paloalto TECHDOCS

PAN-OS® 网络管理员指南

Version 11.1 & later



docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

© 2023-2024 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

May 1, 2024

Table of Contents

网络 11
网络简介 12
配置接口 15
旁接接口 16
虚拟线路接口 18
虚拟线路上的第 2 层和第 3 层数据包 19
虚拟线路接口的端口速度 19
虚拟线路上的 LLDP 20
虚拟线路的聚合接口 20
虚拟线路支持高可用性 20
虚拟线路接口的区域保护 20
VLAN 标记的流量 20
Virtual Wire 子接口 21
配置虚拟线路 23
第 2 层接口 26
不带 VLAN 的第 2 层接口 26
带 VLAN 的第 2 层接口 27
配置第 2 层接口 28
配置第 2 层接口、子接口和 VLAN 28
管理每个 VLAN 生成树 (PVST+) BPDU 重写 29
第 3 层接口 32
配置第 3 层接口 36
使用 NDP 管理 IPv6 主机 45
蜂窝接口 50
为蜂窝接口配置 5G 50
升级 5G 固件 67
在子接口上配置 PPPoE 客户端 78
配置 IPv6 PPPoE 客户端 82
配置聚合接口组 88
配置用于网络分段的 Bonjour Reflector 92
使用接口管理概要文件限制访问 94
虚拟路由器 97
虚拟路由器概述 98
配置虚拟路由器 99
服务路由 101

 ©2024 Palo Alto Networks, Inc.

服务路由概述 102
配置服务路由 103

静态路由 105
静态路由概述 106
基于路径监控删除静态路由 107
配置静态路由 109
为静态路由配置路径监控 111

RIP 113
RIP 概述 114
配置 RIP 115

OSPF 117
OSPF 概念 118
OSPFv3 118
OSPF 邻居 118
OSPF 区域 118
OSPF 路由器类型 119
配置 OSPF 120
配置 OSPFv3 123
配置 OSPF 平稳重启 127
确认 OSPF 运行 128
查看路由表 128
确认 OSPF 邻居 128
确认建立了 OSPF 连接 128

BGP 129
BGP 概述 130
MP-BGP 131
配置 BGP 133
为 IPv4 或 IPv 6 单播配置带 MP-BGP 的 BGP 对等设备 141
为 IPv4 多播配置带 MP-BGP 的 BGP 对等设备 144
BGP 联合 146

IP 多播 153
IGMP 154
PIM 155
最短路径树 (SPT) 和共享树 157
PIM 断言机制 158
反向路径转发 159

 ©2024 Palo Alto Networks, Inc.

配置 IP 多播 160
查看 IP 多播信息 168
路由重新分发 171
路由重新分发概述 172
配置路由重新分发 173
GRE 隧道 177
GRE 隧道概述 178
创建 GRE 隧道 180
DHCP 183
DHCP 概述 184
防火墙作为 DHCP 服务器和客户端 185
防火墙作为 DHCPv6 客户端 186
DHCP 消息 188
DHCP 寻址 189
DHCP 地址分配方法 189
DHCP 租借 189
DHCP 选项 191
预定义 DHCP 选项 191
DHCP 选项的多个值 192
DHCP 选项 43、55 和 60 以及其他自定义选项 192
管理接口上的动态 IPv6 寻址 194
将接口配置为 DHCP 服务器 198
将接口配置为 DHCPv4 客户端 202
使用前缀委派将接口配置为 DHCPv6 客户端 204
将管理接口配置为 DHCP 客户端 219
配置用于动态 IPv6 地址分配的管理接口 222
将接口配置为 DHCP 中继代理 225
对 DHCP 进行监控和故障排除 226
查看 DHCP 服务器信息 226
清除 DHCP 租借 226
查看 DHCP 客户端信息 227
收集 DHCP 的相关调试输出 227
DNS 229
DNS 概述 230
DNS 代理对象 232
DNS 服务器配置文件 233
多租户 DNS 部署 234

 ©2024 Palo Alto Networks, Inc.

配置 DNS 代理对象 235
配置 DNS 服务器配置文件 240
配置 Web 代理 241
配置显式代理 242
配置透明代理 258
为显式 Web 代理配置身份验证 271
配置显式代理身份验证的豁免 283
为所有显式代理流量免除身份验证 285
用例 1：防火墙要求执行 DNS 解析 287
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。 290
用例 3：防火墙充当客户端和服务器之间的 DNS 代理 293
DNS 代理规则和 FQDN 匹配 295

DDNS 299

动态 DNS 概述 300
为防火墙接口配置动态 DNS 302

NAT 305

NAT 策略规则 306
NAT 策略概述 306
已被标识为地址对象的 NAT 地址池 307
NAT 地址池的代理 ARP 307
源 NAT 和目标 NAT 309
源 NAT 309
目标 NAT 313
DNS 重写目标 NAT 用例 315
NAT 规则容量 320
动态 IP 和端口 NAT 超额订阅 321
数据面板 NAT 内存统计信息 322
配置 NAT 323
将内部客户端 IP 地址转换为公共 IP 地址（源 DIPP NAT） 324
创建具有持久 DIPP 的源 NAT 规则 325
PAN-OS 326
Strata Cloud Manager 327
使内部网络上的客户端能够访问公共服务器（目标 U-Turn NAT） 329
为面向公众的服务器启用双向地址转换（静态源 NAT） 330
配置 DNS 重写目标 NAT 330
使用动态 IP 地址配置目标 NAT 331
修改 DIPP NAT 的超额订阅率 333

 ©2024 Palo Alto Networks, Inc.

保留动态 IP NAT 地址 334
为特定主机或接口禁用 NAT 335
NAT 配置示例 336
目标 NAT 示例 — 一对一映射 336
带有端口转换示例的目标 NAT 337
目标 NAT 示例 — 一对多映射 338
源和目标 NAT 示例 338
Virtual Wire 源 NAT 示例 340
Virtual Wire 静态 NAT 示例 341
Virtual Wire 目标 NAT 示例 341
NPTv6 343
NPTv6 概述 344
唯一本地地址 344
使用 NPTv6 的理由 345
NPTv6 的运作方式 346
校验和中性映射 347
双向转换 347
应用于特定服务的 NPTv6 348
NDP 代理 349
NPTv6 和 NDP 代理示例 350
NPTv6 示例中的 ND 高速缓存 350
NPTv6 示例中的 NDP 代理 350
NPTv6 示例中的 NPTv6 转换 350
不会转换 ND 高速缓存中的邻居 351
创建 NPTv6 策略 352
NAT64 355
NAT64 概况 356
嵌入 IPv4 的 IPv6 地址 357
DNS64 服务器 358
路径 MTU 发现 359
IPv6 启动的通信 360
为 IPv6 启动的通信配置 NAT64 362
为 IPv4 启动的通信配置 NAT64 366
通过端口转换为 IPv4 启动的通信配置 NAT64 369
ECMP 373
ECMP 负载均衡算法 374
在虚拟路由器上配置 ECMP 376

 ©2024 Palo Alto Networks, Inc.

为多个 BGP 自治系统启用 ECMP....379
验证 ECMP....380
LLDP....381
LLDP 概述....382
LLDP 内支持的 TLV....383
LLDP Syslog 消息和 SNMP 陷阱....385
配置 LLDP....386
查看 LLDP 设置和状态....388
清除 LLDP 统计信息....390
BFD....391
BFD 概述....392
BFD 模式、接口和客户端支持....392
BFD 不支持的 RFC 部件....393
用于静态路由的 BFD....393
BFD 用于静态路由协议....393
配置 BFD....395
参考资料：URL 详细信息....402
会话设置和超时....407
传输层会话....408
TCP....409
“TCP 半闭合”和“TCP 等待时间”计时器....409
“未验证的 RST”计时器....410
TCP 分离握手丢弃....411
最大分段大小 (MSS)....412
UDP....414
ICMP....415
基于 ICMP 和 ICMPv6 数据包的安全策略规则....415
ICMPv6 速率限制....416
控制特定 ICMP 或 ICMPv6 类型和代码....417
配置会话超时....418
配置会话设置....420
会话分发策略....424
会话分发策略说明....424
更改会话分发策略和查看统计信息....426
阻止 TCP 分离握手会话建立....428
隧道内容检测....429
隧道内容检测概述....430

 ©2024 Palo Alto Networks, Inc.

配置隧道内容检测 433
查看已检测的隧道活动 440
查看日志中的隧道信息 441
基于标记的隧道流量创建自定义报告 442
隧道加速行为 443
禁用隧道加速 445

网络数据包代理 447
网络数据包代理概述 448
网络数据包代理的运作方式 450
准备部署网络数据包代理 452
配置透明桥接安全链 454
配置第 3 层路由安全链 458
网络数据包代理 HA 支持 463
网络数据包代理的用户界面更改 464
网络数据包代理的限制 466
对网络数据包代理进行故障排除 468

高级路由 469
启用高级路由 471
逻辑路由器概述 476
配置逻辑路由器 477
创建静态路由 481
在高级路由引擎上配置 BGP 485
创建 BGP 路由配置文件 499
为高级路由引擎创建筛选器 512
在高级路由引擎上配置 OSPFv2 532
创建 OSPF 路由配置文件 540
在高级路由引擎上配置 OSPFv3 547
创建 OSPFv3 路由配置文件 556
在高级路由引擎上配置 RIPv2 562
创建 RIPv2 路由配置文件 566
创建 BFD 配置文件 570
配置 IPv4 组播 572
配置 MSDP 580
创建多播路由配置文件 586
创建 IPv4 MRoute 589

PoE 591
PoE 概述 592

 ©2024 Palo Alto Networks, Inc.

配置 PoE.....593

 ©2024 Palo Alto Networks, Inc.

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。

- 网络简介

网络简介

网络是防火墙的基本构建块，因为它们必须能够接收、处理和转发数据。在防火墙上配置以太网端口时，可以选择 Tap、Virtual Wire、第 2 层、第 3 层或 AE 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。

要开始使用网络，您应该首先访问 PAN-OS® 管理员指南中的入门主题。您可在其中了解如何对网络进行分段以及 Configure Interfaces and Zones（配置接口和区域）；该初始任务说明了如何配置第 3 层接口以连接到互联网、内部网络和数据中心应用程序。

本 PAN-OS 网络管理员指南详细介绍了有关如何配置 Tap、Virtual Wire、第 2 层、第 3 层和 AE 接口等主题的信息。网络接口配置完成后，可以以 PDF 或 CSV 格式 Export Configuration Table Data（导出配置表数据），以进行内部审查或审核。

本指南还说明了防火墙如何支持多个虚拟路由器获取通往其他子网的第 3 层路由并维护单独的路由集。其余章节介绍静态路由、动态路由协议以及支持在防火墙上使用网络的主要功能。



您可以决定启用高级路由。高级路由引擎使用逻辑路由器而不是虚拟路由器。

- 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
- DDNS
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP
- BFD
- 会话设置和超时
- 隧道内容检测

 ©2024 Palo Alto Networks, Inc.

- 网络数据包代理
- PoE

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

配置接口

Palo Alto Networks® 下一代防火墙可以同时在多个部署中运行，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。

以下主题介绍每种类型的接口部署及其配置方式、如何配置 Bonjour Reflector 以及如何使用接口管理配置文件。

- 旁接接口
- 虚拟线路接口
- 第 2 层接口
- 第 3 层接口
- 蜂窝接口
- （PAN-OS 11.0.1 以及更高版本 11.1）在子接口上配置 PPPoE 客户端
- 配置 IPv6 PPPoE 客户端
- 配置聚合接口组
- 配置用于网络分段的 Bonjour Reflector
- 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。

- Configure Log Forwarding（配置日志转发）。
- Configure Syslog Monitoring（配置 Syslog 监控）。

STEP 4 | 创建 Security Profiles（安全配置文件）以扫描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。

 ©2024 Palo Alto Networks, Inc.

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。

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 | （仅支持的防火墙）如果接口对应于防火墙上的 PoE（以太网供电）端口，则可以选择配置 PoE。

STEP 7 | **Commit**（提交）配置。

STEP 8 | 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。

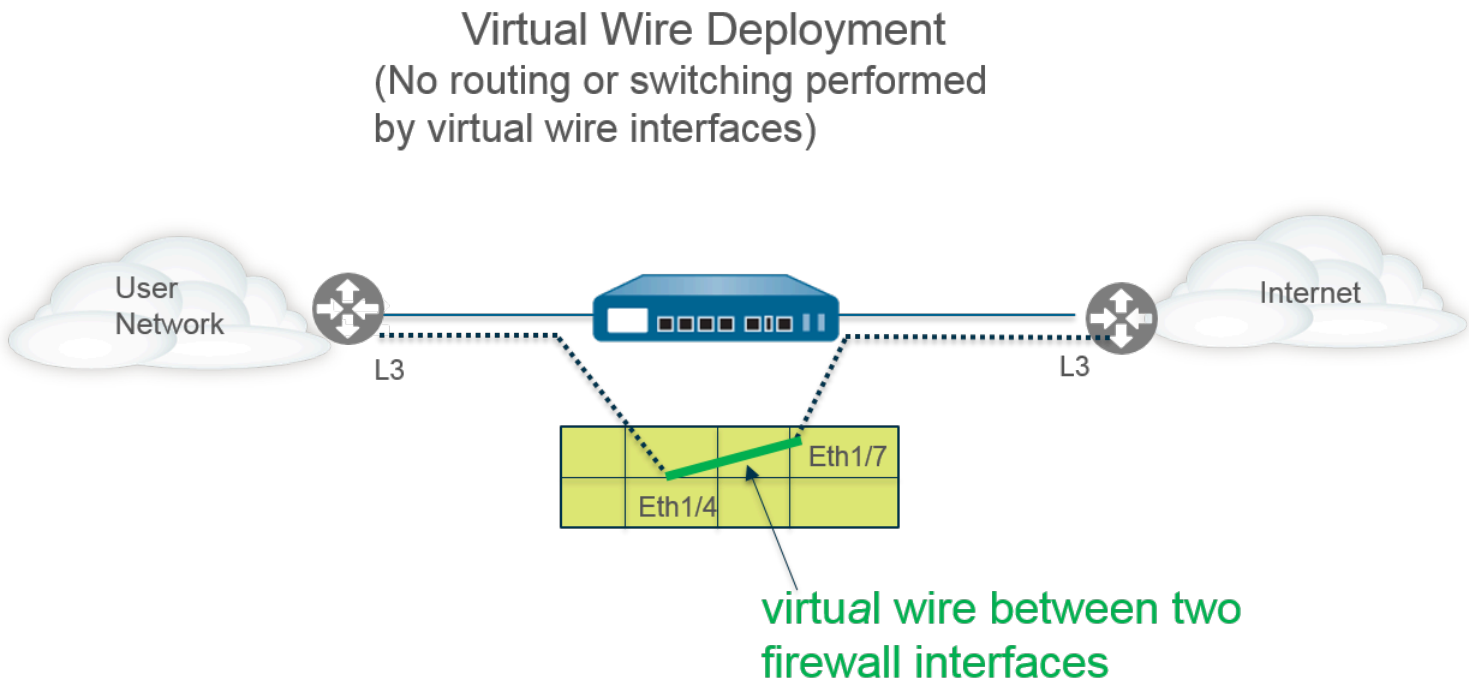
©2024 Palo Alto Networks, Inc.

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。



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。

©2024 Palo Alto Networks, Inc.

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。

©2024 Palo Alto Networks, Inc.

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。

在虚拟线上，仅当链路未在防火墙上聚合时，Palo Alto Networks 防火墙才能传递 Cisco LACP 流量。在虚拟线上，如果链路已经聚合，则防火墙可能会将数据包转发到聚合以太网中的错误端口，导致 LACP 在对等点之间无法工作。

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。

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 碎片所需数据包。

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。

©2024 Palo Alto Networks, Inc.

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。
- **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。此任务为可选任务，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）时才需要执行此任务。

您也可以使用 IP 分类器来管理无标记流量。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。

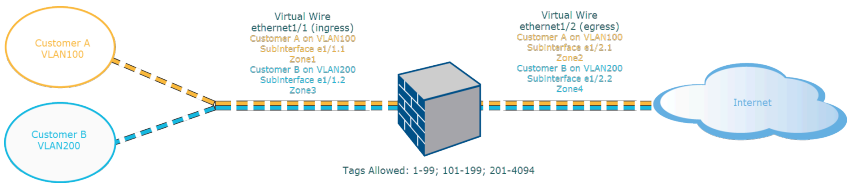


图 **1:** 子接口的 **Virtual Wire** 部署（仅适用于 **VLAN** 标记）

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。

 ©2024 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。

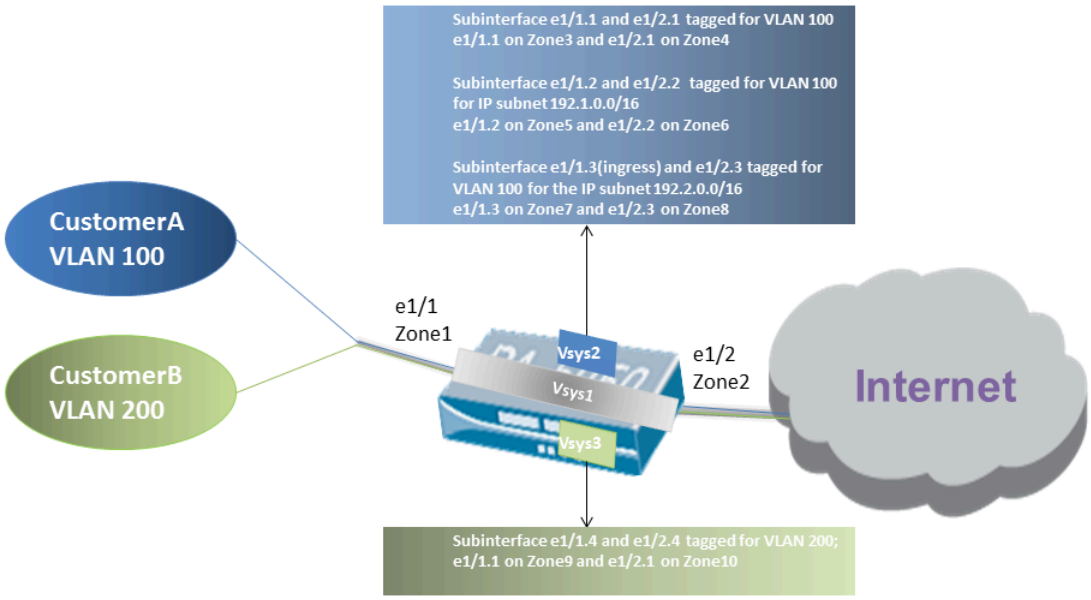


图 **2:** 子接口的 **Virtual Wire** 部署（适用于 **VLAN** 标记和 **IP** 分类器）

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。

©2024 Palo Alto Networks, Inc.

用户	Vsys	Vwire 子接口	区域	VLAN 标记	IP 分类器
A	2	e1/1.1（入口） e1/2.1（出口）	区域 3 区域 4	100 100	None
	2	e1/1.2（入口） e1/2.2（出口）	区域 5 区域 6	100 100	IP 子网 192.1.0.0/16
	2	e1/1.3（入口） e1/2.3（出口）	区域 7 区域 8	100 100	IP 子网 192.2.0.0/16
B	3	e1/1.4（入口） e1/2.4（出口）	区域 9 Zone10	200 200	None

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。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）。

©2024 Palo Alto Networks, Inc.

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。
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。

 ©2024 Palo Alto Networks, Inc.

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 | （仅支持的防火墙）如果接口对应于防火墙上的 PoE（以太网供电）端口，则可以选择配置 PoE。

STEP 9 | **Commit**（提交）更改。

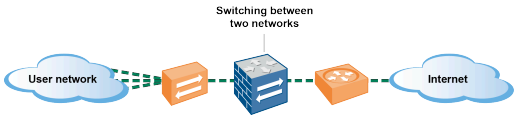
STEP 10 | （可选）配置 LLDP 配置文件并将其应用于虚拟线路接口（请参阅 配置 LLDP）。

STEP 11 | （可选）将非 IP 协议控制应用于虚拟线路区域（Configure Protocol Protection（配置协议保护））。否则，所有非 IP 流量都将通过虚拟线路转发。

©2024 Palo Alto Networks, Inc.

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

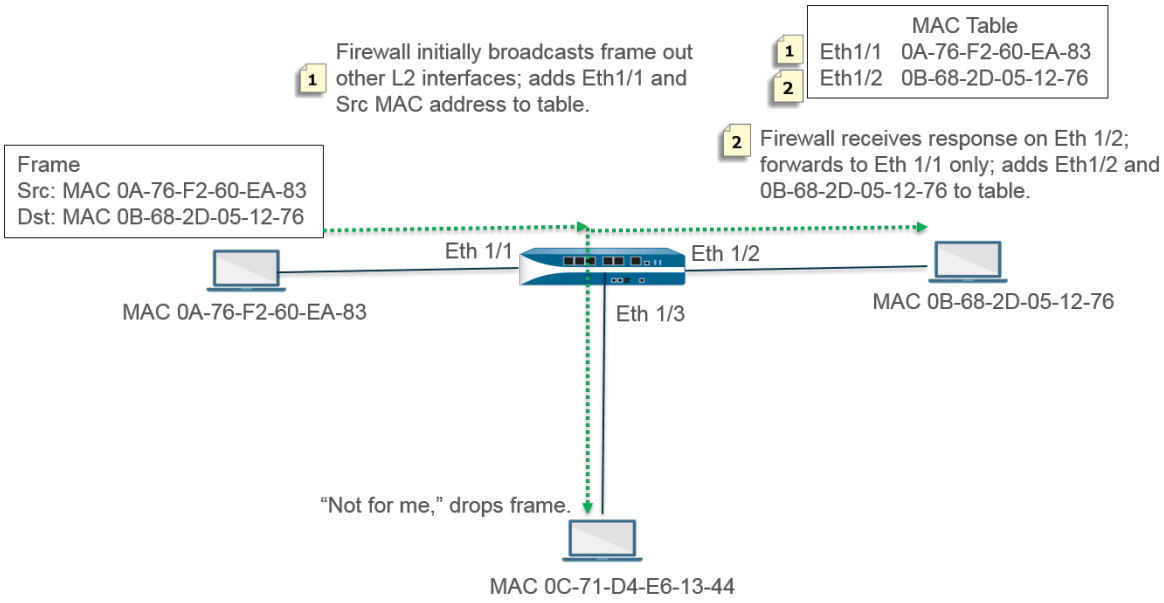
不带 VLAN 的第 2 层接口

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。

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。

©2024 Palo Alto Networks, Inc.



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。

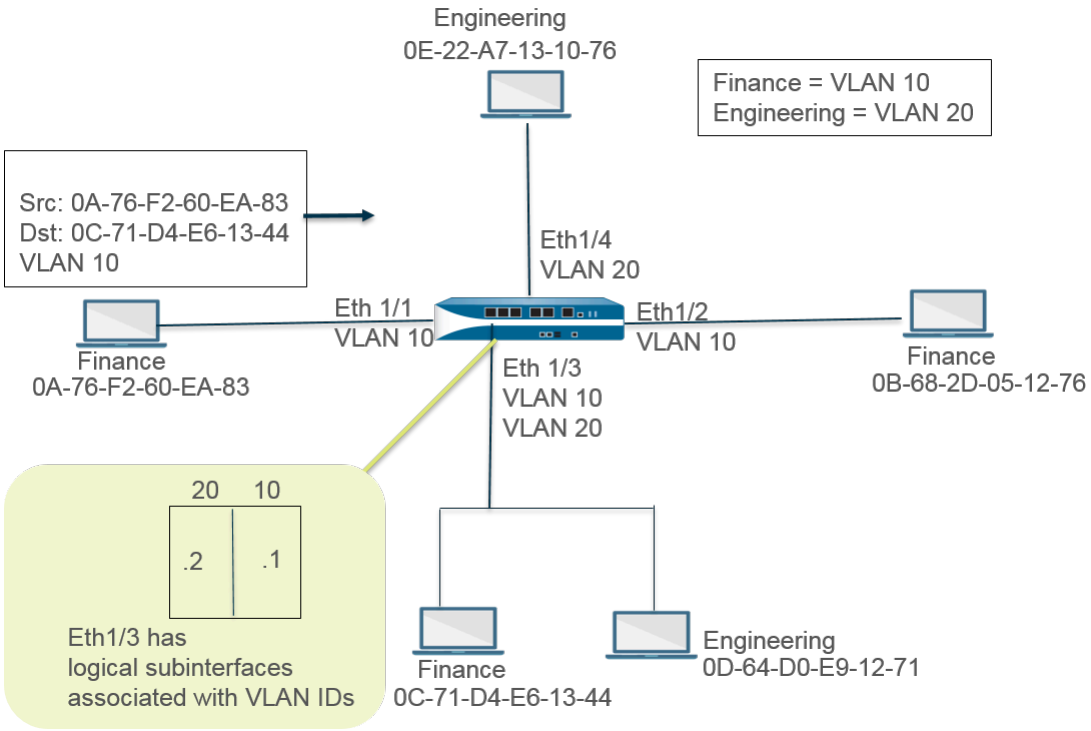
带 VLAN 的第 2 层接口

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。

 ©2024 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。

 ©2024 Palo Alto Networks, Inc.

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）。
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 至 9,999。
9. 输入 VLAN **Tag**（标记）ID，范围为 1 至 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。

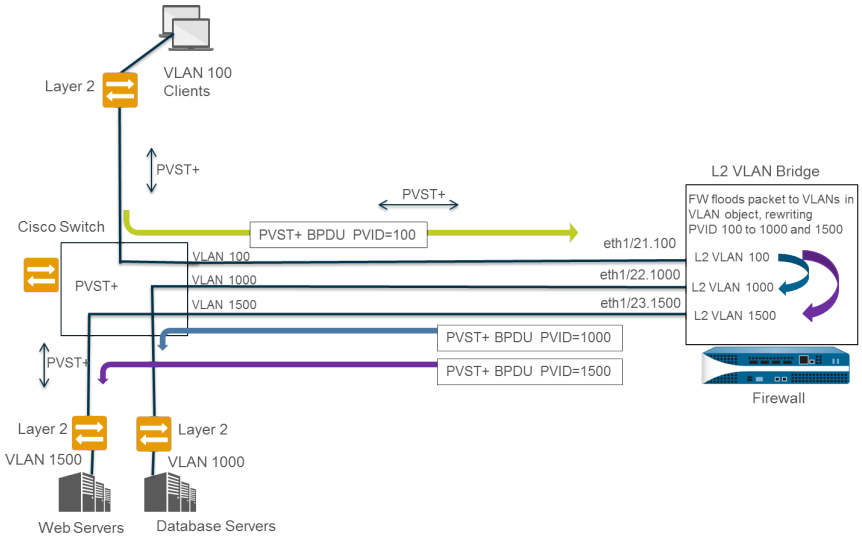
属于 VLAN_BRIDGE 的子接口如下所示：

 ©2024 Palo Alto Networks, Inc.

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

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

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>
```


©2024 Palo Alto Networks, Inc.

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。

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。

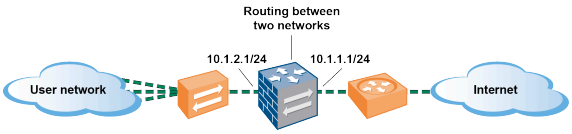
show counter global

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。

 ©2024 Palo Alto Networks, Inc.

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。在能够配置第 3 层接口之前，必须先配置希望防火墙用于为每个第 3 层接口路由流量的虚拟路由器或逻辑路由器。



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内联防火墙。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。

重复 **IP** 地址支持

从 PAN-OS® 11.1.4 及更高版本开始，当多个防火墙接口使用不同逻辑路由器时，重复（重叠）IP 地址支持允许您在多个防火墙接口上使用相同 IP 地址，还可以使用以下组合之一：

- 区域不同，虚拟系统相同。
- 区域相同，虚拟系统不同。
- 区域不同，虚拟系统不同。

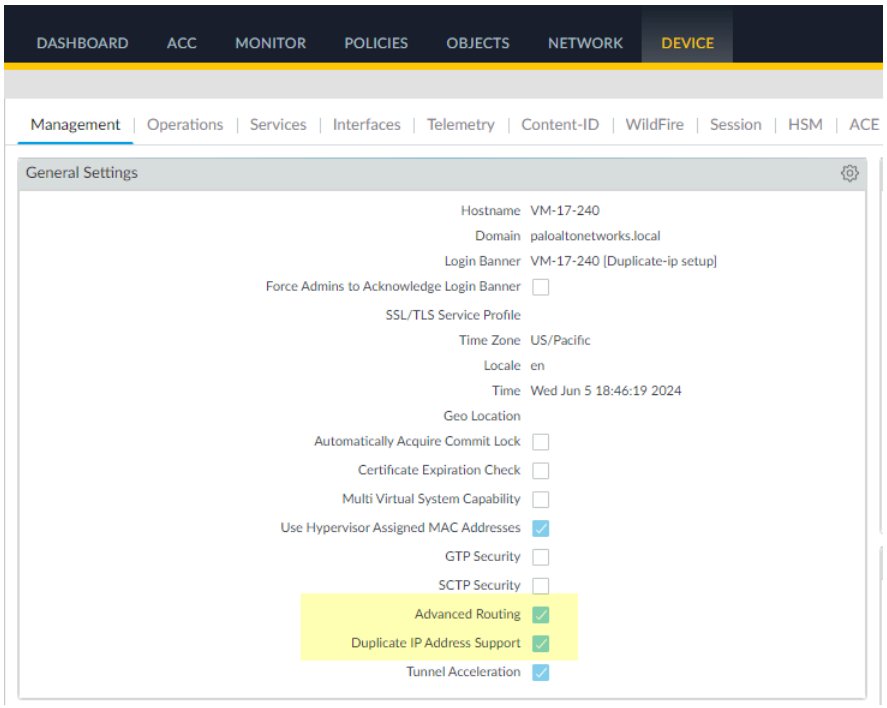
了解这些要求非常重要，因为如果您尝试在同一区域和同一虚拟系统的多个接口上配置重复地址，则不会出现提交失败的情况，这可防止配置错误。

同一个逻辑路由器上的多个接口不能使用同一个 *IP* 地址。

PA-1400 系列、VM 系列防火墙和 Panorama 模板堆栈支持重叠 IP 地址。

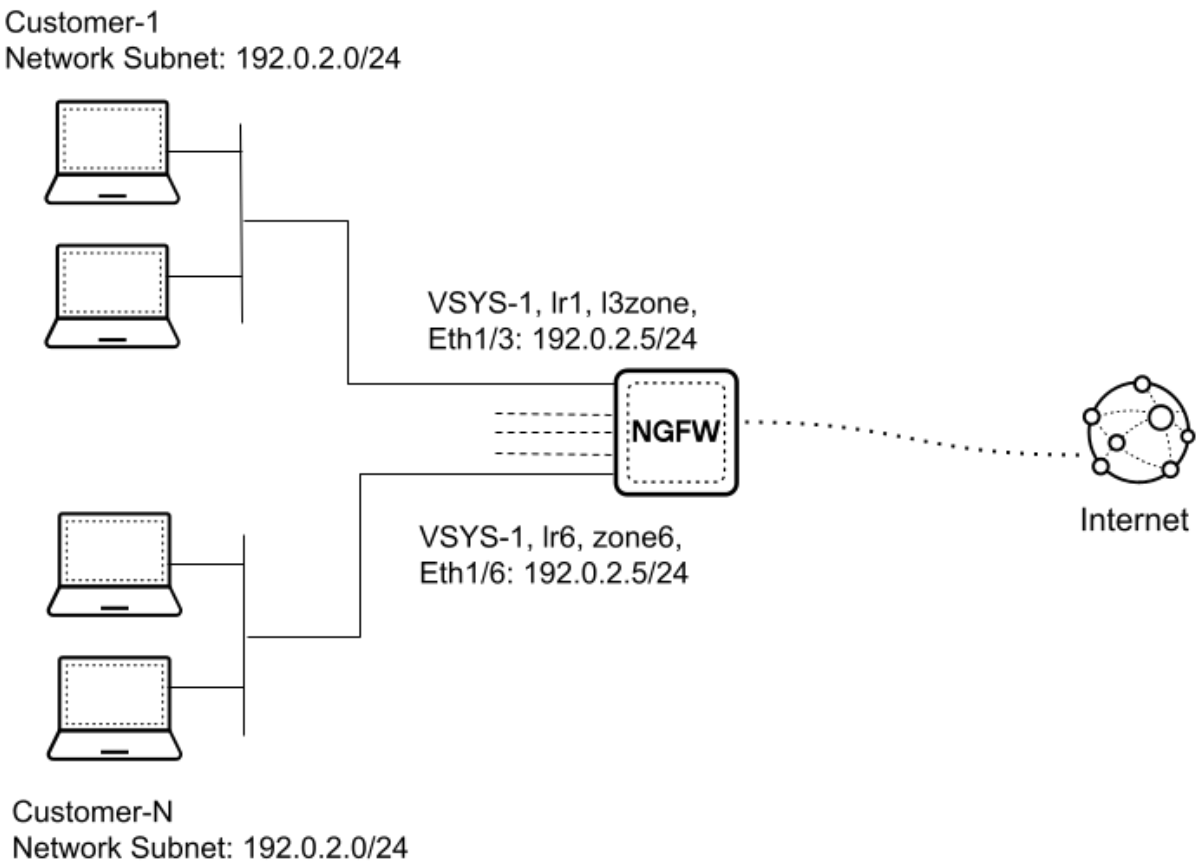
需要高级路由引擎才能支持重叠 IP 地址。启用高级路由；然后可以启用 **Duplicate IP Address Support**（重复 **IP** 地址支持）。在配置重复的 IP 地址之前，请按照标准程序提交并重新启动防火墙。

©2024 Palo Alto Networks, Inc.

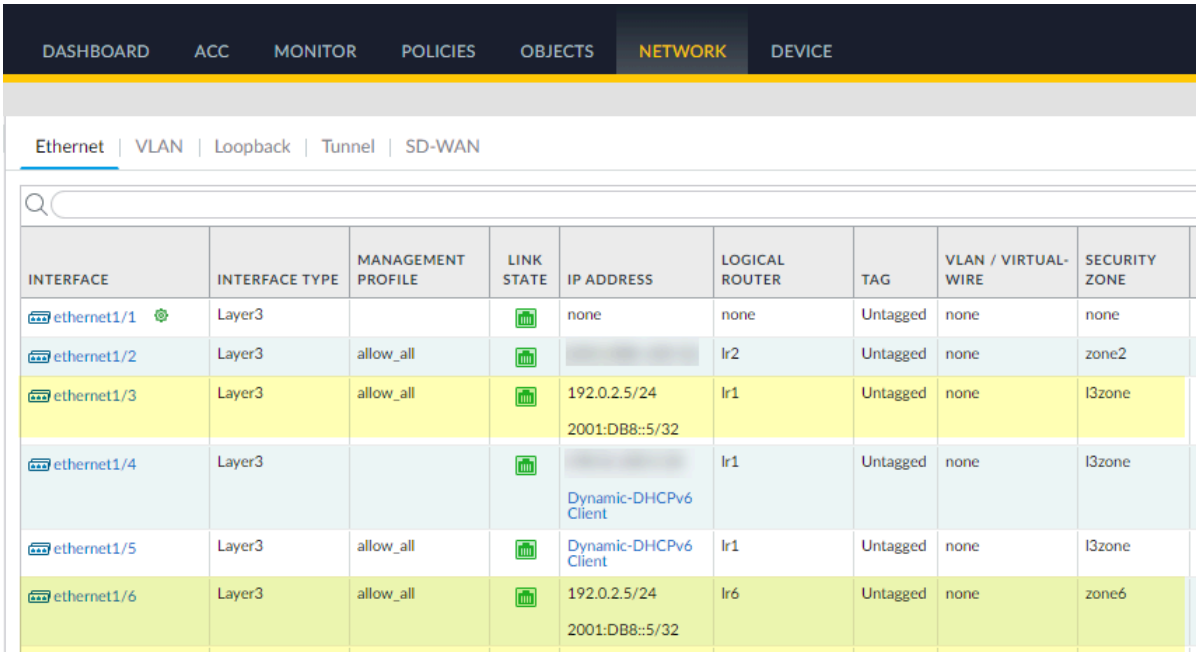


然后，您可以继续使用重复的 IP 地址配置第 3 层接口。示例拓扑说明了同一 IP 地址（192.0.2.5/24）在两个接口（Ethernet1/3 和 Ethernet 1/6）上，这两个接口属于不同逻辑路由器（lr1 和 lr6）、同一个虚拟系统 (VSYS-1) 和不同区域（l3zone 和 zone6）。

 ©2024 Palo Alto Networks, Inc.



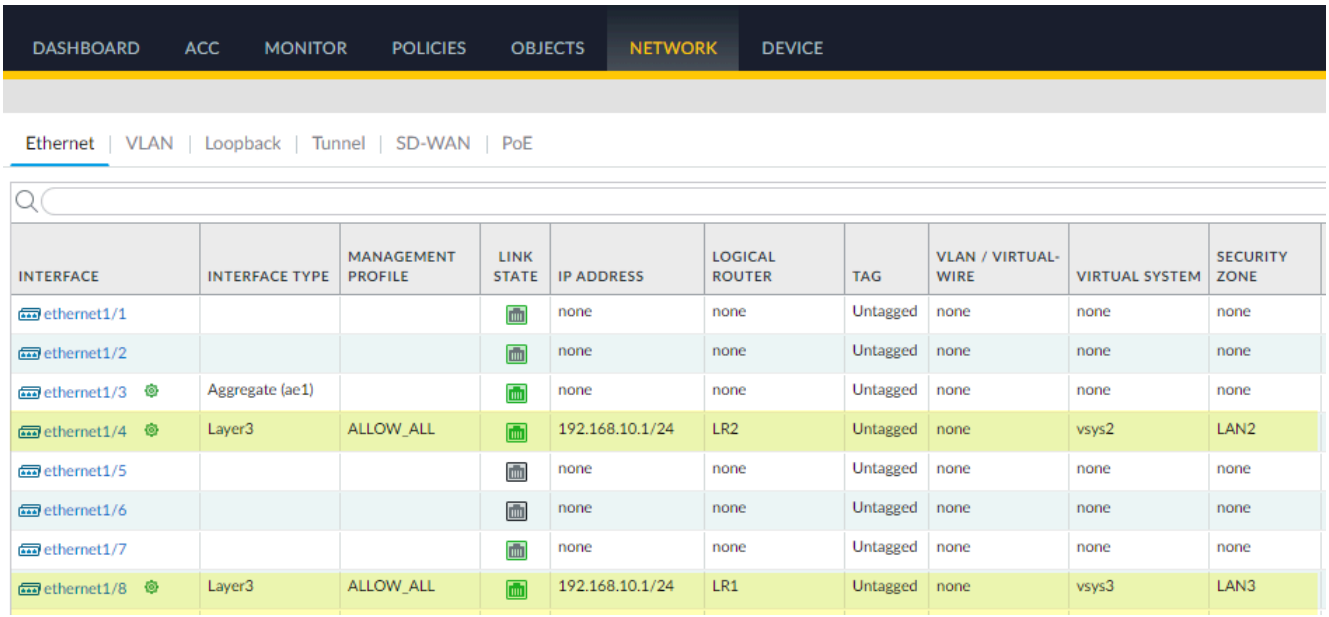
这些接口还可以共享 IPv6 地址。从示例拓扑中生成的配置示例将如下所示：



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	LOGICAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3			none	none	Untagged	none	none
ethernet1/2	Layer3	allow_all			lr2	Untagged	none	zone2
ethernet1/3	Layer3	allow_all		192.0.2.5/24 2001:DB8::5/32	lr1	Untagged	none	l3zone
ethernet1/4	Layer3			Dynamic-DHCPv6 Client	lr1	Untagged	none	l3zone
ethernet1/5	Layer3	allow_all		Dynamic-DHCPv6 Client	lr1	Untagged	none	l3zone
ethernet1/6	Layer3	allow_all		192.0.2.5/24 2001:DB8::5/32	lr6	Untagged	none	zone6

 ©2024 Palo Alto Networks, Inc.

一个单独的配置示例显示了 Ethernet1/4 和 Ethernet1/8，其中为不同的逻辑路由器、不同的虚拟系统和不同的区域配置了重叠的 IP 地址：



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	LOGICAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	VIRTUAL SYSTEM	SECURITY ZONE
ethernet1/1				none	none	Untagged	none	none	none
ethernet1/2				none	none	Untagged	none	none	none
ethernet1/3	Aggregate (ae1)			none	none	Untagged	none	none	none
ethernet1/4	Layer3	ALLOW_ALL		192.168.10.1/24	LR2	Untagged	none	vsys2	LAN2
ethernet1/5				none	none	Untagged	none	none	none
ethernet1/6				none	none	Untagged	none	none	none
ethernet1/7				none	none	Untagged	none	none	none
ethernet1/8	Layer3	ALLOW_ALL		192.168.10.1/24	LR1	Untagged	none	vsys3	LAN3

指示板上的“General Information（一般信息）”显示防火墙设置：`Duplicate IP Enabled`（重复 IP 已启用）或 `Duplicate IP Disabled`（重复 IP 已禁用）。

重叠 IP 地址支持静态和动态分配的 IPv4 和 IPv6 地址。所有第 3 层接口类型（以太网、VLAN、隧道、环回、聚合以太网 [AE] 和 AE 子接口）都支持重叠 IP 地址。支持包括网关接口。

管理接口不支持重叠 *IP* 地址。

配置了重复 IP 地址的接口支持以下服务：Ping、SSH、Telnet、HTTP 和 HTTPS。启用“Duplicate IP Address Support（重复 IP 地址支持）”后，ping 和 traceroute 命令要求您指定逻辑路由器，以区分重复地址中的源 IP 地址。因此，响应返回到正确的 IP 地址。使用 CLI 操作命令：

- **`ping source ip host ip logical-router logical-router-name`**
- **`traceroute source ip host ip logical-router logical-router-name`**

您可以通过具有重叠 IP 地址的接口来访问接口管理配置文件服务。

Inter-vSys 路由支持重叠 IP 地址，因此您可以在虚拟系统之间进行路由。

与重复 IP 地址支持相关的其他 CLI 命令包括：

- **`set deviceconfig setting duplicate-ip <yes|no>`**

  启用或禁用重复 IP 地址支持。
- **`show system info`**

  查看“Duplicate IP（重复 IP）”设置（Enabled（已启用）或 Disabled（已禁用））。
- **`show counter global name session_duplicate_ip_alt_srcnat_xlat`**

  查看重复 IP 替代源 NAT 转换的计数器。

©2024 Palo Alto Networks, Inc.

下面链接的第一个主题描述了如何配置第 3 层接口。后一个主题链接介绍如何使用邻居发现协议 (NDP) 配置 IPv6 主机，以及查看本地链路网络上设备的 IPv6 地址以快速定位设备。

- 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。在执行以下任务之前，请在旧版路由引擎上定义一个或多个虚拟路由器，或在高级路由引擎上定义逻辑路由器。

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。

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。单个第 *3* 层接口支持多个静态 *IPv4* 和静态 *IPv6* 地址。在任何给定时间，第 *3* 层接口类型可以是静态 *IPv4*、*DHCPv4* 或 *PPPoEv4*。在任何给定时间，第 *3* 层接口类型可以是静态 *IPv6*、*DHCPv6* 或继承。

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。

从 PAN-OS 11.1.4 开始，您可以在高级路由引擎的第 3 层接口上配置重复（重叠）IP 地址。前提条件是您首先启用高级路由。如果您需要重复（重叠）IP 地址，请先了解这些地址，然后再根据以下过程来启用。

STEP 1 | （PAN-OS 11.1.4 及更高版本）（可选）启用重叠 IP 地址。

1. 选择 **Device**（设备） > **Setup**（设置） > **Management**（管理），然后编辑“General Settings（常规设置）”。
2. 选择 **Duplicate IP Address Support**（重复 **IP** 地址支持）。
3. **Commit**（提交）更改。

STEP 2 | 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）。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 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 Client**（**DHCP** 客户端） -— 防火墙接口充当 DHCP 客户端，并接收动态分配的 IPv4 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）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 将接口配置为 PPPoE 终止点。

PPPoE 在 *HA* 主动/主动模式下不受支持。

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 5 | 将接口配置为 DHCPv4 客户端，以便可以接收动态分配的 IPv4 地址。

在 *HA* 主动/主动模式下不支持 *DHCP* 客户端。

STEP 6 | 将接口配置为 DHCPv6 客户端（使用或不使用前缀委派），使其接收动态分配的 IPv6 地址。

在 *HA* 主动/主动模式下不支持 *DHCPv6* 客户端。

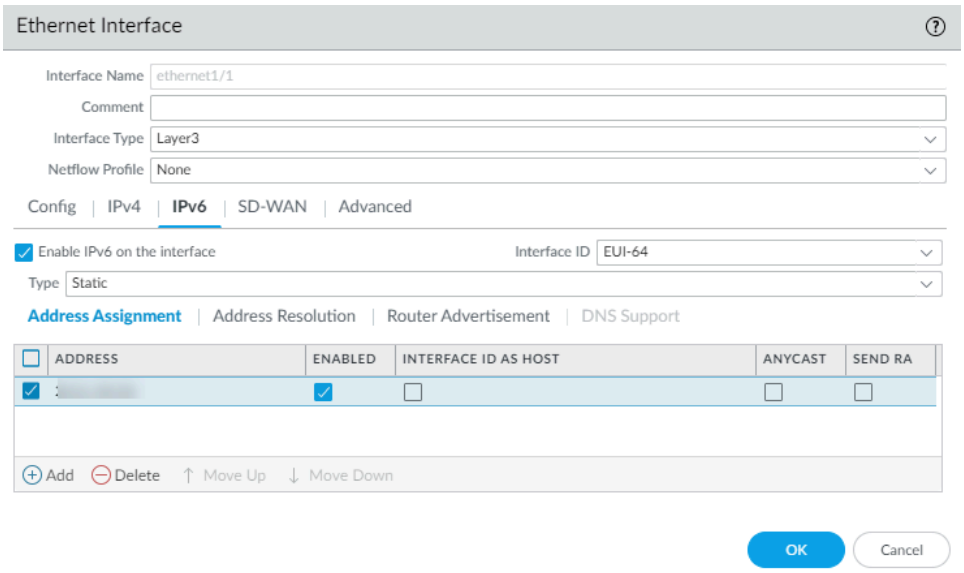
STEP 7 | 配置带静态 IPv6 地址的接口。

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**

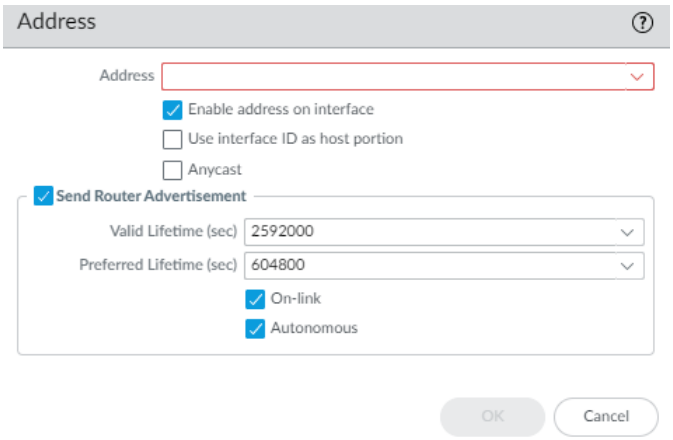
 ©2024 Palo Alto Networks, Inc.

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. 选择**Address Assignment**（地址分配）并**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。



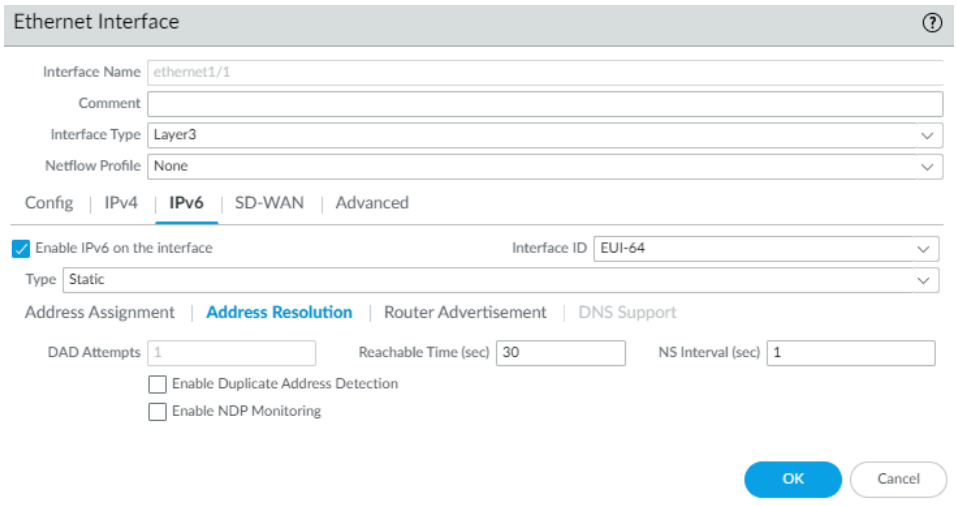
9. （仅限以太网接口）选择 **Send Router Advertisement**（发送路由器通告）(RA)，使防火墙能够在路由器通告中发送该地址，在这种情况下，您还必须在接口上启用全局 **Enable Router Advertisement**（启用路由器通告）（下一步）。
10. （仅限以太网接口）以秒输入防火墙认为该地址有效的 **Valid Lifetime (sec)**（有效生存时间（秒））。有效生命周期必须等于或超过 **Preferred Lifetime(sec)**（首选生存时间（秒））（默认为 2,592,000）。

 ©2024 Palo Alto Networks, Inc.

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 8 | 对于静态 IPv6 接口，配置地址解析。

1. 选择 **Address Resolution**（地址解析）。
2. 如果您希望在将 IPv6 地址分配给接口之前验证该地址的唯一性，请 **Enable Duplicate Address Detection**（启用重复地址检测）(DAD)（默认为启用）。
3. 如果选择了 **Enable Duplicate Address Detection**（启用重复地址检测），请指定尝试识别邻居失败之前在邻居请求 (NS) 间隔内进行 **DAD Attempts**（**DAD** 尝试）的次数；范围为 0 到 10；默认值为 1。
4. 输入**Reachable Time (sec)**（可达时间（秒）），即客户端在收到可达确认消息后假设邻居达到的时间长度；范围为 10 到 36,000；默认值为 30。
5. 输入 **NS Interval (sec)**（**NS** 间隔（秒））（邻居请求间隔），邻居请求之间的时间长度；范围为 1 到 3,600；默认值为 1。
6. **Enable NDP Monitoring**（启用 **NDP** 监控）以启用邻居发现协议监控。启用后，您可以选择 NDP 图标（功能列中的 ）并查看信息，如防火墙发现的邻近对象的 IPv6 地址、相应的 MAC 地址和 User-ID（在最佳情况下）。



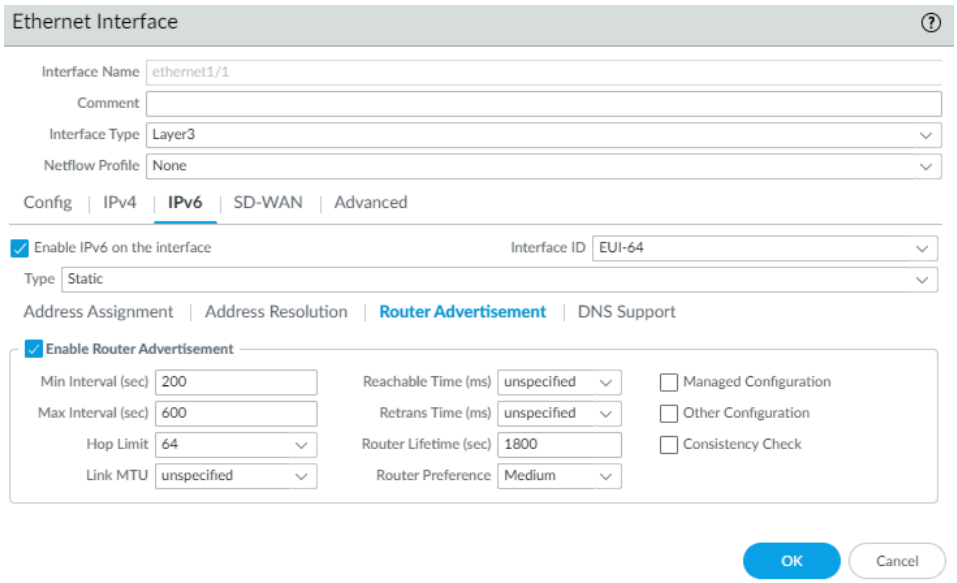
7. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | （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）。

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 1,280-1,500；默认为 **unspecified**（未指定））。为无链路 MTU 选择 **unspecified**（未指定）。
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））。

 ©2024 Palo Alto Networks, Inc.

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）。

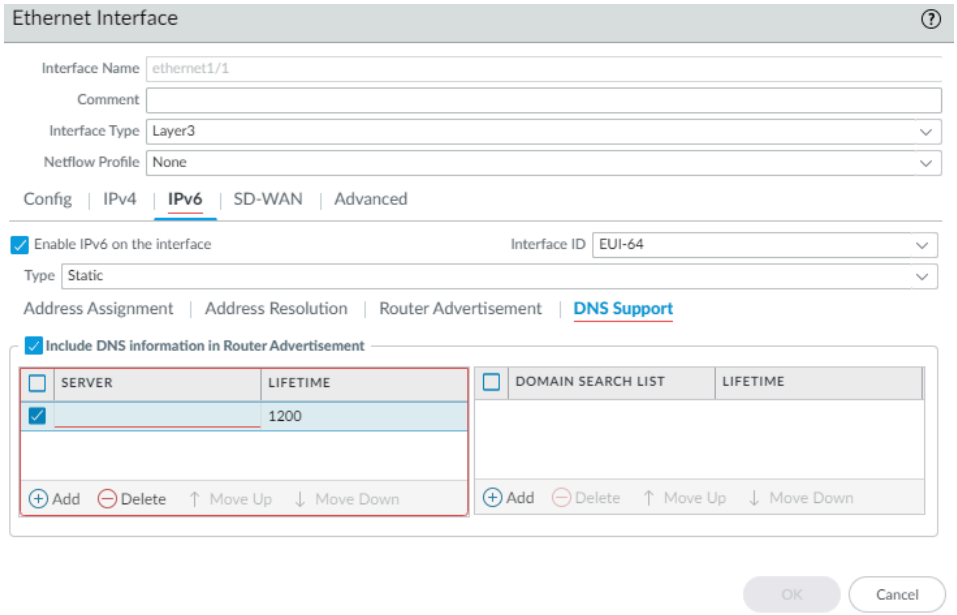
 ©2024 Palo Alto Networks, Inc.

STEP 10 | （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。

必须在 ***Router Advertisement***（路由器通告）选项卡上选择 ***Enable Router Advertisement***（启用路由器通告），才能使 *DNS* 支持选项卡可用。

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。
5. 对于 DNS **Server**（服务器），**Add**（添加）递归 DNS 服务器的 IPv6 地址（最多添加八台服务器）。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. **Add**（添加）**Domain Search List**（域搜索列表）（域名最大 255 字节）。最多添加八个条目。防火墙按自上而下的顺序在 ICMPv6 路由器通告中发送域。
8. 以秒为单位指定 **Lifetime**（生存时间），这是客户端可以使用列表的最长秒数。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）。

 ©2024 Palo Alto Networks, Inc.

STEP 11 | （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。
5. 单击 **OK**（确定）。

STEP 12 | （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 13 | （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 14 | **Commit**（提交）更改。

STEP 15 | 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 16 | 验证接口是否处于活动状态。

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 17 | 配置静态路由和/或动态路由协议，以便虚拟路由器或逻辑路由器可以路由流量。

 ©2024 Palo Alto Networks, Inc.

STEP 18 | 配置默认路由。

为虚拟路由器或创建静态路由逻辑路由器配置静态路由，并将其设置为默认路由。

STEP 19 | （仅支持的防火墙）如果接口对应于防火墙上的 PoE（以太网供电）端口，则可以选择配置 PoE。

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：

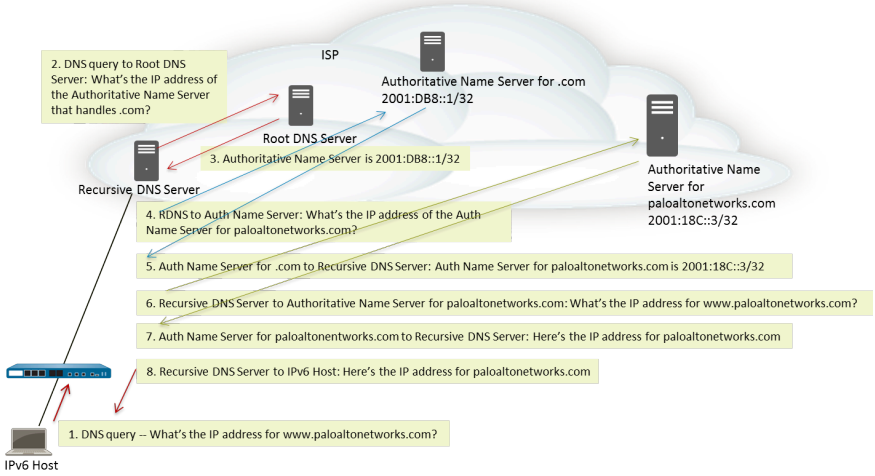
- 可以解析 DNS 查询的 RDNS 服务器地址。
- 在将域名输入 DNS 查询之前，DNS 客户端（一次一个）将其添加到一个非限定域名的域名列表（后缀）。

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。

 ©2024 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）。

 ©2024 Palo Alto Networks, Inc.

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。
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。

 ©2024 Palo Alto Networks, Inc.

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。

单击 **Commit**（提交）。

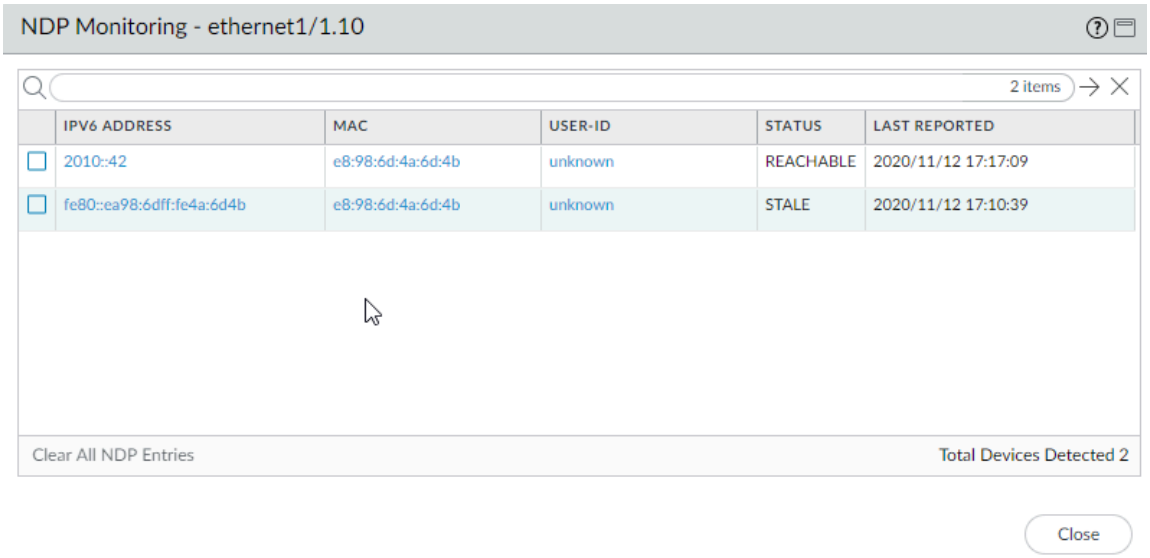
 ©2024 Palo Alto Networks, Inc.

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。

©2024 Palo Alto Networks, Inc.

蜂窝接口

PA-415-5G 平台上提供了 5G 蜂窝接口。该接口可让您提供互联网主连接，或者在主连接不可用时配置辅助连接以实现冗余。该接口使用 5G 移动网络提供数据连接，如果 5G 网络不可用，则会自动切换到 4G 或 3G 网络。您还可以配置 5G 接口以使用加权循环实现负载平衡。使用指示板小部件可轻松监控 5G 网络状态信息。

可以配置主 SIM 卡和副 SIM 卡（如果可用）。如果您有副 SIM 卡，则可以将防火墙配置为在一张 SIM 卡不可用时切换到另一张 SIM 卡。为安全起见，请为 SIM 卡启用 PIN 码，以防止滥用。

当运营商提供新功能更新并解决问题时，您可以从客户支持门户下载蜂窝固件升级并将固件升级安装在防火墙上。这让防火墙内能够将更新推送给网络上的适当用户。界面简洁，您可以轻松查看、管理和部署 5G 网络上的蜂窝固件更新。保持蜂窝固件最新不仅能够获得新的特性和能力，还有助于保护您的用户免受威胁和漏洞的侵害。

以下主题提供了有关配置 5G 网络接口以及如何升级 5G 接口上的蜂窝固件的指导。

- 为蜂窝接口配置 5G
- 升级 5G 固件

为蜂窝接口配置 5G

可以使用包含集成 5G 模块的 PA-415-5G 来实现 4G/5G 功能。这种配置通过蜂窝接口为互联网主连接或作为链路的冗余提供了一个接口。

5G 模块需要 *PAN-OS 11.1* 或更高版本。

配置 5G 蜂窝接口后，便可使用 5G 移动网络提供数据连接。如果 5G 网络不可用，防火墙会自动切换到 4G 或 3G 网络。

初始化时，调制解调器处于活动状态，默认情况下未启用无线电选项。如果有一个或多个 SIM 卡可用，并且您启用了无线电选项，防火墙在尝试建立数据包会话会使用您在 APN 配置文件中为主 SIM 卡槽配置的 SIM 卡。

如果没有自定义 *APN* 配置文件，防火墙将使用 ***auto*** *APN* 配置文件。

要升级 5G 固件，请从客户支持门户下载固件更新并将其安装在防火墙上。

5G 蜂窝接口支持以下功能：

- 路由（包括 BGP、BFD 和静态路由）

  5G 蜂窝接口支持带加权循环的负载平衡。传统路由堆栈不支持动态 *IP* 接口上的 *BGP*；作为替代措施，请使用环回接口。
- IPv4
- 第 3 层接口
- 第 2 层封装

 ©2024 Palo Alto Networks, Inc.

- 隧道和 VPN（包括 IKE、IPSec 和 GRE）

  5G 蜂窝接口使用环回接口支持 GRE。

- NAT
- PBF

  5G 蜂窝接口不支持对称返回。

- 区域和区域保护配置文件
- DoS 保护策略
- 隧道检测
- 使用环回接口的服务路由
- HA 主动/被动（不支持会话同步和会话连续性）

5G 蜂窝接口不支持以下功能：

- IPv6
- ECMP
- 多 vsys
- HA 主动/主动
- 巨型帧
- OSPF
- 组播或 ACL 卸载

STEP 1 | 创建接入点名称 (APN) 配置文件。

您必须正确配置 APN 配置文件才能访问互联网。APN 配置文件定义了允许设备访问的一个或多个网络，并确定设备接收的是动态 IP 地址还是静态 IP 地址。为允许访问数据服务，除了网络运营商的 APN 配置文件外，一些移动虚拟网络运营商 (MVNO) 还需要一个单独的 APN 配置文件。根据运营商，您可能还需要启用额外的安全措施，将 APN 限制为经过身份验证的用户。

STEP 2 | 使用动态 IP 地址配置动态 NAT 安全策略规则，以允许 5G 流量。

©2024 Palo Alto Networks, Inc.

STEP 3 | 配置蜂窝接口。

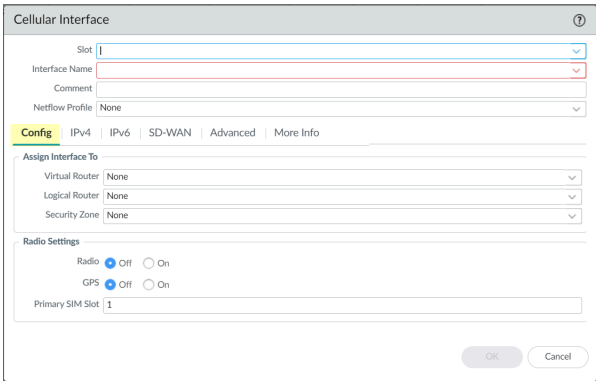
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Cellular**（蜂窝）。

   对于 Panorama，选择 **Network**（网络）。选择要使用的模板，然后选择 **Interfaces**（接口） > **Cellular**（蜂窝）。您可以使用模板为设备添加配置，然后将该模板应用到其他设备。
2. （仅限 Panorama）选择 **Slot**（插槽）。

   为非机箱型号选择 **Slot 1**（插槽 **1**）。
3. 选择 **Interface Name**（接口名称），以选择要使用的接口名称。
4. （可选）在 **Comment**（注释）中输入内容，以描述接口。
5. 选择 **Netflow Profile**（**Netflow** 配置文件），或选择 **New Netflow Profile**（新建 **Netflow** 配置文件）以新建一个配置文件。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 配置 5G 连接。



1. 在 **Config**（配置）选项卡中，选择 **Virtual Router**（虚拟路由器），即要分配接口的虚拟路由器，或选择 **New Virtual Router**（新建虚拟路由器）以新建一个虚拟路由器.
2. 选择 **Logical Router**（逻辑路由器），即要分配接口的逻辑路由器，或选择 **New Logical Router**（新建逻辑路由器）以新建一个逻辑路由器。
3. 选择 **Security Zone**（安全区）以选择安全区，或选择 **New Zone**（新建区域）以新建一个安全区。
4. 选择调制解调器的 **Radio**（无线电）设置。

   此选项可让您在故障排除期间重置无线电设置。

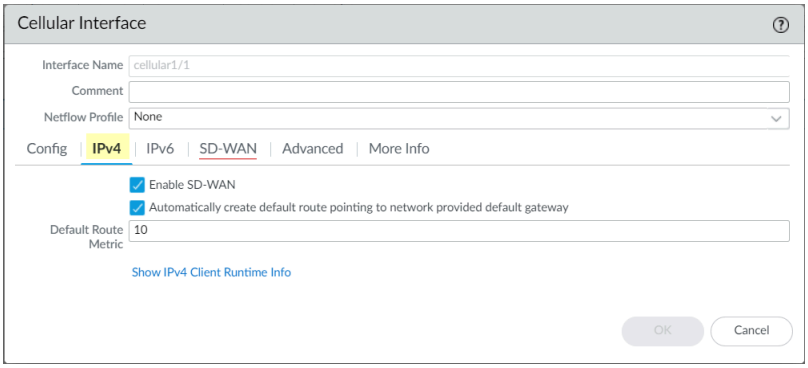
   要启用 *GPS* 选项，必须同时启用 ***Radio***（无线电）选项和 ***GPS*** 选项。

   - **Off**（关闭）—（默认值）禁用无线电设置和蜂窝接口。
   - **On**（开启）—启用无线电设置和蜂窝接口。
5. 选择 **GPS** 设置。
   - **Off**（关闭）—（默认值）禁用 GPS 设置。
   - **On**（开启）—启用 GPS 设置。
6. 选择 **Primary SIM Slot**（主 **SIM** 插槽）。

   默认情况下，防火墙使用插槽 1 (SIM1) 中的卡来尝试与网络连接。如果您配置了第二个 SIM 插槽，那么在使用主 SIM 连接不成功的情况下，防火墙将自动尝试使用副 SIM 与网络连接。可以选择将第二个插槽 (SIM2) 配置为 **Primary SIM Slot**（主 **SIM** 插槽）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 配置 IPv4 设置。



1. （可选）（PAN-OS 11.2.3 及更高版本 11.2，SD-WAN 插件 3.3.1 及更高版本 3.3 版本）在 **IPv4** 选项卡上，选择 **Enable SD-WAN**（启用 **SD-WAN**）以在蜂窝接口上启用 SD-WAN。如果蜂窝接口启用了 SD-WAN，则系统会自动将其添加为 DIA SD-WAN VIF 成员；系统将创建隧道并自动将隧道添加到 SD-WAN 隧道 VIF。系统会在 5G 分支或 5G 集线器设备与对等设备之间创建隧道，接口名称以“cellular”结尾。

   在蜂窝接口中启用 SD-WAN 后，您的蜂窝接口将支持所有 SD-WAN 功能。

   - 无法在两个蜂窝接口之间建立 *SD-WAN* 隧道。
   - 在蜂窝接口中启用 *SD-WAN* 时，不支持全网状拓扑。
   - 我们建议您最好是将启用 *5G* 的防火墙配置为分支设备。如果您尚未在防火墙上启用 *SD-WAN* 功能，则只能将该 *4G/5G* 防火墙配置为集线器设备。请注意，*VPN* 群集中只能有一个 *4G/5G* 集线器设备。
   - 对于互联网服务提供商之间的网关 *ping* 值，并没有现成的标准。由于蜂窝接口不允许对网关执行本机 *ICMP ping* 操作。因此，我们建议您配置 *SaaS* 配置文件，而不是 *ICMP* 配置文件。

   以下防火墙在蜂窝接口中支持 SD-WAN 配置：

   - PA-415-5G
   - PA-450R-5G
   - PA-415R-5G
   - PA-455-5G
   - PA-455R-5G

2. 在 **IPv4** 选项卡上，根据需要选择 **Automatically create default route pointing to network provided default gateway**（自动创建指向默认网关所提供的网络的默认路由）。

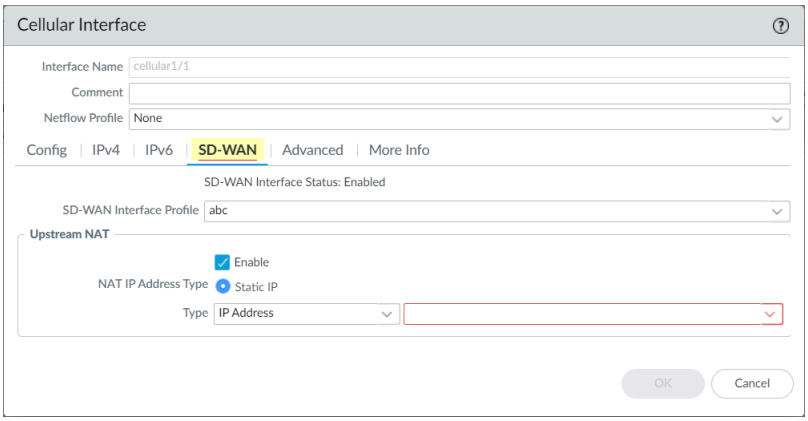
   默认启用此选项，并创建指向网络所提供默认网关的默认路由。

3. 指定 **Default Route Metric**（默认路由指标）。

   默认为 10；范围为 1 到 65535。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | （可选）（PAN-OS 11.2.3 及更高版本 11.2，SD-WAN 插件 3.3.1 及更高版本 3.3 版本）配置 SD-WAN 设置。



只有在 **IPv4** 选项卡中启用了 SD-WAN 时，才能配置 **SD-WAN** 设置。

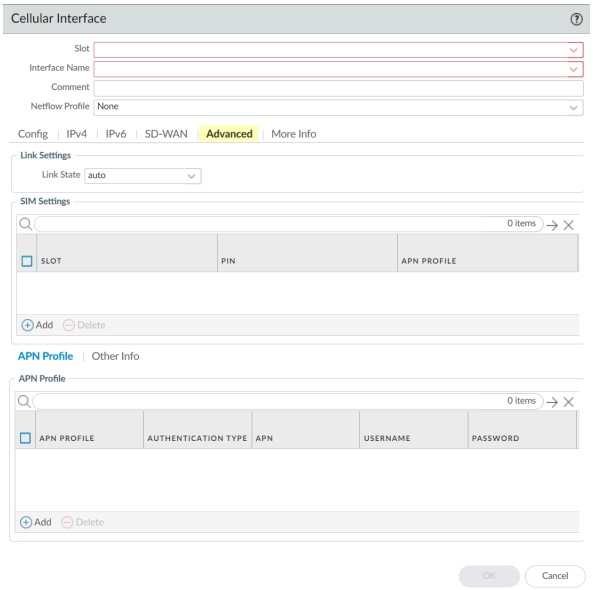
如果要在为分支执行 NAT 的设备后面添加一个分支，则必须指定该上游 NAT 执行设备上面向公众的接口的 IP 地址或 FQDN，或者选择 DDNS 以指示 NAT 设备上接口的 IP 地址是 从 Palo Alto Networks DDNS 服务中获得的。因此，自动 VPN 配置使用该公共 IP 地址作为分支的隧道端点。分支机构的 IKE 和 IPSec 流必须可以抵达该 IP 地址。（您必须已经 为 SD-WAN 配置一个物理以太网接口。）

1. 选择已配置的 SD-WAN 接口配置文件或创建新 SD-WAN 接口配置文件。
2. 在 **Upstream NAT**（上游 **NAT**）中，启用 **Upstream NAT**（上游 **NAT**）。
3. 如果选择 **NAT IP Address Type**（**NAT IP** 地址类型）为 **Static IP**（静态 **IP**），请选择 **IP Address**（**IP** 地址）或 **FQDN**，然后分别输入不带子网掩码的 IPv4 地址（例如，192.168.3.4），或是上游设备的 FQDN。

©2024 Palo Alto Networks, Inc.

STEP 7 | 在 **Advanced**（高级）选项卡上，选择 **Link State**（链路状态）。

- **auto**（自动）—该接口仅在存在对等连接时才可用。
- **up**（运行）—接口可用。
- **down**（关闭）—接口不可用。

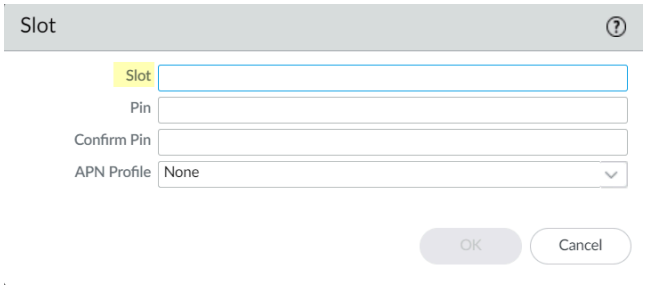


 ©2024 Palo Alto Networks, Inc.

STEP 8 | 配置 SIM 设置。

1. 依次选择 **Add**（添加）、**SIM Settings**（**SIM** 设置）。
2. 指定 **Slot**（插槽）。

   在同一时间，只能有一个 SIM 插槽处于有效状态。默认情况下，有效 SIM 插槽是 `SIM1`。调制解调器使用此 SIM 搜索网络连接。如果防火墙在 5 分钟内无法建立会话，则会尝试使用备用 SIM 插槽建立会话。



3. 若系统要求输入 PIN 以防止未经授权使用 SIM 插槽，请输入 **Pin**，然后按 **Confirm Pin**（确认 **PIN**）。

   您也可以要求输入 *PIN* 才能访问 *SIM*；有关详细信息，请参阅步骤 17。

4. 选择 **APN Profile**（**APN**配置文件）。

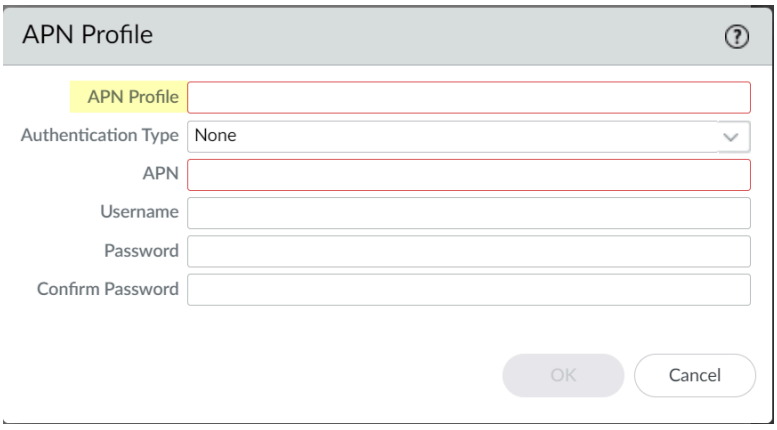
   指定您希望 SIM 卡默认使用的 APN 配置文件。SIM 插槽使用此 APN 配置文件，除非您用自定义 APN 配置文件将其覆盖。如果未指定 APN 配置文件，防火墙将使用默认 APN 配置文件 `auto`。如果需要指定自定义 APN 配置文件，可以在步骤 9.a 中指定

5. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 定义 **APN**配置文件。

1. 添加默认的 **APN** 配置文件。
   如有必要，可通过选择 APN 配置文件来覆盖指定插槽的默认 APN 配置文件。

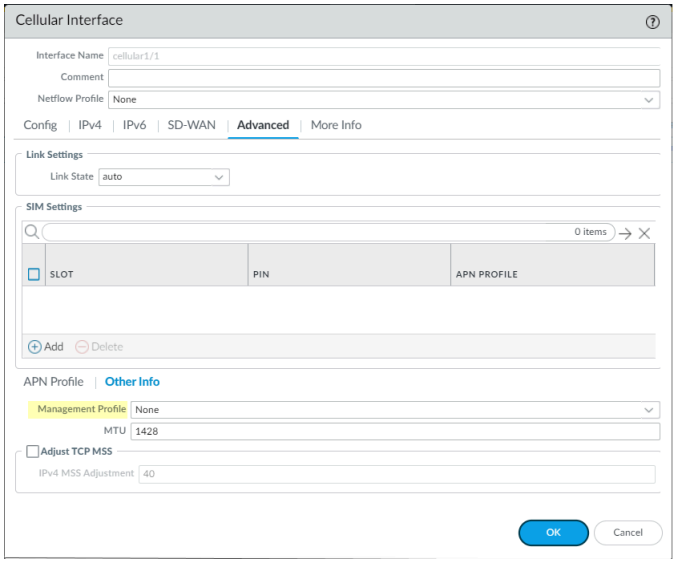


2. 为 APN 连接选择 **Authentication Type**（身份验证类型）。
   - **None**（无）—（默认设置）防火墙不需要对 APN 连接进行身份验证。
   - **CHAP**—使用质询握手身份验证协议 (CHAP) 连接到 APN。
   - **PAP**—使用密码身份验证协议 (PAP) 连接到 APN。
   - **auto**（自动）—允许防火墙根据服务提供商自动检测身份验证类型。如果与初始身份验证类型的连接不成功，防火墙将尝试使用备用身份验证类型进行连接。
3. 在 **APN** 中输入 APN。
4. 在 **Username**（用户名） 中输入用户名。
5. 在 **Password**（密码）中输入密码，然后单击 **Confirm Password**（确认密码）。
6. 单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

STEP 10 | 根据您的网络要求配置其他信息，如最大传输单元 (MTU)。

1. 选择 **Other Info**（其他信息）选项卡。
2. 选择 **Management Profile**（管理配置文件）。



3. 以字节为单位指定 **MTU**。

   默认值为 1428 个字节；范围为 576 至 1500 个字节。
4. 如果要因延迟而调整数据包大小，可以选择 **Adjust TCP MSS**（调整 **TCP MSS**）以配置最大段大小并指定 **IPv4 MSS Adjustment**（**IPv4 MSS** 调整）值。

   默认为 40；范围为 40 到 300。
5. 单击 **OK**（确定）。

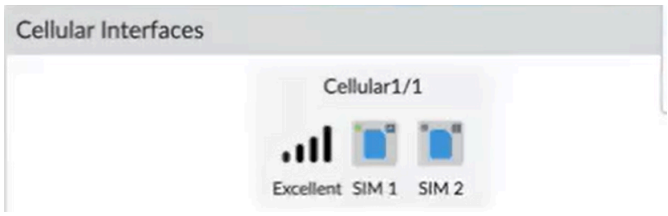
STEP 11 | **Commit**（提交）更改。

您必须提交您的更改，确保接口已启用且连接成功，然后才能在防火墙或 Panorama 上获得以下信息。

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 使用小部件监视您的蜂窝接口。

1. 选择 **Dashboard**（指示板） > **Widgets**（小部件） > **System**（系统） > **Cellular Interfaces**（蜂窝接口）。
2. 查看有关蜂窝接口的信息，如信号强度。要查看更多信息，请将鼠标悬停在图标上。



3. 选择 **Dashboard**（指示板） > **Widgets**（小部件） > **System**（系统） > **Interfaces**（接口）。

   蜂窝接口以及您配置的其他接口将显示在小部件中。要查看更多信息，请将鼠标悬停在图标上。

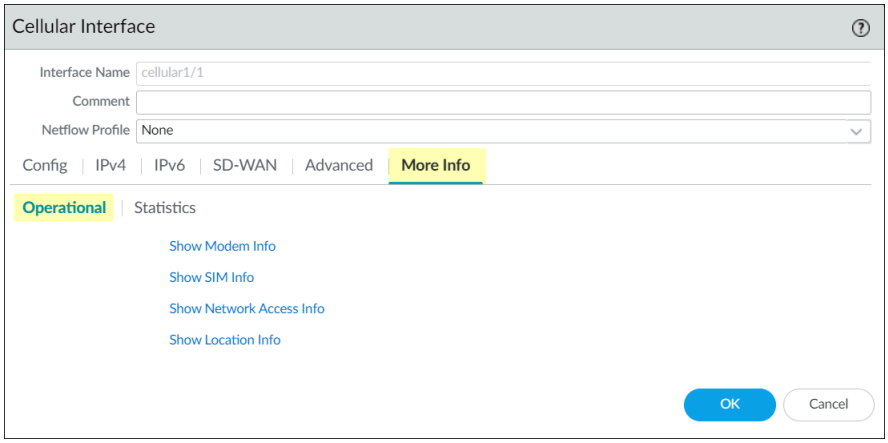


 ©2024 Palo Alto Networks, Inc.

STEP 13 | 验证配置的运行信息是否正确。

要使用 *Panorama* 查看统计信息和运行信息，请先选择设备，然后选择要查看的信息。

1. 选择您配置的蜂窝接口，然后单击 **More Info**（更多信息）**o > Operational**（运行）。

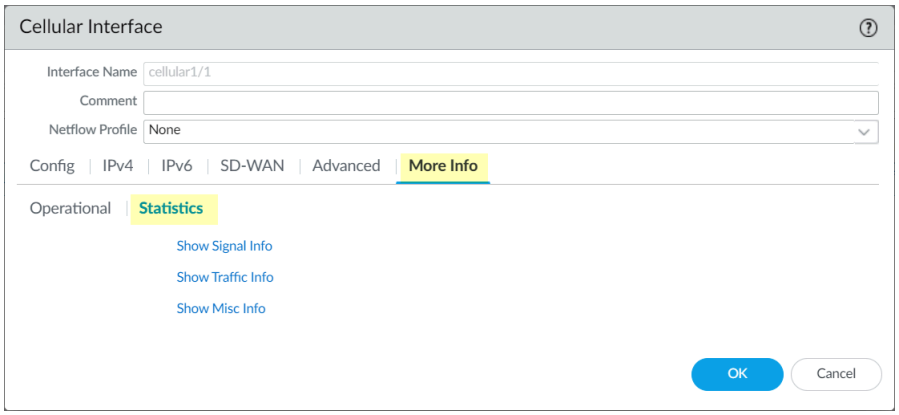


2. 选择 显示调制解调器信息（**Show Modem Info**）以验证调制解调器信息（如 IMEI 和 FSN）。
3. 选择 **Show SIM Info**（显示 **SIM** 信息）以验证 SIM 信息，如 SIM 卡数量及其 IMSI 号码。
4. 选择 **Show Network Access Info**（显示网络访问信息）以验证网络访问信息（例如，频带和小区 ID）。
5. 选择 **Show Location Info**（显示位置信息）以验证 GPS 信息，例如状态、纬度和经度。您必须启用 GPS 才能查看此信息。

©2024 Palo Alto Networks, Inc.

STEP 14 | 查看有关蜂窝接口上活动的信息。

1. 选择您配置的蜂窝接口，然后单击 **More Info**（更多信息） > **Statistics**（统计信息）。

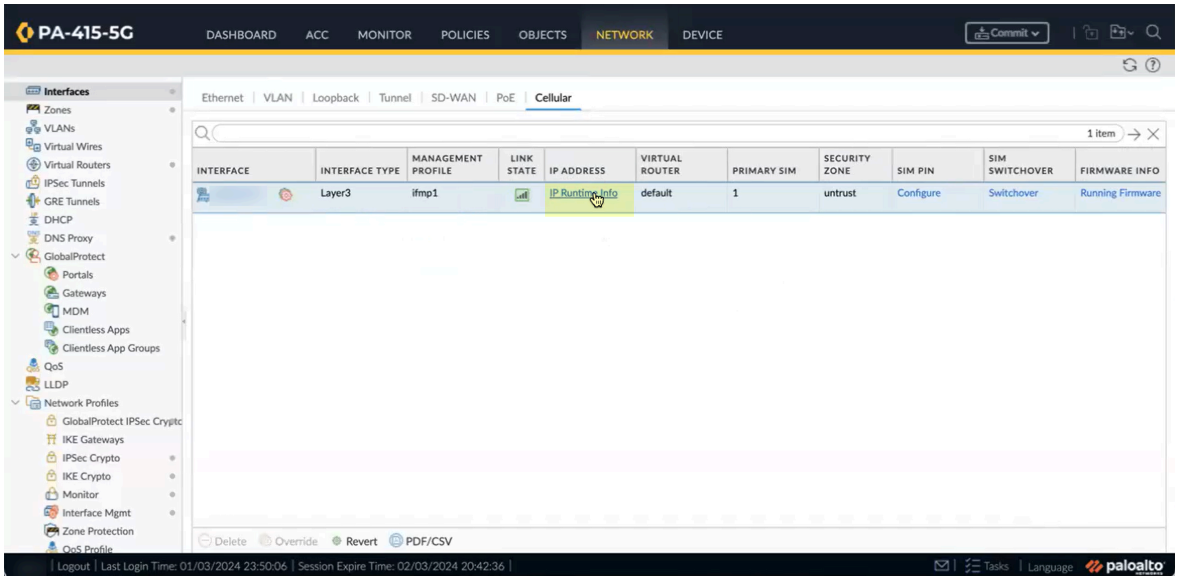


2. 选择 **Show Signal Info**（显示信号信息）以查看信号信息（如RSSI 和 RSRP）。
3. 选择 **Show Traffic Info**（显示流量信息）可查看流量信息，如有关接收和发送的字节数、丢包数、错误数和溢出数。
4. 选择 **Show Misc Info**（显示其他信息）以查看其他信息，包括调制解调器和无线电复位、切换和网络断开的次数。

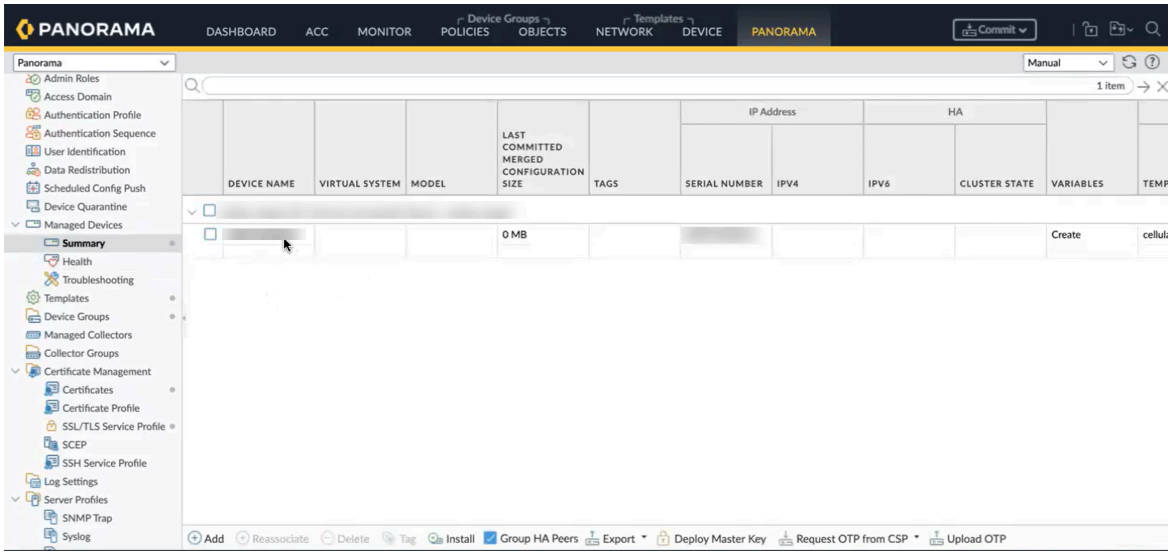
 ©2024 Palo Alto Networks, Inc.

STEP 15 | 监视蜂窝接口上当前会话的相关信息。

1. 选择蜂窝接口的 **IP runtime info**（**IP** 运行时信息）。



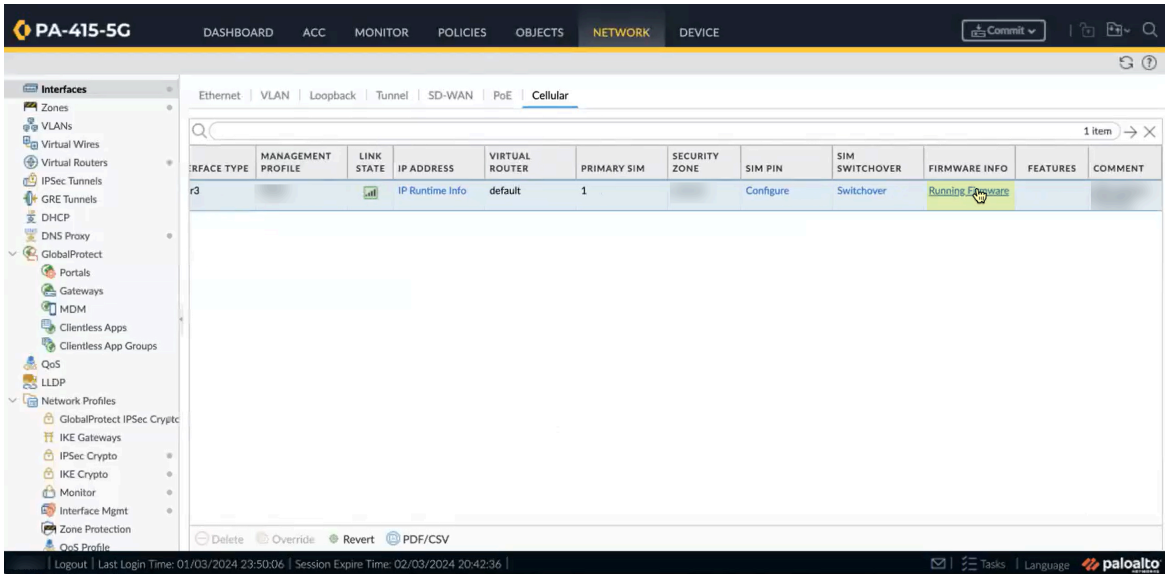
2. 选择 **Data Session Details**（数据会话详细信息）查看数据会话详细信息，如 IP 地址、网关信息以及主要和次要 DNS 接口。
3. （仅限 Panorama）如果使用 Panorama，则可以通过选择 **Panorama** > **Managed Devices**（托管设备）**Summary**（摘要）来查看蜂窝接口。



 ©2024 Palo Alto Networks, Inc.

STEP 16 | 查看接口的固件信息。

1. 为蜂窝接口选择 **Running Firmware**（运行固件）。



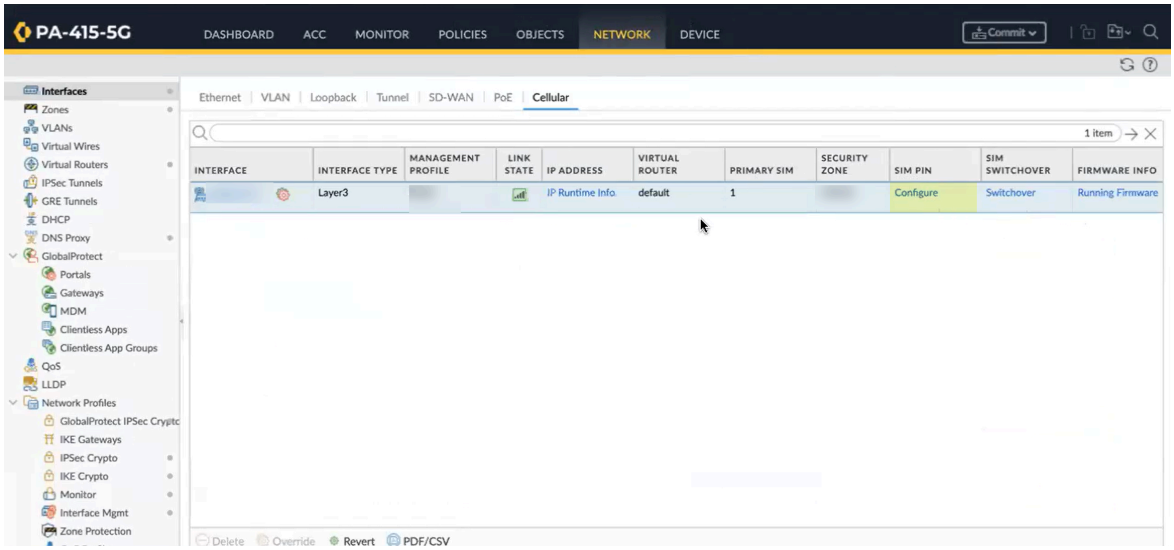
2. 选择 **Firmware Details**（固件详细信息）以查看固件详细信息，包括当前版本、主速率接口 (PRI) 版本，以及 PRI 及其相应固件版本、PRI 版本和运营商的列表。

STEP 17 | （推荐）为增强安全性，请为您的 SIM 卡启用 PIN。

SIM PIN 可防止未经授权使用 SIM 卡。如果您启用 SIM PIN，SIM 会要求您输入 PIN 码来解锁 SIM，然后调制解调器才能访问蜂窝网络和启动数据会话。

在三次尝试解锁 SIM 失败后，SIM 将无法访问，除非您输入个人解锁密钥 (PUK)。无法访问有效 SIM 卡时，系统会自动切换到副 SIM 卡（如果存在）。有关详细信息，请参阅步骤 18。

1. 依次选择 **Configure**（配置）、**SIM PIN**。



2. 确保对于 **SIM PIN Operation**（**SIM PIN** 操作），针对 PIN 选择了 **Enable**（启用）。
3. 选择包含要启用 PIN 的 SIM 卡的 **SIM** 插槽。
4. 输入 **PIN**，然后单击 **Configure**（配置）。

 ©2024 Palo Alto Networks, Inc.

STEP 18 | 如果您启用了 SIM PIN，请管理 SIM PIN 操作。

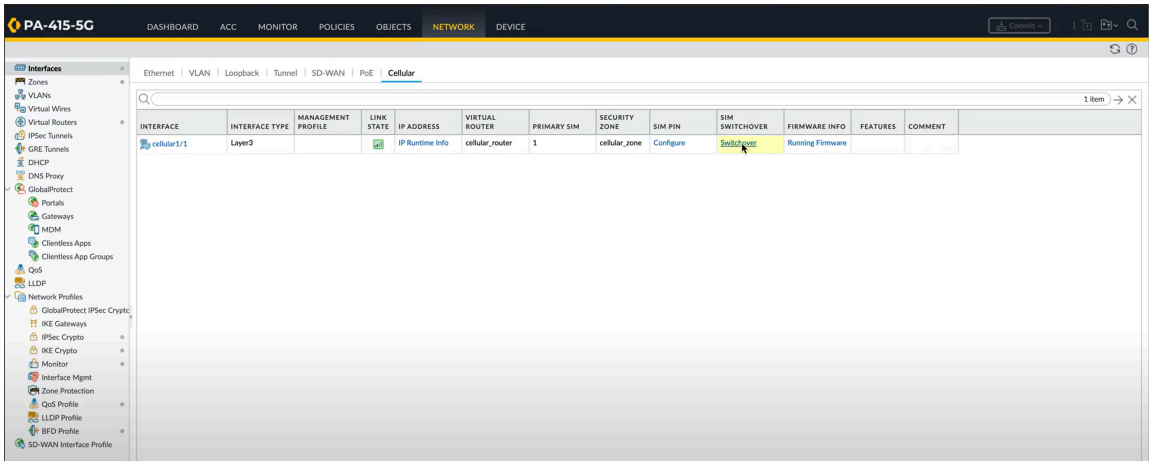
必须先启用 SIM PIN 才能配置新 PIN、禁用 PIN 或解锁 PIN。

- 要禁用 SIM PIN，请对 **SIM PIN Operation**（**SIM PIN** 操作）选择 **Disable**（禁用），确认 **SIM** 插槽，输入 **PIN**，然后单击 **Configure**（配置）。
- 要配置新 PIN，请对 **SIM PIN Operation**（**SIM PIN** 操作）选择 **Change**（更改），确认 **SIM** 插槽，在 **PIN** 和 **New PIN**（新 **PIN**）中分别输入现有 PIN 和新 PIN，然后单击 **Configure**（配置）。
- 要解锁 PIN，请对 **SIM PIN Operation**（**SIM PIN** 操作）选择 **Unblock**（解锁），确认 **SIM** 插槽，在 **New PIN**（新 **PIN**）中输入新 PIN，并输入个人解锁密钥 **(PUK)**，然后单击 **Configure**（配置）。

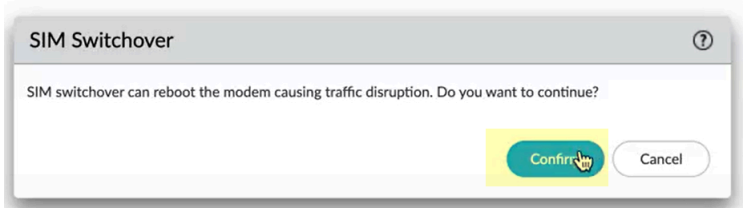
©2024 Palo Alto Networks, Inc.

STEP 19 | 要从当前生效的 SIM 卡切换到其他 SIM 卡，请完成以下步骤。

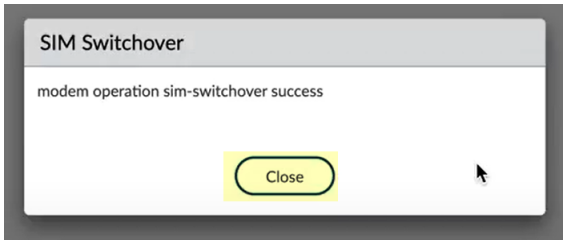
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Cellular**（蜂窝）。
2. 单击 **Switchover**（切换）。



3. 单击 **Confirm**（确认）以确认您要切换当前 SIM 卡。



4. 单击 **Close**（关闭）以关闭显示的确认 SIM 卡更改的通知窗口。



5. SIM 卡更换完成后（约 40 至 60 秒），使用指示板小部件验证更改（请参见步骤 12.c）。

©2024 Palo Alto Networks, Inc.

升级 5G 固件

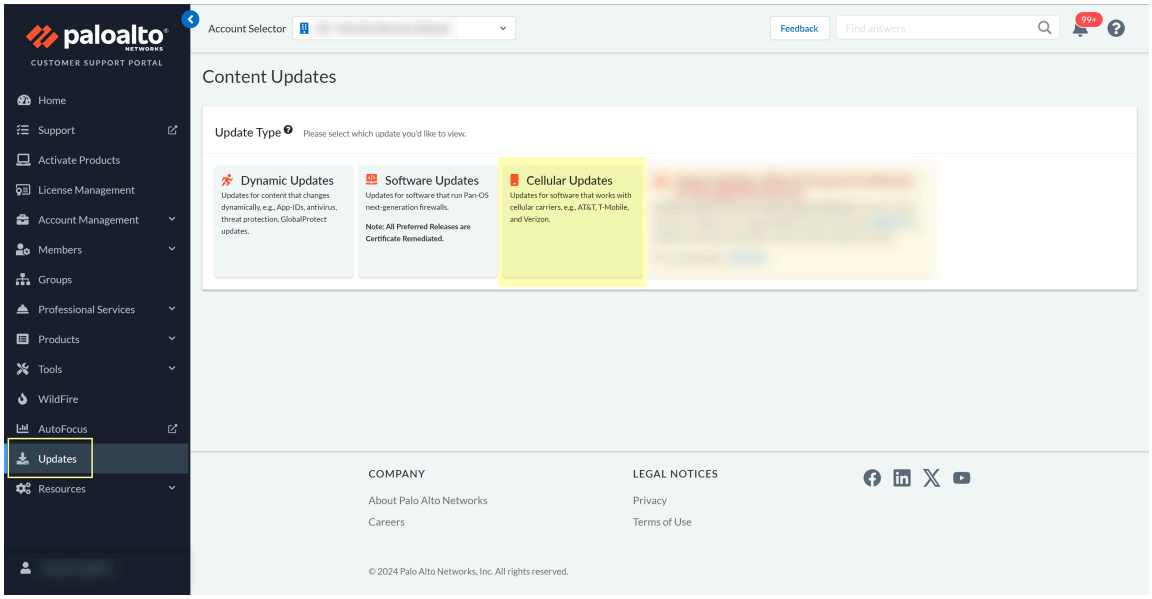
如果您已配置 5G 接口，并且要升级特定无线运营商的固件，请按照以下步骤在防火墙上下载并安装更新。

为确保您获得最新功能和支持，并保护您的网络和用户免受恶意活动侵害，关键步骤是更新固件。

©2024 Palo Alto Networks, Inc.

STEP 1 | 从客户支持门户下载固件更新。

1. 登录到客户支持门户。
2. 选择 **Updates**（更新） > **Cellular Updates**（蜂窝更新）。

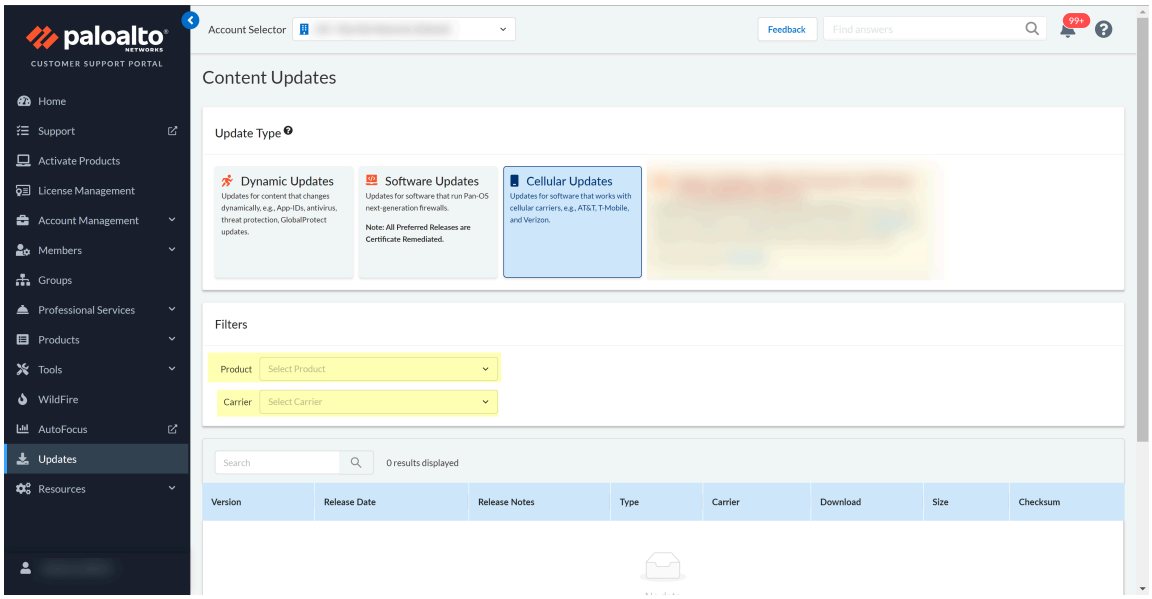


 ©2024 Palo Alto Networks, Inc.

3. 选择 **Product**（产品）和 **Carrier**（运营商），即您要更新的产品和运营商。您必须选择这两项才能查看可用的更新。

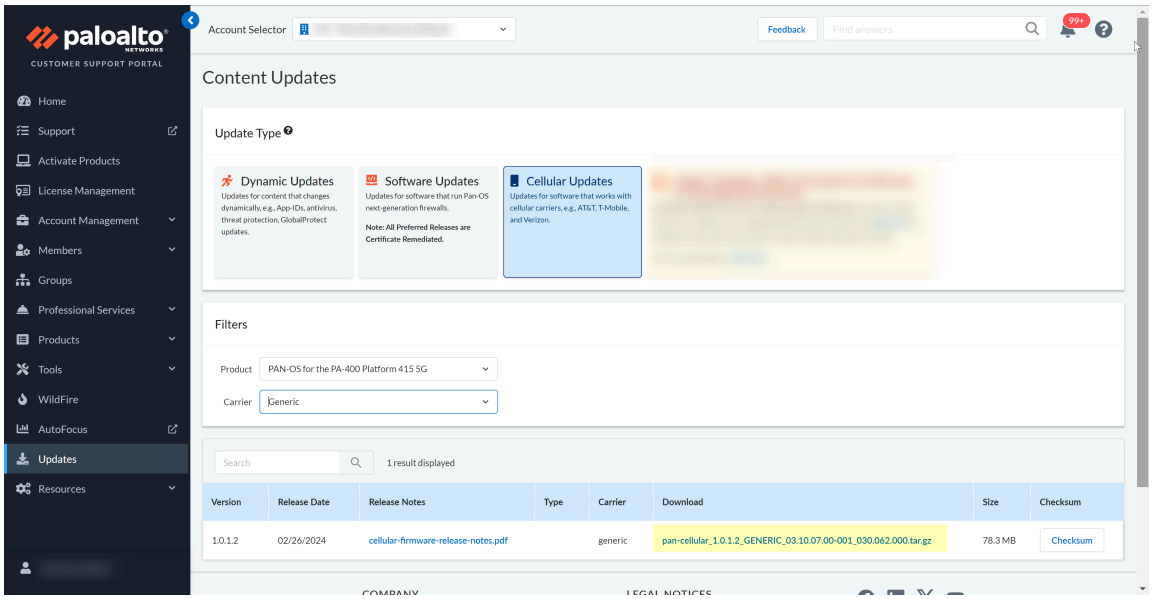
   可用的固件取决于指定的无线运营商。

 ©2024 Palo Alto Networks, Inc.



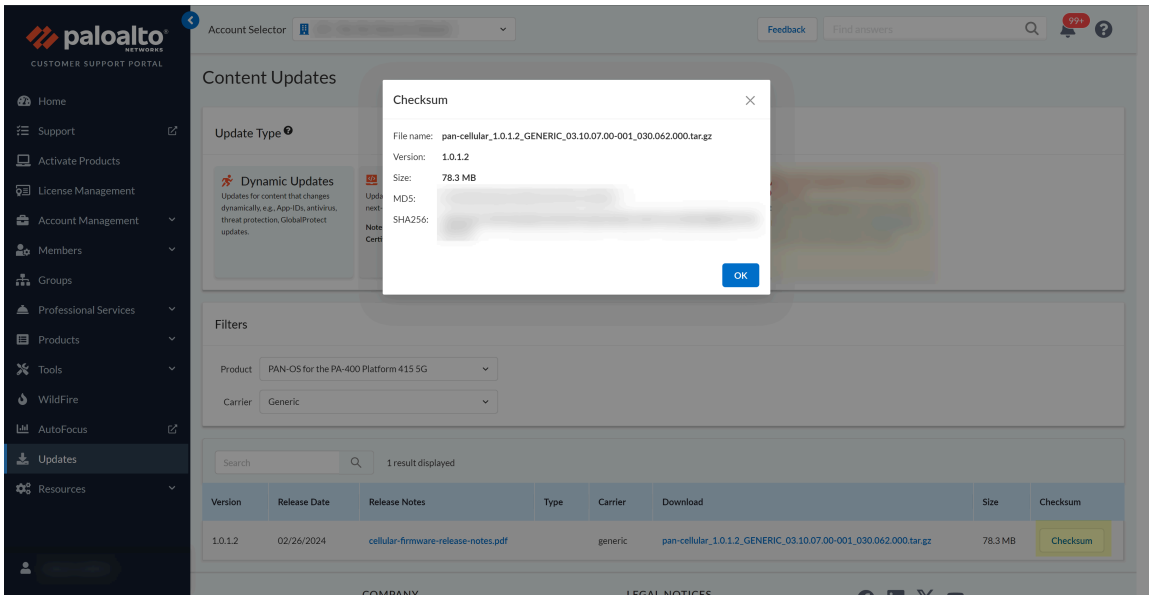
4. 单击 **Download**（下载）以下载要在防火墙上安装的固件更新。

 ©2024 Palo Alto Networks, Inc.



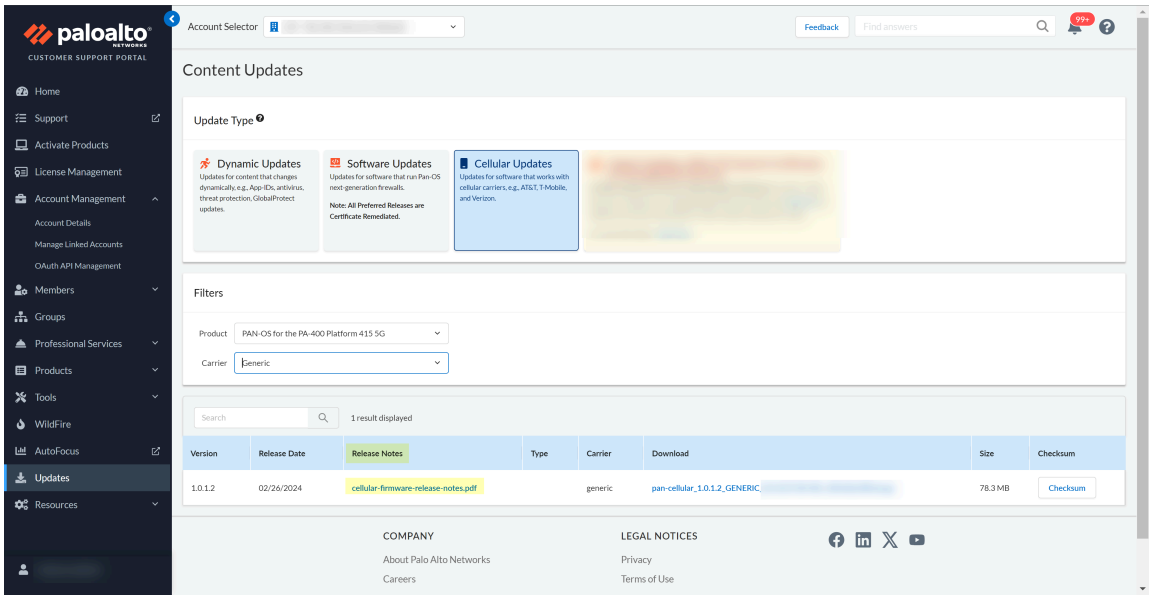
5. （可选）单击 **Checksum**（校验和）以查看有关更新的详细信息。

 ©2024 Palo Alto Networks, Inc.



6. （可选）阅读发行说明以了解有关更新的详细信息。

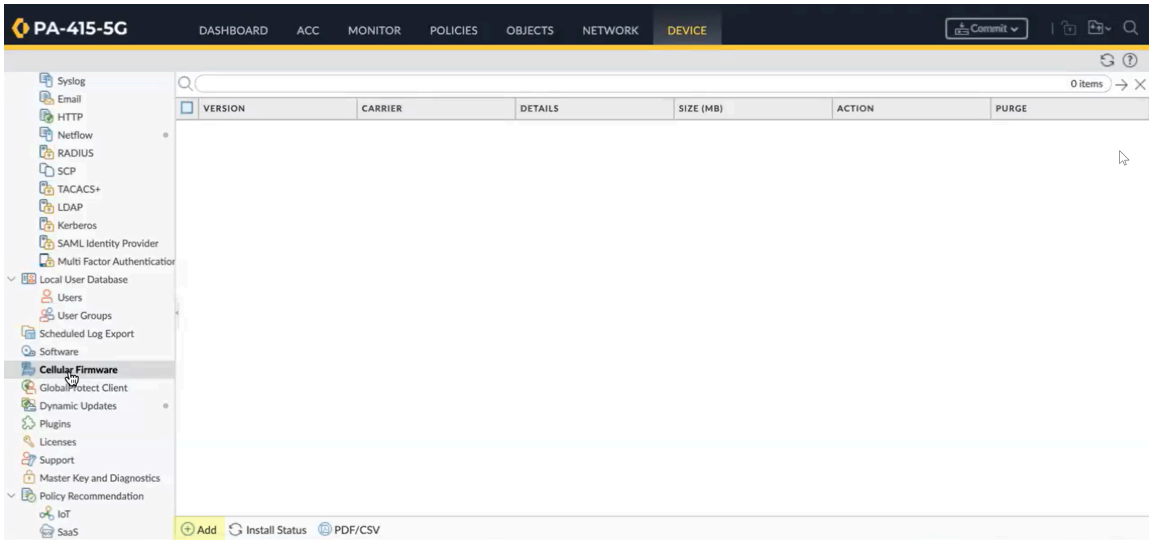
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在防火墙上安装固件更新。

1. 在防火墙上，选择 **Device**（设备） > **Cellular Firmware**（蜂窝固件）。
2. 单击 **Add**（添加）以添加新固件。

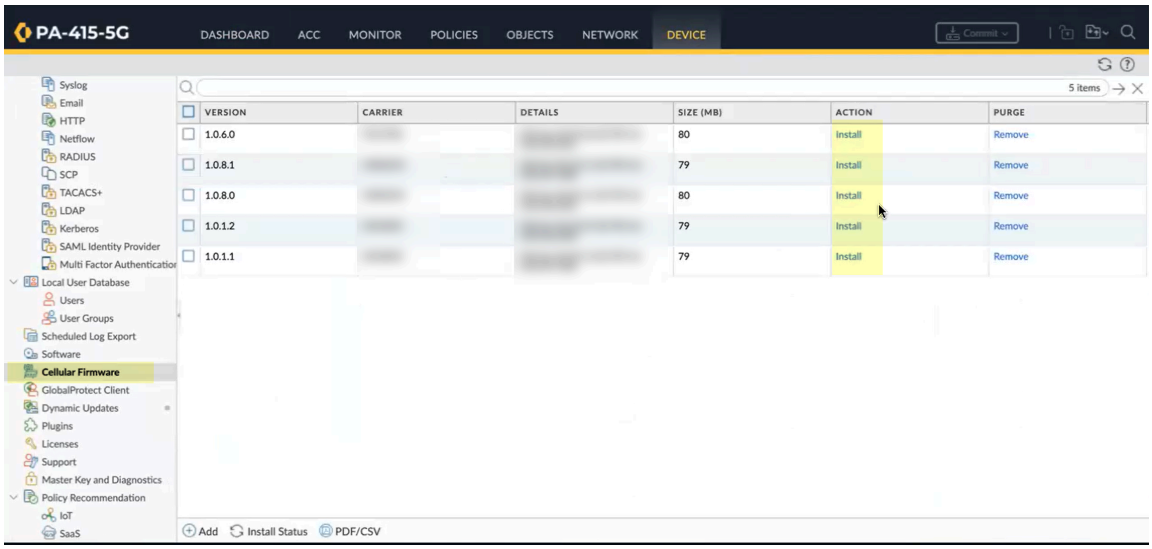


3. 单击 **Browse**（浏览）以浏览到您从客户支持门户下载的固件的位置，选择更新，然后单击 **OK**（确定）以确认您的选择。



4. 单击 **Install**（安装）以安装新固件。

 ©2024 Palo Alto Networks, Inc.



5. 单击 **Confirm**（确认）以确认您要安装新固件。

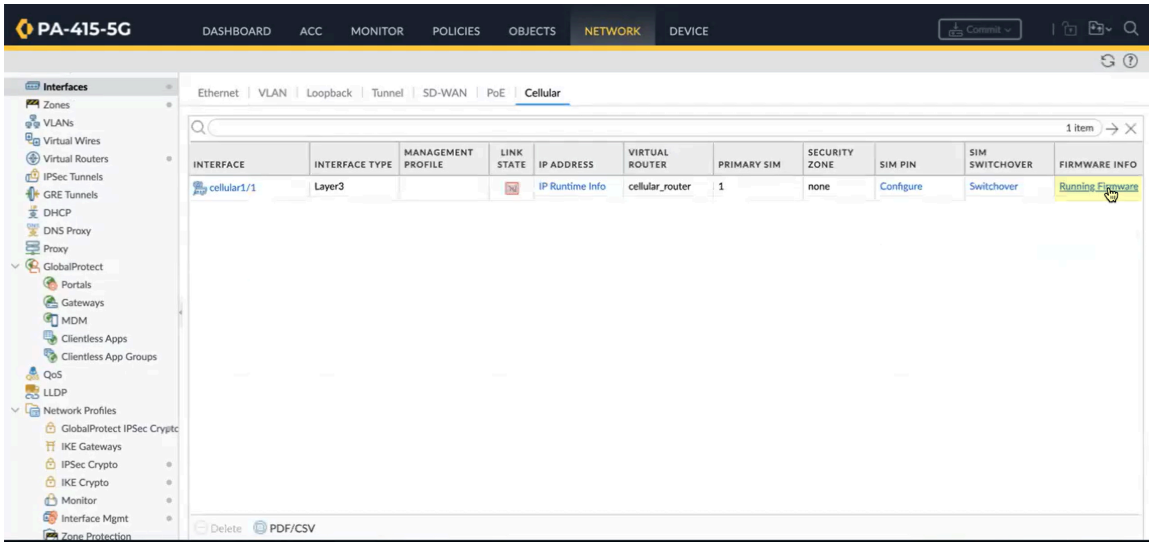


在您确认后，防火墙会在适用的设备上安装新固件。固件升级完成后，设备将使用该特定运营商的新固件作为当前版本。

©2024 Palo Alto Networks, Inc.

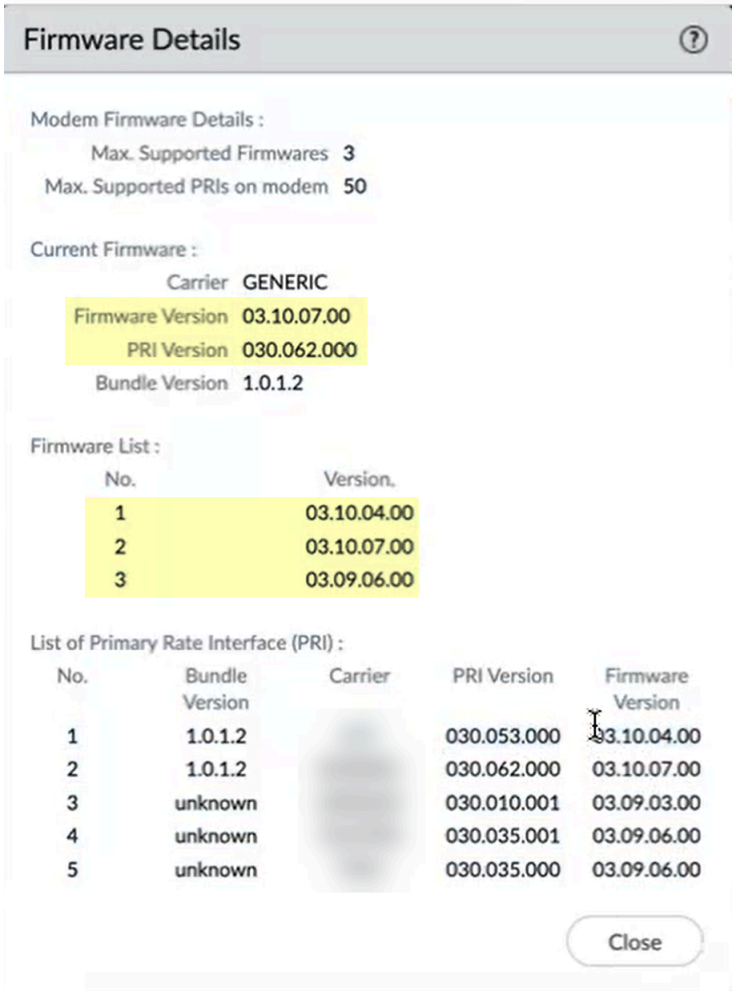
STEP 3 | 验证固件更新是否成功。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Cellular**（蜂窝）。
2. 在 **Firmware Info**（固件信息）列中单击 **Running Firmware**（运行固件）。



3. 验证新固件是否显示在 **Firmware List**（固件列表）中，并验证指定无线运营商的 **Firmware Version**（固件版本）和 **PRI Version**（PRI 版本）均显示为 **Current Firmware**（最新固件）。

 ©2024 Palo Alto Networks, Inc.



Firmware Details

Modem Firmware Details :

Max. Supported Firmwares	3
Max. Supported PRIs on modem	50

Current Firmware :

Carrier	GENERIC
Firmware Version	03.10.07.00
PRI Version	030.062.000
Bundle Version	1.0.1.2

Firmware List :

No.	Version.
1	03.10.04.00
2	03.10.07.00
3	03.09.06.00

List of Primary Rate Interface (PRI) :

No.	Bundle Version	Carrier	PRI Version	Firmware Version
1	1.0.1.2		030.053.000	03.10.04.00
2	1.0.1.2		030.062.000	03.10.07.00
3	unknown		030.010.001	03.09.03.00
4	unknown		030.035.001	03.09.06.00
5	unknown		030.035.000	03.09.06.00

Close

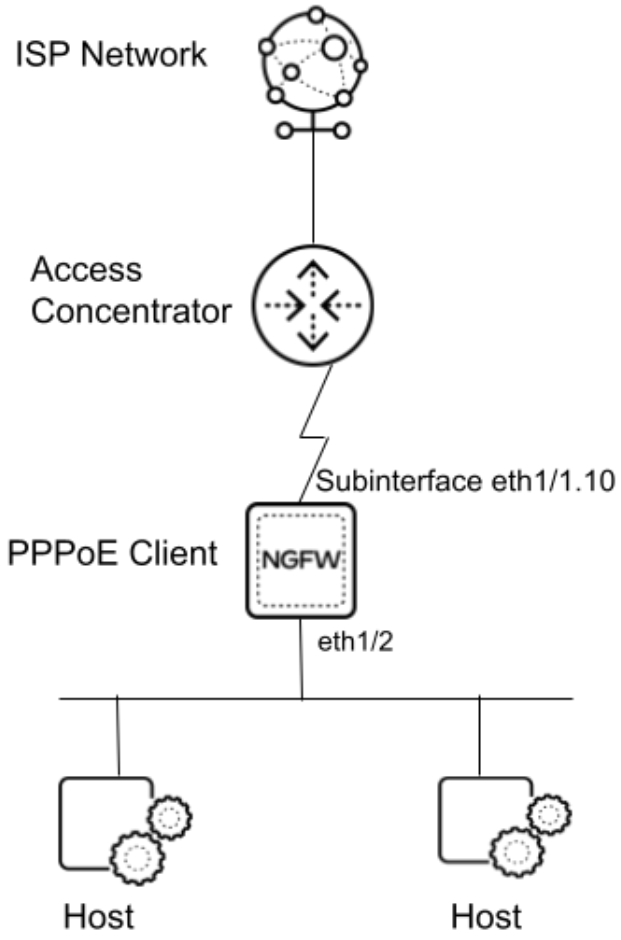
©2024 Palo Alto Networks, Inc.

在子接口上配置 PPPoE 客户端

从 PAN-OS 11.0.1 开始，当 ISP 指示 802.1Q VLAN 上的 PPPoE 是连接到其互联网服务的方式时，您可以在第 3 层子接口上配置 PPPoE（以太网点对点协议）客户端。防火墙使用 802.1Q VLAN 标记与 ISP 建立 PPPoE 连接。您在子接口上配置的 PPPoE 客户端从 ISP 学习其 IPv4 地址以及其他信息，例如服务器的 IP 地址、DNS 信息和 MTU。

子接口支持 IPv4 地址。您可以在物理接口或子接口上配置 PPPOE 客户端，但不能同时配置 PPPOE 客户端。一个物理接口上仅支持一个 PPPoE 子接口。在开始配置 PPPoE 客户端之前，请询问您的 ISP 用于连接的 VLAN 标记。配置子接口编号和 **Tag**（标记）时，必须输入该标记。以下任务假设您已在防火墙上配置了具有安全区域的第 3 层以太网接口。

以下示例拓扑在防火墙和访问集中器之间具有 PPPoE 连接。

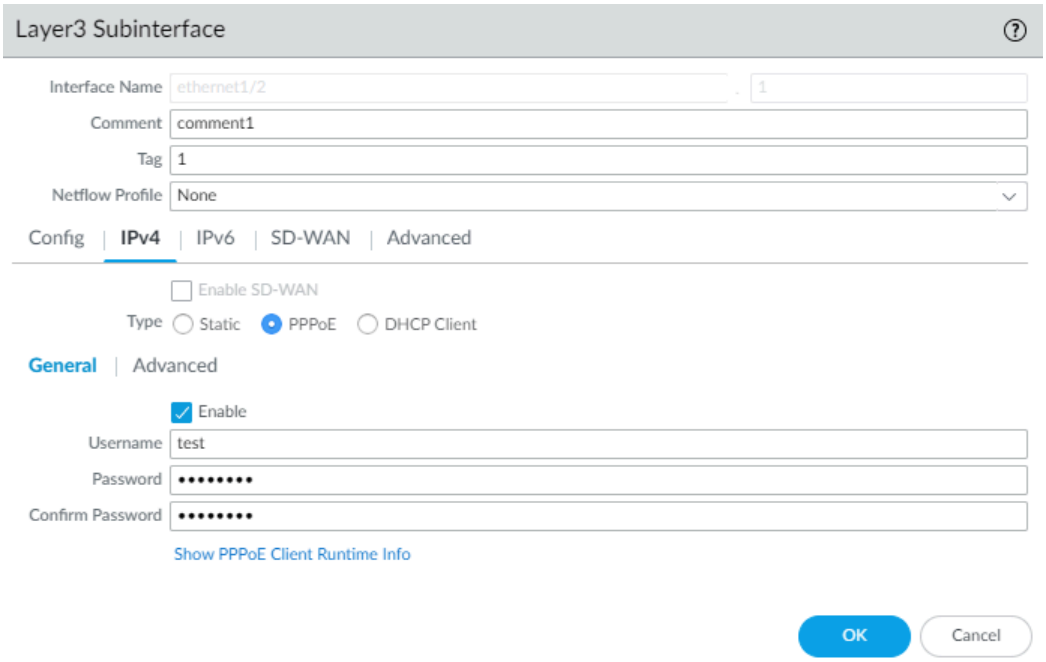


防火墙将来自主机的北向流量（PPPoE 数据包）封装在 802.1Q 帧中，并将其发送到 PPPoE 链路的另一端，然后发送到 ISP 网络。同样，防火墙在将 PPPoE 数据包发送到主机之前，会解封来自 802.1Q 帧的南向流量。

©2024 Palo Alto Networks, Inc.

STEP 1 | 将子接口配置为 PPPoE 客户端（终结点）。

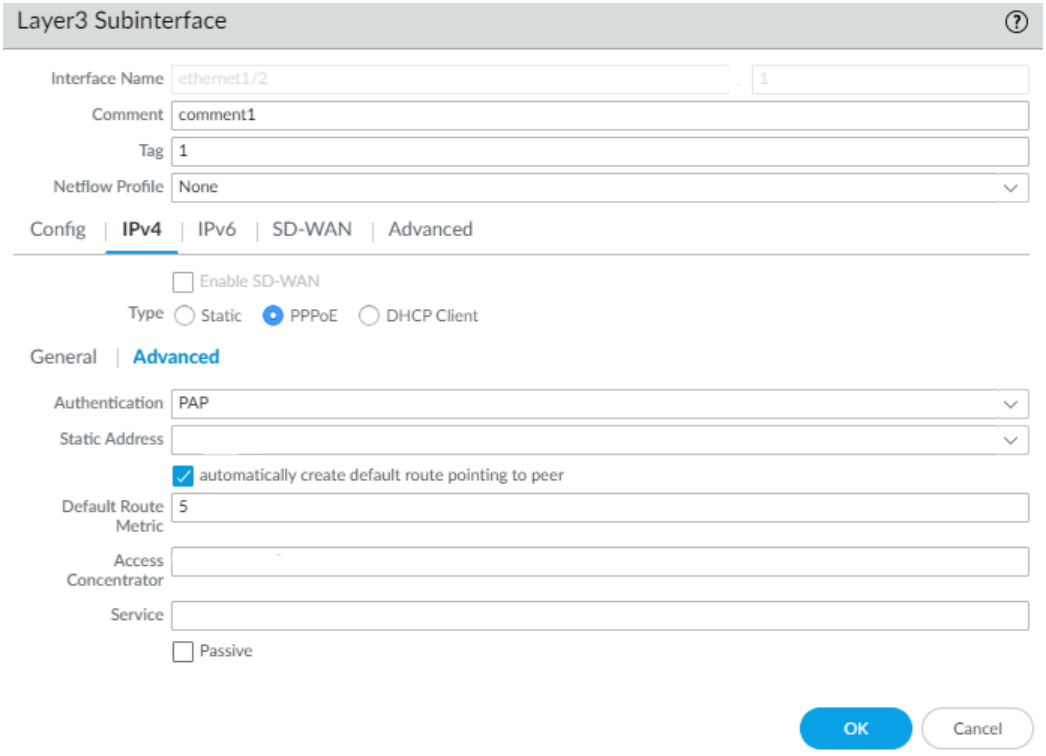
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）并突出显示第 3 层以太网接口。
2. **Add Subinterface**（添加子接口）。
3. 在 **Interface Name**（接口名称）和点的右侧，输入子接口编号；使用 ISP 提供的 VLAN 标记号。此子接口编号仅供参考；VLAN 标记 ID 是从标记字段中读取的。
4. 输入**Tag**（标记），这是您的 ISP 提供的 VLAN 标记号。实际的 VLAN 标记 ID 从此标记字段中读取。
5. 选择 **IPv4**。
6. 选择地址 **Type**（类型）为 **PPPoE**。
7. 选择 **General**（常规） 并 **Enable**（启用） 子接口。
8. 输入您将在下一步中选择的身份验证的 **Username**（用户名）。
9. 输入 **Password**（密码）和 **Confirm Password**（确认密码）。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 配置 PPPoE 子接口的其他特征。

1. 选择 **Advanced**（高级）。
2. 选择身份验证的 **Type**（类型）：
   - **None**（无）—（默认值）如果保留此设置，防火墙将 选择 **auto**（自动） 作为身份验证协议。
   - **CHAP**— 防火墙使用质询握手身份验证协议 (CHAP)。
   - **PAP** — 防火墙使用密码身份验证协议 (PAP)。PAP 将以纯文本形式发送用户名和密码，因此不如 CHAP 安全。
   - **auto**（自动）— 防火墙与 PPPoE 服务器协商身份验证方法（CHAP 或 PAP）。
3. 要请求 PPPoE 服务器为子接口分配特定的 IPv4 地址，请指定一个 **Static Address**（静态地址）。（PPPoE 服务器可以自行决定分配请求的地址或其他地址。默认为 **None**（无）。
4. 要自动创建指向 PPPoE 服务器提供的默认网关的默认路由，请选择自动创建指向对等方的默认路由。
5. 输入 PPPoE 连接的 **Default Route Metric**（默认路由跃点数）（优先级）；范围为 1 到 65,535；默认为 10）。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。
6. 输入 ISP 提供的 **Access Concentrator**（访问集中器）访问集中器的名称（如果有）（字符串值为 0 到 255 个字符）。防火墙将连接此访问集中器。
7. 输入您的 ISP 提供的 **Service**（服务）（如果有）（字符串值为 0 到 255 个字符）。
8. 如果希望 PPPoE 客户端（防火墙）等待 PPPoE 服务器启动连接，请选择 **Passive**（被动）。如果未选择被动，则允许防火墙启动连接。



 ©2024 Palo Alto Networks, Inc.

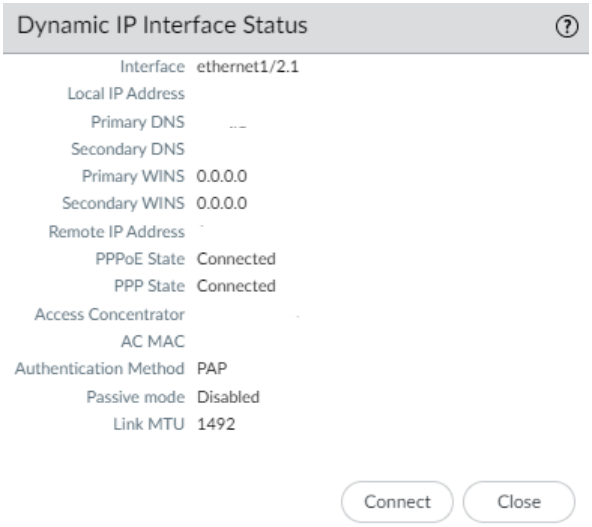
STEP 3 | 单击 **OK**（确定）。

STEP 4 | **Commit**（提交）更改。

STEP 5 | 查看有关 PPPoE 客户端的信息。从 PPPoE 服务器接收本地 IP 地址、主 DNS、辅助 DNS、主 WINS、辅助 WINS、远程 IP 地址、访问集中器名称和 AC MAC 地址。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后在您配置的子接口行中，选择 **Dynamic-PPPoE**（动态 **PPPoE**）。

   或者，您可以选择子接口、***IPv4***，和 ***Show PPPoE Client Runtime Info***（显示 ***PPPoE*** 客户端运行时信息）。



2. **Close**（关闭）窗口。

 ©2024 Palo Alto Networks, Inc.

配置 IPv6 PPPoE 客户端

防火墙支持让以太网第 3 层接口或子接口充当以太网点对点协议 (PPPoE) IPv6 客户端，用于连接提供 IPv6 互联网服务的 ISP。在 PPPoE 模式下，接口或子接口可以在有状态或无状态模式下使用 DHCPv6 动态获取 IPv6 地址。在有状态模式下，PPPoE 接口从 DHCPv6 服务器动态获取所有连接参数。在无状态模式下，PPPoE 接口的 IPv6 地址是使用无状态地址自动配置 (SLAAC) 获得的，但其他参数（DNS 和前缀委派）是通过 DHCPv6 获得的。有状态和无状态 DHCPv6 可减少配置工作量和错误，并简化地址管理。

使用有状态 *DHCPv6* 来分配 *PPPoEv6* 客户端地址，因为这比无状态自动配置更安全。

只有以太网第 3 层接口和子接口支持 IPv6 PPPoE 客户端（隧道、AE、VLAN 和环回接口不支持 IPv6 PPPoE 客户端）。第 3 层接口及其子接口不能同时充当 PPPoEv6 客户端。

一个限制是，使用 *PPPoEv6* 配置的接口无法从路由器通告 *(RA-DNS)* 获取 *DNS* 服务器地址和/或 *DNS* 前缀。您必须依靠 *DHCPv6* 来获取 *DNS* 信息或手动配置这些参数。

为 *PPPoE* 配置了这些参数后，就无法为接口分配静态 *IP* 地址。

如果您仅配置单堆栈 *PPPoE* 客户端（*IPv4* 或 *IPv6*），则不能同时使用 *IPv4* 和 *IPv6* *PPPoE* 客户端连接。如果您配置了 *PPpoEv4* 客户端并连接到 *ISP*，则只能使用 *IPv4* 连接。如果您配置了 *PPPoEv6* 客户端并连接到 *ISP*，则只能使用 *IPv6* 连接。（如果您配置了 *PPPoE v4/v6* 客户端（双堆栈模式）并连接到 *ISP*，则可以同时使用 *IPv4* 和 *IPv6* 连接。）

如果来自宽带网络网关 (BNG) 或其他设备的 RA 中的托管地址配置标志 (M-flag) 设置为 0，则 PPPoE 客户端将使用无状态自动配置。如果将其设置为 1，则客户端将尝试使用有状态 DHCPv6 从 DHCPv6 服务器获取其 IPv6 地址。

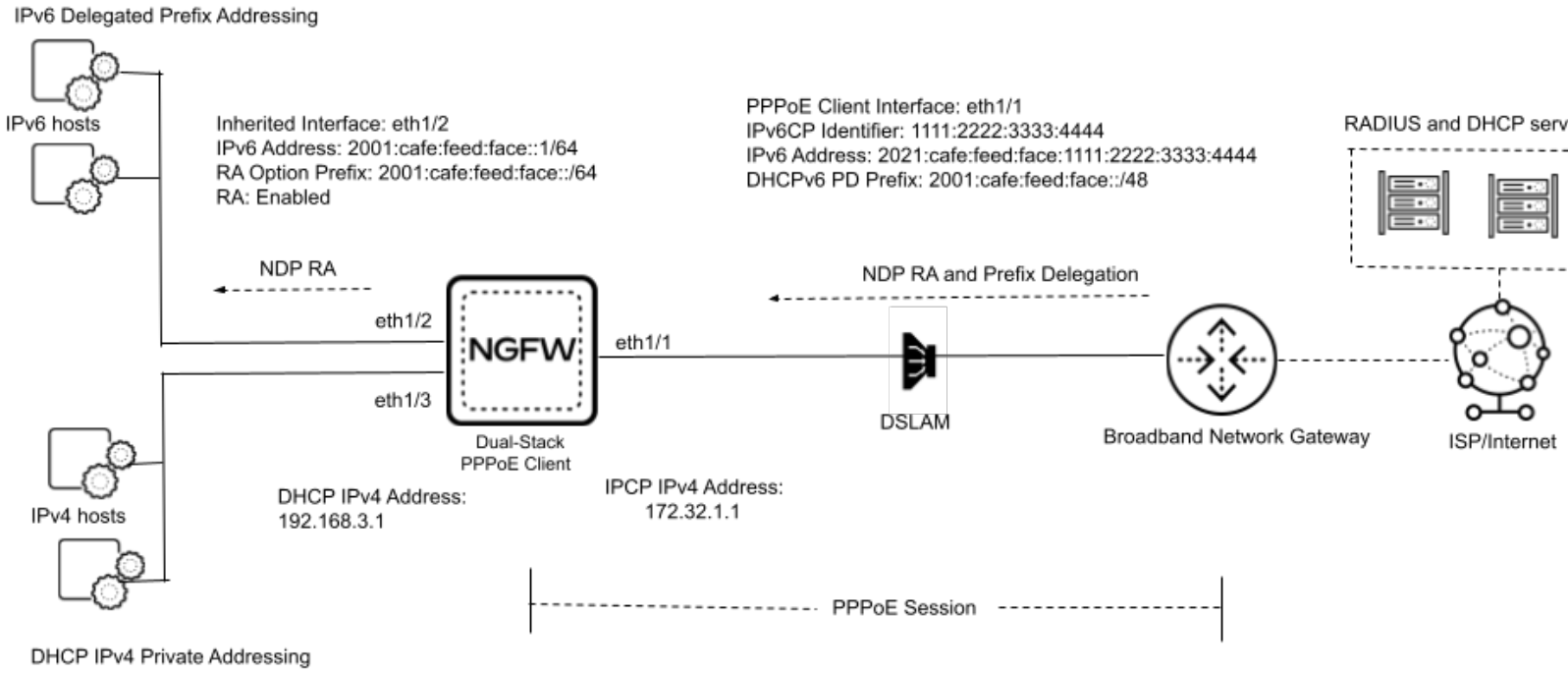
当其他配置标志 (O-Flag) 设置为 1 时，应该可以从 DHCPv6 服务器获得除 IPv6 地址之外的配置信息，例如递归 DNS 服务器的委托前缀和地址。

IPv6CP 协商客户端接口的接口标识符。

以下用例适用于有状态 DHCPv6。下图说明了防火墙使用有状态 DHCPv6 来接收其 IPv6 地址和委托前缀。以太网接口 1/1 充当 PPPoEv6 客户端，面向接入集中器、宽带网络网关、数字用户线接入多路复用器 (DSLAM) 或 PPPoEv6 服务器（取决于 ISP 的部署）。PPPoEv6 客户端接口通过 IPv6 控制协议 (IPv6CP) 获知其 IPv6 接口标识符 (IID)。协商完此 IPv6 参数后，它将用于为接口分配 IPv6 链路本地地址 (LLA)。由于 IID 已经过协商，因此不会执行重复地址检测 (DAD)。将继续通过 DHCPv6 分配地址。连接的网关也可从路由器通告 (RA) 获取。

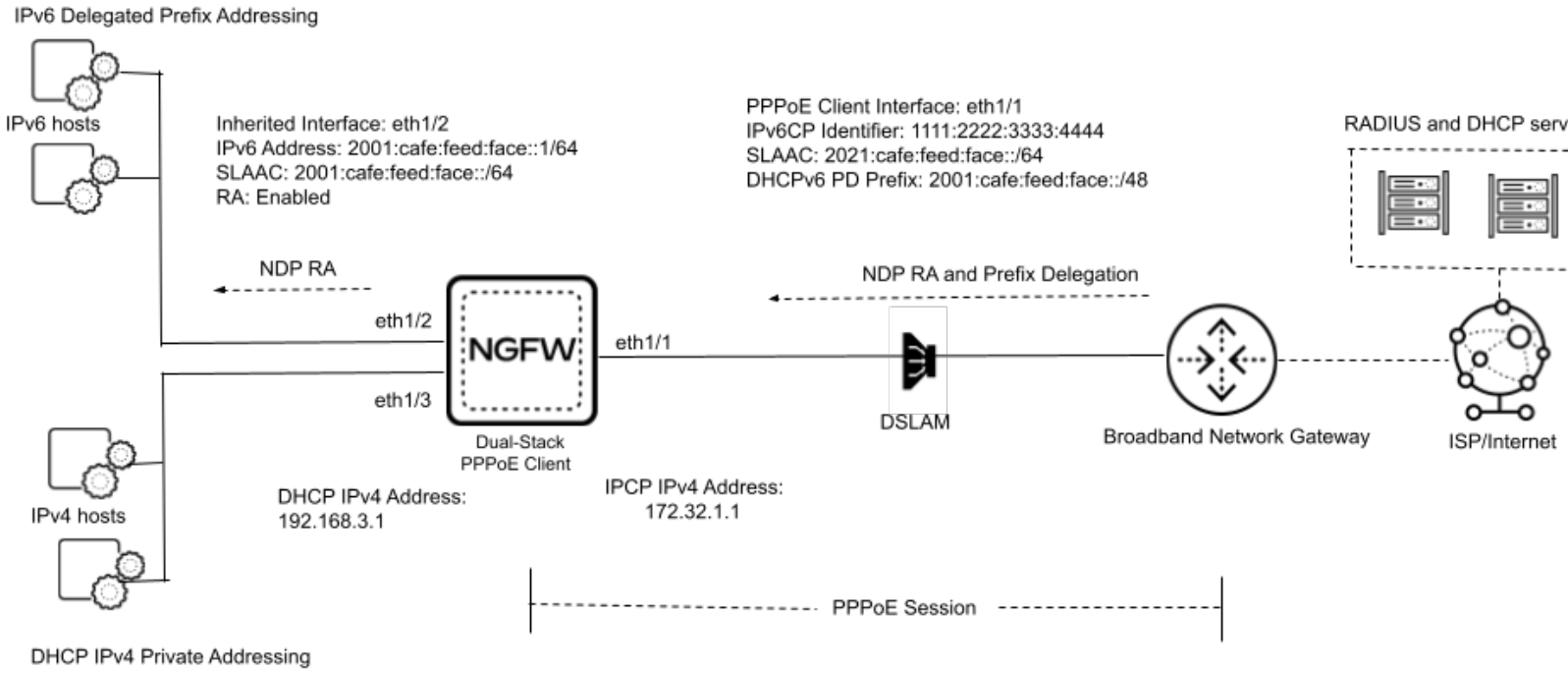
PPPoEv6 客户端接收来自 ISP 的 DHCPv6 委托前缀。PPPoEv6 客户端可以使用该信息将其分配给池。然后该池可能被分成多个 /64 前缀，这些前缀又被分配给继承接口 eth1/2。Eth1/2 将使用 EUI-64 机制创建 IPv6 地址。连接到 eth1/2 的局域网分段上的主机将使用 SLAAC 创建其 IPv6 地址。

 ©2024 Palo Alto Networks, Inc.



以下用例适用于无状态 DHCPv6 (SLAAC)。下图说明了防火墙使用无状态 DHCPv6 来接收其 IPv6 地址并将前缀委派给 IPv6 主机。以太网接口 1/1 充当 PPPoEv6 客户端，面向接入集中器、宽带网络网关、DSLAM 或 PPPoEv6 服务器（取决于互联网服务提供商的部署）。PPPoEv6 客户端接口通过 IPv6 控制协议 (IPv6CP) 获知其 IPv6 接口标识符 (IID)。协商完此 IPv6 参数后，它将用于为接口分配 IPv6 链路本地地址 (LLA)。不会执行 DAD，因为 IID 已经协商完毕。事件继续进行，并通过 SLAAC 分配地址。连接网关也是从 RA 获得的。

 ©2024 Palo Alto Networks, Inc.



防火墙将北向流量（来自 IPv6 主机）封装在 PPPoE 中，并将流量发送到互联网。

STEP 1 | 将以太网第 3 层接口或子接口配置为 IPv6 PPPoE 客户端。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）并选择一个接口。
2. 为 **Interface Type**（接口类型）选择 **Layer3**。

   或者，您可以选择第 *3* 层接口，添加子接口，输入子接口号，添加标签，然后继续将子接口配置为 *PPPoEv6* 客户端。
3. 选择 **IPv6** 和 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。
4. 选择无状态地址分配要使用的 **EUI-64**（扩展唯一标识符），以便主机可以为自己分配唯一的 64 位 V6 接口标识符。
5. 对于地址分配的 **Type**（类型），选择 **PPPoEv6 Client**（**PPPoEv6** 客户端）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 配置 PPPoEv6 客户端的常规设置。

1. **Enable**（启用）接口。
2. 如果您已经为 PPPoE 客户端 (IPv4) 配置了接口，则可以考虑选择 **Apply IPv4 Parameters**（应用 **IPv4** 参数）选项，这会将 IPv4 参数复制到 PPPoEv6 客户端。（复制的参数包括身份验证类型、用户名、密码、访问集中器名称、服务和被动设置。）

   - 如果您随后在 *PPPoE IPv4* 客户端上重新配置参数，则新的参数值将复制到 *PPPoE IPv6* 客户端。
   - 如果重新配置任一客户端的参数，则会重新建立会话，从而导致流量中断。

   即使您独立配置 *PPPoE IPv4* 客户端和 *PPPoE IPv6* 客户端，也必须使用相同的身份验证类型、用户名、密码、访问集中器名称、服务和被动设置来配置这两个客户端。
3. 如果你想让 PPPoEv6 客户端（接口）等待 PPPoEv6 服务器启动连接，请选择 **Passive**（被动）。如果未选择“Passive（被动）”，则会允许此接口启动连接。
4. 为接口选择身份验证类型。

   如果您还将此接口配置为 *PPPoE IPv4* 客户端，则必须使用相同的身份验证类型、用户名、密码、访问集中器名称和服务来配置这两个客户端。

   - **CHAP**—接口使用质询握手身份验证协议 (CHAP)。
   - **PAP**—接口使用密码身份验证协议 (PAP)。PAP 将以纯文本形式发送用户名和密码，因此不如 CHAP 安全。
   - **auto**（自动）—接口与 PPPoEv6 服务器协商身份验证方法（CHAP 或 PAP）。
5. 在 **Username**（用户名）中，输入用于身份验证的用户名。
6. 输入 **Password**（密码）和 **Confirm Password**（确认密码）。
7. 如果您的 ISP 已告知您要连接的接入集中器名称，请在 **Access Concentrator**（接入集中器）中输入此名称（0 到 255 个字符的字符串）。
8. 如果您希望接口作为 PPPoEv6 客户端从 PPPoEv6 服务器请求特定服务，请在 **Service**（服务）中输入服务（0 到 255 个字符的字符串）。

STEP 3 | 配置地址选项。

1. 选择 **Address Assignment**（地址分配）。
2. **Accept Router Advertised Route**（接受路由器通告路由）选项允许 PPPoEv6 客户端接受 RA。
3. 针对从接口到 ISP 的路由，设置 **Default Route Metric**（默认路由指标）选项；范围是 1 到65,535；默认值为 10。
4. 设置 PPPoEv6 客户端接口的 **Preference**（首选项）选项：**High**（高）（默认值）、**Medium**（中）或 **Low**（低）。如果您有两个接口（每个接口都连接到不同的 ISP 以实现冗余），您可以为一个 ISP 分配比另一个 ISP 接口优先级更高的接口。连接到首选接口的 ISP 将是提供委派前缀以发送到面向主机的接口的 ISP。如果接口具有相同的首选项，则两个 ISP 都会提供一个委派前缀，并且主机决定使用哪个前缀。

©2024 Palo Alto Networks, Inc.

STEP 4 | （对于无状态自动配置）让防火墙使用 IPv6 控制协议 (IPv6CP) 接口标识符和路由器通告中的前缀（使用 SLAAC）自动配置接口的 IPv6 地址。

1. 选择 **Autoconfig**（自动配置）。
2. 启用自动配置。
3. 继续配置地址解析。

STEP 5 | （对于有状态配置）或者，使用 DHCPv6 配置地址分配。

1. 在 **Address Assignment**（地址分配）选项卡上，选择 **DHCPv6**。
2. 启用 DHCPv6。
3. 选择 **DHCPv6 Options**（**DHCPv6** 选项）。
4. **Enable IPv6 Address**（启用 **IPv6** 地址）选项允许 PPPoEv6 客户端使用 DHCPv6 服务器分配的地址。
5. 选择 **Rapid Commit**（快速提交） 以使用 Solicit 和 Reply 消息（两条消息）的 DHCPv6 进程，而不是 Solicit、Advertise、Request 和 Reply 消息（四条消息）的进程。
6. 选择接口用来向 DHCPv6 服务器标识自身的 **DUID** 类型（**DHCPv6** 唯一标识符）：
   - **DUID-LLT**—接口的链路层地址，与时间戳串联在一起。
   - **DUID-LL**—接口的链路层地址。

STEP 6 | 如果您选择使用 DHCPv6 进行地址分配，请配置前缀委派。

1. 选择 **Prefix Delegation**（前缀委派）。
2. **Enable Prefix Delegation**（启用前缀委派）选项允许防火墙支持前缀委派功能。这意味着接口从上游 DHCPv6 服务器接受前缀并将前缀放入前缀池，防火墙从中通过 RA 将前缀委派给主机。启用或禁用接口前缀委派的能力允许防火墙支持多个 ISP（每个接口一个 ISP）。在此接口上启用前缀委派控制哪个 ISP 提供前缀。委派前缀用于面向主机的接口，其 IPv6 地址由 MAC 地址和 EUI-64 输入构成。
3. 选择 **DHCP Prefix Length Hint**（**DHCP** 前缀长度提示） 使防火墙能够将首选的 DHCPv6 前缀长度发送到 DHCPv6 服务器。
4. 为 **DHCP Prefix Length (bits)**（**DHCP** 前缀长度（位））输入首选值，它作为提示发送到 DHCPv6 服务器；范围为 0 到 128；默认值为 48。DHCPv6 服务器可以自行决定发送它选择的任何前缀长度。

   例如，请求 */48* 的前缀长度会为子网（*/64* 减去 */48*）留下 *16* 位，这表明您需要对该前缀进行许多细分才能进行委派。如果请求前缀长度为 */63*，则系统会留下 *1* 位用于仅委派两个子网。在 *128* 位中，还有 */64* 位用于主机地址。

   接口可以接收 */48* 前缀，但委派 */64* 前缀，例如，这意味着防火墙正在细分它委托的前缀。
5. 输入池的 **Prefix Pool Name**（前缀池名称）（防火墙将接收到的前缀存储在此池中）。该名称必须唯一，并且最多包含 63 个字母数字字符、连字符、句点和下划线。

   使用反映 *ISP* 的前缀池名称以便于识别。

 ©2024 Palo Alto Networks, Inc.

6. 使用 **Show Prefix Pool Assignment**（显示前缀池分配） 可查看每个面向主机的继承接口：继承前缀（接口分配给主机的前缀），继承接口本身的分配 IPv6 地址（基于前缀并从 MAC 地址构建）、路由器首选项和接口状态。

STEP 7 | 配置地址解析。

1. 选择 **Address Resolution**（地址解析）。
2. 启用重复地址检测 (DAD)。
3. 设置 **DAD Attempts**（**DAD** 尝试次数）， 也就是在尝试标识邻居失败之前在邻居请求 (NS) 间隔内的 DAD 尝试次数；范围为 1 至 10，默认为 1。
4. 设置 **Reachable Time (sec)**（可访问时间（秒）），即查询和响应成功后邻居保持可访问状态的秒数；范围为 10 到 36,000；默认值为 30。
5. 设置 **NS Interval (sec)**（**NS** 间隔（秒））；即 DAD 尝试多少秒后表明失败；范围为 1 到 3,600；默认值为 1。
6. **Enable NDP Monitoring**（启用 **NDP** 监控）（邻居发现协议监控）。

STEP 8 | 配置 DNS 支持。

1. 选择 **DNS Support**（**DNS** 支持）。
2. 选择 **DNS Recursive Name Server**（**DNS** 递归域名服务器）。选择 **Type**（类型）：
   - **DHCPv6** — 让 DHCPv6 服务器发送递归 DNS (RDNS) 名称服务器信息。
   - **Manual**（手动）—添加 **RDNS** 域名服务器的 IPv6 地址和生命周期，即客户端可以使用特定 RDNS 服务器解析域名的最大秒数；范围为 4 到 3,600；默认值为 1,200。如果 PPPoEv6 客户端使用 SLAAC 自动配置其 IPv6 地址，请选择“Manual（手动）”。
3. 选择 **Domain Search List**（域名搜索列表），然后选择 **Type**（类型）：
   - **DHCPv6**— 让 DHCPv6 服务器发送域搜索列表信息。
   - 手动 —为 DNS 搜索列表 (DNSSL) 添加一个或多个域名（后缀），并添加 **Lifetime**（生命周期）的值，即客户端可以使用特定域名搜索列表的最大秒数；范围为 4 到 3,600；默认值为 1,200。如果 PPPoEv6 客户端使用 SLAAC 自动配置其 IPv6 地址，请选择“Manual（手动）”。

STEP 9 | 单击 **OK**（确定）

STEP 10 | **Commit**（提交）。

STEP 11 | 查看 PPPoEv6 客户端信息。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后选择已配置的接口。
2. 显示 **PPPoEv6** 客户端运行时信息。

 ©2024 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。所有 Palo Alto Networks® 防火墙都支持聚合组。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、25Gbps、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，输入一个数字以标识该聚合组。范围为 1 到防火墙支持的最大聚合接口组数。
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 | 对于第 3 层接口，如果要配置静态 IPv4 地址，请选择 **IPv4** 并参考配置第 3 层接口来配置静态 IPv4 地址。

STEP 3 | 对于第 3 层接口，如果要配置静态 IPv6 地址，请选择 **IPv6** 并参考配置第 3 层接口来配置静态 IPv6 地址。

STEP 4 | 对于第 3 层接口，如果要将接口配置为 DHCP 客户端以接收 IPv4 地址，请选择 **IPv4** 并参考将接口配置为 DHCPv4 客户端来配置 DHCP 客户端。

STEP 5 | 对于第 3 层接口，如果要将接口配置为 DHCPv6 客户端以接收 IPv6 地址（使用或不适用前缀委派），请选择 **IPv6** 并参考 Configure an Interface as a DHCPv6 Client（将接口配置为 DHCPv6 客户端） 来配置 DHCPv6 客户端。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 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。
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 7 | 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 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 9 | 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 10 | （仅支持的防火墙）如果接口对应于防火墙上的 PoE（以太网供电）端口，则可以选择配置 PoE。

STEP 11 | **Commit**（提交）更改。

STEP 12 | 验证聚合组状态。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 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。
3. 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。

STEP 13 | （仅限 PA-7050 和 PA-7080 防火墙）如果您的聚合接口组具有位于不同线路卡上的接口，则最佳做法是启用防火墙，以便它可以处理在 AE 组中分布在多张卡上的多个接口接收的片段式 IP 数据包。为此，请使用以下带有 **hash** 关键字的 CLI 操作命令。（为了完整性，还会显示另外两个关键字。）

1. 访问 CLI。

 ©2024 Palo Alto Networks, Inc.

2. 使用以下操作 CLI 命令：**set ae-frag redistribution-policy** <**self** | **fixed sXdpX** | **hash**>
   - **self**—（默认）此关键字用于遗留行为；它不允许防火墙处理在 AE 接口组中的多个接口上接收的片段式数据包。
   - **fixed s**<*slot-number*>**dp**<*dataplane-cpu-number*>—替换 *slot-number* 变量，并将 *data-plane-cpu-number* 变量替换为将处理所有 AE 接口的所有成员收到的所有 IP 片段的数据平面的数据平面编号。**fixed** 关键字主要用于故障排除目的，不应在生产中使用。
   - **hash**—用于使防火墙能够处理它在 AE 接口组中位于多个线路卡上的多个接口接收的片段式数据包。

 ©2024 Palo Alto Networks, Inc.

配置用于网络分段的 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 层接口 (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发现，且不受在线时间 (TTL) 值或跃点限制的影响。

以下平台支持 *Bonjour* 流量转发：

- *PA-220* 系列
- *PA-800* 系列
- *PA-3200*

启用此选项后，防火墙将 Bonjour 流量重定向到已启用此选项的第 3 层和 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，如果希望特定第 3 层接口将 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-400	*N/A*
PA-800	*200*
PA-3200	*500*

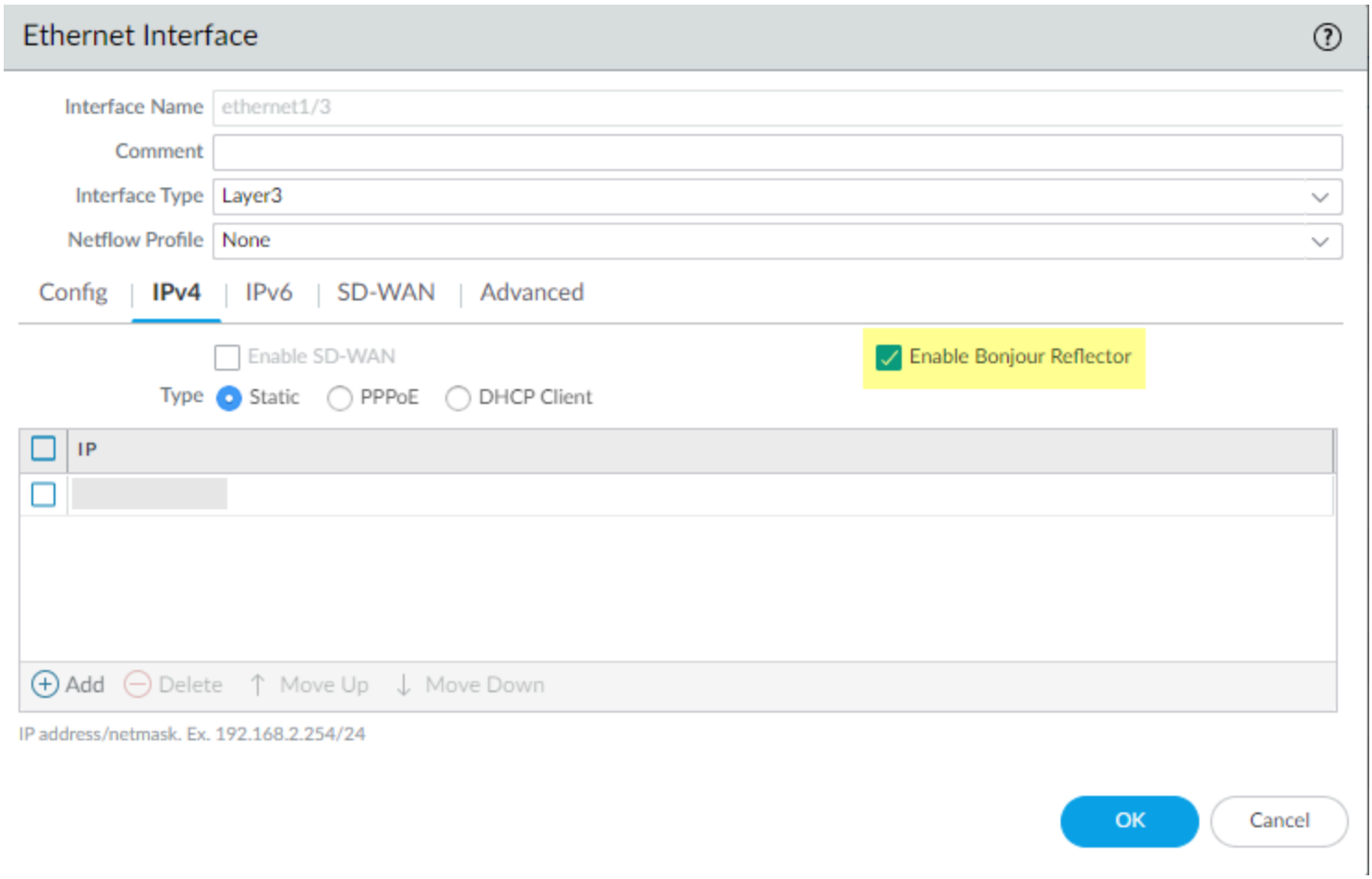
STEP 1 | 选择 **Network**（网络） > **Interfaces**（接口）。

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。

 ©2024 Palo Alto Networks, Inc.



STEP 4 | 单击 **OK**（确定）。

STEP 5 | 针对想要转发 Bonjour 流量的所有第 3 层 (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 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
```

