，而是用于在安全策略允许应用程序或类别后对通信进行扫描。

本防火墙为您提供了默认安全配置文件，可以直接即用，开始保护您的网络免受威胁。有关在安全策略中使用默认配置文件的信息，请参阅设置基本安全策略。随着您对网络上安全需求更加深入的了解，要了解如何创建自定义配置文件，请参阅创建最佳实践之互联网网关安全配置文件。



有关安全配置文件的最佳实践设置的建议，请参阅创建最佳实践之互联网网关安全配置文件。

您可添加通常一起应用至创建安全配置文件组的安全配置文件；该组配置文件可作为一个单元处理并通过一个步骤添加至安全策略（或者在您选择设置默认安全配置文件组时默认包含在安全策略中）。

| 配置文件类型 | 说明 |
| --- | --- |
| 防病毒配置文件 | 抗病毒配置文件可防御病毒、蠕虫和特洛伊木马以及间谍软件下载。使用基于流的防恶意软件引擎（从收到第一个数据包时开始检查通信），Palo Alto Networks 抗病毒解决方案可以在不显著影响防火墙性能的前提下为客户端提供保护。此配置文件可以扫描可执行文件、PDF 文件中的各种恶意软件，还可以扫描 HTML 和 JavaScript 病毒，包括对压缩文件和数据编码方案的内部扫描支持。如果您已在防火墙上启用解密，配置文件也会启用解密内容的扫描。<br><br>默认配置文件将检查列出的所有协议解码器中有无病毒，对 SMTP、IMAP 和 POP3 协议生成警报，而阻止 FTP、HTTP 和 SMB 协议。您可以为解码器或者抗病毒签名配置操作，并规定防火墙应该如何响应威胁事件：<br>• **Default**（默认）— 对每一个 Palo Alto Networks 定义的威胁签名和抗病毒签名，设定内部默认操作。典型的默认操作是警报，或者警报的同时重置。默认操作显示在括号内，例如，遇到威胁或者抗病毒签名时默认（警报）。<br>• **Allow**（允许）— 允许应用程序通信。<br><br>*Allow*（允许）操作不会生成与签名或配置文件相关的日志。<br><br>• **Alert**（警报）— 为每个应用程序通信流生成警报。警报保存在威胁日志中。<br>• **Drop**（丢弃）— 丢弃应用程序通信。<br>• **Reset Client**（重置客户端）— 对 TCP 来说，重置客户端一侧的连接。对 UDP 来说，删除连接。<br>• **Reset Server**（重置服务器）— 对 TCP 来说，重置服务器一侧的连接。对 UDP 来说，删除连接。<br>• **Reset Both**（重置两者）— 对 TCP 来说，重置服务器和服务器两端的连接。对 UDP 来说，删除连接。<br><br>自定义配置文件可以用于对受信安全区域之间的流量执行最低限度的防病毒检查，并对从非受信区域（如 Internet）接收到的流量以及发送到高敏感目标（如服务器场）的流量执行最大限度的检查。 |



© 2019 Palo Alto Networks, Inc.

| 配置文件类型 | 说明 |
| --- | --- |
| | Palo Alto Networks WildFire 系统还提供更具逃避性的持续性威胁和其他抗病毒解决方案可能尚未发现的威胁签名。在 WildFire 发现威胁时，将快速创建签名，然后将其集成到“威胁阻止”订户可每日下载（WildFire 订户不到一小时即可下载）的标准防病毒签名中。 |
| 防间谍软件配置文件 | 防间谍软件配置文件阻止受影响的主机上的间谍软件尝试回拨或向外部命令与控制 (C2) 服务器发送信号，让您可以检测受感染客户端上离开网络的恶意流量。您可以在区域之间应用各种级别的保护。例如，您可能需要设立一个自定义防间谍软件配置文件，最大限度地减少可信区域之间的检查，而最大限度地增加对来自不可信区域（例如面向 Internet 的区域）的通信的检查。当防火墙由 Panorama 管理服务器管理时，ThreatID 将映射到防火墙上相应的自定义威胁，使防火墙生成已填充有自定义 ThreatID 的威胁日志。<br><br>您可定义自己的自定义防间谍软件配置文件，或者在向安全策略规则应用防间谍软件时选择以下预定义配置文件之一：<br><br>• **Default**（默认）— 按照创建签名时 Palo Alto Networks 指定的设置，对每个签名使用默认操作。<br>• **Strict**（严格）— 替代关键、高和中等严重性威胁的默认操作以阻止操作，而不管签名文件中定义的操作如何。该配置文件仍然使用低等和信息性严重程度签名的默认操作。<br><br>当防火墙检测到威胁事件时，您可以在防间谍软件配置文件中配置以下操作：<br><br>• **Default**（默认）— 对每一个 Palo Alto Networks 定义的威胁签名和防间谍软件签名，设定内部默认操作。通常默认操作是发出警报，或者同时进行重置。默认操作显示在括号内，例如，遇到威胁或者抗病毒签名时默认（警报）。<br>• **Allow**（允许）— 允许应用程序流量。<br><br>*Allow*（允许）操作不会生成与签名或配置文件相关的日志。<br><br>• **Alert**（警报）— 为每个应用程序通信流生成警报。警报保存在威胁日志中。<br>• **Drop**（丢弃）— 丢弃应用程序通信。<br>• **Reset Client**（重置客户端）— 对 TCP 来说，重置客户端一侧的连接。对 UDP 来说，删除连接。<br>• **Reset Server**（重置服务器）— 对 TCP 来说，重置服务器一侧的连接。对 UDP 来说，删除连接。<br>• **Reset Both**（重置两者）— 对 TCP 来说，重置服务器和服务器两端的连接。对 UDP 来说，删除连接。<br><br>在某些情况下，当配置文件操作设置为 *reset-both*（重置两者）时，相关联的威胁日志可能会显示操作为 *reset-server*（重置服务器）。当防火墙在会话开始时检测到威胁，并通过 *503* 阻止页面向客户显示时，会发生这种情况。因为阻止页面不允许连接，因此，不需要重置客户端侧，仅重置服务器侧连接。<br><br>• **Block IP**（阻止 **IP**）— 不管流量来自源还是源-目标对，都将被该操作阻止。可以在规定的时段内对其进行配置。<br><br>此外，可以在防间谍软件配置文件中启用 DNS Sinkholing 操作，让防火墙对已知恶意域名的 DNS 查询伪造响应，从而致使将恶意域名解析为定义的 IP 地址。此功能有助于使用 DNS 流量识别受保护网络上的受感染主机。然后，可以在流量和威胁日志中轻易地识别受感染的主机，因为试图连接到 Sinkhole IP 地址的任何主机最有可能被恶意软件感染。 |


© 2019 Palo Alto Networks, Inc.

| 配置文件类型 | 说明 |
| --- | --- |
| | 防间谍软件配置文件与漏洞保护配置文件的配置方法类似。 |
| 漏洞保护配置文件 | 漏洞防护配置文件阻止试图利用系统缺陷或者获得未授权的系统访问。防间谍配置文件有助于在流量离开网络时确定受感染主机，而漏洞保护配置文件有助于防止威胁进入网络。例如，漏洞保护配置文件可以防御缓冲区溢出、非法代码执行及其他尝试利用系统漏洞的行为。默认漏洞保护配置文件保护客户端和服务器免受所有已知的关键、高和中等严重性威胁。还可以创建例外，以便允许更改对特定签名的响应。当防火墙由 Panorama 管理服务器管理时，ThreatID 将映射到防火墙上相应的自定义威胁，使防火墙生成已填充有自定义 ThreatID 的威胁日志。<br><br>当防火墙检测到威胁事件时，您可以在防间谍软件配置文件中配置以下操作：<br>• **Default**（默认）— 对每一个 Palo Alto Networks 定义的威胁签名和防间谍软件签名，设定内部默认操作。通常默认操作是发出警报，或者同时进行重置。默认操作显示在括号内，例如，遇到威胁或者抗病毒签名时默认（警报）。<br>• **Allow**（允许）— 允许应用程序流量。<br><br>*Allow*（允许）操作不会生成与签名或配置文件相关的日志。<br><br>• **Alert**（警报）— 为每个应用程序通信流生成警报。警报保存在威胁日志中。<br>• **Drop**（丢弃）— 丢弃应用程序通信。<br>• **Reset Client**（重置客户端）— 对 TCP 来说，重置客户端一侧的连接。对 UDP 来说，删除连接。<br>• **Reset Server**（重置服务器）— 对 TCP 来说，重置服务器一侧的连接。对 UDP 来说，删除连接。<br>• **Reset Both**（重置两者）— 对 TCP 来说，重置服务器和服务器两端的连接。对 UDP 来说，删除连接。<br><br>在某些情况下，当配置文件操作设置为 *reset-both*（重置两者）时，相关联的威胁日志可能会显示操作为 *reset-server*（重置服务器）。当防火墙在会话开始时检测到威胁，并通过 *503* 阻止页面向客户显示时，会发生这种情况。因为阻止页面不允许连接，因此，不需要重置客户端侧，仅重置服务器侧连接。<br>• **Block IP**（阻止 **IP**）— 不管流量来自源还是源-目标对，都将被该操作阻止。可以在规定的时段内对其进行配置。 |
| URL 筛选配置文件 | URL 筛选配置文件可让您监控和控制用户通过 HTTP 和 HTTPS 访问 Web 的方式。可以配置自带默认配置文件的防火墙以阻止某些网站，如已知的恶意软件网站、钓鱼网站和成人内容网站。您可以使用安全策略中的默认配置文件，克隆它用作新 URL 筛选配置文件的起点，或添加含所有类别设置的新 URL 配置文件以允许深入了解网络中的流量。然后，可以自定义新添加的 URL 配置文件，并添加应始终阻止或允许的特定网站列表，提供对 URL 类别的更准确控制。 |
| 数据过滤配置文件 | 数据筛选配置文件有助于阻止像信用卡或社会保险号这样的敏感信息离开受保护的网络。数据筛选配置文件还可以筛选关键字，例如敏感项目名称和 Confidential（机密）一词。请务必让配置文件集中处理目标文件类型，以减少误报情况。例如，您可能仅需要搜索 Word 文档或 Excel 电子表格，还可能仅需要扫描 Web 浏览通信或 FTP。<br><br>您可以创建自定义数据模式对象并将其附加到数据筛选配置文件中，以定义要筛选的信息类型。根据以下内容创建数据模式对象： |



© 2019 Palo Alto Networks, Inc.

| 配置文件类型 | 说明 |
| --- | --- |
| | • **Predefined Patterns**（预定义模式）— 使用预定义模式筛选信用卡和社会安全号（带或不带破折号）。<br>• **Regular Expressions**（正则表达式）— 筛选字符串。<br>• **File Properties**（文件属性）— 根据文件类型筛选文件属性和值。<br><br>如果使用第三方端点数据丢失保护 *(DLP)* 解决方案来填充文件属性以指示敏感内容，则此选项将使防火墙能够执行 *DLP* 策略。<br><br>要开始，请设置数据筛选。 |
| 文件传送阻止配置文件 | 针对指定的应用程序和指定的会话流方向（入站/出站/两者），防火墙使用文件传送阻止配置文件来阻止指定的文件类型。您可以设置配置文件以在上载和/或下载时发出警报或进行阻止，并且可以指定哪些应用程序应服从文件传送阻止配置文件。还可以配置在用户尝试下载指定文件类型时显示的自定义阻止页面。这样将为用户留出一些时间来考虑他们是否希望下载文件。<br><br>您可以定义自己的自定义文件阻止配置文件，或者在将文件阻止应用于安全策略规则时，选择以下预定义配置文件之一。内容发布版本 653 及更高版本可用的预定义配置文件允许您快速启用最佳实践文件阻止设置：<br><br>• **basic file blocking**（基本文件阻止）— 将此配置文件附加到安全策略规则，允许流量往来于较不敏感的应用程序，以阻止通常包含在恶意软件攻击活动中的文件，或是没有上传/下载的真正用例。此配置文件阻止 PE 文件 (.scr, .cpl, .dll, .ocx, .pif, .exe)、Java 文件 (.class, .jar)、帮助文件 (.chm, .hlp) 以及其他潜在的恶意文件类型 (.vbe, .hta, .wsf, .torrent, .7z, .rar, .bat) 的上传和下载。此外，它提示用户确认何时尝试下载加密的 rar 或加密的 zip 文件。此规则会对所有其他文件类型发出警报，以便您全面了解进出网络的所有文件类型。<br>• **strict file blocking**（严格文件阻止）— 在安全策略规则中使用更严格的配置文件，允许访问最敏感的应用程序。此配置文件阻止与其他配置文件相同的文件类型，另外阻止 Flash、.tar、多级编码、.cab、.msi、加密的 rar 和加密的 zip 文件。<br><br>按以下操作配置文件阻止配置文件：<br><br>• **Alert**（警报）— 检测到指定文件类型时，将在数据筛选日志中生成日志。<br>• **Block**（阻止）— 检测到指定文件类型时，将阻止该文件并向用户呈现可自定义的阻止页面。同时会在数据筛选日志中生成日志。<br>• **Continue**（继续）— 检测到指定文件类型时，将向用户呈现可自定义的响应页面。用户可以单击此页面下载文件。同时会在数据筛选日志中生成日志。由于该类转发操作需要用户交互，因此仅适用于 Web 流量。<br><br>要开始，请设置数据阻止。 |
| WildFire 分析配置文件 | 使用 WildFire 分析配置文件可让防火墙为 WildFire 分析转发未知文件或电子邮件链接。根据应用程序、文件类型和传输方向（上传或下载）来指定转发以便进行分析的文件。与配置文件规则匹配的文件或电子邮件链接将被转发至 WildFire 公共云或 WildFire 私人云（托管在 WF-500 设备上），具体取决于规则定义的分析位置。如果配置文件规则设置为将文件转发到 WildFire 公共云，除未知文件外，防火墙还会转发与现有防病毒签名相匹配的文件。<br><br>您还可以使用 WildFire 分析配置文件来设置 WildFire 混合云部署。如果您使用 WildFire 设备在本地分析敏感文件（如 PDF），则可以指定 WildFire 公共云分析敏感度较低的文件类型（如 PE 文件），或者 WildFire 设备分析不支持的文件类型（如 APK）。通过综合运用 WildFire 设备和 WildFire 云进行分析，您能够迅速判 |


© 2019 Palo Alto Networks, Inc.

| 配置文件类型 | 说明 |
| --- | --- |
| | 断云已经处理过的文件，以及设备分析不支持的文件，并从中受益，进而释放设备处理敏感内容的能力。 |
| DoS 保护配置文件 | DoS 保护配置文件提供拒绝服务 (DoS) 保护策略的详细控制。DoS 策略允许基于聚合会话或者源和/或目标 IP 地址控制接口、区域、地址和国家/地区之间的会话数。Palo Alto Networks 防火墙支持以下两种 DoS 保护机制。<br>• **Flood Protection**（泛滥攻击保护）— 检测并阻止网络中充满数据包，从而导致过多的半开会话和/或服务无法响应每个请求的攻击。在这种情况下，攻击的源地址通常已发生欺诈行为。请参阅针对新会话的泛滥攻击配置 DoS 保护。<br>• **Resource Protection**（资源保护）— 检测并阻止会话耗尽攻击。在这种类型的攻击中，使用大量主机 (bot) 尽可能多地建立许多完全建立的会话，以便耗尽所有的系统资源。<br>您可在单个 DoS 保护配置文件中启用两类保护机制。<br>DoS 配置文件用于指定要采取的操作类型及有关 DoS 策略的匹配条件的详细信息。DoS 配置文件定义 SYN、UDP 和 ICMP flood 攻击的设置，可以启用资源保护及定义最大数量的并发连接。在配置 DoS 保护配置文件后，可以将其附件到 DoS 策略中。<br>配置 DoS 保护时，请务必分析您的环境，以便设置正确的阈值，并且由于定义 DoS 保护策略具有一定的复杂性，因此本指南将不提供详细的示例。 |
| Zone Protection Profiles | 区域保护配置文件在特定网络区域之间提供额外保护，以保护区域不受攻击。由于必须将配置文件应用于整个区域，因此请务必认真测试这些配置文件，以防止正常遍历区域的通信出现问题。为区域保护配置文件定义每秒数据包数 (pps) 阈值限制时，此阈值是根据与之前建立的会话不匹配的每秒数据包数确定的。 |
| 安全配置文件组 | 安全配置文件组是一组安全配置文件，其可被视为一个单元，然后便利地添加到安全策略。可以将通常一起分配的配置文件添加到配置文件组中，以简化安全策略的创建。您也可设置默认安全配置文件组 - 新的安全策略将使用在默认配置文件组中定义的设置来检查和控制匹配安全策略的流量。将安全配置文件组命名为 default，从而默认将该组中的配置文件添加至新的安全策略。这可让您不断将自己组织首选的配置文件设置自动加入新的策略，无需在每次新建策略时手动添加安全配置文件。<br>请参阅创建安全配置文件组和设置或替代默认安全配置文件组。<br>有关安全配置文件的最佳实践设置的建议，请参阅创建最佳实践之互联网网关安全配置文件。 |

# 创建安全配置文件组

使用以下步骤来创建安全配置文件组并将其添加至安全策略。

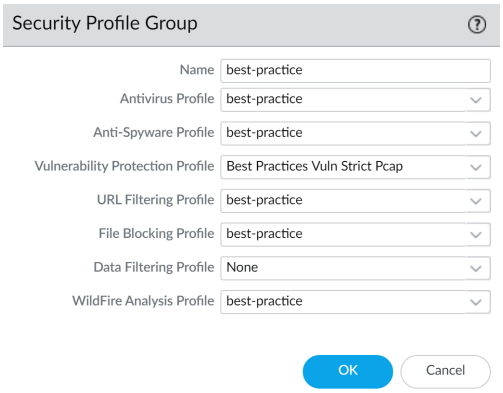
STEP 1 | 创建安全配置文件组。

如果您将组命名为 *default*，防火墙会自动将其附加到您创建的所有新规则。如果您希望确保一组首选安全配置文件附加到每个新规则，此方式可节约时间。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Objects**（对象）> **Security Profile Groups**（安全配置文件组），并 **Add**（添加）新的安全配置文件组。
2. 为配置文件组赋予描述性 **Name**（名称），例如 Threats（威胁）。
3. 如果防火墙处于多虚拟系统模式下，可让配置文件由所有虚拟系统 **Shared**（共享）。
4. 将现有配置文件添加至组。




5. 单击 **OK**（确定）以保存配置文件组。

STEP 2 | 向安全策略添加安全配置文件组。

1. 选择 **Policies**（策略）> **Security**（安全），并 **Add**（添加）或修改安全策略规则。
2. 选择 **Actions**（操作）选项卡。
3. 在配置文件设置部分，选择 **Profile Type**（配置文件类型）的 **Group**（组）。
4. 在 **Group Profile**（组配置文件）下拉列表中，选择您创建的组（例如选择最佳实践组）：




5. 单击 **OK**（确定）以保存策略，然后 **Commit**（提交）更改。

STEP 3 | 保存更改。

单击 **Commit**（提交）。

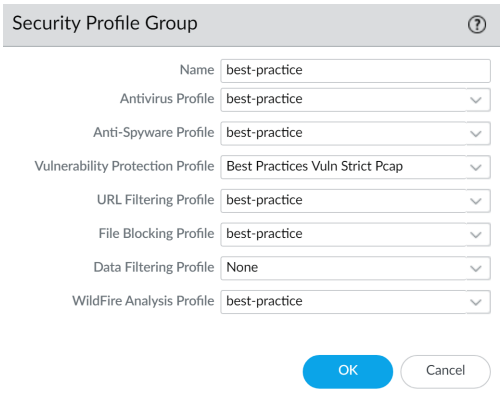
# 设置或替代默认安全配置文件组

使用以下选项来设置要在新的安全策略中使用的默认安全配置文件组，或者替代现有默认组。在管理员创建新的安全策略时，将自动把默认配置文件组选择为策略的配置文件设置，并且将根据在配置文件组中定义的设置检查符合策略的流量（管理员可根据需要选择手动选择不同的配置文件设置）。使用以下选项来设置默认安全配置文件组或者替代默认设置。

如果不存在默认的安全配置文件，则默认情况下，新的安全策略的配置文件设置会设置为 *None*（无）。

- 创建安全配置文件组。
  1. 选择 **Objects**（对象）> **Security Profile Groups**（安全配置文件组），并 Add（添加）新的安全配置文件组。
  2. 为配置文件组赋予描述性 **Name**（名称），例如 Threats（威胁）。
  3. 如果防火墙处于多虚拟系统模式下，可让配置文件由所有虚拟系统 **Shared**（共享）。
  4. 将现有配置文件添加至组。有关创建配置文件的详细信息，请参阅安全配置文件。


© 2019 Palo Alto Networks, Inc.

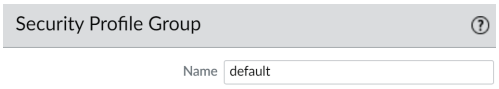



5. 单击 **OK**（确定）以保存配置文件组。
6. 向安全策略添加安全配置文件组。
7. **Add**（添加）或修改安全策略规则并选择**Actions**（操作）选项卡。
8. 选择 **Profile Type**（配置文件类型）的 **Group**（组）。
9. 在 **Group Profile**（组配置文件）下拉列表中，选择您创建的组（例如选择威胁组）：




10. 单击 **OK**（确定）以保存策略，然后 **Commit**（提交）更改。

- 设置默认安全配置文件组。
  1. 选择 **Objects**（对象）> **Security Profile Groups**（安全配置文件组），并添加新的安全配置文件组或修改现有安全配置文件组。
  2. 将安全配置文件组**Name**（命名）为 **`default`**：




  3. 单击 **OK**（确定）和 **Commit**（提交）。
  4. 确认 default 安全配置文件组默认包含在新的安全策略中：
     1. 选择 **Policies**（策略）> **Security**（安全），并 **Add**（添加）新的安全策略。
     2. 选择**Actions**（操作）选项卡并查看**Profile Setting**（配置文件设置）字段：




     默认设置下，新的安全策略正确显示设置为“组”的 **Profile Type**（配置文件类型）并选中 default **Group Profile**（组配置文件）。

- 替代默认安全配置文件组。

  如果您当前已有默认安全配置文件组，并且不希望该组策略附加至新的安全策略，则可根据您的首选项继续修改“配置文件设置”字段。通过为您的策略选择不同的配置文件类型开始（**Policies**（策略）> **Security**（安全）> **Security Policy Rule**（安全策略规则）> **Actions**（操作））。



© 2019 Palo Alto Networks, Inc.

# 跟踪规则库内规则

要跟踪规则库内规则，您可以参考规则号，此数字因规则库中规则的顺序而异。规则号可确定防火墙使用规则的顺序。

即使规则被修改，规则的通用唯一标识符 *(UUID)*也不会发生变化，例如更改规则名称时。通过 UUID，您可以跟踪规则库内规则，即使是在规则已被删除的情况下。

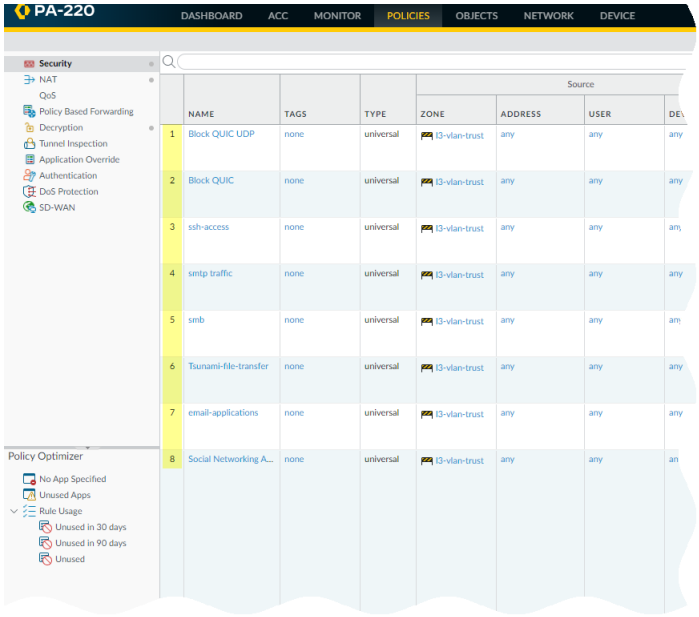
## 规则号

防火墙自动为规则库内每个规则编号；当您移动或重新排序规则时，该编号会根据新的顺序发生改变。在筛选规则列表以查找匹配指定条件的规则时，防火墙会在规则库中显示每条规则与其在整组规则的编号及其在评估顺序中的位置。

Panorama 将独立对前导规则、后规则和默认规则进行编号。当 Panorama 推送规则到防火墙时，规则编号反应了共享规则、设备组前导规则、防火墙规则、设备组后规则和默认规则的层次和评估顺序。您可以在 Panorama 中 **Preview Rules**（预览规则）以显示了关于防火墙的所有规则的有序列表视图。

- 查看防火墙上规则的已编号列表。

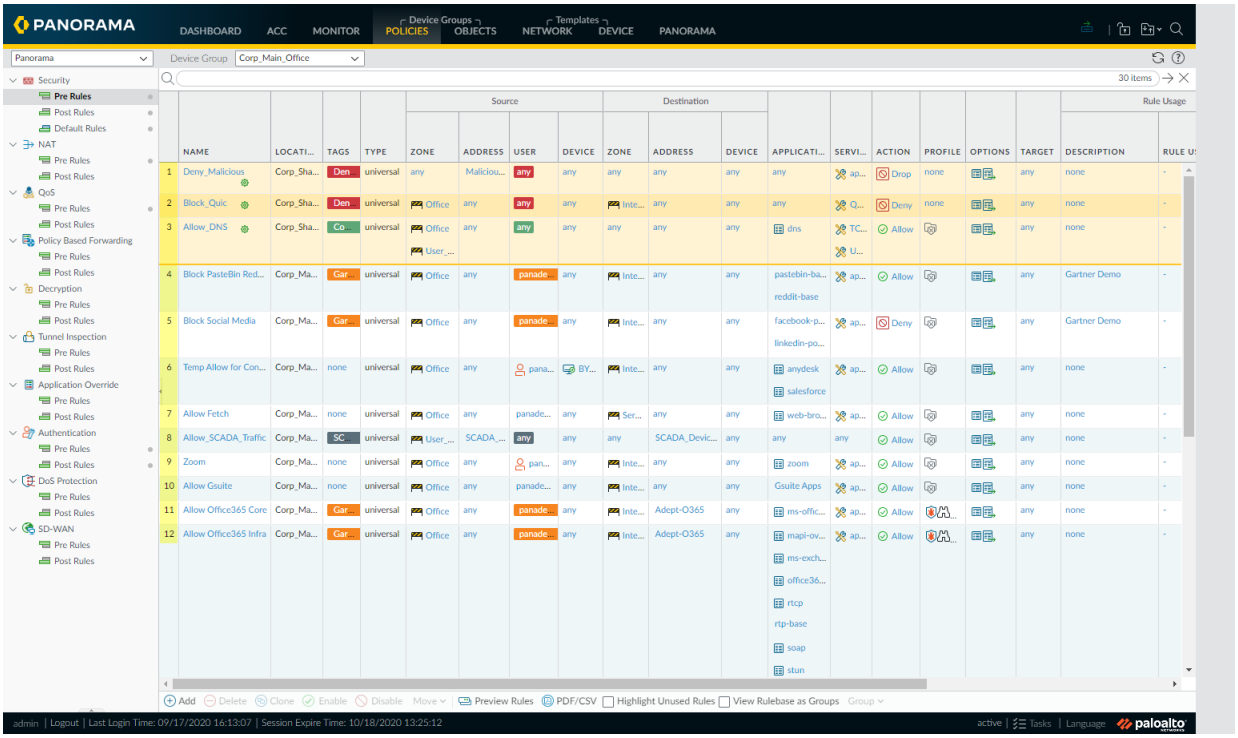
  选择 **Policies**（策略）及其下方的任何规则库。例如，**Policies**（策略）> **Security**（安全）。表格中最左侧的列显示规则编号。




- 查看 Panorama 上规则的已编号列表。

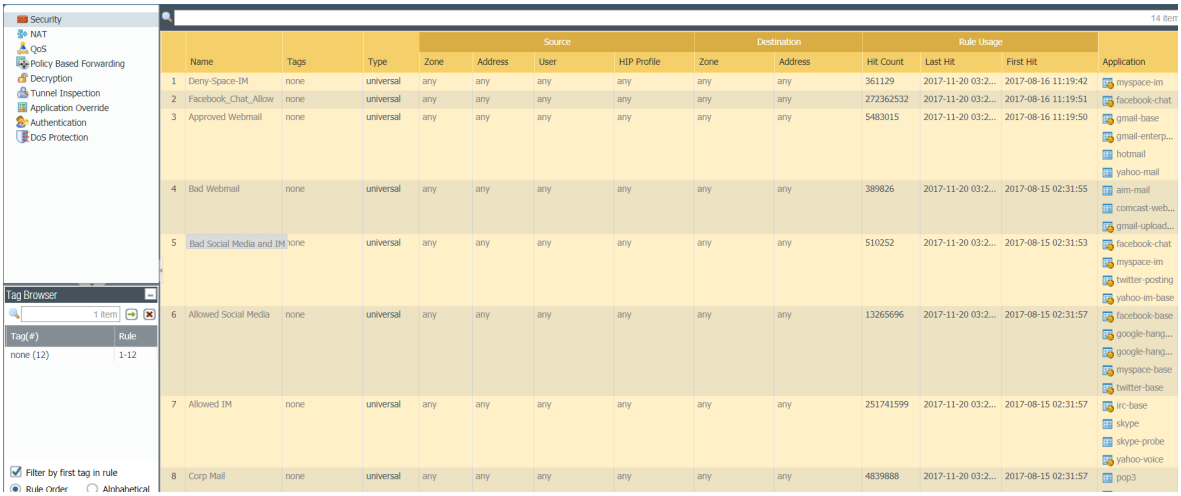
  选择 **Policies**（策略）及其下方的任何规则库。例如，**Policies**（策略）> **Security**（安全）> **Pre-rules**（前导规则）。


© 2019 Palo Alto Networks, Inc.




- 在您从 Panorama 推送规则之后，在防火墙上查看附带编码的完整的规则列表。

  从防火墙的 Web 界面，选择 **Policies**（策略）并选择下面的任意一个规则库。例如，选择 **Policies**（策略）> **Security**（安全）并查看防火墙将要评估的完整的已编号规则。




# 规则 UUID

规则的通用唯一标识符 (UUID) 是指防火墙或 Panorama 分配给规则的一个由 32 个字符组成的字符串（基于网络地址和创建时间戳等数据）。UUID 使用的格式为 8-4-4-4-12。其中，8、4 和 12 代表唯一字符数，由连字符分隔。UUID 可标识所有策略规则库中的规则。此外，您还可以使用 UUID 标识下列日志类型中的适用规则：流量、威胁、URL 筛选、WildFire 提交内容、数据筛选、GTP、SCTP、隧道检测、配置和统一。

通过使用 UUID 搜索规则，您可以在具有类似或相同名称的数千个规则中找到您想要找到的特定规则。此外，UUID 还可以简化不支持名称的第三方系统（例如，票据或协调）内规则的自动化和集成操作。



© 2019 Palo Alto Networks, Inc.

在某些情况下，您可能需要为现有规则库生成新的 UUID。例如，如果想导出配置到另一个防火墙，您需要在导入配置时为此规则重新生成 *UUID*，确保不会出现重复的 UUID。如果重新生成 UUID，则再也无法使用其之前的 UUID 跟踪这些规则，且这些规则的点击数据和应用程序使用数据也将重置。

当您执行以下操作时，防火墙或 Panorama 会分配 UUID：

- 创建新规则
- 克隆现有规则
- 替代默认安全规则
- 加载已命名配置并重新生成 UUID
- 加载的已命名规则包含不在运行配置中的新规则
- 将防火墙或 Panorama 升级到 PAN-OS 9.0 版

当加载的配置包含带 UUID 的规则时，如果规则名称、规则库、以及虚拟系统都匹配，则防火墙会将规则视为相同规则。如果规则名称、规则库、以及设备组都匹配，则 Panorama 会将规则视为相同规则。

请记住以下 UUID 的要点：

- 如果从 Panorama 管理防火墙策略，会在 Panorama 上生成 UUID，因此，必须从 Panorama 推送 UUID。如果配置未在将防火墙升级到 PAN-OS 9.0 之前从 Panorama 推送，则防火墙升级将不会成功，原因是防火墙不包含 UUID。
- 此外，如果您正在升级 HA 对，在升级到 PAN-OS 9.0 时，每个对等都会为每个策略规则独立分配 UUID。因此，在您同步配置之前，对等将显示为不同步（**Dashboard**（仪表板）> **Widgets**（小部件）> **System**（系统）> **High Availability**（高可用性）> **Sync to peer**（同步到对等））。
- 如果在升级到 PAN-OS 9.0 后删除现有高可用性 (HA) 配置，您必须在其中一个对等上重新生成 UUID（**Device**（设备）> **Setup**（设置）> **Operations**（操作）> **Load named configuration snapshot**（加载已命名配置快照）> **Regenerate UUIDs for the selected named configuration**（为选中的已命名配置重新生成 **UUID**）），并提交更改，以避免出现 UUID 重复。
- 从 Panorama 推送的所有规则将共享相同的 UUID；防火墙所有本地规则都将具有不同的 UUID。如果您在将规则从 Panorama 推送到防火墙后在防火墙上本地创建规则，则您本地创建的规则拥有其自己的 UUID。
- 要替换 RMA Panorama，请务必在您加载已命名的 Panorama 配置快照时 **Retain Rule UUIDs**（保留规则 **UUID**）。如果未选择此选项，Panorama 将从配置快照中删除先前所有规则 UUID，并将新 UUID 分配给 Panorama 上的规则，这意味着与先前 UUID 相关的信息将不会被保留，例如，策略规则点击数。

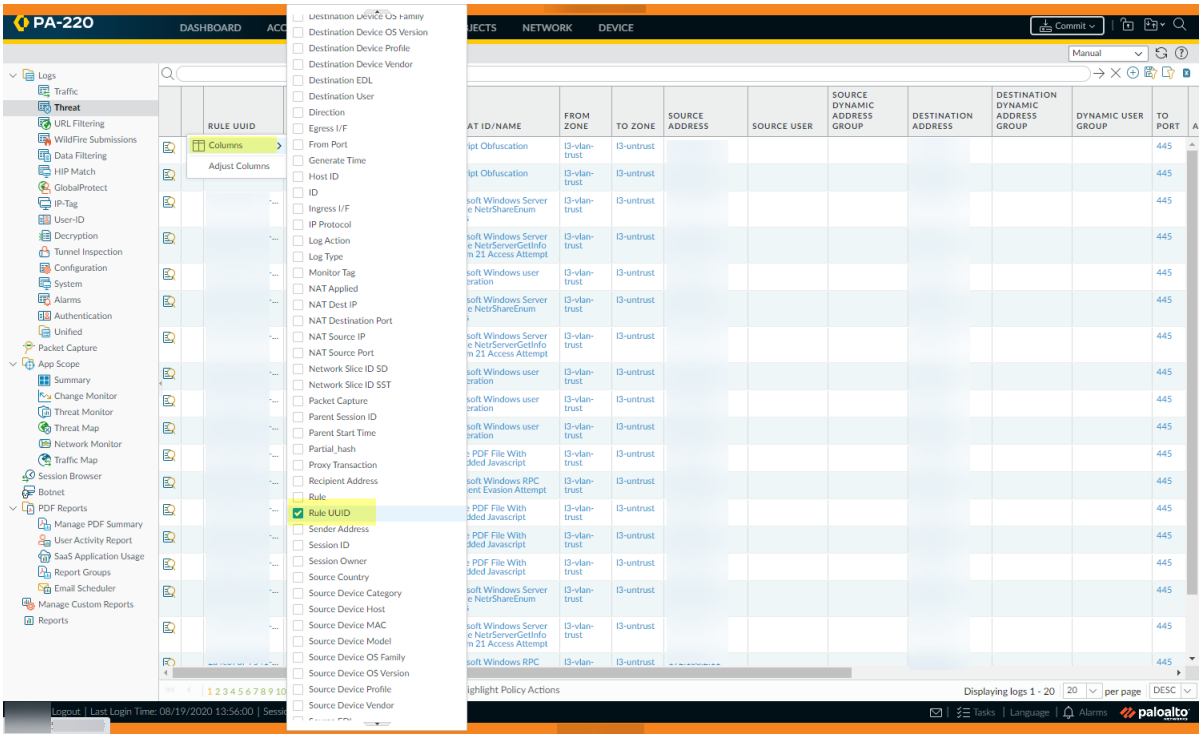
- 显示用于日志的规则 UUID 列和用于策略规则的 UUID 列。

  要查看 UUID，您必须显示默认不会显示的列。

  - 要在日志中显示 UUID：

    1. 选择 **Monitor**（监控），然后展开列标题（ ）。
    2. 选择 **Columns**（列）。
    3. 启用 **Rule UUID**（规则 **UUID**）。

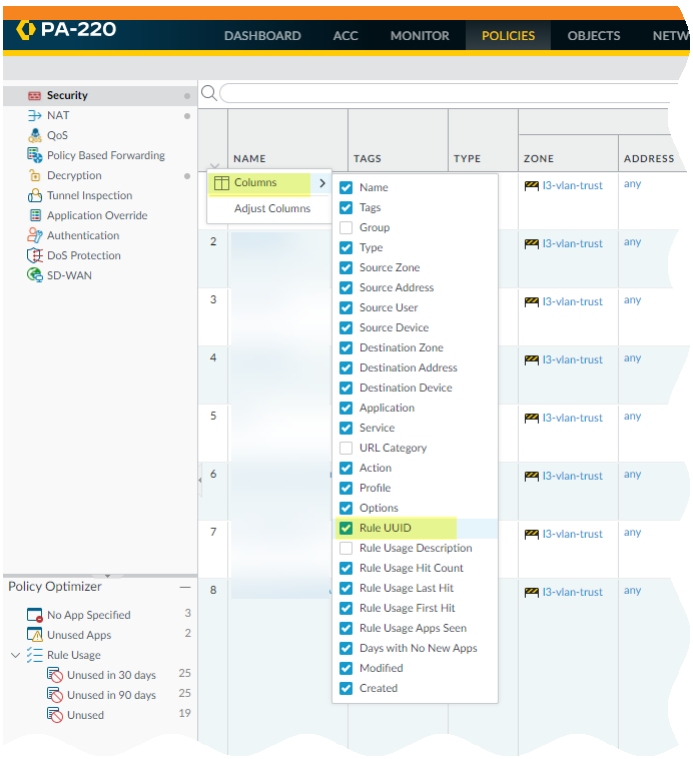

© 2019 Palo Alto Networks, Inc.




- 要在策略规则库上显示 UUID：

1. 选择 **Policies**（策略），然后展开列标题（ ）。
2. 选择 **Columns**（列）。
3. 启用 **Rule UUID**（规则 **UUID**）。

   UUID 可用于所有策略规则库。



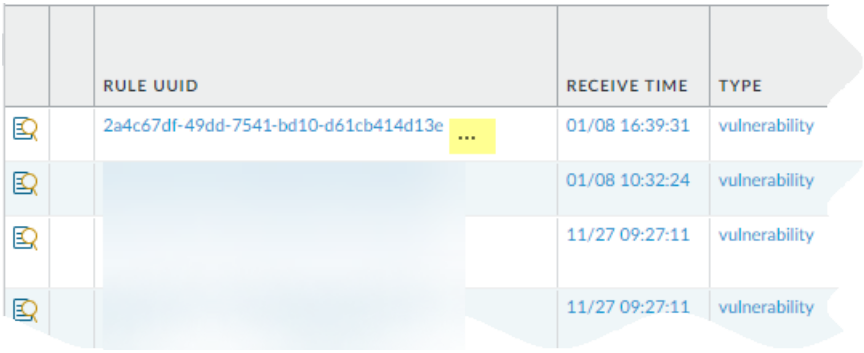



© 2019 Palo Alto Networks, Inc.

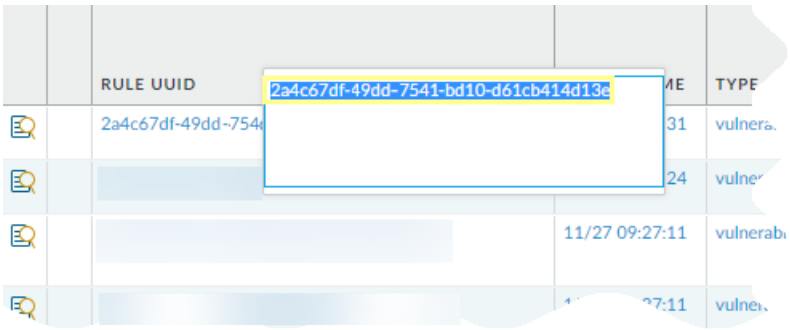
- 复制用于日志或策略规则的 UUID。

  通过复制 UUID，您可以将 UUID 粘贴到搜索、ACC、自定义报告、筛选器、以及您想找到根据此 UUID 标识的规则的任何位置。

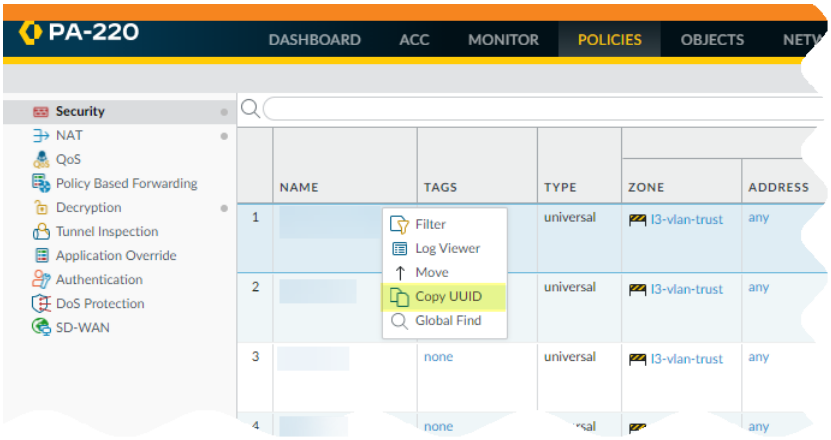
  1. 将光标移到规则 UUID 列中的条目上时，选择显示的省略号。




  2. 从弹出窗口复制 UUID。




  此外，您还可以前往 **Policies**（策略）选项卡，单击规则名称右侧的箭头，然后 **Copy UUID**（复制 **UUID**）。




- 选中配置日志以查看已删除规则的 UUID。

  要查看已删除规则的 UUID，请选择 **Monitor**（监控）> **Logs**（日志）> **Configuration**（配置）。



© 2019 Palo Alto Networks, Inc.

# 实施策略规则描述、标记和审核注释

当创建或修改规则时，您可要求输入规则描述、标记和审核注释，以确保您的策略规则库被正确组织和分组，并保留重要的规则记录以用于审核。通过要求规则描述、标记和审核注释，您可以通过确保规则适当分组，从而简化您的策略规则库审查，且在创建或修改规则时追踪规则更改记录。为了统一，您可以设置审核注释可以包含的特定要求。

默认情况下，描述、标记和审核注释的执行不会被启用。您可以指定是否需要描述、标记、审核注释或这三项的组合，以成功添加或修改规则。审核注释档案让您可以查看为某个选中的规则输入的审核注释，查看配置日志记录，并对比规则配置版本。

STEP 1 | 启动 Web 界面。

STEP 2 | 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑策略规则库设置。

STEP 3 | 配置您想要执行的设置。此例中，所有策略都需要标记和审核注释。

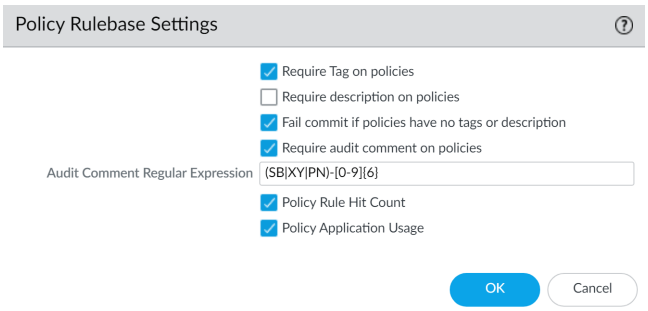
为策略规则执行审核注释，以获取管理员创建或修改规则的原因。要求策略规则的审核注释有助于维持准确的规则记录，以进行审核。

STEP 4 | 配置审核注释正则表达式，以规定审核注释格式。

当管理员创建或修改规则时，您可以要求其输入符合特定格式的审核注释，该格式通过规定字母和数字表达式以满足您的业务和审核需要。例如，您可以使用此设置规定与您的票据数字格式相符的正则表达式：

- **[0-9]{<Number of digits>}** — 要求审核注释包含从 0 到 9 的至少一个数字位数。例如，**[0-9]{6}** 要求在表达式中至少有 0 到 9 的六位数字。
- **<Letter Expression>** — 要求审核注释包含字母表达式。例如，**Reason for Change-** 要求管理员以此字母表达式作为审核注释的开头。
- **<Letter Expression>-[0-9]{<Number of digits>}** — 要求审核注释包含预定的字符，后接从 0 到 9 的至少一个数字位数。例如，**SB-[0-9]{6}**要求审核注释格式以 **SB-** 开头，后接至少六位数的从 0 到 9 的数字表达式。例如，**SB-012345**。
- **(<Letter Expression>)|(<Letter Expression>)|(<Letter Expression>)|-[0-9]{<Number of digits>}** — 需要审核注释包含预定字母表达式作为前缀，后接从 0 到 9 的至少一个数字位数。例如，**(SB|XY|PN)-[0-9]{6}** 要求审核注释格式以**SB-**、**XY-**或**PN-** 开头，后接至少六位数的从 0 到 9 的数字表达式。例如，**SB-012345**、**XY-654321** 或 **PN-012543**。

STEP 5 | 点击 **OK**（确定）以应用新的策略规则库设置。

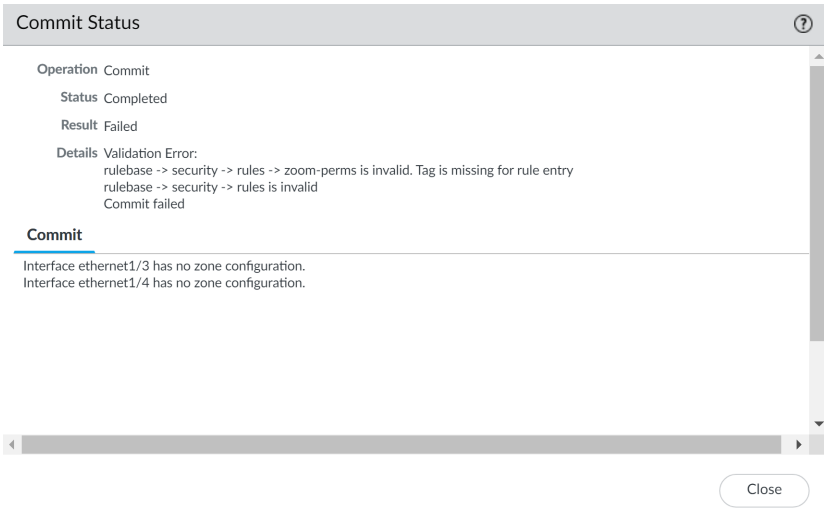



STEP 6 | **Commit**（提交）更改。



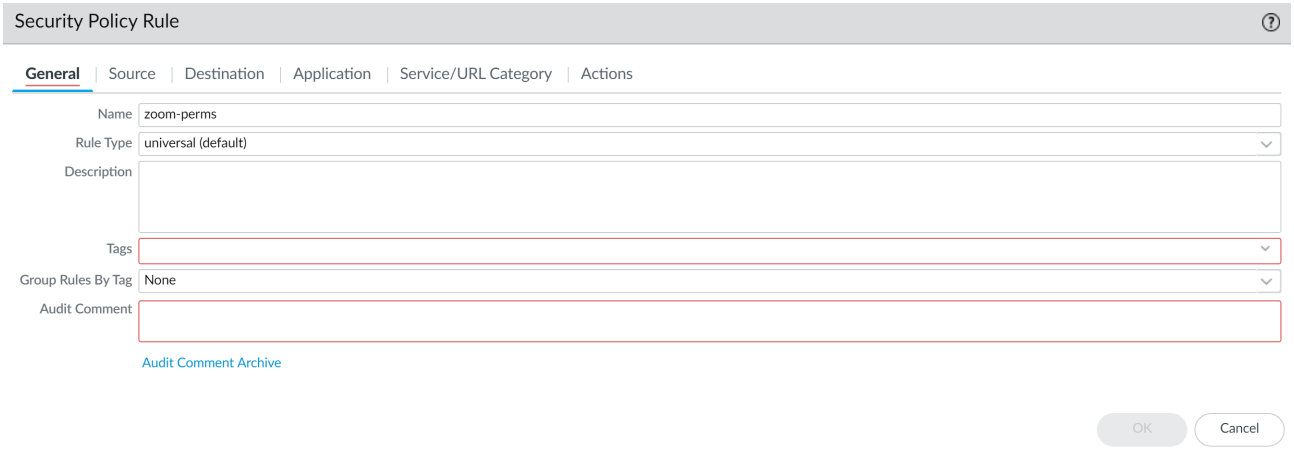
© 2019 Palo Alto Networks, Inc.

在您提交策略规则库设置更改后，根据您决定执行的规则库设置修改现有策略规则。




STEP 7 | 确认防火墙正在执行新的策略规则库设置。

1. 选择 **Policies**（策略），然后 **Add**（添加）新规则。
2. 确认您必须添加标记并输入审核注释，点击 **OK**（确定）。





© 2019 Palo Alto Networks, Inc.

