PAN-OS Web 界面帮助

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

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

Last Revised

December 10, 2020

Table of Contents

Web 界面基础知识 13
防火墙概述 14
功能与优点 15
最后登录时间及失败登录尝试 16
每日消息 17
任务管理器 18
语言 20
警报 21
提交更改 22
保存待选配置 25
恢复更改 28
锁定配置 31
全局查找 32
威胁详细信息 33
AutoFocus 情报摘要 35
配置表格导出 37

仪表盘 39
仪表盘小部件 40

ACC 43
ACC 简介 44
ACC 选项卡 46
ACC 小部件 47
ACC 操作 49
使用选项卡和小部件 49
使用过滤器 — 本地过滤器和全局过滤器 50

监视 53
Monitor（监控）> Logs（日志）..... 54
日志类型 54
日志操作 58
Monitor（监控）> External Logs（外部日志）..... 61
Monitor（监控）> Automated Correlation Engine（自动关联引擎）..... 62
Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlation Objects（关联对象）..... 62
Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlated Events（关联事件）..... 63
Monitor（监控）> Packet Capture（数据包捕获）..... 65
数据包捕获概述 65
构建自定义数据包捕获的块 66
启用威胁数据包捕获 67
监视 > App Scope 69
App Scope 概述 69
App Scope 摘要报告 69
App Scope 更改监控报告 70
App Scope 威胁监控报告 72

App Scope 威胁地图报告 73
App Scope 网络监控报告 75
App Scope 流量地图报告 76
监视 > 会话浏览器 78
Monitor（监控）> Block IP List（阻止 IP 列表）..... 79
阻止 IP 列表条目 79
查看或删除阻止 IP 列表条目 80
监视 > Botnet 81
Botnet 报告设置 81
Botnet 配置设置 81
Monitor（监控）> PDF Reports（PDF 报告）..... 83
Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要）..... 83
监视 > PDF 报告 > 用户活动报告 84
Monitor（监控）> PDF Reports（PDF 报告）> SaaS Application Usage（SaaS 应用程序使用）..... 85
Monitor（监控）> PDF Reports（PDF 报告）> Report Groups（报告组）..... 87
Monitor（监控）> PDF Reports（PDF 报告）> Email Scheduler（电子邮件调度程序）..... 88
Monitor（监控）> Manage Custom Reports（管理自定义报告）..... 89
监测 > 报告 91

策略 93
策略类型 94
移动或克隆策略规则 95
审核注释存档 96
审核注释 96
配置日志（在注释之间）..... 96
规则更改 97
规则使用点击数查询 98
规则使用点击数查询的设备规则使用情况 98
Policies（策略）> Security（安全）..... 100
安全策略概述 100
安全策略规则中的构建块 101
创建和管理策略 108
替代或恢复安全策略规则 111
应用程序和使用情况 113
安全策略优化器 115
Policies（策略）> NAT 117
NAT 策略常规选项卡 117
NAT 原始数据包选项卡 118
NAT 转换后数据包选项卡 118
NAT 主动/主动 HA 绑定选项卡 120
NAT Target（NAT 目标）选项卡 121
Policies（策略）> QoS 122
Policies（策略）> Policy Based Forwarding（基于策略的转发）..... 126
基于策略的转发常规选项卡 126
基于策略的转发源选项卡 127
基于策略的转发目标/应用程序/服务选项卡 127
基于策略的转发转发选项卡 128
Policy Based Forwarding Target（基于策略的转发目标）选项卡 129
Policies（策略）> Decryption（解密）..... 130
解密常规选项卡 130

解密源选项卡 131
解密目标选项卡 132
解密服务/URL 类别选项卡 132
解密选项选项卡 132
Decryption Target（解密目标）选项卡 133
Policies（策略）> Tunnel Inspection（隧道检测）135
隧道检测策略中的构建块 135
Policies（策略）> Application Override（应用程序替代）140
应用程序替代常规选项卡 140
应用程序替代源选项卡 141
应用程序替代目标选项卡 141
应用程序替代协议/应用程序选项卡 142
Application Override Target（应用程序覆盖目标）选项卡 142
Policies（策略）> Authentication（身份验证）143
身份验证策略规则中的构建块 143
创建和管理身份验证策略 147
Policies（策略）> DoS Protection（DoS 保护）149
DoS 保护常规选项卡 149
DoS 保护源选项卡 150
DoS 保护目标选项卡 150
DoS 保护选项/保护选项卡 151
DoS Protection Target（DoS 保护目标）选项卡 153
Policies（策略）> SD-WAN 154
SD-WAN“General”（常规）选项卡 154
SD-WAN“Source”（源）选项卡 154
SD-WAN“Destination”（目标）选项卡 155
SD-WAN“Application/Service”（应用程序/服务）选项卡 156
SD-WAN“Path Selection”（路径选择）选项卡 157
SD-WAN“Target”（目标）选项卡 157

对象 159
移动、克隆、替代或恢复对象 160
移动或克隆对象 160
替代或恢复对象 160
Objects（对象）> Addresses（地址）161
Objects（对象）> Address Groups（地址组）163
Objects（对象）> Regions（地区）165
Objects（对象）> Dynamic User Groups（动态用户组）166
Objects（对象）> Applications（应用程序）168
应用程序概述 168
应用程序支持的操作 171
定义应用程序 173
Objects（对象）> Application Groups（应用程序组）177
Objects（对象）> Application Filters（应用程序过滤器）178
Objects（对象）> Services（服务）179
Objects（对象）> Services Groups（服务组）181
Objects（对象）> Tags（标记）182
创建标记 182
将规则库视为组 183
管理标记 186
Objects（对象）> Devices（设备）188
Objects（对象）> External Dynamic Lists（外部动态列表）189
Objects（对象）> Custom Objects（自定义对象）193

Objects（对象）> Custom Objects（自定义对象）> Data Patterns（数据模式）.....193
Objects（对象）> Custom Objects（自定义对象）> Spyware/Vulnerability（间谍软件/漏洞）.....198
Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）.....201
Objects（对象）> Security Profiles（安全配置文件）.....203
安全配置文件中的操作.....203
Objects（对象）> Security Profiles（安全配置文件）> Antivirus（防病毒）.....206
Objects（对象）> Security Profiles（安全配置文件）> Anti-Spyware Profile（防间谍软件配置文件）.....209
Objects（对象）> Security Profiles（安全配置文件）> Vulnerability Protection（漏洞保护）.....213
Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）.....217
URL 过滤常规设置.....217
URL 过滤类别.....218
URL 过滤设置.....220
用户凭据检测.....221
HTTP 标头插入.....222
URL 过滤 Inline ML.....223
Objects（对象）> Security Profiles（安全配置文件）> File Blocking（文件传送阻止）.....225
Objects（对象）> Security Profiles（安全配置文件）> WildFire Analysis（WildFire 分析）.....227
Objects（对象）> Security Profiles（安全配置文件）> Data Filtering（数据过滤）.....228
Objects（对象）> Security Profiles（安全配置文件）> DoS Protection（DoS 保护）.....230
Objects（对象）> Security Profiles（安全配置文件）> Mobile Network Protection（移动网络保护）.....233
Objects（对象）> Security Profiles（安全配置文件）> SCTP Protection（SCTP 保护）.....238
Objects（对象）> Security Profile Groups（安全配置文件组）.....243
Objects（对象）> Log Forwarding（日志转发）.....244
Objects（对象）> Authentication（身份验证）.....247
Objects（对象）> Decryption Profile（解密配置文件）.....249
解密配置文件常规设置.....249
控制解密流量的设置.....250
控制未解密流量的设置.....254
控制解密 SSH 流量的设置.....255
Objects（对象）> Decryption（解密）> Forwarding Profile（转发配置文件）.....256
Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）.....258
Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Path Quality Profile（路径质量配置文件）.....258
Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> SaaS Quality Profile（SaaS 质量配置文件）.....259
Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Traffic Distribution-Profile（流量分发配置文件）.....260
Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Error Correction Profile（纠错配置文件）.....260
Objects（对象）> Schedules（计划）.....262

网络.....263
Network（网络）> Interfaces（接口）.....264
防火墙接口概述.....264
防火墙接口的通用构建块.....265
PA-7000 系列防火墙接口的通用构建块.....266

旁接接口 267
HA 接口 267
虚拟线路接口 268
虚拟线路子接口 269
PA-7000 系列第 2 层接口 270
PA-7000 系列第 2 层子接口 271
PA-7000 系列第 3 层接口 272
第 3 层接口 280
第 3 层子接口 288
日志卡接口 295
日志卡子接口 296
解密镜像接口 297
聚合以太网 (AE) 接口组 297
聚合以太网 (AE) 接口 300
Network（网络）> Interfaces（接口）> VLAN 305
Network（网络）> Interfaces（接口）> Loopback（回环） 312
Network（网络）> Interfaces（接口）> Tunnel（隧道） 314
Network（网络）> Interfaces（接口）> SD-WAN 316
Network（网络）> Zones（区域） 317
安全区域概述 317
安全区域的构建块 317
Network（网络）> VLAN 320
Network（网络）> Virtual Wires（虚拟线路） 321
Network（网络）> Virtual Routers（虚拟路由器） 322
虚拟路由器的常规设置 322
静态路由 323
路由重新分发 325
RIP 326
OSPF 328
OSPFv3 332
BGP 337
IP 多播 348
ECMP 351
有关虚拟路由器的更多运行时统计数据 353
有关逻辑路由器的更多运行时统计数据 362
Network（网络）> Routing（路由）> Logical Routers（逻辑路由器） 366
逻辑路由器的常规设置 366
逻辑路由器的静态路由 368
逻辑路由器的 BGP 路由 370
Network（网络）> Routing（路由）> Routing Profiles（路由配置文件）> BGP 372
Network（网络）> IPSec Tunnels（IPSec 隧道） 375
IPSec VPN 隧道管理 375
IPSec 隧道常规选项卡 375
IPSec 隧道代理 ID 选项卡 377
防火墙中的 IPSec 隧道状态 378
IPSec 隧道重新启动或刷新 378
Network（网络）> GRE Tunnels（GRE 隧道） 379
GRE 隧道 379
Network（网络）> DHCP 381
DHCP 概述 381
DHCP 寻址 381
DHCP 服务器 382
DHCP 中继 384

Dhcp 客户端 385
Network（网络）> DNS Proxy（DNS 代理）..... 386
DNS 代理概述 386
DNS 代理设置 386
其他 DNS 代理操作 388
Network（网络）> QoS 390
QoS 接口设置 390
QoS 接口统计信息 391
Network（网络）> LLDP 393
LLDP 概述 393
LLDP 的构建块 393
Network（网络）> Network Profiles（网络配置文件）..... 396
Network（网络）> Network Profiles（网络配置文件）> GlobalProtect IPSec Crypto（GlobalProtect IPSec 加密）..... 396
Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）..... 396
Network（网络）> Network Profiles（网络配置文件）> IPSec Crypto（IPSec 加密）..... 402
Network（网络）> Network Profiles（网络配置文件）> IKE Crypto（IKE 加密）..... 403
Network（网络）> Network Profiles（网络配置文件）> Monitor（监控）..... 404
Network（网络）> Network Profiles（网络配置文件）> Interface Mgmt（接口管理）..... 405
Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）..... 406
Network（网络）> Network Profiles（网络配置文件）> QoS 420
Network（网络> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件）..... 421
Network（网络> Network Profiles（网络配置文件）> BFD Profile（BFD 配置文件）..... 422
Network（网络）> Network Profiles（网络配置文件）> SD-WAN Interface Profile（SD-WAN 接口配置文件）..... 424

设备 427
Device（设备）> Setup（设置）..... 428
Device（设备）> Setup（设置）> Management（管理）..... 429
Device（设备）> Setup（设置）> Operations（操作）..... 449
启用 SNMP 监控 454
Device（设备）> Setup（设置）> HSM 456
硬件安全模块提供商设置 456
HSM 身份验证 457
硬件安全操作 457
硬件安全模块提供商配置和状态 458
硬件安全模块状态 458
Device（设备）> Setup（设置）> Services（服务）..... 459
配置全局和虚拟系统服务 459
全局服务设置 459
服务路由配置的 IPv4 和 IPv6 支持 461
目标服务路由 464
Device（设备）> Setup（设置）> Interfaces（接口）..... 465
Device（设备）> Setup（设置）> Telemetry（遥测）..... 468
Device（设备）> Setup（设置）> Content-ID 469
Device（设备）> Setup（设置）> WildFire 474

Device（设备）> Setup（设置）> Session（会话）.....477
会话设置.....477
会话超时.....480
TCP 设置.....482
解密设置：证书撤消检查.....484
解密设置：转发代理服务器证书设置.....485
VPN 会话设置.....486
Device（设备）> High Availability（高可用性）.....487
配置 HA 的重要注意事项.....487
HA 常规设置.....488
HA 通信.....491
HA 链路和路径监视.....494
HA 主动/主动配置.....495
集群配置.....497
Device（设备）> Log Forwarding Card（日志转发卡）.....498
Device（设备）> Config Audit（配置审核）.....500
Device（设备）> Password Profiles（密码配置文件）.....501
用户名和密码要求.....501
Device（设备）> Administrators（管理员）.....503
Device（设备）> Admin Roles（管理员角色）.....505
Device（设备）> Access Domain（访问域）.....507
Device（设备）> Authentication Profile（身份验证配置文件）.....508
身份验证配置文件.....508
来自身份验证配置文件的 SAML 元数据导出.....513
Device（设备）> Authentication Sequence（身份验证序列）.....515
Device（设备）> Data Redistribution（数据重新分发）.....516
Device（设备）> Data Redistribution（数据重新分发）> Agents（代理）.....516
Device（设备）> Data Redistribution（数据重新分发）> Clients（客户端）.....517
Device（设备）> Data Redistribution（数据重新分发）> Collector Settings（收集器设置）.....517
Device（设备）> Data Redistribution（数据重新分发）> Include/Exclude Networks（包括/排除网络）.....518
Device（设备）> Device Quarantine（设备隔离）.....519
Device（设备）> VM Information Sources（VM 信息源）.....520
为 VMware ESXi 或 vCenter 服务器启用 VM 信息源设置.....521
为 AWS VPC 启用 VM 信息源设置.....522
为 Google Compute Engine 启用 VM 信息源设置.....523
Device（设备）> Troubleshooting（故障排除）.....525
安全策略匹配.....525
QoS 策略匹配.....526
身份验证策略匹配.....527
解密/SSL 策略匹配.....528
NAT 策略匹配.....529
基于策略的转发策略匹配.....530
DoS 策略匹配.....531
路由.....532
测试 Wildfire.....533
威胁库.....533
Ping.....534
跟踪路由.....535
日志收集器连接性.....536
外部动态列表.....537
更新服务器.....537
测试云日志记录服务状态.....537

测试云 GP 服务状态 538
Device（设备）> Virtual Systems（虚拟系统）539
Device（设备）> Shared Gateways（共享网关）542
Device（设备）> Certificate Management（证书管理）543
Device（设备）> Certificate Management（证书管理）> Certificates（证书）544
管理防火墙和 Panorama 证书 544
管理默认可信证书授权机构 548
Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）549
Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者）551
Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）552
Device（设备）> Certificate Management（证书管理）> SCEP 554
Device（设备）> Certificate Management（证书管理）> SSL Decryption Exclusion（SSL 解密排除）557
Device（设备）> Certificate Management（证书管理）> SSH Service Profile（SSH 服务配置文件）559
Device（设备）> Response Pages（响应页面）561
Device（设备）> Log Settings（日志设置）563
选择日志转发目标 563
定义警报设置 565
清除日志 567
Device（设备）> Server Profiles（服务器配置文件）568
Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱）569
Device（设备）> Server Profiles（服务器配置文件）> Syslog 571
Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）573
Device（设备）> Server Profiles（服务器配置文件）> HTTP 575
Device（设备）> Server Profiles（服务器配置文件）> NetFlow 578
Device（设备）> Server Profiles（服务器配置文件）> RADIUS 579
Device（设备）> Server Profiles（服务器配置文件）> TACACS+ 581
Device（设备）> Server Profiles（服务器配置文件）> LDAP 582
Device（设备）> Server Profiles（服务器配置文件）> Kerberos 584
Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商）585
Device（设备）> Server Profiles（服务器配置文件）> DNS 588
Device（设备）> Server Profiles（服务器配置文件）> Multi Factor Authentication（多因素身份验证）589
Device（设备）> Local User Database（本地用户数据库）> Users（用户）591
Device（设备）> Local User Database（本地用户数据库）> User Groups（用户组）592
Device（设备）> Scheduled Log Export（计划日志导出）593
Device（设备）> Software（软件）595
Device（设备）> Dynamic Updates（动态更新）597
Device（设备）> Licenses（许可证）600
Device（设备）> Support（支持）601
Device（设备）> Master Key and Diagnostics（主密钥和诊断）602
部署主密钥 603
Device（设备）> Policy Recommendation（策略建议）605

用户标识 607
Device（设备）> User Identification（用户标识）> User Mapping（用户映射）608
Palo Alto Networks User-ID 代理设置 608
监控服务器 614

包括或排除用户映射的子网 617
Device（设备）> User Identification（用户标识）> Connection Security（连接安全性）618
Device（设备）> User Identification（用户标识）> Terminal Server Agents（终端服务器代理）619
Device（设备）> User Identification（用户标识）> Group Mapping Settings（组映射设置）选项卡 620
Device（设备）> User Identification（用户标识）> Authentication Portal（身份验证门户）624

GlobalProtect 627
Network（网络）> GlobalProtect > Portals（门户）628
GlobalProtect 门户常规选项卡 629
GlobalProtect 门户身份验证配置选项卡 630
GlobalProtect 门户 Portal Data Collection（门户数据收集）选项卡 632
GlobalProtect 门户代理选项卡 632
GlobalProtect 门户无客户端 VPN 选项卡 649
GlobalProtect 门户卫星选项卡 652
Network（网络）> GlobalProtect > Gateways（网关）655
GlobalProtect 网关常规选项卡 655
GlobalProtect 网关身份验证选项卡 656
GlobalProtect 网关代理选项卡 658
GlobalProtect 网关卫星选项卡 666
Network（网络）> GlobalProtect > MDM 669
Network（网络）> GlobalProtect > Device Block List（设备阻止列表）670
Network（网络）> GlobalProtect > Clientless Apps（无客户端应用）671
Network（网络）> GlobalProtect > Clientless App Groups（无客户端应用组）672
Objects（对象）> GlobalProtect > HIP Objects（HIP 对象）673
HIP 对象常规选项卡 673
HIP 对象移动设备选项卡 675
HIP 对象修补程序管理选项卡 676
HIP 对象防火墙选项卡 676
HIP 对象反恶意软件选项卡 677
HIP 对象磁盘备份选项卡 677
HIP 对象磁盘加密选项卡 677
HIP 对象数据丢失保护选项卡 678
HIP 对象证书选项卡 678
HIP 对象自定义检查选项卡 679
Objects（对象）> GlobalProtect > HIP Profiles（HIP 配置文件）680
Device（设备）> GlobalProtect Client（GlobalProtect 客户端）682
管理 GlobalProtect 应用程序软件 682
设置 GlobalProtect 应用程序 683
使用 GlobalProtect 应用程序 683

Panorama Web 界面 685
使用 Panorama Web 界面 686
上下文切换 690
Panorama 提交操作 691
在 Panorama 上定义策略 698
传统模式下 Panorama 虚拟设备的日志存储分区 700
Panorama > Setup（设置）> Interfaces（接口）701
Panorama > High Availability（高可用性）704

Panorama > Managed WildFire Clusters（受管 Wildfire 集群）.....706
受管 Wildfire 集群任务.....706
受管 Wildfire 设备任务.....707
受管 Wildfire 信息.....708
受管 WildFire 集群和设备管理.....711
Panorama > Administrators（管理员）.....721
Panorama > Admin Roles（管理员角色）.....723
Panorama > Access Domains（访问域）.....725
Panorama > Managed Devices（受管设备）> Summary（摘要）.....726
受管防火墙管理.....726
受管防火墙信息.....727
防火墙软件和内容更新.....730
防火墙备份.....731
Panorama > Device Quarantine（设备隔离）.....731
Panorama > Managed Devices（受管设备）> Health（运行状况）.....732
Panorama 中的详细设备运行状况.....734
Panorama > Templates（模板）.....738
模板.....738
模板堆栈.....738
Panorama > Templates（模板）> Template Variables（模板变量）.....739
Panorama > Device Groups（设备组）.....742
Panorama > Managed Collectors（受管收集器）.....744
日志收集器信息.....744
日志收集器配置.....745
专用日志收集器的软件更新.....752
Panorama > Collector Groups（收集器组）.....754
收集器组配置.....754
收集器组信息.....758
Panorama > Plugins（插件）.....759
Panorama > SD-WAN.....760
SD-WAN 设备.....760
SD-WAN VPN 集群.....761
SD-WAN 监控.....762
SD-WAN 报告.....763
Panorama > VMware NSX.....765
配置通知组.....765
创建服务定义.....766
配置对 NSX Manager 的访问权限.....766
创建控制规则.....768
Panorama > Log Ingestion Profile（日志提取配置文件）.....769
Panorama > Log Settings（日志设置）.....770
Panorama > Server Profiles（服务器配置文件）> SCP.....772
Panorama > Scheduled Config Export（计划配置导出）.....773
Panorama > Software（软件）.....775
管理 Panorama 软件更新.....775
显示 Panorama 软件更新信息.....776
Panorama > Device Deployment（设备部署）.....777
管理软件和内容更新.....777
显示软件和内容更新信息.....779
调度动态内容更新.....779
从 Panorama 恢复内容版本.....780
管理防火墙许可证.....781

Web 界面基础知识

以下主题对防火墙进行了概述并说明了基本管理任务。

> 防火墙概述
> 功能与优点
> 最后登录时间及失败登录尝试
> 每日消息
> 任务管理器
> 语言
> 警报
> 提交更改
> 保存待选配置
> 恢复更改
> 锁定配置
> 全局查找
> 威胁详细信息
> AutoFocus 情报摘要

防火墙概述

Palo Alto Networks® 新一代防火墙可检测所有流量，包括应用程序、威胁和内容，然后将流量与用户绑定，不论其位置或设备类型如何。用户、应用程序、和内容这三项推动您的业务开展的要素构成了企业安全策略中的一个完整部分。这样，您可以将安全性与您的业务策略对齐，并编写易于理解和维护的规则。

作为安全操作平台的一部分，我们的下一代防火墙将为您的组织提供以下功能：

- 对所有流量分类（无论端口如何），从而安全地启用应用程序（包括软件即服务应用程序）、用户和内容。
- 允许所有所需应用程序，阻止其他应用程序，并通过积极的实施模式降低攻击风险。
- 使用安全策略阻止已知漏洞利用、病毒、勒索软件、间谍软件、botnet 和其他未知恶意软件，例如高级持续性威胁。
- 细分数据和应用程序，并实施零信任原则，以保护您的数据中心（包括虚拟化数据中心）。
- 在内部部署和云环境中使用一致的安全性。
- 将安全操作平台可扩展到用户和设备，不受其地理位置的限制，打来安全的移动计算。
- 获得集中可视性，简化网络安全，使您的数据可操作，从而防止成功的网络攻击。
- 停止向非法网站提供有效的公司凭证，并通过在网络层实施身份验证策略抵消攻击者使用被盗凭证进行横向移动或网络危害的能力，从而标识和防止盗用凭证。

© 2019 Palo Alto Networks, Inc.

功能与优点

Palo Alto Networks 下一代防火墙可以对允许访问您网络的通信进行粒度控制。主要功能与优点包括：

- **Application-based policy enforcement (App-ID™)**（基于应用程序的策略实施 **(App-ID™)**）— 根据应用程序类型进行访问控制的有效性将远超只基于协议和端口号的应用程序标识。App-ID 服务可以阻止高风险应用程序以及高风险行为（如文件共享），而使用安全套接字层 (SSL) 协议加密的通信可以接受解密和检查。
- 用户标识 **(User-ID™)** — 管理员可以使用 User-ID 功能根据用户和用户组（而非网络区域和地址或除此之外）来配置和实施防火墙策略。防火墙可与许多目录服务器（例如 Microsoft Active Directory、eDirectory、SunOne、OpenLDAP 以及大多数其他基于 LDAP 的目录服务器）通信以向防火墙提供用户和组信息。然后，您可以使用此信息进行可按用户或组定义的安全应用程序启用。例如，管理员可允许某个组织使用基于 Web 的应用程序，但不允许公司内的所有其他组织使用同一应用程序。您还可以基于用户和组为应用程序的某些组件进行粒度控制配置（请参阅用户标识）。
- **Threat prevention**（威胁防御）— 威胁防御服务可以保护网络免遭病毒、蠕虫、间谍软件以及其他恶意流量的攻击，这些服务因应用程序和通信源的不同而有所差异（请参阅 Objects（对象）> Security Profiles（安全配置文件））。
- **URL filtering**（**URL** 过滤）— 可对出站连接进行过滤，以防访问不当的网站（请参阅 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤））。
- 通讯可视化— 广泛的报告、日志和通知机制可让您详细地看到网络应用程序通信和安全事件。Web 界面中的应用程序命令中心 (ACC) 可识别流量最大和安全风险最高的应用程序（请参阅监控）。
- 网络的多功能性和速度 — Palo Alto Networks 防火墙可以增强或取代现有防火墙，并可以透明地安装在任何网络中或配置为支持交换或路由环境。数千兆的速度配合单通道架构使得这些服务对网络延迟只会产生很小的影响或不会产生影响。
- **GlobalProtect** — 通过允许从全球任意位置方便安全地登录，GlobalProtect™ 软件可确保客户端系统（如在现场使用的便携式计算机）的安全性。
- **Fail-safe operation**（防故障操作）— 高可用性 (HA) 支持会在出现任何硬件或软件崩溃的情况下自动进行故障转移（请参阅 Device（设备）> Virtual Systems（虚拟系统））。
- **Malware analysis and reporting**（恶意软件分析和报告）— WildFire™ 基于云的安全服务会提供有关通过防火墙的恶意软件的详细分析和报告。与 AutoFocus™ 威胁情报服务集成，可让您评估与组织、行业和全球层面的网络流量相关联的风险。
- **VM-Series firewall**（**VM** 系列防火墙）— VM 系列防火墙会提供一个专用于虚拟数据中心环境的 PAN-OS® 虚拟实例，尤其适用于专用、公共和混合云计算环境。
- **Management and Panorama**（管理和 **Panorama**）— 您可以通过直观的 Web 界面或通过命令行界面 (CLI) 来管理各个防火墙，也可以通过 Panorama™ 集中式管理系统集中管理所有防火墙，该系统的 Web 界面与 Palo Alto Networks 防火墙的 Web 界面非常相似。

© 2019 Palo Alto Networks, Inc.

最后登录时间及失败登录尝试

为检测对特权账户（如 Palo Alto Networks 防火墙或 Panorama 上的管理账户）的误用并防止不当利用，Web 界面和命令行界面 (CLI) 将在您登录时，显示您用户名的最后登录时间及所有失败登录尝试。此信息可让您轻松识别是否他人正使用您的管理凭据发起攻击。

您登录 Web 界面后，最后登录时间 信息将显示于此窗口的左下角。如果在最近一次成功登录后出现了一次或多次失败登录，则最后登录信息右侧将出现一个警告图标。将鼠标悬停于警告图标上方即可查看失败登录尝试的次数，或单击此图标即可查看 **Failed Login Attempts Summary**（失败登录尝试汇总）窗口，其中将列出管理帐户名、源 IP 地址，以及登录失败的原因。

如果您发现非本人操作的多次失败登录尝试，您应与网络管理员协作，一同找出进行此蛮力攻击的系统，然后调查用户和主机以识别并根除任何恶意活动。如果您发现最后登录日期和时间表明存在账户窃取情况，您应立即更改密码，然后执行配置审核，确定是否已提交可疑的配置更改。如果您发现日志被清除，或难以确定是否账户被用于进行不当更改，请将配置恢复到已知的正确配置。

© 2019 Palo Alto Networks, Inc.

每日消息

如果您或其他管理员已配置当日消息或 Palo Alto Networks 已将其嵌入为软件或内容版本的一部分，则在用户登录到 Web 界面时将自动显示 Message of the Day（当日消息）对话框。这可确保用户能够看见可能影响要执行任务的重要信息，如即将发生的系统重启。

此对话框每页显示一则消息。如果此对话框中包含 **Do not show again**（不再显示）这一待选项，您可针对在后续登录后不希望对话框显示的消息，选中此选项。

一旦 *Message of the Day*（当日消息）发生更改，即使您在之前登录时已选中 *Do not show again*（不再显示），此消息仍会在下一次会话中出现。因此，您必须重新选择此选项，以免在后续会话中再次看到已修改的消息。

如需导航对话框页面，请单击对话框两侧向右（ ）和向左（ ）的箭头，或单击对话框底部周围的页面选择器（ ）。选择 **Close**（关闭）对话框后，您可通过单击 Web 界面底部的消息（ ），以手动方式重新打开此对话框。

要配置当日消息，请选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑横幅和消息设置。

© 2019 Palo Alto Networks, Inc.

任务管理器

单击 Web 界面底部的 **Tasks**（任务）以显示自上次防火墙重启之后，您、管理员或 PAN-OS 发起的任务（例如手动提交或自动 FQDN 刷新）。对于每个任务，任务管理器提供信息以及下表中描述的操作。

一些列默认是隐藏的。要显示或隐藏特定列，可打开任何列标头中的下拉列表，选择 *Columns*（列）并选择（显示）或清除（隐藏）列名称。

字段/按钮	说明
Q→×	要过滤任务，可根据其中一列中的值输入文本字符串并应用过滤器 (→)。例如，输入 **edl** 将过滤列表，以仅显示 EDLFetch（获取外部动态列表）任务。要去除过滤，可删除过滤器 (×)。
类型	任务的类型，诸如日志请求、许可证刷新或提交。如果和任务相关的信息（诸如警告）过长而不适配消息列，则可单击类型值来查看所有详细信息。
状态	指示任务是否为挂起（诸如带 Queued（排队）状态的提交）、进行中（例如带 Active（活动）状态的日志请求）、已完成或失败对于进行中的提交操作，Status（状态）将表明完成百分比。
作业 ID	确定任务的数字。在 CLI 中，您可使用作业 ID 来查看有关任务的更多详细信息。您如，您可通过输入以下内容查看提交队列中提交任务的位置： `> show jobs id <job-id>` 该列默认为隐藏状态。
结束时间	任务完成时的日期和时间。该列默认为隐藏状态。
启动时间	任务开始时的日期和时间。对于提交任务，Start Time（开始时间）指示何时将提交添加至提交队列。
消息	显示有关任务的详细信息。如果条目指示消息过多，则可单击任务类型来查看消息。 对于提交任务，消息包括离开队列时间，以指示 PAN-OS 何时开始执行提交。如需查看管理员输入的提交说明，请单击 **Commit Description**（提交说明）。有关详细信息，请参阅提交更改。.
操作	单击 **x** 以取消由管理员或 PAN-OS 发起的挂起的提交。该按钮仅可供具有以下预定义角色之一的管理员使用：超级用户、设备管理员、虚拟系统管理员或 Panorama 管理员。
显示	选择必须显示的任务： • **All Tasks**（所有任务）（默认） • 特定类型（**Jobs**（作业）、**Reports**（报告）或 **Log Requests**（日志请求））的 **All**（所有）任务

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	• 所有 **Running**（正在运行）任务（进行中） • 特定类型（**Jobs**（作业）、**Reports**（报告）或 **Log Requests**（日志请求））的所有 **Running**（正在运行）任务 • （仅限 Panorama）使用第二下拉列表来显示 **Panorama**（默认）的任务或特定受管防火墙。
清除提交队列	取消所有由管理员或 PAN-OS 发起的挂起的提交。该按钮仅可供具有以下预定义角色之一的管理员使用：超级用户、设备管理员、虚拟系统管理员或 Panorama 管理员。

© 2019 Palo Alto Networks, Inc.

语言

默认情况下，用于登录防火墙的计算机的语言设置可确定管理 Web 界面显示的语言。要手动更改语言，请单击 **Language**（语言）（Web 界面底部），请从下拉列表中选择指定语言，然后单击 **OK**（确定）。刷新后 Web 界面将以所选语言显示。

支持的语言包括：法语、日语、西班牙语、简体中文和繁体中文。

© 2019 Palo Alto Networks, Inc.

警报

警报是防火墙生成的消息，其中将指明超出事件类型所配置阈值的特定类型事件（如加密、解密故障等）发生的次数（请参阅定义警报设置）。生成警报时，防火墙将创建警报日志，并打开系统警报对话框以显示警报。关闭此对话框后，您可随时通过 Web 界面底部的 **Alarms**（警报）（

）将其重新打开。要防止防火墙因特定警报而自动打开此对话框，请选择 Unacknowledged Alarms（未确认警报）并单击 **Acknowledge**（确认）以将警报移动到 Acknowledged Alarms（已确认警报）列表。

© 2019 Palo Alto Networks, Inc.

提交更改

单击 Web 界面右上角的 **Commit**（提交），并为对防火墙配置的暂挂更改指定一个操作：commit（提交（激活））、validate（验证）或 preview（预览）。您可以按管理员或位置过滤暂挂的更改，然后仅预览、验证并提交这些更改。位置可以是特定虚拟系统、共享策略和对象，或共享设备和网络设置。

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

使用任务管理器可取消提交或查看暂挂、进行中、已完成或失败提交的详细信息。

Commit（提交）对话框显示下表中所述的选项。

字段/按钮	说明
提交所有更改	提交您具有管理权限的所有更改（默认）。选择此选项后，您无法手动过滤防火墙提交的配置更改范围。而是分配给您用于登录的帐户的管理员角色确定了提交范围： • **Superuser role**（超级用户角色）— 防火墙提交所有管理员的更改。 • **Custom role**（自定义角色）— 分配给帐户的管理员角色配置文件的权限确定了提交范围（请参阅 Device（设备）> Admin Roles（管理员角色））。如果管理员角色配置文件包括 **Commit For Other Admins**（为其他管理员提交）权限，则防火墙提交由任何和所有管理员配置的更改。如果管理员角色配置文件不包括 **Commit For Other Admins**（为其他管理员提交）权限，则防火墙仅提交您的更改，而不提交其他管理员的更改。 如果您已实施访问域，防火墙自动应用这些域以过滤提交范围（请参阅 Device（设备）> Access Domain（访问域））。无论您的管理角色怎样，防火墙仅提交分配给帐户的访问域中的配置更改。
提交更改者	过滤防火墙提交的配置更改范围。分配给您用于登录的帐户的管理角色确定了过滤选项： • **Superuser role**（超级用户角色）— 您可以将提交范围限制为特定管理员所作的更改以及在特定位置所作的更改。 • **Custom role**（自定义角色）— 分配给帐户的管理员角色配置文件的权限确定了过滤选项（请参阅 Device（设备）> Admin Roles（管理员角色））。如果管理员角色配置文件包括 **Commit For Other Admins**（为其他管理员提交）权限，则您可以将提交范围限制为特定管理员配置的更改以及在特定位置所作的更改。如果管理员角色配置文件不包括 **Commit For Other Admins**（为其他管理员提交）权限，则您只能将提交范围限制为在特定位置所作的更改。 过滤提交范围如下： • **Filter by administrator**（按管理员过滤）— 即使您的角色允许提交其他管理员的更改，默认情况下提交范围仅包括您的更改。要将其他管理员添加到提交范围，请单击 **<usernames>** 链接，选择管理员，然后单击 **OK**（确定）。 • **Filter by location**（按位置过滤）— 选择要包括在提交中的更改的特定位置。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	如果您已实施访问域，防火墙根据这些域自动过滤提交范围（请参阅 Device（设备）> Access Domain（访问域））。无论您的管理角色和过滤选择怎样，提交范围仅包括分配给帐户的访问域中的配置更改。 加载配置后（Device（设备）> Setup（设置）> Operations（操作）），必须 *Commit All Changes*（提交所有更改）。 在将更改提交到虚拟系统时，必须包括对该虚拟系统中的同一规则库加载、删除或重定位规则的所有管理员的更改。
提交范围	列出拥有要提交的更改的位置。列表是否包括所有更改或部分更改取决于多个因素，如提交所有更改和提交更改者所述。这些位置可以是以下任何之一： • **shared-object**（共享对象）— 在共享位置中定义的设置。 • **policy-and-objects**（策略和对象）— 在没有多个虚拟系统的防火墙上定义的策略规则或对象。 • **device-and-network**（设备和网络）— 全局网络和设备设置（如接口管理配置文件），而不属于虚拟系统。这也适用于没有多个虚拟系统的防火墙上的网络和设备设置。 • **<virtual-system>** — 在拥有多个虚拟系统的防火墙上定义的策略规则或对象中虚拟系统的名称。这也包括属于虚拟系统（如区域）的网络和设备设置。
位置类型	此列用于对暂挂更改的位置进行分类： • **Virtual Systems**（虚拟系统）— 在特定虚拟系统中定义的设置。 • **Other Changes**（其他更改）— 不属于虚拟系统（如共享对象）的设置。
包括中提交中 （仅限部分提交）	能让您选择要提交的更改。默认情况下，选择 **Commit Scope**（提交范围）内的所有更改。此列仅在您选择 **Commit Changes Made By**（提交更改者）特定管理员后才会显示。 可能存在影响包括在提交中的更改的依赖关系。例如，如果您添加一个对象且其他管理员然后编辑该对象，则您无法提交其他管理员的更改，也不会提交自己的更改。
按位置类型分组	按 **Location Type**（位置类型）对 **Commit Scope**（提交范围）中的配置更改列表进行分组。
预览变更	能让您将在 **Commit Scope**（提交范围）中选择的配置与正在运行的配置进行比较。预览窗口使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。 为了帮助您将更改与 Web 界面的各部分进行匹配，您可以配置预览窗口以显示每次更改之前和之后的 **Lines of Context**（上下文行）。这些行是您进行比较的待选配置和正在运行配置的文件中的行。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	由于预览结果会在新浏览器窗口中显示，所以您的浏览器必须设置允许窗口弹出。如果预览窗口未打开，请参阅浏览器文档，了解允许窗口弹出的相关步骤。
更改摘要	列出您用于提交更改的各个设置。**Change Summary**（更改摘要）列表显示各个设置的以下信息： • **Object Name**（对象名称）— 用于标识策略、对象、网络设置或设备设置的名称。 • **Type**（类型）— 设置的类型（如地址、安全规则或区域）。 • **Location Type**（位置类型）— 指示设置是否在 **Virtual Systems**（虚拟系统）中定义。 • **Location**（位置）— 定义设置的虚拟系统的名称。该列显示 **Shared**（共享）不属于虚拟系统的设置。 • **Operations**（操作）— 指示自上次提交以来对设置执行的每个操作（创建、编辑或删除）。 • **Owner**（所有者）— 对设置进行最后更改的管理员。 • **Will Be Committed**（将提交）— 指示提交当前是否包括设置。 • **Previous Owners**（以前的所有者）— 在最后更改之前对设置进行更改的管理员。 （可选）可以选择 **Group By**（分组方式）列名称进行分组（如 **Type**（类型））。 在更改列表中选择一个对象以查看 **Object Level Difference**（对象级别差异）。
验证提交	验证防火墙配置是否具有正确的语法且语义完整。输出包括与提交显示相同的错误和警告，其中包括规则阴影和应用程序相关性警告。验证过程能让您在提交之前查找和修复错误（不会对正在运行的配置进行任何更改）。如果您拥有固定提交窗口，并且希望确保提交将成功而没有出现错误，这将非常有用。
说明	可让您输入说明（最多 512 个字符），帮助其他管理员了解您所作的更改。 提交事件的系统日志将截断长度超过 *512* 个字符的说明。
提交	启动提交，或者如果其他提交处于暂挂状态时，将您的提交添加到提交队列。
提交状态	在提交期间提供进度，然后在提交之后提供结果。提交结果包括成功或失败、提交更改的详细信息和提交警告。警告包括： • **Commit**（提交）— 列出常规提交警告。 • **App Dependency**（应用程序相关性）— 列出现有规则所需的任何应用程序相关性。 • **Rule Shadow**（规则阴影）— 列出任何阴影规则。

© 2019 Palo Alto Networks, Inc.

保存待选配置

选择防火墙或 Panorama Web 界面右上角的 **Config**（配置）> **Save Changes**（保存更改），可为待选配置保存新的快照文件，或者可替换现有配置文件。如果防火墙或 Panorama 在您提交更改前重启，您之后可将待选配置恢复为保存的快照，以便还原您在最近一次提交后所作的更改。要恢复为快照，请选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作）和 **Load named configuration snapshot**（加载已命名的配置快照）。如果您在重启后未恢复为此快照，则待选配置将和上次提交的配置（正在运行的配置）相同。

您可以根据管理员或位置过滤要保存的配置更改。位置可以是特定虚拟系统、共享策略和对象，或共享设备和网络设置。

您应该定期保存您的更改，以免在防火墙或 *Panorama* 重启时丢失这些数据。

保存您的待选配置更改，不能激活这些更改；必须提交更改才能激活这些更改。

Save Changes（保存更改）对话框将显示下表所介绍的选项：

字段/按钮	说明
保存所有更改	保存您有管理权限管理的所有更改（默认值）。在选中此选项后，不能手动过滤防火墙保存的配置更改的范围。而为登录所使用的帐户分配的管理员角色可确定保存范围： • 超级用户角色 — 防火墙可保存所有管理员的更改。 • 自定义角色 — 为您的帐户分配的管理员角色配置文件的权限可确定保存范围（请参阅 Device（设备）> Admin Roles（管理员角色））。如果配置文件包含 **Save For Other Admins**（为其他管理员保存）这一权限，则防火墙可保存所有管理员配置的更改。如果管理员角色配置文件不包含 **Save For Other Admins**（为其他管理员保存）这一权限，则防火墙只能保存您的更改，不能保存其他管理员的更改。 如果您已应用访问域，防火墙会自动应用这些域过滤保存范围（请参阅 Device（设备）> Access Domain（访问域））。不管是何管理角色，防火墙都仅保持为您的帐户分配的访问域中的配置更改。
所作更改保存依据	过滤防火墙保存的配置更改的范围。分配给您用于登录的帐户的管理角色确定了过滤选项： • 超级用户角色 — 您可以将保存范围限制为特定管理员所作的更改和特定位置中的更改。 • **Custom role**（自定义角色）— 分配给帐户的管理员角色配置文件的权限确定了过滤选项（请参阅 Device（设备）> Admin Roles（管理员角色））。如果配置文件包含 **Save For Other Admins**（为其他管理员保存）这一权限，则可将保存范围限制为特定管理员配置的更改和特定位置中的更改。如果管理员角色配置文件不包含 **Save For Other Admins**（为其他管理员保存）这一权限，则可将保存范围仅限制为您在特定位置中所作的更改。 按以下说明过滤保存范围：

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	• 按管理员过滤 — 默认情况下，即使您的角色允许保存其他管理员的更改，保存范围也仅包含您的更改。要将其他管理员添加到保存范围，请单击 **<usernames>** 链接，选择管理员，然后单击 **OK**（确定）。 • 按位置过滤 — 选择要加入保存的特定位置的更改。 如果您已应用访问域，防火墙会根据这些域自动过滤保存范围（请参阅 Device（设备）> Access Domain（访问域））。不管是何管理角色和过滤选择，保存范围都仅包含为您的帐户分配的访问域中的配置更改。
保存范围	列出要保存更改的位置。列表中是包含所有更改还是更改的子集，取决于多种因素，如保存所有更改和所作更改保存依据选项所述。这些位置可以是以下任何之一： • **shared-object**（共享对象）— 在共享位置中定义的设置。 • **policy-and-objects**（策略和对象）—（仅限防火墙）在没有多个虚拟系统的防火墙上定义的策略规则或对象。 • **device-and-network**（设备和网络）—（仅限防火墙）不是特定于虚拟系统的全局网络和设备设置（如接口管理配置文件）。 • **<virtual-system>** —（仅限防火墙）在包含多个虚拟系统的防火墙上定义策略规则或对象的虚拟系统的名称。这也包括属于虚拟系统（如区域）的网络和设备设置。 • **<device-group>** —（仅限 Panorama）定义策略规则或对象的设备组的名称。 • **<template>** —（仅限 Panorama）定义设置的模板或模板堆栈的名称。 • **<log-collector-group>** —（仅限 Panorama）定义设置的收集器组的名称。 • **<log-collector>** —（仅限 Panorama）定义设置的日志收集器的名称。
位置类型	此列可对所作更改的位置分类： • **Virtual Systems**（虚拟系统）—（仅限防火墙）在特定虚拟系统中定义的设置。 • **Device Groups**（设备组）—（仅限 Panorama）在特定设备组中定义的设置。 • **Templates**（模板）—（仅限 Panorama）在特定模板或模板堆栈中定义的设置。 • **Collector Groups**（收集器组）—（仅限 Panorama）特定于收集器组配置的设置。
加入保存 （仅限部分保存）	可让您选择要保存的更改。默认情况下，选择 **Save Scope**（保存范围）内的所有更改。仅在为 **Save Changes Made By**（所作更改保存依据）选择特定管理员后，才显示此列。 对于您加入保存的更改，可能存在着依赖项。例如，如果您添加了特定对象，之后其他管理员编辑了此对象，那么您如果不同时保存自己的更改，就不能保存其他管理员的更改。
按位置类型分组	按 **Location Type**（位置类型）对 **Save Scope**（保存范围）中的配置更改列表分组。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
预览变更	可让您比较在 **Save Scope**（保存范围）中选择的配置和正在运行的配置。预览窗口使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。 为了帮助您将更改与 Web 界面的各部分进行匹配，您可以配置预览窗口以显示每次更改之前和之后的 **Lines of Context**（上下文行）。这些行是您进行比较的待选配置和正在运行配置的文件中的行。 由于预览结果会在新窗口中显示，所以您的浏览器必须设置为允许弹出窗口。如果预览窗口未打开，请参阅浏览器文档，了解允许弹出窗口的相关步骤。
更改摘要	列出要保存更改的单独设置。**Change Summary**（更改摘要）列表显示各个设置的以下信息： • **Object Name**（对象名称）— 用于标识策略、对象、网络设置或设备设置的名称。 • **Type**（类型）— 设置的类型（如地址、安全规则或区域）。 • **Location Type**（位置类型）— 指示设置是否在 **Virtual Systems**（虚拟系统）中定义。 • **Location**（位置）— 定义设置的虚拟系统的名称。该列显示 **Shared**（共享）不属于虚拟系统的设置。 • **Operations**（操作）— 指示自上次提交以来对设置执行的每个操作（创建、编辑或删除）。 • **Owner**（所有者）— 对设置进行最后更改的管理员。 • **Will Be Saved**（即将保存）— 指示保存操作项是否会包含此设置。 • **Previous Owners**（以前的所有者）— 在最后更改之前对设置进行更改的管理员。 （可选）可以选择 **Group By**（分组方式）列名称进行分组（如 **Type**（类型））。
保存	将所选更改保存到配置快照文件： • 如果选择 **Save All Changes**（保存所有更改），防火墙会替换默认配置快照文件 (.snapshot.xml)。 • 如果选择 **Save Changes Made By**（所作更改保存依据），则指定新配置文件或现有配置文件的 **Name**（名称），然后单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

恢复更改

选择防火墙或 Panorama Web 界面右上角的 **Config**（配置）> **Revert Changes**（恢复更改），可撤消自上次提交后对待选配置所作的更改。恢复更改可将设置还原为正在运行的配置的值。您可以根据管理员或位置过滤要恢复的配置更改。位置可以是特定虚拟系统、共享策略和对象，或共享设备和网络设置。

在防火墙或 Panorama 处理完暂挂或进行中的所有提交之前，不能恢复更改。在启动恢复进程后，防火墙或 Panorama 会自动锁定待选配置和正在运行的配置，以使其他管理员无法编辑设置或提交更改。在完成恢复进程后，防火墙或 Panorama 会自动解除锁定。

Revert Changes（恢复更改）对话框将显示下表所介绍的选项：

字段/按钮	说明
恢复所有更改	恢复您有管理权限管理的所有更改（默认值）。在选中此选项后，不能手动过滤防火墙恢复的配置更改的范围。而为登录所使用的帐户分配的管理员角色可确定恢复范围： • 超级用户角色 — 防火墙可恢复所有管理员的更改。 • 自定义角色 — 为您的帐户分配的管理员角色配置文件的权限可确定恢复范围（请参阅 Device（设备）> Admin Roles（管理员角色））。如果配置文件包含 **Commit For Other Admins**（为其他管理员提交）这一权限，则防火墙可恢复所有管理员配置的更改。如果管理员角色配置文件不包含 **Commit For Other Admins**（为其他管理员提交）这一权限，则防火墙只能恢复您的更改，不能恢复其他管理员的更改。 在管理员角色配置文件中，提交的相关权限也适用于恢复。 如果您已应用访问域，防火墙会自动应用这些域过滤恢复范围（请参阅 Device（设备）> Access Domain（访问域））。不管是何管理角色，防火墙都仅恢复为您的帐户分配的访问域中的配置更改。
所作更改恢复依据	过滤防火墙所恢复的配置更改的范围。分配给您用于登录的帐户的管理角色确定了过滤选项： • 超级用户角色 — 您可以将恢复范围限制为特定管理员所作的更改和特定位置中的更改。 • **Custom role**（自定义角色）— 分配给帐户的管理员角色配置文件的权限确定了过滤选项（请参阅 Device（设备）> Admin Roles（管理员角色））。如果配置文件包含 **Commit For Other Admins**（为其他管理员提交）这一权限，则可将恢复范围限制为特定管理员配置的更改和特定位置中的更改。如果管理员角色配置文件不包含 **Commit For Other Admins**（为其他管理员提交）这一权限，则可将恢复范围仅限制为您在特定位置中所作的更改。 按以下说明过滤恢复范围： • 按管理员过滤 — 默认情况下，即使您的角色允许恢复其他管理员的更改，恢复范围也仅包含您的更改。要将其他管理员添加到提交范围，请单击 **<usernames>** 链接，选择管理员，然后单击 **OK**（确定）。 • 按位置过滤 — 选择要加入恢复的特定位置的更改。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	如果您已应用访问域，防火墙会根据这些域自动过滤恢复范围（请参阅 Device（设备）> Access Domain（访问域））。不管是何管理角色和过滤选择，恢复范围都仅包含为您的帐户分配的访问域中的配置更改。
恢复范围	列出要恢复更改的位置。列表中是包含所有更改还是更改的子集，取决于多种因素，如恢复所有更改和所作更改恢复依据选项所述。这些位置可以是以下任何之一： • **shared-object**（共享对象）— 在共享位置中定义的设置。 • **policy-and-objects**（策略和对象）—（仅限防火墙）在没有多个虚拟系统的防火墙上定义的策略规则或对象。 • **device-and-network**（设备和网络）—（仅限防火墙）不是特定于虚拟系统的全局网络和设备设置（如接口管理配置文件）。 • **<virtual-system>** —（仅限防火墙）在包含多个虚拟系统的防火墙上定义策略规则或对象的虚拟系统的名称。这也包括属于虚拟系统（如区域）的网络和设备设置。 • **<device-group>** —（仅限 Panorama）定义策略规则或对象的设备组的名称。 • **<template>** —（仅限 Panorama）定义设置的模板或模板堆栈的名称。 • **<log-collector-group>** —（仅限 Panorama）定义设置的收集器组的名称。 • **<log-collector>** —（仅限 Panorama）定义设置的日志收集器的名称。
位置类型	此列可对所作更改的位置分类： • **Virtual Systems**（虚拟系统）—（仅限防火墙）在特定虚拟系统中定义的设置。 • **Device Group**（设备组）—（仅限 Panorama）在特定设备组中定义的设置。 • **Template**（模板）—（仅限 Panorama）在特定模板或模板堆栈中定义的设置。 • **Log Collector Group**（日志收集器组）—（仅限 Panorama）特定于收集器组配置的设置。 • **Log Collector**（日志收集器）—（仅限 Panorama）特定于日志收集器配置的设置。 • **Other Changes**（其他更改）— 不是特定于上述任何配置区域（如共享对象）的设置。
加入恢复 （仅限部分恢复）	可让您选择要恢复的更改。默认情况下，选择 **Revert Scope**（恢复范围）内的所有更改。仅在为 **Revert Changes Made By**（所作更改恢复依据）选择特定管理员后，才显示此列。 对于您加入恢复的更改，可能存在着依赖项。例如，如果您添加了特定对象，之后其他管理员编辑了此对象，那么您如果不同时恢复其他管理员的更改，就不能恢复自己的更改。
按位置类型分组	按 **Location Type**（位置类型）列出 **Revert Scope**（恢复范围）中的配置更改。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
预览变更	可让您比较在 **Revert Scope**（恢复范围）中选择的配置和正在运行的配置。预览窗口使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。 为了帮助您将更改与 Web 界面的各部分进行匹配，您可以配置预览窗口以显示每次更改之前和之后的 **Lines of Context**（上下文行）。这些行是您进行比较的待选配置和正在运行配置的文件中的行。 由于预览结果会在新窗口中显示，所以您的浏览器必须设置为允许弹出窗口。如果预览窗口未打开，请参阅浏览器文档，了解允许弹出窗口的相关步骤。
更改摘要	列出要恢复更改的单独设置。**Change Summary**（更改摘要）列表显示各个设置的以下信息： • **Object Name**（对象名称）— 用于标识策略、对象、网络设置或设备设置的名称。 • **Type**（类型）— 设置的类型（如地址、安全规则或区域）。 • **Location Type**（位置类型）— 指示设置是否在 **Virtual Systems**（虚拟系统）中定义。 • **Location**（位置）— 定义设置的虚拟系统的名称。该列显示 **Shared**（共享）不属于虚拟系统的设置。 • **Operations**（操作）— 指示自上次提交以来对设置执行的每个操作（创建、编辑或删除）。 • **Owner**（所有者）— 对设置进行最后更改的管理员。 • **Will Be Reverted**（即将恢复）— 指示恢复操作项是否会包含此设置。 • **Previous Owners**（以前的所有者）— 在最后更改之前对设置进行更改的管理员。 （可选）可以选择 **Group By**（分组方式）列名称进行分组（如 **Type**（类型））。
恢复	恢复所选更改。

© 2019 Palo Alto Networks, Inc.

锁定配置

为了帮助您在并发登录会话期间与其他防火墙管理员协调配置任务，Web 界面能让您应用配置或提交锁定，以便其他管理员无法更改配置或提交更改，直到删除锁定。

在 Web 界面的右上角，锁定的挂锁 ( ) 表示已设置一项或多项锁定（用括号中锁的数目来表示）；未锁定的挂锁 ( ) 表示未设置任何锁定。单击任一挂锁打开 Locks（锁）对话框，其中将提供以下选项和字段。

要配置防火墙在管理员更改待选配置后自动设置提交锁定，请选择 *Device*（设备）> *Setup*（设置）> *Management*（管理），编辑 *General Settings*（常规设置），启用 *Automatically Acquire Commit Lock*（自动获取提交锁定），然后单击 *OK*（确定），再单击 *Commit*（提交）。

恢复更改（*Config*（配置）> *Revert Changes*（恢复更改））时，防火墙自动锁定正在运行的待选配置，以使其他管理员无法编辑设置或提交更改。完成恢复过程后，防火墙自动删除锁定。

字段/按钮	说明
admin	设置锁定的管理员的用户名。
位置	在配备有一个以上虚拟系统 (vsys) 的防火墙上，锁定范围可以是特定虚拟系统或共享位置。
类型	锁定类型可以是： • **Config Lock**（配置锁定）— 阻止其他管理员对待选配置进行更改。只有超级用户或设置锁定的管理员可将其删除。 • **Commit Lock**（提交锁定）— 阻止其他管理员提交对待选配置进行的更改。在所有锁定释放之前，提交队列不会接受任何新提交。此种类型的锁定可防止多个管理员在并发登录会话期间进行更改时发生冲突，也可防止在其他管理员完成操作前，某个管理员先完成并发起提交时发生冲突。完成管理员为之设置锁定的提交后，防火墙可自动删除此锁定。超级用户或设置锁定的管理员也可手动将其删除。
注释	输入最多 256 个字符的文本。此文本可为其他想要了解锁定原因的管理员提供有用的参考信息。
创建时间	管理员设置锁定的日期和时间。
登录	表示设置锁定的管理员当前是否处于登录状态。
执行锁定	如需设置锁定，**Take a Lock**（执行锁定），请选择 **Type**（类型），选择 **Location**（位置）（仅限多虚拟系统型防火墙），输入可选的 **Comments**（注释），单击 **OK**（确定），然后单击 **Close**（关闭）。
删除锁	要释放锁定，请选中锁定，再选择 **Remove Lock**（删除锁定），单击 **OK**（确定），然后单击 **Close**（关闭）。

© 2019 Palo Alto Networks, Inc.

全局查找

全局查找可让您在防火墙或 Panorama 上搜索特定字符串的待选配置，如 IP 地址、对象名称、策略名称、威胁 ID、规则 UUID 或应用程序名称。搜索结果已按类别进行分组，并在 Web 界面上提供指向配置位置的链接，这样您可以轻松找到字符串存在或被引用的所有位置。

要启动全局查找，单击位于 Web 界面右上角的 **Search**（搜索）图标 。全局查找适用于所有 Web 界面页面和位置。以下是全局查找功能的列表，可以帮助您成功执行搜索：

- 如果您在已启用多个虚拟系统的防火墙上开始搜索或如果已定义管理角色，则全局查找将只返回您拥有访问权限的防火墙区域的结果。全局查找同样适用于 Panorama 设备组；您将只能看到您具有管理访问权限的设备组的搜索结果。
- 搜索文本中的空格作为 AND 操作进行处理。例如，如果您搜索 `corp policy`，则 **corp** 和 **policy** 必须同时存在于搜索结果包含的配置项目中。
- 要查找一个精确短语，必须用引号将该短语引起来。
- 要重新运行以前的搜索，单击 Global Find（全局查找），随即会显示最后 20 个搜索的列表。单击列表中的任何项目可重新运行该搜索。搜索历史记录列表对于每个管理帐户都是唯一。

全局查找适用于可搜索的每个字段。例如，在安全策略的情况下，您可以针对下列字段进行搜索：名称、标记、区域、地址、用户、HIP 配置文件、应用程序、UUID 和服务。要执行搜索，需单击任意这些字段旁边的下拉列表，然后单击 **Global Find**（全局查找）。例如，如果单击名为 l3-vlan-trust 的区域上的 **Global Find**（全局查找），则全局搜索会搜索该区域名称的整个配置，并将返回引用区域的每个位置的结果。搜索结果已按类别进行分组，您可以将鼠标悬停在任意项目上方以查看详细信息，或者您可以单击项目以导航至该项目的配置页面。

全局查找不会搜索防火墙分配给用户的动态内容（如日志、地址范围或单个 DHCP 地址）。在 DHCP 的情况下，您可以针对 DHCP 服务器属性（如 DNS 条目）进行搜索，但不能搜索分配给用户的单个地址。又例如，启用 User-ID™ 功能后，防火墙收集的用户名。在这种情况下，如果配置中存在名称或组（如在策略中定义用户组时），则只能搜索 User-ID 数据库中存在的用户名或用户组。通常，只能搜索防火墙写入配置的内容。

了解更多？

了解有关使用全局查找搜索防火墙或 Panorama 配置的更多信息。

© 2019 Palo Alto Networks, Inc.

威胁详细信息

- Monitor（监控）> Logs（日志）> Threat（威胁）
- ACC > Threat Activity（威胁活动）
- Objects（对象）> Security Profiles（安全配置文件）> Anti-Spyware/Vulnerability Protection（防间谍软件/漏洞防护）

使用 Threat Details（威胁详细信息）对话框了解有关威胁签名（防火墙通过该签名而配备）以及触发这些签名的事件的更多信息。威胁详细信息针对以下方面提供：

- 记录防火墙检测到的威胁的威胁日志（**Monitor**（监控）> **Logs**（日志）> **Threat**（威胁））
- 在网络中发现的最大威胁（**ACC** > **Threat Activity**（威胁活动））
- 您希望修改或从实施项目中排除的威胁签名（**Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware/Vulnerability Protection**（防间谍软件/漏洞防护））

当您找到需要了解的威胁签名时，悬停在 **Threat Name**（威胁名称）或威胁 **ID** 上方，并单击 **Exception**（异常）来查看威胁详细信息。威胁详细信息可让您方便地检查是否根据您的安全策略将威胁签名配置为异常，并确定有关特定威胁的最新威胁库信息。Palo Alto Networks 威胁库数据库与防火墙集成，可让您在防火墙的上下文中查看有关威胁签名的更多详细信息，或者在新的浏览器窗口中为记录的威胁启动威胁库搜索。

根据您正在查看的威胁的类型，详细信息包括在下表中描述的威胁详细信息的全部或部分。

威胁详细信息	说明
名称	威胁签名名称。
ID	独有威胁签名 ID。选择 **View in Threat Vault**（在威胁库中查看）以在新的浏览器窗口中打开威胁库搜索，并查找 Palo Alto Networks 威胁数据库具有的针对该签名的最新信息。这对威胁签名的威胁库条目可包括额外的详细信息，包括首次和最新内容发布，以包括签名的更新和支持签名所需的最低 PAN-OS 版本。
说明	有关触发签名的威胁的信息。
严重性级别	威胁严重性级别：信息、低、中、高或严重。
CVE	与威胁相关的公开的安全漏洞。常见漏洞和暴露 (CVE) 标识符是查找有关独有漏洞的信息的最有用标识符，因为供应商特定的 ID 通常涵盖多个漏洞。
Bugtraq ID	与威胁相关的 Bugtraq ID。
供应商 ID	针对安全漏洞的供应商特定标识符。例如，MS16-148 是一个或多个 Microsoft 漏洞的供应商 ID，而 APBSB16-39 是一个或多个 Adobe 漏洞的供应商 ID。
引用	研究您可用于了解有关威胁的更多信息的源。
免除配置文件	为威胁签名定义不同实施操作而非默认签名操作的安全配置文件。威胁异常仅在免除配置文件附加至安全策略规则时活动（检查异常是否用在当前安全规则中）。
在当前安全规则中使用	活动的威胁异常 - 该列中的复选标记指示防火墙主动实施威胁异常（定义威胁异常的免除配置文件附加至安全策略规则）。 如果清除了该列，则防火墙仅根据建议的默认签名操作实施威胁。

© 2019 Palo Alto Networks, Inc.

威胁详细信息	说明
免除 IP 地址	免除 IP 地址 - 您可添加 IP 地址，在其上过滤威胁异常或查看现有 **Exempt IP Addresses**（免除 **IP** 地址）。该选项仅在相关会话具有匹配免除 IP 地址的源或目标 IP 地址时实施威胁异常。对于其他所有会话，根据默认签名操作实施威胁。

如果您在查看威胁详细信息方面存在问题，请检查是否满足以下条件：

- 防火墙威胁预防许可证有效（*Device*（设备）> *Licenses*（许可证））。
- 已安装最新的防病毒和威胁以及应用程序内容更新。
- 启用了威胁库访问权限（选择 *Device*（设备）> *Setup*（设置）> *Management*（管理）并编辑 *Logging and Reporting*（日志记录和报告）设置为 *Enable Threat Vault Access*（启用威胁库访问权限））。
- 已将默认（或自定义）防病毒软件、防间谍软件和漏洞防护安全配置文件应用至您的安全策略。

© 2019 Palo Alto Networks, Inc.

AutoFocus 情报摘要

您可以查看 AutoFocus 编译的威胁情报的图形概述，以帮助您评估以下防火墙构件的普遍性和风险：

- IP 地址
- 网址
- 域
- 用户代理（数据过滤日志的“用户代理”列）
- 威胁名称（仅对于子类型病毒和 WildFire 病毒的威胁）
- 文件名
- SHA-256 哈希（WildFire 提交日志的“文件摘要”列）

要查看 AutoFocus Intelligence Summary（AutoFocus 情报摘要）窗口，必须首先拥有一个有效的 AutoFocus 订阅，并启用 AutoFocus 威胁情报（选择**Device**（设备）> **Setup**（设置）> **Management**（管理）并编辑 AutoFocus 设置）。

启用 AutoFocus 情报后，将鼠标悬停在构件的日志或外部动态列表以打开下拉列表 (⌄)，然后单击 **AutoFocus**：

- 查看流量、威胁、URL 筛选、WildFire 提交、数据筛选和统一日志（**Monitor**（监控）> **Logs**（日志））。
- 查看外部动态列表条目。

您还可以从防火墙启动 AutoFocus 搜索，进一步调查您发现的有趣或可疑构件。

字段/按钮	说明
AutoFocus 搜索...	单击以启动 AutoFocus 搜索构件。
分析信息选项卡	
会话	WildFire 在其中检测到构件的专用会话数。专用会话是仅在与支持账户相关的防火墙上运行的会话。将鼠标悬停在会话栏上方以查看每月的会话数。
样本	与构件相关联并按 WildFire 判定（良性、灰色软件、恶意软件、钓鱼）分组的组织和全局样本（文件和电子邮件链接）。全局是指所有 WildFire 提交的样本，而组织仅指贵组织提交到 WildFire 的样本。 单击 WildFire 判定以启动 AutoFocus 搜索按范围（组织或全局）和 WildFire 判定过滤的构件。
匹配标记	与构件相匹配的 AutoFocus 标记： • **Private Tags**（私有标记）— 只有与支持帐户相关联的 AutoFocus 用户才能看到。 • **Public Tags**（公共标记）— 所有 AutoFocus 用户都可以看到。 • **Unit 42 Tags**（**Unit 42** 标记）— 标识构成直接安全风险的威胁和活动。这些标记都是由 Unit 42（Palo Alto Networks 威胁情报研究团队）所创建。 • **Informational Tags**（信息标记）— 标识商品威胁的 Unit 42 标记。 将鼠标悬停在标记上方以查看标记说明和其他标记详细信息。 单击标记以启动 AutoFocus 搜索该标记。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	要查看构件的更多匹配标记，单击省略号 (...) 以启动 AutoFocus 搜索该构件。AutoFocus 搜索结果中的“标记”列会显示构件的多个匹配标记。
被动 DNS 选项卡 Passive DNS（被动 DNS）选项卡显示与构件相关联的被动 DNS 历史记录。如果构件是 IP 地址、域或 URL，则此选项卡仅显示匹配的信息。	
请求	提交 DNS 请求的域。单击域以启动 AutoFocus 搜索该域。
类型	DNS 请求类型（示例：A、NS、CNAME）。
响应	DNS 请求解析的 IP 地址或域。单击 IP 地址或域以启动 AutoFocus 进行搜索。 *Response*（响应）列不显示私有 *IP* 地址。
计数	执行请求的次数。
首次查看	根据被动 DNS 历史记录首次查看请求、响应和类型组合的日期和时间。
上次查看	根据被动 DNS 历史记录最近查看请求、响应和类型组合的日期和时间。
匹配哈希选项卡 Matching Hashes（匹配哈希）选项卡显示 WildFire 检测到构件的五个最新的专用样本。专用样本是仅在与支持帐户相关联的防火墙上检测到的样本。	
SHA256	样本的 SHA-256 哈希。单击哈希以启动 AutoFocus 搜索该哈希。
文件类型	样本的文件类型。
创建日期	WildFire 分析样本并为其分配 WildFire 判定的日期和时间。
更新日期	WildFire 更新样本的 WildFire 判定的日期和时间。
结论	样本的 WildFire 判定：良性、灰色软件、恶意软件或钓鱼。

© 2019 Palo Alto Networks, Inc.

配置表格导出

管理用户可以 PDF 文件或 CSV 文件的形式以表格格式导出策略规则库、对象、受管设备和接口上的数据。导出的数据是 Web 界面上显示的数据。对于筛选的数据，仅导出符合筛选要求的数据。如果未应用任何筛选程序，则所有数据均会导出。

所有敏感数据（如密码）均用通配符 (*) 符号隐藏。

系统日志和下载链接在配置表格导出成功时生成。使用下载链接将 PDF 或 CSV 文件保存在本地。关闭包含下载链接的窗口后，该特定导出的下载链接不再可用。

要导出表格数据，请单击 **PDF/CSV** 并配置以下设置：

导出设置	说明
文件名	输入名称（最多 32 个字符）以标识导出的数据。该名称即为导出生成的下载文件的名称。
文件类型	选择要生成的导出输出的类型。您可以选择 PDF 或 CSV 格式。
页面规格	默认页面规格为 Letter（8.5 英寸 x 11.0 英寸）。您无法更改页面规格。默认情况下，纵向生成 PDF 并通过横向更改来适应最大列数。
说明 （仅限 PDF）	输入说明（最多 255 个字符）以提供有关导出的上下文和其他信息。
表格数据	显示将要导出的表格数据。如需清除先前设置的筛选设置，请单击 **Show All Columns**（显示所有列）以显示所选策略类型的所有策略规则。然后，您可以添加或删除列并根据需要应用筛选程序。
显示所有列	删除所有筛选程序并显示所有表格列。

单击 **Export**（导出）以生成配置表格下载链接。

© 2019 Palo Alto Networks, Inc.

仪表盘

仪表盘小部件显示常规防火墙或 Panorama™ 信息，如软件版本、各个接口的状态、资源利用率以及多种日志类型中每一种类型的最多 10 个条目；日志小部件显示最后一小时的条目。

仪表盘小部件主题描述了如何使用仪表盘，并介绍了可用的小部件。

仪表盘小部件

默认情况下，**Dashboard**（仪表盘）以 **3 Columns**（**3** 列）的 **Layout**（布局）显示小部件，但您可以自定义 **Dashboard**（仪表盘）仅显示 **2 Columns**（**2** 列）。

此外，您还可以决定要显示或隐藏的小部件，以便仅看到要监控的小部件。要显示小部件，请从 **Widgets**（小部件）下拉列表中选择小部件类别，然后选择要将其添加到 Dashboard（仪表盘）的小部件（已经显示以渐变灰色文本显示的小部件名称）。通过关闭小部件隐藏（停止显示）小部件（小部件标题中的 ✕ ）。防火墙和 Panorama 保存整个登录期间的小部件显示设置（对于每个管理员都是单独执行）。

请参阅 **Last updated**（上次更新）时间，以确定上一次刷新仪表盘数据的时间。您可以手动刷新整个 **Dashboard**（仪表盘）（仪表盘右上角的 ），也可以刷新各个小部件（各个小部件标题中的 ）。使用仪表盘手动刷新选项 ( ) 旁边的未标记下拉列表选择整个 **Dashboard**（仪表盘）的自动刷新间隔（分钟）：**1 min**（**1** 分钟）、**2 mins**（**2** 分钟）或 **5 mins**（**5** 分钟）；要禁用自动刷新整个 **Dashboard**（仪表盘），请选择 **Manual**（手动）。

仪表盘小部件	说明
应用程序小部件	
热门应用程序	显示会话最多的应用程序。块大小表示会话的相对数量（将鼠标置于块之上可查看数字），颜色表示安全风险 — 从绿色（最低）到红色（最高）。单击应用程序可查看其应用程序配置文件。
热门高风险应用程序	与热门应用程序类似，同时还显示会话最多、风险最高的应用程序。
ACC 风险因素	显示过去一周处理的网络通信平均风险因子 (1-5)。值越高表示风险越大。
系统小部件	
常规信息	显示防火墙或 Panorama 名称和型号、Panorama CPU 和 RAM、Panorama 系统模式、PAN-OS® 或 Panorama 软件版本、IPv4 和 IPv6 的管理 IP 信息、序列号、CPU ID 和 UUID、应用程序、威胁、URL 过滤定义版本、当前日期和时间、以及自上次启动以来的时间长度。
接口 （仅限防火墙）	表示每个接口的状态为开启（绿色）、关闭（红色）还是未知（灰色）。
系统资源	显示管理 CPU 使用率、数据平面使用率以及会话计数（通过防火墙或 Panorama 建立的会话数目）。
高可用性	如果已启用高可用性 (HA)，则指示本地和对端防火墙/Panorama 的 HA 状态 — 绿色（主动）、黄色（被动）或黑色（其他）。有关高可用性的更多信息，请参阅 Device（设备）> Virtual Systems（虚拟系统）或 Panorama > High Availability（高可用性）。
锁	显示管理员设置的配置锁定。
登录管理	显示当前登录的每个管理员的源 IP 地址、会话类型（Web 界面或 CLI）和会话开始时间。

© 2019 Palo Alto Networks, Inc.

仪表盘小部件	说明
日志小部件	
威胁日志	显示威胁日志中最后 10 个条目的威胁 ID、应用程序以及日期和时间。威胁 ID 是违反 URL 过滤配置文件的恶意软件说明或 URL。仅显示最后 60 分钟的条目。
URL 过滤日志	显示 URL 过滤日志中最后 60 分钟的说明以及日期和时间。
数据过滤日志	显示数据过滤日志中最后 60 分钟的说明以及日期和时间。
配置日志	显示配置日志中最后 10 个条目的管理员用户名、客户端（Web 界面或 CLI）以及日期和时间。仅显示最后 60 分钟的条目。
系统日志	显示系统日志中最后 10 个条目的说明以及日期和时间。 “已安装配置”条目表示配置更改提交成功。仅显示最后 *60* 分钟的条目。

© 2019 Palo Alto Networks, Inc.

ACC

应用程序命令中心 (ACC) 是一个分析工具，提供与网络中的活动有关的可执行的智能。ACC 使用防火墙日志来以图表形式展示网络流量的趋势。图形表示可让您与数据交互，并且查看网络上的事件之间的关系，包括网络使用情况模式、流量模式，以及可疑的活动和异常。

> ACC 简介
> ACC 选项卡
> ACC 小部件
> ACC 操作
> 使用选项卡和小部件
> 使用过滤器 — 本地过滤器和全局过滤器

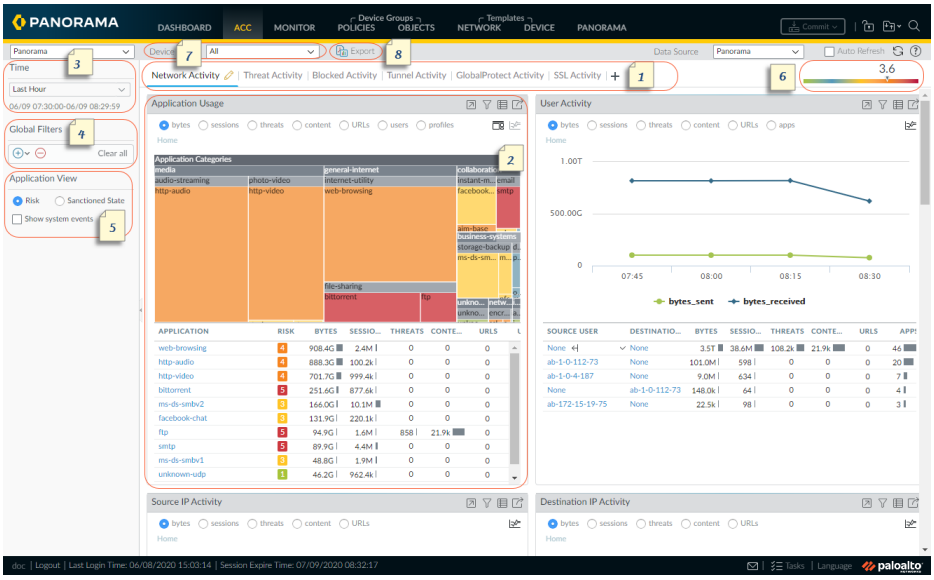
了解更多？

请参阅使用应用程序命令中心。

ACC 简介

下表显示 ACC 选项卡并说明每个组件。

ACC 简介



1	**Tabs**（选项卡）	ACC 包括可在其中查看网络流量、威胁活动、阻止活动、隧道活动和移动网络活动（如果已启用 GTP 安全）的预定义选项卡。有关每个选项卡的信息，请参阅 ACC 选项卡。
2	小部件	每个选项卡都包括一组默认的小部件，这些小部件最能代表与选项卡相关联的事件和趋势。小部件可让您使用以下过滤器调查数据：字节（传入和传出）、会话、内容（文件和数据）、URL 类别、应用程序、用户、威胁（恶意、良性、灰色软件、钓鱼）以及计数。有关每个小部件的信息，请参阅 ACC 小部件。
3	时间	每个小部件中的图表和图形提供实时视图和历史视图。可以选择一个自定义范围，或者使用从最近 15 分钟至最近 90 天内（或最近 30 个日历日内）的一个预定义时间段。 默认情况下，用于展示数据的时间段为最后一小时。会在屏幕上显示日期和时间间隔。例如： `11/11 10:30:00-01/12 11:29:59`
4	全局过滤器	全局过滤器可让您设置适用于所有选项卡的过滤器。图表和图形会在展示数据之前应用选定的过滤器。有关使用过滤器的信息，请参阅 ACC 操作。
5	**Application View**（应用程序视图）	应用程序视图可让您通过正在网络上使用的批准或未批准应用程序，或通过正在网络上使用的应用程序的风险级别对 ACC 视图进行筛选。绿色表示批准的应用程序，蓝色表示未批准的应用程序，黄色表示在不同虚拟系统或设备组中拥有不同批准状态的应用程序。

© 2019 Palo Alto Networks, Inc.

ACC 简介		
6	**Risk Meter**（风险计量器）	风险计量器（最低级别 1 到最高级别 5）指示网络中的相对安全风险。而且它使用各种因素，例如在网络中看到的应用程序的类型、与应用程序相关联的风险级别、通过阻止的威胁的数量看到的威胁活动和恶意软件，以及指向恶意主机和域的受影响的主机或流量。
7	源	用于显示防火墙和 Panorama™ 之间不同的数据。您可以使用以下选项选择用于在 ACC 上生成视图的数据： **Virtual System**（虚拟系统）：在为多个虚拟系统启用的防火墙中，则可以使用 **Virtual System**（虚拟系统）下拉列表更改 ACC 显示，以包括所有虚拟系统或者仅包括选定的虚拟系统。 设备组：在 Panorama 上，您可以使用 **Device Group**（设备组）下拉菜单来更改 ACC 显示，以包括所有设备组或者仅包括选定设备组的数据。 **Data Source**（数据源）：在 Panorama 中，还可以将显示更改为使用 **Panorama** 或 **Remote Device Data**（远程设备数据）（即受管防火墙数据）。如果数据源是 **Panorama**，则可以过滤特定设备组的显示。
8	导出	可以将当前选项卡中显示的小部件导出为 PDF。

© 2019 Palo Alto Networks, Inc.

ACC 选项卡

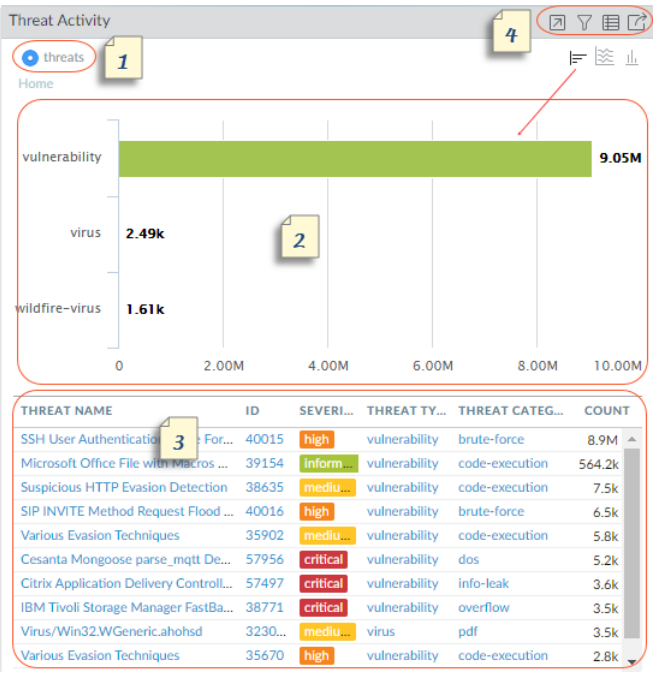
- **Network Activity**（网络活动）— 简要显示网络上的流量和用户活动。该视图专注于最常用的热门应用程序、热门用户（即通过深入分析用户访问的字节、内容、威胁和 URL 而产生流量的用户），以及最常用的安全策略规则（针对发生的流量匹配）。此外，您可以按照源或目标区域、地区、IP 地址、Ingress 和 Egress 接口以及主机信息（例如网络中最常用的设备的操作系统）来查看网络活动。
- **Threat Activity**（威胁活动）— 简要显示网络上的威胁。它专注于排名靠前的威胁，即安全漏洞、间谍软件、病毒、访问恶意域或 URL 的主机、按文件类型和应用程序提交的顶级 WildFire，以及使用非标准端口的应用程序。Compromised Hosts（受影响的主机）小部件使用更好的可视化技术对检测进行补充。它使用来自关联事件选项卡（Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlated Events（关联事件）的信息来按照源用户或 IP 地址提供网络中的受影响主机的数据的聚合视图，按严重性排序。
- **Blocked Activity**（阻止的活动）— 专门显示被阻止进入网络的流量此选项卡中的小部件可让您查看被以下项拒绝的活动：应用程序名称、用户名、威胁名称、内容（文件和数据），以及含有阻止流量的拒绝操作的热门安全规则。
- **Mobile Network Activity**（移动网络活动）— 使用根据安全策略规则配置生成的 GTP 日志显示网络上的移动流量可视化表示。该视图包括您可以向其应用 ACC 筛选程序并深入分析以隔离所需信息的交互式和可自定义的 GTP 事件、移动订户活动和 GTP 拒绝原因小部件。启用 SCTP 安全性时，此选项卡上的小部件将显示防火墙上 SCTP 事件的直观表示形式和详细信息，以及每个 SCTP 关联 ID 发送和接收的块的个数。
- **Tunnel Activity**（隧道活动）— 根据隧道检测策略显示防火墙检测的隧道流量活动。信息包括基于隧道 ID、监控标签、用户和隧道协议（如通用路由封装 (GRE)、用户数据 (GTP-U) 的通用分组无线服务 (GPRS) 隧道协议和非加密 IPSec）的隧道使用情况。
- **GlobalProtect Activity**（**GlobalProtect** 活动）— 显示 GlobalProtect 部署中的用户活动概述。信息包括用户数量、用户连接次数、用户连接的网关、连接失败数和失败原因、使用的身份验证方法和 GlobalProtect 应用程序版本的摘要以及被隔离的端点数量。
- **SSL Activity**（**SSL** 活动）— 根据您的解密策略和配置文件显示已加密和未解密的 TLS/SSL 流量活动。您可以查看 TLS 活动与非 TLS 活动的对比、解密通信量与未解密通信量的对比、解密失败原因、成功的 TLS 版本以及密钥交换活动。您可以基于这些信息，识别导致解密失败的流量，然后，使用解密日志和自定义解密报告模板深入了解该流量的详细信息和上下文，这样就可以精确地诊断并修复问题。

您还可以根据使用选项卡和小部件中的说明自定义选项卡和小部件。

© 2019 Palo Alto Networks, Inc.

ACC 小部件

每个选项卡上的小部件都是交互式的。可以设置过滤器，并且深入分析显示，从而自定义视图并重点关注所需的信息。



每个小部件都经过结构化，以显示以下信息：

1	查看	可以按照字节、会话、威胁、计数、用户、内容、应用程序、URL、恶意、良性、灰色软件、钓鱼、文件（名）、数据、配置文件、对象、门户、网关和配置文件来对数据进行排序。各个小部件的可用选项有所不同。
2	图形	图形显示选项有树状图、线形图、水平条形图、堆栈区域图形、堆栈条形图、饼图以及地图。各个小部件的可用选项有所不同，并且每个图形类型的交互体验也不同。例如，使用非标准端口的应用程序的小部件可让您选择树状图和线形图。 要深入分析显示，可单击图形。单击的区域会成为过滤器，可让您放大所选的内容，并且查看有关该内容的更详细的信息。
3	表	在图形下方的表格中，会显示用于展示图形的数据的详细视图。 可以在表格中单击并设置针对元素的本地过滤器或全局过滤器。使用本地过滤器，可以更新图形，并且按照此过滤器来对表格进行排序。 使用全局过滤器，能够以 ACC 为中心进行查看，从而仅显示特定于此过滤器的信息。
4	操作	以下为小部件标题栏中的可用操作： • **Maximize view**（最大化视图）— 可让您放大小部件，从而在更大的屏幕空间中进行查看。在最大化视图中，您可以查看除默认小部件视图中显示的前十个项目以外的更多项目。 • **Set up local filters**（设置本地过滤器）— 可让您添加过滤器以调整小部件中显示的内容。请参阅使用筛选程序 — 本地筛选程序和全局筛选程序。

© 2019 Palo Alto Networks, Inc.

		• （跳到日志）— 可让您直接导航到日志（**Monitor**（监控）> **Logs**（日志）> **<log-type>**）。在展示图形的时间段内对日志进行过滤。 如果已设置本地过滤器和全局过滤器，则日志查询会合并时间段和过滤器，并且仅显示与设置的过滤器相匹配的日志。 • 导出 — 可让您将图形导出为 PDF。

对于每个小部件的说明，请参阅使用 ACC 中的详细信息。

© 2019 Palo Alto Networks, Inc.

ACC 操作

要自定义和调整 ACC 显示，可以添加和删除选项卡、添加和删除小部件、设置本地过滤器和全局过滤器，以及与小部件进行交互。

- 使用选项卡和小部件
- 使用过滤器 — 本地过滤器和全局过滤器

使用选项卡和小部件

以下选项说明了如何使用和自定义选项卡和小部件。

- 添加自定义选项卡
  1. 选择 Add（添加）( ) 以及选项卡列表。
  2. 添加 **View Name**（视图名称）。此名称会用作选项卡的名称。最多可以添加 10 个自定义选项卡。

- 编辑选项卡。

  选择选项卡，然后单击选项卡名称旁边的 Edit（编辑）以编辑选项卡。

  示例：Threat Activity。

- 设置选项卡为默认
  1. 编辑选项卡。
  2. 选择 以将当前选项卡为默认。每次您登录到防火墙时，都将显示该选项卡。

- 保存选项卡状态
  1. 编辑选项卡。
  2. 选择 以将您当前选项卡中的首选项保存为默认设置。

     包括任何您已设置的过滤器的选项卡状态在各个 HA 对等之间同步。

- 导出选项卡
  1. 编辑选项卡。
  2. 选择 以导出当前选项卡。选项卡以 .txt 文件的形式下载至您的计算机。您必须启用弹出窗口方可下载文件。

- 导入选项卡
  1. 添加自定义选项卡
  2. 选择 以导入选项卡。
  3. 浏览至文本 (.txt) 文件并将其选中。

- 查看视图中包括哪些小部件。
  1. 选择视图，然后单击编辑 ( )。
  2. 选择 **Add Widgets**（添加小部件）下拉列表可查看选定的小部件。

© 2019 Palo Alto Networks, Inc.

- 添加小部件或小部件组。
  1. 添加新的选项卡，或者编辑预定义的选项卡。
  2. 选择 **Add Widgets**（添加小部件），然后选中要添加的小部件。最多可以添加 12 个小部件。
  3. （可选）如需创建双列布局，请选择 **Add Widget Group**（添加小部件组）。可以将小部件拖放到双列显示中。将小部件拖动到布局中时，会在放置小部件之处显示占位符。

     不能命名小部件组。

- 删除选项卡、小部件或小部件组。
  - 如需删除自定义选项卡，请选中相应选项卡，然后单击删除(Test)。

    不能删除预定义的选项卡。
  - 如需删除小部件或小部件组，请编辑选项卡，然后单击 Delete（删除）([X])。不能撤消删除。

- 重置默认视图。

  可以在预定义的视图（例如阻止的活动视图）中删除一个或多个小部件。如果要重置布局以包括选项卡的默认小部件组，可编辑选项卡并 **Reset View**（重置视图）。

使用过滤器 — 本地过滤器和全局过滤器

如需深入分析详细信息，同时更好地控制 ACC 显示，您可选择使用筛选程序。

- **Local Filters**（本地筛选程序）— 可对特定的小部件应用本地筛选程序。本地过滤器可让您与图形进行交互，并且自定义显示的内容，从而能够深入分析详细信息，以及访问要在特定小部件上监控的信息。您可采用两种方式应用本地过滤程序 - 单击图形或表格中的属性，或者选择小部件内的 **Set Filter**（设置过滤器）。**Set Filter**（设置筛选程序）可让您设置在重新启动之后仍然可以持续发挥作用的本地筛选程序。
- **Global filters**（全局筛选程序）— 可以跨 ACC 应用全局筛选程序。全局过滤器可让您立即根据自己最为关注的详细信息来调整显示的内容，并且从当前显示中排除无关的信息。例如，要查看与特定用户和应用程序相关的所有事件，可以应用用户的 IP 地址并指定应用程序以创建全局过滤器，从而通过 ACC 中的所有选项卡和小部件仅显示关于该用户和应用程序的信息。在各次登录之间全局过滤器的效果不是永久性的。

  可以采用三种方式应用全局过滤器：

- 从表格设置全局筛选器 — 从任何小部件的表格中选择属性，然后将其应用为全局筛选器。
- **Add a widget filter to be a global filter**（将小部件过滤程序添加到全局过滤程序）- 将鼠标悬停于属性上方，然后单击属性右侧的箭头图标。此选项可让您提升小部件中使用的本地过滤程序，同时全局应用属性，以更新 ACC 上所有选项卡的显示内容。
- 定义全局筛选器 — 使用 ACC 上的 **Global Filters**（全局筛选器）窗格定义筛选器。

- 设置本地过滤器。

  还可以在图形下方的表格中单击某个属性，以将其应用为本地过滤器。

  1. 选择小部件，然后单击 Filter（筛选）()。

© 2019 Palo Alto Networks, Inc.

2. 添加要应用的( ) 筛选器。
3. 单击应用。这些过滤器在重新启动之后仍然可以持续发挥作用。

小部件名称旁边会表示在小部件中应用的本地过滤器的数量。

- 从表格设置全局过滤器。

  将鼠标悬停于表格中属性的上方，然后单击出现在此属性右侧的箭头。

- 使用全局筛选程序窗格设置全局筛选程序。

  添加 ( ) 要应用的筛选程序。

- 将本地过滤器升级为全局过滤器。
  1. 在小部件中的任意表格上，选择一个属性。这样会将该属性设置为本地过滤器。
  2. 如需将该筛选程序升级为全局筛选程序，请将鼠标悬停于属性上方，然后单击属性右侧的箭头。

- 删除过滤器。

  单击 Remove（删除）( ) 可删除筛选器。

  - **Global filters**（全局筛选程序）— 位于 Global Filters（全局筛选程序）窗格中。
  - **Local filters**（本地筛选程序）— 单击 Filter（筛选程序）( ) 会跳出 Set Local Filters（设置本地筛选程序）对话框，然后可选择筛选程序并将其删除。

- 清除所有筛选器。

  - **Global filters**（全局筛选器）— **Clear all**（清除所有）全局筛选器。
  - **Local filters**（本地筛选程序）— 选择一个小部件，然后单击 Filter（筛选程序）( )。然后启用“设置本地筛选器”小部件中的 **Clear All**（清除所有）。

- 过滤器求反。

  选择一个属性，然后对筛选器进行 Negate（求反）( )。

  - **Global filters**（全局筛选程序）— 位于 Global Filters（全局筛选程序）窗格中。
  - **Local filters**（本地筛选程序）— 单击 Filter（筛选程序）( ) 会跳出 Set Local Filters（设置本地筛选程序）对话框，添加筛选程序，然后对其进行求反。

- 查看正在使用的过滤器。

  - **Global filters**（全局筛选程序）— Global Filters（全局筛选程序）下方的左窗格中会显示已应用的全局筛选程序的数量。
  - **Local filters**（本地筛选程序）— 小部件名称旁边会显示在小部件中应用的本地筛选程序的数量。如需查看筛选程序，请单击 **Set Local Filters**（设置本地筛选程序）。

© 2019 Palo Alto Networks, Inc.

监视

以下主题介绍可用于监控网络中的活动的防火墙报告和日志：

> Monitor（监控）> Logs（日志）
> Monitor（监控）> External Logs（外部日志）
> Monitor（监控）> Automated Correlation Engine（自动关联引擎）
> Monitor（监控）> Packet Capture（数据包捕获）
> 监视 > App Scope
> 监视 > 会话浏览器
> Monitor（监控）> Block IP List（阻止 IP 列表）
> 监视 > Botnet
> Monitor（监控）> PDF Reports（PDF 报告）
> Monitor（监控）> Manage Custom Reports（管理自定义报告）
> 监测 > 报告

Monitor（监控）> Logs（日志）

以下主题提供有关监控日志的其他信息。

您想了解什么内容？	请参阅：
了解不同类型的日志。	日志类型
筛选日志。 导出日志。 查看各日志条目的详细信息。 修改日志显示。	日志操作
了解更多？	监控并管理日志。

日志类型

- **Monitor**（监控）> **Logs**（日志）

防火墙将显示所有日志，以便尊重基于角色的管理权限。仅显示您有权限查看的信息，而且这些信息因所查看的日志类型而异。有关管理员权限的信息，请参阅 设备> 管理员角色。

日志类型	说明
通信	每个会话的开始和结束显示一个条目。每个条目均包括日期和时间，源和目标区域、地址和端口，应用程序名称，应用到流的安全规则名称，规则操作（允许、拒绝或丢弃）、Ingress 和 Egress 接口、字节数和会话结束原因。 类型列显示条目是用于会话的开始还是结束，或者会话已拒绝还是已丢弃。“drop”表示阻止通信的安全规则指定了“any”应用程序，而“deny”则表示规则标识了特定应用程序。 如果在标识应用程序之前丢弃通信，例如当规则丢弃特定服务的所有通信时，应用程序将显示为“not-applicable”。 深入分析流量日志，了解有关各条目、构件和操作的更多详细信息： • 单击详细信息 ( ) 可查看有关会话的其他详细信息，比如 ICMP 条目是否在相同源和目标之间聚合多个会话（**Count**（计数）值将大于 1）。 • 在带活动 AutoFocus™ 许可证的防火墙上，将鼠标悬停于 IP 地址、文件名、URL、用户代理、威胁名称或日志条目所含哈希的旁边，然后单击下拉列表 ( ) 来打开该构件的 AutoFocus 情报摘要。 • 若要添加设备到隔离列表（**Device**（设备）> **Device Quarantine**（设备隔离）），请打开设备的 **Host ID**（主机 **ID**）下拉列表，并（在弹出的对话框中）**Block Device**（阻止设备）。
威胁	针对防火墙生成的每个安全警报显示一个条目。每个条目包括日期和时间，威胁名称或 URL，源和目标区域、地址和端口，应用程序名称，应

© 2019 Palo Alto Networks, Inc.

日志类型	说明
	用于流量的安全规则名称，以及警报操作（**allow**（允许）或 **block**（阻止））和严重性。 Type（类型）列将指明威胁的类型，如“virus（病毒）”或“spyware（间谍软件）”；Name（名称）列为威胁说明或 URL；Category（类别）列为威胁类别（如“keylogger（键盘记录程序”）或 URL 类别。 深入分析威胁日志，了解有关各条目、构件和操作的更多详细信息： • 单击详细信息 ( ) 可查看有关威胁的其他详细信息，比如条目是否在相同源和目标之间聚合相同类型的多个威胁（**Count**（计数）值将大于 1）。 • 在带活动 AutoFocus 许可证的防火墙上，将鼠标悬停于 IP 地址、文件名、URL、用户代理、威胁名称或日志条目所含哈希的旁边，然后单击下拉列表 ( ) 来打开该构件的 AutoFocus 情报摘要。 • 如果已启用本地数据包捕获，请单击下载 ( ) 来访问捕获的数据包。要启用本地数据包捕获，请参阅 **Objects**（对象）> **Security Profiles**（安全配置文件）下面的小节。 • 要查看有关威胁的更多详细信息或直接人威胁日志快速配置威胁免除，请单击 **Name**（名称）列中的威胁名称。免除配置文件列表显示所有自定义防病毒、防间谍软件和漏洞保护配置文件。要配置威胁签名的免除，请选中安全配置文件名称旁边的复选框，并保存更改。要添加 IP 地址免除（每个签名最多 100 个 IP 地址），请突出显示安全配置文件，在 Exempt IP Addresses（免除 IP 地址）部分中添加 IP 地址，然后单击 **OK**（确定）保存。要查看或修改免除，请转到相关联的安全配置文件，然后单击 **Exceptions**（免除）选项卡。例如，如果威胁类型为漏洞，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Vulnerability Protection**（漏洞保护），单击相关联的配置文件，然后单击 **Exceptions**（免除）选项卡。 • 若要添加设备到隔离列表（**Device**（设备）> **Device Quarantine**（设备隔离）），请打开设备的 **Host ID**（主机 **ID**）下拉列表，并（在弹出的对话框中）**Block Device**（阻止设备）。
URL 筛选	显示 URL 过滤器的日志，该过滤器用于控制对网站的访问以及用户是否可以向网络提交凭据。 选择 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）以定义 URL 过滤设置，包括要阻止或允许以及要向其授予或禁用凭据提交的 URL 类别。您也可以启用 URL 的 HTTP 标题日志记录选项。 在带活动 AutoFocus 许可证的防火墙上，将鼠标悬停于 IP 地址、文件名、URL、用户代理、威胁名称或日志条目所含哈希的旁边，然后单击下拉列表 ( ) 来打开该构件的 AutoFocus 情报摘要。
WildFire 提交内容	显示防火墙转发用于 WildFire™ 分析的文件和电子邮件链接的日志。WildFire 云分析样本并返回分析结果，其中包括分配给样本的 WildFire 判定（良性、恶意软件、灰色软件或网络钓鱼）。您可以通过查看 Action（操作）列确认防火墙是否允许或阻止基于安全策略规则的文件。

© 2019 Palo Alto Networks, Inc.

日志类型	说明
	在带活动 AutoFocus 许可证的防火墙上，将鼠标悬停于 IP 地址、文件名、URL、用户代理、威胁名称或日志条目所含哈希（文件摘要）列中）的旁边，然后单击下拉列表 ( ) 来打开该构件的 AutoFocus 情报摘要。
数据筛选	显示安全策略（附有数据筛选配置文件）的日志，以防信用卡或社交安全号等敏感信息离开防火墙保护的区域，同时也会显示文件传送阻止配置文件，该配置文件可防止特定文件类型被上传或下载。 要对访问日志条目的详细信息配置密码保护，请单击 ↓。输入密码，然后单击**OK**。有关更改或删除数据保护密码的说明，请参阅 Device（设备）> Response Pages（响应页面）。 系统在每个会话中只会提示一次输入密码。
HIP 匹配	显示在将代理报告的原始 HIP 数据与定义的 HIP 对象和 HIP 配置文件进行比较时，GlobalProtect™ 网关识别的所有 HIP 匹配。与其他日志不同，即使与安全策略不匹配，也会记录 HIP 匹配。有关更多信息，请参阅 Network（网络）> GlobalProtect > Portals（门户）。 要添加设备到隔离列表（**Device**（设备）> **Device Quarantine**（设备隔离）），请打开设备的 **Host ID**（主机 **ID**）下拉列表，并（在弹出对话框中）**Block Device**（阻止设备）。
GlobalProtect	显示 GlobalProtect 连接日志。使用此信息来标识您的 GlobalProtect 用户及其客户端操作系统版本，对连接和性能问题进行故障排除，以及标识用户连接的门户和网关。 若要添加设备到隔离列表（**Device**（设备）> **Device Quarantine**（设备隔离）），请打开设备的 **Host ID**（主机 **ID**）下拉列表，并（在弹出的对话框中）**Block Device**（阻止设备）。
IP 标记	显示标记应用于特定 IP 地址的方式和时间相关的信息。使用此信息可确定特定 IP 地址放置在地址组中的时间和方式，以及会影响该地址的策略规则。日志包括接收时间（第一个和最后一个会话数据包到达的日期和时间）、虚拟系统、源 IP 地址、标记、事件、超时、源名称和源类型。
User-ID™	显示有关 IP 地址到用户名映射的信息，如映射信息的源、User-ID 代理执行映射的时间以及映射过期之前的剩余时间。您可以使用这些信息帮助排除 User-ID 问题。例如，如果防火墙为用户应用错误的策略规则，则您可以查看日志以验证是否已将该用户映射到正确的 IP 地址以及组关联是否正确。
解密	显示不解密配置文件控制的流量的解密会话和未解密会话相关的信息，包括 GlobalProtect 会话。 日志默认显示失败的 SSL 解密握手相关的信息。您可以在解密策略规则 **Options**（选项）中为成功的 SSL 解密握手启用日志记录。日志可显示大量信息，您可以通过这些信息识别弱协议和密码套件（密钥交换、加密和身份验证算法）、绕过的解密活动、解密失败以及失败原因（例如，证书链不完整、客户端身份验证、固定证书）、会话结束原因等。

© 2019 Palo Alto Networks, Inc.

日志类型	说明
	例如，使用此信息可确定是否要允许使用弱协议和算法的站点。最好是阻止开展业务不需要访问的弱站点。 对于防火墙不会解密以及您应用了不解密配置文件的流量，日志将显示因为服务器证书验证问题而被阻止的会话。 解密日志默认大小为 32 MB。但是，如果要解密大量流量或是您启用了记录成功的 SSL 解密握手，那么，您可能需要增加日志大小（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（日志记录和报告设置），然后编辑 **Log Storage**（日志存储）配额）。如果您没有未分配的日志空间，可考虑在解密日志大小和其他日志大小之间进行权衡。记录的数据越多越多，日志需要消耗的资源就越多。
GTP	显示基于事件的日志，包括有关各种 GTP 属性的信息。这些信息包括 GTP 事件类型、GTP 事件消息类型、APN、IMSI、IMEI、最终用户 IP 地址，以及新一代防火墙识别的 TCP/IP 信息，如应用程序、源和目标地址以及时间戳。
隧道检测	显示检测到的每个隧道会话的开始和结束的条目。日志包括接收时间（会话中第一个和最后一个数据包到达的日期和时间）、隧道 ID、监控标记、会话 ID 以及应用于隧道流量的安全规则等。有关更多信息，请参阅 Policies（策略）> Tunnel Inspection（隧道检测）。
SCTP	在执行状态检查、协议验证和筛选 SCTP 通信时，根据防火墙生成的日志显示 SCTP 事件和关联。SCTP 日志包括有关广泛的 SCTP 及其负载协议属性的信息，例如 SCTP 事件类型、块类型、SCTP 原因代码、Diameter 应用程序 ID、Diameter 命令代码和块。除了防火墙标识的一般信息之外，还提供此 SCTP 信息，例如源和目标地址、源和目标端口、规则和时间戳。有关更多信息，请参阅 Objects（对象）> Security Profiles（安全配置文件）> SCTP Protection（SCTP 保护）。
配置	每个配置更改显示一个条目。每个条目均包括日期和时间、管理员用户名、从其进行更改的 IP 地址、客户端类型（Web 界面或 CLI）、执行的命令类型、命令成功还是失败、配置路径以及更改前后的值。
system	每个系统事件显示一个条目。每个条目均包括日期和时间、事件严重性和事件说明。
警报	警报日志记录有关系统生成的警报的详细信息。Alarms（警报）中也将报告此日志中的信息。请参阅定义警报设置。
身份验证	显示有关当最终用户尝试访问由身份验证策略规则控制访问的网络资源时发生的身份验证事件的信息。您可以使用此信息帮助排除访问问题，并根据需要调整身份验证策略。结合关联对象，您还可以使用身份验证日志识别网络中的可疑活动（如暴力攻击）。 或者，您可以将身份验证规则配置为日志身份验证超时。这些超时与用户只需要对资源进行一次身份验证但可以重复访问的时间段相关。查看有关超时的信息有助于您确定是否以及如何进行调整。

© 2019 Palo Alto Networks, Inc.

日志类型	说明
	系统日志记录与 *GlobalProtect* 以及管理员访问 *Web* 界面相关的身份验证事件。
统一	在单个视图中显示最新通信、威胁、URL 筛选、WildFire 提交和数据筛选日志条目。集中式日志视图可让您同时调查并筛选不同类型的日志，而不必单独搜索每一个已设置的日志。或者，您可以选择要显示的日志类型：单击过滤器字段左侧的箭头，选择 **traffic**（流量）、**threat**（威胁）、**url**、**data**（数据）和/或 **wildfire** 以仅显示选中的日志类型。 在带活动 AutoFocus 许可证的防火墙上，将鼠标悬停于 IP 地址、文件名、URL、用户代理、威胁名称或日志条目所含哈希的旁边，然后单击下拉列表 ( ) 来打开该构件的 AutoFocus 情报摘要。 防火墙将显示所有日志，以便尊重基于角色的管理权限。查看日志时，所显示的内容只会包括有权查看日志。例如，没有权限查看 WildFire Submissions（WildFire 提交）日志的管理员在查看统一日志时，将无法看见 WildFire Submissions（WildFire 提交）日志条目。有关管理员权限的信息，请参阅 Device（设备）> Admin Roles（管理员角色）。 您可以将统一日志集与 *AutoFocus* 威胁情报门户结合使用。设置 AutoFocus 搜索可将 *AutoFocus* 搜索过滤器直接添加到统一日志过滤器字段。 要添加设备到隔离列表（**Device**（设备）> **Device Quarantine**（设备隔离）），请打开设备的 **Host ID**（主机 **ID**）下拉列表，并（在弹出对话框中）**Block Device**（阻止设备）。

日志操作

下表介绍日志操作。

操作	说明

筛选日志	每个日志页面的顶部均有过滤字段。您可将构件（如 IP 地址或时间范围）添加到该字段，以便查找匹配的日志条目。使用该字段右侧的图标可应用、清除、创建、保存及加载过滤器。
	Last 90 Days
	• 创建过滤：
	  • 单击日志条目中的构件可将其添加到过滤器。
	  • 单击 **Add**（添加）( ) 可定义新搜索条件。对于每一项条件，请选择定义搜索类型（**and**（和）或 **or**（或））的 **Connector**（连接符）、所搜索库的 **Attribute**（属性）、定义搜索范围的 **Operator**（运算符），以及对日志条目进行评估的 **Value**（值）。将每一项条件 **Add**（添加）到过滤器字段，并在完成操作后选择 **Close**（关闭）。之后，您便可应用 (→) 此过滤器。
	如果 *Value*（值）字符串与 *Operator*（运算符）（如 *has* 或 *in*等）相匹配，请将该字符串放入引号内，以免造成语法错误。例如，如果要按目标国家/地区进行过滤，且将 ***IN*** 用作指定 *INDIA*（印度）的 *Value*（值），请以 ***(dstloc eq "IN")*** 格式输入过滤器。

© 2019 Palo Alto Networks, Inc.

操作	说明
	日志过滤器 ***(receive_time in last-60-seconds)*** 可使显示的日志条目（和日志页面）数随时间增加或减少。 • 应用过滤器 — 单击 Apply Filter（应用过滤器）(→) 可显示与当前过滤器相匹配的日志条目。 • 删除过滤器 — 单击 Clear Filter（清除过滤器）(×) 可清除过滤器字段。 • 保存过滤器 — 单击 Save Filter（保存过滤器）( )，输入过滤器名称，然后单击 **OK**（确定）。 • 使用保存的过滤器 — 单击 Load Filter（加载过滤器）( ) 可将已保存的过滤器添加到过滤器字段。
导出日志	单击 Export to CSV（导出到 CSV）( ) 可将所有与当前过滤器相匹配的日志导出到 CSV 格式的报告并继续 **Download file**（下载文件）。默认情况下，该报告可最多包含 2,000 行日志。要更改生成的 CSV 报告的行数限制，请选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（日志记录和报告设置）> **Log Export and Reporting**（日志导出和报告），然后输入新的 **Max Rows in CSV Export**（**CSV** 导出中的最大行数）值。
突出显示策略操作	选择此选项以突出显示与操作相匹配的日志条目。过滤的日志将以下列颜色突出显示： • 绿色 — 允许 • 黄色 — 继续或替代 • 红色 — 拒绝、丢弃、丢弃-icmp、重置-客户端、重置-服务器、重置-两者、阻止-继续、阻止-替代、阻止-url、丢弃-所有、sinkhole

更改日志显示	自定义日志显示：
	• 更改自动刷新时间间隔 — 从时间间隔下拉列表中选择一种间隔设置（**60 seconds**（60 秒）、**30 seconds**（30 秒）、**10 seconds**（10 秒）或 **Manual**（手动））。
	• 更改每页显示的条目数和顺序 — 在由 10 页组成的分块中检索日志条目。
	  • 使用页底的页码控件可以浏览日志列表。
	  • 要更改每页的日志条目数，请从每页的下拉列表中选择行数（**20**、**30**、**40**、**50**、**75** 或 **100**）。
	  • 要按照升序或降序对结果进行排序，可以使用 **ASC** 或 **DESC** 下拉列表。
	• 将 IP 地址解析为域名 — 选择 **Resolve Hostname**（解析主机名）可开始将外部 IP 地址解析为域名。
	• 更改日志显示的顺序 — 选择 **DESC** 可将日志按降序排列显示，并将接收时间最近的日志条目排在开始处。选择 **ASC** 可将日志按升序排列显示，并将接收时间最久远的日志条目排在开始处。

查看各日志条目的详细信息	查看各日志条目的信息： • 要显示其他详细信息，请单击条目的 Details（详细信息）( )。如果源或目标在 **Addresses**（地址）页面中定义了 IP 地址到域或用户名的映射，则会显示名称而不是 IP 地址。要查看关联的 IP 地址，请将光标移至名称上。

© 2019 Palo Alto Networks, Inc.

操作	说明
	• 在带活动 AutoFocus 许可证的防火墙上，将鼠标悬停于 IP 地址、文件名、URL、用户代理、威胁名称或日志条目所含哈希的旁边，然后单击下拉列表 ( ) 可打开该构件的 AutoFocus 情报摘要。

© 2019 Palo Alto Networks, Inc.

Monitor（监控）> External Logs（外部日志）

使用此页面可查看从 Traps™ Endpoint Security Manager (ESM) 提取到由 Panorama™ 管理的日志收集器的日志。要在 Panorama 上查看 Traps ESM 日志，请执行以下操作：

- 在 Traps ESM 服务器上，将 Panorama 配置为 Syslog 服务器，然后选择要转发到 Panorama 的日志记录事件。这些事件包括安全事件、策略变更、ESM 服务器状态变更，以及设置设置变更等。
- 在使用一个或多个受管日志收集器部署在 Panorama 模式下的 Panorama 上，请设置提取配置文件 (Panorama > Log Ingestion Profile（日志提取配置文件）)，然后将配置文件附加到在其中存储 Traps ESM 日志的收集器组 (Panorama > Collector Groups（收集器组）)。

外部日志与设备组不关联，且只有在选择 **Device Group:All**（设备组：全部）后才会显示，因为日志不是从防火墙转发。

日志类型	说明
Monitor（监控）> **External Logs**（外部日志）> **Traps ESM** > **Threat**（威胁）	这些威胁事件包括 Traps 客户端所报告的所有防御、通知、临时和检测后事件。
Monitor（监控）> **External Logs**（外部日志）> **Traps ESM** > **System**（系统）	ESM 服务器系统事件包括与 ESM 状态、许可证、ESM 技术支持文件以及与 WildFire 通信相关的更改。
Monitor（监控）> **External Logs**（外部日志）> **Traps ESM** > **Policy**（策略）	策略变更事件包括对规则、保护级别、内容更新、哈希控制日志和判定的更改。
Monitor（监控）> **External Logs**（外部日志）> **Traps ESM** > **Agent**（代理）	在端点上发生的客户端更改事件包括对内容更新、许可证、软件、连接状态、一次性操作规则、进程和服务以及隔离文件的更改。
Monitor（监控）> **External Logs**（外部日志）> **Traps ESM** > **Config**（配置）	ESM 配置更改事件包括对许可、管理用户和角色、进程、限制设置和条件的系统范围更改。

Panorama 可以将端点上的离散安全事件与网络上的事件进行相关联，以跟踪端点和防火墙之间的任何可疑或恶意的活动。要查看 Panorama 识别的关联事件，请参阅Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlated Events（关联事件）。

© 2019 Palo Alto Networks, Inc.

Monitor（监控）> Automated Correlation Engine（自动关联引擎）

自动关联引擎跟踪网络中的模式，并且关联表示可疑行为中的升级情况的事件，或者涉及恶意活动的事件。引擎会用作个人安全分析师，它会在防火墙上的不同日志组之间仔细检查孤立的事件、查询特定模式的数据，以及将各个点连接起来，以便获得实用的信息。

关联引擎使用生成关联事件的关联对象。关联事件会核对相关证据，以跟踪看似无关的网络事件之间的共性，并且关注事件响应。

以下型号支持自动关联引擎：

- Panorama — M 系列设备和虚拟设备
- PA-3200 系列防火墙
- PA-5200 系列防火墙
- PA-7000 系列防火墙

您想了解什么内容？	请参阅：
什么是关联对象？	Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlation Objects（关联对象）
什么是关联事件？ 在何处查看关联匹配的匹配证据？	Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlated Events（关联事件）
如何查看关联匹配的图形视图？	请参阅 ACC 中受影响的主机小部件。
了解更多？	使用自动关联引擎

Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlation Objects（关联对象）

针对漏洞和恶意软件分发方法的发展，关联对象扩展了防火墙中基于签名的恶意软件检测功能。它们提供了关于在不同的日志组之间识别可疑行为模式的智能，并且收集调查和推动事件响应所需的证据。

关联对象是定义文件，指定用于匹配的模式、用于执行查询的数据源，以及查找这些模式的时间段。模式是查询数据源的条件的布尔结构，每个模式都分配了严重性和阈值（在指定的时间限制之内出现模式匹配的次数）。出现模式匹配时，会记录关联事件。

用于执行查找的数据源可以包括以下日志：应用程序统计信息、流量、流量摘要、威胁摘要、威胁、数据过滤和 URL 过滤。例如，关联对象的定义可以包括一组模式，这些模式会查询关于以下内容的日志：受感染主机的证据、恶意软件模式的证据、流量中恶意软件的横向移动、URL 过滤和威胁。

关联对象由 Palo Alto Networks® 定义，并且包含在内容更新数据包中。必须具备有效的威胁防御许可证才能获得内容更新。

默认情况下，所有关联对象都处于启用状态。要禁用对象，请将其选中并单击 **Disable**（禁用）。

© 2019 Palo Alto Networks, Inc.

关联对象字段	说明
名称和标题	表示关联对象检测到的活动的类型的标签。
ID	识别关联对象的编号，此编号是唯一的。而且此编号属于 6000 系列。
类别	针对网络、用户或主机的威胁或伤害的类型的摘要。
状态	表示关联对象的状态，即启用（活动）还是禁用（不活动）。
说明	说明会指出防火墙或 Panorama 分析日志的匹配条件。它还会描述用于识别恶意活动或可疑主机行为的升级模式或进度路径。

Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlated Events（关联事件）

关联事件扩展了防火墙和 Panorama 中的威胁检测功能，并且会收集网络中的用户或主机存在可疑行为或异常行为的证据。

通过关联对象，可以重点关注特定的条件或行为，并且跟踪多个日志源之间的共性。在网络中观察到关联对象中指定的一组条件时，每个匹配项都会记录为关联事件。

关联事件包含下表中列出的详细信息。

字段	说明
Match Time（匹配时间）	关联项目触发匹配项的时间。
Update Time（更新时间）	上一次更新匹配项的时间戳。
项目名称	触发匹配项的关联项目的名称。
Source Address（源地址）	产生流量的用户的 IP 地址。
源用户	目录服务器的用户和用户组信息（如果启用 User-ID™）。
严重性级别	根据造成的损害程度对风险进行分类的等级。
Summary（摘要）	汇总收集的针对关联事件的证据的说明。
主机 ID	设备的主机 ID。 若要添加设备到隔离列表（**Device**（设备）> **Device Quarantine**（设备隔离）），请单击设备**Host ID**（主机 **ID**）旁边的向下箭头，然后在显示的弹出窗口中，选择**Block Device**（阻止设备）。

© 2019 Palo Alto Networks, Inc.

要查看详细的日志视图，请单击条目的 Details（详细信息）( )。详细的日志视图包括匹配项的所有证据：

选项卡	说明
Match Information（匹配信息）	**Object Details**（对象详细信息）— 提供触发匹配项的关联对象的信息。有关关联对象的信息，请参阅 Monitor（监控）> Automated Correlation Engine（自动关联引擎）> Correlation Objects（关联对象）。
	Match Details（匹配详细信息）— 匹配详细信息的摘要包括匹配时间、匹配证据中的上一次更新时间、事件的严重性，以及事件摘要。
Match Evidence（匹配证据）	此选项卡包括确认关联事件的所有证据。它列出为每个会话收集的证据的详细信息。

在 **Correlated Events**（关联事件）选项卡中查看信息的图形显示，在 **ACC** > **Threat Activity**（威胁活动）选项卡中查看受影响的主机小部件。在 Compromised Hosts （受影响的主机）小部件中，按照源用户和 IP 地址聚合显示的内容，并且按照严重性进行排序。

要在记录关联事件时配置通知，可转到 **Device**（设备） > **Log Settings**（日志设置）或 **Panorama** > **Log Settings**（日志设置）选项卡。

© 2019 Palo Alto Networks, Inc.

Monitor（监控）> Packet Capture（数据包捕获）

所有 Palo Alto Networks 防火墙都具有内置的数据包捕获 (pcap) 功能，可以使用此功能捕获遍历防火墙中的网络接口的数据包。然后可以将捕获的数据用于故障排除，或者创建自定义应用程序签名。

数据包捕获功能会占用大量的 *CPU* 资源，可能会降低防火墙性能。仅在必要时使用此功能，并且确保在收集所需的数据包之后关闭此功能。

您想了解什么内容？	请参阅：
防火墙可以使用哪些不同的方法来捕获数据包？	数据包捕获概述
如何生成自定义数据包捕获？	构建自定义数据包捕获的块
如何在防火墙检测到威胁时生成数据包捕获？	启用威胁数据包捕获
在何处下载数据包捕获？	数据包捕获概述
了解更多？	
• 打开安全配置文件的扩展数据包捕获。	Device（设备）> Setup（设置）> Content-ID
• 使用数据包捕获写入自定义应用程序签名。	请参阅自定义签名。
• 防止防火墙管理员查看数据包捕获。	定义 Web 界面管理员访问。
• 请参阅示例。	请参阅执行数据包捕获。

数据包捕获概述

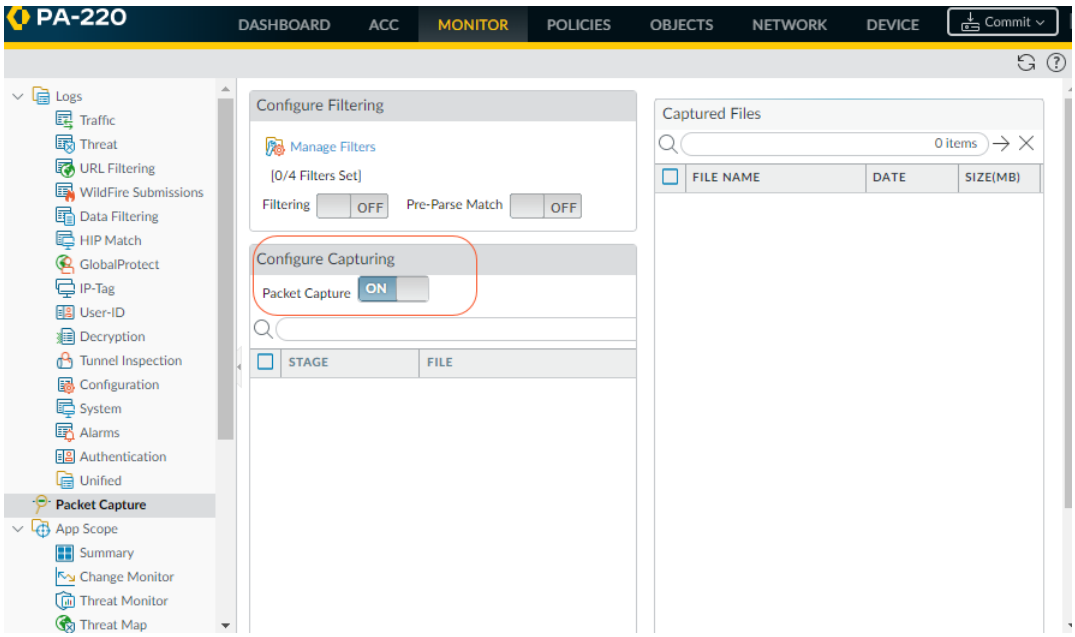
可以配置 Palo Alto Networks 防火墙以执行自定义数据包捕获或威胁数据包捕获。

- 自定义数据包捕获 — 捕获所有流量的数据包，或根据定义的过滤器捕获特定流量的数据包。例如，可以配置防火墙，以便仅捕获进出特定源和目标 IP 地址或端口的数据包。使用这些数据包捕获可解决网络流量相关问题，或收集应用程序属性以编写自定义应用程序签名（**Monitor**（监控）> **Packet Capture**（数据包捕获））。您可以根据阶段（丢弃、防火墙、接收或传输）定义文件名，并且在完成 PCAP 之后，可以在 Captured Files（捕获文件）部分下载 PCAP。
- 威胁数据包捕获 — 在防火墙检测到病毒、间谍软件或漏洞时捕获数据包。您可在防病毒、防间谍软件和漏洞防护安全配置文件中启用此功能。这些数据包捕获提供关于威胁的上下文，可帮助您确定攻击是否成功，或者了解有关攻击者使用的方法的详细信息。必须将威胁的操作设置为“允许”或“警报”，否则威胁会被阻止，并且不能捕获数据包。您可在 **Objects**（对象）> **Security Profiles**（安全配置文件）中配置此类型的数据包捕获。要下载（↓）pcap，请选择 **Monitor**（监控）> **Threat**（威胁）。

© 2019 Palo Alto Networks, Inc.

构建自定义数据包捕获的块

下表介绍 **Monitor**（监控）> **Packet Capture**（数据包捕获）页面的组件，这些组件可用于配置数据包捕获、启用数据包捕获以及下载数据包捕获文件。



自定义数据包捕获构建块	配置位置	说明
管理过滤器	配置筛选	启用自定义数据包捕获时，应该定义过滤器，以便仅捕获与过滤器匹配的数据包。这样更便于在 pcap 中定位需要的信息，并且减少防火墙执行数据包捕获所需的工作量。 单击添加以添加新的过滤器，并配置以下字段： • **ID** — 输入或选择过滤器的标识符。 • **Ingress** 接口 — 选择要捕获其流量的 Ingress 接口。 • 源 — 指定要捕获的流量的源 IP 地址。 • 目标 — 指定要捕获的流量的目标 IP 地址。 • 源端口 — 指定要捕获的流量的源端口。 • 目标端口 — 指定要捕获的流量的目标端口。 • 协议 — 指定要过滤的协议号 (1-255)。例如，ICMP 是协议号 1。 • 非 **IP** — 选择如何处理非 IP 流量（排除所有 IP 流量、包括所有 IP 流量、仅包括 IP 流量或不包括 IP 过滤器）。广播和 AppleTalk 就是典型的非 IP 流量。 • **IPv6** — 选择此选项可将 IPv6 数据包包括在过滤器中。
过滤	配置筛选	定义过滤器后，请将 **Filtering**（过滤）设置为 **ON**（开）。如果过滤为关，则会捕获所有流量。
预分析匹配	配置筛选	此选项用于高级故障排除目的。在数据包进入入口端口之后，它先继续穿过几个处理步骤，然后按预配置的过滤器分析它的匹配情况。

© 2019 Palo Alto Networks, Inc.

自定义数据包捕获构建块	配置位置	说明
		数据包可能由于故障而无法到达过滤阶段。例如，如果路由查找失败，就会发生这种情况。 如果将预分析匹配的设置设置为开，则可以对进入系统的每个数据包模拟正匹配。这将允许防火墙捕获未到达过滤阶段的数据包。如果数据包能够到达过滤阶段，则会按照过滤器配置处理它，如果它未能符合过滤条件，则被放弃。

数据包捕获	配置捕获	单击切换开关将数据包捕获设置为 **On**（开）或 **OFF**（关）。
		必须至少选择一个捕获阶段。单击添加，并指定以下项：
		• 阶段 — 指示开始捕获数据包的点：
		  • 丢弃 — 当数据包处理遇到错误并且要将数据包丢弃时使用。
		  • 防火墙- 当数据包有会话时匹配或成功创建具有会话的第一个数据包时使用。
		  • 接收- 在数据平面处理器上接收数据包时使用。
		  • 传输 — 当数据包要在数据平面处理器上传输时使用。
		• 文件- 指定捕获文件名。文件名应当以字母开头，并且可以包括字母、数字、句点、下划线或连字符。
		• 数据包计数 — 指定在最多捕获多少数据包后捕获停止。
		• **Byte Count**（字节计数）— 指定在最多捕获多少字节后捕获停止。

已捕获文件	已捕获文件	包含防火墙之前生成的自定义数据包捕获的列表。单击文件以将其下载到自己的计算机。如需删除数据包捕获，请将其选定并单击 **Delete**（删除）。 • 文件名 — 列出数据包捕获文件。文件名基于为捕获阶段指定的文件名。 • 日期 — 生成文件的日期。 • 大小 **(MB)** — 捕获文件的大小。 如果打开数据包捕获随后又将其关闭，则必须单击 Refresh（刷新）（ ），然后新的 PCAP 文件才会显示在该列表中。
清除所有设置	设置	单击清除所有设置可关闭数据包捕获，并且清除所有数据包捕获设置。 这不会关闭在安全配置文件中设置的数据包捕获。有关在安全配置文件中启用数据包捕获的信息，请参阅启用威胁数据包捕获。

启用威胁数据包捕获

- Objects（对象）> Security Profiles（安全配置文件）

© 2019 Palo Alto Networks, Inc.

要在防火墙检测到威胁时在防火墙中启用数据包捕获，可在安全配置文件中启用数据包捕获选项。

首先选择 **Objects**（对象）> **Security Profiles**（安全配置文件），然后根据下表中的说明修改所需的配置文件：

安全配置文件中的数据包捕获选项	位置
反病毒	选择自定义防病毒配置文件，然后在 **Antivirus**（防病毒软件）选项卡中选择 **Packet Capture**（数据包捕获）。
防间谍软件	选择自定义防间谍软件配置文件，单击 **DNS** 签名选项卡，然后在数据包捕获下拉列表中选择单个数据包或扩展捕获。
漏洞保护	选择自定义漏洞保护配置文件，然后在规则选项卡中单击添加，以添加新规则或选择现有规则。然后选择数据包捕获下拉列表，并且选择单个数据包或扩展捕获。

在防间谍软件配置文件和漏洞保护配置文件中，还可以启用关于例外情况的数据包捕获。单击 *Exceptions*（例外情况）选项卡，然后在签名的“数据包捕获”列中，单击下拉列表并选择 *single-packet*（单个数据包）或 *extended-capture*（扩展捕获）。

（可选）要根据已捕获数据包的数量（基于全局设置）定义威胁数据包捕获的长度，请选择 **Device**（设备）> **Setup**（设置）> **Content-ID**，然后在 Content-ID™ Settings（Content-ID™ 设置）部分中修改 **Extended Packet Capture Length (packets field)**（扩展数据包捕获长度（数据包））字段（范围为 1-50，默认为 5）。

在安全配置文件中启用数据包捕获之后，需要验证配置文件是安全规则的一部分。有关如何向安全规则添加安全配置文件的信息，请参阅安全策略概述。

如果已在安全配置文件上启用了数据包捕获，则一旦防火墙检测到威胁，您便可下载（↓）或导出相关的数据包捕获。

© 2019 Palo Alto Networks, Inc.

监视 > App Scope

以下主题介绍 App Scope 功能。

- App Scope 概述
- App Scope 摘要报告
- App Scope 更改监控报告
- App Scope 威胁监控报告
- App Scope 威胁地图报告
- App Scope 网络监控报告
- App Scope 流量地图报告

App Scope 概述

App Scope 报告能让您以图形的方式更好地了解网络的以下几个方面：

- 应用程序使用情况和用户活动的更改
- 占用大多数网络带宽的用户和应用程序
- 网络威胁

使用 App Scope 报告，您可以快速查看是否有任何不寻常或意外的行为，并有助于指出有问题的行为；每个报告都可提供网络的动态的用户可自定义窗口。报告包括选择数据和显示范围的选项。在 Panorama 上，您还可以选择所显示的信息的数据源。默认数据源（在新的 Panorama 安装软件上）使用 Panorama 上的本地数据库，该数据库会存储受管防火墙转发的日志；升级后，默认的数据源为 **Remote Device Data**（远程设备数据）（即受管防火墙数据）。要直接从受管防火墙中提取、显示数据统计图，您必须将数据源从 **Panorama** 切换至 **Remote Device Data**（远程设备数据）。

将鼠标悬停于图表上的行或栏并单击该行或该栏可切换至 ACC，并提供有关特定应用程序、应用程序类别、用户或源的详细信息。

应用程序命令中心图表	说明
Summary（摘要）	App Scope 摘要报告
更改监视器	App Scope 更改监控报告
威胁监视器	App Scope 威胁监控报告
威胁地图	App Scope 威胁地图报告
网络监视器	App Scope 网络监控报告
通信地图	App Scope 流量地图报告

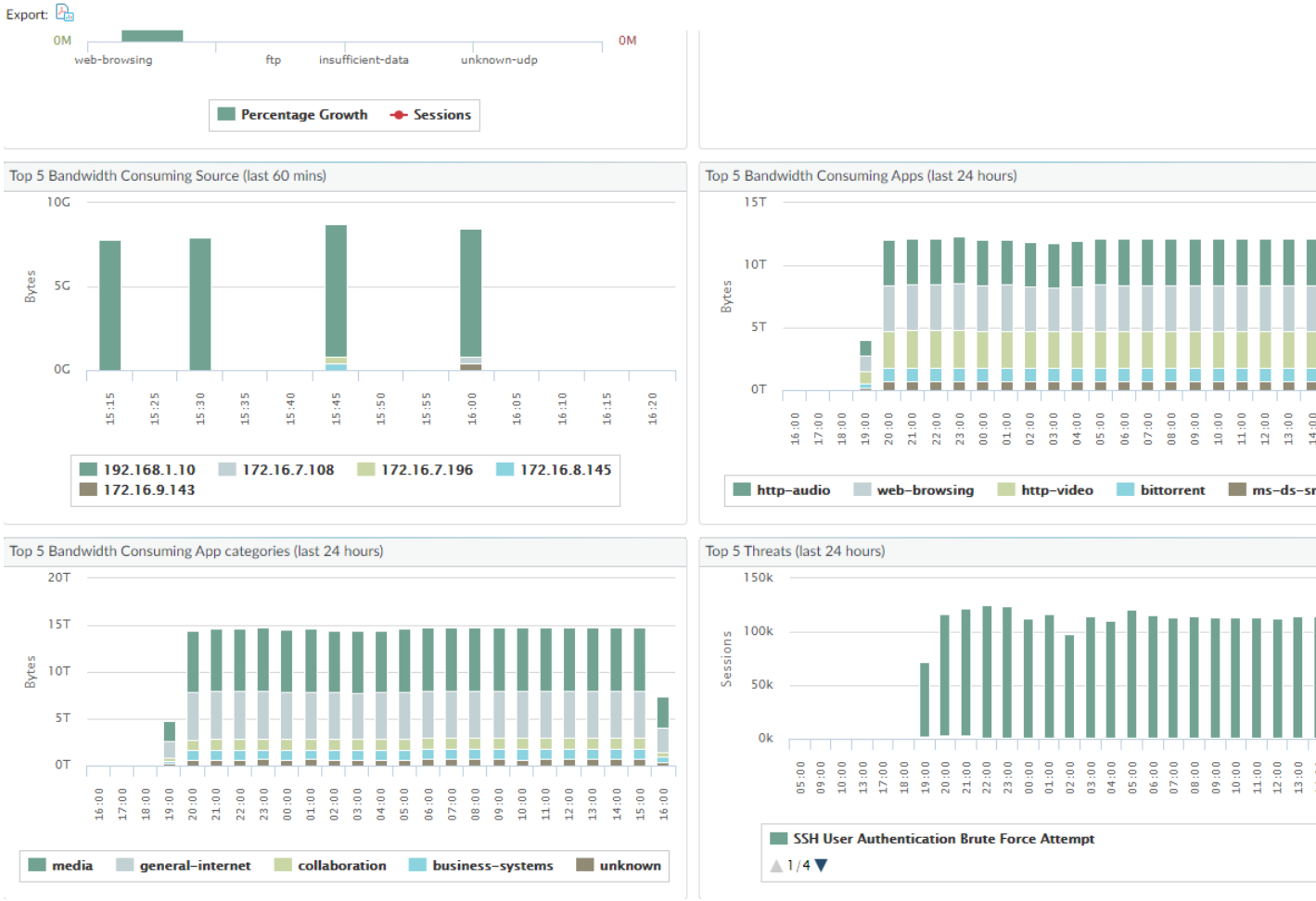
App Scope 摘要报告

摘要报告显示前五个胜利者、失败者和带宽消耗应用程序、应用程序类别、用户和源的图表。

要将摘要报告中的图表导出为 PDF，请单击 **Export**（导出）（ ）。每个图表都已另存为 PDF 输出中的页面。

App Scope 摘要报告

© 2019 Palo Alto Networks, Inc.

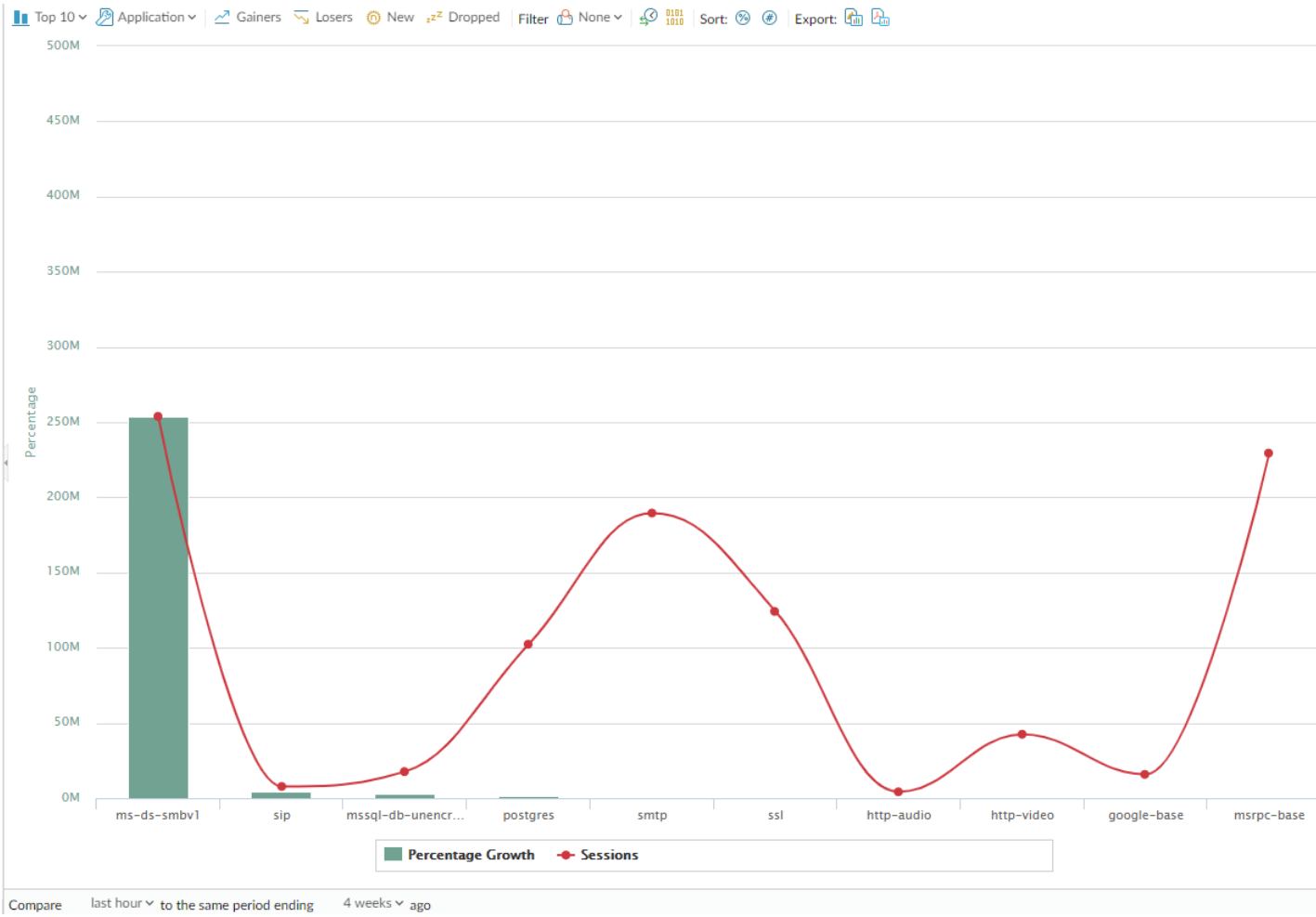


App Scope 更改监控报告

异动监控报告显示指定时间段内的更改。例如，下图显示在与过去 24 小时时段相比较的最后一小时内使用得最多的若干应用程序。排在前面的应用程序由会话数决定，并按百分比排序。

App Scope 更改监控报告

© 2019 Palo Alto Networks, Inc.



此报告包含以下选项。

异动监测报告选项	说明
顶栏	
Top 10	确定具有图表所包括的最高测量结果的记录数。
应用程序	确定报告的项目的类型：应用程序、应用程序类别、源或目标。
Gainers（获得者）	显示测量期间已增加的项目的测量结果。
Losers（失败者）	显示测量期间已减少的项目的测量结果。
New（新增项）	显示在测量期间所添加的项目的测量结果。
Dropped（已丢弃）	显示测量期间中断的项目的测量结果。
Filter（筛选器）	应用筛选器以仅显示所选项目。无显示所有条目。
计入对话与计入字节	确定是显示会话信息还是显示字节信息。

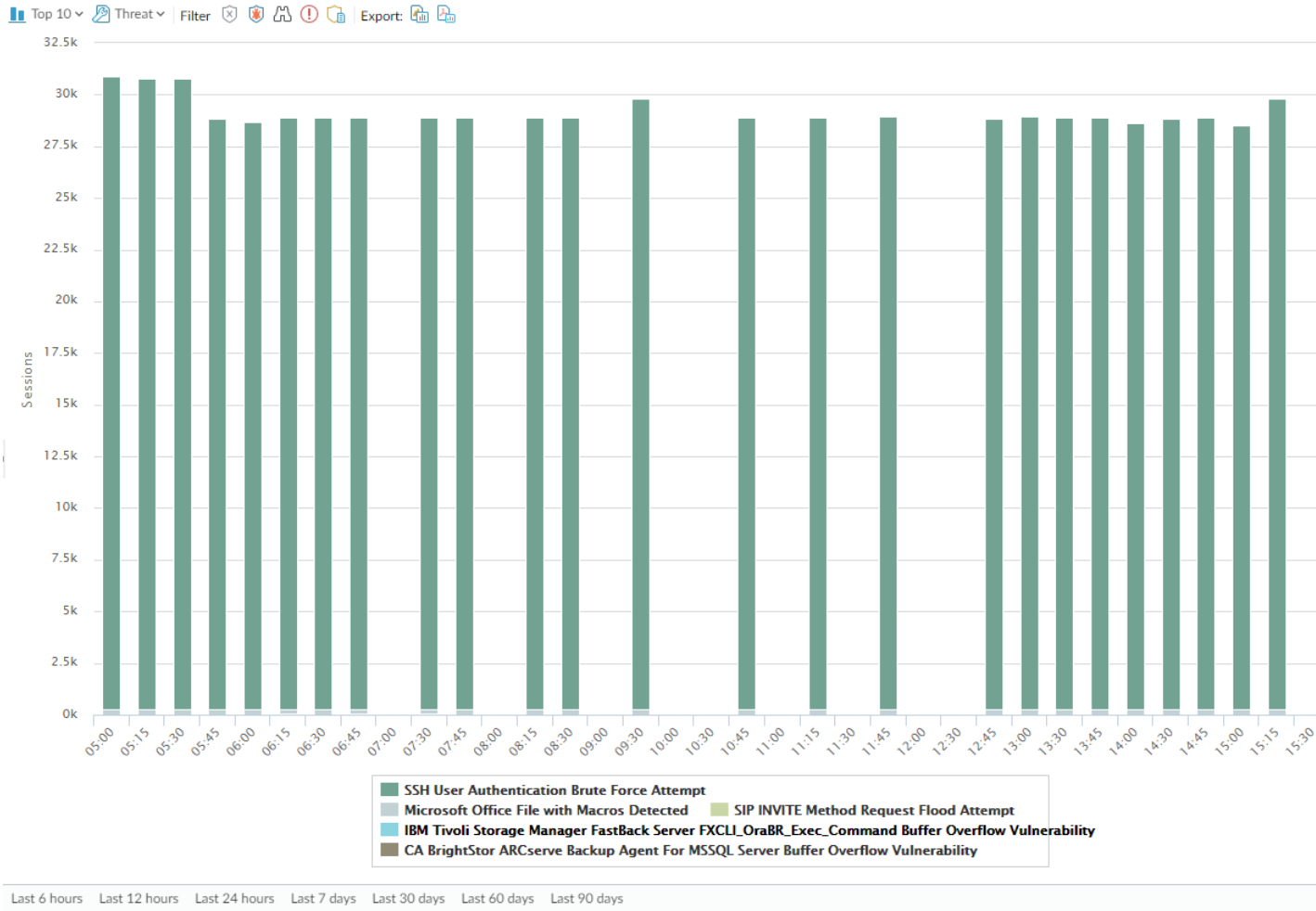
© 2019 Palo Alto Networks, Inc.

异动监测报告选项	说明
Sort（排序）	确定是按百分比还是按原始增长量对条目进行排序。
导出	导出图表作为 .png 图像或 PDF。
底栏	
比对（间隔时间）	指定执行更改测量的时间段。

App Scope 威胁监控报告

威胁监控报告显示所选时间段内排名靠前的威胁计数。例如，下图显示了过去 6 小时内排在前面的 10 种威胁类型。

App Scope 威胁监控报告



每个威胁类型均用颜色进行标记，如图表下面的图例所示。此报告包含以下选项。

© 2019 Palo Alto Networks, Inc.

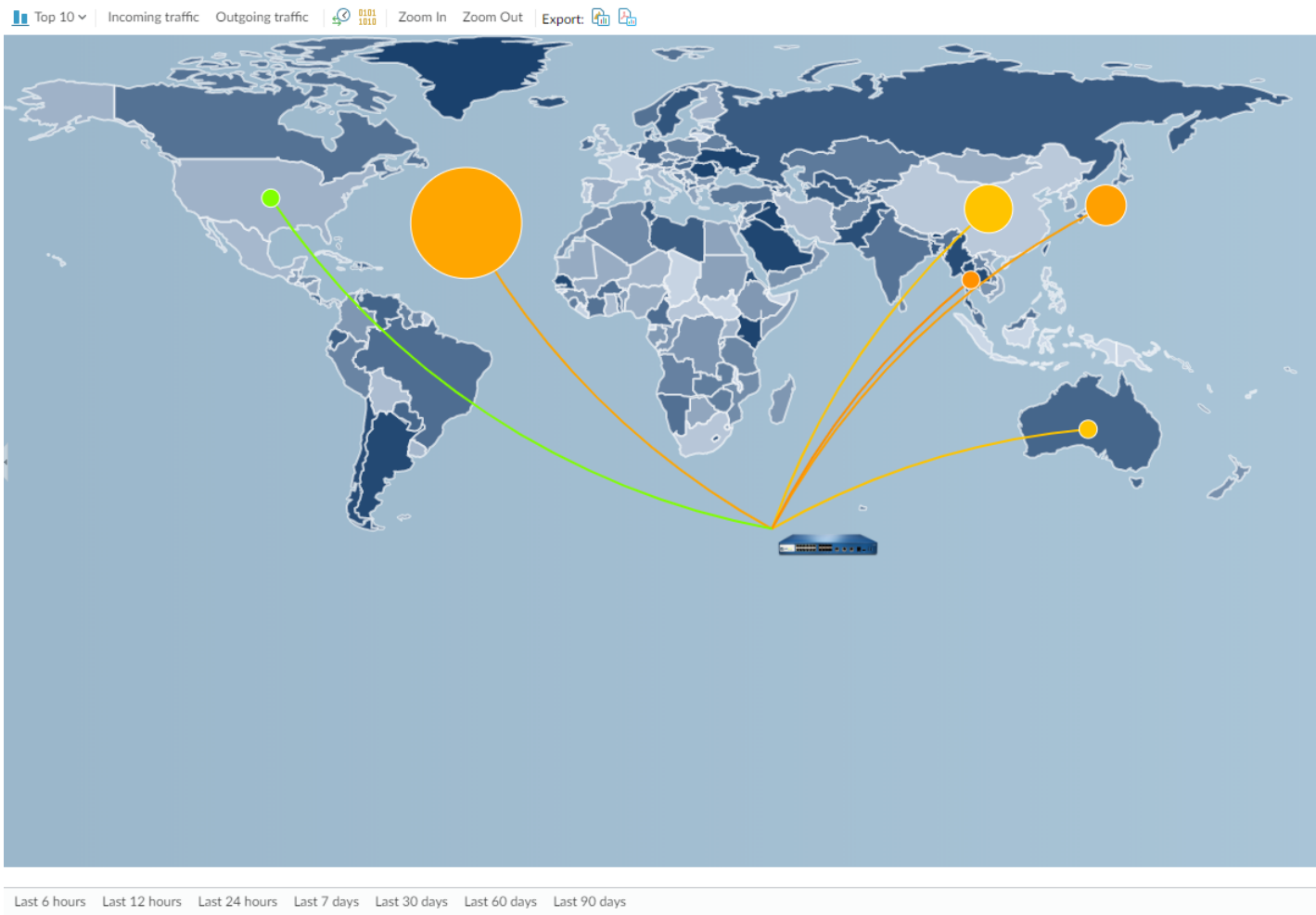
威胁监控报告选项	说明
顶栏	
Top 10	确定具有图表所包括的最高测量结果的记录数。
威胁	确定测量的项目的类型：威胁、威胁类别、源或目标。
Filter（筛选器）	应用筛选器以仅显示所选项目。
	确定是通过堆积柱形图还是通过堆积面积图来呈现信息。
导出	导出图表作为 .png 图像或 PDF。
底栏	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days	指定执行测量的时间段。

App Scope 威胁地图报告

威胁地图报告显示威胁（包括严重性）的地理视图。

App Scope 威胁地图报告

© 2019 Palo Alto Networks, Inc.



每个威胁类型均用颜色进行标记，如图表下面的图例所示。单击地图上的国家/地区可按需进行 **Zoom In**（放大）和 **Zoom Out**（缩小）。此报告包含以下选项。

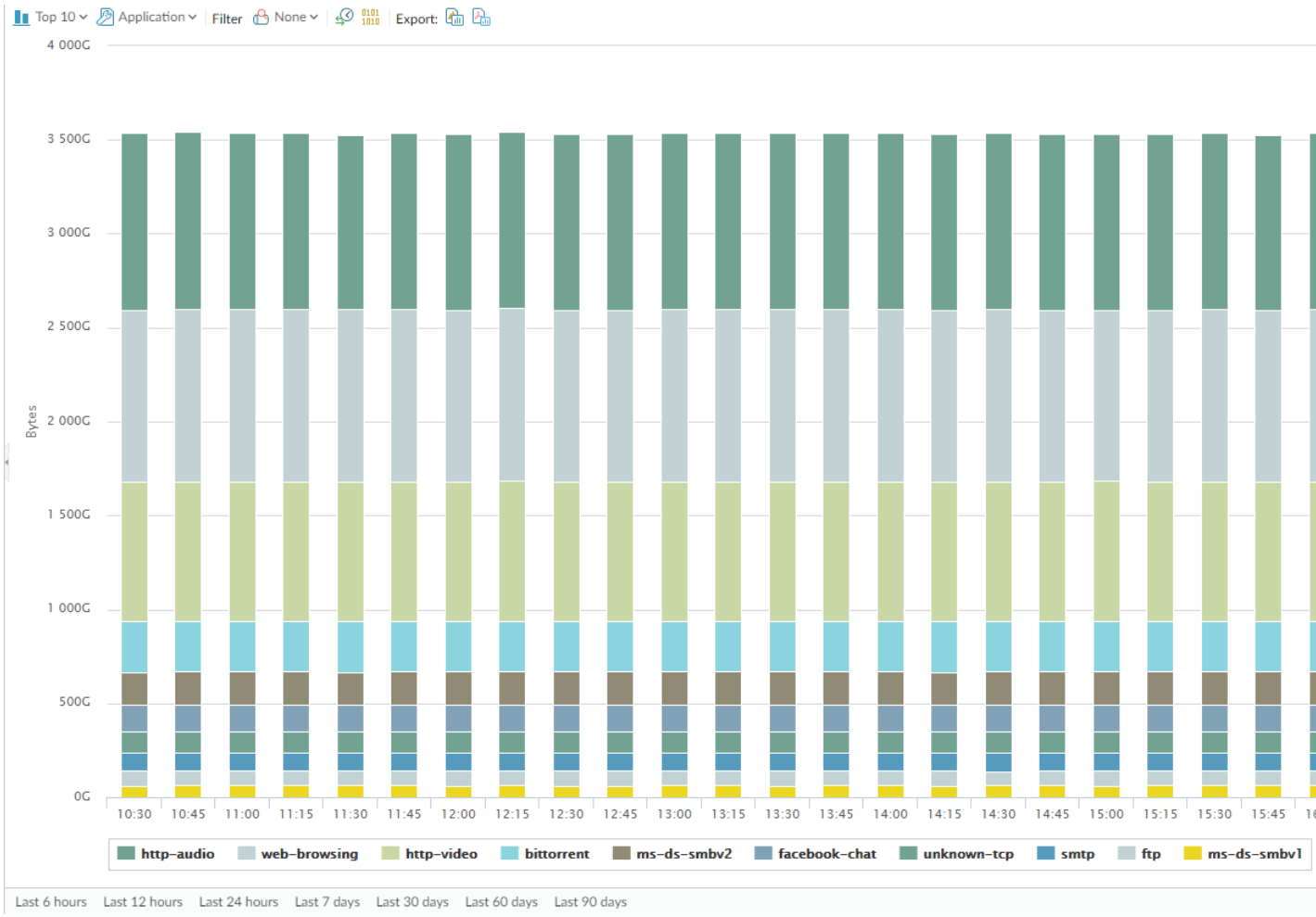
威胁地图报告选项	说明
顶栏	
Top 10	确定具有图表所包括的最高测量结果的记录数。
传入威胁	显示传入威胁。
传出威胁	显示传出威胁。
Filter（筛选器）	应用筛选器以仅显示所选项目。
放大和缩小	放大和缩小地图。
导出	导出图表作为 .png 图像或 PDF。
底栏	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	表示执行测量的时间段。

© 2019 Palo Alto Networks, Inc.

App Scope 网络监控报告

网络监控报告显示指定时间段内专用于不同网络功能的带宽。每个网络功能均用颜色进行标记，如图表下面的图例所示。例如，下图显示了过去 7 天基于会话信息的应用程序带宽。

App Scope 网络监控报告



此报告包含以下选项。

网络监控报告选项	说明
顶栏	
Top 10	确定具有图表所包括的最高测量结果的记录数。
应用程序	确定报告的项目的类型：应用程序、应用程序类别、源或目标。
Filter（筛选器）	应用筛选器以仅显示所选项目。**None**（无）显示所有条目。
计入对话与计入字节	确定是显示会话信息还是显示字节信息。
	确定是通过堆积柱形图还是通过堆积面积图来呈现信息。

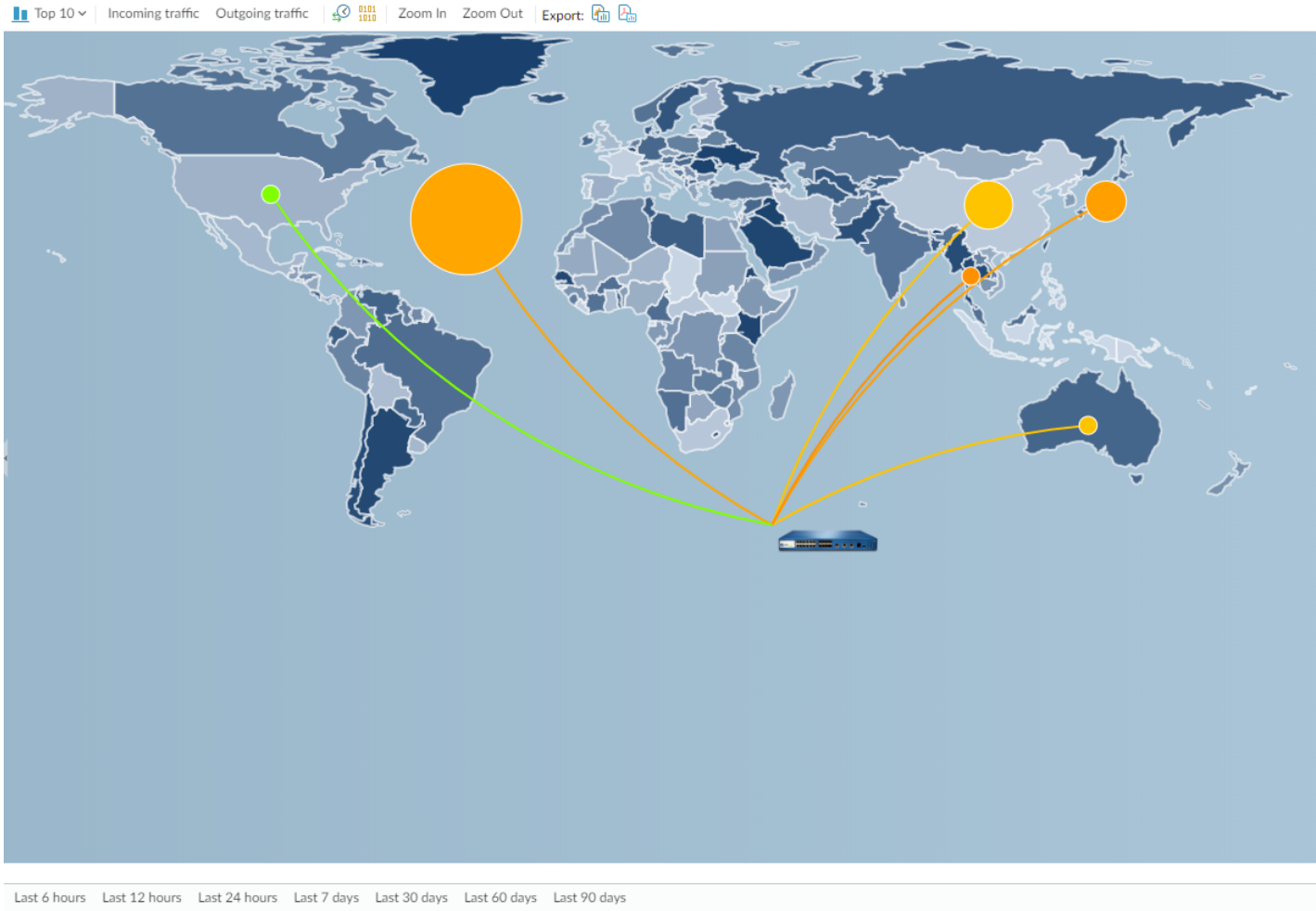
© 2019 Palo Alto Networks, Inc.

网络监控报告选项	说明
导出	导出图表作为 .png 图像或 PDF。
底栏	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	表示执行更改测量的时间段。

App Scope 流量地图报告

通信地图报告按照会话数或流量显示通信流的地理视图。

App Scope 流量地图报告



每个通信类型均用颜色进行标记，如图表下面的图例所示。此报告包含以下选项。

通信地图报告选项	说明
顶栏	
Top 10	确定具有图表所包括的最高测量结果的记录数。

© 2019 Palo Alto Networks, Inc.

通信地图报告选项	说明
传入通信	显示传入通信。
传出通信	显示传出通信。
计入对话与计入字节	确定是显示会话信息还是显示字节信息。
放大和缩小	放大和缩小地图。
导出	导出图表作为 .png 图像或 PDF。
底栏	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	表示执行更改测量的时间段。

© 2019 Palo Alto Networks, Inc.

监视 > 会话浏览器

选择 **Monitor**（监控） > **Session Browser**（会话浏览器）可浏览并筛选当前在防火墙上运行的会话。有关此页面的过滤选项的信息，请参阅日志操作。

© 2019 Palo Alto Networks, Inc.

Monitor（监控）> Block IP List（阻止 IP 列表）

您可以配置防火墙以多种方式将 IP 地址放在阻止列表中，包括下列方式：

- 通过 Action（操作）将 DoS 保护策略规则配置为 **Protect**（保护），并将分类 DoS 保护配置文件应用到规则。该配置文件包括 Block Duration（阻止期限）。
- 通过 Action（操作）将包含使用规则的漏洞保护配置文件的安全策略规则配置为 **Block IP**（阻止 **IP**），并将规则应用到区域。

PA-3200 系列、PA-5200 系列和 PA-7000 系列防火墙支持阻止 IP 列表。

您想了解什么内容？	请参阅：
阻止 IP 列表字段指示什么？	阻止 IP 列表条目
如何过滤、导航或删除阻止 IP 列表条目？	查看或删除阻止 IP 列表条目
了解更多？	设置防病毒软件、防间谍软件和漏洞保护 DoS 保护新会话不受泛滥攻击 监控阻止 IP 列表

阻止 IP 列表条目

- **Monitor**（监控）> **BlockIPList**

下表说明了防火墙阻止的源 IP 地址的阻止列表条目。

字段	说明
阻止时间	IP 地址进入阻止 IP 列表的的月/日和时:分:秒。
类型	阻止操作的类型：是硬件 (hw) 还是软件 (sw) 阻止 IP 地址。 配置 DoS 保护策略或安全策略使用漏洞保护配置文件阻止与源 IPv4 地址的连接时，防火墙在这些数据包使用 CPU 或数据包缓冲资源之前自动阻止硬件流量。如果攻击流量超过硬件的阻止能力，则防火墙会使用软件阻止流量。
源 IP 地址	防火墙阻止的数据包的源 IP 地址。
入口区域	分配给数据包进入防火墙的接口的安全区域。
剩余时间	IP 地址在阻止 IP 列表中的剩余秒数。
阻止源	分类 DoS 保护配置文件的名称或在其中指定阻止 IP 操作的漏洞保护对象名称。
阻止 IP 地址总数：x 与 y 之比（已使用 z%）	阻止 IP 地址数 (x) 与防火墙支持的阻止 IP 地址数 (y) 之比，即使用的阻止 IP 地址的相应百分比 (z)。

© 2019 Palo Alto Networks, Inc.

查看或删除阻止 IP 列表条目

浏览阻止 IP 列表条目，查看详细信息，并根据需要删除条目。

查看或删除阻止 IP 列表条目	
搜索特定的阻止 IP 列表信息。	选择列中的值，由此在 **Filters**（过滤器）字段中输入过滤器，并单击右侧箭头以开始具有该值的条目的搜索。 单击 X 可删除过滤器。
超出当前屏幕查看阻止 IP 列表条目	在 **Page**（页面）字段输入页码或单击单个箭头来查看条目的 Next Page（下一页）或 Previous Page（上一页）。单击双箭头以查看条目的 Last Page（最后一页）或 First Page（第一页）。
查看有关阻止 IP 列表上的 IP 地址的详细信息。	单击条目的源 IP 地址，该地址使用关于该地址的信息链接到 网络解决方案 Whois。
删除阻止 IP 列表条目	选择条目，然后单击 **Delete**（删除）。 通过 *Web* 界面仅能删除硬件条目。但是，通过 *CLI* 可删除硬件和软件条目。
清除整个阻止 IP 列表	单击 **Clear All**（全部清除）永久地删除所有条目，这意味着不再阻止那些数据包。 通过 *Web* 界面仅能清除硬件条目的阻止 *IP* 列表。但是，通过 *CLI* 可清除硬件和软件条目。

© 2019 Palo Alto Networks, Inc.

监视 > Botnet

Botnet 报告功能可让您使用基于行为的机制来识别网络中可能感染恶意软件和 Botnet 的主机。该报告会为每个主机指定从 1 到 5 的置信度，以指明存在 Botnet 感染的可能性，其中 5 表示最大可能性。在调度报告或即期运行报告之前，必须配置其将通信类型标识为可疑。有关详细信息，请参阅《PAN-OS® 管理员指南》中的解读 Botnet 报告输出。

- Botnet 报告设置
- Botnet 配置设置

Botnet 报告设置

- 监视 > Botnet > 报告设置

生成 Botnet 报告之前，您必须指定表明潜在 Botnet 活动的通信类型（请参阅配置 Botnet 报告）。要调度每日报告或即期运行该报告，请单击 **Report Setting**（报告设置），然后填写以下字段。要导出报告，请将其选定，然后选择 **Export to PDF**（导出为 **PDF**）、**Export to CSV**（导出为 **CSV**）或 **Export to XML**（导出为 **XML**）。

Botnet 报告设置	说明
测试运行时间框架	选择报告的时间间隔 — **Last 24 Hours**（最后 **24** 小时（默认））或 **Last Calendar Day**（最后一个日历天）。
立即运行	单击 **Run Now**（立即运行）可通过手动方式立即生成报告。该报告将显示在 Botnet Report（Botnet 报告）对话框内的新选项卡中。
行数	指定报告中显示的行数（默认为 100）。
已计划	选中此选项可每天自动生成报告。默认情况下，已启用此选项。
查询生成器	（可选）**Add**（添加）到查询生成器可按属性（如源/目标 IP 地址、用户或区域）筛选报告输出。例如，如果确定由 IP 地址“192.0.2.0”发起的通信中不含潜在 Botnet 活动，即可将 `not (addr.src in 192.0.2.0)` 添加为查询，以从报告输出中排除该主机。 • **Connector**（连接符）— 选择逻辑连接符（**and** 或 **or**）。如果选择 **Negate**（求反），则报告会排除查询指定的主机。 • **Attribute**（属性）— 选择与防火墙就 Botnet 活动进行评估的主机相关的区域、地址或用户。 • **Operator**（运算符）— 选择使 **Attribute**（属性）与 **Value**（值）相关的运算符。 • **Value**（值）— 输入要匹配的查询的值。

Botnet 配置设置

- Monitor（监控）> Botnet > Configuration（配置）

如需指定表明潜在 Botnet 活动的通信类型，请单击 **Botnet** 页面右侧的 **Configuration**（配置），然后填写以下字段。配置报告后，您可即期运行或调度其每天运行（请参阅 Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要））。

© 2019 Palo Alto Networks, Inc.

默认的 *Botnet* 报告配置是最佳的。如果您认为默认值可标识误报，则创建一个支持票据，这样，*Palo Alto Networks* 可对值进行重新评估。

Botnet 配置设置	说明
HTTP 通信	**Enable**（启用）并定义报告将包括的每种类型的 HTTP 流量的 **Count**（计数）。输入的 **Count**（计数）值为每种通信类型必须发生的最小事件数，其必要性在于须使报告可列出带有更高置信度（即存在 Botnet 感染的可能性更高）的关联主机。如果事件次数小于 **Count**（计数），报告将会显示较低的置信度评分，而对于某些流量类型，则不会显示主机的条目。 • **Malware URL visit**（恶意软件 **URL** 访问）（范围为 2-1000，默认为 5）— 根据恶意软件和 Botnet URL 筛选类别来识别与已知恶意软件 URL 进行通信的用户。 • **Use of dynamic DNS**（动态 **DNS** 的使用）（范围为 2–1000，默认为 5）— 查找可能指示恶意软件、Botnet 通信或渗透代码工具包的动态 DNS 查询通信。一般而言，使用动态 DNS 域存在很高的风险。恶意软件通常会使用动态 DNS 来避免 IP 地址阻止列表。建议使用 URL 过滤阻止此类通信。 • **Browsing to IP domains**（浏览到 **IP** 域）（范围为 2-1000，默认为 10）— 识别浏览到 IP 域而非 URL 的用户。 • **Browsing to recently registered domains**（浏览到最近注册的域）（范围为 2-1000，默认为 5）— 查找流向在过去 30 天内注册的域的流量。攻击者、恶意软件和渗透代码工具包通常会使用新注册的域。 • **Executable files from unknown sites**（来自未知站点的可执行文件）（范围为 2-1000，默认为 5）— 识别从未知 URL 下载的可执行文件。可执行文件是很多感染的一部分，且如果与其他类型的可疑通信相组合，可帮助您优先执行主机调查。
未知应用程序	定义阈值，以便确定报告是否包含与可疑的未知 TCP 或未知 UDP 应用程序相关的通信。 • **Sessions Per Hour**（每小时的会话数）（范围为 1–3600，默认为 10）— 报告将包含涉及每小时最大指定应用程序会话数的通信。 • **Destinations Per Hour**（每小时的目标数）（范围为 1–3600，默认为 10）— 报告将包含涉及每小时最大指定应用程序目标数的通信。 • **Minimum Bytes**（最小字节数）（范围为 1–200，默认为 50）— 报告将包含等于应用程序负载或超出指定大小的通信。 • **Minimum Bytes**（最大字节数）（范围为 1–200，默认为 100）— 报告将包含等于应用程序负载或小于指定大小的通信。
IRC	选中此选项可包含涉及 IRC 服务器的通信。

© 2019 Palo Alto Networks, Inc.

Monitor（监控）> PDF Reports（PDF 报告）

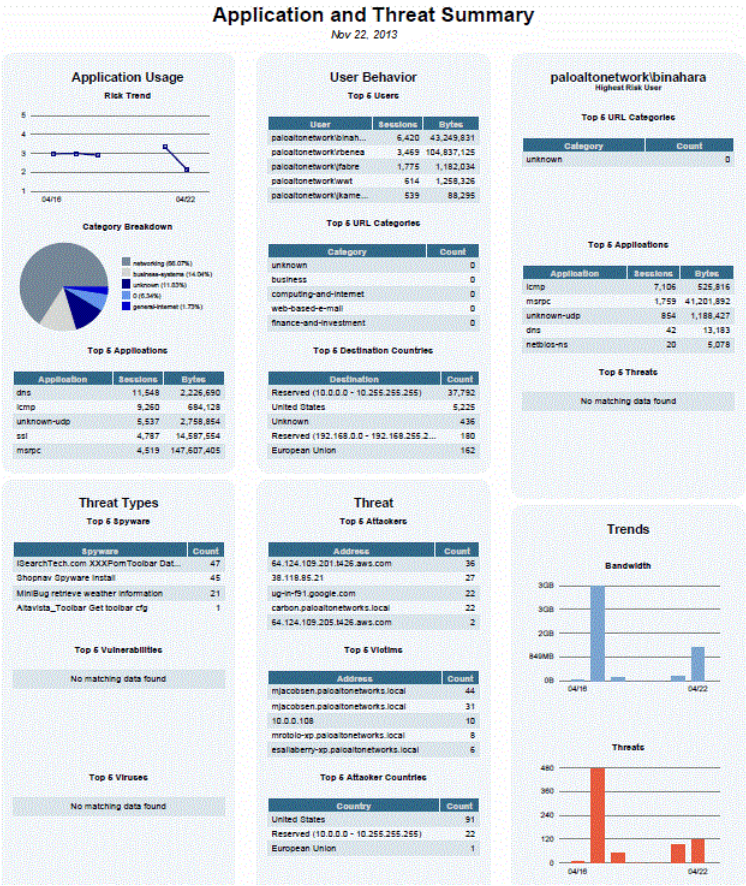
以下主题介绍 PDF 报告。

- Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要）
- 监视 > PDF 报告 > 用户活动报告
- Monitor（监控）> PDF Reports（PDF 报告）> SaaS Application Usage（SaaS 应用程序使用）
- Monitor（监控）> PDF Reports（PDF 报告）> Report Groups（报告组）
- Monitor（监控）> PDF Reports（PDF 报告）> Email Scheduler（电子邮件调度程序）

Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要）

PDF 摘要报告包含根据现有报告编译的信息，此信息基于每个类别中前 5 条数据（而不是前 50 条数据）。它们还包含在其他报告中没有的趋势图表。

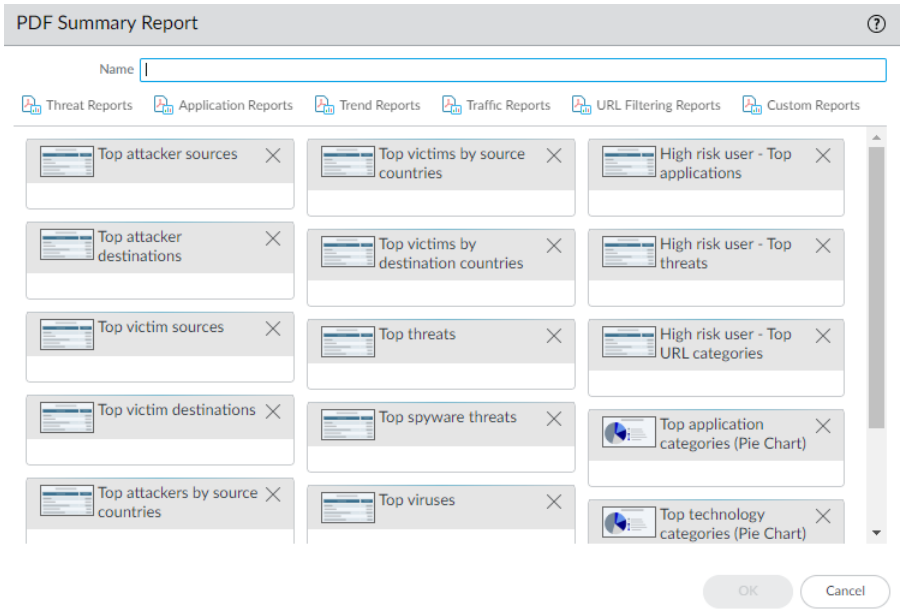
PDF 摘要报告



要创建 PDF 摘要报告，请单击 **Add**（添加）。**PDF Summary Report**（**PDF** 摘要报告）页面可以显示所有可用的报告元素。

管理 PDF 报告

© 2019 Palo Alto Networks, Inc.



可以使用下列一个或多个选项来设计报告：

- 如需将元素从报告中删除，请单击删除 ([X]) 或从合适的下拉列表中取消选择此项。
- 如需选择其他元素，请在合适的下拉列表中将其选中。
- 拖放元素可将其移到报告的其他区域。

最多允许 *18* 个报告元素。如果已配置 *18* 个报告元素，则必须在添加新元素前，删除现有元素。

要 **Save**（保存）报告，请输入报告名称，然后单击 **OK**（确定）。

要显示 PDF 报告，请选择 **Monitor**（监控）> **Reports**（报告），单击 **PDF Summary Report**（**PDF** 摘要报告）以选择报告，然后单击日历中的某天来下载当天的报告。

新的 *PDF* 摘要报告将不会出现，直到报告运行之后，这将在每 *24* 小时的上午 *2* 点自动发生。

监视 > PDF 报告 > 用户活动报告

使用此页面可以创建用于总结各个用户或用户组的活动情况的报告。单击 **Add**（添加），并指定以下信息：

用户/组活动报告设置	说明
姓名	输入名称以标识报告（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
类型	对于用户活动报告：选择用户并输入报告主题的用户的用户名或 **IP** 地址（IPv4 或 IPv6）。
	对于组活动报告：选择 **Group**（组），然后输入 **Group Name**（组名）。
其他筛选程序	选择 **Filter Builder**（筛选程序构建器）以创建用户/组活动报告的筛选程序。

© 2019 Palo Alto Networks, Inc.

用户/组活动报告设置	说明
时间期限	从下拉列表中选择报告的时间框架。
包括详细的浏览活动	（可选）选中此选项可在报告中包括详细的 URL 日志。 详细的浏览活动信息可能包含所选用户或用户组的大量日志（成千上万条日志），这将使报告变得非常大。

组活动报告不包括 *URL* 类别的浏览摘要；用户活动报告和组活动报告中的其他所有信息都是常见信息。

要按需运行报告，请单击 **Run Now**（立即运行）。要更改报告中显示的最大行数，请参阅记录和报告设置。

要保存报告，请单击确定。然后，您可以计划通过电子邮件传递的报告（Monitor（监控）> PDF Reports（PDF 报告）> Email Scheduler（电子件邮调度程序））。

添加日志筛选程序

构建用户活动和组活动报告的日志筛选程序以自定义报告。您可以根据应用程序、应用程序特征等条件来筛选活动报告。例如，如果您对没有认证的 SaaS 应用程序感兴趣，则可以基于此应用程序特征构建筛选程序。

添加日志筛选程序字段	说明
日志筛选程序文本框	编写希望应用于日志的筛选程序。您可以编写多个筛选程序。
连接器	给筛选程序添加一个附加筛选选项。选中 **Negate**（求反）框不会将连接器应用于您所编写的筛选程序。
属性	选择希望从菜单中附加的属性。
运算符	选择属性是否应等于值。
值	设置属性的值。如果可用，可以使用包含可能值的下拉菜单。

选择 **Apply**（应用）以将构建的筛选程序应用于用户活动或组活动报告。

Monitor（监控）> PDF Reports（PDF 报告）> SaaS Application Usage（SaaS 应用程序使用）

使用此页面生成 SaaS 应用程序使用报告，其中汇总了与遍历网络的 SaaS 应用程序关联的安全风险。此预定义报告显示了已批准应用程序和未批准应用程序的比较信息，总结了具有不利托管特征的高风险 SaaS 应用程序，并通过在详细页面上列出每个类别的热门应用程序来突出显示应用程序的活动、使用情况和合规性。您可以使用此详细风险信息来对要在网络上允许或阻止的 SaaS 应用程序实施策略。

为了生成准确而翔实的报告，您必须在网络上标记已批准应用程序（请参阅生成 SaaS 应用程序使用报告）。防火墙和 Panorama 会将任何没有此预定义标记的应用程序视为其使用不受网络约束的应用程序。有

© 2019 Palo Alto Networks, Inc.

必要了解在网络上较为普遍的约束和未约束应用程序，因为未约束 SaaS 应用程序可能会对信息安全造成威胁，您不可允许其使用您的网络，以免造成专用数据和敏感性数据的丢失。

确保在所有防火墙或设备组中始终标记应用程序。如果同一个应用程序在一个虚拟系统中标记为受约束，而未在其他虚拟系统中进行同样的标记，或在 *Panorama* 上，如果一个应用程序在父设备组中标记为未约束，而在子设备组中标记为约束（或反之），则 *SaaS* 应用程序使用报告将产生重叠的报告结果。

在 ACC 上，将 *Application View*（应用程序视图）设置为 *By Sanctioned State*（按批准状态）可直观识别在虚拟系统或设备组中具有不同批准状态的应用程序。绿色表示批准的应用程序，蓝色表示未批准的应用程序，黄色表示在不同虚拟系统或设备组中拥有不同批准状态的应用程序。

要配置此报告，请单击 **Add**（添加），然后指定以下信息：

SaaS 应用程序使用报告设置	说明
姓名	输入名称以标识报告（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
时间期限	从下拉列表中选择报告的时间框架。报告包括当天（生成报告的当天）的数据。
包括日志，来自	从下拉列表中，选择是否在所选用户组、所选区域上或为在防火墙或 Panorama 上配置的所有用户组和区域生成报告。 • **For a selected user group**（对于所选用户组）— 选择防火墙或 Panorama 将过滤日志的 **User Group**（用户组）。 • **For a selected user group**（对于所选区域）— 选择防火墙或 Panorama 将过滤日志的 **Zone**（区域）。 • **For all user groups and zones**（对于所有用户组和区域）— 可以报告所有组或最多选择要查看的 25 个用户组。如果您拥有的组超过 25 个，则防火墙或 Panorama 将显示报告中的前 25 个组，并将剩余用户组分配给 Others（其他）组。
包括报告中的用户组信息 （如果选择在 **Selected User Group**（所选用户组）上生成报告，则不可用。）	此选项将过滤要包含在报告中的用户组的日志。选择 **manage groups**（管理组）或 **manage groups for the selected zone**（管理所选区域的组）链接，最多可以选择要查看的 25 个用户组。 为所选区域中的特定用户组生成报告时，会将不属于任何所选组的成员的用户分配给名为 Others（其他）的用户组。
用户组	选择要为其生成报告的用户组。此选项只有在 **Include logs from**（包括日志，来自）下拉列表中选择 **Selected User Group**（所选用户组）时才会显示。
区域	选择要为其生成报告的区域。此选项只有在 **Include logs from**（包括日志，来自）下拉列表中选择 **Selected Zone**（所选区域）时才会显示。 然后，您可以选择包括报告中的用户组信息。
在报告中包括详细的应用程序类别信息	SaaS 应用程序使用 PDF 报告由两部分构成。默认情况下，会同时生成此报告所含的两个部分。报告第一部分（十页）主要针对报告期间在网络上使用的 SaaS 应用程序。 对于报告第一部分列出的每一个应用程序子类别，如果不需要包含有 SaaS 和非 SaaS 应用程序相关详情的第二部分报告，请取消选中此选项。报告第二部分包括

© 2019 Palo Alto Networks, Inc.

SaaS 应用程序使用报告设置	说明
	每个子类别中顶部应用程序的名称，以及用户、用户组、文件、传输字节、应用程序威胁的相关信息。 如不包含详细信息，则此报告仅有十页。
将报告中的最大子类别数限制为	选择是否要在 SaaS 应用程序使用报告中使用所有应用程序子类别，或是否将最大数限制为 10、15、20 或 25 个子类别。 如果减少最大子类别数，详细报告就会变短，因为您限制了报告中包含的 SaaS 和非 SaaS 应用程序活动信息。

单击 **Run Now**（立即运行）可即期生成报告。

您可以根据需要生成此报告，也可以对其进行调度以使其每天、每周或每月运行一次。要调度报告，请参阅调度通过电子邮件传递的报告。

在 PA-220 和 PA-220R 系列防火墙中，SaaS 应用程序使用报告不会在电子邮件中以 PDF 附件的形式发送。而是通过电子邮件为您提供一个链接，您可用其在 Web 浏览器中打开报告。

了解有关报告的更多信息，请参阅管理报告。

Monitor（监控）> PDF Reports（PDF 报告）> Report Groups（报告组）

报告组允许您创建报告集合，系统可以对此集合进行编译并将其作为单个聚合 PDF 报告来发送，该报告中包含可选的标题页和所有成员报告。

报告组设置	说明
姓名	输入名称以标识报告组（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
标题页	选中此选项可在报告中包括标题页。
标题	输入显示为报告标题的名称。
报告选择/小部件	对于要包含在组中的每个报告，请选择左列中的报告，然后将其 **Add**（添加）到右列。您可以选择以下报告类型： • 预定义报告 • 自定义报告 • PDF 摘要报告 • Csv • 日志视图 — 每次创建自定义报告时，防火墙都会自动创建名称相同的日志视图报告。日志视图报告显示防火墙用于构建自定义报告内容的日志。要包括日志视图数据，创建报告组时，添加 **Custom Reports**（自定义报告），然后添加匹配的 **Log View**（日志视图）报告。为报告组生成的聚合报告显示自定义报告数据，后跟日志数据。 保存报告组后，Report Groups（报告组）页面的 Widgets（小部件）列会列出已添加到组的报告。

© 2019 Palo Alto Networks, Inc.

要使用报告组，请参阅 Monitor（监控）> PDF Reports（PDF 报告）> Email Scheduler（电子邮件调度程序）。

Monitor（监控）> PDF Reports（PDF 报告）> Email Scheduler（电子邮件调度程序）

使用电子邮件计划程序可以计划通过电子邮件传递的报告。在添加计划之前，必须定义报告组和电子邮件配置文件。请参阅 Monitor（监控）> PDF Reports（PDF 报告）> Report Groups（报告组）和 Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）。

计划的报告在 2:00 AM 开始运行，而且电子邮件转发发生在所有计划的报告已完成运行之后。

电子邮件计划程序设置	说明
姓名	输入名称以标识调度（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
报告组	选择要高度的报告组 (Monitor（监控）> PDF Reports（DF 报告）> Report Groups（报告组））或 SaaS 应用程序使用报告（Monitor（监控）> PDF Reports（PDF 报告）> SaaS Application Usage（SaaS 应用程序使用））。
电子邮件配置文件	选择定义电子邮件设置的配置文件。有关定义电子邮件配置文件的信息，请参阅 Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）。
重复	选择生成并发送报告的频率。
替代电子邮件地址	输入可选电子邮件地址，替代在电子邮件配置文件中指定的收件人。
发送测试电子邮件	单击此选项可将测试电子邮件发送到在选定 **Email Profile**（电子邮件配置文件）中定义的电子邮件地址。

© 2019 Palo Alto Networks, Inc.

Monitor（监控）> Manage Custom Reports（管理自定义报告）

您可以创建自定义报告以按需或按计划运行（每天晚上）。对于预定义报告，请选择 **Monitor**（监控）> **Reports**（报告）。

防火墙生成计划的自定义报告之后，如果您修改其配置以更改未来输出，则可能会使得该报告过去的结果无效。如果需要修改计划报告配置，最佳实践是创建一个新报告。

Add（添加）自定义报告以创建新的报告。要使报告基于现有模板，请单击 **Load Template**（加载模板）并选择模板。要根据需要生成报告（而不是或除 **Scheduled**（计划）时间之外，请单击 **Run Now**（立即运行）。指定以下设置以定义报告。

自定义报告设置	说明
姓名	输入名称以标识报告（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入自定义报告的说明。
数据库	选择要用作报告的数据源的数据库。
已计划	选中此选项可每晚运行报告。然后，通过选择 **Monitor**（监控）> **Reports**（报告）可以使报告变为可用。
Time frame	选择固定时间框架，或选择自定义以指定日期和时间范围。
排序关键字	选择用于组织报告的排序选项，包括要包括在报告中的信息量。可用选项取决于数据库的选择。
分组依据	选择用于组织报告的分组选项，包括要包括在报告中的信息量。可用选项取决于数据库的选择。
列	选择 Available Columns（可用列）可包含自定义报告，并将其添加 (⊕) 到 Selected Columns（选定列）。选择 **Up**（上）、**Down**（下）、**Top**（置顶）和 **Bottom**（置底）可对选定列进行重新排序。必要时，可选中之前选择的列，并将其删除 (⊖)。
查询生成器	要构建报告查询，请指定以下项，并单击添加。根据需要重复操作以构造完整查询。 • **Connector**（连接符）— 选择位于所添加表达式之前的连接符（**and** 或 **or**）。 • **Negate**（求反）— 选中此选项可将查询解释为否定。在前面的示例中，否定选项将产生不在过去 24 小时内或不来自不可信区域的匹配条目。 • 属性- 选择数据元素。可用选项取决于数据库的选择。 • 运算符- 选择用于确定属性是否应用的标准（比如 = ）。可用选项取决于数据库的选择。 • 值- 指定要匹配的属性值。

© 2019 Palo Alto Networks, Inc.

有关详细信息，请参阅生成自定义报告。

© 2019 Palo Alto Networks, Inc.

监测 > 报告

防火墙会提供前一天或前一周中选定日期的通信统计信息的各种“前 50”报告。

要查看报告，请展开页面右侧的报告类别（如自定义报告），然后选择报告名称。该页面列出了各个部分中的报告。您可以查看所选时间段的每个报告的信息。

默认情况下，防火墙显示上一个日历日的所有报告。要查看其他日期的报告，请在页面右下角的日历中选择报告生成日期。

要查看防火墙以外系统的报告，请选择导出选项：

- 导出至 **PDF**
- 导出为 **CSV**
- 导出为 **XML**

© 2019 Palo Alto Networks, Inc.

策略

以下主题介绍防火墙策略类型、如何移动或克隆策略，还介绍策略设置：

> 策略类型
> 移动或克隆策略规则
> 审核注释存档
> 规则使用点击数查询
> Policies（策略）> Security（安全）
> Policies（策略）> NAT
> Policies（策略）> QoS
> Policies（策略）> Policy Based Forwarding（基于策略的转发）
> Policies（策略）> Decryption（解密）
> Policies（策略）> Tunnel Inspection（隧道检测）
> Policies（策略）> Application Override（应用程序替代）
> Policies（策略）> Authentication（身份验证）
> Policies（策略）> DoS Protection（DoS 保护）
> Policies（策略）> SD-WAN

策略类型

通过强制执行规则和自动执行操作，策略可让您控制防火墙操作。防火墙支持以下策略类型：

- 基本安全策略，用于根据应用程序、源和目标区域和地址以及（可选）服务（端口和协议）阻止或允许网络会话。区域标识发送或接收通信的物理接口或逻辑接口。请参阅 Policies（策略）> Security（安全）。
- 网络地址转换 (NAT) 策略，用于转换地址和端口。请参阅 Policies（策略）> NAT。
- 服务质量 (QoS) 策略，用于确定当通信通过启用了 QoS 的接口时如何对通信进行分类处理。请参阅 Policies（策略）> QoS。
- 基于策略的转发策略，用于替代路由表，和指定流量的 egress 接口。请参阅 Policies（策略）> Policy Based Forwarding（基于策略的转发）。
- 解密策略，用于指定安全策略的通信解密。每个策略均可以为要解密的通信指定 URL 类别。SSH 解密用于标识和控制除 SSH 外壳访问以外的 SSH 隧道。请参阅 Policies（策略）> Decryption（解密）。
- 隧道检测策略，用于对隧道流量执行安全、DoS 保护和 QoS 策略，以及查看隧道活动。请参阅 Policies（策略）> Tunnel Inspection（隧道检测）。
- 替代策略，用于替代由防火墙提供的应用程序定义。请参阅 Policies（策略）> Application Override（应用程序替代）。
- 身份验证策略，用于定义访问网络资源的最终用户的身份验证。请参阅 Policies（策略）> Authentication（身份验证）。
- 拒绝服务 (DoS) 策略，用于防御 DoS 攻击，并在响应规则匹配时采取保护措施。请参阅 Policies（策略）> DoS Protection（DoS 保护）。
- SD-WAN 策略，用于在链路路径运行状况下降到低于批准、配置的运行状况指标时，确定源和目标区域之间的链路路径管理。请参阅 Policies（策略）> SD-WAN。

从 Panorama™ 推送的共享策略在防火墙 Web 界面上使用橙色显示。您只能在 Panorama上编辑这些共享策略；不能在防火墙上编辑这些策略。

将规则库视为组 查看规则库中使用的所有标记组。在具有大量规则的规则库中，将规则库视为组可简化显示，只需在保留已建立的规则层次结构的同时在每个组中提供标记、颜色代码和规则数即可。

© 2019 Palo Alto Networks, Inc.

移动或克隆策略规则

在移动或克隆策略时，可以为您有其访问权限的策略分配 **Destination**（目标）（防火墙上的虚拟系统或 Panorama 上的设备组），包括共享位置。

要移动策略规则，请在 **Policies**（策略）选项卡中选择规则，单击 **Move**（移动），选择 **Move to other vsys**（移动到其他虚拟系统）（仅限防火墙）或 **Move to different rulebase or device group**（移动到不同的规则库或设备组）（仅限 Panorama），在随后的表格中指定字段，然后单击 **OK**（确定）。

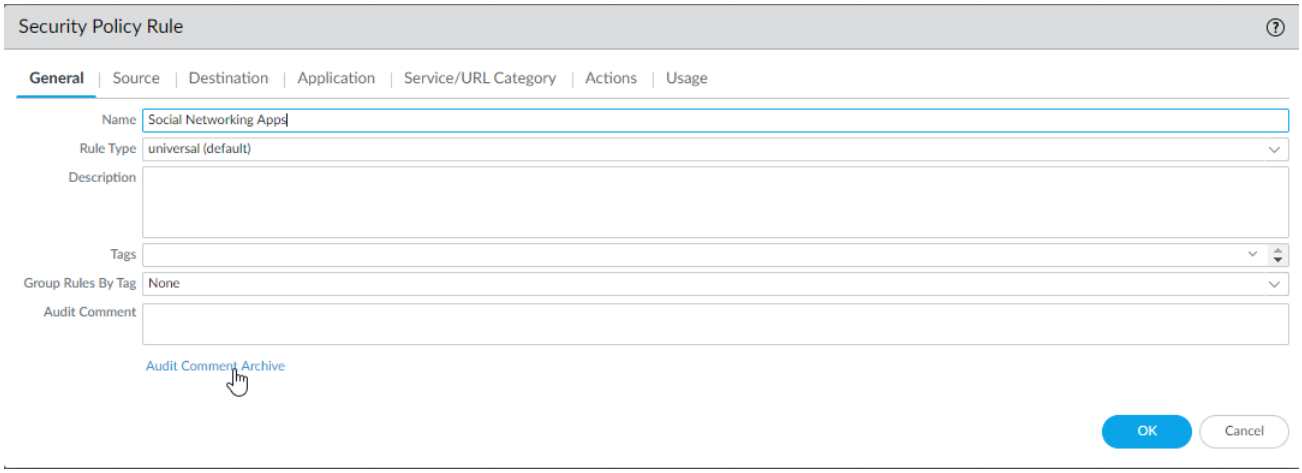
如需克隆策略规则，请在 **Policies**（策略）选项卡中选择规则，单击 **Clone**（克隆），在随后的表格中指定字段，然后单击 **OK**（确定）。

移动/克隆设置	说明
所选规则	显示为操作选择的策略规则的名称和当前位置（虚拟系统或设备组）。
目标	为策略或对象选择新位置：虚拟系统、设备组或共享位置。默认值是在策略或对象选项卡中选择的虚拟系统或设备组。
规则顺序	选择相对于其他规则的规则位置： • 移至顶部 — 此规则将位于所有其他规则的前面。 • 移至底部 — 此规则将位于所有其他规则的后面。 • 前导规则 — 在相邻下拉列表中，选择随后的规则。 • 后继规则 — 在相邻下拉列表中，选择前面的规则。
输出验证中第一个检测到的错误	选中此选项（默认选中）可让防火墙或 Panorama 显示其找到的第一个错误，并停止检查更多错误。例如，如果目标不包含要移动的策略规则所引用的对象，则会出错。如果取消选中此选项，防火墙或 Panorama 会在显示错误前，找到所有错误。

© 2019 Palo Alto Networks, Inc.

审核注释存档

选择 **Audit Comment Archive**（审核注释存档）以查看选中规则的审核注释历史记录、配置日志和规则更改历史记录。



- 审核注释
- 配置日志（在注释之间）
- 规则更改

审核注释

查看所选策略规则的 **Audit Comment**（审核注释）历史记录。应用并保存筛选程序，从而快速标识特定审核注释，并以 CSV 格式导出所显示的审核注释。

字段	说明
提交时间	提交审核注释的时间。
审核注释	审核注释的内容。
管理员	添加或更改审核注释的用户。
配置版本	配置版本的版本。0 表示第一次创建策略规则并将其提交给 Panorama。

配置日志（在注释之间）

查看注释之间选中策略规则生成的配置日志。应用并保存筛选条件，从而快速标识特定配置日志，并以 CSV 格式导出所显示的配置日志。

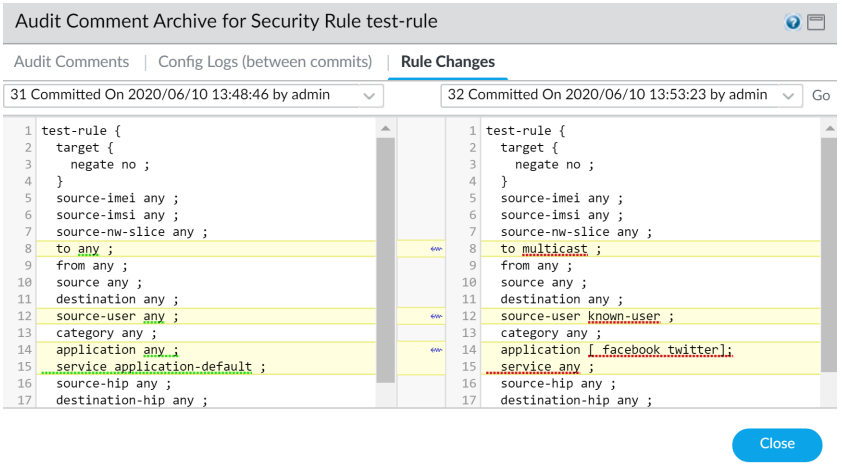
字段	说明
时间	提交审核注释的时间。
管理员	审核注释的内容。

© 2019 Palo Alto Networks, Inc.

字段	说明
命令	执行的命令类型。
在更改之前	在更改之前的规则信息。例如，如果重命名规则，则会显示以前的名称。
在更改之后	在更改之后的规则信息。例如，如果重命名规则，则会显示新名称。
设备名称	在更改审核注释之前的设备名称。

规则更改

查看并比较选中策略规则的配置版本，以分析发生的更改。在下拉列表中，选择想要进行比较的两个策略规则配置版本。



© 2019 Palo Alto Networks, Inc.

规则使用点击数查询

- **Policies**（策略）> **Rule Usage**（规则使用情况）

使用规则使用查询过滤指定时间段内选中的规则库。通过规则使用查询，您可以快速过滤您的策略规则库以标识未使用的规则，从而进行删除，这样，您可以减少攻击者的开放入口点。点击 **PDF/CSV** 以导出 PDF 或 CSV 格式的过滤规则。要使用规则使用点击数查询，必须启用 **Policy Rule Hit Count**（策略规则点击数）设置（Device（设备）> Setup（设置）> Management（管理））。

默认情况下，当您在策略规则库中查询规则使用情况时，将显示 **Name**（名称）、**Location**（位置）、**Created**（已创建）、**Modified**（已修改）和 **Rule Usage**（规则使用情况）列。您可以添加多个列以查看关于策略规则的其他信息。

任务	说明
点击数	
时间段	指示查询所选规则库的时间段。从预定义时间范围选择，或是设置 **Custom**（自定义）时间段。
使用情况	选择要查询的规则使用情况：**Any**（任何）、**Unused**（未使用）、**Used**（已使用）或 **Partially Used**（部分使用）（仅限 Panorama）。
从	（仅限自定义时间段）选择要查询策略规则库的日期和时间。
排除最后_天的规则重置	选中此选项后，可排除用户在指定天数内手动重置的任何规则。
操作	
删除	删除所选的一个或多个策略规则。
启用	启用所选的一个或多个策略规则（若已禁用）。
禁用	禁用所选的一个或多个策略规则。
PDF/CSV	导出当前以 PDF 或 CSV 格式显示、经过筛选的策略规则。
重置规则命中次数计数器	重置 **Selected rules**（所选规则）或当前显示的经过筛选的 **All rules**（所有规则）的规则使用数据。
标记	将一个或多个组标记应用于所选的一个或多个策略规则。若要标记策略规则，组标记必须已经存在。
取消标记	取消所选的一个或多个策略规则中的组标记。

规则使用点击数查询的设备规则使用情况

在查看 Panorama 管理服务器策略规则的规则使用情况时，可以查看设备和虚拟系统的规则使用情况。**Reset Rule Hit Counter**（重置规则点击数）可重置点击数、第一次点击和最后一次点击。

点击 **PDF/CSV** 以导出 PDF 或 CSV 格式的过滤规则。

© 2019 Palo Alto Networks, Inc.

字段	说明
设备组	设备或虚拟系统所属的设备组。
设备名称/虚拟系统	设备组或虚拟系统的名称。
点击数	策略规则的流量匹配总数。
最后一次点击	最后一次流量与策略规则匹配的日期和时间。
第一次点击	第一次流量与策略规则匹配的日期和时间。
收到的最后更新	最后一次从 Panorama 管理服务器设备收到规则使用信息的日期和时间.
创建于	策略规则创建的日期和时间。
已修改	最后一次修改策略规则的日期和时间。如果尚未修改策略规则，则该列为空。
状态	设备的连接状态：`Connected` 或 `Disconnected`。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> Security（安全）

安全策略规则引用安全区域，可让您根据应用程序、用户或用户组以及服务（端口和协议）允许、限制和跟踪网络上的流量。默认情况下，防火墙包含一个名为 *rule1* 的安全规则，它允许从信任区域到不信任区域的所有流量。

您想了解什么内容？	请参阅：
安全策略是什么？	安全策略概述 对于 Panorama，请参阅移动或克隆策略规则
哪些字段可用于创建安全策略规则？	安全策略规则中的构建块
我要如何使用 Web 界面管理安全策略规则？	创建和管理策略 替代或恢复安全策略规则 应用程序和使用情况 安全策略优化器
了解更多？	安全策略

安全策略概述

安全策略可让您强制执行规则并执行操作，根据需要可以是一般的，也可以是特定的。将针对传入通信按顺序对策略规则进行比较，并且因为将应用第一个与通信匹配的规则，所以特定性更强的规则必须位于一般性更强的规则前面。例如，如果所有其他与通信相关的设置均相同，则适用于单个应用程序的规则必须位于适用于所有应用程序的规则前面。

要确保最终用户在尝试访问您的网络资源时接受身份验证，防火墙需要在评估安全策略之前先评估身份验证策略。有关详细信息，请参阅 Policies（策略）> Authentication（身份验证）。

对于与任何用户定义的规则不匹配的流量，将应用默认规则。在安全规则库底部显示的默认规则是预定义的规则，用于允许所有区域内（在区域内部）流量和拒绝所有区域间（在区域之间）流量。尽管这些规则是预定义配置的一部分且默认为只读，但您可以 **Override**（覆盖）它们并更改数量有限的设置，包括标记、操作（允许或拒绝）、日志设置和安全策略。

界面包含以下定义安全策略规则的选项卡。

- **General**（常规）— 选择 **General**（常规）选项卡可以配置安全策略规则的名称和说明。
- **Source**（源）— 选择 **Source**（源）选项卡可以定义流量起源的源区域或源地址。
- **User**（用户）— 选择 **User**（用户）选项卡可以对单个用户或用户组强制实施策略。如果使用启用主机信息配置文件 (HIP) 的 GlobalProtect™，则还可以让策略基于 GlobalProtect 所收集的信息。例如，用户的访问级别可以通过 HIP 确定，该配置文件可将用户本地配置告知防火墙。HIP 信息可以用来根据正在主机上运行的安全程序、注册表值和许多其他检查（如主机是否已安装防病毒软件）进行粒度控制访问。
- **Destination**（目标）— 选择 **Destination**（目标）选项卡可以定义流量的目标区域或目标地址。
- **Application**（应用程序）— 选择 **Application**（应用程序）选项卡可以根据应用程序或应用程序组针对发生的操作制定策略。此外，管理员也可以使用现有的 App-ID™ 签名进行自定义，以检测专用应用程序或现有应用程序的特定属性。在 **Objects**（对象）> **Applications**（应用程序）中可定义自定义应用程序。
- **Service/URL Category**（服务/URL 类别）— 选择 **Service/URL Category**（服务/URL 类别）选项卡，可以指定特定 TCP 和/或 UDP 端口号或 URL 类别作为策略中的匹配标准。

© 2019 Palo Alto Networks, Inc.

- **Action**（操作）— 选择 **Action**（操作）选项卡，以根据与所定义的策略属性匹配的流量确定将执行的操作。
- **Target**（目标）—选择 **Target**（目标）选项卡，以指定用于安全策略规则的设备或标签。
- **Usage**（使用情况）— 选择**Usage**（使用情况） 选项卡可查看规则的使用情况，包括规则上显示的应用程序数、规则上出现最后一个新应用程序的时间、点击数数据、过去 30 天的流量、规则创建和最后一次编辑的时间。

安全策略规则中的构建块

- Policies（策略）> Security（安全）

以下部分介绍安全策略规则的各个组件。在创建安全策略规则时，可以配置下面介绍的选项。

安全规则的构建块	配置位置	说明
规则号	N/A	防火墙会自动对每个规则进行编号，并且规则的顺序会随着规则的移动而改变。在筛选规则以匹配特定筛选程序时，会将每个规则连同其在规则库中整组规则上下文中的编号及其在评估顺序中的位置一起显示。 Panorama 单独地对前导规则和后续规则进行编号。当 Panorama 将规则推送至受管防火墙时，规则编号将前导规则、防火墙规则和后续规则中的层次结构加入规则库并反映规则顺序及其评估顺序。
姓名	**General**（常规）	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
规则类型:		指定将规则应用于区域内部、区域之间还是两者的流量： • 通用（默认）- 将规则应用于指定源和目标区域中的所有匹配区域间和区域内流量。例如，如果您使用源区域 A 和 B 及目标区域 A 和 B 创建通用规则，则该规则将适用于区域 A 内部的所有流量、区域 B 内部的所有流量、从区域 A 至区域 B 以及从区域 B 至区域 A 的所有流量。 • 区域内 — 将规则应用于指定源区域内部的所有匹配流量（您不能为区域内规则指定目标区域）。例如，如果您将源区域设置为 A 和 B，则规则将适用于区域 A 和区域 B 内部的所有流量，但不适用于区域 A 和 B 之间的流量。 • 区域间 — 将规则应用于指定源区域和目标区域之间的所有匹配流量。例如，如果您将源区域设置为 A、B 和 C，并将目标区域设置为 A 和 B，则该规则将适用于从区域 A 至区域 B、从区域 B 至区域 A、从区域 C 至区域 A 以及从区域 C 至区域 B 的流量，但不适用于区域 A、B 或 C 内部的流量。
说明		输入策略的说明（最多 1024 个字符）。
标记		指定策略的标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“解密”和“不解密”等特

© 2019 Palo Alto Networks, Inc.

安全规则的构建块	配置位置	说明
		定关键字标记某些规则，或者将特定数据中心的名称用于和该位置关联的策略。 您还可以将标记添加到默认规则。
Source Zone（源区域）	源	**Add**（添加）源区域（默认为 **Any**（任何））。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅 Network（网络）> Zones（区域）。 多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。
Source Address（源地址）	源	**Add**（添加）源地址、地址组或地区（默认为 **Any**（任何））。从下拉列表中选择，或选择 **Address**（地址）对象、**Address Group**（地址组）或 **Regions**（地区）（在下拉列表的底部），以指定设置。Objects（对象）> Addresses（地址）和 Objects（对象）> Address Groups（地址组）用于分别描述“安全”策略规则支持的地址对象和地址组类型。 通过选择 **Negate**（求反）选项，可将规则应用于指定区域的源地址，但指定地址的除外。
源用户	源	根据策略 **Add**（添加）源用户或用户组： • **any**（任何）— 无论用户数据怎样，包括任何流量。 • **pre-logon**（预登录）— 包括使用 GlobalProtect 连接到网络的远程用户，但尚未登录到自己的系统。当在 GlobalProtect 端点门户网站上配置 Pre-logon（预登录）选项时，可以通过用户名 pre-logon 标识当前尚未登录到自己计算机的所有用户。然后，您可以为预登录用户创建策略，尽管用户没有直接登录，但也可以在域中对其计算机进行身份验证，好像他们已经完全登录。 • **known-user**（已知用户）— 包括所有已经过身份验证的用户，这意味着包括含有映射的用户数据的所有 IP 地址。此选项相当于域中的域用户组。 • 未知 — 包括所有未经身份验证的用户，这意味着包括尚未映射到用户的 IP 地址。例如，您可以使用来宾级别 **unknown**（未知）访问权限访问内容，因为它们在网络中拥有 IP 地址，但没有对域进行身份验证，且在防火墙上没有 IP 地址到用户的映射信息。 • **select** — 包括由此窗口中的选择项所确定的选定用户。例如，您可能想要添加一个用户、个人列表、一部分组或手动添加用户。 如果防火墙从 *RADIUS*、*TACACS+* 或 *SAML* 标识提供商服务器（而非 *User-ID*™ 代理）收集用户信息，则不会显示用户列表；您必须手动输入用户信息。
源设备	源	**Add**（添加）受策略约束的主机设备： • **any**（任何）— 包括任何设备。

© 2019 Palo Alto Networks, Inc.

安全规则的构建块	配置位置	说明
		• **no-hip**（无 **hip**）— 不需要 HIP 信息。此设置可以从无法收集或提交 HIP 信息的第三方设备访问。 • **quarantine**（隔离）— 包括列入隔离列表中的任何设备（**Device**（设备）> **Device Quarantine**（设备隔离））。 • **select**（选择）— 包括由您的配置所确定的选定设备。例如，您可以基于型号、OS、OS 系列或供应商添加设备对象。
源 HIP 配置文件	源	添加主机信息配置文件 (HIP)，以收集有关终端主机安全状态的信息，例如终端主机是否已安装最新的安全补丁和防病毒定义。使用策略实施的主机信息配置文件可启用粒度安全功能，确保远程主机能够访问得到充分维护的关键资源，并且保证遵循安全标准之后才允许访问网络资源。支持以下源 HIP 配置文件： • **any**（任何）— 无论 HIP 信息怎样，包括任何端点。 • **select**（选择）— 包括由您的配置所确定的选定 HIP 配置文件。例如，您可以添加一个 HIP 配置文件、HIP 配置文件列表或手动添加 HIP 配置文件。 • **no-hip**（无 **hip**）— 不需要 HIP 信息。此设置可以从无法收集或提交 HIP 信息的第三方客户端访问。
源订户	源	在 5G 或 4G 网络中 **Add**（添加）一个或多个采用以下格式的源订户： • 任何 • （仅限 5G）5G 用户永久标识符 (SUPI)，包括 IMSI。 • IMSI（14 或 15 位数字） • IMSI 值的范围为 11-15 位数字，用连字符隔开 • IMSI 前缀为 6 位数字，并在前缀后使用一个星号 (*) 作为通配符 • 用于指定 IMSI 的 EDL
源设备		在 5G 或 4G 网络中 **Add**（添加）一个或多个采用以下格式的源设备 ID： • 任何 • （仅限 5G）5G 永久设备标识符 (PEI)，包括国际移动设备识别码 (IMEI) • IMEI（11-16 位数字） • IMEI 前缀为 8 位数的类型分配代码 (TAC) • 用于指定 IMEI 的 EDL

网络切片	源	在 5G 网络中基于网络切片服务类型 (SST) **Add**（添加）一个或多个源网络切片，如下所示：
		• 标准化（预定义）**SST**
		  • **eMBB**（增强型移动宽带）— 用于实现更快的速度、更高的数据速率，例如，视频流。
		  • **URLLC**（超可靠低时延通信）— 适用于对延迟敏感的任务关键型应用程序，例如，关键 IoT（医疗保健、无线支付、家居控制以及车辆通信）。

© 2019 Palo Alto Networks, Inc.

安全规则的构建块	配置位置	说明
		• **MIoT**（大规模物联网）— 例如，智能计量、智能废弃物管理、防盗窃、资产管理以及位置跟踪。 • 网络切片 **SST** - 特定于运营商— 您可以命名并指定切片。切片名称的格式为文本 + 逗号 (,) + 数字（范围为 128-255）的形式。例如，Enterprise Oil2,145。
目标区域	目标	**Add**（添加）目标区域（默认为 **any**（任何区域））。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅 Network（网络）> Zones（区域）。 多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。 在区域内规则上，您不能定义目标区域，因为这些类型的规则只与同一区域内部的源和目标流量匹配。要指定与区域内规则匹配的区域，您仅需要指定源区域。
目标地址		**Add**（添加）目标地址、地址组或地区（默认为 **Any**（任何地址））。从下拉列表中选择，或单击 **Address**（地址）对象、**Address Group**（地址组）或 **Regions**（地区）（在下拉列表的底部），以指定地址设置。Objects（对象）> Addresses（地址）和 Objects（对象）> Address Groups（地址组）用于分别描述“安全”策略规则支持的地址对象和地址组类型。 通过选择 **Negate**（求反）选项，可将规则应用于指定区域的目标地址，但指定地址的除外。
目标设备		**Add**（添加）受策略约束的主机设备： • **any**（任何）— 包括任何设备。 • **quarantine**（隔离）— 包括列入隔离列表中的任何设备（**Device**（设备）> **Device Quarantine**（设备隔离））。 • **select**（选择）— 包括由您的配置所确定的选定设备。例如，您可以基于型号、OS、OS 系列或供应商添加设备对象。
应用程序	应用程序	**Add**（添加）安全策略规则的特定应用程序。如果应用程序具有多项功能，则可以选择整个应用程序或个别功能。如果选择整个应用程序，则所有功能均将包含，而且在将来添加功能时会自动更新应用程序定义。 如果在安全策略规则中使用应用程序组、筛选程序或容器，则可以通过将鼠标悬停在 Application（应用程序）列中的对象上方，打开下拉菜单，然后选择 **Value**（值），来查看这些对象的详细信息。此操作可让您直接从策略查看应用程序成员，无需导航到 **Object**（对象）选项卡。 始终指定一个或多个应用程序，这样，仅允许想在您网络上出现的应用程序，从而减少攻击面，更好地控制网络通信。切勿设置应用程序为

© 2019 Palo Alto Networks, Inc.