 ©2024 Palo Alto Networks, Inc.

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：
     - **Captive Portal**（强制网络门户）—为了提供强制网络门户响应页面，防火墙将端口在第 3 层接口上保持打开状态：6081 用于透明模式下的强制网络门户，6082 用于重定向模式下的强制网络门户。有关详细信息，请参阅身份验证策略和身份验证门户。
     - **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**（用户标识）—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）。

 ©2024 Palo Alto Networks, Inc.

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。
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）。

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

虚拟路由器

了解防火墙上的虚拟路由器如何参与第 3 层路由并配置虚拟路由器。

- 虚拟路由器概述
- 配置虚拟路由器

虚拟路由器概述

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）来获取其他子网的第 3 层路由。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。

您可以在每个虚拟路由器中配置一个回环接口，在两个回环接口之间创建一个静态路由，然后配置一个动态路由协议在这两个接口之间对等，从而配置从一个虚拟路由器到另一个虚拟路由器的动态路由。防火墙仅支持在虚拟路由器之间有一个跃点。例如，对于虚拟路由器 A、B 和 C，路由不能从 A 到 B 再到 C，而必须直接从 A 到 C。

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。

©2024 Palo Alto Networks, Inc.

配置虚拟路由器

在防火墙上创建虚拟路由器以参与第 3 层路由。

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。

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。

在 PAN OS 11.0.1 和更高版本 11.1 中，对于以太网接口，您可以在子接口上配置 PPPoE 客户端。

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

服务路由

了解防火墙如何使用服务路由向外部服务发送请求并配置服务路由。

- 服务路由概述
- 配置服务路由

服务路由概述

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对防火墙进行全局 配置服务路由或为虚拟系统自定义服务路由，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。

 ©2024 Palo Alto Networks, Inc.

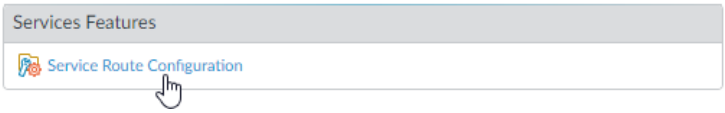
配置服务路由

通过以下步骤，可以配置服务路由，以更改防火墙用于向外部服务（如 Palo Alto Network 云服务）发送请求或用于日志转发的接口。对于高可用性(HA) 配置中的防火墙，服务路由配置在 HA 对等体之间同步

对于主动/被动高可用性(HA)防火墙，为利用外部服务或日志转发而配置的服务路由仅能在主动 HA 对等体上发现活动，而如果您将以太网接口配置为 **Source Interface**（源接口），则被动 HA 对等体将不能发现任何活动。例如，用 Ethernet 1/3 作为源接口配置一个服务路由，以将日志转发到 Cortex 数据湖。在此情境中，所有日志都从主动 HA 对等体转发，但没有日志（包括系统日志和配置日志）从被动 HA 对等体转发。但是，如果将 MGT 接口配置为服务路由的**Source Interface**（源接口），则活动同时发生在主动和被动 HA 对等体上。

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。如果已在选定接口上配置了地址对象，则也可以将其引用为源地址。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。

       服务路由源地址不会从引用的接口继承配置更改，反之亦然。将接口 *IP* 地址修改为不同的 *IP* 地址或地址对象不会更新相应的服务路由源地址。这可能会导致提交失败，并要求您将服务路由更新为有效的源地址值。
     - 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。

 ©2024 Palo Alto Networks, Inc.

- 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 | **Commit**（提交）。

 ©2024 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 对等体之间的 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。

©2024 Palo Alto Networks, Inc.

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：

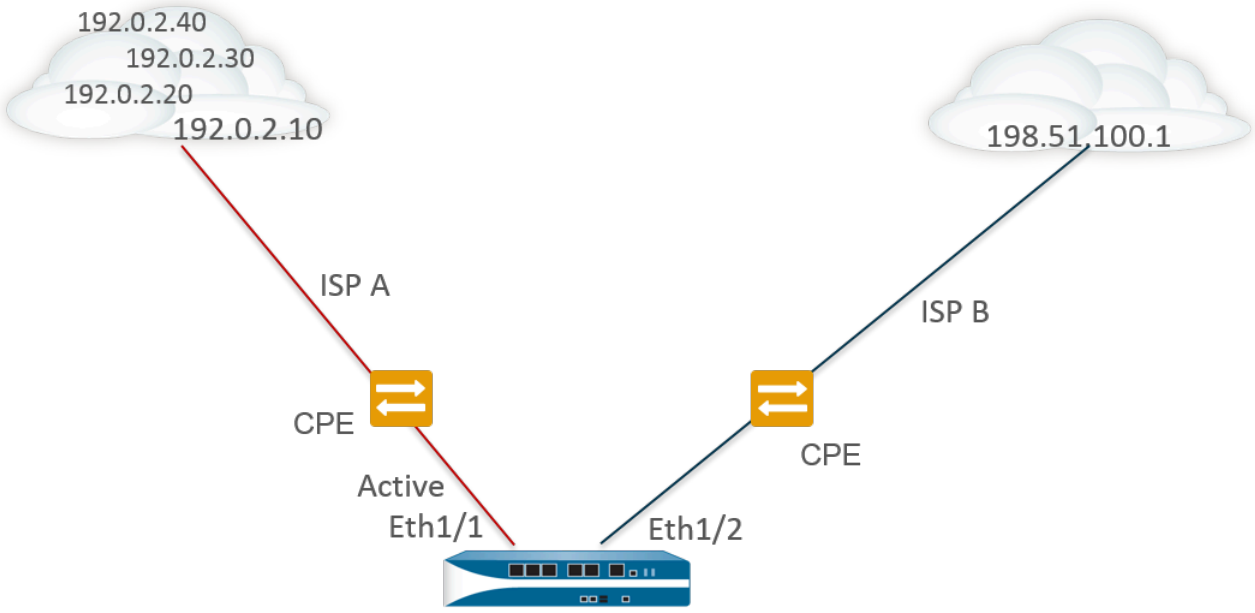
- 静态或默认路由。
- 已重新分发到路由协议的静态或默认路由。
- 其中一个对端不支持 BFD 时的静态或默认路由。（最佳实践是请勿在单个接口上同时启用 BFD 和路径监控。）
- 不使用 PBF 路径监控的静态或默认路由，不会从 RIB、FIB 或重新分发策略中删除发生故障的静态路由。

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。

©2024 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 remove
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。
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。

 ©2024 Palo Alto Networks, Inc.

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. 为路由添加名称（最多 63 个字符）。名称必须以字母数字字符开头，可以由字母数字字符、下划线(_)、连字符(-)、句点(.)和空格组合而成。
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。

     在防火墙上为虚拟路由器配置静态路由时，可以输入下一个跃点路由器的 *IP* 地址。*Palo Alto Networks* 防火墙将下一个跃点 *IP* 地址视为地址对象。因此，如果您将下一个跃点 *IP* 地址（***Network***（网络） > ***Virtual Router***（虚拟路由器） > ***Static Routes***（静态路由））值配置为与配置的地址对象名称（***Objects***（对象） > ***Addresses***（地址））相同，则对地址对象的任何修改也将反映在下一个跃点 *IP* 地址值中。也就是说，重命名地址对象（***Objects***（对象） > ***Addresses***（地址））也会重命名下一个跃点 *IP* 地址。
   - **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。

 ©2024 Palo Alto Networks, Inc.

- **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。
- 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，以便防火墙可以在静态路由失败时，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。

 ©2024 Palo Alto Networks, Inc.

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）。
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

 ©2024 Palo Alto Networks, Inc.

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）。

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。

 ©2024 Palo Alto Networks, Inc.

RIP

考虑 RIP 是否是适合您网络的路由协议，如果是，请配置 RIP。

- RIP 概述
- 配置 RIP

RIP 概述

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。在配置 RIP 之前，请考虑当需要超过 15 个跃点时，将不会路由流量。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。

 ©2024 Palo Alto Networks, Inc.

配置 RIP

请执行以下步骤以配置 RIP。

STEP 1 | 配置虚拟路由器的常规设置。

STEP 2 | 配置 RIP 的常规配置设置。

1. 选择一个虚拟路由器（**Network**（网络） > **Virtual Routers**（虚拟路由器）），然后为该虚拟路由器选择 **RIP**。
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 Default Route**（通告默认路由）可将默认路由通告到具有指定标准值的 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. （可选）要为虚拟路由器全局启用 RIP 的 BFD，请选择 **BFD** 配置文件。
8. 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 计时器的间隔秒数（范围为 1 至 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 至 3,600；默认为 30）。
3. 指定 **Expire Intervals**（到期间隔），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 至 3600，默认为 120）。
4. 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 至 3,600，默认为 180）。

©2024 Palo Alto Networks, Inc.

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

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（范围为 0 至 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。

 ©2024 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

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。

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。

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

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

配置 OSPF

了解OSPF 概念之后，请执行以下步骤来配置 OSPF。

STEP 1 | 配置虚拟路由器的常规设置。

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。

 ©2024 Palo Alto Networks, Inc.

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。
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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

配置 OSPFv3

OSPF 支持 IPv4 和 IPv6。如果使用的是 IPv6，则必须使用OSPFv3。

STEP 1 | 配置虚拟路由器的常规设置。

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）。

©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

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。
     - **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。

©2024 Palo Alto Networks, Inc.

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。

 ©2024 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。

©2024 Palo Alto Networks, Inc.

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。

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）。

©2024 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 Confederations（BGP 联合）、路由翻动惩罚和平滑重启）。
- 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。
- BGP 支持前缀 AS_PATH 列表中最多 255 个 AS 号码。

 ©2024 Palo Alto Networks, Inc.

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：

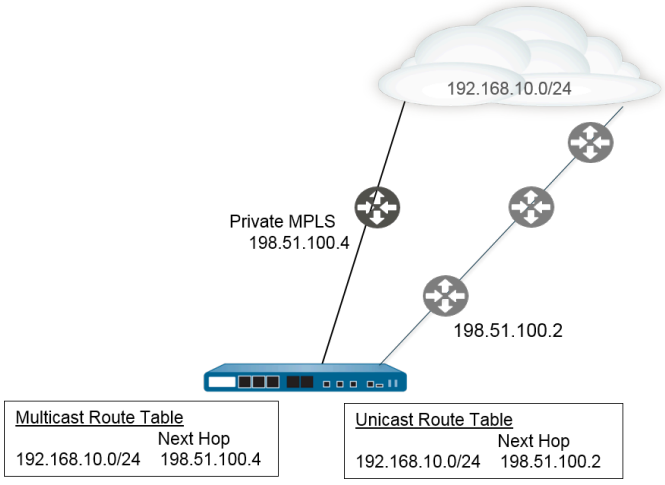
- 地址系列编号中 IANA 定义的地址系列标识符 (AFI)，表示目标前缀是 IPv4 或 IPv6 地址。（PAN-OS 支持 IPv4 和 IPv6 AFI。）
- PAN-OS 中的随后地址系列标识符 (SAFI)，表示目标前缀是单播或多播地址（如果 AFI 为 IPv4），或者目标前缀为单播地址（如果 AFI 为 IPv6）。PAN-OS 不支持 IPv6 多播。

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。

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。



 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

配置 BGP

请执行以下任务以配置 BGP。

STEP 1 | 配置虚拟路由器的常规设置。

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。
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）。

©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

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。
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）。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

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），输入要从对等方导入的 IP 前缀的最大数量（范围是 1 到 100,000）或选择 **unlimited**（无限）。
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。

     选择 ***Disable BFD***（禁用 ***BFD***）可对 *BGP* 对端禁用 *BFD*。
9. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

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（最多 63 个字符）。名称必须以字母数字字符开头，可以由字母数字字符、下划线(_)、连字符(-)、句点(.)和空格组合而成。
2. **Enable**（启用）规则。
3. **Add**（添加）路由器要从中导入的 **Peer Group**（对端组）。
4. 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。
5. 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。
6. 单击 **OK**（确定）。
7. 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。导出规则的名称最多可以包含 31 个字符。

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）。

 ©2024 Palo Alto Networks, Inc.

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。
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。

 ©2024 Palo Alto Networks, Inc.

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，会先检查 BGP 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 号在 AS_PATH 列表中，防火墙不会通告路由。通常接收方会执行循环检测，但这一优化功能会让发送方来执行循环检测。禁用此功能可让接收方执行循环检测。
13. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

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）。
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。

 ©2024 Palo Alto Networks, Inc.

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。

      不支持选择 ***IPv6 Only***（仅 ***IPv6***）的 ***Multicast***（多播）。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 查看路由表。

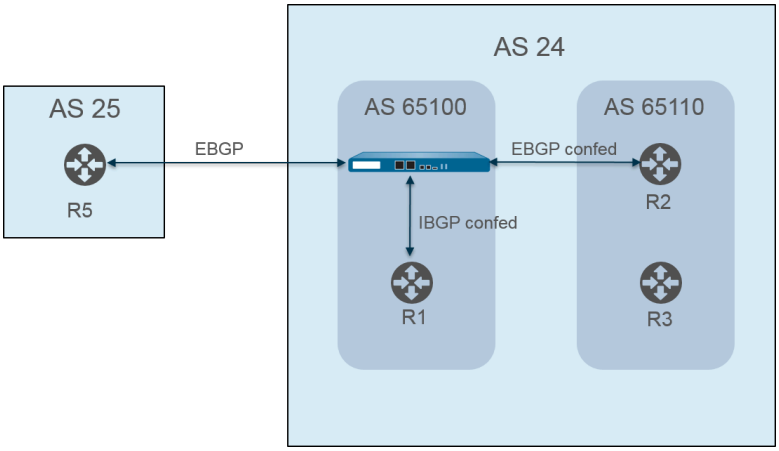
1. 选择**Network**（网络） > **Virtual Routers**（虚拟路由器）。
2. 在虚拟路由器的行中，单击 **More Runtime Stats**（更多运行时统计数据）。
3. 选择 **Routing**（路由） > **Route Table**（路由表）。
4. 对于 **Route Table**（路由表），请选择 **Unicast**（单播）或 **Multicast**（多播），仅显示那些路由。
5. 对于 **Display Address Family**（显示地址系列），请选择 **IPv4 Only**（仅 **IPv4**）、**IPv6 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。

 ©2024 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。



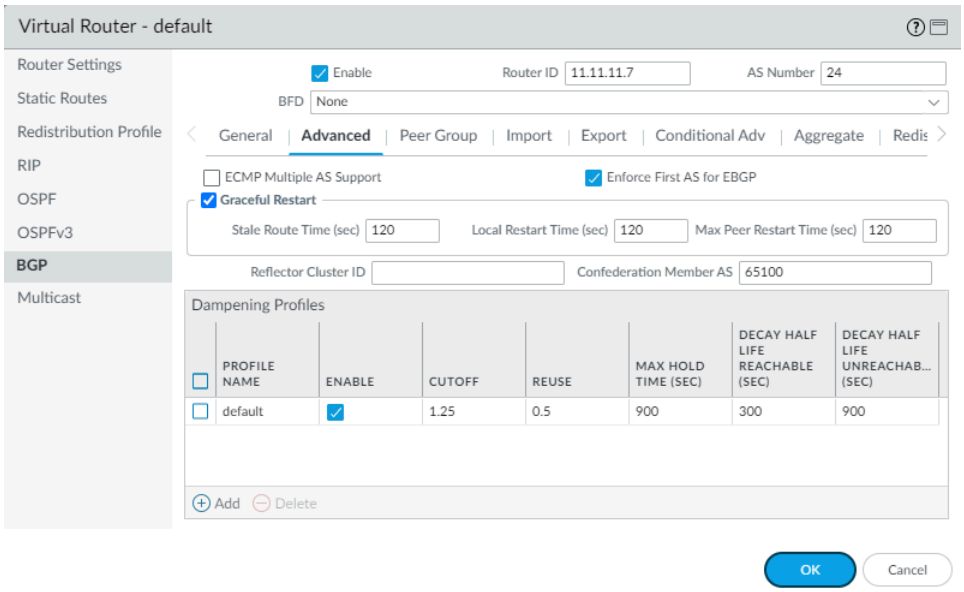
自治系统使用公共（全局分配的）AS 编号进行标识，例如上图中的 AS24 和 AS25。在 PAN-OS 环境中，您可以为每个子自治系统分配一个唯一的“联合会员 AS”编号，这也是仅在 AS 内可见的专用编号。在该图中，联合编号为 AS 65100 和 AS 65110。（自治系统 (AS) RFC6996 保留以供专用，表示 IANA 将 AS 编号 64512-65534 保留供专用。）

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

 ©2024 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

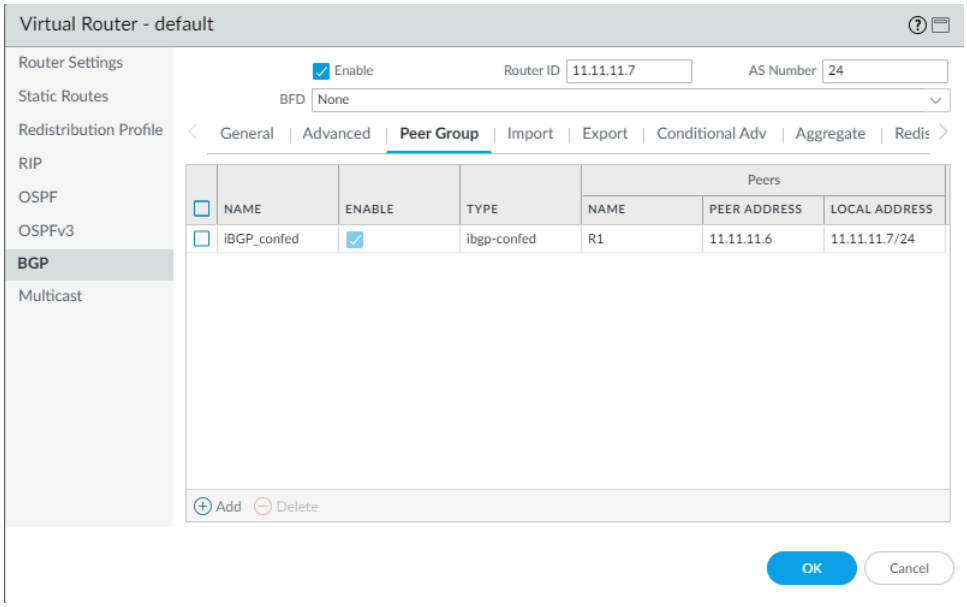
R5 配置如下：

- AS — 25

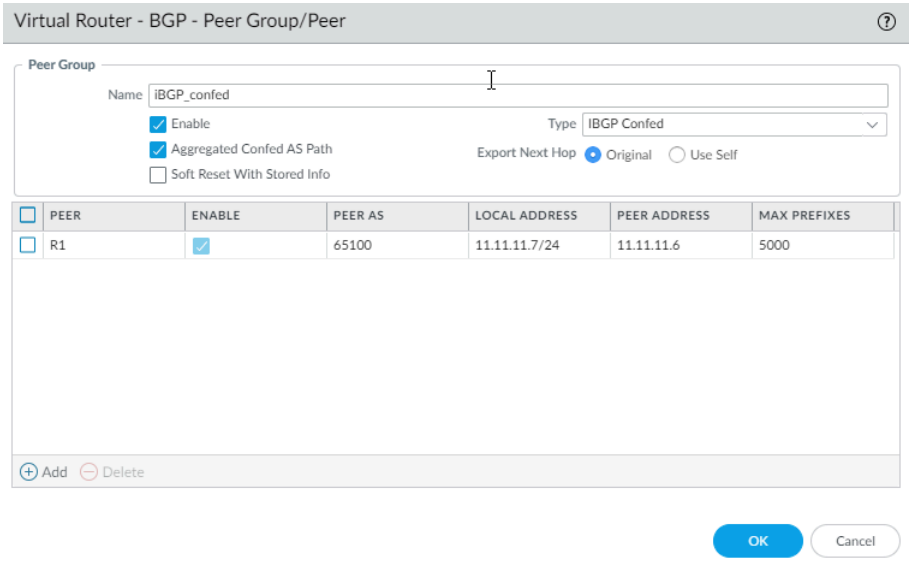
 ©2024 Palo Alto Networks, Inc.

- 对等类型 —EBGP
- 对等 AS — 24

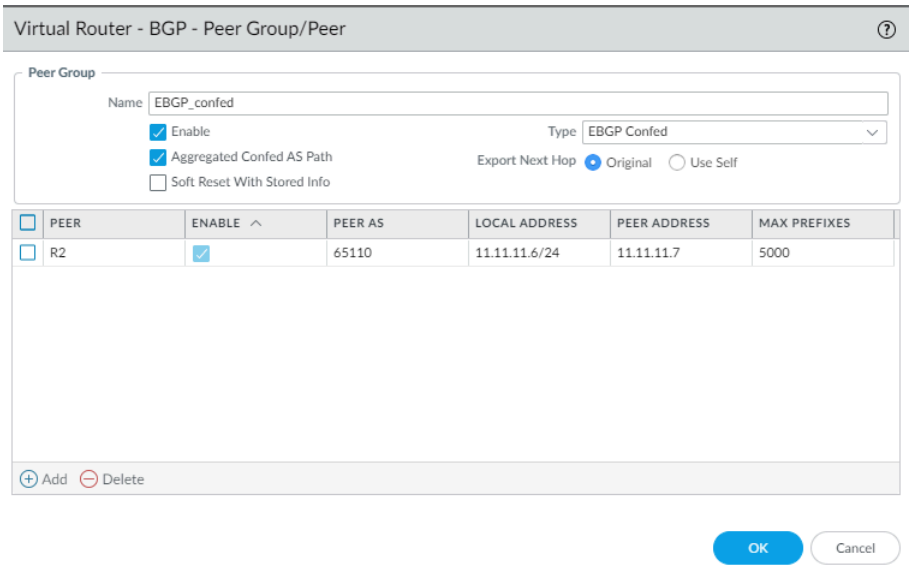
防火墙配置为与 R1、R2 和 R5 对等后，其对等体出现在 **Peer Group**（对等组）选项卡上：

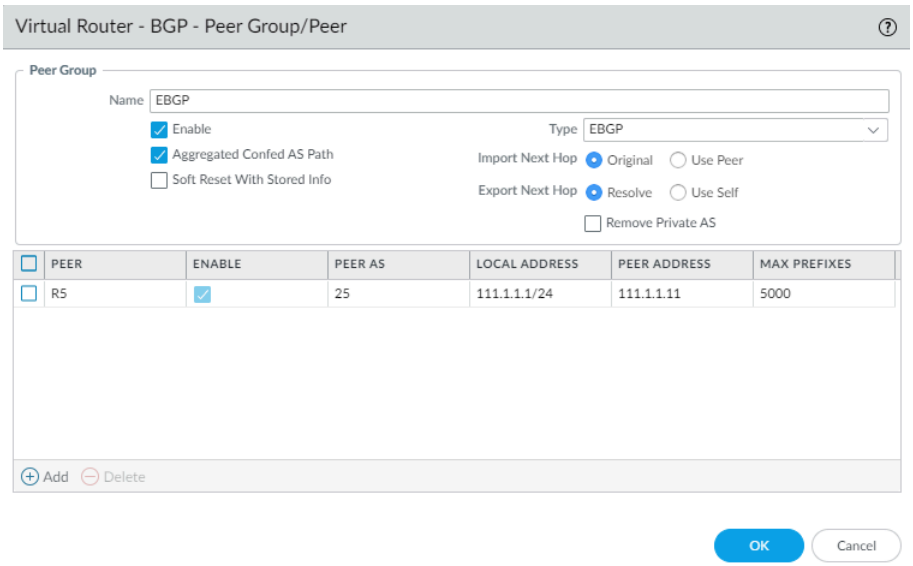


防火墙显示 R1、R2 和 R5 对等体：



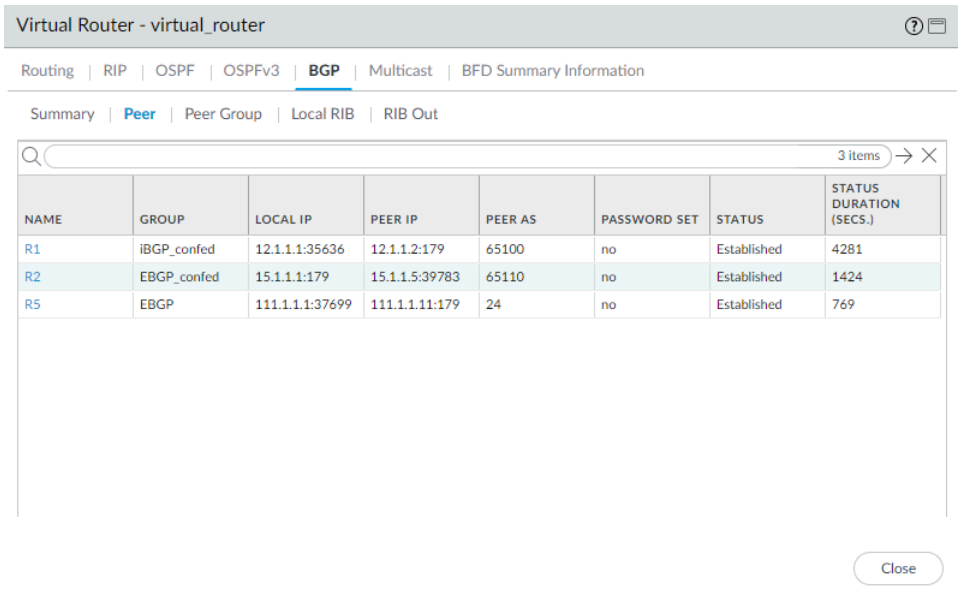
 ©2024 Palo Alto Networks, Inc.



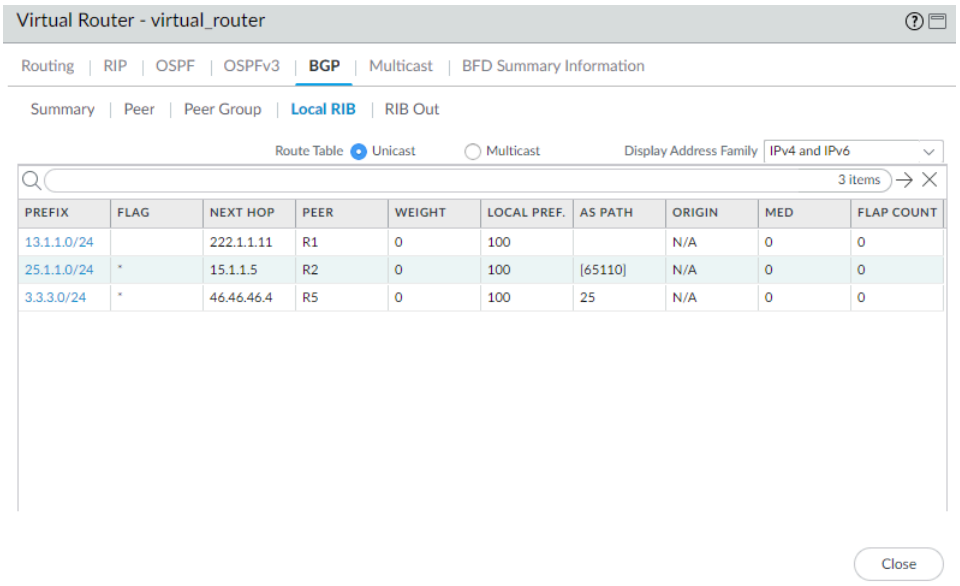


要验证是否已建立从防火墙到对等体的路由，请在虚拟路由器屏幕上选择 **More Runtime Stats**（更多运行时统计数据），然后选择 **Peer**（对等设备）选项卡。

 ©2024 Palo Alto Networks, Inc.

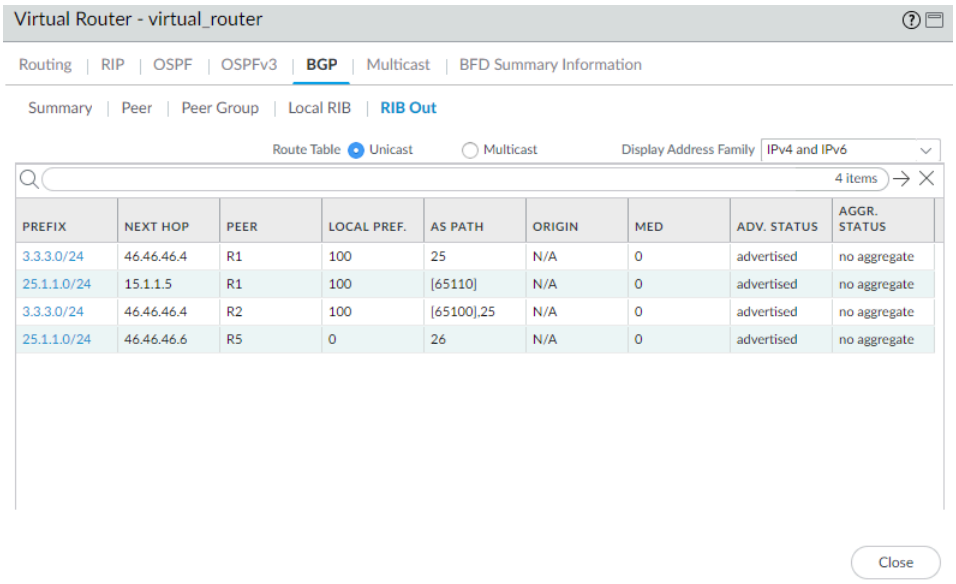


选择 **Local RIB**（本地 **RIB**）选项卡以查看有关路由信息库 **(RIB)** 中存储的路由信息。



然后选择 **RIB Out**（**RIB** 输出）选项卡。

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

 ©2024 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。

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。

 ©2024 Palo Alto Networks, Inc.

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。虚拟路由器（位于旧版路由引擎上）和逻辑路由器（位于高级路由引擎上）都支持 PIM。

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。可以通过调整特定源的地址空间来覆盖默认 SSM 地址空间 (232.0.0.0/8)。组权限也需要进行调整。

在 Palo Alto Networks 防火墙上 Configure IP Multicast（配置 IP 组播）时，即使是在面向接收器的接口，也必须启用接口的 PIM 以转发组播流量。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。）

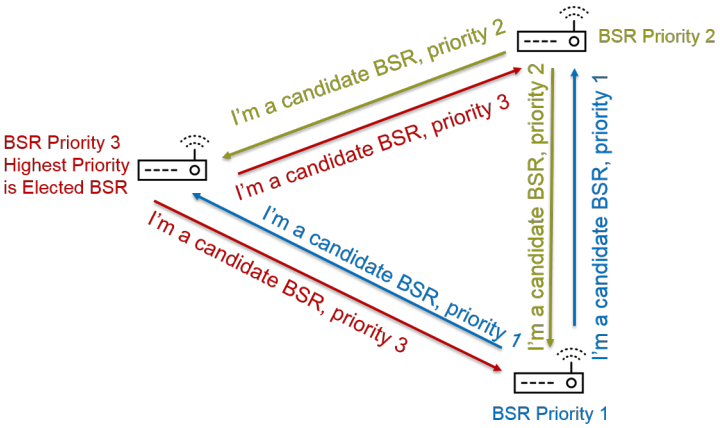
在 ASM 环境中，虚拟路由器可采用两种方式确定哪一个路由器是多播组的 RP：

- 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。

 ©2024 Palo Alto Networks, Inc.

- 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：

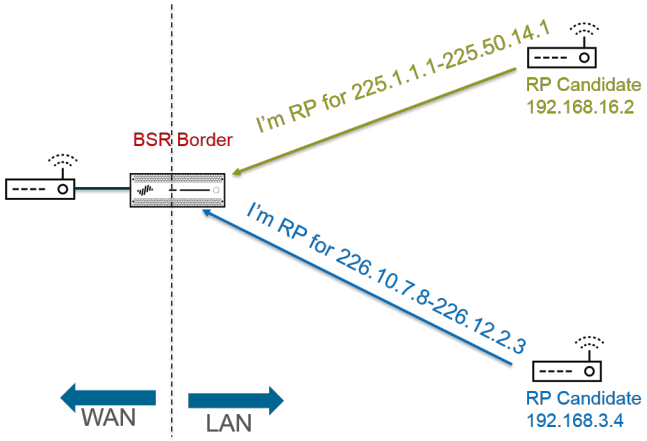
RPs Advertise Their BSR Candidacy; Highest Priority Wins



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。

BSR Border Router Discovers RPs;
Keeps PIM RP Candidacy Messages Within LAN



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

 ©2024 Palo Alto Networks, Inc.

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。

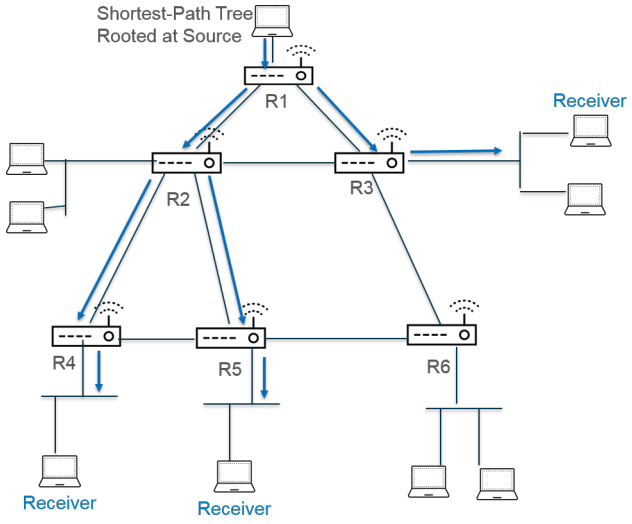
您可以指定接口组将运行用于与虚拟路由器对等的 PIM 邻居（路由器）的 IP 地址。默认情况下，启动了 PIM 的路由器可以是 PIM 邻居，但限制邻居的选项可提供保护 PIM 环境中虚拟路由器的一步。

- 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：

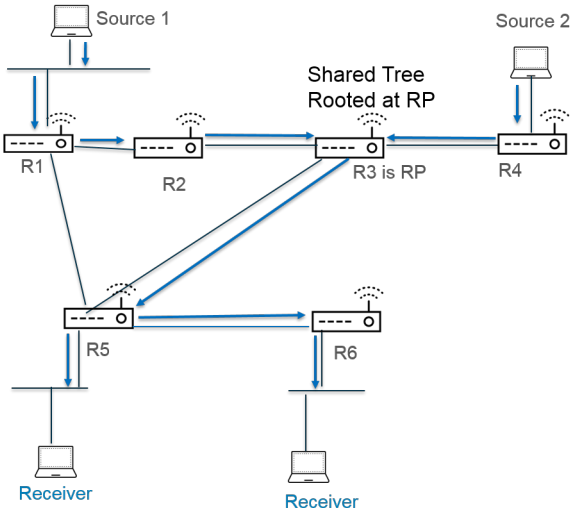
- 源树 — 通过网络从多播源（树根）到多播组内接收器的一条路径。源树是多播数据包从源到接收器采用的最短路径，因此，也称为最短路径树 **(SPT)**。发送方和接收方注释为源和多播组对，缩写为 (S, G)；例如 (192.168.1.1, 225.9.2.6)。下图说明了从源到三个接收器的三个最短路径树。



- 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

 ©2024 Palo Alto Networks, Inc.

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。

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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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。

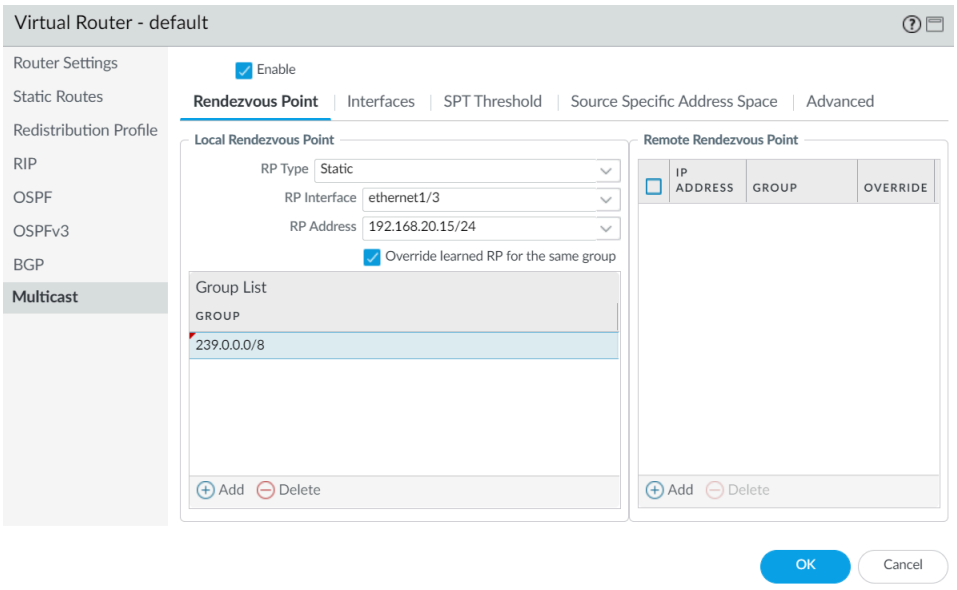
1. 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。
2. 选择 **Multicast**（多播），并 **Enable**（启用）IP 多播。

 ©2024 Palo Alto Networks, Inc.

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））：

   - **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。

 ©2024 Palo Alto Networks, Inc.

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）。

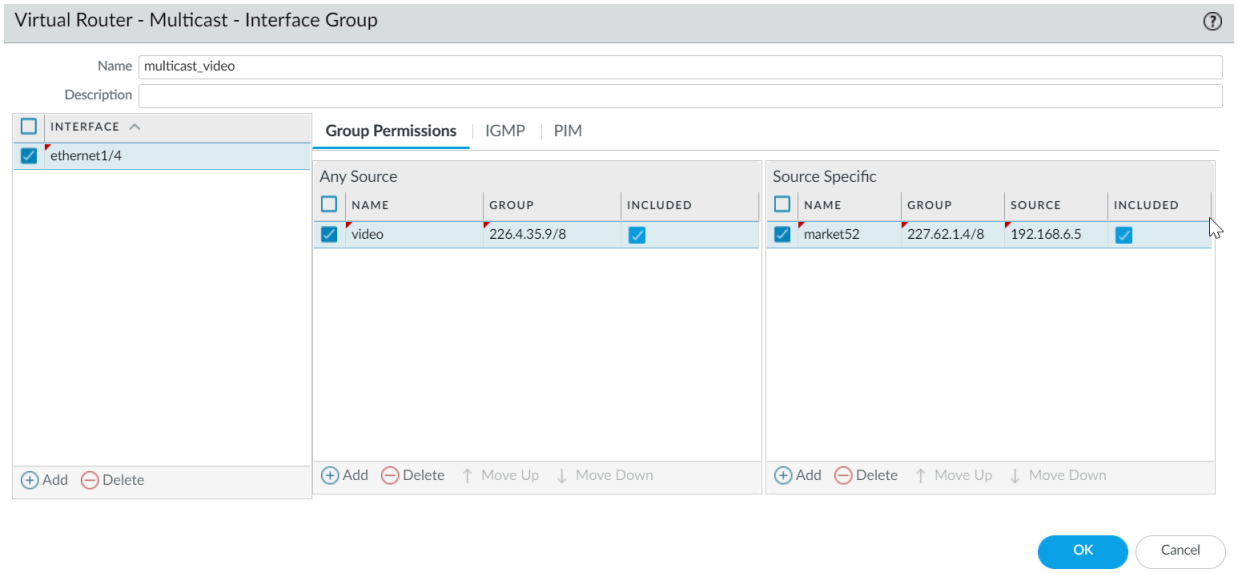
1. 在 **Interfaces**（接口）选项卡上，**Add**（添加）接口组 **Name**（名称）。
2. 输入 **Description**（说明）。
3. **Add**（添加） **Interface**（接口），并选择属于接口组的一个或多个第三层接口。

 ©2024 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）。



 ©2024 Palo Alto Networks, Inc.

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））。
   - **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”。

 ©2024 Palo Alto Networks, Inc.

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 1 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 4,294,967,295；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。

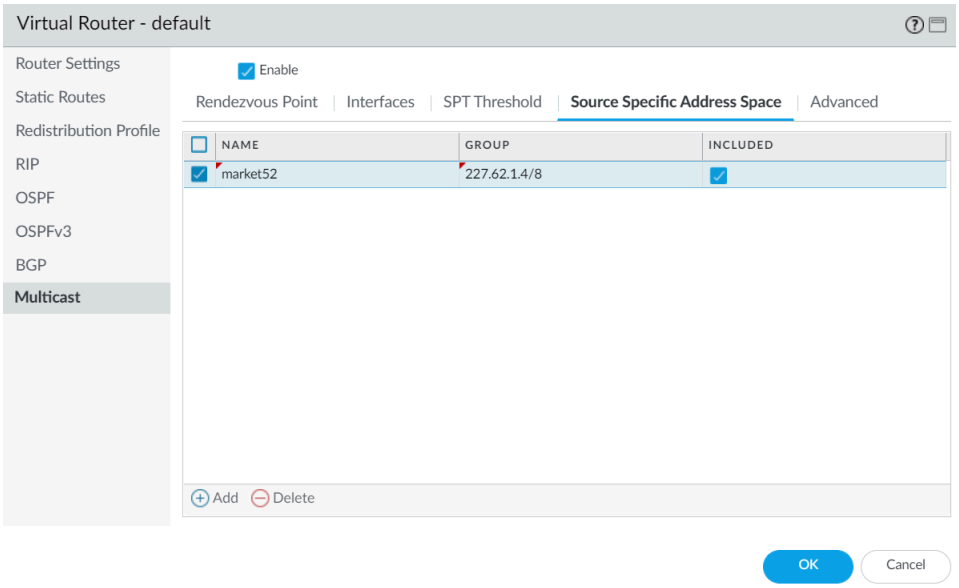
STEP 8 | （可选）根据最短路径树 (SPT) 和共享树更改最短路径树 (SPT) 阈值。

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。

 ©2024 Palo Alto Networks, Inc.

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。
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

 ©2024 Palo Alto Networks, Inc.

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。

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。

©2024 Palo Alto Networks, Inc.

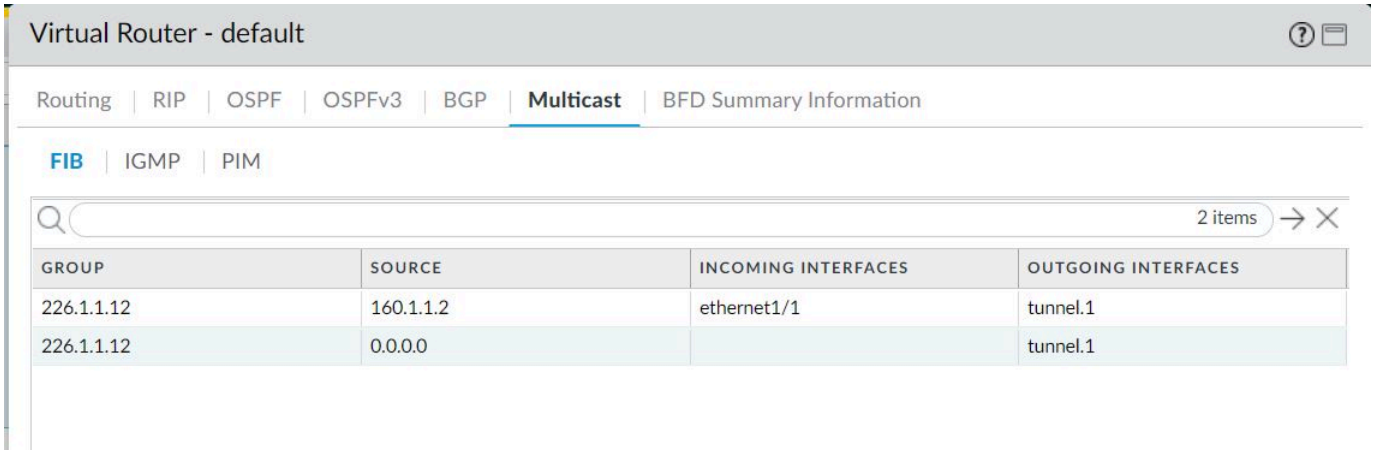
查看 IP 多播信息

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。

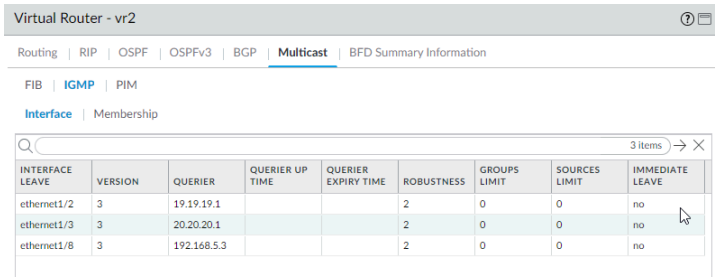
 ©2024 Palo Alto Networks, Inc.

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）。

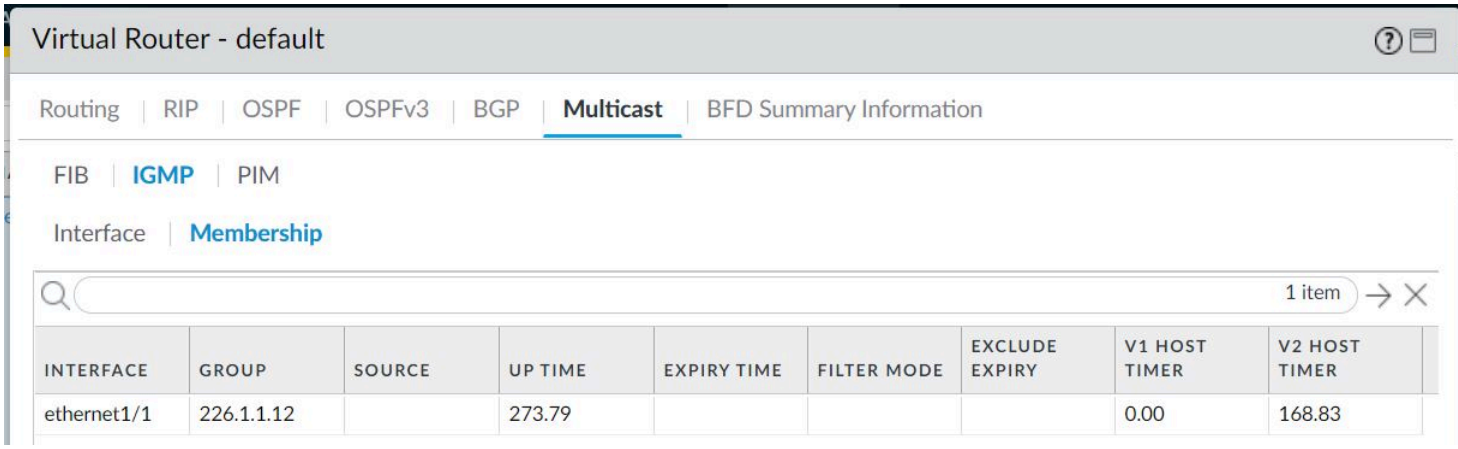
1. 选择 **Routing**（路由） > **Route Table**（路由表），然后选择 **Multicast**（多播）单选按钮，以便仅显示多播路由（目标 IP 多播组、指向该组的下一个跃点以及传出接口）。此信息来自 mRIB。
2. 选择 **Multicast**（多播） > **FIB** 以查看源自 mFIB 的多播路由信息：虚拟路由器所属的多播组、相应的源、传入接口以及指向接收器的传出接口。



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。

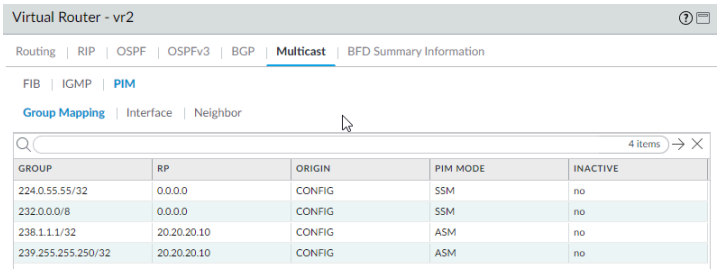


4. 选择 **Multicast**（多播） > **IGMP** > **Membership**（成员关系）以查看基于 IGMP 的接口和其所属的多播组、源以及其他 IGMP 信息。

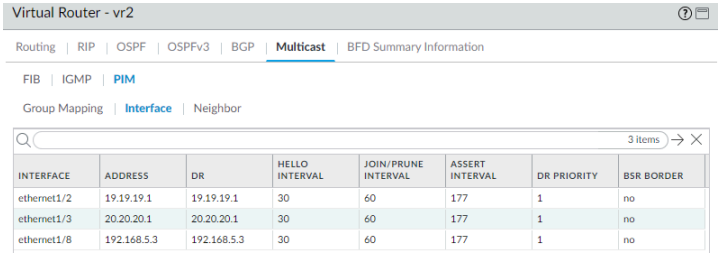


 ©2024 Palo Alto Networks, Inc.

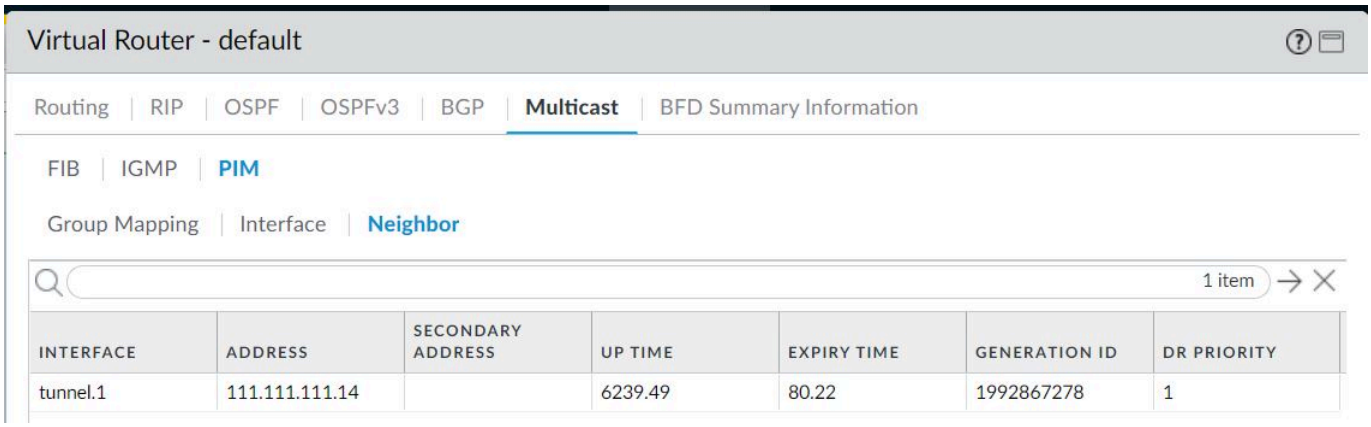
5. 选择 **Multicast**（多播） > **PIM** > **Group Mapping**（组映射）以查看映射到 RP 的多播组、RP 映射的来源、组的 PIM 模式（ASM 或 SSM）以及组是否未激活。SSM 模式下的组不会使用 RP，因此，RP 地址显示为 0.0.0.0。默认 SSM 组为 232.0.0.0/8。



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。



 ©2024 Palo Alto Networks, Inc.

路由重新分发

了解并配置路由重新分发以提高网络流量的可访问性。

- 路由重新分发概述
- 配置路由重新分发

路由重新分发概述

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。

要配置路由重新分发，请先创建一个重新分发配置文件。

©2024 Palo Alto Networks, Inc.

配置路由重新分发

请执行以下步骤以配置路由重新分发。

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）。

 ©2024 Palo Alto Networks, Inc.

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。
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）。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

 ©2024 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）。

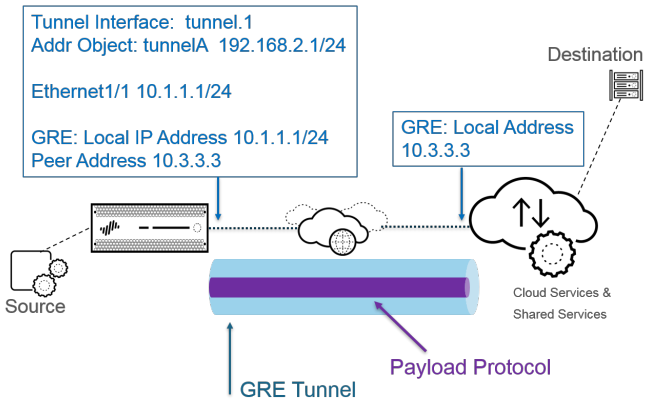
- GRE 隧道概述
- 创建 GRE 隧道

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)。

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：

 ©2024 Palo Alto Networks, Inc.

- 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，我们建议您设置 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。

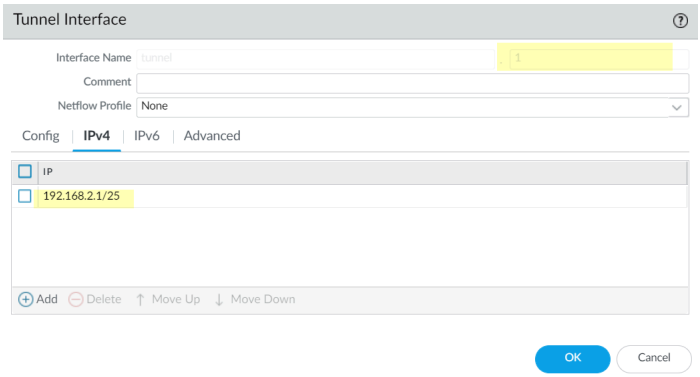
 ©2024 Palo Alto Networks, Inc.

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`**。
   - (仅限 IPv6) 在 **IPv6** 选项卡中，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**（默认的 **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）。

©2024 Palo Alto Networks, Inc.

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。
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）。

 ©2024 Palo Alto Networks, Inc.

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传出 **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**

 ©2024 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
- 防火墙作为 DHCPv6 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 DHCPv4 客户端
- 使用前缀委派将接口配置为 DHCPv6 客户端
- 将管理接口配置为 DHCP 客户端
- 配置用于动态 IPv6 地址分配的管理接口
- 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）。服务器发送到客户端的DHCP 消息将发送到端口 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。

防火墙还可以充当 DHCPv6 客户端，使用或不使用前缀委派。

该防火墙支持 DHCPv4 服务器和 DHCPv6 中继。

DHCP 服务器的 Palo Alto Networks 实施仅支持 IPv4 地址。其 DHCP 中继实施支持 IPv4 和 IPv6。DHCP 客户端支持 IPv4 和 IPv6 地址。DHCP 客户端在高可用性主动/主动模式下不受支持。

防火墙上的管理接口同时支持 DHCP 客户端和动态 IPv6 地址分配。

 ©2024 Palo Alto Networks, Inc.

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：

- 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。

  防火墙还可以充当 DHCPv6 客户端。

从 PAN-OS 11.1.4 及更高版本开始，防火墙支持采用不同逻辑路由器的第 3 层接口上的重复（重叠）IPv4 和 IPv6 地址。在启用重复 IP 地址支持和配置重叠 IP 地址之前，请先了解此功能。

©2024 Palo Alto Networks, Inc.

防火墙作为 DHCPv6 客户端

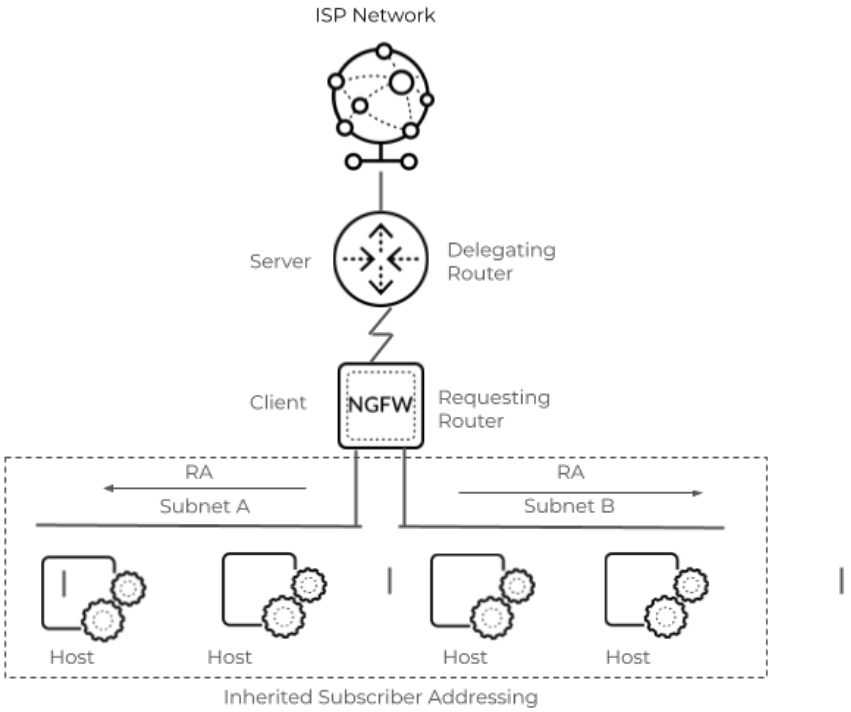
防火墙可以充当 DHCPv6 客户端，从 DHCPv6 服务器请求其接口的 IPv6 地址以及 IPv6 前缀和相关选项（例如 DNS 和域搜索列表），从而提供第 3 层以太网、VLAN 或聚合以太网 (AE) 接口。启用 IPv6 的接口向委派路由器发送路由器请求消息以获取附加信息，例如网关。DHCPv6 客户端减少了您的 IPv6 地址配置工作和潜在错误，并自动执行将您的主机连接到网络的任务。

此外，DHCPv6 客户端防火墙支持前缀委派。ISP 将前缀（前缀长度从 /48 到 /64）分配给 DHCPv6 服务器，而 DHCPv6 服务器又将前缀分配给 DHCPv6 客户端防火墙。然后，防火墙将委派前缀的前缀池中的一个子网分配给一个或多个面向主机的接口。委派接口使用带有 SLAAC 的邻居发现协议 (NDP) 将地址从委派池分发到本地网络。委派接口还使用 NDP 提供其他参数。如果有主机连接到需要动态 IPv6 寻址的防火墙，请配置前缀委派。前缀委派简化了面向客户的 LAN 网络上的网络配置。

要配置面向网络上主机的防火墙接口，请将接口类型配置为 **inherited**（继承）。只有继承的接口才能将那些从前缀池中选择的前缀通告给主机（通过 RA）。每台主机使用委派前缀及其 MAC 地址或 EUI-64（扩展唯一标识符）构建自己的 IPv6 地址，由主机自行决定。只有前缀被委派（继承），而不是完整地址。

DHCPv6 的功能与 *DHCPv4* 不同，因为防火墙不会接收完整的 *IPv6* 地址来分配给主机。防火墙不知道主机的完整 *IPv6* 地址。

以下示例拓扑有一个防火墙、防火墙北面的 DHCPv6 服务器和防火墙南面两个 LAN 上的主机。



面向委派路由器的防火墙接口是无状态地址自动配置 (SLAAC) 客户端。面向主机的防火墙接口是 SLAAC 服务器；主机是 SLAAC 客户端。DHCPv6 客户端从前缀池中为继承的接口分配一个 /64

 ©2024 Palo Alto Networks, Inc.

前缀。防火墙使用 SLAAC 在继承的接口上配置 IPv6 地址，并发送带有前缀的 RA 以使用 SLAAC 自动配置主机接口。

RFC 8415 将身份关联 (IA) 定义为分配给客户端的租约集合。DHCPv6 服务器提供：

- IA_NA（非临时地址的身份关联）和 IA_TA（临时 地址的身份关联）用于防火墙分配给面向委派路由器和 ISP 的接口。
- IA_PD （委派前缀的身份关联）用于防火墙分配给前缀池；面向主机的防火墙接口继承前缀。防火墙从池中选择一个前缀并通过 RA 将其分配给主机。主机接收前缀并构建自己的 IPv6 地址。

当您 配置面向 ISP 的防火墙接口 时，您将接口类型配置为 **DHCPv6 Client**（**DHCPv6** 客户端）。防火墙为其接口请求非临时地址或临时地址（或两者）。防火墙每个接口仅支持一个 DHCPv6 服务器。您可以有多个接口，每个接口面向不同的 ISP，这样如果与一个 ISP 的连接断开，您可以访问另一个 ISP。

您在面向 ISP 的接口上配置前缀委派，因为这是面向提供前缀的 DHCPv6 服务器的接口。如果您有多个面向 ISP 的接口，请使用优先级来控制哪个 ISP 向主机提供委派前缀。

如果防火墙是 *IPv6* 流量的最终消费者并且没有连接的 *LAN*，则防火墙可以简单地作为 *DHCPv6* 客户端并且不需要前缀委派。

如果您启用了高级路由，您配置的第 3 层接口将分配给逻辑路由器。

从 PAN-OS 11.1.4 及更高版本开始，防火墙支持采用不同逻辑路由器的第 3 层接口上的重复（重叠）IPv4 和 IPv6 地址。在启用重复 IP 地址支持和配置重叠 IP 地址之前，请先了解此功能。

 ©2024 Palo Alto Networks, Inc.

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： • 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。 • 确认先前分配的地址是否正确（例如，在系统重启之后）。 • 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。
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。

©2024 Palo Alto Networks, Inc.

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。

 ©2024 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** 命令清除过期租期，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。

 ©2024 Palo Alto Networks, Inc.

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（主要和辅助）
44	Windows互联网名称服务 (WINS) 服务器地址（主和辅助）
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

 ©2024 Palo Alto Networks, Inc.

DHCP 选项	DHCP 选项名称
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。 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。

 ©2024 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。

 ©2024 Palo Alto Networks, Inc.

管理接口上的动态 IPv6 寻址

NGFW 上的管理 (MGT) 接口支持动态 IPv6 地址分配。为动态 IPv6 地址分配（而不是静态地址）配置管理接口可以更轻松地在 IPv6 网络中插入和管理防火墙。

有两种寻址类型可供选择：有状态或无状态。在网段上，您可以控制路由器，在其中设置标志以指示 MGT 接口将是以下接口之一：

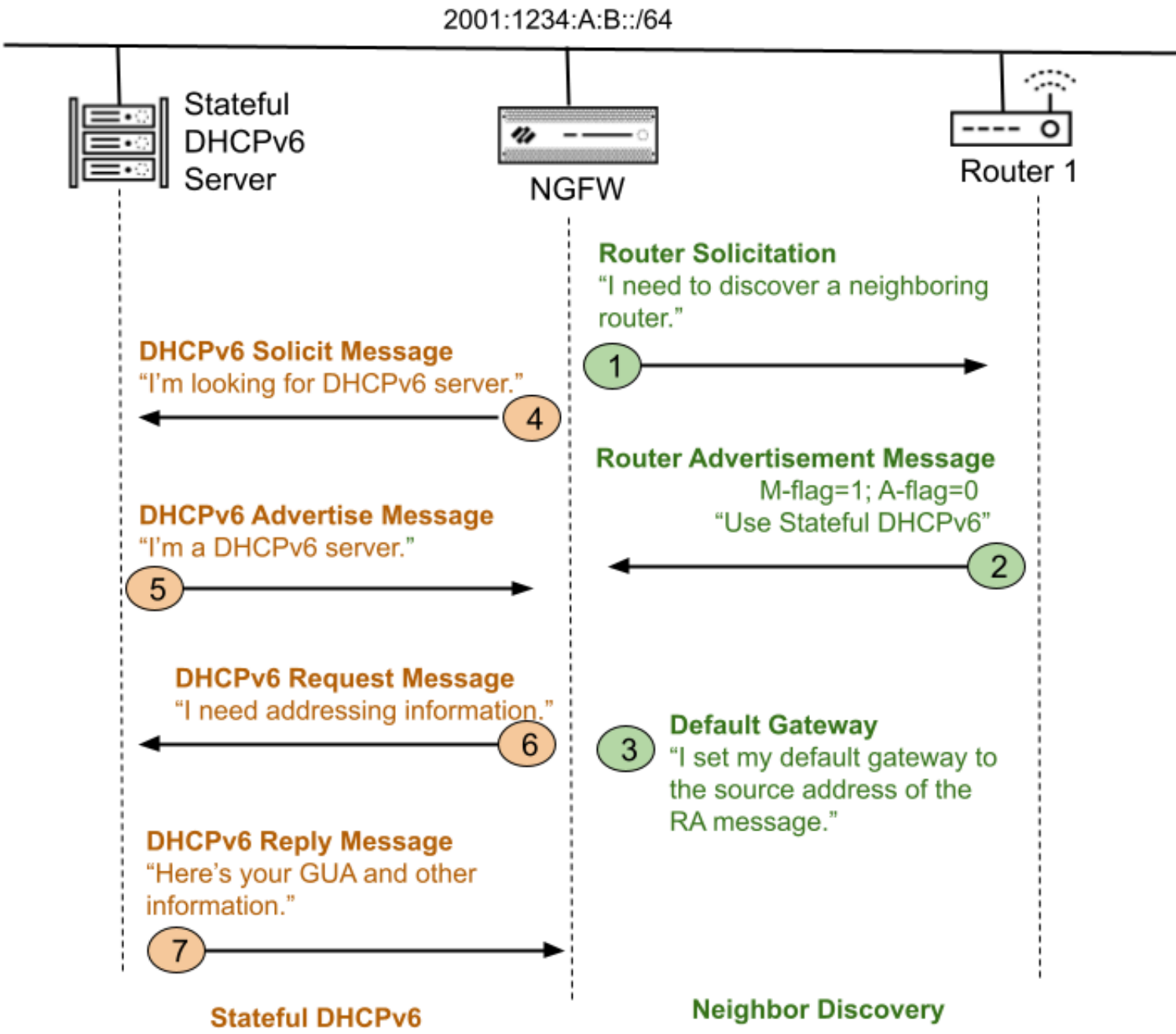
- 有状态 DHCPv6 客户端，此客户端从 DHCPv6 服务器接收其 IPv6 地址、前缀长度和其他配置。
- IPv6 无状态地址自动配置 (SLAAC) 客户端，此客户端自动生成其 IPv6 地址。无状态 IPv6 地址可避免 DHCPv6 服务器必须存储有关客户端的动态状态信息；这在具有大量端点的环境中很有用。

防火墙使用邻居发现协议 (NDP) 向链路上的所有路由器发送路由器请求。链路上的唯一路由器（或首选路由器）会向防火墙发送路由器通告 (RA)，RA 中的标志控制防火墙是使用 SLAAC 还是有状态 DHCPv6 来获取 MGT 接口的动态地址。

但目前的情况是，当在 RA 消息中设置了自治 (A) 标志时，防火墙会同时选择 DHCPv6 地址和 SLAC 地址。理想情况下，防火墙应仅选择 SLAAC 地址，不应发送 DHCPv6 Solicit 消息。由于这个已知问题，如果分段上有 DHCPv6 服务器并且此服务器可以分配 IPv6 地址，则防火墙更倾向于 DHCPv6 地址分配，而不是 SLAAC。

以下示例说明了有状态 DHCPv6 地址分配。

 ©2024 Palo Alto Networks, Inc.