# 将策略规则或对象移动或克隆到不同的虚拟系统

关于拥有不止一个虚拟系统 (vsys) 的防火墙，您可以移动或克隆策略规则和对象到不同的 vsys 或到共享的位置。移动和克隆将保存删除、重新创建和重命名规则和对象的结果。如果您从 vsys 移动或克隆的策略规则或对象引用了 vsys 里的对象，那么请同时移动或克隆被引用的对象。如果被引用的是共享对象，那么您不必在移动或克隆时包含它们。您可以使用全局查找搜索防火墙或 Panorama 管理服务器来引用。

复制多个策略规则时，选择规则的顺序将决定它们复制到设备组的顺序。例如，如果您有规则 *1-4*，并且您的选择顺序为 *2-1-4-3*，则复制这些规则的设备组将按照您选择的相同顺序显示规则。但是，一旦成功复制，您可以按照您的意愿重新组织规则。

STEP 1 | 选择策略类型（例如，**Policy**（策略）> **Security**（安全））或对象类型（例如，**Objects**（对象）> **Addresses**（地址））。

STEP 2 | 选择 **Virtual System**（虚拟系统）并选择一个或多个策略规则或对象。

STEP 3 | 执行以下步骤之一：

- 选择 **Move**（移动）> **Move to other vsys**（移动到其他 **vsys**）（适用于策略规则）。
- 单击 **Move**（移动）（对于对象）。
- 单击 **Clone**（克隆）（对于规则或对象）。

STEP 4 | 在 **Destination**（目标）下拉列表中，选择新的虚拟系统或 **Shared**（共享）。

STEP 5 | （仅适用于策略规则）选择 **Rule order**（规则顺序）。

- **Move top**（置顶）（默认）— 此规则将位于所有其他规则的之前。
- **Move bottom**（置底）— 此规则将位于所有其他规则的之后。
- **Before rule**（前导规则）— 在相邻下拉列表中，选择所选规则之后的规则。
- **After rule**（后继规则）— 在相邻下拉列表中，选择所选规则之前的规则。

STEP 6 | 默认情况下，**Error out on first detected error in validation**（输出验证中第一个检测到的错误）复选框处于选中状态。当防火墙发现第一个错误时，将停止执行对移动或克隆操作的检查，并显示错误信息。例如，如果 **Destination**（目标）vsys 不包含要移动的策略规则所引用的对象，则会出错，防火墙将显示错误信息并停止执行进一步的验证。如果您一次移动或克隆多个项目，则通过选中此复选框可一次查找一个错误并解决其问题。如果您清除此复选框，防火墙将收集并显示错误列表。如果验证中出现错误，则不会移动或克隆对象，直到您修正所有错误。

STEP 7 | 单击 **OK**（确定）开始执行错误验证。如果防火墙显示错误，请修正错误并重新尝试移动或克隆操作。如果防火墙没有找到错误，则会成功移动或克隆对象。操作完成后，单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 使用地址对象表示 IP 地址

在防火墙上创建地址对象以分组 IP 地址或指定 FQDN，然后在防火墙策略规则、筛选器或其他功能中引用此地址对象，以避免在规则、筛选器或其他功能中单独指定多个 IP 地址。

此外，您可以在多个策略规则、筛选器或其他功能中引用相同的地址对象，无需在每次使用时指定相同的单个地址。例如，您可以创建一个地址对象指定 IPv4 地址范围，然后在安全策略规则、NAT 策略规则和自定义报告日志筛选器中引用地址对象。

- 地址对象
- 创建地址对象

## 地址对象

地址对象是 IP 地址的集，您可以在统一进行管理，然后在多个防火墙策略规则、筛选器和其他功能中使用。有四种地址对象类型：**IP Netmask**（**IP** 掩码）、 **IP Range**（**IP** 范围）、 **IP Wildcard Mask**（**IP** 通配符掩码）和 **FQDN**。

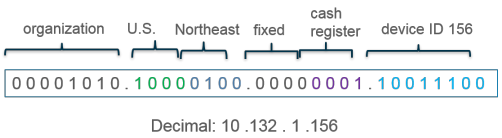
**IP Netmask**（**IP** 掩码）、**IP Range**（**IP** 范围）或 **FQDN** 类型的地址对象可指定 IPv4 或 IPv6 地址。**IP Wildcard Mask**（**IP** 通配符掩码）类型的地址对象仅可指定 IPv4 地址。

**IP Netmask**（**IP** 掩码）类型的地址对象要求您用斜杠计法输入 IP 地址或网络，以表示 IPv4 网络或 IPv6 前缀长度。例如，192.168.18.0/24 或 2001:db8:123:1::/64。

**IP Range**（**IP** 范围）类型的地址对象要求您输入 IPv4 或 IPv6 地址范围，并以连字符分隔。

**FQDN** 类型的地址对象（例如 paloaltonetworks.com）提供更简便的使用方法，因为 DNS 提供对 IP 地址的 FQDN 解析，从而无需知道 IP 地址，并在每次 FQDN 解析新 IP 地址时手动更新。

当您定义专用 IPv4 地址至内部设备，且您的地址结构对地址中某些位分配含义时，**IP Wildcard Mask**（**IP** 通配符掩码）类型的地址对象非常有用。例如，根据位的分配，美国东北部的收银机 156 的 IP 地址可能为 10.132.1.156：




**IP Wildcard Mask**（**IP** 通配符掩码）类型的地址对象指定哪些源或目标位置受安全策略规则的约束。例如，10.132.1.1/0.0.2.255。在掩码中零 (0) 位表示被比较的位必须与零覆盖的 IP 地址中的位匹配。掩码（通配符位）中的一 (1) 位表示被比较的位无需与 IP 地址中的位匹配。IP 地址和通配符掩码的下列片段代表其如何产生四种匹配：




在您 创建地址对象之后：

- 您可以在策略规则中引用 **IP Netmask**（**IP** 掩码）、**IP Range**（**IP** 范围）或 **FQDN** 类型地址对象，用于安全、验证、NAT、NAT64、解密、DoS 保护、基于策略的转发 (PBF)、QoS、应用程序替代或隧道检查；或在 NAT 地址池、VPN 隧道、路径监控、外部动态列表、侦察保护、ACC 全局筛选器、日志筛选器或自定义报告日志筛选器中。


© 2019 Palo Alto Networks, Inc.

- 您只能在安全策略规则中引用 **IP Wildcard Mask**（**IP** 通配符掩码）类型的地址对象。

## 创建地址对象

创建 地址对象 以显示一个或多个 IP 地址，然后在一个或多个策略规则、筛选器或其他防火墙功能中引用此地址对象。如果您想要更改地址集，可更改地址对象一次，而不是更改多个策略规则或筛选器，从而减少操作开销。

STEP 1 | 创建地址对象。

1. 选择 **Objects**（对象）> **Addresses**（地址），并按 **Name**（名称）**Add**（添加）地址对象。名称区分大小写，必须是唯一的，且最多可包含 63 个字符（字母、数字、空格、连字符和下划线）。
2. 选择地址对象 **Type**（类型）。
   - **IP Netmask**（**IP** 网络掩码）— 指定单 Ipv4 或 Ipv6 地址，带斜线计法的 Ipv4 网络，或 IPv6 地址和前缀。例如，192.168.80.0/24 或 2001:db8:123:1::/64。或者单击 **Resolve**（解析）以查看相关 FQDN（基于防火墙或 Panorama 的 DNS 配置）。要将地址对象类型从 **IP Netmask**（**IP** 网络掩码）更改为 **FQDN**，选择 FQDN 并点击 **Use this FQDN**（使用此 **FQDN**）。**Type**（类型）会变更为 **FQDN**，同时您选择的 FQDN 会显示在文本字段中。
   - **IP Range**（**IP** 范围）— 指定 IPv4 地址或 IPv6 地址范围，用连字符分隔。例如，192.168.40.1-192.168.40.255 或 2001:db8:123:1::1-2001:db8:123:1::22。
   - **IP Wildcard Mask**（**IP** 通配符掩码）— 指定 IP 通配符地址（IPv4 地址后跟斜杠和通配符掩码，必须以 0 开头）。例如：10.5.1.1/0.127.248.2。在掩码中零位 (0) 表示被比较的位必须与零覆盖的 IP 地址中的位匹配。掩码（通配符位）中的一 (1) 表示被比较的位无需与一覆盖的 IP 地址中的位匹配。
   - **FQDN** — 指定域名。FQDN 最初在提交时进行解析。只要 TTL 大于或等于您配置的 **`Minimum FQDN Refresh Time`**（最短 **`FQDN`** 刷新时间）（或默认的 30 秒），防火墙就会根据 DNS 内 FQDN 的生存时间 (TTL) 刷新 FQDN。如果配置代理，则 FQDN 由系统 DNS 服务器或 DNS 代理对象解析。单击 **Resolve**（解析）以查看相关 IP 地址（基于防火墙或 Panorama 的 DNS 配置）。要将地址对象类型从 FQDN 更改为 IP 网络掩码，选择 IP 网络掩码并点击 **Use this address**（使用此地址）。**Type**（类型）会变更为 **IP Netmask**（**IP** 网络掩码），同时您选择的 IP 地址会显示在文本字段中。
3. （可选）输入一个或多个 使用标记分组并以可视方式区分对象 以应用至地址对象。
4. 单击 **OK**（确定）。

STEP 2 | **Commit**（提交）更改。

STEP 3 | 查看按照地址对象、地址组或通配符地址筛选的日志。

1. 例如，选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）来查看流量日志。
2. 选择 **+** 以添加日志筛选器。
3. 选择 **Address**（地址）属性，**in** 运算符，然后输入您想要查看日志的地址对象名称。或者，输入地址组名称或通配符地址，如 10.155.3.4/0.0.240.255。
4. 单击应用。

STEP 4 | 查看基于地址对象的自定义报告。

1. 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告）并选择使用数据库的报告，如流量日志。
2. 选择 **Filter Builder**（筛选器生成器）。
3. 选择 **Address**（地址）、**Destination Address**（目标地址）或 **Source Address**（源地址）等属性，再选择一个运算符，然后输入您想要查看报告的地址对象名称。

STEP 5 | 在 ACC 中使用筛选器，查看基于源 IP 地址或目标 IP 地址（使用地址对象）的网络活动。

1. 选择 **ACC** > **Network Activity**（网络活动）。



© 2019 Palo Alto Networks, Inc.

2. 查看源 **IP** 活动 — 对于全局筛选器，单击 **+** 以添加筛选器并选择下列内容之一：**Address**（地址）或 **Source**（源） > **Source Address**（源地址）或 **Destination**（目标） > **Destination Address**（目标地址），然后选择一个地址对象。
3. 查看目标 **IP** 活动 — 对于全局筛选器，单击 **+** 以添加筛选器并选择下列内容之一：**Address**（地址）或 **Source**（源） > **Source Address**（源地址）或 **Destination**（目标） > **Destination Address**（目标地址），然后选择一个地址对象。


© 2019 Palo Alto Networks, Inc.

# 使用标记分组并以可视方式区分对象

您可以标记对象来对相关项目进行分组，并通过对标记添加颜色来可视地区分标记的对象。您可以为以下对象创建标记：地址对象、地址组、用户组、区域、服务组以及策略规则。

防火墙和 Panorama 支持静态标记和动态标记。动态标记通过各种源注册，不会和静态标记一起显示，因为动态标记并非防火墙或 Panorama 配置的一部分。有关动态注册标记的信息，请参阅动态注册 IP 地址和标记。在该部分中讨论的标记会以静态方式添加并且是设备配置的一部分。

您可以应用一个或多个标记到对象和策略规则，每个对象最多64个标记。Panorama 最多支持 10,000 个标记，可在 Panorama（共享组和设备组）和受管设备（包括具有多个虚拟系统的设备）上分配它们。

- 创建并应用标记
- 修改标记
- 按标记组查看规则

## 创建并应用标记

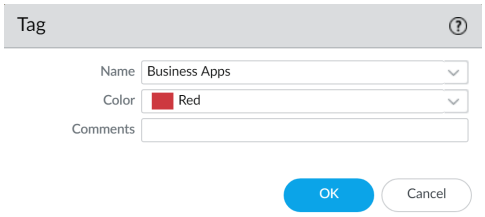
使用标签识别规则或配置对象的目的，帮助您更好的组织规则库。要确保策略规则被正确标记，请参阅如何实施策略规则描述、标记和审核注释。此外，您可以通过先创建标签，然后将此标签设置为组标签来 按标记组查看规则。

STEP 1 | 创建标记。



要标记区域，您必须创建名称和区域一样的标记。如果在策略规则中附加了区域，标记颜色会自动显示为区域名称的背景色。

1. 选择**Objects**（对象）> **Tags**（标记）。
2. 在 Panorama 或多个虚拟系统防火墙上，选择 **Device Group**（设备组）或 **Virtual System**（虚拟系统）使标签可用。
3. **Add**（添加）标签，输入 **Name**（名称）以识别标签，或选择区域 **Name**（名称），为区域创建标签。最大长度为 127 个字符。
4. （可选）选择 **Shared**（共享）以在共享位置创建对象，作为 Panorama 中的共享对象以进行访问，或在多个虚拟系统防火墙中跨所有虚拟系统进行使用。
5. （Optional（可选））从 17 种预定义颜色中分配一种 **Color**（颜色）。默认情况下，**Color**（颜色）为**None**（空）。




6. 单击 **OK**（确定）和 **Commit**（提交），保存您的更改。

STEP 2 | 将标记应用到策略。

1. 选择 **Policies**（策略）及其下方的任何规则库。
2. **Add**（添加）策略规则并使用您在步骤 1 中创建的标签对象。
3. 检查标记是否已被使用。



© 2019 Palo Alto Networks, Inc.

| | NAME | TAGS | TYPE | Source | | | | Destination | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 1 | General Business Apps | Business Apps | universal | any | any | known-user | any | any | any |

STEP 3 | 将标记应用至地址对象、地址组、服务或服务组。

1. 创建对象。

   例如要创建服务组，可选择 **Objects**（对象）> **Service Groups**（服务组）> **Add**（添加）。
2. 选择标签（**Tags**（标签））或在字段内输入名称以创建新标签。

   要编辑标记或向标记添加颜色，请参阅修改标记。

# 修改标记

- 选择 **Objects**（对象）> **Tags**（标记）以对标记执行以下任何操作：
  - 单击 **Name**（名称）来编辑标记的属性。
  - 选择表格中的标记，并 **Delete**（删除）防火墙中的标记。
  - **Clone**（克隆）标记以使用相同的属性对其进行复制。将数字后缀添加至标记名称（例如，FTP-1）。

  有关创建标记的详细信息，请参阅创建并应用标记。有关使用标记的详细信息，请参阅按标记组查看规则。

# 按标记组查看规则

以标记组查看您的策略规则库，从而根据您创建的标记结构，对规则进行视觉分组。在此视图中，您可以执行操作程序，例如在所选标记组中更轻松地添加、删除和移动规则。按标记组查看规则库可保持规则评估顺序，在整个规则中可能多次出现单个标记，从而在视觉上保留规则层次结构。

您必须先创建标记，然后才可将其分配为作规则的组标记。PAN-OS 9.0 升级上已标记的策略规则具有第一个被作为组标记自动分配的标记。在升级至 PAN-OS 9.0 之前，查看规则库中标记的规则，以确保将规则正确分组。如果在升级至 PAN-OS 9.0 之后，如果您的规则分组错误，您必须手动编辑各个标记规则，并配置正确的组标记。



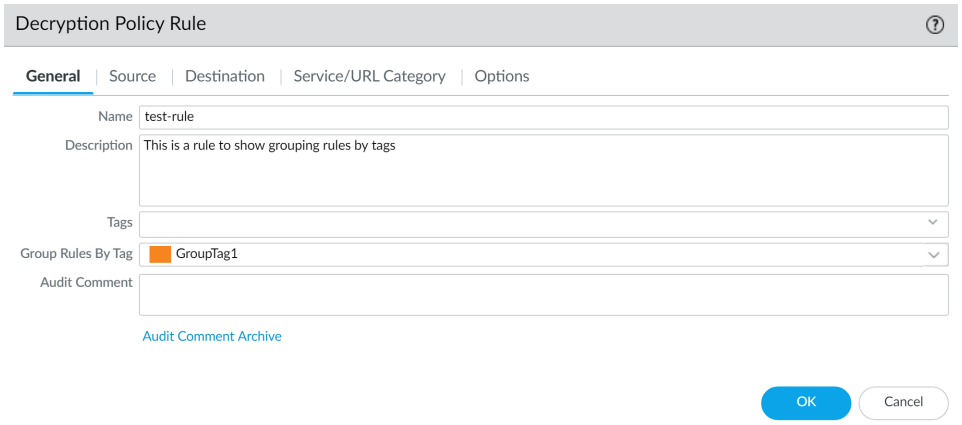

STEP 1 | 启动 Web 界面。

STEP 2 | 创建并应用标记用于分组规则。

STEP 3 | 分配策略规则至标记组。

1. 创建策略规则。参见 策略 了解关于创建策略规则的更多信息。
2. 在 **Group Rules by Tag**（按标记分组规则）字段中，从下拉列表中选择标记并按下 **OK**（确定）。


© 2019 Palo Alto Networks, Inc.

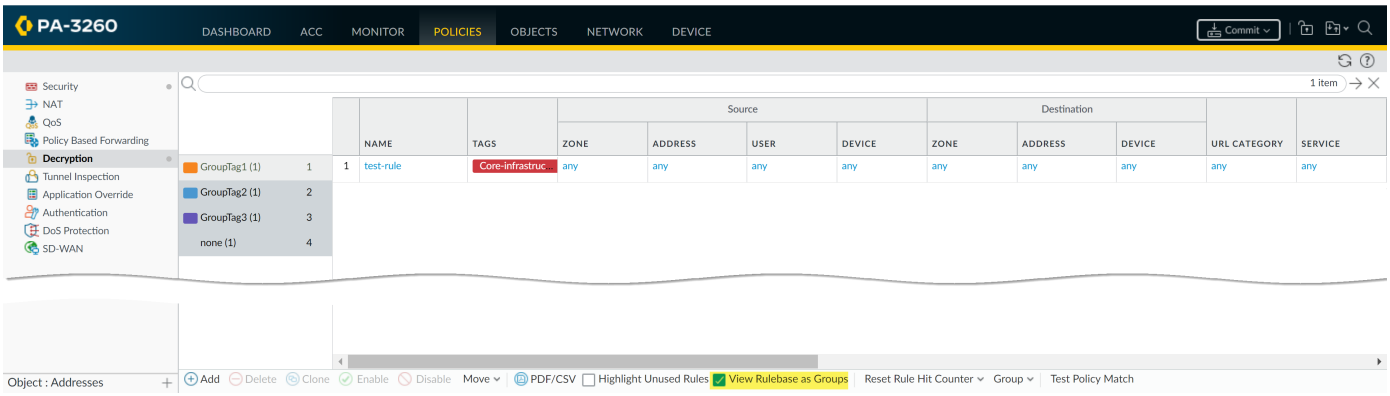



3. **Commit**（提交）更改。

STEP 4 | 以组查看您的策略规则库。

1. （仅限 Panorama）从 **Device Group**（设备组）中选择设备组规则库以查看，或查看所有共享规则。
2. 点击 **Policies**（策略）并选择您在第 2 步中创建了规则的规则库。
3. 选择底部的 **View Rulebase as Groups**（按组查看规则库）选项。

未分配标记组的规则显示为 *None*（无）。

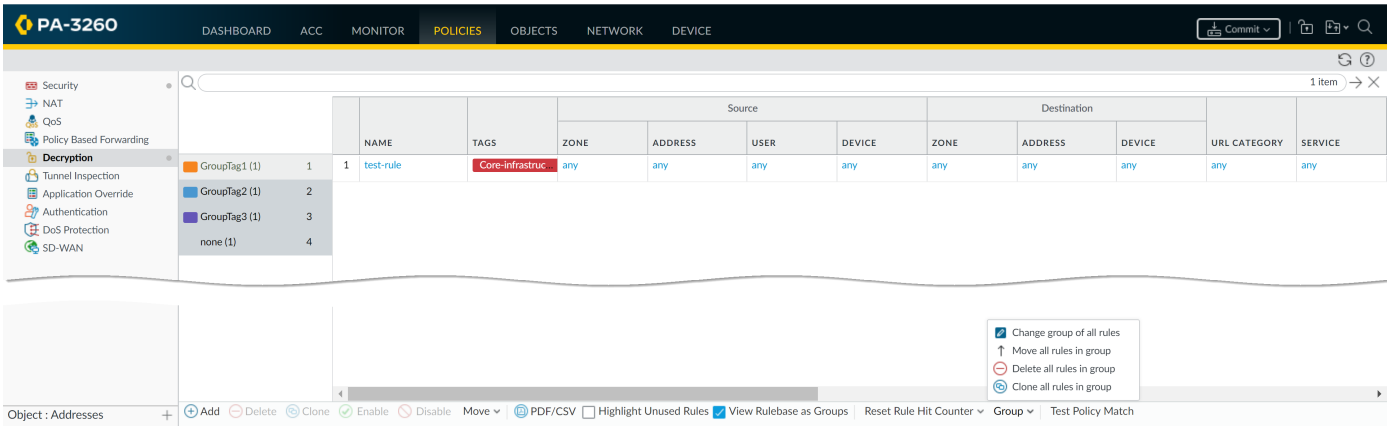



STEP 5 | 根据需要执行分组操作。

1. 点击 **Group**（分组）以对所选标记组内的规则进行分组操作。
   - （仅限 Panorama）**Move rules in group to a different rulebase or device group**（将组内规则移至不同规则库或设备组）— 将所选标记组内的所有策略规则移至前期规则库或后期规则库，或将这些规则移至不同设备组。
   - **Change group of all rules**（更改所有规则组）— 将选中标记组内所有规则移至不同的标记组。
   - **Move all rules in group**（移动组内所有规则）— 移动选中标记组内的所有规则，以更改规则优先级顺序。
   - **Delete all rules in group**（删除组内所有规则）— 删除所选标记组内所有规则。
   - **Clone all rules in group**（克隆组内所有规则）— 克隆所选标记组内所有规则。



© 2019 Palo Alto Networks, Inc.




2. **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 在策略中使用外部动态列表

外部动态列表（之前称为动态阻止列表）是您或另一个源放在外部 web 服务器上的一个文本文件，以便防火墙可以导入对象 — IP 地址、URL、域名 — 在列表的条目上实施策略。更新列表时，防火墙以配置好的间隔动态导入列表并实施策略，不需要更改配置或在防火墙上提交。


- 外部动态列表
- 格式化外部动态列表方针
- 内置外部动态列表
- 将防火墙配置为访问外部动态列表
- 从 Web 服务器检索外部动态列表
- 查看外部动态列表条目
- 从外部动态列表中排除条目
- 在外部动态列表上实施策略
- 查找身份验证失败的外部动态列表
- 禁用外部动态列表的身份验证


## 外部动态列表

外部动态列表是外部 web 服务器上的一个文本文件，以便防火墙可以导入列表中包含的对象 — IP 地址、URL、域、国际移动设备身份码 (IMEI)、国际移动用户识别码 (IMSI)，并实施策略。要在外部动态列表包含的条目上实施策略，您必须在受支持的策略规则或配置文件中引用列表。当引用多个列表时，您可以确定评估顺序的优先顺序，确保最重要的 EDL 能够在到达容量限制之前提交。当您修改列表时，防火墙以配置好的间隔动态导入列表并实施策略，不需要修改配置或在防火墙上提交。如果 Web 服务器无法访问，防火墙将使用最新成功检索的列表实施策略，直到与 Web 服务器的连接修复。如果 EDL 身份验证失败，安全策略将停止实施 EDL。要检索外部动态列表，防火墙使用已配置 **Palo Alto Networks Services**（**Palo Alto Networks** 服务）服务路由的接口。

防火墙支持这些类型的外部动态列表：

- 预先定义 **IP** 地址 — 预先定义 IP 地址列表是其中一种 IP 地址列表，指具有固定或“预先定义”内容的内置动态 IP 列表。。如果您拥有有效的威胁防护许可证，用于防弹托管提供商、已知恶意软件以及高风险 IP 地址的内置外部动态列表均被自动添加到您的防火墙。预先定义 IP 地址列表还可以将使用其中一个内置列表的 EDL 引用为源。因为您不能修改预先定义列表的内容，因此，如果您想添加或排除列表条目，您可以使用预先定义列表作为不同 EDL 的源。
- **Predefined URL List**（预先定义 **URL** 列表）— 这种类型的外部动态列表包含应用程序用于背景服务（例如，更新或证书吊销列表 (CRL) 检查）的预填充 URL，以及防火墙可从身份验证策略中安全排除的预填充 URL。Palo Alto Networks 通过内容更新来修订和维护这种类型的外部动态列表（也称为身份验证门户排除列表）。
- **IP Address**（**IP** 地址）— 防火墙通常针对防火墙上定义为静态对象的源或目标 IP 地址实施策略（请参阅在外部动态列表中实施策略）。如果您需要针对出现的源或目标 IP 地址列表实施策略时具备敏捷度，您可以将类型 IP 地址的外部动态列表用作策略规则中的源或目标地址对象，将防火墙配置为拒绝或允许访问此列表中包含的 IP 地址（IPv4 和 IPv6 地址，IP 范围和 IP 子网）。此外，还可以使用 SD-WAN 策略规则中的源或目标 IP 地址 EDL。防火墙将类型 IP 地址的外部动态列表视为地址对象；列表中包含的所有 IP 地址都作为一个地址对象进行处理。
- **Domain**（域）— 这种类型的外部动态列表使您可以导入自定义域名到防火墙，以通过防间谍配置文件或 SD-WAN 策略规则实施策略。如果您订阅第三方威胁情报馈送，并在了解到恶意域时希望保护您的网络免受新威胁或恶意软件源感染，反间谍配置文件中的 EDL 将非常有用。对于您包含在外部动态列表中的每个域名，防火墙都会创建一个自定义的基于 DNS 的间谍软件签名，使您能够启用 DNS 阻断。基于 DNS 的间谍软件签名是中等强度的类型间谍软件，每个签名都命名为 **`Custom Malicious DNS Query <domain name>`**。您还可以指定可包含指定域的子域的防火墙。例如，如果您的域列表包含 paloaltonetworks.com，则域名的所有较低级别组件（例如，*.paloaltonetworks.com）均包含在列表



© 2019 Palo Alto Networks, Inc.

中。启用这一设置后，给定列表中的每个域都需要一个附加条目，使列表使用的条目数翻倍。有关配置域列表的详细信息，请参阅为自定义域列表配置 DNS Sinkholing。

- **URL** — 这种类型的外部动态列表让您能够敏捷地使网络免于新的威胁源或恶意软件源。防火墙将 URL 的外部动态列表处理为自定义 URL 类别，您可以通过两种方法进行利用：
  - 作为安全策略规则、解密策略规则和 QoS 策略规则中的匹配条件，允许、拒绝、解密、不解密或为自定义类别中的 URL 分配带宽。
  - 在您能定义更多粒度操作的 URL 筛选配置文件中，例如继续、警报或替代，在您附加配置文件到安全策略规则之前（请参阅使用 URL 筛选配置文件中的外部动态列表）。
- **Equipment Identity**（设备身份码）— 您可以在安全策略规则（用于控制连接到 5G 或 4G 网络的设备的流量）中引用国际移动设备身份码 (IMEI) 定义的 IoT 设备外部动态列表。有关在受支持的防火墙型号上配置设备 ID 安全的信息，请参阅《移动网络基础结构入门》。
- **Subscriber Identity**（用户识别码）— 您可以在安全策略规则（用于控制连接到 5G 或 4G 网络的用户的流量）中引用国际移动用户识别码 (IMSI) 的外部动态列表。有关在受支持的防火墙型号上配置用户 ID 安全的信息，请参阅《移动网络基础结构入门》。

对于每个防火墙型号，您最多可以添加 30 个具有唯一源的自定义 EDL，以实施策略。外部动态列表限制不适用于 Panorama。当使用 Panorama 管理为多个虚拟系统启用的防火墙时，如果您超出了防火墙限制，Panorama 上将显示提交错误。源是一个包含 IP 地址或主机名、路径及外部动态列表文件名的 URL。防火墙将匹配 URL（完整字符串）以确定源是否唯一。

如果防火墙未对特定列表类型的列表数量加以限制，则将执行以下限制：

- IP 地址 — PA-5200 系列和 PA-7000 系列防火墙可最多支持共计 150000 个 IP 地址；所有其他型号可最多支持共计 50000 个 IP 地址。不限每个列表的 IP 地址数量。如果防火墙达到所支持的最大数量的 IP 地址限制，就会生成一个系统日志信息。预定义 IP 地址列表中的 IP 地址不会纳入限制。
- URL 和域 — 受支持的 URL 和域最大数量因型号而异。每个列表的 URL 或域条目数量不受限制。通过以下表格了解有关您型号的具体信息：

| 模型 | URL 列表条目限制 | 域列表条目限制 |
|---|---|---|
| PA-5200 系列、PA-7000 系列（采用 PA-7000 20GXM NPC、PA-7000 20GQXM NPC、或 PA-7000 100G NPC 升级）。<br><br>带混合 *NPC* 的 *PA-7000* 设备仅支持标准容量。 | 250,000 | 4,000,000 |
| VM-500、VM-700 | 100,000 | 2,000,000 |
| PA-850、PA-820、PA-3200 系列 | 100,000 | 1,000,000 |
| PA-7000 系列（和采用 PA-7000 20GQ NPC 或 PA-7000 20G NPC 升级的设备）、VM-300 | 100,000 | 500,000 |


© 2019 Palo Alto Networks, Inc.

| 模型 | URL 列表条目限制 | 域列表条目限制 |
| --- | --- | --- |
| PA-220、VM-50、VM-50 (Lite)、VM-100、VM-1000-HV | 50,000 | 50,000 |

仅当列表条目属于策略中引用的外部动态列表时，才会将其纳入防火墙限制。

- 解析列表时，防火墙会跳过不匹配列表类型的条目，忽略超过型号最大支持数的条目。为确保条目不超过限制，请检查策略中当前使用的条目数。选择 *Objects*（对象）> *External Dynamic Lists*（外部动态列表），然后单击 *List Capacities*（列表容量）。
- 外部动态列表必须包含条目。如果要停止使用列表，请从策略规则或配置文件中删除引用，而不是将列表留空。如果列表不包含任何条目，则防火墙无法刷新列表并继续使用其检索到的最后一条信息。
- 最佳做法是，*Palo Alto Networks* 建议在使用多个虚拟系统时使用共享 *EDL*。对于每个虚拟系统，使用带重复条目的单个 *EDL* 占的内存更大，可能会过度利用防火墙资源。
- 对运行多个虚拟系统的防火墙上的 *EDL* 条目计数时，可考虑 *DAG*、虚拟系统数、规则库等其他因素，从而生成更准确的容量消耗列表。从 *PAN-OS 8.x* 版本升级后，这一操作可能会导致容量使用情况出现差异。
- 根据防火墙上启用的功能，由于内存分配更新，在到达 *EDL* 容量限制之前，可能会超出内存使用限制。最佳做法是，*Palo Alto Networks* 建议检查 *EDL* 容量，并在必要时，删除 *EDL* 或将其合并到共享列表中，以减少内存使用。

# 格式化外部动态列表方针

某一个类型的外部动态列表-IP 地址，URL 或域名-只能包括那种类型的条目。预定义 IP 地址列表中的条目符合 IP 地址列表的格式化方针。

- IP 地址列表
- 域列表
- URL 列表

## *IP* 地址列表

外部动态列表可以包含单个 IP 地址，子网地址（地址/掩码），或 IP 地址范围。此外，阻止列表可以包含注释和特殊字符，例如 ***、:、;、#或/**。列表中每行的语法为 **[IP address, IP/Mask, or IP start range-IP end range] [space] [comment]**。

在新行中输入每个 IP 地址/范围/子网；在该列表中不支持 URL 或域。一个子网或一个 IP 地址范围（如 92.168.20.0/24 或 192.168.20.40-192.168.20.50）被视为一个 IP 地址条目，而不是多个 IP 地址。如果您添加注释，注释所在行必须和 IP 地址/范围/子网一样。IP 地址末尾的空格是分隔符，用于将注释和 IP 地址分隔。

IP 地址列表示例：

```
192.168.20.10/32
 2001:db8:123:1::1 #test IPv6 address
 192.168.20.0/24 ; test internal subnet
 2001:db8:123:1::/64 test internal IPv6 range
 192.168.20.40-192.168.20.50
```

对于被拦截的 *IP* 地址，您只能在协议为 *HTTP* 时显示通知页面。



© 2019 Palo Alto Networks, Inc.

## 域列表

您可以在域列表中使用占位符字符以配置单个条目，匹配多个网站的子域、页面、包括整个顶级域，以及匹配特定的 web 页面。

创建域列表条目时，请遵循这些指南：

- 在新行中输入每个域名；在该列表中不支持 URL 或 IP 地址。
- 域名不要使用协议 http:// 或 https:// 作为前缀。
- 您可以使用星号 (*) 表示通配符值。
- 您可以使用插入符号 (^) 表示精确匹配值。
- 以下字符将视为令牌分隔符：. / ? & = ; +

  由一个或两个这种字符分隔的每个字符串就是一个令牌。使用通配符作为令牌占位符，表明特定令牌可以包含任何值。
- 通配符必须是令牌中唯一的字符，但是，条目可以包含多个通配符。
- 每个域条目的最大长度为 255 个字符。

何时使用星号 (*) 通配符：

使用星号 (*) 通配符指示一个或多个变量子域。例如，要在忽略已使用域扩展名（有可能是一个或两个子域，视位置而定）的前提下指定 Palo Alto Network 的网站实施，您可以添加以下条目：**`*.paloaltonetworks.com`**。此条目必须与 docs.paloaltonetworks.com 和 support.paloaltonetworks.com 匹配。

您也可以使用此通配符表示整个顶级域。例如，要指定名称为 .work 的 TLD 实施，您应添加条目：**`*.work`**。其与所有以 .work 结尾的网站匹配。

(*) 通配符仅可加入域条目中。

星号 (*) 示例

| EDL 域列表条目 | 匹配网站 |
|---|---|
| **`*.company.com`** | eng.tools.company.com<br>support.tools.company.com<br>tools.company.com<br>docs.company.com |
| **`*.click`** | 所有以 .click 顶级域结尾的网站。 |

何时使用插入符号 (^) 字符：

使用插入符号 (^) 以表示子域的精确匹配。例如，**`^paloaltonetworks.com`** 仅与paloaltonetworks.com 匹配。此条目不与其他任何站点匹配。

插入符号 (^) 示例

| EDL 域列表条目 | 匹配网站 |
|---|---|
| **`^company.com`** | company.com |
| **`^eng.company.com`** | eng.company.com |



© 2019 Palo Alto Networks, Inc.

## URL 列表

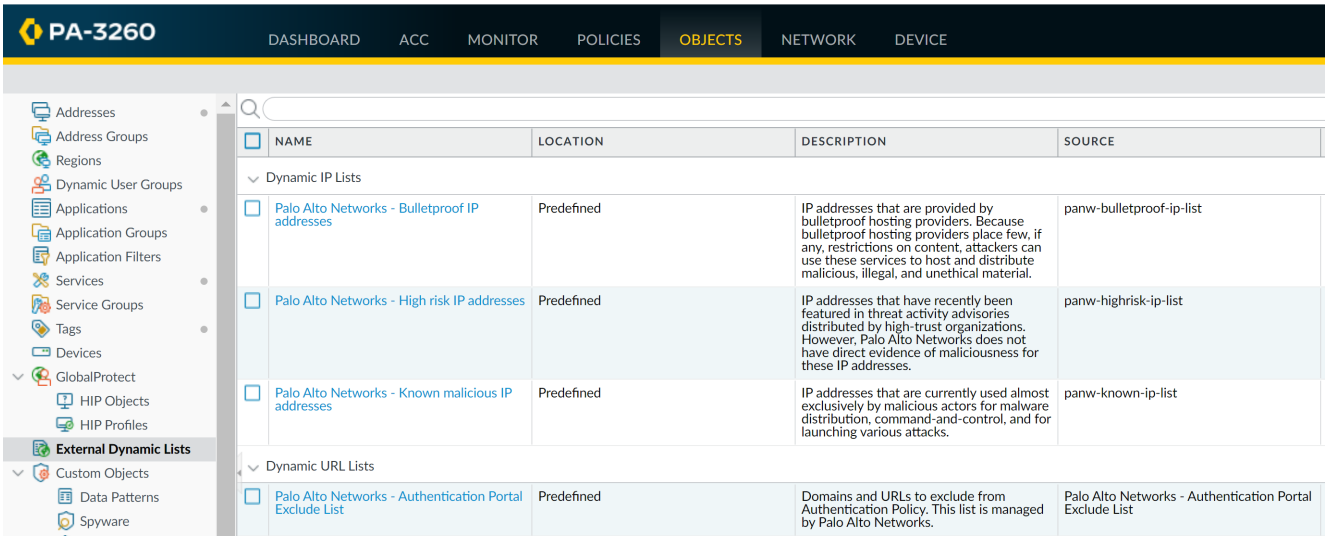
请参阅URL 类别异常。

# 内置外部动态列表

通过激活威胁阻止许可证，Palo Alto Networks 提供多个可用于阻止恶意主机的内置 IP 地址 EDL。

- **Palo Alto Networks** 防弹 **IP** 地址 — 包含防弹托管供应商提供的 IP 地址。由于防弹托管供应商即便有对内容的限制也很少，攻击者可频繁使用这些服务托管和分发恶意、非法和不道德的材料。
- **Palo Alto Networks** 高风险 **IP** 地址 — 包含由受信任的第三方组织发布的威胁通知中提供的恶意 IP 地址。Palo Alto Networks 编制威胁通知列表，但无法直接证明 IP 地址的恶意性。
- **Palo Alto Networks** 已知恶意 **IP** 地址 — 包含根据 WildFire 分析、Unit 42 研究和从遥测收集的数据（与 Palo Alto Networks 共享威胁情报）经过验证的恶意 IP 地址。攻击者几乎完全使用这些 IP 地址来分发恶意软件、启动命令和控制活动，并发动攻击。

防火墙通过内容更新接收这些馈送更新，从而允许防火墙根据 Palo Alto Networks 的最新威胁情报自动实施策略。您无法修改内置列表的内容。按原样使用它们（请参阅在外部动态列表上实施策略），或创建使用列表之一作为源的自定义外部动态列表（请参阅将防火墙配置为访问外部动态列表）并按需从列表中排除条目。




# 将防火墙配置为访问外部动态列表

必须在防火墙和托管外部动态列表的源之间建立连接，然后才能在外部动态列表的条目上实施策略。

STEP 1 | （可选）自定义防火墙用于检索外部动态列表的服务路由。

选择 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Service Route Configuration**（服务路由配置）> **Customize**（自定义）并修改 **External Dynamic Lists**（外部动态列表）服务路由。

防火墙不使用外部动态列表服务路由检索内置外部动态列表；内容更新修改或更新这些列表中的内容（需要激活威胁防护许可证）。

STEP 2 | 找到要与防火墙一起使用的外部动态列表。

- 创建外部动态列表，并将其托管在 Web 服务器上。在空白文本文件中输入 IP 地址、域或 URL。列表中每个条目必须单独占一行。例如：

```
financialtimes.co.in
```



© 2019 Palo Alto Networks, Inc.

`www.wallaby.au/joey`

`www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx`

请参阅外部动态列表的格式化原则，以确保防火墙不会跳过列表条目。为了防止提交错误或无效条目，请勿对任何条目加前缀 http:// 或 https://。

- 使用由另一个源托管的外部动态列表，并验证其是否遵循外部动态列表的格式化原则。

STEP 3 | 选择**Objects**（对象）> **External Dynamic Lists**（外部动态列表）。

STEP 4 | 单击 **Add**（添加）并输入列表的描述性 **Name**（名称）。

STEP 5 | （可选）选择 **Shared**（共享）以和为多个虚拟系统启用的设备上的所有虚拟系统共享列表。默认设置下，会在当前已在 **Virtual Systems**（虚拟系统）下拉列表中选择的虚拟系统上创建对象。



最佳做法是，*Palo Alto Networks* 建议在使用多个虚拟系统时使用共享 *EDL*。对于每个 *vsys*，使用带重复条目的单个 *EDL* 占的内存更大，可能会过度利用防火墙资源。

STEP 6 | （仅 Panorama）选择**Disable override**（禁用替代），确保防火墙管理员不能在本地替代来自 Panorama 通过设置组提交，来自该配置的防火墙的设置。

STEP 7 | 选择列表 **Type**（类型）（例如 **URL List**（**URL** 列表））。

确保列表只包括列表类型的 IP 地址。请参阅验证外部动态列表中的条目已忽略或跳过。

如果使用域列表，您可以选择启用 **Automatically expand to include subdomains**（自动扩展以包含子域），从而包含指定域的子域。例如，如果您的域列表包含 paloaltonetworks.com，则域名的所有较低级别组件（例如，*.paloaltonetworks.com）均包含在列表中。请注意，启用这一设置后，给定列表中的每个域都需要一个附加条目，这使得列表使用的条目数翻倍。

STEP 8 | 输入您刚在 Web 服务器上创建的列表的 **Source**（源）。源必须包括访问列表的完整路径。例如，`https://1.2.3.4/EDL_IP_2015`。

- 如果要创建预定义 IP 外部动态列表，请选择 Palo Alto Networks 恶意 IP 地址馈送作为源。
- 如果创建预定义 URL 外部动态列表，请选择 **panw-auth-portal-exclude-list**作为源。

STEP 9 | 如果列表源使用 SSL 进行安全保护（即具有 HTTPS URL 的列表），请启用服务器身份验证。选择 **Certificate Profile**（证书配置文件）或创建 **New Certificate Profile**（新的证书配置文件），以对托管列表的服务器进行身份验证。您选择的证书配置文件必须具有与正在进行身份验证的服务器上安装的证书相匹配的根证书颁发机构(CA)和中间 CA 证书。



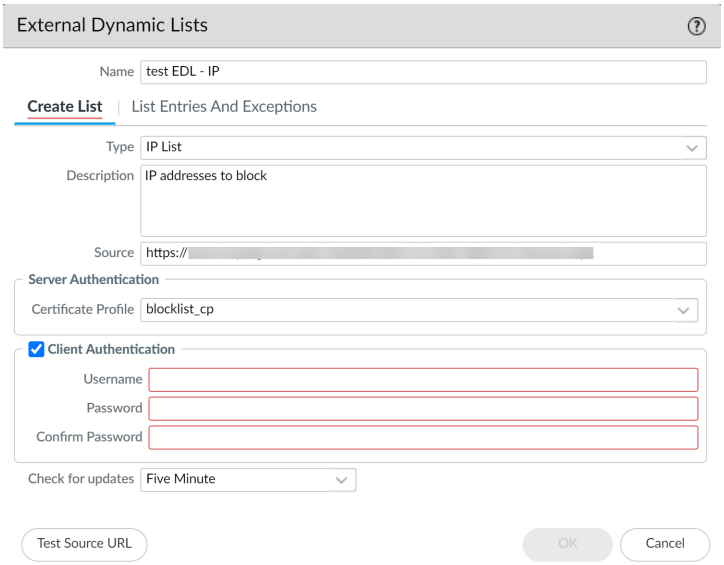
最大化您可以用来执行策略的外部动态列表的数量。使用相同的证书配置文件对从同一源 *URL* 的外部动态列表进行身份验证。如果将不同的证书配置文件分配给同一源 *URL* 的外部动态列表，则防火墙将每个列表作为唯一的外部动态列表进行计数。

STEP 10 | 如果列表源具有 HTTPS URL 并且需要基本的 HTTP 身份验证以访问列表，则启用客户端身份验证。

1. 选择 **Client Authentication**（客户端身份验证）。
2. 输入访问列表的有效 **Username**（用户名）。
3. 输入 **Password**（密码）和 **Confirm Password**（确认密码）。



© 2019 Palo Alto Networks, Inc.




STEP 11 | （Panorama 上不可用或不可用于预定义 URL EDL）单击 **Test Source URL**（测试源 **URL**）来验证防火墙是否可连接至 Web 服务器。

*EDL* 访问需要执行身份验证时，*Test Source URL*（测试源 *URL*）功能将不可用。

STEP 12 | （可选）指定防火墙应为列表执行的 **Check for updates**（检查更新）频率。默认情况下，防火墙每小时检索列表一次，并提交变化。

间隔与最后一次提交有关。所以对于5分钟的间隔，如果最后一次提交在一个小时前，那么提交就在5分钟后。要立即检索列表，请参阅从 Web 服务器检索外部动态列表。

STEP 13 | 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 14 | （可选）EDL 按评估顺序从上到下进行显示。使用页面底部的方向控制更改列表顺序。这样，您可以对列表进行重新排序，确保最重要的 EDL 能够在到达容量限制之前提交。

取消选中 *Group By Type*（按类型分组）后，您只能更改 *EDL* 顺序。

STEP 15 | 在外部动态列表中的条目上实施策略。

如果服务器或客户端身份验证失败，防火墙将根据上次成功检索的外部动态列表停止执行策略。查找身份验证失败的外部动态列表，并查看身份验证失败的原因。

# 从 Web 服务器检索外部动态列表

将防火墙配置为访问外部动态列表时，可以配置防火墙以每小时（默认）、每五分钟、每天、每周或每月从 Web 服务器检索列表。如果您在列表上已添加或删除 IP 地址并需要立即刷新，则使用以下流程来获取更新列表。

STEP 1 | 要根据需要检索列表，请选择 **Objects**（对象）> **External Dynamic Lists**（外部动态列表）。

STEP 2 | 选择您想要刷新的列表，点击**Import Now**（选择导入）。导入列表的任务已排入队列中。



© 2019 Palo Alto Networks, Inc.

STEP 3 | 要查看任务管理器中的任务状态，请查阅管理和监控管理任务。

STEP 4 | （可选）防火墙检索列表后，查看外部动态列表条目。

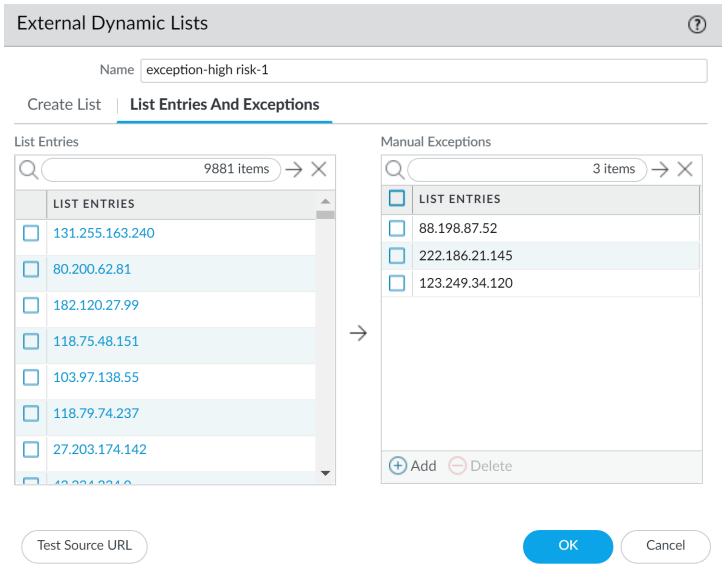
# 查看外部动态列表条目

在外部动态列表上实施策略之前，您可以直接在防火墙上查看外部动态列表的内容，以检查其是否包含某些 IP 地址、域或 URL。显示的条目基于防火墙最近检索到的外部动态列表版本。

STEP 1 | 选择**Objects**（对象）> **External Dynamic Lists**（外部动态列表）。

STEP 2 | 单击您要查看的外部动态列表。

STEP 3 | 单击 **List Entries and Exceptions**（列表条目和例外），然后查看防火墙从列表中检索到的对象。




该列表可能为空，如果：

- 防火墙尚未检索外部动态列表。要强制防火墙立即检索列表，请参阅从 Web 服务器检索外部动态列表。
- 防火墙无法访问承载外部动态列表的服务器。单击 **Test Source URL**（测试源 **URL**）来验证防火墙是否可连接至服务器。

STEP 4 | 在筛选器字段和应用筛选器 (→) 中输入 IP 地址、域或 URL（取决于列表类型），以检查其是否包含在列表中。根据您需要阻止或允许的 IP 地址、域和 URL，从外部动态列表中排除条目。

STEP 5 | （可选）查看 AutoFocus 情报摘要中的列表条目。将鼠标悬停在条目上方以打开下拉列表，然后单击 **AutoFocus**。

# 从外部动态列表中排除条目

查看外部动态列表的条目时，可从列表中排除最多 100 个条目。从外部动态列表中排除条目的功能可让您能够选择在列表中的某些（但不是全部）条目上执行策略。这在您不能编辑外部动态列表的内容（例如 Palo Alto Networks 高风险 IP 地址馈送）时将非常有用，因为该列表来自第三方来源。

STEP 1 | 查看外部动态列表条目。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 最多可以从列表中选择 100 个条目排除，然后单击“提交” (→) 或手动 **Add**（添加）列表异常。

- 如果 Manual Exceptions（手动例外）列表中有重复的条目，则不能将更改内容保存到外部动态列表中。要标识重复条目，请查找带红色下划线的条目。
- 手动异常必须与列表条目完全匹配。例如，如果 IP 地址范围包含列表条目，并且手动将此范围内的单个 IP 地址输入为列表异常，则防火墙将继续对该范围内的所有 IP 地址执行策略。因此，要排除该单个 IP 地址，必须首先确保它是独立的外部动态列表条目，然后手动将相同的 IP 地址添加到例外列表中。

STEP 3 | 单击 **OK**（确定）和 **Commit**（提交），保存您的更改。

STEP 4 | （可选）在外部动态列表上实施策略。

## 在外部动态列表上实施策略

阻止或允许基于外部动态列表中 IP 地址或 URL 的流量，或使用具有 DNS Sinkhole 的动态域列表来防止访问恶意域。



使用外部动态列表在防火墙上执行策略的提示：

- 查看防火墙上外部动态列表（*Objects*（对象）> *External Dynamic Lists*（外部动态列表））时，单击 *List Capacities*（列表容量）将策略中当前使用的 *IP* 地址、域和 *URL* 数量与防火墙支持每个列表类型的条目总数进行对比。
- 为属于策略中使用的一个或多个外部动态列表的域、*IP* 地址或 *URL* 使用全局查找搜索防火墙或 Panorama 管理服务器。这有助于确定导致防火墙阻止或允许某个域、*IP* 地址或 *URL* 的外部动态列表（在安全策略规则中引用）。
- 使用页面底部的方向控制更改 *EDL* 的评估顺序。这样，您可以对列表进行重新排序，确保 *EDL* 中最重要的条目能够在到达容量限制之前提交。



取消选中 *Group By Type*（按类型分组）后，您只能更改 *EDL* 顺序。

- 为自定义域列表配置 DNS Sinkholing。
- 使用 URL 筛选配置文件中的外部动态列表。
- 在安全策略规则中用类型 **URL** 的外部动态列表作为匹配条件。
  1. 选择 **Policies**（策略）> **Security**（安全）。
  2. 点击 **Add**（添加），为规则输入一个描述性**Name**（名称）。
  3. 在**Source**（源）选项卡中选择**Source Zone**（源区域）。
  4. 在 **Destination**（目标）选项卡中选择**Destination Zone**（目标区域）。
  5. 在 **Service/URL Category**（服务/**URL** 类目）选项卡中点击 **Add**（添加），从 URL 类别列表中选择合适的外部动态列表。
  6. 在 **Actions**（操作）选项卡中，将 **Action Setting**（操作设置）设置为 **Allow**（允许）或 **Deny**（拒绝）。
  7. 单击 **OK**（确定）和 **Commit**（提交）。
  8. 验证外部动态列表中的条目已忽略或跳过。

     在防火墙上使用以下 CLI 命令查看列表的详细信息。

```
request
system external-list show type <domain | ip | url> name_of_list
```



© 2019 Palo Alto Networks, Inc.