安全规则的构建块	配置位置	说明
		any（任何），这会允许任何应用程序的流量，从而增加攻击面。
服务	服务/**URL** 类别	选择要限制到特定 TCP 或 UDP 端口号的服务。从下拉列表中选择以下选项之一： • **any**（任何）— 所选应用程序在任何协议或端口上均得到许可或遭到拒绝。 • **application-default**（应用程序-默认）— 仅在 **ports defined by Palo Alto Networks**（**Palo Alto Networks** 定义的默认端口）®上允许或拒绝所选应用程序。建议选择此选项可让您使用各项策略，因为这些策略可以防止在不寻常的端口和协议上运行应用程序，如果发生异常情况，则这可能是发生意外应用程序行为和用途的迹象。 使用此选项时，防火墙仍然会检查在所有端口上运行的所有应用程序，但只允许在自己的默认端口和协议上运行应用程序。 对于大多数应用程序，使用*application-default*（应用程序 - 默认）阻止应用程序使用非标准端口，或是出现其他规避行为。如果应用程序的默认端口发生更改，防火墙会自动将规则更新为正确的默认端口。对于使用非标准端口的应用程序，例如内部自定义应用程序，请修改应用程序，或是创建一个指定非标准端口的规则，并只将此规则用于需要此应用程序的流量。 • **Select**（选择）— **Add**（添加）现有服务或选择 **Service**（服务）或 **Service Group**（服务组）以指定新条目。（或者，选择 Objects（对象）> Services（服务）和 Objects（对象）> Service Groups（服务组））。
URL 类别		选择安全规则的 URL 类别。 • 选择任何将允许或拒绝所有会话，而不考虑 URL 类别。 • 要指定类别，请从下拉列表中 **Add**（添加）一个或多个特定类别（包括自定义类别）。选择 Objects（对象）> External Dynamic Lists（外部动态列表）以定义自定义类别。
操作设置	操作	选择防火墙对与规则中定义属性匹配的流量执行的**Action**（操作）。 • **Allow**（允许）（默认）— 允许匹配的流量。 • **Deny**（拒绝）— 阻止匹配的流量，并执行为被拒绝的应用程序定义的默认拒绝操作。要查看为应用程序默认定义的拒绝操作，请查看应用程序详细信息（**Objects**（对象）> **Applications**（应用程序））。 由于默认拒绝操作因应用程序而异，防火墙可能会阻止会话，并对一个应用程序发送重置消息，同时可能会对另一个应用程序静默丢弃会话。

© 2019 Palo Alto Networks, Inc.

安全规则的构建块	配置位置	说明
		• 丢弃 — 静默丢弃应用程序。不向主机或应用程序发送 TCP 重置消息，除非选择 **Send ICMP Unreachable**（发送 **ICMP** 无法访问）。 • 重置客户端 — 向客户端设备发送 TCP 重置消息。 • 重置服务器 — 向服务器端设备发送 TCP 重置消息。 • **Reset both client and server**（重置客户端和服务器）— 向客户端和服务器端设备发送 TCP 重置消息。 • **Send ICMP Unreachable**（发送 **ICMP** 无法访问）— 仅可用于第 3 层接口。将安全策略规则配置为丢弃流量或重置连接时，流量无法到达目标主机。在这种情况下，对于所有 UDP 流量和丢弃的 TCP 流量，您可以让防火墙向流量起源的源 IP 地址发送“ICMP 无法访问”响应。启用此设置，可让流量源正常关闭或清除会话，防止应用程序遭到破坏。 要查看在防火墙上配置的“ICMP 无法访问数据包率”，请查看 Session Settings（会话设置）（**Device**（设备）> **Setup**（设置）> **Session**（会话））。 要替代预定义区域间和区域内规则中定义的默认操作：请参阅替代或恢复安全策略规则。
配置文件设置	操作	若要指定防火墙对匹配安全配置文件规则的数据包执行的其他检查，请选择单个防病毒、漏洞保护防间谍软件、URL 过滤、文件阻止、数据筛选、WildFire 分析、移动网络保护和 SCTP 保护配置文件。 若要指定配置文件组，而非单个配置文件，请选择 **Profile Type**（配置文件）作为**Group**（组），然后选择 **Group Profile**（组配置文件）。 若要定义新配置文件或配置文件组，请单击相应配置文件旁的 **New**（新建）或选择 **New Group Profile**（新组配置文件）。 您还可以将安全配置文件（或配置文件组）附加到默认规则中。
日志设置和其他设置	操作	要在本地通信日志中为匹配此规则的通信生成条目，请选择以下选项： • **Log At Session Start**（在会话开始时记录）（默认为禁用）— 生成关于会话开始的流量日志条目。 除非出于故障排除的原因，或是方便隧道会话日志在 *ACC* 中显示活动的 *GRE* 隧道，否则，不得启用 *Log at Session Start*（在会话开始时记录）。如果应用程序在几个数据包后发生更改，例如，从 *facebook-base* 到 *facebook-chat*，在会话结束时记录可消耗更少的资源，且能标识具体的应用程序。 • **Log At Session End**（在会话结束时记录）（默认为启用）— 生成关于会话结束的流量日志条目。 如果记录了会话开始或结束条目，则 *drop* 和 *deny* 条目也随之记录下来。

© 2019 Palo Alto Networks, Inc.

安全规则的构建块	配置位置	说明
		• **Log Forwarding Profile**（日志转发配置文件）— 要将本地流量日志和威胁日志条目转发到远程目标，如 Panorama 和 Syslog 服务器，请选择一个 **Log Forwarding Profile**（日志转发配置文件）。 由安全配置文件决定是否生成威胁日志条目。根据需要定义 *New*（新建）日志配置文件（请参阅 Objects（对象）> Log Forwarding（日志转发））。 创建并启用"日志转发"配置文件，以发送日志到专用的外部存储设备。这会保存日志，因为防火墙的日志存储空间有限，一旦空间消耗完毕，防火墙就会清除最旧的日志。 您也可以修改默认规则的日志设置。指定以下选项的任意组合： • **Schedule**（调度）— 要限制规则有效的天数和时间，请从下拉列表中选择调度。根据需要定义 **New**（新建）调度（请参阅控制解密 SSL 流量的设置）。 • **QoS Marking**（**QoS** 标记）— 要更改与规则匹配的数据包的服务质量 (QoS) 设置，请选择 **IP DSCP** 或 **IP Precedence**（**IP** 优先级），并以二进制形式输入 QoS 值，或从下拉列表中选择预定义的值。有关 QoS 的更多信息，请参阅服务质量。 • **Disable Server Response Inspection**（禁用服务器响应检查）— 禁用从服务器到客户端的数据包检查。此选项在默认情况下禁用。 为保证最佳安全状况，请不要启用 *Disable Server Response Inspection*（禁用服务器响应检查）。选择此选项后，防火墙仅检查从客户端到服务器的流量，而不会检查从服务器到客户端的流量，因此无法标识这些流量流中是否存在任何威胁。
基础知识	规则使用情况	• **Rule Created**（已创建规则）— 规则的创建日期和时间。 • **Last Edited**（最后一次编辑）— 最后一次编辑规则的日期和时间。
活动	规则使用情况	• **Hit Count**（命中次数）— 与规则匹配（命中）的流量总次数。 • **First Hit**（第一次命中）— 第一次匹配规则的时间。 • **Last Hit**（最后一次命中）— 最后一次匹配规则的时间。
应用程序	规则使用情况	• **Applications Seen**（查看的应用程序）— 规则允许的应用程序数。 • **Last App Seen**（最后查看应用程序）— 自在规则上看到最后一个新应用程序（先前从未查看过的应用程序）以来的天数。 • **Compare Applications & Applications Seen**（比较应用程序和看到的应用程序）— 单击以将规则上配置的应用程序与规

© 2019 Palo Alto Networks, Inc.

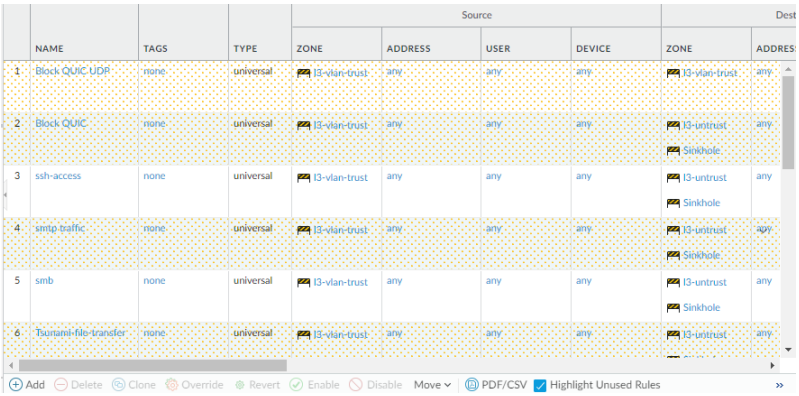
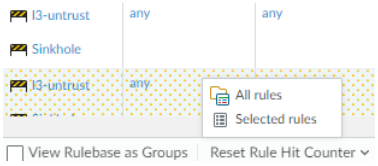
安全规则的构建块	配置位置	说明
		则上看到的应用程序进行比较。使用此工具，可发现与规则匹配的应用程序，并将应用程序添加到规则中。
流量（过去 30 天）	规则使用情况	• **Bytes**（字节）— 过去 30 天与规则匹配的流量（以字节为单位）。 超过 *30* 天可能会导致旧规则停留在列表顶部，这是因为这些规则可能包含最多的累积流量。这可能会导致列表中新规则排在旧规则的后面，即使是新规则发现大量的流量。
任何（针对所有设备） 仅限 Panorama	目标	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备 仅限 Panorama		选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记 仅限 Panorama		**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备 仅限 Panorama		启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

创建和管理策略

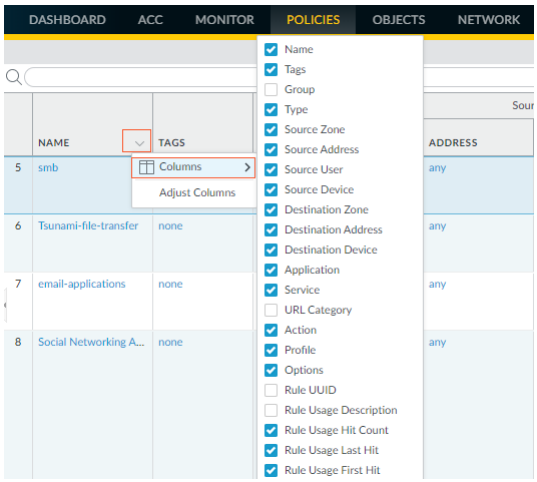
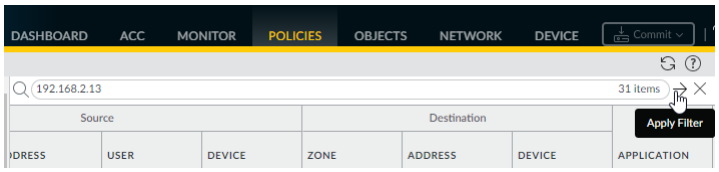
选择 **Policies**（策略）> **Security**（安全）页面可添加、修改和管理安全策略：

任务	说明
添加	**Add**（添加）新策略规则，或是选择一个基于新规则的规则，并 **Clone Rule**（克隆规则）。复制的规则（“rule*n*”）将插入到所选规则的下面，其中，*n* 是使规则名称保持唯一的下一个可用整数。有关克隆的详细信息，请参阅移动或克隆策略规则。
修改	选中规则以修改其设置。 如果此规则是从 Panorama 推送的，则此规则在防火墙上是只读规则，并且不能在本地进行编辑。
	Override（替代）和 **Revert**（恢复）操作仅适用于安全规则库底部显示的默认规则。这些预定义规则（允许所有区域内流量，拒绝所有区域间流量）可指导防火墙如何处理与规则库中任何其他规则不匹配的流量。由于它们是预定义配置的一部分，因此您必须 **Override**（替代）它们以便编辑选定的策略设置。如果您使用 Panorama，也可以 **Override**（替代）默认规则，然后在设备组或共享上下文中将它们推送到防火墙。您也可以恢复默认规则，这样可以还原预定义的设置或从 Panorama 推送的设置。有关详细信息，请参阅替代或恢复安全策略规则。
移动	规则按照 **Policies**（策略）页面上所列举的自上而下的顺序进行评估。如需更改对网络流量评估规则的顺序，请选择一个规则，然后单击 **Move Up**（向上移动）、**Move Down**（向下

© 2019 Palo Alto Networks, Inc.

任务	说明
	移动）、**Move Top**（移至顶部）或 **Move Bottom**（移至底部），或是 **Move to a different rulebase or device group**（移至不同的规则库或设备组）。有关详细信息，请参阅移动或克隆策略规则。
复制 UUID	将规则的 UUID 复制到剪贴板，以在搜索配置或日志时使用。
删除	选中并**Delete**（删除）现有规则。
启用/禁用	要禁用规则，选中规则并将其 **Disable**（禁用）；要启用已禁用的规则，选中规则并将其 **Enable**（启用）。
监控规则使用情况	如需标识自防火墙最近一次重启后尚未使用的规则，请选择 **Highlight Unused Rules**（突出显示未使用的规则）。未使用规则带有虚线背景。随后可以决定是 **Disable**（禁用）还是 **Delete**（删除）此规则。当前未使用的规则将用附点黄色背景显示。若启用策略规则命中次数，则可使用点击数数据确定规则是否未使用。 每个防火墙都为具有匹配项的规则来维护通信标记。由于标记在重新引导或重新启动时由于数据平面重置而重置，因此作为最佳实践，应该在删除或禁用规则之前，定期监控此列表以确定规则自从上次检查以来是否具有了匹配项。 
重置规则命中次数	**Hit Count**（命中次数）用于跟踪策略规则的总流量命中次数。在重新启动、升级和数据平面重启过程中，总流量命中次数持续增加。 或者，**Reset Rule Hit Counter**（重置规则命中计数器）（底部菜单）。要清除命中次数统计信息，选中 **All Rules**（全部规则），或者选择特定规则，然后仅重置 **Selected rules**（所选规则）的命中次数统计信息。  查看 **First Hit**（第一次命中）以标识第一次命中安全策略的时间。日期格式为 XX 年 XX 月 XX 日 XX 时 XX 分 XX 秒。您无法重置此值。 查看 **Last Hit**（最后一次命中）以标识最后使用安全策略的时间。日期格式为 XX 年 XX 月 XX 日 XX 时 XX 分 XX 秒。您无法重置此值。

© 2019 Palo Alto Networks, Inc.

任务	说明
显示/隐藏列	显示或隐藏 **Policies**（策略）下显示的列。选择列名称以切换显示。 
应用筛选程序	要对列表应用过滤器，请从过滤器规则下拉列表中选择规则。要定义过滤器，从项目下拉列表中选择 **Filter**（过滤器）。 默认规则不是用于过滤的规则库的一部分，并且始终显示在过滤规则列表中。
	要查看作为策略的匹配项记录的网络会话，请从规则名称下拉列表中选择 **Log Viewer**（日志查看器）。
	要显示当前值，请从条目下拉列表中选择 **Value**（值）。您还可以直接从列菜单编辑、过滤或删除项目。例如，要查看地址组中包含的地址，请将鼠标悬停在 **Addres**（地址）列中的对象上方，然后从下拉列表中选择 **Value**（值）。此操作可让您快速查看地址组的成员和相应 IP 地址，无需导航到 **Object**（对象）选项卡。
	如需根据对象名称或 IP 地址查找策略中使用的对象，请使用过滤器。应用过滤器后，您将只会看到与该过滤器相匹配的项目。过滤器也适用于嵌入的对象。例如，如果对 10.1.4.8 进行筛选，则仅会显示包含该地址的策略： 
预览规则（仅限 Panorama）	使用 **Preview Rules**（预览规则）可查看在将规则推送到受管防火墙之前的规则列表。在每个规则库内，每个设备组（和受管防火墙）的规则级联可在视觉上进行划定，从而使得更容易通过大量规则进行扫描。
导出配置表格	具有最小只读访问权限的管理角色可以将策略规则库导出为 **PDF/CSV**。您可以根据需要应用筛选程序来创建更多特定的表格配置输出，以用于审计等事宜。将仅导出 Web 界面中所显示的列。请参阅配置表格导出。

© 2019 Palo Alto Networks, Inc.

任务	说明
突出显示未使用的规则	在 **Rule Usage**（规则使用情况）列中突出显示与流量不匹配的任何策略规则。
群组	选中 **View Rulebase as Groups**（将规则库视为组）框后，即可管理标记组。您可以执行以下操作： • **Move rules in group to different rulebase or device group**（将组内规则移至不同的规则库或设备组）— 将所选标记组移至不同的设备组。 • **Change group of all rules**（更改所有规则组）— 将选中标记组内规则移至规则库内不同的标记组。 • **Delete all rules in group**（删除组内所有规则）— 删除所选标记组内所有规则。 • **Clone all rules in group**（克隆组内所有规则）— 将所选标记组内规则克隆到设备组。
将规则库视为组	**View Rulebase as Groups**（将规则库视为组）以使用 **Group Rules by Tag**（使用标记对规则分组）内使用的标记查看策略规则库。可见的策略规则是那些属于所选标记组的规则。
测试策略匹配	对所选策略规则库执行保护策略测试，以验证是否拒绝或允许正确的通信。

替代或恢复安全策略规则

默认安全规则（区域间默认规则和区域内默认规则）具有可在防火墙或 Panorama 上替代的预定义设置。如果防火墙收到来自设备组的默认规则，还可以替代设备组设置。执行替代操作的防火墙或虚拟系统的配置中可存储规则的本地版本。可以替代的设置是完整集合的子集（下表列出了安全规则子集）。有关默认安全规则的详细信息，请参阅 Policies（策略）> Security（安全）。

要替代规则，请在防火墙上选择 **Policies**（策略）> **Security**（安全），或在 Panorama 上选择 **Policies**（策略）> **Security**（安全）> **Default Rules**（默认规则）。Name（名称）列将对可替代的规则显示继承图标（）。选择规则，单击替代，然后在随后的表格中编辑设置。

要将替代的规则恢复为其预定义设置或从 Panorama 设备组推送的设置，请在防火墙上选择 **Policies**（策略）> **Security**（安全），或在 Panorama 上选择 **Policies**（策略）> **Security**（安全）> **Default Rules**（默认规则）。名称列将对有替代值的规则显示替代图标（）。选择规则，单击恢复，然后单击是以确认操作。

替代默认安全规则的字段	说明
“常规”选项卡	
姓名	用于识别规则的名称是只读字段；不能替代它。
规则类型:	规则类型是只读字段；不能替代它。
说明	说明是只读字段；不能替代它。
标记	从下拉列表中选择标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“入站到 DMZ”来标记某些安全策略，使用关键字“解

© 2019 Palo Alto Networks, Inc.

替代默认安全规则的字段	说明
	密”或“不解密”标记特定解密策略，或者将特定数据中心的名称用于和该位置关联的策略。
操作选项卡	
操作设置	为与规则匹配的流量选择合适的操作。 • 允许 — （默认）允许流量。 • 拒绝 — 阻止流量，并强制执行为防火墙所拒绝应用程序定义的默认拒绝操作。要查看为应用程序默认定义的拒绝操作，请在 **Objects**（对象）> **Applications**（应用程序）中查看应用程序详细信息。 • 丢弃 — 静默丢弃应用程序。防火墙不向主机或应用程序发送 TCP 重置消息。 • 重置客户端 — 向客户端设备发送 TCP 重置消息。 • 重置服务器 — 向服务器端设备发送 TCP 重置消息。 • 重置两者 — 向客户端和服务器端设备发送 TCP 重置消息。
配置文件设置	**Profile Type**（配置文件类型）— 将配置文件或配置文件组分配给安全规则： • 若要指定默认安全配置文件执行的检查，请选择 **Profiles**（配置文件），然后选择一个或多个单独的 **Antivirus**（防病毒）、**Vulnerability Protection**（漏洞保护）、**Anti-Spyware**（防间谍软件）、**URL Filtering**（**URL** 过滤）、**File Blocking**（文件阻止）、**Data Filtering**（数据筛选）、**WildFire Analysis**（**WildFire** 分析）、**SCTP Protection**（**SCTP** 保护）、和 **Mobile Network Protection**（移动网络保护）配置文件。 • 要分配配置文件组，而非单个配置文件，请选择 **Group**（组），然后从下拉列表中选择 **Group Profile**（组配置文件）。 • 要定义新配置文件（Objects（对象）> Security Profiles（安全配置文件））或配置文件组，请单击相应配置文件或组的下拉列表中的 **New**（新建）。

日志设置	指定以下选项的任意组合：
	• 日志转发 — 要将本地流量日志和威胁日志条目转发到远程目标，如 Panorama 和 Syslog 服务器，请从下拉列表中选择日志转发配置文件。安全配置文件用于决定是否生成威胁日志条目。要定义新的日志转发配置文件，请在下拉列表中选择 **Profile**（配置文件）（请参阅 Objects（对象）> Log Forwarding（日志转发））。
	• 要在本地通信日志中为匹配此规则的通信生成条目，请选择以下选项：
	  • **Log at Session Start**（在会话开始时记录）— 生成关于会话开始的流量日志条目（默认选中）。
	  • **Log at Session End**（在会话结束时记录）— 生成关于会话结束的流量日志条目（默认未选中）。
	如果将防火墙配置为在通信日志中包含会话开始或会话结束条目，则其中还将包含丢弃和拒绝条目。

© 2019 Palo Alto Networks, Inc.

应用程序和使用情况

- Policies（策略）> Security（安全）> Policy Optimizer（策略优化器）> No App Specified（未指定应用程序）> Compare（比较）（或者单击 **Apps Seen**（查看的应用程序）中的数字）
- Policies（策略）> Security（安全）> Policy Optimizer（策略优化器）> Unused Apps（未使用的应用程序）> Compare（比较）（或者单击 **Apps Seen**（查看的应用程序）中的数字）
- Policies（策略）> Security（安全）并单击 **Apps Seen**（查看的应用程序）中的数字

在“安全”策略规则的“使用情况”选项卡上，您还可以 **Compare Applications & Applications Seen**（比较应用程序和查看的应用程序）来访问有助于您从基于端口的“安全”策略规则迁移到基于应用程序的“安全”策略规则的工具，从而删除 **Applications & Usage**（应用程序和使用情况）的规则内未使用的应用程序。

字段	说明
时间段	应用程序信息的时间段： • **Anytime**（任何时间）— 显示在规则生命周期内查看的应用程序。 • **Past 7 days**（过去 **7** 天）— 仅显示过去 7 天查看的应用程序。 • **Past 15 days**（过去 **15** 天）— 仅显示过去 15 天查看的应用程序。 • **Past 30 days**（过去 **30** 天）— 仅显示过去 30 天查看的应用程序。
规则中的应用程序	规则中配置的应用程序或 **Any**（任何）（如果规则中未配置特定应用程序）。必要时，可以 **Browse**（浏览）、**Add**（添加）和 **Delete**（删除）应用程序；针对规则配置应用程序。Apps on Rule（符合规则的应用程序）旁边带圆圈的数字表示应用程序的数量。从此位置添加应用程序的方式与在“安全”策略规则 **Application**（应用程序）选项卡上添加应用程序的方式相同。
看到的应用程序	在与规则匹配的防火墙上查看和允许的所有应用程序。“查看的应用程序”旁边带圆圈的数字表示根据规则查看的应用程序数量。 • **Applications**（应用程序）— 根据规则查看的应用程序。例如，如果规则允许 Web 浏览流量（Apps on Rule（符合规则的应用程序）），则可能会在列表中看到大量应用程序，因为存在大量的 Web 浏览应用程序。 • **Subcategory**（子类别）— 应用程序的子类别。 • **Risk**（风险）— 应用程序的风险等级。 • **First Seen**（首次查看）— 应用程序在网络上第一次被查看的日期。 • **Last Seen**（上次查看）— 应用程序在网络上最近一次被查看的日期。 “首次查看”和“上次查看”的测量粒度都是一天，因此，在您定义规则的当天，“首次查看”和“上次查看”为同一天。 • **Traffic (30 days)**（流量（**30** 天））—在过去 30 天内看到的通信量（以字节为单位）。 时间段越长，越可能导致旧规则停留在列表顶部，这是因为这些规则可能包含最多的累积流量。这可能会导致列表中新规则排在旧规则的后面，即使是新规则发现大量的流量。

© 2019 Palo Alto Networks, Inc.

字段	说明
“查看的应用程序”操作	可以在 **Apps Seen**（看到的应用程序）上完成的操作： • **Create Cloned Rule**（创建克隆规则）— 克隆当前规则。从基于端口的规则迁移到基于应用程序的规则时，先克隆基于端口的规则，然后编辑克隆，从而创建可允许流量的基于应用程序的规则。将克隆规则插入到策略列表内基于端口的规则前面。此迁移方法可确保您不会无意中拒绝想要允许的流量 — 如果克隆规则不允许您需要的所有应用程序，随后基于端口的规则会允许。监视基于端口的规则，并根据需要调整（克隆）基于应用程序的规则。若您确定基于应用程序的规则允许您想要的流量，而仅不需要的流量被基于端口的规则筛选掉，则可以安全地删除基于端口的规则。 • **Add to This Rule**（添加到此规则）— 将应用程序从“查看的应用程序”添加到规则。添加应用程序到规则可将配置为匹配 **Any**（任何）应用程序（基于端口的应用程序）的规则转换为基于应用程序的规则，从而允许您指定的应用程序（新的基于应用程序的规则替代基于端口的规则）。规则将拒绝所有未添加的应用程序，就像拒绝任何其他基于应用程序的规则一样。确保已标识想要允许的所有应用程序，并将其添加到规则，这样，应用程序就不会被意外拒绝。 • **Add to Existing Rule**（添加到现有规则）—将应用程序从“查看的应用程序”添加到现有基于应用程序 (App-ID) 的规则。这使您可以从基于端口的规则中克隆基于 App-ID 的规则，然后稍后将根据基于端口的规则查看的更多应用程序添加到 App-ID 规则中。 • **Match Usage**（匹配使用情况）— 将所有“查看的应用程序”移至规则中（**Match Usage**（匹配使用情况）后，这些应用程序将在 Apps on Rule（符合规则的应用程序）中列出）。如果您确定规则应允许所有列出的应用程序，使用 **Match Usage**（匹配使用情况）就非常方便。但是，您必须确保所有列出的应用程序都是您想要在网络上出现的应用程序。如果在规则上看到大量应用程序（例如，在允许 Web 浏览的规则中），最好是克隆规则，然后转换为基于应用程序的规则。对于应用于知名应用程序的简单规则而言，适合适用 **Match Usage**（匹配使用情况）。例如，端口 22 的基于端口的规则仅查看 SSH 流量（且只能查看此类流量），执行 **Match Usage**（匹配使用情况）就很安全。

Clone（克隆）对话框
“添加到此规则”对话框
“添加应用程序到现有规则”对话框
	从 **Apps Seen**（查看的应用程序）选择应用程序，并**Create Cloned Rule**（创建克隆规则）或 **Add to Rule**（添加到规则）（该规则拥有相关应用程序）时，这些对话框将列出：
	• **Name**（名称）（仅“克隆”和“添加应用程序到现有规则”对话框）。
	  • 克隆：输入新克隆规则的名称。
	  • 添加应用程序到现有规则：从下拉菜单中选择要向其添加应用程序的规则，或者输入规则的名称。
	• **Applications**（应用程序）：
	  • 添加容器应用程序（默认）：选择以下项的复选框：所有容器应用程序、根据规则查看的应用程序，以及容器中未根据规则查看的应用程序。
	  • 添加特定查看的应用程序：只选择已根据规则实际查看的应用程序，取消选择其他所有应用程序。（您可以手动选择容器应用程序和其他应用程序。）
	• **Applications**（应用程序）：

© 2019 Palo Alto Networks, Inc.

字段	说明
	• 已根据规则查看的所选应用程序以绿色突出显示。 • 容器应用程序以灰色突出显示，相应的单个应用程序如下所示。 • 容器中已根据规则查看但未在 **Applications & Usage**（应用程序和使用情况）中选择的单个应用程序（普通文本）。 • 未根据规则查看的容器内单个应用程序（斜体）。 • 日期应用程序是符合规则的 **Last Seen**（上次查看）。 • **Dependent Applications**（相关应用程序）： • 默认勾选用于添加应用程序相关性的复选框，因为，要使选中的应用程序运行，需要这些应用程序。 • **Depends On**（相关）— 用于选中应用程序的相关应用程序列表。要使选中的应用程序运行，需要这些相关应用程序。 • **Required By**（必须）— 需要相关应用程序的应用程序列表（**Depends On**（相关））。（有时，相关应用程序反过来又会需要其他相关应用程序。） 通过 **Clone**（克隆）、**Add to Rule**（添加到规则）和 **Add Apps to Existing Rule**（添加应用程序到现有规则）对话框，可确保应用程序不会中断，并在将来对规则进行证明，方法是纳入与克隆或添加到规则的应用程序有关的相关单个应用程序。

安全策略优化器

- Policies（策略）> Security（安全）> Policy Optimizer（策略优化器）

Policies（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）显示如下内容：

- 未指定应用程序 — 设置应用程序为 **any**（任何）的规则，这样，您可以标识基于端口的规则，从而将其转换为基于应用程序的规则。
- 未使用的应用程序 — 包含从而与规则匹配的应用程序。
- **Rule Usage**（规则使用情况）—不同时间段的规则使用情况信息，包括未在不同时间段使用的规则。

字段	说明
名称	安全策略规则的名称。
服务	与安全策略规则关联的任何服务。
流量（字节数，30 天）	**Traffic (30 days)**（流量（**30** 天））—在过去 30 天内看到的通信量（以字节为单位）。 时间段越长，越可能导致旧规则停留在列表顶部，这是因为这些规则可能包含最多的累积流量。这可能会导致列表中新规则排在旧规则的后面，即使是新规则发现大量的流量。
允许的应用程序	规则允许的应用程序。打开 **Application**（应用程序）对话框，您可以在其中添加和删除规则上的应用程序。

© 2019 Palo Alto Networks, Inc.

字段	说明
看到的应用程序	规则中看到的应用程序。单击数字以打开 **Applications & Usage**（应用程序和使用情况）对话框，这样，您可以将规则上配置的应用程序与规则上看到的应用程序进行对比，并修改应用程序。
没有新应用程序的天数	自上一次在规则上看到新应用程序以来的天数。
比较	打开 **Applications & Usage**（应用程序和使用情况）对话框，将规则上配置的应用程序与规则上看到的应用程序进行对比，并修改规则。
（规则使用情况）上一次点击	最近一次流量与规则匹配的时间。
（规则使用情况）第一次点击	第一次流量与规则匹配的时间。
（规则使用情况）点击数	流量与规则匹配的次数。
已修改	上一次修改该规则的日期时间。
创建于	该规则创建的日期时间。
时间段（仅限规则使用情况）	数据显示的时间段（天数）。
使用情况（仅限规则使用情况）	显示： • 指定时间段内防火墙上的 **Any**（任何）（所有）规则，无论流量与规则匹配（已使用规则）还是不匹配（未使用规则）。 • **Unused**（未使用）规则是指在指定时间段内流量未匹配 。 • **Used**（已使用）规则是指在指定时间段内流量已匹配。
排除过去 *xx* 天内的规则重置（仅限规则使用情况）	不会显示指定天数（从 1-5,000 天）内 **Reset Rule Hit Counter**（重置规则命中次数计数器）的规则。例如，通过此操作，您可以检查时间段内未匹配流量的较旧规则，同时排除可能有时间与流量匹配的较新规则。
重置日期（仅限规则使用情况）	上次重置规则命中次数计数器的日期。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> NAT

如果在防火墙上定义第 3 层接口，可以配置网络地址转换 (NAT) 策略，以指定在公用和专用地址和端口之间，是转换源 IP 地址和端口还是目标 IP 地址和端口。例如，从内部（受信）区域向公用（非受信）区域发送流量时，专用源地址可以转换为公用地址。虚拟线路接口同样支持 NAT。

NAT 规则基于源区域和目标区域、源地址和目标地址以及应用程序服务（比如 HTTP）。与安全策略一样，针对传入流量按顺序对 NAT 策略规则进行比较，并应用与流量匹配的第一个规则。

根据需要，将静态路由添加到本地路由器，以便将发送到所有公用地址的流量路由到防火墙。此外，可能需要将静态路由添加到防火墙上的接收接口，才能将流量路由回专用地址。

下表介绍了 NAT 和 NPTv6 (IPv6 到 IPv6 的网络前缀转换）设置：

- NAT 策略常规选项卡
- NAT 原始数据包选项卡
- NAT 转换后数据包选项卡
- NAT 主动/主动 HA 绑定选项卡
- （仅限 Panorama）NAT Target（NAT 目标）选项卡

了解更多？

请参阅 NAT

NAT 策略常规选项卡

- **Policies**（策略）> **NAT** > **General**（常规）

选择 **General**（常规）选项卡可以配置 NAT 或 NPTv6 策略的名称和说明。此外，也可配置标记，以便在存在许多策略时对其进行排序和筛选。可以选择要创建的 NAT 策略的类型，从而影响 **Original Packet**（原始数据包）和 **Translated Packet**（转换后的数据包）选项卡上的可用字段。

NAT 规则 — 常规设置	说明
姓名	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
说明	输入规则的说明（最多 1024 个字符）。
标记	如果要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。
NAT 类型	指定转换类型： • **ipv4** — 在 IPv4 地址之间转换。 • **nat64** — 在 IPv6 和 IPv4 地址之间转换。 • **nptv6** — 在 IPv6 前缀之间转换。

© 2019 Palo Alto Networks, Inc.

NAT 规则 — 常规设置	说明
	无法在单个 NAT 规则中合并 IPv4 和 IPv6 地址范围。
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。

NAT 原始数据包选项卡

- Policies（策略）> NAT > Original Packet（原始数据包）

选择 **Original Packet**（原始数据包）选项卡可定义防火墙将要转换的数据包的源和目标区域，且可选择指定目标接口和服务类型。您可配置类型相同的多个源和目标区域，也可对特定的网络或特定 IP 地址应用此规则。

NAT 规则 — 原始数据包设置	说明
源区域/目标区域	选择原始（非 NAT）数据包的一个或多个源区域和目标区域（默认为任何区域）。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅 Network（网络）> Zones（区域）。 您可指定多个区域，以简化管理。例如，可以配置设置，以便可以将多个内部 NAT 地址定向到同一外部 IP 地址。
目标接口	指定防火墙转换的数据包的目标接口。如果网络连接到具有不同 IP 地址池的两个 ISP，则目标接口可用于以不同方式转换 IP 地址。
服务	指定防火墙为其转换源或目标地址的服务。要定义新服务组，请参阅 Objects（对象）> Service Groups（服务组）。
源地址/目标地址	指定要防火墙转换的源和目标地址的组合。 对于 NPTv6，为 **Source Address**（源地址）和 **Destination Address**（目标地址）配置的前缀必须使用 xxxx:xxxx::/yy 格式。此地址不能定义接口标识符（主机）部分。支持的前缀长度范围为 /32 - /64。

NAT 转换后数据包选项卡

- Policies（策略）> NAT > Translated Packet（转换后的数据包）

对于源地址转换，选择 **Translated Packet**（转换后的数据包）选项卡可以确定对源、地址以及源转换到的可能端口执行的转换类型。

也可以为通过公用 IP 地址访问的内部主机启用 Destination Address Translation（目标地址转换）。在这种情况下，您可以在 **Original Packet**（原始数据包）选项卡中为内部主机定义公用源地址和目标地址，并在 **Translated Packet**（转换后的数据包）选项卡中配置 **Static IP**（静态 Ip）或或 **Dynamic IP (with session distribution)**（动态 **IP**（包含会话分发）），然后输入 **Translated Address**（转换后的地址）。然后，在访问公用地址时，需将其转换为内部主机的内部（目标）地址。

© 2019 Palo Alto Networks, Inc.

NAT 规则 — 转换后的数据包设置	说明
源地址转换	选择 **Translation Type**（转换类型）（动态或静态地址池），然后输入源地址转换到的 IP 地址或地址范围 (address1-address2)（**Translated Address**（转换后的地址））。地址范围的大小受到地址池类型的限制： • **Dynamic IP And Port**（动态 **IP** 和端口）— 根据源 IP 地址的哈希值选择地址。对于给定的源 IP 地址，防火墙会将同一转换的源地址用于所有会话。在 NAT 池中，动态 IP 和端口 (DIPP) 源 NAT 支持在每个 IP 地址上运行约 64,000 个并发会话。某些型号支持过度订阅，即允许单个 IP 托管超过 64,000 个并发会话。 Palo Alto Networks® DIPP NAT 支持的 NAT 会话数多于可用 IP 地址和端口数所支持的 NAT 会话数。启用过度订阅后，如果目标 IP 地址唯一，则防火墙在 PA-220、PA-820、PA-850、VM-50、VM-300 和 VM-1000-HV 防火墙上可以同时使用两次 IP 地址和端口组合，在 PA-5220 防火墙和 PA-3200 系列防火墙上可以同时使用四次，在 PA-5250、PA-5260、PA-5280、PA-7050、PA-7080、VM-500 和 VM-700 防火墙上可以同时使用八次。 • **Dynamic IP**（动态 **IP**）— 转换到指定范围中的下一个可用地址，但未更改端口号。最多支持 32,000 个连续 IP 地址 。 动态 IP 池可包含多个子网，因此您可以将内部网络地址转换为两个或多个单独的公用子网。 • **Advanced (Dynamic IP/Port Fallback)**（高级（动态 **IP**/端口回退））— 使用此选项创建回退池，此池执行 IP 和端口转换，并在主池地址不足时使用。使用 **Translated Address**（转换后的地址）选项或 **Interface Address**（接口地址）选项可为池定义地址，后一个选项适用于动态接收 IP 地址的接口。创建回退池时，请确保上述地址与主池中的地址不重叠。
源地址转换（续）	• 静态 **IP** — 转换始终使用同一地址，并且端口保持不变。例如，如果源范围为 192.168.0.1—192.168.0.10 且转换范围为 10.0.0.1—10.0.0.10，则始终将地址 192.168.0.2 转换为 10.0.0.2。实际上，地址范围不受限制。 必须使用 **Static IP**（静态 **IP**）转换对 NPTv6 进行源地址转换。对于 NPTv6，为 **Translated Address**（转换后的地址）配置的前缀必须使用 xxxx:xxxx::/yy 格式，而且地址不能定义接口标识符（主机）部分。支持的前缀长度范围为 /32 - /64。 • 无— 不执行转换。
双向	（可选）如果希望防火墙按所配置转换的相反方向创建相应的转换（NAT 或 NPTv6），则对 **Static IP**（静态 **IP**）源地址转换启用双向转换。 如果启用双向转换，则必须确保正确使用安全策略来对流量进行双向控制。如不使用此策略，双向功能将允许同时在两个方向上对数据包进行自动转换。
目标地址转换	配置以下选项以使防火墙执行目标 NAT。通常使用目标 NAT 以允许从公用网络访问内部服务器，如电子邮件服务器。
转换类型和转换后的地址	选择防火墙对目标地址执行的转换类型： • **None**（无）（默认） • **Static IP**（静态 **IP**）— 输入 **Translated Address**（转换后的地址）（作为 IP 地址或 IP 地址范围）和 **Translated Port**（转换后的端口）号（1 到 65535），以转换原始目标地址和端口号。如果 **Translated Port**（转换后的端口）字段为空，则不会更改目标端口。

© 2019 Palo Alto Networks, Inc.

NAT 规则 — 转换后的数据包设置	说明
	对于 NPTv6，为目标前缀 **Translated Address**（转换后的地址）配置的前缀必须使用 xxxx:xxxx::/yy 格式。此地址不能定义接口标识符（主机）部分。支持的前缀长度范围为 /32 - /64。 *NPTv6 不支持转换后的端口，因为 NPTv6 是严格的前缀转换。只需原样转发端口和主机地址部分。* *IPv4 的静态 IP 转换还允许您 Enable DNS Rewrite（启用 DNS 重写）（如下所述）。* • **Dynamic IP (with session distribution)**（动态 **IP**（包含会话分发））— 选择或输入 **Translated Address**（转换后的地址）（可为 FQDN、地址对象或防火墙从中选择转换后的地址的地址组）。如果 DNS 服务器为 FQDN 返回多个地址，或者地址对象或地址组转换为多个 IP 地址，则防火墙使用指定的 **Session Distribution Method**（会话分发方法）在这些地址之间分发会话。
会话分发方法	如果选择目标 NAT 转换为 **Dynamic IP (with session distribution)**（动态 **IP**（包含会话分发）），则转换为 FQDN、地址对象或地址组的目标地址可以解析为多个地址。您可以选择防火墙在这些地址之间分发（分配）会话的方式，以提供更均衡的会话分发： • **Round Robin**（循环调度）—（默认）按轮流顺序分配新会话到 IP 地址。除非您的环境要求您选择其他分发方法之一，否则，请使用此方法。 • **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，则选择除 **Source IP Hash**（源 **IP** 哈希）之外的一种方法。 • **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）— 使用源和目标 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发。
启用 DNS 重写	在 PAN-OS 9.0.2 及 9.0 更高版本中，若目标 NAT 策略规则类型为 **ipv4**，且目标地址转换类型为 **Static IP**（静态 **IP**），则可使用 **Enable DNS Rewrite**（启用 **DNS** 重写）选项。如果使用目标 NAT 并还在防火墙一侧使用 DNS 服务来解析防火墙另一侧上客户端的 FQDN，则可启用 DNS 重写。当 DNS 响应通过防火墙时，防火墙会按照 NAT 策略规则中 DNS 响应匹配的原始目标地址或转换后的目标地址，重写 DNS 响应中的 IP 地址。单个 NAT 策略规则可让防火墙对符合规则的数据包执行 NAT，并对符合规则的 DNS 响应中的 IP 地址执行 NAT。您必须指定防火墙按照 NAT 规则对 DNS 响应中的 IP 地址上执行 NAT 的方式 — 反向或正向： • **reverse**（反向）—（默认）如果数据包是与规则中转换后的目标地址匹配的 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 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 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。

NAT 主动/主动 HA 绑定选项卡

- Policies（策略）> NAT > Active/Active HA Binding（主动/主动 HA 绑定）

© 2019 Palo Alto Networks, Inc.

仅当防火墙处于高可用性 (HA) 主动/主动配置时，Active/Active HA Binding（主动/主动 HA 绑定）选项卡才可用。在此配置中，您必须将每个源 NAT 规则（无论是静态还是动态 NAT）绑定到设备 ID 0 或设备 ID 1；必须将每个目标 NAT 规则绑定到设备 ID **0**、设备 ID **1**、**both**（两者）（设备 ID 0 和设备 ID 1）或主动 **primary**（主）防火墙。

选择 **Active/Active HA Binding**（主动/主动 **HA** 绑定）设置可将 NAT 规则绑定到 HA 防火墙，如下所述：

- **0** — 将 NAT 规则绑定到拥有 HA 设备 ID 0 的防火墙。
- **1** — 将 NAT 规则绑定到拥有 HA 设备 ID 1 的防火墙。
- **both**（两者）— 将 NAT 规则同时绑定到拥有 HA 设备 ID 0 和 HA 设备 ID 1 的防火墙。此设置不支持动态 IP 或动态 IP 和端口 NAT。
- **primary**（主要）— 将 NAT 规则绑定到处于 HA 主动-主要状态的防火墙。此设置不支持动态 IP 或动态 IP 和端口 NAT。

通常，如果两个 HA 对端拥有唯一的 NAT IP 地址池，则可配置设备特定的 NAT 规则。

防火墙创建新会话后，通过 HA 绑定即可确定与该会话相匹配的 NAT 规则。绑定中必须包含要匹配的规则的会话所有者。会话设置防火墙将执行 NAT 规则匹配，但会话将与绑定到会话所有者并按其中一条规则进行转换的 NAT 规则进行比较。对于设备特定的规则，防火墙将跳过所有未绑定至会话所有者的 NAT 规则。例如，假设带有设备 ID 1 的防火墙是会话所有者和会话设置防火墙。当设备 ID 1 尝试将会话与 NAT 规则匹配时，它会忽略所有绑定到设备 ID 0 的规则。

如果一个对端出现故障，则第二个对端会继续为来自故障对端的同步会话处理通信，包括 NAT 转换等。Palo Alto Networks 建议用户创建绑定到第二个设备 ID 的重复 NAT 规则。因此，将存在两个带有相同源转换地址和目标转换地址的 NAT 规则，同时对每个设备 ID 绑定一个规则。此配置可允许 HA 对端执行新会话设置任务，并对绑定到其设备 ID 的 NAT 规则执行 NAT 规则匹配。如不使用重复 NAT 规则，则功能对端将尝试执行 NAT 策略匹配，但会话不会匹配防火墙自身的设备特定规则，且防火墙会跳过所有未绑定到其设备 ID 的其他 NAT 规则。

了解更多？

请参阅主动/主动 HA 模式下的 NAT。

NAT Target（NAT 目标）选项卡

- （仅限 Panorama）**Policies**（策略）> **NAT** > **Target**（目标）

选择 **Target**（目标）选项卡，以选择要将策略规则推送到设备组中的哪一个受管防火墙。您可以通过选择受管防火墙或是指定标记等方式指定要推送到哪一个受管防火墙。此外，您还可以配置策略规则目标，以推送到除指定防火墙以外的所有受管防火墙。

NAT 规则 - 目标设置	说明
任何（针对所有设备）	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备	选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记	**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备	启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> QoS

添加 QoS 策略规则，可定义接收特定 QoS 处理的流量，而为每个 QoS 策略规则分配特定 QoS 类，可指定在与相关规则匹配的所有流量退出启用 QoS 的接口时，对其应用所分配的服务类。

从 Panorama 推送到防火墙的 QoS 策略规则将以橙色显示，且无法在防火墙级别上进行编辑。

此外，要完全让防火墙提供 QoS，请执行以下操作：

- 为每个 QoS 服务类设置带宽限制（选择 Network（网络）> Network Profiles（网络配置文件）> QoS 以添加或修改 QoS 配置文件）。
- 在接口上启用 QoS（选择 Network（网络）> QoS）。

有关完整的 QoS 工作流程、概念及用例，请参阅服务质量。

添加新规则或克隆现有规则，然后定义以下字段。

QoS 策略规则设置	
“常规”选项卡	
名称	输入名称以标识规则（最多 63 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入可选说明。
标记	如果需要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“入站到 DMZ”来标记某些安全策略，使用关键字“解密”和“不解密”标记解密策略，或者将特定数据中心的名称用于和该位置关联的策略。
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。
Source 选项卡	
Source Zone（源区域）	选择一个或多个源区域（默认为 **any**（任何））。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。
Source Address（源地址）	指定可替代已标识应用程序的 IPv4 或 IPv6 源地址的组合。如需选择特定地址，请从下拉列表中选择 **select**（选择），然后执行以下任意操作： • 在可用列中相应的地址和/或地址组旁，选中此选项，然后单击 **Add**（添加），将选择项添加到选定列。

© 2019 Palo Alto Networks, Inc.

QoS 策略规则设置	
	• 在搜索字段中输入名称的前几个字符，列出所有以这些字符开头的地址和地址组。通过选中列表中的某项，即可在 Available（可用）列中启用该选项。可根据需要不断重复此过程，然后单击添加。 • 输入一个或多个 IP 地址（每行一个），带或不带网络掩码均可。一般格式如下：*<ip_address>/<mask>* • 如需删除地址，请在 Selected（选定）列中将其选中，然后单击 **Delete**（删除），或者选择 **any**（任何），清除所有地址和地址组。 要添加可用于此策略或其他策略的新地址，请单击新建地址。要定义新的地址组，请选择 Objects（对象）> Address Groups（地址组）。
源用户	指定将应用 QoS 策略的源用户和组。
求反	选择此选项可在此选项卡上的指定信息不匹配时应用策略。
Destination 选项卡	
目标区域	选择一个或多个目标区域（默认为 **any**（任何））。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。
目标地址	指定可替代已标识应用程序的 IPv4 或 IPv6 源地址的组合。如需选择特定地址，请从下拉列表中选择 **select**（选择），然后执行以下任意操作： • 在可用列中相应的地址和/或地址组旁，选中此选项，然后将选择项 **Add**（添加）到 选定列。 • 在搜索字段中输入名称的前几个字符，列出所有以这些字符开头的地址和地址组。通过选中列表中的某项，即可在 Available（可用）列中启用该选项。可根据需要不断重复此过程，然后单击添加。 • 输入一个或多个 IP 地址（每行一个），带或不带网络掩码均可。一般格式如下：*<ip_address>/<mask>* • 如需删除地址，请在 Selected（选定）列中将其选中，然后单击 **Delete**（删除），或者选择 **any**（任何），清除所有地址和地址组。 要添加可用于此策略或其他策略的新地址，请单击新建地址。
求反	选择此选项可在此选项卡上的指定信息不匹配时应用策略。
应用程序选项卡	
应用程序	选择 QoS 规则的特定应用程序。要定义新应用程序或应用程序组，请选择 **Objects**（对象）> **Applications**（应用程序）。 如果应用程序具有多项功能，则可以选择整个应用程序或个别功能。如果选择整个应用程序，则所有功能均将包含，而且在将来添加功能时会自动更新应用程序定义。 如果您正在 QoS 规则中使用应用程序组、过滤器或容器，则可以通过将鼠标悬停在应用程序列中的对象上方，查看有关这些对象的详细信息，单击向下箭头并选择 **Value**（值）。此操作可让您直接从策略轻松查看应用程序成员，无需转到 **Objects**（对象）选项卡。
服务/URL 类别选项卡	

© 2019 Palo Alto Networks, Inc.

QoS 策略规则设置	
服务	选择要限制到特定 TCP 和/或 UDP 端口号的服务。从下拉列表中选择以下选项之一： • **any**（任何）— 所选应用程序在任何协议或端口上均得到许可或遭到拒绝。 • **application-default**（应用程序-默认）— 仅在 **Palo Alto Networks** 定义的默认端口上允许或拒绝所选应用程序。建议对允许策略使用此选项。 • **Select**（选择）— 单击 **Add**（添加）。选择现有服务或选择服务或服务组以指定新条目。
URL 类别	选择 QoS 规则的 URL 类别。 • 选择任何将确保无论 URL 类别是什么，会话均可与此 QoS 规则匹配。 • 要指定类别，请单击添加，然后从下拉列表中选择特定类别（包括自定义类别）。您可以添加多个类别。有关定义自定义类别的信息，请参阅 Objects（对象）> External Dynamic Lists（外部动态列表）。
DSCP/TOS 选项卡	
任何	选择 **Any**（任何）（默认设置）可允许策略匹配通信，而不考虑为通信定义的区分化服务代码点 (DSCP) 值或 IP 优先级/服务类型 (ToS)。
代码点	选择代码点以使通信能按定义数据包 IP 标头的 DSCP 或 ToS 值来接收 QoS 处理。DSCP 和 ToS 值用于指明为通信请求的服务级别，如高优先级或尽力交付。使用代码点作为 QoS 策略的匹配标准能让会话根据会话开始时检测到的代码点来接收 QoS 处理。 继续添加 **Add**（添加）代码点可将通信与 QoS 策略匹配： • 为代码点条目分配描述性名称。 • 选择想要用作 QoS 策略匹配标准的代码点类型，然后选择具体的代码点值。您还可以通过输入 **Codepoint Name**（代码点名称）和 **Binary Value**（二进制值）来创建 **Custom Codepoint**（自定义代码点）。
其他设置选项卡	
类	选择要分配到规则的 QoS 类，并单击确定。类特征在 QoS 配置文件中定义。有关配置 QoS 类设置的信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> QoS。
计划	• 选择 **None**（无）以使策略规则始终保持活动状态。 • 从下拉列表中选择 **Schedule**（调度）（日历图标）可设置规则保持活动状态的单个时间范围或重复性时间范围。
目标选项卡（仅限 Panorama）	
任何（针对所有设备）	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备	选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记	**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。

© 2019 Palo Alto Networks, Inc.

QoS 策略规则设置	
针对这些指定的设备和标签之外的所有设备	启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> Policy Based Forwarding（基于策略的转发）

通常，当通信进入防火墙时，将由入口接口虚拟路由器根据目标 IP 地址指出用于确定传出接口和目标安全区域的路由。通过创建基于策略的转发 (PBF) 规则，您可以指定其他信息来确定传出接口，其中包括源区域、源地址、源用户、目标地址、目标应用程序和目标服务。在给定目标 IP 地址和与应用程序关联的端口上的初始会话与应用程序特定规则不匹配，并将根据后续 PBF 规则（不指定应用程序）或虚拟路由器的转发表进行转发。对于同一应用程序，该目标 IP 地址和端口上的所有后续会话均与特定于应用程序的规则匹配。若要确保通过 PBF 规则进行转发，建议不使用特定于应用程序的规则。

需要时，PBF 规则可以用于强制使用 Forward-to-VSYS 转发操作来实现通过其他虚拟系统的通信。在这种情况下，需要定义其他 PBF 规则，用于通过防火墙上的特定出口接口将来自目标虚拟系统的数据包转发出去。

下表介绍了基于策略的转发设置：

- 基于策略的转发常规选项卡
- 基于策略的转发源选项卡
- 基于策略的转发目标/应用程序/服务选项卡
- 基于策略的转发转发选项卡
- （仅限 Panorama）Policy Based Forwarding Target（基于策略的转发目标）选项卡

了解更多？

请参阅基于策略的转发

基于策略的转发常规选项卡

选择 **General**（常规）选项卡可以配置 PBF 策略的名称和说明。此外，也可以配置标记以便在存在大量策略时对其进行排序和过滤。

字段	说明
名称	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
说明	输入策略的说明（最多 1024 个字符）。
标记	如果需要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“入站到 DMZ”来标记某些安全策略，使用关键字“解密”和“不解密”标记解密策略，或者将特定数据中心的名称用于和该位置关联的策略。
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。

© 2019 Palo Alto Networks, Inc.

字段	说明
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。

基于策略的转发源选项卡

选择 **Source**（源）选项卡，可以定义源区域或源地址，用于定义将应用转发策略的传入源流量。

字段	说明
Source Zone（源区域）	如需选择源区域（默认为 any（任何）），请单击 **Add**（添加），并从下拉列表中选择。要定义新区域，请参阅 Network（网络）> Zones（区域）。 多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。 仅基于策略的转发支持第 *3* 层类型区域。
Source Address（源地址）	单击添加可以添加源地址、地址组或地区（默认为任何地区）。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）、**Address Group**（地址组）或 **Regions**（地区），并指定设置。
源用户	单击添加可以选择适用于策略的源用户或用户组。支持以下源用户类型： • 任何 — 无论用户数据怎样，包括任何流量。 • **pre-logon**（预登录）— 包括使用 GlobalProtect™ 连接到网络，但尚未登录到其系统的远程用户。当在 GlobalProtect 应用程序门户网站上配置 Pre-logon（预登录）选项时，可以通过用户名 pre-logon 标识当前尚未登录到自己计算机的所有用户。然后，您可以为预登录用户创建策略，尽管用户没有直接登录，但也可以在域中对其计算机进行身份验证，好像他们已经完全登录。 • 已知用户 — 包括所有已经过身份验证的用户，这意味着包括含有映射的用户数据的所有 IP。此选项相当于域中的“域用户”组。 • 未知 — 包括所有未经身份验证的用户，这意味着包括尚未映射到用户的 IP 地址。例如，您可以使用来宾级别未知访问权限访问内容，因为它们在网络中拥有 IP 地址，但没有对域进行身份验证，且在防火墙上没有 IP 地址到用户的映射信息。 • **select** — 包括由此窗口中的选择项所确定的选定用户。例如，您可能想要添加一个用户、个人列表、一部分组或手动添加用户。 如果防火墙从 *RADIUS*、*TACACS+* 或 *SAML* 标识提供商服务器（而非 *User-ID*™ 代理）收集用户信息，则不会显示用户列表；您必须手动输入用户信息。

基于策略的转发目标/应用程序/服务选项卡

选择 **Destination/Application/Service**（目标/应用程序/服务）选项卡可以定义将要应用到与转发规则匹配的流量的目标设置。

© 2019 Palo Alto Networks, Inc.

字段	说明
目标地址	单击 **Add**（添加）可以添加目标地址或地址组（默认为任何）。默认情况下，规则应用到任何 IP 地址。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）或 **Address Group**（地址组），并指定设置。
应用程序/服务	选择 PBF 规则的特定应用程序或服务。要定义新应用程序，请参阅定义应用程序。要定义应用程序组，请参阅 Objects（对象）> Application Groups（应用程序组）。 不建议将特定于应用程序的规则用于 PBF。如果可行，可使用服务对象，其为协议或应用程序使用的第 *4* 层端口（*TCP* 或 *UDP*）。 您可以通过将鼠标悬停在 **Application**（应用程序）列中的对象上方，单击向下箭头并选择 **Value**（值），查看有关这些应用程序的详细信息。您可以使用此操作直接通过策略轻松查看应用程序信息，无需转到 Object（对象）选项卡。 您不能在 *PBF* 规则中使用自定义应用程序、应用程序过滤器或应用程序组。

基于策略的转发转发选项卡

选择 **Forwarding**（转发）选项卡可以定义将要应用到与转发策略匹配的流量的操作和网络信息。可以将流量转发到下一个跃点 IP 地址、虚拟系统，或者可以丢弃流量。

字段	说明
操作	选择以下任一选项： • 转发— 指定下一个跃点的 IP 地址和出口接口（数据包为到达指定的下一个跃点所使用的接口）。 • **Forward To VSYS**（转发到 **VSYS**）— 从下拉列表中选择要转发到的虚拟系统。 • 丢弃— 丢弃数据包。 • 无 **PBF**— 不改变数据包将采取的路径。此选项可排除与规则中所定义源/目标/应用程序/服务的条件匹配的数据包。匹配数据包使用路由表而非 PBF；防火墙使用路由表从重定向端口排除匹配的流量。 使用 *Forward*（转发）或 *Forward to VSYS*（转发到 *VSYS*）作为操作，这样，您可以应用监控配置文件到流量。（当操作不能转发流量时，不能应用监控配置文件。）对 *IP* 地址实施监控配置文件。如果与 *IP* 地址的连接失败，则监控配置文件指定操作。
出口接口	将数据包引导至特定 Egress 接口。
下一个跃点	如果将数据包引导至特定接口，则采用以下方式之一为此数据包指定下一个跃点：

© 2019 Palo Alto Networks, Inc.

字段	说明
	• **IP Address**（**IP** 地址）— 选择 IP 地址，并选择使用 IPv4 或 IPv6 地址的地址对象（或是创建新地址对象）。 • **FQDN**— 选择 FQDN，并选择使用 FQDN 的地址对象（或是创建新地址对象）。 • **None**（无）—没有下一个跃点；数据包被丢弃。
监视	启用监控来验证目标 **IP** 地址的连接或下一个跃点 IP 地址的连接。选择 **Monitor**（监控）并附加监控 **Profile**（配置文件）（默认或自定义，**Network**（网络）> **Network Profiles**（网络配置文件）> **Monitor**（监控））以指定在 IP 地址无法访问时的操作。 配置监控配置文件，并启用监控，这样，如果入口接口失败或路由中断，防火墙也能在配置文件中执行操作，或是阻止服务中断。
强制对称返回	（非对称路由环境必需项）选择 **Enforce Symmetric Return**（强制对称返回），并在 **Next Hop Address**（下一个跃点地址）列表中输入一个或多个 IP 地址。 启用对称返回，可确保返回流量（例如，从 LAN 上的信任区域传输到 Internet）通过从 Internet 传入流量的相同接口转发出去。
计划	如需限制规则生效的时间和日期，请从下拉列表中选择调度。要定义新调度，请参阅用于控制解密的 SSL 流量的设置。

Policy Based Forwarding Target（基于策略的转发目标）选项卡

- （仅限 Panorama）**Policies**（策略）> **Policy Based Forwarding**（基于策略的转发）> **Target**（目标）

选择 **Target**（目标）选项卡，以选择要将策略规则推送到设备组中的哪一个受管防火墙。您可以通过选择受管防火墙或是指定标记等方式指定要推送到哪一个受管防火墙。此外，您还可以配置策略规则目标，以推送到除指定防火墙以外的所有受管防火墙。

NAT 规则 - 目标设置	说明
任何（针对所有设备）	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备	选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记	**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备	启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> Decryption（解密）

可以将防火墙配置为解密通信以实现可见性、控制和粒度安全性。解密策略可以应用于安全套接字层 (SSL)（包括 IMAP(S)、POP3(S)、SMTP(S) 和 FTP(S) 等 SSL 封装的协议）和安全外壳 (SSH) 流量。SSH 解密可用于解密出站和入站 SSH 流量，以确保安全协议未被用于不允许隧道的应用程序和内容。

添加解密策略规则可定义要解密的流量（例如，您可根据 URL 分类来解密流量）。针对通信按顺序对解密策略规则进行比较，因此特定性更强的规则必须位于一般性更强的规则前面。

如果用户要连接的服务器拥有防火墙信任的 CA 所签署的证书，则 SSL 转发代理的解密过程需要对要呈现给用户的可信证书进行配置。在 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）页面上创建证书，然后单击证书的名称，并选择 **Forward Trust Certificate**（转发信任证书）。

防火墙不会因为它们使用固定证书或客户端身份验证等而解密从技术上破解解密的应用程序。

请参阅排除 SSL 解密的应用程序的列表。

下表介绍了解密策略设置：

- 解密常规选项卡
- 解密源选项卡
- 解密目标选项卡
- 解密服务/URL 类别选项卡
- 解密选项选项卡
- （仅限 Panorama）Decryption Target（解密目标）选项卡

了解更多？

请参阅解密

解密常规选项卡

选择 **General**（常规）选项卡可配置解密策略的名称和说明。此外，也可配置标记，以便在存在许多策略时对其进行排序和过滤。

字段	说明
姓名	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
说明	输入规则的说明（最多 1024 个字符）。
标记	如果需要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“入站到 DMZ”来标记某些安全策略，使用关键字“解密”和“不解密”标记解密策略，或者将特定数据中心的名称用于和该位置关联的策略。

© 2019 Palo Alto Networks, Inc.

字段	说明
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。

解密源选项卡

选择 **Source**（源）选项卡可以定义源区域或源地址，用于定义将要应用到解密策略的传入源流量。

字段	说明
Source Zone（源区域）	单击添加以选择源区域（默认为任何区域）。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅 Network（网络）> Zones（区域）。 多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。
Source Address（源地址）	单击添加可以添加源地址、地址组或地区（默认为任何地区）。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）、**Address Group**（地址组）或 **Regions**（地区），并指定设置。选择 **Negate**（求反）可选择除所配置的地址以外的任何地址。
源用户	单击添加可以选择适用于策略的源用户或用户组。支持以下源用户类型： • 任何 — 无论用户数据怎样，包括任何流量。 • 预登录 — 包括使用 GlobalProtect 连接到网络的远程用户，但尚未登录到自己的系统。当在 GlobalProtect 应用程序门户网站上配置 Pre-logon（预登录）选项时，可以通过用户名 pre-logon 标识当前尚未登录到自己计算机的所有用户。然后，您可以为预登录用户创建策略，尽管用户没有直接登录，但也可以在域中对其计算机进行身份验证，好像他们已经完全登录。 • 已知用户 — 包括所有已经过身份验证的用户，这意味着包括含有映射的用户数据的所有 IP。此选项相当于域中的“域用户”组。 • 未知 — 包括所有未经身份验证的用户，这意味着包括尚未映射到用户的 IP 地址。例如，您可以使用来宾级别访问权限访问未知的内容，因为它们在网络中拥有 IP 地址，但没有对域进行身份验证，且在防火墙上没有用户映射信息的 IP 地址。 • **select** — 包括由此窗口中的选择项所确定的选定用户。例如，您可能想要添加一个用户、个人列表、一部分组或手动添加用户。 如果防火墙从 *RADIUS*、*TACACS+* 或 *SAML* 标识提供商服务器（而非 *User-ID*™ 代理）收集用户信息，则不会显示用户列表；您必须手动输入用户信息。

© 2019 Palo Alto Networks, Inc.

解密目标选项卡

选择 **Destination**（目标）选项卡可以定义目标区域或目标地址，用于定义将要应用到策略的目标流量。

字段	说明
目标区域	单击添加可以选择目标区域（默认为任何区域）。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅Network（网络）> Zones（区域）。 多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。
目标地址	单击添加可以添加目标地址、地址组或地区（默认为任何地区）。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）、**Address Group**（地址组）或 **Regions**（地区），并指定设置。选择 **Negate**（求反）可选择除所配置的地址以外的任何地址。

解密服务/URL 类别选项卡

选择 **Service/URL Category**（服务/**URL** 类别）选项卡可将解密策略应用到基于 TCP 端口号的流量，或应用到任何 URL 类别（或类别列表）。

字段	说明
服务	将解密策略应用到基于特定 TCP 端口号的流量。从下拉列表中选择以下选项之一： • **any**（任何）— 所选应用程序在任何协议或端口上均得到许可或遭到拒绝。 • **application-default**（应用程序-默认）— 仅在 Palo Alto Networks 为应用程序定义的默认端口上解密（或免除解密）所选应用程序。 • **Select**（选择）— 单击 **Add**（添加）。选择现有服务或指定新的服务或服务组。（或选择 Objects（对象）> Services（服务）和 Objects（对象）> Services Groups（服务组））。
URL 类别”选项卡	选择解密规则的 URL 类别。 • 选择任何以匹配任何会话，无论 URL 类型是什么。 • 要指定类别，请单击添加，然后从下拉列表中选择特定类别（包括自定义类别）。您可以添加多个类别。请参阅有关定义自定义类别的信息。

解密选项选项卡

选择 **Options**（选项）选项卡可确定是否应对匹配的流量进行解密。如果设置为解密，可以指定解密类型。您也可以通过配置或选择解密配置文件添加其他解密功能。

© 2019 Palo Alto Networks, Inc.

字段	说明
操作	选择通信的解密或无解密。
类型	从下拉列表中选择要解密的通信类型： • **SSL** 转发代理— 指定策略将解密发往外部服务器的客户端通信。 • **SSH** 代理— 指定策略将解密 SSH 通信。此选项允许您通过指定 ssh-tunnel App-ID 在策略中控制 SSH 隧道。 • **SSL** 入站检查— 指定策略将解密 SSL 入站检查通信。
解密配置文件	将解密配置文件附加到策略规则，以便对通信的某些方面进行阻止和控制。有关创建解密配置文件的详细信息，请参考Objects（对象）> Decryption Profile（解密配置文件）。
日志设置	
记录成功的 SSL 握手	（可选）为成功的 SSL 解密握手创建详细日志。默认情况下禁用。 日志会占用存储空间。在记录成功的 *SSL* 握手之前，必须确保有足够的资源存储日志。编辑*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Logging and Reporting Settings*（记录和报告设置）以检查当前日志内存分配，并为各种日志类型分配内存。
记录失败的 SSL 握手	为失败的 SSL 解密握手创建详细日志，以便您能找到导致解密失败的原因。默认情况下启用。 日志会占用存储空间。若要分配更多（或更少）的日志存储空间给解密日志，请编辑日志内存分配（*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Logging and Reporting Settings*（记录和报告设置））。
日志转发	指定转发 GlobalProtect SSL 握手（解密）日志的方法和位置。

Decryption Target（解密目标）选项卡

- （仅限 Panorama）**Policies**（策略）> **Decryption**（解密）> **Target**（目标）

选择 **Target**（目标）选项卡，以选择要推送策略规则给设备组中的哪一个受管防火墙。您可以通过选择受管防火墙或是指定标记等方式指定要推送给哪一个受管防火墙。此外，您还可以配置策略规则目标，以推送到除指定防火墙以外的所有受管防火墙。

NAT 规则 - 目标设置	说明
任何（针对所有设备）	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备	选择与要推送策略规则的设备组关联的一个或多个受管防火墙。

© 2019 Palo Alto Networks, Inc.

NAT 规则 - 目标设置	说明
标记	**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备	启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> Tunnel Inspection（隧道检测）

您可以配置防火墙，以检测以下明文隧道协议的流量内容：

- 通用路由封装 (GRE)
- 用户数据通用分组无线服务 (GPRS) 隧道协议 (GTP-U)；仅支持 GTP 的防火墙支持。
- 非加密 IPSec 流量（IPSec 和传输模式 AH IPSec 的 NULL 加密算法）
- 虚拟可扩展 LAN (VXLAN)

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）执行安全、DoS 保护和 QoS 策略。

创建特定隧道检测策略，即在匹配传入数据包时，确定防火墙要在数据包中检测的隧道协议，并指定防火墙丢弃或继续处理数据包的条件。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。

防火墙支持对 Ethernet 接口和子接口、AE 接口、VLAN 接口以及 VPN 和 LSVPN 隧道执行隧道内容检测。第 3 层、第 2 层、Virtual Wire 和旁接部署支持此功能。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。

您想了解什么内容？	请参阅：
哪些字段可用于创建隧道检测策略？	隧道检测策略中的构建块
我要如何查看隧道检测日志？	日志类型和严重性级别
了解更多？	隧道内容检测

隧道检测策略中的构建块

选择 **Policies**（策略）> **Tunnel Inspection**（隧道检测）以添加隧道检测策略规则。您可以使用防火墙检测明文隧道协议（GRE、GTP-U、非加密 IPSec 和 VXLAN）的内容，并利用隧道内容检测对这些类型的隧道中的流量执行安全、DoS 保护和 QoS 策略。所有防火墙模型都支持 GRE 和非加密 IPSec 隧道的隧道内容检测，但只有防火墙支持 GTP-U 隧道的 GTP 隧道内容检测。下表介绍了用于配置隧道检测策略的字段。

隧道检测策略中的构建块	配置位置	说明
姓名	**General**（常规）	输入隧道检测策略的名称，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、点或空格字符。
说明		（可选）输入隧道检测策略的说明。
标记		（可选）输入用于报告和记录的一个或多个标记，以标识数据包符合隧道检测策略。

© 2019 Palo Alto Networks, Inc.

隧道检测策略中的构建块	配置位置	说明
使用标记对规则分组		输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。
审核注释		输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档		查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。
Source Zone（源区域）	源	**Add**（添加）应用隧道检测策略的数据包的一个或多个源区域（默认为 **Any**（任何））。
Source Address（源地址）		（可选）**Add**（添加）应用隧道检测策略的数据包的源 IPv4 或 IPv6 地址、地址组或地理区域地址对象（默认为 **Any**（任何））。
源用户		（可选）**Add**（添加）应用隧道检测策略的数据的源用户（默认为 **any**（任何））。
求反		（可选）选择 **Negate**（求反）可选择除指定地址以外的任何地址。
目标区域	目标	**Add**（添加）应用隧道检测策略的数据包的一个或多个目标区域（默认为 **Any**（任何））。
目标地址		（可选）**Add**（添加）应用隧道检测策略的数据包的目标 IPv4 或 IPv6 地址、地址组或地理区域地址对象（默认为 **Any**（任何））。
求反		（可选）选择 **Negate**（求反）可选择除指定地址以外的任何地址。
隧道协议	**Inspection**（检测）	**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。 要从列表中删除协议，请选中协议并将其 **Delete**（删除）。

© 2019 Palo Alto Networks, Inc.

隧道检测策略中的构建块	配置位置	说明
最大隧道检测级别	**Inspection**（检测）> **Inspect Options**（检测选项）	指定防火墙将检测 **One Level**（一个级别）（默认）还是 **Two Levels (Tunnel In Tunnel)**（两个级别（隧道中的隧道））的封装。对于 VXLAN，因为仅在外层进行检测，因此，请选择 **One Level**（一个级别）。
如果超过最大隧道检查级别，则丢弃数据包		（可选）丢弃包含比为最大隧道检测级别指定的更多级别的封装的数据包。
如果隧道协议严格标头检查失败，则丢弃数据包		（可选）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。 如果防火墙使用实现比 *RFC 2890* 更早版本的 *GRE* 的设备实现 *GRE* 隧道，则不要启用此选项。
如果隧道中存在未知协议，则丢弃数据包		（可选）丢弃包含防火墙无法识别的隧道内的协议的数据包。
返回扫描的 VXLAN 隧道到源		（可选）启用此选项，返回流量到原始 VXLAN 隧道端点(VTEP)。例如，使用此选项，返回封装数据包到源 VTEP。仅在第 3 层、第 3 层子接口、第 3 层聚合接口以及 VLAN 得到支持。
启用安全选项	**Inspection**（检测）> **Security Options**（安全选项）	（可选）**Enable Security Options**（启用安全选项）为隧道内容的单独安全策略处理分配安全区域。内部内容来源将属于指定的 **Tunnel Source Zone**（隧道源区域），内部内容目标将属于指定的 **Tunnel Destination Zone**（隧道目标区域）。 如果不 **Enable Security Options**（启用安全选项），则内部内容来源默认属于与外部隧道来源相同的区域，且内部内容目标属于与外部隧道目标相同的区域。因此，内部内容来源和目标都须符合应用于外部隧道的源区域和目标区域的相同安全策略。
隧道源区域		如果 **Enable Security Options**（启用安全选项），则在选中您创建的隧道区域时，内部内容会将此源区域用于策略执行。 否则，内部内容来源默认属于与外部隧道来源相同的区域，且外部隧道源区域的策略同样适用于内部内容源区域。
隧道目标区域		如果 **Enable Security Options**（启用安全选项），则在选中您创建的隧道区域时，内部内容会将此目标区域用于策略执行。 否则，内部内容目标默认属于与外部隧道目标相同的区域，且外部隧道目标区域的策略同样适用于内部内容目标区域。

© 2019 Palo Alto Networks, Inc.

隧道检测策略中的构建块	配置位置	说明
监控名称	**Inspection**（检测）> **Monitor Options**（监控选项）	（可选）输入监控名称以将类似的流量分组在一起，从而监控日志和报告中的流量。
监控标记(数字)		（可选）输入可以将类似流量分组在一起以便记录和报告的监控标记编号（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 *VXLAN* 网络标识符*(VNI)*。
在会话开始时记录		（可选）选择此选项可在符合隧道检测策略的明文隧道会话开始时生成日志。此设置替代适用于会话的安全策略规则中的在会话开始时记录设置。 隧道日志与流量日志分开存储。包含外部隧道会话（GRE、非加密 IPSec 或 GTP-U）的信息存储在隧道日志中，而内部流量流存储在流量日志中。这种分离使您可以轻松报告包含 ACC 和报告功能的隧道活动（而不是内部内容活动）。 隧道日志的最佳做法是在会话开始时记录和在会话结束时记录，因为对于日志记录来说，隧道的存在时间可能非常长。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。如果未选择在会话开始时记录，则将永远无法发现 *ACC* 中存在活动的 *GRE* 隧道。
在会话结束时记录		（可选）选择此选项可在符合隧道检测策略的明文隧道会话结束时捕获日志。此设置替代适用于会话的安全策略规则中的在会话结束时记录设置。
日志转发		（可选）从下拉列表中选择一个日志转发配置文件，以指定转发隧道检测日志的位置。（此设置与适用于流量日志的安全策略规则中的日志转发设置不同。）
姓名	**隧道 ID** 默认情况下，如果未配置 VXLAN ID，则对所有流量进行检测。 如果配置有 VXLAN Id，则可以将其用作匹配标准，限制对特定 VNI 的流量检测。	（可选）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、点或空格字符。**Name**（名称）描述您正在分组的 VNI。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。
VXLAN ID (VNI)		（可选）输入单个 VNI、以逗号分隔的 VNI 列表、最多包含 1600 万个 VNI 的范围（用连字符分隔）、或这些的组合。例如： 1-54,1024,1677011-1677038,94 每个策略的最大 VXLAN ID 数量是 4096。要保存配置内存，请尽可能使用范围。

© 2019 Palo Alto Networks, Inc.

隧道检测策略中的构建块	配置位置	说明
任何（针对所有设备） 仅限 Panorama	目标	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备 仅限 Panorama		选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记 仅限 Panorama		**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备 仅限 Panorama		启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> Application Override（应用程序替代）

要更改防火墙将网络通信分类到应用程序中的方式，可以指定应用程序替代策略。例如，如果要控制一个自定义应用程序，则可以按照区域、源和目标地址、端口和协议，使用应用程序替代策略来标识该应用程序的通信。如果网络应用程序的类别为“unknown”，则可以为其创建新应用程序定义（请参见定义应用程序）。

如果可能，应避免使用应用程序替代策略，因为这会阻止防火墙使用 *App-ID* 标识应用程序，并对威胁执行第 *7* 层检查。要支持互联网专用应用程序，最好是创建包含应用程序签名的自定义应用程序，这样，防火墙可对执行第 *7* 层检查，并对应用程序流量进行扫描，以查找威胁。如果商业应用程序不包含 *App-ID*，则提交新的 App-ID 请求。如果公共应用程序定义（默认端口或签名）发生更改，则防火墙不再能正确标识应用程序，请创建支持票据，这样，*Palo Alto Networks* 就可以更新定义。同时创建自定义应用程序，以便防火墙继续对流量执行第 *7* 层检查。

安全策略一样，根据需要，应用程序替代策略可以是一般的，也可以是特定的。针对通信按顺序对策略规则进行比较，因此特定性更强的规则必须位于一般性更强的规则前面。

因为 PAN-OS 中的应用程序 ID 引擎通过在网络通信中识别特定于应用程序的内容来对通信进行分类，所以自定义应用程序定义不能简单地只使用端口号来标识应用程序。应用程序定义还必须包括通信（受到源区域、源 IP 地址、目标区域和目标 IP 地址的限制）。

要创建包含应用程序替代的自定义应用程序，请执行以下操作：

- 创建自定义应用程序（请参阅定义应用程序）。如果应用程序仅用于应用程序替代规则，则无需为应用程序指定签名。
- 定义应用程序替代策略，以指定应当调用自定义应用程序的时间。策略通常包括运行自定义应用程序的服务器的 IP 地址和一组受限的源 IP 地址或一个源区域。

使用下表配置应用程序替代规则。

- 应用程序替代常规选项卡
- 应用程序替代源选项卡
- 应用程序替代目标选项卡
- 应用程序替代协议/应用程序选项卡
- （仅限 Panorama）Application Override Target（应用程序覆盖目标）选项卡

了解更多？

请参阅在策略中使用应用程序对象

应用程序替代常规选项卡

选择 **General**（常规）选项卡可配置应用程序替代策略的名称和说明。此外，也可以配置标记以便在存在大量策略时对其进行排序和过滤。

字段	说明
姓名	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。

© 2019 Palo Alto Networks, Inc.

字段	说明
说明	输入规则的说明（最多 1024 个字符）。
标记	如果需要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“入站到 DMZ”来标记某些安全策略，使用关键字“解密”和“不解密”标记解密策略，或者将特定数据中心的名称用于和该位置关联的策略。
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据 **Tag**（标记）选择组规则。
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。审核注释存档可采用 CSV 格式导出。

应用程序替代源选项卡

选择 **Source**（源）选项卡可定义源区域或源地址，用于定义将要应用到应用程序替代策略的传入源流量。

字段	说明
Source Zone（源区域）	**Add**（添加）源区域（默认为 **any**（任何））。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅Network（网络）> Zones（区域）。 多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。
Source Address（源地址）	**Add**（添加）源地址、地址组或地区（默认为 **any**（任何））。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）、**Address Group**（地址组）或 **Regions**（地区），并指定设置。 选择 **Negate**（求反）可选择除所配置的地址以外的任何地址。

应用程序替代目标选项卡

选择 **Destination**（目标）选项卡可以定义目标区域或目标地址，用于定义将要应用到策略的目标流量。

字段	说明
目标区域	单击添加可以选择目标区域（默认为任何区域）。区域类型必须相同（第 2 层、第 3 层或虚拟线路）。要定义新区域，请参阅Network（网络）> Zones（区域）。

© 2019 Palo Alto Networks, Inc.

字段	说明
	多个区域可以用于简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。
目标地址	单击添加可以添加目标地址、地址组或地区（默认为任何地区）。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）、**Address Group**（地址组）或 **Regions**（地区），并指定设置。 选择 **Negate**（求反）可选择除所配置的地址以外的任何地址。

应用程序替代协议/应用程序选项卡

选择 **Protocol/Application**（协议/应用程序）选项卡可定义协议（TCP 或 UDP）、端口和应用程序，用于进一步定义与策略匹配的应用程序的属性。

字段	说明
协议	选择允许应用程序替代的协议（**TCP** 或 **UDP**）。
端口	输入指定目标地址的端口号（0 到 65535）或端口号范围 (port1-port2)。多个端口或范围必须以逗号分隔。
应用程序	为匹配上述规则条件的通信流选择替代应用程序。替代为自定义应用程序时，不会执行任何威胁检查。但替代为支持威胁检查的预定义应用程序除外。 要定义新应用程序，请参阅 Objects（对象）> Applications（应用程序））。

Application Override Target（应用程序覆盖目标）选项卡

- （仅限 Panorama）**Policies**（策略）> **Application Override**（应用程序覆盖）> **Target**（目标）

选择 **Target**（目标）选项卡，以选择要推送策略规则给设备组中的哪一个受管防火墙。您可以通过选择受管防火墙或是指定标记等方式指定要推送给哪一个受管防火墙。此外，您还可以配置策略规则目标，以推送到除指定防火墙以外的所有受管防火墙。

NAT 规则 - 目标设置	说明
任何（针对所有设备）	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备	选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记	**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备	启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> Authentication（身份验证）

身份验证策略可让您在最终用户访问网络资源之前验证他们的身份。

您想了解什么内容？	请参阅：
哪些字段可用于创建身份验证规则？	身份验证策略规则中的构建块
我要如何使用 Web 界面管理身份验证策略？	创建和管理身份验证策略 对于 Panorama，请参阅移动或克隆策略规则
了解更多？	身份验证策略

身份验证策略规则中的构建块

每当用户请求资源时（如访问网页时），防火墙都会评估身份验证策略。根据匹配策略规则，防火墙会提示用户对登录和密码、语音、短信、推送或一次性密码 (OTP) 身份验证等不同因素（类型）的一个或多个挑战作出响应。在用户对所有因素作出响应后，防火墙会评估安全策略（请参阅 Policies（策略）> Security（安全））以确定是否允许访问资源。

如果用户通过内部或隧道模式下的 GlobalProtect™ 网关访问非基于 *Web* 的资源（如打印机），则防火墙不会提示他们进行身份验证。相反，用户将会看到连接失败消息。要确保用户可以访问这些资源，需要设置一个身份验证门户，并培训用户在看到连接失败时进行访问。请咨询您的 *IT* 部门以设置身份验证门户。

下表介绍了身份验证策略规则中的每个构建块或组件。在添加规则之前，请完成创建和管理身份验证策略中所述的先决条件。

身份验证规则的构建块	配置位置	说明
规则号	N/A	每个规则会自动编号，并且顺序会随着规则的移动改变。在筛选规则以匹配特定筛选程序时，**Policies**（策略）> **Authentication**（身份验证）页面会将每个规则连同其在规则库中整组规则上下文中的编号及其在评估顺序中的位置一起列出。有关详细信息，请参阅规则顺序及其评估顺序。
姓名	**General**（常规）	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
说明		输入规则的说明（最多 1024 个字符）。
标记		选择用于排序和过滤规则的标记（请参阅 Objects（对象）> Tags（标记））。

© 2019 Palo Alto Networks, Inc.

身份验证规则的构建块	配置位置	说明
使用标记对规则分组		输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。
审核注释		输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档		查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。
Source Zone（源区域）	源	**Add**（添加）区域以将规则仅应用于来自您指定的区域中的接口的流量（默认为 **any**（任何））。 要定义新区域，请参阅 Network（网络）> Zones（区域）。
Source Address（源地址）		**Add**（添加）地址或地址组以将规则仅应用于来自您指定的源的流量（默认为 **any**（任何））。 选择 **Negate**（求反）可选择除所选地址以外的任何地址。 要定义新的地址或地址组，请参阅 Objects（对象）> Addresses（地址）和 Objects（对象）> Address Groups（地址组）。
源用户	用户	选择应用规则的源用户或用户组： • **any**（任何）— 无论源用户怎样，包括任何流量。 • **pre-logon**（预登录）— 包括未登录到其客户端系统，但其客户端系统通过 GlobalProtect 预登录功能连接到网络的远程用户。 • **known-user**（已知用户）— 包括其防火墙在规则引发身份验证之前已经拥有 IP 地址到用户名映射的所有用户。 • **unknown**（未知）— 包括其防火墙不具有 IP 地址到用户名映射的所有用户。在规则引发身份验证后，防火墙将根据未知用户输入的用户名为其创建用户映射。 • **Select**（选择）— 仅包括 **Add**（添加）到源用户列表的用户和用户组。 如果防火墙从 *RADIUS*、*TACACS+* 或 *SAML* 标识提供商服务器（而非 *User-ID*™ 代理）收集用户信息，则不会显示用户列表；您必须手动输入用户信息。
源 HIP 配置文件		**Add**（添加）主机信息配置文件 (HIP) 可让您收集有关终端主机安全状态的信息，例如终端主机是否有最新的安全修补程序和防病毒定义。有关详细信息和要定义新的 HIP，请参阅 Objects（对象）> GlobalProtect > HIP Profiles（HIP 配置文件）。

© 2019 Palo Alto Networks, Inc.

身份验证规则的构建块	配置位置	说明
目标区域	目标	**Add**（添加）区域以将规则仅应用于流向您指定的区域中的接口的流量（默认为 **any**（任何））。要定义新区域，请参阅 Network（网络）> Zones（区域）。
目标地址		**Add**（添加）地址或地址组以将规则仅应用于您指定的目标（默认为 **any**（任何））。 选择 **Negate**（求反）可选择除所选地址以外的任何地址。 要定义新的地址或地址组，请参阅 Objects（对象）> Addresses（地址）和 Objects（对象）> Address Groups（地址组）。
服务	服务/**URL** 类别	选择以下选项以将规则仅应用于特定 TCP 和 UDP 端口号的服务： • **any**（任何）— 指定任何端口上并使用任何协议的服务。 • **default**（默认）— 仅指定 Palo Alto Networks 定义的默认端口上的服务。 • **Select**（选择）— 能让您 **Add**（添加）服务或服务组。要创建新的服务和服务组，请参阅 Objects（对象）> Services（服务）和 Objects（对象）> Service Groups（服务组）。 默认选择是 *service-http*。使用身份验证门户的身份验证策略时，还要启用 *service-https* ，确保防火墙知悉所有 *Web* 流量的用户到 *IP* 地址映射。
URL 类别		选择要应用规则的 URL 类别： • 选择 **any**（任何）以指定所有流量，而不考虑 URL 类别。 • **Add**（添加）类别。要定义自定义类别，请参阅 Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）。
身份验证执行	操作	选择指定防火墙用于对用户进行身份验证的方法（如身份验证门户或浏览器质询）和身份验证配置文件的身份验证执行对象（Objects（对象）> Authentication（身份证验））。身份验证配置文件定义用户是对单个质询还是对多因素身份验证响应（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。您可以选择预定义或自定义的身份验证执行对象。 如果必须排除身份验证门户策略中的主机或服务器，则将其添加到身份验证配置文件，以指定 *no-captive-portal* 作为 *Authentication Enforcement*（身份验证执行）。但是，身份验证门户策略有助于防火

© 2019 Palo Alto Networks, Inc.

身份验证规则的构建块	配置位置	说明
		墙知悉用户到 *IP* 地址的映射，并应尽可能使用。
超时		要减少可能会中断用户工作流程的身份验证质询的步骤，您可以指定当防火墙提示用户仅对重复访问资源进行一次身份验证的时间间隔（分钟）（默认为 60）。 如果 **Authentication Enforcement**（身份验证执行）对象指定多因素身份验证，则用户必须对每个因素进行一次身份验证。防火墙记录时间戳，并且只有当因素的超时到期后才能重新发出质询。将时间戳重新分发给其他防火墙能让您应用超时，即使最初允许用户访问的防火墙与以后控制该用户访问的防火墙不同。 *Timeout*（超时）是更严格的安全（身份验证提示之间的时间更短）和用户体验（身份验证提示之间的时间更长）之间的权衡。访问关键系统和敏感区域（例如数据中心）时，进行更频繁的身份验证通常是很正确的选择。在网络外围设备以及对于用户体验为核心的业务，进行更少的身份验证往往是比较正确的选择。 对于外围资源，将值设为 *480* 分钟（*8* 小时）；对于数据中心资源和关键系统，设一个最小的值，例如 *60* 分钟，以加强安全性。监控该值，并根据需要进行调整。
日志身份验证超时		如果您希望防火墙在与身份验证因素相关联的 **Timeout**（超时）到期后生成身份验证日志，则请选择此选项（默认禁用）。启用此选项可提供更多数据来解决访问问题。结合关联对象，您还可以使用身份验证日志识别网络中的可疑活动（如暴力攻击）。 启用此选项会增加日志流量。
日志转发		如果您希望防火墙将身份验证日志转发到 Panorama 或外部服务（如 syslog 服务器）（请参阅 Objects（对象）> Log Forwarding（日志转发）），请选择日志转发配置文件。
任何（针对所有设备） 仅限 Panorama	目标	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备 仅限 Panorama		选择与要推送策略规则的设备组关联的一个或多个受管防火墙。

© 2019 Palo Alto Networks, Inc.

身份验证规则的构建块	配置位置	说明
标记 仅限 Panorama		**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备 仅限 Panorama		启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

创建和管理身份验证策略

选择 **Policies**（策略）> **Authentication**（身份验证）页面可创建和管理身份验证策略规则：

任务	说明
添加	在创建身份验证策略规则前，请执行以下先决条件： □ 配置 User-ID™ 身份验证门户设置（请参阅 Device（设备）> User Identification（用户标识）> Authentication Portal Settings（身份验证门户设置））。防火墙使用身份验证门户显示身份验证规则需要的第一个身份验证因素。身份验证门户还使防火墙能够记录与身份验证超时时间段相关的时间戳并更新用户映射。 □ 配置服务器配置文件，以指定防火墙如何访问将对用户进行身份验证的服务（请参阅 Device（设备）> Server Profiles（服务器配置文件））。 □ 为指定身份验证设置（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））的身份验证配置文件分配服务器配置文件。 □ 为指定身份验证方法（请参阅 Objects（对象）> Authentication（身份验证））的身份验证执行对象分配身份验证配置文件。 要创建规则，请执行下列步骤之一，然后填写身份验证策略规则中的构建块中所述的字段： • 单击添加。 • 选择新规则要基于的规则，然后单击 **Clone Rule**（克隆规则）。防火墙将复制的规则（名为 <rulename>#）插入到所选规则的下面，其中 # 为使规则名称保持唯一的下一个可用整数，然后为克隆的规则生成一个新的 UUID。有关详细信息，请参阅移动或克隆策略规则。
修改	要修改规则，单击规则名称，然后编辑身份验证策略规则中的构建块中所述的字段。 如果防火墙收到来自 *Panorama* 的规则，则该规则为只读；您只能在 *Panorama* 上进行编辑。
移动	匹配流量时，防火墙按 **Policies**（策略）> **Authentication**（身份验证）页面列出的自上而下顺序评估规则。要更改评估顺序，请选择一个规则，然后单击 **Move Up**（上移）、**Move Down**（下移）、**Move Top**（移至顶部）或 **Move Bottom**（移至底部）。有关详细信息，请参阅移动或克隆策略规则。
删除	要删除现有规则，请将其选定并单击 **Delete**（删除）。

© 2019 Palo Alto Networks, Inc.

任务	说明
启用/禁用	要禁用规则，请将其选定并单击 **Disable**（禁用）。要重新启用禁用的规则，请将其选定并单击 **Enable**（启用）。
突出显示未使用的规则	要识别自防火墙最近一次重启后尚未匹配的流量，请选择 **Highlight Unused Rules**（突出显示未使用的规则）。然后，可以决定是禁用还是删除未使用的规则。该页面使用虚线黄色背景突出显示未使用的规则。
预览规则（仅限 Panorama）	单击 **Preview Rules**（预览规则）可查看在将规则推送到受管防火墙之前的规则列表。在每个规则库中，页面直观显示每个设备组（和受管防火墙）的规则层次结构，以便扫描众多规则。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> DoS Protection（DoS 保护）

DoS 保护策略可让您保护单个关键资源免遭 DoS 攻击，只需指定是拒绝还是允许与源接口、区域、地址或用户和/或目标接口、区域或用户匹配的数据包即可。

或者，您也可以选择保护操作，指定一个 DoS 配置文件，您可在其中设置触发警报、激活保护操作的阈值（每秒会话数或数据包数），并指出丢弃所有新连接需要超过的最高速率。因此，您可以根据聚合会话或者源和/或目标 IP 地址控制接口、区域、地址和国家/地区之间的会话数。例如，您可以控制发送到和来自特定地址或地址组的流量，或者来自特定用户和适用于特定服务的流量。

防火墙会在执行安全策略规则之前先执行 DoS 保护策略规则，以确保最有效地使用其资源。如果 DoS 保护策略规则拒绝了某数据包，则此数据包决不会进入安全策略规则匹配阶段。

下表介绍了 DoS 保护策略设置：

- DoS 保护常规选项卡
- DoS 保护源选项卡
- DoS 保护目标选项卡
- DoS 保护选项/保护选项卡
- （仅限 Panorama）DoS Protection Target（DoS 保护目标）选项卡

了解更多？

请参阅 DoS 保护配置文件 和 Objects（对象）> Security Profiles（安全配置文件）> DoS Protection（DoS 保护）。

DoS 保护常规选项卡

- **Policies**（策略）> **DoS Protection**（**DoS** 保护）> **General**（常规）

选择 **General**（常规）选项卡可配置 DoS 保护策略的名称和说明。此外，也可配置标记，以便在存在许多策略时对其进行排序和过滤。

字段	说明
姓名	输入标识 DoS 保护策略规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
说明	输入规则的说明（最多 1024 个字符）。
标记	如果要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您已定义许多策略，并且希望查看用特定关键字标记的策略，则标记非常有用。例如，您可能希望使用 Inbound to DMZ（入站到 DMZ）标记某些安全策略，使用关键字 Decrypt（解密）或 No-decrypt（不解密）标记解密策略，或者将特定数据中心的名称用于和该位置关联的策略。
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据**Tag**（标记）选择组规则。

© 2019 Palo Alto Networks, Inc.

字段	说明
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。您可以采用 CSV 格式导出“审核注释存档”。

DoS 保护源选项卡

选择 **Source**（源）选项卡可定义源接口或源区域，以及可选的源地址和源用户，用于定义要应用 DoS 策略规则的传入流量。

字段	说明
类型	选择要应用 DoS 保护策略规则的源类型： • **Interface**（接口）— 将规则应用于来自指定接口或接口组的流量。 • **Zone**（区域）— 将规则应用于来自指定区域中任何接口的流量。 单击 **Add**（添加）可选择多个接口或区域。
Source Address（源地址）	选择 **Any**（任何）或 **Add**（添加），然后指定要应用 DoS 保护策略规则的一个或多个源地址。 （可选）选择 **Negate**（求反）以指定将规则应用于除指定地址以外的任何地址。
源用户	选择要应用 DoS 保护策略规则的一个或多个源用户： • **any**（任何）— 无论源用户怎样，都包括数据包。 • **pre-logon**（预登录）— 包括来自使用 GlobalProtect 连接到网络的远程用户的数据包，但尚未登录到自己的系统。当在 GlobalProtect 应用程序门户网站上配置 **pre-logon**（预登录）选项时，可以通过用户名 pre-logon 识别当前尚未登录到自己计算机的所有用户。然后，您可以为预登录用户创建策略，尽管用户没有直接登录，但也可以在域中对其计算机进行身份验证，好像他们已经完全登录。 • **known-user**（已知用户）— 包括所有已经过身份验证的用户，这意味着包括含有映射的用户数据的所有 IP 地址。此选项相当于域中的“域用户”组。 • 未知 — 包括所有未经身份验证的用户，这意味着包括尚未映射到用户的 IP 地址。例如，您可以使用来宾级别 **unknown**（未知）访问权限访问内容，因为它们在网络中拥有 IP 地址，但没有对域进行身份验证，且在防火墙上没有 IP 地址到用户名的映射信息。 • **Select**（选择）— 包括在此窗口中指定的用户。例如，您可以选择一个用户、个人列表、一部分组或手动添加用户。 如果防火墙从 *RADIUS*、*TACACS+* 或 *SAML* 标识提供商服务器（而非 *User-ID*™ 代理）收集用户信息，则不会显示用户列表；您必须手动输入用户信息。

DoS 保护目标选项卡

选择 **Destination**（目标）选项卡可以定义目标区域或接口和目标地址，用于定义要应用策略的目标流量。

© 2019 Palo Alto Networks, Inc.

字段	说明
类型	选择要应用 DoS 保护策略规则的目标类型： • **Interface**（接口）— 将规则应用于指向指定接口或接口组的数据包。单击 **Add**（添加），然后选择一个或多个接口。 • **Zone**（区域）— 将规则应用于指向指定区域中任何接口的数据包。单击 **Add**（添加），然后选择一个或多个区域。
目标地址	选择 **Any**（任何）或 **Add**（添加），然后指定要应用 DoS 保护策略规则的一个或多个目标地址。 （可选）选择 **Negate**（求反）以指定将规则应用于除指定地址以外的任何地址。

DoS 保护选项/保护选项卡

选择 **Option/Protection**（选项/保护）选项卡可配置 DoS 保护策略规则的选项，例如，要应用规则的服务类型、要针对与规则相匹配的数据采取的操作，以及是否为匹配的流量触发日志转发。您可以定义当规则处于活动状态时的计划。

此外，您还可以选择聚合 DoS 保护配置文件和/或分类的 DoS 保护配置文件，以确定可导致防火墙采取保护措施（如触发警报）、激活某个操作（如随机早期丢弃）以及丢弃超过最大阈值速率的数据包的阈值速率（如果超出）。

字段	说明
服务	单击 **Add**（添加），然后选择一个或多个要应用 DoS 保护策略的服务。默认为 **Any**（任何）服务。例如，如果 DoS 策略保护 Web 服务器，请为 Web 应用程序指定 HTTP、HTTPS 和任何其他适当的服务端口. 对于关键服务器，创建单独的 *DoS* 保护规则保护未使用服务端口，以帮助防止有针对性的攻击。
操作	选择防火墙对与 DoS 保护策略规则相匹配的数据包执行的操作： • **Deny**（拒绝）— 丢弃与规则相匹配的所有数据包。 • **Allow**（允许）— 允许与规则相匹配的所有数据包。 • **Protect**（保护）—强制实施与规则匹配的数据包上指定 DoS 保护配置文件内指定的保护。将与规则相匹配的数据包计入 DoS 保护配置文件中的阈值速率，从而触发警报、激活其他操作以及在超出最大速率时触发数据包丢弃。 应用 *DoS* 保护的对象旨在保护 *DoS* 攻击，因此，您通常应使用 *Protect*（保护）。*Deny*（拒绝）丢弃合法流量和 *DoS* 流量， 而 *Allow*（允许）不会停止 *DoS* 攻击。仅在组内处理例外时使用 *Deny*（拒绝）和 *Allow*（允许）。例如，您可以拒绝来自大多数组的流量，但允许该流量的子集，或是允许来自大多数组的流量，但拒绝该流量的子集。
计划	指定当 DoS 保护策略规则生效时的计划。默认设置为 **None**（无），表示无计划；策略始终有效。 或者，选择一个计划或创建新计划，以控制 DoS 保护策略规则生效的时间。输入计划的 **Name**（名称）。选择 **Shared**（共享）可与多个虚拟系统防火墙上的每个虚拟系统共享此计

© 2019 Palo Alto Networks, Inc.

字段	说明
	划。选择 **Daily**（每天）、**Weekly**（每周）或 **Non-recurring**（非重复）的 **Recurrence**（重复）。采用 24 小时制 (HH:MM) 添加 **Start Time**（开始时间）和 **End Time**（结束时间）。
日志转发	如果您想要触发将匹配流量的威胁日志条目转发到外部服务（如 Syslog 服务器或 Panorama），请选择日志转发配置文件，或单击 **Profile**（配置文件）以创建新的转发配置文件。 防火墙仅记录和转发与规则中操作匹配的流量。 为了便于管理，分开转发来自其他威胁日志的 *DoS* 日志，并将其通过电子邮件直接发送给管理员和日志服务器。
聚合	聚合 DoS 保护配置文件设置适用于 DoS 保护规则内指定的组合设备组的阈值，以保护这些服务器组。例如，10000 CPS 的警报速率阈值意味着当整组的新 CPS 总数超过 10000 CPS 时，防火墙触发警报消息。 选择一个聚合 DoS 保护配置文件，该配置文件指定传入连接数/秒触发警报、激活操作并超过最大速率的阈值速率。所有传入连接都（聚合）计入聚合 DoS 保护配置文件中指定的阈值。 聚合配置文件设置为 **None**（无），表示没有适用于聚合流量的阈值设置。请参阅 Objects（对象）> Security Profiles（安全配置文件）> DoS Protection（DoS 保护）。
分类	分类 DoS 保护配置文件设置适用于 DoS 保护规则内指定的每个单独设备的阈值，以保护单个或一小组的关键服务器。例如，10000 CPS 的警报速率阈值意味着当规则中指定的任何单个服务器的新 CPS 总数超过 10000 CPS 时，防火墙触发警报消息。 选择此选项，然后指定以下各项： • **Profile**（配置文件）— 选择要应用于此规则的分类 DoS 保护配置文件。 • **Address**（地址）— 选择是否将传入连接数计入配置文件中的阈值（如果这些阈值与 **source-ip-only**、**destination-ip-only** 或 **src-dest-ip-both** 相匹配）。 防火墙在跟踪 *src-dest-ip-both* 计数器时消耗的资源大于仅跟踪源 *IP* 或仅跟踪目标 *IP* 计数器时消耗的资源。 如果指定分类 DoS 保护配置文件，则仅将与源 IP 地址、目标 IP 地址或源和目标 IP 地址对相匹配的传入连接数计入配置文件中指定的阈值。例如，可以按 **Max Rate**（最大速率）为 100 cps 指定分类 DoS 保护配置文件，并在规则中指定 **source-ip-only** 的 **Address**（地址）设置。结果是将该特定源 IP 地址限制为每秒 100 次连接。 因为防火墙无法存储所有可能的互联网 *IP* 地址计数器，因此，请勿将 *source-ip-only* 或 *src-dest-ip-both* 用于面向互联网的区域。在周边区域中使用 *destination-ip-only*。 使用 *destination-ip-only* 保护单个关键设备。 使用 *source-ip-only* 和 *Alarm*（警报）阈值监控非面向互联网区域中的可疑主机。 请参阅 Objects（对象）> Security Profiles（安全配置文件）> DoS Protection（DoS 保护）。

© 2019 Palo Alto Networks, Inc.

DoS Protection Target（DoS 保护目标）选项卡

- （仅限 Panorama）**Policies**（策略）> **DoS Protection**（**DoS** 保护）> **Target**（目标）

选择 **Target**（目标）选项卡，以选择要将策略规则推送到设备组中的哪一个受管防火墙。您可以通过选择受管防火墙或是指定标记等方式指定要推送到哪一个受管防火墙。此外，您还可以配置策略规则目标，以推送到除指定防火墙以外的所有受管防火墙。

NAT 规则 - 目标设置	说明
任何（针对所有设备）	启用（勾选）以推送策略规则到设备组中所有受管防火墙。
设备	选择与要推送策略规则的设备组关联的一个或多个受管防火墙。
标记	**Add**（添加）一个或多个标记，以通过特定标记将策略规则推送到设备组的受管防火墙。
针对这些指定的设备和标签之外的所有设备	启用（勾选）以推送策略规则到与设备组关联的所有受管防火墙（选中的设备和标记除外）。

© 2019 Palo Alto Networks, Inc.

Policies（策略）> SD-WAN

添加 SD-WAN 策略以根据每个应用程序配置链路路径管理设置，或是根据您配置的运行状况抖动、延迟和数据包丢失运行状况指标，为遍历相同链路的一组应用程序配置链路路径管理设置。当关键应用程序的源和目标之间的某些路径经历降级时，SD-WAN 策略规则将选择新的最佳路径，确保敏感和关键应用程序会根据在 SD-WAN 策略规则中为其分配的路径质量配置文件执行。

- SD-WAN“General”（常规）选项卡
- SD-WAN“Source”（源）选项卡
- SD-WAN“Destination”（目标）选项卡
- SD-WAN“Application/Service”（应用程序/服务）选项卡
- SD-WAN“Path Selection”（路径选择）选项卡
- （仅限 Panorama）SD-WAN“Target”（目标）选项卡

SD-WAN“General”（常规）选项卡

- **Policies**（策略）> **SD-WAN** > **General**（常规）

选择 **General**（常规）选项卡，以配置 SD-WAN 策略的名称和说明。此外，也可以配置标记以便在存在大量策略时对其进行排序和过滤。

字段	说明
名称	输入标识规则的名称。名称区分大小写，最多可以包含 63 个字符，可以是字母、数字、空格、连字符和下划线。名称在防火墙上必须是唯一的，并且在 Panorama 上，在其设备组以及所有父对象或子对象设备组中必须是唯一的。
说明	输入规则的说明（最多 1,024 个字符）。
标记	如果需要标记策略，请 **Add**（添加）并指定标记。 策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能想用唯一的标签来标记某些 SD-WAN 策略，而这些标签用于标识应用规则的特定中心或分支。
使用标记对规则分组	输入标记，对类似策略规则进行分组。通过组标记，您可以查看基于这些标记的策略规则库。您可以根据 **Tag**（标记）选择组规则。
审核注释	输入注释，以审核策略规则的创建或编辑情况。审核注释区分大小写，最多可以包含 256 个字符，可以是字母、数字、空格、连字符和下划线。
审核注释存档	查看策略规则先前使用的**Audit Comments**（审核注释）。审核注释存档可采用 CSV 格式导出。

SD-WAN“Source”（源）选项卡

- **Policies**（策略）> **SD-WAN** > **Source**（源）

选择 **Source**（源）选项卡，以定义源区域、源地址以及源用户，而这些内容定义了 SD-WAN 策略适用的传入数据包。

© 2019 Palo Alto Networks, Inc.

字段	说明
Source Zone（源区域）	要指定源区域，请选择 **Add**（添加），然后选择一个或多个区域，或者选择 **Any**（任何）区域。 指定多个区域可以简化管理。例如，若在不同的区域中有三个分支，并且希望这三个分支的其余匹配条件和路径选择相同，则可创建一个 SD-WAN 规则，并指定三个源区域来涵盖这三个分支。 *SD-WAN 策略规则仅支持第 3 层类型的区域。*
Source Address（源地址）	要指定源地址，请 **Add**（添加）源地址或外部动态列表 (EDL)，从下拉列表中选择，或者选择 **Address**（地址），然后创建一个新的地址对象。或者，选择 **Any**（任何）源地址（默认）。
源用户	要指定特定用户，请选择 **Add**（添加）（相应类型随后指示 **select**（选择）），输入用户、用户列表或用户组。或者，选择用户类型： • **any**（任何）—（默认）包括任何用户，不受用户数据影响。 • **pre-logon**（预登录）— 包括使用 GlobalProtect™ 连接到网络但尚未登录到其系统的远程用户。当在 GlobalProtect 应用程序门户网站上配置 Pre-logon（预登录）选项时，可以通过用户名 pre-logon 标识当前尚未登录到自己计算机的所有用户。然后，您可以为预登录用户创建策略，尽管用户没有直接登录，但也可以在域中对其计算机进行身份验证，好像他们已经完全登录。 • **known-user**（已知用户）— 包括所有已经过身份验证的用户，这意味着包括含有映射的用户数据的所有 IP 地址。此选项相当于域中的“域用户”组。 • 未知 — 包括所有未经身份验证的用户，这意味着包括尚未映射到用户的 IP 地址。例如，您可以选择 **unknown**（未知）来宾级别的访问权限访问内容，因为它们在网络中拥有 IP 地址，但没有向域验证身份，且在防火墙上没有 IP 地址到用户的映射信息。 *如果防火墙从 RADIUS、TACACS+ 或 SAML 标识提供商服务器（而非 User-ID™ 代理）收集用户信息，则不会显示用户列表；您必须手动输入用户信息。*

SD-WAN“Destination”（目标）选项卡

- **Policies**（策略）> **SD-WAN** > **Destination**（目标）

选择 **Destination**（目标）选项卡可以定义目标区域或目标地址，从而定义要应用 SD-WAN 策略规则的流量。

字段	说明
目标区域	**Add**（添加）目标区域（默认为任何）。区域必须为第 3 层。要定义新区域，请参阅 Network（网络）> Zones（区域）。 添加多个区域，以简化管理。例如，如果有三个不同内部区域（市场部、销售部和公关部）都定向到非受信目标区域，则可以创建一个涵盖所有情况的规则。

© 2019 Palo Alto Networks, Inc.

字段	说明
目标地址	**Add**（添加）目标地址、地址组、外部动态列表 (EDL) 或地区（默认为 **Any**（任何））。从下拉列表中选择，或在下拉列表的底部单击 **Address**（地址）或 **Address Group**（地址组），并指定设置。 选择 **Negate**（求反）可选择除所配置的地址以外的任何地址。

SD-WAN“Application/Service”（应用程序/服务）选项卡

- **Policies**（策略）> **SD-WAN** > **Application/Service**（应用程序/服务）

选择 **Application/Service**（应用程序/服务）选项卡以指定应用 SD-WAN 策略规则的应用程序或服务，并指定应用到应用程序或服务的配置文件（路径质量、SaaS 质量和纠错配置文件）。

字段	说明
路径质量配置文件	选择路径质量配置文件，用于确定要应用于指定应用程序和服务的最大抖动、延迟和数据包丢失百分比阈值。若尚未创建路径质量配置文件，可创建 **New SD-WAN Path Quality Profile**（新 **SD-WAN** 路径质量配置文件）。
SaaS 质量配置文件	选择 SaaS 质量配置文件以指定具有软件即服务(SaaS)应用程序直接互联网访问(DIA)链路的中心或分支防火墙的延迟、抖动和数据包丢失的路径质量阈值。若尚未创建 SaaS 质量配置文件，可创建 **New SaaS Quality Profile**（新 **SaaS** 质量配置文件）。默认为 **None**（无）（已禁用）。
纠错配置文件	选择 **Error Correction Profile**（纠错配置文件）或创建新的 纠错配置文件，以指定用于控制规则中所指定应用程序或服务的前向纠错 (FEC) 或路径重复的参数。此配置文件既可用于中心防火墙，也可用于分支防火墙。默认为 **None**（无）（已禁用）。
应用程序	为 SD-WAN 策略规则 **Add**（添加）特定应用程序，或选择 **Any**（任何）。如果应用程序具有多项功能，则选择整个应用程序或个别功能。如果选择整个应用程序，则所有功能均将包含，而且在将来添加功能时会自动更新应用程序定义。 如果在 SD-WAN 策略规则中使用应用程序组、过滤器或容器，则通过将鼠标悬停在应用程序列中的对象上方，打开下拉列表，然后选择 **Value**（值）来查看这些对象的详细信息。此操作可让您直接从策略查看应用程序成员，无需导航到 **Object**（对象）选项卡。 仅添加受延迟、抖动或数据包丢失影响的业务关键型应用程序。避免添加应用程序类别或子类别，因为它们太宽泛，不允许按应用程序进行控制。
服务	为 SD-WAN 策略规则 **Add**（添加）特定服务，选择在哪些端口上允许或拒绝来自这些服务的数据包： • **any**（任何）— 任何协议或端口均允许或拒绝所选服务。 • **application-default**（应用程序-默认）— 仅在 **ports defined by Palo Alto Networks®**（**Palo Alto Networks®** 定义的默认端口）上允许或拒绝所选服务。建议对指定 **allow**（允许）操作的各项策略使用此选项，因为

© 2019 Palo Alto Networks, Inc.

字段	说明
	其可以防止在不常用的端口和协议上运行服务，如果发生异常，则这可能是发生意外服务行为和用途的迹象。 使用此选项后，仅默认端口与 *SD-WAN* 策略匹配，并强制执行操作。根据安全策略规则，可能会允许默认端口以外的其他服务，但这些服务与 *SD-WAN* 策略不匹配，因此不会采取任何 *SD-WAN* 策略规则操作。 对于大多数服务，使用 *application-default*（应用程序 - 默认）来阻止服务使用非标准端口，或是出现其他规避行为。如果服务的默认端口发生变化，防火墙就会自动将规则更新为正确的默认端口。对于使用非标准端口的服务，如内部自定义服务，则请修改服务，或是创建一个指定非标准端口的规则，并只将该规则应用于需要此服务的流量。 • **Select**（选择）— **Add**（添加）现有服务或选择 **Service**（服务）或 **Service Group**（服务组）以指定新条目。（或者，选择 Objects（对象）> Services（服务）和 Objects（对象）> Service Groups（服务组））。

SD-WAN“Path Selection”（路径选择）选项卡

- **Policies**（策略）> **SD-WAN** > **Path Selection**（路径选择）

如果主路径质量超过路径质量配置文件中配置的路径质量阈值，请选择 **Path Selection**（路径选择）选项卡以定义用于切换到的应用程序或服务流量的路径。

字段	说明
流量分发配置文件	从下拉列表中，选择流量分发配置文件，当首选路径的其中一个路径状况指标超过该规则的路径质量配置文件中配置的阈值时，该配置文件将确定防火墙如何为应用程序或服务流量选择其他路径。

SD-WAN“Target”（目标）选项卡

- **Policies**（策略）> **SD-WAN** > **Target**（目标）

选择 **Target**（目标）选项卡，以选择将推送 SD-WAN 策略规则到其中的受管设备。仅 Panorama 管理服务器支持此选项卡。

字段	说明
任何（针对所有设备）	启用（勾选）以便 Panorama 管理服务器将 SD-WAN 策略规则推送到所有设备。
设备	选择一个或多个推送 SD-WAN 策略规则的设备。您可以根据设备状态、平台、设备组、模板、标签或 HA 状态筛选设备。
标记	指定策略的标记。

© 2019 Palo Alto Networks, Inc.

字段	说明
	策略标记是允许您对策略进行排序或过滤的关键字或短语。如果您定义了许多策略，并且希望查看用特定关键字标记的策略，那么它会非常有用。例如，您可能希望使用“解密”和“不解密”等特定关键字标记某些规则，或者将特定数据中心的名称用于和该位置关联的策略。 您还可以将标记添加到默认规则。
针对这些指定的设备和标签之外的所有设备	启用（勾选）此选项即可定位并将策略规则推送到所有设备，所选的 **Devices**（设备）或 **Tags**（标签）除外。

对象

对象是可用于构建、调度和搜索策略规则的元素，而安全配置文件可在策略规则中提供威胁防护。

本节介绍如何配置安全配置文件，以及您可在策略中使用的对象：

- 移动、克隆、替代或恢复对象
- Objects（对象）> Addresses（地址）
- Objects（对象）> Address Groups（地址组）
- Objects（对象）> Regions（地区）
- Objects（对象）> Applications（应用程序）
- Objects（对象）> Application Groups（应用程序组）
- Objects（对象）> Application Filters（应用程序过滤器）
- Objects（对象）> Services（服务）
- Objects（对象）> Service Groups（服务组）
- Objects（对象）> Tags（标记）
- Objects（对象）> Devices（设备）
- Objects（对象）> GlobalProtect > HIP Objects（HIP 对象）
- Objects（对象）> GlobalProtect > HIP Profiles（HIP 配置文件）
- Objects（对象）> External Dynamic Lists（外部动态列表）
- Objects（对象）> Custom Objects（自定义对象）
- Objects（对象）> Security Profiles（安全配置文件）
- Objects（对象）> Security Profiles（安全配置文件）> Mobile Network Protection（移动网络保护）
- Objects（对象）> Security Profiles（安全配置文件）> SCTP Protection（SCTP 保护）
- Objects（对象）> Security Profile Groups（安全配置文件组）
- Objects（对象）> Log Forwarding（日志转发）
- Objects（对象）> Authentication（身份验证）
- Objects（对象）> Decryption Profile（解密配置文件）
- Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）
- Objects（对象）> Schedules（计划）

移动、克隆、替代或恢复对象

请参阅以下主题，了解用于修改现有对象的各个选项：

- 移动或克隆对象
- 替代或恢复对象

移动或克隆对象

在移动或克隆对象时，可以为您有其访问权限的策略或对象分配 **Destination**（目标）（防火墙上的虚拟系统或 Panorama™ 上的设备组），包括共享位置。

如需移动对象，请在 **Objects**（对象）选项卡中选择对象，单击 **Move**（移动），选择 **Move to other vsys**（移动到其他虚拟系统）（仅限防火墙）或 **Move to other device group**（移动到其他设备组）（仅限 Panorama），在随后的表格中填写字段，然后单击 **OK**（确定）。

如需克隆对象，请在 **Objects**（对象）选项卡中选择对象，单击 **Clone**（克隆），在随后的表格中填写字段，然后单击 **OK**（确定）。

移动/克隆设置	说明
所选对象	显示为操作选择的策略或对象的名称和当前位置（虚拟系统或设备组）。
目标	为策略或对象选择新位置：虚拟系统、设备组或共享位置。默认值是在策略或对象选项卡中选择的虚拟系统或设备组。
输出验证中第一个检测到的错误	选中此选项（默认选中）可让防火墙或 Panorama 显示其找到的第一个错误，并停止检查更多错误。例如，如果目标不包含要移动的策略规则所引用的对象，则会出错。如果取消选中此选项，防火墙或 Panorama 会在显示错误前，找到所有错误。

替代或恢复对象

在 Panorama 中，可以在多达四级的树层次结构中嵌套设备组。在底层级别中，设备组在依次更高的级别中可以拥有父级、祖父级和曾祖父级设备组（统称为父对象），底层级别设备组可从父对象中继承策略和对象。在顶层级别中，设备组可以拥有子级、孙级和曾孙级设备组 — 统称后代。您可以替代子对象中的对象，以使其值与父对象中的对象值不同。此替代功能在默认情况下已启用。但是，不能替代共享对象或默认（预配置）对象。Web 界面通过显示 图标表示某对象已继承值，通过显示 图标表示某继承对象已替代值。

- 替代对象 — 选择 **Objects**（对象）选项卡，选择将包含替代版本的子对象设备组，选择对象，单击 **Override**（替代），然后编辑设置。您不能替代对象的 **Name**（名称）或 **Shared**（共享）设置。
- 将替代对象恢复为其继承值 — 选择 **Objects**（对象）选项卡，选择有替代版本的设备组，选择对象，单击 **Revert**（恢复），然后单击 **Yes**（是）确认操作。
- 禁用对象的替代功能 — 选择 **Objects**（对象）选项卡，选择此对象所驻留的设备组，单击要编辑的对象名称，选中 **Disable override**（禁用替代），然后单击 **OK**（确定）。随后在继承所选设备组中的对象的所有设备组中，已禁用该对象的替代功能。
- 将 **Panorama** 中的所有对象替代项替换为从共享位置或父对象设备组继承的值 — 选择 **Panorama** > **Setup**（设置）> **Management**（管理），编辑 Panorama 设置，选择 **Ancestor Objects Take Precedence**（父对象优先），然后单击 **OK**（确定）。随后必须提交到 Panorama 和包含替代项的设备组，才能推送继承的值。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Addresses（地址）

地址对象可以包括 IPv4 或 IPv6 地址（单个 IP 地址、地址范围或子网）、FQDN 或通配符地址（IPv4 地址后跟斜杠和通配符掩码）。地址对象允许您在策略规则、筛选程序或防火墙其他功能中重复使用该地址或该地址组作为源地址或目标地址，而无需为每个实例手动添加每个地址。可以使用 Web 界面或 CLI 配置对象，并且需要对更改执行提交操作才能使对象成为配置的一部分。

首先 **Add**（添加）一个新的地址对象，然后指定以下值：

地址对象设置	说明
姓名	输入描述将作为此对象的一部分的地址的名称（最多 63 个字符）。定义安全策略规则时，此名称将出现在地址列表中。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。
共享	如果希望与以下项共享此地址对象，请选择此选项： • **Every virtual system (vsys) on a multi-vsys firewall**（多虚拟系统防火墙上的每个虚拟系统 **(vsys)**）— 如果不选择此选项，地址对象将仅对 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）可用。 • **Panorama** 上的每个设备组— 如果不选择此选项，地址对象将仅对 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）可用。
禁用替代（仅限 Panorama）	选择此选项可阻止管理员替代继承此对象的设备组中此地址对象的设置。默认情况下，禁用此选项，这意味着管理员可以替代继承对象的任何设备组的设置。
说明	输入对象的说明（最多 1,023 个字符）。

类型	指定地址对象的类型和条目：
	• **IP Netmask**（**IP** 网络掩码）— 使用以下表示法输入 IPv4 或 IPv6 地址或者 IP 地址范围：*ip_address/mask*（掩码）或*ip_address*，其中，掩码是用于地址的网络部分的显著二进制数字的数量。对于 IPv6 地址，最好只指定网络部分，而不指定主机部分。例如：
	  • **192.168.80.150/32**— 指示一个地址。
	  • **192.168.80.0/24**— 指示从 192.168.80.0 到 192.168.80.255 的所有地址。
	  • **2001:db8::/32**
	  • **2001:db8:123:1::/64**
	• **IP** 范围— 使用以下格式输入地址范围：*ip_address–ip_address*，其中，范围的两个界限值均为 IPv4 地址或 IPv6 地址。例如：2001:db8:123:1::1-2001:db8:123:1::22
	• **IP Wildcard Mask**（**IP** 通配符掩码）—输入 IP 通配符地址，格式为：IPv4 地址后跟斜杠和通配符掩码（必须以 0 开头）；例如 10.182.1.1/0.127.248.0。在通配符掩码中，零(0)位表示被比较的位必须与 0 覆盖的 IP 地址中的位匹配。掩码中的一（1）是通配符位，表示被比较的位无需与 1 覆盖的 IP 地址中的位进行匹配。将 IP 地址和通配符掩码转换为二进制。为了说明匹配：在二进制片段 0011 中，通配符掩码 1010 可导致四个匹配（0001、0011、1001 和 1011）。
	您只能在安全策略规则中使用 *IP* 类通配符掩码的地址对象。

© 2019 Palo Alto Networks, Inc.

地址对象设置	说明
	• **FQDN**— 输入域名。FQDN 最初在提交时进行解析。如果 TTL 大于等于最短 FQDN 刷新时间，随后，FQDN 条目会根据 FQDN 的 TTL 进行刷新；否则，FQDN 条目将会在最短 FQDN 刷新时间时刷新。如果配置代理，则 FQDN 由系统 DNS 服务器或 DNS 代理对象解析。
解析	选择地址类型并输入 IP 地址或 FQDN 后，请单击 **Resolve**（解析）以分别查看关联的 FQDN 或 IP 地址（基于防火墙或 Panorama 的 DNS 配置）。 您可以将地址对象从 FQDN 更改为 IP 网络掩码，或者将地址对象从 IP 网络掩码更改为 FQDN。要将地址对象从 FQDN 更改为 IP 网络掩码，请单击 **Resolve**（解析）以查看 FQDN 解析成的 IP 地址，然后选择一个并 **Use this address**（使用此地址）。地址对象的 Type（类型）会动态变更为 IP 网络掩码，同时您选择的 IP 地址会显示在文本字段中。 或者，要将地址对象从 IP 网络掩码更改为 FQDN，请单击 **Resolve**（解析）以查看 IP 网络掩码解析成的 DNS 名称，然后选择 FQDN 并 **Use this FQDN**（使用此 **FQDN**）。Type（类型）会变更为 FQDN，同时 FQDN 会显示在文本字段中。
标记	选择或输入您希望应用到此地址对象的标记。您可以在这里定义标记或使用 Objects（对象）> Tags（标记）选项卡创建新标记。

© 2019 Palo Alto Networks, Inc.

Objects（对象） > Address Groups（地址组）

要简化创建安全策略，可以将需要相同安全设置的地址组合到地址组中。地址组可以是静态地址组，也可以是动态地址组。

- 动态地址组：动态地址组使用查找标记和基于标记的过滤器动态填充其成员。如果使用可以在其中频繁更改虚拟机位置/IP 地址的广泛虚拟基础架构，则动态地址组非常有用。例如，您可以频繁使用灵活的故障转移设置或配置新虚拟机，并将策略应用到流量表或新计算机，而无需修改防火墙的配置/规则。

  要在策略中使用动态地址组，必须完成以下任务：

  - 定义动态地址组，并在策略规则中引用该动态地址组。
  - 通知 IP 地址和相应标记的防火墙，以便形成动态地址组的成员。要完成该任务，请利用防火墙中使用 XML API 的外部脚本，而对于基于 VMware 的环境，可选择 **Device**（设备）> **VM Information Sources**（虚拟机信息源）来配置防火墙上的设置。

  动态地址组也可以包括静态定义的地址对象。如果创建地址对象和应用已分配给动态地址组的相同标记，则动态地址组将包括与标记匹配的所有静态和动态对象。因此，您可以在同一个地址组中使用标记合并动态和静态对象。
- 静态地址组：静态地址组可以包括静态地址对象、动态地址组或者是地址对象和动态地址组的组合。

  要创建地址组，单击添加，然后填写以下字段：

地址组设置	说明
姓名	输入描述地址组的名称（最多63个字符）。定义安全策略时，此名称将出现在地址列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享	如果想要将地址组用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则地址组只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则地址组只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的地址组对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
说明	输入对象的说明（最多 1023 个字符）。
类型	选择静态或动态。 要创建动态地址组，可以使用匹配条件构成该组要包括的成员。可以使用 **AND** 或 **OR** 运算符定义匹配条件。 要查看匹配条件的属性列表，必须配置防火墙访问和检索源/主机的属性。可以将为其配置信息源的每台虚拟机注册到防火墙，并且防火墙可以轮询虚拟机以检索 *IP* 地址或配置更改，而无需在防火墙上进行任何修改。 对于静态地址组，单击添加，然后选择一个或多个地址。单击添加可以将对象或地址组添加到地址组。地址组可以包含地址对象，以及静态和动态地址组。

© 2019 Palo Alto Networks, Inc.

地址组设置	说明
标记	选择或输入您希望应用到此地址组的标记。有关标记的信息，请参阅 Objects（对象）> Tags（标记）。

成员计数和地址	在添加地址组后，**Objects**（对象）> **Address Groups**（地址组）页面上的 Members Count（成员计数）列会指示组中的对象是采用动态方式还是静态方式进行填充的。
	• 对于静态地址组，您可以查看地址组中的成员计数。
	• 对于使用标记动态填充成员的地址组，或包含静态和动态成员的地址组，要查看成员，只需单击 Address（地址）列中的 **More...**（更多...）链接。即可查看已注册到地址组的 IP 地址。
	  • Type（类型）用于指示 IP 地址是静态地址对象还是动态注册的地址，并显示 IP 地址。
	  • Action（操作）用于为 IP 地址取消注册标记。单击链接可添加注册源，并指定要取消注册的标记。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Regions（地区）

防火墙支持创建应用于指定国家/地区或其他地区的策略规则。在指定安全策略、解密策略和 DoS 策略的源和目标时，地区可作为选项。可以从国家/地区的标准列表中选择，或者使用这一节描述的地区设置来定义要包括的自定义地区，作为安全策略规则的选项。

下表介绍了地区设置：

地区设置	说明
姓名	选择描述地区的名称。定义安全策略时，此名称将出现在地址列表中。
地理位置	若要指定纬度和经度，请选中此选项并指定值（xxx.xxxxxx 格式）。此信息在 App-Scope 的通信和威胁映射中使用。请参阅 Monitor（监控）> Logs（日志）。
地址	使用以下任意格式指定用于标识地区的 IP 地址、IP 地址的范围或子网： x.x.x.x x.x.x.x-y.y.y.y x.x.x.x/n

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Dynamic User Groups（动态用户组）

要创建动态用户组，请选择 **Objects**（对象）> **Dynamic User Groups**（动态用户组），**Add**（添加）一个新的动态用户组，然后配置以下设置：

动态用户组设置	说明
姓名	输入描述动态用户组的 **Name**（名称）（最多 63 个字符）。定义安全策略规则时，此名称将出现在源用户列表中。该名称必须唯一，且只能使用字母数字字符、空格、连字符和下划线。
说明	输入对象的 **Description**（说明）（最多 1,023 个字符）。
共享 （仅限 Panorama）	若希望 Panorama 上的每个设备组都能使用动态用户组的匹配条件，请选择此选项。 *Panorama* 不会与设备组共享组成员。 如果取消选中此选项，则动态用户组的匹配条件仅可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代 （仅限 Panorama）	选择此选项，即可阻止管理员在继承对象的设备组中替代此动态用户组的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
匹配	**Add Match Criteria**（添加匹配条件），以使用 **AND** 或 **OR** 运算符定义动态用户组中的成员，从而包含多个标签。 *Add Match Criteria*（添加匹配条件）时，仅显示现有标签。您可选择现有的标签或创建新的标签。
标记	（可选）选择或输入要应用于动态用户组对象的静态对象标签。这会标记动态用户组对象本身，而不是组中的成员。所选的标签将允许您对相关项目进行分组，且与匹配条件无关。有关标记的信息，请参阅 Objects（对象）> Tags（标记）。

添加动态用户组后，您可以查看下列组信息：

动态用户组列	说明
位置 （仅限 Panorama）	确定动态用户组的匹配条件是否可用于 Panorama 上每个设备组（**Shared**（共享））或所选设备组。
用户	选择 **more**（更多）以查看动态用户组中的用户列表。

© 2019 Palo Alto Networks, Inc.

动态用户组列	说明
	• 要将标签添加到用户以包含在组中，请 **Register Users**（注册用户），然后选择要应用到该用户的 **Registration Source**（注册源）和 **Tags**（标签）。若用户的标签与组的条件匹配，则防火墙会将该用户添加到动态用户组中。 • （可选）指定 **Timeout**（超时）（以分钟为单位）（默认为 0；范围为 0 至 43,200），可在达到指定时间后将用户从组中移除。 • （可选）**Add**（添加）**Users**（用户）到组中，或从组中 **Delete**（删除）用户。 • 要移除用户的标签以阻止其成为组的成员，请选择用户，**Unregister Users**（取消注册用户），然后选择 **Registration Source**（注册源）和 **Tags**（标签）。 • 查看或修改动态用户组用户列表后，单击 **Close**（关闭）。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Applications（应用程序）

以下主题介绍 **Applications**（应用程序）页面。

您在查找什么内容？	请参阅
了解应用程序页面上显示的应用程序设置和属性。	应用程序概述 应用程序支持的操作
添加新应用程序或修改现有应用程序。	定义应用程序

应用程序概述

Applications（应用程序）页面列出了每个应用程序定义的各种属性，如应用程序的相对安全风险（1 到 5）。风险值基于一些条件，例如应用程序是否可以共享文件、是否容易误用或是否尝试规避防火墙。值越高表示风险越大。

页面顶部的应用程序浏览器区域列出可以用于过滤显示的属性，如下所示。每个条目左侧的数字表示具有该属性的应用程序的总数。

每周发布的内容定期放入了可以制作签名的新解码器和上下文。

下表介绍了应用程序详细信息 — 自定义应用程序和 Palo Alto® Networks 应用程序可能会显示部分或全部这些字段。

应用程序详细信息	说明
姓名	应用程序的名称。
说明	应用程序的说明（最多 255 个字符）。
其他信息	指向包含应用程序更多相关信息的 Web 源（Wikipedia、Google 和 Yahoo!）的链接。
标准端口	应用程序用于与网络通信的端口。
取决于	必须依赖此应用程序才能运行的其他应用程序的列表。在创建允许所选应用程序的策略规则时，还必须确保允许此应用程序所依赖的任何其他应用程序。

© 2019 Palo Alto Networks, Inc.

应用程序详细信息	说明
隐式使用	所选应用程序所依赖的，但无需添加到允许所选应用程序的安全策略规则中的其他应用程序，因为这些应用程序是隐式支持的应用程序。
之前已识别为	对于新的 App-ID™，或已更改的 App-ID，均表明此应用程序之前已识别为此 App-ID。此标识可帮助您根据应用程序更改评估策略更改是否是必需的。如果禁用 App-ID，则与该应用程序关联的会话会像之前已识别为 App-ID 的应用程序一样与策略匹配。同样，禁用的 App-ID 会像之前已识别为 App-ID 的应用程序一样显示在日志中。
拒绝操作	App-ID 是为默认拒绝操作开发的，默认拒绝操作规定了应用程序包含在有拒绝操作的安全策略规则中时防火墙的响应方式。默认拒绝操作可以指定静默丢弃或 TCP 重置。您可以在安全策略中替代此默认操作。
Characteristics	
回避	将端口或协议用于其原始预期目的之外，以期穿过防火墙。
过多带宽	正常使用中稳定地消耗至少 1 Mbps 带宽。
易误用	经常用于不法目的，或可轻易设置使其暴露非用户期望的信息。
SaaS	在防火墙上，软件即服务 (SaaS) 的特点是服务，其中软件和基础架构归应用程序服务提供商所有和管理，但您可以保留数据的完全控制权，包括创建、访问、共享和传输数据。 请记住，在应用程序的特点方面，SaaS 应用程序与 Web 服务不同。Web 服务是托管应用程序，其中用户不能拥有数据（例如，Pandora），或者服务主要由大量订户为社交提供的共享数据组成（例如，LinkedIn、Twitter 或 Facebook）。
能够传输文件	能通过网络将文件从一个系统传输到另一个系统。
其他隧道应用程序	能够在其协议内传输其他应用程序。
由恶意软件使用	已知恶意软件利用该应用程序进行传播、攻击或数据窃取，或其随恶意软件一起散布。
有已知漏洞	已经公开报告存在漏洞。
普遍性	可能有超过 1000000 个用户。
为其他应用程序继续扫描	指示防火墙继续尝试匹配其他应用程序签名。如果不选择此选项，则防火墙会在第一次匹配签名后停止查找其他应用程序匹配项。
SaaS 特征	
数据泄露	在过去三年内可能已向不可信来源发布安全信息的应用程序。
不当服务条款	具有可能损坏企业数据的不利服务条款的应用程序。

© 2019 Palo Alto Networks, Inc.

应用程序详细信息	说明
未认证	应用程序当前不符合行业计划或认证，如 SOC1、SOC2、SSAE16、PCI、HIPAA、FINRAA 或 FEDRAMP。
财务可行性不佳	在未来 18 至 24 个月内有可能会停止运行的应用程序。
无 IP 限制	用户访问权限不受 IP 限制的应用程序。
分类	
类别	应用程序类别是以下类别之一： • 商务系统 • 协作 • 一般 Internet • 介质 • 网络 • 未知
子类别	对应用程序分类使用的子类别。不同的类别具有与之关联的不同子类别。例如，协作类别中的子类别包括电子邮件、文件共享、即时消息、互联网会议、社交商业、社交网络、VoIP 视频和 Web 发布。而商业系统类别中的子类别包括身份验证服务、数据库、erp-crm、通用商业、管理、Office 程序、软件更新和存储备份。
技术	应用程序技术是以下类别之一： • 客户端-服务器：此应用程序使用客户端-服务器模型，其中，有一个或多个客户端在网络中与服务器进行通信。 • 网络-协议：此应用程序通常用于系统与系统间的通信，以便执行网络操作。这包括大多数 IP 协议。 • 对端到对端：此应用程序直接与其他客户端通信来传输信息，而不依赖于中心服务器进行通信。 • 基于浏览器：此应用程序依赖于 Web 浏览器运行。
Risk	应用程序的指定风险。 要自定义此设置，请单击 **Customize**（自定义）链接，输入一个值 (1-5)，然后单击 **OK**（确定）。
标记	已分配给应用程序的标记。 **Edit Tags**（编辑标记）即可为应用程序添加或移除标记。
选项	
会话超时	应用程序由于不活动而变为超时需要经过的时间段（以秒为单位，范围为 1-604800 秒）。此超时适用于 TCP 或 UDP 以外的协议。有关 TCP 或 UDP，请参见此表的后几行。 要自定义此设置，请单击自定义链接，输入值，然后单击确定。
TCP 超时(秒)	终止 TCP 应用程序流时超时（以秒为单位，范围为 1-604800）。

© 2019 Palo Alto Networks, Inc.

应用程序详细信息	说明
	要自定义此设置，请单击自定义链接，输入值，然后单击确定。 值为 0 表示将使用全局会话计时器，TCP 的超时为 3600 秒。
UDP 超时(秒)：	终止 UDP 应用程序流时超时（以秒为单位，范围为 1-604800 秒）。 要自定义此设置，请单击自定义链接，输入值，然后单击确定。
TCP 半闭合(秒)	在接收第一个 FIN 数据包和接收第二个 FIN 数据包或 RST 数据包之间，会话保持在会话表中范围内的最大时间长度（以秒为单位）。如果计时器超时，会话将关闭（范围为 1-604800）。 默认：如果在应用层未配置计时器，将会使用全局设置。 如果已在应用层配置此值，则它将替代全局 **TCP** 半闭合设置。
TCP 等待时间(秒)	在接收第二个 FIN 数据包或 RST 数据包后，会话保持在会话表中范围内的最大时间长度（以秒为单位）。如果计时器超时，会话将关闭（范围为 1-600）。 默认：如果在应用层未配置计时器，将会使用全局设置。 如果已在应用层配置此值，则它将替代全局 **TCP** 等待时间设置。
已启用 App-ID	指示已启用还是已禁用 App-ID。如果已禁用 App-ID，该应用程序的流量在安全策略和日志中会被视为 **Previously Identified As**（之前已识别为）App-ID 的流量。对于在内容发行版本 490 之后添加的应用程序，您可以在查看新应用程序的策略影响时禁用它们。在查看策略后，您可能会选择启用 App-ID。您还可以禁用之前启用的应用程序。在多虚拟系统防火墙上，可以在每个虚拟系统中单独禁用 App-ID。

如果防火墙无法使用 App-ID 识别应用程序，则将流量分类为“未知”：unknown-tcp 或 unknown-udp。此行为适用于所有未知应用程序，完全模拟 HTTP 的未知应用程序除外。有关详细信息，请参阅监视 > Botnet。

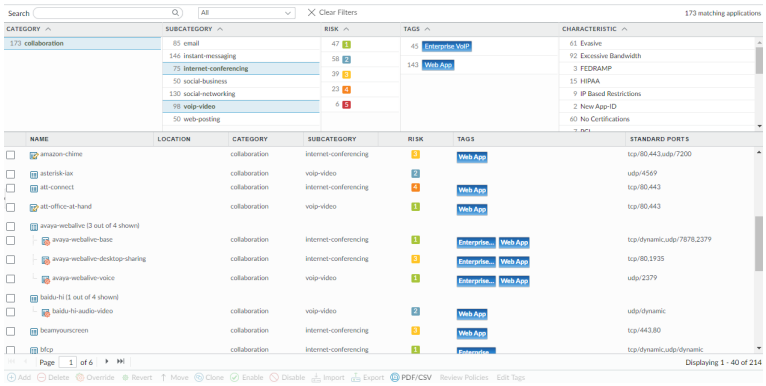
可以为未知应用程序创建新定义，然后定义新应用程序定义的安全策略。此外，可以将需要相同安全设置的应用程序组合到应用程序组中，以简化安全策略的创建。

应用程序支持的操作

您可以在此页上执行下列任意操作：

应用程序支持的操作	说明
通过应用程序过滤	• 如需搜索特定应用程序，请在 **Search**（搜索）字段中输入应用程序名称或说明，然后按 **Enter** 键。使用下拉列表可搜索或筛选特定的应用程序，或查看 **All**（所有）应用程序、**Custom applications**（自定义应用程序）、**Disabled applications**（已禁用的应用程序）或 **Tagged applications**（已标记的应用程序）。 随即列出应用程序，并更新过滤器列以显示匹配搜索的应用程序的统计信息。搜索将匹配部分字符串。定义安全策略时，可以写入应用于与已保存过滤器匹配的所有应用程序的规则。通过匹配过滤器的内容更新添加新应用程序时，此类规则将得到动态更新。

© 2019 Palo Alto Networks, Inc.

应用程序支持的操作	说明
	• 如需按显示于此页面上的应用程序属性进行筛选，请单击用作筛选依据的项。例如，要将列表限制为协作类别，请单击 **Collaboration**（协作），列表将仅显示此类别的应用程序。  • 要在其他列上执行过滤，请在其他列中选择一个条目。将连续进行过滤 ：依次应用类别筛选程序、子类别筛选程序、技术筛选程序、风险筛选程序和特征筛选程序。例如，如果应用类别、子类别和风险筛选程序，即使尚未显示应用技术筛选程序，Technology（技术）列也会自动限制为与所选类别和子类别一致的技术。每次应用筛选程序时，应用程序列表都会自动更新。要创建新的应用程序过滤器，请参阅 Objects（对象）> Application Filters（应用程序过滤器）。
添加新应用程序。	要添加新应用程序，请单击定义应用程序。
查看和/或自定义应用程序的详细信息。	单击应用程序名称链接可查看应用程序的相关说明，包括应用程序的标准端口和特征、风险等等。有关应用程序设置的详细信息，请参阅定义应用程序。 如果应用程序名称左侧有一个黄色铅笔图标（ ），则表明该应用程序是一个自定义应用程序。
禁用应用程序	您可以 **Disable**（禁用）某个应用程序（或多个应用程序），以使此应用程序的签名与流量不匹配。禁用应用程序后，为阻止、允许或强制执行匹配应用程序定义的安全规则不适用于应用程序流量。您可能会选择禁用包含在新内容发行版本中的应用程序，因为在唯一标识应用程序后，应用程序的策略实施可能会改变。例如，在新内容版本安装之前，防火墙允许标识为 Web 浏览流量的应用程序；在安装内容更新后，唯一标识的应用程序与允许 Web 浏览流量的安全规则不再匹配。在这种情况下，可以选择禁用应用程序，以使与应用程序签名匹配的流量继续被归类为 Web 浏览流量，并允许此流量。
启用应用程序	选择已禁用的应用程序，然后 **Enable**（启用）此应用程序，以便防火墙根据配置的安全策略管理应用程序。
导入应用程序	若要导入应用程序，请单击导入。浏览以选择文件，并从 **Destination**（目标）下拉列表中选择目标虚拟系统。
导出应用程序	要导出应用程序，请选择应用程序的此选项，并单击 **Export**（导出）。执行提示的操作以保存文件。

© 2019 Palo Alto Networks, Inc.

应用程序支持的操作	说明
导出应用程序配置表格	以 **PDF/CSV** 格式导出所有应用程序中的信息。仅导出了 Web 界面中所显示的列。请参阅导出配置表格数据。
安装新内容版本后，评估策略影响	**Review Policies**（查看策略）以便评估安装某内容发行版本前后应用程序基于策略的执行情况。使用“策略查看”对话框，查看策略对下载内容发行版本中包含的新应用程序的影响。Policy Review（策略查看）对话框可让您在现有安全策略规则中添加或删除暂挂应用程序（通过内容发行版本下载的，但未安装到防火墙上的应用程序）；在安装相应的内容发行版本后，暂挂应用程序的策略更改才生效。在 **Device**（设备）> **Dynamic Updates**（动态更新）页面上下载和安装内容发行版本时，也可以访问“策略查看”对话框。
标记应用程序	名为 **sanctioned** 的预定义标记可用于标记 SaaS 应用程序。就应用程序特征相关的详细信息而言，SaaS 应用程序是一种标识为 **Saas=yes** 的应用程序，您可在任何应用程序上使用约束标记。 将应用程序标记为 *sanctioned*（已批准），有助于区分已批准的 *SaaS* 应用程序流和未批准的 *SaaS* 应用程序流，例如，在检查 *SaaS* 应用程序使用情况报告时，或是对网络上的应用程序进行评估时。 选择应用程序，单击 **Edit Tags**（编辑标记），然后从下拉列表中选择预定义的 **Sanctioned**（已批准）标记，即可标识任何要在网络上明确允许的应用程序。生成 SaaS 应用程序使用报告后（请参阅 Monitor（监控）> PDF Reports（PDF 报告）> SaaS Application Usage（SaaS 应用程序使用）），您可对网络上使用的约束和未约束 SaaS 应用程序进行应用程序相关的统计信息比对。 将某应用程序标记为“约束”后，以下限制即适用： • 约束标记不可应用于应用程序组。 • 约束标记不可在 **Shared**（共享）级别上应用；仅可对每个设备组或虚拟系统标记一个应用程序。 • 约束标记不可用于标记 facebook-mail（属于 Facebook 容器应用程序）等容器应用程序中包含的应用程序。 您也可选择 **Remove tag**（删除标记）或 **Override tag**（替代标记）。其中，替代选项仅在已从 Panorama 推送的设备组继承设置的防火墙上可用。

定义应用程序

选择 **Objects**（对象）> **Applications**（应用程序）可 **Add**（添加）新的自定义应用程序，以便防火墙评估应用策略的时机。

新建应用程序设置	说明
配置选项卡	
姓名	输入应用程序名称（最多 31个字符）。定义安全策略时，此名称将出现在应用程序列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、句点、连字符和下划线。第一个字符必须是字母。

© 2019 Palo Alto Networks, Inc.

新建应用程序设置	说明
共享	如果想要将应用程序用于以下位置，请选择此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选择此选项，则应用程序只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则应用程序只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选择此选项可防止管理员在继承对象的设备组中替代此应用程序对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
说明	输入应用程序说明，供一般参考（最多 255 个字符）。
类别	选择应用程序类别，如电子邮件或数据库。此类别用于生成前十个应用程序类别图表，且可供过滤（请参阅 ACC）。
子类别	选择应用程序子类别，如电子邮件或数据库。此子类别用于生成前十个应用程序类别图表，且可供过滤（请参阅 ACC）。
技术	选择应用程序的技术。
父应用程序	指定此应用程序的父应用程序。当会话与父应用程序和自定义应用程序都匹配时，则应用此设置；但是，只报告自定义应用程序，因为它更明确。
Risk	选择与此应用程序关联的风险级别（最低级别 1 到最高级别 5）。
Characteristics	选择可能使应用程序处于风险中的应用程序特征。有关各种特征的说明，请参阅特征。
高级选项卡	
端口	如果应用程序使用的协议是 TCP 和/或 UDP，则选择端口并输入协议和端口号的一种或多种组合（每行输入一种）。一般格式如下： *<protocol>/<port>* 其中，*<port>* 是单个端口号，或使用 **dynamic**（动态）表示动态端口分配。 示例：TCP/动态或 UDP/32。 在安全规则的 Service（服务）列中使用 **app-default** 时，将应用此设置。
IP 协议	要指定除 TCP 或 UDP 以外的 IP 协议，请选择**IP** 协议，并输入协议号（1 到 255）。
ICMP 类型	要指定互联网控制消息协议版本 4 (ICMP) 类型，请选择 **ICMP Type**（**ICMP** 类型），并输入类型号（范围为 0-255）。
ICMP6 类型	要指定互联网控制消息协议版本 6 (ICMPv6) 类型，请选择 **ICMP6 Type**（**ICMP6** 类型），并输入类型号（范围为 0-255）。
None	若要指定与协议无关的签名，请选择无。

© 2019 Palo Alto Networks, Inc.

新建应用程序设置	说明
超时	输入空闲应用程序流终止之前经过的秒数（范围为 0-604800 秒）。零表示将使用应用程序的默认超时。在所有情况下，此值均可用于除 TCP 和 UDP 以外的协议，并且在未指定 TCP 超时和 UDP 超时的情况下，用于 TCP 和 UDP 超时。
Tcp 超时	输入空闲 TCP 应用程序流终止之前经过的秒数（范围为 0-604800 秒）。零表示将使用应用程序的默认超时。
UDP 超时	输入空闲 UDP 应用程序流终止之前经过的秒数（范围为 0-604800 秒）。零表示将使用应用程序的默认超时。
TCP 半闭合	输入会话将保持在会话表中范围内的最大时间长度，即在接收第一个 FIN 和接收第二个 FIN 或 RST 之间。如果计时器超时，会话将关闭。 默认：如果在应用层未配置计时器，将会使用全局设置（范围为 1-604800 秒）。 如果已在应用层配置此值，则它将替代全局 TCP 半闭合设置。
TCP 等待时间	输入会话保持在会话表中范围内的最大时间长度，即在接收第二个 FIN 或 RST 之后。如果计时器超时，会话将关闭。 默认：如果在应用层未配置计时器，将会使用全局设置（范围为 1-600 秒）。 如果已在应用层配置此值，则它将替代全局 TCP 等待时间设置。
正在扫描	选中要基于安全配置文件（文件类型、数据模式和病毒）允许的扫描类型。
Signature 选项卡	

签名	单击添加以添加新签名，并指定以下信息：
	• 签名名称— 输入名称以标识该签名。
	• 注释— 输入可选说明。
	• 排序条件匹配— 选择签名条件的定义顺序是否重要。
	• **Scope**（范围）— 选择是仅将此签名应用于当前 **Transaction**（事务）还是完整用户 **Session**（会话）。
	指定标识该签名的条件。这些条件将用于生成签名，以便防火墙用其匹配应用程序模式并控制通信：
	• 要添加条件，请选择 **Add And Condition**（添加 **And** 条件）或 **Add Or Condition**（添加 **Or** 条件）。要在组中添加条件，请选择组，然后单击添加条件。
	• 从下拉列表中选择一个 **Operator**（运算符）。可用选项为 **Pattern Match**（模式匹配）、**Greater Than**（大于）、**Less Than**（小于）和 **Equal To**（等于），然后指定以下选项：
	（仅限模式匹配）
	  • 上下文— 从可用上下文中选择。将使用动态上下文更新来更新这些上下文。
	  • **Pattern**（模式）— 指定正则表达式，以指定应用于自定义应用程序的唯一字符串上下文值。

© 2019 Palo Alto Networks, Inc.

新建应用程序设置	说明
	执行数据包捕获以标识上下文。有关正则表达式的模式规则，请参阅模式规则语法。 （仅限大于，小于） • 上下文— 从可用上下文中选择。将使用动态上下文更新来更新这些上下文。 • **Value**（值）— 指定要匹配的值（范围为 0-4294967295）。 • **Qualifier and Value**（限定符和值）—（可选）添加限定符/值对。 （仅限等于） • **Context**（上下文）— 从 TCP 或 UDP 的未知请求和响应中选择（如 unknown-req-tcp），或使用通过动态内容更新提供的其他上下文（如 dnp3-req-func-code）。 对于 TCP 或 UDP 的未知请求和响应，请指定： • 位置— 在负载中的前四字节或第二个四字节之间选择。 • 掩码— 指定一个 4 字节的十六进制值，例如，0xffffff00。 • **Value** — 指定 4 字节十六进制值，例如，0xaabbccdd。 对于所有其他上下文，请指定一个与应用程序相关的 **Value**（值）。 如需在组中移动条件，请选择条件，然后选择 **Move Up**（上移）或 **Move Down**（下移）。如需移动组，请选择组，然后选择 **Move Up**（上移）或 **Move Down**（下移）。无法将条件从一个组移动到另一个组。

如果应用程序仅用于应用程序替代规则，则无需为应用程序指定签名。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Application Groups（应用程序组）

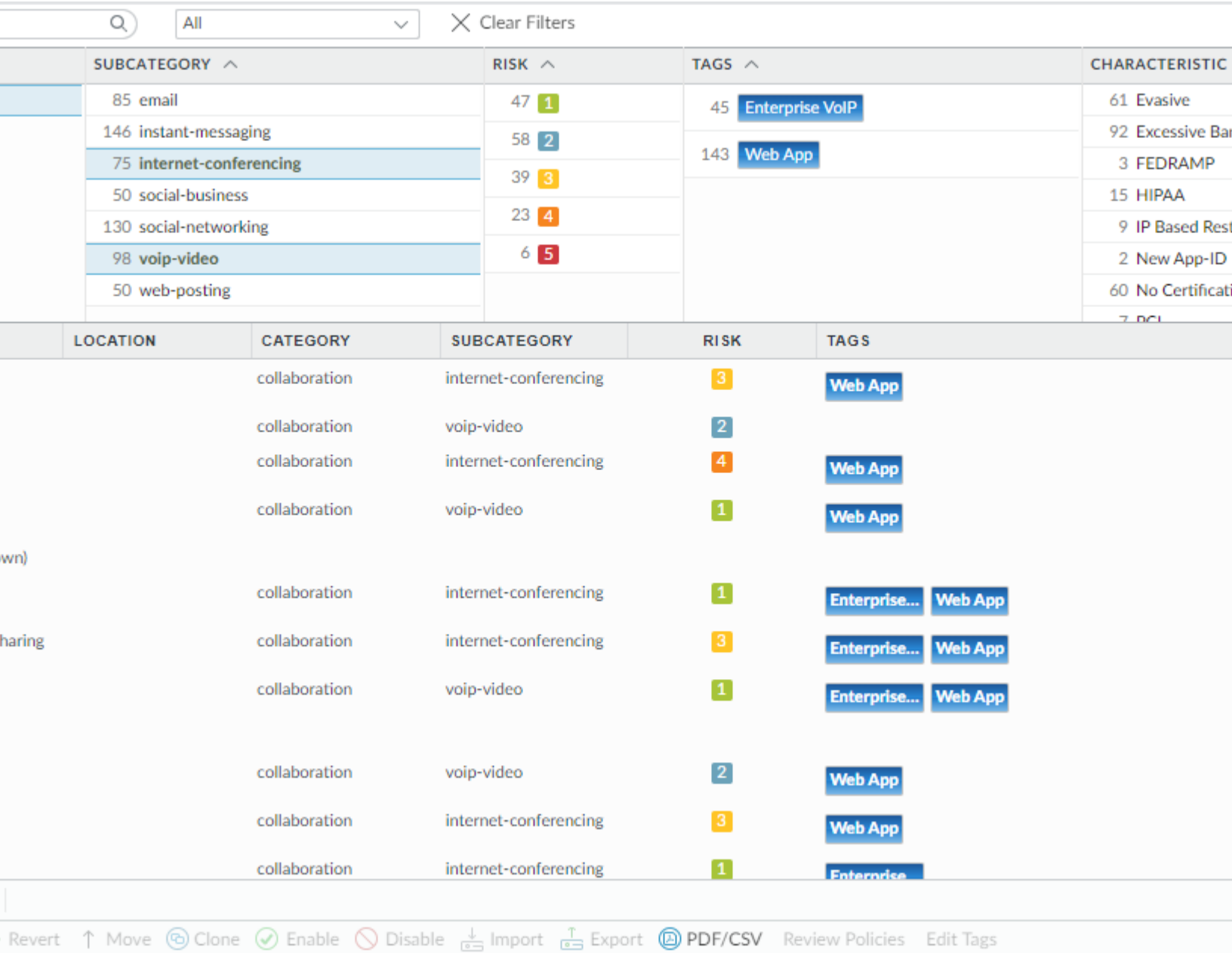
要简化安全策略的创建，可以通过创建应用程序组来组合需要相同安全设置的应用程序。（要定义新应用程序，请参阅定义应用程序。）

新建应用程序组设置	说明
姓名	输入描述应用程序组的名称（最多 31 个字符）。定义安全策略时，此名称将出现在应用程序列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享	如果想要将应用程序组用于以下位置，请选中此选项： 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则应用程序组只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 Panorama 上的每个设备组。如果取消选中此选项，则应用程序组只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的应用程序组对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
应用程序	单击添加，然后选择此组中要包括的应用程序、应用程序过滤器和/或其他应用程序组。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Application Filters（应用程序过滤器）

应用程序过滤器可帮助简化重复的搜索。要定义应用程序过滤器，请单击 **Add**（添加），然后输入新过滤器的名称。在窗口的上方区域中，单击要用作过滤基础的项。例如，要将列表限制为 Collaboration（协作）类别，请单击 **collaboration**（协作）。



要过滤其他列，请在这些列中选择一个条目。过滤按顺序连续进行：依次应用类别过滤器、子类别过滤器、技术过滤器、风险过滤器、标签和特征过滤器。

选择过滤器后，页面上显示的应用程序列表将会自动更新。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Services（服务）

定义特定应用程序的安全策略时，可以选择一项或多项服务以限制应用程序可以使用的端口号。默认服务是 **any**（任何），即允许所有 TCP 和 UDP 端口。虽然预定义了 HTTP 和 HTTPS 服务，但仍可以添加其他服务定义。可以将通常一起分配的服务组合到服务组中，以简化安全策略的创建（请参阅 Objects（对象）> Service Groups（服务组））。

此外，您可以使用服务对象指定基于服务的会话超时 — 这意味着，即使这些组使用相同的 TCP 或 UDP 服务，您也可以将不同的超时应用于不同的用户组；或者，如果要将自定义应用程序从基于端口的安全策略迁移至基于应用程序的安全策略，您可以轻松地维护您的自定义应用程序超时。

下表介绍了服务设置：

服务设置	说明
姓名	输入服务名称（最多63个字符）。定义安全策略时，此名称将出现在服务列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入服务的说明（最多 1023 个字符）。
共享	如果想要将服务对象用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则服务对象只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则服务对象只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的服务对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
协议	选择服务使用的协议（**TCP** 或 **UDP**）。
目标端口	输入服务使用的目标端口号（0 到 65535）或端口号范围 (port1-port2)。多个端口或范围必须以逗号分隔。目标端口为必填字段。
源端口	输入由服务使用的源端口号（0 到 65535）或端口号的范围 (port1-port2)。多个端口或范围必须以逗号分隔。源端口可选。
会话超时	定义服务的会话超时： • **Inherit from application**（从应用程序继承）（默认）— 不应用基于服务的超时，而应用应用程序超时。 • **Override**（替代）— 定义服务的自定义会话超时。继续填充 TCP Timeout（TCP 超时）、TCP Half Closed（TCP 半闭合）和 TCP Wait Time（TCP 等待时间）字段。
仅当您选择替代应用程序超时并为服务创建自定义会话超时时，才会显示以下设置：	
Tcp 超时	设置数据传输开始后 TCP 会话可保持打开的最长时间（以秒为单位）。如果该时间到期，会话将关闭。

© 2019 Palo Alto Networks, Inc.

服务设置	说明
	范围为 1 - 604800。默认值为 3600 秒。
TCP 半闭合	设置仅连接的一端尝试关闭连接时会话保持打开的最长时间（以秒为单位）。 此设置适用于： • 在防火墙收到第一个 FIN 数据包（指示连接的一端正在尝试关闭会话）之后和收到第二个 FIN 数据包（指示连接的另一端正在关闭会话）之前的时间段。 • 接收 RST 数据包之前的时间段（指示尝试重置连接）。 如果计时器到期，会话将关闭。 范围为 1 - 604800。默认值为 120 秒。
TCP 等待时间	设置收到终止会话所需的两个 FIN 数据包中的第二个数据包后或收到重置连接的 RST 数据包后，会话保持打开的最长时间（以秒为单位）。 如果计时器到期，会话将关闭。 范围为 1 - 600。默认值为 15 秒。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Services Groups（服务组）

要简化安全策略的创建，可以将具有相同安全设置的服务组合到服务组中。要定义新服务，请参阅 Objects（对象）> Services（服务）。

下表介绍了服务组设置：

服务组设置	说明
姓名	输入服务组名称（最多63个字符）。定义安全策略时，此名称将出现在服务列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享	如果想要将服务组用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则服务组只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则服务组只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的服务组对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
服务	单击添加将服务添加到组。从下拉列表中选择，或在下拉列表的底部单击 **Service**（服务），然后指定设置。有关设置的说明，请参阅 Objects（对象）> Services（服务）。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Tags（标记）

标记可让您使用关键字或词组将对象进行分组。您可以将标签应用到地址对象、地址组（静态和动态）、应用程序、区域、服务、服务组和策略规则。您还可以使用 SD-WAN 接口配置文件将链路标记应用于以太网接口。可以使用标记排序或筛选对象，并根据颜色从视觉上分辨对象。当将颜色应用到标记时，**Policy**（策略）选项卡将显示拥有背景颜色的对象。

在使用该标记对规则进行分组之前，必须创建标记。按标记分配分组规则后，**View Rulebase as Groups**（将规则库视为组）以根据分配标记查看策略规则库的可视化表示.将规则库视为组时，将保留策略顺序和优先级。在此视图中，选择组标记以查看按此标记分组的所有规则。

名为 **Sanctioned** 的预定义标记可用于标记应用程序（**Objects**（对象）> **Applications**（应用程序））。要获取准确性，必须使用这些标记（Monitor（监控）> PDF Reports（PDF 报告）> SaaS Application Usage（SaaS 应用程序使用））。

您想了解什么内容？	请参阅：
如何创建标记？	创建标记
如何将规则库视为组？	将规则库视为组
搜索已标记的规则 使用标记对规则分组。 查看策略中使用的标记。 将标记应用到策略。	管理标记
了解更多？	• 使用标记分组并以可视方式区分对象 • SD-WAN 链路标签

创建标记

- **Objects**（对象）> **Tags**（标记）

选择 **Tags**（标记）可以创建标记，分配颜色，或删除、重命名和克隆标记。每个对象最多可以拥有 64 个标记；当某对象拥有多个标记时，它会显示应用的第一个标记的颜色。

在防火墙上，**Tags**（标记）选项卡会显示在防火墙上本地定义的标记或从 Panorama 推送到防火墙的标记。在 Panorama 上，此**Tags**（标记）选项卡会显示在 Panorama 上定义的标记。此选项卡不会显示为构成动态地址组从防火墙上定义的虚拟机信息源动态检索的标记，或显示使用 XML 或 REST API 定义的标记。

在创建新标记时，标记会在当前在防火墙或 Panorama 上选择的虚拟系统或设备组中自动创建。

标记设置	说明
姓名	输入唯一的标记名称（最多 127 个字符）。名称不区分大小写。
共享	如果想要将标记用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则标记只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。

© 2019 Palo Alto Networks, Inc.

标记设置	说明
	• Panorama 上的每个设备组。如果禁用（取消选中）此选项，则标记只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选择此选项可防止管理员在继承标记的设备组中替代此标记的设置。默认清除此选项，这意味着管理员可以替代继承标记的任何设备组的设置。
颜色	从下拉列表的调色板中选择一种颜色（默认为无）。
注释	可以添加使用标记的标签或说明。

- 添加标记：**Add**（添加）标记，然后填写完成以下字段：

  在**Policies (策略)**选项卡中创建或编辑策略时，也可以创建新标记。标记会在当前选择的设备组或虚拟系统中自动创建。
- 编辑标记：单击标记进行编辑、重命名，或是给标记分配一个颜色。
- 删除标记：单击 **Delete**（删除），并选择标记。不能删除预定义的标记。
- 移动或克隆标记：移动或克隆标记的选项可让您在为多个虚拟系统启用的防火墙上复制标记，或将标记移到不同的设备组或虚拟系统。

  移动或克隆，并选择标记。选择 **Destination**（目标）位置（设备组或虚拟系统）。如果希望验证过程发现对象的所有错误后再显示错误，请禁用（取消选择） **Error out on first detected error in validation**（输出验证中第一个检测到的错误）。默认情况下，已启用此选项，并且验证过程会在检测到第一个错误时停止，且仅显示此错误。
- 替代或恢复标记（仅限 Panorama）：如果在创建标记时尚未选择 **Disable override**（禁用替代）选项，则 **Override**（替代）选项可用。**Override**（替代）选项可让您替代从共享或父对象设备组继承的标记的分配颜色。**Location**（位置）是当前设备组。您还可以 **Disable override**（禁用替代）以防止未来发生的替代尝试。

  Revert（恢复）更改可撤销对标记所作的更改。恢复标记时，**Location (位置)**字段显示继承标记的源设备组或虚拟系统。

将规则库视为组

- **Policies**（策略）> **<Rulebase Type>**

View Rulebase as Groups（将规则库视为组）以使用组标记显示策略规则库。将规则库视为组时，将保留策略顺序和优先级。在此视图中，选择组标记以查看按此标记分组的所有规则。

将规则库视为组时，单击 **Group**（组）以移动、更改、删除或克隆选中标记组内所有规则。下表介绍了将规则库视为组时可用的规则管理选项。

选项	说明
将组内规则移至不同的规则库或设备组	将选中标记组内所有策略规则移至不同的规则库或设备组。
更改所有规则组	将选中标记组内所有规则移至不同的标记组。
移动组内所有规则	在规则库内移动选中标记组内所有规则。
删除组内所有规则	删除选中标记组内所有规则。

© 2019 Palo Alto Networks, Inc.

选项	说明
克隆组内所有规则	克隆选中标记组内所有规则。

将组内规则移至不同的规则库或设备组

如果需要组织规则库，请选择包含要移动的规则的标记组，并 **Move Rules in Group to Different Rulesbase or Device Group**（将组内规则移至不同的规则库或设备组）以将它们重新分配到不同的规则库或设备组（而不是单独移动每个规则）。在将标记组内规则移动到不同的设备组之前，设备组必须已经存在（不能在移动的同时进行创建设备组）。此外，您可以将标记组内规则移动到相同设备组的不同规则库中。

要将规则移至不同的规则库或设备组，请输入以下内容：

字段	说明
目标	移动策略规则的目标设备组。
（仅限 Panorama）目标类型	选择是否移动规则到目标设备组的 **Pre-Rulebase**（前导规则库）或 **Post-Rulebase**（后续规则库）。
规则顺序	选择规则库中移动规则的位置。您可以选择： • **Move Top**（移至顶部）可将规则移至目标设备组规则库的顶部。 • **Move Bottom**（移至底部）可将规则移至目标设备组规则库的底部。 • **Before Rule**（前导规则）将规则移动到目标设备组规则库选中规则的前面。 • **After Rule**（后续规则）将规则移动到目标设备组规则库选中规则的后面。
输出验证中第一个检测到的错误	勾选此框，可确定验证中所遇到错误的显示方式。如果勾选，则每个错误都会单独显示。如果未勾选，则错误会聚合，并显示为单个错误。 验证中检测到的错误会导致规则移动工作失败，且不会将规则移动到目标设备组。

更改所有规则组

不是编辑每个组，而是 **Change Group of All Rules**（更改所有规则组）将整个策略规则组从一个标记组移至另一个现有标记组。移到新标记组后，标记组规则的规则顺序将保持不变，但您可以选择将新规则放在目标标记组中规则的前面，也可以是它的后面。

要将规则移到不同的标记组，请指定目标标记组以及移动规则的放置位置。

字段	说明
从其外观顺序选择组	选择目标标记组。
移至顶部	**Move Top**（移至顶部）可从目标标记组顶部插入规则。
移至底部	**Move bottom**（移至底部）可从目标标记组底部插入规则。

© 2019 Palo Alto Networks, Inc.

移动组内所有规则

不是单独重新排序每个规则，而是 **Move All Rules in Group**（移动组内所有规则）以在规则层次结构中向上或向下移动选中标记组内所有规则。移到标记组后，标记组规则内已移动规则的规则顺序将保持不变，但您可以选择将新规则放在目标标记组中规则的前面，也可以是它的后面。

要移动规则，请指定目标标记组以及移动规则的放置位置。

字段	说明
从其外观顺序选择组	选择目标标记组。
移至顶部	**Move Top**（移至顶部）可从目标标记组前面插入规则。
移至底部	**Move Top**（移至顶部）可从目标标记组后面插入规则。

删除组内所有规则

要简化规则管理，您可以 **Delete All Rules in Group**（删除组内所有规则）来降低安全风险，并通过删除与所选标记组关联的未使用或不需要规则，从而确保您的策略规则库的规整性。

克隆组内所有规则

不是在标记组内手动重新创建现有策略规则，而是 **Clone All Rules in Group**（克隆组内所有规则），快速复制选中设备组和规则库内选中标记组中的规则。在将标记组内规则克隆到不同的设备组之前，设备组必须已经存在（不能在克隆的同时进行创建设备组）。此外，您可以将标记组内规则克隆到相同设备组的不同数据库中。

克隆规则可添加规则名称和以下格式：`<Rule Name>-1`。如果规则克隆到第一个克隆规则的同一个位置，且名称未做更改，则名称会附加。例如，`<Rule Name>-2`、`<Rule Name>-3` 等。

要克隆规则，请配置以下字段：

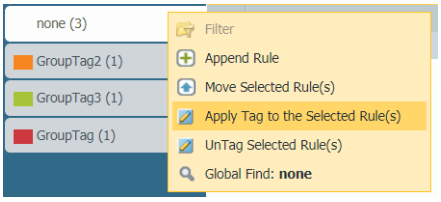
字段	说明
目标	克隆策略规则的目标设备组。
（仅限 Panorama）目标类型	选择是否克隆规则到目标设备组的 **Pre-Rulebase**（前导规则库）或 **Post-Rulebase**（后续规则库）。
规则顺序	选择规则库中克隆规则的位置。您可以选择： • **Move Top**（移至顶部）可从目标设备组规则库顶部插入克隆规则。 • **Move Bottom**（移至底部）可从目标设备组规则库底部插入克隆规则。 • **Before Rule**（前导规则）将克隆规则插入到目标设备组规则库选中规则的前面。 • **After Rule**（后续规则）将克隆规则插入到目标设备组规则库选中规则的后面。
输出验证中第一个检测到的错误	选中此选项，可确定验证中所遇到错误的显示方式。如果启用，则每个错误都会单独显示。如果禁用（清除），则错误会聚合，并显示为单个错误。 验证中检测到的错误会导致规则克隆工作失败，且不会将规则克隆到目标设备组。

© 2019 Palo Alto Networks, Inc.

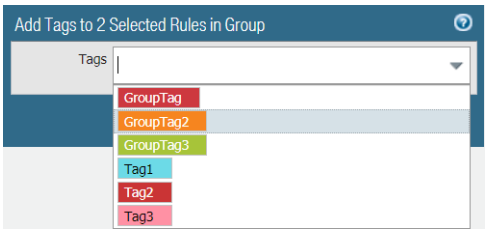
管理标记

下表列出了按组标记对规则进行分组时执行的操作。

- 标记规则。
  1. 选择 **View Rules as Groups**（将规则视为组）。
  2. 在右侧窗格上选择一个或多个规则。
  3. 从组标记下拉列表中，**Apply Tag to the Selected Rules**（应用标记到选中规则）。

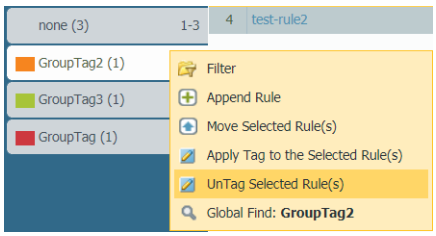


  4. 添加标记到选定规则。

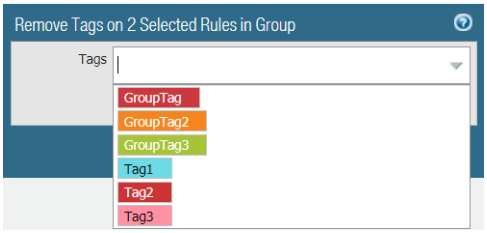


- 查看已分配有组标记的规则。
  1. **View Rulebase as Groups**（将规则库视为组）以查看您规则分配到的组标记。
  2. 右侧窗格会更新显示具有任何所选标记的组标记规则。
  3. 选中组标记以查看分配到该组的规则。未分配有组标记的规则将显示在 **none**（无）组中。

- 取消标记规则。
  1. **View Rulebase as Groups**（将规则库视为组）以查看您规则分配到的组标记。
  2. 在右侧窗格上选择一个或多个规则。
  3. 从组标记下拉列表中，**Apply Tag to the Selected Rules**（应用标记到选中规则）。



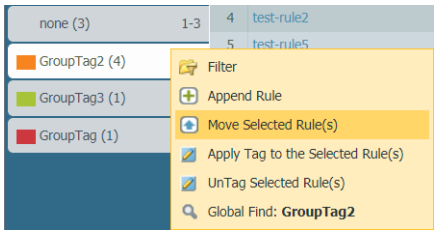
  4. 将标记移至选中规则中。此外，您可以对分配给规则的标记执行 **Delete All**（全部删除）。



- 使用标记对规则重新排序。

© 2019 Palo Alto Networks, Inc.

当您 **View Rulebase as Groups**（将规则视为组）时，选中组标记中的一个或多个规则，将鼠标悬停在规则编号上，然后从下拉列表中选择 **Move Selected Rule(s)**（移动选定规则）。如果想要移动所选组标记中所有规则，请勿选择任何规则。



在移动规则窗口中，从下拉列表中选择一个组标记，然后选择是要 **Move Before**（前移）还是 **Move After**（后移）在下拉列表中选择的标记。

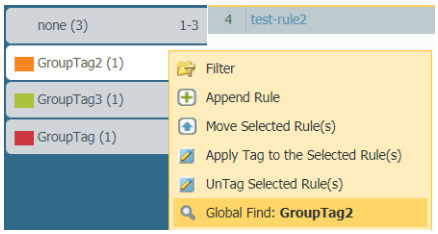
- 添加应用所选标记的新规则。

  当您 **View Rulebase as Groups**（将规则库视为组），将鼠标悬停在组标记上，然后从下拉列表中选择 **Append Rule**（附加规则）。

  新规则将附加到已分配到组标记中的规则列表末尾。

- 搜索组标记。

  当您 **View Rulebase as Groups**（将规则库视为组），将鼠标悬停在组标记上，然后从下拉列表中选择 **Append Rule**（附加规则）。



- 导出标记配置表格。

  管理角色可以 **PDF/CSV** 格式导出对象配置表格，并可应用筛选程序来自定义仅包含所需列的表格输出。仅导出 Export（导出）对话框中显示的列。请参阅导出配置表格数据。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Devices（设备）

也称为设备目录，该页面包括设备对象元数据。查看现有设备对象的信息，或是添加新的设备对象。在安全策略中将设备对象用作匹配标准，这样，您可以创建基于设备的策略，从而允许防火墙动态更新并应用安全策略到新设备和现有设备。Palo Alto Networks 将通过动态更新的方式更新设备目录，您可以通过**Device**（设备）> **Dynamic Updates**（动态更新）> **Device-ID Content**（设备 **ID** 内容）进行查看。

按钮/字段	说明
姓名	设备对象的名称。
位置	设备对象的设备组位置。
类别	设备对象的类别（例如，视频音频会议）。
配置文件	设备对象的设备配置文件。
模型	设备对象的型号。
操作系统版本	设备对象的操作系列版本。
操作系统系列	设备对象的操作系列系列。
供应商	设备对象的供应商。
添加	单击 **Add**（添加）以添加新的设备对象。输入 **Name**（名称），也可以选择输入 **Description**（说明）。选择设备的其他元数据，例如，**Category**（类别）、**OS**和 **Model**（型号）。您还可以 **Browse**（浏览）设备列表以选择您要添加的设备。单击 **OK**（确定）以确认您的更改。
删除	选择您再也不需要的设备对象，然后 **Delete**（删除）它。
移动	选择您要移动的设备对象，然后**Move**（移动）它。
克隆	选择您要在其上面放置新设备对象的设备对象，然后 **Clone**（克隆）它。
PDF/CSV	导出 **PDF/CSV** 格式的设备列表。您可以应用筛选器以根据需要创建更多的指定输出。将仅导出 Web 界面中所显示的列。请参阅配置表格导出。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> External Dynamic Lists（外部动态列表）

外部动态列表是指基于导出的 IP 地址、URL、域名、国际移动设备识别码(IMEI) 或国际移动用户识别码 (IMSI) 列表创建的地址对象，您可以在策略规格中使用该列表来阻止或允许流量。此列表必须是文本文件，并且必须保存到防火墙可以访问的 Web 服务器上。默认情况下，防火墙使用管理 (MGT) 接口检索此列表。

通过激活威胁阻止许可证，Palo Alto Networks 提供多个可用于阻止恶意主机的内置动态 IP 列表。这些列表会每日根据我们最新的威胁研究进行更新。

您可以将 IP 地址列表用作策略规则的源地址对象和目标地址对象；您可以在 URL 过滤配置文件（Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤））中使用 URL 列表，或将其用作安全策略规则的匹配标准；您可以将域列表用于 Objects（对象）> Security Profiles（安全配置文件）> Anti-Spyware Profile（防间谍软件配置文件），以便对指定域名执行 Sinkhole 操作。

对于每个防火墙型号，所有安全策略规则中可使用的唯一来源的外部动态列表上限是 30 个。防火墙支持的每个列表类型的最大条目数因防火墙型号而异（请参阅不同防火墙对每个外部动态列表类型设定的限制）。仅在策略规则中使用外部动态列表时，才考虑列表条目上限。如果超过防火墙型号所支持的最大条目数，防火墙将生成系统日志，并跳过超过该限制的条目。要检查策略中当前使用的 IP 地址、域、URL、IMEI 和 IMSI 的数量以及防火墙所支持的总数，请单击 **List Capacities**（列表容量）（仅限防火墙）。

外部动态列表根据评估顺序从上到下进行显示。使用页面底部的方向控制更改列表顺序。这样，您可以对列表进行重新排序，确保外部动态列表中最重要的条目能够在到达容量限制之前提交。

当列表按类型分组时，您无法更改外部动态列表顺序。

要检索外部动态列表承载服务器中的外部动态列表的最新版本，请选择一个外部动态列表，并 **Import Now**（立即导入）。

对于 *Palo Alto Networks* 恶意 *IP* 地址源，不能删除、克隆或编辑其设置。

Add（添加）新的外部动态列表，并配置下表所述的设置。

外部动态列表设置	说明
姓名	输入标识外部动态列表的名称（最多 32 个字符）。该名称用于标识策略规则实施列表。
共享 （仅限多个虚拟系统 (multi-vsys) 和 Panorama）	如果想要将外部动态列表用于以下位置，请启用此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。 如果禁用（取消选中）此选项，则外部动态列表只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。 如果禁用（取消选中）此选项，则外部动态列表只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。

© 2019 Palo Alto Networks, Inc.

外部动态列表设置	说明
禁用替代（仅限 Panorama）	启用此选项后，可阻止管理员替代设备组中继承对象的外部动态列表对象的设置。默认情况下，禁用（取消选中）此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
测试源 URL（仅限防火墙）	**Test Source URL**（测试源 **URL**）可验证防火墙是否可连接至承载外部动态列表的服务器。 此测试不能检查服务器验证是否成功。
创建列表选项卡	

类型
不能在单个列表中混用 *IP* 地址、*URL* 和域名。每个列表必须仅包含一种类型的条目。
	请从以下类型的外部动态列表中进行选择：
	• **Predefined IP List**（预定义 **IP** 列表）— 使用 Palo Alto Networks 标识为防弹 IP 地址、已知恶意 IP 地址或高风险 IP 地址的列表充当列表条目源（需要有效的威胁预防许可证）。
	• **Predefined URL List**（预定义 **URL** 列表）— 使用 Palo Alto Networks 标识为可信的域列表来从身份验证策略中排除这些域。
	• **IP List**（**IP** 列表）（默认）— 每个列表都可能包括 IPv4 或 IPv6 地址、地址范围和子网。此列表的每行必须仅包含一个 IP 地址、范围或子网。例如：
	`192.168.80.150/32`
	`2001:db8:123:1::1 or 2001:db8:123:1::/64`
	`192.168.80.0/24`
	`2001:db8:123:1::1 - 2001:db8:123:1::22`
	在上面的示例中，第一行指示的是从 192.168.80.0 到 192.168.80.255 的所有地址。一个子网或一个 IP 地址范围（如 92.168.20.0/24 或 192.168.20.40-192.168.20.50）被视为一个 IP 地址条目，而不是多个 IP 地址。
	• **Domain List**（域列表）— 每个列表的每行仅包含一个域名。例如：
	`www.p301srv03.paloalonetworks.com`
	`ftp.example.co.uk`
	`test.domain.net`
	对于外部动态列表中包含的域列表，防火墙将创建一组中等严重性的间谍软件类型的自定义签名，以允许对自定义的域列表使用 Sinkhole 操作。
	• **URL List**（**URL** 列表）— 每个列表的每行仅可有一个 URL 条目。例如：
	`financialtimes.co.in`
	`www.wallaby.au/joey`
	`www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx`
	`*.example.com/*`

© 2019 Palo Alto Networks, Inc.

外部动态列表设置	说明
	对于每个 URL 列表，默认操作均设为**Allow**（允许）。要编辑默认操作，请参阅 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 筛选）。
类型（续）	• **Subscriber Identity List**（订户标识列表）— 每个列表包括 3G、4G 或 5G 网络的用户 ID。在源字段中，输入 URL 以便防火墙访问列表。 • **Equipment Identity List**（设备标识列表）— 每个列表包括 3G、4G 或 5G 网络的设备 ID。在源字段中，输入 URL 以便防火墙访问列表。 根据您需要动态外部动态列表和静态条目支持的 *3G*、*4G* 和 *5G* 网络标识符总数，确定要购买的防火墙型号。
说明	输入外部动态列表的说明（最多 255 个字符）。
源	• 如果外部动态列表是预定义 IP 列表，则选择 **Palo Alto Networks - Bulletproof IP addresses**（防弹 **IP** 地址）-**Palo Alto Networks-High risk IP addresses**（高风险 **IP** 地址）或 **Palo Alto Networks - Known malicious IP addresses**（已知的恶意 **IP** 地址）作为列表源。 • 如果外部动态列表是预定义 URL 列表，则默认设置为 **panw-auth-portal-exclude-list**。 • 如果外部动态列表是 IP 列表、域列表或 URL 列表，则输入包括文本文件的 HTTP 或 HTTP URL 路径（例如，`http://192.0.2.20/myfile.txt`）。 • 如果外部动态列表是域列表，则默认设置为 **Automatically expand to include subdomains**（自动扩展以包括子域）。选中此选项后，PAN-OS® 软件可对外部动态列表文件中列出的域名的所有较低级构件进行评估。 • 如果外部动态列表是用户标识列表或设备标识列表，则输入包括列表的 URL 路径。 如果您的外部动态列表包含子域，则这些扩展条目将计入您的设备型号容量计数中。如果您想手动定义子域，则可以禁用此功能。但是，策略规则不会对该列表中未明确定义的子域进行评估。
证书配置文件 （仅限 IP 列表、域列表或 URL 列表）	如果外部动态列表包含 HTTPS URL，则选择现有证书配置文件（防火墙和 Panorama），或创建新的证书配置文件（仅限防火墙）来验证承载列表的 Web 服务器。有关配置证书配置文件的详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）。 默认：**None (Disable Cert profile)**（无（禁用证书配置文件）） 为最大限度地提高用于执行策略的外部动态列表数量，请使用相同的证书配置文件来验证使用相同源 *URL* 的外部动态列表，以便系统将这些列表仅视为一个外部动态列表。具有相同源 *URL*，使用不同证书配置文件的外部动态列表被视为唯一的外部动态列表。

© 2019 Palo Alto Networks, Inc.

外部动态列表设置	说明
客户端身份验证	启用此选项（默认情况下禁用）后，可为防火墙添加用户名和密码，以便在访问需要 HTTP 基本身份验证的外部动态列表源时使用。此设置仅在外部动态列表有 HTTPS URL 时可用。 • **Username**（用户名）— 输入访问列表的有效用户名。 • **Password/Confirm Password**（密码/确认密码）— 输入用户名的密码并确认。
检查更新	指定防火墙从 Web 服务器检索列表的频率。可以将防火墙检索列表的时间间隔设置为**Every Five Minutes**（每 5 分钟）（默认）、**Hourly**（每小时）、**Daily**（每天）、**Weekly**（每周）或 **Monthly**（每月）一次。间隔与最后一次提交有关。所以对于 5 分钟的间隔，如果最后一次提交在一个小时前，那么提交就在 5 分钟后。此提交将更新引用此列表的所有策略规则，以便防火墙可成功实施策略规则。 不必配置预定义 *IP* 列表的频率，因为防火墙可使用有效的威胁预防许可证动态接收内容更新。
列表条目和例外选项卡	
列表条目	显示外部动态列表的条目。 • **Add an entry as a list exception**（将条目添加为例外列表）— 最多选择 100 个条目，并单击 **Submit**（提交）(→)。 • **View an AutoFocus threat intelligence summary for an item**（查看项目的 **AutoFocus** 威胁情报摘要）— 将鼠标悬停于项目上方，然后从下拉列表中选择 **AutoFocus**。您必须具有 AutoFocus™ 许可证，并启用 AutoFocus 威胁情报以查看项目摘要（选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑**AutoFocus**设置）。 • **Check if an IP address, domain, or URL is in the external dynamic list**（检查外部动态列表中是否有 **IP** 地址、域或 **URL**）— 在过滤器字段中输入值，并单击 **Apply Filter**（应用过滤器）（→）。 **Clear Filter**（清除过滤器）（**[X]**）可重新查看完整列表。
手动例外	显示外部动态列表的例外。 • **Edit an exception**（编辑例外）— 选择例外，并更改内容。 • **Manually enter an exception**（手动输入例外）— 手动添加新的例外。 • **Remove an exception from the Manual Exceptions list**（从手动例外列表中删除例外）— 选择并 **Delete**（删除）列外。 • **Check if an IP address, domain, or URL is in the Manual Exceptions list**（检查手动例外列表中是否有 **IP** 地址、域或 **URL**）— 在过滤器字段中输入值，并单击 **Apply Filter**（应用过滤器）（→）。 **Clear Filter**（清除过滤器）（**[X]**）可重新查看完整列表。如果 Manual Exceptions（手动例外）列表中有重复的条目，则不能将更改内容保存到外部动态列表中。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Custom Objects（自定义对象）

创建自定义数据模式、漏洞和间谍软件签名，以及 URL 类别，以便与策略一同使用：

- Objects（对象）> Custom Objects（自定义对象）> Data Patterns（数据模式）
- Objects（对象）> Custom Objects（自定义对象）> Spyware/Vulnerability（间谍软件/漏洞）
- Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）

Objects（对象）> Custom Objects（自定义对象）> Data Patterns（数据模式）

以下主题介绍数据模式。

您在查找什么内容？	请参阅：
创建数据模式。	数据模式设置
了解有关正则表达式数据模式语法的更多信息，并查看某些示例。	正则表达式数据模式的语法 正则表达式数据模式示例

数据模式设置

选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **Data Patterns**（数据模式）以定义可能要筛选的敏感信息的类别。有关定义数据过滤配置文件的信息，请参阅 Objects（对象）> Security Profiles（安全配置文件）> Data Filtering（数据过滤）。

您可以创建在扫描敏感信息时防火墙要使用的三种数据模式：

- **Predefined**（预定义）— 使用预定义的数据模式扫描文件以获取社会保障号和信用卡号。
- **Regular Expression**（正则表达式）— 使用正则表达式创建自定义数据模式。
- **File Properties**（文件属性）— 扫描文件以获取特定文件属性和值。

数据模式设置	说明
姓名	输入数据模式名称（最多 31个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入数据模式的说明（最多 255 个字符）。
共享	如果想要将数据模式用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则数据模式只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则数据模式只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。

© 2019 Palo Alto Networks, Inc.

数据模式设置	说明
禁用替代（仅限 Panorama）	选择此选项可防止管理员在继承对象的设备组中替代此数据模式对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
模式类型	选择要安装的数据模式类型： • 预定义模式 • 正则表达式 • 文件属性
预定义模式	Palo Alto Networks 提供预定义数据模式以扫描文件中某些类型的信息，如信用卡号或社会保障号。要根据预定义模式配置数据过滤，请 **Add**（添加）模式并选择以下各项： • **Name**（名称）— 选择要用于过滤敏感数据的预定义模式。如果选择预定义模式，**Description**（说明）会自动填充。 • 选择要在其中检测预定义模式的 **File Type**（文件类型）。
正则表达式	**Add**（添加）自定义数据模式。输入模式的描述性 **Name**（名称），设置要扫描数据模式的 **File Type**（文件类型），然后输入定义 **Data Pattern**（数据模式）的正则表达式。 有关正则表达式数据模式的语法细节和示例，请参阅： • 正则表达式数据模式的语法 • 正则表达式数据模式示例
文件属性	构建数据模式以扫描文件属性和关联值。例如，**Add**（添加）数据模式以过滤 Microsoft Word 文档和 PDF，其中文档标题包括“敏感”、“内部”或“机密”词语。 • 输入数据模式的描述性 **Name**（名称）。 • 选择要扫描的 **File Type**（文件类型）。 • 选择要扫描特定值的 **File Property**（文件属性）。 • 输入要扫描的 **Property Value**（属性值）。

正则表达式数据模式的语法

用于创建数据模式的常规模式要求和语法取决于您启用的模式匹配 引擎：经典或增强（默认）。

模式要求	经典	增强
模式长度	需要 7 个文字字符，但不包括句号 (`.`)、星号(`*`)、加号 (`+`) 或范围 (`[a-z]`)。	需要 2 个文字字符。
不区分大小写	需要您定义所有可能的字符串的模式，以匹配各种不同形式的词语。 示例：要匹配指定为机密的所有文档，必须创建包含“confidential”、“Confidential”和“CONFIDENTIAL”的模式。	允许您在子模式上使用 **i** 选项。 示例：**`((?i)\bconfidential\b)`** 匹配 `ConfiDential`

© 2019 Palo Alto Networks, Inc.

PAN-OS® 中的正则表达式语法与传统正则表达式引擎类似，但每个引擎都是唯一的。经典语法和增强语法表用于描述 PAN-OS 模式匹配引擎支持的语法。

Classic Syntax（经典语法）

模式语法	说明
。	匹配任意单个字符。
?	与前面的字符或表达式匹配 0 次或 1 次。必须将常规表达式包含在圆括号内。 示例：**(abc)?**
*	与前面的字符或表达式匹配 0 次或多次。必须将常规表达式包含在圆括号内。 示例：**(abc)***
+	与前面的字符或正则表达式匹配一次或多次。必须将常规表达式包含在圆括号内。 示例：**(abc)+**
|	指定一个“或”另一个。 必须将替代子字符串包含在圆括号内。 示例：**((bif)|(scr)|(exe))** 匹配 bif、scr或 exe。
-	指定一个范围。 示例：**[c-z]** 匹配c和z之间的任意字符，包括 c 和 z。
[ ]	匹配任何指定的字符。 示例：**[abz]** 匹配 a、b 或 z中的任意字符。
^	匹配指定字符以外的任意字符。 示例：**[abz]** 匹配 a、b 或 z中的任意字符（特殊字符除外）。
{ }	匹配包含最小值和最大值的字符串。 示例：**{10-20}**匹配长度为 10 到 20 个字节的任意字符串，包含 10 个和 20 个字节。必须直接在固定字符串前面指定此字符，并且只能使用连字符 (-)。
\	对任意字符执行文字匹配。必须在指定字符前加上反斜杠 (\)。
&amp	与号 (&) 是特殊字符，因此要在字符串中查找 &，必须使用 **&amp**。

Enhanced Syntax（增强语法）

增强模式匹配引擎支持所有经典语法和下列语法：

© 2019 Palo Alto Networks, Inc.

模式语法	说明
Shorthand character classes（速记字符类） 代表特定类型字符的符号，例如，数字或空格。您可以使用大写字符来求反任何这些速记字符类。	
\s	匹配任何空格字符。 示例：**\s** 匹配空格、制表符、换行符或换页符。
\d	匹配 [0-9] 数字字符。 示例：**\d** 匹配 0。
\w	匹配 ASCII 字符[A-Za-z0-9_]。 示例：**\w\w\w** 匹配 PAN。
\v	匹配垂直空格字符，这包括所有 unicode 换行符。 示例：**\v** 匹配垂直空格字符。
\h	匹配水平空格字符，这包括制表符和所有“空格分隔符”unicode 字符。 示例：**\h** 匹配水平空格字符。
Bounded repeat quantifiers（有界重复量词） 指示重复上一项的次数。	
{n}	精确匹配次数 (*n*)。 示例：**a{2}** 匹配 aa。
{n,m}	**{n,m}**匹配 *n* 到 *m* 次。 示例：**a{2,4}** 匹配 aa、aaa和 aaaa
{n, }	**{n,}** 匹配至少 *n* 次。 示例：**a{2,}** 匹配 aaaaab 中的aaaaa。
Anchor characters（锚定字符） 指定匹配表达式的位置。	
^	在字符串开始匹配。如果启用多行模式 (**m**)，在每个换行符之后也匹配。 示例：假定字符串 abc，则 **^a** 匹配 a，但**^b**不与任何字符匹配，因为 b 不会出现在字符串的开头。
$	在字符串末尾匹配，或是在字符串末尾的换行符之前匹配。如果启用多行模式 (**m**)，在每个换行符之前也匹配。 示例：假定字符串 abc，则 **c$** 匹配 c，但**a$**不与任何字符匹配，因为 a 不会出现在字符串的末尾。

© 2019 Palo Alto Networks, Inc.

模式语法	说明
\A	在字符串开始匹配。即使启用多行模式 (m)，也不会在每个换行符之后匹配。
\Z	在字符串末尾以及最后的换行符之前匹配。即使启用多行模式 (m)，也不会在其他换行符之前匹配。
\z	在字符串绝对结尾处匹配。不会在换行符之前匹配。
Option modifiers（选项修饰符） 更改子模式的行为。输入要启用的 **(?<option>)** 或要禁用的 **(?-<option>)**。	
i	启用“不区分大小写”。 示例：**((?i)\bconfidential\b)** 匹配 ConfiDential。
m	使 **^** 和 **$** 在行的开头和末尾处匹配。
s	使 **.** 匹配任何字符，包括换行符。
x	忽略正则表达式标记之间的空格。

正则表达式数据模式示例

有效的自定义模式示例如下：

- .*((Confidential)|(CONFIDENTIAL))
  - 在任意位置查找单词“Confidential”或“CONFIDENTIAL”
  - 开头的“.*”指定在流中的任意位置进行查找
  - 根据解码器区分大小写的要求，此内容可能与“confidential”（全部小写）不匹配
- .*((Proprietary &amp Confidential)|(Proprietary and Confidential))
  - 查找“Proprietary & Confidential”或“Proprietary and Confidential”
  - 比查找“Confidential”更精确
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
  - 查找后接单词 draft 的各种形式的“Press Release”（这可能表明发行版并未准备好发往公司外部）
- .*(Trinidad)
  - 查找项目代号，如“Trinidad”

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Custom Objects（自定义对象）> Spyware/Vulnerability（间谍软件/漏洞）

防火墙支持使用防火墙威胁引擎来创建自定义间谍软件和漏洞签名的功能。可以编写自定义正则表达式模式，以标识间谍软件 Phone Home 通信或漏洞利用。生成的间谍软件和漏洞模式可在任意自定义漏洞配置文件中使用。防火墙在网络通信中查找自定义的模式并针对漏洞利用采取指定操作。

每周发布的内容定期放入了可以制作签名的新解码器和上下文。

通过每个间隔指定一个阈值以便为响应攻击而触发可能的操作，可以在定义自定义签名时可选地包括时间属性。只有在达到阈值之后，才会执行操作。

使用 **Custom Spyware Signature**（自定义间谍软件签名）页面可以定义防间谍软件配置文件的签名。使用 **Custom Vulnerability Signature**（自定义漏洞签名）页面可以定义漏洞防护配置文件的签名。

自定义漏洞和间谍软件签名设置	说明
配置选项卡	
威胁 ID	输入配置的数字标识符（间谍软件签名范围为 15000-18000 和 6900001 - 7000000；漏洞签名范围为 41000-45000 和 6800001-6900000）。
姓名	指定威胁名称。
共享	如果想要将自定义签名用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则自定义签名只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则自定义签名只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承签名的签名的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承签名的所有设备组的设置。
注释	输入可选注释。
严重性级别	分配表示威胁严重性的级别。
默认操作	如果符合威胁条件，则分配要执行的默认操作。有关操作列表，请参阅安全配置文件中的操作。
direction	表示评估威胁时是从客户端到服务器还是从服务器到客户端，或者两者皆是。
受影响系统	表示威胁是涉及客户端、服务器还是两者均涉及。适用于漏洞签名，而不适用于间谍软件签名。

© 2019 Palo Alto Networks, Inc.

自定义漏洞和间谍软件签名设置	说明
CVE	指定常见的漏洞枚举 (CVE) 作为外部参考以获取更多的背景和分析信息。
供应商	指定漏洞的供应商标识符作为外部参考以获取更多的背景和分析信息。
Bugtraq	指定 bugtraq（与 CVE 类似）作为外部参考以获取更多背景和分析信息。
引用	添加指向附加分析或背景信息的链接。当用户单击 ACC、日志或漏洞配置文件中的威胁时，会显示此信息。
Signature 选项卡	

标准签名	选择 **Standard**（标准），然后添加一个新签名。指定以下信息：
	• 标准— 输入名称以标识签名。
	• 注释— 输入可选说明。
	• 排序条件匹配— 选择签名条件的定义顺序是否重要。
	• 范围— 选择是仅将此签名应用于当前事务还是完整用户会话。
	单击 **Add Or Condition**（添加 **Or** 条件）或 **Add And Condition**（添加 **And** 条件），即可添加条件。要在组中添加条件，请选择组，然后单击添加条件。将条件添加到签名，以便在定义的条件参数适用时为流量生成签名。从下拉列表中选择一个 **Operator**（运算符）。运算符定义匹配流量时必须适用于自定义签名的条件的类型。从 **Less Than**（小于）、**Equal To**（等于）、**Greater Than**（大于）或 **Pattern Match**（模式匹配）中选择运算符。
	• 选择模式匹配运算符时，可指定以下适用于签名的选项来匹配流量：
	  • 上下文— 从可用上下文中选择。
	  • 模式— 指定正则表达式。有关正则表达式的模式规则，请参阅模式规则语法。
	  • 限定符和值—（可选）添加限定符/值对。
	  • **Negate**（求反）— 选择 **Negate**（求反），以使自定义签名仅在定义的“模式匹配”条件不成立时，才与流量匹配。此选项可让您确保在某些情况下，不触发自定义签名。
	  自定义签名不能仅使用“求反”条件创建；必须包含至少一个求正条件，才能指定求反条件。此外，如果签名范围设置为“会话”，则不能将“求反”条件配置为匹配流量的最后一个条件。
	  当流量与签名和签名例外都匹配时，可以使用生成求反签名的新选项定义自定义漏洞或间谍软件签名的例外。使用此选项可以允许网络中可以其他方式归类为间谍软件或漏洞攻击的某些流量。在这种情况下，可为与模式匹配的流量生成签名；对于与模式匹配同时与模式例外匹配的流量，则不生成签名，和任何关联的策略操作（例如阻止或丢弃）。例如，可以为重定向 URL 定义要生成的签名；但是，如果不对重定向到受信域的 URL 生成签名，也可以立即创建例外。

	• 选择 **Equal To**（等于）、**Less Than**（小于）或 **Greater Than**（大于）运算符时，可指定以下适用于签名的选项来匹配流量： • 上下文— 从 TCP 或 UDP 的未知请求和响应中选择。

© 2019 Palo Alto Networks, Inc.

自定义漏洞和间谍软件签名设置	说明
	• 位置— 在负载中的前四字节或第二个四字节之间选择。 • 掩码— 指定一个 4 字节的十六进制值，例如，0xffffff00。 • **Value** — 指定 4 字节十六进制值，例如，0xaabbccdd。
组合签名	选择 **Combination**（组合），然后指定以下信息： 选择 **Combination Signatures**（组合签名），指定用于定义签名的条件： • 通过单击添加 **AND** 条件或添加 **OR** 条件，添加条件。要在组中添加条件，请选择组，然后单击添加条件。 • 要在组中移动条件，请选择条件，然后单击 **Move Up**（上移）或 **Move Down**（下移）。要移动组，请选择组，然后单击 **Move Up**（上移）或 **Move Down**（下移）。无法将条件从一个组移动到另一个组。 选择 **Time Attribute**（时间属性）可指定以下信息： • 命中数— 指定将触发任何基于策略操作的阈值，作为在指定秒数 (1-3600) 中的很多匹配数 (1-1000)。 • 聚合标准— 指定按源 IP 地址、目标 IP 地址或源和目标 IP 地址的组合来跟踪匹配。 • 要在组中移动条件，请选择条件，然后单击 **Move Up**（上移）或 **Move Down**（下移）。要移动组，请选择组，然后单击 **Move Up**（上移）或 **Move Down**（下移）。无法将条件从一个组移动到另一个组。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）

使用自定义 URL 类别页面可创建自定义 URL 列表，并将其用于 URL 过滤配置文件，或在策略规则中用作匹配标准。在自定义 URL 类别中，您可逐个添加 URL 条目，或导入包含 URL 列表的文本文件。

添加到自定义类别的 *URL* 条目不区分大小写。

下表介绍了自定义 URL 设置：

自定义 URL 类别设置	说明
姓名	输入一个名称以标识自定义 URL 类别（最多 31 个字符）。此名称会在定义 URL 过滤策略时显示在类别列表中，同时也会在策略规则中显示为 URL 类别的匹配标准。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入 URL 类别的说明（最多 255 个字符）。
类型	选择类别类型： • **Category Match**（类别匹配）— 选择 **Category Match**（类别匹配）即可定义一个新的自定义类别，其中包含匹配所有指定 URL 类别的 URL（URL 必须与列表中的所有类别匹配）。指定 2-4 个类别。 • **URL List**（**URL** 列表）— 选择 **URL List**（**URL** 列表）即可添加或导入该类别的 URL 列表。此类别类型还包含 PAN-OS 9.0 之前添加的 URL。
共享	如果想要将 URL 类别用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果禁用（取消选中）此选项，则 URL 类别只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果禁用（取消选中）此选项，则 URL 类别只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的自定义 URL 对象的设置。默认情况下，禁用此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
站点	管理自定义 URL 类别的站点（添加或导入的每个 URL 最多可包含 255 个字符）。 • **Add**（添加）— **Add**（添加）URL，每行仅一个。每个 URL 的格式都可以是“www.example.com”，也可以包含通配符，如“*.example.com”。了解有关支持格式的其他信息，请参阅Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）中的阻止列表。 • **Import**（导入）— **Import**（导入），然后浏览以选择包含 URL 列表的文本文件。每行只能输入一个 URL。每个 URL 的格式都可以是“www.example.com”，也可以包含通配符，如“*.example.com”。

© 2019 Palo Alto Networks, Inc.

自定义 URL 类别设置	说明
	了解有关支持格式的其他信息，请参阅Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）中的阻止列表。 • **Export**（导出）— **Export**（导出）列表中包含的自定义 URL 条目（以文本文件方式导出）。 • **Delete**（删除）— **Delete**（删除）条目以将该 URL 从列表中删除。 要删除已在 *URL* 过滤配置文件中使用的自定义类别，则必须将操作设为 *None*（无），然后才可删除自定义类别。请参阅Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）中的类别操作。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）

安全配置文件在安全策略中提供威胁防护。每个安全策略规则可以包含一个或多个安全配置文件。可用配置文件类型如下：

- 防病毒配置文件，可防御蠕虫、病毒和特洛伊木马以及阻止间谍软件下载。请参阅 Objects（对象）> Security Profiles（安全配置文件）> Antivirus（防病毒）。
- 防间谍软件配置文件，可阻止受感染主机上的间谍软件尝试回拨或向外部命令与控制 (C2) 服务器发送信号。请参阅 Objects（对象）> Security Profiles（安全配置文件）> Anti-Spyware Profile（防间谍软件配置文件）。
- 停止尝试利用系统缺陷或获取未经授权的系统访问的漏洞保护配置文件。请参阅 Objects（对象）> Security Profiles（安全配置文件）> Vulnerability Protection（漏洞防护）。
- URL 过滤配置文件，可将用户访问限制到特定网站和/或网站类别，例如购物或赌博。请参阅 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）。
- 文件传送阻止配置文件，可按指定会话流方向（入站/出站/两者）阻止所选文件类型。请参阅 Objects（对象）> Security Profiles（安全配置文件）> File Blocking（文件阻止）。
- WildFire™ 分析配置文件，可指定要在 WildFire 设备本地或在 WildFire 云中执行的文件分析。请参阅 Objects（对象）> Security Profiles（安全配置文件）> WildFire Analysis（WildFire 分析）。
- 数据过滤配置文件，有助于阻止像信用卡或社会保险号这样的敏感信息离开受保护的网络。请参阅 Objects（对象）> Security Profiles（安全配置文件）> Data Filtering（数据过滤）。
- DoS 保护配置文件，可与 DoS 保护策略规则一起用于保护防火墙，抵御大量单会话和多会话攻击。请参阅 Objects（对象）> Security Profiles（安全配置文件）> DoS Protection（DoS 保护）。
- 移动网络保护配置文件，可让防火墙检测、验证和过滤 GTP 流量。

除单个配置文件以外，还可以组合通常一起应用的配置文件，并创建安全配置文件组（**Objects**（对象）> **Security Profile Groups**（安全配置文件组））。

安全配置文件中的操作

操作可指定防火墙响应威胁事件的方式。Palo Alto Networks 所定义的每一个威胁或病毒签名都包含默认操作，通常设置为 **Alert**（警报）（使用您启用的通知选项通知您）或 **Reset Both**（重置两者）（重置连接两端）。但是，您可以在防火墙上定义或替代操作。在定义防病毒配置文件、防间谍软件配置文件、漏洞保护配置文件、自定义间谍软件对象、自定义漏洞对象或 DoS 保护配置文件时，以下操作适用。

操作	说明	防病毒配置文件	防间谍软件配置文件	漏洞保护配置文件	自定义对象 — 间谍软件和漏洞	DoS 保护配置文件
Default（默认）	采取为每个威胁签名内部指定的默认操作。 对于防病毒配置文件，采取病毒签名的默认操作。	✓	✓	✓	—	随机早期丢弃
允许	允许应用程序流量。 *Allow*（允许）操作不会	✓	✓	✓	✓	—

© 2019 Palo Alto Networks, Inc.

操作	说明	防病毒配置文件	防间谍软件配置文件	漏洞保护配置文件	自定义对象 — 间谍软件和漏洞	DoS 保护配置文件
	生成与签名或配置文件相关的日志。					
警报	为每个应用程序流量流生成警报。警报保存在威胁日志中。	✓	✓	✓	✓	✓ 当攻击量 (cps) 达到配置文件中设置的警报阈值时生成警报。
Drop（丢弃）	丢弃应用程序流量。	✓	✓	✓	✓	—
重置客户端	对于 TCP，重置客户端连接。 对于 UDP，丢弃此连接	✓	✓	✓	✓	—
重置服务器	对于 TCP，重置服务器端连接。 对于 UDP，丢弃此连接	✓	✓	✓	✓	—
重置二者	对于 TCP，重置客户端和服务器端的连接。 对于 UDP，丢弃此连接	✓	✓	✓	✓	—
阻止 **IP**	阻止来自源或源-目标对的流量；指定时间段是可配置的。	—	✓	✓	✓	✓
Sinkhole	此操作可将对恶意域进行的 DNS 查询指向 Sinkhole IP 地址。 此操作适用于 Palo Alto Networks DNS 签名，以及 Objects（对象）> External Dynamic Lists（外部动态列表）中包含的自定义域。	—	—	—	—	—

© 2019 Palo Alto Networks, Inc.