在拓扑示例中，防火墙连接到充当默认网关的路由器。防火墙是连接到 DHCPv6 服务器的 IPv6 SLAAC/DHCPv6 客户端。在 MGT 接口上启用 IPv6，选择动态地址类型和动态默认网关类型并提交后，将发生以下过程。

 ©2024 Palo Alto Networks, Inc.

1. 使用路由器请求 (RS) 和路由器通告 (RA) 进行默认网关分配（图形右侧）。

   主机根据连接到链路的唯一（或首选）路由器的源地址设置其默认网关。防火墙使用邻居发现协议 (NDP) 向链路上的所有路由器发送 RS。如果只有一台路由器连接到链路，则防火墙使用该路由器的 ICMPv6 RA 消息的源地址作为其默认网关地址。如果防火墙从连接到链路的多台路由器接收 RA，则防火墙会默认路由器优先级最高（低、中或高）的 RA 消息的源地址作为其默认网关地址。

   为响应 RS，路由器发送到防火墙的 RA 中的标志会表明防火墙将使用 SLAAC 还是有状态 DHCPv6 来获取管理接口的动态地址，如下所示：

   - 如果 Autonomous（自治，缩写为 A）标志设置为 1，则指示防火墙使用 SLAAC 自动生成全球单播地址 (GUA)。防火墙使用 RA 消息中前缀选项中的前缀以及 MGT 接口的 EUI-64 接口 ID 为 MGT 接口创建 GUA。接口 ID 是根据管理接口的 MAC 地址创建的。（如果此标志设置为 0，则不允许在分段上进行自动配置。）
   - 如果 Other Configuration（其他配置，缩写为 O）设置为 1，则告知防火墙可以从无状态 DHCPv6 服务器获取 DNS 服务器列表和域名（但不能获取寻址信息）。通常 O 标志适用于 SLAAC 自动配置，并且 A 标志和 O 标志都设置为 1。

     目前，*O* 标志（无状态 *DHCPv6*）存在已知问题，此版本不支持 *O* 标志。

   - 如果 Managed（托管，缩写为 M）标志设置为 1，则告知防火墙从有状态 DHCPv6 服务器获取其 IPv6 网络参数（例如其全局地址、DNS 和域名）。防火墙将联系 DHCPv6 服务器以请求 GUA 和其他信息。通常，这意味着不允许在网段上使用 SLAAC 自动寻址，并且 A 标志和 O 标志都设置为 0。

     目前存在一个已知问题：即即使未设置 *M* 标志，防火墙也会发送 *DHCPv6 Solicit* 消息。

   以下步骤对应于图中的注解。

   - 步骤 1—防火墙向所有路由器的已知组播地址 (FF02:: 2) 发送 RS。
   - 第 2 步—作为响应，路由器 1 生成 RA，将 M 标志设置为 1，A 标志设置为 0，向防火墙表明此网段不允许 SLAAC，而是必须使用有状态 DHCPv6 进行寻址和其他配置。
   - 第 3 步—收到 RA 后，防火墙将路由器 1 的源 IPv6 地址设置为其默认网关。由于 A 标志设置为 0，因此防火墙不执行 SLAAC。

 ©2024 Palo Alto Networks, Inc.

2. 使用 DHCPv6 进行动态地址分配（图左侧）。
   - 第 4 步—由于在 RA 中将 M 标志设置为 1，防火墙会据此向所有 DHCPv6 代理的已知多播地址（FF01:: 1:2）发送 DHCPv6 请求消息，从而搜索 DHCPv6 服务器。
   - 第 5 步—收到 Solicit 消息后，服务器将一条 DHCPv6 通告消息单播到防火墙的本地链路地址。
   - 第 6 步—防火墙知道 DHCPv6 服务可用并发送寻址信息请求。
   - 第 7 步—收到请求后，服务器发送 DHCPv6 回复，其中包含 GUA 和所有其他可供分配的信息。（DNS 信息来自 DHCPv4 服务器，而不是 DHCPv6 服务器。）
   - 防火墙对收到的 GUA 执行重复地址检测 (DAD)，以确认 GUA 是唯一的。如果 DAD 确定 IPv6 地址是重复的（无论是 SLAAC、DHCPv6，还是本地链路地址），则接口中不会显示 IPv6 地址。

或者，您可以将路由器 1 配置为使用 IPv6 SLAAC（图中未显示），以进行动态地址分配。在这种情况下，路由器 1 会发送 A 标志设置为 1 的 RA，表示防火墙必须使用 SLAAC 创建 GUA。您可以配置 RA 消息中的 Prefix（前缀）选项以及 A 标志。除 EUI-64 接口 ID 外，防火墙还使用来自 RA 前缀选项的前缀（在示例拓扑中为 2001:1234: A:: /64）来创建一个或多个 GUA。可以基于 MGT 接口 (EUI-64) 的 MAC 地址创建接口 ID。

要将 MGT 接口配置为 DHCPv6 客户端，需要请求非临时或临时地址、快速提交选项、DHCPv6 唯一 ID 类型的类型以及指定静态或动态默认网关地址。

接下来是为动态 IPv6 地址分配配置管理接口。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 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。

 ©2024 Palo Alto Networks, Inc.

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。
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）。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

将接口配置为 DHCPv4 客户端

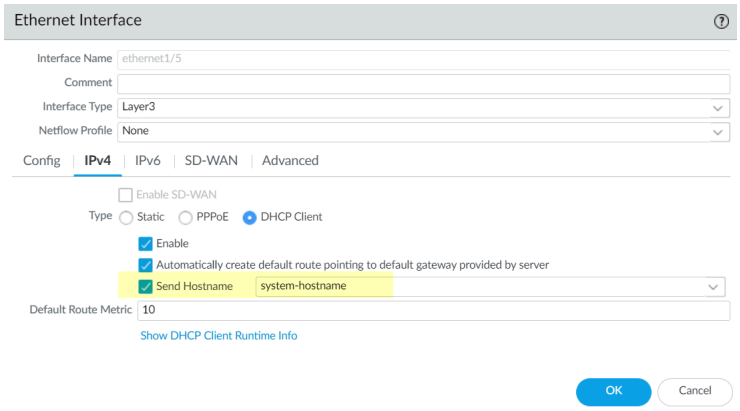
在将防火墙接口配置为 DHCP 客户端之前，请确保您已配置第 3 层接口（Ethernet、Ethernet 子接口、VLAN、VLAN 子接口、聚合或聚合子接口），并确保已将该接口分配给某个虚拟路由器和区域。如果需要使用 DHCP 为接口请求 IPv4 地址，请将接口配置为 DHCP 客户端。

您还可以将管理接口配置为 DHCP 客户端。

如果防火墙接口需要动态 *IPv6* 地址，请 Configure an Interface as a DHCPv6 Client（将接口配置为 DHCPv6 客户端）（使用或不使用前缀委派）。

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 DHCPv4 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

 ©2024 Palo Alto Networks, Inc.

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*。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。

 ©2024 Palo Alto Networks, Inc.

使用前缀委派将接口配置为 DHCPv6 客户端

在配置 DHCPV6 客户端之前，了解防火墙上的第 3 层以太网、VLAN 或 AE 接口如何充当 DHCPv6 客户端，使用或不使用前缀委派。

以下任务首先展示如何将面向 DHCPv6 服务器的接口配置为 DHCPv6 客户端并为其自身请求非临时或临时地址。该接口还代表面向主机的接口请求委派前缀。然后，该任务说明如何将面向主机的接口配置为向 LAN 主机提供前缀委派的 继承 接口。

STEP 1 | 选择以太网、AE 或 VLAN 接口（面向 DHCPv6 服务器和 ISP）作为 DHCPv6 客户端。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 或选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 并选择一个 AE 接口，或选择 **Network**（网络） > **Interfaces**（接口） > **VLAN**。
2. 对于 **Interface Type**（接口类型），请选择 **Layer3**（第 **3** 层）。
3. （可选）如果要将面向 ISP 的单个以太网或 VLAN 接口分成子接口，请 添加子接口 。
4. 在 **Config**（配置） 选项卡上，将接口分配给 **Virtual Router**（虚拟路由器） 和 **Security Zone**（安全区域）。

STEP 2 | 选择 **IPv6**。

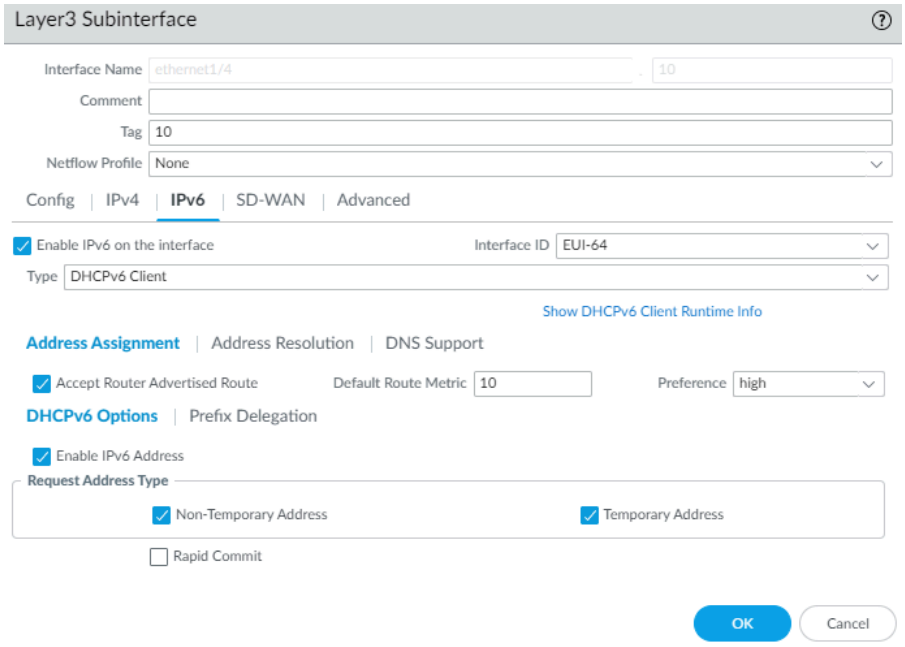
STEP 3 | 在接口上启用 **IPv6**。

STEP 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。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 将面向 ISP 的接口配置为 DHCPv6 客户端，并请求其租用的临时 IPv6 地址和/或非临时 IPv6 地址。

1. 对于 **Type**（类型），选择 **DHCPv6 Client**（**DHCPv6** 客户端）。
2. 选择 **Address Assignment**（地址分配） 和 **Accept Router Advertised Route**（接受路由器通告路由） 以允许 DHCPv6 客户端接受路由器通告。



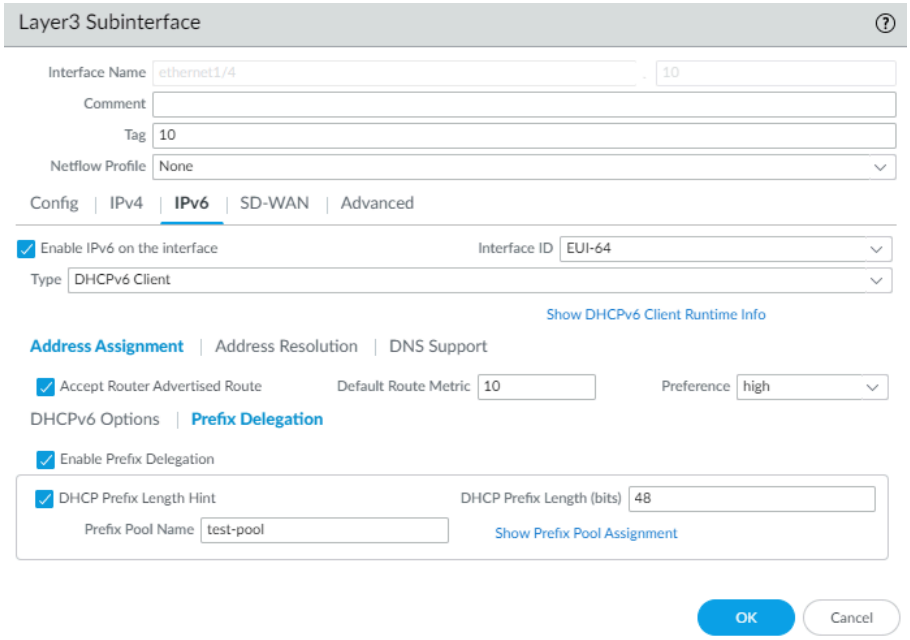
3. 为从接口到 ISP 的路由输入 **Default Route Metric**（默认路由度量） ；范围是 1 到 65,535；默认值为 10。
4. 选择 DHCPv6 客户端接口的 **Preference**（首选项） （低、 中 或 高），这样，如果您有两个接口（每个接口都连接到不同的 ISP 以实现冗余），您可以为一个 ISP 分配比另一个 ISP 接口优先级更高的接口。连接到首选接口的 ISP 将是提供委派前缀以发送到面向主机的接口的 ISP。如果接口具有相同的首选项，则两个 ISP 都会提供一个委派前缀，并且主机决定使用哪个前缀。
5. 选择 **DHCPv6 Options**（**DHCPv6** 选项） 和 **Enable IPv6 Address**（启用 **IPv6** 地址）。
6. 在请求地址类型区域中，选择 **Non-Temporary Address**（非临时地址） （默认设置）。这种地址类型的寿命更长。
7. 选择 **Temporary Address**（临时地址） 以获得更高级别的安全性，因为该地址仅供短期使用。

   您是否为接口请求非临时地址或临时地址取决于您的判断和 *DHCPv6* 服务器的能力；有些服务器只能提供一个临时地址。最佳做法是同时选择非临时地址和临时地址，在这种情况下，防火墙将首选非临时地址。
8. 选择 **Rapid Commit**（快速提交） 以使用 Solicit 和 Reply 消息（两条消息）的 DHCPv6 进程，而不是 Solicit、Advertise、Request 和 Reply 消息（四条消息）的进程。
9. 选择 **Prefix Delegation**（前缀委派） 和 **Enable Prefix Delegation**（启用前缀委派） 以允许防火墙支持前缀委派功能。这意味着接口从上游 DHCPv6 服务器接受前缀并将前缀放入前缀池，防火墙从中通过 RA 将前缀委派给主机。启用或禁用接口前缀委派的能力允许

 ©2024 Palo Alto Networks, Inc.

防火墙支持多个 ISP（每个接口一个 ISP）。在此接口上启用前缀委派控制哪个 ISP 提供前缀。

委派前缀用于面向主机的接口，其 *IPv6* 地址由 *MAC* 地址和 *EUI-64* 输入构成。在我们的示例中，继承接口接收步骤中显示的继承前缀以查看 *DHCPv6* 信息。



10. 选择 **DHCP Prefix Length Hint**（**DHCP** 前缀长度提示） 使防火墙能够将首选的 DHCPv6 前缀长度发送到 DHCPv6 服务器。
11. 输入 48 到 64 范围内的首选 **DHCP Prefix Length (bits)**（**DHCP** 前缀长度（位）），它作为提示发送到 DHCPv6 服务器。DHCPv6 服务器可以自行决定发送它选择的任何前缀长度。

    例如，请求 *48* 的前缀长度会为子网 *(64-48)* 留下 *16* 位，这表明您需要对该前缀进行许多细分才能进行委派。另一方面，请求前缀长度为 *63* 会留下 *1* 位用于仅委派两个子网。在 *128* 位中，还有 *64* 位用于主机地址。

    接口可以接收 */48* 前缀，但委派 */64* 前缀，例如，这意味着防火墙正在细分它委托的前缀。
12. 为防火墙存储接收到的前缀的池输入 **Prefix Pool Name**（前缀池名称）。该名称必须是唯一的，并且最多包含 63 个字母数字字符、连字符、句点和下划线。

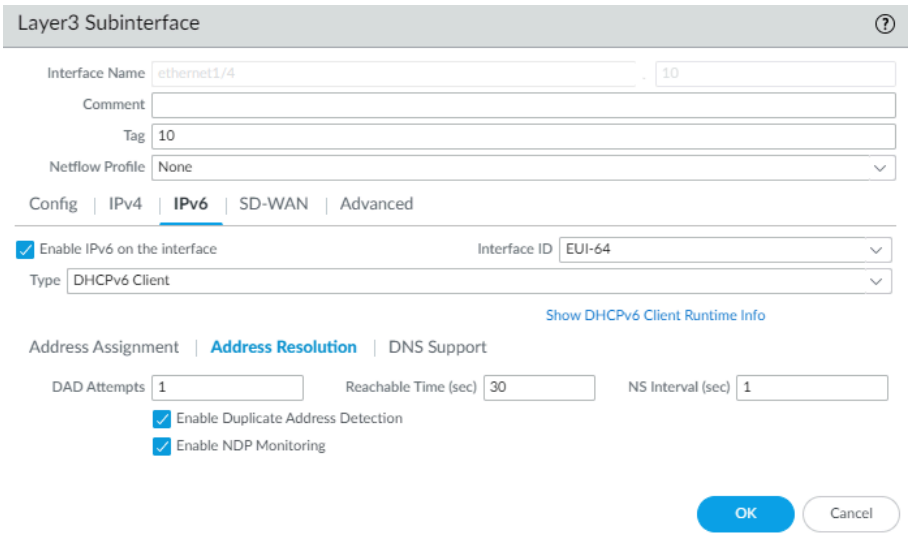
    使用反映 *ISP* 的前缀池名称以便于识别。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 对于 DHCPv6 客户端，配置地址解析。

1. 选择 **Address Resolution**（地址解析）
2. 如果您希望在将潜在 IPv6 地址分配给接口之前验证其唯一性，请**Enable Duplicate Address Detection**（启用重复地址检测）(DAD)（默认情况下启用）。
3. 如果选择 **Enable Duplicate Address Detection**（启用重复地址检测），请指定在尝试识别邻居失败之前邻居请求 (NS) 间隔内的 **DAD Attempts**（**DAD** 尝试） 次数；范围是 1 到 10；默认为 1。
4. 输入 **Reachable Time (sec)**（可达时间（秒）），客户端在收到可达确认消息后假定邻居可达的时间长度；范围是 10 到 36,000；默认值为 30。
5. 输入 **NS Interval (sec)**（**NS** 间隔（秒）），这是邻居请求之间的时间长度；范围是 1 到 3,600；默认为 1。

   使用众所周知的多播组每秒发送一次邻居请求。该接口通过发送 NS 来询问网络上是否存在具有相同 IPv6 地址的设备，在请求中包括它自己的地址。如果另一个设备具有相同的地址，它会响应这些请求。
6. **Enable NDP Monitoring**（启用 **NDP** 监控） 以启用邻居发现协议监控。启用后，您可以选择 NDP 图标（功能列中的 ）并查看信息，如防火墙发现的邻居的 IPv6 地址、相应的 MAC 地址、 用户 ID 和状态（在最佳情况下）。

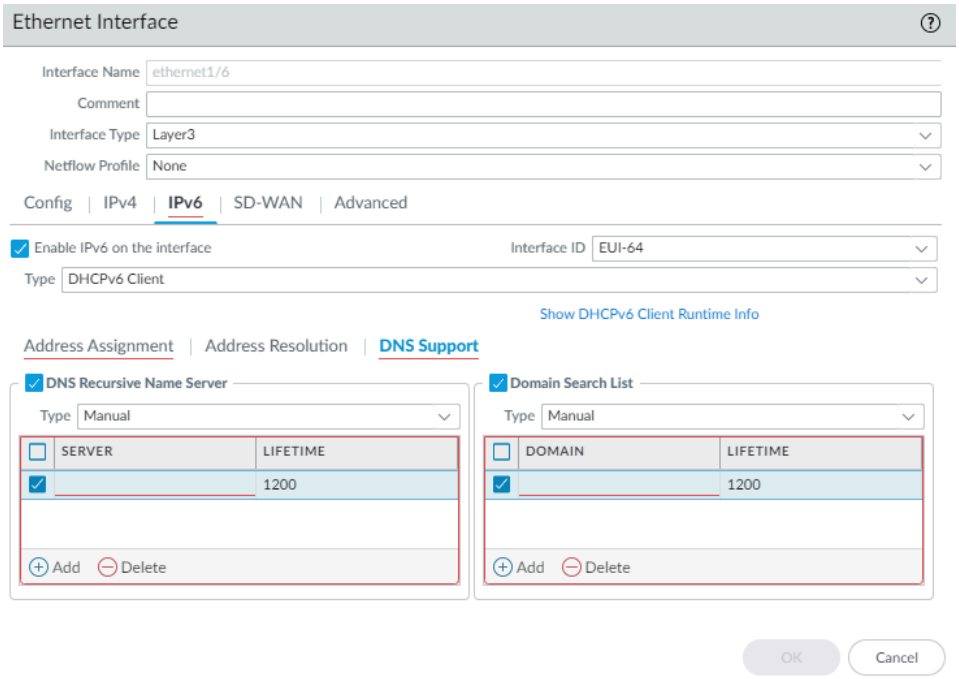


STEP 7 | 对于 DHCPv6 客户端，配置 DNS 支持。

1. 选择 **DNS Support**（**DNS** 支持）。
2. 启用 **DNS Recursive Name Server**（**DNS** 递归名称服务器） 并选择：
   - **DHCPv6**— 让 DHCPv6 服务器向客户端发送 DNS 递归名称服务器信息。
   - **Manual**（手动）— 手动配置 DNS 递归名称服务器。**Add**（添加）**Server**（服务器）的 IPv6 地址，例如 2001:4860:4860:0:0:0:8888。以秒为单位输入 **Lifetime**（生

 ©2024 Palo Alto Networks, Inc.

存时间），这是客户端可以使用特定 DNS 递归名称服务器解析域名的最长秒数。生存时间范围是 4 到 3,600；默认值为 1,200。



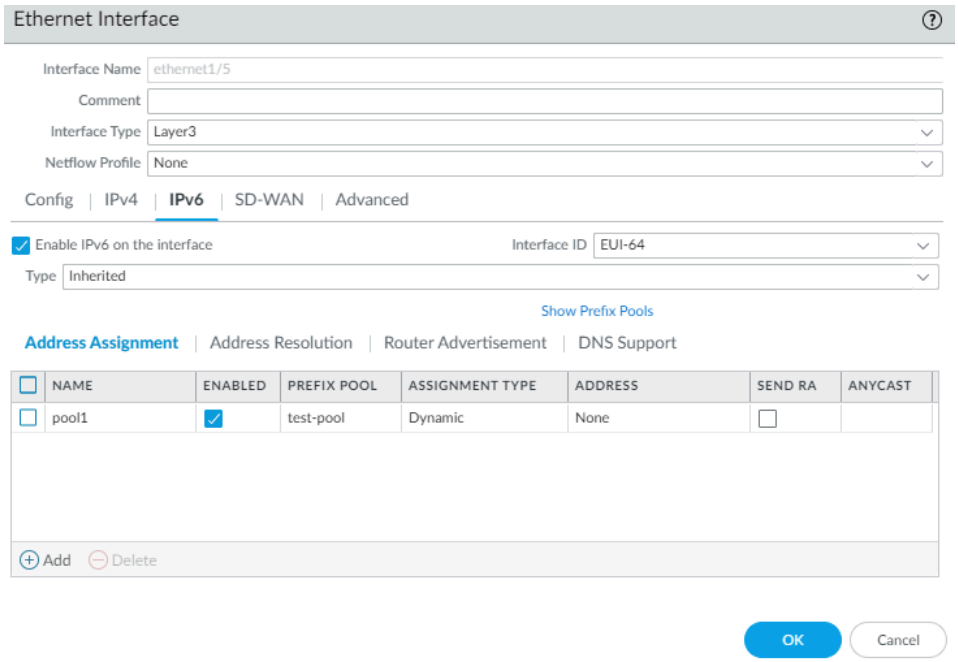
3. 启用 **Domain Search List**（域搜索列表） 并选择：
   - **DHCPv6**— 让 DHCPv6 服务器向客户端发送域搜索列表信息。
   - **Manual**（手动）— 手动配置域搜索列表。**Add**（添加）**Domain**（域） 后缀以添加到 DNS 中的部分名称以形成完全限定域名。例如，输入 company.org。为列表输入以秒为单位的 **Lifetime**（生存时间）；范围是 4 到 3,600；默认值为 1,200。

STEP 8 | 单击 **OK**（确定） 以保存 DHCPv6 客户端配置。

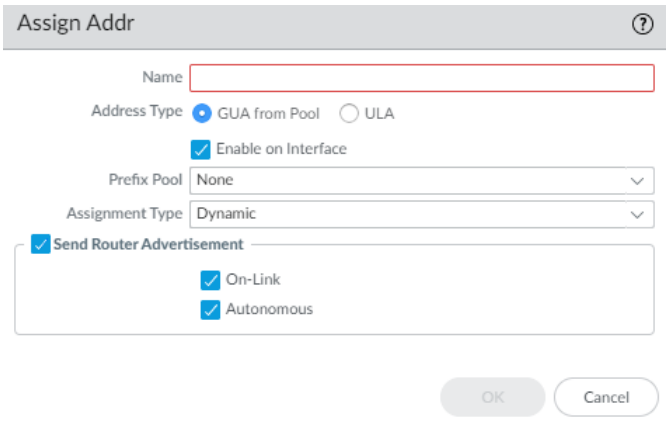
 ©2024 Palo Alto Networks, Inc.

STEP 9 | 配置面向主机的接口以继承 IPv6 前缀并将池中分配的 /64 前缀通告给主机。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 或选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 并选择一个 AE 接口，或选择 **Network**（网络） > **Interfaces**（接口） > **VLAN**。
2. 选择第 3 层接口。
3. 选择 **IPv6**。
4. 在接口上启用 **IPv6**。
5. 对于 **Type**（类型），选择 **Inherited**（继承）。



6. 选择 **Address Assignment**（地址分配） 并通过输入 **Name**（名称）**Add**（添加） 地址。名称最多可以包含 63 个字母数字字符、连字符、句点和下划线。



7. 对于 **Address Type**（地址类型），选择以下选项之一：
   - **GUA from Pool**（来自池的 **GUA**） —来自下面选择的前缀池的全球单播地址 (GUA)。

 ©2024 Palo Alto Networks, Inc.

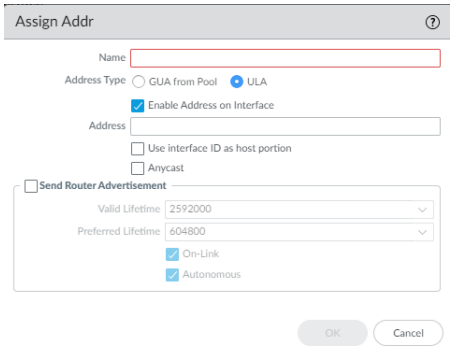
- **ULA**—唯一本地地址是地址范围 fc00::/7 中的专用地址，用于专用网络内的连接。如果没有 DHCPv6 服务器，请选择 ULA。DHCPv6 服务器可以自行决定发送它选择的任何前缀长度。

  建议还配置一个 *ULA* 以在与 *DHCPv6* 服务器的连接丢失时保持本地连接。

8. **Enable on Interface**（在接口上启用） (GUA) 或 **Enable Address on Interface**（在接口上启用地址） (ULA) 以启用此地址。
9. （仅限 GUA）选择要从中获取 GUA 的 **Prefix Pool**（前缀池） 。
10. （仅限 GUA）选择 **Assignment Type**（分配类型） ：
    - **Dynamic**（动态）— DHCPv6 客户端负责选择一个标识符来配置继承的接口。
    - **Dynamic with Identifier**（带有标识符的动态）— 您负责在 0 到 4,000 范围内选择一个标识符，并在 DHCPv6 客户端中维护一个唯一的标识符。

      如果您从 *DHCPv6* 服务器收到 */64* 前缀，请不要选择 ***Dynamic with Identifier***（带有标识符的动态）。

      如果您将 ***Dynamic with Identifier***（带标识符的动态） 应用于多个地址，请将最低标识符值分配给第一个地址，并将较高的标识符值分配给您配置的每个后续地址。
11. （仅限 ULA）输入 **Address**（地址）。
12. （仅限 ULA）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。
13. （仅限 ULA）选择 **Anycast**（任意播）使 IPv6 地址为任意播地址，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。



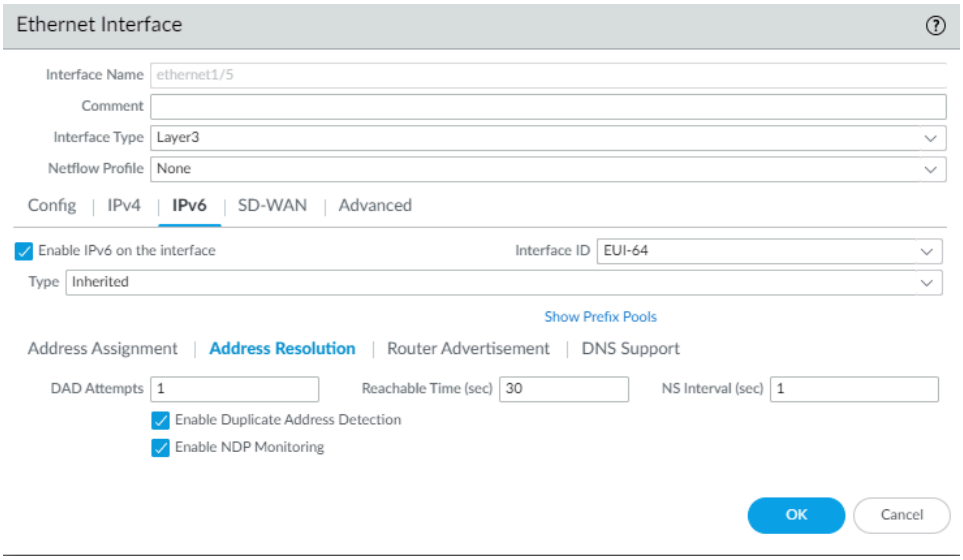
14. 选择 **Send Router Advertisement**（发送路由器通告） 将 RA 从继承的接口发送到 LAN 主机。
15. 如果您选择 ULA，请输入 **Valid Lifetime**（有效生存时间） 和 **Preferred Lifetime**（首选生存时间）。
16. 如果能在不使用路由器的情况下访问前缀中包含地址的系统，请选中**On-link**（在链路上）。
17. 如果系统可以通过结合使用通告前缀和接口 IP 来独立创建 IPv6 地址，请选择**Autonomous**（自治）。

 ©2024 Palo Alto Networks, Inc.

18. 单击 **OK**（确定） 保存地址分配。

STEP 10 | 对于继承的接口，配置地址解析。

1. 选择 **Address Resolution**（地址解析）。

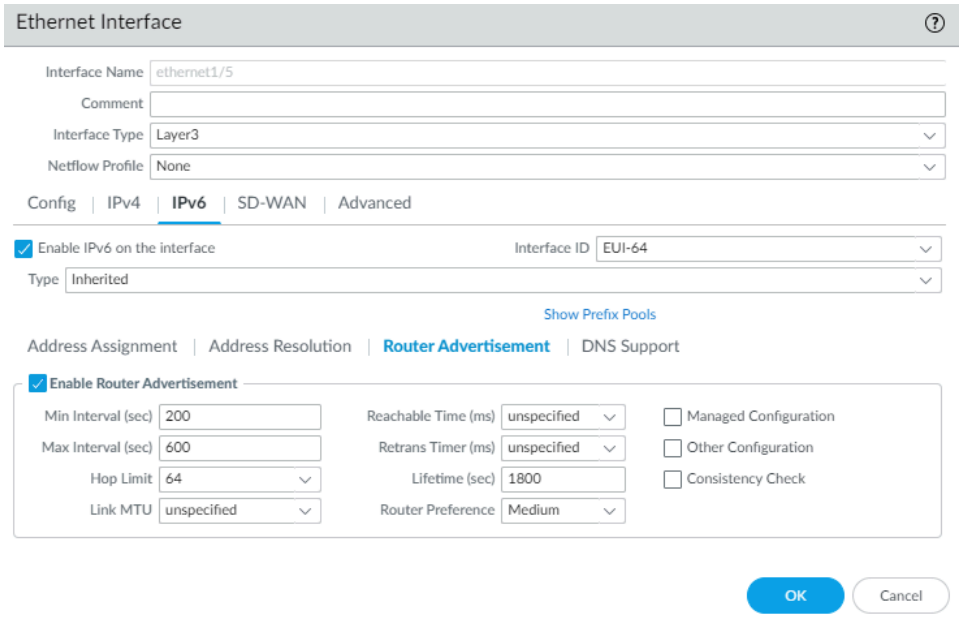


2. 如果您需要 **Enable Duplicate Address Detection**（启用重复地址检测） (DAD)（默认启用），请启用该检测。
3. 如果选择 **Enable Duplicate Address Detection**（启用重复地址检测），请指定在尝试识别邻居失败之前邻居请求 (NS) 间隔内的 **DAD Attempts**（**DAD** 尝试） 次数；范围是 1 到 10；默认为 1。
4. 指定 **Reachable Time (sec)**（可达时间（秒）），该时间是客户端用于在收到可达确认消息后假定可以到达邻居的时间；范围是 10 到 36,000；默认为 30。
5. 输入 **NS Interval (sec)**（**NS** 间隔（秒）），这是邻居请求之间的时间长度；范围是 1 到 3,600；默认为 1。
6. **Enable NDP Monitoring**（启用 **NDP** 监控） 以启用邻居发现协议监控。启用后，您可以选择 NDP 图标（功能列中的 ）并查看信息，如防火墙发现的邻居的 IPv6 地址、相应的 MAC 地址、 用户 ID 和状态（在最佳情况下）。

 ©2024 Palo Alto Networks, Inc.

STEP 11 | 对于继承的接口，配置路由器通告，以便此接口可以将 RA 发送到主机，通告前缀，主机可以使用该前缀来构建自己的 IPv6 地址。

1. 选择 **Router Advertisement**（路由器通告） 和 **Enable Router Advertisement**（启用路由器通告），以便此接口可以通过向主机发送 RA 来回复来自主机的路由器请求（默认为启用）。以下 11 个字段都属于 RA。



2. 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。
3. 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。
4. 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）。选择 **unspecified**（未指定） 以使用系统默认值。
5. 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 1,280-9,216；默认为 **unspecified**（未指定））。
6. 设置 **Reachable Time (ms)**（可达时间（毫秒）），该时间是客户端用于在收到可达确认消息后假定可以到达邻居的时间（范围为 0-3,600,000；默认为 **unspecified**（未指定））。
7. 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）。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））。
8. 设置 **Lifetime (sec)**（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， 单位为秒（范围为 0-9,000；默认值为 1,800）。零用于指定防火墙不是默认网

 ©2024 Palo Alto Networks, Inc.

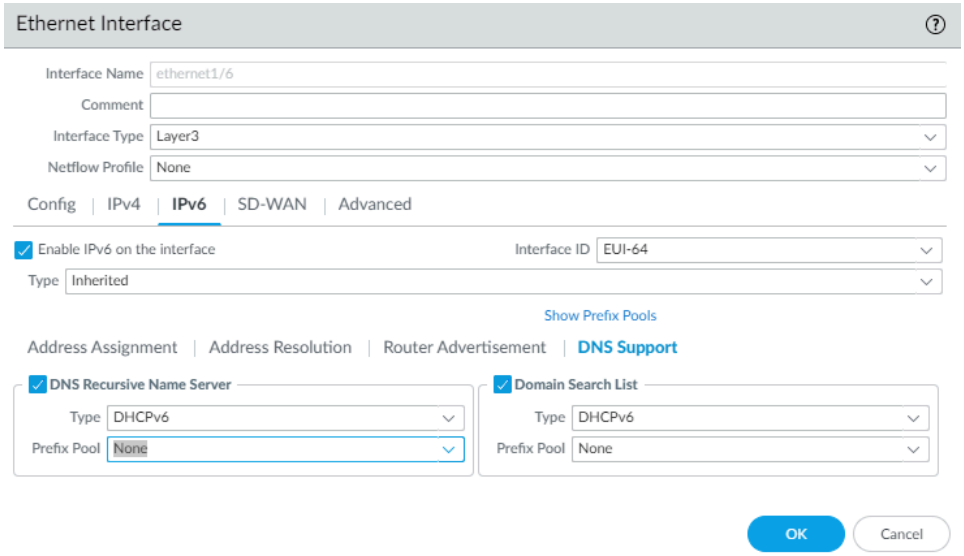
关。当生存时间到期后，客户端会从其默认路由器列表删除防火墙条目，并将另一个路由器用作默认网关。

9. 设置 **Router Preference**（路由器首选项），以防不同路由器上有两个或多个继承接口向主机发送 RA。**High**（高）、**Medium**（中）或 **Low**（低） 是 RA 通告的优先级，指示相对优先级，主机使用优先级较高的路由器的前缀。
10. 选择 **Managed Configuration**（管理配置）以向客户端指示可通过 DHCPv6 使用该地址。
11. 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）。
12. 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。

STEP 12 | 对于继承接口，配置 DNS 支持。

1. 选择 **DNS Support**（**DNS** 支持）。
2. 启用 **DNS Recursive Name Server**（**DNS** 递归名称服务器） 并选择 **DHCPv6** 或 **Manual**（手动）：

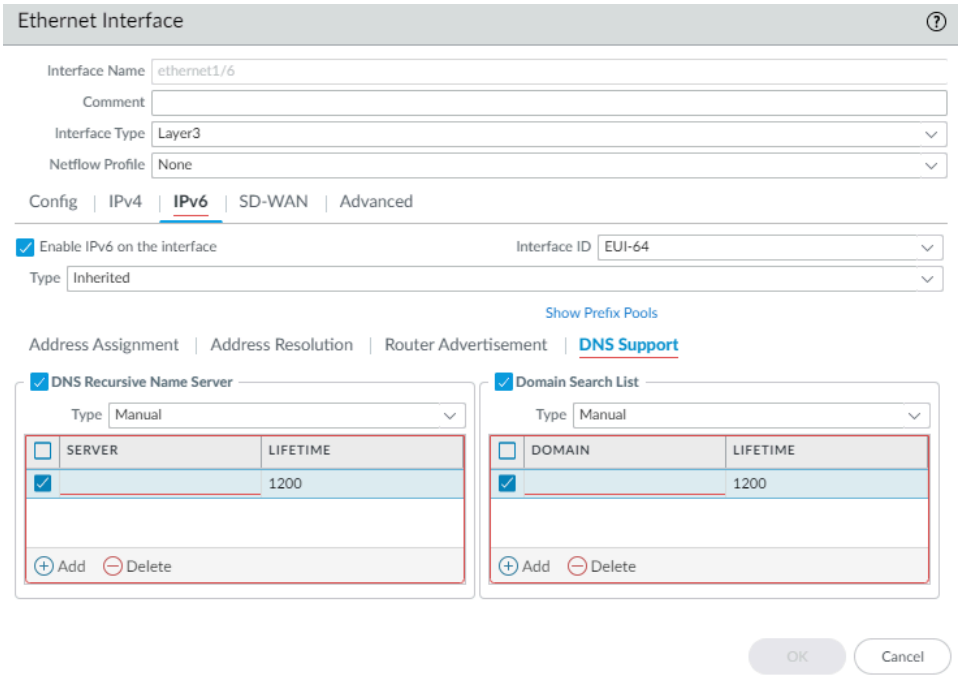
   - **DHCPv6**— 让 DHCPv6 服务器发送 DNS 递归名称服务器信息。选择 **Prefix Pool**（前缀池）。当 DNS 递归名称服务器来自 DHCPv6 服务器时，继承的接口可以间接从前缀池中获取信息。（如果在 **Address Assignment**（地址分配） 选项卡上您将地址类型配置为 **ULA**，则前缀池将为 **None**（无）。）



   - **Manual**（手动）— 手动配置 DNS 递归名称服务器。**Add**（添加）**Server**（服务器）的 IPv6 地址，例如 2001:4860:4860:0:0:0:8888。输入服务器的**Lifetime**（生存时间）；范围是等于或介于 **Max Interval**（最大间隔）（在 **Router**

 ©2024 Palo Alto Networks, Inc.

Advertisement（路由器通告）选项卡上配置）和最大间隔两倍之间的任何值。默认值为 1200 秒。



3. 启用 **Domain Search List**（域搜索列表） 并选择：
   - **DHCPv6**— 让 DHCPv6 服务器发送域搜索列表信息。选择 **Prefix Pool**（前缀池）。当域搜索列表来自 DHCPv6 服务器时，继承的接口可以间接从前缀池中获取信息。（如果在 **Address Assignment**（地址分配选项） 卡上您将地址类型配置为 **ULA**，则前缀池将为 **None**（无）。）
   - **Manual**（手动）— 手动配置域搜索列表。**Add**（添加）**Domain**（域） 后缀以添加到 DNS 中的部分名称以形成完全限定域名。例如，输入 company.org。输入域的 **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）和最大间隔两倍之间的任何值。默认值为 1200。

STEP 13 | 单击 **OK**（确定） 以保存继承的接口。

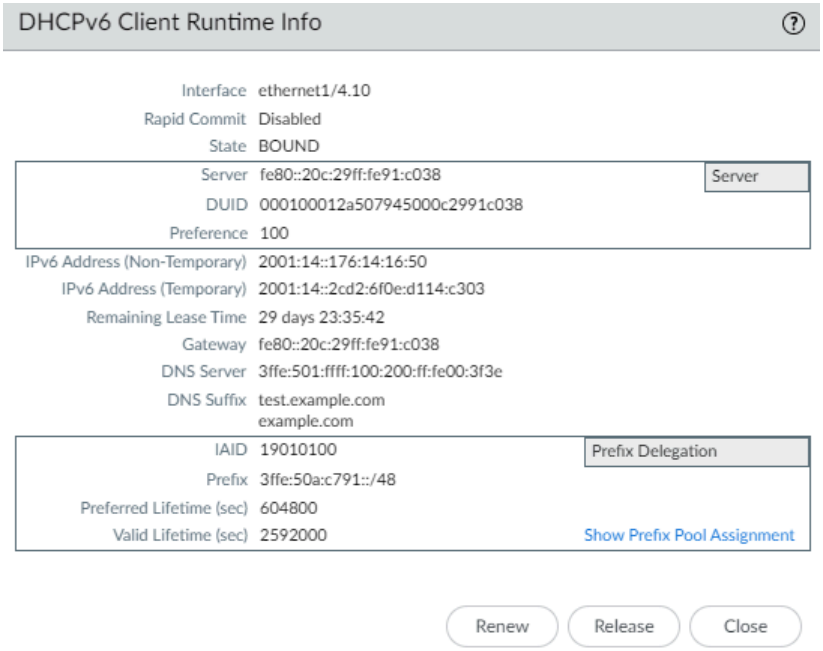
STEP 14 | **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

STEP 15 | 查看接口的 DHCPv6 信息。

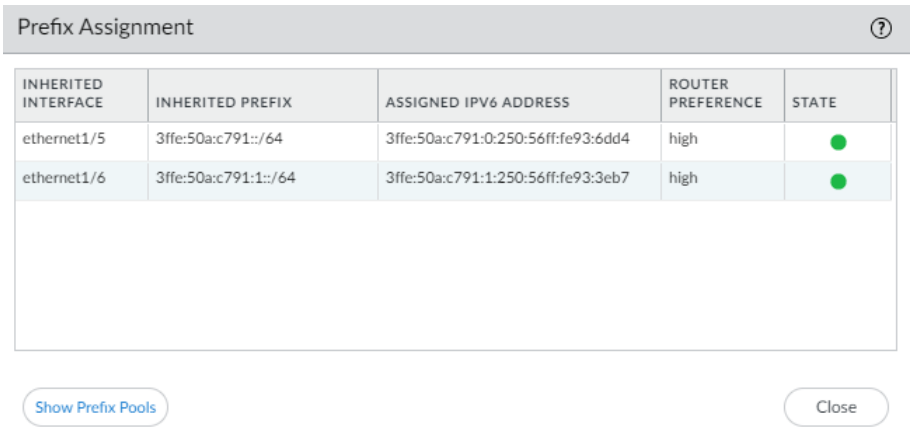
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 或 **VLAN** 或 **AE Group**（**AE** 组）。
2. 在您配置的接口行中，选择 IP 地址列中的 **Dynamic-DHCP Client**（动态 **DHCP** 客户端）链接以查看 DHCPv6 服务器分配给此 DHCPv6 客户端的设置。

   或者，您可以选择接口，然后选择 ***Show DHCPv6 Client Runtime Info***（显示 ***DHCPv6*** 客户端运行时信息）。
3. 查看信息。
   - 在下面的示例中，中间部分显示面向 ISP 的接口收到了一个非临时地址和一个临时地址。剩余租用时间适用于这两个地址。
   - 前缀委派部分显示该接口还收到了一个前缀，面向主机的继承接口可以在 RA 中向主机通告该前缀。



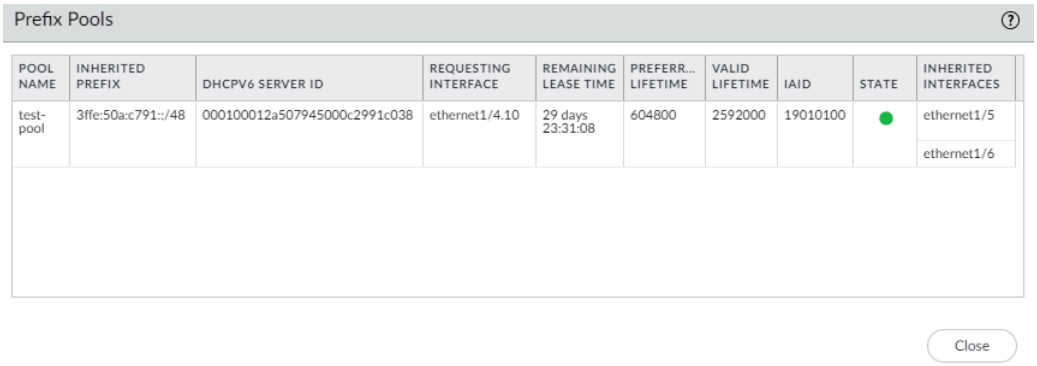
4. 选择 **Show Prefix Pool Assignment**（显示前缀池分配） 以查看每个面向主机的继承接口：继承前缀（接口分配给主机的前缀），继承接口本身的分配 IPv6 地址（基于前缀并从 MAC 地址构建） 、路由器首选项和接口状态。

 ©2024 Palo Alto Networks, Inc.



DHCPv6 客户端从服务器请求 */48* 的前缀长度并收到它，但随后将该前缀分成 */64* 前缀并将它们委派给继承接口。继承的接口向主机通告 */64* 前缀。

5. 选择 **Show Prefix Pools**（显示前缀池） 以查看创建的前缀池。

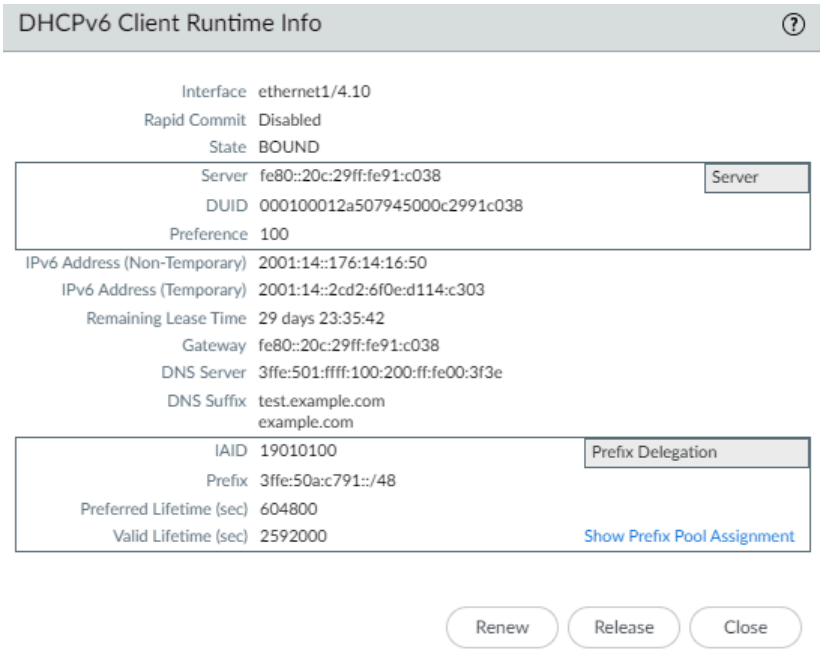


6. **Close**（关闭） 前缀池列表。

 ©2024 Palo Alto Networks, Inc.

STEP 16 | 如果您想在防火墙请求的自动续订之前续订，请使用 DHCPv6 服务器续订 DHCPv6 租约（无论租期如何）。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 或 **VLAN** 或 **AE Group**（**AE** 组）。
2. 在您配置的接口行中，选择 IP 地址列中的 **Dynamic-DHCP Client**（动态 **DHCP** 客户端）链接。
3. 从 DHCPv6 客户端运行时信息屏幕中选择 **Renew**（续订）。



4. **Close**（关闭） DHCPv6 客户端运行时信息。

 ©2024 Palo Alto Networks, Inc.

STEP 17 | 如果您在生存时间到期前不再需要这些选项，请释放来自 DHCPv6 服务器的以下 DHCP 选项。

- 前缀
- IPv6 地址（非临时）
- IPv6 地址 (临时)
- 剩余租借时间
- 网关
- DNS 服务器
- 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。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） 或 **VLAN** 或 **AE Group**（**AE** 组）。
2. 在您配置的接口行中，选择 IP 地址列中的 **Dynamic-DHCP Client**（动态 **DHCP** 客户端）链接。
3. 从 DHCPv6 客户端运行时信息屏幕中选择 **Release**（释放） 。
4. **Close**（关闭） DHCPv6 客户端运行时信息。

 ©2024 Palo Alto Networks, Inc.

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。

从 *PAN-OS 11.1.0* 开始，管理接口还支持 动态 IPv6 地址分配。

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 Configure an Interface as a DHCP Server（将接口配置为 DHCP 服务器） 中的第 *6* 步预留地址。

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。

 ©2024 Palo Alto Networks, Inc.

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） > **Interfaces**（接口），然后选择 **Management**（管理）接口。

   《*PAN-OS* 管理员指南：入门 / 将防火墙集成到您的管理网络中 / 初始配置》中记录了与动态地址无关的选择（例如速度、*MTU*、允许的 *IP* 地址、管理服务和网络服务）：
2. 选择 **IPv4**。
3. 对于 **Type**（类型），选择 **DHCP Client**（**DHCP** 客户端）。
4. （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。
   - **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。
5. 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） > **Interfaces**（接口），然后选择“Management（管理）”接口。
2. 单击 **Show DHCP Client Runtime Info**（显示 **DHCP** 客户端运行时信息）。

 ©2024 Palo Alto Networks, Inc.

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） > **Interfaces**（接口），然后选择“Management（管理）”接口。
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`**。

 ©2024 Palo Alto Networks, Inc.

配置用于动态 IPv6 地址分配的管理接口

在为动态 IPv6 地址分配配置管理 (MGT) 接口之前，请阅读“管理接口上的动态 IPv6 寻址”，以了解 IPv6 无状态地址自动配置 (SLAAC) 或 DHCPv6 如何确定地址。

WildFire 和 Panorama 型号上的管理接口不支持 DHCPv6 功能。

- 对于基于硬件的防火墙型号（而非 *VM* 系列），尽可能使用静态 *IPv6* 地址配置管理接口。
- 如果防火墙通过 *DHCPv6* 获得管理接口地址，在服务防火墙的 *DHCPv6* 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。

如果使用无状态模式 *(SLAAC/autoconfig)*，请在安全环境中使用。

作为在管理界面上使用动态 *IPv6* 地址分配的替代方法，您可以使用 *IPv4* 将管理接口配置为 DHCP 客户端。

如果将 MGT 接口配置为 DHCPv6 客户端，则存在以下限制：

- 您不能在 HA 配置中使用 MGT 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。
- 如果自定义服务路由（**Device**（设备） > **Setup**（设置） > **Services**（服务） > **Service Route Configuration**（服务路由配置） > **Customize**（定制）），无法选择 **MGT** 作为源接口。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。
- 您无法使用 MGT 接口的动态 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。
- 另一个限制是，当 MGT 接口上的 IPv6 地址的首选生命周期到期时，现有的 IPv6 会话将断开。具体而言，配置是由 DHCPv6 服务器和 RADVD 服务器发送的。防火墙从这些来自服务器的 RA 消息中获取有效生命周期和首选生命周期，并根据收到的值来设置时间。RFC 8415 规定，如果首选生命周期到期（会话在首选生命周期和有效生命周期之间的时间内必须处于活动状态），则现有通信必须在有效生命周期内保留。但 NGFW 存在如下限制：会话在首选生命周期到期时丢失。

获取 DHCPv6 地址的前提条件是 MGT 接口必须能够访问 DHCPv6 服务器。

STEP 1 | 为动态 IPv6 地址分配配置 MGT 接口。

1. 选择 **Device**（设备） > **Setup**（设置） > **Interfaces**（接口），然后选择 **Management**（管理）接口。

   《*PAN-OS* 管理员指南：执行初始配置。

2. 选择 **IPv6**，然后选择 **Enable IPv6**（启用 **IPv6**）。
3. 选择 **Dynamic**（动态）作为 **Type**（类型）。

STEP 2 | 在“DHCPv6 Client Options（DHCPv6 客户端选项）”部分中，选择 **Non Temporary Address**（非临时地址）（默认设置）。这种地址类型的生命周期长于临时地址。

 ©2024 Palo Alto Networks, Inc.

您是否为接口请求非临时地址或临时地址取决于您的判断和 *DHCPv6* 服务器的能力；有些服务器仅可提供临时地址。您可以选择非临时地址或临时地址，但不能同时选择两者。

STEP 3 | 选择 **Temporary Address**（临时地址） 以获得更高级别的安全性，因为该地址仅供短期使用。

IPv6 地址不会自动续订，当有效时间达到 *0* 时将过期。

STEP 4 | 选择 **Rapid Commit**（快速提交） 以使用 Solicit 和 Reply 消息（两条消息）的 DHCPv6 进程，而不是 Solicit、Advertise、Request 和 Reply 消息（四条消息）的进程。

STEP 5 | 选择接口用来向 DHCPv6 服务器标识自身的 **DUID** 类型（**DHCPv6** 唯一标识符）(RFC-6355)：

- **duid-type-llt**—DUID-LLT；MGT 接口的链路层地址，与时间戳连接。
- **duid-type-ll**—DUID-LL；MGT 接口的链路层地址。

STEP 6 | 选择 **Default Gateway Type**（默认网关类型）：

- **Static**（静态）—在 **Default IPv6 Gateway Address**（默认 **IPv6** 网关地址）中输入。
- **Dynamic**（动态）—防火墙从来自相邻路由器（网关）的路由器通告 (RA) 消息中获知 MGT 接口的 IPv6 默认网关地址，以响应路由器请求 (RS)。如果只有一台路由器连接到链路，则会将通告 RA 的路由器的源地址（链路本地地址）配置为 MGT 接口的默认网关地址。链路本地地址特定于接口，并且是使用 EUI-64 方法自动配置的。如果链路上连接了多台路由器，防火墙会将其默认网关地址设置为路由器优先级值最高（低、中或高）的 RA 消息的源地址。

STEP 7 | **Commit**（提交）更改。

STEP 8 | （可选）查看 DHCPv6 网关地址。

1. 访问 CLI。
2. **>show dhcp client ipv6-gateway-address**

STEP 9 | （可选）查看 DHCPv6 客户端信息。

1. **>show dhcp client mgmt6-interface-state**
2. 请参阅 hostname、IPv6 address、life-starts、max-life、preferred-life 和 dhcpv6-server。

STEP 10 | （可选）使用 DHCPv6 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. **>show dhcp client mgmt6-interface-state**
2. 续订。

 ©2024 Palo Alto Networks, Inc.

STEP 11 | （可选）释放从 DHCPv6 服务器获取的 DHCPv6 地址。（不会释放 SLAAC 地址。）

解除 *IPv6* 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。

1. **>show dhcp client mgmt6-interface-state**
2. 释放。

 ©2024 Palo Alto Networks, Inc.

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 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）。

 ©2024 Palo Alto Networks, Inc.

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
```

```
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。

 ©2024 Palo Alto Networks, Inc.

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>
```

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
```

 ©2024 Palo Alto Networks, Inc.

 ©2024 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
- 配置 Web 代理
- 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

为让用户能够访问网络资源，DNS 的作用至关重要，有了 DNS，用户无需便记住 IP 地址，并且单个计算机也不需要存储映射到 IP 地址的大量域名。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。

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）。

从 PAN-OS 11.2.1 及更高版本开始，您可以使用加密的 DNS 进行 DNS 代理。您还可以对管理接口使用加密的 DNS，无论管理接口连接到 DNS 服务器还是使用 DNS 代理。加密 DNS 通过预防中间人攻击，提高了客户端和服务器之间 DNS 流量的用户隐私和安全性。加密 DNS 发生在以下设备之间：

- 对于管理接口，加密 DNS 发生在防火墙和 DNS 服务器之间。

 ©2024 Palo Alto Networks, Inc.

- 对于 DNS 代理，可以在两个方向上配置加密 DNS；可以指定防火墙将从 DNS 客户端接受的一种或多种加密 DNS 类型，也可以仅指定防火墙将与 DNS 服务器一起使用的一种加密 DNS 类型。

防火墙支持两种 DNS 加密类型：基于 HTTPS 的 DNS (DoH) 和基于 TLS 的 DNS (DoT)。您可以选择在 DNS 服务器拒绝加密 DNS 或超时（在配置的 TCP 超时期限内未收到来自主要或辅助 DNS 服务器的响应）的情况下让防火墙回退到传统 DNS（明文）。为某一接口配置加密 DNS 时，该接口不得托管 TCP 端口 443 或 853 上的其他流量。

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。配置主辅 DNS 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。
- (PAN-OS 11.2.1 及更高版本）为管理接口配置加密 DNS，如执行初始配置中所示。
- 配置 DNS 代理对象。
- (PAN-OS 11.2.1 及更高版本）为 DNS 代理对象配置加密 DNS。
- 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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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 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 与用例 1 的行为相同	绑定：特定 vsys 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 服务路由：接收到 DNS 请求的接口和 IP 地址。 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

 ©2024 Palo Alto Networks, Inc.

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。

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。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | （PAN-OS 11.2.1 及更高版本）（可选）配置 DNS 代理以接受来自 DNS 客户端的加密 DNS 查询并将加密的 DNS 查询发送到 DNS 服务器。

1. 在 **Encrypted DNS**（加密 **DNS**）选项卡上，选择 **Enable Encrypted DNS**（启用加密 **DNS**）。

   如果未选择 ***Enable Encrypted DNS***（启用加密 ***DNS***），则无论客户端 *DNS* 请求是否加密，*DNS* 代理都会向 *DNS* 服务器发送明文 *DNS* 请求。

2. 对于服务器设置，选择防火墙（DNS 代理）将用于与 DNS 服务器通信的连接类型：

   - **DoH**—基于 HTTPS（超文本传输协议安全）的 DNS。DoH 使用端口 443。启用加密 DNS 并且连接类型为 DoH 时：
     - 需要一个主 DNS 地址，DNS 代理使用 DoH 将所有 DNS 请求发送到主 DNS 服务器。如果主 DNS 服务器没有响应，DNS 代理会将 DoH 请求发送到辅助 DNS 服务器。
     - 充当 DNS 代理的接口上不允许任何其他 HTTPS 服务。
     - 必须配置从 DNS 客户端到 DNS 服务器的 SSL 解密策略，以便 DNS 代理可以解密 DoH 流量。
   - **DoT**—基于 TLS（传输层安全性）的 DNS。DoT 使用端口 853，这是 DoT 流量的专用端口。启用加密 DNS 并且连接类型为 DoT 时：
     - 需要一个主 DNS 地址，DNS 代理使用 DoT 将所有 DNS 请求发送到主 DNS 服务器。如果主 DNS 服务器没有响应，DNS 代理会将 DoT 请求发送到辅助 DNS 服务器。
     - 充当 DNS 代理的接口上不允许任何其他 TLS 服务。
   - 原点—DNS 代理使用与从客户端收到的 DNS 类型相同的 DNS 类型将所有 DNS 请求发送到主 DNS 服务器。主 DNS 地址是必需的。如果 DNS 代理在 TCP 超时时间内没有收到主 DNS 服务器的 DNS 响应，DNS 代理会将 DNS 请求发送至备用 DNS 服务器。
   - 明文— 未加密的纯文本 DNS 流量。

3. 如果选择 **Fallback on Unencrypted DNS**（未加密 **DNS** 的回退），则在 DNS 服务器拒绝加密 DNS 或超时（DNS 代理在配置的 TCP 超时期限内未从主 DNS 服务器或辅助 DNS 服务器收到配置的连接类型 [DoH 或 DoT] 的响应）的情况下，DNS 代理将回退到传统 DNS（明文）。

4. 在 **TCP Timeout (sec)**（**TCP** 超时（秒））中，以秒为单位输入超时值，也就是主 DNS 服务器必须在多长时间内响应（超过此时间后将向辅助 DNS 服务器查询 DNS）；另请

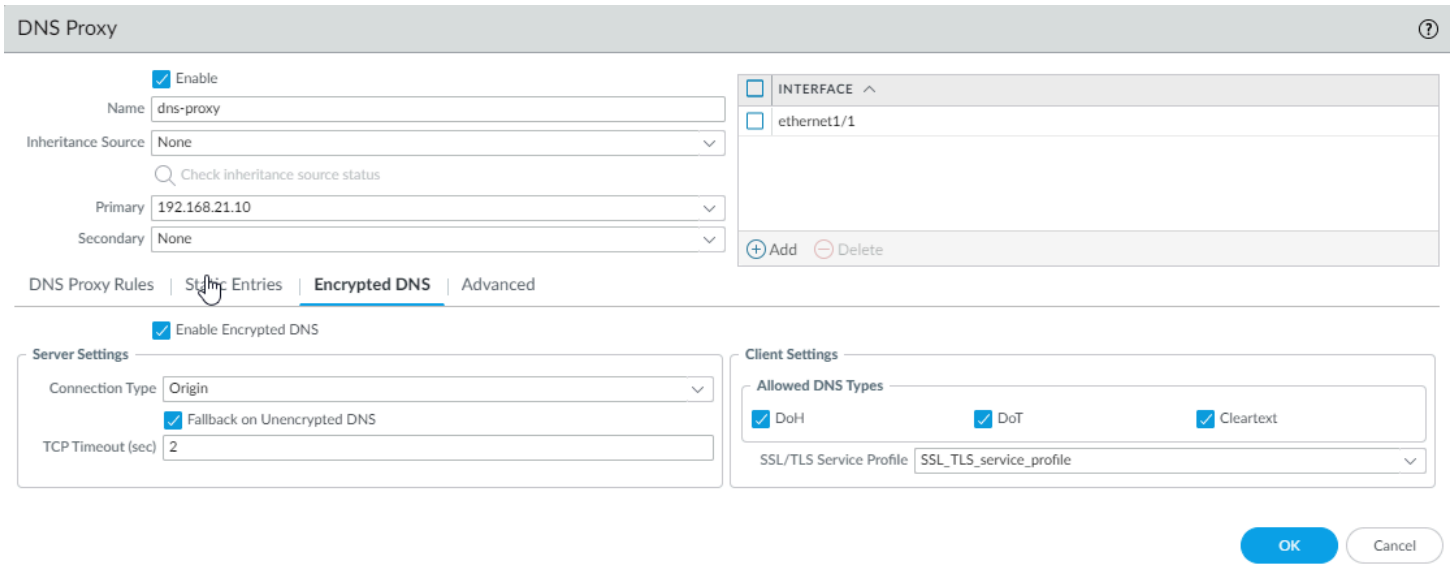
 ©2024 Palo Alto Networks, Inc.

输入辅助 DNS 服务器必须在多长时间内响应（超过此时间后，DNS 查询将回退到名为 DNS 通信）；范围是 1 到 10；默认值为 1 秒。

5. 对于客户端设置，选中一个或多个 **Allowed DNS Types**（允许的 **DNS** 类型），也就是 DNS 代理将从客户端接受的 DNS 类型：
   - **DoH**—DNS 代理必须按照为服务器设置指定的方式解密 DoH 流量和代理 DNS：
     - 如果“Server Setting（服务器设置）”的值是“Origin（来源）”，则 DNS 代理将以 DoH 形式发送 DNS 请求。
     - 如果“Server Setting（服务器设置）”的值是“DoH”，则 DNS 代理将以 DoH 形式发送 DNS 请求。
     - 如果“Server Setting（服务器设置）”的值是“DoT”，则 DNS 代理将以 DoT 形式发送 DNS 请求。
   - **DoT**—DNS 代理必须按照为服务器设置指定的方式解密 DoT 流量和代理 DNS：
     - 如果“Server Setting（服务器设置）”的值是“Origin（来源）”，则 DNS 代理将以 DoT 形式发送 DNS 请求。
     - 如果“Server Setting（服务器设置）”的值是“DoH”，则 DNS 代理将以 DoH 形式发送 DNS 请求。
     - 如果“Server Setting（服务器设置）”的值是“DoT”，则 DNS 代理将以 DoT 形式发送 DNS 请求。
   - 明文—DNS 代理必须按照为服务器设置指定的方式代理 DNS 请求：
     - 如果“Server Setting（服务器设置）”的值是“Origin（来源）”，则 DNS 代理将以明文形式发送 DNS 请求。
     - 如果“Server Setting（服务器设置）”的值是“DoH”，则 DNS 代理将以 DoH 形式发送 DNS 请求。
     - 如果“Server Setting（服务器设置）”的值是“DoT”，则 DNS 代理将以 DoT 形式发送 DNS 请求。

   如果客户端设置中禁用了明文，DNS 代理将忽略或丢弃明文流量。
6. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）以选择一个配置文件，或创建一个新的 SSL/TLS 服务配置文件以用于客户端和 DNS 代理之间的 DNS 加密，或者选择 **None**（无）。
7. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.



STEP 5 | 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。
   - **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），您必须启用 **Cache**（缓存）（默认启用），并选择一个虚拟系统，然后选择 **General**（常规） > **DNS Proxy**（**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 到 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 6 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

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）。
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）。

 ©2024 Palo Alto Networks, Inc.

配置 Web 代理

在何处可以使用？	需要提供什么？
• NGFW（云管理） • NGFW（PAN-OS 或 Panorama 托管）	❑ Web 代理许可证 ❑ （对于云管理的 NGFW）AIOps for NGFW Premium许可证。

如果您的网络使用代理设备来确保安全，您现在可以使用 PAN-OS 11.0 的本地 Web 代理功能来利用相同级别的保护。Web 代理功能支持从现有 Web 代理架构迁移到简单的统一管理控制台的其他选项。将 Web 代理功能与 Prisma Access 结合使用提供了一种无缝方法，用于从易于使用和简化的接口迁移、部署和维护安全 Web 网关 (SWG) 配置。Web 代理在从本地到云的过渡过程中提供帮助，不会影响安全性或效率。

Web 代理支持两种路由流量的方法：

- 对于显式代理方式，请求中包含配置代理的目标 IP 地址，客户端浏览器直接向代理发送请求。您可以使用以下方法之一通过显式代理对用户进行身份验证：
  - Kerberos，需要 Web 代理许可证。
  - SAML 2.0，需要 Panorama、Prisma Access 许可证、云服务 3.2.1 插件（及更高版本）和附加 Web 代理许可证。
  - 云身份引擎，需要 Panorama、Prisma Access 许可证、云服务 3.2.1 插件（及更高版本）和附加 Web 代理许可证。
- 对于透明代理方法，请求包含 Web 服务器的目标 IP 地址，代理透明地拦截客户端请求（通过内联或流量控制）。没有客户端配置，Panorama 是可选的。透明代理需要环回接口、代理区域中的用户 ID 配置以及特定的目标 NAT (DNAT) 规则。透明代理不支持 X-Authenticated Users (XAU) 或 Web 缓存通信协议 (WCCP)。

您还可以将高级路由与 Web 代理一起使用。

以下产品支持 Web 代理：

- PA-1400 系列防火墙
- PA-3400 系列防火墙
- PA-5400 系列防火墙（不包括 PA-5450）
- VM 系列防火墙（至少有四个 vCPU）
- 运行 PAN-OS 11.1 的 Panorama 管理系统

要使用 SAML 身份验证配置 显式代理，Web 代理需要云服务插件 3.2.1 或更高版本。

Web 代理支持 *IPv4*。

要了解如何配置 Web 代理，请选择您要配置的代理类型或代理功能：

- 配置显式代理

 ©2024 Palo Alto Networks, Inc.

- 配置透明代理
- 为显式 Web 代理配置身份验证
- 配置显式代理身份验证的豁免

配置显式代理

在何处可以使用？	需要提供什么？
• NGFW（云管理） • NGFW（PAN-OS 或 Panorama 托管）	❑ Web 代理许可证 ❑ （对于云管理的 NGFW）AIOps for NGFW Premium许可证。

您可以在防火墙上配置的其中一种 Web 代理类型是显式代理。Web 代理使您能够利用代理设备的相同功能，同时提供了一个简单、统一界面来管理代理。

特别是，显式代理方法允许您更轻松地解决问题，因为客户端浏览器知道代理的存在。

- PAN-OS
- Cloud Management

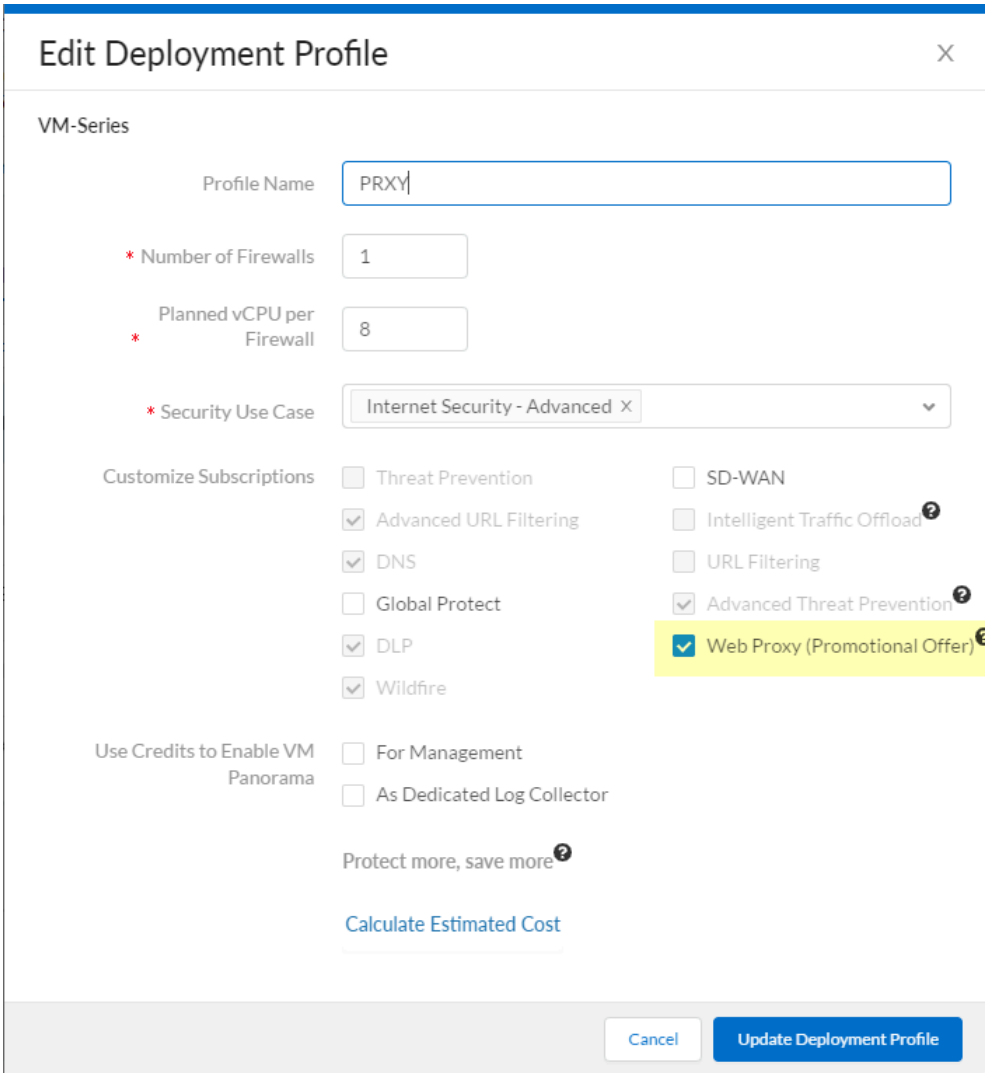
PAN-OS

 ©2024 Palo Alto Networks, Inc.

STEP 1 | （仅限 VM 系列）如果您尚未这样做，请激活 Web 代理的许可证。

您必须激活 *PA-1400* 系列、*PA-3400* 系列和 *VM* 系列的 *Web* 代理许可证。在以下步骤中了解如何 激活 PA-1400 系列和 PA-3400 系列的订阅许可证 或激活 *VM* 系列的 *Web* 代理许可证。

1. 登录到客户服务门户 (CSP)。
2. **Edit** （编辑） 部署配置文件。
3. 选择 **Web Proxy (Promotional Offer)** （**Web** 代理（促销优惠））。



4. 单击 **Update Deployment Profile**（更新部署配置文件）。
5. 在防火墙上，从服务器检索 许可证密钥 。

如果许可证密钥检索不成功，请重新启动防火墙并在继续之前重复此步骤。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 设置必要的接口和区域。

作为最佳实践，对 *Web* 代理使用的三个接口使用第 *3* 层 *(L3)*，并在相同的虚拟路由器和相同的虚拟系统中为每个接口配置一个单独的区域。

1. 为客户端流量配置接口。

   请务必仔细复制此接口的 *IP* 地址并将其保存在安全位置，因为在配置 *Web* 代理时必须将其作为 ***Proxy IP***（代理 ***IP***）地址输入。
2. 为到 Internet 的传出流量配置接口。
3. 为代理配置环回接口。

   所有传入流量都通过此接口路由到代理。

STEP 3 | 为显式代理设置 DNS 代理。

1. 为代理连接配置 DNS 代理对象 。
2. 使用主 DNS 服务器和辅助 DNS 服务器配置 DNS 服务器配置文件 。

   您必须为 *Web* 代理配置主 *DNS* 服务器和辅助 *DNS* 服务器。
3. 指定代理连接的 接口 。

   指定流量入口接口或 环回 接口。

STEP 4 | 要为 MITM 检测启用解密，请创建 自签名根 CA 证书 或导入由您的企业证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅 管理访问的最佳做法。

STEP 5 | 确保您已完成要配置的身份验证方法的预部署步骤。

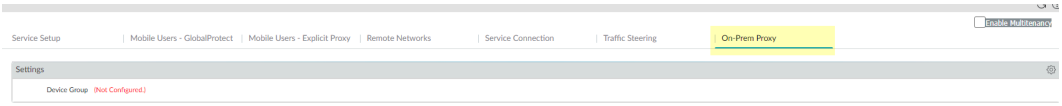
- 配置 Kerberos 身份验证
- 配置 SAML 身份验证
- 配置云身份引擎身份验证

 ©2024 Palo Alto Networks, Inc.

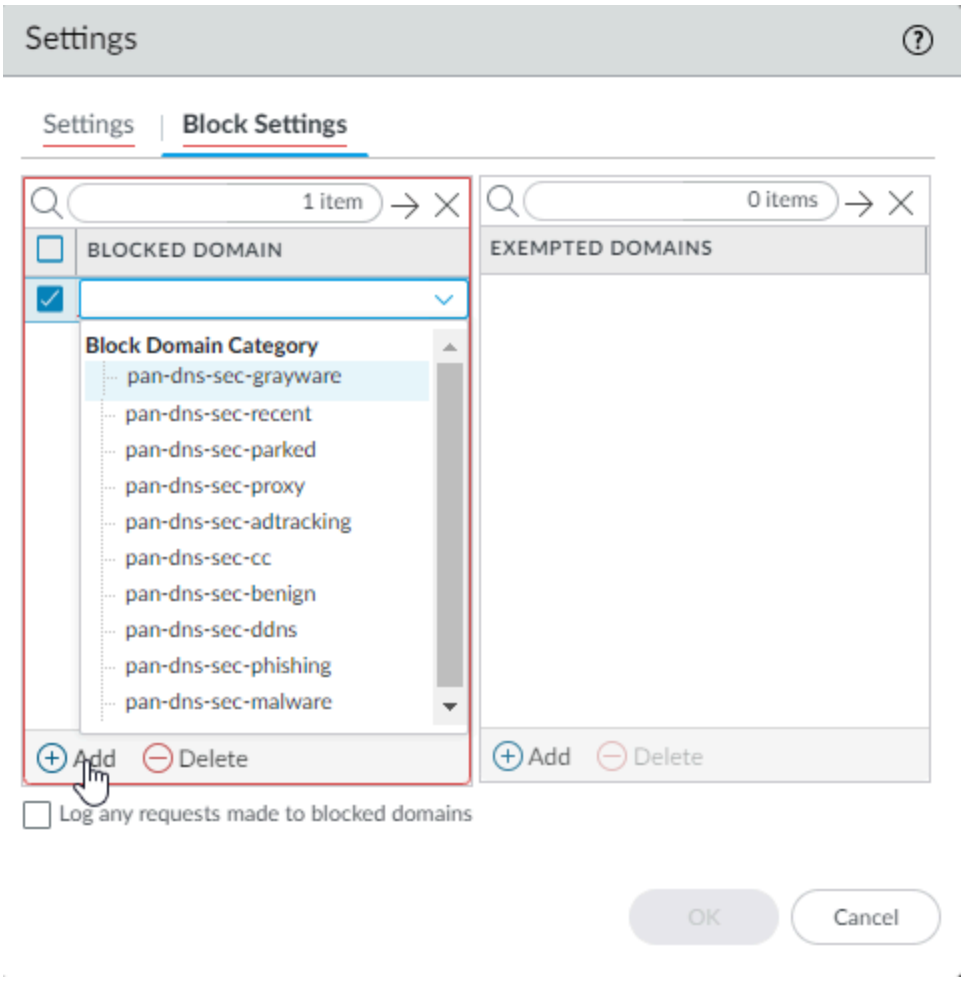
STEP 6 | 如果您有 DNS 安全订阅，请将 Web 代理防火墙与显式代理集成，以吸收与您指定的 DNS 安全类别匹配的任何请求。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **On-Prem Proxy**（本地代理）。
2. **Edit**（编辑） 设置，然后选择您希望 Web 代理防火墙使用的 **Device Grou**（设备组） 或 **Add**（添加） 新设备组。

   要将 *Web* 代理防火墙与 *Prisma Access* 集成，您必须在不包含其他防火墙或虚拟系统的单独设备组中配置 *Web* 代理防火墙。如果防火墙已经是设备组的成员，则创建子设备组作为子组并将防火墙移动到子设备组。



3. （可选）选择 **Block Settings**（阻止设置） 以 **Add**（添加） **Blocked Domain**（被阻止域） 或任何属于 **Exempted Domains**（豁免域） 的域，因为它们因匹配一个或多个 DNS 安全类别而被吸收。



4. （可选）选择是否要 记录对被阻止域发出的任何请求。

 ©2024 Palo Alto Networks, Inc.

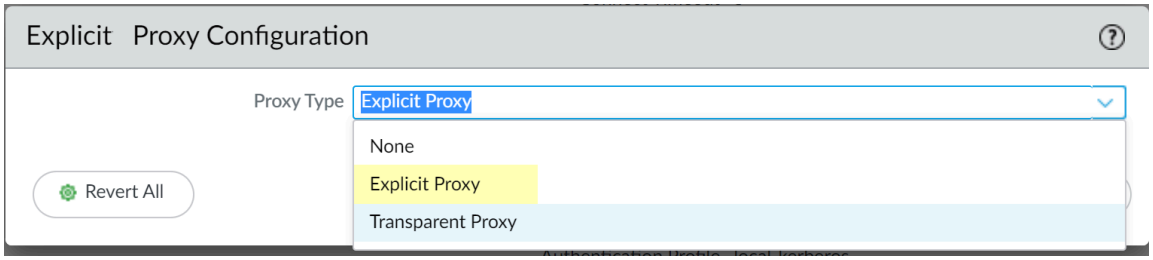
5. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

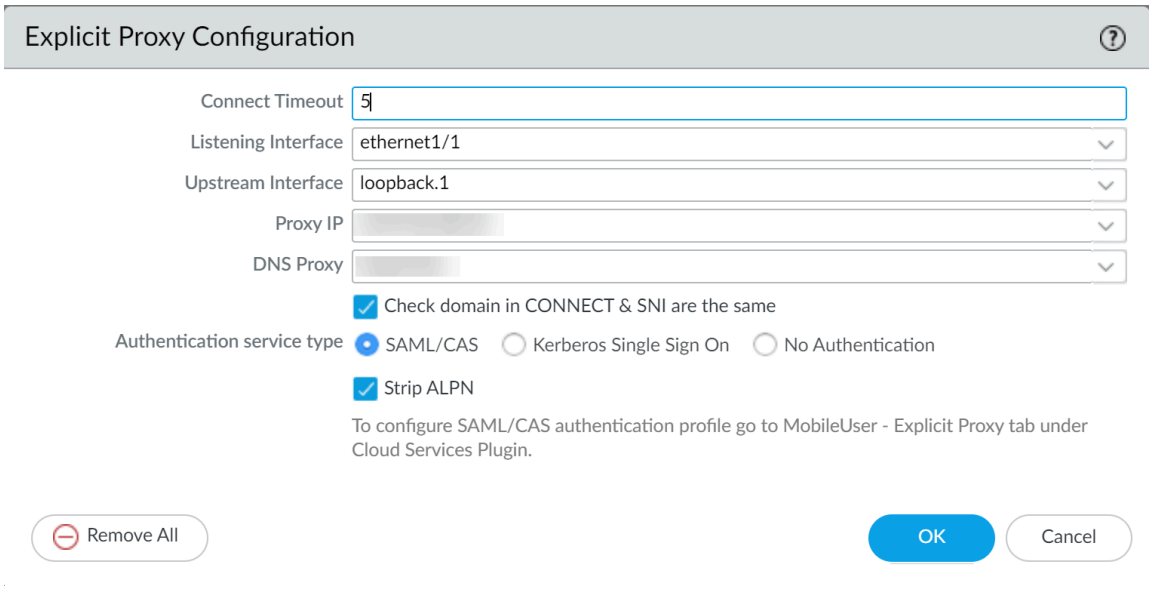
STEP 7 | 设置显式代理。

1. 在防火墙上，选择 **Network**（网络） > **Proxy**（代理），然后选择 **Edit**（编辑） **Proxy Enablement**（代理启用） 设置。
2. 选择 **Explicit Proxy**（显式代理） 作为 **Proxy Type**（代理类型），然后单击 **OK**（确定） 以确认更改。

   如果唯一可用的选项是无，请验证您是否具有 *Web* 代理功能的有效许可证。



3. **Edit**（编辑） **Explicit Proxy Configuration**（显式代理配置）。



4. 指定 **Connect Timeout**（连接超时） 以定义（以秒为单位）代理等待 Web 服务器响应的时间。如果在指定的时间过去后没有响应，代理将关闭连接。
5. 选择包含要启用 Web 代理的防火墙的 **Listening Interface**（侦听接口）。

   指定客户端流量的入口接口。

6. 选择包含与将流量重新路由到服务器的 Web 代理的接口的 **Upstream Interface**（上游接口）。

 ©2024 Palo Alto Networks, Inc.

如果您使用环回接口，请将该接口指定为 ***Upstream Interface***（上游接口）。

7. 将侦听接口的 IP 地址指定为 **Proxy IP**（代理 **IP**）。

   输入您在之前的步骤中创建的接口的 IP 地址。

8. 指定您在之前的步骤中创建的 **DNS** 代理对象
9. 选择 检查 **CONNECT** 和 **SNI** 中的域是否一致，通过在 CONNECT 请求和 HTTP 标头中的服务器名称指示 (SNI) 字段之间指定不同的域来防止域前端攻击。
10. 选择您要使用的 身份验证服务类型 （**SAML/CAS**或 **Kerberos Single Sign On**（**Kerberos** 单点登录））。

    请务必为您选择的身份验证方法完成所有必要的预部署和配置步骤。仅选择以下身份验证方法之一：

    - 配置 Kerberos 身份验证
    - 配置 SAML 身份验证
    - 配置云身份引擎身份验证

11. 单击 **OK**（确定） 以确认更改。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 配置必要的安全策略规则以解密流量并将适用的流量重新路由到代理。

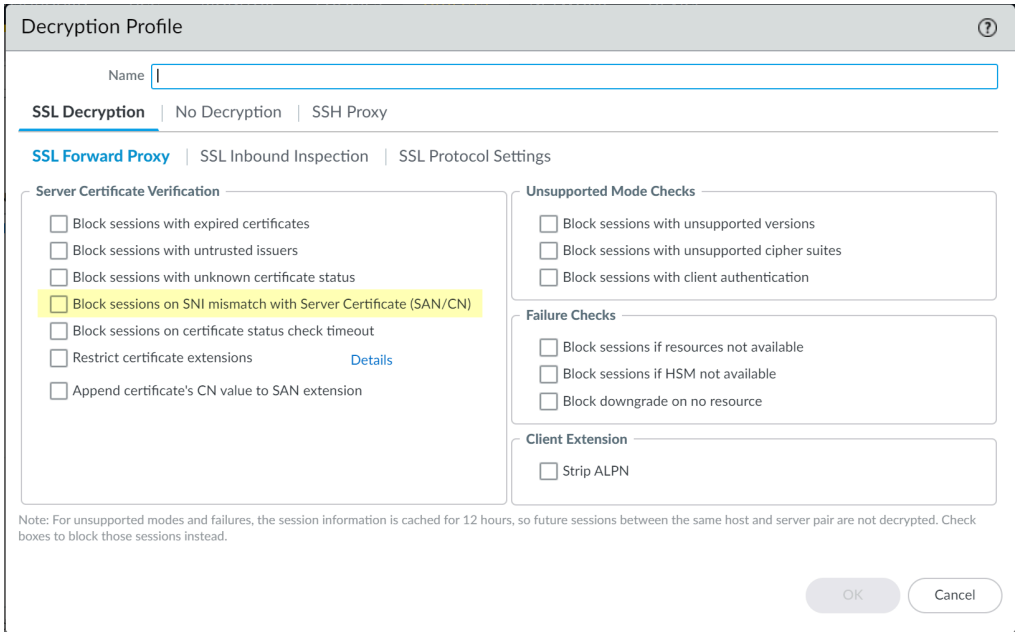
您将需要创建以下类型的规则：

- Source NAT（源 NAT）（如果适用）
- Decryption（解密）
- Security（安全）

1. 配置解密策略以 解密 流量，以便在必要时重新路由。

   为避免两次解密流量，请选择包含上游接口的区域作为解密策略的源区域。

2. （可选，但推荐）选择 **Objects**（对象） > **Decryption Profile**（解密配置文件） 并选择 在 **SNI** 与服务器证书 **(SAN/CN)** 不匹配 时阻止会话以自动拒绝服务器名称指示 (SNI) 与服务器证书不匹配的任何会话。



3. 配置必要的安全策略规则。
   - 创建安全策略规则以允许从客户端到您选择作为侦听接口的接口的流量。
   - 配置安全策略规则以允许来自包含上游接口的区域的流量到互联网。
   - 配置安全策略规则以允许从 DNS 代理区域到 Internet 的流量。
4. 使用您在之前的步骤中配置的身份验证配置文件配置安全策略规则以适当地将流量路由到代理。
5. 如果这是初始透明 Web 代理配置，请在代理配置（**Network**（网络） > **DNS Proxy**（**DNS** 代理））和接口配置（**Network**（网络） > **Interfaces**（接口））中进行更改，然后选择 **Commit**（提交）提交更改以确保透明 Web 代理配置在防火墙上正确填充。

 ©2024 Palo Alto Networks, Inc.

Cloud Management

仅传统路由器堆栈支持 *Strata Cloud Manager* 的显式 *Web* 代理。如果您希望启用此功能，请联系您的客户团队。

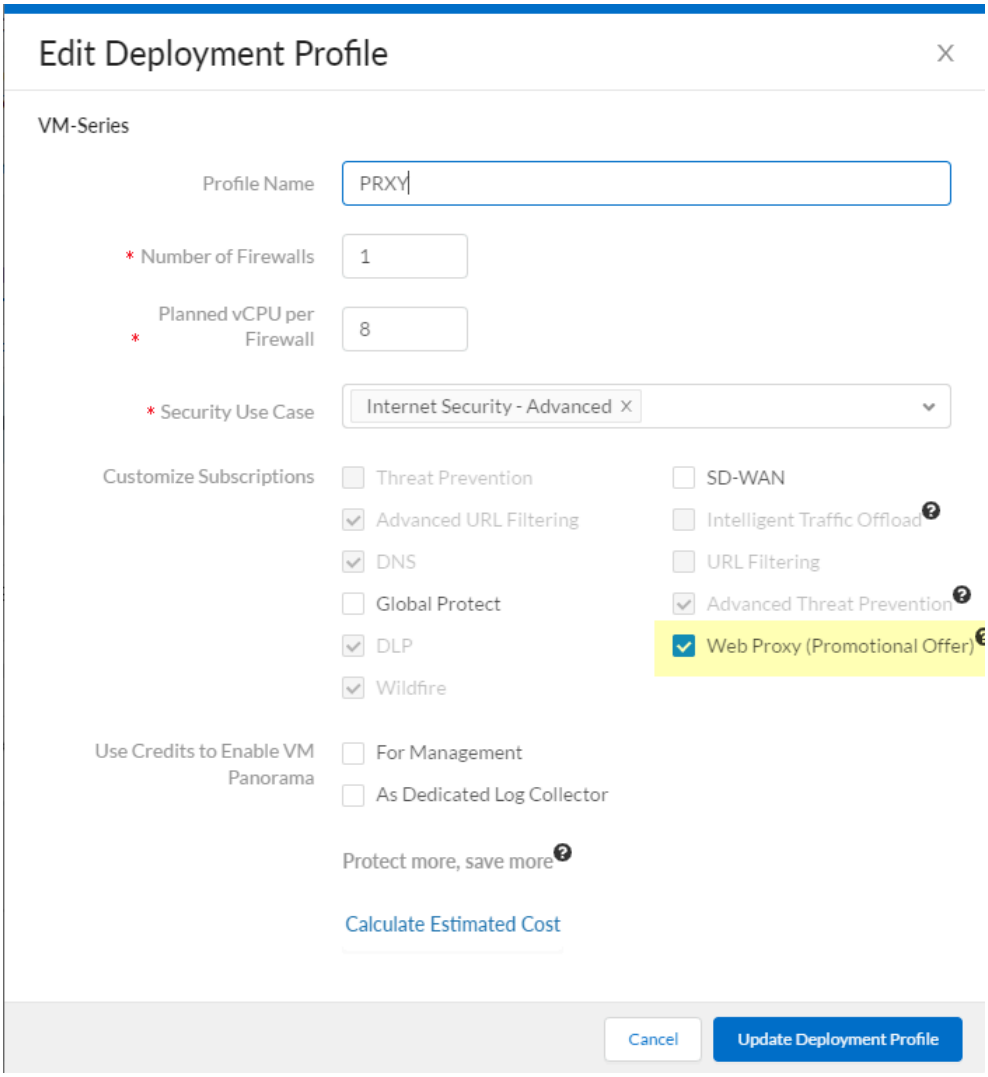
您可以使用 Strata Cloud Manager 在云管理防火墙上配置显式 Web 代理。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | （仅限 VM 系列）如果您尚未这样做，请激活 Web 代理的许可证。

您必须激活 *PA-1400* 系列、*PA-3400* 系列和 *VM* 系列的 *Web* 代理许可证。在以下步骤中了解如何 激活 PA-1400 系列和 PA-3400 系列的订阅许可证 或激活 *VM* 系列的 *Web* 代理许可证。

1. 登录到客户服务门户 (CSP)。
2. **Edit** （编辑） 部署配置文件。
3. 选择 **Web Proxy (Promotional Offer)** （**Web** 代理（促销优惠））。



4. 单击 **Update Deployment Profile**（更新部署配置文件）。
5. 在防火墙上，从服务器检索 许可证密钥 。

如果许可证密钥检索不成功，请重新启动防火墙并在继续之前重复此步骤。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 设置必要的接口和区域。

请勿编辑代理区域。

作为最佳实践，对 *Web* 代理使用的三个接口使用第 *3* 层 *(L3)*，并在相同的虚拟路由器和相同的虚拟系统中为每个接口配置一个单独的区域。

1. 为客户端流量配置接口。

   请务必仔细复制此接口的 *IP* 地址并将其保存在安全位置，因为在配置 *Web* 代理时必须将其作为 ***Proxy IP***（代理 ***IP***）地址输入。
2. 为到 Internet 的传出流量配置接口。
3. （可选）为代理配置环回接口。

   Strata Cloud Manager 会自动创建环回接口。如果您想使用不同的环回接口，则只需配置一个。

   所有传入流量都通过此接口路由到代理。

STEP 3 | 要为 MITM 检测启用解密，请创建 自签名根 CA 证书 或导入由您的企业证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅 管理访问的最佳做法。

STEP 4 | 确保您已完成要配置的身份验证方法的预部署步骤。

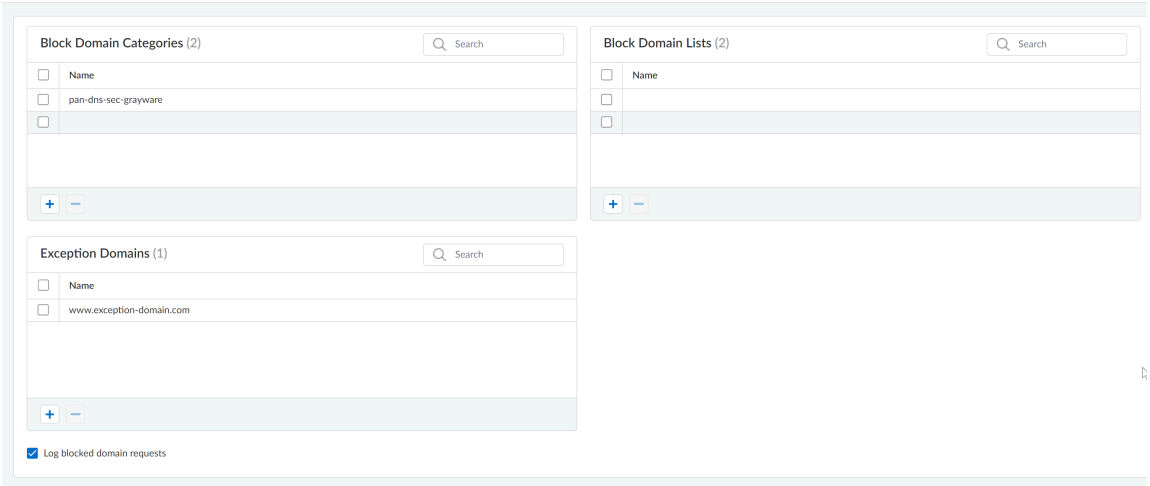
- 如果您使用 SAML，则必须已经为移动用户配置显式代理。
- 如果您正在使用 Kerberos，则必须已完成 Kerberos 的预部署要求。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 如果您有 DNS 安全订阅，请将 Web 代理防火墙与显式代理集成，以吸收与您指定的 DNS 安全类别匹配的任何请求。

1. 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备设置） > **Proxy**（代理） > **Block Domains**（阻止域） > **Customize**（定制）。
2. （可选）选择 **Block Domain Categories**（阻止域类别）、**Block Domain Lists**（阻止域列表）或 **Exception Domains**（例外域）以添加对应内容，因为它们因匹配一个或多个 DNS 安全类别而被吸收。

   Block Domains

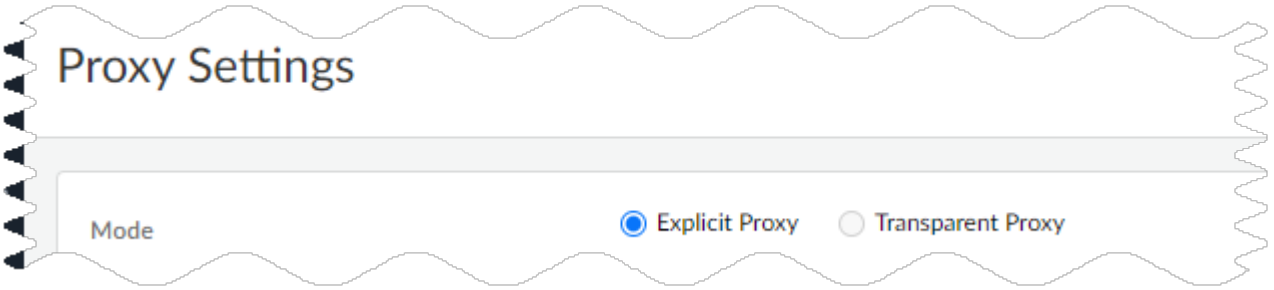
   

3. （可选）根据需要选择 **Log blocked domain requests**（记录阻止的域请求）选项。
4. 单击 **Save**（保存）以保存您的选择。

 ©2024 Palo Alto Networks, Inc.

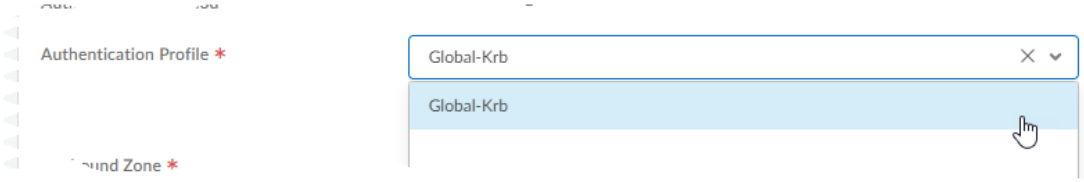
STEP 6 | 设置显式代理。

1. 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备设置） > 配置范围（**Configuration Scope**）。
2. 选择要配置显式代理的文件夹或片段。
3. 选择 **Device Settings**（设备设置） > **Proxy**（代理） > **Proxy Settings**（代理设置） > **Customize**（定制）。
4. 针对 **Mode**（模式），选择 **Explicit Proxy**（显式代理）。



5. 选择 **Authentication Method**（身份验证方法）以选择您想要使用的身份验证方法（**Kerberos Single Sign On**（**Kerberos** 单点登录）或 **SAML/CAS**）。

   请务必为您选择的身份验证方法完成所有必要的预部署和配置步骤。
6. 如果您选择了 **Kerberos Single Sign On**（**Kerberos** 单点登录），请指定在配置 Kerberos 时创建的身份验证配置文件。



7. 指定面向客户端的接口。

   这是您在之前的步骤中配置的客户端流量接口。
8. 为传出到互联网的流量指定出站区域。

   如果尚未配置出站区域，则可以选择 **Create New**（新建）以新建一个区域。
9. 指定要连接到的主 DNS 服务器和辅助 DNS 服务器的 IP 地址。
10. 指定 DNS 代理连接的接口。
11. （可选）指定 **Connect Timeout**（连接超时）以定义（以秒为单位）代理等待 Web 服务器响应的时间。如果在指定的时间过去后没有响应，代理将关闭连接。默认值为 5 秒。
12. （可选）如果您希望 Web 流量使用特殊端口，请指定 **Web Traffic Service Port**（网络流量服务端口）。默认端口为 80 和 443。
13. （可选）指定您在之前的步骤中配置的代理的环回接口。
14. （可选）如有合法业务需要，请取消选中 **Reset if SNI does not match HTTP CONNECT**（**SNI** 与 **HTTP CONNECT** 不匹配时重置）。

 ©2024 Palo Alto Networks, Inc.

建议保持此功能启用状态，在 CONNECT 请求和 HTTP 标头中的服务器名称指示 (SNI) 字段之间指定不同的域，从而防止域前端攻击。

15. 选择 **Save**（保存）以确认更改。

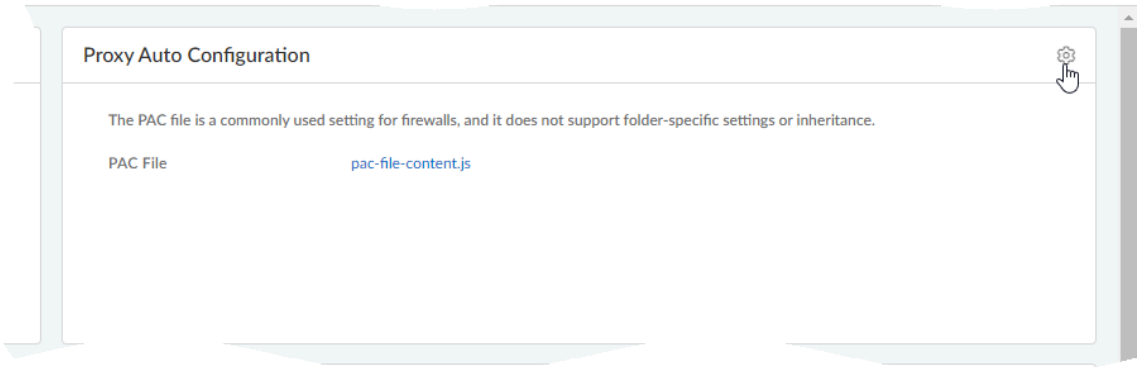
STEP 7 | 创建 Source NAT policy rule（源 NAT 策略规则）（如果适用于您的部署）。

STEP 8 | 定制 Web 访问策略，以设置您可能需要的默认策略的任何例外情况。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 如果这是您初始的显式 Web 代理配置，请更改您的代理自动配置 (PAC) 文件。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（NGFW 和 **Prisma Access**） > **Device Settings**（设备设置） > **Proxy**（代理） > **Proxy Auto Configuration**（代理自动配置）



2. 按照 PAC 文件指南 对 PAC 文件进行必要的更改。

 ©2024 Palo Alto Networks, Inc.



3. 完成更改后，保存文件。

PAC 文件将应用于与您的 *Strata Cloud Manager* 租户关联的所有防火墙。如果不同的防火墙需要不同的 *PAC* 文件，则必须手动将不同的 *PAC* 文件上传到这些防火墙。

 ©2024 Palo Alto Networks, Inc.

配置透明代理

在何处可以使用？	需要提供什么？
• NGFW（云管理） • NGFW（PAN-OS 或 Panorama 托管）	❑ Web 代理许可证 ❑ （对于云管理的 NGFW）AIOps for NGFW Premium许可证。

使用透明代理，客户端浏览器不知道代理。透明代理支持内联模式部署，不支持 Web 缓存通信协议 (WCCP)。透明代理对用户是透明的，不需要额外的身份验证。

- PAN-OS
- Strata Cloud Manager

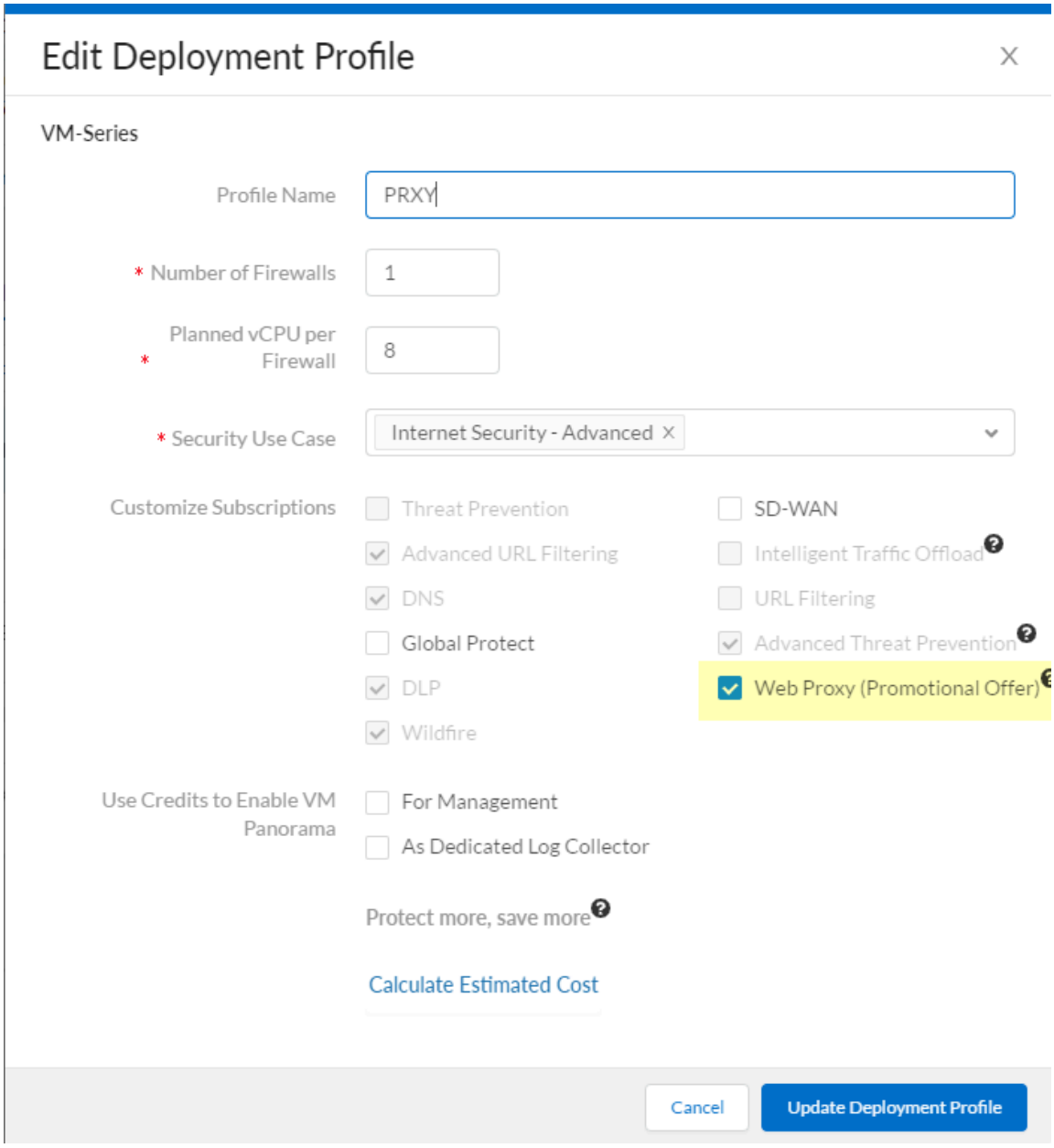
 ©2024 Palo Alto Networks, Inc.

PAN-OS

STEP 1 | （仅限 VM 系列）如果您尚未这样做，请激活 Web 代理的许可证。

PA-1400、*PA-3400* 和 *VM* 系列需要此步骤。以下步骤适用于 *VM* 系列；对于 *PA-1400* 和 *PA-3400*，请按照步骤激活订阅许可证。

1. 登录到客户服务门户 (CSP)。
2. **Edit**（编辑）部署配置文件。
3. 选择 **Web Proxy (Promotional Offer)**（**Web** 代理（促销优惠））。



4. 单击 **Update Deployment Profile**（更新部署配置文件）。
5. 在防火墙上，从服务器检索 许可证密钥 。

 ©2024 Palo Alto Networks, Inc.

如果许可证密钥检索不成功，请重新启动防火墙并在继续之前重复此步骤。

STEP 2 | 设置区域和接口。

作为最佳实践，对所有接口使用第 *3* 层 *(L3)*，并在相同的虚拟路由器和相同的虚拟系统中为每个接口配置一个单独的区域。

1. 为客户端配置一个接口。
2. 为到 Internet 的传出流量配置接口。
3. 为代理配置环回接口。

   所有传入流量都通过此接口路由到代理。请务必仔细复制此接口的 *IP* 地址并将其保存在安全位置，因为在配置 *Web* 代理时必须将其作为 ***Proxy IP***（代理 ***IP***）地址输入。

STEP 3 | 为透明代理设置 DNS 代理。

1. 为代理连接配置 DNS 代理对象 。
2. 使用主 DNS 服务器和辅助 DNS 服务器配置 DNS 服务器配置文件 。

   您必须为 *Web* 代理配置主 *DNS* 服务器和辅助 *DNS* 服务器。

3. 指定代理连接的环回 接口 。

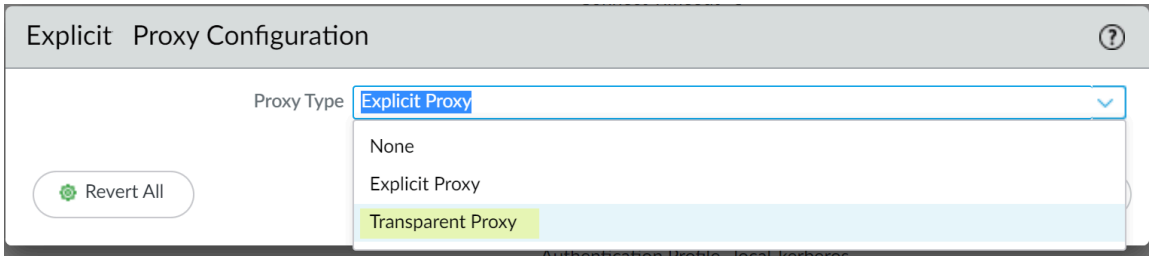
STEP 4 | 要为 MITM 检测启用解密，请创建 自签名根 CA 证书 或导入由您的企业证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅 管理访问的最佳做法。

 ©2024 Palo Alto Networks, Inc.

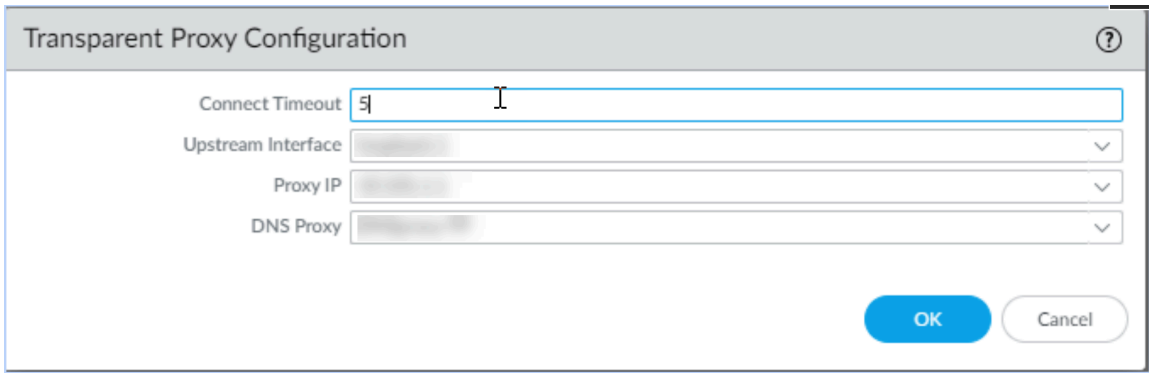
STEP 5 | 设置透明代理。

1. 在防火墙上，选择 **Network**（网络） > **Proxy**（代理），然后选择 **Edit**（编辑） **Proxy Enablement**（代理启用） 设置。
2. 选择 **Transparent Proxy**（透明代理） 作为 **Proxy Type**（代理类型），然后单击 **OK**（确定） 以确认更改。

   如果唯一可用的选项是无，请验证您是否具有 *Web* 代理功能的有效许可证。



3. **Edit**（编辑） **Transparent Proxy Configuration**（透明代理配置）。



4. 指定 **Connect Timeout**（连接超时） 以定义（以秒为单位）代理等待来自 Web 服务器的 TCP 响应的时间。如果在指定的时间过去后没有响应，代理将关闭连接。
5. 选择 **Upstream Interface**（上游接口）。

   上游接口必须是不与任何其他子网关联的环回接口。

6. 将环回接口的 IP 地址指定为 **Proxy IP**（代理 **IP**）。
   输入您在之前的步骤中配置的接口的 IP 地址。
7. 指定您在之前的步骤中创建的 **DNS** 代理对象

   将环回接口指定为 ***Upstream Interface***（上游接口）。

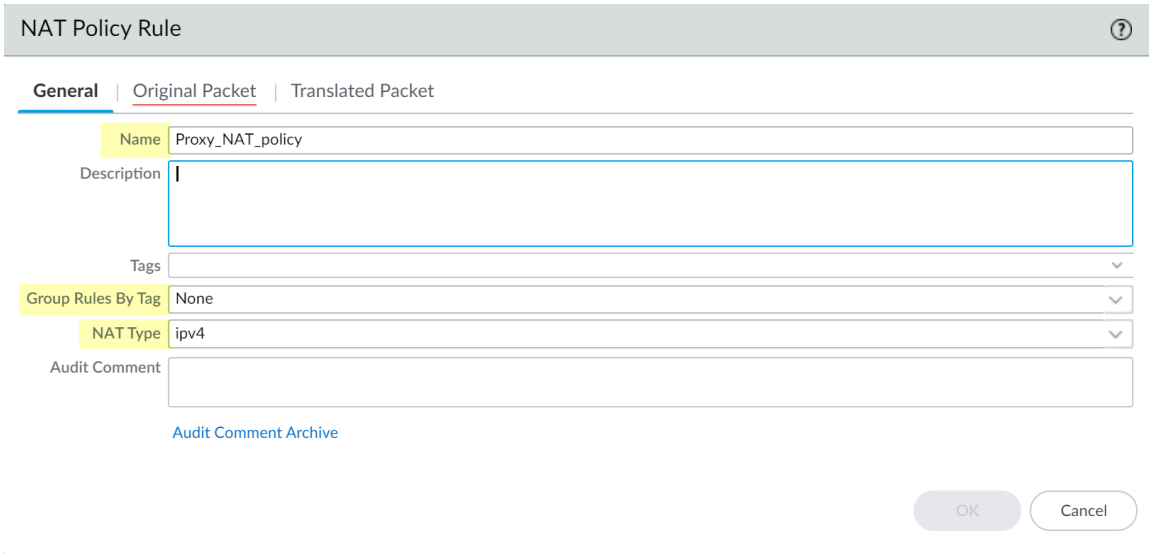
8. 单击 **OK**（确定） 以确认更改。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 配置目标网络地址转换 (DNAT) 策略。

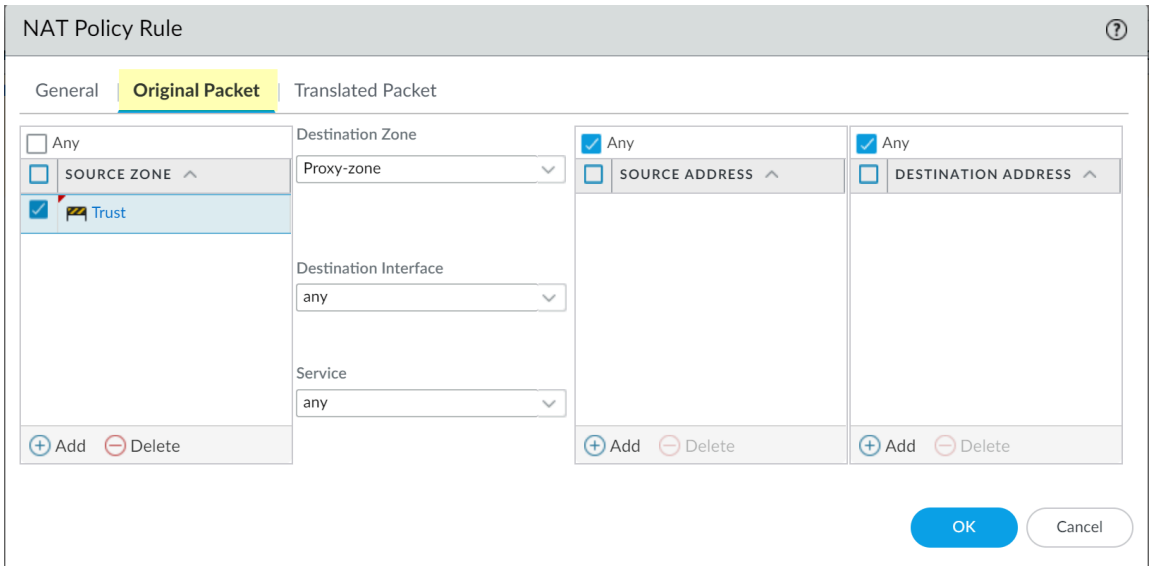
您必须完全按照以下步骤中的描述配置 *DNAT* 策略规则，防火墙才能成功使用 *Web* 代理路由流量。请务必配置 *DNAT* 策略规则，使其位于源网络地址转换 *(SNAT)* 策略规则之前。

1. 依次选择 **Policies**（策略） > **NAT**、**Add**（添加）、NAT，以添加一个 NAT 策略规则。
2. 输入一个唯一的 **Name**（名称） 并验证 **Group Rules by Tag**（使用标记对规则分组） 是否为 **None**（无），然后选择 **NAT Type**（**NAT** 类型）。

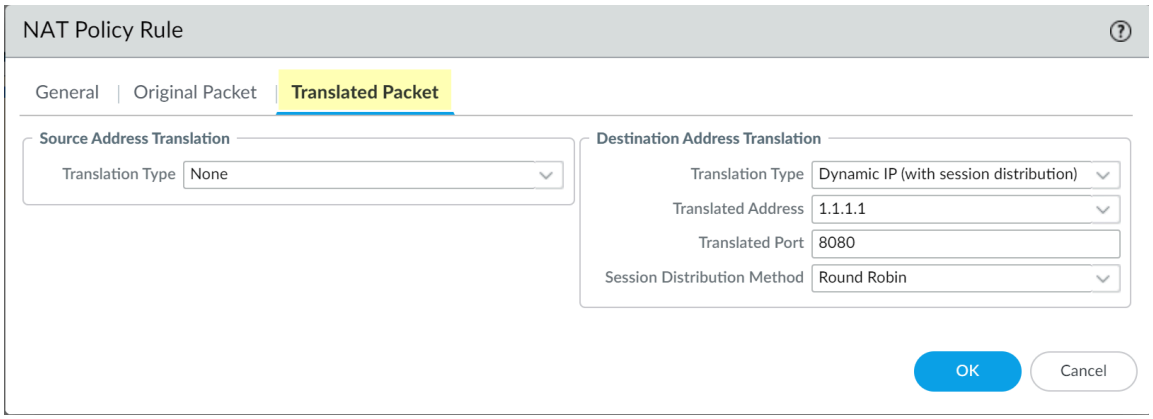


3. 选择 **Original Packet**（原始数据包） 并 **Add**（添加） 受信任区域作为 **Source Zone**（源区域） 和 **Destination Zone**（目标区域） 作为包含 Web 代理的接口。

 ©2024 Palo Alto Networks, Inc.