例如：

```
request system
external-list show type url EBL_ISAC_Alert_List
```

9. 测试是否实施了策略操作。
    1. 查看外部动态列表条目以获取 URL 列表，并尝试从列表中访问 URL。
    2. 验证您定义的操作是否已执行。
    3. 监控防火墙上的活动：
        - 选择 **ACC** 并添加 URL 域作为查看访问 URL 的 Network Activity（网络活动）和 Blocked Activity（阻止的活动）的全局筛选器。
        - 选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 筛选）访问详细的日志视图。

- 在安全策略规则中使用 **IP** 外部动态列表或预先定义的 **IP** 外部动态列表作为源或目标地址对象。

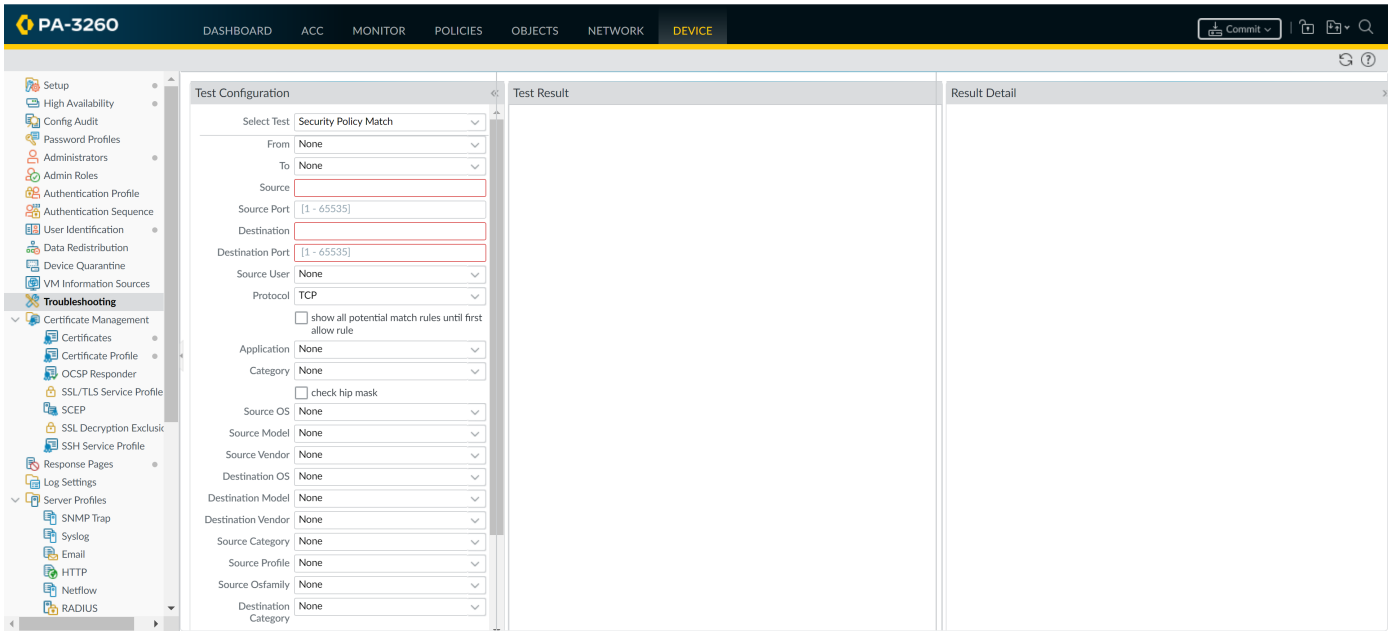
  如果您想部署新的服务器，而且想要允许对新部署的服务器进行访问，而不用要求防火墙提交的话，这项功能很有用。

  1. 选择 **Policies**（策略）> **Security**（安全）。
  2. 单击 **Add**（添加）并为规则提供一个描述性 **Name**（名称）。
  3. 在 **Source/Destination**（源/目标）选项卡中，将要使用的外部动态列表设为 **Source/Destination Address**（源/目标地址）。
  4. 在 Service/ URL Category（服务/URL 类别）选项卡中，确保将 **Service**（服务）设置为 **application-default**。
  5. 在 Actions（操作）选项卡中，将 Action Setting（操作设置）设置为 **Allow**（允许）或 **Deny**（拒绝）。

     如果您希望指定对于特定 *IP* 地址的允许和拒绝操作，可创建单独的动态阻止列表。
  6. 为所有的其他选项保留默认值。
  7. 单击 **OK**（确定）保存更改。
  8. **Commit**（提交）更改。
  9. 测试是否实施了策略操作。
      1. 查看外部动态列表条目以获取外部动态列表，并尝试从列表中访问 IP 地址。
      2. 验证您定义的操作是否已执行。
      3. 选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）并查看会话的日志条目。
      4. 要验证与流量匹配的策略规则，请选择 **Device**（设备）> **Troubleshooting**（故障排除），并执行安全策略匹配测试：


© 2019 Palo Alto Networks, Inc.




- 使用预先定义的 **URL** 外部动态列表将应用程序用于背景流量的良性域从身份验证策略中排除。

  选择 **panw-auth-portal-exclude-list** EDL 类型后，就可以轻松将很多应用程序用于背景流量（例如，更新和其他可信服务）的域从身份验证策略执行中排除。这样可确保防火墙不会阻止这些服务产生的必要流量，也不会中断应用程序维护。

  1. 选择 **Policies**（策略）> **Authentication**（身份验证）。
  2. 在 **Service/URL Category**（服务/**URL** 类别）选项卡中，选择预先定义的 URL EDL 作为 **URL Category**（**URL** 类别）。
  3. 在 **Actions**（操作）选项卡中，选择 **`default-no-captive-portal`** 作为 **Authentication Enforcement**（身份验证实施）。
  4. 单击 **OK**（确定）。
  5. 将规则移动到顶部，使其成为策略中的第一个规则。
  6. **Commit**（提交）更改。

# 查找身份验证失败的外部动态列表

当需要 SSL 的外部动态列表进行客户端或服务器身份验证失败时，防火墙将生成关键严重性的系统日志。因为在身份验证失败后，防火墙将根据外部动态列表停止执行策略，因此日志至关重要。使用以下步骤查看关键的系统日志消息，通知您与外部动态列表相关的身份验证失败。

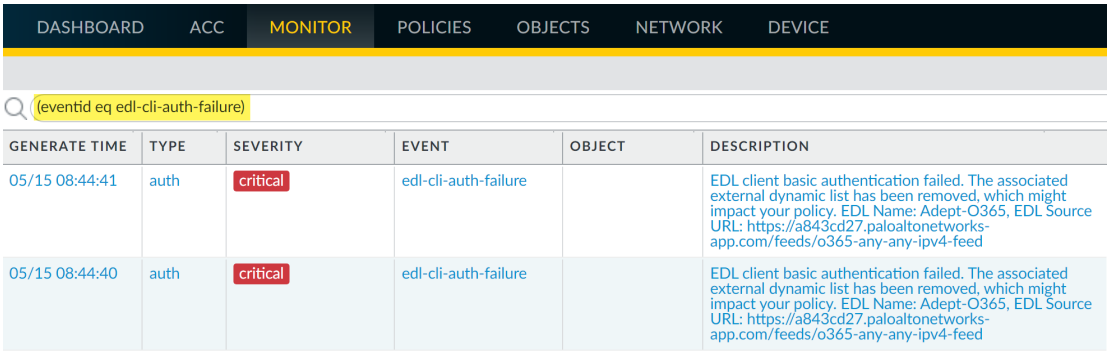
STEP 1 | 选择 **Monitor**（监控）> **Logs**（日志）> **System**（系统）。

STEP 2 | 构建以下筛选器以查看与身份验证失败相关的所有消息，并应用筛选器。有关更多信息，请查看筛选日志的完整工作流程。

- 服务器身份验证失败 — **`(eventid eq tls-edl-auth-failure)`**
- 客户端身份验证失败 — **`(eventid eq edl-cli-auth-failure)`**



© 2019 Palo Alto Networks, Inc.




STEP 3 | 查看系统日志消息。消息说明包括外部动态列表的名称、列表的源 URL 以及身份验证失败的原因。

如果证书已过期，托管外部动态列表的服务器的身份验证将会失败。如果已通过证书吊销列表 (CRL) 或在线证书状态协议 (OCSP) 配置证书配置文件以检查证书吊销状态，则服务器还可能会在发生以下情况下身份验证失败：

- 证书被吊销。
- 证书的吊销状态未知。
- 当防火墙尝试连接到 CRL/OCSP 服务时，连接超时。

有关证书配置文件设置的更多信息，请参阅配置证书配置文件中的步骤。

验证您是否将服务器的根 *CA* 和中间 *CA* 添加到使用外部动态列表配置的证书配置文件中。否则，防火墙将无法对列表进行正常身份验证。

如果您为外部动态列表输入不正确的用户名和密码组合，则客户端身份验证失败。

STEP 4 | （可选）禁用外部动态列表的身份验证是身份验证失败的权宜之计，直至列表所有者更新承载列表的服务器证书为止。

# 禁用外部动态列表的身份验证

Palo Alto Networks 建议您为托管防火墙上配置的外部动态列表的服务器启用身份验证。但是，如果查找身份验证失败的外部动态列表，并且更愿意为这些列表禁用服务器身份验证，则可以通过 CLI 执行此操作。以下步骤仅适用于使用 SSL 保护的外部动态列表（即具有 HTTPS URL 的列表）；防火墙不会对具有 HTTP URL 的列表执行服务器身份验证。

禁用外部动态列表的服务器身份验证也会禁用客户端身份验证。禁用客户端身份验证后，防火墙将无法连接到需要用户名和密码进行访问的外部动态列表。

STEP 1 | 启动 CLI 并切换到配置模式，如下所示：

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

符号从 > 更改为 # 表示您现在正处于配置模式。

STEP 2 | 为列表类型输入相应的 CLI 命令：

- IP 地址


© 2019 Palo Alto Networks, Inc.

```
set external-list <external dynamic list name> type ip certificate-profile
 None
```

- 域

```
set external-list <external dynamic list name> type domain certificate-
profile None
```

- 网址

```
set external-list <external dynamic list name> type url certificate-
profile None
```

STEP 3 | 验证外部动态列表是否已禁用身份验证。

触发列表刷新（请参阅从 Web 服务器检索外部动态列表）。如果防火墙成功检索列表，则禁用服务器身份验证。



© 2019 Palo Alto Networks, Inc.

# 动态注册 IP 地址和标记

为应对扩展、缺乏灵活性和性能的难题，如今网络架构允许根据需要对虚拟机 (VM) 和应用程序进行配置、更改和删除。这种敏捷性给安全管理员带来了挑战，因为他们对动态配置的 VM 和可在这些虚拟资源上启用的众多应用程序的 IP 地址的可见性有限。

防火墙（基于硬件的型号以及 VM 系列型号）支持动态注册 IP 地址、IP 设置（IP 范围和子网）和标记的功能。IP 地址和标记可以直接在防火墙上注册，也可通过 Panorama 注册。您还可以自动删除防火墙日志中包含的源 IP 地址和目标 IP 地址上的标记。



*PAN-OS* 仅支持 *IPv4 IP* 子网和动态地址组内的范围。

您可以使用以下任意选项启用此动态注册过程：

- **Windows User-ID** 代理 — 在您已经部署 User-ID 代理的环境中，您可启用 User-ID 代理来监控最多 100 个 VMware ESXi 和/或 vCenter 服务器。在您配置或修改这些 VMware 服务器上的虚拟机时，代理可检索 IP 地址更改并将它们和防火墙共享。
- **VM** 信息源 — 可让您本地监控防火墙上的 VMware ESXi、vCenter 服务器、AWS-VPC 或 Google Compute Engine，并可在您配置或修改这些源上的虚拟机时检索 IP 地址更改。VM 信息源选项轮询预定义的属性组，并且无需外部脚本即可通过 XML API 注册 IP 地址。请参阅监控虚拟环境中的变化。
- **Panorama** 插件 — 可让您启用 Panorama™ M 系列或虚拟设备，以连接到您的 Azure 或 AWS 公共云环境，并检索订阅或 VPC 中部署的虚拟机的相关信息。随后，Panorama 将 VM 信息注册到已配置通知的受管 Palo Alto Networks 防火墙，之后您可以使用这些属性定义动态地址组，并将其附加到安全策略规则以允许或拒绝来往于这些 VM 的流量。
- **VMware Service Manager**（仅可用于集成 NSX 解决方案）— 集成 NSX 解决方案专为使用 Panorama 自动配置和分发 Palo Alto Networks 下一代 Security Operating Platform® 和提供基于动态上下文的安全策略而设计。NSX Manager 用在该集成解决方案中部署的虚拟机关联的 IP 地址、IP 设置和标记相关的最新信息更新 Panorama。有关该解决方案的信息，请参阅设置 VM-Series NSX 版本防火墙。
- **XML API** — 防火墙和 Panorama 支持使用标准 HTTP 请求的 XML API 来收发数据。您可使用该 API 来向防火墙或 Panorama 注册 IP 地址和标记。API 调用可直接从命令行实用程序（例如 cURL）发起，也可以使用任何支持基于 REST 的服务的脚本或应用程序框架发起。有关详细信息，请参阅 PAN-OS XML API 使用指南。
- **Auto-Tag**（自动标记）— 在防火墙上生成日志时自动标记源 IP 地址或目标 IP 地址，并将 IP 地址和标记映射注册到防火墙或 Panorama 上的 User-ID 代理，或通过 HTTP 服务器配置文件注册到远程 User-ID 代理。例如，每当防火墙生成威胁日志时，您可以配置防火墙以使用特定标记名称标记威胁日志中的源 IP 地址。有关详细信息，请参阅使用自动标记实现安全操作自动化。

  此外，您可以将防火墙配置为在经过配置的时间之后，通过超时动态取消注册标记。例如，您可以将超时配置为与 IP 地址的 DHCP 租用超时相同的持续时间。这样，IP 地址到标记映射与 DHCP 租用同时过期，因此，在重新分配 IP 地址时，您不会在无意间应用策略。

  请参阅将日志转发到 HTTP(S) 目标。

有关创建和使用动态地址组的信息，请参阅在策略中使用动态地址组。

有关动态注册标记所使用的 CLI 命令，请参阅动态 IP 地址和标记的 CLI 命令。



© 2019 Palo Alto Networks, Inc.

# 在策略中使用动态用户组

通过动态用户组，您可以创建一种可为用户异常行为和恶意活动提供自动修复、同时保留用户可见性的策略。创建好组并提交更改后，防火墙会注册用户和关联标记，然后自动更新动态用户组的成员身份。动态用户组成员身份的更新是自动完成的，因此，您可以使用动态用户组（而非静态组对象）响应用户行为的更改或潜在威胁，无需手动更改策略。

为了确定哪些用户可以包含这些成员，动态用户组使用标记作为筛选条件。只要用户符合筛选条件，此用户就可成为动态用户组的成员。基于标记的筛选器使用逻辑 *and* 与 *or* 运算符。每个标记都是您静态或动态注册在源上的一个元数据元素或属性值对。静态标记是防火墙配置的一部分，而动态标记是运行时配置的一部分。因此，如果动态标记已与您在防火墙上提交的策略相关联，就无需提交这些标记的更新

要动态注册标记，您可以使用：

- XML API
- User-ID 代理
- Panorama
- 防火墙 Web 界面

防火墙将动态用户组标记重新分发给包含其他防火墙、Panorama 或专用日志收集器、以及 Cortex 应用程序在内的侦听重新分发代理。

为支持动态用户组标记的重新分发，所有防火墙都必须使用 *PAN-OS 9.1* 接收来自注册源的标记。

防火墙将动态用户组标记重新分发给下一个跃点后，您可以配置日志转发以发送日志到特定服务器。此外，您还可通过日志转发使用自动标记根据日志中事件自动添加或删除动态用户组成员。

STEP 1 | 选择 **Objects**（对象）> **Dynamic User Groups**（动态用户组），并 **Add**（添加）新的动态用户组。

STEP 2 | 定义动态用户组的成员身份。

1. 输入组 **Name**（名称）。
2. （可选）输入组 **Description**（说明）。
3. 通过自动标记 **Add Match Criteria**（添加匹配条件）以定义动态用户组中的成员。
4. （可选）将 **And** 或 **Or**运算符与您想要进行筛选或匹配的标记一起使用。
5. 单击 **OK**（确定）。
6. （可选）选择您想分配到组本身的 **Tags**（标记）。

   此标记显示在 *Dynamic User Group*（动态用户组）的 *Tags*（标记）列中，定义动态组对象，而非组内成员。
7. 单击 **OK**（确定）并 **Commit**（提交）更改。

   如果更新用户组筛选器，必须提交更改以更新配置。

STEP 3 | 根据您将用作匹配条件的日志信息，请通过创建日志转发配置文件或配置日志设置配置自动标记。

- 对于身份验证、数据、威胁、流量、隧道检测、URL 和 WildFire 日志，请创建日志转发配置文件。
- 对于 User-ID、HIP 匹配、GlobalProtect 和 IP 标记日志，请配置日志设置。



© 2019 Palo Alto Networks, Inc.

STEP 4 | （Optional（可选））要在特定时段结束后将动态用户组成员返回到其原始组，请输入 **Timeout**（超时）值（以分钟计，范围为 0-43200，默认为 0）。

STEP 5 | 使用 policy（策略）中的动态用户组管理组成员的流量。

您至少需要创建两条规则：一条规则用于允许初始流量填充动态用户组，另一条规则用于拒绝您想要阻止的活动的流量。为了标记用户，允许流量的规则在规则库中的规则编号必须大于拒绝流量的规则。

1. 从步骤 1 中选择动态用户组作为 **Source User**（源用户）。
2. 创建 **Action**（操作）拒绝动态用户组成员流量的规则。
3. 创建允许流量填充动态用户组成员的规则。
4. 如果在步骤 3 中已配置 **Log Forwarding**（日志转发）配置文件，请选中此配置文件，并将其添加到策略。
5. **Commit**（提交）更改。

STEP 6 | （可选）优化组成员身份，并定义用于用户到标记映射更新的注册源。

如果初始用户到标记映射检索到非成员用户，或是如果初始用户到标记映射不包含本是成员的用户，请修改组成员，以包含您想对其实施策略的用户，并指定源进行映射。

1. 在 **Users**（用户）列中，选择 **more**（更多）。
2. 通过 **Register Users**（注册用户）将用户添加到组，然后选择用于标记和用户到标记映射的 **Registration Source**（注册源）。
   - **Local**（本地）（默认）— 注册用于防火墙上本地动态用户组成员的标记和映射。
   - **Panorama User-ID Agent**（**Panorama User-ID** 代理）— 注册用于连接至 Panorama 的 User-ID 代理上动态用户组成员的标记和映射。如果动态用户组源自 Panorama，则该行显示为黄色，且组名称、说明、匹配条件和标记为只读。但是，您仍可以在组中注册或取消注册用户。
   - **Remote device User-ID Agent**（远程设备 **User-ID** 代理）— 注册用于远程 User-ID 代理上动态用户组成员的标记和映射。要选中此选项，必须配置 HTTP 服务器配置文件。
3. 选择您想通过用于配置组的标记在源上注册的 **Tags**（标记）。
4. （Optional（可选））要在特定时段结束后将动态用户组成员返回到其原始组，请输入 **Timeout**（超时）值（以分钟计，范围为 0-43200，默认为 0）。
5. 根据需要 **Add**（添加）或 **Delete**（删除）用户。
6. （可选）通过 **Unregister Users**（取消注册用户）删除其标记和用户到标记映射。

STEP 7 | 验证防火墙是否正确填充动态用户组中的用户。

1. 确认流量、威胁、URL 筛选、WildFire 提交、数据筛选和隧道检测日志中的 **Dynamic User Group**（动态用户组）列是否正确显示动态用户组。
2. 使用 **`show user group list dynamic`** 命令显示所有动态用户组列表和动态用户组总数。
3. 使用 **`show object registered-user all`** 命令显示已注册成为动态用户组成员的用户列表。
4. 使用 **`show user group name`** ***`group-name`*** 命令显示动态用户组相关信息，例如源类型。


© 2019 Palo Alto Networks, Inc.

# 使用自动标记实现安全操作自动化

自动标记允许防火墙或 Panorama 在接收到匹配特定条件的日志时标记策略对象，并建立 IP 地址到标记或用户到标记映射。例如，每当防火墙生成威胁日志时，您可以配置防火墙以特定标记名称标记威胁日志中的源 IP 地址或源用户。随后，您可以使用这些标记自动填充动态用户组或动态地址组等策略对象，这些对象稍后可用于实现安全、身份验证或解密策略中的安全操作自动化。例如，当您在 **Credential Detected**（检测到的凭据）列中将 URL 日志筛选器创建为 `yes`（是）时，您可以将标记应用至实施身份验证策略的用户，该策略需要用户使用多重因素身份验证 (MFA) 进行身份验证。

通过将 IP 地址到标记映射和用户到标记映射注册到防火墙或 Panorama 上的 PAN-OS 集成 User-ID 代理，或是通过 HTTP 服务器配置文件注册到远程 User-ID 代理，可重新分发您网络中的映射。一旦您将超时配置为日志转发配置文件内置操作的一部分，或是日志转发设置的一部分，防火墙可自动删除（取消注册）与 IP 地址或用户关联的标记。例如，如果防火墙检测到用户凭据可能受到攻击，您可以配置防火墙，要求在给定时段内对此用户进行 MFA 身份验证，然后配置超时，以将用户从 MFA 要求组中删除。

STEP 1 | 根据您想要进行标记的日志类型，请创建日志转发配置文件或配置日志设置，以定义您希望防火墙或 Panorama 处理日志的方式。

- 对于身份验证、数据、威胁、流量、隧道检测、URL 和 WildFire 日志，请创建日志转发配置文件。
- 对于 User-ID、HIP 匹配、GlobalProtect 和 IP 标记日志，请配置日志设置。

STEP 2 | 定义用于确定防火墙或 Panorama 何时将标记添加到策略对象的匹配列表条件。

例如，您可以使用筛选器配置阀值或定义值（例如，用于标识防火墙未映射用户的 **`user eq "unknown"`**）；一旦防火墙达到此阀值或发现此值，防火墙将添加标记。

- 要创建日志转发配置文件，请 **Add**（添加）此文件，然后选择您想根据匹配列表条件进行监控的 **Log Type**（日志类型）（**Objects**（对象）> **Log Forwarding**（日志转发））。
- 要配置日志设置，请 **Add**（添加）您想根据匹配列表条件进行监控的日志类型的日志设置（**Device**（设备）> **Log Settings**（日志设置））。

STEP 3 | 复制并粘贴 **Filter**（筛选器）值，或使用 **Filter Builder**（筛选器生成器）定义日志匹配条件。

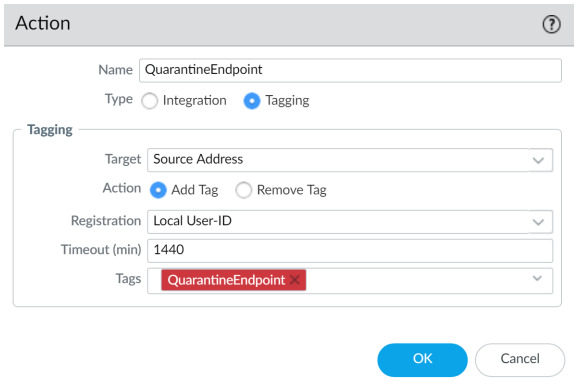
STEP 4 | 添加内置操作以标记策略对象。

1. **Add**（添加）您想让防火墙或 Panorama 在日志包含符合匹配列表条件的条目时执行的 **Built-in Actions**（内置操作）。
2. 输入操作 **Name**（名称）。
3. 选择想要标记的 **Target**（目标）类型（**Destination Address**（目标地址）、**Source Address**（源地址）、**User**（用户）或 **X-Forwarded-For Address**）。
4. 确认 **Action**（操作）为 **Add Tag**（添加标记）。
5. 选择用于标记的 **Registration**（注册）源，以确定防火墙或 Panorama 重新分发 IP 地址到标记映射的方式。
   - **Local User-ID**（本地 **User-ID** ）— 重新分发防火墙或 Panorama 的 User-ID 代理上的 IP 地址到标记映射。
   - **Panorama User-ID**— 重新分发 Panorama 上的 IP 地址到标记映射。
   - **Remote User-ID**（远程 **User-ID**）— 使用 HTTP 服务器配置文件重新分发另一个 User-ID 代理上的 IP 地址到标记映射。如果选中此选项，必须配置 HTTP 服务器配置文件（请参阅步骤 5）。
6. 输入或选择您想添加到策略对象的 **Tags**（标记）。

   您可能需要单击字段之外的区域，或是按下 Enter 以启用 **OK**（确定）按钮。
7. 单击 **OK**（确定）。

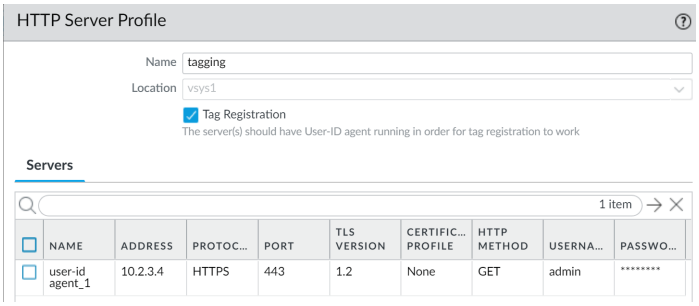


© 2019 Palo Alto Networks, Inc.




STEP 5 | （仅限远程 User-ID）配置 HTTP 服务器配置文件以将日志转发到远程 User-ID 代理。

1. 选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **HTTP**。
2. **Add**（添加）配置文件，并指定服务器配置文件的 **Name**（名称）。
3. （仅限虚拟系统）选择 **Location**（位置）。所有虚拟系统中的配置文件可以 **Shared**（共享），也可以属于特定虚拟系统。
4. 选择 **Tag Registration**（标记注册），使防火墙能将 IP 地址和标记映射注册到远程防火墙上的 User-ID 代理。启用标记注册后，您不能指定有效负载格式。
5. **Add**（添加）服务器连接详情，以访问远程 User-ID 代理，并单击 **OK**（确定）。




6. 选择您创建的日志转发配置文件，然后选择此服务器配置文件作为 **Remote User-ID**（远程 **User-ID**）标记 **Registration**（注册）的 HTTP 服务器配置文件。

STEP 6 | 定义您想应用标记的策略对象。

1. 创建或选择下列其中一个策略对象：动态地址组、在策略中使用动态用户组、地址、地址组、区域、策略规则、服务或服务组。
2. 输入您想根据 **Match**（匹配）条件应用至对象的标记。

   确认此标记与步骤 4 中的标记一致。

STEP 7 | 添加标记过的策略对象到您的策略中。

此工作流使用安全策略作为示例，但您还可以在身份验证策略中使用标记过的策略对象。

1. 选择 **Policies**（策略）> **Security**（安全）。
2. 单击 **Add**（添加），然后为策略输入 **Name**（名称）和 **Description**（说明）（可选）。
3. 添加流量开始的 **Source Zone**（源区域）。
4. 添加流量终止的 **Destination Zone**（目标区域）。
5. 选择您在步骤 5.1 中创建的 **Source**（源）对象。
6. 选择规则是 **Allow**（允许）还是 **Deny**（拒绝）流量。

STEP 8 | 如果日志已配置为转发配置文件，请将其分配到您的安全策略中。


© 2019 Palo Alto Networks, Inc.

您可以为每个策略分配一个日志转发配置文件，但是，每个配置文件可采取多种分配方法和操作。例如，请参阅在策略中使用动态地址组。

STEP 9 | **Commit**（提交）更改。

STEP 10 | （可选）配置超时，以在指定时间结束后删除策略对象中的标记。

指定防火墙删除策略对象中的标记之前花费的时间量（以分钟计）。范围为 0-43,200。如果将超时值设为零，则 IP 地址到标的映射不会超时，且必须通过显式操作删除。如果将超时值设为最大值 43,200 分钟，则防火墙在 30 天后删除标记。



您不能通过 *Remove Tag*（删除标记）操作配置超时。

1. 选择日志转发配置文件。
2. **Add**（添加）或编辑其中一个 **Built-in Actions**（内置操作）。
3. 指定 **Timeout**（超时）（以分钟计）。指定时间结束后，防火墙或 Panorama 将删除标记。



将 *IP* 标记超时设为与 *IP* 地址的 *DHCP* 租用超时一样的值。这样，*IP* 地址到标记映射与 *DHCP* 租用同时过期，因此，在重新分配 *IP* 地址时，您不会在无意间应用策略。

4. 单击 **OK**（确定）并 **Commit**（提交）更改。



© 2019 Palo Alto Networks, Inc.

# 监控虚拟环境中的变化

要保护应用程序并在不断出现新用户和服务器的环境中阻止威胁，您的安全策略必须敏捷。要变得敏捷，防火墙必须能了解新的或修改的 IP 地址并在无需在防火墙上进行配置更改的情况下不断应用策略。

该功能通过在防火墙上 **VM Information Sources**（**VM** 信息源）和**Dynamic Address Groups**（动态地址组）功能之间进行协调来提供。防火墙和 Panorama 提供自动的方式来收集每个监控的源上虚拟机（或来宾）库存的信息，并创建策略对象，这些对象与网络上的动态更改保持同步。

- 启用 VM 监控以跟踪虚拟网络上的更改
- 云平台虚拟机上受监控的属性
- 在策略中使用动态地址组

## 启用 VM 监控以跟踪虚拟网络上的更改

VM 信息源提供自动的方法来收集每个监控源（主机）上虚拟机 (VM) 的信息；防火墙可监控 VMware ESXi、vCenter Server、AWS-VPC、Microsoft Azure VNet 以及 Google Cloud。在部署或移动虚拟机（或来宾）后，防火墙会将预先定义的属性（或元数据元素）集作为标记收集；然后这些标记可用于定义动态地址组（请参阅在策略中使用动态地址组）并根据策略匹配。

您可以直接配置防火墙或使用 Panorama 模板最多监控 10 个 VM 信息源。**VM Information Sources**（**VM** 信息源）提供简便配置并可让您监控预先定义的 16 元数据元素或属性集。相关列表，请参阅云平台虚拟机上受监控的属性。默认设置下，防火墙和监控的源之间的流量使用防火墙上的管理 (MGT) 端口。

- 监控作为 VM 系列 NSX 版解决方案一部分的 *ESXi* 主机时，请使用动态地址组来了解虚拟环境中的变化，而非使用 *VM* 信息源。对于 *VM* 系列 *NSX* 版解决方案，*NSX Manager* 将为 *Panorama* 提供 *IP* 地址所属 *NSX* 安全组的相关信息。来自 *NSX Manager* 的信息将为定义动态地址组中的匹配条件提供完整的上下文。由于此信息将服务配置文件 *ID* 用作专有属性，所以当不同的 *NSX* 安全组中存在重复 *IP* 地址时，可确保策略得以正确实施。最多可在 *IP* 地址中注册 *32* 个标记（从 *vCenter* 服务器和 *NSX Manager*）。
- 要监控 *Azure* 部署中的虚拟机（而不是 *VM* 监控源），您需要部署能够在 *Azure* 公共云中虚拟机上运行的 VM 监控脚本。此脚本收集 *Azure* 资产的 *IP* 地址到标记映射信息，并将其发布到您在脚本中指定的防火墙和相应的虚拟系统。
- 对于 *Panorama 8.1.3* 及更高版本，还可以使用 *AWS* 或 *Azure* 的 *Panorama* 插件来检索 *VM* 信息，并将其注册到受管防火墙。有关详细信息，请参阅云平台虚拟机上受监控的属性。

STEP 1 | 启用 VM 监控。

每个防火墙或支持多虚拟系统的防火墙上的每个虚拟系统最多可配置 *10* 个*VM* 信息源。

如果您的防火墙在高可用性配置中配置：

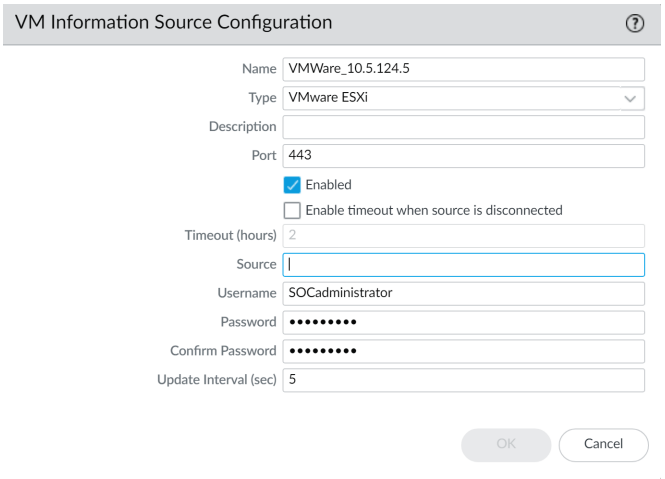
- 在主动/被动设置中，只有主动的防火墙可以监控 VM 源。
- 在主动/被动设置中，只有优先级值为“主要”的防火墙可以监控 VM 源。

1. 选择 **Device**（设备）> **VM Information Sources**（**VM** 信息源）。此示例显示如何添加 VMware ESX(i) 或 vCenter Server。
2. 单击**Add**（添加），并输入以下信息：
   - **Name**（名称）用于标识要监控的源。
   - 选择 **Type**（类型）来指示源是 **AWS VPC**、**Google Compute Engine**实例、**VMware ESX(i)** 服务器、或 **VMware vCenter** 服务器。


© 2019 Palo Alto Networks, Inc.

显示字段由选中的类型决定。

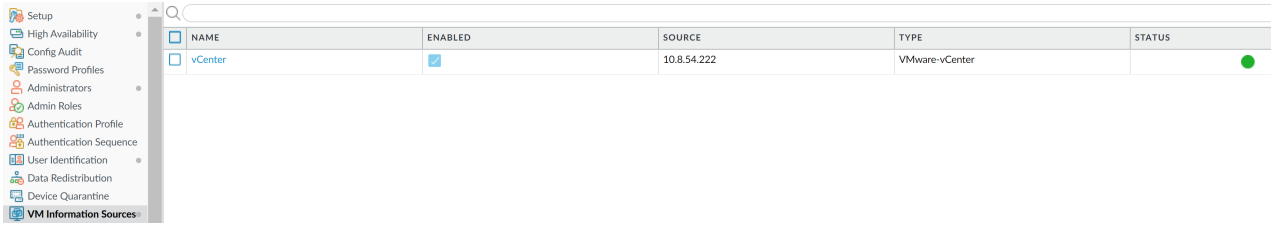
- 指定源要侦听的 **Port**（端口）。
- 要更改默认值，请选择复选框**Enable timeout when the source is disconnected**（源中断时启用超时）并指定一个值。到达指定限制时，或者如果主机无法访问或无响应，防火墙将关闭源连接。
- 输入凭据（**Username**（用户名）和 **Password**（密码））来向上面指定的服务器进行验证。
- 定义 **Source**（源）— 主机名或 IP 地址。
- （可选）将 **Update interval**（更新间隔）修改为 5-600 秒之间的值。默认情况下，防火墙会每隔 5 秒轮询一次。每隔 60 秒将对 API 调用进行排队和检索，从而更新需要的时间可能最长为 60 秒加上配置的轮询间隔。




- 单击**OK**（确定）并**Commit**（提交）更改。
- 验证连接 **Status**（状态）是否显示为已连接。

STEP 2 | 验证连接状态。

验证连接 **Status**（状态）是否显示为已连接。




如果连接状态为挂起或断开，则检查源是否正常工作，并且防火墙能够访问源。如果您使用 MGT 之外的端口来和监控的源通信，则必须更改服务路由（**Device**（设备）> **Setup**（设置）> **Services**（服务），单击 **Service Route Configuration**（服务路由配置）链接并修改 **VM Monitor**（**VM** 监控）服务的 **Source Interface**（源接口））。

# 云平台虚拟机上受监控的属性

在私有云或公共云中部署或删除虚拟机时，可以在下一代防火墙上使用 Panorama 插件、VM 监控脚本或 VM 信息源来监控虚拟环境中虚拟机 (VM) 的变化。

**VM** 信息源 — 对于硬件或 VM 系列防火墙，在对 AWS、ESXi 或 vCenter Server 或 AWS 等受监控源上配置的来宾进行配置或修改时，可以监控虚拟机实例，并检索更改。对于每个防火墙和/或虚拟机（如果防火墙具有多个虚拟系统功能），可以最多配置 10 个源。关于 VM 信息源和动态地址组如何同步工作，并使您能够监控虚拟环境变化的信息，请参阅《VM 系列防火墙部署指南》。如果您的防火墙采用高可用性配置：



© 2019 Palo Alto Networks, Inc.

- 在主动/被动设置中，只有主动的防火墙可以监控 VM 信息源。
- 在主动/主动设置中，只有主要防火墙可以监控 VM 信息源。

**Panorama** 插件 — 对于硬件设备或虚拟设备运行版本为 8.1.3 的 Panorama，可以为 Microsoft Azure 和 AWS 安装插件。您可以通过此插件将 Panorama 连接至 Azure 公共云订阅或 AWS VPC，并检索虚拟机的 IP 地址到标记映射。然后，Panorama 将 VM 信息注册到您配置用于通知的 Palo Alto Networks® 受管防火墙。

使用以下部分查看每个云供应商支持的选项，以及监控用于创建动态地址组的虚拟机属性：

- VMware ESXi
- Amazon Web Services (AWS)
- Microsoft Azure
- Google

## VMware ESXi

受监控 ESXi 或 vCenter 服务器上的每一个 VM 都必须安装并运行 VMware 工具。VMware 工具能够收集分配给各个 VM 的 IP 地址和其他值。



监控作为 *VM* 系列 *NSX* 版解决方案一部分的 *ESXi* 主机时，请使用动态地址组来了解虚拟环境中的变化（而非使用 *VM* 信息源）。对于 *VM* 系列 *NSX* 版解决方案，*NSX Manager* 将为 *Panorama* 提供 *IP* 地址所属 *NSX* 安全组的相关信息。来自 *NSX Manager* 的信息将为定义动态地址组中的匹配条件提供完整的上下文。由于此信息将服务配置文件 *ID* 用作专有属性，所以当不同的 *NSX* 安全组中存在重复 *IP* 地址时，可确保策略得以正确实施。

最多可在 *IP* 地址中注册 *32* 个标记（从 *vCenter* 服务器和 *NSX Manager*）。

为了收集分配给受监控 VM 的值，使用防火墙上的 VM 信息源来监控以下 ESXi 预定义属性集：

| VMware 源所监控的属性 |
| --- |
| UUID |
| 姓名 |
| 来宾操作系统 |
| VM 状态 — 电源状态可以为关闭、开启、待机和未知。 |
| 注释 |
| 版本 |
| 网络 — 虚拟交换机名称、端口组名和 VLAN ID |
| 容器名称 — vCenter 名称、数据中心对象名称、资源池名称、集群名称、主机、主机 IP 地址。 |

## Amazon Web Services (AWS)

在 AWS VPC 中配置或修改虚拟机时，有两种方法可以监控这些实例，并检索用作动态地址组内匹配条件的标记。

- **VM** 信息源 — 在下一代防火墙上，您最多可以监控共计 32 个标记，包括 14 个预定义和 18 个用户定义的表项值对（标记）。可以将以下属性（或标记名称）用作动态地址组的匹配条件。


© 2019 Palo Alto Networks, Inc.

- **Panorama 上的 AWS 插件** — AWS 的 Panorama 插件允许您将 Panorama 连接到 AWS VPC，并检索 AWS 虚拟机的 IP 地址到标签映射。然后，Panorama 将 VM 信息注册到您配置用于通知的 Palo Alto Networks® 受管防火墙。使用插件后，Panorama 最多可为每个虚拟机检索共计 32 个标记，包括 11 个预定义标记和最多 21 个用户定义的标记。

| AWS-VPC 所监控的属性 | 防火墙上的 VM 信息源 | Panorama 上的 AWS 插件 |
|---|---|---|
| 架构 | 是 | 否 |
| 来宾操作系统 | 是 | 否 |
| AMI ID | 是 | 是 |
| IAM 实例配置文件 | 否 | 是 |
| 实例 ID | 是 | 否 |
| 实例状态 | 是 | 否 |
| 实例类型 | 是 | 否 |
| 密钥名称 | 是 | 是 |
| 所有者 ID | 否 | 是 |
| 放置 — 租户 | 是 | 是 |
| 放置 — 资源组 | 是 | 是 |
| 放置 — 可用区域 | 是 | 是 |
| 私有 DNS 名称 | 是 | 否 |
| 公共 DNS 名称 | 是 | 是 |
| 子网 ID | 是 | 是 |
| 安全组 ID | 否 | 是 |
| 安全组名称 | 否 | 是 |
| VPC ID | 是 | 是 |
| 标记（密钥，值） | Yes;<br>最多可支持 18 个用户定义标记。用户定义的标记按字母顺序排序，且前 18 个标记可用于防火墙。 | Yes;<br>最多支持 21 个用户定义的标记。用户定义的标记按字母顺序排序，且前 21 个标记可用于 Panorama 和防火墙。 |



© 2019 Palo Alto Networks, Inc.

## Microsoft Azure

对于 Azure 上的 VM 监控，您需要检索 Azure VM 的 IP 地址到标签映射，并将其用作动态地址组内的匹配条件。Microsoft Azure 的 Panorama 插件允许您将 Panorama 连接到您的 Azure 公共云订阅，并检索 Azure 虚拟机的 IP 地址到标签映射。Panorama 可为每台虚拟机共计检索 26 个标签，即 11 个预定义标签和最多 15 个用户定义标签，并将 VM 信息注册到您配置用于通知的托管 Palo Alto Networks® 防火墙。

您可以使用 Azure 的 Panorama 插件监控 Microsoft Azure 部署内的以下虚拟机属性集。

| Microsoft Azure 上受监控的属性 | Panorama 上的 Azure 插件 |
|---|---|
| VM 名称 | 是 |
| VM 大小 | 否 |
| 网络安全组名称 | 是 |
| OS 类型 | 是 |
| OS 发行商 | 是 |
| OS 产品 | 是 |
| OS SKU | 是 |
| 子网 | 是 |
| VNet | 是 |
| Azure 区域 | 是 |
| 资源组名称 | 是 |
| 订阅 ID | 是 |
| 用户定义的标记 | 是<br>最多支持 15 个用户定义的标记。用户定义标记按字母顺序排序，前 15 个标记可用于 Panorama 和防火墙。 |

## Google

使用下一代防火墙上的 VM 信息源监控以下 Google Compute Engine (GCE) 的预定义属性集。

防火墙不支持高可用性。

| Google Compute Engine 上受监控的属性 |
|---|
| VM 主机名 |



© 2019 Palo Alto Networks, Inc.

| Google Compute Engine 上受监控的属性 |
| --- |
| 机器类型 |
| 项目 ID |
| 源（操作系统类型） |
| STATUS（状态） |
| 子网络 |
| VPC 网络 |

## 在策略中使用动态地址组

在策略中使用了动态地址组。这可让您创建自动适应更改（添加、移动或删除服务器）的策略。这也可实现根据定义服务器在网络、操作系统上角色的标记或其处理的不同类型的流量将不同规则应用至相同服务器的灵活性。

动态地址组使用标记作为筛选条件来确定其成员。筛选器使用逻辑 *and* 及 *or* 运算符。匹配筛选条件的所有 IP 地址或地址组成为动态地址组的成员。可以静态方式在防火墙上定义标记和/或动态地向防火墙注册。静态和动态标记之间的差异在于静态标记是防火墙上配置的一部分，而动态标记则是运行时配置的一部分。这意味着无需提交即可更新动态标记；但标记必须由策略中引用的动态地址组使用，并且必须在设备上提交策略。

要动态注册标记，您可在防火墙或 User-ID 代理上使用 XML API 或 VM 监控代理。每个标记是在防火墙或 Panorama 上注册的元数据元素或属性值对。例如 IP1 {tag1, tag2,.....tag32}，其中 IP 地址和相关的标记作为列表保留；每个注册的 IP 地址最多可有 32 个标记，例如它所属的操作系统、数据中心或虚拟交换机。接收 API 调用后，防火墙注册 IP 地址和相关标记，并自动更新动态地址组的成员信息。

可为每个型号注册的最大 IP 地址数目不同。使用以下表格了解有关您型号的具体信息：

| 模型 | 动态注册的 IP 地址的最大数目 |
| --- | --- |
| M 系列和 Panorama 虚拟设备 | 500，000 |
| PA-5200 系列、VM-7000 SMC-B 系列 | 500，000 |
| VM-500、VM-700 | 300，000 |
| PA-3200 系列、VM-300 | 200，000 |
| PA-7000 系列 | 100，000 |
| PA-850、 VM-100 | 2，500 |
| PA-820、PA-220、VM-50 | 1，000 |



如果将一个 *IP* 集（例如 *IP* 范围或子网）计入到各防火墙型号支持的最大注册 *IP* 地址数中，该 *IP* 集将被视为一个已注册 *IP* 地址。



© 2019 Palo Alto Networks, Inc.

以下示例展示了动态地址组如何简化网络安全实施。示例工作流显示了如何：

- 在防火墙上启用 VM 监控代理，由此监控 VMware ESX(i) 主机或 vCenter 服务器并注册 VM IP 地址和相关标记。
- 创建动态地址组并定义要筛选的标记。在该示例中，创建了两个地址组。其中一个仅筛选动态标记，另一个则筛选静态和动态标记以填写组成员。
- 在防火墙上验证是否已填充动态地址组的成员。
- 在策略中使用动态地址组。该示例使用两个不同的安全策略：
  - 部署为 FTP 服务器的所有 Linux 服务器的安全策略；该规则匹配动态注册的标记。
  - 部署为 Web 服务器的所有 Linux 服务器的安全策略；该规则匹配使用静态和动态标记的动态地址组。
- 验证动态地址组的成员是否随着新 FTP 或 Web 服务器的部署而更新。这可确保也在这些新的虚拟机上实施安全规则。

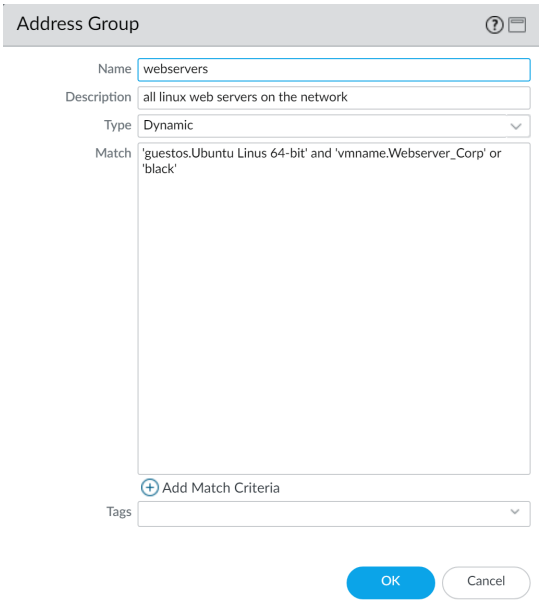
STEP 1 | 启用 VM 源监控。

请参阅启用 VM 监控以跟踪虚拟网络上的更改。

STEP 2 | 在防火墙上创建动态地址组。

查看教程观看功能的大视图。

1. 登录防火墙的 Web 界面。
2. 选择 **Object**（对象）> **Address Groups**（地址组）。
3. 单击 **Add**（添加），然后为地址组输入 **Name**（名称）和 **Description**（说明）。
4. 选择 **Dynamic**（动态）作为 **Type**（类型）。
5. 定义匹配条件。您可将动态和静态标记选择为匹配条件来填充组成员。单击 **Add Match Criteria**（添加匹配条件），并选择 **And** 或 **Or** 运算符以及您想要筛选或排除的属性，然后单击 **OK**（确定）。




6. 单击 **Commit**（提交）。

STEP 3 | 该示例中每个动态地址组中的匹配条件如下：

ftp_server：在来宾操作系统 “Linux 64-bit”上匹配并注释为 “ftp”（“guestos.Ubuntu Linux 64-bit”和“annotation.ftp”）。


© 2019 Palo Alto Networks, Inc.