操作	说明	防病毒配置文件	防间谍软件配置文件	漏洞保护配置文件	自定义对象 — 间谍软件和漏洞	DoS 保护配置文件
随机早期丢弃	当每秒连接数达到应用于 DoS 保护规则的 DoS 保护配置文件中的激活速率阈值时，促使防火墙随机丢弃数据包。	—	—	—	—	✓
同步 **Cookie**	当每秒连接数达到应用于 DoS 保护规则的 DoS 保护配置文件中的激活速率阈值时，促使防火墙生成 SYN Cookie 以便从客户端对 SYN 进行身份验证。	—	—	—	—	✓

不能删除策略规则中使用的配置文件；首先必须从策略规则中删除配置文件。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> Antivirus（防病毒）

使用防病毒配置文件页面可以配置防火墙用于扫描所定义流量的病毒的选项。设置应用程序应检测病毒和在检测到病毒时要执行的操作。默认配置文件对列出的所有协议解码器进行病毒检查，为简单邮件传输协议 (SMTP)、Internet 消息访问协议 (IMAP) 和邮局协议版本 3 (POP3) 生成警报，以及对其他应用程序采取默认操作（警报或拒绝），具体取决于检测到的病毒类型。配置文件可附加到安全策略规则中，用于确定将要检测的遍历特定区域的流量。

自定义的配置文件可以用于对受信安全区域之间的通信执行最低限度的防病毒检查，并对从非受信区域（如 Internet）接收到的通信以及发送到高敏感目标（如服务器场）的通信执行最大限度的检查。

如需添加新防病毒配置文件，选择添加，然后输入以下设置：

字段	说明
姓名	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在防病毒配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符、句点和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享 （仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的防病毒配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
Action Tab（操作选项卡） 指定针对不同流量类型的操作，例如 FTP 和 HTTP。	
启用数据包捕获	如果要捕获所识别的数据包，请选中此选项。
解码器和操作	对于要进行病毒检查的各种流量类型，请从下拉列表中选择操作。您可以为标准防病毒签名（**Signature Action**（签名操作）列）、 WildFire 系统生成的签名（**WildFire Signature Action**（**WildFire** 签名操作）列）、WildFire Inline ML 模型实时检测到的恶意威胁（**WildFire Inline ML Action**（**WildFire Inline ML** 操作）列）定义各种不同的操作。 某些环境可能需要较长的防病毒签名预备时间，因此该选项可以用来为 Palo Alto Networks 提供的两种防病毒签名类型设置不同操作。例如，在发布之前需要经过较长的预备时间（24 小时）的标准防病毒签名，以及在检测到威胁后可以在 15 分钟内生成和发布的 WildFire 签名。为此，您可以选择 WildFire 签名的警报操作，而不是阻止。

© 2019 Palo Alto Networks, Inc.

字段	说明
	为了获得最佳安全性，克隆默认防病毒配置文件，并将所有解码器的操作和 *WildFire* 操作设置为 *reset-both*（重置两者），然后附加配置文件到允许流量的所有安全策略规则。
应用程序例外和操作	**Applications Exception**（应用程序例外）表可让您定义不接受检查的应用程序。例如，若要阻止除特定应用程序以外的所有 HTTP 通信，则可以定义该应用程序对其是例外情况的防病毒配置文件。阻止是针对 HTTP 解码器的操作，而允许是针对该应用程序的例外情况。对于每个应用程序例外情况，选择检测到威胁时要采取的操作。有关操作列表，请参阅安全配置文件中的操作。 若要查找应用程序，请开始在文本框中键入应用程序名称。随即将显示应用程序的匹配列表，然后可以进行选择。 如果您认为合法应用程序被错误标识为携带病毒（误报），则使用 *TAC* 打开支持案例，这样，*Palo Alto Networks* 就可以进行分析，并修复错误的标识病毒。问题得到解决后，请删除该配置文件中的例外。

Signature Exceptions Tab（签名例外选项卡）

使用 **Signature Exceptions**（签名例外）选项卡以定义防病毒配置文件忽略的威胁的列表。

仅当您确定标识的病毒不是威胁时才能创建病毒例外（误报）。如果您认为自己发现一个误报，则使用 *TAC* 打开支持案例，这样，*Palo Alto Networks* 就可以进行分析，并修复错误的标识病毒签名。一旦问题得到解决，应立即删除该配置文件中的例外。

威胁 ID	要添加要忽略的特定威胁，请一次输入一个威胁 ID，然后单击 **Add**（添加）。威胁 ID 显示为威胁日志信息的一部分。请参阅 Monitor（监控）> Logs（日志）。

WildFire Inline ML Tab（**WildFire Inline ML** 选项卡）

使用 **WildFire Inline ML**选项卡，可通过基于防火墙的机器学习模型启用和配置文件的 WildFire 实时分析。

Palo Alto Networks 建议在启用 *Wildfire inline ML* 后，转发样本到 *Wildfire* 云。这样，可在第二次分析时自动纠正触发误报的样本。此外，还可提供数据用于在未来更新时改善 *ML* 模型。

可用模型	对于每个可用的 WildFire inline ML **Model**（模型），您可以选择以下操作设置之一： • **enable (inherit per-protocol actions)**（启用（继承每个协议操作））— 根据您在 **Action**（操作）选项卡解码器部分 **WildFire Inline ML Action**（**WildFire Inline ML** 操作）列中的选择检查流量。 • **alert-only (override more strict actions to alert)**（仅限警报（覆盖最严格的警报操作））— 根据您在 **Action**（操作）选项卡解码器部分 **WildFire Inline ML Action**（**WildFire Inline ML** 操作）列中的选择检查流量。严重性级别高于警报的任何操作（丢失、重置客户端、重置服务器、重置两者）都将被覆盖为警报，允许流量通过，同时又能在威胁日志中生成并保存警报。 • **disable (for all protocols)**（禁用（对于所有协议））— 允许流量通过，无需任何策略操作。
文件例外	通过 **File Exceptions**（文件例外）表，您可以定义您不想分析的特定文件，例如，误报。

© 2019 Palo Alto Networks, Inc.

字段	说明
	要创建新的文件例外条目，请 **Add**（添加）新条目，并提供要从实施中排除的文件的部分哈希、文件名和说明。 要查找现有文件例外，请从在文本框中输入部分哈希值、文件名或说明开始。与任何这些值匹配的文件例外列表都将显示。 您可以在威胁日志中查找部分哈希（*Monitor*（监视）> *Logs*（日志）> *Threat*（威胁））。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> Anti-Spyware Profile（防间谍软件配置文件）

您可以将防间谍软件配置文件附加到安全策略规则中，以便检测系统上安装的间谍软件以及各种类型的命令和控制 (C2) 恶意软件在您的网络中启动的连接。您可以在两个预定义防间谍软件配置文件之间进行选择，以附加到安全策略规则中。每个配置文件都有一组按威胁的严重性组织的预定义规则（包含威胁签名）；每个威胁签名都包含一个由 Palo Alto Networks 指定的默认操作。

- 默认 — 默认配置文件按照创建签名时 Palo Alto Networks 内容数据包指定的设置，对每个签名使用默认操作。
- 严格 — 严格配置文件将替代严重、高和中等严重性威胁的签名文件中定义的操作，并将其设置为**reset-both**（重置两者）操作。对严重性为低和信息性的威胁执行默认操作。
- 此外，您也可以创建自定义配置文件。例如，可以降低对受信安全区域之间的流量执行防间谍软件检查的严格性要求，对从 Internet 接收到的流量或发送到受保护资产（如服务器场）的流量执行最大限度地检查。

下表介绍了防间谍软件配置文件设置：

防间谍软件配置文件设置	说明
姓名	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在防间谍软件配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符、句点和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的防间谍软件配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
Signature Policies Tab（签名策略选项卡） 防间谍软件规则可让您定义自定义严重性、要对任何威胁执行的操作、包含所输入文本的特定威胁名称和/或按威胁类别（如广告软件）进行定义。 添加新规则，或选择现有规则，然后选择 **Find Matching Signatures**（查找匹配的签名），根据该规则过滤威胁签名。	
规则名称	指定规则名称。

© 2019 Palo Alto Networks, Inc.

防间谍软件配置文件设置	说明
威胁名称	输入任何以匹配所有签名，或输入文本以匹配包含输入的文本（作为签名名称的一部分）的任何签名。
类别	选择一个类别，或是选择任何以匹配所有类别。
操作	为每个威胁选择操作。有关操作列表，请参阅安全配置文件中的操作。 默认操作以预定义的操作为基础，是 Palo Alto Networks 提供的每个签名的一部分。要查看签名的默认操作，请选择**Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件），然后 **Add**（添加）或选择现有配置文件。单击 **Exceptions**（例外）选项卡，然后单击 **Show all signatures**（显示所有签名），以查看所有签名和关联操作的列表。 为了获得最佳安全性，请使用预定义 *strict*（严格）配置文件中的操作设置。
数据包捕获	如果要捕获所识别的数据包，请选中此选项。 选择**single-packet**（单个数据包）选项可以在检测到威胁时捕获一个数据包，或选择**extended-capture**（扩展捕获）选项可以捕获 1 至 50 个数据包（默认为 5 个数据包）。扩展捕获可以在分析威胁日志时提供有关威胁的更多上下文信息。要查看数据包捕获，请选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），并找到所需的日志条目，然后单击第二列中的绿色向下箭头。要定义要捕获的数据包数量，请选择 **Device**（设备）> **Setup**（设置）> **Content-ID**，然后编辑 Content-ID™ 设置。 如果针对特定威胁的操作是允许，则防火墙不会触发威胁日志，也不会捕获数据包。如果操作是警报，则您可以将数据包捕获设为单个数据包捕获或扩展捕获。所有阻止操作（丢弃、阻止和重置操作）都能捕获单个数据包。默认操作取决于设备上的内容数据包。 为严重、高和中等严重性事件启用扩展捕获。使用 *5* 个数据包的默认扩展捕获值，这可提供足够的信息以分析大多数情况下的威胁。（过多数据包捕获流量可能会导致丢弃数据包捕获。）请勿为信息性和低严重性事件启用扩展捕获，因为与较高严重性事件相关的捕获信息相比，它不是很有用，且会创建相对较高的低值流量。
严重性级别	选择安全级别（严重、高、中、低或信息性）。
Signature Exceptions Tab（签名例外选项卡） 可让您更改特定签名的操作。例如，您可以对一组特定签名生成警报，阻止与所有其他签名匹配的所有数据包。在发生误报时通常会配置威胁异常。要简化威胁例外的管理，可以直接从 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁）列表添加威胁例外。确保获取最新的内容更新，以便防御新的威胁，拥有所有假阳性误报的新签名。	
异常	**Enable**（启用）想要分配操作的每个威胁，或选择 **All**（全部），以响应所有列出的威胁。列表取决于所选主机、类别和严重性。如果列表为空，则对于当前选择项不存在威胁。 使用 IP 地址免除可以向威胁例外添加 IP 地址过滤器。如果将 IP 地址添加到威胁例外中，则仅当其源或目标 IP 地址与例外中的 IP 地址匹配的会话触发签名

© 2019 Palo Alto Networks, Inc.

防间谍软件配置文件设置	说明
	时，该签名的威胁例外操作才会替代规则的操作。每个签名最多可以添加 100 个 IP 地址。使用此选项，无需创建新策略规则和新漏洞配置文件，即可为特定 IP 地址创建异常。 仅当您确定标识为间谍软件的签名不是威胁时才能创建例外（这是误报）。如果您认为自己发现一个误报，则使用 *TAC* 打开支持案例，这样，*Palo Alto Networks* 就可以进行分析，并修复错误的标识签名。一旦问题得到解决，应立即删除该配置文件中的例外。
DNS Policies Tab（DNS 策略选项卡） **DNS Policies（DNS 策略）**设置提供用于标识网络上感染的主机的其他方法。这些签名会检测与基于 DNS 的威胁关联的主机名的特定 DNS 查找。	
您可以使用单独的策略操作、日志严重性级别和数据包捕获设置配置特定的 DNS 签名源。botnet 报告中会显示执行恶意软件域的 DNS 查询的主机。此外，如果要对恶意 DNS 查询执行 Sinkhole 操作，可以在**DNS Sinkhole Settings（DNS Sinkhole 设置）**中指定执行 Sinkhole 操作的 IP。	
DNS 签名源	可在出现 DNS 查询时，让您选择要执行操作的列表。有两个默认 DNS 签名策略选项： • **Palo Alto Networks Content（Palo Alto Networks 内容）**— 通过动态内容更新更新的本地可下载签名列表。 • **DNS Security（DNS 安全）**— 基于云的 DNS 安全服务，可对 DNS 数据执行主动分析，并提供对整个 Palo Alto Networks DNS 签名数据库的实时访问。 除威胁防护许可证外，此服务还需要购买和激活 *DNS* 安全许可证。 • **External Dynamic Lists（外部动态列表）**— 已创建的动态域列表，该列表用于基于列表类型实施特定操作，例如，允许列表。域列表策略操作默认配置为 **Allow（允许）**，且优先于所有其他签名类型。 除威胁防护许可证外，此服务还需要购买和激活 *DNS* 安全许可证。 默认情况下，对本地访问的 Palo Alto Networks 内容 DNS 签名执行 Sinkhole 操作，同时将基于云的 DNS 安全设置为允许。如果想要使用 DNS 安全启用 sinkholing，则必须将 DNS 查询上的操作配置为 Sinhole。用于执行 Sinkhole 操作的默认地址属于 Palo Alto Networks(sinkhole.paloaltonetworks.com)。此地址不是静态地址，可通过防火墙或 Panorama 上的内容更新进行修改。 **Add（添加）**新列表，然后选择已创建的类型域的外部动态列表。要创建新列表，请参阅 Objects（对象）> External Dynamic Lists（外部动态列表）。
日志严重性	允许您指定防火墙检测到与 DNS 签名匹配的域时记录的日志严重性级别。
策略操作	选择在执行 DNS 查找以获取已知恶意软件站点时执行的操作。可选操作为 **alert（警报）**、**allow（允许）**、**block（阻止）**或 **sinkhole**。适用于 Palo Alto Networks DNS 签名的默认操作为 **sinkhole**。 DNS Sinkhole 操作可以为管理员提供使用 DNS 流量确定网络中受感染的主机的方法，即使防火墙在本地 DNS 服务器中检测不到任何内容（例如，防火墙检测不到 DNS 查询的来源）。在安装威胁预防许可证和在安全配置文件中启用防

© 2019 Palo Alto Networks, Inc.

防间谍软件配置文件设置	说明
	间谍软件配置文件后，基于 DNS 的签名将会触发恶意软件域中的定向 DNS 查询。在防火墙在本地 DNS 服务器中检测不到任何内容的典型部署中，威胁日志将确定本地 DNS 解析器作为流量的来源，而不是实际受感染的主机。Sinkholing 恶意 DNS 查询通过伪造对恶意域中定向查询的响应解决这种可见性问题，以便客户端试图连接到恶意域（如对于命令和控制），而不是试图连接到管理员指定的 IP 地址。然后，可以在流量日志中轻易地识别受感染的主机，因为试图连接到 Sinkhole IP 地址的任何主机最有可能被恶意软件感染。 当防火墙无法看到 *DNS* 查询的来源时（通常是当防火墙在本地 *DNS* 服务器中检测不到任何内容时），启用 *DNS sinkhole* 操作，以便您标识受感染的主机。如果不能对流量执行 *sinkhole* 操作，则阻止它。
数据包捕获	如果要捕获所识别的数据包，请为给定源选中此选项。 对执行过 *sinkhole* 操作的流量启用数据包捕获，这样，您可以对其进行分析，并获取有关受感染主机相关的信息。
DNS Sinkhole 设置	确定 DNS 签名源的 Sinkhole 操作后，请指定要用于 Sinkhole 操作的 IPv4 和/或 IPv6 地址。默认情况下，Sinkhole IP 地址设置为 Palo Alto Networks 服务器。之后，您可使用流量日志，或构建一个定制报告，以过滤 Sinkhole IP 地址并标识受影响的客户端。 以下是在 DNS 请求启用 Sinkhole 操作后将要发生的事件顺序： 受恶意软件感染的客户端计算机发送 DNS 查询解析 Internet 中的恶意主机。 将客户端的 DNS 查询发送到内部 DNS 服务器，然后查询位于防火墙另一端的公共 DNS 服务器。 DNS 查询对指定 DNS 签名数据库源中的 DNS 条目进行匹配，以便针对查询执行 Sinkhole 操作。 然后，受感染的客户端试图与主机开始会话，但使用伪造的 IP 地址。伪造的 IP 地址是在选择 Sinkhole 操作时在防间谍软件配置文件“DNS 签名”选项卡上定义的地址。 管理员在威胁日志中收到恶意 DNS 查询的警报，然后可以搜索 Sinkhole IP 地址的流量日志，并轻松找到用来试图与 Sinkhole IP 地址开始会话的客户端 IP 地址。

DNS Exceptions Tab（DNS 例外选项卡）

您可以通过 DNS 签名例外从策略实施中排除特定威胁 ID，并为批准的域源指定域/FQDN 允许列表。

要添加想要从策略中排除的特定威胁，请选择或搜索 **Threat ID**（威胁 **ID**），并单击 **Enable**（启用）。每个条目可提供对象的威胁 **Threat ID**（威胁 **ID**）、**Name**（名称）和 **FQDN**。

若要 **Add**（添加）域或 FQDN 允许列表，请提供允许列表的位置以及适当的说明。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> Vulnerability Protection（漏洞保护）

安全策略规则包括指定漏洞防护配置文件，后者可根据缓冲区溢出、非法代码执行以及其他利用系统漏洞的尝试来确定保护的级别。有两种预定义的配置文件适用于漏洞保护功能：

- 默认配置文件将默认操作应用到所有客户端和服务器的关键、高和中等严重性漏洞。它不检测低和信息漏洞保护事件。默认操作取决于设备上的 Palo Alto Networks 内容数据包。
- 严格配置文件将阻止响应应用到所有客户端和服务器的关键、高和中等严重性间谍事件，并使用低和信息漏洞保护事件的默认操作。

自定义的配置文件可以用于对受信安全区域之间的通信执行最低限度的漏洞检查，并对从非受信区域（如 Internet）接收到的通信以及发送到高敏感目标（如服务器场）的通信执行最大限度的检查。要将漏洞防护配置文件应用到安全策略，请参阅 Policies（策略）> Security（安全）。

应用漏洞保护配置文件到允许流量的每个安全策略规则，防止缓冲区溢出，不合法的代码执行，以及其他试图探测客户端和服务器端漏洞的行为。

“规则”设置指定要启用的签名的集合，以及触发集合中的签名时要执行的操作。

使用“异常”设置可以更改对特定签名的响应。例如，可阻止匹配某个签名的所有数据包，但有一个所选数据包除外，它将生成警报。异常选项卡支持过滤功能。

漏洞保护页面提供一组默认列。通过使用列选择器可获得其他信息列。单击列标题右侧的箭头，然后从“列”子菜单中选择列。

下表介绍了漏洞防护配置文件设置：

漏洞保护配置文件设置	说明
姓名	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在漏洞防护配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符、句点和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的漏洞防护配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
规则选项卡	
规则名称	指定名称以标识规则。

© 2019 Palo Alto Networks, Inc.

漏洞保护配置文件设置	说明
威胁名称	指定要匹配的文本字符串。防火墙通过搜索此文本字符串的签名名称，将一组签名应用于规则。
CVE	如果要将签名限制为同时与指定的 CVE 匹配的签名，则指定常见漏洞和暴露 (CVE)。 每个 CVE 的格式均为 CVE-yyyy-xxxx，其中 yyyy 为年份，xxxx 是唯一标识符。可对此字段执行字符串匹配。例如，要查找 2011 年的漏洞，请输入“2011”。
主机类型	指定将规则的签名限制为客户端、服务器端还是二者任意一项（任何）的签名。
严重性级别	如果要将签名限制为同时与指定的严重性匹配的签名，则选择要匹配的严重性（信息性、低、中、高或严重）。
操作	选择触发规则时要执行的操作。有关操作列表，请参阅安全配置文件中的操作。 默认操作以预定义的操作为基础，是 Palo Alto Networks 提供的每个签名的一部分。要查看签名的默认操作，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Vulnerability Protection**（漏洞防护），然后 **Add**（添加）或选择现有配置文件。单击 **Exceptions**（例外）选项卡，然后单击 **Show all signatures**（显示所有签名），以查看所有签名和关联操作的列表。 为了获得最佳安全性，设置客户端和服务器关键、高和中等严重性事件的操作为 *reset-both*（重置两者），并为信息性和低严重性事件使用默认操作。
数据包捕获	如果要捕获所识别的数据包，请选中此选项。 选择**single-packet**（单个数据包）选项可以在检测到威胁时捕获一个数据包，或选择**extended-capture**（扩展捕获）选项可以捕获 1 至 50 个数据包（默认为 5 个数据包）。扩展捕获可以在分析威胁日志时提供威胁的更多上下文信息。要查看数据包捕获，请选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），并找到所需的日志条目，然后单击第二列中的绿色向下箭头。要定义应捕获的数据包数量，请选择 **Device**（设备）> **Setup**（设置）> **Content-ID**，然后编辑 Content-ID 设置。 如果针对特定威胁的操作是允许，则防火墙不会触发威胁日志，也不会捕获数据包。如果操作是警报，则您可以将数据包捕获设为单个数据包捕获或扩展捕获。所有阻止操作（丢弃、阻止和重置操作）都能捕获单个数据包。默认操作取决于设备上的内容数据包。 为严重、高和中等严重性事件启用扩展捕获，为低严重性事件启用单数据包捕获。使用 5 个数据包的默认扩展捕获值，这可提供足够的信息以分析大多数情况下的威胁。（过多数据包捕获流量可能会导致丢弃数据包捕获。）请勿为信息性事件启用数据包捕获，因为与较高严重性事件相关的捕获信息相比，它不是很有用，且会创建相对较高的低值流量。 使用您用于确定要记录的流量的相同逻辑应用扩展数据包捕获 — 为您记录的流量启用扩展捕获，包括您阻止的流量。
Exceptions 选项卡	

© 2019 Palo Alto Networks, Inc.

漏洞保护配置文件设置	说明
启用	为需要分配操作的每个威胁选择 **Enable**（启用），或选择 **All**（全部），以响应所有列出的威胁。列表取决于所选主机、类别和严重性。如果列表为空，则对于当前选择项不存在威胁。
ID	
供应商 ID	如果要将签名限制为同时与指定的供应商 ID 匹配的签名，则指定供应商 ID。 例如，Microsoft 供应商 ID 的形式为 Msyy-xxx，其中 yy 为两位数的年份，xxx 是唯一标识符。例如，要匹配 2009 年的 Microsoft，请在搜索字段输入“MS09”。
威胁名称	仅当您确定标识的威胁不是威胁时才能创建威胁例外（误报）。如果您认为自己发现一个误报，则使用 *TAC* 打开支持案例，这样，*Palo Alto Networks* 就可以进行调查错误的标识威胁。一旦问题得到解决，应立即删除该配置文件中的例外。 漏洞签名数据库包含可以指示暴力攻击的签名；例如，在 FTP 暴力攻击时，将触发威胁 ID 40001。在特定时间阈值内发生某种情况时，将触发暴力签名。阈值是为暴力攻击签名预配置的，可以通过单击 **Vulnerability**（漏洞）选项卡上威胁名称旁边的编辑图标 ( ) 进行更改（选择 **Custom**（自定义）选项后）。可以指定每个单位时间的匹配数，以及阈值是应用于源或目标还是同时应用于源和目标。 阈值可以应用于源 IP、目标 IP 或源 IP 和目标 IP 的组合。 默认操作用圆括号括起。
IP 地址免除	单击 **IP Address Exemptions**（**IP** 地址免除）列，可将 IP 地址过滤器**Add**（添加）到威胁例外中。在将 IP 地址添加到威胁例外中后，仅当其源或目标 IP 地址与例外中的 IP 地址匹配的会话触发签名时，该签名的威胁例外操作才优先于规则的操作。每个签名最多可以添加 100 个 IP 地址。必须输入单播 IP 地址（即没有网络掩码的地址），如 10.1.7.8 或 2001:db8:123:1::1。添加 IP 地址免除后，无需创建新策略规则和新漏洞配置文件，即可为特定 IP 地址创建例外。
rule	
CVE	**CVE**列显示常见漏洞和暴露 (CVE) 的标识符。这些唯一的公共标识符用于熟知的信息安全漏洞。
主机	
类别	如果要将签名限制为与该类别匹配的签名，则选择漏洞类别。
严重性级别	
操作	从下拉列表中选择操作，或从列表顶部的 **Action**（操作）下拉列表中选择操作，可将相同的操作应用到所有威胁。
数据包捕获	如果要捕获已标识的数据包，请选中 **Packet Capture**（数据包捕获）。

© 2019 Palo Alto Networks, Inc.

漏洞保护配置文件设置	说明
显示所有签名	启用 **Show all signatures**（显示所有签名）以列出所有签名。如果禁用 **Show all signatures**（显示所有签名），则仅列出例外签名。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）

您可以使用 URL 过滤配置文件控制对 Web 内容的访问，还可控制用户与 Web 内容交互的方式。

您在查找什么内容？	请参阅：
根据 URL 类别控制访问网站。	URL 过滤类别
检测公司凭据提交情况，然后控制用户提交凭据所使用的 URL 类别。	用户凭据检测 URL 过滤类别
在最终用户未使用最严格的安全搜索设置时阻止搜索结果。	URL 过滤设置
启用 HTTP 标头的日志记录。	URL 过滤设置
使用自定义 HTTP 标头控制对网站的访问。	HTTP 标头插入
启用 inline ML 以实时分析 Web 页面，确定该页面是否包含恶意内容。	URL 过滤 Inline ML
了解更多？	• 了解有关如何配置 URL 过滤的更多信息。 • 使用 URL 类别防止凭据网络钓鱼。 • 要创建自定义类别，请选择 Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）。 • 要导入您想实施的 URL 列表，请选择Objects（对象）> External Dynamic Lists（外部动态列表）。

URL 过滤常规设置

下表介绍了常规 URL 过滤设置：

常规设置	说明
名称	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在 URL 过滤配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。

© 2019 Palo Alto Networks, Inc.

常规设置	说明
	• Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选择该选项以防止管理员在继承配置文件的设备组中覆盖该 URL 过滤配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。

URL 过滤类别

选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）> **Categories**（类别）以根据 URL 类别控制对网站的访问权限。

类别设置	说明
类别	显示您可以为其定义 Web 访问和使用策略的 URL 类别以及列表。默认情况下，所有类别的 **Site Access**（站点访问）和 **User Credential Submission**（用户凭证提交）权限设置为 **Allow**（允许）。 URL 类别和列表可通过三个下拉列表进行分组： • **Custom URL Categories**（自定义 **URL** 类别）— 选择 Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）以定义自定义 URL 类别。您可以将自定义 URL 类别基于 URL 列表或多个预定义类别。 • **External Dynamic URL Lists**（外部动态 **URL** 列表）— 选择Objects（对象）> External Dynamic Lists（外部动态列表）后可使防火墙从 Web 服务器导入 URL 列表。 • **Pre-defined Categories**（预定义列表）— 列出 PAN-DB、Palo Alto Networks URL 和 IP 云数据库定义的所有 URL 类别列表。 *Block*（阻止）所有危险的已知 *URL* 类别，以防止利用漏洞、恶意软件下载、命令和控制活动以及数据泄露：*command-and-control*（命令和控制）、*copyright-infringement*（版权侵权）、*dynamic-dns*（动态 *DNS*）、*extremism*（极端主义）、*malware*（恶意软件）、*phishing*（网络钓鱼）、*proxy-avoidance-and-anonymizers*（代理规避和匿名者）、*unknown*（未知）、*newly-registered-domain*（新注册域）、*grayware*（灰色软件）和 *parked*（寄放）。 要在阻止策略中分级，则将类别设为 *continue*（继续），并创建自定义响应页面，告知客户您的使用策略，警告他们正在访问的站点可能有威胁。经过一段适当的时间后，转换为可以阻止这些潜在恶意站点的策略。
站点访问	对于每个 URL 类别，选择当用户尝试访问该类别中的 URL 时要采取的操作： • **alert**（警报）— 允许访问网站，但在每次用户访问 URL 时会将警报添加到 URL 日志。 设置 *alert*（警报）为用于您不会阻止的流量类别的操作，这样，就可以记录访问尝试，并提供对流量的可见性。 • **allow**（允许）— 允许访问网站。

© 2019 Palo Alto Networks, Inc.

类别设置	说明
	因为 *allow*（允许）不能记录未阻止流量，如果您想记录访问尝试，并提供对流量的可见性，可以设置 *alert*（警报）为用于您不会阻止的流量类别的操作。 • **block**（阻止）— 阻止访问网站。如果 URL 类别的站点访问设置为阻止，则也会自动将用户凭证提交权限设置为阻止。 • **continue**（继续）— 向用户显示警告页面，以阻止他们访问网站。然后，如果用户决定忽略该警告，则必须选择 **Continue**（继续）访问该网站。 继续（警告）页面不会正常显示在配置为使用代理服务器的客户端机器上。 • **override**（替代）— 显示响应页面，提示用户输入有效的密码以获得站点的访问权限。配置 URL Admin Override（URL 管理员替代）设置（**Device**（设备）> **Setup**（设置）> **Content ID**（内容 **ID**））可管理密码和其他替代设置。（另请参见 Device（设备）> Setup（设置）> Content-ID 中的“管理设置”表）。 替代页面不会正常显示在配置为使用代理服务器的客户端机器上。 • **none**（无）（仅限自定义 URL 类别）— 如果已创建自定义 URL 类别，请将操作设置为 **none**（无）以允许防火墙继承 URL 数据库供应商提供的 URL 过滤类别分配。将操作设置为 **none**（无）可让您灵活地选择忽略 URL 过滤配置文件中的自定义类别，同时也能让您将自定义 URL 类别用作策略规则中的匹配条件（安全、解密和 QoS）以允许例外情况或执行不同的操作。如需删除自定义 URL 类别，您必须在使用自定义类别的配置文件中，将操作设置为 **none**（无）。有关自定义 URL 类别的信息，请参阅 Objects（对象）> Custom Objects（自定义对象）> URL Category（URL 类别）。
用户凭证提交	对于每个 URL 类别，选择 **User Credential Submissions**（用户凭证提交）以允许或禁止用户向该类别中的 URL 提交有效的公司凭证。在根据 URL 类别控制用户凭证提交之前，您必须启用凭证提交检测（选择 **User Credential Detection**（用户凭证检测）选项卡）。 设置为阻止的具有 **Site Access**（站点访问）的 URL 类别自动设置为也阻止用户凭证提交。 • **alert**（警报）— 允许用户向网站提交凭证，但是每次用户在该类别中向站点提交凭证时生成 URL 过滤日志。 • **allow**（允许）（默认）— 允许用户向网站提交凭证。 • **block**（阻止）— 阻止用户向网站提交凭证。默认的防网络钓鱼的响应页面阻止用户凭证提交。 • **continue**（继续）— 向用户显示响应页面，提示他们选择 **Continue**（继续）以向站点提交凭证。默认情况下，显示防网络钓鱼延续页面，以在用户尝试向不建议进行凭证提交的站点提交凭证时警告用户。您可选择创建自定义响应页面，警告用户防范网络钓鱼企图或提示他们不要在其他网站上再次使用有效的公司凭证。
检查 URL 类别	单击以访问 PAN-DB URL Filtering 数据库，从中可输入 URL 或 IP 地址查看分类信息。

© 2019 Palo Alto Networks, Inc.

类别设置	说明
动态 URL 过滤（默认禁用） （仅限配置 BrightCloud）	选择启用云查询以便对 URL 进行分类。只有当本地数据库无法对 URL 进行分类时才会调用此选项。 如果在 5 秒超时过后未解析 URL，响应显示为 `Not resolved URL`。 使用 *PAN-DB*，默认情况下此选项为启用状态，但不可配置。

URL 过滤设置

选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）> **URL Filtering Settings**（**URL** 筛选设置）可执行安全搜索设置并启用 HTTP 标头日志记录。

URL 过滤设置	说明
仅限日志容器页面 默认：已启用	选中此选项可以仅记录与所指定的内容类型匹配的 URL。在会话期间，防火墙不会记录相关的 Web 链接，例如通告和内容链接，这会在记录相关 URL 时减少日志记录和内存负载。 如果使用掩码源的原始 *IP* 地址的代理，则启用 HTTP 标头日志记录 *X-Forwarded-For*选项以保留发起 *Web* 页面请求的用户的原始 *IP* 地址。
启用安全搜索执行 默认：禁用 使用此功能不需要 URL 筛选许可证。	选中此选项可执行严格的安全搜索筛选。 很多搜索引擎都有安全搜索设置，用以筛选搜索查询返回流量中的成人图像和视频。当您选择设置为 Enable Safe Search Enforcement（启用安全搜索执行）时，如果最终用户未在搜索查询中使用最严格的安全搜索设置，则防火墙会阻止搜索结果。防火墙可以针对以下搜索提供商执行安全搜索：Google、Yahoo、Bing、Yandex 和 YouTube。这是一项尽力而为的设置，搜索提供商并不能保证适用于每个网站。 要使用安全搜索执行，您必须启用该设置，然后附加 URL 过滤配置文件安全策略规则。之后，防火墙会阻止所有未使用最严格安全搜索设置的匹配搜索查询返回流量。 如果在登录到 *Yahoo* 帐户的同时在 *Yahoo Japan (yahoo.co.jp)* 上执行搜索，必须启用搜索设置的锁定选项。 要防止用户通过使用其他搜索引擎提供商绕过此功能，可以配置 *URL* 过滤配置文件阻止搜索引擎类别，然后允许 *Bing*、*Google*、*Yahoo*、*Yandex* 和 *YouTube*。
HTTP 标头日志记录	启用 HTTP 标题日志记录可让您查看发送到服务器的 HTTP 请求中包含的属性。当启用一个或多个在 URL 过滤日志中记录的以下属性值对时： • 用户代理 — 用户用于访问 URL 的 Web 浏览器。此信息在 HTTP 请求中发送到服务器。例如，用户代理可以是 Internet Explorer 或 Firefox。日志中的用户代理值最多支持 1024 个字符。

© 2019 Palo Alto Networks, Inc.

URL 过滤设置	说明
	• 引用站点 — 用户链接到其他网页的网页的 URL；它是用户重定向（引用）到所请求的网页的源。日志中的引用站点值最多支持 256 个字符。 • X-Forwarded-For — 用于保留请求网页的用户的 IP 地址的标头字段选项。它可让您识别用户的 IP 地址，如果网络上拥有代理服务器或已实施源 NAT，则该属性值对非常有用，即屏蔽似乎来自代理服务器 IP 地址的所有请求的用户 IP 地址或公用 IP 地址。日志中的 x-forwarded-for 值最多支持 128 个字符。

用户凭据检测

选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）> **User Credential Detection**（用户凭据检测）可启用防火墙检测用户何时提交公司凭证。

配置用户凭据检测，这样，用户只能向指定 *URL* 类别中的站点提交凭据，从而通过阻止向不可信类别中的站点提交凭据减少攻击面。如果阻止 *URL* 过滤配置文件的所有 *URL* 类别进行用户凭据提交，则无需检查凭据。

防火墙使用三种方法之一来检测提交至网页的有效凭证。每种方法需要 User-ID™，这可让防火墙将网页的用户名和密码提交与有效的公司凭证比较。选择这些方法中的一种，然后根据 URL 类别继续防止凭证网络钓鱼。

您必须将防火墙配置为解密要监控的用户凭据的流量。

用户凭证检测设置	说明
IP 用户	该凭证检测方法检查用户名提交是否有效。您可使用该方法来检测包含有效公司用户名的凭证提交（无论附带的密码为何）。防火墙通过验证用户名匹配在会话的源 IP 地址中登录的用户，确定用户名匹配。要使用该方法，防火墙根据其 IP 地址到用户名的映射表匹配提交的用户名。要使用该方法，您可使用将 IP 地址映射到用户中描述的任何用户映射方法。
组映射	防火墙确定用户提交至受限站点的用户名是否匹配任何有效的公司用户名。为此，防火墙将提交的用户名和其用户到组的映射表中的用户名列表匹配，以在用户向受限类别中的站点提交公司用户名时检测到该情况。 该方法仅根据 LDAP 组成员身份检查公司用户名提交，让配置更简单，但是更容易发生误报。您必须启用组映射方可使用该方法。
域凭证	该凭证检测方法可让防火墙检查公司用户名和相关密码是否有效。防火墙确定用户提交的用户名和密码是否匹配同一用户的公司用户名和密码。 为此，防火墙必须能够将凭证提交与有效的公司用户名和密码匹配，并验证提交的用户名是否映射至登录用户的 IP 地址。仅对基于 Windows 的 User-ID 代理支持该模式，并要求 User-ID 代理安装在只读域控制器 (RODC) 上并配备 User-ID 凭证服务插件。若要使用该方法，您还必须让 User-ID 能够使用任何支持的用户映射方法（包括身份验证策略和身份验证门户以及 GlobalProtect™）将 IP 地址映射至用户。 有关防火墙可用于检查公司凭证提交是否有效的这些方法中每一种的详细信息，以及启用网络钓鱼防范的步骤，请参阅防止凭证网络钓鱼。

© 2019 Palo Alto Networks, Inc.

用户凭证检测设置	说明
检测到的有效用户名日志严重程度	设置日志的严重性，这些日志指示防火墙检测到对于网站的有效用户名提交。 该日志严重性和事件相关，在这些事件中有效的用户名提交至具有凭证权限以进行报警、阻止或继续的网站。在用户将有效的用户名提交至网站时进行记录的日志，对于该网站允许凭证提交的严重程度为“信息”。选择 **Categories**（类别）来查看或调整允许或阻止凭证提交的 URL 类别。 设置日志严重性为中等或更严重。

HTTP 标头插入

要通过将 HTTP 标头及其值插入 HTTP 请求来启用防火墙管理 Web 应用程序访问权限，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 筛选）> **HTTP Header Insertion**（**HTTP** 标头插入）。

防火墙仅支持 *HTTP/1.x* 流量的标头插入；防火墙不支持 *HTTP/2* 流量的标头插入。

您可以根据预定义的 HTTP 标头插入类型创建插入条目，也可以创建自己的自定义类型。标头插入通常针对自定义 HTTP 标头执行，但您也可以插入标准 HTTP 标头。

以下情况下会发生标头插入：

1. HTTP 请求将安全策略规则与一个或多个配置的 HTTP 标头插入条目匹配。
2. 指定的域与 HTTP 主机标头中找到的域匹配。
3. 操作指的是除阻止以外的任何操作。

防火墙只能对 *GET*、*POST*、*PUT* 和 *HEAD* 方法执行 *HTTP* 标头插入。

如果启用 HTTP 标头插入，并且请求中缺少标识的标头，则防火墙会插入标头。如果请求中已存在标识的标头，则防火墙将使用您指定的值覆盖标头值。

Add（添加）插入条目，或选择现有的插入条目进行修改。如有必要，您还可以选择插入条目并 **Delete**（删除）。

新的 *HTTP* 标头插入条目的默认阻止列表操作为 `Block`（阻止）。如果想要执行其他操作，请转至 URL 过滤类别，然后选择相应的操作。或者，将插入条目添加到使用指定操作配置的配置文件。

HTTP 标头插入设置	说明
姓名	该 HTTP 标头插入条目的 **Name**（名称）。
类型	要创建的条目 **Type**（类型）。条目可以预定义或自定义。防火墙将使用内容更新来填充和维护预定义条目。 要在 HTTP 标头中包含用户名，请选择 **Dynamic Fields**（动态字段）。
域	当此列表中的域与 HTTP 请求的主机标头相匹配时，会发生标头插入。

© 2019 Palo Alto Networks, Inc.

HTTP 标头插入设置	说明
	如果要创建预定义条目，则在内容更新中预定义域列表。这对大多数用例而言已足够，但您也可以根据需要添加或删除域。 要创建自定义条目，请至少将一个域 **Add**（添加）到此列表中。 每个域名最多可以包含 256 个字符，每个条目最多可以标识 50 个域。您可以将星号 (*) 用作通配符，即将任何请求匹配到指定域（例如 * .etrade.com）。
标头	如果创建了预定义条目，则通过内容更新预填充标头列表。这对大多数用例而言已足够，但您也可以根据需要添加或删除标头。 如果要创建自定义条目，请将一个或多个标头（最多五个）添加到此列表中。 标头名称最多可以包含 100 个字符，但不能包含空格。 要在 HTTP 标头中包含用户名，请选择 **X-Authenticated-User**，然后选择 **Value**（值）或 **Add**（添加）新标头。
值	最多使用 512 个字符配置 **Value**（值）。标头值因要包含在指定域的 HTTP 标头中的信息而异。例如，通过选择预定义类型或使用自定义条目来管理用户对 SaaS 应用程序的访问权限。 要在 HTTP 标头中包含用户名，请选择安全设备要求的域和用户名格式： • **`($domain)\($user)`** • **`WinNT://($domain)/($user)`** 或者，使用 **`($user)`** 和 **`($domain)`** 动态令牌（例如 **`($user)@($domain)`**）输入自定义格式。 防火墙使用组映射配置文件中的主用户名填充用户和域动态令牌。 每个值仅使用每个 ***`($user)`*** 和 ***`($domain)`*** 动态令牌一次。
日志	选择 **Log**（日志）可启用此标头插入条目的日志记录。

URL 过滤 Inline ML

选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **URL Filtering**（**URL** 过滤）> **Inline ML**，以使用基于防火墙的机器算法模式启用并配置网页的实时分析。

字段	说明
使用 **Inline ML** 选项卡以启用并配置策略操作。	
可用模型	对于每个可用的 ML 模型，您可以选择以下操作设置之一： • **Alert**（警报）— 允许网站且在 URL 过滤日志中生成日志条目。 • **Allow**（允许）— 允许网站且不生成任何日志条目。 • **Block**（阻止）— 阻止网站，用户将无法继续访问网站。同时会在 URL 筛选日志中生成日志条目。

© 2019 Palo Alto Networks, Inc.

字段	说明
异常	您可以为不需要分析的特定网站定义 URL **Exceptions**（例外），例如，可能触发误报的网站。 若要添加 URL 例外，必须先定义一个有效的 EDL（外部动态列表）或自定义 URL 类别。单击 **Add**（添加）以查看并从可用选项中进行选择。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> File Blocking（文件传送阻止）

您可以将文件阻止配置文件附加到安全策略规则（Policies（策略）> Security（安全））中，以便在用户试图上传或下载指定文件类型时，阻止用户上传或下载指定文件类型，或生成警报。

为了获得最佳安全性，请使用预定义 *strict*（严格）配置文件。如果需要支持使用 *strict*（严格）配置文件阻止的文件类型的关键应用程序，则克隆 *strict*（严格）配置文件，并仅使用您需要的文件类型例外。应用克隆配置文件到安全策略规则，该规则将例外限制为仅需要使用文件类型的源、目标和用户。此外，还可以使用 *Direction*（方向）限制上传或下载例外。

如果不阻止所有 *Windows PE* 文件，则发送所有未知文件到 *WildFire* 进行分析。对于用户账户，设置操作为 *continue*（继续），有助于阻止恶意 *Web* 网站、电子邮件或弹出窗口导致用户无意中下载恶意文件的偷渡式下载。告诉用户，他们无意识发起的文件传输的继续提示意味着可能会下载恶意文件。

下表介绍了文件阻止配置文件设置。

文件传送阻止配置文件设置	说明
姓名	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在文件传送阻止配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的文件阻止配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
规则	定义一个或多个规则，用于指定为所选文件类型采取的操作（如果存在）。要添加规则，请指定以下内容，并单击添加： • **Name**（名称）— 输入规则名称（最多 31 个字符）。 • 应用程序— 选择要应用规则的应用程序，或选择任何。 • **File Types**（文件类型）— 单击文件类型字段，然后单击 **Add**（添加）以查看支持的文件类型的列表。单击文件类型可将其添加到配置文件，并在必要时，继续添加其他文件类型。如果选择 **Any**（任何），则对所有支持的文件类型执行定义的操作。 • 方向— 选择文件传输方向（上载、下载或两者）。 • 操作— 选择检测到所选文件类型时所执行的操作： • 警报— 向威胁日志添加条目。

© 2019 Palo Alto Networks, Inc.

文件传送阻止配置文件设置	说明
	• 继续— 向用户给出一条消息，指示已请求下载，并要求用户确认是否继续。目的是警告用户可能的未知下载（也称为“下载驱动”），并让用户选择继续或停止下载。 创建具有操作 **continue**（继续）的文件传送阻止配置文件时，只能选择应用程序 **web-browsing**（**Web** 浏览）。如果选择任何其他应用程序，由于系统不会向用户显示继续页面加以提示，因此与安全策略规则匹配的流量不会通过防火墙。 • 阻止— 阻止文件。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> WildFire Analysis（WildFire 分析）

使用 WildFire 分析配置文件可以指定要在 WildFire 设备本地或在 WildFire 云中执行的 WildFire 文件分析。您可以根据文件类型、应用程序或文件传输方向（上传或下载），指定要转发到公共云或私有云的流量。在创建 WildFire 分析配置文件后，进一步将此配置文件添加到策略（**Policies**（策略）> **Security**（安全）），可将此配置文件设置应用到与该策略匹配的所有通信（例如，在策略中定义的 URL 类别）。

使用预定义默认配置文件转发所有未知文件到 WildFire 进行分析。此外，设置 WildFire 设备内容更新为每分钟下载和安装，这样，您始终拥有最新支持。

WildFire 分析配置文件设置	
姓名	输入 WildFire 分析配置文件的描述性名称（最多 31 个字符）。定义安全策略规则时，此名称将出现在可供您选择的 WildFire 分析配置文件列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	（可选）介绍配置文件规则或配置文件的预期用途（最多 255 个字符）。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的漏洞防护配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。

规则	定义一个或多个规则，以便指定要转发到 WildFire 公共云或 WildFire 设备（私有云）进行分析的流量。
	• 输入添加到配置文件的所有规则的描述性名称（最多 31 个字符）。
	• 添加应用程序，以便所有应用程序流量都与规则匹配，并转发到指定分析目标。
	• 为规则选择在定义分析目标分析的文件类型。
	WildFire 私有云（由 WildFire 设备托管）不支持对 APK、Mac OS X、archive 和 Linux 文件进行分析。
	• 根据传输方向将规则应用到流量。可以将规则应用到上传流量、下载流量或这两者。
	• 选择要转发以进行 **Analysis**（分析）的流量目标：
	  • 选择公共云，以使与规则匹配的所有流量转发到 WildFire 公共云进行分析。
	  • 选择私有云，以使与规则匹配的所有流量转发到 WildFire 设备进行分析。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> Data Filtering（数据过滤）

数据过滤可让防火墙检测敏感信息（如信用卡号、社会保险号、公司内部文档），并防止这类数据脱离安全网络。在启用数据过滤之前，需选择 Objects（对象）> Custom Objects（自定义对象）> Data Patterns（数据模式），以定义要过滤的数据的类型（如社会保险号或包含“机密”字样的文档标题）。您可以在单个数据过滤配置文件中添加多个数据模式对象，在将此配置文件附加到安全策略规则中后，防火墙可在允许的流量中扫描每个数据模式，并根据数据过滤配置文件设置阻止匹配的流量。

数据过滤配置文件设置	说明
姓名	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在日志转发配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的数据过滤配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
数据捕获	选中此选项可自动收集被过滤器阻止的数据。 在设置页面上为 *Manage Data Protection* 指定密码，以查看捕获的数据。请参阅 Device（设备）> Setup（设置）> Management（管理）。
数据模式	添加现有数据模式用于过滤，或选择 **New**（新建）配置新的数据模式对象（Objects（对象）> Custom Objects（自定义对象）> Data Patterns（数据模式））。
应用程序	指定要包含在过滤规则中的应用程序： • 选择任何可以将过滤器应用到所有列出的应用程序。此选择不会阻止所有可能的应用程序，只阻止列出的应用程序。 • 单击添加以指定个别应用程序。
文件类型	指定要包括在过滤规则中的文件类型： • 选择任何可以将过滤器应用到所有列出的文件类型。此选择不阻止所有可能的文件类型，只阻止列出的文件类型。 • 单击添加以指定个别文件类型。

© 2019 Palo Alto Networks, Inc.

数据过滤配置文件设置	说明
direction	指定是要在上载方向、下载方向还是两个方向上同时应用过滤器。
警报阈值	指定触发警报之前，必须在文件中检测到数据模式的次数。
阻止阈值	阻止的文件中至少包含数据模式的多个实例。
日志严重性	针对与数据过滤配置文件规则匹配的事件，定义记录的日志严重性。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> DoS Protection（DoS 保护）

DoS 保护配置文件可用于高度精确定位和增强区保护配置文件。DoS 保护配置文件可指定每秒新连接数 (CPS) 触发警报和操作的阈值速率（DoS 保护策略中已指定）。DoS 保护配置文件还可指定每秒最高连接速率以及阻止的 IP 地址保留在阻止 IP 列表中的时间。您可以在 DoS 保护策略规则中指定 DoS 保护配置文件，其中，您可以指定数据包与规则匹配的条件。策略规则可以确定应用配置文件的设备。

创建 *DoS* 保护配置文件和策略以保护关键个人设备或小的设备组，尤其是诸如 *Web* 服务器和数据库服务器等面向互联网的设备。

您可以配置聚合和分类 DoS 保护配置文件。您可以将聚合配置文件、分类配置文件或其中任何一种类型应用至 DoS 保护策略规则。如果规则使用两种类型的配置文件，则防火墙将首先应用聚合配置文件，然后根据需要应用分类配置文件。

- 分类 DoS 保护配置文件是 **Type**（类型）选择为 **Classified**（已分类）的配置文件。当将分类 DoS 保护配置文件应用至其操作为 **Protect**（保护）的 DoS 保护规则时，如果数据包满足指定的地址类型： source-ip-only、destination-ip-only 或 src-dest-ip-both，则防火墙会将连接数计入配置文件的 CPS 阈值。
- 聚合 DoS 保护配置文件是 **Type**（类型）选择为 **Aggregate**（聚合）的配置文件。当将聚合 DoS 保护配置文件应用至其操作为 **Protect**（保护）的 DoS 保护规则时，防火墙会将计算规则中所有满足配置文件 CPS 阈值的连接数（在规则中指定设备组的组合连接数）。

要将 DoS 保护配置文件应用于 DoS 保护策略，请参阅 Policies（策略）> DoS Protection（DoS 保护）。

如果您拥有多个虚拟系统（多 *vsys*）环境，则必须配置以下内容：

- 外部区域，用于在虚拟系统之间进行通信
- 共享网关，允许虚拟系统共享用于外部通信的通用接口和单个 *IP* 地址

在外部区域中禁用下列区域和 *DoS* 保护机制：

- *SYN Cookies*
- *IP* 分片
- *ICMPv6*

要启用 *IP* 分片和 *ICMPv6* 保护，请为共享网关创建单独的区保护配置文件。

要在共享网关上防御 *SYN* 泛滥攻击，可以通过随机早期丢弃或 *SYN cookie* 来应用 *SYN* 泛滥攻击保护配置文件。在外部区域中，只有随机早期丢弃适用于 *SYN* 泛滥攻击保护。

DoS 保护配置文件设置	
姓名	输入配置文件名称（最多31个字符）。定义安全策略时，此名称将出现在日志转发配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	输入配置文件的说明（最多 255 个字符）。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。

© 2019 Palo Alto Networks, Inc.

DoS 保护配置文件设置	
	• Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的 DoS 保护配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
类型	选择以下配置文件类型之一： • **Aggregate**（聚合）— 将配置文件中所配置的 DoS 阈值应用于与应用此配置文件的规则标准匹配的所有连接。例如，SYN 泛滥攻击 **Alarm Rate**（警报速率）阈值为 10000 CPS 的聚合规则会计算与 DoS 规则匹配的所有设备的组合连接数。当组的总 CPS 超过可触发警报的 10000 CPS 时，无论 CPS 如何，都会在设备上传播。 • **classified**（已分类）— 将配置文件中配置的 DoS 阈值应用于符合分类标准（源 IP 地址、目标 IP 地址或源及目标 IP 地址对）的每个单独连接。例如，SYN 泛滥攻击 **Alarm Rate**（警报速率）阈值为 10000 CPS 的分类规则允许每个设备最多为 10000 CPS，并在 DoS 规则中指定的任何单个设备超过 10000 CPS 时触发警报。
Flood Protection 选项卡	

SYN 泛滥攻击选项卡
UDP 泛滥攻击选项卡
ICMP 泛滥攻击选项卡
ICMPv6 泛滥攻击选项卡
其他 IP 泛滥攻击选项卡
	选中此选项可启用选项卡上指明的泛滥攻击保护类型，并指定以下设置：
	• **Action**（操作）—（仅限 **SYN Flood**（**SYN** 泛滥攻击））在 DoS 保护策略操作是 **Protect**（保护），且传入 CPS 达到 **Activate Rate**（激活速率）时，防火墙所执行的操作。选择以下选项之一：
	  • **Random Early Drop**（随机早期丢弃）— 在每秒连接数达到 **Activate Rate**（激活速率）阈值时随机丢弃数据包。
	  • **SYN cookie** — 使用 SYN cookie 生成确认消息，以便在出现 SYN 泛滥攻击时不必丢弃连接。
	  从可以公平处理合法流量，但会消耗更多防火墙资源的 *SYN* 泛滥攻击开始。监控 *CPU* 和内存利用率，并在 *SYN Cookies* 消耗资源过多时切换到 *RED*。如果在网络（互联网）周边没有用于保护大量 *DoS* 攻击的专用 *DDoS* 防护设备，则始终使用 *RED*。
	• **Alarm Rate**（警报速率）— 指定生成 DoS 警报的阈值速率 (CPS)（范围为 0 - 2,000,000 cps；默认为 10,000 cps）。
	  对于分类配置文件，最佳做法是将阈值设置为高于设备平均 CPS 速率 15-20%，以适应正常波动，并在收到过多警报时调整阈值。对于聚合配置文件，最佳做法是将阈值设置为高于组平均 CPS 速率的 15-20%。监控该阈值，并根据需要进行调整。
	• **Activate Rate**（激活速率）— 指定激活 DoS 响应的阈值速率 (cps)。DoS 响应在 DoS 保护配置文件的 **Action**（操作）字段中进行配置（随机早期丢弃或 SYN cookie）。**Activate Rate**（激活速率）范围为 0 - 2,000,000 cps；默认为 10,000 cps。
	  如果配置文件的 **Action**（操作）是 **Random Early Drop**（随机早期丢弃）(RED)，则在每秒传入连接数达到 **Activate Rate**（激活速率）阈值时，会执行随机早期丢弃这一操作。如果 CPS 速率提高，则 RED 速率会根据算

© 2019 Palo Alto Networks, Inc.

DoS 保护配置文件设置	
	法提高。防火墙会继续执行 RED 操作，直至 CPS 速率达到 **Max Rate**（最大速率）阈值。 分类配置文件对单个设备应用精确的 CPS 限制，且将这些限制基于受保护神的容量，所以，您无需逐渐调节 CPS，可以将 **Activate Rate**（激活速率）设置为与 **Max Rate**（最大速率）相同的阈值。仅当您希望在达到**Max Rate**（最大速率）之前开始将流量丢弃到单个服务器时，将**Activate Rate**（激活速率） 设置为低于**Max Rate**（最大速率）的值。对于聚合配置文件，将阈值设置为刚好高于组 CPS 速率峰值的值。监控该阈值，并根据需要进行调整。 • **Max Rate**（最大速率）— 指定防火墙允许的每秒传入连接的阈值速率。达到 **Max Rate**（最大速率）阈值时，防火墙会丢弃全部新连接（范围为 2 - 2,000,000 cps；默认为 40,000 cps）。 对于分类配置文件，将 **Max Rate**（最大速率）基于您正在保护的设备容量，这样，设备就不会遭受泛滥攻击。对于聚合配置文件，设置 **Max Rate**（最大速率）为组容量的 80-90%。监控该阈值，并根据需要进行调整。 • **Block Duration**（阻止期限）— 指定攻击性 IP 地址保留在阻止 IP 列表中以及阻止此 IP 地址的连接的时长（以秒为单位）。防火墙不会将阻止期限内到达的数据包数计入警报速率、激活速率或最大速率阈值（范围为 1 - 21,600 秒；默认为 300 秒）。
资源保护选项卡	
会话	选中此选项可启用资源保护。
最大并发会话数	指定最大并发会话数。 • 对于 **Aggregate**（聚合）配置文件类型，此限制将应用于符合应用 DoS 保护配置文件的 DoS 保护规则的所有流量。 • 对于 **Classified**（已分类）配置文件类型，此限制将基于分类（源 IP、目标 IP 或源及目标 IP)应用于符合应用 DoS 保护配置文件的 DoS 保护规则的流量。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> Mobile Network Protection（移动网络保护）

移动网络保护配置文件可使防火墙检测 5G 服务化架构 (SBA) 流量中的 GTP 和 HTTP/2。要查看此配置文件，必须在 Device（设备）> Setup（设置）> Management（管理）中启用 GTP 安全。

使用配置文件中的选项来启用 5G HTTP/2、GTP v1-C、GTP v2-C 和 GTP-U 的状态检测，启用 GTPv1-C、GTP v2-C 和 GTP-U 的协议验证，启用 GTP-U 内容检查，以扫描 GTP-U 隧道内的用户数据。它还使您能根据 APN、IMSI/IMSI-Prefix 和 RAT 筛选 GTP 会话，并防止最终用户 IP 地址欺骗。

GTP 检测配置文件设置	
GTP 检测	

GTP-C	• 选中 **Stateful Inspection**（状态检测），可让防火墙检测 **GTPv1-C** 或 **GTPv2-C**，或者这二者。启用状态检测后，防火墙会使用源 IP、源端口、目标 IP、目标端口、协议和隧道端点 ID (TEID) 跟踪 GTP 会话。还会检查和验证建立 GTP 隧道使用的不同类型 GTP 消息的顺序。TEID 是 GSN 隧道端点的唯一标识。上行链路和下行链路的隧道各自独立，使用不同的 TEID。
	• 选择有效性检查失败后防火墙执行的操作（**Block**（阻止）或 **Alert**（警报））。执行警报操作，将允许流量，但会生成日志；执行阻止操作，将拒绝流量，并会生成日志。
	• 指定防火墙必须对负载中的 GTP 标头和信息元素 (IE) 执行的有效性检查。防火墙会使用您在下面选择的阻止或警报操作来处理错误。您可以配置防火墙，以验证以下内容：
	  • **Reserved IE**（保留 **IE**）— 检查 GTPv1-C 或 GTPv2-C 消息是否使用保留 IE 值。
	  • **Order of IE**（**IE** 顺序）（仅限 GTPv1-C）— 检查 GTPv1-C 消息中的 IE 顺序是否准确。
	  • **Length of IE**（**IE** 长度）— 检查 GTPv1-C 或 GTPv2-C 消息是否包含无效的 IE 长度。
	  • **Reserved field in header**（标头中的保留字段）— 检查格式错误的数据包的标头中是否使用无效值或保留值。
	  • **Unsupported message type**（不支持的消息类型）— 检查未知或不正确的消息类型。

GTP-U	启用 GTPv1-C 和/或 GTPv2-C 的状态检测后，将自动启用 GTPU-U 的状态检测。 可以为 GTP-U 负载指定以下有效性检查。 • **Reserved IE**（保留 **IE**）— 在负载中检查 GTP-U 消息是否使用保留 IE 值。 • **Order of IE**（**IE** 顺序）— 检查 GTP-U 消息中的 IE 顺序是否正确。 • **Length of IE**（**IE** 长度）— 检查消息是否包含无效的 IE 长度。 • **Reserved field in header**（标头中的保留字段）— 检查格式错误的数据包的标头中是否使用无效值或保留值。 • **Unsupported message type**（不支持的消息类型）— 检查未知或不正确的消息类型。

© 2019 Palo Alto Networks, Inc.

GTP 检测配置文件设置	
	此外，还可以在以下情况下配置允许、阻止或警报操作： • **End User IP Address Spoofing**（最终用户 **IP** 地址欺诈）— 配置防火墙，在订户用户设备中 GTP-U 数据包的源 IP 地址与隧道设置时交换的相应 GTP-C 消息中的 IP 地址不同时，执行阻止或警报操作。 • **GTP-in-GTP**（**GTP** 中的 **GTP**）— 配置防火墙，在检测到 GTP 中的 GTP 消息时，执行阻止或警报操作。检测后，防火墙会生成严重级严重性的 GTP 日志。 • 对于 4G 和 3G，如果想要检查策略，并将其应用于 GTP-U 数据包的用户数据负载，则启用 **GTP-U Content Inspection**（**GTP-U** 内容检查）。检查 GTP-U 内容，可将 GTP-C 消息中的 IMSI 和 IMEI 信息与 GTP-U 数据包中封装的 IP 流量关联。
5G-C	对于 5G，启用**5G-HTTP2**以启用可能包括订户 ID、设备 ID 和网络切片信息的 5G HTTP/2 控制数据包的检测。这样，您可以将从 HTTP/2 消息中获得订户 ID (IMSI)、设备 ID (IMEI)和网络切片 ID 消息与封装在 GTP-U 数据包内的 IP 流量关联。 启用 **5G-HTTP2** 可禁用配置文件的 GTP-C。
过滤选项	
RAT 过滤	默认情况下，允许所有无线接入技术 (RAT)。对于 GTP-C 创建 PDP 请求和创建会话请求消息，将根据 RAT 过滤器进行过滤或允许。对于用户设备访问移动核心网络所使用的以下 RAT，您可以指定允许、阻止或警报操作： • **UTRAN** • **GERAN** • **WLAN** • **GAN** • **HSPA** 发展 • **EUTRAN** • 虚拟 • **EUTRAN-NB-IoT** • **LTE-M** • **NR** 启用 **5G-HTTP2**后，下列 RAT 可用： • **WLAN** • **EUTRAN** • 虚拟 • **NR**
IMSI 过滤	IMSI（国际移动订户标识）是与订户标识模块 (SIM) 卡中设置的 GSM、UMTS 和 LTE 网络订户关联的唯一标识。 IMSI 通常显示为 15 位数字（8 字节），但其长度可以缩减。IMSI 由三部分组成： • 移动国家/地区代码 (MCC)，由三位数组成。MCC 是移动订户所在国家/地区的唯一标识。 • 移动网络代码 (MNC)由两位或三位数组成；2 位数是欧洲标准，3 位数是北美标准。MNC 用于标识移动订户的归属 PLMN。

© 2019 Palo Alto Networks, Inc.

GTP 检测配置文件设置	
	• 移动订户标识号 (MSIN)，用于标识 PLMN 内的移动订户。 **IMSI Prefix**（**IMSI** 前缀）合并了 MCC 和 MNC，可让您对特定 PLMN 中的 GTP 流量执行 **allow**（允许）、**block**（阻止）或 **alert**（警报）操作。默认情况下，允许所有 IMSI。 可以在防火墙中手动输入或导入有 IMSI 或 IMSI 前缀的 CSV 文件。IMSI 可以包含通配符，例如 310* 或 240011*。 防火墙最多支持 5000 个 IMSI 或 IMSI 前缀。
APN 过滤	接入点名称 (APN) 是指用户设备连接到 Internet 所需的 GGSN/ PGW。在 5G 中，有一种数据网络名称 (DNN) 格式是 APN。APN 由一个或两个标识符组成： • APN 网络标识符，用于定义 GGSN/PGW 连接到的外部网络，也可以定义移动工作站请求的服务。这部分 APN 是必需项。 • APN 运营商标识符，用于定义 GGSN/PGW 所归属的 PLMN GPRS/EPS 骨干网。这部分 APN 是可选项。 默认情况下，允许所有 APN。APN 过滤器可让您根据 APN 值对 GTP 流量执行允许、阻止或警报操作。对于 GTP-C 创建 PDP 请求和创建会话请求消息，将根据 APN 过滤所定义的规则进行过滤或允许。 可以在防火墙中手动添加或导入 APN 过滤列表。APN 值必须包括网络 ID 或网络域名（例如 example.com），也可以包括运营商 ID。 对于 APN 筛选，通配符 '*' 允许您匹配所有 APN。通配符不支持 '*' 和其他字符的组合。例如，“internet.mnc*”被视为常规 APN，不会筛选以 internet.mnc 为开头的所有条目。 防火墙最多支持 1000 个 APN 过滤器。
GTP 隧道限制	
每个目标允许的最大并发隧道数	用于限制目标 IP 地址（例如 GGSN）的最大 GTP-U 隧道数（范围为 0-100,000,000 个隧道）。
每个目标最大并发隧道数警报	指定防火墙确定达到目标的最大 GTP-U 隧道数后触发警报的阈值。在达到配置的隧道限制时，将生成高严重性 GTP 日志消息。
日志记录频率	在超过配置的 GTP 隧道限制时防火墙在生成日志之前计入的事件数量。此设置可让您减少记录消息的数量（范围为 0-100,000,000；默认为 100）。
超额计费保护	在防火墙上选择用作 Gi/ Sgi 防火墙的虚拟系统。Gi/ Sgi 防火墙可检测通过 Gi/ Sgi 接口从 PGW/ GGSN 传输到 Internet 等外部 PDN（数据包数据网络）的移动订户 IP 流量，并保护移动订户的 Internet 访问。 当 GGSN 为移动订户分配最终用户 IP 地址库中之前使用的 IP 地址时，会发生超额计费。由于之前的订户发起的会话没有关闭，此会话在 Gi 防火墙上仍处于打开状态，Internet 中的恶意服务器会继续向此 IP 地址发送数据包。为阻止发送数据，在 GTP 隧道被删除（根据删除 PDP 或删除会话消息检测到）或连接超时的情况下，为超额计费保护启用的防火墙会通知 Gi/ Sgi 防火墙删除属于会话表中订户的所有会话。GTP 安全和 SGi/ Gi 防火墙应该在同一物理防火墙上进行配置，但可归属于不同的虚拟系统。要根据 GTP-C 事件删除会话，防火墙需要了解所有相关会话信息，只有在移动核心网络中管理来自 SGi + S11 或 S5 接口

© 2019 Palo Alto Networks, Inc.

GTP 检测配置文件设置	
	（对于 GTPv2）和 Gi + Gn 接口（对于 GTPv1）的流量，防火墙才能获悉这类信息。
其他日志设置 默认情况下，防火墙不记录允许的 GTP 消息。如果需要，您可以选择启用在故障排除时记录允许的 GTP 消息这一功能，这样会生成大量日志。除允许的日志消息以外，此选项卡还可让您选择启用记录用户位置信息。	
GTPv1-C 允许的消息	如果已启用 GTPv1?C 的状态检测，此设置可让您选择启用记录允许的 GTPv1-C 消息。这些消息会生成日志，必要时可帮助您排除故障。 默认情况下，防火墙不记录允许的消息。允许的 GTPv1-C 消息的日志记录选项如下： • **Tunnel Management**（隧道管理）— 这些 GTPv1-C 消息用于管理 GTP-U 隧道，此隧道可承载封装的 IP 数据包以及 SGSN 和 GGSN 等网络节点对之间的信号传送消息。其中包括创建 PDP 上下文请求、创建 PDP 上下文响应、更新 PDP 上下文请求、更新 PDP 上下文响应、删除 PDP 上下文请求、删除 PDP 上下文响应等消息。 • **Path Management**（路径管理）— 这些 GTPv1-C 消息通常是由 GSN 或无线网络控制器 (RNC) 发送到其他 GSN 或 RNC 的消息，旨在了解对等设备是否处于活动状态。其中包括回显请求和回显响应等消息。 • **Others**（其他）— 这些消息包括位置管理、移动管理、RAN 信息管理和多媒体广播多播服务 (MBMS) 消息。
日志用户位置	使您在 GTP 日志中加入用户位置信息，如区域代码和单元 ID。
数据包捕获	使您捕获 GTP 事件。
GTPv2-C 允许的消息	如果已启用 GTPv2-C 的状态检测，此设置可让您选择启用记录允许的 GTPv2-C 消息。这些消息会生成日志，必要时可帮助您排除故障。 默认情况下，防火墙不记录允许的消息。允许的 GTPv2-C 消息的日志记录选项如下： • **Tunnel Management**（隧道管理）— 这些 GTPv2-C 消息用于管理 GTP-U 隧道，此隧道可承载封装的 IP 数据包以及 SGW 和 PGW 等网络节点对之间的信号传送消息。其中包括以下类型的消息：创建会话请求、创建会话响应、创建载体请求、创建载体响应、修改载体请求、修改载体响应、删除会话请求、和删除会话响应。 • **Path Management**（路径管理）— 这些 GTPv2-C 消息通常是由 SGW 或 PGW 等网络节点发送到其他 PGW、SGW 的消息，旨在了解对端设备是否处于活动状态。其中包括回显请求和回显响应等消息。 • **Others**（其他）— 这些消息包括移动管理和非 3GPP 访问相关消息。
GTP-U 允许的消息	如果已启用 GTPv2-C 或 GTPv1-C 的状态检测，此设置可让您选择启用记录允许的 GTP-U 消息。这些消息会生成日志，必要时可帮助您排除故障。 允许的 GTP-U 消息的日志记录选项如下： • **Tunnel Management**（隧道管理）— 这些消息是 GTP-U 信号传送消息，如错误指示。 • **Path Management**（路径管理）— 这些 GTP-U 消息是由一个网络节点（如 eNodeB）发送到另一个网络节点（如 SGW）的消息，旨在了解对端设备是否处于活动状态。其中包括回显请求/响应等消息。

© 2019 Palo Alto Networks, Inc.

GTP 检测配置文件设置	
	• **G-PDU** — G-PDU (GTP-U PDU) 用于承载移动核心网络的网络节点内的用户数据包；其中包含一个 GTP 标头和一个 T-PDU。
每个新 GTP-U 隧道记录的 G-PDU 数据包	启用此选项后，可验证防火墙是否在检测 GTP-U PDU。防火墙会为每个新 GTP-U 隧道中指定数量的 G-PDU 数据包生成日志（范围为 1-10；默认为 1）。
5G 允许的消息	选择 **N11** 可选择性地启用允许 N11 消息的日志记录功能。N11 消息有助于您进行故障排除，深入了解在不同程序中 N11 接口上交换的 HTTP/2 消息。仅当您启用移动网络保护配置文件中 **5G-C** 选项卡的 **5G-HTTP2**后，该字段才可用。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profiles（安全配置文件）> SCTP Protection（SCTP 保护）

创建流控制传输协议 (SCTP) 保护配置文件，以指定您希望防火墙验证和筛选 SCTP 块的方式。您必须先启用 SCTP 安全（**Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（常规设置））才能在安全配置文件下查看此配置文件类型。您还可以限制多宿主环境中每个 SCTP 端点的 IP 地址数，并且可以指定防火墙何时记录 SCTP 事件。创建 SCTP 保护配置文件后，您需要将该配置文件应用于区域的安全策略规则。

支持 SCTP 安全的防火墙型号具有预定义 SCTP 保护配置文件 (*default-ss7*)，您可以按原样使用它，也可以克隆 default-ss7 配置文件作为新的 SCTP 保护配置文件的基础。选择 **Object**（对象）> **Security Profiles**（安全配置文件）> **SCTP Protection**（**SCTP** 保护）并选择 **default-ss7** 以查看导致此预定义配置文件警报的操作代码。

SCTP 保护配置文件设置	
姓名	输入 SCTP 保护配置文件的名称。
说明	输入 SCTP 保护配置文件的说明。
SCTP 检测	
未知块	选择防火墙接收包含未知块的 SCTP 数据包时的操作（RFC3758、RFC4820、RFC4895、RFC4960、RFC5061 或 RFC 6525 中未对块进行定义）： • **allow**（允许）（默认）— 允许数据包通过而无需修改。 • **alert**（警报）— 允许数据包通过而无需修改并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。 • **block**（阻止）— 在传递数据包之前取消块并生成 SCTP 日志。
块标志	选择防火墙接收包含与 RFC4960 不符的块标志的 SCTP 数据包时的操作： • **allow**（允许）（默认）— 允许数据包通过而无需修改。 • **alert**（警报）— 允许数据包通过而无需修改并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。 • **block**（阻止）— 丢弃数据包并生成 SCTP 日志。
无效长度	选择防火墙接收长度无效的 SCTP 块时的操作： • **allow**（允许）（默认）— 允许数据包或块通过而无需修改。 • **block**（阻止）— 丢弃数据包并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志存储选项卡。
多宿主的 IP 地址限制	输入您可以在防火墙生成警报消息之前为 SCTP 端点配置的最大 IP 地址数（范围为 1 至 8，默认为 4）。

© 2019 Palo Alto Networks, Inc.

SCTP 保护配置文件设置	
	SCTP 多宿主是指端点支持多个 IP 地址以与对端进行关联的能力。如果通往端点的一条路径出现故障，则 SCTP 将选择为该关联提供的其他目标 IP 地址之一。
日志设置	选择任意设置组合以生成允许的块、关联开始和结束以及状态失效事件的 SCTP 日志： • 在关联开始时记录 • 在关联结束时记录 • 记录允许的关联初始化块 • 记录允许的检测信号块 • 记录允许的关联终止块 • 记录所有控制块 • 记录状态失效事件 要让防火墙存储 SCTP 日志，您需要分配 SCTP 日志存储（请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。
过滤选项	
SCTP 筛选	
姓名	输入 SCTP 筛选程序的名称。
PPID	指定 SCTP 筛选程序的 PPID。 • **any**（任何）— 使防火墙对包含 PPID 的所有 SCTP 数据块执行您指定的操作。 • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA** • **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • 输入有效的 PPID 值（下拉列表中未显示的值）。例如，H.323 的 PPID 值是 13。 每个 SCTP 筛选程序只能指定一个 PPID，但您可以为 SCTP 保护配置文件指定多个 SCTP 筛选程序。
操作	指定防火墙对包含指定 PPID 的数据块执行的操作： • **allow**（允许）（默认）— 允许块通过而无需修改。 • **alert**（警报）— 允许块通过而无需修改并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志

© 2019 Palo Alto Networks, Inc.

SCTP 保护配置文件设置	
	存储选项卡：Device（设备）> Setup（设置）> Management（管理））。 • **block**（阻止）— 在传递数据包之前取消块并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。
SCTP 数据包与列表中的筛选程序自上而下匹配。如果为配置文件创建多个 SCTP 筛选程序，则 SCTP 筛选程序的顺序会有所不同。选择筛选程序进行 **Move Up**（上移）或 **Move Down**（下移），以更改其在 SCTP 筛选列表中的相对优先级。	
Diameter 筛选	
姓名	输入 Diameter 筛选程序的名称。
操作	指定防火墙对包含指定 Diameter 应用程序 ID、命令代码和 AVP 的 Diameter 块执行的操作。如果检查的块包含指定 Diameter 应用程序 ID 和任何指定 Diameter 命令代码以及任何指定 Diameter AVP，则： • **allow**（允许）（默认）— 允许块通过而无需修改。 • **alert**（警报）— 允许块通过而无需修改并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。 • **block**（阻止）— 在传递数据包之前取消块并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。
Diameter 应用程序 ID	指定防火墙对其执行指定操作的块的 Diameter 应用程序 ID。 • 任何 • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • **Diameter** 基础会计 • **Diameter** 通用消息 • **Diameter** 信用控制 或者，您可以输入 Diameter 应用程序 ID 的数值（范围为 0-4,294,967,295）。Diameter 筛选程序只能有一个应用程序 ID。
Diameter 命令代码	指定防火墙对其执行指定操作的块的 Diameter 命令代码。选择 **any**（任何），从下拉列表中选择其中一个 Diameter 命令代码，或输入一个特定值（范围为 0-16,777,215）。下拉列表中仅包含适用于所选 Diameter 应用程序 ID 的命令代码。您可以在 Diameter 筛选程序中添加多个 Diameter 命令代码。

© 2019 Palo Alto Networks, Inc.

SCTP 保护配置文件设置	
Diameter AVP	指定防火墙对其执行指定操作的块的 Diameter 属性值对 (AVP) 代码。输入一个或多个 AVP 代码或值（范围为 1-16,777,215）。
如果为配置文件创建多个 Diameter 筛选程序，则 Diameter 筛选程序的顺序会有所不同。选择筛选程序进行 **Move Up**（上移）或 **Move Down**（下移），以调整其在 Diameter 筛选列表中的相对优先级。	
SS7 筛选	
姓名	输入 SS7 筛选程序的名称。
操作	指定防火墙对包含指定 SS7 筛选程序要素的 SS7 块执行的操作。如果正在检查的块包含 SCCP 主叫方 SSN 和任何指定 SCCP 主叫方全局标题 (GT) 值以及任何指定操作代码，则： • **allow**（允许）（默认）— 允许块通过而无需修改。 • **alert**（警报）— 允许块通过而无需修改并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。 • **block**（阻止）— 在传递数据包之前取消块并生成 SCTP 日志（您需要为这些日志分配日志存储 — 请参阅日志记录和报告设置项下的日志存储选项卡：Device（设备）> Setup（设置）> Management（管理））。
SCCP 主叫方 SSN	指定防火墙对其执行指定操作的块的 SCCP 主叫方 SSN。从下拉列表中选择 **any-map** 或 **Add**（添加）其中一个 SCCP 主叫方 SSN： • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** • **CAP** • **INAP** • **SCCP 管理** SS7 筛选程序只能有一个 SCCP 主叫方 SSN。
SCCP 主叫方 GT	指定防火墙对其执行指定操作的块的 SCCP 主叫方 GT 值。选择 **Any**（任何）或 **Add**（添加）最多包含 15 位数字的数值。您还可以输入一组使用前缀的 SCCP 主叫方 GT 值。例如：876534*。您可以在 SS7 筛选程序中添加多个 SCCP 主叫方 GT 值。 对于 SCCP 主叫方 SSN：**INAP** 和 **SCCP Management**（**SCCP 管理**），此选项被禁用。
操作代码	指定防火墙对其执行指定操作的块的操作代码。

© 2019 Palo Alto Networks, Inc.

SCTP 保护配置文件设置	
	对于以下 SCCP 主叫方 SSN，请从下拉列表中选择 **any**（任何）或一个操作代码，或输入一个特定值（范围为 1-255）： • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** 对于 SCCP 主叫方 SSN：**CAP**，输入一个值（范围为 1-255）。 对于 SCCP 主叫方 SSN：**INAP** 和 **SCCP Management**（**SCCP** 管理），此选项被禁用。 您可以在 SS7 筛选程序中添加多个操作代码。
如果为配置文件创建多个 SS7 筛选程序，则 SS7 筛选程序的顺序会有所不同。选择筛选程序进行 **Move Up**（上移）或 **Move Down**（下移），以调整其在 SS7 筛选列表中的相对优先级。	

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Security Profile Groups（安全配置文件组）

防火墙支持创建安全配置文件组的功能，用户可利用此功能，指定被视为一个单元的安全配置文件集合，然后将其添加到安全策略中。例如，可以创建一个威胁安全配置文件组，其中包括防病毒、防间谍软件和漏洞防护的配置文件，然后再创建一个包括威胁配置文件的安全策略规则。

对于那些通常一起分配的防病毒、防间谍软件、漏洞保护、URL 过滤以及文件传送阻止配置文件，可以将它们组合到配置文件组中，以简化安全策略的创建。

要定义新的安全配置文件，请选择 **Objects**（对象）> **Security Profiles**（安全配置文件）。

下表介绍了安全配置文件设置：

安全配置文件组设置	说明
姓名	输入配置文件组名称（最多 31 个字符）。定义安全策略时，此名称将出现在配置文件列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享（仅限 Panorama）	如果想要将配置文件组用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件组只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件组只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的安全配置文件组对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
配置文件	选择要包括在此组中的防病毒软件、防间谍软件、漏洞防护、URL 筛选和/或文件传送阻止配置文件。还可以在安全配置文件组中指定数据筛选配置文件。请参阅 Objects（对象）> Security Profiles（安全配置文件）> Data Filtering（数据过滤）。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Log Forwarding（日志转发）

默认情况下，防火墙生成的日志仅驻留在其本地存储器中。但是，您可以定义日志转发配置文件并将其分配给安全、身份验证、DoS 保护和隧道检测策略规则，以使用 Panorama™、日志记录服务或外部服务（如 syslog 服务器）集中监控日志信息。日志转发配置文件可定义以下日志类型的转发目标：身份验证、数据筛选、GTP、SCTP、威胁、通信、隧道、URL 筛选和 WildFire® 提交日志。

出于以下原因，您应转发日志到 *Panorama* 或外部存储：合规性、冗余、运行分析、集中监控、审查威胁行为和长期模式。此外，防火墙具有的日志存储容量有限，在存储空间填满时，应删除最旧的日志。必须转发威胁日志和 *WildFire* 日志。

要转发其他日志类型，请参阅 Device（设备）> Log Settings（日志设置）。

要启用 *PA-7000* 系列防火墙将日志或文件转发到 *WildFire®*，您必须首先在 *PA-7000* 系列防火墙上配置日志卡接口。配置此接口后，防火墙将自动使用此端口 — 不需要特殊配置。只需将其中一个 *PA-7000* 系列网络处理卡 *(NPC)* 上的数据端口配置为日志卡接口类型，并确保所使用的网络可以与日志服务器进行通信。对于 *WildFire* 转发，网络必须与 *WildFire* 云或 *WildFire* 设备（或两者）成功通信。

下表介绍了日志转发配置文件设置。

日志转发配置文件设置	说明
姓名	输入标识配置文件的名称（最多 64 个字符）。定义安全策略规则时，此名称将出现在日志转发配置文件的列表中。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • **Every virtual system (vsys) on a multi-vsys firewall**（多虚拟系统防火墙上的每个虚拟系统 **(vsys)**）— 如果禁用（取消选中）此选项，配置文件仅对 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）可用。 • **Every device group on Panorama**（**Panorama** 上的每个设备组）— 如果禁用（取消选中）此选项，配置文件仅对 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）可用。
启用对 Cortex 数据湖的增强型应用程序日志记录（包括流量和 url 日志）（仅限 Panorama）	订阅 Cortex 数据湖后，Palo Alto Networks 云服务的增强应用程序日志可用。通过增强的应用程序日志记录，防火墙可收集专门用于提高 Palo Alto Networks 云服务环境中运行的应用程序的网络活动可见性的数据。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承配置文件的日志转发配置文件的设置。默认情况下，禁用（取消选中）此选项，这意味着管理员可以替代继承配置文件的任何设备组的设置。
说明	输入说明，解释此日志转发配置文件的用途。
匹配列表（未标记）	添加一个或多个指定转发目标、基于日志属性的过滤器的匹配列表配置文件（最多 64 个），以便控制防火墙转发的日志，以及对日志执行的操作（如

© 2019 Palo Alto Networks, Inc.

日志转发配置文件设置	说明
	自动标记）。为各匹配列表配置文件填写以下两个字段（Name（名称）和 Description（说明））。
名称（匹配列表配置文件）	输入标识匹配列表配置文件的名称（最多 31 个字符）。
说明（匹配列表配置文件）	输入说明（最多 1,023 个字符），解释此匹配列表配置文件的用途。
日志类型	选择此匹配列表配置文件适用的日志类型：（**auth**（身份验证））、**data**（数据）、**gtp**、**sctp**、**threat**（威胁）、**traffic**（通信）、**tunnel**（隧道）、**URL** 或 **WildFire**。
Filter（筛选器）	默认情况下，防火墙会转发所选日志类型的所有日志。要转发日志的子集，请从下拉列表中选择现有过滤器，或选择 **Filter Builder**（过滤器生成器）以添加新的过滤器。对于新过滤器中的每个查询，指定以下字段并 **Add**（添加）查询： • **Connector**（连接符）— 为查询选择逻辑连接符 (and/or)。如果想要应用逻辑否定，则选择 **Negate**（求反）。例如，要避免从不可信区域转发日志，可选择 **Negate**（求反），选择 **Zone**（区域）作为 Attribute（属性），选择 **equal**（等于）作为 Operator（运算符），然后在 Value（值）列中输入不可信区域的名称。 • **Attribute**（属性）— 选择日志属性。可用属性取决于日志类型。 • **Operator**（运算符）— 选择确定属性是否适用的标准（如 **equal**（等于））。可用标准取决于日志类型。 • 值- 指定要匹配的属性值。 要显示或导出与过滤器匹配的日志，请 **View Filtered Logs**（查看过滤的日志），此选项卡中提供与 **Monitoring**（监控）选项卡页面相同的选项（如 **Monitoring**（监控）> **Logs**（日志）> **Traffic**（流量））。
Panorama Panorama/日志记录服务（仅限 Panorama）	如果想要将日志转发到日志收集器或 Panorama 管理服务器，或者将日志转发到日志记录服务，请选中 **Panorama**。 如果启用此选项，必须将日志转发配置为 Panorama。 要使用日志记录服务，您还必须 **Enable**（启用）Device（设备）> Setup（设置）> Management（管理）中的日志记录服务。
SNMP	添加一个或多个 SNMP 陷阱服务器配置文件，以便以 SNMP 陷阱形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱））。
email	添加一个或多个电子邮件服务器配置文件，以便以电子邮件通知形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件））。
Syslog	添加一个或多个 Syslog 服务器配置文件，以便以 syslog 消息形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Syslog）。
Http	添加一个或多个 HTTP 服务器配置文件，以便以 HTTP 请求形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> HTTP）。
内置操作	**Add**（添加）操作以执行标记和集成时，您可以从两种类型的内置操作中进行选择。

© 2019 Palo Alto Networks, Inc.

日志转发配置文件设置	说明
	• 标记— 在日志条目的源 IP 地址或目标 IP 地址中自动添加或删除标记，并将 IP 地址和标记映射注册到防火墙或 Panorama 上的 User-ID 代理中，或注册到远程 User-ID 代理中，以便您响应事件并动态执行安全策略。使用动态地址组标记 IP 地址和动态执行策略的功能，可增强可见性和控制，改善上下文，不管在网络何处移动 IP 地址，都可持续执行安全策略。 配置以下设置： • 添加一项操作，并输入描述操作的名称。 • 选择要标记的目标 IP 地址 — **Source Address**（源地址）或 **Destination Address**（目标地址）。 可以对日志条目中包括源 IP 地址或目标 IP 地址的所有日志类型执行一项操作。在关联日志和 HIP 匹配日志中，只能标记源 IP 地址；不能为系统日志和配置日志配置操作，因为这些日志类型的日志条目中不包含 IP 地址。 • 选择操作 — **Add Tag**（添加标记）或 **Remove Tag**（删除标记）。 • 选择是将 IP 地址和标记映射注册到防火墙或 Panorama 上的本地 **User-ID** 代理中，还是注册到远程 **User-ID** 代理中。 • 要将 IP 地址和标记映射注册到远程 **User-ID** 代理中，请选择启用转发功能的 HTTP 服务器配置文件（Device（设备）> Server Profiles（服务器配置文件）> HTTP）。 • 配置要设置的 IP 标记**Timeout**（超时）（以分钟为单位），即，维护 IP 地址到标记映射的时间量。设置超时为 0，意味着 IP 标记映射未超时（范围为 0-43200（30 天），默认为 0）。 您只能使用*Add Tag*（添加标记）配置超时。 • 输入或选择要应用或从目标源或目标 IP 地址删除的 **Tags**（标记）。 • **Integration**（集成）— 仅供在 Azure 上的 VM 系列防火墙上使用。此选项允许您使用 **Azure-Security-Center-Integration** 操作将所选日志转发到 Azure 安全中心。 要根据日志转发配置文件筛选器添加设备到隔离列表，请选择 **Quarantine**（隔离）。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Authentication（身份验证）

身份验证执行对象可指定验证访问网络资源的最终用户所使用的方法和服务。您可以为身份验证策略规则分配对象，当流量与规则匹配时，就会调用身份验证方法和服务（请参阅 Policies（策略）> Authentication（身份验证））。

防火墙具有以下预定义的只读身份验证执行对象：

- **default-browser-challenge** — 防火墙采用透明的方式获取用户身份验证凭据。如果选择此操作，则在配置身份验证门户 时，必须启用 Kerberos 单一登入 (SSO) 或 NT LAN Manager (NTLM) 身份验证。如果 Kerberos SSO 身份验证失败，那么防火墙将回退到 NTLM 身份验证。如果没有配置 NTLM 或者 NTLM 身份验证失败，则防火墙将回退到预定义 **default-web-form** 对象所指定的身份验证方法。
- **default-web-form** — 为验证用户身份，防火墙将使用配置身份验证门户 时所指定的证书配置文件或身份验证配置文件。如果已指定身份验证配置文件，防火墙会忽略配置文件中的所有 Kerberos SSO 设置，显示身份验证门户页面，供用户输入身份验证凭据。
- **default-no-captive-portal** — 防火墙在不验证用户身份的情况下评估安全策略。

在创建自定义身份验证执行对象之前，需要执行以下操作：

- 配置服务器配置文件，以指定连接到身份验证服务的方式（请参阅Device（设备）> Server Profiles（服务器配置文件））。
- 为身份验证配置文件分配服务器配置文件，以指定 Kerberos 单一登入参数等身份验证设置（请参阅Device（设备）> Authentication Profile（身份验证配置文件））。

要创建自定义身份验证执行对象，请单击 **Add**（添加），然后填写以下字段：

身份验证执行设置	说明
姓名	输入描述性名称（最多 31 个字符），帮助您在定义身份验证规则时标识对象。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享（仅限 Panorama）	如果想要将对象用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则对象只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则对象只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承对象的身份验证执行对象的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承对象的所有设备组的设置。
身份验证方法	选择一种方法： • **browser-challenge** — 防火墙采用透明的方式获取用户身份验证凭据。如果选择此操作，您选择的 **Authentication Profile**（身份验证配置文件）必须已启用 Kerberos SSO。 • **web-form** — 为验证用户身份，防火墙将使用配置身份验证门户 时所指定的证书配置文件，或在身份验证执行对象中选择的身份验证配置文件。如果选择 **Authentication Profile**（身份验证配置文件），防火墙会忽略配置文件中的所有 Kerberos SSO 设置，显示身份验证门户页面，供用户输入身份验证凭据。

© 2019 Palo Alto Networks, Inc.

身份验证执行设置	说明
	• **no-captive-portal** — 防火墙在不验证用户身份的情况下评估安全策略。
身份验证配置文件	选择身份验证配置文件，以指定用于验证用户身份的服务。
消息	输入说明，指导用户如何响应在其流量触发身份验证规则时所看到的首次身份验证质询。该信息将显示在 **Authentication Portal Comfort Page**（身份验证门户认证页面）中。如果没有输入消息，则显示默认的 **Authentication Portal Comfort Page**（身份验证门户认证页面）（请参阅 Device（设备）> Response Pages（响应页面））。 防火墙仅对首次身份验证质询（因素）显示 *Authentication Portal Comfort Page*（身份验证门户认证页面），您可以在 *Authentication Profile*（身份验证配置文件）的 *Authentication*（身份验证）选项卡中对此进行定义（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。对于在配置文件的 *Factors*（因素）选项卡中定义的多重因素身份验证 *(MFA)* 质询，防火墙将显示 *MFA* 登录页面。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Decryption Profile（解密配置文件）

解密配置文件使您能够阻止和控制您为解密指定的 SSL 和 SSH 通信以及您明确从解密中排除的通信的特定方面。创建解密配置文件后，可以将此配置文件添加到解密策略；与解密策略匹配的所有通信，均可根据配置文件设置另行强制执行。

默认解密配置文件可在防火墙上进行配置，并可自动包含到新的解密策略中（不能修改默认解密配置文件）。单击添加以创建新的解密配置文件，或者选择现有配置文件，以克隆或修改它。

您在查找什么内容？	请参阅：
添加新解密配置文件。 启用解密的流量的端口镜像。	解密配置文件常规设置
阻止和控制 SSL 解密的流量。	控制解密 SSL 流量的设置
阻止和控制排除解密的流量（例如，分类为医疗保健和医药或金融服务的流量）。	控制未解密流量的设置
阻止和控制解密的 SSH 流量。	控制解密 SSH 流量的设置

解密配置文件常规设置

下表介绍了解密配置文件常规设置。

解密配置文件 — 常规设置	说明
姓名	输入配置文件名称（最多31个字符）。定义解密策略时，此名称将出现在解密配置文件的列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享（仅限 Panorama）	如果想要将配置文件用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则配置文件只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选择此选项可防止管理员在继承标记的设备组中替代此解密配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。
解密镜像接口 （适用于所有模型，但 AWS、Azure、NSX 版本和 Citrix SDX 上	选择接口以用于解密端口镜像。 在启用解密端口镜像之前，必须获取解密端口镜像许可证，安装此许可证，然后重新启动防火墙。

© 2019 Palo Alto Networks, Inc.

解密配置文件 — 常规设置	说明
的 VM 系列防火墙除外。）	
仅被转发 （适用于所有模型，但 AWS、Azure、NSX 版本和 Citrix SDX 上的 VM 系列防火墙除外。）	如果要仅在安全策略实施后镜像解密流量，请选择 **Forwarded Only**（仅被转发）。使用此选项，只镜像通过防火墙转发的流量。如果将解密的流量转发到其他威胁检测设备（如 DLP 设备或其他入侵防御系统 (IPS)），可以使用此选项。如果清除此选项（默认设置），防火墙会在安全策略查询之前将所有解密的流量镜像到接口，这可让您重播事件和分析生成威胁或触发丢弃操作的流量。

控制解密流量的设置

下表介绍了用于您用于控制流量的设置，防火墙使用正向代理解密或入站检查解密这些流量。您可以根据包括外部服务器证书状态、不支持的密码套件或协议版本的使用情况，或处理解密的系统资源的可用性在内的条件，使用这些设置限制或阻止 TLS 会话。

SSL 解密选项卡设置	说明
SSL 转发代理选项卡 选择此选项可限制或阻止使用正向代理解密的 TLS 流量。	
服务器证书验证 — 选择此选项可控制解密流量的服务器证书。	
阻止具有过期证书的会话	如果服务器证书过期，则终止 TLS 连接。此选项将阻止用户接受过期证书和无法继续 TLS 会话。 阻止具有过期证书的会话可阻止对潜在不安全站点的访问。
阻止具有不可信颁发者的会话	如果服务器证书颁发者不可信，则终止 TLS 会话。 阻止具有不可信颁发者的会话，因为不可信颁发者可能表示中间人攻击、重播攻击或其他攻击。
如果证书状态未知，则阻止会话	如果服务器返回“未知”证书吊销状态，则终止 TLS 会话。证书吊销状态指示是否已吊销证书的信任。 阻止证书状态未知的会话，已获得更严格的安全性。但是，因为由于多种原因，证书状况可能是未知，这会过多地加强安全性。如果阻止未知证书状态会影响您处理业务所需的站点，则请勿阻止具有未知证书状态的会话。
如果证书状态检查超时，则阻止会话	如果在为防火墙配置的停止等待证书状态服务响应的时间内未能检索到证书状态，则终止 TLS 会话。在创建或修改证书配置文件（**Device**（设备）>

© 2019 Palo Alto Networks, Inc.

SSL 解密选项卡设置	说明
	Certificate Management（证书管理）> **Certificate Profile**（证书配置文件））时，可以配置 **Certificate Status Timeout**（证书状态超时）值。 在状态检查超时时阻止会话是更严格的安全和更好的用户体验之间的权衡。如果证书吊销服务器响应缓慢，则超时阻止可能会阻止具有有效证书的站点。如果您担心超时有效证书，您可以增加证书吊销检查(CRL)和在线证书状态协议(OCSP)的超时值。
限制证书延期	将用于动态服务器证书的证书扩展限于密钥用法和扩展密钥用法。 如果您的部署无需其他证书延期，则限制证书延期。
将证书的 CN 值附加到 SAN 扩展	启用防火墙以向它作为 TLS 转发代理解密的一部分向客户端提供的模拟证书添加主题备选名称 (SAN) 扩展。当服务器证书仅包含通用名称 (CN) 时，防火墙会根据服务器证书 CN 向模拟证书添加 SAN 扩展。 如果浏览器需要服务器证书才能使用 SAN，并且不再支持基于 CN 的证书匹配，则此选项非常有用；它确保最终用户可以继续访问其请求的 Web 资源，并且即使服务器证书仅包含 CN，防火墙也可以继续解密会话。 附加证书 *CN* 值到 *SAN* 扩展，这有助于确保对请求 *Web* 资源的访问。
不受支持模式检查 — 选择选项可控制不受支持的 TLS 应用程序。	
阻止具有不受支持版本的会话	如果 PAN-OS 不支持“客户端呼叫”消息，则终止会话。PAN-OS 支持 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2 和 TLSv1.3。 始终阻止具有不受支持版本的会话，防止访问具有弱协议的站点。在 *SSL Protocol Settings*（*SSL* 协议设置）选项卡上，设置最高协议版本为 *TLSv1.2*，以阻止具有弱协议版本的站点。如果您出于业务目的需要访问的站点使用弱协议，则单独创建一个允许较弱协议的解密配置文件，并在仅适用于您必须允许较弱协议的站点的解密策略规则中予以指定。
阻止具有不受支持加密套件的会话	如果 PAN-OS 不支持在 TLS 握手中指定的密码套件，则终止会话。 阻止使用您不支持的密码套件的会话。您可以在 *SSL Protocol Settings*（*SSL* 协议设置）选项卡上配置允许的密码套件（加密算法）。不得允许用户连接到具有弱加密套件的站点。
阻止具有客户端认证的会话	终止具有转发代理通信的客户端身份验证的会话。 阻止具有客户端认证的会话，除非有重要的应用程序需要它，在这种情况下，您应创建一个单独的解密配置文件，并仅将其应用至需要客户端身份验证的流量。
失败检查 — 如果系统资源不可用于处理解密，则选择要执行的操作。	

© 2019 Palo Alto Networks, Inc.

SSL 解密选项卡设置	说明
如果资源不可用，则阻止会话	如果系统资源无法用于处理解密，则终止会话。 是否应在资源不可用时阻止会话是更严格的安全与更好的用户体验之间的权衡。如果在资源不可用时未阻止会话，在资源受到影响时，防火墙将无法解密您想要解密的流量。但是，若在资源不可用时阻止会话，则会影响用户体验，因为通常可访问的站点可能暂时无法访问。
HSM 不可用时阻止会话	如果硬件安全模块 (HSM) 不能用于签署证书，则终止会话。 在 HSM 不可用时是否阻止会话取决于您关于私钥来自何处以及您想要在 HSM 不可用时处理解密流量的方式等方面的合规性规则。
阻止在没有资源的情况下降级	如果没有可用于处理 TLSv1.3 握手的系统资源，则终止会话（而不是降级到 TLSv1.2）。 是否应在资源不可用时阻止会话是更严格的安全与更好的用户体验之间的权衡。如果您在 TLSv1.3 资源不可用时阻止握手降级到 TLSv1.2，则防火墙将丢弃会话。如果不阻止降级握手，那么，一旦没有可用于 TLSv1.3 握手的资源，防火墙将降低到 TLSv1.2。
客户端扩展	
剥离 ALPN	防火墙默认处理并检查 HTTP/2 流量。但是，您可以通过指定防火墙进行 **Strip ALPN**（剥离 **ALPN**）禁用 HTTP/2 检查。选择此选项后，防火墙可删除应用层协议协商(ALPN) TLS 扩展中包含的任何值）。 因为 ALPN 用于确保 HTTP/2 连接安全，因此，当没有为该 TLS 扩展指定值时，防火墙会将 HTTP/2 流量降级为 HTTP/1.1，或将其分类为未知 TCP 流量。

对于不受支持的模式和故障模式，会话信息会缓存 *12* 个小时，因此相同主机和服务器对之间的未来会话将不会被解密。可启用选项来阻止这些会话。

SSL 入站检查选项卡 选择此选项可限制或阻止使用入站检查的流量。	
不受支持模式检查 — 如果在 TLS 流量中检测到不受支持的模式，则选择此选项来控制会话。	
阻止具有不受支持版本的会话	如果 PAN-OS 不支持“客户端呼叫”消息，则终止会话。PAN-OS 支持 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2 和 TLSv1.3。 始终阻止具有不受支持版本的会话，防止访问具有弱协议的站点。在 *SSL Protocol Settings*（*SSL* 协议设置）选项卡上，设置最高协议版本为 *TLSv1.2*，以阻止具有弱协议版本的站点。如果您出于业务目的需要访问的站点使用弱协议，则单独创建一个允许较弱协议的解密配置文件，并在仅适用于您必须允许较弱协议的站点的解密策略规则中予以指定。
阻止具有不受支持加密套件的会话	如果 PAN-OS 不支持使用的密码套件，则终止会话。

© 2019 Palo Alto Networks, Inc.

SSL 解密选项卡设置	说明
	阻止使用您不支持的密码套件的会话。您可以在 *SSL Protocol Settings*（*SSL* 协议设置）选项卡上配置允许的密码套件（加密算法）。不得允许用户连接到具有弱加密套件的站点。
失败检查 — 如果系统资源不可用，则选择要执行的操作。	
如果资源不可用，则阻止会话	如果系统资源无法用于处理解密，则终止会话。 是否应在资源不可用时阻止会话是更严格的安全与更好的用户体验之间的权衡。如果在资源不可用时未阻止会话，在资源受到影响时，防火墙将无法解密您想要解密的流量。但是，若在资源不可用时阻止会话，则会影响用户体验，因为通常可访问的站点可能暂时无法访问。
HSM 不可用时阻止会话	如果硬件安全模块 (HSM) 不能用于解密会话密钥，则终止会话。 在 HSM 不可用时是否阻止会话取决于您关于私钥来自何处以及您想要在 HSM 不可用时处理解密流量的方式等方面的合规性规则。
阻止在没有资源的情况下降级	如果没有可用于处理 TLSv1.3 握手的系统资源，则终止会话（而不是降级到 TLSv1.2）。 是否应在资源不可用时阻止会话是更严格的安全与更好的用户体验之间的权衡。如果您在 TLSv1.3 资源不可用时阻止握手降级到 TLSv1.2，则防火墙将丢弃会话。如果不阻止降级握手，那么，一旦没有可用于 TLSv1.3 握手的资源，防火墙将降低到 TLSv1.2。
SSL 协议设置选项卡 选择以下设置可以对 TLS 会话流量强制执行协议版本和密码套件。	
协议版本	对 TLS 会话强制使用最低和最高协议版本。
最小版本	设置最低协议版本，以便用于建立 TLS 连接。 设置最低版本为 *TLSv1.2*，以提供最强安全性。查看不支持 *TLSv1.2* 的站点，检查是否这些站点确实具有合法的业务目的。对于您想要访问，但又不支持 *TLSv1.2* 的站点，单独创建一个指定站点支持的最强协议版本的解密配置文件，并将其应用于解密策略规则。该规则将弱版本的使用限制到仅允许来自必要源（区域、地址、用户）的必要站点。
最大版本	设置最高协议版本，以便用于建立 TLS 连接。可以选择最高版本选项，以便不指定最高版本；在这种情况下，支持不低于所选最低版本的协议版本。 将最高版本设置为 *Max*（最高），这样，随着协议的提升，防火墙会自动支持它们。 但是，如果解密策略支持移动应用程序，且其中有很多都使用固定证书，请将 *Max Version*（最高版本）设为 *TLSv1.2*。因为 *TLSv1.3* 会对在之前 *TLS* 版本中未加密的证书信息进行加密，防火墙无法根据证书信息自动添加解密排除项，这会影响某些移动应用程序。因此，一旦启用 *TLSv1.3*，除非您已为该流量创建不解密策略，否则，防火墙可能会丢弃某些移动应用程序流量。如果您出于业务目的而使用的移动应用程序是已知的，则考虑为

© 2019 Palo Alto Networks, Inc.

SSL 解密选项卡设置	说明
	这些应用程序创建单独的解密策略和配置文件，这样，您可以为所有其他流量启用 *TLSv1.3*。
密钥交换算法	对 TLS 会话强制使用选定的密钥交换算法。 默认启用所有三种算法（**RSA**、**DHE**和**ECDHE**）。**DHE** (Diffie-Hellman)和 **ECDHE**（椭圆曲线 Diffie-Hellman）可为 SSL 转发代理或入站检查解密启用完全向前保密 (PFS)。
加密算法	对 TLS 会话强制使用所选加密算法。 不支持 *3DES* 或 *RC4* 弱加密算法。（当您使用 *TLSv1.2* 或更高版本作为最低协议版本时，防火墙自动阻止这两个算法。）如果您设置例外，并支持较弱协议版本，则取消选中解密配置文件中的 *3DES* 和 *RC4*。如果出于业务目的，您必须访问使用 *3DES* 或 *RC4* 加密算法的站点，请单独创建一个解密配置文件，并将其应用至仅适用于这些站点的解密策略规则。
身份验证算法	对 TLS 会话强制使用所选身份验证算法。 阻止旧的 *MD5* 弱算法（默认阻止）。如果没有必要的站点使用 *SHA1* 身份验证，请阻止 *SHA1*。如果出于业务目的，您必须访问使用 *SHA1* 的站点，请单独创建一个解密配置文件，并将其应用至仅适用于这些站点的解密策略规则。

控制未解密流量的设置

可以使用 **No Decryption**（无解密）选项卡启用相关设置来阻止以下通信：与使用 **No Decrypt**（无解密）操作（**Policies**（策略）> **Decryption**（解密）> **Action**（操作））配置的解密策略匹配的通信。使用这些选项可以控制会话的服务器证书，但防火墙不能解密和检查会话流量。

无解密选项卡设置	说明
阻止具有过期证书的会话	如果服务器证书过期，则终止 SSL 连接。此选项将阻止用户接受过期证书和无法继续 SSL 会话。 阻止具有过期证书的会话可阻止对潜在不安全站点的访问。
阻止具有不可信颁发者的会话	如果服务器证书颁发者不可信，则终止 SSL 会话。 阻止具有不可信颁发者的会话，因为不可信颁发者可能表示中间人攻击、重播攻击或其他攻击。

© 2019 Palo Alto Networks, Inc.

控制解密 SSH 流量的设置

下表介绍了用于控制解密入站和出站 SSH 流量的设置。这些设置可让您根据包括不支持算法的使用情况、SSH 错误检测或处理 SSH 代理解密的资源可用性在内的条件，限制或阻止 SSH 隧道流量。

SSH 代理选项卡设置	说明
不受支持模式检查 — 如果在 SSH 流量中检测到不受支持的模式，则使用这些选项控制会话。受支持的 SSH 版本为 SSH 版本 2。	
阻止具有不受支持版本的会话	如果 PAN-OS 不支持“客户端呼叫”消息，则终止会话。 始终阻止具有不受支持版本的会话，防止访问具有弱协议的站点。在 *SSL Protocol Settings*（*SSL* 协议设置）选项卡上，设置最高协议版本为 *TLSv1.2*，以阻止具有弱协议版本的站点。如果您出于业务目的需要访问的站点使用弱协议，则单独创建一个允许较弱协议的解密配置文件，并在仅适用于您必须允许较弱协议的站点的解密策略规则中予以指定。
阻止具有不受支持算法的会话	如果 PAN-OS 不支持客户端或服务器指定的算法，则终止会话。 始终阻止具有不受支持算法的会话，防止访问具有弱算法的站点。
失败检查 — 如果发生 SSH 应用程序错误且系统资源不可用，则选择要执行的操作。	
如果发生 SSH 错误，则阻止会话	如果发生 SSH 错误，则终止会话。
如果资源不可用，则阻止会话	如果系统资源无法用于处理解密，则终止会话。 是否应在资源不可用时阻止会话是更严格的安全与更好的用户体验之间的权衡。如果在资源不可用时未阻止会话，在资源受到影响时，防火墙将无法解密您想要解密的流量。但是，若在资源不可用时阻止会话，则会影响用户体验，因为通常可访问的站点可能暂时无法访问。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Decryption（解密）> Forwarding Profile（转发配置文件）

您可以设置解密转发配置文件，以使防火墙充当解密代理。解密代理防火墙将其已解密和检查的通信转发到安全链（一组内联第三方安全设备）以进行进一步实施。您还可以配置防火墙为安全链提供会话分发，以确保安全链设备不会被超额预订。从安全链接收通信时，防火墙会重新加密通信并将其转发到相应的目的地。

在创建解密转发配置文件以启用解密代理之前，您必须：

- 启用 SSL 转发代理解密。
- 在防火墙上至少分配两个第 3 层接口，用于将解密通信转发到安全链（选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），编辑接口，选择 **Advanced**（高级）> **Other Info**（其他信息），然后启用 Decrypt Forward（解密转发））。重复此任务以启用第二个接口作为解密转发界面。

完成这些任务后，创建解密转发配置文件以对两个接口进行配对，并定义防火墙将解密通信转发到的安全链的设置。

要详细了解受支持的解密代理和安全链部署并了解启用防火墙充当解密代理的完整工作流程，请参阅解密代理。

解密转发设置	说明
姓名	指定配置文件的描述性名称。
说明	（可选）描述配置文件设置。
“常规”选项卡	
安全链类型	选择防火墙将解密通信转发到的安全链的类型： • **Routed (Layer 3)**（路由（第 3 层））：此类安全链中的设备使用第 3 层接口连接到安全链网络 — 每个接口必须具有分配的 IP 地址和子网掩码。安全链设备配置有静态路由（或动态路由），以将入站和出站通信引导到安全链中的下一个设备并返回到防火墙。 • **Transparent Bridge**（透明桥接）：在透明桥接安全链网络中，所有安全链设备均配置有两个连接到安全链网络的接口。这两个数据面板接口均配置为透明桥接模式；它们不具有分配的 IP 地址、子网掩码、默认网关和本地路由表。透明桥接模式的安全链设备在一个接口上接收通信，然后在通信经由另一个接口流出至下一个内联安全链设备之前对通信进行分析和实施。
流方向	指定防火墙引导解密入站和出站会话通过安全链的方式：相同方向（单向）或相反方向（双向）。您选择的流方向取决于构成安全链的设备的类型。例如，如果安全链包含可以检查会话两端的无状态设备，则可以选择单向流。
主接口	选择防火墙将用于将通信转发到安全链的主接口和辅助接口。主接口和辅助接口共同构成一对解密转发接口。仅显示您配置为解密转发接口的接口。
辅助接口	
安全链选项卡	
启用	启用安全链。

© 2019 Palo Alto Networks, Inc.

解密转发设置	说明
姓名	指定安全链的描述性名称。
第一个设备 最后一个设备	选择安全链中第一个设备和最后一个设备的 IPv4 地址，或者定义新的地址对象以轻松引用设备。
会话分发方法	如要转发到多路由（第 3 层）安全链，请选择防火墙将用于在安全链中分发解密会话的方法： • **IP Modulo**（**IP** 模）— 防火墙根据源和目标 IP 地址的模块哈希分配会话。 • **IP Hash**（**IP** 哈希）— 防火墙根据源和目标 IP 地址的 IP 哈希及端口号分配会话。 • **Round Robin**（循环）— 防火墙在安全链中均匀分配会话。 • **Lowest Latency**（最低延迟）— 防火墙以最低延迟向安全链分配更多会话。要使此方法按预期工作，您还必须启用延迟监控和 HTTP 监控（选择 **Health Monitor**（运行状况监控））。
运行状况监控选项卡	
未通过运行状况检查	如果与此解密转发配置文件关联的所有安全链未通过运行状况检查，请为防火墙选择 **Bypass Security Chain**（绕过安全链）（允许会话通信）或 **Block Session**（阻止会话）。 这意味着，当解密配置文件配置了多个安全链时，如果单个安全链未通过运行状况检查，则防火墙将根据 **Security Chains**（安全链）选项卡上指定的方法在剩余的运行状况良好的安全链中执行会话分配 — 如果每个安全链均未通过运行状况检查，则防火墙仅基于此设置阻止或允许通信。
未通过运行状况检查的条件	将未通过运行状况检查定义为符合任何运行状况监控条件（**OR Condition**（**OR** 条件））或符号所有条件（**AND Condition**（**AND** 条件））的事件。
路径监视 延迟监控 HTTP 监控	启用路径、延迟或 HTTP 监控或三者的任意组合，以标识安全链未有效处理解密通信的情况。对于您启用的每种监控类型，定义将触发未通过运行状况检查的时间段和计数。 启用： • 路径监控以检查设备连接性。 • 延迟监控以检查设备处理速度和效率。 • HTTP 监控以检查设备可用性和响应时间。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）

创建可应用至 SD-WAN 策略规则中指定应用程序和服务集的配置文件。每种配置文件都可控制 SD-WAN 链路管理各个方面。

- Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Path Quality Profile（路径质量配置文件）
- Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> SaaS Quality Profile（SaaS 质量配置文件）
- Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Traffic Distribution Profile（流量分发配置文件）
- Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Error Correction Profile（纠错配置文件）

Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Path Quality Profile（路径质量配置文件）

SD-WAN 允许您为具有独特网络质量要求的每组应用程序、应用程序过滤器、应用程序组、服务、服务对象和服务组对象创建路径质量配置文件，然后在 SD-WAN 策略规则中引用该配置文件。在配置文件中，为三个参数设置了最大阈值：延迟、抖动和数据包丢失。若 SD-WAN 链路超过任何一个阈值，则防火墙会为与应用了此配置文件的 SD-WAN 规则匹配的数据包选择一个新的最佳路径。

通过每个路径质量参数的敏感性设置，可告知防火墙哪个参数对应用配置文件的应用程序更重要（首选）。与设置为中或低敏感性的参数相比，防火墙更重视设置为高敏感性的参数。例如，某些应用程序对数据包丢失比对抖动或延迟更为敏感，因此，您可以将数据包丢失设置为高敏感性，这会使防火墙首先检查数据包丢失。

若将延迟、抖动和数据包丢失的敏感性设置保留为默认设置（中），或者将所有三个参数都设置为同一设置，则配置文件的优先顺序为数据包丢失、延迟和抖动 。

默认情况下，防火墙每 200 毫秒测量延迟和抖动一次，取最后三个测量值的平均值，从而衡量滑动窗口中的路径质量。您可以通过在配置 SD-WAN 接口配置文件时选择积极或宽松的路径监控来修改这一行为。

	路径质量配置文件设置
姓名	输入路径质量配置文件的名称，可使用字母数字字符、下划线、连字符、空格和句点（最多 31 个字符）。
延迟（毫秒）	**Threshold**（阈值）— 输入允许数据包离开防火墙并到达 SD-WAN 隧道另一端，以及响应数据包在超过阈值之前返回到防火墙的毫秒数（范围为 10 至 2,000；默认为 100）。
	Sensitivity（敏感性）— 选择 **high**（高）、**medium**（中）或 **low**（低）（默认为 **medium**（中）。
抖动（毫秒）	**Threshold**（阈值）—输入毫秒数（范围为 10-1,000；默认为 100）。
	Sensitivity（敏感性）— 选择 **high**（高）、**medium**（中）或 **low**（低）（默认为 **medium**（中）。

© 2019 Palo Alto Networks, Inc.

	路径质量配置文件设置
数据包丢失 (%)	**Threshold**（阈值）— 输入超过阈值之前链路上的数据包丢失百分比（范围为 1 至 100.0；默认为 1）。
	Sensitivity（敏感性）— 数据包丢失的敏感性设置不受影响，因此，可以不管默认设置（**medium**（中））。

Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> SaaS Quality Profile（SaaS 质量配置文件）

您可以通过 SD-WAN 创建软件即服务 (SaaS) 质量配置文件，以测量中心或分支防火墙与服务器侧 SaaS 应用程序之间的路径运行状况质量，从而准确地监视 SaaS 应用程序的可靠性，并在路径运行状况质量下降时更换路径。这样，防火墙可准确确定将故障转移到其他互联网直接接入 (DIA) 链路的时间。

通过 SaaS 质量配置文件，您可以使用用于监视应用程序活动的自适应学习算法指定要监视的 SaaS 应用程序，或是通过使用应用程序 IP 地址、FQDN 或 URL 指定 SaaS 应用程序。

	SaaS 质量配置文件设置
姓名	输入路径质量配置文件的名称，可使用字母数字字符、下划线、连字符、空格和句点。
共享（仅限 Panorama）	勾选（启用）此选项可使所有设备组共享 SaaS 质量配置文件。
禁用替代（仅限 Panorama）	勾选（启用）此选项可受管防火墙上本地替代 SaaS 质量配置文件设置这一功能。
SaaS 监视模式	
自适应	监视 SaaS 应用程序会话活动以发送和接收活动，且路径运行状况自动派生，无需在 SD-WAN 接口上执行任何其他运行状况检查。默认勾选此选项。
静态 IP 地址	**IP Address/Object**（**IP** 地址/对象）—指定使用应用程序 IP 地址进行监视的 SaaS 应用程序。 • **IP Address**（**IP** 地址）— SaaS 应用程序的 IP 地址。 • **Probe Interval (Sec)**（探测间隔（秒））— 指定防火墙探测防火墙和 SaaS 应用程序之间路径运行状况质量的间隔（以秒为单位）。默认值为 3 秒。 最多支持 4 个静态 IP 地址。
	FQDN— 指定使用应用程序完全限定域名 (FQDN) 进行监视的 SaaS 应用程序。 • **FQDN**— SaaS 应用程序的 FQDN。若要指定 FQDN，必须配置一个 FQDN 地址对象。 SaaS 应用程序 FQDN 必须是可以解析的，以便成功监视 SaaS 应用程序。 • **Probe Interval (sec)**（探测间隔（秒））— 指定防火墙探测分支防火墙和 SaaS 应用程序之间路径运行状况质量的间隔（以秒为单位）。默认值为 3 秒。
HTTP/HTTPS	指定使用 HTTP/HTTPS URL 进行监视的 SaaS 应用程序。 • **Monitored URL**（受监视的 **URL**）— SaaS 应用程序的 HTTP 或 HTTPS URL。

© 2019 Palo Alto Networks, Inc.

	SaaS 质量配置文件设置
	• **Probe Interval (sec)**（探测间隔（秒））— 指定防火墙探测防火墙和 SaaS 应用程序之间路径运行状况质量的间隔（以秒为单位）。默认值为 3 秒。

Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Traffic Distribution-Profile（流量分发配置文件）

对于此流量分发配置文件，选择防火墙用于分发会话并在路径质量降低时故障转移到更好的路径的方法。添加防火墙在确定其用于转发 SD-WAN 流量的链路时会考虑的链路标签。将流量分发配置文件应用于所创建的每个 SD-WAN 策略规则。

	流量分发配置文件
姓名	输入流量分发配置文件的名称，使用字母数字字符、连字符、空格、下划线和句点（最多 31 个字符）。
最佳可用路径	在不计成本且允许应用程序使用分支以外的任何路径时，选择最佳可用路径。防火墙会根据路径质量指标从属于列表中所有链路标签的链路中，分发流量并故障转移到链路，从而为用户提供最佳的应用程序体验。
自上而下优先级	如果您只想将高成本或低容量链路用作最后的选择或备用链路，请选择自上而下优先级方法，将包含这些链路的标签置于此配置文件中链路标签列表的最后一位。防火墙首先使用列表中排名第一的链路标记确定会话负载流量使用的链路以及执行故障转移的链路。如果排第一的链路标签中的链路都不合格，则防火墙将从列表中排名第二的链路标签中选择一个链路。如果排名第二的链路标记中的链路也都不合格，则根据需要继续执行此过程，直至防火墙在之后一个链路标记中找到合格的链路。如果所有关联链路都过载，且没有链路满足质量阈值要求，则防火墙使用最佳可用路径方法选择用于转发流量的链路。 如果应用程序的抖动、延迟或数据包丢失超过了配置的阈值，则防火墙从链路标签自上而下的列表顶部开始，查找用于进行故障转移的链路。
加权会话分发	如果您想手动加载与规则匹配的流量到 ISP 和 WAN 链路，且您无需在电源不足情况下执行故障转移，请选择加权会话分发。您可以在应用新会话静态百分比时，手动指定链路负载。此会话是采用单个标记进行分组的接口所获取的会话。对于对延迟不敏感，且需要大量链路带宽容量（例如，大的分支备份和大的文件传输）的应用程序，您可以选择此方法。请记住，如果链路出现掉电的情况，防火墙不会将匹配流量反映到不同的链路。
链路标签	添加您希望防火墙在为此配置文件选择的链路选择过程中考虑的链路标签。如果您选择自上而下优先级方法，则标签顺序很重要；请使用上移或下移标签来更改标签顺序。
重量	若选择加权会话分发方法，请为添加的每个链路标签输入百分比。百分比值之和必须为 100%。

Objects（对象）> SD-WAN Link Management（SD-WAN 链路管理）> Error Correction Profile（纠错配置文件）

如果您的 SD-WAN 流量包含对数据包丢失或损坏敏感的应用程序（例如，音频、VoIP 或视频会议），您可以将前向纠错 (FEC) 或数据包重复用作纠错方式。通过 FEC，接收防火墙（解码器）可通过部署编码器嵌入到应用程序流中奇偶校验位来恢复丢失或损坏的数据包。数据包重复是另一种纠错方式，在这种方式中，应

© 2019 Palo Alto Networks, Inc.

用程序会话从一个隧道复制到第二个隧道。两种方式都需要额外的带宽和 CPU 开销；因此，仅将 FEC 或数据包重复应用至可从此方法中受益的应用程序。要使用其中一种方法，请创建纠错配置文件，并在 SD-WAN 策略规则中将其引用至特定应用程序。

（此外，您还必须通过在 SD-WAN 接口配置文件中指示接口为 **Eligible for Error Correction Profile interface selection**（纠错配置文件接口的选择条件）的方式，指定防火墙选择用于纠错的接口）

	纠错配置文件设置
姓名	添加纠错配置文件的描述性名称，最多使用 31 个字符。
共享	勾选此选项可将纠错配置文件用于 Panorama 上的所有设备组，以及您推送配置的多虚拟系统中心或分支上的每个虚拟系统。 Panorama 可访问防火墙配置验证中共享的纠错配置文件，并成功将配置提交并推送到分支和中心。如果 Panorama 无法引用纠错配置文件，则提交失败。
禁用替代	选择此选项可防止管理员在继承配置文件的设备组中替代此纠错配置文件的设置。（如果选择 **Shared**（共享），则 **Disable override**（禁用替代）可用。）
激活阈值（数据包丢失百分比）	一旦数据包丢失超过此百分比，则会为应用纠错配置文件的 SD-WAN 策略规则中配置的应用程序激活 FEC 或数据包重复。范围为 1 至 99；默认为 2。
前向纠错/数据包重复	选择是否部署前向纠错 (FEC) 或数据包重复。数据包重复需要的资源比 FEC 大得多。
数据包丢失纠正率	（仅限前向纠错）奇偶验证位与数据包的比率。编码器发送到解码器的奇偶验证位与数据包的比率越高，解码器修复数据包丢失的几率越高。但是，比率越高，需要的冗余就更多，因此，会需要更多的带宽开销，这是为实现纠错的权衡做法。请选择其中一个预定义比率： • **10% (20:2)**（默认） • **20% (20:4)** • **30% (20:6)** • **40% (20:8)** • **50% (20:10)** 奇偶验证比率适用于编码防火墙传出流量。例如，如果中心的奇偶验证比率为 50%，分支的奇偶验证比率为 20%，那么，中心可接受的比率为 20%，分支可接受的比率为 50%。
恢复持续时间（毫米）	接收防火墙（解码器）使用接收到的奇偶验证数据包对丢失的数据包执行数据包恢复所花费的最长毫秒数；范围为 1-5,000；默认为 1,000。 防火墙立即发送其接收到的数据包给目标。在恢复数据块期间，防火墙将为任何丢失的数据包执行数据包恢复。一旦恢复持续时间耗尽，用于该数据块的关联奇偶验证位将被丢弃。 编码器发送恢复持续时间值给解码器；这不会影响解码器上的恢复持续时间设置。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> Schedules（计划）

默认情况下，安全策略规则始终有效（适用于任何日期和时间）。如需将安全策略规则限制到特定时间，可以定义调度，然后将调度应用到合适的策略。对于每个计划，可以指定固定的日期和时间范围或重复性的每日或每周计划。要将调度应用到安全策略，请参阅 Policies（策略）> Security（安全）。

由定义的调度调用安全策略规则时，仅新会话受所应用的安全策略规则影响。现有会话不受调度的策略影响。

调度设置	说明
姓名	输入调度名称（最多 31 个字符）。定义安全策略时，此名称将出现在调度列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享（仅限 Panorama）	如果想要将调度用于以下位置，请选中此选项： • 多虚拟系统防火墙上的每个虚拟系统 (vsys)。如果取消选中此选项，则调度只可用于在 **Objects**（对象）选项卡中选择的 **Virtual System**（虚拟系统）。 • Panorama 上的每个设备组。如果取消选中此选项，则调度只可用于在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）。
禁用替代（仅限 Panorama）	选中此选项后，可阻止管理员替代设备组中继承此调度的调度的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承调度的所有设备组的设置。
重复	选择调度类型（**Daily**（每天）、**Weekly**（每周）或 **Non-Recurring**（非重复））。
每天	单击 **Add**（添加），然后采用 24 小时制 (HH:MM) 指定 **Start Time**（开始时间）和 **End Time**（结束时间）。
每周	单击 **Add**（添加），然后采用 24 小时制 (HH:MM) 选择 **Day of Week**（星期几），并指定 **Start Time**（开始时间）和 **End Time**（结束时间）。
非重复	单击 **Add**（添加），然后指定 **Start Date**（开始日期）、**Start Time**（开始时间）、**End Date**（结束日期）和 **End Time**（结束时间）。

网络

以下主题介绍防火墙网络设置。

> Network（网络）> Virtual Wires（虚拟线路）
> Network（网络）> Interfaces（接口）
> Network（网络）> Virtual Routers（虚拟路由器）
> Network（网络）> Zones（区域）
> Network（网络）> VLAN
> Network（网络）> IPSec Tunnels（IPSec 隧道）
> Network（网络）> GRE Tunnels（GRE 隧道）
> Network（网络）> DHCP
> Network（网络）> DNS Proxy（DNS 代理）
> Network（网络）> QoS
> Network（网络）> LLDP
> Network（网络）> Network Profiles（网络配置文件）

Network（网络）> Interfaces（接口）

防火墙接口（端口）使防火墙可以与其他网络设备以及防火墙之内的其他接口相连。以下主题将介绍接口类型及其配置方式：

您在查找什么内容？	请参阅
什么是防火墙接口？	防火墙接口概述
我不太了解防火墙接口；防火墙接口有哪些部分组成？	防火墙接口的通用构建块 PA-7000 系列防火墙接口的通用构建块
我已经了解防火墙接口；怎样才能找到有关配置特定接口类型的信息？	**物理接口 (Ethernet)** 旁接接口 HA 接口 虚拟线路接口 虚拟线路子接口 PA-7000 系列第 2 层接口 PA-7000 系列第 2 层子接口 PA-7000 系列第 3 层接口 第 3 层接口 第 3 层子接口 日志卡接口 日志卡子接口 解密镜像接口 聚合以太网 (AE) 接口组 聚合以太网 (AE) 接口 **逻辑接口** Network（网络）> Interfaces（接口）> VLAN Network（网络）> Interfaces（接口）> Loopback（回环） Network（网络）> Interfaces（接口）> Tunnel（隧道） Network（网络）> Interfaces（接口）> SD-WAN
了解更多？	networking（网络）

防火墙接口概述

通过对防火墙数据端口进行接口配置可以使通信进入和退出防火墙。Palo Alto Networks® 防火墙可以在多个部署中同时运行，因为您可以配置接口以支持不同部署。例如，您可以在防火墙上为虚拟线路、第 2 层、第 3 层和 TAP 模式配置以太网接口。防火墙支持的接口有：

© 2019 Palo Alto Networks, Inc.

- **Physical Interfaces**（物理接口）— 防火墙有两种介质，即铜线和光纤接口，它们能以不同的传输速率发送和接收流量。您可以将 Ethernet 接口配置为以下类型：旁接、高可用性 (HA)、日志卡（接口和子接口）、解密镜像、virtual wire（接口和子接口）、第 2 层（接口和子接口）、第 3 层（接口和子接口）及聚合 Ethernet。可用的接口类型和传输速率因硬件型号而异。
- **Logical Interfaces**（逻辑接口）— 包括虚拟局域网 (VLAN) 接口、回环接口、隧道接口和 SD-WAN 接口。在定义 VLAN、SD-WAN 或隧道接口之前，您必须先设置物理接口。

防火墙接口的通用构建块

选择 **Network**（网络）> **Interfaces**（接口）可显示并配置多数接口类型通用的组件。

有关在配置 *PA-7000* 系列防火墙上的接口时或在使用 *Panorama*™ 配置任意防火墙上的接口时所遇到的特有或不同组件的说明，请参阅 PA-7000 系列防火墙接口的通用构建块。

防火墙接口构建块	说明
接口（接口名称）	接口名称是预定义的，您不能对其进行更改。但是，您可以为子接口、聚合接口、VLAN 接口、回环接口、隧道接口和 SD-WAN 接口附加数字后缀。
接口类型	对于以太网接口（**Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）），您可以选择接口类型： • 旁接 • **HA** • **Decrypt Mirror**（解密镜像）（适用于所有防火墙，但 VM 系列 NSX、Citrix SDX、AWS 和 Azure 除外。） • 虚拟线路 • 第 **2** 层 • 第 **3** 层 • **Log Card**（日志卡）（仅限 PA-7000 系列防火墙） • 聚合以太网
管理配置文件	选择 **Management Profile**（管理配置文件）（**Network**（网络）> **Interfaces**（接口）> **<if-config** > **Advanced**（高级）> **Other Info**（其他信息））可定义协议（如 SSH、Telnet 和 HTTP），之后您可用其通过该接口来管理防火墙。
链接状态	对于 Ethernet 接口，Link State（链接状态）列将指示接口当前是否可访问并可接收网络上的通信： • **Green**（绿色）— 已配置并启用 • **Red**（红色）— 已配置但关闭或禁用 • **Gray**（灰色）— 未配置 将鼠标悬停在链接状态上可显示工具提示，以指示接口的链接速度和双工设置。
IP 地址	（可选）配置 Ethernet、VLAN、回环或隧道接口的 IPv4 或 IPv6 地址。对于 IPv4 地址，您也可选择接口的寻址模式（**Type**（类型））：**Static**（静态）、**DHCP Client**（**DHCP** 客户端）或 **PPPoE**。
虚拟路由器	将虚拟路由器分配给接口，或单击 **Virtual Router**（虚拟路由器）可定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。

© 2019 Palo Alto Networks, Inc.

防火墙接口构建块	说明
标记（仅限子接口）	输入该子接口的 VLAN 标记 (1-4,094)。
vlan	选择 **Network**（网络）> **Interfaces**（接口）> **VLAN**，并修改现有的 **VLAN** 或 **Add**（添加）新的 VLAN（请参阅 Network（网络）> VLAN）。选择 **None**（无）可从接口删除当前 VLAN 分配。要启用第 2 层接口之间的切换，或要通过 VLAN 接口启用路由，必须配置 VLAN 对象。
虚拟系统	如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域	选择接口的 **Security Zone**（安全区域）（**Network**（网络）> **Interfaces**（接口）> **<if-config** > **Config**（配置）），或选择 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
功能	对于 Ethernet 接口，此列可指明以下功能是否已启用： DHCP 客户端 DNS 代理 GlobalProtect™ 网关已启用 链路聚合控制协议 (LACP) 链路层发现协议 (LLDP) NDP 监控 NetFlow 配置文件 服务质量 (QoS) 配置文件 SD-WAN
注释	有关接口功能或用途的说明。

PA-7000 系列防火墙接口的通用构建块

下表介绍了在配置 PA-7000 系列防火墙上的接口时或在使用 Panorama 配置任意防火墙上的接口时会遇到的 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）页面上的特有或不同组件。请单击 **Add Interface**（添加接口）以创建新接口，或选择现有接口（如 ethernet1/1）以对其进行编辑。

在 *PA-7000* 系列防火墙上，您必须在一个数据端口上配置日志卡接口。

© 2019 Palo Alto Networks, Inc.

PA-7000 系列防火墙接口构建块	说明
插槽	选择接口的插槽号 (1-12)。只有 PA-7000 系列防火墙有多个插槽。如果使用 Panorama 为任何其他防火墙型号配置接口，请选择 **Slot 1**（插槽 **1**）。
接口（接口名称）	选择与所选插槽关联的接口的名称。

旁接接口

- Network（网络）> Interfaces（接口）> Ethernet

可以使用旁接接口监控端口上的通信。

要配置旁接接口，请单击还未配置的接口的名称（例如，ethernet1/1），并指定以下信息。

旁接接口设置	配置位置	说明
接口名称	以太网接口	接口名称是预定义的，您不能对其进行更改。
注释		输入接口的可选说明。
接口类型		选择旁接。
Netflow 配置文件		如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）即可定义新的配置文件（请参阅Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
虚拟系统	**Ethernet Interface**（以太网接口）> **Config**（配置）	如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
链接速度	**Ethernet Interface**（以太网接口）> **Advanced**（高级）	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择 **auto**（自动）以使防火墙自动确定速度。
链接双工		选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态		选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。

HA 接口

- Network（网络）> Interfaces（接口）> Ethernet

各个高可用性 (HA) 接口都有特定的功能：一个接口用于配置同步和检测信号，另一个接口用于状态同步。如果启用了主动/主动高可用性，防火墙可以使用第三个 HA 接口来转发数据包。

© 2019 Palo Alto Networks, Inc.

有些 *Palo Alto Networks* 防火墙包括 *HA* 部署中使用的专用物理端口（一个用于控制链接，一个用于数据链接）。对于那些不包括专用端口的防火墙，必须指定 *HA* 要使用的数据端口。有关 *HA* 的其他信息，请参阅 *Device*（设备）> *Virtual Systems*（虚拟系统）。

要配置 HA 接口，请单击还未配置的接口的名称（例如，ethernet1/1），并指定以下信息。

高可用性接口设置	说明
接口名称	接口名称是预定义的，您不能对其进行更改。
注释	输入接口的可选说明。
接口类型	选择 **HA**。
链接速度	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择 **auto**（自动）以使防火墙自动确定速度。
链接双工	选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态	选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。

虚拟线路接口

- Network（网络）> Interfaces（接口）> Ethernet

虚拟线路将两个以太网接口以逻辑方式绑定在一起，从而允许在接口之间传递所有通信，或仅允许传递具有所选 VLAN 标记的通信（没有其他交换或路由服务可用）。您可以创建虚拟线路子接口，以根据 IP 地址、IP 范围或子网对通信进行分类。虚拟线路不需要对相邻网络设备进行更改。虚拟线路可以将相同类型（均为铜或均为光纤）的两个以太网接口绑定在一起，或将一个铜接口和一个光纤接口绑定在一起。

要设置虚拟线路，请确定要绑定哪两个接口（**Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网））并按下表所述配置其设置。

如果您将现有接口用于 *Virtual Wire*，先从任何相关的安全区域删除接口。

Virtual Wire 接口设置	配置位置	说明
接口名称	以太网接口	接口名称是预定义的，您不能对其进行更改。
注释		输入接口的可选说明。
接口类型		选择 **Virtual Wire**。
虚拟线路	**Ethernet Interface**（以太网接口）> **Config**（配置）	选择虚拟线路或单击 **Virtual Wire**（虚拟线路）可定义新的虚拟线路（Network（网络）> Virtual Wires（虚拟线路））。选择 **None**（无）可从接口删除当前 Virtual Wire 分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。

© 2019 Palo Alto Networks, Inc.

Virtual Wire 接口设置	配置位置	说明
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
链接速度	**Ethernet Interface**（以太网接口）> **Advanced**（高级）	选择特定的接口速度（以 Mbps 为单位），或选择 **auto**（自动）以使防火墙自动确定速度。虚拟线路中的两个接口必须具有相同的速度。
链接双工		选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。虚拟线路中的两个接口必须采用相同的传输模式。
链接状态		选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。
启用 LLDP	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **LLDP**	选择此选项可在接口上启用链路层发现协议 (LLDP)。链路层上的 LLDP 功能可发现邻近设备及其功能。
配置文件		如果已启用 LLDP，请选择要分配给接口的 LLDP 配置文件，或单击 **LLDP Profile**（**LLDP** 配置文件）以创建新的配置文件（请参阅 Network（网络）> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件））。选择 **None**（无）可将防火墙配置为使用全局默认值。
在高可用性被动状态中启用		如果 LLDP 已启用，请选中此选项以配置 HA 被动防火墙在变为主动前，与其对端预先协商 LLDP。 如果 LLDP 未启用，请选中此选项以配置 HA 被动防火墙仅使 LLDP 数据包通过该防火墙。

虚拟线路子接口

- Network（网络）> Interfaces（接口）> Ethernet

Virtual wire (vwire) 子接口可通过 VLAN 标记或通过 VLAN 标记和 IP 分类器的组合来分隔通信，将标记的通信分配到不同的区域和虚拟系统，然后对与所定义条件匹配的通信实施安全策略。

如需添加虚拟线路接口，请选中该接口所在的行，单击 **Add Subinterface**（添加子接口），然后指定以下信息。

Virtual Wire 子接口设置	说明
接口名称	只读的 **Interface Name**（接口名称）字段会显示您所选 vwire 接口的名称。在相邻字段中，输入数字后缀 (1-9,999) 以标识子接口。
注释	输入子接口的可选说明。
标记	输入该子接口的 VLAN 标记 (0-4,094)。
Netflow 配置文件	果您想要导出从 ingress 子接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）即可定义新的配置文件（参阅Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择无可从子接口删除当前 NetFlow 服务器分配。

© 2019 Palo Alto Networks, Inc.

Virtual Wire 子接口设置	说明
IP 分类器	单击添加并输入 IP 地址、IP 范围或子网，以对该 vwire 子接口上的通信进行分类。
虚拟线路	选择 Virtual Wire，或单击 **Virtual Wire** 可定义新的 Virtual Wire（参阅Network（网络）> Virtual Wires（虚拟线路））。选择 **None**（无）可从子接口删除当前 Virtual Wire 分配。
虚拟系统	如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于子接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域	选择子接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从子接口删除当前区域分配。

PA-7000 系列第 2 层接口

- Network（网络）> Interfaces（接口）> Ethernet

选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）可配置第 2 层接口。请单击未配置的接口的名称（例如 ethernet1/1），并指定以下信息。

第 2 层接口设置	配置位置	说明
接口名称	以太网接口	接口名称是预定义的，您不能对其进行更改。
注释		输入接口的可选说明。
接口类型		选择第 **2** 层。
Netflow 配置文件		如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）可定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
vlan	**Ethernet Interface**（以太网接口）> **Config**（配置）	要启用第 2 层接口之间的切换，或启用通过 VLAN 接口的路由，请选择现有的 VLAN，或单击 **VLAN** 以定义新的 VLAN（请参阅 Network（网络）> VLAN）。选择 **None**（无）可从接口删除当前 VLAN 分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
链接速度	**Ethernet Interface**（以太网接口）> **Advanced**（高级）	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择自动以使防火墙自动确定速度。
链接双工		选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态		选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。

© 2019 Palo Alto Networks, Inc.

第 2 层接口设置	配置位置	说明
启用 LLDP	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **LLDP**	选择此选项可在接口上启用链路层发现协议 (LLDP)。链路层上的 LLDP 功能可发现邻近设备及其功能。
配置文件		如果已启用 LLDP，请选择要分配给接口的 LLDP 配置文件，或单击 **LLDP Profile**（**LLDP** 配置文件）以创建新的配置文件（请参阅 Network（网络）> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件））。选择 **None**（无）可将防火墙配置为使用全局默认值。
在高可用性被动状态中启用		如果已启用 LLDP，请选中此选项以允许 HA 被动防火墙在变为主动前，与其对端设备预先协商 LLDP。

PA-7000 系列第 2 层子接口

- Network（网络）> Interfaces（接口）> Ethernet

对于配置为第 2 层物理接口的每个 Ethernet 端口，您可以为分配给该端口所接收通信的每个 VLAN 标记定义一个附加的第 2 层逻辑接口（子接口）。要启用第 2 层子接口之间的切换，请为这些子接口分配相同的 VLAN 对象。

要配置 PA-7000 系列第 2 层接口，请选中该物理接口所在的行，单击 **Add Subinterface**（添加子接口），然后指定以下信息。

第 2 层子接口设置	说明
接口名称	只读的 Interface Name（接口名称）会显示您所选物理接口的名称。在相邻字段中，输入数字后缀 (1-9,999) 以标识子接口。
注释	输入子接口的可选说明。
标记	输入该子接口的 VLAN 标记 (1-4,094)。
Netflow 配置文件	如果您想要导出从接收子接口遍历到 NetFlow 服务器的单向 IP 流量，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件），以定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从子接口删除当前 NetFlow 服务器分配。
vlan	要启用第 2 层接口之间的切换，或启用通过 VLAN 接口的路由，请选择一个 VLAN，或单击 **VLAN** 以定义新的 VLAN（请参阅 Network（网络）> VLAN）。选择 **None**（无）可从子接口删除当前 VLAN 分配。
虚拟系统	如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于子接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域	选择子接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从子接口删除当前区域分配。

© 2019 Palo Alto Networks, Inc.

PA-7000 系列第 3 层接口

- Network（网络）> Interfaces（接口）> Ethernet

要配置第 3 层接口，请选择接口（例如，ethernet1/1），并指定以下信息。

第 3 层接口设置	配置位置	说明
接口名称	以太网接口	接口名称是预定义的，您不能对其进行更改。
注释		输入接口的可选说明。
接口类型		选择第 **3** 层。
Netflow 配置文件		如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）可定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
虚拟路由器	**Ethernet Interface**（以太网接口）> **Config**（配置）	选择虚拟路由器，或单击 **Virtual Router**（虚拟路由器）以定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
链接速度	**Ethernet Interface**（以太网接口）> **Advanced**（高级）	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择 **auto**（自动）。
链接双工		选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态		选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。
管理配置文件	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **Other Info**（其他信息）	选择配置文件以定义可用来通过该接口管理防火墙的协议（例如，SSH、Telnet 和 HTTP）。选择 **None**（无）可从接口删除当前配置文件分配。
MTU		输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 9,192；默认为 1,500）。如果防火墙两端的机器执行路径 MTU 发现 (PMTUD) 且接口收到的数据包超过 MTU，则防火墙向源端返回 *ICMP fragmentation needed* 消息以表示该数据包太大。
调整 TCP MSS		选择此选项可调整最大分段大小 (MSS) 以容纳任何在接口 MTU 字节大小范围内的标头字节。MTU 字节大小减去 MSS 调整大小即等于 MSS 字节大小，此大小因 IP 协议而异：

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
		• **IPv4 MSS Adjustment Size**（**IPv4 MSS** 调整大小）— 范围为 40 至 300，默认为 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 60 至 300，默认为 60。 使用这些设置可在通过网络的 **tunnel**（隧道）需要更小的 MSS 时，解决相关问题。如果数据包拥有的字节超过没有分片的 MSS，则此设置将启用调整。 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 标记的隧道流量等的字节。
未标记子接口		指定不标记所有属于第 3 层接口的子接口。PAN-OS® 根据数据包目标选择一个未标记子接口作为接收接口。如果目的地是无标记子接口的 IP 地址，可将其映射到子接口。这也意味着数据包必须将其源地址转换为无标记子接口的 IP 地址才能逆向传送。按产品的分类机制是将所有多播和广播数据包分配到基接口，而非任何子接口。由于开放式最短路径优先 (OSPF) 使用多播，因此防火墙在无标记子接口上不支持此功能。
IP 地址 MAC 地址	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **ARP Entries**（**ARP** 条目）	要添加一个或多个静态地址解析协议 (ARP) 条目，请单击 **Add**（添加），然后输入 IP 地址及其关联的硬件 (MAC) 地址。要删除条目，请选择条目，并单击删除。静态 ARP 条目减少 ARP 处理，并且排除指定地址的“中间人”（man-in-the-middle）攻击。
IPv6 地址 MAC 地址	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **ND Entries**（**ND** 条目）	要为邻居发现协议 (NDP) 提供邻居信息，请单击 **Add**（添加），然后输入邻居的 IP 地址和 MAC 地址。
启用 NDP 代理	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **NDP Proxy**（**NDP** 代理）	选中此选项可为接口启用相邻设备发现协议 (NDP) 代理。防火墙将对为该列表中 IPv6 地址请求 MAC 地址的 ND 数据包做出响应。在 ND 响应中，防火墙会针对接口发送它自己的 MAC 地址，以表明它会通过响应发往这些地址的数据包来作为代理。 如果使用了网络前缀转换 IPv6 (NPTv6)，建议您选中启用 **NDP** 代理。 如果已选中 **Enable NDP Proxy**（启用 **NDP** 代理），则可通过输入搜索字符串并单击 Apply Filter（应用过滤器）(→) 对多个地址条目进行过滤。
地址		单击添加可输入一个或多个会将防火墙当作 NDP 代理的 IPv6 地址、IP 范围、IPv6 子网或地址对象。在这些地址中，最好要有一个地址和 NPTv6 中的源转换的地址相同。地址的顺序无关紧要。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
		如果地址所对应的是一个子网络，那么防火墙将针对该子网中的所有地址发送 ND 响应，所以建议您还要添加防火墙的 Ipv6 相邻设备，然后选择 **Negate**（求反）以指示防火墙不要响应这些 IP 地址。
求反		为某个地址选择 **Negate**（求反）可为该地址阻止 NDP 代理。可以对指定 IP 地址范围或 IP 子网的子集进行求反。
启用 LLDP	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **LLDP**	选择此选项可在接口上启用链路层发现协议 (LLDP)。链路层上的 LLDP 功能可发现邻近设备及其功能。
LLDP 配置文件		如果已启用 LLDP，请选择要分配给接口的 LLDP 配置文件，或单击 **LLDP Profile**（**LLDP** 配置文件）以创建新的配置文件（请参阅 Network（网络）> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件））。选择 **None**（无）可将防火墙配置为使用全局默认值。
在高可用性被动状态中启用		如果已启用 LLDP，请选中此选项以允许防火墙在变为主动前，以 HA 被动防火墙身份与其对端设备预先协商 LLDP。
类型	**Ethernet Interface**（以太网接口）> **IPv4**	选择为接口分配 IPv4 地址类型的方法： • 静态 — 您必须手动指定 IP 地址。 • **PPPoE** — 防火墙将使用 Ethernet 上的点对点协议 (PPPoE) 的接口。 • **DHCP** 客户端 — 启用接口作为动态主机配置协议 (DHCP) 客户端并接受动态分配 IP 地址。 防火墙在主动/主动高可用性 *(HA)* 模式下不支持 *PPPoE* 或 *DHCP* 客户端。 该选项卡中显示的选项将因您所选的 IP 地址方法而异。
设置	**Ethernet Interface**（以太网接口）> **Advanced**（高级）> **DDNS**	选择 **Settings**（设置）使 DDNS 字段可进行配置。
启用		在接口上启用 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。）
更新间隔时间（天）		输入防火墙发送至 DDNS 服务器以更新映射到 FQDN 的 IP 地址的更新之间的间隔时间（天）（范围为 1 至 30，默认为 1）。 此外，防火墙还应在接收到 *DHCP* 服务器接口新的 *IP* 地址时更新 *DDNS*。
证书配置文件		创建证书配置文件以验证 DDNS 服务。DDNS 服务可向防火墙提供由证书授权机构(CA)签署的证书。
主机名		输入在 DDNS 服务器上注册的接口主机名（例如，host123.domain123.com 或 host123）。除了确认语法使用 DNS 允许的域名有效字符外，防火墙不得验证主机名。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
供应商		选择向该接口提供 DDNS 的 DDNS 供应商（和版本）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** 如果选择的防火墙指定的旧版本 *DDNS* 服务将在特定日期之后逐步淘汰，请移至新版本。 供应商名称后面的 **Name**（名称）和 **Value**（值）字段是特定于供应商的。您可以通过只读字段知道防火墙用于连接到 DDNS 服务的参数。配置其它字段，例如，DDNS 服务为您提供的密码以及防火墙在未接收到 DDNS 服务器响应时使用的超时。
IPv4 选项卡 — IP		添加接口上配置的 IPv4 地址，然后选中。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
IPv6 选项卡 — IPv6		添加接口上配置的 IPv6 地址，然后选中。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
显示运行时信息		显示 DDNS 注册：DDNS 提供商、已解析的 FQDN 和已映射的 IP 地址（带星号(*)，用于指示主 IP 地址）。每个 DDNS 提供商都有自己的返回代码，用于指示主机名更新状态，以及返回日期，以便进行故障排出。
IPv4 地址类型 = 静态		
IP	**Ethernet Interface**（以太网接口）> **IPv4**	单击添加，然后执行下列步骤之一，以指定接口的静态 IP 地址和网络掩码。 • 以无类别域间路由 (CIDR) 格式键入条目：*ip_address/mask*（掩码）（例如，192.168.2.0/24）。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 单击 **Address**（地址）可创建 **IP netmask**（**IP** 网络掩码）类型的地址对象。 可以为接口输入多个 IP 地址。防火墙使用转发信息库 (FIB) 来确定 IP 地址的最大数。 要删除 IP 地址，请选择地址并单击删除。
IPv4 地址类型 = **PPPoE**		
启用	**Ethernet Interface**（以太网接口）> **IPv4** > **PPPoE** > **General**（常规）	选中此选项可激活此接口的 PPPoE 终端。
用户名		输入用于点对点连接的用户名。
密码/确认密码		输入并确认用户名的密码。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
显示 PPPoE 客户端运行时信息		（可选）打开一个对话框，该对话框会显示防火墙与 Internet 服务提供商 (ISP) 协商用于建立连接的参数。具体的信息取决于 ISP。
身份验证	**Ethernet Interface**（以太网接口）> **IPv4** > **PPPoE** > **Advanced**（高级）	选择用于 PPPoE 通信的身份验证协议。**CHAP**（质询握手身份验证协议）、**PAP**（密码身份验证协议）或默认自动（防火墙确定协议）。选择 **None**（无）可从接口删除当前协议分配。
静态地址		执行下列步骤之一可指定 Internet 服务提供商分配的 IP 地址（无默认值）： • 以无类别域间路由 (CIDR) 格式键入条目：*ip_address/mask*（例如，192.168.2.0/24）。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 单击 **Address**（地址）可创建 **IP netmask**（**IP** 网络掩码）类型的地址对象。 • 选择无可从接口删除当前地址分配。
自动创建指向对端的默认路由		选中此选项可在连接时自动创建指向 PPPoE 对端设备的默认路由。
默认路由跃点数		（可选）对于防火墙与 Internet 服务提供商之间的路由，请输入要与默认路由关联并用于路径选择的路由跃点数（优先级）（范围为 1 至 65,535）。数值越小，优先级越高。
访问集中器		（可选）输入防火墙要连接到的 Internet 服务提供商端访问集中器的名称（无默认值）。
服务		（可选）输入服务字符串（无默认值）。
被动		选中此选项可使用被动模式。在被动模式中，PPPoE 结束点将等待访问集中器发送第一个帧。
IPv4 地址类型 = **DHCP**		
启用	**Ethernet Interface**（以太网接口）> **IPv4**	选择此选项可在接口上激活 DHCP 客户端。
自动创建指向服务器所提供的默认网关的默认路由		选择此选项可自动创建指向 DHCP 服务器提供的默认网关的默认路由。
发送主机名		选中此选项使防火墙（作为 DHCP 客户端）发送接口主机名（选项 12）到 DHCP 服务器。如果发送主机名，则默认将会选择主机名字段中的防火墙主机名。您可以发送该名称或是输入自定义主机名（最多 64 个字符，包括大写字母、小写字母、数字、句点、连字符和下划线）。
默认路由跃点数		对于防火墙与 DHCP 服务器之间的路由，可以输入要与默认路由关联和用于路径选择的路由跃点数（优先级）（范围为 1 至 65,535，无默认值）。数值越小，优先级越高。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
显示 DHCP 客户端运行时信息		选中此选项可显示从 DHCP 服务器收到的所有设置，包括 DHCP 租借状态、动态 IP 地址分配情况、子网掩码、网关、服务器设置（DNS、NTP、域、WINS、NIS、POP3 和 SMTP）。
在接口上启用 IPv6	**Ethernet Interface**（以太网接口）> **IPv6**	选择可在此接口上启用 IPv6 寻址。
接口 ID		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。

地址		单击添加并为每个 IPv6 地址配置以下参数：
		• **Address**（地址）— 输入 IPv6 地址和前缀长度（例如 2001:400:f00::1/64）。您也可以选择现有的 IPv6 地址对象，或单击 **Address**（地址）以创建地址对象。
		• **Enable address on interface**（在接口上启用地址）— 单击可在接口上启用 IPv6 地址。
		• **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）— 选择可将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。
		• **Anycast**（任意播）— 选择以包括通过最近节点的路由。
		• **Send Router Advertisement**（发送路由器通告）— 选中此选项可启用此 IP 地址的路由器通告 (RA)。（您还必须在接口上启用全局 **Enable Router Advertisement**（启用路由器通告）选项。）有关路由器通告的详细信息，请参阅启用路由器通告。
		其余字段只有在启用 RA 后才适用。
		  • **Valid Lifetime**（有效生存时间）— 防火墙认为地址有效的时间长度（秒）。有效生命周期必须等于或超过 **Preferred Lifetime**（首选生命周期）（默认为2,592,000）。
		  • **Preferred Lifetime**（首选生存时间）— 首选的有效地址的时间长度（秒），这意味着防火墙可以用它来发送和接收流量。在首选生命周期到期后，防火墙不能使用此地址来建立新的连接，但在有效生命周期到期（默认为 604,800）之前，任何现有的连接都是有效的。
		  • **On-link**（在链路上）— 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，请选中此选项。
		  • **Autonomous**（自治）— 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，请选择此选项。

启用重复地址检测	**Ethernet Interface**（以太网接口）> **IPv6** > **Address Resolution**（地址解析）	选中此选项可启用重复地址检测 (DAD)，然后配置本部分中的其他字段。
DAD 尝试次数		指定在尝试标识邻居失败之前在邻居请求间隔（**NS Interval**（**NS** 间隔））内的 DAD 尝试次数（范围为 1 至 10，默认为 1）。
可达到时间		指定成功查询和响应之后邻居可继续访问的时间长度（秒）（范围为 10 至 36,000；默认为 30）。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
NS 间隔（邻居请求间隔）		指定在指示失败之前 DAD 尝试的秒数（范围为 1 至 10，默认为 1）。
启用 NDP 监控		选择此选择可启用邻近对象发现协议 (NDP) 监控。启用此功能后， 可选择 NDP Monitor（NDP 监控）（功能列中的 ），然后查看防火墙发现的相邻设备的相关信息，如 IPv6 地址、相应的 MAC 地址和 User-ID（在最理想的情况下）。
启用路由器通告	**Ethernet Interface**（以太网接口）> **IPv6** > **Router Advertisement**（路由器通告）	要在 IPv6 接口上提供无状态地址自动配置 (SLAAC)，请选中此选项，然后配置本部分中的其他字段。IPv6 DNS 客户端使用此信息接收路由器通告 (RA) 消息。 路由器通告将防火墙用作非静态配置的 IPv6 主机的默认防火墙，并向该主机提供用于地址配置的 IPv6 前缀。您可以将独立的 DHCPv6 服务器与此功能结合使用，以向客户端提供 DNS 和其他设置。 这是适用于接口的全局设置。如果您要为单个 IP 地址设置路由器通告选项，请单击 IP 地址表中的 **Add**（添加），然后配置地址。如果您要为任何 IP 地址设置路由器通告，则必须选中接口的启用路由器通告选项。
最小间隔（秒）		指定防火墙将要发送路由器通告之间的最小间隔（秒）（范围为 3 至 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知。
最大间隔（秒）		指定防火墙将要发送路由器通告之间的最大间隔（秒）（范围为 4 至 1,800，默认为 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知。
跃点限制		指定适用于发送数据报的客户端的跃点限制（范围为 1 至 255，默认为 64）。输入 0 表示没有跃点限制。
链接 MTU		指定要应用到客户端的链路最大传输单元 (MTU)。选择 **unspecified**（未指定）表示无链路 MTU（范围为 1,280 至 9,192，默认为未指定）。
可访问时间（毫秒）		指定可访问时间（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邻居的时间。选择 **unspecified**（未指定）表示没有可访问时间值（范围为 0 至 3,600,000，默认为未指定）。
重传时间（毫秒）		指定重传计时器确定客户将在重传邻居请求消息之前将要等待的时间（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，默认为未指定）。
路由器生存时间（秒）		指定客户端将防火墙用作默认网关的时间（范围为 0 至 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。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
路由器首选项		如果网段拥有多个 IPv6 路由器，则客户端会使用此字段来选择首选路由器。选择防火墙路由器相对于网段中的其他路由器认为路由器通告拥有高、中（默认）还是低优先级。
托管配置		选择此选项以向客户端指示可通过 DHCPv6 使用该地址。
一致性检查	**Ethernet Interface**（以太网接口）> **IPv6** > **Router Advertisement (cont)**（路由器通告（续））	如果您希望防火墙验证从其他路由器发出的 RA 是否是正在链路上通告一致信息，请选择此选项。防火墙记录系统日志中的任何不一致；类型为 **ipv6nd**。
其他配置		选择此选项可向客户端指示可通过 DHCPv6 使用其他地址信息（例如，DNS 相关设置）。
路由器通告中包括 DNS 信息	**Ethernet Interface**（以太网接口）> **IPv6** > **DNS Support**（**DNS** 支持）	选中此选项可让防火墙通过此 IPv6 Ethernet 接口以 NDP 路由器通告 (RA) 消息形式发送 DNS 信息。此表中的其他 DNS 支持字段仅在选择此选项后才可见。
服务器		为防火墙 **Add**（添加）一个或多个递归 DNS (RDNS) 服务器地址，以便从此 IPv6 以太网接口发送 NDP 路由器通告中的信息。RDNS 服务器向根 DNS 和权威 DNS 服务器发送一系列 DNS 查找请求，以最终向 DNS 客户端提供 IP 地址。 您最多可以配置八个 RDNS 服务器，防火墙会按从上到下列出的顺序以 NDP 路由器通告形式将这些服务器地址发送给收件人，后者随后会按相同的顺序使用这些地址。选择服务器并 **Move Up**（上移）或 **Move Down**（下移）以更改服务器的顺序，或在不再需要时从列表中 **Delete**（删除）服务器。
生命周期		输入 IPv6 DNS 客户端收到可以使用 RDNS 服务器解析域名的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。
后缀		为 DNS 搜索列表 (DNSSL) **Add**（添加）并配置一个或多个域名（后缀）。最长为 255 个字节。 DNS 搜索列表是在 DNS 查询中输入名称之前 DNS 客户端路由器附加（一次一个）到非限定域名的域后缀列表，从而在 DNS 查询中使用完全限定域名。例如，如果 DNS 客户端尝试提交一个名称为“quality”且没有后缀的 DNS 查询，则路由器会将一个句点和 DNS 搜索列表中的第一个 DNS 后缀附加到该名称中，然后传输此 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，路由器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。在 DNS 查询成功（忽略剩余的后缀）之前或在路由器尝试使用完列表中的所有后缀之前，路由器会一直尝试使用 DNS 后缀。 在邻近对象发现 DNSS 选项中，使用要提供给 DNS 客户端路由器中的后缀配置防火墙；DNS 客户端使用其非限定 DNS 查询中的后缀接收 DNSSL 选项。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	配置位置	说明
		您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的八个 DNS 搜索列表域名（后缀）（按照自上而下列出的顺序），然后按相同的顺序使用这些地址。选择后缀并 **Move Up**（上移）或 **Move Down**（下移）以更改顺序，或在不再需要时 **Delete**（删除）后缀。
生命周期		输入 IPv6 DNS 客户端收到可以使用 DNS 搜索列表中的域名（后缀）的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。

第 3 层接口

- **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）

配置以太网第 3 层接口，您可以将流量路由到该接口。

第 3 层接口设置	说明
接口名称	只读的接口名称字段会显示您所选物理接口的名称。
注释	输入接口的简要说明。
接口类型	选择第 **3** 层。
NetFlow 配置文件	如果您想要导出从接收接口遍历到 NetFlow 服务器的单向 IP 通信，请选择 NetFlow 配置文件或选择 **Netflow Profile**（**Netflow** 配置文件）以创建新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
Config（配置）选项卡	
虚拟路由器	要将虚拟路由器分配给接口，或单击 **Virtual Router**（虚拟路由器）可定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统	如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或选择 **Virtual System**（虚拟系统）以定义新的 vsys。
安全区域	选择接口的安全区域，或选择 **Zone**（区域）以定义新区域。选择 **None**（无）可从接口删除当前区域分配。
IPv4 选项卡	
启用 SD-WAN	选择 **Enable SD-WAN**（启用 **SD-WAN**）即可对以太网接口启用 SD-WAN 功能。
启用 Bonjour Reflector	（仅限 PA-220、PA-800 和 PA-3200 系列）启用此选项后，防火墙将该端口上接收到的 Bonjour 多播通告和查询转发至已启用该选项的所有其他 L3 和 AE 接口和子接口。这样，可确保出于安全或管理目的而使用分段路由流量的网络环境中用户的可访问性和设备的可发现性。您最多可在 16 个接口上启用此选项。
IPv4 Type = Static（**IPv4** 类型为静态）	

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
IP	添加并执行下列步骤之一，以指定接口的静态 IP 地址和网络掩码。 • 以无类别域间路由 (CIDR) 格式键入条目：*ip_address/mask*（例如，192.168.2.0/24）。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 创建 **IP netmask**（**IP** 网络掩码）类型的 **Address**（地址）对象。 可以为接口输入多个 IP 地址。系统使用转发信息库 (FIB) 来确定 IP 地址的最大数。 不再需要时 **Delete**（删除）IP 地址。
SD-WAN 网关	如果选择 **Enable SD-WAN**（启用 **SD-WAN**），请输入 SD-WAN 网关的 IPv4 地址。
IPv4 Type = PPPoE（**IPv4** 类型为 **PPPoE**），**General Tab**（常规选项卡）	
启用	选择 **Enable**（启用）即可激活以太网上的点对点协议 (PPPoE) 终止接口。该接口是指 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。
用户名	输入 ISP 为点对点连接提供的用户名。
密码和确认密码	输入密码并确认密码。
显示 PPPoE 客户端运行时信息	选择以查看有关 PPPoE 接口的信息。
IPv4 Type = PPPoE（**IPv4** 类型为 **PPPoE**），**Advanced**（高级）选项卡	
身份验证	选择身份验证方法： • **None**（无）—（默认）不对 PPPoE 接口进行身份验证。 • **CHAP** — 防火墙对 PPPoE 接口使用质询握手身份验证协议 — RFC-1994。 • **PAP** — 防火墙对 PPPoE 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）— 防火墙与 PPPoE 服务器协商身份验证方法（CHAP 或 PAP）。
静态地址	从 PPPoE 服务器请求所需的 IPv4 地址。PPPoE 服务器可能会分配该地址或其他地址。
自动创建指向对端的默认路由	选择此选项可自动创建指向 PPPoE 服务器提供的默认网关的默认路由。
默认路由跃点数	输入 PPPoE 连接的默认路由跃点数（优先级）（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。
访问集中器	若 ISP 提供了访问集中器的名称，则输入该名称。防火墙将在 IPS 端连接此访问集中器。此字符串值为 0 到 255 个字符。
服务	防火墙（PPPoE 客户端）可以向 PPPoE 服务器提供所需的服务请求。此字符串值为 0 到 255 个字符。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
被动	防火墙（PPPOE 客户端）等待 PPPOE 服务器启动连接。若未启用此选项，则防火墙启动连接。
IPv4 选项卡，Type = DHCP Client（类型为 DHCP 客户端）	
启用	启用接口作为动态主机配置协议 (DHCP) 客户端并接收动态分配 IP 地址。 防火墙在主动/主动高可用性 *(HA)* 模式下不支持 *DHCP* 客户端。
自动创建指向服务器所提供的默认网关的默认路由	勾选此选项以指示防火墙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，该默认网关非常有用。
发送主机名	选择此选项即可分配主机名至 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。
默认路由跃点数	输入防火墙和 DHCP 服务器间路由的默认路由跃点数（优先级）（范围为 1 到 65,535；没有默认跃点数）。数值越小的路由，在路由选择期间的优先级越高。例如，相对于跃点数为 100 的路由，会先使用跃点数为 10 的路由。
显示 DHCP 客户端运行时信息	勾选此选项以查看客户端从其 DHCP 服务器继承的所有设置，包括 DHCP 租借状态、动态 IP 地址分配情况、子网掩码、网关和服务器设置（DNS、NTP、域、WINS、NIS、POP3 和 SMTP）。
IPv6 Tab 选项卡	
在接口上启用 IPv6	选择此项即可在接口上启用 IPv6 寻址。
接口 ID	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。
地址	添加 IPv6 地址和前缀长度（例如 2001:400:f00::1/64）。或者，选择现有的 IPv6 地址对象，或创建新的 IPv6 地址对象。
在接口上启用地址	选择以在接口上启用 IPv6 地址。
使用接口 ID 作为主机部分	选择此项以将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。
任意广播	选择此项以包括通过最近节点的路由。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
发送路由器通告	选择此项以启用此 IP 地址的路由器通告 (RA)。（您还必须在接口上启用全局 **Enable Router Advertisement**（启用路由器通告）选项。）有关 RA 的详细信息，请参阅此表中的启用路由器通告。以下字段仅在您启用路由器通告时才适用： • **Valid Lifetime**（有效生存时间）— 防火墙认为地址有效的时间长度（以秒为单位）。有效生存时间必须等于或超过首选生存时间。默认值为 2,592,000。 • **Preferred Lifetime**（首选生存时间）— 首选有效地址的时间长度（以秒为单位），这意味着防火墙可以用它来发送和接收流量。在首选生存时间到期后，防火墙不能使用地址来建立新的连接，但任何现有的连接仍然有效，直到 **Valid Lifetime**（有效生存时间）到期。默认值为 604,800。 • **On-link**（在链路上）— 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，请选中此选项。 • **Autonomous**（自治）— 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，请选择此选项。
IPv6 选项卡，**Address Resolution**（地址解析）选项卡	
启用重复地址检测	选择此项以启用重复地址检测 (DAD)，然后配置 DAD 尝试次数、可访问时间（秒）和 NS 间隔。
DAD 尝试次数	指定在尝试标识邻居失败之前在邻居请求间隔（**NS Interval**（**NS** 间隔））内的 DAD 尝试次数（范围为 1 至 10，默认为 1）。
可访问时间（秒）	指定成功查询和响应之后邻居可继续访问的时间长度（秒）（范围为 1 至 36,000，默认为 30）。
NS 间隔（秒）	指定在指示失败之前 DAD 尝试的秒数（范围为 1 至 10，默认为 1）。
启用 NDP 监控	选择此选择可启用邻近对象发现协议 (NDP) 监控。启用后，您可以选择 NDP（功能列中的 ）以查看有关防火墙发现的邻近对象的信息（如 IPv6 地址）、相应的 MAC 地址和 User-ID（在最佳情况下）。
IPv6 选项卡，**Router Advertisement**（路由器通告）选项卡	
启用路由器通告	要在 IPv6 接口上提供邻近对象发现功能，请选择并配置本节中的其他字段。IPv6 DNS 客户端使用此信息接收路由器通告 (RA) 消息。 路由器通告将防火墙用作非静态配置的 IPv6 主机的默认防火墙，并向该主机提供用于地址配置的 IPv6 前缀。您可以将独立的 DHCPv6 服务器与此功能结合使用，以向客户端提供 DNS 和其他设置。 这是适用于接口的全局设置。如果要设置各个 IP 地址的路由器通告选项，请在 IP 地址表中 **Add**（添加）并配置 IPv6 地址。如果您要为任何 IPv6 地址设置路由器通告选项，则必须对接口 **Enable Router Advertisement**（启用路由器通告）。
最小间隔（秒）	指定防火墙将要发送路由器通告之间的最小间隔（秒）（范围为 3 至 1,350，默认为 200）。防火墙将会以所配置的最小值和最大值之间的随机间隔时间发送路由器通告。
最大间隔（秒）	指定防火墙将要发送路由器通告之间的最大间隔（秒）（范围为 4 至 1,800，默认为 600）。防火墙将会以所配置的最小值和最大值之间的随机间隔时间发送路由器通告。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
跃点限制	指定要应用于传出数据包的客户端的跃点限制（范围为 1 至 255；默认为 64），或者选择 **unspecified**（未指定），即映射到系统默认值。
链接 MTU	指定要应用到客户端的链路最大传输单位 (MTU)（范围为 1,280 到 1,500），或默认为 **unspecified**（未指定），即映射到系统默认值。
可访问时间（毫秒）	指定可访问时间（以毫秒为单位），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邻居的时间（范围为 0 到 3,600,000），或默认为 **unspecified**（未指定），即映射到系统默认值。
重传时间（毫秒）	指定重新传输计时器以确定客户端在重传邻居请求消息之前将要等待的时间（以毫秒为单位）（范围为 0 到 4,294,967,295 ），或默认为 **unspecified**（未指定），即映射到系统默认值。
路由器生存时间（秒）	指定客户端将防火墙用作默认网关的时间（秒）（范围为 0 至 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。
路由器首选项	如果网段拥有多个 IPv6 路由器，则客户端会使用此字段来选择首选路由器。选择防火墙路由器相对于网段中的其他路由器认为路由器通告拥有高、中（默认）还是低优先级。
托管配置	选择此选项以向客户端指示可通过 DHCPv6 使用该地址。
其他配置	选择此选项可向客户端指示可通过 DHCPv6 使用其他地址信息（例如，DNS 相关设置）。
一致性检查	如果您希望防火墙验证从其他路由器发出的 RA 是否是正在链路上通告一致信息，请选择此选项。防火墙记录系统日志中的任何不一致；类型为 **ipv6nd**。
若在 **Router Advertisement**（路由器通告）选项卡上 **Enable Router Advertisement**（启用路由器通告），则 **DNS Support**（**DNS** 支持）选项卡可用	
路由器通告中包括 DNS 信息	为防火墙选择此选项，以便从此 IPv6 以太网接口发送 NDP 路由器通告中的 DNS 信息。其他 DNS 支持字段（服务器、生命周期、后缀和生命周期）仅在选择此选项后才可见。
服务器	为防火墙 **Add**（添加）一个或多个递归 DNS (RDNS) 服务器地址，以便从此 IPv6 以太网接口发送 NDP 路由器通告中的信息。RDNS 服务器向根 DNS 和权威 DNS 服务器发送一系列 DNS 查找请求，以最终向 DNS 客户端提供 IP 地址。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的八个 RDNS 服务器（按照自上而下列出的顺序），然后按相同的顺序使用这些地址。选择服务器并 **Move Up**（上移）或 **Move Down**（下移）以更改服务器的顺序，或在不再需要时从列表中 **Delete**（删除）服务器。
生命周期	输入 IPv6 DNS 客户端收到路由器通告后，客户端可以使用 RDNS 服务器解析域名之前的最大秒数（范围为 **Max Interval (sec)**（最大间隔（秒））到最大间隔（秒）两倍的值；默认为 1,200）。
后缀	为 DNS 搜索列表 (DNSSL) **Add**（添加）一个或多个域名（后缀）。最长为 255 个字节。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
	DNS 搜索列表是在 DNS 查询中输入名称之前 DNS 客户端路由器附加（一次一个）到非限定域名的域后缀列表，从而在查询中使用完全限定域名。例如，如果 DNS 客户端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”，则路由器生成的查询为完全限定域名“quality.company.com”。 如果 DNS 查询失败，路由器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。路由器使用 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附加该列表中的所有后缀。 在邻近对象发现 DNSS 选项中，使用要提供给 DNS 客户端路由器中的后缀配置防火墙；DNS 客户端使用其非限定 DNS 查询中的后缀接收 DNSSL 选项。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的 8 个 DNS 搜索列表选项域名（后缀）（按照自上而下列出的顺序），然后按相同的顺序使用它们。选择后缀并 **Move Up**（上移）或 **Move Down**（下移）以更改顺序，或在不再需要时 **Delete**（删除）后缀。
生命周期	输入 IPv6 DNS 客户端收到可以使用 DNS 搜索列表中的域名（后缀）的路由器通告后的最大秒数（范围为 **Max Interval (sec)**（最大间隔（秒））到最大间隔（秒）两倍的值；默认为 1,200）。
SD-WAN 选项卡	
SD-WAN 接口状态	若在 **IPv4** 选项卡上选择了 **Enable SD-WAN**（启用 **SD-WAN**），则防火墙会指示 `SD-WAN 接口状态：Enabled`（已启用）。如果未 **Enable SD-WAN**（启用 **SD-WAN**），将显示 `Disabled`（已禁用）。
SD-WAN 接口配置文件	选择 SD-WAN 接口配置文件应用到该以太网接口，或者添加一个新的 SD-WAN 接口配置文件。 您必须先对接口 *Enable SD-WAN*（启用 *SD-WAN*），然后才能应用 *SD-WAN* 接口配置文件。
上游 NAT	如果 SD-WAN 中心或分支位于执行 NAT 的设备下游，则为该中心或分支 **Enable**（启用）上游 NAT。
NAT IP 地址类型	选择 IP 地址分配类型，并指定执行 NAT 设备的面向公众接口的 IP 地址或 FQDN，或指定该 DDNS 派生的地址。这样，自动 VPN 就能将该地址用作中心或分支的隧道端点。 • **Static IP**（静态 **IP**）— 选择 **Type**（类型）为 **IP Address**（**IP** 地址）或 **FQDN**，并输入 IPv4 地址或 FQDN。 • **DDNS**—动态 DNS (DDNS) 派生上游 NAT 设备的 IP 地址。
高级选项卡	
链接速度	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择 **auto**（自动）。
链接双工	选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态	选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
Advanced（高级）选项卡。**Other Info**（其他信息）选项卡	
管理配置文件	选择配置文件以定义可用来通过该接口管理防火墙的协议（例如，SSH、Telnet 和 HTTP）。选择 **None**（无）可从接口删除当前配置文件分配。
MTU	输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 9,192，默认为 1,500）。如果防火墙两端的机器执行路径 MTU 发现 (PMTUD) 且接口收到的数据包超过 MTU，则防火墙向源端返回 *ICMP fragmentation needed* 消息以表示该数据包太大。
调整 TCP MSS	选择此选项可调整最大分段大小 (MSS) 以容纳任何在接口 MTU 字节大小范围内的标头字节。MTU 字节大小减去 MSS 调整大小即等于 MSS 字节大小，此大小因 IP 协议而异： • **IPv4 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 40 至 300，默认为 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 60 至 300，默认为 60。 使用这些设置可在通过网络的 **tunnel**（隧道）需要更小的 MSS 时，解决相关问题。如果数据包拥有的字节超过没有分片的 MSS，则此设置将启用调整。 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。
未标记子接口	若未标记该接口的相应子接口，则选择此选项。
Advanced（高级）选项卡，**ARP Entries**（**ARP** 条目）选项卡	
IP 地址 MAC 地址	要添加一个或多个静态地址解析协议 (ARP) 条目，请 **Add**（添加）IP 地址及其关联的硬件 [介质访问控制 (MAC)] 地址。要删除条目，请选择条目，并单击删除。静态 ARP 条目减少 ARP 处理。
Advanced（高级）选项卡，**ND Entries**（**ND** 条目）选项卡	
IPv6 地址 MAC 地址	要为邻居发现协议 (NDP) 提供邻居信息，请 **Add**（添加）邻居的 IPv6 地址和 MAC 地址。
Advanced（高级）选项卡，**NDP Proxy**（**NDP** 代理）选项卡	
启用 NDP 代理	为接口启用邻居发现协议 (NDP) 代理。防火墙将对为该列表中 IPv6 地址请求 MAC 地址的 ND 数据包做出响应。在 ND 响应中，防火墙会针对接口发送它自己的 MAC 地址，以便防火墙接收对列表中的地址有意义的数据包。 如果正在使用网络前缀转换 IPv6 (NPTv6)，建议您启用 NDP 代理。 如果选择 **Enable NDP Proxy**（启用 **NDP** 代理），则可以输入过滤器并单击 Apply Filter（应用过滤器）（灰色箭头），以便对大量 **Address**（地址）条目进行过滤。
地址	**Add**（添加）一个或多个会将防火墙当作 NDP 代理的 IPv6 地址、IP 范围、IPv6 子网或地址对象。在这些地址中，最好要有一个地址和 NPTv6 中的源转换的地址相同。地址的顺序无关紧要。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
	如果地址所对应的是一个子网络，那么防火墙将针对该子网中的所有地址发送 ND 响应，所以建议您还要添加防火墙的 IPv6 邻居，然后单击 **Negate**（求反）以指示防火墙不要响应这些 IP 地址。
求反	对某个地址进行 **Negate**（求反）可为该地址防止 NDP 代理。可以对指定 IP 地址范围或 IP 子网的子集进行求反。
Advanced（高级）选项卡，**LLDP** 选项卡	
启用 LLDP	对接口启用链路层发现协议 (LLDP)。LLDP 在链路层起作用，可通过与邻居之间收发 LLDP 数据单元来发现邻居设备及其功能。
LLDP 配置文件	选择 LLDP 配置文件或者创建新的 LLDP 配置文件。该配置文件即是您在配置 LLDP 模式、启用 syslog 和 SNMP 通知以及配置想传输到 LLDP 对端的可选类型长度值 (TLV) 时所采用的方式。
Advanced（高级）选项卡，**DDNS Tab**（**DDNS** 选项卡）	
设置	选择 **Settings**（设置）使 DDNS 字段可进行配置。
启用	在接口上启用 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。）
更新间隔时间（天）	输入防火墙发送至 DDNS 服务器以更新映射到 FQDN 的 IP 地址的更新之间的间隔时间（天）（范围为 1 至 30，默认为 1）。 此外，防火墙还应在接收到 *DHCP* 服务器接口新的 *IP* 地址时更新 *DDNS*。
证书配置文件	创建证书配置文件以验证 DDNS 服务。DDNS 服务可向防火墙提供由证书授权机构(CA)签署的证书。
主机名	输入在 DDNS 服务器上注册的接口主机名（例如，host123.domain123.com 或 host123）。除了确认语法使用 DNS 允许的域名有效字符外，防火墙不得验证主机名。
供应商	选择向该接口提供 DDNS 的 DDNS 供应商（和版本）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1** • **No-IP v1** • （PAN-OS 10.0.3 以及 10.0 更高版本）**Palo Alto Networks DDNS**（仅适用于带 DDNS 的全网状 SD-WAN ） 如果选择的防火墙指定的旧版本 *DDNS* 服务将在特定日期之后逐步淘汰，请移至新版本。

© 2019 Palo Alto Networks, Inc.

第 3 层接口设置	说明
	供应商名称后面的 **Name**（名称）和 **Value**（值）字段是特定于供应商的。您可以通过只读字段知道防火墙用于连接到 DDNS 服务的参数。配置其它字段，例如，DDNS 服务为您提供的密码以及防火墙在未接收到 DDNS 服务器响应时使用的超时。
IPv4 选项卡	添加接口上配置的 IPv4 地址，然后选中。您只能选择 DDNS 提供商允许的 IPv4 地址数。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
IPv6 Tab 选项卡	添加接口上配置的 IPv6 地址，然后选中。您只能选择 DDNS 提供商允许的 IPv6 地址数。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
显示运行时信息	显示 DDNS 注册：DDNS 提供商、已解析的 FQDN 和已映射的 IP 地址（带星号(*)，用于指示主 IP 地址）。每个 DDNS 提供商都有自己的返回代码，用于指示主机名更新状态，以及返回日期，以便进行故障排出。

第 3 层子接口

- Network（网络）> Interfaces（接口）> Ethernet

对于已配置为第 3 层物理接口的各个 Ethernet 端口，您可以定义附加的第 3 层逻辑接口（子接口）。

要配置 PA-7000 系列第 3 层接口，请选中该物理接口，单击 **Add Subinterface**（添加子接口），然后指定以下信息。

第 3 层子接口设置	配置位置	说明
接口名称	第 **3** 层子接口	只读的接口名称字段会显示您所选物理接口的名称。在相邻字段中，输入数字后缀（1 至 9,999）以标识子接口。
注释		输入子接口的可选说明。
标记		输入该子接口的 VLAN 标记（1 至4,094）。
Netflow 配置文件		如果您想要导出从接收子接口遍历到 NetFlow 服务器的单向 IP 流量，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件），以定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从子接口删除当前 NetFlow 服务器分配。
虚拟路由器	**Layer3 Subinterface**（第 **3** 层子接口）> **Config**（配置）	要将虚拟路由器分配给接口，或单击 **Virtual Router**（虚拟路由器）可定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于子接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择子接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从子接口删除当前区域分配。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
类型	**Layer3 Subinterface > IPv4**	选择为子接口分配 IPv4 地址类型的方法： • 静态 — 您必须手动指定 IP 地址。 • **DHCP** 客户端 — 启用子接口作为动态主机配置协议 (DHCP) 客户端并接受动态分配 IP 地址。 防火墙在主动/主动高可用性 *(HA)* 模式下不支持 *DHCP* 客户端。 该选项卡中显示的选项将因您所选的 IP 地址方法而异。
启用 Bonjour Reflector	**Layer3 Subinterface > IPv4**	（仅限 PA-220、PA-800 和 PA-3200 系列）启用此选项后，防火墙将该端口上接收到的 Bonjour 多播通告和查询转发至已启用该选项的所有其他 L3 和 AE 接口和子接口。这样，可确保出于安全或管理目的而使用分段路由流量的网络环境中用户的可访问性和设备的可发现性。您最多可在 16 个接口上启用此选项。
IP	**Layer3 Subinterface**（第 3 层子接口）**> IPv4, Type = Static**（**IPv4**，类型 = 静态）	**Add**（添加）并执行下列步骤之一，以指定接口的静态 IP 地址和网络掩码。 • 以无类别域间路由 (CIDR) 格式键入条目：*ip_address/mask*（例如，192.168.2.0/24）。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 创建 **IP netmask**（**IP** 网络掩码）类型的 **Address**（地址）对象。 可以为接口输入多个 IP 地址。系统使用转发信息库 (FIB) 来确定 IP 地址的最大数。 不再需要时 **Delete**（删除）IP 地址。
启用	**Layer3 Subinterface**（第 3 层子接口）**> IPv4, Type = DHCP**（**IPv4**，类型 = **DHCP**）	选择此选项可在接口上激活 DHCP 客户端。
自动创建指向服务器所提供的默认网关的默认路由		选择此选项可自动创建指向 DHCP 服务器提供的默认网关的默认路由。
发送主机名		选中此选项使防火墙（作为 DHCP 客户端）发送接口主机名（选项 12）到 DHCP 服务器。如果默认情况下发送主机名，则默认将会选择主机名字段中的防火墙主机名。您可以发送该名称或是输入自定义主机名（最多 64 个字符，包括大写字母、小写字母、数字、句点、连字符和下划线）。
默认路由跃点数		（可选）对于防火墙与 DHCP 服务器之间的路由，可以输入要与默认路由关联和用于路径选择（范围为 1 至 65535，无默认值）的路由跃点数（优先级）。数值越小，优先级越高。
显示 DHCP 客户端运行时信息		选择 **Show DHCP Client Runtime Info**（显示 **DHCP** 客户端运行时信息）可显示从 DHCP 服务器收到的所有设置，包括 DHCP 租借状态、动态 IP 地址分配、子网掩码、网关和服务器设置（DNS、NTP、域、WINS、NIS、POP3 和 SMTP）。
在接口上启用 IPv6	**Layer3 Subinterface**（第	选择可在此接口上启用 IPv6 寻址。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
接口 ID	**3** 层子接口 ）> **IPv6**	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。

地址		单击添加并为每个 IPv6 地址配置以下参数：
		• **Address**（地址）— 输入 IPv6 地址和前缀长度（例如 2001:400:f00::1/64）。您也可以选择现有的 IPv6 地址对象，或单击 **Address**（地址）以创建地址对象。
		• **Enable address on interface**（在接口上启用地址）— 单击可在接口上启用 IPv6 地址。
		• **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）— 选择可将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。
		• **Anycast**（任意播）— 选择以包括通过最近节点的路由。
		• **Send Router Advertisement**（发送路由器通告）— 选中此选项可启用此 IP 地址的路由器通告 (RA)。（您还必须在接口上启用全局 **Enable Router Advertisement**（启用路由器通告）选项。）有关路由器通告的详细信息，请参阅此表中的启用路由器通告。
		其余字段只有在启用 RA 后才适用。
		  • **Valid Lifetime**（有效生存时间）— 防火墙认为地址有效的时间长度（秒）。有效生存时间必须等于或超过首选生存时间。默认值为 2,592,000。
		  • **Preferred Lifetime**（首选生存时间）— 首选的有效地址的时间长度（秒），这意味着防火墙可以用它来发送和接收流量。在首选生存时间到期后，防火墙不能使用地址来建立新的连接，但任何现有的连接仍然有效，直到有效生存时间到期。默认值为 604,800。
		  • **On-link**（在链路上）— 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，请选中此选项。
		  • **Autonomous**（自治）— 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，请选择此选项。

启用重复地址检测	**Layer3 Subinterface**（第 **3** 层子接口 ）> **IPv6** > **Address Resolution**（地址解析）	选中此选项可启用重复地址检测 (DAD)，然后配置本部分中的其他字段。
DAD 尝试次数		指定在尝试标识邻居失败之前在邻居请求间隔（**NS Interval**（**NS** 间隔））内的 DAD 尝试次数（范围为 1 至 10，默认为 1）。
可达到时间		指定成功查询和响应之后邻居可继续访问的时间长度（秒）（范围为 1 至 36,000，默认为 30）。
NS 间隔（邻居请求间隔）		指定在指示失败之前 DAD 尝试的秒数（范围为 1 至 10，默认为 1）。
启用 NDP 监控		选择此选择可启用邻近对象发现协议 (NDP) 监控。启用后，您可以选择 NDP（功能列中的 ）以查看有关发现的邻近防火墙的信息（如 IPv6 地址）、相应的 MAC 地址和 User-ID（在最佳情况下）。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
启用路由器通告	**Layer3 Subinterface**（第 3 层子接口）> **IPv6** > **Router Advertisement**（路由器通告）	要在 IPv6 接口上提供邻近对象发现功能，请选择并配置本节中的其他字段。IPv6 DNS 客户端使用此信息接收路由器通告 (RA) 消息。 路由器通告将防火墙用作非静态配置的 IPv6 主机的默认防火墙，并向该主机提供用于地址配置的 IPv6 前缀。您可以将独立的 DHCPv6 服务器与此功能结合使用，以向客户端提供 DNS 和其他设置。 这是适用于接口的全局设置。如果要设置单个 IP 地址的路由器通告选项，请在 IP 地址表中 **Add**（添加）并配置地址。如果您要为任何 IP 地址设置路由器通告选项，必须选择接口的 **Enable Router Advertisement**（启用路由器通告）选项。
最小间隔（秒）		指定防火墙将要发送路由器通告之间的最小间隔（秒）（范围为 3 至 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知。
最大间隔（秒）		指定防火墙将要发送路由器通告之间的最大间隔（秒）（范围为 4 至 1,800，默认为 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知。
跃点限制		指定适用于发送数据报的客户端的跃点限制（范围为 1 至 255，默认为 64）。输入 0 表示没有跃点限制。
链接 MTU		指定要应用到客户端的链路最大传输单元 (MTU)。选择 **unspecified**（未指定）表示无链路 MTU（范围为 1,280 至 9,192，默认为未指定）。
可访问时间（毫秒）		指定可访问时间（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邻居的时间。选择 **unspecified**（未指定）表示没有可访问时间值（范围为 0 至 3,600,000，默认为未指定）。
重传时间（毫秒）		指定重传计时器确定客户将在重传邻居请求消息之前将要等待的时间（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，默认为未指定）。
路由器生存时间（秒）		指定客户端将防火墙用作默认网关的时间（秒）（范围为 0 至 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。
路由器首选项		如果网段拥有多个 IPv6 路由器，则客户端会使用此字段来选择首选路由器。选择防火墙路由器相对于网段中的其他路由器认为路由器通告拥有高、中（默认）还是低优先级。
托管配置		选择此选项以向客户端指示可通过 DHCPv6 使用该地址。
其他配置		选择此选项可向客户端指示可通过 DHCPv6 使用其他地址信息（例如，DNS 相关设置）。
一致性检查	**Layer3 Subinterface**（第 3 层子接口）>	如果您希望防火墙验证从其他路由器发出的 RA 是否是正在链路上通告一致信息，请选择此选项。防火墙记录系统日志中的任何不一致；类型为 **ipv6nd**。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
	IPv6 > Router Advertisement (cont)（路由器通告（续））	
路由器通告中包括 DNS 信息	**Layer3 Subinterface**（第 3 层子接口）**> IPv6 > DNS Support**（**DNS** 支持）	为防火墙选择此选项，以便从此 IPv6 以太网子接口发送 NDP 路由器通告中的 DNS 信息。此表中的其他 DNS 支持字段仅在选择此选项后才可见。
服务器		为防火墙 **Add**（添加）一个或多个递归 DNS (RDNS) 服务器地址，以便从此 IPv6 以太网接口发送 NDP 路由器通告中的信息。RDNS 服务器向根 DNS 和权威 DNS 服务器发送一系列 DNS 查找请求，以最终向 DNS 客户端提供 IP 地址。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的 8 个 RDNS 服务器（按照自上而下列出的顺序），然后按相同的顺序使用这些地址。选择服务器并 **Move Up**（上移）或 **Move Down**（下移）以更改服务器的顺序，或在不再需要时从列表中 **Delete**（删除）服务器。
生命周期		输入 IPv6 DNS 客户端收到可以使用 RDNS 服务器解析域名的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。
后缀	**Layer3 Subinterface**（第 3 层子接口）**> IPv6 > DNS Support**（**DNS** 支持）（续）	为 DNS 搜索列表 (DNSSL) **Add**（添加）一个或多个域名（后缀）。最长为 255 个字节。 DNS 搜索列表是在 DNS 查询中输入名称之前 DNS 客户端路由器附加（一次一个）到非限定域名的域后缀列表，从而在查询中使用完全限定域名。例如，如果 DNS 客户端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”，则路由器生成的查询为完全限定域名“quality.company.com”。 如果 DNS 查询失败，路由器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。路由器使用 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附加该列表中的所有后缀。 在邻近对象发现 DNSS 选项中，使用要提供给 DNS 客户端路由器中的后缀配置防火墙；DNS 客户端使用其非限定 DNS 查询中的后缀接收 DNSSL 选项。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的 8 个 DNS 搜索列表选项域名（后缀）（按照自上而下列出的顺序），然后按相同的顺序使用它们。选择后缀并 **Move Up**（上移）或 **Move Down**（下移）以更改顺序，或在不再需要时 **Delete**（删除）后缀。
生命周期	**Layer3 Subinterface**（第 3 层子接口）**> IPv6 > DNS**	输入 IPv6 DNS 客户端收到可以使用 DNS 搜索列表中的域名（后缀）的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
	Support（**DNS** 支持）（续）	
管理配置文件	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **Other Info**（其他信息）	管理配置文件 — 选择配置文件以定义可用来通过该接口管理防火墙的协议（例如，SSH、Telnet 和 HTTP）。选择 **None**（无）可从接口删除当前配置文件分配。
MTU		输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 9,192，默认为 1,500）。如果防火墙两端的机器执行路径 MTU 发现 (PMTUD) 且接口收到的数据包超过 MTU，则防火墙向源端返回 *ICMP fragmentation needed* 消息以表示该数据包太大。
调整 TCP MSS	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **Other Info**（其他信息）	选择此选项可调整最大分段大小 (MSS) 以容纳任何在接口 MTU 字节大小范围内的标头字节。MTU 字节大小减去 MSS 调整大小即等于 MSS 字节大小，此大小因 IP 协议而异： • **IPv4 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 40 至 300，默认为 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 60 至 300，默认为 60。 使用这些设置可在通过网络的 **tunnel**（隧道）需要更小的 MSS 时，解决相关问题。如果数据包拥有的字节超过没有分片的 MSS，则此设置将启用调整。 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。
IP 地址 MAC 地址	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **ARP Entries**（**ARP** 条目）	要添加一个或多个静态地址解析协议 (ARP) 条目，请 **Add**（添加）IP 地址及其关联的硬件 [介质访问控制 (MAC)] 地址。要删除条目，请选择条目，并单击删除。静态 ARP 条目减少 ARP 处理。
IPv6 地址 MAC 地址	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **ND Entries**（**ND** 条目）	要为邻居发现协议 (NDP) 提供邻居信息，请 **Add**（添加）邻居的 IP 地址和 MAC 地址。
启用 NDP 代理	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **NDP Proxy**（**NDP** 代理）	为接口启用邻居发现协议 (NDP) 代理。防火墙将对为该列表中 IPv6 地址请求 MAC 地址的 ND 数据包做出响应。在 ND 响应中，防火墙会针对接口发送它自己的 MAC 地址，以便防火墙接收对列表中的地址有意义的数据包。 如果正在使用网络前缀转换 IPv6 (NPTv6)，建议您启用 NDP 代理。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
		如果选择 **Enable NDP Proxy**（启用 **NDP** 代理），则可以输入过滤器并单击 Apply Filter（应用过滤器）（灰色箭头），以便对大量 **Address**（地址）条目进行过滤。
地址		**Add**（添加）一个或多个会将防火墙当作 NDP 代理的 IPv6 地址、IP 范围、IPv6 子网或地址对象。在这些地址中，最好要有一个地址和 NPTv6 中的源转换的地址相同。地址的顺序无关紧要。 如果地址所对应的是一个子网络，那么防火墙将针对该子网中的所有地址发送 ND 响应，所以建议您还要添加防火墙的 IPv6 邻居，然后单击 **Negate**（求反）以指示防火墙不要响应这些 IP 地址。
求反		对某个地址进行 **Negate**（求反）可为该地址防止 NDP 代理。可以对指定 IP 地址范围或 IP 子网的子集进行求反。
设置	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **DDNS**	选择 **Settings**（设置）使 DDNS 字段可进行配置。
启用		在接口上启用 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。）
更新间隔时间（天）	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **DDNS**	输入防火墙发送至 DDNS 服务器以更新映射到 FQDN 的 IP 地址的更新之间的间隔时间（天）（范围为 1 至 30，默认为 1）。 此外，防火墙还应在接收到 *DHCP* 服务器接口新的 *IP* 地址时更新 *DDNS*。
证书配置文件		创建证书配置文件以验证 DDNS 服务。DDNS 服务可向防火墙提供由证书授权机构(CA)签署的证书。
主机名		输入在 DDNS 服务器上注册的接口主机名（例如，host123.domain123.com 或 host123）。除了确认语法使用 DNS 允许的域名有效字符外，防火墙不得验证主机名。
供应商	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **DDNS**	选择向该接口提供 DDNS 的 DDNS 供应商（和版本）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** 如果选择的防火墙指定的旧版本 *DDNS* 服务将在特定日期之后逐步淘汰，请移至新版本。 供应商名称后面的 **Name**（名称）和 **Value**（值）字段是特定于供应商的。您可以通过只读字段知道防火墙用于连接到 DDNS 服务的参数。配置其它字段，例如，DDNS 服务为您提供的密码以及防火墙在未接收到 DDNS 服务器响应时使用的超时。

© 2019 Palo Alto Networks, Inc.

第 3 层子接口设置	配置位置	说明
IPv4 选项卡 — IP		添加接口上配置的 IPv4 地址，然后选中。您只能选择 DDNS 提供商允许的 IPv4 地址数。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
IPv6 选项卡 — IP		添加接口上配置的 IPv6 地址，然后选中。您只能选择 DDNS 提供商允许的 IPv6 地址数。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
显示运行时信息	**Layer3 Subinterface**（第 3 层子接口）> **Advanced**（高级）> **DDNS**	显示 DDNS 注册：DDNS 提供商、已解析的 FQDN 和已映射的 IP 地址（带星号(*)，用于指示主 IP 地址）。每个 DDNS 提供商都有自己的返回代码，用于指示主机名更新状态，以及返回日期，以便进行故障排出。

日志卡接口

- Network（网络）> Interfaces（接口）> Ethernet

如果在 PA-7000 系列防火墙上通过日志处理卡(LPC)配置日志转发，必须将一个数据端口配置为 **Log Card**（日志卡）类型。这是因为此防火墙型号的流量和日志记录功能超出了管理 (MGT) 接口的功能。日志卡数据端口会为 syslog、电子邮件、简单网络管理协议 (SNMP)、Panorama 日志转发和 WildFire™ 文件转发进行日志转发。

只能将防火墙上的一个端口设置为 *Log Card*（日志卡）类型。如果启用日志转发，但不将接口配置为 *Log Card*（日志卡）类型，则在尝试提交更改时可能会发生错误。

要配置日志卡接口，请选择未配置的接口（如 ethernet1/16），并按下表所述配置设置。

日志卡接口设置	配置位置	说明
插槽	以太网接口	选择接口的插槽号 (1-12)。
接口名称		接口名称是预定义的，您不能对其进行更改。
注释		输入接口的可选说明。
接口类型		选择日志卡。
IPv4	**Ethernet Interface**（以太网接口）> **Log Card Forwarding**（日志卡转发）	如果网络使用的是 IPv4，请定义以下各项： • **IP** 地址 — 端口的 IPv4 地址。 • **Netmask**（网络掩码）— 端口的 IPv4 地址的网络掩码。 • 默认网关 — 端口的默认网关的 IPv4 地址。
IPv6		如果网络使用的是 IPv6，请定义以下各项： • **IP** 地址 — 端口的 IPv6 地址。 • 默认网关 — 端口的默认网关的 IPv6 地址。

© 2019 Palo Alto Networks, Inc.

日志卡接口设置	配置位置	说明
链接速度	**Ethernet Interface**（以太网接口）> **Advanced**（高级）	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择 **auto**（自动）以使防火墙根据连接来自动确定速度。对于速度不可配置的接口，**auto**（自动）是唯一选项。 针对连接推荐的最小速度为 *1000 (Mbps)*。
链接双工		选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是根据连接自动协商 (**auto**)。默认值是 **auto**（自动）。
链接状态		选择接口状态为启用 (**up**)、禁用 (**down**) 还是根据连接自动确定 (**auto**)。默认值是 **auto**（自动）。

日志卡子接口

- Network（网络）> Interfaces（接口）> Ethernet

要添加 日志卡接口，请选择该接口所在的行，单击 **Add Subinterface**（添加子接口），然后指定以下信息。

日志卡子接口设置	配置位置	说明
接口名称	**LPC** 子接口	只读的 **Interface Name**（接口名称）会显示您所选日志卡接口的名称。在相邻字段中，输入数字后缀 (1-9,999) 以标识子接口。
注释		输入接口的可选说明。
标记		输入该子接口的 VLAN **Tag**（标记）(0-4,094)。 为了便于使用，将该标记与子接口编号保持一致。
虚拟系统	**LPC Subinterface**（**LPC** 子接口）> **Config**（配置）	选择日志处理卡 (LPC) 子接口被分配至的虚拟系统 (vsys)。或者，您可以单击 **Virtual Systems**（虚拟系统）以添加新的 vsys。在将 LPC 子接口分配给某个 vsys 后，该接口会用作从日志卡转发日志（syslog、电子邮件、SNMP）的所有服务的源接口。
IPv4	**Ethernet Interface**（以太网接口）> **Log Card Forwarding**（日志卡转发）	如果网络使用的是 IPv4，请定义以下各项： • **IP** 地址 — 端口的 IPv4 地址。 • **Netmask**（网络掩码）— 端口的 IPv4 地址的网络掩码。 • 默认网关 — 端口的默认网关的 IPv4 地址。
IPv6		如果网络使用的是 IPv6，请定义以下各项： • **IP** 地址 — 端口的 IPv6 地址。 • 默认网关 — 端口的默认网关的 IPv6 地址。

© 2019 Palo Alto Networks, Inc.

解密镜像接口

- Network（网络）> Interfaces（接口）> Ethernet

要使用解密端口镜像功能，必须选择解密镜像接口类型。此功能可以创建来自防火墙的已解密流量的副本，并且将其发送到能够接收原始数据包捕获（如 NetWitness 或 Solera）的流量收集工具以用于存档和分析。对于需要用于取证和历史研究目的的全面数据捕获和数据遗失防护 (DLP) 功能的企业而言，此功能是必需的。要启用此功能，必须获取和安装免费许可证。

VM 系列没有适用于公共云平台（AWS、Azure、Google Cloud Platform）、VMware NSX 和 Citrix SDX 的解密端口镜像功能。

要配置解密镜像接口，请单击还未配置的接口的名称（例如，ethernet1/1），并指定以下信息。

解密镜像接口设置	说明
接口名称	接口名称是预定义的，您不能对其进行更改。
注释	输入接口的可选说明。
接口类型	选择解密镜像。
链接速度	选择接口速度，以 Mbps 为单位（**10**、**100** 或 **1000**），或选择 **auto**（自动）以使防火墙自动确定速度。
链接双工	选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态	选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。

聚合以太网 (AE) 接口组

- Network（网络）> Interfaces（接口）> Ethernet（以太网）> Add Aggregate Group（添加聚合组）

聚合以太网 (AE) 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其他防火墙。AE 接口组将通过平衡各组合接口中的负载流量来增加对端之间的带宽。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。

配置 AE 接口组之前，必须配置 AE 的接口。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（1Gbps、10Gbps、40Gbps 或 100Gbps）和接口类型（HA3、虚拟线路、第 2 层或第 3 层）必须相同。

您可以添加的 AE 接口组数量取决于防火墙型号。产品选择工具指示了每个防火墙型号支持的最大聚合接口数。每个 AE 接口组最多可有 8 个接口。

对于 PA-3200 系列、PA-5200 系列以及大部分 PA-7000 系列防火墙，仅前 8 个 AE 接口组支持 QoS。而带有 PA-7000-100G-NPC-A 和 SMC-B 的 PA-7000 系列防火墙则不包含在内，对于这些防火墙，仅前 16 个 AE 接口组支持 QoS。

除 VM 系列型号外的所有 Palo Alto Networks 防火墙均支持 AE 接口组。

您可在高可用性 (HA) 主动/主动配置中聚合 HA3（数据包转发）接口，但此操作仅适用于以下防火墙型号：

- *PA-220*
- *PA-800 ⋎#*

© 2019 Palo Alto Networks, Inc.

- *PA-3200 系列*
- *PA-5200 系列*

要配置 AE 接口组，请单击 **Add Aggregate Group**（添加聚合组）按下表中所述配置设置，然后将接口分配给组（请参阅聚合以太网 (AE) 接口）。

聚合接口组设置	配置位置	说明
接口名称	聚合以太网接口	只读的 **Interface Name**（接口名称）会设置为 **ae**。在相邻字段中，输入数字后缀以标识 AE 接口组。数字后缀的范围根据防火墙型号支持的 AE 组数量而定。请参阅产品选择工具中各个防火墙型号支持的最大聚合接口数。
注释		（可选）输入接口的说明。
接口类型		选择接口类型，用于控制其余配置要求和选项： • **HA** — 仅当接口为主动/主动部署中的两个防火墙间的 HA3 链路时才选择此选项。或者，选择 **Netflow Profile**（**Netflow** 配置文件），并配置 **LACP** 选项卡中的设置（请参阅启用 LACP）。 • **Virtual Wire**（虚拟线路）—（可选）选择 **Netflow Profile**（**Netflow** 配置文件），并按虚拟线路设置中所述，对 **Config**（配置）和 **Advanced**（高级）选项卡中的设置进行配置。 • **Layer 2**（第 2 层）—（可选）选择 **Netflow Profile**（**Netflow** 配置文件）；按第 2 层接口设置中所述，对 **Config**（配置）和 **Advanced**（高级）选项卡中的设置进行配置；并（可选）配置 **LACP** 选项卡（请参阅启用 LACP）。 • **Layer 3**（第 3 层）—（可选）选择 **Netflow Profile**（**Netflow** 配置文件）；按第 3 层接口设置中所述，对 **Config**（配置）、**IPv4** 或 **IPv6** 和 **Advanced**（高级）选项卡中的设置进行配置；并（可选）配置 **LACP** 选项卡（请参阅启用 LACP）。
Netflow 配置文件		如果您想要导出从接收接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或 **Netflow Profile**（**Netflow** 配置文件），以定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从 AE 接口组删除当前 NetFlow 服务器分配。
启用 LACP	**Aggregate Ethernet Interface**（聚合以太网接口）> **LACP**	如果要为 AE 接口组启用链路聚合控制协议 (LACP)，请选择此选项。在默认情况下禁用 LACP。 如果启用 LACP，则接口故障检测将在物理层和数据链路层自动进行，不论防火墙及其 LACP 对端是否直接连接。（如不启用 LACP，则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。）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（请参阅最大端口数）。
模式		选择防火墙的 LACP 模式。我们建议在任何两个 LACP 对等之间配置一个主动，一个被动。如果两个对端均为被动模式，则 LACP 无法正常运行。 • 被动（默认）— 防火墙被动地对对端的 LACP 状态查询做出响应。 • 主动 — 防火墙主动查询对端的 LACP 状态（可用或无响应）。

© 2019 Palo Alto Networks, Inc.

聚合接口组设置	配置位置	说明
传输速率		选择防火墙与对端交换查询和响应的速率： • 快 — 每一秒 • 慢（默认）— 每 30 秒
快速故障转移		当某个接口出现故障后，如果您希望防火墙在一秒钟内故障转移至操作接口，请选择此选项。否则，以标准 IEEE 802.1AX 定义的速度进行故障转移（至少三秒）。
系统优先级	**Aggregate Ethernet Interface**（聚合以太网接口）> **LACP (cont)**	用于确定防火墙或其对等覆盖对方的端口优先级的数字（参阅下面的最大端口数）。 数字越小，优先级越高（范围为 *1-65,535*，默认为 *32,768*）。
最大端口数		在 LACP 聚合组中可以在任何指定时间启用的接口数（1-8 个）。该值不得超过您分配给组的接口数。如果分配的接口数超过活动接口数，则防火墙使用接口的 LACP 端口优先级来确定处于待机模式的接口。您可以在为组配置单个接口时设置 LACP 端口优先级（请参阅聚合以太网 (AE) 接口）。
在高可用性被动状态中启用		对于部署在 HA 主动/被动配置中的防火墙，请选择此选项以允许被动防火墙在故障转移发生之前，与其主动对等预先协商 LACP。预先协商会加快故障转移，因为被动防火墙无需在变为主动前，协商 LACP。
为主动-被动高可用性模式使用相同的系统 MAC 地址	**Aggregate Ethernet Interface**（聚合以太网接口）> **LACP (cont)**	此选项仅适用于在 HA 主动/被动配置中部署的防火墙；主动/主动配置中的防火墙需要唯一的 MAC 地址。 HA 防火墙对端具有相同的系统优先级值。但是，在主动/被动部署中，每个防火墙的系统 ID 可以是相同或不同，具体取决于您是否分配相同的 MAC 地址。 如果 *LACP* 对端（也在高可用性模式下）已经虚拟化（显示为网络作为一个单一的设备），则对防火墙使用相同的系统 *MAC* 地址可在故障转移期间最大限度减少延迟。如果 *LACP* 对端未虚拟化，则对每个防火墙使用唯一的 *MAC* 地址可最大限度减少故障转移延迟。 LACP 使用 MAC 地址来获得每个 LACP 对端的系统 ID。如果防火墙对和对端对拥有相同的系统优先级值，LACP 会使用系统 ID 值来确定凭借端口优先级覆盖其他对的防火墙对和对端对。如果两个防火墙拥有相同的 MAC 地址，则它们拥有相同的系统 ID，该 ID 可能会比 LACP 对端的系统 ID 更高或更低。如果高可用性防火墙拥有唯一的 MAC 地址，可能一个防火墙拥有比 LACP 对端更高的系统 ID，另一个防火墙拥有比 LACP 对端更低的系统 ID。在后一种情况下，当在防火墙上进行故障转移时，LACP 对端和防火墙之间的端口优先级切换会变成主动。
MAC 地址	**Aggregate Ethernet Interface**（聚合	如果 **Use Same System MAC Address**（使用相同的系统 **MAC** 地址），可以为主动/被动 HA 对中的两个防火墙选择系统生成的 MAC 地址或输入自己的 MAC 地址。您必须验证该地址是否是全局唯一。

© 2019 Palo Alto Networks, Inc.

聚合接口组设置	配置位置	说明
	以太网接口) > **LACP (cont)**	

聚合以太网 (AE) 接口

- Network (网络) > Interfaces (接口) > Ethernet

要配置聚合以太网 (AE) 接口，首先配置聚合以太网 (AE) 接口组，然后单击分配给该组的接口的名称。在分配给任何特定组的接口中，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 (例如，第 3 层) 必须相同。而且，即使在配置每个接口时会将类型更改为 **Aggregate Ethernet** (聚合以太网) ，接口类型也必须与为 AE 接口组定义的接口相同。为分配给组的每个接口指定以下信息。

如果为 *AE* 接口组启用了链路聚合控制协议 *(LACP)*，为该组中的每个接口选择相同的 *Link Speed* (链接速度) 和 *Link Duplex* (链路双工) 。对于非匹配值，提交操作会显示警告且 *PAN-OS* 默认为更高的速度和全双工。

聚合接口设置	配置位置	说明
接口名称	聚合以太网接口	接口名称是预定义的，您不能对其进行更改。
注释		(可选) 输入接口的说明。
接口类型		选择 **Aggregate Ethernet** (聚合以太网) 。
聚合组		将接口分配到聚合组。
链接速度		选择接口速度，以 Mbps 为单位 (**10**、**100** 或 **1000**) ，或选择 **auto** (自动) 以使防火墙自动确定速度。
链接双工		选择接口传输模式为全双工 (**full**)、半双工 (**half**) 还是自动协商 (**auto**)。
链接状态		选择接口状态为启用 (**up**)、禁用 (**down**) 还是自动确定 (**auto**)。
LACP 端口优先级		防火墙只有在为聚合组启用链路聚合控制协议 (LACP) 后才会使用该字段。如果分配给组的接口数超过活动接口数 (最大端口数字段) ，则防火墙使用接口的 LACP 端口优先级来确定处于待机模式的接口。数字越小，优先级越高 (范围为 1-65,535，默认为 32,768) 。
虚拟路由器	**Aggregate Ethernet Interface** (聚合以太网接口) > **Config** (配置)	选择为其分配聚合以太网接口的虚拟路由器。
安全区域		选择为其分配聚合以太网接口的安全区域。
启用 Bonjour Reflector	**Aggregate Ethernet Interface** (聚合以太网接口) > **IPv4**	(仅限 PA-220、PA-800 和 PA-3200 系列) 启用此选项后，防火墙将该端口上接收到的 Bonjour 多播通告和查询转发至已启用该选项的所有其他 L3 和 AE 接口和子接口。这样，可确保出于安全或管理目的而使用分段路由流量的网络环境中用户的可访问性和设备的可发现性。您最多可在 16 个接口上启用此选项。

© 2019 Palo Alto Networks, Inc.