4. 选择 **Translated Packet**（转换后的数据包） 并确认 **Source Address Translation**（源地址转换）的 **Translation Type**（转换类型） 是 **None**（无）。



5. 选择 **Dynamic IP (with session distribution)**（动态 IP（带会话分发） 作为 **Destination Address Translation**（目标地址转换）的 **Translation Type**（转换类型）。
6. 输入 Web 代理的 IP 地址作为 **Translated Address**（转换后的地址）。

   输入与之前步骤中指定的代理 IP 地址相同的 IP 地址。
7. 输入 **8080** 作为 **Translated Port**（转换后的端口）。
8. 选择 **Session Distribution Method**（会话分发方法） （例如， **Round Robin**（循环法））。

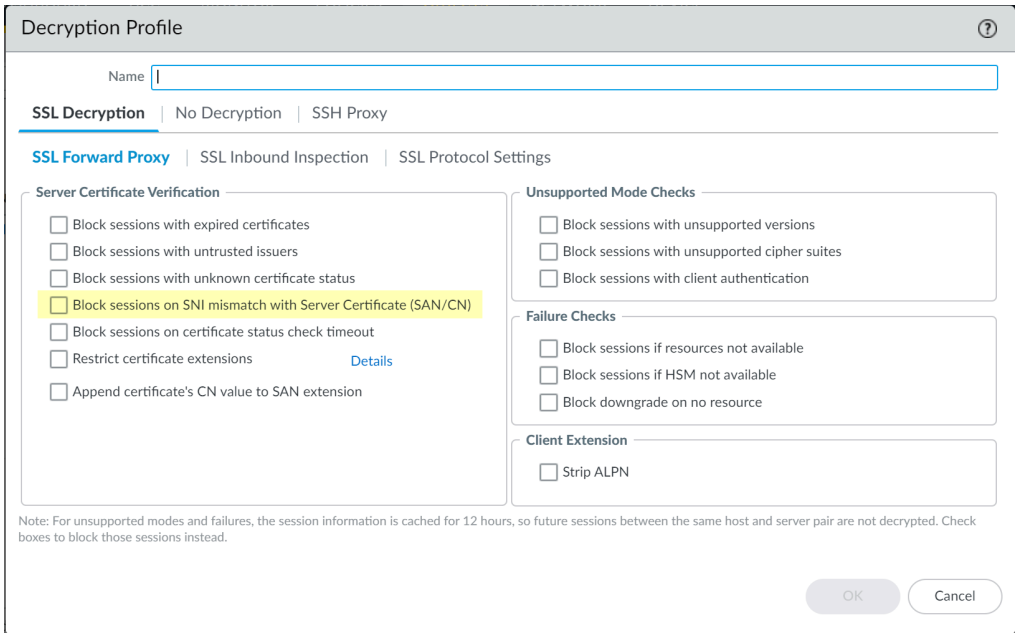
   会话分发方法不适用于 Web 代理。
9. 单击 **OK**（确定）并 **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 配置安全策略以允许和路由代理流量。

1. 在 DNAT 规则之后配置源网络地址转换 (SNAT) 策略规则。
2. 配置解密策略对流量进行 解密 。

   选择包含代理接口的区域作为源区域。
3. （可选，但推荐）选择 **Objects**（对象） > **Decryption Profile**（解密配置文件） 并选择 在 **SNI** 与服务器证书 **(SAN/CN)** 不匹配 时阻止会话以自动拒绝服务器名称指示 (SNI) 与服务器证书不匹配的任何会话。



4. 配置策略规则以允许客户端和代理访问 DNS 代理服务器。
5. 配置策略规则以允许从客户端到代理的流量。
6. 配置策略规则以允许从代理到互联网的流量。

STEP 8 | 如果这是初始透明 Web 代理配置，请在代理配置（**Network**（网络） > **DNS Proxy**（**DNS** 代理））和接口配置（**Network**（网络） > **Interfaces**（接口））中进行更改，然后选择 **Commit**（提交）提交更改以确保透明 Web 代理配置在防火墙上正确填充。

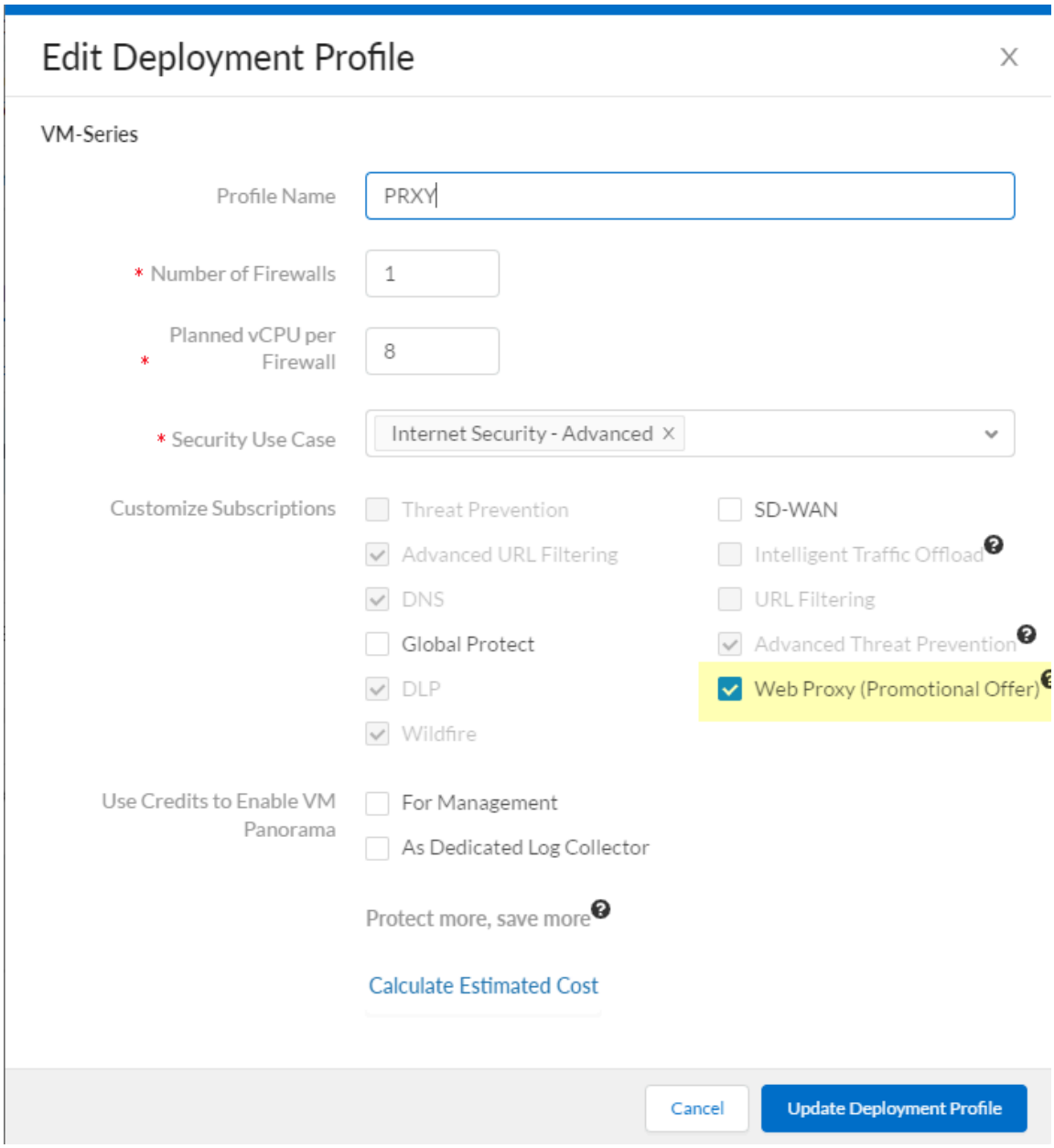
Strata Cloud Manager

 ©2024 Palo Alto Networks, Inc.

STEP 1 | （仅限 VM 系列）如果您尚未这样做，请激活 Web 代理的许可证。

PA-1400、*PA-3400* 和 *VM* 系列需要此步骤。以下步骤适用于 *VM* 系列；对于 *PA-1400* 和 *PA-3400*，请按照步骤激活订阅许可证。

1. 登录到客户服务门户 (CSP)。
2. **Edit**（编辑） 部署配置文件。
3. 选择 **Web Proxy (Promotional Offer)**（**Web** 代理（促销优惠））。



4. 单击 **Update Deployment Profile**（更新部署配置文件）。
5. 在防火墙上，从服务器检索 许可证密钥 。

如果许可证密钥检索不成功，请重新启动防火墙并在继续之前重复此步骤。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 设置必要的接口和区域。

请勿编辑代理区域。

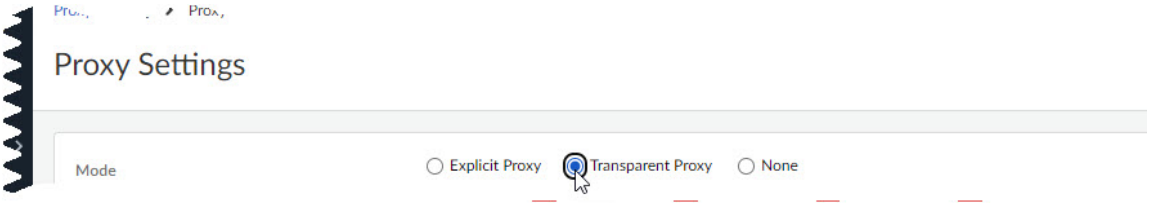
作为最佳实践，对所有接口使用第 3 层 (L3)，并在相同的虚拟路由器和相同的虚拟系统中为每个接口配置一个单独的区域。

1. 为客户端配置一个接口。
2. 为到 Internet 的传出流量配置接口。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 设置透明代理。

1. 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（设备设置） > 配置范围（**Configuration Scope**）。
2. 选择您想要配置透明代理的文件夹、片段或设备。
3. 选择 **Device Settings**（设备设置） > **Proxy**（代理） > **Proxy Settings**（代理设置） > **Customize**（定制）。
4. 针对 **Mode**（模式），选择 **Transparent Proxy**（透明代理）。



5. 指定面向客户端的接口。

   这是您在之前的步骤中配置的客户端流量接口。
6. 为传出到互联网的流量指定出站区域。

   如果尚未配置出站区域，则可以选择 **Create New**（新建）以新建一个区域。
7. 指定要连接的主 DNS 服务器和辅助 DNS 服务器的 IP 地址以及 DNS 代理连接的接口。

   推送配置后，Strata Cloud Manager 将在您的设备上自动创建具有这些规范的 DNS 代理对象。您可以在设备本身上查看对象，但不能在 Strata Cloud Manager 中查看。
8. （可选）指定 **Connect Timeout**（连接超时）以定义（以秒为单位）代理等待 Web 服务器响应的时间。如果在指定的时间过去后没有响应，代理将关闭连接。默认值为 5 秒。
9. （可选）如果您希望 Web 流量使用特殊端口，请指定 **Web Traffic Service Port**（网络流量服务端口）。默认端口为 80 和 443。
10. （可选）使用默认环回接口 **(loopback.999)** 或输入其他接口。

    环回接口必须遵循格式 **loopback.x**，其中 x 是任意整数值。

    在您推送配置后，Strata Cloud Manager 将自动在您的设备上创建具有这些规格的环回接口。您可以在设备本身上查看接口，但不能在 Strata Cloud Manager 中查看。
11. （可选）选择 是否对出站流量进行 **NAT**，然后在 **Outbound Interface**（出站接口）中输入出站接口。

    这将创建一个源 NAT 规则。如果您的网络无法直接访问互联网，请选择此项。
12. **Save**（保存）。

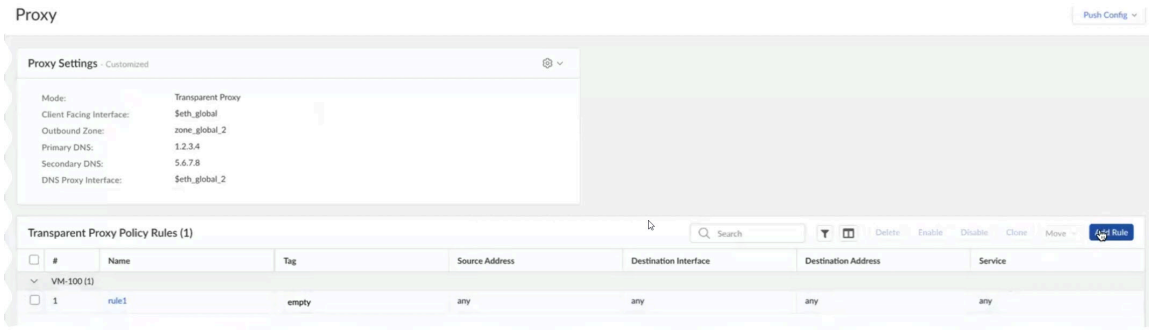
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 配置透明代理策略规则。

这组规则可决定哪些流量能够通过代理。在您推送配置后，这些规则会在您的设备上创建目标 NAT 规则，这些规则会将 NAT 应用于通过先前配置的环回接口的流量。

但在 Strata Cloud Manager 中，透明代理策略规则仅在 **Web** 代理配置中显示，在应用程序中其他地方的 **NAT** 中不会显示。

1. 选择 **Add Rule**（添加规则）。

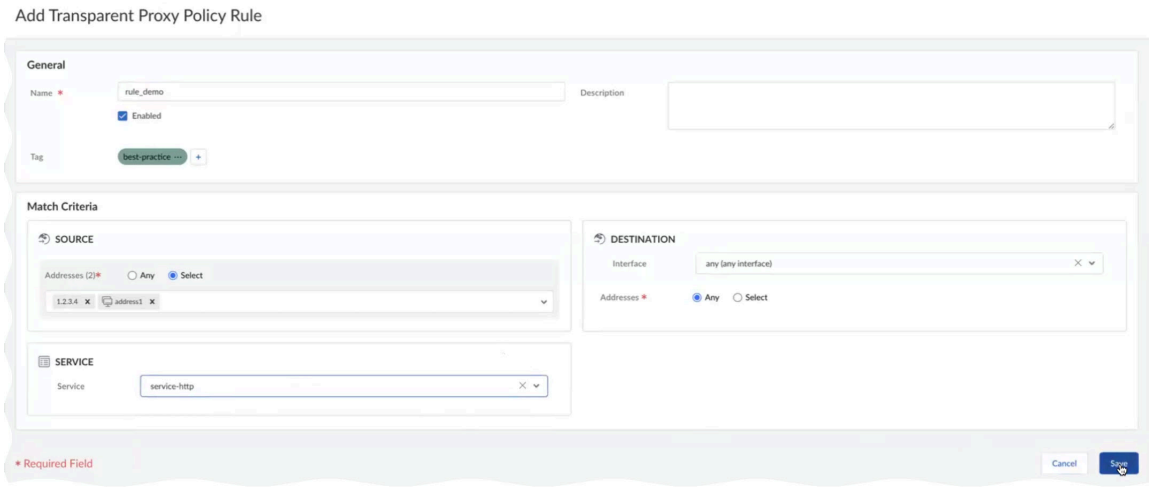


2. 选择 **Name**（命名）以命名规则。
3. （可选）添加标签来标记您的规则。
4. 指定源地址或将其保留为 **Any**。
5. 指定目标地址或将其保留为 **Any**。
   （可选）指定目标接口。

 ©2024 Palo Alto Networks, Inc.

6. （可选）选择 **Service**（服务）。
7. **Save**（保存）。

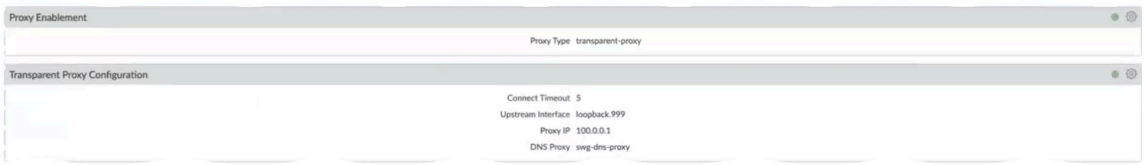
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 5 | 推送您的配置并在防火墙上验证。

1. 要进行验证，请登录防火墙并选择 **Network**（网络） > **Proxy**（代理）。
2. 您应该会看到与您刚刚配置的透明代理相对应的信息。



为显式 Web 代理配置身份验证

配置显式 Web 代理时，请配置以下用户身份验证方法之一：

- 配置 Kerberos 身份验证
- 配置 SAML 身份验证
- 配置云身份引擎身份验证

如果要对来自特定设备（如打印机）的通信免除身份验证，则可以配置显式代理身份验证的豁免。

如果不需要为 Web 代理流量配置身份验证，则可以为所有显式代理流量免除身份验证。

配置 Kerberos 身份验证

STEP 1 | 为目录创建服务帐户（如果尚未配置），并在服务帐户属性中启用对 AES128 和 AES256 加密的支持。

STEP 2 | 为代理 FQDN 注册服务主体名称 (SPN)，为 Kerberos 单点登录 (SSO) 创建密钥表文件。

Kerberos 密钥表体名称必须与解析为代理接口 IP 地址的主机名相匹配。

STEP 3 | 在防火墙上，为 Kerberos 服务器创建服务器配置文件。

STEP 4 | 配置身份验证配置文件以使用 Kerberos 并将密钥表导入到身份验证配置文件中。

 ©2024 Palo Alto Networks, Inc.

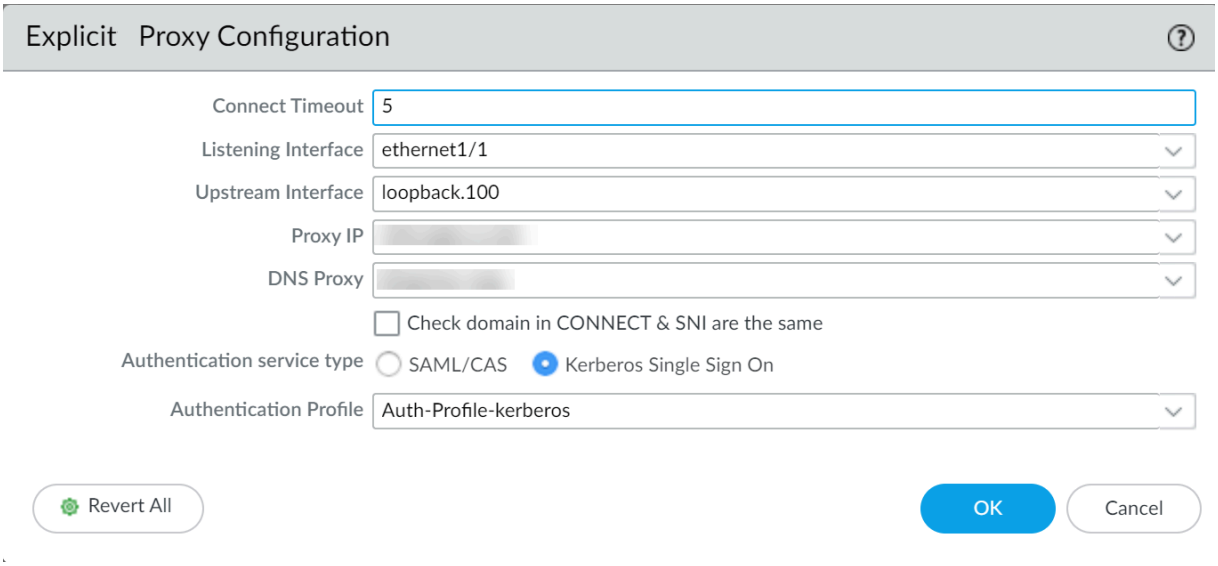
STEP 5 | （可选，但推荐）如果您使用 Panorama 管理防火墙，请配置日志转发配置文件以将日志转发到 Cortex 数据湖 (CDL)、Panorama 或两者。

默认情况下，防火墙不将日志转发到 CDL 或 Panorama。转发日志可确保完整的身份验证日志信息可用于帮助解决任何潜在的身份验证问题。

最佳做法是，如果您使用 *Panorama* 管理 *Web* 代理防火墙，请在共享 *Panorama* 位置配置代理使用的任何对象，并在不包含其他防火墙或虚拟系统的单独设备组中配置 *Web* 代理防火墙。如果防火墙已经是设备组的成员，则创建子设备组作为子组并将防火墙移动到子设备组。

如果使用 *Chrome* 浏览器时遇到浏览器质询问题，我们建议您使用其他浏览器。

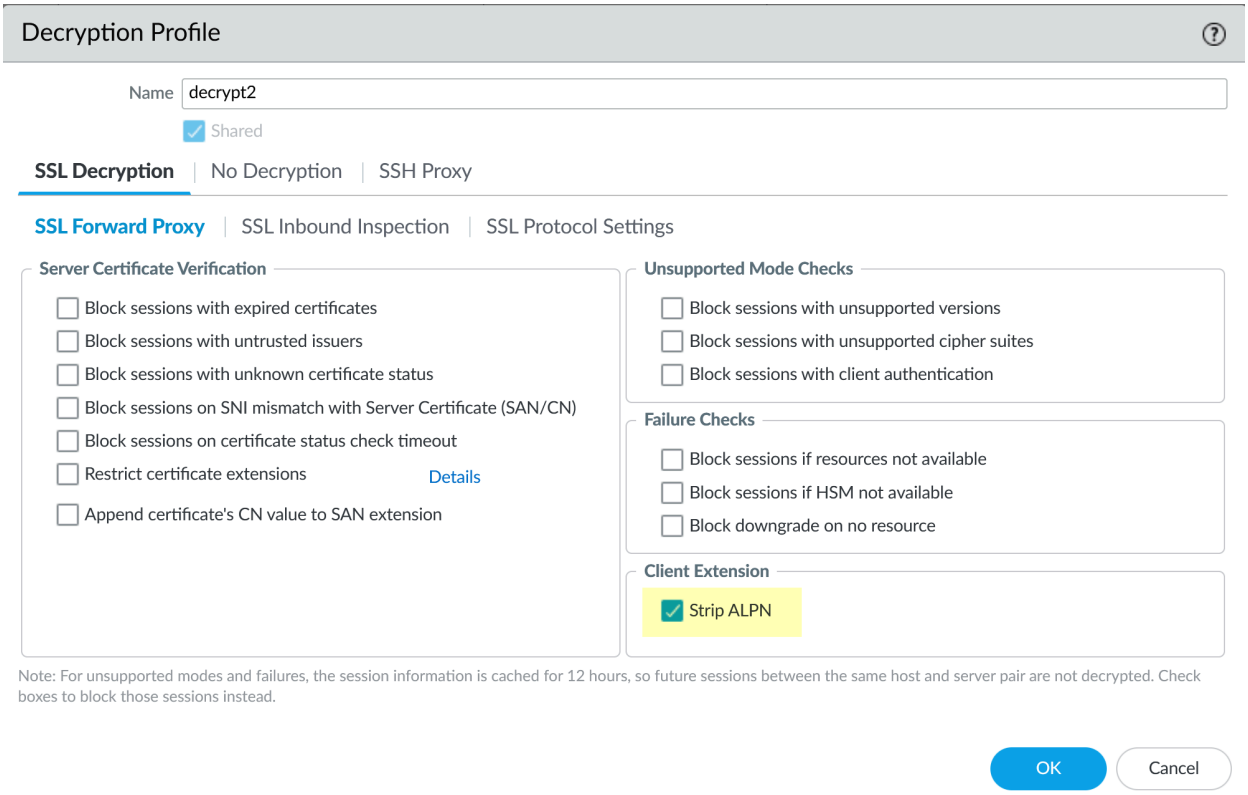
STEP 6 | 在 **Explicit Proxy Configuration**（显式代理配置）（**Network**（网络） > **Proxy**（代理） > **Explicit Proxy Configuration**（显式代理配置））中，选择 **Kerberos Single Sign On**（**Kerberos** 单点登录）作为身份验证服务类型。



 ©2024 Palo Alto Networks, Inc.

STEP 7 | （可选，但建议使用）如果您对流量使用解密策略，请选择 **Strip ALPN**（删除 **ALPN**）以删除应用层协议协商 (ALPN) 中的值。

此选项需要 *HTTPS*。



STEP 8 | 选择您在步骤 4 中创建的 **Authentication Profile**（身份验证配置文件）。

STEP 9 | 完成剩余的步骤以配置 Web 代理。

配置 SAML 身份验证

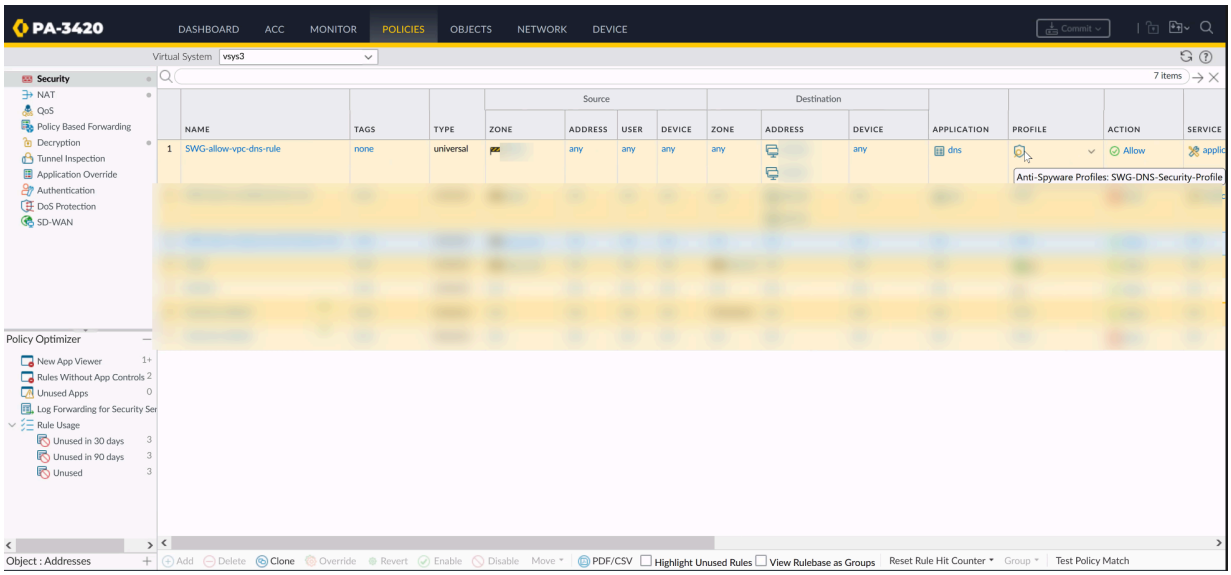
显式 *Web* 代理的 *SAML* 身份验证需要 *Panorama* 和云服务插件版本 *3.2.1*（及更高版本）。

为了简化显式 Web 代理的基于 SAML 的身份验证的配置，防火墙或 Panorama 会自动生成以下规则以允许必要的流量。如果您使用的是 Panorama，则必须选择单个防火墙才能查看规则。

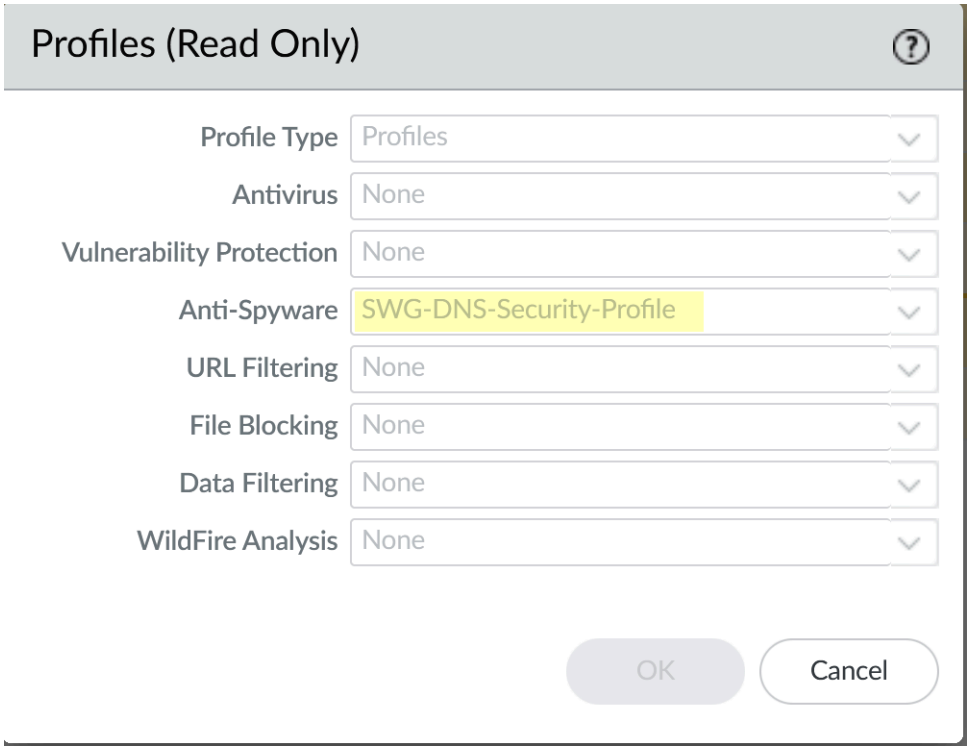
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PRO
1	SWG-allow-vpc-dns-rule	none	universal	swg	any	any	any	any		any	dns	application-...	Allow	
2	SWG-block-unsollicited-dns-rule	none	universal	swg	any	any	any	any		any	dns	application-...	Drop	none
3	SWG-allow-outbound-auth-domain-rule	none	universal	swg	any	any	any	any	any	any	any	any	Allow	none

 ©2024 Palo Alto Networks, Inc.

- **SWG-allow-vpc-dns-rule** — 允许从 Web 代理上游接口所在区域的流量流向 Web 代理的主 DNS 服务器地址和辅助 DNS 服务器地址。

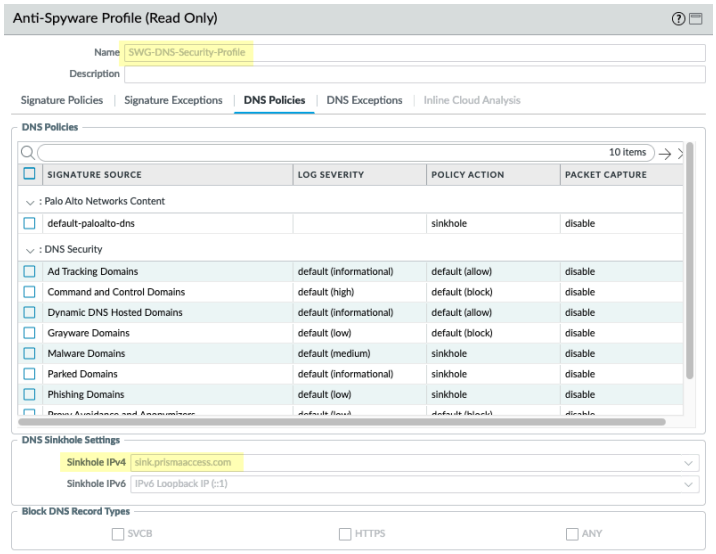


防火墙还会生成防间谍软件配置文件 `SWG-DNS-Security-Profile`，以允许所需的流量。



自动生成的规则 `SWG-allow-vpc-dns-rule` 将此配置文件应用于适用的流量。

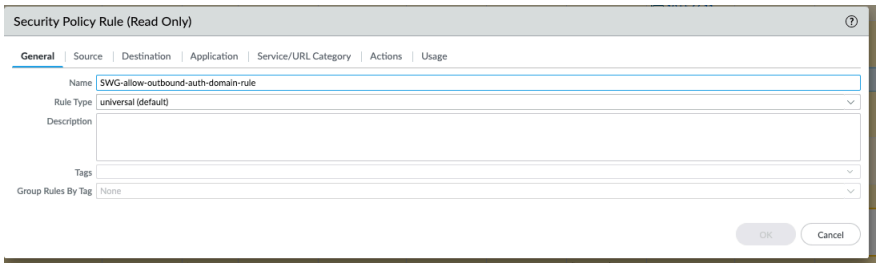
 ©2024 Palo Alto Networks, Inc.



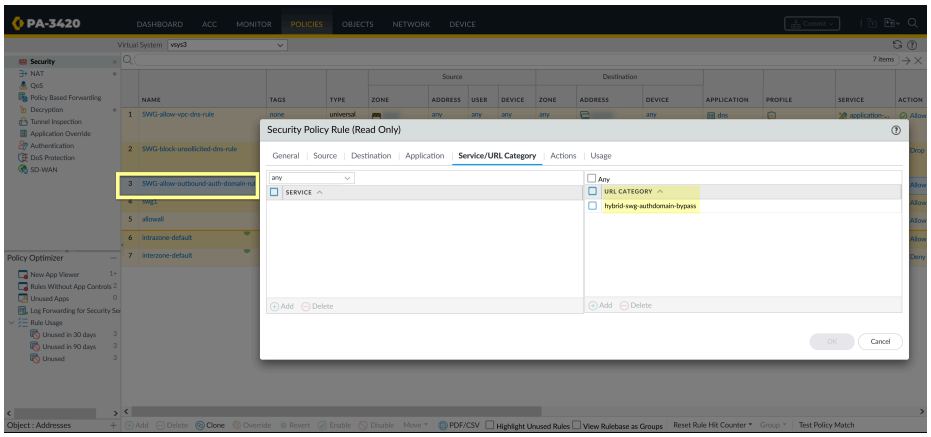
- **SWG-block-unsolicited-dns-rule** —阻止未经授权的流量流向 Web 代理的主 DNS 服务器地址和辅助 DNS 服务器地址。

 ©2024 Palo Alto Networks, Inc.

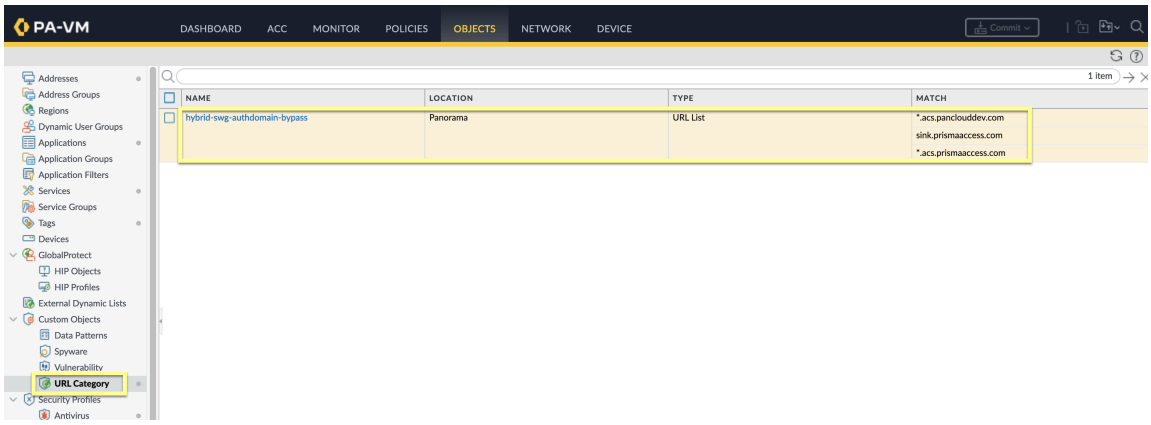
- **SWG-allow-outbound-auth-domain-rule** —（仅支持 SAML 身份验证的显式代理）允许流量从 Web 代理上游接口所在区域流向云服务插件。



自动生成的规则 `SWG-allow-outbound-auth-domain-rule` 将 `hybrid-swg-authdomain-bypass` URL 类别应用于适用的流量。



URL 类别 `hybrid-swg-authdomain-bypass`包含所需域的必要预定义条目。



STEP 1 | 如果您尚未这样做，请为移动用户配置显式代理。

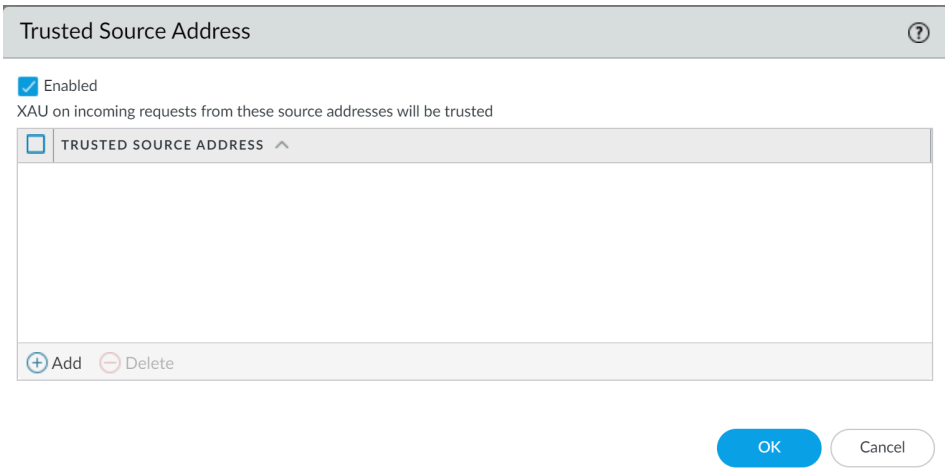
这是本地 Web 代理身份验证和 Prisma Access 显式代理的典型身份验证方法，后者需要许可证。Prisma Access Cookie 和超时值的显式代理设置也适用于显式 Web 代理配置。在继续操作之前，您必须提交更改并将其推送到相关的防火墙。

STEP 2 | 如果您尚未这样做，请配置 SAML 身份验证配置文件。

 ©2024 Palo Alto Networks, Inc.

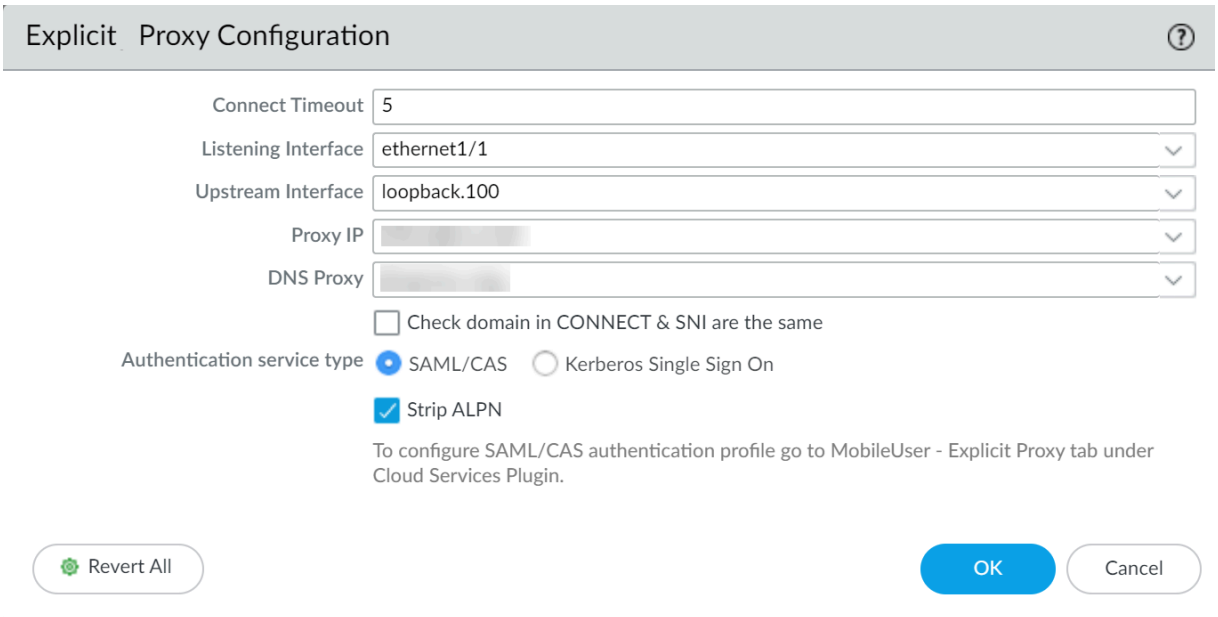
STEP 3 | （仅适用于 XAU）如果下游代理发送 XAU 标头，请为下游代理配置可信源地址。

1. 选择 **Device**（设备） > **User Identification**（用户识别） > **Trusted Source Address**（可信源地址）。
2. **Edit**（编辑）可信源地址的设置，将状态更改为 **Enabled**（启用）。



3. **Add**（添加）您想要允许 X 身份验证用户 (XAU) 的任何地址对象。
   显式 Web 代理需要一个 IP 地址对象作为可信源地址。
4. 单击 **OK**（确定）。

STEP 4 | 在 **Explicit Proxy Configuration**（显式代理配置）（**Network**（网络） > **Proxy**（代理） > **Explicit Proxy Configuration**（显式代理配置））中，选择 **SAML/CAS** 作为身份验证服务类型。



 ©2024 Palo Alto Networks, Inc.

STEP 5 | （可选，但建议使用）如果您对流量使用解密策略，请选择 **Strip ALPN**（去除 **ALPN**）以删除应用层协议协商 (ALPN) 中的值。

此选项需要 *HTTPS*。

STEP 6 | 完成其余步骤以配置配置 Web 代理。

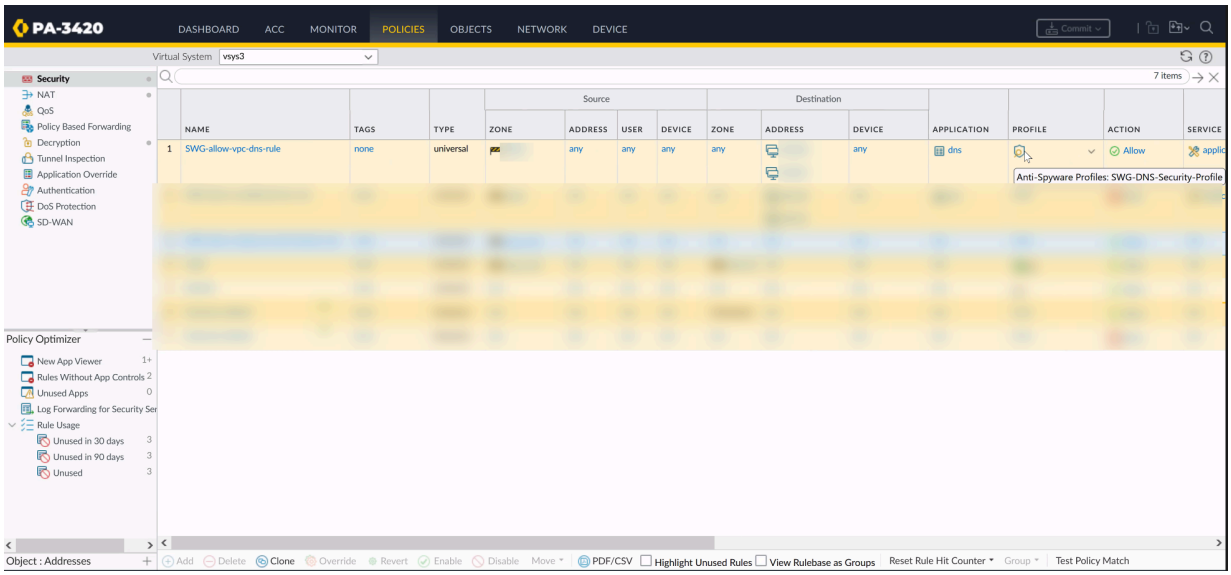
配置云身份引擎身份验证

为了简化显式 Web 代理的基于 SAML 的身份验证的配置，防火墙或 Panorama 会自动生成以下规则以允许必要的流量。如果您使用的是 Panorama，则必须选择单个防火墙才能查看规则。

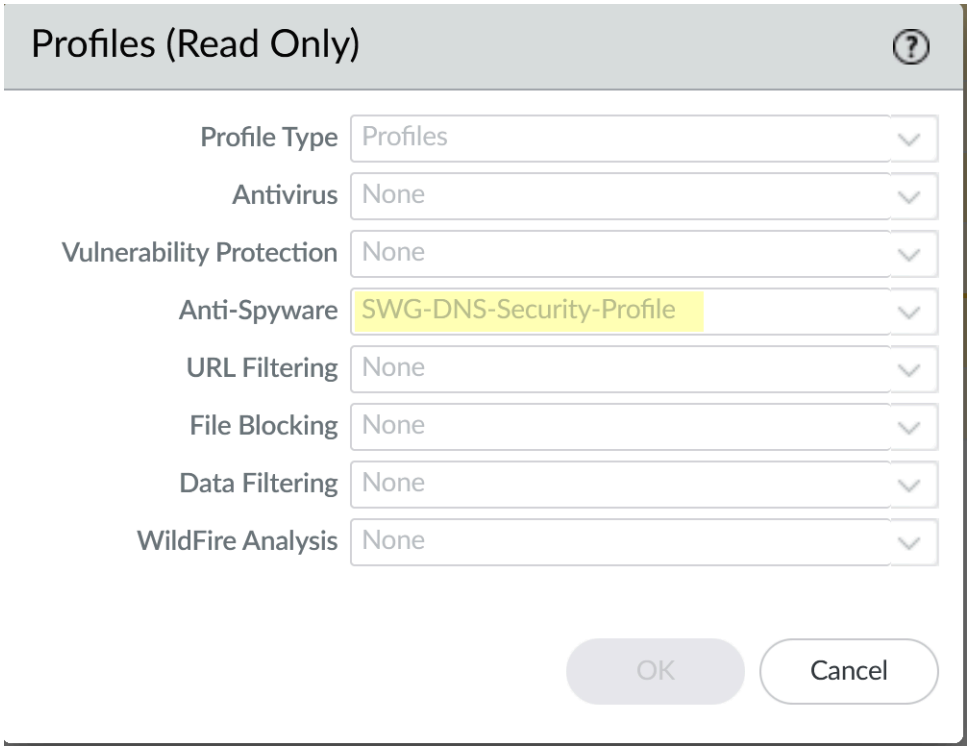
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PRO
1	SWG-allow-vpc-dns-rule	none	universal	swg	any	any	any	any	[redacted]	any	dns	application-...	Allow	
2	SWG-block-unsollicited-dns-rule	none	universal	swg	any	any	any	any	[redacted]	any	dns	application-...	Drop	none
3	SWG-allow-outbound-auth-domain-rule	none	universal	swg	any	any	any	any	any	any	any	any	Allow	none

 ©2024 Palo Alto Networks, Inc.

- **SWG-allow-vpc-dns-rule** — 允许从 Web 代理上游接口所在区域的流量流向 Web 代理的主 DNS 服务器地址和辅助 DNS 服务器地址。

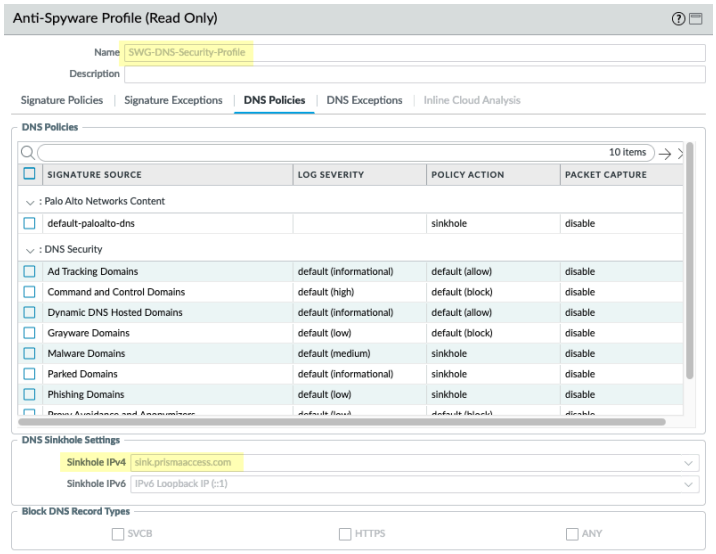


防火墙还会生成防间谍软件配置文件 `SWG-DNS-Security-Profile`，以允许所需的流量。



自动生成的规则 `SWG-allow-vpc-dns-rule` 将此配置文件应用于适用的流量。

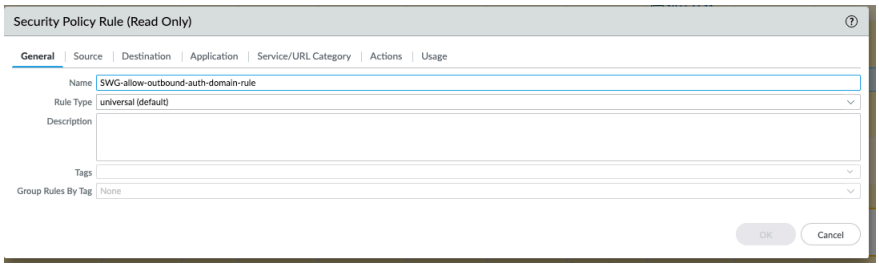
 ©2024 Palo Alto Networks, Inc.



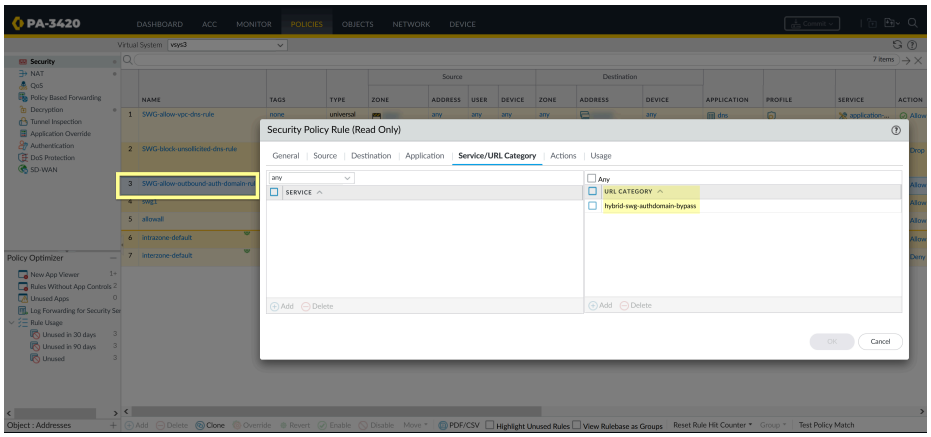
- **SWG-block-unsolicited-dns-rule** —阻止未经授权的流量流向 Web 代理的主 DNS 服务器地址和辅助 DNS 服务器地址。

 ©2024 Palo Alto Networks, Inc.

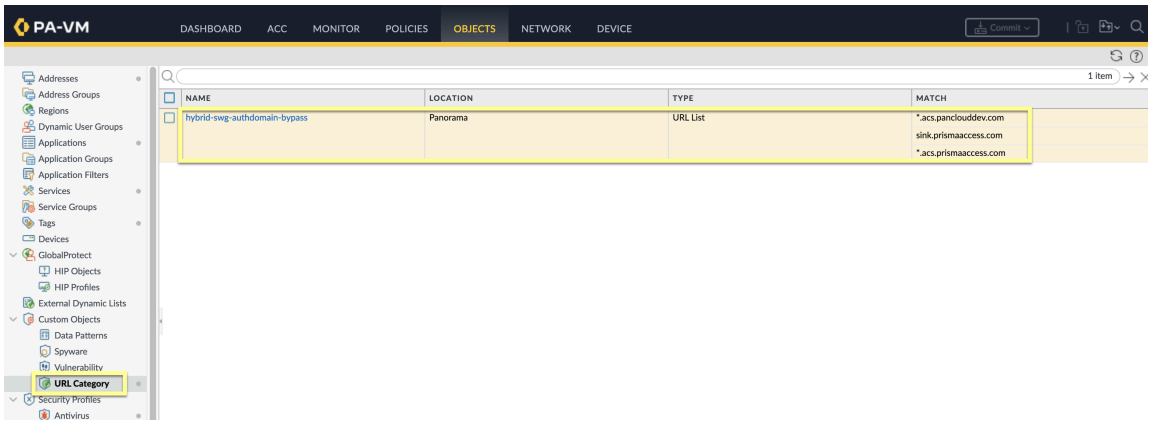
- **SWG-allow-outbound-auth-domain-rule** —（仅支持 SAML 身份验证的显式代理）允许流量从 Web 代理上游接口所在区域流向云服务插件。



自动生成的规则 `SWG-allow-outbound-auth-domain-rule` 将 `hybrid-swg-authdomain-bypass` URL 类别应用于适用的流量。



URL 类别 `hybrid-swg-authdomain-bypass`包含所需域的必要预定义条目。



STEP 1 | 如果您尚未这样做，请为移动用户配置显式代理。

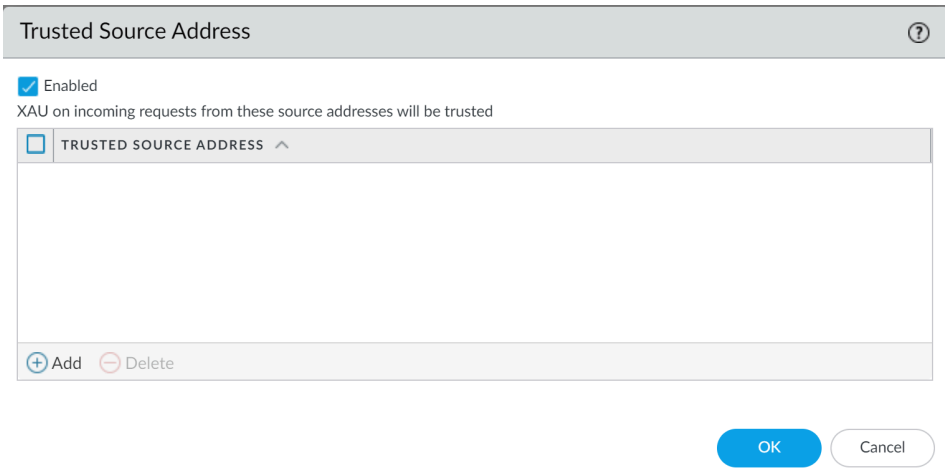
在继续操作之前，您必须提交更改并将其推送到相关的防火墙。

STEP 2 | 如果您尚未这样做，请使用云身份引擎配置身份验证并配置云身份引擎身份验证配置文件。

 ©2024 Palo Alto Networks, Inc.

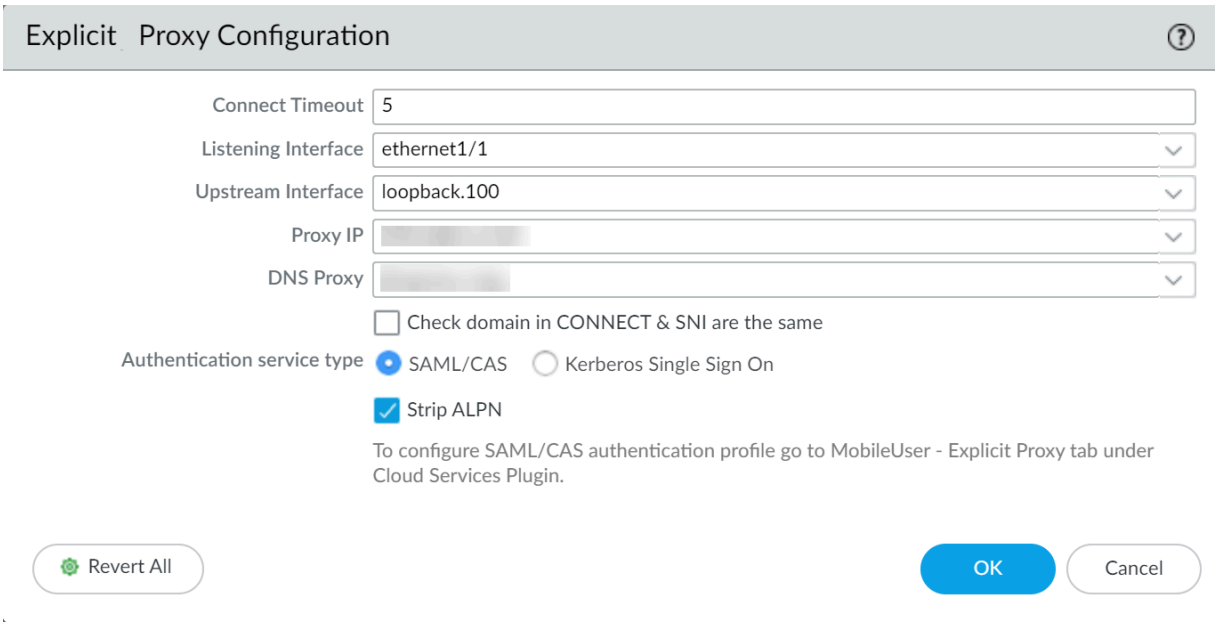
STEP 3 | （仅适用于 XAU）如果下游代理发送 XAU 标头，请为下游代理配置可信源地址。

1. 选择 **Device**（设备） > **User Identification**（用户识别） > **Trusted Source Address**（可信源地址）。
2. **Edit**（编辑）可信源地址的设置，将状态更改为 **Enabled**（启用）。



3. **Add**（添加）您想要允许 X 身份验证用户 (XAU) 的任何地址对象。
   显式 Web 代理需要一个 IP 地址对象作为可信源地址。
4. 单击 **OK**（确定）。

STEP 4 | 在 **Explicit Proxy Configuration**（显式代理配置）（**Network**（网络） > **Proxy**（代理） > **Explicit Proxy Configuration**（显式代理配置））中，选择 **SAML/CAS** 作为身份验证服务类型。



STEP 5 | （可选，但推荐）选择 **Strip ALPN**（去除 **ALPN**） 以删除应用层协议协商 (ALPN) 中的值。

此选项需要 *HTTPS*。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 完成其余步骤以配置配置 Web 代理。

配置显式代理身份验证的豁免

使用 Web 代理允许您通过统一的界面使用来自网络中的代理设备的信息。但是，打印机或其他物联网设备等资源无法响应来自代理的身份验证请求，也不支持证书和 PAC 文件。

您可以使用源的地址对象和/或自定义 URL 类别例外列表作为目标，从而为这些设备免除代理身份验证请求。通过为显式代理配置身份验证豁免，可确保来自这些关键资源的流量不会中断，并允许来自这些受信任设备的流量按照您的网络架构通过代理。

您可以在身份验证策略中创建最多 *20* 个 *Web* 代理豁免。

如果不需要验证显式代理流量，则可以为所有显式代理流量免除身份验证。

STEP 1 | 如果还没有这样做，请配置显式代理，然后定义您想要免除身份验证请求的代理流量类型。

您可以根据源域和/或目标域来免除流量。

- 配置一个包含受信任设备的源 IP 地址的地址对象（**Objects**（对象） > **Addresses**（地址））。源 IP 可以是地址或者地址组。
- 配置 自定义 URL 类别例外列表（**Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别）），其中包含您要允许的 Web 服务的目标 URL 域。

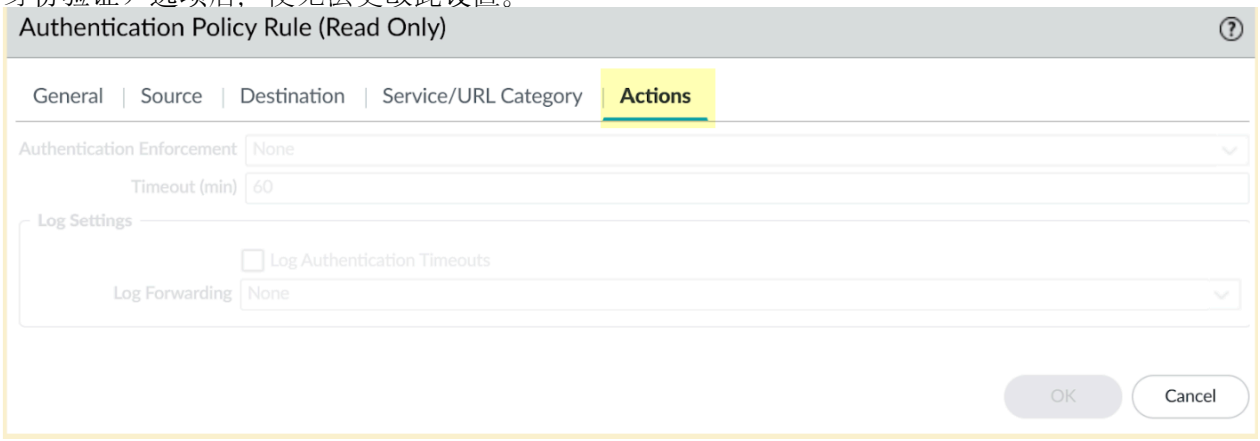
STEP 2 | 启用身份验证门户（如果尚未启用）。

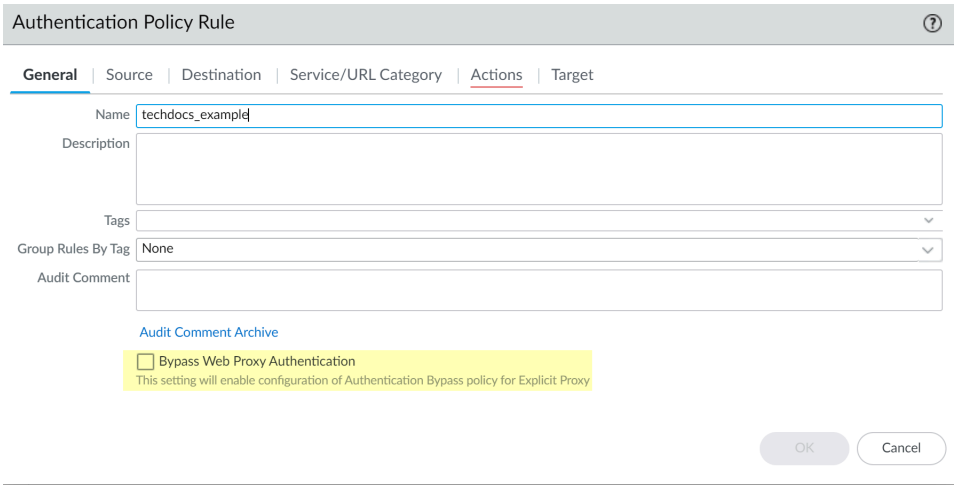
要强制执行策略规则，必须执行此步骤。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 编辑或创建您的身份验证策略规则（**Policies**（策略） > **Authentication**（身份验证））然后选择 **Bypass Web Proxy Authentication**（绕过 **Web** 代理身份验证）。

启用 ***Bypass Web Proxy Authentication***（绕过 ***Web*** 代理身份验证）选项时，***Action***（操作） 选项卡上的 ***Authentication Enforcement***（身份验证强制）选项将设置为 ***None***（无）；启用 ***Bypass Web Proxy Authentication***（绕过 ***Web*** 代理身份验证）选项后，便无法更改此设置。





STEP 4 | 在身份验证策略规则中定义您想要免于身份验证的代理流量类型，然后单击 **Commit**（提交）以提交您的更改。

您可以豁免源和/或目标。

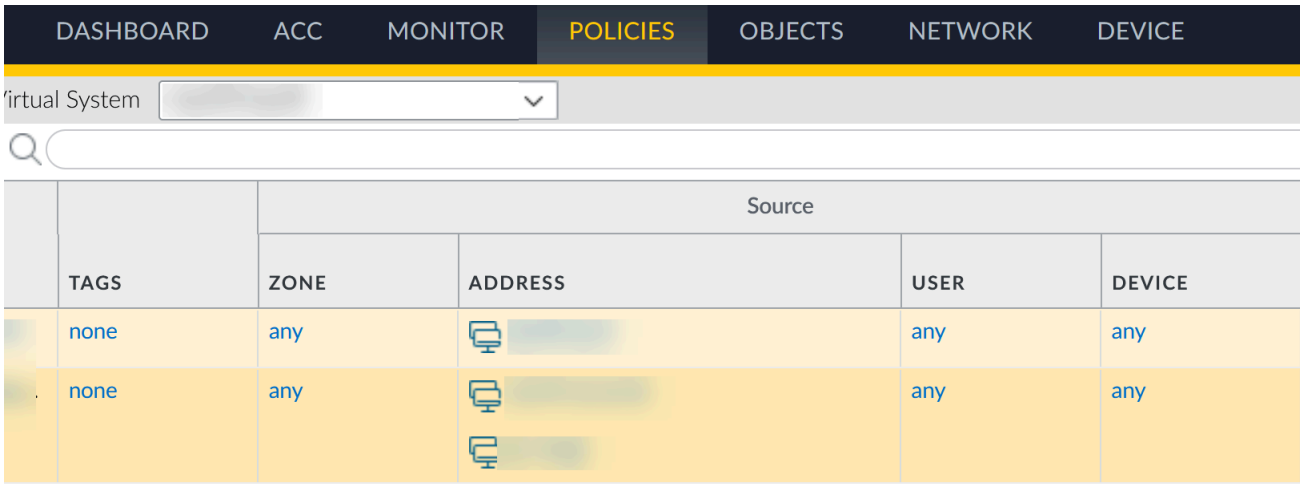
- 选择 **Source**（源）选项卡，然后选择您在第一步中配置的地址对象作为 **Source Address**（源地址），然后单击 **OK**（确定）。
- 选择 **Destination**（目标）选项卡，然后选择您在第一步中配置的 URL 类别

您必须先创建自定义 URL 类别例外列表，然后才能选择此类别作为目标。在此步骤中，您无法创建新的自定义 *URL* 类别例外列表作为目标。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 单击 **Commit**（提交）以提交您的更改并验证您的配置。

1. 查看您的策略规则（**Policies**（策略） > **Authentication**（身份验证））并确认在您启用豁免的规则的 **Bypass Web Proxy Authentication**（绕过 **Web** 代理身份验证）列中显示了复选标记。



2. 根据您的身份验证方法，使用 CLI 命令查看代理流量的豁免。
   - 如果使用 SAML 身份验证方法，则可以使用 **`show counter global name ctd_eproxy_skip_auth_url_match`** 命令来验证配置。此命令显示代理流量的 SAML 身份验证豁免的数量。
   - 如果您使用 Kerberos 身份验证服务类型，则可以使用 **`show counter global name flow_swg_ep_kerberos_skip_auth`** 命令来验证配置。此命令显示代理流量的 Kerberos 身份验证豁免数量。

为所有显式代理流量免除身份验证

如果您不想为显式代理流量配置任何身份验证，则可以为所有显式代理流量免除身份验证。如果为所有代理流量免除身份验证，防火墙或 Panorama 不会验证代理连接，也不会为身份验证事件创建任何日志。

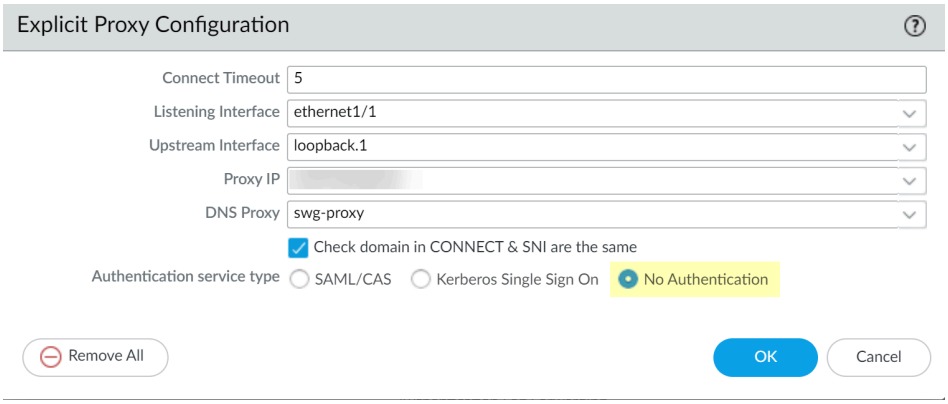
要仅为特定流量免除身份验证，您可以配置显式代理身份验证的豁免。

STEP 1 | 如果您尚未这样做，请为您的网络代理流量配置显式代理。

©2024 Palo Alto Networks, Inc.

STEP 2 | 编辑或创建您的 Web 代理配置（**Network**（网络） > **Proxy**（代理） > **Explicit Proxy**（显式代理）），对 **Authentication service type**（身份验证服务类型）选择 **No authentication**（无身份验证），然后单击 **OK**（确定）。

如果选择此选项，则会为所有代理连接免除身份验证，防火墙或 *Panorama* 不会为身份验证事件创建日志。

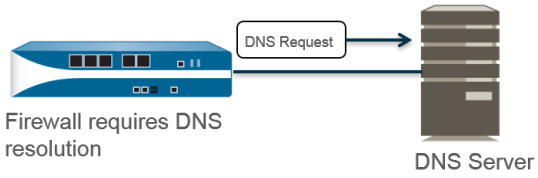


STEP 3 | **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.

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 | 编辑服务设置（对于支持多个虚拟系统的防火墙，请依次选择 **Device**（设备） > **Setup**（设置） > **Services**（服务） > **Global**（全局）；否则请依次选择 **Device**（设备） > **Setup**（设置） > **Services**（服务））。

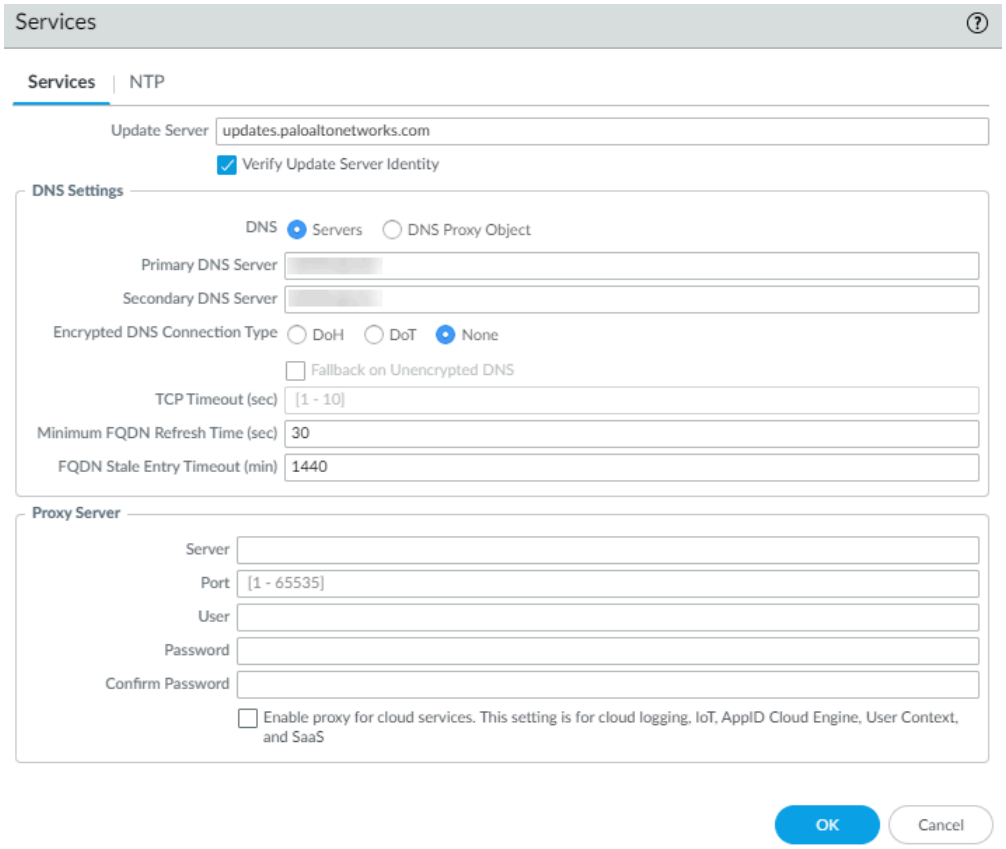
STEP 2 | 配置与 DNS 服务器（可提供 DNS 解析能力）的连接。

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. 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。
2. （PAN-OS 11.2.1 及更高版本）（可选）要为服务器连接配置加密 DNS，请执行以下操作：
   1. 选择 **Encrypted DNS Connection Type**（加密 **DNS** 连接类型）（请勿选择默认设置 **None**（无））：
      - **DoH**—基于 HTTPS（超文本传输协议安全）的 DNS。DoH 使用端口 443。当连接类型为 DoH 时，需要主 DNS 地址，防火墙将使用 DoH 将所有 DNS 请求发送到主 DNS 服务器。如果主 DNS 服务器没有响应，防火墙会将 DoH 请求发送到辅助 DNS 服务器。
      - **DoT**—基于 TLS（传输层安全性）的 DNS。DoT 使用端口 853，这是 DoT 流量的专用端口。当连接类型为 DoT 时，需要主 DNS 地址，防火墙将使用 DoT 将所有 DNS 请求发送到主 DNS 服务器。如果主 DNS 服务器没有响应，防火墙会将 DoT 请求发送到辅助 DNS 服务器。
      - **None**（无）—默认设置。没有为服务器连接指定加密 DNS。
   2. 如果选择 **Fallback on Unencrypted DNS**（未加密 **DNS** 的回退），则在 DNS 服务器拒绝加密 DNS 或超时（防火墙在配置的 TCP 超时期限内未从主 DNS 服务器或辅助 DNS 服务器收到配置的连接类型 [DoH 或 DoT] 的响应）的情况下，防火墙将回退到传统 DNS（明文）。

 ©2024 Palo Alto Networks, Inc.

3. 输入 **TCP Timeout (sec)**（**TCP** 超时（秒））的值，范围为 1 到 10；默认值为 1 秒。



3. 继续步骤 4。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 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，则可以配置 DNS 代理对象，这可以作为指定 DNS 服务器的替代方法。从 PAN-OS 11.2.1 开始，DNS 代理支持加密 DNS。

1. 在 **Services**（服务）选项卡上，对于 **DNS**，请单击 **DNS Proxy Object**（**DNS** 代理对象）。
2. 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）。
   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。
3. （PAN-OS 11.2.1 及更高版本）（可选）使用加密 DNS 配置 DNS 代理对象。
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 4 | （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 5 | （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。

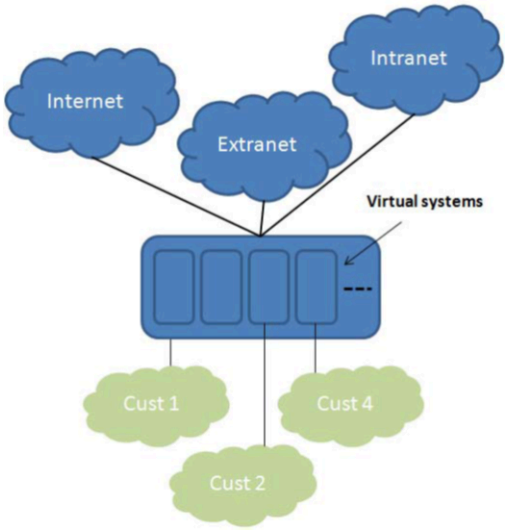
确保 *FQDN Stale Entry Timeout*（*FQDN* 失效条目超时）足够短，不会允许错误的流量转发（这会带来安全风险），但又足够长，以允许流量连续移动，不会导致计划外的网络中断。

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

 ©2024 Palo Alto Networks, Inc.

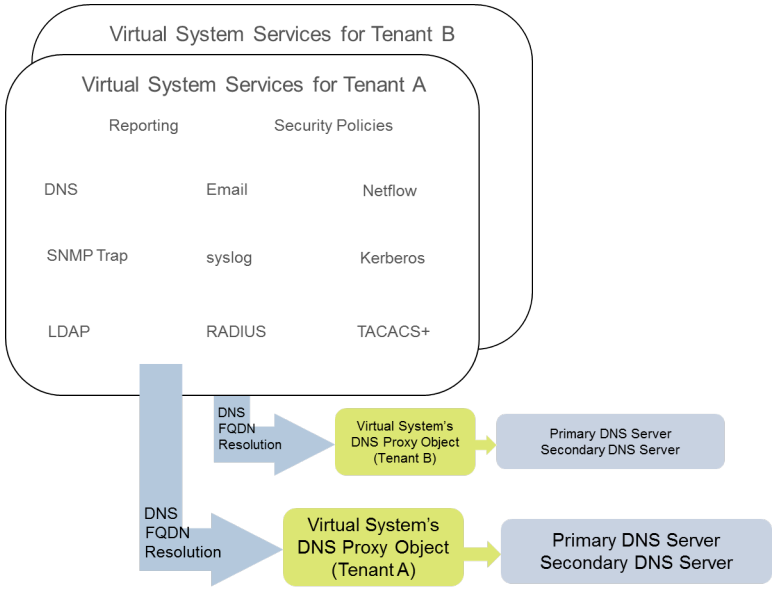
用例 2：ISP 租户使用 DNS 代理在其虚拟系统中对安全策略、报告和服务执行 DNS 解析。

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。



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。



 ©2024 Palo Alto Networks, Inc.

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。

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**

 ©2024 Palo Alto Networks, Inc.

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：

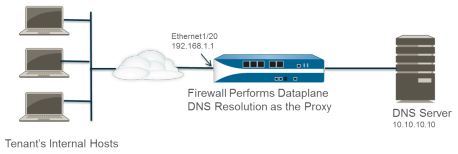
```
警告：DNS 代理对象中定义的 DNS 服务路由与 DNS 代理规则的服务路由不同。使用 DNS 代理对象的服务路由。
```

- 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。

 ©2024 Palo Alto Networks, Inc.

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。

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。

 ©2024 Palo Alto Networks, Inc.

STEP 11 | 双击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

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** 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。 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。	规则：***.boat.com** FQDN：**www.boat.com** — 匹配 FQDN：**www.blue.boat.com** — 匹配 FQDN：**boat.com** — 不匹配
	规则：***** FQDN：**boat** — 匹配 FQDN：**boat.com** — 匹配 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** FQDN：**www.boat.com** — 匹配 FQDN：**www.blue.boat.com** — 匹配
	规则：**www.boat.*** FQDN：**www.boat.com** — 匹配 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** FQDN：**a.b.d.e.com** — 匹配 FQDN：**a.b.c.d.e.f.com** — 匹配

©2024 Palo Alto Networks, Inc.

FQDN 与 DNS 代理规则的比较	例如
	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） 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。 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： 规则：***.*.boat.com** FQDN：**www.blue.boat.com** — 匹配 FQDN：**www.blue.sail.boat.com** — 匹配
	标记之间的连续通配符： 规则：**www.*.*.boat.com** FQDN：**www.blue.sail.boat.com** — 匹配 FQDN：**www.big.blue.sail.boat.com** — 匹配
	尾部标记的连续通配符： 规则：**www.boat.*.*** FQDN：**www.boat.fish.com** — 匹配 FQDN：**www.boat.fish.ocean.com** — 匹配
	仅连续通配符： 规则：*.* FQDN：**boat** — 不匹配 FQDN：**boat.com** — 匹配 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** 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） 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：	规则：**www.boat.fish** FQDN：**www.boat.fish.com** — 匹配

 ©2024 Palo Alto Networks, Inc.

FQDN 与 DNS 代理规则的比较	例如
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。	FQDN：**www.boat.fish.ocean.com** — 匹配 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.*** FQDN：**www.boat.fish.com** — 匹配 FQDN：**www.boat.fish.ocean.com** — 匹配 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 规则2：***.com** — 匹配 规则3：**boat.fish.com** — 匹配和平局 FQDN：**boat.fish.com** 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 规则2：***.com** — 匹配 规则3：**boat.fish.com** — 不匹配 FQDN：**fish.com** 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 规则2：***.com** — 匹配 规则3：**boat.fish.com** — 不匹配 FQDN：**blue.boat.fish.com** 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。	将： 规则：**www.boat** 替换为： 规则：**www.boat.com**

 ©2024 Palo Alto Networks, Inc.

FQDN 与 DNS 代理规则的比较	例如
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。	
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。 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。 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 规则：**www.corporation.com** — DNS 服务器 B 规则：***.internal.corporation.com** — DNS 服务器 C 规则：**www.internal.corporation.com** — DNS 服务器 D FQDN：**mail.internal.corporation.com** — 与 DNS 服务器 C 匹配 FQDN：**mail.corporation.com** — 与 DNS 服务器 A 匹配

 ©2024 Palo Alto Networks, Inc.

DDNS

了解动态 DNS (DDNS) 服务如何更新域名到 IP 地址的映射，以向 DNS 客户端提供准确的 IP 地址。

- 动态 DNS 概述
- 为防火墙接口配置动态 DNS

动态 DNS 概述

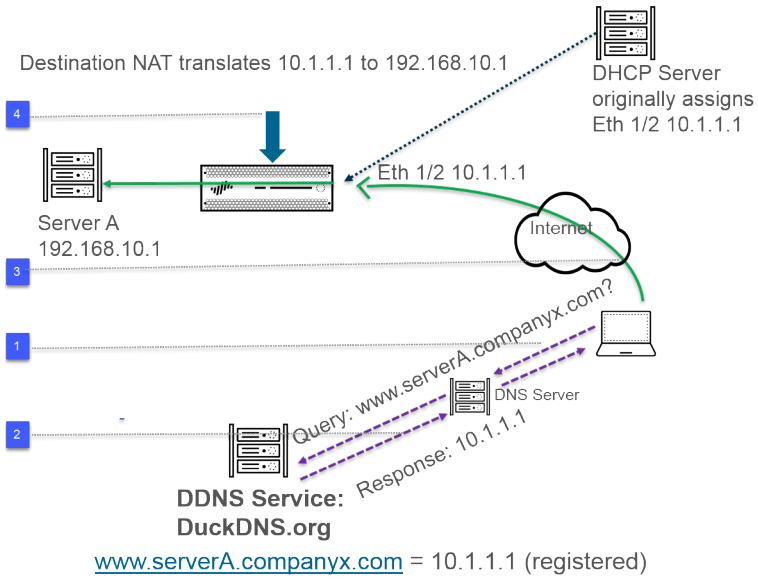
当您在防火墙后托管服务，并在防火墙上使用目标 NAT 策略访问这些服务，或者您需要提供对防火墙的远程访问时，您可以为通过动态 DNS (DDNS) 服务供应商为接口注册 IPv4 地址更改（接口为接收动态地址或具有静态地址的 DHCP 客户端）或 IPv6 地址更改（仅限静态地址）。DDNS 服务自动更新域名至 IP 地址映射，以向 DNS 客户端提供准确的 IP 地址，从而访问防火墙和防火墙后的服务。DDNS 通常用于托管服务的分支部署。防火墙接口没有了 DDNS 支持后，您需要外部部件以向客户端提供准确的 IP 地址。

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。

防火墙不支持以太网点对点协议 *(PPPoE)* 终止点接口上的 *DDNS*。

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)。

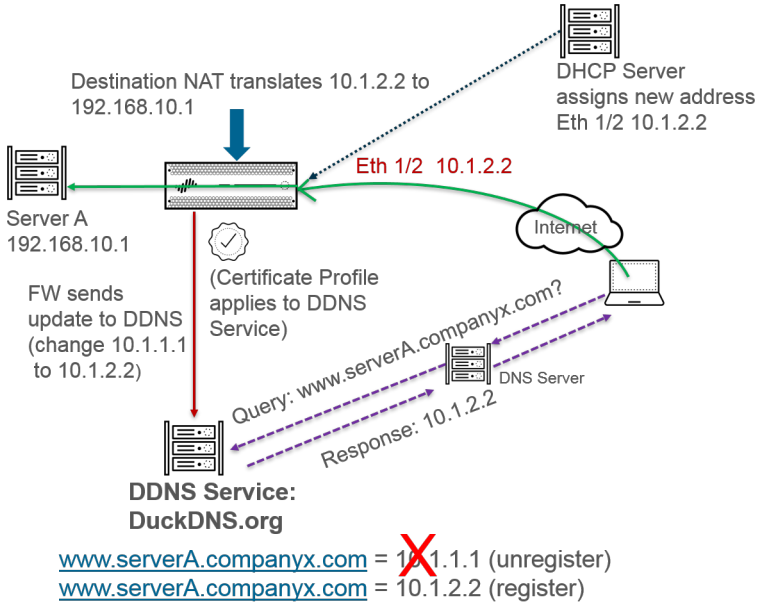


1. 当用户尝试联系 www.serverA.companyx.com 时，用户将查询该 IP 地址的本地 DNS 服务器。www.serverA.companyx.com（例如被设为 duckdns.org 记录：serverA.companyx.duckdns.org 的 CNAME）是属于 DDNS 供应商的域名（此例中为 DuckDNS）。DNS 服务器与 DDNS 提供商一同检查记录以解决查询。

 ©2024 Palo Alto Networks, Inc.

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 192.168.11.1。

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：



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。）

 ©2024 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。

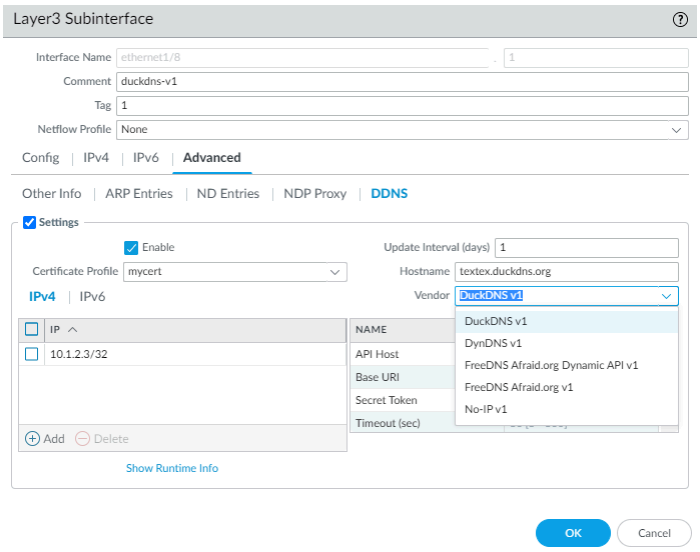
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）并选择 3 层接口、子接口或聚合以太网 (AE) 接口；或选择 **Network**（网络） > **Interfaces**（接口） > **VLAN** 并选择一个接口或子接口。
2. 选择 **Advanced**（高级） > **DDNS** 并选择 **Settings**（设置）。
3. **Enable**（启用）DDNS。您必须首先启用 DDNS 进行配置。（如果您的 DDNS 配置尚未完成，您可以在不启用的情况下进行保存，这样，就不会丢失部分配置。）
4. 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

 ©2024 Palo Alto Networks, Inc.

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）。



Palo Alto Networks® 可能通过内容更新更改支持的 *DDNS* 服务供应商。

在“供应商”字段中，*Palo Alto Network DDNS* 选型是针对 *Palo Alto Networks* 功能（如 *SD-WAN* 和 *ZTP*）保留的一项 *DDNS* 服务，不应选择用于此当前任务。如果您在相应的支持功能未启用时错误地选择了 *Palo Alto Networks DDNS*，将显示错误消息。

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）。

 ©2024 Palo Alto Networks, Inc.

 ©2024 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。

重要的是要了解在防火墙策略规则（包括 NAT）中，IPv4 地址集被视为 IPv6 地址集的子集。但是，IPv6 地址集不是 IPv4 地址集的子集。一个 IPv4 地址可以匹配一组或一系列 IPv6 地址；但 IPv6 地址无法匹配一组或一系列 IPv4 地址。

在所有策略类型中，源地址或目标地址的关键字 **any**（任何）表示任何 IPv4 或 IPv6 地址。关键字 **any**（任何）等同于 ::/0。如果要表示“任何 IPv4 地址”，请指定 0.0.0.0/0。

在策略匹配期间，防火墙会将 IPv4 地址转换为前 96 位为 0 的 IPv6 前缀。地址 ::/8 表示，如果前 8 位为 0，则匹配规则。所有 IPv4 地址都将匹配 ::/8、::/9、::/10、::/11、... ::/16、... ::/32 ... 至 ::/96。

如果您想表达“任何 IPv6 地址，但没有 IPv4 地址”，则您必须配置两条规则。第一条规则 denies 0.0.0.0/0 拒绝任何 IPv4 地址（作为源地址或目标地址），第二条规则有 ::/0 表示任何 IPv6 地址（作为源地址或目标地址），以满足您的要求.

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。

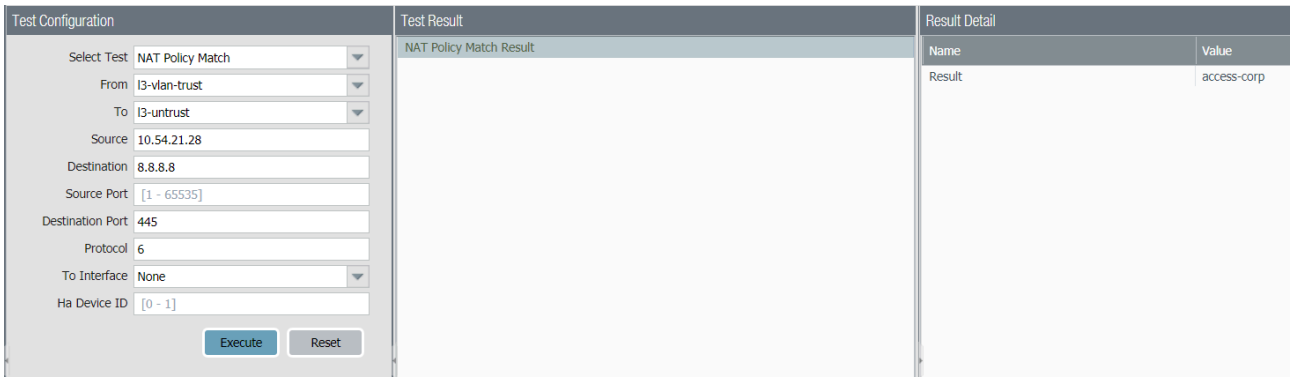
安全策略有别于 NAT 规则，因为安全策略会检查 NAT 前区域以确定数据包是否被允许。由于 NAT 的最根本目的是要修改源或目标 IP 地址（可能会导致数据包的传出接口和区域被修改），因此安全策略会被强制应用于 NAT 后区域。

 ©2024 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

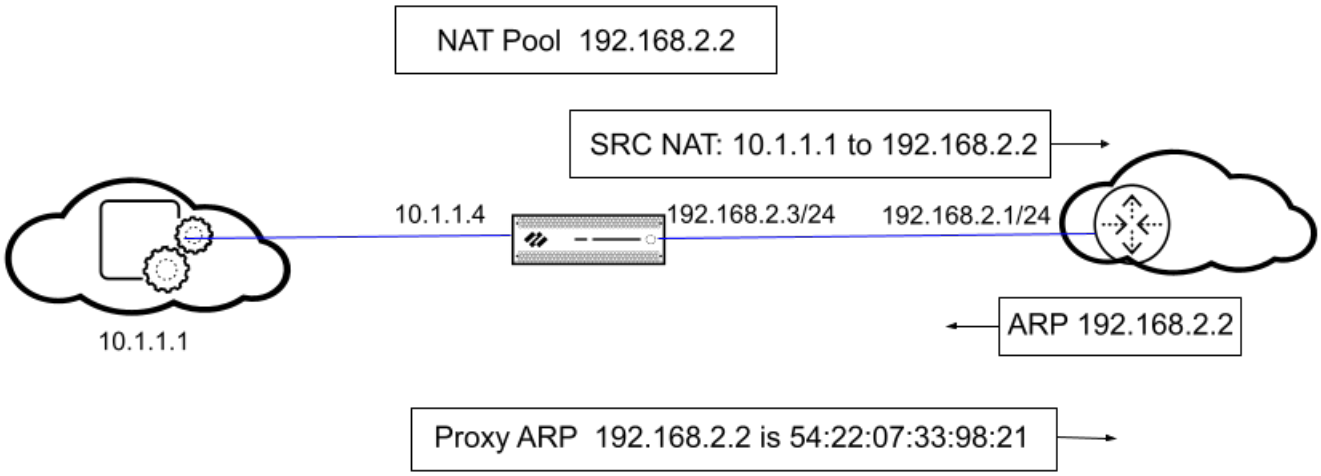
在 NAT 策略规则中，在 NAT 策略规则中配置 **Dynamic IP**（动态 **IP**）或 **Dynamic IP and Port**（动态 **IP** 与端口）NAT 地址池时，通常使用地址目标配置转换后的地址池。每个地址目标可以是主机 IP 地址、IP 地址范围或 IP 子网。

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。

 ©2024 Palo Alto Networks, Inc.



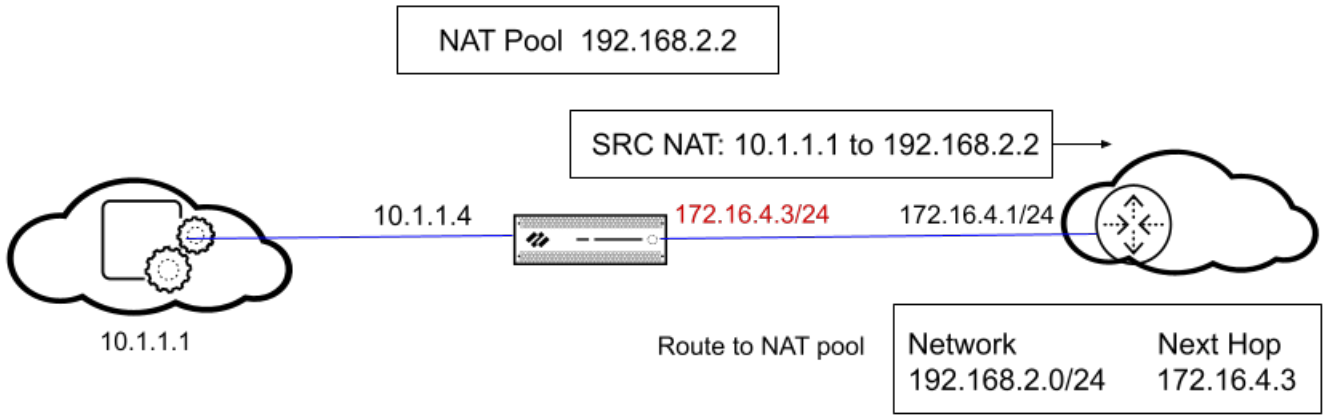
防火墙为客户端执行源 NAT，将源地址 10.1.1.1 转换为地址池中的地址 192.168.2.2。已转换数据包将发送到路由器。

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。

在我们的第一种场景中，当 NAT 池地址 (192.168.2.2) 与出口/入口接口 IP 地址 (192.168.2.3/24) 位于同一子网时，防火墙可以向路由器发送代理 ARP 回复，指示 192.168.2.2 的二层 MAC 地址为 54:22:07:33:98:21，如上图所示。

当 **NAT** 池地址不是出口/入口接口的子网时，没有代理 **ARP**

在我们的第二个场景中，NAT 池地址 (192.168.2.2) 不是防火墙上接口的子网，因此防火墙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。



 ©2024 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互联网；源地址会被转换并保持私有状态。源 NAT 有几种类型：静态 IP、动态 IP 以及动态 IP 和端口 (DIPP)。DIPP 可以配置为非持久性或持久性。

- 静态 **IP**—允许对源 IP 地址进行一对一、静态转换，但保持源端口不变。静态 IP 转换常用于必须可供互联网使用的内部服务器。
- 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。
- 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)。

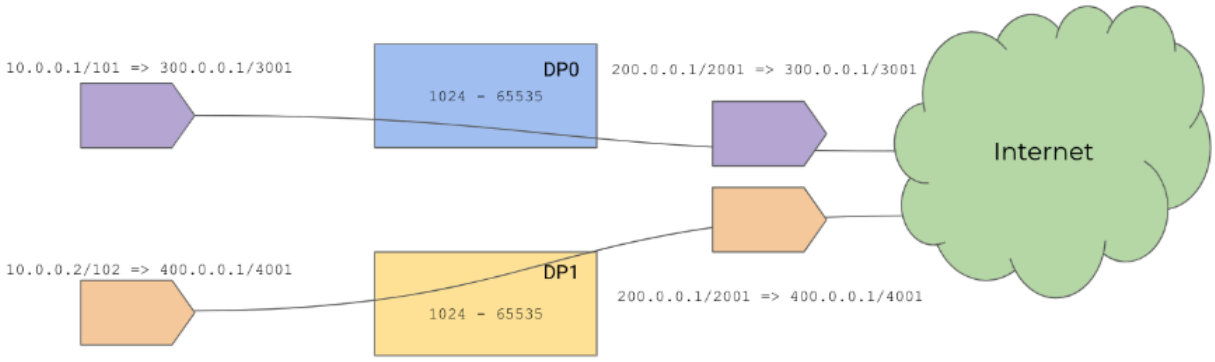
  DIPP 有默认的 NAT 超额订阅率，即可以同时使用同一转换后 IP 地址和端口对的次数。有关更多信息，请参阅动态 IP 和端口 NAT 超额订阅和修改 DIPP NAT 的超额订阅率。

  （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。

  在多数据平面 (DP) 防火墙模型上配置常规（非持久性）DIPP 时，超额订阅率适用于本地池；不会在 DP 之间强制执行超额订阅。一个 DP 的源端口可以被不同 DP 重复使用。完全可以重

 ©2024 Palo Alto Networks, Inc.

复使用常规 DIPP 的端口，因为常规流量发往不同目标。在此图中，两个会话的源都转换为 200.0.0.1/2001：



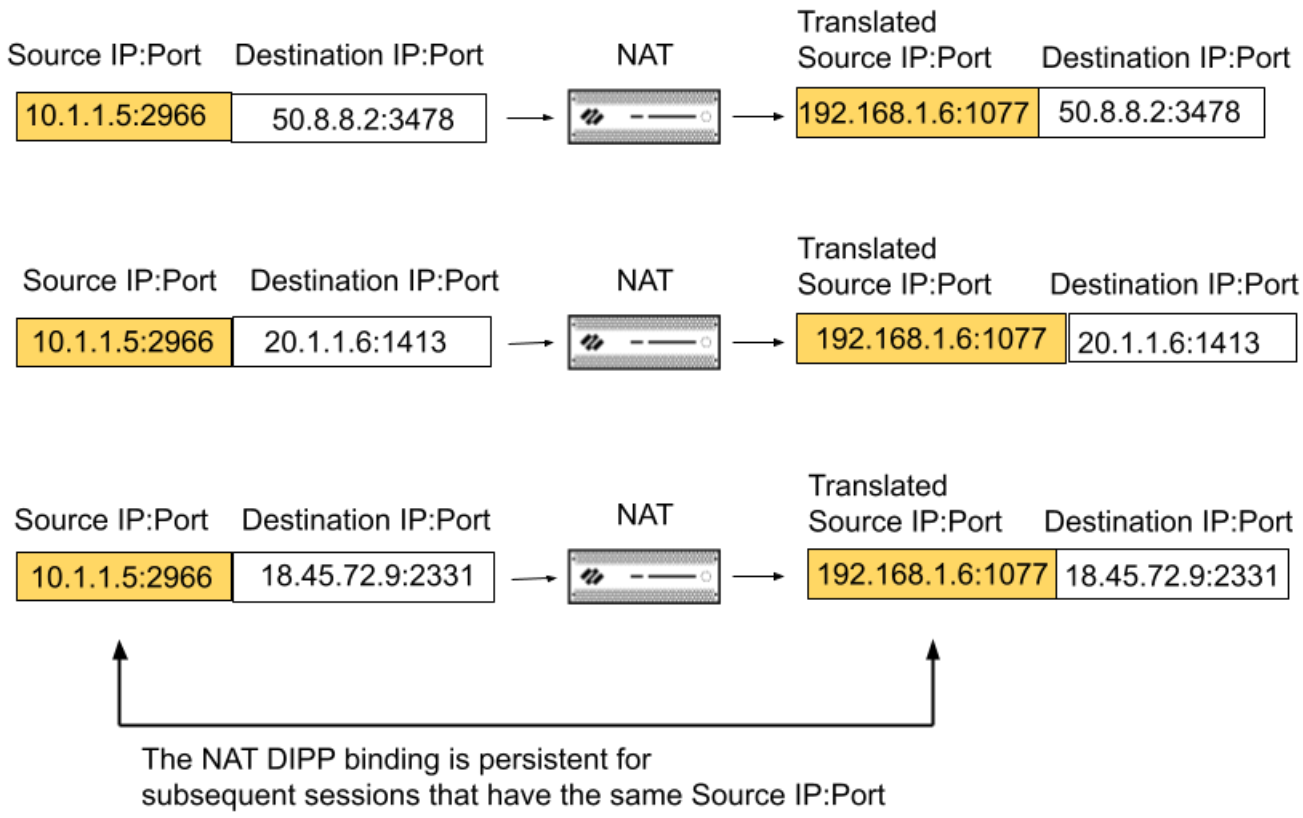
- （PAN-OS 11.1.0 及更低版本）**DIPP** 的持久 **NAT**（也称为持久 DIPP 或持久 NAT）—在所有防火墙上可用。VoIP、视频、基于云的视频会议、音频会议和其他应用程序通常使用 DIPP，可能需要适用于 NAT (STUN) 协议的会话遍历实用程序。DIPP NAT 使用对称 NAT，这可能与使

 ©2024 Palo Alto Networks, Inc.

用 STUN 的应用程序存在兼容性问题。为了缓解这些问题，DIPP 的持久 NAT 为与此类应用程序的连接提供了额外支持。

在 PAN-OS 11.1.0 及更低版本中，当您为 DIPP 启用持久 NAT 时，它适用于所有 NAT 和 NAT64 规则；它是一个全局设置。管理平面或数据平面日志将显示已启用 `NAT DIPP/STUN` 支持。

启用 DIPP 的持久 NAT 时，私有源 IP 地址/端口对与特定的公共（转换后的）源 IP 地址/端口对的绑定将持续绑定到具有相同原始源 IP 地址/端口对的后续会话中。以下示例显示了三个会话：



在此示例中，原始源 IP 地址/端口 10.1.1. 5:2966 绑定到会话 1 中转换后的源 IP 地址/端口 192.168.1. 6:1077。这种绑定在会话 2 和会话 3 中是持久的，它们的原始源 IP 地址/端口相同，但目标地址不同。在该源 IP 地址/端口对的所有会话结束后，绑定的持久性即告结束。

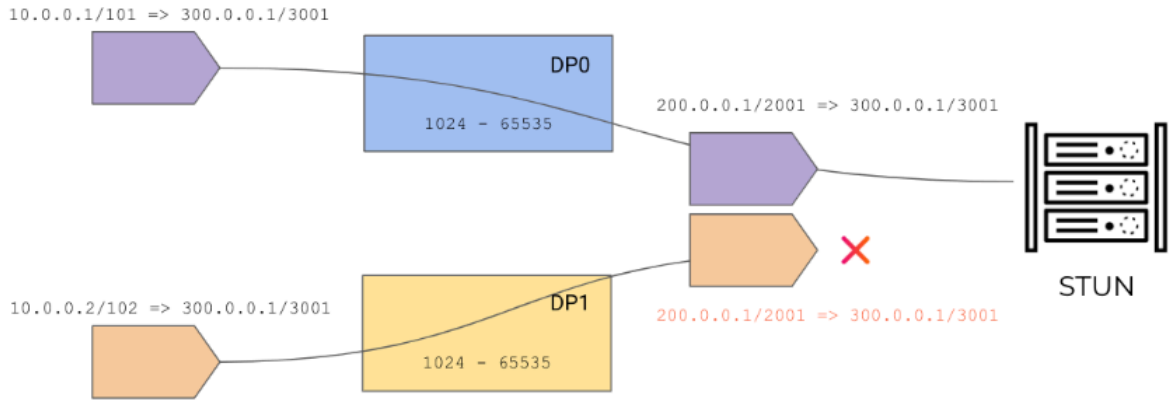
在示例的会话 1 中，目标端口是 3478，即默认 STUN 端口。

DIPP 的持久 NAT 设置（启用或禁用）在防火墙重新启动后仍然有效。

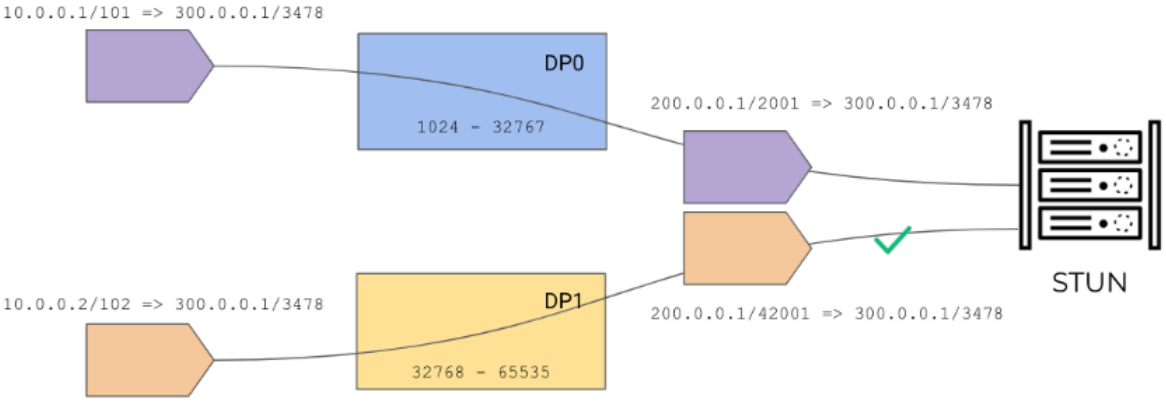
使用常规 DIPP NAT 规则，如果多对相同的 [源 IP 地址/端口] 组合将流量发送到不同目标，则将获得不同转换。通过持久 DIPP 规则，如果多对相同的 [源 IP 地址/端口] 组合将流量发送到不同目标，则将获得相同转换，如以上三个会话所示。

持久性 NAT 不能在 DP 之间重复使用端口号，因为如果多个 DP 尝试使用相同的端口号，某些会话可能无法到达 STUN，如下所示：

 ©2024 Palo Alto Networks, Inc.



解决方案是在 DP 之间划分源端口；这样端口号将是唯一的，并且您可以避免重复会话：



- （PAN-OS 11.1.1 及更高版本）基于策略的持久 **DIPP**—从 PAN-OS 11.1.1 及更高版本开始，您可以在单独的 NAT 策略规则中配置持久 DIPP，而不必进行全局配置。如果将 NAT 或 NAT64 用于防火墙后面的视频或语音应用程序并且需要访问 STUN，请使用持久动态 **IP** 和端口的转换类型来创建 NAT 策略规则。

  基于策略的持久性 DIPP 允许常规（非持久性）DIPP 与持久性 DIPP 共存，因为持久性 DIPP 不是全局性的；粒度在 NAT 策略规则范围内。全局配置持久性 DIPP 时，系统范围内可用的源端口只有 64,512 个，即使对于常规 DIPP 流量，也会限制转换的总数。通过实现常规 DIPP 与持

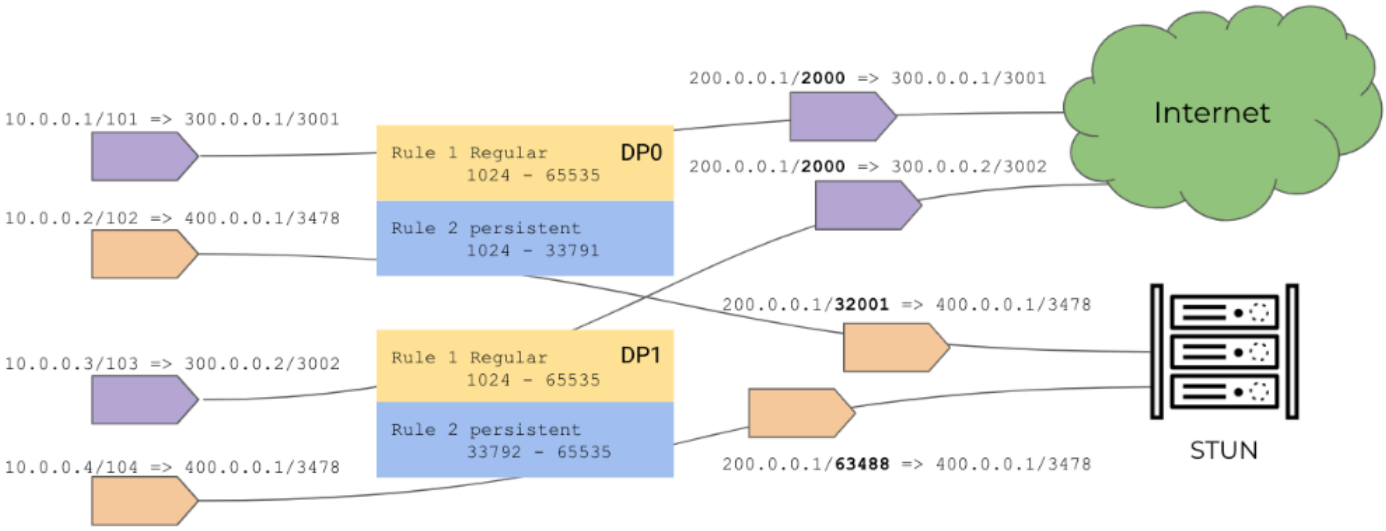
 ©2024 Palo Alto Networks, Inc.

久 DIPP 规则在系统中共存，常规 DIPP 不必与持久 DIPP 共享端口，并且可以具有大于 1 的超额订阅率，从而释放常规 DIPP 转换的总数。

持久 *DIPP* 规则和常规 *DIPP* 规则可以转换为相同的 *IP* 地址范围。为了获得最佳性能，请配置持久 *DIPP* 和常规 *DIPP* 来管理单独的源端口池，因为流量应该流向不同的目的地。单独的端口池可以包含重叠的端口范围。

对于持久 DIPP 规则，超额订阅率为 1（禁止超额订阅）。常规 DIPP 规则使用系统配置中设置的超额订阅率。防火墙上启用持久 DIPP 时，这种设计可获得最佳性能。

如图所示，来自 DP0 和 DP1 的紫色会话使用常规 NAT 规则并使用同一个转换后的源 IP 地址/端口 (200.0.0.1/2000)。这些会话对于互联网的目标 IP 地址各不相同。来自 DP0 和 DP1 的橙色会话发往 STUN 端口。这些会话使用持久 DIPP NAT 规则并使用同一个转换后的源 IP 地址 (200.0.0.1) 但使用不同的端口号（32001 和 63488）。



总之，每个策略的持久 DIPP 允许两种流量类型（常规 DIPP 和持久 DIPP）在防火墙上共存。常规 DIPP 规则和持久 DIPP 规则可以共享单个转换后的 IP 地址（请注意，图中的四个会话都具有转换后的源地址 200.0.0.1）。常规 DIPP 规则可以共享同一个转换后的源 IP 地址和端口（紫色会话），因为它们的目的地不同。常规 DIPP 规则类型和持久 DIPP 规则类型可以各自控制自己的源端口池。

持久性 DIPP 不支持热交换内联卡。

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

 ©2024 Palo Alto Networks, Inc.