Web 服务器：以两个条件匹配 - 黑色标记或来宾操作系统是否为 Linux 64 位并且服务器的名称为 Web_server_Corp。（“guestos.Ubuntu Linux 64-bit”和“vmname.WebServer_Corp”或“black”）

| | NAME | LOCATION | MEMBERS COUNT | ADDRESSES |
|---|---|---|---|---|
| ☐ | ftp_servers | | dynamic | more... |
| ☐ | Web_servers | | dynamic | more... |

Click to see members/registered IP addresses

STEP 4 | 在策略中使用动态地址组。

查看教程。

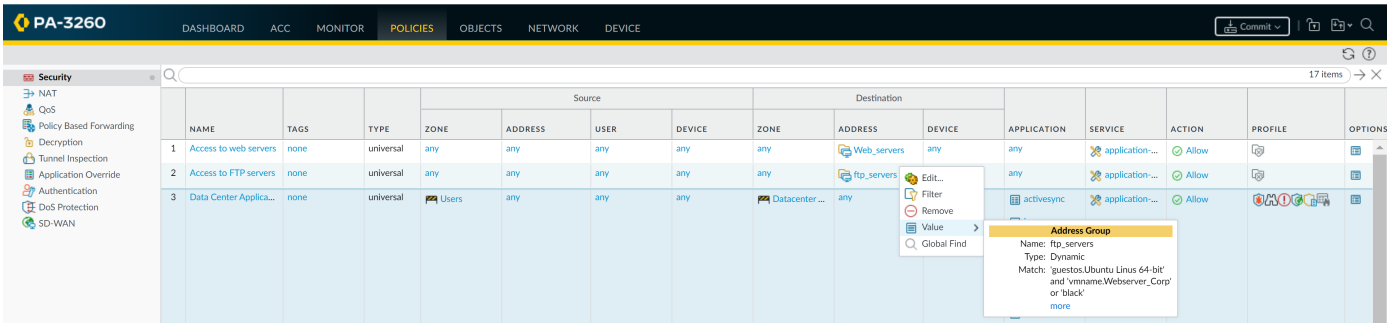
1. 选择 **Policies**（策略）> **Security**（安全）。
2. 单击 **Add**（添加），然后为策略输入 **Name**（名称）和 **Description**（说明）。
3. 添加 **Sources Zone**（源区域）来指定产生流量的区域。
4. 添加流量于其中终止的 **Destination Zone**（目标区域）。
5. 对于 **Destination Address**（目标地址），选择刚创建的动态地址组。
6. 为流量指定操作 - **Allow**（允许）或 **Deny**（拒绝），并可选地将默认安全配置文件附加至规则。
7. 重复步骤 1 至 6 来创建另一个策略规则。
8. 单击 **Commit**（提交）。

STEP 5 | 该示例说明了如何创建两个策略：一个用于访问 FTP 服务器，另一个用于访问 Web 服务器。

| | NAME | TAGS | TYPE | Source ZONE | Source ADDRESS | Source USER | Source DEVICE | Destination ZONE | Destination ADDRESS | Destination DEVICE | APPLICATION | SERVICE | ACTION | PROFILE | OPTI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Access to web servers | none | universal | any | any | any | any | any | Web_servers | any | any | application-... | Allow | | |
| 2 | Access to FTP servers | none | universal | any | any | any | any | any | ftp_servers | any | any | application-... | Allow | | |

STEP 6 | 在防火墙上验证是否已填充动态地址组的成员。

1. 选择 **Policies**（策略）> **Security**（安全），并选择规则。
2. 选择地址组链接旁的下拉箭头，然后选择 **Value**（值）。您还可以验证匹配条件是否准确。




3. 单击more（更多）链接，然后验证是否显示已注册 IP 地址列表。

   将对属于此地址组，并在此显示的所有 IP 地址实施策略。

如果您想删除注册的所有 *IP* 地址，请使用 *CLI* 命令 ***debug object registered-ip clear all***，然后在清除标记后重启防火墙。



© 2019 Palo Alto Networks, Inc.

# 动态 IP 地址和标记的 CLI 命令

防火墙和 Panorama 上的命令行界面可让您详细查看在其中动态注册标记和 IP 地址的不同源。它还可让您审核注册和未注册的标记。以下示例说明了 CLI 中的功能。

| 示例 | CLI 命令 |
| --- | --- |
| 查看匹配标记 `state.poweredOn` 的所有注册的 IP 地址或未标记为 `vSwitch0` 的地址。 | **show log iptag tag_name equal state.poweredOn**<br>**show log iptag tag_name not-equal switch.vSwitch0** |
| 查看由 VM 信息源发起的具有名称 `vmware1` 并标记为 `poweredOn` 的所有动态注册的 IP 地址。 | **show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all**<br>registered IP Tags<br>---------- ----------<br>fe80::20c:29ff:fe69:2f76 "state.poweredOn"<br>10.1.22.100 "state.poweredOn"<br>2001:1890:12f2:11:20c:29ff:fe69:2f76"state.poweredOn"<br>fe80::20c:29ff:fe69:2f80 "state.poweredOn"<br>192.168.1.102 "state.poweredOn"<br>10.1.22.105 "state.poweredOn"<br>2001:1890:12f2:11:2cf8:77a9:5435:c0d"state.poweredOn"<br>fe80::2cf8:77a9:5435:c0d "state.poweredOn" |
| 清除所有从特定 VM 监控源获取的 IP 地址以及标记而不和源断开连接。 | **debug vm-monitor clear source-name *<name>*** |
| 显示通过所有源注册的 IP 地址。 | **show object registered-ip all** |
| 显示通过所有源注册的 IP 地址计数。 | **show object registered-ip all option count** |
| 清除通过所有源注册的 IP 地址。 | **debug object registered-ip clear all** |
| 添加或删除使用 XML API 注册的给定 IP 地址的标记。 | **debug object registered-ip test [<register/unregister>] <ip/netmask><tag>** |
| 查看通过特定信息源注册的所有标记。 | **show vm-monitor source source-name vmware1 tag all**<br>vlanId.4095<br>vswitch.vSwitch1<br>host-ip.10.1.5.22<br>portgroup.TOBEUSED |



© 2019 Palo Alto Networks, Inc.

| 示例 | CLI 命令 |
| --- | --- |
| | hostname.panserver22<br>portgroup.VM Network 2<br>datacenter.ha-datacenter<br>vlanId.0<br>state.poweredOn<br>vswitch.vSwitch0<br>vmname.Ubuntu22-100<br>vmname.win2k8-22-105<br>resource-pool.Resources<br>vswitch.vSwitch2<br>guestos.Ubuntu Linux 32-bit<br>guestos.Microsoft Windows Server 2008 32-bit<br>annotation.<br>version.vmx-08<br>portgroup.VM Network<br>vm-info-source.vmware1<br>uuid.564d362c-11cd-b27f-271f-c361604dfad7<br>uuid.564dd337-677a-eb8d-47db-293bd6692f76<br>Total: 22 |
| 查看通过特定数据源注册的所有标记，例如通过防火墙上的 VM 监控代理、XML API、Windows User-ID 代理或 CLI。 | • 要查看通过 CLI 注册的标记：<br>**show log iptag datasource_type equal unknown**<br>• 要查看通过 XML API 注册的标记：<br>**show log iptag datasource_type equal xml-api**<br>• 要查看通过 VM 信息源注册的标记：<br>**show log iptag datasource_type equal vm-monitor**<br>• 要查看通过 Windows User-ID 代理注册的标记：<br>**show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent** |
| 查看为特定 IP 地址注册的所有标记（在所有源上）。 | **debug object registered-ip show tag-source ip ip_address tag all** |



© 2019 Palo Alto Networks, Inc.

# 对上游设备背后的端点和用户实施策略

如果您在您网络上的用户和防火墙之间部署了显式代理服务器或负载均衡器等上游设备，防火墙可能将上游设备 IP 地址视为 HTTP/HTTPS 流量中代理转发的源 IP 地址而非请求内容的客户端的 IP 地址。在大多数情况下，上游设备会在 HTTP 请求中添加 X-Forwarded-For (XFF) 标头，其中包含请求内容的客户端或请求来源的准确 IPv4 或 IPv6 地址。

在这种情况下，您可以将防火墙配置为从 XFF 字段提取 IP 地址，并将其映射到具有 User-ID 的用户，或是根据 IP 地址应用安全策略。

- **Use X-Forwarded-For Header in User-ID**（在 **User-ID** 中使用 **X-Forwarded-For** 标头）— 这使您可以使用基于用户的策略，让代理服务器背后的用户安全访问基于 Web 的应用程序。此外，如果 User-ID 能够将 XFF IP 地址映射到用户名，则防火墙会将该用户名显示为流量、威胁、WildFire 提交和 URL 筛选日志中的源用户，以查看代理背后用户的 Web 活动。
- **Use X-Forwarded-For Header in Security Policy**（在安全策略中使用 **X-Forwarded-For** 标头）— 这使您可以使用 HTTP 标头 XFF 字段中的 IP 地址，根据源 IP 地址实施安全策略。此外，将策略应用于包含 XFF 字段中 IP 地址的流量后，您可以配置流量、威胁、数据过滤和 Wildfire 提交日志，以协助执行故障排除和修复。

要确保攻击者不能读取和利用为了从外部服务器检索内容，而从防火墙发出的网络请求数据包中的 XFF 值，您还可以配置防火墙从传出数据包中去除 XFF 值。在 User-ID 或策略中使用 XFF IP 地址以及将 XFF 值剥离并非相互独立的：如果您配置了两者，仅当防火墙在策略实施和日志记录中使用了 XFF 值之后才会清空这些值。



您不能将防火墙配置为在 *User-ID* 的 *XFF* 字段以及安全策略中同时使用 *IP* 地址。

- 为策略使用 XFF 值并记录源用户日志
- 在安全策略和日志记录中使用 XFF IP 地址值
- 使用 XFF 标头中的 IP 地址来对事件进行故障排查

## 在基于源用户的策略中使用 XFF 值

您可以将防火墙配置为通过用户 ID 将 XFF 标头中的 IP 地址映射到用户名，这样，您可以查看并基于用户策略控制代理服务器背后用户的 Web 流量，否则，将无法标识这些用户。为了将 IP 地址从 XFF 标头映射至用户名，必须首先启用 User-ID。

启用该选项后，防火墙可以将 XFF 标头中的 IP 地址仅用于用户映射。防火墙日志记录的源 IP 地址仍是代理服务器的 IP 地址，而不是源用户的 IP 地址。当您看到归属于用户的日志事件，且映射防火墙正对其进行使用，以及从 XFF 标头提取的 IP 地址，可能很难跟踪事件相关的特定设备。要简化代理服务器背后用户事件的调试和故障排除，还必须将防火墙配置为使用 XFF 标头中的 IP 地址来填充 URL 筛选日志的 X-Forwarded-For 列，这样，您可以跟踪与 URL 筛选日志条目相关联的日志事件相关的特定用户和设备。

代理服务器添加的 XFF 标头必须包含发起请求的最终用户的源 IP 地址。如果标头包含多个 IP 地址，则防火墙仅使用第一个 IP 地址。如果标头包含非 IP 地址的信息，则防火墙将不会执行用户映射。



启用防火墙以使用 *X-Forwarded-For* 标头执行用户映射并不能使防火墙将 *XFF* 标头中的客户端 *IP* 地址用作为日志中的源地址；日志仍将代理服务器 *IP* 地址显示为源地址。但是，要简化调试和故障排除过程，您可以将防火墙配置为添加 XFF 值到 URL 过滤日志以显示 *URL* 筛选日志中的客户端 *IP* 地址。

STEP 1 | 让防火墙在策略和日志的源用户字段中使用 XFF 值。

1. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID**（内容-**ID**）并编辑 X-Forwarded-For 标头设置。



© 2019 Palo Alto Networks, Inc.

2. 选择 **Use X-Forwarded-For Header in User-ID**（在 **User-ID** 中使用 **X-Forwarded-For** 标头）。

STEP 2 | 从出站 web 请求中删除 XFF 值。

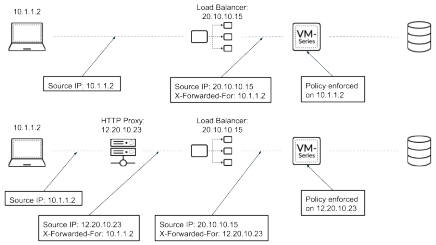
1. 选择 **Strip X-Forwarded-For Header**（去除 **X-Forwarded-For** 标头）。
2. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 3 | 验证防火墙填充日志的源用户字段。

1. 选择包含源用户字段的日志类型（例如，**Monitor**（监控）> **Logs**（日志）> **Traffic**（流量））。
2. 验证“源用户”列显示访问 Web 应用程序的用户的用户名。

# 在安全策略和日志记录中使用 XFF IP 地址值

您可以将防火墙配置为在 HTTP 标头的 X-Forwarded-For (XFF) 字段使用 IP 地址以实施安全策略。如果数据包在到达防火墙之前通过单个代理服务器，则 XFF 字段将包括原始端点的 IP 地址，防火墙将使用该 IP 来实施安全策略。但是，如果数据包通过多个上游设备，则防火墙使用最近添加的 IP 地址实施策略，或是使用其他依赖 IP 信息的功能。




- 在策略中使用 XFF 值
- 在日志中显示 XFF 值
- 在报告中显示 XFF 值

## 在策略中使用 *XFF* 值

实施安全策略时，完成下列程序以在 XFF 标头中使用客户端 IP 地址。

在 *Microsoft Azure* 中，应用程序网关默认会将原始源 *IP* 地址和端口插入到 *XFF* 标头中。若要在防火墙策略中使用 *XFF* 标头，您必须将应用程序网关配置为忽略 *XFF* 标头中的端口。详细信息，请参阅 Azure 文档。

STEP 1 | 登录防火墙。

STEP 2 | 选择 **Device**（设备）> **Setup**（设置）> **Content-ID** > **X-Forwarded-For Headers**（**X-Forwarded-For** 标头）。

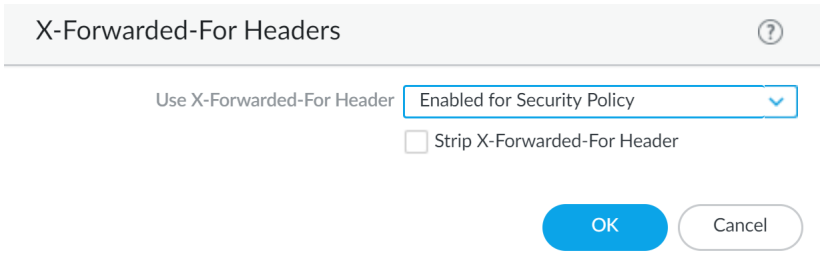
STEP 3 | 单击编辑图标。

STEP 4 | 从 **Use X-Forwarded-For Header**（使用 **X-Forwarded-For** 标头）下拉列表中选择 **Enabled for Security Policy**（为安全策略启用）。

您不能同时为安全策略和 *User-ID* 启用“使用 *X-Forwarded-For* 标头”。



© 2019 Palo Alto Networks, Inc.




STEP 5 | （可选）选择 **Strip X-Forwarded-For Header**（去除 **X-Forwarded-For** 标头）。选择此选项后，将在防火墙转发请求之前删除 XFF 标头。此选项不会禁用 XFF 标头；防火墙将使用 XFF 标头实施策略和日志记录。

STEP 6 | 单击 **OK**（确定）。

STEP 7 | **Commit**（提交）更改。

## 在日志中显示 *XFF* 值

除了可以在安全策略中使用 XFF 标头外，您还可以在各种日志、报告和应用程序命令中心 (ACC) 中查看 XFF IP 地址，以协助监控和故障排除。您可以在流量、威胁、数据过滤和 Wildfire 提交日志中添加 X-Forwarded-For 列。

若要在日志中查看 XFF IP 地址，请完成以下步骤。

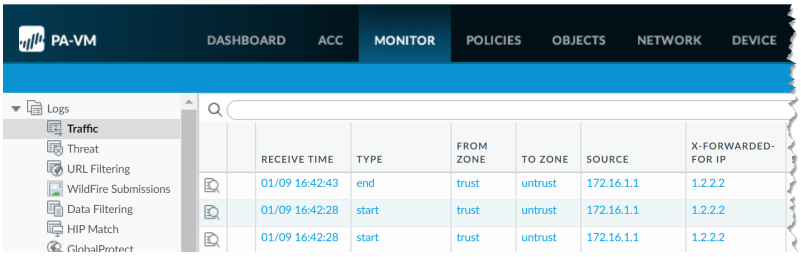
STEP 1 | 登录防火墙。

STEP 2 | 选择 **Monitoring**（监控）> **Logs**（日志）。

STEP 3 | 选择 **Traffic**（流量）、**Threat**（威胁）、 **Data Filtering**（数据过滤）或 **Wildfire Submissions**（**Wildfire** 提交）。

STEP 4 | 单击任意列标题右侧的箭头，然后选择 **Columns**（列）。

STEP 5 | 选择 **X-Forwarded-For IP** 以在日志中显示 XFF IP。




## 在报告中显示 *XFF* 值

防火墙生成的预定义报告不包含 XFF 值。若要在报告中查看 XFF IP 地址，防火墙包括的内置报告模板应包含 XFF 信息。

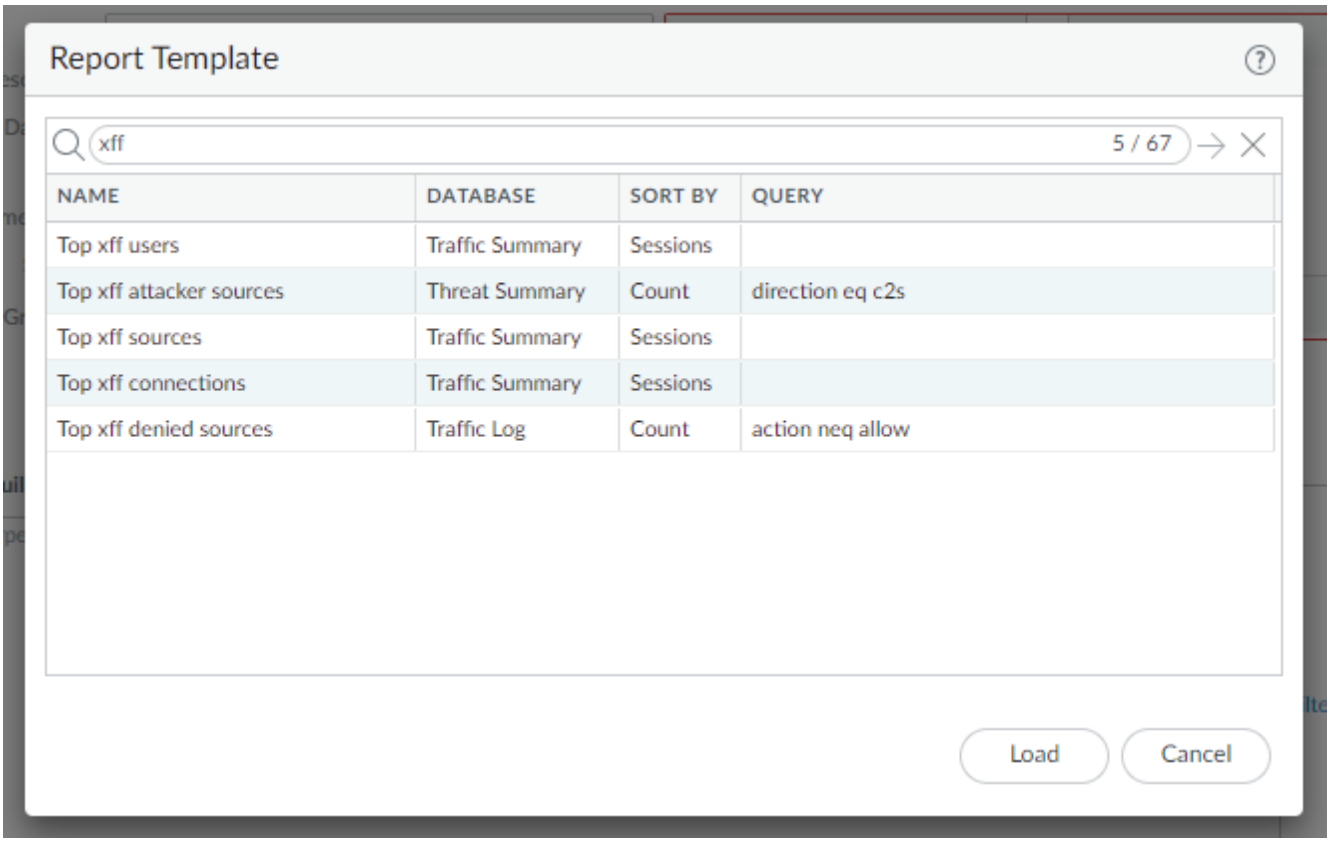
STEP 1 | 登录防火墙。

STEP 2 | 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告）> **Add**（添加）。


© 2019 Palo Alto Networks, Inc.

STEP 3 | 单击 **Load Template**（加载模板）。

STEP 4 | 在搜索栏输入 XFF，然后单击搜索按钮以查找内置 XFF 报告模板。




STEP 5 | 单击**Load**（加载）。

STEP 6 | 配置自定义报告的 **Time Frame**（时间范围）、**Sort By**（排序标准）和 **Group By**（分组标准）以根据您的需要显示 XFF 信息。

STEP 7 | （可选）单击 **Run Now**（立即运行）以根据需要（而不是或除**Scheduled Time**（计划时间）之外）生成报告。

## 使用 XFF 标头中的 IP 地址来对事件进行故障排查

默认情况下，即使您使用 X-Forwarded-For (XFF) 标头中的此地址进行用户映射，防火墙也不会记录代理服务器后面客户端的源地址。因此，虽然可以识别与日志事件关联的特定用户，但将无法轻松识别发起日志事件的源设备。要简化代理服务器后面用户事件的调试和故障排除，必须在 URL 筛选配置文件中 HTTP 标头日志记录内启用 X-Forwarded-For 选项，该配置文件被附加到允许访问基于 Web 的应用程序安全策略规则。启用此选项后，防火墙会将 XFF 标头中的 IP 地址记录为与规则匹配的所有流量的源地址。

启用防火墙以将 *XFF* 标头作为 *URL* 筛选日志中的源地址使用，这不会启用用户映射源地址。要填充源用户字段，请参阅为策略使用 XFF 值并记录源用户日志。

STEP 1 | 启用 URL 筛选配置文件中 HTTP 标头日志记录内的 X-Forwarded-For 选项。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选），然后选择要配置的 URL 筛选配置文件，或添加一个新配置文件。



© 2019 Palo Alto Networks, Inc.



您不能在默认的 *URL* 筛选配置文件中启用 *XFF* 日志记录。

2. 选择 **Settings**（设置）选项卡，然后选中 **X-Forwarded-For**。
3. 单击 **OK**（确定）保存配置文件。

STEP 2 | 将 URL 筛选配置文件附加到安全策略规则以允许用户的 Web 应用程序。

1. 选择 **Policies**（策略）> **Security**（安全）并单击规则。
2. 选择 **Actions**（操作）选项卡，将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件），并选择您刚才为 X-Forwarded-For HTTP 标头日志记录创建的 **URL Filtering**（**URL** 筛选）配置文件。
3. 单击 **OK**（确定）和 **Commit**（提交）。

STEP 3 | 验证防火墙正在记录 XFF 值。

1. 选择 **Monitor**（监控）> **Logs**（日志）> **URL Filtering**（**URL** 筛选）。
2. 按以下方法之一查看 XFF 值：
   - 要显示单一 URL 筛选日志的 XFF 值 — 单击小望远镜图标来显示日志详细信息。HTTP 标头部分显示 X-Forwarded-For 值。
   - 要显示所有 URL 筛选日志的 XFF 值 — 打开任何列标题下的下拉列表，选择 **Columns**（列），然后选中 **X-Forwarded-For**。随后页面显示 X-Forwarded-For 列。

STEP 4 | 使用 URL 筛选日志中的 XFF 字段来对另一种日志类型中的日志事件进行故障排查。

虽然只有 URL 筛选日志会在日志的 X-Forwarded-For 列中显示源用户 IP 地址，但是，如果您发现与 HTTP/HTTPS 流量关联的事件，却由于其位于代理服务器上而无法识别源 IP 地址时，您可以在相关 URL 筛选日志中使用 X-Forwarded-For 值来帮助您识别与日志事件关联的源地址。为此，需要进行如下操作：

1. 在“流量”、“威胁” 或“WildFire 提交”日志中查找要调查的事件，以将代理服务器的 IP 地址作为源地址显示。
2. 单击小望远镜图标以显示日志详细信息，并在“详细日志查看器”窗口底部查找关联的“URL 筛选日志”。
3. 选择标头行，然后从 **Columns**（列）下拉列表中选择 **X-Forwarded-For** 以显示此值。在 X-Forwarded-For 列中，此列中的 IP 地址代表的是代理服务器后面源用户的 IP 地址。使用此 IP 地址可以跟踪触发您正在调查事件的设备。


© 2019 Palo Alto Networks, Inc.

# 基于策略的转发

通常情况下，防火墙使用数据包中的目标 IP 地址来确定传出接口。防火墙使用和接口所连接的虚拟路由器关联的路由表来执行路由查找。基于策略的转发 (PBF) 可让您替代路由表，并根据特定参数（例如源或目标 IP 地址或流量类型）指定传出或出口接口。

- PBF
- 创建基于策略的转发规则
- 用例：采用双 ISP 的出站访问的 PBF

## PBF

PBF 规则可让流量从路由表中指定的下个中继段采用备选路径，并且通常因为安全或性能的原因用于指定 egress 接口。假设您的公司在公司办公室和分支办公室之间有两个链接：较为便宜的互联网链接以及较为昂贵的租赁线路。租赁的线路属于高带宽、低延迟链接。为增强安全性，您可使用 PBF 在专用的租赁线路上发送不属于加密流量（例如 FTP 流量）的应用程序，并在互联网链接上传输其他所有流量。或者出于性能考虑，在通过较便宜的链接发送其他所有流量（例如 Web 浏览）时您可选择于租赁的线路上路由业务关键应用程序。

- Egress 路径和对称返回
- 用于 PBF 的路径监控
- PBF 中的服务和应用程序

### *Egress* 路径和对称返回

使用 PBF，您可将流量引导至防火墙上的特定接口、丢弃流量或者将流量引导至另一个虚拟系统（在为多个虚拟系统启用的系统上）。

在采用非对称路由的网络中，例如双 ISP 环境中，会在流量抵达防火墙上的一个接口并从另一个接口离开时发生连接问题。如果路由为非对称，其中的转发（SYN 数据包）和返回 (SYN/ACK) 路径不同，防火墙将无法跟踪整个会话的状态，并且这会导致连接失败。为了确保流量使用对称路径（这意味着抵达在其上创建会话的接口并从该接口离开），可启用对称返回选项。

对于对称返回，虚拟路由器会替代返回流量的路由查找并将流量引导回自身在其上接收 SYN 数据包（或第一个数据包）的 MAC 地址。但是，如果目标 IP 地址所在的子网和 ingress/egress 接口的 IP 地址相同，则会执行路由查找，并且不会执行对称返回。该行为可防止流量被静默丢弃。

为确定对称返回的下个中继段，防火墙使用了地址解析协议 *(ARP)* 表。该 *ARP* 表支持的最大条目数受防火墙型号的限制并且该值不可由用户配置。要确定您型号的限值，可使用 *CLI* 命令：***show pbf return-mac all***。

### 用于 *PBF* 的路径监控

路径监视可让您验证对于 IP 地址的连接性，从而在需要时防火墙可引导流量通过备选路由。防火墙使用 ICMP ping 作为心跳来验证是否可访问指定的 IP 地址。

监视配置文件可让您指定心跳的阈值，从而确定是否可访问 IP 地址。如果无法访问监视的 IP 地址，则可禁用 PBF 规则或指定 *fail-over* 或 *wait-recover* 操作。禁用 PBF 规则可让虚拟路由器接管路由决策。如果采用故障转移或等待恢复操作，监视配置文件继续监视目标 IP 地址是否可达。如果恢复备份，则防火墙重新使用初始路由。

下表列出了新会话和既有会话上路径监视失败行为上的差异。



© 2019 Palo Alto Networks, Inc.

| 有关监控失败的会话的行为 | 如果在监控的 IP 地址无法访问时规则保持启用状态 | 如果在监控的 IP 地址无法访问时规则为禁用状态 |
|---|---|---|
| 对于既有会话 | **wait-recover**（等待恢复）— 继续使用在 PBF 规则中指定的出口接口 | **wait-recover**（等待恢复）— 继续使用在 PBF 规则中指定的出口接口 |
| | **fail-over**（故障转移）- 使用路由表（无 PBF）确定的路径 | **fail-over**（故障转移）- 使用路由表（无 PBF）确定的路径 |
| 对于新的会话 | **wait-recover**（等待恢复）— 使用路由表（无 PBF）确定的路径 | **wait-recover**（等待恢复）- 检查其余 PBF 规则。如果不匹配，则使用路由表 |
| | **fail-over**（故障转移）- 使用路由表（无 PBF）确定的路径 | **fail-over**（故障转移）—检查剩下的 PBF 规则。如果不匹配，则使用路由表 |

### *PBF 中的服务和应用程序*

PBF 规则应用在第一数据包 (SYN) 或对第一数据包 (SYN/ACK) 的首个响应上。这意味着在防火墙拥有足够的信息来确定应用程序之前，可应用 PBF 规则。因此，不建议将特定于应用程序的规则用于 PBF。如果可行，可使用服务对象，其为协议或应用程序使用的第 4 层端口（TCP 或 UDP）。

但是，如果您在 PBF 规则中指定应用程序，防火墙则会执行 *App-ID 缓存*。当应用程序首次通过防火墙时，防火墙没有足够的信息来确定应用程序，因此无法实施 PBF 规则。随着抵达的数据包变多，防火墙可确定应用程序并在 App-ID 缓存中创建条目并为会话保留该 App-ID。如果创建了具有相同目标 IP 地址、目标端口和协议 ID 的新会话，防火墙可将应用程序标识为和初始会话中一样的应用程序（根据 App-ID 缓存）并应用 PBF 规则。因此，对于并非精确匹配和并非相同应用程序的会话，可根据 PBF 规则进行转发。

此外，具有依赖关系和应用程序标识的应用程序可随着防火墙接收更多数据包而更改。由于 PBF 在会话开始时进行路由决策，防火墙无法在应用程序标识中实施更改。例如 YouTube 在进行 Web 浏览时启动，但是会根据页面上包含的不同链接和视频更改为 Flash、RTSP 或 YouTube。但是对于 PBF，由于防火墙在会话启动时将应用程序标识为 Web 浏览，此后无法识别应用程序中的更改。

您不能在 *PBF* 规则中使用自定义应用程序、应用程序筛选器或应用程序组。

## 创建基于策略的转发规则

使用 PBF 规则将流量引导至防火墙上的特定出口接口，并覆盖流量的默认路径。

STEP 1 | 创建基于策略的转发 (PBF) 规则。

在创建 PBF 规则时，您必须为规则、源区域或接口指定名称，并指定出口接口。其他所有组件为可选或者有默认值。

您可以使用 *IP* 地址、地址对象或 *FQDN* 指定源地址和目标地址。

1. 选择 **Policies**（策略）> **Policy Based Forwarding**（基于策略的转发），然后 **Add**（添加）PDB 策略规则。
2. 为规则提供一个描述性名称（**General**（常规））。
3. 选择 **Source**（源），然后配置以下内容：


© 2019 Palo Alto Networks, Inc.

1. 选择将向其应用转发策略的 **Type**（类型）（**Zone**（区域）或**Interface**（接口）），并指定相关区域或接口。如果要强制执行对称返回，则必须选择源接口。

   仅第 *3* 层接口支持 *PBF*；回环接口不支持 *PBF*。

2. （可选）指定将向其应用 PBF 规则的 **Source Address**（源地址）。例如，您想从中转发流量至该规则中指定的接口或区域的特定 IP 地址或子网 IP 地址。

   单击 *Negate*（求反），从 *PBF* 规则排除一个或多个 *Source Addresses*（源地址）。例如，如果您的 *PBF* 规则将所有流量从指定的区域引导至 *Internet*，*Negate*（求反）可让您从 *PBF* 规则中排除内部 *IP* 地址。

   评估顺序为自上而下。将数据包与满足定义条件的第一个规则相匹配；触发匹配后，将不评估后面的规则。

3. （可选）**Add**（添加）并选择将向其应用策略的 **Source User**（源用户）或用户组。

4. 选择 **Destination/Application/Service**（目标/应用程序/服务），然后配置以下内容：

   1. **Destination Address**（目标地址）— 默认情况下，规则适用于 **Any**（任何）IP 地址。单击 **Negate**（求反）从 PBF 规则排除一个或多个目标 IP 地址。
   2. **Add**（添加）您要使用 PBF 控制的任何 **Application**（应用程序）和 **Service**（服务）。

      不建议将特定于应用程序的规则用于 *PBF*，因为可能在防火墙具有足够信息来确定应用程序之前就已使用 *PBF* 规则。如果可行，可使用服务对象，其为协议或应用程序使用的第 *4* 层端口（*TCP* 或 *UDP*）。有关更多详细信息，请参阅PBF 中的服务和应用程序。

STEP 2 | 指定如何转发与规则匹配的数据包。

如果要在多 VSYS 环境中配置 PBF，则必须为每个虚拟系统创建单独的 *PBF* 规则（并创建适当的安全策略规则以启用流量）。

1. 选择 **Forwarding**（转发）。
2. 将 **Action**（操作）设置为在匹配数据包时执行：
   - **Forward**（转发）— 将数据包引导至指定的 **Egress Interface**（出口接口）。
   - **Forward to VSYS**（转发至 **VSYS**）（在为多个虚拟系统启用的防火墙上）— 选择向其转发数据包的虚拟系统。
   - 丢弃— 丢弃数据包。
   - **No PBF**（无 **PBF**）— 排除与规则中定义的源、目标、应用程序或服务的条件相符的数据包。匹配数据包使用路由表而非 PBF；防火墙使用路由表从重定向端口排除匹配的流量。
3. 要以每日、每周或非循环频率触发指定的 **Action**（操作），可创建并附加 **Schedule**（计划）。
4. 对于 **Next Hop**（下一个跃点），请选择以下选项之一：
   - **IP Address**（**IP** 地址）— 输入一个防火墙向其转发匹配数据包的 IP 地址，或选择一个防火墙向其转发匹配数据包的 IP 网络掩码类型地址对象。IPv4 地址对象必须有一个 /32 网络掩码，IPv6 地址对象必须有一个 /128 网络掩码。
   - **FQDN**— 输入一个防火墙向其转发匹配数据包的 FQDN（或选择或创建一个防火墙向其转发匹配数据包的 FQDN 类型地址对象）。FQDN 可以解析为 IPv4 地址或 IPv6 地址，或两者。如果 FQDN 解析为 IPv4 和 IPv6 地址，PBF 规则就有两个下一个跃点：一个 IPv4 地址和一个 IPv6 地址。可以为 IPv4 和 IPv6 流量使用相同的 PBF 规则。IPv4 流量转发至 IPv4 下一个跃点；IPv6 流量转发到 IPv6 下一个跃点。

     此 *FQDN* 必须解析出一个属于与您为 *PBF* 配置的接口相同子网的 *IP* 地址，防火墙拒绝解析，*FQDN* 仍保持不解析。



© 2019 Palo Alto Networks, Inc.

防火墙仅使用从 *FQDN* 的 *DNS* 解析出的一个 *IP* 地址（来自每个 *IPv4* 或 *IPv6* 系列类型）。如果 *DNS* 解析出多个地址，则防火墙会使用与配置用于下一个跃点的 *IP* 系列类型（*IPv4* 或 *IPv6*）匹配的首选 *IP* 地址。此首选 *IP* 地址是 *DNS* 服务器在其初始响应中返回的第一个地址。只要地址在后续响应中出现，无论其顺序如何，防火墙都会将该地址视为首选地址。

- **None**（无）— 没有下一个跃点表明数据包的目标 IP 地址被用作下一个跃点。如果目标 IP 地址与出口接口不再同一个子网中，在转发失败。

5. （可选）如果未指定 IP 地址，则启用监控来验证对于目标 IP 地址或**Next Hop**（下一个跃点）IP 地址的连接性。选择 **Monitor**（监控）并附加监控 **Profile**（配置文件）（默认或自定义），该配置文件指定在监控地址无法访问时的操作。
   - 您可以在 **Disable this rule if nexthop/monitor ip is unreachable**（下一个跃点/监视 **IP** 不可达时禁用此规则）。
   - 输入要监控的目标 **IP Address**（**IP** 地址）。

   **Egress Interface**（出口接口）可同时拥有 IPv4 地址和 IPv6 地址，**Next Hop**（下一个跃点）FQDN 可以解析为 IPv4 地址和 IPv6 地址。在这种情况下：

   1. 如果出口接口同时拥有 IPv4 地址和 IPv6 地址，且下一个跃点 FQDN 仅解析出一个地址系列类型，则防火墙监控解析出的 IP 地址。如果 FQDN 解析出 IPv4 地址和 IPv6 地址，但出口接口仅有一个地址系列类型的地址，则防火墙监视解析出的与出口接口地址系列匹配的下一个跃点地址。
   2. 如果出口接口和下一个跃点 FQDN 都拥有 IPv4 地址和 IPv6 地址，则防火墙监控 IPv4 下一个跃点地址。
   3. 如果出口接口拥有一个地址系列类型的地址，且下一个跃点 FQDN 解析出不同的地址系列类型的地址，则防火墙不会监视任何内容。

6. （非对称路由环境必需项；或者可选项）选择 **Enforce Symmetric Return**（强制对称返回），并在 **Next Hop Address List**（下一个跃点地址列表）中 **Add**（添加）一个或多个 IP 地址。最多可以添加 8 个下一个跃点 IP 地址；隧道和 PPoE 接口不能作为下一个跃点 IP 地址使用。

   启用对称返回，可确保返回流量（例如，从 LAN 上的信任区域传输到互联网）通过从互联网传入流量的相同接口转发出去。

STEP 3 | **Commit**（提交）更改。PBF 规则即生效。

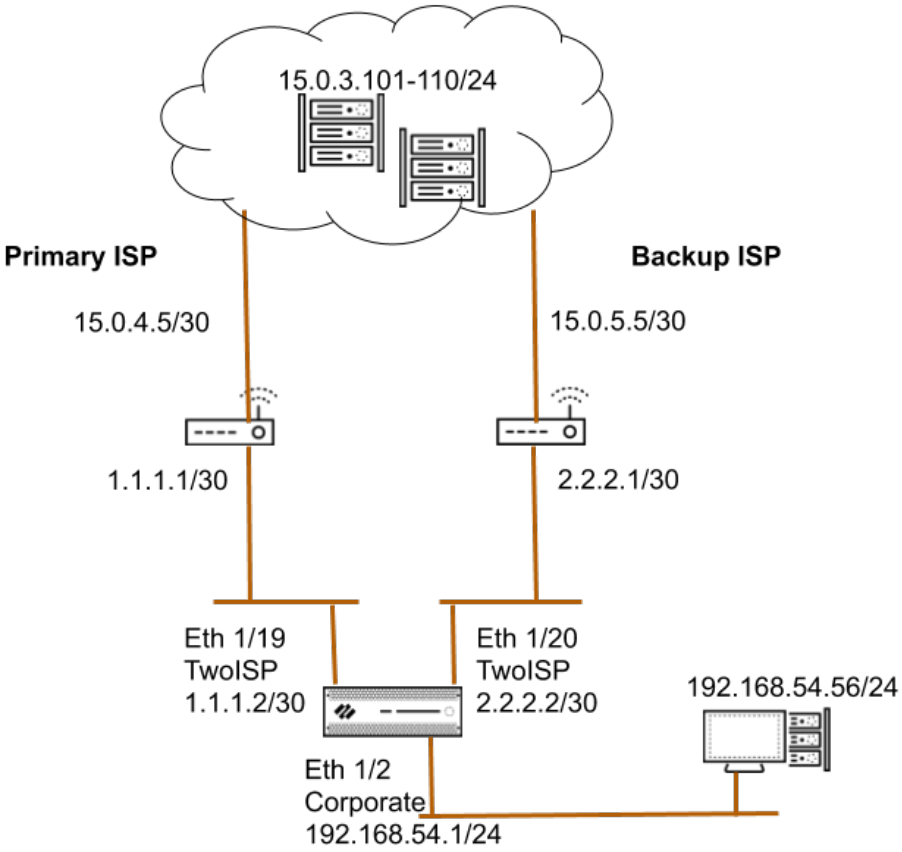
| | Source | | | Destination | | | Forwarding | | | Monitoring | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| NAME | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | DISABLE IF UNREACHABLE |
| pdf2 | ethernet1/3 | any | any | HQ-subnet | service-http | forward | ethernet1/1.100 | 192.168.100.2 | false | none | false |

# 用例：采用双 ISP 的出站访问的 PBF

在该用例中，分支办公室具有双 ISP 配置，并为冗余互联网访问实施 PBF。备份 ISP 是从客户端到 Web 服务器的流量的默认路由。为了实现冗余互联网访问而不使用 BGP 等互联网协议，我们将 PBF 用于基于目标接口的源 NAT 和静态路由，并如下配置防火墙：

- 启用将流量路由经过主要 ISP 的 PBF 规则，并将监控文件附加至规则。在主要 ISP 不可用时，监控配置文件让防火墙使用默认路由经过备份 ISP。
- 为主要和备用 ISP 定义源 NAT 规则，这些规则指示防火墙将和 egress 接口关联的源 IP 地址用于相应 ISP。这可确保传出流量具有正确的源 IP 地址。
- 将静态路由添加至备份 ISP，从而在主要 ISP 不可用时，默认路由开始生效并且引导流量通过备份 ISP。


© 2019 Palo Alto Networks, Inc.




STEP 1 | 配置防火墙上的入口和出口接口。

Egress 接口可位于相同区域。

1. 选择 **Network**（网络）> **Interfaces**（接口）并选择要配置的接口。

   在本示例中使用的防火墙上的接口配置如下：

   - 连接至主要 ISP 的 Ethernet 1/19：
     - 区域：TwoISP
     - IP 地址：1.1.1.2/30
     - 虚拟路由器：默认
   - 连接至备份 ISP 的 Ethernet 1/20：
     - 区域：TwoISP
     - IP 地址：2.2.2.2/30
     - 虚拟路由器：默认
   - Ethernet 1/2 为入口接口，由网络客户端用于连接至 Internet：
     - 区域：公司
     - IP 地址：192.168. 54.1/24
     - 虚拟路由器：默认

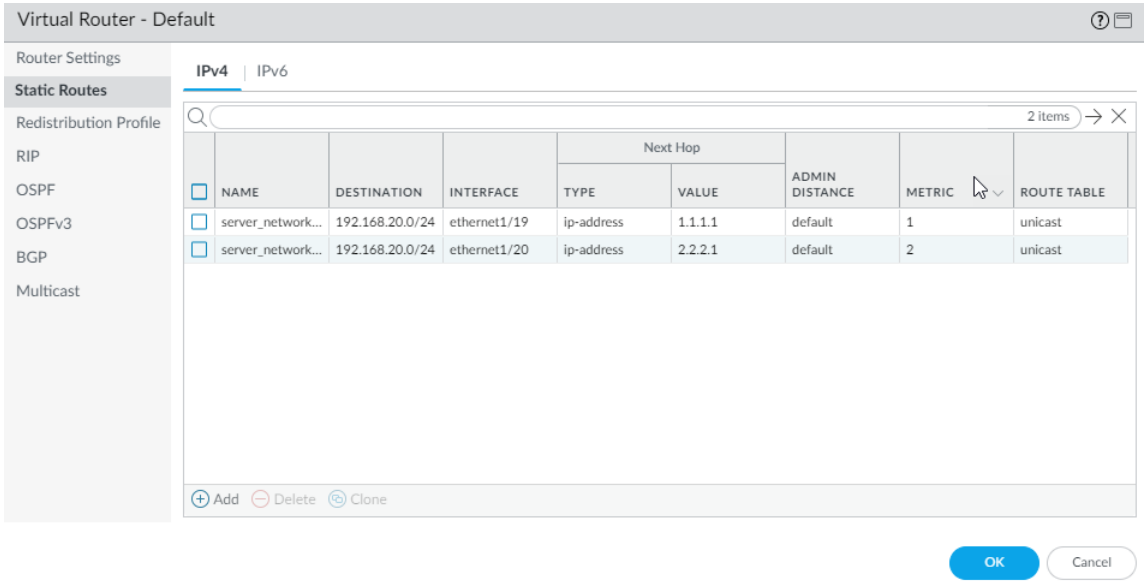


© 2019 Palo Alto Networks, Inc.

2. 要保存接口配置，请单击 **OK**（确定）。

STEP 2 | 在虚拟路由器上，将静态路由添加至备份 ISP。

1. 请选择 **Network**（网络）> **Virtual Router**（虚拟路由器），然后选择 **default**（默认）链接来打开虚拟路由器对话框。
2. 选择 **Static Routes**（静态路由），然后单击 **Add**（添加）。为路由输入**Name**（名称）并指定要为其定义静态路由的**Destination**（目标）IP 地址。在此示例中，我们对所有流量使用 0.0.0.0/0。
3. 选择 **IP Address**（**IP** 地址）单选按钮并为您连接至备份互联网网关的路由器设置 **Next Hop**（下一个跃点）IP 地址（不能将域名用于下一个跃点）。在该示例中为 2.2.2.1。
4. 为路由指定成本指标。




5. 单击 **OK**（确定）两次，以保存虚拟路由器配置。

STEP 3 | 创建将流量引导至与主要 ISP 连接的接口的 PBF 规则。

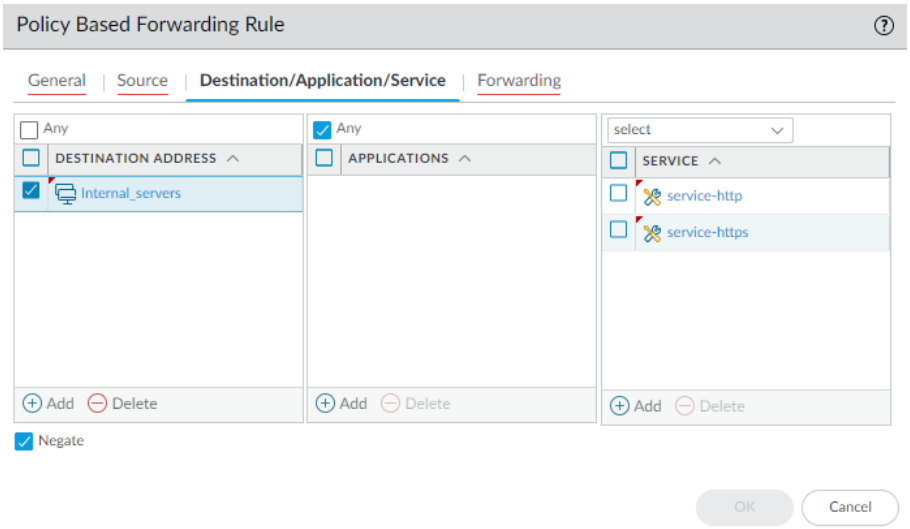
确保排除目的地为内部服务器/或 PBF 中 IP 地址的流量。定义求反规则，从而目的地为内部 IP 地址的流量不会路由经过 PBF 规则中定义的 egress 接口。

1. 选择 **Policies**（策略）> **Policy Based Forwarding**（基于策略的转发），然后单击 **Add**（添加）。
2. 在 **General**（常规）选项卡中为规则提供一个描述性的 **Name**（名称）。
3. 在 **Source**（源）选项卡中，设置 **Source Zone**（源区域）；在本例中，区域为 Corporate。
4. 在**Destination/Application/Service**（目标/应用程序/服务）选项卡中，进行以下设置：
   1. 在目标地址部分，为内部网络上的服务器**Add**（添加）IP 地址或地址范围，或者为您的内部服务器创建地址对象。选择**Negate**（求反）阻止上面列出的 IP 地址或地址对象使用该规则。
   2. 在“服务”部分，**Add**（添加）**service-http** 和 **service-https** 服务以让 HTTP 和 HTTPS 流量使用默认端口。对于安全策略允许的其他所有流量，将使用默认路由。



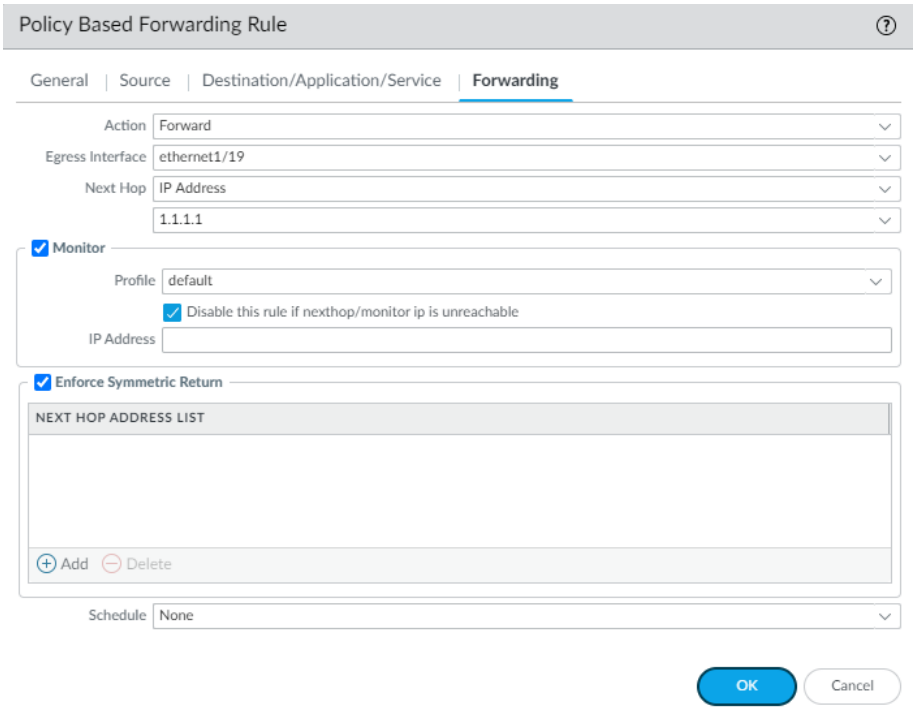
要使用 *PBF* 转发所有流量，可将服务设置为 *Any*（任意）。


© 2019 Palo Alto Networks, Inc.