聚合接口设置	配置位置	说明
在接口上启用 IPv6	**Aggregate Ethernet Interface**（聚合以太网接口）> **IPv6**	选择以在此接口上启用 IPv6。
接口 ID		以十六进制格式输入 64 位扩展唯一标识符 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果将此字段留空，则防火墙使用根据物理接口的 MAC 地址生成的 EUI-64。如果在添加地址时启用 **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）选项，则防火墙使用接口 ID 作为该地址的主机部分。

地址		**Add**（添加）IPv6 地址并配置以下参数：
		• **Address**（地址）— 输入 IPv6 地址和前缀长度（如 2001:400:f00::1/64）。您也可以选择现有的 IPv6 地址对象，或单击 **Address**（地址）以创建地址对象。
		• **Enable address on interface**（在接口上启用地址）— 单击可在接口上启用 IPv6 地址。
		• **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）— 选择可将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。
		• **Anycast**（任意播）— 选择以包括通过最近节点的路由。
		• **Send RA**（发送路由器通告）— 选择以启用此 IP 地址的路由器通告 (RA)。如果选择此选项，还必须在接口上全局 **Enable Router Advertisement**（启用路由器通告）。有关路由器通告的详细信息，请参阅启用路由器通告。
		应用的其余字段只有在启用 RA 后才可见。
		  • **Valid Lifetime**（有效生存时间）— 防火墙认为地址有效的时间长度（秒）。有效生存时间必须等于或超过首选生存时间。默认值为 2,592,000。
		  • **Preferred Lifetime**（首选生存时间）— 首选的有效地址的时间长度（秒），这意味着防火墙可以用它来发送和接收流量。在首选生存时间到期后，防火墙不能使用地址来建立新的连接，但任何现有的连接仍然有效，直到超过 **Valid Lifetime**（有效生存时间）。默认值为 604,800。
		  • **On-link**（在链路上）— 如果能在不使用路由器的情况下访问通告前缀中包含 IP 地址的系统，请选择此选项。
		  • **Autonomous**（自治）— 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，请选择此选项。

启用重复地址检测	**Aggregate Ethernet Interface**（聚合以太网接口）> **IPv6** > **Address Resolution**（地址解析）	选择启用重复地址检查 (DAD)，然后可让您指定 **DAD Attempts**（**DAD** 尝试次数）。
DAD 尝试次数		指定在尝试标识邻居失败之前在邻居请求间隔（**NS Interval**（**NS** 间隔））内的 DAD 尝试次数（范围为 1-10，默认为 1）。
可达到时间		指定成功查询和响应之后邻居可继续访问的时间长度（秒）（范围为 1-36,000，默认为 30）。
NS 间隔（邻居请求间隔）		指定在指示失败之前 DAD 尝试的时间长度（秒）（范围为 1-10，默认为 1）。

© 2019 Palo Alto Networks, Inc.

聚合接口设置	配置位置	说明
启用 NDP 监控		选择启用邻近对象发现协议监控。启用后，您可以选择 NDP（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）。
启用路由器通告	**Aggregated Ethernet Interface**（聚合以太网接口）> **IPv6** > **Router Advertisement**（路由器通告）	选择在 Ipv6 接口上提供邻近对象发现功能，并配置本节中的其他字段。IPv6 DNS 客户端使用此信息接收路由器通告 (RA) 消息。 路由器通告将防火墙用作非静态配置的 IPv6 主机的默认防火墙，并向该主机提供用于地址配置的 IPv6 前缀。您可以将独立的 DHCPv6 服务器与此功能结合使用，以向客户端提供 DNS 和其他设置。 这是适用于接口的全局设置。如果要设置单个 IP 地址的路由器通告选项，请在 IP 地址表中 **Add**（添加）并配置地址。如果您要为任何 IP 地址设置路由器通告选项，必须选择接口的 **Enable Router Advertisement**（启用路由器通告）选项。
最小间隔（秒）		指定防火墙将要发送路由器通告之间的最小间隔（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知。
最大间隔（秒）		指定防火墙将要发送路由器通告之间的最大间隔（秒）（范围为 4-1,800，默认为 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知。
跃点限制		指定适用于发送数据报的客户端的跃点限制（范围为 1-255，默认为 64）。输入 **0** 表示没有跃点限制。
链接 MTU		指定要应用到客户端的链路最大传输单元 (MTU)。选择 **unspecified**（未指定）表示无链路 MTU（范围为 1,280-9,192，默认为未指定）。
可访问时间（毫秒）		指定可访问时间（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 0-3,600,000，默认为未指定）。
重传时间（毫秒）		指定重传计时器确定客户将在重传邻居请求消息之前将要等待的时间（毫秒）。选择 **unspecified**（未指定）表示没有重传时间（范围为 0-4,294,967,295，默认为未指定）。
路由器生存时间（秒）		指定客户端将防火墙用作默认网关的时间（秒）（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。
路由器首选项		如果网段拥有多个 IPv6 路由器，则客户端会使用此字段来选择首选路由器。选择防火墙路由器相对于网段中的其他路由器认为路由器通告拥有高、中（默认）还是低优先级。
托管配置		选择此选项以向客户端指示可通过 DHCPv6 使用该地址。
其他配置		选中此选项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）。

© 2019 Palo Alto Networks, Inc.

聚合接口设置	配置位置	说明
一致性检查	**Aggregated Ethernet Interface**（聚合以太网接口）> **IPv6** > **Router Advertisement (cont)**（路由器通告）（续）	如果您希望防火墙验证从其他路由器发出的 RA 是否是正在链路上通告一致信息，请选择此选项。防火墙记录系统日志中的任何不一致；类型为 **ipv6nd**。
路由器通告中包括 DNS 信息	**Aggregated Ethernet Interface**（聚合以太网接口）> **IPv6** > **DNS Support**（**DNS** 支持）	为防火墙选择此选项，以便从此 IPv6 聚合以太网接口发送 NDP 路由器通告 (RA) 消息中的 DNS 信息。此表中的其他 DNS 支持字段仅在选择此选项后才可见。
服务器		为防火墙 **Add**（添加）一个或多个递归 DNS (RDNS) 服务器地址，以便从此 IPv6 聚合以太网接口发送 NDP 路由器通告中的信息。RDNS 服务器向根 DNS 服务器和权威 DNS 服务器发送一系列 DNS 查找请求，以最终向 DNS 客户端提供 IP 地址。 您最多可以配置八个 RDNS 服务器，防火墙会按从上到下列出的顺序以 NDP 路由器通告形式将这些服务器地址发送给收件人，后者随后会按相同的顺序使用这些地址。选择服务器并 **Move Up**（上移）或 **Move Down**（下移）以更改服务器的顺序，或在不再需要时 **Delete**（删除）服务器。
生命周期		输入 IPv6 DNS 客户端收到可以使用 RDNS 服务器解析域名的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。
后缀		为 DNS 搜索列表 (DNSSL) **Add**（添加）并配置一个或多个域名（后缀）。最大后缀长度为 255 个字节。 DNS 搜索列表是在 DNS 查询中输入名称之前 DNS 客户端路由器附加（一次一个）到非限定域名的域后缀列表，从而在 DNS 查询中使用完全限定域名。例如，如果 DNS 客户端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“quality.company.com”。 如果 DNS 查询失败，路由器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。路由器会尝试附加 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附加该列表中的所有后缀。 在邻近对象发现 DNSS 选项中，使用要提供给 DNS 客户端路由器中的后缀配置防火墙；DNS 客户端使用其非限定 DNS 查询中的后缀接收 DNSSL 选项。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的八个 DNS 搜索列表域名（后缀）（按照自上而下列出的顺序），然后按相同的顺序使用它们。选择后缀并 **Move Up**（上移）或 **Move Down**（下移）以更改后缀的顺序，或在不再需要时从列表中 **Delete**（删除）后缀。

© 2019 Palo Alto Networks, Inc.

聚合接口设置	配置位置	说明
生命周期	**Aggregated Ethernet Interface**（聚合以太网接口）> **IPv6** > **DNS Support (cont)**（**DNS** 支持）（续）	输入 IPv6 DNS 客户端收到可以使用 DNS 搜索列表中的域名（后缀）的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Interfaces（接口）> VLAN

VLAN 接口可提供至第 3 层网络（IPv4 和 IPv6）的路由。可以将一个或多个第 2 层以太网端口（请参阅 PA-7000 系列第 2 层接口）添加到一个 VLAN 接口。

VLAN 接口设置	配置位置	说明
接口名称	**VLAN 接口**	只读的 **Interface Name**（接口名称）会设置为 **vlan**。在相邻字段中，输入数字后缀 (1 至 9,999) 以标识接口。
注释		输入接口的可选说明。
Netflow 配置文件		如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）可定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
vlan	**VLAN 接口** > **配置**	选择 VLAN，或单击 **VLAN** 可定义新的 VLAN（请参阅 Network（网络）> VLAN）。选择 **None**（无）可从接口删除当前 VLAN 分配。
虚拟路由器		要将虚拟路由器分配给接口，或单击 **Virtual Router**（虚拟路由器）可定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
管理配置文件	**VLAN Interface**（**VLAN** 接口）> **Advanced**（高级）> **Other Info**（其他信息）	管理配置文件 — 选择配置文件以定义可用来通过该接口管理防火墙的协议（例如，SSH、Telnet 和 HTTP）。选择 **None**（无）可从接口删除当前配置文件分配。
MTU		输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 9,192，默认为 1,500）。如果防火墙两端的机器执行路径 MTU 发现 (PMTUD) 且接口收到的数据包超过 MTU，则防火墙向源端返回 *ICMP fragmentation needed* 消息以表示该数据包太大。
调整 TCP MSS		选择此选项可调整最大分段大小 (MSS) 以容纳任何在接口 MTU 字节大小范围内的标头字节。MTU 字节大小减去 MSS 调整大小即等于 MSS 字节大小，此大小因 IP 协议而异： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 调整大小）— 范围为 40 至 300，默认为 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 60 至 300，默认为 60。 使用这些设置可在通过网络的 **tunnel**（隧道）需要更小的 MSS 时，解决相关问题。如果数据包拥有的字节超过没有分片的 MSS，则此设置将启用调整。

© 2019 Palo Alto Networks, Inc.

VLAN 接口设置	配置位置	说明
		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。
IP 地址 MAC 地址 接口	**VLAN Interface**（**VLAN** 接口）> **Advanced**（高级）> **ARP Entries**（**ARP** 条目）	要添加一个或多个静态地址解析协议 (ARP) 条目，请单击添加，输入 IP 地址及其关联的硬件 [介质访问控制 (MAC)] 地址，然后选择可访问该硬件地址的第 3 层接口。要删除条目，请选择条目，并单击删除。静态 ARP 条目减少 ARP 处理，并且排除指定地址的“中间人”（man-in-the-middle）攻击。
IPv6 地址 MAC 地址	**VLAN Interface**（**VLAN** 接口）> **Advanced**（高级）> **ND Entries**（**ND** 条目）	要为邻居发现协议 (NDP) 提供邻居信息，请单击 **Add**（添加），然后输入邻居的 IPv6 地址和 MAC 地址。
启用 NDP 代理	**VLAN Interface**（**VLAN** 接口）> **Advanced**（高级）> **NDP Proxy**（**NDP** 代理）	选择此项可为接口启用邻居发现协议 (NDP) 代理。防火墙将对为该列表中 IPv6 地址请求 MAC 地址的 ND 数据包做出响应。在 ND 响应中，防火墙会针对接口发送它自己的 MAC 地址，这基本上就是在说“请将对这些地址有意义的数据包发给我”。 （建议）如果正在使用网络前缀转换 IPv6 (NPTv6)，请启用 NDP 代理。 如果 **Enable NDP Proxy**（启用 **NDP** 代理），则可对大量 **Address**（地址）条目进行过滤：首先输入过滤器，然后应用该过滤器（绿色箭头）。
地址		**Add**（添加）一个或多个会将防火墙当作 NDP 代理的 IPv6 地址、IP 范围、IPv6 子网或地址对象。在这些地址中，最好要有一个地址和 NPTv6 中的源转换的地址相同。地址的顺序无关紧要。 如果地址所对应的是一个子网络，那么防火墙将针对该子网中的所有地址发送 ND 响应，所以建议您还要添加防火墙的 IPv6 邻居，然后单击 **Negate**（求反）以指示防火墙不要响应这些 IP 地址。
求反		为某个地址选择 **Negate**（求反）可为该地址阻止 NDP 代理。可以对指定 IP 地址范围或 IP 子网的子集进行求反。
设置	**VLAN Interface**（**VLAN** 接口）> **Advanced**（高级）> **DDNS**	选择 Settings（设置）使 DDNS 字段可进行配置。
启用		在接口上启用 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。）
更新间隔时间（天）		输入防火墙发送至 DDNS 服务器以更新映射到 FQDN 的 IP 地址的更新之间的间隔时间（天）（范围为 1 至 30，默认为 1）。 此外，防火墙还应在接收到 *DHCP* 服务器接口新的 *IP* 地址时更新 *DDNS*。

© 2019 Palo Alto Networks, Inc.

VLAN 接口设置	配置位置	说明
证书配置文件		选择您创建的证书配置文件（或创建一个新的配置文件），以验证 DDNS 服务。DDNS 服务可向防火墙提供由证书授权机构(CA)签署的证书。
主机名		输入在 DDNS 服务器上注册的接口主机名（例如，host123.domain123.com 或 host123）。除了确认语法使用 DNS 允许的域名有效字符外，防火墙不得验证主机名。
供应商		选择向该接口提供 DDNS 的 DDNS 供应商（和版本号）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** 如果选择的防火墙指定的旧版本 *DDNS* 服务将在特定日期之后逐步淘汰，请移至新版本。 供应商名称后面的 **Name**（名称）和 **Value**（值）字段是特定于供应商的。有些字段为只读，这样，您可以知道防火墙用于连接到 DDNS 服务的参数。配置其它字段，例如，DDNS 服务为您提供的密码以及防火墙在未接收到 DDNS 服务器响应时使用的超时。
IPv4 选项卡 — IP		添加接口上配置的 IPv4 地址，然后选中。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
IPv6 选项卡 — IPv6	**VLAN Interface**（**VLAN** 接口）> **Advanced**（高级）> **DDNS**（续）	添加接口上配置的 IPv6 地址，然后选中。所有选中的 IP 地址都通过 DDNS 提供商（供应商）注册。
显示运行时信息		显示 DDNS 注册：DDNS 提供商、已解析的 FQDN 和已映射的 IP 地址（带星号(*)，用于指示主 IP 地址）。每个 DDNS 提供商都有自己的返回代码，用于指示主机名更新状态，以及返回日期，以便进行故障排出。
对于 **IPv4** 地址		
类型	**VLAN Interface**（**VLAN** 接口）> **IPv4**	选择为接口分配 IPv4 地址类型的方法： • 静态 — 您必须手动指定 IP 地址。 • **DHCP** 客户端 — 启用接口作为动态主机配置协议 (DHCP) 客户端并接受动态分配 IP 地址。 防火墙在主动/主动高可用性 *(HA)* 模式下不支持 *DHCP* 客户端。 该选项卡中显示的选项将因您所选的 IP 地址方法而异。
• IPv4 地址类型 = 静态		

© 2019 Palo Alto Networks, Inc.

VLAN 接口设置	配置位置	说明
IP	**VLAN Interface（VLAN 接口）> IPv4**	单击添加，然后执行下列步骤之一，以指定接口的静态 IP 地址和网络掩码。 • 以无类别域间路由 (CIDR) 格式键入条目：*ip_address/mask*（例如，192.168.2.0/24）。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 创建 **IP netmask**（**IP** 网络掩码）类型的 **Address**（地址）对象。 可以为接口输入多个 IP 地址。系统使用转发信息库 (FIB) 来确定 IP 地址的最大数。 不再需要时 **Delete**（删除）IP 地址。
IPv4 地址类型 = **DHCP**		
启用	**VLAN Interface（VLAN 接口）> IPv4**	选择此选项可在接口上激活 DHCP 客户端。
自动创建指向服务器所提供的默认网关的默认路由		选择此选项可自动创建指向 DHCP 服务器提供的默认网关的默认路由。
发送主机名		选中此选项配置防火墙（作为 DHCP 客户端）以发送接口主机名（选项 12）到 DHCP 服务器。如果发送主机名，则默认将会选择主机名字段中的防火墙主机名。您可以发送该名称或是输入自定义主机名（最多 64 个字符，包括大写字母、小写字母、数字、句点、连字符和下划线）。
默认路由跃点数		对于防火墙与 DHCP 服务器之间的路由，可以输入要与默认路由关联和用于路径选择（范围为 1 至 65,535，无默认值）的路由跃点数（优先级）。数值越小，优先级越高。
显示 DHCP 客户端运行时信息		选中此选项可显示从 DHCP 服务器收到的所有设置，包括 DHCP 租借状态、动态 IP 地址分配情况、子网掩码、网关、服务器设置（DNS、NTP、域、WINS、NIS、POP3 和 SMTP）。
对于一个 **IPv6** 地址		
在接口上启用 IPv6	**VLAN Interface（VLAN 接口）> IPv6**	选择可在此接口上启用 IPv6 寻址。
接口 ID		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。
地址	**VLAN Interface（VLAN 接口）> IPv6（续）**	单击添加并为每个 IPv6 地址配置以下参数： • **Address**（地址）— 输入 IPv6 地址和前缀长度（如 2001:400:f00::1/64）。您也可以选择现有的 IPv6 地址对象，或单击 **Address**（地址）以创建地址对象。 • **Enable address on interface**（在接口上启用地址）— 单击可在接口上启用 IPv6 地址。

© 2019 Palo Alto Networks, Inc.

VLAN 接口设置	配置位置	说明

		• **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）— 选择可将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。
		• **Anycast**（任意播）— 选择以包括通过最近节点的路由。
		• **Send RA**（发送路由器通告）— 选择以启用此 IP 地址的路由器通告 (RA)。如果选择此选项，还必须在接口上全局 **Enable Router Advertisement**（启用路由器通告）。有关路由器通告的详细信息，请参阅启用路由器通告。
		
		其余字段只有在启用 RA 后才适用。
		
		  • **Valid Lifetime**（有效生存时间）— 防火墙认为地址有效的时间长度（秒）。有效生存时间必须等于或超过首选生存时间。默认值为 2,592,000。
		  • **Preferred Lifetime**（首选生存时间）— 首选的有效地址的时间长度（秒），这意味着防火墙可以用它来发送和接收流量。在首选生存时间到期后，防火墙不能使用地址来建立新的连接，但任何现有的连接仍然有效，直到超过 **Valid Lifetime**（有效生存时间）。默认值为 604,800。
		  • **On-link**（在链路上）— 如果能在不使用路由器的情况下访问通告前缀中包含 IP 地址的系统，请选择此选项。
		  • **Autonomous**（自治）— 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，请选择此选项。

启用重复地址检测	**VLAN Interface**（**VLAN** 接口）> **IPv6** > **Address Resolution**（地址解析）	选择可启用重复地址检查 (DAD)，这可让您指定 **DAD Attempts**（**DAD** 尝试次数）。
DAD 尝试次数		指定在尝试标识邻居失败之前在邻居请求间隔（**NS Interval**（**NS** 间隔））内的 DAD 尝试次数（范围为 1 至 10，默认为 1）。
可达到时间		指定成功查询和响应之后邻居可继续访问的时间长度（秒）（范围为 1 至 36,000，默认为 30）。
NS 间隔（邻居请求间隔）		指定在指示失败之前 DAD 尝试的秒数（范围为 1 至 10，默认为 1）。
启用 NDP 监控		选择启用邻近对象发现协议监控。启用后，您可以选择 NDP（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）。
启用路由器通告	**VLAN Interface**（**VLAN** 接口）> **IPv6** > **Router Advertisement**（路由器通告）	选择在 Ipv6 接口上提供邻近对象发现功能，并配置本节中的其他字段。IPv6 DNS 客户端使用此信息接收路由器通告 (RA) 消息。 路由器通告将防火墙用作非静态配置的 IPv6 主机的默认防火墙，并向该主机提供用于地址配置的 IPv6 前缀。您可以将独立的 DHCPv6 服务器与此功能结合使用，以向客户端提供 DNS 和其他设置。 这是适用于接口的全局设置。如果要设置单个 IP 地址的路由器通告选项，请将地址 **Add**（添加）到 IP 地址表并进行配置。如果您要为任何 IP 地址设置路由器通告选项，必须选择接口的 **Enable Router Advertisement**（启用路由器通告）选项。

© 2019 Palo Alto Networks, Inc.

VLAN 接口设置	配置位置	说明
最小间隔（秒）		指定防火墙将要发送路由器通告之间的最小间隔（秒）（范围为 3 至 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知。
最大间隔（秒）		指定防火墙将要发送路由器通告之间的最大间隔（秒）（范围为 4 至 1,800，默认为 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知。
跃点限制		指定适用于发送数据报的客户端的跃点限制（范围为 1 至 255，默认为 64）。输入 **0** 表示没有跃点限制。
链接 MTU		指定要应用到客户端的链路最大传输单元 (MTU)。选择 **unspecified**（未指定）表示无链路 MTU（范围为 1,280 至 9,192，默认为未指定）。
可访问时间（毫秒）		指定可访问时间（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，默认为未指定）。
重传时间（毫秒）		指定重传计时器确定客户将在重传邻居请求消息之前将要等待的时间（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，默认为未指定）。
路由器生存时间（秒）		指定客户端将防火墙用作默认网关的时间（秒）（范围为 0 至 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。
路由器首选项		如果网段拥有多个 IPv6 路由器，则客户端会使用此字段来选择首选路由器。选择防火墙路由器相对于网段中的其他路由器认为路由器通告拥有高、中（默认）还是低优先级。
托管配置		选择此选项以向客户端指示可通过 DHCPv6 使用该地址。
其他配置		选择此选项可向客户端指示可通过 DHCPv6 使用其他地址信息（例如，DNS 相关设置）。
一致性检查	**VLAN Interface**（**VLAN** 接口）> **IPv6** > **Router Advertisement (cont)**（路由器通告（续））	如果您希望防火墙验证从其他路由器发出的 RA 是否是正在链路上通告一致信息，请选择此选项。防火墙记录系统日志中的任何不一致；类型为 **ipv6nd**。
路由器通告中包括 DNS 信息	**VLAN Interface**（**VLAN** 接口）> **IPv6** > **DNS Support**（**DNS** 支持）	为防火墙选择此选项，以便从此 IPv6 VLAN 以太网子接口发送 NDP 路由器通告中的 DNS 信息。此表中的其他 DNS 支持字段仅在选择此选项后才可见。
服务器		为防火墙 **Add**（添加）一个或多个递归 DNS (RDNS) 服务器地址，以便从此 IPv6 VLAN 接口发送 NDP 路由器通告中的信息。RDNS 服务器向

© 2019 Palo Alto Networks, Inc.

VLAN 接口设置	配置位置	说明
		根 DNS 服务器和权威 DNS 服务器发送一系列 DNS 查找请求，以最终向 DNS 客户端提供 IP 地址。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的八个 RDNS 服务器（按照自上而下列出的顺序），然后按相同的顺序使用这些地址。选择服务器并 **Move Up**（上移）或 **Move Down**（下移）以更改服务器的顺序，或在不再需要时从列表中 **Delete**（删除）服务器。
生命周期		输入 IPv6 DNS 客户端收到可以使用 RDNS 服务器解析域名的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。
后缀		为 DNS 搜索列表 (DNSSL) **Add**（添加）并配置一个或多个域名（后缀）。最大后缀长度为 255 个字节。 DNS 搜索列表是在 DNS 查询中输入名称之前 DNS 客户端路由器附加（一次一个）到非限定域名的域后缀列表，从而在 DNS 查询中使用完全限定域名。例如，如果 DNS 客户端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，然后发送 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“quality.company.com”。 如果 DNS 查询失败，路由器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。路由器会尝试附加 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附加该列表中的所有后缀。 在邻近对象发现 DNSS 选项中，使用要提供给 DNS 客户端路由器中的后缀配置防火墙；DNS 客户端使用其非限定 DNS 查询中的后缀接收 DNSSL 选项。 您可以在 NDP 路由器通告中最多配置防火墙向收件人发送的八个 DNS 搜索列表域名（后缀）（按照自上而下列出的顺序），然后按相同的顺序使用这些地址。选择后缀并 **Move Up**（上移）或 **Move Down**（下移）以更改顺序，或在不再需要时从列表中 **Delete**（删除）后缀。
生命周期		输入 IPv6 DNS 客户端收到可以使用 DNS 搜索列表中的域名（后缀）的路由器通告后的最大秒数（范围为最大间隔（秒）到最大间隔两倍的值；默认为 1,200）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Interfaces（接口）> Loopback（回环）

使用以下字段配置回环接口：

回环接口设置	配置位置	说明
接口名称	回环接口	只读的 **Interface Name**（接口名称）会设置为 **loopback**。在相邻字段中，输入数字后缀 (1-9999) 以标识接口。
注释		输入接口的可选说明。
Netflow 配置文件		如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）可定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
虚拟路由器	**Loopback Interface**（回环接口）> **Config**（配置）	要将虚拟路由器分配给接口，或单击 **Virtual Router**（虚拟路由器）可定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
管理配置文件	**Tunnel Interface**（隧道接口）> **Advanced**（高级）> **Other Info**（其他信息）	管理配置文件 — 选择配置文件以定义可用来通过该接口管理防火墙的协议（例如，SSH、Telnet 和 HTTP）。选择 **None**（无）可从接口删除当前配置文件分配。
MTU		输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576-9,192；默认为 1,500）。如果防火墙两端的机器执行路径 MTU 发现 (PMTUD) 且接口收到的数据包超过 MTU，则防火墙向源端返回 *ICMP fragmentation needed* 消息以表示该数据包太大。
调整 TCP MSS		选择此选项可调整最大分段大小 (MSS) 以容纳任何在接口 MTU 字节大小范围内的标头字节。MTU 字节大小减去 MSS 调整大小即等于 MSS 字节大小，此大小因 IP 协议而异： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 调整大小）— 范围为 40-300，默认为 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 调整大小）— 范围为 60-300，默认为 60。 使用这些设置可在通过网络的 **tunnel**（隧道）需要更小的 MSS 时，解决相关问题。如果数据包拥有的字节超过没有分片的 MSS，则此设置将启用调整。

© 2019 Palo Alto Networks, Inc.

回环接口设置	配置位置	说明
		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。
对于 **IPv4** 地址		
IP	**Loopback Interface**（回环接口）> **IPv4**	单击添加，然后执行下列步骤之一，以指定接口的静态 IP 地址和网络掩码。 • 输入子网掩码为 /32 的 IPv4 地址；例如 192.168.2.1/32。仅支持 /32 子网掩码。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 单击 **Address**（地址）可创建 **IP netmask**（**IP** 网络掩码）类型的地址对象。 可以为接口输入多个 IP 地址。系统使用转发信息库 (FIB) 来确定 IP 地址的最大数。 要删除 IP 地址，请选择地址并单击删除。
对于一个 IPv6 地址		
在接口上启用 IPv6	**Loopback Interface**（回环接口）> **IPv6**	选择可在此接口上启用 IPv6 寻址。
接口 ID		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。
地址		单击添加并为每个 IPv6 地址配置以下参数： • **Address**（地址）— 输入 IPv6 地址和前缀长度（如 2001:400:f00::1/64）。您也可以选择现有的 IPv6 地址对象，或单击 **Address**（地址）以创建地址对象。 • **Enable address on interface**（在接口上启用地址）— 单击可在接口上启用 IPv6 地址。 • **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）— 选择可将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。 • **Anycast**（任意播）— 选择以包括通过最近节点的路由。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Interfaces（接口）> Tunnel（隧道）

使用以下字段配置隧道接口：

隧道接口设置	配置位置	说明
接口名称	隧道接口	只读的 **Interface Name**（接口名称）会设置为 **tunnel**。在相邻字段中，输入数字后缀 (1-9,999) 以标识接口。
注释		输入接口的可选说明。
Netflow 配置文件		如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）可定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
虚拟路由器	隧道接口 > 配置	要将虚拟路由器分配给接口，或单击 **Virtual Router**（虚拟路由器）可定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统		如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或单击 **Virtual System**（虚拟系统）可定义新的 vsys。
安全区域		选择接口的安全区域，或单击 **Zone**（区域）可定义新区域。选择 **None**（无）可从接口删除当前区域分配。
管理配置文件	**Tunnel Interface**（隧道接口）> **Advanced**（高级）> **Other Info**（其他信息）	管理配置文件 — 选择配置文件以定义可用来通过该接口管理防火墙的协议（例如，SSH、Telnet 和 HTTP）。选择 **None**（无）可从接口删除当前配置文件分配。
MTU		输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576-9,192；默认为 1,500）。如果防火墙两端的机器执行路径 MTU 发现 (PMTUD) 且接口收到的数据包超过 MTU，则防火墙向源端返回 *ICMP fragmentation needed* 消息以表示该数据包太大。
对于 IPv4 地址		
IP	隧道接口 > **IPv4**	单击添加，然后执行下列步骤之一，以指定接口的静态 IP 地址和网络掩码。 • 以无类别域间路由 (CIDR) 格式键入条目：ip_address/mask（例如，192.168.2.0/24）。 • 选择 **IP** 网络掩码类型的现有地址对象。 • 单击 **Address**（地址）可创建 **IP netmask**（**IP** 网络掩码）类型的地址对象。 可以为接口输入多个 IP 地址。系统使用转发信息库 (FIB) 来确定 IP 地址的最大数。

© 2019 Palo Alto Networks, Inc.

隧道接口设置	配置位置	说明
		要删除 IP 地址，请选择地址并单击删除。
对于一个 IPv6 地址		
在接口上启用 IPv6	**Tunnel Interface**（隧道接口）> **IPv6**	选择可在此接口上启用 IPv6 寻址。
接口 ID	**Tunnel Interface**（隧道接口）> **IPv6**	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。
地址		单击添加并为每个 IPv6 地址配置以下参数： • **Address**（地址）— 输入 IPv6 地址和前缀长度（如 2001:400:f00::1/64）。您也可以选择现有的 IPv6 地址对象，或单击 **Address**（地址）以创建地址对象。 • **Enable address on interface**（在接口上启用地址）— 单击可在接口上启用 IPv6 地址。 • **Use interface ID as host portion**（使用接口 **ID** 作为主机部分）— 选择可将 **Interface ID**（接口 **ID**）用作 IPv6 地址的主机部分。 • **Anycast**（任意播）— 选择以包括通过最近节点的路由。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Interfaces（接口）> SD-WAN

创建一个 SD-WAN 虚拟接口，并添加一个或多个指向相同目标的物理以太网接口成员。

SD-WAN 接口设置	
接口名称	只读的 **Interface Name**（接口名称）会设置为 **sdwan**。在相邻字段中，输入数字后缀（1 至 9,999）来标识 SD-WAN 虚拟接口。
注释	最佳做法是输入接口的简要说明，比如到 `Internet` 或到美国西部中心。添加注释可更方便于识别接口，无需尝试解密日志和报告中自动生成的名称。
Netflow 配置文件	如果您想要导出从入口接口遍历到 NetFlow 服务器的单向 IP 通信，请选择服务器配置文件或单击 **Netflow Profile**（**Netflow** 配置文件）可定义新的配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> NetFlow）。选择 **None**（无）可从接口删除当前 NetFlow 服务器分配。
Config（配置）选项卡	
虚拟路由器	分配虚拟路由器给接口，或选择 **Virtual Router**（虚拟路由器）以定义新的虚拟路由器（请参阅 Network（网络）> Virtual Routers（虚拟路由器））。选择 **None**（无）可从接口删除当前虚拟路由器分配。
虚拟系统	如果防火墙支持多个虚拟系统且已启用该功能，请选择适用于接口的虚拟系统 (vsys)，或选择 **Virtual System**（虚拟系统）以定义新的 vsys。
安全区域	选择接口的安全区域，或选择 **Zone**（区域）以定义新区域。选择 **None**（无）可从接口删除当前区域分配。SD-WAN 虚拟接口及其所有接口成员均必须处于同一安全区域，确保从分支到同一目的地的所有路径均使用相同的安全策略规则。
高级选项卡	
接口	选择构成此 SD-WAN 虚拟接口的第 3 层以太网接口（对于直接 Internet 访问 [DIA]）或虚拟 VPN 隧道接口（对于中心）。防火墙虚拟路由器通过此 SD-WAN 虚拟接口将 SD-WAN 流量路由到 DIA 或中心位置。接口可以有不同的标签。如果输入多个接口，这些接口的类型必须一致（VPN 隧道或 DIA）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Zones（区域）

以下主题介绍网络安全区域。

您在查找什么内容？	请参阅：
安全区域有何用途？	安全区域概述
哪些字段可用于配置安全区域？	安全区域的构建块
了解更多？	使用接口和区域对网络进行分段

安全区域概述

安全区域是一种对防火墙上的物理和虚拟接口进行分组的逻辑方法，其目的在于控制并记录遍历网络中特定接口的流量。必须先将防火墙上的接口分配给安全区域，之后这些接口才能处理通信。一个区域可以分配到多个同类型接口（如旁接、第 2 层或第 3 层接口），但一个接口只能属于一个区域。

防火墙上的策略规则将使用安全区域来标识通信的来源及去向。流量可在某个区域内自由流动，但不能在不同区域之间流动，除非您定义一个允许此操作的安全策略规则。要允许或拒绝区域间流量，安全策略规则必须引用特定源区域和目标区域（而非接口），并且这些区域的类型必须相同；即安全策略规则只能允许或拒绝从一个第 2 层区域传到另一个第 2 层区域的流量。

安全区域的构建块

要定义安全区域，请单击 **Add**（添加），然后指定以下信息：

安全区域设置	说明
姓名	输入区域名称（最多 31 个字符）。定义安全策略和配置接口时，此名称出现在区域列表中。名称区分大小写，且必须在虚拟路由器中具有唯一性。仅可使用字母、数字、空格、连字符、句点和下划线。
位置	此字段只有在防火墙支持多个虚拟系统 (vsys) 且已启用该功能时才会出现。选择要应用此区域的虚拟系统。
类型	选择区域类型（**Tap**（旁接）、**Virtual Wire**（虚拟线路）、**Layer2**（第 2 层）、**Layer3**（第 3 层）、**External**（外部）或 **Tunnel**（隧道））可查看未分配给区域的该类型的所有 **Interfaces**（接口）。第 2 层和第 3 层区域类型列出该类型的所有 Ethernet 接口和子接口。**Add**（添加）要分配给该区域的接口。 外部区域用于控制单个防火墙上的多个虚拟系统之间的通信。该区域将仅在支持多个虚拟系统的防火墙上显示，且仅当 **Multi Virtual System Capability**（多虚拟系统功能）已启用时才会显示。有关外部区域的信息，请参阅防火墙内保留的 Inter-VSYS 通信。 在一个虚拟系统中，一个接口仅可属于一个区域。
接口	将一个或多个接口添加到该区域。

© 2019 Palo Alto Networks, Inc.

安全区域设置	说明
Zone Protection Profiles	选择配置文件，以指定防火墙如何响应来自此区域的攻击。要创建新的配置文件，请参阅 Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）。最佳做法是使用区域保护配置文件保护每个区域。
启用数据包缓冲区保护	全局配置数据包缓冲区保护（Device（设备）> Setup（设置）> Session（会话）），并将其应用于每个区域。防火墙仅在入口区域使用数据包缓冲区保护。默认启用基于缓冲区利用率百分比的数据包缓冲区保护。或者配置基于延迟的数据包缓冲区保护。最佳做法是启用每个区域的数据包缓冲区保护，以保护防火墙缓冲区。
日志设置	选择日志转发配置文件，用于将区域保护日志转发到外部系统。 如果您拥有名为 default 的日志转发配置文件，则在定义新安全区域时会自动为此下拉列表选择该配置文件。您可以在设置新安全区域时通过继续选择不同的日志转发配置文件随时替代此默认设置。要定义或添加新的日志转发配置文件（并将该配置文件命名为 default 以便自动填充此下拉列表），可单击 **New**（新建）（请参阅 Objects（对象）> Log Forwarding（日志转发））。 如果在 *Panorama* 模板中配置区域，则 *Log Setting*（日志设置）下拉列表仅列出共享的日志转发配置文件；要指定非共享配置文件，必须键入其名称。
启用用户标识	如果已将 User-ID™ 配置为执行 IP 地址到用户名的映射（发现），则最佳做法是 **Enable User Identification**（启用用户标识），以将映射信息应用到该区域中的通信。如果禁用此选项，则防火墙日志、报告和策略会将用户映射排除在区域内通信之外。 默认情况下，如果选择此选项，则防火墙会将用户映射信息应用到该区域中所有子网络的通信。要将信息限制于该区域中的特定子网络，请使用包括列表和排除列表。 仅在可信区域上启用 *User-ID*。如果在外部不可信区域（如互联网）上启用 *User-ID* 和客户端探测，则可以在受保护的网络之外发送探测，从而导致 *User-ID* 代理服务帐户名称、域名和加密密码哈希的信息披露，这可能会允许攻击者未经授权访问受保护的资源。 仅当该区域落在 *User-ID* 所监控的网络范围内时，*User-ID* 才会针对该区域执行发现操作。如果该区域不在此范围内，则即使选择 *Enable User Identification*（启用用户标识），防火墙也不会将用户映射信息应用到该区域。有关详细信息，请参阅包括或排除用户映射的子网。
用户标识 ACL 包括列表	默认情况下，如果未在该列表中指定子网络，则防火墙会将其发现的用户映射信息应用于该区域的所有通信，以便用于日志、报告和策略。 要将用户映射信息的应用限值于该区域内的特定子网络，请针对各个子网络单击添加并选择地址（或地址组）对象或输入 IP 地址范围（例如，10.1.1.1/24）。因为 **Include List**（包含列表）是一个允许列表，所以，所有其他子网络都会被隐式排除，无需将其添加到 **Exclude List**（排除列表）中。 将条目添加到排除列表中只会为包括列表中的子网络子集排除用户映射信息。例如，如果将 10.0.0.0/8 添加到包括列表中并将 10.2.50.0/22 添加到排除列

© 2019 Palo Alto Networks, Inc.

安全区域设置	说明
	表中，则防火墙会为 10.0.0.0/8 种除 10.2.50.0/22 以外的所有区域子网络包括用户映射信息，并会为不在 10.0.0.0/8 中的所有区域子网络排除信息。 您只能将落在 *User-ID* 所监控的网络范围内的子网络包括进来。有关详细信息，请参阅包括或排除用户映射的子网。
用户标识 ACL 排除列表	要为 **Include List**（排除列表）中的子网络子集排除用户映射信息，请针对要排除的各个子网络 **Add**（添加）地址（或地址组）对象或键入 IP 地址范围。 如果将条目添加到排除列表中，但不添加到包括列表中，则防火墙会为该区域中的所有子网络（不只是所添加的子网络）排除用户映射信息。

© 2019 Palo Alto Networks, Inc.

Network（网络）> VLAN

防火墙支持符合 IEEE 802.1Q 标准的 VLAN。在防火墙上定义的每个第 2 层接口都可以与 VLAN 相关联。同一个 VLAN 可以分配给多个第 2 层接口，但每个接口只能属于一个 VLAN。

VLAN 设置	说明
姓名	输入 VLAN 名称（最多 31 个字符）。配置接口时，此名称出现在 VLAN 列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
VLAN 接口	选择 Network（网络）> Interfaces（接口）> VLAN 以允许在 VLAN 之外路由流量。
接口	指定 VLAN 的防火墙接口。
静态 MAC 配置	指定可通过其访问 MAC 地址的接口。这将替代任何已获得的接口到 MAC 映射。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Virtual Wires（虚拟线路）

在防火墙上指定两个虚拟线路接口（Network（网络）> Interfaces（接口））后，选择 **Network**（网络）> **Virtual Wires**（虚拟线路）可对虚拟线路进行定义。

虚拟线路设置	说明
虚拟线路名称	输入虚拟线路名称（最多**31**个字符）。配置接口时，此名称出现在虚拟线路列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
接口	从显示的列表中为虚拟线路配置选择两个以太网接口。只有当接口具有虚拟线路接口类型并且尚未分配给其他虚拟线路时，它们才会在此处列出。 有关虚拟线路接口的信息，请参阅虚拟线路接口。
允许的标记	为虚拟线路上允许的通信输入标记编号 (0-4094) 或标记编号的范围 (tag1-tag2)。标记值为零（默认）表示未标记流量。多个标记或范围必须以逗号分隔。会丢弃标记值为排除的通信。 传入或传出数据包上的标记值不会更改。 在使用虚拟线路子接口时，允许的标记列表将使所有带有所列标记的通信分类到父虚拟线路中。虚拟线路子接口必须使用父允许的标记列表中不存在的标记。
多播防火墙	如果希望将安全规则应用到多播通信，请选择此选项。如果未启用此设置，则多播通信将转发到整个虚拟线路中。
链接状态传递	如果您想在检测到链路状态关闭时关闭虚拟线路对中的其他接口，请选择此选项。如果不选择或禁用此选项，则链路状态不会传播到整个虚拟线路。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Virtual Routers（虚拟路由器）

防火墙需要虚拟路由器来获取其他子网的路由，获取方式可以是使用您手动定义的静态路由或参与第 3 层路由协议（动态路由）。在防火墙上定义的每个第 3 层接口、回环接口和 VLAN 接口都必须与虚拟路由器关联。每个接口只能属于一个虚拟路由器。

定义虚拟路由器需要进行常规设置，并按网络要求对静态路由或动态路由协议进行任意组合。您也可配置其他功能，如路由重新分发、ECMP 等等。

您在查找什么内容？	请参阅
虚拟路由的必要元素有哪些？	虚拟路由器的常规设置
配置：	静态路由 路由重新分发 RIP OSPF OSPFv3 BGP IP 多播 ECMP
查看有关虚拟路由器的信息	有关虚拟路由器的更多运行时统计数据
了解更多？	networking（网络）

虚拟路由器的常规设置

- Network（网络）> Virtual Routers（虚拟路由器）> Router Settings（路由器设置）> General（常规）

所有虚拟路由器都需要指定第 3 层接口和管理距离跃点数，如下表所述。

虚拟路由器常规设置	说明
姓名	指定名称以描述虚拟路由器（最多31个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
接口	选择要包含在虚拟路由器中的接口。因此，这些接口可在虚拟路由器的路由表中用作传出接口。 要指定接口类型，请参阅 Network（网络）> Interfaces（接口）。 添加接口时，会自动添加它所连接的路由。
管理距离	指定以下管理距离：

© 2019 Palo Alto Networks, Inc.

虚拟路由器常规设置	说明
	• **Static routes**（静态路由）— 范围为 10-240，默认为 10。 • **OSPF Int** — 范围为 10-240，默认为 30。 • **OSPF Ext** — 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。

静态路由

- Network（网络）> Virtual Routers（虚拟路由器）> Static Routes（静态路由）

可选择输入一个或多个静态路由。单击 **IP** 或 **IPv6** 选项卡，可使用 IPv4 或 IPv6 地址指定路由。通常需要在此处配置默认路由 (0.0.0.0/0)。对于在虚拟路由器的路由表中以其他方式找不到的目标应用默认路由。

静态路由设置	说明
名称	输入标识静态路由的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
目标	以无类别域间路由 (CIDR) 格式输入 IP 地址和网络掩码：*ip_address/mask*（掩码）（例如，192.168.2.0/24（对于 IPv4）或 2001:db8::/32（对于 IPv6））。或者，可创建 IP 网络掩码类型的地址对象。
接口	选择用来将数据包转发到目标的接口，并/或配置下一个跃点设置。
下一个跃点	在以下各项中选择一项： • **IP Address**（**IP** 地址）— 选中此选项以输入下一个跃点的 IP 地址，或是选择或创建 IP 网络掩码类型的地址对象。该地址对象必须具有 /32 (IPv4) 或 /128 (IPv6) 的网络掩码。 • **Next VR**（下一个 **VR**）— 选中以选择防火墙中的虚拟路由器作为下一个跃点。此选项可让您在单个防火墙内的虚拟路由器之间进行内部路由。 • **FQDN** — 选中此选项可按 FQDN 标识下一个跃点。然后，选择 FQDN 类型的地址对象，或是创建一个新的 FQDN 类别地址对象。 • 丢弃— 选择是否要丢弃发往此目标的通信。 • 无- 如果路由没有下一个跃点，请选择此项。
管理距离	指定静态路由的管理距离（10-240，默认为 10）。
指标	指定静态路由的有效跃点数值 (1 - 65535)。
路由表	选择防火墙在其中安装静态路由的路由表： • **Unicast**（单播）— 将路由安装到单播路由表。 • **Multicast**（多播）— 将路由安装到多播路由表。 • **Both**（两者）— 将路由安装到单播和多播路由表。 • **No Install**（无安装）— 不在路由表 (RIB) 中安装路由；在删除静态路由之前，防火墙会保留此路由以供将来参考。

© 2019 Palo Alto Networks, Inc.

静态路由设置	说明
BFD 配置文件	要对 PA-3200 系列、PA-5200 系列、PA-7000 系列或 VM 系列防火墙上的静态路由启用双向转发检测 (BFD)，请在以下各项中选择一项： • **default**（默认）（即默认的 BFD 设置） • 已在防火墙上创建的 BFD 配置文件 • **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 BFD 配置文件 选择 **None (Disable BFD)**（无（禁用 **BFD**））可对静态路由禁用 BFD。 如需在静态路由上使用 BFD： • 静态路由相反端上的防火墙和对等都必须支持 BFD 会话。 • 静态路由 **Next Hop**（下一个跃点）类型必须为 **IP Address**（**IP** 地址），且您必须输入有效的 IP 地址。 • **Interface**（接口）设置不可为 **None**（无）；必须选择一个接口（即便正在使用 DHCP 地址，也不例外）。
路径监视	选中此选项可对静态路由启用路径监控。
失败条件	选择防火墙认为受监控路径停用，因此静态路由停用所依据的条件： • **Any**（任何）— 如果 ICMP 不可访问任一静态路由受监控目标，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动态或静态路由。 • **All**（所有）— 如果 ICMP 不可访问所有静态路由受监控目标，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动态或静态路由。 选择 **All**（所有）可避免单个受监控目标在离线维护时发送静态路由失败的信号。
抢占保留时间(分)	输入以下值：在防火墙将静态路由重新安装到 RIB 中之前，停用的路径监控必须保持激活状态（路径监控评估其所有成员受监控目标，且必须保持激活状态）的时长，以分钟为单位。如果计时器到期，但链接没有断开或翻动，链接被视为处于稳定状态，则路径监控可以保持激活状态，并且防火墙可以将静态路由添加回 RIB 中。 如果链接在保留时间内断开或翻动，则路径监控失败，并且计时器会在停用的监控返回激活状态时重启。如果抢占保留时间为零，防火墙会在路径监控激活时将静态路由立即重新安装到 RIB 中。范围为 0-1,440；默认为 2。
名称	输入受监控目标的名称（最多 31 个字符）。
启用	选中此选项可为静态路由的特定目标启用路径监控；防火墙会向此目标发送 ICMP ping。
源 IP	选择防火墙用作受监控目标的 ICMP ping 消息源的 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

© 2019 Palo Alto Networks, Inc.

静态路由设置	说明
	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。
目标 Ip	输入防火墙为其监控路径的 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）
Ping 间隔(秒)	指定确定防火墙监控路径的频率的 ICMP ping 间隔（以秒为单位，ping 受监控目标，范围为 1-60，默认为 3）。
Ping 计数	指定在防火墙认为链接断开之前受监控目标未返回的 ICMP ping 连续数据包的数量。根据任何或所有故障条件，在路径监控处于失败状态的情况下，防火墙会从 RIB 删除静态路由（范围为 3-10，默认为 5）。 例如，如果 Ping Interval（Ping 间隔）为 3 秒，Ping Count（Ping 计数）为 5 次缺失 ping 数据包（防火墙在过去 15 秒没有收到 ping 数据包），则表示路径监控检测到链接故障。如果路径监控处于失败状态，防火墙在 15 秒后收到 ping 数据包，则链接会被视为处于激活状态；根据任何或所有故障条件，对任何或所有受监控目标的路径监控会被视为处于激活状态，并且抢占保留时间开始计时。

路由重新分发

- Network（网络）> Virtual Router（虚拟路由器）> Redistribution Profiles（重新分发配置文件）

重新分发配置文件指示防火墙根据需要的网络行为筛选、设置优先级和执行操作。路由重新分发允许静态路由和其他协议获得的路由通过指定的路由协议进行通告。

重新分发配置文件必须应用于路由协议才能生效。如果没有重新分发规则，每个协议单独运行，且不会在其范围之外通信。配置完所有路由协议并且建立随之而生的网络拓扑之后，可以添加或修改重新分发配置文件。

通过定义导出规则，将重新分发配置文件应用于 RIP 和 OSPF 协议。在重新分发规则选项卡中应用再分发配置文件到 BGP。请参阅下表。

重新分发配置文件设置	说明
名称	添加一个重新分发配置文件，并输入配置文件的名称。
优先级	输入此配置文件的优先级（范围为 1-255）。配置文件是按顺序进行匹配的（最小的数字最先）。
重新分发	选择是否根据此窗口中的设置执行路由重新分发。 • 重新分发— 选择该项可重新分发匹配的候选路由。如果选择此选项，则输入新的跃点数值。较低的跃点数值表示更首选的路由。 • 无重新分发— 选择该项不会重新分发匹配的候选路由。
常规过滤器选项卡	
类型	选择候选路由的路由类型。
接口	选择接口以指定候选路由的转发接口。

© 2019 Palo Alto Networks, Inc.

重新分发配置文件设置	说明
目标	要指定候选路由的目标，请输入目标 IP 地址或子网（格式为 x.x.x.x 或 x.x.x.x/n），然后单击添加。如需删除条目，请单击删除 (⊖)。
下一个跃点	要指定候选路由的网关，请输入代表下一个跃点的 IP 地址或子网（格式为 x.x.x.x 或 x.x.x.x/n），然后单击添加。如需删除条目，请单击删除 (⊖)。
OSPF 过滤器选项卡	
路径类型	选择候选 OSPF 路由的路由类型。
区域	指定候选 OSPF 路由的区域标识符。输入 **OSPF area ID**（**OSPF** 区域 **ID**）（格式为 x.x.x.x），并单击 **Add**（添加）。 如需删除条目，请单击删除 (⊖)。
标记	指定 OSPF 标记值。输入标记数值 (1-255)，然后单击“添加”。 如需删除条目，请单击删除 (⊖)。
BGP 过滤器选项卡	
社区	指定 BGP 路由策略的社区。
扩展的社区	指定 BGP 路由策略的扩展社区。

RIP

- Network（网络）> Virtual Routers（虚拟路由器）> RIP

配置路由信息协议 (RIP) 包括以下常规设置：

RIP 设置	说明
启用	选中此选项可启用 RIP。
拒绝默认路由	（建议）如果不想通过 RIP 获得任何默认路由，请选中此选项。
BFD	如需对 PA-5200 系列、PA-7000 系列和 VM 系列防火墙上虚拟路由器的 RIP 全局启用双向转发检测 (BFD)，请在以下各项中选择一项： • **default**（默认值）（带默认 BFD 设置的配置文件） • 已在防火墙上创建的 BFD 配置文件 • **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 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。

此外，还必须配置以下选项卡上的 RIP 设置：

- **Interfaces**（接口）：请参阅 RIP Interfaces（接口）选项卡。
- **Timers**（计时器）：请参阅 RIP Timers（计时器）选项卡。

© 2019 Palo Alto Networks, Inc.

- **Auth Profiles**（身份验证配置文件）：请参阅 RIP Auth Profiles（身份验证配置文件）选项卡。
- **Export Rules**（导出规则）：请参阅 RIP Export Rules（导出规则）选项卡。

RIP 接口选项卡

- Network（网络）> Virtual Routers（虚拟路由器）> RIP > Interfaces（接口）

使用以下字段可配置 RIP 接口。

RIP – 接口设置	说明
接口	选择运行 RIP 协议的接口。
启用	选择该项可启用这些设置。
通告	选中即可对具有指定跃点数值的 RIP 对端启用默认路由通告。
指标	指定路由器通告的跃点数值。仅当启用 **Advertise**（通告）时，此字段可见。
身份验证配置文件	选择配置文件。
模式	选择正常、被动或仅发送。
BFD	如需对 RIP 接口启用 BFD（只要 BFD 未在虚拟路由器级别上对 RIP 禁用，则将因此而覆盖 RIP 的 BFD 设置），请在以下各项中选择一项： • **default**（默认值）（带默认 BFD 设置的配置文件） • 已在防火墙上创建的 BFD 配置文件 • **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 BFD 配置文件 选择 **None (Disable BFD)**（无（禁用 **BFD**））可对 RIP 接口禁用 BFD。

RIP 计时器选项卡

- 网络 > 虚拟路由器 > RIP > 计时器

下表将介绍控制 RIP 路由更新和到期的计时器。

RIP – 计时器设置	说明
RIP 计时	
间隔(秒)	定义计时器时间间隔的长度（以秒为单位）。此持续时间用于剩余的 RIP Timing 字段（范围为 1-60）。
更新间隔	输入路由更新声明之间的时间间隔数（范围为 1-3,600）。
到期间隔	输入自上次更新路由直至路由过期之间的时间间隔数（范围为 1-3,600）。
删除间隔	输入自路由过期直至路由删除之间的时间间隔数（范围为 1-3,600）。

© 2019 Palo Alto Networks, Inc.

RIP 身份验证配置文件选项卡

- 网络 > 虚拟路由器 > RIP > 身份验证配置文件

默认情况下，防火墙不会对邻居之间的 RIP 消息进行身份验证。如需对邻居之间的 RIP 消息进行身份验证，请创建一个身份验证配置文件，然后将其应用到虚拟路由器上运行 RIP 的接口。下表介绍了身份验证配置文件选项卡的设置。

RIP – 身份验证配置文件设置	说明
配置文件名称	输入用于对 RIP 消息进行身份验证的身份验证配置文件的名称。
密码类型	选择密码类型（Simple 或 MD5）。 • 如果选择简单，则输入简单密码，然后确认。 • 如果选择 **MD5**，请输入一个或多个密码条目，包括 **Key-ID** (0-255)、密钥和可选的首选状态。对于每个条目，单击添加，然后单击**OK**。要指定用来对传出消息进行身份验证的密钥，请选择首选选项。

RIP 导出规则选项卡

- 网络 > 虚拟路由器 > RIP > 导出规则

RIP 导出规则可让您控制虚拟路由器发送到对端的路由。

RIP – 导出规则设置	说明
允许再分发默认路由	选中此选项可允许防火墙将其默认路由重新分发到对端设备。
重新分发配置文件	单击 **Add**（添加），然后选择或创建一个重新分发配置文件，以便根据所需网络行为修改路由重新分发、筛选程序、优先级和操作。请参阅路由重新分发。

OSPF

- Network（网络）> Virtual Router（虚拟路由器）> OSPF

配置开放式最短路径优先 (OSPF) 协议需要配置以下常规设置（可选项 BFD 除外）：

OSPF 设置	说明
启用	选中此选项可启用 OSPF 协议。
拒绝默认路由	（建议）如果不想通过 OSPF 获得任何默认路由，请选中此选项。
路由器 ID	指定与此虚拟路由器中的 OSPF 实例关联的路由器 ID。OSPF 协议使用路由器 ID 来对 OSPF 实例进行唯一标识。
BFD	如需对 PA-5200 系列、PA-7000 系列或 VM 系列防火墙上虚拟路由器的 OSPF 全局启用双向转发检测 (BFD)，请在以下各项中选择一项： • **default**（默认）（即默认的 BFD 设置） • 已在防火墙上创建的 BFD 配置文件

© 2019 Palo Alto Networks, Inc.

OSPF 设置	说明
	• **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 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；无法为单个 OSPF 接口启用 BFD。

此外，还必须在以下选项卡中配置 OSPF 设置：

- **Areas**（区域）：请参阅 OSPF Areas（区域）选项卡。
- **Auth Profiles**（身份验证配置文件）：请参阅 OSPF Auth Profiles（身份验证配置文件）选项卡。
- **Export Rules**（导出规则）：请参阅 OSPF Export Rules（导出规则）选项卡。
- 高级：请参阅 OSPF Advanced（高级）选项卡。

OSPF 区域选项卡

- Network（网络）> Virtual Router（虚拟路由器）> OSPF > Areas（区域）

以下字段介绍了 OSPF 区域设置：

OSPF – 区域设置	说明
区域	
区域 ID	配置可应用 OSPF 参数的区域。 以 x.x.x.x 格式输入区域的标识符。这是每个邻居必须接受才能成为同一区域成员的标识符。
类型	选择以下某个选项。 • 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，若您想要接受来自其他区域的此类型的链接状态通告 (LSA)，请选择接受摘要。并且指定是否将默认路由 LSA 随关联的跃点数值（范围为 1-255）一起包含在发送到存根区域的通告中。 如果禁用 stub 区域“区域边界路由器”(ABR) 接口中的接受摘要选项，则 OSPF 区域将相当于“完全末梢区域”(TSA)，且 ABR 将不会传播任何摘要 LSA。 • **NSSA** (Not-So-Stubby Area) — 可以直接离开区域，但只能由 OSPF 路由除外的其他路由进行。如果选择此选项，若您想要接受此类型的 LSA，请选择接受摘要。选择 **Advertise Default Route**（通告默认路由）以指定是否将默认路由 LSA 随关联的跃点数值 (1-255) 一起包含在发送到 stub 区域的通告中。并且选择用于通告默认 LSA 的路由类型。如果想要启用或禁止将通过 NSSA 获得的外部路由通告到其他区域，请单击 **External Ranges**（外部范围）部分中的 **Add**（添加），并输入范围。
范围	单击添加将区域中的 LSA 目标地址聚合到子网中。启用或禁止通告与子网匹配的 LSA，然后单击确定。重复该过程以添加其他范围。
接口	添加要包含在区域中的接口，然后输入以下信息： • 接口— 选择接口。 • 启用— 使 OSPF 接口设置生效。

© 2019 Palo Alto Networks, Inc.

OSPF – 区域设置	说明

	• **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。在必须手动定义邻居时，请选择 **p2mp**（点对多点）。只有在 p2mp 模式时才可手动定义邻居。
	• 跃点数— 输入此接口的 OSPF 跃点数 (0-65,535)。
	• 优先级— 输入此接口的 OSPF 优先级 (0-255)。它是根据 OSPF 协议将路由器选为指定路由器 (DR) 或备份 DR (BDR) 的优先级。值为零时，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。
	• **BFD** — 要为 OSPF 对端接口启用双向转发检测 (BFD)（只要未在虚拟路由器级别对 OSPF 禁用 **BFD**，就可替代 OSPF 的 **BFD** 设置），请在以下各项中选择一项：
	  • **default**（默认）（即默认的 BFD 设置）
	  • 已在防火墙上创建的 BFD 配置文件
	  • **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 BFD 配置文件
	  • 选择 **None (Disable BFD)**（无（禁用 **BFD**））可对 OSPF 对端接口禁用 BFD。
	• **Hello Interval (sec)**（呼叫间隔（秒））— OSPF 进程向其直接连接的相邻设备发送呼叫数据包的间隔秒数（范围为 0-3600，默认为 10）。
	• 间隔次数 — 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。**Hello Interval**（呼叫间隔）乘以 **Dead Counts**（间隔次数）等于间隔计时器的值（范围为 3-20，默认为 4）。
	• **Retransmit Interval (sec)**（重传间隔（秒））— OSPF 在重传 LSA 之前等待接收相邻设备的链路状态通告 (LSA) 的时长（以秒为单位，范围为 0-3,600；默认为 10）。
	• **Transit Delay (sec)**（传输延迟（秒））— 在将 LSA 发送到接口之前延迟的时长秒数（范围为 0-3,600，默认为 1）。

接口（续）	• **Graceful Restart Hello Delay (sec)**（正常重启呼叫延迟（秒））— 当配置主动/被动高可用性时适用于 OSPF 接口。**Graceful Restart Hello Delay**（平稳重新启动呼叫延迟）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 **Hello Interval**（呼叫间隔）乘以 **Dead Counts**（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至少是 **Graceful Restart Hello Delay**（平稳重新启动呼叫延迟）的值的四倍。例如，**Hello Interval**（呼叫间隔）值为 10 秒，**Dead Counts**（间隔次数）值为 4 次，而间隔计时器的值则为 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新启动期间不会超时（范围为 1-10；默认为 10）。
虚拟链接	配置虚拟链接设置以维护或增强骨干网区域连通性。这些设置必须为区域边界路由器定义，且必须在骨干网区域 (0.0.0.0) 中定义。单击添加，并为每个要包含在骨干网区域中的虚拟链接输入以下信息，然后单击确定。 • 名称— 输入虚拟链接的名称。 • 邻居 **ID**— 输入虚拟链接另一端的路由器（邻居）的路由器 ID。

© 2019 Palo Alto Networks, Inc.

OSPF – 区域设置	说明
	• 中转区域— 输入实际包含虚拟链接的中转区域的区域 ID。 • 启用— 选择该项可启用虚拟链接。 • 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。

OSPF 身份验证配置文件选项卡

- 网络 > 虚拟路由器 > OSPF > 身份验证配置文件

以下字段介绍了 OSPF 身份验证配置文件设置：

OSPF – 身份验证配置文件设置	说明
配置文件名称	输入身份验证配置文件的名称。要对 OSPF 消息进行身份验证，请在**OSPF**选项卡上先定义身份验证配置文件，然后将它们应用于接口。
密码类型	选择密码类型（Simple 或 MD5）。 • 如果选择简单，请输入密码。 • 如果选择 **MD5**，请输入一个或多个密码条目，包括 **Key-ID** (0-255)、密钥和可选的首选状态。对于每个条目，单击添加，然后单击**OK**。要指定用来对传出消息进行身份验证的密钥，请选择首选选项。

OSPF 导出规则选项卡

- 网络 > 虚拟路由器 > OSPF > 导出规则

下表介绍了用于导出 OSPF 路由的字段：

OSPF – 导出规则设置	说明
允许再分发默认路由	选中此选项可允许通过 OSPF 重新分发默认路由。
姓名	选择重新分发配置文件的名称。值必须是 IP 子网或有效的重新分发配置文件的名称。
新路径类型	选择要应用的跃点数类型。
新标记	为匹配路由指定具有 32 位值的标记。
指标	（可选）指定要与导出的路由关联并用于路径选择的路由跃点数（范围为 1-65,535）。

OSPF 高级选项卡

- 网络 > 虚拟路由器 > OSPF > 高级

以下字段介绍了 RFC 1583 兼容性、OSPF 计时器和正常重启：

© 2019 Palo Alto Networks, Inc.

OSPF – 高级设置	说明
RFC 1583 兼容性	选中此选项后，可确保与 RFC 1583 兼容（OSPF 版本 2）。
计时器	• **SPF Calculation Delay (sec)**（**SPF** 计算延迟（秒））— 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。应通过类似方式调整与防火墙对等的路由以优化收敛时间。 • **LSA Interval (sec)**（**LSA** 间隔（秒））— 指定同一个 LSA（相同路由器、相同类型、相同 LSA ID）的两个实例传输之间的最短时间。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。
平稳重启	• **Enable Graceful Restart**（启用正常重启）— 默认情况下启用，启用此功能的防火墙会在相邻路由器转换状态，向其汇报临时关闭时，指示该路由器继续通过防火墙路由流量。 • **Enable Helper Mode**（启用帮助程序模式）— 默认情况下启用，启用此模式的防火墙会在相邻设备重启时，继续将流量转发到该设备。 • **Enable Strict LSA Checking**（启用严格的 **LSA** 检查）— 默认情况下启用，此功能会让启用 OSPF 帮助程序模式的防火墙在拓扑更改时，退出帮助程序模式。 • **Grace Period (sec)**（宽限期（秒））— 相邻设备重新设置或路由器重启时，对端设备应将流量继续转发到该防火墙的时间段（以秒为单位，范围为 5-1,800，默认为 120）。 • **Max Neighbor Restart Time**（相邻设备最长重启时间）— 防火墙接受的充当帮助模式路由器的最长宽限期（以秒为单位）。如果对端设备在其宽限 LSA 中提供更长的宽限期，那么防火墙不会进入帮助程序模式（范围为 5-1,800；默认为 140）。

OSPFv3

- Network（网络）> Virtual Router（虚拟路由器）> OSPFv3

配置开放式最短路径优先 v3 (OSPFv3) 协议，需要配置下表中的前三项设置（BFD 是可选项）：

OSPFv3 Settings	说明
启用	选中此选项可启用 OSPF 协议。
拒绝默认路由	如果不想通过 OSPF 获得任何默认路由，请选中此选项。
路由器 ID	指定与此虚拟路由器中的 OSPF 实例关联的路由器 ID。OSPF 协议使用路由器 ID 来对 OSPF 实例进行唯一标识。
BFD	如需对 PA-5200 系列、PA-7000 系列和 VM 系列防火墙上虚拟路由器的 OSPFv3 全局启用双向转发检测 (BFD)，请在以下各项中选择一项： • **default**（默认）（即默认的 BFD 设置） • 已在防火墙上创建的 BFD 配置文件 • **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 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 OSPFv3 接口禁用 BFD；无法对单个 OSPFv3 接口启用 BFD。

© 2019 Palo Alto Networks, Inc.

此外，还需要在以下选项卡中配置 OSPFv3 设置：

- **Areas**（区域）：请参阅 OSPFv3 Areas（区域）选项卡。
- **Auth Profiles**（身份验证配置文件）：请参阅 OSPFv3 Auth Profiles（身份验证配置文件）选项卡。
- **Export Rules**（导出规则）：请参阅 OSPFv3 Export Rules（导出规则）选项卡。
- 高级：请参阅 OSPFv3 Advanced（高级）选项卡。

OSPFv3 区域选项卡

- Network（网络）> Virtual Router（虚拟路由器）> OSPFv3 > Areas（区域）

使用以下字段可配置 OSPFv3 区域。

OSPv3 – 区域设置	说明
身份验证	选择要为该 OSPF 区域指定的身份验证配置文件的名称。
类型	在以下各项中选择一项： • 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，若您想要接受来自其他区域的此类型的链接状态通告 (LSA)，请选择接受摘要。并且指定是否将默认路由 LSA 随关联的跃点数值 (1-255) 一起包含在发送到 stub 区域的通告中。 如果禁用 stub 区域“区域边界路由器”(ABR) 接口中的接受摘要选项，则 OSPF 区域将相当于“完全末梢区域”(TSA)，且 ABR 将不会传播任何摘要 LSA。 • **NSSA** (Not-So-Stubby Area) — 可以直接离开区域，但只能由 OSPF 路由除外的其他路由进行。如果选择此选项，若您想要接受此类型的 LSA，请选择接受摘要。指定是否将默认路由 LSA 随关联的跃点数值 (1-255) 一起包含在发送到 stub 区域的通告中。并且选择用于通告默认 LSA 的路由类型。如果想要启用或禁止将通过 NSSA 获得的外部路由通告到其他区域，请单击 **External Ranges**（外部范围）部分中的 **Add**（添加），并输入范围
范围	单击 **Add**（添加）以在区域中按照子网聚合 LSA 目标 IPv6 地址。启用或禁止通告与子网匹配的 LSA，然后单击确定。重复该过程以添加其他范围。
接口	单击添加，并为每个要包含在区域中的接口输入以下信息，然后单击确定。 • 接口— 选择接口。 • 启用— 使 OSPF 接口设置生效。 • 实例 **ID** — 输入 OSPFv3 实例 ID 号。 • **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。在必须手动定义邻居时，请

© 2019 Palo Alto Networks, Inc.

OSPv3 – 区域设置	说明

	选择 **p2mp**（点对多点）。只有在 p2mp 模式时才可手动定义邻居。
	• 跃点数— 输入此接口的 OSPF 跃点数 (0-65,535)。
	• 优先级— 输入此接口的 OSPF 优先级 (0-255)。它是根据 OSPF 协议将路由器选为指定路由器 (DR) 或备份 DR (BDR) 的优先级。值为零时，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。
	• **BFD** — 要为 OSPFv3 对端接口启用双向转发检测 (BFD)（只要未在虚拟路由器级别对 OSPFv3 禁用 **BFD**，就可替代 OSPFv3 的 **BFD** 设置），请在以下各项中选择一项：
	  • **default**（默认）（即默认的 BFD 设置）
	  • 已在防火墙上创建的 BFD 配置文件
	  • **New BFD Profile**（新建 **BFD** 配置文件）可创建新的 BFD 配置文件
	  选择 **None (Disable BFD)**（无（禁用 **BFD**））可对 OSPFv3 对端接口禁用 BFD。
	• **Hello Interval (sec)**（呼叫间隔（秒））— OSPF 进程向其直接连接的相邻设备发送呼叫数据包的间隔秒数（范围为 0-3600，默认为 10）。
	• 间隔次数 — 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。**Hello Interval**（呼叫间隔）乘以 **Dead Counts**（间隔次数）等于间隔计时器的值（范围为 3-20，默认为 4）。
	• **Retransmit Interval (sec)**（重传间隔（秒））— OSPF 在重传 LSA 之前等待接收相邻设备的链路状态通告 (LSA) 的时长（以秒为单位，范围为 0-3,600；默认为 10）。
	• **Transit Delay (sec)**（传输延迟（秒））— 在防火墙将 LSA 发送到接口之前延迟的时长（以秒为单位，范围为 0-3,600；默认为 1）。

接口（续）	• **Graceful Restart Hello Delay (sec)**（正常重启呼叫延迟（秒））— 当配置主动/被动高可用性时适用于 OSPF 接口。**Graceful Restart Hello Delay**（平稳重新启动呼叫延迟）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 **Hello Interval**（呼叫间隔）乘以 **Dead Counts**（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至少是 **Graceful Restart Hello Delay**（平稳重新启动呼叫延迟）的值的四倍。例如，**Hello Interval**（呼叫间隔）值为 10 秒，**Dead Counts**（间隔次数）值为 4 次，而间隔计时器的值则为 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新启动期间不会超时（范围为 1-10；默认为 10）。 • 邻居 — 对于 p2pmp 接口，输入可通过此接口访问的所有邻居的 IP 地址。

© 2019 Palo Alto Networks, Inc.

OSPv3 – 区域设置	说明
虚拟链接	配置虚拟链接设置以维护或增强骨干网区域连通性。这些设置必须为区域边界路由器定义，且必须在骨干网区域 (0.0.0.0) 中定义。单击添加，并为每个要包含在骨干网区域中的虚拟链接输入以下信息，然后单击确定。 • 名称— 输入虚拟链接的名称。 • 实例 **ID** — 输入 OSPFv3 实例 ID 号。 • 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。 • 启用— 选择该项可启用虚拟链接。 • 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。

OSPFv3 身份验证配置文件选项卡

- Network（网络）> Virtual Router（虚拟路由器）> OSPFv3 > Auth Profiles（身份验证配置文件）

使用以下字段可配置 OSPFv3 的身份验证。

OSPFv3 – 身份验证配置文件设置	说明
配置文件名称	输入身份验证配置文件的名称。要对 OSPF 消息进行身份验证，请在**OSPF**选项卡上先定义身份验证配置文件，然后将它们应用于接口。
SPI	指定安全参数索引 (SPI)，以供数据包遍历远程防火墙到达对等端设备。
协议	指定以下任意一个协议： • **ESP** — 封装式安全措施负载协议。 • **AH** — 身份验证头协议
加密算法	指定以下某个加密算法 • 无 — 不会使用任何加密算法。 • **SHA1**（默认值）— 安全散列算法 1。 • **SHA256** — 安全散列算法 2。四个哈希函数的集合，具有 256 位摘要。 • **SHA384** — 安全散列算法 2。四个哈希函数的集合，具有 384 位摘要。 • **SHA512** — 安全散列算法 2。四个哈希函数的集合，具有 512 位摘要。 • **MD5** — MD5 消息摘要算法。
密钥/确认密钥	输入并确认身份验证密钥。

© 2019 Palo Alto Networks, Inc.

OSPFv3 – 身份验证配置文件设置	说明
加密（仅限 ESP 协议）	指定以下某个加密选项： • **3des**（默认值）— 应用使用三个 56 位加密密钥的三重数据加密算法 (3DES)。 • **aes-128-cbc** — 应用使用 128 位加密密钥的高级加密标准 (AES)。 • **aes-192-cbc** — 应用使用 192 位加密密钥的高级加密标准 (AES)。 • **aes-256-cbc** — 应用使用 256 位加密密钥的高级加密标准 (AES)。 • **null** — 不加密。
密钥/确认密钥	输入并确认加密密钥。

OSPFv3 导出规则选项卡

- Network（网络）> Virtual Router（虚拟路由器）> OSPFv3 > Export Rules（导出规则）

使用以下字段可导出 OSPFv3 路由。

OSPFv3 – 导出规则设置	说明
允许再分发默认路由	选中此选项可允许通过 OSPF 重新分发默认路由。
姓名	选择重新分发配置文件的名称。值必须是 IP 子网或有效的重新分发配置文件的名称。
新路径类型	选择要应用的跃点数类型。
新标记	为匹配路由指定具有 32 位值的标记。
指标	（可选）指定要与导出的路由关联并用于路径选择的路由跃点数（范围为 1-65,535）。

OSPFv3 高级选项卡

- Network（网络）> Virtual Router（虚拟路由器）> OSPFv3 > Advanced（高级）

使用以下字段可禁用 SPF 计算的中转路由、配置 OSPFv3 计时器，以及配置 OSPFv3 正常重启。

OSPFv3 – 高级设置	说明
禁用 SRF 计算的转接路由	如果要在路由器 LSA 中设置从该防火墙发送的 R 位，以表示防火墙处于不活动状态，则选中此选项。处于此状态时，防火墙会参与 OSPFv3，但是其他路由器不会发送中转流量。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

© 2019 Palo Alto Networks, Inc.

OSPFv3 – 高级设置	说明
	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。
计时器	• **SPF Calculation Delay (sec)**（**SPF** 计算延迟（秒））— 此选项是一个延迟计时器，用来调整接收新拓扑信息和执行 SPF 计算之间的延迟时间。值越低 OSPF 重新收敛速度越快。应通过类似方式调整与防火墙对等的路由以优化收敛时间。 • **LSA** 间隔(秒)— 此选项可指定同一个 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。
平稳重启	• **Enable Graceful Restart**（启用正常重启）— 默认情况下启用，启用此功能的防火墙会在相邻路由器转换状态，向其汇报临时关闭时，指示该路由器继续通过防火墙路由流量。 • **Enable Helper Mode**（启用帮助程序模式）— 默认情况下启用，启用此模式的防火墙会在相邻设备重启时，继续将流量转发到该设备。 • **Enable Strict LSA Checking**（启用严格的 **LSA** 检查）— 默认情况下启用，此功能会让启用 OSPF 帮助程序模式的防火墙在拓扑更改时，退出帮助程序模式。 • **Grace Period (sec)**（宽限期（秒））— 相邻设备重新设置或路由器重启时，对端设备将流量继续转发到该防火墙的时间段（以秒为单位，范围为 5-1,800，默认为 120）。 • **Max Neighbor Restart Time**（相邻设备最长重启时间）— 防火墙接受的充当帮助模式路由器的最长宽限期（以秒为单位）。如果对端设备在其宽限 LSA 中提供更长的宽限期，那么防火墙不会进入帮助程序模式（范围为 5-800；默认为 140）。

BGP

- Network（网络）> Virtual Router（虚拟路由器）> BGP

配置边界网关协议 (BGP) 需要配置基本 BGP 设置以启用 BGP，并按下表所述配置路由器 ID 和 AS 编号。此外，还必须配置 BGP 对端作为 BGP 对端组的一部分。

根据网络需要，在以下选项卡上配置剩余 BGP 设置：

- **General**（常规）：请参阅 BGP 常规选项卡。
- 高级：请参阅 BGP 高级选项卡。
- **Peer Group**（对端组）：请参阅 BGP 对端组选项卡。
- 导入：请参阅 BGP 导入和导出选项卡。
- **Export**（导出）：请参阅 BGP 导入和导出选项卡。
- **Conditional Adv**（有条件通告）：请参阅 BGP 有条件通告选项卡。
- **Aggregate**（聚合）：请参阅 BGP 聚合选项卡。
- **Redist Rules**（重新分发规则）：请参阅 BGP 重新分发规则选项卡。

基本 *BGP* 设置

要在虚拟路由器上使用 BGP，必须启用 BGP 并配置路由器 ID 和 AS 编号；可以选择启用 BFD。

© 2019 Palo Alto Networks, Inc.

BGP 设置	配置位置	说明
启用	**BGP**	选择以启用 BGP。
路由器 ID		输入要分配给虚拟路由器的 IP 地址。
AS 编号		根据路由器 ID，输入虚拟路由器所属的 AS 的编号（范围为 1 至 4,294,967,295）。
BFD		如需对 PA-5200 系列、PA-7000 系列或 VM 系列防火墙上虚拟路由器的 BGP 全局启用双向转发检测 (BFD)，请在以下各项中选择一项： • **default**（默认）（即默认的 BFD 设置） • 防火墙上的现有 BFD 配置文件 • 创建 **New BFD Profile**（新的 **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。 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 *BGP* 通信。因此，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。

BGP 常规选项卡

- 网络 > 虚拟路由器 > BGP > 常规

使用以下字段配置常规 BGP 设置。

BGP 常规设置	配置位置	说明
拒绝默认路由	**BGP** > 常规	选择此选项可忽略由 BGP 对端通告的任何默认路由。
安装路由		选择此选项可在全局路由表中安装 BGP 路由。
聚合 Med		选择该项以启用路由聚合，即使路由有不同的多出口鉴别 (MED) 值也如此。
默认本地首选项		指定防火墙可以用于确定不同路径中首选项的值。
As 格式		选择 2 字节（默认）或 4 字节格式。可配置此设置以便于互操作。
始终比较 Med		允许对源自不同自治系统中的邻居的路径进行 MED 比较。
确定性 MED 比较		允许 MED 比较过程中在 iBGP 对端（同一自治系统中的 BGP 对端）通告的路由之间进行选择。
身份验证配置文件		**Add**（添加）新的身份验证配置文件，并配置以下设置： • **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。

© 2019 Palo Alto Networks, Inc.

BGP 常规设置	配置位置	说明
		不再需要时删除 (⊖) 配置文件。

BGP 高级选项卡

- 网络 > 虚拟路由器 > BGP > 高级

高级 BGP 设置包括各种功能。可以通过多个 BGP 自治系统运行 ECMP。您可以要求 eBGP 对端列出自己的 AS 作为 AS_PATH 属性中的第一个 AS（以防止欺诈更新数据包）。还可以配置 BGP 优雅重启，这是 BGP 对端指示在 BGP 重启期间它们是否可以保留转发状态的一种手段，从而最大限度减轻路由翻动（上升和下降）的后果。此外，还可以配置路由反射器和 AS 联合，这两种方法可避免在 AS 中拥有全网状 BGP 对端。您可以配置路由惩罚以防止在 BGP 网络不稳定和路由翻动时产生不必要的路由器收敛。

BGP 高级设置	配置位置	说明
ECMP 多个 AS 支持	**BGP** > 高级	如果要为虚拟路由器启用 ECMP 且通过多个 BGP 自治系统运行 ECMP，请选择此选项。
强制执行 EBGP 的第一个 AS		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。这样可以防止 BGP 进一步处理来自相邻 AS 以外的欺诈或错误的更新数据包。默认为启用。
优雅重新启动		激活优雅重启选项。 • **Stale Route Time**（失效路由时间）— 指定路由可以在已失效状态中停留的时长秒数（范围为 1-3,600，默认为 120）。 • **Local Restart Time**（本地重启时长）— 指定防火墙重启所需时长（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**（最长对端重新启动时间）— 指定防火墙接受的作为对端设备优雅重启时间的最长时间（以秒计）（范围为 1-3,600 秒，默认为 120 秒）。
反射器集群 ID		指定代表反射器集群的 IPv4 标识符。AS 中的路由反射器（路由器）执行重新通告路由以认识其对端的作用（而不需要全网状连接和所有对端彼此发送路由）。路由反射器简化了配置。
Confederation Member As		指定仅在 BGP 联合内可见的自治系统号码标识符（也称为子自治系统号码）。使用 BGP 联合将自治系统划分为多个子自治系统，以此减少全网状对端。
抑制配置文件	**BGP** > **Advanced (cont)**（高级（续））	路由惩罚是一种确定通告是否会因路由翻动而抑制路由的方法。路由惩罚可以减少由于路由翻动而强制路由器重新收敛的次数。设置包括： • **Profile Name**（配置文件名称）— 输入名称以标识配置文件。 • 启用— 激活配置文件。 • **Cutoff**（截断）— 指定路由收回阈值，高于该值的路由通告将会被禁止（范围为 0.0-1,000.0，默认为 1.25）。 • **Reuse**（重用）— 指定路由收回阈值，低于该值的被禁止路由将会再次使用（范围为 0.0-1,000.0，默认为 5）。

© 2019 Palo Alto Networks, Inc.

BGP 高级设置	配置位置	说明
		• **Max. Hold Time**（最长保持时间）— 指定路由可被禁止的最长时间，而不论其如何不稳定（以秒计）（范围为 0-3,600 秒，默认为 900 秒）。 • **Decay Half Life Reachable**（可到达半衰期）— 指定一段时间的长度，超过该时间后，如果防火墙认为路由可访问，则路由的稳定性跃点数将会减半（以秒计）（范围为 0-3,600 秒，默认为 300 秒）。 • **Decay Half Life Unreachable**（无法到达半衰期）— 指定一段时间的长度，超过该时间后，如果防火墙认为路由不可访问，则路由的稳定性跃点数将会减半（以秒计）（范围为 0-3,600 秒，默认为 300 秒）。 不再需要时删除（⊖）配置文件。

BGP 对端组选项卡

- Network（网络）> Virtual Router（虚拟路由器）> BGP > Peer Group（对端组）

BGP 对端组是共享设置的 BGP 对端集合，如对端组的类型（如 EBGP），或从更新数据包中虚拟路由器发送的 AS_PATH 列表中删除私有 AS 编号的设置。BGP 对端组可让您无需使用相同设置配置多个对端。您至少必须配置一个 BGP 对端组才能配置属于该组的 BGP 对端。

BGP 对端组设置	配置位置	说明
姓名	**BGP** > 对端组	输入用于标识对端组的名称。
启用		选择以激活对端组。
聚合 Confed AS 路径		选择以包括配置的聚合联合 AS 路径。
使用存储的信息执行软重置		选择将在更新对端设置后执行防火墙的软重置。

类型		指定对等端或组的类型并配置关联设置（请参阅下表中对 **Import Next Hop**（导入下一个跃点）和 **Export Next Hop**（导出下一个跃点）的描述）。
		• **IBGP** — 指定以下各项；
		  • 导出下一个跃点
		• **EBGP Confed** — 指定以下各项；
		  • 导出下一个跃点
		• **IBGP Confed** — 指定以下各项；
		  • 导出下一个跃点
		• **EBGP**— 指定以下各项；
		  • 导入下一个跃点
		  • 导出下一个跃点
		  • **Remove Private AS**（删除私有 **AS**）（如果要强制 BGP 从 AS_PATH 属性删除私有 AS 编号，请选择此选项）。

© 2019 Palo Alto Networks, Inc.

BGP 对端组设置	配置位置	说明
导入下一个跃点		选择用于导入下一个跃点的选项： • **original**（原始）— 使用原始路由通告中提供的下一个跃点地址。 • **Use Peer**（使用对端）— 使用对端的 IP 地址作为下一个跃点地址。
导出下一个跃点		选择用于导出下一个跃点的选项： • **Resolve**（解析）— 使用转发信息库 (FIB) 解析下一个跃点地址。 • **original**（原始）— 使用原始路由通告中提供的下一个跃点地址。 • **Use Self**（使用自身）— 用此虚拟路由器的 IP 地址替换下一个跃点地址以确保它出现在转发路径中。
删除专用 AS		选择以从 AS_PATH 列表中删除私有自治系统。
姓名	**BGP** > 对端组 > 对端	添加 **New**（新的）BGP 对端，然后输入用于标记该对端的名称。
启用		选择该项可激活对等端。
对等 AS		指定对端的自治系统 (AS)。
启用 MP-BGP 扩展	**BGP** > **Peer Group**（对端组）> **Peer**（对端）> **Addressing**（寻址）	启用防火墙以支持 IPv4 和 IPv6 的多协议 BGP 地址系列标识符，以及每个 RFC 4760 的后续地址系列标识符选项。
地址系列类型		选择与此对端的 BGP 会话将支持的 **IPv4** 或 **IPv6** 地址系列。
后续地址系列		选择与此对端的 BGP 会话将承载的 **Unicast**（单播）或 **Multicast**（多播）后续地址系列协议。
本地地址 — 接口		选择防火墙接口。
本地地址 — IP		选择本地 IP 地址
对端地址 — 类型和地址		选择标识对端设备的地址类型： • **IP** — 选择 IP，并选择使用 IP 地址的地址对象（或是创建使用 IP 地址的新地址对象）。 • **FQDN** — 选择 FQDN，并选择使用 FQDN 的地址对象（或是创建使用 FQDN 的新地址对象）。
身份验证配置文件	**BGP** > **Peer Group**（对端组）> **Peer**（对端）> **Connection Options**（连接选项）	选择配置文件或从下拉列表中选择 **New Auth Profile**（新建身份验证配置文件）。输入配置文件的**Name**（名称）和 **Secret**（密钥），然后输入 **Confirm Secret**（确认密钥）。
保持活动间隔		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禁止来自对端的路由（范围为 0-1,200 秒，默认为 30 秒）。
多个跃点		设置 IP 标头中的生存时间 (TTL) 值（范围为 1-255，默认为 0）。默认为 0 表示 1 代表 eBGP。默认为 0 表示 255 代表 iBGP。
打开延迟时间		指定在打开对端 TCP 连接和发送第一个 BGP 打开消息之间的延迟时间（范围为 0-240 秒，默认为 0 秒）。

© 2019 Palo Alto Networks, Inc.

BGP 对端组设置	配置位置	说明
保持时间		指定在关闭对等连接之前，从对等端发出连续的 KEEPALIVE 或 UPDATE 消息之间所经历的时间（范围为 3-3,600 秒，默认为 90 秒）。
空闲保持时间		指定在重试与对端连接之前在空闲状态中等待的时间（范围为 1-3,600 秒，默认为 15 秒）。
传入连接 — 远程端口		指定传入端口号，并 **Allow**（允许）传入此端口的流量。
传出连接 — 本地端口		指定传出端口号，并 **Allow**（允许）此端口传出的流量。
反射器客户端	**BGP** > **Peer Group**（对端组）> **Peer**（对端）> **Advanced**（高级）	选择反射器客户端的类型（**Non-Client**（非客户端）、**Client**（客户端）或 **Meshed Client**（网状客户端））。从反射器客户端接收的路由将会与所有内部和外部 BGP 对等端共享。
对等类型		指定双边对端或保持未指定。
最大前缀数		指定受支持的 IP 前缀的最大数目（1-100,000 或无限制）。
启用发送端循环检测		启用此选项以促使防火墙在更新中发送路由之前检查其 FIB 中路由的 AS_PATH 属性，以确保对端 AS 编号不在 AS_PATH 列表中。如果对端 AS 编号在 AS_PATH 列表中，则防火墙会将其删除以防止循环。通常接收器会执行循环检测，但此优化功能会使用发送器执行循环检测。
BFD		可对 BGP 对端启用双向转发检测 (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），选择默认配置文件（默认 BFD 设置）、现有的 BFD 配置文件、**Inherit-vr-global-setting**（以继承全局 **BGP BFD** 配置文件），或选择 **New BFD Profile**（新建 **BFD** 配置文件）（以创建新的 BFD 配置文件）。**Disable BFD**（禁用 **BFD**）可对 BGP 对端禁用 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端到程序 *BFD* 的 *BGP* 连接进行阻止。对端设备将发现 *BGP* 连接丢弃，这可导致重新收敛，进而对生产流量造成影响。因此，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。

BGP 导入和导出选项卡

- 网络 > 虚拟路由器 > BGP > 导入
- 网络 > 虚拟路由器 > BGP > 导出

Add（添加）新的导入或导出规则以导入或导出 BGP 路由。

© 2019 Palo Alto Networks, Inc.

BGP 导入和导出设置	配置位置	说明
规则	**BGP** > **Import or Export**（导入或导出）> **General**（常规）	指定名称以标识规则。
启用		选择此选项可激活规则。
Used by		选择将使用此规则的对端组。
AS 路径正则表达式	**BGP** > **Import or Export**（导入或导出）> **Match**（匹配）	指定用于过滤 AS 路径的正则表达式。
社区正则表达式		指定用于过滤社区字符串的正则表达式。
扩展的社区正则表达式		指定用于过滤扩展的社区字符串的正则表达式。
MED		指定用于路由过滤的多出口鉴别值，范围为 0-4,294,967,295。
路由表		对于 **Import Rule**（导入规则），指定将导入匹配路由的路由表：**unicast**（单播）、**multicast**（多播）或 **both**（两者）。 对于 **Export Rule**（导出规则），指定将导出匹配路由的路由表：**unicast**（单播）、**multicast**（多播）或 **both**（两者）。
地址前缀		指定用于路由过滤的 IP 地址或前缀。
下一个跃点		指定用于路由过滤的下一个跃点路由器或子网。
从对端		指定用于路由过滤的对端路由器。
操作	**BGP** > **Import or Export**（导入或导出）> **Action**（操作）	指定在符合匹配条件时要执行的操作（**Allow**（允许）或 **Deny**（拒绝））。
抑制		指定惩罚参数（仅当操作是 **Allow**（允许）时）。
本地首选项		指定本地首选项跃点数（仅当操作是 **Allow**（允许）时）。
MED		指定 MED 值 (0 - 65,535)（仅当操作是 **Allow**（允许）时）。
重量		指定权重值 (0 - 65,535)（仅当操作是 **Allow**（允许）时）。
下一个跃点		指定下一个跃点路由器（仅当操作是 **Allow**（允许）时）。
原始		指定原始路由的路径类型：IGP、EGP 或 incomplete（仅当操作是允许时）。
AS 路径限制		指定 AS 路径限制（仅当操作是 **Allow**（允许）时）。
AS 路径		指定 AS 路径：无、删除、预先设置和删除并预先设置（仅当操作是允许时）。

© 2019 Palo Alto Networks, Inc.

BGP 导入和导出设置	配置位置	说明
社区		指定社区选项：无、删除全部、删除正则表达式、追加或覆盖（仅当操作是允许时）。
扩展的社区		指定社区选项：无、删除全部、删除正则表达式、追加或覆盖（仅当操作是允许时）。
		不再需要时 **Delete**（删除）⊖ 规则或在适当时 **Clone**（克隆）规则。还可以选择规则，并 **Move Up**（上移）或 **Move Down**（下移）以更改规则顺序。

BGP 有条件通告选项卡

- 网络 > 虚拟路由器 > BGP > 有条件通告

通过 BGP 有条件通告可以控制当在本地 BGP 路由表 (LocRIB) 中首选路由不可用时，由哪个路由发出通告，以指示对端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（除非与预先选定的提供商断开连接），此功能特别有用。

对于有条件通告，您可以配置指定首选路由的非现有过滤器（**Address Prefix**（地址前缀）），以及标识首选路由的任何其他属性（如 AS 路径正则表达式）。如果在本地 BGP 路由表中找不到与非现有过滤器匹配的任何路由，则防火墙允许通告其通告过滤器中指定的替代路由（到其他非首选提供商的路由）。

要配置有条件通告，选择 **Conditional Adv**（有条件通告）选项卡，**Add**（添加）有条件通告，然后按下表所述配置值。

BGP 有条件通告设置	配置位置	说明
策略	**BGP** > **Conditional Adv**（有条件通告）	指定此有条件通告策略规则的名称。
启用		选择以启用此有条件通告策略规则。
Used by		**Add**（添加）将使用此有条件通告策略规则的对端组。
非现有过滤器	**BGP** > **Conditional Adv**（有条件通告） > **Non Exist Filters**（非现有筛选程序）	使用此选项卡指定首选路由的前缀。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过滤器匹配，则通告将被禁止。） **Add**（添加）非现有过滤器，并指定用于标识此过滤器的名称。
启用		选择以激活非现有过滤器。
AS 路径正则表达式		指定用于过滤 AS 路径的正则表达式。
社区正则表达式		指定用于过滤社区字符串的正则表达式。
扩展的社区正则表达式		指定用于过滤扩展的社区字符串的正则表达式。

© 2019 Palo Alto Networks, Inc.

BGP 有条件通告设置	配置位置	说明
MED		指定用于路由过滤的 MED 值（范围为 0-4,294,967,295）。
路由表		指定防火墙将搜索以查看是否存在匹配的路由的路由表（**unicast**（单播）、**multicast**（多播）或 **both**（两者））。如果该路由表中不存在匹配的路由，则防火墙仅允许替代路由的通告。
地址前缀		为首选路由 **Add**（添加）确切的网络层可达性信息 (NLRI) 前缀。
下一个跃点		指定用于路由过滤的下一个跃点路由器或子网。
从对端		指定用于路由过滤的对端路由器。
通告过滤器	**BGP** > **Conditional Adv**（有条件通告）> **Advertise Filters**（通告筛选程序）	使用此选项卡指定本地 RIB 路由表中的路由前缀，如果非现有过滤器中的路由在本地路由表中不可用，则通告此前缀。 如果要通告的前缀与非现有过滤器不匹配，将发生通告。 **Add**（添加）通告过滤器，并指定用于标识此过滤器的名称。
启用		选择以激活过滤器。
AS 路径正则表达式		指定用于过滤 AS 路径的正则表达式。
社区正则表达式		指定用于过滤社区字符串的正则表达式。
扩展的社区正则表达式		指定用于过滤扩展的社区字符串的正则表达式。
MED		指定用于路由过滤的 MED 值（范围为 0-4,294,967,295）。
路由表		指定要有条件通告匹配的路由时防火墙使用的路由表：**unicast**（单播）、**multicast**（多播）或 **both**（两者）。
地址前缀		如果首选路由不可用，可以为要通告的路由 **Add**（添加）确切的网络层可达性信息 (NLRI) 前缀。
下一个跃点		指定用于路由过滤的下一个跃点路由器或子网。
从对端		指定用于路由过滤的对端路由器。

BGP 聚合选项卡

- 网络 > 虚拟路由器 > BGP > 聚合

路由聚合是为了减少防火墙必须发送的路由通告，并减少路由表中的路由记录，而将特定路由（前缀较长）组合成单个路由（前缀较短）的行为。

© 2019 Palo Alto Networks, Inc.

BGP 聚合设置	配置位置	说明
姓名	**BGP** > 聚合	输入聚合规则的名称。
前缀		输入将用于聚合较长前缀的摘要前缀（IP 地址/前缀长度）。
启用		选择以启用此路由聚合。
Summary（摘要）		选择以汇总路由。
AS 集合		为此聚合规则选择以促使防火墙在聚合路由的 AS 路径中包括一组 AS 编号（AS 集）。AS 集是来自聚合的各个路由的原始 AS 编号的无序列表。
姓名	**BGP** > **Aggregate**（聚合）> **Suppress Filters**（禁止筛选程序）	定义用于禁止相匹配的路由的属性。单击 **Add**（添加），然后输入禁止过滤器的名称。
启用		选择以启用禁止过滤器。
AS 路径正则表达式		指定 AS_PATH 的正则表达式以过滤将要聚合的路由，如 ^5000 表示来自 AS 5000 的路由。
社区正则表达式		指定社区的正则表达式以过滤将要聚合的路由，如 500:.* 与使用 500:x 过滤的社区匹配。
扩展的社区正则表达式		指定扩展社区的正则表达式以过滤要聚合的路由。
MED		指定 MED 以过滤要聚合的路由。
路由表		指定用于应禁止的聚合路由的路由表（未通告）：**unicast**（单播）、**multicast**（多播）或 **both**（两者）。
地址前缀		输入要禁止通告的 IP 地址。
下一个跃点		输入要禁止的 BGP 前缀的下一个跃点地址。
从对端		输入收到（要禁止的）BGP 前缀的对端 IP 地址。
姓名	**BGP** > **Aggregate**（聚合）> **Suppress Filters**（禁止筛选程序）	定义通告过滤器的属性，促使防火墙向对端通告与过滤器相匹配的任何路由。单击 **Add**（添加），然后输入通告过滤器的名称。
启用		选择以启用此通告过滤器。
AS 路径正则表达式		指定 AS_PATH 的正则表达式以过滤要通告的路由。
社区正则表达式		指定社区的正则表达式以过滤要通告的路由。
扩展的社区正则表达式		指定扩展社区的正则表达式以过滤要通告的路由。
MED		指定 MED 值以过滤要通告的路由。

© 2019 Palo Alto Networks, Inc.

BGP 聚合设置	配置位置	说明
路由表		指定用于聚合路由的通告过滤器的路由表：**unicast**（单播）、**multicast**（多播）或 **both**（两者）。
地址前缀		输入希望 BGP 通告的 IP 地址。
下一个跃点		输入希望 BGP 通告的 IP 地址的下一个跃点地址。
从对端		输入从中收到希望 BGP 通告的前缀的对端 IP 地址。
	BGP > **Aggregate**（聚合）> **Aggregate Route Attributes**（聚合路由属性）	定义聚合路由的属性。
本地首选项		本地首选项范围为 0-4,294,967,295。
MED		多出口鉴别范围为 0-4,294,967,295。
重量		重量范围为 0-65,535。
下一个跃点		下一个跃点 IP 地址。
原始		路由的起点：**igp**、**egp** 或 **incomplete**（未完成）。
AS 路径限制		AS 路径限制范围为 1-255。
AS 路径		选择类型：**None**（无）或 **Prepend**（预先设置）。
社区		选择类型：**None**（无）、**Remove All**（删除全部）、**Remove Regex**（删除正则表达式）、**Append**（追加）或 **Overwrite**（覆盖）。
扩展的社区		选择类型：**None**（无）、**Remove All**（删除全部）、**Remove Regex**（删除正则表达式）、**Append**（追加）或 **Overwrite**（覆盖）。

BGP 重新分发规则选项卡

- 网络 > 虚拟路由器 > BGP > 重新分发规则

按下表中所述配置设置以创建重新分发 BGP 路由的规则。

BGP 重新分发规则设置	配置位置	说明
允许再分发默认路由	**BGP** > 重新分发规则	允许防火墙将其默认路由重新分发到 BGP 对端。
姓名		**Add**（添加）IP 子网或首先创建重新分发规则。
启用		选择以启用此重新分发规则。
路由表		指定将路由重新分发到的路由表：**unicast**（单播）、**multicast**（多播）或 **both**（两者）。

© 2019 Palo Alto Networks, Inc.

BGP 重新分发规则设置	配置位置	说明
指标		输入跃点数，范围为 1-65,535。
设置原始值		选择重新分发路由的源点（**igp**、**egp** 或 **incomplete**（未完成））。值 **incomplete**（未完成）表示连接的路由。
设置 MED		输入重新分发路由的 MED，范围为 0-4,294,967,295。
设置本地首选项		输入重新分发路由的本地首选项，范围为 0-4,294,967,295。
设置 AS 路径限制		输入重新分发路由的 AS 路径限制，范围为 1-255。
设置社区		选择或输入 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 之间。最多输入 10 个社区。
设置扩展的社区		输入 64 位值，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。最多输入五个扩展社区。

IP 多播

- 网络 > 虚拟路由器 > 多播

配置多播协议需要配置以下标准设置：

多播设置	说明
启用	选中此选项可启用多播路由。

此外，还必须配置以下选项卡上的设置：

- **Rendezvous Point**（集合点）：请参阅多播集合点选项卡。
- **Interfaces**（接口）：请参阅多播接口选项卡。
- **SPT Threshold**（**SPT** 阈值）：请参阅多播 SPT 阈值选项卡。
- **Source Specific Address Space**（特定源地址空间）：请参阅多播特定源地址选项卡。
- 高级：请参阅多播高级选项卡。

多播集合点选项卡

- Network（网络）> Virtual Router（虚拟路由器）> Multicast（多播）> Rendezvous Point（集合点）

使用以下字段配置 IP 多播集合点：

多播设置 — 集合点	说明
RP 类型	选择此虚拟路由器上将运行的集合点 (RP) 的类型。必须在其他 PIM 路由器上显式配置静态 RP，但自动选择候选 RP。 • **None**（无）— 如果没有 RP 在此虚拟路由器上运行，则选择此项。

© 2019 Palo Alto Networks, Inc.

多播设置 — 集合点	说明

	• **Static**（静态）— 为 RP 指定静态 IP 地址，然后从下拉列表中选择 **RP Interface**（**RP** 接口）和 **RP Address**（**RP** 地址）的选项。如果要使用指定的 RP 而非为此组选择的 RP，则选择 **Override learned RP for the same group**（替代相同组的已获知的 **RP**）。
	• 待选— 为在此虚拟路由器上运行的候选 RP 指定以下信息。
	  • **RP** 接口— 选择 RP 的接口。有效的接口类型包括回环、L3、VLAN、聚合以太网和隧道。
	  • **RP** 地址— 选择 RP 的 IP 地址。
	  • 优先级— 指定候选 RP 消息的优先级（默认为 192）。
	  • 通告间隔— 指定通告候选 RP 消息之间的时间间隔。
	• 组列表— 如果选择静态或待选，则单击添加可指定建议将此候选 RP 作为其 RP 的组的列表。

远程集合点	单击添加，并指定以下项： • **IP** 地址— 指定 RP 的 IP 地址。 • **Override learned RP for the same group**（替代相同组的已获知的 **RP**）— 选择此选项将使用指定的 RP 而非为此组选择的 RP。 • 组— 指定所指定地址将充当其 RP 的组的列表。

多播接口选项卡

- 网络 > 虚拟路由器 > 多播 > 接口

使用以下字段配置共享 IGMP、PIM 和组权限设置的多播接口：

多播设置 — 接口	说明
姓名	输入名称以标识接口组。
说明	输入可选说明。
接口	**Add**（添加）属于接口组的一个或多个防火墙接口，因此共享多播组权限、IGMP 设置和 PIM 设置。
组权限	指定参与 PIM 任意源多播 (ASM) 或 PIM 特定源多播 (SSM) 的多播组： • **Any Source**（任意源）— **Add**（添加）一个 **Name**（名称）以标识允许从接口组中的接口上的任何源接收多播通信的多播 **Group**（组）。默认情况下，组 **Included**（包含）在 **Any Source**（任意源）列表中。取消选中 **Included**（包含）可在不删除组配置的情况下轻松排除组。 • **Source Specific**（特定源）— 为允许接口组中的接口上的多播通信的多播 **Group**（组）和 **Source**（源） IP 地址 **Add**（添加）一个 **Name**（名称）。默认情况下，Group（组）和 Source（源）对 **Included**（包含）在 Source Specific（特定源）列表中。取消选中 **Included**（包含）可在不删除配置的情况下轻松排除 Group（组）和 Source（源）对。
IGMP	指定 IGMP 通信的设置。必须为面向多播接收器的接口启用 IGMP。 • **Enable**（启用）— 选择此选项可启用 IGMP 配置。 • **IGMP** 版本— 选择在接口上运行版本 1、2 或 3。

© 2019 Palo Alto Networks, Inc.

多播设置 — 接口	说明

	• **Enforce Router-Alert IP Option**（强制路由器-警报 **IP** 选项）— 对于 IGMPv2 或 IGMPv3，选择此选项将需要 router-alert IP 选项。要与 IGMPv1 兼容，必须禁用此选项。
	• **Robustness**（稳定）— 选择一个整数值以表示网络上的丢包情况（范围为 1-7，默认为 2）。如果经常丢包，则选择较高的值。
	• **Max Sources**（最大源数）— 指定接口组允许的最大源特定成员身份数量（范围为 1-65,535 或 **unlimited**（无限））。
	• **Max Groups**（最大组数）— 指定此接口组允许的最大多播组数量（范围为 1-65,535 或 **unlimited**（无限））。
	• 查询配置— 指定以下各项：
	  • **Query interval**（查询间隔）— 指定向所有接收器发送常规查询的时间间隔。
	  • **Max Query Response Time**（最长查询响应时间）— 指定接收器中常规查询与响应之间的最长时间。
	  • 最后一个成员查询间隔 — 指定组或源特定查询消息（包括为响应离组消息而发送的消息）之间的时间间隔。
	  • **Immediate Leave**（立即离开）— 选择此选项可在收到离开消息后立即离开组。

PIM 配置	指定协议无关多播 (PIM) 设置： • **Enable**（启用）— 选择该选项将允许此接口接收和/或转发 PIM 消息必须启用接口才能转发多播通信。 • **Assert Interval**（声明间隔）— 指定 PIM 声明消息之间的时间间隔以选择 PIM 转发器。 • 呼叫间隔— 指定 PIM 呼叫消息之间的时间间隔。 • **Join Prune Interval**（加入修剪间隔）— 指定 PIM 加入消息（以及 PIM 修剪消息）之间的秒数，默认为 60。 • **DR Priority**（**DR** 优先级）— 指定此接口的指派路由器优先级 • **BSR Border**（**BSR** 边界）— 选择此选项可使用接口作为自举路由器。 • **PIM Neighbors**（**PIM** 邻居）— **Add**（添加）将使用 PIM 进行通信的邻居的列表。

多播 *SPT* 阈值选项卡

- 网络 > 虚拟路由器 > 多播 > SPT 阈值

最短路径树 (SPT) 阈值定义虚拟路由器将多播组或前缀的多播路由从共享树分发（源自集合点）切换到源树（也称为最短路径树或 SPT）的点。为多播组或前缀 **Add**（添加）一个 SPT 阈值。

SPT 阈值	说明
多播组/前缀	当组或前缀的吞吐量达到阈值设置时，指定多播路由切换到其 SPT 分发的多播地址或前缀。
阈值 **(kbps)**	选择一个设置，以指定多播路由切换到相应多播组或前缀的 SPT 分发点： • **0**（打开第一个数据包）—（默认）当组或前缀的多播数据包到达时，虚拟路由器切换到 SPT 分发。

© 2019 Palo Alto Networks, Inc.

SPT 阈值	说明
	• 从不（不切换到 **SPT**）—虚拟路由器继续将多播通信转发到共享树下的该组或前缀。 • 输入可以在任何接口和任何时间段内到达相应多播组或前缀的多播数据包的千比特总数（范围为 1-4,294,967,295）。当吞吐量达到这个数值时，虚拟路由器切换到 SPT 分发。

多播特定源地址空间选项卡

- 网络 > 虚拟路由器 > 多播 > 特定源地址空间

Add（添加）只能从特定源接收多播数据包的多播组。您指定的这些多播组和名称与 **Multicast**（多播）> **Interfaces**（接口）> **Group Permissions**（组权限）选项卡上的 Source Specific（特定源）相同。

多播设置 — 特定源地址空间	说明
姓名	标识防火墙将为其提供特定源多播 (SSM) 服务的多播组。
群组	指定只能接受来自特定源的多播数据包的多播组地址。
包括	选择此选项可在 SSM 地址空间中包括多播组。

多播高级选项卡

- Network（网络）> Virtual Router（虚拟路由器）> Multicast（多播）> Advanced（高级）

配置会话结束后多播路由保留在路由表中的时间长度。

多播高级设置	说明
路由年龄超时（秒）	让您可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，范围为 210-7200，默认为 210）。

ECMP

- Network（网络）> Virtual Routers（虚拟路由器）> Router Settings（路由器设置）> 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。
- 充分利用所有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，流量会动态转移到同一目标的另一个 ECMP 成员，而不是等待路由协议或 RIB 表选定替代路径，这可以帮助当链路出现故障时减少停机时间。

ECMP 负载平衡为会话级操作，而非数据包级操作。这意味着防火墙会在新会话开始时选择等成本路径，而不是在防火墙每次收到数据包时选择。

© 2019 Palo Alto Networks, Inc.

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。

要为虚拟路由器配置 ECMP，请选择一个虚拟路由器，然后针对 **Router Settings**（路由器设置）选择 **ECMP** 选项卡并按照所述配置 ECMP 设置。

您在查找什么内容？	请参阅：
哪些字段可用于配置 ECMP？	ECMP 设置
了解更多？	ECMP

ECMP 设置

- Network（网络）> Virtual Routers（虚拟路由器）> Router Settings（路由器设置）> ECMP

使用以下字段配置等价多路径 (ECMP) 设置。

ECMP 设置	说明
启用	**Enable**（启用）ECMP。 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，这有时会导致现有会话终止。
对称返回	（可选）单击 **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。这会将防火墙配置为使用接收接口来发送返回数据包，而不是使用 ECMP 接口，这意味着 **Symmetric Return**（对称返回）设置优先于负载平衡。该行为仅适用于从服务器到客户端的通信流。
严格源路径	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。选择 **Strict Source Path**（严格源路径），确保源自防火墙的 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，就可以启用严格源路径。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 默认会根据所配置的 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**Strict Source Path**（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。
最大路径	选择等成本路径的最大数：可从 RIB 复制到 FIB 的至目标网络的（2、3 或 4）（默认为 2）。
方法	选择以下任一 ECMP 负载平衡算法以用于虚拟路由器。ECMP 负载平衡为会话级操作，而非数据包级操作。这意味着，防火墙 (ECMP) 会在新会话开始时选择等成本路径，而不是在每次收到数据包时选择。 • **IP Modulo**（**IP** 模）（默认）— 虚拟路由器负载均衡会话使用数据包标头中的源和目标 IP 地址的散列来确定要使用的 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：

© 2019 Palo Alto Networks, Inc.

ECMP 设置	说明
	• 如果选择 **IP Hash**（**IP** 哈希），防火墙默认使用源 IP 地址和目标 IP 地址的哈希。 • 如果 **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），那么，防火墙可确保属于同一源 IP 地址的所有会话始终使用相同的路径。 • 如果还 **Use Source/Destination Ports**（使用源/目标端口），那么，防火墙可将端口包含在任一哈希计算中。还可以输入 **Hash Seed**（哈希种子）值（整数），以进一步实现负载平衡的随机化。 • **Weighted Round Robin**（加权循环调度）— 您可以使用此算法可将不同链路容量和速度纳入考虑范围。选择此算法后，接口对话框即会打开。**Add**（添加）并选择要纳入加权循环调度组的**Interface**（接口）。针对各个接口，输入要用于该接口的 **Weight**（权重）。（范围为 1-255；默认为 100）。特定等成本路径的权重越高，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。然后，您可以 **Add**（添加）另一接口和权重。 • **Weighted Round Robin**（加权循环调度）— 将传入 ECMP 会话平均分布到各个链路上。

有关虚拟路由器的更多运行时统计数据

配置虚拟路由器的静态路由或路由协议后，请选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择最后一列中的 **More Runtime Stats**（更多运行时统计数据）以查看有关虚拟路由器的详细信息，如路由表、转发表、路由协议和配置的静态路由。这些窗口可以提供比适合虚拟路由器的单个屏幕更多的信息。该窗口会显示以下选项卡：

- **Routing**（路由）：请参阅路由选项卡。
- **RIP**:请参阅 RIP 选项卡。
- **BGP**:请参阅 BGP 选项卡。
- **Multicast**（多播）:请参阅多播选项卡。
- **BFD Summary Information**（**BFD** 摘要信息）：请参阅 BFD 摘要信息选项卡。

“路由”选项卡

下表将介绍虚拟路由器的路由表、转发表和静态路由监控表的运行时统计数据。

运行时统计数据	说明
路由表	
路由表	选择 **Unicast**（单播）或 **Multicast**（多播）可显示单播或多播路由表。
显示地址系列	选择 **IPv4 Only**（仅限 **IPv4**）、**IPv6 Only**（仅限 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）（默认值）可控制要在表中显示的地址组。
目标	虚拟路由器可访问的网络的 IPv4 地址和网络掩码或 IPv6 地址和前缀长度。
下一个跃点	至目标网络的下一个跃点上的设备的 IP 地址。如果下一个跃点为 0.0.0.0，即是指默认路由。

© 2019 Palo Alto Networks, Inc.

运行时统计数据	说明
指标	路由的跃点数。当路由协议使用多个至同一目标网络的路由时，会优先选择跃点数值最低的路由。各路由协议使用不同类型的跃点数；例如 RIP 使用跃点计数。
重量	路由的权重。例如，当 BGP 使用多个至同一目标的路由时，会优先选择最高权重的路由。
Flags（标记）	• **A?B** — 处于活动状态，且通过 BGP 获得 • **A C** — 处于活动状态，且是根据某个内部接口（已连接）得出的结果 - 目标 = 网络 • **A H** — 处于活动状态，且是根据某个内部接口（已连接）得出的结果 - 目标 = 仅主机 • **A R** — 处于活动状态，且通过 RIP 获得 • **A S** — 处于活动状态，且为静态 • **S** — 处于非活动状态（因为该路由的跃点数较大），且为静态 • **O1** — OSPF 外部类型 1 • **O2** — OSPF 外部类型 2 • **Oi** — OSPF 区域内 • **Oo** — OSPF 区域间
年龄	路由表中的路由条目的年龄。静态路由没有年龄。
接口	将用于访问下一个跃点的虚拟路由器的出口接口。
刷新	单击此选项可刷新表中的运行时统计数据。

转发表

防火墙从至特定目标网络的路由表 *(RIB)* 中选择最佳路由，以放入 *FIB* 中。

显示地址系列	选择 **IPv4 Only**（仅限 **IPv4**）、**IPv6 Only**（仅限 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）（默认值）可控制要显示的路由表。
目标	虚拟路由器可访问的，可从路由表选择的网络的最佳 IPv4 地址和网络掩码，或 IPv6 地址和前缀长度。
下一个跃点	至目标网络的下一个跃点上的设备的 IP 地址。如果下一个跃点为 0.0.0.0，即是指默认路由。
Flags（标记）	• **u** — 路由已激活。 • **h** — 路由目标是主机。 • **g** — 路由目标是网关。 • **e** — 防火墙使用等成本多路径 (ECMP) 选择路由。 • * — 路由是至目标网络的首选路径。
接口	虚拟路由器访问下一个跃点所使用的 Egress 接口。
MTU	最大传输单元 (MTU)；防火墙以单个 TCP 数据包的形式向此目标传输的最大字节数。
刷新	单击此选项可刷新表中的运行时统计数据。

© 2019 Palo Alto Networks, Inc.

运行时统计数据	说明
静态路由监控	
目标	虚拟路由器可访问的网络的 IPv4 地址和网络掩码或 IPv6 地址和前缀长度。
下一个跃点	至目标网络的下一个跃点上的设备的 IP 地址。如果下一个跃点为 0.0.0.0，即是指默认路由。
指标	路由的跃点数。当有多个至同一目标网络的静态路由时，防火墙会优先选择跃点数值最低的路由。
重量	路由的权重。
Flags（标记）	• **A?B** — 处于活动状态，且通过 BGP 获得 • **A C** — 处于活动状态，且是根据某个内部接口（已连接）得出的结果 - 目标 = 网络 • **A H** — 处于活动状态，且是根据某个内部接口（已连接）得出的结果 - 目标 = 仅主机 • **A R** — 处于活动状态，且通过 RIP 获得 • **A S** — 处于活动状态，且为静态 • **S** — 处于非活动状态（因为该路由的跃点数较大），且为静态 • **O1** — OSPF 外部类型 1 • **O2** — OSPF 外部类型 2 • **Oi** — OSPF 区域内 • **Oo** — OSPF 区域间
接口	将用于访问下一个跃点的虚拟路由器的出口接口。
路径监视(未启用)	如果为此静态路由启用路径监控，则 Fail On（未启用）表示： • **All**（所有）— 防火墙认为静态路由处于停用状态，并且在静态路由的所有受监控目标处于停用状态时会进行故障转移。 • **Any**（任何）— 防火墙认为静态路由处于停用状态，并且在静态路由的任一受监控目标处于停用状态时会进行故障转移。 如果对静态路由禁用路径监控，则 Fail On（未启用）表示禁用。
状态	基于 ICMP ping 的至受监控目标的静态路由的状态：**Up**（激活）、**Down**（停用），或 **Disabled**（禁用）静态路由的路径监控。
刷新	刷新表中的运行时统计数据。

RIP 选项卡

下表将介绍虚拟路由器的 RIP 运行时统计数据。

RIP 运行时统计数据	说明
摘要选项卡	

© 2019 Palo Alto Networks, Inc.

RIP 运行时统计数据	说明
间隔(秒)	间隔时间（以秒为单位）。RIP 使用此值（特定时长）控制其更新、到期和删除间隔。
更新间隔	虚拟路由器发送到对端设备的 RIP 路由通告更新之间相隔的间隔数。
到期间隔	自虚拟路由器从对端设备接收到最后一个更新后，在虚拟路由器将来自对端设备的路由标记为不可使用之前，所经历的间隔数。
删除间隔	在路由被标记为不可用后，防火墙在未收到更新的情况下从路由表删除该路由之前所经历的间隔数。
接口选项卡	
地址	虚拟路由器上启用了 RIP 的接口的 IP 地址。
身份验证类型	身份验证的类型：简单密码、MD5 或无。
允许发送	选中标记表示允许该接口发送 RIP 数据包。
允许接收	选中标记表示允许该接口接收 RIP 数据包。
通告默认路由	选中标记表示 RIP 将向其对端通告其默认路由。
默认路由跃点数	分配给默认路由的跃点数（跃点计数）。跃点数值越小，其在路由表中被选为首选路径的优先级就越高。
密钥 ID	用于对端的身份验证密钥。
首选	身份验证的首选密钥。
对端选项卡	
对等地址	虚拟路由器 RIP 接口的对端的 IP 地址。
最后更新	从该对端收到上一个更新时的日期和时间。
RIP 版本	对端正在运行的 RIP 版本。
数据包无效	从该对端收到无效数据包的计数。有关防火墙无法解析 RIP 数据包的可能原因：超过路由边界 x 个字节，数据包中的路由过多，子网有问题，地址非法，身份验证失败，或是内存不足。
路由无效	从该对端收到无效路由的计数。可能的原因：路由无效，导入失败，或是内存不足。

BGP 选项卡

下表将介绍虚拟路由器的 BGP 运行时统计数据。

© 2019 Palo Alto Networks, Inc.

BGP 运行时统计数据	说明
摘要选项卡	
路由器 ID	分配给 BGP 实例的路由器 ID。
拒绝默认路由	指明“拒绝默认路由”选项是否已配置，该选项会使 VR 忽略 BGP 对端通告的任何默认路由。
重新分发默认路由	指明“允许重新分发默认路由”选项是否已配置。
安装路由	指明“安装路由”选项是否已配置，该选项会使 VR 安装全局路由表中的 BGP 路由。
平稳重新启动	指明“平稳重新启动”是否已启用（支持）。
AS 大小	指明所选的 AS 格式大小是 2 个字节还是 4 个字节。
本地 AS	VR 从属的 AS 的编号。
本地成员 AS	本地成员 AS 的编号（仅当 VR 在某个联合内时才有效）。如果 VR 不在任何联合内，此字段为 0。
集群 ID	显示已配置的反射器群集 ID。
默认本地首选项	显示已为 VR 配置的默认本地首选项。
始终比较 Med	指明“始终比较 MED”选项是否已配置，该选项会启用比较，以便在源自不同自治系统中邻居的路由之间进行选择。
聚合(不管 MED)	指明“聚合 MED”选项是否已配置，该选项会启用路由聚合，即使路由的 MED 值不同。
确定性 MED 处理	指明“确定性 MED 比较”选项是否已配置，该选项会启用 MED 比较，以便在 IBGP 对端（同一 AS 中的 BGP 对端）通告的路由之间进行选择。
当前 RIB 输出条目	“RIB 输出”表中的条目数。
RIB 峰值条目	任何一次分配的 Adj-RIB-Out 路由的峰值数量。
对端选项卡	
姓名	对等的名称。
群组	该对端从属的对端组的名称。
本地 IP	VR 上的 BGP 接口的 IP 地址。
对等 IP	对端的 IP 地址。
对等 AS	对端从属的自治系统。
密码集合	使用“是”或“否”指明是否已设置身份验证。

© 2019 Palo Alto Networks, Inc.

BGP 运行时统计数据	说明
STATUS（状态）	对端的状态，如：活动、连接、已建立、空闲、OpenConfirm 或 OpenSent。
状态持续时间(秒)	对端状态的持续时间。
“对端组”选项卡	
组名称	对端组的名称。
类型	已配置的对端组的类型，如 EBGP 或 IBGP。
聚合联合AS	使用“是”或“否”指明“聚合联合 AS”选项是否已配置。
软重置支持	使用“是”或“否”指明对端组是否支持软重置。当 BGP 对端的路由策略更改时，路由表更新可能会受影响。BGP 会话的软重置优先于硬重置，因为软重置允许路由表在不清除 BGP 会话的情况下进行更新。
下一个跃点本身	使用“是”或“否”指明该选项是否已配置。
下一个跃点第三方	使用“是”或“否”指明该选项是否已配置。
删除专用 AS	指明更新在被发送之前是否会从 AS_PATH 属性中删除专用 AS 编号。
本地 RIB 选项卡	
前缀	本地路由信息库中的网络前缀和子网掩码。
标记	* 指明是否已将路由选作最佳 BGP 路由。
下一个跃点	至前缀的下一个跃点的 IP 地址。
对等	对端的名称。
重量	已分配给前缀的权重属性。如果防火墙拥有至同一前缀的多个路由，则权重最高的路由会安装在 IP 路由表中。
本地首选项	路由的本地首选项属性，用于在有多个出口时选择至前缀的出口。优先级较高的本地首选项优先于优先级较低的本地首选项。
AS 路径	会列出至前缀网络的路径中的自治系统；该列表会在 BGP 更新中通告。
原始	前缀的原始属性；BGP 获得路由的方式。
MED	路由的多出口鉴别 (MED) 属性。MED 是路由的一个度量属性，由通告路由的 AS 向外部 AS 推荐。较小的 MED 优先于较大的 MED。
翻动计数	路由的标记数量。
RIB Out 选项卡	
前缀	路由信息库中的网络路由条目。

© 2019 Palo Alto Networks, Inc.

BGP 运行时统计数据	说明
下一个跃点	至前缀的下一个跃点的 IP 地址。
对等	VR 会将该路由通告至的对端。
本地首选项	用于访问前缀的本地首选项属性，用于在有多个出口时选择至前缀的出口。优先级较高的本地首选项优先于优先级较低的本地首选项。
AS 路径	会列出至前缀网络的路径中的自治系统。
原始	前缀的原始属性；BGP 获得路由的方式。
MED	前缀的多出口鉴别 (MED) 属性。MED 是路由的一个度量属性，由通告路由的 AS 向外部 AS 推荐。较小的 MED 优先于较大的 MED。
通告STATUS（状态）	路由的通告状态。
聚合STATUS（状态）	指明该路由是否已与其他路由聚合。

“多播”选项卡

下表将介绍虚拟路由器的 IP 多播运行时统计数据。

多播运行时统计数据	说明
FIB 选项卡	
群组	转发信息库中的路由条目 (FIB)；虚拟路由器将数据包转发到的多播组地址。
源	组的多播数据包的源地址。
传入接口	组的多播数据包到达的接口。
传出接口	虚拟路由器将组的多播数据包向外转发的接口。
IGMP 接口选项卡	
接口	已启用 IGMP 的接口。
版本	虚拟路由器上运行的第 1、2 或 3 版互联网组管理协议 (IGMP)。
查询器	连接到接口的多路访问段上的 IGMP 查询器 IP 地址。
查询器正常运行时间	IGMP 查询器已运行的秒数。
查询器到期时间	“其他查询器出现”计时器到期之前的剩余秒数。
稳定	IGMP 接口的“稳定”变量。
组限制	IGMP 可以同时处理的每个接口的最大组数。

© 2019 Palo Alto Networks, Inc.

多播运行时统计数据	说明
源限制	IGMP 可以同时处理的每个接口的最大源数。
立即离开	使用“是”或“否”指明“立即离开”是否已配置。“立即离开”表明虚拟路由器将在不发送接口 IGMP 组特定查询的情况下从转发表中删除接口。
IGMP 成员选项卡	
接口	属于组的接口的名称。
群组	接口所属多播组的地址。
源	将多播数据包发送到组的源的 IP 地址。
运行时间	该成员身份已运行的秒数。
到期时间	成员身份到期前的剩余秒数。
过滤模式	包括或排除源。虚拟路由器会配置为包括所有通信、仅限来自该源的通信（包括）或是来自该源之外的任意源的通信（排除）。
排除到期	接口“排除”状态到期之前的剩余秒数。
V1 主机计时器	在本地路由器做出如下假设之前的剩余时间：IP 子网上不会再有任何 IGMP 第 1 版成员与该接口相连。
V2 主机计时器	在本地路由器做出如下假设之前的剩余时间：IP 子网上不会再有任何 IGMP 第 2 版成员与该接口相连。
PIM 组映射子选项卡	
群组	已映射至集合点的组的 IP 地址。
RP	组的集合点的 IP 地址。
原始	指明虚拟路由器获得 RP 的位置。
PIM 模式	ASM 或 SSM。
非活动	指明组至 RP 的映射是否处于非活动状态。
PIM 接口选项卡	
接口	参与 PIM 的接口的名称。
地址	接口的 IP 地址。
DR	连接到接口的多路访问段上的指定路由器 IP 地址。
呼叫间隔	已配置的呼叫间隔（以秒为单位）。

© 2019 Palo Alto Networks, Inc.

多播运行时统计数据	说明
加入/修剪间隔	配置用于加入和修剪消息之间的间隔（秒）。
断言间隔	配置用于虚拟路由器发送断言消息的 PIM 断言间隔（秒）。PIM 使用断言机制启动选择用于多路访问网络的 PIM 转发器。
DR 优先级	配置用于连接到接口的多路访问段上的指定路由器优先级。
BSR 边界	使用“是”或“否”指明接口是否位于作为企业 LAN 边界的自举路由器 (BSR) 的虚拟路由器上。
PIM 邻居选项卡	
接口	虚拟路由器中接口的名称。
地址	从接口可访问的 PIM 邻居的 IP 地址。
辅助地址	从接口可访问的 PIM 邻居的辅助 IP 地址。
运行时间	邻居已运行的时间长度。
到期时间	在邻居因虚拟路由器未收到来自邻居的呼叫数据包而要到期之前的剩余时间长度。
生成 ID	每次在接口上启动或重新启动 PIM 转发时（包括路由器自身重启时）重新生成的随机生成的 32 位值。
DR 优先级	虚拟路由器通过上一个 PIM 呼叫消息从该邻居那里接收到的指定路由器优先级。

BFD 摘要信息选项卡

BFD 摘要信息包括以下数据。

BFD 摘要信息运行时统计信息	说明
接口	正在运行 BFD 的接口。
协议	静态路由（静态路由的 IP 地址系列）或正在接口上运行 BFD 的动态路由协议。
本地 IP 地址	配置 BFD 的接口的 IP 地址。
邻居 IP 地址	BFD 邻居的 IP 地址。
状态	本地和远程 BFD 对端的 BFD 状态：**admin down**（管理员关闭）、**down**（关闭）、**init**（启动）或 **up**（启动）。
运行时间	BFD 已经启动的时间长度（小时、分钟、秒和毫秒）。
鉴别（本地）	本地 BFD 对端的鉴别。鉴别是对端用于区分它们之间多个 BFD 会话的独特非零值。

© 2019 Palo Alto Networks, Inc.

BFD 摘要信息运行时统计信息	说明
鉴别（远程）	远程 BFD 对端的鉴别。
错误	BFD 错误数。
会话详细信息	单击 **Details**（详细信息）可查看会话的 BFD 信息，如本地和远程邻居的 IP 地址、上次接收的远程诊断代码、发送和接收的控制数据包数、错误数和有关导致状态发生变化的最后一个数据包的信息等。

有关逻辑路由器的更多运行时统计数据

配置逻辑路由器的静态路由或路由协议后，请选择 **Network**（网络）> **Logical Routers**（逻辑路由器），然后选择最后一列中的 **More Runtime Stats**（更多运行时统计数据）以查看有关逻辑路由器的详细信息，如路由表、转发表、路由协议和配置的静态路由。这些窗口可以提供比适合逻辑路由器的单个屏幕更多的信息。该窗口会显示以下选项卡：

- 逻辑路由器的路由统计数据
- 逻辑路由器的 BGP 统计数据

逻辑路由器的路由统计数据

下表将介绍逻辑路由器的路由表、转发表和静态路由监控表的运行时统计数据。

运行时统计数据	说明
路由表	
显示地址系列	选择 **IPv4 Only**（仅限 **IPv4**）、**IPv6 Only**（仅限 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）（默认值）可控制要在表中显示的地址组。
目标	逻辑路由器可访问的网络的 IPv4 地址和网络掩码或 IPv6 地址和前缀长度。
下一个跃点	至目标网络的下一个跃点上的设备的 IP 地址。如果下一个跃点为 0.0.0.0，即是指默认路由。
协议	指示该路由是静态路由还是连接路由，还是通过 BGP 获知的路由。
指标	路由的跃点数。当路由协议使用多个至同一目标网络的路由时，会优先选择跃点数值最低的路由。各路由协议使用不同类型的跃点数；例如 RIP 使用跃点计数。
已选择	如果启用，该字段为 true；如果禁用，则为空。
年龄	路由表中的路由条目的年龄。
活跃	如果启用，该字段为 true；如果禁用，则为空。

© 2019 Palo Alto Networks, Inc.

运行时统计数据	说明
接口	将用于访问下一个跃点的逻辑路由器的出口接口。
刷新	单击此选项可刷新表中的运行时统计数据。
转发表	
防火墙从至特定目标网络的路由表 *(RIB)* 中选择最佳路由，以放入 *FIB* 中。	
目标	逻辑路由器可访问的，可从路由表选择的网络的最佳 IPv4 地址和网络掩码，或 IPv6 地址和前缀长度。
下一个跃点	至目标网络的下一个跃点上的设备的 IP 地址。如果下一个跃点为 0.0.0.0，即是指默认路由。
MTU	最大传输单元 (MTU)；防火墙以单个 TCP 数据包的形式向此目标传输的最大字节数。
Flags（标记）	• **u** — 路由已激活。 • **h** — 路由目标是主机。 • **g** — 路由目标是网关。 • **e** — 防火墙使用等成本多路径 (ECMP) 选择路由。 • * — 路由是至目标网络的首选路径。
接口	逻辑路由器访问下一个跃点所使用的出口接口。
静态路由监控	
目标	逻辑路由器可访问的网络的 IPv4 地址和网络掩码或 IPv6 地址和前缀长度。
下一个跃点	至目标网络的下一个跃点上的设备的 IP 地址。如果下一个跃点为 0.0.0.0，即是指默认路由。
指标	路由的跃点数。当有多个至同一目标网络的静态路由时，防火墙会优先选择跃点数值最低的路由。
接口	将用于访问下一个跃点的逻辑路由器的出口接口。
路径监视(未启用)	如果为此静态路由启用路径监控，则 Fail On（未启用）表示： • **All**（所有）— 防火墙认为静态路由处于停用状态，并且在静态路由的所有受监控目标处于停用状态时会进行故障转移。 • **Any**（任何）— 防火墙认为静态路由处于停用状态，并且在静态路由的任一受监控目标处于停用状态时会进行故障转移。 如果对静态路由禁用路径监控，则 Fail On（未启用）表示禁用。
状态	基于 ICMP ping 的至受监控目标的静态路由的状态：**Up**（激活）、**Down**（停用），或 **Disabled**（禁用）静态路由的路径监控。

© 2019 Palo Alto Networks, Inc.

运行时统计数据	说明
刷新	刷新表中的运行时统计数据。

逻辑路由器的 *BGP* 统计数据

下表列出了逻辑路由器的 BGP 运行时统计数据。

BGP 运行时统计数据	说明
摘要选项卡	
已启用	BGP 已启用：是或否。
路由器 ID	逻辑路由器的路由器 ID。
本地 AS	逻辑路由器所属的 AS。
强制执行第一个 AS	如果启用，该字段为 true；如果未启用，则为空。
快速外部故障转移	如果启用，该字段为 true；如果未启用，则为空。
默认本地首选项	已配置的默认本地首选项。
平稳重新启动	如果启用，该字段为 true；如果未启用，则为空。
最长对等重启时间（秒）	为平稳重启的最长对等重启时间配置的秒数。
失效路由时间（秒）	为平稳重启的失效路由时间配置的秒数。
始终比较 Med	如果启用，该字段为 true；如果未启用，则为空。
确定性 MED 比较	如果启用，该字段为 true；如果未启用，则为空。
对端选项卡	
姓名	对等的名称。
Peer Group（对等组）	该对端从属的对端组的名称。
本地 IP	逻辑路由器 BGP 接口的 IP 地址。
本地 AS	本地 BGP 防火墙所属的 AS。
对等 IP	对端的 IP 地址。
远程 AS	对等所属的 AS。
上行/下行	对等为上行或下行。
状态	已建立

© 2019 Palo Alto Networks, Inc.

BGP 运行时统计数据	说明
“对端组”选项卡	
姓名	对端组的名称。
类型	已配置的对等组类型，如 EBGP 或 IBGP。
保持活动状态（秒）	保持活动状态的时间（秒）。
保持时间（秒）	以秒为单位的保持时间。
IP	如果启用，该字段为 true；如果未启用，则为空。
IPv6	如果启用，该字段为 true；如果未启用，则为空。
最短路由间隔（秒）	以秒为单位的最短路由间隔。
单播	如果启用，该字段为 true；如果未启用，则为空。
路由	
姓名	路由表中的 IPv4 或 IPv6 路由：IPv4 或 IPv6 地址和前缀长度。
AS 路径	路径中的下一个 AS。
最佳路径	如果启用，该字段为 true；如果未启用，则为空。
MED	0 或为空
指标	0 或为空
网络	
下一个跃点	用于到达被标识为路由（名称）的网络的下一个跃点 IP 地址。
原始	路由的起点：IGP 或未完成
路径	路径中的下一个 AS。
路径起点	指示外部。
对等名称	
前缀	
前缀长度	
有效性	如果启用，该字段为 true；如果未启用，则为空。
重量	路由的权重。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Routing（路由）> Logical Routers（逻辑路由器）

防火墙需要逻辑路由器来获取其他子网的路由，获取方式可以是使用您手动定义的静态路由或参与第 3 层路由协议（动态路由）。在防火墙上定义的每个第 3 层接口、回环接口和 VLAN 接口都必须与逻辑路由器关联。每个接口只能属于一个逻辑路由器。

在 **Device**（设备）> **Setup**（设置）> **Management**（管理）的“常规设置”中启用 **Advanced Routing**（高级路由）并提交和重新启动防火墙后，逻辑路由器将可用。

高级路由引擎当前仅处于预览模式，其提供的功能集有限。

定义逻辑路由器需要您添加第三层接口到逻辑路由器，并配置网络所需的任何静态路由和 BGP 路由组合。您也可以配置 ECMP 等其他功能。

您在查找什么内容？	请参阅
逻辑路由器所需元素	逻辑路由器的常规设置
配置：	静态路由 BGP BGP 路由配置文件 ECMP
查看有关逻辑路由器的信息。	有关逻辑路由器的更多运行时统计数据

逻辑路由器的常规设置

- Network（网络）> Routing（路由）> Logical Routers（逻辑路由器）> General（常规）

启用高级路由（**Device**（设备）> **Setup**（设置）> **Management**（管理））后，防火墙将使用逻辑路由器进行静态和动态路由。逻辑路由器要求您根据下表所述分配名称和第三层接口。防火墙上的高级路由路由引擎只支持一个逻辑路由器。

您可以为逻辑路由器配置等价多路径 (ECMP)（可选）。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。
- 充分利用所有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，流量会动态转移到同一目标的另一个 ECMP 成员，而不是等待路由协议或 RIB 表选定替代路径，这可以帮助当链路出现故障时减少停机时间。

ECMP 负载平衡为会话级操作，而非数据包级操作。这意味着防火墙会在新会话开始时选择等成本路径，而不是在防火墙每次收到数据包时选择。

© 2019 Palo Alto Networks, Inc.

逻辑路由器常规设置	说明
姓名	指定名称以描述逻辑路由器（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
接口	选择要包含在逻辑路由器中的第 3 层接口。这些接口可在逻辑路由器的路由表中用作传出接口。 要指定接口类型，请参阅 Network（网络）> Interfaces（接口）。 添加接口时，会自动添加它所连接的路由。
ECMP	
启用	为逻辑路由器启用等价多路径 (ECMP)。
对称返回	（可选）单击 **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 ingress 接口来发送返回数据包，而不是使用 ECMP 接口，所以 **Symmetric Return**（对称返回）设置优先于负载平衡。该行为仅适用于从服务器到客户端的通信流。
严格源路径	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。选择 **Strict Source Path**（严格源路径），确保源自防火墙的 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，就可以启用严格源路径。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 默认会根据所配置的 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。
最大路径	选择等成本路径的最大数：可从 RIB 复制到 FIB 的至目标网络的（2、3 或 4）。默认为 2。

负载均衡法	选择以下任一 ECMP 负载平衡算法以用于虚拟路由器。ECMP 负载平衡为会话级操作，而非数据包级操作。这意味着，防火墙 (ECMP) 会在新会话开始时选择等成本路径，而不是在每次收到数据包时选择。
	• **IP Modulo**（**IP** 模）— 默认情况下，虚拟路由器负载会使用该选项来平衡会话，它会使用数据包标头中的源和目标 IP 地址的散列来确定要使用的 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：
	  • 如果选择 **IP Hash**（**IP** 哈希），防火墙默认使用源 IP 地址和目标 IP 地址的哈希。
	  • 或者，您可以选择 **Use Source Address Only**（仅使用源地址）（在 PAN-OS 8.0.3 及更高版本中可用）。这种 IP 哈希方法确保属于同一源 IP 地址的所有会话始终采用相同的路径。
	  • （可选）选择 **Use Source/Destination Ports**（使用源/目标端口）可将端口包含在任一哈希计算中。还可以输入 **Hash Seed**（哈希种子）值（整数），以进一步实现负载平衡的随机化。

© 2019 Palo Alto Networks, Inc.

逻辑路由器常规设置	说明
	• **Weighted Round Robin**（加权循环调度）— 使用此算法可将不同链路容量和速度纳入考虑范围。选择此算法后，“接口”窗口即会打开。请单击 **Add**（添加），然后选择要纳入加权循环调度组的 **Interface**（接口）。针对各个接口，输入要用于该接口的 **Weight**（权重）。**Weight**（权重）默认为 100，范围为 1-255。特定等成本路径的权重越高，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。再次单击 **Add**（添加）可添加另一接口和权重。 • **Weighted Round Robin**（加权循环调度）— 将传入 ECMP 会话平均分布到各个链路上。

逻辑路由器的静态路由

- Network（网络）> Routing（路由）> Logical Routers（逻辑路由器）> Static（静态）

可选择输入一个或多个静态路由。选择 **IP** 或 **IPv6** 选项卡，并使用 IPv4 或 IPv6 地址**Add**（添加）路由。通常需要在此处配置默认路由 (0.0.0.0/0)。对于在逻辑路由器的路由表中以其他方式找不到的目标应用默认路由。

静态路由设置	说明
名称	输入标识静态路由的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
目标	以无类别域间路由 (CIDR) 格式输入 IP 地址和网络掩码：*ip_address/mask*（掩码）（例如，192.168.2.0/24（对于 IPv4）或 2001:db8::/32（对于 IPv6））。或者，可创建 IP 网络掩码类型的地址对象。
接口	选择用来将数据包转发到目标的传出接口，并/或配置下一个跃点设置。指定此接口来严格控制防火墙使用的接口，而不是使用路由表中用于此路由下一个跃点的接口。
下一个跃点	在以下各项中选择一项： • **IP Address**（**IP** 地址）— 选中此选项以输入下一个跃点的 IP 地址，或是选择或创建 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。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。 • 丢弃— 选择是否要丢弃发往此目标的通信。 • 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。
管理距离	指定静态路由的管理距离（范围为 10-240；默认为 10）。
指标	指定静态路由的有效跃点数值（范围为 1 - 65,535；默认为 10）。
路径监视	选中此选项可对静态路由启用路径监控。
失败条件	选择防火墙认为受监控路径停用，因此静态路由停用所依据的条件：

© 2019 Palo Alto Networks, Inc.

静态路由设置	说明
	• **Any**（任何）— 如果 ICMP 不可访问任一静态路由受监控目标，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动态或静态路由。 • **All**（所有）— 如果 ICMP 不可访问所有静态路由受监控目标，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动态或静态路由。 选择 **All**（所有）可避免单个受监控目标在离线维护时发送静态路由失败的信号。
抢占保留时间(分)	输入以下值：在防火墙将静态路由重新安装到 RIB 中之前，停用的路径监控必须保持激活状态（路径监控评估其所有成员受监控目标，且必须保持激活状态）的时长，以分钟为单位。如果计时器到期，但链接没有断开或翻动，链接被视为处于稳定状态，则路径监控可以保持激活状态，并且防火墙可以将静态路由添加回 RIB 中。 如果链接在保留时间内断开或翻动，则路径监控失败，并且计时器会在停用的监控返回激活状态时重启。如果抢占保留时间为零，防火墙会在路径监控激活时将静态路由立即重新安装到 RIB 中。范围为 0 至 1440；默认为 2。
名称	输入受监控目标的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
启用	选中此选项可为静态路由的特定目标启用路径监控；防火墙会向此目标发送 ICMP ping。
源 IP	选择防火墙用作受监控目标的 ICMP ping 消息源的 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。
目标 Ip	输入防火墙为其监控路径的 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）
Ping 间隔(秒)	指定确定防火墙监控路径的频率的 ICMP ping 间隔（以秒为单位，ping 受监控目标，范围为 1-60，默认为 3）。
Ping 计数	指定在防火墙认为链接断开之前受监控目标未返回的 ICMP ping 连续数据包的数量。根据 **Any**（任何）或**All**（所有）故障条件，在路径监控处于失败状态的情况下，防火墙会从 RIB 删除静态路由（范围为 3-10，默认为 5）。 例如，如果 Ping Interval（Ping 间隔）为 3 秒，Ping Count（Ping 计数）为 5 次缺失 ping 数据包（防火墙在过去 15 秒没有收到 ping 数据包），则表示路径监控检测到链接故障。如果路径监控处于失败状态，防火墙在 15 秒后收到 ping 数据包，则链接会被视为处于激活状态；根据任何或所有故障条件，对任何或所有受监控目标的路径监控会被视为处于激活状态，并且抢占保留时间开始计时。

© 2019 Palo Alto Networks, Inc.

逻辑路由器的 BGP 路由

- Network（网络）> Routing（路由）> Logical Routers（逻辑路由器）> BGP

下表列出了配置 BGP、对等组、对等以及逻辑路由器重新分发等设置。

BGP 设置	说明
General（常规）	
启用	启用逻辑路由器的 BGP。
路由器 ID	为逻辑路由器的 BGP 分配一个路由器 ID，通常为 IPv4 地址，以确保路由器 ID 的唯一性。
本地 AS	根据路由器 ID 分配逻辑路由器所属的本地自治系统 (AS)（2 字节或 4 字节 AS 编号范围为 1 - 4,294,967,295）。
ECMP 多个 AS 支持	如果您已配置 ECMP 并希望通过多个 BGP 自治系统运行 ECMP，请启用此选项。
强制执行第一个 AS	选择此选项，以使防火墙丢弃来自 EBGP 对等的传入更新消息，而 EBGP 对等未列出自己的 AS 编号作为 AS_PATH 属性中的第一个 AS 编号。（默认启用。）
快速故障转移	默认启用 EBGP 的快速故障转移。如果 EBGP 快速故障转移使防火墙在不必要的情况下撤回 BGP 路由，则禁用此选项。
默认本地首选项	指定可用于确定不同路径之间首选项的默认本地首选项；范围为 0 - 4,294,967,295，默认为 100。
平稳重启— 启用	启用 BGP 平稳重启后，数据包转发不会在 BGP 重启时中断（默认启用）。
失效路由时间	指定路由可以在已失效状态中停留的时长秒数（范围为 1-3,600，默认为 120）。
最长对等重启时间	指定本地设备接受的作为对等设备平稳重启时间的最大时长（以秒计，范围是 1-3,600 秒，默认为 120）。
路径选择 — 始终对比 MED	勾选此选项以从不同自治系统中的邻居处选择路径；默认禁用。多出口标识符 (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。
确定性 MED 比较	勾选此选项后，可在 IBGP 对等（同一自治系统中的 BGP 对等）通告的路由之间进行选择。默认为启用。
Peer Group（对等组）	
姓名	输入 BGP 对等名称。
启用	启用对等组。
类型	选择对等组类型为 **IBGP**（内部 BGP，AS 内对等）或 **EBGP**（外部 BGP - 两个自治系统之间对等）。

© 2019 Palo Alto Networks, Inc.

BGP 设置	说明
AFI IP 单播	选择或创建 AFI IPv4 配置文件以将配置文件中的设置应用于对等组；默认为 **None**（无）。
AFI IPv6 单播	选择或创建 AFI IPv6 配置文件以将配置文件中的设置应用于对等组；默认为 **None**（无）。
身份验证配置文件	选择或创建用于对 BGP 对等通信执行身份验证的身份验证配置文件；默认为 **None**（无）。
计时器配置文件	选择或创建要应用到对等组的计时器配置文件；默认为 **None**（无）。
多个跃点	设置 IP 标头中的生存时间 (TTL) 值。范围为 1-255；设置为 0 表示使用默认值：1 表示 EBGP；255 表示 IBGP。
对等	
姓名	输入 BGP 对等的名称。
启用	启用 BGP 对等。
对等 AS	输入对等所属的 AS；范围为 1 -4,294,967,295。
对等 — 寻址	
从对等组继承 AFI/SAFI 配置	为对等勾选此选项后，可从对等组继承 AFI 和并发 AFI (SAFI)。
AFI IP 单播	（此选项在禁用 **Inherit AFI/SAFI config from peer**（从对等组继承 **AFI/SAFI** 配置）后可用）选择或创建 AFI IPv4 配置文件以将配置文件中的设置应用于对等；默认为 **None**（无）。
AFI IPv6 单播	（此选项在禁用 **Inherit AFI/SAFI config from peer**（从对等端组继承 **AFI/SAFI** 配置）后可用）选择或创建 AFI IPv6 配置文件以将配置文件中的设置应用于对等；默认为 **None**（无）。
本地地址 — 接口	选择您正在配置 BGP 的第三层接口。配置有静态 IP 地址的接口以及配置为 DHCP 客户端的接口可供选择。如果选择 DHCP 分配地址的接口，则 **IP** 地址将显示 **None**（无）。DHCP 稍后将分配 IP 地址给接口；您可以在查看逻辑路由器的**More Runtime Stats**（更多运行时统计数据）时看到此地址。
IP	如果接口有多个 IP 地址，请输入您要使用的 IP 地址和网络掩码。
对等地址 - IP	输入对等的 IP 地址。
对等 — 连接选项 这些设置可覆盖您为该对等所属的对等组设置的相同选项。	
身份验证配置文件	选择或创建身份验证配置文件。或者，选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承）或 **None**（无），这两个选项都可使对等使用指定用于对等组的身份验证配置文件。

© 2019 Palo Alto Networks, Inc.

BGP 设置	说明
计时器配置文件	选择或创建计时器配置文件。或者，请选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承）或 **None**（无），这两个选项都可使对等使用指定用于对等组的计时器配置文件。
多个跃点	选择 **inherit (Inherit from Peer-Group)**（继承（从对等组继承）或 **None**（无），这两个选项都可使对等使用指定用于对等组的值。
对等 — 高级	
启用发送端循环检测	勾选此选项以促使防火墙在更新中发送路由之前检查其转发信息库 (FIB) 中路由的 AS_PATH 属性，以确保对等 AS 编号不在 AS_PATH 列表中。如果对端 AS 编号在 AS_PATH 列表中，则防火墙会将其删除以防止循环。默认为启用。
BGP 重新分发	
重新分发规则	
IPv4 单播	选择或创建用于指定重新分发到 IPv4 单播路由表的静态或已连接的 IPv4 路由的重新分发配置文件。默认为 **None**（无）。
IPv6 单播	选择或创建用于指定重新分发到 IPv6 单播路由表的静态或已连接的 IPv6 路由的重新分发配置文件。默认为 **None**（无）。
网络	
IPv4 或 IPv6	选择 **IPv4** 或 **IPv6**。
网络	添加相应的 IPv4 或 IPv6 网络地址；带匹配网络地址的子网将被通告给逻辑路由器的 BGP 对等。
单播	勾选此选项以将匹配路由安装到所有 BGP 对等的单播路由表中。

Network（网络）> Routing（路由）> Routing Profiles（路由配置文件）> BGP

对于逻辑路由器，请使用 BGP 配置文件以将配置有效地应用到 BGP 对等组、对等设备或重新分发规则。例如，您可以将计时器配置文件或身份验证配置文件应用到 BGP 对等组或对等设备。您可以将 IPv4 和 IPv6 的地址系列 (AFI) 应用到对等组。您可以将 IPv4 和 IPv6 的重新分发配置文件应用到 BGP 重新分发。

BGP 路由配置文件	说明
BGP Auth Profile（BGP 身份验证配置文件）	
姓名	输入身份验证配置文件的名称（最多 31 个字符）。
秘密	输入秘密，并 **Confirm Secret**（确认秘密）。该密钥被用作 MD5 身份验证的密钥。

© 2019 Palo Alto Networks, Inc.

BGP 路由配置文件	说明
BGP Timers Profile（BGP 计时器配置文件）	
姓名	输入计时器配置文件的名称（最多 31 个字符）。
保持活动状态间隔（秒）	输入一个时间间隔，在该时间间隔之后，将根据保持时间设置抑制来自对等的路由（以秒为单位，范围为 0-1,200，默认为 30）。
保持时间（秒）	输入在关闭对等连接之前，从对等发出连续的 Keepalive 或 Update 消息之间所经历的时间（以秒为单位，范围为 3-3,600，默认为 90）。
最小路由通告间隔（秒）	输入（BGP 发言者[防火墙]发送给通告路由或撤销路由的 BGP 对等）的两条连续 Update 消息之间必然会发生的最短时间（以秒为单位，范围为 1 至 600，默认为 30）。
BGP Address Family Profile（BGP 地址系列配置文件）	
姓名	输入地址族标识符 (AFI) 配置文件的名称（最多 31 个字符）。
IPv4 或 IPv6	选择 API 配置文件的类型（IPv4 或 IPv6）。
通告所有路径到对等设备	通告 BGP 路由信息库 (RIB) 中的所有路由。
通告每个相邻 AS 的最佳路径	启用此选项，确保 BGP 为各个相邻 AS 通告最佳路径，而不是为所有自治系统通告通用路径。如果您要向所有自治系统通告相同的路径，则禁用此选项。
允许 AS	指定是否允许包括防火墙自己的自治系统 (AS) 编号的路由： • **Origin**（原始）— 即使 AS_PATH 中存在防火墙自己的 AS，也接受路由。 • **Occurrence**（发生）—防火墙自己的 AS 出现在 AS_PATH 中的次数。 • **None**（无）—（默认设置）没有执行任何操作。
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个 AS（例如，AS 64512），且他们之间没有另一个 AS，则可以使用 BGP AS 替代功能。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 ASN（例如，AS 64522）。
发起默认路由	勾选此选项以通告默认路由。如果您只需通告前往指定目标的路由，则禁用此选项。
Num_prefixes	输入要从对等设备接受的最大前缀数。
阈值 (%)	输入最大前缀数的阈值百分比。如果对等设备通告多个阈值，那么，防火墙将采取指定的操作（警告或重新启动）。范围为 1 到 100%。
操作	指定防火墙在超过最大前缀数后对 BGP 连接采取的操作：**Warning Only**（仅警告）消息出现在日志中，或是 **Restart**（重新启动）BGP 对等连接。
下一个跃点	选择下一个跃点： • **None**（无）— 没有操作；计算该邻居的下一个跃点。 • **Self**（自身）— 禁用下一个跃点计算，并使用下一个跃点通告路由。

© 2019 Palo Alto Networks, Inc.

BGP 路由配置文件	说明
	• **Self Force**（自身强制）— 强制将反射路由的下一个跃点设为自身。
删除专用 AS	要让 BGP 从更新（防火墙发送给另一个 AS 的对等设备）的 AS_PATH 属性中删除专用 AS 号 ，请选择以下选项之一： • **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。
路由反射器客户端	启用防火墙充当 BGP 路由反射器客户端。
发送社区	选择在出站更新消息中发送的 BGP 社区属性类型： • **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。 • **Large**（大）— 发送大社区。 • **Standard**（标准）— 发送标准社区。 • **None**（无）— 不发送任何社区。
BGP Redistribution Profile（**BGP** 重新分发配置文件）	
姓名	输入重新分发配置文件的名称（最多 31 个字符）。
IPv4 或 IPv6	选择 IPv4 或 IPv6 地址族标识符 (AFI) 以指定要重新分发的路由类型。
静态	选择 **Static**（静态）和 **Enable**（启用）以将（与所选 AFI 匹配的）IPv4 或 IPv6 静态路由重新分发给 BGP 对等的 BGP 路由信息库 (RIB)。
指标	输入适用于被重新分发给 BGP 的静态路由的指标（范围为 1- 65,535）。
连接	选择 **Connected**（连接） 和 **Enable**（启用）以将（与所选 AFI 匹配的）IPv4 或 IPv6 连接路由重新分发给 BGP 对等的 BGP 路由信息库 (RIB)。
指标	输入适用于被重新分发给 BGP 的连接路由的指标（范围为 1- 65,535）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> IPSec Tunnels（IPSec 隧道）

选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）可在防火墙之间建立 IPSec VPN 隧道并对其进行管理。这是 IKE/IPSec VPN 设置的阶段 2 部分。

您在查找什么内容？	请参阅：
管理 IPSec VPN 隧道。	IPSec VPN 隧道管理
配置 IPSec 隧道。	IPSec 隧道常规选项卡
	IPSec 隧道代理 ID 选项卡
查看 IPSec 隧道状态。	防火墙中的 IPSec 隧道状态
重新启动或刷新 IPSec 隧道。	IPSec 隧道重新启动或刷新
了解更多？	建立 IPSec 隧道。

IPSec VPN 隧道管理

- Network（网络）> IPSec Tunnels（IPSec 隧道）

下表介绍了如何管理 IPSec VPN 隧道。

管理 IPSec VPN 隧道的字段	
添加	**Add**（添加）新的 IPSec VPN 隧道。有关配置新隧道的说明，请参阅 IPSec 隧道常规选项卡。
删除	**Delete**（删除）不再需要的隧道。
启用	**Enable**（启用）已禁用的隧道（默认启用隧道）。
禁用	**Disable**（禁用）不想使用但尚未准备删除的隧道。
PDF/CSV	以 **PDF/CSV** 格式导出 IPSec 隧道配置。您可以应用筛选程序来自定义表格输出并仅添加所需的列。仅导出 Export（导出）对话框中显示的列。请参阅导出配置表格数据。

IPSec 隧道常规选项卡

- Network（网络）> IPSec Tunnels（IPSec 隧道）> General（常规）

使用以下字段设置 IPSec 隧道。

© 2019 Palo Alto Networks, Inc.

IPSec 隧道常规设置	说明
姓名	输入 **Name**（名称）以标识隧道（最多 63 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。 此字段最多只能包含 63 个字符，其中除代理 ID（以冒号字符分隔）之外，还包括隧道名称。
隧道接口	选择一个现有隧道接口，或单击新建隧道接口。有关创建隧道接口的信息，请参阅 Network（网络）> Interfaces（接口）> Tunnel（隧道）。
IPv4 或 IPv6	选择 **IPv4** 或 **IPv6** 以将隧道配置为包含此类 IP 地址的端点。
类型	选择是使用自动生成的安全密钥还是手动输入的安全密钥。建议使用自动密钥。
自动键	如果选择自动密钥，则指定以下各项： • **IKE Gateway**（**IKE** 网关）— 有关 IKE 网关设置的说明，请参阅 Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）。 • **IPSec** 加密配置文件— 选择现有配置文件或保留默认配置文件。要定义新的配置文件，请单击 **New**（新建），并按照 Network（网络）> Network Profiles（网络配置文件）> IPSec Crypto（IPSec 加密）中的说明操作。 • 单击显示高级选项以访问其余字段。 • **Enable Replay Protection**（启用重播保护）— 选择此选项以防止重播攻击 • 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。此选项还会复制 Explicit Congestion Notification (ECN)（显示拥挤通知 (ECN)）字段。 • **Add GRE Encapsulation**（添加 **GRE** 封装）— 选择此选项以添加 IPSec 隧道中封装的 GRE 标头。防火墙在 IPSec 标头之后生成 GRE 标头，以便与其他供应商的隧道端点进行互操作，从而实现 GRE 隧道与 IPSec 隧道共享。 • **Tunnel Monitor**（隧道监控）— 选择此选项以便在隧道出现故障时向设备管理员发出警报并自动故障转移到另一个接口。 您需要向隧道接口分配一个 *IP* 地址才能进行监控。 • 目标 **IP** — 在此隧道另一端指定一个 IP 地址，隧道监测器将使用此地址确定此隧道是否正常工作。 • **Profile**（配置文件）— 选择现有配置文件以确定在隧道故障时所采取的操作。如果监视器配置文件中指定的操作是等待恢复，那么防火墙会等待隧道恢复正常运行，而不会使用路由表寻找替代路径。如果使用的是故障转移操作，那么防火墙会检查路由表，以确定是否存在可用于到达目标的替代路由。有关更多信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> Monitor（监控）。
手动密钥	如果选择手动密钥，则指定以下各项： • 本地 **SPI** — 指定本地安全参数索引 (SPI)，以供数据包从本地防火墙遍历到对端。SPI 是添加到 IPSec 隧道标头的十六进制索引，用于帮助区分各个 IPSec 通信流。 • 接口— 选择作为隧道端点的接口。 • 本地地址— 为作为隧道端点的本地接口选择 IP 地址。 • 远程 **SPI**— 指定远程安全参数索引 (SPI)，以供数据包遍历远程防火墙到达对等端设备。

© 2019 Palo Alto Networks, Inc.

IPSec 隧道常规设置	说明
	• 协议— 选择对通过隧道的通信使用的协议（**ESP**或**AH**）。 • 身份验证 — 选择对隧道访问使用的身份验证类型（**SHA1**、**SHA256**、**SHA384**、**SHA512**、**MD5** 或无）。 • 密钥/确认密钥— 输入并确认身份验证密钥。 • **Encryption**（加密）— 选择用于隧道通信的加密选项（**3des**、**aes-128-cbc**、**aes-192-cbc**、**aes-256-cbc**、**des** 或 **null** [不加密]）。 • 密钥/确认密钥— 输入并确认加密密钥。
GlobalProtect 卫星	如果选择**GlobalProtect** 卫星，则指定以下各项： • 名称— 输入名称以标识隧道（最多**31**个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。 • **Tunnel Interface**（隧道接口）— 选择一个现有隧道接口，或单击 New Tunnel Interface（新建隧道接口）。 • **Portal Address**（门户地址）— 输入 GlobalProtect™ 门户的 IP 地址。 • **Interface**（接口）— 从下拉列表中选择接口，此接口是用于访问 GlobalProtect 门户的出口接口。 • **Local IP Address**（本地 **IP** 地址）— 输入连接 GlobalProtect 门户的出口接口的 IP 地址。 • 高级选项 • **Publish all static and connected routes to Gateway**（将所有静态路由和已连接的路由发布到网关）— 选择此选项将所有路由从卫星发布到与此卫星连接的 GlobalProtect 网关。 • 子网— 单击添加以手动为此卫星位置添加本地子网。如果其他卫星正使用相同的子网信息，您必须通过 NAT 将所有通信传输到隧道接口 IP。而且，在此情况下，该卫星不能共享路由，所以所有路由都将通过隧道 IP 完成。 • **External Certificate Authority**（外部证书授权机构）— 如果您使用外部 CA 管理证书，则选择此选项。证书生成后，需要您将其导入到卫星中，然后选择要使用的 **Local Certificate**（本地证书）和 **Certificate Profile**（证书配置文件）。

IPSec 隧道代理 ID 选项卡

- Network（网络）> IPSec Tunnels（IPSec 隧道）> Proxy IDs（代理 ID）。

IPSec 隧道代理 **ID** 选项卡被分隔为两个选项卡：**IPv4** 和 **IPv6**。这两类的帮助类似；下表中的本地和远程字段介绍了 IPv4 和 IPv6 之间的差别。

IPSec 隧道代理 **ID** 选项卡还用于为 IKEv2 指定通信选择器。

代理 ID IPv4 和 IPv6 设置	说明
代理 ID	单击添加并输入名称以标识代理。 对于 IKEv2 通信选择器，此字段会用作“名称”。
本地	对于 IPv4：输入一个 IP 地址或子网，格式为 x.x.x.x/掩码（例如，10.1.2.0/24）。

© 2019 Palo Alto Networks, Inc.

代理 ID IPv4 和 IPv6 设置	说明
	对于 IPv6：输入一个 IP 地址和前缀长度，格式为 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/前缀长度（或按照 IPv6 约定，例如，2001:DB8:0::/48）。 IPv6 寻址不需要写出所有的零；前导零可以省略，一组连续零可用两个相邻冒号 (::) 代替。 对于 IKEv2 通信选择器，此字段会转换为源 IP 地址。
远程	如果对端需要： 对于 IPv4，输入一个 IP 地址或子网，格式为 x.x.x.x/掩码（例如，10.1.1.0/24）。 对于 IPv6，输入一个 IP 地址和前缀长度，格式为 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/前缀长度（或按照 IPv6 约定，例如，2001:DB8:55::/48）。 对于 IKEv2 通信选择器，此字段会转换为目标 IP 地址。
协议	指定本地和远程端口的协议以及端口号： **Number** — 指定协议号（用于与第三方设备进行互操作）。 • **any** — 允许进行 TCP 和/或 UDP 通信。 • **TCP**— 指定本地和远程 TCP 端口号。 • **UDP**— 指定本地和远程 UDP 端口号。 所配置的每个代理 ID 都将计入防火墙的 IPSec VPN 隧道容量。 此字段还会用作 IKEv2 通信选择器。

防火墙中的 IPSec 隧道状态

- Network（网络）> IPSec Tunnels（IPSec 隧道）

要查看当前所定义 IPSec VPN 隧道的状态，请打开 **IPSec** 隧道页面。该页面将报告以下状态信息：

- 隧道状态（第一个状态列）— 绿色表示 IPSec 阶段 2 安全关联 (SA) 隧道。红色表示 IPSec 阶段 2 SA 不可用或已过期。
- IKE 网关状态 — 绿色表示有效的 IKE 阶段 1 SA 或 IKEv2 IKE SA。红色表示该 IKE 阶段 1 SA 不可用或已过期。
- 隧道接口状态 — 绿色表示隧道接口已打开（因为隧道监视器已禁用，或因为隧道监视器状态为 UP 且监控 IP 地址可到达）。红色表示隧道接口已关闭，因为隧道监视器已启用且远程隧道监控 IP 地址不可到达。

IPSec 隧道重新启动或刷新

- Network（网络）> IPSec Tunnels（IPSec 隧道）

选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）可显示隧道状态。在第一个状态列中，有一个至 Tunnel Info（隧道信息）的链接。单击要重新启动或刷新的隧道，即可打开该隧道的 **Tunnel Info**（隧道信息）页面。单击列表中的某个条目，然后单击：

- **Restart**（重新启动）— 重新启动所选隧道。重新启动会破坏通过隧道的流量。
- **Refresh**（刷新）— 显示当前 IPSec SA 状态。

© 2019 Palo Alto Networks, Inc.

Network（网络）> GRE Tunnels（GRE 隧道）

通用路由封装(GRE)隧道协议是用于封装有效协议的运营商协议。GRE 数据包本身被封装在传输协议中（IPv4 或 IPv6）。GRE 隧道将防火墙和路由器（或另一个防火墙）之间的点对点逻辑链接中的两个端点连接起来。Palo Alto Networks 防火墙支持终止 GRE 隧道。

您在查找什么内容？	请参阅：
GRE 隧道的构建块	GRE 隧道
如何提供与其他供应商隧道端点的互操作？	创建 IPSec 隧道时，请选择 **Add GRE Encapsulation**（添加 **GRE** 封装）。
了解更多？	GRE 隧道

GRE 隧道

- Network（网络）> GRE Tunnels（GRE 隧道）

首先配置隧道接口（Network（网络）> Interfaces（接口）> Tunnel（隧道））。然后，添加通用路由封装(GRE)隧道，并根据您创建的隧道接口提供以下信息：

GRE 隧道字段	说明
姓名	GRE 隧道名称。
接口	选择用作本地 GRE 隧道端点的接口（源接口），该接口是以太网接口、聚合以太网 (AE) 接口、回环接口或 VLAN 接口。
本地地址	选择用作隧道接口地址的接口本地 IP 地址。
对等地址	输入 GRE 隧道另一端的 IP 地址。
隧道接口	选择您配置的隧道接口。（该接口在路由下一跳时标识隧道。）
TTL	输入封装在 GRE 数据包中的 IP 数据包的 TTL（范围为 1 到 255，默认为 64）。
复制 ToS 标头	选择以将服务类型 (ToS) 字段从封装的数据包的内部 IP 标头复制到外部 IP 标头，以保留原始 ToS 信息。
保持活动状态	选择以启用 GRE 隧道的保持活动状态功能（默认禁用）。如果启用保持活动状态，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。

© 2019 Palo Alto Networks, Inc.

GRE 隧道字段	说明
间隔(秒)	设置 GRE 隧道本地端发送给隧道对端设备的 keepalive 数据包之间的间隔，以及每个保留计时器在成功 keepalive 数据包之后、防火墙重新与隧道对端设备建立通信之前等待的时间间隔（范围为 1 到 50，默认为 10）。
重试	设置 keepalive 数据包在防火墙考虑关闭隧道对端设备之前未返回的间隔数（范围为 1 到 255，默认为 3）。
保持计时器	设置 keepalive 数据包在防火墙重新与隧道对端设备建立通信之前获得成功的间隔数（范围为 1 到 64，默认为 5）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> DHCP

动态主机配置协议 (DHCP) 是一个标准化协议，可向 TCP/IP 网络上的动态配置主机提供 TCP/IP 和链路层配置参数及网络地址。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。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。

您在查找什么内容？	请参阅：
什么是 DHCP？	DHCP 概述
DHCP 服务器如何分配地址？	DHCP 寻址
在防火墙上配置接口作为：	
	DHCP 服务器
	DHCP 中继
	Network（网络）> DNS Proxy（DNS 代理）
了解更多？	DHCP

DHCP 概述

- Network（网络）> DHCP

DHCP 使用“客户端-服务器”通信模型。该模型由防火墙可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）的防火墙可以从 DHCP 服务器请求 IP 地址和其他配置设置。客户端防火墙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 服务器的其他网络资源和选项。
- 充当 DHCP 服务器的防火墙可以为客户端提供服务。通过使用任一种 DHCP 寻址机制，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。服务器还可以向多个客户端提供 IP 寻址和 DHCP 选项。
- 充当 DHCP 中继代理的防火墙会侦听广播和单播 DHCP 消息，并在 DHCP 客户端和服务器间中继这些消息。

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。

DHCP 寻址

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。

© 2019 Palo Alto Networks, Inc.

- 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防火墙的 **MAC Address**（**MAC** 地址）相对应的 **Reserved Address**（保留地址）。即使客户端断开连接（注销、重启、断电等），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，如果客户端防火墙被用于执行某些关键任务，那么即使该防火墙出现关机、拔下插头、重启或断电情况，也必须保持相同的 IP 地址。

  在配置保留地址时，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）中的每一个地址都分配为 **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 服务器不会向任何防火墙分配 **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 服务器

- Network（网络）> DHCP > DHCP Server（DHCP 服务器）

以下部分将介绍 DHCP 服务器的各个组件。在配置 DHCP 服务器之前，您应该已经配置了分配给某个虚拟路由器和区域的第 3 层 Ethernet 或第 3 层 VLAN 接口。您还应该通过自己的网络计划了解有效的 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。

在添加 DHCP 服务器时，您会配置下表所述的设置。

DHCP 服务器设置	配置位置	说明
接口	**DHCP** 服务器	将充当 DHCP 服务器的接口的名称。
模式		选择 **enabled**（启用）或 **auto**（自动）模式。自动（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。
分配新 IP 时，Ping IP	**DHCP Server**（**DHCP** 服务器）> **Lease**（租借）	如果单击 **Ping IP when allocating new IP**（在分配新 **IP** 时 **Ping IP**），那么服务器会在将 IP 地址分配给其客户端之前对该地址执行 ping 操作。如果 Ping 收到响应，这意味着另一防火墙已拥有该地址，因此该地址不可分配。服务器会转而分配池中的下一个地址。如果选择该选项，显示屏上的“探测 IP”列会有一个选中标记。
租借		指定租借类型。 • **Unlimited**（无限制）可让服务器从 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。

© 2019 Palo Alto Networks, Inc.

DHCP 服务器设置	配置位置	说明
IP 池		指定有状态的 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。 您可以输入单个地址“地址/<掩码长度>”（如 192.168.1.0/24）或地址范围（如 192.168.1.10-192.168.1.20）。
保留地址		（可选）从 IP 池中指定一个您不希望由 DHCP 服务器动态分配的 IP 地址（格式为 x.x.x.x）。 如果也已指定 **MAC Address**（**MAC** 地址）（格式为 xx:xx:xx:xx:xx:xx），则当与该 MAC 地址关联的防火墙通过 DHCP 请求 IP 地址时，**Reserved Address**（保留地址）会被分配给该防火墙。
继承源	**DHCP Server**（**DHCP** 服务器）> **Options**（选项）	选择无（默认值）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。 指定继承源的一个好处在于：DHCP 选项会从源 DHCP 客户端的上游服务器快速传输。如果继承源上的选项有所更改，客户端的选项也能得到更新。例如，如果继承源防火墙更换了其 NTP 服务器（已被标识为 **Primary NTP**（主 **NTP**）服务器），则客户端会将该新地址自动继承为其**Primary NTP**（主 **NTP**）服务器。
检查继承源状态		如果已选择 **Inheritance Source**（继承源），则单击 **Check inheritance source status**（检查继承源状态）可打开动态 IP 接口状态窗口，该窗口会显示继承自 DHCP 客户端的选项。
网关	**DHCP Server**（**DHCP** 服务器）> **Options (cont)**（选项）（续）	指定用于访问和此 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。
子网掩码		指定应用于 **IP** 池中地址的网络掩码。
选项		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服务的远程服务器的 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。 DHCP 服务器会将这些设置发送到其客户端。 • 主 **DNS**、辅助 **DNS** — 首选和备用域名系统 (DNS) 服务器的 IP 地址。 • 主 **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。

© 2019 Palo Alto Networks, Inc.

DHCP 服务器设置	配置位置	说明
		• **Primary NTP**（主 **NTP**）、**Secondary NTP**（辅助 **NTP**）— 可用的网络时间协议 (NTP) 服务器的 IP 地址。 • **POP3 Server**（**POP3** 服务器）— 邮局协议版本 3 (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）— 客户端在无法解析所输入的非限定主机名时要在本地使用的后缀。
自定义 DHCP 选项		单击 **Add**（添加），然后输入希望 DHCP 服务器发送到客户端的自定义选项的 **Name**（名称）。 输入**Option Code**（选项代码）（范围为 1-254）。 如果输入 **Option Code 43**（选项代码 **43**），则会出现“供应商类标识符 (VCI)”字段。输入将与来自客户端选项 60 的传入 VCI 进行比较的匹配条件。防火墙会检查来自客户端选项 60 的传入 VCI，在它自己的 DHCP 服务器表中找到匹配的 VCI，然后将对应的值返回至选项 43 中的客户端。VCI 匹配条件是一个字符串或十六进制值。十六进制值的前缀必须为“0x”。 单击 **Inherited from DCHP server inheritance source**（从 **DHCP** 服务器继承源继承）可使服务器继承来自继承源的该选项代码的值，无需输入 **Option Value**（选项值）。 除了选中此选项之外，您也可以选择继续设置以下各项： **Option Type**（选项类型）：选择 **IP Address**（**IP** 地址）、**ASCII** 或 **Hexadecimal**（十六进制），以指定用于“选项值”的数据类型。 针对 **Option Value**（选项值），单击 **Add**（添加）并输入自定义选项的值。

DHCP 中继

- Network > DHCP > DHCP 中继

在将防火墙接口配置为 DHCP 中继代理之前，请确保您已配置第 3 层以太网或第 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。您会希望该接口能在客户端和服务器之间传递 DHCP 消息。每个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。客户端会将 DHCPDISCOVER 消息发送至所有已配置的服务器，而防火墙则会中继第一个响应客户端请求的服务器的 DHCPDISCOVER 消息。

DHCP 中继设置	说明
接口	将成为 DHCP 中继代理的接口的名称。
IPv4 / IPv6	选择您将指定的 DHCP 服务器和 IP 地址的类型。

© 2019 Palo Alto Networks, Inc.

DHCP 中继设置	说明
DHCP 服务器 IP 地址	输入将收发中继 DHCP 消息的 DHCP 服务器的 IP 地址。
接口	如果选择了 IPv6 作为 DHCP 服务器的 IP 地址协议并指定了多播地址，您还必须指定传出接口。

Dhcp 客户端

- Network（网络）> Interfaces（接口）> Ethernet> IPv4
- Network（网络）> Interfaces（接口）> VLAN > IPv4

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 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。如果需要使用 DHCP 为防火墙上的接口请求 IPv4 地址，请执行此任务。

DHCP 客户端设置	说明
类型	选择 **DHCP Client**（**DHCP** 客户端），然后选择 **Enable**（启用）可将接口配置为 DHCP 客户端。
自动创建指向服务器所提供的默认网关的默认路由	使防火墙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。
默认路由跃点数	（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）。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（范围为 1-65535，无默认值）。
显示 DHCP 客户端运行时信息	显示从 DHCP 服务器收到的所有设置，包括 DHCP 租借状态、动态 IP 分配、子网掩码、网关和服务器设置（DNS、NTP、域、WINS、NIS、POP3 和 SMTP）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> DNS Proxy（DNS 代理）

DNS 服务器会使用 IP 地址执行域名解析服务，反之亦然。如果将防火墙配置为 DNS 代理，它会充当客户端和服务器之间的中介，并会通过解析来自 DNS 高速缓存的查询或将查询转发到其他 DNS 服务器来充当 DNS 服务器。使用该页面可配置相应设置，以确定防火墙将以何种方式充当 DNS 代理。

您想了解什么内容？	请参阅：
防火墙代理 DNS 请求如何工作？	DNS 代理概述
如何配置 DNS 服务器？	DNS 代理设置
如何配置 FQDN 至 IP 地址的静态映射？	
如何管理 DNS 代理？	其他 DNS 代理操作
了解更多？	DNS

DNS 代理概述

您可以配置防火墙充当 DNS 服务器。首先创建 DNS 代理，并选择代理应用的接口。然后，指定防火墙在其 DNS 代理缓存中找不到域名（以及当域名与代理规则不匹配时）发送 DNS 查询的默认 DNS 主和辅助服务器。

要根据域名将 DNS 查询引导至不同的 DNS 服务器，请创建 DNS 代理规则。指定多个 DNS 服务器可确保 DNS 查询的本地化并提高效率。例如，您可以将所有企业 DNS 查询转发到企业 DNS 服务器，并将所有其他查询转发到 ISP DNS 服务器。

使用以下选项卡定义 DNS 代理（超出默认 DNS 主和辅助服务器）：

- **Static Entries**（静态条目）— 允许您配置防火墙缓存并发送到主机以响应 DNS 查询的静态 FQDN 到 IP 地址映射。
- **DNS Proxy Rules**（**DNS** 代理规则）— 允许您指定域和相应的主和辅助 DNS 服务器，以解析与规则相匹配的查询。如果在 DNS 代理缓存中找不到域名，则防火墙会在 DNS 代理（位于 DNS 查询到达的接口）中搜索匹配项，并根据匹配结果将查询转发到 DNS 服务器。如果没有匹配结果，防火墙会将查询发送到默认 DNS 主和辅助服务器。您可以启用与规则相匹配的域的缓存。
- **Advanced**（高级）— 若将使用 DNS 代理对象来解析防火墙生成的 DNS/FQDN 查询，则必须启用缓存（选择 **Cache**（缓存））和 **Cache EDNS Responses**（缓存 **EDNS** 响应）。还可以在 Advanced（高级）选项卡还允许您控制 TCP 查询和 UDP 查询重试。防火墙通过配置的接口发送 TCP 或 UDP DNS 查询。如果 DNS 查询响应对于单个 UDP 数据包来说太长，则 UDP 查询切换到 TCP。

DNS 代理设置

单击 **Add**（添加），并配置防火墙充当 DNS 代理。在防火墙上最多可以配置 256 个 DNS 代理。

DNS 代理设置	配置位置	说明
启用	**DNS** 代理	选择以启用此 DNS 代理。

© 2019 Palo Alto Networks, Inc.

DNS 代理设置	配置位置	说明
姓名		指定一个用于标识 DNS 代理对象的名称（最多 **31** 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置		指定 DNS 代理对象适用于的虚拟系统： • **Shared**（共享）：代理适用于所有虚拟系统。如果选择共享，服务器配置文件字段不可用。相反，输入 **Primary**（主）和 **Secondary**（辅助）DNS 服务器的 IP 地址或地址对象。 • 选择虚拟系统以使用此 DNS 代理；首先，必须配置虚拟系统。选择 **Device**（设备）> **Virtual Systems**（虚拟系统），选择虚拟系统，然后选择 **DNS Proxy**（**DNS** 代理）。
继承源 （仅限共享位置）		选择要从中继承默认 DNS 服务器设置的源。这常用于防火墙 WAN 接口由 DHCP 或 PPPoE 寻址的分支办公室部署。
检查继承源状态 （仅限共享位置）		选择此选项可查看当前分配给 DHCP 客户端和 PPPoE 客户端接口的服务器设置。这些设置可包括 DNS、WINS、NTP、POP3、SMTP 或 DNS 后缀。
主/辅助 （仅限共享位置）		指定防火墙（作为 DNS 代理）向其发送 DNS 查询的默认主和辅助 DNS 服务器的 IP 地址。如果找不到主 DNS 服务器，则防火墙使用辅助 DNS 服务器。
服务器配置文件 （仅限虚拟系统位置）		选择或创建新的 DNS 服务器配置文件。如果虚拟系统的“位置”被指定为“共享”，则此字段不会出现。
接口		**Add**（添加）一个接口作为 DNS 代理。可以添加多个接口。要从接口中删除 DNS 代理，请选择该代理，然后单击 **Delete**（删除）。 如果 DNS 代理仅用于服务路由功能，则不需要接口。如果您希望由目标服务路由设置源 IP 地址，则应将目标服务路由用于没有接口的 DNS 代理。否则，DNS 代理选择接口 IP 地址用作源（在没有设置 DNS 服务路由的情况下）。
姓名	**DNS Proxy**（**DNS** 代理）> **DNS Proxy Rules**（**DNS** 代理规则）	名称为必填项，这样才可通过 CLI 引用和修改条目。
为此映射解析的域启用缓存		选择此选项可缓存由此映射解析的域。
域名		**Add**（添加）一个或多个域名，以便防火墙用来与传入 FQDN 进行比较。如果 FQDN 与规则中的其中一个域相匹配，防火墙会将查询转发到为此代理指定的主/辅助 DNS 服务器。要从规则中删除域名，请选择该域名，然后单击 **Delete**（删除）。
DNS 服务器配置文件 （仅限共享位置）		选择或添加 DNS 服务器配置文件以定义虚拟系统的 DNS 设置，包括防火墙向其发送域名查询的主和辅助 DNS 服务器。

© 2019 Palo Alto Networks, Inc.

DNS 代理设置	配置位置	说明
主/辅助 （仅限虚拟系统位置）		输入防火墙向其发送匹配的域名查询的主和辅助 DNS 服务器的主机名或 IP 地址。
姓名	**DNS Proxy**（**DNS** 代理）> **Static Entries**（静态条目）	输入静态条目的名称。
FQDN		输入要映射到在 Address（地址）字段中定义的静态 IP 地址的完全限定域名 (FQDN)。
地址		**Add**（添加）一个或多个要映射到此位置的 IP 地址。防火墙在其 DNS 响应中包括所有这些地址，且客户端选择要使用的 IP 地址。要删除地址，请选择地址并单击删除。
TCP 查询	**DNS Proxy**（**DNS** 代理）> **Advanced**（高级）	选择此选项可启用使用 TCP 的 DNS 代理。指定防火墙将支持的并发暂挂 TCP DNS 请求数的最大数（即 **Max Pending Requests**（最大挂起请求数），范围为 64-256，默认为 64）。
UDP 查询重试	**DNS Proxy**（**DNS** 代理）> **Advanced**（高级）	指定 UDP 查询尝试的设置： • **Interval**（时间间隔）— DNS 代理在未收到任何响应的情况下发送另一个请求相隔的时间（秒）（范围为 1-30，默认为 2）。 • **Attempts**（尝试次数）— 在尝试下一个 DNS 服务器之前的最大尝试次数（不包括第一次尝试）（范围为 1-30，默认为 5）。
缓存	**DNS Proxy**（**DNS** 代理）> **Advanced**（高级）	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 **Device**（设备）> **Virtual Systems**（虚拟系统）下，选择虚拟系统和 **General**（常规）> **DNS Proxy**（**DNS** 代理）），则必须启用 **Cache**（缓存）（默认已启用）。然后，指定以下项： • **Enable TTL**（启用 **TTL**）— 限制防火墙缓存代理对象的 DNS 条目的时间长度。默认禁用 TTL。然后，输入 **Time to Live (sec)**（生存时间（秒））— 删除代理对象的所有缓存条目以及必须再次解析和缓存新的 DNS 请求之前的秒数。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，则必须启用缓存 DNS 扩展机制 (EDNS) 响应。为了成功查询 FQDN 地址对象，防火墙必须能够缓存 DNS 响应。

其他 DNS 代理操作

在将防火墙配置为 DNS 代理后，可在 **Network**（网络）> **DNS Proxy**（**DNS** 代理）页面上执行以下操作以管理 DNS 代理配置：

- **Modify**（修改）— 要修改 DNS 代理，请单击 DNS 代理配置的名称。

© 2019 Palo Alto Networks, Inc.

- **Delete**（删除）— 选择 DNS 代理条目，然后单击 **Delete**（删除）可删除 DNS 代理配置。
- **Disable**（禁用）— 要禁用 DNS 代理，请单击 DNS 代理条目的名称并取消选中 **Enable**（启用）选项。要启用已禁用的 DNS 代理，请单击 DNS 代理条目的名称并选中启用。

© 2019 Palo Alto Networks, Inc.

Network（网络）> QoS

以下主题介绍服务质量 (QoS)。

您在查找什么内容？	请参阅：
设置接口的带宽限制，并为退出接口的流量执行 QoS。	QoS 接口设置
监控退出已启用 QoS 接口的流量。	QoS 接口统计信息
了解更多？	请参阅服务质量，了解完整的 QoS 工作流程、概念及用例。
	选择Policies（策略）> QoS 为 QoS 类分配匹配的流量，或选择Network（网络）> Network Profiles（网络配置文件）> QoS 可最多为八个 QoS 类定义带宽限制和优先级。

QoS 接口设置

在接口上启用 QoS 可为该接口设置带宽限制，并/或启用接口以为出口流量实施 QoS。启用 QoS 接口时要将 QoS 配置文件附加到该接口。物理接口支持 QoS，子接口和聚合 Ethernet (AE) 接口也支持 QoS，但具体取决于防火墙型号。请查看 Palo Alto Networks 产品比较工具，以了解您的防火墙型号的 QoS 功能支持情况。

首先，请添加或修改 QoS 接口，然后按下表所述配置设置。

QoS 接口设置	配置位置	说明
接口名称	**QoS Interface（Qos 接口）> Physical Interface（物理接口）**	选择要启用 QoS 的防火墙接口。
最大出口速率 (Mbps)		输入通过此接口离开防火墙的通信的最大吞吐量 (Mbps)。默认值为 0，指定了防火墙的速率限值（PAN-OS 7.1.16 及更高版本中为 60,000 Mbps，PAN-OS 7.1.15 及更低版本中为 16,000 Mbps）。 尽管这不是一个必填字段，但建议始终定义 *QoS* 接口的 *Egress Max*（最大出口速率）。
为此接口启用 QoS 功能		选中此选项可在选定的接口上启用 QoS。
明文 隧道接口	**QoS Interface（QoS 接口）> Physical Interface（物理接口）> Default Profile（默认配置文件）**	选择明文通信和隧道通信的默认 QoS 配置文件。每项都必须指定默认配置文件。对于明文通信，默认配置文件以聚合的形式应用到所有明文通信。对于隧道通信，默认配置文件分别应用到在详细配置部分没有分配特定配置文件的各个隧道。有关定义 QoS 配置文件的说明，请参阅 Network（网络）> Network Profiles（网络配置文件）> QoS。
隧道接口		

© 2019 Palo Alto Networks, Inc.

QoS 接口设置	配置位置	说明
出口保障速率 (Mbps)	**QoS Interface**（**QoS** 接口）> **Clear Text Traffic/ Tunneled Traffic**（明文通信/隧道通信）	输入来自此接口的明文或隧道通信的保证带宽。
最大出口速率 (Mbps)		输入通过此接口离开防火墙的明文或隧道通信的最大吞吐量 (Mbps)。默认值为 0，指定了防火墙的速率限值（PAN-OS 7.1.16 及更高版本中为 60,000 Mbps，PAN-OS 7.1.15 及更低版本中为 16,000 Mbps）。明文或隧道通信的 **Egress Max**（最大出口速率）必须小于或等于物理接口的 **Egress Max**（最大出口速率）。

添加		• 单击 **Clear Text Traffic**（明文流量）选项卡上的 **Add**（添加），可定义处理明文流量的其他粒度。单击个别条目可配置以下设置：
		  • 名称— 输入能辨别这些设置的名称。
		  • **QoS** 配置文件— 选择应用于指定接口和子网的 QoS 配置文件。有关定义 QoS 配置文件的说明，请参阅 Network（网络）> Network Profiles（网络配置文件）> QoS。
		  • 源接口— 选择防火墙接口。
		  • 源子网— 选择子网以限制来自该源的通信设置，或保持默认的任何值，以对任何通过指定接口的通信均应用这些设置。
		• 单击 **Tunneled Traffic**（隧道通信）选项卡中的 **Add**（添加），可替代默认分配给特定隧道的配置文件，并配置以下设置：
		  • 隧道接口— 选择防火墙上的隧道接口。
		  • **QoS** 配置文件— 选择应用于指定隧道接口的 QoS 配置文件。
		例如，假定配置两个站点，其中一个与防火墙的连接速度为 45 Mbps，另一个为 T1。您可以对 T1 站点应用限制性 QoS 设置，以便该连接不会超载，同时还允许对 45 Mbps 的站点应用更灵活的设置。
		如需删除明文通信或隧道通信条目，请将其取消选中，然后单击 **Delete**（删除）。
		如果明文通信和隧道通信选项为空，则会使用“物理接口”选项卡“默认配置文件”中指定的值。

QoS 接口统计信息

- Network（网络）> QoS > Statistics（统计信息）

对于 QoS 接口，选择 **Statistics**（统计信息）可查看已配置的 QoS 接口的带宽、会话和应用程序信息。

QoS 统计信息	说明
带宽	显示所选节点和类的实时带宽图。此信息每隔两秒更新一次。 为 *QoS* 类配置的 *QoS* 最大出口和保证的出口限制可能和 *QoS* 统计信息屏幕中显示的值略有不同。此为正常行为，由硬件引擎对带宽限制和计数器的汇总方式引起。当带宽利用率图表显示实时值和数量时，不存在运行问题。
应用程序	列出所选 QoS 节点和/或类的所有活动应用程序。

© 2019 Palo Alto Networks, Inc.

QoS 统计信息	说明
源用户	列出所选 QoS 节点和/或类的所有活动源用户。
目标用户	列出所选 QoS 节点和/或类的所有活动目标用户。
安全规则	列出匹配并实施所选 QoS 节点和/或类的安全规则。
QoS 规则	列出匹配并实施所选 QoS 节点和/或类的 QoS 规则。

© 2019 Palo Alto Networks, Inc.

Network（网络）> LLDP

链路层发现协议 (LLDP) 可以自动在链路层中发现邻近设备及其功能。

您在查找什么内容？	请参阅：
什么是 LLDP？	LLDP 概述
配置 LLDP。	LLDP 的构建块
配置 LLDP 配置文件。	Network（网络> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件）
了解更多？	LLDP

LLDP 概述

LLDP 允许防火墙收发邻居的包含 LLDP 数据单元 (LLDPDU) 的 Ethernet 帧。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 能使网络设备映射其网络拓扑并了解已连接设备的功能，从而使故障排除变得更容易 — 尤其是对于通常在网络拓扑中检测不到防火墙的虚拟线路部署。

LLDP 的构建块

要在防火墙上启用 LLDP，请单击 Edit（编辑），再单击 **Enable**（启用），（可选）然后，如果默认设置不适合您的环境，请配置下表中显示的四个设置。表中的其余条目将介绍状态和对端统计数据。

LLDP 设置	配置位置	说明
传输间隔（秒）	**LLDP** 常规	指定传输 LLDPDU 的间隔秒数（范围为 1-3,600，默认为 30）。
传输延迟（秒）		指定在典型长度值 (TLV) 元素更改和 LLDP 传输发送之间相隔的延迟秒数。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 1-600，默认为 2）。
保持时间多个		指定一个值，将该值乘以 **Transmit Interval**（传输间隔）可确定 TTL 保持总时间（范围为 1-100，默认为 4）。 TTL 保持时间是指防火墙使来自对端的信息保持有效状态的时间长度。无论乘数值是多少，最大的 TTL 保持时间都为 65,535 秒。
通知间隔		指定 syslog 和 SNMP 陷阱通知在 MIB 发生变化时的传输间隔秒数（范围为 1-3,600，默认为 5）。

© 2019 Palo Alto Networks, Inc.

LLDP 设置	配置位置	说明
小望远镜过滤器	**LLDP** > **Status**（状态）	（可选）在过滤行中输入数据值并单击灰色箭头，这样便只会显示包含该数据值的行。单击红色的 X 可清除过滤器。
接口		已被分配到 LLDP 配置文件的接口的名称。
LLDP		LLDP 状态：启用或禁用。
模式		接口的 LLDP 模式：Tx/Rx、仅 Tx 或仅 Rx。
配置文件		已分配给接口的配置文件的名称。
传输的总数		已传出接口的 LLDPDU 的计数。
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。
接收的总数		接口已收到的 LLDP 帧的计数。
丢弃的 TLV		在收到后被放弃的 LLDP 帧的计数。
错误		接口已收到且包含错误的“时间长度值 (TLV)”元素的计数。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。
未识别		接口已收到但 LLDP 本地代理未能识别（如因 TLV 类型属于保留的 TLV 范围）的 TLV 的计数。
已过期		因相应 TTL 到期而从接收 MIB 中删除的项目的计数。
清除 LLDP 统计信息		选择以清除所有 LLDP 统计信息。
小望远镜过滤器	**LLDP** > **Peers**（对端）	（可选）在过滤行中输入数据值并单击灰色箭头，这样便只会显示包含该数据值的行。单击红色的 X 可清除过滤器。
本地接口		防火墙上检测到邻居设备的接口。
远程机箱 ID		对端的机箱 ID；使用 MAC 地址。
端口 ID	**LLDP** > **Peers**（对端（续））	对端的端口 ID。
姓名		对等的名称。
更多信息		单击 **More Info**（更多信息）可查看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		机箱类别为 MAC 地址。
MAC 地址		对端的 MAC 地址。
系统名称		对等的名称。

© 2019 Palo Alto Networks, Inc.

LLDP 设置	配置位置	说明
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。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Network Profiles（网络配置文件）

以下主题介绍网络配置文件：

- Network（网络）> Network Profiles（网络配置文件）> GlobalProtect IPSec Crypto（GlobalProtect IPSec 加密）
- Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）
- Network（网络）> Network Profiles（网络配置文件）> IPSec Crypto（IPSec 加密）
- Network（网络）> Network Profiles（网络配置文件）> IKE Crypto（IKE 加密）
- Network（网络）> Network Profiles（网络配置文件）> Monitor（监控）
- Network（网络）> Network Profiles（网络配置文件）> Interface Mgmt（接口管理）
- Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）
- Network（网络）> Network Profiles（网络配置文件）> QoS
- Network（网络> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件）
- Network（网络> Network Profiles（网络配置文件）> BFD Profile（BFD 配置文件）
- Network（网络）> Network Profiles（网络配置文件）> SD-WAN Interface Profile（SD-WAN 接口配置文件）

Network（网络）> Network Profiles（网络配置文件）> GlobalProtect IPSec Crypto（GlobalProtect IPSec 加密）

使用 **GlobalProtect IPSec** 加密配置文件页面可以为 GlobalProtect 网关和客户端之间的 VPN 隧道中的身份验证和加密操作指定算法。算法的添加顺序就是防火墙应用这些算法的顺序，会影响隧道的安全性和性能。如需更改顺序，请选择算法，然后单击 **Move Up**（上移）或 **Move Down**（下移）。

对于 *GlobalProtect* 网关和卫星（防火墙）之间的 *VPN* 隧道，请参阅 Network（网络）> Network Profiles（网络配置文件）> IPSec Crypto（IPSec 加密）。

GlobalProtect IPSec 加密配置文件设置	
姓名	输入名称以标识配置文件。此名称区分大小写，必须是唯一的，且最多可包含 **31** 个字符。仅可使用字母、数字、空格、连字符和下划线。
加密	单击添加，然后选择所需的加密算法。要获得最高安全级别，请将顺序（由上至下）更改为：**aes-256-gcm**、**aes-128-gcm**、**aes-128-cbc**。
身份验证	单击添加，然后选择身份验证算法。目前，仅有的一个选项为 **sha1**。

Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）

使用本页可以管理或定义网关，包括与对端网关进行 Internet 密钥交换 (IKE) 协议协商时所需的配置信息。这是 IKE/IPSec VPN 设置的阶段 1 部分。

要管理、配置、重新启动或刷新 IKE 网关，请参阅以下内容：

- IKE 网关管理

© 2019 Palo Alto Networks, Inc.

- IKE 网关常规选项卡
- IKE 网关“高级选项”选项卡
- IKE 网关重新启动或刷新

IKE 网关管理

- Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）

下表介绍了如何管理 IKE 网关。

管理 IKE 网关	说明
添加	要创建新的 IKE 网关，请单击添加。有关配置新网关的说明，请参阅 IKE 网关常规选项卡和 IKE 网关高级选项选项卡。
删除	要删除某个网关，请选择该网关，并单击删除。
启用	要启用已禁用的网关，请选择该网关，并单击启用（这是网关的默认设置）。
禁用	要禁用某个网关，请选择该网关，并单击禁用。
PDF/CSV	具有最小只读访问权限的管理角色可以将对象配置表格导出为 **PDF/CSV**。您可以应用筛选程序来创建更多特定的表格配置输出，以用于审计等事宜。将仅导出 Web 界面中所显示的列。请参阅配置表格导出。

IKE 网关常规选项卡

- Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）> General（常规）

下表介绍了配置 IKE 网关时一开始的几个步骤。IKE 是 IKE/IPSec VPN 流程的阶段 1。配置这些设置后，请参阅 IKE 网关高级选项选项卡。

IKE 网关常规设置	说明
姓名	输入 **Name**（名称）以标识网关（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
版本	选择网关支持的 IKE 版本，而且必须同意用于对端网关：**IKEv1 only mode**（仅 **IKEv1** 模式）、**IKEv2 only mode**（仅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式）。IKEv2 首选模式导致网关为 IKEv2 进行协商，如果对端也支持 IKEv2，则它们将使用该模式；否则，网关将回退到 IKEv1。
地址类型	选择网关所使用的 IP 地址的类型：**IPv4** 或 **IPv6**。
接口	指定到 VPN 隧道的传出防火墙接口。
本地 IP 地址	为作为隧道端点的本地接口选择或输入 IP 地址。
对等 IP 地址 类型	选择以下其中一个设置并输入对端的相应信息： • **Dynamic**（动态）— 如果对端 IP 地址或 FQDN 值未知，请选择此选项。当对端 IP 地址类型为动态时，由对端发起 IKE 网关协商。

© 2019 Palo Alto Networks, Inc.

IKE 网关常规设置	说明
	• **IP** — 输入 **Peer Address**（对端地址）作为 IPv4 或 IPv6 地址，或为 IPv4 或 IPv6 地址的地址对象。 • **FQDN** — 输入 **Peer Address**（对端地址）作为 FQDN 或使用 FQDN 的地址对象。 如果输入解析为多个 IP 地址的 FQDN 或 FQDN 地址对象，则防火墙将从与 IKE 网关的地址类型（IPv4 或 IPv6）匹配的一组地址中选择首选地址，如下所示： • 如果尚未协商 IKE 安全关联 (SA)，则首选地址为具有最小值的 IP 地址。 • 如果某地址被 IKE 网关使用并位于返回地址集中，则会使用该地址（不管它是否最小）。 • 如果某地址被 IKE 网关使用但不在返回地址集中，则会选择一个新地址：集合中的最小地址。 使用 *FQDN* 或 *FQDN* 地址对象可以减少对端受动态 *IP* 地址变更影响的环境中的问题（否则，需要您重新配置此 *IKE* 网关对端地址）。
身份验证	选择身份验证类型：对端网关将要采用的 **Pre-Shared Key**（预共享密钥）或 **Certificate**（证书）。根据选择，请参阅预共享密钥或证书字段。
预共享密钥字段	
预共享密钥/ 确认预共享密钥	如果选择 **Pre-Shared Key**（预共享密钥），请输入要用于跨隧道对称身份验证的单个安全密钥。**Pre-Shared Key**（预共享密钥）值是管理员使用最多 255 个 ASCII 或非 ASCII 字符创建的字符串。生成一个字典式攻击很难破解的密钥；如有必要，请使用预共享密钥生成器。
本地标识	定义本地网关的格式和标识，它们将和预共享密钥一同用于 IKEv1 阶段 1 SA 和 IKEv2 SA 建立。 选择以下任一类型，然后输入值：**FQDN**（主机名）、**IP address**（**IP** 地址）、**KEYID**（以十六进制表示的二进制格式 ID 字符串）或 **User FQDN**（用户 **FQDN**）（电子邮件地址）。 如果未指定值，则网关将使用本地 IP 地址作为 **Local Identification**（本地标识）值。
对端标识	定义对端网关的类型和标识，它们将在 IKEv1 阶段 1 SA 和 IKEv2 SA 建立期间与预共享密钥结合使用。 选择以下任一类型，然后输入值：**FQDN**（主机名）、**IP address**（**IP** 地址）、**KEYID**（以十六进制表示的二进制格式 ID 字符串）或 **User FQDN**（用户 **FQDN**）（电子邮件地址）。 如果未指定值，则网关将使用对端的 IP 地址作为 **Peer Identification**（对端标识）值。
证书字段	
本地证书	如果选择证书作为身份验证类型，请从下拉列表中选择防火墙中已存在的证书。 或者，可以如下所示地导入证书或生成新证书：

© 2019 Palo Alto Networks, Inc.

IKE 网关常规设置	说明

	导入：
	• 证书名称 — 输入您正导入的证书的名称。
	• 共享 — 如果要在多个虚拟系统间共享该证书，请单击此选项。
	• **Certificate File**（证书文件）— 单击 **Browse**（浏览）按钮以导航至证书文件所在位置。单击文件并选择 **Open**（打开）。
	• 文件格式 — 选择以下任一项：
	  • **Base64** 编码证书 **(PEM)** — 包含证书，但不含密钥。明文。
	  • 加密私钥和证书 **(PKCS12)** — 包含证书和密钥。
	• 硬件安全模块上的私钥 — 如果防火墙是密钥所在的 HSM 服务器客户端，请单击此选项。
	• **Import Private Key**（导入私钥）— 如因和证书在不同文件中而要导入私钥，请单击此选项。
	  • **Block Private Key Export**（阻止私钥导出）— 一旦选择 **Import Private Key**（导入私钥），包括超级用户在内的任何管理员都不能导出私钥。
	  • 密钥文件 — 浏览并导航至要导入的密钥文件。如果选择 PEM 作为文件格式，请指定此条目。
	  • 密码和确认密码 — 输入以访问密钥。

本地证书（续）	生成： • 证书名称 — 输入您正创建的证书的名称。 • **Common Name**（公用名）— 输入公用名，即要显示在证书上的 IP 地址或 FQDN。 • 共享 — 如果要在多个虚拟系统间共享该证书，请单击此选项。 • 签名者 — 选择“外部颁发机构 (CSR)”或输入防火墙 IP 地址。此条目必须为 CA。 • 证书颁发机构 — 如果防火墙为根 CA，请单击此选项。 • **Block Private Key Export**（阻止私钥导出）—阻止超级用户在内的任何管理员导出私钥。 • **OCSP Responder**（**OCSP** 响应者）— 输入用于跟踪证书是有效还是已吊销的 OSCP。 • 算法 — 选择用于为证书生成密钥的 RSA 或椭圆曲线 DSA。 • 位数 — 选择 512、1024、2048 或 3072 作为密钥的位数。 • 摘要 — 选择 md5、sha1、sha256、sha384 或 sha512 作为从散列恢复字符串的方法。 • 到期（天数）— 输入证书的有效天数。 • 证书属性：**Type**（类型）—（可选）从下拉列表中选择证书的其他属性类型。 • 值 — 输入属性的值。
HTTP 证书交换	单击 **HTTP Certificate Exchange**（**HTTP** 证书交换）并输入 **Certificate URL**（证书 **URL**），以便使用“散列和 URL”方式告知对端要从何处提取证书。证书 URL 就是存储证书的远程服务器的 URL。 如果对端表明自己也支持散列和 URL，则会通过 SHA1 散列和 URL 交换来交换证书。 当对端收到 IKE 证书负载时，它会看到 HTTP URL，并从该服务器提取证书。然后，对端使用证书负载中指定的散列来检查从 HTTP 服务器下载的证书。

© 2019 Palo Alto Networks, Inc.

IKE 网关常规设置	说明
本地标识	标识证书标识本地对端的方式。选择以下任一类型，然后输入值：**Distinguished Name**（可分辨名称）（主题）、**FQDN**（主机名）、**IP address**（**IP** 地址）或 **User FQDN**（用户 **FQDN**）（电子邮件地址）。
对端标识	标识证书标识远程对端的方式。选择以下任一类型，然后输入值：**Distinguished Name**（可分辨名称）（主题）、**FQDN**（主机名）、**IP address**（**IP** 地址）或 **User FQDN**（用户 **FQDN**）（电子邮件地址）。
对端设备 ID 检查	选择精确或通配符。此设置适用于正在接受检查以验证证书的对端标识。例如，如果对端标识为相当于 domain.com 的名称，而且您选择了 **Exact**（精确），同时 IKE ID 负载中的证书名称为 mail.domain2.com，那么 IKE 协商将失败。但是，如果选择了 **Wildcard**（通配符），那么只有名称字符串中通配符星号 (*) 前面的字符必须匹配，而通配符后面的所有字符都可以不同。
允许对等设备标识和证书负载标识不匹配	如果希望即使在对端标识与证书负载不匹配时也能灵活地成功完成 IKE Sa，请选择此选项。
证书配置文件	选择配置文件或创建新的 **Certificate Profile**（证书配置文件），以便配置适用于本地网关发送至对端网关的证书的证书选项。请参阅 Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）。
启用对端扩展密钥使用的严格验证	如果想要严格控制使用密钥的方式，请选择此选项。

IKE 网关“高级选项”选项卡

- Network（网络）> Network Profiles（网络配置文件）> IKE Gateways（IKE 网关）> Advanced Options（高级选项）

配置高级 IKE 网关设置（如被动模式）、NAT 遍历和 IKEv1 设置（如对端失效检测）。

IKE 网关高级选项	说明
启用被动模式	单击以使防火墙仅响应 IKE 连接，并且从不启动此类连接。
启用 NAT 遍历	单击以对 IKE 和 UDP 协议使用 UDP 封装，从而使这些协议通过中间 NAT 设备。 如果在设备上的 IPSec VPN 端点间配置了网络地址转换 (NAT)，则请启用 NAT 遍历。
IKEv1 选项卡	
交换模式	选择自动、主动或主。处于自动模式（默认值）时，设备可以接受主模式和主动模式的协商请求；但是，只要有可能，该设备便会启动协商，并允许以主模式进行交换。必须使用相同交换模式配置对端设备，以便接受从第一个设备启动的协商请求。
Ike 加密配置文件	选择现有配置文件、保留默认配置文件或创建新配置文件。可以为 IKEv1 和 IKEv2 选择不同的配置文件。

© 2019 Palo Alto Networks, Inc.