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，即使用 FQDN 且可以从 DNS 返回多个地址的地址对象。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。

  如果在 **Policy**（策略） > **NAT** > **Original Packet**（原始数据包）中将预 NAT 地址配置为 FQDN 对象，必须为目标地址转换类型（**Policy**（策略） > **NAT** > **Translated Packet**（转换数据包）选择 **Dynamic IP (with session distribution)**（动态 **IP**（带会话分发））。

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： 192.168.1.1 始终映射到 2.2.2.1

 ©2024 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
			192.168.1.2 始终映射到 2.2.2.2 192.168.1.3 始终映射到 2.2.2.3 192.168.1.4 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： 192.168.1.1 始终映射到 2.2.2.1 192.168.1.2 始终映射到 2.2.2.2 192.168.1.3 始终映射到 2.2.2.3 192.168.1.4 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 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，

 ©2024 Palo Alto Networks, Inc.

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

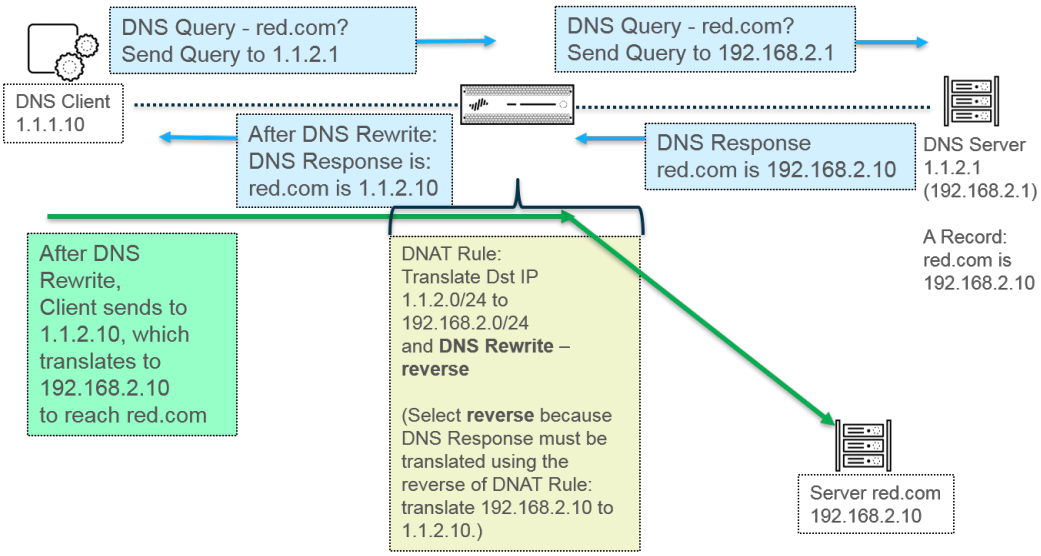
DNS 反向重写目标 NAT 用例

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。）

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。

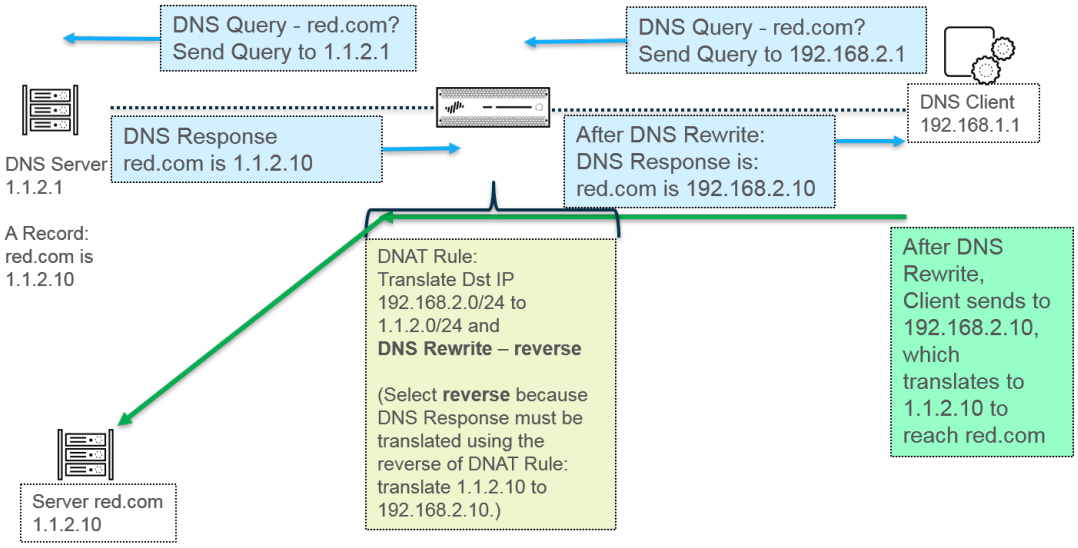
用例 1 摘要：DNS 客户端和目标服务器位于防火墙的相对侧。DNS 服务器提供 NAT 规则内与转换目标位置相匹配的地址，从而通过 NAT 规则的反向转换进行 DNS 响应的转换。

 ©2024 Palo Alto Networks, Inc.



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。



要执行 DNS 重写，请配置 DNS 重写目标 NAT。

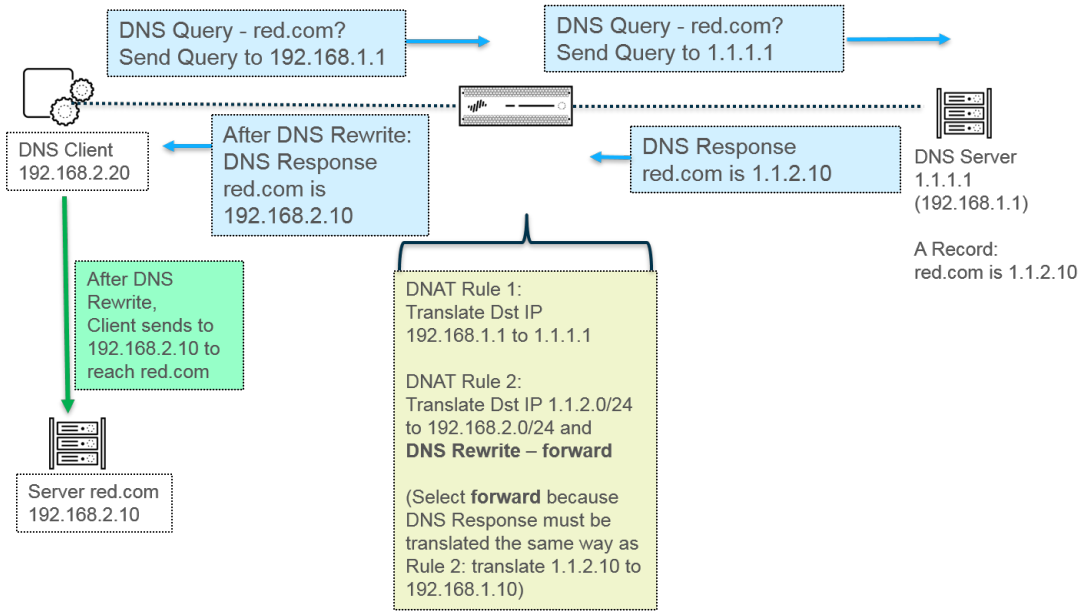
 ©2024 Palo Alto Networks, Inc.

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。

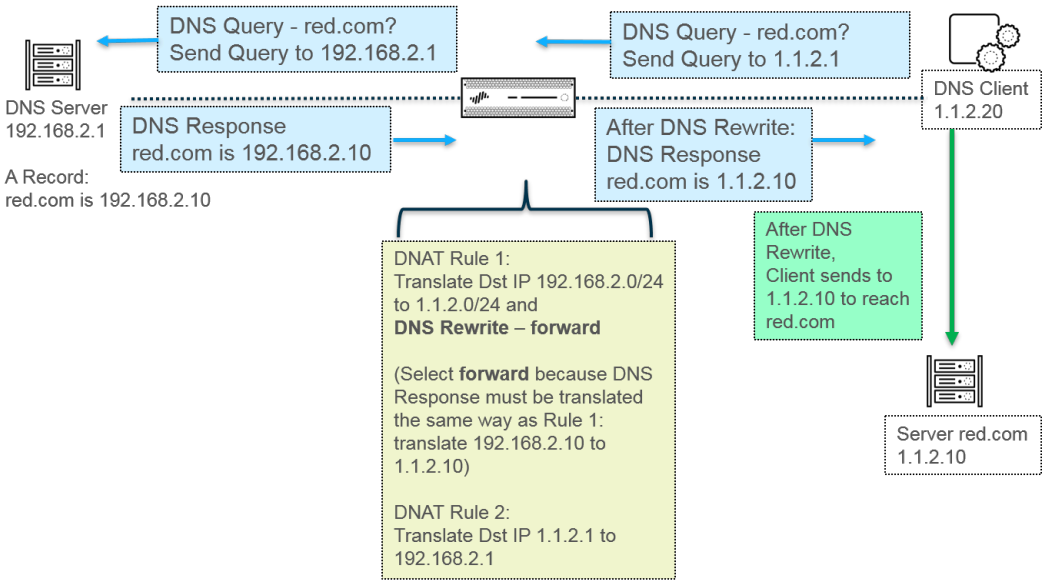
用例 3 摘要：DNS 客户端和目标服务器位于防火墙的相同侧。DNS 服务器提供 NAT 规则内与原始目标位置相匹配的地址，从而通过 NAT 规则的相同（正向）转换进行 DNS 响应的转换。



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。

 ©2024 Palo Alto Networks, Inc.



要执行 DNS 重写，请配置 DNS 重写目标 NAT。

 ©2024 Palo Alto Networks, Inc.

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。

©2024 Palo Alto Networks, Inc.

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，并且会应用平台的 NAT 默认 DIPP 池超额订阅率（如产品选择工具所示）。如果使用 **Platform Default**（平台默认值）设置，软件版本可以升级或降级。

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。

 ©2024 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。

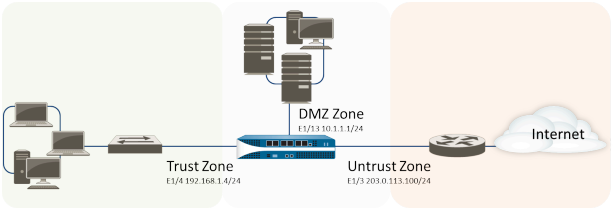
```
admin@PA-7050-HA-0 (active-primary)> show running nat-rule-ippool rule nat1

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

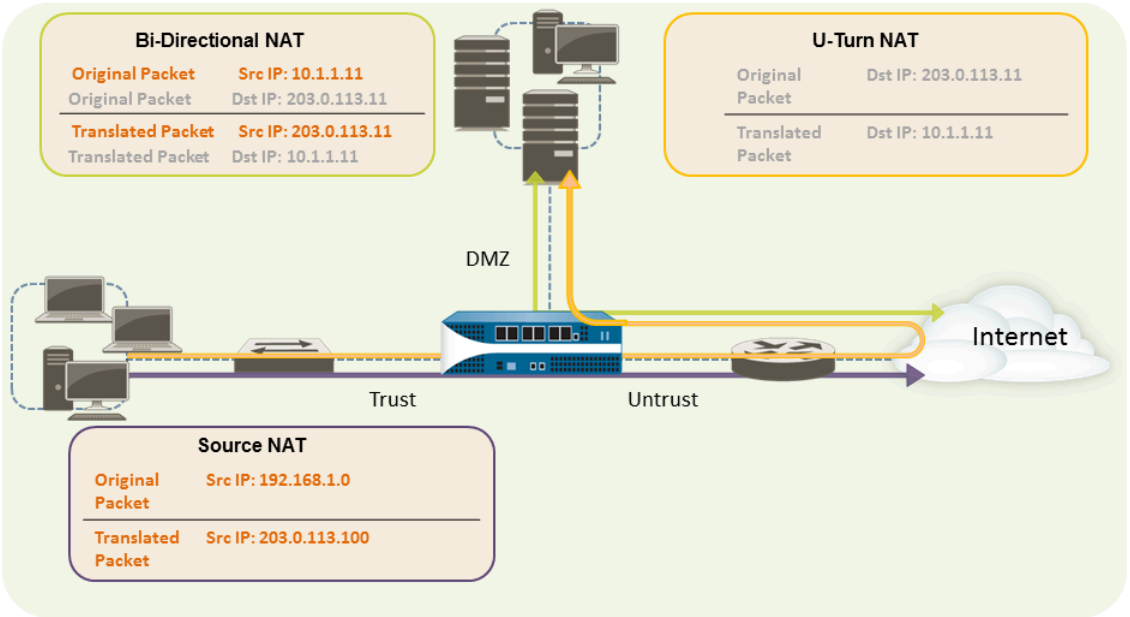
请执行以下任务以配置 NAT 的各个方面。除了以下示例，NAT 配置示例部分中还有一些示例。

- 将内部客户端 IP 地址转换为公共 IP 地址（源 DIPP NAT）
- 创建具有持久 DIPP 的源 NAT 规则
- 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

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）。

©2024 Palo Alto Networks, Inc.

- 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。

此任务涵盖常规 *DIPP*，并且此任务还包括在 *PAN-OS 11.1.0* 及更低版本中为 *DIPP* 启用持久 *NAT* 的步骤。要在 *PAN-OS 11.1.1* 及更高版本中为 *DIPP* 启用持久 *NAT*，请创建具有持久 DIPP 的源 NAT 规则。

STEP 1 | 为计划使用的外部 IP 地址创建一个地址对象。

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）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。

 ©2024 Palo Alto Networks, Inc.

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 | （PAN-OS 11.1.0 及更低版本）为 DIPP 启用持久 NAT。（常规 DIPP 跳过此步骤。）

1. 访问 CLI。
2. >设置系统设置 **`persistent-dipp enable yes`**
3. **`>request restart system`**
4. 如果您配置了 HA，请在另一个 HA 对等体上重复此步骤。

STEP 5 | （可选）验证翻译。

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。

创建具有持久 DIPP 的源 NAT 规则

在何处可以使用？	需要提供什么？
• NGFW (Strata Cloud Manager) — 请与您的支持客户代表联系以启用此功能。 • NGFW（PAN-OS 或 Panorama 托管）	❑ 需要 AIOps for NGFW Premium 才能使用 Strata Cloud Manager 管理 NGFW

 ©2024 Palo Alto Networks, Inc.

从 PAN-OS 11.1.1 及更高版本开始，您可以在单个 NAT 策略规则中配置持久 DIPP。如果将 NAT 用于防火墙后面的视频或语音应用程序并且需要访问 STUN，请使用持久动态 IP 和端口的转换类型来创建策略规则。

- PAN-OS
- Strata Cloud Manager

PAN-OS

对于 PAN-OS，请按照此过程创建具有持久 DIPP 的源 NAT 规则。

STEP 1 | 为计划使用的外部 IP 地址创建一个地址对象。

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）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**（转换数据包）选项卡上，为 **Translation Type**（转换类型）选择 **Persistent Dynamic IP And Port**（持久动态 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）。选择您创建的地址对象或输入转换后的源地址。

   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 | **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | （可选）使用 CLI 操作命令查看持久 DIPP 信息。

1. 访问 CLI。
2. **> show running persistent-dipp-pool**
3. **> show running persistent-dipp-client pool <nat-pool-index>**
4. **> show running persistent-dipp-client-translation ip <client-ip-address>**

在运行时使用最后两个 *show* 命令可按照客户端 *IP* 地址来跟踪持久 *NAT* 资源使用情况。

STEP 5 | （可选）使用 CLI 配置命令来监控持久 DIPP 池利用率。如果资源利用率超过您配置的阈值，则会生成 syslog。

1. 访问 CLI。
2. > 配置
3. **# set deviceconfig setting session persistent-dipp-alert-enable <no|yes>**
4. **# set deviceconfig setting session persistent-dipp-alert-threshold <1-99>**
5. **# set deviceconfig setting session persistent-dipp-alert-interval <5-120>**

Strata Cloud Manager

从 SCM R3 开始，Strata Cloud Manager 支持采用了持久 DIPP 的 NAT 规则。

STEP 1 | 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。

STEP 2 | 选择 **Network Policies**（网络策略） > **NAT**

STEP 3 | 选择 **Add Rule**（添加规则）以添加规则，然后在 **Name**（名称）中输入源 NAT 策略规则的名称。

STEP 4 | 配置原始数据包源区域和地址、目标区域、接口和地址以及服务。

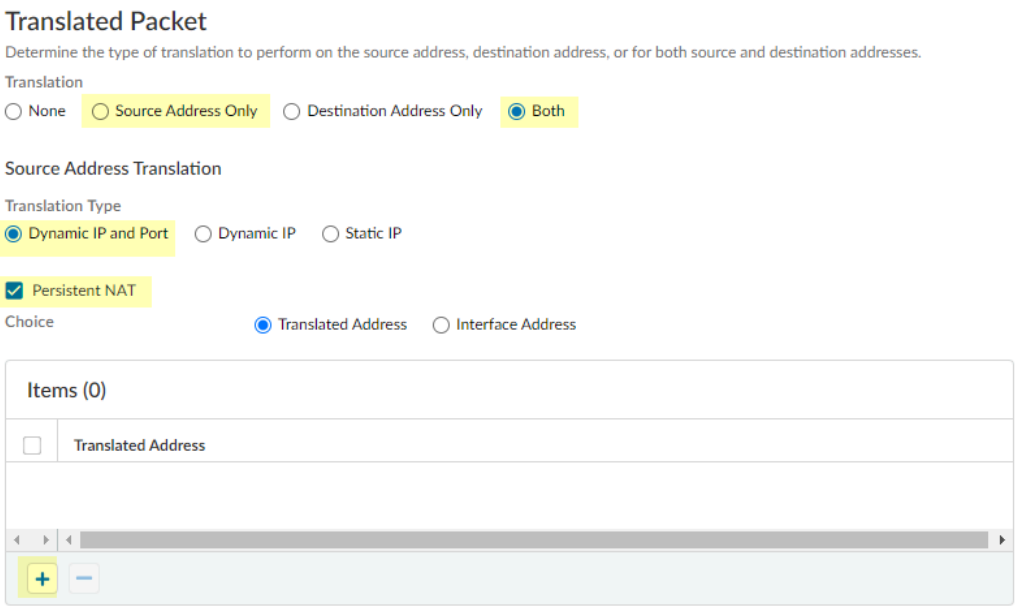
STEP 5 | 对于转换后的数据包，选择 **Source Address Only**（仅限源地址）或 **Both**（两者）（源地址和目标地址）。

STEP 6 | 对于转换类型，选择 **Dynamic IP and Port**（动态 **IP** 和端口）。

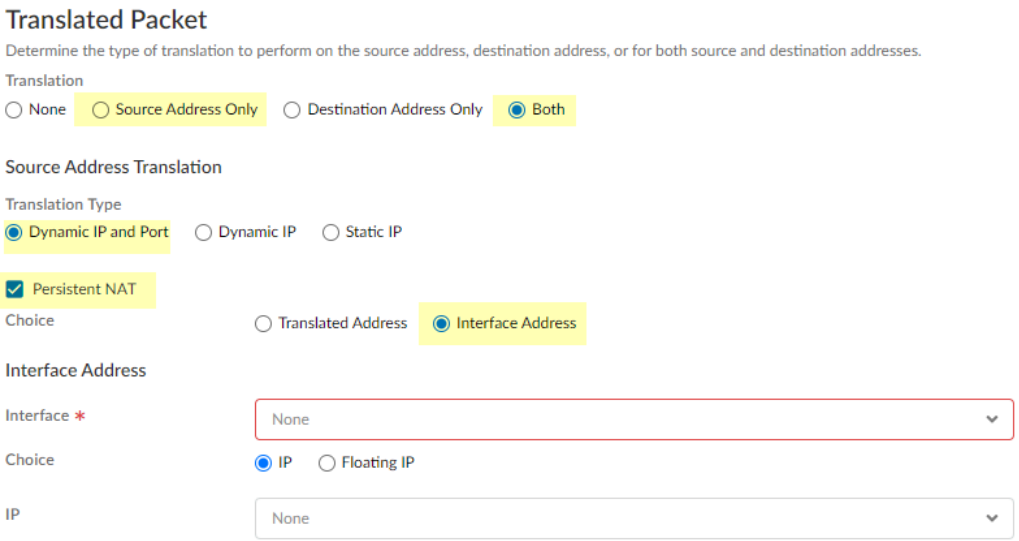
STEP 7 | 选择 **Persistent NAT**（持久 **NAT**）。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 您可以选择 **Translated Address**（转换后的地址），然后选择“+”来选择您创建的地址对象，或是输入转换后的源地址。



STEP 9 | 或者，您页可以选择 **Interface Address**（接口地址），在这种情况下，转换后的地址将是接口的 IP 地址。对于此选项，如果接口有多个 IP 地址，请选择一个接口和一个 **IP** 地址。也可以选择 **Floating IP**（浮动 **IP**）选项（并选择一个地址对象）。



STEP 10 | 如果选择了 **Both**（两者） 选项（即源转换和目标转换），接下来请配置目标的 **Translated Address**（转换后地址）和 **Translated Port**（转换后端口）选项。

STEP 11 | **Save**（保存）配置。

 ©2024 Palo Alto Networks, Inc.

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。

   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）。

 ©2024 Palo Alto Networks, Inc.

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。
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，您也可以配置该规则，以便防火墙根据为规则配置的原始或已转换 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。

 ©2024 Palo Alto Networks, Inc.

查看 DNS 重写用例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 规则中的原始或转换目标地址相匹配时，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。

使用动态 IP 地址配置目标 NAT

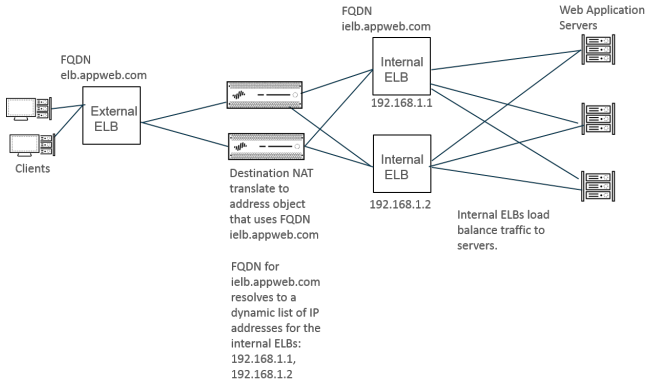
使用 目标 NAT 将原目标地址转换为拥有动态 IP 地址且使用 FQDN 的目标主机或服务器。使用动态 IP 地址的目标 NAT 在云部署中尤其有用，通常使用动态 IP 寻址。当云中的主机或服务器有新的（动态）IP 地址时，不必通过持续查询 DNS 服务器手动更新 NAT 策略规则，也无需使用单独的外部组件通过最新 FQDN 到 IP 地址映射来更新 DNS 服务器。

使用动态 IP 地址配置目标 NAT 时，应仅使用 FQDN（而不是 IP 网络掩码或 IP 范围）。

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

 ©2024 Palo Alto Networks, Inc.

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。

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）。

 ©2024 Palo Alto Networks, Inc.

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 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。

   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）您可以配置防火墙刷新 FQDN 的频率（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。

 ©2024 Palo Alto Networks, Inc.

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：

```
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

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

NAT 配置示例

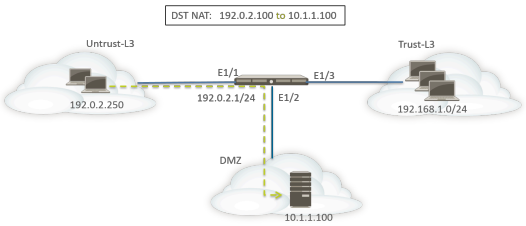
- 目标 NAT 示例 — 一对一映射
- 带有端口转换示例的目标 NAT
- 目标 NAT 示例 — 一对多映射
- 源和目标 NAT 示例
- Virtual Wire 源 NAT 示例
- Virtual Wire 静态 NAT 示例
- Virtual Wire 目标 NAT 示例

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。

 ©2024 Palo Alto Networks, Inc.

- 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 address: webserver-private

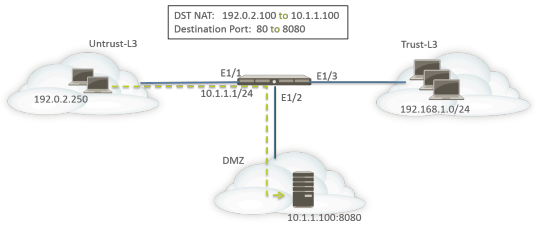
NAT 规则的方向基于路由查找的结果。

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	

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 address: webserver-private port: 8080

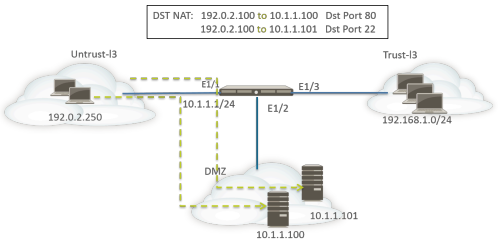
NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

使用 **`show session all`** CLI 命令验证转换。

©2024 Palo Alto Networks, Inc.

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：

		Original Packet						Translated Packet	
NAME	TAGS	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 address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

安全规则类似于下图：

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
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

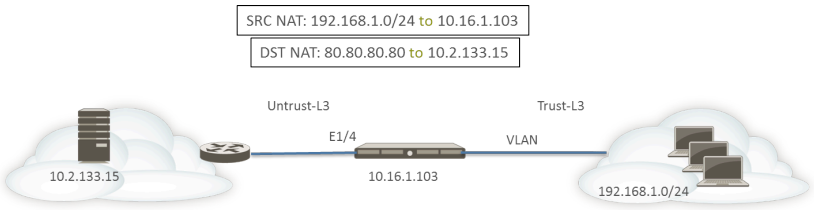
源和目标 NAT 示例

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。

 ©2024 Palo Alto Networks, Inc.

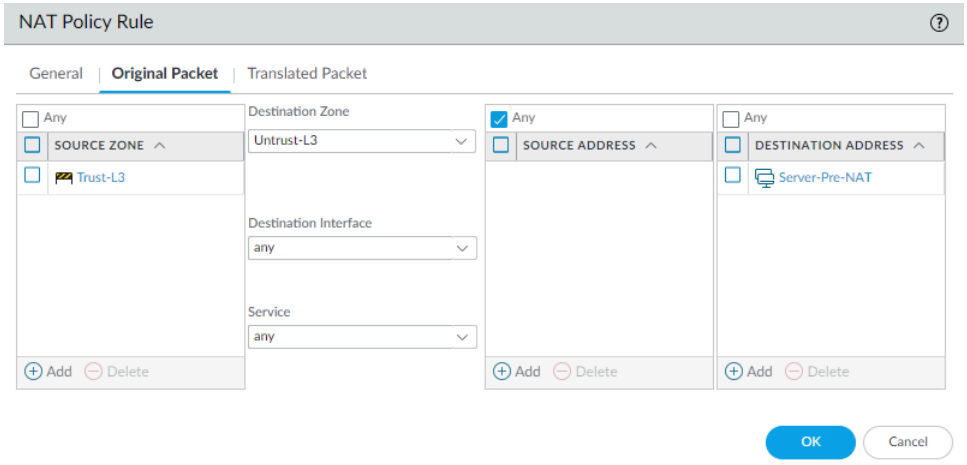
- 目标 NAT — 从客户端到服务器的数据包中的目标地址将从服务器的公共地址 (80.80.80.80) 转换为服务器的专用地址 (10.2.133.15)。

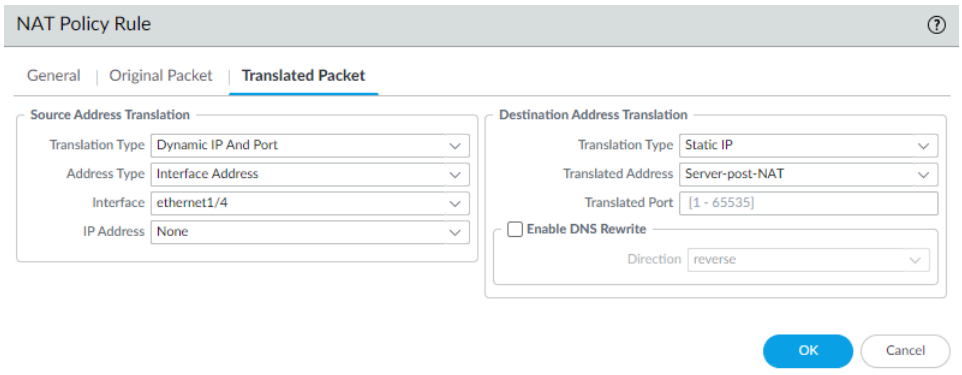


为目标 NAT 创建了以下地址对象。

- 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。





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。

 ©2024 Palo Alto Networks, Inc.

Virtual Wire 源 NAT 示例

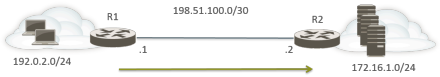
Palo Alto Networks® 防火墙的 Virtual Wire 部署包括以透明方式为终端设备提供安全保障的优势。可以为 Virtual Wire 中配置的接口配置 NAT。允许所有 NAT 类型：源 NAT（动态 IP、动态 IP 和端口、静态）和目标 NAT。

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：



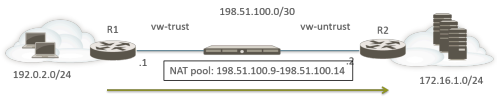
R1 上的路由：

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

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。

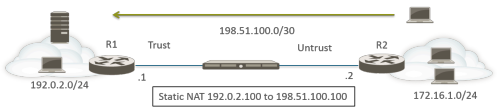
 ©2024 Palo Alto Networks, Inc.

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。



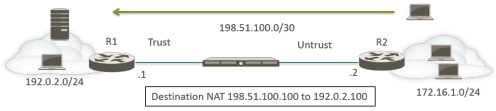
R2 上的路由：

目标	下一个跃点
198.51.100.100/32	198.51.100.1

NAME	Original Packet						Translated Packet	
	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 webserver-public 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：

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 address: webserver-private

 ©2024 Palo Alto Networks, Inc.

 ©2024 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局路由的地址。

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、不可路由的 IPv4 地址转换为一个或多个可全局路由的 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。

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。

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。

以下防火墙型号支持 NPTv6（NPTv6 带有硬件查找，但数据包经过 CPU）：

- PA-7000 系列防火墙
- PA-5400 系列防火墙
- PA-5200 系列防火墙
- PA-3200 系列防火墙
- PA-800 防火墙
- PA-220 防火墙

VM 系列防火墙支持 NPTv6，但没有能力让硬件执行会话查找。

- 唯一本地地址
- 使用 NPTv6 的理由

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。

©2024 Palo Alto Networks, Inc.

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的地址。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。

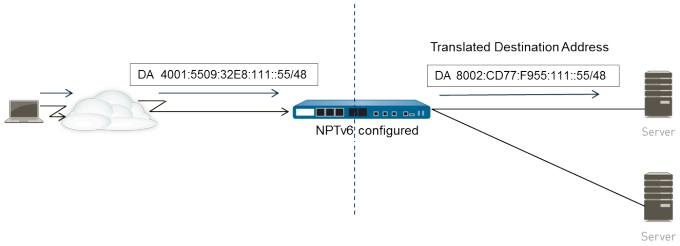
©2024 Palo Alto Networks, Inc.

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。
- 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。

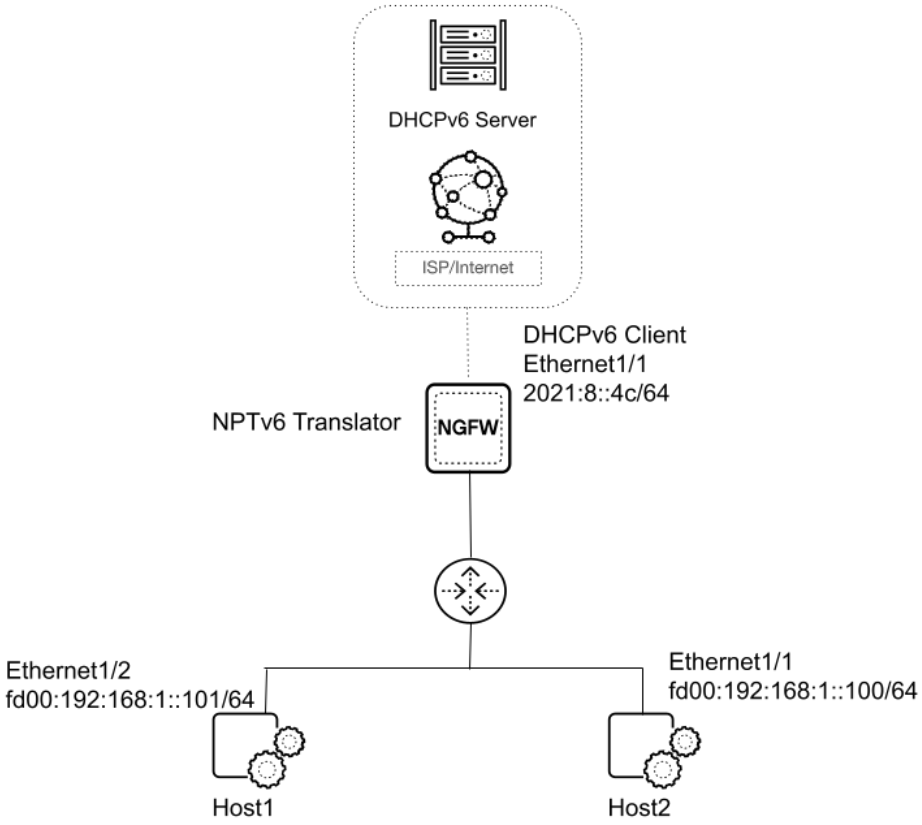
如果防火墙在隧道起源和终止，NPTv6 只会与 IPSec IPv6 一起使用。IPSec 流量中转将失败，因为源和/或目标 IPv6 地址会修改。可封装数据包的 NAT 遍历技术允许 IPSec IPv6 与 NPTv6 一起使用。

- 校验和中性映射
- 双向转换
- 应用于特定服务的 NPTv6

©2024 Palo Alto Networks, Inc.

具有动态分配 **IPv6** 地址前缀的 **NPTv6**

从 PAN-OS 11.1.5 开始，防火墙支持使用动态分配 IPv6 地址前缀的 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

当您使用时创建 NPTv6 策略，“已转换的数据包”选项卡中的“双向”选项可让您让防火墙按照与您配置的转换相反的方向创建相应的 NAT 或 nptV6 转换。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。

 ©2024 Palo Alto Networks, Inc.

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，以在原始数据包中指定 **Service**（服务）。

©2024 Palo Alto Networks, Inc.

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：

- 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。

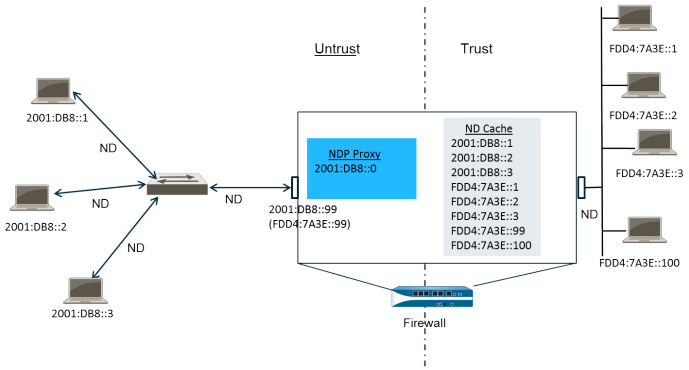
为了成功的支持 NDP，防火墙不会为以下各项执行 NDP 代理：

- 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）。

 ©2024 Palo Alto Networks, Inc.

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。

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。

©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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）。
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 到 /112。
   - **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

 ©2024 Palo Alto Networks, Inc.

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 /112（含）范围内的值。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。

STEP 5 | 提交配置。

单击 **OK**（确定）和 **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

 ©2024 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。

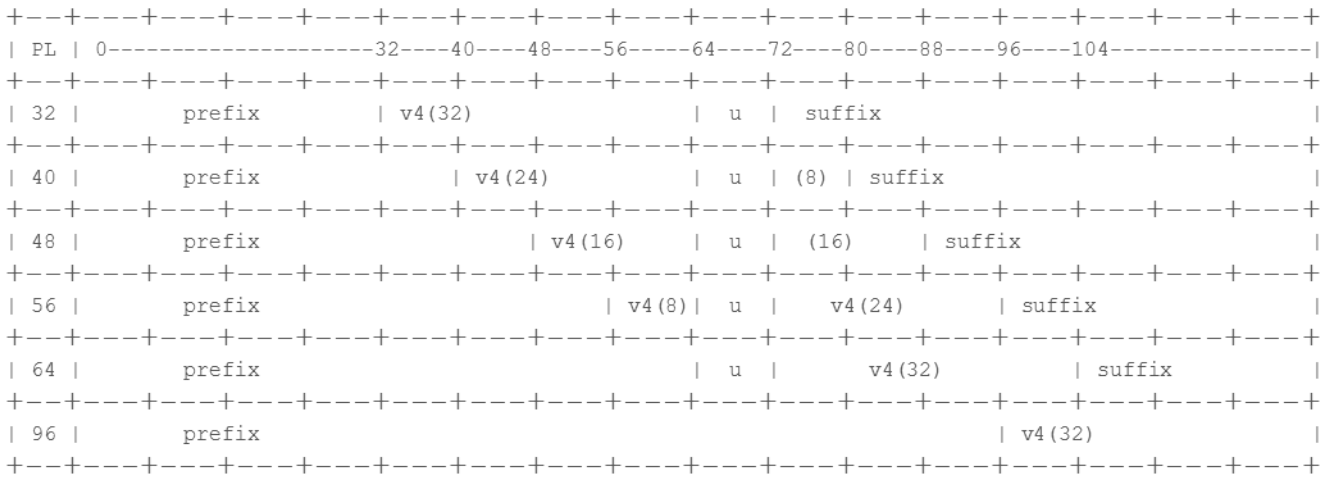
Palo Alto Networks 支持以下 NAT64 功能：

- DIPP 的持久 NAT
- 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。

©2024 Palo Alto Networks, Inc.

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：



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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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。

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)。

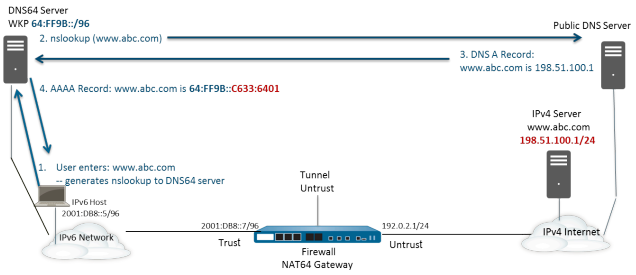
2.DNS64 服务器向 www.abc.com 的公共 DNS 服务器发送一个 nslookup，请求其 IPv4 地址。

3.DNS 服务器返回一个向 DNS64 服务器提供 IPv4 地址的 A 记录。

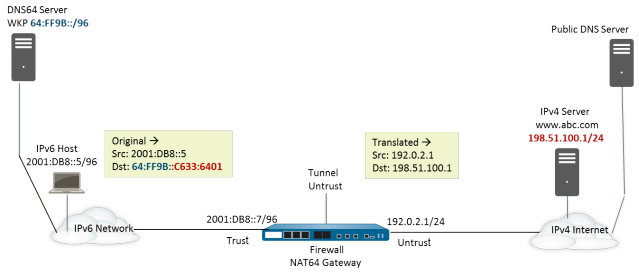
4.DNS64 服务器向 IPv6 用户发送一条 AAAA 记录，将 IPv4 点分十进制地址 198.51.100.1 转换为十六进制数 C633:6401，并将其嵌入到自己的 IPv6 前缀 64:FF9B::/96 中。 [198 = C6 hex; 51 = 33 hex; 100 = 64 hex; 1 = 01 hex.] The result is IPv4-Embedded IPv6 Address 64:FF9B::C633:6401.

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。

 ©2024 Palo Alto Networks, Inc.



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。



 ©2024 Palo Alto Networks, Inc.

为 IPv6 启动的通信配置 NAT64

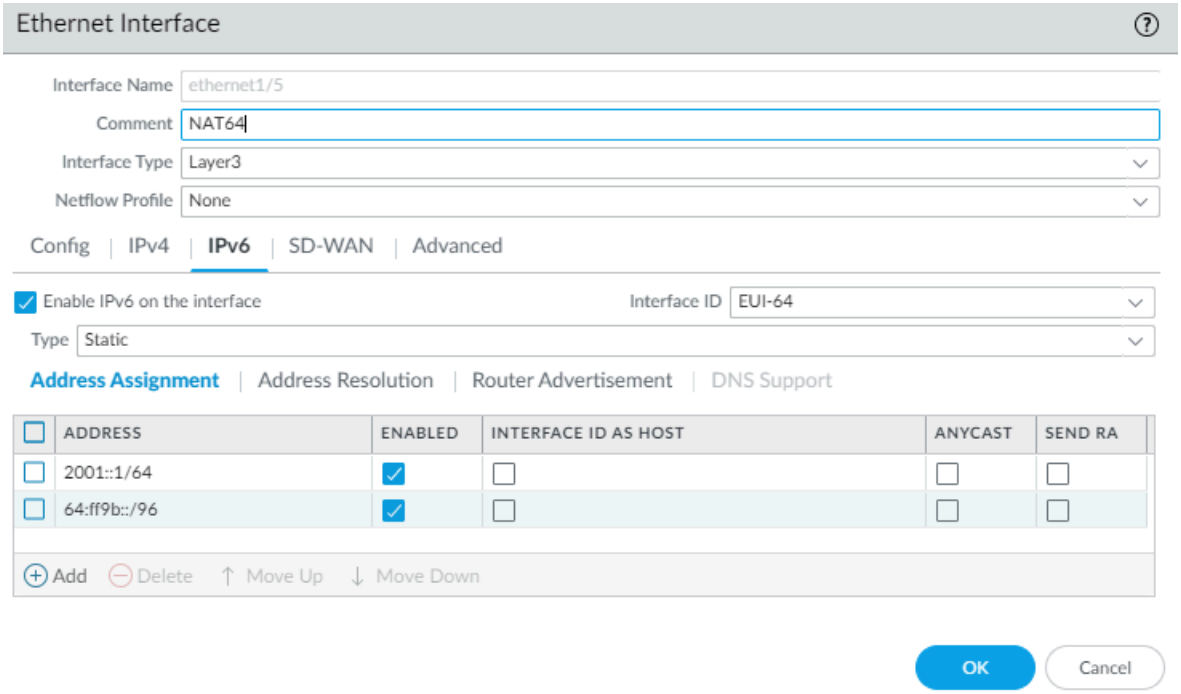
该配置任务及其地址对应于 IPv6 启动的通信中的数字。

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 | 配置 IPv6 寻址的接口。

1. 选择 **Network**（网络） > **Interfaces**（接口），然后选择执行 NAT 的接口。
2. 选择 **IPv6** 选项卡。
3. 选择 **Enable IPv6 address on interface**（在接口上启用 **IPv6** 地址）。
4. 添加专用 IPv6 前缀。
5. 添加众所周知的前缀 64:ff9b::/96。
6. 单击 **OK**（确定）。



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 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 4 | （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 5 | （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 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_ipv6_init。
3. （可选）输入 **Description**（说明）。
4. 对于 **NAT Type**（**NAT** 类型），请选择 **nat64**。

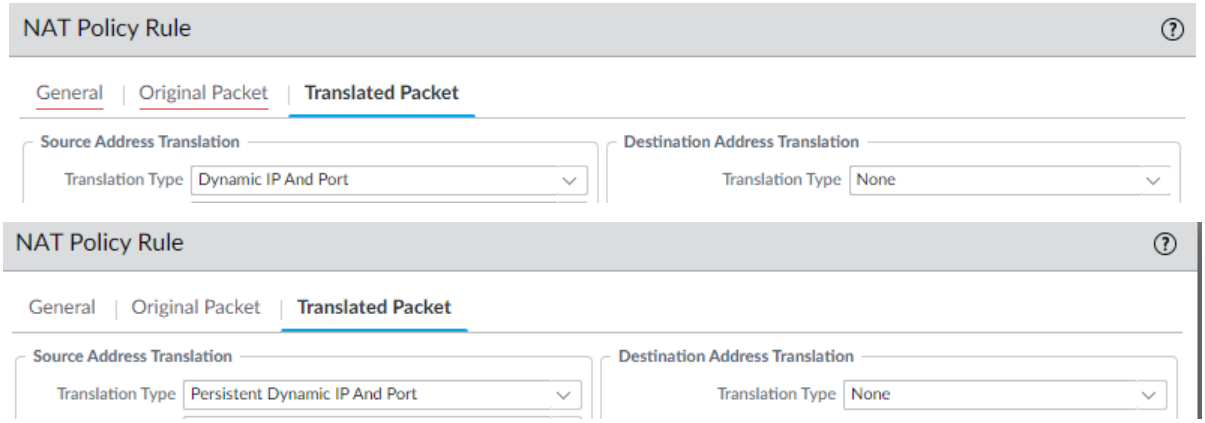
 ©2024 Palo Alto Networks, Inc.

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））。
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 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 **Dynamic IP and Port**（动态 **IP** 和端口）。对于 PAN-OS 11.0 及更低版本中的持久 DIPP，请选择 **Dynamic IP and Port**（动态 **IP** 和端口）。对于 PAN-OS 11.0 之后版本中的持久 DIPP，请选择 持久动态 **IP** 和端口（**Persistent Dynamic IP and Port**）。



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。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 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（不信区域）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 10 | 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 11 | 提交更改。

单击 **Commit**（提交）。

STEP 12 | （仅在 PAN-OS 11.1.0 及更低版本中启用持久 DIPP）为 DIPP 启用持久 NAT。

1. 访问 CLI。
2. >设置系统设置 **`persistent-dipp enable yes`**
3. **`>request restart system`**
4. 如果您配置了 HA，请在另一个 HA 对等体上重复此步骤。

STEP 13 | 排除 NAT64 会话故障或查看 NAT64 会话。

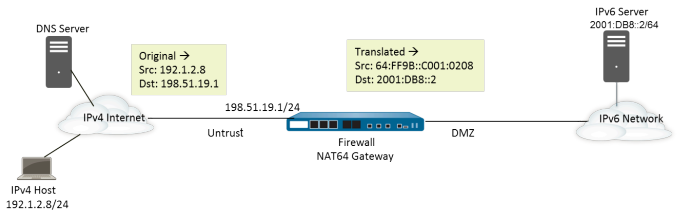
```
> show session id <session-id>
```

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

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。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）。

 ©2024 Palo Alto Networks, Inc.

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）。

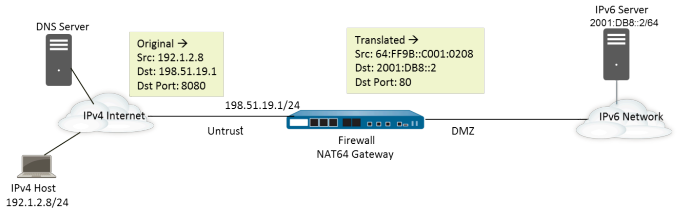
STEP 11 | 排除 NAT64 会话故障或查看 NAT64 会话。

```
> show session id <session-id>
```

 ©2024 Palo Alto Networks, Inc.

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，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）。

 ©2024 Palo Alto Networks, Inc.

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）。
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。

 ©2024 Palo Alto Networks, Inc.

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>
```

 ©2024 Palo Alto Networks, Inc.

 ©2024 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。

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。

对于高可用性对等设备出现故障时如何选择 ECMP 路径的相关信息，请参阅主动/主动 HA 模式下的 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
- 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。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 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

 ©2024 Palo Alto Networks, Inc.

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。

©2024 Palo Alto Networks, Inc.

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.

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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。

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。

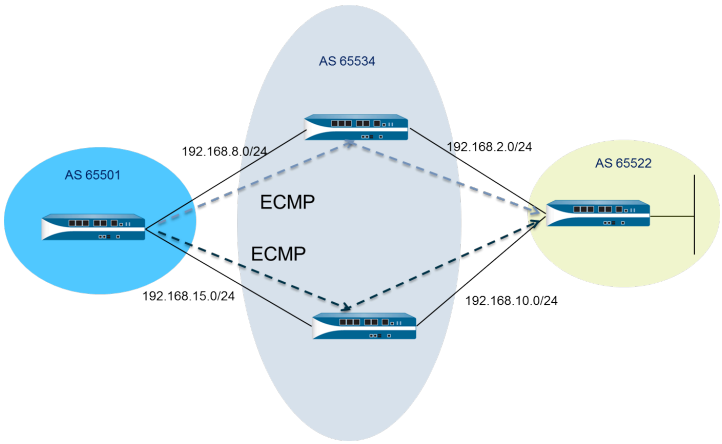
STEP 9 | 提交更改。

Commit（提交）配置。

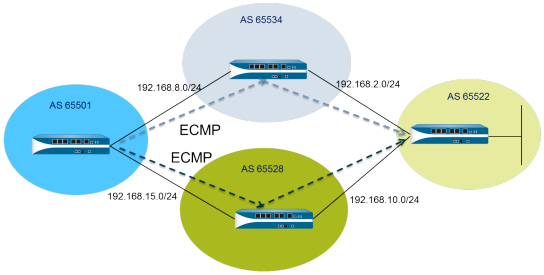
 ©2024 Palo Alto Networks, Inc.

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。

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）。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 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

链路层发现协议 (LLDP) 使用 MAC 地址在 OSI 模型的第 2 层运行。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® 防火墙只支持一个 MAC 地址传输和接收 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

 ©2024 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： • L3 接口通过路由器（位 6）功能和另一个位（位 1）通告。 • L2 接口通过 MAC 网桥（位 3）功能和另一个位（位 1）通告。 • 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： • 管理 (MGT) 接口的 IP 地址 • 接口的 IPv4 和/或 IPv6 地址

©2024 Palo Alto Networks, Inc.

可选 TLV	TLV 类型	有关防火墙实施的用途和说明
		• 回环地址 • 在管理地址字段中输入的用户定义的地址 如果未提供管理 IP 地址，会默认使用传输接口的 MAC 地址。 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）。 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。 此为可选参数，可以保持禁用状态。

 ©2024 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`。

©2024 Palo Alto Networks, Inc.

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）。范围为 1 至 3600；默认为 30。
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）。范围为 1 至 600；默认为 2。
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。范围为 1 至 100；默认为 4。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）。范围为 1 至 3600；默认为 5。
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

 ©2024 Palo Alto Networks, Inc.

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
   - 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 | **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.

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。
   - **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。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 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
- 参考资料：URL 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向对方发送控制数据包（其运作方式与呼叫数据包相似）。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 也支持 RFC 5881 (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 遵循 RFC 5883 (www.rfc-editor.org/rfc/rfc5883.txt) 中所述的 BFD 封装。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
- OSPFv2 和 OSPFv3（接口类型包括广播、点对点和点对多点）

 ©2024 Palo Alto Networks, Inc.

- 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 LACP 的 BFD（带 LAG 接口的 micro-BFD）

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。

 ©2024 Palo Alto Networks, Inc.

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。

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”。

 ©2024 Palo Alto Networks, Inc.

配置 BFD

阅读完BFD 概述（其中包含防火墙型号和支持的接口）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，请配置一个路由协议（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

 ©2024 Palo Alto Networks, Inc.

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。

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）。

 ©2024 Palo Alto Networks, Inc.

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。

 ©2024 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。

 ©2024 Palo Alto Networks, Inc.

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。

   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。

 ©2024 Palo Alto Networks, Inc.

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）。

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。

 ©2024 Palo Alto Networks, Inc.

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>
```

 ©2024 Palo Alto Networks, Inc.

参考资料：URL 详细信息

要查看虚拟路由器的以下 BFD 信息，请参阅配置 BFD的步骤 12 “查看 BFD 摘要和详细信息”。

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。 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。
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：

©2024 Palo Alto Networks, Inc.

姓名	值（示例）	说明
		0—无诊断 1—控制检测时间耗尽 2—回显功能故障 3—邻居信号显示会话关闭 4—转发面板重置 5—路径关闭 6—连接路径关闭 7—管理关闭 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。
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。

 ©2024 Palo Alto Networks, Inc.

姓名	值（示例）	说明
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。 • 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。

 ©2024 Palo Alto Networks, Inc.

姓名	值（示例）	说明
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。

 ©2024 Palo Alto Networks, Inc.

 ©2024 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、加速老化和强制网络门户身份验证之外）。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)。

 ©2024 Palo Alto Networks, Inc.

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 分离握手丢弃介绍了如何阻止 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)

您可以配置 packet-based attack protection（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）。

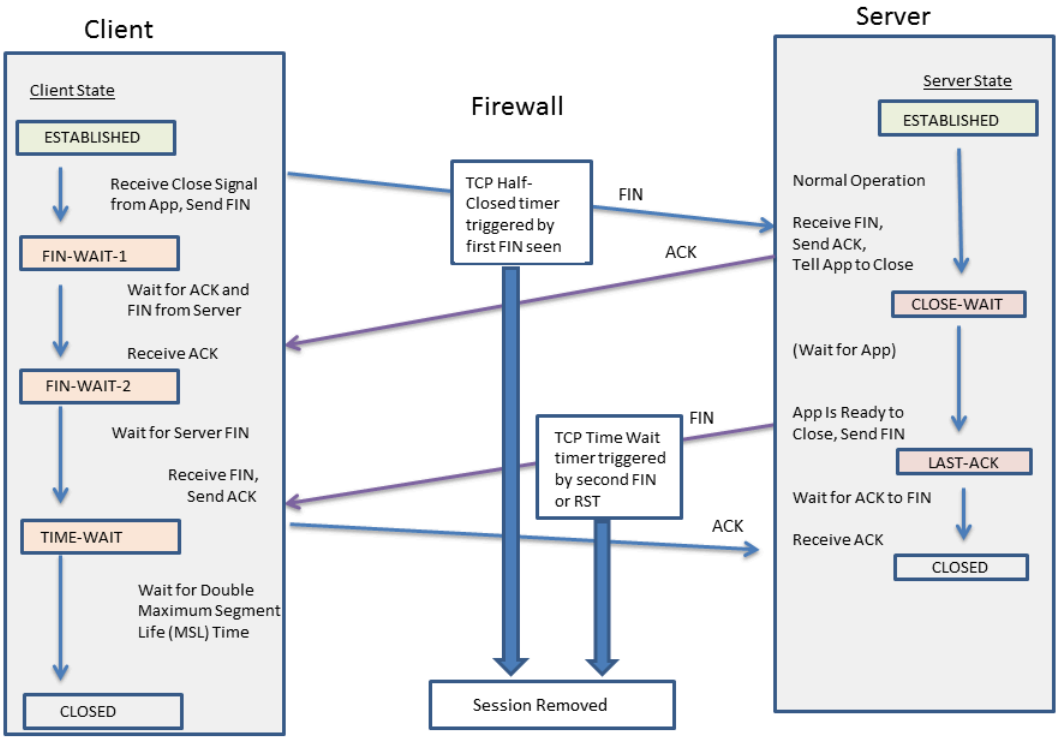
“TCP 半闭合”和“TCP 等待时间”计时器

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。

 ©2024 Palo Alto Networks, Inc.



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。

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。

 ©2024 Palo Alto Networks, Inc.

- 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。

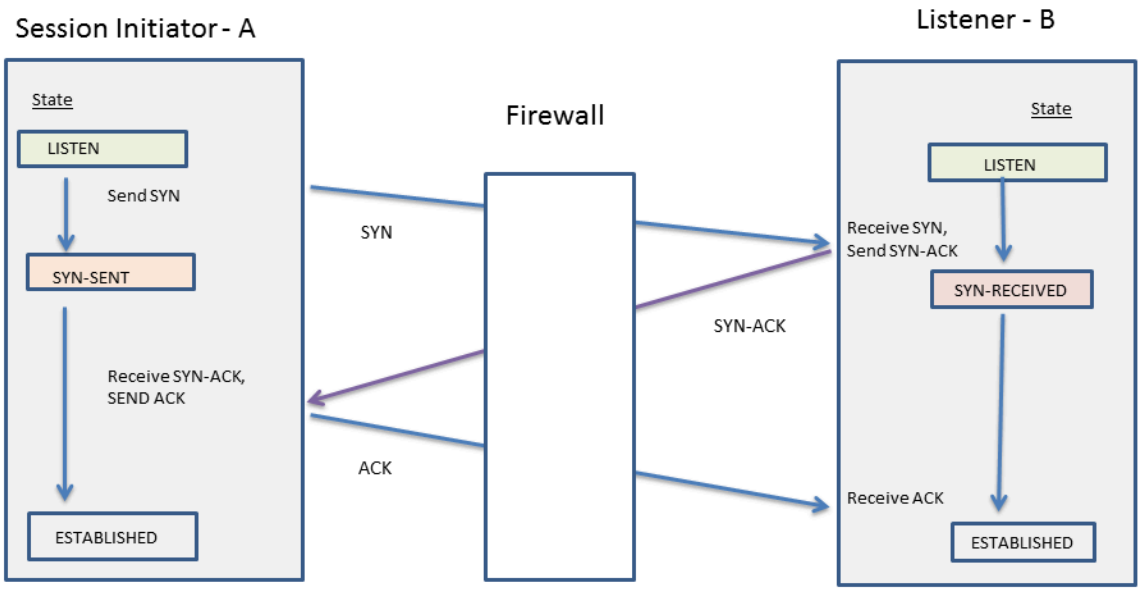
TCP 分离握手丢弃

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。

 ©2024 Palo Alto Networks, Inc.

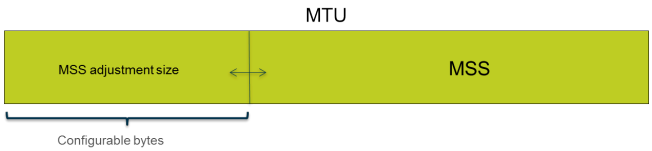
4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 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

 ©2024 Palo Alto Networks, Inc.

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。

若要配置 MSS 调整大小，请参阅配置会话设置。

 ©2024 Palo Alto Networks, Inc.

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)。

您可以在防火墙上使用区域保护配置文件配置 flood protection（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。）

 ©2024 Palo Alto Networks, Inc.

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。
- 配置 Flood Protection（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）。
- 配置 Packet-Based Attack Protection（基于数据包的攻击保护）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 Packet-Based Attack Protection（基于数据包的攻击保护）来替换 ICMPv6 类型的此默认行为。）

 ©2024 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。

 ©2024 Palo Alto Networks, Inc.

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）。

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）。

 ©2024 Palo Alto Networks, Inc.

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、强制网络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）—强制网络门户 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。

 ©2024 Palo Alto Networks, Inc.

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。范围为 1-15,999,999；默认为 90。
- **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。范围为 1 至 15,999,999，默认为 3,600。
- **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。范围为 1-60；默认为 10。
- **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。范围为 1-60；默认为 5。
- **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。范围为 1-604,800；默认为 120。
- **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。范围为 1-600；默认为 15。
- **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。范围为 1-600；默认为 30。
- 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。范围为 1-15,999,999；默认为 60。
- **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。范围为 1-15,999,999；默认为 30。
- 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。范围为 1-15,999,999；默认为 6。
- 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。

 ©2024 Palo Alto Networks, Inc.

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。

- **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。

 ©2024 Palo Alto Networks, Inc.

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 帧所占内存最多为普通数据包的五倍，能将可用数据包缓冲区的数量减少 *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。

如果您导入（***Device***（设备）**>** ***Setup***（设置）**>** ***Operations***（操作）**>** ***Import***（导入））并加载启用巨型帧的配置，然后提交至尚未启用巨型帧的防火墙，则 ***Enable Jumbo Frame***（启用巨型帧）设置不会提交至配置。您应该先 ***Enable Jumbo Frame***（启用巨型帧）、重新启动，然后导入、加载和提交配置。

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。

 ©2024 Palo Alto Networks, Inc.

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。

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。

 ©2024 Palo Alto Networks, Inc.

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。

1. 选择**Device**（设备） > **Setup**（设置） > **Operations**（操作）。
2. 单击 **Reboot Device**（重新启动设备）。

 ©2024 Palo Alto Networks, Inc.

会话分发策略

会话分发策略定义了 PA-5200 系列和 PA-7000 系列和 PA-7500 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-7500 系列	取决于数据处理卡 (DPC) 的安装数量。每个 DPC 有六个数据平面处理器。 如果 *PA-7500* 系列防火墙充当 *NGFW* 集群中的节点，这些节点必须使用相同类型的会话分发策略（固定、哈希、入口槽、随机、循环、会话负载或对称哈希）。
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 *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
PA-5450 防火墙	取决于数据处理卡 (DPC) 的安装数量。

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。

 ©2024 Palo Alto Networks, Inc.

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)。 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。 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。 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。 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。 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。 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。 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

 ©2024 Palo Alto Networks, Inc.

会话分发策略	说明
	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）。 在高需求 IPSec 或 GTP 部署中使用此策略。 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。 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。 会话分发策略 所有权分配策略：入口插槽 启用流的线卡： [2, 10, 11, 12]启用数据包处理的线卡： [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。 例如，要选择会话加载策略，请输入以下命令： **>**设置会话分发策略会话负载

 ©2024 Palo Alto Networks, Inc.

任务	命令
	如果 *PA-7500* 系列防火墙充当 *NGFW* 集群中的节点，这些节点必须使用相同类型的会话分发策略（固定、哈希、入口槽、随机、循环、会话负载或对称哈希）。
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。 以下输出来自 PA-7080 防火墙： `> 显示会话分布统计信息 DP 活动调度调度/秒 ---------- ---------- s1dp0 78698 78298 18 1473 s1dp1 78775 7831384 1535 s3dp0 7796 73663 9 1488 s3dp1 7707 737026 1442` `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。 `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。 `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。 *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)*。

©2024 Palo Alto Networks, Inc.

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）。
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）。

 ©2024 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，以执行故障排除。

- 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
- 隧道加速行为
- 禁用隧道加速

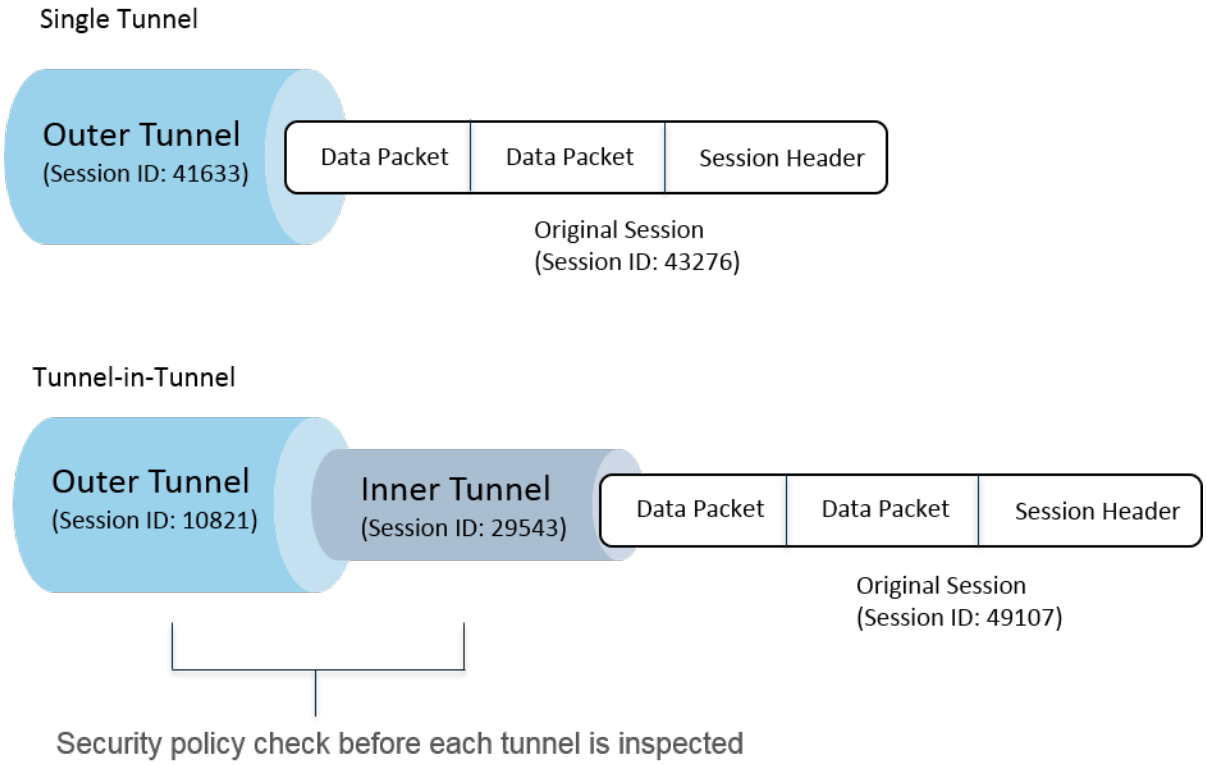
隧道内容检测概述

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。



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。

©2024 Palo Alto Networks, Inc.

- 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。

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	✓	✓	✓

©2024 Palo Alto Networks, Inc.

策略类型	外部隧道会话	内部隧道会话	内部原始会话
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。

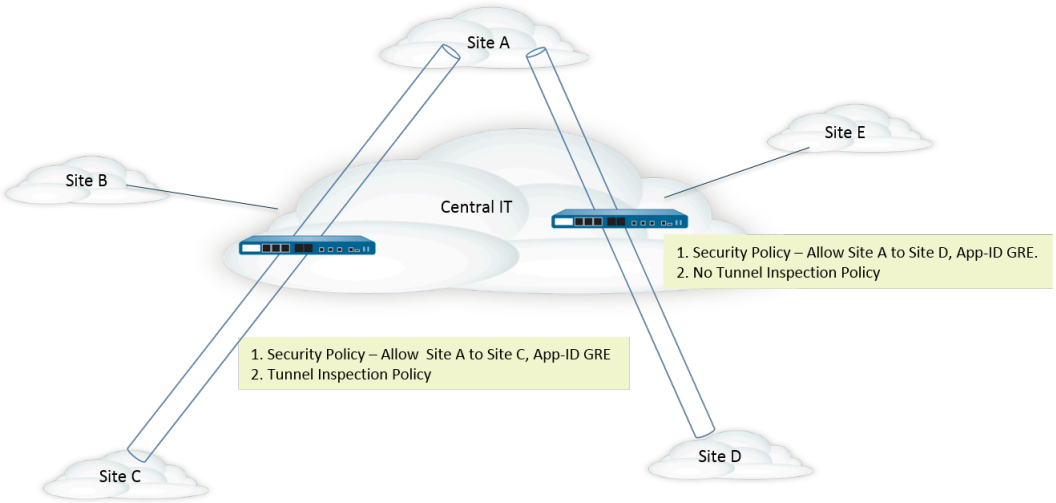
您可以在 ACC 上查看已检测的隧道活动，或是查看日志中的隧道信息。为了快速查看，请配置监控标记，以便您可以监控隧道活动并根据该标记筛选日志结果。

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。



 ©2024 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。
4. （可选）选择 **Negate**（求反）可选择除指定地址以外的任何地址。

©2024 Palo Alto Networks, Inc.

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）— 防火墙仅检查外部隧道中的内容。

     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）。

 ©2024 Palo Alto Networks, Inc.

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。
- **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。

 ©2024 Palo Alto Networks, Inc.

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）。

 ©2024 Palo Alto Networks, Inc.

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

 ©2024 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）。

 ©2024 Palo Alto Networks, Inc.

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**（碎片流量）。
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。

 ©2024 Palo Alto Networks, Inc.

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。

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。

 ©2024 Palo Alto Networks, Inc.

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）。
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。

©2024 Palo Alto Networks, Inc.

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。

©2024 Palo Alto Networks, Inc.

隧道加速行为

以下部分提供了有关 GTP-U、GRE 和 VXLAN 隧道加速的背景信息，在您决定禁用隧道加速 之前了解这些信息可能会有所帮助。

- GTP-U
- GRE
- VXLAN

GTP-U

启用 **GTP** 隧道加速之前必须满足的条件：

1. 在 **Device**（设备） > **Setup**（设置） > **Management**（管理）下启用通用隧道加速（在常规设置中，选中隧道加速）。
2. GTP 安全在 **Device**（设备） > **Setup**（设置） > **Management**（管理）下启用（在常规设置中，选中 GTP 安全）。
3. 没有启用 GTP-U 协议的隧道检查策略规则。
4. 提交配置后，您必须重新启动以加载 GTP-U 解析器程序。

硬件中识别 **GTP-U** 数据包的标准：

1. UDP 目标端口为 2152。
2. GTP.version 为 1，GTP.protocol_type 为 1。

隧道加速如何改变流 **ID**：

- 如果 GTP-U 数据包通过两个识别标准，则防火墙在流密钥中设置以下内容：
  - 编码位：1个
  - UDP 目标端口：隧道端点标识符（TEID）
  - 源地址：0
- 否则，数据包将作为普通 UDP 数据包处理。

GTP-U 隧道加速的好处

如果启用 GTP-U 加速，如果有大量隧道流量可以卸载，那么主要好处就会出现。很大一部分 GTP 流量来自移动设备，主要是网络流量，在检查内部有效负载时不会卸载这些流量。

GTP 安全功能无需加速即可完全发挥作用，性能优势与硬件可以卸载的内部有效负载流量相关。例如，任何通常被标记为 L7 完成 的东西都将作为 GTP 内部的内部应用程序在硬件中卸载和处理。

GRE

GRE 生效的隧道加速标准：

- 在 **Device**（设备） > **Setup**（设置） > **Management**（管理）下启用通用隧道加速（在常规设置中，选中隧道加速）。

硬件中识别 **GRE** 数据包的标准：

 ©2024 Palo Alto Networks, Inc.

- IP 协议 47

隧道加速如何改变流 **ID**：

- 流键在有和没有隧道加速的情况下是一样的。

GRE 隧道加速的好处

- 使用 **TCI**：与没有隧道加速的相同流量相比，使用隧道加速的 GRE 直通流量在流量处理方面的性能将提高约 30%。
- 不使用 **TCI**：如果未使用通道内容检查（TCI）策略，则禁用通道加速不会对 GRE 通信量的性能产生影响。

VXLAN

VXLAN 生效的隧道加速标准：

- 在 **Device**（设备） > **Setup**（设置） > **Management**（管理）下启用通用隧道加速（在常规设置中，选中隧道加速）。

硬件中识别 **VXLAN** 数据包的标准：

- UDP 目标端口为 4789。

改变了什么：

- UDP 目标端口从 VXLAN 标头更改为 VXLAN 网络标识符 (VNI) 值。
- 编码更改为 2。

VXLAN 隧道加速的好处

- 通用：消耗的会话资源更少，因为我们只需要 VNI 会话而不需要外部 VXLAN UDP 会话。对于 VXLAN，我们将解析 VXLAN 标头以提取 VNI，并使用 VNI 为 VXLAN 隧道内的每个 VNI 派生唯一的流 ID。
- 使用 **TCI**：与没有隧道加速的相同流量相比，使用隧道加速的 VXLAN 直通流量的流处理性能将提高约 30%。
- 不使用 **TCI**：即使不使用 TCI，与没有隧道加速的相同流量相比，我们也会看到使用隧道加速的流量处理性能提高了大约 10%。不同的流 ID 可能会导致流被放置在不同的数据平面上，从而导致单个 VXLAN 隧道的负载如何分配给将在隧道中传递的各种 VNI。除非有多个 VNI 的 VXLAN 流，否则性能影响几乎可以忽略不计。

 ©2024 Palo Alto Networks, Inc.

禁用隧道加速

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。

PA-3200 系列防火墙、PA-5450 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。

如果未使用通道内容检查（*TCI*）策略，则禁用通道加速不会对 *GRE* 通信量的性能产生影响。

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。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

网络数据包代理

网络数据包代理筛选网络流量并将其转发到一个或多个第三方安全设备的外部安全链。网络数据包代理取代了 PAN-OS 8.1 中引入的解密代理功能，并将其功能扩展至包括转发非解密 TLS 流量和非 TLS 流量（明文）以及解密 TLS 流量。在金融和政府机构等安全性非常高的环境中，处理所有类型流量的能力尤其重要。

PA-7000 系列、PA-7000b、PA-5400 系列、PA-5200 系列、PA-3400 系列和 PA-3200 系列设备以及 VM-300 和 VM-700 型号支持网络数据包代理。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。

- 网络数据包代理概述
- 网络数据包代理的运作方式
- 准备部署网络数据包代理
- 配置透明桥接安全链
- 配置第 3 层路由安全链
- 网络数据包代理 HA 支持
- 网络数据包代理的用户界面更改
- 网络数据包代理的限制
- 对网络数据包代理进行故障排除

网络数据包代理概述

如果您使用一个或多个第三方安全设备（安全链）作为整体安全套件的一部分，则可以使用网络数据包代理筛选网络流量并将其转发到这些安全设备。网络数据包代理取代了 PAN-OS 8.1 中引入的解密代理功能。

与解密代理一样，网络数据包代理提供解密功能和安全链管理。通过消除支持这些功能的专用设备的复杂性，简化了您的网络，并降低了资本和运营成本。与解密代理一样，网络数据包代理提供确保到安全链的路径运行状况良好的运行状况检查，并提供在链中断时处理流量的选项。

网络数据包代理扩展了防火墙的安全链转发功能，因此您不仅可以筛选解密 TLS 流量，还可以筛选非解密 TLS 流量和非 TLS（明文）流量，并将其转发到基于应用程序、用户、设备、IP 地址和区域的一个或多个安全链。这些功能在金融和政府机构等安全性非常高的环境中特别有价值。

升级和降级：

- 当您在具有解密代理许可证的防火墙上升级到 PAN-OS 11.1 时：
  - 重新启动防火墙后，许可证名称将自动更改为网络数据包代理。

    无论防火墙是独立防火墙、*HA* 对的一部分，还是从 *Panorama* 将网络数据包代理许可证推送到防火墙，都必须重新启动防火墙才能使许可证生效并更新用户界面。
  - PAN-OS 将任何现有的解密代理转发配置文件（**Profiles**（配置文件） > **Decryption**（解密） > **Forwarding Profile**（转发配置文件））转换为数据包代理配置文件。
  - PAN-OS 将用于转发流量到安全链的任何现有解密策略规则转换为网络数据包代理策略规则。
  - PAN-OS 从用户界面中删除解密代理配置文件，并将其替换为数据包代理配置文件（**Profiles**（配置文件） > **Packet Broker**（数据包代理）），同时还添加网络数据包代理策略（**Policies**（策略） > **Network Packet Broker**（网络数据包代理））。
- 从 PAN-OS 10.1 降级到 PAN-OS 10.0 时：
  - PAN-OS 将任何现有的数据包代理配置文件转换为解密代理转发配置文件。
  - PAN-OS 删除网络数据包代理规则库并打印一条警告消息。您必须将网络数据包代理策略规则重新配置为解密转发的解密策略规则。
  - 许可证名称仍为网络数据包代理（重新启动后，所有 PAN-OS 版本中的许可证名称从解密代理更改为网络数据包代理，不影响解密代理的运行）。但是，该功能是解密代理功能，而不是网络数据包代理功能。
  - PAN-OS 从用户界面移除网络数据包代理配置文件，并将其替换为解密转发配置文件，同时还从用户界面移除网络数据包代理策略（未发生替换；您使用解密策略规则仅将解密转发代理流量转发到安全链）。

使用网络数据包代理的要求：

- 您必须在防火墙上安装免费的数据包代理许可证。没有免费许可证就无法访问界面中的数据包代理策略和配置文件。

 ©2024 Palo Alto Networks, Inc.

- 防火墙必须至少有两个可用的第 3 层以太网接口，以用作专用数据包代理转发接口对。
  - 您可以配置多对专用网络数据包代理转发接口，以连接到不同的安全链。
  - 对于每个安全链，专用网络数据包代理接口对必须位于同一安全区域中。

    安全策略必须允许在每组配对的网络数据包代理接口之间进行流量。默认情况下，***intrazone-default***（区域内默认）安全策略规则允许同一区域内的流量。但是，如果您在策略规则库之前有一条“全部拒绝” 策略规则，则必须创建明确的允许规则以允许网络数据包代理流量。
  - 专用接口对连接到安全链中的第一个和最后一个设备。

    网络数据包代理支持第 *3* 层路由安全链和第 *1* 层透明桥接安全链。对于第 *3* 层路由链，一对数据包代理转发接口可以使用正确配置的交换机、路由器或其他设备连接到多个第 *3* 层安全链，以在防火墙与安全链之间执行所需的第 *3* 层路由。
- 专用网络数据包代理转发接口不能使用动态路由协议。
- 安全链中的任何设备都不能修改原始会话的源或目标 IP 地址、源或目标端口或协议，因为防火墙无法将修改后的会话与原始会话匹配，从而会丢弃流量。
- 您必须启用防火墙以允许转发解密的内容 （**Device**（设备） > **Setup**（设置） > **Content-ID**（内容 **ID**））。

网络数据包代理支持：

- 解密 TLS、非解密 TLS 和非 TLS 流量。
- SSL 转发代理、SSL 入站检查和加密 SSH 流量。
- 第 3 层路由安全链。
- 第 1 层透明桥接安全链。

  您可以在同一防火墙上配置第 *3* 层路由安全链和第 *1* 层透明桥接安全链，但必须为每种类型使用不同的转发接口对。
- 通过链的单向流量：流向链的所有流量在一个专用接口上离开防火墙，并在另一个专用接口上返回到防火墙，因此所有流量通过一对专用网络数据包代理接口朝相同的方向流动。

  两个防火墙转发接口必须位于同一区域中。
- 通过安全链的双向流量：
  - 客户端到服务器 (c2s) 流量在一个专用防火墙代理接口上离开防火墙，并在另一个专用防火墙代理接口上返回到防火墙。
  - 服务器到客户端 (s2c) 流量使用与 c2s 流量相同的两个专用防火墙代理接口，但流量以相反的方向流经安全链。s2c 流量进入链的防火墙代理接口与 c2s 流量从链返回到防火墙的接口相同。s2c 流量返回到防火墙的防火墙代理接口与 c2s 流量流出链的接口相同。

    两个防火墙转发接口必须位于同一区域中。

网络数据包代理不支持组播、广播或解密 *SSH* 流量。

 ©2024 Palo Alto Networks, Inc.

网络数据包代理的运作方式

将防火墙连接到第三方安全设备链的高级工作流程是：

1. 确定要转发的非解密 TLS、解密 TLS 和非 TLS（TCP 和 UDP）流量。
2. 确定安全链拓扑。确定每个安全链的设备是否透明地（桥接）转发流量，或者设备是否基于第 3 层信息路由流量。使用多个安全链有助于负载均衡流量。此外，决定安全链未通过运行状况检查时是绕过安全链（流量在防火墙上经过正常处理，并相应地被转发或阻止）还是阻止流量。
3. 在将流量转发到安全链的防火墙上安装免费的网络数据包代理许可证。
4. 确定一对或多对防火墙接口以将流量转发到一个或多个安全链，并在这些接口上启用网络数据包代理。
5. 配置至少一个数据包代理配置文件。
6. 配置至少一个网络数据包代理策略。

要使用一系列第三方安全设备来检查流量，请在防火墙上配置以下三个对象：

- **Interfaces**（接口）—一对或多对第 3 层以太网防火墙接口，用于将流量从防火墙转发到安全链并接收从安全链返回的处理后流量。在配置配置文件和策略规则之前配置网络数据包代理接口对，因为您需要在配置文件中指定接口对。
- **Packet Broker profiles**（数据包代理配置文件）—配置文件控制如何将您在策略中定义的流量转发到安全链。每个网络数据包代理策略规则都有一个关联的数据包代理配置文件。配置文件定义安全链是第 3 层路由链还是第 1 层透明桥接链、通过链的流量方向（单向或双向）、专用网络数据包代理防火墙接口以及如何监控防火墙与安全链之间连接的运行状况。对于多个第 3 层路由安全链，您可以指定每个链的第一个和最后一个设备以及关联流量的会话分发（负载均衡）方法。
- **Network Packet Broker policy rules**（网络数据包代理策略规则）—策略规则定义要转发到每个安全链或要对多个路由（第 3 层）链进行负载均衡的应用程序流量。策略规则定义要转发到安全链的流量的来源和目的地、用户、应用程序和服务。策略规则还定义要转发到安全链的流量类型：您可以选择解密 TLS 流量、非解密 TLS 流量、非 TLS 流量或流量类型的任意组合。您还可以在每个策略规则中添加一个数据包代理配置文件，以指定要向其转发流量的安全链（以及所有其他配置文件特征）。

  使用 Policy Optimizer（策略优化器）来审查和收紧网络数据包代理策略规则。

为了将应用程序流量与网络数据包代理策略规则匹配，网络数据包代理会在防火墙 App-ID 缓存中查找应用程序。如果应用程序不在 App-ID 缓存中，则防火墙会绕过安全链并将安全策略允许规则中配置的任何威胁检查应用于流量。如果应用程序位于 App-ID 缓存中，则防火墙会以网络数据包代理策略规则及其关联数据包代理配置文件指定的方式将流量转发到安全链。

对于非解密 TLS 和非 TLS 流量，防火墙会在第一个会话的 App-ID 缓存中安装应用程序，因此防火墙会按照网络数据包代理策略和配置文件中的规定处理流量。

对于解密 TLS 流量，在应用程序的第一个会话中，网络数据包代理不知道会话正在被解密，并将“ssl”视为应用程序。底层特定应用程序尚不可知或未安装在 App-ID 缓存中，因此代理查找失败并且流量绕过安全链。流量仍受安全策略允许规则中配置的任何威胁检查的约束。当防火墙解密流量时，防火墙会获悉特定的应用程序并将其安装在 App-ID 缓存中。对于同一应用程序的第二个

 ©2024 Palo Alto Networks, Inc.

和后续解密会话，网络数据包代理查找成功，因为特定应用程序现在位于 App-ID 缓存中，且防火墙会按预期将流量转发到安全链。

 ©2024 Palo Alto Networks, Inc.

准备部署网络数据包代理

采取以下操作准备部署网络数据包代理：

1. 获取并激活免费的网络数据包代理许可证。
   1. 登录到客户支持门户。
   2. 在左侧导航窗格中选择**Assets**（资产） > **Devices**（设备）。
   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）。
   4. 在“激活许可证”下，选择 **Activate Feature License**（激活功能许可证）
   5. 选择 **Network Packet Broker**（网络数据包代理）免费许可证。
   6. 单击 **Agree and Submit**（同意并提交）。
2. 在防火墙上安装许可证。
   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. 验证 **Device**（设备） > **Licenses**（许可证）页面是否显示防火墙上的 **Network Packet Broker**（网络数据包代理）许可证现在处于活动状态。
   4. 重启防火墙（**Device**（设备） > **Setup**（设置） > **Operations**（操作））。在防火墙重新启动之前，无法配置网络数据包代理。

   您可以将网络数据包代理许可证从 *Panorama* 推送到受管防火墙。您必须重新启动防火墙才能使许可证生效并更新用户界面。
3. 为网络数据包代理启用 App-ID 缓存。
   1. 默认情况下，App-ID 缓存处于禁用状态。使用配置模式 CLI 命令启用：

      ```
      admin@PA-3260# set deviceconfig setting application cache yes
      ```
   2. 启用防火墙以使用 App-ID 缓存来识别应用程序：

      ```
      admin@PA-3260# set deviceconfig setting application use-cache-
      for-identification yes
      ```

   验证设置是否显示 `Application cache`（应用程序缓存）已设置为 `yes`（是），`Use cache for appid`（为 `appid` 使用缓存）也已设置为 `yes`（是）：

   ```
   admin@PA-3260> show running application setting Application
    setting:Application cache : yes Supernode : yes Heuristics : yes
    Cache Threshold :1 Bypass when exceeds queue limit: no Traceroute
    appid : yes Traceroute TTL threshold :30 Use cache for appid : yes
    Use simple appsigs for ident : yes Use AppID cache on SSL/SNI : no
   ```


©2024 Palo Alto Networks, Inc.

```
Unknown capture : on Max. unknown sessions :5000 Current unknown
sessions :33 Application capture : off
```

```
Current APPID Signature Memory Usage :16768 KB (Actual 16461 KB)
 TCP 1 C2S : regex 11898 states TCP 1 S2C : regex 4549 states UDP 1
 C2S : regex 4263 states UDP 1 S2C : regex 1605 states
```

4. 启用防火墙以允许转发解密的内容（**Device**（设备） > **Setup**（设置） > **Content-ID**（内容 **ID**））。
5. 确定要转发到一个或多个安全链的流量。
6. 确定每个安全链的拓扑结构，并确定是使用第 1 层透明桥接转发还是第 3 层路由转发，这决定了您在防火墙上配置的安全链类型。考虑事项包括：
   - 您是想在多个链上实现流量负载均衡（使用第 3 层路由安全链通过路由器、交换机或其他路由设备在多个链上分发会话）、使用单个链还是对不同类型的流量使用不同的安全链。对于多个第 1 层透明桥接链，每个安全链都需要一对专用防火墙接口，因为第 1 层连接没有路由。
   - 是使用单向还是双向流量通过安全链。
7. 确定哪对防火墙接口用作专用网络数据包代理转发接口。
   - 对于第 1 层透明桥接链，每个第 1 层安全链都需要一对专用防火墙接口。您可以配置策略规则以将特定流量发送到不同的安全链。
   - 对于第 3 层路由链，一对专用防火墙接口可以通过交换机、路由器或其他支持路由功能的设备在多个第 3 层安全链之间对流量进行负载均衡。
   - 对于第 3 层路由链，您可以使用多对专用防火墙接口，根据不同的策略规则将特定流量发送到不同的安全链。

安全策略必须允许在每组配对的网络数据包代理接口之间进行流量。默认情况下，***intrazone-default***（区域内默认）安全策略规则允许同一区域内的流量。但是，如果您在策略规则库之前有一条“全部拒绝”策略规则，则必须创建明确的允许规则以允许网络数据包代理流量。

 ©2024 Palo Alto Networks, Inc.

配置透明桥接安全链

第 1 层透明桥接安全链通过一系列直接连接的数据检查和处理安全设备转发来自一个防火墙接口的流量，然后通过不同的防火墙接口转发回设备，无需路由流量。

在配置第 1 层透明桥接安全链之前，请执行以下步骤以 准备部署网络数据包代理，包括确保防火墙和安全链设备之间的物理连接是正确的，并且您允许防火墙转发解密的内容。

要在多个透明桥接安全链之间分发会话，请在防火墙上为要用于负载均衡流量的每个安全链创建一个第 1 层透明桥接安全链。防火墙上的每个透明桥接安全链都需要两个专用第 3 层以太网接口。检查以确保您有足够的空闲以太网接口用于要配置的拓扑。

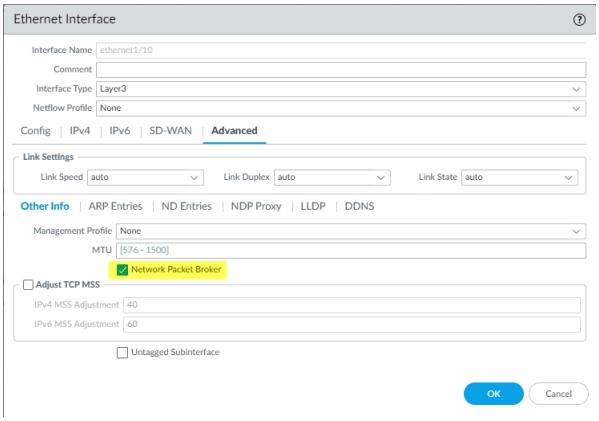
第 1 层透明桥接安全链无法故障转移到另一个安全链，因为它们没有路由。

STEP 1 | 启用两个第 3 层以太网接口作为网络数据包代理转发接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 选择一个未使用的以太网接口作为两个网络数据包代理转发接口之一。
3. 将 **Interface Type**（接口类型）设置为 **Layer3**（第 3 层）。
4. 在 **Config**（配置）选项卡中，选择要向其分配接口的区域。

   您必须在同一区域中配置两个安全链接口。

   安全策略必须允许在每组配对的网络数据包代理接口之间进行流量。默认情况下，***intrazone-default***（区域内默认）安全策略规则允许同一区域内的流量。但是，如果您在策略规则库之前有一条“全部拒绝”策略规则，则必须创建明确的允许规则以允许网络数据包代理流量。
5. 作为最佳实践，在 **Config**（配置）选项卡中，使用或创建要向其分配接口的专用虚拟路由器。使用专用虚拟路由器可确保网络数据包代理接口流量与其他流量保持分离。
6. 依次选择 **Advanced**（高级）和 **Network Packet Broker**（网络数据包代理）以启用该接口。



7. 单击 **OK**（确定）以保存接口配置。
8. 对另一个未使用的以太网接口重复以上操作，以配置另一个网络数据包代理转发接口。

©2024 Palo Alto Networks, Inc.

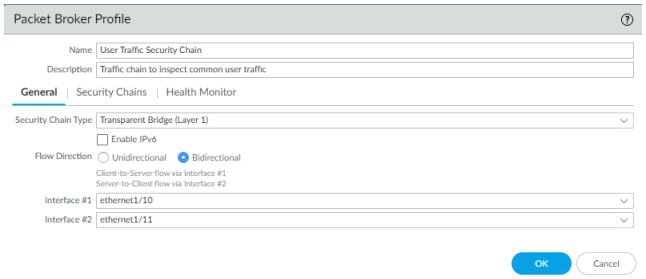
STEP 2 | 配置数据包代理配置文件以控制如何将流量转发到第 1 层透明桥接安全链。

1. 选择 **Objects**（对象） > **Packet Broker Profile**（数据包代理配置文件），然后 **Add**（添加）新配置文件或修改现有配置文件。
2. 为配置文件提供 **Name**（名称）和 **Description**（说明），以便您轻松确定其用途。
3. 在 **General**（常规）选项卡中：
   - 选择 **Transparent Bridge (Layer 1)**（透明桥接（第 **1** 层））作为 **Security Chain Type**（安全链类型）。
   - 如果流量是 IPv6 流量，则 **Enable IPv6**（启用 **IPv6**）。
   - 选择 **Flow Direction**（流向）。

     您的网络拓扑决定了使用单向流还是双向流。使用任一方法的性能大致相同。

     要使用一个防火墙接口同时将 c2s 和 s2c 会话流转发到安全链，并使用另一个防火墙接口接收从安全链返回的这两个会话流，请选择 **Unidirectional**（单向）。

     要使用接口 **1** 将 c2s 流转发到安全链并接收来自安全链的 s2c 流，同时使用接口 **2** 将 s2c 流转发到安全链并接收来自安全链的 c2s 流，请选择 **Bidirectional**（双向）。
   - 指定网络数据包代理转发接口对接口 **1** 和接口 **2**。必须已启用两个接口才能使用网络数据包代理（请参阅 准备部署网络数据包代理）。在配置哪个接口是接口 **1**，哪个接口是接口 **2** 时，请注意流向。



4. **Security Chains**（安全链）选项卡不用于透明桥接。
5. 在 **Health Monitor**（运行状况监控）选项卡中：
   - 选择您要执行的运行状况监控类型，以便您可以控制在安全链出现故障时发生的情况。您可以从 **Path Monitoring**（路径监控）、**HTTP Monitoring**（**HTTP** 监控）和 **HTTP Monitoring Latency**（**HTTP** 监控延迟）中选择一项、两项或全部。

     Path Monitoring（路径监控）—使用 ping 检查设备连接。

     HTTP Monitoring（**HTTP** 监控）—检查设备可用性和响应时间。

     HTTP Monitoring Latency（**HTTP** 监控延迟）—检查设备处理速度和效率。当您选择此选项时，也会自动启用 **HTTP Monitoring**（**HTTP** 监控）。
   - 启用一种或多种类型的运行状况监控会激活 **On Health Check Failure**（运行状况检查失败）选项，该选项确定防火墙在出现安全链运行状况故障时如何处理安全链流量。选项包括 **Bypass Security Chain**（绕过安全链）和 **Block Session**（阻止会话）。

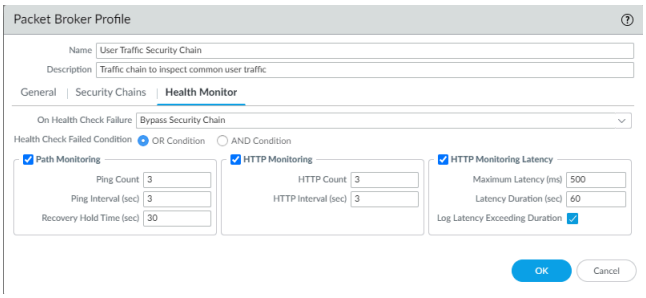
 ©2024 Palo Alto Networks, Inc.

Bypass Security Chain（绕过安全链）—防火墙将流量转发到其目的地而不是安全链，并将任何配置的安全配置文件和保护应用于流量。

Block Session（阻止会话）—防火墙会阻止会话。

您选择的方法取决于当无法运行流量通过安全链时您希望如何处理流量。

- 如果您选择多个运行状况检查选项，请选择是当任何一个监控选项记录失败条件时（**OR Condition**（**OR** 条件））还是仅当所有选定监控选项都记录失败条件（**AND Condition**（**AND** 条件））时，防火墙将运行状况检查视为失败（**Health Check Failed Condition**（运行状况检查失败条件））。例如，如果您启用全部三个运行状况检查选项，且其中一个选项记录到失败条件，则当您选择 **OR Condition**（**OR** 条件）时，防火墙会视为安全链连接失败并执行您在 **On Health Check Failure**（运行状况检查失败）中指定的操作。如果您选择 **AND Condition**（**AND** 条件），防火墙仍会视为连接运行状况良好，因为其中两个运行状况指标仍然正常。



6. 单击 **OK**（确定）保存配置文件。

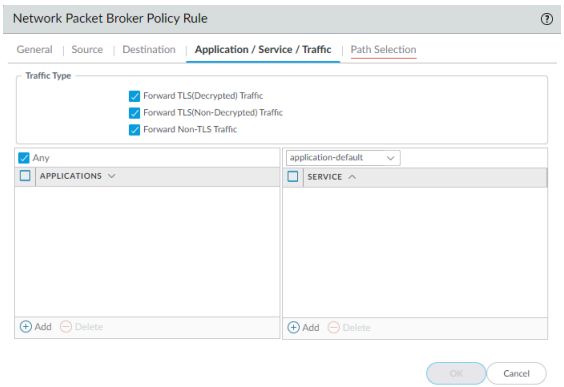
STEP 3 | 配置数据包代理策略以定义要转发到第 1 层透明桥接安全链的流量。

1. 选择 **Policies**（策略） > **Network Packet Broker**（网络数据包代理），然后 **Add**（添加）新的策略规则或修改现有的策略规则。
2. 在 **General**（常规）选项卡中，为策略规则指定 **Name**（名称）和 **Description**（说明），以便您轻松识别其用途、添加 **Audit Comment**（审核注释）并应用标签（如有使用）。
3. 在 **Source**（源）选项卡中，确定您希望规则转发到安全链的流量的源区域、IP 地址、用户和设备。
4. 在 **Destination**（目标）选项卡中，确定您希望规则转发到安全链的流量的目标区域、IP 地址和设备。
5. 在 **Application/Service/Traffic**（应用程序/服务/流量）选项卡中，确定您希望规则转发到安全链的应用程序和服务。除非您希望规则控制应用程序使用非标准端口（例如内部自定义应用程序），否则最佳做法是将 **Service**（服务）设置为 **Application Default**（应用程序默认值），以便阻止使用非标准端口表现出规避行为的应用程序。

   对于 **Traffic Type**（流量类型），选择您希望规则转发到安全链的所有流量类型。**Forward TLS(Decrypted) Traffic**（转发 **TLS**（解密）流量）是默认选择。您可以选择 **Forward TLS(Decrypted) Traffic**（转发 **TLS**（解密）流量）、**Forward TLS(Non-Decrypted)**（转发

 ©2024 Palo Alto Networks, Inc.

TLS（非解密）流量）和 **Forward Non-TLS Traffic**（转发非 **TLS** 流量）的任意组合以转发到安全链。



6. 在 **Path Selection**（路径选择）选项卡中，选择您在第 2 步中创建的数据包代理配置文件或创建一个新配置文件，以控制如何将策略规则控制的流量发送到安全链。

STEP 4 | 重复第 1 步到第 3 步以创建更多的第 1 层透明桥接安全链。

对于每个第 1 层透明桥接安全链：

- 用作网络数据包代理转发接口的两个以太网接口必须专用于每个安全链。用于透明桥接安全链的以太网接口不能用于任何其他用途或承载任何其他流量。
- 每对网络数据包代理转发接口都连接到一个第 1 层透明桥接安全链。

您可以通过创建在透明桥接安全链之间相对平均地分配流量的网络数据包代理策略规则来负载均衡流量。您还可以使用策略规则引导特定流量和流量类型通过特定安全链。

第 1 层透明桥接安全链无法故障转移到另一个安全链，因为它们没有路由。使用数据包代理配置文件中的 ***Health Monitor***（运行状况监控）选项卡配置当透明桥接安全链发生故障时如何处理流量。

 ©2024 Palo Alto Networks, Inc.

配置第 3 层路由安全链

第 3 层路由安全链使用防火墙上的两个专用转发接口，将流量转发到一系列数据检查和处理安全设备，然后转发回防火墙。

在配置路由的第 3 层安全链之前，请采取步骤准备部署网络数据包代理，包括确保防火墙和安全链设备之间的物理连接正确以及允许防火墙转发解密的内容。检查以确保防火墙上有足够的空闲以太网接口用于要配置的拓扑。

您在防火墙上配置的每个第 3 层路由安全链都需要两个专用第 3 层以太网接口，它们可以通过防火墙与安全链之间正确配置的路由器、交换机或类似设备连接到一个第 3 层安全链或将会话（负载均衡）最多分发到 64 个第 3 层安全链。

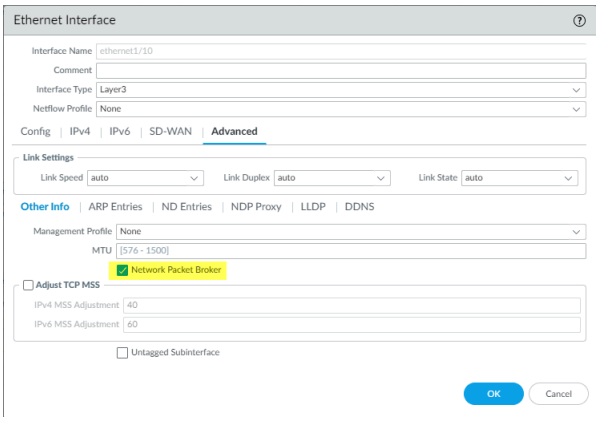
网络数据包代理无法在第 3 层路由安全链上转发 IPv6 流量。要转发 IPv6 流量，请使用透明桥接（第 1 层）安全链。

STEP 1 | 启用两个第 3 层以太网接口作为网络数据包代理转发接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 选择一个未使用的以太网接口作为两个网络数据包代理转发接口之一。
3. 将 **Interface Type**（接口类型）设置为 **Layer3**（第 3 层）。
4. 在 **Config**（配置）选项卡中，选择要向其分配接口的区域。

   您必须在同一区域中配置两个安全链接口。

   安全策略必须允许在每组配对的网络数据包代理接口之间进行流量。默认情况下，***intrazone-default***（区域内默认）安全策略规则允许同一区域内的流量。但是，如果您在策略规则库之前有一条“全部拒绝”策略规则，则必须创建明确的允许规则以允许网络数据包代理流量。
5. 作为最佳实践，在 **Config**（配置）选项卡中，使用或创建要向其分配接口的专用虚拟路由器。使用专用虚拟路由器可确保网络数据包代理接口流量与其他流量保持分离。
6. 依次选择 **Advanced**（高级）和 **Network Packet Broker**（网络数据包代理）以启用该接口。



7. 单击 **OK**（确定）以保存接口配置。
8. 对另一个未使用的以太网接口重复以上操作，以配置另一个网络数据包代理转发接口。

 ©2024 Palo Alto Networks, Inc.

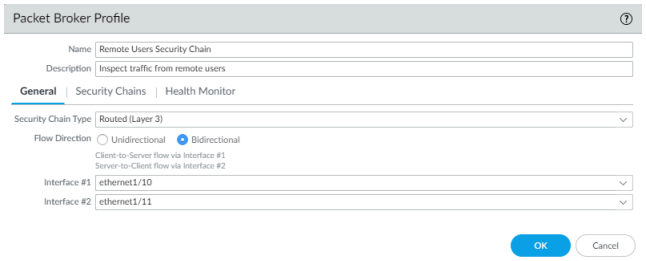
STEP 2 | 配置数据包代理配置文件以控制如何将流量转发到第 3 层路由安全链。

1. 选择 **Objects**（对象） > **Packet Broker Profile**（数据包代理配置文件），然后 **Add**（添加）新配置文件或修改现有配置文件。
2. 为配置文件提供 **Name**（名称）和 **Description**（说明），以便您轻松确定其用途。
3. 在 **General**（常规）选项卡中：
   - 选择 **Routed (Layer 3)**（路由（第 3 层））作为 **Security Chain Type**（安全链类型）。
   - 选择 **Flow Direction**（流向）。

     您的网络拓扑决定了使用单向流还是双向流。使用任一方法的性能大致相同。

     要使用一个防火墙接口同时将 c2s 和 s2c 会话流转发到安全链，并使用另一个防火墙接口接收从安全链返回的这两个会话流，请选择 **Unidirectional**（单向）。

     要使用接口 **1** 将 c2s 流转发到安全链并接收来自安全链的 s2c 流，同时使用接口 **2** 将 s2c 流转发到安全链并接收来自安全链的 c2s 流，请选择 **Bidirectional**（双向）。
   - 指定网络数据包代理转发接口对接口 **1** 和接口 **2**。必须已启用两个接口才能使用网络数据包代理（请参阅第 1 步）。在配置哪个接口是接口 **1**，哪个接口是接口 **2** 时，请注意流向。

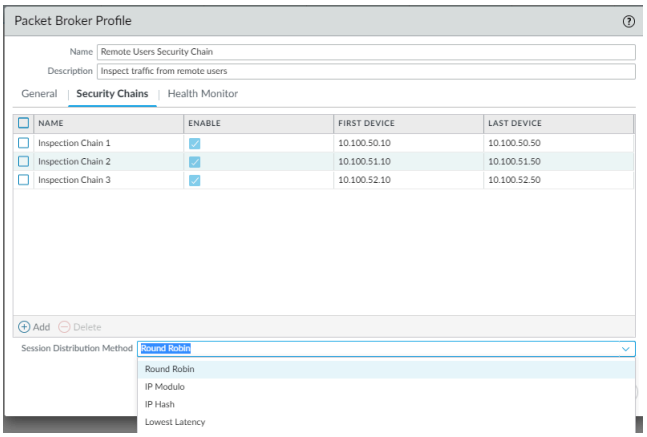


会话分发（负载均衡）仅适用于新会话。防火墙不会在会话中间重新均衡流量。防火墙只会将会话分发到状态为 “*up*”（活动状态、运行状况良好）的安全链。

4. 在 **Security Chains**（安全链）选项卡中，**Add**（添加）要连接的每个第 3 层路由安全链中第一个和最后一个设备的 IP 地址。您必须至少指定一个安全链，否则防火墙无法将流量路由到安全链并且您无法保存配置文件。

   如果指定多个第 3 层路由安全链，则还需要在防火墙与安全链之间放置正确配置的路由器、交换机或类似设备以执行正确的路由。此外，指定 **Session Distribution Method**（会话分发方法）以在安全链之间负载均衡流量。

 ©2024 Palo Alto Networks, Inc.



5. 在 **Health Monitor**（运行状况监控）选项卡中：

   - 选择您要执行的运行状况监控类型，以便您可以控制在安全链出现故障时发生的情况。

     您可以从 **Path Monitoring**（路径监控）、**HTTP Monitoring**（**HTTP** 监控）和 **HTTP Monitoring Latency**（**HTTP** 监控延迟）中选择一项、两项或全部。

     Path Monitoring（路径监控）—使用 ping 检查设备连接。

     HTTP Monitoring（**HTTP** 监控）—检查设备可用性和响应时间。

     HTTP Monitoring Latency（**HTTP** 监控延迟）—检查设备处理速度和效率。当您选择此选项时，也会自动启用 **HTTP Monitoring**（**HTTP** 监控）。

   - 启用一种或多种类型的运行状况监控会激活 **On Health Check Failure**（运行状况检查失败）选项，该选项确定防火墙在出现安全链运行状况故障时如何处理安全链流量。

     如果在一组第 3 层路由网络数据包代理接口上配置多个安全链，则在一个安全链发生故障时，流量将故障转移到其余运行状况良好的安全链。如果没有可用于处理故障转移流量的安全链，防火墙将采取 **On Health Check Failure**（运行状况检查失败）中配置的操作。选项包括 **Bypass Security Chain**（绕过安全链）和 **Block Session**（阻止会话）。

     Bypass Security Chain（绕过安全链）—防火墙将流量转发到其目的地而不是安全链，并将任何配置的安全配置文件和保护应用于流量。

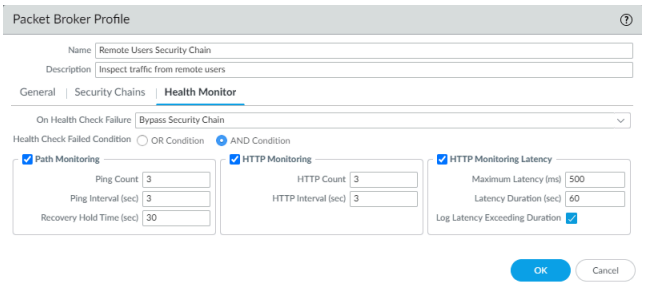
     Block Session（阻止会话）—防火墙会阻止会话。

     您选择的方法取决于当无法运行流量通过安全链时您希望如何处理流量。

   - 如果您选择多个运行状况检查选项，请选择是当任何一个监控选项记录失败条件时（**OR Condition**（**OR** 条件））还是仅当所有选定监控选项都记录失败条件（**AND Condition**（**AND** 条件））时，防火墙将运行状况检查视为失败（**Health Check Failed Condition**（运行状况检查失败条件））。例如，如果您启用全部三个运行状况检查选项，且其中一个选项记录到失败条件，则当您选择 **OR Condition**（**OR** 条件）时，防火墙会视为安全链连接失败并执行您在 **On Health Check Failure**（运行状况检查失败）中指

 ©2024 Palo Alto Networks, Inc.

定的操作。如果您选择 **AND Condition**（**AND** 条件），防火墙仍会视为连接运行状况良好，因为其中两个运行状况指标仍然正常。

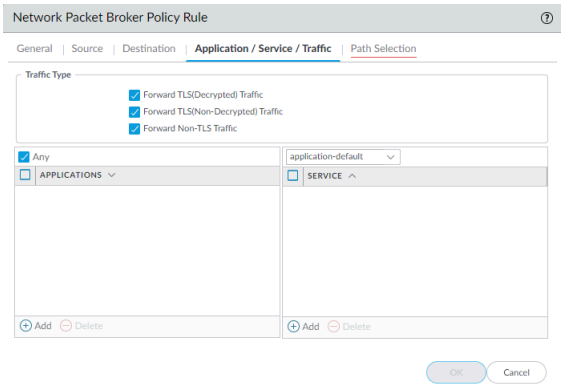


6. 单击 **OK**（确定）保存配置文件。

STEP 3 | 配置数据包代理策略以定义要转发到第 3 层路由安全链的流量。

1. 选择 **Policies**（策略） > **Network Packet Broker**（网络数据包代理），然后 **Add**（添加）新的策略规则或修改现有的策略规则。
2. 在 **General**（常规）选项卡中，为策略规则指定 **Name**（名称）和 **Description**（说明），以便您轻松识别其用途、添加 **Audit Comment**（审核注释）并应用标签（如有使用）。
3. 在 **Source**（源）选项卡中，确定您希望规则转发到安全链的流量的源区域、IP 地址、用户和设备。
4. 在 **Destination**（目标）选项卡中，确定您希望规则转发到安全链的流量的目标区域、IP 地址和设备。
5. 在 **Application/Service/Traffic**（应用程序/服务/流量）选项卡中，确定您希望规则转发到安全链的应用程序和服务。除非您希望规则控制应用程序使用非标准端口（例如内部自定义应用程序），否则最佳做法是将 **Service**（服务）设置为 **Application Default**（应用程序默认值），以便阻止使用非标准端口表现出规避行为的应用程序。

   对于 **Traffic Type**（流量类型），选择您希望规则转发到安全链的所有流量类型。**Forward TLS(Decrypted) Traffic**（转发 **TLS**（解密）流量）是默认选择。您可以选择 **Forward TLS(Decrypted) Traffic**（转发 **TLS**（解密）流量）、**Forward TLS(Non-Decrypted)**（转发 **TLS**（非解密）流量）和 **Forward Non-TLS Traffic**（转发非 **TLS** 流量）的任意组合以转发到安全链。



6. 在 **Path Selection**（路径选择）选项卡中，选择您在第 2 步中创建的数据包代理配置文件或创建一个新配置文件，以控制如何将策略规则控制的流量发送到安全链。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 如果要创建使用不同专用防火墙接口对的单独第 3 层路由安全链，请重复第 1 步到第 3 步以创建更多网络数据包代理安全链。用作网络数据包代理转发接口的两个第 3 层以太网接口必须专用于安全链，不能用于任何其他用途或承载任何其他流量。

 ©2024 Palo Alto Networks, Inc.

网络数据包代理 HA 支持

除了数据包代理配置文件中可用于防止安全链故障的路径和延迟运行状况监控外，您还可以对具有网络数据包代理转发接口的防火墙配置 High Availability（高可用性）(HA) 以防止防火墙故障。配置路径监控和 HA 不仅可防止安全链故障，还能防止防火墙故障。

网络数据包代理支持主动/被动 HA 对。主动/主动 HA 对不受支持，因为必须在数据包代理配置文件中指定专用代理转发接口。

发生故障转移后，解密 SSL 流量会被重置，因为 SSL 状态未在 HA 节点之间同步。如果正确同步了会话并正确重新获悉了 TCP 序列，则明文流量会恢复。

©2024 Palo Alto Networks, Inc.

网络数据包代理的用户界面更改

网络数据包代理取代了 PAN-OS 8.1 中引入的解密代理功能，并将其功能扩展至包括将非解密 TLS 流量和非 TLS 流量以及解密 TLS 流量转发到安全链。为了支持网络数据包代理，PAN-OS 11.1 用户界面进行了以下更改：

- 新策略（**Policies**（策略） > **Network Packet Broker**（网络数据包代理））使您可以配置要转发到安全链的特定流量，并附加数据包代理配置文件以控制如何将指定的流量转发到安全链。

  解密代理使用解密策略规则仅将解密 *TLS* 流量转发到安全链。而采用新的网络数据包代理策略规则，您不仅可以选择解密 *TLS* 流量，还可以选择加密 *TLS* 流量和非 *TLS* 流量。

- 新配置文件（**Objects**（对象） > **Packet Broker Profile**（数据包代理配置文件））取代了旧的配置文件（**Objects**（对象） > **Decryption**（解密） > **Decryption Broker Profile**（解密代理配置文件）），并使您能够准确配置如何将流量转发到安全链并监控路径和延迟运行状况。在 **General**（常规）选项卡中，输入专用防火墙网络数据包代理转发接口对的字段名称分别从“主接口”和“辅助接口”更改为 **Interface #1**（接口 **1**）和 **Interface #2**（接口 **2**）。
- 选择 **Policies**（策略） > **Network Packet Broker**（网络数据包代理）后，可以在 **Policy Optimizer**（策略优化器）中选择任何 Rule Usage（规则使用）选项，以查看网络数据包代理策略使用信息。**Rule Usage**（规则使用）统计信息可帮助您评估是需要保留未使用的网络数据包代理规则，还是可以删除这些规则并加强规则库以减少攻击面。
- 网络数据包代理取代了解密代理，因此解密策略不再处理到安全链的代理流量。因此，在 **Options**（选项）选项卡中，**Decrypt and Forward**（解密和转发）选项不再是策略可以执行的 **Action**（操作），并且 **Forwarding Profile**（转发配置文件）字段也被删除，因为现在只有解密配置文件对解密策略有效。
- 在 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）中，当您将 **Interface Type**（接口类型）设置为第 3 层然后选择 **Advanced**（高级）选项卡时，启用接口作为网络数据包代理转发接口的复选框名称将从“解密转发”更改为 **Network Packet Broker**（网络数据包代理）。
- 对于 **Device**（设备） > **Admin Roles**（管理员角色），在 **Web UI** 选项卡中，发生了以下两处更改：
  - 在 **Policies**（策略）下，您现在可以配置 **Network Packet Broker**（网络数据包代理）管理员角色权限。
  - 在 **Objects**（对象）下，**Decryption**（解密） > **Forwarding Profile**（转发配置文件）选项已删除，并替换为管理员角色权限的 **Packet Broker Profile**（数据包代理配置文件）选项。
- 在防火墙上，对于 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告），当您从详细日志中选择 **Traffic Log**（流量日志）作为 **Database**（数据库）时，您现在可以在 **Available Columns**（可用列）列表中选择 **Forwarded to Security Chain**（已转发到安全链）。

  在 Panorama 上，对于 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告），当您从详细日志中选择 **Panorama Traffic Log**（**Panorama** 流量日志）作为 **Database**（数据库）时，您现在可以在 **Available Columns**（可用列）列表中选择 **Forwarded to Security Chain**（已转发到安全链）。

 ©2024 Palo Alto Networks, Inc.

- 在流量日志中，“解密转发”列被重命名为 **Forwarded to Security Chain**（已转发到安全链）。在流量日志详细视图的 **Flags**（标志）部分中，“解密转发”复选框被重命名为 **Forwarded to Security Chain**（已转发到安全链）。
- 该功能的免费许可证从“解密代理”重命名为 **Packet Broker**（数据包代理）。如果您的防火墙上有免费解密代理许可证，则在升级到 PAN-OS 10.1 时，名称将自动更改。更改只体现在名称上，对功能没有影响。

 ©2024 Palo Alto Networks, Inc.