STEP 4 | 指定转发流量的位置。

1. 在**Forwarding**（转发）选项卡中，指定您要向其转发流量的接口并启用路径监视。
2. 要转发流量，可将 **Action**（操作）设置为 **Forward**（转发），然后选择 **Egress Interface**（**Egress** 接口）并指定 **Next Hop**（下个中继段）。在该示例中，出口接口为 ethernet1/19，下一个跃点 IP 地址为 1.1.1.1（不能将 FQDN 用于下一个跃点）。




3. 启用 **Monitor**（监视程序）并附加默认监视配置文件以触发指向备份 ISP 的故障转移。在该示例中，我们没有指定要监视的目标 IP 地址。防火墙将监视下个中继段 IP 地址；如果该 IP 地址无法访问，则防火墙将把流量引导至在虚拟路由器上指定的默认路由。
4. （出现非对称路由时需要）选择 **Enforce Symmetric Return**（强制对称返回）可确保通过有流量从互联网进入的相同接口向外转发从公司区域至互联网的返回流量。
5. NAT 确保来自互联网的流量返回至防火墙上正确的接口/IP 地址。
6. 单击 **OK**（确定）保存更改。



© 2019 Palo Alto Networks, Inc.

| | | Source | | | Destination | | | | Forwarding | | | Monitoring | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | APPLICATION | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | TARGET | DISABLE IF UNR |
| 1 | pbf_rule_source_zone | Corporate | 192.168.10.2 | any | any | any | service-http<br>service-https | forward | ethernet1/19 | 1.1.1.1 | true | default | none | true |

STEP 5 | 根据出口接口和 ISP 创建 NAT 规则。这些规则可确保将正确的源 IP 地址用于传出连接。

1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 在该示例中，我们为每个 ISP 创建的 NAT 规则如下：

   主要 **ISP** 的 **NAT**

   在**Original Packet**（原始数据包）选项卡中，

   **Source Zone**（源区域）：公司

   **Destination Zone**（目标区域）：TwoISP

   在**Translated Packet**（转换后的数据包）选项卡中的源地址转换下

   **Translation Type**（转换类型）：动态 IP 和端口

   **Address Type**（地址类型）：接口地址

   **Interface**（接口）：ethernet1/19

   **IP Address**（IP 地址）：1.1.1.2/30

   备份 **ISP** 的 **NAT**

   在**Original Packet**（原始数据包）选项卡中，

   **Source Zone**（源区域）：公司

   **Destination Zone**（目标区域）：TwoISP

   在**Translated Packet**（转换后的数据包）选项卡中的源地址转换下

   **Translation Type**（转换类型）：动态 IP 和端口

   **Address Type**（地址类型）：接口地址

   **Interface**（接口）：ethernet1/20

   **IP Address**（IP 地址）：2.2.2.2/30

| | | | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATI |
| 1 | NAT for Primary ISP | none | Corporate | TwoISP | any | any | any | any | dynamic-ip-and-port<br>ethernet1/19<br>1.1.1.2/30 | none |
| 2 | NAT for Backup ISP | none | Corporate | TwoISP | any | any | any | any | dynamic-ip-and-port<br>ethernet1/20<br>2.2.2.2/30 | none |

STEP 6 | 创建安全策略以允许对于互联网的出站访问。

要安全地启用应用程序，可创建简单的规则，允许对于互联网的访问，并附加防火墙上可用的安全配置文件。

1. 选择 **Policies**（策略）> **Security**（安全），并单击 **Add**（添加）。
2. 在 **General**（常规）选项卡中为规则提供一个描述性的 **Name**（名称）。
3. 在 **Source**（源）选项卡中，为公司设置 **Source Zone**（源区域）。



© 2019 Palo Alto Networks, Inc.

4. 在 **Destination**（目标）选项卡中，将 **Destination**（目标区域）设置为 TwoISP。
5. 在 **Service/ URL Category**（服务/URL 类别）选项卡中，保留默认**application-default**（应用程序-默认）。
6. 在 **Actions**（操作）选项卡中，完成以下任务：
   1. 将 **Action Setting**（操作设置）设置为 **Allow**（允许）。
   2. 在 **Profile Setting**（配置文件设置）下附加防病毒、防间谍软件、漏洞保护和 URL 筛选的默认配置文件。
7. 在 **Options**（选项）下验证是否已启用在会话结束时进行日志记录。只有与安全规则相匹配的流量才会被记录。

| | NAME | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| 1 | Copr2ISP | none | universal | Corporate | any | any | any | TwoISP | any | any | any | any | Allow |

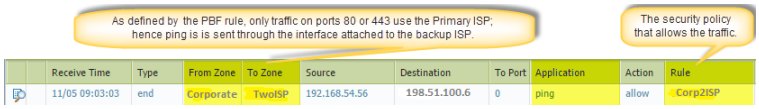
STEP 7 | 将策略保存到防火墙上正在运行的配置。

单击 **Commit**（提交）。

STEP 8 | 验证 PBF 规则是否为活动状态，并且主要 ISP 是否用于互联网访问。

1. 启动 Web 浏览器并访问 Web 服务器。在防火墙上检查 Web 浏览活动的流量日志。
2. 在网络上的客户端中，使用 ping 实用程序验证对于互联网上 Web 服务器的连接性，并检查防火墙上的流量日志。

```
C:\Users\pm-user1>ping 198.51.100.6
Pinging 198.51.100.6 with 32 bytes of data:
Reply from 198.51.100.6: bytes=32 time=34ms TTL=117
Reply from 198.51.100.6: bytes=32 time=13ms TTL=117
Reply from 198.51.100.6: bytes=32 time=25ms TTL=117
Reply from 198.51.100.6: bytes=32 time=3ms TTL=117
Ping statistics for 198.51.100.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum = 3ms, Maximum = 34ms, Average = 18ms
```




3. 要确认 PBF 规则处于活动状态，请使用以下 CLI 命令：

```
admin@PA-NGFW> show pbf rule all
Rule        ID     Rule State Action   Egress IF/VSYS  NextHop
=========== ===  ========== ======  ==============
Use ISP-Pr 1 Active     Forward ethernet1/1 1.1.1.1
```

STEP 9 | 验证是否发生了指向备份 ISP 的故障转移，并且正确应用了源 NAT。

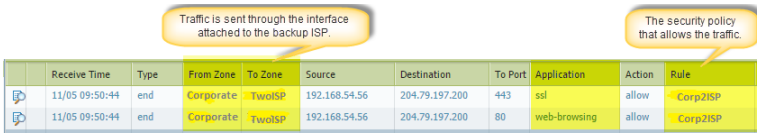
1. 断开与主要 ISP 的连接。
2. 要确认 PBF 规则处于非活动状态，请使用以下 CLI 命令：

```
admin@PA-NGFW> show pbf rule all
Rule        ID     Rule State Action   Egress IF/VSYS  NextHop
=========== ===  ========== ======  ============== ===
Use ISP-Pr 1 Disabled Forward ethernet1/19     1.1.1.1
```



© 2019 Palo Alto Networks, Inc.

3. 访问 Web 服务器，并检查流量日志以确保流量通过备份 ISP 转发。




4. 查看会话详细信息以确认 NAT 规则正确发挥作用。

```
admin@PA-NGFW> show session all
--------------------------------------------------------------
ID Application    State   Type Flag Src[Sport]/Zone/Proto (translated
 IP[Port]) Vsys Dst[Dport]/Zone (translated IP[Port])
--------------------------------------------------------------
87212 ssl ACTIVE  FLOW  NS   192.168.54.56[53236]/Corporate/6
 (2.2.2.2[12896]) vsys1 204.79.197.200[443]/TwoISP (204.79.197.200[443])
```

5. 从输出获取会话标识号并查看会话详细信息。



未使用 *PBF* 规则，因此未列在输出中。

```
admin@PA-NGFW> show session id 87212
Session           87212
c2s flow:
                source:      192.168.54.56 [Corporate]
                dst:         204.79.197.200
                proto:       6
                sport:       53236           dport:       443
                state:       ACTIVE          type:        FLOW
                src user:    unknown
                dst user:    unknown
s2c flow:
                source:      204.79.197.200 [TwoISP]
                dst:         2.2.2.2
                proto:       6
                sport:       443             dport:       12896
                state:       ACTIVE          type:        FLOW
                src user:    unknown
                dst user:    unknown
start time                    : Wed Nov5 11:16:10 2014
        timeout                         : 1800 sec
        time to live                    : 1757 sec
        total byte count(c2s)           : 1918
        total byte count(s2c)           : 4333
        layer7 packet count(c2s)        : 10
        layer7 packet count(s2c)        : 7
        vsys                            : vsys1
        application                     : ssl
        rule                            : Corp2ISP
        session to be logged at end     : True
        session in session ager         : True
        session synced from HA peer     : False
        address/port translation        : source
       nat-rule           : NAT-Backup ISP(vsys1)
        layer7 processing               : enabled
        URL filtering enabled           : True
        URL category                    : search-engines
        session via syn-cookies         : False
        session terminated on host      : False
```



© 2019 Palo Alto Networks, Inc.

```
        session traverses tunnel       : False
        authentication portal session         : False
        ingress interface        : ethernet1/2
    egress interface        : ethernet1/20
        session QoS rule               : N/A (class 4)
```



© 2019 Palo Alto Networks, Inc.

# 测试策略规则

在您运行的配置中测试策略规则，确保您的策略正确地允许和拒绝流量以及对应用程序和网站访问，符合您的业务需求。您可以直接从 Web 接口测试并验证您的策略规则是否通过为防火墙执行策略匹配测试，允许和拒绝正确的流量。

STEP 1 | 启动 Web 界面。

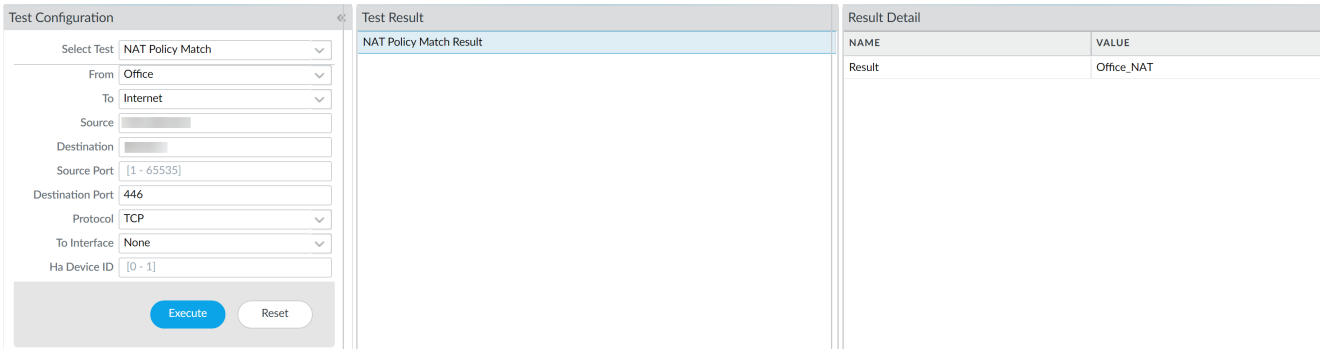
STEP 2 | 选择 **Device**（设备）> **Troubleshooting**（故障排除）以执行策略匹配或连接测试。

STEP 3 | 输入所需的信息，以执行策略匹配测试。此例中，我们运行 NAT 策略匹配测试。

1. **Select Test**（选择测试）—选择 **NAT Policy Match**（**NAT** 策略匹配）。
2. **From**（来自）—选择区域流量来自哪里。
3. **To**（至）—选择流量目标区域。
4. **Source**（源）—输入发起通信的 IP 地址。
5. **Destination**（目标）—输入流量目标设备的 IP 地址。
6. **Destination Port**（目标端口）—输入流量所用的端口。此端口随下列步骤中所用的 IP 协议而变化。
7. **Protocol**（协议）—输入流量所用的 IP 协议。
8. 如有必要，输入与您的 NAT 策略规则测试相关的其他信息。

STEP 4 | **Execute**（执行） NAT 策略匹配测试。

STEP 5 | 查看 **NAT Policy Match Result**（**NAT** 策略匹配结果）以了解与测试条件相符的策略规则。






© 2019 Palo Alto Networks, Inc.

# 虚拟系统

本主题介绍虚拟系统、其优势、典型用例以及配置方法。本主题还提供了一些指向其他主题的链接，在这些主题中记录了某些虚拟系统（当这些虚拟系统与其他功能一起发挥作用时）。


> 虚拟系统概述
> 虚拟系统之间的通信
> 共享网关
> 配置虚拟系统
> 在防火墙中配置虚拟系统间通信
> 配置共享网关
> 自定义虚拟系统的服务路由
> 包含其他特征的虚拟系统功能

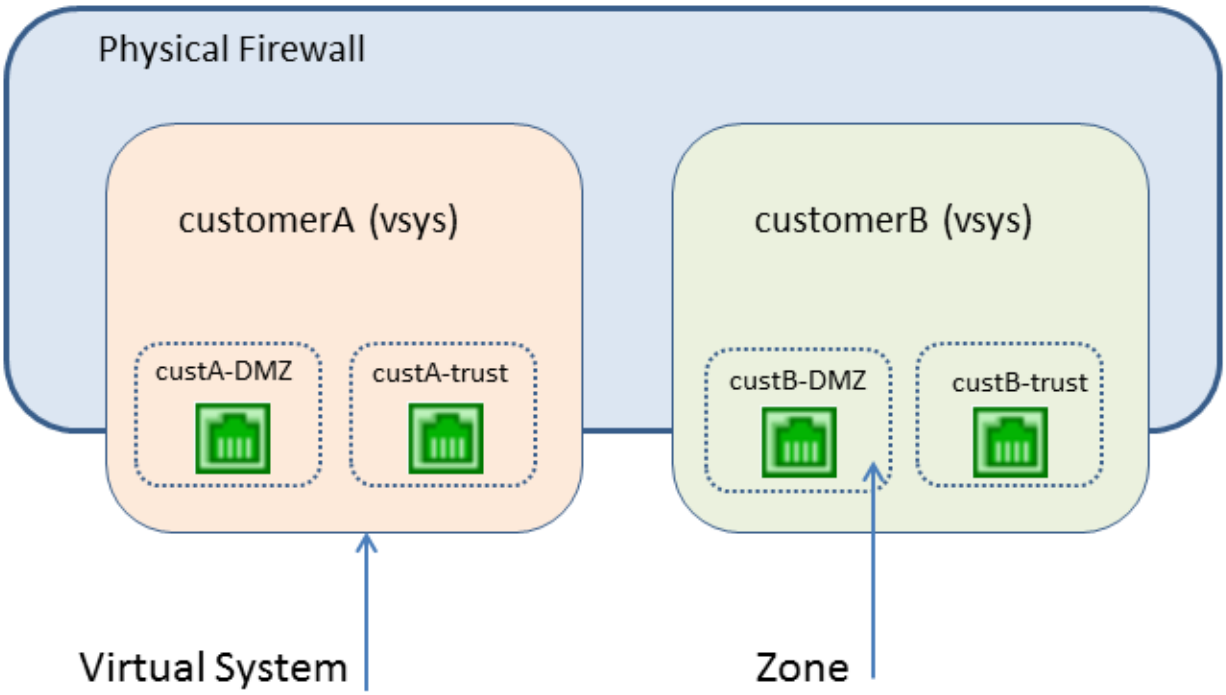
# 虚拟系统概述

虚拟系统是单个物理 Palo Alto Networks 防火墙中的独立逻辑防火墙实例。托管服务提供商和企业可以使用一对防火墙（实现高可用性）并在这对防火墙上启用虚拟系统，而不必使用多个防火墙。每个虚拟系统 (vsys) 都是一个独立、单独管理的防火墙，其流量与其他虚拟系统的流量分隔开。

- 虚拟系统组件和分段
- 虚拟系统的优势
- 虚拟系统的用例
- 虚拟系统的平台支持和许可
- 虚拟系统的管理角色
- 虚拟系统的共享对象

## 虚拟系统组件和分段

虚拟系统是一个创建管理边界的对象，如下图中所示。




虚拟系统由物理和逻辑接口及子接口（包括 VLAN 和 Virtual Wire）、虚拟路由器以及安全区域的集合组成。您将选择每个虚拟系统的部署模式（Virtual Wire、第 2 层或者第 3 层的任意组合）。通过使用虚拟系统，您可以将下列任何对象进行分段：

- 管理访问
- 所有策略的管理（安全性、NAT、QoS、基于策略的转发、解密、应用程序替代、隧道检查、身份验证和 DoS 保护）
- 所有对象（如地址对象、应用程序组和筛选器、外部动态列表、安全配置文件、解密配置文件、自定义对象等等）
- User-ID
- 证书管理
- 服务器配置文件



© 2019 Palo Alto Networks, Inc.

- 日志记录、报告和可见性功能

虚拟系统将影响防火墙的安全功能，但是虚拟系统自身不会影响联网功能，如静态和动态路由。您可以通过为每个虚拟系统创建一个或多个虚拟路由器来为每个虚拟系统的路由进行分段。

- 如果您对一个组织中多个部分部署了虚拟系统，并且所有部门的网络流量均在一个公用网络中，则可以为多个虚拟系统创建单个虚拟路由器。
- 如果您希望路由分段并且每个虚拟系统的流量必须与其他虚拟系统的流量隔离，则可以为每个虚拟系统创建一个或多个虚拟路由器。
- 如果您想要对用户映射分段，以免在虚拟系统之间共享所有映射，您可以在非 User-ID 中心的虚拟系统上配置 User-ID 源。请参阅共享跨虚拟系统的 User-ID 映射。

## 虚拟系统的优势

虚拟系统提供了与物理防火墙相同的基本功能，还具有以下额外优势：

- 分段管理 — 不同组织（或者客户或业务单位）可以控制（并监控）一个单独的防火墙实例，以便这些组织可以控制自己的流量，而不会干扰同一物理防火墙上其他防火墙实例的流量或策略。
- 可扩展性 — 在配置了物理防火墙之后，可以高效率地添加或移除客户或业务单位。ISP、托管安全服务提供商或企业可以为每位客户提供不同安全服务。
- 降低资本费用和运营费用 — 借助虚拟系统，无需在一个位置部署多个物理防火墙，因为虚拟系统在一个防火墙上共存。由于无需购买多个防火墙，组织可以节省硬件费用、电费和机架空间，并可降低维护和管理费用。
- 共享 **IP** 地址到用户名映射的能力 — 通过将虚拟系统指定为 User-ID 中心，您可以在虚拟系统之间共享 IP 地址到用户名映射，以充分利用防火墙的 User-ID 容量，并降低操作复杂性。

## 虚拟系统的用例

有多种方法在网络中使用虚拟系统。对于 ISP 或托管安全服务提供商 (MSSP)，一种常见方法是通过单个防火墙向多个客户交付服务。客户可以选择一系列广泛的服务（可以轻松启用或禁用这些服务）。防火墙的基于角色的管理可让 ISP 或 MSSP 控制每位客户对各种功能（如日志记录和报告）的访问权，同时隐藏或提供对其他功能的只读能力。

另一个常见用例是在需要不同防火墙实例的大型企业中（由于多个部门之间的不同技术或保密要求）。与以上用例一样，不同组可以具有不同级别的访问权，而 IT 部门管理防火墙自身。可以将服务跟踪和/或回单至部门，以便能够在组织中实现财政问责。

## 虚拟系统的平台支持和许可

PA-3200 系列、PA-5200 系列和 PA-7000 系列防火墙支持虚拟系统。每个防火墙系列支持基本数量的虚拟系统；此数量因平台而异。需要虚拟系统许可证来支持 PA-3200 系列防火墙上的多个虚拟系统，并创建超过平台所支持基本数量的虚拟系统。

有关许可证信息，请参阅订阅。有关受支持虚拟系统的基本数量和最大数量，请参阅比较防火墙工具。

PA-220、PA-800 系列或 VM 系列防火墙上不支持多个虚拟系统。



默认为 *vsys1*。因为 *vsys1* 与防火墙上的内部层次结构相关，因此无法删除；*vsys1* 甚至会出现在不支持多个虚拟系统的防火墙型号上。

您可以对虚拟系统允许的会话、规则和 VPN 隧道限制资源分配，从而控制防火墙资源。各资源设置显示值的有效范围，并随防火墙型号改变。默认值为 0，表示虚拟系统的限制是防火墙型号的限制。但是，对于每个虚拟系统而言，特定设置的限制不能复制。例如，如果防火墙有 4 个虚拟系统，则每个虚拟系统不能具有每个防火墙允许的解密规则总数。在所有虚拟系统的解密规则总数达到防火墙限制后，您无法再继续添加。



© 2019 Palo Alto Networks, Inc.

## 虚拟系统的管理角色

**superuser**（超级用户）管理员可以创建虚拟系统并添加 **Device Administrator**（设备管理员）、**vsysadmin** 或 **vsysreader**。**Device Administrator**（设备管理员）可以访问所有虚拟系统，但是无法添加管理员。当您创建管理员角色配置文件并选择该角色成为 **Virtual System**（虚拟系统）时，角色应用于防火墙上的特定虚拟系统。在 **Command Line**（命令行）选项卡中，有两种类型的虚拟系统管理角色：

- **vsysadmin** — 在防火墙上访问特定虚拟系统，以创建和管理虚拟系统的特定方面。虚拟系统管理员无法访问网络接口、VLAN、虚拟线路、虚拟路由器、IPSec 隧道、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。具有 vsysadmin 权限的用户只能对获得分配的虚拟系统执行配置。
- **vsysreader** — 在防火墙上只读访问特定虚拟系统，以及虚拟系统的特定方面。虚拟系统阅读器无法访问网络接口、VLAN、虚拟线路、虚拟路由器、IPSec 隧道、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。

虚拟系统管理员只能查看为该管理员分配的虚拟系统的日志。**Superuser**（超级用户）或 **Device administrator**（设备管理员）可以查看所有日志，选择虚拟系统进行查看，或将虚拟系统配置为 User-ID 中心。

## 虚拟系统的共享对象

如果您的管理员帐户扩展到多个虚拟系统，则可以选择为特定虚拟系统配置对象（如地址对象）和策略或者配置为共享对象，后者将应用于防火墙上的所有虚拟系统。如果您尝试创建一个与虚拟系统中某个现有对象的名称和类型相同的共享对象，则将使用虚拟系统对象。



© 2019 Palo Alto Networks, Inc.

# 虚拟系统之间的通信

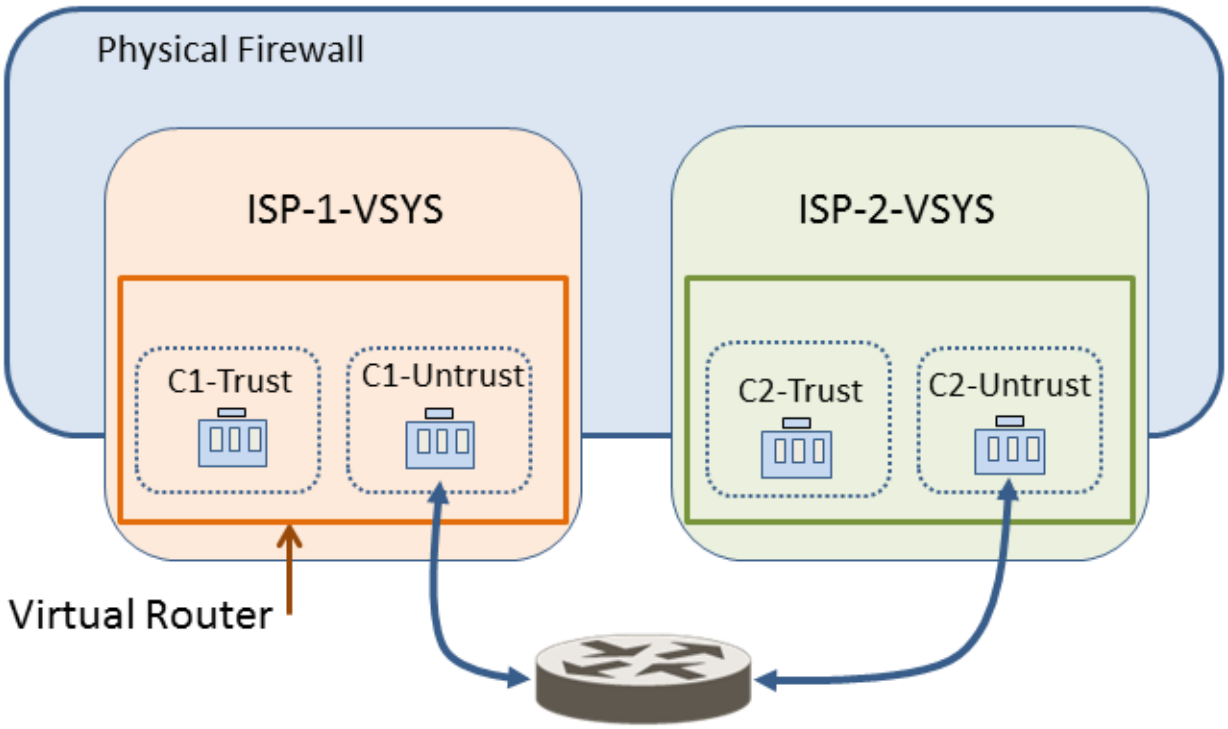
在以下两种典型情况中需要虚拟系统之间的通信（vsys 间流量）。在多租户环境中，可以通过下列方式来进行虚拟系统之间的通信：让流量离开防火墙，经过 Internet，然后再重新进入防火墙。在单一组织环境中，虚拟系统之间的通信可以留在防火墙中。本节同时讨论了上述两种情况。

- 必须离开防火墙的 VSYS 间流量
- 留在防火墙的 VSYS 间流量
- VSYS 间的通信使用两个会话

## 必须离开防火墙的 VSYS 间流量

在防火墙中具有多个客户（称为多租户）的 ISP 可以对每个客户使用一个虚拟系统，从而让每位客户控制自己的虚拟系统配置。ISP 向客户授予 **vsysadmin**（虚拟系统管理员）权限。每位客户的流量和管理与其他客户隔离。每个虚拟系统必须配置有自身的 IP 地址以及一个或多个虚拟系统才能管理流量以及自身与互联网的连接。

如果虚拟系统需要彼此通信，则该流量离开防火墙进入另一个第 3 层路由设备，然后回到防火墙，即使同一个物理防火墙上存在虚拟系统，如下图中所示。




## 留在防火墙的 VSYS 间流量

与前面的多租户情况不同，防火墙上的虚拟系统可以由单个组织来控制。组织希望同时隔离虚拟系统之间的流量，并且允许虚拟系统之间的通信。当组织希望提供部门级别隔离并且仍让部门能够彼此通信或连接到相同网络时，便会出现这种常见用例。在这种情况下，vsys 间通信留在防火墙中，如下列主题中所述：

- 外部区域
- 防火墙中流量的外部区域和安全策略



© 2019 Palo Alto Networks, Inc.

## 外部区域

以上用例中需要的通信是通过配置指向或源自外部区域的安全策略而实现。外部区域是一个安全对象，与其可以访问的特定虚拟系统进行关联；此区域相对于虚拟系统是外部的。一个虚拟系统只能有一个外部区域，无论虚拟系统中有多少安全区域。需要外部区域才能允许不同虚拟系统中区域之间的流量，流量不会离开防火墙。

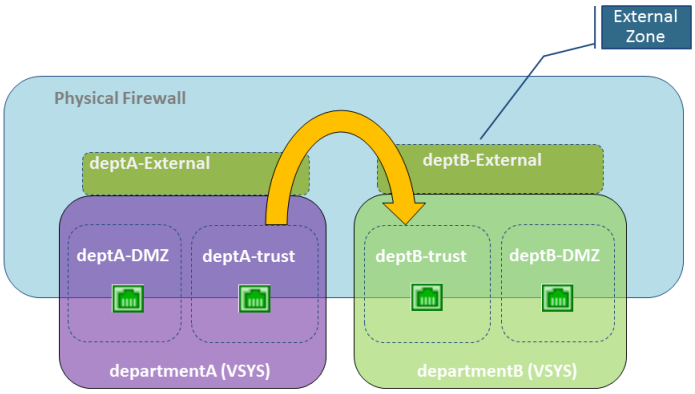
虚拟系统管理员配置允许两个虚拟系统之间的流量所需要的安全策略。与安全区域不同，外部区域不与某个接口相关联；其与虚拟系统相关联。安全策略允许或拒绝安全（内部）区域与外部区域之间的流量。

由于外部区域没有接口或 IP 地址与其关联，部分区域保护配置文件在外部区域中不受支持。

切记，每个虚拟系统是防火墙的一个单独实例，这意味着在虚拟系统之间移动的每个数据包都会针对安全策略进行检查并进行 App-ID 评估。

## 防火墙中流量的外部区域和安全策略

在以下示例中，企业具有两个单独管理组：虚拟系统 departmentA 和 departmentB。下图显示了与每个虚拟系统相关联的外部区域，还显示了流量从一个信任区域（离开外部区域）流入另一个虚拟系统的外部区域并流入其信任区域。




要创建外部区域，防火墙管理员必须配置虚拟系统，他们对彼此可见。外部区域之间没有安全策略，因为它们的虚拟系统彼此可见。

要在虚拟系统之间通信，防火墙上的 ingress 和 egress 接口分配给单个虚拟路由器，否则他们使用虚拟路由器间的静态路由进行连接。这两种方法中，较简单的一种是将所有必须彼此通信的虚拟系统分配给单个虚拟路由器。

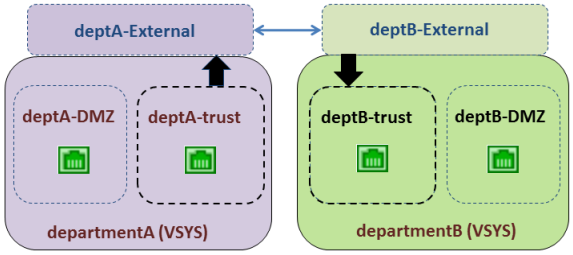
虚拟系统需要具有自己的虚拟路由器的一个可能原因是，虚拟系统使用了重叠的 IP 地址范围。可以在虚拟系统之间路由流量，但每个虚拟路由器必须将指向其他虚拟路由器的静态路由作为下一个跃点。

引用上图中的情况，我们有一家包含以下两个管理组的企业：departmentA 和 departmentB。组 departmentA 管理本地网络和 DMZ 资源。组 departmentB 管理网络的销售部门的进出流量。所有流量均在本地网络上，因此使用了单个虚拟路由器。针对两个虚拟系统之间的通信，配置了两个外部区域。虚拟系统 departmentA 在安全策略中使用了下列三个区域：deptA-DMZ、deptA-trust 和 deptA-External。虚拟系统 departmentB 也具有下列三个区域：deptB-DMZ、deptB-trust 和 deptB-External。这两个组都可以控制通过其虚拟系统的流量。

要允许从 deptA-trust 到 deptB-trust 的流量，需要两个安全策略。在下图中，两个垂直箭头表示安全策略（在下图中描述）控制流量的位置。



© 2019 Palo Alto Networks, Inc.




- 安全策略 1：在上图中，流量的目标是 deptB-trust 区域。流量离开 deptA-trust 区域并进入 deptA-External 区域。安全策略必须允许从源区域 (deptA-trust) 到目标区域 (deptA-External) 的流量。虚拟系统允许任何策略类型用于此流量，包括 NAT。

  外部区域之间不需要策略，因为发送到外部区域的流量将出现在其他外部区域中或者具有对其他外部区域的自动访问权，而这些外部区域对原始外部区域可见。
- 安全策略 2：在上图中，来自 deptB-External 的流量仍以 deptB-trust 区域为目标，并且必须配置一个安全策略以允许此行为。策略必须允许从源区域 (deptB-External) 到目标区域 (deptB-trust) 的流量。

可以将虚拟系统 departmentB 配置为组织来自虚拟系统 departmentA 的流量，反之亦然。与来自任何其他区域的流量一样，必须通过策略明确允许来自外部区域的流量达到虚拟系统中的其他区域。

除了不离开防火墙的虚拟系统间流量所需要的外部区域外，如果您配置共享网关，则还需要外部区域，在这种情况下，流量将离开防火墙。

## VSYS 间的通信使用两个会话

两个虚拟系统之间的通信使用两个会话，与此不同的是，单个虚拟系统只使用一个会话，理解这一点很有帮助。我们来比较一下不同情况。

情况 1 — Vsys1 具有两个区域：trust1 和 untrust1。trust1 区域中的主机在需要与 untrust1 区域中的设备通信时会启动流量。主机将流量发送到防火墙，并且防火墙为源区域 trust1 到目标区域 untrust1 创建会话。此流量仅需要一个会话。

情况 2 — vsys1 中的主机需要访问 vsys2 上的服务器。trust1 区域中的主机启动到防火墙的流量，并且防火墙创建第一个会话：源区域 trust1 到目标区域 untrust1。流量路由到 vsys2（以内部或外部方式）。然后防火墙创建第二个会话：源区域 untrust2 到目标区域 trust2。这种 vsys 间流量需要两个会话。


© 2019 Palo Alto Networks, Inc.

# 共享网关

本主题包括有关共享网关的以下信息：

- 外部区域和共享网关
- 共享网关的注意事项

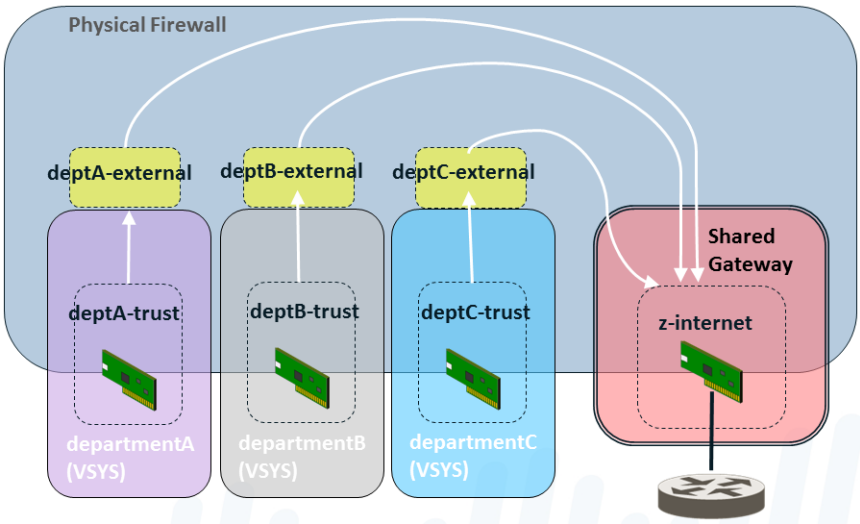
## 外部区域和共享网关

共享网关是多个虚拟系统共享的接口，以便通过互联网进行通信。每个虚拟系统需要一个充当中介的外部区域，以配置安全策略，用于允许或拒绝从虚拟系统内部区域到共享网关的流量。

共享网关使用单个虚拟路由器来路由所有虚拟系统的流量。当某个接口不需要与其相关的完整管理边界时，或者当多个虚拟系统必须共享单个互联网连接时，将使用共享网关。如果 ISP 提供为组织仅提供了一个 IP 地址（接口），但多个虚拟系统需要外部通信，则会出现第二种情况。

与虚拟系统之间的行为不同，不会在虚拟系统与共享网关之间执行安全策略和 App-ID 评估。这就是为何使用共享网关来访问互联网会比创建虚拟系统来访问互联网所需要的开销更低。

在下图中，三个客户共享一个防火墙，但是仅有一个接口能够访问 Internet。如果创建另一个虚拟系统，对于通过所增加的虚拟系统发送到接口的流量，将会增加 App-ID 和安全策略评估的开销。为避免添加另一个虚拟系统，解决方案是配置一个共享网关，如下图中所示。




共享网关具有一个可全球路由的 IP 地址，用于与外部世界进行通信。虚拟系统中的接口也具有 IP 地址，但是这些 IP 地址为专用、不可路由的 IP 地址。

您需要记住一点，管理员必须指定某个虚拟系统是否对另一个虚拟系统可见。与虚拟系统不同，共享网关始终对防火墙上的所有虚拟系统可见。

共享网关 ID 编号在 Web 界面中显示为 **sg<ID**。建议您使用包含共享网关 ID 号的名称来命名共享网关。

向共享网关中添加区域或接口之类的对象时，共享网关在 vsys 菜单中显示为可用的虚拟系统。

共享网关是虚拟系统的限制版本；它支持 NAT 和基于策略的转发 (PBF)，但不支持安全性、DoS 策略、QoS、解密、应用程序替代或身份验证策略。

## 共享网关的注意事项

在配置共享网关时，切记以下几点。



© 2019 Palo Alto Networks, Inc.

- 共享网关情况中的虚拟系统通过共享网关的物理接口，使用单个 IP 地址来访问 Internet。如果虚拟系统的 IP 地址不是可全球路由，请配置源 NAT 以将这些地址转换为可全球路由的 IP 地址。
- 虚拟路由器通过共享网关路由所有虚拟系统的流量。
- 虚拟系统的默认路由应指向共享网关。
- 必须为每个虚拟系统配置安全策略以允许内部区域与外部区域（对共享网关可见）之间的流量。
- 防火墙管理员应控制虚拟路由器，以便虚拟系统的任何成员都不会影响其他虚拟系统的流量。
- 在 Palo Alto Networks 防火墙中，一个数据包可能从一个虚拟系统跳跃到另一个虚拟系统或共享网关。一个数据包不能遍历两个以上的虚拟系统或共享网关。例如，数据包无法从 vsys1 至 vsys2 至 vsys3，或类似的从 vsys1 至 vsys2 至共享网关 1。两个例子都设计两个以上的虚拟系统，这是不被允许的。

为了节省配置时间和精力，请考虑共享网关的以下优势：

- 您可以为共享网关配置 NAT，而不是为与共享网关相关联的多个虚拟希望配置 NAT。
- 您可以为共享网关配置基于策略的路由 (PBR)，而不是为与共享网关相关联的多个虚拟希望配置 NAT。


© 2019 Palo Alto Networks, Inc.

# 配置虚拟系统

创建虚拟系统要求您满足以下条件：

- **superuser**（超级用户）管理角色。
- 配置了接口。
- 虚拟系统许可证（如果创建的虚拟系统数量超过平台上支持的基本数量）。请参阅虚拟系统的平台支持和许可。

STEP 1 | 启用虚拟系统

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑 常规设置。
2. 选中 **Multi Virtual System Capability**（多个虚拟系统功能）复选框，然后单击 **OK**（确定）。如果您批准，则此操作将触发提交。

   只有在启用虚拟系统之后，**Device**（设备）选项卡才会显示 **Virtual Systems**（虚拟系统）和 **Shared Gateways**（共享网关）选项。

STEP 2 | 创建虚拟系统。

1. 选择 **Device**（设备）> **Virtual Systems**（虚拟系统），单击 **Add**（添加），然后输入附加在“vsys”后面的虚拟系统 **ID**（范围为 1 至 255）。

   默认为 *vsys1*。因为 *vsys1* 与防火墙上的内部层次结构相关，因此无法删除；*vsys1* 甚至会出现在不支持多个虚拟系统的防火墙型号上。
2. 如果您希望允许防火墙将解密内容转发到外部服务，请选择 **Allow forwarding of decrypted content**（允许转发解密内容）。例如，您必须启用此选项，防火墙才能将解密内容发送到 WildFire 进行分析。
3. 输入虚拟系统的描述性 **Name**（名称）。允许使用字母数字（最多 31 个）、空格和下划线字符。

STEP 3 | 将接口分配给虚拟系统。

虚拟路由器、虚拟线路或 VLAN 可能已经配置，或者您可以稍后配置，届时可指定与其相关的虚拟系统。

1. 在 **General**（常规）选项卡上，如果您希望将 DNS 代理规则应用于接口，请选择 **DNS Proxy**（DNS 代理）对象。
2. 在 **Interfaces**（接口）字段中，单击 **Add**（添加）以输入要分配给虚拟系统的接口或子接口。一个接口只能属于一个虚拟系统。
3. 根据您的虚拟系统中需要的部署类型，执行以下任何操作：
   - 在 **VLANs** 字段中，单击 **Add**（添加）以输入要分配给 vsys 的 VLAN。
   - 在 **Virtual Wires** 字段中，单击 **Add**（添加）以输入要分配给 vsys 的 Virtual Wire。
   - 在 **Virtual Routers**（虚拟路由器）字段中，单击 **Add**（添加）以输入要分配给 vsys 的虚拟路由器。
4. 在 **Visible Virtual System**（可见虚拟系统）字段中，选中应对正在配置的虚拟系统设为可见的所有虚拟系统。对于需要彼此通信的虚拟系统，这是必需的。

   在需要严格管理边界的多租户情况下，将不会检查虚拟系统。
5. 单击 **OK**（确定）。

STEP 4 | （可选）限制对虚拟系统允许的会话、规则和 VPN 隧道的资源分配。能够根据虚拟系统分配限制，这种灵活性可让您有效地控制防火墙资源。

1. 在 **Resource**（资源）选项卡上，可以选择设置虚拟系统的限制。每个字段显示值的有效范围，该值因防火墙型号而异。默认值为 0，表示虚拟系统的限制是防火墙型号的限制。但是，对于每个虚拟系



© 2019 Palo Alto Networks, Inc.

统而言，特定设置的限制不能复制。例如，如果防火墙有 4 个虚拟系统，则每个虚拟系统不能具有每个防火墙允许的解密规则总数。在所有虚拟系统的解密规则总数达到防火墙限制后，您无法再继续添加。

- 会话限制

  如果使用 *show session meter CLI* 命令，将显示每个数据面板允许的最大会话数、虚拟系统正在使用的当前会话数，以及每个虚拟系统的会话调节次数。在 *PA-5200* 或 *PA-7000* 系列防火墙上，因为每个虚拟系统有多个数据面板，当前使用的会话数可能会大于配置的最大会话限制。*PA-5200* 系列或 *PA-7000* 系列防火墙上配置的会话限制依据每个数据面板而定，将导致每个虚拟系统较高的最大值。
- 安全规则
- **NAT** 规则
- 解密规则
- **QoS** 规则
- 应用程序替代规则
- 基于策略的转化规则
- 身份验证规则
- **DoS** 保护规则
- 站点到站点 **VPN** 隧道
- 并发 **SSL VPN** 隧道

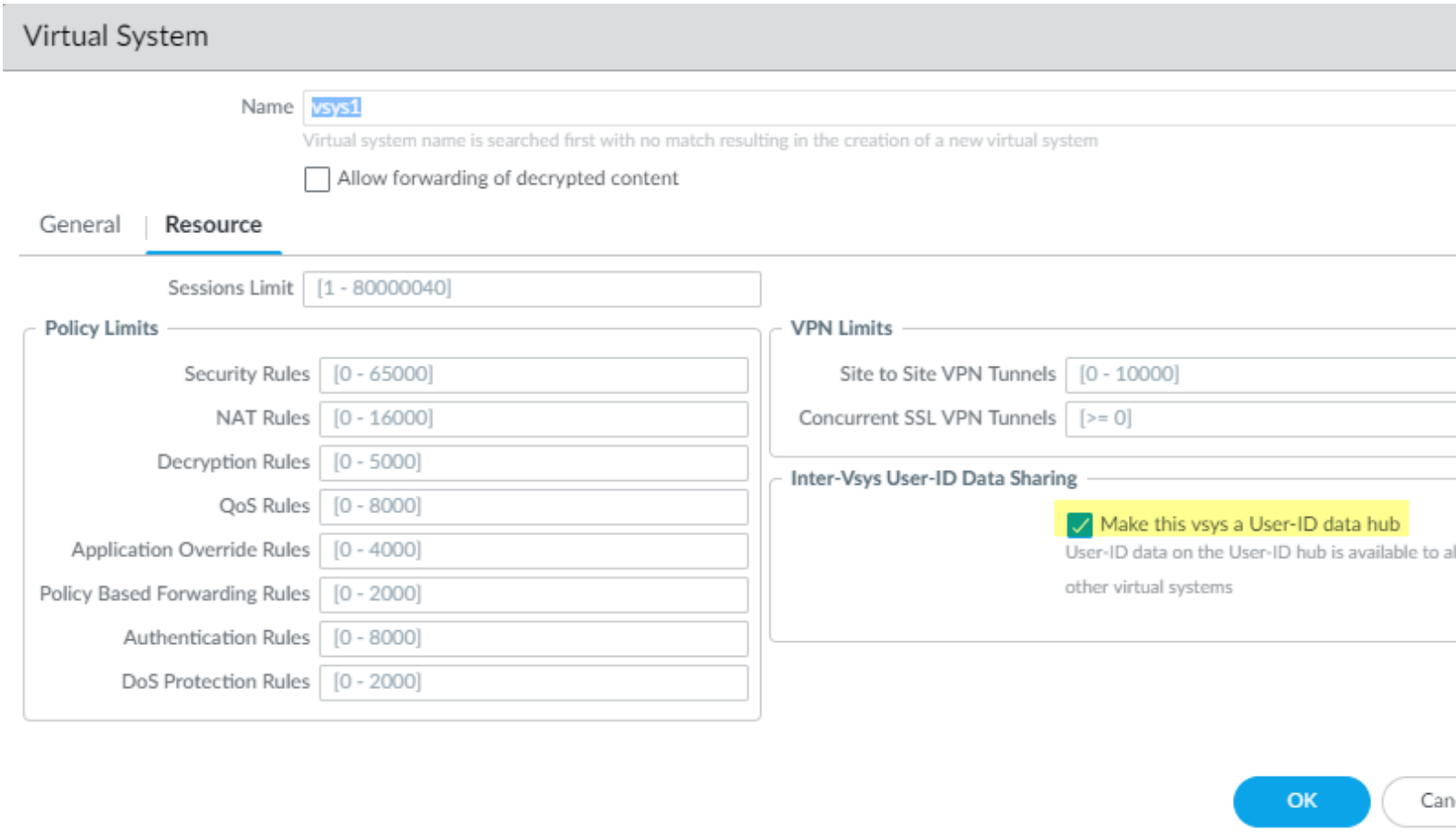
2. 单击 **OK**（确定）。

STEP 5 | （可选）配置虚拟系统为 User-ID 中心，以共享跨虚拟系统的 User-ID 映射。

源自终端服务代理和组映射的 *IP* 地址和端口到用户名的映射信息不能在虚拟系统集线器和连接虚拟系统之间共享。

1. 对于任何现有虚拟系统，将您想要共享的 User-ID 源配置（例如，受监控服务器和 User-ID 代理）传输到您想要用作中心的虚拟系统。
2. 在 **Resource**（资源）选项卡上，选择 **Make this vsys a User-ID data hub**（将此 **vsys** 设为 **User-ID** 数据中心）。


© 2019 Palo Alto Networks, Inc.

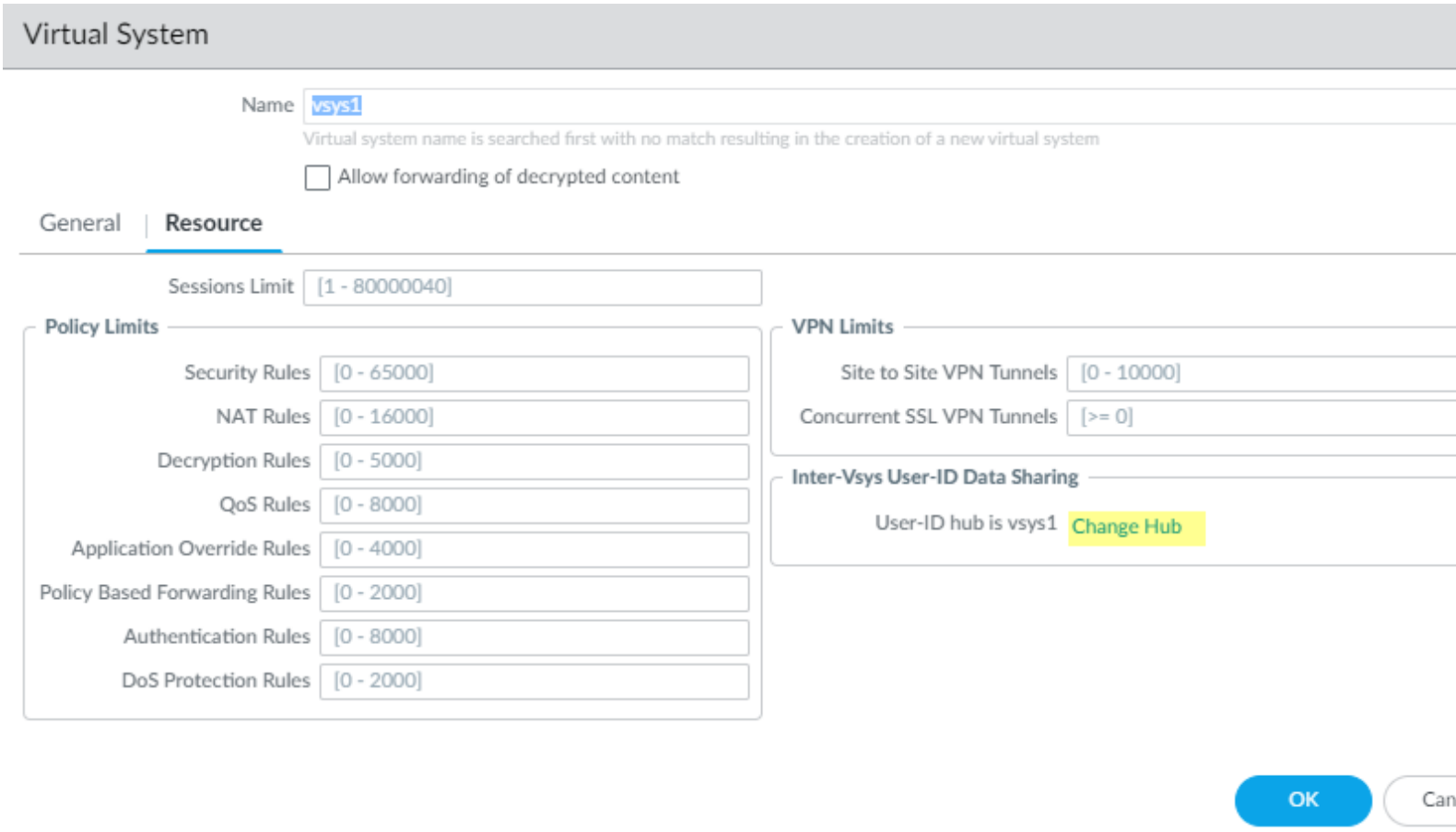



3. 单击 **Yes**（是）以确认，然后单击 **OK**（确定）。

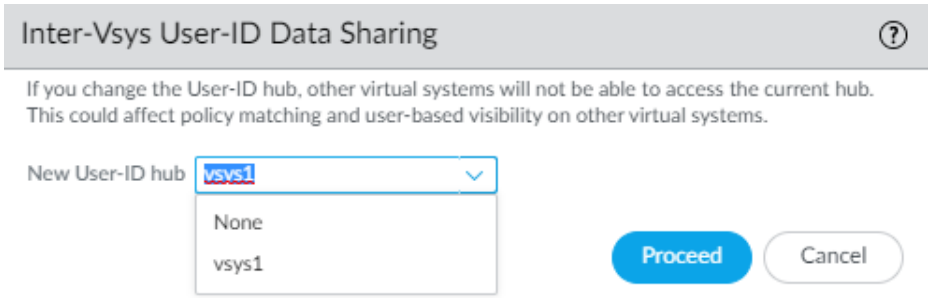
   如果要将 User-ID 中心更改为不同的虚拟系统或禁用 User-ID 中心，请选择当前配置为 User-ID 中心的虚拟系统，然后选择 **Resource**（资源）> **Change Hub**（更改中心）。



© 2019 Palo Alto Networks, Inc.