IKE 网关高级选项	说明
	有关 IKE 加密配置文件的信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> IKE Crypto（IKE 加密）。
启用碎片	单击可允许本地网关接收碎片 IKE 数据包。最大的碎片数据包大小为 576 字节。
Dead Peer Detection	单击可启用并输入间隔（2 - 100 秒）和重试前的延迟（2 - 100 秒）。失效对端检测可识别不活动或不可用的 IKE 对端，并可帮助还原在对端不可用时丢失的资源。
IKEv2 选项卡	
Ike 加密配置文件	选择现有配置文件、保留默认配置文件或创建新配置文件。可以为 IKEv1 和 IKEv2 选择不同的配置文件。 有关 IKE 加密配置文件的信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> IKE Crypto（IKE 加密）。
严格 Cookie 验证	单击可在 IKE 网关上启用严格 **Cookie** 验证。 • 启用 **Strict Cookie Validation**（严格 **Cookie** 验证）后，将始终实施 IKEv2 cookie 验证；发起程序必须发送包含 cookie 的 IKE_SA_INIT。 • 禁用 **Strict Cookie Validation**（严格 **Cookie** 验证）（默认设置）后，系统将针对全局 **Cookie Activation Threshold**（**Cookie** 激活阈值）检查半开 SA 的数量（这是一个 VPN 会话设置）。如果半开 SA 的数量超过 **Cookie** 激活阈值，发起程序必须发送包含 cookie 的 IKE_SA_INIT。
活性检查	IKEv2 活性检查始终处于打开状态；所有的 IKEv2 数据包都用于活性检查。单击此框可让系统在对端空闲指定秒数后发送空信息数据包。范围：2-100。默认：5. 如有必要，试图发送 IKEv2 数据包的一端最多会尝试进行 10 次活性检查（所有 IKEv2 数据包都会计入重新传输设置）。如果得不到响应，发送方会关闭并删除 IKE_SA 和 CHILD_SA。发送方会发出另一个 IKE_SA_INIT，以便从头开始。

IKE 网关重新启动或刷新

- Network（网络）> IPSec Tunnels（IPSec 隧道）

选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道）可显示隧道状态。在第二个 Status（状态）列中，有一个至 IKE Info（IKE 信息）的链接。单击想要重新启动或刷新的网关。“IKE 信息”页面随即会打开。单击列表中的某个条目，然后单击：

- **Restart**（重新启动）— 重新启动所选网关。重新启动会破坏通过隧道的流量。如下所示，IKEv1 和 IKEv2 的重新启动行为有所不同：
  - **IKEv1** — 可以单独重新启动（清除）阶段 1 SA 或阶段 2 SA，只会影响相应的 SA。
  - **IKEv2** — 重新启动 IKEv2 SA 时，会导致所有子 SA（IPSec 隧道）被清除。

    如果重新启动 IKEv2 SA，所有底层 IPSec 隧道也会被清除。

    如果重新启动与 IKEv2 SA 相关的 IPSec 隧道（子 SA），重新启动不会影响 IKEv2 SA。
- **Refresh**（刷新）— 显示当前 IKE SA 状态。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Network Profiles（网络配置文件）> IPSec Crypto（IPSec 加密）

选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **IPSec Crypto**（**IPSec** 加密）可根据 IPSec SA 协商（阶段 2）配置为 VPN 隧道中的身份验证和加密指定协议和算法的 IPSec Crypto 配置文件。

对于 *GlobalProtect* 网关和客户端之间的 *VPN* 隧道，请参阅 Network（网络）> Network Profiles（网络配置文件）> GlobalProtect IPSec（GlobalProtect IPSec 加密）。

IPSec 加密配置文件设置	说明
姓名	输入**Name**（名称）以标识配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
IPSec 协议	选择协议以确保遍历 VPN 隧道的数据的安全性： • **ESP** — 封装式安全措施负载协议会加密数据、对源进行身份验证并验证数据完整性。 • **AH** — 身份验证头协议会对源进行身份验证并验证数据完整性。 使用 *ESP* 协议，因为它可提供连接机密性（加密）和身份验证。
加密（仅限 ESP 协议）	单击添加，然后选择所需的加密算法。如需获得最高安全级别，请使用 **Move Up**（上移）和 **Move Down**（下移），以更改为如下顺序（由上至下）：**aes-256-gcm**、**aes-256-cbc**、**aes-192-cbc**、**aes-128-gcm**、**aes-128-ccm** (the VM-Series firewall doesn't support this option)（VM 系列防火墙不支持该选项）、**aes-128-cbc**、**3des**和**des**。您还可以选择 **null**（不加密）。 使用*AES*形式加密。（*DES* 和 *3DES* 是较弱且易受攻击的算法。）
身份验证	单击添加，然后选择所需的身份验证算法。如需获得最高安全级别，请使用 **Move Up**（上移）和 **Move Down**（下移），以更改为如下顺序（由上至下）：**sha512**、**sha384**、**sha256**、**sha1**、**md5**。如果 **IPSec** 协议为 **ESP**，您还可以选择无（不进行身份验证）。 因为 *md5* 和 *sha1* 不安全，请使用 *sha256* 或更强的身份验证。对于短暂会话，可使用 *sha256*，而对于需要最安全的身份验证的流量（例如，金融交易），则使用 *sha384* 或更高版本。
DH 组	为 Internet 密钥交换 (IKE) 选择 Diffie-Hellman (DH) 组：**group1**、**group2**、**group5**、**group14**、**group19**或**group20**。要获得最高安全级别，请选择编号最大的组。如果不想续订防火墙在 IKE 阶段 1 中创建的密钥，请选择 **no-pfs**（不进行完全向前保密）：防火墙会重复使用当前密钥进行 IPSec 安全关联 (SA) 协商。
生命周期	选择单位，并输入协商密钥保持有效的时间长度（默认为一小时）。
生存期	选择可选单位，并输入密钥可用于加密的数据量。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Network Profiles（网络配置文件）> IKE Crypto（IKE 加密）

使用 **IKE Crypto Profiles**（**IKE** 加密配置文件）页面可以为标识、身份验证和加密操作（IKEv1 或 IKEv2，阶段 1）指定协议和算法。

如需更改算法或组的排列顺序，请选择该项目，然后单击 **Move Up**（上移）或 **Move Down**（下移）。该顺序将确定与远程对端协商设置时的第一选择。首先尝试的是列表顶部的设置，然后沿列表向下移动，直到尝试成功。

IKE 加密配置文件设置	说明
姓名	输入配置文件的名称。
DH 组	指定 Diffie-Hellman (DH) 组的优先级。单击添加并选择组：**group1**、**group2**、**group5**、**group14**、**group19** 或**group20**。如需获得最高安全级别，请选择该项目，然后单击 **Move Up**（上移）或 **Move Down**（下移），将具有更多标识符的组移到列表顶部。例如，将**group14**移到**group2**上方。
身份验证	指定哈希算法的优先级。单击添加并选择算法。如需获得最高安全级别，请选择项目，然后单击 **Move Up**（上移）或 **Move Down**（下移），以更改为如下顺序（由上至下）： • **sha512** • **sha384** • **sha256** • **sha1** • **md5** • （PAN-OS 10.0.3 以及 10.0 的更高版本）**none**（无） 如果选择 *AES-GCM* 算法进行加密，必须选择身份验证设置 *none*（无）。哈希会根据所选 *DH* 组自动选择。*DH* 组 *19* 及以下使用 *sha256*；*DH* 组 *20* 使用 *sha384*。
加密	选择适当的封装式安全措施负载 (ESP) 身份验证选项。单击添加并选择算法。如需获得最高安全级别，请选择项目，然后单击 **Move Up**（上移）或 **Move Down**（下移），以更改为如下顺序（由上至下）： • （PAN-OS 10.0.3 以及 10.0 的更新版本）**aes-256-gcm**（要求使用 IKEv2；DH 组应设为 **group20**（组 **20**）） • （PAN-OS 10.0.3 以及 10.0 的更新版本）**aes-128-gcm**（要求使用 IKEv2 且 DH 组设为 **group19**（组 **19**）） • **aes-256-cbc** • **aes-192-cbc** • **aes-128-cbc** • **3des** • **des**

© 2019 Palo Alto Networks, Inc.

IKE 加密配置文件设置	说明
	aes-256-gcm 和 *aes-128-gcm* 算法内置有身份验证；因此，在这种情况下，您必须选择*Authentication*（身份验证）设置为 *none*（无）。
关键生命周期	选择时间单位，并输入协商 IKE 阶段 1 密钥的有效时间长度（默认为 8 小时）。 • IKEv2 — 在该密钥的生命周期到期之前，必须重新为 SA 生成密钥或采取其他措施；一旦到期，SA 必须开始新的阶段 1 密钥协商。 • IKEv1 — 在到期之前，不会主动执行阶段 1 重新生成密钥操作。只有在 IKEv1 IPSec SA 到期时，才会触发 IKEv1 阶段 1 重新生成密钥操作。
IKEv2 身份验证多个	指定一个值（范围为 0-50，默认为 0），该值乘以密钥生命周期后可确定身份验证计数。身份验证计数是网关在必须开始重新进行 IKEv2 身份验证之前可以执行 IKEv2 IKE SA 重新生成密钥操作的次数。值 0 会禁用重新身份验证功能。

Network（网络）> Network Profiles（网络配置文件）> Monitor（监控）

监视配置文件用于监视 IPSec 隧道，并根据基于策略的转发 (PBF) 规则监视下一个跃点设备。在两种情况下，监视配置文件均可用来指定源（IPSec 隧道或下一个跃点设备）不可用时要采取的操作。监视配置文件是可选的，但是在维护站点间连接性以及确保 PBF 规则处于维护中时，此功能特别有用。以下设置可用于配置监视配置文件。

字段	说明
姓名	输入名称以标识监视器配置文件（最多**31**个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
操作	指定在隧道不可用时要执行的操作。如果丢失的检测信号个数达到阈值，防火墙将执行指定操作。 • 等待恢复— 等待隧道恢复，不执行其他操作。数据包将继续根据 PBF 规则发送。 • 故障转移 — 通信将切换到备份路径（如果存在）。防火墙使用路由表查询以确定此会话持续时间的路由。 在以上两种情况下，防火墙将尝试协商新 IPSec 密钥，以加速恢复。
间隔	指定检测信号之间的时间（范围为 2-10，默认为 3）。
阈值	指定在防火墙执行指定操作之前所要丢失的检测信号数（范围为 2-10，默认为 5）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Network Profiles（网络配置文件）> Interface Mgmt（接口管理）

接口管理配置文件可防止通过定义防火墙接口允许的服务和 IP 地址，对防火墙进行未授权访问。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）。要指定接口管理配置文件，请参阅 Network（网络）> Interfaces（接口）。

请勿将允许 *Telnet*、*SSH*、*HTTP* 或 *HTTPS* 的接口管理配置文件附加到允许从互联网或企业安全边界内的其他不可信区域访问的接口。这类接口包括您配置 *GlobalProtect* 门户或网关的接口；*GlobalProtect* 不需要接口管理配置文件即可访问门户或网关。有关如何保护对防火墙和 *Panorama* 的访问权限的详细信息，请参阅保护管理访问权限的最佳做法。

请勿将允许 *Telnet*、*SSH*、*HTTP* 或 *HTTPS* 的接口管理配置文件附加到已配置 *GlobalProtect* 门户或网关的接口，因为这会将管理接口暴露给互联网。

字段	说明
姓名	输入配置文件名称（最多**31**个字符）。配置接口时，此名称出现在接口管理配置文件列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
管理管理服务	• **Telnet** — 用于访问防火墙 CLI。Telnet 使用初始明文，但其安全性不及 SSH。 为接口上的管理流量启用 *SSH* 而非 *Telnet*。 • **SSH** — 用于对防火墙 CLI 进行安全访问。 • **HTTP** — 用于访问防火墙 Web 界面。HTTP 使用初始明文，但其安全性不及 HTTPS。 为接口上的管理流量启用 *HTTPS* 而非 *Telnet*。 • **HTTPS** — 用于对防火墙 Web 界面进行安全访问。

网络服务	• **Ping** — 用于测试与外部服务的连接性。例如，您可对管理接口执行 Ping 命令，以验证其是否能从 Palo Alto Networks 更新服务器接收 PAN-OS 软件和内容更新。
	• **HTTP OCSP** — 用于将防火墙配置为联机证书状态协议 (OCSP) 响应者。有关详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者）。
	• **SNMP** — 用于处理来自 SNMP 管理器的防火墙统计信息查询。有关详细信息，请参阅启用 SNMP 监控。
	• **Response Pages**（响应页面）— 用于启用以下各项的响应页面：
	  • **Authentication Portal**（身份验证门户）— 用于服务身份验证门户响应页面的端口会在第 3 层接口上保持打开状态：用于 NTLM 的端口 6080、用于不包含 SSL/TLS 服务器配置文件的身份验证门户的端口 6081 以及用于包含 SSL/TLS 服务器配置文件的身份验证门户的端口 6082。有关详细信息，请参阅 Device（设备）> User Identification（用户标识）> Authentication Portal Settings（身份验证门户设置）。
	  • **URL Admin Override**（**URL** 管理替代）— 有关详细信息，请参阅 Device（设备）> Setup（设置）> Content-ID。

© 2019 Palo Alto Networks, Inc.

字段	说明
	• **User-ID** — 用于启用防火墙中用户映射的重新分发。 • **User-ID Syslog Listener-SSL**（**User-ID** 系统日志侦听器 **SSL**）— 用于允许 PAN-OS 集成 User-ID 代理通过 SSL 收集系统日志消息。有关详细信息，请参阅配置对受监控服务器的访问权限。 • **User-ID Syslog Listener-UDP**（**User-ID** 系统日志侦听器 **UDP**）— 用于允许 PAN-OS 集成 User-ID 代理通过 UDP 收集系统日志消息。有关详细信息，请参阅配置对受监控服务器的访问权限。
允许的 IP 地址	输入可允许接口访问的 IPv4 或IPv6 地址列表。

Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）

将区域保护配置文件应用到区域可以针对最常见的泛滥攻击、侦察攻击、其他基于数据包的攻击、使用非 IP 协议以及带 802.1Q（以太网类型 0x8909）的具有特定安全组标记 (SGT) 的标头提供保护。区域保护配置文件的目的是在入口区域（流量进入防火墙的区域）提供广泛的保护，而不是用于保护特定终端主机或将流量转到特定目的地区域。可以将一个区域保护配置文件附加到区域。

在所有区域使用区域保护配置文件，以便为 *IP* 泛滥、侦察、基于数据包的攻击和非 *IP* 协议攻击提供额外保护。防火墙上的区域保护应该是互联网周边专用 *DDoS* 设备之后的第二层保护。

要在防火墙上加强区域保护功能，可配置 DoS 保护策略（Policies（策略）> DoS Protection（DoS 保护））针对特定区域、接口、IP 地址或用户进行匹配。

区域保护仅在数据包与会话不匹配时才执行，因为区域保护基于新的连接数/秒 *(cps)*，而不是基于数据包数/秒 *(pps)*。如果数据包与现有会话匹配，则它将会绕过区域保护设置。

您在查找什么内容？	请参阅：
如何创建区域保护配置文件？	区域保护配置文件的构建块 Flood 保护 侦察保护 基于数据包的攻击保护 协议保护 以太网 SGT 保护

区域保护配置文件的构建块

要创建区域保护配置文件，**Add**（添加）一个配置文件并为其命名。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置	配置位置	说明
姓名	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）	输入配置文件名称（最多31个字符）。配置区域时，此名称出现在区域保护配置文件列表中。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格和下划线。
说明		输入区域保护配置文件的可选说明。

根据区域所需的保护类型，配置任意组合的设置，以便继续创建区域保护配置文件：

- Flood 保护
- 侦察保护
- 基于数据包的攻击保护
- 协议保护
- 以太网 SGT 保护

如果您拥有多个虚拟系统环境，则必须启用以下内容：

- 外部区域，用于在虚拟系统之间进行通信
- 共享网关，允许虚拟系统共享用于外部通信的通用接口和单个 *IP* 地址

在外部区域中将会禁用下列区域和 *DoS* 保护机制：

- *SYN Cookies*
- *IP* 分片
- *ICMPv6*

要为共享网关启用 *IP* 分片和 *ICMPv6* 保护，您必须单独为共享网关创建区域保护配置文件。

要在共享网关上防止 *SYN* 泛滥攻击，可以通过随机早期丢弃或 *SYN cookie* 来应用 *SYN* 泛滥攻击保护配置文件；在外部区域中，只有随机早期丢弃适用于 *SYN* 泛滥攻击保护。

Flood 保护

- Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）> Flood Protection（泛滥攻击保护）

配置用于防御对 SYN、ICMP、ICMPv6、SCTP INIT 和 UDP 数据包以及其他类型的 IP 数据包进行泛滥攻击的配置文件。速率以每秒连接数为单位；例如，与现有会话不匹配的传入 SYN 数据包被视为新的连接。

区域保护配置文件设置 — 泛滥攻击保护	配置位置	说明
SYN	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）	选择以启用对 SYN 泛滥攻击的保护。
操作		选择响应 SYN Flood 攻击时要执行的操作。 • **Random Early Drop**（随机早期丢弃）— 导致丢弃 SYN 数据包以缓解泛滥攻击： • 流量超过 **Alert**（警告）速率阈值时，生成警报。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 泛滥攻击保护	配置位置	说明
		• 当流量超过 **Activate**（激活）速率阈值时，防火墙将随机丢弃个别 SYN 数据包以限制流量。 • 当流量超过 **Maximum**（最大）速率阈值时，将丢弃 100% 的传入 SYN 数据包。 • **SYN Cookie** — 使防火墙充当代理，拦截 SYN，代表 SYN 针对的服务器生成 Cookie，并将包含 Cookie 的 SYN-ACK 发送到原始源。只有当源将包含 Cookie 的 ACK 返回到防火墙时，防火墙才会认为源有效并将 SYN 转发到服务器。这是首选操作。 *SYN Cookies 公平地处理合法流量，但会比 RED 消耗更多的防火墙资源。如果 SYN Cookies 消耗的资源过多，则切换到 RED。如果您未在防火墙的上游使用专用 DDoS 防护设备（在互联网周边），则始终使用 RED。*
警报速率（连接数/秒）	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	输入区域每秒接收的将触发警报的 SYN 数据包数（与现有会话不匹配）。您可以在仪表盘和威胁日志（Monitor（监控）> Packet Capture（数据包捕获））中查看警报。范围为 0 - 2,000,000，默认为 10,000。 最佳做法是将阈值设置为高于平均区域 CPS 速率 15-20%，以适应正常波动，并在收到过多警报时调整阈值。
激活（连接数/秒）		输入区域每秒接收的将触发在此区域保护配置文件中指定的操作的 SYN 数据包数（与现有会话不匹配）。防火墙使用算法随着攻击速率的增加而逐渐丢弃更多的数据包，直到速率达到最大速率。如果传入速率下降到激活阈值以外，则防火墙将停止丢弃 SYN 数据包。范围为 1-2,000,000，默认为 10,000。 最佳做法是将阈值设置刚好高于区域峰值 CPS 速率，以避免限制合法流量，并根据需要调整阈值。
最大（连接数/秒）		输入在丢弃超过最大速率的数据包之前区域每秒接收的最大 SYN 数据包数（与现有会话不匹配）。范围为 1 至 2,000,000，默认为 40,000。越过此阈值可阻止新连接，直至 CPS 速率降至阈值以下。 最佳做法是将阈值设置为防火墙容量的 80-90%，同时考虑会消耗防火墙资源的其他功能。
ICMP	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	选择以启用对 ICMP 泛滥攻击的保护。
警报速率（连接数/秒）		输入区域每秒接收的将触发攻击警报的 ICMP 回显请求数（ping 与现有会话不匹配）。范围为 0 - 2,000,000，默认为 10,000。 最佳做法是将阈值设置为高于平均区域 CPS 速率 15-20%，以适应正常波动，并在收到过多警报时调整阈值。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 泛滥攻击保护	配置位置	说明
激活（连接数/秒）		输入在丢弃后续 ICMP 数据包之前区域每秒接收的 ICMP 数据包数（与现有会话不匹配）。防火墙使用算法随着攻击速率的增加而逐渐丢弃更多的数据包，直到速率达到最大速率。如果传入速率下降到激活阈值以外，则防火墙将停止丢弃 ICMP 数据包。范围为 1-2,000,000，默认为 10,000。 最佳做法是将阈值设置刚好高于区域峰值 CPS 速率，以避免限制合法流量，并根据需要调整阈值。
最大（连接数/秒）		输入在丢弃超过最大速率的数据包之前区域每秒接收的最大 ICMP 数据包数（与现有会话不匹配）。范围为 1 至 2,000,000，默认为 40,000。 最佳做法是将阈值设置为防火墙容量的 80-90%，同时考虑会消耗防火墙资源的其他功能。
SCTP INIT	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	选择以启用防御对包含启动 (INIT) 块的流控制传输协议 (SCTP) 数据包进行泛滥攻击。其中一个 INIT 块不能与其他块捆绑在一起，因此，该数据包被称为 SCTP INIT 数据包。
警报速率（连接数/秒）		输入区域每秒接收的将触发攻击警报的 SCTP INIT 数据包（与现有会话不匹配）数。范围为 0 - 2,000,000。各防火墙型号的默认值如下： • **PA-5280** — 10,000 • **PA-5260**—7,000 • **PA-5250**—5,000 • **PA-5220** — 3,000 • **VM-700**—1,000 • **VM-500**—500 • **VM-300**—250 • **VM-100**—200 • **VM-50**—100
激活（连接数/秒）		输入在丢弃后续 SCTP INIT 数据包之前区域每秒接收的 SCTP INIT 数据包（与现有会话不匹配）数。防火墙使用算法随着攻击速率的增加而逐渐丢弃更多的数据包，直到速率达到最大速率。如果传入速率下降到激活阈值以外，则防火墙将停止丢弃 SCTP INIT 数据包。范围为 1-2,000,000。各防火墙型号的默认值与警报速率的默认值相同。
最大（连接数/秒）	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	输入在丢弃超过最大速率的数据包之前区域每秒接收的最大 SCTP INIT 数据包（与现有会话不匹配）数。范围为 1-2,000,000。各防火墙型号的默认值如下： • **PA-5280**—20,000 • **PA-5260**—14,000 • **PA-5250**—10,000 • **PA-5220**—6,000 • **VM-700**—2,000

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 泛滥攻击保护	配置位置	说明
		• **VM-500**—1,000 • **VM-300**—500 • **VM-100**—400 • **VM-50**—200
UDP	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	选择以启用对 UDP 泛滥攻击的保护。
警报速率（连接数/秒）		输入区域每秒接收的将触发攻击警报的 UDP 数据包数（与现有会话不匹配）。范围为 0 - 2,000,000，默认为 10,000。 最佳做法是将阈值设置为高于平均区域 CPS 速率 15-20%，以适应正常波动，并在收到过多警报时调整阈值。
激活（连接数/秒）		输入区域每秒接收的将触发随机丢弃 UDP 数据包的 UDP 数据包数（与现有会话不匹配）。防火墙使用算法随着攻击速率的增加而逐渐丢弃更多的数据包，直到速率达到最大速率。如果传入速率下降到激活阈值以外，则防火墙将停止丢弃 UDP 数据包。范围为 1-2,000,000，默认为 10,000。 最佳做法是将阈值设置刚好高于区域峰值 CPS 速率，以避免限制合法流量，并根据需要调整阈值。
最大（连接数/秒）		输入在丢弃超过最大速率的数据包之前区域每秒接收的最大 UDP 数据包数（与现有会话不匹配）。范围为 1 至 2,000,000，默认为 40,000。 最佳做法是将阈值设置为防火墙容量的 80-90%，同时考虑会消耗防火墙资源的其他功能。
ICMPv6	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	选择以启用对 ICMPv6 泛滥攻击的保护。
警报速率（连接数/秒）		输入区域每秒接收的将触发攻击警报的 ICMPv6 回显请求数（ping 与现有会话不匹配）。范围为 0 - 2,000,000，默认为 10,000。 最佳做法是将阈值设置为高于平均区域 CPS 速率 15-20%，以适应正常波动，并在收到过多警报时调整阈值。
激活（连接数/秒）		输入在丢弃后续 ICMPv6 数据包之前区域每秒接收的 ICMPv6 数据包数（与现有会话不匹配）。防火墙使用算法随着攻击速率的增加而逐渐丢弃更多的数据包，直到速率达到最大速率。如果传入速率下降到激活阈值以外，则防火墙将停止丢弃 ICMPv6 数据包。范围为 1-2,000,000，默认为 10,000。 最佳做法是将阈值设置刚好高于区域峰值 CPS 速率，以避免限制合法流量，并根据需要调整阈值。
最大（连接数/秒）		输入在丢弃超过最大速率的数据包之前区域每秒接收的最大 ICMPv6 数据包数（与现有会话不匹配）。范围为 1 至 2,000,000，默认为 40,000。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 泛滥攻击保护	配置位置	说明
		最佳做法是将阈值设置为防火墙容量的 80-90%，同时考虑会消耗防火墙资源的其他功能。
其他 **IP**	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Flood Protection**（泛滥攻击保护）（续）	选择以启用防御对其他 IP（非 TCP、非 ICMP、非 ICMPv6、非 SCTP 和非 UDP）进行泛滥攻击。
警报速率（连接数/秒）		输入区域每秒接收的将触发攻击警报的其他 IP 数据包（非 TCP、非 ICMP、非 ICMPv6 和非 UDP 数据包）（与现有会话不匹配）数。范围为 0 - 2,000,000，默认为 10,000。 最佳做法是将阈值设置为高于平均区域 CPS 速率 15-20%，以适应正常波动，并在收到过多警报时调整阈值。
激活（连接数/秒）		输入区域每秒接收的将触发随机丢弃其他 IP 数据包的其他 IP 数据包数（非 TCP、非 ICMP、非 ICMPv6 和非 UDP 数据包）（与现有会话不匹配）。防火墙使用算法随着攻击速率的增加而逐渐丢弃更多的数据包，直到速率达到最大速率。如果传入速率下降到激活阈值以外，则防火墙将停止丢弃其他 IP 数据包。范围为 1-2,000,000，默认为 10,000。 最佳做法是将阈值设置刚好高于区域峰值 CPS 速率，以避免限制合法流量，并根据需要调整阈值。
最大（连接数/秒）		输入在丢弃超过最大速率的数据包之前区域每秒接收的最大其他 IP 数据包数（非 TCP、非 ICMP、非 ICMPv6 和非 UDP 数据包）（与现有会话不匹配）。范围为 1 至 2,000,000，默认为 40,000。 最佳做法是将阈值设置为防火墙容量的 80-90%，同时考虑会消耗防火墙资源的其他功能。

侦察保护

- Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）> Reconnaissance Protection（侦察保护）

以下设置定义了侦察保护：

区域保护配置文件设置 - 侦察保护	配置位置	说明
TCP 端口扫描	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Reconnaissance**	启用配置配置文件可启用对 TCP 端口扫描的防护。
UDP 端口扫描		启用配置配置文件可启用对 UDP 端口扫描的防护。
主机清除		启用配置配置文件可启用对主机扫掠的防护。
操作		系统为响应对应的侦查尝试而执行的操作： • **Allow**（允许）— 允许端口扫描或主机扫掠侦察。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 - 侦察保护	配置位置	说明
	Protection（侦察保护）	• **Alert**（警报）— 对于在指定时间间隔内达到阈值的每次端口扫描或主机扫掠生成警报（默认操作）。 • **Block**（阻止）— 丢弃在指定时间间隔的剩余时间内从源到目标的所有后续数据包。 • **Block IP**（阻止 **IP**）— 在指定的持续时间（以秒计，范围为 1-3,600 秒）内丢弃所有后续数据包。**Track By**（跟踪标准）— 确定是否阻止源或源到目标的通信。例如，如果尝试次数超过单个源所设间隔时间内的对应阈值，则进行阻止（严格阻止），或如果尝试中包含有源和目标对，则进行阻止（非严格阻止）。 阻止除内部漏洞测试扫描之外的所有侦察扫描。
间隔(秒)		TCP 或 UDP 端口扫描检测的时间间隔（以秒为单位，范围为 2-65,535，默认为 2）。 主机扫掠检测的时间间隔（以秒为单位，范围为 2-65,535，默认为 10）。
阈值(事件)		触发操作的指定间隔时间内，扫描端口事件或主机扫掠事件的数量（范围为 2-65,535，默认为 100）。 在阻止侦察尝试之前，使用默认事件阈值记录几个数据包，以进行分析。
源地址排除		您要从侦察保护中排除的 IP 地址。此列表最多支持 20 个 IP 地址或网络掩码地址对象。 • **Name**（名称）—输入要排除地址的描述性名称。 • **Address Type**（地址类型）—从下拉列表中选择 IPv4 或 IPv6。 • **Address**（地址）—从下拉列表中选择地址或地址对象，或者手动输入地址。 仅排除执行漏洞测试的可信内部组的 *IP* 地址。

基于数据包的攻击保护

- 网络 > 网络配置文件 > 区域保护 > 基于数据包的攻击保护

您可以配置基于数据包的攻击保护，以丢弃以下类型的数据包：

- IP 丢弃
- TCP 丢弃
- ICMP 丢弃
- IPv6 丢弃
- ICMPv6 丢弃

© 2019 Palo Alto Networks, Inc.

IP 丢弃

要指示防火墙如何处理其在区域中接收的某些 IP 数据包，请指定以下设置：

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
欺诈 IP 地址	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Packet Based Attack Protection**（基于数据包的攻击保护）> **IP Drop**（**IP** 丢弃）	检查入口数据包的源 IP 地址是否可路由，路由接口是否与入口接口位于同一区域。如果任一条件都不成立，则丢弃该数据包。 仅丢弃内部区域的欺诈 *IP* 地址数据包，确保入口处的源地址匹配防火墙路由表。
严格 IP 地址检查		检查两个条件是否都成立： • 源 IP 地址不是入口接口的子网广播 IP 地址。 • 源 IP 地址可通过正确的入口接口路由。 如果任一条件都不成立，则丢弃该数据包。 对于常见标准 (CC) 模式下的防火墙，您可启用对丢弃的数据包进行记录。在防火墙的 Web 界面中，选择 **Device**（设备）> **Log Settings**（日志设置）。在 Manage Logs（管理日志）部分中，选择 **Selective Audit**（选择性审核），然后启用 **Packet Drop Logging**（数据包丢弃记录）。
碎片通信		丢弃分段的 IP 数据包。
IP 选项丢弃		选择此组中的设置可启用防火墙以丢弃包含这些 IP 选项的数据包。
严格源路由		丢弃已选中 Strict Source Routing（严格源路由）IP 选项的数据包。Strict Source Routing（严格源路由）是数据报源通过网关提供路由信息或主机必须发送数据报使用的选项。 丢弃具有严格源路由的数据包，因为源路由允许攻击者绕过使用目标 *IP* 地址作为匹配标准的安全策略规则。
松散源路由		丢弃已选中 Loose Source Routing（松散源路由）IP 选项的数据包。Loose Source Routing（松散源路由）是数据报源提供路由信息，以及允许网关或主机选择多个中间网关的任何路由以便数据报获取路由中下一个地址使用的选项。 丢弃具有松散源路由的数据包，因为源路由允许攻击者绕过使用目标 *IP* 地址作为匹配标准的安全策略规则。
时间戳		丢弃已选中 Timestamp（时间戳）IP 选项的数据包。
记录路由		丢弃已选中 Record Route（记录路由）IP 选项的数据包。如果数据报启用此选项，则路由数据报的每个路由器都会将自己的 IP 地址添加到标头，从而为接收者提供路径。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
安全		如果已定义安全选项，则抛弃数据包。
流 ID		如果已定义 Stream ID 选项，则抛弃数据包。
未知		如果类和编号未知，则抛弃数据包。 放弃未知数据包。
格式不正确		如果数据包包含不正确的类、编号、长度组合（基于 RFC 791、1108、1393 和 2113），则抛弃数据包。 放弃格式不正确的数据包。

TCP 丢弃

要指示防火墙对其在区域中收到的特定 TCP 数据包采取什么操作，可指定以下设置。

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
不匹配的重叠 TCP 分段	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP Drop**（**TCP** 丢弃）	攻击者可通过有重叠但是不同的数据来构建连接，使得连接被误解。攻击者可使用 IP 欺骗和序列号预测来解释用户的连接并插入自己的数据。分段数据在以下情况中不匹配时，使用该设置来报告重叠不匹配并丢弃数据包。 • 分段位于其他分段之内。 • 分段与其他分段的部分内容重叠。 • 分段覆盖其他分段。 此保护机制使用序列号确定数据包在 TCP 数据流中的位置。 丢弃带有不匹配的重叠 *TCP* 分段的数据包。
分离握手		如果 TCP 会话建立程序未使用众所周知的三向握手，则阻止该会话建立。四向或五向分离握手，亦或是同步开放式会话建立程序，都是不允许的变体示例。 Palo Alto Networks 新一代防火墙能在不配置 **Split Handshake**（分离握手）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。如果为区保护配置文件配置了该选项，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。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
		通过分离握手丢弃数据包。
TCP 与数据同步		在三向握手期间，如果 TCP SYN 数据包包含数据，则会阻止 TCP 会话建立。默认情况下启用。
TCP 与数据同步确认		在三向握手期间，如果 TCP SYN-ACK 数据包包含数据，则会阻止 TCP 会话建立。默认情况下启用。
拒绝非 SYN TCP		确定在 TCP 会话设置的第一个数据包不是 SYN 数据包时是否要拒绝该数据包： • 全局 — 使用通过**TCP Settings**（**TCP** 设置）或 CLI 分配的系统级设置。 • 是 — 拒绝非 SYN TCP。 • 否 — 接受非 SYN TCP。 如果在发生阻止之后未设置客户端和/或服务器连接，那么允许非 *SYN TCP* 通信可能使文件阻止策略无法按预期运行。 如果在区域上配置隧道内容检测，并启用 *Rematch Sessions*（重新匹配对话），则仅对于该区域，禁用 *Reject Non-SYN TCP*（拒绝非 *SYN TCP*），这样，启用或编辑隧道内容检测策略不会导致防火墙丢弃现有的隧道会话。
非对称路径		确定是否丢弃或绕过包含非同步 ACK 或超出范围序列号的数据包： • 全局 — 使用通过**TCP Settings**（**TCP** 设置）或 CLI 分配的系统级设置。 • 丢弃— 丢弃包含非对称路径的数据包。 • 绕过— 绕过对包含非对称路径的数据包的扫描。
去除 TCP 选项		确定是否从 TCP 数据包中剥离 TCP Timestamp（TCP 时间戳）或 TCP Fast Open（TCP 快速打开）选项。
TCP 时间戳	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Packet Based Attack Protection**（基于数据包的攻击保护）> **TCP**	确定数据包在报头中是否拥有 TCP 时间戳，如果有时间戳，将会从报头中删除时间戳。 从数据包中剥离 *TCP* 时间戳，以防止时间戳 *DOS* 攻击。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
	Drop（**TCP** 丢弃）	
TCP 快速打开		在 TCP 三向握手期间，从 TCP SYN 或 SYN-ACK 数据包剥离 TCP Fast Open（TCP 快速打开）选项（以及数据负载，如果存在）。 在对此进行清除（禁用）之后，会允许 TCP Fast Open（TCP 快速打开），该选项通过包含数据传输来保留连接速度的设置。该功能独立于 TCP SYN with Data（TCP 与数据同步）和 TCP SYN-ACK with Data（TCP 与数据同步确认）。默认情况下禁用。
多路径 TCP (MPTCP) 选项		MPTCP 是 TCP 的扩展，其允许客户端通过同时使用多个路径来连接至目的地主机来维持连接。默认情况下，会根据全局 MPTCP 设置禁用 MPTCP 支持。 为和该配置文件关联的安全区域查看或调节 MPTCP 设置： • **no**（否）- 启用 MPTCP 支持（不剥离 MPTCP 选项）。 • **yes**（是）- 禁用 MPTCP 支持（剥离 MPTCP 选项）。在对此进行配置之后，MPTCP 连接会转换为标准 TCP 连接，因为 MPTCP 可向后兼容 TCP。 • **(Default) global**（（默认）全局）- 根据全局 MPTCP 设置支持 MPTCP。默认情况下，全局 MPTCP 设置为 yes（是），使得 MPTCP 禁用（从数据包中剥离了 MPTCP 选项）。您可以使用 **TCP Settings**（**TCP** 设置）中的 **Strip MPTCP option**（剥离 **MPTCP** 选项）或以下 CLI 命令查看或调整全局 MPTCP 设置： `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

ICMP 丢弃

要指示防火墙丢弃在区域中收到的某些 ICMP 数据包，请选择以下设置以启用它们。

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
ICMP Ping ID 为 0	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Packet Based Attack Protection**（基于数据包的攻击	如果 ICMP ping 数据包有标识符值 0，则抛弃数据包。
ICMP 碎片		丢弃由 ICMP 分段组成的数据包。
ICMP 大型数据包 (>1024)		丢弃大于 1024 字节的 ICMP 数据包。
放弃嵌入了错误消息的 ICMP		丢弃嵌入了错误消息的 ICMP 数据包。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
禁止 ICMP TTL 过期错误	保护) > **ICMP Drop** (**ICMP** 丢弃)	停止发送 ICMP TTL 过期消息。
禁止 ICMP Frag 需要		停止发送需要 ICMP 分片的消息，以响应超过接口 MTU，且具有不分片 (DF) 位集合的数据包。此设置将干扰主机在防火墙后执行的 PMTUD 过程。

IPv6 丢弃

要指示防火墙丢弃在区域中收到的某些 IPv6 数据包，请选择以下设置以启用它们。

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
类型 0 路由标头	**Network** (网络) > **Network Profiles** (网络配置文件) > **Zone Protection** (区域保护) > **Packet Based Attack Protection** (基于数据包的攻击保护) > **IPv6 Drop** (**IPv6** 丢弃)	丢弃包含类型 0 路由标头的 IPv6 数据包。有关类型 0 路由标头的信息，请参阅 RFC 5095。
IPv4 兼容地址		丢弃被定义为与 RFC 4291 IPv4 兼容的 IPv6 地址的 IPv6 数据包。
任意播源地址		丢弃包含任意播源地址的 IPv6 数据包。
多余的碎片标头		丢弃带有最新碎片标头 (M=0) 且零偏离的 IPv6 数据包。
ICMP“数据包太大”中的 MTU 小于 1280 字节		在最大传输单元 (MTU) 小于 1,280 字节时丢弃包含“Packet Too Big (数据包太大)”ICMPv6 消息的 IPv6 数据包。
逐跳扩展		丢弃包含 Hop-by-Hop Options (逐跃点选项) 扩展标头的 IPv6 数据包。
路由扩展		丢弃包含路由扩展标头的 IPv6 数据包，该标头会将数据包在其前往目标的路上引至一个或多个中间节点。
目标扩展		丢弃包含目标选项扩展的 IPv6 数据包，该扩展中包含仅适用于数据包目标的选项。
扩展标头中的 IPv6 选项无效		丢弃扩展标头中包含无效 IPv6 选项的 IPv6 数据包。
非零保留字段		丢弃标头的保留字段未设为零的 IPv6 数据包。

ICMPv6 丢弃

要指示防火墙如何处理在区域中收到的某些 ICMPv6 数据包，请选择以下设置以启用它们。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 — 基于数据包的攻击保护	配置位置	说明
ICMPv6 目标不可访问 - 需要显式安全规则匹配	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Packet Based Attack Protection**（基于数据包的攻击保护）> **ICMPv6 Drop**（**ICMPv6** 丢弃）	对于 Destination Unreachable（目标不可访问）ICMPv6 消息，需要进行显式安全策略匹配，即使该消息与现有会话关联也不例外。
ICMPv6 数据包太大 - 需要显式安全规则匹配		对于 Packet Too Big（数据包太大）ICMPv6 消息，需要进行显式安全策略匹配，即使该消息与现有会话关联也不例外。
ICMPv6 超时 - 需要显式安全规则匹配		对于 Time Exceeded（超时）ICMPv6 消息，需要进行显式安全策略匹配，即使该消息与现有会话关联也不例外。
ICMPv6 参数问题 - 需要显式安全规则匹配		对于 Parameter Problem（参数问题）ICMPv6 消息，需要进行显式安全策略匹配，即使该消息与现有会话关联也不例外。
ICMPv6 重定向 - 需要显式安全规则匹配		对于 Redirect（重定向）ICMPv6 消息，需要进行显式安全策略匹配，即使该消息与现有会话关联也不例外。

协议保护

- Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）> Protocol Protection（协议保护）

防火墙通常允许第 2 层区域之间和 Virtual Wire 区域之间使用非 IP 协议。协议保护可让您控制第 2 层 VLAN 或 Virtual Wire 的安全区域之间或之内所允许（包含）或拒绝（排除）的非 IP 协议。非 IP 协议的示例包括 AppleTalk、Banyan VINES、Novell、NetBEUI 以及监控和数据采集 (SCADA) 系统，如面向通用对象的变电站事件 (GOOSE)。

在区域保护配置文件中配置协议保护后，可将此配置文件应用于第 2 层 VLAN 或 Virtual Wire 的 ingress 安全区域。

通过启用面向互联网的区域上的协议保护，可防止来自您不使用的协议中的第 *2* 层流量进入您的网络。

区域保护配置文件设置 - 协议保护	配置位置	说明
规则类型:	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Protocol**	指定要为协议保护创建的列表的类型： • **Include List**（包含列表）— 除了 IPv4 (0x0800)、IPv6 (0x86DD)、ARP (0x0806) 和 VLAN 标记帧 (0x8100) 以外，仅允许此列表上的协议。无条件拒绝（阻止）所有其他协议。 • **Exclude List**（排除列表）— 仅拒绝此列表上的协议；无条件允许所有其他协议。不能排除 IPv4 (0x0800)、IPv6 (0x86DD)、ARP (0x0806) 或 VLAN 标记帧 (0x8100)。

© 2019 Palo Alto Networks, Inc.

区域保护配置文件设置 - 协议保护	配置位置	说明
	Protection（协议保护）	使用包括列表仅允许您使用的第 *2* 层协议，并拒绝所有其他协议。这会拒绝您在网络上不使用的协议，从而降低攻击面。防火墙仅拒绝您添加到排除列表的协议，并允许列表以外的所有其他协议。如果未配置协议保护，则所有第二层协议均为允许。
协议名称		输入您要添加到列表的以太类型代码所对应的协议名称。防火墙不能验证协议名称是否与以太类型代码匹配，但以太类型代码可确定协议过滤器。
启用		在列表上启用以太类型代码。如果想要禁用有测试用途的协议，但不删除此协议，则禁用即可。
以太网类型(十六进制)		输入以 0x 开头表示十六进制的以太类型代码（协议）（范围为 0x0000 - 0xFFFF）。列表中最多可包含 64 个以太类型。 某些以太类型代码源包括： • IEEE 十六进制以太类型 • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

以太网 *SGT* 保护

- Network（网络）> Network Profiles（网络配置文件）> Zone Protection（区域保护）> Ethernet SGT Protection（以太网 SGT 保护）

对于 Cisco TrustSec 网络中的防火墙，请创建一个包含您要排除的第二层安全组标记 (SGT) 列表的区域保护配置文件。将区域保护配置文件应用到第 2 层、虚拟线或旁接接口。如果带有 802.1Q（以太网 0x8909）标头的传入数据包的 SGT 与列表中的 SGT 匹配，则防火墙将丢弃此数据包。

区域保护配置文件设置	配置位置	说明
第 2 层 SGT 排除列表	**Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护）> **Ethernet SGT Protection**（以太网 **SGT** 保护）	输入安全组标记 (SGT) 列表的名称。
标记		输入您要在 SGT 与应用到区域的区域保护配置文件中该列表匹配时排除的数据包标头中的第 2 层 SGT（范围为 0- 65,535）。
启用		**Enable**（启用）（默认）此以太网 SGT 保护排除列表。取消选择 **Enable**（启用）选项以禁用排除列表。

© 2019 Palo Alto Networks, Inc.

Network（网络）> Network Profiles（网络配置文件）> QoS

Add（添加）QoS 配置文件可定义带宽限制，并为最多八种服务类定义优先级。您可以为独立类和集合类服务定义保证或最大带宽。优先级确定出现冲突时对通信的处理方式。

要全面启用防火墙提供 QoS，还可以：

- 定义要接收 QoS 处理的流量（选择 Policies（策略）> QoS 以添加或修改 QoS 策略）。
- 在接口上启用 QoS（选择 Network（网络）> QoS）。

请参阅服务质量，了解完整的 QoS 工作流程、概念及用例。

QoS 配置文件设置	
配置文件名称	输入名称以标识配置文件（最多 **31** 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
最大出口	输入通过此接口离开防火墙的通信的最大吞吐量 (Mbps)。默认值为 0，指定了防火墙的速率限值（PAN-OS 7.1.16 及更高版本中为 60,000 Mbps，PAN-OS 7.1.15 及更低版本中为 16,000 Mbps）。 QoS 配置文件的 **Egress Max**（最大出口速率）必须小于或等于用 QoS 启用的物理接口的 **Egress Max**（最大出口速率）。请参阅 Network（网络）> QoS。 尽管这不是一个必填字段，但建议始终定义 *QoS* 配置文件的 *Egress Max*（最大出口速率）。
保证的出口	输入此配置文件的保证带宽 (Mbps)。如果超过保证的出口带宽，防火墙会尽量让流量通过。

类	**Add**（添加）并指定处理各个 QoS 类的方式。可以选择要配置的一个或多个类：
	• 类— 即使不配置类，仍可在 QoS 策略中包括类。在这种情况下，通信受限于总体 QoS 限制。将与 QoS 策略不匹配的通信分配给类 4。
	• 优先级 — 单击并选择优先级以分配给某类。
	  • 实时
	  • 高
	  • **Medium**（中）
	  • 低
	发生冲突时，先删除分配了较低优先级的通信。实时优先级使用自己的单独队列。
	• **Egress Max**（最大出口速率）— 单击并输入此类的最大吞吐量 (Mbps)。默认值为 0，指定了防火墙的速率限值（PAN-OS 7.1.16 及更高版本中为 60,000 Mbps，PAN-OS 7.1.15 及更低版本中为 16,000 Mbps）。QoS 类的 **Egress Max**（最大出口速率）必须小于或等于 QoS 配置文件的 **Egress Max**（最大出口速率）。
	尽管这不是一个必填字段，但建议始终定义 *QoS* 配置文件的 *Egress Max*（最大出口）速率值。

© 2019 Palo Alto Networks, Inc.

QoS 配置文件设置	
	• 出口保证 — 单击并输入此类的保证带宽 (Mbps)。分配给某个类别的保证带宽并非为该类别保留的带宽，如不使用，则将继续对所有流量保持可用状态。但是，如果超过流量类的保证出口带宽，则防火墙会尽量让流量通过。

Network（网络> Network Profiles（网络配置文件）> LLDP Profile（LLDP 配置文件）

链路层发现协议 (LLDP) 配置文件即是您在配置防火墙的 LLDP 模式、启用 syslog 和 SNMP 通知以及配置想传输到 LLDP 对端的可选类型长度值 (TLV) 时所采用的方式。配置好 LLDP 配置文件后，您会将该配置文件分配给一个或多个接口。

了解有关 LLDP 的更多信息，包括如何配置和监控 LLDP。

LLDP 配置文件设置	说明
姓名	输入 LLDP 配置文件的名称。
模式	选择 LLDP 的工作模式：**transmit-receive**、**transmit-only**或**receive-only**。
SNMP Syslog 通知	启用 SNMP 陷阱和 syslog 通知，这些通知将按照全局通知间隔发送。如果启用，防火墙将按照**Device**（设备）> **Log Settings**（日志设置）> **System**（系统）> **SNMP Trap Profile**（**SNMP** 陷阱配置文件）和 **Syslog Profile**（**Syslog** 配置文件）中的配置发送 SNMP 陷阱和 syslog 事件。
端口说明	使防火墙的 ifAlias 对象能通过“端口说明”TLV 来发送。
系统名称	使防火墙的 ifAlias 对象能通过“系统名称”TLV 来发送。
系统说明	使防火墙的 sysDescr 对象能通过“系统说明”TLV 来发送。
系统功能	使接口的部署模式（L3、L2 或 virtual wire）能通过“系统功能”TLV 按照以下映射来发送。 • 如果是 L3，防火墙会通告路由器（位 6）功能和另一个位（位 1）。 • 如果是 L2，防火墙会通告 MAC 网桥（位 3）功能和另一个位（位 1）。 • 如果是 virtual wire，防火墙会通告中继器（位 2）功能和另一个位（位 1）。 SNMP MIB 会将接口上已配置的功能组合到单个条目中。
管理地址	使管理地址能通过“管理地址”TLV 来发送。您最多可以输入四个管理地址，这些地址会按照指定顺序发送。如需更改此顺序，请使用 **Move Up**（上移）或 **Move Down**（下移）。
姓名	指定管理地址的名称。
接口	选择其 IP 地址将成为管理地址的接口。如果选择 **None**（无），则可在 IPv4 或 IPv6 选项旁的字段中输入 IP 地址。
IP 选项	选择 **IPv4** 或 **IPv6**，然后在相邻字段中选择或输入要作为管理地址来传输的 IP 地址。如果启用了 **Management Address**（管理地址）TLV，那么至少需要一个管理

© 2019 Palo Alto Networks, Inc.

LLDP 配置文件设置	说明
	地址。如果未配置管理 IP 地址，则系统会使用传输接口的 MAC 地址作为被传输的管理地址。

Network（网络> Network Profiles（网络配置文件）> BFD Profile（BFD 配置文件）

双向转发检测 (BFD) 可在极短时间内完成链路故障的检测，以便故障更快地转移到其他路由。

您在查找什么内容？	请参阅：
什么是 BFD？	BFD 概述
哪些字段可用于创建 BFD 配置文件？	BFD 配置文件的构建块
查看虚拟路由器的 BFD 状态。	查看 BFD 摘要和详细信息
了解更多？	了解和配置 BFD。 配置下列组件的 BFD： 静态路由 BGP OSPF OSPFv3 RIP

BFD 概述

BFD 是一种协议，可识别两个转发引擎（如接口、数据链路或实际转发引擎）之间的双向路径故障。在 PAN-OS 实施中，一个转发引擎为防火墙上的接口，而另一个则为已配置 BFD 的相邻对端。两个引擎之间的 BFD 故障检测用时极短，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。

BFD 检测到故障后，则会通知路由协议切换至对端备用路径。如果已为静态路由配置 BFD，则防火墙会从 RIB 和 FIB 表中删除受影响的路由。

支持 BFD 的接口类型所列如下：物理 Ethernet、AE、VLAN、隧道（站点到站点 VPN 和 LSVPN），以及第 3 层接口的子接口。对于每个静态路由或动态路由协议，您可启用或禁用 BFD、选择默认 BFD 配置文件，或配置 BFD 配置文件。

BFD 配置文件的构建块

- Network（网络> Network Profiles（网络配置文件）> BFD Profile（BFD 配置文件）

您可通过应用默认或创建的 BFD 配置文件，为静态路由或动态路由协议启用 BFD。默认配置文件会使用默认 BFD 设置且不可更改。您可 **Add**（添加）新 BFD 配置文件，并指定以下信息。

© 2019 Palo Alto Networks, Inc.

BFD 配置文件设置	说明
姓名	BFD 配置文件的名称（最多 31 个字符）。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。
模式	BFD 运行的模式： • **Active**（主动）— BFD 发起控制数据包的发送（默认）。BFD 对端中至少有一个要为主动；两个对端可同时为主动。 • **Passive**（被动）— BFD 等待对端发送控制数据包，并在必要时作出响应。
理想最小 Tx 间隔时间（毫秒）	希望 BFD 协议发送 BFD 控制数据包的最小间隔时间（毫秒）。对于 PA-7000 系列，最小值为 50；对于 PA-3200 系列，最小值为 100；对于 VM 系列，最小值为 200（最大值为 2000；默认为 1000）。 如果有多个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 *Tx* 间隔时间）。
必要最小 Rx 间隔时间（毫秒）	BFD 能够接收 BFD 控制数据包的最小间隔时间（毫秒）。对于 PA-7000 系列，最小值为 50；对于 PA-3200 系列，最小值为 100；对于 VM 系列，最小值为 200（最大值为 2000；默认为 1000）。
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 未从其对端接收到 BFD 控制数据包，则会出现故障（范围为 2-50，默认为 3）。
保持时间（毫秒）	防火墙传输 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。如果防火墙在 **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，默认为 0）。默认设置为 0，表示不会应用传输 **Hold Time**（保持时间）；防火墙将在链路建立后，即刻收发 BFD 控制数据包。
启用多跳	在多个跃点上启用 BFD。仅适用于 BGP 实施
最小 Rx TTL	BFD 会在支持多跳 BFD 时接受（接收）的最小生存时间 (TTL) 值（跃点数）。仅适用于 BGP 实施（范围为 1-254，无默认值）。

查看 **BFD** 摘要和详细信息

- Network（网络）> Virtual Routers（虚拟路由器）

下表描述 BFD 摘要信息。

查看 BFD 信息	
查看 BFD 摘要。	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）。选择 **BFD Summary Information**（**BFD** 摘要信息）选项卡。

© 2019 Palo Alto Networks, Inc.

查看 BFD 信息	
查看 BFD 详细信息。	在所需接口的行中，选择 **Details**（详细信息），即可查看 BFD Details（BFD 详细信息）。

Network（网络）> Network Profiles（网络配置文件）> SD-WAN Interface Profile（SD-WAN 接口配置文件）

创建 SD-WAN 接口配置文件，即可按链路标签对物理链路进行分组，并控制链路的速度以及防火墙监控此链路的频率。

	SD-WAN 接口配置文件
姓名	输入 SD-WAN 接口配置文件的名称，最多使用 31 个字母数字字符。名称必须以字母数字字符开头，并可包含字母、数字、下划线 (_)、连字符 (-)、句点 (.) 和空格。
链路标签	选择此配置文件将分配给接口的链路标签，或者添加一个新标签。链路标签绑定了物理链路（不同的 ISP），供防火墙在路径选择和故障转移期间进行选择。
说明	最佳做法是输入配置文件的简要说明。
链路类型	从预定义列表中选择物理链路类型（**ADSL/DSL**、**Cable Modem**（电缆调制解调器）、**Ethernet**（以太网）、**Fiber**（光纤）、**LTE/3G/4G/5G**、**MPLS**、**Microwave/Radio**（微波/无线电）、**Satellite**（卫星）、**WiFi** 或 **Other**（其他））。防火墙支持实现防火墙以太网连接和移交的任何 CPE 设备，例如，WiFi 接入点、LTE 调制解调器、激光微波 CPE 等都可通过以太网移交实现。
最大下载速度 (Mbps)	输入 ISP 提供的最大下载速度，以 Mbps 为单位，范围为 1 至 100,000；没有默认值。询问 ISP 以获取链路速度，或使用 speedtest.net 等工具采样链路的最大速度，并取很长一段时间内的平均最大值。
最大上传速度 (Mbps)	输入 ISP 提供的最大上传速度，以 Mbps 为单位，范围为 1 至 100,000；没有默认值。询问 ISP 以获取链路速度，或使用 speedtest.net 等工具采样链路的最大速度，并取很长一段时间内的平均最大值。
纠错配置文件接口的选择条件	勾选此设置以使（应用此配置文件的）接口符合防火墙编码要求，从而选择将这些接口用于前向纠错 (FEC) 或数据包重复。您可以取消选择该设置，以便永远不会在应用配置文件的昂贵链接（接口）上使用昂贵的 FEC 或数据包重复。指定用于该配置文件的 **Link Type**（链路类型）可确定是否勾选 **Eligible for Error Correction Profile interface selection**（纠错配置文件接口的选择条件）的默认设置。 若要配置 FEC 或数据报重复，请创建 SD-WAN 纠错配置文件。
VPN 数据隧道支持	确定从分支到中心的流量以及回传流量是流经 VPN 隧道以增强安全性（默认启用），还是从 VPN 隧道外流过以避免加密开销。 • 对具有 Internet 直接连接或 Internet 中断功能的公共链路类型启用 **VPN Data Tunnel Support**（**VPN** 数据隧道支持），例如，电缆调制解调器、ADSL 等其他 Internet 连接。 • 您可以对不具有互联网中断功能的 MPLS、卫星或微波等私有链路类型禁用**VPN Data Tunnel Support**（**VPN** 数据隧道支持）。但是，您必须先确定此流量不会因为在 VPN 隧道外传输而被拦截。

© 2019 Palo Alto Networks, Inc.

	SD-WAN 接口配置文件
	• 很多分支拥有的 DIA 流量都需要故障转移到与中心连接的私有 MPLS 链路，然后从中心到达 Internet。**VPN Data Tunnel Support**（**VPN** 数据隧道支持）设置决定了私有数据流量是否经过 VPN 隧道传输，以及故障转移流量是否使用私有数据流量不会使用的其他连接。防火墙使用区域对源自 MPLS 私有流量的 DIA 故障转移流量进行分段。
VPN 故障转移指标	（PAN-OS 10.0.3 以及 10.0 的更高版本）一旦配置 DIA AnyPath，就需要一种方法来指定绑定到用于 DIA 故障转移的中心虚拟接口或分支虚拟接口的各个 VPN 隧道的故障转移顺序。指定 VPN 隧道（链路）的 VPN 故障转移指标；范围为 1- 65,535；默认为 10。指标值越低，在故障转移时选择的隧道（应用此配置文件的链路）优先级越高。 例如，将此指标设为一个较低的值，并应用配置文件到宽带接口；然后创建一个不同的配置文件，该配置文件会设置一个较高的指标，以将其应用到昂贵的 LTE 接口，确保仅在宽带完成故障转移后才会使用此接口。
路径监视	选择防火墙用于监控（应用此 SD-WAN 接口配置文件的）接口的路径监控模式。 • **Aggressive**（积极）—（默认适用于除 LTE 和卫星之外的所有链路类型）防火墙以固定的频率将探测数据包发送到 SD-WAN 链路的另一端。 如果您需要针对电源不足和停电情况进行快速检测和故障转移，请使用积极模式。 • **Relaxed**（宽松的）—（默认适用于 LTE 和卫星链路类型）防火墙发送探测数据包集之间会安排几秒钟的间歇时间（**Probe Idle Time**（探测空闲时间）），从而降低路径监视的频率。探测空闲时间结束后，防火墙根据配置的 **Probe Frequency**（探测频率）发送为时七秒钟的探测数据包。 如果您使用的链路为低带宽、按使用情况收费（例如，*LTE*），或是在快速检测不如节省成本和带宽重要时，可以使用宽松模式。
探测频率（每秒）	输入探测频率，即防火墙在一秒内发送探测数据包到 SD-WAN 链路另一端的次数（范围为 1 至 5；默认为 5）。
探测空闲时间（秒）	如果选择 **Relaxed**（宽松）路径监控，则可以设置防火墙在发送探测数据包后等待多长的时间（即探测空闲时间，以秒为单位，范围为 1 到 60；默认为 60）再继续发送。
故障恢复保持时间（秒）	输入防火墙在链路执行故障转移后将此链路恢复为首选链路之前，等待链路恢复以保持合格的时间长度（以秒为单位，范围为 20 至 120；默认值为 120）。故障恢复保持时间可防止过快地将恢复的链路恢复为首选链路从而导致其立即再次发生故障。

© 2019 Palo Alto Networks, Inc.

设备

以下各节可用作防火墙基本系统配置和维护任务的现场参考：

> Device（设备）> Setup（设置）
> Device（设备）> High Availability（高可用性）
> Device（设备）> Log Forwarding Card（日志转发卡）
> Device（设备）> Config Audit（配置审核）
> Device（设备）> Password Profiles（密码配置文件）
> Device（设备）> Administrators（管理员）
> Device（设备）> Admin Roles（管理员角色）
> Device（设备）> Access Domain（访问域）
> Device（设备）> Authentication Profile（身份验证配置文件）
> Device（设备）> Authentication Sequence（身份验证序列）
> Device（设备）> User Identification（用户标识）
> Device（设备）> Data Redistribution（数据重新分发）
> Device（设备）> Device Quarantine（设备隔离）
> Device（设备）> VM Information Sources（VM 信息源）
> Device（设备）> Troubleshooting（故障排除）
> Device（设备）> Virtual Systems（虚拟系统）
> Device（设备）> Shared Gateways（共享网关）
> Device（设备）> Certificate Management（证书管理）
> Device（设备）> Response Pages（响应页面）
> Device（设备）> Log Settings（日志设置）
> Device（设备）> Server Profiles（服务器配置文件）
> Device（设备）> Local User Database（本地用户数据库）> Users（用户）
> Device（设备）> Local User Database（本地用户数据库）> User Groups（用户组）
> Device（设备）> Scheduled Log Export（计划日志导出）
> Device（设备）> Software（软件）
> Device（设备）> GlobalProtect Client（GlobalProtect 客户端）
> Device（设备）> Dynamic Updates（动态更新）
> Device（设备）> Licenses（许可证）
> Device（设备）> Support（支持）
> Device（设备）> Master Key and Diagnostics（主密钥和诊断）
> Device（设备）> Policy Recommendation（策略建议）

Device（设备）> Setup（设置）

- Device（设备）> Setup（设置）> Management（管理）
- Device（设备）> Setup（设置）> Operations（操作）
- Device（设备）> Setup（设置）> HSM
- Device（设备）> Setup（设置）> Services（服务）
- Device（设备）> Setup（设置）> Interfaces（接口）
- Device（设备）> Setup（设置）> Telemetry（遥测）
- Device（设备）> Setup（设置）> Content-ID
- Device（设备）> Setup（设置）> WildFire
- Device（设备）> Setup（设置）> Session（会话）

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Management（管理）

- **Device**（设备）> **Setup**（设置）> **Management**（管理）
- **Panorama** > **Setup**（设置）> **Management**（管理）

在防火墙上，选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）可配置管理设置。

在 Panorama™ 上，选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）可配置使用 Panorama 模板管理的防火墙。选择**Panorama** > **Setup**（设置）> **Management**（管理）可配置 Panorama 管理设置。

以下管理设置同时适用于防火墙和 Panorama，除非另有说明。

- 常规设置
- 身份验证设置
- 策略规则库设置
- Panorama 设置：Device（设备）> Setup（设置）> Management（管理）（在连接到 Panorama 的防火墙上配置设置）
- Panorama 设置：Panorama > Setup（设置）> Management（管理）（在连接到防火墙的 Panorama 上配置设置）
- 记录和报告设置
- 横幅和消息
- 最小密码复杂性
- AutoFocus™
- Cortex 数据湖
- SSH 管理配置文件设置

项目	说明
常规设置	
主机名	输入主机名（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。 如果您未输入任何值，PAN-OS® 会将防火墙型号（如 PA-5220_2）用作默认值。 或者，您也可配置防火墙使用 DHCP 服务器提供的主机名。请参阅接受 DHCP 服务器提供的主机名（仅限防火墙）。 配置唯一主机名，以轻松标识您正在管理的设备。
域	输入防火墙的网络域名（最多 31 个字符）。 或者，您也可配置防火墙和 Panorama 使用 DHCP 服务器提供的域。请参阅接受 DHCP 服务器提供的域（仅限防火墙）。
接受 DHCP 服务器提供的主机名（仅限防火墙）	（仅适用于管理接口 IP 类型为 DHCP 客户端的情况）选择此选项可让管理接口接受从 DHCP 服务器接收的主机名。来自服务器的主机名（如有效）可替换 Hostname（主机名）字段中指定的任何值。

© 2019 Palo Alto Networks, Inc.

项目	说明
接受 DHCP 服务器提供的域（仅限防火墙）	（仅适用于管理接口 IP 类型为 DHCP 客户端的情况）选择此选项可让管理接口接受从 DHCP 服务器接收的域（DNS 后缀）。来自服务器的域可替换 **Domain**（域）字段中指定的任何值。
登录提示	输入文本（最多 3,200 个字符）以在 **Name**（名称）和 **Password**（密码）字段下的 Web 界面登录页面上显示。
强制管理员确认登录横幅	选择此选项可（在登录页面的登录横幅上方）显示 **I Accept and Acknowledge the Statement Below**（我接受并确认以下陈述）选项，并强制管理员选择此选项，从而强制管理员确认，他们理解并接受此消息的内容后才能 **Login**（登录）。
SSL/TLS 服务配置文件	分配现有的 SSL/TLS 服务配置文件或创建新的 SSL/TLS 服务配置文件，以指定管理接口上允许的证书和 SSL/TLS 协议设置（请参阅 Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件））。防火墙或 Panorama 使用此证书对通过管理 (MGT) 接口或支持 HTTP/HTTPS 管理流量的任何其他接口访问 Web 界面的管理员进行身份验证（请参阅 Network（网络）> Network Profiles（网络配置文件）> Interface Mgmt（接口管理））。如果选择 **None**（无）（默认），则防火墙或 Panorama 将使用预定义证书。 为方便起见，提供了预定义证书。为了实现更好的安全性，请分配一个 *SSL/TLS* 服务配置文件。为确保信任，必须通过客户端系统的受信任根证书存储中的证书颁发机构 *(CA)* 证书进行签名。
时区	选择防火墙的时区。
区域设置	从下拉列表中选择用于 PDF 报告的语言。请参阅 Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要）。 即使您已为 Web 界面设置了特定语言首选项，PDF 报告仍会使用为 **Locale**（区域设置）指定的语言。
日期	在防火墙上设置日期；输入当前日期（格式为 YYYY/MM/DD），或从下拉列表中选择日期。 您还可以定义 *NTP* 服务器（*Device*（设备）> *Setup*（设置）> *Services*（服务））。
时间	在防火墙上设置日期；输入当前时间（24 小时制格式）或从下拉列表中选择时间。 您还可以定义 *NTP* 服务器（*Device*（设备）> *Setup*（设置）> *Services*（服务））。
序列号	输入 Panorama 的序列号。您可以在 Palo Alto Networks® 发送给您的订单完成电子邮件中找到序列号。

© 2019 Palo Alto Networks, Inc.

项目	说明
（仅限 Panorama 虚拟设备）	
纬度	输入防火墙的纬度（-90.0 至 90.0）。
经度	输入防火墙的经度（-180.0 至 180.0）。
自动获取提交锁定	更改待选配置时，请选中此选项以自动应用提交锁定。有关更多信息，请参阅锁定配置。 启用 *Automatically Acquire Commit Lock*（自动获取提交锁定），这样，在第一个管理员提交更改前，其他管理员不能对配置进行更改。
证书到期检查	指示防火墙在证书接近其到期日时创建警告消息。 启用 *Certificate Expiration Check*（证书到期检查）以在证书接近其到期日时生成警告消息。
多虚拟系统功能	启用使用支持此功能的防火墙上的多个虚拟系统（请参阅 Device（设备）> Virtual Systems（虚拟系统））。 要在防火墙上启用多个虚拟系统，则防火墙策略不得引用超过 *640* 个不同的用户组。必要时，可减少引用的用户组的数量。然后，在您启用并添加多个虚拟系统后，策略将可为每个附加的虚拟系统引用另外的 *640* 个用户组。
URL 筛选数据库 （仅限 Panorama）	选择与 Panorama 搭配使用的 URL 过滤服务供应商：**brightcloud** 或 **paloaltonetworks** (PAN-DB)。
使用虚拟机监控程序分配的 MAC 地址 （仅限 VM 系列防火墙）	选择此选项可使 VM 系列防火墙使用虚拟机监控程序分配的 MAC 地址，而不是使用 PAN-OS 自定义模式生成 MAC 地址。 如果启用此选项且使用接口的 IPv6 地址，则接口 ID 不得使用 EUI-64 格式，这可以根据接口 MAC 地址派生出 IPv6 地址。在高可用性 (HA) 主动/被动配置中，如果使用 EUI-64 格式，则可能会出现提交错误。
GTP 安全	选择此选项以启用检查 GPRS 隧道协议 (GTP) 通信中控制面板和用户数据平面消息的功能。请参阅 Objects（对象）> Security Profiles（安全配置文件）> Mobile Network Protection（移动网络保护）以配置移动网络保护配置文件，以便可以对 GTP 通信执行策略。
SCTP 安全	选择此选项以启用检查和筛选流控制传输协议 (SCTP) 数据包和块的功能，并应用 SCTP 启动 (INIT) 泛滥攻击保护。请参阅 Objects（对象）> Security Profiles（安全配置文件）> SCTP Protection（SCTP 保护）。有关 SCTP INIT 泛滥攻击保护，请参阅配置 SCTP INIT 泛滥攻击保护。

© 2019 Palo Alto Networks, Inc.

项目	说明
高级路由	勾选此选项可启用支持 BGP 和静态路由的高级路由引擎。要使路由引擎的新更改生效（或更改为旧路由引擎），您必须提交并重新启动防火墙。 高级路由处于预览模式，其功能集有限。
隧道加速	勾选此选项以提高性能和通过 GRE 隧道、VXLAN 隧道和 GTP-U 隧道的流量吞吐量。此选项默认被启用。 • **GRE and VXLAN tunnel acceleration**（**GRE** 和 **VXLAN** 隧道加速）— PA-3200 系列防火墙以及使用 PA-7000-NPC 和 SMC-B 的 PA-7000 系列防火墙均支持 GRE 和 VXLAN 隧道加速。 • **GTP-U tunnel acceleration**（**GTP-U** 隧道加速）— 使用 A-7000-NPC 和 SMC-B 的 PA-7000 系列防火墙均支持 GTP-U 隧道加速。对于使用隧道加速的 GTP-U 隧道流量，必须启用隧道加速和 GTP，但不能为 GTP-U 协议配置隧道内容检测 (TCI) 策略规则，此外，附加有移动网络保护配置文件的安全策略规则必须允许 GTP 流量。 如果禁用或重新启用隧道加速并提交，那么，必须重新启动防火墙。
Device Certificate（设备证书）	
获取证书	单击以输入从 Palo Alto Networks 客户支持门户生成的一次性密码 (OTP)。为使用 CSP 成功对 Panorama 执行身份验证，并利用零接触配置 (ZTP)、IoT、设备遥测以及企业数据丢失防护 (DLP) 等云服务，必须使用设备证书。设备证书安装成功后，将显示如下内容： • **Current Device Certificate Status**（当前设备证书状态）— 设备证书的当前状态（有效、无效或已过期） • **Not Valid Before**（有效开始时间）— 指示设备证书有效期开始时间的时间戳。 • **Not Valid After**（有效结束时间）—指示设备证书有效性到期的时间戳，设备证书变为无效或到期。 • **Last Fetched Message**（上次获取消息）— 显示设备证书是否安装成功的消息。 • **Last Fetched Status**（上次获取状态）— 获取设备证书的状态（成功或失败）。 • **Last Fetched Timestamp**（上次获取时间戳）—上次设备证书安装尝试的时间戳。
身份验证设置	
身份验证配置文件	选择防火墙用于对在外部服务器（而非在防火墙上本地）定义的管理帐户进行身份验证的身份验证配置文件（或序列）（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。当外部管理员登录时，防火墙从外部服务器请求身份验证和身份验证信息（如管理角色）。

© 2019 Palo Alto Networks, Inc.

项目	说明
	根据身份验证配置文件指定的服务器类型为需要其他步骤的外部管理员启用身份验证，服务器类型必须为下列之一： • RADIUS • TACACS+ • SAML 管理员可以使用 *SAML* 对 *Web* 界面进行身份验证，而不对 *CLI* 进行身份验证。 选择 **None**（无）可禁用外部管理员的身份验证。 对于（在防火墙上）本地定义的管理帐户，防火墙使用分配给这些帐户的身份验证配置文件进行身份验证（请参阅 Device（设备）> Administrators（管理员））。
证书配置文件	选择证书配置文件以验证配置为基于证书访问防火墙 Web 界面的管理员的客户端证书。有关配置证书配置文件的说明，请参阅 Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）。 配置证书配置文件，确保管理员的主机具有正确的证书，以便使用证书配置文件中定义的根 *CA* 证书进行身份验证。
空闲超时	输入在管理员自动注销之前 Web 界面或 CLI 上没有执行任何活动的最长时间（分钟）（范围为 0 至 1,440，默认为 60）。值为 0 表示不活动不会触发自动注销。 手动和自动刷新 *Web* 界面页面（如 *Dashboard*（仪表盘）和 *System Alarms*（系统警报）对话框）将重置 *Idle Timeout*（空闲超时）计数器。要使防火墙在支持自动刷新的页面上强制执行超时，请将刷新时间间隔设置为 *Manual*（手动）或设置为大于 *Idle Timeout*（空闲超时）的值。也可以在 *ACC* 选项卡中禁用 *Auto Refresh*（自动刷新）。 设置 *Idle Timeout*（空闲超时）为 *10* 分钟，以防止在管理员打开防火墙会话时未经授权的用户访问防火墙。
API 密钥生命周期	输入 API 密钥有效的时间长度（以分钟为单位，范围为 0-525,600，默认为 0）。值为 0 表示 API 密钥永不过期。 **Expire All API Keys**（使所有 **API** 密钥过期）可使先前生成的所有 API 密钥无效。请谨慎使用此选项，因为现在所有密钥都将变得无效，且您当前正在使用这些 API 密钥的所有操作都将停止运行。 可在维护窗口期间使用此操作，这样，您可以在不会中断应用 *API* 密钥的当前操作的情况下更换密钥。

© 2019 Palo Alto Networks, Inc.

项目	说明
API 密钥上次过期	显示 API 密钥上次过期的时间戳。如果您从未重置您的密钥，则此字段没有值。
失败的尝试次数	输入锁定管理员帐户之前防火墙允许的 Web 界面和 CLI 登录尝试失败次数（范围为 0 至 10 次）。值 0 代表没有登录尝试限制。防火墙处于正常运行模式时，默认值为 0；防火墙处于 FIPS-CC 模式时，默认值为 10。限制登录尝试可以帮助防火墙防止暴力攻击。 如果将失败的尝试次数设置为除 *0* 以外的值，但将锁定时间保留为 *0*，则忽略失败的尝试次数且从不锁定用户。 将 *Failed Attempts*（失败的尝试次数）设置为 *5* 或更少，以便在输入错误时容纳合理的重试次数，同时防止恶意系统尝试通过暴力攻击方法登录到防火墙。
锁定时间	输入达到 **Failed Attempts**（失败的尝试次数）限制后，防火墙锁定管理员访问 Web 界面和 CLI 所需的分钟数（范围为 0 至 60 分钟）。值为 0（默认）表示应用锁定，直到其他管理员手动解锁用户帐户。 如果设置 *Failed Attempts*（失败的尝试次数）为除 *0* 以外的一个值，但将*Lockout Time*（锁定时间）设置为 *0*，那么，在设置失败登录尝试次数后，用户将被锁定，直到其他管理员手动解锁此账户。 设置 *Lockout Time*（锁定时间）为至少 *30* 分钟，防止恶意操作者连续登录尝试。
最大会话计数	输入所有管理员和用户账户允许的并发会话数（范围为 0-4）。值为 0（默认值）则表示允许的并发会话数无上限。 在 *FIPS-CC* 模式下，范围为 *1-4*，默认值为 *4*。
最长会话时间	输入活跃，非空闲管理员可以保持登录状态的分钟数（范围为 60-1,499）。一旦达到该最长会话时间，会话将终止，并要求重新进行身份验证，然后才能开始另一个会话。默认值设为 0（30 天），该值不能手动输入。如果未输入值，**Max Session Time**（最长会话时间）默认值将为 0。 在 *FIPS-CC* 模式下，范围为 *60-1,499*，默认值为 *720*。如果未输入值，*Max Session Time*（最长会话时间）默认值将为 *720*。
策略规则库设置	
策略所需标记	创建新策略规则时，至少需要一个标记。如果在启用此选项时策略规则已存在，在下次编辑规则时，您必须至少添加一个标记。

© 2019 Palo Alto Networks, Inc.

项目	说明
策略所需说明	要求您在创建新策略规则时添加的 **Description**（说明）。如果在启用此选项时策略规则已存在，在下次编辑规则时，您必须添加 **Description**（说明）。
如果策略无标记或说明，则提交失败	如果未向策略规则添加任何标记或说明，则强制您提交失败。如果在启用此选项时策略规则已存在，在下次编辑规则时若未添加标记或说明，则提交将会失败。 要使提交失败，您必须添加 **Require tag on policies**（策略所需标记）或 **Require description on policies**（策略所需说明）。
策略所需审核注释	创建新策略规则时，需要 **Audit Comment**（审核注释）。如果在启用此选项时策略规则已存在，在下次编辑规则时，您必须添加 **Audit Comment**（审核注释）。
审核注释正则表达式	指定审核注释中注释格式参数的要求。
策略规则命中次数	跟踪通信与您在防火墙上配置的策略规则匹配的频率。启用此选项后，您可以查看针对每个规则的总流量匹配数的总命中次数，以及规则创建、修改、第一次命中和最后一次命中的日期和时间。
策略应用程序使用情况	

Panorama 设置：Device（设备）> Setup（设置）> Management（管理）

在防火墙或 Panorama 的模板中配置以下设置。这些设置用于建立从防火墙到 Panorama 的连接。

您还必须在 Panorama 上配置连接和对象共享设置（Panorama 设置：Panorama > Setup（设置）> Management（管理））。

防火墙将使用带 *AES256* 加密的 *SSL* 连接来进行 *Panorama* 注册。默认情况下，使用预定义的 *2,048* 位证书使 *Panorama* 和防火墙相互验证身份，再使用 *SSL* 连接进行配置管理和日志收集。要进一步保护 *Panorama*、防火墙和日志收集器之间的 *SSL* 连接，请参阅安全客户端通信以配置防火墙和 *Panorama* 或日志收集器之间的自定义证书。

Panorama 服务器	输入 Panorama 服务器的 IP 地址或 FQDN。如果 Panorama 采用高可用性 (HA) 配置，请在第二个 **Panorama Servers**（**Panorama** 服务器）字段中输入辅助 Panorama 服务器的 IP 地址或 FQDN。
连接到 Panorama 的接收超时	输入从 Panorama 接收 TCP 消息的超时值（以秒为单位，范围为 1 至 240，默认为 240）。
连接到 Panorama 的发送超时	输入将 TCP 消息发送到 Panorama 的超时值（以秒为单位，范围为 1 至 240，默认为 240）。
对 Panorama 的 SSL 发送的重试次数	输入在将安全套接字层 (SSL) 消息发送到 Panorama 时的重试次数（范围为 1 至 64，默认为 25）。
启用自动提交恢复	启用此选项后，可使防火墙在以下情况中自动验证其与 Panorama 管理服务器的连接：提交配置并将其推送到防火墙时，以及成功推送配置后按配置的时间间隔进行验证。

© 2019 Palo Alto Networks, Inc.

项目	说明
	启用后，防火墙无法验证其与 Panorama 管理服务器的连接，防火墙和 Panorama 管理服务器会自动将其配置恢复为之前运行的配置，以恢复连接。
检查 Panorama 连接的尝试次数	**Enable Automated Commit Recovery**（启用自动提交恢复）启用后，配置防火墙测试其与 Panorama 管理服务器连接的次数。
重试时间间隔（秒）	**Enable Automated Commit Recovery**（启用自动提交恢复）启用后，配置防火墙进行与 Panorama 管理服务器连接测试的间隔时间（以秒为单位）。

安全客户端通信	启用 **Secure Client Communication**（安全客户端通信）可确保防火墙使用配置的自定义证书（而非默认证书），对与 Panorama 或日志收集器的 SSL 连接进行身份验证。
	• **None**（无）（默认）— 不配置任何设备证书，而使用默认预定义证书。
	• **Local**（本地）— 防火墙使用在防火墙上生成或从现有企业 PKI 服务器导入的本地设备证书和相应私钥。
	  • **Certificate**（证书）— 选择您生成或导入的本地设备证书。此证书可能是防火墙的唯一证书（基于该防火墙的序列号的哈希），也可能是连接到 Panorama 的所有防火墙使用的公共设备证书。
	  • **Certificate Profile**（证书配置文件）— 从下拉列表中选择证书配置文件。证书配置文件定义用于验证客户端证书的 CA 证书以及如何验证证书吊销状态。
	• **SCEP** — 防火墙通过简单证书注册协议 (SCEP) 服务器生成的设备证书和私钥。
	  • **SCEP Profile**（**SCEP** 配置文件）— 从下拉列表中选择Device（设备）> Certificate Management（证书管理）> SCEP。SCEP 配置文件为 Panorama 提供通过企业 PKI 中的 SCEP 服务器对客户端设备进行身份验证所需的信息。
	  • **Certificate Profile**（证书配置文件）— 从下拉列表中选择Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）。证书配置文件定义用于验证客户端证书的 CA 证书以及如何验证证书吊销状态。

	• **Customize Communication**（自定义通信）— 防火墙使用其配置的自定义证书对所选设备进行身份验证。
	  • **Panorama Communication**（**Panorama** 通信）— 防火墙使用配置的客户端证书与 Panorama 进行通信。
	  • **PAN-DB Communication**（**PAN-DB** 通信）— 防火墙使用配置的客户端证书与 PAN-DB 设备进行通信。
	  • **WildFire Communication**（**WildFire** 通信）— 防火墙使用配置的客户端证书与 WildFire® 设备进行通信。
	  • **Log Collector Communication**（日志收集器通信）— 防火墙使用配置的客户端证书与日志收集器进行通信。
	  • **Check Server Identity**（检查服务器标识）—（仅限 Panorama 和日志收集器通信）防火墙通过将通用名称 (CN) 与服务器的 IP 地址或 FQDN 进行匹配来确认服务器标识。

© 2019 Palo Alto Networks, Inc.

项目	说明
禁用/启用 Panorama 策略和对象	仅当在防火墙（而非 Panorama 的模板中）上编辑 **Panorama Settings**（**Panorama** 设置）时，会显示此选项。 **Disable Panorama Policy and Objects**（禁用 **Panorama** 策略和对象）可禁用传播到防火墙的设备组策略和对象。默认情况下，该操作还会将这些策略和对象从防火墙中删除。如需在防火墙上保留设备组策略和对象的本地副本，请在单击此选项后打开的对话框中选择 **Import Panorama Policy and Objects before disabling**（禁用前导入 **Panorama** 策略和对象）。在执行提交之后，这些策略和对象就会成为防火墙配置的一部分且 Panorama 不再管理它们。 在正常运行情况下，不需要禁用 Panorama 管理，禁用会让防火墙的维护和配置变得复杂。通常，该选项适用于防火墙需要不同于在设备组中所定义的规则和对象值的情况。例如，在防火墙完成生产并移入实验室环境进行测试时。 要将防火墙策略和对象管理恢复到 Panorama 中，请单击启用 **Panorama** 策略和对象。
禁用/启用设备和网络模板	仅当在防火墙（而非 Panorama 的模板中）上编辑 **Panorama Settings**（**Panorama** 设置）时，会显示此选项。 **Disable Device and Network Template**（禁用设备和网络模板）可禁用传播到防火墙的模板信息（设备和网络配置）。默认情况下，该操作还会将模板信息从防火墙中删除。如需在防火墙上保留模板信息的本地副本，请在单击此选项后打开的对话框中，选择**Import Device and Network Templates before disabling**（禁用前导入设备和网络模板）。在执行提交之后，模板信息就会成为防火墙配置的一部分且 Panorama 不再管理该信息。 在正常运行情况下，不需要禁用 *Panorama* 管理，禁用会让防火墙的维护和配置变得复杂。通常，该选项适用于防火墙需要不同于在模板中组所定义的设备和网络配置值的情况。例如，在防火墙完成生产并移入实验室环境进行测试时。 要配置防火墙再次接受模板，请单击启用设备和网络模板。

Panorama 设置：Panorama > Setup（设置）> Management（管理）

如要使用 Panorama 来管理防火墙，请在 Panorama 上配置以下设置。这些设置可确定从 Panorama 到受管防火墙的连接的超时和 SSL 消息尝试次数，以及还确定对象共享参数。

您还必须在防火墙或 Panorama 的模板中配置 Panorama 连接设置：请参阅 Panorama 设置：Device（设备）> Setup（设置）> Management（管理））。

防火墙将使用带 *AES256* 加密的 *SSL* 连接来进行 *Panorama* 注册。默认情况下，使用预定义的 *2,048* 位证书使 *Panorama* 和防火墙相互验证身份，再使用 *SSL* 连接进行配置管理和日志收集。要进一步保护这些 *SSL* 连接，请参阅自定义安全服务器通信以配置 *Panorama* 及其客户端之间的自定义证书。

连接到设备的接收超时	输入从所有受管防火墙接收 TCP 消息的超时值（以秒为单位，范围为 1 至 240，默认为 240）。

© 2019 Palo Alto Networks, Inc.

项目	说明
连接到设备的发送超时	输入将 TCP 消息发送到所有受管防火墙的超时值（以秒为单位，范围为 1 至 240，默认为 240）。
对设备的 SSL 发送的重试次数	输入在将安全套接字层 (SSL) 消息发送到受管防火墙时的允许重试次数（范围为 1 至 64，默认为 25）。
与设备共享未使用的地址和服务对象	选择此选项（默认启用）可与受管防火墙共享所有 Panorama 共享对象和设备组特定对象。 如果禁用此选项，设备将检查 Panorama 的地址、地址组、服务和服务组对象的引用策略，而且不会共享任何非引用对象。该选项可确保设备只将所需对象发送至受管防火墙，从而减少总对象数。 如果您有一个面向设备组中特定设备的策略规则，那么该策略中使用的对象将被认为在该设备组中使用。
在父对象中定义的对象将具有较高的优先级	选择此选项（默认禁用）可指定当层次结构不同级别中的设备组拥有相同的类型和名称但值不同时，父对象组中的对象值的优先级高于子对象组中的对象值。这意味着在您执行设备组提交时，祖先值将会替换所有替代值。同样，此选项可使共享对象的值替代设备组中相同类型和名称的对象的值。 选择此选项将显示查找替代对象链接。
查找替代对象	选择此选项（Panorama Settings（Panorama 设置）对话框底部）可列出任何阴影对象。阴影对象是设备组中具有相同名称但具有不同值的共享位置中的对象。该链接仅在您指定在父对象中定义的对象将具有较高的优先级时才会显示。
在组中启用报告和过滤	选择此选项（默认显示），以使 Panorama 能够在本地存储从防火墙接收的用户名、用户组名称和用户到组映射信息。此选项是适用于 Panorama 中所有设备组的全局设置。但是，您还必须通过指定主设备并将防火墙配置为从主设备存储用户和组，在每个设备组级别启用本地存储。
安全通信设置：Panorama > Setup（设置）> Management（管理）	
自定义安全服务器通信	• **Custom Certificate Only**（仅自定义证书）— 启用后，Panorama 仅接受用于对受管防火墙和日志收集器进行身份验证的自定义证书。 • **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）— 从下拉列表中选择 SSL/TLS 服务配置文件。此配置文件定义防火墙可以用于与 Panorama 进行通信的证书和支持的 SSL/TLS 版本。 • **Certificate Profile**（证书配置文件）— 从下拉列表中选择证书配置文件。此证书配置文件定义证书吊销检查行为和用于对客户端提供的证书链进行身份验证的根 CA。 • **Authorization List**（授权列表）— 使用以下字段 **Add**（添加）并配置新的授权配置文件，以设置授权可连接到 Panorama 的客户端设备的标准。Authorization List（授权列表）最多支持 16 个配置文件条目。 • **Identifier**（标识符）— 选择 **Subject**（主题）或 **Subject Alt**。**Name**（主题备选名称）作为授权标识符。

© 2019 Palo Alto Networks, Inc.

项目	说明
	• **Type**（类型）— 如果选择 **Subject Alt.Name**（主题备选名称）作为标识符，则选择 **IP**、**hostname**（主机名）或 **e-mail**（电子邮件）作为标识符类型。如果选择了 **Subject**（主题），则必须使用 **common name**（公共名称）作为标识符类型。 • **Value**（值）— 输入标识符值。 • **Authorize Clients Based on Serial Number**（根据序列号对客户端进行授权）— Panorama 根据设备序列号哈希对客户端设备进行授权。 • **Check Authorization List**（检查身份验证列表）— Panorama 根据身份验证列表检查客户端设备标识。设备只需要与列表中的一个项目相匹配，即可获得授权。如果找不到匹配项，则不对设备进行授权。 • **Disconnect Wait Time (min)**（断开连接等待时间（分钟））— Panorama 在与其受管设备断开当前连接之前等待的时间（以分钟为单位）。然后，Panorama 使用配置的安全服务器通信设置重新建立与其受管设备的连接。等待时间自您提交安全服务器通信配置后开始算起。

安全客户端通信	使用 **Secure Client Communication**（安全客户端通信）可确保客户端 Panorama 使用配置的自定义证书（而非默认预定义证书），对与 HA 对或 WildFire 设备中的其他 Panorama 设备的 SSL 连接进行身份验证。
	• **Predefined**（预定义）（默认）— 不配置任何设备证书，Panorama 使用默认预定义证书。
	• **Local**（本地）— Panorama 使用在防火墙上生成或从现有企业 PKI 服务器导入的本地设备证书和相应私钥。
	  • **Certificate**（证书）— 选择本地设备证书。
	  • **Certificate Profile**（证书配置文件）— 从下拉列表中选择证书配置文件。
	• **SCEP** — Panorama 使用简单证书注册协议 (SCEP) 服务器生成的设备证书和私钥。
	  • **SCEP Profile**（**SCEP** 配置文件）— 从下拉列表中选择 SCEP 配置文件。
	  • **Certificate Profile**（证书配置文件）— 从下拉列表中选择证书配置文件。
	• 自定义通信
	  • **HA Communication**（**HA** 通信）— Panorama 使用配置的客户端证书与及 HA 对端进行 HA 通信。
	  • **WildFire Communication**（**WildFire** 通信）— Panorama 使用配置的客户端证书与 WildFire 设备进行通信。

记录和报告设置

使用此部分可修改：

- 适用于报告和下列日志类型的过期期限和存储配额。在高可用性对之间同步的设置。
  - 防火墙在本地生成和存储的所有类型的日志（**Device**（设备）> **Setup**（设置）> **Management**（管理））。应用到防火墙上所有虚拟系统的设置。

© 2019 Palo Alto Networks, Inc.

项目	说明
	• Panorama 模式下的 M 系列设备和 Panorama 虚拟设备在本地生成和存储的日志：系统、配置、应用程序统计信息和 User-ID™ 日志（**Panorama** > **Setup**（设置）> **Management**（管理））。 • 传统模式下的 Panorama 虚拟设备本地生成或从防火墙收集的所有类型的日志（**Panorama** > **Setup**（设置）> **Management**（管理））。 对于防火墙发送到 *Panorama* 日志收集器的日志，可以在每个收集器组中设置存储配额和过期期限（请参阅 Panorama > Collector Groups（收集器组））。 • 用于计算和导出用户活动报告的属性。 • 防火墙或 Panorama 上创建的预定义报告。
日志存储选项卡 （除 PA-5200 系列和 PA-7000 系列防火墙以外的 Panorama 管理服务器和所有防火墙型号） 如果编辑日志记录和报告设置（*Panorama* > *Setup*（设置）> *Management*（管理）），*Panorama* 将显示此选项卡。如果使用 *Panorama* 模板配置防火墙的设置（*Device*（设备）> *Setup*（设置）> *Management*（管理）），请参阅单磁盘存储和多磁盘存储选项卡。	对于每种日志类型，请指定： • **Quota**（配额）— 在硬盘上以百分比为单位为日志存储分配的**Quota**（配额）。更改配额值时，相关联的磁盘分配情况会自动更改。如果所有值的总和超出 100%，则会显示红色消息，并将在您尝试保存设置时显示错误消息。如果发生这种情况，请调整百分比值以使总和在 100% 限制范围内。 *VM* 系列防火墙默认为 *SCTP* 日志存储、*SCTP Summary*（*SCTP* 摘要）、*Hourly SCTP Summary*（每小时 *SCTP* 摘要）、*Daily SCTP Summary*（每日 *SCTP* 摘要）和 *Weekly SCTP Summary*（每周 *SCTP* 摘要）分配 *0#* 的配额，因此您必须分配一定百分比，以便这些防火墙记录 *SCTP* 信息。 • **Max Days**（最大天数）— 日志过期期限的时间长度（以天为单位，范围为 1 至 2,000）。防火墙或 Panorama 设备会自动删除超过指定期限的日志。默认情况下，未设置过期期限，这意味着日志不会过期。 防火墙或 Panorama 设备在创建日志期间会对日志进行评估，并会删除超过过期期限或配额大小的日志。 如果每周摘要日志在防火墙删除日志后达到两次之间的过期阈值，则其期限可能会在下一次删除之前超过阈值。日志配额达到最大限度时，新日志条目将开始替换最旧的日志条目。如果减小日志配额大小，则防火墙或 *Panorama* 会在您提交更改后删除最旧的日志。在 *HA* 主动/被动配置中，被动对端不会收到日志，因此不会将其删除，除非发生故障转移且变成主动对端。
	• **Core Files**（核心文件）— 如果防火墙遇到系统进程故障，它将生成一个核心文件，其中包含有关进程及其失败原因的详细信息。如果核心文件对于默认核心文件存储位置（`/var/cores`）太大，则可以启用 **`large-core`** 文件选项分配备用和更大的存储位置 (`/opt/panlogs/cores`)。Palo Alto Networks 支持工程师可以根据需要增加分配的存储空间。 要启用或禁用 **`large-core`** 文件选项，请从配置模式输入以下 CLI 命令，然后 **`commit`** 配置：

© 2019 Palo Alto Networks, Inc.

项目	说明

	`# set deviceconfig setting management large-core [yes|no]`
	
	禁用此选项后，会删除核心文件。
	
	您必须从操作模式使用 SCP 导出核心文件：
	
	`> scp export core-file large-corefile`
	
	只有 *Palo Alto Networks* 支持工程师才能解释核心文件的内容。
	
	• **Restore Defaults**（还原默认值）— 选择此选项可还原为默认值。

Session Log Storage（会话日志存储）和 **Management Log Storage**（管理日志存储）选项卡 （仅限 PA-5200 系列和 PA-7000 系列防火墙）	PA-5200 系列和 PA-7000 系列防火墙将管理日志和会话日志存储在单独的磁盘上。选择每组日志的选项卡，并按日志存储选项卡所述配置设置： • **Session Log Storage**（会话日志存储）— 选择 **Session Log Quota**（会话日志配额），并设置通信、威胁、URL 筛选、HIP 匹配、User-ID、GTP/隧道、SCTP 和身份验证日志以及扩展威胁 PCAP 的配额和过期期限。 • **Management Log Storage**（管理日志存储）— 设置系统、配置、应用统计日志、HIP 报告、数据过滤捕获、应用 PCAP 和调试过滤器 PCAP 的配额和过期期限。
Single Disk Storage（单磁盘存储）和 **Multi Disk Storage**（多磁盘存储）选项卡 （仅限 Panorama 模板）	如果使用 Panorama 模板配置日志配额和过期期限，请根据分配给模板的防火墙配置以下一个或两个选项卡中的设置： • **PA-5200** 系列和 **PA-7000** 系列防火墙 — 选择 **Multi Disk Storage**（多磁盘存储），并配置会话日志存储和管理日志存储选项卡中的设置。 *PA-5200 系列防火墙默认为 SCTP 日志存储、SCTP Summary（SCTP 摘要）、Hourly SCTP Summary（每小时 SCTP 摘要）、Daily SCTP Summary（每日 SCTP 摘要）和 Weekly SCTP Summary（每周 SCTP 摘要）分配 0# 的配额，因此您必须分配一定百分比，以便这些防火墙记录 SCTP 信息。* • 所有其他防火墙型号 — 选择 **Single Disk Storage**（单磁盘存储），并选择 **Session Log Quota**（会话日志配额），然后配置日志存储选项卡中的设置。
日志导出和报告选项卡	根据需要配置以下日志导出和报告设置： • 配置审核的版本数 — 输入在放弃最旧配置版本之前要保存的配置版本数（默认值为 100）。您可以使用这些保存的版本进行审计和比较配置中的更改。

© 2019 Palo Alto Networks, Inc.

项目	说明
	• **Number of Versions for Config Backups**（配置备份的版本数）— （仅限 Panorama）输入在放弃最旧的配置备份版本之前要保存的配置备份数（默认为 100）。 • **Max Rows in CSV Export**（CSV 导出中的最大行数）— 输入从通信日志视图 **Export to CSV**（导出到 **CSV**）后，生成的 CSV 报告中将显示的最大行数（范围为 1 至 1,048,576，默认为 65,535）。 • **Max Rows in User Activity Report**（用户活动报告中的最大行数）— 输入详细用户活动报告支持的最大行数（范围为 1 至 1,048,576，默认为 5,000）。
Log Export and Reporting（日志导出和报告）选项卡（续）	• **Average Browse Time (sec)**（平均浏览时间（秒））— 配置此变量可调整 Monitor（监控）> PDF Reports（PDF）> User Activity Report（用户活动报告）中浏览时间（以秒为单位）的计算方式（范围为 0 至 300 秒，默认为 60 秒）。 此计算将忽略类别为“Web 通告”和“内容分发网络” 的两类站点。此浏览时间计算将以 URL 过滤日志中记录的容器页面为基础。由于外部站点的许多站点加载内容都不应考虑在内，因此容器页面将用作此计算的基础。有关容器页面的更多信息，请参阅容器页面。平均浏览时间设置是管理员认为用户浏览网页所用的平均时间。平均浏览时间过后进行的任何请求将被视为新的浏览活动。计算将忽略在第一次请求时间（开始时间）与平均浏览时间之间加载的任何新网页。此行为旨在排除所需网页内加载的任何外部站点。示例：如果平均浏览时间设置为 2 分钟，那么用户打开一个网页并查看该页面 5 分钟，则此页面的浏览时间仍然为 2 分钟。由于无法确定用户查看给定页面的时间，因此系统将执行此操作。 • **Page Load Threshold (sec)**（页面加载阈值（秒））— 允许您调整在页面上加载页面元素所用的假定时间（以秒为单位，范围为 0 至 60，默认为 20）。第一次页面加载和页面加载阈值之间发生的任何请求都会被假定为页面元素。在页面加载阈值之外发生的任何请求都会被假定为用户单击页面内链接的操作。页面加载阈值还可以用在 Monitor（监控）> PDF Reports（PDF 报告）> User Activity Report（用户活动报告）的计算中。 • **Syslog HOSTNAME Format**（**Syslog** 主机名格式）— 选择是使用 syslog 消息标头中的 FQDN、主机名还是 IP 地址（IPv4 或 IPv6）。该标头标识发出消息的防火墙或 Panorama 管理服务器。 • **Report Runtime**（报告运行时）— 选择防火墙或 Panorama 设备开始生成每日计划报告当天的时间（默认为凌晨 2 点）。 • **Report Expiration Period**（报告过期期限）— 设置以天数为单位的报告过期期限（范围为 1 至 2,000）。默认情况下，未设置过期期限，这意味着报告不会过期。防火墙或 Panorama 设备将根据其系统时间，于每天的凌晨 2 点删除过期报告。
	• **Stop Traffic when LogDb full**（**LogDb** 被填满时，停止通信）（仅限防火墙，默认禁用）— 如果您希望通过防火墙的通信在日志数据库填满时停止，请选择此选项。 • **Enable Threat Vault Access**（启用威胁库访问）（默认启用）— 启用此选项可让防火墙访问威胁库，以收集有关检测到的威胁的最新信息。此信息可用于威胁日志和在 ACC 上绘制的最盛行的威胁活动。

© 2019 Palo Alto Networks, Inc.

项目	说明
	• **Enable Log on High DP Load**（启用高 **DP** 负载上的日志）（仅限防火墙，默认禁用）— 选择此选项，可指定当防火墙上的数据包处理负载达到 100% CPU 使用率时生成系统日志条目。 管理员可通过 *Enable Log on High DP Load*（启用高 *DP* 负载上的日志）调查并确定高 *CPU* 利用率的原因。 高 *CPU* 负载可能会导致操作性能降级，因为 *CPU* 没有足够的周期来处理所有数据包。系统日志将向您警告此问题（每分钟生成一个日志条目），并协助您调查可能的原因。 • **Enable High Speed Log Forwarding**（启用高速日志转发）（仅限 PA-5200 系列和 PA-7000 系列防火墙，默认禁用）— 作为最佳做法，选择此选项以高达 120,000 条日志/秒的最高速率将日志转发到 Panorama。禁用后，防火墙仅以 80,000 条日志/秒的最高速率将日志转发到 Panorama。 如果启用此选项，防火墙不会在本地存储日志或将其显示在 **Dashboard**（仪表盘）、**ACC** 或 **Monitor**（监控）选项卡中。此外，您必须配置为将日志转发到 Panorama 才能使用此选项。 • **Log Collector Status**（日志收集器状态）— 显示防火墙是否已成功建立与分布式日志收集器体系结构的连接，是否已发送日志到该体系结构。如果防火墙也配置为向日志记录服务发送日志，请验证 **Logging Service Status**（日志记录服务状态）在日志记录服务部分。
（仅限 Panorama）	• **Buffered Log Forwarding from Device**（已缓冲从设备转发的日志）（默认启用）— 允许防火墙在丢失与 Panorama 的连接时缓冲其硬盘（本地存储器）上的日志条目。与 Panorama 的连接恢复后，防火墙将日志条目转发到 Panorama；可用于缓冲的磁盘空间取决于防火墙型号的日志存储配额以及暂挂的滚动日志量。如果可用空间耗尽，最旧的条目将被删除，以便记录新事件。 启用 *Buffered Log Forwarding from Device*（已缓冲从设备转发的日志）后，若与 *Panorama* 的连接断开，则有助于防止日志丢失。 • **Get Only New Logs on Convert to Primary**（仅获取转换成主设备时的新日志）（默认禁用）— 此选项仅适用于传统模式下将日志写入网络文件系统 (NFS) 的 Panorama 虚拟设备。使用 NFS 日志记录后，只有主 Panorama 会装入到 NFS。因此，防火墙只会向主动主要 Panorama 发送日志。该选项可让您配置防火墙，从而在出现 HA 故障转移且辅助 Panorama 恢复向 NFS 记录日志时（提升为主 Panorama 后），只向 Panorama 发送新生成的日志。启用此选项通常是为了阻止防火墙在很长时间之后恢复与 Panorama 的连接时发送大量的缓冲日志。 • **Only Active Primary Logs to Local Disk**（仅由主动主设备将日志保存到本地磁盘）（默认禁用）— 此选项仅适用于传统模式下的 Panorama 虚拟设备。此选项可让您配置仅由主动 Panorama 将日志保存到本地磁盘。

© 2019 Palo Alto Networks, Inc.

项目	说明
	Pre-Defined Reports（预定义报告）（默认启用）— 应用程序、通信、威胁、URL 筛选和流控制传输协议 (SCTP) 的预定义报告可用在防火墙和 Panorama 上。在**Device**（设备）> **Setup**（设置）> **Management**（管理）> **General Settings**（常规设置）中启用 SCTP 安全后，SCTP 的预定义报告可用在防火墙和 Panorama 上。 因为每隔一小时，防火墙就会生成这些结果，因此会消耗内存资源（将结果转发给 Panorama，对其进行聚合和编译以进行查看，这也会消耗内存），为了减少内存使用，可以禁用与您无关的报告。要禁用报告，请禁用报告的此选项。 使用 **Select All**（全选）或 **Deselect All**（取消全选）选项可完全启用或禁用预定义报告的生成。 禁用报告之前，请确认组报告或 *PDF* 报告未使用该报告。如果禁用了分配到报告组的预定义报告，则整个报告组将不会有任何数据。

横幅和消息

要查看 Message of the Day（当日消息）对话框中的所有消息，请参阅当日消息。

配置 *Message of the Day*（当日消息）并单击 *OK*（确定）后，后续登录的管理员和刷新其浏览器的管理员将立即看到新的或更新的消息，而无需进行提交操作。这可让您在执行提交操作前，对即将执行提交操作的其他管理员作出警示。

每日消息 （复选框）	选择此选项可在管理员登录到 Web 界面时启用显示 Message of the Day（当日消息）对话框。
每日消息 （文本输入字段）	输入 Message of the Day（当日消息）对话框的文本（最多 3,200 个字符）。
允许不再显示	选择此选项（默认禁用）可在 Message of the Day（当日消息）对话框中包含 **Do not show again**（不再显示）选项。管理员选择此选项后，可避免在后续登录中看到同一消息。 如果您修改了 *Message of the Day*（当日消息）文本，则该消息仍将对选定了 *Do not show again*（不再显示）选项的管理员显示。因此，管理员必须重新选择此选项，以免在后续会话中再次看到修改后的消息，除非再次修改消息。
标题	输入 Message of the Day（当日消息）标头的文本（默认为 `Message of the Day`）。
背景颜色	选择 Message of the Day（当日消息）对话框的背景颜色。默认值（**None**（无））代表浅灰色背景。
图标	选择将在 Message of the Day（当日消息）对话框文本上方出现的预定义图标。

© 2019 Palo Alto Networks, Inc.

项目	说明
	• None（无）（默认） • Error（错误） • Help（帮助） • Information（信息） • Warning（警告）
标头横幅	输入标头横幅将显示的文本（最多 3,200 个字符）。
标头颜色	选择标头背景的颜色。默认值（None（无））代表透明背景。
标头文本颜色	选择标头文本的颜色。默认值（None（无））代表黑色。
标头和脚注的相同横幅	如果您想要脚注横幅与标头横幅具有相同的文本和颜色，请选中此选项（默认情况下已启用）。启用此选项后，脚注横幅的文本和颜色字段将显示为灰色。
脚注横幅	输入脚注横幅将显示的文本（最多 3,200 个字符）。
脚注颜色	选择脚注背景的颜色。默认值（None（无））代表透明背景。
脚注文本颜色	选择脚注文本的颜色。默认值（None（无））代表黑色。
最小密码复杂性	
已启用	启用本地帐户的最小密码要求。使用此功能，可以确保防火墙上的本地管理员帐户遵从已定义的一组密码要求。 还可以使用这些选项的子集创建密码配置文件，这些选项的子集将替代这些设置并可应用到特定帐户。有关更多信息，请参阅 Device（设备）> Password Profiles（密码配置文件）；有关可用于帐户的有效字符的信息，请参阅用户名和密码要求。 最大密码长度为 *31* 个字符。避免设置 *PAN-OS* 不会接受的要求。例如，不要设置包括 *10* 个大写字母、*10* 个小写字母、*10* 个数字和 *10* 个特殊字符的要求，因为此组合将超出 *31* 个字符的最大长度限制。 如果您已配置高可用性 (HA)，请在配置密码复杂性选项时始终使用主对端，并在更改后立即提交。 最小密码复杂性设置不适用于您为其指定 **Password Hash**（密码哈希）的本地数据库帐户（请参阅 Device（设备）> Local User Database（本地用户数据库）> Users（用户））。 需要使用强密码，这有助于防止暴力网络访问攻击取得成功。需要定义密码的最小长度，且每个密码应至少包括大写字母、小写字母、数值和特殊字符。此外，阻止密码中字符和用户名过多重复，设置密码重复使用的频率限制，并设置定期密码更改，以便密码不会长时间使用。所需密码越强，攻击者破解密码的

© 2019 Palo Alto Networks, Inc.

项目	说明
	难度就越大。请务必使用密码强度最佳实践确保密码的强度。
最小长度	要求最小密码长度（范围为 1 至 15 个字符）。
最小大写字母数	要求最少大写字母数（范围为 0 至 15 个字符）。
最小小写字母数	要求最少小写字母数（范围为 0 至 15 个字符）。
最小数字字母数	要求最少数字字母数（范围为 0 至 15 个数字）。
最小特殊字符数	要求最少特殊字符（非字母数字）数（范围为 0 至 15 个字符）。
阻止重复的字符	指定密码允许的连续重复字符数（范围为 2 至 15）。 如果将值设置为 2，密码可以连续两次包含同一字符，但如果连续三次或多次使用同一字符，则密码不允许。 例如，如果将值设置为 2，系统将接受密码 test11 或 11test11，但不接受 test111，因为数字 1 连续出现三次。
阻止包括用户名（反之亦然）	选择此选项可防止在密码中使用帐户用户名（或相反的名称版本）。
字符不同的新密码	管理员更改其密码时，字符必须按指定的值而有所不同。
在第一次登录时需要更改密码	选择此选项将在管理员第一次登录防火墙时提示其更改其密码。
阻止密码重用限制	要求系统根据指定计数不得重用之前的密码。例如，如果将值设置为 4，则不能重用最后 4 个密码的任意一个（范围为 0 至 50）。
阻止密码更改期限（天数）	达到指定天数（范围为 0 至 365 天）后，用户才能更改其密码。
需要密码更改期限（天数）	需要管理员定期更改其密码（以天为单位，范围为 0 至 365 天）。例如，如果将值设置为 90，则系统将每隔 90 天提示管理员更改一次密码。 您还可以设置 0 至 30 天的到期警告，并指定宽限期。
到期警告期限（天数）	如果设置了 **Required Password Change Period**（规定的密码更改期限），在规定更改日期之前不足指定的剩余天数（范围为 0 至 30 天）时，您可以使用该 **Expiration Warning Period**（到期警告期限）提示用户在每次登录时更改其密码。
发布到期后管理员登录次数（次数）	允许管理员在规定更改日期后登录指定次数（范围为 0 至 3 次）。例如，如果将此值设置为 3 且其帐户已过期，则管理员可以在其帐户被锁定之前在不更改其密码的情况下再登录 3 次。
发布到期宽限期（天数）	允许管理员在其帐户到期后在指定天数内登录（范围为 0 至 30 天）。
AutoFocus™	

© 2019 Palo Alto Networks, Inc.

项目	说明
已启用	启用防火墙连接到 AutoFocus 门户，以检索威胁情报数据并在防火墙和 AutoFocus 之间启用集成搜索。 连接到 AutoFocus 之后，防火墙会显示与通信、威胁、URL 过滤、WildFire 提交以及数据筛选日志条目相关的 AutoFocus 数据（**Monitor**（监控）> **Logs**（日志））。您可单击这些类型的日志条目中的构件（如 IP 地址或 URL），以显示其 AutoFocus 搜索结果和统计信息的摘要。之后，您可直接从防火墙打开构件的扩展 AutoFocus 搜索。 检查 *AutoFocus* 许可证在防火墙上是否处于活动状态（*Device*（设备）> *Licenses*（许可证））。如果未显示 *AutoFocus* 许可证，请使用 *License Management*（许可证管理）中的选项来激活许可证。
AutoFocus URL	输入 AutoFocus URL： `https://autofocus.paloaltonetworks.com:10443`
查询超时（秒）	设置防火墙尝试查询 AutoFocus 以获取威胁情报数据的持续时间（以秒为单位）。如果 AutoFocus 门户在指定期限结束前未作出响应，防火墙将关闭连接。

Cortex 数据湖

使用此部分配置 VM 系列和基于硬件的防火墙，以将日志转发到Cortex Data Lake。以下是配置下述选项的完整工作流程：

- 开始记录到 Cortex Data Lake（无 Panorama）
- 开始记录到 Cortex Data Lake（对于 Panorama 管理的防火墙）

日志记录服务现已更名为 *Cortex Data Lake*；但是，一些防火墙功能和按钮仍然显示“日志记录服务”名称。

启用 Cortex 数据湖	选择此选项，以使防火墙（或者，若您使用的是 Panorama，则为属于所选 **Template**（模板）的防火墙）将日志转发到 Cortex Data Lake（Cortex Data Lake 即以前的“日志记录服务”）。 配置日志转发（Objects（对象）> Log Forwarding（日志转发））后，防火墙关于将日志直接转发到 Cortex Data Lake — 即使对于 Panorama 管理的防火墙也是如此。
启用重复日志记录（仅适用于 Panorama 管理的防火墙）	**Enable Duplicate Logging**（启用重复日志记录），除了将日志发送到 Cortex Data Lake，还会继续将日志发送到 Panorama 和分布式日志收集器。 若您在评估 Cortex Data Lake，则此选项很有用 — 启用后，属于所选模板的防火墙会将日志的副本保存到 Cortex Data Lake 和 Panorama 或分布式日志收集架构中。
启用增强的应用程序日志记录	如果希望防火墙收集可提高 Palo Alto Networks 应用程序的网络可见性的数据，请选择 **Enable Enhanced Application Logging**（启用增强

© 2019 Palo Alto Networks, Inc.

项目	说明
	的应用程序日志记录）。例如，这种增加的网络可见性使 Palo Alto Networks Cortex XDR 应用程序能够更好地对正常网络活动进行分类和建立基线，以便防火墙可以检测到可能指示攻击的异常行为。 增强的应用程序日志记录功能需要日志记录服务 (Cortex Data Lake) 许可证。您无法查看这些日志，因为其仅供 Palo Alto Networks 应用程序使用。
区域	选择防火墙将向其转发日志的 Cortex 数据湖（日志记录服务）实例所在的地理区域。登录到 Cortex 中心，确认 Cortex 数据湖实例部署所在的区域（在中心内，选择顶部菜单栏上的设置齿轮图标和 **Manage Apps**（管理应用程序））。
PA-7000 系列 和 PA-5200 系列防火墙 的 Cortex 数据湖连接计数	（仅限 PA-7000 系列和 PA-5200 系列防火墙）指定从防火墙向 Cortex 数据湖发送日志的连接数（范围为 1 至 20，默认为 5）。您可以在防火墙上使用 **`request logging-service-forwarding status`** CLI 命令，以验证防火墙和 Cortex Data Lake 之间的活动连接数。
在没有 Panorama 的情况下登录 （对于不受 Panorama 管理的防火墙）	您可以启用不受 Panorama 管理的防火墙发送日志到 Cortex 数据湖。为此，需要先在 Cortex 数据湖应用程序中生成一个密钥。此密钥可使防火墙能够进行身份验证并安全地连接到 Cortex Data Lake。生成并输入密钥，然后启用防火墙以开始将日志转发到 Cortex 数据湖。
日志记录服务状态	查看与 Cortex Data Lake 的连接状态。**Show Status**（显示状态）以查看下列检查的详细信息： • **License**（许可证）— `OK` 或 `Error`，指示防火墙是否具有转发日志到 Cortex Data Lake 的有效许可证。 • **Certificate**（证书）— `OK` 或 `Error`，指示防火墙是否成功获取对 Cortex Data Lake 进行身份验证所需的证书。 • **Customer Info**（客户信息）— `OK`（确定）或 `Error`（错误），指示防火墙是否具有使用 Cortex 数据湖所需的客户识别号。若状态为 `OK`，则还可以查看客户标识号。 • **Device Connectivity**（设备连接）— 指示防火墙是否已成功连接到 Cortex Data Lake。
SSH 管理配置文件设置	
服务器配置文件	一种应用到网络上 CLI 管理连接的 SSH 会话的 SSH 服务配置文件。若要应用现有服务器配置文件，请选择配置文件，然后单击 **OK**（确定），并**Commit**（提交）您的更改。 您必须从 *CLI* 中执行 *SSH* 服务重新启动，以激活配置文件。 有关详细信息，请参阅Device（设备）> Certificate Management（证书管理）> SSH Service Profile（SSH 服务配置文件）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Operations（操作）

您可执行以下任务，以管理防火墙和 Panorama™ 的运行中配置和待选配置。如果使用 Panorama 虚拟设备，还可以使用此页面上的设置配置传统模式下 Panorama 虚拟设备的日志存储分区。

对于在待选配置中所作的更改，您必须提交更改以将其激活，此时这些更改将成为运行中配置的一部分。作为最佳做法，应定期保存待选配置。

您可使用来自 CLI 的安全复制 (SCP) 命令以将配置文件、日志、报告和其他文件导出到 *SCP* 服务器，然后将文件导入其他防火墙或 *Panorama M* 系列或虚拟设备。但是，由于日志数据库过大而无法执行导出或导入操作，以下型号不支持导出或导入整个日志数据库：*PA-7000* 系列防火墙（所有 *PAN-OS®* 版本）、运行 *Panorama 6.0* 或更新版本的 *Panorama* 虚拟设备，以及 *Panorama M* 系列设备（所有 *Panorama* 版本）。

功能	说明
配置管理	
恢复到上次保存的配置	还原待选配置的默认快照 (.snapshot.xml)（选择 Web 界面右上角的 **Config**（配置）> **Save Changes**（保存更改）后创建或替换的快照）。 （仅限 Panorama）**Select Device Groups & Templates**（选择设备组和模板）以选择要恢复的特定设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
恢复到运行配置	还原当前运行的配置。此操作将撤销自上次提交之后，每位管理员对待选配置所作的所有更改。要仅还原特定管理员所作的更改，请参阅恢复更改。 （仅限 Panorama）**Select Device Groups & Templates**（选择设备组和模板）以选择要恢复的特定设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
保存已命名的配置快照	创建不会替换默认快照 (.snapshot.xml) 的待选配置快照。输入快照的 **Name**（名称）或选择要替换的现有已命名快照。 （仅限 Panorama）**Select Device Groups & Templates**（选择设备组和模板）以选择要保存的特定设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
保存待选配置	使用当前待选配置创建或替换待选配置 (.snapshot.xml) 的默认快照。此操作等同于选择 Web 界面右上角的 **Config**（配置）> **Save Changes**（保存更改）。要仅保存特定管理员所作的更改，请参阅保存待选配置。 （仅限 Panorama）**Select Device Groups & Templates**（选择设备组和模板）以选择要保存的特定设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
加载已命名的配置快照（防火墙） 或者	使用下列选项之一替换当前待选配置： • 自定义命名的待选配置快照（而非默认快照）。 • 已导入的自定义命名的运行配置。 • 当前运行的配置。

© 2019 Palo Alto Networks, Inc.

功能	说明
加载已命名的 Panorama 配置快照	配置必须位于要加载它的防火墙或 Panorama 上。 选择配置的 **Name**（名称），然后输入 **Decryption Key**（解密密钥），该密钥是防火墙或 Panorama 的主密钥（请参阅 Device（设备）> Master Key and Diagnostics（主密钥和诊断））。对配置中的所有密码和私钥进行解密时需要使用主密钥。如果加载导入的配置，则必须输入从中导入的防火墙或 Panorama 的主密钥。在加载操作完成后，加载配置的防火墙或 Panorama 的主密钥将对密码和私钥进行重新加密。 要为配置中所有规则生成新的 UUID（例如，如果从另一个防火墙加载配置，但希望在加载此配置时保持唯一规则），超级用户必须 **Regenerate Rule UUIDs for selected named configuration**（为选中的已命名配置重新生成规则 **UUID**），以便为所有规则生成新的 UUID。 （仅限 Panorama）通过选择下列内容，指定对象、策略、设备组或模板配置从已命名配置中部分加载配置： • **Load Shared Objects**（加载共享对象）— 仅加载共享对象以及所有设备组和模板配置。 • **Load Shared Policies**（加载共享策略）— 仅加载共享策略以及所有设备组和模板配置。 • **Select Device Groups & Templates**（选择设备组和模板）— 指定待加载的设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。 • **Retain Rule UUIDs**（保留规则 **UUID**）— 将 UUID 保留在当前运行的配置。
加载配置版本（防火墙） 或者 加载 Panorama 配置版本	使用存储在防火墙或 Panorama 上的运行配置的以前版本替换当前待选配置。 选择配置的 **Name**（名称），然后输入 **Decryption Key**（解密密钥），该密钥是防火墙或 Panorama 的主密钥（请参阅 Device（设备）> Master Key and Diagnostics（主密钥和诊断））。对配置中的所有密码和私钥进行解密时需要使用主密钥。在加载操作完成后，主密钥将对密码和私钥进行重新加密。 （仅限 Panorama）通过选择下列内容，指定对象、策略、设备组或模板配置从已命名配置中部分加载配置： • **Load Shared Objects**（加载共享对象）— 仅加载共享对象以及所有设备组和模板配置。 • **Load Shared Policies**（加载共享策略）— 仅加载共享策略以及所有设备组和模板配置。 • **Select Device Groups & Templates**（选择设备组和模板）— 指定待加载的设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
导出已命名的配置快照	导出当前运行的配置、待选配置快照，或之前导入的配置（待选配置或正在运行的配置）。防火墙会将配置导出为带有指定名称的 XML 文件。您可将此快照保存在任何网络位置中。 （仅限 Panorama）**Select Device Groups & Templates**（选择设备组和模板）以选择要导出的特定设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
导出配置版本	将运行中配置的 **Version**（版本）导出为 XML 文件。

© 2019 Palo Alto Networks, Inc.

功能	说明
	（仅限 Panorama）**Select Device Groups & Templates**（选择设备组和模板）以选择要导出的特定设备组、模板或模板堆栈配置。设备组和模板管理员只能选择其分配访问域中指定的设备组、模板或模板堆栈。
导出 Panorama 及设备配置包 （仅限 Panorama）	生成和导出每个受管防火墙和运行配置备份的 Panorama 的最新版本。要实现每天创建配置包并将其导出到 SCP 或 FTP 服务器的流程自动化，请参阅 Panorama > Device Deployment（设备部署）。
导出或推送设备配置包 （仅限 Panorama）	提示您选择防火墙，并对存储在 Panorama 上的防火墙配置执行下列操作之一： • 将配置推送和提交到防火墙。该操作会清理防火墙（删除其所有本地配置），并推送存储在 Panorama 上的防火墙配置。在导入防火墙配置后，使用此选项可清理防火墙，以便可以使用 Panorama 进行管理。 • 将配置导出到防火墙，而不加载。要加载配置，必须访问防火墙 CLI 并运行配置模式命令 **load device-state**。此命令按照与推送和提交选项相同的方式清理防火墙。 这些选项仅适用于运行 *PAN-OS 6.0.4* 及更新版本的防火墙。
导出设备状态 （仅限防火墙）	将防火墙状态信息导出为状态包。除正在运行的配置之外，状态信息将包含从 Panorama 推送的设备组和模板设置。如果防火墙为 GlobalProtect™ 门户，则此状态包也会包含证书信息、此门户管理的卫星的列表，以及卫星身份验证信息。如果您更换了防火墙或门户，您可通过导入状态包来还原更换时导出的信息。 您必须手动运行防火墙状态导出，或创建调度的 *XML API* 脚本，以便将文件导出到远程服务器。因卫星证书经常改变，所以此操作应定期完成。 要从 CLI 创建防火墙状态文件，请从配置模式运行 **`save device state`** 命令。此文件将被命名为 `device_state_cfg.tgz` 并存储在 `/opt/pancfg/mgmt/device-state` 中。导出防火墙状态文件的操作命令为 **`scp export device-state`**（也可以使用 **`tftp export device-state`**）。 有关使用 XML 或 REST API 的信息，请参阅《PAN-OS 和 Panorama API 指南》。
导入已命名的配置快照	从任意网络位置导入正在运行的配置或待选配置。单击浏览并选择要导入的配置文件。
导入设备状态 （仅限防火墙）	选择 **Export device state**（导出设备状态）后，导入从防火墙导出的状态信息包。除正在运行的配置之外，状态信息将包含从 Panorama 推送的设备组和模板设置。如果防火墙为 GlobalProtect 门户，则此状态信息包也会包含证书信息、卫星列表，以及卫星身份验证信息。如果更换防火墙或门户，您可通过导入状态包来还原更换信息。
将设备配置导入 Panorama （仅限 Panorama）	将防火墙配置导入 Panorama。Panorama 自动创建模板以包含网络和设备配置。对于防火墙上的每个虚拟系统 (vsys)，Panorama 自动创建设备组以包含策略和对象配置。设备组在层次结构中将是共享位置下的一个级别，尽管您可以在完成导入后重新将其分配给不同的父设备组（请参阅 Panorama > VMware NSX）。 *Panorama* 的内容版本(如应用程序和威胁数据库）必须与从其中导入配置的防火墙的版本相同或更高。

© 2019 Palo Alto Networks, Inc.

功能	说明
	配置以下导入选项： • 设备 — 选择 Panorama 将从中导入配置的防火墙。下拉列表仅包含已连接到 Panorama 且尚未分配给任何设备组或模板的防火墙。只能选择整个防火墙，而不是单个虚拟系统。 • 模板名称 — 输入将包含导入的设备和网络设置的模板的名称。对于多虚拟系统防火墙，该字段留空。对于其他防火墙，默认值为防火墙名称。您不能使用现有模板的名称。 • **Device Group Name Prefix**（设备组名称前缀）（仅限多虚拟系统防火墙）—（可选）添加一个字符串作为每个设备组名称的前缀。 • 设备组名称 — 对于多虚拟系统防火墙，每个设备组默认都拥有一个虚拟系统名称。对于其他防火墙，默认值为防火墙名称。您可以编辑默认名称，但不能使用现有设备组的名称。 • **Import devices' shared objects into Panorama's shared context**（将设备的共享对象导入 **Panorama** 的共享上下文）（默认启用）— Panorama 将导入属于在防火墙中共享的对象，以便在 Panorama 中共享。 *Panorama* 将所有对象视为没有多个虚拟系统的防火墙上的共享对象。如果禁用此选项，*Panorama* 会将共享防火墙对象复制到设备组，而不是共享。此设置具有以下例外： • 如果共享防火墙对象具有与现有共享 Panorama 对象相同的名称和值，则导入排除该防火墙对象。 • 如果共享防火墙对象的名称或值不同于共享 Panorama 对象，则 Panorama 将防火墙对象导入每个设备组。 • 如果已导入模板的配置引用共享防火墙对象，则 Panorama 将对象导入共享，无论您是否选择此选项。 • 如果共享防火墙对象引用已导入模板的配置，则 Panorama 将对象导入设备组，无论您是否选择此选项。 • 规则导入位置 — 选择 Panorama 将导入策略是作为前导规则还是后续规则。无论您的选择怎样，Panorama 都会将默认安全规则（区域内默认和区域间默认）导入后续规则库。 如果 *Panorama* 拥有名称与所导入的防火墙规则相同的规则，*Panorama* 会同时显示两个规则。但是，规则名称必须唯一：在 *Panorama* 上执行提交前应删除其中一个规则，否则提交将失败。
设备操作	
重新启动	要重新启动防火墙或 Panorama，请单击 **Reboot Device**（重新启动设备）。防火墙或 Panorama 会将您注销、重新加载软件（PAN-OS 或 Panorama）和主动配置、关闭和记录现有会话以及创建用于显示启动关机的管理员的姓名的系统日志条目。尚未保存或提交的任何配置更改将丢失（请参阅 Device（设备）> Setup（设置）> Operations（操作））。 如果 *Web* 界面不可用，请使用以下操作 *CLI* 命令： `request restart system`

© 2019 Palo Alto Networks, Inc.

功能	说明
关机	要正常关闭防火墙或 Panorama，请单击 **Shutdown Device**（关闭设备）或 **Shutdown Panorama**（关闭 **Panorama**），然后在出现提示时单击 **Yes**（是）。未保存或提交的任何配置更改将丢失。所有管理员都将注销，并且将发生以下进程： • 所有登录会话都将注销。 • 接口将禁用。 • 所有系统进程都将停止。 • 现有会话将被关闭和记录。 • 系统会创建显示启动关闭的管理员名称的系统日志。如果无法写入此日志条目，则系统将显示警告且不会关闭。 • 磁盘驱动程序将完全卸除，防火墙或 Panorama 将关闭。 您必须拔出电源并在开启防火墙或 Panorama 前插回电源。 如果 *Web* 界面不可用，请使用 *CLI* 命令： **`request shutdown system`**
重启数据平面	要在不重新启动机器的情况下重新启动防火墙的数据功能，请单击 **Restart Dataplane**（重启数据平面）。此选项在 Panorama 或 PA-220、PA-800 系列或 VM 系列防火墙上不可用。 如果 *Web* 界面不可用，请使用 *CLI* 命令： ***`request restart dataplane`*** 在 PA-7000 系列防火墙上，每个 NPC 都拥有一个数据平面，因此您可以通过运行以下命令重新启动 NPC 以执行此操作： **`request chassis restart slot`**。
其他	
自定义徽标	单击 **Custom Logos**（自定义徽标）可自定义以下任意一项： • **Login Screen**（登录屏幕）背景图像 • **Main UI**（主 **UI**）（Web 界面）标头图像 • **PDF Report Title Page**（**PDF** 报告标题页）图像。请参阅 Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要）。 • **PDF Report Footer**（**PDF** 报告页脚）图像 上传（<image>）图像文件进行预览或删除 () 之前上传的图像。 要恢复默认徽标，请删除您的条目并 **Commit**（提交）。 对于 **Login Screen**（登录屏幕）和 **Main UI**（主 **UI**），可以显示 () 将出现的图像，如有必要，防火墙可对图像进行修剪以适应登录屏幕和主 UI。对于 PDF 报告，防火墙会自动调整图像大小以适应不裁剪的情形。在所有情况下，预览均显示建议采用的图像尺寸。 任何徽标的最大图像大小均为 128KB。支持的文件类型有 .png、.gif 和 .jpg。防火墙不支持隔行扫描或包含 Alpha 通道的图像文件，因为这些文件会干扰 PDF

© 2019 Palo Alto Networks, Inc.

功能	说明
	报告生成。您可能需要联络创建此图片的制图者删除 alpha 通道，或者确保您所使用的图形软件不会保存带有 alpha 通道功能的文件。 有关生成 PDF 报告的信息，请参阅 Monitor（监控）> PDF Reports（PDF 报告）> Manage PDF Summary（管理 PDF 摘要）。
SNMP 设置	启用 SNMP 监控。
存储分区设置（仅限 Panorama）	传统模式下 Panorama 虚拟设备的日志存储分区。

启用 SNMP 监控

- Device（设备）> Setup（设置）> Operations（操作）

简单网络管理协议 (SNMP) 是用于监视网络设备的一个标准协议。选择 **Operations**（操作）可配置防火墙使用 SNMP 管理器支持的 SNMP 版本（SNMPv2c 或 SNMPv3）。了解必须加载到 SNMP 管理器以便解释从防火墙收集的统计信息的 MIB 列表，请参阅支持的 MIB。要对服务器配置文件（该文件用于支持防火墙与网络上的 SNMP 陷阱目标进行通信）进行配置，请参阅 Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱）。SNMP MIB 可定义防火墙生成的所有 SNMP 陷阱。SNMP 陷阱可以识别带有唯一对象标识 (OID) 的事件，且各个字段将定义为变量绑定 (varbind) 列表。单击 **SNMP Setup**（**SNMP** 设置），并指定以下设置以允许从 SNMP 管理器发送 SNMP GET 请求：

字段	说明
物理位置	指定防火墙的物理位置。如果生成日志和陷阱，该信息可使您识别（在 SNMP 管理器）生成此通知的防火墙。
联系人	输入负责维护防火墙的人员的姓名或电子邮件地址。此设置在标准系统信息 MIB 中已提供。
使用特定陷阱定义	默认选中此选项，这意味着防火墙将根据事件类型使用每个 SNMP 陷阱的唯一 OID。如果取消选中此选项，则每个陷阱都将拥有相同的 OID。
版本	选择 SNMP 版本：**V2c**（默认）或 **V3**。您的选择可控制对话框显示的其余字段。
对于 **SNMP V2c**	
Snmp 社区字符串	输入团体字符串，不但可用于识别 SNMP 管理器和监控设备的 SNMP 团体，并且还可用作密码在团体成员交换 SNMP 获取（统计信息请求）和陷阱消息时对其彼此进行身份验证。字符串最多可以包含 127 个字符，接受所有字符且区分大小写。 请不要使用默认团体字符串 *public*。由于 *SNMP* 消息包含明文团体字符串，因此在定义团体成员（管理员访问权限）时需要考虑网络的安全要求。
对于 **SNMP V3**	
名称/视图	您可以将一个或一组视图分配给 SNMP 管理器的用户，以控制用户可以从防火墙获取的 MIB 对象（统计信息）。每个视图是一个配对的 OID 和位掩码：OID 指定

© 2019 Palo Alto Networks, Inc.

字段	说明
	MIB，掩码（十六进制格式）指定可以在 MIB 内部（包括匹配）或外部（排除匹配）访问的对象。 例如，如果 **OID** 为 1.3.6.1，将匹配 **Option**（选项）设置为 **include**（包括）且 **Mask**（掩码）为 0xf0，则用户请求的对象必须拥有与 1.3.6.1 的前四个节点 (f = 1111) 匹配的 OID。对象不需要匹配其余节点。在本例中，1.3.6.1.2 与掩码相匹配，而 1.4.6.1.2 则不匹配。 对于每组视图，单击 **Add**（添加），输入组的 **Name**（名称），然后配置 **Add**（添加）到组的每个视图的下列设置： • **View**（视图）— 指定视图的名称。此名称最多可以包含 31 个字符，包括字母数字、句点、下划线或连线。 • **OID** — 指定 MIB 的 OID。 • **Option**（选项）— 选择应用到 MIB 的匹配逻辑。 • **Mask**（掩码）— 指定掩码（十六进制格式）。 要访问所有管理信息，使用顶层 *OID 1.3.6.1*，将 *Mask*（掩码）设置为 *0xf0* 并将匹配 *Option*（选项）设置为 *include*（包括）。
用户	当防火墙转发陷阱和 SNMP 管理器获取防火墙统计信息时，SNMP 用户帐户可提供身份验证、隐私和访问控制。对于每位用户，单击 **Add**（添加）并配置以下设置： • **Users**（用户）— 指定用户名以标识 SNMP 用户帐户。在防火墙上配置的用户名必须与在 SNMP 管理器上配置的用户名相匹配。用户名最多可以包含 31 个字符。 • **View**（视图）— 将一组视图分配给用户。 • **Auth Password**（身份验证密码）— 指定用户的身份验证密码。在转发陷阱并对统计信息请求做出响应时，防火墙将使用密码对 SNMP 管理器进行身份验证。防火墙将使用安全哈希算法 (SHA-1 160) 对密码进行加密。密码长度必须为 8-256 个字符，且允许使用所有字符。 • **Priv Password**（私人密码）— 指定用户的私人密码。防火墙将使用密码和高级加密标准 (AES-128) 对 SNMP 陷阱进行加密，并对统计信息请求做出响应。密码长度必须为 8-256 个字符，且允许使用所有字符。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> HSM

选择 **Device**（设备）> **Setup**（设置）> **HSM** 可配置硬件安全模块 (HSM)、执行操作并查看 HSM 状态。

您在查找什么内容？	请参阅：
硬件安全模块 (HSM) 的用途是什么以及在哪里可以找到详细的配置步骤？	安全密钥与硬件安全模块
配置：	硬件安全模块提供商设置
	HSM 身份验证
执行硬件安全操作	硬件安全操作
如何查看 HSM 状态？	硬件安全模块提供商配置和状态
	硬件安全模块状态

硬件安全模块提供商设置

如需在防火墙上配置硬件安全模块 (HSM)，请编辑 Hardware Security Module Provider（硬件安全模块供应商）设置：

硬件安全模块提供商设置	说明
已配置供应商	选择 HSM 供应商： • **None**（无）（默认）— 防火墙未连接到任何 HSM。 • **SafeNet Network HSM** • **nCipher nShield Connect** *HSM* 服务器版本必须与防火墙上的 HSM 客户端版本 兼容。
模块名称	添加 HSM 的模块名称。该名称可以是任意 ASCII 字符串，长度最多 31 个字符。如果要配置独立或高可用性 SafeNet HSM 配置，最多添加 16 个模块名称。
服务器地址	为要配置的任何 HSM 模块指定 IPv4 地址。
高可用性 （仅限 SafeNet Network）	（可选）如果要配置高可用性配置中的 SafeNet HSM 模块，请选择此选项。必须配置各个 HSM 模块的模块名称和服务器地址。
自动恢复重试 （仅限 SafeNet Network）	指定故障转移到 HSM HA 配置中另一个 HSM 之前，防火墙尝试恢复与 HSM 连接的次数（范围为 0-500，默认为 0）。

© 2019 Palo Alto Networks, Inc.

硬件安全模块提供商设置	说明
高可用性组名 （仅限 SafeNet Network）	指定要用于 HSM HA 组的组名。该名称供防护墙内部使用。该名称可以是任意 ASCII 字符串，长度最多 31 个字符。
删除文件系统地址 （仅限 nCipher nShield Connect）	配置 nShield Connect HSM 配置中所用的远程文件系统的 IPv4 地址。

HSM 身份验证

选择 **Setup Hardware Security Module**（设置硬件安全模块），并配置以下设置以向防火墙验证 HSM。

HSM 移动身份验证	
服务器名称	从下拉列表中选择 HSM 服务器名称，然后选择是否使用自动或手动生成证书进行身份验证，并建立信任。 • **Automatic**（自动） • **Manual**（手动） 如果选择**Manual**（手动），您需要导入并安装 HSM 服务器手动生成证书。导出 HSM 客户端证书，将其安装在 HSM 服务器上。
管理员密码	输入 HSM 的管理员密码以向防火墙验证 HSM。

硬件安全操作

要对硬件安全模块 (HSM) 或连接到 HSM 的防火墙执行操作，请选择 **Device**（设备）> **Setup**（设置）> **HSM** 并选择下列硬件安全操作中的一项：

硬件安全操作	
设置硬件安全模块	配置防火墙以对 HSM 进行身份验证。
显示详细信息	显示有关 HSM 服务器、HSM 高可用性状态和 HSM 硬件的信息。
与远程文件系统同步（仅限 nCipher nShield Connect）	将 nShield Connect 远程文件系统的密钥数据与防火墙进行同步。
重置配置	删除与防火墙的所有 HSM 连接。重置 HSM 配置后，必须重复所有身份验证步骤。
选择 HSM 客户端版本（仅限 SafeNet Network）	允许您选择在 HSM 客户端（防火墙）上运行的软件版本。HSM 客户端版本必须与 HSM 服务器版本兼容。有关客户端-服务器版本兼容性的矩阵，请参阅 HSM 供应商文档。

© 2019 Palo Alto Networks, Inc.

硬件安全模块提供商配置和状态

Hardware Security Module Provider（硬件安全模块提供商）部分显示 HSM 的 HSM 配置设置和连接状态。

硬件安全模块提供商状态	
已配置供应商	选择在防火墙上配置的 HSM 供应商： • **None** • **SafeNet Network HSM** • **nCipher nShield Connect**
高可用性	（仅限 SafeNet Network）如果选择 HSM 高可用性，将予以配置。
高可用性组名	（仅限 SafeNet Network）防火墙上为 HSM 高可用性配置的组名。
删除文件系统地址	（仅限 nShield Connect）远程文件系统地址。
防火墙源地址	用于 HSM 服务的端口地址。默认为管理端口地址。通过使用 **Device**（设备）> **Setup**（设置）> **Services**（服务）中的服务路由配置，也可以指定为其他端口。
防火墙上的 HSM 客户端版本	显示已安装的 HSM 客户端版本。
HSM 加密的主密钥	如果选中此复选框，主密钥将在 HSM 上加密。
状态	如果已连接防火墙并对 HSM 进行身份验证，则显示为绿色；如果未对防火墙进行身份验证或网络与 HSM 的连接断开，则显示为红色。 有关 HSM 连接的更多详细信息，请参阅硬件安全模块状态。

硬件安全模块状态

硬件安全模块状态包括有关已成功进行身份验证的 HSM 的以下信息。显示内容因所配置的 HSM 提供商而异（SafeNet 或 nCipher）。

硬件安全模块状态	
SafeNet Network HSM	• **Serial Number**（序列号）— 如果 HSM 分区验证成功，会显示此 HSM 分区的序列号。 • **Partition**（分区）— 分配到防火墙的 HSM 上的分区名称。 • **Module State**（模块状态）— HSM 连接的当前操作状态。如果 HSM 显示在此表中，则此字段显示 **Authenticated**（已验证）。
nCipher nShield Connect HSM	• **Name**（名称）— HSM 的服务器名称。 • **IP address**（IP 地址）— 分配到此防火墙的 HSM 的 IP 地址。 • **Module State**（模块状态）— HSM 连接的当前操作状态。如果防火墙对 HSM 进行身份验证成功，则此设置显示 **Authenticated**（已验证）；如果防火墙对 HSM 进行身份验证失败，则此设置显示 **Not Authenticated**（未验证）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Services（服务）

以下主题介绍防火墙的全局和虚拟系统服务设置：

- 配置全局和虚拟系统服务
- 全局服务设置
- 服务路由配置的 IPv4 和 IPv6 支持
- 目标服务路由

配置全局和虚拟系统服务

在启用多个虚拟系统的防火墙上，选择 **Services**（服务）选项卡以显示 **Global**（全局）和 **Virtual Systems**（虚拟系统）选项卡，您可以在其中分别设置防火墙或其虚拟系统用于提高操作效率的服务。（如果防火墙是单个虚拟系统或如果已禁用多个虚拟系统，则 **Virtual Systems**（虚拟系统）选项卡不会显示。）

选择 **Global**（全局）可设置整个防火墙的服务。此外，还可以将这些设置用作没有自定义服务设置的虚拟系统的默认值。

- 编辑 **Services**（服务）可定义 DNS 服务器、更新服务器和代理服务器的目标 IP 地址。使用专用 **NTP** 选项卡可配置网络时间协议设置。请参阅表 12，以获取可用 Services（服务）选项的字段描述。
- 在 **Service Features**（服务功能）中，单击 **Service Route Configuration**（服务路由配置）可指定防火墙与提供服务的其他服务器/设备（如 DNS、电子邮件、LDAP、RADIUS 和系统日志等）进行通信的方式。可以通过两种方式配置全局服务路由：
  - **Use Management Interface for all**（对所有项使用管理接口）选项将通过管理接口 (MGT) 强制执行与外部服务器的所有防火墙服务通信。如果选择此选项，则必须配置 MGT 接口以允许防火墙与提供服务的服务器/设备进行通信。要配置 MGT 接口，请选择 Device（设备）> Setup（设置）> Management（管理），并编辑设置。
  - 自定义选项可让您通过配置服务在其响应中用作目标接口和目标 IP 地址的特定源接口和 IP 地址粒度控制服务通信。（例如，您可以对防火墙与电子邮件服务器之间的所有电子邮件通信配置接口的特定源 Ip/接口，并为 Palo Alto Networks 服务使用不同的源IP/接口。）选择您要自定义以拥有相同设置的一个或多个服务，然后单击设置所选服务路由。服务将在表 13 中列出，其中将指明是否可为 **Global**（全局）防火墙或 **Virtual Systems**（虚拟系统）配置某项服务，以及该服务是否支持 IPv4 和/或 IPv6 源地址。

目标选项卡是可以自定义的另一个全局服务路由功能。此选项卡将显示在 Service Route Configuration（服务路由配置）窗口中，如目标服务路由中所述。

使用虚拟系统选项卡可指定单个虚拟系统的服务路由。选择一个位置（虚拟系统），并单击服务路由配置。选择虚拟系统的 **Inherit Global Service Route Configuration**（继承全局服务路由配置）或 **Customize**（自定义）服务路由。如果选择自定义设置，可以选择 **IPv4** 或 **IPv6**。选择您要自定义以拥有相同设置的一个或多个服务，然后单击设置所选服务路由。请参阅表 13，了解可以自定义的服务。

要控制和重定向共享和特定虚拟系统之间的 DNS 查询，可以使用 DNS 代理和 DNS 服务器配置文件。

全局服务设置

- Device（设备）> Setup（设置）> Services（服务）

要控制和重定向共享和特定虚拟系统之间的 DNS 查询，可以使用 DNS 代理和 DNS 服务器配置文件。

© 2019 Palo Alto Networks, Inc.

全局服务设置	说明
服务	
更新服务器	表示用于从 Palo Alto Networks 下载更新的服务器的 IP 地址或主机名。当前值为 **updates.paloaltonetworks.com**。除非技术支持人员要求，否则请勿更改此设置。
验证更新服务器的身份	如果启用该选项，防火墙或 Panorama 将验证从其中下载软件或内容数据包的服务器是否拥有由可信认证机构签署的 SSL 证书。该选项可为防火墙或 Panorama 服务器和更新服务器之间的通信添加额外的安全级别。 验证更新服务器标识，以验证服务器是否具有可信认证机构签署的 *SSL* 证书。
DNS 设置	选择防火墙为支持 FQDN 地址对象、日志记录和防火墙管理而启动的所有 DNS 查询的 DNS 服务类型（**Servers**（服务器）或 **DNS Proxy Object**（**DNS** 代理对象））。这些选项包括： • 提供域名解析的主 DNS 服务器和辅助 DNS 服务器。 • 可以选择在防火墙上配置的 DNS 代理配置 DNS 服务器。若要启用 DNS 代理，则必须启用 **Cache**（缓存）和 **EDNS Cache Responses**（**EDNS** 缓存响应）（**Network**（网络）> **DNS Proxy**（**DNS** 代理）> **Advanced**（高级））。
主 DNS 服务器	为防火墙的 DNS 查询输入主 DNS 服务器的 IP 地址。例如，查找更新服务器、解析日志中的 DNS条目或解析基于 FDQN 的地址对象。
辅助 DNS 服务器	（可选）输入在主服务器不可用时要使用的辅助 DNS 服务器的 IP 地址。
最短 FQDN 刷新时间（秒）	设置防火墙刷新其从 DNS 接收的 FQDN 的速度限制。只要 TTL 大于等于该 **Minimum FQDN Refresh Time**（最短 **FQDN** 刷新时间）（秒），防火墙就会根据 FQDN 的 TTL 刷新 FQDN。如果 TTL 小于该最短 FQDN 刷新时间，则防火墙会根据此最短 FQDN 刷新时间刷新 FQDN（即，防火墙使用的 TTL 不会大于该设置）。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（范围为 0 到 14400，默认为 30）。设置为 0 表示防火墙将根据 DNS 中的 TTL 值刷新 FQDN，不会强制执行最短 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。
FQDN 失效条目超时（分钟）	指定防火墙在出现网络故障或无法访问 DNS 服务器时（当 FQDN 未刷新时）继续使用失效 FQDN 解析的时间长度（分钟）（范围为 0 到 10,080，默认为 1,440）。值为 0 意味着防火墙不会继续使用失效条目。如果在状态超时时仍无法访问 DNS 服务器，则 FQDN 条目将变得无法解析（失效解析已被删除）。 确保 *FQDN Stale Entry Timeout*（*FQDN* 失效条目超时）值足够短，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。
“代理服务器”部分	

© 2019 Palo Alto Networks, Inc.

全局服务设置	说明
服务器	如果防火墙需要使用代理服务器才能访问 Palo Alto Networks 更新服务，则请输入代理服务器的 IP 地址或主机名。
端口	输入代理服务器的端口。
用户	输入管理员在访问代理服务器时要输入的用户名。
密码/确认密码	输入并确认管理员在访问代理服务器时要输入的密码。
通过代理，将日志发送到 Cortex 数据湖	启用防火墙以通过代理服务器发送日志到 Cortex 数据湖。
Ntp	
NTP 服务器地址	输入将用于同步防火墙时钟的 NTP 服务器的 IP 地址或主机名。或者，可以输入在主服务器不可用时用于同步防火墙时钟的辅助 NTP 服务器的 IP 地址或主机名。 当 *NTP* 服务器保持所有网络防火墙时钟同步时，计划作业按预期运行，且时间戳可帮助标识涉及多个设备的问题的根本原因。如果主 *NTP* 服务器无法访问，则配置主和辅助 *NTP* 服务器。

身份验证类型	您可以启用防火墙，以对来自 NTP 服务器的时间更新进行身份验证。请针对各个 NTP 服务器为防火墙选择身份验证类型，以便使用：
	• **None**（无）（默认值）— 选择此选项可禁用 NTP 身份验证。
	• **Symmetric Key**（对称式密钥）— 为要使用对称式密钥交换（共享机密）对 NTP 服务器的时间更新进行身份验证的防火墙选择该选项。如果选择了对称式密钥，请继续指定以下值：
	  • **Key ID**（密钥 **ID**）— 输入密钥 ID (1-65534)。
	  • **Algorithm**（算法）— 选择用于 NTP 身份验证的 MD5 或 SHA1 算法。
	  • **Authentication Key/Confirm Authentication Key**（身份验证密钥/确认身份验证密钥）— 输入并确认身份验证算法的身份验证密钥。
	• **Autokey**（自动密钥）— 为要使用自动密钥（公钥加密）对 NTP 服务器的时间更新进行身份验证的防火墙选择该选项。
	
	启用 *NTP* 服务器身份验证，这样，*NTP* 服务器可批准客户端，并提供同步更新。

服务路由配置的 IPv4 和 IPv6 支持

下表显示针对全局和虚拟系统的服务路由配置的 IPv4 和 IPv6 支持。

© 2019 Palo Alto Networks, Inc.

服务路由配置设置	全局		虚拟系统	
	IPv4	IPv6	IPv4	IPv6
AutoFocus — AutoFocus™ 服务器。	✓	—	—	—
CRL 状态 — 证书吊销列表 (CRL) 服务器。	✓	✓	—	—
DDNS — 动态 DNS 服务。	✓	✓	✓	✓
Panorama 推送更新 — 从 Panorama™ 部署的内容和软件更新。	✓	✓	—	—
DNS — 域名系统服务器。 * 对于虚拟系统，DNS 在 DNS 服务器配置文件中完成。	✓	✓	✓ *	✓ *
外部动态列表 — 外部动态列表的更新。	✓	✓	—	—
电子邮件 — 电子邮件服务器。	✓	✓	✓	✓
HSM — 硬件安全模块服务器。	✓	—	—	✓
HTTP — HTTP 转发。	✓	✓	✓	✓
Kerberos — Kerberos 身份验证服务器。	✓	—	✓	✓
LDAP — 轻型目录访问协议服务器。	✓	✓	✓	✓
MDM — 移动设备管理服务器。	✓	✓	—	—
多因素身份验证 — 多因素身份验证 (MFA) 服务器。	✓	✓	✓	✓
NetFlow — 收集网络通信统计信息的 NetFlow 收集器。	✓	✓	✓	✓
NTP — 网络时间协议服务器。	✓	✓	—	—
Palo Alto Networks 服务 — Palo Alto Networks® 和 WildFire® 公共服务器更新。同时，这也是将 10.0 版本以前的遥测数据转发到 Palo Alto Networks 的服务路由。（当前遥测支持将其数据转发到 Cortex 数据湖。在这种情况下，不会使用该服务路由。）	✓	—	—	—
Panorama — Panorama 管理服务器。	✓	✓	—	—
Panorama 日志转发（仅限 PA-5200 系列防火墙）— 从防火墙将日志转发到日志收集器。	✓	✓	—	—

© 2019 Palo Alto Networks, Inc.

服务路由配置设置	全局		虚拟系统	
	IPv4	IPv6	IPv4	IPv6
代理 — 用作防火墙代理的服务器。	✓	✓	—	—
RADIUS — 远程身份验证拨入用户服务服务器。	✓	✓	✓	✓
SCEP — 用于请求并分发客户端证书的简单证书注册协议。	✓	✓	✓	—
SNMP 陷阱 — 简单网络管理协议陷阱服务器。	✓	—	✓	—
Syslog — 系统消息日志记录服务器。	✓	✓	✓	✓
TACACS+ — 提供身份验证、授权和计费 (AAA) 服务的增强的终端访问控制器访问控制系统 (TACACS+) 服务器。	✓	✓	✓	✓
UID 代理 — User-ID 代理服务器。	✓	✓	—	✓
URL 更新 — 统一资源定位符 (URL) 更新服务器。	✓	✓	—	—
VM Monitor（**VM** 监控）— 在启用 Device（设备）> VM Information Sources（VM 信息来源）后监控虚拟机信息。 将监控虚拟机的公共云部署中的 *VM* 系列防火墙必须使用 *MGT* 接口。不得将数据面板接口用作服务路由。	✓	✓	✓	✓
WildFire 私有 — Palo Alto Networks WildFire 私有服务器。	✓	—	—	—

如果要自定义 **Global**（全局）服务路由，请选择 **Service Route Configuration**（服务路由配置），然后在 **IPv4** 或 **IPv6** 选项卡上从可用服务列表中选择一项服务；您也可以选择多项服务和 **Set Selected Service Routes**（设置所选服务路由）以一次性配置多个服务路由。要限定 **Source Address**（源地址）下拉列表中的选项，请依次选择 **Source Interface**（源接口）和 **Source Address**（源地址）（源接口的源地址）。将 Source Interface（源接口）设置为 **Any**（任何）可让您选择任何可用接口的 Source Address（源地址）。"源地址"中将显示分配给所选接口的 IPv4 或 IPv6 地址；所选 IP 地址将成为服务通信的源地址。如果希望防火墙使用服务路由的管理接口，您可以选择 **Use default**（使用默认）；但是，如果数据包目标 IP 地址与配置的目标 IP 地址匹配，则将源 IP 地址设置为配置用于 Destination（目标）的 Source Address（源地址）。由于在配置各项服务时已配置目标，因此无需定义目标地址。例如，定义 DNS 服务器（**Device**（设备）> **Setup**（设置）> **Services**（服务））后，您将设置 DNS 查询的目标。您可以为服务同时指定 IPv4 和 IPv6 地址。

自定义 **Global**（全局）服务路由的另一种方法是选择 **Service Route Configuration**（服务路由配置）并选择 **Destination**（目标）。指定与传入数据包进行比较的 **Destination**（目标）IP 地址。如果数据包目标地址与配置的目标 IP 地址匹配，则将源 IP 地址设置为配置用于 Destination（目标）的 Source Address（源地址）。要限定 **Source Address**（源地址）下拉列表中的选项，请依次选择 **Source Interface**（源接口）和 **Source Address**（源地址）（源接口的源地址）。将 Source Interface（源接口）设置为 **Any**（任何）可让您选择任何可用接口的 Source Address（源地址）。**MGT** 源接口可使防火墙使用服务路由的管理接口。

© 2019 Palo Alto Networks, Inc.

配置 **Virtual System**（虚拟系统）的服务路由时，选择 **Inherit Global Service Route Configuration**（继承全局服务路由配置）意味着虚拟系统的所有服务都将会继承全局服务路由设置。或者，您可以选择 **Customize**（自定义），选择 **IPv4** 或 **IPv6**，然后选择一项服务；您也可以选择多项服务和 **Set Selected Service Routes**（设置所选服务路由）。源接口包含下列三个选择：

- **Inherit Global Setting**（继承全局设置）— 所选服务继承这些服务的全局设置。
- 任何 — 可让您选择任何可用接口（特定虚拟系统的接口）的源地址。
- **An interface from the drop-down**（下拉列表中的接口）— 将 **Source Address**（源地址）的下拉列表限定为此接口的 IP 地址。

对于源地址，从下拉列表中选择地址。对于所选服务，将服务器的响应发送到此源地址。

目标服务路由

- 设备 > 设置 > 服务 > 全局

在 **Global**（全局）选项卡中，依次单击 **Service Route Configuration**（服务路由配置）和 **Customize**（自定义）后，随即将显示 **Destination**（目标）选项卡。只有全局选项卡（非虚拟系统选项卡）下的目标服务路由才可用，因此单个虚拟系统的服务路由无法替代不与该虚拟系统相关联的路由表条目。

您可以使用目标服务路由添加 **Customize**（自定义）服务列表不支持的自定义服务重定向。目标服务路由是一种设置路由以替代转发信息库 (FIB) 路由表的方法。目标服务路由中的任何设置均会替代路由表条目。可以将它们与任何服务进行关联或取消关联。

目标选项卡适用于下列用案：

- 当服务没有应用程序服务路由时。
- 在单个虚拟系统内，当您要使用多个虚拟系统或者虚拟路由器和管理端口的组合时。

目标服务路由设置	说明
目标	输入目标 IP 地址。具有与此地址相匹配的目标地址的传入数据包将作为您为此服务路由指定的源地址的地址来源。
源接口	要限制源地址的下拉列表，请选择 **Source Interface**（源接口）。选择 **Any**（任何）可使源地址下拉列表中显示所有接口上的所有 IP 地址。选择 **MGT**可使防火墙使用 MGT 接口作为服务路由。
Source Address（源地址）	选择服务路由的 **Source Address**（源地址）；该地址将用于从目标地址返回的数据包。您无需输入目标地址的子网。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Interfaces（接口）

使用此页面为所有防火墙型号和 PA-5200 系列防火墙的辅助接口（AUX-1 和 AUX-2）配置管理 (MGT) 接口的连接设置、允许服务和管理访问权限。

Palo Alto Networks 建议您始终为每个接口指定 IP 地址和网络掩码（对于 IPv4）或前缀长度（对于 IPv6）和默认网关。如果省略 MGT 接口的任何设置（如默认网关），则只能通过控制台端口访问防火墙以便将来更改配置。

要在 *M-500* 设备或 *Panorama* 虚拟设备上配置 *MGT* 接口，请参阅 Panorama > Setup（设置）> Interfaces（接口）。

您可以将回环接口用作防火墙管理的 *MGT* 接口的备选（请参阅 Network（网络）> Interfaces（接口）> Loopback（回环））。

项目	说明

类型
（仅限 MGT 接口）
	选择一个：
	• **Static**（静态）— 要求手动输入 **IP Address**（**IP** 地址）(IPv4)、**Netmask**（网络掩码）(IPv4) 和 **Default Gateway**（默认网关）。
	• **DHCP Client**（**DHCP** 客户端）— 将管理接口配置为 DHCP 客户端，使防火墙能发送 DHCP Discover（DHCP 发现）或 Request（请求）消息，以找到 DHCP 服务器。服务器作出响应，即提供 IP 地址 (IPv4)，网络掩码 (IPv4) 和管理接口的默认网关。默认情况下，管理接口上的 DHCP 将因 VM 系列防火墙（AWS 和 Azure 中的 VM 系列防火墙除外）而关闭。如果您选择 **DHCP Client**（**DHCP** 客户端），则可以同时选择以下两个客户端选项或者任选一项：
	  • **Send Hostname**（发送主机名）— 使 MGT 接口将其主机名发送到 DHCP 服务器，以作为 DHCP Option 12 的一部分。
	  • **Send Client ID**（发送客户端 **ID**）— 使 MGT 接口发送其客户端标识符，以作为 DHCP Option 61 的一部分。
	如果您选择 **DHCP Client**（**DHCP** 客户端），则可选择单击 **Show DHCP Client Runtime Info**（显示 **DHCP** 客户端运行时信息）以查看动态 IP 接口状态：
	• 接口 — 表示 MGT 接口。
	• IP 地址 — 管理接口的 IP 地址。
	• 网络掩码 — IP 地址的子网掩码，表示属于网络或子网地址的位，属于主机地址的位。
	• 网关 — 管理接口流出流量的默认网关。
	• 主/辅助 NTP — 管理接口所用 NTP 服务器（最多两个）的 IP 地址。如果 DHCP 服务器返回 NTP 服务器地址，防火墙将仅在您未手动配置 NTP 服务器地址的情况下，处理这些地址。如果您手动配置了 NTP 服务器地址，则防火墙不会用 DHCP 服务器提供的地址来替换这些地址。
	• 租借时间 — 分配 DHCP IP 地址的天数、小时数、分钟数和秒数。
	• 到期时间 — 年/月/日、时/分/秒和时区，表示 DHCP 租借将到期的时间。
	• DHCP 服务器 — 响应 MGT 接口 DHCP 客户端的 DHCP 服务器的 IP 地址。
	• 域 — 管理接口所属域的名称。
	• DNS 服务器 — 管理接口所用 DNS 服务器（最多两个）的 IP 地址。如果 DHCP 服务器返回 DNS 服务器地址，防火墙将仅在您未手动配置 DNS 服务器

© 2019 Palo Alto Networks, Inc.

项目	说明
	地址的情况下，处理这些地址。如果您手动配置了 DNS 服务器地址，则防火墙不会用 DHCP 服务器提供的地址来替换这些地址。 或者，您也可以为分配到 MGT 接口的 IP 地址 **Renew**（续订）DHCP 租赁。否则，请**Close**（关闭）此窗口。
Aux 1/Aux 2 （仅限 PA-5200 系列防火墙）	选择以下任一选项以启用辅助接口。这些接口可以为下列功能提供 10Gbps (SFP+) 吞吐量： • 防火墙管理流量 — 必须启用访问 Web 界面和 CLI 以管理防火墙时管理员使用的网络服务（协议）。 为 *Web* 界面启用 *HTTPS*（而非 *HTTP*），并为 *CLI* 启用 *SSH*（而非 *Telnet*）。 • 防火墙对等之间的高可用性 (HA) 同步 — 配置接口后，必须选择它作为 HA 控制链路（**Device**（设备）> **High Availability**（高可用性）> **General**（常规））。 • 将日志转发到 Panorama — 必须配置启用了 **Panorama Log Forwarding**（**Panorama** 日志转发）服务的服务路由（请参阅 Device（设备）> Setup（设置）> Services（服务））。
IP 地址 (IPv4)	如果网络使用 IPv4，请为接口分配 IPv4 地址。此外，您还可以分配防火墙管理回环接口的 IP 地址（请参阅 Network（网络）> Interfaces（接口）> Loopback（回环））。默认情况下，输入的 IP 地址是用于转发日志的源地址。
网络掩码 (IPv4)	如果已为接口分配 IPv4 地址，还必须输入网络掩码（例如，255.255.255.0）。
默认网关	如果已为接口分配 IPv4 地址，还必须为默认网关分配 IPv4 地址（网关与接口必须在同一子网中）。
IPv6 地址/前缀长度	如果网络使用 IPv6，请为接口分配 IPv6 地址。为了指明网络掩码，请输入 IPv6 前缀长度（例如，2001:400:f00::1/64）。
默认 IPv6 网关	如果已为接口分配 IPv6 地址，还必须为默认网关分配 IPv6 地址（网关与接口必须在同一子网中）。
速度	配置接口的数据速率和双工选项。选项包括 10Mbps、100Mbps 和 1Gbps（全双工或半双工）。使用默认自动协商设置可使防火墙确定接口速度。 此设置必须与邻近网络设备上的端口设置匹配。要确保设置匹配，请在相邻设备支持自动协商选项的情况下选择此选项。
MTU	输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 1,500，默认为 1,500）。
管理管理服务	• **HTTP** — 使用此服务访问防火墙 Web 界面。 *HTTP* 使用初始明文，但其安全性不及 *HTTPS*。因此，*Palo Alto Networks* 建议您为接口上的管理流量启用 *HTTPS* 而非 *HTTP*。 • **Telnet** — 使用此服务访问防火墙 CLI。

© 2019 Palo Alto Networks, Inc.

项目	说明
	Telnet 使用初始明文，但其安全性不及 *SSH*。因此，*Palo Alto Networks* 建议您为接口上的管理流量启用 *SSH* 而非 *Telnet* 。 • **HTTPS** — 使用此服务对防火墙 Web 界面进行安全访问。 • **SSH** — 使用此服务对防火墙 CLI 进行安全访问。
网络服务	选择要在接口上启用的服务： • **HTTP OCSP** — 使用此服务将防火墙配置为联机证书状态协议 (OCSP) 响应者。有关详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者）。 • **Ping** — 使用此服务测试与外部服务的连接性。例如，您可对管理接口执行 Ping 命令，以验证其是否能从 Palo Alto Networks 更新服务器接收 PAN-OS 软件和内容更新。在高可用性 (HA) 部署中，HA 对将使用 Ping 命令来交换检测信号备份信息。 • **SNMP** — 使用此服务处理来自 SNMP 管理器的防火墙统计信息查询。有关详细信息，请参阅启用 SNMP 监控。 • **User-ID** — 使用此服务启用防火墙中用户映射的重新分发。 • **User-ID Syslog Listener-SSL**（**User-ID Syslog** 侦听器 **SSL**）— 使用此服务启用 PAN-OS 集成的 User-ID™ 代理通过 SSL 收集 syslog 管理。有关详细信息，请参阅配置对受监控服务器的访问权限。 • **User-ID Syslog Listener-UDP**（**User-ID Syslog** 侦听器 **UDP**）— 使用此服务启用 PAN-OS 集成的 User-ID 代理通过 SSL 收集 syslog 管理。有关详细信息，请参阅配置对受监控服务器的访问权限。
允许的 IP 地址	输入管理可以通过接口从中访问防火墙的 IP 防火墙的 IP 地址。空列表（默认）指定可从任何 IP 地址进行访问。 不要将列表留空；仅指定防火墙管理员的 *IP* 地址以防止未经授权的访问。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Telemetry（遥测）

遥测是指收集并发送数据以进行威胁和支持分析，以及启用应用程序逻辑的过程。若要收集遥测数据并发送到 Palo Alto Networks，必须先选择目标区域。如果您的组织当前有 Cortex 数据湖许可证，那么，您的目标区域限制为您的 Cortex 数据湖实例所在位置的区域。

遥测数据用于增强应用程序功能，从而提高您管理和配置 Palo Alto Networks 产品和服务的能力。这些应用程序可为您提供有关设备运行状况、性能、容量规划和配置的更好的可见性。Palo Alto Networks 还会继续使用此数据提高威胁防护能力，帮助您最大程度地获得使用产品带来的好处。

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

Generate Telemetry File（生成遥测文件）以获取防火墙将在下一个遥测传输间隔将发送到 Palo Alto Networks 的数据实时示例。

若要完全禁用遥测传输，请不要勾选**Enable Telemetry**（启用遥测），然后提交您的更改。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Content-ID

使用 **Content-ID**™ 选项卡定义 URL 过滤、数据保护和容器页面的设置。

Content-ID 设置	说明
URL 筛选	
动态 URL 缓存超时	单击 **Edit**（编辑），并输入超时（以小时为单位）。此值用于动态 URL 过滤，以确定条目从 URL 过滤服务返回后保留在缓存中的时间长度。仅在使用 BrightCloud 数据库时，此选项才适用于 URL 过滤。有关 URL 过滤的更多信息，请参阅 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）。
URL 继续超时	指定用户执行 **Continue**（继续）操作后，用户必须再次对相同类别 URL 按“继续”之前的时间间隔（范围为 1 至 86,400 分钟；默认为 15）。
URL 管理替代超时	指定用户输入 **Admin Override**（管理替代）密码后，用户必须对相同类别 URL 重新输入该密码之前的时间间隔（范围为 1 至 86,400 分钟；默认为 15）。
保持客户端类别查找请求	启用此选项即可指定在防火墙无法在本地缓存中找到 URL 的类别信息时，其会在查询 PAN-DB 时保持 Web 请求。 该选项在默认情况下已禁用。将其作为最佳实践 URL 筛选配置文件的一部分启用。
类别查找超时（秒）	指定防火墙在确定类别为未解析之前尝试查找 URL 类别的时间（以秒为单位）（范围为 1 至 60 秒；默认为 2）。
URL 管理锁定超时	指定三次尝试不成功后，禁止用户使用 URL 管理替代密码的时间段（范围为 1 至 86,400 分钟；默认为 30）。
PAN-DB 服务器 （连接到私有 PAN-DB 服务器所需）	指定网络中私有 PAN-DB 服务器的 IPv4 地址、IPv6 地址或 FQDN。最多可以添加 20 个条目。 默认情况下，会将防火墙连接到公共 PAN-DB 云。私有 PAN-DB 解决方案适用于那些不允许防火墙直接访问公共云中 PAN-DB 服务器的企业。防火墙访问 URL 数据库、URL 更新和 URL 查询的此 PAN-DB 服务器列表所包含的服务器，以便对网页进行分类。
URL 管理替代	
Settings for URL admin override	对于要为 URL 管理替代配置的每个虚拟系统，**Add**（添加）并指定当 URL 过滤配置文件阻止一个页面且指定 **Override**（替代）操作时要应用的设置（有关详细信息，请参阅 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤））。 • **Location**（位置）—（仅限多虚拟系统防火墙）从下拉列表中选择虚拟系统。 • **Password/Confirm Password**（密码/确认密码）— 输入用户必须输入的密码以替代阻止页面。

© 2019 Palo Alto Networks, Inc.

Content-ID 设置	说明
	• **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）— 要指定在通过指定服务器进行重定向时用来保护通信的证书和允许的 TLS 协议版本，可以选择 SSL/TLS 服务配置文件。有关详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）。 • **Mode**（模式）— 确定阻止页面是透明传递（似乎源自受阻网站）还是将用户重定向到指定服务器。如果选择 **Redirect**（重定向），则输入用于重定向的 IP 地址。 您还可以 **Delete**（删除）条目。
内容云设置	
服务 URL	用于扫描企业数据丢失防护 (DLP) 文件的云服务服务器。 • 亚太地区 — **`apac.hawkeye.services-edge.paloaltonetworks.com`** • 欧洲 — **`eu.hawkeye.services-edge.paloaltonetworks.com`** • 美国 — **`us.hawkeye.services-edge.paloaltonetworks.com`**
Content-ID 设置	
允许转发解密内容	启用此选项即可配置防火墙，以在端口镜像或发送 WildFire® 文件进行分析时将解密的内容转发到外部服务。 启用此选项，并将解密流量中所有未知文件发送到 *WildFire* 进行分析。 对于具有多个虚拟系统（多个 vsys）功能的防火墙，可以为每个虚拟系统单独启用此选项。选择 **Device**（设备）> **Virtual Systems**（虚拟系统），然后选择要在其中启用解密内容转发的虚拟系统。此选项在虚拟系统对话框中可用。
扩展数据包捕获长度	设置防间谍软件和漏洞保护配置文件中启用扩展捕获选项时要捕获的数据包数量（范围为 1 至 50，默认为 5）。
转发超过 TCP App-ID™ 检查队列的分段	启用此选项可转发分段，并在 App-ID 队列超过 64 段限制时将应用程序归类为 `unknown-tcp`。使用以下全局计数器可查看超出此队列的段数（不论是否启用此选项）： `appid_exceed_queue_limit` 禁用此选项可防止防火墙在 App-ID 检查队列被填满时，转发 TCP 分段及跳过 App-ID 检查。 默认禁用此选项，您应该将其禁用以获得最大的安全性。 在禁用此选项时，您可能会注意到在排队等待 *App-ID* 处理的分段超过 *64* 段时会增加数据流的延迟。

© 2019 Palo Alto Networks, Inc.

Content-ID 设置	说明

转发超过 TCP 内容检查队列的分段	启用此选项可转发 TCP 分段，并在 TCP 内容检查队列被填满时跳过内容检查。等待内容引擎做出反应时，防火墙可最多对 64 个分段进行队列排列。防火墙转发分段且因内容检查队列被填满而跳过内容检查时，它将增量以下全局计数器：
	
	`ctd_exceed_queue_limit`
	
	禁用此选项可防止防火墙在内容检查队列被填满时，转发 TCP 分段及跳过内容检查。在禁用此选项时，防火墙会丢弃所有超出队列限制的分段，并增量以下全局计数器：
	
	`ctd_exceed_queue_limit_drop`
	
	此对全局计数器适用于 TCP 和 UDP 数据包。查看全局计数器后，如果您决定更改设置，可以使用以下 CLI 命令从 CLI 中进行修改：
	
	`set deviceconfig setting ctd tcp-bypass-exceed-queue`
	
	此选项默认启用，但 *Palo Alto Networks* 建议您禁用此选项，以确保最大程度的安全性。但是，由于 *TCP* 重新传输已拒绝流量，禁用此选项可能会导致性能下降且某些应用程序可能会丧失其功能 — 尤其是在大流量的环境下。

转发超过 UDP 内容检查队列的数据报	启用此选项可转发 UDP 数据报，并在 UDP 内容检查队列被填满时跳过内容检查。等待内容引擎作出反应时，防火墙可最多对 64 个数据报进行队列排列。防火墙转发数据报且因 UDP 内容检查队列溢出而跳过内容检查时，它将增量以下全局计数器：
	
	`ctd_exceed_queue_limit`
	
	禁用此选项可防止防火墙在 UDP 内容检查队列被填满时，转发数据报及跳过内容检查。禁用此选项的情况下，防火墙会丢弃所有超出队列限制的数据报，并增量以下全局计数器：
	
	`ctd_exceed_queue_limit_drop`
	
	此对全局计数器适用于 TCP 和 UDP 数据包。查看全局计数器后，如果您决定更改设置，可以使用以下命令从 CLI 中进行修改：
	
	`set deviceconfig setting ctd udp-bypass-exceed-queue`
	
	此选项默认启用，但 *Palo Alto Networks* 建议您禁用此选项，以确保最大程度的安全性。但是，由于已丢弃数据包，禁用此选项可能会导致性能下降且某些应用程序可能会丧失其功能 — 尤其是在大流量的环境下。

© 2019 Palo Alto Networks, Inc.

Content-ID 设置	说明
允许 HTTP 部分响应	启用此 HTTP 部分响应选项可让客户端仅提取文件的一部分。传输路径中的下一代防火墙识别并丢弃恶意文件后，它将终止与 RST 数据包的 TCP 会话。如果 Web 浏览器实施了 HTTP Range（HTTP 范围）选项，则它将启动新会话，以便仅提取该文件的剩余部分。这可防止防火墙因缺乏上下文而触发相同的签名到初始会话，同时允许 Web 浏览器重组文件并发送恶意内容；为防止这种情况发生，请确保禁用此选项。 默认情况下，启用 *Allow HTTP partial response*（允许 *HTTP* 部分响应）选项，但 *Palo Alto Networks* 建议您禁用此选项，以确保最大程度的安全性。禁用此选项不会影响设备性能，但可能会影响 *HTTP* 文件传输的中断恢复。此外，禁用此选项可能会影响流媒体服务，如 *Netflix*、*Microsoft* 更新和 *Palo Alto Networks* 内容更新。
实时签名查询	
DNS 签名查询超时 (ms)	指定防火墙查询 DNS 安全服务的持续时间（以毫秒为单位）。如果云在指定时间段结束之前没有响应，防火墙会向请求客户端释放关联的 DNS 响应（范围为 0 至 60,000，默认为 100）。
X-Forwarded-For 标头	
使用 X-Forwarded-For 标头	您不能同时为 *User-ID* 和安全策略启用 *X-Forwarded-For*。 • **Disabled**（已禁用）— 一旦禁用，防火墙将无法在客户端请求中读取来自 X-Forwarded-For (XFF)标头的 IP 地址。 • **Enable for User-ID**（启用用于 **User-ID**）— 启用此选项，即可在 Internet 和代理服务器之间部署防火墙时，指定 User-ID 读取来自请求 Web 服务的客户端内 X-Forwarded-For (XFF) 标头中的 IP 地址，否则代理服务器会隐藏客户端 IP 地址。User-ID 与其使用策略引用的用户名读取的 IP 地址相匹配，以便这些策略可以控制和记录相关联的用户和组进行的访问。如果标头拥有多个 IP 地址，则 User-ID 使用左侧的第一个条目。 在某些情况下，标头值是一个字符串，而不是 IP 地址。如果该字符串与 User-ID 映射到 IP 地址的用户名相匹配，则防火墙将该用户名用于策略中的组映射引用。如果不存在该字符串的任何 IP 地址映射，则防火墙调用设置为 **any**（任何）或 **unknown**（未知）的源用户的策略规则。 URL 过滤日志显示“源用户”字段中匹配的用户名。如果 User-ID 无法执行匹配或没有为与 IP 地址相关联的区域启用，“源用户”字段会显示含有前缀 **`x-fwd-for`** 的 XFF IP 地址。 允许在 *User-ID* 中使用 *XFF* 标头，从而使原始客户端 *IP* 地址出现在日志中，以便在需要调查问题时为您提供帮助。 • **Enable for Security Policy**（启用用于安全策略）— 一旦启用此选项，即可在客户端和防火墙之间部署上游设备（例如，代理服务器或负载均衡器）时，指定防火墙读取来自请求 Web 服务的客户端内 X-Forwarded-For (XFF)标头中的 IP 地址。代理服务器或负载均衡器 IP 地址将客户端 IP 地址替换为请求源 IP。然后，防火墙可以使用 XFF 标头中的 IP 地址实施策略。

© 2019 Palo Alto Networks, Inc.

Content-ID 设置	说明
	防火墙将使用最近添加到 *XFF* 字段的 *IP* 地址。如果该请求通过多个上游设备，则防火墙将根据最后添加的 *IP* 地址应用策略。
Strip-X-Forwarded-For 标头	启用此选项可删除 X-Forwarded-For (XFF) 标头，其中包含在 Internet 和代理服务器之间部署防火墙时请求 Web 服务的客户端的 IP 地址。防火墙会在转发请求之前将标头值归零：转发的数据包不包含内部源 IP 信息。 启用此选项不会禁用将 *XFF* 标头用于策略中的用户属性；防火墙只有在将 *XFF* 标头用于用户属性后才会将 *XFF* 值归零。 当允许在 *User-ID* 中使用 *XFF* 标头时，还可以在转发数据包之前剥离 *XFF* 标头，以保护用户隐私，同时不会失去跟踪用户的能力。启用这两个选项后，您可以记录并跟踪原始用户 *IP* 地址，同时通过不转发其原始 *IP* 地址来保护用户隐私。
内容 ID 功能	
管理数据保护	对访问可能包含敏感信息（如信用卡号或社会保险号）的日志增强保护。 单击 **Manage Data Protection**（管理数据保护），以执行以下任务： • **Set Password**（设置密码）— 如果未配置密码，则输入并确认一个新密码。 • **Change Password**（更改密码）— 输入旧密码，然后输入并确认新密码。 • **Delete Password**（删除密码）— 删除密码和受保护的数据。
容器页面	使用这些设置可根据内容类型（如 application/pdf、application/soap+xml、application/xhtml+、text/html、text/plain 和 text/xml）指定防火墙将跟踪或记录的 URL 类型。按虚拟系统（从 **Location**（位置）下拉列表中选择）设置容器页面。如果虚拟系统没有明确定义的容器页面，则防火墙会使用默认内容类型。 **Add**（添加）并输入某个内容类型，或选择现有的内容类型。 为虚拟系统添加新内容类型时，将替代内容类型的默认列表。如果没有与虚拟系统关联的内容类型，则将使用内容类型的默认列表。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> WildFire

选择 **Device**（设备）> **Setup**（设置）> **WildFire** 可配置防火墙和 Panorama 的 WildFire 设置。您可以同时启用要用来执行文件分析的 WildFire 云和 WildFire 设备。还可以设置将报告的文件大小限制和会话信息。在填充 WildFire 设置后，您可以通过创建 **WildFire Analysis**（**WildFire** 分析）配置文件指定要转发到 WildFire 云或 WildFire 设备的文件（**Objects**（对象）> **Security Profiles**（安全配置文件）> **WildFire Analysis**（**WildFire** 分析））。

要将解密内容转发到 *WildFire*，请参阅转发 WildFire 分析的解密 SSL 通信。

WildFire 设置	说明
常规设置	
WildFire 私有云	要将文件发送到在美国托管的 WildFire 全局云进行分析，请输入 **`wildfire.paloaltonetworks.com`**。或者，您可以将文件发送到 WildFire 区域云进行分析。区域云旨在遵循您可能依赖于您所在位置的数据隐私期望。 转发样本到 *WildFire* 区域云，确保满足您所在区域特定的数据隐私和合规标准。区域云包括： • 欧洲 — ***`eu.wildfire.paloaltonetworks.com`*** • 日本 — ***`jp.wildfire.paloaltonetworks.com`*** • 新加坡 — ***`sg.wildfire.paloaltonetworks.com`***
WildFire 私有云	指定 WildFire 设备的 IPv4/IPv6 地址或 FQDN。 防火墙将要分析的文件发送到指定的 WildFire 设备。 Panorama 从 WildFire 设备收集威胁 ID，以便在设备组中配置的在防间谍软件配置文件（仅限 DNS 签名）和防病毒配置文件中添加威胁异常。此外，Panorama 还会从 WildFire 设备收集信息，以填充从运行 PAN-OS 7.0 之前软件版本的防火墙接收到的 WildFire 提交日志中缺少的字段。
文件大小限制	指定将转发到 WildFire 服务器的最大文件大小。对于文件大小限制相关的所有最佳实践推荐，如果限制过大且阻止防火墙同时转发多个大型零日文件，则根据可用的防火墙缓冲区空间量降低并调整最大限制。如果可提供更多的缓冲区空间，您可以将文件大小限制增大至最佳实践推荐之上。最佳实践推荐是设置不会过度使用防火墙资源的有效限制的良好起点。可用范围为： • **pe**（可移植可执行文件）— 范围为 1MB 至 50MB，默认为 16MB。 设置 *PE* 文件的大小为 *16MB*。 • **apk**（Android 应用程序）— 范围为 1MB 至 50MB，默认为 10MB。 设置 *APK* 文件的大小为 *10MB*。 • **pdf**（可移植文档格式）— 范围为 100KB 至 51,200KB，默认为 3,072KB。

© 2019 Palo Alto Networks, Inc.

WildFire 设置	说明
	设置 *PDF* 文件的大小为 *3,072KB*。 • **ms-office** (Microsoft Office) — 范围为 200KB 至 51,200KB，默认为 16,384KB。 设置 *ms-office* 文件的大小为 *16,384KB*。 • **jar**（封装 Java 类文件）— 范围为 5MB 至 20MB，默认为 1MB。 设置 *jar* 文件的大小为 *5MB*。 • **flash** (Adobe Flash) — 范围为 1MB 至 10MB，默认为 5MB。 设置 *flash* 文件的大小为 *5MB*。 • **MacOSX**（DMG/MAC-APP/MACH-O PKG 文件）— 范围为 10MB 至 50MB，默认为 1MB。 设置 *MacOSX* 文件的大小为 *1MB*。 • **archive**（RAR 和 7z 文件）— 范围为 50MB 至 50MB，默认为 1MB。 设置存档文件的大小为 *50MB*。 • **linux**（ELF 文件）— 范围为 1MB 至 50MB，默认为 50MB。 设置 *linux* 文件的大小为 *50MB*。 • **script**（脚本）（JScript、VBScript、PowerShell 和 Shell Script 文件）— 范围为 10 到 4096KB，默认为 20KB。 设置脚本文件的大小为 *20KB*。 前面的值可能据 *PAN-OS* 或内容发行的版本不同而相异。要查看有效范围，请单击 *Size Limit*（大小限制）字段，随即会出现一个显示有可用范围和默认值的弹出窗口。
报告良性文件	启用该选项后（默认禁用），经 WildFire 分析确定为良性的文件将出现在 **Monitor**（监控）> **WildFire Submissions**（**WildFire** 提交）日志中。 即使在防火墙上启用了该选项，被 WildFire 视为良性的电子邮件链接仍会因已处理链接的潜在数量而无法记录到日志中。
报告灰色软件文件	启用该选项后（默认禁用），经 WildFire 分析确定为灰色的文件将出现在 **Monitor**（监控）> **WildFire Submissions**（**WildFire** 提交）日志中。

© 2019 Palo Alto Networks, Inc.

WildFire 设置	说明
	即使已在防火墙中启用该选项，*WildFire* 确定为灰色的电子邮件链接仍会因已处理链接的潜在数量而无法记录到日志中。 启用报告灰色软件文件以记录会话信息、网络活动、主机活动以及其他有助于分析的信息。
会话信息设置	
设置	指定要转发到 WildFire 服务器的信息。默认情况下会选中所有选项，且最佳实践是转发所有会话信息，以提供统计信息和其他指标，从而允许您采取行动以阻止威胁事件： • 源 **IP**— 发送可疑文件的源 IP 地址。 • 源端口— 发送可疑文件的源端口。 • 目标 **IP**— 可疑文件的目标 IP 地址。 • 目标端口— 可疑文件的目标端口。 • **Vsys**— 用于标识可能的恶意软件的防火墙虚拟系统。 • 应用程序— 用于传输文件的用户应用程序。 • 用户— 目标用户。 • **URL**— 与可疑文件关联的 URL。 • 文件名— 所发送的文件的名称。 • **Email sender**（电子邮件发件人）— 当在 SMTP 和 POP3 通信中检测到恶意电子邮件链接时，将在 WildFire 日志和 WildFire 详细报告中提供发件人姓名。 • **Email recipient**（电子邮件收件人）— 当在 SMTP 和 POP3 通信中检测到恶意电子邮件链接时，将在 WildFire 日志和 WildFire 详细报告中提供收件人姓名。 • **Email subject**（电子邮件主题）— 当在 SMTP 和 POP3 通信中检测到恶意电子邮件链接时，将在 WildFire 日志和 WildFire 详细报告中提供电子邮件主题。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Setup（设置）> Session（会话）

选择 **Device**（设备）> **Setup**（设置）> **Session**（会话）可配置会话老化时间、解密证书设置以及与全局会话相关的设置（例如，用防火墙保护 IPv6 通信以及在策略更改时将安全策略与现有会话重新匹配）。该选项卡包含以下部分：

- 会话设置
- 会话超时
- TCP 设置
- 解密设置：证书撤消检查
- 解密设置：转发代理服务器证书设置
- VPN 会话设置

会话设置

下表介绍了会话设置。

会话设置	说明
重新匹配会话	如果单击 **Edit**（编辑）并选择 **Rematch Sessions**（重新匹配会话），防火墙就会将新配置的安全策略应用于已在进行的会话。该功能在默认情况下已启用。如果禁用该设置，那么所有策略规则更改都只会应用于在更改提交后发起的这些会话。 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规则更改以拒绝 Telnet，那么防火墙会将这个经过修订的策略规则应用于当前会话并阻止该对话。 启用 *Rematch Sessions*（重新匹配会话）以应用最新安全策略规则到当前活动会话。
ICMPv6 令牌桶大小	输入 ICMPv6 错误消息的比率限制的桶大小。令牌桶大小是令牌桶算法的参数，用于控制 ICMPv6 错误数据包的数量（范围为 10-65,535 个数据包，默认为 100）。
ICMPv6 错误数据包比率	输入每一秒全局允许通过防火墙的 ICMPv6 错误数据包平均数（范围为 10-65,535；默认为 100 ）。此值应用于所有接口。如果防火墙达到该 ICMPv6 错误数据包速率，就会使用 ICMPv6 令牌桶启用 ICMPv6 错误消息节流。
启用 IPv6 防火墙	如需为 IPv6 启用防火墙功能，请 **Edit**（编辑）并选中 **IPv6 Firewalling**（**IPv6** 防火墙）。 如果未启用 IPv6 防火墙，则防火墙忽略所有基于 IPv6 的配置。即使您已在接口上启用 IPv6 流量，要使 IPv6 防火墙起效，还必须启用 **IPv6 Firewalling**（**IPv6** 防火墙）。
启用巨帧 全局 MTU	选择可启用 Ethernet 接口上的 Jumbo frame 支持。巨型帧的最大传输单位 (MTU) 为 9192 字节，仅某些型号的设备可使用此功能。

© 2019 Palo Alto Networks, Inc.

会话设置	说明
	• 如果未 **Enable Jumbo Frame**（启用巨型帧），**Global MTU**（全局 **MTU**）默认为 1,500 字节（范围为 576-1,500）。 • 如果 **Enable Jumbo Frame**（启用巨型帧），则 **Global MTU**（全局 **MTU**）默认为 9,192 字节（范围为 9,192–9,216 字节）。 巨型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* 开始启用巨型帧全局 *MTU* 配置，并重启您的防火墙，则将重新分发数据包缓冲区，以更有效地处理巨型帧。 如果启用了巨型帧并存在 MTU 未经专门配置的接口，那么这些接口将自动继承该巨型帧大小。因此，在启用巨型帧之前，如果存在不希望其包含巨型帧的任何接口，您必须将该接口的 MTU 设置为 1500 字节或其他值。要为接口配置 MTU（**Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）），请参阅 PA-7000 系列第 3 层接口。
DHCP 广播会话	如果防火墙充当 DHCP 服务器，请选择此选项，从而为 DHCP 广播数据包启用会话日志。通过 DHCP 广播会话选项，可为 DHCP 生成仅用于 IoT 安全等服务的增强型应用程序日志（EAL 日志）。如果未启用此选项，则防火墙将转发数据包，而不会为 DHCP 广播数据包创建日志。
NAT64 IPv6 最小网络 MTU	输入 IPv6 转换通信的全局 MTU。默认值 1,280 字节基于 IPv6 通信的标准最小 MTU（范围为 1,280 - 9,216）。
NAT 超额订阅率	选择 DIPP NAT 超额订阅率，即防火墙可以同时使用同一转换 IP 地址和端口对的次数。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。 • **Platform Default**（平台默认设置）— 禁用超额订阅率的显式配置，为此型号的设备应用默认超额订阅率。（要查看不同防火墙型号的默认超额订阅率，请访问 https://www.paloaltonetworks.com/products/product-selection.html）。 • **1x** — 1 次。这表示没有超额订阅率；防火墙不能多次同时使用同一转换 IP 地址和端口对。 • **2x** — 2 次 • **4x** — 4 次 • **8x** — 8 次
ICMP 无法访问数据包率(每秒)	定义防火墙每秒可以发送的 ICMP 无法访问响应的最大数。此限制由 IPv4 和 IPv6 数据包共享。 默认值为每秒 200 条消息（范围为 1-65,535）。
加速老化	可加快空闲会话的超时。 选中此选项可启用加速超时，并可指定阈值 (%) 和换算因数。 会话表一旦达到加速老化阈值（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。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。

© 2019 Palo Alto Networks, Inc.

会话设置	说明
	启用加速老化阈值，并设置可接受的换算系数，以便在会话表开始填满时更快地释放会话表。
数据包缓冲区保护	从 PAN-OS 10.0 开始，全局以及每个区域都默认启用数据包缓冲区保护。作为最佳实践，在全局和每个区域上启用数据包缓冲区保护，可保护防火墙缓冲区免遭 DoS 攻击和攻击性会话和源的攻击。此选项可防止防火墙上的接收缓冲区遭遇攻击或滥用流量，从而导致备份系统资源以及丢弃合法流量。数据包缓冲区保护标识攻击性会话，使用随机早期检测 (RED) 作为第一道防线，并在继续滥用的情况下丢弃会话或阻止攻击性 IP 地址。如果防火墙在特定 IP 地址中检测到许多小会话或快速创建的会话（或这两者），则会阻止此 IP 地址。 对防火墙数据包缓冲区利用率进行基线测量，以了解防火墙容量，确保防火墙正确配置，这样，仅攻击才会导致缓冲区的使用情况大幅增加。 • **Alert (%)**（警报 (%)）— 当数据包缓冲区使用率超过此阈值 10 秒钟以上时，防火墙会每分钟创建一个日志事件。当全局启用数据包缓冲区保护时，防火墙会生成日志事件（范围为 0% 到 99%；默认为 50% ）。如果值为 0%，则表示防火墙不能创建日志事件。从默认阈值开始，根据需要进行调整。 • **Activate (%)**（激活 (%)）— 在达到此阈值时，防火墙开始削减滥用最严重的会话（范围为 0% 到 99%；默认为 80% ）。如果值为 0%，则表示防火墙不能应用 RED。从默认阈值开始，根据需要进行调整。

数据包缓冲区保护（续）	• （运行 PAN-OS 10.0 或更高版本的硬件防火墙）这是一种基于利用率百分比（如上所述）的数据包缓冲区保护替代方法，您可以通过启用 **Buffering Latency Based**（基于缓冲延迟）并配置以下设置，触发基于 CPU 处理延迟的数据包缓冲区保护。
	
	  • **Latency Alert (milliseconds)**（延迟警报（毫秒））— 一旦延迟超过该值，防火墙就开始每隔一分钟生成一个警报日志事件（范围为 1 - 20,000；默认为 50）。
	  • **Latency Activate (milliseconds)**（延迟激活（毫秒）— 一旦延迟超过该值，防火墙就会激活传入数据包的随机早期检测 (RED)，并开始每隔 10 秒生成一个激活日志（范围为 1 - 20,000；默认为 200）。
	  • **Latency Max Tolerate (milliseconds)**（允许的最大延迟（毫秒））—一旦延迟大于等于该值，防火墙将使用 RED 且丢弃概率接近 100%（范围为 1 - 20,000ms；默认为 500ms）。
	
	  如果当前延迟值介于延迟激活阈值和允许的最大延迟阈值之间，防火墙按下列方式计算 RED 丢弃概率：（当前延迟 - **Latency Activate**（延迟激活）阈值）/ (**Latency Max Tolerate**（允许的最大延迟）阈值 - **Latency Activate**（延迟激活）阈值）。例如，如果当前延迟值为 300， 延迟激活值为 200，允许的最大延迟值为 500，那么 (300-200)/(500-200) = 1/3，这表示防火墙的 RED 丢弃概率约为 33%。

数据包缓冲区保护（续）	• **Block Hold Time (sec)**（阻止保持时间（秒））— 在丢弃会话或阻止源 IP 地址之前允许会话继续保持的时间（以秒为单位，范围为 0 到 65,535；默认为 60）。此计时器可监控使用 RED 削减的会话，以确定这些会话是否仍然会使缓冲区使用率或延迟超过配置的阈值。如果滥用行为继续的时间超过阻止保持时间，则会丢弃会话。如果值为 0，则表示防火墙不能根据数据包缓冲区保护丢弃会话。从默认值开始，监控数据包缓冲区利用率或延迟，根据需要调整时间值。 • **Block Duration (sec)**（阻止持续时间（秒））— 丢弃的会话保持丢弃状态或阻止的 IP 地址保持阻止状态的时间（以秒为单位，范围为 1 到 15,999,999；默

© 2019 Palo Alto Networks, Inc.

会话设置	说明
	认为 3,600）。使用默认值，除非阻止 IP 地址一个小时会对您的业务状况造成严重损失，在这种情况下，您可以缩短持续时间。监控数据包缓冲区利用率或延迟，根据需要调整持续时间。 网络地址转换*(NAT)*可提升数据包缓冲区利用率。如果这会影响缓冲区利用率，则缩短阻止保持时间以更快阻止单个会话，并缩短阻止持续时间，这样，来自基础 *IP* 地址的其他会话就不会遭受过度惩罚。
多播路由设置缓存	选中此选项（默认情况下禁用）可启用多播路由设置缓存，以使防火墙能在多播路由或转发信息库 (FIB) 条目尚不存在的情况下，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。
多播路由设置缓存区大小	如果启用了 Multicast Route Setup Buffering（多播路由设置缓存），则可调整缓存区大小，以指定每流的缓存区大小（范围为 1 - 2,000，默认为 1,000）。 防火墙可最多缓存 5,000 个数据包。

会话超时

某些会话超时将定义 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。丢弃会话超时定义 PAN-OS 根据安全策略规则拒绝会话后会话保持打开状态的最长时间。

您可以在防火墙上定义 TCP、UDP、ICMP、尤其是 SCTP 会话的超时数值。**Default**（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。

除了全局设置以外，您还可以在 **Objects**（对象）> **Applications**（应用程序）选项卡中灵活地定义单个应用程序的超时值。可用于该应用程序的超时值会显示在“选项”窗口中。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、UDP 或 SCTP 会话超时值。

请使用该部分中的选项来配置全局会话超时设置，尤其是为 TCP、UDP、ICMP、SCTP 以及所有其他类型的会话进行配置。

默认是最佳值，最佳做法是使用默认值。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。

会话超时设置	说明
Default（默认）	非 TCP/UDP、非 SCTP 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长（以秒为单位，范围为 1 - 15,999,999，默认为 30）。
放弃默认值	非 TCP/UDP/SCTP 会话在 PAN-OS 根据防火墙上配置的安全策略规则拒绝会话后保持打开状态的最长时长（以秒为单位，范围为 1 - 15,999,999，默认为 60）。
放弃 TCP	TCP 会话在 PAN-OS 根据防火墙上配置的安全策略规则拒绝会话后保持打开状态的最长时长（以秒为单位，范围为 1 - 15,999,999，默认为 90）。

© 2019 Palo Alto Networks, Inc.

会话超时设置	说明
放弃 UDP	UDP 会话在 PAN-OS 根据防火墙上配置的安全策略规则拒绝会话后保持打开状态的最长时长（以秒为单位，范围为 1 - 15,999,999，默认为 60）。
ICMP	ICMP 会话能在没有 ICMP 响应的情况下处于打开状态的最长时长（范围为 1 - 15,999,999，默认为 6）。
扫描	在防火墙清除会话并恢复该会话使用的缓冲区资源之前，会话可处于非活动状态的最大时间长度（以秒为单位）。非活动时间是指自会话上次通过数据包或事件刷新以来所经过的时间长度。范围为 5 至 30；默认为 10。
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长（范围为 1 - 15,999,999，默认为 3,600）。
TCP 握手	从接收 SYN-ACK 及后续 ACK 开始到完全建立会话的最长时长（以秒为单位，范围为 1 - 60，默认为 10）。
TCP init	启动 TCP 握手计时器之前，接收 SYN 和 SYN-ACK 之间间隔的最长时长（以秒为单位，范围为 1 - 60，默认为 5）。
TCP 半闭合	接收第一个 FIN 和第二个 FIN 或 RST 之间间隔的最长时长（以秒为单位，范围为 1 - 604,800，默认为 120）。
TCP 等待时间	接收第二个 FIN 或 RST 后，TCP 等待的最长时长（以秒为单位，范围为 1 - 600，默认为 15）。
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）之后间隔的最长时长（以秒为单位，范围为 1 - 600，默认为 30）。
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长（以秒为单位，范围为 1 - 1,599,999，默认为 30）。
身份验证门户	身份验证门户 Web 表单的身份验证会话超时（以秒为单位，默认为 30，范围为 1 - 1,599,999）。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。 身份验证门户 Web 表单的身份验证会话超时（以秒为单位，默认为 30，范围为 1 - 1,599,999）。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。
SCTP INIT	从防火墙停止启动 SCTP 关联之前必须接收 INIT ACK 块的防火墙接收 SCTP INIT 块的最长时长（以秒为单位，范围为 1 - 60，默认为 5）。
SCTP COOKIE	从防火墙停止启动 SCTP 关联之前必须接收包含 Cookie 的 COOKIE ECHO 块的防火墙接收包含状态 COOKIE 参数的 SCTP INIT ACK 块的最长时长（以秒为单位，范围为 1 - 600，默认为 60）。
丢弃 SCTP	SCTP 关联在 PAN-OS 根据防火墙上配置的安全策略规则拒绝会话后保持打开状态的最长时长（以秒为单位，范围为 1 - 604,800，默认为 30）。

© 2019 Palo Alto Networks, Inc.

会话超时设置	说明
SCTP	关联在其中的所有会话超时之前可能经历无 SCTP 通信的最长时长（以秒为单位，范围为 1 - 604,800，默认为 3,600）。
SCTP SHUTDOWN	防火墙在 SCTP SHUTDOWN 块之后等待在其忽略 SHUTDOWN 块之前接收 SHUTDOWN ACK 块的最长时长（以秒为单位，范围为 1 - 600，默认为 30）。

TCP 设置

下表介绍了 TCP 设置。

TCP 设置	说明
转发超过 TCP 无序队列的分段	若要防火墙转发超过 TCP 无序队列限制（每个对话 64 个分段）的分段，请选中此选项。如果禁用此选项，防火墙将丢弃超过无序队列限制的分段。如需查看防火墙因启用此选项而丢弃的分段的计数，请运行以下 CLI 命令： `show counter global tcp_exceed_flow_seg_limit` 该选项为默认禁用，并且应当对大多数安全部署保持该方式。对于以无序方式接收 *64* 个分段以上的特定数据流，禁用此选项可能导致其延迟增加。应当不存在连接丢失，因为 *TCP* 堆栈应当处理缺失段重传。
允许响应 SYN 的任意 ACK	启用此选项以在 TCP 会话设置的第一个数据包不是 SYN 数据包时是全局拒绝该数据包。 若要控制单个区域保护配置文件的设置，请在TCP 丢弃中更改*Reject Non-SYN TCP*（拒绝非 *SYN TCP*）设置。
丢弃带有无效时间戳选项的分段	当发送段和允许防火墙验证时间戳对于该会话是否有效时，将会记录 TCP 时间戳，以防包装 TCP 序列号。TCP 时间戳也可用于计算往返时间。在弃用该选项的情况下，防火墙丢弃具有 null 时间戳的数据包。如需查看防火墙因启用此选项而丢弃的分段的计数，请运行以下 CLI 命令： `show counter global tcp_invalid_ts_option` 该选项为默认启用，并且应当对大多数安全部署保持该方式。启用此选项不至于导致性能降级。但如果网络堆栈错误地生成了带无效 *TCP* 时间戳选项值的分段，启用此选项可能导致连接问题。
非对称路径	全局设置是否丢弃或绕过包含非同步 ACK 或超出范围序列号的数据包。

© 2019 Palo Alto Networks, Inc.

TCP 设置	说明
	• **Drop**（丢弃）— 丢弃包含非对称路径的数据包。 • **Bypass**（绕过）— 绕过对包含非对称路径的数据包的扫描。 若要控制单个区域保护配置文件的设置，请在TCP 丢弃中更改 *Asymmetric Path*（非对称路径）设置。
紧急数据标志	使用此选项可配置防火墙是否允许 TCP 标头中的紧急指针（URG 位标志）。TCP 标头中的紧急指针用于促使防火墙将某个数据包从处理队列中取出，并通过主机中的 TCP/IP 堆栈进行加速，从而立即进行处理。此过程称为带外处理。 由于实施紧急指针会因主机不同而相异，所以请将该选项设置为 **Clear**（清除）（默认以及建议的设置），以便通过拒绝带外处理来消除歧义，这将使有效负载中的带外字节变成该负载的一部分，且数据包不会得到紧急处理。此外，**Clear**（清除）设置确保防火墙将协议堆栈中的精确流视为发送数据包的目标主机。当该选项设置为 **Clear**（清除）时，要查看防火墙在其中清除了 URG 标志的段数计数，可运行以下 CLI 命令： `show counter global tcp_clear_urg` 默认情况下，该标志设置为 *Clear*（清除）并且应当对大多数安全部署保持该方式。这样不会导致性能降级，但在极少数应用程序（如 *Telnet*）使用紧急数据功能的实例中，*TCP* 可能受到影响。如果您将该标志设置为 *Do Not Modify*（请勿修改），防火墙将允许 *TCP* 标头中带 *URG* 位标志的数据包，并启用带外处理（不推荐）。
丢弃不带标志的分段	无任何标志设置的不合法 TCP 分段可被用于规避内容检查。在启用该选项的情况下（默认设置），防火墙会丢弃在 TCP 标头中未设置标志的数据包。如需查看防火墙因此选项而丢弃的分段的计数，请运行以下 CLI 命令： `show counter global tcp_flag_zero` 该选项为默认启用，并且应当对大多数安全部署保持该方式。启用此选项不至于导致性能降级。但如果网络堆栈错误地生成了无 *TCP* 标志的分段，启用此选项可能导致连接问题。
剥离 MPTCP 选项	默认全局启用以将（多路径 TCP）MPTCP 连接转换为标准 TCP 连接。 要更改 *MPTCP*，请在TCP 丢弃 中更改 *Multipath TCP (MPTCP) Options*（多路径 *TCP(MPTCP)* 选项）设置。
SIP TCP 明文	选择下列选项之一，以在检测到分段的 SIP 标头时设置 SIP TCP 会话的明文代理行为。

© 2019 Palo Alto Networks, Inc.

TCP 设置	说明
	• **Always Off**（总是关闭）— 禁用明文代理。在下列情况下禁用代理：当 SIP 消息大小通常小于 MSS 且 SIP 消息适合在单个分段中时，或者如果您需要将 TCP 代理资源保留用于 SSL 转发代理或 HTTP/2 时。 • **Always enabled**（始终启用）— 默认设置。将 TCP 代理用于 TCP 会话上的所有 SIP，以帮助纠正 TCP 分段的重组和排序，从而实现正确的 ALG 操作。 • **Automatically enable proxy when needed**（根据需要自动启用代理）— 选择后，将为 ALG 检测到 SIP 消息分段的会话自动启用明文代理。这有助于在将代理用于 SSL 转发代理或 HTTP/2 时对其进行优化。
TCP 重新传输扫描 （PAN-OS 10.0.2 或更高版本）	启用后，一旦检测到重新传输数据包，就会扫描原始数据的校验和。如果原始数据包和重新传输数据包之间的校验和不一致，则重新传输数据包将被视为恶意，并被丢弃。

解密设置：证书撤消检查

选择 **Session**（会话），然后在 Decryption Settings（解密设置）中选择 **Certificate Revocation Checking**（证书撤销检查）以设置下表所述参数。

会话功能：证书撤销检查设置	说明
启用：CRL	选择此选项可使用证书吊销列表 (CRL) 方法来验证证书的吊销状态。 如果还启用了联机证书状态协议 (OCSP)，则防火墙首先会尝试使用 OCSP；如果 OCSP 服务器不可用，则防火墙随后会尝试使用 CRL 方法。 有关解密证书的更多信息，请参阅用于解决的密钥和证书。
接收超时：CRL	如果已启用 CRL 方法来验证证书吊销状态，请指定防火墙在过后将停止等待 CRL 服务响应的时间间隔（秒）（范围为 1 至 60 秒，默认为 5 秒）。
启用：OCSP	选中此选项可使用 OCSP 来验证证书的吊销状态。
接收超时：OCSP	如果已启用 OCSP 方法来验证证书吊销状态，请指定防火墙在过后将停止等待 OCSP 响应者响应的时间间隔（秒）（范围为 1 至 60 秒，默认为 5 秒）。
如果证书状态未知，则阻止会话	选中此选项可在 OCSP 或 CRL 服务回到未知证书吊销状态后阻止 SSL/TLS 会话。否则，防火墙会继续进行会话。
如果证书状态检查超时，则阻止会话	选中此选项可在防火墙注册 OCSP 或 CRL 请求超时后阻止 SSL/TLS 会话。否则，防火墙会继续进行会话。
证书状态超时	请指定防火墙在过后将停止等待任何证书状态服务响应并应用您选择定义的所有会话阻止逻辑的时间间隔（秒）（范围为 1 至 60 秒，默认为 5 秒）。将 **Certificate Status Timeout**（证书状态超时）与 OCSP/CRL **Receive Timeout**（接收超时）进行关联，如下所示： • 如果同时启用 OCSP 和 CRL — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或两个 **Receive Timeout**（接收超时）值的总和。

© 2019 Palo Alto Networks, Inc.

会话功能：证书撤销检查设置	说明
	• 如果只启用 OCSP — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或 OCSP **Receive Timeout**（接收超时）值。 • 如果只启用 CRL — 防火墙在两个时间间隔中的较小时间间隔之后注册请求超时：**Certificate Status Timeout**（证书状态超时）值或 CRL **Receive Timeout**（接收超时）值。

解密设置：转发代理服务器证书设置

在 Decryption Settings（解密设置）（**Session**（会话）选项卡）中，选择 **SSL Forward Proxy Settings**（**SSL** 转发代理设置），以便为防火墙在建立 SSL/TLS 转发代理解密会话时递交给客户端的证书配置 **RSA Key Size**（**RSA** 密钥大小）或 **ECDSA Key Size**（**ECDSA** 密钥大小）和哈希算法。下表介绍了参数。

会话功能：转发代理服务器证书设置	

RSA 密钥大小	在以下各项中选择一项：
	• **Defined by destination host**（按目标主机定义）（默认）— 如果您希望防火墙根据目标服务器所用密钥来生成证书，请选择此选项：
	  • 如果目标服务器使用 RSA 1,024 位密钥，则防火墙会生成使用该密钥大小和 SHA1 哈希算法的证书。
	  • 如果目标服务器使用大小大于 1,024 位（例如，2,048 位或 4,096 位）的密钥，则防火墙会生成使用 2,048 位密钥和 SHA-256 算法的证书。
	• **1024-bit RSA**（**1,024** 位 **RSA**）— 如果无论目标服务器所用的密钥大小如何您都希望防火墙生成使用 1,024 位密钥和 SHA1 哈希算法的证书，请选择此选项。自 2013 年 12 月 31 日起，公共证书授权机构 (CA) 和常用浏览器为所用密钥小于 2048 位的 X.509 证书提供有限支持。将来，当出现此类密钥时，浏览器将根据安全设置向用户发出警告或全面阻止 SSL/TLS 会话。
	• **2048-bit RSA**（**2,048** 位 **RSA**）— 如果无论目标服务器所用的密钥大小如何您都希望防火墙生成使用 RSA 2,048 位密钥和 SHA-256 哈希算法的证书，请选择此选项。公共 CA 和常用浏览器支持 2,048 位密钥，此类密钥的安全性高于 1,024 位密钥。

ECDSA 密钥大小	在以下各项中选择一项：
	• **Defined by destination host**（按目标主机定义）（默认）— 如果您希望防火墙根据目标服务器所用密钥来生成证书，请选择此选项：
	  • 如果目标服务器使用 ECDSA 256 位或 384 位密钥，则防火墙会生成使用该密钥大小的证书。
	  • 如果目标服务器使用大小大于 384 位的密钥，则防火墙会生成使用 521 位密钥的证书。
	• **256-bit ECDSA**（**256** 位 **ECDSA**）— 如果无论目标服务器所用的密钥大小如何您都希望防火墙生成使用 ECDSA 256 位密钥的证书，请选择此选项。
	• **384-bit ECDSA**（**384** 位 **ECDSA**）— 如果无论目标服务器所用的密钥大小如何您都希望防火墙生成使用 ECDSA 384 位密钥的证书，请选择此选项。

© 2019 Palo Alto Networks, Inc.