网络数据包代理的限制

大多数 Palo Alto Networks 平台都支持网络数据包代理，但有少部分不支持，还有少部分设有一些限制：

- Prisma Access 或 NSX 中不提供支持。
- AWS、Azure 和 GCP 仅支持第 3 层路由安全链。

网络数据包代理在 Panorama 上对托管防火墙设有一些限制，同时设有一些使用限制。在 Panorama 上：

- 如果将网络数据包代理许可证推送到托管防火墙，则必须重新启动防火墙才能安装许可证和关联的用户界面元素。
- 您无法在 **Shared**（共享）上下文中创建数据包代理配置文件，因为您在数据包代理配置文件中配置了特定接口。
- 不同的设备组不能共享相同的数据包代理配置文件。
- Panorama 无法将网络数据包代理配置（网络数据包代理策略规则和配置文件）推送到包含运行早于 10.1 的 PAN-OS 版本的防火墙的设备组。

  如果要在包含运行多个 PAN-OS 版本的防火墙的设备组中使用网络数据包代理，并且其中一些防火墙运行的 PAN-OS 版本早于 10.1，则必须将 11.1 之前的防火墙升级到 PAN-OS 11.1 或从设备组中删除 11.1 之前的防火墙，然后再推送网络数据包代理配置。

  您可以使用 *Panorama* 将附加到解密策略规则的数据包代理配置文件推送到安装了解密代理许可证的 *10.1* 之前的防火墙。对规则（***Options***（选项）选项卡）的 ***Action***（操作）必须是 ***Decrypt and Forward***（解密和转发），并且您必须将数据包代理配置文件附加到规则（***Options***（选项）选项卡中的 ***Decryption Profile***（解密配置文件）设置）。*11.1* 之前的防火墙使用数据包代理配置文件作为解密代理的解密转发配置文件。解密策略规则确定防火墙应用配置文件的流量。

  解密策略规则控制的流量必须是解密 *SSL* 流量（解密代理不支持加密 *SSL* 流量或明文流量）。
- 当您从 PAN OS 10.0 升级到 PAN OS 10.1 时，只有用于解密代理的本地解密策略规则才会迁移到网络数据包代理规则。从 Panorama 推送到防火墙的解密代理策略规则会在 Panorama 上自动迁移，但不会在防火墙上自动迁移。在防火墙本地配置的解密代理策略规则仅迁移到该防火墙上的网络数据包代理规则。对于在 Panorama 上配置的规则，Panorama 必须向防火墙执行另一个提交推送，以同步已迁移到 Panorama 上的网络数据包代理规则的解密代理规则。
- 当您从 PAN-OS 11.1 降级到 PAN-OS 10.0 时，网络数据包代理规则会自动删除。

网络数据包代理也设有一些使用限制：

©2024 Palo Alto Networks, Inc.

- 如果网络数据包代理防火墙也执行源网络地址转换 (SNAT) 并且流量是明文流量，则防火墙对流量执行 NAT 并将流量转发到安全链。安全链设备只能看到 NAT 地址，看不到原始源地址：

  1. 防火墙对客户端的流量执行 NAT。
  2. 防火墙将流量转发到安全链，并且任何路由都必须基于 NAT 地址。
  3. 由于数据包中的源地址现在是 NAT 地址，因此安全链设备只能看到 NAT 地址。它们看不到实际的客户端源地址。
  4. 当安全链将流量转发回防火墙时，防火墙不知道用户是谁。

  您可以通过检查会话的流量日志并将数据包与这些日志相关联来找出该会话的源用户是谁。流量日志包括原始源地址（您可以据此确定源用户）和 SNAT 地址。

  您可以通过在防火墙以外的设备上执行 *NAT* 来避免这种情况。

- 不支持解密 SSH、组播和广播流量。
- 使用 RSA 证书时，SSL 入站检查不支持客户端身份验证。
- 在第 1 层透明桥接模式下，如果安全链出现故障，则不会发生故障转移，因为当您使用透明桥接连接时，每对专用网络数据包代理防火墙接口仅连接到一个安全链。（您无法在第 1 层路由流量，您只能将其转发到下一个连接的设备。）
- 您只能在第 1 层透明桥接模式下转发 IPv6 流量。您无法在路由（第 3 层）模式下转发 IPv6 流量。
- 您不能将隧道或回环接口用作网络数据包代理接口。
- 网络数据包代理接口不能使用动态路由协议。
- 两个接口必须位于同一区域中。
- 安全链中的设备不能修改原始会话的源 IP 地址、目标 IP 地址、源端口、目标端口或协议，因为防火墙无法将修改后的会话与原始会话匹配，从而会丢弃流量
- 仅主动/被动 HA 防火墙对支持网络数据包代理的高可用性。主动/主动防火墙对不支持网络数据包代理的高可用性。
- SSL 流量不支持高可用性。SSL 会话在故障转移时重置。
- 当您从 PAN OS 10.0 升级到 PAN OS 10.1 时，用于解密代理的本地解密策略规则会迁移到网络数据包代理规则。
- 当您从 PAN-OS 11.1 降级到 PAN-OS 10.0 时，网络数据包代理规则会自动删除。

 ©2024 Palo Alto Networks, Inc.

对网络数据包代理进行故障排除

如果您在配置网络数据包代理时遇到问题，请检查以下项目：

- 防火墙配置：
  - 检查转发接口对上的下一跳路由，确保其指定了正确的设备接口。
  - 链设备和防火墙接口的 IP 地址，并确保在数据包代理配置文件中对其进行了正确输入。
  - 如果启用了 HA，请检查配置文件中是否指定了正确的接口。
  - 检查流量通过链的流向。
  - 确保配置文件注明了适当的安全链类型。
- 安全链配置；检查：
  - 安全链中每个设备的 IP 地址、下一跳地址和默认网关。
  - 防火墙与安全链之间任何设备（路由器、交换机等）的配置是否存在 IP 寻址、下一跳和默认网关配置错误。
  - 防火墙与链之间的路径。
- 检查防火墙流量日志以验证您是否看到了为代理流量设置的预期“转发”标志。
- 有用的 CLI 命令包括：
  - `show rulebase network-packet-broker`
  - `show running network-packet-broker status`
  - `show running network-packet-broker statistics`
  - `show running application-cache all`
  - `show running application setting`—确认已启用 App-ID 缓存并且该缓存用于 App-ID，检查缓存阈值设置等

 ©2024 Palo Alto Networks, Inc.

高级路由

PAN-OS® 提供了一个高级路由引擎，允许防火墙进行扩展，并为大型数据中心、ISP、企业和云用户提供稳定、高性能和高可用性的路由功能。高级路由引擎通过基于标准的配置简化了操作，由于它与其他路由器供应商的配置类似，因此可以缩短您的学习曲线。协议配置配置文件和粒度筛选配置文件可跨多个逻辑路由器和虚拟系统工作。路由重新分发通过重新分发配置文件得以简化。BGP对等组和对等体可以继承配置，使BGP更加灵活。

高级路由引擎支持静态路由、BGP、MP-BGP、OSPFv2、OSPFv3、RIPv2、IPv4多播路由、BFD、重新分发、路由过滤到RIB、访问列表、前缀列表和路由映射。

使用 Advanced Routing Engine Migration Reference（高级路由引擎迁移参考）来规划从旧版路由引擎的迁移，并查看旧版和高级路由引擎之间的区别以及例外情况。

以下型号支持高级路由引擎：

- PA-7000 系列
- PA-5400 系列
- PA-5200 系列
- PA-3400 系列
- PA-3200 系列
- PA-1400 系列
- PA-400 系列
- CN-系列
- VM-SERIES
- M-700设备
- M-600 设备
- M-500 设备
- M-300设备
- M-200 设备

了解高级路由配置文件，并执行以下任务来配置高级路由：

- 启用高级路由
- 逻辑路由器概述
- 配置逻辑路由器
- 创建静态路由
- 在高级路由引擎上配置 BGP
- 创建 BGP 路由配置文件
- 为高级路由引擎创建筛选器
- 在高级路由引擎上配置 OSPFv2

- 创建 OSPF 路由配置文件
- 在高级路由引擎上配置 OSPFv3
- 创建 OSPFv3 路由配置文件
- 在高级路由引擎上配置 RIPv2
- 创建 RIPv2 路由配置文件
- 创建 BFD 配置文件
- 配置 IPv4 组播
- 配置 MSDP
- 创建多播路由配置文件
- 创建 IPv4 MRoute

 ©2024 Palo Alto Networks, Inc.

启用高级路由

尽管受支持的防火墙可同时拥有使用旧版路由引擎的配置和使用高级路由引擎的配置，但一次只有一个路由引擎有效。每次更改防火墙将使用的引擎（启用或禁用高级路由以分别访问高级引擎或旧版引擎）时，必须提交配置并重新启动防火墙才能使更改生效。

在切换到高级路由引擎之前，请备份当前的配置。

同样地，如果您使用启用或禁用了高级路由的模板配置 Panorama，则在提交并将模板推送到设备后，您必须重新启动模板中的设备才能使更改生效。

配置 *Panorama* 时，为所有使用相同高级路由设置（全部启用或全部禁用）的设备创建设备组和模板。*Panorama* 不会将启用了高级路由的配置推送到不支持高级路由的低端防火墙。对于这些防火墙，*Panorama* 将推送旧版配置（如有）。

高级路由引擎支持多个逻辑路由器（在旧版路由引擎上称为虚拟路由器）。具体支持的逻辑路由器数量取决于防火墙型号，并且与旧版路由引擎支持的虚拟路由器数量相同。例如，高级路由引擎具有更便捷的菜单选项，并且您可以在配置文件（身份验证、计时器、地址系列或重新分发配置文件）中轻松配置很多应用于 BGP 对等组或对等体的设置。高级路由引擎上还有很多静态路由、OSPF、OSPFv3、RIPv2、组播和 BFD 设置。

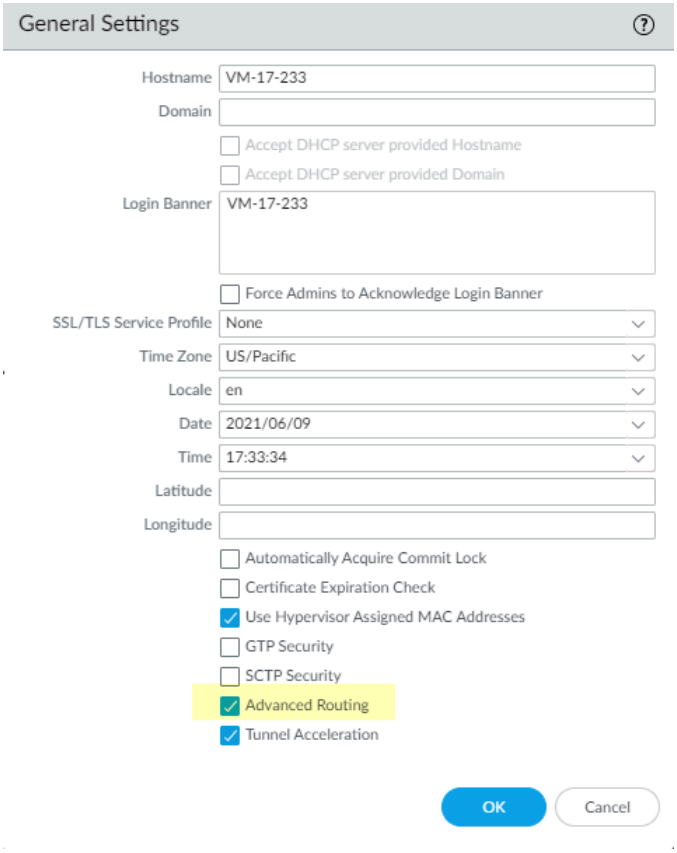
高级路由引擎支持 RIB 筛选，这意味着您可以创建路由映射来匹配静态路由或从其他路由协议接收的路由，从而筛选在 RIB 中为逻辑路由器安装的路由。该功能适用于 RIB 或 FIB 容量较小的防火墙；您仍然可以传播必要的路由更新，而无需使用其他地方需要的内存。

STEP 1 | 在启用高级路由之前备份当前的配置。

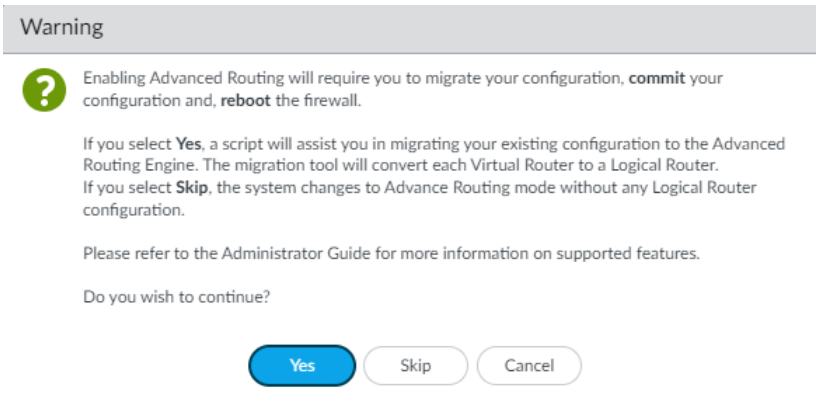
 ©2024 Palo Alto Networks, Inc.

STEP 2 | 启用高级路由引擎。

1. 选择 **Device**（设备） > **Setup**（设置） > **Management**（管理），然后编辑“General Settings（常规设置）”。
2. 启用 **Advanced Routing**（高级路由）。



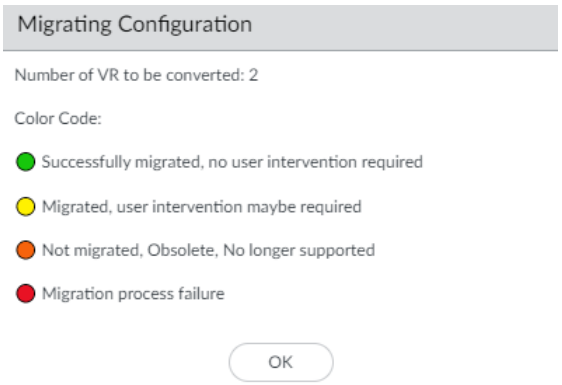
3. 单击确定之前，请确保已备份旧版路由引擎的配置。
4. 单击 **OK**（确定）。
5. 出现警告：



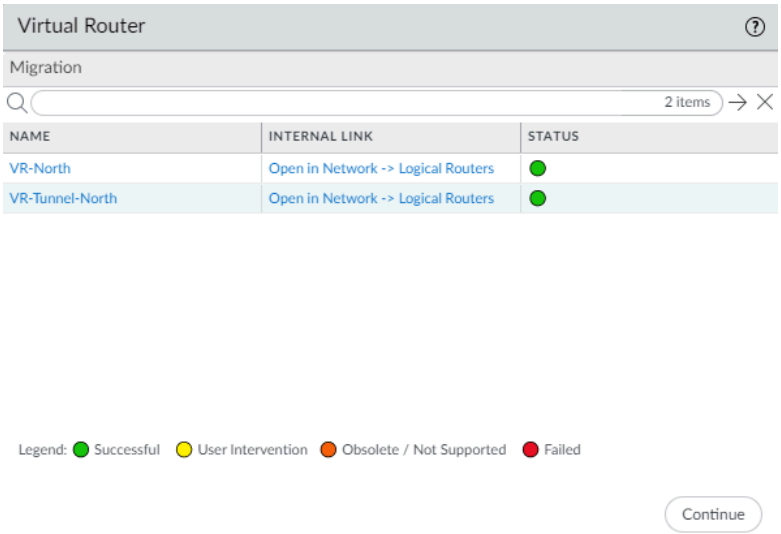
选择 **Yes**（是），让迁移脚本将每个虚拟路由器转换为逻辑路由器，并将您的配置迁移到高级路由引擎。选择 **Skip**（跳过）以使用空白配置重启系统。选择 **Cancel**（取消）以取消启用高级路由的进程。

6. 单击 **OK**（确定）以批准迁移。

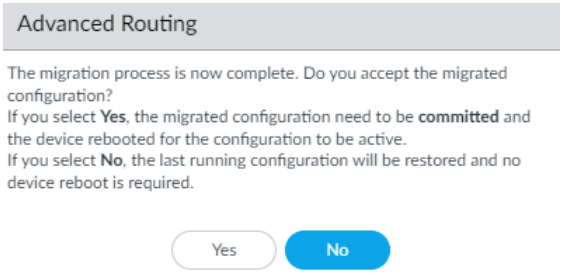
 ©2024 Palo Alto Networks, Inc.



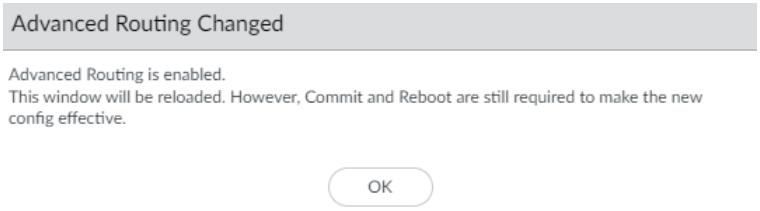
7. 列出了虚拟路由器、逻辑路由器的链接及其颜色编码状态。解决所有需要用户干预的问题。选择 **Continue**（继续）



8. 单击 **Yes**（是）以接受迁移的配置。



9. （PAN-OS 11.0.2 以及更高版本 11.1）单击 **OK**（确定）。



 ©2024 Palo Alto Networks, Inc.

10. 选择 **Commit**（提交）进行提交，然后选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后选择 **Reboot Device**（重启设备）。然后重新登录防火墙。

    如果迁移不成功，请生成技术支持文件，登录 Palo Alto Networks 客户支持门户，并报告您的问题以获得有关产品的帮助。

11. （可选）成功迁移后，您可以使用 CLI 配置模式命令删除所有虚拟路由器：

    1. 访问 CLI。
    2. 执行以下命令以从旧路由引擎中移除所有配置：

    ```
    username@hostname# delete network virtual-router <vr-name>
    ```

    > 如果要更改逻辑路由器配置，则可以删除虚拟路由器，这会使虚拟路由器配置过时，从而导致提交失败。虽然删除虚拟路由器可以避免提交失败，但请注意，删除虚拟路由器也会永久移除旧路由引擎中的所有配置，并且您将无法恢复配置。

    3. 将更改提交到防火墙。

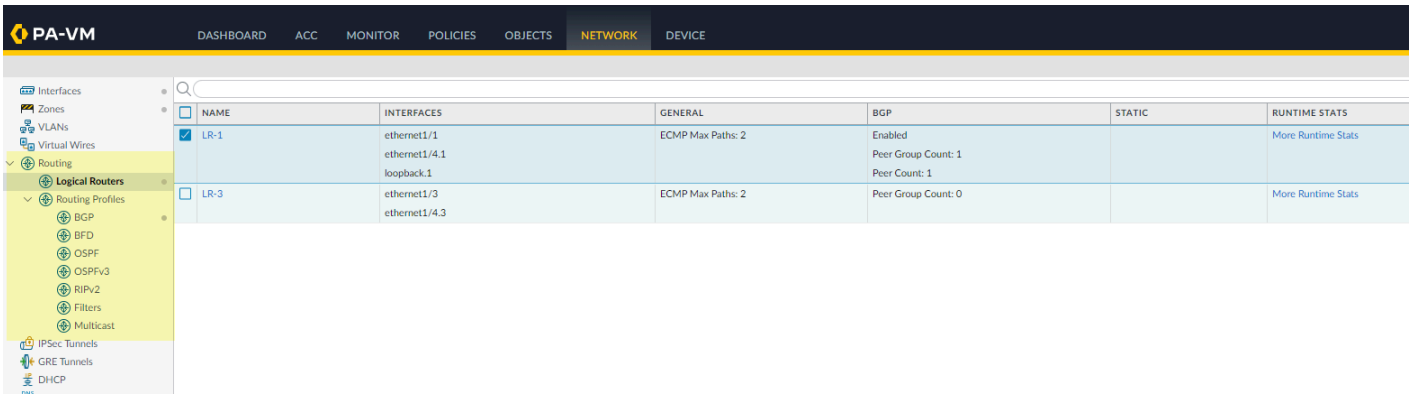
    ```
    username@hostname# commit
    ```

    > 在 *Panorama* 中进行配置时，您可以选择 ***Network***（网络） ***> Virtual Routers***（虚拟路由器）以删除所有虚拟路由器。提交更改并将其推送到相关防火墙，然后再继续。

STEP 3 | 重新登录防火墙。

STEP 4 | 选择 **Network**（网络）。

请注意菜单项，它们比旧版菜单上的单个项目（虚拟路由器）更符合行业标准并且更详细。**Routing**（路由）中包含 **Logical Routers**（逻辑路由器）和 **Routing Profiles**（路由配置文件），其中包括 **BGP**、**BFD**、**OSPF**、**OSPFv3**、**RIPv2**、**Filters**（筛选器）和 **Multicast**（多播）。

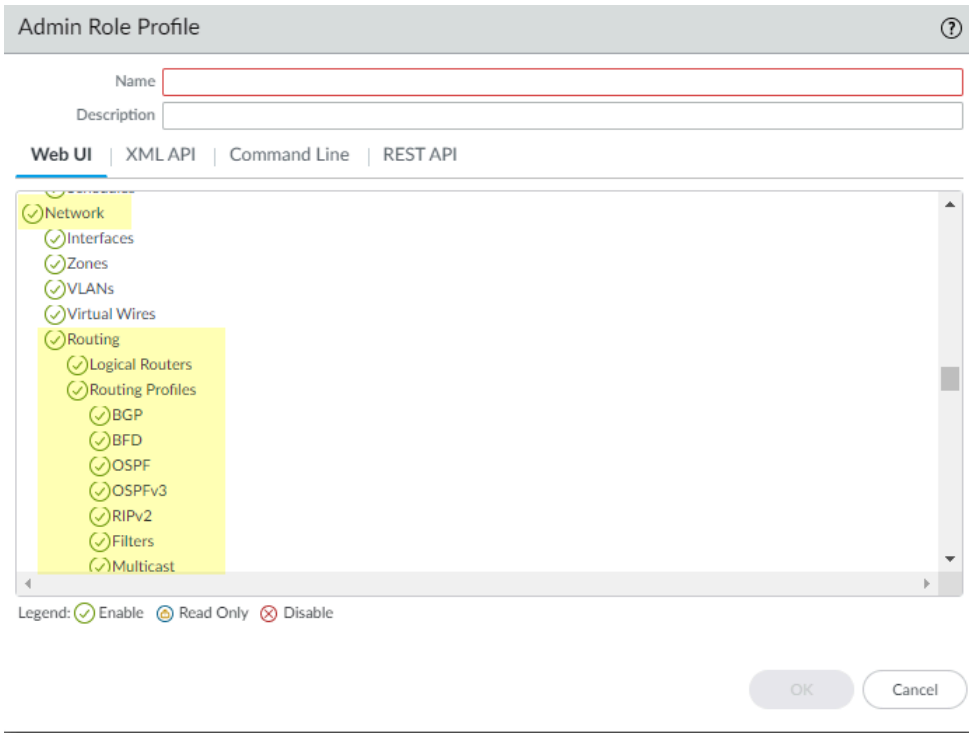


STEP 5 | 选择 **Interfaces**（接口），将一个或多个 Layer 3 interfaces（第 3 层接口）配置为静态 IP 地址或配置为 DHCPv4 客户端，以接收动态分配的地址。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | （可选）创建管理员角色配置文件，以控制对高级路由引擎的逻辑路由器和路由配置文件的精细访问。

1. 选择 **Device**（设备） > **Admin Roles**（管理员角色），然后按 **Name**（名称）**Add**（添加）管理员角色配置文件。
2. 选择 **Web UI**。
3. **Enable**（启用）、**Disable**（禁用）或选择 **Read Only**（只读）以下选项：**Network**（网络）、**Routing**（路由）、**Logical Routers**（逻辑路由器）、**Routing Profiles**（路由配置文件）、**BGP**、**BFD**、**OSPF**、**OSPFv3**、**RIPv2**、**Filters**（筛选器）和 **Multicast**（多播）（默认为启用）。



4. 单击 **OK**（确定）。
5. 为管理员分配角色。配置防火墙管理员帐户。

STEP 7 | **Commit**（提交）更改。

STEP 8 | 配置逻辑路由器以继续。

 ©2024 Palo Alto Networks, Inc.

逻辑路由器概述

防火墙使用逻辑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）来获取其他子网的第 3 层路由。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，逻辑路由器从 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逻辑路由器，则逻辑路由器可路由到同一防火墙内的其他逻辑路由器中。

您可以配置第 3 层接口来参与动态路由协议（BGP、OSPF、OSPFv3 或 RIP）以及添加静态路由。您还可以创建多个逻辑路由器，每个都用于维护不在逻辑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。

您可以在每个逻辑路由器中配置一个回环接口，在两个回环接口之间创建一个静态路由，然后配置一个动态路由协议在这两个接口之间对等，从而配置从一个逻辑路由器到另一个逻辑路由器的动态路由。防火墙仅支持在逻辑路由器之间有一个跃点。例如，对于逻辑路由器 A、B 和 C，路由不能从 A 到 B 再到 C，而必须直接从 A 到 C。

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逻辑路由器关联。虽然每个接口仅可属于一个逻辑路由器，但是可以为逻辑路由器配置多个路由协议和静态路由。无论是否为逻辑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。

 ©2024 Palo Alto Networks, Inc.

配置逻辑路由器

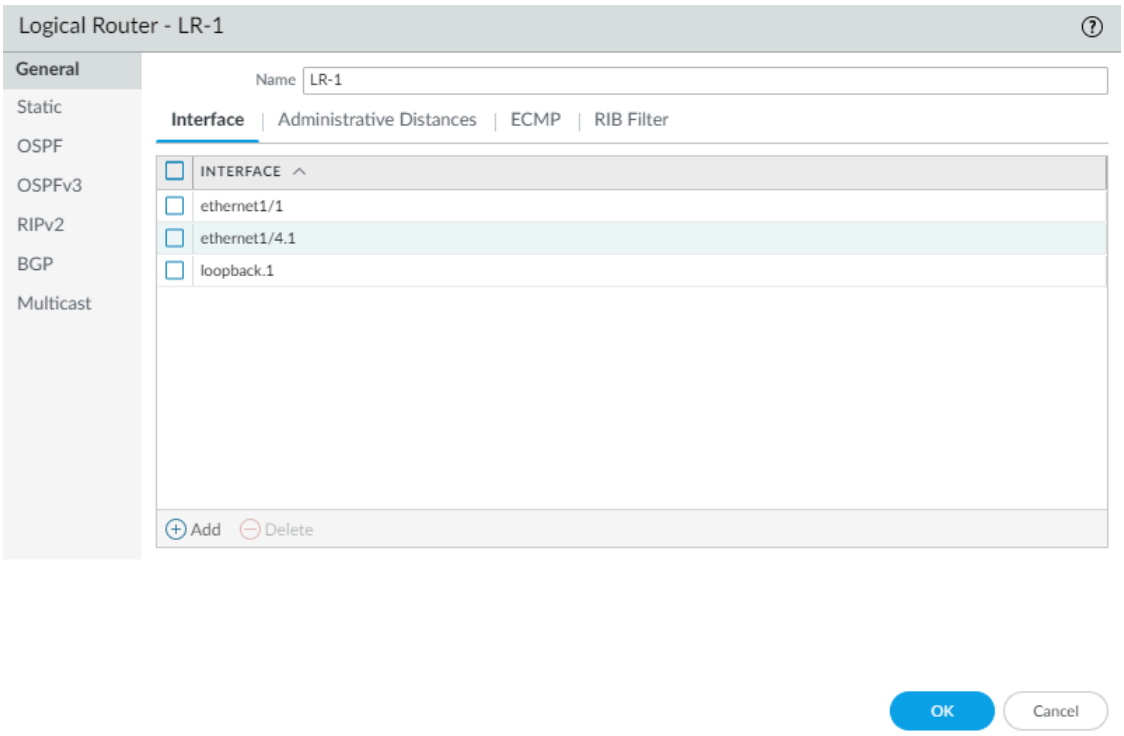
为了执行网络路由，高级路由引擎需要您至少配置一台逻辑路由器；默认没有逻辑路由器。逻辑路由器维护的是单独的路由信息库，防止将路由暴露给其他逻辑路由器。高级路由引擎支持的逻辑路由器数量因防火墙型号而异。

配置逻辑路由器前，必须先启用高级路由。

STEP 1 | 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后通过输入 **Name**（名称）（最多 31 个字符） **Add**（添加）逻辑路由器。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线(_)或连字符(-)组合而成。但不得包含句点(.)或空格。

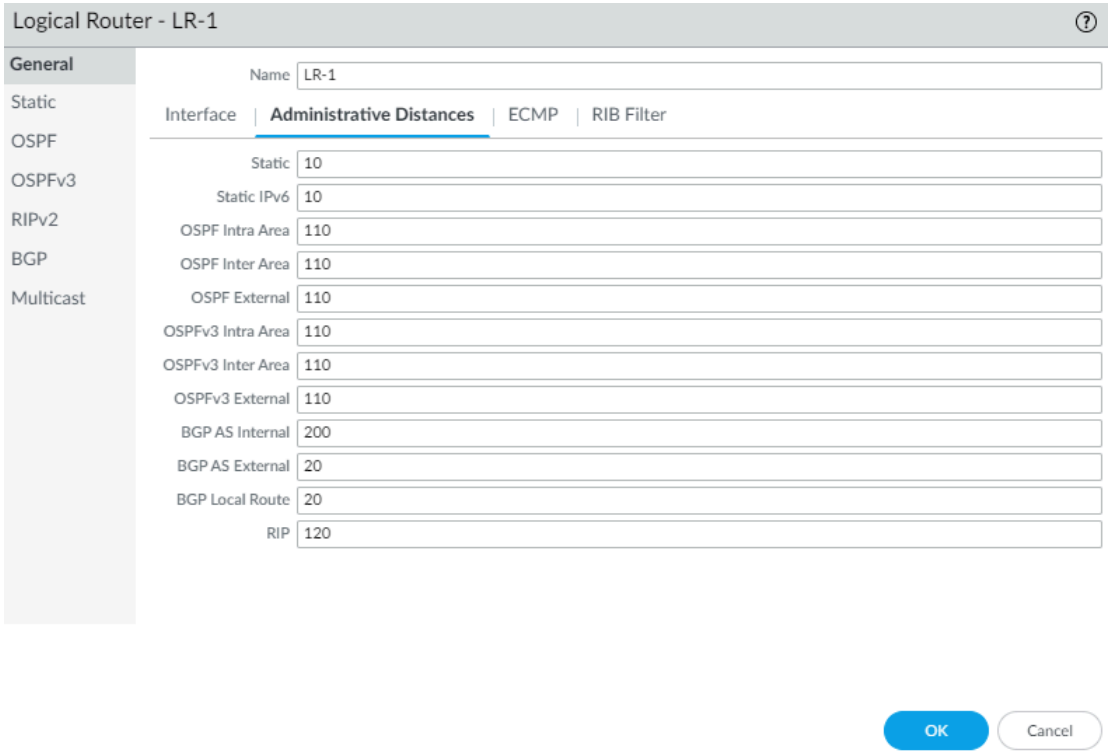
STEP 2 | 为辑路由器添加接口。

1. 在辑路由器的 **General**（常规）选项卡中，选择 **Interface**（接口）选项卡。
2. 从接口列表中选择接口，将接口 **Add**（添加）到逻辑路由器。每个接口只能属于一个逻辑路由器。要想添加更多接口，重复上述步骤即可，如下面列出的为名称为 LR-1 的逻辑路由器添加接口的示例：



 ©2024 Palo Alto Networks, Inc.

STEP 3 | （可选）选择 **Administrative Distances**（管理距离）以更改各类路由的全局管理距离（默认设置）。



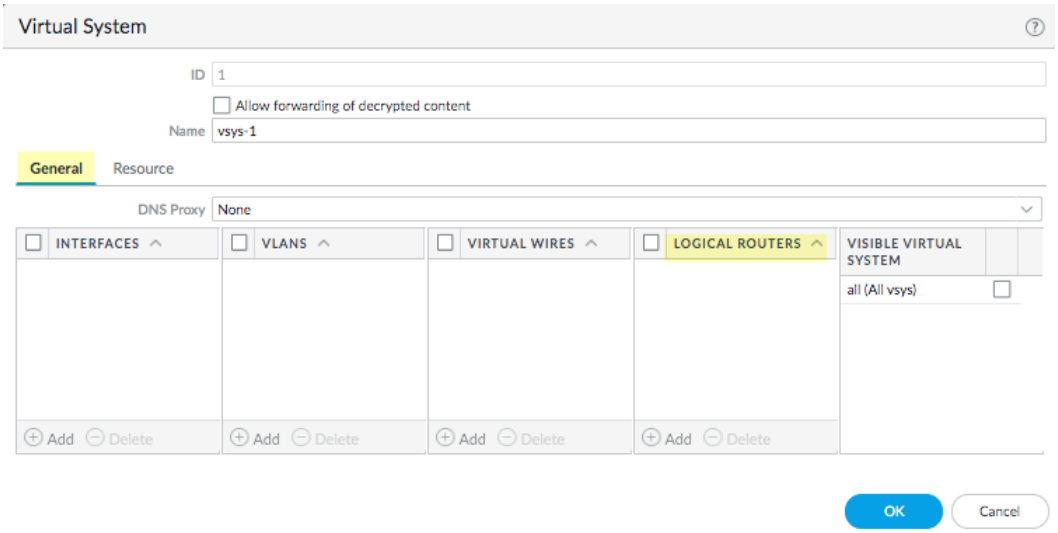
- **Static**（静态） — 范围为 1-255；默认为 10。
- **Static IPv6**（静态 **IPv6**） — 范围为 1-255；默认为 10。
- **OSPF Intra Area**（**OSPF** 区域内） — 范围为 1-255；默认为 110。
- **OSPF Inter Area**（**OSPF** 区域间） — 范围为 1-255；默认为 110。
- **OSPF External**（**OSPF** 外部）— 范围为 1-255；默认为 110。
- **OSPFv3 Intra Area**（**OSPFv3** 区域内） — 范围为 1-255；默认为 110。
- **OSPFv3 Inter Area**（**OSPFv3** 区域间） — 范围为 1-255；默认为 110。
- **OSPFv3 External**（**OSPFv3** 外部） — 范围为 1-255；默认为 110。
- **BGP AS Internal**（**BGP AS** 内部）— 范围为 1-255；默认为 200。
- **BGP AS External**（**BGP AS** 外部）— 范围为 1-255；默认为 20。
- **BGP Local Route**（**BGP** 本地路由） — 范围为 1-255；默认为 20。
- **RIP** — 范围为 1-255；默认为 120。

STEP 4 | 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | （在支持多个虚拟系统的防火墙上）将逻辑路由器分配给虚拟系统。

1. 选择 **Device**（设备） > **Virtual Systems**（虚拟系统），然后选择虚拟系统，最后选择 **General**（常规）。
2. 添加一个或多个**Logical Routers**（逻辑路由器）。
3. 单击 **OK**（确定）。



STEP 6 | 单击 **OK**（确定）。

STEP 7 | （可选）为逻辑路由器配置 ECMP：导航到 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），选择逻辑路由器，然后选择**General**（常规） > **ECMP**。为逻辑路由器配置 ECMP 的流程跟在传统路由引擎上配置虚拟路由器的流程基本一样。

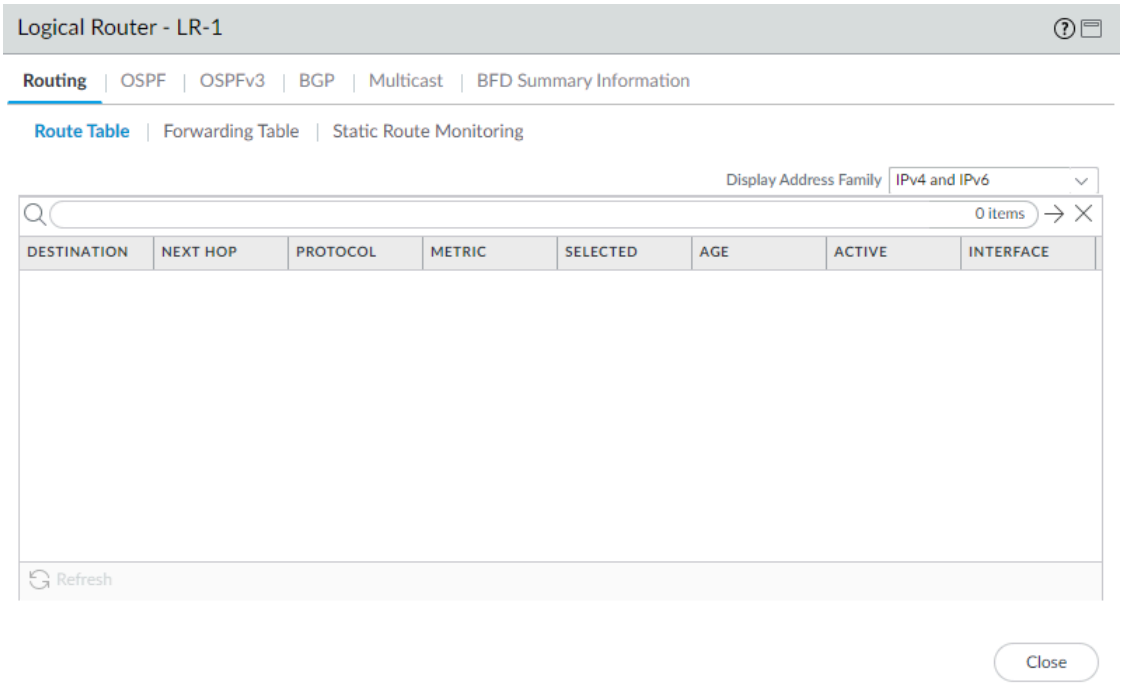
STEP 8 | **Commit**（提交）更改。

STEP 9 | 对于具有预先存在的配置的防火墙，选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作） 和 **Reboot Device**（重启设备）。然后重新登录防火墙。

 ©2024 Palo Alto Networks, Inc.

STEP 10 | （可选）查看逻辑路由器的运行时统计数据。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），对于特定的逻辑路由器，选择最右侧的 **More Runtime Stats**（更多运行时统计）。
2. 要查看所有协议的路由表，请在 **Routing**（路由）选项卡中选择 **Route Table**（路由表）和 **Display Address Family**（显示地址系列）：**IPv4 and IPv6**（**IPv4** 和 **IPv6**）、**IPv4 Only**（仅 **IPv4**）或 **IPv6 Only**（仅 **IPv6**）。



3. 要查看转发信息库 (FIB) 中的条目，请选择 **Forwarding Table**（转发表）。
4. 选择 **Static Route Monitoring**（静态路由监控）后可以查看正在监视的静态路由。
5. 选择 **BGP** 选项卡，然后选择 **Summary**（摘要），以查看 BGP 设置。
6. 选择 **Peer**（对等）以查看 BGP 对等设置。
7. 选择 **Peer Group**（对等组）以查看 BGP 对等组设置。
8. 选择 **Route**（路由）和 **Display Address Family**（显示地址系列）：**IPv4 and IPv6**（**IPv4** 和 **IPv6**）、**IPv4 Only**（仅 **IPv4**）或 **IPv6 Only**（仅 **IPv6**）以查看 BGP 路由的属性。

STEP 11 | 访问 CLI 以查看高级路由信息。PAN-OS CLI 快速入门指南在 CLI 速查表中列出了以下命令：Networking（下一步：网络）。

 ©2024 Palo Alto Networks, Inc.

创建静态路由

为高级路由引擎中的逻辑路由器创建静态路由。

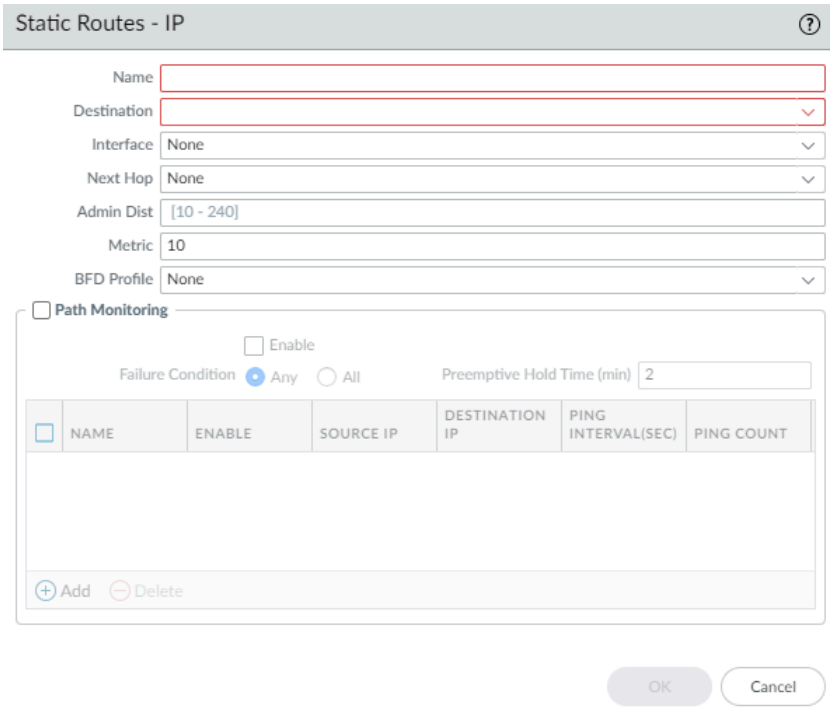
STEP 1 | 配置逻辑路由器.

STEP 2 | 创建静态路由。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择相应逻辑路由器。
2. 选择 **Static**（静态）并按 **Name**（名称）（最多 63 个字符）**Add**（添加）**IPv4** 或 **IPv6** 静态路由。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 对于 **Destination**（目标），输入路由和子网掩码（例如，192.168.2.0/24 用于 IPv4 地址或 2001:db8:123:1::0/64 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）。您也可以选择或创建 IP 网络掩码类型的地址对象。
4. 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。指定此接口来更严格控制防火墙使用的接口，而不是使用路由表中用于此静态路由下一个跃点的接口。
5. 对于 **Next Hop**（下一个跃点），请选择以下选项之一：
   - **IP Address**（**IP** 地址）或 **IPv6 Address**（**IPv6** 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 LR**（下一个 **LR**）— 选择此选项可使逻辑路由器列表中的下一个逻辑路由器成为下一个跃点。
   - **FQDN** — 输入完全限定域名。
   - **Discard**（丢弃）— 选择是否要丢弃发往此目标的数据包。
   - 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。
6. 输入静态路由的 **Admin Dist**（管理距离）（范围为 10 - 240；默认为10）。此值将覆盖为逻辑路由器指定的 **Static**（静态）或 **Static IPv6**（静态 **IPv6**）管理距离。
7. 输入静态路由的 **Metric**（指标）（范围为 1 - 65,535；默认为 10）。

©2024 Palo Alto Networks, Inc.

8. （可选）如果要使用 BFD，请选择所创建的 **BFD Profile**（**BFD** 配置文件），或选择默认默认配置文件，或创建一个 BFD 配置文件，以应用于静态路由；默认值为 **None (Disable BFD)**（无（禁用**BFD**））。



STEP 3 | （可选）为静态路由配置路径监视；您最多可以监控 128 条静态路由。

1. 选择 **Path Monitoring**（路径监视），以允许配置路径监视（默认为禁用）。
2. **Enable**（启用）路径监视（默认为禁用）。
3. **Failure Condition**（故障条件）确定静态路由的路径监视是基于其中一个（任何）还是所有受监视目标。选择如果 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指标且指向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。

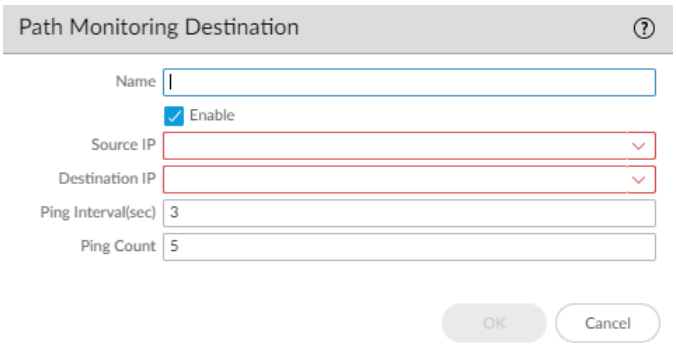
4. （可选）指定 **Preemptive Hold Time (min)**（抢占保持时间（分钟）），这是在防火墙将静态路由重新安装到 RIB 之前，停用的路径监视必须保持在激活状态的分钟数；范围为 0

 ©2024 Palo Alto Networks, Inc.

- 1,440；默认为 2。如果设置为零(0)，则防火墙会在路径监视激活时将路由立即重新安装到 RIB 中。

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。如果链路在保持时间内断开或翻动，当链路恢复时，路径监视器将恢复，抢占保持时间将重置，从而使计时器从零重新开始计时。

5. 按 **Name**（名称）**Add**（添加）路径监视目标。



6. **Enable**（启用）路径监视目标。
7. 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。
8. 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）。

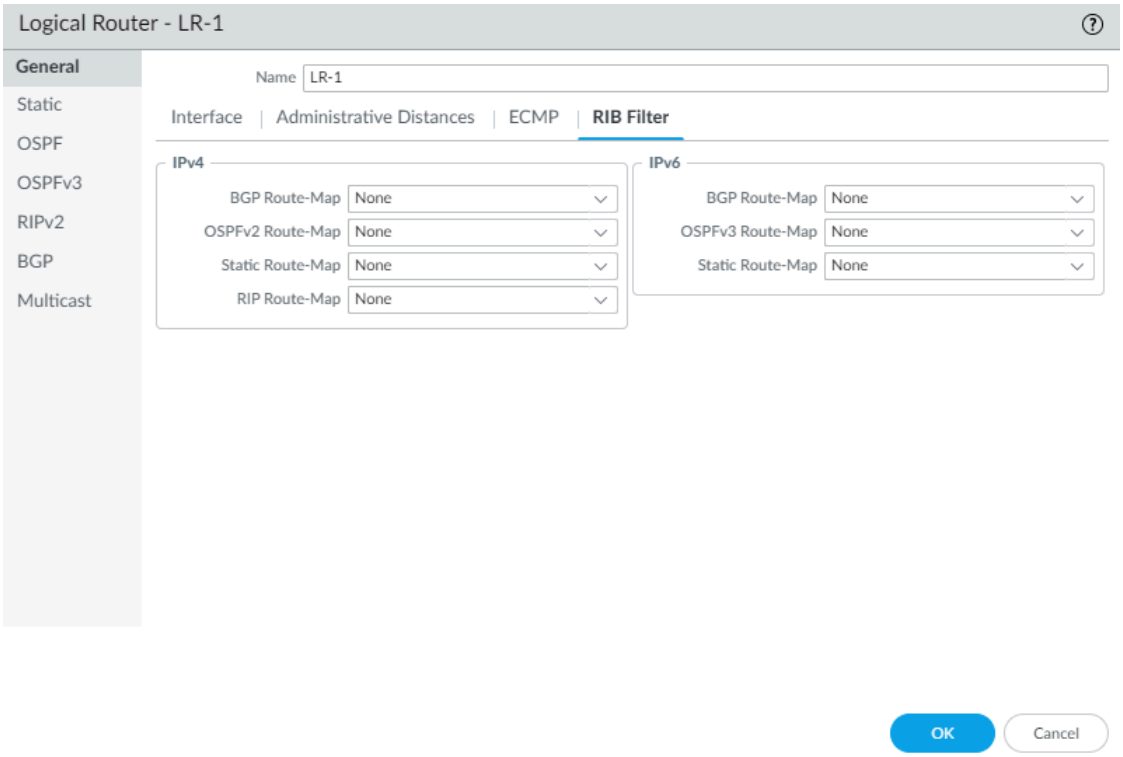
   目标 *IP* 地址应属于可靠的端点；不得对本身不稳定或不可靠的设备进行路径监视。
9. （可选）指定 ICMP **Ping Interval (sec)**（**Ping** 间隔（秒））（以秒为单位），以确定防火墙监控路径的频率（范围为 1 - 60；默认为 3）。
10. （可选）在防火墙认为静态路由出现故障并将其从 RIB 和 FIB 中删除之前，指定不从目标返回的数据包的 ICMP **Ping Interval (sec)**（**Ping** 间隔（秒））（范围为 3 - 10；默认为 5）。
11. 单击 **OK**（确定），以保存路径监视目标。
12. 单击 **OK**（确定）两次，以保存静态路由。

©2024 Palo Alto Networks, Inc.

STEP 4 | （可选）控制放置在全局 RIB 中的静态路由。

您可能会配置并重新分发静态路由，但不希望它们出现在协议的本地路由表或全局 RIB 中。您可能只想向全局 RIB 添加特定的静态路由。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择 **RIB Filter**（**RIB** 筛选器），以允许路由进入或阻止将路由添加到全局 RIB。



3. 要筛选 IPv4 静态路由和互联路由，对于 **Static Route-Map**（静态路由映射），请选择一个重新分发路由映射或新建一个。
4. 要筛选 IPv6 静态路由和互联路由，对于 **Static Route-Map**（静态路由映射），请选择一个重新分发路由映射或新建一个。
5. 单击 **OK**（确定）。

STEP 5 | （可选）更改逻辑路由器内静态 IPv4 和静态 IPv6 路由的默认管理距离。

STEP 6 | **Commit**（提交）更改。

STEP 7 | Access the CLI（访问 CLI）以查看静态路由路径监视器：**`show advanced-routing static-route-path-monitor`**。PAN-OS CLI 快速入门指南在 CLI 速查表中列出了其他命令：Networking（下一步：网络）。

 ©2024 Palo Alto Networks, Inc.

在高级路由引擎上配置 BGP

执行以下任务，为Advanced Routing Engine（高级路由引擎）上的逻辑路由器配置 BGP。

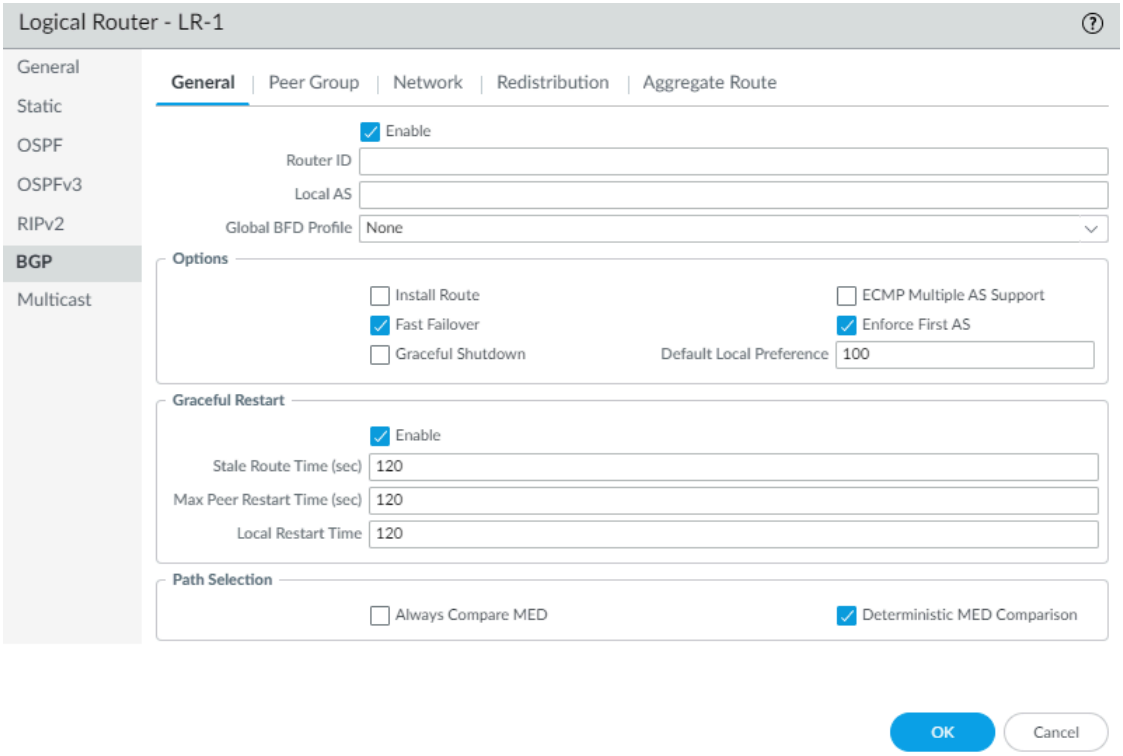
在配置 BGP 之前，请考虑大量可应用于 BGP 对等组、对等体、重新分发规则和聚合路由策略的有用路由配置文件和筛选器，从而节省配置时间并保持一致性。您可以提前或在配置 BGP 的过程中创建配置文件和筛选器。

STEP 1 | 配置逻辑路由器.

©2024 Palo Alto Networks, Inc.

STEP 2 | 启用 BGP 并配置 BGP 常规设置。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 为此逻辑路由器选择 **BGP** > **General**（常规），然后 **Enable**（启用）BGP。



3. 为逻辑路由器的 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。
4. 分配 **Local AS**（本地 **AS**），即逻辑路由器所属的 AS号；范围为 1 到 4,294,967,295。
5. 如果要将 BFD 应用于 BGP，对于 **Global BFD Profile**（全局 **BFD** 配置文件），选择所创建的 BFD 配置文件，或选择默认配置文件，或创建新的 BFD 配置文件；默认为**None (Disable BFD)**（无（禁用 **BFD**））。
6. 选择 **Install Route**（安装路由），将学习到的 BGP 路由安装到全局路由表中；默认为禁用。
7. 选择 **Fast Failover**（快速故障转移），让 BGP 在与相邻对等体的链路断开时终止与该对等体的会话，而无需等待 Hold Time（保持时间）终止；默认启用。
8. 选择 **Graceful Shutdown**（正常关机），让 BGP 在维护操作期间降低 eBGP 对等链路的优先级，以便 BGP 可以根据 RFC 8326 选择和传播替代路径；默认为禁用。
9. 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）；默认为禁用。
10. **Enforce First AS**（执行第一个 **AS**）后，促使防火墙丢弃来自 eBGP 对等体的传入更新数据包，而 eBGP 对等体未列出自己的 AS 编号作为 AS_PATH 属性中的第一个 AS 编号；默认为禁用。
11. 指定可用于确定不同路径之间首选项的 **Default Local Preference**（默认本地首选项）；范围为 0 - 4,294,967,295，默认为 100。

 ©2024 Palo Alto Networks, Inc.

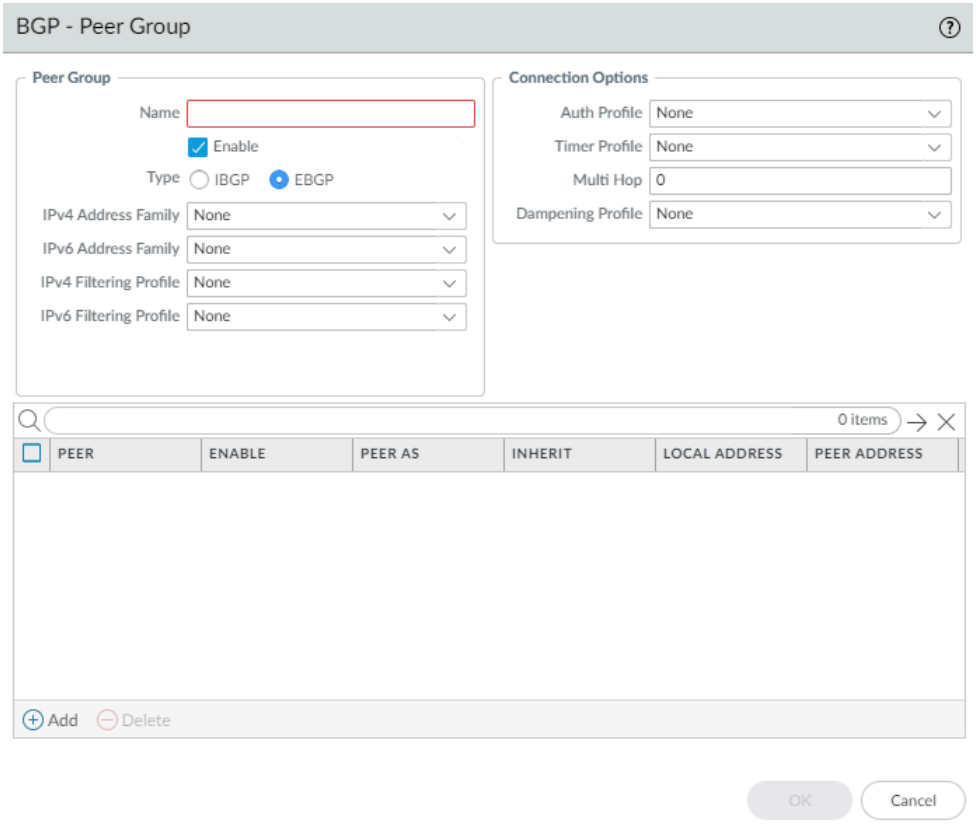
12. **Enable Graceful Restart**（启用正常重启）并配置以下计时器：
    - **Stale Route Time (sec)**（路由停滞时长（秒））— 指定路由可保持停滞状态的时长（以秒计，范围为 1-3,600，默认为 120）。
    - **Max Peer Restart Time (sec)**（最长对端重启时间（秒））— 指定本地设备接受的对端设备最长平滑重启时间（以秒计，范围是 1-3,600，默认为 120）。
    - **Local Restart Time**（本地重启时长）— 指定本地设备重启的时长（以秒计）。该值将被通告到对端（范围为 1-3,600，默认为 120）。
13. 对于 **Path Selection**（路径选择）：
    - **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；默认为禁用。
    - **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；默认为禁用。
14. 单击 **OK**（确定）。

STEP 3 | 配置 BGP 对端组。

1. 选择 > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择 **BGP** > **Peer Group**（对等组），然后按 **Name**（名称）**Add**（添加） BGP 对等组（最多 63 个字符）。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点(.)开头，

 ©2024 Palo Alto Networks, Inc.

可以包含字母数字字符、下划线、连字符和句点。不允许有空格。此名称在该逻辑路由器和所有逻辑路由器中必须唯一。



3. **Enable**（启用）对等组。
4. 选择对端组 **Type**（类型）：**IBGP** 或 **EBGP**。
5. 要为对等组指定多个 **IPv4 Address Family**（**IPv4** 地址系列） 选项，请选择所创建的 **AFI Profile**（**AFI** 配置文件）， 然后选择默认配置文件，或新建一个 BGP 地址系列配置文件；默认为 **None**（无）。
6. 要为对等组指定多个 **IPv6 Address Family**（**IPv6** 地址系列） 选项，请选择所创建的 **AFI Profile**（**AFI** 配置文件）， 然后选择默认配置文件，或新建一个 BGP 地址系列配置文件；默认为 **None**（无）。
7. 要将 **IPv4 Filtering Profile**（**IPv4** 筛选配置文件）选项应用于对等组，请选择所创建的 **BGP Filtering Profile**（**BGP** 筛选配置文件）或新建一个 BGP 筛选配置文件；默认为 **None**（无）。

   BGP Filtering Profile（BGP 筛选配置文件）描述了如何为 *IPv4* 配置多个 *BGP* 选项，例如导入或导出 *BGP* 路由、接受或阻止将路由添加到本地 *BGP RIB*、有条件地通告路由以及取消抑制受阻或汇总的路由。
8. 要将 **IPv6 Filtering Profile**（**IPv6** 筛选配置文件）选项应用于对等组，请选择所创建的 **BGP Filtering Profile**（**BGP** 筛选配置文件）或创建新的 BGP 筛选配置文件；默认为 **None**（无）。

 ©2024 Palo Alto Networks, Inc.

BGP Filtering Profile（BGP 筛选配置文件）描述了如何为 *IPv6* 配置多个 *BGP* 选项，例如导入或导出 *BGP* 路由、接受或阻止将路由添加到本地 *BGP RIB*、有条件地通告路由以及取消抑制受阻或汇总的路由。

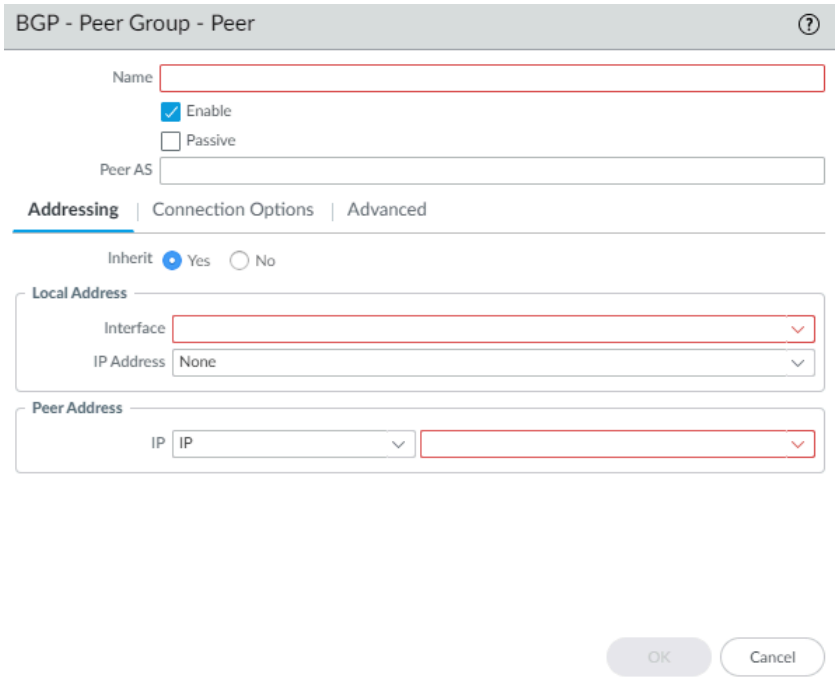
9. 对于连接选项，选择一个 **Auth Profile**（身份验证配置文件）或新建一个 BGP 身份验证配置文件，以控制对等组中 BGP 对等体之间的 MD5 身份验证。默认为 **None**（无）。
10. 选择一个**Timer Profile**（计时器配置文件）或创建一个新的 BGP 计时器配置文件，以控制影响通告路由的 keepalive 和更新消息的各种 BGP 计时器。默认为 **None**（无）。
11. 设置 **Multi Hop**（多个跃点）— 设置 IP 标头中的生存时间(TTL)值（范围为 0-255，默认为 0）。默认为 0 表示 1 代表 eBGP。默认为 0 表示 255 代表 iBGP。
12. 选择一个**Dampening Profile**（抑制配置文件）或新建一个抑制配置文件，以确定如何惩罚翻动路线以阻止其被使用，直到其变稳定。默认为 **None**（无）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 将 BGP 对等体添加到对等组。

1. 按 **Name**（名称）（最多 63 个字符）**Add**（添加） 对等体。名称必须以字母数字字符、下划线 (_) 、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。此名称在该逻辑路由器和所有逻辑路由器中必须唯一。
2. **Enable**（启用）对等体；默认为启用。
3. 选择 **Passive**（被动）， 以防止对等体发起与其邻居的会话；默认为禁用。
4. 输入对等体所属的 **Peer AS**（对等体 **AS**） ；范围为 1 - 4,294,967,295。
5. 选择 **Addressing**（寻址）， 然后选择对等体是否将从对等组**Inherit**（继）承 IPv4 和 IPv6 AFI 和筛选配置文件：**Yes**（是） （默认）或 **No**（否）。
6. 如果选择 **Yes**（是）， 请为对等体指定：
   - 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， 请选择要成为 BGP 对等体的接口 IP 地址。
   - 对于 **Peer Address**（对等地址）， 请选择 **IP** 并选择 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。

   防火墙仅使用来自 *FQDN* 的 *DNS* 解析中的一个 *IP* 地址（该地址来自各个 *IPv4* 或 *IPv6* 地址类型）。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。



7. 如果您选择**No**（否）， 即不从对等组**Inherit**（继承）地址， 请为对等体指定：
   - 要为对等体指定多个 **IPv4 Address Family**（**IPv4** 地址系列）选项，请选择所创建的 **AFI Profile**（**AFI** 配置文件）、选择默认 配置文件、选择 **inherit (Inherit from Peer-**

 ©2024 Palo Alto Networks, Inc.

Group)（继承（从对等组继承）），或新建 BGP 地址系列配置文件；默认为无（禁用 **IPv4 AFI**）。

AFI 配置文件允许您指定对等体是路由反射器客户端。路由反射器将所有对等体的所有通告反射到所有其他对等体，因而无需将 *iBGP* 完全网格化。如果您将对等体声明为路由反射器客户端，则 *BGP* 进程会将所有更新反射到该对等体。

- 要为对等体指定多个 **IPv6 Address Family**（**IPv6** 地址系列）选项，请选择所创建的 **AFI Profile**（**AFI** 配置文件）、选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承）），或新建 BGP 地址系列配置文件；默认为**none (Disable IPv6 AFI)**（无（禁用 **IPv6 AFI**））。

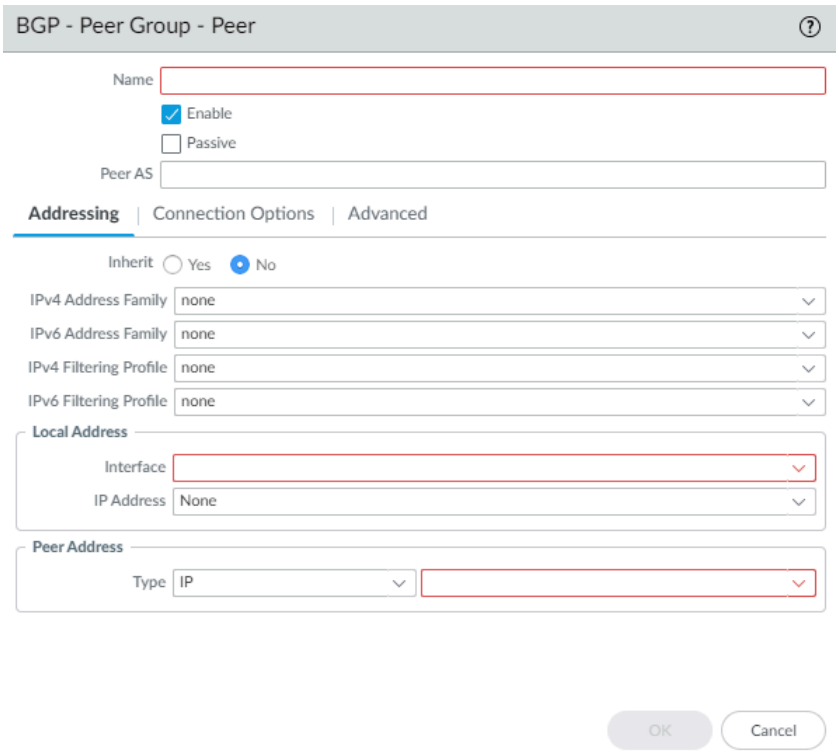
AFI 配置文件允许您指定对等体是路由反射器客户端。路由反射器将所有对等体的所有通告反射到所有其他对等体，因而无需将 *iBGP* 完全网格化。如果您将对等体声明为路由反射器客户端，则 *BGP* 进程会将所有更新反射到该对等体。

- 要将 **IPv4 Filtering Profile**（**IPv4** 筛选配置文件）选项应用于对等体，请选择所创建的 **BGP Filtering Profile**（**BGP** 筛选配置文件），选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承）），或新建 BGP 筛选配置文件；默认值为无（禁用 **IPv4** 筛选）。
- 要将 **IPv6 Filtering Profile**（**IPv6** 筛选配置文件）选项应用于对等体，请选择所创建的 **BGP Filtering Profile**（**BGP** 筛选配置文件），选择 **inherit (Inherit from Peer-**

 ©2024 Palo Alto Networks, Inc.

Group)（继承（从对等组继承）），或新建 BGP 筛选配置文件；默认值为无（禁用 **IPv6** 筛选）。

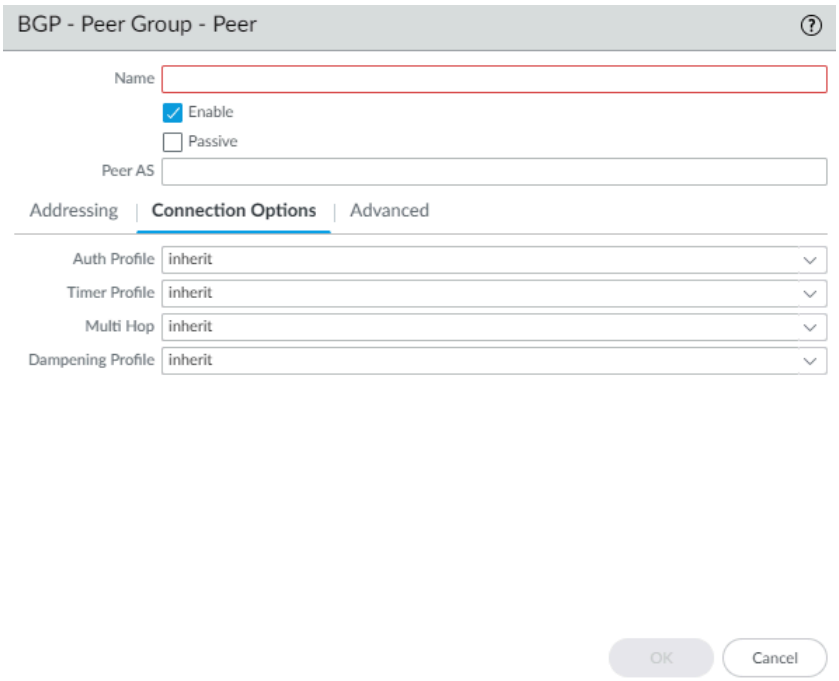
- 对于 **Local Address**（本地地址），请选择正在配置 BGP 的 **Interface**（接口）。如果接口有多个 IP 地址，请输入要成为 BGP 对等体的接口 **IP** 地址。
- 对于 **Peer Address**（对等地址），请选择 **IP** 并选择 IP 地址，或选择或创建一个地址对象，或是选择 **FQDN** 并输入类别 FQDN 的 FQDN 或地址对象。



BGP 对等体组（或对等体）可以同时应用 *IPv4* 地址族配置文件和 *IPv6* 地址族配置文件。属于该对等组的所有对等体将自动将寻址设置为继承 ***No***（否）。对等组中的所有对等体默认还会将 *IPv4* 地址系列配置文件、*IPv6* 地址系列配置文件、*IPv4* 筛选配置文件和 *IPv6* 筛选配置文件设置为无。为了使路由正常工作，对等接口必须同时分配 *IPv4* 地址和 *IPv6* 地址。您可以选择继承（从对等组继承）对等组，也可以通过为对等体选择特定配置文件来覆盖对等组。例如，您可以将对等体配置为继承 *IPv4* 地址系列配置文件并继承 *IPv4* 筛选配置文件，然后选择 *IPv6* 地址系列配置文件和 *IPv6* 筛选配置文件，以覆盖对等组中的这些配置文件。

8. 为对等体选择 **Connection Options**（连接选项），以应用与对等组不同的设置。

 ©2024 Palo Alto Networks, Inc.

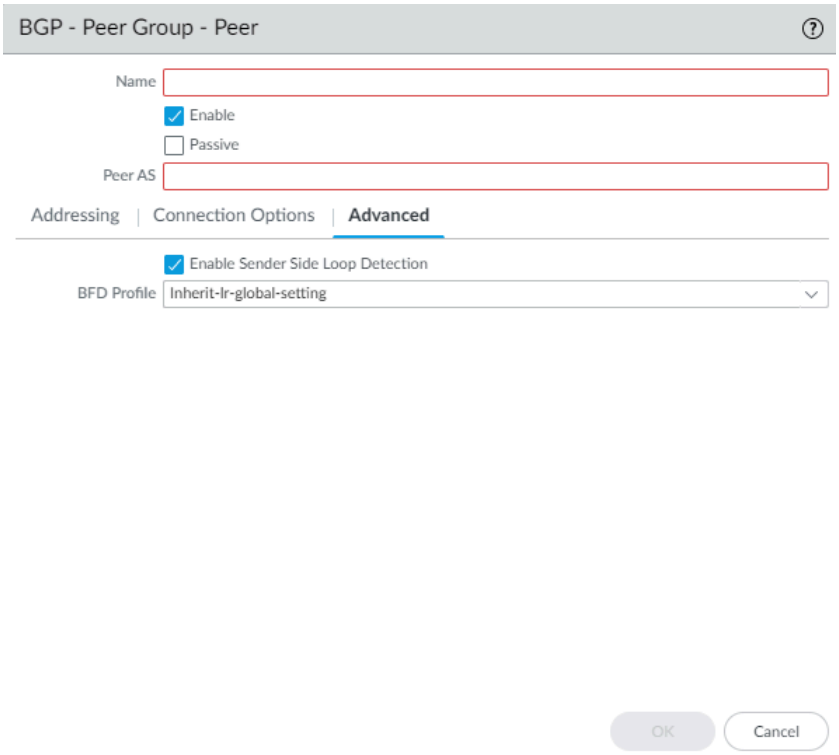


9. 选择一个**Auth Profile**（身份验证配置文件），然后选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承））（默认），或新建 BGP 身份验证配置文件来控制 BGP 对等体之间的 MD5 身份验证。
10. 选择一个**Timer Profile**（计时器配置文件），然后选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承））（默认），新建一个 BGP 计时器配置文件，或者选择默认配置文件，以控制影响通告路由的 keepalive 和更新消息的各种 BGP 计时器。
11. 设置 **Multi Hop**（多个跃点），即 IP 标头中的生存时值(TTL)值（范围为 0-255）。默认设置为 **inherit (Inherit from Peer-Group)**（继承（从对等组继承））。
12. 选择一个**Dampening Profile**（抑制配置文件），然后选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承））（默认），或新建一个抑制配置文件，以确定如何惩罚翻动路线以阻止其被使用，直到其变稳定。
13. 选择 **Advanced**（高级）和 **Enable Sender Side Loop Detection**（启用发送端循环检测）后，可让防火墙在更新中发送路由之前检查 BGP RIB 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 号在 AS_PATH 列表中，防火墙

 ©2024 Palo Alto Networks, Inc.

不会通告路由。通常接收方会执行循环检测，但这一优化功能会让发送方来执行循环检测。禁用此功能可让接收方执行循环检测。

14. 要将 **BFD Profile**（**BFD** 配置文件） 应用到对等体（只要未在逻辑路由器级别对 BGP 禁用 BFD，就会覆盖 BGP 的 BFD 设置），请选择以下之一：
    - 默认配置文件。
    - 现有 BFD 配置文件。
    - **Inherit-lr-global-setting**（继承协议的全局 **BFD** 配置文件）（默认）— 对等体将继承您为逻辑路由器的 BGP 选择的全局 BFD 配置文件。
    - **None**（无） — 为对等体停用 BFD。
    - 新建 BFD 配置文件。



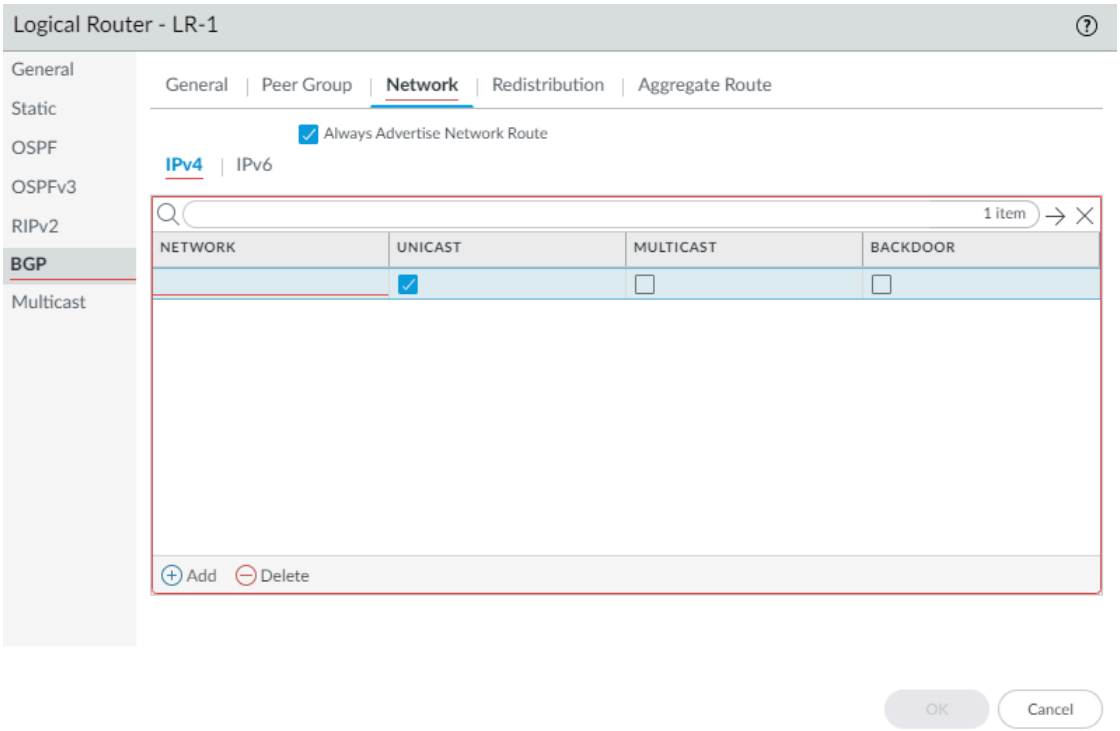
15. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 指定要向邻居通告的网络前缀。

将防火墙移动到不同的子网或临时更改网络后，***Network***（网络）功能将特别有用。

1. 选择 **Network**（网络）。
2. **Always Advertise Network Route**（总是通告网络路由）（默认启用）始终允许向 BGP 对等体通告所配置的网络路由，无论是否可达。如果未选中此选项，防火墙将仅在使用本地路由表解析网络路由时才会通告网络路由。
3. 选择 **IPv4** 或 **IPv6** 以选择前缀类型。
4. **Add**（添加）**Network**（网络）前缀，以向邻居通告。
5. 选择 **Unicast**（单播），在单播地址系列中通告该网络路由；默认为启用。如果未选中，防火墙将不会在单播 SAFI 中通告路由。
6. （仅限 IPv4）选择组播，将此网络路由通告到组播地址系列。默认为禁用；防火墙将不会在组播 SAFI 中通告此网络路由。
7. （仅限 IPv4）选择 **Backdoor**（后门）可防止 BGP 在 AS 外部通告前缀，而是将路由保留在 AS 内。后门是一个管理距离高于 IGP 路由的 BGP 路由。在内部，前缀的管理距离将增加，因此前缀不是首选，但如有需要，当其他位置发生链路故障时，前缀仍然可用。默认为禁用。

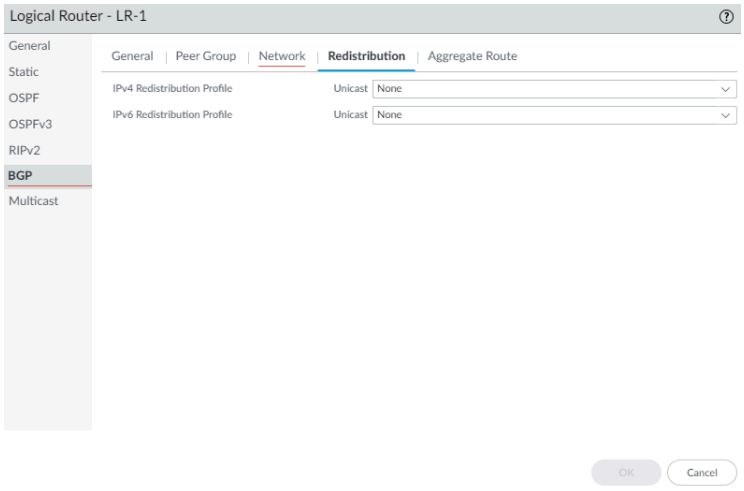


 ©2024 Palo Alto Networks, Inc.

STEP 6 | 将静态路由、已连接路由、OSPF、OSPFv3 或 RIPv2 路由重新分发到 BGP。

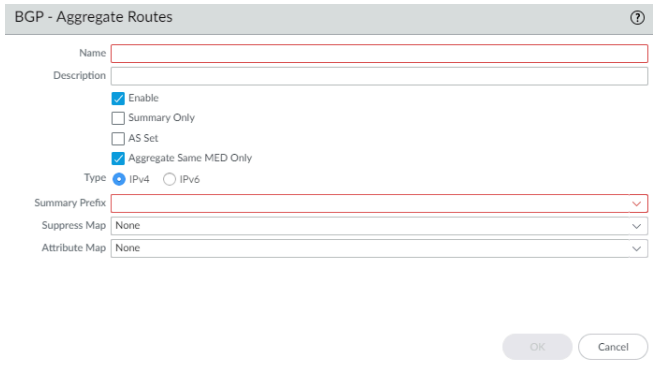
在 *BGP* 重新分发配置文件中，利用路由映射的灵活性来指定用于确定要重新分发哪些路由的条件并指定要设置的属性。

1. 选择 **Redistribution**（重新分发）。
2. 要重新分发 IPv4 路由，对于 **IPv4 Redistribution Profile -- Unicast**（**IPv4** 重新分发配置文件--单播），选择一个 BGP 重新分发配置文件或新建一个重新分发配置文件；默认为 **None**（无）。
3. 要重新分发 IPv6 路由，对于 **IPv6 Redistribution Profile -- Unicast**（**IPv6** 重新分发配置文件--单播），选择一个 BGP 重新分发配置文件或新建一个重新分发配置文件；默认为 **None**（无）。



STEP 7 | 创建聚合路由策略以汇总 BGP 学习并随后向对等体通告的路由。

1. 选择 **Aggregate Route**（聚合路由），然后并按 **Name**（名称）（最多 63 个字符）**Add**（添加） 聚合路由策略。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。
2. 输入对策略有用的 **Description**（描述）。
3. **Enable**（启用）策略。



4. 选择 **Summary Only**（仅汇总），以仅向邻居通告 **Summary Prefix**（汇总前缀）而不是汇总的路由；这会减少流量并避免不必要地增加邻居路由表的大小（默认为禁用）。如

 ©2024 Palo Alto Networks, Inc.

果要同时通告聚合路由和构成聚合路由的各个路由，请不要选中 **Summary Only**（仅汇总）。

Summary Only（仅汇总）和 ***Suppress Map***（抑制映射）为互斥选项，因此不能同时指定两者。

如果要使用 ***Summary Only***（仅汇总），但还想通告单个路由，则创建一个 BGP Filtering Profile（BGP 筛选配置文件）并在其中包含与该单个路由匹配的 ***Unsuppress Map***（抑制映射）路由映射。

5. 选择 **AS Set**（**AS** 集合），以通告前缀与构成聚合路由的 AS 编号列表；默认为禁用。
6. 选择 **Aggregate Same MED Only**（仅聚合相同的 **MED**），以仅在路由具有相同的多出口鉴别器(MED)值时才聚合路由；默认为启用。
7. 选择聚合路由的 **Type**（类型）：**IPv4** 或 **IPv6**。
8. 计算您要汇总的路由，然后通过指定 IP 地址/网络掩码或地址对象，输入跨越这些路由的 **Summary Prefix**（汇总前缀）。
9. 要防止各个路由聚合（抑制聚合），请选择 **Suppress Map**（抑制映射） 路由映射或新建一个 BGP 路由映射，并在其匹配标准中指定包含这些路由的 IPv4 或 IPv6 地址访问列表或前缀列表；默认为 **None**（无）。

   请注意，抑制路由映射的目的是防止某些路由在通告中聚合。因此，在路由映射中，您将允许要禁止聚合的路由（不拒绝您要禁止聚合的路由）。

   Summary Only（仅汇总）和 ***Suppress Map***（抑制映射）为互斥选项，因此不能同时指定两者。
10. 要设置该汇总前缀的属性信息（此时还没有属性，因为您刚刚才创建了此路由组合），请选择一个 **Attribute Map**（属性映射）路由映射或新建一个 BGP 路由映射，然后设置汇总前缀的属性（无匹配标准）。如果没有路由映射（**None**（无）），汇总前缀将具有默认属性。默认为 **None**（无）。

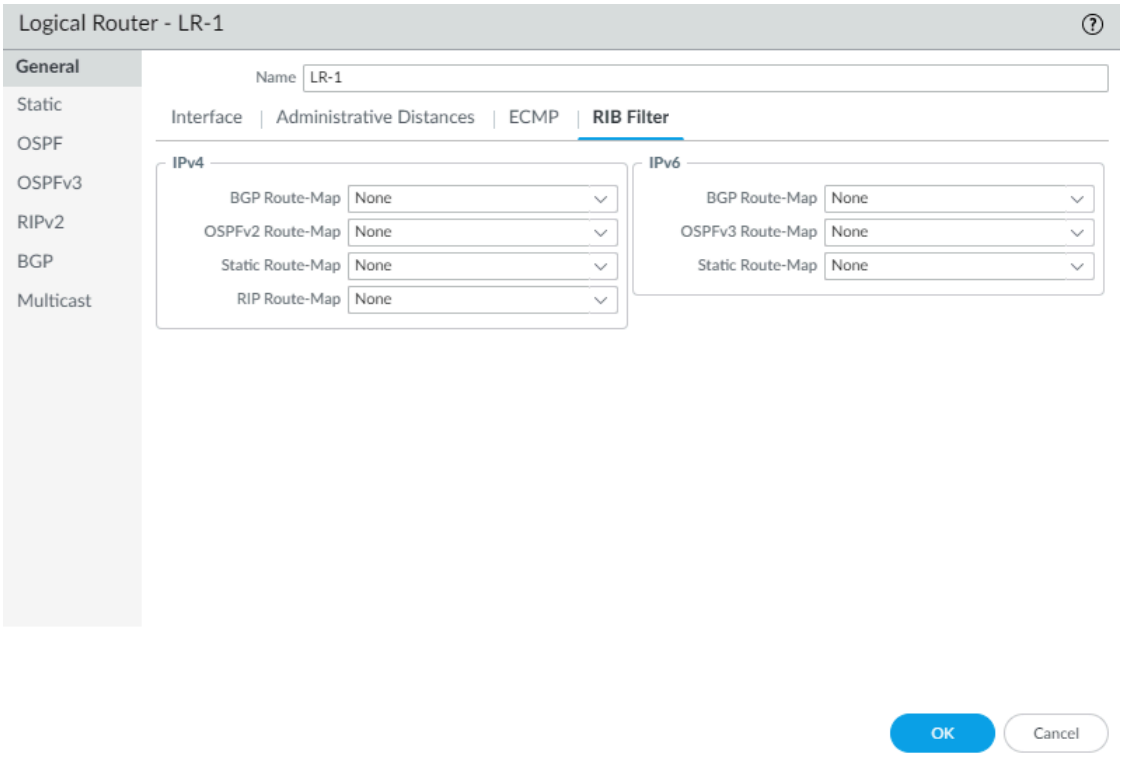
STEP 8 | 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | （可选）控制放置在全局 RIB 中的 BGP 路由。

您可能想要学习并重新分发路由，但又不希望它们出现在协议的本地路由表或全局 RIB 中。您可能只想将特定路由添加到全局 RIB。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择 **RIB Filter**（**RIB** 筛选器），以允许路由进入或阻止将路由添加到全局 RIB。



3. 要筛选 IPv4 BGP 路由，在 IPv4 区域中，对于 **BGP Route-Map**（**BGP** 路由映射），选择一个重新分发路由映射或新建一个。
4. 要筛选 IPv6 BGP 路由，在 IPv6 区域中，对于 **BGP Route-Map**（**BGP** 路由映射），选择一个重新分发路由映射或新建一个。
5. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

创建 BGP 路由配置文件

在高级路由引擎上，您可以在配置文件中轻松配置 BGP 的很多设置，然后应用于 BGP 对等组或对等体或重新分发规则。重复使用配置文件可将其应用于多个逻辑路由器和虚拟系统。创建同一类型的多个配置文件，以不同方式处理不同的对等组和对等体。BGP 对等组和对等体将继承全局配置文件；您还可以为 BGP 对等组创建配置文件以覆盖全局配置文件，并为 BGP 对等体创建配置文件，以覆盖对等体所属对等组的配置文件。

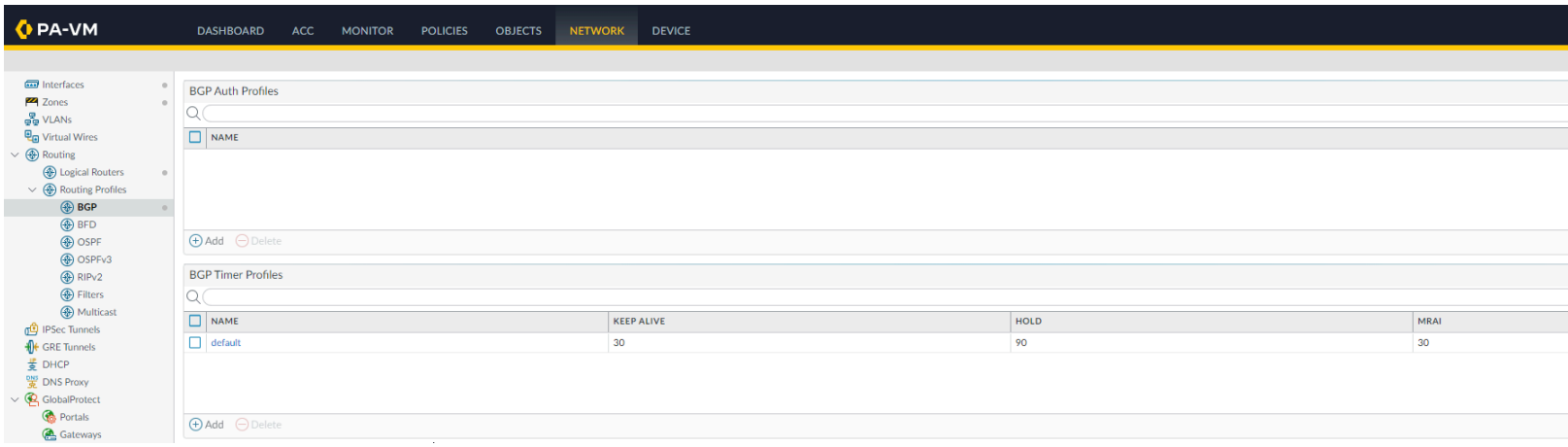
本主题将介绍 BGP 路由配置文件以及如何创建。

- **BGP Authentication Profiles**（**BGP** 身份验证配置文件） — 指定 MD5 身份验证的密钥，该密钥在 BGP 对等体的协商期间使用，以确定它们是否可以相互通信。在 BGP 对等组或对等配置中引用配置文件。
- **BGP Timer Profiles**（**BGP** 计时器配置文件） — 控制影响 keepalive 和更新消息（用于通告路由）的各种 BGP 计时器。在 BGP 对等组或对等配置中引用配置文件。
- **BGP Address Family Profiles**（**BGP** 地址系列配置文件） — 确定当 BGP 自治系统同时使用这两种类型的地址时 IPv6 或 IPv4 的行为。在 BGP 对等组或对等配置中引用配置文件。
- **BGP Dampening Profiles**（**BGP** 抑制配置文件） — 确定如何惩罚翻动路由，以阻止其被使用，直到其变稳定。在 BGP 对等组或对等配置中引用配置文件。
- **BGP Redistribution Profiles**（**BGP** 重新分发配置文件） — 将静态、互联、OSPF、OSPFv3 或 RIP 路由（满足所分配的路由映射的条件）重新分发到 BGP 中，并将路由映射集属性应用于重新分发的路由。**Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器） > **BGP** > **Redistribution**（重新分发）中的路由。
- **BGP Filtering Profiles**（**BGP** 筛选配置文件） — 同时将多个筛选器应用于对等组或对等体以执行以下操作：
  - 接受来自特定 AS 路径的路由（基于 AS 路径访问列表）。
  - 具有特定 AS 路径的路由（基于 AS 路径访问列表）。
  - 根据分发列表或前缀列表（不在同一筛选配置文件中）接受到本地 BGP RIB 的路由。分发列表基于源 IP 地址（具有通配符掩码，以获取前缀范围）。前缀列表基于网络地址/前缀长度。
  - 根据分发列表或前缀列表（不在同一筛选配置文件中）从本地 BGP RIB 通告路由。
  - 满足路由映射属性条件的路由进入本地 BGP RIB 中，并选择性地设置属性。
  - 满足路由映射属性条件的路由，并选择性地设置属性。
  - 有条件地通告存在的路由（满足存在条件）。
  - 有条件地通告不满足条件（满足不存在条件）的路由。
  - 抑制的受阻或汇总的路由。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 创建 BGP 身份验证配置文件。

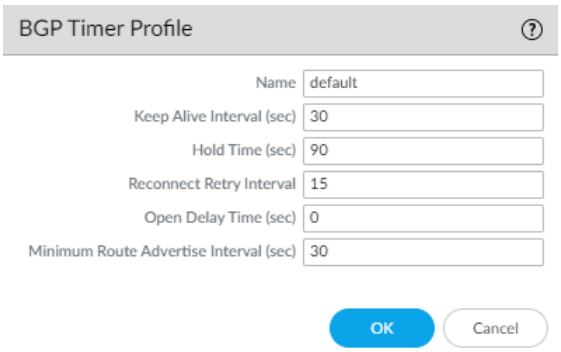
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BGP**。



2. 按 **Name**（名称）（最多 63 个字符 ）**Add**（添加）**BGP Auth Profile**（**BGP** 身份验证配置文件），以识别该配置文件。名称必须以字母数字字符、下划线 (_) 、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。
3. 输入 **Secret**（密码），然后 **Confirm Secret**（确认密码）。该密钥被用作 MD5 身份验证的密钥。
4. 单击 **OK**（确定）。

STEP 2 | 创建 BGP 计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BGP**。
2. 在 BGP 计时器配置文件窗口中，选择默认的 BGP 计时器配置文件，以查看默认配置文件设置：



3. 如果默认的 BGP 计时器配置文件设置并不是您需要的，可按 **Name**（名称）（最多 63 个字符）（添加）**BGP Timer Profile**（**BGP** 计时器配置文件）。名称必须以字母数字字符、下划线 (_) 、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。
4. 设置 **Keep Alive Interval (sec)**（保持活动状态间隔（秒））— BGP 发言者向对等体发送 Keepalive 的间隔（以秒为单位）（范围为 0 - 1,200；默认为 30）。如果在保持时间间

 ©2024 Palo Alto Networks, Inc.

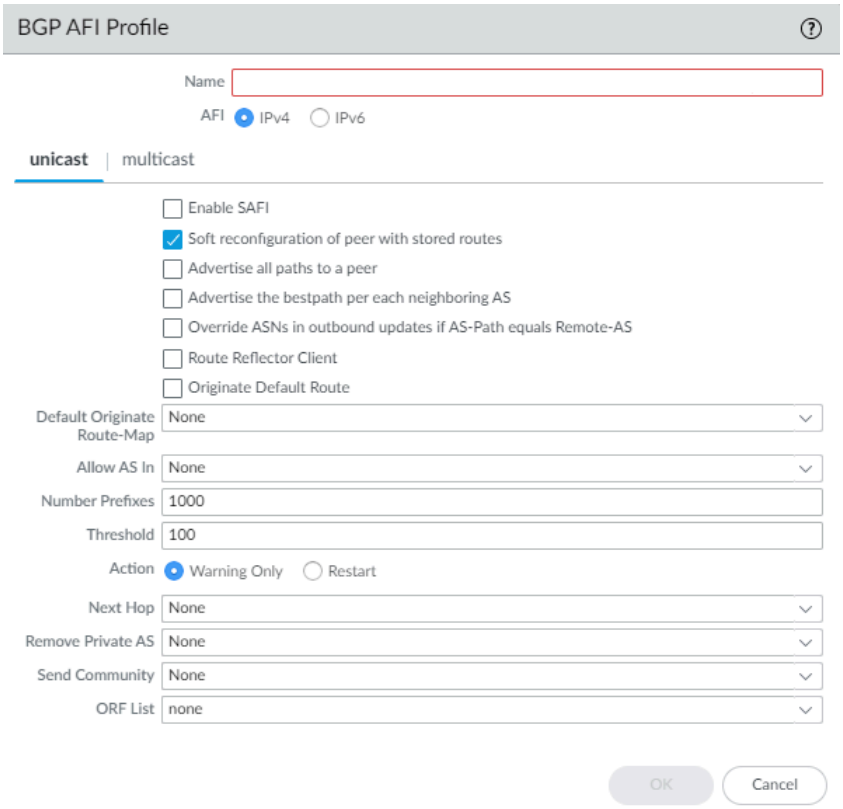
隔内未从对等体收到 Keepalive，则 BGP 对等将关闭。保持时间通常是保持活动状态间隔的三倍，以便在 BGP 对等关闭之前允许错过三次 Keepalive。

5. 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）。
6. 设置 **Reconnect Retry Interval**（重新连接重试间隔）— 输入在空闲状态下等待的秒数，然后重新尝试连接到对等体（范围为 1 到 3,600；默认为 15）。
7. 设置**Open Delay Time (sec)**（打开延迟时间（秒））— 从打开与对等体的 TCP 连接到发送第一条 BGP 打开消息（以建立 BGP 连接）的延迟秒数（范围为 0 - 240；默认值=为 0）。
8. 设置 **Minimum Route Advertise Interval (sec)**（最小路由通告间隔（秒））— 从通告到 BGP 发言者向对等体撤回到特定目标的路由必须经过的最短时间（秒）（范围为 1 - 600；默认为 30）。
9. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 要使用 MP-BGP，请创建共享属性的 BGP 地址系列标识符(AFI)配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BGP**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**BGP** 地址系列配置文件。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。



3. 选择 **IPv4** 或 **IPv6** AFI 以指定配置文件的类型。
4. 选择 **unicast**（单播）或 **multicast**（组播）。

   仅 ***IPv4*** *AFI* 配置文件支持***Multicast***（组播）。

5. 在 **unicast**（单播）选项卡中，**Enable SAFI**（启用 **SAFI**），为配置文件启用单播 SAFI。在 **multicast**（组播）选项卡中，**Enable SAFI**（启用 **SAFI**），为配置文件启用组播

 ©2024 Palo Alto Networks, Inc.

SAFI。如果同时为**unicast**（单播）和**multicast**（组播）选择了**Enable SAFI**（启用**SAFI**），则两种 SAFI 都会启用。必须至少启用一个 SAFI，BGP 配置文件才能生效。

6. 选择 **Soft reconfiguration of peer with stored routes**（使用存储路由进行对等体软重置），以使防火墙在更新其任何 BGP 对等体的设置后执行自身的软重置。（默认启用。）
7. **Advertise all paths to peers**（向对等体通告所有路径）— 让 BGP 向邻居通告所有已知路径，以保持网络内的多路径功能。
8. **Advertise the bestpath for each neighboring AS**（通告每个相邻 **AS** 的最佳路径），让 BGP 向邻居通告已知路径，以保留网络内的多路径功能。如果您要向所有自治系统通告相同的路径，则禁用此选项。
9. **Override ASNs in outbound updates if AS-Path equals Remote-AS**（如果 **AS-Path** 等于 **Remote-AS**，则替代出站更新中的 **ASN**）— 如果您有多个站点属于同一 AS 编号（例如 AS 64512），并且它们之间有另一个 AS，则此设置很有用。两个站点之间的路由器将收到更新，该更新通告可以访问 AS 64512 的路由。为避免第二个站点因为更新也在 AS 64512 中从而丢弃此更新，中间路由器可将 AS 64512 替换为自己的 AS 编号(ASN)（例如，AS 64522）。
10. 启用 **Route Reflector Client**（路由反射器客户端），使 BGP 对等体成为 IBGP 网络中的路由反射器客户端。
11. **Originate Default Route**（发起默认路由）— 选择此选项可生成默认路由并将其放置到本地 BGP RIB 中。
12. **Default Originate Route-Map**（默认发起路由映射）— 选择或创建路由映射以控制默认路由的属性。
13. **Allow AS in**（允许 **AS**）：
    - **Origin**（原始）— 即使 AS_PATH 中存在防火墙自己的 AS，也接受路由。
    - **Occurrence**（出现次数）— 防火墙自己的 AS 在 AS_PATH 中出现的次数。
    - **None**（无）—（默认设置）没有执行任何操作。
14. **Number Prefixes**（数字前缀）— 从对等体接受（学习）的最大前缀数。范围为 1 - 4,294,967,295；默认为 1,000。
15. **Threshold**（阈值）— 输入最大前缀数的阈值百分比。前缀将添加到 BGP 本地 RIB。如果对等体通告多个阈值，那么，防火墙将采取指定的操作（**Warning Only**（仅警告）或**Restart**（重新启动））。范围为 1 - 100；默认为 100。
16. **Action**（操作）— 系统日志中的 **Warning Only**（仅警告）消息，或在超过最大前缀数后 **Restart**（重新启动） BGP 对等连接。
17. 选择 **Next Hop**（下一个跃点）：
    - **Self**（自己）— 使防火墙在发送之前将所收到的更新中的下一个跃点地址更改为其自己的 IP 地址。当防火墙与 EBGP 路由器（在另一个 AS 中）和 IBGP 路由器（在自己的 AS 中）通信时，这将很有用。例如，假设到达 AS 64512 的 BGP 更新中的下一个跃点地址是路由器 2 传出接口的 IP 地址，其中更新传出 AS 64518。此更新指示要访问路由器 2 正在通告的网络，请使用路由器 2 的下一个跃点地址。但是，如果防火墙将该更新发送到 AS 64512 中的 iBGP 邻居，则路由器 2 中未更改的下一个跃点位于 AS 64512 外部，并且 iBGP 邻居没有指向它的路由。选择 **Self**（自己）时，防火墙会将下一个跃点更改为其自己的 IP 地址，以便 iBGP 邻居可以使用该下一个跃点访问防火墙，而防火墙又可以访问 eBGP 路由器。

 ©2024 Palo Alto Networks, Inc.

- **Self Force**（自身强制）— 强制将反射路由的下一个跃点设为自身。
- **None**（无）—（默认设置）在属性中保留原始的下一个跃点。

18. 要让 BGP 从更新（防火墙发送给另一个 AS 中的对等体）的 AS_PATH 属性中删除专用 AS 号，请在 **Remove Private AS**（删除专用 **AS**）中选择以下选项之一：
    - **All**（全部）— 删除所有专用 AS 号。
    - **Replace AS**（替换 **AS**）— 将所有专用 AS 号替换为防火墙的 AS 号。
    - **None**（无）—（默认设置）没有执行任何操作。
19. 对于 **Send Community**（发送社区），请选择要在出站更新数据包中发送的 BGP 社区属性的类型：
    - **All**（所有）— 发送所有社区。
    - **Both**（两者）— 发送标准和扩展社区。
    - **Extended**（扩展）— 发送扩展社区 (RFC 4360)。
    - **Large**（大型）— 发送大型社区 (RFC 8092)。
    - **Standard**（标准）— 发送标准社区 (RFC 1997)。
    - **None**（无）—（默认设置）不发送任何社区。
20. 对于 **ORF List**（**ORF** 列表）— 通告对等组或对等体发送前缀列表和/或接收前缀列表的能力，以便在源位置执行出站路由筛选(ORF)，从而最大限度减少发送或接收更新中不需要的前缀。选择 ORF 功能设置：
    - **none**（无）—（默认设置）应用了此 AFI 配置文件的对等组或对等体没有 ORF 功能。
    - **both**（二者）— 通告应用了此 AFI 配置文件的对等组或对等体可以 **send**（发送）前缀列表并 **receive**（接收）前缀列表以实现 ORF。
    - **receive**（接收）— 通告应用了此 AFI 配置文件的对等组或对等体可以接收前缀列表以实现 ORF。本地对等体接收远程对等体的 ORF 功能和前缀列表，并将其实现为出站路由筛选器。
    - **send**（发送）— 通告应用了此 AFI 配置文件的对等组或对等体可以发送前缀列表以实现 ORF。具有接收功能的远程对等体接收 ORF 功能，并在向发送方通告路由时实现它作为出站路由筛选器接收的前缀列表。

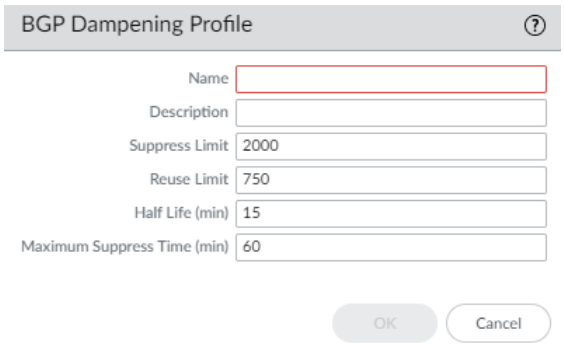
    ORF 是两个潜在问题的解决方案：a) 通告不需要的路由会浪费带宽；b) 筛选接收对等体可能需要的路由前缀。通过执行以下操作实现 ORF：

    1. 在地址系列配置文件中指定 ORF 功能。
    2. 对于作为发送方（**send**（发送）或 **both**（二者））的对等组或对等体，请创建一个前缀列表，其中包含对等组/对等体要接收的前缀集。
    3. 创建 BGP 筛选配置文件，然后在入站前缀列表中，选择您创建的前缀列表。
    4. 对于 BGP 对等组，请选择所创建的地址系列配置文件以将其应用于对等组。对于发送方，还要选择所创建的筛选配置文件（指示前缀列表）。如果对等组或对等体仅是 ORF 接收方，则不需要筛选配置文件，只需要有地址系列配置文件来指示 ORF **receive**（接收）功能。
21. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 创建 BGP 抑制配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BGP**。
2. 按 **Name**（名称）**Add**（添加）**BGP Dampening Profile**（**BGP** 抑制配置文件）。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。
3. 输入有用的 **Description**（说明）。
4. **Suppress Limit**（抑制门限）— 输入抑制值（翻动惩罚的累积值），达到此值后，来自对等体的所有路由都将被抑制。范围为 1 - 20,000；默认为 2,000。
5. **Reuse Limit**（重用门限）— 根据 **Half Life**（半衰期）中描述的步骤，输入控制何时可以重复使用路由的值。范围为 1 - 20,000；默认为 750。
6. **Half Life (min)**（半衰期（分钟））— 输入半衰期的分钟数，以控制应用于翻动路由的稳定性指标（惩罚）。范围是 1 至 45；默认为 15。稳定性指标从 1,000 开始。在受惩罚的路由稳定后，半衰期计时器将倒计时，直到归零，此时应用于路由的下一个稳定性指标仅为上一个值(500)的一半。连续截断会持续进行，直到稳定性指标小于重用门限的一半，然后再从路由中删除稳定性指标。
7. **Maximum Suppress Time (min)**（最大抑制时间（分钟））— 输入路径可以被抑制的最大分钟数，无论路由有多不稳定。范围是 1 至 255；默认为 60。

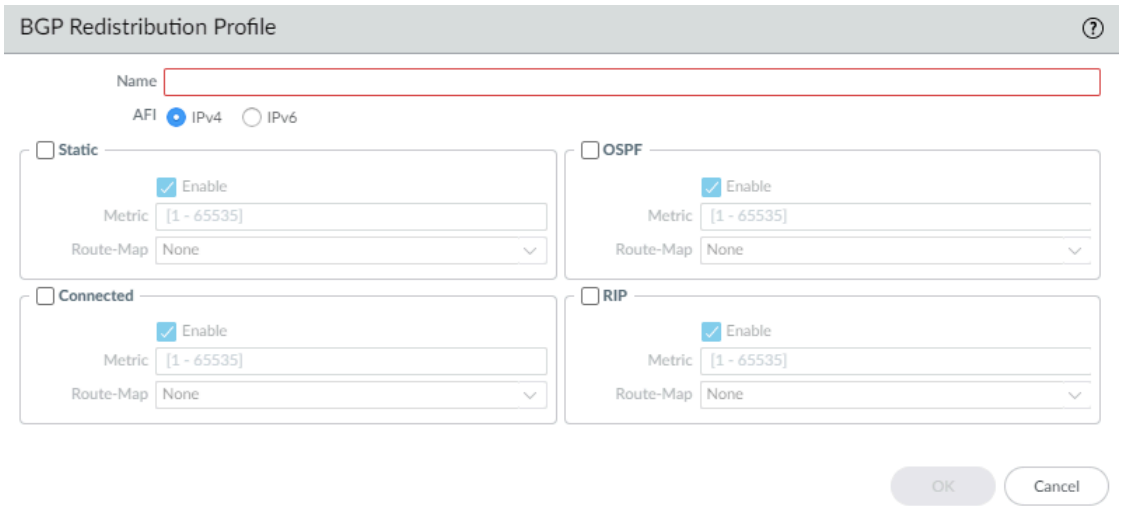


8. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 创建 BGP 重新分发配置文件，将静态路由、互联路由和 OSPF 路由（与相应的路由映射匹配）重新分发到 BGP。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BGP**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**BGP Redistribution Profile**（**BGP** 重新分发配置文件）。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。
3. 选择要重新分发的路由的 **AFI**：**IPv4** 或 **IPv6**。



4. 选择 **Static**（静态）以配置静态路由重新分发。
5. **Enable**（启用）IPv4 或 IPv6 静态路由的重新分发（基于所选择的 AFI）。
6. 配置适用于被重新分发给 BGP 的静态路由的 **Metric**（指标）（范围为 1- 65,535）。
7. 选择 **Route-Map**（路由映射），以指定用于确定要重新分发哪些静态路由的匹配标准。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
8. 选择 **Connected**（互联），以配置互联路由的重新分发。
9. **Enable**（启用）本地连接的 IPv4 或 IPv6 路由的重新分发（基于所选择的 AFI）。
10. 配置适用于被重新分发给 BGP 的互联路由的 **Metric**（指标）（范围为 1- 65,535）。
11. 选择 **Route Map**（路由映射），以指定用于确定要重新分发哪些互联路由的匹配标准。默认值是 None（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
12. （仅限 IPv4 AFI）选择 **OSPFv2** 以配置 OSPFv2 路由的重新分发。
13. **Enable**（启用） OSPFv2 路由的重新分发。
14. 配置适用于被重新分发给 BGP 的 OSPF 路由的 **Metric**（指标）（范围为 1- 65,535）。
15. 选择 **Route-Map**（路由映射），以指定用于确定要重新分发哪些 OSPF 路由的匹配标准。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
16. （仅限 IPv4 AFI）选择 **RIPv2** 以配置 RIPv2 路由的重新分发。
17. **Enable**（启用）RIPv2 路由的重新分发。

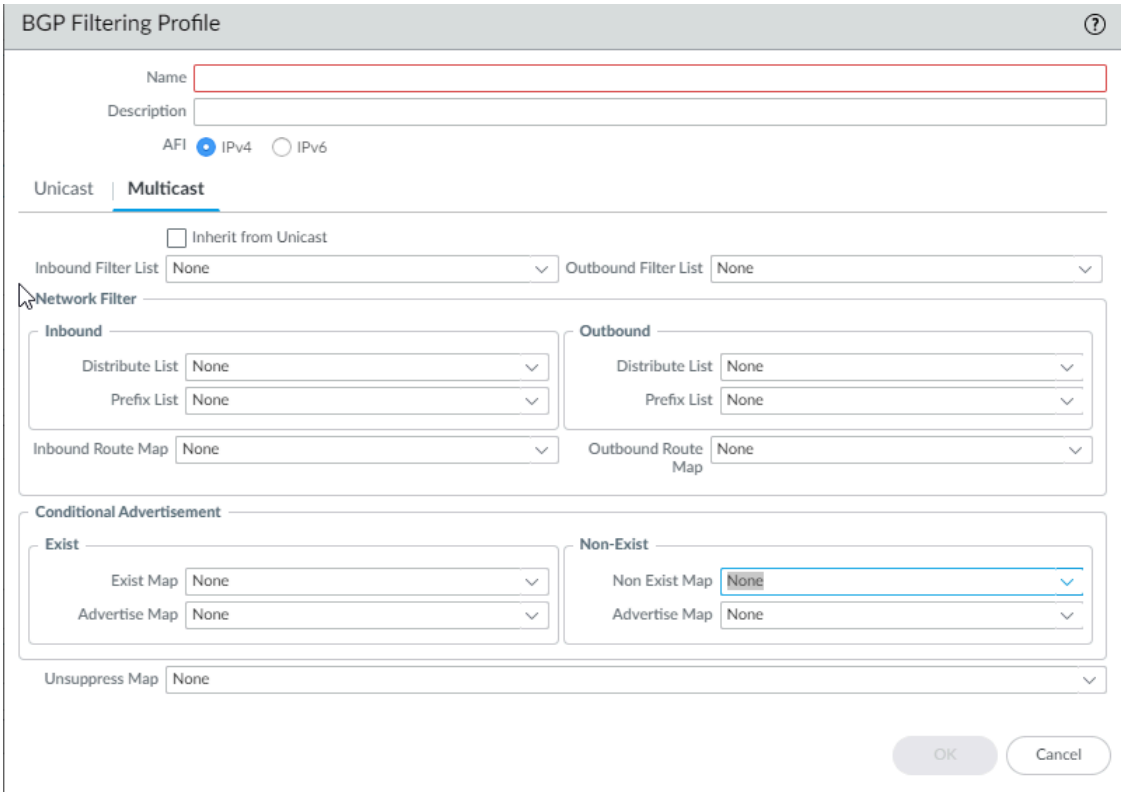
 ©2024 Palo Alto Networks, Inc.

18. 配置适用于被重新分发给 BGP 的 RIP 路由的 **Metric**（指标）（范围为 1- 65,535）。
19. 选择 **Route-Map**（路由映射），以指定用于确定要重新分发哪些 RIP 路由的匹配标准。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
20. （仅限 IPv6 AFI）选择 **OSPFv3** 以配置 OSPFv3 路由的重新分发。
21. **Enable**（启用）OSPFv3 路由的重新分发。
22. 配置适用于被重新分发给 BGP 的 OSPFv3 路由的 **Metric**（指标）（范围为 1-65,535）。
23. 选择 **Route-Map**（路由映射），以指定用于确定要重新分发哪些 OSPFv3 路由的匹配标准。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
24. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 创建 BGP 筛选配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BGP**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**BGP Filtering Profile**（**BGP** 筛选配置文件）。名称必须以字母数字字符、下划线 (_) 、连字符 (-) 或句点 (.) 开头，可以包含字母数字字符、下划线、连字符和句点。不允许有空格。
3. 输入有用的 **Description**（说明）。
4. 选择 **IPv4** 或 **IPv6** 地址系列标识符(AFI)，以指示要筛选的路由类型。



5. 选择 **Unicast**（单播）或 **Multicast**（组播）后续地址系列标识符(SAFI)。
6. 对于 **Unicast**（单播）、**Inbound Filter List**（入站筛选器列表）— 选择一个 AS 路径访问列表或新建一个 AS 路径访问列表，以指定在从对等体接收路由时，仅从对等组或对等体导入具有相同 AS 路径的路由，这意味着将添加到本地 BGP RIB。
7. 在 Network Filter（网络筛选器）区域中，**Inbound**（入站）— **Distribute List**（分发列表）— 使用访问列表（仅限源地址；不适用于目标地址）来筛选 BGP 收到的 BGP 路由信息。与单个筛选配置文件中的入站前缀列表互斥。
8. **Prefix List**（前缀列表）— 使用前缀列表根据网络前缀筛选 BGP 接收的 BGP 路由信息。与单个筛选配置文件中的入站分发列表互斥。
9. **Inbound Route Map**（入站路由映射）— 使用路由映射以更好地控制允许哪些路由进入本地 BGP RIB（匹配标准）并设置路由的属性（设置选项）。例如，可以通过将 AS 附加到路由的 AS 路径来控制路由首选项。

如果为入站路由映射配置了入站分发列表或前缀列表，则必须同时满足路由映射和列表的条件（逻辑 *AND*）。

 ©2024 Palo Alto Networks, Inc.