从列表中选择 **New User-ID hub**（新 **User-ID** 中心），或选择 **none**（无）以禁用 User-ID 中心，并停止在虚拟系统之间共享映射。




单击 **OK**（确定）以确认，然后提交更改。

STEP 6 | 提交配置。

单击 **Commit**（提交）。虚拟系统现在是一个可从 **Objects**（对象）选项卡中访问的对象。

STEP 7 | 为每个虚拟系统创建至少一个虚拟路由器，以使虚拟系统能够处理联网功能，如静态路由和动态路由。

或者，您的虚拟系统可能使用 VLAN 或 Virtual Wire，取决于您的部署。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后按 **Name**（名称）**Add**（添加）虚拟路由器。
2. 对于 **Interfaces**（接口），单击 **Add**（添加），然后选择属于虚拟路由器的接口。
3. 单击 **OK**（确定）。



© 2019 Palo Alto Networks, Inc.

STEP 8 | 为虚拟系统中的每个接口配置一个安全区域。

针对至少一个接口，创建第 3 层安全区域。请参阅配置接口和区域。

STEP 9 | 配置安全策略规则以允许或拒绝在虚拟系统区域之间进入和传出流量。

请参阅创建安全策略规则。

STEP 10 | 提交配置。

单击 **Commit**（提交）。



在创建虚拟系统后，您可以使用 *CLI* 仅为某个特定虚拟主机提交配置。

```
commit partial vsys <vsys-id>
```

STEP 11 | （可选）查看为虚拟系统配置的安全策略。

打开 SSH 会话以使用 CLI。要在操作模式下查看某个虚拟系统的安全策略，请使用以下命令：

```
set system setting target-vsys <vsys-id>
show running security-policy
```



© 2019 Palo Alto Networks, Inc.

# 在防火墙中配置虚拟系统间通信

如果以下用例（可能是在单个企业中）：您希望虚拟系统能够在防火墙中彼此通信，请执行以下任务。留在防火墙的 VSYS 间流量中描述了此类情况。此任务假定：

- 您已完成任务，请配置虚拟系统。
- 在 **Visible Virtual System**（可见虚拟系统）字段中配置虚拟系统时，您选中了必须彼此通信的所有虚拟系统的框，以使彼此可见。

STEP 1 | 为每个虚拟系统配置一个外部区域。

1. 选择 **Network**（网络）> **Zones**（区域），然后按 **Name**（名称）**Add**（添加）一个新区域。
2. 对于 **Location**（位置），请选择要创建外部区域的虚拟系统。
3. 对于 **Type**（类型），请选择 **External**（外部）。
4. 对于 **Virtual Systems**（虚拟系统），请单击 **Add**（添加），并输入外部区域可以访问的虚拟系统。
5. （可选）选择一个提供泛滥、侦察或基于数据包的攻击防护的 **Zone Protection Profile**（区域保护配置文件）（或稍后配置一个）。
6. （可选）在 **Log Setting**（日志设置）中，选择日志转发配置文件，用于将区域保护日志转发到外部系统。
7. （可选）选中 **Enable User Identification**（启用用户标识）以便为外部区域启用 User-ID。
8. 单击 **OK**（确定）。

STEP 2 | 配置安全策略规则以允许或拒绝从虚拟系统内部区域到外部区域（和反向）的流量。

- 请参阅创建安全策略规则。
- 请参阅留在防火墙的 VSYS 间流量。

STEP 3 | 提交更改。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 配置共享网关

如果您需要多个虚拟系统共享某个与 Internet 的接口（共享网关），请执行此任务。此任务假定：

- 可以使用可全球路由的 IP 地址来配置接口，这将成为一个共享网关。
- 您已完成先前的任务，请配置虚拟系统。对于接口，您选择了具有可全球路由的 IP 地址的外部面向接口。
- 在 **Visible Virtual System**（可见虚拟系统）字段中配置虚拟系统时，您选中了必须通信的所有虚拟系统的框，以使彼此可见。

STEP 1 | 配置共享网关。

1. 选择 **Device**（设备）> **Shared Gateway**（共享网关），单击 **Add**（添加），然后输入 **ID**。
2. 输入一个有意义的 **Name**（名称），首选包括网关的 **ID**。
3. 在 **DNS Proxy**（**DNS** 代理）字段中，如果您希望将 DNS 代理规则应用于接口，请选择 DNS 代理对象。
4. **Add**（添加）一个连接到外部世界的 **Interface**（接口）。
5. 单击 **OK**（确定）。

STEP 2 | 配置共享网关的区域。



向共享网关中添加区域或接口等对象时，共享网关自身将在 *VSYS* 菜单中列为可用的 *vsys*。

1. 选择 **Network**（网络）> **Zones**（区域），然后按 **Name**（名称）**Add**（添加）一个新区域。
2. 对于 **Location**（位置），请选择要创建区域的共享网关。
3. 对于 **Type**（类型），请选择 **Layer3**（第 2 层）。
4. （可选）选择一个提供泛滥、侦察或基于数据包的攻击防护的 **Zone Protection Profile**（区域保护配置文件）（或稍后配置一个）。
5. （可选）在 **Log Setting**（日志设置）中，选择日志转发配置文件，用于将区域保护日志转发到外部系统。
6. （可选）选中 **Enable User Identification**（启用用户标识）复选框以便为共享网关启用 User-ID。
7. 单击 **OK**（确定）。

STEP 3 | 提交更改。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 自定义虚拟系统的服务路由

为多个虚拟系统启用防火墙时，虚拟系统将继承全局服务和服务路由设置。例如，防火墙可以使用共享电子邮件服务器向所有虚拟系统发出电子邮件警报。在某些情况下，您需要为每个虚拟系统创建不同的服务路由。

在虚拟系统级配置服务路由的一个用例是，比如您是需要在单个 Palo Alto Networks 防火墙上支持多个单独租户的 ISP。每个租户都需要自定义服务路由来访问服务，如 DNS、Kerberos、LDAP、NetFlow、RADIUS、TACACS +、多重因素身份验证、电子邮件、SNMP 陷阱、syslog、HTTP、User-ID 代理、VM 监控和 Panorama（内容部署和软件更新）。另一个用例是 IT 组织希望为组（为服务设置了服务器）提供完全自治权。每个组都可以有虚拟系统并定义其自己的服务路由。

对于虚拟系统中的服务路由，您可以选择虚拟路由器；不能选择传出接口。在选择虚拟路由器且防火墙从虚拟路由器发送数据包后，该防火墙会根据目标 *IP* 地址选择传出接口。因此，如果虚拟系统有多个虚拟路由器，则发送到服务的所有服务器的数据包必须仅从一个虚拟路由器传出。具有接口源地址的数据包可能从不同的接口传出，但返回的流量可能从具有源 *IP* 地址的接口传入，从而形成非对称流量。

- 将服务路由自定义为虚拟系统的服务
- 将 PA-7000 系列防火墙配置为对每个虚拟系统进行记录
- 配置每个虚拟系统或防火墙的管理员访问权限

## 将服务路由自定义为虚拟系统的服务

如果已启用多个虚拟系统功能，则没有配置特定服务路由的任何虚拟系统都会继承防火墙的全局服务和服务路由设置。您可以将虚拟系统配置为使用不同的服务路由，如以下工作流程所述。

具有多个虚拟系统的防火墙必须有 IP 地址不重叠的接口和子接口。针对 SNMP 陷阱或 Kerberos 的每虚拟系统服务路由仅可使用 IPv4 地址。

服务的服务路由将严格遵循您为该服务配置服务器配置文件的方式：

- 如果定义共享位置的服务器配置文件（**Device**（设备）> **Server Profiles**（服务器配置文件）），则防火墙将全局服务路由用于该服务。
- 如果定义特定虚拟系统的服务器配置文件，则防火墙将虚拟系统特定服务路由用于该服务。
- 如果定义特定虚拟系统的服务器配置文件，但未配置该服务的虚拟系统特定服务路由，则防火墙将全局服务路由用于该服务。

防火墙支持根据虚拟系统转发 *Syslog*。当要将防火墙上的多个虚拟系统连接到使用 *SSL* 传输的 *Syslog* 服务器时，防火墙可以生成唯一的证书，用于保护通信安全。防火墙不支持每个虚拟系统都拥有专用证书。

STEP 1 | 自定义虚拟系统的服务路由。

1. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Virtual Systems**（虚拟系统），并选择要配置的虚拟系统。
2. 单击 **Service Route Configuration**（服务路由配置）链接。
3. 选择一个：
   - **Inherit Global Service Route Configuration**（继承全局服务路由配置）— 可让虚拟系统继承虚拟系统相关的全局服务路由设置。如果选择此选项，请跳过自定义步骤。
   - **Customize**（自定义）— 允许您指定每项服务的源地址。
4. 如果选择 **Customize**（自定义），请根据提供服务供使用的服务器寻址类型选择 **IPv4** 或 **Ipv6** 选项卡。您可以为服务同时指定 IPv4 及 IPv6 地址。点击服务。（仅与虚拟系统相关的服务可用。）



© 2019 Palo Alto Networks, Inc.

要轻松使用多个服务的相同源地址，请选中服务的复选框，单击 *Set Selected Routes*（设置所选路由），然后继续。

- 要限制源地址列表，请选择 **Source Interface**（源接口），然后选择源地址（来自该接口）作为服务路由。选择 **Any**（任何）源接口，以在您从中选择地址的源地址列表中为虚拟系统可用的所有接口上的所有 IP 地址。您可以选择 **Inherit Global Setting**（继承全局设置）。
- 如果您为 **Source Interface**（源接口）选择 **Inherit Global Setting**（继承全局设置），则 **Source Address**（源地址）会指示 **Inherited**（已继承），或者会指示所选的源地址。如果您为 **Source Interface**（源接口）选择了 **Any**（任意），请从列表中选择 IP 地址，或者输入 IP 地址（使用与所选选项相匹配的 IPv4 或 IPv6 格式），以指定要在发送到外部服务的数据包中使用的源地址。
- 如果您修改了地址对象和 IP 类型 (IPv4/IPv6)，则需要 **Commit**（提交）以更新要使用的服务路由类型。

5. 单击 **OK**（确定）。
6. 重复之前的步骤以配置其他外部服务的源地址。
7. 单击 **OK**（确定）。

STEP 2 | 提交更改。

单击 **Commit**（提交）和 **OK**（确定）。

如果您正在为 PA-7000 系列防火墙的日志记录服务配置每个虚拟系统的服务路由，请继续执行任务将 PA-7000 系列防火墙配置为对每个虚拟系统进行记录。

# 将 PA-7000 系列防火墙配置为对每个虚拟系统进行记录

对于流量、HIP 匹配、威胁和 WildFire 日志类型，PA-7000 系列防火墙对 SNMP 陷阱、Syslog 和电子邮件服务不使用服务路由。相反，PA-7000 系列防火墙通过日志记录卡提供支持。

根据您的防火墙配置，您可能拥有以下卡类型之一：

- 日志处理卡 **(LPC)** —支持从本地部署的交换机上的 LPC 子接口到服务器上的相应服务的特定虚拟系统路径。对于系统和配置日期，PA-7000 系列防火墙使用全局服务路由，而不是 LPC。如果您的防火墙已安装 LPC，您需要配置一个日志卡端口。
- 日志转发卡 **(LFC)** — 支持将所有数据平面日志的高速日志转发至外部日志收集器（例如，Panorama 和系统日志服务器）。您可以为虚拟系统创建和配置子接口。如果您的防火墙已安装 LFC，您无需配置日志卡端口。

在其他 Palo Alto Networks 模式下，该数据面板会将日志记录路由流量发送到管理面板，从而将流量发送到日志记录服务器。在 PA-7000 系列防火墙上，LPC 或 LFC 仅有一个接口，且多个虚拟系统的数据面板会将日志记录服务器流量（类型如上所述）发送到 PA-7000 系列防火墙日志记录卡。日志记录卡配有多个子接口，平台通过这些子接口将日志服务流量发送到客户的交换机，而客户的交换机可连接到多个日志服务器。

每个子接口可配置一个子接口名称和一个点分子接口号。该子接口会分配给为日志记录服务配置的虚拟系统。PA-7000 系列防火墙功能上的其他服务路由与其他 Palo Alto Networks 平台上的服务路由相似。有关 LPC 或 LFC 的信息，请参阅《PA-7000 系列硬件参考指南》。

- 将 PA-7000 系列 LPC 配置为对每个虚拟系统进行记录
- 将 PA-7000 系列 LFC 配置为对每个虚拟系统进行记录

## 将 *PA-7000* 系列 *LPC* 配置为对每个虚拟系统进行记录

如果您已在安装了日志处理卡 (LPC) 的 PA-7000 系列防火墙上启用多个虚拟系统功能，则可以为不同的虚拟系统配置日志记录，具体流程如下所述。

STEP 1 | 创建日志卡子接口。



© 2019 Palo Alto Networks, Inc.

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择要充当日志卡接口的接口。
2. 输入 **Interface Name**（接口名称）。
3. 对于 **Interface Type**（接口类型），请选择 **Log Card**（日志卡）。
4. 单击 **OK**（确定）。

STEP 2 | 在 LPC 物理接口上为每个租户添加子接口。

1. 高亮显示属于日志卡接口类型的 Ethernet 接口，然后单击 **Add Subinterface**（添加子接口）。
2. 对于 **Interface Name**（接口名称），完成添加后，输入分配给租户的虚拟系统的子接口。
3. 对于 **Tag**（标记），输入 VLAN 标记值。

   为了便于使用，让该标记与子接口编号保持一致，但编号可能不同。

4. （可选）输入 **Comment**（注释）。
5. 在 **Config**（配置）选项卡上的 **Assign Interface to Virtual System**（将接口分配给虚拟系统）字段中，选择分配了 LPC 子接口的虚拟系统。此外，可以单击 **Virtual Systems**（虚拟系统）链接以添加新的虚拟系统。
6. 单击 **OK**（确定）。

STEP 3 | 输入分配给子接口的地址，然后配置默认网关。

1. 选择 **Log Card Forwarding**（日志卡转发）选项卡，然后执行以下其中一项或两项操作：
   - 对于 IPv4 部分，输入分配给子接口的 **IP Address**（IP 地址）和 **Netmask**（子网掩码）。输入 **Default Gateway**（默认网关）（要发送数据包的下一个跃点在路由信息库 [RIB] 中没有已知的下一个跃点地址）。
   - 对于 IPv6 部分，输入分配给子接口的 **IPv6 Address**（IPv6 地址）。输入 **IPv6 Default Gateway**（IPv6 默认网关）。
2. 单击 **OK**（确定）。

STEP 4 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

STEP 5 | 如果尚未执行上述操作，请为虚拟系统配置剩余的服务路由。

自定义虚拟系统的服务路由。

## 将 *PA-7000* 系列 *LFC* 配置为对每个虚拟系统进行记录

如果您已在安装了日志转发卡 (LFC) 的 PA-7000 系列防火墙上启用多个虚拟系统功能，则可以为不同的虚拟系统配置日志记录，具体流程如下所述。

STEP 1 | 创建日志转发卡子接口。

1. 选择 **Device**（设备）> **Log Forwarding Card**（日志转发卡）并添加子接口。
2. 对于 **Interface Name**（接口名称），完成添加后，输入分配给租户的虚拟系统的子接口。
3. （可选）输入 **Comment**（注释）。
4. 对于 **Tag**（标记），输入 VLAN 标记值。

   为了便于使用，让该标记与子接口编号保持一致，但编号可能不同。


© 2019 Palo Alto Networks, Inc.

5. 在 **Config**（配置）选项卡上的 **Assign Interface to Virtual System**（将接口分配给虚拟系统）字段中，选择分配了 LFC 子接口的虚拟系统。此外，可以单击 **Virtual Systems**（虚拟系统）链接以添加新的虚拟系统。
6. 单击 **OK**（确定）。

STEP 2 | （可选）输入分配给子接口的地址，然后配置默认网关。

1. 选择 **Network**（网络）选项卡，然后执行以下其中一项或两项操作：
   - 对于 IPv4 部分，输入分配给子接口的 **IP Address**（IP 地址）和 **Netmask**（子网掩码）。输入 **Default Gateway**（默认网关）（要发送数据包的下一个跃点在路由信息库 [RIB] 中没有已知的下一个跃点地址）。
   - 对于 IPv6 部分，输入分配给子接口的 **IPv6 Address**（IPv6 地址）。输入 **IPv6 Default Gateway**（IPv6 默认网关）。
2. 单击 **OK**（确定）。

STEP 3 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

# 配置每个虚拟系统或防火墙的管理员访问权限

如果您拥有超级用户管理帐户，就可以为 vsysadmin 或设备管理员角色创建和配置更精细的权限。

STEP 1 | 创建授予或禁止管理员配置或只读网络接口多个区域的权限的管理员角色配置文件。

1. 选择 **Device**（设备）> **Admin Roles**（管理员角色），然后 **Add**（添加）一个 **Admin Role Profile**（管理员角色配置文件）。
2. 输入配置文件的 **Name**（名称），也可选择输入 **Description**（说明）。
3. 对于 **Role**（角色），请指定配置文件会影响的控制级别：
   - **Device**（设备）— 配置文件允许管理全局设置和任何虚拟系统。
   - **Virtual System**（虚拟系统）— 配置文件允许只管理分配给拥有此配置文件的管理员的虚拟系统。（管理员可以访问 **Device**（设备）> **Setup**（设置）> **Services**（服务）> **Virtual Systems**（虚拟系统），但不能访问 **Global**（全局）选项卡。）
4. 在管理员角色配置文件的 **Web UI** 选项卡上，向下滚动到 **Device**（设备），并保留绿色标记（启用）。
   - 在 **Device**（设备）下，启用 **Setup**（设置）。在 **Setup**（设置）下，启用该配置文件要为管理员授予配置权限的区域，如下图所示。（如果允许授予此设置只读权限，则启用/禁用旋转中会显示只读锁定图标。）
     - **Management**（管理）— 允许管理员使用该配置文件在 **Management**（管理）选项卡上配置设置。
     - **Operations**（操作）— 允许管理员使用该配置文件在 **Operations**（操作）选项卡上配置设置。
     - **Services**（服务）— 允许管理员使用该配置文件在 **Services**（服务）选项卡上配置设置。管理员必须启用 **Services**（服务），以访问 **Device**（设备）> **Setup Services**（设置服务）> **Virtual Systems**（虚拟系统）选项卡。如果在上一步骤中将 **Role**（角色）指定为 **Virtual System**（虚拟系统），**Services**（服务）是在 **Device**（设备）> **Setup**（设置）下唯一可启用的设置。
     - **Content-ID** — 允许管理员使用该配置文件在 **Content-ID** 选项卡上配置设置。
     - **WildFire** — 允许管理员使用该配置文件在 **WildFire** 选项卡上配置设置。
     - **Session**（会话）— 允许管理员使用该配置文件在 **Session**（会话）选项卡上配置设置。
     - **HSM** — 允许管理员使用该配置文件在 **HSM** 选项卡上配置设置。
5. 单击 **OK**（确定）。
6. （可选）根据需要重复所有步骤以创建包含不同权限的其他管理员角色配置文件。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 将管理员角色配置文件应用到管理员。

1. 选择 **Device**（设备）> **Administrators**（管理员），单击 **Add**（添加），然后输入 **Name**（名称）以添加管理员。
2. （可选）选择 **Authentication Profile**（身份验证配置文件）。
3. （可选）选择 **Use only client certificate authentication(Web)**（仅使用客户端证书身份验证 **(Web)**）以执行双向身份验证；以及让服务器对客户端进行身份验证。
4. 输入 **Password**（密码）和 **Confirm Password**（确认密码）。
5. （可选）如果您想使用一种更强大的基于私钥的身份验证方法（使用 SSH 公钥而非只是密码），请选择 **Use Public Key Authentication (SSH)**（使用公钥身份验证 **(SSH)**）。
6. 对于 **Administrator Type**（管理员类型），请选择 **Role Based**（基于角色）。
7. 对于 **Profile**（配置文件），请选择刚创建的配置文件。
8. （可选）选择 **Password Profile**（密码配置文件）。
9. 单击 **OK**（确定）。

STEP 3 | 提交配置。

单击 **Commit**（提交）。



© 2019 Palo Alto Networks, Inc.

# 包含其他特征的虚拟系统功能

大部分防火墙的特征和功能都可以按照虚拟系统被配置、查看、记录或报告。因此，在文档中的其他相关位置中提到了虚拟系统，并且此处不会重复这一信息。以下是部分具体章节：

- 如果您在配置主动/被动 HA，则两个防火墙必须具有相同的虚拟系统能力（单个或多个虚拟系统能力）。请参阅高可用性。
- 要为虚拟系统配置 QoS，请参阅为虚拟系统配置 QoS。
- 有关在使用子接口（以及 VLAN 标记）的虚拟线路部署中配置带有虚拟系统的防火墙的信息，请参阅虚拟线路接口。
- 如果您配置了 User-ID 和多个虚拟系统，您可以在虚拟系统之间共享用户映射。请参阅共享跨虚拟系统的 User-ID 映射。

# 区域保护和 *DoS* 保护

将网络分段为功能和组织区域可减少网络攻击面 — 网络暴露于潜在攻击者的部分。区域保护可为区域防御泛滥攻击、侦察尝试、基于数据包的攻击、以及使用非 IP 协议的攻击。自定义用于保护各个区域的区域保护配置文件（您可将相同的配置文件应用于类似区域）。拒绝服务 (DoS) 保护为特定关键系统提供针对泛滥攻击的防御，尤其是用户通过 Internet 访问的设备，例如 Web 服务器和数据库服务器，并保护资源免遭会话泛滥攻击。自定义用于保护每组关键设备的 DoS 保护配置文件和策略规则。访问最佳实践文档门户，获取区域保护和 DoS 保护最佳实践列表。



测量并监控防火墙数据面板 *CPU* 消耗，确保每个防火墙的大小适当，可支持 *DoS* 和区域保护以及消耗 *CPU* 周期的任何其他特征，例如解密。如果使用 *Panorama* 管理防火墙，则使用设备监控（*Panorama* > *Managed Devices*（受管设备）> *Health*（健康））以便一次性检查和监控所有受管防火墙的 *CPU* 消耗。

- 使用区域进行网络分段
- 区域如何保护网络？
- 区域防御
- 配置区域保护以提高网络安全性
- DoS 保护新会话不受泛滥攻击

# 使用区域进行网络分段

网络越大越难保护。一个庞大且未分段的网络攻击面较大，难以进行管理和保护。因为流量和应用程序可以访问整个网络，一旦进入网络，攻击者便可在网络上横向移动以访问关键数据。此外，监控和控制大的网络难度也较大。分段网络阻止区域之间的横向移动，进而限制攻击者在网络上移动的能力。

安全区域是一组一个或多个物理或虚拟防火墙接口以及连接到区域接口的网络分段组成。您可以单独控制每个区域的保护，以便每个区域获得所需的特定保护。例如，用于财务部门的区域可能不需要接受 IT 区域允许的所有应用程序。

为了充分保护您的网络，所有流量必须流经防火墙。配置接口和区域为不同的功能区域（如互联网网关、敏感数据存储和商务应用程序）以及不同的组织组（如财务、IT、营销和工程）创建单独区域。无论功能、应用程序使用情况或用户访问权限是否存在逻辑划分，您都可以创建一个单独的区域来隔离和保护该区域，并应用适当的安全策略规则，以防止不必要地访问只有一个组或某些组需要访问的数据和应用程序。区域越精细，对网络流量的可见性和控制就越多。将您的网络划分为多个区域有助于创建一个零信任体系结构，该体系结构执行安全理念，即不信任任何用户、设备、应用程序或数据包，并验证所有内容。最终目标是创建一个允许仅访问具有合法业务需求的用户、设备和应用程序，并拒绝所有其他流量的网络。

如何适当限制和允许访问区域取决于网络环境。例如，诸如半导体制造地板或机器人组装工厂（其中工作站控制敏感的制造设备或高度受限的访问区域）之类的环境可能需要不允许外部设备访问的物理分段（无移动设备访问）。

在用户可以使用移动设备访问网络的环境中，启用 User-ID 和 App-ID，并将网络分段成区域，确保用户能在任何网络访问接口接收到适当的访问权限，因为访问权限与用户或用户组相关，而不是绑定到特定区域中的设备。

不同功能区和组的保护要求也可能不同。例如，处理大量流量的区域可能需要与通常处理较少流量的区域不同的泛滥攻击阈值。为每个区域定义适当保护的能力是进行网络分段的另一个原因。适当的保护类型取决于您的网络架构、您要保护的内容以及您要允许和拒绝的流量。



© 2019 Palo Alto Networks, Inc.

# 区域如何保护网络？

区域不仅可以通过将网络分割成更小、更易管理的区域来进行保护，而且还可以在您能控制区域访问以及区域之间流量移动的情况下保护网络。

区域防止不受控制的流量通过防火墙接口进入您的网络，因为防火墙接口在分配给区域之前无法处理流量。防火墙在入口接口（流量按从始发客户端到响应服务器 (c2s) 的流向进入防火墙）上应用区域保护，以在进入区域之前筛选流量。

防火墙接口类型和区域类型（旁接、虚拟线路、L2、L3、隧道或外部）必须匹配，这有助于防止网络允许不属于某个区域的流量。例如，您可以将 L2 接口分配到 L2 区域或将 L3 接口分配到 L3 区域，但不能将 L2 接口分配到 L3 区域。

另外，防火墙接口只能属于一个区域。专用于不同区域的流量不能使用相同的接口，这有助于防止不当流量进入区域，并使您能够配置适用于每个区域的保护。您可以将多个防火墙接口连接到区域以增加带宽，但每个接口只能与一个区域相连接。

在防火墙允许流量进入区域之后，流量在该区域内自由流动，并且不会被记录。创建的每个区域越小，访问每个区域的流量的控制就越多，恶意软件在区域之间的网络间横向移动就越困难。除非安全策略规则允许，并且区域具有相同的区域类型（旁接、虚拟线路、L2、L3、隧道或外部），否则流量不能在区域之间流动。例如，安全策略规则可以允许两个 L3 区域之间的流量流动，但不允许在 L3 区域和 L2 区域之间的流量流动。当安全策略规则允许区域间流量时，防火墙记录在区域之间流动的流量。

默认情况下，安全策略规则可防止区域之间流量的横向移动，因此恶意软件无法访问一个区域，然后通过网络自由移动到其他目标。



隧道区域用于未加密的隧道。您可以对隧道内容和外部隧道的区域应用不同的安全策略规则，如隧道内容检测概述中所述。



© 2019 Palo Alto Networks, Inc.

# 区域防御

区域保护配置文件将为区域防御泛滥、侦察、基于数据包和基于非 IP 协议的攻击。DoS 保护策略规则中的 DoS 保护配置文件为特定的关键设备防御针对目标泛滥和基于资源的攻击。DoS 攻击会使网络或目标关键系统出现大量不需要的流量，从而尝试中断网络服务。

计划保护您的网络免受不同类型的 DoS 攻击：

- 基于应用程序的攻击——攻击特定应用程序软肋，耗尽应用程序资源，致使合法用户无法使用应用程序。其中一个示例是 Slowloris 攻击。
- 基于协议的攻击 — 也称为状态表耗尽攻击，这些攻击针对协议弱点。SYN 洪泛攻击为其中一个常见案例。
- 容量攻击 — 尝试攻陷可用网络资源（尤其是带宽），并降低目标以阻止合法用户访问这些资源的大容量攻击。其中一个示例是 UDP 泛滥攻击。

不存在默认区域保护配置文件或 DoS 保护配置文件和 DoS 保护策略规则。根据每个区域的流量特征配置并应用区域保护，并基于您想要在每个区域中保护的各个关键系统配置 DoS 保护。

- 区域防御工具
- 区域防御工具如何运行？
- 适用于 Dos 保护的防火墙布置
- 区域保护配置文件
- 数据包缓冲区保护
- DoS 保护配置文件和策略规则

## 区域防御工具

有效的 DoS 攻击防御需要使用分层方法。第一层防御应是面向 Internet 的网络外围中的大容量专用 DDoS 保护设备、外围路由器、交换机或其他具有适当的访问控制列表 (ACL) 的基于硬件的数据包丢弃设备，以防止基于会话的防火墙不能处理的容量攻击。防火墙增添了更细粒度的 DoS 攻击防御，并且还可以查看专用 DDoS 设备无法提供的应用程序流量。

Palo Alto Networks 防火墙提供四种互补工具，以便对您网络区域和关键设备的 DoS 保护提供分层保护：

- 区域保护配置文件可为入口区域边缘防御 IP 泛滥攻击、侦查端口扫描和主机扫掠、基于 IP 数据包的攻击以及非 IP 协议攻击。入口区域是流量依据从客户端流向服务器 (c2s) 的方向进入防火墙的位置，其中客户端是流量的始发者，服务器是响应者。区域保护配置文件通过限制区域内新的每秒连接数(CPS)的方式，根据进入区域的聚合流量提供针对 DoS 攻击的第二层广泛防御。区域保护配置文件应用于进入区域的聚合流量，因此，不考虑单个设备（IP 地址）。

  在防火墙执行 DoS 保护策略和安全策略规则查找之前，区域保护配置文件会在会话形成时保护网络，并且比 DoS 保护策略或安全策略规则查找消耗更少的 CPU 周期。如果区域保护配置文件拒绝流量，则防火墙不会在策略规则查找上消耗 CPU 周期。

  将区域保护配置文件应用于每个区，包括面向 Internet 和内部。
- **DoS 保护配置文件和策略规则**为特定的单个端点和资源提供针对泛滥攻击的防御，尤其是用户从 Internet 访问的高价值目标。虽然区域保护配置文件可防御区域免受泛滥攻击，但具有适当的 DoS 保护配置文件的 DoS 保护策略规则可以保护区域中单个关键系统免遭目标泛滥攻击，提供针对 DoS 攻击的第三层更细粒度的防御。

  因为 *DoS* 保护旨在保护关键设备，并且需要消耗资源，因此，*DoS* 保护仅保护您在 *DoS* 保护策略规则中指定的设备。其他设备不受保护。



© 2019 Palo Alto Networks, Inc.

DoS 保护配置文件会设置泛滥攻击保护阈值（新的 CPS 限制）、资源保护阈值（指定端点和资源的会话限制），以及配置文件是否适用于聚合或分类流量。DoS 保护策略规则指定匹配条件（源、目标、服务端口）、流量匹配规则时采取的操作、以及与每个规则相关联的聚合和分类 DoS 保护配置文件。

聚合 DoS 保护策略规则将在聚合 DoS 保护配置文件中定义的 CPS 阈值应用于符合 DoS 保护策略规则匹配条件的所有设备的组合流量。例如，如果配置聚合 DoS 保护配置文件以限制 CPS 速率为 20000，则 20000 CPS 限制将被应用于整个组的聚合连接数。在这种情况下，一个设备可以接收大多数的允许连接。

分类 DoS 保护策略规则将在分类 DoS 保护配置文件中定义的 CPS 阈值应用于符合策略规则的每个单独设备。例如，如果配置分类 DoS 保护配置文件以限制 CPS 速率为 4000，则组内设备最多可以接收 4000 CPS。DoS 保护策略可以有一个聚合配置文件和一个分类配置文件。



分类配置文件可以按源 *IP*、目标 *IP* 或两者对连接进行分类。对于面向 *Internet* 的区域，因为防火墙无法扩展以保存 *Internet* 路由表，因此只能按 目标 *IP* 进行分类。

仅对关键设备使用 DoS 保护，尤其是用户从 Internet 访问的常用攻击目标，例如 Web 服务器和数据库服务器。

- 对于现有会话，数据包缓冲区保护可通过使用阈值和计时器来减少滥用会话的方式保护防火墙（以及区域）免遭尝试攻陷防火墙数据包缓冲区的单会话 DoS 攻击。全局配置数据包缓冲区保护，并将其应用于每个区域。
- 安全策略规则会影响会话的传入和传出流。要建立会话，传入流量必须匹配现有的安全策略规则。如果不匹配，则防火墙丢弃该数据包。安全策略可以通过使用标准（包括区域、IP 地址、用户、应用程序、服务和 URL 类别）来允许或拒绝区域之间（区域间）和区域内（区域内）的流量。



为每个安全策略规则使用漏洞保护配置文件的最佳实践，这有助于防御 *DoS* 攻击。

默认安全策略规则不允许流量在区域之间传输，因此如果要允许区域间流量，则需要配置安全策略规则。默认情况下，允许所有区域内流量。您可以配置安全策略规则来匹配和控制区域内、区域间或通用（区域内和区域间）流量。



区域保护配置文件、*DoS* 保护配置文件和策略规则，以及安全策略规则仅影响防火墙上的数据平面流量。源自防火墙管理接口的流量不会跨越数据面板，因此防火墙不会将管理流量与这些配置文件或策略规则相匹配。

- 此外，还可以按哈希、CVE、签名 ID、域名、URL 或 IP 地址搜索 Palo Alto Networks 威胁库，以查找威胁。

## 区域防御工具如何运行？

当数据包到达防火墙时，防火墙将根据从数据包标头导出的入口区域、出口区域、源 IP 地址、目标 IP 地址、协议和应用程序，尝试将数据包与现有会话进行匹配。如果防火墙发现能够匹配，则该数据包使用已经控制会话的安全策略规则。如果防火墙不能匹配现有会话，则防火墙使用区域保护配置文件、DoS 保护配置文件和策略规则，以及安全策略规则来确定是建立会话还是丢弃数据包，以及数据包接收的访问级别。

流量通过面向 Internet 网络边缘的专用 DDoS 设备后，防火墙应用的第一个保护是区域保护配置文件的广泛防御（如果已连接到区域）。防火墙从数据包到达的接口（每个接口仅分配给一个区域，并且所有携带流量的接口必须属于某个区域）确定区域。如果区域保护配置文件拒绝此数据包，则防火墙丢弃数据包并保存资源，无需查看 DoS 保护策略或安全策略。防火墙仅将区域保护配置文件应用于新会话（与现有会话不匹配的数据包）。防火墙建立会话后，防火墙会绕过区域保护配置文件，进而在会话中查找后续数据包。

如果区域保护配置文件未丢弃数据包，则防火墙应用的第二个保护是 DoS 保护策略规则。区域保护配置文件根据总聚合流量允许数据包进入该区域，但如果该数据包将前往某个特定目标或来自已超出规则的 DoS 保护配置文件的泛滥攻击保护或资源保护设置的特定源，DoS 保护策略规则可能会拒绝该数据包。如果数据包


© 2019 Palo Alto Networks, Inc.

与一个 DoS 保护策略规则匹配，则防火墙将规则应用于该数据包。如果规则拒绝访问，则防火墙丢弃该数据包，并且不执行安全策略查找。如果规则允许访问，防火墙将执行安全策略查找。与区域保护配置文件一样，防火墙仅在新会话上执行 DoS 保护策略。

防火墙应用的第三个保护是安全策略查找，只会在区域保护配置文件和 DoS 保护策略规则允许数据包时发生。如果防火墙发现没有安全策略规则与该数据包相匹配，则防火墙将丢弃该数据包。如果防火墙发现匹配的安全策略规则，则防火墙将规则应用于该数据包。防火墙在会话的整个生命周期中执行双向流量（c2s 和 s2c）的安全策略规则。为每个安全策略规则使用漏洞保护配置文件的最佳实践，这有助于防御 DoS 攻击。

防火墙应用的第四个保护是数据包缓冲区保护，此时，您可以全局应用以保护设备，还可以单独应用于区域以阻止试图攻陷防火墙数据包缓冲区的单会话 DoS 攻击。对于全局保护，当流量超过保护阈值时，防火墙使用随即早期丢弃 (RED) 丢弃数据包（而不是会话）。对于每区域保护，如果违反数据包缓冲区阈值，防火墙阻止源 IP 地址。与区域和 DoS 保护不一样，数据包缓冲区保护应用于现有会话。

# 适用于 Dos 保护的防火墙布置

防火墙是一种基于会话的设备，其设计并不能扩展至数百万每秒连接数 (CPS) 以抵御大容量的 DoS 攻击。防火墙将唯一流（基于入口和出口区域、源和目标 IP、协议和应用程序）视为会话，在端口和 IP 级别的数据包检查上花费 CPU 周期以提供对应用程序流量的可见性，且必须对泛滥阈值计数器的每个会话进行计数，因此，防火墙布置对避免防火墙泛滥至关重要。

为了获得最佳 DoS 保护，尽可能将防火墙布置在您正在保护的资源附近。这样，可以减少防火墙需要处理的会话数，从而减少提供 DoS 保护所需的防火墙资源量。

在面向 Internet 的外围中，不得将用于 DoS 保护或区域保护的防火墙布置在专用 DDoS 设备以及外围路由器和交换机的前面。使这些大容量设备成为 DoS 防护的第一线，从而缓解容量耗尽型泛滥攻击。对于外围的区域和 DoS 保护，使用高容量防火墙，并将其布置在高容量设备之后。通常，防火墙越靠近外围，处理流量所需的容量就越大。

将网络划分为区域后，可有助于缓解内部 DoS 攻击。区域越小，流量可见性就越高，防止恶意软件横向移动的效果就越好，因为更多的流量必须跨过区域，此外，允许区域间流量需要您创建一个特定的安全策略规则（默认情况下，允许所有区域间流量）。如果网络相对而言未进行分段，则考虑重新审视您的分段方法。

# 用于设置泛滥阈值的 CPS 基线测量

泛滥保护阈值确定区域（区域保护配置文件）、区域内一组设备（聚合 DoS 保护策略）或区域内单个设备（分类 DoS 保护策略）何时限制新连接以开始缓解潜在泛滥攻击，以及何时丢弃所有新连接的新每秒连接数 (CPS)。因为每个网络都是唯一的，因此大多数网络都不适合使用默认的区域保护配置文件和 DoS 保护配置文件的泛滥保护阈值。您需要了解每个网络的聚合正常和峰值 CPS，以设置有效的区域保护配置文件阈值，以及您更想要保护的各个关键系统，以设置有效的 DoS 保护配置文件阈值；不要无意间将这些阈值设得太高，从而允许泛滥攻击；也不要设置得太低以限制流量。

- 待执行的 CPS 测量
- 如何测量 CPS

## 待执行的 *CPS* 测量

在至少五个工作日内测量 CPS 流量的平均值和峰值，或是测量 CPS 流量的平均值和峰值直到您确信测量能反应网络的典型流量模式；测量期越长，测量越准确。考虑可能会增加您需要支持的 CPS 数量的特殊事件、季度事件和年度事件。如果防火墙具有处理额外流量的能力，可能需要调整区域保护配置文件，并安排调整过的 DoS 保护策略规则适用于这些类型的事件。采取下列基线测量：

- 对于区域保护配置文件，测量每个区域传入的 CPS 平均值和峰值。
- 对于聚合 Dos 保护配置文件，测量想要保护的每个设备组的总体 CPS 平均值和峰值。
- 对于分类 Dos 保护配置文件，测量想要保护的单个设备组的 CPS 平均值和峰值。

还需了解防火墙的容量以及其他资源消耗功能（解密等）是如何影响每个防火墙可以控制的连接数。一般而言，防火墙越靠近外围，所需的容量就越大，因为需要处理更多的流量。每个型号的防火墙的数据包都包含



© 2019 Palo Alto Networks, Inc.

防火墙支持的每秒新会话数 (CPS)，您可以通过防火墙比较工具对各种型号的防火墙的 CPS（和其他指标）进行对比。

## 如何测量 *CPS*

可通过多种方式测量 CPS：

- 如果使用 Panorama 管理防火墙，则使用设备监控测量进入防火墙的 CPS（**Panorama** > **Managed Devices**（受管设备）> **Health**（健康）> **All Devices**（所有设备））。设备监控还可以展示 90 天的 CPU 平均值和峰值使用趋势线，帮助您了解每个防火墙的典型可用容量。
- 运行可操作的 CLI 命令 **`show session info`**。

  可操作的 *CLI* 命令 ***`show counter interface`*** 显示的是实际 *CPS* 值的两倍。如果使用此命令，应将 *CPS* 值除以 *2* 以得出实际 *CPS* 值。
- 要设置适当的 DoS 保护配置文件阈值，请与应用程序团队合作，了解其服务器的正常 CPS 和高峰 CPS，以及这些服务器可以支持的最大 CPS。

  此外，您还可以筛选防火墙流量日志和威胁日志，以获取想要保护的关键设备的目标 IP 地址，从而获得正常和高峰会话活动信息。
- 使用如 Wireshark 或 NetFlow 等第三方工具收集和分析网络流量。
- 使用脚本执行自动 CPS 信息收集和持续监控，并从日志中挖掘信息。
- 在防火墙上配置每个安全策略规则，以 **Log at Session End**（在会话结束时记录）。如果您没有 NetFlow 或 Wireshark 等监控工具，且无法获取或开发自动脚本，请 **Log at Session End**（在会话结束时记录）以捕获会话结束时的连接数。虽然这不会提供有关 CPS 的信息，但是，会向您展示选定持续时间内结束的会话数量，这样，您就可以根据此信息，大致计算出每秒会话数。

为了节省资源，防火墙以 *10* 秒为间隔测量聚合 *CPS*。为此，防火墙上进行的测量值可能无法在 *10* 秒间隔内捕获突发。尽管 *CPS* 平均值的测量不受影响，但 *CPS* 峰值测量可能不准确。例如，如果防火墙日志在 *10* 秒间隔内报告 *5000 CPS* 平均值，则可能有 *4000 CPS* 在 *1* 秒内涌入，而剩余的 *1000 CPS* 在剩余的 *9* 秒内分散。

若要收集一段时间内的历史 CPS 数据，在使用 SNMP 服务器的情况下，您可以使用自己的管理工具来轮询 SNMP MIB。但是，必须要知晓，MIB 中的 CPS 测量显示的是实际 CPS 值的两倍（例如，如果实际 CPS 值为 10,000，则 MIB 中显示的值为 20,000）。您仍可以通过 MIB 判断趋势，并且可以通过将 CPS 值除以 2 来获得实际值。SNMP MIB OID 包括：PanZoneActiveTcpCps、PanZoneActiveUdpCps 和 PanZoneOtherIpCps。因为防火墙只进行测量，并每隔 10 秒更新 SNMP 服务器一次，每隔 10 秒轮询一次。

此外，为泛滥事件创建单独的日志转发文件，这样，相应的管理员可获得仅包含泛滥（潜在 DoS 攻击）事件的电子邮件。为区域保护和 DoS 保护阈值事件设置日志转发。

实施区域和 *DoS* 保护后，使用这些方法监控部署，这样，您可以随网络的发展和流量模式的变化调整泛滥保护阈值。

# 区域保护配置文件

将区域保护配置文件应用到每个区域，以根据进入入口区域的聚合流量来进行保护。

除了配置区域保护和 *DoS* 保护，还应为每个安全策略规则使用漏洞保护配置文件的最佳实践，这有助于防御 *DoS* 攻击。

- Flood 保护
- 侦察保护
- 基于数据包的攻击保护


© 2019 Palo Alto Networks, Inc.

- 协议保护
- 以太网 SGT 保护

## *Flood* 保护

配置有泛滥攻击保护功能的区域保护配置文件可以保护整个入口区域免受 SYN、ICMP、ICMPv6、UDP 和其他 IP 泛滥攻击。防火墙以新的每秒连接数 (CPS) 为单位测量进入区域的每种泛滥攻击的总数，并将该总数与区域保护配置文件中配置的阈值进行比较。（您使用 DoS 保护配置文件和策略规则保护区域内关键独立设备。）



测量并监控防火墙数据面板 *CPU* 消耗，确保每个防火墙的大小适当，可支持 *DoS* 和区域保护以及消耗 *CPU* 周期的任何其他特征，例如，解密。如果使用 *Panorama* 管理您的防火墙，设备监控（*Panorama* > *Managed Devices*（受管设备）> *Health*（健康）> *All Devices*（所有设备））将向您展示每个受管防火墙的 *CPU* 和内存消耗。还可以展示 *90* 天的 *CPU* 平均值和峰值使用趋势线，帮助您了解每个防火墙的典型可用容量。

对于每种泛滥攻击类型，可以为进入该区的新 CPS 设置三个阈值，然后，为 SYN 泛滥攻击设置丢弃 **Action**（操作）。如果您知道该区的基线 CPS 速率，请使用这些指南设置初始阈值，然后进行监控，并在必要时调整阈值。

- 警报速率 — 用于触发警报的新 CPS 阈值。目标是设置 **Alarm Rate**（警报速率）为大于该区平均 CPS 速率的 15-20%，这样，正常波动就不会引发警报。
- 激活 — 用于激活泛滥保护机制并开始丢弃新连接的新 CPS 阈值。对于 ICMP、ICMPv6、UDP 和其他 IP 泛滥攻击，保护机制是随即早期丢弃 (RED)，也称为随机早期检测。仅对于 SYN 泛滥攻击而言，可以设置丢弃 **Action**（操作）为 SYN Cookies 或 RED。目标是设置 **Activate**（激活）速率为刚好大于该区峰值 CPS 速率，以开始缓解潜在泛滥攻击。
- **Maximum**（最大）— 当 RED 为保护机制时，丢弃传入数据包的每秒连接数。目标是设置 **Maximum**（最大）速率为防火墙容量的约 80-90%，同时考虑消耗防火墙资源的其他特征。

如果您不知道该区的基线 CPS 速率，则首先设置 **Maximum**（最大）CPS 速率为防火墙容量的约 80-90%，然后通过其获得合理的泛滥缓解警报和激活速率。根据最大速率设置 **Alarm Rate**（警报速率）和 **Activate**（激活）速率。例如，可以设置 **Alarm Rate**（警报速率）为 **Maximum**（最大）速率的一半，然后根据您接收到的警报数和消耗的防火墙资源进行调整。设置 **Activate Rate**（激活速率）时应谨慎，因为它会丢弃连接。因为正常流量负载的波动较大，因此最好不要大肆丢弃连接。如果防火墙资源受到影响，高的一侧将会报错，并调整速率。



*SYN* 泛滥保护是您设置丢弃 *Action*（操作）的唯一类型。首先，设置 *Action*（操作）为 *SYN Cookies*。*SYN Cookies* 公平处理合法流量，仅丢弃未通过 *SYN* 握手的流量，同时，使用随机早期丢弃随机丢弃流量，因此，*RED* 可能会影响合法流量。但是，*SYN Cookies* 占用的资源较多，因为防火墙充当目标服务器的代理，处理此服务器的三向握手。权衡不是丢弃合法流量 *(SYN Cookies)*，而是保留防火墙资源 *(RED)*。监控防火墙，并在 *SYN Cookies* 消耗过多资源时，切换到 *RED*。如果防火墙前方目前没有专门的 *DDoS* 防护设备，请始终使用 *RED* 作为丢弃机制。

默认值应比较高，以便激活区域保护配置文件时不会意外删除合法流量。调整阈值，以适合您的网络流量。了解如何设置合理泛滥阈值的最佳做法是对每种类型的泛滥攻击的平均值和峰值 CPS 实施基线测量，以确定每个区域的正常流量条件，了解防火墙容量，包括解密等其他消耗资源的功能的影响。根据需要和网络情况监控并调整泛滥阈值。



具有多个数据平面处理器 *(DP)* 的防火墙跨 *DP* 分配连接。防火墙通常会将跨 *DP* 平均分配 *CPS* 阈值设置。例如，如果防火墙拥有五个 *DP*，可以设置 *Alarm Rate*（警报速率）为 *20000 CPS*，每个 *DP* 均拥有一个 *4000 CPS (20000 / 5 = 4000)* 的 *Alarm Rate*（警报速率），因此，如果 *DP* 上的新会话超过 *4000*，则会触发此 *DP* 的 *Alarm Rate*（警报速率）阈值。



© 2019 Palo Alto Networks, Inc.