VPN 会话设置

选择 **Session**（会话），然后在 VPN Session Settings（VPN 会话设置）中配置与建立 VPN 会话的防火墙相关联的全局设置。下表介绍了这些全局设置。

VPN 会话设置	说明
Cookie 激活阈值	指定每个防火墙允许的 IKEv2 半开 IKE SA 的最大数，高于该数字就会触发 Cookie 验证。如果半开 IKE SA 数量超过 Cookie 激活阈值，响应者将会请求 Cookie，且发起者必须使用包含 Cookie 的 IKE_SA_INIT 进行响应。如果 Cookie 验证成功，可以启动其他 SA 会话。 值为 0 表示 Cookie 验证应始终开启。 Cookie 激活阈值是一个全局防火墙设置，且应低于同样为全局设置的最大半开 SA 设置（范围为 0 至 65535；默认为 500）。
最大半开 SA	指定发起者可以发送到防火墙而不会获得响应的 IKEv2 半开 IKE SA 的最大数。在达到最大数后，防火墙不会对新的 IKE_SA_INIT 数据包做出响应（范围为 1 至 65535；默认为 65535）。
最大缓存证书	指定通过防火墙可以缓存的 HTTP 检索的对端证书授权机构 (CA) 证书的最大数。此值仅供 IKEv2 哈希和 URL 功能使用（范围为 1 至 4000；默认为 500）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> High Availability（高可用性）

- Device（设备）> High Availability（高可用性）

为实现冗余，请在 HA 对或 HA 集群的高可用性配置中部署 Palo Alto Networks 下一代防火墙。当两个 HA 防火墙充当一个 HA 对时，就会有两个 HA 部署：

- 主动/被动 — 在此部署中，主动对端会通过两个专用接口不断与被动对端同步其配置和会话信息。在主动防火墙出现硬件或软件崩溃的情况下，被动防火墙可自动转为主动并提供所有服务。所有接口模式均支持主动/被动 HA 部署：虚拟线路、第 2 层接口或第 3 层接口。
- 主动/主动 — 在此部署中，两个高可用性对端均为主动，且可处理通信。对于涉及非对称路由的场景，或在要让动态路由协议（OSPF、BGP）保持两个对端均处于主动状态的情况下，此种部署方式最为合适。仅在虚拟线路和第 3 层接口模式下，支持主动/主动高可用性。除 HA1 和 HA2 链路外，主动/主动部署还需要专用的 HA3 链路。HA3 链路可用作会话设置和非对称流量处理的数据包转发链路。

> 在高可用性对中，两个对端必须型号相同，必须运行同一 *PAN-OS* 版本和内容发行版本，且许可证必须为同一组。
>
> 此外，对于 *VM* 系列防火墙，两个对端必须在同一虚拟机监控程序中，且必须拥有在每个对端上分配的相同数量的 *CPU* 核心。

在受支持的防火墙型号上，您可以创建 HA 防火墙集群，以在数据中心内以及之间确保会话生存能力。如果链路断开，会话将故障转移给集群中的另一个防火墙。此类同步在 HA 对等分布到多个数据中心，或是 HA 对等分布在活动数据中心和备用数据中心之间的用例中极其有用。另一个用例是水平扩展，即，您可以添加 HA 集群成员到单个数据中心，以扩展安全，确保会话存活能力。HA 对可以属于 HA 集群，他们在集群中被视为两个防火墙。HA 集群中支持的防火墙数量根据防火墙型号而定。

- 配置 HA 的重要注意事项
- HA 常规设置
- HA 通信
- HA 链路和路径监视
- HA 主动/主动配置
- 集群配置

配置 HA 的重要注意事项

配置 HA 对时需要注意的事项如下所示。

- 用于本地和对等 IP 的子网不应在虚拟路由器上的其他任何地方使用。
- OS 和内容发行版本在每个防火墙上都应该相同。如出现不匹配，则可能影响对端防火墙的同步。
- LED 在主动防火墙的 HA 端口上呈绿色，而在被动防火墙上的该端口上呈琥珀色。
- 通过在左选择框中选择所需本地配置，以及在右选择框中选择所需对等配置，可以使用设备选项卡上的配置审核工具比较本地和对等防火墙上的配置。
- 通过单击 **Dashboard**（仪表盘）选项卡上 HA 小部件中的 **Push Configuration**（推送配置），即可从 Web 界面同步防火墙。从中推送配置的防火墙上的配置将覆盖对端防火墙上的配置。如需在主动防火墙上通过 CLI 同步防火墙，请使用命令 request high-availability sync-to-remote running-config。

> 在防火墙使用 *10* 千兆 *SFP+* 端口的高可用性 *(HA)* 主动/被动配置中，如果发生故障转移且主动防火墙变成被动状态，则 *10* 千兆以太网端口会关闭，然后重新打开以进行刷新，但在防火墙再次变为主动之前，不会启用传输。如果您监控了临近设备上的软件，将看到此端口不断反复，因为此端口一直在循环关闭和打开。该行为与对其他端口（如 *1* 千兆以太网端口）的操作不同，后者已禁用但仍允许传输，因此临近设备不会检测到此反复。

© 2019 Palo Alto Networks, Inc.

HA 常规设置

- Device（设备）> High Availability（高可用性）> General（常规）

要配置高可用性(HA)对或 HA 集群成员，首选请选择**Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后配置常规设置。

HA 设置	说明
“常规”选项卡	
HA 对设置 — 设置	**Enable HA Pair**（启用 **HA** 对）以激活 HA 对功能和访问下列设置： • **Group ID**（组 **ID**）— 输入标识 HA 对的数字（1 到 63）。如果多个 HA 对驻留于相同的广播域上，则此字段为必填字段（且必须具备唯一性）。 • **Description**（说明）—（可选）输入 HA 对的说明。 • **Mode**（模式）— 设置 HA 部署的类型：**Active Passive**（主动/被动）或 **Active Active**（主动/主动）。 • **Device ID**（设备 **ID**）— 在主动/主动配置中，设置设备 ID 以确定作为主动-主要设备的对端（将 **Device ID**（设备 **ID**）设置为 **0**），以及作为主动-辅助设备的对端（将 **Device ID**（设备 **ID**）设置为 **1**）。 • **Enable Config Sync**（启用配置同步）— 选中此选项即可启用对端之间配置设置的同步。 启用配置同步，确保两个设备始终具有相同的配置，且以相同的方式处理流量。 • **Peer HA1 IP Address**（对端 **HA1 IP** 地址）— 输入对端防火墙 HA1 接口的 IP 地址。 • **Backup Peer HA1 IP Address**（备份对等 **HA1 IP** 地址）— 输入该对等的备份控制链路的 IP 地址。 配置备份对等 *HA1 IP* 地址，这样，如果主链路发生故障，备份链路可使防火墙保持同步和最新。

主动/被动设置	• **Passive Link State**（被动链路状态）— 在以下各选项中选择一项，指定被动防火墙上的数据链路是否应保持开启状态。此选项不适用于 AWS 中的 VM 系列防火墙。
	  • **Shutdown**（关闭）— 强制使接口链接处于关闭状态。此为默认选项，用于确保不会在网络中创建循环。
	  • **Auto**（自动）— 具备物理连接性的链路将保持物理性开启，但在禁用状态下，这些链路不会参与 ARP 学习或数据包转发。这将节省提供链路的时间，从而有助于优化故障转移期间的收敛时间。为避免网络回环，请勿在防火墙已配置任何第 2 层接口的情况下选中此选项。
	  如果防火墙未配置第 *2* 层接口，设置 *Passive Link State*（被动链路状态）为 *auto*（自动）。
	• **Monitor Fail Hold Down Time (min)**（监控失败保持时间（分钟））— 防火墙在变成被动之前处于非运行状态的间隔分钟数（范围为 1-60）。如果因链接或路径监控发生故障而出现缺少检测信号或呼叫信息，可以使用此计时器。

© 2019 Palo Alto Networks, Inc.

HA 设置	说明
选择设置	指定或启用以下设置： • 设备优先级— 输入优先级值以标识主动防火墙。对等中两个防火墙都启用抢先功能后，值较低（优先级较高）的防火墙将成为主动防火墙（范围为 0-255）。 • **Preemptive**（抢先）— 使较高优先级的防火墙可在从故障恢复后继续主动（主动/被动）或主动-主要（主动/主动）运行。您必须在优先级较高的两个防火墙上启用抢先选项，以在从故障中恢复后继续主动或主动-主要运行。如果禁用此设置，则优先级较低的防火墙将保持主动或主动-主要状态，即使优先级较高的防火墙从故障中恢复后也是如此。 是否启用 *Preemptive*（抢先）选项取决于您的业务需求。如果需要主设备成为活动设备，则启用 *Preemptive*（抢先），这样，从故障中恢复后，主设备会抢先辅助设备。如果需要最少的故障转移事件，则禁用 *Preemptive*（抢先）选项，这样，在故障转移后，*HA* 对不会再次进行故障转移，使具有较高优先级的防火墙成为主防火墙。 • **Heartbeat Backup**（检测信号备份）— 使用 HA 防火墙上的管理端口，为检测信号和呼叫消息提供备份路径。管理端口的 IP 地址将通过 HA1 控制链路与 HA 对共享。无需进行其他配置。 如果使用带内端口用于 *HA1* 和 *HA1* 备份链接，则启用 *Heartbeat Backup*（检测信号备份）。如果使用管理端口用于 *HA1* 或 *HA1* 备份链接，则不得启用 *Heartbeat Backup*（检测信号备份）。

	• **HA Timer Settings**（**HA** 计时器设置）— 选择其中一个预设配置文件：
	  • 建议：用于典型故障转移计时器设置。除非您确定需要不同的设置，否则，最好是使用 **Recommended**（建议）设置。
	  • 积极：用于更快地故障转移计时器设置。
	  要查看配置文件内个别计时器的预设值，请选择*Advanced*（高级）和*Load Recommended*（建议加载）或*Load Aggressive*（积极加载）。此屏幕上将显示硬件模型的预设值。
	  • 高级：允许您为以下各个计时器自定义值以满足您的网络需求：
	  • **Promotion Hold Time (ms)**（提升保持时间（毫秒））— 被动对等（在主动/被动模式下）或主动-辅助对等（在主动/主动模式下）在与 HA 对等丢失联系之后，作为主动对等或主动-主要对等接管之前将等待的毫秒数。此保持时间仅在发出对等失败声明后才会开始。
	  • **Hello Interval (ms)**（呼叫间隔（毫秒））— 为验证另一个防火墙上的 HA 程序是否正常运行而发送的呼叫数据包之间相隔的毫秒数（范围为 8,000-60,000，默认为 8,000）。
	  • **Heartbeat Interval(ms)**（检测信号间隔（毫秒））— 指定 HA 对等以 ICMP Ping 的形式交换检测信号消息的频率（范围为 1,000-60,000 毫秒，无默认值）。

	• **Flap Max**（最大翻动数）—当防火墙在最后一次保留主动状态后的 15 分钟内仍保留该状态时，计一次翻动。指定在确定要挂起防火墙并且由被动防火墙接管之前允许的最大翻动次数（范围为 0-16，默认为 3）。值为 0 表示没有最大值（无论翻动多少次，都不会由被动防火墙接管）。

© 2019 Palo Alto Networks, Inc.

HA 设置	说明
	• **Preemption Hold Time (min)**（抢先持有时间（分钟））— 被动对等或主动-辅助对等在作为主动对等或主动-主要对等接管之前将等待的分钟数（范围为 1-60，默认为 1）。 • **Monitor Fail Hold Up Time (ms)**（监视失败持续时间（毫秒））— 防火墙在路径监视或链路监视失败后将保持活动状态的时间间隔（以毫米为单位）。建议使用此设置，以避免因邻近设备的偶尔翻动而导致 HA 出现故障转移（范围为 0 至 60,000；默认为 0 ）。 • **Additional Master Hold Up Time (ms)**（额外主设备持续时间（毫秒））— 此额外时间适用于与监视失败持续时间相同的事件（以毫秒为单位）（范围为 0 至 60,000 ；默认为 500 ）。其他时间间隔仅适用于主动/被动模式下的主动对端，以及主动/主动模式下的主动-主要对端。建议使用此计时器，以免两个对等在同时遇到相同链接或路径监控失败时，发生故障转移。
SSH HA 配置文件设置	一种应用到网络上高可用性(HA)设备 SSH 会话的 SSH 服务配置文件。若要应用现有 HA 配置文件，请选择配置文件，然后单击 **OK**（确定），并 **Commit**（提交）更改。 *您必须从 CLI 中执行 SSH 服务重新启动，以激活配置文件。* 有关详细信息，请参阅Device（设备）> Certificate Management（证书管理）> SSH Service Profile（SSH 服务配置文件）。
集群设置	**Enable Cluster Participation**（启用集群参与）以访问集群设置。支持 HA 集群的防火墙允许成员防火墙集群（单个防火墙对中每个防火墙都计入到总数的 HA 对）。防火墙型号支持的每个集群的成员数如下所示： • PA-3200 系列：6 个成员 • PA-5200 系列：16 个成员 • PA-7080 系列：4 个成员 • PA-7050 系列：6 个成员 配置集群： • **Cluster ID**（集群 **ID**）—HA 集群的唯一数字 ID，在此集群中，所有成员都可以共享会话状态（范围为 1-99；没有默认值）。 • **Cluster Description**（集群说明）— 集群简短而有用的说明。 • **Cluster Synchronization Timeout (min)**（集群同步超时（分钟））— 这是本地防火墙在另一个集群成员（例如，处于未知状态时）阻止集群完全同步时，进入活动状态之前等待的最大分钟数（范围为 0-30；默认值为 0）。 • **Monitor Fail Hold Down Time (min)**（监视失败抑制时间（分钟））— 经过此分钟数后，将重新测试下行链路以查看该链路是否备份（范围为 1-60；默认值为 1）。
操作命令	
挂起本地设备 （或启用本地设备）	使用以下 CLI 操作命令将本地 HA 对等设置为挂起状态，并临时禁用该对等上的 HA 功能： • `request high-availability state suspend` 使用以下 CLI 操作命令将挂起的本地 HA 对等恢复为运行状态： • `request high-availability state functional`

© 2019 Palo Alto Networks, Inc.

HA 设置	说明
	若要测试故障转移，可以禁用主动（或主动-主要）防火墙。

HA 通信

- Device（设备）> High Availability（高可用性）> HA Communications（HA 通信）

若要配置 HA 对或 HA 集群的 HA 链路，请选择 **Device**（设备）> **High Availability**（高可用性）> **HA Communications**（**HA** 通信）。

HA 链接	说明
控制链接 (HA1)/控制链接（HA1 备份）	HA 对中的防火墙使用 HA 链接同步数据和维护状态信息。一些防火墙具有专用控制链路和专用备用控制链路；例如，PA-5200 系列防火墙具有 HA1-A 和 HA1-B。在这种情况下，您应启动选择设置中的检测信号备份选项。如果要对控制链路 HA 链路使用专用 HA1 端口，对控制链路（HA 备份）使用数据端口，建议您启用检测信号备份选项。 对于 PA-220 防火墙等无专用高可用性端口的防火墙，您应为控制链接高可用性连接配置管理端口，并为控制链接 HA1 备份连接配置类型为高可用性的数据端口接口。由于管理端口在此种情况下使用，且检测备份信号选项已通过管理接口连接发生，因此无需启用检测信号备份选项。 在 AWS 中的 VM 系列防火墙上，可将管理端口用作 HA1 链路。 对 *HA* 控制链路使用数据端口时，应注意，由于控制消息必须在数据平面与管理面板之间通信，因此如果数据平面中发生故障，则对端将无法传达 *HA* 控制链路信息，同时还会发生故障转移。最佳做法是使用专用 *HA* 端口，或在无专用 *HA* 端口的防火墙上使用管理端口。
控制链接 (HA1)/控制链接（HA1 备份）	为主 HA 控制链路和备份 HA 控制链路指定以下设置： • 端口— 选择主 HA1 接口和备份 HA1 接口的 HA 端口。备份设置是可选的。 • **IPv4/IPv6** 地址— 输入主 HA1 接口和备份 HA1 接口的 HA1 接口的 IPv4 或 IPv6 地址。备份设置是可选的。 *PA-3200 系列防火墙不支持备份 HA1 接口的 IPv6 地址；请使用 IPv4 地址。* • **Netmask**（网络掩码）— 输入主 HA1 接口和备份 HA1 接口的 IP 地址的网络掩码（如 255.255.255.0）。备份设置是可选的。 • 网关— 输入主 HA1 接口和备份 HA1 接口的默认网关的 IP 地址。备份设置是可选的。 • **Link Speed**（链路速度）—（仅限具有专用 HA 端口的型号）为专用的 HA1 端口选择防火墙之间控制链路的速度。 • **Link Duplex**（链路双工）—（仅限具有专用 HA 端口的型号）为专用的 HA1 端口选择防火墙之间控制链路的双工选项。 • **Encryption Enabled**（启用加密）— 从 HA 对端导出 HA 密钥并将其导入此防火墙后，启用加密。还必须从此防火墙中导出防火墙的 HA 密钥，然后将其导入到 HA 对端中。请为主 HA1 接口配置此设置。“证书”页面上的导入/导出密钥（请参阅 Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件））。

© 2019 Palo Alto Networks, Inc.

HA 链接	说明
	防火墙未直接连接时，启用加密（*HA1* 连接通过的网络设备可以检测、处理或捕获流量）。 • **Monitor Hold Time (ms)**（监视保持时间（毫秒））— 输入声明控制链路故障导致对等失败之前防火墙将等待的时间长度（毫秒）（范围为 1,000 至 60,000，默认为 3,000）。此选项可监视 HA1 端口的物理链路状态。
数据链接(HA2) 配置 *HA2* 备份链路时，如果发生物理链路故障，则将故障转移到备份链路。启用“*HA2* 保持活动状态”选项后，如果根据定义的阈值“*HA* 保持活动状态”消息发生故障，则同样会发生故	为主数据链路和备份数据链路指定以下设置： • 端口— 选择 HA 端口。请为主要和备份 HA2 接口配置此设置。备份设置是可选的。 • **IP** 地址— 指定主 HA2 接口和备份 HA2 接口的 HA 接口的 IPv4 或 IPv6 地址。备份设置是可选的。 • 网络掩码— 指定主 HA2 接口和备份 HA2 接口的 HA 接口的网络掩码。备份设置是可选的。 • 网关— 指定主 HA2 接口和备份 HA2 接口的 HA 接口的默认网关。备份设置是可选的。如果防火墙的 HA2 IP 地址在同一子网中，则 Gateway（网关）字段应留空。 • 启用会话同步— 允许与被动防火墙同步会话信息，并选择传输选项。 启用会话同步，这样，辅助设备可在其数据平面中具有会话，从而允许防火墙将数据包与同步会话进行匹配，并快速转发数据包。如果未启用会话同步，则防火墙必须再次创建会话，这会引入延迟，会导致连接断开。

© 2019 Palo Alto Networks, Inc.

HA 链接	说明
障转移。	

	• 传输— 选择以下任一传输选项：
	  • 以太网- 当防火墙以后端到后端的方式或者通过交换机 (Ethertype 0x7261) 连接时，请使用此选项。
	  • **IP**- 需要第 3 层传输时，请使用此选项（IP 协议号为 99）。
	  • **UDP**- 使用此选项，系统将对整个数据库，而不是只对标头计算校验和，正如 IP 选项一样（UDP 端口为 29281）。使用 UDP 模式的优势在于可借助 UDP 校验和来验证会话同步消息的完整性。
	• （仅限具有专用 HA 端口的型号）**Link Speed**（链路速度）—为专用的 HA2 端口选择对等之间控制链路的速度。
	• （仅限具有专用 HA 端口的型号）**Link Duplex**（链路双工）—为专用的 HA2 端口选择对等之间控制链路的双工选项。
	• **HA2 Keep-alive**（**HA2** 保持活动状态）— 最佳做法是选中此选项来监控 HA 对等之间 HA2 数据链路的健康状态。此选项默认为禁用，您可在一个对端上启用，或同时在两个对端上启用。启用此选项后，对端将使用 keep-alive（保持活动状态）消息监控 HA2 连接，以便根据已设定的 **Threshold**（阈值）（默认为 10,000 毫秒）来检测故障。如果启用 HA2 keep-alive（HA2 保持活动状态），则将执行 HA2 keep-alive（HA2 保持活动状态）恢复操作。选择 **Action**（操作）：
	  • **Log Only**（仅记录）—在系统日志中，将 HA2 接口故障记录为重要事件。对于主动/被动部署，请选择此选项，因为主动对端是唯一转发流量的防火墙。被动对端处于备份状态，且不会转发流量，因而不需要拆分数据路径。如果未配置任何 HA2 备份链路，状态同步将关闭。如果 HA2 路径恢复，则生成参考日志。
	  • **Split Datapath**（拆分数据路径）— 在主动/主动 HA 部署中，选择此选项可指示每个对端在检测到 HA2 接口故障时，取得对其本地状态和会话表的所有权。若无 HA2 连接，则无法执行状态和会话同步；此操作允许对会话表进行独立管理，以确保各 HA 对端能成功转发流量。为防止此情况发生，请配置 HA2 备份链路。
	• **Threshold (ms)**（阈值（毫秒））— 保持活动状态消息在上述任一操作触发之前发生故障的持续时间（范围为 5,000 至 60,000，默认为 10,000）。

集群链路	配置 HA4 链路设置，HA4 链路是专用的集群链路，用于同步具有相同集群 ID 的所有集群成员的会话状态。集群成员之间的 HA4 链路用于检测集群成员之间的连接故障。 • **Port**（端口）—选择用作 HA4 链路的 HA 接口（例如，ethernet1/1）。 • **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）— 输入本地 HA 接口的 IP 地址。 • **Netmask**（网络掩码）— 输入网络掩码。 • **HA4 Keep-alive Threshold (ms)**（**HA4** 保持时间阈值（毫秒））— 防火墙必须从集群成员接收 keepalive 从而知晓集群成员是否正常运行的时间长度（范围为 5,000 - 60,000；默认值为 10,000）。 配置 HA4 备份设置： • **Port**（端口）—选择用作 HA4 备份链路的 HA 接口。 • **IPv4/IPv6 Address**（**IPv4/IPv6** 地址）— 输入本地 HA 备份链路的 IP 地址。 • **Netmask**（网络掩码）— 输入网络掩码。

© 2019 Palo Alto Networks, Inc.

HA 链路和路径监视

- Device（设备）> High Availability（高可用性）> Link and Path Monitoring（链路监视和路径监视）

若要定义 HA 故障转移条件，请配置 HA 链路和路径监视；并选择 **Device**（设备）> **High Availability**（高可用性）> **Link and Path Monitoring**（链路和路径监视）。

链路和路径监视不适用于 *AWS* 中的 *VM* 系列防火墙。

HA 链路和路径监视设置	说明
链接监视	指定以下项： • 已启用 — 启用链路监视。链路监控允许在物理链路或物理链路组失败时触发故障转移。 • 失败条件 — 选择当部分或所有受监视链路组失败时是否进行故障转移。 启用并配置路径监控或链路监控，以在路径或链路断开时帮助触发故障转移。至少为路径监控配置一个 *Path Group*（路径组），并至少为链路监控配置一个 *Link Group*（链路组）。
链接组	定义一个或多个链路组以监视特定以太网链路。要添加链接组，请指定以下内容，并单击添加： • 名称 — 输入链接组名称。 • 已启用 — 启用链路组。 • **Failure Condition**（失败条件）— 选择当部分或所有选定链接失败时是否发生失败。 • 接口 — 选择要监视的一个或多个以太网接口。

路径监视	指定以下项：
	• **Enabled**（已启用）— 基于组合或单个虚拟线路路径监视、VLAN 路径监视和虚拟路由器*路径监视启用路径监视。通过发送 ICMP ping 消息，路径监控使防火墙可以监视指定的目标 IP 地址以确保它们可以作出响应。路径监控用于 Virtual Wire、第 2 层或第 3 层配置，在这些配置中，只有链路监控不足以进行故障转移，还必需监控其他网络设备。
	• **Failure Condition**（失败条件）：
	  • **Any**（任何）—（默认）一旦虚拟线路或 VLAN 或虚拟路由器*的路径监视发生故障，防火墙就会触发 HA 故障转移。
	  • **All**（所有）—一旦虚拟线路和 VLAN 和虚拟路由器*三个其中一个的路径监视发生故障，防火墙就会触发 HA 故障转移。
	 * 如果已启用高级路由，逻辑路由器将替代虚拟路由器，您可以启用逻辑路由器路径监视。
	 启用并配置路径监控或链路监控，以在路径或链路断开时帮助触发故障转移。至少为路径监控配置一个 *Path Group*（路径组），并至少为链路监控配置一个 *Link Group*（链路组）。

© 2019 Palo Alto Networks, Inc.

HA 链路和路径监视设置	说明

路径组	定义一个或多个路径组以监视接口类型的特定目标地址。**Add Virtual Wire Path**（添加虚拟线路路径）和 **Add VLAN Path**（添加 **VLAN** 路径）和 **Add Virtual Router Path**（添加虚拟路由器路径）。（如果已启用高级路由，您可以 **Add Logical Router Path**（添加逻辑路由器路径））。
	
	对于添加的各种类型的路径监视，请指定以下内容：
	
	• **Name**（名称）— 选择要监视的虚拟线路、VLAN 或虚拟路由器*（根据添加的路径监视类型从下拉列表中进行选择）。
	• **Source IP**（源 **IP**）— 对于虚拟线路和 VLAN 接口，输入在发送到下一个跃点路由器（目标 IP 地址）的 ping 中使用的源 IP 地址。本地路由器必须能够将地址路由到防火墙。（与虚拟路由器*关联的路径组的源 IP 地址将自动配置为接口 IP 地址，该 IP 地址在路由表中指示为指定目标 IP 地址的传出接口。）
	• **Enabled**（已启用）— 启用虚拟线路、VLAN 或虚拟路由器*的监视。
	• **Failure Condition**（失败条件）：
	  • **Any**（任何）（默认）— 防火墙确定在任何目标 IP 组发生 ping 故障时，失败的虚拟线路、VLAN 或虚拟路由器*。
	  • **All**（所有）（默认）— 防火墙确定在所有目标 IP 组发生 ping 故障时，失败的虚拟线路、VLAN 或虚拟路由器*。
	
	实际的 *HA* 故障转移取决于您为路径监视设置的失败条件，该条件考虑了虚拟线路、*VLAN* 或虚拟路由器* 路径监视（无论启用哪个）。
	• **Ping Interval**（**Ping** 间隔）— 指定发送到目标IP 地址的 Ping 之间的间隔（范围为 200 至 60,000 毫秒，默认为 200 毫秒）。
	• **Ping Count**（**Ping** 计数）— 在声明故障前指定失败 Ping 的计数（范围为 3 至 10，默认为 10）。
	
	* 如果已启用高级路由，逻辑路由器将替代虚拟路由器，您可以启用逻辑路由器路径监视。

路径组目标 IP	• **Destination IP**（目标 **IP**）—为路径组 **Add**（添加）一个或多个要监视的目标 IP 地址组。
	  • **Destination IP Group**（目标 **IP** 组）— 输入组名称。
	  • 为组**Add**（添加）一个或多个要监视的 **Destination IP**（目标 **IP**）地址。
	  • **Enabled**（已启用）— 勾选此选项以启用目标 IP 组。
	  • **Failure Condition**（失败条件）：选择 **Any**（任何）（以指定是否会在组中任何 IP 地址出现 ping 故障时，将目标组也视为失败）或 **All**（所有）（以指定是否在组中所有 IP 地址出现 ping 故障时，将目标组视为失败）。

HA 主动/主动配置

- Device（设备）> High Availability（高可用性）> Active/Active Config（主动/主动配置）

若要配置主动/主动 HA 对设置，请选择 **Device**（设备）> **High Availability**（高可用性）> **Active/Active Config**（主动/主动配置）。

© 2019 Palo Alto Networks, Inc.

主动/主动配置设置	说明
数据包转发	**Enable**（启用）对端通过 HA3 链路转发数据包，以进行会话设置和非对称性路由会话的第 7 层检查（应用程序 ID、内容 ID 和威胁检查）。
HA3 接口	选择要用于在主动/主动 HA 对端之间转发数据包的数据接口。所使用的接口必须为已设置接口类型为 **HA** 的专用第 2 层接口。 如果 *HA3* 链路失败，主动-辅助对端将转换为非功能状态。为防止此种情况发生，请将带有两个或多个物理接口的链路聚合组 *(LAG)* 接口配置为 *HA3* 链路。防火墙不支持 *HA3* 备份链路。带多个接口的聚合接口将提供额外的容量和链路冗余，以支持 *HA* 对端之间的数据包转发。 使用 HA3 接口时，必须在防火墙和所有中间网络设备上启用巨帧。若要启用巨型帧，请选择 **Device**（设备）> **Setup**（设置）> **Session**（会话），并在会话设置部分选择此选项以 **Enable Jumbo Frame**（启用巨型帧）。
VR 同步	强制同步 HA 对端上配置的所有虚拟路由器。 未对动态路径协议配置虚拟路由时，请使用此选项。两个对等必须通过交换式网络连接到相同的下一个跃点路由器，并且只能使用静态路由。
QoS 同步	同步所有物理接口上的 QoS 配置文件选择。如果两个对端具有类似的链路速度，且在所有物理接口中均需使用相同的 QoS 配置文件，请使用此选项。此设置将影响网络选项卡中的 QoS 同步设置。无论此设置如何，QoS 策略都会同步。
试验保持时间（秒）	当处于 HA 主动/主动配置中的防火墙失败时，防火墙会进入试验状态。从试验状态转为主动-辅助状态将触发 Tentative Hold Time（试验保持时间），在此期间，防火墙将尝试构建路由邻接体，并在处理任何数据包之前填充其路由表。如果没有此计时器，恢复中的防火墙会立即进入主动二级状态，并且会因为没有必需的路由而静默丢弃数据包（默认为 60 秒）。
会话拥有者选择	会话拥有者将负责此会话的所有第 7 层检查（应用程序 ID 和内容 ID），并负责生成此会话的所有通信日志。选择以下选项以指定数据包会话拥有者的确定方式： • **First packet**（第一个数据包）— 选中此选项可将接收会话中第一个数据包的防火墙指定为会话拥有者。这是最佳配置，可最大限度减少通过 HA3 的流量，并在对端中分布数据平面负载。 • **Primary Device**（主要设备）— 如果希望主动-主要防火墙拥有所有会话，请选中此选项。在此情况下，如果主动-辅助防火墙接收了第一个数据包，它会通过 HA3 链路将第 7 层检查所需的所有数据包转发到主动-主要防火墙。
虚拟地址	单击 **Add**（添加），选择 **IPv4** 或 **IPv6** 选项卡，再单击 **Add**（添加）以输入选项，以指定要使用的 HA 虚拟地址类型：浮动或 ARP 负载共享。您还可以在对中混合使用多种虚拟地址类型。例如，您可使用 LAN 接口上的 ARP 负载共享，以及 WAN 接口上的浮动 IP。 • **Floating**（浮动）— 输入在链接或系统发生故障时在 HA 对端之间移动的 IP 地址。请在接口上配置两个浮动 IP 地址，以使每个防火墙都拥有一个地址，然后设置优先级。如果任意一个防火墙发生故障，则浮动 IP 地址将转换到 HA 对端。 • **Device 0 Priority**（设备 **0** 优先级）— 为带 Device ID 0 的防火墙设置优先级，以确定哪个防火墙拥有浮动 IP 地址。值最低的防火墙优先级最高。

© 2019 Palo Alto Networks, Inc.

主动/主动配置设置	说明
	• **Device 1 Priority**（设备 **1** 优先级）— 为带 Device ID 1 的防火墙设置优先级，以确定哪个防火墙拥有浮动 IP 地址。值最低的防火墙优先级最高。 • **Failover address if link state is down**（如果链接状态为失效，则对地址执行故障转移）— 接口上的链接状态为失效时使用故障转移地址。 • **Floating IP bound to the Active-Primary HA device**（将浮动 **IP** 绑定到主动-主要 **HA** 设备）— 选中此选项可将浮动 IP 地址绑定到主动-主要对端。在一个对端出现故障的情况下，流量将不断地被发送到主动-主要对端，即便故障防火墙恢复并成为主动-辅助对端也不例外。

虚拟地址（续）	• **ARP Load Sharing**（**ARP** 负载共享）— 输入 HA 对将共享的 IP 地址，并为主机提供网关服务。仅当防火墙与主机位于同一广播域时，才需选择此选项。选择设备选择算法：
	  • **IP Modulo**（**IP** 模）— 根据 ARP 请求者 IP 地址的奇偶校验，选择响应 ARP 请求的防火墙。
	  • **IP Hash**（**IP** 哈希）— 根据 ARP 请求者 IP 地址的哈希，选择响应 ARP 请求的防火墙。

集群配置

- Device（设备）> High Availability（高可用性）> Cluster Config（集群配置）

通过选择**Device**（设备）> **High Availability**（高可用性）> **Cluster Config**（集群配置），添加成员到 HA 集群。

集群配置	说明
添加	**Add**（添加）集群成员。您必须添加本地防火墙，且如果您使用的是 HA 对，还必须将该对的两个 HA 对等均添加为集群成员。 • （受支持的防火墙）**Device Serial Number**（设备序列号）— 输入集群成员的唯一序列号。 • （Panorama）**Device**（设备）—从下拉列表中选设备，然后输入**Device Name**（设备名称）。 • **HA4 IP Address**（**HA4 IP** 地址）— 输入集群成员 HA4 链路的 IP 地址。 • **HA4 Backup IP Address**（**HA4** 备份 **IP** 地址）— 输入集群成员 HA4 链路备份的 IP 地址。 • **Session Synchronization**（会话同步）— 勾选此选项以启用与此集群成员的会话同步。 • **Description**（说明）— 输入有用的说明。
删除	选择一个或多个集群成员，并从集群中 **Delete**（删除）这些成员。
启用	（受支持的防火墙）您可以确定是否使集群成员与其他成员实现会话同步。默认允许所有成员同步会话。如果已禁用一个或多个成员的同步，请选择 **Enable**（启用）以重新启用一个或多个成员的同步。
禁用	（受支持的防火墙）选择一个或多个成员，并 **Disable**（禁用）与其他成员的同步。
刷新	（Panorama）选择 **Refresh**（刷新）以刷新 HA 集群中 HA 设备列表。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Log Forwarding Card（日志转发卡）

- Device（设备）> Log Forwarding Card（日志转发卡）

日志转发卡 (LFC) 是一种高性能日志卡，可将数据平面上所有数据（例如，流量和威胁）从防火墙转发至一个或多个外部日志记录系统，例如 Panorama 或 syslog 服务器。因为数据平面日志在本地防火墙上不再可用，因此 ACC 选项卡从管理 Web 界面移除，且 Monitor（监控）> Logs（日志）仅包含管理日志（配置、系统和警报）。

您需要为 LFC 配置端口。端口 1 以 10Gbps 的速度运行，端口 9 以 40Gbps 的速度运行。在 **Device**（设备）**> Log Forwarding Card**（日志转发卡）中配置端口。防火墙使用这些端口将数据平面上所有日志转发到外部系统，例如 Panorama 或 syslog 服务器。

有关 LFC 要求和组件的信息，请参阅 PA-7000 系列硬件参考指南 。

对于 LFC 接口，按下表所述配置设置。

LFC 接口设置	说明
姓名	输入接口名称。对于 LFC，您必须选择 **lfc1/1**或 **lfc1/9**。
注释	输入接口的可选说明。
IPv4	如果网络使用的是 IPv4，请定义以下各项： • **IP** 地址 — 端口的 IPv4 地址。 • **Netmask**（网络掩码）— 端口的 IPv4 地址的网络掩码。 • 默认网关 — 端口的默认网关的 IPv4 地址。
IPv6	如果网络使用的是 IPv6，请定义以下各项： • **IP** 地址 — 端口的 IPv6 地址。 • 默认网关 — 端口的默认网关的 IPv6 地址。
链接速度	选择接口速度，以 Mbps 为单位（**10000** 或 **40000**），或选择 **auto**（自动）（默认）以使防火墙根据连接来自动确定速度。可用的接口速度取决于使用的端口（lfc1/1 或 lfc1/9）。对于速度不可配置的接口，**auto**（自动）是唯一选项。
链接状态	选择接口状态为启用 (**up**)、禁用 (**down**) 还是根据连接自动确定 (**auto**)。默认值是 **auto**（自动）。
LACP 端口优先级	防火墙只有在为聚合组启用链路聚合控制协议 (LACP) 后才会使用该字段。如果分配给组的接口数超过活动接口数（最大端口数字段），则防火墙使用接口的 LACP 端口优先级来确定处于待机模式的接口。数字越小，优先级越高（范围为 1-65,535，默认为 32,768）。

如果启用多虚拟系统，则可以使用子接口。要配置 LFC 子接口，请添加子接口，并按下表所述配置设置。

© 2019 Palo Alto Networks, Inc.

LFC 子接口设置	说明
接口名称	只读的 **Interface Name**（接口名称）会显示您所选日志卡接口的名称。在相邻字段中，输入数字后缀 (1-9,999) 以标识子接口。
注释	输入接口的可选说明。
标记	输入该子接口的 VLAN **Tag**（标记）(0-4,094)。 为了便于使用，将该标记与子接口编号保持一致。
虚拟系统	选择日志转发卡 (LFC) 子接口被分配至的虚拟系统 (vsys)。或者，也可以单击 **Virtual Systems**（虚拟系统）以添加新的 vsys。在将 LFC 子接口分配给某个 vsys 后，该接口会用作从日志卡转发日志（syslog、电子邮件、SNMP）的所有服务的源接口。
IPv4	如果网络使用的是 IPv4，请定义以下各项： • **IP** 地址 — 端口的 IPv4 地址。 • **Netmask**（网络掩码）— 端口的 IPv4 地址的网络掩码。 • 默认网关 — 端口的默认网关的 IPv4 地址。
IPv6	如果网络使用的是 IPv6，请定义以下各项： • **IP** 地址 — 端口的 IPv6 地址。 • 默认网关 — 端口的默认网关的 IPv6 地址。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Config Audit（配置审核）

选择 **Device**（设备）> **Config Audit**（配置审核）可查看配置文件之间的差异。此页面将在独立的窗格中以并排方式显示各类配置，并使用不同颜色逐行高亮显示其间差异：绿色表示新增，黄色表示修改，红色表示删除：

Added	Modified	Deleted

配置审核设置	说明
配置名称下拉列表（未标记）	选择两项配置以在未标记的配置名称下拉列表中进行比较（默认为 **Running config**（正在运行的配置）和 **Candidate config**（待选配置））。 您可通过输入所需配置相关的提交操作的 *Description*（说明）值，过滤下拉列表（请参阅提交更改）。
上下文下拉列表	使用 **Context**（上下文）下拉列表可指定各文件高亮差异前后显示的行数。指定更多行数有助于使审核结果与 Web 界面设置相关联。如果将 **Context**（上下文）设置为 **All**（全部），则审核结果将包含所有配置文件。
转至	单击 **Go**（转至）可开始审核。
上一步(<<)和 下一步(>>)	如果已在配置名称下拉列表中选择连续配置版本，则可以启用这些导航箭头。单击 << 以比较下拉列表中的前一对配置，或单击 >> 以比较后一对配置。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Password Profiles（密码配置文件）

- Device（设备）> Password Profiles（密码配置文件）
- Panorama > Password Profiles（密码配置文件）

选择 **Device**（设备）> **Password Profiles**（密码配置文件）或 **Panorama** > **Password Profiles**（密码配置文件）可设置个人本地帐户的基本密码要求。密码配置文件将替代您为所有本地帐户定义的所有最小密码复杂性设置（**Device**（设备）> **Setup**（设置）> **Management**（管理））。

要将密码配置文件应用到帐户，请选择 **Device**（设备）> **Administrators**（管理员）（对于防火墙）或 **Panorama** > **Administrators**（管理员）（对于 Panorama），选择一个帐户，然后选择 **Password Profile**（密码配置文件）。

不能将密码配置文件分配给使用本地数据库身份验证的管理帐户（请参阅 Device（设备）> Local User Database（本地用户数据库）> Users（用户））。

要创建密码配置文件，请 **Add**（添加）并指定下表中的信息。

密码配置文件设置	说明
姓名	输入名称以标识密码配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
需要密码更改期限（天数）	需要管理员根据指定天数定期更改其密码（范围为 0 至 365 天）。例如，如果值设置为 90，则系统将每隔 90 天提示管理员更改一次密码。您还可以设置 0 至 30 天的到期警告，并指定宽限期。
到期警告期限（天数）	如果已设置需要密码更改期限，则此设置可用于提示用户根据强制密码更改日期方法，更改每个日志的密码（范围为 0 至 30 天）。
发布到期后管理员登录次数	允许管理员在其帐户到期后进行指定次数的登录。例如，如果值设置为 3，且其帐户已过期，则此用户最多可在帐户锁定前进行 3 次登录（范围为 0 至 3 次）。
发布到期宽限期（天数）	允许管理员在其帐户到期后在指定天数内登录（范围为 0 至 30 天）。

用户名和密码要求

下表列出了可在 PAN-OS 和 Panorama 帐户的用户名和密码中使用的有效字符。

帐户类型	用户名和密码限制
密码字符集	对任何密码字段字符集都没有限制。
远程管理员、SSL-VPN 或身份验证门户	用户名不允许使用以下字符： • 反撇号 (`) • 尖括号（< 和 >）

© 2019 Palo Alto Networks, Inc.

帐户类型	用户名和密码限制
	• 与号 (&) • 星号 (*) • At 符号 (@) • 问号 (?) • 分隔符 (|) • 单引号 (‘) • 分号 (;) • 双引号 (") • 美元符号 ($) • 圆括号 ('('和')') • 冒号 (':')
本地管理员帐户	本地用户名允许使用以下字符： • 小写字母 (a-z) • 大写字母 (A-Z) • 数字 (0-9) • 下划线 (_) • 句号 (.) • 连字号 (-) 登录名不能以连字符 (-) 开头。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Administrators（管理员）

管理员帐户可控制对防火墙和 Panorama 的访问。防火墙管理员可以对单个防火墙或单个防火墙上的虚拟系统进行完全或只读访问。防火墙具有可执行完全访问的预定义管理员帐户。

要定义 *Panorama* 管理员，请参阅 Panorama > Managed Devices（受管设备）> Summary（摘要）。

支持以下身份验证选项：

- 密码身份验证 — 管理员输入登录用户名和密码。该身份验证不需要证书。可以将其与身份验证配置文件结合使用，或用于本地数据库身份验证。
- 客户端证书身份验证 (Web) — 该身份验证不需要用户名或密码；只需使用证书就能对防火墙访问权限进行身份验证。
- 公钥身份验证 (SSH) — 管理员会在需要访问防火墙的计算机上生成公钥/私钥对，然后将公钥上传到防火墙，以使管理员不必输入用户名和密码即可进行安全访问。

要添加管理员，请单击 **Add**（添加）并填写以下信息：

管理员帐户设置	说明
姓名	输入管理员的登录名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、连字符、句点和下划线。登录名不能以连字符 (-) 开头。
身份验证配置文件	选择用于进行管理员身份验证的身份验证配置文件。此设置可用于 RADIUS、TACACS+、LDAP、Kerberos、SAML 或本地数据库身份验证。有关详细信息，请参阅 Device（设备）> Authentication Profile（身份验证配置文件）。
仅使用客户端证书身份验证 (Web)	选中此选项将对 Web 访问使用客户端证书身份验证。如果选择此选项，不需要用户名和密码；证书即足以对访问防火墙进行身份验证。
新密码 确认新密码	输入并确认管理员的区分大小写的密码（最多 31 个字符）。您也可以选择 **Setup**（设置）> **Management**（管理）以执行最小密码长度。 为确保设备管理接口保持安全，我们建议您使用小写字母、大写字母和数字的组合方式定期更改管理密码。您也可为防火墙上的所有管理员配置最小密码复杂性设置。
使用公钥身份验证(SSH)	选择此选项将使用 SSH 公钥身份验证。单击导入密钥并浏览以选择公钥文件。上载的密钥显示在只读文本区域中。 支持的密钥文件格式为 IETF SECSH 和 OpenSSH。支持的密钥算法为 DSA（1,024 位）和 RSA（768 - 4,096 位）。 如果公钥身份验证失败，防火墙将提示管理员输入用户名和密码。

© 2019 Palo Alto Networks, Inc.

管理员帐户设置	说明
管理员类型	为该管理员分配角色。角色将确定管理员可以查看和修改的内容。 如果选择 **Role Based**（基于角色），请从下拉列表中选择自定义的角色配置文件。有关详细信息，请参阅 Device（设备）> Admin Roles（管理员角色）。 如果选择 **Dynamic**（动态），则可选择下列预定义角色中的一项： • **Superuser**（超级用户）— 对防火墙有完全访问权，且可定义新管理员帐户和虚拟系统。您必须拥有超级用户权限才能用其创建管理用户。 • **Superreader (read-only)**（超级用户（只读））— 对防火墙有只读访问权。 • **Device administrator**（设备管理员）— 对所有防火墙有完全访问权，但无权定义新帐户或虚拟系统。 • **Device administrator (read-only)**（设备管理员（只读））— 对所有防火墙设置有只读访问权，但不包括密码配置文件（无访问权）和管理员帐户（仅登录帐户可见）。 • **Virtual system administrator**（虚拟系统管理员）— 可访问防火墙上的特定虚拟系统，以创建和管理虚拟系统的特定方面（若已启用多虚拟系统功能）。虚拟系统管理员无法访问网络接口、虚拟路由器、IPSec 隧道、VLAN、虚拟线路、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。 • **Virtual system administrator**（虚拟系统管理员）（只读）— 对防火墙上的特定虚拟系统有只读访问权限，可查看虚拟系统的特定方面（若已启用多虚拟系统功能）。具有只读访问权限的虚拟系统管理员无法访问网络接口、虚拟路由器、IPSec 隧道、VLAN、虚拟线路、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。
虚拟系统 （仅限虚拟系统管理员角色）	单击 **Add**（添加）可选择管理员能够访问的虚拟系统。
密码配置文件	请选择密码配置文件（如果适用）。要创建新的密码配置文件，请参阅 Device（设备）> Password Profiles（密码配置文件）。 为管理员创建密码配置文件，确保管理员密码在配置时间段结束后过期。定期更改管理员密码有助于防止攻击者使用已保存或盗用的凭证。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Admin Roles（管理员角色）

选择 **Device**（设备）> **Admin Roles**（管理员角色）可定义管理员角色配置文件，此自定义角色可确定管理用户的访问权限和职责。创建管理员帐户（Device（设备）> Administrators（管理员））时可以分配管理员角色配置文件或动态角色。

要定义 *Panorama* 管理员的管理员角色配置文件，请参阅 Panorama > Managed Devices（受管设备）> Summary（摘要）。

防火墙具备可用于常见标准的 3 个预定义角色。您应先对初始防火墙配置使用超级用户角色，然后为安全管理员、审核管理员和加密管理员创建管理员帐户。创建这些帐户并应用合适的常见标准管理员角色后，可以使用这些帐户进行登录。联邦信息处理标准 (FIPS)/常见标准 (CC) FIPS-CC 模式下的默认超级用户帐户为 **admin**，默认密码为 **paloalto**。在标准操作模式下，默认管理员密码为管理员。预定义的“管理员角色”已创建，其中不存在功能重叠，但具有审核跟踪的只读访问权限的管理员角色除外（除非审核管理员具有完全的读取/删除权限）。这些管理员角色不能修改，其定义如下：

- 审核管理员 — 审核管理员负责定期查看防火墙的审核数据。
- 加密管理员 — 加密管理员负责与防火墙建立安全连接相关的加密元素的配置和维护。
- 安全管理员 — 安全管理员负责其他两个管理角色不处理的所有其他管理任务（如创建安全策略）。

要添加管理员角色配置文件，请单击 **Add**（添加）并按下表所述指定设置。

创建自定义角色，将管理员访问权限限制为每种类型管理员所需的权限。对于每种类型的管理员，启用、禁用或设置 *Web UI*、*XML API*、 *Command Line*（命令行）以及 *REST API* 访问的只读访问权限。

管理员角色设置	
姓名	输入名称以标识此管理员角色（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	（可选）输入角色说明（最多 255 个字符）。
角色	选择管理职责范围： • **Device**（设备）— 此角色适用于所有防火墙，不论其是否具有一个以上的虚拟系统 (vsys)。 • **Virtual System**（虚拟系统）— 此角色适用于防火墙上的特定虚拟系统，以及虚拟系统的特定方面（若已启用多虚拟系统功能）。基于 **Virtual System**（虚拟系统）的管理员角色配置文件在 **Web UI** 选项卡上无权限访问网络接口、VLAN、虚拟线路、IPSec 隧道、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件。创建管理帐户（Device（设备）> Administrators（管理员））时可以选择虚拟系统。
WebUI	单击此特定 Web 界面功能 的图标可设置允许的访问权限： • **Enable**（启用）— 对选定功能有读取/写入访问权。 • **Read Only**（只读）— 对选定功能有只读访问权。 • **Disable**（禁用）— 对选定功能无访问权。
XML API	单击特定 XML API 功能的图标可设置允许的访问权限（**Enable**（启用）或 **Disable**（禁用））。

© 2019 Palo Alto Networks, Inc.

管理员角色设置	

命令行	选择 CLI 访问的角色类型。默认为 **None**（无），即表明不允许访问 CLI。其他选项因角色不同而相异：
	• 设备
	  • **superuser**（超级用户）— 对防火墙有完全访问权，且可定义新管理员帐户和虚拟系统。您必须拥有超级用户权限才能用其创建管理用户。
	  • **superreader**（超级读者）— 对防火墙有只读访问权。
	  • **deviceadmin**（设备管理员）— 对所有防火墙有完全访问权，但无权定义新帐户或虚拟系统。
	  • **devicereader**（设备读者）— 对所有防火墙设置有只读访问权，但不包括密码配置文件（无访问权）和管理员帐户（仅登录帐户可见）。
	• 虚拟系统
	  • **vsysadmin** — 在防火墙上访问特定虚拟系统，以创建和管理虚拟系统的特定方面。**vsysadmin** 设置并不控制防火墙级别或网络级别功能（如静态和动态路由、接口的 IP 地址、IPSec 隧道、VLAN、虚拟线路、虚拟路由器、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件）。
	  • **vsysreader** — 对防火墙上的特定虚拟系统以及虚拟系统的特定方面有只读访问权限。**vsysreader** 设置无权限访问防火墙级别或网络级别功能（如静态和动态路由、接口的 IP 地址、IPSec 隧道、VLAN、虚拟线路、虚拟路由器、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件）。

REST API	单击特定 REST API 功能的图标可设置允许的访问权限（**Enable**（启用）、**Read Only**（只读）或 **Disable**（禁用））。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Access Domain（访问域）

- Device（设备）> Access Domain（访问域）

配置访问域以限制管理员对防火墙上特定虚拟系统的访问权限。防火墙仅在您使用 RADIUS、TACACS+ 或 SAML 标识服务器 (IdP) 服务器管理管理员身份验证和授权时才支持访问域。要启用访问域，您必须定义：

- 外部身份验证服务器的服务器配置文件，请参阅 Device（设备）> Server Profiles（服务器配置文件）> RADIUS、Device（设备）> Server Profiles（服务器配置文件）> TACACS+ 和 Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商）。
- RADIUS 供应商的特定属性 (VSA)、TACACS+ VSA 或 SAML 属性。

管理员尝试登录防火墙时，防火墙会向外部服务器查询管理员的访问域。外部服务器返回关联域，然后防火墙限制管理员对您在访问域中指定的虚拟系统的访问权限。如果防火墙不使用外部服务器进行身份验证和对管理员进行授权，则忽略 **Device**（设备）> **Access Domain**（访问域）设置。

在 *Panorama* 上，您可以在本地通过使用 *RADIUS VSA*、*TACACS+ VSA* 或 *SAML* 属性管理访问域（请参阅 Panorama > Access Domains（访问域））。

访问域设置	说明
姓名	输入访问域的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、连字符、下划线和句点。
虚拟系统	在 Available（可用）列中选择虚拟系统，然后 **Add**（添加）。 访问域只在支持虚拟系统的防火墙上受支持。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Authentication Profile（身份验证配置文件）

使用此页面可配置身份验证管理员和最终用户的设置。防火墙和 Panorama 均支持本地、RADIUS、TACACS+、LDAP、Kerberos、SAML 2.0 和多因素身份验证 (MFA) 服务。

至少创建一个身份验证配置文件以提供外部身份验证，这将所有身份验证请求保存在同一位置，可方便管理，并使用包含跟踪等服务在内的标准身份验证过程。若身份验证失败，最好是采用不同的方法创建多个身份验证配置文件，并对其进行优化（*Device*（设备）> *Authentication Sequence*（身份验证序列）），然后至少创建一个本地登录账户，以便在所有外部方法都失败后予以使用。

您也可以使用此页面向 SAML 标识提供商 (IdP) 注册防火墙或 Panorama 服务（如 Web 界面的管理访问权限）。注册服务使得防火墙或 Panorama 能够使用 IdP 对请求该服务的用户进行身份验证。您可以通过在 IdP 上输入其 SAML 元数据注册服务。防火墙和 Panorama 通过根据您分配给服务的身份验证配置文件自动生成 SAML 元数据文件进行轻松注册；您可以将此元数据文件导出到 IdP。

- 身份验证配置文件
- 来自身份验证配置文件的 SAML 元数据导出

身份验证配置文件

- Device（设备）> Authentication Profile（身份验证配置文件）

选择 **Device**（设备）> **Authentication Profile**（身份验证配置文件）或 **Panorama** > **Authentication Profile**（身份验证配置文件）以管理身份验证配置文件。要创建新的配置文件，**Add**（添加）一个配置文件并填写以下字段。

配置身份验证配置文件后，使用 ***test authentication*** *CLI* 命令，以确定防火墙或 *Panorama* 管理服务器是否可以与后端身份验证服务器进行通信，以及身份验证请求是否成功。您可以在待选配置中执行身份验证测试，以在提交前确定配置是否正确。

身份验证配置文件设置	说明
姓名	输入名称以标识配置文件。名称区分大小写，最多可以包含 31 个字符，只能包括字母、数字、空格、连字符和下划线和句点。名称在与其他身份验证配置文件和身份验证序列相对的当前位置（防火墙或虚拟系统）中必须唯一。 在处于多个虚拟系统模式下的防火墙中，如果身份验证配置文件的 *Location*（位置）为虚拟系统，请不要输入与共享位置中身份验证序列相同的名称。同样，如果配置文件 *Location*（位置）为共享，请不要输入与虚拟系统中序列相同的名称。在这些情况下，尽管您可以提交具有同一名称的身份验证配置文件和序列，但可能会导致引用错误。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。

© 2019 Palo Alto Networks, Inc.

身份验证配置文件设置	说明
身份验证选项卡 调用在因素选项卡中添加的任何多因素身份验证 (MFA) 服务前，防火墙会调用在此选项卡中配置的身份验证服务 如果防火墙通过 *RADIUS*（而非供应商 *API*）与 *MFA* 供应商集成，则必须为该供应商配置 *RADIUS* 服务器配置文件，而不是 *MFA* 供应商配置文件。	
类型	选择提供用户看到的第一个（且（可选）唯一）身份验证质询的服务的类型。根据您的选择，将显示一个对话框，其中显示为服务定义的其他设置。选项如下： • **None**（无）— 不使用任何身份验证。 • **Local Database**（本地数据库）— 在防火墙上使用本地身份验证数据库。此选项在 Panorama 上不可用。 • **RADIUS** — 使用远程身份验证拨入用户服务 (RADIUS) 服务器。 • **TACACS+** — 使用增强的终端访问控制器访问控制系统 (TACACS+) 服务器。 • **LDAP** — 使用轻型目录访问协议 (LDAP) 服务器。 • **Kerberos** — 使用 Kerberos 服务器。 • **SAML** — 使用安全断言标记语言 2.0 (SAML 2.0) 标识提供商 (IdP)。 管理员可以使用 *SAML* 对防火墙或 *Panorama Web* 界面进行身份验证，而不对 *CLI* 进行身份验证。
服务器配置文件 （仅限 RADIUS、TACACS+、LDAP 或 Kerberos）	从下拉列表中选择身份验证服务器配置文件。请参阅 Device（设备）> Server Profiles（服务器配置文件）> RADIUS、Device（设备）> Server Profiles（服务器配置文件）> TACACS+、Device（设备）> Server Profiles（服务器配置文件）> LDAP 或者 Device（设备）> Server Profiles（服务器配置文件）> Kerberos。
IdP 服务器配置文件 （仅限 SAML）	从下拉列表中选择 SAML 标识提供商服务器配置文件。请参阅 Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商）。
从 RADIUS 检索用户组 （仅限 RADIUS）	选择此选项可从在 RADIUS 服务器上定义的供应商特定属性 (VSA) 收集用户组信息。防火墙使用信息根据允许列表条目匹配身份验证用户，而不是执行策略或生成报告。
从 TACACS+ 检索用户组 （仅限 TACACS+）	选择此选项可从在 TACACS+ 服务器上定义的供应商特定属性 (VSA) 收集用户组信息。防火墙使用信息根据允许列表条目匹配身份验证用户，而不是执行策略或生成报告。
登录属性 （仅限 LDAP）	输入 LDAP 目录属性将用户和功能唯一标识为该用户的登录 ID。
密码到期警告 （仅限 LDAP）	如果身份验证配置文件适用于 GlobalProtect 用户，则输入密码到期之前的天数以开始向用户显示通知消息，以提醒他们其密码将在 x 天后到期。默认情况下，会在密码过期（范围为 1 至 255 天）前七天显示通知消息。如果密码过期，用户将无法访问 VPN。

© 2019 Palo Alto Networks, Inc.

身份验证配置文件设置	说明
	建议将代理配置为使用预登录连接方法。这样，即使密码过期，用户仍能连接域以更改其密码。 如果用户允许其密码过期，管理员可以分配临时 LDAP 密码以使用户能够登录 VPN。在这一工作流程中，我们推荐将门户配置中的 **Authentication Modifier**（身份验证修饰符）设置为 **Cookie authentication for config refresh**（配置刷新的 **Cookie** 身份验证）（否则，将使用临时密码对门户进行身份验证，但是网关登录会失败，以防止 VPN 访问）。
签名请求证书 （仅限 SAML）	选择防火墙将用于对发送给标识提供商 (IdP) 的 SAML 消息进行签名的证书。如果在 **IdP Server Profile**（**IdP** 服务器配置文件）中启用 **Sign SAML Message to IdP**（向 **IdP** 签署 **SAML** 消息）选项，则此字段为必填字段（请参阅 Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商））。否则，可以选择证书以对 SAML 消息进行签名。 当生成或导入证书及其关联私钥时，在证书中指定的密钥使用属性控制可以使用密钥的方式： • 如果证书明确列出密钥使用属性，则其中一个属性必须为数字签名，该属性在防火墙上生成的证书中不可用。在这种情况下，必须从企业证书机构 (CA) 或第三方 CA 导入证书和密钥。 • 如果证书没有指定密钥使用属性，则可以将密钥用于任何目的，包括对消息进行签名。在这种情况下，可以使用任何方法获取证书和密钥对 SAML 消息进行签名。 *Palo Alto Networks 建议使用签名证书来确保发送给 IdP 的 SAML 消息的完整性。*
启用单点注销 （仅限 SAML）	选择此选项可让用户通过注销任何单个服务来注销每个身份验证服务。单点注销 (SLO) 仅适用于用户通过 SAML 身份验证访问的服务。这些服务可以在贵组织的外部或内部（如防火墙 Web 界面）。此选项只有您在 IdP 服务器配置文件中输入 **Identity Provider SLO URL**（标识提供商 **SLO URL**）后才适用。您无法为身份验证门户用户启用 SLO。 注销用户后，防火墙自动删除其 IP 地址到用户名映射。
证书配置文件 （仅限 SAML）	选择防火墙将用于验证的证书配置文件： • 在 IdP 服务器配置文件中指定的 **Identity Provider Certificate**（标识提供商证书）。IdP 使用此证书对防火墙进行身份验证。**Commit**（提交）身份验证配置文件配置时，防火墙会验证证书。 • IdP 发送到防火墙进行单点登录 (SSO) 和单点注销 (SLO) 身份验证的 SAML 消息。IdP 使用在 IdP 服务器配置文件中指定的 **Identity Provider Certificate**（标识提供商证书）对消息进行签名。 请参阅 Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）。
用户域 和	防火墙使用 **User Domain**（用户域）根据允许列表条目匹配身份验证用户，并用于 User-ID 组映射。

© 2019 Palo Alto Networks, Inc.

身份验证配置文件设置	说明
用户名修饰符 （除 SAML 以外的所有身份验证类型）	您可以指定 **Username Modifier**（用户名修饰符）来修改用户登录时输入的域和用户名格式。防火墙使用修改后的字符串进行身份验证。可以选择下列选项： • 要只发送未修改的用户输入，将 **User Domain**（用户域）留空（默认），并将 **Username Modifier**（用户名修饰符）设置为变量 **%USERINPUT%**（默认）。 • 要将域预置到用户输入，输入 **User Domain**（用户域），并将 **Username Modifier**（用户名修饰符）设置为 **%USERDOMAIN%\%USERINPUT%**。 • 要将域附加到用户输入，输入用户域并将用户名修饰符设置为 **%USERINPUT%@%USERDOMAIN%**。 如果用户名修饰符包括变量 *%USERDOMAIN%*，则用户域值会替换用户输入的所有域字符串。如果指定 *%USERDOMAIN%* 变量并将 *User Domain*（用户域）留空，则防火墙会删除所有用户输入的域字符串。防火墙将域名解析为 *User-ID* 组映射的相应 *NetBIOS* 名称。这同时适用于父域和子域。用户域修饰符的优先级高于自动衍生的 *NetBIOS* 名称。 • 要允许防火墙使用服务器配置文件类型，以确定在身份验证序列中如何以及何时修改用户输入的格式，请手动输入 **None**（无）作为 **Username Modifier**（用户名修饰符）。有关此选项的更多信息，请参阅《PAN-OS 管理员指南》中的配置身份验证配置文件和序列。
Kerberos 领域 （除 SAML 以外的所有身份验证类型）	如果网络支持 Kerberos 单点登录 (SSO)，请输入 **Kerberos** 领域（最多 127 个字符）。这是用户登录名的主机名部分。例如，用户帐户名 user@EXAMPLE.LOCAL 的领域为 EXAMPLE.LOCAL。
Kerberos Keytab （除 SAML 以外的所有身份验证类型）	如果网络支持 Kerberos 单点登录 (SSO)，请单击 **Import**（导入），单击 **Browse**（浏览）找到 keytab 文件，然后单击 **OK**（确定）。keytab 包含防火墙的 Kerberos 帐户信息（主体名称和哈希密码），执行单点登录身份验证时需要该信息。每个身份验证配置文件都可以拥有一个 keytab。在执行身份验证时，防火墙将首先尝试使用 keytab 建立单点登录。如果成功且用户尝试访问位于 Allow List（允许列表）中，则身份验证立即成功。否则，身份验证过程回滚到指定 **Type**（类型）的手动身份验证（用户名/密码），这不需要 Kerberos。 如果防火墙处于 *FIPS/CC* 模式，则算法必须为 *aes128-cts-hmac-sha1-96* 或 *aes256-cts-hmac-sha1-96*。否则，您也可以使用 *des3-cbc-sha1* 或 *arcfour-hmac*。但是，如果 *keytab* 中的算法与票据授予服务签发给客户端以启用 *SSO* 的服务票据中的算法不匹配，则 *SSO* 进程失败。*Kerberos* 管理员确定服务票据使用的算法。
用户名属性 （仅限 SAML）	输入 SAML 属性，以标识来自 IdP 的消息中身份验证用户的用户名（默认为 **username**）。如果 **IdP Server Profile**（**IdP** 服务器配置文件）包含指定用户名属性的元数据，则防火墙使用该属性自动填充此字段。防火墙将从 SAML 消息检索的用户名与身份验证配置文件的 **Allow List**（允许列表）中的用户和用户组进行相匹配。因为您无法配置防火墙修改 SAML 登录时用户输入的域/用户名字符串，因此登录用户名必须与 **Allow List**（允许列表）条目完全匹配。这是唯一必需的 SAML 属性。 *SAML* 消息可能会在主题字段中显示用户名。如果用户名属性没有显示用户名，防火墙会自动检查主题字段。
用户组属性	输入 SAML 属性，以标识来自 IdP 的消息中身份验证用户的用户组（默认为 **usergroup**）。如果 **IdP Server Profile**（**IdP** 服务器配置文件）包含指定用户组属性

© 2019 Palo Alto Networks, Inc.

身份验证配置文件设置	说明
（仅限 SAML）	的元数据，则此字段自动使用该属性。防火墙使用组信息根据 **Allow List**（允许列表）条目匹配身份验证用户，而不是执行策略或生成报告。
管理员角色属性 （仅限 SAML）	输入 SAML 属性，以标识来自 IdP 的消息中身份验证用户的管理员角色（默认为 **admin-role**）。此属性仅适用于防火墙管理员，而不适用于最终用户。如果 **IdP Server Profile**（**IdP** 服务器配置文件）包含指定管理员角色属性的元数据，则防火墙使用该属性自动填充此字段。防火墙将其预定义（动态）角色或管理员角色配置文件与从 SAML 消息检索的角色进行相匹配，以执行基于角色的访问控制。如果 SAML 消息对于只拥有一个角色的管理员拥有多个管理员角色值，则匹配仅适用于管理员角色属性中的第一个（最左侧）值。对于拥有多个角色的管理员，匹配可以适用于属性中的多个值。
访问域属性 （仅限 SAML）	输入 SAML 属性，以标识来自 IdP 的消息中身份验证用户的访问域（默认为 **access-domain**）。此属性仅适用于防火墙管理员，而不适用于最终用户。如果 **IdP Server Profile**（**IdP** 服务器配置文件）包含指定访问域属性的元数据，则防火墙使用该属性自动填充此字段。防火墙将其本地配置的访问域与从 SAML 消息检索的访问域进行相匹配，以执行访问控制。如果 SAML 消息对于只拥有一个访问域的管理员拥有多个访问域值，则匹配仅适用于访问域属性中的第一个（最左侧）值。对于拥有多个访问域的管理员，匹配可以适用于属性中的多个值。
因素选项卡	
启用附加身份验证因素	如果您希望防火墙在用户成功响应第一个因素（在 **Authentication**（身份验证）选项卡的 **Type**（类型）字段中指定）后调用其他身份验证因素（质询），请选择此选项。 其他身份验证因素仅能通过身份验证策略对最终用户身份验证进行支持。其他因素不支持 *GlobalProtect* 门户和网关的远程用户身份验证，或 *PAN-OS* 或 *Panorama Web* 界面的管理员身份验证。尽管您可以配置其他因素，但这些用例不会执行其他因素。但是，您可以使用 *RADIUS* 或 *SAML* 与所有身份验证用例的 *MFA* 供应商进行集成。 配置使用多因素身份验证 (MFA) 的身份验证配置文件后，必须将其分配给身份验证执行对象（Objects（对象）> Authentication（身份验证）），然后将对象分配给控制对网络资源访问的身份验证策略规则（Policies（策略）> Authentication（身份验证））。
因素	在用户成功响应第一个因素（在 **Authentication**（身份验证）选项卡的 **Type**（类型）字段中指定）后，为防火墙将调用的每个身份验证因素添加 MFA 服务器配置文件（Device（设备）> ServerProfiles（服务器配置文件）> Multi Factor Authentication（多因素身份验证））。防火墙按照列出提供因素的 MFA 服务的自上而下顺序调用每个因素。要更改顺序，选择服务器配置文件，然后选择 **Move Up**（上移）或 **Move Down**（下移）。您最多可以指定三个其他因素。每个 MFA 服务都提供一个因素。一些 MFA 服务允许用户从多个列表中选择一个因素。防火墙通过供应商 API 与这些 MFA 服务集成。通过应用程序或应用程序和威胁内容更新定期添加其他 MFA 供应商 API 集成。
高级选项卡	
允许列表	单击 **Add**（添加），然后选择 **all**（所有）或选择可以使用此配置文件进行身份验证的特定用户和组。当用户进行身份验证时，防火墙会根据该列表中的条目匹配相关联的用户名或组。如果不添加条目，则用户无法进行身份验证。

© 2019 Palo Alto Networks, Inc.

身份验证配置文件设置	说明
	要仅对拥有合法业务访问需求的用户进行身份验证，并减少攻击面，请指定用户或用户组，切勿使用*all*（所有）。 如果输入用户域值，则不需要在允许列表中指定域。例如，如果 *User Domain*（用户域）为 ***businessinc*** 且您要将用户 ***admin1*** 添加到 *Allow List*（允许列表），则输入 ***admin1*** 与输入 ***businessinc\admin1*** 的效果相同。您可以指定目录服务中已经存在的组或根据 *LDAP* 筛选程序指定自定义组。
失败的尝试次数 （除 SAML 以外的所有身份验证类型）	输入防火墙在锁定用户帐户之前允许的连续失败登录尝试次数 (0-10)。值 0 代表没有登录尝试限制。防火墙处于正常运行模式时，默认值为 0；防火墙处于 FIPS-CC 模式时，默认值为 10。 将 *Failed Attempts*（失败的尝试次数）设置为 *5* 或更少，以便在输入错误时容纳合理的重试次数，同时防止恶意系统尝试通过暴力攻击方法登录到防火墙。 如果将失败的尝试次数设置为除 *0* 以外的值，但将锁定时间保留为 *0*，则忽略失败的尝试次数且从不锁定用户。
锁定时间 （除 SAML 以外的所有身份验证类型）	输入设备在用户达到 **Failed Attempts**（失败的尝试次数）后锁定用户帐户的分钟数（范围为 0 至 60，默认为 0）。值为 0 表示应用锁定，直到管理员手动解锁用户帐户。 设置 *Lockout Time*（锁定时间）为至少 *30* 分钟，防止恶意操作者连续登录尝试。 如果将锁定时间设置为除 *0* 以外的值，但将失败的尝试次数保留为 *0*，则忽略锁定时间且从不锁定用户。

来自身份验证配置文件的 SAML 元数据导出

- Device（设备）> Authentication Profile（身份验证配置文件）

防火墙和 Panorama 可以使用 SAML 标识提供商 (IdP) 对请求服务的用户进行身份验证。对于管理员，服务可以是访问 Web 界面。对于最终用户，服务可以是访问您的网络资源的身份验证门户或 GlobalProtect。要为服务启用 SAML 身份验证，您必须通过以 SAML 元数据的形式在 IdP 上输入相关信息注册该服务。防火墙和 Panorama 通过根据您分配给服务的身份验证配置文件自动生成 SAML 元数据文件简化注册，并且您可以将此元数据文件导出到 IdP。导出元数据的另一种最简单的方法是在 IdP 中输入每个元数据字段的值。

导出文件中的一些元数据来自于分配给身份验证配置文件的 *SAML IdP* 服务器配置文件（Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商））。但是，无论在 *SAML IdP* 服务器配置文件中指定的方法怎样，导出文件始终将 *POST* 指定为 *HTTP* 绑定方法。*IdP* 将使用 *POST* 方法将 *SAML* 消息发送到防火墙或 *Panorama*。

要从身份验证配置文件导出 SAML 元数据，单击 Authentication（身份验证）列中的 SAML **Metadata**（元数据）链接，并填写以下字段：要将元数据文件导入 IdP，请参阅您的 IdP 文档。

© 2019 Palo Alto Networks, Inc.

SAML 元数据导出设置	说明
命令	选择要为其导出 SAML 元数据的服务： • **management**（管理）（默认）— 提供管理员对 Web 界面的访问权限。 • **authentication-portal**（身份验证门户）— 通过身份验证门户为最终用户提供对网络资源的访问权限。 • **global-protect**（全局保护）— 通过 GlobalProtect 为最终用户提供对网络资源的访问权限。 所作选择将确定此对话框显示的其他字段。
[管理 | 身份验证门户 | GlobalProtect] 身份验证配置文件	输入要从中导出元数据的身份验证配置文件的名称。默认值是通过单击 **Metadata**（元数据）链接打开对话框的配置文件。
管理选择 （仅限管理）	选择用于指定为管理流量启用的接口（如 MGT 接口）： • **Interface**（接口）— 从防火墙的接口列表中选择接口。 • **IP Hostname**（**IP** 主机名）— 输入服务器的 IP 地址或主机名。如果输入主机名，DNS 服务器必须具有映射到 IP 地址的地址 (A) 记录。
[身份验证门户 | GlobalProtect] 虚拟系统 （仅限身份验证门户或 GlobalProtect）	选择已为其定义身份验证门户设置或 GlobalProtect 门户的虚拟系统。
IP 主机名 （仅限身份验证门户或 GlobalProtect）	输入服务的 IP 地址或主机名。 • **Authentication Portal**（身份验证门户）— 输入 **Redirect Host**（重定向主机）IP 地址或主机名（**Device**（设备）> **User Identification**（用户标识）> **Authentication Portal Settings**（身份验证门户设置））。 • **GlobalProtect** — 输入 GlobalProtect 门户的 **Hostname**（主机名）或 **IP Address**（**IP** 地址）。 如果输入主机名，DNS 服务器必须具有映射到 IP 地址的地址 (A) 记录。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Authentication Sequence（身份验证序列）

- Device（设备）> Authentication Sequence（身份验证序列）
- Panorama > Authentication Sequence（身份验证序列）

在某些环境中，用户帐户驻留在多个目录中（如 LDAP 和 RADIUS）。身份验证序列是防火墙在用户登录时尝试用于对其进行身份验证的一组身份验证配置文件。防火墙尝试依次使用列表自上而下的配置文件 — 应用每个配置文件的身份验证、Kerberos 单点登录、允许列表和帐户锁定值 — 直到某个配置文件成功对用户进行身份验证。防火墙只有在当身份验证序列中的所有配置文件进行身份验证失败时才可拒绝访问。有关身份验证配置文件的详细信息，请参阅 Device（设备）> Authentication Profile（身份验证配置文件）。

使用多个身份验证配置文件配置身份验证序列，这些配置文件均使用不同的身份验证方法。至少配置两个外部身份验证方法和一个本地（内部）方法，这样，身份验证就不会因连接问题而中断。将本地身份验证配置文件置于序列的最后一个位置，这样，仅在所有外部身份验证方法都失败后才会使用。（外部身份验证提供专用、可靠且集中的身份验证服务，包括日志记录和故障排除功能。）

身份验证序列设置	说明
姓名	输入名称以标识序列。名称区分大小写，最多可以包含 31 个字符，只能包括字母、数字、空格、连字符和下划线和句点。名称在与其他身份验证序列和身份验证配置文件相对的当前位置（防火墙或虚拟系统）中必须唯一。 在拥有多个虚拟系统的防火墙中，如果身份验证序列的位置为虚拟系统 *(vsys)*，请不要输入与共享位置中身份验证配置文件相同的名称。同样，如果序列 *Location*（位置）为共享，请不要输入与虚拟系统中配置文件相同的名称。在这些情况下，尽管您可以提交具有同一名称的身份验证序列和配置文件，但可能会发生引用错误。
位置	选择在其中使用序列的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存序列后，您无法更改其位置。
使用域确定身份验证配置文件	如果您希望防火墙将用户在登录时输入的域名来匹配与序列相关联的身份验证配置文件的 **User Domain**（用户域）或 **Kerberos Realm**（**Kerberos** 领域），然后使用该配置文件对用户进行身份验证，则可以选择此选项（默认为选定）。防火墙用来相匹配的用户输入可以是用户名前面的文本（带有反斜杠分隔符）或用户名后面的文本（带有 @ 分隔符）。如果防火墙找不到匹配，则尝试按自上而下顺序使用序列中的身份验证配置文件。
身份验证配置文件	单击添加，然后从下拉列表中选择要添加到序列的每个身份验证配置文件。要更改列表顺序，选择一个配置文件，然后单击向上移或向下移。要删除配置文件，请将其选中，并单击删除。 您不能添加指定多因素身份验证 *(MFA)* 服务器配置文件或安全断言标记语言 *(SAML)* 标识提供商服务器配置文件的身份验证配置文件。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Data Redistribution（数据重新分发）

这些设置定义防火墙或 Panorama 使用的数据重新分发方法。

您在查找什么内容？	请参阅：
添加或删除数据重新分发代理。	Device（设备）> Data Redistribution（数据重新分发）> Agents（代理）
查看数据重新分发客户端的信息。	Device（设备）> Data Redistribution（数据重新分发）> Clients（客户端）
配置数据重新分发代理收集器和预共享密钥。	Device（设备）> Data Redistribution（数据重新分发）> Collector Settings（收集器设置）
定义数据重新分发代理在重新分发数据时包括或排除的子网。	Device（设备）> Data Redistribution（数据重新分发）> Include/Exclude Networks（包括/排除网络）

Device（设备）> Data Redistribution（数据重新分发）> Agents（代理）

使用序列号或主机和端口信息添加数据重新分发代理。

数据重新分发代理设置	说明
姓名	输入数据重新分发代理的名称（最多 31 个字符）。仅可使用字母、数字、空格、连字符和下划线。
已启用	勾选此选项可启用数据重新分发代理。

添加代理的方式	选择您想如何添加数据重新分发代理：
	• **Serial Number**（序列号）— 勾选此选项，然后选择序列号。
	• **Host and Port**（主机和端口）—勾选此选项，然后输入以下主机和端口信息：
	  • **Host**（主机）— 输入主机名。
	  • **LDAP Proxy**（**LDAP** 代理）— 勾选此选项以将主机用作 LDAP 代理。
	  • **Port**（端口）— 输入代理侦听请求的端口号。
	  • **Collector Name**（收集器名称）—输入将防火墙或虚拟系统标识为 User-ID 代理的 **Collector Name**（收集器名称）和 **Pre-Shared Key**（预共享密钥）。

数据类型	选择您想重新分发的数据类型（IP 用户映射、IP 标记、用户标记、HIP 或隔离列表）。

© 2019 Palo Alto Networks, Inc.

配置数据重新分发代理后，您可以查看重新分发代理的下列信息：

数据重新分发代理信息	说明
序列号	代理的标识号。
主机	主机的信息。
收集器名称	收集器代理的名称。
HIP	代理的主机信息配置文件。
IP 用户映射	IP 地址到用户名映射信息。
IP 标记	IP 地址到标记映射信息。
隔离列表	显示正在隔离的设备列表。
动态用户组	用户名到标记映射信息。
连接	指示代理是否连接到重新分发服务。

Device（设备）> Data Redistribution（数据重新分发）> Clients（客户端）

选择**Device**（设备）> **Data Redistribution**（数据重新分发）> **Clients**（客户端）以显示各个重新分发客户端的下列信息：

重新分发代理信息	说明
主机信息	客户端的主机信息。
端口	重新分发客户端使用的端口。
Vsys ID	与重新分发客户端连接的虚拟系统的标识。
版本	客户端的 PAN-OS 版本。
STATUS（状态）	显示重新分发客户端的状态。
PDF/CSV	具有最小只读访问权限的管理角色可以将数据重新分发信息导出为 **PDF/CSV**。
刷新连接	更新连接的所有重新分发客户端的信息。

Device（设备）> Data Redistribution（数据重新分发）> Collector Settings（收集器设置）

若要配置与 User-ID 重新分发代理的连接，请输入收集器名称和预共享密钥。

© 2019 Palo Alto Networks, Inc.

数据重新分发代理设置设置	说明
收集器名称	输入用于标识重新分发代理的 **Collector Name**（收集器名称）（最多 255 个字母数字字符）。
收集器预共享密钥/确认收集器预共享密钥	输入并确认收集器的 **Pre-Shared Key**（预共享密钥）（最多 255 个字母数字字符）。

Device（设备）> Data Redistribution（数据重新分发）> Include/Exclude Networks（包括/排除网络）

使用包括/排除网络列表定义重新分发代理在重新分发映射时包括或排除的子网。

任务	说明
添加	要将发现限制到特定的子网，请 **Add**（添加）子网配置文件并填写以下字段： • **Name**（名称）— 输入标识此子网的名称。 • **Enabled**（已启用）— 选中此选项可启用服务器监控中要包括或排除的子网。 • **Discovery**（发现）— 选择 User-ID 代理是否会 **Include**（包括）或 **Exclude**（排除）此子网。 • **Network Address**（网络地址）— 输入此子网的 IP 地址范围。 代理会将“隐式排除全部”规则应用到该列表。例如，如果使用 **Include**（包括）选项添加子网 10.0.0.0/8，则即使不将其他子网添加到列表中，代理也会将其排除。只有当您希望代理排除已明确包含的子网的一个子集时，您才需要使用**Exclude**（排除）选项添加条目。例如，如果您使用包含选项添加 10.0.0.0/8，并使用排除选项添加 10.2.50.0/22，则 User-ID 代理将对除 10.2.50.0/22 外的所有 10.0.0.0/8 子网执行发现，并且排除 10.0.0.0/8 之外的所有子网。如果添加**Exclude**（排除）配置文件而不添加任何**Include**（包括）配置文件，则代理会排除所有子网，而不只是已添加的子网。
删除	要将子网从列表中删除，请选中子网并将其 **Delete**（删除）。 **提示:**要从 Include/Exclude Networks（包括/排除网络）列表中删除子网，但不删除其配置，请编辑子网配置文件并取消选中 **Enabled**（已启用）。
自定义包括/排除网络	默认情况下，代理会按添加子网的顺序（从顶部第一个到底部最后一个）来评估子网。要更改评估顺序，请单击自定义包含/排除网络顺序。然后，您可 **Add**（添加）、**Delete**（删除）、**Move Up**（上移）或**Move Down**（下移）子网以创建自定义评估顺序。

© 2019 Palo Alto Networks, Inc.

Device（设备） > Device Quarantine（设备隔离）

Device（设备） > **Device Quarantine**（设备隔离）页面会显示隔离列表中的设备。设备会因下列操作出现在该列表中：

- 系统管理员手动添加设备到该列表。

  若要手动 **Add**（添加）设备，请输入您想隔离的设备的 **Host ID**（主机 **ID**）和 **Serial Number**（序列号）（可选）。
- 系统管理员从流量、GlobalProtect 或威胁日志中选择主机 ID 列，从该列中选择设备，然后选择 **Block Device**（阻止设备）。
- 设备与拥有日志转发配置文件的安全策略规则匹配，且该配置文件的匹配列表具有已设为 **Quarantine**（隔离）的内置操作。

  主机 *ID* 自动显示在 *GlobalProtect* 日志中。对于要显示在流量、威胁或统一日志中的主机 *ID*，防火墙必须至少有一个将 *Source Device*（源设备）设为 *Quarantine*（隔离）的安全策略规则。如果未在安全策略中执行此设置，“流量”、“威胁”或“统一”日志就没有主机 *ID*，且日志转发配置文件也不会生效。
- 使用 API 添加设备到隔离列表。
- 防火墙将隔离列表作为重新分发条目的一部分接收（从另一个 Panorama 设备或防火墙重新分发隔离列表）。

设备隔离表包含以下字段。

字段	说明
主机 ID	被阻止主机的主机 ID。
原因	设备被隔离的原因。原因**Admin Add**（管理员添加）意味着管理员自动添加设备到表格。
时间戳	管理员或安全策略规则添加设备到隔离列表的时间。
源设备/应用程序	添加设备到隔离列表的 Panorama、防火墙或第三方应用程序的 IP 地址。
序列号	（可选）隔离设备的序列号（如有）。
用户名	（可选）在设备隔离时登录到设备的 GlobalProtect 客户端用户的用户名。

© 2019 Palo Alto Networks, Inc.

Device（设备）> VM Information Sources（VM 信息源）

使用此选项卡可以主动跟踪部署在以下任意源上的虚拟机 (VM) 所发生的变化：VMware ESXi 服务器、VMware vCenter 服务器、Amazon Web 服务虚拟私有云 (AWS-VPC) 或 Google Compute Engine (GCE)。

> 监控作为 *VM* 系列 *NSX* 版解决方案一部分的 *ESXi* 主机时，请使用动态地址组来了解虚拟环境中的变化，而非使用 *VM* 信息源。对于 *VM* 系列 *NSX* 版解决方案，*NSX Manager* 将为 *Panorama* 提供 *IP* 地址所属 *NSX* 安全组的相关信息。来自 *NSX Manager* 的信息将为定义动态地址组中的匹配条件提供完整的上下文。由于此信息将服务配置文件 *ID* 用作专有属性，所以当不同的 *NSX* 安全组中存在重复 *IP* 地址时，可确保策略得以正确实施。
>
> 您最多可以为一个 *IP* 地址注册 *32* 个标记。

监控 VM 信息源的方式有两种：

- 防火墙可以监控您的 VMware ESXi 服务器、VMware vCenter 服务器、GCE 实例或 AWS-VPC，并在您提供或修改受监控源中配置的来宾时检索到相应变化。对于各个防火墙或是配置多个虚拟系统的防火墙上的各个虚拟系统，您最多可以配置 10 个源。

  当您的防火墙配置为高可用性 (HA) 配置时，以下条件适用：

  - **Active/passive HA configuration**（主动/被动 **HA** 配置）— 只有主动防火墙可以监控 VM 信息源。
  - **Active/active HA configuration**（主动/主动 **HA** 配置）— 只有优先级值为主要的防火墙可以监控 VM 信息源。

  想要了解 VM 信息源和动态地址组是如何实现同步工作并使您能够监控虚拟环境变化的，请参阅《VM-Series 部署指南》。
- 对于用户名映射的 IP 地址，您可以对 Windows User-ID 代理或防火墙上的 VM 信息源进行配置，以便监控 VMware ESXi 和 vCenter 服务器，并在您提供或修改服务器中配置的来宾时检索到相应变化。Windows User-ID 代理最多支持 100 个源。User-ID 代理不支持 AWS 和 Google Compute Engine。

  > 受监控 *ESXi* 或 *vCenter* 服务器上的每一个 *VM* 都必须安装并运行 *VMware* 工具。*VMware* 工具能够收集分配给各个 *VM* 的 *IP* 地址和其他值。

要收集分配给受监控 VM 的值，防火墙将监控下列表格中的属性。

VMware 源所监控的属性
• UUID • 姓名 • 来宾操作系统 • 注释 • VM 状态 — 电源状态可以为关闭、开启、待机或未知。 • 版本 • 网络 — 虚拟交换机名称、端口组名称和 VLAN ID • 容器名称 — vCenter 名称、数据中心对象名称、资源池名称、集群名称、主机和主机 IP 地址。

© 2019 Palo Alto Networks, Inc.

AWS-VPC 所监控的属性
• 架构 • 来宾操作系统 • 映像 ID • 实例 ID • 实例状态 • 实例类型 • 密钥名称 • 位置 — 租户、组名称和可用性区域 • 私有 DNS 名称 • 公共 DNS 名称 • 子网 ID • 标记（键、值）；每个实例最多支持 18 个标记 • VPC ID

受监控 Google Compute Engine (GCE) 属性
• VM 主机名 • 机器类型 • 项目 ID • 源（操作系统类型） • 状态 • 子网络 • VPC 网络 • 区域

Add（添加）— 为 VM 监控 **Add**（添加）新源，然后根据所监控的源填写详细信息：

- 对于 VMware ESXi 或 vCenter 服务器，请参阅为 VMware ESXi 或 vCenter 服务器启用 VM 信息源设置。
- 对于 AWS-VPC，请参阅为 AWS VPC 启用 VM 信息源设置。
- 对于 Google Compute Engine (GCE)，请参阅为 Google Compute Engine 启用 VM 信息源设置。

Refresh Connected（刷新已连接）— 刷新屏幕显示中的连接状态；这不会刷新防火墙和受监控源之间的连接。

Delete（删除）— 删除您选择的任何配置的 VM 信息源。

PDF/CSV— 将 VM 信息源配置表格导出为 PDF 或逗号分隔值 (CSV) 文件。请参阅配置表格导出。

为 VMware ESXi 或 vCenter 服务器启用 VM 信息源设置

下表介绍了您配置的为 VMware ESXi 和 vCenter 服务器启用 VM 信息源的设置。

要检索虚拟机的标签，防火墙需要一个对 *VMware ESXi* 和 *vCenter* 服务器具有只读访问权限的帐户。

© 2019 Palo Alto Networks, Inc.

为 VMware ESXi 或 vCenter 服务器启用 VM 信息源的设置	
名称	输入名称以标识受监控源（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
类型	选定受监控主机/源是 **ESXi** 服务器还是 **vCenter** 服务器。
说明	（可选）添加用于标识来源的位置和功能的标签。
端口	指定主机/源要侦听的端口。（默认端口 443）。
已启用	默认情况下，会启用防火墙和所配置源之间的通信。 受监控源和防火墙之间的连接状态将如下所示显示在界面中： • 已连接 • 已断开连接 • 暂挂；禁用受监控源时，连接状态也会显示为黄色。 取消选中 **Enabled**（启用）选项可禁用主机和防火墙之间的通信。
超时	输入时间间隔（以小时为单位，范围为 2-10，默认为 2），在此时间后，如果主机无响应，则与受监控源的连接将关闭。 （可选）要更改默认值，请选中 **Enable timeout when the source is disconnected**（源中断时启用超时），并指定一个值。达到指定限制时，或者如果主机无法访问或无响应，防火墙将关闭源连接。
源	输入受监控主机/源的 FQDN 或 IP 地址。
用户名	指定向源进行验证时需要使用的用户名。
密码	输入密码并确认输入。
更新间隔	指定防火墙从源检索信息的间隔秒数（范围为 5-600，默认为 5）。

为 AWS VPC 启用 VM 信息源设置

下表介绍了您配置的为 AWS VPC 启用 VM 信息源的设置。

为 AWS VPC 启用 VM 信息源设置	
名称	输入名称以标识受监控源（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
类型	选择 **AWS VPC**。
说明	（可选）添加用于标识来源的位置和功能的标签。
已启用	默认情况下，会启用防火墙和所配置源之间的通信。 受监控源和防火墙之间的连接状态将如下所示显示在界面中：

© 2019 Palo Alto Networks, Inc.

为 AWS VPC 启用 VM 信息源设置	
	• 已连接 • 已断开连接 • 暂挂；禁用受监控源时，连接状态也会显示为黄色。 取消选中 **Enabled**（启用）选项可禁用主机和防火墙之间的通信。
源	添加虚拟私有云所在的 URI。例如，ec2.us-west-1.amazonaws.com 语法为：ec2.<*your_AWS_region*>.amazonaws.com；对于 AWS China，语法为：ec2.<AWS_region>.amazonaws.com.cn
访问密钥 ID	输入字母文本字符串，该字符串应能唯一标识拥有或有权访问 AWS 帐户的用户。 AWS 安全证书包含这一信息。防火墙需要这些证书（访问密钥 ID 和秘密访问密钥），才能为针对 AWS 服务执行的 API 调用进行数字签名。
秘密访问密钥	输入密码并确认输入。
更新间隔	指定防火墙从来源检索信息的间隔秒数（范围为 60 - 1,200，默认为 60）。
超时	时间间隔（以小时为单位，默认为 2），在此时间后，如果主机无响应，则与受监控源的连接将关闭。 （可选）源中断时启用超时。达到指定限制时，或者如果源无法访问或无响应，防火墙将关闭源连接。
VPC ID	输入要监控的 AWS-VPC 的 ID，例如 vpc-1a2b3c4d。只会监控部署在该 VPC 中的 EC2 实例。 如果将帐户配置为使用默认 VPC，AWS 帐户属性下会列出默认 VPC ID。

为 Google Compute Engine 启用 VM 信息源设置

Device（设备）> **VM Information Sources**（**VM** 信息源）> **Add**（添加）

下表介绍了您在 Google Cloud Platform 上为 Google Compute Engine 实例启用 VM 信息源所需配置的设置。启用 Google Compute Engine (GCE) 实例监控，以允许防火墙（物理或虚拟内部部署或在 Google Cloud 中运行）检索有关在指定项目的特定 Google Cloud 区域中运行的实例的标记、标签和其他元数据。有关 Google Cloud Platform 上 VM 系列的信息，请参阅《VM 系列部署指南》。

为 Google Compute Engine 启用 VM 信息源设置	
名称	输入名称以标识受监控源（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。
类型	选择 **Google Compute Engine**。
说明	（可选）添加用于标识来源的位置和功能的标签。
已启用	默认情况下，会启用防火墙和所配置源之间的通信。 受监控源和防火墙之间的连接状态将如下所示显示在界面中：

© 2019 Palo Alto Networks, Inc.

为 Google Compute Engine 启用 VM 信息源设置	
	• 🟢 — 已连接 • 🔴 — 已断开连接 • 🟡 — 暂挂或受监控源被禁用。 取消选中 **Enabled**（启用）选项可禁用所配置源和防火墙之间的通信。 禁用通信后，所有已注册的 IP 地址和标记将从关联的动态地址组中删除。这意味着，策略规则将不适用于此 Google Cloud 项目的 GCE 实例。
服务身份验证类型	选择在 GCE 上运行的 VM 系列或服务帐户。 • **VM-Series running on GCE**（在 **GCE** 上运行的 **VM** 系列）— 如果您启用 VM 监控的基于硬件的防火墙或 VM 系列防火墙未部署在 Google Cloud Platform 中，请选择此选项。 • **Service Account**（服务帐户）— 如果要在未部署在 Google Cloud Platform 上的防火墙上监控 Google Cloud Engine 实例，请选择此选项。此选项允许您使用属于虚拟机或应用程序的特殊 Google 帐户，而不是使用个人最终用户帐户。 服务帐户必须采用授权访问 Google API 并允许其查询 Google Cloud 项目中的虚拟机以获取虚拟机元数据的 IAM 策略（**Compute Engine** > **Compute Viewer**特权）。
服务帐户凭据	（仅适用于服务帐户）上传包含服务帐户凭据的 JSON 文件。该文件允许防火墙对实例进行身份验证并授权访问元数据。 您可以在 Google Cloud 控制台创建帐户（**IAM & admin**（**IAM** 与管理员）> **Service Accounts**（服务帐户））。有关如何创建帐户、如何向帐户中添加密钥以及如何下载需要上传到防火墙的 JSON 文件的信息，请参阅 Google 文档。
项目 ID	输入唯一标识您要监控的 Google Cloud 项目的字母数字文本字符串。
区域名称	以字符串（长度最多为 63 个字符）形式输入区域信息。例如：`us-west1-a`。
更新间隔	指定防火墙从源检索信息的时间间隔（以秒为单位，范围为 60-1,200，默认为 60）。
超时	时间间隔（以小时为单位，默认为 2），在此时间后，如果主机无响应，则与受监控源的连接将关闭。 （可选）源中断时启用超时。到达指定限制时，如果源无法访问或无响应，防火墙将关闭与源的连接。如果源断开连接，则该项目中已注册的所有 IP 地址和标记都将从动态地址组中删除。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Troubleshooting（故障排除）

- **Device**（设备）> **Troubleshooting**（故障排除）
- **Panorama** > **Managed Devices**（受管设备）> **Troubleshooting**（故障排除）

在提交设备组或模板配置更改之前，测试 Web 界面的功能，以验证此更改是否未引入运行配置中的连接问题，以及您的策略是否正确允许或拒绝流量。

- 策略匹配测试
  - 安全策略匹配
  - QoS 策略匹配
  - 身份验证策略匹配
  - 解密/SSL 策略匹配
  - NAT 策略匹配
  - 基于策略的转发策略匹配
  - DoS 策略匹配
- 连接测试
  - 路由
  - 测试 Wildfire
  - 威胁库
  - Ping
  - 跟踪路由
  - 日志收集器连接性
  - 外部动态列表
  - 更新服务器
  - 测试云日志记录服务状态
  - 测试云 GP 服务状态

安全策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/VSYS)，指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。
到	选择流量目标区域。

© 2019 Palo Alto Networks, Inc.

字段	说明
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。
目标端口	输入流量前往的特定目标端口。
源用户	输入发起通信的用户。
协议	输入用于路由的 IP 协议。可以是 0 到 255。
显示首次允许规则之前的所有潜在匹配规则	启用此选项后，可显示首次匹配规则结果之前的所有潜在规则匹配。禁用（取消选中）以在测试结果中仅返回第一个匹配规则。
应用程序	选择要测试的应用程序流量。
类别	选择要测试的流量类别。
（仅限防火墙）检查 HIP 掩码	选中此选项可检查正在访问您网络的终端设备的安全状态。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。
	  • `Shared policy disabled on device`（设备上禁用共享策略）—设备上的 Panorama 设置不允许从 Panorama 推送策略。

QoS 策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。

© 2019 Palo Alto Networks, Inc.

字段	说明
到	选择流量目标区域。
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。
目标端口	输入流量前往的特定目标端口。
源用户	选择发起通信的用户。
协议	输入用于路由的 IP 协议。可以是 0 到 255。
应用程序	选择要测试的应用程序流量。
类别	选择要测试的流量类别。
代码点类型	选择要测试的代码点编码类型：
代码点值	指定代码点编码值： • **DSCP** — 0 到 63 • **ToS** — 0 到 7

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。
	  • `Shared policy disabled on device`（设备上禁用共享策略）—设备上的 Panorama 设置不允许从 Panorama 推送策略。

身份验证策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。

© 2019 Palo Alto Networks, Inc.

字段	说明
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。
到	选择流量目标区域。
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。
类别	选择要测试的流量类别。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。
	  • `Shared policy disabled on device`（设备上禁用共享策略）—设备上的 Panorama 设置不允许从 Panorama 推送策略。

解密/SSL 策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/VSYS)，指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。
到	选择流量目标区域。
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。

© 2019 Palo Alto Networks, Inc.

字段	说明
应用程序	选择要测试的应用程序流量。
类别	选择要测试的流量类别。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。

NAT 策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。
到	选择流量目标区域。
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。
源端口	输入发起流量的特定端口。
目标端口	输入流量前往的特定目标端口。
协议	输入用于路由的 IP 协议。可以是 0 到 255。
目标接口	输入流量前往的设备的目标接口。
HA 设备 ID	输入 HA 设备的 ID： • **0** — 主 HA 对等

© 2019 Palo Alto Networks, Inc.

字段	说明
	• **1** — 辅助 HA 对等

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。
	  • `Shared policy disabled on device`（设备上禁用共享策略）—设备上的 Panorama 设置不允许从 Panorama 推送策略。

基于策略的转发策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。
源接口	输入发起流量的设备接口。
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。
目标端口	输入流量前往的特定目标端口。
源用户	输入发起通信的用户。
协议	输入用于路由的 IP 协议。可以是 0 到 255。
应用程序	选择要测试的应用程序流量。
HA 设备 ID	HA 设备的 ID： • **0** — 主 HA 对等

© 2019 Palo Alto Networks, Inc.

字段	说明
	• **1** — 辅助 HA 对等

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。
	  • `Shared policy disabled on device`（设备上禁用共享策略）—设备上的 Panorama 设置不允许从 Panorama 推送策略。

DoS 策略匹配

字段	说明
测试配置	
选择测试	选择要执行的策略匹配测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
从	输入流量源区域。
到	选择流量目标区域。
源接口	输入发起流量的设备接口。
目标接口	输入流量前往的设备的目标接口。
源	输入流量源 IP 地址。
目标	输入流量目标 IP 地址。
目标端口	输入流量前往的特定目标端口。
源用户	输入发起通信的用户。
协议	输入用于路由的 IP 协议。可以是 0 到 255。
结果	选择以查看已执行测试的“结果详细信息”。

© 2019 Palo Alto Networks, Inc.

字段	说明

	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：Success（成功）或Failure（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • N/A（不适用）—测试不适合该设备。
	  • Device not connected（设备未连接）—设备连接已断开。

路由

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
FiB 查找，Mfib 查找	选择以下查找之一： • **FiB** — 在激活路由表中执行路由查找 • **Mfib** — 在激活路由表中执行多播路由查找
目标 Ip	输入流量前往的 IP 地址。
虚拟路由器	执行路由测试的特定虚拟路由器。从下拉列表中选择虚拟路由器。
ECMP	
源 IP	输入发起通信的特定 IP 地址。
源端口	输入发起通信的特定端口。
目标 Ip	输入流量前往的特定 IP 地址。
目标端口	输入流量前往的特定目标端口。
结果	选择以查看已执行测试的“结果详细信息”。 （仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息： • 设备组 — 正在处理流量的防火墙所属的设备组名称。 • 防火墙 — 正在处理流量的防火墙名称。 • 状态 — 显示测试的状态：Success（成功）或Failure（失败）。 • 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：

© 2019 Palo Alto Networks, Inc.

字段	说明
	• N/A（不适用）—测试不适合该设备。 • Device not connected（设备未连接）—设备连接已断开。

测试 Wildfire

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/VSYS），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
渠道	选择 WildFire 通道：**Public** 或 **Private**。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：Success（成功）或Failure（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • N/A（不适用）—测试不适合该设备。
	  • Device not connected（设备未连接）—设备连接已断开。

威胁库

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/VSYS），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
结果	选择以查看已执行测试的“结果详细信息”。 （仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息： • 设备组 — 正在处理流量的防火墙所属的设备组名称。 • 防火墙 — 正在处理流量的防火墙名称。

© 2019 Palo Alto Networks, Inc.

字段	说明

	• 状态 — 显示测试的状态：Success（成功）或Failure（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • N/A（不适用）—测试不适合该设备。
	  • Device not connected（设备未连接）—设备连接已断开。

Ping

仅运行 PAN-OS 9.0 或更高版本的防火墙支持 ping 故障排除测试。

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
绕过路由表，使用指定接口	启用此选项可绕过路由表并使用自动接口禁用（取消选中）此选项可测试已配置的路由表。
计数	输入要发送的请求数。默认计数是 5。
请勿切碎回显请求数据包 (IPv4)	启用此选项后，不会切碎测试用的回显请求数据包。禁用
强制到 IPv6 目标	启用对 IPv6 目标的强制测试。
间隔	指定请求之间的间隔，以秒为单位（范围为 1 至 2,000,000,000）
源	输入回显请求的源地址。
请勿象征性地打印地址	启用此选项可在测试结果中显示 IP 地址，且不会解析 IP 地址主机名。禁用（取消选中）可解析 IP 地址主机名。
模式	指定十六进制填充模式。
大小	输入请求数据包的大小，以字节为单位（范围为 0 至 65468）。
Tos	输入 IP 服务类型值（范围为 1 至 255）。
TTL	输入跃点的 IP 在线时间值，即 IPv6 跃点限制值（范围为 1 至 255）。
显示详细输出	启用以显示测试结果的详细输出
主机	输入远程主机的主机名或 IP 地址。
结果	选择以查看已执行测试的“结果详细信息”。

© 2019 Palo Alto Networks, Inc.

字段	说明

	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：Success（成功）或Failure（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • N/A（不适用）—测试不适合该设备。
	  • Device not connected（设备未连接）—设备连接已断开。

跟踪路由

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/VSYS)，指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
使用 IPv4	启用此选项可使用选中设备的 IPv4 地址。
使用 IPv6	启用此选项可使用选中设备的 IPv6 地址。
第一个 TTL	输入在第一个传出探测数据包中使用的在线时间值（范围为 1 至 255）。
最大 TTL	输入最大在线时间值跃点（范围为 1 至 255）。
端口	输入探测中的基本端口号。
Tos	输入 IP 服务类型值（范围为 1 至 255）。
等待	输入等待响应的秒数（范围为 1 至 99,999）。
暂停	输入探测之间暂停的时间，以毫米为单位（范围为 1 至 2,000,000,000）。
设置“不要分段”位	启用此选项后，如果路径不支持已配置的最大传输单元(MTU)，则不得将 ICMP 数据包分为多个数据包。
启用套接字级别调试	启用此选项后，您可以对套接字级别进行调试。
网关	最多指定 8 个松散源路由网关。
请勿象征性地打印地址	启用此选项可在测试结果中显示 IP 地址，且不会解析 IP 地址主机名。禁用（取消选中）可解析 IP 地址主机名。

© 2019 Palo Alto Networks, Inc.

字段	说明
绕过路由表，并直接将其发送到主机	启用此选项后，可以绕过任何已配置的路由表，并直接与主机进行测试。
源	输入传出探测数据包内的源地址。
主机	输入远程主机的主机名或 IP 地址。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：Success（成功）或Failure（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • N/A（不适用）—测试不适合该设备。
	  • Device not connected（设备未连接）—设备连接已断开。

日志收集器连接性

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出已选中进行测试的设备和虚拟系统。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：Success（成功）或Failure（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • N/A（不适用）—测试不适合该设备。
	  • Device not connected（设备未连接）—设备连接已断开。

© 2019 Palo Alto Networks, Inc.

外部动态列表

字段	说明
选择测试	选择要执行的连接测试。
（仅限 Panorama）选择设备	**Select device/VSYS**（选择设备/**VSYS**），指定测试其策略功能的设备和虚拟系统。根据访问域，管理员和设备组&“模板”用户与设备和虚拟系统一同显示。此外，您可以选择 Panorama 管理服务器作为设备。
（仅限 Panorama）选中设备	列出选中进行测试的设备和虚拟系统。
URL 测试	指定测试此连接的 URL。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。

更新服务器

字段	说明
选择测试	选择要执行的连接测试。

结果	选择以查看已执行测试的“结果详细信息”。
	（仅限 Panorama）对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息：
	• 设备组 — 正在处理流量的防火墙所属的设备组名称。
	• 防火墙 — 正在处理流量的防火墙名称。
	• 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。
	• 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：
	  • `N/A`（不适用）—测试不适合该设备。
	  • `Device not connected`（设备未连接）—设备连接已断开。

测试云日志记录服务状态

测试用作服务的云日志记录连接状态。此测试仅适用于安装运行云服务插件版本 1.3 或更高版本的 Panorama 管理服务器。

© 2019 Palo Alto Networks, Inc.

字段	说明
选择测试	选择要执行的连接测试。
结果	选择以查看已执行测试的“结果详细信息”。 对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息： • 设备组 — 正在处理流量的防火墙所属的设备组名称。 • 防火墙 — 正在处理流量的防火墙名称。 • 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。 • 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：

测试云 GP 服务状态

测试用作服务的 GlobalProtect 连接状态。此测试仅适用于安装运行云服务插件版本 1.3 或更高版本的 Panorama 管理服务器。

字段	说明
选择测试	选择要执行的连接测试。
结果	选择以查看已执行测试的“结果详细信息”。 对多个受管设备进行测试时，“结果”将显示每个已测试设备的下列信息： • 设备组 — 正在处理流量的防火墙所属的设备组名称。 • 防火墙 — 正在处理流量的防火墙名称。 • 状态 — 显示测试的状态：`Success`（成功）或`Failure`（失败）。 • 结果 — 显示测试结果。如果无法执行测试，则会显示以下其中一项：

© 2019 Palo Alto Networks, Inc.

Device（设备）> Virtual Systems（虚拟系统）

虚拟系统 (vsys) 是可以在物理防火墙内单独管理的独立（虚拟）防火墙实例。每个虚拟系统都可以作为带有其自身安全策略、接口和管理员的独立防火墙；虚拟系统允许您分段管理防火墙提供的所有策略、报告和可视性功能。

例如，如果要为与财务部门关联的通信自定义安全功能，您可以定义财务虚拟系统，然后定义仅与该部门有关的安全策略。要优化策略管理，可以在创建允许访问个别虚拟系统的虚拟系统管理员帐户时，针对整个防火墙和网络功能分别维护管理员帐户。这使得财务部门中的虚拟系统管理员可以仅管理用于该部门的安全策略。

网络功能（如静态和动态路由、接口的 IP 地址以及 IPSec 隧道）与整个防火墙及其所有虚拟系统有关。虚拟系统配置（**Device**（设备）> **Virtual Systems**（虚拟系统））并不会控制防火墙级别和网络级别功能（如静态和动态路由、接口的 IP 地址、IPSec 隧道、VLAN、虚拟线路、虚拟路由器、GRE 隧道、DHCP、DNS 代理、QoS、LLDP 或网络配置文件）。对于每个虚拟系统，您可以指定一组物理和逻辑防火墙接口（包括 VLAN 和 Virtual Wire）以及安全区域。如果需要对各个虚拟系统进行路由分割，必须创建并分配其他虚拟路由器，并根据需要分配接口、VLAN 和虚拟线路。

如果使用 Panorama 模板定义虚拟系统，可以将一个虚拟系统配置为默认虚拟系统。默认虚拟系统和多虚拟系统功能将确定防火墙在提交模板时是否接受虚拟系统特定配置：

- 启用了多虚拟系统功能的防火墙接受在模板中定义的任何虚拟系统的虚拟系统特定配置。
- 未启用多虚拟系统功能的防火墙仅接受默认虚拟系统的虚拟系统特定配置。如果未配置默认虚拟系统，则这些防火墙将不接受虚拟系统特定配置。

PA-3200 系列、*PA-5200* 系列及 *PA-7000* 系列防火墙可以支持多个虚拟系统。但是，*PA-3200* 系列防火墙需要许可证才能启用多个虚拟系统。*PA-220* 和 *PA-800* 系列防火墙不支持多个虚拟系统。

在启用多个虚拟系统之前，请考虑以下事项：

- 虚拟系统管理员可为所分配的每个虚拟系统创建和管理安全策略所需的所有项目。
- 区域是虚拟系统中的对象。在定义策略或策略对象之前，从 **Policies**（策略）或 **Objects**（对象）选项卡的下拉列表中选择合适的 **Virtual System**（虚拟系统）。
- 您可以将可用的远程日志记录目标（SNMP、syslog 和电子邮件）、应用程序、服务和配置文件设置为所有虚拟系统（共享）或单个虚拟系统。
- 如果您有多个虚拟系统，则可以选择虚拟系统作为 User-ID 中心，以在虚拟系统之间共享 IP 地址到用户名映射信息。
- 可以配置全局（为防火墙上的所有虚拟系统）或虚拟系统特定服务路由（Device（设备）> Setup（设置）> Services（服务））。
- 您只能在本地防火墙上重命名虚拟系统。无法在 Panorama 上重命名虚拟系统。如果您在 Panorama 上重命名虚拟系统，您将创建一个全新的虚拟系统，或者新的虚拟系统名称可能会映射到防火墙上的错误虚拟系统。

定义虚拟系统之前，您必须首先启用防火墙上的多虚拟系统功能。选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），编辑 **General Settings**（常规设置），选择 **Multi Virtual System Capability**（多虚拟系统功能），然后单击 **OK**（确定）。这会添加 **Device**（设备）> **Virtual Systems**（虚拟系统）页面。选择该页面，**Add**（添加）虚拟系统，并指定以下信息。

虚拟系统设置	说明
ID	输入虚拟系统的整数标识符。有关支持的虚拟系统数量的信息，请参阅防火墙型号的数据表。

© 2019 Palo Alto Networks, Inc.

虚拟系统设置	说明
	如果使用 *Panorama* 模板配置虚拟系统，则此字段不会显示。
姓名	输入用于标识虚拟系统的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。 如果使用 *Panorama* 模板推送虚拟系统配置，则模板中的虚拟系统名称必须与防火墙上的虚拟系统名称相匹配。
允许转发解密内容	选择此选项，可以让虚拟系统在端口镜像或发送 WildFire 文件进行分析时将解密的内容转发到外部服务。另请参阅解密端口镜像。
“常规”选项卡	如果要将 DNS 代理规则应用至此虚拟系统，请选择 **DNS Proxy**（**DNS** 代理）对象。（Network（网络）> DNS Proxy（DNS 代理））。 要包括特定类型的对象，请选择该类型（接口、VLAN、虚拟线路、虚拟路由器或可见虚拟系统），**Add**（添加）对象，然后从下拉列表中选择对象。可以添加一个或多个任何类型的对象。要删除对象，选择该对象，然后单击 **Delete**（删除）。
资源选项卡	指定此虚拟系统允许的以下资源限制。每个字段显示值的有效范围，该值因防火墙型号而异。默认设值为 0，表示虚拟系统的限制是防火墙型号的限制。但是，对于每个虚拟系统而言，特定设置的限制不能复制。例如，如果防火墙有 4 个虚拟系统，则每个虚拟系统不能具有每个防火墙允许的解密规则总数。在所有虚拟系统的解密规则总数达到防火墙限制后，您无法再继续添加。 • **Sessions Limit**（会话限制）— 最大会话数。 如果使用 `show session meter` *CLI* 命令，防火墙将显示每个数据平面允许的最大会话数、虚拟系统正在使用的当前会话数，以及每个虚拟系统的会话调节次数。在 *PA-5200* 系列和 *PA-7000* 系列防火墙上，因为每个虚拟系统有多个数据平面，当前使用的会话数可能会大于配置的最大会话限制。*PA-5200* 系列或 *PA-7000* 系列防火墙上配置的会话限制依据每个数据平面而定，将导致每个虚拟系统较高的最大值。 • **Security Rules**（安全规则）— 最大安全规则数。 • **NAT Rules**（**NAT** 规则）— 最大 NAT 规则数。 • **Decryption Rules**（解密规则）— 最大解密规则数。 • **QoS Rules**（**QoS** 规则）— 最大 QoS 规则数。 • **Application Override Rules**（应用程序替代规则）— 最大应用程序替代规则数。 • **Policy Based Forwarding Rules**（基于策略的转发规则）— 最大基于策略的转发 (PBF) 规则数。 • **DoS Protection Rules**（**DoS** 保护规则）— 最大拒绝服务 (DoS) 规则数。 • **Site to Site VPN Tunnels**（站点到站点 **VPN** 隧道）— 最大站点到站点 VPN 隧道数。 • **Concurrent GlobalProtect Tunnels**（并发 **GlobalProtect** 隧道）— 最大并发远程 GlobalProtect 用户数。 • **Inter-Vsys User-ID Data Sharing**（**Inter-Vsys User-ID** 数据共享）—**Make this vsys a User-ID data hub**（使此虚拟系统成为 **User-ID** 数据中心）以允

© 2019 Palo Alto Networks, Inc.

虚拟系统设置	说明
	许防火墙上所有其他虚拟系统访问共享用户映射信息或**Change hub**（更改中心），并选择新的虚拟系统以将此虚拟系统重新分配为 User-ID 数据中心.需要超级用户或管理员权限.

© 2019 Palo Alto Networks, Inc.

Device（设备）> Shared Gateways（共享网关）

共享网关允许多个虚拟系统共同使用一个接口进行外部通信（通常连接到一般上行网络，如互联网服务供应商）。所有虚拟系统都使用一个 IP 地址通过物理接口与外界通信。单个虚拟路由器用于通过共享网关路为所有虚拟系统路由通信。

共享网关使用第 3 层接口，因此必须至少配置一个第 3 层接口作为共享网关。通信起源于一个虚拟系统，并且通过共享网关退出防火墙，因此需要类似的策略在两个虚拟系统之间传递通信。您可以配置“外部 vsys”区域，以在虚拟系统中定义安全规则。

共享网关设置	说明
ID	网关标识符（不能由防火墙使用）。
姓名	输入共享网关的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。仅名称是必需的。
DNS 代理	（可选）如果配置了 DNS 代理，请选择要用于域名查询的 DNS 服务器。
接口	选择共享网关将使用的接口。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）

- Device（设备）> Certificate Management（证书管理）> Certificates（证书）
- Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）
- Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者）
- Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）
- Device（设备）> Certificate Management（证书管理）> SCEP
- Device（设备）> Certificate Management（证书管理）> SSL Decryption Exclusion（SSL 解密排除）
- Device（设备）> Certificate Management（证书管理）> SSH Service Profile（SSH 服务配置文件）

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> Certificates（证书）

选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）可管理（生成、导入、续订、删除和吊销）证书，以便保护网络通信。您还可以导出和导入用于保护网络上高可用性对端之间连接的高可用性 (HA) 密钥。选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Default Trusted Certificate Authorities**（默认可信证书授权机构）可查看、启用和禁用防火墙信任的证书授权机构 (CA)。

有关如何在防火墙或 *Panorama* 上实施证书的更多信息，请参阅证书管理。

- 管理防火墙和 Panorama 证书
- 管理默认可信证书授权机构
- Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）
- Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者）
- Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）
- Device（设备）> Certificate Management（证书管理）> SCEP
- Device（设备）> Master Key and Diagnostics（主密钥和诊断）

管理防火墙和 Panorama 证书

- Device（设备）> Certificate Management（证书管理）> Certificates（证书）> Device Certificates（设备证书）
- Panorama > 证书管理 > 证书

选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）或 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）可显示防火墙或 Panorama 用于保护 Web 界面访问、SSL 解密或 LSVPN 等任务的证书。

以下是一部分适用于证书的设置：在生成证书后，定义证书的使用（请参阅 管理默认可信证书授权机构）。

- **Forward Trust**（转发信任）— 如果对服务器证书进行签名的证书授权机构 (CA) 在防火墙的信任 CA 列表中，则防火墙将使用此证书来对其在 SSL 转发代理解密期间为客户端提供的服务器证书副本进行签名。
- **Forward Untrust**（转发不信任）— 如果对服务器证书进行签名的证书授权机构 (CA) 不在防火墙的信任 CA 列表中，则防火墙将使用此证书来对其在 SSL 转发代理解密期间为客户端提供的服务器证书副本进行签名。
- **Trusted Root CA**（可信根 **CA**）— 对于 SSL 转发代理解密、GlobalProtect、URL 管理替代和身份验证门户，防火墙会将此证书用作可信任的 CA。防火墙具有现有可信 CA 的大型列表。可信根 CA 证书针对的是企业信任的其他 CA，但不属于预安装信任列表的一部分。
- **SSL Exclude**（**SSL** 排除）— 如果您已配置解密例外以从 SSL/TLS 解密中排除特定的服务器，则防火墙将使用此证书。
- **Certificate for Secure Syslog**（安全系统日志的证书）— 防火墙将使用此证书以确保以系统日志消息的形式发送日志到 Syslog 服务器。

要生成证书，请单击 Generate（生成）并指定以下字段：

© 2019 Palo Alto Networks, Inc.

生成证书后，页面显示管理证书的其他支持操作。

用来生成证书的设置	说明
证书类型	选择生成证书的实体： **Local**（本地）— 防火墙或 Panorama 生成证书。 **SCEP** — 简单证书注册协议 (SCEP) 服务器生成证书，并将其发送到防火墙或 Panorama。
证书名称	（必填）输入用于识别证书的名称（在防火墙上最多可包含 63 个字符，或在 Panorama 上最多可包含 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
SCEP 配置文件	（仅限 SCEP 证书）选择 **SCEP Profile**（**SCEP** 配置文件）可定义防火墙或 Panorama 与 SCEP 服务器进行通信的方式，并定义 SCEP 证书的设置。有关详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> SCEP。您可以配置用作 GlobalProtect 门户的防火墙，以便根据需要请求 SCEP 证书并自动将证书部署到端点。 Generate Certificate（生成证书）对话框中的其余字段不适用于 SCEP 证书。指定 **Certificate Name**（证书名称）和 **SCEP Profile**（**SCEP** 配置文件）后，单击 **Generate**（生成）。
常见名称	（必要）输入将显示在证书上的 IP 地址或 FQDN。
共享	在拥有多个虚拟系统 (vsys) 的防火墙上，如果您希望证书可用于每个虚拟系统，请选中 **Shared**（共享）。
签名者	要对证书进行签名，可以使用导入防火墙的证书颁发机构 (CA) 证书。在防火墙为 CA 的情况下，证书也可以是自签名证书。如果使用的是 Panorama，则还可以选择为 Panorama 生成自签名证书。 如果您已导入证书颁发机构证书或在防火墙上对任何证书进行签名（自签名），则下拉列表将包含可用于对所创建证书进行签名的证书颁发机构。 要生成证书签名请求 (CSR)，请选择外部颁发机构 **(CSR)**。在防火墙生成证书和密钥对后，可以导出 CSR 并将其发送到 CA 进行签名。
证书授权机构	如果您希望防火墙颁发证书，请选中此选项。 将此证书标记为 CA 可让您对防火墙中的其他证书进行签名。
阻止私钥导出	生成证书后，可勾选此选项以阻止包括超级用户在内的所有管理员导出私钥。
OCSP 响应者	从下拉列表中选择 OCSP 响应者配置文件（请参阅 Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者））。相应的主机名会显示在证书中。
算法	选择证书的密钥生成算法：**RSA** 或椭圆曲线 **DSA** (ECDSA)。 ECDSA 使用的密钥大小比 RSA 算法更小，因此可以提供处理 SSL/TLS 连接的性能增强功能。此外，ECDSA 还可以提供相当于或高于 RSA 的安全性。建议将

© 2019 Palo Alto Networks, Inc.

用来生成证书的设置	说明
	ECDSA 用于客户端浏览器和操作系统，但可能会要求您选择 RSA 才能与传统浏览器和操作系统兼容。 运行 *PAN-OS 6.1* 或之前版本的防火墙将会删除从 *Panorama* 推送的所有 *ECDSA* 证书，并且在这些防火墙上由 *ECDSA* 证书授权机构 *(CA)* 签发的所有 *RSA* 证书都将无效。 不能使用硬件安全模块 (HSM) 存储用于 SSL 转发代理或入站检测解密的专用 ECDSA 密钥。
位数	选择证书的密钥长度。 如果防火墙处于 FIPS-CC 模式且密钥生成 **Algorithm**（算法）为 **RSA**，则生成的 RSA 密钥必须为 **2048** 或 **3027** 位。如果算法为椭圆曲线 **DSA**，可以使用两个密钥长度选项（**256** 和 **384**）。
摘要	选择证书的摘要算法。可用选项取决于密钥生成算法： • **RSA — MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512** • 椭圆曲线 **DSA — SHA256** 或 **SHA384** 如果防火墙处于 FIPS-CC 模式且密钥生成 **Algorithm**（算法）为 **RSA**，必须选择 **SHA256**、**SHA384** 或 **SHA512** 作为 **Digest**（摘要）算法。如果算法为椭圆曲线 **DSA**，则可以使用两个摘要算法（**SHA256** 和 **SHA384**）。 在请求依赖 *TLSv1.2*（如管理员访问 *Web* 界面）的防火墙服务时使用的客户端证书不能将 *SHA512* 作为摘要算法。客户端证书必须使用较低的摘要算法（如 *SHA384*），或在配置防火墙服务的 *SSL/TLS* 服务配置文件时必须将 *Max Version*（最高版本）限制为 *TLSv1.1*（请参阅 Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件））。
到期（天数）	指定证书有效的天数（默认为 365）。 如果在 *GlobalProtect* 卫星配置中指定有效期限，则该值将替代在此字段中输入的值。
证书属性	**Add**（添加）其他 **Certificate Attributes**（证书属性），可标识证书将颁发到的实体。您可以添加以下任意属性：**Country**（国家/地区）、**State**（州）、**Locality**（地点）、**Organization**（公司/组织）、**Department**（部门）和 **Email**（电子邮件）。此外，您可以指定以下“使用者备用名称”字段：主机名 (SubjectAltName:DNS)、**IP** (SubjectAltName:IP) 和 **Alt** 电子邮件 (SubjectAltName:email)。 要将国家/地区添加为证书属性，请从类型列中选择国家/地区，然后单击值列查看 *ISO 6366* 国家/地区代码。

如果已配置硬件安全模块 *(HSM)*，则私钥存储在外部 *HSM* 存储设备上，而不是存储在防火墙中。

© 2019 Palo Alto Networks, Inc.

管理证书的其他支持操作

在生成证书后，页面上将显示证书详细信息，并提供以下操作：

管理证书的其他支持操作	说明
删除	选择证书，然后单击 **Delete**（删除）可删除证书。 如果防火墙有解密策略，则您无法删除用法已设为 *Forward Trust Certificate*（转发信任证书）或 *Forward Untrust Certificate*（转发不信任证书）的证书。要更改证书用法，请参阅管理默认可信证书颁发机构。
吊销	选择要吊销的证书，然后单击吊销。证书将立即设置为已吊销状态。不需要进行任何提交。
续订	如果证书到期或即将到期，请选择对应的证书并单击续订。设置证书的有效期限（以天为单位），然后单击确定。 如果防火墙是签发证书的 CA，则防火墙将它替换为拥有不同序列号的新证书，但属性与旧证书相同。 如果外部证书颁发机构 (CA) 签发证书，且防火墙使用在线证书状态协议 (OCSP) 验证证书吊销状态，则防火墙使用 OCSP 响应者信息更新证书状态
导入	导入证书，然后按照以下说明进行配置： • 输入标识证书的证书名称。 • 浏览到证书文件。如果导入 **PKCS12** 证书和私钥，则两者均包含在单个文件中。如果导入 **PEM** 证书，则文件将仅包含证书。 • 选择证书的文件格式。 • 如果 HSM 存储此证书的密钥，请选中 **Private key resides on Hardware Security Module**（硬件安全模块上的私钥）。有关 HSM 的详细信息，请参阅 Device（设备）> Setup（设置）> HSM。 • 根据需要**Import Private Key**（导入私钥）（仅限 PEM 格式）。如果选择 **PKCS12** 作为证书的 **File Format**（文件格式），则所选 **Certificate File**（证书文件）包含密钥。如果选择 **PEM** 格式，请浏览到加密私钥文件（通常命名为 *.key）。对于上述两种格式，请输入密码和确认密码。 一旦导入证书并选择 **Import Private Key**（导入私钥），请选择**Block Private Key Export**（阻止私钥导出）以阻止包括超级用户在内的任何管理员导出私钥。 在将证书导入处于 *FIPS-CC* 模式的 *Palo Alto Networks* 防火墙或 *Panorama* 服务器时，必须将证书导入为 *Base64* 编码证书 *(PEM)*，并且必须使用 *AES* 对私钥加密。此外，还必须使用 *SHA1* 作为基于密码的密钥派生方法。 要导入 PKCS12 证书，请将证书转换为 PEM 格式（使用 OpenSSL 等工具）；请确保转换过程中所使用的密码至少包含 6 个字符。
导出	选择要导出的证书，单击 **Export**（导出），然后选择文件格式： • Encrypted Private Key and Certificate (PKCS12)（加密私钥和证书 (PKCS12)）— 导出文件将包含证书和私钥。

© 2019 Palo Alto Networks, Inc.

管理证书的其他支持操作	说明
	• Base64 Encoded Certificate (PEM)（Base64 编码证书 (PEM)）— 如果想要同时导出私钥，请选择 Export Private Key（导出私钥），然后输入密码和确认密码。 • 二进制编码证书 (DER)）— 仅可导出此证书，而无法导出密钥：忽略导出私钥和密码字段。
导入 HA 密钥	HA 密钥必须在两个防火墙对等之间交换；即必须将防火墙 1 的密钥导出，然后将其导入到防火墙 2 中，然后逆向执行此操作。 要导入高可用性 (HA) 的密钥，请单击 **Import HA Key**（导入 **HA** 密钥）和 **Browse**（浏览）以指定要导入的密钥文件。 要导出 HA 的密钥，请单击导出 **HA** 密钥，然后指定保存文件的位置。
导出 HA 密钥	
定义证书用法	在 Name（名称）列中选择证书，然后选中适用于预计证书使用要求的选项。
PDF/CSV	具有最小只读访问权限的管理角色可以将受管证书配置表格导出为 **PDF/CSV**。您可以应用筛选程序来创建更多特定的表格配置输出，以用于审计等事宜。将仅导出 Web 界面中所显示的列。请参阅配置表格导出。

管理默认可信证书授权机构

- Device（设备）> Certificate Management（证书管理）> Certificates（证书）> Default Trusted Certificate Authorities（默认可信证书授权机构）

此页面用于查看、禁用或导出防火墙信任的预先包含的证书颁发机构 (CA)。预先安装的 CA 列表包括负责颁发防火墙确保与互联网连接所需的证书的最常见可信证书提供商。将为每个可信根 CA 显示名称、使用者、颁发者、到期日期和验证状态。

默认情况下，防火墙不信任中间 CA，因为中间 CA 不是防火墙和可信根 CA 之间的信任链的一部分。您必须手动添加您希望防火墙信任的任何中间 CA 以及您的组织要求的任何其他可信企业 CA（**Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书））。

可信证书颁发机构设置	说明
启用	如果已禁用 CA，则可以将其重新 **Enable**（启用）。
禁用	选择 CA 并将其 **Disable**（禁用）。只有在信任特定 CA，或要禁用所有其他 CA 而仅信任本地 CA 时才可使用此选项。
导出	选中并 **Export**（导出）CA 证书。您可以导入其他系统或脱机查看证书。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）

- **Device**（设备）> **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）
- **Panorama** > **Certificate Management**（证书管理）> **Certificate Profile**（证书配置文件）

证书配置文件定义要用于验证客户端证书、验证证书吊销状态的方法和状态限制访问的方式的证书颁发机构 (CA) 证书。您可以在为身份验证门户、GlobalProtect、站点到站点 IPSec VPN、动态 DNS (DDNS) 和防火墙/Panorama Web 界面访问配置证书身份验证时选择配置文件。可以为这些服务的每个服务配置单独的证书配置文件。

证书配置文件设置	说明
姓名	（必填）输入用于识别配置文件的名称（在防火墙上最多 63 个字符，或在 Panorama 上最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
用户名字段	如果 GlobalProtect 仅使用证书进行门户和网关身份验证，则 PAN-OS 软件会使用您在 **Username Field**（用户名字段）下拉列表中选择的证书字段作为用户名，并将其与 User-ID 服务的 IP 地址进行匹配： • **Subject**（主题）— 公用名称。 • **Subject Alt**（主题备选）— 电子邮件或主体名称。 • **None**（无）— 通常用于 GlobalProtect 设备或预登录身份验证。
域	输入 NetBIOS 域，这样 PAN-OS 软件就能通过 User-ID 映射用户。
CA 证书	（必要）**Add**（添加）**CA Certificate**（**CA** 证书）以分配配置文件。 （可选）如果防火墙使用在线证书状态协议 (OCSP) 验证证书吊销状态，可配置以下字段覆盖默认行为。对于大多数部署，这些字段不适用。 • 默认情况下，防火墙使用证书的授权信息访问(AIA)信息提取 OCSP 响应者信息。要替代 AIA 信息，请输入 **Default OCSP URL**（默认 **OCSP URL**）（以 `http://` 或 `https://` 为开头）。 • 默认情况下，防火墙使用在 **CA** 证书字段中选择的证书验证 OCSP 响应者。要使用不同的证书进行验证，可在 **OCSP** 验证 **CA** 证书字段中进行选择。 此外，输入 **Template Name**（模板名称）以标识用于签名证书的模板。
使用 CRL	选中此选项可使用证书吊销列表 (CRL) 来验证证书的吊销状态。
使用 OCSP	选中此选项可使用 OCSP 来验证证书的吊销状态。

© 2019 Palo Alto Networks, Inc.

证书配置文件设置	说明
	如果同时选择 *OCSP* 和 *CRL*，则防火墙首先尝试使用 *OCSP*，并且只有在 *OCSP* 响应者不可用时返回来使用 *CRL* 方法。
Crl 接收超时	指定防火墙在过后将停止等待 CRL 服务响应的时间间隔（1 至 60 秒）。
Ocsp 接收超时	指定防火墙在过后将停止等待 OCSP 响应者响应的时间间隔（1 至 60 秒）。
证书状态超时	指定防火墙在过后将停止等待任何证书状态服务响应并应用您定义的所有会话阻止逻辑的时间间隔（1 至 60 秒）。
如果证书状态未知，则阻止会话	如果您希望防火墙在 OCSP 或 CRL 服务返回未知证书吊销状态时阻止会话，请选择此选项。否则，防火墙会继续进行会话。
如果无法在超时时间内检索到证书状态，则阻止会话	如果您希望防火墙在注册 OCSP 或 CRL 请求超时后阻止会话，请选择此选项。否则，防火墙会继续进行会话。
如果证书未发送至执行身份验证的设备，则阻止会话	（仅限 GlobalProtect）如果您希望防火墙在客户端证书主题中包含的序列号属性与 GlobalProtect 代理为客户机端点报告的主机 ID 不匹配时阻止会话，请选则此选项。否则，防火墙会允许会话。此选项仅适用于 GlobalProtect 证书身份验证。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> OCSP Responder（OCSP 响应者）

选择 **Device**（设备）> **Certificate Management**（证书管理）> **OCSP Responder**（**OCSP** 响应者）可定义联机证书状态协议 (OCSP) 响应者（服务器），以验证证书的吊销状态。

除了添加 OCSP 响应者之外，启用 OCSP 时还需要执行以下任务：

- 启用防火墙和 OCSP 服务器之间的通信：选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），在 Management Interface Settings（管理接口设置）中选择 **HTTP OCSP**，然后单击 **OK**（确定）。
- 如果防火墙将解密出站 SSL/TLS 通信，则可以选择将其配置为验证目标服务器证书的吊销状态：选择 **Device**（设备）> **Setup**（设置）> **Sessions**（会话），单击 **Decryption Certificate Revocation Settings**（解密证书吊销设置），在 OCSP 设置中选择 **Enable**（启用），输入 **Receive Timeout**（接收超时）（防火墙在此时间过后将停止等待 OCSP 响应的时间间隔），然后单击 **OK**（确定）。
- （可选）要配置防火墙作为 OCSP 响应者，可将接口管理配置文件添加到 OCSP 服务使用的接口。首先，选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Interface Mgmt**（接口管理），单击 **Add**（添加），选择 **HTTP OCSP**，然后单击 **OK**（确定）。其次，选择**Network**（网络）> **Interfaces**（接口），单击将被防火墙用于 OCSP 服务的接口的名称，选择**Advanced**（高级）> **Other info**（其他信息），选择您已配置的接口管理配置文件，然后单击 **OK**（确定）和 **Commit**（提交）。

启用 *OCSP* 响应者，这样，如果证书被吊销，会通知您采取适当的操作来建立到门户和网关的安全连接。

OCSP 响应者设置	说明
姓名	输入名称以标识响应者（最多 31 个字符）。名称区分大小写。它必须是唯一且只能使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用响应者的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择位置；其值预定义为共享。在保存响应者后，您无法更改其位置。
主机名	输入 OCSP 响应者的主机名（推荐）或 IP 地址。根据此值，PAN-OS 自动派生一个 URL，并将其添加到正在验证的证书。如果将防火墙配置作为 OCSP 响应者，则主机名必须在防火墙用于 OCSP 服务的接口中解析 IP 地址。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）

- Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）
- Panorama > Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）

SSL/TLS 服务配置文件可指定使用 SSL/TLS（如 Web 界面的管理访问权限）的防火墙或 Panorama 服务的证书和协议版本或版本范围。通过定义协议版本，配置文件可让您限制用来与请求服务的客户端系统进行安全通信的密码套件。

在请求防火墙或 *Panorama* 服务的客户端系统中，证书信任列表 *(CTL)* 必须包括颁发在 *SSL/TLS* 服务配置文件中指定的证书的证书颁发机构 *(CA)* 证书。否则，用户在请求服务时会看到证书出错。客户端浏览器默认提供大多数第三方 *CA* 证书。如果企业或防火墙生成的 *CA* 证书是颁发者，则必须将该 *CA* 证书部署到客户端浏览器中的 *CTL*。

要添加配置文件，单击 **Add**（添加）并填写下表中的字段。

SSL/TLS 服务配置文件设置	说明
姓名	输入名称以标识配置文件（最多 31 个字符）。名称区分大小写。它必须是唯一且只能使用字母、数字、空格、连字符和下划线。
共享	如果防火墙拥有多个虚拟系统 (vsys)，选择此选项可使配置文件对所有虚拟系统均可用。默认情况下，未选择此选项，且配置文件仅适用于在 **Device**（设备）选项卡的 **Location**（位置）下拉列表中选择的虚拟系统。
证书	选择、导入或生成与配置文件相关联的服务器证书（请参阅管理防火墙和 Panorama 证书）。 请不要使用 *SSL/TLS* 服务的证书授权机构 *(CA)* 证书；只能使用签名的证书。
最小版本 最大版本	选择服务可以使用的最早（**Min Version**（最低版本））和最新（**Max Version**（最高版本））的 TLS 版本：**TLSv1.0**、**TLSv1.1**、**TLSv1.2**、**TLSv1.3**或 **Max**（最高）（最新可用版本）。 在运行 *PAN-OS 8.0* 或更高版本的 *FIPS/CC* 模式的防火墙上，*TLSv1.1* 是最早支持 *TLS* 的版本；请勿选择 *TLSv1.0*。 在请求依赖 *TLSv1.2* 的防火墙服务时使用的客户端证书不能将 *SHA512* 作为摘要算法。客户端证书必须使用较低的摘要算法（如 *SHA384*），或者您必须将服务的 *Max Version*（最高版本）限制为 *TLSv1.1*。

© 2019 Palo Alto Networks, Inc.

SSL/TLS 服务配置文件设置	说明
	使用您能提供的最强版本的协议，为您的网络提供最强安全性。如果可以，设置 *Min Version*（最低版本）为 *TLSv1.2* ，并设置 *Max Version*（最高版本）为 *Max*（最高）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> SCEP

简单证书注册协议 (SCEP) 提供用于为端点、网关和卫星设备签发唯一证书的机制。选择 **Device**（设备）> **Certificate Management**（证书管理）> **SCEP** 可创建 SCEP 配置。

有关如何创建 *SCEP* 配置文件的更多信息，请参阅使用 SCEP 部署证书。

要开始新的 SCEP 配置，请单击 **Add**（添加），然后填写以下字段：

SCEP 设置	说明
姓名	指定用于标识此 SCEP 配置的描述性名称，如 SCEP_*Example*。该名称用于区分此 SCEP 实例与配置文件中可能已存在的其他实例。
位置	如果系统具备多个虚拟系统，则请为配置文件选择一个位置。此位置表示可使用 SCEP 配置的位置。
一次性密码(挑战)	
SCEP 质询	（可选）要让基于 SCEP 的证书生成更安全，您可在公钥基础结构 (PKI) 与门户之间，为各证书请求配置 SCEP 质询-响应机制（一次性密码 (OTP)）。 配置此机制后，其操作不可见，您无需再进行任何输入操作。 您选择的质询机制确定了 OTP 的来源。如果选择 **Fixed**（固定），请从 PKI 的 SCEP 服务器复制注册质询密码，然后在配置为 **Fixed**（固定）时显示的门户 **Password**（密码）对话框中输入字符串。门户每次请求证书时，都会使用此密码通过 PKI 进行身份验证。如果选择 **Dynamic**（动态），请输入所选项的用户名和密码（可能是 PKI 管理员的凭据）以及门户-客户端提交这些凭据的 SCEP **Server URL**（服务器 **URL**）。此用户名和密码将保持不变，同时 SCEP 服务器会在发出每个证书请求后，以透明方式生成门户的 OTP 密码。（每次提出证书请求后，您可在 The enrollment challenge password is（注册质询密码为）字段所在屏幕刷新后发现此 OTP 更改。）PKI 会以透明方式将各新密码传到门户，然后门户可将此密码用于其证书请求。 为了符合《美国联邦信息处理标准 *(FIPS)*》，请选择 *Dynamic*（动态），指定使用 *HTTPS* 的 *Server URL*（服务器 *URL*），并启用 *SCEP Server SSL Authentication*（*SCEP* 服务器 *SSL* 身份验证）。（*FIPS-CC* 操作已在防火墙登录页面及防火墙状态栏中予以指明。）
配置	

© 2019 Palo Alto Networks, Inc.

SCEP 设置	说明
服务器 URL	输入门户从 SCEP 服务器请求并接收客户端证书的 URL。示例： `http://<hostname or IP>/certsrv/mscep/.`
CA-IDENT 名称	输入标识 SCEP 服务器的字符串。最长为 255 个字节。

主题	配置主题以包括有关设备和可选用户的标识信息，并向 SCEP 服务器提供证书签署请求 (CSR) 中的此信息。
	当用于为端点请求客户端证书时，端点将发送包含其主机 ID 值在内的设备相关标识信息。主机 ID 值视设备类型而定，为接口 (Mac) 的 GUID (Windows) MAC 地址、Android ID（Android 设备）、UDID（iOS 设备）或 GlobalProtect 分配的唯一名称 (Chrome)。当用于为卫星设备请求证书时，主机 ID 值为设备序列号。
	要在 CSR 中指定其他信息，请输入主题名称。该主题必须是格式为 *<attribute>=<value>* 的专有名称，且必须包含公用名 (CN) 键。例如：
	`O=acme,CN=acmescep`
	可以通过两种方法指定 CN：
	• （推荐）**Token-based Cn**（基于令牌的 **CN**）— 输入支持的令牌之一：**$USERNAME**、**$EMAILADDRESS** 或 **$HOSTID**。使用用户名或电子邮箱地址变量，以确保门户为特定用户请求证书。要仅为设备请求证书，请指定主机 ID 变量。当 GlobalProtect 门户将 SCEP 设置推送到代理时，将会使用证书所有者的实际值（用户名、主机 ID 或电子邮箱地址）替换主题名称的公用名 (CN) 部分。例如：
	`O=acme,CN=$HOSTID`
	• 静态 **CN** — 将指定要使用的 CN 作为 SCEP 服务器签发的所有证书的主题。例如：
	`O=acme,CN=acmescep`

主题备选名称类型	选择 **None**（无）之外的其他类型后，将显示对话框供您输入合适的值： • **RFC 822 Name**（**RFC 822** 名称）— 输入证书主题或“主题备选名称”扩展中的电子邮件名称。 • **DNS Name**（**DNS** 名称）— 输入用于评估证书的 DNS 名称。 • **Uniform Resource Identifier (URI)**（统一资源标识符 **(URI)**）— 输入客户端获取证书的 URI 源的名称。
加密设置	• **Number of Bits**（位数）— 选择证书的密钥 **Number of Bits**（位数）。如果防火墙处于 FIPS-CC 模式下，则生成的密钥至少要有 2,048 位。（FIPS-CC 操作已在防火墙登录页面及防火墙状态栏中予以指明。） • **Digest**（摘要）— 选择证书的 **Digest**（摘要）算法：**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。如果防火墙处于 FIPS-CC 模式，则必须选择 **SHA256**、**SHA384** 或 **SHA512** 作为 **Digest**（摘要）算法。

© 2019 Palo Alto Networks, Inc.

SCEP 设置	说明
Use as digital signature（用作数字签名）	选择此选项可配置端点使用证书中的私钥来验证数字签名。
Use for key encipherment（用于密钥加密）	选择此选项可配置客户端使用证书中的私钥，对通过 SCEP 服务器颁发的证书建立的 HTTPS 所交换的数据进行加密。
CA 证书指纹	（可选）为确保门户连接到正确的 SCEP 服务器，请输入 **CA Certificate Fingerprint**（**CA** 证书指纹）。该指纹可从 SCEP 服务器界面的 **Thumbprint**（指纹）字段中获取。 登录到 SCEP 服务器的管理用户界面（例如，http://<hostname or IP>/CertSrv/mscep_admin/）。复制指纹并将其输入 **CA Certificate Fingerprint**（**CA** 证书指纹）。
SCEP 服务器 SSL 身份验证	要启用 SSL，选择 SCEP 服务器的根 **CA Certificate**（**CA** 证书）。或者，您也可以通过选择 **Client Certificate**（客户端证书）在 SCEP 服务器和 GlobalProtect 门户之间启用相互 SSL 身份验证。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> SSL Decryption Exclusion（SSL 解密排除）

查看和管理 SSL 解密排除。可以使用两种类型的解密排除，即预定义解密排除和自定义解密排除：

- 预定义解密排除允许在防火墙将其解密以保持加密时可能中断应用程序和服务。Palo Alto Networks 定义了预定义解密排除，并定期提供预定义解密排除列表的更新和增添作为应用程序和威胁内容更新的一部分。默认启用预定义解密排除，但您可以根据需要选择禁用预定义解密排除。
- 您可以创建自定义解密排除以排除解密服务器流量。以目标服务器为源或目标地址的所有流量仍保持加密。

您还可以根据应用程序、源、目标、*URL* 类别和服务排除解密流量。

使用此页面上的设置可修改或添加解密排除并管理解密排除。

SSL 解密排除设置	说明
修改或 **Add**（添加）解密排除	
主机名	输入 **Hostname**（主机名）以定义自定义解密排除。防火墙将主机名与客户端请求的 SNI 或服务器证书中显示的 CN 进行比较。防火墙在解密时会排除服务器提供包含定义域的 CN 的会话。 您可以使用星号 (*) 作为通配符来创建用于多个域关联主机名的解密排除项。星号与插入符号 (^) 在用于 URL 类别异常时的行为方式相同 — 每个星号控制主机名中一个变量子域（标签）。这样，您既可以创建非常具体的排除，也可以创建非常笼统的排除。例如： • mail.*.com 与 mail.company.com 匹配，但不与 mail.company.sso.com 匹配。 • *.company.com 与 tools.company.com 匹配，但不与 eng.tools.company.com 匹配。 • *.*.company.com 与 eng.tools.company.com 匹配，但不与 eng.company.com 匹配。 • *.*.*.company.com 与 corp.exec.mail.company.com 匹配，但不与 corp.mail.company.com 匹配。 • mail.google.* 与 mail.google.com 匹配，但不与 mail.google.uk.com 匹配。 • mail.google.*.* 与 mail.google.co.uk 匹配，但不与 mail.google.com 匹配。 例如，要使用通配符从解密中排除 video-stats.video.google.com，而不是从解密中排除 video.google.com，请排除 *.*.google.com。 不管主机名之前的星号通配符数量是多少（主机名之前没有非通配符标签），主机名必须与条目匹配。例如，**.google.com*、**.*.google.com* 和 **.*.*.google.com* 全部都与 *google.com* 匹配。但是，**.dev.*.google.com* 不与 *google.com* 匹配，原因在于有一个标签 *(dev)* 不是通配符。

© 2019 Palo Alto Networks, Inc.

SSL 解密排除设置	说明
	主机名对于每个条目都应该是唯一的，如果将预定义条目传递到与现有自定义条目匹配的防火墙，则自定义条目优先。 无法编辑预定义解密排除的主机名。
共享	选择 **Shared**（共享）可在多个虚拟系统防火墙中的所有虚拟系统之间共享解密排除。 尽管默认共享预定义解密排除，但您仍可同时启用和禁用特定虚拟系统的预定义和自定义条目。
说明	（可选）介绍排除解密的应用程序，包括解密时应用程序中断的原因。
排除	排除解密应用程序。禁用此选项可开始解密先前排除解密的应用程序。
管理解密排除	
启用	**Enable**（启用）一个或多个条目以将其从解密中排除。
禁用	**Disable**（禁用）一个或多个预定义解密排除。 由于解密排除可标识在解密时中断的应用程序，因此禁用其中一个条目可能会导致应用程序不受支持。防火墙将尝试解密应用程序，并且应用程序将中断。如果要确保某些加密的应用程序不进入您的网络，可以使用此选项。
显示过期	**Show obsoletes**（显示过期）可查看 Palo Alto Networks 不再定义为解密排除的预定义条目。 有关过期条目的更多信息： 将预定义解密排除的更新（包括预定义条目的删除）传递给防火墙作为应用程序和威胁内容更新的一部分。当防火墙接收到不再包括该条目的内容更新时，启用 **Exclude from decryption**（排除解密）的预定义条目将自动从 SSL 解密排除列表中删除。 但是，即使在防火墙接收到不再包括该条目的内容更新后，禁用 **Exclude from decryption**（排除解密）的预定义条目仍保留在 SSL 解密列表中。选择 **Show obsoletes**（显示过期）后，目前将不会执行这些已禁用的预定义条目；可以根据需要手动删除这些条目。
显示本地排除缓存	**Show Local Exclusion Cache**（显示本地排除缓存）显示防火墙出于预防解密等技术原因（例如，固定证书、客户端身份验证或不受支持的密码）从解密中排除的站点。本地 SSL 解密缓存不同于 SSL 解密排除列表（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除）），该列表包括防止 Palo Alto Networks 已识别解密的站点，且您还可以将选择添加的永久解密排除添加到该列表中。 防火墙将根据与用于控制流量的解密策略规则关联的解密配置文件设置，采用本地检测到的解密例外填充本地 SSL 解密缓存。 排除站点会在本地缓存中保留 12 小时，然后将过期。每个排除条目都包含如下信息：应用程序、服务器、防火墙自动从解密中排除站点的原因、应用至流量的解密配置文件以及 Vsys。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Certificate Management（证书管理）> SSH Service Profile（SSH 服务配置文件）

您可以通过 SSH 服务配置文件，限制用于加密和保护数据完整性的密码、密钥交换和消息认证码算法。具体而言，这些配置文件可在命令行接口 (CLI) 与网络上管理连接和高可用性 (HA) 设备之间出现 SSH 会话时，加强数据保护。此外，您还可以生成新的 SSH 主机密钥，并指定用于启动 SSH 密钥更新的阈值（数据量、时间间隔和数据包计数）。

若要配置 SSH 服务配置文件，请 **Add**（添加）HA 或管理 — 服务器配置文件，根据需要填写下表中的字段，然后单击 **OK**（确定）并 **Commit**（提交）更改。

配置文件的应用过程因配置文件类型而异。

- 若要应用 HA 配置文件，请选择 Device（设备）> High Availability（高可用性）> General（常规）。在 SSH HA 配置文件设置下，选择现有配置文件。单击 **OK**（确定）并 **Commit**（提交）更改。
- 要应用管理 — 服务器配置文件，请选择 Device（设备）> Setup（设置）> Management（管理）。在 SSH 管理配置文件设置下，选择现有配置文件。单击 **OK**（确定）并 **Commit**（提交）更改。

应用配置文件后，您必须从 *CLI* 中执行 *SSH* 服务重新启动，已激活配置文件。

SSH 服务配置文件设置	说明
姓名	输入配置文件的名称（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。
密码	选择服务器支持用于 SSH 会话加密的密码算法。
KEX	选择服务器在 SSH 会话期间支持的密钥交换算法。
MAC	选择服务器在 SSH 会话期间支持的消息认证码算法。
主机密钥	选择主机密钥类型和密钥长度以生成指定主机密钥算法和密码长度的新密钥对。 选择主机密钥类型后，您可以输入密钥长度。默认密钥类型和长度为 *RSA 2048*。
数据	设置 SSH 密钥更新之前传输的最大数据量（以 MB 为单位）（范围为 10-4000；默认为您选择的密码值）。
间隔	设置 SSH 密钥更新之前最大时间间隔（以秒为单位）（范围为 10-3600；默认为不基于时间的密钥更新）。

© 2019 Palo Alto Networks, Inc.

SSH 服务配置文件设置	说明
数据包	设置 SSH 密钥更新之前的最大数据包数 (2^n)。 如果未配置该参数，会话将在 2^{28} 个数据包后执行密钥更新。为确保更频繁的密钥更新，请指定一个介于 *12* 到 *27* 的值。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Response Pages（响应页面）

自定义响应页面是用户尝试访问 URL 时显示的网页。可以提供下载和显示（而不是请求）的网页或文件的自定义 HTML 消息。

每个虚拟系统都可以有自己的自定义响应页面。下表描述了支持客户消息的自定义响应页面类型。

自定义响应页面类型	说明
防病毒阻止页面	因病毒感染而阻止访问。
应用程序阻止页面	因应用程序被安全策略规则阻止而阻止访问。
身份验证门户认证页面	防火墙显示此页面以便用户可以输入登录凭据以访问符合身份验证策略规则的服务（请参阅 Policies（策略）> Authentication（身份验证））。输入一条消息，告诉用户如何对此身份验证质询作出响应。防火墙根据在分配给身份验证规则的身份验证执行对象中指定的 **Authentication Profile**（身份验证配置文件）对用户进行身份验证（请参阅 Objects（对象）> Authentication（身份验证））。 您可以通过在关联的身份验证执行对象中输入 *Message*（消息），以显示每个身份验证规则的唯一身份验证说明。在对象中定义的消息将替代在身份验证门户 *Web* 认证页面中定义的消息。
“数据过滤阻止”页面	因为检测到敏感信息，因此，内容与数据筛选配置文件匹配，并被阻止。
文件阻止继续页面	此页面供用户确认应继续进行下载。此选项仅在安全配置文件中启用继续功能时才可用。选择 Objects（对象）> Security Profiles（安全配置文件）> File Blocking（文件传送阻止）。
文件阻止阻止页面	因为阻止对文件的访问，所以访问受阻。
GlobalProtect 应用帮助页面	GlobalProtect 用户的自定义帮助页面（可从 GlobalProtect 状态面板上的设置菜单访问）。
GlobalProtect 门户登录页面	用户尝试对 GlobalProtect 门户网页进行身份验证的登录页面。
GlobalProtect 网络门户主页	用户已成功对 GlobalProtect 门户网页进行身份验证的主页
GlobalProtect 应用欢迎页面	用户已成功连接到 GlobalProtect 的欢迎页面。
MFA 登录页面	防火墙显示此页面以便用户可以在访问符合身份验证策略规则的服务时对多因素身份验证 (MFA) 质询作出响应（请参阅 Policies（策略）> Authentication（身份验证））。输入一条消息，告诉用户如何对 MFA 质询作出响应。

© 2019 Palo Alto Networks, Inc.

自定义响应页面类型	说明
SAML 身份验证内部错误页面	告知用户 SAML 身份验证失败的页面。该页面包括用户重试身份验证的链接。
SSL 证书错误通知页面	已吊销 SSL 证书的通知。
SSL 解密退出页面	表明防火墙将解密 SSL 会话以进行检查的用户警告页面。
URL 过滤和类别匹配阻止页面	URL 过滤配置文件阻止访问，或因安全策略规则阻止 URL 类别而阻止访问。
URL 过滤继续和替代页面	含有可使用户绕过阻止的初始阻止策略的页面。例如，认为阻止页面不当的用户可单击 **Continue**（继续）进入该页面。 使用替代页面时，用户需要密码来替代阻止此 URL 的策略。有关设置替代密码的说明，请参阅 URL 管理替代一节。
URL 过滤安全搜索执行阻止页面	安全策略规则阻止访问，该策略中的 URL 过滤配置文件已启用 **Safe Search Enforcement**（安全搜索执行）选项。 如果使用 Bing、Google、Yahoo、Yandex 或 YouTube 执行搜索，且其浏览器或搜索引擎帐户的安全搜索设置未设置为严格，则用户可以看到此页面。阻止页面将指导用户将“安全搜索设置”设置为严格。
防钓鱼阻止页面	当用户尝试在阻止凭据提交的网页上输入有效的公司凭据（用户名或密码）时向用户显示的页面。用户可以继续访问该站点，但仍然无法向任何关联的网络表单提交有效的公司凭据。 选择 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤）以启用凭据检测，并根据 URL 类别控制向网页提交凭据。
防钓鱼继续页面	此页面警告用户不要将公司凭据（用户名和密码）提交到网站。警告用户不要提交凭据可以帮助阻止他们重复使用公司凭据，并向他们讲解有关可能的网络钓鱼尝试的风险。当用户尝试将凭据提交到已将 **User Credential Submission**（用户凭据提交）权限设置为 **continue**（继续）的站点时，他们可以看到此页面（请参阅 Objects（对象）> Security Profiles（安全配置文件）> URL Filtering（URL 过滤））。他们必须选择 **Continue**（继续）才能在站点上输入凭据。

您可以在 **Response Pages**（响应页面）下执行以下任何功能。

- 要导入自定义 HTML 响应页面，请单击要更改的页面类型的链接，然后单击“导入”/“导出”。浏览以找到页面。将显示一条消息，指示导入是否成功。为了使导入成功，文件必须为 HTML 格式。
- 要导出自定义 HTML 响应页面，请单击页面类型的 **Export**（导出）。选择是要打开文件还是将文件保存到硬盘，且在适当情况下，请选择 **Always use the same option**（始终使用相同选项）。
- 要启用或禁用 **Application Block**（应用程序阻止）页面或 **SSL Decryption Opt-out**（**SSL** 解密退出）页面，请单击页面类型的 **Enable**（启用）。视情况选择或取消选择 **Enable**（启用）。
- 要使用默认响应页面（而不是先前加载的自定义页面），请删除自定义阻止页面并提交操作。该操作会将默认阻止页面设置为新主动页面。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Log Settings（日志设置）

选择 **Device**（设备）> **Log Settings**（日志设置）可配置警报、清除日志或启用日志转发到 Panorama、日志记录服务和其他外部服务。

- 选择日志转发目标
- 定义警报设置
- 清除日志

选择日志转发目标

Device（设备）> **Log Settings**（日志设置）

Log Settings（日志设置）页面允许您将日志转发配置到：

- **Panorama, SNMP trap receivers, email servers, Syslog servers, and HTTP servers**（**Panorama**、**SNMP** 陷阱接收器、电子邮件服务器、**Syslog** 服务器和 **HTTP** 服务器）— 您还可以在日志条目中添加或删除源 IP 地址或目标 IP 地址中的标记；除系统日志和配置日志以外的所有日志类型都支持标记。
- **Logging Service**（日志记录服务）— 如果您订阅了日志记录服务并启用了日志记录服务（Device（设备）> Setup（设置）> Management（管理）），则在您将日志转发配置到 Panorama/日志记录服务时，防火墙会将日志发送到日志记录服务。Panorama 将查询日志记录服务，以访问日志、显示日志并生成报告。
- **Azure Security Center**（**Azure** 安全中心）— 与 Azure 安全中心的集成仅适用于 Azure 上的 VM 系列防火墙。
  - 如果您从 Azure 安全中心启动 VM 系列防火墙，则防火墙会自动为您启用包含日志转发配置文件的安全策略规则。
  - 如果您从 Azure 市场或使用自定义 Azure 模板启动 VM 系列防火墙，则必须手动选择 **Azure-Security-Center-Integration**（**Azure** 安全中心集成）以将系统日志、User-ID 日志和 HIP 匹配日志转发到 Azure 安全中心，然后使用其他日志类型的日志转发配置文件（请参阅 Objects（对象）> Log Forwarding（日志转发））。

    您的 *Azure* 订阅自动启用了免费级安全中心。

您可转发以下日志类型：系统、配置、User-ID、HIP 匹配和关联日志。要为各日志类型指定目标，请添加一个或多个匹配列表配置文件（最多 64 个），然后填写下表所介绍的字段。

要转发流量、威胁、*WildFire* 提交、*URL* 过滤、数据过滤、隧道检测、*GTP* 和身份验证日志，必须配置日志转发配置文件（请参阅 Objects（对象）> Log Forwarding（日志转发））。

匹配列表配置文件设置	说明
名称	输入标识匹配列表配置文件的名称（最多 31 个字符）。有效的名称必须以字母数字字符开头，可以包含零、字母数字字符、下划线、连字符、句点或空格。
Filter（筛选器）	默认情况下，防火墙会转发您添加匹配列表配置文件的相应类型的所有日志。要转发日志的子集，请打开下拉列表，并选择现有过滤器，或选择 **Filter Builder**（过滤器生成器）以添加新的过滤器。对于新过滤器中的每个查询，指定以下字段并 **Add**（添加）查询：

© 2019 Palo Alto Networks, Inc.

匹配列表配置文件设置	说明
	• **Connector**（连接符）— 为查询选择逻辑连接符 (AND/OR)。如果想要应用逻辑否定，则选择 **Negate**（求反）。例如，要避免从不可信区域转发日志，可选择 **Negate**（求反），选择 **Zone**（区域）作为 Attribute（属性），选择 **equal**（等于）作为 Operator（运算符），然后在 Value（值）列中输入不可信区域的名称。 • **Attribute**（属性）— 选择日志属性。可用属性因日志类型而异。 • **Operator**（运算符）— 选择确定属性是否适用的标准（如 **equal**（等于））。可用标准因日志类型而异。 • 值- 指定要匹配的属性值。 要显示或导出与过滤器匹配的日志，请选择 **View Filtered Logs**（查看过滤的日志）。此选项卡提供与 **Monitoring**（监控）选项卡页面相同的选项（如**Monitoring**（监控）> **Logs**（日志）> **Traffic**（通信））。 设置筛选程序以转发所有事件严重性级别的日志（默认筛选程序是 *All Logs*（所有日志））。要创建用于不同严重性级别的单独日志转发方法，在 *Filter*（筛选程序）中指定一个或多个严重性级别，配置 *Forward Method*（转发方法），然后对剩余严重性级别重复执行该流程。
说明	输入说明（最多 1,023 个字符），解释此匹配列表配置文件的用途。
Panorama/日志记录服务	如果想要将日志转发到日志记录服务、日志收集器或 Panorama 管理服务器，则选中 **Panorama/Logging Service**（**Panorama/**日志记录服务）。如果启用此选项，必须将日志转发配置为 Panorama。 您不可将关联日志从防火墙转发到 *Panorama*。*Panorama* 将根据其接收的防火墙日志，来生成关联日志。
SNMP	添加一个或多个 SNMP 陷阱服务器配置文件，以便以 SNMP 陷阱形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱））。
email	添加一个或多个电子邮件服务器配置文件，以便以电子邮件通知形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件））。
Syslog	添加一个或多个 Syslog 服务器配置文件，以便以 syslog 消息形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Syslog）。
Http	添加一个或多个 HTTP 服务器配置文件，以便以 HTTP 请求形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> HTTP）。
内置操作	**Add**（添加）操作以执行标记和集成时，您可以从两种类型的内置操作中进行选择。 • **Tagging**（标记）— 可以为日志条目中包括源 IP 地址或目标 IP 地址的所有日志类型添加一项操作，只需根据需要配置以下设置即可。

© 2019 Palo Alto Networks, Inc.

匹配列表配置文件设置	说明
	您只能在关联日志和 *HIP* 匹配日志中标记源 *IP* 地址。不能为系统日志和配置日志配置任何操作，因为这些日志类型的日志条目中不包含 *IP* 地址。 • **Add**（添加）一项操作，并输入描述操作的名称。 • 选择要自动标记的 IP 地址 — **Source Address**（源地址）或 **Destination Address**（目标地址）。 • 选择操作 — **Add Tag**（添加标记）或 **Remove Tag**（删除标记）。 • 选择是将 IP 地址和标记映射注册到防火墙或 Panorama 上的本地 **User-ID** 代理中，还是注册到远程 **User-ID** 代理中。 • 要将 IP 地址和标记映射注册到远程 **User-ID** 代理中，请选择启用转发功能的 HTTP 服务器配置文件（Device（设备）> Server Profiles（服务器配置文件）> HTTP）。 • 配置要设置的 IP 标记**Timeout**（超时）（以分钟为单位），即，维护 IP 地址到标记映射的时间量。设置超时为 0，意味着 IP 标记映射未超时（范围为 0-43200（30 天），默认为 0）。 您只能使用*Add Tag*（添加标记）配置超时。 • 输入或选择要应用或从目标源或目标 IP 地址删除的 **Tags**（标记）。 • **Integration**（集成）— 仅供在 Azure 上的 VM 系列防火墙上使用。**Add**（添加）一个名称并使用此操作将所选日志转发到 Azure 安全中心。如未显示此选项，则表明可能未启用 Azure 安全中心的 Azure 订阅功能。 要根据日志转发配置文件筛选器添加设备到隔离列表，请选择 **Quarantine**（隔离）。

定义警报设置

- Device（设备）> Log Settings（日志设置）

使用 Alarm Settings（警报设置）可配置 CLI 和 Web 界面的警报。您可配置以下事件的通知：

- 已按指定阈值和在指定时间间隔内对安全规则（或一组规则）进行匹配。
- 达到加密/解密失败阈值。
- 各种日志类型的日志数据库几乎已满；当已经使用 90% 的可用磁盘空间时，默认将配额设置为通知。配置警报可让您在磁盘装满之前采取措施，并清除日志。

启用警报后，可通过单击 Web 界面底部的 **Alarms**（警报）（Alarms）查看当前列表。

要添加警报，请编辑下表中所述的警报设置。

警报日志设置	说明
启用警报	仅当 **Enable Alarms**（启用警报）后警报才会处于可见状态。 如果禁用警报，防火墙不会提醒您需要采取操作的关键事件。例如，警报会告诉您主密钥即将过期的时间；如果密钥在更改前过

© 2019 Palo Alto Networks, Inc.

警报日志设置	说明
	期，则防火墙会重新启动进入维护模式，然后需要执行出厂重置。
启用 CLI 警报通知	发生警报后立即启用 CLI 警报通知。
启用 Web 警报通知	将打开一个显示用户会话相关警报的窗口，其中包括警报的发生时间和确认时间。
启用有声警报	管理员登录 Web 界面且存在未确认警报时，有声警报提示音会每隔 15 秒在其计算机上播放一次。警报提示音会一直播放，直至管理员确认所有警报为止。 要查看并确认警报，请单击 **Alarms**（警报）。 此功能仅适用于 FIPS-CC 模式下的防火墙。
加密/解密失败阈值	指定生成警报之前的加密/解密失败次数。
<*Log-type*> 日志 DB	当日志数据库达到最大大小的指示百分比时，系统将生成警报。
安全违反阈值/ 安全违反时间期限	如果某个特定的 IP 地址或端口在 **Security Time Period**（安全违反时间期限）设置中指定的时间段（秒）内命中某项拒绝规则的次数达到 **Security Violations Threshold**（安全违反阈值）设置中指定的次数，则会生成警报。
违反阈值/ 违反时间期限/ 安全策略标记	在违反时间期限字段指定的期限内，如果规则集合达到在违反阈值字段中指定的规则限制违反次数，则生成警报。会话与显式拒绝策略匹配时视为冲突。 使用安全策略标记指定规则限制阈值将因其生成警报的标记。定义安全策略时，可以指定这些标记。
选择性审核	选择性审核选项仅适用于 FIPS-CC 模式下的防火墙。 指定以下设置： • **FIPS-CC Specific Logging**（**FIPS-CC** 特定日志记录）— 启用符合常见标准 (CC) 所需的详细记录。 • **Packet Drop Logging**（数据包丢弃日志记录）— 记录被防火墙丢弃的数据包。 • **Suppress Login Success Logging**（禁止登录成功日志记录）— 停止对管理员成功登录防火墙进行记录。 • **Suppress Login Failure Logging**（禁止登录失败日志记录）— 停止对管理员登录防火墙失败进行记录。 • **TLS Session Logging**（**TLS** 会话日志记录）— 记录 TLS 会话的建立。 • **CA (OCSP/CRL) Session Establishment Logging**（**CA (OCSP/CRL)** 会话建立日志记录）— 当防火墙使用联机证书状态协议或证书吊销列表服务器请求，来发送证书吊销状态的检查请求时，记录防火墙和证书授权机构之间的会话建立。（默认禁用。） • **IKE Session Establishment Logging**（**IKE** 会话建立日志记录）— 当防火墙上的 VPN 网关使用对端进行身份验证时，记录 IPSec IKE 会话建立。此对端可以是 Palo Alto Networks 防火墙或用于开启和终止 VPN 连接的其他安全设备。日志中指定的接口名称即绑定到 IKE 网关的接口。如适用，IKE 网关名称也会显示。禁用此选项可停止记录所有 IKE 事件记录。（默认启用。） • **Suppressed Administrators**（被禁止的管理员）— 停止记录所列管理员对防火墙配置所作的更改。

© 2019 Palo Alto Networks, Inc.

清除日志

- Device（设备）> Log Settings（日志设置）

在 Log Settings（日志设置）页面上进行日志管理时，您可清除防火墙上的日志。单击要清除的日志类型，然后单击 **Yes**（是）以确认请求。

要自动删除日志和报告，您可配置过期期限。有关详细信息，请参阅记录和报告设置。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）

以下主题介绍可以在防火墙上配置的服务器配置文件设置：

- Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱）
- Device（设备）> Server Profiles（服务器配置文件）> Syslog
- Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）
- Device（设备）> Server Profiles（服务器配置文件）> HTTP
- Device（设备）> Server Profiles（服务器配置文件）> NetFlow
- Device（设备）> Server Profiles（服务器配置文件）> RADIUS
- Device（设备）> Server Profiles（服务器配置文件）> TACACS+
- Device（设备）> Server Profiles（服务器配置文件）> LDAP
- Device（设备）> Server Profiles（服务器配置文件）> Kerberos
- Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商）
- Device（设备）> Server Profiles（服务器配置文件）> DNS
- Device（设备）> Server Profiles（服务器配置文件）> Multi Factor Authentication（多因素身份验证）

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱）

简单网络管理协议 (SNMP) 是用于监视网络设备的一个标准协议。为了提醒您网络上的系统事件或威胁，受监控设备会将 SNMP 陷阱发送到 SNMP 管理器（陷阱服务器）。选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **SNMP Trap**（**SNMP** 陷阱）或 **Panorama** > **Server Profiles**（服务器配置文件）> **SNMP Trap**（**SNMP** 陷阱）可配置服务器配置文件，以使防火墙或 Panorama 将陷阱发送到 SNMP 管理器。要启用 SNMP GET 消息（从 SNMP 管理器请求的统计信息），请参阅启用 SNMP 监控。

在创建服务器配置文件后，必须指定将触发防火墙发送 SNMP 陷阱的日志类型（参阅 Device（设备）> Log Settings（日志设置））。有关必须加载到 SNMP 管理器以便解释陷阱的 MIB 列表，请参阅支持的 MIB。

请不要删除任何系统日志设置或日志记录配置文件使用的服务器配置文件。

SNMP 陷阱服务器配置文件设置	说明
姓名	输入 SNMP 配置文件的名称（最多31个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
版本	选择 SNMP 版本：**V2c**（默认）或 **V3**。您的选择可控制对话框显示的其余字段。对于任一版本，最多可以添加四个 SNMP 管理器。 使用可提供身份验证和其他功能的 *SNMPv3*，以保证网络连接的安全性。
对于 **SNMP V2c**	
姓名	指定 SNMP 管理器的名称。此名称最多可以包含 31 个字符，包括字母数字、句点、下划线或连线。
SNMP 管理器	指定 SNMP 管理器的 FQDN 或 IP 地址。
社区	输入团体字符串，不但可用于识别 SNMP 管理器和监控设备的 SNMP 团体，并且还可用作密码在转发陷阱时对团体成员彼此进行身份验证。字符串最多可以包含 127 个字符，接受所有字符且区分大小写。 切勿使用默认社区字符串（不得将社区字符串设置为 *public*（公用）或 *private*（私用））。使用唯一社区字符串，以便在使用多个 *SNMP* 服务时发生冲突。由于 *SNMP* 消息包含明文团体字符

© 2019 Palo Alto Networks, Inc.

SNMP 陷阱服务器配置文件设置	说明
	串，因此在定义团体成员（管理员访问权限）时需要考虑网络的安全要求。
对于 **SNMP V3**	
姓名	指定 SNMP 管理器的名称。此名称最多可以包含 31 个字符，包括字母数字、句点、下划线或连线。
SNMP 管理器	指定 SNMP 管理器的 FQDN 或 IP 地址。
用户	指定用于标识 SNMP 用户帐户的用户名（最多 31 个字符）。在防火墙上配置的用户名必须与在 SNMP 管理器上配置的用户名相匹配。
引擎 ID	指定防火墙的引擎 ID。当 SNMP 管理器和防火墙相互进行身份验证时，陷阱消息使用此值唯一标识防火墙。如果将此字段留空，则消息将防火墙序列号用作 **EngineID**（引擎 **ID**）。如果输入一个值，则其格式必须为十六进制，前缀为 0x 且包含表示 5-64 个字节的任意数量的其他 10-128 个字符（每个字节 2 个字符）。对于高可用性 (HA) 配置中的防火墙，将此字段留空，以便 SNMP 管理器可以标识已发送陷阱的高可用性对端；否则，值同步且两个对端都将使用同一 **EngineID**（引擎 **ID**）。
身份验证密码	指定 SNMP 用户的身份验证密码。防火墙使用该密码对 SNMP 管理器进行身份验证。防火墙将使用安全哈希算法 (SHA-1 160) 对密码进行加密。密码长度必须为 8-256 个字符，且允许使用所有字符。
私人密码	指定 SNMP 用户的私人密码。防火墙使用密码和高级加密标准 (AES-128) 对陷阱进行加密。密码长度必须为 8-256 个字符，且允许使用所有字符。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> Syslog

选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Syslog** 或 **Panorama** > **Server Profiles**（服务器配置文件）> **Syslog** 可配置服务器配置文件，以将防火墙、Panorama 和日志收集器日志作为 syslog 消息转发到 syslog 服务器。要定义 syslog 服务器配置文件，单击 **Add**（添加）并指定 New Syslog Server（新建 Syslog 服务器）字段。

- 要选择系统、配置、*User-ID*、*HIP* 匹配和关联日志的 *Syslog* 服务器配置文件，请参阅 Device（设备）> Log Settings（日志设置）。
- 要选择流量、威胁、*Wildfire*、*URL* 过滤、数据过滤、隧道检测、身份验证和 *GTP* 日志的 *Syslog* 服务器配置文件，请参阅 Objects（对象）> Log Forwarding（日志转发）。
- 无法删除防火墙用于任何系统、配置日志设置或日志转发配置文件的服务器配置文件。

Syslog 服务器设置	说明
姓名	输入 syslog 配置文件的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
服务器选项卡	
姓名	单击 **Add**（添加），并输入 Syslog 服务器的名称（最多 31个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
服务器	输入 syslog 服务器的 IP 地址或 FQDN。
传输	选择通过 UDP、TCP 还是 SSL 端口传输 syslog 消息。 使用*SSL* 加密数据，并将数据安全发送到 *syslog* 服务器。数据通过 *UDP* 或 *TCP* 以明文形式发送，并且在传输过程中是可读的。
端口	输入 syslog 服务器的端口号（UDP 的标准端口号为 514；SSL 的标准端口号为 6514；对于 TCP，必须指定端口号）。
Format	指定要使用的 syslog 格式：BSD（默认格式）或 IETF。
工具	选择一个 Syslog 标准值。选择该值可以映射 Syslog 服务器使用工具字段管理消息的方式。有关工具字段的详细信息，请参阅 RFC 3164（BSD 格式）或 RFC 5424（IETF 格式）。
自定义日志格式选项卡	

© 2019 Palo Alto Networks, Inc.

Syslog 服务器设置	说明
日志类型	单击日志类型将打开一个对话框，您可以在此对话框中指定自定义日志格式。在该对话框中，单击字段可以将其添加到“日志格式”区域。其他文本字符串均可在“日志格式”区域中直接编辑。单击 **OK**（确定）以保存设置。查看可用于自定义日志 的每个字段的说明。 有关可用于自定义日志的字段的详细信息，请参阅 Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）。
转义	指定转义序列。**Escaped characters**（转义符）为字符列表，其中列出了所有要转义而不带空格的字符。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）

选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Email**（电子邮件）或 **Panorama** > **Server Profiles**（服务器配置文件）> **Email**（电子邮件），以配置服务器配置文件，从而将日志作为电子邮件通知转发。要定义电子邮件服务器配置文件，请 **Add**（添加）配置文件，并指定 Email Notification Settings（电子邮件通知设置）。

- 要选择系统、配置、*User-ID*、*HIP* 匹配和关联日志的电子邮件服务器配置文件，请参阅 Device（设备）> Log Settings（日志设置）。
- 要选择流量、威胁、*Wildfire*、*URL* 过滤、数据筛选、隧道检测、身份验证和 *GTP* 日志的电子邮件服务器配置文件，请参阅 Objects（对象）> Log Forwarding（日志转发）。
- 您还可以安排电子邮件报告（ Monitor（监控）> PDF Reports（PDF 报告）> Email Scheduler（电子邮件计划程序））。
- 无法删除防火墙用于任何系统、配置日志设置或日志转发配置文件的服务器配置文件。

电子邮件通知设置	说明
姓名	输入服务器配置文件的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置 （仅限虚拟系统）	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
服务器选项卡	
姓名	输入名称以标识服务器（最多 31 个字符）。此字段仅是一个标签，不必用作现有电子邮件服务器的主机名。
电子邮件显示名称	输入在电子邮件的发件人字段中显示的名称。
从	输入发件人电子邮件地址，例如 ecurity_alert@company.com。
到	输入收件人的电子邮件地址。
其他接收人	（可选）输入其他收件人的电子邮件地址。只能添加一个其他收件人。要添加多个收件人，请添加通讯组列表的电子邮件地址。
电子邮件网关	输入发送电子邮件的服务器的 IP 地址或主机名。
协议	选择您想用于发送电子邮件的协议（**Unauthenticated SMTP**（未经身份验证的 **SMTP**）或 **SMTP over TLS**）。
端口	输入您要用于发送电子邮件的端口号（如果不是默认端口）（SMTP 为端口 25；TLS 为端口 587）。
TLS 版本	选择您要使用的 TLS 版本（**1.2** 或 **1.1**）。

© 2019 Palo Alto Networks, Inc.

电子邮件通知设置	说明
（仅限 SMTP over TLS）	作为最佳做法，我们强烈建议您使用最新版 *TLS*。
身份验证方法 （仅限 SMTP over TLS）	选择您要使用的身份验证方法： • **Auto**（自动）（默认）— 允许客户端和服务器确定身份验证方法。 • **Login**（登录）— 对用户名和密码使用 Base64 编码，并分别进行传输。 • **Plain**（普通）— 对用户名和密码使用 Base64 编码，并一起传输。
证书配置文件 （仅限 SMTP over TLS）	选择防火墙用于对电子邮件服务器执行身份验证的证书配置文件。
用户名 （仅限 SMTP over TLS）	输入发送电子邮件的账户的用户名。
密码 （仅限 SMTP over TLS）	输入发送电子邮件的账户的密码。
确认密码 （仅限 SMTP over TLS）	确认发送电子邮件的账户的密码。
测试连接 （仅限 SMTP over TLS）	确认电子邮件服务器和防火墙之间的连接。
自定义日志格式选项卡	
日志类型	单击日志类型将打开一个对话框，您可以在此对话框中指定自定义日志格式。在该对话框中，单击字段可以将其添加到“日志格式”区域。单击 **OK**（确定）保存更改。
转义	指定不带空格的 **Escaped Characters**（转义字符）（所有字符都不能从字面上解释），然后指定转义序列的 **Escape Character**（转义字符）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> HTTP

选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **HTTP** 或 **Panorama** > **Server Profiles**（服务器配置文件）> **HTTP** 可配置用于转发日志的服务器配置文件。您可以配置防火墙将日志转发到 HTTP(S) 目标，或与公开 API 的任何基于 HTTP 的服务集成，并根据需求修改 HTTP 请求中的 URL、HTTP 标头、参数和有效负载。还可以使用 HTTP 服务器配置文件访问正在运行集成的 PAN-OS User-ID 代理的防火墙，并将一个或多个标记注册到防火墙生成的日志中的源或目标 IP 地址。

使用 *HTTP* 服务器配置文件转发日志：

- 请参阅系统、配置、*User-ID*、*HIP* 匹配和关联日志的 Device（设备）> Log Settings（日志设置）。
- 请参阅流量、威胁、*WildFire*、*URL* 过滤、数据过滤、隧道检测、身份验证和 *GTP* 日志的 Objects（对象）> Log Forwarding（日志转发）。

如果 *HTTP* 服务器配置文件用于转发日志，则不能将其删除。要删除防火墙或 *Panorama* 上的服务器配置文件，必须从 *Device*（设备）> *Log settings*（日志设置）或 *Objects*（对象）> *Log Forwarding*（日志转发）配置文件删除对配置文件的引用。

要定义 HTTP 服务器配置文件，请 **Add**（添加）新的配置文件，并配置下表中的设置。

HTTP 服务器设置	说明
姓名	输入服务器配置文件的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。有效的名称必须以字母数字字符开头，可以包含零、字母数字字符、下划线、连字符、点或空格。
位置	选择在其中使用服务器配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其 **Location**（位置）。
标记注册	标记注册可让您添加或删除日志条目中源或目标 IP 地址中的标记，并使用 HTTP(S) 将 IP 地址和标记映射注册到防火墙上的 User-ID 代理。然后，可以将使用这些标记的动态地址定义为过滤条件以确定其成员，并根据标记对 IP 地址实施策略规则。 **Add**（添加）连接详细信息以启用对防火墙上的 User-ID 代理的 HTTP(S) 访问。 要将标记注册到 Panorama 上的 User-ID 代理，不需要服务器配置文件。此外，不能使用 HTTP 服务器配置文件将标记注册到正在 Windows 服务器上运行的 User-ID 代理。
服务器选项卡	
姓名	**Add**（添加）HTTP(S) 服务器，并输入远程（最多 31 个字符）或远程 User-ID 代理。有效的名称必须唯一且以字母数字字符开头；名称可以包含零、字母数字字符、下划线、连字符、点或空格。 服务器配置文件最多可以包括四个服务器。

© 2019 Palo Alto Networks, Inc.

HTTP 服务器设置	说明
地址	输入 HTTP(S) 服务器的 IP 地址。 对于标记注册，请将配置的防火墙 IP 地址指定为 User-ID 代理。
协议	选择协议：HTTP 或 HTTPS。
端口	输入访问服务器或防火墙的端口号。HTTP 的默认端口号为 80，HTTPS 的默认端口号为 443。 对于标记注册，防火墙使用 HTTP 或 HTTPS 连接到配置为 User-ID 代理的防火墙上的 Web 服务器。
TLS 版本	选择服务器上 SSL 支持的 TLS 版本。默认为 **1.2**。
证书配置文件	选择用于与服务器进行 TLS 连接的证书配置文件。 在与服务器建立安全连接时，防火墙会使用指定的证书配置文件来验证服务器证书。
HTTP 方法	选择服务器支持的 HTTP 方法。选项包括 GET、PUT、POST（默认）和 DELETE。 对于 User-ID 代理，请使用 GET 方法。
用户名	输入具有访问权限的用户名，以完成所选择的 HTTP 方法。 如果将标记注册到防火墙上的 User-ID 代理，则用户名必须是具有超级用户角色的管理员。
密码	输入用于对服务器或防火墙进行身份验证的密码。
测试服务器连接	选择服务器和 **Test Server Connection**（测试服务器连接）以测试与服务器的网络连接。 此测试不会测试与正在运行 User-ID 代理的服务器的连接。
负载格式选项卡	
日志类型	可以显示 HTTP 转发的日志类型。单击日志类型将打开一个对话框，您可以在此对话框中指定自定义日志格式。
Format	显示日志类型是使用默认格式、预定义格式还是定义的自定义负载格式。
预定义格式	选择服务或供应商发送日志的格式。预定义格式通过内容更新推送，并且每次在防火墙或 Panorama 上安装新的内容更新时可以进行更改。
姓名	输入自定义日志格式的名称。
URI 格式	指定使用 HTTP(S) 要向其发送日志的资源。 如果创建自定义格式，则 **URI** 是 HTTP 服务的资源端点。防火墙将 URI 附加到之前定义的 IP 地址，以构建 HTTP 请求的 URL。确保 URI 和负载格式与第三方供应商所需的语法相匹配。您可以使用 HTTP 标头、参数、值对和请求负载中所选日志类型所支持的任何属性。

© 2019 Palo Alto Networks, Inc.

HTTP 服务器设置	说明
HTTP 标头	添加标头及其相应值。
参数	包括可选参数和值。
负载	选择要包括作为外部 Web 服务器的 HTTP 消息中负载的日志属性。
发送测试日志	单击此按钮以验证外部 Web 服务器是否收到请求且是否处于正确的负载格式。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> NetFlow

Palo Alto Networks 防火墙可以将有关其接口上的 IP 流量的统计信息作为 NetFlow 字段导出到 NetFlow 收集器。NetFlow 收集器是一种出于安全、管理、核算和故障排除目的用于分析网络流量的服务器。所有 Palo Alto Networks 防火墙都支持 NetFlow 9 版。以上防火墙仅支持单向 NetFlow，而不支持双向 NetFlow。防火墙支持对接口上所有 IP 数据包执行 NetFlow 处理，不支持采样 NetFlow。可以为第 3 层、第 2 层、虚拟线路、旁接、VLAN、回环和隧道接口导出 NetFlow 记录。对于聚合以太网接口，您可以导出聚合组的记录，但不能导出组内各个接口的记录。防火墙支持 NetFlow 收集器用于解密 NetFlow 字段的标准和企业（特定于 PAN-OS）NetFlow 模板。防火墙根据导出数据的类型选择模板：IPv4 或 IPv6 流量、包含或不包含 NAT、标准或专用于企业的字段。

要配置 NetFlow 导出，请 **Add**（添加）NetFlow 服务器配置文件以指定接收导出数据的 NetFlow 服务器，并指定导出参数。在将配置文件分配给接口后（请参阅 Network（网络）> Interfaces（接口）），防火墙会将遍历该接口的所有流量的 NetFlow 数据导出至指定服务器。

Netflow 设置	说明
姓名	输入 Netflow 服务器配置文件的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
模板刷新率	防火墙定期刷新 NetFlow 模板，以重新评估使用哪一个模板（以防导出数据类型变化），并将所有更改应用于所选模板中的字段。根据 NetFlow 收集器的要求，指定防火墙刷新 NetFlow 的频率（以**Minutes**（分钟）为单位，范围为 1 至 3,600，默认为 30）或 **Packets**（数据包数）（导出记录 — 范围为 1 至 600，默认为 20）。在任一阈值过后，防火墙将刷新模板。所需的刷新频率取决于 NetFlow 收集器。如果在服务器配置文件中添加多个 NetFlow 收集器，请使用刷新速率最高的收集器的值。
主动超时	指定防火墙为各个会话导出数据时的频率（分钟）（范围为 1 至 60，默认为 5）。根据您希望 NetFlow 收集器隔多久更新一次通信统计数据来设置频率。
PAN-OS 字段类型	导出 Netflow 记录中 App-ID 和 User-ID 服务的 PAN-OS 特定字段。
servers	
姓名	指定用于标识服务器的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
服务器	指定服务器的主机名或 IP 地址。每个配置文件最多可添加两台服务器。
端口	指定用于访问服务器的端口号（默认为 2055）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> RADIUS

选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **RADIUS**或 **Panorama** > **Server Profiles**（服务器配置文件）> **RADIUS**可为身份验证配置文件引用的远程身份验证拨入用户服务 (RADIUS) 服务器配置设置（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。您可以使用 RADIUS 对访问网络资源（通过 GlobalProtect 或身份验证门户）的最终用户进行身份验证，对在防火墙或 Panorama 上本地定义的管理员进行身份验证，以及对在 RADIUS 服务器上外部定义的管理员进行身份验证和授权。

RADIUS 服务器设置	说明
配置文件名称	输入名称以标识服务器配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
仅供管理员使用	选择此选项可指定只能使用配置文件进行身份验证的管理员帐户。对于拥有多个虚拟系统的防火墙，此选项只有在当 **Location**（位置）为 **Shared**（共享）时显示。
超时	输入时间间隔（以秒单位），在此之后身份验证请求会超时（范围为 1–120，默认为 3）。 如果使用 *RADIUS* 服务器配置文件将防火墙与 *MFA* 服务进行集成，请输入能够让用户拥有足够的时间对身份验证质询做出响应的时间间隔。例如，如果 *MFA* 服务提示输入一次性密码 *(OTP)*，则用户需要时间查看其端点设备上的 *OTP*，然后在 *MFA* 登录页面输入 *OTP*。
身份验证协议	选择防火墙用于保护与 RADIUS 服务器的连接的 **Authentication Protocol**（身份验证协议）。 • **PEAP-MSCHAPv2**—（默认）采用 Microsoft 质询握手身份验证协议 (MSCHAPv2) 的受保护 EAP (PEAP) 通过在加密隧道中传输用户名和密码提高 PAP 或 CHAP 的安全性。 • **PEAP with GTC**（采用 **GTC** 的 **PEAP**）— 选择采用通用令牌卡 (GTC) 的受保护 EAP (PEAP) 可在加密隧道中使用一次性令牌。 • **EAP-TTLS with PAP**（采用 **PAP** 的 **EAP-TTLS**）— 选择采用隧道传输层安全 (TTLS) 和 PAP 的 EAP 可在加密隧道中传输 PAP 的纯文本凭据。 • **CHAP** — 如果 RADIUS 服务器不支持 EAP 或 PAP 或未为其配置 EAP 或 PAP，请选择质询握手身份验证协议 (CHAP)。 • **PAP** — 如果 RADIUS 服务器不支持 EAP 或 CHAP 或未为其配置 EAP 或 CHAP，请选择密码身份验证协议 (PAP)。
允许用户在密码过期后更改密码	（采用 GlobalProtect 4.1 或更高版本的 PEAP-MSCHAPv2）选择此选项可允许 GlobalProtect 用户更改过期密码。

© 2019 Palo Alto Networks, Inc.

RADIUS 服务器设置	说明
使外部身份匿名	（PEAP-MSCHAPv2、采用 GTC 的 PEAP 或采用 PAP 的 EAP-TTLS）默认启用此选项，以使用户身份在防火墙对服务器进行身份验证后创建的外部隧道中匿名。 某些 *RADIUS* 服务器配置可能不支持匿名外部标识，因此您可能需要清除该选项。清除后，用户名将以明文形式传输。
证书配置文件	（PEAP-MSCHAPv2、采用 GTC 的 PEAP 或采用 PAP 的 EAP-TTLS）选择或配置证书配置文件可与 RADIUS 服务器配置文件关联。防火墙使用证书配置文件对 RADIUS 服务器进行身份验证。
重试次数	指定超时后的重试次数（范围为 1 - 5，默认为 3）。
servers	以首选顺序配置每个服务器的信息。 • 名称 — 输入名称以标识服务器。 • **RADIUS** 服务器 — 输入服务器 IP 地址或 FQDN。 • 密钥/确认密钥 — 输入并确认密钥，以验证并加密防火墙和 RADIUS 服务器之间的连接。 • 端口 — 输入用于身份验证请求的服务器端口（范围为 1–65,535，默认为 1812）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> TACACS+

选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **TACACS+** 或 **Panorama** > **Server Profiles**（服务器配置文件）> **TACACS+** 以配置设置，从而定义防火墙或 Panorama 连接到终端访问控制器访问控制系统加强版 (TACACS+) 服务器的方式（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。您可以使用 TACACS+ 对访问网络资源（通过 GlobalProtect 或身份验证门户）的最终用户进行身份验证，对在防火墙或 Panorama 上本地定义的管理员进行身份验证，以及对在 RADIUS 服务器上外部定义的管理员进行身份验证和授权。

TACACS+ 服务器设置	说明
配置文件名称	输入名称以标识服务器配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
仅供管理员使用	选择此选项可指定只能使用配置文件进行身份验证的管理员帐户。对于拥有多个虚拟系统的防火墙，此选项只有在当 **Location**（位置）为 **Shared**（共享）时显示。
超时	输入身份验证请求超时后以秒为单位的时间间隔（范围为 1-20，默认为 3）。
身份验证协议	选择防火墙用于保护与 TACACS+ 服务器的连接的 **Authentication Protocol**（身份验证协议）。 • **CHAP** — 质询握手身份验证协议(CHAP) 为默认和首选协议，因为它比 PAP 更安全。 • **PAP** — 如果 TACACS+ 服务器不支持 CHAP 或未为其配置 CHAP，请选择密码身份验证协议 (PAP)。 • **Auto**（自动）— 防火墙首先尝试使用 CHAP 进行身份验证。如果 TACACS+ 服务器未响应，则防火墙回退至 PAP。
对所有身份验证使用单个连接	选择此选项可以为所有身份验证使用相同的 TCP 会话。此选项可以通过避免启动所需的过程并为每个身份验证事件拆解单独的 TCP 会话以提高性能。
servers	单击添加并为每个 TACACS+ 服务器指定下列设置： • 名称 — 输入名称以标识服务器。 • **TACACS+** 服务器 — 输入 TACACS+ 服务器的 IP 地址或 FQDN。 • **Secret/Confirm Secret**（密钥/确认密钥）— 输入并确认密钥，以验证并加密防火墙和 RADIUS 服务器之间的连接。 • 端口 — 输入用于身份验证请求的服务器端口（默认为 49）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> LDAP

- **Device**（设备）> **Server Profiles**（服务器配置文件 > **LDAP**
- **Panorama** > **Server Profiles**（服务器配置文件）> **LDAP**

Add（添加）或选择 LDAP 服务器配置文件可为身份验证配置文件引用的轻型目录访问协议 (LDAP) 服务器配置设置（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。您可以使用 LDAP 对访问网络资源的最终用户（通过 GlobalProtect 或身份验证门户）和在防火墙或 Panorama 上本地定义的管理员进行身份验证。

LDAP 服务器设置	说明
配置文件名称	输入名称以标识配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
仅供管理员使用	选择此选项可指定只能使用配置文件进行身份验证的管理员帐户。对于拥有多个虚拟系统的防火墙，此选项只有在当 **Location**（位置）为 **Shared**（共享）时显示。
使用此配置文件检查序列号。	选择此选项可使 LDAP 服务器配置文件从受管端点收集序列号。GlobalProtect 门户和网关可使用此信息来验证端点是否受管（活动目录中是否存在序列号）。
服务器列表	对于每个 LDAP 服务器，**Add**（添加）主机 **Name**（名称）、IP 地址或 FQDN（**LDAP Server**（**LDAP** 服务器））和 **Port**（端口）（默认为 389）。 至少配置两个 *LDAP* 服务器以提供冗余。
类型	从下拉列表中选择服务器类型。
基本 DN	在目录服务器中指定根上下文，以缩小用户或组信息的搜索范围。
绑定 Dn	为目录服务器指定登录名称（专有名称）。 绑定 *DN* 帐户必须有权读取 *LDAP* 目录。
密码/确认密码	指定绑定帐户密码。代理将在配置文件中保存加密密码。
绑定超时	指定连接到目录服务器时施加的时间限制（秒）（范围为 1 至 30 秒，默认为 30）。
搜索超时	指定执行目录搜索时施加的时间限制（秒）（范围为 1 至 30，默认为 30）。

© 2019 Palo Alto Networks, Inc.

LDAP 服务器设置	说明
重试时间间隔	指定以秒为单位的时间间隔，在此之后系统将尝试在上一次失败尝试后连接到 LDAP 服务器（范围为 1 至 3,600，默认为 60）。
需要 SSL/TLS 安全连接	如果您希望防火墙使用 SSL 或 TLS 与目录服务器进行通信，请选中此选项。协议取决于服务器端口： • 389（默认）— TLS（具体来说，防火墙使用启动 TLS 操作，这可以将初始明文连接升级至 TLS。） • 636 — SSL • 任何其他端口 — 防火墙首先尝试使用 TLS。如果目录服务器不支持 TLS，则防火墙回滚至 SSL。 此选项为最佳实践，因为，它可提高安全性，且默认为选中。
验证 SSL 会话的服务器证书	如果您希望防火墙验证目录服务器为建立 SSL/TLS 连接提供的证书，可以选择此选项（默认为未选择）。防火墙在两个方面对证书进行验证： • 证书可信且有效。对于防火墙要信任的证书、其根证书授权机构 (CA) 和任何中间证书，均必须存储在 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）> **Device Certificates**（设备证书）下的证书中。 • 证书名称必须与 LDAP 服务器的主机名称相匹配。防火墙首先检查证书属性主题备选主题是否相匹配，然后尝试使用属性主题 DN。如果证书使用目录服务器的 FQDN，则必须使用 **LDAP** 服务器字段中的 FQDN 匹配名称才能成功。 如果验证失败，则连接也会失败。要启用此验证，还必须选择 **Require SSL/TLS secured connection**（需要 **SSL/TLS** 安全连接）。 使防火墙验证 *SSL* 会话的服务器证书，从而提高安全性。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> Kerberos

选择 **Device**（设备）> **Server Profiles**（服务器配置文件）> **Kerberos** 或 **Panorama** > **Server Profiles**（服务器配置文件）> **Kerberos** 可配置服务器配置文件，以便让用户在本地对 Active Directory 域控制器或 Kerberos V5 兼容的身份验证服务器进行身份验证。在配置 Kerberos 服务器配置文件后，可以将其分配给身份验证配置文件（参阅（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。您可以使用 Kerberos 对访问网络资源的最终用户（通过 GlobalProtect 或身份验证门户）和在防火墙或 Panorama 上本地定义的管理员进行身份验证。

要使用 *Kerberos* 身份验证，必须能够通过 *IPv4* 地址访问后端 *Kerberos* 服务器。不支持 *IPv6* 地址。

Kerberos 服务器设置	说明
配置文件名称	输入名称以标识服务器（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
仅供管理员使用	选择此选项可指定只能使用配置文件进行身份验证的管理员帐户。对于拥有多个虚拟系统的防火墙，此选项只有在当 **Location**（位置）为 **Shared**（共享）时显示。
servers	对于每个 Kerberos 服务器，请单击添加，并指定以下设置： • 名称 — 输入服务器的名称。 • **Kerberos** 服务器 — 输入服务器 IPv4 地址或 FQDN。 • **Port**（端口）— 输入与服务器进行通信的可选端口（范围为 1 至 65,535，默认为 88）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商）

使用此页面可以将安全断言标记语言 (SAML) 2.0 标识提供商 (IdP) 注册到防火墙或 Panorama。注册是启用防火墙或 Panorama 充当 SAML 服务提供商必须执行的步骤，这可以控制对网络资源的访问。当管理员和最终用户请求资源时，服务提供商会将用户重定向到 IdP 进行身份验证。最终用户可以是 GlobalProtect 或身份验证门户用户。管理员可以在防火墙和 Panorama 上进行本地管理，也可以在 IdP 标识存储中进行外部管理。可以配置 SAML 单点登录 (SSO)，以便每个用户可以在登录后自动访问多个资源。还可以配置 SAML 单点注销 (SLO)，以便每个用户可以通过注销任何单个服务同时注销每个启用 SSO 的服务。

身份验证序列不支持用于指定 *SAML* 服务器配置文件的身份验证配置文件。

在大多数情况下，不能使用 *SSO* 访问同一移动设备上的多个应用。

您无法为身份验证门户用户启用 *SLO*。

创建 SAML IdP 服务器配置文件的最简单方法是从 IdP **Import**（导入）包含注册信息的元数据文件。使用导入的值保存服务器配置文件后，可以编辑配置文件以修改值。如果 IdP 不提供元数据文件，可以 **Add**（添加）服务器配置文件并手动输入信息。创建服务器配置文件后，将其分配给特定防火墙或 Panorama 服务的身份验证配置文件（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。

SAML 标识提供商服务器设置	说明
配置文件名称	输入名称以标识服务器（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用配置文件的范围。在拥有多个虚拟系统的防火墙的上下文中，选择一个虚拟系统或选择 **Shared**（共享）（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存配置文件后，您无法更改其位置。
仅供管理员使用	选择此选项可指定只能使用配置文件进行身份验证的管理员帐户。对于拥有多个虚拟系统的防火墙，此选项只有在当 **Location**（位置）为 **Shared**（共享）时显示。
标识提供商 ID	输入 IdP 的标识符。IdP 提供此信息。
标识提供商证书	选择 IdP 用于对发送给防火墙的 SAML 消息进行签名的证书。您必须选择 IdP 证书来确保 IdP 发送给防火墙的消息的完整性。要根据证书颁发机构 (CA) 验证 IdP 证书，必须在引用 IdP 服务器配置文件的身份验证配置文件中指定 **Certificate Profile**（证书配置文件）（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。 当生成或导入证书及其关联私钥时，请记住在证书中指定的密钥使用属性控制可以使用该密钥。如果证书明确列出密钥使用属性，则其中一个属性必须为数字签名，该属性在防火墙上生成的证书中不可用。在这种情况下，必须从企业证书机构 (CA) 或第三方 CA 导入证书和密钥。如果证书没有指定密钥使用属性，则可以将密钥用于任何目的，包括对消息进行签名。在这种情况下，可以使用任何方法获取证书和密钥对 SAML 消息进行签名。

© 2019 Palo Alto Networks, Inc.

SAML 标识提供商服务器设置	说明
	IdP 证书支持以下算法： • 公钥算法 — RSA（1,024 位或更大）和 ECDSA（所有大小）。FIPS/CC 模式下的防火墙支持 RSA（2,048 位或更大）和 ECDSA（所有大小）。 • **Signature algorithms**（签名算法）— SHA1、SHA256、SHA384 和 SHA512。FIPS/CC 模式下的防火墙支持 SHA256、SHA384 和 SHA512。
标识提供商 SSO URL	输入 IdP 为其单点登录 (SSO) 服务通告的 URL。 如果通过导入元数据文件创建服务器配置文件且该文件指定多个 SSO URL，则防火墙使用指定 POST 或重定向绑定方法的第一个 URL。 *Palo Alto Networks 强烈建议使用依赖 HTTPS 的 URL，尽管 SAML 也支持 HTTP。*
标识提供商 SLO URL	输入 IdP 为其单点注销 (SLO) 服务通告的 URL。 如果通过导入元数据文件创建服务器配置文件且该文件指定多个 SLO URL，则防火墙使用指定 POST 或重定向绑定方法的第一个 URL。 *Palo Alto Networks 强烈建议使用依赖 HTTPS 的 URL，尽管 SAML 也支持 HTTP。*
SSO SAML HTTP 绑定	选择与 **Identity Provider SSO URL**（标识提供商 **SSO URL**）相关联的 HTTP 绑定。防火墙使用绑定将 SAML 消息发送到 IdP。选项如下： • **POST** — 防火墙使用 base64 编码的 HTML 表单发送消息。 • **Redirect**（重定向）— 防火墙在 URL 参数中发送 base64 编码和 URL 编码的 SSO 消息。 *如果导入拥有多个 SSO URL 的 IdP 元数据文件，则防火墙使用使用 POST 或重定向方法的第一个 URL 绑定。防火墙忽略使用其他绑定的 URL。*
SLO SAML HTTP 绑定	选择与 **Identity Provider SLO URL**（标识提供商 **SLO URL**）相关联的 HTTP 绑定。防火墙使用绑定将 SAML 消息发送到 IdP。选项如下： • **POST** — 防火墙使用 base64 编码的 HTML 表单发送消息。 • **Redirect**（重定向）— 防火墙在 URL 参数中发送 base64 编码和 URL 编码的 SSO 消息。 *如果导入拥有多个 SLO URL 的 IdP 元数据文件，则防火墙使用使用 POST 或重定向方法的第一个 URL 绑定。防火墙忽略使用其他绑定的 URL。*
标识提供商元数据	此字段仅在 **Import**（导入）从 IdP 上传到防火墙的 IdP 元数据文件时才显示。该文件指定新 SAML IdP 服务器配置文件的值和签名证书。**Browse**（浏览）到文件，指定配置文件名称和最大时钟偏移，然后单击 **OK**（确定）创建配置文件。或者，可以编辑配置文件以更改导入的值。

© 2019 Palo Alto Networks, Inc.

SAML 标识提供商服务器设置	说明
验证标识提供商证书	选择此选项即可验证信任链和 IdP 签名证书的吊销状态（可选）。 要启用此选项，证书颁发机构 (CA) 必须为您签发 IdP 签名证书。您创建的证书配置文件必须包含颁发 IdP 签名证书的 CA。在身份验证配置文件中，选择 SAML 服务器配置文件和证书配置文件以验证 IdP 证书（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。 如果您的 IdP 签名证书是一个自签名证书，则不存在信任链；因此，您无法启用此选项。无论是否启用 **Validate Identity Provider Certificate**（验证标识提供商证书）选项，防火墙始终都会根据您配置的标识提供商证书验证 SAML 响应或断言的签名。如果您的 IdP 提供自签名证书，请务必使用 PAN-OS 10.0 来降低 CVE-2020-2021 带来的风险。
向 IdP 签署 SAML 消息	选择此选项以指定防火墙对发送到 IdP 的消息进行签名。防火墙使用在身份验证配置文件中指定的 **Certificate for Signing Requests**（签名请求证书）（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。 使用签名证书来确保发送给 *IdP* 的消息的完整性。
最大时钟偏移	输入在防火墙验证从 IdP 接收的消息时 IdP 和防火墙系统时间之间的最大可接受时间差（秒）（范围为 1 至 900，默认为 60）。如果时间差超过此值，则验证（并因此进行身份验证）失败。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> DNS

要简化虚拟系统配置，DNS 服务器配置文件可让您指定要配置的虚拟系统，继承源或 DNS 服务器的主和辅助 DNS 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）。源接口和源地址可用作 DNS 服务器回复的目标接口和目标地址。

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。

DNS 服务器配置文件设置	说明
姓名	DNS 服务器配置文件的名称。
位置	选择要应用配置文件的虚拟系统。
继承源	如果没有继承 DNS 服务器地址，则应选择无。否则，指定配置文件应从中继承设置的 DNS 服务器。
检查继承源状态	单击可查看继承源信息。
主 DNS	指定主 DNS 服务器的 IP 地址。
辅助 DNS	指定辅助 DNS 服务器的 IP 地址。
服务路由 IPv4	如果要指定将数据包转发到以 IPv4 地址为源地址的 DNS 服务器，可选择此选项。
源接口	指定将数据包转发到的 DNS 服务器要使用的源接口。
Source Address（源地址）	指定将数据包转发到的 DNS 服务器用作源地址的 IPv4 源地址。
服务路由 IPv6	如果要指定将数据包转发到以 IPv6 地址为源地址的 DNS 服务器，可选择此选项。
源接口	指定将数据包转发到的 DNS 服务器要使用的源接口。
Source Address（源地址）	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）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Server Profiles（服务器配置文件）> Multi Factor Authentication（多因素身份验证）

使用此页面可配置多因素身份验证 (MFA) 服务器配置文件，以定义防火墙连接到 MFA 服务器的方式。MFA 可以通过确保攻击者无法访问网络并通过折衷单个身份验证因素以防止恣意妄为（如窃取登录凭据）来保护最敏感的资源。配置服务器配置文件后，将其分配给需要身份验证的服务的身份验证配置文件（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。

对于以下身份验证用例，防火墙使用 RADIUS 和 SAML 与多因素身份验证 (MFA) 供应商集成：

- 通过 GlobalProtect™ 门户和网关进行远程用户身份验证。
- PAN-OS 和 Panorama™ Web 界面中的管理员身份验证。
- 通过身份验证策略进行身份验证。

此外，防火墙还可以使用 API 与 MFA 供应商集成，以通过仅适用于最终用户身份验证的身份验证策略来执行 MFA（不适用于 GlobalProtect 身份验证或管理员身份验证）。

除创建服务器配置文件以外，使用完整流程可配置需要额外任务的 *MFA*。

身份验证序列不支持用于指定 *MFA* 服务器配置文件的身份验证配置文件。

如果防火墙通过 *RADIUS* 与 *MFA* 供应商集成，请配置 *RADIUS* 服务器配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> RADIUS）。防火墙通过 *RADIUS* 支持所有 *MFA* 供应商。

MFA 服务器设置	说明
配置文件名称	输入名称以标识服务器（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	在拥有多个虚拟系统 (vsys) 的防火墙中，选择一个虚拟系统或选择 **Shared**（共享）（所有虚拟系统）。保存配置文件后，您无法更改其 **Location**（位置）。
证书配置文件	在建立与服务器的安全连接时，选择 **Certificate Profile**（证书配置文件）可指定防火墙将用于验证 MFA 服务器证书的证书颁发机构 (CA) 证书。有关详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）。

MFA 供应商/值	选择 MFA 供应商的 **MFA Vendor**（**MFA** 供应商），并输入每个供应商属性的 **Value**（值）。属性因供应商而异。如需正确的值，请参阅供应商文档。
	• **Duo v2**：
	  • **API Host**（**API** 主机）— Duo v2 服务器的主机名。
	  • **Integration Key**（集成密钥）和 **Secret Key**（密钥）— 防火墙使用这些密钥对 Duo v2 服务器进行身份验证，并对其发送到服务器的身份验证请求进行签名。要保护这些密钥，防火墙的主密钥自动对其进行加密，以使其明文值不会暴露在防火墙存储中的任何位置。请联系您的 Duo v2 管理员以获取密钥。

© 2019 Palo Alto Networks, Inc.