10. **Outbound Filter List**（出站筛选器列表）— 选择一个 AS 路径访问列表或新建一个 AS 路径访问列表，以指定仅将具有相同 AS 路径的路由通告到对等路由器（应用了此筛选器的对等组或对等路由器）。
11. **Outbound**（出站）— **Distribute List**（分发列表）— 使用访问列表根据目标的 IP 地址筛选 BGP 通告的 BGP 路由信息。与单个筛选配置文件中的出站前缀列表互斥。
12. **Prefix List**（前缀列表）— 使用前缀列表根据网络前缀筛选 BGP 通告的 BGP 路由信息。与单个筛选配置文件中的出站分发列表互斥。
13. **Outbound Route Map**（出站路由映射）— 使用路由映射以更好地控制 BGP 通告哪些路由（匹配标准）并设置所通告路由的属性。

    如果为出站路由映射配置了出站分发列表或前缀列表，则必须同时满足路由映射和列表的条件（逻辑 *AND*）。
14. 配置条件通告，这将允许您控制在本地 BGP RIB 中存在或不存在不同路由时要通告的路由。本地 BGP RIB 中不存在的路由可能表示对等连接或可访问性故障。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），有条件通告将特别有用。在有条件通告的 **Exist**（存在）区域中：
    - 在 **Exist Map**（存在映射）区域中，选择或创建路由映射，以指定有条件通告的匹配标准。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。

©2024 Palo Alto Networks, Inc.

- **Advertise Map**（通告映射）— 选择或创建路由映射以指定在满足条件时要通告的路由（本地 BGP RIB 有来自于存在映射的路由）。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。

15. 在有条件通告的 **Non-Exist**（不存在）区域中：
    - 在 **Non-Exist Map**（不存在的映射）字段中，选择或创建路由映射，以指定本地 BGP RIB 中不存在哪些路由的匹配标准，从而实现有条件地通告。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。
    - **Advertise Map**（通告映射）— 选择或创建路由映射，以指定当不存在的映射中的路由不在本地 BGP RIB 中时要通告的路由。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。
16. **Unsuppress Map**（取消抑制映射）— 选择或创建要取消抑制的路由的路由映射（它们之前可能因为汇总而被抑制，或者因为满足抑制条件而被抑制，但您现在希望取消抑制特定路径以进行通告）。
17. （仅限 IPv4 AFI）选择 **Multicast**（组播）以筛选 MP-BGP 组播路由。如果希望单播 SAFI 的所有筛选项也应用于组播 SAFI，请选择 **Inherit from Unicast**（从单播继承）。否则，请继续配置以下筛选字段。
18. 对于 **Multicast**（组播）、**Inbound Filter List**（入站筛选器列表）— 指定一个 AS 路径访问列表或新建一个 AS 路径访问列表，以指定在从对等体接收路由时，仅从对等组或对等体导入具有相同 AS 路径的路由，这意味着将添加到本地 BGP RIB。
19. 在 Network Filter（网络筛选器）区域中，**Inbound**（入站）— **Distribute List**（分发列表）— 使用访问列表（仅限源地址；不适用于目标地址）来筛选 BGP 收到的 BGP 路由信息。与单个筛选配置文件中的入站前缀列表互斥。
20. **Prefix List**（前缀列表）— 使用前缀列表根据网络前缀筛选 BGP 接收的 BGP 路由信息。与单个筛选配置文件中的入站分发列表互斥。
21. **Inbound Route Map**（入站路由映射）— 使用路由映射以更好地控制允许哪些路由进入本地 BGP RIB（匹配标准）并设置路由的属性（设置选项）。例如，可以通过将 AS 附加到路由的 AS 路径来控制路由首选项。

    如果为入站路由映射配置了入站分发列表或前缀列表，则必须同时满足路由映射和列表的条件（逻辑 *AND*）。
22. **Outbound Filter List**（出站筛选器列表）— 选择一个 AS 路径访问列表或新建一个 AS 路径访问列表，以指定仅将具有相同 AS 路径的路由通告到对等路由器（应用了此筛选器的对等组或对等路由器）。
23. **Outbound**（出站）— **Distribute List**（分发列表）— 使用访问列表根据目标的 IP 地址筛选 BGP 通告的 BGP 路由信息。与单个筛选配置文件中的出站前缀列表互斥。
24. **Prefix List**（前缀列表）— 使用前缀列表根据网络前缀筛选 BGP 通告的 BGP 路由信息。与单个筛选配置文件中的出站分发列表互斥。
25. **Outbound Route Map**（出站路由映射）— 使用路由映射以更好地控制 BGP 通告哪些路由（匹配标准）并设置所通告路由的属性。

    如果为出站路由映射配置了出站分发列表或前缀列表，则必须同时满足路由映射和列表的条件（逻辑 *AND*）。

 ©2024 Palo Alto Networks, Inc.

26. 配置条件通告，这将允许您控制在本地 BGP RIB 中存在或不存在不同路由时要通告的路由。本地 BGP RIB 中不存在的路由可能表示对等连接或可访问性故障。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），有条件通告将特别有用。在有条件通告的 **Exist**（存在）区域中：
    - 在 **Exist Map**（存在映射）区域中，选择或创建路由映射，以指定有条件通告的匹配标准。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。
    - **Advertise Map**（通告映射）— 选择或创建路由映射以指定在满足条件时要通告的路由（本地 BGP RIB 有来自于存在映射的路由）。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。
27. 在有条件通告的 **Non-Exist**（不存在）区域中：
    - 在 **Non-Exist Map**（不存在的映射）字段中，选择或创建路由映射，以指定本地 BGP RIB 中不存在哪些路由的匹配标准，从而实现有条件地通告。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。
    - **Advertise Map**（通告映射）— 选择或创建路由映射，以指定当不存在的映射中的路由不在本地 BGP RIB 中时要通告的路由。在此字段中，仅会考虑路由映射的匹配部分；设置部分将被忽略。
28. **Unsuppress Map**（取消抑制映射）— 选择或创建要取消抑制的路由的路由映射（它们之前可能因为汇总而被抑制，或者因为满足抑制条件而被抑制，但您现在希望取消抑制特定路径以进行通告）。
29. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

为高级路由引擎创建筛选器

高级路由引擎支持本主题中所述的筛选器。访问列表、前缀列表和重新分发路由映射可应用于 BGP、OSPFv2、OSPFv3 和 RIPv2。访问列表和前缀列表也适用于 IPv4 组播。组播路由映射适用于 IPv4 组播。AS 路径访问列表、社区列表和 BGP 路由映射仅适用于 BGP。

创建一个筛选器并在配置文件或其他适当位置引用该筛选器，以便轻松一致地应用可控制以下方面的设置：从对等体接受路由到本地 RIB、向对等体通告路由、有条件通告、设置属性、将路由导出到其他路由器或从其他路由器导入路由、路由聚合以及路由重新分发。

- **Access Lists**（访问列表）— 使用访问列表：
  - 根据 IPv4/IPv6 源地址和 IPv4 目标地址筛选网络路由。对于 IPv4 访问列表，可以通过地址与通配符掩码来指定源地址个目标地址，以表示地址范围。IPv6 访问列表可以指定源地址和子网。
  - 在 BGP 筛选配置文件中，指定入站分发列表（访问列表），以控制 BGP 将从对等组或对等体（邻居）接受哪些路由。这意味着与拒绝访问列表规则匹配的路由不会被放置到本地 BGP RIB 中；与允许访问列表规则匹配的路由将被放置到本地 BGP RIB 中。您可以将 BGP 筛选配置文件应用于筛选 IPv4 单播或筛选 IPv6 单播字段中的 BGP 对等组或对等体。（若要为对等体执行此操作，请选择 **Inherit No**（不继承））。对等设置优先于对等组设置。
  - 在 BGP 筛选配置文件中，指定出站分发列表（访问列表），以根据网络和 BGP 部署控制防火墙向其对等组或对等体通告哪些路由。然后，将 BGP 筛选配置文件应用于筛选 IPv4 单播或筛选 IPv6 单播字段中的 BGP 对等组或对等体。（若要为对等体执行此操作，请选择 **Inherit No**（不继承））。对等设置优先于对等组设置。
  - 作为重新分发路由映射中的匹配标准，指定 IPv4 或 IPv6 目标地址、下一个跃点或路由来源。
  - 在 BGP 路由映射中，作为 IPv4 地址、下一个跃点或路由来源以及 IPv6 地址的匹配标准。
  - 在 OSPFv2 和 OSPFv3 中，区域边界路由器(ABR)的导入列表和导出列表。
  - 为 IPv4 组播指定 PIM 组权限。

  访问列表不用于筛选用户流量或提供安全性。

  访问列表可以有多个规则；路由将根据相应顺序按照规则进行评估。当路由与某个规则匹配时，将执行拒绝或允许操作，并且不会再根据后续规则评估该路由。

  聚合视图显示所有已配置的访问列表；您可以高亮显示某个访问列表，然后进行修改或删除。
- **Prefix Lists**（前缀列表）— 使用前缀列表：
  - 根据路由前缀和前缀长度筛选添加到本地 RIB 的网络路由。
  - 在 BGP 筛选配置文件中，指定入站前缀列表以控制 BGP 将从对等组或对等体（邻居）接受哪些路由。这意味着与拒绝前缀列表规则匹配的路由不会被放置到本地 BGP RIB 中；与允许前缀列表规则匹配的路由将被放置到本地 BGP RIB 中。然后，将 BGP 筛选配置文件应用于筛选 IPv4 单播或筛选 IPv6 单播字段中的 BGP 对等组。（若要为对等体执行此操作，请选择不继承）。对等设置优先于对等组设置。

 ©2024 Palo Alto Networks, Inc.

- 在 BGP 筛选配置文件中，指定出站前缀列表，以根据网络和 BGP 部署控制防火墙向其对等组或对等体通告哪些路由。然后，将 BGP 筛选配置文件应用于筛选 IPv4 单播或筛选 IPv6 单播字段中的 BGP 对等组或对等体。（若要为对等体执行此操作，请选择不继承）。对等设置优先于对等组设置。
- 作为重新分发路由映射中的匹配标准，指定 IPv4 或 IPv6 目标地址、下一个跃点或路由来源。
- 在 BGP 路由映射中，作为 IPv4 地址、下一个跃点或路由来源以及 IPv6 地址的匹配标准。
- 对于某个区域的 OSPFv2 或 OSPFv3 ABR，在入站筛选列表或出站筛选列表中。
- 在 IPv4 组播 PIM 通用配置中指定 SPT 阈值。
- 在 IPv4 组播路由映射中。

一个前缀列表可以有多个规则；路由将根据相应顺序按照规则进行评估。当路由与某个规则匹配时，将执行拒绝或允许操作，并且不会再根据后续规则评估路由。前缀列表非常灵活，因为它允许您为前缀配置一个前缀长度（用于共同标识前缀），并且还可以通过指定前缀长度大于、小于或等于某个值来指定范围。防火墙评估前缀列表的效率要高于访问列表。

- **Redistribution Route Maps**（重新分发路由映射）— 使用重新分发配置文件中的重新分发路由映射，指定要重新分发到 BGP、OSPFv2、OSPFv3、RIP 或本地 RIB（目标协议）的 BGP、OSPFv2、OSPFv3、RIP、互联路由或静态路由（源协议）。您也可以将 BGP 主机路由重新分发给 BGP 对等体。匹配标准可以包括由访问列表和前缀列表指定的 IPv4 和 IPv6 地址；

  一个重新分发路由映射可以有多个条目；路由将按相应顺序对照条目进行评估。当路由与某个条目匹配时，将允许或拒绝该路由，并且不会再对照后续条目进行评估。如果匹配条目的操作为允许，防火墙还会将已配置的属性从路由映射设置为重新分发的路由。
- **Multicast Route Maps**（组播路由映射） — 创建组播路由映射，以筛选动态 IGMP 接口的来源。

以下筛选器仅适用于 BGP。

- **AS Path Access Lists**（**AS** 路径访问列表）— 创建 AS 路径访问列表：
  - 要控制将来自其他路由器的 BGP 路由的导入本地 BGP RIB 的操作，请在 BGP 筛选配置文件中的入站筛选器列表中使用。例如，您希望仅导入通过特定自治系统的路由。
  - 要控制将 BGP 路由导出到另一个路由器的操作，请在 BGP 筛选配置文件的出站筛选器列表中使用。
  - 要执行 BGP 路由映射可以执行的任何操作，请在 BGP 路由映射中用作匹配标准。
  - 要重新分发 BGP 路由，请在 BGP 重新分发路由映射（AS路径）中用作匹配标准。

  AS 路径访问列表最多可以有 64 条规则，最后一条规则为隐式 **Permit Any**（允许任何）规则。使用 AS 路径访问列表拒绝自治系统。路由将根据相应顺序按照规则进行评估。当路由与某个规则匹配时，将执行拒绝或允许操作，并且不会再根据后续规则评估路由。

 ©2024 Palo Alto Networks, Inc.

- **Community Lists**（社区列表）— 创建社区列表：
  - 在 BGP 路由映射中引用，以匹配您希望以某种方式控制的路由的 BGP 社区属性。例如，您可以将一组路由（共享一个社区属性）设置为具有特定指标或本地首选项。
  - 在 BGP 路由映射的设置操作中引用，以从满足匹配标准的路由中移除社区。
  - 匹配要使用重新分发路由映射重新分发的路由中的 BGP 社区。

  社区列表可以有多个规则；路由将根据相应顺序按照规则进行评估。当路由与某个规则匹配时，将执行拒绝或允许操作，并且不会再根据后续规则评估路由。
- **BGP Route Maps**（**BGP** 路由映射）— 创建 BGP 路由映射：
  - 对于 BGP AFI 配置文件的 **Default Originate Route-Map**（默认始发路由映射）字段；匹配标准定义了何时生成默认路由(0.0.0.0)。将 BGP AFI 配置文件应用于 BGP 对等组或对等体。匹配标准可以是任何参数，并且如果存在与现有 BGP 路由的匹配，将创建默认路由；不使用路由映射的集合部分。相反，您可以使用出站路由映射来设置所生成的默认路由的属性。
  - 设置（覆盖）BGP 发送到对等体的 BGP 属性。
  - 对于 NAT，要为所通告的某组前缀设置源地址和 IPv4 下一个跃点，请输入 NAT 池中的公用 IP 地址以替换专用 IP 地址。
  - 将静态路由、连接路由或 OSPF 路由重新分发到 BGP；然后在 BGP 重新分发配置文件中引用该 BGP 路由映射。
  - 在 BGP 筛选配置文件中，使用**Inbound Route Map**（入站路由映射）或**Outbound Route Map**（出站路由映射）中的 BGP 路由映射来筛选从 BGP 对等体接受（学习）到本地 BGP RIB（入站）或通告到 BGP 对等体（出站）的路由。
  - 要有条件地通告 BGP 路由，请在 BGP 筛选配置文件中创建一个 **Exist Map**（存在映射），该映射指定如果路由中存在这些条件，则根据通告映射通告该路由。或者，指定如果这些条件不存在，则根据 **Non-Exist Advertise Map**（不存在通告映射）通告该路由。
  - 在 BGP 筛选配置文件中，将 IPv4 下一个跃点设置为使用公共 NAT 地址，而不是专用地址。
  - 在 BGP 筛选配置文件中，使用 BGP 路由映射来取消抑制由于路由抑制或聚合而被抑制的路由。
  - 要有条件地筛选更具体的路由，请为逻辑路由器配置 BGP **Aggregate Routes**（聚合路由）并提供**Suppress Map**（抑制映射）。
  - 要为逻辑路由器设置聚合路由的属性，请配置 BGP **Aggregate Routes**（聚合路由）并提供 **Attribute Map**（属性映射）。

一个筛选器可以有多个规则；防火墙将根据筛选器中的规则按规则序号 **(Seq)** 的顺序评估数据包或路由。当数据包或路由与某个规则匹配时，将执行拒绝或允许操作，并且不会再根据后续规则评估该数据包或路由。



除 *AS* 路径访问列表之外，所有筛选器的最后一个规则都是隐式的 ***Deny Any***（拒绝任何）规则。除 *AS* 路径访问列表之外，所有筛选器都必须至少有一个 ***Permit***（允许）规则；否则，将拒绝所检查的全部路由/数据包。*AS* 路径访问列表的最后一个规则是隐式的 ***Permit Any***（允许任何）规则。

选择一个已配置的 **Seq**（序号），以打开规则并进行修改。在已配置的规则中选择 **Action**（操作）字段，以仅修改允许或拒绝操作。

 ©2024 Palo Alto Networks, Inc.

添加规则时，请在规则之间保留足够的未使用序号，以便将来在筛选器中插入规则。例如，使用序号 *10*、*20*、*30* 等。

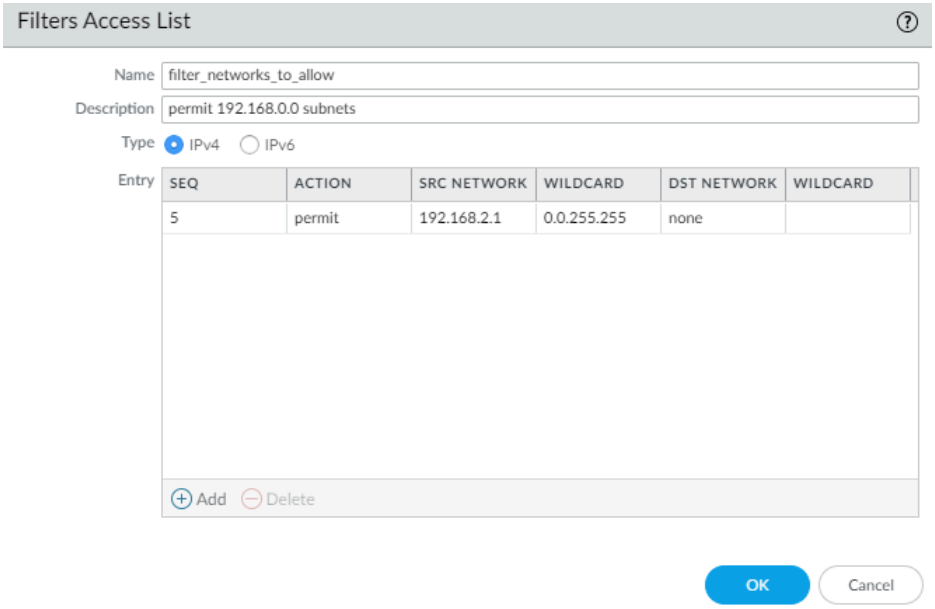
STEP 1 | 创建访问列表以允许或拒绝应用此筛选器的 IPv4 或 IPv6 地址。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Filters**（过滤器）。
2. 按 **Name**（名称）（最多63个字符）**Add**（添加）**Filters Access List**（筛选器访问列表）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入有用的 **Description**（说明）。
4. 选择访问列表的 **Type**（类型）：**IPv4** 或 **IPv6**。
   1. 对于 IPv4，请 **Add**（添加）**IPv4 Entry**（**IPv4** 条目）并输入规则 **Seq**（序号）（范围为 1 到 65,535）。
   2. 选择 **Actions**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许）。
   3. 对于 **Source Address**（源地址），有三个选项：选择 **Address**（地址），然后在随后出现的 **Address**（地址）字段中输入 IPv4 地址。输入一个**Wildcard**（通配符）掩码以指示范围。掩码中的零(0)表示该位必须与地址中的相应位匹配；掩码中的一(1)表示“无关”位。此外，还有选项 **Any**（任何）或 **None**（无）。
   4. 对于 **Destination Address**（目标地址），选择 **Address**（地址），然后在随后出现的 **Address**（地址）字段中输入 IPv4 地址。输入一个**Wildcard**（通配符）。掩码中

 ©2024 Palo Alto Networks, Inc.

的零(0)表示必须匹配的位；掩码中的一(1)表示“无关”位。此外，还有选项 **Any**（任何）或 **None**（无）。

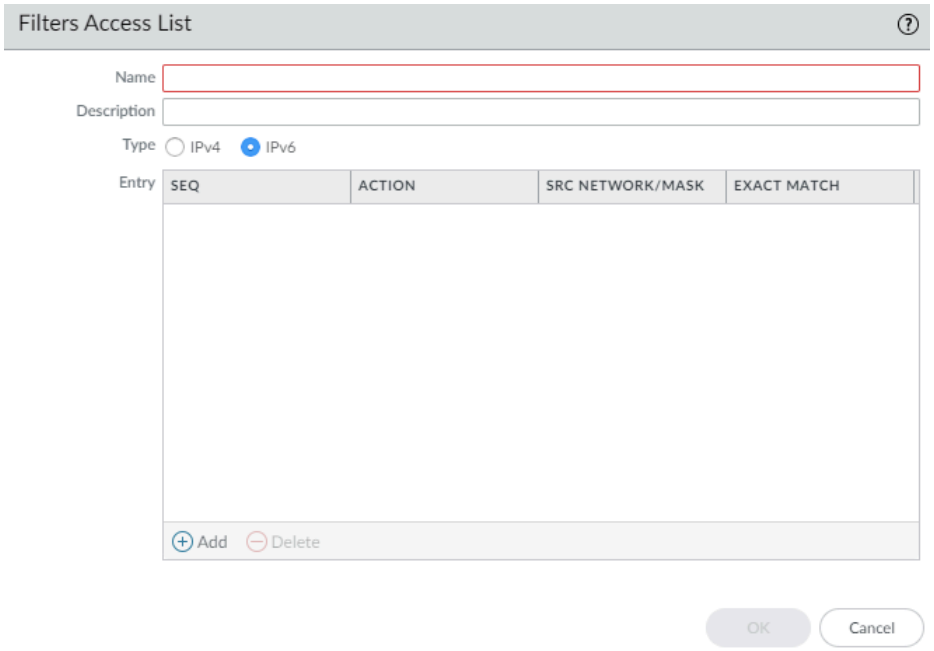
5. 单击 **OK**（确定）保存条目。



5. 或者，在 **Type**（类型）中选择 **IPv6**。
   1. 对于 IPv6，请 **Add**（添加）**IPv6 Entry**（**IPv4** 条目）并输入 **Seq**（序号）（范围为 1 到 65,535）。
   2. 选择 **Actions**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许）。
   3. 对于 **Source Address**（源地址），有三个选项：选择 **Address**（地址），然后在随后出现的 **Address**（地址）字段中输入 IPv6 地址。（可选）选择**Exact Match of this address**（完全匹配此地址），使防火墙比较前缀和前缀长度，并且它们必须完全匹配；否则，防火墙将根据路由是否位于与配置的前缀相同的子网中来确定是否匹配。(如果源地址为 **Any**（任何）或 **None**（无），则不能选择 **Exact Match of this address**（完全匹配此地址）。）此外，还有选项 **Any**（任何）或 **None**（无）。

 ©2024 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）保存条目。（可选）添加更多条目。

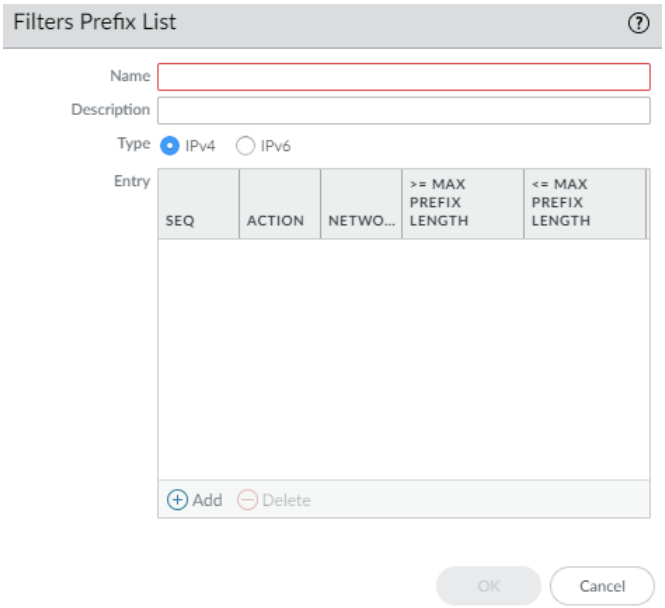


6. 单击 **OK**（确定）保存访问列表。

©2024 Palo Alto Networks, Inc.

STEP 2 | 创建前缀列表。

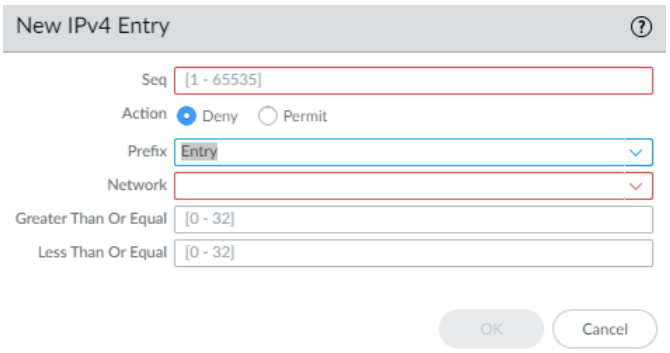
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Filters**（过滤器）。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**Filters Prefix List**（筛选器前缀列表）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入有用的 **Description**（说明）。
4. 选择此规则要筛选的前缀 **Type**（类型）：**IPv4** 或 **IPv6**。



1. 对于 IPv4，请 **Add**（添加）**IPv4 Entry**（**IPv4** 条目）并输入规则 **Seq**（序号）（范围为 1 到 65,535）。
2. 选择 **Actions**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许）。
3. 对于 **Prefix**（前缀），有三个选项；默认值为 **None**（无）。另一个选项是选择 **Network any**（任何网络）。第三个选项是选择 **Entry**（条目）并输入 IPv4 **Network**（网络）前缀（带斜杠）与基本前缀长度（二者共同指定网络），例如 192.168.2.0/24。（可选）将前缀长度指定为 **Greater Than Or Equal**（大于等于）某个数字（该数字至少与指定的基本长度一样大;范围为 0 - 32）。通过指定 **Less Than**

 ©2024 Palo Alto Networks, Inc.

Or Equal（小于等于）某个数字（至少与基本长度和 **Greater Than Or Equal**（大于等于）长度（如已配置）一样大）来指定范围的上限（可选）；范围为 0 - 32）。



路由与前缀规则（IPv4 或 IPv6）将分两步进行比较：1) 先将前缀与网络匹配。2) 再将前缀长度与掩码范围匹配（大于等于 - 小于等于）。例如，考虑网络为 192.168.3.0/24 且前缀长度大于等于 26且小于等于 30 的前缀列表规则。下表列出了经过测试的路由，以及它们是否通过了规则的评估。对于通过规则评估的路由，将执行所配置的操作（拒绝或允许）。

路由示例	结果
192.168.3.0/28	通过：网络和前缀长度与规则匹配。
192.168.2.0/30	未通过：网络与规则不匹配。
192.168.3.0/32	未通过：前缀长度与规则不匹配。

在规则的输出摘要中，LOU 为逻辑运算符单元（等于、大于等于、小于等于）。>= 表示前缀长度大于或等于该值；它是前缀长度范围的最小值。<= 表示前缀长度小于或等于该值；它是前缀长度范围的最大值。

5. 或者，**Add**（添加）**IPv6 Entry**（**IPv6** 条目），然后按照与 IPv4 前缀规则类似的步骤操作。IPv6 前缀长度的范围是 **Greater Than or Equal**（大于等于）0 - 128，且 **Less Than Or Equal**（小于等于） 0 - 128。

   例如，考虑网络为2001:db8:1/48 且前缀长度大于等于 56且小于等于 64 的前缀列表规则。下表列出了经过测试的路由，以及它们是否通过了规则的评估。对于通过规则评估的路由，将执行所配置的操作（拒绝或允许）。

路由示例	结果
2001:db8:1/64	通过：网络和前缀长度与规则匹配。
2001:db8:2/48	未通过：网络与规则不匹配。

©2024 Palo Alto Networks, Inc.

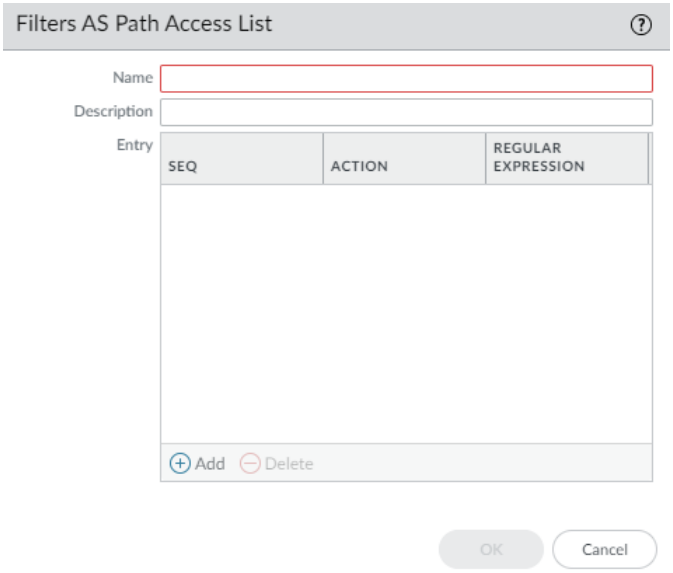
路由示例	结果
2001:db8:1/65	未通过：前缀长度与规则不匹配。

6. 单击 **OK**（确定）保存前缀条目。（可选）添加更多条目。
7. 单击 **OK**（确定）保存前缀列表。

STEP 3 | 为 BGP 创建 AS 路径访问列表。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Filters**（过滤器）。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**AS Path Acess List**（**AS** 路径访问列表）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入有用的 **Description**（说明）。
4. **Add**（添加）**Entry**（条目）并输入 **Seq**（序号）（范围为 1 - 65,535）。
5. 选择 **Actions**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许）。

   每个 *AS* 路径访问列表的最后一个规则都是隐式的 ***Permit Any***（允许任何）规则。使用 *AS* 路径访问列表拒绝自治系统。
6. 输入格式为 **regex1:regex2:regex3** 的 **Aspath Regex**（**AS** 路径正则表达式），以冒号(:)分隔三个AS值。允许的字符为 1234567890_^|[,{}()]$*+.?-\。例如，Deny 语句中的 .*65000 不包括来源于 AS 65000 的前缀。

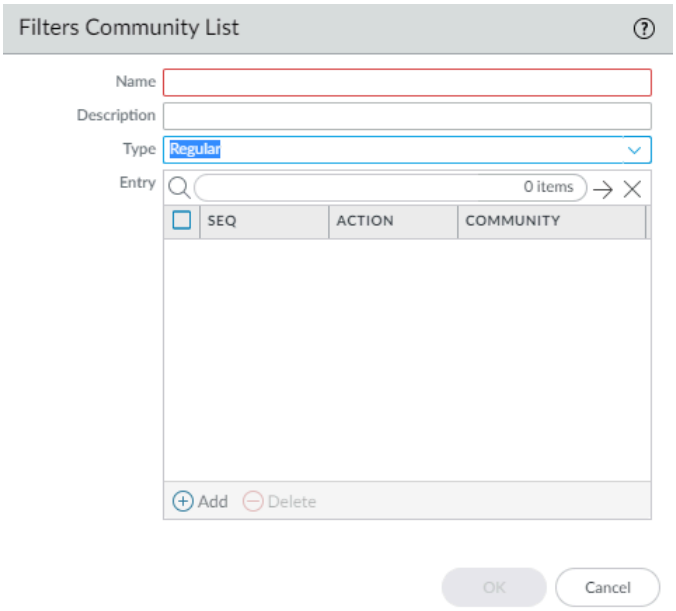


7. 单击 **OK**（确定）保存条目。可以添加更多条目；AS 路径访问列表中最多允许有 64 个条目。
8. 单击 **OK**（确定）保存 AS 路径访问列表。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 创建社区列表。

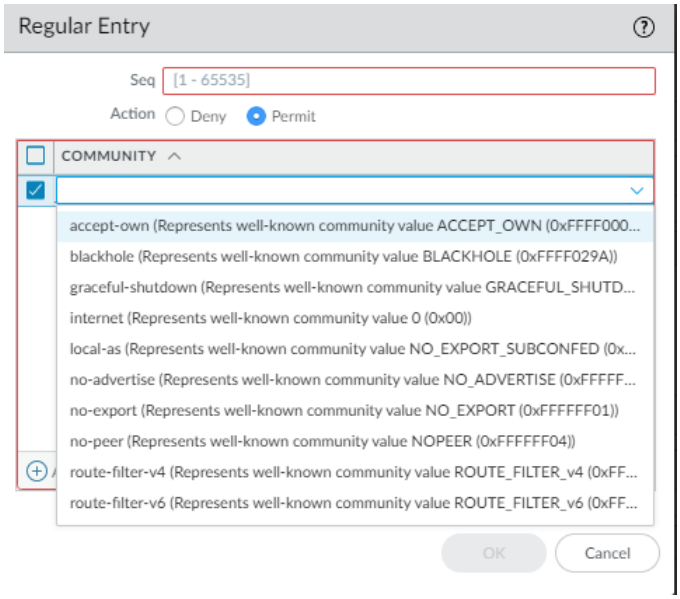
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Filters**（过滤器）。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**Filters Community List**（筛选器社区列表）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入有用的 **Description**（说明）。



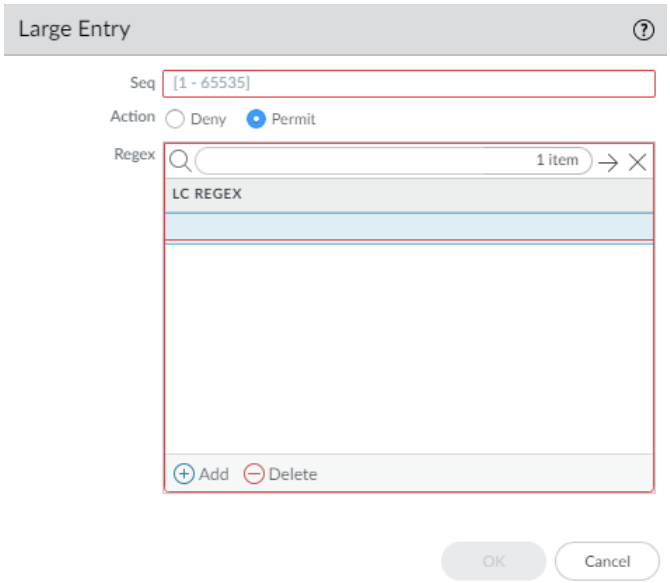
4. 选择 **Type**（类型）：
   - **Regular**（常规）— **Add**（添加）一个 **Seq**（序号）（范围为 1 - 65,535），然后选择 **Action**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许），然后 **Add**（添加）一个或多个社区值，选择一个或多个已知社区，或输入社区值和已知社区的组合。使用竖线(|)分隔多个社区，例如 **`6409:10|6520:13|internet`**。在 **Regular**（常规）条目（规则）中最多可输入 16 个社区。
     - 常规社区值的格式为 AA:NN，其中 AA 为 AS 编号，NN 是网络编号（每个编号的范围都是 0 - 65,535）。
     - **accept-own** — 表示已知社区值 ACCEPT-OWN(0xFFFF0001)
     - **blackhole** — 表示已知社区值 BLACKHOLE(0xFFFF029A)。相邻网络应丢弃去往该前缀的流量。
     - **graceful-shutdown** — 表示已知社区值 GRACEFUL_SHUTDOWN(0xFFFF0000)
     - **internet** — 表示已知社区值 0(0x00)。将前缀通告给所有 BGP 邻居。
     - **local-as** — 表示已知社区值 NO_EXPORT_SUBCONFED(0xFFFFFF03)。其作用是不向联合中的子 AS 之外通告该前缀。
     - **no-advertise** — 表示已知社区值 NO_ADVERTISE(0xFFFFFF02)。将此社区添加到前缀意味着接收 BGP 对等体将把前缀放入其 BGP 路由表，但不会将该前缀通告给其他邻居。

 ©2024 Palo Alto Networks, Inc.

- **no-export** — 表示已知社区值NO_EXPORT (0xFFFFFF01)。将此社区添加到前缀意味着接收 BGP 对等体将仅向 iBGP 邻居通告该前缀，而不会向 AS 外部的邻居通告。
- **no-peer** — 表示已知社区值NOPEER (0xFFFFFF04)。
- **route-filter-v4** — 表示已知社区值 ROUTE_FILTER_v4(0xFFFF0003)。
- **route-filter-v6** — 表示已知社区值 OUTE_FILTER_v6(0xFFFF0005)。

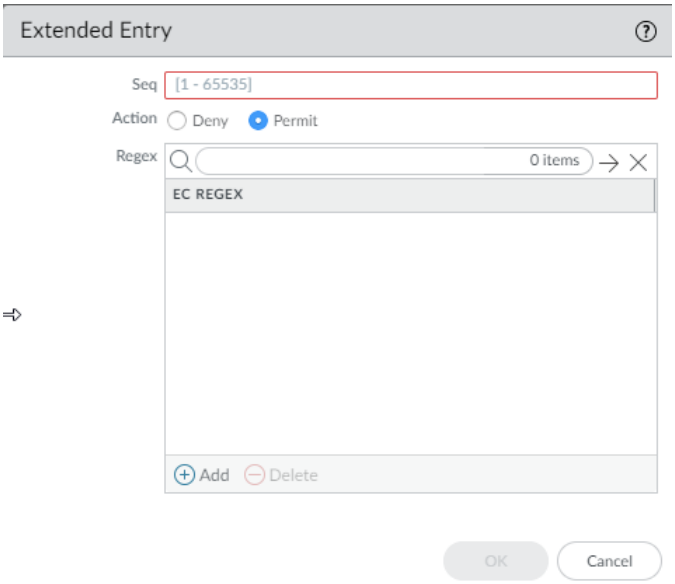


- **Large**（大型）— **Add**（添加）一个 **Seq**（序号）（范围为 1 - 65,535），然后选择 **Action**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许），然后添加一个大型社区正则表达式 (LC REGEX) 条目。条目中允许的字符为 1234567890_^|[,{}()]$*+.?-\。每个社区的格式必须为 **regex1:regex2:regex3**；例如，**203[1-2]:205[2-5]:206[5-6]**。在 **Large**（大型）条目（规则）中，最多可输入八个社区。



 ©2024 Palo Alto Networks, Inc.

- **Extended**（扩展）— **Add**（添加）一个 **Seq**（序号）（范围为 1 - 65,535），然后选择 **Action**（操作）：**Deny**（拒绝）（默认）或 **Permit**（允许），然后**Add**（添加）BGP 扩展社区正则表达式 (EC REGEX)。允许的字符为 1234567890_^|[,{}()]$*+.?-\。每个扩展社区的格式必须为 **regex1:regex2**；例如，**204*[3-8]:205*[4-8]**。在 **Extended**（扩展）条目（规则）中最多可输入八个社区。

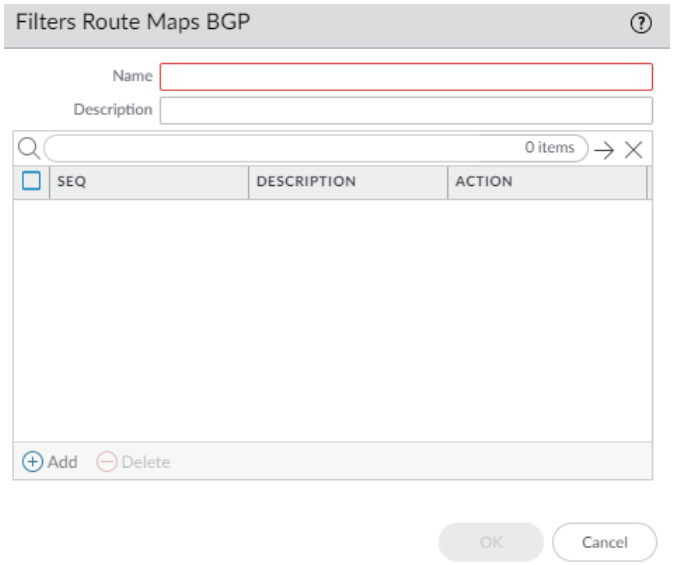


5. 单击 **OK**（确定），将条目保存在社区列表中。（可选）添加多个相同类型的条目（常规、大型或扩展）。
6. 单击 **OK**（确定）保存社区列表。

©2024 Palo Alto Networks, Inc.

STEP 5 | 创建 BGP 路由映射。

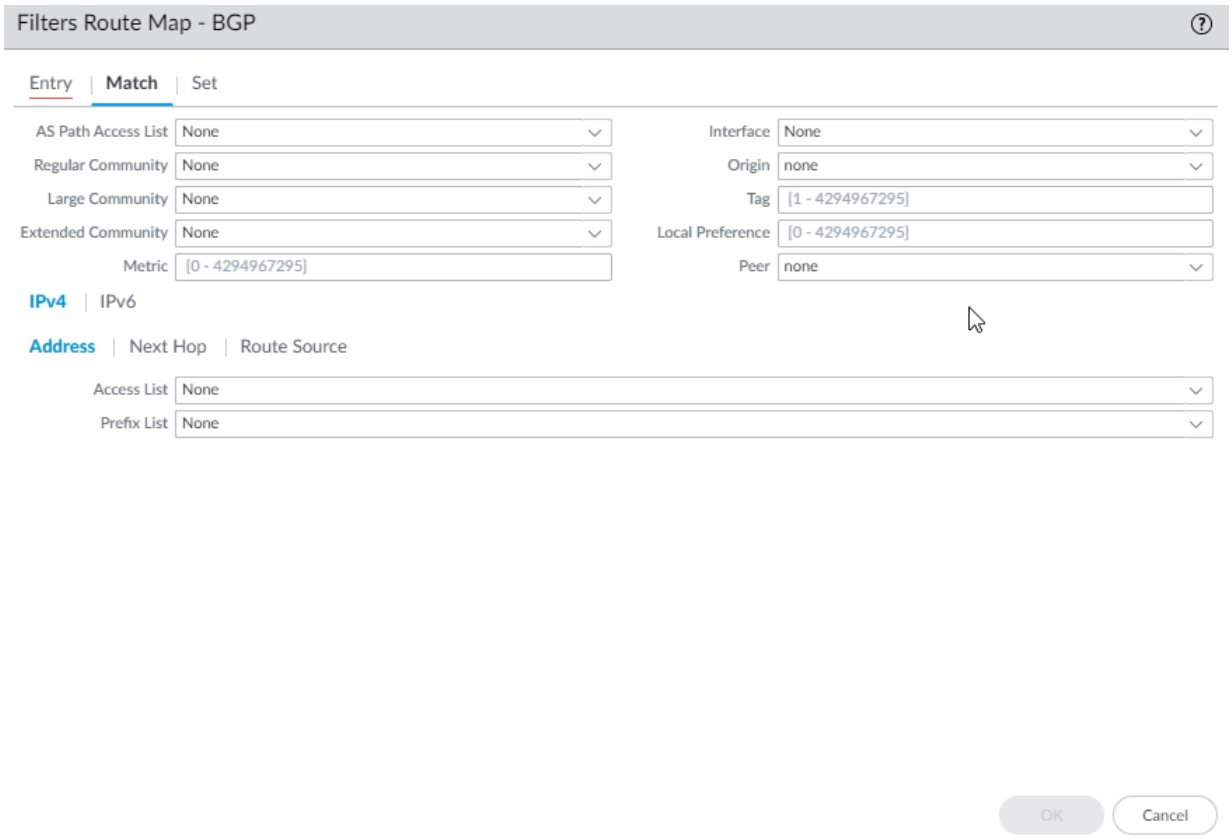
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Filters**（过滤器）。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**Filters Route Maps BGP**（筛选器路由映射 **BGP**）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入对路由映射的有用 **Description**（描述）。



4. **Add**（添加）一个路由映射，然后在 **Entry**（条目）选项卡中分配一个 **Seq**（序号）；范围为 1 - 65,535。

   分配间隔五个或更多数字的序号，以便将来可以有未使用的序号来插入其他条目。
5. 输入对条目（规则）的有用 **Description**（描述）。
6. 对于 **Action**（操作），请选择 **Deny**（拒绝）或 **Permit**（允许）。
7. 在**Match**（匹配）选项卡中，指定用于确定对哪些路由执行使用此路由映射的功能的条件。多个属性在逻辑上为 AND 关系，这意味着必须满足所有条件。

 ©2024 Palo Alto Networks, Inc.



- **AS Path Access List**（**AS** 路径访问列表）— 选择 AS 路径列表。默认为 **None**（无）。
- **Regular Community**（常规社区）— 选择一个社区列表。默认为 **None**（无）。
- **Large Community**（大型社区）— 选择大型社区列表。默认为 **None**（无）。
- **Extended Community**（扩展社区）— 选择一个扩展社区列表。默认为 **None**（无）。
- **Metric**（指标）— 输入 0 - 4,294,967,295 范围内的值。
- **Interface**（接口）— 从所有逻辑路由器的所有接口列表中选择一个本地接口。确保选择属于您所配置的逻辑路由器的接口。默认为 **None**（无）。提交时，防火墙会检查您选择的接口是否属于您所配置的逻辑路由器。
- **Origin**（起点）— 选择路由的起点：**ebgp**、**ibgp** 或 **incomplete**（不完整）。默认为 **None**（无）。
- **Tag**（标记）— 输入一个在网络中有意义的标记值，范围为 0 - 4,294,967,295。
- **Local Preference**（本地首选项）— 输入一个 0 - 4,294,967,295 范围内的值。
- **Peer**（对等）— 选择对等体名称或 **local (Static or Redistributed routes)**（本地（静态或重新分发路由））。默认为 **None**（无）。

8. 选择 **IPv4** 或 **IPv6** 以匹配各种类型的地址。如果选择 **IPv4**：
   - 在 **Address**（地址）选项卡中，选择一个**Access List**（访问列表）以指定要匹配的地址。

©2024 Palo Alto Networks, Inc.

- 选择一个**Prefix List**（前缀列表）以指定要匹配的地址。其将与从对等体接收到的前缀或从另一个协议重新分发到相应协议的前缀匹配。

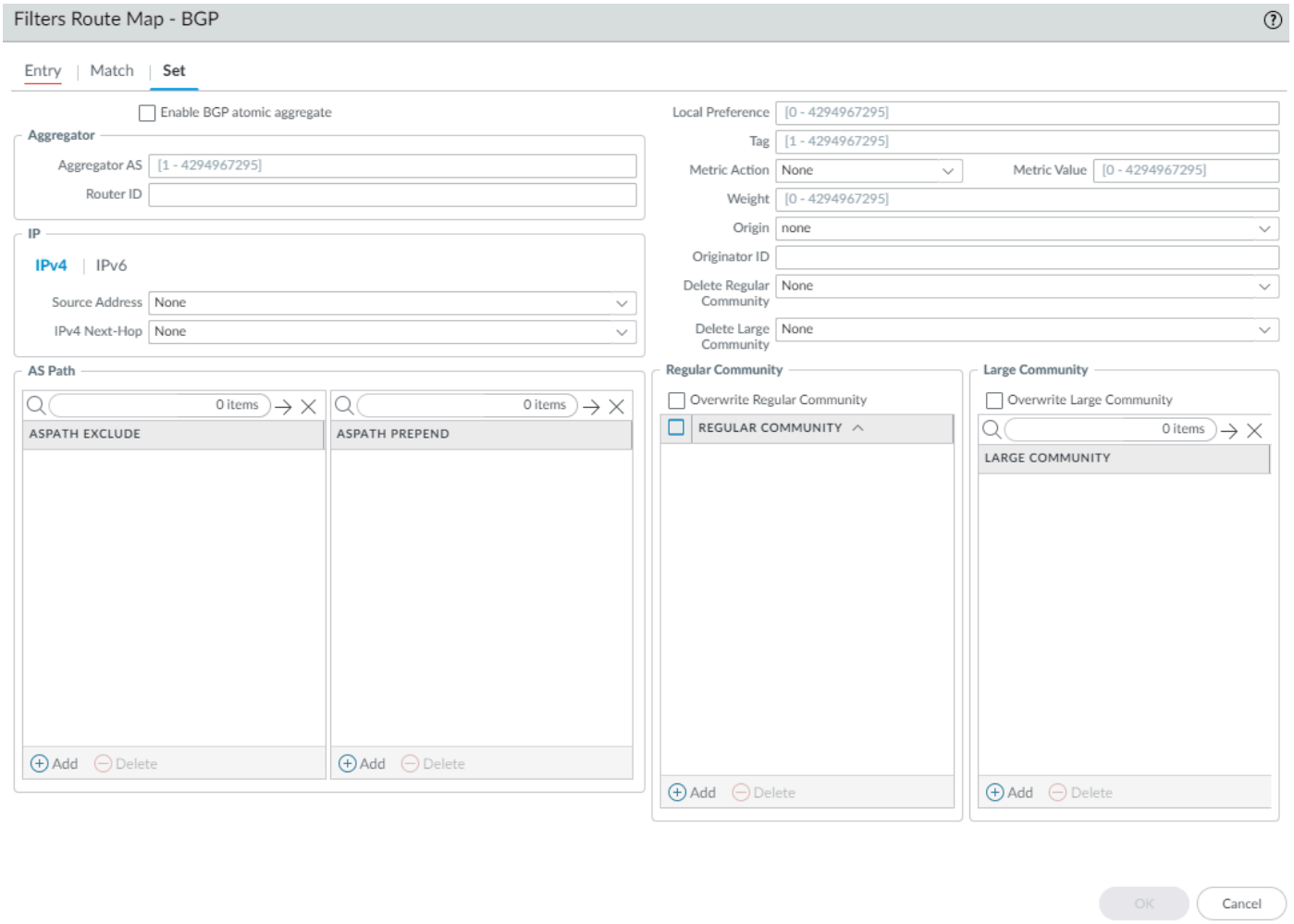
  如果同时指定了访问列表和前缀列表，则必须同时满足这两个要求（逻辑 *AND*）。
- 在 **Next Hop**（下一个跃点）选项卡中，选择一个**Access List**（访问列表）以指定要匹配得下一个跃点地址。
- 选择一个**Prefix List**（前缀列表）以指定要匹配的下一个跃点地址。
- 在 **Route Source**（路由来源）选项卡中，选择一个**Access List**（访问列表）以指定要匹配的路由来源 IP 地址。例如，访问列表可以允许地址为 192.168.2.2 的远距离对等体将路由通告到某个前缀。您可以使此 BGP 路由映射与路由的源地址 192.168.2.2 匹

 ©2024 Palo Alto Networks, Inc.

配，然后可能根据匹配对等地址 192.168.2.2 作为路由源来筛选路由，或者为匹配该路由来源的路由设置下一个跃点。

- 指定一个**Prefix List**（前缀列表），以指定要匹配的一个或多个源网络前缀。

9. 如果选择 **IPv6**：
   - 在 **Address**（地址）选项卡中，选择一个**Access List**（访问列表）以指定要匹配的地址。
   - 选择一个**Prefix List**（前缀列表）以指定要匹配的地址。
   - 在 **Next Hop**（下一个跃点）选项卡中，选择一个**Access List**（访问列表）以指定要匹配得下一个跃点地址。
10. 为符合匹配标准的路由 **Set**（设置）以下任何属性：



- **Enable BGP atomic aggregate**（启用 **BGP** 原子聚合）— 将路由标记为不太具体的路由，因为其已聚合。ATOMIC_AGGREGATE 是公认任意属性，它会警告路径上的 BGP 发言者，信息由于路由聚合已丢失，因此聚合路径可能不是到达目的地的最佳路径。当某个路由器被聚合器聚合时，聚合器会将其 Router-ID 附加到聚合路由的 AGGREGATOR-ID 属性中，并根据是否保留来自聚合路由器的 AS_PATH 信息设置 ATOMIC_AGGREGATE 属性。

 ©2024 Palo Alto Networks, Inc.

- **Aggregator AS**（聚合器 **AS**） — 输入聚合器 AS。聚合器属性包括 AS 编号和发起聚合路由的路由器的 IP 地址。IP 地址是执行路由聚合的路由器的路由器 ID。
- **Router ID**（路由器 **ID**） — 输入聚合器的路由器 ID（通常是回环地址）。
- **Local Preference**（本地首选项） — 输入要设置匹配路由的本地首选项；范围为 0 - 4,294,967,295。IBGP 更新数据包携带本地首选项，该首选项仅会通告给 IBGP 对等体。当有多个路由指向另一个 AS 时，防火墙会首选优先级最高的本地首选项。
- **Tag**（标记）— 设置标记；范围是 1 - 4,294,967,295。
- **Metric Action**（指标操作）— 选择一个操作：**set**（设置）、**add**（加）或 **subtract**（减）。您可以设置指定的指标值，或将指定的指标值添加到匹配路由的原始指标值，或从匹配路由的原始指标值中减去指定的指标值；默认为设置。选择加或减操作以调整指标值，从而确定匹配路由的优先级或降低其优先级。
- **Metric Value**（指标值） — 输入指标值，以设置匹配路由，或将其加到原始指标值中，或从原始指标值中减去此指标值；范围为 0 - 4,294,967,295。
- **Weight**（权重）— 设置权重（在本地应用；不会传播）;范围为 0 - 4,294,967,295。
- **Origin**（起点）— 设置匹配路线的起点：**ebgp**、**ibgp** 或 **incomplete**（不完整）（不清楚路由如何添加到 RIB）。
- **Originator ID**（发起方 **ID**） — 设置匹配路由的发起方的 IP 地址。
- **Delete Regular Community**（删除常规社区）— 选择要删除的常规社区。默认为 **None**（无）。
- **Delete Large Community**（删除大型社区）— 选择要删除的大型社区。默认为 **None**（无）。
- 选择 **IPv4** 或 **IPv6** 作为 AFI。
- 在 **IPv4** 选项卡中中，从所有逻辑路由器的所有源地址列表中选择要设置的**Source Address**（源地址），或选择 **None**（无）。提交时，防火墙会检查您选择的源地址是否属于您所配置的逻辑路由器。
- 选择 **IPv4 Next-Hop**（**IPv4** 下一个跃点），以设置：**none**（无）、**peer-address (Use Peer Address)**（对等地址（使用对等地址））或 **unchanged**（未更改）。
- 在 **IPv6** 选项卡中，选择 **IPv6 Nexthop Prefer Global Address**（**IPv6** 下一个跃点首选全局地址），以便在下一个跃点首选全局单播地址，而不是其他 IPv6 地址类型（链路本地地址、任意播地址或组播地址）。（默认情况下，所连接的对等体首选链路本地下一个跃点地址，而不是全局下一个跃点地址。）
- 在 **IPv6** 选项卡中中，从所有逻辑路由器的所有源地址列表中选择要设置的**Source Address**（源地址），或选择 **None**（无）。提交时，防火墙会检查您选择的源地址是否属于您所配置的逻辑路由器。
- 选择 **IPv6 Next-Hop**（**IPv6** 下一个跃点），以设置：**none**（无）或 **peer-address (Use Peer Address)**（对等地址（使用对等地址））。
- 在 AS 路径窗口中，**Add**（添加）最多四个要从匹配路由的 AS 路径中 **Exclude**（排除）的 AS 路径，以从联合中删除一个 AS。
- **Add**（添加）最多四个AS路径，以 **Prepend**（附加）到匹配路由的 AS 路径中（使通告中的路由变得不太合适）。

 ©2024 Palo Alto Networks, Inc.

- 在常规社区窗口中，选择 **Overwrite Regular Community**（覆盖常规社区）以覆盖常规社区。
- **Add**（添加）**Regular Community**（常规社区）以添加一个或多个常规社区。
- 在 Large Community（大型社区）窗口中，选择 **Overwrite Large Community**（覆盖大型社区）以覆盖大型社区。
- **Add**（添加）**Large Community**（大型社区）以添加一个或多个大型社区。
- 在常规社区窗口中，选择 **Overwrite Regular Community**（覆盖常规社区）以覆盖常规社区。
- **Add**（添加）**Regular Community**（常规社区）以添加一个或多个常规社区。
- 在 Large Community（大型社区）窗口中，选择 **Overwrite Large Community**（覆盖大型社区）以覆盖大型社区。
- **Add**（添加）**Large Community**（大型社区）以添加一个或多个大型社区。

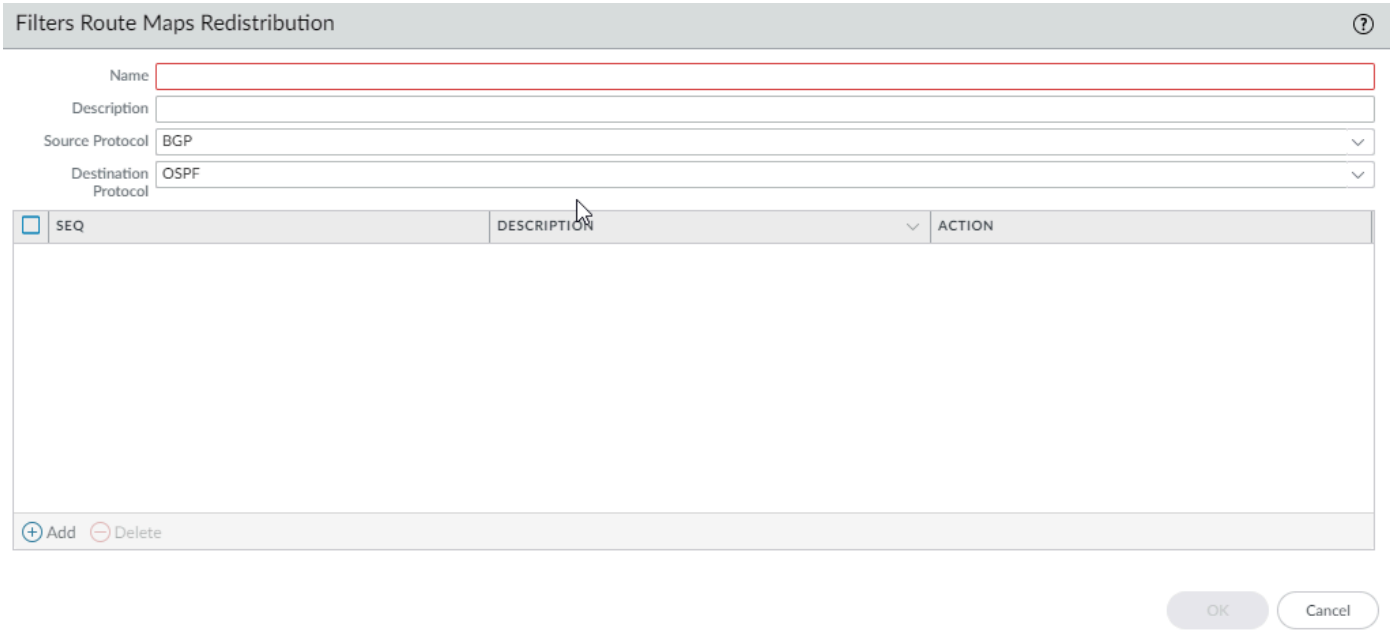
11. 单击 **OK**（确定）保存路由映射条目。（可选）添加更多条目。
12. 单击 **OK**（确定）保存 BGP 路由映射。

STEP 6 | 创建重新分发路由映射。

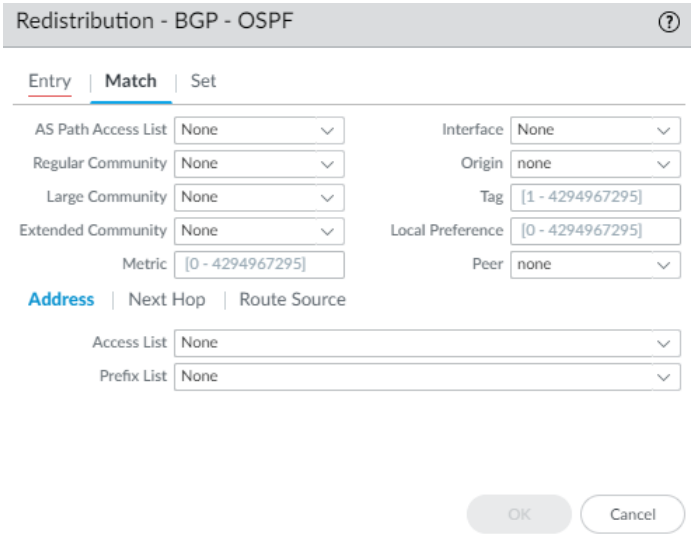
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Filters**（过滤器）。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**Filters Route Maps Redistribution**（筛选器路由映射重新分发）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入有用的 **Description**（说明）。
4. 要从 **Source Protocol**（源协议）重新分发，请选择 **BGP**、**OSPF**、**OSPFv3**、**RIP** 或 **Connected Static**（已连接静态）。源协议是将应用 匹配选项的位置。
5. 要将路由重新分发到 **Destination Protocol**（目标协议）或本地 RIB，请选择 **BGP**、**OSPF**、**OSPFv3**、**RIP** 或 **Rib**。目标协议是将应用设置选项的位置。下拉列表中

 ©2024 Palo Alto Networks, Inc.

可用的目标协议取决于所选的源协议。（此步骤显示了将 BGP 重新分发到 OSPF 的示例。）



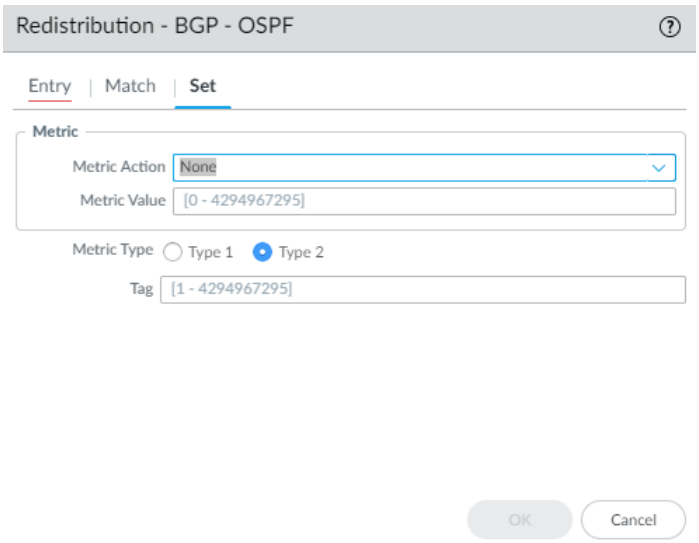
6. **Add**（添加）**Entry**（条目）并输入 **Seq**（序号）（范围为 1 - 65,535）。
7. 输入有用的 **Description**（说明）。
8. 选择 **Actions**（操作）：**Deny**（拒绝）或 **Permit**（允许）。
9. 选择 **Match**（匹配）选项卡以配置源协议的条件；此示例指定了要匹配的 BGP 属性。



10. 选择一个 **AS Path Access List**（**AS** 路径访问列表）；默认为 **None**（无）。
11. 选择一个**Regular Community**（常规社区）；默认为 **None**（无）。
12. 选择一个**Large Community**（大型社区）；默认为 **None**（无）。
13. 选择一个**Extended Community**（扩展社区）；默认为 **None**（无）。
14. 输入一个**Metric**（指标）值；范围为 0 - 4,294,967,295。

 ©2024 Palo Alto Networks, Inc.

15. 选择一个**Interface**（接口）；默认为 **None**（无）。
16. 选择路由的 **Origin**（起点）：**ebgp**、**ibgp** 或 **incomplete**（不完整）；默认为 **none**（无）。
17. 输入一个**Tag**（标记）值；范围为 1 - 4,294,967,295。
18. 输入一个**Local Preference**（本地首选项）值；范围为 0 - 4,294,967,295。
19. 选择一个**Peer**（对等体）名称或选择 **local (Static or Redistributed routes)**（本地（静态或重新分发路由））；默认为 **none**（无）。
20. **Address**（地址）选项卡显示路由中的目标地址。选择一个**Access List**（访问列表），以指定目标地址必须匹配才能重新分发的路由。默认为 **None**（无）。
21. 选择一个前缀列表，以指定目标地址必须匹配才能重新分发的路由。默认为 **None**（无）。
22. 选择 **Set**（设置）选项卡以配置要对匹配此规则的路由执行的操作，这些路由将被重新分发到目标协议。（在本例中，目标协议为 OSPF。）



23. 选择重新分发规则的 **Metric Action**（指标操作）：您可以 **set**（设置）指标值，将指定的**Metric Value**（指标值） **add**（加）到匹配路由的原始指标值中，或从匹配路由的原始指标值中 **subtract**（减）去指定的**Metric Value**（指标值）；默认为 **None**（无）。选择 **add**（加）或 **subtract**（减）操作以调整指标值，从而确定匹配路由的优先级或降低其优先级。

    例如，您可以使用重新分发将 IGP 的指标放入 BGP。指标会动态变化，您可以简单地将其值相加，而不是将其设置为绝对值。
24. 输入要设置、加入或从相应指标中减去的**Metric Value**（指标值）。范围为 0 - 4,294,967,295。
25. 选择 **Metric Type**（指标类型）：**Type 1**（类型 **1**）或**Type 2**（类型 **2**）（因为本例使用 OSPF 作为目标协议）。
26. 指定一个**Tag**（标记）值；范围为 1 - 4,294,967,295。
27. 单击 **OK**（确定）保存规则。（可选）添加更多规则。
28. 单击 **OK**（确定），保存重新分发路由映射。

©2024 Palo Alto Networks, Inc.

在高级路由引擎上配置 OSPFv2

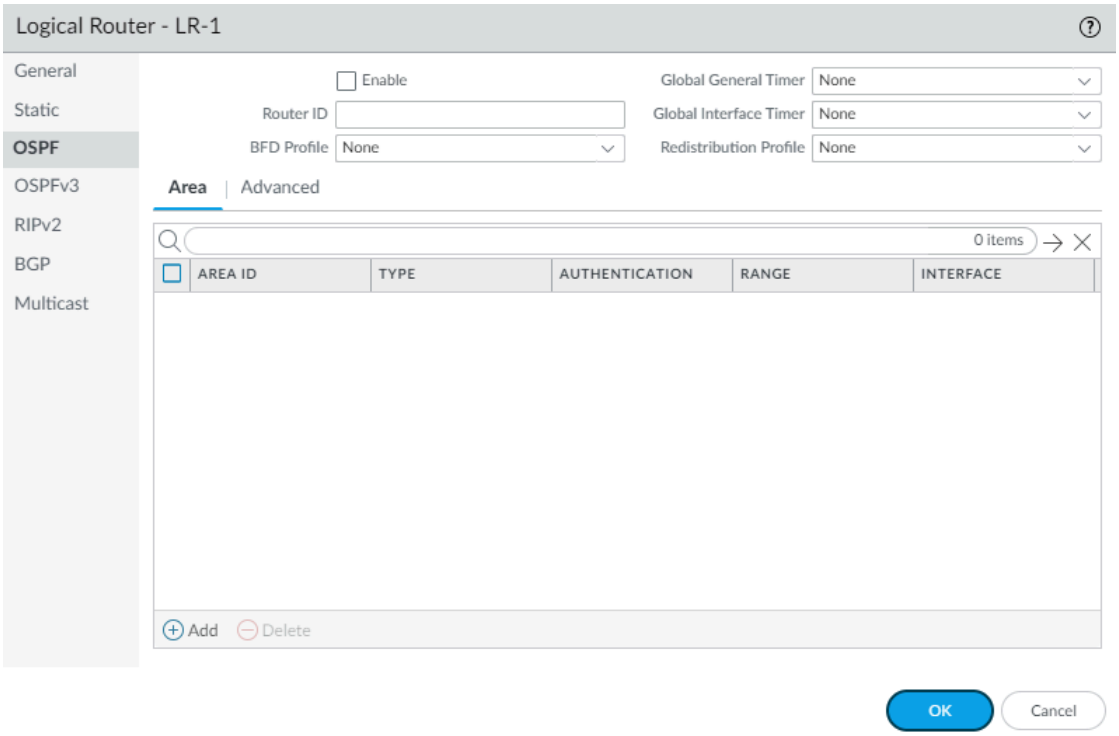
高级路由引擎支持 OSPFv2，而 OSPFv2 仅支持 IPv4 寻址。在配置 OSPFv2 之前，您应了解OSPF 概念。

请考虑可应用于 OSPF 的 OSPF Routing Profiles（OSPF 路由配置文件）和筛选器，从而节省配置时间并确保一致性。您可以提前创建配置文件和筛选器，也可以在配置 OSPFv2 时创建。

STEP 1 | 配置逻辑路由器.

STEP 2 | 启用 OSPFv2 并配置常规设置。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择并**Enable**（启用）**OSPF**。



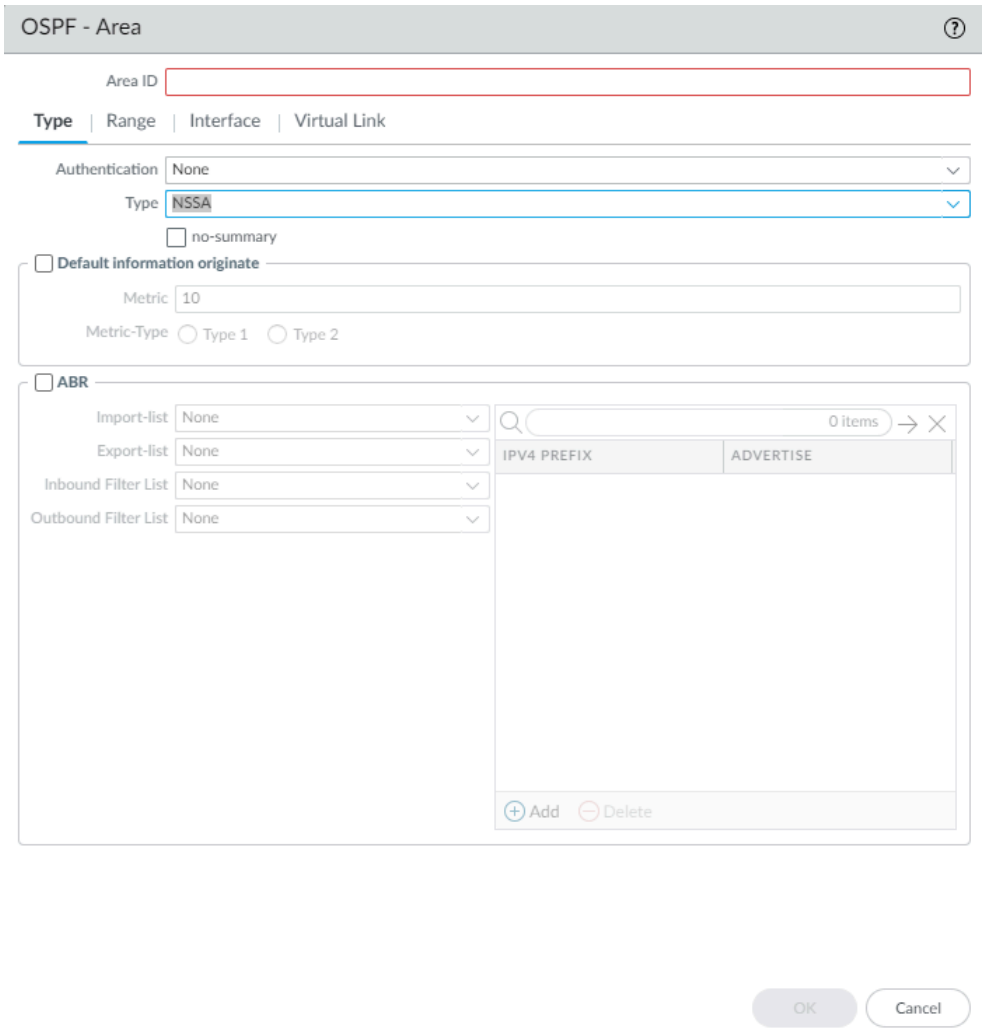
3. 以 IPv4 地址格式输入 **Router ID**（路由器 **ID**）。
4. 如果要将 BFD 应用于 OSPF，请选择所创建的 **BFD Profile**（**BFD** 配置文件），或选择默认配置文件，或新建一个 BFD 配置文件。默认值是 **None (Disable BFD)**（无（禁用 **BFD**））。
5. 选择 OSPF **Global General Timer**（全局通用计时器）配置文件或新建一个。
6. 选择 OSPF **Global Interface Timer**（全局接口计时器）配置文件或新建一个。
7. 选择 OSPF **Redistribution Profile**（重新分发配置文件）或新建一个，以将 IPv4 静态路由、互联路由、RIPv2 路由、IPv4 BGP 路由或 IPv4 默认路由重新分发到 OSPF。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 创建 OSPF 区域并根据区域类型指定特征。

1. 选择 **Area**（区域），然后 **Add**（添加）以 **Area ID**（区域 **ID**）（格式为 x.x.x.x）识别的区域。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. 选择 **Type**（类型），选项卡，在 **Authentication**（身份验证）部分中，选择身份验证配置文件或新建一个身份验证配置文件。
3. 选择区域 **Type**（类型）：
   - **Normal**（一般）— 没有限制；该区域可以承载所有类型的路径（区域内路径、区域间路径和外部路径）。
   - 存根— 区域没有出口。要到达该区域以外的目的地，流量必须通过连接到其他区域的区域边界路由器(ABR)。
   - **NSSA**（非完全末节区域）— NSSA 实现了末节或完全末节功能，但包含自治系统边界路由器(ASBR)。ASBR 生成的 7 类 LSA 由 ABR 转换为 5 类，并涌到 OSPF 域的其余部分。（下图显示选中了 NSSA。）
4. （仅限末节和 NSSA 区域）选择 **no-summary**（无摘要）可防止该区域接收 3 类摘要 LSA，从而减少该区域的流量。
5. （仅限 NSSA 区域）选择 **Default information originate**（默认信息来源）可使 OSPF 源自默认路由。
   - 输入默认路由的 **Metric**（指标）；范围为 1 - 16,777,214；默认为 10。
   - 选择 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）。类型 E1 的成本是到达该路由的外部成本加上内部成本的总和。类型 E2 仅为该路由的外部成本。例如，当您想要对同一外部路由进行负载均衡时，这可能很有用。

 ©2024 Palo Alto Networks, Inc.



6. 选择 **ABR** 以筛选进入或离开该区域的前缀，然后配置以下筛选器：
   - 选择 **Import-list**（导入列表）或新建一个访问列表，以根据 IPv4 源地址将来自另一个路由器的网络路由筛选到 LSA 中的区域，从而允许或阻止将路由添加到全局 RIB（将访问列表的目标地址留空）。
   - 选择 **Export-list**（导出列表）或新建一个访问列表，以筛选源自该区域的网络路由，从而允许或阻止将路由通告到其他区域。
   - 选择一个**Inbound Filter List**（入站筛选器列表）或新建一个前缀列表，以筛选进入该区域的网络前缀。
   - 选择一个**Outbound Filter List**（出站筛选器列表）或新建一个前缀列表，以筛选源自该区域的网络前缀，从而防止将路由通告到其他区域。
   - 如果区域的**Type**（类型）为 **NSSA** 并且选择了 **ABR**，则 **Add**（添加）一个 **IPv4 Prefix**（**IPv4** 前缀），一组外部子网汇总到 7 类 LSA，然后在选择 **Advertise**（通告）时将其转换为 5 类 LSA 并向骨干区域通告。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 指定该区域的网络范围。

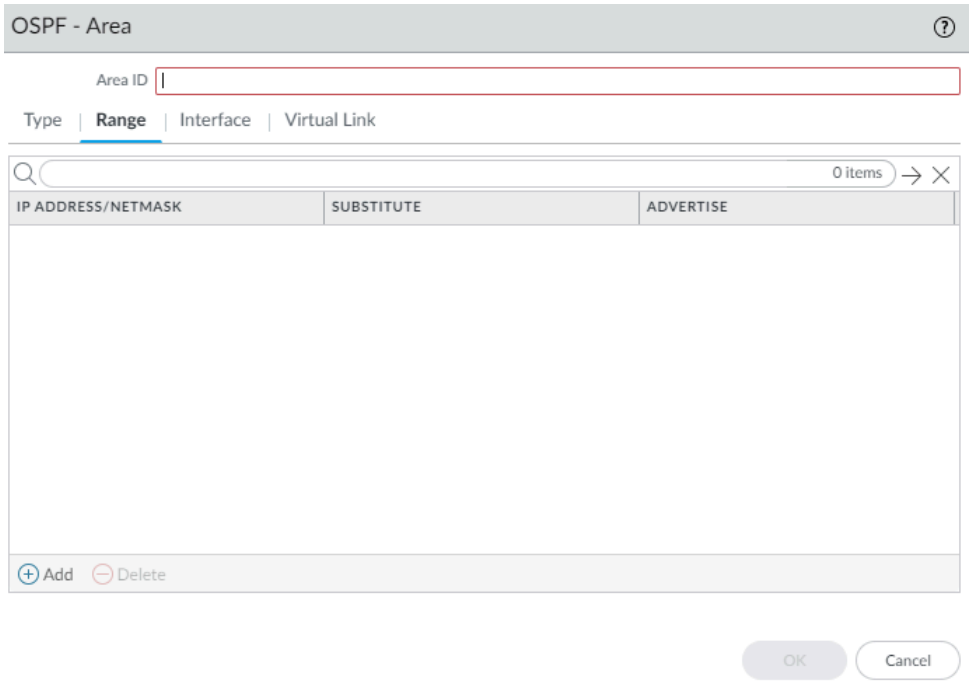
1. 选择 **Range**（范围），然后 **Add**（添加）**IP Address/Netmask**（**IP** 地址/网络掩码）（用于汇总该区域的路由）。因此，如果该区域包含至少一个区域内网络（即，使用路由器或网络 LSA 描述），则路由信息与此范围匹配的 3 类摘要 LSA 将被通告到骨干区域。

   查看该区域的 *LSDB* 中已学习的路由，并使用此范围来汇总路由，从而减少 *LSA* 流量。

2. 输入 **Substitute**（替代） IP 地址/网络掩码，以便在骨干区域中包含至少一个来自上一步中指定的 **IP** 地址/网络掩码的区域内网络时，将具有此 IP 地址/网络掩码 的 3 类摘要 LSA 通告到骨干区域。

   使用替代 *IP* 地址/网络掩码，将专用地址转换为公共地址。如果禁用了通告，则替代地址将不起作用。

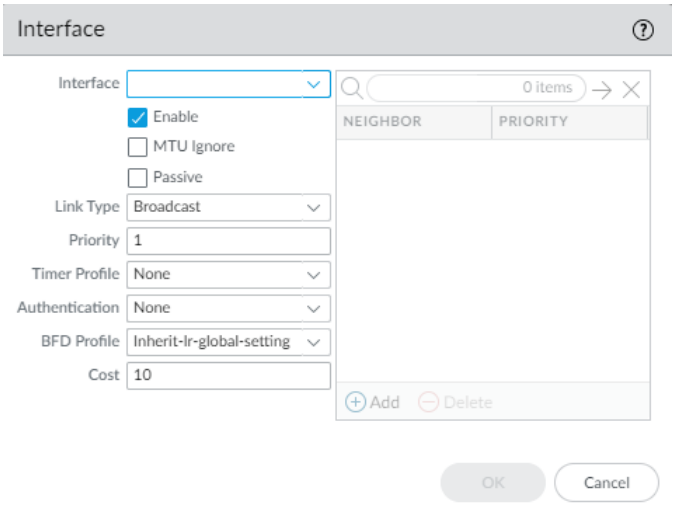
3. 选择 **Advertise**（通告），以发送与子网匹配的链路状态通告(LSA)；默认为启用。



 ©2024 Palo Alto Networks, Inc.

STEP 5 | 配置要在该区域中包含的每个接口。

1. 选择一个 **Interface**（接口）以 **Add**（添加），然后 **Enable**（启用）。
2. 选择 **MTU Ignore**（**MTU** 忽略），以在尝试建立邻接时忽略最大传输单位(MTU)的不匹配（默认为禁用；进行 MTU 匹配检查）。RFC 2328 将接口 MTU 定义为“可以发送到相关接口而不会产生碎片的最大 IP 数据报的大小（以字节为单位）”。
3. 选择 **Passive**（被动）以允许通告接口的网络，但不在该接口上建立邻居关系；这对于叶接口很有用。

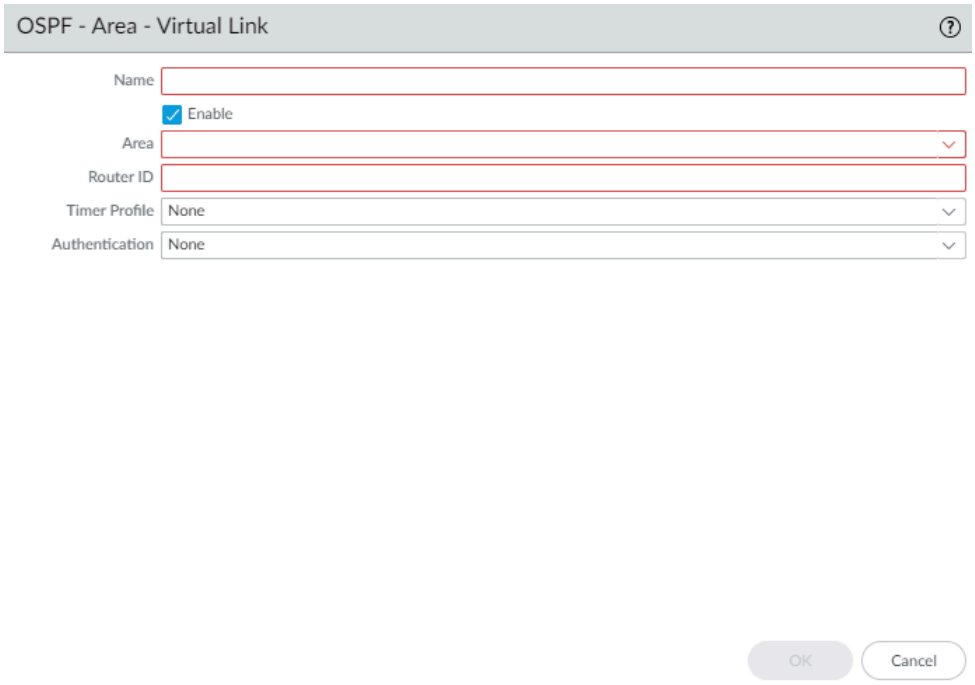


4. 选择 **Link Type**（链路类型）：
   - **Broadcast**（广播）— 通过组播 OSPF 呼叫消息自动发现所有能够通过接口访问的邻居（如 Ethernet 接口）。
   - **p2p**（点对点）— 自动发现邻居。
   - **p2mp**（点对多点）— 必须手动定义邻居：**Add**（添加）可通过此接口访问的所有邻居的 **Neighbor**（邻居）IP 地址，并添加要选作指定路由器(DR)或备份 DR 的每个邻居的 **Priority**（优先级）；范围为 0 - 255；默认值为 1。
5. 输入要选作指定路由器(DR)或备份 DR(BDR)的接口的 OSPF **Priority**（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。
6. 选择要应用于接口的**Timer Profile**（计时器配置文件），或新建一个 OSPF 接口计时器配置文件。此 OSPF 接口计时器配置文件将覆盖应用于 OSPF 的全局接口计时器。
7. 选择要应用于接口的**Authentication Profile**（身份验证配置文件），或新建一个 OSPF 接口身份验证配置文件。此身份验证配置文件将覆盖应用于类型选项卡中区域的身份验证配置文件。
8. 默认情况下，接口将为 OSPF 继承应用于逻辑路由器的 BFD 配置文件 **(Inherit-lr-global-setting)**。或者，选择默认配置文件，选择其他 **BFD Profile**（**BFD** 配置文件），新建一个 BFD 配置文件，或选择 **None (Disable BFD)**（无（禁用 **BFD**））为接口禁用 BFD。
9. 输入接口的 OSPF **Cost**（成本），这会影响路由选择；范围为 1 - 65,5535；默认为 10。在选择路径时，累积成本较低的路由（所用每个接口的附加成本）优先于累积成本较高的路由。
10. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 如果 ABR 没有到骨干区域的物理链路，请在具有到骨干区域的物理链路的同一区域内配置到邻居 ABR 的虚拟链路。

1. 选择 **Virtual Link**（虚拟链路）。
2. 按 **Name**（名称）**Add**（添加）虚拟链路。
3. **Enable**（启用）虚拟链路。



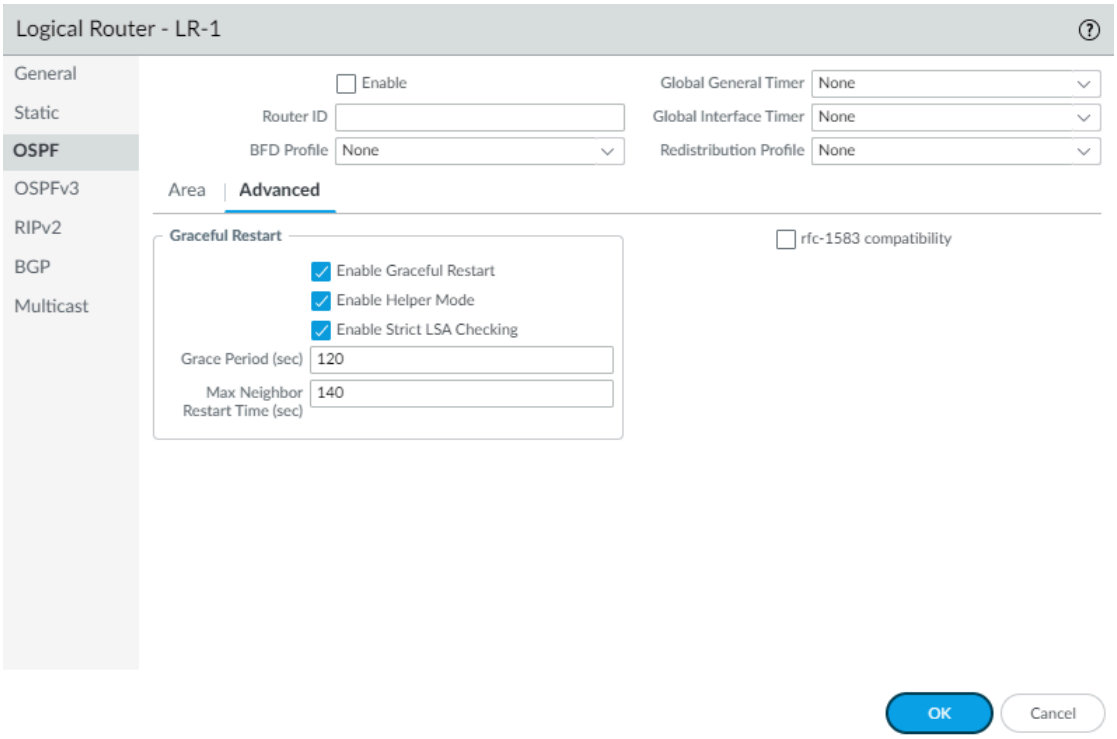
4. 选择具有到骨干区域的物理链路的邻居 ABR 所在的中转 **Area**（区域）。
5. 输入虚拟链路远程端的邻居 ABR 的**Router ID**（路由器 **ID**）。
6. 选择一个**Timer Profile**（计时器配置文件）或新建一个计时器配置文件，以应用于虚拟链路。此 OSPF 接口计时器配置文件将覆盖应用于 OSPF 的全局接口计时器和应用于该接口的 OSPF 接口计时器配置文件。
7. 选择一个**Authentication**（身份验证）配置文件或新建一个身份验证配置文件，以应用于虚拟链路。此身份验证配置文件将覆盖应用于类型选项卡中区域的身份验证配置文件和应用于该接口的身份验证配置文件。
8. 单击 **OK**（确定）。

STEP 7 | 单击 **OK**（确定）以保存区域。

©2024 Palo Alto Networks, Inc.

STEP 8 | 为 OSPFv2 配置 OSPF Graceful Restart（OSPF 正常重启）和 RFC 1583 兼容性。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择相应逻辑路由器。
2. 选择 **OSPF** > **Advanced**（高级）。
3. 选择 **rfc-1583** 兼容性以强制兼容 RFC 1583，RFC 1583 允许使用一个到 OSPF 路由表中自治系统边界路由器(ASBR)的最佳路由。默认为禁用，这意味着 OSPF 路由表可以在路由表中维护多个 AS 内部路径，从而防止路由循环。



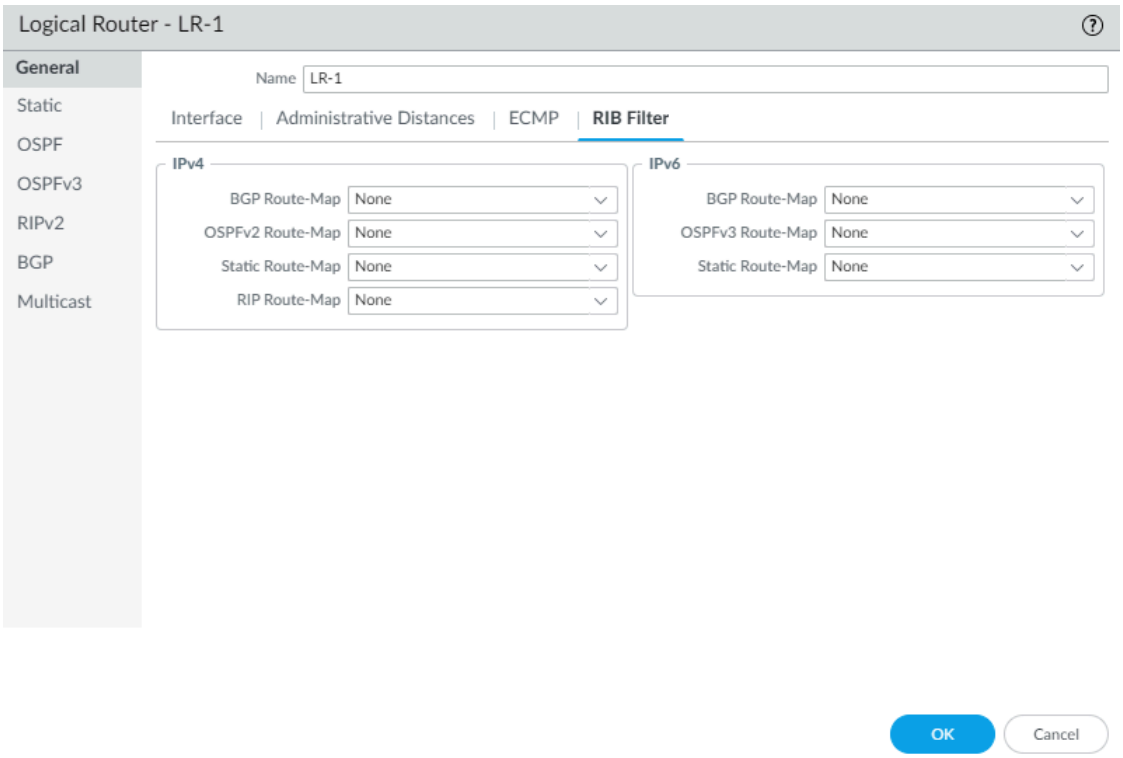
4. **Enable Graceful Restart**（启用正常重启），为逻辑路由器启用 OSPF Graceful Restart（OSPF 正常重启）。默认为启用。
5. **Enable Helper Mode**（启用帮助程序模式），使逻辑路由器能够在正常重启帮助程序模式下运行。默认为启用。
6. **Enable Strict LSA Checking**（启用严格的 **LSA** 检查）可使帮助程序路由器停止执行帮助程序模式，并在链路状态通告指示网络拓扑发生变化时导致正常重启过程停止。默认为启用。
7. 指定 **Grace Period (sec)**（宽限期（秒））— 防火墙关闭或不可用时，逻辑路由器将执行正常重启的时限（秒数）；范围为 5 - 1,800；默认为 120。
8. 指定 **Max Neighbor Restart Time (sec)**（最大邻居重启时间（秒））；范围为 5 - 1,800；默认为 140。
9. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 配置区域内筛选以确定在全局 RIB 中放置哪些 OSPFv2 路由。

您可能会学习并重新分发 OSPFv2 路由，但不希望将他们放置在全局 RIB 中；您可能希望仅允许在全局 RIB 中放置特定的 OSPFv2 路由。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择 **RIB Filter**（**RIB** 筛选器）。
3. 要筛选全局 RIB 的 **IPv4** OSPFv2 路由，请在 **OSPFv2 Route-Map**（**OSPFv2** 路由映射）中选择所创建的重新分发路由映射，或者新建一个重新分发路由映射，其中源协议为 OSPF，目标协议为 RIB。



4. 单击 **OK**（确定）。

STEP 10 | （可选）更改逻辑路由器内的 OSPF 区域内、区域间和外部路由的默认管理距离。

STEP 11 | **Commit**（提交）。

STEP 12 | 查看 OSPFv2 和链路状态数据库(LSDB)的高级路由信息。PAN-OS CLI 快速入门指南在 CLI 速查表中列出了以下命令：Networking（下一步：网络）。

 ©2024 Palo Alto Networks, Inc.

创建 OSPF 路由配置文件

高级路由引擎支持 OSPFv2；创建以下配置文件以应用于该协议，使配置更加简单、一致。这些配置文件可以在多个逻辑路由器和虚拟系统中使用。本主题将介绍这些配置文件以及如何配置它们。

- **OSPF Global Timer Profiles**（**OSPF** 全局计时器配置文件） — 为 OSPFv2 区域配置链路状态通告(LSA)最短到达时间和最短路径优先(SPF)计时器。在 OSPF 常规配置中应用配置文件。
- **OSPF Interface Authentication Profiles**（**OSPF** 接口身份验证配置文件） — 使用密码或 MD5 指定身份验证方式；将此类配置文件应用于 OSPF 区域、接口和/或虚拟链路。
- **OSPF Interface Timer Profiles**（**OSPF** 接口计时器配置文件） — 配置与接口操作相关的计时器，例如 OSPF 呼叫和正常重启。将此类配置文件应用于 OSPF 常规配置、接口和/或虚拟链路。
- **OSPF Redistribution Profiles**（**OSPF** 重新分发配置文件） — 指定如何重新分发 IPv4 静态路由、互联路由、BGP IPv4 路由、RIPv2 路由以及指向 OSPF 的 IPv4 默认路由。在 OSPF 常规配置中应用配置文件。

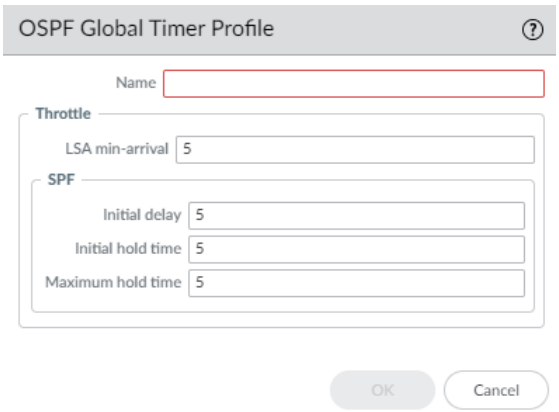
STEP 1 | 创建 OSPF 全局计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPF**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPF Global Timer Profile**（**OSPF** 全局计时器配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入 **LSA min-arrival**（**LSA** 最短到达时间），即同一个 LSA（相同通告路由器 ID、相同 LSA 类型和相同 LSA ID）的两个实例传输的最短间隔时间（秒）。如果同一个 LSA 比配置的时间间隔更早到达，则丢弃该 LSA。范围为 1 - 10；默认为 5。LSA 最短到达时间相

 ©2024 Palo Alto Networks, Inc.

当于 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。

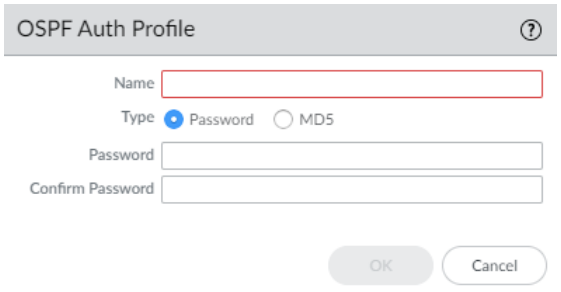
4. 在 SPF 区域中，输入从逻辑路由器接收到拓扑变更到其执行最短路径优先(SPF)计算之间的 **Initial delay**（初始延迟）（秒）；范围为 0 - 600；默认为 5。值越低 OSPF 重新收敛速度越快。与防火墙对等的路由器应使用相同的延迟值来优化收敛时间。
5. 输入连续 SPF 计算之间的 **Initial hold time**（初始保持时间）（秒）；范围为 0 - 600；默认为 5。
6. 输入 **Maximum hold time**（最大保持时间）（秒），这是保持时间限制到保持稳定的最大值；范围为 0 到 600；默认为 5。



7. 单击 **OK**（确定）。

STEP 2 | 创建 OSPF 接口身份验证配置文件。

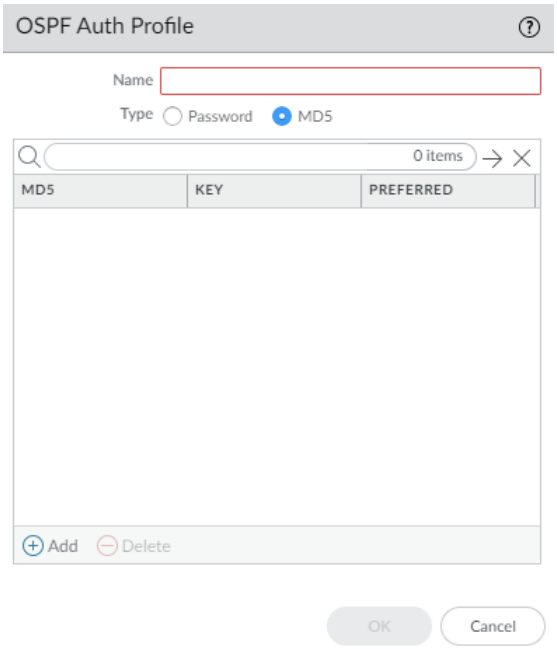
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPF**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPF Auth Profile**（**OSPF** 身份验证配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 选择身份验证 **Type**（类型）：**Password**（密码）或 **MD5**。
   - 如果选择 **Password**（密码），请输入 **Password**（密码）（最多八个字符并 **Confirm Password**（确认密码）。



   - 如果选择 **MD5**，请 **Add**（添加）MD5 密钥 ID（范围为 0 - 255）和 **Key**（密钥）（最多 16 个字母数字字符）。选择 **Preferred**（首选），以首选 MD5 密钥而不是其他 MD5 密钥。在提交过程中，防火墙将从上到下遍历密钥列表，而首选密钥会

 ©2024 Palo Alto Networks, Inc.

移至列表顶部；因此将使用顶部的首选密钥。（换句话说，如果您选择了多个首选 MD5 密钥，则最后一个被选为首选的密钥就是首选密钥。）

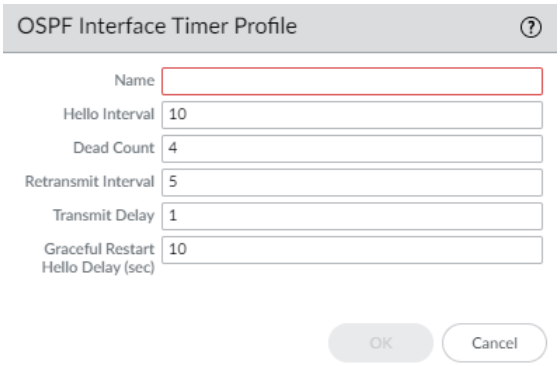


4. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 创建 OSPF 接口计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPF**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPF Interface Timer Profile**（**OSPF** 接口计时器配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。

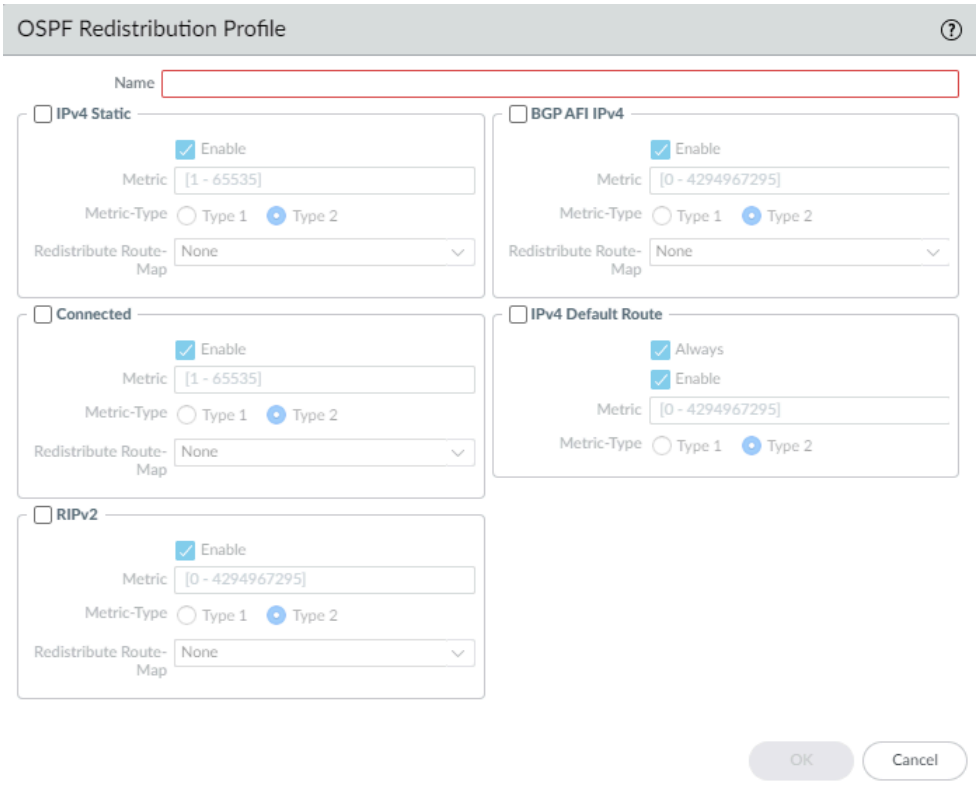


3. 输入 **Hello Interval**（呼叫间隔），即防火墙从接口发出呼叫数据包以维持邻居关系的间隔（秒）；范围为 1 - 3600；默认为 10。
4. 输入 **Dead Count**（间隔次数），即在 OSPF 认为邻居关闭之前，邻居可以发生呼叫间隔的次数，而无需 OSPF 接收邻居的呼叫数据包；范围为 3 - 20；默认为 4。
5. 输入 **Retransmit Interval**（重传间隔），即 LSA 重新传输到相邻路由器所间隔的秒数；范围是 1 - 1800；默认为 5。
6. 输入 **Transmit Delay**（传输延迟），即通过接口传输链路状态更新数据包所需的秒数。更新数据包中的链路状态通告将在其被传输之前按此数字递增其存在时间；范围是 1 - 1800；默认为 1。
7. 输入 **Graceful Restart Hello Delay (sec)**（正常重启呼叫延迟（秒））；当配置主动/被动高可用性时，该延迟适用于 OSPF 接口。正常重启呼叫延迟是防火墙以 1 秒间隔发送宽限 LSA 数据包期间的时间长度。在此期间，不会从重新启动防火墙发送任何呼叫数据包。在重新启动期间，间隔计时器（其值等于呼叫间隔乘以间隔次数）也会倒计时。如果间隔计时器太短，邻居将会在平稳重新启动期间因呼叫延迟而关闭。因此，建议将间隔计时器的值设置为正常重启呼叫延迟值的至少四倍。例如，呼叫间隔为 10 秒，间隔次数为 4 次，则间隔计时器为 40 秒。如果将正常重启呼叫延迟设置为 10 秒，则呼叫数据包的 10 秒延迟正好在间隔计时器的 40 秒内，因此相邻设备在正常重启期间不会超时。范围为 1 - 10；默认为 10。
8. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 创建 OSPF 重新分发配置文件，以指定要重新分发到 OSPF 的 IPv4 静态路由、互联路由、BGP IPv4 路由、RIPv2 路由和默认 IPv4 路由的任意组合。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPF**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPF Redistribution Profile**（**OSPF** 重新分发配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。



3. 选择 **IPv4 Static**（**IPv4** 静态），以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 IPv4 静态部分。
   - 指定适用于被重新分发给 OSPF 的静态路由的 **Metric**（指标）（范围为 1-65,535）。
   - 指定 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）（OSPF 成本）或 **Type 2**（类型 **2**）（默认）。如果有两条指向目的地的静态路由，并且它们的成本相同，则类型 2 路由优先于类型 1 路由。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制将哪些 IPv4 静态路由重新分发到 OSPF。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发

 ©2024 Palo Alto Networks, Inc.

的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。

4. 选择 **Connected**（互联），以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的互联部分。
   - 输入适用于被重新分发给 OSPF 的连接路由的**Metric**（指标）（范围为 1- 65,535）。
   - 指定 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）（默认）。类型 E1 的成本是到达该路由的外部成本加上内部成本的总和。类型 E2 仅为该路由的外部成本。例如，当您想要对同一外部路由进行负载均衡时，这可能很有用。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制将哪些互联路由重新分发到 OSPF。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。
5. 选择 **RIPv2**，以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 RIPv2 部分。
   - 指定适用于被重新分发给 OSPF 的 RIPv2 路由的**Metric**（指标）（范围为 0-4,294,967,295）。
   - 指定 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）（默认）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制将哪些 RIPv2 路由重新分发到 OSPF。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。
6. 选择 **BGP AFI IPv4**，以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 BGP AFI IPv4 部分。
   - 指定适用于被重新分发给 OSPF 的 BGP 路由的**Metric**（指标）（范围为 0-4,294,967,295）。
   - 指定 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）（默认）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制将哪些 BGP IPv4 路由重新分发到 OSPF。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发

 ©2024 Palo Alto Networks, Inc.

的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。

7. 选择 **IPv4 Default Route**（**IPv4** 默认路由），以允许配置该配置文件的这一部分。
   - 选择 **Always**（始终），以始终将 IPv4 默认路由重新分发到 OSPF；此选项默认启用。
   - **Enable**（启用）配置文件的 IPv4 默认路由部分。
   - 指定适用于被重新分发给 OSPF 的默认路由的**Metric**（指标）（范围为 0-4,294,967,295）。
   - 指定 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）（默认）。
8. 单击 **OK**（确定）。

STEP 5 | **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

在高级路由引擎上配置 OSPFv3

高级路由引擎支持 OSPFv3，而 OSPFv3 仅支持 IPv6 寻址。在配置 OSPFv3 之前，您应了解OSPF 概念。

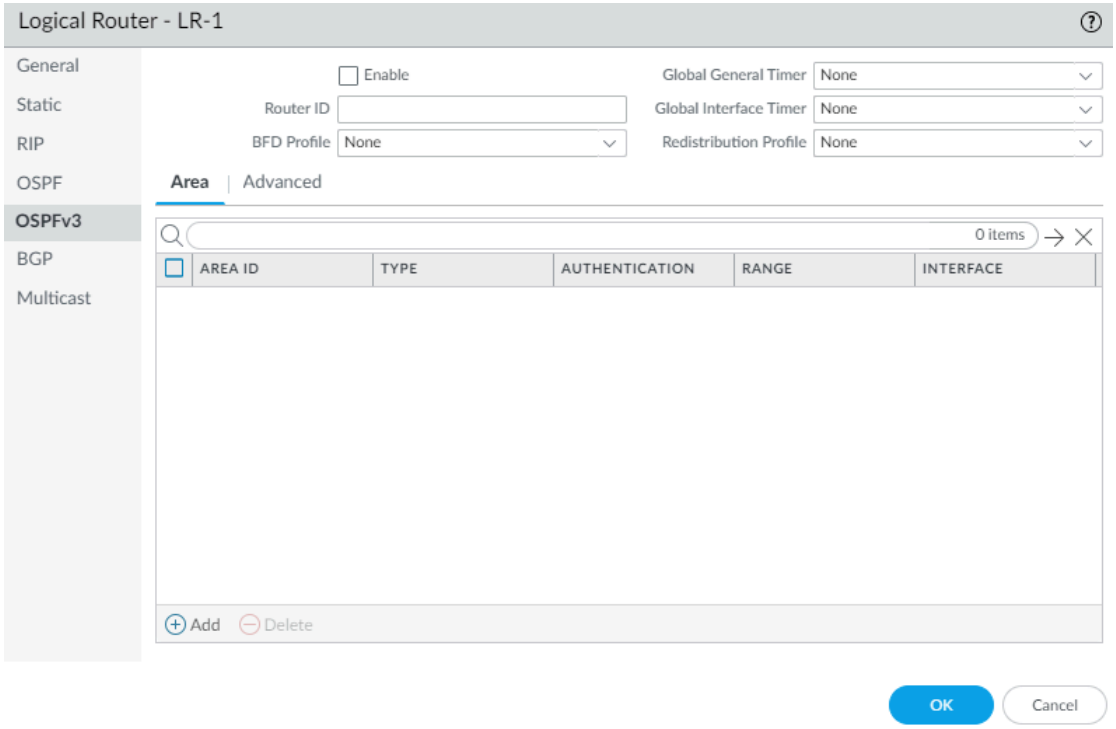
请考虑可应用于 OSPFv3 的 OSPFv3 Routing Profiles（OSPFv3 路由配置文件）和筛选器，从而节省配置时间并确保一致性。您可以提前创建配置文件和筛选器，也可以在配置 OSPFv3 时创建。

STEP 1 | 配置逻辑路由器.

©2024 Palo Alto Networks, Inc.

STEP 2 | 配置常规 OSPFv3 路由选项。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择相应逻辑路由器。
2. 选择并**Enable**（启用）**OSPFv3**。



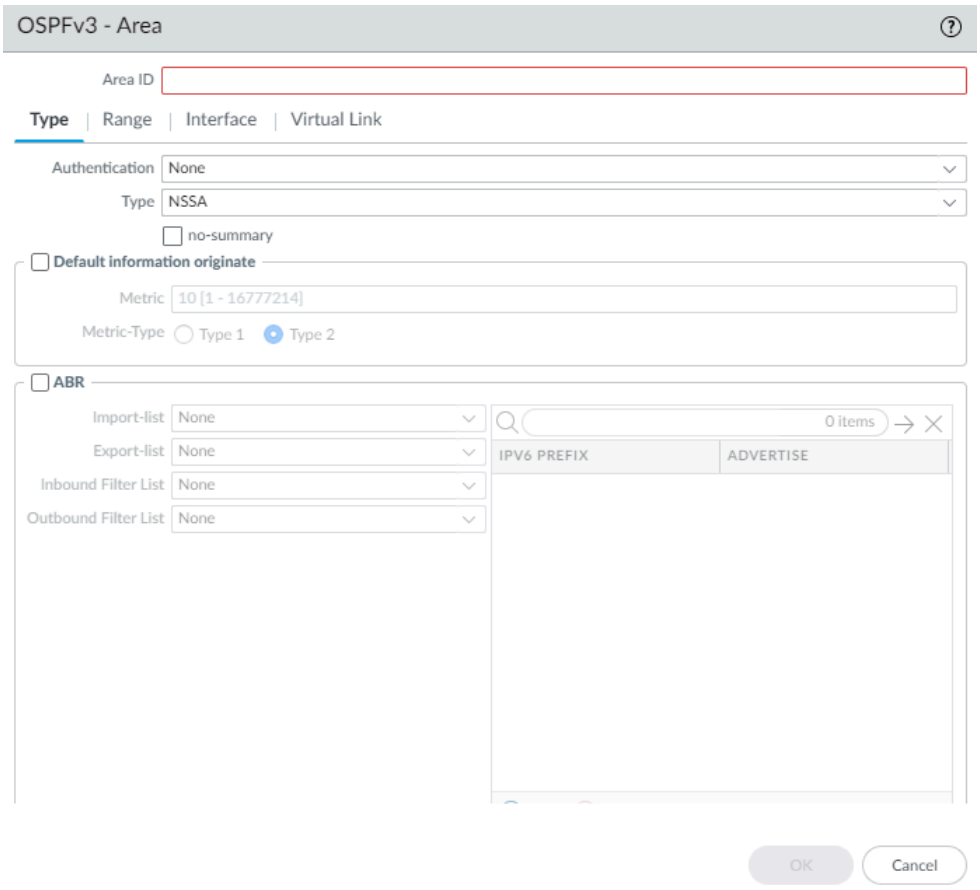
3. 为逻辑路由器的 OPSFv3 分配 **Router ID**（路由器 **ID**）（通常为 IPv4 地址，即使 OSPFv3 用于 IPv6 寻址），确保路由器 ID 具有唯一性。
4. 如果要将 BFD 应用于OSPFv3，请选择所创建的 **BFD Profile**（**BFD** 配置文件），或选择默认配置文件，或新建一个 BFD 配置文件，以应用于属于逻辑路由器的所有 OSPFv3 接口。默认值是 **None (Disable BFD)**（无（禁用 **BFD**））。
5. 选择一个**Global General Timer**（全局通用计时器）配置文件或新建一个，以设置 SPF 限制计时器，并设置同一链路状态通告(LSA)的到达实例之间的最短间隔时间。
6. 选择一个**Global Interface Timer**（全局接口计时器）配置文件或新建一个，以设置呼叫间隔、重新传输间隔等设置。
7. 选择一个**Redistribution Profile**（重新分发配置文件）或新建一个，以将 IPv6 静态路由、互联路由、IPv6 BGP路由或 IPv6 默认路由重新分发到 OSPFv3。
8. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 创建 OSPFv3 区域并根据区域类型指定特征。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择相应逻辑路由器。
2. 选择 **OSPFv3** > **Area**（区域），然后按 **Area ID**（区域 **ID**）（一个 IPv4 地址）**Add**（添加）区域。
3. 在 **Type**（类型）选项卡中，为该区域选择一个**Authentication**（身份验证）配置文件或新建一个。
4. 指定区域 **Type**（类型）：
   - 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。要到达该区域以外的目的地，流量必须通过连接到其他区域和区域 0 的区域边界路由器(ABR)。
   - **NSSA**（非完全末节区域）— 流量仅可通过非 OSPF 路由直接离开此区域。
5. （仅限末节和 NSSA 区域）选择 **no-summary**（无摘要）可防止该区域接收 3 类摘要 LSA，从而减少该区域的流量。
6. （仅限 NSSA 区域）选择 **Default information originate**（默认信息来源）可使 OSPFv3 源自默认路由。
   - 输入默认路由的 **Metric**（指标）；范围为 1 - 16,777,214；默认为 10。
   - 选择 **Metric-Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）。类型 E1 的成本是到达该路由的外部成本加上内部成本的总和。类型 E2 仅为该路由的外部成本。例如，当您想要对同一外部路由进行负载均衡时，这可能很有用。

 ©2024 Palo Alto Networks, Inc.