## 侦察保护

与侦察的军事定义类似，侦察的网络安全定义是指攻击者试图通过秘密探测网络找到弱点的方式来获取有关您的网络漏洞的信息。侦察活动往往是网络攻击的前奏。在所有区域上启用侦察保护，以防御端口扫描和主机扫掠：

- 端口扫描发现网络上的开放端口。端口扫描工具将客户端请求发送到主机上的一系列端口号中，目的是定位可在攻击中使用的活动端口。区域保护配置文件可防止 TCP 和 UDP 端口扫描。
- 主机扫掠检查多个主机以确定特定端口是否打开，是否有漏洞。

您可以将侦察工具用于合法目的，例如，用于渗透测试防火墙网络安全或强度。最多可指定 20 个 IP 地址或子网掩码地址对象，以从侦察保护中排除，这样，您的内部 IT 部门便可进行渗透测试来查找和修复网络漏洞。

您可以设置当配置侦察保护时侦察流量（不包括渗透测试流量）超过配置阈值时采取的操作。在阻止侦察操作之前，保留默认 **Interval**（间隔）和 **Threshold**（阈值）以记录几个数据包进行分析。

## 基于数据包的攻击保护

基于数据包的攻击有多种方式。区域保护配置文件检查 IP、TCP、ICMP、IPv6 和 ICMPv6 数据包标头，并通过以下方式保护区域：

- 丢弃具有不良特性的数据包。
- 在允许数据包传入区域之前，从中删除不需要的选项。

当您配置基于数据包的攻击保护时，选择用于每种数据包类型的丢弃特征。每种 IP 协议的最佳做法是：

- **IP Drop**（**IP** 丢弃）——丢弃**Unknown**（未知）和**Malformed**（异常）数据包。此外，还应丢弃 **Strict Source Routing**（严格源路由）和 **Loose Source Routing**（松散源路由），因为这些选项允许攻击者绕过使用目标 IP 地址充当匹配条件的安全策略规则。仅对于内部区域而言，检查 **Spoofed IP Address**（欺诈 **IP** 地址），这样，仅带有与防火墙路由表匹配的源地址的流量才能访问此区域。
- **TCP Drop**（**TCP** 丢弃）— 默认保留 **TCP SYN with Data**（带数据的 **TCP SYN**）和 **TCP SYNACK with Data**（带数据的 **TCP SYNACK**）丢弃，并丢弃 **Mismatched overlapping TCP segment**（不匹配的重叠 **TCP** 分段）和 **Split Handshake**（不匹配的重叠 **TCP** 分段）数据包，然后从数据包中删除 **TCP Timestamp**（**TCP** 时间戳）。

  启用 *Rematch Sessions*（重新匹配会话）（*Device*（设备）> *Setup*（设置）> *Session*（会话）> *Session Settings*（会话设置））是将已提交的新配置或编辑安全策略规则应用于现有会话的最佳做法。但是，如果您在区域内配置隧道内容检测并启用 *Rematch Sessions*（重新匹配会话），则还必须禁用 *Reject Non-SYN TCP*（拒绝非 *SYN TCP*）（选择从 *Global*（全局）更改为 *No*（否））；否则，防火墙将在您启用或编辑隧道内容检测时丢弃所有现有隧道会话。创建单独的区域保护配置文件，以便仅禁用具有隧道内容检测的区域上的 *Reject Non-SYN TCP*（拒绝非 *SYN TCP*），以及仅在启用 *Rematch Sessions*（重新匹配会话）时进行禁用。
- **ICMP Drop**（**ICMP** 丢弃）— 没有标准的最佳实践设置，因为丢弃 ICMP 数据包取决于您使用 ICMP 的方式（或是您是否使用 ICMP）。例如，如果想要阻止 ping 活动，则可以阻止 **ICMP Ping ID 0**。
- **IPv6 Drop**（**IPv6** 丢弃）— 如果合规性很重要，则防火墙必须丢弃具有不合规路由标头和扩展等的数据包。
- **ICMPv6 Drop**（**ICMPv6** 丢弃）— 如果合规性很重要，则防火墙必须丢弃不符合安全策略规则的某些数据包。

## 协议保护

在区域保护配置文件中，协议保护可防御基于非 IP 协议的攻击。启用协议保护以阻止或保护第二层 VLAN 或虚拟线路上安全区域之间，或是第二层 VLAN 上单个区域内接口之间的非 IP 协议（第三层接口和区域丢弃非 IP 协议，因此，非 IP 协议保护不适用）。配置协议保护通过阻止安全性更低的协议进入区域或进入某个区域的接口来降低安全风险，确保符合法律规定。


© 2019 Palo Alto Networks, Inc.

如果未配置用于阻止相同区域内非 *IP* 协议从一个第二层接口进入另一个接口的区域保护配置文件，因为默认区域间允许安全策略规则，因此，防火墙将允许流量通过。可以在区域内创建阻止 LLDP 等协议的区域保护配置文件，阻止发现可通过其他区域接口进行访问的网络。

如果需要发现正在您网络上运行的非 IP 协议，则使用 NetFlow、Wireshark 等监控工具或其他第三方工具发现您网络上的非 IP 协议。可以阻止或允许的非 IP 协议示例包括 LLDP、NetBEUI、跨越树以及监控和数据采集 (SCADA) 系统，如面向通用对象的变电站事件 (GOOSE) 等。

创建 **Exclude List**（排除列表）或 **Include List**（包含列表）以便为区域配置协议保护。**Exclude List**（排除列表）是一个阻止列表 — 防火墙可阻止您放置在 **Exclude List**（排除列表）内的所有协议，允许其他所有协议。**Include List**（包含列表）是一个允许列表 — 防火墙仅允许您在列表中指定的协议，并阻止所有其他协议。

为协议保护使用包含列表，而非排除列表。包含列表专门约束您想要允许和阻止您不需要，或是您不知道是否存在于您网络上的协议，从而减少攻击面，并阻止未知流量。

列表最多支持 64 个 Ethertype 条目，每个条目由其 IEEE 十六进制 Ethertype 代码标识。Ethertype 代码的其他来源为 standards.ieee.org/develop/regauth/ethertype/eth.txt 和 http://www.cavebear.com/archive/cavebear/Ethernet/type.html。在具有聚合以太网 (AE) 接口的区域上配置非 IP 协议的区域保护时，因为 AE 接口成员被视为一个组，因此只能在一个 AE 接口成员上阻止或允许非 IP 协议。

协议保护不允许阻止 *IPv4 (Ethertype 0x0800)*、*IPv6 (0x86DD)*、*ARP (0x0806)* 或 *VLAN* 标记帧 *(0x8100)*。即使您没有明确列出这四个 *Ethertypes*，也不允许将其添加到 *Exclude List*（排除列表），防火墙始终在 *Include List*（包含列表）中隐式允许这四个 *Ethertypes*。

## 以太网 *SGT* 保护

在 Cisco TrustSec 网络中，Cisco 身份服务引擎(ISE)将 16 位的第 2 层安全组标记(SGT)分配给用户或端点会话。一旦防火墙成为 Cisco TrustSec 网络的一部分，就可以采用以太网 SGT 保护创建区域保护配置文件。防火墙可以检测特定第 2 层安全组标记 (SGT) 值为 802.1Q (Ethertype 0x8909) 的标头，并且，如果 SGT 与您为附加到接口的区域保护配置文件配置的列表匹配，防火墙会丢弃数据包。确定要拒绝访问区域的 SGT 值。

# 数据包缓冲区保护

数据包缓冲区保护功能可保护您的防火墙和网络免受单会话 DoS 攻击，这些攻击可能会攻陷防火墙的数据包缓冲区并导致合法流量被丢弃。虽然您未在区域保护配置文件、DoS 保护配置文件或策略规则中配置数据包缓冲区保护，但数据包缓冲区保护可保护入口区域。区域和 DoS 保护应用于新会话（连接），且非常精确，而数据包缓冲区保护应用于现有会话，且是全局的。

您可以全局配置数据包缓冲区保护，以保护整个防火墙，还能在每个区域上启用数据包缓冲区保护以保护区域：

- 全局数据包缓冲区保护 — 防火墙监控所有区域的会话（无论区域内是否启用数据包缓冲区保护）以及这些会话如何利用数据包缓冲区。您必须全局配置数据包缓冲区保护（**Device**（设备）> **Setup**（设置）> **Session Settings**（会话设置））以保护防火墙，并在单个区域上启用。当数据包缓冲区消耗达到配置的 **Activate**（激活）百分比时，防火墙使用随即早期丢弃 (RED) 丢弃违规会话中的数据包（防火墙不会在全局上丢弃整个会话）。
- 每区域数据包缓冲区保护— 在每个区域上启用数据包缓冲区保护（**Network**（网络）> **Zones**（区域））以进行第二层保护。当数据包缓冲区消耗超过 **Activate**（激活）阈值时，全局保护开始应用 RED 到会话流量，这将启动 **Block Hold Time**（阻止保持时间）计时器。**Block Hold Time**（阻止保持时间）是违规会话在防火墙阻止整个会话之前继续存在的时间量（秒）。违规会话仍保持被阻止的状态，直至 **Block Duration**（阻止期限）时间到期。



© 2019 Palo Alto Networks, Inc.

您必须在全局启用数据包缓冲区保护，使其在区域内处于活动状态。

有两种类型的数据包缓冲区保护：

- 基于缓冲区利用率的数据包缓冲区保护
- 基于延迟的数据包缓冲区保护

基于缓冲区利用率的数据包缓冲区保护

默认启用基于缓冲区利用率的数据包缓冲区保护。在一段时间内（至少一个工作周，但测量时间越长，基线越好）对防火墙数据包缓冲区利用率进行基线测量，以了解典型用法。

若要查看特定时间段内的数据包缓冲区利用率（或查看至少使用 2% 数据包缓冲区的前 5 名会话），请使用可操作的 CLI 命令：

```
admin1138@thxvm1>show running resource-monitor [day | hour | ingress-backlogs
 | minute | second | week]
```

CLI 命令提供特定时间段内缓冲区利用率的屏幕截图，但此操作既不是自动的，也不具有连续性。若要自动执行连续的数据包缓冲区利用率测量以便您可以监控行为和异常事件的变化，请使用脚本。您可以通过修改 Palo Alto Networks 客户团队提供的示例脚本编写自己的脚本；但是，该脚本不受官方支持，也不会为脚本使用情况或修改提供技术支持。

如果基线测量始终显示异常高的数据包缓冲区利用率，则防火墙的容量可能对于典型流量负载而言过小。在这种情况下，请考虑重新调整防火墙部署的规模。否则，您需要仔细调整数据包缓冲区保护阈值，防止受影响的缓冲区遭受溢出影响（并阻止丢弃合法流量）。当防火墙规模刚好适合于部署时，只有攻击才会导致缓冲区利用率大幅增加。

过多使用防火墙数据包缓冲区将会对防火墙数据包转发能力造成负面影响。当缓冲区已满时，不仅是遭受攻击的接口，其他任何接口上的防火墙内均没有数据包可以进入。

设置阈值的最佳做法是：

- **Alert**（警报）和 **Activate**（激活）— 从默认阈值开始，监控数据包缓冲区利用率，并在必要时调整阈值。默认 **Alert**（警报）阈值为 50%；一旦数据包缓冲区利用率超过该阈值 10 秒以上，防火墙将每分钟在系统日志中创建一个警报条目。默认 **Activate**（激活）阈值为 80%；一旦达到该阈值，防火墙将开始缓解最滥用的会话。如果防火墙规模正确，则缓冲区利用率应远低于 50%。
- **Block Hold Time**（阻止保持时间）— 当数据包缓冲区利用率触发 **Activate**（激活）阈值时，**Block Hold Time**（阻止保持时间）设置违规会话在防火墙阻止会话前可以持续的时间量。在 **Block Hold Time**（阻止持续时间）期间，防火墙持续将 RED 应用于违规会话的数据包。从默认 **Block Hold Time**（阻止持续时间）阈值开始（60 秒），监控数据包缓冲区利用率，并在必要时调整阈值。如果在 **Block Hold Time**（阻止持续时间）过期之前，数据包缓冲区利用率百分比低于 **Activate**（激活）阈值，则计时器将重置，且不会开始，直至再次超过 **Activate**（激活）阈值。增加 **Block Hold Time**（阻止持续时间）将会对违规会话实施更大的惩罚，而减少阻止持续时间则会对违规会话减轻惩罚。
- **Block Duration**（阻止期限）— **Block Hold Time**（阻止持续时间）过期后，防火墙阻止 **Block Duration**（阻止期限）规定时间段内的违规会话。从默认阈值开始（3600 秒），监控数据包缓冲区利用率，并在必要时调整阈值。在区域上启用数据包缓冲区保护后，即使只有一个来自 IP 地址的会话过度使用数据包缓冲区，则 **Block Duration**（阻止期限）仍会对 IP 地址的每个会话产生影响。如果您认为阻止 IP 地址一个小时（3600 秒）的惩罚太大，则将 **Block Duration**（阻止期限）降至可接受的值。

除监控各个会话缓冲区使用率外，如果满足某些标准，则数据包缓冲区保护也可以阻止 IP 地址。当防火墙监控数据包缓冲区时，如果检测到源 IP 地址快速创建不会被视为攻击的会话，则在配置的 **Block Duration**（阻止期限）内阻止该 IP 地址。


© 2019 Palo Alto Networks, Inc.

网络地址转换 (NAT)（使用源 *NAT* 转换其互联网绑定流量的外部源）可以因 *IP* 地址转换活动而出现更大的数据包缓冲区利用率。如果发生这种情况，则请以惩罚单个会话，而非底层 *IP* 地址的方式调整阈值（这样，才不会影响来自相同 *IP* 地址的其他会话）。为此，请缩短 *Block Hold Time*（阻止持续时间），这样，防火墙可以阻止快速过度使用缓冲区的单个会话，并减少 *Block Duration*（阻止期限），这样，底层 *IP* 地址不会被过度惩罚。

基于延迟的数据包缓冲区保护

作为基于利用率的数据包缓冲区保护的替代方法，您可以触发基于延迟的数据包缓冲区保护，该延迟由数据平面数据包缓存（表明防火墙出现堵塞）引起。此种数据包缓冲区保护通过向您发出堵塞警报，并对数据包执行随机早期丢弃 (RED) 来缓解队头堵塞。基于延迟的数据包缓冲区保护可在延迟敏感型协议或应用程序受到影响之前触发保护。

如果流量包括延迟敏感型协议或应用程序，在这种情况下，基于延迟的数据包缓冲区保护就比基于缓冲区利用率的数据包缓冲区保护更有用。

基于延迟的数据包缓冲区保护包括设置 **Latency Alert**（延迟警报）阈值（以毫秒为单位），一旦超过该值，防火墙将开始生成警报日志事件。**Latency Activate**（延迟激活）阈值指示防火墙何时对传入数据包执行 RED，并开始生成“激活”日志。**Latency Max Tolerate**（最大延迟容忍）阈值指示防火墙何时使用接近 100% 丢弃率执行 RED。

基于延迟的数据包缓冲区保护的**Block Hold Time**（组织保持时间）和**Block Duration**（阻止持续时间）设置的功能与基于利用率的数据包缓冲区保护相同。

# DoS 保护配置文件和策略规则

DoS 保护配置文件与 DoS 保护策略规则相结合，保护关键资源组和单个关键资源免遭会话泛滥攻击。相较于用于保护整个区域免遭泛滥攻击的区域保护配置文件而言，DoS 保护为特定系统提供精细防御，尤其是用户从互联网访问，且经常成为攻击目标的关键系统，例如 Web 服务器和数据库服务器。使用两种类型的保护，因为如果仅使用区域保护配置文件，在每秒连接 (CPS) 总数不超过该区域的 **Activate**（激活）和 **Maximum**（最大）速率的情况下，专门针对区域内特定系统的 DoS 攻击就会成功。

DoS 保护占用的资源较多，因此仅用于关键系统。与区域保护配置文件类似，DoS 保护配置文件指定泛滥阈值。DoS 保护策略规则确定使用 DoS 配置文件的设备、用户、区域和服务。

除了配置 *DoS* 保护和区域保护，还应为每个安全策略规则使用漏洞保护配置文件的最佳实践，这有助于防御 *DoS* 攻击。

- 分类与聚合 DoS 保护
- DoS 保护配置文件
- DoS 保护策略规则

## 分类与聚合 *DoS* 保护

您可以配置聚合和分类 DoS 保护配置文件，并在配置 DoS 保护时将一个配置文件或每种类型的配置文件中一个用于DoS 保护策略规则。

- **Aggregate**（聚合）— 设置适用于 DoS 保护策略规则内指定的整个设备组（而非每个独立设备）的阈值，这样，一个设备就可以接收大部分允许的连接流量。例如，**Max Rate**（最大速率）为 20000 CPS 意味着该组的总 CPS 为 20000。如果其他设备无连接，则独立设备最多可接收 20000 CPS。当您对特定子网、用户或服务实施额外约束时，聚合 DoS 保护策略可为特定的关键设备组提供另一层的广泛保护（在互联网外围的专用 DDoS 设备以及区域保护配置文件之后）。
- **Classified**（分类）—设置适用于 DoS 保护策略规则内指定的每个独立设备的泛滥阈值。例如，如果设置 **Max Rate**（最大速率）为 5000 CPS，规则内指定的每个设备在丢弃新连接之前最多可接收 5000 CPS。如果将分类 DoS 保护策略规则应用于多个设备，受此规则管理的设备在容量以及想要如何控制其 CPS 速率方面应该类似，因为分类阈值适用于每个独立设备。分类配置文件保护个人关键资源。



© 2019 Palo Alto Networks, Inc.

使用分类 Dos 保护配置文件配置 Dos 保护策略规则时（**Option/Protection**（选项/保护）> **Classified**（分类）> **Address**（地址）），应根据与 **source-ip-only**（仅源 **IP**）、**destination-ip-only**（仅目标 **IP**）或 **scr-dest-ip-both**（源 **IP** 和目标 **IP**）的匹配情况使用 **Address**（地址）字段指定传入连接是否对配置文件阈值计数（防火墙根据阈值对源 IP 地址和目标 IP 地址匹配情况进行计数）。计数器会消耗资源，因此，计算地址匹配的方式会影响防火墙的资源消耗。可以使用分类 DoS 保护：

- 保护关键独立设备，尤其是用户通过互联网访问且常常遭遇攻击的服务器，例如 Web 服务器、数据库服务器和 DNS 服务器。在分类 DoS 保护配置文件中设置适当的泛滥和资源保护阈值。创建将配置文件应用于每个服务器 IP 地址的 DoS 保护策略规则，方法是将 IP 地址添加为规则的目标条件；设置 **Address**（地址）为 **destination-ip-only**（仅目标 **IP**）。

  请勿在分类 *DoS* 保护策略规则中对面向 *internet* 的区域使用 *source-IP-only*（仅源 *IP*）或 *src-dest-ip-both*（源 *IP* 和目标 *IP*），因为防火墙无法将每个可能 *IP* 地址计数器存储在互联网上。仅为内部区域或相同区域规则增加源 *IP* 阈值计数器。在外围区域使用 *destination-ip-only*（仅目标 *IP*）。
- 监控可疑主机或主机组的 CPS 速率（包含主机的区域不能面向互联网）。在分类 DoS 保护配置文件内设置适当的警报阈值，以通知您主机是否发起了大量异常连接。创建将配置文件应用于单个源或源地址组的 DoS 保护策略规则，设置 **Address**（地址）为 **source-ip-only**（仅源 **IP**）。调查能发起足够新连接的主机以启动警报。

如果配置分类配置文件的 **Address**（地址）（**source-ip-only**（仅源 **IP**）、**destination-ip-only**（仅目标 **IP**）或 **src-dest-ip-both**（源 **IP** 和目标 **IP**））取决于您的 DoS 保护目标、保护内容、以及保护设备是否位于面向互联网的区域。

防火墙使用更多资源来跟踪作为 *Address*（地址）的 *src-dest-ip-both*（源 *IP* 和目标 *IP*），而非跟踪 *source-IP-only*（仅源 *IP*）或 *destination-ip-only*（仅目标 *IP*），因为计数器会消耗源 *IP* 和目标 *IP* 地址的资源，而非仅仅是其中之一。

如果聚合和分类 DoS 保护配置文件均使用相同的 DoS 保护策略规则，则防火墙将首先应用聚合配置文件，然后根据需要应用分类配置文件。例如，通过 DoS 保护策略规则中的两种配置文件类型保护一组共五个 Web 服务器。当组内 **Max Rate**（最大速率）合计达到 25000 CPS 时，聚合配置文件配置将丢弃新连接。当组内 **Max Rate**（最大速率）合计达到 6000 CPS 时，分类配置文件配置将把新连接丢弃至组内任何单个 Web 服务器。有三种流量超过 **Max Rate**（最大速率）阈值的情况：

- 新的 CPS 速率超过聚合 **Max Rate**（最大速率），但未超过分类 **Max Rate**（最大速率）。在这种情况下，防火墙应用聚合配置文件，并阻止在已配置的阻止期限内的所有新连接。
- CPS 速率未超过聚合 **Max Rate**（最大速率），但其中一个 Web 服务器的 CPS 超过分配 **Max Rate**（最大速率）。在这种情况下，防火墙检查聚合配置文件，并发现该组的速率低于 25000 CPS，因此防火墙不会基于此对新连接发起阻止。接下来，防火墙检查分类聚合文件，并发现某个特定服务器的速率超过 6000 CPS。防火墙应用分类配置文件，并阻止在已配置的阻止期限内此特定服务器的新连接。因为组内其他服务器在分类配置文件的**Max Rate**（最大速率）内，因此其流量不受影响。
- 新的 CPS 速率超过聚合 **Max Rate**（最大速率），也超过其中一个 Web 服务器的分类 **Max Rate**（最大速率）。在这种情况下，防火墙检查聚合配置文件，并发现该组的速率超过 25000 CPS，因此防火墙将阻止新连接，以限制该组的总 CPS。随后，防火墙检查分类配置文件，并发现某个特定服务器的速率超过 6000 CPS（因此，聚合配置文件将强制实施该组的组合限制，但这也不足以保护此特定服务器）。防火墙应用分类配置文件，并阻止在已配置的阻止期限内此特定服务器的新连接。因为组内其他服务器在分类配置文件的**Max Rate**（最大速率）内，因此其流量不受影响。

如果想要聚合和分类 *DoS* 保护配置文件均应用于相同的流量，则两个配置文件必须使用相同的 *DoS* 保护策略规则。如果聚合配置文件使用一个规则，分类配置文件使用另一个规则，即使指定的流量完全相同，防火墙也只能使用其中一个配置文件，因为当流量与第一个 *DoS* 保护策略规则匹配时，防火墙将执行此规则内指定的 *Action*（操作），不会将流量与任何后续规则进行对比，因此，流量不会匹配第二个规则，而且防火墙也无法应用此操作。（这与安全策略规则的工作原理相同）。


© 2019 Palo Alto Networks, Inc.

## DoS 保护配置文件

DoS 保护配置文件设置阈值，以保护新会话 IP 泛滥攻击，并提供资源保护（指定端点和资源的最大并行会话数限制）。DoS 保护配置文件保护特定设备（分类配置文件）和设备组（聚合配置文件）免遭 SYN、UDP、ICMP、ICMPv6 和其他 IP 泛滥攻击。在 DoS 保护配置文件中配置泛滥保护阈值的方式与在区域保护配置文件中配置Flood 保护类似，但是，区域保护配置文件保护整个入口区域，而 DoS 保护配置文件和策略规则更精细，更有针对性，甚至可以归类到单个设备（IP 地址）。防火墙测量设备组的聚合每秒连接数 (CPS)（聚合配置文件）或测量单个设备的 CPS（分类配置文件）。



测量并监控防火墙数据面板 *CPU* 消耗，确保每个防火墙的大小适当，可支持 *DoS* 和区域保护以及消耗 *CPU* 周期的任何其他特征，例如，解密。如果使用 *Panorama* 管理您的防火墙，设备监控（*Panorama* > *Managed Devices*（受管设备）> *Health*（健康）> *All Devices*（所有设备））将向您展示每个受管防火墙的 *CPU* 和内存消耗。还可以展示 *90* 天的 *CPU* 平均值和峰值使用趋势线，帮助您了解每个防火墙的典型可用容量。

对于每种泛滥类型，可以为设备组（聚合）或独立设备（分类）的新 CPU 设置三个阈值和一个 **Block Duration**（阻止期限），此外，还可以设置 SYN 泛滥的丢弃 **Action**（操作）：

- **Alarm Rate**（警报速率）— 当新 CPU 超过此阈值时，防火墙会生成 DoS 警报。对于分类配置文件，速率设置应高于设备平均 CPS 速率的 15-20%，这样，正常波动才不会引发警报。对于聚合配置文件，速率设置应高于组平均 CPU 速率的 15-20%。
- **Activate Rate**（激活速率）— 当新 CPU 超过此阈值，防火墙开始丢弃新连接，以缓解泛滥攻击，直至 CPS 速率降至阈值以下。对于分类配置文件，**Max Rate**（最大速率）应是正在保护的设备的可接受 CPS 速率（**Max Rate**（最大速率）不会使关键设备遭受泛滥攻击）。可以将 **Activate Rate**（激活速率）的阈值设置成与 **Max Rate**（最大速率）一样，这样，防火墙不会在速率达到 **Max Rate**（最大速率）时开始丢弃流量。只有当您想在速率达到 **Max Rate**（最大速率）之前丢弃流量时才能将 **Activate Rate**（激活速率）设置成低于 **Max Rate**（最大速率）的值。对于聚合配置文件，为组设置的阈值应刚好大于平均峰值 CPS 速率，以开始使用 RED 缓解泛滥攻击（或 SYN Cookies 缓解 SYN 泛滥攻击）。
- **Max Rate**（最大速率）— 当新 CPS 超过此阈值时，在指定的 **Block Duration**（阻止期限）时间段内，防火墙阻止（丢弃）来自攻击性 IP 地址的所有新连接。对于分类配置文件，根据您正在保护的设备容量设置 **Max Rate**（最大速率）阈值，这样，CPS 速率不会对其泛滥攻击。对于综合配置文件，设置为组容量的 80-90%。
- **Block Duration**（阻止期限）— 当新 CPS 超过 **Max Rate**（最大速率）时，防火墙阻止来自攻击性 IP 地址的新连接。**Block Duration**（阻止期限）指定防火墙持续阻止 IP 地址新连接的时长。虽然防火墙阻止新连接，但不会对传入连接计数，也不会增加阈值计数器。对于分类和聚合配置文件，均会使用默认值（300 秒）来阻止攻击会话，在很长一段时间内不会对来自源的合法会话进行处罚。



*SYN* 泛滥保护是您设置丢弃 *Action*（操作）的唯一类型。首先，设置 *Action*（操作）为 *SYN Cookies*。*SYN Cookies* 公平处理合法流量，仅丢弃未通过 *SYN* 握手的流量，同时，使用随机早期丢弃随机丢弃流量，因此，*RED* 可能会影响合法流量。但是，*SYN Cookies* 占用的资源较多，因为防火墙充当目标服务器的代理，处理此服务器的三向握手。权衡不是丢弃合法流量 *(SYN Cookies)*，而是保留防火墙资源 *(RED)*。监控防火墙，并在 *SYN Cookies* 消耗过多资源时，切换到 *RED*。如果防火墙前方目前没有专门的 *DDoS* 防护设备，请始终使用 *RED* 作为丢弃机制。

默认阈值应比较高，以便 DoS 保护配置文件不会以外丢弃合法流量。监控连接流量，调整阈值，以适合您的网络。首先，对每种泛滥类型的平均峰值 CPS 进行基准测量，以确定想要保护的关键设备的正常流量条件。因为正常流量负载的波动较大，因此最好不要大肆丢弃连接。根据需要和网络情况监控并调整泛滥阈值。

另一种设置泛滥阈值的方法是使用基线测量设置想要允许的最大 CPS，并从此处返回以获得合理的泛滥缓解警报和激活速率。



具有多个数据平面处理器 *(DP)* 的防火墙跨 *DP* 分配连接。防火墙通常会将跨 *DP* 平均分配 *CPS* 阈值设置。例如，如果防火墙拥有五个 *DP*，可以设置 *Alarm Rate*（警报速率）为 *20000 CPS*，每个 *DP* 均拥有一个 *4000 CPS (20000 / 5 = 4000)* 的 *Alarm Rate*（警报速



© 2019 Palo Alto Networks, Inc.

率），因此，如果 *DP* 上的新会话超过 *4000*，则会触发此 *DP* 的 *Alarm Rate*（警报速率）阈值。

除了设置 IP 泛滥阈值外，还可以使用 DoS 保护配置文件来检测并防止会话耗尽攻击，其中，大量主机 (bot) 会建立尽可能多地会话，以使用目标资源。在配置文件的 **Resources Protection**（资源保护）选项卡上，可以将 DoS 保护策略规则中定义设备的最大并行会话数设置为配置文件可以接受的会话数。当并行会话数达到其最大限制时，新会话将被丢弃。

设置的最大并行会话数取决于您的网络环境。了解是否可以处理您正在保护的资源的最大并行会话数（在可以附加配置文件的 DoS 保护策略规则中定义）。设置阈值为资源容量的约 80%，然后根据需要监控并调整阈值。

对于聚合配置文件，将 **Resources Protection**（资源保护）阈值应用于策略规则中定义的设备上的所有流量（源和目标）。对于分类配置文件，根据以下标准将 **Resources Protection**（资源保护）阈值应用于流量：分类策略规则仅应用于源 IP，仅应用于目标 IP，或源和目标 IP 两者。

## *DoS* 保护策略规则

DoS 保护策略规则控制哪些防火墙可将 DoS 保护应用于系统（附加到 DoS 保护策略规则中的 DoS 保护配置文件内配置的泛滥阈值）、流量匹配规则中定义的条件时应采取哪些操作、以及如何记录 DoS 流量。因为 DoS 保护会消耗防火墙资源，因此，仅将其用于防护特定的关键资源，防止会话泛滥，尤其是用户从互联网访问的常见目标，例如 Web 服务器和数据库服务器。使用区域保护配置文件保护整个区域免遭泛滥和其他攻击。DoS 保护策略规则提供精细的匹配标准，以便您可以灵活地定义要保护的内容：

- 源区域、接口、IP 地址（包括整个区域）和用户。
- 目标区域、接口、和 IP 地址（包括整个区域）。
- 服务（按端口和协议）。DoS 保护仅适用于您指定的服务。但是，指定服务并不会允许服务，并隐式阻止所有其他服务。指定服务将 DoS 保护专用于这些服务，但不会阻止其他服务。



除了保护关键服务器上正在使用的服务端口，还可以保护关键服务器未使用服务端口上的 *DoS* 攻击。对于关键系统，您可以通过创建一个 *DoS* 保护策略规则和配置文件来保护有服务正在运行的端口，并创建另一个不同的 *DoS* 保护策略规则和配置文件来保护没有服务运行的端口。例如，您可以通过一个策略/配置文件来保护 *Web* 服务器的正常服务端口（*80* 和 *443* 等），并使用另一个策略/配置文件来保护所有其他服务端口。请注意防火墙的容量，以免在为 *DoS* 计数器服务时会影响性能。

当流量符合 DoS 保护策略规则时，防火墙采取以下三种操作之一：

- 拒绝 — 防火墙拒绝访问，不应用 DoS 保护配置文件。与规则匹配的流量被阻止。
- 允许 — 防火墙允许访问，不应用 DoS 保护配置文件。与规则匹配的流量被允许。
- 保护 — 防火墙通过将指定的 DoS 保护配置文件或配置文件阈值应用于与规则匹配的流量，保护 DoS 保护策略规则中定义的设备。一个规则可以拥有一个聚合 DoS 保护配置文件和一个分类 DoS 保护配置文件。就分类配置文件而言，您可以使用源 IP、目标 IP 或两者来增加泛滥阈值计数器，如分类与聚合 DoS 保护所述。如果符合规则，传入数据包将对两个 DoS 保护配置文件进行计数。

如果 **Action**（操作）选择为 **Protect**（保护），则防火墙仅应用 DoS 保护配置文件。如果 DoS 保护策略规则的 **Action**（操作）选择为 **Protect**（保护），请在规则中指定适当的聚合和/或分类的 DoS 保护配置文件，以便防火墙将 DoS 保护配置文件阈值应用于符合规则的流量。大多数规则都是 **Protect**（保护）规则。

您可以通过 **Allow**（允许）和 **Deny**（拒绝）操作在较大的组内实施例外，但不对流量进行 DoS 保护。例如，您可以拒绝组内大多数的流量，但允许此流量的子集。相反，您可以允许组内大多数的流量，但拒绝此流量的子集。

当 DoS 保护策略激活时，您可以实施 **Schedule**（计划）（开始和结束时间，重复周期）。在一天或周内不同的时间应用不通过的泛滥阈值就是其中一个计划用例。例如，如果您的业务在夜间需要的流量明显低于白天，则您可能希望在白天应用更高的泛滥阈值，而非夜间。另一个用例是为特殊事件计划特殊阈值，但前提是防火墙支持 CPS 速率。



© 2019 Palo Alto Networks, Inc.

为了便于管理和精细报告，配置 **Log Forwarding**（日志转发），将 DoS 保护日志与其他威胁日志区分开来。除了将日志转发给 SNMP 或 syslog 服务器等服务器之外，还可以将 DoS 阈值违规事件通过电子邮件直接转发给管理员。如果防火墙的大小合适，则阈值违规就不会频繁出现，也可称为攻击尝试的强有力指标。



© 2019 Palo Alto Networks, Inc.

# 配置区域保护以提高网络安全性

以下主题提供区域保护配置示例：

- 配置侦察保护
- 配置基于数据包的攻击保护
- 配置协议保护
- 配置数据包缓冲区保护
- 配置基于延迟的数据包缓冲区保护
- 配置以太网 SGT 保护

## 配置侦察保护

为防火墙配置以下侦察保护操作之一以响应相应的侦察尝试：

- **Allow**（允许）— 防火墙允许端口扫描或主机扫掠侦察以继续。
- **Alert**（警报）— 防火墙对于在指定时间间隔内达到配置阈值的每次端口扫描或主机扫掠生成警报。警报是默认动作。
- **Block**（阻止）— 防火墙丢弃在指定时间间隔的剩余时间内从源到目标的所有后续数据包。
- **Block IP**（阻止 **IP**）— 防火墙在指定的 **Duration**（持续时间）（以秒计，范围为 1-3,600 秒）内丢弃所有后续数据包。**Track By**（跟踪标准）确定防火墙是否阻止源或源到目标的通信。

STEP 1 | 配置侦察保护。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）。
2. 选择区域保护配置文件或 **Add**（添加）新配置文件并输入 **Name**（名称）。
3. 在“侦察保护”选项卡上，选择要保护的扫描类型。
4. 为每次扫描选择一个 **Action**（操作）。如果选择“阻止 IP”，您还必须配置 **Track By**（跟踪标准）（源或源到目标）和 **Duration**（持续时间）。
5. 以秒为单位设置 **Interval**（间隔）。此选项对端口扫描和主机扫掠检测的时间间隔进行定义。
6. 设置 **Threshold**（阈值）。阈值定义了在触发操作的上述配置间隔内发生的端口扫描事件或主机扫掠数。

STEP 2 | （可选）配置源地址排除。

1. 在“侦察保护”选项卡上，**Add**（添加）源地址排除。
   1. 输入要排除地址的描述性 **Name**（名称）。
   2. 将地址类型设置为 **IPv4** 或 **IPv6**，然后选择地址对象或输入 IP 地址。
   3. 单击 **OK**（确定）。
2. 单击 **OK**（确定）以保存区域保护配置文件。
3. **Commit**（提交）更改。

## 配置基于数据包的攻击保护

为增强区域的安全性，基于数据包的攻击保护允许您指定防火墙是否丢弃具有某些特性的 IP、IPv6、TCP、ICMP 或 ICMPv6 数据包或从数据包中删除某些选项。

例如，您可以在 TCP 三向握手期间删除负载中包含数据的 TCP SYN 和 SYN-ACK 数据包。默认情况下，区域保护配置文件设置为丢弃包含数据的 SYN 和 SYN-ACK 数据包（必须将配置文件应用于该区域）。

TCP 快速打开选项 (RFC 7413) 通过在 SYN 和 SYN-ACK 数据包负载中包含数据来保持连接设置的速度。区域保护配置文件将使用 TCP 快速打开选项的握手与其他 SYN 和 SYN-ACK 数据包分开处理；如果已包含有效的快速打开 cookie，则配置文件默认设置为允许握手数据包。



© 2019 Palo Alto Networks, Inc.

如果在升级到 *PAN-OS 8.0* 时已经存在完整的区域保护配置文件，则三个默认设置将应用于每个配置文件，并且防火墙将相应地执行操作。

从 PAN-OS 8.1.2 及更高版本开始，您可以使用 CLI 命令（此任务的第四步）使防火墙在接收并丢弃下列类型的数据包后生成威胁日志，这样，您可以更容易地对这些事件进行分析，同时又能满足审计和合规性要求：

- 泪滴攻击
- 采用死亡之 Ping 进行 DoS 攻击

此外，如果您启用相应的基于数据包的攻击保护，则还可将相同的 CLI 命令使防火墙为下列类型的数据包生成威胁日志：

- 分段的 IP 数据包
- IP 地址欺诈
- 大于 1024 字节的 ICMP 数据包
- 包含 ICMP 片段的数据包
- 嵌入了错误消息的 ICMP 数据包
- TCP 会话中第一个非 SYN 数据包的数据包

STEP 1 | 创建区域保护配置文件，并配置基于数据包的攻击保护设置。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），并 **Add**（添加）新的配置文件。
2. 输入配置文件的 **Name**（名称）和 **Description**（说明）（可选）。
3. 选择 **Packet Based Attack Protection**（基于数据包的攻击保护）。
4. 在每个选项卡（**IP Drop**、**TCP Drop**、**ICMP Drop**、**IPv6 Drop** 和 **ICMPv6 Drop**）上，选择要执行保护区域的基于数据包的攻击保护设置。
5. 单击 **OK**（确定）。

STEP 2 | 将区域保护配置文件应用于已分配给要保护的接口的安全区域。

1. 选择 **Network**（网络）> **Zones**（区域），然后选择要将区域保护配置文件分配到的区域。
2. **Add**（添加）属于区域的 **Interfaces**（接口）。
3. 对于 **Zone Protection Profile**（区域保护配置文件），请选择刚创建的配置文件。
4. 单击 **OK**（确定）。

STEP 3 | **Commit**（提交）更改。

STEP 4 | （PAN-OS 8.1.2 及更高版本）如果您启用相应的基于数据包的攻击保护（在第一步），则启用防火墙为泪滴攻击和使用死亡之 Ping 进行 DoS 攻击生成威胁日志，还可为上面列出的数据包类型生成威胁日志。例如，如果您为 **Spoofed IP address**（欺诈 **IP** 地址）启用基于数据包的攻击保护，则在防火墙接收并丢弃带有欺诈 IP 地址的数据包时，使用下列 CLI 将导致防火墙生成威胁日志。

1. 访问 CLI。
2. 使用 CLI 操作命令 **`set systemsetting additional-threat-log on`**。默认为 **`off`**。

# 配置协议保护

通过使用协议保护从非 IP 协议数据包保护虚拟线路或第 2 层安全区域。

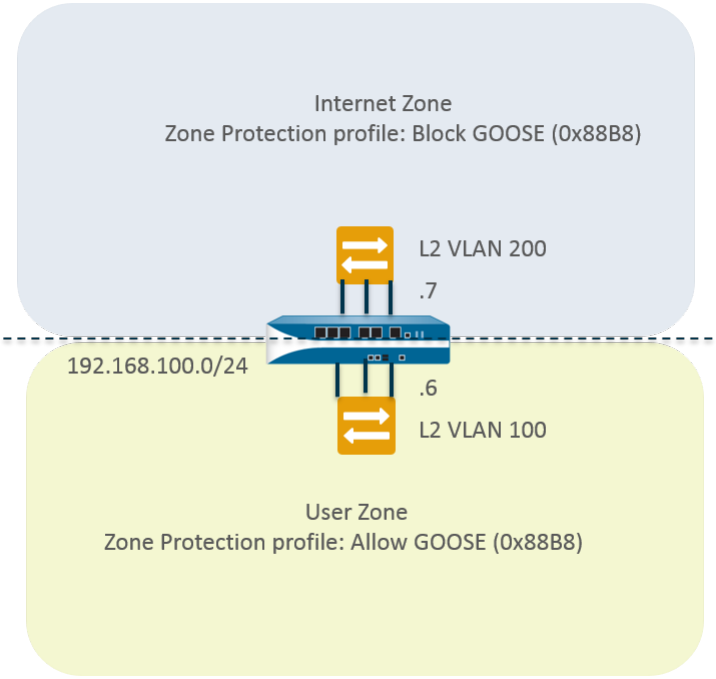
- 用例：第 2 层接口上安全区域之间的非 IP 协议保护
- 用例：第 2 层接口上安全区域内的非 IP 协议保护



© 2019 Palo Alto Networks, Inc.

## 用例：第 2 层接口上安全区域之间的非 IP 协议保护

在该用例中，防火墙在第 2 层 VLAN 中被分成两个子接口。VLAN 100 是 192.168.100.1/24，子接口为 .6。VLAN 200 是 192.168.100.1/24，子接口为 .7。非 IP 协议保护适用于入口区域。在该用例中，如果 Internet 区域是入口区域，则防火墙将阻止面向通用对象的变电站事件 (GOOSE) 协议。如果用户区域是入口区域，则防火墙允许 GOOSE 协议。防火墙隐式允许在两个区域中使用 IPv4、IPv6、ARP 和 VLAN 标记的帧。




STEP 1 | 配置两个 VLAN 子接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **VLAN** 并 **Add**（添加）一个接口。
2. **Interface Name**（接口名称）默认为 vlan。在此之后，请输入 7。
3. 在 **Config**（配置）选项卡上，**Assign Interface To**（将接口分配到）**VLAN** 200。
4. 单击 **OK**（确定）。
5. 选择 **Network**（网络）> **Interfaces**（接口）> **VLAN** 并 **Add**（添加）一个接口。
6. **Interface Name**（接口名称）默认为 vlan。在此之后，请输入 6。
7. 在 **Config**（配置）选项卡上，**Assign Interface To**（将接口分配到）**VLAN** 100。
8. 单击 **OK**（确定）。

STEP 2 | 在区域保护配置文件中配置协议保护以阻止 GOOSE 协议数据包。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称）阻止 GOOSE。
3. 选择 **Protocol Protection**（协议保护）。
4. 选择 **Exclude List**（排除列表）的 **Rule Type**（规则类型）。
5. 输入 **Protocol Name**（协议名称）GOOSE 以轻松识别列表上的 Ethertype。防火墙不会验证您输入的名称是否与 Ethertype 代码匹配；而仅使用 Ethertype 代码进行筛选。
6. 输入 **Ethertype** 代码 0x88B8。Ethertype 必须以 0x 开头，表示十六进制值。范围从 0x0000 到 0xFFFF。
7. 选中 **Enable**（启用）以执行协议保护。您可以禁用列表中的协议，例如测试。
8. 单击 **OK**（确定）。


© 2019 Palo Alto Networks, Inc.

STEP 3 | 将区域保护配置文件应用于 Internet 区域。

1. 选择 **Network**（网络）> **Zones**（区域）并 **Add**（添加）区域。
2. 输入区域的 **Name**（名称），例如 Internet。
3. 对于 **Location**（位置），请选择区域应用的虚拟系统。
4. 对于 **Type**（类型），请选择 **Layer2**（第 2 层）。
5. **Add**（添加）属于该区域 vlan.7 的 **Interface**（接口）。
6. 对于 **Zone Protection Profile**（区域保护配置文件），请选择配置文件“阻止 GOOSE”。
7. 单击 **OK**（确定）。

STEP 4 | 配置协议保护以允许 GOOSE 协议数据包。

创建另一个名为“允许 GOOSE”的区域保护配置文件，然后选择 **Include List**（包括列表）的 **Rule Type**（规则类型）。

配置包括列表时，应包括所有必需的非 *IP* 协议；列表内容不完整会阻止合法的非 *IP* 流量。

STEP 5 | 将区域保护配置文件应用于用户区域。

1. 选择 **Network**（网络）> **Zones**（区域）并 **Add**（添加）区域。
2. 输入区域的 **Name**（名称），“用户”。
3. 对于 **Location**（位置），请选择区域应用的虚拟系统。
4. 对于 **Type**（类型），请选择 **Layer2**（第 2 层）。
5. **Add**（添加）属于该区域 vlan.6 的 **Interface**（接口）。
6. 对于 **Zone Protection Profile**（区域保护配置文件），请选择配置文件“允许 GOOSE”。
7. 单击 **OK**（确定）。

STEP 6 | 提交。

单击 **Commit**（提交）。

STEP 7 | 根据协议保护查看防火墙已丢弃的非 IP 数据包数。

访问 CLI。

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```

## 用例：第 2 层接口上安全区域内的非 *IP* 协议保护

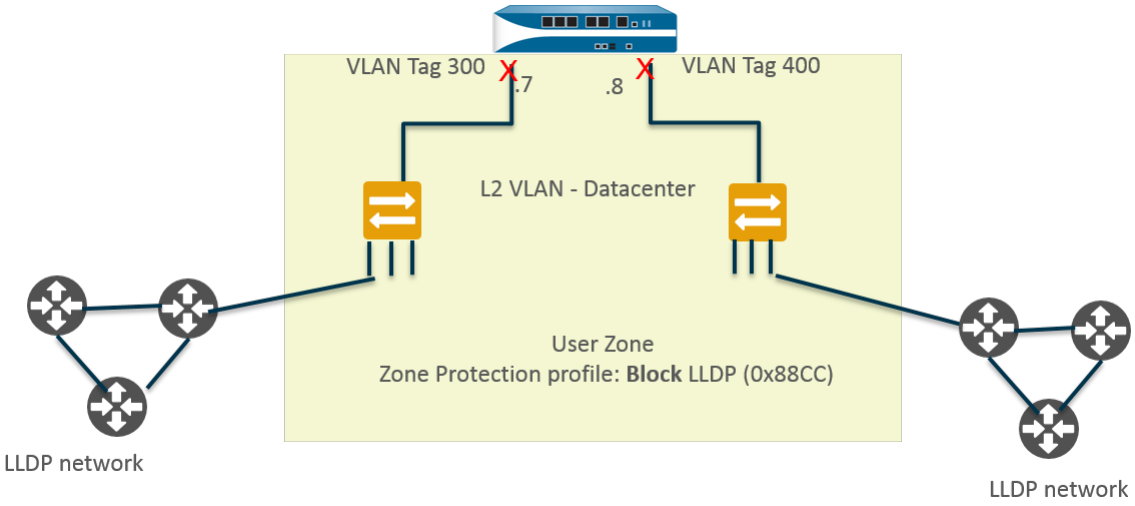
如果没有实施具有非 IP 协议保护的区域保护配置文件，则防火墙允许单个区域中的非 IP 协议从一个第 2 层接口转到另一个。在该用例中，阻止 LLDP 数据包可确保网络的 LLDP 不会发现可通过该区域中另一个接口进行访问的网络。

在下图中，名为 Datacenter 的第 2 层 VLAN 划分为两个子接口：192.168.1.1/24（子接口 .7）和 192.168.1.2/24（子接口 .8）。该 VLAN 属于用户区域。通过区域保护配置文件，可将 LLDP 阻止到用户区域：

- 子接口 .7 阻止从交换机到左边红色 X 处防火墙的 LLDP，防止流量到达子接口 .8。
- 子接口 .8 阻止从交换机到右边红色 X 处防火墙的 LLDP，防止流量到达子接口 .7。



© 2019 Palo Alto Networks, Inc.




STEP 1 | 为以太网接口创建一个子接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择第 2 层接口，在本例中为 ethernet1/1。
2. 选择 **Add Subinterfaces**（添加子接口）。
3. **Interface Name**（接口名称）默认为接口 (ethernet 1/1)。在此之后，请输入 7。
4. 对于 **Tag**（标记），请输入 300。
5. 对于 **Security Zone**（安全区域），请选择用户。
6. 单击 **OK**（确定）。

STEP 2 | 为以太网接口创建第二个子接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后选择第 2 层接口：ethernet1/1。
2. 选择 **Add Subinterfaces**（添加子接口）。
3. **Interface Name**（接口名称）默认为接口 (ethernet 1/1)。在此之后，请输入 8。
4. 对于 **Tag**（标记），请输入 400。
5. 对于 **Security Zone**（安全区域），请选择用户。
6. 单击 **OK**（确定）。

STEP 3 | 为第 2 层接口和两个子接口创建一个 VLAN。

1. 选择 **Network**（网络）> **VLANs** 并 **Add**（添加）VLAN。
2. 输入 VLAN 的 **Name**（名称）；在本示例中，请输入 Datacenter。
3. 对于 **VLAN Interface**（**VLAN** 接口），选择 **None**（无）。
4. 对于 **Interfaces**（接口），单击 **Add**（添加）并选择第 2 层接口 (ethernet1/1) 和两个子接口（ethernet1/1.7 和 ethernet1/1.8）。
5. 单击 **OK**（确定）。

STEP 4 | 阻止区域保护配置文件中的非 IP 协议数据包。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），并 **Add**（添加）配置文件。
2. 输入 **Name**（名称），在本例中为“阻止 LLDP”。
3. 输入配置文件 **Description**（说明）— 从 LLDP 网络到区域内其它接口的“阻止 LLDP”数据包（区域内）。
4. 选择 **Protocol Protection**（协议保护）。
5. 选择 **Exclude List**（排除列表）的 **Rule Type**（规则类型）。


© 2019 Palo Alto Networks, Inc.