MFA 服务器设置	说明

	• **Timeout**（超时）— 输入当尝试与 **API Host**（**API** 主机）进行通信时防火墙超时后的时间（秒）（范围为 5 至 600，默认为 30）。此时间间隔必须比 API 主机与用户端点设备之间的超时更长。
	• **Base URI**（基 **URI**）— 如果贵组织托管 Duo v2 服务器的本地身份验证代理服务器，请输入代理服务器 URI（默认为 /auth/v2）。
	• **Okta Adaptive**：
	  • **API Host**（**API** 主机）— Okta 服务器的主机名。
	  • **Base URI**（基 **URI**）— 如果贵组织托管 Okta 服务器的本地身份验证代理服务器，请输入代理服务器 URI（默认为 /api/v1）。
	  • **Token**（令牌）— 防火墙使用此令牌对 Okta 服务器进行身份验证，并对其发送到服务器的身份验证请求进行签名。要保护令牌，防火墙的主密钥自动对其进行加密，以使其明文值不会暴露在防火墙存储中的任何位置。请联系您的 Okta 管理员以获取令牌。
	  • **Organization**（组织）— 贵组织在 **API Host**（**API** 主机）中的子域。
	  • **Timeout**（超时）— 输入当尝试与 **API Host**（**API** 主机）进行通信时防火墙超时后的时间（秒）（范围为 5 至 600，默认为 30）。此时间间隔必须比 API 主机与用户端点设备之间的超时更长。
	• **PingID**：
	  • **Base URI**（基 **URI**）— 如果贵组织托管 PingID 服务器的本地身份验证代理服务器，请输入代理服务器 URI（默认为 /pingid/rest/4）。
	  • **Host name**（主机名）— 输入 PingID 服务器的主机名（默认为 idpxnyl3m.pingidentity.com）。
	  • **Use Base64 Key**（使用 **Base64** 密钥）和 **Token**（令牌）— 防火墙使用密钥和令牌对 PingID 服务器进行身份验证，并对其发送到服务器的身份验证请求进行签名。要保护密钥和令牌，防火墙的主密钥自动对其进行加密，以使其明文值不会暴露在防火墙存储中的任何位置。请联系您的 PingID 管理员以获取值。
	  • **PingID Client Organization ID**（**PingID** 客户端组织 **ID**）— 贵组织的 PingID 标识符。
	  • **Timeout**（超时）— 输入当尝试与 **Host name**（主机名）字段中指定的 PingID 服务器进行通信时防火墙超时后的时间（秒）（范围为 5 至 600，默认为 30）。此时间间隔必须比 PingID 服务器与用户端点设备之间的超时更长。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Local User Database（本地用户数据库）> Users（用户）

您可以在防火墙上设置本地数据库，以存储防火墙管理员、身份验证门户最终用户以及向 GlobalProtect 门户和 GlobalProtect 网关验证身份的最终用户的身份验证信息。本地数据库身份验证不需要外部身份验证服务；您可以在防火墙上执行所有帐户管理。在创建本地数据库和（可选）将用户分配给组后（请参阅 Device（设备）> Local User Database（本地用户数据库）> User Groups（用户组）），可以根据本地数据库选择 Device（设备）> Authentication Profile（身份验证配置文件）。

不能为使用本地数据库身份验证的管理帐户配置 Device（设备）> Password Profiles（密码配置文件）。

要将本地用户 **Add**（添加）到数据库，请按下表所述配置设置。

本地用户设置	说明
姓名	输入名称以标识用户（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用用户帐户的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存用户帐户后，您无法更改其位置。
模式	使用此字段可指定身份验证选项： • 密码 — 输入并确认用户密码。 • 密码哈希— 输入哈希密码字符串。例如，如果要重复使用现有 Unix 帐户的凭据，但不知道明文密码，仅知道哈希密码，则此选项非常有用。无论用于生成哈希值的算法怎样，防火墙接受最多 63 个字符的任何字符串。当防火墙处于正常模式时，操作 CLI 命令 **`request password-hash password`** 使用 MD5 算法；当防火墙处于 CC/FIPS 模式时，该命令使用 SHA256 算法。 您为防火墙（*Device*（设备）> *Setup*（设置）> *Management*（管理））设置的任何最小密码复杂性参数不适用于使用 *Password Hash*（密码哈希）的帐户。
启用	选择此选项可激活用户帐户。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Local User Database（本地用户数据库）> User Groups（用户组）

选择 **Device**（设备）> **Local User Database**（本地用户数据库）> **User Groups**（用户组）可将用户组信息添加到本地数据库。

本地用户组设置	说明
姓名	输入名称以标识组（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	选择在其中使用用户组的范围。在拥有多个虚拟系统 (vsys) 的防火墙的上下文中，选择一个虚拟系统或选择共享（所有虚拟系统）。在任何其他上下文中，您无法选择 **Location**（位置）；其值预定义为共享（防火墙）或为 Panorama。在保存用户组后，您无法更改其位置。
所有本地用户	单击添加以选择要添加到组中的用户。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Scheduled Log Export（计划日志导出）

您可以计划导出日志，并以 CSV 格式将其保存到文件传输协议 (FTP) 服务器，或使用安全复制 (SCP) 在防火墙和远程主机之间安全地传输数据。日志配置文件包含调度和 FTP 服务器信息。例如，配置文件可指定每天凌晨 3 点收集前一天的日志，并将其存储在特定 FTP 服务器上。

单击添加并填写以下详细信息：

已调度日志导出设置	说明
姓名	输入名称以标识配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。 创建配置文件后无法再更改其名称。
说明	输入可选说明（最多 255 个字符）。
启用	选择此选项可启用日志导出计划。
日志类型	选择日志类型（**traffic**（通信）、**threat**（威胁）、**gtp**、**sctp**、**tunnel**（隧道）、**userid**、**auth**、**url**、**data**（数据）、**hipmatch** 或 **wildfire**）。默认为通信。
计划导出开始时间（每天）	使用 24 小时制输入导出开始的时间 (hh:mm)(00:00 - 23:59)。
协议	选择用于将日志从防火墙导出到远程主机的协议： • **FTP** — 此协议不安全。 • **SCP** — 此协议安全。在填写剩余字段后，必须单击 **Test SCP server connection**（测试 **SCP** 服务器连接）以测试防火墙与 SCP 服务器之间的连接，且必须验证和接受 SCP 服务器的主机密钥。
主机名	输入将用于导出的 FTP 服务器的主机名或 IP 地址。
端口	输入 FTP 服务器将使用的端口号。默认为 21。
路径	指定 FTP 服务器上用于存储导出信息的路径。
启用 FTP 被动模式	选择此选项可使用被动模式进行导出。默认情况下，此选项处于选中状态。
用户名	输入用于访问 FTP 服务器的用户名。默认为匿名。
密码/确认密码	输入用于访问 FTP 服务器的密码。如果用户为匿名，则不需要密码。
测试 SCP 服务器连接 （仅限 SCP 协议）	如果将 **Protocol**（协议）设置为 **SCP**，则必须单击此按钮以防火墙和 SCP 服务器之间的连接，然后验证和接受 SCP 服务器的主机密钥。 如果使用 *Panorama* 模板配置日志导出计划，必须在将模板配置提交到防火墙后执行此步骤。在提交模板后，登录到每个防火墙，

© 2019 Palo Alto Networks, Inc.

已调度日志导出设置	说明
	打开日志导出计划，然后单击 *Test SCP server connection*（测试 *SCP* 服务器连接）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Software（软件）

选择 **Device**（设备）> **Software**（软件）可查看可用的软件版本、下载或上传版本、安装版本（需要支持许可证）、从防火墙删除软件映像或查看发行说明。

在升级或降级软件版本之前：

- 检查当前发行说明可查看新功能的说明和版本默认行为的更改以及查看升级软件的迁移路径。
- 查看升级和降级注意事项和《PAN-OS® 10.0 新功能指南》中的升级说明。
- 确保防火墙上的日期和时间设置是当前日期和时间。对 PAN-OS 软件进行数字签名，并在安装新版本之前由防火墙检查该签名。如果防火墙上的日期和时间设置不是当前日期和时间，并且防火墙认为软件签名在将来会出错，则防火墙会显示以下消息：

```
Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into
 PAN software manager.
```

下表提供了有关使用软件页面的帮助。

软件选项字段	说明
版本	列出了 Palo Alto Networks 更新服务器上当前提供的软件版本。要检查 Palo Alto Networks 中是否提供了新的软件发行版，请单击立即检查。防火墙将使用服务路由连接更新服务器，并检查是否有新版本，如果有可用更新，会将这些更新显示在列表顶部。
大小	指示软件映像的大小。
发布日期	指示 Palo Alto Networks 发布新版本的日期和时间。
可用	指示已上传或下载到防火墙的软件映像的相应版本。
当前已安装	指示是激活还是目前在防火墙上运行软件映像的相应版本。
操作	指示可以为对应软件映像采取的操作，如下所示： • **Download**（下载）— 对应的软件版本可从 Palo Alto Networks 更新服务器获取；单击 **Download**（下载）可下载可用的软件版本。 • **Install**（安装）— 已将相应的软件版本下载或上传到防火墙；单击 **Install**（安装）可安装软件。需要重新启动才能完成升级过程。 • **Reinstall**（重装）— 之前已安装相应的软件版本；单击 **Reinstall**（重装）可重装相同版本。
发行说明	提供了指向相应软件更新的发行说明的链接。此链接仅适用于从 Palo Alto Networks 更新服务器下载的更新：不适用于上传的更新。
☒	从防火墙中删除先前下载或上传的软件映像。您只需删除无需升级的较早版本的基本映像。例如，如果运行 7.0，可以删除 6.1 的基本映像，除非您认为可能需要降级。
立即检查	检查 Palo Alto Networks 是否提供了新的软件更新。

© 2019 Palo Alto Networks, Inc.

软件选项字段	说明
上传	从防火墙可以访问的计算机导入软件更新映像。通常情况下，如果防火墙无法访问 Internet（当从 Palo Alto Networks 更新服务器下载更新时需要），可以执行此操作。对于上传，请使用已连接 Internet 的计算机来访问 Palo Alto Networks 站点，从支持站点（软件更新）下载软件映像，下载更新到您的计算机，然后选择防火墙上的 **Device**（设备）> **Software**（软件）并 **Upload**（上传）软件映像。在高可用性 (HA) 配置中，您可选择 **Sync To Peer**（同步到对端）以将导入的软件映像推送到高可用性对端。上传后，**Software**（软件）页面会显示相同的信息（如版本和大小）以及用于上传和下载软件的**Install/Reinstall**（安装/重装）选项。**Release Notes**（发行说明）选项不适用于上传软件。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Dynamic Updates（动态更新）

- Device（设备）> Dynamic Updates（动态更新）
- Panorama > Dynamic Updates（动态更新）

Palo Alto Networks 通过动态更新发布包括新应用程序和修改应用程序、威胁保护和 GlobalProtect 数据文件在内的更新。防火墙可以检索这些更新，并使用这些更新以实施策略，无需更改配置。应用程序和一些防病毒软件的更新无需订阅就可获取；而其他更新则需要订阅。

您可以查看最新更新，阅读各个更新的发行说明，然后选择要下载和安装的更新。还可以恢复到之前安装的更新版本。

为动态更新设置时间表，使您能够定义防火墙检查和下载或安装新更新的频率。特别是对于应用程序和威胁内容更新，您可能需要设置一个时间表，使新应用程序和修改的应用程序更新在威胁更新之后进行；这会让您有更多时间来评估新应用程序和修改应用程序如何影响您的安全策略，同时确保防火墙始终具有最新的威胁防护功能。

动态更新选项	说明
版本	列出了 Palo Alto Networks 更新服务器上当前提供的版本。要检查 Palo Alto Networks 中是否提供了新的软件发行版，请单击立即检查。防火墙将使用服务路由连接更新服务器，并检查是否有新的内容发行版本，如果有可用更新，会将这些更新显示在列表顶部。
最后检查	显示防火墙最后一次连接到更新服务器并检查是否有可用更新的日期和时间。
计划	允许您计划检索更新的频率。 您可定义动态内容更新发生的频率和时间，即 **Recurrence**（重复）和时间，并定义是 **Download Only**（仅下载）还是 **Download and Install**（下载并安装）计划更新 对于防病毒软件及应用程序和威胁更新，您可以选择设置在防火墙安装之前必须可用的内容更新的最短时间阈值。极少情况下，内容更新中可能存在错误，并且此阈值可确保防火墙仅下载指定时间内可在客户环境中使用和运行的内容版本。 对于应用程序和威胁内容更新，您还可以设置一个阈值，专门用于新应用程序和修改应用程序的内容更新。扩展的应用程序阈值使您有更多时间来根据新应用程序和修改的应用程序所作的更改来评估和调整您的安全策略。 对于 WildFire 更新，您可以选择实时检索签名，这样，您可在签名生成时立即访问签名。样本检查期间下载的签名将被保存在防火墙缓存中，可用于快速（本地）查找。此外，为扩大覆盖范围，防火墙还可在启用实时签名后，定期自动下载其他签名数据包。这些补充签名将被添加到防火墙缓存中，且一直可用，直至签名失效，被刷新或被新签名覆盖。 有关如何最佳地启用应用程序和威胁内容更新以实现持续应用程序可用性和最新威胁防护的指导，请查看应用程序和威胁更新的最佳做法。

© 2019 Palo Alto Networks, Inc.

动态更新选项	说明
文件名	列示文件名；其中包括内容版本信息。
功能	列出内容版本可能包含的签名类型。 对于应用程序和威胁内容发行版本，此字段可能会显示用于查看 **Apps, Threats**（应用程序，威胁）的选项。单击此选项可查看自上次在防火墙上安装内容发行版本以来提供的新应用程序签名。您也可以使用 **New Applications**（新建应用程序）对话框，以 **Enable/Disable**（启用/禁用）新应用程序。如果您希望避免唯一标识应用程序对策略造成任何影响，可以选择禁用内容发行版本中包含的新应用程序（如果已确定之前未知的应用程序并对其进行不同分类，则在安装内容之前和之后可能要区别对待应用程序）。
类型	指示下载是完整数据库更新还是增量更新。
大小	显示内容更新数据包的大小。
发布日期	Palo Alto Networks 发布内容发行版本的日期和时间。
已下载	此列中的复选标记指示已将相应内容发行版本下载到防火墙。
当前已安装	此列中的复选标记指示目前正在防火墙上运行相应内容发行版本。
操作	指示可以为对应软件映像采取的操作，如下所示： • **Download**（下载）— 对应的内容版本可从 Palo Alto Networks 更新服务器获取；单击 **Download**（下载）可下载此内容发行版本。如果防火墙无法访问互联网，请使用连接到互联网的计算机访问客户支持门户，然后选择 **Dynamic Updates**（动态更新）。找到您想要的内容发行版本并单击 **Download**（下载）可将更新程序包保存到本地计算机。然后，将软件映射手动 **Upload**（上传）到防火墙。此外，下载应用程序和威胁内容发行版本可启用选项 **Review Policies**（查看策略），这些策略可能会受该版本包含的新应用程序签名影响。 • **Review Policies**（查看策略）（仅限应用程序和威胁内容）— 查看内容发行版本中包含的新应用程序的任何策略影响。使用此选项可评估对在安装内容更新之前和之后接收的应用程序的处理。您还可以使用 Policy Review（查看策略）对话框将待处理应用程序（已通过内容发行版本下载应用程序，但未在防火墙上安装）添加到现有安全策略规则或将其删除；待处理应用程序的策略更改不会生效，直到安装相应内容发行版本。 • **Review Apps**（查看应用程序）（仅限应用程序和威胁内容）— 查看自上次在防火墙上安装内容发行版本以来提供的新应用程序和修改应用程序签名。如果内容更新做出了可能影响关键应用程序执行的更改，则这些应用程序将被标记为建议查看策略。单击“查看策略”可查看内容更新如何影响您的现有安全策略，或者您可以先禁用应用程序，直到有时间查看应用程序的策略影响为止。 • **Install**（安装）— 已将相应的内容版本下载或上传到防火墙；单击 **Install**（安装）可安装此更新。在安装新的应用程序和威胁内容发行版本时，将会提示您使用选项在内容更新中禁用新应用程序。此选项不但可防止最新的威胁，同时还可让您在因新应用程序签名的影响而准备任何策略更新后灵活启用应用程序（要启用之前禁用的应用程序，请选择 Dynamic Updates（动态更新）页面中的 **Apps, Threats**（应用程序，威胁）或选择 **Objects**（对象）> **Applications**（应用程序））。

© 2019 Palo Alto Networks, Inc.

动态更新选项	说明
	• **Revert**（恢复）— 之前已下载相应的内容发行版本。如需重装相同版本，请单击 **Revert**（恢复）。
文档	提供了指向对应版本发行说明的链接。
☒	从防火墙中删除先前下载的内容发行版本。
上传	如果防火墙无法访问 Palo Alto Networks 更新服务器，可以手动从 Dynamic Updates（动态更新）部分中的 Palo Alto Networks 支持站点下载动态更新。将更新下载到计算机后，可将更新 **Upload**（上传）到防火墙。然后，可以选择 **Install From File**（从文件安装），并选择下载的文件。
从文件安装	将更新文件手动上传到防火墙后，使用此选项可安装该文件。在 **Package Type**（数据包类型）下拉列表中，选择要安装更新的类型（**Application and Threats**（应用程序和威胁）、**Antivirus**（防病毒软件）或 **WildFire**），单击 **OK**（确定），选择要安装的文件，然后再单击 **OK**（确定）可启动安装。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Licenses（许可证）

选择 **Device**（设备）> **Licenses**（许可证）可在所有防火墙型号上激活许可证。从 Palo Alto Networks 购买订阅后，将收到一个授权代码，用于激活一个或多个许可证密钥。

在 VM 系列防火墙上，此页可还可让您停用虚拟机 (VM)。

许可证页面上提供了以下操作：

- 从许可证服务器检索许可证密钥：选择此选项可启用需要授权码且已在支持门户上激活的已订购订阅。
- 使用授权代码激活功能：选择此选项可启用需要授权码且之前未在支持门户上激活的已订购订阅。输入授权码，然后单击 **OK**（确定）。
- 手动上传许可证密钥：如果防火墙未连接到许可证服务器且要手动上传许可证密钥，请从 https://support.paloaltonetworks.com 下载许可证密钥文件，然后将其保存在本地。单击 Manually upload license key（手动上传许可证密钥），单击 Browse（浏览），选择文件，然后单击 OK（确定）。

  要为 *URL* 过滤启用许可证，必须安装许可证并下载文件，然后单击激活。如果使用 *PAN-DB* 进行 *URL* 过滤，需要先 *Download*（下载）初始种子数据库，然后单击 *Activate*（激活）。

  您也可运行 *CLI* 命令 ***request url-filtering download paloaltonetworks region < regionname>***。
- 停用 **VM**：此选项可以在具有支持永久和基于期限的许可证的具有自带许可证模型的 VM 系列防火墙上可用；按需许可证模型不支持此功能。如果不再需要 VM 系列防火墙的实例，请单击 **Deactivate VM**（停用 **VM**）。使用此选项可让您释放全部有效许可证 — 订阅许可证、VM 容量许可证和支持授权。许可证会退回到您的帐户，然后您可以在需要时对 VM 系列防火墙的新实例应用许可证。停用许可证后，VM 系列防火墙的功能将处于禁用状态，而防火墙则处于未经许可状态。但是，配置保持不变。
  - 如果 VM 系列防火墙无法直接访问互联网，请单击 **Continue Manually**（手动继续）。防火墙生成令牌文件。单击 **Export license token**（导出许可证令牌）可将令牌文件保存到本地计算机，然后重新启动防火墙。登录到 Palo Alto Networks 支持门户，选择 **Assets**（资产）> **Devices**（设备），然后选择 **Deactivate Vm**（禁用 **VM**）可使用此令牌文件并完成停用过程。
  - 单击 **Continue**（继续）可停用 VM 系列防火墙的许可证。单击立即重新启动以完成许可证停用过程。
  - 如果要取消并关闭 Deactivate VM（停用 VM）窗口，请单击 **Cancel**（取消）。
- **Upgrade VM Capacity**（升级 **VM** 容量）：此选项可让您升级当前许可的 VM 系列防火墙的容量。升级容量后，VM 系列防火墙会保留升级之前的所有配置和订阅。
  - 如果防火墙已连接到许可证服务器 — 选择 **Authorization Code**（授权码），在 Authorization Code（授权码）字段中输入授权码，并单击 **Continue**（继续）以启动容量升级。
  - 如果防火墙未连接到许可证服务器 — 选择 **License Key**（许可证密钥），单击 **Complete Manually**（手动完成）以生成令牌文件，并将令牌文件保存到本地计算机。然后，登录到 Palo Alto Networks 支持门户，选择 **Assets**（资产）> **Devices**（设备），然后选择 **Deactivate License(s)**（停用许可证）以使用令牌文件。将 VM 系列防火墙的许可证密钥下载到本地计算机，并将许可证密钥添加到防火墙，然后单击 **Continue**（继续）以完成容量升级。
  - 如果防火墙已连接到许可证服务器但没有授权码 — 选择 **Fetch from license server**（从许可证服务器获取），在尝试升级容量之前升级许可证服务器的防火墙容量许可证，然后在验证许可证服务器的许可证已升级后，单击 **Continue**（继续）以启动容量升级。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Support（支持）

- Device（设备）> Support（支持）
- Panorama > Support（支持）

选择 **Device**（设备） > **Support**（支持）或 **Panorama** > **Support**（支持）可访问支持的相关选项。您可以根据防火墙的序列号查看 Palo Alto Networks 联系信息、查看支持到期日期，以及查看 Palo Alto Networks 中的产品和安全警报。

在此页面上执行以下任何功能：

- **Support**（支持）— 提供有关设备支持状态的信息和使用授权码激活支持的链接。
- 生产警报/应用程序和威胁警报— 访问或刷新此页面时会从 Palo Alto Networks 更新服务器中检索这些警报。要查看生产警报、应用程序和威胁警报的详细信息，请单击警报名称。如果存在与指定发行版相关的大范围召回或紧急问题，将发布生产警报。如果发现重大威胁，将发布应用程序和威胁警报。
- **Links**（链接）— 提供常用支持链接，以帮助您管理设备并访问支持联系信息。
- **Tech Support File**（技术支持文件）— 单击 **Generate Tech Support File**（生成技术支持文件）可生成系统文件，支持团队可使用此文件帮助诊断使用防火墙时遇到的问题。生成此文件后，请单击 **Download Tech Support File**（下载技术支持文件），然后将其发送到 Palo Alto Networks 支持部门。

  如果浏览器已配置在文件下载后自动打开，您应关闭此选项，以使浏览器仅下载支持文件，而不会尝试对其进行打开和提取操作。
- **Stats Dump File**（统计转储文件）（仅限防火墙）— 单击 **Generate Stats Dump File**（生成统计转储文件）可生成一组 XML 报告，该组报告会对过去 7 天内的网络通信进行汇总。生成报告后，您可选择 **Download Stats Dump File**（下载统计转储文件）。Palo Alto Networks 或授权合作伙伴系统工程师将使用此报告生成安全生命周期审查 (SLR)。SLR 通常用作评估流程的一部分，会突出显示网络中发现的问题以及可能存在的相关业务或安全风险 。有关 SLR 的更多信息，请联系 Palo Alto Networks 或授权合作伙伴系统工程师。
- **Core Files**（核心文件）— 如果防火墙遇到系统进程故障，它将生成一个核心文件，其中包含有关进程及其失败原因的详细信息。单击 **Download Core Files**（下载核心文件）链接可查看可用核心文件列表，然后单击核心文件名以下载。下载文件后，将其上传到 Palo Alto Networks 支持案例以获取解决问题的帮助。

  核心文件的内容只能由 *Palo Alto Networks* 支持工程师解释。

© 2019 Palo Alto Networks, Inc.

Device（设备）> Master Key and Diagnostics（主密钥和诊断）

- **Device**（设备）> **Master Key and Diagnostics**（主密钥和诊断）
- **Panorama** > **Master Key and Diagnostics**（主密钥和诊断）

编辑加密防火墙或 Panorama 的所有密码和私钥的主密钥（如用于对访问 CLI 的管理员进行身份验证的 RSA 密钥）。加密密码和密钥通过确保其明文值不会暴露在防火墙或 Panorama 上的任何位置来提高安全性。

恢复默认主密钥的唯一方法是执行出厂重置。

Palo Alto Networks 建议您配置新的主密钥而不是使用默认密钥，将密钥存储在安全位置，并定期更改密钥。为了增强隐私性，您可以使用硬件安全模块来加密主密钥（请参阅 Device（设备）> Setup（设置）> HSM）。在每个防火墙或 Panorama 管理服务器上配置一个唯一的主密钥，可确保已获得某个设备的主密钥的攻击者无法访问任何其他设备的密码和私钥。但是，在以下情况下，您必须在多个设备上使用相同的主密钥：

- **High availability (HA) configurations**（高可用性 **(HA)** 配置）— 如果在 HA 配置中部署防火墙或 Panorama，可同时在对中的防火墙或 Panorama 管理服务器上使用相同的主密钥。否则，HA 同步不起作用。
- **Panorama pushes configurations to firewalls**（**Panorama** 将配置推送到防火墙）— 如果使用 Panorama 将配置推送到受管防火墙，可在 Panorama 和受管防火墙上使用相同的主密钥。否则，Panorama 的推送操作将失败。

要配置主密钥，请编辑 Master Key（主密钥）设置，并使用下表确定适当的值：

主密钥和诊断设置	说明
主密钥	启用以配置唯一主密钥。禁用（取消选择）以使用默认主密钥。
当前主密钥	指定当前用来对防火墙中所有私钥和密码进行加密的密钥。
新主密钥 确认主密钥	要更改主密钥，请输入长度为 16 个字符的字符串，并确认新密钥。
生命周期	指定主密钥过期之前的 **Days**（天）数和 **Hours**（小时）数。范围为 1 到 438,000 天（50 年）。 您必须在当前密钥过期之前配置新主密钥。如果主密钥过期，防火墙或 Panorama 在维护模式下自动重新启动。然后，必须执行出厂重置。 根据设备执行加密的个数，将 *Lifetime*（生命周期）设为两年或更短。设备执行的加密次数越多，则应设置更短的*Lifetime*（生命周期）。关键的考虑因素在于唯一加密次数不会在更改主密钥之前用完。每个主密钥最多可提供 *2^^32* 个唯一加密，然后加密会重复，从而造成安全风险。 设置主密钥 *Time for Reminder*（提醒时间），并在出现提醒通知后，更改主密钥。

© 2019 Palo Alto Networks, Inc.

主密钥和诊断设置	说明
提醒时间	输入在防火墙生成过期警报时主密钥过期之前的 **Days**（天）数和 **Hours**（小时）数。防火墙自动打开系统警报对话框以显示警报。 设置提醒，以便其在计划维护时间窗口中过期之前，您有充足的时间配置新的主密钥。一旦达到 *Time for Reminder*（提醒时间）且防火墙或 *Panorama* 发送了通知日志，就立即更改主密钥，不要等到 *Lifetime*（生命周期）结束。对于已分组设备，跟踪每个设备（例如，*Panorama* 管理的防火墙以及防火墙 *HA* 对），并在组内任何设备达到提醒时间时，更改主密钥。 要确保显示过期警报，请选择 *Device*（设备）> *Log Settings*（日志设置），然后编辑警报设置并 *Enable Alarms*（启用警报）。
保存在 HSM 上	仅当主密钥是在硬件安全模块 (HSM) 上进行加密时才启用此选项。不能在诸如 DHCP 客户端或 PPPoE 之类的动态接口上使用 HSM。 在高可用性模式下，对端防火墙之间的 HSM 配置不会同步。因此，HA 对中的每个对等都可以连接到不同的 HSM 源。如果您使用 Panorama 且需要两个对端上配置保持同步，请使用 Panorama 模板配置受管防火墙的 HSM 源。 PA-220 不支持 HSM。
自动续订主密钥	启用以自动续订指定天数和小时数的主密钥。禁用（取消选择）以允许主密钥在配置密钥生命周期结束后过期。 指定延长主密钥加密的 **Days**（天）数和 **Hours**（小时）数，从而 **Auto Renew with Same Master Key**（使用相同主密钥自动续订）（范围为 1 小时到 730 天）。 如果启用 *Auto Renew Master Key*（自动续订主密钥），请进行设置，确保总时间（生命周期 + 自动续订时间）不会使设备用完唯一加密。例如，如果您认为设备将在两年半的时间内用完主密钥的唯一加密次数，您可以将*Lifetime*（生命周期）设为两年，将*Time for Reminder*（提醒时间）设为 *60* 天，将*Auto Renew Master Key*（自动续订主密钥）设为 *60-90* 天，这样，您可以在*Lifetime*（生命周期）到期前有额外的时间配置新的主密钥。但是，最佳做法仍是在生命周期到期前更改主密钥，确保设备不会重复使用加密。
常见标准	在常见标准模式下，可以使用其他选项运行加密算法自检和软件完整性自检。还包括一个计划程序，可用于指定两个自检的运行时间。

部署主密钥

部署主密钥，或是直接更新 Panorama 受管防火墙、日志收集器、或 WF-500 设备的现有主密钥。

字段	说明
部署主密钥	

© 2019 Palo Alto Networks, Inc.

字段	说明
Filter（筛选器）	根据平台、设备组、模板、标记、HA 状态或软件版本过滤要显示的受管设备。
设备名称	受管防火墙的名称。
软件版本	受管防火墙上运行的软件版本。
STATUS（状态）	受管设备的连接状况：可能是 `Connected`、`Disconnected` 或 `Unknown`。
部署主密钥操作状态	
设备名称	受管防火墙的名称。
STATUS（状态）	主密钥部署操作的状态。
结果	主密钥部署操作的结果。可能是 `OK` 或 `FAIL`。
进度	主密钥部署操作的进度 (%)。
详细信息	主密钥部署操作相关的详细信息。如果操作失败，则会在此处显示描述失败原因的详细信息。
Summary（摘要）	
进度	显示指示主密钥部署操作进度的进度条。将显示以下信息： • **Results Succeeded**（结果成功）— 成功部署主密钥的设备数。 • **Results Pending**（结果待定）— 当前主密钥部署操作处于待定状态的设备数。 • **Results Failed**（结果失败）— 主密钥部署操作失败的设备数。

© 2019 Palo Alto Networks, Inc.

Device（设备） > Policy Recommendation（策略建议）

从 IoT 安全应用程序查看策略规则建议相关的信息。策略规则建议使用防火墙从网络流量收集的元数据来确定设备允许的行为。您可以在 **Device**（设备） > **Dynamic Updates**（动态更新） > **Device-ID Content**（设备 **ID** 内容）中检查策略规则建议版本。

按钮/字段	说明
策略导入详细信息	查看策略规则建议的详细信息，例如，设备组 **Location**（位置）、**rule name**（规则名称）、导入策略的 **user**（用户）、策略规则建议是否 **Is Updated**（已更新）、策略规则建议导入时间以及策略规则建议上次更新的时间。
设备配置文件	用于策略规则建议中源设备的设备配置文件。
源区域	策略规则建议的源区域。
地址	策略规则建议的源地址。
位置	该策略规则建议可用的 Panorama 上的设备组。
目标设备配置文件	防火墙允许用于策略规则建议的目标设备配置文件。
设备 IP	策略规则建议允许的设备的 IP 地址。
FQDN	策略规则建议基于典型的设备行为，将其标识为允许的完全限定域名(FQDN)。
目标区域	策略规则建议允许的目标区域。
安全配置文件	策略规则建议允许的安全配置文件。
服务	策略规则建议允许的服务（例如 `ssl`）。
URL 类别	策略规则建议允许的 URL 过滤类别。
应用程序	策略规则建议允许的应用程序。
标记	用于标识策略规则建议的策略规则的标记。 请勿更改策略规则标记；一旦更改标记，防火墙将无法重建策略映射。
内部设备	用于识别设备来源于网络内部区域（是）还是来源于面向 Internet 的外部区域（否）。

© 2019 Palo Alto Networks, Inc.

按钮/字段	说明
活动建议	用于识别此策略规则建议是处于活动状态且正在安全策略中使用，还是已从安全策略中删除。
操作	用于识别此策略规则建议的操作（默认为允许）。
新更新可用	用于识别是否此策略规则建议存在您必须从 IoT 安全应用程序中导入的新更新。导入策略规则建议更新时，防火墙自动更新安全策略规则。如果有多个设备组，那么，在您导入策略规则建议更新到所有设备组之前，该值仍为 `Yes`（是）。
导入策略	使用 IoT 安全应用程序 **Activate**（激活）策略规则建议后，请 **Import Policy**（导入策略）以导入策略规则建议，并将其用于安全策略规则中。
删除策略映射	如果设备不再需要策略规则建议，请从设备中**Remove Policy Mapping**（删除策略映射）。 您还必须删除策略规则建议的策略规则。
重建所有映射	如果映射不同步（例如，如果您还原以前的配置），那么，您可以 **Rebuild All Mappings**（重建所有映射）以恢复策略规则建议映射。

用户标识

用户标识 (User-ID™) 是 Palo Alto Networks® 新一代防火墙的一个功能，可与各类企业目录和终端服务无缝集成，以将应用程序活动和策略绑定至用户名和组，而不仅仅是 IP 地址。配置 User-ID 还能使应用程序命令中心 (ACC)、App Scope、报告和日志都将包含用户名和用户 IP 地址。

> Device（设备）> User Identification（用户标识）> User Mapping（用户映射）
> Device（设备）> User Identification（用户标识）> Connection Security（连接安全性）
> Device（设备）> User Identification（用户标识）> Terminal Server Agents（终端服务器代理）
> Device（设备）> User Identification（用户标识）> Group Mapping Settings（组映射设置）
> Device（设备）> User Identification（用户标识）> Authentication Portal Settings（身份验证门户设置）

了解更多？

请参阅 User-ID

Device（设备）> User Identification（用户标识）> User Mapping（用户映射）

配置在防火墙上运行的 PAN-OS 集成 User-ID 代理，以将 IP 地址映射到用户名。

您在查找什么内容？	请参阅：
配置 PAN-OS 集成 User-ID 代理。	Palo Alto Networks User-ID 代理设置
管理对 User-ID 代理监控的服务器的访问权限，以获取用户映射信息。	监控服务器
管理防火墙在将 IP 地址映射到用户时包括或排除的子网。	包括或排除用户映射的子网
了解更多？	使用 PAN-OS 集成的 User-ID 代理来配置用户映射。

Palo Alto Networks User-ID 代理设置

这些设置定义 User-ID 代理用于执行用户映射的方法。

您在查找什么内容？	请参阅：
启用 User-ID 代理使用 Windows 管理规范 (WMI) 探测 HTTP 或 HTTPS 上的客户端系统和 Windows 远程管理 (WinRM)，以获取用户映射信息。	服务器监视账户
使用 User-ID 代理监控服务器日志以获取用户映射信息。	服务器监视
启用 User-ID 代理探测客户端系统，以获取用户映射信息。	客户端探测
确保用户在漫游并获取新 IP 地址时，防火墙具有最新的用户映射信息。	缓存
配置 User-ID 代理解析 Syslog 消息，以获取用户映射信息。	Syslog 筛选器
配置 User-ID 代理省略来自映射进程的特定用户名。	忽略用户列表

© 2019 Palo Alto Networks, Inc.

服务器监视账户

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Server Monitor Account**（服务器监控账户）

要配置 PAN-OS 集成 User-ID 代理使用 Windows 管理规范 (WMI) 探测 HTTP 或 HTTPS 上的客户端系统和 Windows 远程管理 (WinRM)，以获取用户映射信息，请填写下列字段。

此外，您还可以通过配置 Kerberos 服务器配置对受监控服务器的访问权限，以使用 HTTP 或 HTTPS 上的 Windows 远程管理 (WinRM) 对服务器监视进行身份验证。

由于 *WMI* 探测是从端点报告信任数据，因此 *Palo Alto Network* 建议您不要使用此方法在高安全性网络中获取 *User-ID* 映射信息。如果您配置 *User-ID* 代理通过解析 *Active Directory (AD)* 安全事件日志或 *syslog* 消息，或使用 *XML API* 来获取映射信息，*Palo Alto Networks* 建议您禁用 *WMI* 探测。

如果您使用 *WMI* 探测，请不要在外部不可信接口上启用它。这样会导致代理在网络外部发送包含敏感信息的 *WMI* 探测，如 *User-ID* 代理服务帐户的用户名、域名和密码哈希。攻击者可能会潜在利用此信息渗透并进一步访问您的网络。

Active Directory 身份验证设置	说明
用户名	为防火墙将用于访问 Windows 资源的帐户输入域凭据（**User Name**（用户名）和 **Password**（密码））。此帐户需要权限才能执行客户端计算机上的 WMI 查询，并监控 Microsoft Exchange 服务器和域控制器。使用 **User Name**（用户名）的域/用户名语法。如果您配置对受监控服务器的访问权限使用 Kerberos 对服务器进行身份验证，请输入 Kerberos 用户主体名称(UPN)。
域的 DNS 名称	输入受控服务器的 DNS 名称。如果您配置对受监控服务器的访问权限使用 Kerberos 对服务器进行身份验证，请输入 Kerberos Realm 域。如果在您配置对受监控服务器的访问权限使用 **WinRM-HTTP** 作为传输协议，则必须配置该设置。
密码/确认密码	为防火墙用于访问 Windows 资源的账户输入密码，并确认。
Kerberos 服务器配置文件	选择可控制对 Realm 访问的 Kerberos 服务器的 Kerberos 服务配置文件，以使用 HTTP 或 HTTPS 上的 WinRM 从受控服务器检索安全日志和会话信息。

除定义 *Active Directory* 身份验证设置以外，配置 *PAN-OS* 集成 *User-ID* 代理以监控服务器和探测客户端的完整流程需要执行附加任务。

服务器监视

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Server Monitor**（服务器监控）

要启用 User-ID 代理通过搜索服务器安全事件日志中的登录事件将 IP 地址映射到用户名，请配置下表中所述的设置。

如果对 *Windows* 服务器日志、*Windows* 服务器会话或 *eDirectory* 服务器的查询负载很高，则观察到的查询之间的延迟可能明显超出指定的频率或时间间隔。

© 2019 Palo Alto Networks, Inc.

除配置服务器监控设置以外，配置 *PAN-OS* 集成 *User-ID* 代理监控服务器的完整流程需要执行附加任务。

服务器监控设置	说明
启用安全日志	选择此选项可启用 Windows 服务器上的安全日志监控。
服务器日志监控频率（秒）	指定防火墙查询 Windows 服务器安全日志以获取用户映射信息的频率（以秒为单位，范围为 1-3600，默认为 2）。这是防火墙完成处理最后一条查询与发送下一条查询之间的时间间隔。 如果日志监控不是经常发生，则最新的 *IP* 地址到用户映射可能不可用。如果防火墙经常监控日志，这会影响域控制器、内存、*CPU* 和 *User-ID* 策略实施。从 *2-30* 秒范围的值开始，然后，根据性能影响或用户映射更新频率修改该值。
启用会话	选中此选项可启用受监控服务器上的用户会话监控。每次用户与服务器连接时都会创建一个会话；防火墙可用此信息来标识用户 IP 地址。 请不要 *Enable Session*（启用会话）。此设置要求 *User-ID* 代理具有拥有服务器操作员权限的 *Active Directory* 帐户，以便它可以读取所有用户会话。相反，您应使用 *Syslog* 或 *XML API* 集成监控捕获所有设备类型和操作系统（而不仅仅是 *Windows* 操作系统）的登录和注销事件的来源，如无线控制器和 *NAC*。
服务器会话读取频率（秒）	指定防火墙查询 Windows 服务器用户会话以获取用户映射信息的频率（以秒为单位，范围为 1-3600，默认为 10）。这是防火墙完成处理最后一条查询与开始下一条查询之间的时间间隔。
Novell eDirectory 查询间隔（秒）	指定防火墙查询 Novell eDirectory 服务器以获取用户映射信息的频率（以秒为单位，范围为 1-3600，默认为 30）。这是防火墙完成处理最后一条查询与开始下一条查询之间的时间间隔。
Syslog 服务配置文件	选择 SSL/TLS 服务配置文件，该配置文件用于指定防火墙与 User-ID 代理监控的任何 Syslog 发件人之间进行通信所需要的证书和 SSL/TLS 版本。有关详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）和 Syslog 筛选程序。如果选择 **None**（无），防火墙将使用其预定义的自签名证书。

客户端探测

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Client Probing**（客户端探测）

您可配置 User-ID 代理，对用户映射进程识别的各个客户端系统执行 WMI 客户端检测。User-ID 代理将定期探测每个获悉的 IP 地址，以验证同一用户在登录。如果遇到没有用户映射的 IP 地址，防火墙会将该地址发送至代理以立即进行探测。如需配置客户端探测设置，请填写以下字段。

© 2019 Palo Alto Networks, Inc.

请不要在高安全性网络中启用客户端探测。请不要在外部不可信接口中启用客户端探测。客户端探测可能会产生大量网络流量，在配置错误时可能会造成安全威胁。如果在外部不可信区域启用客户端探测，则会允许攻击者在您的网络外面发送探测，并导致 *User-ID* 代理服务账户名称、域名和加密密码哈希泄漏。相反，从多个孤立和可信的来源（如域控制器）以及通过与 *Syslog* 或 *XML API* 集成来收集用户映射信息，这能够让您从任何设备类型或操作系统安全地捕获用户映射信息，而不只是从 *Windows* 客户端收集。

除配置客户端探测设置以外，配置 *PAN-OS* 集成 *User-ID* 代理探测客户端的完整流程需要执行附加任务。

PAN-OS 集成 *User-ID* 代理不支持 *NetBIOS* 探测，但 基于 Windows 的 User-ID 代理支持。

客户端探测设置	说明
启用探测	选择此选项可启用 WMI 探测。
探测间隔时间（分钟）	输入以分钟为单位的探测间隔时间（范围为 1-1440，默认为 20）。防火墙完成处理最后一条请求与开始下一条请求之间的时间间隔。 在大型部署中，必须正确设置探测间隔，以便具有足够的时间探测用户映射进程已标识的每个客户端。例如，如果具有 6,000 个用户且间隔为 10 分钟，则需要从每个客户端每秒执行 10 次 WMI 请求。 如果探测请求负载很高，则观察到的请求之间的延迟可能明显超出指定的时间间隔。

缓存

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Cache**（缓存）

要确保用户在漫游并获取新 IP 地址时，防火墙具有最新的用户映射信息，请配置超时，以便从防火墙缓存中清除用户映射：此超时适用于通过除身份验证门户以外的任何方法获得的用户映射。对于通过身份验证门户获得的映射，请在身份验证门户设置中设置超时（Device（设备）> User Identification（用户标识）> Authentication Portal Settings（身份验证门户设置）、**Timer**（计时器）和 **Idle Timer**（空闲计时器）字段）。

要匹配从 User-ID 源收集的用户名（即使未包含域），请配置防火墙以允许匹配不包含域的用户名。如果不需要跨域复制公司/组织中的用户名，则仅使用此选项。

缓存设置	说明
启用用户标识超时	选择此选项可启用用户映射条目的超时值。某一条目达到此超时值后，防火墙会将其清除并收集新映射。这将确保用户在漫游并获取新 IP 地址时，防火墙具有最新的信息。 启用超时，确保防火墙拥有最新的用户到 *IP* 地址映射信息。
用户标识超时（分钟）	设置以分钟为单位的用户映射条目的超时值（范围为 1 至 3,600，默认为 45）。

© 2019 Palo Alto Networks, Inc.

缓存设置	说明
	设置超时值为 *DHCP* 租赁的半衰期或 *Kerberos* 票据生命周期。 如果配置防火墙重新分发映射信息，则每个防火墙将根据您在该防火墙上设置的超时（而非在转发防火墙上设置的超时）清除其接收到的映射条目。
允许匹配不包含域的用户名	如果域不是由 User-ID 源提供，请选择此选项以允许防火墙匹配用户。为防止用户被错误标识，如果不需要跨域复制您的用户名，请选择此选项。 在启用此选项之前，请验证防火墙是否已从 *LDAP* 服务器获取组映射。

重新分发

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Redistribution**（重新分发）

要启用防火墙或虚拟系统用作重新分发用户映射信息以及与身份验证质询相关联的时间戳的 User-ID 代理，请配置下表中所述的设置。当您以后将此防火墙连接到将接收映射信息和时间戳的设备（如 Panorama）时，设备使用这些字段将防火墙或虚拟系统标识为 User-ID 代理。

除指定重新分发设置以外，配置防火墙重新分发用户映射信息和身份验证时间戳的完整流程需要执行附加任务。

默认情况下，具有多个虚拟系统的防火墙不会在其多个虚拟系统之间重新分发用户映射信息，尽管您可以配置它们进行重新分发。

重新分发设置	说明
收集器名称	输入用于将防火墙或虚拟系统标识为 User-ID 代理的收集器名称（最多 255 个字母数字字符）。
预共享密钥/确认预共享密钥	输入用于将防火墙或虚拟系统标识为 User-ID 代理的预共享密钥（最多 255 个字母数字字符）。

Syslog 筛选器

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Syslog Filters**（**Syslog** 筛选程序）

User-ID 代理使用 Syslog 解析配置文件筛选代理进行监控以获取 IP 地址到用户名的映射信息的 syslog 发件人发送的 syslog 消息（请参阅配置对受监控服务器的访问权限）。每个配置文件都可以解析以下任一种事件类型的 syslog 消息，但不能同时解析两种事件类型的 syslog 消息：

- 身份验证（登录）事件 — 用于将用户映射添加到防火墙。
- 注销事件 — 用于删除不再是当前的用户映射。在 IP 地址分配经常会更改的环境中，删除过时的映射很有用。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks 通过应用程序内容更新为防火墙提供预定义的 Syslog 解析配置文件。要在供应商开发新过滤器时动态更新配置文件列表，请计划这些动态内容更新（请参阅 Device（设备）> Dynamic Updates（动态更新））。预定义配置文件是防火墙的全局配置文件，而您配置的自定义配置文件仅适用于在 **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）中选择的虚拟系统（**Location**（位置））。

Syslog 消息必须符合以下条件 User-ID 代理才能进行解析：

- 每个消息都必须是单行文本字符串。新行 (\n) 或回车加上新行 (\r\n) 是换行符的分隔符。
- 单个消息的最大大小为 8000 字节。
- 通过 UDP 传送的消息必须包含于单个数据包中；通过 SSL 传送的 Syslog 消息可跨多个数据包。单个数据包可能包含多个消息。