7. 如果要配置筛选选项，请选择 **ABR**。
8. 选择一个**Import-list**（导入列表）或新建一个访问列表，以筛选 3 类 LSA；适用于作为 3 类摘要 LSA 宣告进入指定区域的路径。
9. 选择一个**Export-list**（导出列表）或新建一个访问列表，以筛选从指定区域的区域内路径向其他区域宣告的 3 类摘要 LSA。
10. 选择一个**Inbound Filter List**（入站筛选器列表）或新建一个前缀列表，以筛选进入该区域的 3 类摘要 LSA。

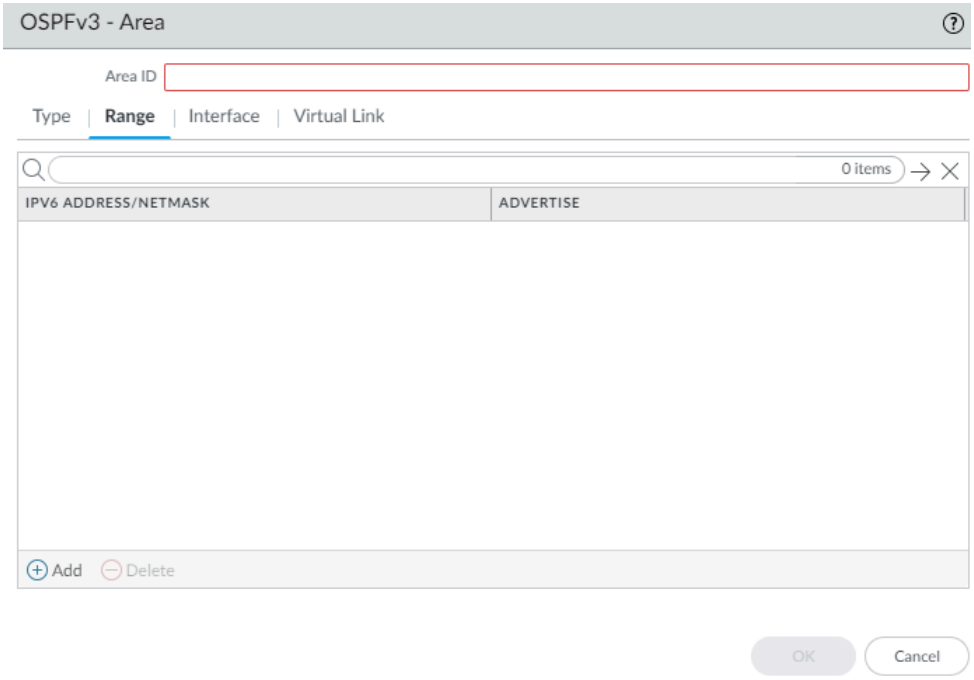
    如果应用导入访问列表和入站前缀列表，防火墙将使用 *AND* 操作（必须同时符合这两个列表）。
11. 选择一个**Outbound Filter List**（出站筛选器列表）或新建一个前缀列表，以筛选来自该区域的 3 类摘要 LSA。

    如果应用导出访问列表和出站前缀列表，防火墙将使用 *AND* 操作（必须同时符合这两个列表）。
12. 如果区域的**Type**（类型）为 **NSSA** 并且选择了 **ABR**，则 **Add**（添加）一个 **IPv6 Prefix**（**IPv6** 前缀），一组外部子网汇总到 7 类 LSA，然后在选择 **Advertise**（通告）时将其转换为 5 类 LSA 并向骨干区域通告。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 指定 3 类摘要 LSA 向骨干区域宣告的网络范围，前提是该区域包含至少一个来自此范围的区域内网络（即，以路由器或网络 LSA 描述）。

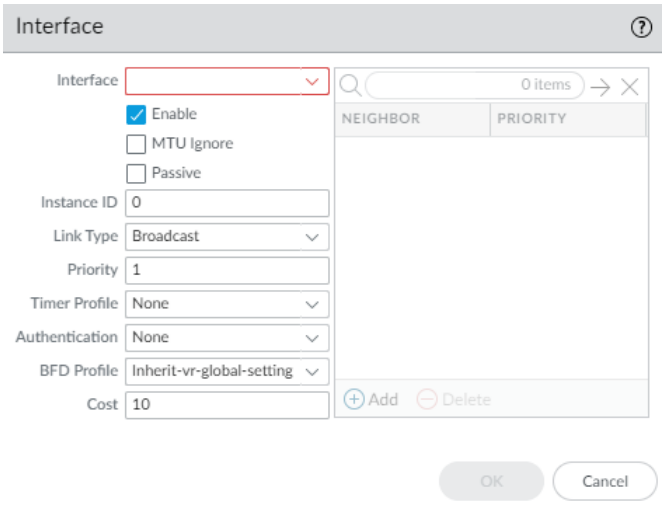
1. 选择 **Range**（范围），然后 **Add**（添加）**IPv6 Address/Netmask**（**IPv6** 地址/网络掩码）（用于汇总该区域的路由）。如果该区域包含至少一个区域内网络，则路由信息与此范围匹配的 3 类摘要 LSA 将被宣告到骨干区域。
2. 选择 **Advertise**（通告）以将 LSA 中匹配的子网通告到骨干区域。如果 **Advertise**（通告）设置为否，则该区域中存在的任何匹配的区域内前缀都不会被通告到骨干区域。



 ©2024 Palo Alto Networks, Inc.

STEP 5 | 将接口添加到该区域。

1. 在**Interface**（接口）选项卡中，通过选择接口来 **Add**（添加）**Interface**（接口）。
2. **Enable**（启用）接口。



3. 选择 **MTU Ignore**（**MTU** 忽略），以在尝试建立邻接时忽略最大传输单(MTU)的不匹配（默认为禁用；进行 MTU 匹配检查）。
4. 选择 **Passive**（被动），以阻止将 OSPF 呼叫数据包发送出接口，从而阻止本地路由器与邻居创建 OSPF 邻接关系；但是，该接口仍包含在链路状态数据库中。您可以将接口设为被动接口，例如，由于您不希望在没有路由器的位置发送呼叫数据包，因此接口连接到了交换机。
5. 仍将 **Instance ID**（实例 **ID**）设置为 0，因为仅允许一个 OSPFv3 实例。
6. 选择 **Link Type**（链路类型）：
   - **Broadcast**（广播）— 通过组播 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）。
   - **p2p**（点对点）— 自动发现邻居。
   - **p2mp**（点对多点）— 必须手动定义邻居：**Add**（添加）可通过此接口访问的所有邻居的 **Neighbor**（邻居）IPv6 地址，并添加要选作指定路由器(DR)或备份 DR 的每个邻居的 **Priority**（优先级）；范围为 0 - 255；默认为 1。
7. 输入接口的 **Priority**（优先级）；要选作指定路由器(DR)或备份 DR(BDR)的接口的优先级；范围为 0 至 255；默认为 1。值配置为零时，路由器不会被选为 DR 或 BDR。
8. 选择一个 OSPFv3 接口**Timer Profile**（计时器配置文件）或新建一个，以应用于该接口。此 OSPFv3 接口计时器配置文件将覆盖应用于 OSPFv3 的全局接口计时器。
9. 选择一个 OSPFv3 接口**Authentication**（身份验证）配置文件或新建一个，以应用于该接口。此身份验证配置文件将覆盖应用于类型选项卡中区域的身份验证配置文件。
10. 默认情况下，接口将为 OSPFv3 继承应用于逻辑路由器的 BFD 配置文件 **(Inherit-vr-global-setting)**。或者，选择默认配置文件、选择所创建的 **BFD Profile**（**BFD** 配置文

 ©2024 Palo Alto Networks, Inc.

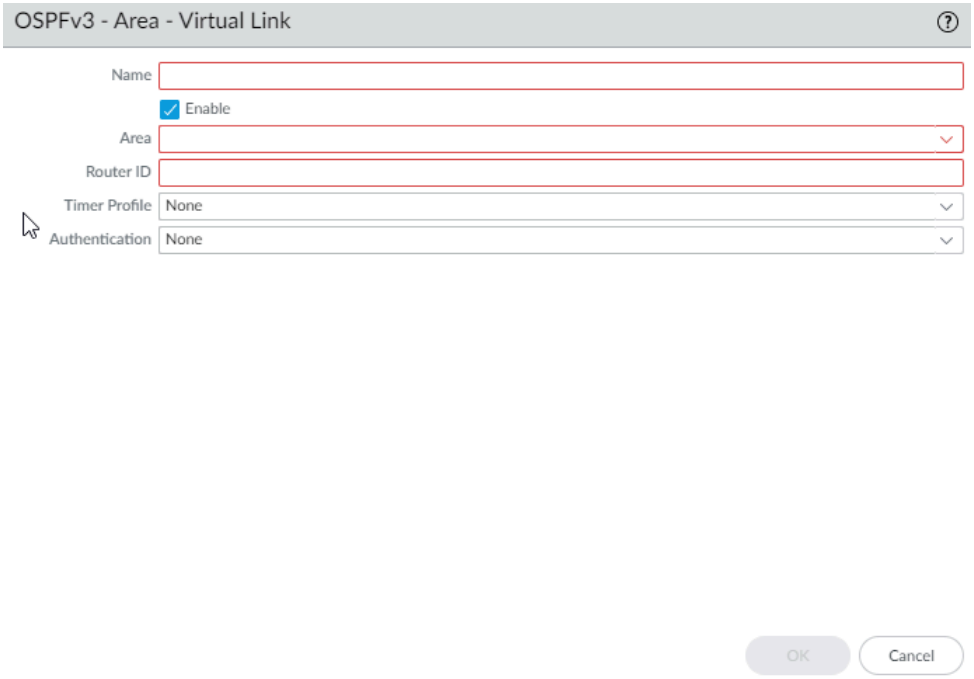
件）、新建一个或选择 **None (Disable BFD)**（无（禁用 **BFD**）），以覆盖在 OSPFv3 层级应用的 BFD 配置文件。

11. 输入该接口的 OSPFv3 **Cost**（成本），这会影响路由选择；范围为 1 - 65,5535；默认为 10。在选择路径时，累积成本较低的路由（所用每个接口的附加成本）优先于累积成本较高的路由。
12. 单击 **OK**（确定）以保存接口。

STEP 6 | 如果 ABR 没有到骨干区域的物理链路，请在具有到骨干区域的物理链路的同一区域内配置到邻居 ABR 的虚拟链路。

必须为区域边界路由器*(ABR)*定义以下设置，且必须在骨干网区域*(0.0.0.0)*中定义。

1. 选择 **Virtual Link**（虚拟链路）。
2. 按 **Name**（名称）（最多 31 个字符）**Add**（添加）**Virtual Link**（虚拟链路）。
3. **Enable**（启用）虚拟链路。



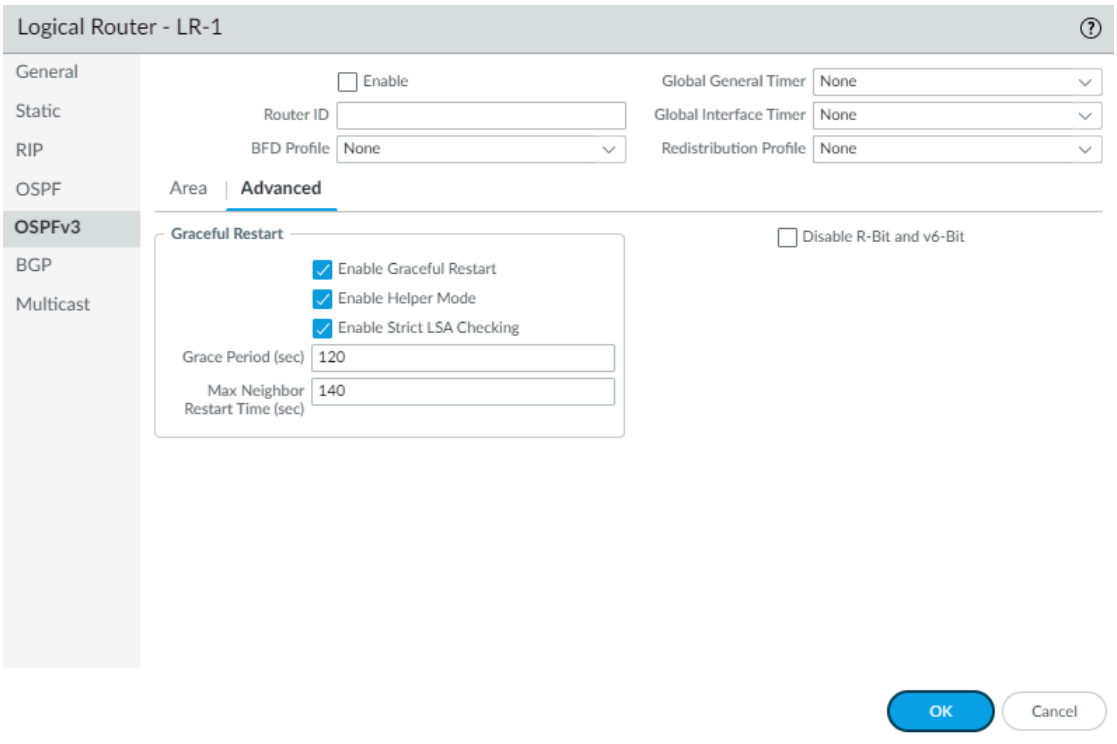
4. 选择具有到骨干区域的物理链路的邻居 ABR 所在的中转 **Area**（区域）。
5. 输入虚拟链路远程端的邻居 ABR 的**Router ID**（路由器 **ID**）。
6. 选择一个 OSPFv3 接口**Timer Profile**（计时器配置文件）或新建一个计时器配置文件，以应用于虚拟链路。此 OSPFv3 接口计时器配置文件将覆盖应用于 OSPFv3 的全局接口计时器和应用于该接口的 OSPFv3 接口计时器配置文件。
7. 选择一个 OSPF 接口**Authentication**（身份验证）配置文件或新建一个身份验证配置文件，以应用于虚拟链路。此身份验证配置文件将覆盖应用于类型选项卡中区域的身份验证配置文件和应用于该接口的身份验证配置文件。
8. 单击 **OK**（确定）。

STEP 7 | 单击 **OK**（确定）以保存区域。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 配置高级 OSPFv3 功能。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择相应逻辑路由器。
2. 选择 **OSPFv3** > **Advanced**（高级）。
3. **Enable Graceful Restart**（启用正常重启），为逻辑路由器启用正常重启。默认为启用。
4. **Enable Helper Mode**（启用帮助程序模式），使逻辑路由器能够在正常重启帮助程序模式下运行。默认为启用。
5. **Enable Strict LSA Checking**（启用严格的 **LSA** 检查）可使帮助程序路由器停止执行帮助程序模式，并在链路状态通告指示网络拓扑发生变化时导致正常重启过程停止。默认为启用。
6. 输入 **Grace Period (sec)**（宽限期（秒））— 防火墙关闭或不可用时，逻辑路由器将执行正常重启的时限（秒数）；范围为 5 - 1,800；默认为 120。
7. 输入 **Max Neighbor Restart Time (sec)**（最大邻居重启时间（秒））逻辑路由器处于帮助程序模式时逻辑路由器从邻居接受的宽限期的最大秒数；范围为 5 - 1,800；默认为 140。
8. 选择 **Disable R-Bit and v6-Bit**（禁用 **R** 位和 **v6** 位）以清除从该逻辑路由器发送的路由器 LSA 中的 R 位和 V6 位，以表示防火墙处于不活动状态。处于此状态时，防火墙会参与 OSPFv3，但是不会发送中转流量或 IPv6 数据报。在此状态中，仍然会将本地流量转发到防火墙。使用双宿网络执行维护时，这非常有用，因为可以在防火墙周围重新路由流量，同时仍然可以对其进行访问。请参阅 RFC 5340。



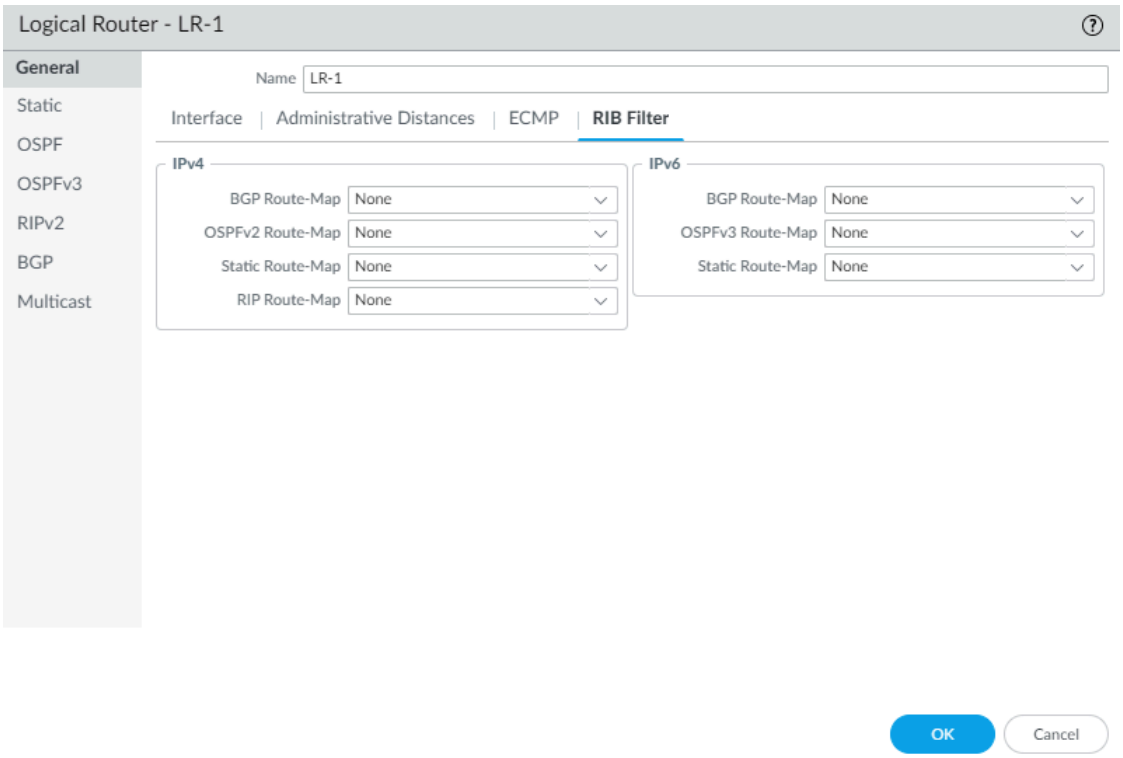
9. 单击 **OK**（确定）以保存高级设置。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 配置区域内筛选以确定在全局 RIB 中放置哪些 OSPFv3 路由。

您可能会学习并重新分发 OSPFv3 路由，但不希望将他们放置在全局 RIB 中；您可能希望仅允许在全局 RIB 中放置特定的 OSPFv3 路由。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择 **RIB Filter**（**RIB** 筛选器）。
3. 要筛选全局 RIB 的 **IPv6** OSPFv3 路由，对于 **OSPFv3 Route-Map**（**OSPFv2** 路由映射），请选择所创建的重新分发路由映射，或者新建一个重新分发路由映射，其中源协议为 OSPFv3，目标协议为 RIB。



4. 单击 **OK**（确定）。

STEP 10 | （可选）更改与逻辑路由器相关的 OSPFv3 区域内、OSPFv3 区域间和 OSPFv3 外部路由的默认管理距离。

STEP 11 | **Commit**（提交）。

STEP 12 | 查看 OSPFv3 和链路状态数据库(LSDB)的高级路由信息。PAN-OS CLI 快速入门指南在 CLI 速查表中列出了以下命令：Networking（下一步：网络）。

 ©2024 Palo Alto Networks, Inc.

创建 OSPFv3 路由配置文件

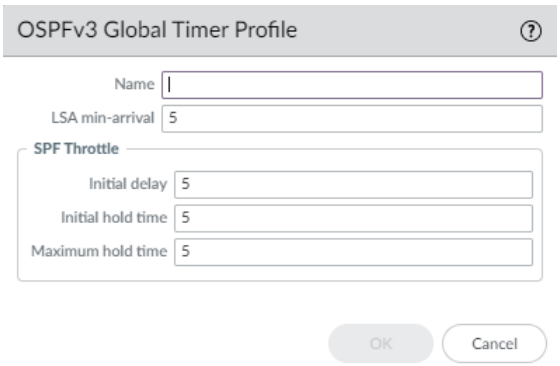
高级路由引擎支持 OSPFv3；创建 OSPFv3 全局计时器配置文件、身份验证配置文件、接口计时器配置文件和重新分发配置文件以应用于 OSPFv3。本主题将介绍这些配置文件及其创建方法。当您在高级路由引擎上配置 OSPFv3 时引用参考。

- **OSPFv3 Global Timer Profiles**（**OSPFv3** 全局计时器配置文件） — 指定应用于所有 OSPFv3 区域的链路状态通告(LSA)间隔、SPF 计算延迟、初始保持时间和最大保持时间的计时器。SPF 限制设置允许协议在网络不稳定（正在更改拓扑结构）时减慢 LSA 更新数据的发送速度。在常规 OSPFv3 配置中应用配置文件。逻辑路由器上的 OSPFv3 配置文件用于全局；您可以创建多个配置文件来轻松更改全局计时器。
- **OSPFv3 Interface Authentication Profiles**（**OSPFv3** 接口身份验证配置文件） — OSPFv3 没有自带的身份验证功能；它依靠 IPsec 来保护邻居之间的 OSPFv3 消息。在 **OSPFv3 Area**（**OSPFv3** 区域） > **Type**（类型）选项卡中应用配置文件。
- **OSPFv3 Interface Timer Profiles**（**OSPFv3** 接口计时器配置文件） — 指定与接口操作相关的计时器，例如 OSPFv3 呼叫和正常重启。在常规 OSPFv3 配置中应用配置文件。
- **OSPFv3 Redistribution Profiles**（**OSPFv3** 重新分发配置文件） — 将 IPv6 静态路由、互联路由或 IPv6 BGP 路由或 IPv6 默认路由重新分发到 OSPFv3。在常规 OSPFv3 配置中应用配置文件。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 创建 OSPFv3 全局计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPFv3**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPFv3 Global Timer Profile**（**OSPFv3** 全局计时器配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入 **LSA min-arrival**（**LSA** 最短到达时间）（秒），即防火墙重新计算 SPF 树的最小间隔；范围是 1 - 10；默认为 5。防火墙会以更大的间隔重新计算（低于设置的频率）。
4. 在 SPF 限制区域中，输入从逻辑路由器接收到拓扑变更到其执行最短路径优先(SPF)计算之间的 **Initial delay**（初始延迟）（秒）；范围为 0 - 600；默认为 5。
5. 输入前两次连续 SPF 计算之间的 **Initial hold time**（初始保持时间）（秒）；范围为 0 - 600；默认为 5。每个后续的保持时间是前一个保持时间的两倍，直到达到最大保持时间。
6. 输入 **Maximum hold time**（最大保持时间）（秒），即保持时间保持稳定前能达到的最大值；范围为 0 - 600；默认为 5。

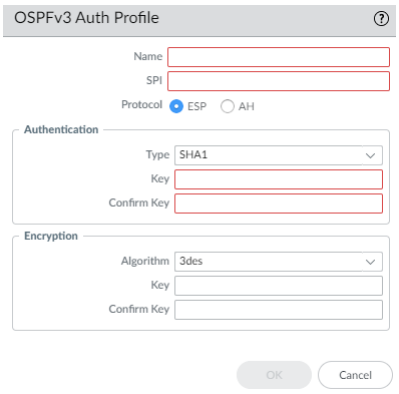


7. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 创建 OSPFv3 接口身份验证配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPFv3**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPFv3 Auth Profile**（**OSPFv3** 身份验证配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 输入 **SPI**（安全策略索引），该索引必须在 OSPFv3 相邻设备的两端之间匹配。
4. 选择 **Protocol**（协议）：**ESP**（封装安全载荷）（推荐）或 **AH**（身份验证头）。
5. 选择身份验证 **Type**（类型）：
   - **SHA1**（默认值）— 安全散列算法 1。
   - **SHA256**
   - **SHA384**
   - **SHA512**
   - **MD5**
   - 无
6. 输入身份验证 **Key**（密钥），使用由 8 个十六进制字符组成的 5 个十六进制区段，共 40 个十六进制字符（例如 A5DEC4DD155A695A8B983AACEAA5A97C6AECB6D1）。
7. **Confirm Key**（确认密钥）：输入相同的密钥。



8. （仅限 ESP）选择加密 **Algorithm**（算法）：
   - **3des**（默认）
   - **aes-128-cbc**
   - **aes-192-cbc**
   - **aes-256-cbc**
   - **null**
9. 输入十六进制格式的加密 **Key**（密钥）；根据 ESP 加密类型使用正确的区段数量：
   - **3des** —在密钥中共使用 6 个十六进制区段。
   - **aes-128-cbc** — 在密钥中共使用 4 个十六进制区段。
   - **aes-192-cbc** — 在密钥中共使用 6 个十六进制区段。

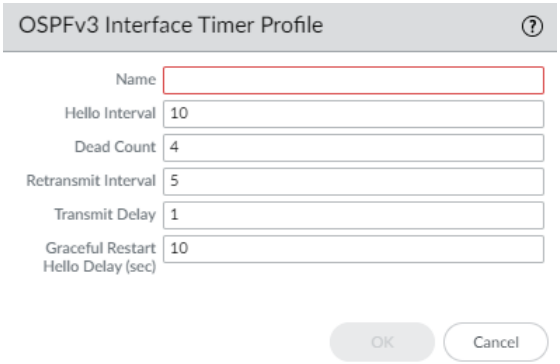
 ©2024 Palo Alto Networks, Inc.

- **aes-256-cbc** — 在密钥中共使用 8 个十六进制区段。

10. **Confirm Key**（确认密钥）：输入相同的密钥。
11. 单击 **OK**（确定）。

STEP 3 | 创建 OSPFv3 接口计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPFv3**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPFv3 Interface Timer Profile**（**OSPFv3** 接口计时器配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。

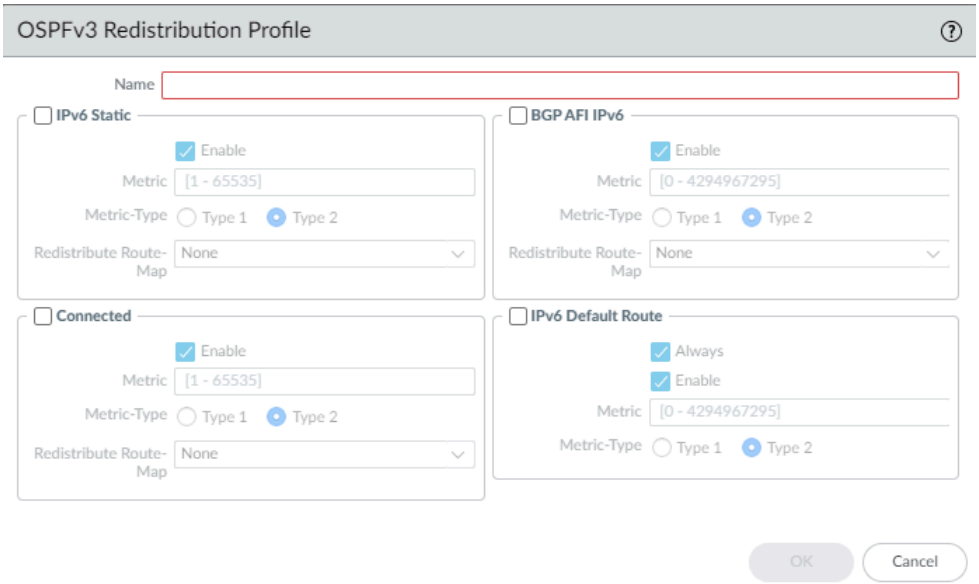


3. 输入 **Hello Interval**（呼叫间隔），即 OSPFv3 发送呼叫数据包的时间间隔（秒）；范围为 1 - 3,600；默认为 10。
4. 输入 **Dead Count**（间隔次数），即在 OSPFv3 认为邻居关闭之前，邻居可以发生呼叫间隔的次数，而无需 OSPFv3 接收邻居的呼叫数据包；范围为 3 - 20；默认为 4。
5. 输入 **Retransmit Interval**（重传间隔），即在 OSPFv3 重传 LSA 之前，OSPFv3 等待从邻居接收 LSA 的秒数：范围为 1 - 1,800；默认为 5。
6. 输入 **Transmit Delay**（传输延迟），即 OSPFv3 在将 SLA 发送到接口之前延迟传输 LSA 的秒数；范围为 1 - 1,800；默认为 1。
7. 输入 **Graceful Restart Hello Delay (sec)**（正常重启呼叫延迟（秒））；范围为 1 - 10；默认为 10。如果配置了主动/被动 HA，则此设置适用于 OSPFv3 接口。正常重启呼叫延迟是防火墙以 1 秒间隔发送宽限 LSA 数据包期间的秒数。在此期间，不会从重新启动防火墙发送任何呼叫数据包。在重新启动期间，间隔计时器（其值等于 **Hello Interval**（呼叫间隔）乘以 **Dead Count**（间隔次数））也会倒计时。如果间隔计时器太短，邻居将会在平稳重新启动期间因呼叫延迟而关闭。因此，建议将间隔计时器的值设置为“正常重启呼叫延迟”值的至少四倍。例如，**Hello Interval**（呼叫间隔）为 10 秒，**Dead Counts**（间隔次数）为 4 次，则间隔计时器的值为 40 秒。如果将 **Graceful Restart Hello Delay**（正常重启呼叫延迟）设置为 10 秒，则呼叫数据包的 10 秒延迟正好在间隔计时器的 40 秒内，因此相邻设备在正常重启期间不会超时。
8. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 创建 OSPFv3 重新分发配置文件，以指定要重新分发到 OSPFv3 的 IPv6 静态路由、互联路由、IPv6 BGP 路由和默认 IPv6 路由的任意组合。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **OSPFv3**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**OSPFv3 Redistribution Profile**（**OSPFv3** 重新分发配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。



3. 选择 **IPv6 Static**（**IPv6** 静态），以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 IPv6 静态重新分发部分。
   - 输入要应用于重新分发到 OSPFv3 的 IPv6 静态路由的**Metric**（指标）；范围为 1 - 65,535。
   - 选择 **Metric Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制要重新分发到 OSPFv3 的 IPv6 静态路由。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。
4. 选择 **Connected**（互联），以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的互联路由重新分发部分。
   - 输入要应用于重新分发到 OSPFv3 的互联路由的**Metric**（指标）；范围为 1 - 65,535。
   - 选择 **Metric Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制要重新分发到 OSPFv3 的互联路由。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，

 ©2024 Palo Alto Networks, Inc.

对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。

5. 选择 **BGP AFI IPv6**，以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 BGP AFI IPv6 路由重新分发部分。
   - 输入要应用于重新分发到 OSPFv3 的 IPv6 BGP 路由的**Metric**（指标）；范围为 0 - 4,294,967,295。
   - 选择 **Metric Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制要重新分发到 OSPFv3 的 IPv6 BGP 路由。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。同样，路由映射设置配置中的指标类型优先于此重新分发配置文件中配置的指标类型。
6. 选择 **IPv6 Default Route**（**IPv6** 默认路由），以允许配置该配置文件的这一部分。
   - 选择 **Always**（始终），以始终创建默认路由并将其重新分发到 OSPFv3，即使路由器上没有默认路由；默认启用。如果未设置为 **Always**（总是），则当 ABR 上没有默认路由时，不会重新分发默认路由。
   - **Enable**（启用）配置文件的 IPv6 默认路由重新分发部分。
   - 输入要应用于重新分发到 OSPFv3 的 IPv6 默认路由的**Metric**（指标）；范围为 0 - 4,294,967,295。
   - 选择 **Metric Type**（指标类型）：**Type 1**（类型 **1**）或 **Type 2**（类型 **2**）。
7. 单击 **OK**（确定）。

STEP 5 | **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

在高级路由引擎上配置 RIPv2

高级路由引擎支持 RIPv2。

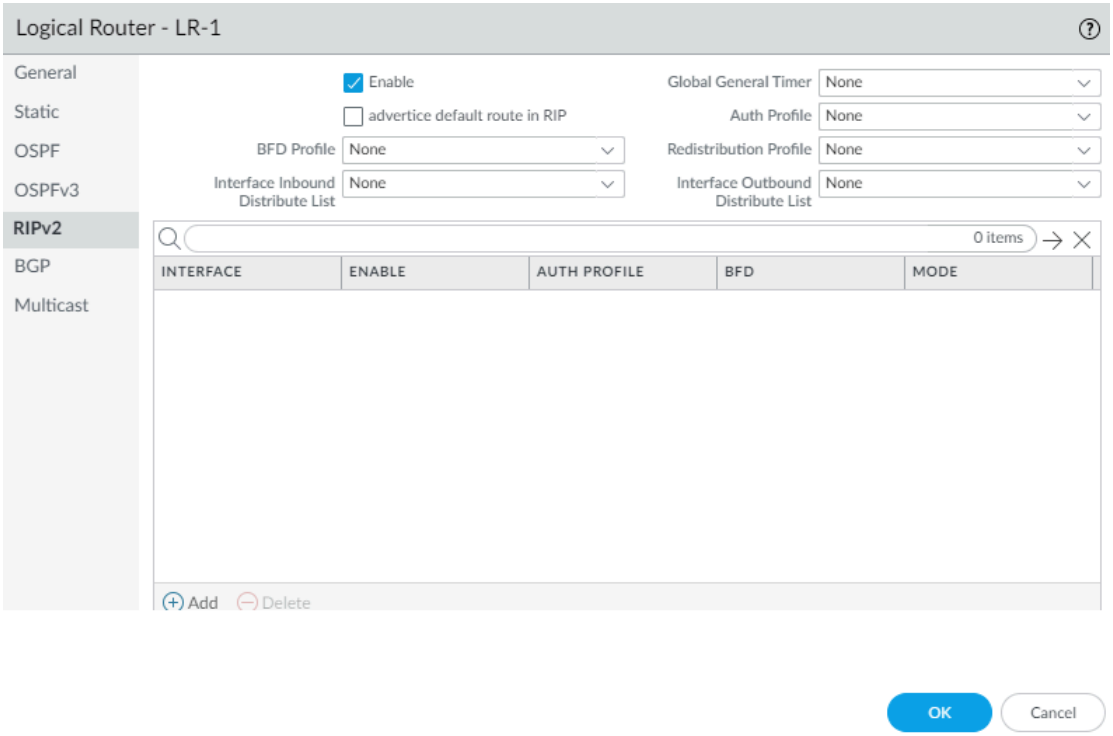
请考虑可应用于 RIPv2 的 RIPv2 Routing Profiles（RIPv2 路由配置文件）和筛选器，从而节省配置时间并确保一致性。您可以提前创建配置文件和筛选器，也可以在配置 RIPv2 时创建。

STEP 1 | 配置逻辑路由器.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 启用 RIPv2 并配置常规设置。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择并 **Enable**（启用）**RIPv2**。

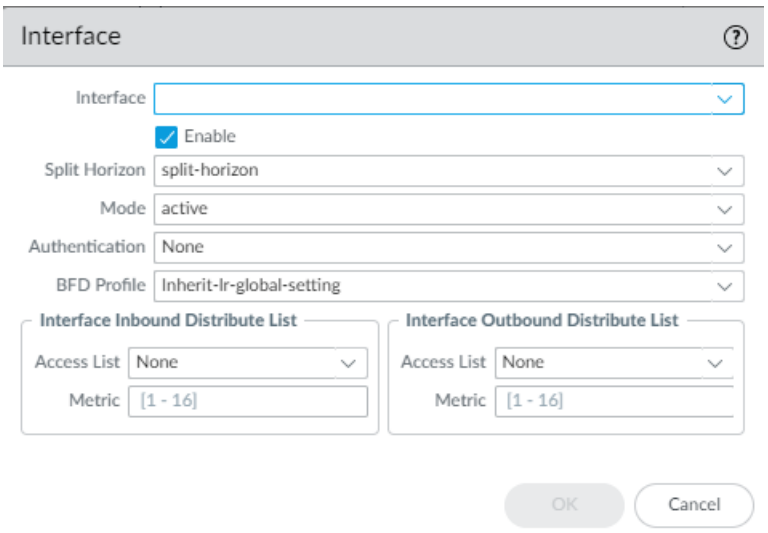


3. 选择 **advertise default route in RIP**（在 **RIP** 中通告默认路由）以通告默认路由，即使路由引擎的 RIB 中不存在该路由。
4. 如果要将 BFD 应用于 RIPv2，请选择所创建的 **BFD Profile**（**BFD** 配置文件），或选择默认配置文件，或新建一个 BFD 配置文件。默认值是 **None (Disable BFD)**（无（禁用 **BFD**））。
5. 选择一个**Global General Timer**（全局通用计时器）或新建一个 RIPv2 全局通用计时器。
6. 选择一个**Auth Profile**（身份验证配置文件）或新建一个 RIPv2 身份验证配置文件。
7. 选择一个**Redistribution Profile**（重新分发配置文件），或新建一个，以将 IPv4 静态路由、互联路由、BGP IPv4 路由或 OSPFv2 路由重新分发到 RIPv2。
8. 选择一个**Global Inbound Distribute List**（全局入站分发列表）以控制所接受的传入路由。
9. 选择一个**Global Outbound Distribute List**（全局出站分发列表），以控制向 RIP 邻居通告的路由。

©2024 Palo Alto Networks, Inc.

STEP 3 | 为 RIPv2 配置接口。

1. 选择一个接口以 **Add**（添加） **Interface**（接口），然后 **Enable**（启用）它。



2. 对于 **Split Horizon**（水平分割），请选择以下之一：
   - **split-horizon**（水平分割）— 不在接收路由的同一个接口上通告路由。
   - **no-split-horizon**（无水平分割）— 禁用水平分割。
   - **no-split-horizon-with-poison-reverse**（未使用毒性逆转进行水平分割）— 允许通告返回到接收通告的同一接口上，并将这些路由的指标设置为 RIP 允许的最大值，即 16。
3. 选择 **Mode**（模式）：
   - **active**（主动）— 接口将通告网络并发送 RIP 更新。
   - **passive**（被动）— 接口将通告网络，但不发送 RIP 更新。（对于以下情况非常有用：网络中没有 RIP 路由器，因此没有理由在接口上发送 RIP 更新）。
   - **send-only**（仅发送）— 如果防火墙是终端节点，而您只想向 RIP 通告前缀，则可以使用此选项，不过可以使用静态路由或默认路由访问外部前缀。
4. 如果要覆盖应用于逻辑路由器级别的配置文件，请选择一个**Authentication**（身份验证）配置文件。
5. 默认情况下，接口将为 RIPv2 继承应用于逻辑路由器的 BFD 配置文件 **(Inherit-lr-global-setting)**。或者，选择其他 **BFD Profile**（**BFD** 配置文件），新建一个 BFD 配置文件，或选择 **None (Disable BFD)**（无（禁用 **BFD**）） 为接口禁用 BFD。
6. 对于 **Interface Inbound Distribute List**（接口入站分发列表），请选择一个访问列表以控制到达该接口的路由。
7. 指定应用于传入路由的**Metric**（指标）；范围为 1 - 16。
8. 对于 **Interface Outbound Distribute List**（接口出站分发列表），选择一个**Access List**（访问列表）以控制从该接口通告到 RIP 邻居的路由。
9. 指定要应用于通告路由的**Metric**（指标）；范围为 1 - 16。
10. 单击 **OK**（确定）。

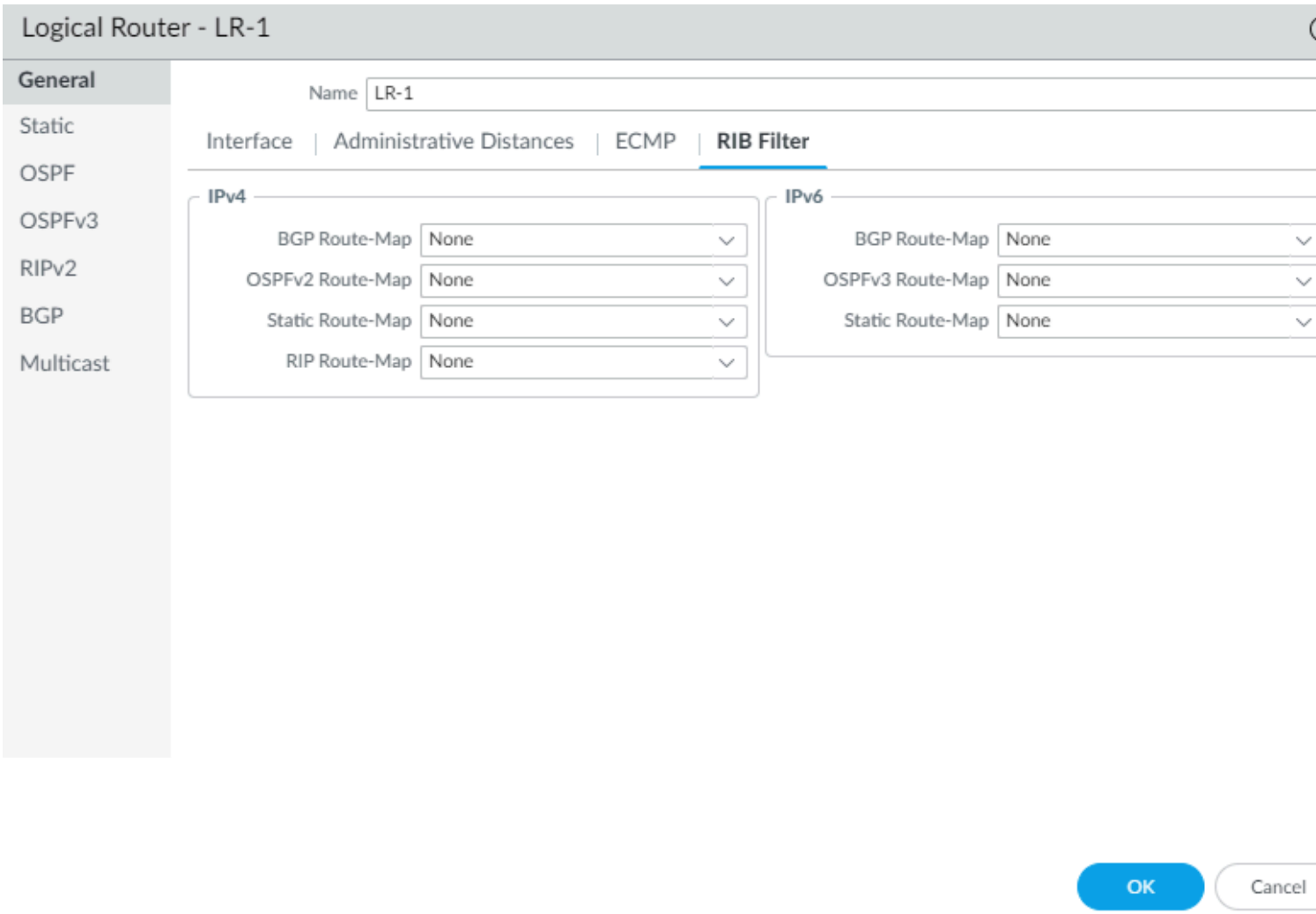
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 单击 **OK**（确定）。

STEP 5 | （可选）控制放置在全局 RIB 中的 RIP 路由。

您可能想要学习并重新分发路由，但又不希望它们出现在协议的本地路由表或全局 RIB 中。您可能只想将特定路由添加到全局 RIB。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。
2. 选择 **RIB Filter**（**RIB** 筛选器），以允许路由进入或阻止将路由添加到全局 RIB。



3. 要筛选到 RIB 的 RIPv2 路由，请在 IPv4 区域中，为 **RIP Route-Map**（**RIP** 路由映射）选择一个重新分发路由映射或新建一个。
4. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

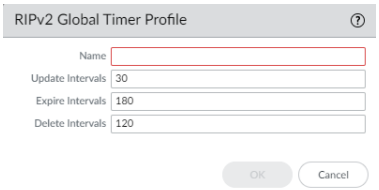
创建 RIPv2 路由配置文件

高级路由引擎支持 RIPv2；创建以下配置文件以应用于此协议。这些配置文件可以在多个逻辑路由器和虚拟系统中使用。本主题将介绍这些配置文件以及如何配置它们。

- **RIPv2 Global Timer Profiles**（**RIPv2** 全局计时器配置文件） — 指定 RIPv2 的更新、过期和删除间隔时间。在 RIPv2 常规配置中应用该配置文件。
- **RIPv2 Interface Authentication Profiles**（**RIPv2** 接口身份验证配置文件） — 指定使用密码或 MD5 的 RIPv2 身份验证；在 RIPv2 常规配置中应用该配置文件。
- **RIPv2 Redistribution Profiles**（**RIPv2**重新分发配置文件） — 指定如何将 IPv4 静态路由、互联路由、BGP IPv4 路由和 OSPFv2 路由重新分发到 RIPv2。在 RIPv2 常规配置中应用该配置文件。

STEP 1 | 创建 RIPv2 全局计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **RIPv2**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**RIPv2 Global Timer Profile**（**RIPv2** 全局计时器配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。

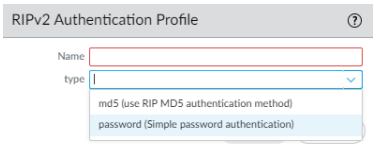


3. 指定 **Update Interval**（更新间隔）（秒），即定期计划的更新消息之间所间隔的时长。范围为 5 - 2,147,483,647；默认为 30。
4. 指定 **Expire Interval**（到期间隔）（秒），即路由可以在路由表中保留而不被更新的时长。范围为 5 - 2,147,483,647；默认为 180。在达到到期间隔后，该路由仍包含在更新消息中，直至达到删除间隔。
5. 指定 **Delete Interval**（删除间隔）（秒）；范围为 5 - 2,147,483,647；默认为 120。当路由表中的过期路由达到删除间隔时，该路由将从路由表中删除。
6. 单击 **OK**（确定）。

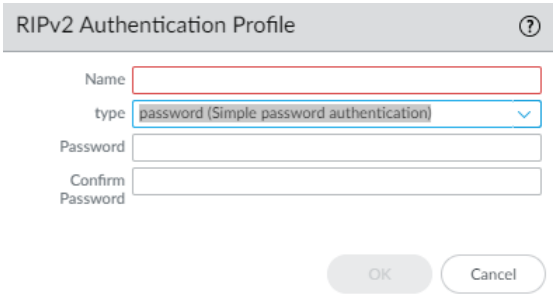
©2024 Palo Alto Networks, Inc.

STEP 2 | 创建 RIPv2 身份验证配置文件。

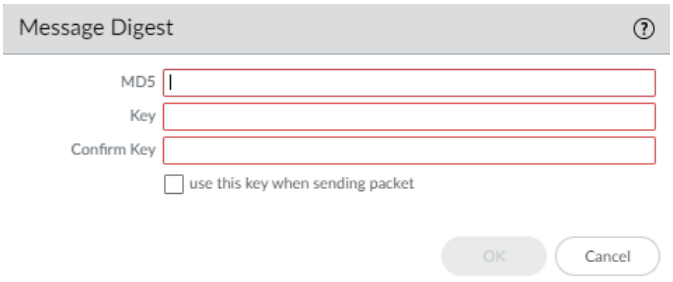
1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **RIPv2**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**RIPv2 Authentication Profile**（**RIPv2** 身份验证配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。



3. 选择身份验证类型：**md5**（使用 RIP MD5 身份验证方法）或 **password**（密码）（简单密码身份验证）。
4. 对于简单密码身份验证，请输入 **Password**（密码）（最多 16 个字符），然后 **Confirm Password**（确认密码）。



5. 对于 **RIP MD5** 身份验证：
   - **Add**（添加）一个 MD5 密钥 ID；范围为 0 - 255。
   - 输入 **Key**（密钥）（最多 16 个字母数字字符），然后 **Confirm Key**（确认密钥）。
   - 选择 **use this key when sending packet**（发送数据包时使用此密钥），使此密钥成为首选密钥。

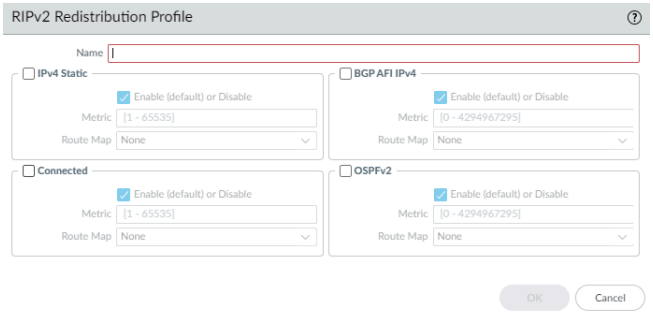


6. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 创建 RIPv2 重新分发配置文件，以指定要重新分发到 RIPv2 的 IPv4 静态路由、互联路由、BGP IPv4 路由和 OSPFv2 路由的任意组合。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **RIPv2**。
2. 按 **Name**（名称）（最多 63 个字符）**Add**（添加）**RIPv2 Redistribution Profile**（**RIPv2** 重新分发配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。



3. 选择 **IPv4 Static**（**IPv4** 静态），以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 IPv4 静态重新分发部分。
   - 输入适用于被重新分发给 RIPv2 的静态路由的**Metric**（指标）（范围为 1- 65,535）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射，其匹配标准可控制将哪些 IPv4 静态路由重新分发到 RIPv2。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
4. 选择 **Connected**（互联），以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的互联路由重新分发部分。
   - 输入适用于被重新分发给 RIPv2 的连接路由的**Metric**（指标）（范围为 1- 65,535）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
5. 选择 **BGP AFI IPv4**，以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 BGP IPv4 路由重新分发部分。
   - 指定适用于被重新分发给 RIPv2 的 BGP 路由的**Metric**（指标）（范围为 0- 4,294,967,295）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用

 ©2024 Palo Alto Networks, Inc.

于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。

6. 选择 **OSPFv2**，以允许配置该配置文件的这一部分。
   - **Enable**（启用）配置文件的 OSPFv2 路由重新分发部分。
   - **Enable**（启用）配置文件的 IPv4 默认路由重新分发部分。
   - 指定适用于被重新分发给 RIPv2 的默认路由的**Metric**（指标）（范围为 0-4,294,967,295）。
   - 选择一个**Redistribute Route-Map**（重新分发路由映射）或新建一个重新分发路由映射。默认为 **None**（无）。如果路由映射集配置包括指标操作和指标值，则它们将应用于重新分发的路由。否则，对此重新分发配置文件配置的指标将应用于重新分发的路由。
7. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

创建 BFD 配置文件

在高级路由引擎上，您可以使用双向转发检测(BFD)配置文件，轻松地将 BFD 设置应用于静态路由或路由协议。您可以使用默认配置文件（只读）或创建新的 BFD 配置文件。

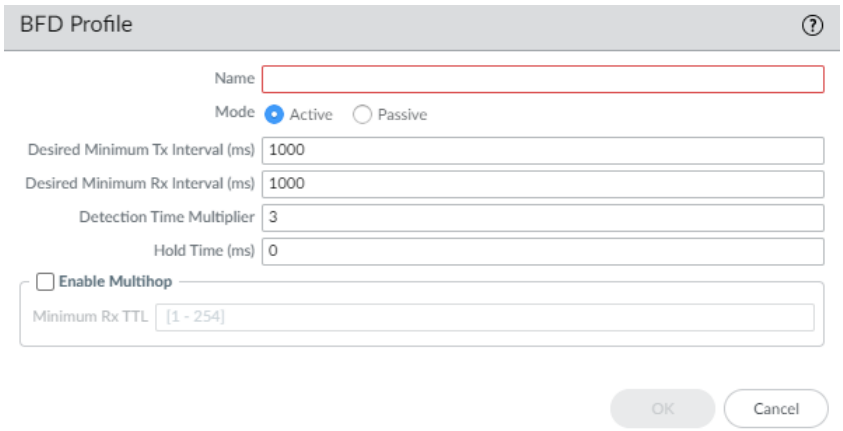
创建 BFD 配置文件之前，请执行以下操作：

- 配置逻辑路由器.
- 如果要将 BFD 应用于静态路由，则配置一个或多个静态路由。
- 如果要将 BFD 应用于路由协议，则配置一个路由协议（**BGP**、**OSPF**、**OSPFv3** 或 **RIPv2**）。例如，您可以在配置 BGP 常规设置时应用 BFD 配置文件。

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 | 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **BFD**。

STEP 2 | 按 **Name**（名称）（最多 63 个字符）**Add**（添加） BFD 配置文件。名称区分大小写，且必须在防火墙上具有唯一性。只能使用字母、数字、连字符和下划线。但不得包含句点(.)或空格。



STEP 3 | 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 4 | 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 协议发送 BFD 控制数据包的最短间隔时间（毫秒）；因此您与对等体协商传输间

 ©2024 Palo Alto Networks, Inc.

隔。PA-7000 系列、PA-5200 系列和 PA-5450 防火墙的范围为 50 - 10,000；PA-3200 系列的范围为 100 - 10,000；VM 系列的范围为 200 - 10,000。默认为 1,000。

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）。

在 *PA-7000* 系列防火墙上，将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。

STEP 5 | 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 系列、PA-5200 系列和 PA-5450 防火墙的范围为 50 - 10,000；PA-3200 系列的范围为 100 - 10,000；VM 系列的范围为 200 - 10,000。默认为 1,000。

在 *PA-7000* 系列防火墙上，将理想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。

STEP 6 | 输入 **Detection Time Multiplier**（检测时间乘数）。范围为 2 - 255；默认为 3。

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。

创建 *BFD* 配置文件时，要考虑防火墙是一种基于会话的设备，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 7 | 输入 **Hold Time (ms)**（保持时间（毫秒）），即 BFD 传输 BFD 控制数据包之前，链路启用后的延迟。**Hold Time**（保持时间）仅适用于 BFD **Active**（主动）模式。如果 BFD 在保持时间内收到 BFD 控制数据包，则它会忽略这些数据包。范围为 0 - 120,000；默认为 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 8 | 输入 **Minimum Rx TTL**（最短接收 **TTL**），即 BFD 会在在 BFD 控制数据包中接受（接收）的最小生存时间(TTL)值（跃点数）（如果 BGP 支持多跃点 BFD）。范围为 1 至 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，如果对等体距离有 5 个跃点，而对等体传输一个 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 9 | 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

配置 IPv4 组播

高级路由引擎支持逻辑路由器的 IPv4 组播。您应该熟悉 IP 多播、IGMP 和 PIM 概念。

高级路由引擎上的 IPv4 组播支持传统路由引擎不支持的功能：

- IGMP 静态加入，即能够在接口上指定静态 IGMPv3 或 IGMPv2 接收器。相应的 PIM 加入消息将发送到上游。
- 协议无关组播(PIM)支持反向路径转发(RPF)查找模式：仅 MRIB、仅 URIB，先 MRIB 再 URIB。

IPv4 组播不支持 IGMPv1。

配置 IPv4 组播时，需对 PIM 接口计时器和 IGMP 接口查询 创建多播路由配置文件，以简化配置并确保一致。您可以创建组播路由映射来控制 PIM 组权限。

如果您希望单播流量采用与组播流量不同的路由，也可以创建 IPv4 MRoute。

STEP 1 | 配置逻辑路由器.

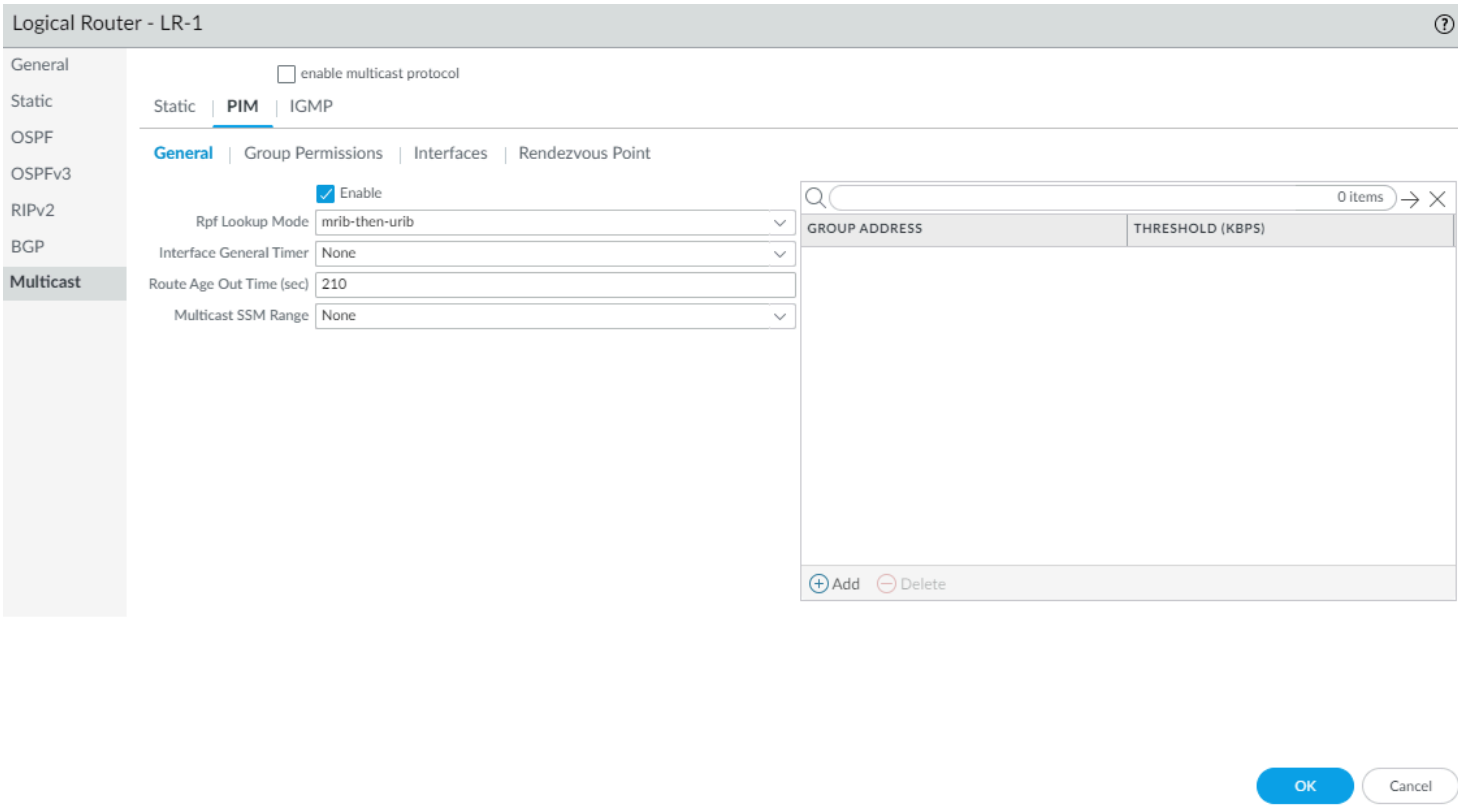
STEP 2 | 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。

STEP 3 | 选择 **Multicast**（组播）并启用组播协议。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 为逻辑路由器配置常规 PIM 参数。

1. 选择 **PIM > General**（常规），然后 **Enable**（启用）PIM。



2. 选择 **RPF lookup mode**（**RPF** 查找模式），该模式确定逻辑路由器查找的位置以找到传出接口，从而访问组播数据包中包含的源地址。如果存储在 RIB 中的传出界面与组播数据包到达的界面匹配，则逻辑路由器接受并转发数据包；否则，它将丢弃该数据包。
   - **mrib-only** — 仅在组播 RIB 中查找。
   - **mrib-then-urib** — 先查找组播 RIB；如果路由在组播 RIB 中不存在，再查找单播 RIB。
   - **urib-only** — 仅在单播 RIB 中查找。

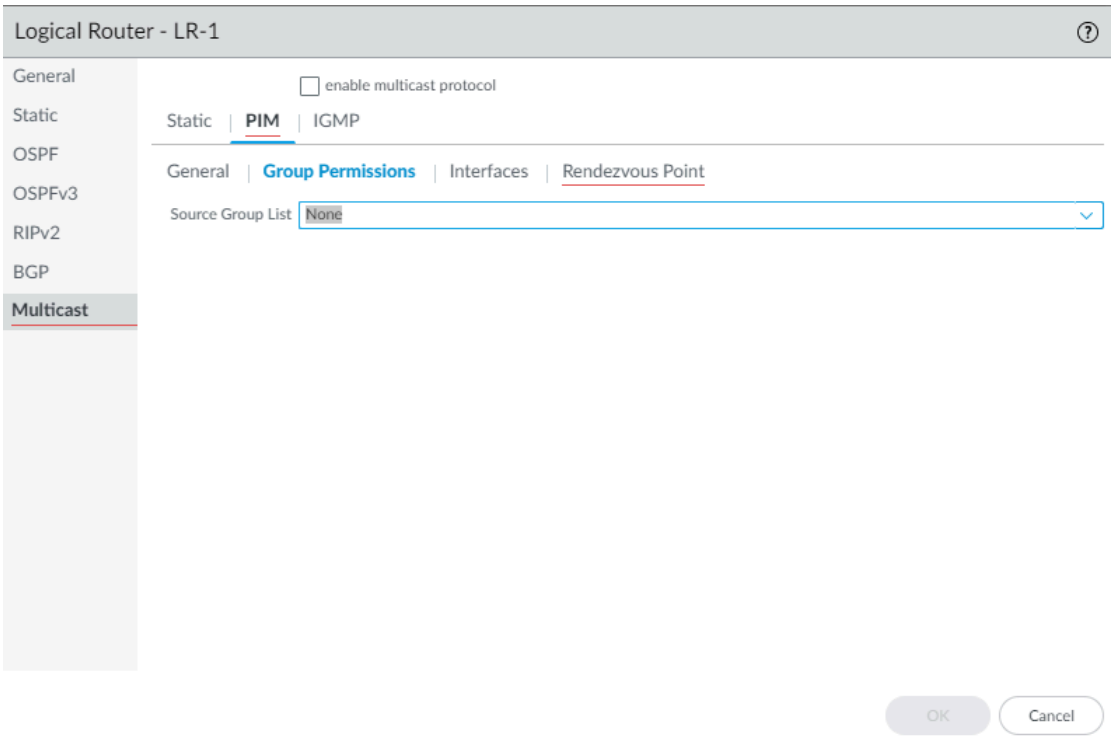
   RPF 查找模式还可控制在哪些位置进行路由查找，以选择用于 PIM 加入的路由。
3. 对于 **Interface General Timer**（接口通用计时器），请选择一个 PIM 接口计时器配置文件或新建一个 IPv4 PIM 接口计时器配置文件；默认值为 **None**（无）。
4. 指定 **Route Age Out Time (sec)**（路由年龄超时（秒））— 组播组和源之间的会话结束后，组播路由保留在 mRIB 中的秒数；范围为 210 - 7,200；默认为 210。
5. 若要配置特定源组播(SSM)，请在 **Multicast SSM Range**（组播 **SSM** 范围）中选择一个前缀列表（或新建一个），该列表指定了允许将组播流量发送到接收器的源地址；默认值为 **None (no prefix list)**（无（无前缀列表））。
6. 要为组播组或前缀配置最短路径树(SPT)阈值，请选择一个Prefix List（前缀列表）或新建一个，以 **Add**（添加）**Group Address**（组地址）（要为其指定分发树的组播组或前缀）。

 ©2024 Palo Alto Networks, Inc.

7. 以千比特/秒 (kbps) 为单位指定 **Threshold**（阈值）速率；如果组播组/前缀的组播流量到达逻辑路由器的速度快于此阈值速率，则到指定组/前缀的路由将从共享树（源自集合点[RP]）切换到 SPT 分布:
   - **0 (switch on first data packet)**（**0**（在第一个数据包上切换））— （默认）当逻辑路由器接收到该组/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。
   - 输入在任何接口、任何时间段内到达用于组播组/前缀的每秒千比特总数，此时，逻辑路由器将更改为此组播组或前缀的 SPT 分发；范围为 0 至 4294967295。
   - **never (do not switch to spt)**（从不（不会切换到 **SPT**））— PIM 路由器持续使用共享树将数据包转发至该组播组或前缀。

STEP 5 | 指定 PIM 组权限以控制逻辑路由器接受哪些 PIM 加入消息和注册消息，以及逻辑路由器转发哪些组播流量。

1. 选择 **PIM > Group Permissions**（组权限）。
2. 要控制从某些来源（S、G）发送至特定目标组播组的数据包以传输逻辑路由器，对于 **Source Group List**（来源组列表），请选择所创建的Access List（访问列表）或新建一个。访问列表可以是扩展访问列表，其中的源指定了组播源，目标指定了组播组。默认为 **None (no access list)**（无（无访问列表））。

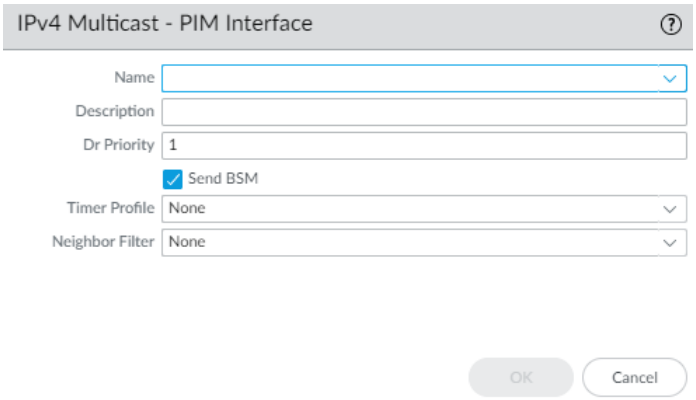


当您通过删除或更改源组访问列表来修改 *PIM* 组权限时，新权限不会从现有流的多播 *RIB* 表 *(mRIB)* 或多播 *FIB* 表 *(mFIB)* 中追溯清除多播路由。要更改 *mRIB* 或 *mFIB* 中现有流的条目，您需要强制离开或清除 *mroute* 条目。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 配置接口的 PIM 特性。

1. 选择 **PIM** > **Interfaces**（接口）并按 **Name**（名称）**Add**（添加）接口。



2. 输入对接口的有用 **Description**（说明）。
3. 指定接口的 **DR Priority**（**DR** 优先级）（指定路由器优先级），以控制哪个路由器将 PIM 加入消息、PIM 注册消息和修剪消息转发到集合点(RP)；范围为 1 - 4,294,967,295；默认值为 1。在 LAN 上的 PIM 设备中，如果配置了 DR 优先级，则优先级值最高的设备被选为 DR。
4. **Send BSM**（发送 **BSM**）以允许传播引导消息（默认启用）。

   高级路由引擎并不能充当 *BSR*，但可以发送和中继 *BSM* 消息。

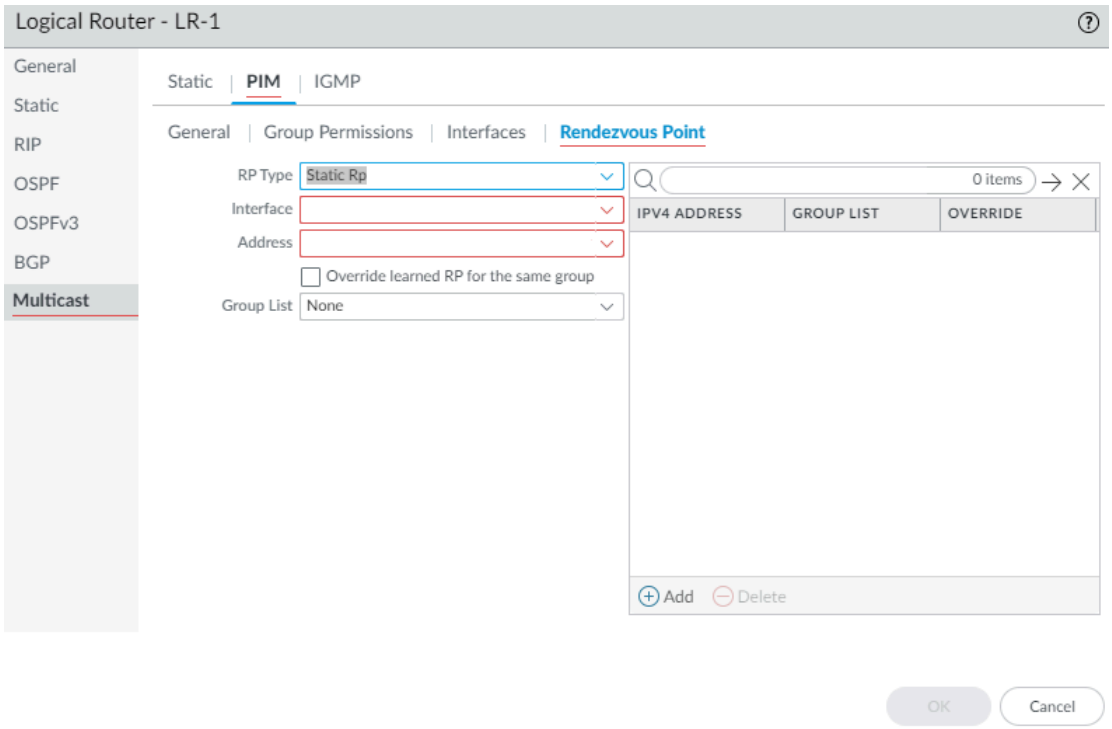
5. 除非通过选择 IPv4 PIM 接口计时器配置文件来覆盖，否则接口的**Timer Profile**（计时器配置文件）将继承自常规 PIM 部分；默认值为 **None**（无）。
6. 使用您创建的访问列表指定**Neighbor Filter**（邻居筛选器），或新建一个访问列表来指定允许成为或拒绝成为逻辑路由器的 PIM 邻居的设备前缀。
7. 单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

STEP 7 | （仅限 ASM）为任意源组播(ASM)环境配置PIM Rendezvous Point (RP)（PIM 集合点(RP)）。

您可以配置候选 *RP* 和静态 *RP*；二者并不相互排斥。

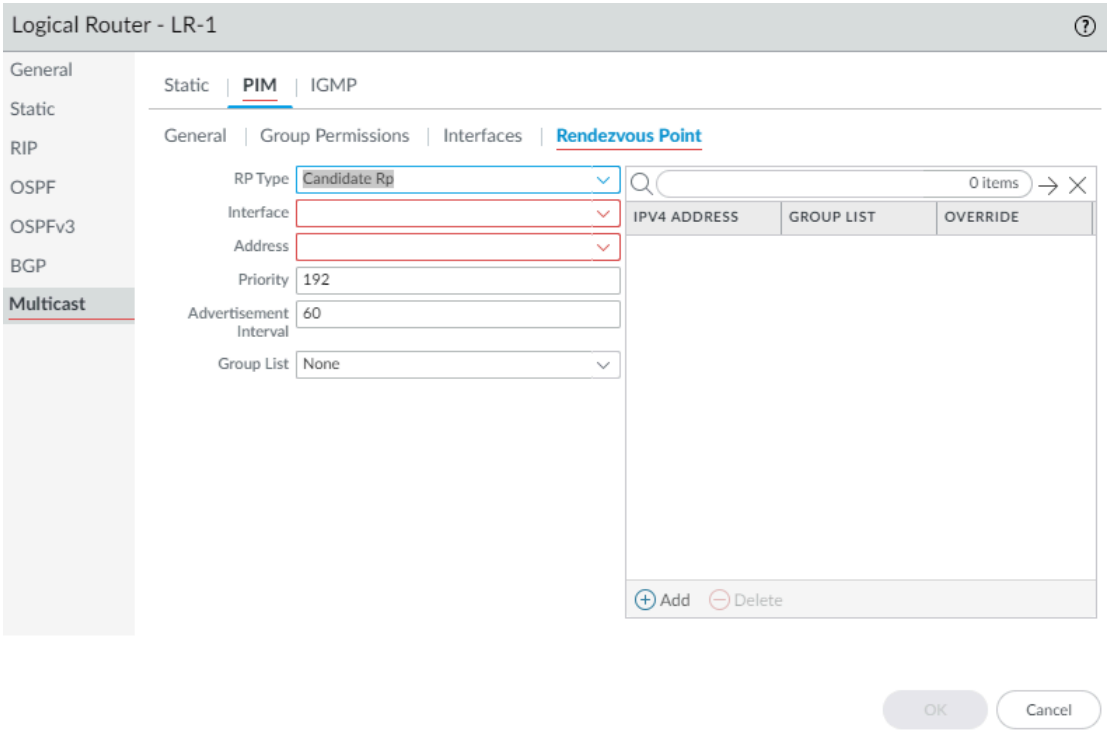
1. 选择 **PIM** > **Rendezvous Point**（集合点）。
2. 选择本地 **RP Type**（**RP** 类型）：**Static RP**（静态 **RP**）或 **Candidate RP**（候选 **RP**）；默认为 **None**（无）。
3. 如果选择 **Static RP**（静态 **RP**），则会建立 RP 到组播组的静态映射。您必须在 PIM 域中的其他 PIM 路由器上明确配置相同的 RP。配置以下设置：
   - 选择 RP 用于接收和发送组播数据包的 RP **Interface**（接口）。有效的接口类型为第 3 层接口（包括以太网、VLAN、回环、聚合以太网(AE)、隧道和子接口）。
   - 选择接口的 **Address**（地址）；所选接口的 IP 地址将填充到列表中。
   - 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。
   - 通过选择Access List（访问列表）或新建一个，指定静态 RP 充当 RP 的组播组的 **Group List**（组列表）。默认为 **None**（无）（无访问列表）。



4. 如果您选择 **Candidate RP**（候选 **RP**）：
   - 选择候选 RP 用于接收和发送组播数据包的 **Interface**（接口）。有效的接口类型为第 3 层接口（包括以太网、VLAN、回环、聚合以太网(AE)、隧道和子接口）。
   - 接口的 **Address**（地址）。
   - 指定候选 RP 的 **Priority**（优先级）；范围为 0 - 255；默认为 192。优先级值越小，表示优先级越高。

 ©2024 Palo Alto Networks, Inc.

- 指定 **Advertisement Interval**（通告间隔），即候选 RP 向其他路由器发送通告的频率（以秒为单位）；范围为 1 - 26,214；默认值为 60。
- 要控制候选 RP 接受的组，请选择一个**Group List**（组列表）（即您创建的 IPv4 访问列表），或新建一个访问列表。默认为 **None**（无）（无访问列表）。如果没有应用访问列表，则逻辑路由器将开始将自己通告为所有组的 RP。



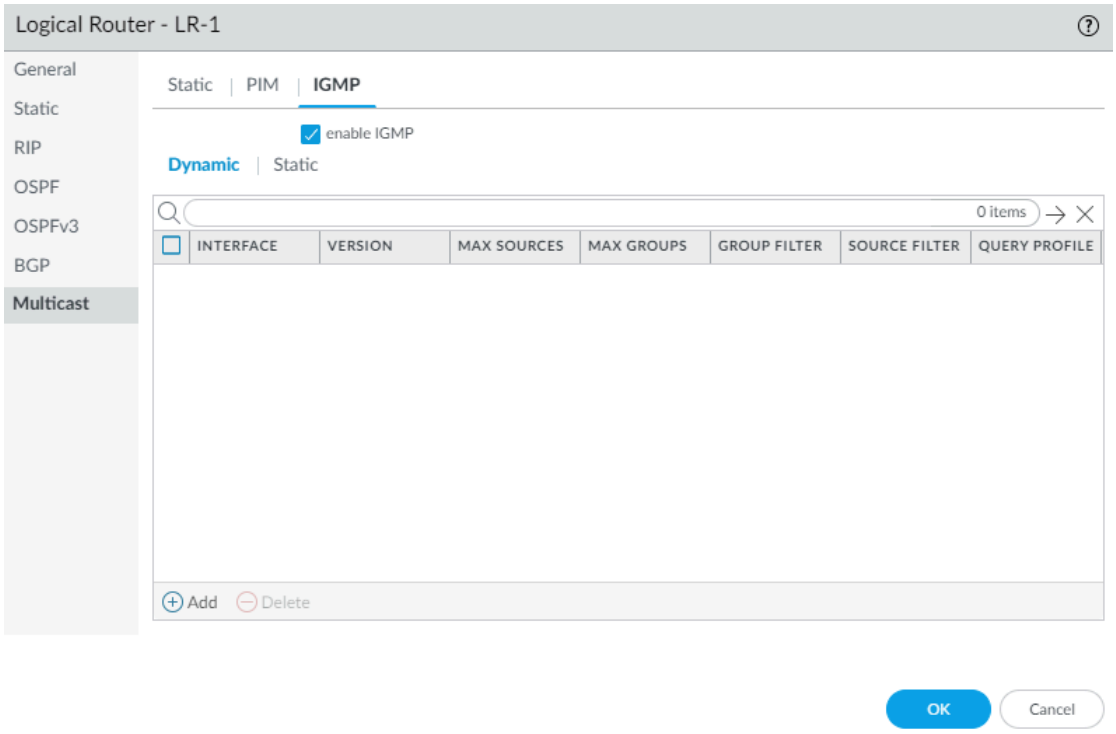
5. **Add**（添加）远程（外部）RP 的 **IPv4 Address**（**IPv4** 地址）。
6. 选择一个**Group List**（组列表），以指定远程 RP 充当 RP 的组播组，或新建一个访问列表。默认为 **None**（无）（无访问列表）。
7. 如果希望将静态配置的远程 RP 用作 RP，而不是为组列表中的组动态获取（选择）的 RP，请选择 **Override**（覆盖）。
8. 单击 **OK**（确定）。

STEP 8 | 单击 **OK**（确定）以保存 PIM 设置。

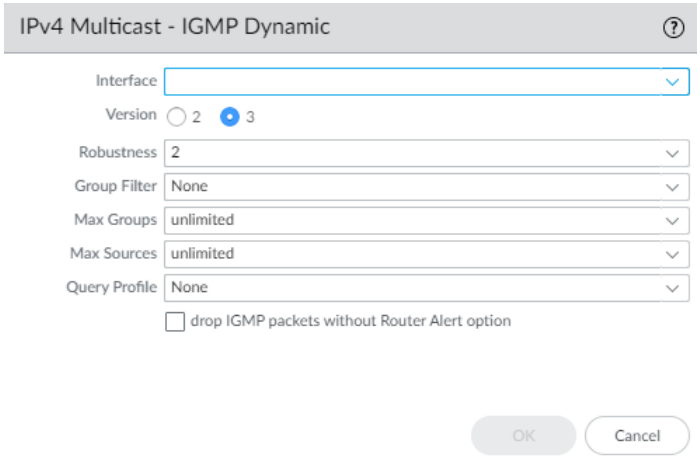
 ©2024 Palo Alto Networks, Inc.

STEP 9 | 在面向组播接收器的接口上启用 IGMP。

1. 选择 **IGMP** 并启用 **IGMP**。



2. 要配置动态 IGMP 接口，请选择 **Dynamic**（动态）。
   1. 通过从列表中选择来 **Add**（添加）**Interface**（接口）。



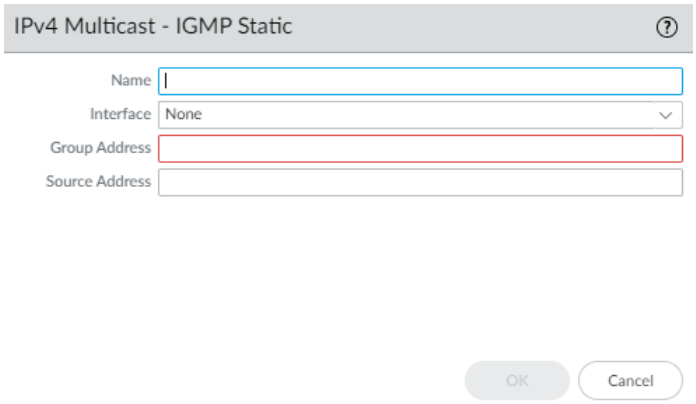
   2. 选择 IGMP **Version**（版本）:**2** 或 **3**。
   3. 选择 **Robustness**（稳定）值，范围为 1 - 7；默认为 2。

> *(Robustness * QueryInterval) + MaxQueryResponseTime* 决定了加入消息在逻辑路由器上的有效时间。如果逻辑路由器收到离开组消息，*Robustness * LastMemberQueryInterval* 是逻辑路由器在删除离开组条目之前等待的时间长度。如果此逻辑路由器所在的子网容易丢失数据包，请增大稳定值。对于加入消息，稳定值 *1* 将被忽略。对于离开组消息，逻辑路由器还将稳定值用作最后一个成员查询计数。

 ©2024 Palo Alto Networks, Inc.

4. 对于 **Group Filter**（组筛选），请选择一个访问列表或新建一个，以控制接口将接受 IGMP 加入的源和组；默认为 **None**（无）（无访问列表）。
5. 对于 **Max Groups**（最大组数），输入 IGMP 可以同时为接口处理的最大组数。范围为 1 - 65,535；默认为 **unlimited**（无限制），表示该范围内的最大值。
6. 对于 **Max Sources**（最大源数），输入 IGMP 可以同时为接口处理的最大源数。范围为 1 - 65,535；默认为 **unlimited**（无限制），表示该范围内的最大值。
7. 对于 **Query Profile**（查询配置文件），请选择所创建的 IGMP 接口查询配置文件或新建一个，以应用于接口；默认值为 **None**（无）。
8. 选择 丢弃无路由器警报选项的 **IGMP** 数据包，以要求传入的 IGMPv2 或 IGMPv3 数据包具有 IP 路由器警报选项 RFC 2113，否则将其丢弃。（默认为禁用。）
9. 单击 **OK**（确定）以保存动态 IGMP 接口。

3. 要配置静态 IGMP 接口，请选择 **Static**（静态）。
   1. 按 **Name**（名称）**Add**（添加）静态接口。



   2. 选择要充当静态 IGMP 接口的**Interface**（接口）。
   3. 输入静态 IGMP 成员的组播 **Group Address**（组地址）。
   4. 输入将组播流量传输到组播组（S、G）的发送端的 **Source Address**（源地址）。静态 IGMP 接口上允许此（S、G）组合的流量。
   5. 单击 **OK**（确定）以保存静态 IGMP 接口。

STEP 10 | 单击 **OK**（确定）以保存多播配置。

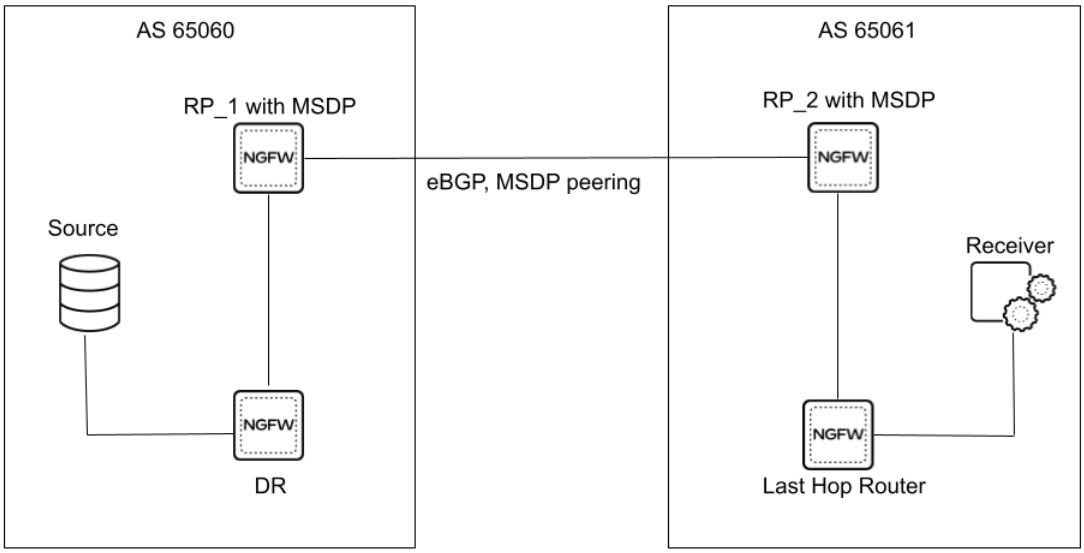
STEP 11 | **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

配置 MSDP

高级路由模式支持 PIM 稀疏模式 (PIM-SM) 中的多播源发现协议 (MSDP)。启用了 MSDP 的防火墙位于一个域对等体中，启用了 MDSP 的设备位于另一个域或自治系统中。对等方交换控制信息并发现自己域外的多播源。MSDP 跟踪活动源并与配置的对等方共享。MSDP 允许域使用域间源树，从而降低了互连多个 PIM-SM 域的复杂性。

在示例 MSDP 拓扑中，多播源和接收器位于不同的域中。每个多播域中都有给定多播组的单个 RP。使用 MSDP，RP_1 向 RP_2 通知 RP_1 充当集合点的活动源。RP_2 能够跨域边界创建多播树。



MSDP 使用众所周知的 TCP 端口 639 进行对等连接。IP 地址较高的对等方侦听端口 639；具有较低 IP 地址的对等方尝试主动连接端口 639。在配置 MSDP 之前，请熟悉 RFC 3618。以下任务假设您已经配置了 IPv4 多播。

支持的 MSDP 消息类型有：

- **Source Active (SA)** — 包含始发集合点 (RP) 的 IP 地址以及通告的一对或多对 (S、G)。也可以包含封装的数据包。
- **Keepalive** —发送该消息是为了保持 MSDP 会话处于活动状态。如果在保持时间间隔内未收到 keepalive 或 SA 消息，则重置 MSDP 会话。
- **Notification**（通知） —在检测到错误时发送。

RP 路由器之间的 MSDP TCP 连接需要底层 IP 单播网络。BGP IPv4 单播必须参与才能与对等方确认反向路径转发 (RPF) 检查，从而保持域间的无环转发。

可以在配置之前或在配置 MSDP 的过程中创建多播路由配置文件。

STEP 1 | 配置逻辑路由器.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。

STEP 3 | 选择 **Multicast**（组播）并启用组播协议。

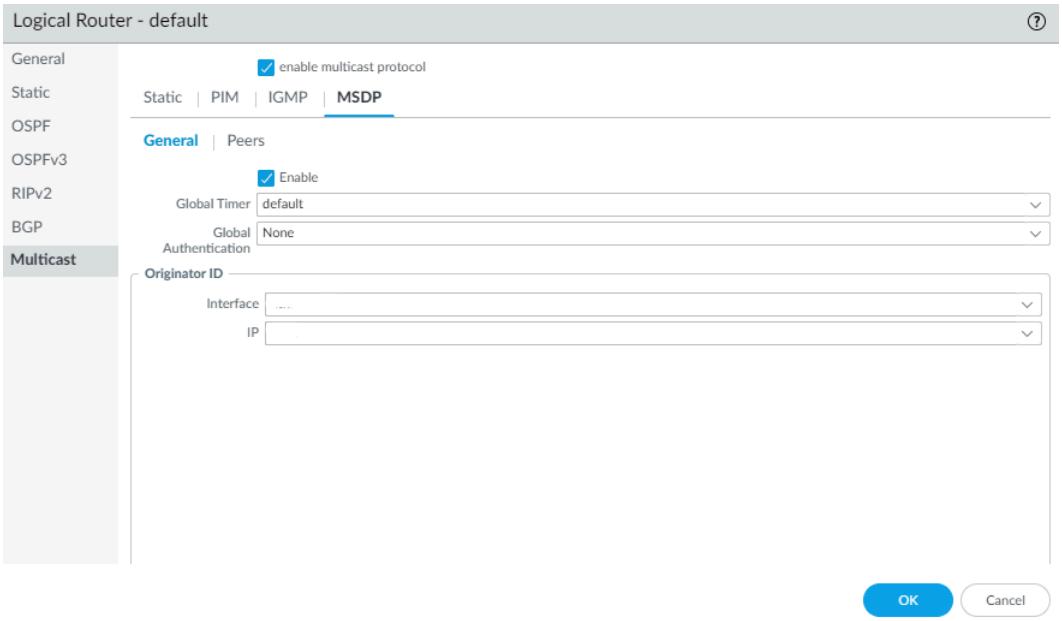
STEP 4 | 选择 **MSDP** > **General**（常规）并 **Enable**（启用） MSDP。

STEP 5 | 选择 **Global Timer**（全局计时器）配置文件，或选择默认配置文件（这是默认设置），或者创建新的计时器配置文件。如果选择默认值，则保持活动间隔设置为 60，消息超时设置为 75，连接重试间隔设置为 30。如果选择 **None**（无），则默认值适用。

STEP 6 | 选择 **Global Authentication**（全局身份验证）配置文件或创建一个新的配置文件。默认为 **None**（无）。

STEP 7 | 对于始发者 ID，选择逻辑路由器用作 Source-Active (SA) 消息中的 RP 接口的 **Interface**（接口）。

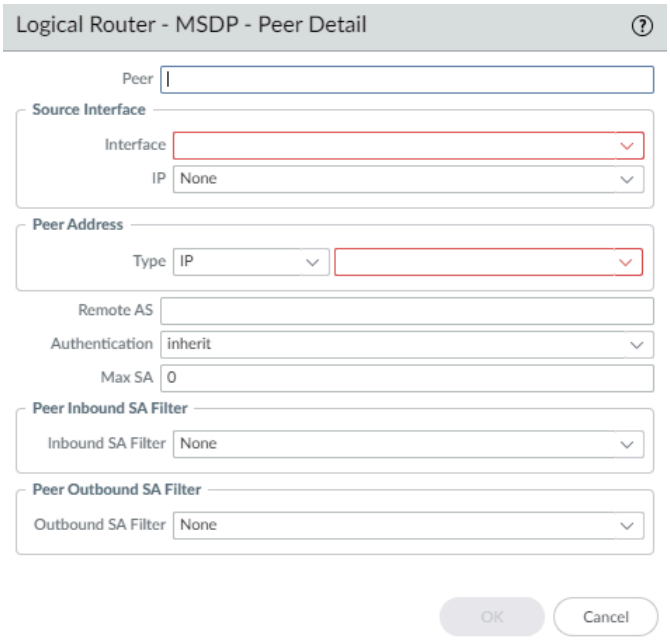
STEP 8 | 选择或输入逻辑路由器在 SA 消息中用作 RP 地址的 **IP Address**（IP 地址）（带前缀长度）。如果未配置始发者 IP 地址，则逻辑路由器使用 PIM RP 地址封装 SA 消息。



STEP 9 | 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 10 | 选择 **Peers**（对等方） 并 **Add**（添加） **Peer**（对等方）名称（最多 63 个字符）。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以由字母数字字符、下划线、连字符或句点组合而成。不允许使用空格。



STEP 11 | 输入用于通过 TCP 与其 MSDP 对等体建立 MSDP 连接的源 **Interface**（接口）。

STEP 12 | 选择源接口的 **IP** 地址。默认为 **None**（无）。

STEP 13 | 选择对端地址的 **Type**（类型）：

- **IP** —（默认），然后选择地址对象或输入 IP 地址。
- **FQDN** —选择或输入对等方的完全限定域名。下拉列表显示所有配置为地址对象的 FQDN 名称。

STEP 14 | 输入 MSDP 对等体所在的 **Remote AS**（远程 **AS**） 的 BGP 自治系统编号。

STEP 15 | 对于 **Authentication**（身份验证），请执行以下操作之一：

- 选择要应用于此对等体的身份验证配置文件，该配置文件将覆盖您在常规页面上应用于 MSDP 的全局身份验证配置文件。
- 继承（从全局身份验证继承）（默认）全局身份验证配置文件。
- 选择 **None**（无）可禁用对此对等体的身份验证，这将覆盖全局身份验证配置文件。

STEP 16 | 对于 **Max SA**（最大 **SA**），输入 SA 缓存将接受来自此 MSDP 对等体的Source-Active (SA) 条目的最大数量。范围为 0 到 1,024；默认值为 0（无限制）。达到此最大值后，来自该对等体的新 SA 消息将被丢弃。

 ©2024 Palo Alto Networks, Inc.

STEP 17 | 对于 **Peer Inbound SA Filter**（对等入站 **SA** 筛选器），选择访问列表或创建新的访问列表，以筛选来自该对等方的传入 SA 消息（阻止不想要的组）。默认为 **None**（无）。

访问列表可以指定 (S, G) 对中的源地址进行筛选，也可以指定 (S, G) 对中的目标（组）地址进行筛选，或两者兼而有之。

STEP 18 | 对于 **Peer Inbound SA Filter**（对等入站 **SA** 筛选器），选择访问列表或创建新的访问列表，以筛选传播到该对等方的传出 SA 消息（阻止不想要的组）。默认为 **None**（无）。

访问列表可以指定 (S, G) 中的源地址进行筛选，也可以指定 (S, G) 中的目标（组）地址进行筛选，或两者兼而有之。

STEP 19 | 单击 **OK**（确定）。

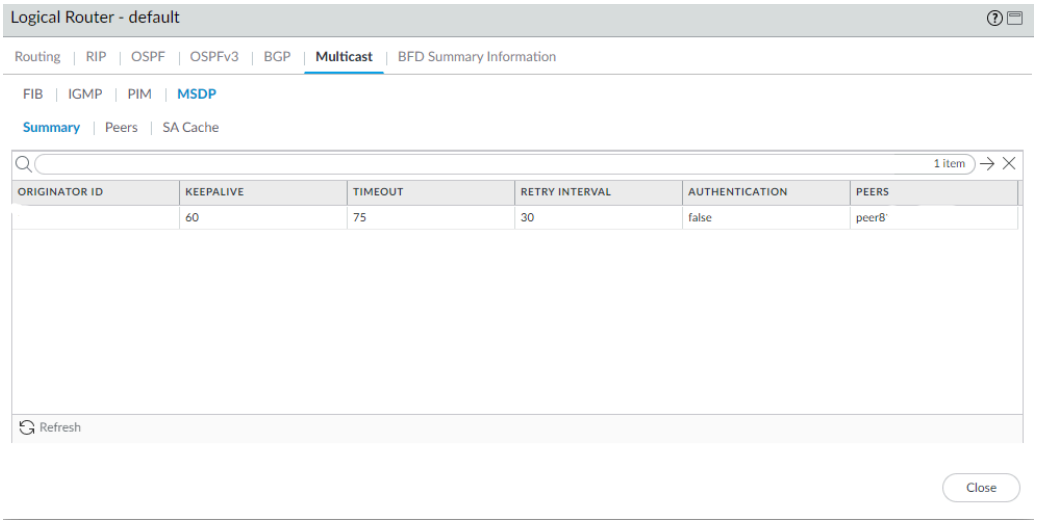
STEP 20 | 创建 MSDP 身份验证和计时器配置文件（如果尚未创建）。

STEP 21 | **Commit**（提交）。

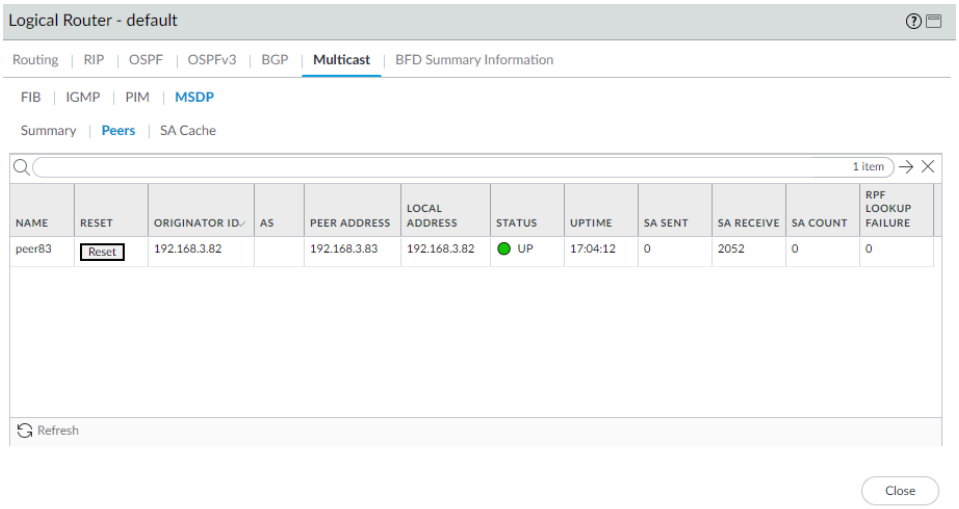
 ©2024 Palo Alto Networks, Inc.

STEP 22 | 查看 MSDP 信息。

1. 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后在您配置的逻辑路由器的行中，选择 **More Runtime Stats**（更多运行时统计）。
2. 选择 **Multicast**（多播） > **MSDP** > **Summary**（摘要） 以查看常规 MSDP 信息，例如始发者 IP 地址、计时器、身份验证和对等方名称。

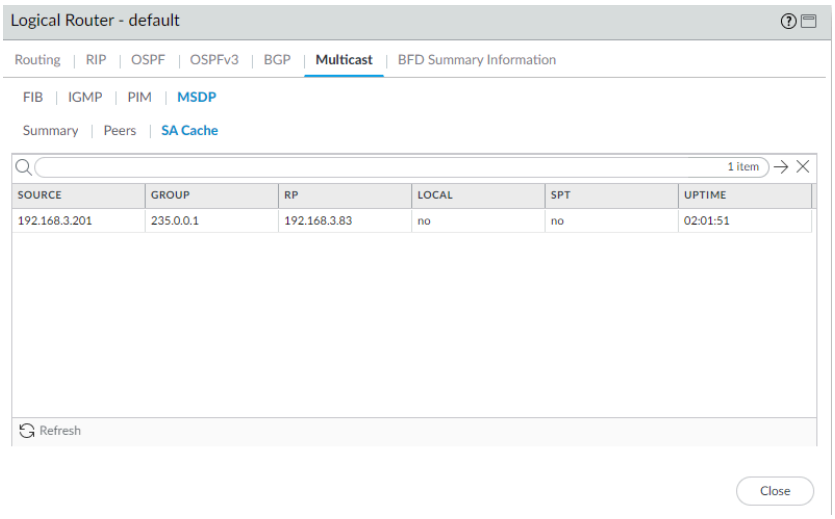


3. 选择 **Peers**（对等体） 以查看有关 MSDP 对等方的信息。



4. 选择 **SA Cache**（**SA** 缓存） 可查看缓存中的 Source-Active 条目。

 ©2024 Palo Alto Networks, Inc.



5. **Refresh**（刷新）或**Close**（关闭）运行时统计信息。

 ©2024 Palo Alto Networks, Inc.

创建多播路由配置文件

在高级路由引擎中，创建以下路由配置文件以应用于 IPv4 组播配置：

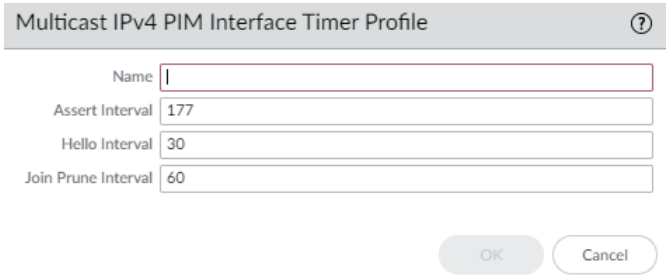
- **Multicast IPv4 PIM Interface Timer Profiles**（组播 **IPv4 PIM** 接口计时器配置文件） — 在 PIM 的常规选项卡（接口通用计时器）和 PIM 的接口选项卡中使用，以覆盖接口通用计时器。
- **Multicast IPv4 IGMP Interface Query Profiles**（组播 **IPv4 IGMP** 接口查询配置文件） — 在 IGMP 选项卡中用于动态 IGMP 接口。

创建以下多播源发现协议 (MSDP) 配置文件以应用于 MSDP 配置。

- **MSDP Authentication Profiles**（**MSDP** 身份验证配置文件）- 在 MSDP 常规选项卡上使用以全局应用配置文件，在 MSDP 对等选项卡上使用以覆盖全局身份验证配置文件。MSDP 使用 MD5 身份验证。
- **MSDP Timer Profiles**（**MSDP** 计时器配置文件）- 在 MSDP 常规选项卡上使用。

STEP 1 | 创建组播 IPv4 PIM 接口计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Multicast**（组播）。
2. 按 **Name**（名称）（最多63个字符）**Add**（添加）**Multicast IPv4 PIM Interface Timer Profile**（组播 **IPv4 PIM** 接口计时器配置文件）。名称必须以字母数字字符、下划线(_)或连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。
3. 指定 **Assert Interval**（断言间隔） — 逻辑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 1 - 65,534；默认为 177）。
4. 指定 **Hello Interval**（**Hello** 间隔） — 逻辑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 1 到 180；默认为 30）。
5. 指定 **Join Prune Interval**（加入剪枝间隔） — 虚拟路由器向上游发送组播源的 PIM 加入消息（和 PIM 剪枝消息）之间的秒数（范围为 60 - 600；默认为 60）。



6. 单击 **OK**（确定）。

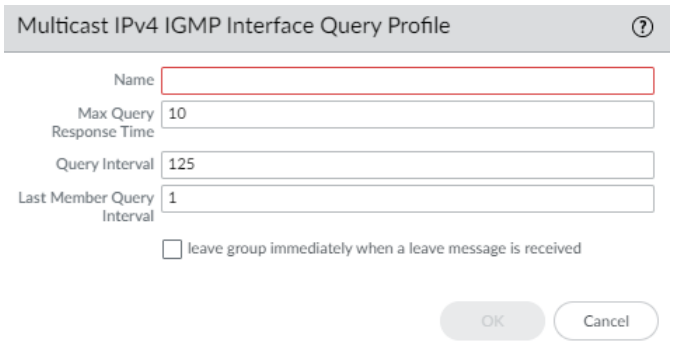
STEP 2 | 创建组播 IPv4 IGMP 接口查询配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Multicast**（组播）。
2. 按 **Name**（名称）（最多63个字符）**Add**（添加）**Multicast IPv4 IGMP Interface Query Profile**（组播 **IPv4 IGMP** 接口查询配置文件）。名称必须以字母数字字符、下划线(_)或

 ©2024 Palo Alto Networks, Inc.

连字符(-)开头，可以由字母数字字符、下划线或连字符组合而成。但不得包含句点(.)或空格。

3. 指定 **Max Query Response Time**（最大查询响应时）— 在逻辑路由器决定此接收器不再想要为该组接收组播数据包之前，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 1 - 25；默认为 10）。
4. 指定 **Query Interval**（查询间隔）— 逻辑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组播数据包的 IGMP 成员资格查询之间的秒数（范围为 1 - 1,800；默认为 125）。
5. 指定 **Last Member Query Interval**（最后成员查询间隔）— 在接收器发送离开组消息后，允许接收器向逻辑路由器发送的特定于组的查询做出响应的秒数（范围为 1 - 25；默认为 1）。
6. 如果启用 **leave group immediately when a leave message is received**（在收到离开消息后立即离开组），当组播组内仅有一位成员，且逻辑路由器接收到该组的 IGMP 离开消息时，该设置将导致逻辑路由器立即将组播路由信息库(mRIB)和组播转发信息库(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。启用此设置可节省网络资源。（默认为禁用。）



7. 单击 **OK**（确定）。

STEP 3 | 创建 MSDP 身份验证配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Multicast**（组播）。
2. 按 **Name**（名称） **Add**（添加）**Multicast MSDP Authentication Profile**（多播 **MSDP** 身份验证配置文件）（最多 63 个字符）。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以由字母数字字符、下划线、连字符或句点组合而成。不允许使用空格。
3. 输入 **Secret**（密钥）（允许使用字母数字字符、!、@、#、% 和 ^）。
4. **Confirm Secret**（确认密钥）。
5. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 创建 MSDP 计时器配置文件。

1. 选择 **Network**（网络） > **Routing**（路由） > **Routing Profiles**（路由配置文件） > **Multicast**（组播）。
2. 按 **Name**（名称） **Add**（添加）**Multicast MSDP Timer Profile**（多播 **MSDP** 计时器配置文件）（最多 63 个字符）。名称必须以字母数字字符、下划线 (_)、连字符 (-) 或句点 (.) 开头，可以由字母数字字符、下划线、连字符或句点组合而成。不允许使用空格。
3. 以秒为单位输入 **Keep Alive Interval**（保持活动间隔）；范围是 1 到 60；默认值为 60。与对等体建立 MSDP 传输连接后，连接的每一端都会按此时间间隔向另一端发送 Keepalive 消息，以保持 MSDP 会话处于活动状态。如果计时器超时，对等方发送一条 Keepalive 消息并重置计时器。如果在消息超时间隔内没有收到 Keepalive 或 SA 消息，则 MSDP 会话将重置。
4. 输入以秒为单位的 **Message Timeout**（消息超时） 间隔，这是 MSDP 对等方在宣布其他对等方关闭之前等待来自其他对等方的 Keepalive 消息的间隔。范围为 1 至 75，默认为 75。
5. 输入以秒为单位的 **Connection Retry Interval**（连接重试间隔），这是对等会话重置后尝试重新建立对等会话之前对等方将等待的间隔。范围为 1 至 60，默认为 30。
6. 单击 **OK**（确定）。

STEP 5 | **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.

创建 IPv4 MRoute

高级路由引擎允许您为逻辑路由器配置 IPv4 组播路由。回想一下，PIM 通过检查单播 RIB 来检查防火墙是否在防火墙用于将单播数据包发送回源的同一接口上接收数据包。

在希望单播数据包采用与组播数据包不同路由的拓扑结构中，可以配置 mroute。mroute 是指向组播源的静态单播路由；mroute 存储在组播 RIB(MRIB)中。PIM 使用 mroute 进行 RPF 检查，而不是使用单播 RIB 进行 RPF 检查。PIM 是使用 MRIB 还是 URIB 进行 RPF 检查取决于为 PIM 配置的 RPF 查找模式。在 RPF 检查期间，使用的 mroute 是具有最长前缀匹配的 mroute。

mroute 非常有用，例如，当路径上的某些设备不支持组播路由时，可以使用隧道来连接组播路由器。

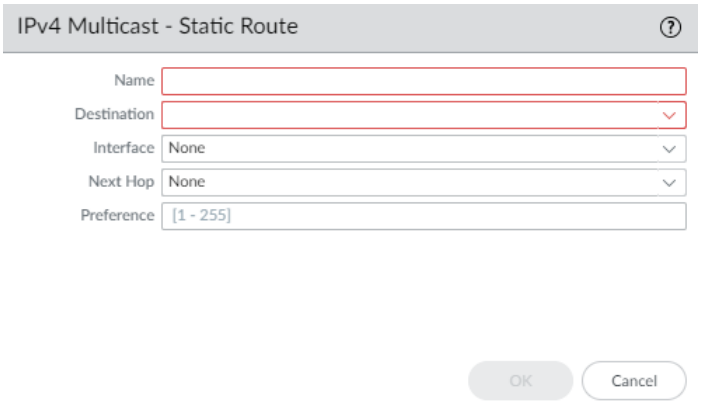
STEP 1 | 配置逻辑路由器.

STEP 2 | 选择 **Network**（网络） > **Routing**（路由） > **Logical Routers**（逻辑路由器），然后选择一个逻辑路由器。

STEP 3 | 选择 **Multicast**（组播）并启用组播协议。

STEP 4 | 建立 mroute。

1. 选择 **Static**（静态）并按 **Name**（名称）**Add**（添加）mroute。名称必须以字母数字字符、下划线 (_) 或连字符 (-) 开头，可以包含零个或多个字母数字字符、下划线或连字符。但不得包含句点(.)或空格。



2. 输入 mroute 的 **Destination**（目标）（IPv4 地址/掩码或地址对象），即防火墙执行 RPF 检查的组播源或子网。
3. 为到组播源的单播路由选择传出 **Interface**（接口）。
4. 输入指向源的 **Next Hop**（下一个跃点）路由器的 IPv4 地址（或地址对象）。
5. 输入路由的 **Preference**（首选项）；范围为 1 - 255。
6. 单击 **OK**（确定）。

STEP 5 | 单击 **OK**（确定）。

STEP 6 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

PoE

您可以在支持的防火墙的接口上配置以太网供电 (PoE)，将电能从防火墙传输到连接的受电设备 (PD)。这使您可以满足 PoE 的电源需求，同时继续使用每个物理 PoE 端口使用一条以太网电缆向其传输数据。

- PoE 概述
- 配置 PoE

PoE 概述

下表列出了每个带有 PoE 端口的 Palo Alto Networks® 下一代防火墙以及它们提供的最大功率、允许的总功率预算及其支持的接口类型。

防火墙	**PoE** 端口	最大预留功率（每个端口）	允许的 **PoE** 总预算（所有端口）	支持的接口类型
PA-415 和 PA-445	6、7、8 和 9	60W	91W	• 聚合以太网 (AE) • 高可用性 (HA) • 第 2 层 • 第 3 层 • 旁接 • 虚拟线路
PA-1410 和 PA-1420	9、10、11 和 12	90W	151W	

选择 **Dashboard**（仪表板） > **Widgets**（小部件） > **System**（系统） > **Interfaces**（接口）以显示每个端口的当前状态。PoE 端口用闪电图标表示。将鼠标悬停在 PoE 端口图标上方可显示 PoE 状态、已分配功率、已用功率和其他配置的详细信息。

同样，选择 **Dashboard**（仪表板） > **Widgets**（小部件） > **System**（系统） > **PoE Power Budget**（**PoE** 供电预算） 以显示圆环图，确认防火墙的可用电量并帮助您决定将哪些 PD 连接到 PoE 端口。

©2024 Palo Alto Networks, Inc.

配置 PoE

以下任务介绍了在防火墙上设置 PoE 的过程。

STEP 1 | 确保要为其供电的设备已使用以太网电缆通过防火墙上受支持的 PoE 端口连接到防火墙。

使用 *Cat 5* 或 *Cat6* 以太网电缆可确保最可靠的电力传输。例如，*Cat 3* 电缆只能传输 *20 W* 的功率。

STEP 2 | 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后选择已连接电缆的接口。

STEP 3 | 默认情况下，PoE 在所有 PoE 端口上处于活动状态。在以太网接口窗口中，选择 **Advanced**（高级）并查看 **PoE Settings**（**PoE** 设置）将显示 **PoE Enable**（**PoE** 启用）已启用。

您还可以使用 *CLI* 启用或禁用 *PoE*。使用终端仿真软件登录到防火墙后，输入 ***configure***，然后输入 ***set network interface ethernet ethernet1/9 poe poe-enabled {yes | no}***，其中“*ethernet 1/9*”对应于您希望启用或禁用的 *PoE* 端口。

在继续下一步之前，确定所连接的受电设备 *(PD)* 支持的最大功率量。该值取决于 *PD* 的类型和等级。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 通过输入 **PoE Rsvd Pwr** 的值（以瓦特为单位），设置端口保留的电量。此值必须是一个介于 **0** 和 PoE 概述 中定义的端口最大保留功率之间的数字。**0** 表示该 PoE 端口未保留电源。

您还可以使用 *CLI* 配置 *PoE* 保留电源。输入 ***configure***，然后输入 ***set network interface ethernet1/9 poe poe-rsvd-pwer <value>***，其中“*ethernet 1/9*”对应于您要配置的 *PoE* 端口，“*<value>*”表示从 *0* 到接口支持的最大功率的瓦特数。

所有 *PoE* 端口的总 ***PoE Rsvd Pwr*** 不应超过允许的 *PoE* 总预算。如果超过允许的 *PoE* 总预算，一个或多个通电设备将进入 ***Den***（电源被拒绝）状态，直到重新分配保留电源。

PoE 端口还可以基于当前的总分配功率进入 ***Den*** 或 ***Dis***（禁用）状态。总分配功率是指所有 *PoE* 端口的保留功率之和或所有 *PD* 允许的实际分配功率之和。如果总保留功率小于总实际分配功率，则 *PoE* 端口进入 ***Dis*** 或 ***Den*** 状态。

处于 ***Dis*** 或 ***Den*** 状态的 *PoE* 端口无法通过断开并重新连接 *PD* 来解决。相反，应使用以下方法之一来恢复检测连接的 *PD* 上的电源：

- 通过取消选中 ***PoE Enable***（*PoE* 启用），禁用接口上的 *PoE*。应用该设置，然后返回到同一接口并选中 ***PoE Enable***（*PoE* 启用）。
- 将受影响的端口链接状态设置为 ***auto***（自动）或 ***up***（启动）。
- 将受影响的 *PoE* 端口的 ***PoE Rsvd Pwr*** 更改为等于大于 *PD* 的电源要求。

如果没有设备连接到 *PoE* 端口，请确保未选中 ***PoE Enable***（*PoE* 启用）或 ***PoE Rsvd Pwr*** 值为 ***0***，以避免消耗部分 *PoE* 预算。

STEP 5 | 单击 **OK**（确定）。

STEP 6 | **Commit**（提交）更改。

STEP 7 | 通过检查防火墙 Web 接口或 CLI 验证 PoE 端口的状态。

1. 要通过防火墙 Web 接口进行验证，请登录防火墙并选择 **Dashboard**（仪表板） > **Widgets**（小部件） > **System**（系统） > **Interfaces**（接口）。将鼠标悬停在 PoE 端口图标上（由闪电符号标识），以了解特定接口的详细信息。选择 **Dashboard**（仪表板） > **Widgets**（小部件） > **System**（系统） > **PoE Power Budget**（**PoE** 供电预算）以获取电源分配信息。要查看状态消息和其他 PoE 信息，请选择 **Network**（网络） > **Interfaces**（接口） > **PoE**。
2. 要使用 CLI 进行验证，请输入 **`show poe`** 或 **`show poe detail`**。

 ©2024 Palo Alto Networks, Inc.