6. 输入 **Protocol Name**（协议名称）LLDP。
7. 输入 **Ethertype** 代码 0x88cc。Ethertype 必须以 0x 开头，表示十六进制值。
8. 选择 **Enable**（启用）。
9. 单击 **OK**（确定）。

STEP 5 | 将区域保护配置文件应用到第 2 层 VLAN 所属的安全区域。

1. 选择**Network**（网络）> **Zones**（区域）。
2. **Add**（添加）区域。
3. 输入区域的 **Name**（名称），“用户”。
4. 对于 **Location**（位置），请选择区域应用的虚拟系统。
5. 对于 **Type**（类型），请选择 **Layer2**（第 2 层）。
6. **Add**（添加）属于该区域 ethernet1/1.7 的 **Interface**（接口）。
7. **Add**（添加）属于该区域 ethernet1/1.8 的 **Interface**（接口）。
8. 对于 **Zone Protection Profile**（区域保护配置文件），请选择配置文件“阻止 LLDP”。
9. 单击 **OK**（确定）。

STEP 6 | 提交。

单击 **Commit**（提交）。

STEP 7 | 根据协议保护查看防火墙已丢弃的非 IP 数据包数。

访问 CLI。

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```

# 配置数据包缓冲区保护

您可以在两个级别上配置数据包缓冲区保护：设备级（全局）和区域级（如果全局启用，则也可以在区域级启用）。全局数据包缓冲区保护（**Device**（设备）> **Setup**（设置）> **Session**（会话））用于保护防火墙资源，确保防火墙不会因恶意流量而无响应。

每个入口区域（**Network**（网络）> **Zones**（区域））的数据包缓冲区保护是第二层保护，一旦 IP 地址继续超出数据包缓冲区保护阈值，此保护就开始阻止攻击性 IP 地址。防火墙可以阻止所有来自攻击性源 IP 地址的流量。切记，如果源 IP 地址是一个转换的 NAT IP 地址，很多用户都可以使用同一个 IP 地址。如果有一个滥用用户触发了数据包缓冲区保护，且入口区域启用了数据包缓冲区保护，一旦防火墙将此攻击性源 IP 地址放入其阻止列表，则来自此 IP 地址的所有流量都可被阻止，甚至包括来自非滥用用户的流量。

一种阻止防火墙背后服务遭受 DoS 攻击的最有效方法是对每个入口区域全局配置数据包缓冲区保护。

您可以对区域 **Enable Packet Buffer Protection**（启用数据包缓冲区保护），但是，该保护直至数据包缓冲区保护被全局启用且指定设置后才处于活跃状态。

STEP 1 | 全局启用数据包缓冲区保护。

1. 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），然后编辑会话设置。
2. 选择 **Packet Buffer Protection**（数据包缓冲区保护）。
3. 定义数据包缓冲区保护行为：
   - **Alert (%)**（警报 (%)）— 当数据包缓冲区使用率超过此阈值 10 秒钟以上时，防火墙会每分钟创建一个日志事件。范围为 0% 至 99%；默认为 50%。如果值为 0%，则表示防火墙不能创建日志事件。
   - **Activate (%)**（激活 (%)）— 一旦数据包缓冲区利用率达到此阈值，防火墙就开始通过应用随机早期丢弃 (RED) 缓解最滥用的会话。范围为 0% 至 99%；默认为 50%。如果值为 0%，则表示防火墙



© 2019 Palo Alto Networks, Inc.

不能应用 RED。如果滥用者进入的是一个已启用数据包缓冲区保护的区域，防火墙还可以丢弃滥用会话，或是阻止攻击性源 IP 地址。从默认阈值开始并根据需要进行调整。

防火墙在系统日志中记录警报事件，并在威胁日志中记录丢弃流量、丢弃会话和阻止 *IP* 地址事件。

- **Block Hold Time (sec)**（阻止保持时间（秒））— 在防火墙丢弃之前允许 RED 减轻会话持续的秒数。范围为 0 至 65,535；默认为 60。如果值为 0，则表示防火墙不能根据数据包缓冲区保护丢弃会话。
- **Block Duration (sec)**（阻止期限（秒））— 此设置定义会话保持丢弃或 IP 地址保持阻止的秒数。范围为 1 至 15,999,999，默认为 3,600。

4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

STEP 2 | 启用入口区域的其他数据包缓冲区保护。

1. 选择**Network**（网络）> **Zones**（区域）。
2. 选择入口区域，然后单击其名称。
3. 在区域保护部分 **Enable Packet Buffer Protection**（启用数据包缓冲区保护）。
4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

## 配置基于延迟的数据包缓冲区保护

配置基于延迟的数据包缓冲区保护，并将其用于所包含的流量由对延迟敏感的协议和应用程序构成的区域。

STEP 1 | 选择 **Device**（设备）> **Setup**（设置）> **Session**（会话）。

STEP 2 | 编辑“会话设置”部分，并启用 **Packet Buffer Protection**（数据包缓冲区保护）。

STEP 3 | 启用 **Buffering Latency Based**（基于缓冲延迟）。

STEP 4 | 输入 **Latency Alert (milliseconds)**（延迟警报（毫秒）阈值，一旦超过该值，防火墙就开始每隔一分钟生成一个警报日志事件；范围为 1 - 20,000；默认为 50。

STEP 5 | 输入 **Latency Activate (milliseconds)**（延迟激活（毫秒）阈值，一旦超过该值，防火墙就会激活传入数据包的随机早期丢弃 (RED)，并开始每隔 10 秒生成一个“激活”日志；范围为 1 - 20,000ms；默认为 200ms。

STEP 6 | 输入 **Latency Max Tolerate (milliseconds)**（允许的最大延迟（毫秒））阈值，一旦超过该值，防火墙将使用 RED 且丢弃概率接近 100%；范围为 1 - 20,000ms；默认为 500ms。

如果当前延迟值介于**Latency Activate**（延迟激活）阈值和 **Latency Max Tolerate**（允许的最大延迟）阈值之间，防火墙按下列方式计算 RED 丢弃概率：（当前延迟 - **Latency Activate**（延迟激活）阈值）/(**Latency Max Tolerate**（允许的最大延迟）阈值 - **Latency Activate**（延迟激活）阈值）。例如，如果当前延迟值为 300，**Latency Activate**（延迟激活）值为 200，**Latency Max Tolerate**（允许的最大延迟）值为 500，那么 (300-200)/(500-200) = 1/3，这表示防火墙的 RED 丢弃概率约为 33%。

STEP 7 | 根据利用率，为 Packet Buffer Protection（数据包缓冲区保护）配置**Block Hold Time**（阻止保持时间）和 **Block Duration**（阻止持续时间）。

STEP 8 | 单击 **OK**（确定）。

STEP 9 | 针对每个想要启用基于延迟的数据包缓冲区保护的区域启用第二层保护。

1. 选择 **Network**（网络）> **Zones**（区域），然后选择区域。


© 2019 Palo Alto Networks, Inc.

2. 启用 **Packet Buffer Protection**（数据包缓冲区保护）。

STEP 10 | **Commit**（提交）。

# 配置以太网 SGT 保护

请执行以下任务以配置一个以太网 SGT 保护配置文件。

STEP 1 | 创建“区域保护”配置文件以提供以太网 SGT 保护。

1. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）。
2. 按 **Name**（名称）**Add**（添加）“区域保护”配置文件。
3. 选择 **Ethernet SGT Protection**（以太网 **SGT** 保护）。
4. 按名称 **Add**（添加）**Layer 2 SGT Exclude List**（第 **2** 层 **SGT** 排除列表）。
5. 在列表中输入一个或多个 **Tag**（标签）值，范围为 0- 65,535。您可以单独输入条目数，表示标签值的连续范围（例如，100-500）。您最多可以在排除列表中添加 100 个（单个或连续）标签条目。
6. **Enable**（启用）第 2 层 SGT 排除列表。您可以随时禁用此列表。
7. 单击 **OK**（确定）。

STEP 2 | 将区域保护配置文件应用到第 2 层、虚拟线或旁接接口所属的安全区域。

1. 选择**Network**（网络）> **Zones**（区域）。
2. **Add**（添加）区域。
3. 输入区域的 **Name**（名称）。
4. 对于 **Location**（位置），请选择区域应用的虚拟系统。
5. 对于 **Type**（类型），请选择 **Layer2**（第 **2** 层）、**Virtual Wire**（虚拟线）或 **Tap**（旁接）。
6. **Add**（添加）属于该区域的 **Interface**（接口）。
7. 对于 **Zone Protection Profile**（区域保护配置文件），请选择创建的配置文件。
8. 单击 **OK**（确定）。

STEP 3 | **Commit**（提交）。

STEP 4 | 查看防火墙因部署了以太网 SGTP 保护的所有区域保护配置文件而丢弃的数据包全局计数器。

1. 访问 CLI。
2. > `show counter global name pan_flow_dos_l2_sec_tag_drop`



© 2019 Palo Alto Networks, Inc.

# DoS 保护新会话不受泛滥攻击

DoS 保护新会话不受泛滥攻击，有益于防范大量单会话和多会话攻击。在单会话攻击中，攻击者利用单个会话将防火墙后的设备设定为目标。如果安全规则允许流量，攻击者会建立会话并开始攻击，攻击者以极高的速率向相同的源 IP 地址和端口号、目标 IP 地址和端口号以及协议发送数据包，试图攻陷目标。在多会话攻击中，攻击者利用从单个主机发起多个会话（或每秒连接数 [cps]）来开展 DoS 攻击。



此功能仅能防御新会话的 *DoS* 攻击，即流量还未被加载到硬件上。已加载攻击不受此功能保护。但是，此主题介绍了如何通过创建安全配置文件来重设客户端；此主题讲解了攻击者如何利用每秒产生大量连接来重新开始攻击以及如何阻止攻击。

DoS 保护配置文件和策略规则共同合作，以提供保护免受大量传入的 SYN、UDP、ICMP 和 ICMPv6 数据库以及其他类型的 IP 数据库的泛滥攻击。确定构成泛滥攻击的阈值。通常，DoS 保护配置文件设置防火墙生成 DoS 警报的阈值，采取诸如随机早期丢弃等操作，并删除其他传入连接。配置为保护（而不是允许或拒绝数据包）的 DoS 保护策略规则确定要匹配的数据包标准（例如源地址），以计入阈值。这种灵活性允许您阻止某些流量，或允许某些流量，并将其他流量视为 DoS 流量。当传入速率超过您的最大阈值时，防火墙会阻止来自源地址的传入流量。

- 多会话 DoS 攻击
- 单会话 DoS 攻击
- 针对新会话的泛滥攻击配置 DoS 保护
- 结束单会话 DoS 攻击
- 识别在包缓冲区中占太多百分比的会话
- 不提交丢弃会话

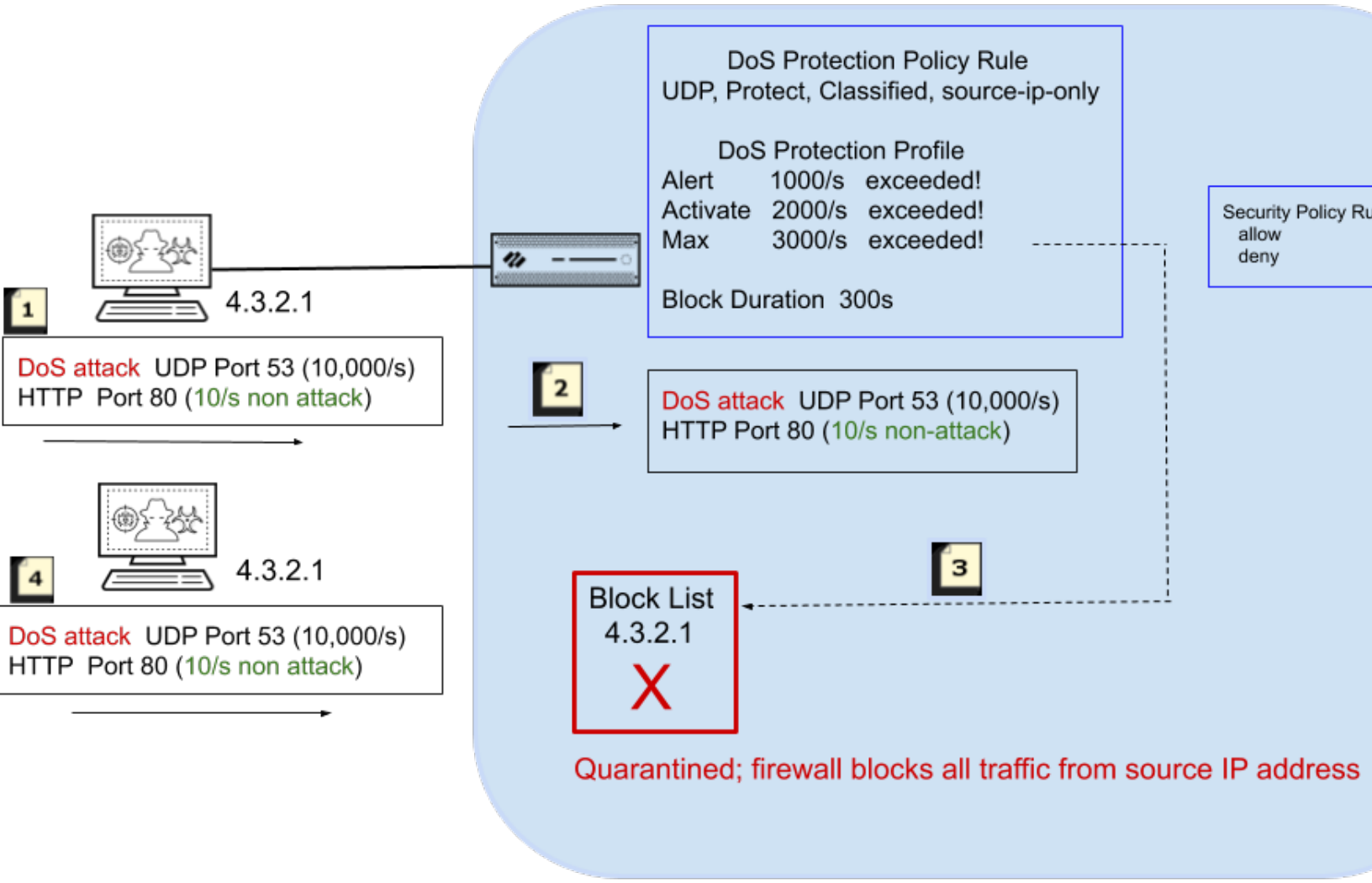
## 多会话 DoS 攻击

通过配置 DoS 保护策略规则来针对新会话的泛滥攻击配置 DoS 保护，从而确定条件，如果传入数据包与条件匹配，则触发 **Protect**（保护）操作。DoS 保护配置文件计算每个新连接的报警率、激活率以及最大速率阈值。如果每秒入站新连接数超出激活速率范围，防火墙将执行 DoS 保护策略规则中指定的操作。

以下示例以图片和表格的形式说明安全策略规则、DoS 保护策略规则和配置文件如何协同工作。



© 2019 Palo Alto Networks, Inc.

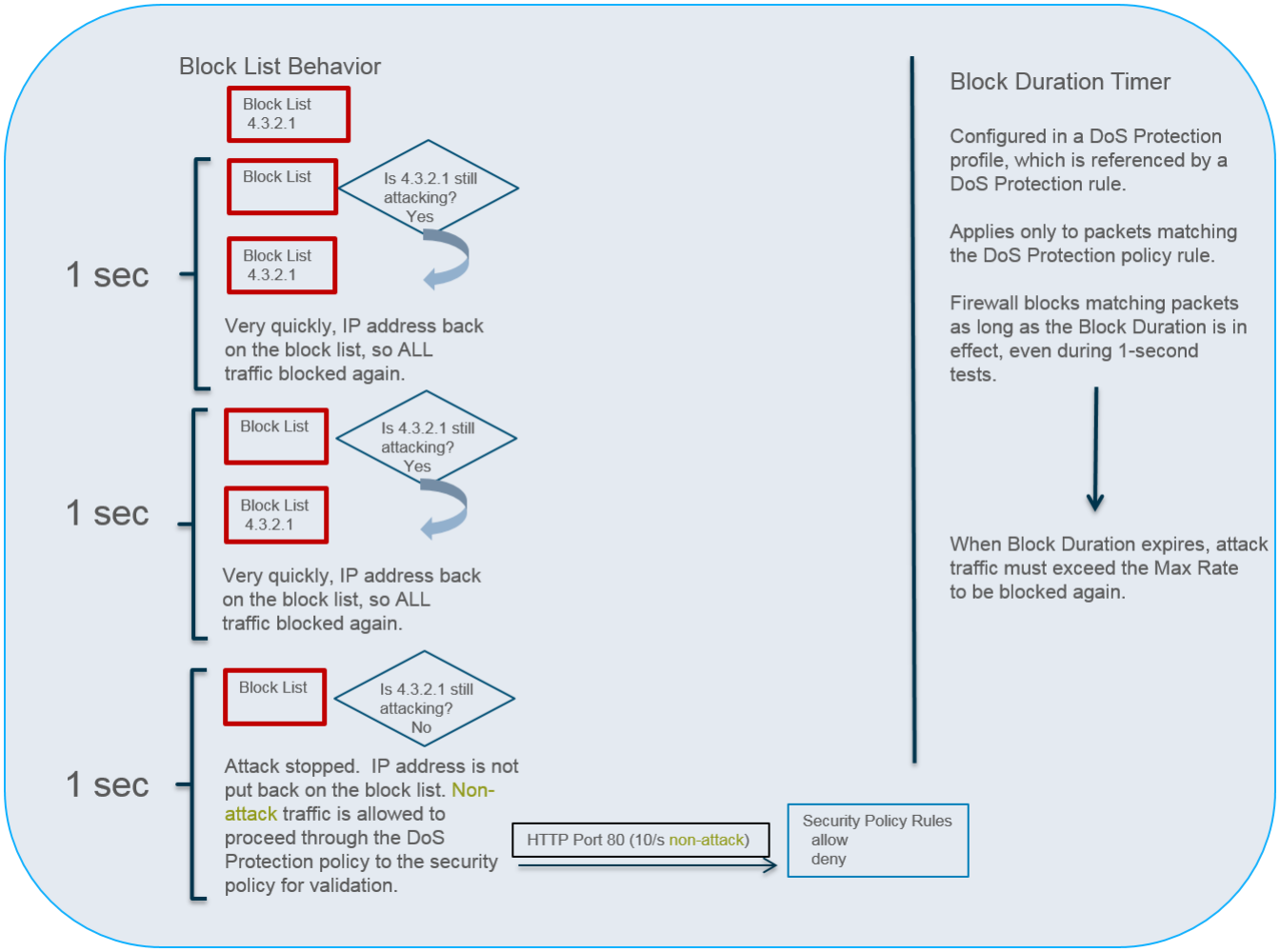



| 防火墙隔离 IP 地址的事件顺序 | |
|---|---|
| 1 | 在此示例中，攻击者以每秒 10,000 次新连接的速率向 UDP 端口 53 发起 DoS 攻击。攻击者同时每秒向 HTTP 端口 80 发送 10 次新连接。 |
| 2 | 这些新连接与 DoS 保护策略规则中的条件匹配，例如源区域或接口、源 IP 地址、目标区域或接口、目标 IP 地址或服务等其他设置。在此示例中，策略规则指定 UDP。<br>DoS 规则还规定了 **Protect**（保护）操作和 **Classified**（分类），这两项设置动态地保持 DoS 保护策略设置生效。DoS 保护配置文件规定可允许的最大速率为每秒发送 3000 个数据包。如果传入数据包匹配 DoS 保护策略规则，则计算 **Alert**（警报）、**Activate**（激活）和 **Max Rate**（最大速率）阈值的新连接数。 |


© 2019 Palo Alto Networks, Inc.

| 防火墙隔离 IP 地址的事件顺序 | |
|---|---|
| | 如果您认为源 *IP* 地址始终具有恶意，还可以使用安全策略规则阻止从该地址发出的所有流量。 |
| 3 | 每秒 10,000 个新连接超过了 **Max Rate**（最大速率）阈值。当以下所有情况出现时：<br>• 超出阈值，<br>• 规定了 **Block Duration**（阻止期限），<br>• **Classified**（分类）被设置为包含源 IP 地址，<br>防火墙阻止列表包含攻击性源 IP 地址。 |
| 4 | 隔离阻止列表中的 IP 地址，意味着从该 IP 地址发出的所有流量都会被阻止。在其他攻击数据包到达安全策略之前，防火墙就阻止了攻击性源 IP 地址。 |

关于匹配 DoS 保护策略规则的 IP 地址被添加到阻止列表之后所发生的情况，下图提供了更多的细节。它还介绍了阻止期限计时器。





© 2019 Palo Alto Networks, Inc.

防火墙允许 IP 地址每秒离开阻止列表一次，以便测试流量模式并判断是否存在攻击。防火墙执行以下操作：

- 在为期 1 秒的测试期间，防火墙允许不匹配 DoS 保护策略条件（此示例中为 HTTP 流量）的数据包通过 DoS 保护策略规则到达安全策略以供验证。只有极少数的数据包（如果有）能够及时通过，因为防火墙在该 IP 地址离开阻止列表之后接收到的第一个攻击数据包将匹配 DoS 保护策略条件，这将导致该 IP 地址在下一秒很快被重新放回阻止列表。防火墙逐秒重复这样的测试，直到攻击停止。
- 防火墙阻止所有经由 DoS 保护策略规则的攻击性流量（地址保留在阻止列表中），直到阻止期限到期。



上图所示的 *1* 秒检查发生在具有多个数据平面 *CPU* 和一个硬件网络处理器的防火墙型号中。所有单个数据平面系统或未装有硬件网络处理器的系统均在软件中执行这一缓解，用时间隔为 *5* 秒。

如果攻击停止，防火墙不会将此 IP 地址放回阻止列表。防火墙允许非攻击性流量通过 DoS 保护策略规则到达安全策略规则以进行评估。您必须配置安全策略规则以允许或拒绝流量，如果未配置，隐藏的拒绝规则将拒绝所有流量。

阻止列表基于源区域和源地址组合。这一行为允许副本 IP 地址存在于属于独立虚拟路由的不同区域。

DoS 保护配置文件中的阻止期限设置规定了防火墙将阻止匹配 DoS 保护策略规则的[攻击性]数据包的时长。防火墙将保持阻止攻击数据包，直到阻止期限到期，此后，攻击数据包必须超出最大速率阈值才会再次被阻止。



如果攻击者利用多个会话或蠕虫发起多个攻击性会话，在没有安全策略拒绝或丢弃规则的情况下，这些会话将向 *DoS* 保护配置文件设置的阈值计数。所以，单会话攻击需要安全策略拒绝或丢弃规则以便为每个数据包根据阈值计数；多会话攻击则无此要求。

因此，针对新会话泛滥攻击的 DoS 保护允许防火墙高效地防御某个源 IP 地址发出的攻击性流量，并且一旦攻击停止，即允许非攻击性流量通过。将攻击性 IP 地址列入设计用于隔离源 IP 地址所有活动（例如，具有不同应用程序的数据包）的阻止列表，使得 DoS 保护功能能够充分利用该阻止列表。隔离试图发起回转程序攻击的现代攻击者发起的所有活动的 IP 地址，他们只需简单地更改应用程序就可以开始新的攻击，或利用不同攻击组合发起混合 DoS 攻击。您可以监控已阻止的 IP 地址以查看阻止列表，从中删除条目，并获取有关阻止列表中 IP 地址的其他信息。



从 *PAN-OS 7.0.2* 开始，防火墙将攻击源 *IP* 地址列入阻止列表的行为有所变化。如果攻击停止，非攻击性流量将被允许到达安全策略执行。匹配 *DoS* 保护配置文件和 *DoS* 保护策略规则的攻击性流量在阻止期限内将保持被阻止状态。

## 单会话 DoS 攻击

单会话 DoS 攻击一般不会触发区域或 DoS 保护配置文件，因为该攻击形成于会话创建之后。安全策略允许创建会话，因此也允许这些攻击，并且会话被创建之后，攻击将提升数据包数量，然后攻陷目标设备。

针对新会话的泛滥攻击配置 DoS 保护以保护新会话不受泛滥攻击（单会话和多会话泛滥攻击）。如果正在受到单会话攻击，您还需要结束单会话 DoS 攻击。

## 针对新会话的泛滥攻击配置 DoS 保护

STEP 1 | 配置安全策略规则以拒绝来自攻击者 IP 地址的流量，并根据您的网络需求允许其他流量。您可以在安全策略规则中指定任何匹配条件，例如源 IP 地址。（对缓解单会话攻击或尚未触发 DoS 保护策略阈值的攻击为必需；对缓解多会话攻击为可选）。



该步骤是阻止现有攻击通常采用的步骤之一。请参阅结束单会话 DoS 攻击。



© 2019 Palo Alto Networks, Inc.

- 创建安全策略规则

STEP 2 | 为泛滥攻击保护配置 DoS 保护配置文件。



由于泛滥攻击可以出现在多个协议上，因此，最佳实践是，在 *DoS* 保护配置文件中为所有泛滥攻击类型激活保护。

1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **DoS Protection**（**DoS** 保护）并 **Add**（添加）配置文件 **Name**（名称）。
2. 选择 **Classified**（已分类）作为 **Type**（类型）。
3. 为 **Flood Protection**（泛滥攻击保护）选择所有类型的泛滥攻击保护：
   - **SYN Flood**（**SYN** 泛滥攻击）
   - **UDP Flood**（**UDP** 泛滥攻击）
   - **ICMP Flood**（**ICMP** 泛滥攻击）
   - **ICMPv6 Flood**（**ICMPv6** 泛滥攻击）
   - **Other IP Flood**（其他 **IP** 泛滥攻击）
4. 启用 **SYN Flood**（**SYN** 泛滥攻击）时，选择每秒连接 (cps) 超过 **Activate Rate**（激活速率）阈值时发生的 **Action**（操作）：
   1. **Random Early Drop**（随机早期丢弃）— 防火墙使用一种算法来逐步开始丢弃该类数据包。如果攻击持续，则传入 cps 速率（高于 **Activate Rate**（激活速率））越高，防火墙丢弃的数据包越多。防火墙会持续丢弃数据包，直到传入 cps 速率达到 **Max Rate**（最大速率），此时防火墙将丢弃所有传入的连接。**Random Early Drop**（随机早期丢弃）(RED) 是 **SYN Flood**（**SYN** 泛滥攻击）的默认动作，是 **UDP Flood**（**UDP** 泛滥攻击）、**ICMP Flood**（**ICMP** 泛滥攻击）、**ICMPv6 Flood**（**ICMPv6** 泛滥攻击）和 **Other IP Flood**（其他 **IP** 泛滥攻击）的唯一动作。RED 比 SYN Cookie 更有效率，可以处理更大的攻击，但不会辨别正常流量和恶意流量。
   2. **SYN Cookies** — 不是立即将 SYN 发送到服务器，而是防火墙先生成一个 cookie（代表服务器），然后再发送 SYN-ACK 到客户端。客户端响应其 ACK 和 cookie；经过验证后，防火墙将 SYN 发送到服务器。**SYN Cookies** 操作比 **Random Early Drop**（随机早期丢弃）需要更多的防火墙资源；由于会影响恶意流量，因此更具辨识力。
5. （可选）在每个泛滥攻击选项卡中，根据您的环境更改以下阈值：
   - **Alarm Rate (connections/s)**（警报速率（连接数/秒））— 指定生成 DoS 警报的阈值速率 (cps)。（范围为 0-2,000,000；默认为 10,000。）
   - **Activate Rate (connections/s)**（激活速率（连接数/秒））— 指定激活 DoS 响应的阈值速率 (cps)。如果达到 **Activate Rate**（激活速率）阈值，则会发生 **Random Early Drop**（随机早期删除）。范围为 0 - 2,000,000，默认为 10,000。（对于 SYN 泛滥攻击，您可以选择发生的操作。）
   - **Max Rate (connections/s)**（最大速率（连接数/秒））— 指定防火墙允许的每秒入站连接的速率阈值。超过阈值时，到达的新连接将被丢弃。（范围为 2-2,000,000；默认为 40,000。）

   此步骤中的默认阈值仅为起始值，可能并不适用于您的网络。您需要分析网络行为并正确设置初始阈值。
6. 在每一个泛滥攻击选项卡中，指定 **Block Duration**（阻止期限）（以秒为单位），在此时间段内，防火墙将阻止与引用该配置文件的 DoS 保护策略文件匹配的数据包。指定的值要大于 0。（范围为1-21,600；默认为 300。）

   如果您担心防火墙对错误标识为攻击性流量的数据包进行不必要的拦截，请设置较低的 *Block Duration*（阻止期限）。

   如果您更希望阻止大量的攻击而不是担心防火墙错误阻止不属于攻击部分的流量，请设置较高的 **Block Duration**（阻止期限）。



© 2019 Palo Alto Networks, Inc.

7. 单击 **OK**（确定）。

STEP 3 | 配置 DoS 保护策略规则来指定入站流量的匹配条件。



防火墙资源有限，因此您不希望在面向 *Internet* 的区域使用源地址进行分类，因为可能存在大量符合 *DoS* 保护策略规则的唯一 *IP* 地址。这将需要许多计数器，防火墙会在跟踪时耗尽资源。相反，应定义使用（所保护的服务器的）目标地址进行分类的 *DoS* 保护策略规则。

1. 选择 **Policies**（策略）> **DoS Protection**（**DoS** 保护）并在 **General**（常规）选项卡中 **Add**（添加）**Name**（名称）。名称区分大小写，最多可包含 31 个字符，包括字母、数字、空格、连字符和下划线。
2. 在 **Source**（源）选项卡中，选择 **Type**（类型）为 **Zone**（区域）或 **Interface**（接口），然后 **Add**（添加）该区域或接口。根据您的部署和您想要保护的内容，选择区域或接口。例如，如果您只有一个接口进入防火墙，请选择“接口”。
3. （可选）对于 **Source Address**（源地址），选择 **Any**（任意），以便任何入站 IP 地址均可匹配匹配规则，或 **Add**（添加）地址对象，例如地理范围。
4. （可选）对于 **Source User**（源用户），选择 **any**（任意）或指定一名用户。
5. （可选）选择 **Negate**（求反）来匹配除了您指定的源之外的任意源。
6. （可选）在 **Destination**（目标）选项卡中，选择 **Type**（类型）为 **Zone**（区域）或 **Interface**（接口），并 **Add**（添加）该目标区域或接口。例如，输入您要保护的安全区域。
7. （可选）对于 **Destination Address**（目标地址），选择 **Any**（任意）或输入要保护的设备的 IP 地址。
8. （可选）在 **Option/Protection**（选项/保护）选项卡中，**Add**（添加）**Service**（服务）。选择服务或单击 **Service**（服务）并输入 **Name**（名称）。选择 **TCP** 或 **UDP**。输入 **Destination Port**（目标端口）。如果没有指定特定的服务，则允许规则匹配任意协议类型的泛滥攻击，与应用程序设定的端口无关。
9. 在 **Option/Protection**（选项/保护）选项卡中，对于 **Action**（操作），选择 **Protect**（保护）。
10. 选择 **Classified**（已分类）。
11. 对于 **Profile**（配置文件），选择创建的 **DoS Protection**（**DoS** 保护）配置文件的名称。
12. 对于 **Address**（地址），选择 **source-ip-only**（仅源 **IP**）或 **src-dest-ip-both**（源 **IP** 和目标 **IP**），这将确定规则应用的 IP 地址类型。根据您要让防火墙如何识别攻击性流量来选择设置：
    - 如果您要让防火墙仅分类源 IP 地址，请指定 **source-ip-only**（仅源 **IP**）。由于攻击者通常会测试主机入口网络来开展攻击，所以 **source-ip-only**（仅源 **IP**）是适用于更广泛测试的典型设置。
    - 如果您只想保护包含指定目标地址的服务器免受 DoS 攻击，同时确保每个源 IP 地址不会超出服务器设定的每秒连接数 (cps) 阈值，请指定 **src-dest-ip-both**（源 **IP** 和目标 **IP**）。
13. 单击 **OK**（确定）。

STEP 4 | 提交。

单击 **Commit**（提交）。

# 结束单会话 DoS 攻击

为减轻单会话 DoS 攻击，您仍需提前针对新会话的泛滥攻击配置 DoS 保护。在某些情况下，在您配置完此功能之后，在您发觉之前，DoS 攻击（从会话 IP 地址发起）可能已经开始了。如果您发现单会话 DoS 攻击，请执行以下任务来中止会话，从该 IP 地址发出的后序连接尝试将触发 DoS 保护新会话免受泛滥攻击。

STEP 1 | 识别发起攻击的源 IP 地址。

例如，利用防火墙数据包捕获功能和目标筛选器收集流向目标 IP 地址的流量样本。另外，可使用目标地址的 ACC 筛选来查看受攻击的目标主机的活动。



© 2019 Palo Alto Networks, Inc.

STEP 2 | 创建 DoS 保护策略规则，当超出攻击阈值时，该规则会阻止攻击者的 IP 地址。

STEP 3 | 创建安全策略规则，拒绝源 IP 地址及其攻击性流量。

STEP 4 | 通过执行 **clear session all filter source *<ip-address>*** 操作命令，可终止攻击性源 IP 地址当前发出的任意攻击。

另外，如果您知道会话 ID，可执行 **clear session id *<value>*** 命令来单独中止会话。



如果您使用 ***clear session all filter source <ip-address>*** 命令，所有匹配源 *IP* 地址的会话都将被中止，无论是否具有恶意。

在您中止当前攻击会话之后，从攻击性会话发出的任意后续尝试都将被安全策略阻止。DoS 保护策略向阈值计数所有的连接尝试。当超出最大速率阈值时，在阻止期限内，源 IP 地址将被阻止，如多会话 DoS 攻击中所述。

## 识别在包缓冲区中占太多百分比的会话

如果防火墙显示出资源用尽的信号，那它有可能正被攻击，对方发送了数量巨大的数据包。那种情况下防火墙开始缓存入站数据包。您很快就能发现包缓冲区中占太多百分比的会话，可以放弃他们，降低影响。

在所有基于硬件的防火墙型号上（不是 VM 系列防火墙）执行以下任务，以便为每个插槽和数据面板识别被使用的数据包缓冲区百分比、使用超过百分之二数据包缓冲区的前五个会话、以及与这些会话关联的源 IP 地址。有了这些信息您就可以采取合适的操作。

STEP 1 | 查看防火墙资源使用，最高会话和会话详情。在 CLI 中执行以下操作命令（以下命令输出示例）

```
admin@PA-7050> show running resource-monitor ingress-backlogs
-- SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 92%  TOTAL: 93%
TOP SESSIONS:SESS-ID      PCT   GRP-ID   COUNT
6            92%   1        156                  7        1732
SESSION DETAILS SESS-ID PROTO SZONESRC       SPORT  DST       DPORT  IGR-
IF    EGR-IF       APP
6    6     trust 192.168.2.35 55653  10.1.8.89 80  ethernet1/21 ethernet1/22
 undecided
```

命令显示了最多5个占用包缓冲区2%以上比例的会话。

上面的示例输出表示，会话6用 TCP 数据包（协议6）占用了包缓冲区的92%，源 IP 地址为 192.168.2.35。

- **SESS-ID** — 表示在其他所有 **show session** 命令中使用的全局会话 ID。全局会话 ID 在防火墙中是唯一的。
- **GRP-ID** — 表示数据包内部处理的阶段。
- **COUNT**（计数）— 表示该会话有多少数据包在 GRP-ID。
- **APP** — 表示从会话信息中提取的 App-ID，有助于您确定流量是否合法。例如，如果数据包使用通用 TCP 或 UDP 端口，但 CLI 输出显示 APP 是 `undecided`，数据包就有可能是攻击流量。当应用程序 IP 解码器不能得到足够信息确定应用程序时，APP 为`undecided`。APP 为`unknown`表示应用程序 IP 解码器不能确定应用程序；在包缓冲区中占用太高比例的`unknown` APP 的会话也是可疑的。

要限制显示输出：

在 PA-7000 系列型号上，您可以将输出限制到一个插槽、数据面板上或两者同时。例如：

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1
```



© 2019 Palo Alto Networks, Inc.

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1 dp
 dp1
```

仅在 PA-5200 系列和 PA-7000 系列型号上，可以将输出限制在数据面板上。例如：

```
admin@PA-5260> show running resource-monitor ingress-backlogs dp dp1
```

STEP 2 | 用命令输出确定占用包缓冲区太高比例的源 IP 地址的源发送的是合法流量还是攻击流量。

以上示例输出中，有可能发生了一个会话攻击。一个会话（会话 ID 6）正在为插槽 1 (DP 1) 使用 92% 的数据包缓冲区，并且此时应用程序为 `undecided`。

- 如果您确定一名用户正在发送攻击，而且流量没有卸载，您可以结束单会话 DoS 攻击。至少，您可以针对新会话的泛滥攻击配置 DoS 保护。
- 在具有现场可编程门阵列 (FPGA) 的硬件型号上，防火墙在可能会提高性能时，将流量卸载到 FPGA。如果流量卸载到硬件，清除会话不起作用，因为必须要软件处理这些连续发来的数据包。相反，您应该不提交丢弃会话。

要查看会话是否已卸载，可使用 CLI 中的 **show session id *<session-id>*** 操作命令，如以下所示。`layer7 processing` 值为已卸载的会话显示为 `completed`，为未卸载的会话显示为 `enabled`。



© 2019 Palo Alto Networks, Inc.

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```

## 不提交丢弃会话

执行该任务永久丢弃会话，如超载包缓冲区的会话。不需要提交；执行命令后会话立刻就被丢弃。命令适用于卸载和没卸载的会话。

STEP 1 | 在 CLI 中，在任意硬件平台上执行以下操作命令：

```
admin@PA-7050> request session-discard [timeout <seconds>] [reason <reason-string>] id <session-id>
```

默认超时为 3,600 秒。

STEP 2 | 验证会话已丢弃。

```
admin@PA-7050> show session all filter state discard
```



© 2019 Palo Alto Networks, Inc.

# 认证

以下主题对如何配置 Palo Alto Networks® 防火墙和应用程序，使其支持通用标准和联邦信息处理标准 140-2 (FIPS 140-2) 的过程进行了说明，这些安全证书可确保采用一套标准的安全保证措施及功能。通常，美国国民政府代理机构和政府承包商会需要这些证书。

有关产品证书和第三方验证的详细信息，请参阅证书页面。


> 启用 FIPS 和通用条件支持
> FIPS-CC 安全功能
> 在 FIPS-CC 模式下清洗防火墙或设备的交换内存

# 启用 FIPS 和通用条件支持

采用以下步骤，在支持通用标准和联邦信息处理标准 140-2 (FIPS 140-2) 的软件版本上启用 FIPS-CC 模式。启用 FIPS-CC 模式后，所有 FIPS 和 CC 功能均被启用。

所有 Palo Alto Networks 下一代防火墙和设备（包括 VM 系列防火墙）都支持 FIPS-CC 模式。要启用 FIPS-CC 模式，首先将防火墙引导到维护恢复工具 (MRT) 中，然后将操作模式从正常模式更改为 FIPS-CC 模式。所有防火墙和设备均采用相同的步骤来更改操作模式，但访问 MRT 的过程各不相同。

启用 *CC/FIPS* 时，防火墙将重置为出厂默认设置，所有配置均将删除。

- 访问维护恢复工具 (MRT)
- 将操作模式更改为 FIPS-CC 模式

## 访问维护恢复工具 (MRT)

维护恢复工具 (MRT) 使您能够在 Palo Alto Networks 防火墙和设备上执行多项任务。例如，您可以将防火墙或设备恢复至出厂默认设置、将 PAN-OS 或内容更新还原至先前版本、在文件系统上运行诊断程序、收集系统信息以及提取日志等。此外，您可以使用 MRT 将操作模式更改为 FIPS-CC 模式或从 FIPS-CC 模式更改为正常模式。

以下步骤介绍了如何访问各种 Palo Alto Networks 产品上的维护恢复工具 (MRT)。

- 访问硬件防火墙和设备（如 PA-220 防火墙、PA-7000 系列防火墙或 M 系列设备）上的 MRT。
  1. 建立到防火墙或设备的串行控制台会话。
     1. 使用串行电缆将计算机上的串行端口与防火墙或设备上的控制台端口相连。

        如果您的计算机没有 *9* 针串行端口，但有 *USB* 端口，请使用串行转 *USB* 转换器建立连接。如果防火墙具有微型 USB 控制台端口，请将使用标准 *A* 型 *USB* 的端口与微型 *USB* 电缆相连接。
     2. 打开计算机上的终端模拟软件，并设置为 9600-8-N-1，然后连接到相应的 COM 端口。

        在 *Windows* 系统上，您可以转到控制面板查看设备和打印机的 *COM* 端口设置，以确定分配给控制台的 *COM* 端口。
     3. 使用管理员帐户登录。（默认的用户名/密码为 admin/admin。）
  2. 输入以下 CLI 命令，然后按 **y** 确认：

     ```
     debug system maintenance-mode
     ```
  3. 将防火墙或设备引导至 MRT 欢迎屏幕（约 2 到 3 分钟）后，按 **Continue**（继续）上的 Enter，访问 MRT 主菜单。

     还可以重启防火墙或设备，然后在维护模式提示符下键入 ***maint***，来访问 *MRT*。需要直接连接串行控制台。

     将防火墙或设备引导至 MRT 后，可以通过与管理 (MGT) 接口 IP 地址建立的 SSH 连接来远程访问 MRT。在登录提示符下，键入 **maint** 作为用户名，并将防火墙或设备序列号作为密码。



© 2019 Palo Alto Networks, Inc.

- 访问部署在私有云（例如 VMware ESXi 或 KVM 管理程序）上 VM 系列防火墙上的 MRT。
  1. 与防火墙的管理 IP 地址建立 SSH 会话，并使用管理员帐户登录。
  2. 输入以下 CLI 命令，然后按 **y** 确认：

     ```
     debug system maintenance-mode
     ```

     防火墙需要约 *2* 到 *3* 分钟才能引导至 *MRT*。在此期间，您的 *SSH* 会话将断开连接。
  3. 将防火墙引导至 MRT 欢迎屏幕后，根据操作模式登录：
     - 正常模式 — 建立与防火墙管理 IP 地址的 SSH 会话，并使用 **maint** 作为用户名，防火墙或设备序列号作为密码进行登录。
     - **FIPS-CC** 模式 — 访问虚拟机管理实用程序（如 vSphere Client）并连接到虚拟机控制台。
  4. 在 MRT 欢迎屏幕，按 **Continue**（继续）上的 Enter 以访问 MRT 主菜单。
- 访问部署在公共云（如 AWS 或 Azure）上 VM 系列防火墙上的 MRT。
  1. 与防火墙的管理 IP 地址建立 SSH 会话，并使用管理员帐户登录。
  2. 输入以下 CLI 命令，然后按 **y** 确认：

     ```
     debug system maintenance-mode
     ```

     防火墙需要约 *2* 到 *3* 分钟才能引导至 *MRT*。在此期间，您的 *SSH* 会话将断开连接。
  3. 将防火墙引导至 MRT 欢迎屏幕后，根据虚拟机类型登录：
     - **AWS** — 以 **ec2-user** 登录，并选择部署时与虚拟机关联的 SSH 公钥。
     - **Azure** — 输入部署 VM 系列防火墙时创建的凭据。
     - **GCP** — 以 **gcp-user** 登录，并选择部署时与虚拟机关联的 SSH 公钥。
  4. 在 MRT 欢迎屏幕，按 **Continue**（继续）上的 Enter 以访问 MRT 主菜单。

# 将操作模式更改为 FIPS-CC 模式

以下步骤介绍如何将 Palo Alto Networks 产品的操作模式从正常模式更改为 FIPS-CC 模式。

STEP 1 | （仅限 VM 系列防火墙或 Panorama 虚拟设备）创建 SHH 密钥并登录到防火墙或 Panorama。

在 Microsoft Azure 等部分公共云平台上，更改为 FIPS-CC 模式后，您必须要有一个 SSH 密钥以防止身份验证失败。验证您是否已将防火墙部署为使用 SSH 密钥进行身份验证。尽管您可以在 Azure 上部署 VM 系列防火墙或 Panorama，并使用用户名和密码进行登录，但是，一旦将操作模式更改为 FIPS-CC，就无法使用用户名和密码进行身份验证。重置为 FIPS-CC 模式后，必须使用 SSH 密钥登录，然后才可以配置随后将用于登录到防火墙 Web 界面的用户名和密码。

STEP 2 | 连接到防火墙或设备，并 访问维护恢复工具 (MRT)。

STEP 3 | 从菜单中选择 **Set FIPS-CC Mode**（设置 FIPS-CC 模式）。

STEP 4 | 选择 **Enable FIPS-CC Mode**（启用 **FIPS-CC** 模式）。模式更改操作开始，状态指示器显示进度。模式更改完成后，状态显示 **Success**（成功）。

STEP 5 | 出现提示时，选择 **Reboot**（重新启动）。


© 2019 Palo Alto Networks, Inc.

如果更改公共云中部署的 *VM* 系列防火墙的操作模式，且在 重新启动之前丢失与 *MRT* 的 *SSH* 连接，则必须等待 *10-15* 分钟才能完成模式更改，登录回 *MRT*，然后重新启动防火墙以完成操作。重置为 *FIPS-CC* 模式后，在 *Panorama* 或 *VM* 系列等某些虚拟化形式上，您只能使用 *SSH* 密钥登录，并且，如果您尚未设置使用 *SSH* 密钥进行身份验证，则再也无法在重新启动后登录到防火墙。

切换到 FIPS-CC 模式后，您会看到以下状态：`FIPS-CC 模式已成功启用。`

此外，将进行以下更改：

- FIPS-CC 始终显示于 Web 界面底部的状态栏。
- 默认管理员登录凭据更改为 admin/paloalto。

有关 FIPS-CC 模式下实施的安全功能的详细信息，请参阅 FIPS-CC 安全功能。



© 2019 Palo Alto Networks, Inc.

# FIPS-CC 安全功能

FIPS-CC 模式启用后，将在所有防火墙和设备上应用以下安全功能：

- 要登录，浏览器必须与 TLS 1.1（或更高版本）兼容；在 WF-500 设备上，您只能通过 CLI 管理设备，且必须使用与 SSHv2 兼容的客户端应用程序进行连接。
- 所有密码必须至少有六个字符。
- 您必须确保身份验证设置的 **Failed Attempts**（失败尝试）及 **Lockout Time (min)**（锁定时间（分钟））大于 0。如果管理员达到 **Failed Attempts**（失败尝试）阈值，则其在 **Lockout Time (min)**（锁定时间（分钟））字段规定的时间内将无法进入。
- 您必须确保身份验证设置中的 **Idle Timeout**（空闲超时）大于 0。如果登录会话的空闲时间长度超过指定值，那么管理员将自动退出。
- 您可以配置 **Absolute Session Length**（绝对会话长度）来设置用户可以登录的最大时间长度（以分钟为单位）。最小长度可以设为 60 分钟。您将在会话超时前 5 分钟收到会话终止警告。在 FIPS-CC 模式下无法禁用此功能，默认会话时间长度为 30 天。
- 您可以配置 **Max No. of Sessions**（最大会话数）以设置可以同时登录到同一管理员账户的用户数。
- 防火墙或设备将自动确定适当的自检级别，并在加密算法和加密套件中实施适当的强度级别。
- 不解密未经批准的 FIPS-CC 算法，因为在解密期间会将其忽略。
- 配置 IPSec VPN 时，管理员必须选择在 IPSec 设置期间向管理员显示的密码套件选项。
- （仅限 Panorama 和 WildFire）可以启用管理接口上的 IPSec 以保护 NTP、RADIUS、TACACS 和 DNS 等协议。
- 自生成和导入的证书必须包含 RSA 2,048 位（或更高）或 ECDSA 256 位（或更高）格式的公钥，并且您还必须使用 SHA256 或更高的摘要。

  不能使用硬件安全模块 (HSM) 来存储用于 SSL 转发代理或 SSL 入站检查的专用 *ECDSA* 密钥。
- Telnet、TFTP 和 HTTP 管理连接不可用。
- 您必须为 HA1 控制链路启用加密。您必须设置自动密钥更新参数；您必须将数据参数设为不超过 1000 MB 的值（不得留为默认）且您必须设置时间间隔（不能将其留为禁用）。
- FIPS-CC 模式下的串行控制台端口仅作为有限状态输出端口使用；CLI 访问不可用。
- 引导到 MRT 的硬件和私有云 VM 系列防火墙上的串行控制台端口提供对 MRT 的交互式访问。
- 引导到 MRT 的管理系统环境中私有云 VM 系列防火墙不支持交互式控制台访问；您只能使用 SSH 访问 MRT。


© 2019 Palo Alto Networks, Inc.

# 刷洗正在 FIPS-CC 模式下运行的防火墙或设备的交换内存

服务器或设备在 FIPS-CC 模式下退役之前，或是将送修之前，应确保敏感信息已从交换内存中删除。使用此过程从交换分区中删除所有加密安全参数 (CSP) 信息。

如果要将由 *Panorama* 管理的防火墙送修，请参阅开始更换 RMA 防火墙之前。

STEP 1 | 打开对防火墙或设备的 SSH 管理会话。

STEP 2 | 运行以下操作命令：

```
request [restart | shutdown] system with-swap-scrub [dod | nnsa]
```

例如，要关闭防火墙或设备并执行国防部 (DoD) 要求的刷洗，则运行以下命令：

```
request shutdown system with-swap-scrub dod
```

STEP 3 | 在出现警告提示时按下 **y** 以启动刷洗。

STEP 4 | 检验清洗是否已成功完成。查看 **System**（系统）日志，并根据 **swap**（交换）一词进行筛选。**System**（系统）日志指示每个交换分区的刷洗状态（一个或多个分区，视型号而定），并显示一条用于指示整个清洗状态的日志条目。如果所有交换分区上的刷洗已成功完成，则 **System**（系统）日志将显示 **Swap space scrub was successful**。

如果一个或多个交换分区上的刷洗失败，则 **System**（系统）日志将显示 `Swap space scrub was unsuccessful`。以下屏幕截屏显示了具有两个分区的防火墙日志结果。

| | | | | | |
|---|---|---|---|---|---|
| 06/08 10:24:02 | general | medium | general | | Swap space scrub was successful |
| 06/08 10:24:02 | general | medium | general | | Scrub performed on swap space /opt/panlogs/.secondary_swapfile |
| 06/08 10:24:02 | general | medium | general | | Scrub performed on swap space /dev/sda7 |

要使用 *CLI* 查看清洗日志，请运行命令 ***show log system | match swap***。

如果使用关闭命令启动刷洗，则防火墙或设备将在刷洗结束后关闭。打开防火墙或设备之前，必须先断开电源，然后重新连接电源。