要配置自定义配置文件，请单击 **Add**（添加）并按下表所述指定设置。此表中的字段说明使用以下格式的 syslog 消息中的登录事件示例：

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain
\johndoe_4 Source:192.168.0.212
```

除创建 *Syslog* 解析配置文件以外，配置 *User-ID* 代理解析用户映射信息的 *syslog* 发件人的完整流程需要执行附加任务。

字段	说明
系统日志解析配置文件	输入配置文件的名称（最多 63 个字母数字字符）。
说明	输入配置文件的说明（最多 255 个字母数字字符）。
类型	指定用于过滤用户映射信息的解析类型： • **Regex Identifier**（正则表达式标识符）— 使用 **Event Regex**（事件正则表达式）、**Username Regex**（用户名正则表达式）和 **Address Regex**（地址正则表达式）字段来指定描述搜索模式的正则表达式 (regex)，以从系统日志消息中标识并提取用户映射信息。防火墙使用此正则表达式来匹配 syslog 消息中的身份验证或注销事件，并用于与其匹配消息中的用户名和 IP 地址进行相匹配。 • **Field Identifier**（字段标识符）— 使用 **Event String**（事件字符串）、**Username Prefix**（用户名前缀）、**Username Delimiter**（用户名分隔符）、**Address Prefix**（地址前缀）、**Address Delimiter**（地址分隔符）和**Addresses Per Log**（每个日志地址）字段来指定字符串，以便匹配身份验证或注销事件并标识系统日志消息中的用户映射消息。 对话框中的其余字段根据您的选择而有所不同。按照以下行所述配置字段。
事件正则表达式	输入用于标识身份验证成功或注销事件的正则表达式。对于与此表一起使用的消息示例，正则表达式 **`(authentication\ success) {1}`** 提取字符串 `authentication success` 的第一个 **`{1}`** 实例。空格之前的反斜杠是标准的正则表达式转义符，表示正则表达式引擎不会将空格视为特殊字符。
用户名正则表达式	输入用于标识身份验证成功或注销消息中用户名字段的正则表达式。对于与此表一起使用的消息示例，正则表达式 **`User:([a-zA-Z0-9\\`**

© 2019 Palo Alto Networks, Inc.

字段	说明
	\._]+) 会匹配字符串 User:johndoe_4，并且会将 acme\johndoe1 提取为用户名。
地址正则表达式	输入用于标识身份验证成功或注销消息的 IP 地址部分的正则表达式。在与此表一起使用的消息示例中，正则表达式 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** 会匹配 IPv4 地址 Source:192.168.0.212，并在用户名映射中添加 192.168.0.212 作为 IP 地址。
事件字符串	输入用于标识身份验证成功或注销消息的匹配字符串。对于与此表一起使用的消息示例，您可以输入字符串 **authentication success**。
用户名前缀	输入用于标识身份验证或注销 syslog 消息中用户名字段的开头部分的匹配字符串。该字段不支持正则表达式，如 **\s**（对于空格）或 **\t** （对于制表符）。在与此表一起使用的消息示例中，User: 标识用户名字段的开头。
用户名分隔符	输入用于标记身份验证或注销消息中用户名字段的结尾部分的分隔符。使用 \s 标识独立空格（如示例消息中）和 \t 表示选项卡。
地址前缀	输入用于标识 syslog 消息中 IP 地址字段的开头部分的匹配字符串。该字段不支持正则表达式，如 **\s**（对于空格）或 **\t** （对于制表符）。在与此表一起使用的消息示例中，Source: 标识地址字段的开头。
地址分隔符	输入用于标记身份验证成功或注销消息中 IP 地址字段的结尾部分的匹配字符串。例如，输入 **\n** 以表示分隔符为换行符。
每个日志的地址	输入您想让防火墙解析的最大 IP 地址数（范围为 1-3；默认为 1）。

忽略用户列表

- **Device**（设备）> **User Identification**（用户标识）> **User Mapping**（用户映射）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理设置）> **Ignore User List**（忽略用户列表）

用户忽略列表定义哪些用户帐户不要求 IP 地址到用户名的映射（如 Kiosk 帐户）。要配置此列表，请单击 **Add**（添加）并输入一个用户名。您可将星号用作通配符，以匹配多个用户名，但仅可用作该条目中的最后一个字符。例如，**corpdomain\it-admin*** 将匹配 **corpdomain** 域中用户名以字符串 **it-admin** 开头的所有管理员。您最多可添加 5,000 个条目，以从用户映射中进行排除。

在充当 *User-ID* 代理（而不是客户端）的防火墙上定义忽略用户列表。如果在客户端防火墙上定义忽略用户列表，在重新分发期间，列表中的用户仍会进行映射。

监控服务器

- Device（设备）> User Identification（用户标识）> User Mapping（用户映射）

使用 Server Monitoring（服务器监控）部分可定义 Microsoft Exchange 服务器、Active Directory (AD) 域控制器、Novell eDirectory 服务器或 User-ID 代理监控登录事件的 Syslog 发件人。

- 配置对受监控服务器的访问权限
- 管理对受监控服务器的访问权限
- 包括或排除用户映射的子网

© 2019 Palo Alto Networks, Inc.

配置对受监控服务器的访问权限

使用服务器监控部分 **Add**（添加）指定防火墙将监控的服务器的服务器配置文件。

至少配置两个受 *User-ID* 监控的服务器，这样，如果其中有一个服务器出现故障，防火墙仍能知悉 *IP* 地址到用户名的映射。

除创建服务器配置文件以外，配置 *PAN-OS* 集成 *User-ID* 代理监控服务器的完整流程需要执行附加任务。

服务器监控设置	说明
姓名	输入服务器的名称。
说明	输入服务器的说明。
已启用	选择此选项可启用此服务器的日志监控。
类型	选择服务器类型。所作选择将决定此对话框会显示哪些其他字段。 • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • **Syslog** 发件人
传输协议（仅限 Microsoft Active Directory 和 Microsoft Exchange）	选择传输协议： • **WMI** —（默认）使用 Windows 管理规范 (WMI)探测已获得的每个 IP 地址，并验证是否同一用户仍保持登录状态。 • **Win-RM-HTTP** — 通过 HTTP 使用 Windows 远程管理 (WinRM) 检测服务器上的安全日志和会话信息。此选项需要使用 服务器监视账户 中的 Kerberos **Domain's DNS Name**（域的 **DNS** 名）。 • **Win-RM-HTTPS** — 通过 HTTPS 使用 Windows 远程管理 (WinRM)检测服务器上的安全日志和会话信息。要在使用 Kerberos 身份验证时使用 Windows 服务器对服务器证书进行验证，确保已在 全局服务设置中配置 NTP，并选择根 CA 作为证书配置文件（Device（设备）> User Identification（用户标识）> Connection Security（连接安全性））。
网络地址	输入受监控服务器的 IP 地址或 FQDN。如果使用 Kerberos 进行服务器身份验证，则必须输入 FQDN。如果 **Type**（类型）为 **Novell eDirectory**，则此选项不适用。
服务器配置文件 （仅限 Novell eDirectory）	选择用于连接到 Novell eDirectory 服务器的 LDAP 服务器配置文件（Device（设备）> Server Profiles（服务器配置文件）> LDAP）。
连接类型 （仅限 Syslog 发件人）	选择 User-ID 代理是否会侦听 **UDP** 端口 (514) 或 **SSL** 端口 (6514) 上的 Syslog 消息。如果选择 **SSL**，则在启用服务器监控时选择的 **Syslog Service Profile**（**Syslog** 服务配置文件）将确定允许的 SSL/TLS 版本，以及防火墙用于保护与 Syslog 发件人的连接的证书。 作为安全最佳做法，在使用 *PAN-OS* 集成 *User-ID* 代理将 *IP* 地址映射到用户名时时，请选择 *SSL*。如果选择 *UDP*，请确保 *Syslog* 发件人和客户

© 2019 Palo Alto Networks, Inc.

服务器监控设置	说明
	端均在某个专用的安全网络上，以防止不可信主机向防火墙发送 *UDP* 流量。
Filter（筛选器） （仅限 Syslog 发件人）	如果服务器 **Type**（类型）为 **Syslog Sender**（**Syslog** 发件人），则 **Add**（添加）一个或多个 Syslog 解析配置文件，用于从此服务器接收的 Syslog 消息中提取用户名和 IP 地址。您可以添加自定义配置文件（请参阅 Syslog 筛选程序）或预定义配置文件。对于每个配置文件，设置 **Event Type**（事件类型）： • **login**（登录）— User-ID 代理解析登录事件的 Syslog 消息以创建用户映射。 • **logout**（注销）— User-ID 代理解析注销事件的 Syslog 消息以删除不再是有效的用户映射。在 IP 地址分配为动态的网络中，自动删除通过确保代理仅将每个 IP 地址映射到当前关联用户来提高映射的准确性。 如果添加预定义的 *Syslog* 解析配置文件，请检查其名称以确定是否旨在匹配登录或注销事件。
默认域名 （仅限 Syslog 发件人）	（可选）如果服务器 **Type**（类型）为 **Syslog Sender**（**Syslog** 发件人），则输入域名以替代您的 Syslog 消息的用户名中的当前域名，或者如果您的 Syslog 消息不包含域，则将域预先加入用户名。

管理对受监控服务器的访问权限

执行 Server Monitoring（服务器监控）部分中的下列任务可管理对 User-ID 所监控服务器的访问权限，以获取用户映射信息。

任务	说明
显示服务器信息	对于每个受监控的服务器，用户映射页面将显示从 User-ID 代理到服务器的连接状态。**Add**（添加）服务器后，防火墙将尝试与之建立连接。如果连接尝试成功，Server Monitoring（服务器监控）部分将在 Status（状态）列显示 Connected（已连接）。如果防火墙未能建立连接，则状态列会显示错误条件，如 `Connection refused` 或 `Connection timeout`。 有关 Server Monitoring（服务器监控）部分显示的其他字段的详细信息，请参阅配置对受监控服务器的访问权限。
添加	要配置对受监控服务器的访问权限，请 **Add**（添加）User-ID 代理为获取用户映射信息而监控的各个服务器
删除	如需从用户映射进程（发现）中删除服务器，请选中该服务器并将其 **Delete**（删除）。 提示:如需从发现中删除服务器，但不删除其配置，请编辑服务器条目并取消选中 **Enabled**（已启用）。
发现	您可选择自动 **Discover**（发现）使用 DNS 的 Microsoft Active Directory 域控制器。防火墙将根据在 **Device**（设备）> **Setup**（设置）> **Management**（管理）页面的 **General Settings**（常规设置）部分中的 **Domain**（域）字段中输入的域名来发现域控制器。发现域控制器后，防火墙会为其在 Server Monitoring（服务器监控）列表中创建一个条目，之后您可启用该服务器进行监控。

© 2019 Palo Alto Networks, Inc.

任务	说明
	Discover（发现）功能仅适用于域控制器，不适用于 *Exchange* 服务器或 *eDirectory* 服务器。

包括或排除用户映射的子网

- Device（设备）> User Identification（用户标识）> User Mapping（用户映射）

使用 Include/Exclude Networks（包括/排除网络）列表可定义 User-ID 代理在执行 IP 地址到用户名的映射（发现）时将包括或排除的子网。默认情况下，如不将任何子网添加到此列表，则 User-ID 代理将对所有子网中的用户标识源执行发现（但不包括对拥有公共 IPv4 地址的客户端系统使用 WMI 探测的情况）。（公共 IPv4 地址即在 RFC 1918 和 RFC 3927 范围之外的地址）。

要启用公共 IPv4 地址的 WMI 探测，必须将其子网添加到此列表，并将其 **Discovery**（发现）选项设置为 **Include**（包括）。如果配置该防火墙将用户映射信息重新分发到其他防火墙，则您在此列表中指定的发现限制将应用到重新分发的信息。

使用包含和排除列表定义防火墙执行用户映射的子网。

您可在 Include/Exclude Networks（包括/排除网络）列表上执行以下任务：

任务	说明
添加	要将发现限制到特定的子网，请 **Add**（添加）子网配置文件并填写以下字段： • **Name**（名称）— 输入标识此子网的名称。 • **Enabled**（已启用）— 选中此选项可启用服务器监控中要包括或排除的子网。 • **Discovery**（发现）— 选择 User-ID 代理是否会 **Include**（包括）或 **Exclude**（排除）此子网。 • **Network Address**（网络地址）— 输入此子网的 IP 地址范围。 User-ID 代理会将隐式排除所有规则应用到该列表。例如，如果使用 **Include**（包括）选项添加子网 10.0.0.0/8，则即使不将其他子网添加到列表中，User-ID 代理也会将其排除。只有当您希望 User-ID 代理排除已明确包含的子网的一个子集事，您才需要使用排除选项添加条目。例如，如果您使用包含选项添加 10.0.0.0/8，并使用排除选项添加 10.2.50.0/22，则 User-ID 代理将对除 10.2.50.0/22 外的所有 10.0.0.0/8 子网执行发现，并且排除 10.0.0.0/8 之外的所有子网。如果添加 **Exclude**（排除）配置文件而不添加任何 **Include**（包括）配置文件，则 User-ID 代理会排除所有子网，而不只是已添加的子网。
删除	要将子网从列表中删除，请选中子网并将其 **Delete**（删除）。 **提示:**要从 Include/Exclude Networks（包括/排除网络）列表中删除子网，但不删除其配置，请编辑子网配置文件并取消选中 **Enabled**（已启用）。
自定义包括/排除网络	默认情况下，User-ID 代理会按添加子网的顺序（从顶部第一个到底部最后一个）来评估子网。要更改评估顺序，请单击自定义包含/排除网络顺序。然后，您可 **Add**（添加）、**Delete**（删除）、**Move Up**（上移）或**Move Down**（下移）子网以创建自定义评估顺序。

© 2019 Palo Alto Networks, Inc.

Device（设备）> User Identification（用户标识）> Connection Security（连接安全性）

编辑 ( ) User-ID 连接安全设置可选择防火墙使用的证书配置文件，以验证 Windows User-ID 代理提供的证书。防火墙使用所选的证书配置文件，通过验证代理提供的服务器证书来验证 User-ID 代理的身份。

任务	说明
User-ID 证书配置文件	从下拉列表中，选择要在对 Windows User-ID 代理进行身份验证或选择 New Certificate Profile（新建证书配置文件）创建新的证书配置文件时使用的证书配置文件。选择 **None**（无）以删除证书配置文件，而是使用默认身份验证配置文件。 要在配置对受监控服务器的访问权限使用 Kerberos 进行服务器身份验证时使用 Windows 服务器对服务器证书进行验证，确保已在 全局服务设置中配置 NTP，并选择根 CA 作为证书配置文件。
删除全部（仅限模板配置）	删除附加到所选模板的 User-ID 连接安全配置的证书配置文件。

© 2019 Palo Alto Networks, Inc.

Device（设备）> User Identification（用户标识）> Terminal Server Agents（终端服务器代理）

在支持多个用户共享同一 IP 地址的系统上，终端服务器 (TS) 代理会通过向各个用户分配端口范围来对其进行识别。TS 代理会通知分配端口范围的每个连接防火墙，以便防火墙可根据用户和用户组来实施策略。

所有防火墙型号都可以从最多 5,000 个多用户系统收集用户名到端口映射信息。防火墙可以从中收集映射信息的 TS 代理数因防火墙型号而异。

在配置对 *TS* 代理的访问权限之前，必须安装并配置 *TS* 代理。除配置与 *TS* 代理的连接以外，为终端服务器用户配置用户映射的完整流程需要执行附加任务。

您可以执行以下任务来管理对 TS 代理的访问权限。

任务	说明
显示信息/刷新连接	在 **Terminal Server Agents**（终端服务器代理）页面中，Connected（已连接）列将显示防火墙与 TS 代理之间连接的状态。其中，绿色图标以表示连接成功，黄色图标表示连接禁用，而红色图标则表示连接失败。如果认为连接状态可能在首次打开页面后发生变化，请单击 **Refresh Connected**（刷新连接）以更新状态显示。
添加	要配置对 TS 代理的访问权限，请 **Add**（添加）代理并配置以下字段： • **Name**（名称）— 输入标识 TS 代理的名称（最多 31个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。 • **Host**（主机）— 输入安装有 TS 代理的终端服务器的 静态 IP 地址或主机名。 • **Port**（端口）— 输入 TS 代理服务用于与防火墙通信的端口号（默认为 5009）。 • **Alternative Hosts**（备选主机）— 如果已安装 TS 代理的终端服务器有多个可显示为传出通信的源 IP 地址的 IP 地址，则 **Add**（添加）并最多输入 8 个附加静态 IP 地址或主机名。 • **Enabled**（启用）— 选择此选项可使防火墙与此 TS 代理通信。
删除	如需删除可对 TS 代理进行访问的配置，请选择代理并单击 **Delete**（删除）。 要禁用对 *TS* 代理的访问，而不删除其配置，请编辑此代理并取消选择 *Enabled*（启用）选项。
PDF/CSV	具有最小只读访问权限的管理角色可以将设备配置表格导出为 **PDF/CSV**。您可以应用筛选程序来创建更多特定的表格配置输出，以用于审计等事宜。将仅导出 Web 界面中所显示的列。请参阅配置表格导出。

© 2019 Palo Alto Networks, Inc.

Device（设备）> User Identification（用户标识）> Group Mapping Settings（组映射设置）选项卡

- **Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）

要根据用户和用户组使用安全策略和报告，防火墙将检索在目录服务器上指定和维护的组列表和相应的成员列表。防火墙支持各种 LDAP 目录服务器，包括 Microsoft Active Directory (AD)、Novell eDirectory 和 Sun ONE Directory Server。

每个防火墙或 Panorama 在所有策略中可以引用的不同用户组数因型号而异。但是，无论何种型号，您都必须在创建组映射配置之前配置 LDAP 服务器配置文件（Device（设备）> Server Profiles（服务器配置文件）> LDAP）。

除创建组映射配置以外，将用户名映射到组的完整流程需要执行附加任务。

根据需要 **Add**（添加）并配置以下字段以创建组映射配置。要删除组映射配置，请将其选定并单击 **Delete**（删除）。要禁用组映射配置而不将其删除，请编辑此配置并取消选择 **Enabled**（已启用）选项。

如果创建多个使用相同的基本专有名称 *(DN)* 或 *LDAP* 服务器的组映射配置，那么，组映射配置不能包括重叠组（例如，一个组映射配置的包括列表不能包含已属于不同组映射配置的组）。

组映射设置 — 服务器配置文件	配置位置	说明
姓名	**Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）	输入标识组映射配置的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
服务器配置文件	**Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）> **Server Profile**（服务器配置文件）	选择用于在该防火墙上进行组映射的 LDAP 服务器配置文件。
更新间隔		指定在防火墙启动与 LDAP 目录服务器的连接以获取任何针对防火墙策略所使用的组的更新之后的间隔秒数（范围为 60 至 86,400）。
用户域		默认情况下，**User Domain**（用户域）字段为空：防火墙自动检测 Active Directory 服务器的域名。如果您输入一个值，则会替代防火墙从 LDAP 源检索到的任何域名。您输入的必须是 NetBIOS 名称。 该字段仅影响从 *LDAP* 源检索到的用户名和组名。要替代与用户身份验证的用户名相关联的域，请配置分配给用户的身份验证配置文件的 *User Domain*（用户域）和 *Username Modifier*（用户名修饰

© 2019 Palo Alto Networks, Inc.

组映射设置 — 服务器配置文件	配置位置	说明
		符）（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。
组对象		• **Search Filter**（搜索过滤器）— 输入指定要检索并跟踪的组的 LDAP 查询。 • **Object Class**（对象类）— 输入组定义。默认为 objectClass=group，即指定系统将在目录中检索与 **Search Filter**（搜索过滤器）匹配且具有 objectClass=group 的所有对象。
用户对象		• **Search Filter**（搜索过滤器）— 输入指定要检索并跟踪的用户的 LDAP 查询。 • **Object Class**（对象类）— 输入用户对象定义。例如，在 Active Directory 中，objectClass 为 *user*。
已启用		选择此选项可启用组映射的服务器配置文件。
获取受管设备列表		对于 GlobalProtect 部署，选中此选项可允许防火墙从 Active Directory 等目录服务器检索序列号。这样，GlobalProtect 能够标识连接端点的状态，并根据出现的端点序列号执行基于 HIP 的安全策略。
用户属性	**Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）> **User and Group Attributes**（用户和组属性）	指定标识用户的目录属性： • **Primary Username**（主用户名）— 指定 User-ID 源提供给用户名的属性（例如，**`userPrincipalName`** 或 **`sAMAccountName`**） 主用户名是防火墙标识日志、报告和策略配置中用户的方式，即使防火墙从 *User-ID* 源接收其他格式亦是如此。如果未指定格式，则防火墙默认对 *Active Directory* 使用 `sAMAccountName` 格式，对 *Novell eDirectory* 和 *Sun ONE Directory Server* 使用 `uid` 格式。 • **E-Mail**（电子邮件）—指定 User-ID 源提供给电子邮件地址的属性。默认为 **`mail`**。 • **Alternate Username 1-3**（备用用户名 **1-3**）— 最多可指定三个与 User-ID 源可以发送的格式相对应的附加属性。 若配置 *Active Directory* 服务器，则默认情况下，备用用户名 *1* 为 `userPrincipalName`。

© 2019 Palo Alto Networks, Inc.

组映射设置 — 服务器配置文件	配置位置	说明
组属性		指定 User-ID 源用于标识组的属性： • **Group Name**（组名称）— 指定 User-ID 源用作组名属性的属性。Active Directory 的默认设值为 `name`，而 Novell eDirectory 或 Sun ONE Directory Server 的默认设值为 `cn`。 • **Group Member**（组成员）— 指定 User-ID 源用作组成员的属性。默认为 `member`。 • **E-Mail**（电子邮件）— 指定 User-ID 源用于电子邮件地址的属性。默认为 `mail`。
可用组 包括的组	**Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）> **Group Include List**（组包含列表）	使用这些字段可在创建安全规则时，限制防火墙显示的组数。浏览 LDAP 树以查找要在规则中使用的组。要包含组，请选中，并将其添加 (⊕) 到可用组列表中。要从列表删除组，请选中，并将其从包含组列表中删除(⊖)。 仅包含您所需的组，这样，防火墙仅检索必要组的用户组映射，不会检索 *LDAP* 目录中的整个树。
姓名 LDAP 过滤器	**Device**（设备）> **User Identification**（用户标识）> **Group Mapping Settings**（组映射设置）> **Custom Group**（自定义组）	创建基于 LDAP 过滤器的自定义组，以便根据与 LDAP 目录中的现有用户组不匹配的用户属性来使用防火墙策略。 User-ID 服务将所有与过滤条件相符的 LDAP 目录用户映射到自定义组。如果创建的自定义组的可辨别名称 (DN) 与现有 Active Directory 组的域名相同，则防火墙会在所有引用中对自定义组应用该名称（例如，在策略和日志中）。如需创建自定义组，**Add**（添加）并配置以下字段： • **Name**（名称）— 输入自定义组的名称（该名称在当前防火墙或虚拟系统的组映射配置中都唯一）。 • **LDAP Filter**（**LDAP** 过滤器）— 输入一个不超过 2,048 字符的过滤器。 仅使用过滤器中的索引属性提高 *LDAP* 搜索的速度，并最大限度减少对 *LDAP* 目录服务器性能的影响；防火墙不验证 *LDAP* 过滤器。 **Included Groups**（包含组）和 **Custom Group**（自定义组）列表的最大组合数为 640 个条目。 要删除自定义组，请将其选择并单击 **Delete**（删除）。要复制自定义组，请将其选定并 **Clone**（克隆），然后在必要时编辑字段。

© 2019 Palo Alto Networks, Inc.

组映射设置 — 服务器配置文件	配置位置	说明
		添加或克隆自定义组后，您必须在策略和对象中使用新的自定义对象之前 *Commit*（提交）更改。

© 2019 Palo Alto Networks, Inc.

Device（设备）> User Identification（用户标识）> Authentication Portal（身份验证门户）

编辑 ( ) 身份验证门户 设置可配置防火墙对其流量与身份验证策略规则相匹配的用户进行身份验证。

如果身份验证门户使用 *SSL/TLS* 服务配置文件（Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件））、身份验证配置文件（Device（设备）> Authentication Profile（身份验证配置文件））或证书配置文件（Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件）），则在开始操作前应配置配置文件。除配置这些配置文件以外，使用完整流程 可配置需要执行额外任务的身份验证门户。

您必须 *Enable Authentication Portal*（启用身份验证门户）才能执行身份验证策略（请参阅 Policies（策略）> Authentication（身份验证））。

字段	说明
启用身份验证门户	选择此选项可启用身份验证门户。
空闲计时器(分钟)	输入用户在身份验证门户会话中用户生存时间(TTL) 值，以分钟为单位（范围为 1 至 1,440，默认为 15）。每次身份验证门户用户产生活动时，都会重置该计时器。如果用户处于空闲状态的时间超过 **Idle Timer**（空闲计时器）值，PAN-OS 将删除身份验证门户用户映射，且用户必须重新登录。
定时器（分钟）	此为最大的 TTL 分钟数，即任何身份验证门户会话可保持映射状态的最长时间（范围为 1 至 1,440，默认为 60）。此时段耗尽后，PAN-OS 将删除映射且用户必须重新进行身份验证，即使会话仍处于活动状态也不例外。该计时器可防止映射失效，并防止此处设置的值替代 **Idle Timer**（空闲计时器）值。 您应始终将过期 *Timer*（计时器）的值设置为高于 *Idle Timer*（空闲计时器）。
SSL/TLS 服务配置文件	要指定安全重定向请求的防火墙服务器证书和允许的协议，请选择 SSL/TLS 服务配置文件（请参阅 Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件））。如果选择 **None**（无），则防火墙使用 SSL/TLS 连接的本地默认证书。 在 *SSL/TLS* 服务配置文件中，设置 *Min Version*（最低版本）为 *TLSv1.2*，设置 *Max Version*（最高版本）为*Max*（最高），以提供针对 *SSL/TLS* 协议漏洞的最强安全性。设置 *Max Version*（最高版本）为 *Max*（最高），一旦出现更强的可用协议，则防火墙会始终使用最新版本。 要透明地重定向用户而不显示证书错误，请将与接口 IP 地址相匹配的证书相关联的配置文件分配给您重定向 Web 请求的接口。
身份验证配置文件	您可以选择身份验证配置文件（Device（设备）> Authentication Profile（身份验证配置文件））在用户的流量与身份验证策略规则相匹配时对其进行身份验证（Policies（策略）> Authentication（身份验证））。但是，您在身份验证门户中选择的身份验证配置文件仅适用于引用其中一个默认身份验证执行对象的规则（Objects（对象）>

© 2019 Palo Alto Networks, Inc.

字段	说明
	Authentication（身份验证））。通常在升级到 PAN-OS 8.0 后出现这样的情况，因为所有身份验证规则最初都是引用默认对象。对于引用自定义身份验证执行对象的规则，请在创建对象时选择身份验证配置文件。
用于入站身份验证提示(UDP)的 GlobalProtect 网络端口	指定 GlobalProtect™ 用于接收多因素 (MFA) 网关的入站身份验证提示的端口。（范围为 1 - 65,536；默认为 4,501）。要支持多因素身份验证，GlobalProtect 端点必须接收并确认从 MFA 网关入站的 UDP 提示。如果 GlobalProtect 端点在指定的网络端口接收 UDP 消息和来自受信任的防火墙或网关的 UDP 消息，则 GlobalProtect 会显示身份验证消息（请参阅自定义 GlobalProtect 应用程序）。
模式	选择防火墙捕获 Web 请求身份验证的方式： • **Transparent**（透明）— 防火墙根据身份验证规则拦截 Web 请求，并模拟原始目标 URL 发出 HTTP 401 消息以提示用户进行身份验证。但是，由于防火墙没有目标 URL 的真正证书，因此浏览器将向尝试访问安全站点的用户显示证书错误。因此，仅可在必要时（例如第 2 层或虚拟线路部署）使用此模式。 • **Redirect**（重定向）— 防火墙根据身份验证规则拦截 Web 请求，并将其重定向到指定的重定向主机。防火墙使用 HTTP 302 重定向以提示用户进行身份验证。最佳做法是使用 **Redirect**（重定向），因为它可提供更好的最终用户体验（显示证书无错误，且允许可实现无缝浏览的会话 cookies，因为 **Redirect**（重定向）不会在超时到期时重新映射）。但是，如果需要您在分配给入口第 3 层接口的接口管理配置文件中启用响应页面（有关详细信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> Interface Mgmt（接口管理）和 PA-7000 系列第 3 层接口）。 重定向模式的另一个优势是可允许会话 Cookie，这可让用户在每次超时到期时可以继续浏览经过身份验证的站点，无需进行重新映射。这对从一个 IP 地址漫游到另一个地址（例如，从公司 LAN 到无线网络）的用户尤为有用，因为只要会话保持打开状态，用户就无需因其 IP 地址变更而重新进行身份验证。 如果身份验证门户使用 *Kerberos SSO*，则需要处于 *Redirect*（重定向）模式下，因为浏览器仅提供受信任站点的凭据。此外，如果身份验证门户使用多因素身份验证 *(MFA)*，也需要处于 *Redirect*（重定向）模式下。
会话 Cookie （仅限重定向模式）	• **Enable**（启用）— 选择此选项可启用会话 Cookie。 • **Timeout**（超时）— 如果 **Enable**（启用）会话 Cookie，则此计时器将指定 Cookie 有效的分钟数（范围为 60-10,080，默认为 1,440）。 设置的超时值应够短，不会导致 *cookies* 中出现失效用户映射条目，但也应足够长，不会使用在会话期间多次提醒用户登录的方式来提升良好的用户体验。开始设置的值应小于等于 *480* 分钟（*8* 小时），并根据需要进行调整。 • **Roaming**（漫游）— 如果 IP 地址在会话处于活动状态时发生更改（如当端点从有线网络迁移到无线网络时），则可以选中此选项以保留 Cookie。仅当 Cookie 超时或用户关闭浏览器时，用户才要重新进行身份验证。
重定向主机 （仅限重定向模式）	指定解析到第 3 层接口（防火墙重定向 Web 请求的目标接口）IP 地址的 Intranet 主机名。 如果用户通过 *Kerberos* 单点登录 *(SSO)* 进行身份验证，则 *Redirect Host*（重定向主机）必须与在 Kerberos keytab 中指定的主机名相同。

© 2019 Palo Alto Networks, Inc.

字段	说明
证书配置文件	您可以选择证书配置文件（Device（设备）> Certificate Management（证书管理）> Certificate Profile（证书配置文件））在用户流量与任何身份验证策略规则相匹配时进行身份验证（Policies（策略）> Authentication（身份验证））。 对于此身份验证类型，身份验证门户会提示用户的端点浏览器提供客户端证书。因此，您必须将客户端证书部署到每个用户系统。此外，在防火墙上，您必须安装颁发客户端证书的证书颁发机构 (CA) 证书，并将 CA 证书分配给证书配置文件。这是对 Mac 操作系统和 Linux 端点启用 **Transparent**（透明）身份验证的唯一身份验证方法。

GlobalProtect

GlobalProtect™ 提供了用于管理移动员工，从而让所有用户进行安全访问而无论其使用何种设备或身在何处的完整基础架构。以下防火墙 Web 界面页面可让您配置和管理 GlobalProtect 组件：

> Network（网络）> GlobalProtect > Portals（门户）
> Network（网络）> GlobalProtect > Gateways（网关）
> Network（网络）> GlobalProtect > MDM
> Network（网络）> GlobalProtect > Device Block List（设备阻止列表）
> Network（网络）> GlobalProtect > Clientless Apps（无客户端应用）
> Network（网络）> GlobalProtect > Clientless App Groups（无客户端应用组）
> Objects（对象）> GlobalProtect > HIP Objects（HIP 对象）
> Objects（对象）> GlobalProtect > HIP Profiles（HIP 配置文件）
> Device（设备）> GlobalProtect Client（GlobalProtect 客户端）

了解更多？

请参阅《GlobalProtect 管理员指南》，了解有关 GlobalProtect 的更多信息，包括有关设置 GlobalProtect 基础设施、如何使用主机信息执行策略以及配置常见 GlobalProtect 部署的分步说明的详细信息。

Network（网络）> GlobalProtect > Portals（门户）

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）可设置并管理 GlobalProtect™ 门户。门户提供了针对 GlobalProtect 基础架构的管理功能。参与 GlobalProtect 网络的每个端点都会从门户收到其配置，其中包括可用网关的相关信息，以及应用程序连接到网关时可能需要的任何客户端证书。此外，门户还控制 GlobalProtect 应用程序软件的行为，以及向 macOS 和 Windows 端点的分发。对于 Linux 端点，必须从支持站点获取软件；对于移动设备，GlobalProtect 应用程序通过 Apple App Store（适用于 iOS 设备）、Google Play（适用于 Android 设备）和 Microsoft Store（适用于 Windows Phone 和其他 Windows UWP 设备）进行分发；对于 Chromebooks，GlobalProtect 应用程序通过 Chromebook Management Console 或 Google Play 进行分发。

要添加门户配置，请单击添加以打开“GlobalProtect 门户”对话框。

您在查找什么内容？	请参阅：
我应为 GlobalProtect 门户配置哪些常规设置？	GlobalProtect 门户常规选项卡
我如何才能将身份验证配置文件分配到门户配置？	GlobalProtect 门户身份验证选项卡
如何定义 GlobalProtect 应用程序从端点收集的数据？	GlobalProtect 门户 Portal Data Collection（门户数据收集）选项卡
我能配置哪些客户端身份验证选项？	GlobalProtect 门户代理身份验证选项卡
我如何才能根据操作系统、用户和/或用户组将配置分配到特定的设备组？	GlobalProtect 门户 Agent Config Selection Criteria（代理配置选择标准）选项卡
我如何才能配置内部网关的设置和优先级？	GlobalProtect 门户代理内部选项卡
我如何才能配置外部网关的设置和优先级？	GlobalProtect 门户代理外部选项卡
我如何才能为不同的用户类型创建单独的客户端配置？	GlobalProtect 门户代理选项卡
我能对 GlobalProtect 应用程序的外观和行为进行哪些自定义设置？	GlobalProtect 门户代理应用程序选项卡
我如何才能配置数据收集选项？	GlobalProtect 门户代理数据收集选项卡
我如何才能配置 GlobalProtect 门户以允许访问 Web 应用程序，而不需要安装 GlobalProtect 应用程序？	GlobalProtect 门户无客户端 VPN 选项卡
我如何才能将 VPN 连接扩展到作为卫星的防火墙？	GlobalProtect 门户卫星选项卡

© 2019 Palo Alto Networks, Inc.

您在查找什么内容？	请参阅：
了解更多？	有关设置门户的详细分步骤说明，请参阅《*GlobalProtect* 管理员指南》中的配置 GlobalProtect 门户。

GlobalProtect 门户常规选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **General**（常规）

选择**General**（常规）选项卡以定义 GlobalProtect 应用程序用于连接到 GlobalProtect 门户的网络设置。或者，您也可以禁用登录页面，或为 GlobalProtect 指定自定义门户登录和帮助页面。有关如何创建和导入自定义页面的信息，请参阅《GlobalProtect 管理员指南》中的自定义门户登录、欢迎和帮助页面。

GlobalProtect 门户设置	说明
姓名	键入门户的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	对于处于多虚拟系统模式下的防火墙，**Location**（位置）是指提供 GlobalProtect 网络门户的虚拟系统 (vsys)。对于不在多虚拟系统模式下的防火墙，**Location**（位置）选项不可用。在保存网络门户后，您无法更改其 **Location**（位置）。
网络设置	
接口	选择防火墙接口的名称，此接口将作为来自远程端点和防火墙的通信的入口。 请勿将允许 *Telnet*、*SSH*、*HTTP* 或 *HTTPS* 的接口管理配置文件附加到已配置 *GlobalProtect* 门户或网关的接口，因为这会将管理接口暴露给互联网。有关如何保护对管理网络的访问权限的更多详细信息，请参阅保护管理访问权限的最佳做法。
IP 地址	指定运行 GlobalProtect 门户网站服务的 IP 地址。选择 **IP Address Type**（**IP** 地址类型），然后输入 **IP Address**（**IP** 地址）。 • IP 地址类型可以是 **IPv4**（仅限 IPv4 流量）、**IPv6**（仅限 IPv6 流量）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。 • IP 地址必须与 IP 地址类型兼容。例如，172.16.1.0（对于 IPv4）或 21DA:D3:0:2F3b（对于 IPv6）。 • 如果您选择 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），请为每个地址输入适当的地址类型。
日志设置	
记录成功的 SSL 握手	（可选）为成功的 SSL 解密握手创建详细日志。默认情况下禁用。 日志会占用存储空间。在记录成功的 *SSL* 握手之前，必须确保有足够的资源存储日志。编辑*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Logging and Reporting Settings*（记

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户设置	说明
	录和报告设置）以检查当前日志内存分配，并为各种日志类型分配内存。
记录失败的 SSL 握手	为失败的 SSL 解密握手创建详细日志，以便您能找到导致解密失败的原因。默认情况下启用。 日志会占用存储空间。若要分配更多（或更少）的日志存储空间给解密日志，请编辑日志内存分配（*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Logging and Reporting Settings*（记录和报告设置））。
日志转发	指定转发 GlobalProtect SSL 握手（解密）日志的方法和位置。
外观	
网络门户登录页面	（可选）选择用户访问门户的自定义登录页面。您可以选择出厂默认值页面或导入自定义页面。默认值是 **None**（无）。要阻止从 Web 浏览器访问此页面，请 **Disable**（禁用）此页面。
网络门户登录页面	（可选）选择门户的自定义登录页面。您可以选择出厂默认值页面或导入自定义页面。默认值是 **None**（无）。
应用帮助页面	（可选）选择帮助用户使用 GlobalProtect 的自定义帮助页面。您可以选择出厂默认值页面或导入自定义页面。出厂默认值帮助页面随 GlobalProtect 应用程序软件一并提供。如果选择自定义帮助页面，GlobalProtect 门户将提供帮助页面和 GlobalProtect 门户配置。如将默认值保留为 **None**（无），GlobalProtect 应用程序会禁用该页面并从菜单中删除该选项。

GlobalProtect 门户身份验证配置选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Authentication**（身份验证）

选择**Authentication**（身份验证）选项卡以配置各种 GlobalProtect™ 门户设置：

- 门户和服务器用于进行身份验证的 SSL/TLS 服务配置文件。此服务配置文件独立于身份验证中的其他设置。
- 主要基于用户端操作系统、其次基于可选身份验证配置文件的唯一身份验证方案。
- （可选）**Certificate Profile**（证书配置文件），可使 GlobalProtect 使用特定的证书配置文件来对用户进行身份验证。来自客户端的证书必须与此证书配置文件相匹配（如果客户端证书为安全方案的一部分）。

GlobalProtect 门户身份验证设置	说明
服务器身份验证	
SSL/TLS 服务配置文件	选择现有的 SSL/TLS 服务配置文件。此配置文件将指定证书和允许的协议，以便保护管理接口上的通信。与配置文件相关联的证书的公用名 (CN) 字段和主题备选名称 (SAN) 字段（如适用）必须与 **General**（常规）选项卡中所选 **Interface**（接口）的 IP 地址或 FQDN 完全匹配。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户身份验证设置	说明
	在 *GlobalProtect VPN* 配置中，使用与来自可信第三方 *CA* 的证书相关联的配置文件或内部企业 *CA* 生成的证书。
客户端身份验证	
姓名	输入名称以标识此客户端身份验证配置。（客户端身份验证配置独立于 SSL/TLS 服务配置文件。） 您可创建多个客户端身份验证配置，并首先通过操作系统加以区分，再通过唯一的身份验证配置文件加以区分（适用于相同的 OS）。例如，您可为不同的操作系统添加客户端身份验证配置，而也可为相同的操作系统添加不同配置，并通过唯一的身份验证配置文件加以区分。（应按从最特定到最通用的顺序，手动对配置进行排序。例如，所有用户和任何操作系统就是最通用的配置。） 您还可以使用 **Pre-logon**（预登录）模式（即在用户登录到系统之前）创建 GlobalProtect 部署到应用程序的配置，或者要应用于任何用户的配置。（Pre-logon（预登录）会在用户登录 GlobalProtect 之前，先建立通往 GlobalProtect 网关的 VPN 隧道。）
OS	要在端点上部署专用于操作系统 (OS) 的客户端身份验证配置文件，请 **Add**（添加）操作系统（**Any**（任何）、**Android**、**Chrome**、**iOS**、**Linux**、**Mac**、**Windows**或 **WindowsUWP**）。操作系统是配置之间的首要区分项。（请参阅“身份验证配置文件”了解如何进行进一步区分。） **Browser**（浏览器）和 **Satellite**（卫星）中的其他选项可让您指定适用于特定场景的身份验证配置文件。选择 **Browser**（浏览器）可指定用于对从 Web 浏览器访问门户且有意下载 GlobalProtect 应用程序（Windows 和 Mac）的用户进行身份验证的身份验证配置文件。选择 **Satellite**（卫星）可指定用于对卫星进行身份验证的身份验证配置文件 (LSVPN)。
身份验证配置文件	除通过操作系统对客户端身份验证配置进行区分外，您还可以通过指定身份验证配置文件来进行进一步区分。（您可选择 **New Authentication Profile**（新建身份验证配置文件）或选择已有的身份验证配置文件。）如需为操作系统配置多个身份验证选项，您可创建多个客户端身份验证配置文件。 如果在 *Gateways*（网关）中配置 *LSVPN*，则不可保存该配置，除非已在此处选择了一个身份验证配置文件。而且，如果想使用序列号来对卫星进行身份验证，则门户必须在无法定位或验证防火墙序列号时，具备可用的身份验证配置文件。 另请参阅 Device（设备）> Authentication Profile（身份验证配置文件）。
用户名标签	指定 GlobalProtect 门户登录的自定义用户名标签。例如，用户名（唯一）或电子邮件地址 **(username@domain)**。
密码标签	指定 GlobalProtect 门户登录的自定义密码标签。例如，密码（土耳其语）或密码（用于基于令牌的双因素身份验证）。
身份验证消息	如需帮助最终用户了解其登录所需的凭据类型，请输入一则消息或保留默认消息。此消息的最大长度为 256 个字符。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户身份验证设置	说明
允许使用用户凭证或客户端证书进行身份验证	如果选择 **No**（否），用户必须使用用户凭证和客户端证书对网关进行身份验证。如果选择 **Yes**（是），用户可以使用用户凭证或客户端证书对网关进行身份验证。
证书配置文件	
证书配置文件	（可选）选择门户用于对来自用户端的客户端证书进行匹配的 **Certificate Profile**（证书配置文件）。选择证书配置文件后，门户将仅当来自客户端的证书与该配置文件相匹配时，才对用户进行身份验证。 如果将 **Allow Authentication with User Credentials OR Client Certificate**（允许使用用户凭证或客户端证书进行身份验证）选项设置为 **No**（否），则必须选择**Certificate Profile**（证书配置文件）。如果将 **Allow Authentication with User Credentials OR Client Certificate**（允许使用用户凭证或客户端证书进行身份验证）选项设置为 **Yes**（是），则可以选择 **Certificate Profile**（证书配置文件）。 此证书配置文件独立于操作系统。此外，即使启用身份验证替代（这将替代身份验证配置文件以允许使用加密 Cookie 进行身份验证），此配置文件也将处于活动状态。

GlobalProtect 门户 Portal Data Collection（门户数据收集）选项卡

选择 **Network**（网络）> **GlobalProtect** > **Portals**（门户）> **<portal-config>** > **Portal Data Collection**（门户数据收集）以定义 GlobalProtect 应用程序从端点收集，并在用户成功登录到门户后在配置选择标准数据中发送的数据。

GlobalProtect 门户数据收集设置	说明
证书配置文件	选择 GlobalProtect 门户用于匹配 GlobalProtect 应用程序发送的机器证书的证书配置文件。
自定义检查	定义您希望应用程序收集的自定义主机信息。 • **Windows — Add**（添加）特定注册表项或键值的选中标记。 • **Windows — Add**（添加）特定 plist 项或键值的选中标记。

GlobalProtect 门户代理选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）

选择**Agent**（代理）选项卡以定义代理配置设置。GlobalProtect 门户会在首次建立连接后，将此配置部署到设备。

您也可指定门户自动部署可信任的根证书授权机构 (CA) 证书和中间证书。如果端点不信任 GlobalProtect 网关和 GlobalProtect Mobile Security Manager 使用的服务器证书，端点将需要这些证书建立到网关或 Mobile Security Manager 的 HTTPS 连接。门户会将您在此处指定的证书推送到客户端，同时也会一并推送客户端配置。

© 2019 Palo Alto Networks, Inc.

如需添加可信任的根 CA 证书，请 **Add**（添加）已有的证书或 **Import**（导入）新证书。如需以透明方式在客户端的证书商店中，安装 SSL 转发代理解密所需的可信任根 CA 证书，请选择 **Install in Local Root Certificate Store**（在本地根证书商店中安装）。

指定 *GlobalProtect* 应用程序用于验证 *GlobalProtect* 门户和网关标识的可信任根 *CA* 证书。如果门户或网关提供的证书尚未由发布可信任根 *CA* 的同一证书颁发机构的签名或颁发，则 *GlobalProtect* 应用程序无法与门户或网关建立连接。

如果有不同类别的用户需要不同配置，则可创建单独的代理配置以对其进行支持。然后，门户将使用用户名/组名和客户端的操作系统来确定要部署的代理配置。与安全规则评估相同，门户会从列表的顶部开始查找匹配项。找到匹配项后，门户会将对应的配置传递到应用程序。因此，如果有多个代理配置，请务必将其排序，以使更特定的配置（也就是适用于特定用户或操作系统的配置）在更通用配置的上方。使用 **Move Up**（上移）和 **Move Down**（下移）可对配置进行重新排序。必要时，请 **Add**（添加）新代理配置。有关配置门户和创建代理配置的详细信息，请参阅《GlobalProtect 管理员指南》中的 GlobalProtect 门户。**Add**（添加）新的代理配置或修改现有的代理配置时，将会打开 **Configs**（配置）窗口并显示五个选项卡，如下表所述：

- GlobalProtect 门户代理身份验证选项卡
- GlobalProtect 门户 Agent Config Selection Criteria（代理配置选择标准）选项卡
- GlobalProtect 门户代理内部选项卡
- GlobalProtect 门户代理外部选项卡
- GlobalProtect 门户代理应用程序选项卡
- GlobalProtect 门户 Agent HIP Data Collection（代理 HIP 数据收集）选项卡

GlobalProtect 门户代理身份验证选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **Authentication**（身份验证）

选择 **Authentication**（身份验证）选项卡以配置应用于代理配置的身份验证设置。

GlobalProtect 门户客户端身份验证配置设置	说明
身份验证选项卡	
姓名	输入该配置的描述性名称以进行客户端身份验证。
客户端证书	（可选）选择将客户端证书分发到端点的源，端点会在收到证书后，将其呈递到网关。如果配置相互 SSL 身份验证，则会需要客户端证书。 如果为门户客户端配置中的预先登录配置了 SCEP，则门户会生成机器证书，该证书存储于系统证书商店中，可用于进行网关身份验证和连接。 要使用属于防火墙 **Local**（本地）的证书，而非通过 **SCEP** 从 PKI 生成的证书，请选择已上传到防火墙的证书。 如果使用内部 CA 将证书分发到端点，请选择 **None**（无）（默认）。选择 **None**（无）后，门户不会将证书推送到端点。
保存用户凭据	选择 **Yes**（是）可在应用程序上保存用户名和密码，或选择 **No**（否）可强制用户在每次连接时，以手动输入方式或通过端点以透明方式提供密码。选择 **Save Username Only**（仅保存用户名）将仅保存用户每次连接时的用户名。选择 **Only with User**

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户客户端身份验证配置设置	说明
	Fingerprint（仅使用用户指纹）以允许生物特征登录。在端点上启用生物特征登录后，若指纹扫描与端点上受信任的指纹模板匹配，则 GlobalProtect 将使用保存的用户凭据。 请勿保存用户凭证，因为未经授权的用户可使用该凭证更轻松地访问敏感资源和机密信息。用户每次连接到 *GlobalProtect* 时，都应手动输入其凭证。
身份验证覆盖	
生成身份验证替代的 Cookie	选中此选项可配置门户生成已加密的、端点特定的 Cookie。门户会在用户首次通过门户进行身份验证之后，将此 Cookie 发送到端点。
接受身份验证覆盖的 Cookie	选择此选项可配置门户通过有效的加密 Cookie 对端点进行身份验证。端点递送有效 Cookie 后，门户将验证此 Cookie 是否已经过门户加密，再对其进行解密，然后对用户进行身份验证。
Cookie 生命周期	指定 Cookie 有效的小时数、天数或周数。典型的生命周期为 24 小时。范围为 1–72 小时、1–52 周或 1–365 天。Cookie 过期后，用户必须输入登录凭据，门户随后会加密要发送到用户端的新 Cookie。
用于加密/解密 Cookie 的证书	选择用于加密和解密 Cookie 的证书。 请确保门户和网关使用相同的证书对 *Cookie* 进行加密和解密。（将此证书配置为网关客户端配置的一部分。）请参阅 Network（网络）> GlobalProtect > Gateways（网关））。
需要动态密码的组件（双因素身份验证）	
如需配置 GlobalProtect 支持动态密码（如一次性密码 (OTP)），请指定要用户输入动态密码的门户或网关类型。在未启用双因素身份验证的情况下，GlobalProtect 将选择进行使用登录凭据（如 AD）和证书的常规身份验证。 如果启用了双因素身份验证的门户或网关类型，则该门户或网关将在初始门户身份验证之后，提示用户提交凭据和附加 OTP（或其他动态密码）。 但如果同时启用了身份验证覆盖，则加密 Cookie 将被用于对用户进行身份验证（在用户首次通过新会话的身份验证之后），因而也会抢占对用户重新输入凭据提出的要求（只要此 Cookie 有效）。所以只要 Cookie 有效，用户在必要时就一定要以透明方式登录。您可以指定 Cookie 的生命周期。	
门户	选中此选项可使用动态密码连接到门户。
内部网关身份验证	选中此选项可使用动态密码连接到内部网关。
外部网关 — 仅限手动	选中此选项可使用动态密码连接到配置为 **Manual**（手动）网关的外部网关。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户客户端身份验证配置设置	说明
外部网关 — 自动发现	选择此选项可使用动态密码连接到应用程序可自动发现的任何余留外部网关（即未被配置为 **Manual**（手动）的网关）。

GlobalProtect 门户 *Agent Config Selection Criteria*（代理配置选择标准）选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **Config Selection Criteria**（配置选择标准）

选择 **Config Selection Criteria**（配置选择标准）选项卡以配置用于标识受管和非受管端点部署中端点类型的匹配标准。门户可根据端点类型将指定配置推送到端点。

GlobalProtect 门户配置选择标准选项卡	说明
用户/用户组选项卡	
OS	**Add**（添加）一个或多个端点操作系统(OS)以指定接收此配置的端点。门户会自动了解端点的操作系统，并将该操作系统的详细信息加入客户端配置中。您可选择 **Any**（任何）操作系统或特定的操作系统（**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows** 或 **WindowsUWP**）。
用户/用户组	**Add**（添加）要将此配置应用到的特定用户或用户组。 必须配置组映射（*Device*（设备）> *User Identification*（用户标识）> *Group Mapping Settings*（组映射设置））之后，才能选择用户组。 要将此配置部署到所有用户，请从 **User/User Group**（用户/用户组）下拉列表中选择 **any**（任何）。要将此配置部署到预登录模式中拥有 GlobalProtect 应用程序的用户，请从 **User/User Group**（用户/用户组）下拉列表中选择 **pre-logon**（预登录）。
设备检查	
机器账户设有设备序列号	根据 Active Directory 中是否存在端点序列号配置匹配标准。
证书配置文件	选择 GlobalProtect 门户用于匹配 GlobalProtect 应用程序发送的机器证书的证书配置文件。
自定义检查	
自定义检查	选择此选项可定义待匹配的自定义主机信息。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户配置选择标准选项卡	说明
注册表项	要在 Windows 端点中检查某个特定注册表项，**Add**（添加）要匹配的 **Registry Key**（注册表项）。要仅匹配缺少指定注册表项或键值的端点，请启用 **Key does not exist or match the specified value data**（键值不存在或不匹配指定的值数据）选项。要匹配特定值，**Add**（添加）**Registry Value**（注册表值）和 **Value Data**（值数据）。要匹配确无指定值或值数据的端点，请选择 **Negate**（求反）。
Plist	要在 macOS 端点中检查属性列表 (plist) 的特定条目，**Add**（添加）**Plist** 名称。要仅匹配无指定 Plist 的端点，请启用 **Plist does not exist**（**Plist** 不存在）选项。要匹配 plist 中的特定键值对，**Add**（添加）**Key**（键）和对应的 **Value**（值）。要匹配确无指定键或值的端点，请选择 **Negate**（求反）。

GlobalProtect 门户代理内部选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **Internal**（内部）

选择 **Internal**（内部）选项卡以配置代理配置的内部网关设置。

GlobalProtect 门户内部设置	说明
内部主机检测	
内部主机检测	选中此选项可让 GlobalProtect 应用程序确定其是否在企业网络内。此选项仅适用于已配置与内部网关进行通信的端点，也是这些端点的最佳实践。 用户尝试登录时，应用程序将从指定的 **Hostname**（主机名）到指定的 **IP Address**（**IP** 地址），对内部主机执行逆向 DNS 查询。如果端点在企业网络内，则主机将作为可访问的参考点。如果应用程序找到主机，表示端点在网络内部，且应用程序会连接到内部网关；如果应用程序无法找到内部主机，表示端点在网络外部，且应用程序会建立通往其中一个外部网关的隧道。 • IP 地址类型可以是 **IPv4**（仅限 IPv4 流量），**IPv6**（仅限 IPv6 流量）或两者。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4** and **IPv6**（IPv4 和 IPv6）。 • IP 地址必须与 IP 地址类型兼容。例如，172.16.1.0（对于 IPv4）或 21DA:D3:0:2F3b（对于 IPv6）。 • 如果您选择 **IPv4** and **IPv6**（IPv4 和 IPv6），请为每个地址输入适当的地址类型。
主机名	输入在内部网络中解析到上述 IP 地址的 **Hostname**（主机名）。
内部网关	
指定应用程序可请求访问的内部网关，同时提供 HIP 报告（如果已在	**Add**（添加）内部网关，且其中包含各网关的下列信息： • **Name**（名称）— 用来标识网关的标签，最多 31 个字符。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户内部设置	说明
GlobalProtect 门户代理数据收集选项卡中启用 HIP）。	• **Address**（地址）— 该网关防火墙接口的 IP 地址或 FQDN。此值必须与网关服务器证书中的公用名 (CN) 和 SAN（如已指定）相匹配。例如，如果已使用 FQDN 生成证书，则必须在此输入 FQDN。 • **Source Address**（源地址）— 端点的源地址或地址池。当用户进行连接时，GlobalProtect 会识别设备的源地址。只有包含在源地址池中的具有 IP 地址的 GlobalProtect 应用程序才可使用此网关进行身份验证，并发送 HIP 报告。 • **DHCP Option 43 Code**（**DHCP** 选项 **43** 代码）（仅限 Windows 和 Mac）— 网关选择的 DHCP 子选项代码。指定一个或多个子选项代码（以十进制表示）。GlobalProtect 应用程序从子选项代码定义的值读取网关地址。

GlobalProtect 门户代理外部选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **External**（外部）

选择**External**（外部）选项卡以配置代理配置的外部网关设置。

GlobalProtect 门户外部设置	说明
截断时间（秒）	指定应用程序在选择最佳网关前，等待所有可用网关响应的秒数。对于后续的连接请求，应用程序将仅尝试连接到中断前作出响应的网关。值为 0 表示应用程序使用 **App**（应用程序）选项卡的 **AppConfigurations**（应用程序配置）中的 **TCP Connection Timeout**（**TCP** 连接超时）（范围为 0-10，默认为 5）。
外部网关	
建立不在公司网络上的隧道后，请指定应用程序可尝试连接的防火墙的列表。	**Add**（添加）外部网关，且其中包含各网关的下列信息： • **Name**（名称）— 用来标识网关的标签，最多 31 个字符。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。 • **Address**（地址）— 配置网关的防火墙接口的 IP 地址或 FQDN。此值必须与网关服务器证书中的 CN（和 SAN（如已指定））相匹配。例如，如果已使用 FQDN 生成证书，则还必须在此输入 FQDN。 • **Source Region**（源区域）— 端点的源区域。当用户进行连接时，GlobalProtect 会识别端点区域，且只允许用户连接到为该区域配置的网关。对于选择网关，请首先考虑源区域，然后考虑网关优先级。 • **Priority**（优先级）— 选择一个值（**Highest**（最高）、**High**（高）、**Medium**（中）、**Low**（低）、**Lowest**（最低）或 **Manual only**（仅手动））以帮助应用程序确定要使用的网关。**Manual only**（仅手动）可防止 GlobalProtect 应用程序在端点启用 **Auto Discovery**（自动发现）的情况下尝试连接到此网关。应用程序将首先联系具有 **Highest**（最高）、**High**（高）或 **Medium**（中）优先级的所有指定网关，并与提供最快响应的网关建立隧道。如果无法访问具有较高优先级的网关，则应用程序接下来会与任何具有较低优先级值的其他网关进行联系（不包括 **Manual only**（仅限手动）网关）。 • **Manual**（手动）— 选中此选项可让用户手动选择（或切换到）网关。GlobalProtect 应用程序能够连接到任何已配置为 **Manual**（手动）的外部网关。应用程序连接到其他网关后，现有隧道将断开连接，同时建立新隧道。与主网关相比，手动网关也可以拥有其他身份验证机制。如果端点已重新启动，或如果已执行重新发现，则 GlobalProtect 应用程序将连接到主网

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户外部设置	说明
	关。如果用户组需要临时连接到特定网关，以访问网络的安全分段，则此功能会很有用。
第三方 VPN	
第三方 VPN	为引导 GlobalProtect 应用程序忽略已选中的第三方 VPN 客户端，以免 GlobalProtect 与之发生冲突，请 **Add**（添加）VPN 客户端的名称：请从列表中选择名称，或在提供的字段中输入名称。如果配置此功能，GlobalProtect 将忽略指定 VPN 客户端的路由设置。

GlobalProtect 门户代理应用程序选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **APP**（应用程序）

选择 **App**（应用程序）选项卡指定最终用户如何与其系统上安装的 GlobalProtect 应用程序进行交互。您可针对所创建的不同 GlobalProtect 代理配置，定义不同的应用程序设置。要了解更多有关 GlobalProtect 应用程序自定义设置的信息，请参阅 GlobalProtect 管理员指南。

GlobalProtect 应用程序配置设置	说明
欢迎页面	选择在最终用户成功连接到 GlobalProtect 之后要向其显示的欢迎页面。您可以选择出厂默认值页面或导入自定义页面。默认值是 **None**（无）。
应用配置	
连接方法	• **On-demand (Manual user initiated connection)**（按需（用户手动启动连接））— 用户必须启动 GlobalProtect 应用程序，然后发起到门户的连接并输入其 GlobalProtect 凭据。此选项主要用于远程访问连接。 • **User-logon (Always On)**（用户登录（始终启用））— 用户登录端点后，GlobalProtect 应用程序自动建立到门户的连接。门户将通过向应用程序提供合适的代理配置来做出响应。然后，应用程序设置到从门户接收的代理配置中指定的其中一个网关的隧道。 • **Pre-logon**（预登录）— 预登录可确保远程 Windows 和 Mac 用户始终连接到公司网络，并在用户登录到端点时启用域策略的用户登录脚本和应用程序。由于端点可以连接到公司网络（就像在内部一样），因此用户可以在密码过期后使用新密码登录，也可以接收密码恢复帮助（如果他们忘记密码）。预登录后，GlobalProtect 应用程序在用户登录端点之前，建立通往 GlobalProtect 网关的隧道；端点将通过提交预安装机器证书到网关来请求进行身份验证。然后，在 Windows 端点上，网关将 VPN 隧道从预登录用户重新分配给登录到端点的用户名；在 Mac 端点上，应用程序断开连接并为用户创建新的 VPN 隧道。 可以使用两种预登录连接方法，任何一种预登录方法都能够在用户登录到端点之前执行相同的预登录功能。但是，在用户登录到端点后，预登录连接方法可确定建立 GlobalProtect 应用程序连接的时间：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	• **Pre-logon (Always On)**（预登录（始终启用））— GlobalProtect 应用程序自动尝试连接并重新连接到 GlobalProtect 网关。移动设备不支持预登录功能，因此如果已指定此连接方法，则默认为 **User-logon (Always On)**（预登录（始终启用））连接方法。 • **Pre-logon then On-demand**（预登录，然后按需）— 用户必须启动 GlobalProtect 应用程序，然后手动启动连接。移动设备不支持预登录功能，因此如果已指定此连接方法，则默认为 **On-demand (Manual user initiated connection)**（按需（用户手动启动连接））连接方法。
GlobalProtect 应用程序配置刷新时间间隔（小时）	指定 GlobalProtect 门户在发起下一次应用程序配置刷新前要等待的小时数（范围为 1 至 168，默认为 24）。
允许用户禁用 GlobalProtect 应用程序	指定是否允许用户禁用 GlobalProtect 应用程序，如允许，则指定在其禁用应用程序前必须执行的操作（如有）： • **Allow**（允许）— 允许任何用户在必要时禁用 GlobalProtect 应用程序。 • **Disallow**（不允许）— 不允许最终用户禁用 GlobalProtect 应用程序。 • **Allow with Comment**（带注释允许）— 允许用户禁用其端点上的 GlobalProtect 应用程序，但要求用户提交其禁用此应用程序的理由。 • **Allow with Passcode**（带通行码允许）— 允许用户通过输入通行码来禁用 GlobalProtect 应用程序。此选项要求用户输入并确认通行码值，比如密码是否在输入时不显示。通常，管理员会在意外事件阻止用户通过使用 GlobalProtect VPN 连接到网络之前，向其提供通行码。您可通过电子邮件提供通行码，或将其发布在企业/组织网站上。 • **Allow with Ticket**（带票据允许）— 此选项可在用户尝试禁用 GlobalProtect 之后，启用质询响应机制，其中端点将显示一个 8 字符的十六进制票据请求号。之后，用户必须联系防火墙管理员或支持团队（为确保安全，建议使用电话联系），以提供此请求号。从防火墙（**Network**（网络）> **GlobalProtect** > **Portals**（门户））中，管理员或支持人员可以单击 **Generate Ticket**（生成票据）并输入票据 **Request**（请求）号以获取 **Ticket**（票据）号（也是一个 8 字符的十六进制数字）。管理员或支持人员将此票据号提供给要将其输入到质询字段以禁用应用程序的用户。
允许用户卸载 GlobalProtect 应用程序	指定是否允许用户卸载 GlobalProtect 应用程序，如允许，则指定在其卸载应用程序前必须执行的操作（如有）： • **Allow**（允许）— 允许任何用户在必要时卸载 GlobalProtect 应用程序。 • **Disallow**（不允许）— 不允许最终用户卸载 GlobalProtect 应用程序。 • **Allow with Password**（允许但要求密码）— 要求提供密码方可卸载 GlobalProtect 应用程序。此选项要求用户输入并确认密码，然后才能继续卸载。您可通过电子邮件提供密码，或将其发布在贵组织网站上。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	此选项要求“内容发布”版本为 8196-5685 或更高。
允许用户升级 GlobalProtect 应用程序	指定最终用户是否可升级 GlobalProtect 应用程序软件，如果可以，则指定其是否可选择何时升级： • **Disallow**（不允许）— 防止用户升级应用程序软件。 • **Allow Manually**（手动允许）— 允许用户通过选择 GlobalProtect 应用程序中的 **Check Version**（检查版本）来手动检查并启动升级。 • **Allow with Prompt**（带提示允许）（默认）— 当新版本在防火墙上激活时，对用户作出提示，并允许用户在方便时升级其软件。 • **Allow Transparently**（透明允许）— 只要门户上有可用的新版本，便自动升级应用程序软件。 • **Internal**（内部）— 当门户上有新版本可用时自动升级应用程序软件，但需要等到端点在内部连接到公司网络。这可以防止由低带宽连接升级引起的延迟。
允许用户退出 GlobalProtect 应用程序 （仅限 Windows、macOS、iOS、Android 和 Chrome）	指定是否允许用户手动退出 Globalprotect 应用程序： • **Yes**（是）— 允许任何用户在必要时退出 GlobalProtect 应用程序。 • **No**（否）— 不允许最终用户退出 GlobalProtect 应用程序。 此选项要求“内容发布”版本为 8196-5685 或更高。
使用单点登录 (Windows)	选择 **No**（否）可禁用单点登录 (SSO)。启用 SSO（默认）后，GlobalProtect 应用程序将自动使用 Windows 登录凭据进行身份验证，然后连接到 GlobalProtect 门户和网关。此外，GlobalProtect 也可包装第三方凭据，以确保 Windows 用户可以进行身份验证并连接，即便是使用第三方凭据提供程序来包装 Windows 登录凭据也不例外。
使用单点登录 (macOS)	选择 **No**（否）可禁用单点登录 (SSO)。启用 SSO（默认）后，GlobalProtect 应用程序将自动使用 macOS 登录凭据进行身份验证，然后连接到 GlobalProtect 门户和网关。 此选项要求“内容发布”版本为 8196-5685 或更高。
退出登录时清空单点登录凭据 （仅限 Windows）	选择 **No**（否）可在用户退出登录时，保留单点登录 (SSO) 凭据。选择 **Yes**（是）（默认）可将此凭据清除，并强制用户在下一次登录时输入凭据。
Kerberos 身份验证失败时使用默认身份验证	选择 **No**（否）可仅使用 Kerberos 身份验证。选择 **Yes**（是）（默认）可在对 Kerberos 进行身份验证失败后，使用默认的身份验证方法进行重试。该功能仅适用于 Mac 和 Windows 端点。
自动恢复 VPN 连接超时	输入一个从 0 到 180 的超时值（以分钟为单位），以指定 GlobalProtect 应用程序在由于网络不稳定或因输入导致端点状态更改而导致隧道断开连接时所采取的操作；默认值为 30。 • 0 — 禁用此功能，以便在隧道断开连接后，GlobalProtect 不会尝试重新建立隧道。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	• 1-180 — 启用此功能，以便 GlobalProtect 在隧道关闭一段时间后尝试重新建立隧道连接，这段时间不会超过您在此处指定的超时值。例如，在超时值为 30 分钟的情况下，如果隧道断开连接 45 分钟，GlobalProtect 不会尝试重新建立隧道。但是，如果隧道断开连接 15 分钟，GlobalProtect将尝试重新连接，因为分钟数未超过超时值。 使用始终启用 *VPN*，如果用户在超时值过期之前从外部网络切换到内部网络，则 *GlobalProtect* 不会执行网络发现。因此，*GlobalProtect* 将隧道重新连接到最后一个已知的外部网关。要触发内部主机检测，用户必须从 *GlobalProtect* 控制台选择重新发现网络。
VPN 连接恢复尝试之间的等待时间	输入启用 **Automatic Restoration of VPN Connection Timeout**（自动恢复 **VPN** 连接超时）后 GlobalProtect 应用程序在尝试重新建立与上次连接网关的连接之间的等待时间（以秒为单位）。根据您的网络状况指定更长或更短的等待时间。范围为 1 到 60 秒：默认值为 5。
强制执行 GlobalProtect 连接进行网络访问	选择 **Yes**（是）可强制所有网络流量遍历 GlobalProtect 隧道。如果访问网络不需要 GlobalProtect，并且在禁用或断开 GlobalProtect 连接后用户仍可访问互联网，可以选择 **No**（否）（默认）。 要在流量被阻止之前向用户说明，配置 **Traffic Blocking Notification Message**（流量阻止通知消息）并可选择指定何时显示该消息（**Traffic Blocking Notification Delay**（流量阻止通知延迟））。 要允许与强制网络门户建立连接所需的流量，请指定 **Captive Portal Exception Timeout**（强制网络门户例外超时）。用户必须在超时到期之前验证至门户。要提供其他说明，请配置 **Captive Portal Detection Message**（强制网络门户检测消息），并指定何时显示消息（**Captive Portal Notification Delay**（强制网络门户通知延迟））（可选）。 在大多数情况下，使用默认选择 *No*（否）。选择 *Yes*（是）可阻止进出端点的所有网络流量，直到应用程序连接到公司内的内部网关或公司网路外的外部网关。
已启用 **Enforce GlobalProtect Connection for Network Access**（强制执行 **GlobalProtect** 连接以访问网络）且未建立 **GlobalProtect** 连接时，允许指向指定主机/网络的流量	若需要，您可以在强制 GlobalProtect 进行网络访问但未建立连接时，配置最多十个您要允许访问的 IP 地址或网段。使用逗号分隔多个值。排除可以在 GlobalProtect 断开连接时允许用户访问本地资源，从而改善用户体验。例如，当未连接 GlobalProtect 时，GlobalProtect 可以排除本地链接地址，以允许访问本地网段或广播域。
强制网络门户例外超时（秒）	要强制使用 GlobalProtect 访问网络，但需要提供宽限期以允许用户有足够的时间连接到强制网络门户，请指定超时（以秒为单位，范围为 0 至 3600）。例如，值为 60 表示用户必须在

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	GlobalProtect 检测到强制网络门户后的一分钟内登录到强制网络门户。值为 0 表示 GlobalProtect 不允许用户连接到强制网络门户，并立即阻止访问。
强制网络门户检测时自动在默认浏览器中启动网页	要在强制网络门户检测时自动启动默认 Web 浏览器，以便用户可以无缝地登录到强制网络门户，请在首次尝试连接（在默认 Web 浏览器启动时发起 Web 流量）时输入您要使用的网站完全限定域名 (FQDN) 或 IP 地址（最大长度为 256 个字符）。随后，强制网络门户会拦截该网站连接尝试，并将默认 Web 浏览器重定向到强制网络门户登录页面。如果此字段为空（默认），则 GlobalProtect 不会在强制网络门户检测时自动启动默认 Web 浏览器。
通信阻塞通知延迟（秒）	指定一个值（以秒为单位），以确定显示通知消息的时间。访问网络后，GlobalProtect 开始倒计时显示通知（范围为 5 至 120，默认为 15）。
显示流量阻止通知消息	指定在访问网络需要使用 GlobalProtect 时是否显示消息。选择 **No**（否）可禁用消息。选择 **Yes**（是）可启用消息（在 GlobalProtect 断开连接但检测到网络可以访问时，GlobalProtect 会显示消息。）
流量阻止通知消息	自定义在使用 GlobalProtect 访问网络时要向用户显示的通知消息。在 GlobalProtect 断开连接但检测到网络可以访问时，GlobalProtect 会显示消息。该消息可以指示阻止流量的原因，并提供如何进行连接的说明。例如： `To access the network, you much first connect to GlobalProtect.` 消息长度必须为 512 个或更少的字符。
允许用户解除流量阻止通知	选择 **No**（否）可始终显示流量阻止通知。默认情况下，将该值设置为 **Yes**（是），表示允许用户关闭通知。
显示强制网络门户检测消息	指定在 GlobalProtect 检测到强制网络门户时是否显示消息。选择 **Yes**（是）可显示消息。选择 **No**（否）（默认）可禁止消息（在 GlobalProtect 检测到强制网络门户时，GlobalProtect 不显示消息）。 如果您启用强制网络门户检测消息，则该消息在强制网络门户例外超时之前 *85* 秒显示。因此，如果强制网络门户例外超时为 *90* 秒或更短，则该消息在检测到强制网络门户后 *5* 秒显示。
强制网络门户检测消息	自定义在 GlobalProtect 检测到网络时要向用户显示的通知消息，从而提供连接到强制网络门户的附加说明。例如： `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet`

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	`provider. If you let the connection time out, open GlobalProtect and click Connect to try again.` 消息长度必须为 512 个或更少的字符。
强制网络门户检测延迟	若启用强制网络门户检测消息，则可以指定强制网络门户检测后 GlobalProtect 显示检测消息的延迟（以秒为单位，范围为 1 到 120，默认为 5）。
客户端证书商店查找	选择应用程序将在其个人证书商店中查找的证书类型。GlobalProtect 应用程序将使用此证书对门户或网关进行身份验证，然后建立通往 GlobalProtect 网关的 VPN 隧道。 • **User**（用户）— 使用用户帐户的本地证书进行身份验证。 • **Machine**（机器）— 使用端点的本地证书进行身份验证。此证书适用于允许使用端点的所有用户账户。 • **User and machine**（用户和机器）（默认）— 使用用户证书和机器证书进行身份验证。
SCEP 证书续订期限（天数）	此机制可在证书实际到期之前，续订 SCEP 生成的证书。您可指定证书到期之前，门户可从 PKI 系统中的 SCEP 服务器请求新证书的最大天数（范围为 0 至 30，默认为 7）。若值为 0，则表示门户不会在其刷新客户端配置时，自动续订客户端证书。 对于要获取新证书的应用程序，用户必须在续订期内进行登录（如果用户不登录，则门户不会在此续订期内为用户请求新证书）。 例如，假定客户端证书的生命周期为 90 天，此证书的续订期为 7 天。如果用户在证书生命周期的最后 7 天进行登录，门户会生成证书，并将其与已刷新的客户端配置一同下载。请参阅 GlobalProtect 应用程序配置刷新时间间隔（小时）。
客户端证书扩展秘钥使用对象标识符 (OID)	通过指定客户端证书的对象标识符 (OID)，输入其扩展秘钥用法。此设置可确保 GlobalProtect 应用程序仅选择预期用于客户端身份验证的证书，且可使 GlobalProtect 保存此证书以便日后使用。
在拆除的智能卡上保持连接 （仅限 Windows）	选择 **Yes**（是）可在用户拆除包含客户端证书的智能卡时保持连接。选择 **No**（否）（默认）可在用户拆除智能卡时终止连接。
允许替代客户端证书中的用户名	选择 **No**（否）可强制 GlobalProtect 使用客户端证书的用户名，并阻止 GlobalProtect 对其进行替代（默认启用）。
启用高级视图	选择 **No**（否）可将应用程序上的用户界面限制为基本的最小视图（默认为启用）。
允许用户解除欢迎页面	选择 **No**（否）可强制欢迎页面在每次用户启动连接时显示。此限制可以防止用户忽略重要信息，如企业保持遵守适用标准可能需要的条款和条件。
启用 Rediscover Network（重新发现网络）选项	选择 **No**（否）可防止用户手动启动网络重新发现。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
启用 Resubmit Host Profile（重新提交主机配置文件）选项	选择 **No**（否）可防止用户手动触发最新 HIP 的重新提交。
允许用户更改门户地址	选择 **No**（否）可禁用 GlobalProtect 应用程序中 **Home**（主页）选项卡上的 **Portal**（门户）字段。但由于用户随后将无法指定要连接到的门户，因此您必须在 Windows 注册表或 Mac plist 中指定缺省门户地址： • **Windows 注册表** — `HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup`，键值为 `Portal` • **Mac plist** — `/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` with key `Portal` 有关预部署门户地址的更多信息，请参阅《GlobalProtect 管理员指南》中的自定义应用程序设置。
允许用户继续使用无效门户服务器证书	选择 **No**（否）可阻止应用程序在门户证书无效的情况下建立与门户的连接。
显示 GlobalProtect 图标	选择 **No**（否）可在端点上隐藏 GlobalProtect 图标。如果此图标为隐藏状态，则用户无法执行某些任务，如查看故障排除信息、更改密码、重新发现网络，或执行按需连接等。但 HIP 通知消息、登录提示和证书对话框会在进行必要的用户交互时显示。
用户交换机隧道重命名超时（秒） （仅限 Windows）	指定远程用户在使用 Microsoft 远程桌面协议 (RDP) 登录端点后，必须接受 GlobalProtect 网关对其进行身份验证的秒数（范围为 0 至 600，默认为 0）。要求远程用户在此时限内接受身份验证将有助于确保安全。 对新用户进行身份验证且切换隧道到该用户后，网关将重命名隧道。 若值为 0，则表示当前用户隧道未被重命名，但已被即刻终止。在此情况下，远程用户可获取新隧道，且在接受网关身份验证时无任何时间限制（而不是已配置的 TCP 超时）。
预登录隧道重命名超时（秒）（仅限 Windows）	此设置控制 GlobalProtect 如何处理将端点连接到网关的预登录隧道。 若值为 -1，则表示预登录隧道在用户登录到端点后不会超时；GlobalProtect 重命名隧道以将其重新分配给用户。但是，即使重命名失败或如果用户未登录到 GlobalProtect 网关，隧道仍然存在。 若值为 0，则表示当用户登录到端点后，GlobalProtect 立即终止预登录隧道，而不是重命名预登录隧道。在这种情况下，GlobalProtect 为用户启动新的隧道，而不是允许用户通过预登录隧道进行连接。通常，如果将 **Connect Method**（连接方法）设置为 **Pre-logon then On-demand**（预登录，然后按需），则此设置最有用，这可以迫使用户在初次登录后手动启动连接。 若值为 1 至 600，则表示在用户登录到端点后预登录隧道可以保持活动状态的秒数。在此期间，GlobalProtect 将在预登录隧道上执

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	行策略。如果用户在超时期限内使用 GlobalProtect 网关进行身份验证，则 GlobalProtect 会将隧道重新分配给用户。如果用户在超时之前未使用 GlobalProtect 网关进行身份验证，则 GlobalProtect 会终止预登录隧道。
用户注销时保留隧道超时（秒）	要使 GlobalProtect 在用户注销其端点后保留现有的 VPN 隧道，请指定 **Preserve Tunnel on User Logoff Timeout**（用户注销时保留隧道超时）的值（范围为 0 到 600 秒，默认为 0 秒）。如果接受默认值 0，则 GlobalProtect 不会在用户注销后保留隧道。
显示系统托盘通知 （仅限 Windows）	选择 **No**（否）可对用户隐藏通知。选择 **Yes**（是）（默认）可在系统托盘区域显示通知。
自定义密码过期消息 （仅限 LDAP 身份验证）	创建要在用户密码即将过期时，向其显示的自定义消息。消息长度不得超过 200 个字符。
在 IPSec 不可靠时自动使用 SSL（小时）	指定您希望 GlobalProtect 应用程序 **Automatically Use SSL When IPSec Is Unreliable**（在 **IPSec** 不可靠时自动使用 **SSL**）的时长（以小时为单位）（范围为 0-168 小时）。如果您配置此选项，GlobalProtect 应用不会在指定时间内尝试建立 IPSec 隧道。每当 IPSec 隧道由于隧道“保持连接”超时而关闭时，此计时器启动。 如果您接受默认值 0，若此应用可以成功建立 IPSec 隧道，则不会回退以建立 SSL 隧道。仅当无法建立 IPSec 隧道时，其会回退以建立 SSL 隧道。 这些选项要求“内容发布”版本为_____ 或更高。
GlobalProtect 连接 MTU（字节）	输入 GlobalProtect 应用程序用于连接到网关的 GlobalProtect 连接最大传输单位(MTU)，该值范围为 1000-1420 字节。默认值为 1400 字节。您可以优化最终用户通过 MTU 值小于标准值 1500 字节的网络进行连接的连接体验。通过减小 MTU，一旦 VPN 隧道连接经过多个 MTU 值小于 1500 字节的互联网服务提供商 (ISP) 和网络路径，您就可以消除因分段导致的性能和连接问题。
最大内部网关连接尝试次数	输入 GlobalProtect 代理在第一次尝试连接到内部网关失败后进行重试的最大允许次数（范围为 0 至 100，默认为 0，“0”表示 GlobalProtect 应用程序不会重试连接）。通过增加该值，您能使应用程序自动连接到临时关闭的内部网关，或自动连接到首次尝试连接期间不可访问但在指定重试次数用尽前恢复正常的内部网关。增加该值还能确保内部网关接收到最新的用户和主机信息。
门户连接超时（秒）	门户连接请求因门户无响应而超时之前的秒数（范围为 1 至 600）。如果防火墙运行的应用程序和威胁内容版本低于 777-4484，则默认值为 30。从内容版本 777-4484 开始，默认值为 5。
TCP 连接超时（秒）	TCP 连接请求因任一连接端无响应而超时之前的秒数（范围为 1-600）。如果防火墙运行的应用程序和威胁内容版本低于

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	777-4484，则默认值为 60。从内容版本 777-4484 开始，默认值为 5。
TCP 接收超时（秒）	TCP 连接请求因 TCP 请求部分响应丢失而超时之前的秒数（范围为 1 至 600，默认为 30）。
使用通道分配的 DNS 服务器解析所有 FQDN（仅限 Windows）	（GlobalProtect 4.0.3 及更高版本）在 Windows 端点上连接 GlobalProtect 隧道时配置 DNS 解析首选项： • 选择 **Yes**（是）（默认）可使 GlobalProtect 应用程序让 Windows 端点使用您在网关上配置的 DNS 服务器来解析所有 DNS 查询，而不让端点将某些 DNS 查询发送到在物理适配器上设置的 DNS 服务器。 • 选择 **No**（否），如果对网关上配置的 DNS 服务器的初始查询未解析，则允许 Windows 端点将 DNS 查询发送到设置在物理适配器上的 DNS 服务器。此选项保留本机 Windows 行为以递归方式查询所有适配器上的所有 DNS 服务器，但可能导致解决某些 DNS 查询很长的等待时间。 要为 GlobalProtect 应用程序 4.0.2 及更低版本配置 DNS 设置，请使用 **Update DNS Settings at Connect**（连接时更新 **DNS** 设置）选项。
连接时更新 DNS 设置 （仅限 Windows）（已弃用）	（GlobalProtect 4.0.2 及更低版本）为 GlobalProtect 隧道配置 DNS 服务器首选项： • 如果未解析对网关上配置的 DNS 服务器的初始查询，选择 **No**（否）（默认）可让 Windows 端点将 DNS 查询发送到在物理适配器上设置的 DNS 服务器。此选项保留本机 Windows 行为以递归方式查询所有适配器上的所有 DNS 服务器，但可能导致解决某些 DNS 查询很长的等待时间。 • 选择 **Yes**（是）可让 Windows 端点解析对您在网关上配置的 DNS 服务器（而非在端点上的物理适配器上设置的 DNS 服务器）的所有 DNS 查询。启用此选项时，GlobalProtect 严格执行网关 DNS 设置并覆盖所有物理适配器的静态设置。 启用此设置（设置为 *Yes*（是））后，*GlobalProtect* 可能无法恢复先前保存的 *DNS* 设置，因此可能阻止端点解析 *DNS* 查询。此功能已遭弃用并由改进后的功能所取代，因此不会发生此情况。如果您之前使用此功能，我们建议升级到 *GlobalProtect* 应用程序 *4.0.3* 或更高版本。 要为 GlobalProtect 应用程序 4.0.3 及更高版本配置 DNS 设置，请使用 **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel**（使用隧道分配的 **DNS** 服务器解析所有 **FQDN**）选项。
检测每个连接的代理 （仅限 Windows）	选择 **No**（否）可自动检测门户连接的代理并使用此代理进行后续连接。选择 **Yes**（是）（默认）可自动检测每个连接的代理。
在代理上设置隧道（仅限 Windows 和 Mac）	指定 GlobalProtect 是否必须使用或绕过代理。选择 **No**（否）要求 GlobalProtect 绕过代理。选择 **Yes**（是）要求 GlobalProtect

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
	使用代理。根据 GlobalProtect 代理使用、端点操作系统和隧道类型，网络流量 的行为将有所不同。
Windows 安全中心 (WSC) 状态变更后立即发送 HIP 报告 （仅限 Windows）	选择 **No**（否）可防止 GlobalProtect 应用程序在 Windows 安全中心 (WSC) 状态变更后发送 HIP 数据。选择 **Yes**（是）（默认）可在 Windows 安全中心 (WSC) 状态变更后立即发送 HIP 数据。
从 MFA 网关启用入站身份验证提示	要支持多因素身份验证 (MFA)，GlobalProtect 端点必须接收并确认从网关入站的 UDP 提示。选择 **Yes**（是）可使 GlobalProtect 端点接收并确认提示。选择 **No**（否）（默认）可使 GlobalProtect 阻止来自网关的 UDP 提示。
入站身份验证提示的网络端口 (UDP)	指定 GlobalProtect 端点用于接收来自 MFA 网关的传入身份验证提示的端口号。默认端口为 4501。要更改端口，请指定从 1 至 65535 之间的数字。
信任的 MFA 网关	指定 GlobalProtect 端点为多因素身份验证信任的防火墙或身份验证网关列表。当 GlobalProtect 端点在指定的网络端口上接收 UDP 消息时，GlobalProtect 仅在 UDP 提示来自受信任的网关时才会显示身份验证消息。
入站身份验证消息	自定义当用户尝试访问需要执行额外身份验证的资源时要显示的通知消息。当用户尝试访问需要额外身份验证的资源时，GlobalProtect 会收到一个包含入站身份验证提示的 UDP 数据包，并显示此消息。该 UDP 数据包还包含您在配置多因素身份验证时指定的身份验证门户页面的 URL。GlobalProtect 自动将 URL 附加到消息中。例如： `You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at` 消息长度必须为 255 个或更少的字符。
首选 IPv6	指定 GlobalProtect 端点通信的首选协议。选择 **No**（否）可将首选协议更改为 IPv4。选择 Yes（是）（默认）可使 IPv6 成为双栈环境的首选连接。
更改密码消息	当用户更改其活动目录 (AD) 密码时，自定义消息以指定密码策略或要求。例如： `Passwords must contain at least one number and one uppercase letter.` 对于双字节的 Unicode 语言（如简体中文），消息长度必须为 255 个或更少的字符。对于日语，消息长度必须为 128 个或更少的字符。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 应用程序配置设置	说明
日志网关选择标准	选择 **Yes**（是）以允许 GlobalProtect 应用程序发送网关选择标准日志到防火墙。默认值为 **No**（否）。应用程序不会发送网关选择标准增强日志到防火墙。
启动时显示状态面板（仅限 Windows）	选择 **Yes**（是）可在用户首次建立连接时显示 GlobalProtect 状态面板。选择 **No**（否）可在用户首次建立连接时禁止显示 GlobalProtect 状态面板。
禁用 GlobalProtect 应用	
通行码/确认通行码	如果 **Allow User to Disable GlobalProtect App**（允许用户禁用 **GlobalProtect** 应用程序）的设置为 **Allow with Passcode**（带通行码允许），请输入通行码，再进行确认。请将此通行码等同于密码对待，作好记录并存储于安全的位置。您可通过电子邮件将通行码分发到新 GlobalProtect 用户，或将其张贴在企业网站的支持区域。 如果环境不允许端点建立 VPN 连接且此功能已禁用，用户可在应用程序界面输入此通行码，以禁用 GlobalProtect 应用程序并获取互联网访问权限，而无需再使用 VPN。
用户可以禁用的最长时间	指定在需要成功连接到防火墙之前用户可禁用 GlobalProtect 的最大次数。默认值为 0，即表示用户可无限次禁用应用程序。
禁用超时（分钟）	指定 GlobalProtect 应用程序可被禁用的最大分钟数。在指定时间过去后，应用程序将尝试连接到防火墙。默认为 0，即表示禁用无时间限制。 设置禁用超时值，以限制用户可以禁用此应用程序的时间量。这样，可确保 *GlobalProtect* 在超时结束后恢复，并建立 *VPN*，从而保护用户和用户对资源的访问。
Mobile Security Manager 设置	
Mobile Security Manager	如果使用 GlobalProtect Mobile Security Manager 进行移动设备管理 (MDM)，请输入 GP-100 设备上设备检入/注册界面的 IP 地址或 FQDN。
注册端口	在移动端点连接到 GlobalProtect Mobile Security Manager 以进行注册时应使用的端口号。默认情况下，Mobile Security Manager 在端口 443 上进行侦听。 保留此端口号，以便移动端点的用户不会在注册期间收到要其使用客户端证书的提示（其他可能的值为 *443*、*7443* 和 *8443*）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户 *Agent HIP Data Collection*（代理 *HIP* 数据收集）选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）> *<agent-config>* > **HIP Data Collection**（**HIP** 数据收集）

选择**HIP Data Collection**（**HIP** 数据收集）选项卡以定义应用程序从 HIP 报告端点中收集的数据：

GlobalProtect HIP 数据收集配置设置	说明
收集 HIP 数据	取消选中此选项可阻止应用程序收集并发送 HIP 数据。 使 *GlobalProtect* 收集基于 *HIP* 策略实施的 *HIP* 数据，这样，防火墙可将从端点收集的 *HIP* 数据与您定义的 *HIP* 对象和/或 *HIP* 配置文件进行匹配，然后应用适当的策略。
最长等待时间（秒）	指定应用程序应在提交可用数据前搜索 HIP 数据的秒数（范围为 10-60，默认为 20）。
证书配置文件	选择 GlobalProtect 门户用于匹配 GlobalProtect 应用程序发送的机器证书的证书配置文件。
排除类别	选择 **Exclude Categories**（排除类别）可指定您不希望应用程序为其收集 HIP 数据的主机信息类别。选择要从 HIP 收集中排除的 **Category**（类别）（如 data-loss-prevention）。选择类别后，您可 **Add**（添加）特定供应商，然后可再 **Add**（添加）来自供应商的产品，以根据需要进一步完善排除设置。单击 **OK**（确定）保存每个对话框中的设置。
自定义检查	选择 **Custom Checks**（自定义检查）可定义您希望应用程序收集的自定义主机信息。例如，如果您有任何必需应用程序未包含在用于创建 HIP 对象的供应商或产品列表中，则您可以创建自定义检查以确定是否已安装应用程序（如已安装，则具有对应的 Windows 注册表或 Mac plist 项），或者是否正在运行（具有对应的运行进程）： • **Windows** — **Add**（添加）特定注册表项或键值的选中标记。 • **Windows** — **Add**（添加）特定 plist 项或键值的选中标记。 • **Process List**（进程列表）— **Add**（添加）要在用户端上查看的进程，以确定其是否正在运行。例如，要确定某个软件应用程序是否正在运行，请将这个可执行文件的名称添加到进程列表中。您可以在 **Windows** 选项卡或 **Mac** 选项卡中添加进程，或同时在两个选项卡中添加。

GlobalProtect 门户无客户端 VPN 选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Clientless VPN**（无客户端 **VPN**）

现在，您可以配置 GlobalProtect 门户远程安全访问使用 HTML、HTML5 和 JavaScript 技术的常见企业 Web 应用程序。用户无需安装 GlobalProtect 软件，即可从启用 SSL 的 Web 浏览器进行安全访问。如果您需要合作伙伴或承包商能够访问应用程序，且安全启用非托管资产（包括个人设备），则这非常有用。此功能需要在从 GlobalProtect 门户托管无客户端 VPN 的防火墙上安装 GlobalProtect 订阅。选择 **Clientless VPN**（无客户端 **VPN**）选项卡可以在门户上配置 GlobalProtect 无客户端 VPN 设置，如下表中所述：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户无客户端配置设置	说明
“常规”选项卡	
无客户端 VPN	选择 **Clientless VPN**（无客户端 **VPN**）以指定有关无客户端 VPN 会话的常规信息：
主机名	托管 Web 应用程序登录页面的 GlobalProtect 门户的 IP 地址或 FQDN。GlobalProtect 无客户端 VPN 使用此主机名重写应用程序 URL。 如果您使用网络地址转换 *(NAT)* 提供 *GlobalProtect* 门户的访问权限，则输入的 *IP* 地址或 *FQDN* 必须与 *GlobalProtect* 门户（公共 *IP* 地址）的 *NAT IP* 地址相匹配（或解析为 *NAT IP* 地址）。
安全区域	无客户端 VPN 配置的区域。在该区域中定义的安全规则控制用户可以访问的应用程序。
DNS 代理	解析应用程序名称的 DNS 服务器。选择 **DNS proxy**（**DNS** 代理）服务器或配置 **New DNS Proxy**（新建 **DNS** 代理）（Network（网络）> DNS Proxy（DNS 代理））。
登录生命周期	无客户端 SSL VPN 会话有效的 **Minutes**（分钟）数（范围为 60 至 1440）或 **Hours**（小时）数（范围为 1 至 24，默认为 3）。在指定时间过后，用户必须重新进行身份验证，并启动新的无客户端 VPN 会话。
不活动超时	无客户端 SSL VPN 会话可以保持空闲的 **Minutes**（分钟）数（范围为 5 至 1440，默认为 30）或 **Hours**（小时）数（范围为 1 至 24）。如果在指定的时间内用户没有执行任何操作，用户必须重新进行身份验证，并启动新的无客户端 VPN 会话。
最大用户数	可以同时登录到门户的最大用户数（默认为 10，范围为 1 到无限）。如果达到最大用户数，其他无客户端 VPN 用户无法登录到门户。
应用程序选项卡	
应用程序到用户的映射	**Add**（添加）一个或多个 **Applications to User Mapping**（应用程序到用户映射）以将用户与发布的应用程序进行相匹配。此映射控制可以使用无客户端 VPN 访问应用程序的用户或用户组。必须先定义应用程序和应用程序组，然后才能将它们映射到用户（Network（网络）> GlobalProtect > Clientless Apps（无客户端应用程序）和 Network（网络）> GlobalProtect > Clientless App Groups（无客户端应用程序组））。 • **Name**（名称）— 输入映射的名称（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。 • **Display application URL address bar**（显示应用程序 **URL** 地址栏）— 选择此选项可显示应用程序 URL 地址栏，用户可从中启动未在应用程序登录页面上发布的应用程序。启用此选项后，用户可以单击页面上的 **Application URL**（应用程序 **URL**）链接并指定 URL。
用户/用户组	您可 **Add**（添加）要应用当前应用程序配置的独立用户或用户组。这些用户拥有使用 GlobalProtect 无客户端 VPN 启动配置的应用程序的权限。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户无客户端配置设置	说明
	必须配置组映射（*Device*（设备）> *User Identification*（用户标识）> *Group Mapping Settings*（组映射设置））之后才能选择组。 除用户和组之外，您还可指定何时将这些设置应用到用户或组： • **any**（任何）— 将应用程序配置应用到所有用户（无需 **Add**（添加）用户或用户组）。 • **select**（选择）— 仅将应用程序配置应用到 **Add**（添加）到该列表的用户和用户组。
应用程序	可以将各个应用程序或应用程序组 **Add**（添加）到映射。配置中包含的 **Source Users**（源用户）可以使用 GlobalProtect 无客户端 VPN 启动添加的应用程序。
加密设置选项卡	
协议版本	选择所需的最低和最高 TLS/SSL 版本。TLS 版本越高，连接越安全。选择包括 **SSLv3**、**TLSv1.0**、**TLSv1.1** 或 **TLSv1.2**。
密钥交换算法	选择支持的密钥交换算法类型。选择包括 **RSA**、Diffie-Hellman (**DHE**) 或临时椭圆曲线 Diffie-Hellman (**ECDHE**)。
加密算法	选择支持的加密算法。建议使用 **AES128** 或更高版本。
身份验证算法	选择支持的身份验证算法。选择包括：**MD5**、**SHA1**、**SHA256**或**SHA384**。建议使用 **SHA256** 或更高版本。
服务器证书验证	为应用程序提供服务器证书时可能会发生的以下问题采取的操作： • **Block sessions with expired certificate**（阻止证书已过期的会话）— 如果服务器证书已过期，则阻止访问应用程序。 • **Block sessions with untrusted issuers**（阻止颁发者不可信的会话）— 如果服务器证书是由不受信任的证书颁发机构颁发，则阻止访问应用程序。 • **Block sessions with unknown certificate status**（阻止证书状态未知的会话）— 如果 OCSP 或 CRL 服务返回未知的证书吊销状态，则阻止访问应用程序。 • **Block sessions on certificate status check timeout**（阻止证书状态检查超时的会话）— 如果证书状态检查在收到任何证书状态服务的响应之前超时，则阻止访问应用程序。
代理选项卡	
姓名	标签最多包含 31 个字符，可标识 GlobalProtect 门户用于访问已发布应用程序的代理服务器。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。
域	添加代理服务器提供的域。
使用代理	选择此选项可使 GlobalProtect 门户使用代理服务器访问发布的应用程序。
服务器	指定代理服务器的主机名（或 IP 地址）和端口号。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户无客户端配置设置	说明
端口	
用户 密码	指定登录到代理服务器所需的用户名和密码。再次输入密码进行验证。
高级设置选项卡	
重写排除域列表	（可选）将域名、主机名或 IP 地址 **Add**（添加）到 **Rewrite Exclude Domain List**（重写排除域列表）。无客户端 VPN 充分反向代理，并修改发布的应用程序返回的页面。当远程用户访问 URL 时，请求将通过 GlobalProtect 门户。在某些情况下，应用程序可能包含不需要通过门户访问的页面。指定应从重写规则中排除且无法重写的域。 主机和域名不支持路径。主机和域名的通配符 (*) 只能出现在名称的开头（如 *.etrade.com）。

GlobalProtect 门户卫星选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Satellite**（卫星）

卫星设备是 Palo Alto Networks® 防火墙，通常设在分支办公室，充当 GlobalProtect 应用程序以使其能够建立与 GlobalProtect 网关的 VPN 连接。与 GlobalProtect 应用程序一样，卫星设备从门户接收其初始配置，这包括证书和 VPN 配置路由信息，以使卫星设备能够连接所有已配置的网关，从而建立 VPN 连接。

在分支机构防火墙上配置 GlobalProtect 卫星设置，必须首先配置与 WAN 连接的接口，然后设置一个允许分支办公室 LAN 与 Internet 通信的安全区域和安全策略。然后可以选择 **Satellite**（卫星）以在门户上配置 GlobalProtect 卫星设置，如下表中所述：

GlobalProtect 门户卫星配置设置	说明
General（常规）	• **Name**（名称）— GlobalProtect 门户上该卫星配置的名称。 • **Configuration Refresh Interval (hours)**（配置刷新间隔（小时））— 指定卫星检查门户配置更新的频率（范围为 1-48，默认为 24）。
设备	使用防火墙 **Serial Number**（序列号）来 **Add**（添加）卫星。门户可接受序列号或登录凭据，用以识别连接请求的发出方；如果门户不接收序列号，即表明需要提供登录凭据。如果通过卫星的防火墙序列号来对其进行识别，则在卫星首次连接时，不需要提供用户登录凭据来获取身份验证证书及其初始配置。 通过序列号或登录凭据对卫星进行身份验证后，**Satellite Hostname**（卫星主机名）将自动添加到门户。
登记用户/用户组	不论是否具备序列号，门户均可使用 **Enrollment User/User Group**（注册用户/用户组）设置，将卫星与配置进行匹配。对于与序列号不匹配的卫星，需将其作为个人用户或用户组成员进行身份验证。 **Add**（添加）要使用此配置控制的用户或组。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户卫星配置设置	说明
	必须启用防火墙中的组映射（*Device*（设备）> *User Identification*（用户标识）> *Group Mapping Settings*（组映射设置））才可将配置限定到特定组。
网关	单击 **Add**（添加）以输入网关卫星的 IP 地址或主机名，以便该配置可用其建立 IPSec 隧道。在网关字段中，输入在其上配置网关的接口的 FQDN 或 IP 地址。可以将 IP 地址指定为 **IPv6**、**IPv4** 或两者。选择 **IPv6 Preferred**（首选 **IPv6**）以指定双栈环境中 IPv6 连接的首选项。 （可选）如果要将两个或多个网关添加到配置，**Routing Priority**（路由优先级）有助于卫星选择首选网关（范围为 1 至 25）。数值越小，优先级越高（适用于可用网关）。卫星会将路由优先级乘以 10 来确定路由跳数。 在卫星上安装网关发布的路由作为静态路由。静态路由的跳数为 *10* 乘以路由优先级。如果拥有多个网关，请确保同时设置路由优先级，以便备份网关通告的路由拥有比主网关通告的同一路由更高的跳数。例如，如果将主网关和备份网关的路由优先级分别设置为 *1* 和 *10*，则卫星将使用 *10* 作为主网关的跳数，并使用 *100* 作为备份网关的跳数。 如果 **Publish all static and connected routes to Gateway**（将所有静态路由和已连接的路由发布到网关）（**Network**（网络）> **IPSec tunnels**（**IPSec** 隧道）> **<tunnel**（**<**隧道）> **Advanced**（高级）—仅当选择 **GlobalProtect Satellite on the <tunnel**（**<**隧道上的 **GlobalProtect** 卫星）> **General**（常规）选项时可用），卫星还会与网关共享其网络和路由信息。
可信的根 CA	单击 **Add**（添加），然后选择用于签发网关服务器证书的 CA 证书。同时，卫星可信根 CA 证书与门户代理配置同时推送到端点。 指定可信根 *CA* 以验证网关服务器证书，并建立到 *GlobalProtect* 网关的安全 *VPN* 隧道连接。所有网关均使用同一颁发者。 您可 *Import*（导入）或 *Generate*（生成）根 *CA* 证书，以便在门户上不存在此证书时，将其用于签发网关服务器证书。
客户端证书	
本地	• **Issuing Certificate**（签发证书）— 选择门户在卫星成功完成身份验证后，用于对其签发证书的根 CA 签发证书。如果防火墙上暂不存在所需的证书，您可选择 **Import**（导入）或 **Generate**（生成）此证书。 如果证书尚未驻留于防火墙上，您可选择 *Import*（导入）或 *Generate*（生成）签发证书。 • **OCSP Responder**（**OCSP** 响应者）— 为卫星选择 OCSP 响应者，以便卫星用其验证门户和网关所呈递的证书吊销状态。选择 **None**（无）以指定不会使用 OCSP 验证证书的吊销。 启用卫星 *OCSP* 响应者，这样，如果证书被吊销，会通知您采取适当的操作来建立到门户和网关的安全连接。要启用卫

© 2019 Palo Alto Networks, Inc.

GlobalProtect 门户卫星配置设置	说明
	星 *OCSP* 响应者，您还必须启用证书吊销检查设置中的*CRL* 和 *OCSP*（*Device*（设备）> *Setup*（设置）> *Session*（会话）> *Decryption Settings*（解密设置））。 • **Validity Period**（有效期限）（天数）— 指定 GlobalProtect 卫星证书的生命周期（范围为 7 至 365 天，默认为 7 天）。 • **Certificate Renewal Period**（证书续订期限）（天数）— 指定到期前证书可被自动续订的天数（范围为 3 至 30 天，默认为 3 天）。
Scep	• **SCEP** — 选择用于生成客户端证书的 SCEP 配置文件。如果此配置文件不在下拉列表中，您可选择 **New**（新建）配置文件。 • **Certificate Renewal Period**（证书续订期限）（天数）— 指定到期前证书可被自动续订的天数（范围为 3 至 30 天，默认为 3 天）。

© 2019 Palo Alto Networks, Inc.

Network（网络）> GlobalProtect > Gateways（网关）

选择 **Network**（网络）> **GlobalProtect** > **Gateways**（网关）可配置 GlobalProtect 网关。网关可为 GlobalProtect 应用程序或 GlobalProtect 卫星提供 VPN 连接。

在 GlobalProtect 网关对话框中 **Add**（添加）新网关配置，或选择已有的网关配置以对其进行修改。

您在查找什么内容？	请参阅：
我能为 GlobalProtect 网关配置哪些常规设置？	GlobalProtect 网关常规选项卡
我要如何配置网关客户端身份验证？	GlobalProtect 网关身份验证选项卡
我要如何配置隧道和网络设置才能使应用程序建立与网关的 VPN 隧道？	GlobalProtect 网关代理选项卡
我要如何配置隧道和网络设置才能使卫星与作为卫星的网关建立 VPN 连接？	GlobalProtect 网关卫星选项卡
了解更多？	有关设置门户的详细分步骤说明，请参阅《GlobalProtect 管理员指南》中的配置 GlobalProtect 门户。

GlobalProtect 网关常规选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **General**（常规）

选择 **General**（常规）选项卡可定义应用程序能够连接到的网关接口并可指定网关对端点进行身份验证的方式。

GlobalProtect 网关常规设置	说明
姓名	输入网关的名称（最多31个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	对于处于多虚拟系统模式下的防火墙，**Location**（位置）是指提供 GlobalProtect 网关的虚拟系统 (vsys)。对于不是处于多虚拟系统模式下的防火墙，**Location**（位置）字段不会出现在 GlobalProtect Gateway（GlobalProtect 网关）对话框中。 在保存网关配置后，您无法更改其 *Location*（位置）。
网络设置区域	
接口	选择将作为远程端点入口接口的防火墙接口的名称。（这些接口必须是现有接口。）

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关常规设置	说明
	请勿将允许 *Telnet*、*SSH*、*HTTP* 或 *HTTPS* 的接口管理配置文件附加到已配置 *GlobalProtect* 门户或网关的接口，因为这会将管理接口暴露给互联网。有关如何保护对管理网络的访问权限的更多详细信息，请参阅保护管理访问权限的最佳做法。
IP 地址	（可选）指定网关访问的 IP 地址。选择 **IP Address Type**（**IP** 地址类型），然后输入 **IP Address**（**IP** 地址）。 • IP 地址类型可以是 **IPv4**（仅限 IPv4 流量）、**IPv6**（仅限 IPv6 流量）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的网络支持双栈配置（IPv4 和 IPv6 同时运行），请使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。 IP 地址必须与 IP 地址类型兼容。例如，172.16.1.0（对于 IPv4）或 21DA:D3:0:2F3b（对于 IPv6）。如果您选择 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），请为每个地址输入适当的地址类型。
日志设置	
记录成功的 SSL 握手	（可选）为成功的 SSL 解密握手创建详细日志。默认情况下禁用。 日志会占用存储空间。在记录成功的 *SSL* 握手之前，必须确保有足够的资源存储日志。编辑*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Logging and Reporting Settings*（记录和报告设置）以检查当前日志内存分配，并为各种日志类型分配内存。
记录失败的 SSL 握手	为失败的 SSL 解密握手创建详细日志，以便您能找到导致解密失败的原因。默认情况下启用。 日志会占用存储空间。若要分配更多（或更少）的日志存储空间给解密日志，请编辑日志内存分配（*Device*（设备）> *Setup*（设置）> *Management*（管理）> *Logging and Reporting Settings*（记录和报告设置））。
日志转发	指定转发 GlobalProtect SSL 握手（解密）日志的方法和位置。

GlobalProtect 网关身份验证选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Authentication**（身份验证）

选择 **Authentication**（身份验证）选项卡可识别 SSL/TLS 服务配置文件，并配置客户端身份验证的详细信息。您可添加多个客户端身份验证配置。

GlobalProtect 网关身份验证设置	
SSL/TLS 服务配置文件	选择 SSL/TLS 服务配置文件，以便对此 GlobalProtect 网关进行保护。有关服务配置文件内容的详细信息，请参阅 Device（设备）> Certificate Management（证书管理）> SSL/TLS Service Profile（SSL/TLS 服务配置文件）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关身份验证设置	
客户端身份验证区域	
姓名	输入可标识此配置的唯一名称。
OS	默认情况下，此配置适用于所有端点。您可按照操作系统（**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows** 或 **WindowsUWP**）、**Satellite**（卫星）设备或第三方 IPSec VPN 客户端 (**X-Auth**) 优化端点列表。 操作系统是多个配置之间的首要区分项。如果需要一个操作系统配备多个配置，您可通过选择身份验证配置文件来对多个配置进行进一步区分。 对配置进行排序，使列表从上到下依次为最特定配置到最常规配置。
身份验证配置文件	从下拉列表中选择用于对网关访问权限进行身份验证的身份验证配置文件或序列。请参阅 Device（设备）> Authentication Profile（身份验证配置文件）。 对于客户端身份验证，确保身份验证配置文件使用 *RADIUS* 或 *SAML* 进行双因素身份验证。如果未使用 *RADIUS* 或 *SAML*，除了身份验证配置文件外，还需配置证书配置文件 。
用户名标签	指定 GlobalProtect 网关登录的自定义用户名标签。例如，用户名（唯一）或电子邮件地址 (**username@domain**)。
密码标签	指定 GlobalProtect 网关登录的自定义密码标签。例如，密码（土耳其语）或密码（用于基于令牌的双因素身份验证）。
身份验证消息	要帮助最终用户了解应用于登录此网关的凭据，您可输入消息或保留默认消息。该消息的最大长度为 256 个字符。
允许使用用户凭证或客户端证书进行身份验证	如果选择 **No**（否），用户必须使用用户凭证和客户端证书对网关进行身份验证。如果选择 **Yes**（是），用户可以使用用户凭证或客户端证书对网关进行身份验证。
证书配置文件	
证书配置文件	（可选）选择网关用于对来自用户端的客户端证书进行匹配的 **Certificate Profile**（证书配置文件）。选择证书配置文件后，网关将仅当来自客户端的证书与该配置文件相匹配时，才对用户进行身份验证。 如果将 **Allow Authentication with User Credentials OR Client Certificate**（允许使用用户凭证或客户端证书进行身份验证）选项设置为 **No**（否），则必须选择**Certificate Profile**（证书配置文件）。如果将 **Allow Authentication with User Credentials OR Client Certificate**（允许使用用户凭证或客户端证书进行身份验

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关身份验证设置	
	证）选项设置为 **Yes**（是），则可以选择 **Certificate Profile**（证书配置文件）。 此证书配置文件独立于操作系统。
阻止隔离设备登录	指定是否阻止隔离列表中 GlobalProtect 客户端设备的网关登录（**Device**（设备）> **Device Quarantine**（设备隔离））。

GlobalProtect 网关代理选项卡

- **Network**（网络）> **GlobalProtect** > **Portals**（门户）> *<portal-config>* > **Agent**（代理）

选择 **Agent**（代理）选项卡可配置隧道设置，以使应用程序能够建立与网关的 VPN 隧道。此外，此选项卡还可让您在不论是否对附加到安全策略规则的 HIP 配置文件进行匹配的情况下，指定 VPN、DNS 和 WINS 的网络服务及 HIP 为最终用户提供通知消息的超时时间。

配置以下选项卡上的 Agent（代理）设置：

- 隧道设置选项卡
- 客户端设置选项卡
- 客户端 IP 池选项卡
- 网络服务选项卡
- 连接设置选项卡
- 视频通信选项卡
- HIP 通知选项卡

隧道设置选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Agent**（代理）> *<agent-config>* > **Tunnel Settings**（隧道设置）

选择 **Tunnel Settings**（隧道设置）选项卡可启用隧道，并配置隧道参数。

仅当在设置外部网关时，才需要隧道参数。如果配置内部网关，则隧道参数是可选的。

GlobalProtect 网关客户端隧道模式配置设置	说明
隧道模式	选择 **Tunnel Mode**（隧道模式）可启用隧道模式，并指定以下设置： • **Tunnel Interface**（隧道接口）— 选择用于访问此网关的隧道接口。 • **Max User**（最大用户数）— 指定可以同时访问网关以进行身份验证、HIP 更新和 GlobalProtect 应用程序更新的最大用户数。如果达到最大用户数，则拒绝后续用户访问，并显示消息，指示已达到最大用户数（范围因平台而有所不同，并在字段为空时显示）。 • **Enable IPSec**（启用 **IPSec**）— 选中此选项可使端点通信使用 IPSec 模式，从而使 IPSec 成为主方法，而 SSL-VPN 成为回退方法。在 IPSec 启用之前，其余选项均不可用。 • **GlobalProtect IPSec** 加密 — 选择 GlobalProtect IPSec 加密配置文件可指定用于 VPN 隧道的身份验证和加密算法。**default**（默认）配置文件使用 AES-128-CBC 加密算法和 SHA1 身份验证。有关详细信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> GlobalProtect IPSec Crypto（GlobalProtect IPSec 加密）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端隧道模式配置设置	说明
	• **Enable X-Auth Support**（启用扩展身份验证支持）— 选中此选项可在启用 IPSec 时启用 GlobalProtect 网关中的扩展身份验证 (X-Auth) 支持。凭借 X-Auth 支持，支持 X-Auth 的第三方 IPSec VPN 客户端（例如 Apple iOS 和 Android 设备上的 IPSec VPN 客户端以及 Linux 上的 VPNC 客户端）可与 GlobalProtect 网关建立 VPN 隧道。使用 X-Auth 选项，可以从 VPN 客户端远程访问某个特定 GlobalProtect 网关。由于 X-Auth 访问仅提供了有限的 GlobalProtect 功能，因此请考虑使用 GlobalProtect 应用以对 GlobalProtect 在 iOS 和 Android 设备上提供的完整安全功能集进行简化访问。 选中 **X-Auth Support**（X-Auth 支持）将激活 **Group Name**（组名）和 **Group Password**（组密码）选项： • 如果指定了组名称和组密码，则身份验证的第一阶段要求双方均使用此凭据进行身份验证。第二个阶段需要有效的用户名和密码（通过在身份验证部分中配置的身份验证配置文件进行验证）。 • 如果未定义组名称和组密码，则身份验证的第一个阶段基于第三方 VPN 客户端提供的有效证书。然后，通过在身份验证部分中配置的证书配置文件验证此证书。 • 默认情况下，当用于建立 IPSec 隧道的密钥过期后，用户不需要重新进行身份验证。若要求用户重新进行身份验证，请取消选中 **Skip Auth on IKE Rekey**（在 **IKE Rekey** 上跳过身份验证）选项。

客户端设置选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Agent**（代理）> *<agent-config>* > **Client Settings**（客户设置）

选择 **Client Settings**（客户端设置）选项卡可在 GlobalProtect 应用程序建立与网关的隧道时，为端点上的虚拟网络适配器配置设置。

仅当启用隧道模式并在隧道设置选项卡上定义隧道接口后，某些 *Client Settings*（客户端设置）选项才可用。

GlobalProtect 网关客户端设置和网络配置	说明
配置选择标准选项卡	
姓名	输入标识客户端设置配置的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
源用户	**Add**（添加）要将此配置应用到的特定用户或用户组。 必须配置组映射（*Device*（设备）> *User Identification*（用户标识）> *Group Mapping Settings*（组映射设置））之后，才能选择用户和组。 要将此配置部署到所有用户，请从 **Source User**（源用户）下拉列表中选择 **any**（任何）。要将此配置部署到预登录模式中拥有

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端设置和网络配置	说明
	GlobalProtect 应用程序的用户，请从 **Source User**（源用户）下拉列表中选择 **pre-logon**（预登录）。 仅当用户匹配 *Source User*（源用户）、*OS* 和 *Source Address*（源地址）的标准时，客户端设置配置才会部署到用户。
OS	要根据端点上运行的操作系统部署此配置，请 **Add**（添加）操作系统（**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows**、**WindowsUWP**）。或者，您也可以将此值设置为 **Any**（任何），以使配置部署仅根据用户或用户组，而不会根据端点的操作系统。 仅当用户匹配 *Source User*（源用户）、*OS* 和 *Source Address*（源地址）的标准时，客户端设置配置才会部署到用户。
Source Address（源地址）	要根据用户位置部署此配置，**Add**（添加）源 **Region**（区域）或本地 **IP Address**（**IP** 地址）（IPv4 和 IPv6）。要将此配置部署到所有用户地址，请不要指定 **Region**（区域）和 **IP Address**（**IP** 地址）。此外，如果用户正在运行 GlobalProtect 应用程序 4.0 及更早版本，还必须将这些字段留空，因为 GlobalProtect 应用程序 4.0 以前的版本不支持此功能。 如果连接用户的位置与 *Region*（区域）或您配置的 *IP Address*（*IP* 地址）匹配，则*Source Address*（源地址）的匹配是成功的。 仅当用户匹配 *Source User*（源用户）、*OS* 和 *Source Address*（源地址）的标准时，客户端设置配置才会部署到用户。
身份验证替代选项卡	
身份验证覆盖	在用户使用由身份验证或证书配置文件指定的身份验证方案，进行首次身份验证之后，使网关能够使用安全、设备特定且已加密的 Cookie 对用户进行身份验证。 • **Generate cookie for authentication override**（生成用于身份验证覆盖的 **Cookie**）— 在 Cookie 的生命周期期间，代理将在每次用户用网关进行身份验证时，递送此 Cookie。 • **Cookie Lifetime**（**Cookie** 生命周期）— 指定 Cookie 有效的小时数、天数或周数。典型的生命周期为 24 小时。范围为 1–72 小时、1–52 周或 1–365 天。Cookie 过期后，用户必须输入登录凭据，网关随后会加密要发送到用户设备的新 Cookie。 • **Accept cookie for authentication override**（接受用于身份验证覆盖的 **Cookie**）— 选择此选项可配置网关接受使用加密 Cookie 进行的身份验证。代理递送此 Cookie 后，网关将在对用户进行身份验证之前，验证 Cookie 是否已被网关加密。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端设置和网络配置	说明
	• **Certificate to Encrypt/Decrypt Cookie**（加密/解密 **Cookie** 的证书）— 选择网关在对 Cookie 进行加密和解密时所使用的证书。 请确保门户和网关均使用相同的证书对 *Cookie* 进行加密和解密。
IP 池选项卡	
从身份验证服务器检索 Framed-IP-Address 属性	选择此选项能使 GlobalProtect 网关使用外部身份验证服务器分配固定 IP 地址。启用此选项后，GlobalProtect 网关会使用身份验证服务器的 Framed-IP-Address 属性来分配用于连接到设备的 IP 地址。
身份验证服务器 IP 池	**Add**（添加）要分配给远程用户的子网或 IP 地址范围。建立隧道后，GlobalProtect 网关会使用身份验证服务器的 Framed-IP-Address 属性，将在此范围内的 IP 地址分配给连接设备。您可以添加 IPv4 地址（例如 192.168.74.0/24 和 192.168.75.1-192.168.75.100）或 IPv6 地址（例如 2001:aa::1-2001:aa::10）。 只有在启用了 **Retrieve Framed-IP-Address attribute from authentication server**（从身份验证服务器检索 **Framed-IP-Address** 属性）之后，才能启用并配置 **Authentication Server IP Pool**（身份验证服务器 **IP** 池）。 身份验证服务器 *IP* 池必须足够大以支持所有的并发连接。*IP* 地址分配为固定，且在用户断开连接后会保留地址分配。从不同子网配置多个范围，可允许系统为客户端提供一个不与该客户端上的其他接口冲突的 *IP* 地址。 网络中的服务器和路由器必须将此 IP 池的通信路由到防火墙。例如，对于 192.168.0.0/16 网络，远程用户可通过其接收地址 192.168.0.10。
Ip 池	**Add**（添加）要分配给远程用户的 IP 地址范围。建立隧道时，将用此范围内的地址在远程用户的端点上创建接口。您可以添加 IPv4 地址（例如 192.168.74.0/24 和 192.168.75.1-192.168.75.100）或 IPv6 地址（例如 2001:aa::1-2001:aa::10）。 为了避免冲突，*IP* 池必须足够大以支持所有的并发连接。网关保持客户端和 *IP* 地址的索引，这样客户端可以在下一次连接时自动收到同一 *IP* 地址。从不同子网配置多个范围，可允许系统为客户端提供一个不与该客户端上的其他接口冲突的 *IP* 地址。 网络中的服务器和路由器必须将此 IP 池的通信路由到防火墙。例如，对于 192.168.0.0/16 网络，可以为远程用户分配地址 192.168.0.10。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端设置和网络配置	说明
拆分隧道选项卡	
访问路由选项卡	
不能直接访问本地网络	选择此选项可禁用拆分隧道，包括在 Windows 和 Mac 操作系统端点上直接访问本地网络。此功能可防止用户将通信发送到代理或本地资源，如家用打印机。在建立隧道后，通过隧道路由所有通信且应符合防火墙执行的策略。
包括	**Add**（添加）要包括在 VPN 隧道中的路由。这些路由是网关推送到远程用户端点的路由，以指定用户端点可以通过 VPN 连接发送的内容。 要包括所有的目标子网或地址对象，则 *Include*（包含）作为访问路由的 *0.0.0.0/0* 和 *::/0*。
排除	**Add**（添加）要从 VPN 隧道中排除的路由。这些路由通过端点上的物理适配器发送，而不是通过虚拟适配器（隧道）发送。 您可以定义通过 VPN 隧道发送的路由作为隧道中包含的路由、从隧道中排除的路由或两者的组合。例如，可以将拆分隧道设置为允许远程用户无需经由 VPN 隧道便可访问互联网。排除的路由应比包括的路由更具体，以避免排除的流量比要排除的流量更多。 如果不包括或排除路由，则每个请求都会通过隧道进行路由（无拆分隧道）。在这种情况下，每个互联网请求均会穿过防火墙，到达网络。该方法可以防止外部某一方访问用户端点，并获得内部网络的访问权限（用户端点在此情况下充当网桥）。
域和应用程序选项卡	
包含域	使用域和端口（可选）添加要包含在 VPN 隧道中的软件即服务 (SaaS) 或公共云应用程序。这些应用程序是网关推送到远程用户端点的应用程序，以指定用户端点可以通过 VPN 连接发送的内容。 您可以为每个域配置端口列表。如果没有配置端口，则指定域的所有端口均受此策略的约束。
排除域	使用域和端口（可选）添加要从 VPN 隧道中排除的软件即服务 (SaaS) 或公共云应用程序。这些应用程序通过端点上的物理适配器发送，而不是通过虚拟适配器（隧道）发送。 您可以为每个域配置端口列表。如果没有配置端口，则指定域的所有端口均受此策略的约束。 如果不包含或排除任何域，则每个请求都会通过隧道进行路由（无拆分隧道）。在这种情况下，每个互联网请求均会穿过防火墙，到达网络。这种方法可以防止外部用户访问用户端点，从而获取内部网络访问权限。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端设置和网络配置	说明
包含客户端应用程序进程名称	使用应用程序进程名称添加要包含在 VPN 隧道中的软件即服务 (SaaS) 或公共云应用程序。这些应用程序是网关推送到远程用户端点的应用程序，以指定用户端点可以通过 VPN 连接发送的内容。
排除客户端应用程序进程名称	使用应用程序进程名称添加要从 VPN 隧道中排除的软件即服务 (SaaS) 或公共云应用程序。这些应用程序通过端点上的物理适配器发送，而不是通过虚拟适配器（隧道）发送。 如果不包含或排除任何应用程序，则每个请求都会通过隧道进行路由（无拆分隧道）。在这种情况下，每个互联网请求均会穿过防火墙，到达网络。这种方法可以防止外部用户访问用户端点，从而获取内部网络访问权限。
网络服务选项卡	
DNS 服务器	指定 DNS 服务器的 IP 地址，以便拥有此客户端设置配置的 GlobalProtect 应用程序向其发送 DNS 查询。您可以采用逗号分隔每个 IP 地址的方式添加多个 DNS 服务器。
DNS 后缀	当输入的非限定主机名无法被端点解析时，指定客户端应在本地使用的 DNS 后缀。可以输入多个 DNS 后缀（以逗号分隔，最多 100 个）。

客户端 *IP* 池选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Agent**（代理）> *<agent-config>* > **Client IP Pool**（客户端 **IP** 池）

选择 **Client IP Pool**（客户端 **IP** 池）选项卡可配置用于将 IPv4 或 IPv6 地址分配给连接到 GlobalProtect™ 网关的所有端点的全局 IP 池。

GlobalProtect 网关客户端 IP 池配置设置	说明
Ip 池	**Add**（添加）要分配给远程用户的 IPv4 或 IPv6 地址范围。建立隧道后，GlobalProtect 网关将此范围内的 IP 地址分配给通过该隧道连接的所有端点。 如果配置网关级别的 *IP* 池（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *GlobalProtect Gateway Configuration*（*GlobalProtect* 网关配置）> *Agent*（代理）> *Client IP Pool*（客户端 *IP* 池）），则不要配置客户端级别的任何 *IP* 池（*Network*（网络）> *GlobalProtect* > *Gateways*（网关）> *<gateway-config>* > *GlobalProtect Gateway Configuration*（*GlobalProtect* 网关配置）> *Agent*（代理）> *Client Settings*（客户端设置）> *<client-*

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端 IP 池配置设置	说明
	setting> > *Configs*（配置）> *IP Pools*（*IP* 池））。

网络服务选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> <*gateway-config*> > **Agent**（代理）> <*agent-config*> > **Network Services**（网络服务）

选择 **Network Services**（网络服务）选项卡可在 GlobalProtect 应用程序建立与网关的隧道时，配置将分配到端点上虚拟网络适配器的 DNS 设置。

仅当您已启用隧道模式并且在隧道设置选项卡上定义隧道接口后，*Network Services*（网络服务）选项才可用。

GlobalProtect 网关客户端网络服务配置设置	说明
继承源	选择一个源，从这个源将所选 DHCP 客户端或 PPPoE 客户端界面中的 DNS 服务器和其他设置传播到 GlobalProtect 应用程序的配置。进行此设置后，从在继承源中选择的界面配置继承 DNS 服务器和 WINS 服务器等所有客户端网络配置。
检查继承源状态	单击 Inheritance Source（继承源）可查看当前分配给客户端界面的服务器设置。
主 DNS 辅助 DNS	输入向客户端提供 DNS 的主辅服务器的 IP 地址。
主 WINS 辅助 WINS	输入向端点提供 Windows 互联网命名服务 (WINS) 的主辅服务器的 IP 地址。
继承 DNS 后缀	选中此选项可继承来自继承源的 DNS 后缀。
DNS 后缀	**Add**（添加）当输入的非限定主机名无法解析时，端点应在本地使用的后缀。可以输入多个后缀（以逗号分隔，最多 100 个）。

连接设置选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> <*gateway-config*> > **Agent**（代理）> <*agent-config*> > **Connection Settings**（连接设置）

选择 **Connection Settings**（连接设置）选项卡以定义 GlobalProtect™ 应用程序的超时设置和身份验证 cookie 使用限制。

GlobalProtect 网关客户端隧道模式连接设置	说明
Timeout configuration	

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关客户端隧道模式连接设置	说明
登录生命周期	指定单个网关登录会话所允许的天数、小时数或分钟数。
非活动注销	指定天数、小时数或分钟数，在此之后将自动注销非活动的会话。
空闲时断开连接	指定应用程序停止路由通过 VPN 隧道的流量后，在端点从 GlobalProtect 应用程序注销之前经过的时间量（以分钟为单位）。
身份验证 Cookie 使用限制	
禁用自动恢复 SSL VPN	启用此选项后，可阻止自动恢复 SSL VPN 隧道。 如果启用此选项，则 *GlobalProtect* 将不支持弹性 *VPN*。
限制身份验证 Cookie 使用（用于自动恢复 VPN 隧道或身份验证替代）	启用此选项后，可根据以下条件之一对身份验证 cookie 使用情况进行限制： • 身份验证 **cookie** 颁发的原始源 **IP** — 限制身份验证 cookie 使用情况到具有与最初颁发 cookie 的端点相同的公共源 IP 地址的端点。 • 原始源 **IP** 网络范围—限制身份验证 cookie 使用情况到指定网络 IP 地址范围内使用公共源 IP 地址的端点。输入 **Source IPv4 Netmask**（源 **IPv4** 网络掩码）以指定 IPv4 地址的范围，或是输入 **Source IPv6 Netmask**（源 **IPv6** 网络掩码）以指定 IPv6 地址的范围。 如果设置网络掩码为 0，则对指定 IP 地址类型禁用此项。例如，如果您的门户或网关仅支持一种 IP 地址类型（IPv4 或 IPv6），或如果您想仅为一种 IP 地址类型启用此选项（当您的门户或网关支持 IPv4 和 IPv6），则设置网络掩码为 0。在指定网关配置中，您只能设置一个网络掩码为 0；您不能同时将两个网络掩码都设置为 0。 如果您接收值为 32 的默认 **Source IPv4 Netmask**（源 **IPv4** 网络掩码），则身份验证 cookie 使用情况将限制为具有与最初颁发 cookie 的端点相同的公共 IP 地址的端点。如果您接收值为128的默认**Source IPv6 Netmask**（源 **IPv6** 网络掩码），则身份验证 cookie 使用情况将限制为具有与最初颁发 cookie 的端点相同的公共 IP 地址的端点。

视频通信选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Agent**（代理）> *<agent-config>* > **Video Traffic**（视频通信）

选择 **Video Traffic**（视频通信）选项卡可排除来自 VPN 隧道的视频流通信。

GlobalProtect 网关视频通信配置设置	说明
从隧道中排除视频应用程序	选择此选项以从 VPN 隧道中排除视频流通性。
应用程序	对您要从 VPN 隧道中排除的视频流应用程序执行 **Add**（添加）或 **Browse**（浏览）操作。 该视频重定向适用于以下应用程序的任何视频通信类型：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关视频通信配置设置	说明
	• Youtube • Dailymotion • Netflix 对于其他视频流应用程序，仅以下视频类型可以重定向： • MP4 • WebM • MPEG 视频流通信只能从 VPN 隧道中排除。如果不排除任何视频流应用程序，则所有请求都会通过隧道（无拆分隧道）进行路由。在这种情况下，每个互联网请求均会穿过防火墙，到达网络。这种方法可以防止外部用户访问用户端点，从而获取内部网络访问权限。

HIP 通知选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Agent**（代理）> *<agent-config>* > **HIP Notification**（**HIP** 通知）

选择 **HIP Notification**（**HIP** 通知）选项卡可定义在实施具有主机信息配置文件 (HIP) 的安全规则时，最终用户将看到的通知消息。

只有创建了 HIP 配置文件并将其添加到安全策略后，才可使用这些选项。

GlobalProtect 代理 HIP 通知配置设置	说明
HIP 通知	**Add**（添加）HIP 通知并配置选项。您可 **Enable**（启用）**Match Message**（匹配消息）和/或 **Not Match Message**（不匹配消息）的通知，然后指定是否 **Show Notification As**（将通知显示为）**System Tray Balloon**（系统托盘气球）或 **Pop Up Message**（弹出消息）。之后再指定是否匹配消息。 使用这些设置可以将机器的状态通知最终用户，比如一条用于说明主机系统未安装某个必需应用的警告消息。对于匹配消息，您还可以启用 **Include Mobile App List**（包含移动应用程序列表）选项，以表明触发 HIP 匹配的应用程序。 可按富 *HTML* 格式化 *HIP* 通知消息，即其中可包括指向外部网站和资源的链接。单击富文本设置工具栏中的链接图标 添加超链接。

GlobalProtect 网关卫星选项卡

- **Network**（网络）> **GlobalProtect** > **Gateways**（网关）> *<gateway-config>* > **Authentication**（身份验证）

卫星是 Palo Alto Networks 防火墙，通常设在分支办公室，充当 GlobalProtect 应用程序以使其能够建立与 GlobalProtect 网关的 VPN 连接。选择 **Satellite**（卫星）选项卡可定义网关隧道和网络设置以使卫星能够与其建立 VPN 连接。您还可配置卫星通告的路由。

© 2019 Palo Alto Networks, Inc.

- 隧道设置选项卡
- 网络设置选项卡
- 路由筛选程序选项卡

GlobalProtect 网关卫星配置设置	说明
隧道设置选项卡	
隧道配置	选择 **Tunnel Configuration**（隧道配置）并选择现有的 **Tunnel Interface**（隧道接口），或从下拉列表中选择 **New Tunnel Interface**（新隧道接口）。有关更多信息，请参阅 **Network**（网络）> **Interfaces**（接口）> **Tunnel**（隧道）。 • **Replay attack detection**（重播攻击检测）— 防御重播攻击。 如果启用卫星隧道配置，则启用 *Replay attack detection*（重播攻击检测）以保护 *GlobalProtect* 卫星免受重播攻击。 • **Copy TOS**（复制 **TOS**）— 将服务类型 (ToS) 标头从封装的数据包的内部 IP 标头复制到外部 IP 标头，以保留原始 ToS 信息。 • **Configuration refresh interval (hours)**（配置刷新间隔（小时））— 指定卫星检查门户配置更新的频率（范围为 1-48，默认为 2）。
隧道监控	选择 **Tunnel Monitoring**（隧道监控）能使卫星监控网关隧道连接，以允许它们在连接失败时故障转移至备份网关。 • **Destination Address**（目标地址）— 为隧道监视器指定将用来确定是否存在网关连接的 **Ipv4** 或 **Ipv6** 地址（例如，受网关保护的网络上的 IP 地址）。或者，如果已配置隧道接口的 IP 地址，可以将此字段留空，并且隧道监视器将改用隧道接口确定连接是否处于活动状态。 • 隧道监视器配置文件 — 故障转移至其他网关是使用 LSVPN 支持的隧道监控配置文件的唯一类型。 如果启用卫星隧道配置，则启用 *Tunnel Monitoring*（隧道监控），并配置隧道监控配置文件。
加密配置文件	选择 **IPSec Crypto Profile**（**IPSec** 加密配置文件），或创建新的配置文件。加密配置文件可确定用于对 VPN 隧道进行标识、身份验证和加密的协议和算法。因为 LSVPN 中的两个隧道端点是组织内受信任的防火墙，因此通常可以使用默认配置文件，该配置文件使用 ESP 协议、DH group2、AES 128 CVC 加密和 SHA-1 身份验证。有关更多信息，请参阅 Network（网络）> Network Profiles（网络配置文件）> GlobalProtect IPSec Crypto（GlobalProtect IPSec 加密）。
网络设置选项卡	
继承源	选择一个来源，从这个来源将所选 DHCP 客户端或 PPPoE 客户端界面中的 DNS 服务器和其他设置传播到 GlobalProtect 卫星配置。进行此设置后，从在 Inheritance Source（继承源）中选择的界面配置继承 DNS 服务器等所有网络配置。
主 DNS 辅助 DNS	输入向卫星提供 DNS 的主辅服务器的 IP 地址。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 网关卫星配置设置	说明
DNS 后缀	单击添加可输入一个后缀，当输入的非限定主机名无法解析时，卫星应在本地使用该后缀。可以输入多个后缀（以逗号分隔）。
继承 DNS 后缀	选中此选项将 DNS 后缀发送给卫星，当输入的非限定主机名无法解析时，卫星会在本地使用该后缀。
Ip 池	**Add**（添加）可创建一个 IP 地址范围，只要有 VPN 隧道建立就会将其中的 IP 地址分配给卫星上的隧道接口。您可以指定 IPv6 或 IPv4 地址。 若要支持所有的并发连接，*IP* 池必须足够大。*IP* 地址分配是动态，卫星断开连接后不会保留地址分配。从不同子网配置多个范围，可允许系统为卫星提供一个不与其上的其他接口冲突的 *IP* 地址。 网络中的服务器和路由器必须将此 IP 池的通信路由到防火墙。例如，对于 192.168.0.0/16 网络，可以为卫星分配地址 192.168.0.10。 如果使用动态路由，请确保指定给卫星的 IP 地址池不会与手动分配给网关和卫星上隧道接口的 IP 地址重叠。
访问路由	单击 **Add**（添加），然后按照以下说明输入路由： • 如果要通过隧道路由卫星的所有流量，将该字段留空。 • 要仅通过网关路由一些流量（称为拆分隧道），指定必须建立隧道的目标子网。在这种情况下，卫星将使用自己的路由表路由不是发往指定访问路由的流量。例如，您可以选择仅将隧道流量发往公司网络，并使用本地卫星启用安全 Internet 访问。 • 如果要在卫星之间启用路由，输入受每颗卫星保护的网络的汇总路由。
路由筛选程序选项卡	
接受发布的路由	选择 **Accept published routes**（接受发布的路由）可接受由卫星在网关的路由表中所通告的路由。如果不选择此选项，则网关将不会接受卫星所通告的任何路由。
允许的子网	如果希望更加严格地限制接受卫星所通告的路由，请 **Add**（添加）允许的子网并定义网关可接受其路由的子网；将筛选掉卫星所通告的不属于该列表的子网。例如，如果所有卫星在 LAN 端都使用 192.168.x.0/24 子网配置，则可以在网关上配置允许的路由 192.168.0.0/16。此配置会导致仅当网关处于 192.168.0.0/16 子网中时，网关才会接受来自卫星的路由。

© 2019 Palo Alto Networks, Inc.

Network（网络） > GlobalProtect > MDM

如果在使用 Mobile Security Manager 管理最终用户移动端点并且在使用支持 HIP 的策略实施，则必须配置网关以与 Mobile Security Manager 通信，从而检索受管端点的 HIP 报告。

Add（添加）Mobile Security Manager 的 MDM 信息，以使网关能够与 Mobile Security Manager 进行通信。

GlobalProtect MDM 设置	说明
姓名	输入 Mobile Security Manager 的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
	如果防火墙处于多虚拟系统模式下，则 MDM 设置将显示 Mobile Security Manager 可用的虚拟系统 (vsys)。对于未处于多虚拟系统模式下的防火墙，此字段将不会出现在 MDM 对话框中。在保存 Mobile Security Manager 后，您无法更改其位置。
连接设置	
服务器	输入网关在 Mobile Security Manager 上将连接到（以检索 HIP 报告）的接口的 IP 地址或 FQDN。确保您具有此接口的服务路由。
连接端口	此连接端口是 Mobile Security Manager 用于侦听 HIP 报告请求的端口。默认端口是 5008，这也是 GlobalProtect Mobile Security Manager 侦听的同一个端口。如果在使用第三方 Mobile Security Manager，请输入该服务器侦听 HIP 报告请求时使用的端口号。
客户端证书	选择在建立 HTTPS 连接时网关要呈递给 Mobile Security Manager 的客户端证书。仅当 Mobile Security Manager 配置为使用相互身份验证时，此证书才是必需的。
可信的根 CA	单击 **Add**（添加），然后选择用于为网关连接以检索 HIP 报告的接口签发证书的根 CA 证书。（此服务器证书可以不同于为 Mobile Security Manager 上的端点检入界面所签发的证书）。您必须导入根 CA 证书并将其添加到此列表。

© 2019 Palo Alto Networks, Inc.

Network（网络）> GlobalProtect > Device Block List（设备阻止列表）

选择 **Network**（网络）> **GlobalProtect** > **Device Block List**（设备阻止列表）（仅限防火墙）可将端点添加到 GlobalProtect 设备阻止列表。此列表上的端点将不可建立 GlobalProtect VPN 连接。

设备阻止列表设置	说明
姓名	输入设备阻止列表的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	对于处于多虚拟系统模式下的防火墙，**Location**（位置）是指提供 GlobalProtect 网关的虚拟系统 (vsys)。对于不是处于多虚拟系统模式下的防火墙，**Location**（位置）字段不会出现在 GlobalProtect Gateway（GlobalProtect 网关）对话框中。在保存网关配置后，您无法更改其 **Location**（位置）。
主机 ID	输入标识端点的唯一 ID，此 ID 为主机名和唯一设备 ID 的组合。对于每个主机 ID，请指定对应的主机名。
主机名	输入标识该设备的主机名（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。

© 2019 Palo Alto Networks, Inc.

Network（网络）> GlobalProtect > Clientless Apps（无客户端应用）

选择 **Network**（网络）> **GlobalProtect** > **Clientless Apps**（无客户端应用程序）可添加通过 GlobalProtect 无客户端 VPN 访问的应用程序。您可以添加单个无客户端应用程序，然后选择 **Network**（网络）> **GlobalProtect** > **Clientless App Groups**（无客户端应用程序组）以定义应用程序组。

GlobalProtect 无客户端 VPN 提供对使用 HTML、HTML5 和 JavaScript 技术的常见企业 Web 应用程序的安全远程访问。用户无需安装 GlobalProtect 软件，即可从启用 SSL 的 Web 浏览器进行安全访问。如果您需要合作伙伴或承包商能够访问应用程序，且安全启用非托管资产（包括个人设备），则这非常有用。

您需要 **GlobalProtect Clientless VPN**（**GlobalProtect** 无客户端 **VPN**）动态更新才能使用此功能。此功能还需要在从 GlobalProtect 门户托管无客户端 VPN 的防火墙上安装 GlobalProtect 订阅。

无客户端应用程序设置	说明
姓名	输入描述应用程序的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
位置	对于处于多虚拟系统模式下的防火墙，**Location**（位置）是指提供 GlobalProtect 网关的虚拟系统 (vsys)。对于不是处于多虚拟系统模式下的防火墙，**Location**（位置）字段不会出现在 GlobalProtect Gateway（GlobalProtect 网关）对话框中。在保存网关配置后，您无法更改其 **Location**（位置）。
应用程序主页 URL	输入应用程序所在的 URL（最多 4095 个字符）。
应用程序说明	（可选）输入应用程序的说明（最多 255 个字符）。仅可使用字母、数字、空格、连字符和下划线。
应用程序图标	（可选）上传图标以标识已发布应用程序页面上的应用程序。您可以浏览以上传图标。

© 2019 Palo Alto Networks, Inc.

Network（网络）> GlobalProtect > Clientless App Groups（无客户端应用组）

选择 **Network**（网络）> **GlobalProtect** > **Clientless App Groups**（无客户端应用程序组）可对通过 GlobalProtect 无客户端 VPN 访问的应用程序进行分组。您可以将现有的无客户端应用程序添加到组或为组配置新的无客户端应用程序。组可以用于同时处理多个应用程序。例如，您可能拥有一组要为无客户端 VPN 访问配置的标准 SaaS 应用程序（如 Workday、JIRA 或 Bugzilla）。

无客户端应用程序组设置	说明
姓名	输入描述应用程序组的名称（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。
位置	对于处于多虚拟系统模式下的防火墙，**Location**（位置）是指提供 GlobalProtect 网关的虚拟系统 (vsys)。对于不是处于多虚拟系统模式下的防火墙，**Location**（位置）字段不会出现在 GlobalProtect Gateway（GlobalProtect 网关）对话框中。在保存网关配置后，您无法更改其 **Location**（位置）。
应用程序	从下拉列表中 **Add**（添加）**Application**（应用程序），或配置新的无客户端应用程序并将其添加到组。要配置新的无客户端应用程序，请参阅 Network（网络）> GlobalProtect > Clientless Apps（无客户端应用程序）。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> GlobalProtect > HIP Objects（HIP 对象）

选择 **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）可定义主机信息配置文件 (HIP) 的对象。HIP 对象将提供匹配条件，以便筛选要用于执行策略的应用程序所报告的原始数据。例如，如果原始主机数据包含有关端点上多个防病毒软件数据包的信息，您可能因为您的企业/组织需要该数据包而关注特定的应用程序。在这种情况下，您将创建 HIP 对象以匹配您要运行的特定应用程序。

确定您需要的 HIP 对象的最佳方法是，确定您将如何使用主机信息来执行策略。切记，HIP 对象仅仅是构建块，可让您创建安全策略能够使用的 HIP 配置文件。因此，您可能希望保持对象简化，与一个对象匹配，例如，是否存在特定类型的必需软件、特定域中的成员身份或者是否存在特定端点操作系统。采用这种方法，您将能够灵活创建很精细的 HIP 扩充策略。

要创建 HIP 对象，请单击添加以打开“HIP 对象”对话框。有关要在特定字段中输入的内容的说明，请参阅下表。

- HIP 对象常规选项卡
- HIP 对象移动设备选项卡
- HIP 对象修补程序管理选项卡
- HIP 对象防火墙选项卡
- HIP 对象反恶意软件选项卡
- HIP 对象磁盘备份选项卡
- HIP 对象磁盘加密选项卡
- HIP 对象数据丢失保护选项卡
- HIP 对象证书选项卡
- HIP 对象自定义检查选项卡

有关创建 HIP 扩充安全策略的更多详细信息，请参阅《*GlobalProtect* 管理员指南》中的配置基于 HIP 的策略实施。

HIP 对象常规选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **General**（常规）

选择 **General**（常规）选项卡可指定新 HIP 对象的名称，配置要与常规主机信息（如，域、操作系统或者其网络连接类型）匹配的对象。

HIP 对象常规设置	说明
姓名	输入 HIP 对象的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
共享	如果选择 **Shared**（共享），则当前 HIP 对象将适用于： 防火墙上的所有虚拟系统 (vsys)（如果您登录到处于多虚拟系统模式下的防火墙）。如果取消选中此选项，则此对象将仅适用于 **Objects**（对象）选项卡 **Virtual System**（虚拟系统）下拉列表中选定的虚拟系统。对于未处于多虚拟系统模式下的防火墙，HIP Object（HIP 对象）对话框中不可使用此选项。 Panorama™ 上的所有设备组。如果取消选中此选项，则此对象将仅适用于 **Objects**（对象）选项卡 **Device Group**（设备组）下拉列表中选定的设备组。

© 2019 Palo Alto Networks, Inc.

HIP 对象常规设置	说明
	在保存对象后，您无法更改其共享设置。选择 **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）可查看当前 **Location**（位置）.
说明	（可选）输入说明。
主机信息	选中此选项可激活配置主机信息的选项。
受管	根据端点是否受管进行过滤。要匹配受管的端点，请选择 **Yes**（是）。要匹配不受管的端点，请选择 **No**（否）。
禁用替代（仅限 Panorama）	控制替代访问设备组中的 HIP 对象，这些设备组是在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）的子对象。选中此选项可通过替代继承值，防止管理员创建子对象设备组中对象的本地副本。默认未选中此选项（即替代已启用）。
域	如需匹配域名，请从下拉列表中选择运算符，并输入要匹配的字符串。
OS	如需匹配主机操作系统，请从第一个下拉列表中选择 **Contains**（包含），从第二个下拉列表中选择供应商，然后从第三个下拉列表中选择操作系统版本，或者选择 **All**（全部）以匹配所选供应商的任何操作系统版本。
客户端版本	要匹配某个特定版本号，请从下拉列表中选择一个运算符，然后在文本框中输入要匹配（或者不匹配）的字符串。
主机名	要匹配特定主机名或主机名的一部分，请从下拉列表中选择一个运算符，然后在文本框中输入要匹配（或者不匹配，取决于您选择的运算符）的字符串。
主机 ID	主机 ID 是 GlobalProtect 分配用于标识主机的唯一 ID。主机 ID 值因设备类型而异： • **Windows** — 存储在 Windows 注册表中的机器 GUID (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) • **macOS** — 第一个内置物理网络接口的 MAC 地址 • **Android** — Android ID • **iOS** — UDID • **Linux** — 从系统 DMI 表检索的产品 UUID • **Chrome** — GlobalProtect 分配的唯一字母数字字符串，长度为 32 个字符 要匹配特定主机名 ID，请从下拉列表中选择一个运算符，然后在文本框中输入要匹配（或者不匹配，取决于您选择的运算符）的字符串。
序列号	要匹配完整的端点序列号或其中一部分，请从下拉列表中选择一个运算符，然后输入要匹配的字符串。
网络	使用此字段可启用对特定移动设备网络配置的筛选。该匹配条件仅适用于移动设备。 从下拉列表中选择一个运算符，然后选择从第二个下拉列表中选择要筛选的网络连接类型：**Wifi**、移动或 **Ethernet**（仅可用于非过滤器）或未知。选择网络类型后，输入要匹配的任何其他字符串（如果可用），如移动设备运营商或 Wifi **SSID**。

© 2019 Palo Alto Networks, Inc.

HIP 对象移动设备选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Mobile Device**（移动设备）

选择 **Mobile Device**（移动设备）选项卡可针对从移动设备（运行 GlobalProtect 应用）收集的数据启用 HIP 匹配。

要收集移动设备属性并在 *HIP* 执行策略中使用这些属性，*GlobalProtect* 需要借助 *MDM* 服务器。*GlobalProtect* 目前支持 *HIP* 与 *AirWatch MDM* 服务器的集成。

HIP 对象移动设备设置	说明
移动设备	选中此选项可启用筛选从运行 GlobalProtect 应用程序的移动设备收集的数据，并启用设备、设置和应用程序选项卡。
设备选项卡	• 型号 — 要匹配特定设备型号，请从下拉列表中选择运算符，并输入要匹配的字符串。 • 标记 — 要匹配 GlobalProtect Mobile Security Manager 上定义的标记值，请从第一个下拉列表中选择运算符，然后从第二个下拉列表中选择一个标记。 • 电话号码 — 要匹配完整的电话号码或其中一部分，请从下拉列表中选择一个运算符，然后输入要匹配的字符串。 • **IMEI** — 要匹配设备的完整国际移动设备标识 (IMEI) 码或其中一部分，请从下拉列表中选择一个运算符，然后输入要匹配的字符串。
设置选项卡	• 通行码 — 根据设备是否设置了通行码来进行过滤。要匹配已设置通行码的设备，请选择 **Yes**（是）。要匹配未设置通行码的设备，请选择否。 • 破解/越狱 — 根据设备已破解或者已越狱来进行过滤。要匹配已破解/越狱的设备，请选择 **Yes**（是）。要匹配未破解/越狱的设备，请选择 **No**（否）。 • 磁盘加密 — 根据设备数据是否已加密来进行过滤。要匹配启用了磁盘加密的设备，请选择是。要匹配未启用磁盘加密的设备，请选择 No（否）。 • 自上一次签入之后的时间 — 根据设备上次在 MDM 中签入之后的时间进行过滤。从下拉列表中选择运算符，然后指定签入窗口的天数。例如，您可以将对象定义为匹配在 5 天内未签入的设备。

应用程序选项卡	• **Apps**（应用程序）—（仅限 Android 设备）选中此选项可根据设备上安装的应用以及设备是否安装了受恶意软件感染的应用来启用筛选。
	• **Criteria**（标准）选项卡
	  • **Has Malware**（有恶意软件）— 选择 **Yes**（是）以匹配安装了受恶意软件感染的应用程序的设备。选择 **No**（否）以匹配未安装受恶意软件感染的应用程序的设备。选择 **None**（无）不使用 **Has Malware**（有恶意软件）作为匹配标准。
	• **Include**（包含）选项卡
	  • **Package**（数据包）— 要匹配安装了特定应用程序的设备，请 **Add**（添加）应用程序，并以反向 DNS 格式输入唯一的应用程序名称。例如 com.netflix.mediaclient，然后输入相应的程序程序 **Hash**（哈希），使 GlobalProtect 应用程序使用设备 HIP 报告进行计算并提交。

© 2019 Palo Alto Networks, Inc.

HIP 对象修补程序管理选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Patch Management**（修补程序管理）

选择**Patch Management**（修补程序管理）选项卡可对 GlobalProtect 端点的修补程序状态启用 HIP 匹配。

HIP 对象修补程序管理设置	说明
补丁程序管理	选中此选项可启用主机的修补程序管理状态匹配，并启用标准和 供应商选项卡。
标准选项卡	指定以下设置： • 已安装 — 匹配主机上是否安装了修补程序管理软件。 • 已启用 — 匹配主机上是否启用了修补程序管理软件。如果取消选中 **Is Installed**（已安装），则此字段会自动设置为 **None**（无）并且被禁止编辑。 • **Severity**（严重性）— 从逻辑运算符列表中进行选择，以匹配主机是否缺少指定严重性值的修补程序。 使用 GlobalProtect 严重性值和 OPSWAT 严重性评级之间的以下映射来了解每个值的含义： • **0** — 低 • **1** — 中等 • **2** — 严重 • **3** — 非常严重 • **Check**（检查）— 匹配端点是否缺少修补程序。 • 修补程序 — 匹配主机是否具有特定修补程序。单击 **Add**（添加），然后输入要检查的特定修补程序的 KB 项 ID。例如，输入 **3128031** 以检查 Microsoft Office 2010 (KB3128031) 32-位版本的更新。
供应商选项卡	可定义要在端点上查找的修补程序管理软件特定供应商和产品，以确定匹配项。单击 **Add**（添加），然后从下拉列表中选择 **Vendor**（供应商）。（可选）单击 Add（添加）以选择特定 **Product**（产品）。单击 **OK**（确定）以保存设置。

HIP 对象防火墙选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Firewall**（防火墙）

选择 **Firewall**（防火墙）选项卡可根据 GlobalProtect 端点的防火墙软件状态启用 HIP 匹配。

HIP 对象防火墙设置
选择 **Firewall**（防火墙）可启用对主机的防火墙软件状态的匹配： • 供应商和产品 — 匹配主机上是否安装了防火墙软件。 • 已启用 — 匹配主机上是否启用了防火墙软件。如果取消选中 **Is Installed**（已安装），则此字段会自动设置为 **None**（无）并且被禁止编辑。 • **Vendor and Product**（供应商和产品）— 定义要在主机上查找的特定防火墙软件供应商和/或产品，以确定匹配项。单击 **Add**（添加），然后从下拉列表中选择 **Vendor**（供应商）。（可选）单击 **Add**（添加）以选择特定 **Product**（产品）。单击 **OK**（确定）以保存设置。 • **Exclude Vendor**（排除供应商）— 选择此选项可匹配不具有指定供应商的软件的主机。

© 2019 Palo Alto Networks, Inc.

HIP 对象反恶意软件选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Anti-Malware**（反恶意软件）

使用 **Anti-Malware**（反恶意软件）选项卡可根据 GlobalProtect 端点的防病毒软件或防间谍软件覆盖范围来启用 HIP 匹配。

HIP 对象反恶意软件设置

选择 **Anti-Malware**（反恶意软件）可根据主机的防病毒软件或防间谍软件覆盖范围来启用匹配。定义匹配项的其他匹配条件，如下所示：

- **Is Installed**（已安装）— 匹配主机上是否安装了防病毒软件或防间谍软件。
- **Real Time Protection**（实时保护）— 匹配主机上是否启用了实时防病毒软件或防间谍软件保护。如果取消选中 **Is Installed**（已安装），则此字段会自动设置为 **None**（无）并且被禁止编辑。
- **Virus Definition Version**（病毒定义版本）— 当病毒定义在指定天数内或发布版本内完成更新时进行匹配。
- **Product Version**（产品版本）— 匹配特定版本的防病毒软件或防间谍软件。要指定版本，请从下拉列表中选择运算符，然后输入表示产品版本的字符串。
- **Last Scan Time**（最后扫描时间）— 指定是否根据防病毒软件或防间谍软件扫描的最后运行时间来进行匹配。从下拉列表中选择运算符，然后指定要匹配的 **Days**（天）数或 **Hours**（小时）数。
- **Vendor and Product**（供应商和产品）— 定义要在主机上查找的特定防病毒软件或防间谍软件供应商和/或产品，以确定匹配项。单击 **Add**（添加），然后从下拉列表中选择 **Vendor**（供应商）。（可选）单击 **Add**（添加）以选择特定 **Product**（产品）。单击 **OK**（确定）以保存设置。
- **Exclude Vendor**（排除供应商）— 选择此选项可匹配不具有指定供应商的软件的主机。

HIP 对象磁盘备份选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Disk Backup**（磁盘备份）

选择**Disk Backup**（磁盘备份）选项卡可根据 GlobalProtect 端点的磁盘备份状态启用 HIP 匹配。

HIP 对象磁盘备份设置

选择 **Disk Backup**（磁盘备份）可启用对主机上的磁盘备份状态的匹配，然后定义匹配项的其他匹配条件，如下所示：

- 已安装 — 匹配主机上是否安装了磁盘备份软件。
- 最后备份时间 — 指定是否根据磁盘备份的最后运行时间来进行匹配。从下拉列表中选择运算符，然后指定要匹配的天或小时数量。
- **Vendor and Product**（供应商和产品）— 定义与主机匹配的特定磁盘备份软件供应商和产品。单击 **Add**（添加），然后从下拉列表中选择 **Vendor**（供应商）。（可选）单击 **Add**（添加）以选择特定 **Product**（产品）。单击 **OK**（确定）以保存设置。
- **Exclude Vendor**（排除供应商）— 选择此选项可匹配不具有指定供应商的软件的主机。

HIP 对象磁盘加密选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Disk Encryption**（磁盘加密）

选择**Disk Encryption**（磁盘加密）选项卡可根据 GlobalProtect 端点的磁盘加密状态启用 HIP 匹配。

© 2019 Palo Alto Networks, Inc.

HIP 对象磁盘加密设置	说明
磁盘加密	选择 **Disk Encryption**（磁盘加密）可启用对主机上磁盘加密状态的匹配。
标准	指定以下设置： • 已安装 — 匹配主机上是否安装了磁盘加密软件。 • 加密位置 — 单击添加可指定在确定匹配项时检查磁盘加密的驱动器或路径： • 加密位置 — 输入用于在主机上检查加密的特定位置。 • 状态 — 指定如何匹配加密位置的状态，方法是从下拉列表中选择运算符，然后选择可能的状态（完全、无、部分或不可用）。 单击 **OK**（确定）以保存设置。
供应商	定义与端点匹配的特定磁盘加密软件供应商和产品。单击 **Add**（添加），然后从下拉列表中选择 **Vendor**（供应商）。（可选）单击 **Add**（添加）以选择特定 **Product**（产品）。单击 **OK**（确定）以保存设置，并返回到 **Disk Encryption**（磁盘加密）选项卡。

HIP 对象数据丢失保护选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Data Loss Prevention**（数据丢失保护）

选择 **Data Loss Prevention**（数据丢失保护）选项卡可配置基于 GlobalProtect 端点是否运行数据丢失保护软件的 HIP 匹配。

HIP 对象数据丢失保护设置
选择 **Data Loss Prevention**（数据丢失保护）可启用对主机上数据丢失防护 (DLP) 状态的匹配（仅限 Windows 主机），然后定义匹配项的其他匹配条件，如下所示： • 供应商和产品 — 匹配主机上是否安装了 DLP 软件。 • **Is Enabled**（已启用）— 匹配主机上是否启用了 DLP 软件。如果取消选中 **Is Installed**（已安装），则此字段会自动设置为 **None**（无）并且被禁止编辑。 • 供应商和产品 — 定义要在主机上查找的特定 DLP 软件供应商和/或产品，以确定匹配项。单击 **Add**（添加），然后从下拉列表中选择 **Vendor**（供应商）。（可选）单击 **Add**（添加）以选择特定 **Product**（产品）。单击 **OK**（确定）以保存设置。 • **Exclude Vendor**（排除供应商）— 选择此选项可匹配不具有指定供应商的软件的主机。

HIP 对象证书选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Certificate**（证书）

选择 **Certificate**（证书）选项卡以根据证书配置文件和其他证书属性启用 HIP 匹配。

HIP 对象证书设置
选择 **Validate Certificate**（验证证书）以根据证书配置文件和其他证书属性启用匹配。然后，定义如下匹配标准：

© 2019 Palo Alto Networks, Inc.

HIP 对象证书设置
• **Certificate Profile**（证书配置文件）— 选择 GlobalProtect 网关将用于验证 HIP 报告中已发送的机器证书的证书配置文件。 • **Certificate Field**（证书字段）— 选择用于匹配机器证书的证书属性。 • **Value**（值）— 设置属性的值。

HIP 对象自定义检查选项卡

- **Objects**（对象）> **GlobalProtect** > **HIP Objects**（**HIP** 对象）> *<hip-object>* > **Custom Checks**（自定义检查）

选择 **Custom Checks**（自定义检查）选项卡可针对您已在 GlobalProtect 门户上定义的任何自定义检查启用 HIP 匹配。有关向 HIP 集合中添加自定义检查的详细信息，请参阅 Network（网络）> GlobalProtect > Portals（门户）。

HIP 对象自定义检查设置	说明
自定义检查	选择 **Custom Checks**（自定义检查）可针对您已在 GlobalProtect 门户上定义的自定义检查启用匹配。
进程列表	要检查某个特定进程的主机系统，请单击添加，然后输入进程名称。默认情况下，应用程序将检查正在运行的进程；如果想查看某个特定进程是否未运行，请取消选中 **Running**（正在运行）选项。进程可以为操作系统级进程或用户空间应用程序进程。
注册表项	要在 Windows 主机中检查某个特定注册表项，请单击 **Add**（添加），然后输入要匹配的 **Registry Key**（注册表项）。要仅匹配缺少指定注册表项或键值的主机，请勾选 **Key does not exist or match the specified value data**（键值不存在或不匹配指定的值数据）框。 要匹配特定值，请单击添加，然后输入注册表值和值数据。要匹配确无指定值或值数据的主机，请选择 **Negate**（求反）。 单击 **OK**（确定）以保存设置。
Plist	要在 Mac 主机中检查属性列表 (plist) 的特定条目，请单击 **Add**（添加），然后输入 **Plist** 名称。要仅匹配无指定 Plist 的主机，请选择 **Plist does not exist**（**Plist** 不存在）。 要匹配 Plist 中的特定键值对，请单击添加，然后输入要匹配的键和对应的值。要匹配确无指定键或值的主机，请选择 **Negate**（求反）。 单击 **OK**（确定）以保存设置。

© 2019 Palo Alto Networks, Inc.

Objects（对象）> GlobalProtect > HIP Profiles（HIP 配置文件）

选择 **Objects**（对象）> **GlobalProtect** > **HIP Profiles**（**HIP** 配置文件）可创建 HIP 配置文件（为监控或实施安全策略要一起评估的 HIP 对象集合），您可使用此文件设置启用 HIP 的安全策略。创建 HIP 配置文件时，可以使用布尔逻辑来合并先前创建的 HIP 对象（以及其他 HIP 配置文件），因而当按照生成的 HIP 配置文件对通信流进行评估时，其结果可能匹配，也可能不匹配。如果存在匹配项，那么将执行对应的策略规则；如果没有匹配项，将按照下一个规则来对通信流进行评估（与任何其他策略匹配标准一样）。

要创建 HIP 配置文件，请单击添加。下表提供了有关在 HIP Profile（HIP 配置文件）对话框上的字段中输入的内容的信息。有关设置 GlobalProtect 以及创建 HIP 扩充安全策略的工作流程的更多详细信息，请参阅《*GlobalProtect* 管理员指南》中的配置基于 HIP 的策略实施。

HIP 配置文件设置	说明
姓名	输入配置文件的名称（最多 **31** 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
说明	（可选）输入说明。
共享	选择 **Shared**（共享）以使当前的 HIP 配置文件可用于： • 防火墙上的所有虚拟系统 (vsys)（如果您登录到处于多虚拟系统模式下的防火墙）。如果取消选中此选项，则此配置文件将仅适用于 **Objects**（对象）选项卡 **Virtual System**（虚拟系统）下拉列表中选定的虚拟系统。对于未处于多虚拟系统模式下的防火墙，此选项将不会出现在 HIP Profile（HIP 配置文件）对话框中。 • Panorama 上的所有设备组。如果取消选中此选项，则此配置文件将仅适用于 **Objects**（对象）选项卡 **Device Group**（设备组）下拉列表中选定的设备组。 在保存配置文件后，您无法更改其共享设置。选择 **Objects**（对象）> **GlobalProtect** > **HIP Profiles**（**HIP** 配置文件）可查看当前 **Location**（位置）。
禁用替代（仅限 Panorama）	控制替代访问设备组中的 HIP 配置文件，这些设备组是在 **Objects**（对象）选项卡中选择的 **Device Group**（设备组）的子对象。如果想要阻止管理员通过替代继承的值在子对象设备组中创建配置文件的本地副本，请选中此选项。默认未选中此选项（即替代已启用）。
匹配	单击添加匹配条件可打开 HIP 对象/配置文件生成器。 选择要用作匹配标准的第一个 HIP 对象或配置文件，然后将其添加 (⊕) 到 HIP Objects/Profiles Builder（HIP 对象/配置文件生成器）对话框上的 **Match**（匹配）文本框。切记，如果您希望仅当对象的标准不适用于流时，HIP 配置文件才将对象评估为匹配项，请在添加对象之前选择 **NOT**（非）。 继续为正在生成的配置文件添加匹配标准，确保在每次添加的标准之间选择相应的布尔运算符（**AND**（与）或 **OR**（或））（如果适用，请再使用 **NOT**（非）运算符）。 要创建复杂的布尔表达式，必须在 **Match**（匹配）文本框中的适当位置手动添加圆括号，以确保使用需要的逻辑对 HIP 配置文件进行求值。例如，以下表达式表示 HIP 配置文件将匹配来自特定主机的流量，此主机使用 FileVault 磁盘加

© 2019 Palo Alto Networks, Inc.

HIP 配置文件设置	说明
	密（Mac OS 系统）或 TrueCrypt 磁盘加密（Windows 系统），同时属于必需的域，并安装了 Symantec 防病毒客户端： `((“MacOS” and “FileVault”) or (“Windows” and “TrueCrypt”)) and “Domain” and “SymantecAV”` 向新 HIP 配置文件添加对象和配置文件后，请单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

Device（设备）> GlobalProtect Client（GlobalProtect 客户端）

以下主题介绍如何设置和管理 GlobalProtect 应用程序。

您在查找什么内容？	请参阅：
查看有关 GlobalProtect 软件版本的更多信息。	管理 GlobalProtect 代理软件
安装 GlobalProtect 软件。	设置 GlobalProtect 代理
使用 GlobalProtect 软件。	使用 GlobalProtect 代理
了解更多？	有关设置 GlobalProtect 软件的详细分步骤说明，请参阅《GlobalProtect 管理员指南》中的部署 GlobalProtect 应用程序软件。

管理 GlobalProtect 应用程序软件

选择 **Device**（设备）> **GlobalProtect Client**（**GlobalProtect** 客户端）（仅限防火墙）可在托管门户的防火墙上下载并激活 GlobalProtect 应用程序软件。之后，连接到门户的端点将下载此应用程序软件。在您在门户上指定的代理配置中，您可定义门户将软件推送到端点的方式和时间。您的配置将决定是否在应用程序连接时自动进行升级，是否提醒最终用户升级，或是否禁止所有或特定用户组进行升级。有关更多详细信息，请参阅允许用户升级 GlobalProtect 应用程序。有关分发 GlobalProtect 应用程序软件的选项的详细信息以及有关部署软件的逐步说明，请参阅《GlobalProtect 管理员指南》中的部署 GlobalProtect 应用程序软件。

对于 *GlobalProtect* 应用程序的初始下载和安装，端点用户必须用管理员权限登录。对于随后的升级，则可以不用管理员权限。

GlobalProtect 客户端设置	说明
版本	此版本号为 Palo Alto Networks 更新服务器上提供的 GlobalProtect 应用程序软件的版本号。如需查看 Palo Alto Networks 是否提供了新的应用程序软件版本，请单击 **Check Now**（立即检查）。防火墙将使用其服务路由连接到更新服务器，以确定是否有新版本可用，如有，则将其显示在列表顶部。
大小	应用程序软件包的大小。
发布日期	Palo Alto Networks 发布新版本的日期和时间。
已下载	此列中的选中标记表示对应版本的应用程序软件包已经下载到防火墙。
当前已激活	此列中的选中标记表示对应版本的应用程序软件包已在防火墙上激活，并且可以通过连接应用程序来下载。一次只能激活软件的一个版本。
操作	表示您可以为对应的应用程序软件包采取的当前操作，如下所示：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 客户端设置	说明
	• **Download**（下载）— Palo Alto Networks 更新服务器上提供的对应的应用程序软件版本。单击 **Download**（下载）可启动下载。如果防火墙无法访问互联网，请使用连接互联网的计算机转至客户支持站点，然后选择**Updates**（更新）> **Software Updates**（软件更新）以查找新的应用程序软件版本，并将其 **Download**（下载）到您的本地计算机。然后，手动 **Upload**（上传）应用程序软件到防火墙。 • **Activate**（激活）— 对应的应用程序软件版本已下载到防火墙，但应用程序尚未将其下载。单击 **Activate**（激活）可激活软件并启用应用程序升级。如需激活手动上传到防火墙的软件更新，请单击 **Activate From File**（从文件激活），然后从下拉列表中选择要激活的版本（可能需要刷新屏幕，以使其显示为 **Currently Activated**（当前已激活））。 • **Reactivate**（重新激活）— 对应的应用程序软件已激活并且可供端点下载。由于一次只能激活 GlobalProtect 应用程序软件的一个版本，如果最终用户需要访问当前激活的版本之外的版本，则必须 **Activate**（激活）其他版本以使其变为 **Currently Active**（当前活动）版本。
发行说明	提供一个链接，指向对应的应用程序版本的 GlobalProtect 发行说明。
☒	从防火墙中删除先前下载的应用程序软件映像。

设置 GlobalProtect 应用程序

GlobalProtect 应用程序是一款安装在端点（通常为便携式计算机）上的应用程序，用于支持与门户和网关的 GlobalProtect 连接。该应用程序由 GlobalProtect 服务 (PanGP Service) 提供支持。

确保为主机操作系统（*32* 位或 *64* 位）选择正确的安装选项。如果在 *64* 位主机上进行安装，请使用 *64* 位浏览器和 *Java* 组合进行初始安装。

要安装应用程序，请打开安装程序文件，并按照屏幕上的说明操作。

使用 GlobalProtect 应用程序

GlobalProtect Settings（**GlobalProtect** 设置）面板在您启动 GlobalProtect 应用程序并从 GlobalProtect 状态面板的 **Settings**（设置）菜单中选择 **Settings**（设置）时会打开，其中的选项卡包含有关状态和设置的有用信息，并提供有助于解决连接问题的信息。

- 常规选项卡 — 显示与 GlobalProtect 帐户关联的用户名和门户。您还可以从此选项卡添加、删除或修改门户。
- **Connection tab**（连接选项卡）— 显示为 GlobalProtect 应用程序配置的网关，并提供有关每个网关的以下信息：
  - 网关名称
  - 隧道状态
  - 身份验证状态
  - 连接类型
  - 网关 IP 地址或 FQDN（仅在外部模式下可用）

对于内部模式，*Connection*（连接）选项卡显示可用网关的完整列表。对于外部模式，*Connection*（连接）选项卡显示所连接的网关以及与其有关的其他详细信息（例如，网关 *IP* 地址和正常运行时间）。

© 2019 Palo Alto Networks, Inc.

- **Host Profile tab**（主机配置文件选项卡）— 显示 GlobalProtect 用于通过主机信息配置文件 (HIP) 监控和执行安全策略的端点数据。单击 **Resubmit Host Profile**（重新提交主机配置文件）以手动将 HIP 数据重新提交到网关。
- **Troubleshooting tab**（故障排除选项卡）— 在 macOS 端点上，此选项卡允许您 **Collect Logs**（收集日志）并设置 **Logging Level**（日志记录级别）。在 Windows 端点上，此选项卡允许您 **Collect Logs**（收集日志）、设置 **Logging Level**（日志记录级别）并查看有助于排除故障的以下信息：
  - **Network Configurations**（网络配置）— 显示当前系统配置。
  - 路由表 — 显示有关当前如何路由 GlobalProtect 连接的信息。
  - 套接字 — 显示当前活动连接的套接字信息。
  - **Logs**（日志）— 允许用户显示 GlobalProtect 应用程序和服务的日志。选择日志类型和调试级别。单击开始开始记录，单击停止终止记录。
- **Notification tab**（通知选项卡）— 显示在 GlobalProtect 应用程序上触发的通知列表。要查看有关特定通知的更多详细信息，请双击相应的通知。

Panorama Web 界面

Panorama™ 是 Palo Alto Networks® 系列新一代防火墙的集中式管理系统。Panorama 提供了一个独特的位置，您可在其中监管您的网络上的所有应用程序、用户和内容，然后使用收集的信息创建控制和保护网络的策略。使用 Panorama 对策略和防火墙进行集中管理，可提高管理分布式防火墙网络的运营效率。Panorama 可用作专用硬件（M 系列）设备和 VMware 虚拟设备（在 ESXi 服务器或 vCloud Air 平台上运行）。

虽然许多 Panorama Web 界面视图和设置与您看到的防火墙 Web 界面视图和设置相同，但以下主题将介绍 Panorama Web 界面所独有的 Panorama、防火墙和日志收集器管理选项。

> 使用 Panorama Web 界面
> 上下文切换
> Panorama 提交操作
> 在 Panorama 上定义策略
> 传统模式下 Panorama 虚拟设备的日志存储分区
> Panorama > Setup（设置）> Interfaces（接口）
> Panorama > High Availability（高可用性）
> Panorama > Managed WildFire Clusters（受管 Wildfire 集群）
> Panorama > Administrators（管理员）
> Panorama > Admin Roles（管理员角色）
> Panorama > Access Domains（访问域）
> Panorama > Managed Devices（受管设备）> Summary（摘要）
> Panorama > Managed Devices（受管设备）> Health（运行状况）
> Panorama > Templates（模板）
> Panorama > Device Groups（设备组）
> Panorama > Managed Collectors（受管收集器）
> Panorama > Collector Groups（收集器组）
> Panorama > Plugins（插件）
> Panorama > SD-WAN
> Panorama > VMware NSX
> Panorama > Log Ingestion Profile（日志提取配置文件）
> Panorama > Log Settings（日志设置）
> Panorama > Server Profiles（服务器配置文件）> SCP
> Panorama > Scheduled Config Export（计划配置导出）
> Panorama > Software（软件）
> Panorama > Device Deployment（设备部署）

了解更多？

有关设置和使用 Panorama 进行集中管理的详细信息，请参阅《Panorama 管理员指南》。

使用 Panorama Web 界面

Panorama 和防火墙的 Web 界面具有相同的外观和操作体验。但 Panorama Web 界面设有可用于管理 Panorama、使用 Panorama 管理防火墙和日志收集器的其他选项和 Panorama 特定的选项卡。

以下共用字段出现在数个 Panorama Web 界面页面的页眉或页脚中。

共用字段	说明
环境	您可使用左侧菜单上方的 **Context**（上下文）下拉列表在 Panorama Web 界面和防火墙 Web 界面间进行切换（参阅上下文切换）。
↻	在 **Dashboard**（仪表盘）和 **Monitor**（监控）选项卡中，单击选项卡标头中的刷新 (↻) 以手动刷新这些选项卡中的数据。您也可使用选项卡标头右侧上无标签的下拉列表来选择以分钟为单位的自动刷新间隔（**1 min**（**1** 分钟）、**2 mins**（**2** 分钟）或 **5 mins**（**5** 分钟））；要禁用自动刷新，请选择 **Manual**（手动）。
访问域	访问域定义特定设备组、模板和各个防火墙的访问权限（通过 **Context**（上下文）下拉列表）。如果您作为具有多个访问域分配在自己帐户中的管理员登录，**Dashboard**（仪表盘）、**ACC** 以及 **Monitor**（监控）选项卡仅对您在 Web 界面的页脚中选择的 **Access Domain**（访问域）显示信息（例如日志数据）。 如果仅有一个访问域分配至您的帐户，*Web* 界面不会显示 *Access Domain*（访问域）下拉列表。
设备组	设备组包括您作为一个组管理的防火墙和虚拟系统（参阅 Panorama > Device Groups（设备组））。**Dashboard**（仪表盘）、**ACC** 和 **Monitor**（监控）选项卡仅对您在选项卡标头中选择的 **Device Group**（设备组）显示信息（例如日志数据）。在 **Policies**（策略）和 **Objects**（对象）选项卡中，可为特定 **Device Group**（设备组）或所有设备组（选择 **Shared**（共享））配置设置。
模板	模板是具有共用网络和设备设置的一组防火墙，而模板堆栈是模板的组合（参阅 Panorama > Templates（模板））。在 **Network**（网络）和 **Device**（设备）选项卡中，配置特定 **Template**（模板）或模板堆栈的设置。由于您只能在各个模板中编辑设置，如果您选择模板堆栈，这些选项卡中的设置为只读。
查看依据:设备 模式	默认情况下，**Network**（网络）和 **Device**（设备）选项卡显示可用于使用正常操作模式并支持多个虚拟系统和 VPN 的防火墙的设置和值。但是您可使用以下选项来过滤选项卡，以仅显示您要编辑的模式特定的设置： • 在 **Mode**（模式）下拉列表中，选择或清除 **Multi VSYS**（多虚拟系统）、**Operational Mode**（操作模式）和 **VPN Mode**（**VPN** 模式）选项。 • 通过在**View by**：（查看依据）中选择特定防火墙，将所有模式选项设置为显示该防火墙的模式配置**Device**（设备）下拉列表。

Panorama 选项卡提供以下用于管理 Panorama 和日志收集器的页面。

© 2019 Palo Alto Networks, Inc.

Panorama 页面	说明
设置	为以下任务选择 **Panorama** > **Setup**（设置）： • 指定数个设置（例如 Panorama 主机名）以及用于身份验证、日志报告、AutoFocus™、横幅、每日消息和密码复杂度的设置。这些设置和您为防火墙配置的设置相似：选择 Device（设备）> Setup（设置）> Management（管理）。 • 备份并还原配置，重新启动 Panorama，然后关闭 Panorama。这些操作和您为防火墙执行的设置相似：选择 Device（设备）> Setup（设置）> Operations（操作）。 • 定义 DNS、NTP 和 Palo Alto Networks 更新的服务器连接。这些设置和您为防火墙配置的设置相似：选择 Device（设备）> Setup（设置）> Services（服务）。 • 定义 Panorama 接口的网络设置。选择 Panorama > Setup（设置）> Interfaces（接口）。 • 指定 WildFire™ 设备的设置。这些设置和您为防火墙配置的设置相似：选择 Device（设备）> Setup（设置）> WildFire。 • 管理硬件安全模块 (HSM) 设置。这些设置和您为防火墙配置的设置相似：选择 Device（设备）> Setup（设置）> HSM。
高可用性	让您能为一对 Panorama 管理服务器配置高可用性 (HA)。选择 Panorama > 高可用性。
配置审核	让您能查看配置文件之间的差异。选择 Device（设备）> Config Audit（配置审核）。
密码配置文件	让您能为 Panorama 管理员定义密码配置文件。选择 Device（设备）> Password Profiles（密码配置文件）。
管理员	让您能配置 Panorama 管理员帐户。选择 Panorama > Administrators（管理员）。 如果管理员帐户被锁定，*Administrators*（管理员）页面将在 *Locked User*（已锁定用户）列中显示一个锁。您可以单击此锁来解锁帐户。
管理角色	让您能定义管理角色，这些角色控制访问 Panorama 的管理员的权限和职责。选择 Panorama > Admin Roles（管理员角色）。
访问域	让您能控制管理员访问设备组、模板、模板堆栈和防火墙的 Web 界面。选择 Panorama > Access Domains（访问域）。
身份验证配置文件	让您能针对 Panorama 的身份验证访问指定配置文件。选择 Device（设备）> Authentication Profile（身份验证配置文件）。
身份验证序列	让您能指定用于授权访问 Panorama 的一系列身份验证配置文件。选择 Device（设备）> Authentication Sequence（身份验证序列）。
用户标识	使您能够配置自定义证书配置文件，以使用 User-ID 代理执行相互身份验证。选择 Device（设备）> User Identification（用户标识）> Connection Security（连接安全性）。

© 2019 Palo Alto Networks, Inc.

Panorama 页面	说明
数据重新分发	使您能够选择性地重新分发数据到其他防火墙或 Panorama 管理系统。选择 Devices（设备）> Data Redistribution（数据重新分发）。
受管设备	让您能管理防火墙，包括添加防火墙到 Panorama 作为受管设备、显示防火墙连接和许可证状态、标记防火墙、更新防火墙软件和内容，以及加载配置备份。选择 Panorama > Managed Devices（受管设备）> Summary（摘要）。
模板	让您能在 **Device**（设备）和 **Network**（网络）选项卡中管理配置选项。模板和模板堆栈可让您在部署具有相同或相似配置的多个防火墙时减少管理员的工作量。选择 Panorama > Templates（模板）。
设备组	让您能配置设备组，以便根据功能、网络分段或地理位置对防火墙进行分组。设备组可以包括物理防火墙、虚拟防火墙和虚拟系统。 通常，一个设备组中的防火墙需要类似的策略配置。通过 Panorama 上的“策略和对象”选项卡，设备组提供了一种方式，可用来实现管理整个受管防火墙网络的策略的分层方法。可以在最多四个级别的树形层次结构中嵌套设备组。后代组自动继承祖先组和共享位置的策略和对象。选择 Panorama > Device Groups（设备组）。
受管收集器	让您能管理日志收集器。由于您使用 Panorama 配置日志收集器，因此这些设备也称为托管收集器。托管收集器可位于 Panorama 管理服务器（M-Series 设备或 Panorama 模式下的 Panorama 虚拟设备）或专用日志收集器（日志收集器模式下的 M-Series 设备）的本地。选择 Panorama > Managed Collectors（受管收集器）。 您也可安装专用日志收集器的软件更新。 您可以将 Panorama 管理服务器转换为专用日志收集器。
收集器组	让您能管理收集器组。收集器组最多可通过逻辑分组方式对日志收集器进行分组，以便您可应用相同的配置设置并对其分配防火墙。Panorama 将日志均匀地分布在日志收集器的所有磁盘以及收集器组的所有成员中。选择 Panorama > Collector Groups（收集器组）。
插件	让您能为第三方集成（例如 VMware NSX）管理插件。选择 Panorama > VMware NSX。
VMware NSX	让您能将 VM-Series 防火墙的配置自动化，方法是启用 NSX Manager 和 Panorama 之间的通信。选择 Panorama > VMware NSX。
证书管理	让您能配置并管理证书、证书配置文件和密钥。选择 Manage Firewall and Panorama Certificates（管理防火墙和 Panorama 证书）。
日志设置	让您能将日志转发至简单网络管理协议 (SNMP) 的陷阱接收器、Syslog 服务器、电子邮件服务器和 HTTP 服务器。选择 Device（设备）> Log Settings（日志设置）。
服务器配置文件	让您能针对不同向 Panorama 提供服务的服务器类型配置配置文件：选择以下任一项来配置特定服务器类型： • Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件） • Device（设备）> Server Profiles（服务器配置文件）> HTTP

© 2019 Palo Alto Networks, Inc.

Panorama 页面	说明
	• Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱） • Device（设备）> Server Profiles（服务器配置文件）> Syslog • Device（设备）> Server Profiles（服务器配置文件）> RADIUS • Device（设备）> Server Profiles（服务器配置文件）> TACACS+ • Device（设备）> Server Profiles（服务器配置文件）> LDAP • Device（设备）> Server Profiles（服务器配置文件）> Kerberos • Device（设备）> Server Profiles（服务器配置文件）> SAML Identity Provider（SAML 标识提供商）
已计划的配置导出	让您能每天将 Panorama 和防火墙配置导出至 FTP 服务器或 Secure Copy（安全复制-SCP）服务器。选择 Panorama > Scheduled Config Export（调度的配置导出）。
软件	让您能更新 Panorama 软件。选择 Panorama > Software（软件）。
动态更新	让您能查看有关新安全威胁的最新应用程序定义和信息，比如防病毒签名（需要威胁防御许可证）等，然后使用这些新定义来更新 Panorama。选择 Device（设备）> Dynamic Updates（动态更新）。
支持	让您能访问 Palo Alto Networks 提供的产品和安全警报。选择 Device（设备）> Support（支持）。
设备部署	让您能向防火墙和日志收集器部署软件和内容更新。选择 Panorama > Device Deployment（设备部署）。
主密钥和诊断	让您能指定主密钥，以在 Panorama 上加密私钥。默认情况下，如果您没有指定新的主密钥，Panorama 以加密形式存储私钥。选择 Device（设备）> Master Key and Diagnostics（主密钥和诊断）。

© 2019 Palo Alto Networks, Inc.

上下文切换

在每个 Panorama Web 界面页面的标题中，您可使用左侧菜单上方的 **Context**（上下文）下拉列表在 Panorama Web 界面和防火墙 Web 界面之间进行切换。选择防火墙后，Web 界面将更新以显示所选防火墙的所有页面和选项，以便您对其进行本地管理。下拉列表仅显示您拥有管理访问权限（请参阅 Panorama > Access Domains（访问域））且已连接至 Panorama 的防火墙。

您可以使用过滤器按平台（型号）、设备组、模板、标记或高可用性状态搜索防火墙。此外，还可以在过滤器栏中输入文本字符串，按设备名称进行搜索。

高可用性 (HA) 模式下的防火墙的图标的背景为彩色，以表示其高可用性状态。

© 2019 Palo Alto Networks, Inc.

Panorama 提交操作

单击 Web 界面右上角的 **Commit**（提交），然后为暂挂的 Panorama 配置更改和 Panorama 推送到防火墙、日志收集器以及 WildFire 集群和设备的更改选择操作：

- **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）— 激活在 Panorama 管理服务器配置中所作的更改。此操作还会将设备组、模板、收集器组以及 WildFire 集群和设备的更改提交到 Panorama 配置，但不会将这些更改推送到防火墙、日志收集器或 WildFire 集群和设备。提交到 Panorama 配置，可让您保存防火墙、日志收集器或 WildFire 集群和设备中未准备激活的更改。

  将配置推送到受管设备后，*Panorama 8.0* 和更高版本会推送正在运行的配置，即已提交到 *Panorama* 的配置。*Panorama 7.1* 和之前的版本会推送待选配置，包括未提交的更改。因此，使用 *Panorama 8.0* 和更高版本时，在先将更改提交到 *Panorama* 之前，不能将更改推送到受管设备。
- **Commit**（提交）> **Push to Devices**（推送到设备）— 将 Panorama 正在运行的配置推送到设备组、模板、收集器组以及 WildFire 集群和设备。
- **Commit**（提交）> **Commit and Push**（提交并推送）— 将所有配置更改提交到本地 Panorama 配置，然后将 Panorama 正在运行的配置推送到设备组、模板、收集器组以及 WildFire 集群和设备。

您可以按管理员或位置过滤暂挂更改，然后仅提交、推送、验证、或预览这些更改。位置可以是特定设备组、模板、收集器组、日志收集器、WildFire 设备和集群、共享设置或 Panorama 管理服务器。

在提交更改后，这些更改成为正在运行的配置的一部分。未提交的更改是待选配置的一部分。Panorama 会将提交请求整理成队列，以便您可在之前的提交操作处于进行状态时，启动新的提交操作。Panorama 按提交启动顺序执行提交，但会优先执行 Panorama 启动的自动提交（如 FQDN 刷新）。但是，如果队列中管理员启动的提交已达到最大数量，则必须等待 Panorama 完成暂挂提交的处理后，才能启动新提交。您可使用任务管理器（Tasks）来清除提交队列，或查看有关提交操作的详细信息。如需了解有关配置更改、提交流程、提交验证和提交队列的详细信息，请参阅《Panorama 提交和验证操作》。您还可以保存待选配置，恢复更改，以及导入、导出或加载配置（Device（设备）> Setup（设置）> Operations（操作））。

以下选项可用于提交、验证或预览配置更改。

字段/按钮	说明
选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）或 **Commit**（提交）> **Commit and Push**（提交并推送）将更改提交到 Panorama 时，需应用以下选项。	
提交所有更改	提交您具有管理权限的所有更改（默认）。在选中此选项后，不能手动过滤 Panorama 提交的配置更改的范围。而是分配给您用于登录的帐户的管理员角色确定了提交范围： • 超级用户角色 — Panorama 可提交所有管理员的更改。 • 自定义角色 — 为您的帐户分配的管理员角色配置文件的权限可确定提交范围（请参阅 Panorama > Admin Roles（管理员角色））。如果配置文件包含 **Commit For Other Admins**（为其他管理员提交）这一权限，则 Panorama 可提交所有管理员配置的更改。如果管理员角色配置文件不包含 **Commit For Other Admins**（为其他管理员提交）这一权限，则 Panorama 只能提交您的更改，不能提交其他管理员的更改。 如果您已应用访问域，Panorama 会自动应用这些域过滤提交范围（请参阅 Panorama > Access Domains（访问域））。不管是何管理角色，Panorama 都仅提交为您的帐户分配的访问域中的配置更改。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
提交更改者	过滤 Panorama 提交的配置更改的范围。分配给您用于登录的帐户的管理角色确定了过滤选项： • **Superuser role**（超级用户角色）— 您可以将提交范围限制为特定管理员所作的更改以及在特定位置所作的更改。 • 自定义角色 — 为您的帐户分配的管理员角色配置文件的权限可确定过滤选项（请参阅 Panorama > Admin Roles（管理员角色））。如果管理员角色配置文件包括 **Commit For Other Admins**（为其他管理员提交）权限，则您可以将提交范围限制为特定管理员配置的更改以及在特定位置所作的更改。如果管理员角色配置文件不包括 **Commit For Other Admins**（为其他管理员提交）权限，则您只能将提交范围限制为在特定位置所作的更改。 过滤提交范围如下： • **Filter by administrator**（按管理员过滤）— 即使您的角色允许提交其他管理员的更改，默认情况下提交范围仅包括您的更改。要将其他管理员添加到提交范围，请单击 *<usernames>* 链接，选择管理员，然后单击 **OK**（确定）。 • **Filter by location**（按位置过滤）— 选择要包括在提交中的更改的特定位置。 如果您已应用访问域，Panorama 会根据这些域自动过滤提交范围（请参阅 Panorama > Access Domains（访问域））。无论您的管理角色和过滤选择怎样，提交范围仅包括分配给帐户的访问域中的配置更改。 加载配置后（Device（设备）> Setup（设置）> Operations（操作））， *必须 Commit All Changes*（提交所有更改）。 在将更改提交到特定设备组后，必须在此设备组中加入添加、删除或重新定位相同规则库规则的所有管理员的更改。
提交范围	列出拥有要提交的更改的位置。列表是否包括所有更改或部分更改取决于多个因素，如提交所有更改和提交更改者所述。这些位置可以是以下任何之一： • **shared-object**（共享对象）— 在共享位置中定义的设置。 • *<device-group>* — 定义策略规则或对象所在的设备组的名称。 • *<template>* — 定义设置所在的模板或模板堆栈的名称。 • *<log-collector-group>* — 定义设置所在的收集器组的名称。 • *<log-collector>* — 定义设置所在的日志收集器的名称。 • *<wildfire-appliances>* — 定义设置所在的 WildFire 设备的序列号。 • *<wildfire-appliance-clusters>* — 定义设置所在的 WildFire 集群的名称。
位置类型	此列用于对暂挂更改的位置进行分类： • **Panorama** — 特定于 Panorama 管理服务器配置的设置。 • **Device Group**（设备组）— 在特定设备组中定义的设置。 • **Template**（模板）— 在特定模板或模板堆栈中定义的设置。 • **Log Collector Group**（日志收集器组）— 特定于收集器组配置的设置。 • **Log Collector**（日志收集器）— 特定于日志收集器配置的设置。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	• **WildFire Appliance Clusters**（**WildFire** 设备集群）— 特定于 WildFire 设备集群配置的设置。 • **WildFire Appliances**（**WildFire** 设备）— 特定于 WildFire 设备的设置。 • **Other Changes**（其他更改）— 不是特定于上述任何配置区域（如共享对象）的设置。
包括中提交中 （仅限部分提交）	能让您选择要提交的更改。默认情况下，选择 **Commit Scope**（提交范围）内的所有更改。此列仅在您选择 **Commit Changes Made By**（提交更改者）特定管理员后才会显示。 可能存在影响包括在提交中的更改的依赖关系。例如，如果您添加一个对象且其他管理员然后编辑该对象，则您无法提交其他管理员的更改，也不会提交自己的更改。
按类型分组	按 **Location Type**（位置类型）对 **Commit Scope**（提交范围）中的配置更改列表进行分组。
预览变更	能让您将在 **Commit Scope**（提交范围）中选择的配置与正在运行的配置进行比较。预览窗口使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。 为了帮助您将更改与 Web 界面的各部分进行匹配，您可以配置预览窗口以显示每次更改之前和之后的 **Lines of Context**（上下文行）。这些行是您进行比较的待选配置和正在运行配置的文件中的行。 由于预览结果会在新浏览器窗口中显示，所以您的浏览器必须设置允许窗口弹出。如果预览窗口未打开，请参阅浏览器文档，了解允许窗口弹出的相关步骤。
更改摘要	列出您用于提交更改的各个设置。**Change Summary**（更改摘要）列表显示各个设置的以下信息： • **Object Name**（对象名称）— 用于标识策略、对象、网络设置或设备设置的名称。 • **Type**（类型）— 设置的类型（如地址、安全规则或区域）。 • **Location Type**（位置类型）— 指示设置是在 **Device Groups**（设备组）中、**Templates**（模板）中、**Collector Groups**（收集器组）中、**WildFire Appliances**（**WildFire** 设备）中还是在 **Wildfire Appliance Clusters**（**WildFire** 设备集群）中定义的。 • **Location**（位置）— 定义设置所在的设备组、模板、收集器组、WildFire 集群或 WildFire 设备的名称。此列将对未在这些位置定义的设置显示 **Shared**（共享）。 • **Operations**（操作）— 指示自上次提交以来对设置执行的每个操作（创建、编辑或删除）。 • **Owner**（所有者）— 对设置进行最后更改的管理员。 • **Will Be Committed**（即将提交）— 指示提交项中是否会包含此设置。 • **Previous Owners**（以前的所有者）— 在最后更改之前对设置进行更改的管理员。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	（可选）可以选择 **Group By**（分组方式）列名称进行分组（如 **Type**（类型））。
验证提交	验证 Panorama 配置的语法是否正确，语义是否完整。输出包括与提交显示相同的错误和警告，其中包括规则阴影和应用程序相关性警告。验证过程能让您在提交之前查找和修复错误（不会对正在运行的配置进行任何更改）。如果您拥有固定提交窗口，并且希望确保提交将成功而没有出现错误，这将非常有用。
在选择 **Commit**（提交）> **Push to Devices**（推送到设备）或 **Commit**（提交）> **Commit and Push**（提交并推送），将配置更改推送到受管设备时，需应用以下选项。	
推送范围	列出要推送更改的位置。默认情况下，范围所包含的位置取决于您在以下选项中选择的选项： • **Commit**（提交）> **Commit and Push**（提交并推送）— 范围包含需要执行 Panorama 提交的更改的所有位置。 • **Commit**（提交）> **Push to Devices**（推送到设备）— 范围包含与 Panorama 运行配置不同步（有关同步状态，请参阅 Panorama > Managed Devices（受管设备）> Summary（摘要）和 Panorama > Managed Collectors（受管收集器））的实体（防火墙、虚拟系统、日志收集器、WildFire 集群、WildFire 设备）关联的所有位置。 对于这两种选择，Panorama 都可以按以下选项过滤推送范围： • **Administrators**（管理员）— Panorama 所应用的过滤器与提交范围的过滤器相同（请参阅提交所有更改或所作更改提交依据）。 • **Access domains**（访问域）— 如果您已应用访问域，Panorama 会根据这些域自动过滤提交范围（请参阅 Panorama > Access Domains（访问域））。不管是何管理角色和过滤选择，范围都仅包含为您的帐户分配的访问域中的配置更改。 您需要为推送范围编辑选择，而不是接受默认位置。
位置类型	此列用于对暂挂更改的位置进行分类： • **Device Groups**（设备组）— 在特定设备组中定义的设置。 • **Templates**（模板）— 在特定模板或模板堆栈中定义的设置。 • **Log Collector Groups**（日志收集器组）— 特定于收集器组配置的设置。 • **WildFire Clusters**（**WildFire** 集群）— 特定于 WildFire 集群配置的设置。 • **WildFire Appliances**（**WildFire** 设备）— 特定于 WildFire 设备配置的设置。
实体	对于每个设备组或模板，此列将列出推送操作中所包含的防火墙（按设备名称或序列号）或虚拟系统（按名称）。 如果将更改推送到特定收集器组，则推送操作将包含此收集器组中的所有日志收集器，即使没有列出也是如此。
编辑选择	单击此选项可选择要包含在推送操作中的实体： • 设备组和模板

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
	• 日志收集器组 • WildFire 设备和集群 *Panorama* 不会让您推送尚未提交到 *Panorama* 配置的更改。
设备组和模板	选择 **Edit Selections**（编辑选择），然后选择 **Device Groups**（设备组）或 **Templates**（模板），可将这些选项显示在后面的行中。
过滤器	筛选模板列表、模板堆栈，或设备组及相关联的防火墙和虚拟系统。 您还可以根据受管防火墙的提交状态、设备状态、标记和高可用性(HA)状态对其进行筛选。
名称	选择要包含在推送操作中的模板、模板堆栈、设备组、防火墙或虚拟系统。
最后提交状态	指示防火墙和虚拟系统配置是否已与 Panorama 中的模板或设备组配置同步。
HA 状态	表明所列防火墙的高可用性状态： • **Active**（主动）— 正常的流量处理操作状态。 • **Passive**（被动）— 正常备份状态。 • **Initiating**（正在启动）— 防火墙将在重启后处于此状态，且时长不超过 60 秒。 • **Non-functional**（无功能）— 错误状态。 • **Suspended**（挂起）— 管理员已禁用此防火墙。 • **Tentative**（试验）— 适用于主动/主动配置中的链接或路径监控事件。
提交暂挂的更改 (Panorama)	指示在将更改推送到所选防火墙和虚拟系统之前是需要（`yes`（是））执行 Panorama 提交还是不需要（`no`（否））执行 Panorama 提交。
预览更改列	选择 **Preview Changes**（预览更改），可比较在 **Push Scope**（推送范围）中选择的配置和 Panorama 正在运行的配置。Panorama 会过滤输出，仅显示您在 **Device Groups**（设备组）或 **Templates**（模板）选项卡中选择的防火墙和虚拟系统的结果。预览窗口使用颜色编码表示添加（绿色）、修改（黄色）或删除（红色）的更改。 由于预览结果会在新浏览器窗口中显示，所以您的浏览器必须设置允许窗口弹出。如果预览窗口未打开，请参阅浏览器文档，了解允许窗口弹出的相关步骤。
全选	选中列表中的所有条目。
取消全选	取消选中列表中的所有条目。
全部展开	显示分配给模板、模板堆栈或设备组的防火墙和虚拟系统。
全部折叠	仅显示模板、模板堆栈或设备组，而不显示防火墙或分配到防火墙的虚拟系统。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
分组 HA 对端	对高可用性 (HA) 配置的对端防火墙分组。分组结果列表会首先显示主动防火墙（或主动/主动配置的主动-主要防火墙），然后在括号中显示被动防火墙（或主动/主动配置的主动-辅助防火墙）。这可让您轻松确定处于高可用性模式下的防火墙。推送共享策略时，可以推送到分组的对，而不是单个对端。 对于主动/被动配置中的高可用性 *(HA)* 对端，应考虑将各防火墙或其虚拟系统均添加到相同的设备组、模板或模板堆栈，以便同时向各对端推送配置。
验证	单击此选项可验证要推送到所选防火墙和虚拟系统的配置。任务管理器会自动打开，以显示验证状态。
过滤器已选择	如果您想要列表仅显示特定防火墙或虚拟系统，请选择这些对象，然后选择 **Filter Selected**（过滤所选项）。
与待选配置合并	（默认情况下已选中）合并从 Panorama 推送的配置更改和管理员在目标防火墙本地执行的所有暂挂配置更改。推送操作会触发 PAN-OS® 提交合并的更改。如果取消选中此选项，则提交项不包含防火墙上的待选配置。 如果允许防火墙管理员在防火墙本地提交更改，请取消选中此选项，这样，在提交 *Panorama* 中的更改时就无需包含此类本地更改。 另一种最佳做法是：在防火墙上执行配置审核，以检查所有本地更改，然后推送 Panorama 中的更改（请参阅 Device（设备）> Config Audit（配置审核））。
包括设备和网络模板 （仅限设备组选项卡）	（默认情况下已选中）一次性将设备组更改和关联的模板更改推送到所选防火墙和虚拟系统。要通过不同的操作推送这些更改，请取消选中此选项。
强制模板值	（默认情况下已禁用）替代所有本地配置设置，删除模板或模板堆栈中没有的，或本地配置中已替代的所选防火墙上的所有对象。推送操作会恢复防火墙上的所有现有配置，并确保防火墙仅继承模板或模板堆栈中定义的设置。 如果在启用 *Force Template Values*（强制模板值）的情况下推送配置，则防火墙上的所有替代值将替换为模板中的值。在使用此选项之前，检查防火墙上的替代值，确保您的提交不会导致任何意外的网络中断，或是因替换这些替代值而产生问题。
日志收集器组	选择 **Edit Selections**（编辑选择），然后选择 **Log Collector Groups**（日志收集器组），可将此对象包含在推送操作中。此选项卡将显示以下选项： • **Select All**（全选）— 选中列表中的每个收集器组。 • **Deselect All**（取消全选）— 取消选中列表中的每个收集器组。
WildFire 设备和集群	选择 **Edit Selections**（编辑选择），然后选择 **WildFire Appliances and Clusters**（**WildFire** 设备和集群），可显示以下选项。

© 2019 Palo Alto Networks, Inc.

字段/按钮	说明
过滤器	过滤 WildFire 设备和集群列表。
名称	选择 Panorama 将更改推送到的 WildFire 设备和集群。
最后提交状态	指示 WildFire 设备和集群配置是否与 Panorama 同步。
移除选择	移除推送范围中列出的所有防火墙。
验证设备组推送	在推送范围列表中验证要推送到设备组的配置。任务管理器会自动打开，以显示验证状态。
验证模板推送	在推送范围列表中验证要推送到模板的配置。任务管理器会自动打开，以显示验证状态。
按位置类型分组	选中此选项可使用位置类型对推送范围列表分组。
在向设备提交 Panorama 配置或推送更改时，需应用以下选项。	
说明	输入说明（最多 512 个字符），以帮助其他管理员了解您所作的更改。 提交事件的系统日志将截断长度超过 *512* 个字符的说明。
提交/推送/提交并推送	启动提交，或在其他提交处于暂挂状态时，将提交请求添加到提交队列中。

© 2019 Palo Alto Networks, Inc.

在 Panorama 上定义策略

Panorama™ 上的设备组可让您集中管理防火墙策略。在 Panorama 上创建策略作为预处理规则或后处理规则；预处理规则和后处理规则可让您在实施策略时创建分层的方法。

可以在共享上下文中定义预处理规则和后处理规则作为适用于所有受管防火墙的共享策略，或在设备组上下文中使其特定于某个设备组。由于已在 Panorama 上定义预处理规则和后处理规则，然后将它们从 Panorama 推送到受管防火墙，因此您可以查看受管防火墙上的规则，但只能编辑 Panorama 中的预处理规则和后处理规则。

- 预处理规则 — 在进行评估前添加到规则序列顶部的规则。您可以使用预处理规则来强制执行组织的可接受使用策略。例如，您可以阻止所有用户访问特定 URL 类别，或者允许所有用户访问 DNS 流量。
- **Post Rules**（后处理规则）— 在使用预处理规则进行评估后添加到规则序列底部且在防火墙本地进行定义的规则。后继规则通常包括根据 App-ID™、User-ID™ 或服务而拒绝访问流量的规则。
- **Default Rules**（默认规则）— 指定防火墙如何处理与任何预处理、后处理规则或本地防火墙规则不匹配流量的规则。这些规则是 Panorama 的预定义配置的一部分。要 **Override**（替代）并编辑在这些规则中选择的设置，请参阅替代或恢复安全策略规则。

使用 **Preview Rules**（预览规则）可查看在将规则推送到受管防火墙之前的所有规则列表。在每个规则库内，每个设备组（和受管防火墙）的规则级联可在视觉上进行划定，从而使得更容易通过大量规则进行扫描。

添加新规则时，将显示规则的静态运行数据。通用唯一标识符(UUID)列显示规则的 UUID （36 个字符）。防火墙基于每个规则生成 UUID。但是，如果从 Panorama 推送规则，这些规则具有相同的 UUID，也会显示在组合规则预览中。**Created**（已创建）列显示规则添加到规则库的时间和日期。此外，**Modified**（已修改）列显示最后一次编辑规则的时间和日期。如果在更新至 PAN-OS 9.0 之前已创建策略规则，则 **First Hit**（第一次命中）数据将用于确定 **Created**（已创建）日期。如果规则没有可用的 **First Hit**（第一次命中）数据，则防火墙或 Panorama 管理服务器更新到 PAN-OS 9.0 的时间和日期将用于确定 **Created**（已创建）日期。

在 Panorama 中添加或编辑规则时，将显示 **Target**（目标）选项卡。可以使用此选项卡将规则应用于定义规则的 **Device Group**（设备组）（或共享位置）的特定防火墙或子设备组。在 **Target**（目标）选项卡中，您可以选择 **Any**（任何）（默认），这意味着规则适用于所有防火墙和子设备组。要定位特定防火墙或设备组，请取消选择 **Any**（任何），然后按名称选择特定防火墙或设备组。要排除特定防火墙或设备组，请取消选择 **Any**（任何），然后按名称选择特定防火墙或设备组，再选择 **Target to all but these specified devices**（定位到除这些指定设备以外的所有设备）。如果设备组和防火墙的列表很长，可以应用过滤器以按属性（如平台）或文本字符串搜索与名称相匹配的条目。

在 Panorama 中成功添加并推送规则后，**Rule Usage**（规则使用情况）将显示规则是被设备组中的所有设备使用、被设备组中的部分设备部分使用还是未被设备组中的设备使用。Panorama 根据受管防火墙和策略规则命中次数（默认启用）确定规则使用情况。在 Panorama 上下文中，您可以查看所有设备组中的共享策略规则的规则使用情况。此外，您可以将上下文更改为单个设备组，并查看设备组中所有设备的总体策略规则使用情况。**Preview Rules**（预览规则）将显示设备组的每个策略规则的 **Hit Count**（命中次数）、**Last Hit**（最后一次命中）和 **First Hit**（第一次命中）。在重新启动、升级和数据平面重启事件期间，总流量命中次数以及第一次和最后一次命中时间戳持续存在。请参阅监控策略规则使用情况。

Group Rules by Tag（使用标记对规则分组）应用于标记后，可允许您对策略规则等进行分组，以便更好地查看规则功能，并轻松地管理规则库内的策略规则。按标签进行分组的规则可显示标记组列表，但保留规则优先级列表。您可将规则附加到标签组的末尾，将规则移至不同的标签组，应用其他标签到标签组内规则，并使用该组标签进行过滤或搜索。

要跟踪策略规则的更改，请添加 **Audit Comment**（审核注释），用以描述您所做的更改以及创建或修改规则的原因。输入结束后，审核注释被输入且配置更改被提交，审核注释保留在 **Audit Comment Archive**（审核注释存档）中，您可以在其中查看所选规则的所有先前审核注释。您可以在全局查找中搜索审核注释。审核注释存档是只读存档。

© 2019 Palo Alto Networks, Inc.

具有 Policies（策略）选项卡访问权限的管理用户可以将 Web 界面上显示的策略规则导出为 **PDF/CSV**。请参阅导出配置表格数据。

要创建策略，请参阅每个规则库的相关章节：

- Policies（策略）> Security（安全）
- Policies（策略）> NAT
- Policies（策略）> QoS
- Policies（策略）> Policy Based Forwarding（基于策略的转发）
- Policies（策略）> Decryption（解密）
- Policies（策略）> Application Override（应用程序替代）
- Policies（策略）> Authentication（身份验证）
- Policies（策略）> DoS Protection（DoS 保护）
- Policies（策略）> SD-WAN

© 2019 Palo Alto Networks, Inc.

传统模式下 Panorama 虚拟设备的日志存储分区

- Panorama > 设置 > 操作

默认情况下，传统模式下的 Panorama 虚拟设备拥有用于所有数据的单个磁盘分区，其中分配 10.89GB 用于日志存储。增加磁盘大小不会增加日志存储容量；但是，可以使用以下选项修改日志存储容量：

- **Network File System (NFS)**（网络文件系统 **(NFS)**）— 安装 NFS 存储的选项仅适用于传统模式并在 VMware ESXi 服务器上运行的 Panorama 虚拟设备。要安装 NFS 存储，选择 Miscellaneous（其他）部分中的 **Storage Partition Setup**（存储分区设置），将 **Storage Partition**（存储分区）设置为**NFS V3**，然后按表：NFS 存储设置.
- **Default internal storage**（默认内部存储）— 恢复为默认内部存储分区（仅适用于 ESXi 服务器或之前配置其他虚拟日志磁盘或挂载到 NFS 的 vCloud Air 平台上的 Panorama 设备）。要恢复为默认内部存储分区，请选择 Miscellaneous（其他）部分中的 **Storage Partition Setup**（存储分区设置），并将 **Storage Partition**（存储分区）设置为 **Internal**（内部）。
- **Virtual logging disk**（虚拟日志记录磁盘）— 可以为在 VMware ESXi 5.5 版及更高版本上运行的 Panorama 设备，或在 VMware vCloud Air 平台上运行的 Panorama 添加其他虚拟磁盘（最多 8TB）。但是，Panorama 在原始磁盘上停止使用默认 10.89GB 日志存储，将任何现有日志复制到新磁盘上。（早期版本的 ESXi 最多仅支持 2TB 虚拟磁盘。）

在更改存储分区设置后必须重新启动 *Panorama*：选择 *Panorama* > *Setup*（设置）> *Operations*（操作）和 *Reboot Panorama*（重新启动 *Panorama*）。

NFS 存储不仅适用于 *Panorama* 模式下的 *Panorama* 虚拟设备或 *M* 系列设备。

表 1: 表：NFS 存储设置

Panorama 存储分区设置 — NFS V3	说明
服务器	指定 NFS 服务器的 FQDN 或 IP 地址。
日志目录	指定日志将驻留的目录的完整路径名称。
协议	指定用于与 NFS 服务器通信的协议（UDP 或 TCP）。
端口	指定用于与 NFS 服务器通信的端口。
读取大小	指定 NFS 读取操作的最大字节数（范围为 256 至 32,768）。
写入大小	指定 NFS 写入操作的最大字节数（范围为 256 至 32,768）。
在设置时复制	选择此选项可在 Panorama 引导时安装 NFS 分区，并将任何现有日志复制到服务器上的目标目录。
测试记录分区	单击此选项可执行安装 NFS 分区的测试，并显示成功或失败消息。

© 2019 Palo Alto Networks, Inc.

Panorama > Setup（设置）> Interfaces（接口）

- Panorama > Setup（设置）> Interfaces（接口）

选择 **Panorama** > **Setup**（设置）> **Interfaces**（接口），可配置 Panorama 管理防火墙和日志收集器、向防火墙和日志收集器部署软件和内容更新、收集防火墙中的日志以及与收集器组通信所使用的接口。默认情况下，Panorama 使用管理 (MGT) 接口与防火墙和日志收集器进行通信。

要减少 *MGT* 接口的流量，请配置其他接口来部署更新、收集日志以及与收集器组通信。在有大量日志流量的环境中，可以配置多个接口来收集日志。此外，为增强流量管理的安全性，还可以为 *MGT* 接口定义一个比其他接口子网的专用性更强的单独子网（*IPv4* 网络掩码或 *IPv6* 前缀长度）。

可用接口因 Panorama 模式而异。

接口	最高速度	《M-500 设备	Panorama 虚拟设备
管理 (MGT)	1Gbps	✓	✓
Ethernet1 (Eth1)	1Gbps	✓	—
以太网2（Eth2）	1Gbps	✓	—
以太网3 (Eth3)	1Gbps	✓	—
以太网4 (Eth4)	10Gbps	✓	—
以太网5 (Eth5)	10Gbps	✓	—

要配置特定接口，请单击此接口名称，并按下表所述配置设置。

对于 *MGT* 接口，始终需要指定 *IP* 地址、网络掩码（对于 *IPv4*）或前缀长度（对于 *IPv6*）和默认网关。如果忽略某些设置（如默认网关）的值，则以后更改配置时只能通过控制台端口访问 *Panorama*。如果没有指定所有（三个）设置，则不能提交其他接口的配置。

接口设置	说明
Eth1/Eth2/Eth3/Eth4/Eth5	必须启用要配置的接口。MGT 接口例外，默认情况下，已启用此接口。
IP 地址 (IPv4)	如果网络使用 IPv4 地址，请为接口分配 IPv4 地址。
网络掩码 (IPv4)	如果已为接口分配 IPv4 地址，还必须输入网络掩码（如 255.255.255.0）。
默认网关 (IPv4)	如果已为接口分配 IPv4 地址，还必须为默认网关分配 IPv4 地址（网关与接口必须在同一子网中）。

© 2019 Palo Alto Networks, Inc.

接口设置	说明
IPv6 地址/前缀长度	如果网络使用 IPv6 地址，请为接口分配 IPv6 地址。要指明网络掩码，请输入 IPv6 前缀长度（如 2001:400:f00::1/64）。 对于部署在私有云环境（*ESXi*、*vCloud Air*、*KVM* 或 *Hyper-V*）中的所有 *M* 系列设备和 *Panorama* 虚拟设备，其上的 *MGT* 接口都支持 *IPv6* 地址。对于部署在公共云环境（*Amazon Web Services (AWS)*、*AWS GovCloud*、*Microsoft Azure* 或 *Google Cloud Platform*）中的 *Panorama* 虚拟设备，其上的 *MGT* 接口不支持 *IPv6* 地址。
默认 IPv6 网关	如果已为接口分配 IPv6 地址，还必须为默认网关分配 IPv6 地址（网关与接口必须在同一子网中）。 对于部署在私有云环境（*ESXi*、*vCloud Air*、*KVM* 或 *Hyper-V*）中的所有 *M* 系列设备和 *Panorama* 虚拟设备，其上的 *MGT* 接口都支持 *IPv6* 地址。对于部署在公共云环境（*Amazon Web Services (AWS)*、*AWS GovCloud*、*Microsoft Azure* 或 *Google Cloud Platform*）中的 *Panorama* 虚拟设备，其上的 *MGT* 接口不支持 *IPv6* 地址。
速度	在全双工或半双工模式下，将接口速度设置为 10Mbps、100Mbps、1Gbps 或 10Gbps（仅限 Eth4 和 Eth5）。使用默认自动协商设置可使 Panorama 确定接口速度。 此设置必须与相邻网络设备上的接口设置匹配。要确保设置匹配，请在相邻设备支持自动协商选项的情况下选择此选项。
MTU	输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 1,500，默认为 1,500）。
设备管理和设备日志收集	启用接口（默认情况下，已启用 MGT 接口）来管理防火墙和日志收集器，并收集其日志。可以启用多个接口来执行这些功能。
收集器组通信	启用接口与收集器组通信（默认值是 MGT 接口）。只有一个接口可以执行此功能。
Syslog 转发	启用用于转发 syslogs 的接口（默认为 MGT 接口）。只有一个接口可以执行此功能。
设备部署	启用接口将软件和内容更新部署到防火墙和日志收集器（默认值是 MGT 接口）。只有一个接口可以执行此功能。
管理管理服务	• **HTTP** — 用于访问 Panorama Web 界面。HTTP 使用初始明文，但其安全性不及 HTTPS。 为接口上的管理流量启用 *HTTPS* 而非 *Telnet*。 • **Telnet** — 用于访问 Panorama CLI。Telnet 使用初始明文，但其安全性不及 SSH。 • **HTTPS** — 用于安全访问 Panorama Web 界面。

© 2019 Palo Alto Networks, Inc.

接口设置	说明
	为接口上的管理流量启用 *SSH* 而非 *Telnet*。 • **SSH** — 用于安全访问 Panorama CLI。
网络连接服务	**Ping** 服务可用于任何接口。您可以使用 ping 测试 Panorama 接口与外部服务之间的连接。在高可用性 (HA) 部署中，HA 对将使用 Ping 命令来交换检测信号备份信息。 以下服务仅可以在 MGT 接口上执行： • **SNMP** — 让 Panorama 处理来自 SNMP 管理器的统计信息查询。有关详细信息，请参阅启用 SNMP 监控。 • **User-ID** — 让 Panorama 重新分发从 User-ID 代理接收的用户映射信息。
允许的 IP 地址	输入管理员通过此接口访问 Panorama 所使用的 IP 地址。空列表（默认）指定可从任何 IP 地址进行访问。 不能将此列表留空；指定 *Panorama* 管理员（仅限）的 *IP* 地址可阻止未授权访问。

© 2019 Palo Alto Networks, Inc.

Panorama > High Availability（高可用性）

要启用 Panorama 的高可用性 (HA)，请按下表所述配置设置。

Panorama HA 设置	说明
设置 单击 Edit（编辑）() 可配置以下设置。	
启用 HA	选中此选项可启用 HA。
对等 HA IP 地址	输入对端设备 MGT 接口的 IP 地址。
启用加密	启用后，MGT 接口会加密 HA 对端之间的通信。在启用加密之前，请从 HA 对端导出 HA 密钥，再将其导入其他对端。您可以在 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）页面上导入和导出 HA 密钥（请参阅管理防火墙和 Panorama 证书）。 在未启用加密时，*HA* 连接使用已启用加密的 *TCP* 端口 *28* 以及 *TCP* 端口 *28769*。
监视保持时间（毫秒）	输入在对控制链路故障起作用之前系统要等待的时间（以毫秒为单位，范围为 1,000 - 60,000，默认为 3,000）。
选择设置 单击 Edit（编辑）() 可配置以下设置。	
优先级 （必须在 Panorama 虚拟设备上操作）	通过此设置即可确定作为防火墙日志主要接收方的对端。在 HA 对中，将一个对端指定为主要设备，而将另一个指定为辅助设备。 在传统模式下为 Panorama 虚拟设备配置日志存储分区时，可以使用其内部磁盘（默认值）或网络文件系统 (NFS) 作为日志存储区。如果您配置 NFS，则仅有主要接收方会收到防火墙日志。如果配置内部磁盘存储区，默认情况下，防火墙会将日志发送到主要和辅助对端设备，但您可以更改此设置，只需在 Logging and Reporting Settings（记录和报告设置）中启用 **Only Active Primary Logs to Local Disk**（仅将主动-主要日志保存到本地磁盘）即可。
抢先	选中此选项可让主要 Panorama 从故障恢复后继续主动运行。如果禁用此设置，则辅助 Panorama 会保持主动状态，即使主要 Panorama 从故障恢复后也是如此。
HA 计时器设置	您的选择将确定剩余 HA 选择设置的值，进而控制故障转移的速度： • **Recommended**（推荐）— 选择此选项可获取故障转移计时器典型（默认）设置。如需查看关联值，请选择 **Advanced**（高级）和 **Load Recommended**（建议加载）。 • **Aggressive**（积极）— 选择此选项可获取故障转移计时器快速设置。如需查看关联值，请选择 **Advanced**（高级）和 **Load Aggressive**（积极加载）。 • **Advanced**（高级）— 选中此选项可显示剩余的 HA 选择设置，并自定义其值。 请查看以下设置的 **Recommended**（推荐）和 **Aggressive**（积极）值。

© 2019 Palo Alto Networks, Inc.

Panorama HA 设置	说明
提升保持时间（毫秒）	输入主要对端设备出现故障后，辅助 Panorama 对端设备在接管之前所等待的时间（以毫秒为单位，范围为 0 - 60,000）。推荐（默认）值为 2,000；积极值为 500。
Hello Interval (ms)	输入为验证其他对端设备是否正常工作发送的呼叫数据包之间的间隔时间（以毫秒为单位，范围为 8,000 - 60,000）。推荐（默认）值和积极值均为 8,000。
检测信号间隔（毫秒）	指定 Panorama 向 HA 对端设备发送 ICMP ping 的频率（以毫秒为单位，范围为 1,000 - 60,000）。推荐（默认）值为 2,000；积极值为 1,000。
Preemption Hold Time (min)	仅当您同时选择了 **Preemptive**（抢占）选项时，才能应用此字段。输入被动 Panorama 对端设备从导致故障转移的事件恢复后，回退到主动状态之前所等待的时间（以分钟为单位，范围为 1 - 60）。推荐（默认）值和积极值均为 1。
监视失败保持运行时间（毫秒）	指定在路径监控失败后 Panorama 尝试重新进入被动状态之前所等待的时间（以毫秒为单位，范围为 0 - 60,000）。在此期间，此被动对端不可在主动对端发生故障的情况下对其进行接管。此间隔可使 Panorama 避免因邻近设备偶然翻动而导致的故障转移。推荐（默认）值和积极值均为 0。
其他主设备保持运行时间(毫秒)	指定抢占对端设备在作为主动对端设备接管之前，保持被动状态的时间（以毫秒为单位，范围为 0 - 60,000）。推荐（默认）值为 7,000；积极值为 5,000。
路径监视 单击编辑 (⚙) 可配置 HA 路径监控。	
已启用	选中此选项可启用路径监控。路径监控可使 Panorama 能够通过发送 ICMP Ping 消息来监控指定的目标 IP 地址，以验证其是否能作出响应。
失败条件	选择是在 **Any**（任何）受监控路径组未能响应时还是在 **All**（所有）受监控路径组未能响应时，发生故障转移。
路径组 如需创建 HA 路径监控的路径组，请单击 **Add**（添加）并完成以下字段的设置。	
名称	指定路径组的名称。
已启用	选中此选项可启用路径组。
失败条件	选择是在 **Any**（任何）或 **All**（所有）指定目标地址未能响应时，发生故障。
Ping 间隔	指定验证目标 IP 地址路径处于正常状态的 ICMP 回显消息之间间隔的时间（以毫秒为单位，范围为 1,000 - 60,000；默认为 5,000）。
Ping 计数	指定声明故障之前的失败 ping 数（范围为 3 - 10；默认为 3）。
目标 IP	输入一个或多个目标 IP 地址以进行监控。多个地址之间用逗号隔开。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed WildFire Clusters（受管 Wildfire 集群）

- Panorama > Managed WildFire Clusters（受管 Wildfire 集群）
- Panorama > Managed WildFire Appliances（受管 WildFire 设备）

您可以采用集群形式来管理 WildFire 设备，也可以将其作为独立于 Panorama M 系列设备或虚拟设备的设备来管理。管理集群（**Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群））和管理独立的设备（**Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备））将共享许多常见的管理和配置任务，以下主题将介绍这两部分内容。

在将 WildFire 设备添加到 Panorama 后，可使用 Web 界面将这些设备添加到集群中，以集群形式管理这些设备，或者将这些设备作为独立的设备来管理。

- 受管 Wildfire 集群任务
- 受管 Wildfire 设备任务
- 受管 Wildfire 信息
- 受管 WildFire 集群和设备管理

受管 Wildfire 集群任务

您可以从 Panorama 创建并删除 WildFire 设备集群。此外，也可以通过将配置从一个集群导入另一个集群来节省配置时间。

任务	说明
创建集群	根据需要 **Create Cluster**（创建集群），输入新集群的名称，然后单击 **OK**（确定）。 在本地配置并通过添加单个 WildFire 设备节点来将其添加到 Panorama 的现有集群与其 WildFire 节点和节点角色一起列出（**Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备））。 集群名称必须是以小写字符和数字为开头的有效子域名，并且只有在当它们不是集群名称中的第一个或最后一个字符时才能包含连字符；不允许包含空格或其他字符。集群名称的最大长度为 63 个字符。 创建集群后，可以将受管 WildFire 设备添加到集群，并在 Panorama 上进行管理。将 WildFire 设备添加到 Panorama 后，会自动将设备注册到 Panorama。 在 Panorama 上最多可以创建 10 个受管 WildFire 集群，每个集群最多可以拥有 20 个 WildFire 设备节点。Panorama 最多可以管理总共 200 个聚合的独立设备和集群节点。
导入集群配置	**Import Cluster Config**（导入集群配置）可导入现有集群配置。如果在 **Import Cluster Config**（导入集群配置）之前选择集群，则 **Controller**（控制器）和 **Cluster**（集群）自动填充所选集群的相应信息。如果在If you do not select a cluster before you **Import Cluster Config**（导入集群配置）未选择集群，则必须选择 **Controller**（控制器）和 **Cluster**（集群）根据所选的控制器模式自动填充。 导入配置后，单击 **Commit to Panorama**（提交到 **Panorama**）将导入的待选配置保存在 Panorama 运行配置中。

© 2019 Palo Alto Networks, Inc.

任务	说明
从 Panorama 中删除	如果不再需要从 Panorama 管理 WildFire 集群，请 **Remove From Panorama**（从 **Panorama** 中删除），然后选择 **Yes**（是）确认删除。从 Panorama 管理服务器删除集群后，您可以从控制器节点本地管理集群。如果您希望再次集中管理集群而不是在本地进行管理，可以随时将集群重新添加到 Panorama 设备。
加密 WildFire 集群设备到设备通信	要加密集群中 WildFire 设备之间的数据通信，请选择 **Secure Cluster Communication**（安全集群通信）中的 **Enable**（启用）加密。 WildFire 使用预定义证书或自定义证书在设备之间进行通信。只有在您 **Customize Secure Server Communication**（自定义安全服务器通信）并启用 **Custom Certificate Only**（仅自定义证书）时才使用自定义证书。 WildFire 集群需要加密才能在 FIPS-CC 模式下运行。FIPS-CC 模式中使用的自定义证书必须符合 FIPS-CC 要求。 启用安全集群通信后，可以将其他受管 WildFire 设备添加到集群。新添加的设备会自动使用安全集群通信设置。

受管 Wildfire 设备任务

您可以在 Panorama 设备上添加、删除和管理独立的 WildFire 设备。添加独立设备后，可以将其添加到 WildFire 设备集群作为集群节点，也可以将其作为单个独立设备进行管理。

任务	说明

添加设备	**Add Appliance**（添加设备）可将一个或多个 WildFire 设备添加到 Panorama 设备进行集中管理。在单独的行（新行）中输入每个 WildFire 设备的序列号。Panorama 最多可以管理 200 个聚合 WildFire 集群节点和独立的 WildFire 设备。
	在要在 Panorama 上管理的每个 WildFire 设备上，可以使用以下 WildFire 设备 CLI 命令配置 Panorama 设备（Panorama 服务器）和可选备份 Panorama 服务器的 IP 地址或 FQDN：
	`set deviceconfig system panorama-server <ip-address | FQDN>`
	`set deviceconfig system panorama-server-2 <ip-address | FQDN>`

导入配置	选择 WildFire 设备和 **Import Config**（导入配置），以便只将该设备的运行配置导入 Panorama。 导入配置后，单击 **Commit to Panorama**（提交到 **Panorama**）将导入的待选配置保存在 Panorama 运行配置中。
删除	如果不再需要从 Panorama 管理 WildFire 设备，请 **Remove**（删除）设备，然后选择 **Yes**（是）确认删除。从 Panorama 管理服务器删除设备后，您可以使用其 CLI 在本地管理设备。如果需要，您可以随时将设备重新添加到 Panorama 设备（如果您希望再次集中管理设备而不是在本地进行管理）。

© 2019 Palo Alto Networks, Inc.

受管 Wildfire 信息

选择 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群）以显示每个受管集群的以下信息（也可以从此页面选择独立设备并显示其信息），或选择 **Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备）以显示独立设备的信息。

除非另有说明，否则下表中的信息同时适用于 WildFire 集群和独立设备。先前为集群或设备配置的信息已预填充。

受管 Wildfire 信息	说明
设备	设备的名称。 受管 WildFire 集群视图显示按集群分组的设备，包括可添加到集群的独立设备和包含设备名称（序列号不是名称的一部分）的序列号（括号中）。
序列号 （仅限受管 WildFire 设备视图）	设备的序列号。受管 WildFire 集群视图显示与设备名称相同列中的序列号（序列号不是名称的一部分）。
软件版本	在设备上安装并运行的软件版本。
IP 地址	设备的 IP 地址。
连接	设备和 Panorama 之间的连接状态 — Connected（已连接）或 Disconnected（已断开连接）
群集名称	将设备作为节点包含在其中的集群的名称；此处不会显示独立设备的任何信息。
分析环境	分析环境（vm1、vm2、vm3、vm4 或 vm5）。每个分析环境均代表一组操作系统和应用程序： • vm-1 支持 Windows XP、Adobe Reader 9.3.3、Flash 9、PE、PDF 和 Office 2003 及更旧版本的 Office 版本。 • vm-2 支持 Windows XP、Adobe Reader 9.4.0、Flash 10n、PE、PDF 和 Office 2007 及更早版本的 Office 版本。 • vm-3 支持 Windows XP、Adobe Reader 11、Flash 11、PE、PDF 和 Office 2010 及更旧版本的 Office 版本。 • vm-4 支持 Windows 7 32 位、Adobe Reader 11、Flash 11、PE、PDF 和 Office 2010 及更旧版本的 Office 版本。 • vm-5 支持 Windows 7 64 位、Adobe Reader 11、Flash 11、PE、PDF 和 Office 2010 及更旧版本的 Office 版本。
内容	内容发行版本的序列号。
角色	设备角色： • **Standalone**（独立）— 设备不是集群节点。 • **Controller**（控制器）— 设备是集群控制器节点。 • **Controller Backup**（控制器备份）— 设备是集群控制器备份节点。 • **Worker**（辅助角色）— 设备是集群中的辅助角色节点。
配置状态	设备的配置同步状态。Panorama 设备检查 WildFire 设备设置，并报告设备配置与在 Panorama 上为该设备保存的配置之间的配置差异。

© 2019 Palo Alto Networks, Inc.

受管 Wildfire 信息	说明
	• **In Sync**（同步）— 设备配置与在 Panorama 上保存的配置保持同步。 • **Out of Sync**（不同步）— 设备配置与在 Panorama 上保存的配置不同步。可以将鼠标悬停在眼镜上方以显示同步失败的原因。

集群状态
（仅限受管 WildFire 集群页面）
	集群状态显示每个集群节点的三种类型信息：
	• 可用服务（正常操作条件）：
	  • **wfpc**（WildFire 私有云）— 恶意软件样本分析和报告服务。
	  • **signature**（签名）— 本地签名生成服务。
	• Progress of operations（操作进度）— 操作名称后跟冒号 (:) 和状态：
	  • **Operations**（操作）— 停用、挂起和重新启动操作的状态。
	  • **Progress status**（进度状态）— 每个操作的操作状态通知都相同：已请求、正在进行、已拒绝、成功或失败。
	  例如，如果挂起某个节点且操作正在进行，则集群状态显示 `suspend:ongoing`，或如果重新启动某个节点且已请求操作但尚未开始，则集群状态显示 `reboot:requested`。
	• 错误条件：
	  集群状态显示以下错误条件：
	  • **Cluster**（集群）— `cluster:offline` 或 `cluster:splitbrain`。
	  • **Service**（服务）— `service:suspended` 或 `service:none`。

最后提交状态	`Commit succeeded`（如果最近的提交成功）或 `commit failed`（如果最近的提交失败）。通过选择状态查看有关最后提交的详细信息。
Utilization（使用率）> View（查看）	

查看	**View**（查看）集群或设备使用率统计信息。只能查看个别设备（**Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备））或集群统计信息（**Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群））。
	• **Appliance**（设备）—（仅限独立设备视图）设备序列号。
	• **Cluster**（集群）—（仅限集群视图）集群名称。您还可以选择要查看的其他集群。
	• **Duration**（期限）— 显示收集和显示统计信息的时间段。您可以选择不同的期限：
	  • **15** 分钟
	  • 最后一小时
	  • 过去 **24** 小时（默认）
	  • 最后 **7** 天
	  • 全部
	Utilization（使用率）**View**（视图）包含四个选项卡，在每个选项卡上可以根据配置的 **Duration**（期限）确定显示的信息。

“常规”选项卡	**General**（常规）选项卡显示集群或设备的聚合资源使用率统计信息。其他选项卡按文件类型显示有关资源使用率的更详细信息： • **Total Disk Usage**（磁盘总体使用率）— 集群或设备磁盘的总体使用率。

© 2019 Palo Alto Networks, Inc.

受管 Wildfire 信息	说明

	• **Verdict**（判定）— 判定的总数，分配给文件的每种判定类型数：**Malware**（恶意软件）、**Grayware**（灰色软件）和 **Benign**（良性）；以及 **Error**（错误）判定的判定数。
	• **Sample Statistics**（样本统计信息）— **Submitted**（已提交）和 **Analyzed**（已分析）样本的总数，以及 **Pending**（挂起）分析的样本数。
	• **Analysis Environment & System Utilization**（分析环境和系统利用率）：
	  • **File Type Analyzed**（已分析文件类型）— 已经分析的文件类型：**Executable**（可执行文件）、**Non-Executable**（不可执行文件）或 **Links**（链路）。
	  • **Virtual Machine Usage**（虚拟机使用率）— 用于各种已分析文件类型和可用于分析各种文件类型的虚拟机数。例如，对于可执行文件，虚拟机使用率可能为 6/10（已使用六台虚拟机，十台虚拟机可供使用）。
	  • **Files Analyzed**（已分析文件）— 已经分析的各种类型的文件数。

可执行文件、不可执行文件和链路选项卡	**Executable**（可执行文件）、**Non-Executable**（不可执行文件）和 **Links**（链路）显示有关各种文件类型的类似信息：
	• **Verdict**（判定）— 有关按文件类型判定的详细信息。您可以过滤结果：
	  • **Search box**（搜索框）— 输入搜索词以过滤判定。搜索框指示列表中文件类型（项目）的数量。输入搜索词后，应用过滤器（→）或清除过滤器（×），然后输入一组不同的搜索词。
	  • **File Type**（文件类型）— 按类型列出文件。例如，**Executable**（可执行文件）选项卡显示 .exe 和 .dll 文件类型；**Non-Executable**（不可执行文件）选项卡显示 .pdf、.jar、.doc、.ppt、.xls、.docx、.pptx、.xlsx、.rtf、class 和 .swf 文件类型；**Links**（链路）选项卡显示 elink 文件类型信息。
	  • 对于每种 **File Type**（文件类型），**Malware**（恶意软件）、**Grayware**（灰色软件）和 **Benign**（良性）文件的判定总数，**Error**（错误）判定数和每个选项卡上显示的判定 **Total**（总数）。
	• **Sample Statistics**（样本统计信息）— 有关按文件类型分析的样本的详细信息。
	  • **Search box**（搜索框）— 与 **Verdict**（判定）搜索框相同。
	  • **File Type**（文件类型）— 与 **Verdict File Type**（判定文件类型）相同。
	  • 对于每种 **File Type**（文件类型），**Submitted**（已提交）进行分析的文件总数、 the total number **Analyzed**（已分析）总数和每个选项卡上显示的 **Pending**（挂起）分析数。

Firewalls Connected（已连接防火墙）> View（查看）	
查看	**View**（查看）有关已连接到集群或设备的防火墙的信息。只能查看个别设备（**Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备））或集群统计信息（**Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群））。 • **Appliance**（设备）—（仅限独立设备视图）设备序列号。 • **Cluster**（集群）—（仅限集群视图）集群名称，您还可以选择要查看的其他集群。 • **Refresh**（刷新）— 刷新显示。
已注册和提交样本选项卡	**Registered**（已注册）选项卡显示有关已注册到集群或设备的防火墙的信息，而不考虑防火墙是否提交样本。

© 2019 Palo Alto Networks, Inc.

受管 Wildfire 信息	说明
	Submitting Samples（提交样本）选项卡显示有关正在积极将样本提交到 WildFire 集群或设备的防火墙的信息。 对于下列两种情况，这些选项卡上显示的信息类型和过滤信息的方式类似： • **Search box**（搜索框）— 输入搜索词以过滤防火墙列表。搜索框指示列表中防火墙（项目）的数量。输入搜索词后，应用过滤器 (→) 或清除过滤器 (×)，然后输入一组不同的搜索词。 • **S/N** — 防火墙的序列号。 • **IP Address**（**IP** 地址）— 防火墙的 IP 地址。 • **Model**（型号）— 防火墙的型号。 • **Software Version**（软件版本）— 在防火墙上安装并运行的软件版本。

受管 WildFire 集群和设备管理

选择 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群），并选择要管理的集群或选择 WildFire 设备（**Panorama** > **Managed WildFire Appliances**（受管 **WildFire** 设备））可管理独立设备。**Panorama** > **Managed WildFire Cluster**（受管 **WildFire** 集群）视图列出了集群节点（作为集群成员的 WildFire 设备）和独立设备，以便可以将可用设备添加到集群。由于集群管理节点，因此集群节点仅提供有限的管理功能。

除非另有说明，否则下表中的设置和说明同时适用于 WildFire 集群和 WildFire 独立设备。先前在集群或设备上配置的信息已预填充。您必须先对 Panorama 上的信息提交更改和添加，然后将新配置推送到设备。

设置	说明
“常规”选项卡	
姓名	集群或设备 **Name**（名称）或设备序列号。
启用 DNS （仅限 WildFire 集群）	集群的 **Enable DNS**（启用 **DNS**）服务。
将防火墙注册到	注册防火墙的域名。格式必须为 `wfpc.service.`*<cluster-name>*`.`*<domain>*。例如，默认域名为 `wfpc.service.mycluster.paloaltonetworks.com`。
内容更新服务器	输入 **Content Update Server**（内容更新服务器）位置或使用默认 `wildfire.paloaltonetworks.com`，以便集群或设备从内容传送网络基础架构中最近服务器接收内容更新。连接到全局云可让您根据来自连接到云的所有源的威胁分析访问签名和更新，而不仅仅是依赖于本地威胁的分析。
检查服务器标识	**Check Server Identity**（检查服务器标识）可通过将证书中的通用名 (CN) 与服务器的 IP 地址或 FQDN 进行相匹配，以确认更新服务器的标识。
WildFire 云服务器	输入全局 **WildFire Cloud Server**（**WildFire** 云服务器）位置或使用默认 `wildfire.paloaltonetworks.com`，以便集群或设备可以将信息发送到最近的服务器。您可以选择是否发送信息以及要发送到全局云（**WildFire Cloud Services**（**WildFire** 云服务））的信息类型。
样本分析图	选择集群或设备用于样本分析的 VM 映像（默认为 vm-5）。您可以获取恶意软件测试文件 (WildFire API) 以查看样本分析的结果。

© 2019 Palo Alto Networks, Inc.

设置	说明
WildFire 云服务	如果已将集群或设备连接到全局 WildFire 云服务器，则可以选择是向全局云 **Send Analysis Data**（发送分析数据）、**Send Malicious Samples**（发送恶意样本）、**Send Diagnostics**（发送诊断），还是三者的任意组合。您还可以选择是否在全局云中执行 **Verdict Lookup**（判定查询）。将信息发送到全局云有利于 WildFire 用户的整个团体，因为共享信息可提高每个设备识别恶意通信并阻止其遍历网络的能力。
样本数据保留	保留良性或灰色软件样本和恶意样本的天数： • **Benign/Grayware**（良性/灰色软件）样本 — 范围为 1 至 90，默认为 14。 • **Malicious**（恶意）样本 — 最小值为 1，没有最大值（无限期），默认为无限期。
分析环境服务	**Environment Networking**（环境网络）能让虚拟机与互联网进行通信。您可以选择 **Anonymous Networking**（匿名网络）以使网络进行匿名通信，但首先必须选择 **Environment Networking**（环境网络），然后才可启用 **Anonymous Networking**（匿名网络）。 不同的网络环境会产生不同类型的分析负载，具体取决于需要分析更多的文档还是需要分析更多的可执行文件。您可以配置 Preferred Analysis Environment（首选分析环境）以将多个资源分配给 **Executables**（可执行文件）或 **Documents**（文档），具体取决于环境需求。**Default**（默认）分配是在 **Executables**（可执行文件）和 **Documents**（文档）之间进行平衡。 可用资源的数量取决于集群中 WildFire 节点的数量。
签名生成	选择是否希望集群或设备为 AV、DNS、URL 或三者的任意组合生成签名。
设备选项卡	
主机名 （仅限独立的 WildFire 设备）	输入 WildFire 设备的主机名。
Panorama Server	输入设备或管理集群的主 Panorama 服务器的 IP 地址或 FQDN。
Panorama 服务器 2	输入设备或管理集群的备份 Panorama 服务器的 IP 地址或 FQDN。
域	输入设备集群或设备的域名。
主 DNS 服务器	输入主 DNS 服务器的 IP 地址。
辅助 DNS 服务器	输入辅助 DNS 服务器的 IP 地址。
timezone	选择要用于集群或设备的时区。
纬度 （仅限独立的 WildFire 设备）	输入 WildFire 设备的纬度。
经度	输入 WildFire 设备的经度。

© 2019 Palo Alto Networks, Inc.

设置	说明
（仅限独立的 WildFire 设备）	
主 NTP 服务器	输入主 NTP 服务器的 IP 地址，并将 Authentication Type（身份验证类型）设置为 **None**（无）（默认）、**Symmetric Key**（对称式密钥）或 **Autokey**（自动密钥）。 将 Authentication Type（身份验证类型）设置为 **Symmetric Key**（对称式密钥）可显示四个以上字段： • **Key ID**（密钥 **ID**）— 输入身份验证密钥 ID。 • **Algorithm**（算法）— 将身份验证算法设置为 **SHA1** 或 **MD5**。 • **Authentication Key**（身份验证密钥）— 输入身份验证密钥。 • **Confirm Authentication Key**（确认身份验证密钥）— 再次输入确认身份验证密钥以确认。
辅助 NTP 服务器	输入辅助 NTP 服务器的 IP 地址，并将 Authentication Type（身份验证类型）设置为 **None**（无）（默认）、**Symmetric Key**（对称式密钥）或 **Autokey**（自动密钥）。 将 Authentication Type（身份验证类型）设置为 **Symmetric Key**（对称式密钥）可显示四个以上字段： • **Key ID**（密钥 **ID**）— 输入身份验证密钥 ID。 • **Algorithm**（算法）— 将身份验证算法设置为 **SHA1** 或 **MD5**。 • **Authentication Key**（身份验证密钥）— 输入身份验证密钥。 • **Confirm Authentication Key**（确认身份验证密钥）— 再次输入确认身份验证密钥以确认。
登录提示	输入当用户登录到集群或设备时显示的横幅消息。
日志记录选项卡（包括系统选项卡和配置选项卡）	
添加	**Add**（添加）日志转发配置文件（**Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群）> *<cluster>* > **Logging**（日志记录）> **System**（系统）或 **Panorama** > **Managed WildFire Clusters**（受管 **WildFire** 集群）> *<cluster>* > **Logging**（日志记录）> **Configuration**（配置））以： • 将系统或配置日志作为 SNMP 陷阱转发到 SNMP 陷阱接收器。 • 将 syslog 消息转发到 syslog 服务器。 • 将电子邮件通知转发到电子邮件服务器。 • 将 HTTP 请求转发到 HTTP 服务器。 不支持任何其他日志类型（请参阅 Device（设备）> Log Settings（日志设置））。 日志转发配置文件指定要转发的日志以及转发到的目标服务器。对于每个配置文件，请完成以下步骤： • **Name**（名称）— 用于标识日志设置的名称（最多 31 个字符），只能包含字母数字字符和下划线，不得包含空格和特殊字符。 • **Filter**（过滤器）— 默认情况下，Panorama 设备转发指定配置文件的 **All Logs**（所有日志）。要转发一部分日志，选择过滤器（**severity eq critical**、**severity eq high**、**severity eq informational**、**severity eq low** 或 **severity eq medium**）或选择 **Filter Builder**（过滤器构建器）创建新的过滤器。

© 2019 Palo Alto Networks, Inc.

设置	说明
	• **Description**（说明）— 输入说明（最多 1,023 个字符），以说明配置文件的用途。

Add（添加）> Filter（过滤器）> Filter Builder（过滤器构建器）	使用 **Filter Builder**（过滤器构建器）创建新的日志过滤器。选择 **Create Filter**（创建过滤器）以构建过滤器，对于新过滤器中的每个查询，请指定以下设置，然后 **Add**（添加）查询：
	• **Connector**（连接符）— 选择连接符逻辑（**and** 或 **or**）。如果要应用求反，请选择 **Negate**（求反）。例如，为避免转发一部分日志说明，请选择 **Description**（说明）作为 Attribute（属性），选择 **contains**（包含）作为 Operator（运算符），然后输入说明字符串作为 Value（值）以标识不希望转发的说明。
	• **Attribute**（属性）— 选择日志属性。选择因日志类型而异。
	• **Operator**（运算符）— 选择确定如何应用属性的标准（如 **contains**（包含））。选择因日志类型而异。
	• 值- 指定要匹配的属性值。
	• **Add**（添加）— 添加新过滤器。
	要显示或导出过滤器匹配的日志，请选择 **View Filtered Logs**（查看过滤的日志）。
	• 要查找匹配的日志条目，您可将构件（如 IP 地址或时间范围）添加到搜索字段。
	• 选择要查看日志的时间段：**Last 15 Minutes**（过去 **15** 分钟）、**Last Hour**（过去 **1** 小时）、**Last 6 Hrs**（过去 **6** 小时）、**Last 12 Hrs**（过去 **12** 小时）、**Last 24 Hrs**（过去 **24** 小时）、**Last 7 Days**（过去 **7** 天）、**Last 30 Days**（过去 **30** 天）或 **All**（全部）（默认）。
	• 使用时间段下拉列表右侧的选项应用、清除、添加、保存和加载筛选程序。
	  • **Apply filters**（应用过滤器）(→) — 显示与搜索字段中的项目相匹配的日志条目。
	  • **Clear filters**（清除过滤器）(×) — 清除过滤器字段。
	  • **Add a new filter**（添加新筛选程序）(⊕) — 定义新的搜索条件（介绍 Add Log Filter（添加日志筛选程序），类似于创建筛选程序）。
	  • **Save a filter**（保存过滤器）( ) — 输入过滤器的名称，然后单击 **OK**（确定）。
	  • **Use a saved filter**（使用保存的过滤器）( ) — 将保存的过滤器添加到过滤器字段。
	  • **Export to CSV**（导出为 **CSV**）( ) — 将日志导出为 CSV 格式报告，然后单击 **Download file**（下载文件）。默认情况下，该报告可最多包含 2,000 行日志。要更改生成的 CSV 报告的行数限制，请选择 **Device**（设备）> **Setup**（设置）> **Management**（管理）> **Logging and Reporting Settings**（日志记录和报告设置）> **Log Export and Reporting**（日志导出和报告），然后输入新的 **Max Rows in CSV Export**（**CSV** 导出中的最大行数）值。
	可以更改每页显示条目的数量和顺序，并使用页面左下角的分页控件浏览日志列表。日志条目以 10 页为一个页面块进行检索。
	• **per page**（每页）— 使用下拉列表更改每页的日志条目数（**20**、**30**、**40**、**50**、**75** 或 **100**）。

© 2019 Palo Alto Networks, Inc.

设置	说明

	• **ASC** 或 **DESC** — 选择 **ASC** 可按升序对结果进行排序（最旧的日志条目排第一），或选择 **DESC** 以按降序对结果进行排序（最新的日志条目排第一）。默认为 **DESC**。
	• **Resolve Hostname**（解析主机名）— 选择此选项可将外部 IP 地址解析为域名。
	• **Highlight Policy Actions**（突出显示策略操作）— 指定操作，并选择以突出显示与该操作相匹配的日志条目。过滤的日志将以下列颜色突出显示：
	  • 绿色 — 允许
	  • 黄色 — 继续或替代
	  • 红色 — 拒绝、丢弃、丢弃-icmp、重置-客户端、重置-服务器、重置-两者、阻止-继续、阻止-替代、阻止-url、丢弃-所有、sinkhole

删除	选择此选项，然后 **Delete**（删除）您希望从系统或配置日志列表中删除的日志转发设置。
身份验证选项卡	
身份验证配置文件	选择配置的身份验证配置文件以定义身份验证服务，该服务验证 WildFire 设备或 Panorama 管理员的登录凭据。
失败的尝试次数	输入 WildFire 设备在锁定管理员之前，允许在 CLI 上使用的失败的登录尝试次数（范围为 0-10；默认为 10）。限制登录尝试可以保护 WildFire 设备免遭暴力攻击。值 0 代表没有登录尝试限制。 如果设置 *Failed Attempts*（失败的尝试次数）为除 *0* 以外的一个值，但将 *Lockout Time*（锁定时间）设置为 *0*，那么此管理员将被无限期锁定，直到其他管理员手动解锁此管理员。如果尚未创建其他管理员，则必须在 *Panorama* 上重新配置 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）设置，并将此配置更改推送到 *WildFire* 设备。要确保管理员永远不被锁定，请为 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）使用默认值 *(0)*。 将 *Failed Attempts*（失败的尝试次数）设置为 *5* 或更少，以便在输入错误时容纳合理的重试次数，同时防止恶意系统尝试通过暴力攻击方法登录到 *WildFire* 设备。
锁定时间（分钟）	输入达到 **Failed Attempts**（失败的尝试次数）限制后，WildFire 设备锁定管理员访问 CLI 所需的分钟数（范围为 0 -60；默认为 5）。值为 0 表示应用锁定，直到其他管理员手动解锁此帐户。 如果设置 *Failed Attempts*（失败的尝试次数）为除 *0* 以外的一个值，但将 *Lockout Time*（锁定时间）设置为 *0*，那么此管理员将被无限期锁定，直到其他管理员手动解锁此管理员。如果尚未创建其他管理员，则必须在 *Panorama* 上重新配置 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）设置，并将此配置更改推送到 *WildFire* 设备。要确保管理员永远不被锁定，请为 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）使用默认值 *(0)*。

© 2019 Palo Alto Networks, Inc.

设置	说明
	设置 *Lockout Time*（锁定时间）为至少 *30* 分钟，防止恶意操作者连续登录尝试。
空闲超时（分钟）	输入在管理员自动注销之前 CLI 上没有执行任何活动的最长分钟数（范围为 0 - 1,440；没有默认值）。值为 0 表示不活动不会触发自动注销。 设置 *Idle Timeout*（空闲超时）为 *10* 分钟，以防止在管理员打开会话时未经授权的用户访问 *WildFire* 设备。
最大会话计数	输入管理员可以同时打开的活跃会话数。默认值为 0 则表示 WildFire 设备可以打开无限个并发活跃会话。
最长会话时间	输入管理员在自动注销之前可登录的分钟数。默认值为 0 则表示管理员可以无限期登录，即使空闲也能如此。
本地管理员	添加并配置 WildFire 设备的新管理员。这些管理员专属于 WildFire 设备，可通过该页面进行管理（**Panorama** > **Managed WildFire Appliances**（受管的 **WildFire** 设备）> **Authentication**（身份验证））。
Panorama 管理员	导入在 Panorama 上配置的现有管理员。这些管理员在 Panorama 上创建，并导入至 WildFire 设备。
集群选项卡（仅限受管 WildFire 集群）和接口选项卡（仅限受管 WildFire 设备） 必须将设备添加到 Panorama 以管理接口，并将设备添加到集群以管理节点接口。	
设备 （仅限集群选项卡）	选择集群节点以访问该节点的 Appliance（设备）和 Interfaces（接口）选项卡。Appliance（设备）选项卡节点信息已预填充，且除主机名以外不可配置。Interfaces（接口）选项卡列出节点接口。选择接口以按下述说明进行管理： • 接口名称管理 • 接口名称分析环境网络 • 接口名称 Ethernet2 • 接口名称 Ethernet3
接口名称管理	管理接口为 Ethernet0。配置或查看管理接口设置。 • **Speed and Duplex**（速度与双工）— 选择 **auto-negotiate**（自动协商）（默认）、**10Mbps-half-duplex**（**10Mbps** 半双工）、**10Mbps-full-duplex**（**10Mbps** 全双工）、**100Mbps-half-duplex**（**100Mbps** 半双工）、**100Mbps-full-duplex**（**100Mbps** 全双工）、**1Gbps-half-duplex**（**1Gbps** 半双工）或 **1Gbps-full-duplex**（**1Gbps** 全双工）。 • **IP Address**（**IP** 地址）— 输入接口 IP 地址。 • **Netmask**（网络掩码）— 输入接口网络掩码。 • **Default Gateway**（默认网关）— 输入默认网关的 IP 地址。 • **MTU** — 以字节为单位输入 MTU（范围为 576 至 1,500，默认为 1,500）。 • **Management Services**（管理服务）— 启用要支持的管理服务。可以支持 **Ping**、**SSH** 和 **SNMP** 服务。 如果使用代理服务器连接到互联网，请配置代理设置： • **Server**（服务器）— 代理服务器的 IP 地址。

© 2019 Palo Alto Networks, Inc.

设置	说明

	• **Port**（端口）— 在代理服务器上配置用于侦听 Panorama 设备请求的端口号。
	• **User**（用户）— 在代理服务器上配置用于进行身份验证的用户名。
	• **Password**（密码）和 **Confirm Password**（确认密码）— 在代理服务器上配置用于进行身份验证的密码。
	• **Clustering Services**（集群服务）（仅限集群选项卡）— 选择高可用性服务：
	  • **HA**（高可用性）— 如果集群中有两个控制器节点，可以配置管理接口作为高可用性接口，以便管理信息可用于两个控制器节点。如果配置的集群节点为主控制器节点，请将其标记为 **HA**（高可用性）接口。
	  根据使用 WildFire 设备以太网接口的方式，您也可以配置 Etherent2 或 Ethernet3 分别作为主控制器节点和备份控制器节点的 HA 接口和 HA 备份接口。例如，您可以使用 Ethernet 2 作为高可用性和高可用性备份接口。主和备份控制器节点的高可用性和高可用性备份接口必须是同一接口（管理、Ethernet2 或 Ethernet3）。您不能使用 Ethernet1 作为高可用性/高可用性备份接口。
	  • **HA Backup**（高可用性备份）— 如果配置的集群节点为备份控制器节点，请将其标记为 **HA Backup**（高可用性备份）接口。
	指定接口允许的 IP 地址：
	• **Search box**（搜索框）— 输入搜索词以过滤允许的 IP 地址列表。搜索框指示列表中 IP 地址（项目）的数量，以便您知道列表的长度。输入搜索词后，应用过滤器（→）或清除过滤器（×），然后输入一组不同的搜索词。
	• **Add**（添加）— **Add**（添加）允许使用的 IP 地址。
	• **Delete**（删除）— 选择并 **Delete**（删除）要从管理接口访问中删除的 IP 地址或地址。

接口名称分析环境网络	配置 WildFire 设备集群或独立 WildFire 设备分析环境网络接口（Ethernet1，也称为 VM 接口）的设置： • **Speed and Duplex**（速度与双工）— 设置为 **auto-negotiate**（自动协商）（默认）、**10Mbps-half-duplex**（**10Mbps** 半双工）、**10Mbps-full-duplex**（**10Mbps** 全双工）、**100Mbps-half-duplex**（**100Mbps** 半双工）、**100Mbps-full-duplex**（**100Mbps** 全双工）、**1Gbps-half-duplex**（**1Gbps** 半双工）或 **1Gbps-full-duplex**（**1Gbps** 全双工）。 • **IP Address**（**IP** 地址）— 输入接口 IP 地址。 • **Netmask**（网络掩码）— 输入接口网络掩码。 • **Default Gateway**（默认网关）— 输入默认网关的 IP 地址。 • **MTU** — 以字节为单位输入 MTU（范围为 576 至 1,500，默认为 1,500）。 • **DNS Server**（**DNS** 服务器）— 输入 DNS 服务器的 IP 地址。 • **Link State**（链路状态）— 将接口链路状态设置为 **Up**（打开）或 **Down**（关闭）。 • Management Services（管理服务）— 如果您希望接口支持 ping 服务，请启用 **Ping**。 指定接口允许的 IP 地址： • **Search box**（搜索框）— 输入搜索词以过滤允许的 IP 地址列表。搜索框指示列表中 IP 地址（项目）的数量，以便您知道列表的长度。输入搜索词后，应用过滤器（→）或清除过滤器（×），然后输入一组不同的搜索词。 • **Add**（添加）— **Add**（添加）允许使用的 IP 地址。

© 2019 Palo Alto Networks, Inc.

设置	说明
	• **Delete**（删除）— 选择要从管理接口访问中删除的 IP 地址或地址，然后单击 **Delete**（删除）。

接口名称 Ethernet2
接口名称 Ethernet3
	可以为 Ethernet2 和 Ethernet3 接口设置相同的参数：
	• **Speed and Duplex**（速度与双工）— 设置为 **auto-negotiate**（自动协商）（默认）、**10Mbps-half-duplex**（**10Mbps** 半双工）、**10Mbps-full-duplex**（**10Mbps** 全双工）、**100Mbps-half-duplex**（**100Mbps** 半双工）、**100Mbps-full-duplex**（**100Mbps** 全双工）、**1Gbps-half-duplex**（**1Gbps** 半双工）或 **1Gbps-full-duplex**（**1Gbps** 全双工）。
	• **IP Address**（**IP** 地址）— 输入接口 IP 地址。
	• **Netmask**（网络掩码）— 输入接口网络掩码。
	• **Default Gateway**（默认网关）— 输入默认网关的 IP 地址。
	• **MTU** — 以字节为单位输入 MTU（范围为 576 至 1,500，默认为 1,500）。
	• Management Services（管理服务）— 如果您希望接口支持 ping 服务，请启用 **Ping**。
	• **Clustering Services**（集群服务）— 选择集群服务：
	  • **HA**（高可用性）— 如果集群中有两个控制器节点，可以配置 Ethernet2 或 Ethernet3 接口作为高可用性接口，以便管理信息可用于两个控制器节点。如果配置的集群节点为主控制器节点，请将其标记为 **HA**（高可用性）接口。
	  根据使用 WildFire 设备以太网接口的方式，您也可以配置管理接口 (Ethernet1) 作为主和备份控制器节点的高可用性和高可用性备份接口。主和备份控制器节点的高可用性和高可用性备份接口必须是同一接口（管理、Ethernet2 或 Ethernet3）。您不能使用 Ethernet1 作为高可用性/高可用性备份接口。
	  • **HA Backup**（高可用性备份）— 如果配置的集群节点为备份控制器节点，请将其标记为 **HA Backup**（高可用性备份）接口。
	  • **Cluster Management**（集群管理）— 配置 Ethernet2 或 Ethernet3 接口作为用于集群范围管理和通信的接口。

角色 （仅限集群选项卡）	如果集群拥有成员设备，则设备角色可以是控制器、控制器备份或辅助角色。选择 **Controller**（控制器）或 **Backup Controller**（备份控制器）可从集群中的设备更改用于每个角色的 WildFire 设备。更改控制器可能会导致角色更改期间的数据丢失。
浏览 （仅限集群选项卡）	**Clustering**（集群）选项卡列出了集群中的 WildFire 设备节点。**Browse**（浏览）以查看并添加 Panorama 设备已经管理的独立 WildFire 设备： • **Search box**（搜索框）— 输入搜索词以过滤节点列表。搜索框指示列表中设备（项目）的数量，以便您知道列表的长度。输入搜索词后，应用过滤器 (→) 或清除过滤器 (×)，然后输入一组不同的搜索词。 • **Add Nodes**（添加节点）— 向集群添加 (⊕) 节点。 添加到集群的第一个 WildFire 设备自动成为控制器节点。添加到集群的第二个 WildFire 设备自动成为控制器备份节点。 最多可以向集群添加 20 个 WildFire 设备。添加控制器和控制器备份节点后，所有后续添加的节点都为辅助角色节点。

© 2019 Palo Alto Networks, Inc.

设置	说明
删除 （仅限集群选项卡）	从设备列表中选择一个或多个设备，然后从集群中将其 **Delete**（删除）。只有在集群中有两个控制器节点时才能删除控制器节点。
管理控制器 （仅限集群选项卡）	选择 **Manage Controller**（管理控制器）可从属于集群的 WildFire 设备节点中指定 **Controller**（控制器）和 **Controller Backup**（控制器备份）。默认情况下，已经选择当前的控制器节点和控制器备份节点。控制器备份节点不能是与主控制器节点相同的节点。
通信选项卡	

自定义安全服务器通信	• **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）— 从下拉列表中选择 SSL/TLS 服务配置文件。此配置文件定义连接设备用于与 WildFire 进行通信的证书和支持的 SSL/TLS 版本。
	• **Certificate Profile**（证书配置文件）— 从下拉列表中选择证书配置文件。此证书配置文件定义证书吊销检查行为和用于对客户端提供的证书链进行身份验证的根 CA。
	• **Custom Certificate Only**（仅自定义证书）— 启用后，WildFire 仅接受用于对连接设备进行身份验证的自定义证书。
	• **Check Authorization List**（检查授权列表）— 根据授权列表检查连接到 WildFire 的客户端设备。设备只需要与要授权的列表中的一个项目相匹配。如果找不到匹配项，则不对设备进行授权。
	• **Authorization List**（授权列表）— **Add**（添加）授权列表并填写以下字段，以设置对客户端设备进行授权的条件。Authorization List（授权列表）最多支持 16 个条目。
	  • **Identifier**（标识符）— 选择 **Subject**（主题）或 **Subject Alt**。**Name**（主题备选名称）作为授权标识符。
	  • **Type**（类型）— 如果选择 **Subject Alt.Name**（主题备选名称）作为标识符，则选择 **IP**、**hostname**（主机名）或 **e-mail**（电子邮件）作为标识符类型。如果选择 **Subject**（主题），则通用名为标识符类型。
	  • **Value**（值）— 输入标识符值。

安全客户端通信	使用 **Secure Client Communication**（安全客户端通信）可确保 WildFire 使用配置的自定义证书（而非默认预定义证书），对与其他 WildFire 设备的 SSL 连接进行身份验证。
	• **Predefined**（预定义）—（默认）不配置任何设备证书，WildFire 使用默认预定义证书。
	• **Local**（本地）— WildFire 使用在防火墙上生成或从现有企业 PKI 服务器导入的本地设备证书和相应私钥。
	  • **Certificate**（证书）：选择本地设备证书。
	  • **Certificate Profile**（证书配置文件）：从下拉列表中选择证书配置文件。
	• **SCEP** — WildFire 使用简单证书注册协议 (SCEP) 服务器生成的设备证书和私钥。
	  • **SCEP Profile**（**SCEP** 配置文件）：从下拉列表中选择 SCEP 配置文件。
	  • **Certificate Profile**（证书配置文件）：从下拉列表中选择证书配置文件。

安全集群通信	选择 **Enable**（启用）可加密 WildFire 设备之间的通信。默认证书使用预定义证书类型。要使用用户定义的自定义证书，必须配置 **Customize Secure Server**

© 2019 Palo Alto Networks, Inc.

设置	说明
	Communication（自定义安全服务器通信）并启用 **Custom Certificate Only**（仅自定义证书）。

© 2019 Palo Alto Networks, Inc.

Panorama > Administrators（管理员）

选择 **Panorama** > **Administrators**（管理员）可创建和管理 Panorama 管理员帐户。

如果以拥有超级用户角色的管理员身份登录 Panorama，则可以单击 Locked User（已锁定用户）列中的锁形图标，解锁其他管理员的帐户。锁定的管理员不能访问 Panorama。Panorama 会根据分配给管理员帐户的身份验证配置文件所定义的规则，锁定连续尝试访问 Panorama 失败的次数超过允许值的管理员（请参阅 Device（设备）> Authentication Profile（身份验证配置文件））。

要创建管理员帐户，请单击 **Add**（添加），并按下表所述配置设置。

管理员帐户设置	说明
名称	输入管理员的登录用户名（最多 15 个字符）。名称区分大小写，必须是唯一的，且只能包含字母、数字、连字符和下划线。
身份验证配置文件	选择身份验证配置文件或序列对此管理员进行身份验证。有关详细信息，请参阅 Device（设备）> Authentication Profile（身份验证配置文件）或 Device（设备）> Authentication Sequence（身份验证序列）。
仅使用客户端证书身份验证 (Web)	选中此选项可对 Web 界面访问使用客户端证书身份验证。如果选择此选项，则无需设置用户名（**Name**（名称））和 **Password**（密码）。
密码/确认密码	输入并确认管理员的区分大小写的密码（最多 15 个字符）。为确保安全，Palo Alto Networks 建议管理员使用小写字母、大写字母和数字的组合形式定期更改其密码。请务必使用密码强度最佳实践确保密码的强度。 设备组和模板管理员不能访问 **Panorama** > **Administrators**（管理员）。要更改其本地密码，这些管理员必须单击其用户名（Web 界面底部 **Logout**（注销）旁边）。此方法同样适用于拥有自定义 Panorama 角色的管理员，其 **Panorama** > **Administrators**（管理员）访问权限已被禁用。 您可以将密码身份验证与身份验证配置文件（或序列）或本地数据库身份验证结合使用。 您可以设置密码到期参数，只需选择一个密码配置文件（请参阅 Device（设备）> Password Profiles（密码配置文件）），然后设置 Minimum Password Complexity（最小密码复杂性）参数（请参阅 Device（设备）> Setup（设置）> Management（管理）），但只能对 Panorama 本地验证的管理帐户设置此参数。
使用公钥身份验证(SSH)	选中此选项可使用 SSH 公钥身份验证：单击 **Import Key**（导入密钥），并浏览以选择公钥文件，然后单击 **OK**（确定）。“管理员”对话框显示在只读文本区域中上传的密钥。 支持的密钥文件格式为 IETF SECSH 和 OpenSSH。支持的密钥算法为 DSA（1024 位）和 RSA（768 - 4096 位）。 如果公钥身份验证失败，则 *Panorama* 提示输入登录名和密码。
管理员类型	类型选择可确定管理角色选项：

© 2019 Palo Alto Networks, Inc.

管理员帐户设置	说明
	• **Dynamic**（动态）— 可对 Panorama 和受管防火墙提供访问权限的角色。添加新功能时，Panorama 会自动更新动态角色的定义；您不需要手动更新这些角色。 • **Custom Panorama Admin**（自定义 **Panorama** 管理员）— 对于 Panorama 功能，拥有读写访问权限、只读访问权限或没有访问权限的可配置角色。 • **Device Group and Template Admin**（设备组和模板管理员）— 对于分配给为该管理员选择的访问域的设备组和模板的功能，拥有读写访问权限、只读访问权限或没有访问权限的可配置角色。

管理角色
（动态管理员类型）
	选择预定义角色：
	• 超级用户 — 对 Panorama 以及所有设备组、模板和受管防火墙都具有完全读写访问权限。
	• 超级用户（只读）— 对 Panorama 以及所有的设备组、模板和受管防火墙具有只读访问权。
	• **Panorama** 管理员 — 对 Panorama 具有完全访问权限，但以下操作除外：
	  • 创建、修改或删除 Panorama 或防火墙管理员及角色。
	  • 导出、验证、恢复、保存、加载或导入配置（**Device**（设备）> **Setup**（设置）> **Operations**（操作））。
	  • 在 **Panorama** 选项卡中配置 **Scheduled Config Export**（调度配置导出）。

配置文件 （Custom Panorama Admin（自定义 Panorama 管理员）管理员类型）	选择自定义 Panorama 角色（请参阅 Panorama > Managed Devices（受管设备）> Summary（摘要））。
访问域管理员角色 （设备组和模板管理员管理员类型）	对于您要分配给管理员的每个访问域（最多 25 个），从下拉列表中 **Add**（添加）一个 **Access Domain**（访问域）（请参阅 Panorama > Access Domains（访问域）），然后单击相邻的 Admin Role（管理员角色）单元格，从下拉列表中选择自定义设备组和模板管理员角色（请参阅 Panorama > Managed Devices（受管设备）> Summary（摘要））。当有权访问多个域的管理员登录 Panorama 时，**Access Domain**（访问域）下拉列表将出现在 Web 界面底部。管理员可以选择任何分配的访问域以过滤 Panorama 显示的监控和配置数据。选择的访问域还可过滤 **Context**（上下文）下拉列表显示的防火墙。 如果您使用 *RADIUS* 服务器对管理员进行身份验证，则必须将管理员角色和访问域映射到 RADIUS VSA。由于 *VSA* 字符串支持的字符数有限，因此如果您为管理员配置最大数量的访问域/角色对 *(25)*，则每个访问域和角色的名称值不得超过平均 *9* 个字符。
密码配置文件	选择一个密码配置文件（请参阅 Device（设备）> Password Profiles（密码配置文件））。

© 2019 Palo Alto Networks, Inc.

Panorama > Admin Roles（管理员角色）

管理员角色配置文件是定义管理员访问权限和责任的自定义角色。例如，分配给管理员的角色可以控制管理员可以生成的报告，以及管理员可以查看或更改的设备组或模板配置。

对于设备组和模板管理员，可以为分配给管理帐户的每个访问域分配单独的角色（请参阅 Panorama > Access Domains（访问域））。将角色映射到访问域，可让您极精细地控制管理员可以在 Panorama 上访问的信息。例如，假定您配置了一个访问域，其数据中心包含防火墙的所有设备组，您将此访问域分配给一个可监控数据中心流量，但不能配置防火墙的管理员。在这种情况下，您将访问域映射到特定角色，此角色拥有所有监控权限，但没有对设备组设置的访问权限。

要创建管理员角色配置文件，请添加配置文件，并按下表所述配置设置。

如果使用 *RADIUS* 服务器对管理员进行身份验证，请将管理员角色和访问映射到 RADIUS 供应商特定属性 (VSA)。

Panorama 管理员角色设置	说明
名称	输入名称以标识此管理员角色（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包含字母、数字、空格、连字符和下划线。
说明	（可选）输入角色的说明。
角色	选择管理职责范围：**Panorama** 或设备组和模板。
Web UI	从以下选项中进行选择，以设置 Panorama 上下文（**Web UI list**（**Web UI** 列表））和防火墙上下文（**Context Switch UI list**（上下文切换 **UI** 列表））中特定功能允许的访问类型： • **Enable**（启用）() — 读写访问 • **Read Only**（只读）() — 只读访问 • **Disable**（禁用）() — 禁止访问
XML API （仅限 Panorama 角色）	选择 Panorama 和受管防火墙的 XML API 访问类型（**Enable**（启用）或 **Disable**（禁用））： • **Report**（报告）— Panorama 和防火墙报告的访问权限。 • **Log**（日志）— Panorama 和防火墙日志的访问权限。 • **Configuration**（配置）— 检索或修改 Panorama 和防火墙配置的权限。 • **Operational Requests**（操作请求）— 在 Panorama 和防火墙上运行操作命令的权限。 • **Commit**（提交）— 提交 Panorama 和防火墙配置的权限。 • **User-ID Agent**（**User-ID** 代理）— User-ID 代理的访问权限。 • **Export**（导出）— 从 Panorama 和防火墙导出文件（如配置、阻止或响应页面、证书和密钥）的权限。 • **Import**（导入）— 将文件（如软件更新、内容更新、许可证、配置、证书、阻止页面和自定义日志）导入 Panorama 和防火墙的权限。
命令行 （仅限 Panorama 角色）	选择 CLI 访问的角色类型： • **None**（无）—（默认值）不允许访问 Panorama CLI。 • **Superuser**（超级用户）— 对 **Panorama** 拥有完全访问权限。

© 2019 Palo Alto Networks, Inc.

Panorama 管理员角色设置	说明

	• **Superreader**（超级读取器）— 对 **Panorama** 拥有只读访问权限。
	• **Panorama-admin**（**panorama** 管理员）— 除以下操作以外，对 **Panorama** 拥有完全访问权限：
	  • 创建、修改或删除 Panorama 管理员及角色。
	  • 导出、验证、恢复、保存、加载或导入配置。
	  • 调度配置导出。

REST API （仅限 Panorama 角色）	选择 Panorama 和受管防火墙应用至各个 REST API 端点的访问类型（**Enable**（启用）、**Read Only**（只读）或 **Disable**（禁用））。您可以将角色访问权限分配给下列类别中的端点。 • 对象 • 策略 • 网络 • 设备

© 2019 Palo Alto Networks, Inc.

Panorama > Access Domains（访问域）

访问域可控制设备组和模板管理员访问特定设备组（以管理策略和对象），访问模板（以管理网络和设备设置），访问受管防火墙的 Web 界面（通过上下文切换），以及受管防火墙的 REST API 所持有的访问权。您最多可定义 4,000 个访问域，并在本地或使用 RADIUS 供应商特定属性 (VSA)、TACACS+ VSA 或 SAML 属性对其进行管理。要创建访问域，请添加域，并按下表所述配置设置。

访问域设置	说明
名称	输入访问域的名称（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包含字母、数字、连字符和下划线。
共享对象	在从共享位置继承的此访问域中为设备组的对象选择下列访问权限之一。无论权限怎样，管理员都可以替代共享或默认（预定义）对象。 • 读 — 管理员可以显示和克隆共享对象，但不能对其执行任何其他操作。当添加非共享对象或克隆共享对象时，目标必须为访问域内的设备组，而不是共享对象。 • 写 — 管理员可以对共享对象执行所有操作。这是默认值。 • 仅共享 — 管理员只能添加要共享的对象。管理员还可以显示、编辑和删除共享对象，但不能移动或克隆。选择此选项的后果是管理员无法对非共享对象执行除显示以外的任何操作。
设备组	在访问域中启用或禁用特定设备组的读写访问权限。还可以单击全部启用或全部禁用。启用设备组的读写访问权限会自动为其后代设备组启用相同的访问权限。如果手动禁用后代设备组，则其最高祖先设备组的访问权限自动更改为只读。默认情况下，将会禁用所有设备组的访问权限。 如果想要列表只显示特定设备组，请选择此设备组的名称，然后选择 **Filter Selected**（已选择过滤）。 如果将共享对象的访问权限设置为 *shared-only*（仅共享），则 *Panorama* 会将只读访问权限应用于您为其指定读写访问权限的所有设备组。
模板	对于要分配的每个模板或模板堆栈，单击添加，然后从下拉列表中进行选择。
设备上下文 （对应于访问域页面中的设备/虚拟系统列）	选中管理员可切换上下文的防火墙以执行本地配置。如果防火墙列表太长，可以按设备状态、平台、设备组、模板、标记和高可用性状态进行过滤。
日志收集器组	对于要分配的每个收集器组，单击 **Add**（添加），然后从下拉列表中进行选择。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed Devices（受管设备）> Summary（摘要）

由 Panorama 管理的 Palo Alto Networks 防火墙称为受管设备。Panorama 可管理运行相同主要版本或更低主要版本的防火墙，但不可管理运行更高主要版本的防火墙。例如，运行 PAN-OS 10.0 的 Panorama 可以管理运行 PAN-OS 10.0 及更低版本的防火墙。此外，不建议管理运行比 Panorama 更高的维护版本的防火墙，因为这可能导致功能无法正常使用。例如，若 Panorama 运行 PAN-OS 10.0.0，则不建议管理运行 PAN-OS 10.0.1 或更高维护版本的防火墙。如需详细了解版本信息，请参阅 PAN-OS 10.0 发行说明。有关受支持 PAN-OS 版本的更多信息，请参阅生命周期结束摘要。

- 受管防火墙管理
- 受管防火墙信息
- 防火墙软件和内容更新
- 防火墙备份

受管防火墙管理

您可在防火墙上执行以下管理任务。

任务	说明
添加	**Add**（添加）防火墙，然后输入其序列号（每行一个）以将其添加作为受管设备。然后，**Managed Devices**（受管设备）窗口将显示受管防火墙信息，包括连接状态、已安装的更新以及初始配置期间设置的属性。 选中 **Associate Devices**（关联设备）以将防火墙与设备组或模板堆栈关联。 以 CSV 格式 **Import**（导入）由 Panorama 管理服务器管理的多个防火墙。提供 CVS 样本文件以供下载。 接下来，输入每个防火墙上 Panorama 管理服务器的 IP 地址（请参阅 Device（设备）> Setup（设置）> Management（管理）），以便 Panorama 可以管理防火墙。 通过带 *AES-256* 加密的 *SSL* 连接将防火墙注册到 *Panorama*。使用 *2,048* 位证书使 *Panorama* 和防火墙相互验证身份，再使用 *SSL* 连接进行配置管理和日志收集。
重新关联	将一个或多个选中防火墙重新分配给不同的设备组或模板堆栈。
删除	选中一个或多个防火墙，然后从 Panorama 管理的防火墙列表中 **Delete**（删除）。
标记	选中一个或多个防火墙，单击 **Tag**（标记），然后输入最多 31 个字符的文本字符串或选择现有标记。不要使用空格。但凡 Web 界面显示防火墙的长列表（如在安装软件的对话框中），标记即可提供一种用于筛选列表的方法。例如，您可使用名为“分支机构”的标记来筛选整个网络中的所有分支机构防火墙。
安装	**Install**（安装）防火墙软件或内容更新。
分组 HA 对端	如果您希望 **Managed Devices**（受管设备）页面对高可用性 (HA) 配置中的对端防火墙进行分组，可以选择 **Group HA Peers**（分组高可用性对端）。然后，您也可仅选择在各 HA 对中的各对端上均执行操作，或均不执行操作。

© 2019 Palo Alto Networks, Inc.

任务	说明
管理（备份）	**Manage**（管理）防火墙备份。
PDF/CSV	具有最小只读访问权限的管理角色可以将受管防火墙表格导出为 **PDF/CSV**。您可以应用筛选程序来创建更多特定的表格配置输出，以用于审计等事宜。将仅导出 Web 界面中所显示的列。请参阅配置表格导出。
部署主密钥	部署一个新主密钥，或是更新一个或多个设备的现有主密钥。

受管防火墙信息

选择 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）可显示每个受管防火墙的下列信息。

受管防火墙信息	说明
设备组	显示成员防火墙中的设备组的名称。默认情况下，此列已隐藏，但可以通过在任何列标头中选择下拉列表并选择 **Columns**（列）> **Device Group**（设备组）来显示。 该页面会根据其设备组显示集群中的防火墙。每个集群都拥有一个标头行，用于显示设备组名称、分配防火墙的总数、连接防火墙的数量和层次结构中的设备组路径。例如，数据中心（已连接 **4** 个设备中的 **2** 个）：> **Shared**（共享）> **Europe**（欧洲）Data center（数据中心）将表示名为 **Data center**（数据中心）的设备组拥有四个成员防火墙（已连接其中两个），且为名为 **Europe**（欧洲）的设备组的子设备组。可以折叠或展开任何设备组以隐藏或显示其防火墙。
设备名称	显示防火墙的主机名或序列号。 对于 VM 系列 NSX 版防火墙，防火墙名称将附加 ESXi 主机的主机名。例如，PA-VM：Host-NY5105
虚拟系统	列出处于多虚拟系统模式下的防火墙上可用的虚拟系统。
模型	显示防火墙型号。
标记	显示为每个防火墙/虚拟系统定义的标记。
序列号	显示防火墙的序列号。
操作模式	显示防火墙的操作模式。可能为 FIPS-CC 或 Normal（正常）。
IP 地址	显示防火墙/虚拟系统的 IP 地址。
	IPv4 — 显示防火墙/虚拟系统的 IPv4 地址。
	IPv6—显示防火墙/虚拟系统的 IPv6 地址。
变量	通过从模板堆栈中的设备复制设备特定的变量定义来创建设备特定的变量定义，或编辑现有变量定义以为设备创建唯一变量。如果设备未与模板堆

© 2019 Palo Alto Networks, Inc.

受管防火墙信息	说明
	栈关联，则此列将为空。默认情况下，变量从模板堆栈继承。请参阅在设备上创建或编辑变量定义。
模板	显示已向其分配防火墙的模板堆栈。
状态	**Device State**（设备状态）— 表示 Panorama 和防火墙之间的连接状态：连接或断开连接。 VM 系列防火墙可以拥有其他两种状态： • **Deactivated**（停用）— 表示您已直接在防火墙上或通过选择 **Deactivate VMs**（停用 **VM**）（**Panorama** > **Device Deployment**（设备部署）> **Licenses**（许可证））停用了虚拟机，且已删除了防火墙上的所有许可证和授权。已停用的防火墙不再连接到 Panorama，因为停用过程已删除 VM 系列防火墙的序列号。 • **Partially deactivated**（部分停用）— 表示您已从 Panorama 启动许可证停用过程，但该过程未全部完成，因为防火墙处于离线状态且 Panorama 无法与其通信。
	HA Status（高可用性状态）— 表示防火墙可能处于以下状态： • **Active**（主动）— 正常的流量处理操作状态 • **Passive**（被动）— 正常备份状态 • **Initiating**（正在启动）— 防火墙将在重启后处于此状态，且时长不超过 60 秒 • **Non-functional**（无功能）— 错误状态 • **Suspended**（挂起）— 管理员已禁用此防火墙 • **Tentative**（试验）— 适用于主动/主动配置中的链接或路径监控事件
	Shared Policy（共享策略）— 表示防火墙上的策略和对象配置是否与 Panorama 同步。
	Template（模板）— 表示防火墙上的网络和设备配置是否与 Panorama 同步。
状态（续）	**Certificate**（证书）— 表示受管设备的客户端证书状态。 • **Pre-defined**（预定义）— 受管设备正在使用预定义证书对 Panorama 进行身份验证。 • **Deployed**（已部署）— 在受管设备上已成功部署自定义证书。 • **Expires in N days N hours**（在 **N** 天 **N** 小时后过期）— 目前安装的证书将在 30 天内过期。 • **Expires in N minutes**（在 **N** 分钟后过期）— 目前安装的证书将在一天内过期。 • **Client Identity Check Passed**（客户端标识检查已通过）— 证书通用名称与连接设备的序列号相匹配。 • **OCSP Status Unknown**（**OCSP** 状态未知）— Panorama 无法从 OCSP 响应者获取 OCSP 状态。 • **OCSP Status Unavailable**（**OCSP** 状态不可用）— Panorama 无法联系 OCSP 响应者。 • **CRL Status Unknown**（**CRL** 状态未知）— Panorama 无法从 CRL 数据库响应者获取吊销状态。

© 2019 Palo Alto Networks, Inc.

受管防火墙信息	说明
	• **CRL Status Unavailable**（**CRL** 状态不可用）— Panorama 无法连接 CRL 数据库。
	• **OCSP/CRL Status Unknown**（**OCSP/CRL** 状态未知）— 当两者都启用时，Panorama 无法获取 OCSP 或吊销状态。 • **OCSP/CRL Status Unavailable**（**OCSP/CRL** 状态不可用）— 当两者都启用时，Panorama 无法连接 OCSP 或 CRL 数据库。 • **Untrusted Issuer**（不可信颁发者）— 受管设备拥有自定义证书，但服务器未对其进行验证。 **Last Commit State**（最后提交状态）— 表示防火墙上的最后提交是否成功。
软件版本 | 应用程序和威胁 | 防病毒软件 | URL 筛选 | GlobalProtect™ 客户端 | WildFire	显示防火墙上目前安装的软件和内容版本。有关详细信息，请参阅防火墙软件和内容更新。
备份	在各次防火墙提交期间，PAN-OS 会自动将防火墙配置备份发送到 Panorama。单击 **Manage**（管理）可查看可用的配置备份，然后视情况选择加载。有关详细信息，请参阅防火墙备份。
最后一次主密钥推送	显示从 Panorama 部署到防火墙的主密钥状态。
	状态 — 显示最近一次主密钥推送状态。可以是 `Success` 或 `Failed`。如果未将主密钥从 Panorama 推送到防火墙，则显示 `Unknown`。
	时间戳 — 显示最近一次从 Panorama 推送主密钥的日期和时间。
容器 — 如果部署 CN 系列防火墙来保护 Kubernetes 集群上容器化应用程序工作负载，请使用以下列。	
容器节点数	显示与注册到 Panorama 的管理平面 (CN-Mgmt) 连接的容器化防火墙数据平面 (CN-NGFW) 数量。 对于每对 CN-Mgmt pod，该值可以是 0—30 个 CN-NGFW pod。
容器说明	未来使用

创建设备变量定义

首次将设备添加到模板堆栈时，您可以选择创建从模板堆栈中的设备复制的设备特定的变量定义，也可以通过 **Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要）编辑模板变量定义。默认情况下，所有变量定义都从模板堆栈继承而来，并且只能替代各个设备的变量定义，而不能删除这些定义。您可以使用变量来替换配置的所有区域中的 IP 地址对象和 IP 地址文字（IP 网络掩码、IP 范围、FQDN）、IKE 网关配置（接口）中的接口和 HA 配置（组 ID）。

创建设备变量定义信息	说明
是否从模板堆栈中的其他设备克隆设备变量定义？	
否	查看现有的变量定义并根据需要进行编辑。请参阅 Panorama > Templates（模板）> Template Variables（模板变量）。

© 2019 Palo Alto Networks, Inc.

创建设备变量定义信息	说明
是	在下拉列表中选择要从中克隆变量定义的设备，然后选择要克隆的特定变量定义。

防火墙软件和内容更新

要在受管防火墙上安装软件或内容更新，请先使用 **Panorama** > **Device Deployment**（设备部署）页面下载或上传 Panorama 更新。然后，选择 **Panorama** > **Managed Devices**（受管设备），单击 **Install**（安装），并填写以下字段。

要减少管理 *(MGT)* 接口的流量，您可以配置 *Panorama* 使用单独的接口部署更新（请参阅 Panorama > Setup（设置）> Interfaces（接口））。

防火墙软件/内容更新安装选项	说明
类型	选择要安装的更新类型：PAN-OS 软件、**GlobalProtect** 客户端软件、应用程序和威胁签名、防病毒软件签名、**WildFire** 或 **URL** 过滤。
文件	选择更新映像。下拉列表仅列出使用 **Panorama** > **Device Deployment**（设备部署）页面下载或上传到 Panorama 的映像。
过滤器	选择过滤器以过滤设备列表。
设备	选择要安装映像的防火墙。
设备名称	防火墙名称。
当前版本	当前已在防火墙上安装的选定 **Type**（类型）的更新版本。
HA 状态	表示防火墙可能处于以下状态： • **Active**（主动）— 正常的流量处理操作状态 • **Passive**（被动）— 正常备份状态 • **Initiating**（正在启动）— 防火墙将在重启后处于此状态，且时长不超过 60 秒 • **Non-functional**（无功能）— 错误状态 • **Suspended**（挂起）— 管理员已禁用此防火墙 • **Tentative**（试验）— 适用于主动/主动配置中的链接或路径监控事件
分组 HA 对端	选中此选项可对高可用性 (HA) 配置的对端防火墙分组。
过滤器已选择	如果您要使设备列表只显示特定防火墙，可以选择相应的设备名称，然后选择 **Filter Selected**（已选择过滤）。
仅上传到设备	选择此选项可在防火墙上上传映像，但不会自动重新启动防火墙。映像将在您手动重启防火墙时完成安装。
安装后重启设备（仅限软件）	选择此选项可上传并安装软件映像。安装过程会触发重新启动。

© 2019 Palo Alto Networks, Inc.

防火墙软件/内容更新安装选项	说明
在内容更新中禁用新应用程序（仅限应用程序和威胁）	选中此选项，可在更新中禁用相对于上次安装的更新是新应用程序的应用程序。这不仅能防止最新威胁的攻击，还能确保您在准备任何策略更新后启用应用程序的灵活性。然后，要启用应用程序，请登录到防火墙，选择 **Device**（设备）> **Dynamic Updates**（动态更新），单击 Features（功能）列中的 **Apps**（应用程序）以显示新应用程序，然后单击要启用的各应用程序的 **Enable/Disable**（启用/禁用）。

防火墙备份

- Panorama > 受管设备

Panorama 将自动备份提交至受管防火墙的每一个配置更改。要管理防火墙的备份，请选择 **Panorama** > **Managed Devices**（受管设备），单击防火墙 Backups（备份）列中的 **Manage**（管理），然后执行以下任务中的任一项。

要配置 *Panorama* 存储的防火墙配置备份的数量，请选择 *Panorama* > *Setup*（设置）> *Management*（管理），编辑 *Logging and Reporting Settings*（记录和报告设置），选择 *Log Export and Reporting*（日志导出和报告）选项卡，然后输入 *Number of Versions for Config Backups*（配置备份的版本数）（默认为 *100*）。

任务	说明
显示有关已保存或已提交配置的详细信息。	在备份的 Version（版本）列中，单击已保存配置的文件名或已提交配置的版本号，以显示相关 XML 文件的内容。
将已保存或已提交配置恢复到待选配置。	在备份的 Action（操作）列中，单击 **Load**（加载），再单击 **Commit**（提交）。 加载防火墙配置将恢复本地设备配置，而不是恢复从 Panorama 推送的配置。**Load**（加载）防火墙备份后，必须对防火墙 Web 接口执行上下文切换或启动防火墙 Web 接口以 **Commit**（提交）。
删除已保存的配置。	在已保存备份的 Action（操作）列中，单击 Delete（删除）（ ✕ ）。

Panorama > Device Quarantine（设备隔离）

Panorama > **Device Quarantine**（设备隔离）页面显示隔离列表中的设备。设备会因下列操作出现在该列表中：

- 系统管理员手动添加设备到该列表。

  若要手动 **Add**（添加）设备，请输入您想隔离的设备的 **Host ID**（主机 **ID**）和 **Serial Number**（序列号）（可选）。
- 系统管理员从流量、GlobalProtect 或威胁日志中选择主机 ID 列，从该列中选择设备，然后选择 **Block Device**（阻止设备）。
- 设备与拥有日志转发配置文件的安全策略规则匹配，且该配置文件的匹配列表具有已设为 **Quarantine**（隔离）的内置操作。

主机 *ID* 自动显示在 *GlobalProtect* 日志中。对于要显示在流量、威胁或统一日志中的主机 *ID*，*Panorama* 设备必须至少有一个将*Source Device*（源设备）设为 *Quarantine*（隔

© 2019 Palo Alto Networks, Inc.

离）的安全策略规则。如果未在安全策略中执行此设置，“流量”、“威胁”或“统一”日志就没有主机 *ID*，且日志转发配置文件也不会生效。

- 使用 API 添加设备到隔离列表。
- Panorama 设备将隔离列表作为重新分发条目的一部分接收（从另一个 Panorama 设备或防火墙重新分发隔离列表）。

设备隔离表包含以下字段。

字段	说明
主机 ID	被阻止主机的主机 ID。
原因	设备被隔离的原因。原因**Admin Add**（管理员添加）意味着管理员自动添加设备到表格。
时间戳	管理员或安全策略规则添加设备到隔离列表的时间。
源设备/应用程序	添加设备到隔离列表的 Panorama、防火墙或第三方应用程序的 IP 地址。
序列号	（可选）隔离设备的序列号（如有）。
用户名	（可选）在设备隔离时登录到设备的 GlobalProtect 客户端用户的用户名。

Panorama > Managed Devices（受管设备）> Health（运行状况）

Panorama™ 允许您监控受管防火墙的硬件资源和性能。Panorama 将时间趋势性能信息（CPU、内存、CPS 和吞吐量）、日志记录性能、环境信息（如风扇、RAID 状态和电源）集中到一起，并将事件（如提交、内容安装和软件升级）与运行状况数据关联。如果防火墙偏离其计算得出的基线，Panorama 会将其报告为偏离设备，以帮助快速标识、诊断和解决任何硬件问题。

您可以使用此页面来：

查看详细的设备运行状况。	查看由 Panorama 管理的设备的运行状况度量标准。
分组 HA 对端	查看哪些防火墙被组合在一起以帮助标识潜在问题，并确定哪些防火墙受到任何硬件资源或性能问题的影响。
PDF/CSV	具有最小只读访问权限的管理角色可以 **PDF/CSV** 格式导出受管防火墙表格。您可以根据需要应用筛选程序来创建更多特定的表格配置输出，以用于审计等事宜。仅导出了 Web 界面中所显示的列。请参阅导出配置表格数据。

Panorama > Managed Devices（受管设备）> *Health*（运行状况）> *All Devices*（所有设备）

使用此页面来查看每个防火墙的以下信息。

© 2019 Palo Alto Networks, Inc.

运行状况信息	说明
设备名称	防火墙的主机名或序列号。 对于 VM 系列 NSX 版防火墙，防火墙名称将附加 ESXi 主机的主机名。例如，PA-VM：Host-NY5105
型号	防火墙的型号。
设备	
吞吐量 (Kbps)	一段时间（平均五分钟）内的数据吞吐量，以千字节每秒为单位。
CPS	一段时间（平均五分钟）内防火墙的每秒总连接数。
会话	
计数（会话）	一段时间（平均五分钟）内的总会话数。
数据层面	
CPU (%)	数据面板的总 CPU 利用率。
管理层面	
CPU (%)	管理面板的总 CPU 利用率。
MEM (%)	管理面板的总内存利用率。
日志记录速率（每秒日志数）	防火墙将日志转发到 Panorama 或日志收集器的速率（平均一分钟）。
风扇	显示每个风扇托盘中风扇的存在、当前状态、RPM 和上一次故障。风扇状态显示为 *A*/*B*，其中 *A* 表示正常运行的风扇数量，*B* 表示防火墙上的风扇总数。虚拟防火墙显示 `N/A`。
电源	显示存在、当前状态和上一次故障时间戳。电源状态显示为 *A*/*B*，其中 *A* 表示正常运行的电源数量，*B* 表示设备上的电源总数。虚拟防火墙显示 `N/A`。
端口	防火墙上所用的端口总数。端口显示为 *A*/*B*，其中 *A* 表示正常运行的端口数量，*B* 表示设备上的端口总数。

Panorama > *Managed Devices*（受管设备）> *Health*（运行状况）> *Deviating Devices*（偏离设备）

偏离设备选项卡显示具有任何偏离其计算得出的基线的度量标准的设备，并将这些偏差度量标准显示为红色。度量标准运行状况基线根据 7 天内按给定度量标准计算得出的运行状况性能平均值加上标准偏差来确定。

© 2019 Palo Alto Networks, Inc.

All Devices | Deviating Devices

4 it

	DEVICE NAME	MODEL	HA STATUS	Device		Session	Data Plane	Management Plane		LOGGING RATE (LOG/SEC)	FANS	POWE SUPPL
				THROUGHPUT (KBPS)	CPS	COUNT (SESSIONS)	CPU (%)	CPU (%)	MEM (%)			
	PA-7080	PA-7080		24117127	100992	23368878	30	18	13	0	18/18	2/8
	[illegible]	PA-5220	Active Primary	0	0	0	0	13	14	0	8/8	2/2
	[illegible]	PA-5220	Active Secondary	1	0	0	0	1	10	0	8/8	2/2
	PA-3260	PA-3260		8999	12658	63772	7	22	23	11329	3/3	2/2

图 **1:** 偏差度量标准示例

Panorama 中的详细设备运行状况

您可以通过在所有设备选项卡或偏离设备选项卡中单击设备名称来查看各个防火墙的详细设备运行状况历史记录。详细设备视图使用时间筛选程序提供运行状况历史记录，并显示与设备关联的元数据。设备运行状况信息以表格或小部件形式显示，以尽可能提供时间趋势数据的图形表示。

管理详细设备视图

除了与防火墙关联的描述性元数据外，详细设备视图还显示详细的防火墙运行状况信息。在适用的情况下，您可以配置小部件其他选项的设置 (⚙) 或最大化面板 (⊡) 以放大小部件。

字段	说明
操作	
时间筛选程序	选择时间筛选程序可从下拉列表中查看设备运行状况历史记录。您可以选择 **Last 12 hours**（过去 **12** 小时）、**24 hours**（**24** 小时）、**7 days**（**7** 天）、**15 days**（**15** 天）、**30 days**（**30** 天）或 **90 days**（**90** 天）。
显示平均值	选择所有时间趋势小部件上显示的平均分布和标准分布。您可以选择 **None**（无）、**Last 24 hours**（过去 **24** 小时）、**7 days**（**7** 天）或 **15 days**（**15** 天）。
刷新	用最新数据刷新显示的信息。
打印 PDF	生成当前显示的选项卡的 PDF。 您需要启用弹出窗口才能选择下载位置并访问 *PDF*。
系统信息	
系统信息	与设备关联的元数据：IP 地址、软件版本、防病毒软件版本、HA 状态、序列号、应用程序和威胁版本、Wildfire 版本、VSYS 模式、型号和设备模式。

会话

会话选项卡显示穿过防火墙的会话信息。此信息显示为六个独立图形。

© 2019 Palo Alto Networks, Inc.

字段	说明
吞吐量	一段时间（平均五分钟）内的数据吞吐量，以千比特每秒 (Kbps) 为单位。
会话计数	一段时间（平均五分钟）内的总会话数。
每秒连接数	一段时间（平均五分钟）内的设备总 CPS。
每秒数据包数	通过设备的每秒总数据包数（平均超过五分钟）。
全局会话表利用率（仅限 PA-7000 和 PA-5200 设备）	具有全局会话表的防火墙在一段时间（平均超过五分钟）内的全局会话表百分比。
会话表利用率	显示防火墙的每个数据平面的会话表使用量随时间（平均超过五分钟）变化的百分比。
SSL 解密的会话信息	显示一段时间（平均超过五分钟）内解密的 SSL 会话数。
SSL 代理会话利用率	显示一段时间（平均超过五分钟）内的代理会话使用百分比。

环境

Environments（环境）选项卡显示硬件（如电源、风扇托架和磁盘驱动器）的存在、状态和运行状况。此选项卡仅显示基于硬件的防火墙的以下项：

字段	说明
风扇状态	显示每个风扇托盘中风扇的存在、当前状态、RPM 和上一次故障。风扇状态显示为 *A*/*B*，其中 *A* 表示正常运行的风扇数量，*B* 表示防火墙上的风扇总数。虚拟防火墙显示 `N/A`。
电源	显示存在、当前状态和上一次故障时间戳。电源状态显示为 *A*/*B*，其中 *A* 表示正常运行的电源数量，*B* 表示设备上的电源总数。虚拟防火墙显示 `N/A`。
热状态	显示是否有与设备的每个插槽关联的任何热警报。如果存在活动警报，防火墙还会在此显示有关确切温度和位置的更多具体信息。
系统磁盘状态	显示 root、pancfg、panlogs 和 panrepo 挂载的可用、已用和利用百分比。 系统磁盘状态还显示启用 RAID 的防火墙的磁盘名称、大小和 RAID 状态。

接口

接口选项卡显示防火墙上所有物理接口的状态和统计信息。

© 2019 Palo Alto Networks, Inc.

字段	说明
接口名称	接口的名称。选择接口可查看所选接口的比特率、每秒数据包数、错误数和丢弃数图表。
STATUS（状态）	接口的状态：AdminUp（管理员开启）、Admin Down（管理员关闭）、OperationalUp（操作启动）或 Operational Down（操作关闭）。
比特率	显示接收和传输数据的比特率 (bps)。
每秒数据包数	显示接收和传输数据的每秒数据包数。
错误	显示接收和传输数据的错误数。
丢弃数	显示接收和传输数据的丢弃连接数。

记录

日志记录选项卡显示各管理防火墙的日志记录速率和连接。

字段	说明
日志记录速率	显示设备将日志转发到 Panorama 或日志收集器的每分钟平均速率。
日志记录连接	显示所有可用的日志转发连接，包括其活动状态或非活动状态。
外部日志转发	显示各种外部日志转发方法的发送、丢弃和平均转发速率（每秒日志数）。

资源

资源选项卡显示防火墙的 CPU 和内存统计信息。

字段	说明
管理面板内存	以百分比形式显示管理面板内存的时间趋势五分钟平均值。
数据包缓冲区	以百分比形式显示数据包缓冲区利用率的时间趋势五分钟平均值。在多数据平面系统中，此显示包括不同颜色的各种数据平面、CPU 和数据包缓冲区。
数据包描述符	以百分比形式显示数据包描述符利用率的时间趋势五分钟平均值。在多数据平面系统中，此显示包括不同颜色的各种数据平面、CPU 和数据包缓冲区。
CPU 管理面板	显示管理面板 CPU 的时间趋势五分钟平均值。
CPU 数据平面	显示数据平面 CPU 的时间趋势五分钟平均每核利用率。对于具有多个数据平面的系统，您可以选择要查看选择器的数据平面。

© 2019 Palo Alto Networks, Inc.

字段	说明
安装	显示设备系统文件信息。此显示包括安装名称、获分配 (KB) 空间、已用 (KB) 空间和可用 (KB) 空间以及利用百分比。

高可用性

高可用性选项卡显示防火墙及其 HA 对端的 HA 状态。顶部小部件显示设备及其对端的配置和内容版本。底部小部件提供有关先前 HA 故障转移的信息以及与之相关的原因，包括出现故障的防火墙。

© 2019 Palo Alto Networks, Inc.

Panorama > Templates（模板）

通过 **Device**（设备）和 **Network**（网络）选项卡，可以使用模板或模板堆栈（模板的组合）将常用基本配置部署到需要相似设置的多个防火墙。使用 Panorama 管理防火墙配置时，可以使用设备组（管理共享策略和对象）和模板（管理共享设备和网络设置）的组合。

除对话框中提供的创建模板或模板堆栈的设置以外，**Panorama** > **Templates**（模板）还会显示以下列：

- **Type**（类型）— 将所列条目识别为模板或模板堆栈。
- **Stack**（堆栈）— 列出分配到模板堆栈的模板。

您想做什么？	请参阅：
添加、克隆、编辑或删除模板	模板
添加、克隆、编辑或删除模板堆栈	模板堆栈
了解更多？	模板和模板堆栈
	管理模板和模板堆栈

模板

Panorama 最多支持 1,024 个模板。可以 **Add**（添加）模板并按下表所述配置设置。创建模板后，您还需要配置模板堆栈并将模板和防火墙添加到模板堆栈中才能管理防火墙。在配置模板之后，您必须在 Panorama 中提交自己的更改（请参阅 Panorama 提交操作）。

删除模板不会删除 *Panorama* 已推送到防火墙的值。

模板设置	说明
名称	输入模板名（最多 31 个字符）。名称区分大小写，必须是唯一的，只能包含字母、数字、空格、连字符、句点和下划线。 此名称将显示在 **Template**（模板）下拉列表的 **Device**（设备）和 **Network**（网络）选项卡中。在这些选项卡中修改的设置仅适用于选定模板。
说明	输入模板的说明。

模板堆栈

可以配置模板堆栈或将模板分配给模板堆栈。将防火墙分配给模板堆栈允许您将所有必要的设置推送到防火墙，而不是将每个设置单独添加到每个模板。Panorama 最多支持 1,024 个堆栈。可以 **Add Stack**（添加堆栈）以创建新的模板堆栈并按下表所述配置设置。在配置模板堆栈之后，您必须在 Panorama 中提交自己的更改（请参阅 Panorama 提交操作）。此外，配置分配到堆栈的防火墙的网络和设备设置后，您必须执行模板提交并将设置推送到防火墙。

删除模板堆栈或者从模板堆栈删除防火墙不会删除 *Panorama* 之前推送到该防火墙的值；但是，当您从模板堆栈删除防火墙时，*Panorama* 不再向该防火墙推送新的更新。

© 2019 Palo Alto Networks, Inc.

模板堆栈设置	说明
名称	输入堆栈名称（最多 31 个字符）。名称区分大小写，必须是唯一的并以字母为开头，且只能包含字母、数字和下划线。在 **Device**（设备）和 **Network**（网络）选项卡中，**Template**（模板）下拉列表将显示堆栈名称及其指定模板。
说明	输入堆栈的说明。
模板	**Add**（添加）每个您要加入堆栈的模板（最多 8 个）。 如果模板包含重复设置，Panorama 只会将列表中推送设置优先级较高的模板的设置推送到指定防火墙。例如，如果列表中 Template_A 的优先级高于 Template_B，且两个模板都定义 ethernet1/1 接口，则 Panorama 将从 Template_A 而不从 Template_B 推送 ethernet1/1 定义。要更改模板在列表中的顺序，请选择模板，然后 **Move Up**（上移）或 **Move Down**（下移）。 *Panorama* 不会验证堆栈中的模板组合，因此，请对模板进行排序以避免无效关系。
设备	选择要添加到堆栈的各个防火墙。 如果防火墙列表太长，可以按 **Platforms**（平台）、**Device Groups**（设备组）、**Tags**（标记）和 **HA Status**（**HA** 状态）筛选列表。 您可以将配备非匹配模式（*VPN* 节点、多虚拟系统模式或操作模式）的防火墙分配到相同的堆栈。*Panorama* 只将模式特定的设置推送到支持这些模式的防火墙。
全选	选中列表中的每个防火墙。
取消全选	取消选中列表中的每个防火墙。
分组 HA 对端	对属于高可用性 (HA) 对的防火墙进行分组。此选项可让您轻松确定拥有高可用性配置的防火墙。从模板堆栈推送模板设置时，您可将其推送到已分组的对端，而不是逐个推送到每个防火墙。
过滤器已选择	要仅显示特定防火墙，则可选中防火墙，然后选中 **Filter Selected**（已选择过滤器）。

Panorama > Templates（模板）> Template Variables（模板变量）

- 创建新的模板变量
- 编辑现有模板变量
- 在设备上创建或编辑变量定义

您可以为模板和模板堆栈定义变量（**Panorama** > **Templates**（模板）），或者可以编辑单个设备的现有变量（**Panorama** > **Managed Devices**（受管设备）> **Summary**（摘要））。变量是在模板或模板堆栈上定义的可在您使用 Panorama 管理防火墙配置时提供灵活性和可重用性的配置组件。您可以使用变量来替换：

- 配置的所有区域中的 IP 地址（包括 IP 网络掩码、IP 范围和 FQDN）。
- IKE 网关配置（接口）和 HA 配置（组 ID）中的接口。
- SD-WAN 配置中的配置元素（AS 号、QoS 配置文件、最大出口、链路标签）。

将防火墙添加到模板堆栈时，它们会自动继承您为模板或模板堆栈创建的变量。

© 2019 Palo Alto Networks, Inc.

模板变量信息	说明
名称	变量定义的名称。
模板（设备和模板堆栈）	显示变量定义所属模板的名称。
类型	显示变量定义的类型： • **IP Netmask**（**IP** 网络掩码）— 定义静态 IP 或网络地址。 • **IP Range**（**IP** 范围）— 定义 IP 范围。例如，192.168.1.10-192.168.1.20。 • **FQDN** — 定义完全限定域名。 • **Group ID**（组 **ID**）— 定义高可用性组 ID。有关更多信息，请参阅主动/被动 HA 配置指南。 • **Device Priority**（设备优先级）— 定义设备优先级以指示防火墙应在主动-被动高可用性 (HA) 配置中承担主动角色的首选项。 • **Device ID**（设备 **ID**）— 定义用于在主动-主动高可用性 (HA) 配置中分配设备优先级值的设备 ID。 • **Interface**（接口）— 定义防火墙上的防火墙接口。只能用于 IKE 网关配置。 • **AS Number**（**AS** 号）— 定义在 BGP 配置中使用的自治系统编号。 • **QoS Profile**（**QoS** 配置文件）— 定义在 QoS 配置中使用的服务质量 (QoS) 配置文件。 • **Egress Max**（最大出口）— 定义 QoS 配置文件配置中使用的最大出口值。 • **Link Tag**（链路标签）— 定义 SD-WAN 配置中使用的链路标签。
值	显示所配置的变量定义值。
添加（模板和模板堆栈）	添加新的模板变量定义。
删除	删除现有模板变量定义。
克隆	克隆现有模板变量定义。
替代（模板堆栈和设备）	替代从模板堆栈或设备继承的现有模板变量定义。您无法更改变量类型和名称，也无法替代设备特定的变量。
恢复（模板堆栈和设备）	要清除模板堆栈或设备级别的任何替代值，请将替代变量恢复为其原始模板变量定义。
仅获取设备上使用的值（仅限设备）	用防火墙上使用的值填充所选变量。需要定义模板或模板堆栈变量并将其推送到防火墙，Panorama 才能检索值。从防火墙获取的值将 **Override**（替代）模板或模板堆栈变量，以创建设备特定的变量。如果未将任何变量定义推送到防火墙，Panorama 将返回找不到该变量的值。

创建新的模板变量

Add（添加）新的模板变量定义。

© 2019 Palo Alto Networks, Inc.

新的模板变量定义信息	说明
名称	给变量定义命名。所有变量定义名称都必须以美元符号 (“$”) 字符为开头。
类型	选择变量定义的类型：**IP Netmask**（**IP** 网络掩码）、**IP Range**（**IP** 范围）、**FQDN**、**Group ID**（组 **ID**）、 **Device Priority**（设备优先级）、**Device ID**（设备 **ID**）、**Interface**（接口）、**AS Number**（**AS** 号）、**QoS Profile**（**QoS** 配置文件）、**Egress Max**（最大出口）或 **Link Tag**（链路标签）。
值	输入所需的变量定义值。

编辑现有模板变量

您可以在创建变量后的任何时间编辑模板或模板堆栈的模板变量定义（**Panorama** > **Templates**（模板））。**Manage**（管理）模板变量以选择变量并根据需要编辑可用值。

在设备上创建或编辑变量定义

转到 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要）以创建变量定义或替代从 Panorama 模板或模板堆栈推送的模板变量。模板变量包括：

- 配置的所有区域中的 IP 地址（IP 网络掩码、IP 范围或 FQDN）。
- IKE 网关配置（接口）或 HA 配置（组 ID）中的接口。
- SD-WAN 配置中的配置元素（AS 号、QoS 配置文件、最大出口、链路标签）。

创建设备变量允许您从同一模板堆栈中的设备复制替代的设备特定变量，而不是单独重新创建设备变量。默认情况下，所有变量定义都从模板或模板堆栈继承而来，您只能替代它们，而不能删除各个设备的变量定义，也不能为各个设备创建新的变量定义。

通过从模板堆栈中的现有设备复制变量定义或者 **Edit**（编辑）现有设备变量定义来 **Create**（创建）设备变量定义。

© 2019 Palo Alto Networks, Inc.

Panorama > Device Groups（设备组）

设备组包含要作为组加以管理的防火墙和虚拟系统，如管理公司中一组分支机构或单个部门的防火墙。在应用策略时，Panorama 将这些组视为一个单元。防火墙只能属于一个设备组，但由于虚拟系统在 Panorama 中是不同的实体，因此可以将防火墙内的虚拟系统分配到不同的设备组。

您可在共享位置下多达四个级别的树形层次结构中嵌套设备组，以实施分层方法来管理整个防火墙网络的策略。在底层级别中，设备组在依次更高的级别中可以拥有父级、祖父级和曾祖父级设备组（统称为父对象），底层级别设备组可从父对象中继承策略和对象。在顶层级别中，设备组可以拥有子级、孙级和曾孙级设备组 — 统称后代。在选择 **Panorama** > **Device Groups**（设备组）后，Name（名称）列将显示此设备组的层次结构。

添加、编辑或删除设备组后，可执行 Panorama 提交和设备组提交（请参阅 Panorama 提交操作）。之后，Panorama 可将配置更改推送到分配给设备组的防火墙；Panorama 最多支持 1,024 个设备组。

要配置设备组，请添加一个设备组，并按下表所述配置设置。

设备组设置	说明
名称	输入名称以标识组（最多 31 个字符）。名称区分大小写，在整个设备组层次结构中必须是唯一的，且只能包含字母、数字、空格、连字符和下划线。
说明	输入设备组的说明。
设备	选择要添加到设备组的各个防火墙。如果防火墙列表太长，可以按设备状态、平台、模板或标记进行过滤。过滤器部分显示（在括号中）每个类别的受管设备的数量。 如果设备组仅用于组织用途（即要包含其他设备组），则不需要为其分配防火墙。
全选	选中列表中的每个防火墙和虚拟系统。
取消全选	取消选中列表中的每个防火墙和虚拟系统。
分组 HA 对端	选中此选项可对高可用性 (HA) 配置的对端防火墙分组。然后，该列表首先会在括号中显示主动（或主动/主动配置中的主动-主要）防火墙和被动（或主动/主动配置中的主动-辅助）防火墙。这可让您轻松确定处于高可用性模式下的防火墙。推送共享策略时，可以推送到分组的对，而不是单个对端。 对于主动/被动配置中的高可用性对，可以考虑将两个防火墙或其虚拟系统添加到同一设备组。这可让您将配置同时推送到两个对端。
过滤器已选择	如果您要使设备列表只显示特定防火墙，可以选中防火墙，然后选中 **Filter Selected**（已选择筛选）。
父设备组	相对于您所定义的设备组，选择在层次结构中正好在其上方的设备组（或共享位置）（默认为 **Shared**（共享））。
主设备	要根据用户名和用户组配置策略规则和报告，必须选择一个主设备。此设备是防火墙，Panorama 可接收此防火墙发送的用户名、用户组名称和用户名到用户组的映射信息。

© 2019 Palo Alto Networks, Inc.

设备组设置	说明
	在更改主设备或将其设置为 *None*（无）时，*Panorama* 会丢失从该防火墙接收的所有用户和用户组信息。
存储主设备所发送的用户和用户组	只有在选择特定主设备时，才显示此选项。此选项可让 Panorama 在本地存储从主设备收到的用户名、用户组名称和用户名到用户组的映射信息。要启用本地存储，还必须选择 **Panorama** > **Setup**（设置）> **Management**（管理），编辑 Panorama 设置，然后对组启用报告和筛选功能。
动态添加设备属性 — 在为设备组添加新设备后，Panorama 会将指定授权码和 PAN-OS 软件版本动态应用到新设备。只有在特定设备组与 Panorama 中的 NSX 服务定义相关联后，才显示此选项。	
授权代码	输入授权码，以应用到为此设备组添加的设备。
SW 版本	选择软件版本，以应用到为此设备组添加的设备。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed Collectors（受管收集器）

Panorama 管理服务器（处于 Panorama 模式的 M 系列设备或 Panorama 虚拟设备）可以管理专用日志收集器（处于日志收集器模式的 M 系列设备或 Panorama 虚拟设备）。每个 Panorama 管理服务器还使用本地预定义的日志收集器（命名为 default）来处理直接从防火墙接收的日志。（处于传统模式的 Panorama 虚拟设备无需使用专用日志收集器，即可存储直接从防火墙接收的日志。）

要使用 Panorama 管理专用日志收集器，请将此日志收集器添加为受管收集器。

您想做什么？	请参阅：
显示日志收集器信息	日志收集器信息
添加、编辑或删除日志收集器	日志收集器配置
在日志收集器上更新 Panorama 软件	专用日志收集器的软件更新
了解更多？	¼¯ÖÐ日志记录和报告
	配置受管收集器

日志收集器信息

选择 **Panorama** > **Managed Collectors**（受管收集器）可显示日志收集器的下列信息。在配置日志收集器期间可以配置其他参数。

日志收集器信息	说明
收集器名称	识别此日志收集器的名称。此名称将显示为日志收集器的主机名。
序列号	用作日志收集器的 Panorama 设备的序列号。如果日志收集器为本地日志收集器，该序列号是 Panorama 管理服务器的序列号。
软件版本	日志收集器上安装的 Panorama 软件版本。
IP 地址	日志收集器管理接口的 IP 地址。
连接	日志收集器和 Panorama 之间的连接状态。
配置状态/详细信息	表示日志收集器上的配置是否与 Panorama 同步。
运行时间状态/详细信息	此日志收集器和收集器组中的其他日志收集器之间的连接状态。
日志重新分发状态	特定操作（如添加磁盘等）将触发日志收集器在其磁盘对中重新分发日志。此列将以百分比表示重新分发进程的完成状态。

© 2019 Palo Alto Networks, Inc.

日志收集器信息	说明
最后提交状态	表示日志收集器的上一次收集器组提交操作是否成功。
统计信息	配置日志收集器完成后，单击 **Statistics**（统计信息）可查看磁盘信息、CPU 性能和平均日志记录速率（日志数/秒）。为了更好地了解正在检查的日志范围，您还可以查看日志收集器收到的最旧日志中的信息。 如果您使用 SNMP 管理器进行集中监控，还可以在 *panLogCollector MIB* 中查看日志统计信息。

日志收集器配置

选择 **Panorama** > **Managed Collectors**（受管收集器）可管理日志收集器。如果 **Add**（添加）新的日志收集器作为受管收集器，则配置的设置根据日志收集器的位置以及是否在高可用性 (HA) 配置中部署 Panorama 而有所不同：

- **Dedicated Log Collector**（专用日志收集器）— 添加日志收集器时，最初不会显示 **Interfaces**（接口）。必须输入日志收集器的序列号（**Collector S/N**（收集器序列号）），单击 **Ok**（确定），然后编辑日志收集器以显示接口设置。
- **Default Log Collector that is local to the solitary (non-HA) or active (HA) Panorama management server**（独立（非 **HA**）或活动 **(HA) Panorama** 管理服务器的本地默认日志收集器）— 输入 Panorama 管理服务器的序列号（**Collector S/N**（收集器序列号））后，Collector（收集器）对话框仅显示 **Disks**（磁盘）、**Communication**（通信）设置以及一部分 **General**（常规）设置。日志收集器根据 Panorama 管理服务器的配置得出所有其他设置的值。
- （仅限高可用性）**Default Log Collector that is local to the passive Panorama management server**（被动 **Panorama** 管理服务器的本地默认日志收集器）— Panorama 将此日志收集器视为远程收集器，因此必须对其进行配置，就像配置专用日志收集器一样。

配置日志收集器的完整流程需要执行附加任务。

您在查找什么内容？	请参阅：
识别日志收集器并定义其与 Panorama 管理服务器和外部服务的连接。	常规日志收集器设置
配置对日志收集器 CLI 的访问权限。	日志收集器身份验证设置
配置专用日志收集器用于管理流量、收集器组通信和日志收集的接口。	日志收集器接口设置
配置存储从防火墙收集的日志的 RAID 磁盘。	日志收集器 RAID 磁盘设置
配置日志收集器从 User-ID 代理接收用户映射信息。	User-ID Agent 设置

© 2019 Palo Alto Networks, Inc.

您在查找什么内容？	请参阅：
配置日志收集器使用 Windows User-ID 代理进行身份验证。	连接安全性
配置与 Panorama、其他日志收集器和防火墙进行通信的安全设置。	通信设置

常规日志收集器设置

- Panorama > Managed Collectors（受管收集器）> General（常规）

配置下表所述设置，以识别日志收集器并定义其对 Panorama 管理服务器、DNS 服务器和 NTP 服务器的连接。

日志收集器常规设置	说明
收集器序列号	（必需）输入用作日志收集器的 Panorama 设备的序列号。如果日志收集器为本地日志收集器，请输入 Panorama 管理服务器的序列号。
收集器名称	输入名称以标识此日志收集器（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。 此名称将显示为日志收集器的主机名。
安全 Syslog 的入站证书	选择受管收集器必须用于从 Traps™ ESM 服务器安全提取日志的证书。此证书称为传入证书，因为 Panorama/受管收集器是 Traps ESM（客户端）向其发送日志的服务器；如果日志提取配置文件的 **Transport**（传输）协议为 **SSL**，则需要此证书。
安全系统日志的证书	选择证书以将系统日志安全地转发到外部系统日志服务器。证书必须包含选定的 **Certificate for Secure Syslog**（安全系统日志的证书）选项（请参阅管理防火墙和 Panorama 证书）。将系统日志服务器配置文件分配给包括此日志收集器的收集器组（请参阅 Panorama > Collector Groups（收集器组），**Panorama** > **Collector Groups**（收集器组）> **Collector Log Forwarding**（收集器日志转发））后，服务器配置文件的 **Transport**（传输）协议必须为 **SSL**（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Syslog）。
Panorama 服务器 IP	指定管理日志收集器的 Panorama 管理服务器的 IP 地址。
Panorama 服务器 IP 2	如果 Panorama 管理服务器部署于高可用性 (HA) 配置中，请指定辅助对端的 IP 地址。
域	输入日志收集器的域名。
主 DNS 服务器	输入主 DNS 服务器的 IP 地址。日志收集器使用此服务器查询 DNS（如查找 Panorama 管理服务器）。
辅助 DNS 服务器	（可选）输入在主服务器不可用时要使用的辅助 DNS 服务器的 IP 地址。

© 2019 Palo Alto Networks, Inc.

日志收集器常规设置	说明
主 NTP 服务器	输入主 NTP 服务器（如果有）的 IP 地址或主机名。如果不使用 NTP 服务器，则可以手动设置日志收集器时间。
辅助 NTP 服务器	（可选）输入在主服务器不可用时要使用的辅助 NTP 服务器的 IP 地址或主机名。
timezone	选择日志收集器的时区。
纬度	输入日志收集器的纬度（-90.0 至 90.0）。流量和威胁映射会将此纬度用于 App-Scope。
经度	输入日志收集器的经度（-180.0 至 180.0）。流量和威胁映射会将此经度用于 App-Scope。

日志收集器身份验证设置

- Panorama > Managed Collectors（受管收集器）> Authentication（身份验证）

日志收集器模式下的 M 系列设备或 Panorama 虚拟设备（专用日志收集器）不具有 Web 接口；只有 CLI。您可以使用 Panorama 管理服务器配置专用日志收集器上的多数设置，但对于某些设置，则需要 CLI 访问权限。要配置 CLI 访问的身份验证设置，请按下表所述配置设置。

日志收集器身份验证设置	说明
身份验证配置文件	选择配置的身份验证配置文件以定义身份验证服务，该服务验证访问专用日志收集器或 Panorama 管理员的登录凭据。
失败的尝试次数	输入专用日志收集器在锁定管理员之前，允许在 CLI 上使用的失败的登录尝试次数（范围为 0-10；默认为 10）。限制登录尝试可以保护 WildFire 设备免遭暴力攻击。值 0 代表没有登录尝试限制。 如果设置 *Failed Attempts*（失败的尝试次数）为除 *0* 以外的一个值，但将 *Lockout Time*（锁定时间）设置为 *0*，那么此管理员将被无限期锁定，直到其他管理员手动解锁此管理员。如果尚未创建其他管理员，则必须在 *Panorama* 上重新配置 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间），并将此配置更改推送到日志收集器。要确保管理员永远不被锁定，请为 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）使用默认值 *(0)*。 将 *Failed Attempts*（失败的尝试次数）设置为 *5* 或更少，以便在输入错误时容纳合理的重试次数，同时防止恶意系统尝试通过暴力攻击方法登录到专用日志收集器。
锁定时间（分钟）	输入达到 **Failed Attempts**（失败的尝试次数）限制后，专用日志收集器锁定管理员访问 CLI 所需的分钟数（范围为 0 -60；默认为 5）。值为 0 表示应用锁定，直到其他管理员手动解锁此帐户。 如果设置 *Failed Attempts*（失败的尝试次数）为除 *0* 以外的一个值，但将 *Lockout Time*（锁定时间）设置为 *0*，那么此管理员将被无限期锁定，直到其他管理员手动解锁此管理员。如果尚未创建其他管理员，则必须

© 2019 Palo Alto Networks, Inc.

日志收集器身份验证设置	说明
	在 *Panorama* 上重新配置 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间），并将此配置更改推送到日志收集器。要确保管理员永远不被锁定，请为 *Failed Attempts*（失败的尝试次数）和 *Lockout Time*（锁定时间）使用默认值 *(0)*。 设置 *Lockout Time*（锁定时间）为至少 *30* 分钟，防止恶意操作者连续登录尝试。
空闲超时（分钟）	输入在管理员自动注销之前 CLI 上没有执行任何活动的最长分钟数（范围为 0 - 1,440；没有默认值）。值为 0 表示不活动不会触发自动注销。 设置 *Idle Timeout*（空闲超时）为 *10* 分钟，以防止在管理员打开会话时未经授权的用户访问专用日志收集器。
最大会话计数	输入管理员可以同时打开的活跃会话数。默认值为 0 则表示专用日志收集器可以打开无限个并发活跃会话。
最长会话时间	输入管理员在自动注销之前可登录的分钟数。默认值为 0 则表示管理员可以无限期登录，即使空闲也能如此。
本地管理员	添加并配置专用日志收集器的新管理员。这些管理员专属于此专用日志收集器，可通过此页面进行管理（**Panorama** > **Managed Collectors**（受管收集器）> **Authentication**（身份验证））。
Panorama 管理员	导入在 Panorama 上配置的现有管理员。这些管理员在 Panorama 上创建，并导入至专用日志收集器。

日志收集器接口设置

- Panorama > Managed Collectors（受管收集器）> Interfaces（接口）

默认情况下，专用日志收集器（日志收集器模式下的 M 系列设备）使用管理 (MGT) 接口进行流量管理、日志收集和收集器组通信。但是，Palo Alto Networks 建议您分配单独的接口进行日志收集和收集器组通信，以减少 MGT 接口的流量。您可以通过为 MGT 接口定义比其他接口的子网更专用的单独子网来提高安全性。要使用单独的接口，首先必须在 Panorama 管理服务器进行配置（请参阅 Device（设备）> Setup（设置）> Management（管理））。可用于日志收集和收集器组通信的接口根据日志收集器设备型号而有所不同。例如，M-500 设备具有以下接口：Ethernet1 (1Gbps)、Ethernet2 (1Gbps)、Ethernet3 (1Gbps)、Ethernet4 (10Gbps) 和 Ethernet5 (10Gbps)。

要配置接口，请选择链接并按下表所述配置设置。

要完成 *MGT* 接口的配置，您必须指定 *IP* 地址、网络掩码（对于 *IPv4*）或前缀长度（对于 *IPv6*）以及默认网关。如果只提交部分配置（如您可能省略默认网关），则以后在执行配置更改时只能通过控制台端口访问防火墙或 *Panorama*。

始终提交完整的 *MGT* 接口配置。只有指定 *IP* 地址、网络掩码（对于 *IPv4*）或前缀长度（对于 *IPv6*）以及默认网关，您才能提交其他接口的配置。

© 2019 Palo Alto Networks, Inc.

日志收集器接口设置	说明
Eth1/Eth2/Eth3/Eth4/Eth5	必须启用要配置的接口。MGT 接口例外，默认情况下，已启用此接口。
速度和双工	配置接口的数据速率和双工选项。选项包括 10Mbps、100Mbps、1Gbps 和 10Gbps（仅限 Eth4 和 Eth5）（全双工或半双工）。使用默认 **auto-negotiate**（自动协商）设置可使日志收集器确定接口速度。 此设置必须与邻近网络设备上的接口设置匹配。
IP 地址 (IPv4)	如果网络使用 IPv4 地址，请为接口分配 IPv4 地址。
网络掩码 (IPv4)	如果已为接口分配 IPv4 地址，还必须输入网络掩码（如 255.255.255.0）。
默认网关 (IPv4)	如果已为接口分配 IPv4 地址，还必须为默认网关分配 IPv4 地址（网关必须与 MGT 接口在同一子网中）。
IPv6 地址/前缀长度	如果网络使用 IPv6 地址，请为接口分配 IPv6 地址。要指明网络掩码，请输入 IPv6 前缀长度（如 2001:400:f00::1/64）。
默认 IPv6 网关	如果已为接口分配 IPv6 地址，还必须为默认网关分配 IPv6 地址（网关与接口必须在同一子网中）。
MTU	输入在此接口上发送的数据包的最大传输单元 (MTU)，以字节为单位（范围为 576 至 1,500，默认为 1,500）。
设备日志收集	启用从防火墙收集日志的接口。对于具有高日志流量的部署，可以启用多个接口以执行此功能。默认已在 MGT 接口上启用此功能。
收集器组通信	启用接口与收集器组通信（默认值是 MGT 接口）。只有一个接口可以执行此功能。
Syslog 转发	启用用于转发 syslogs 的接口（默认为 MGT 接口）。只有一个接口可以执行此功能。
网络连接服务	可以在任何接口上执行 **Ping** 服务，并且能够让您测试日志收集器接口和外部服务之间的连接。 以下服务仅可以在 MGT 接口上执行： • **SSH** — 用于安全访问 Panorama CLI。 • **SNMP** — 能够让接口从 SNMP 管理器接收统计信息查询。有关详细信息，请参阅启用 SNMP 监控。 • **User-ID** — 能够让日志收集器重新分发从 User-ID 代理收到的用户映射信息。
允许的 IP 地址	输入可以通过此接口访问日志收集器的客户端系统的 IP 地址。 空列表（默认）指定可从任何客户端系统进行访问。 *Palo Alto Networks* 建议您不要将此列表留空；指定 *Panorama* 管理员（仅限）的客户端系统，以防止未经授权的访问。

© 2019 Palo Alto Networks, Inc.

日志收集器 *RAID* 磁盘设置

- Panorama > Managed Collectors（受管收集器）> Disks（磁盘）

在 M 系列设备或 Panorama 虚拟设备上配置日志记录磁盘后，可以将其 **Add**（添加）到日志收集器配置。

默认情况下，M 系列设备附带安装在托架 A1 和 A2 中的第一个 RAID 1 磁盘对。在软件中，托架 A1/A2 中的磁盘对命名为磁盘对 A。其余托架按顺序命名：磁盘对 B、磁盘对 C 等。例如，M-500 设备最多支持 12 个磁盘对。可以在同一设备中安装 2TB 或 1TB 磁盘对；但是，每对中两个磁盘的大小必须相同。

Panorama 虚拟设备最多支持 12 个虚拟日志记录磁盘，存储容量为 24TB。

添加磁盘对后，日志收集器会在所有磁盘之间重新分发其现有日志，这样生成每 TB 的日志可能需要几个小时。在重新分发过程期间，会降低最大日志提取速率。在 **Panorama** > **Managed Collectors**（受管收集器）页面中，Log Redistribution State（日志重新分发状态）列将以百分比表示进程的完成状态。

如果您使用 SNMP 管理器进行集中监控，可以在 *panLogCollector MIB* 中查看日志统计信息。

User-ID Agent 设置

- Panorama > Managed Collectors（托管收集器）> User-ID Agents（User-ID 代理）

专用日志收集器可接收来自最多 100 个 User-ID 代理的用户映射。代理可为 PAN-OS 集成的 User-ID 代理，运行在防火墙或基于 Windows 的 User-ID 代理上。在具有多个虚拟系统的防火墙上，每个虚拟系统可用作单独的 User-ID 代理。然后日志收集器可将用户映射重新分发至防火墙或 Panorama 管理服务器。

除了连接至 *User-ID* 代理，配置用户映射和启用用户映射重新分发的完整程序需要执行额外的任务。

要配置专用日志收集器以连接至 User-ID 代理，可 **Add**（添加）一个设置并对其进行配置，如下表中所述。

User-ID Agent 设置	说明
名称	输入用于标识 User-ID 代理的名称（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包括字母、数字、空格、连字符和下划线。 对于作为 *User-ID* 代理的防火墙，此字段无需匹配 Collector Name（收集器名称）字段。
主机	• **Windows-based User-ID agent**（基于 **Windows** 的 **User-ID** 代理）- 输入安装有 User-ID 代理的 Windows 主机的 IP 地址。 • **Firewall (PAN-OS integrated User-ID agent)**（防火墙（**PAN-OS** 集成 **User-ID** 代理））- 输入防火墙用于重新分发用户映射的接口的主机名或 IP 地址。
端口	输入 User-ID 代理将在其上侦听 User-ID 请求的端口号。默认为端口 5007，但您可指定任何可用端口。不同的 User-ID 代理可使用不同的端口。 某些更低版本的 *User-ID* 代理将端口 *2010* 用作默认端口。
收集器名称	这些字段涉及的收集器为 User-ID 代理，而非日志收集器。仅当代理为将用户映射重新分发至日志收集器的防火墙或虚拟系统时，这些字段适用。输入将防火墙或虚拟系统标识为 User-ID 代理的 **Collector Name**（收集器名称）和 **Pre-Shared Key**（预共享密钥）。您输

© 2019 Palo Alto Networks, Inc.

User-ID Agent 设置	说明
收集器预共享密钥/确认收集器预共享密钥	入的值必须和配置防火墙或虚拟系统以用作 User-ID 代理时使用的值一样（请参阅重新分发）。
已启用	选择该项以让日志收集器和 User-ID 代理通信。

连接安全性

- **Device**（设备）> **User Identification**（用户标识）> **Connection Security**（连接安全）。
- **Panorama** > **User Identification**（用户标识）> **Connection Security**（连接安全）

配置日志收集器使用的证书配置文件，以验证 Windows User-ID 代理提供的证书。日志收集器使用所选的证书配置文件，通过验证代理提供的服务器证书来验证 User-ID 代理的身份。

任务	说明
User-ID 证书配置文件	从下拉列表中，选择防火墙或 Panorama 用于对 Windows User-ID 代理进行身份验证的证书配置文件，或是选择**New Certificate Profile**（新建证书配置文件）以创建一个。选择 **None**（无）以删除证书配置文件。

通信设置

- Panorama > Managed Collectors（受管收集器）> Communication（通信）

要配置日志收集器与 Panorama、防火墙和其他日志收集器之间自定义基于证书的身份验证，请按下表所述配置设置。

通信设置	说明
安全服务器通信 — 启用 **Secure Server Communication**（安全服务器通信）验证连接到日志收集器的客户端设备的身份。	
SSL/TLS 服务配置文件	从下拉列表中选择 SSL/TLS 服务配置文件。此配置文件定义日志收集器提供的证书，并指定可与日志收集器通信的可接受 SSL/TLS 版本范围。
证书配置文件	从下拉列表中选择证书配置文件。此证书配置文件定义证书吊销检查行为和用于对客户端提供的证书链进行身份验证的根 CA。
仅自定义证书	启用后，日志收集器仅接受与受管防火墙和日志收集器进行身份验证的自定义证书。
根据序列号对客户端进行身份验证	日志收集器根据使用其序列号的哈希对客户端进行身份验证。
检查身份验证列表	根据身份验证列表检查连接到此日志收集器的客户端设备或设备组。
断开连接等待时间（分钟）	日志收集器在与其受管设备断开当前连接之前等待的时间。然后，日志收集器使用配置的安全服务器通信设置重新建立与其受管设备的连接。提交安全服务器通信配置后，等待时间开始。

© 2019 Palo Alto Networks, Inc.

通信设置	说明
身份验证列表	**Authorization List**（身份验证列表）— 选择 Add（添加），并填写以下字段以设置条件。 • **Identifier**（标识符）— 选择 **Subject**（主题）或 **Subject Alt。Name**（主题备选名称）作为授权标识符。 • **Type**（类型）— 如果选择 Subject Alt.Name（主题备选名称）作为 Identifier（标识符），可选择 **IP**、**hostname**（主机名）或 **e-mail**（电子邮件）作为标识符的类型。如果选择 Subject（主题），可使用通用名称作为标识符类型。 • **Value**（值）— 输入标识符值。
Secure Client Communication（安全客户端通信）— 启用 **Secure Client Communication**（安全客户端通信）可确保使用指定的客户端证书通过与 Panorama、防火墙或其他日志收集器的 SSL 连接对日志收集器进行身份验证。	
证书类型	选择用于进行安全通信的设备证书的类型（None（无）、Local（本地）或 SCEP）。
None	如果选择 **None**（无），既不配置任何设备证书，也不使用任何安全客户端通信。此为默认选择。
本地	日志收集器使用在日志收集器上生成或从现有企业 PKI 服务器导入的本地设备证书和相应私钥。
	Certificate（证书）— 选择本地设备证书。此证书对于防火墙可以是唯一的（基于日志收集器序列号的哈希）或是连接到 Panorama 的所有日志收集器使用的公共设备证书。
	Certificate Profile（证书配置文件）— 从下拉列表中选择证书配置文件。此证书配置文件用来通过使用日志收集器定义服务器身份验证。
Scep	日志收集器使用简单证书注册协议 (SCEP) 服务器生成的设备证书和私钥。
	SCEP Profile（**SCEP** 配置文件）— 从下拉列表中选择 SCEP 配置文件。
	Certificate Profile（证书配置文件）— 从下拉列表中选择证书配置文件。此证书配置文件用来通过使用日志收集器定义服务器身份验证。
检查服务器标识	客户端设备通过将通用名称 (CN) 与服务器的 IP 地址或 FQDN 进行匹配来确认服务器身份。

专用日志收集器的软件更新

- Panorama > Managed Collectors（受管收集器）

要在专用日志收集器上安装软件映像，请将映像下载或上传到 Panorama（请参阅 Panorama > Device Deployment（设备部署）），单击 **Install**（安装），并填写以下字段。

由于 *Panorama* 管理服务器会与本地默认日志收集器共享其操作系统，您可在 *Panorama* 管理服务器上安装软件更新时对它们进行升级（请参阅 Panorama > Software（软件））。

© 2019 Palo Alto Networks, Inc.

对于专用日志收集器，还可选择 *Panorama* > *Device Deployment*（设备部署）> *Software*（软件）来安装更新（请参阅管理软件和内容更新）。

要减少管理 *(MGT)* 接口的流量，您可以配置 *Panorama* 使用单独的接口部署更新（请参阅 Panorama > Setup（设置）> Interfaces（接口））。

用于在日志收集器上安装软件更新的字段	说明
文件	选择已下载或上传的软件映像。
设备	选择要安装软件的日志收集器。对话框将显示各日志收集器的下列信息： • **Device Name**（设备名称）— 专用日志收集器的名称。 • **Current Version**（当前版本）— 当前在日志收集器上安装的 Panorama 软件版本。 • **HA Status**（高可用性状态）— 此列不适用于日志收集器。专用日志收集器不支持高可用性。
过滤器已选择	如需仅显示特定的日志收集器，则可选中日志收集器，然后选中 **Filter Selected**（已选择筛选）。
仅上传到设备（不安装）	选择此选项可将软件上传到日志收集器，但不自动重启此软件。在您登录日志收集器 CLI、运行操作命令 `request restart system`，手动重启之后，才会安装软件映像。
在安装之后重新启动设备	选择此选项可上传并自动安装软件。安装进程将重启日志收集器。

© 2019 Palo Alto Networks, Inc.

Panorama > Collector Groups（收集器组）

每个收集器组最多可包含 16 个日志收集器，您可对其分配防火墙以便转发日志。之后，您可使用 Panorama 来查询日志收集器，以便对聚合日志进行查看和调查。

名为“*default*”的预定义收集器组包含 *Panorama* 管理服务器的本地预定义日志收集器。

- 收集器组配置
- 收集器组信息

收集器组配置

如需配置收集器组，请单击 **Add**（添加）并填写以下字段。

收集器组设置	配置位置	说明
姓名	**Panorama** > **Collector Groups**（收集器组）> **General**（常规）	输入名称以标识此收集器组（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
日志存储		表示收集器组收到的防火墙日志的当前存储配额和可用空间。 单击存储配额链接以设置以下日志类型的存储 **Quota(%)**（配额百分比）和过期期限（**Max Days**（最大天数））： • **Detailed Firewall Logs**（详细防火墙日志）— 包括 **Device**（设备）> **Setup**（设置）> **Logging and Reporting Settings**（记录和报告设置）中的所有日志类型，如流量、威胁、HIP 匹配、动态注册 IP 地址（IP 标记）、扩展 PCAP、GTP 和隧道、应用统计信息等。 • **Summary Firewall Logs**（摘要防火墙日志）— 包括 **Device**（设备）> **Setup**（设置）> **Logging and Reporting Settings**（记录和报告设置）中包括的所有摘要日志，如流量摘要、威胁摘要、URL 摘要，以及 GTP 和隧道摘要。 • **Infrastructure and Audit Logs**（基础架构和审计日记）— 包括配置、系统、User-ID 和身份验证日志。 • **Palo Alto Networks Platform Logs**（**Palo Alto Networks** 平台日志）— 包括 Traps 和其他 Palo Alto Networks 产品的日志。 • **3rd Party External Logs**（第三方外部日志）— 包括 Palo Alto Networks 提供的其他供应商集成日志。 要使用默认设置，请单击 **Restore Defaults**（还原默认值）。
最短保留期限(天)		输入 Panorama 保持收集器组中所有日志收集器的最短日志保留天数（范围为 1-2,000）。如果当前日期减去最早日志

© 2019 Palo Alto Networks, Inc.

收集器组设置	配置位置	说明
		日期小于定义的最短保留期限，则 Panorama 将生成作为警告违反的系统日志。
收集器组成员		**Add**（添加）将作为此收集器组的一部分的日志收集器（最多 16 个）。您可以添加 **Panorama** > **Managed Collectors**（受管收集器）页面中可用的任何日志收集器。任何特定收集器组的所有日志收集器均必须为相同的型号：均为 M-500 设备或均为 Panorama 虚拟设备。 在将日志收集器添加到现有收集器组后，*Panorama* 会在所有日志收集器之间重新分发其现有日志，这样生成每 *TB* 的日志可能需要几个小时。在重新分发过程期间，会降低最大日志记录速率。在 *Panorama* > *Collector Groups*（收集器组）页面中，*Log Redistribution State*（日志重新分发状态）列将以百分比表示进程的完成状态。
启用跨收集器记录冗余		如果选择此选项，则收集器组中的每个日志都将拥有两个副本，且每个副本都将驻留在不同的日志收集器上。如果任何一个日志收集器变成不可用，此冗余可确保不会丢失任何日志：可以查看转发到收集器组的所有日志并运行所有日志数据的报告。日志冗余只有在当收集器组拥有多个日志收集器且每个日志收集器拥有相同数量的磁盘时才可用。 在 **Panorama** > **Collector Groups**（收集器组）页面中，Log Redistribution State（日志重新分发状态）列将以百分比表示进程的完成状态。任何特定收集器组的所有日志收集器均必须为相同的型号：均为 M-500 设备或均为 Panorama 虚拟设备。 由于启用冗余会创建更多日志，因此该配置需要更多存储容量。启用冗余会将收集器组中的日志处理通信增加一倍，从而将其最大日志记录速率降低一半，因为每个日志收集器均必须分发其收到的每个日志的副本。（当收集器组用完容量空间后，将会删除较早的日志。）
转发到首选项列表中的所有收集器		（仅限 PA-5200 系列和 PA-7000 系列防火墙）选择以将日志发送到首选项列表中的每个日志收集器。Panorama 使用循环调度负载均衡选择在任何指定时间接收日志的日志收集器。默认为禁用：防火墙仅将日志发送到列表中的第一个日志收集器，除非该日志收集器变得不可用（请参阅设备/收集器）。
启用安全的 LC 间通信		允许在收集器组中的日志收集器之间使用自定义证书进行相互 SSL 身份验证。

© 2019 Palo Alto Networks, Inc.

收集器组设置	配置位置	说明
位置	**Panorama** > **Collector Groups**（收集器组）> **Monitoring**（监控）	指定收集器组的位置。
联系人		指定电子邮件联系人（如将监控日志收集器的 SNMP 管理员的电子邮件地址）。
版本		指定用于与 Panorama 管理服务器通信的 SNMP 版本：**V2c** 或 **V3**。 SNMP 可让您收集有关日志收集器的信息，包括连接状态、磁盘驱动器统计信息、软件版本、平均 CPU 利用率、平均日志数/秒、每种日志类型的存储持续时间等等。SNMP 信息根据每个收集器组提供。
SNMP 团体字符串（仅限 V2c）		输入 **SNMP Community String**（**SNMP** 团体字符串），不但可用于识别 SNMP 管理器和监控设备（就本例而言，即指日志收集器）的团队，还可用作对团体成员彼此进行身份验证的密码。 切勿使用默认的团体字符串 *public*；该字符串广为人知，因此并不安全。
视图（仅限 V3）		**Add**（添加）一组 SNMP 视图，并在 **Views**（视图）中输入该组的名称。 每个视图是一个配对的对象标识符 (OID) 和位掩码：OID 指定受管信息库 (MIB)，而掩码（十六进制格式）则指定可以在 MIB 内部（包含匹配）或外部（排除匹配）访问的 SNMP 对象。 对于该组内的每个视图，请 **Add**（添加）以下设置： • **View**（视图）— 输入视图的名称。 • **OID** — 输入 OID。 • **Option**（选项）（包含或排除）— 选择视图是否包含 OID。 • **Mask**（掩码）— 指定 OID 中过滤器的掩码值（如 0xf0）。
用户（仅限 V3）		为各 SNMP 用户 **Add**（添加）以下设置： • **Users**（用户）— 输入用于对 SNMP 管理器用户进行身份验证的用户名。 • **View**（视图）— 选择一组用户视图。 • **Authpwd** — 输入用于对 SNMP 管理器用户进行身份验证的密码（至少包含八个字符）。对密码进行加密仅支持安全哈希算法 (SHA)。 • **Privpwd** — 输入用于对 SNMP 管理器的 SNMP 消息进行加密的私人密码（至少包含八个字符）。仅支持高级加密标准 (AES)。
设备/收集器	**Panorama** > **Collector Groups**（收集器组）>	日志转发首选项列表控制哪些防火墙将日志转发到哪些日志收集器。对于 **Add**（添加）到列表的每个条

© 2019 Palo Alto Networks, Inc.

收集器组设置	配置位置	说明
	Device Log Forwarding（设备日志转发）	目，**Modify**（修改）设备列表以分配一个或多个防火墙，并在收集器列表中 **Add**（添加）一个或多个日志收集器。 默认情况下，在列表条目中分配的防火墙仅将日志发送到主（第一个）日志收集器（只要可用）。如果主日志收集器发生故障，则防火墙将日志发送到辅助日志收集器。如果辅助日志收集器发生故障，则防火墙将日志发送到第三个日志收集器，以此类推。如需更改顺序，请选择日志收集器，然后单击 **Move Up**（上移）或 **Move Down**（下移）。 您可以通过在 *General*（常规）选项卡中选择转发到首选项列表中的所有收集器，替代 *PA-5200* 系列和 *PA-7000* 系列防火墙的默认日志转发行为。

system
配置
HIP 匹配
通信
威胁
WildFire
关联
GTP
身份验证
User-ID
Tunnel
IP 标记
	Panorama > **Collector Groups**（收集器组）> **Collector Log Forwarding**（收集器日志转发）	对于要从此收集器组转发到外部服务的每种类型的防火墙日志，请 **Add**（添加）一个或多个匹配列表配置文件。配置文件指定要转发的日志和目标服务器。对于每个配置文件，请完成以下步骤：
		
		• **Name**（名称）— 输入名称（最多 31 个字符），以标识匹配列表配置文件。
		• **Filter**（过滤器）— 默认情况下，防火墙转发此匹配列表配置文件所适用类型的 **All Logs**（所有日志）。要转发一部分日志，选择现有过滤器或选择 **Filter Builder**（过滤器构建器）以添加新过滤器。对于新过滤器中的每个查询，指定以下字段并 **Add**（添加）查询：
		  • **Connector**（连接器）— 选择连接器逻辑（与/或)。如果要应用求反，请选择 **Negate**（求反）。例如，要避免从不可信区域转发日志，可选择 **Negate**（求反），选择 **Zone**（区域）作为 Attribute（属性），选择 **equal**（等于）作为 Operator（运算符），然后在 Value（值）列中输入不可信区域的名称。
		  • **Attribute**（属性）— 选择日志属性。选择因日志类型而异。
		  • **Operator**（运算符）— 选择确定如何应用属性的标准（如 **equal**（等于））。选择因日志类型而异。
		  • 值- 指定要匹配的属性值。
		
		要显示或导出与过滤器匹配的日志，请选择 **View Filtered Logs**（查看过滤的日志）。此选项卡提供与 **Monitoring**（监控）选项卡页面相同的选项（如**Monitoring**（监控）> **Logs**（日志）> **Traffic**（通信））。
		
		• **Description**（说明）— 输入说明（最多 1,023 个字符），以说明此匹配列表配置文件的用途。
		• Destination servers（目标服务器）— 对于每种服务器类型，**Add**（添加）一个或多个服务器配置文件。要配置服务器配置文件，请参阅 Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱）、Device（设备）> Server Profiles（服务器配置文件）> Syslog、Device（设备）> Server Profiles（服务

© 2019 Palo Alto Networks, Inc.

收集器组设置	配置位置	说明
		器配置文件）> Email（电子邮件）或 Device（设备）> Server Profiles（服务器配置文件）> HTTP。 • Built-in Actions（内置操作）— 您可以为除系统和配置日志以外的所有日志类型 **Add**（添加）操作： • 输入 **Action**（操作）的描述性名称。 • 选择要标记的 IP 地址 — **Source Address**（源地址）或 **Destination Address**（目标地址）。您只能在关联日志和 HIP 匹配日志中标记源 IP 地址。 • 选择操作 — **Add Tag**（添加标记）或 **Remove Tag**（删除标记）。 • 选择是在此 Panorama 上使用本地 User-ID 代理还是使用远程 User-ID 代理注册标记。 要使用 **Remote device User-ID Agent**（远程设备 **User-ID** 代理）注册标记，请选择将启用转发的 HTTP 服务器配置文件。 • 配置要设置的 IP 标记**Timeout**（超时）（以分钟为单位），即，维护 IP 地址到标记映射的时间量。设置超时为 0，意味着 IP 标记映射未超时（范围为 0-43200（30 天），默认为 0）。 您只能使用*Add Tag*（添加标记）配置超时。 • 输入或选择要应用或从目标源或目标 IP 地址删除的 **Tags**（标记）。
提取配置文件	**Panorama** > **Collector Groups**（收集器组）> **Log Ingestion**（日志提取）	**Add**（添加）一个或多个允许 Panorama 从 Traps ESM 服务器接收日志的日志提取配置文件。要配置新的日志提取配置文件，请参阅 Panorama > Log Ingestion Profile（日志提取配置文件）。

收集器组信息

选择 **Panorama** > **Collector Groups**（收集器组）以显示收集器组的下列信息。在完成日志收集器配置后可以配置其他字段。

收集器组信息	说明
姓名	识别收集器组的名称。
已启用冗余	表示是否已为收集器组启用日志冗余。可以在完成或修改日志收集器配置后为收集器组启用日志冗余。
收集器	分配到收集器组的日志收集器。
日志重新分发状态	特定操作（如启用日志冗余等）将触发收集器组在其日志收集器中重新分发日志。此列将以百分比表示重新分发进程的完成状态。

© 2019 Palo Alto Networks, Inc.

Panorama > Plugins（插件）

- **Panorama** > **Plugins**（插件）
- **Device**（设备）> **Plugins**（插件）

选择 **Panorama** > **Plugins**（插件）可安装、删除和管理支持 Panorama 上第三方集成的插件。

（仅在 VM 系列防火墙上可用）选择 **Device**（设备）> **Plugins**（插件）可安装、删除和管理 VM 系列防火的插件。

插件	说明
上传	可让您从本地目录上传插件安装文件。此选项不能安装插件。在上传安装文件后，安装链接变为活动状态。
文件名	插件的文件名。 在 Panorama 上安装 **vm_series**（**VM** 系列）插件时，您可以使用 **Device**（设备）> **VM-Series**（**VM** 系列）页面管理并提交公共云环境（AWS、Azure 和 Google）中部署的 VM 系列防火墙上的模板配置。
版本	插件的版本号。
平台	支持插件的模型。
发布日期	该版插件的版本日期。
大小	插件文件大小。
已安装	为 Panorama 上的每个插件提供当前安装状态。
操作	• 安装- 安装指定插件版本。安装新的插件版本将覆盖之前安装的版本。 • **Delete**（删除）— 删除指定插件文件。 • **Remove Config**（删除配置）— 删除与插件相关的所有配置。要完全删除与插件相关的所有配置，还必须在使用**Remove Config**（删除配置）后，执行**Uninstall**（卸载）。 • 卸载- 删除当前插件的安装。这不会从 Panorama 中删除插件文件。如果卸载插件，您将失去与该插件相关的所有配置。请仅在完全删除相关配置时使用。

© 2019 Palo Alto Networks, Inc.

Panorama > SD-WAN

下载并安装 Panorama SD-WAN 插件以集中管理、监视和生成报告。通过添加并关联分支到其相应的中心，配置 SD-WAN 拓扑，并将这些分支和中心设备与适当的区域关联。配置完 SD-WAN 拓扑后，您可以监视配置的所有设备和路径上的路径运行状况指标，从而隔离应用程序和链路问题，以及了解随时间推移链路性能情况。此外，还可以生成报告用于审核。

您想做什么？	请参阅：
添加、编辑或删除分支和中心设备	SD-WAN 设备
添加、编辑或删除 VPN 集群	SD-WAN VPN 集群
监视路径运行状况	SD-WAN 监控
生成运行状况报告	SD-WAN 报告

SD-WAN 设备

- **Panorama** > **SD-WAN** > **Devices**（设备）

SD-WAN 设置是指构成 VPN 集群和 SD-WAN 拓扑的分支或中心。

字段	说明
名称	输入用于标识 SD-WAN 设备的名称。
类型	选择 SD-WAN 设备的类型： • **Hub**（中心）— 部署在主要机构或位置的集中防火墙（例如，数据中心或业务总部），所有分支设备通过 VPN 连接与其相连接。分支之间的流量先经过中心，然后继续流向目标分支。分支与中心连接，从而访问中心位置的集中式资源。中心设备在主要机构或位置处理流量、实施策略规则，并管理链路交换。 • **Branch**（分支）— 部署在物理分支位置的防火墙，它通过 VPN 连接与中心相连接，并提供分支级别的安全保障。分支与中心连接，以访问集中式资源。分支设备在分支位置处理流量、实施策略，并管理链路交换。
虚拟路由器名称	选择用于在 SD-WAN 中心和分支之间进行路由的虚拟路由器。默认情况下，将创建一个 `sdwan-default` 虚拟路由器，促使 Panorama 自动推送路由器配置。
站点	输入用户标识中心或分支的用户友好型站点名称。例如，输入部署分支设备的城市名称。
链路标签	（PAN-OS 10.0.3 以及 10.0 更高版本）对于中心，请选择您为中心虚拟接口创建的链路标签，这样，中心就可参与到 DIA AnyPath。自动 VPN 将此链路应用到整个中心虚拟接口，而不是单个链路。您可以在流量分发配置文件中应用此链路标签，以指示此中心虚拟接口的故障转移顺序。在分支设备上，自动 VPN 将使用此标签填充终止于中心设备的 SD-WAN 虚拟接口的链路标签字段。
从区域到互联网	**Add**（添加）一个或多个用于标识不可信源传入和传出流量的安全区域。

© 2019 Palo Alto Networks, Inc.

字段	说明
从区域到中心	**Add**（添加）一个或多个用于标识 SD-WAN 中心设备传入和传出流量的安全区域。
从区域到分支	**Add**（添加）一个或多个用于标识 SD-WAN 分支设备传入和传出流量的安全区域。
从区域到内部	**Add**（添加）一个或多个用于标识企业网络上可信设备传入和传出流量的安全区域。
路由器 ID	指定 BGP 路由器 ID。所有路由器之间的边界网关协议 (BGP) 路由器 ID 都必须唯一。 使用回环地址作为路由器 *ID*。
回环地址	指定用于 BGP 对等设备的静态 IPv4 回环地址 。
AS 编号	输入自治系统编号以定义通常定义的 Internet 路由策略。每个中心和分支位置的 AS 编号必须是唯一的。 使用 *4* 字节专用 *BGP AS* 编号，以免干扰任何公开路由 *AB* 编号。
重新分发配置文件名称	选择或创建重新分发配置文件，以控制从分支与中心路由器进行通信的本地前缀。默认情况下，所有本地连接 Internet 前缀都将被通告给中心位置。 *Palo Alto Networks* 不会重新分发从 *ISP* 获得的分支机构默认路由。

SD-WAN VPN 集群

- **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 集群）

将 SD-WAN 分支设备与一个或多个 SD-WAN 中心设备关联，从而允许分支和中心位置进行安全通信。在 SD-WAN VPN 集群中关联分支和中心设备时，防火墙将根据您指定的 VPN 集群创建站点之间所需的 IKE 和 IPSec VPN 连接。

字段	说明
名称	输入用于标识 VPN 集群的名称。
类型	选择 SD-WAN VPN 集群的类型： • **Hub Spoke**（中心辐射型）— SD-WAN 拓扑，其中，主办公室或位置的集中式防火墙充当采用 VPN 连接的分支设备之间的网关。分支之间的流量先经过中心，然后继续流向目标分支。
分支	**Add**（添加）一个或多个与一个或多个中心关联的分支设备。
中心	**Add**（添加）一个或多个与一个或多个分支设备关联的中心设备。如果添加多个中心，请根据路径运行状况质量指标确定哪个是主中心，哪个是辅助中心。

© 2019 Palo Alto Networks, Inc.

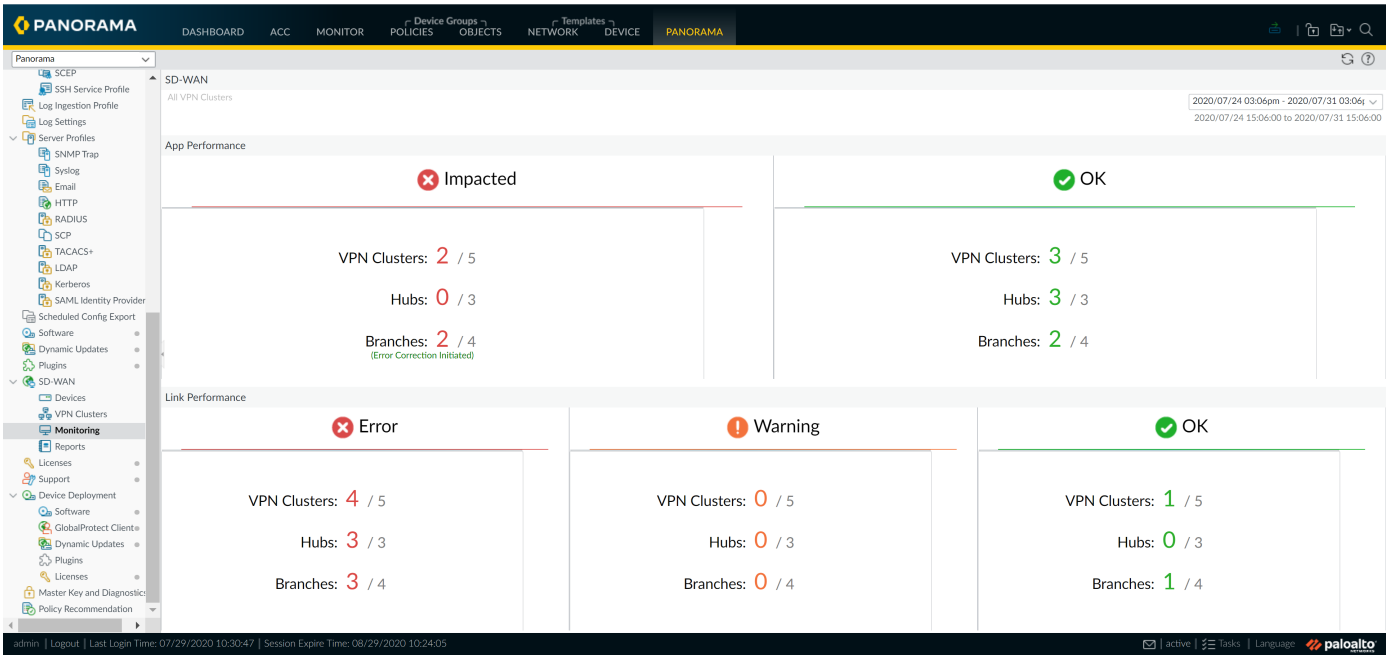
SD-WAN 监控

- **Panorama** > **SD-WAN** > **Monitoring**（监控）

“监控”选项卡是一个仪表盘，其中显示了所有 SD-WAN 设备运行状况指标的摘要小部件。通过此工具，您可以快速标识出现性能问题的应用程序或链路，从而提供有关 SD-WAN 网络上活动的可操作情报。您可以查看特定时间段内所有 VPN 集群或特定 VPN 集群的路径质量和链路性能。

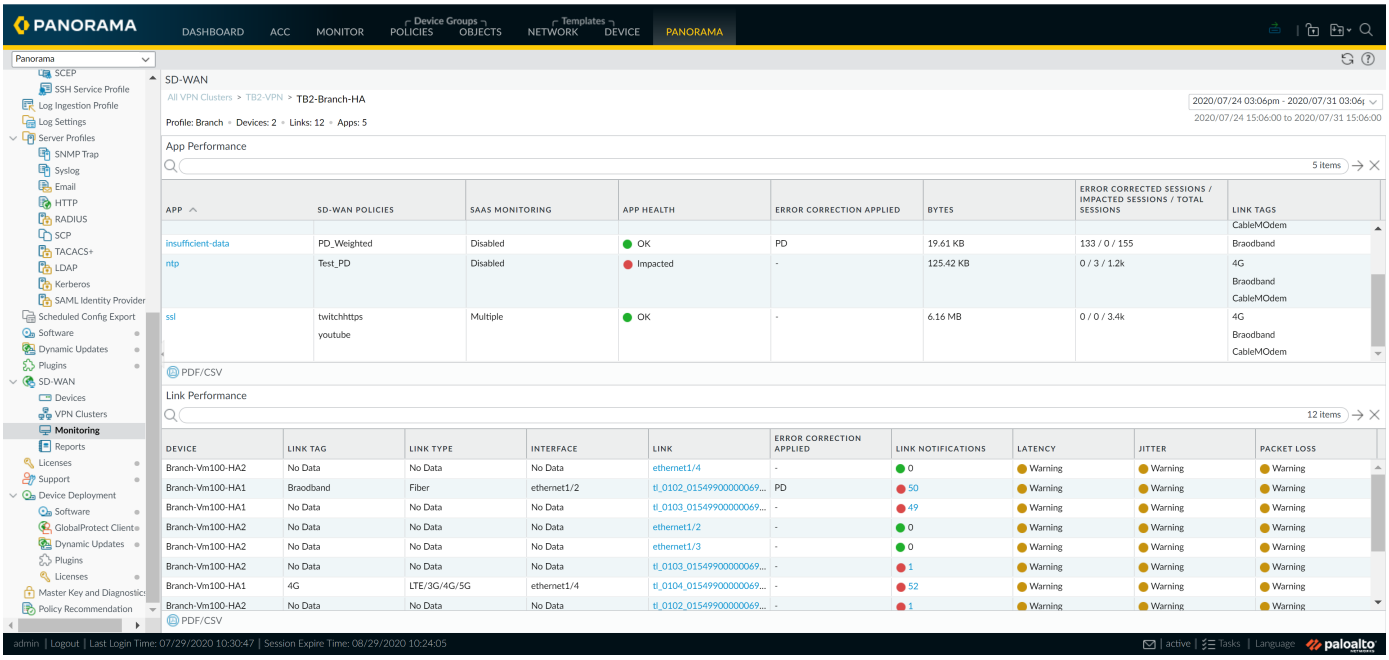
您可以一目了然地查看出现应用程序性能问题以及运行状况良好的分支或中心防火墙的 VPN 集群总数。您可以查看 VPN 集群中出现的下列应用程序和链路运行状况：

- 应用程序性能
  - **Impacted**（受影响的）— VPN 集群中的一个或多个应用程序，其路径的抖动、延迟或数据包丢失性能都没有达到或低于路径列表中选择的路径质量配置文件的指定阈值。
  - **OK**（正常）— VPN 集群中的应用程序状况良好，没有出现抖动、延迟或数据包丢失性能问题。
- 链路性能
  - **Error**（错误）— VPN 集群中的一个或多个站点，其路径的抖动、延迟或数据包丢失性能都没有达到或低于路径列表中选择的路径质量配置文件的指定阈值。
  - **Warning**（警告）— VPN 集群中的一个或多个站点与超过七天指标平均值的抖动、延迟或数据包丢失性能衡量的链路。
  - **OK**（正常）— VPN 集群中的链路状况良好，没有出现抖动、延迟或数据包丢失性能问题。



单击任何小部件以深入了解所有 VPN 集群是否均达到所需运行状况。此外，您可以使用站点筛选器，根据链路通知、延迟偏差、抖动偏差、数据包丢失偏差或受影响的应用程序查看 VPN 集群。

© 2019 Palo Alto Networks, Inc.



SD-WAN 报告

- **Panorama** > **SD-WAN** > **Reports**（报告）

为在指定时间段内最常出现运行状况降级的顶级应用程序或链路的应用程序或链路性能生成报告，以用于审核。报告配置完成后，必须 **Run Now**（立即运行）以查看报告。可以导出报告，功能目前尚不可用。可以采用哪种格式导出报告？

字段	说明
名称	输入用于标识报告目的的名称。
报告类型	选择要运行的报告类型： • **App Performance**（应用程序性能）— 生成一份详细介绍 SD-WAN 中所有应用程序流量运行状况指标的报告。 • **App Performance**（链路性能）— 生成一份详细介绍 SD-WAN 中链路流量运行状况指标的报告。
集群	从下列列表中选择要生成报告的集群。默认选择 **all**（全部）。
站点	从下列列表中选择要生成报告的站点。默认选择 **all**（全部）。 如果为集群选择了 **all**（全部），那么，您必须为属于该集群的所有站点生成报告。如果选择的是特定集群，那么，您可以选择要生成报告的特定站点。
应用程序（仅限应用程序性能报告类型）	从下列列表中选择要生成报告的应用程序。默认选择 **all**（全部）。 如果站点选择的是**all**（全部），那么，您必须为属于该站点的所有应用程序生成报告。如果选择的是特定站点，那么，您可以选择要生成报告的特定应用程序。
链路标签（仅限链路性能报告类型）	从下列列表中选择要生成报告的链路标签。默认选择 **all**（全部）。

© 2019 Palo Alto Networks, Inc.

字段	说明
	如果为站点选择了 **all**（全部），那么，您必须为站点下创建的所有链路标签生成报告。如果选择的是特定站点，那么，您可以选择要生成报告的特定链路标签。
链路类型（仅限链路性能报告类型）	从下列列表中选择要生成报告的链路类型。默认选择 **all**（全部）。 如果为链路标签选择了 **all**（全部），那么，您必须为链路标签下创建的所有链路类型生成报告。如果选择的是特定链路标签，那么，您可以选择要生成报告的特定链路类型。
前 N 项	指定报告中包含的应用程序或链路数。您可以选择该报告包括前 5 个、10 个、25 个、50 个、100 个、250 个、500 个或 1000 个性能最佳的应用程序或链路。默认选择 **5**。
时间期限	设置报告运行时间限制。默认会选择 **None**（无），即使用所有应用程序和链路性能数据生成报告。

© 2019 Palo Alto Networks, Inc.

Panorama > VMware NSX

如需自动配置 VM 系列 NSX 版防火墙，您必须启用 NSX Manager 和 Panorama 之间的通信。当 Panorama 将 VM 系列防火墙注册为 NSX Manager 上的服务时，NSX Manager 即获得在集群中每台 ESXi 主机上配置 VM 系列防火墙的一个或多个实例所需的配置设置。

您想了解什么内容？	请参阅：
我要如何配置通知组？	配置通知组
我如何为 VM 系列 NSX 版防火墙定义配置？	创建服务定义
我如何配置 Panorama 以便与 NSX Manager 进行通信？	配置对 NSX Manager 的访问权限
我如何为 VM 系列 NSX 版防火墙定义操作规则？	创建控制规则
我如何配置防火墙，以便在动态 vSphere 环境中持续实施策略？	选择 Objects（对象）> Address Groups（地址组）和 Policies（策略）> Security（安全） 要让 Panorama 和防火墙了解虚拟环境的相关变更，请在安全策略预处理规则中将动态地址组用作源和目标地址对象。
了解更多？	请参阅设置 VM 系列 NSX 版防火墙

配置通知组

- Panorama > Notify Group（通知组）

下表介绍了 Panorama 通知组设置。

通知组设置	说明
姓名	输入通知组的描述性名称。
通知设备	选中当网络上部署的虚拟机有新增项目或修改时必须要通知的设备组的复选框。 设置新虚拟机或修改现有虚拟机后，系统会以更新形式将虚拟网络中的更改发送到 Panorama。如配置执行此操作，Panorama 将填充并更新策略规则中引用的动态地址对象，以便指定设备组中的防火墙能够接收对动态地址组中注册 IP 地址所作的更改。 要启用通知，请确保已选择要对其启用通知的各个设备组。如果您未能选择设备组（无可用的复选框），则设备组将借由设备组层次结构被自动纳入。 此通知进程可感知上下文并维持网络上应用程序的安全性。例如，如果您有一组基于硬件的边界防火墙，且当部署了新应用程序或 Web 服务器时必须向其发送通知，则此进程会自动刷新指定设备组的动态地址组。所有引用动态地址对象的策略规则随即会自动包含任何新部署或修改的应用程序或 Web 服务器，并会根据您的条件安全启用。

© 2019 Palo Alto Networks, Inc.

创建服务定义

- Panorama > VMware NSX > Service Definitions（服务定义）

服务定义可让您将 VM 系列防火墙注册为 NSX Manager 上的合作伙伴安全服务。您可在 Panorama 上定义最多 32 个服务定义，并在 NSX Manager 上对其进行同步。

通常，您会为 ESXi 集群中的每个租户创建一个服务定义。每个服务定义将指明用于部署防火墙的 OVF（PAN-OS 版）并包含 ESXi 集群上安装的 VM 系列防火墙的配置。为指明配置，服务定义必须具备唯一的模板、唯一的设备组，以及将使用此服务定义部署的防火墙的许可证授权码。防火墙部署完成后，它将连接到 Panorama 并接收其配置设置（包括防火墙将保护的各租户或部门的区域），以及来自服务定义中指定设备组的防火墙策略设置。

要添加新的服务定义，请按下表所述配置设置。

字段	说明
姓名	输入您要在 NSX Manager 上显示的服务的名称。
说明	（可选）输入标签以描述此服务定义的用途或功能。
设备组	选择要为其分配这些 VM 系列防火墙的设备组或设备组层次结构。有关详细信息，请参阅 Panorama > VMware NSX。
模板	选择要对其分配 VM 系列防火墙的模板。有关详细信息，请参阅 Panorama > Templates（模板）。 必须将每个服务定义分配到唯一的模板或模板堆栈。 一个模板可以具备与之相关联的多个区域（NSX 的 NSX 服务配置文件区域）。对于单租户部署，请在模板中创建一个区域（NSX 服务配置文件区域）。如具备多租户部署，请为每个子租户创建一个区域。 创建新 NSX 服务配置文件区域后，它将自动附加到一对虚拟线路子接口。有关详细信息，请参阅 Network（网络）> Zones（区域）。
VM-Series OVF URL	输入 NSX Manager 从中可访问 OVF 文件以设置新 VM 系列防火墙的 URL（IP 地址或主机名和路径）。
通知组	从下拉列表中选择通知组。

配置对 NSX Manager 的访问权限

- Panorama > VMware NSX > Service Managers（服务管理器）

要使 Panorama 能够与 NSX Manager 进行通信，请按下表所述 **Add**（添加）和配置设置。

服务管理器	说明
服务管理器名称	输入名称以将 VM 系列防火墙标识为服务。此名称将显示在 NSX Manager 上并用于按需部署 VM 系列防火墙。 最多支持 63 个字符，只能使用字母、数字、连字符和下划线。
说明	（可选）输入标签以描述此服务的用途或功能。

© 2019 Palo Alto Networks, Inc.

服务管理器	说明
NSX 管理器 URL	指定 Panorama 将用于建立与 NSX Manager 的连接的 URL。
NSX 管理器登录名	输入在 NSX Manager 上配置的身份验证凭据 — 用户名和密码Panorama 使用这些凭据来对 NSX Manager 进行身份验证。
NSX 管理器密码	
确认 NSX Manager 密码	
服务定义	指定与此服务管理器相关联的服务定义。每个服务管理器最多支持 32 个服务定义。

在将更改提交到 Panorama 后，VMware Service Manager（VMware 服务管理器）窗口将显示 Panorama 和 NSX Manager 之间的连接状态。

同步状态	说明
STATUS（状态）	显示 Panorama 和 NSX Manager 之间的连接状态。 连接成功后将显示 Registered（已注册），即表示 Panorama 和 NSX Manager 处于同步状态，且 VM 系列防火墙已注册为 NSX Manager 上的服务。 如果连接失败，则状态可能为： • **Connected Error**（连接错误）— 无法连接到 NSX Manager 或建立与 NSX Manager 的网络连接。 • **Not authorized**（未授权）— 访问凭据（用户名和/或密码）不正确。 • **Unregistered**（未注册）— 服务管理器、服务定义或服务配置文件不可用或已从 NSX Manager 中删除。 • **Out of sync**（不同步）— Panorama 上定义的配置设置与 NSX Manager 上定义的配置设置不同。单击 **Out of sync**（不同步）了解有关故障原因的详细信息。例如，NSX Manager 可能具有某项服务定义，其名称与 Panorama 上定义的名称相同。要修复此错误，请使用错误消息中列出的服务定义名称，以验证 NSX Manager 上的服务定义。在 Panorama 和 NSX Manager 未同步之前，您无法在 Panorama 上添加新的服务定义。
同步动态对象	单击 **Synchronize Dynamic Objects**（同步动态对象）以刷新 NSX Manager 中的动态对象信息。同步动态对象使您能够维持虚拟环境中变化的上下文，还允许您通过自动更新策略规则中使用的动态地址组来安全启用应用程序。 在 *Panorama* 上，您只能查看已在 *NSX Manager* 中进行过动态注册的 *IP* 地址。*Panorama* 不会显示直接在防火墙中注册的动态 *IP* 地址。如果使用 *VM* 信息源（*VM* 系列 *NSX* 版防火墙不支持此信息源）或 *XML API* 向防火墙动态注册 *IP* 地址，则您必须登录各个防火墙，以在防火墙上查看动态 *IP* 地址的完整列表（包括从 *Panorama* 推送的地址和已在本地注册的地址）。
NSX 配置同步	选择 **NSX Config-Sync**（**NSX** 配置同步）可将 Panorama 上配置的服务定义与 NSX Manager 进行同步。如果 Panorama 上没有任何暂挂提交，则此选项不可用。

© 2019 Palo Alto Networks, Inc.

同步状态	说明
	如果同步失败，请在错误消息中查看详细信息，了解错误是发生在 Panorama 上还是 NSX Manager 上。例如，在 Panorama 上删除服务定义后，如果此服务定义是 NSX Manager 规则中引用的服务定义，则与 NSX Manager 同步将会失败。使用错误消息中提供的信息，确定故障发生原因以及在何位置进行纠正（在 Panorama 或 NSX Manager 上）。

创建控制规则

- Panorama > VMware NSX > Steering Rules（控制规则）

控制规则确定从集群中的来宾控制到 VM 系列防火墙的流量。

字段	说明
自动生成控制规则	根据以下规则的安全规则生成控制规则： • 属于注册到 NSX Service Manager 的父或子设备组。 • 拥有与源和目标（不是任何到任何）相同的区域。 • 只拥有一个区域。 • 不拥有为策略配置的静态地址组、IP 地址范围或网络掩码。 默认情况下，通过 Panorama 生成的控制规则不拥有配置的 NSX 服务，并将 NSX 通信方向设置为 inout。生成控制规则后，可以更新各个控制规则以更改 NSX 通信方向或添加 NSX 服务。自动生成控制规则时，Panorama 自动填充以下字段（Description（说明）和 NSX Services（NSX 服务）字段除外）。
姓名	输入您要在 NSX Manager 上显示的控制规则的名称。自动生成时，Panorama 将前缀 auto_ 添加到每个控制规则，并将安全策略规则名称中的任何空格替换为下划线（_）。
说明	（可选）输入标签以描述此服务定义的用途或功能。
NSX 通信方向	指定重定向到 VM 系列防火墙的通信的方向。 • **inout** — 在 NSX 上创建 INOUT 规则。将源和目标之间指定类型的通信重定向到 VM 系列防火墙。Panorama 使用此通信方向自动生成控制规则。 • **in** — 在 NSX 上创建 IN 规则。将从目标到源的指定类型的通信重定向到 VM 系列防火墙。 • **out** — 在 NSX 上创建 OUT 规则。将从源到目标的指定类型的通信重定向到 VM 系列防火墙。
NSX 服务	选择要重定向到 VM 系列防火墙的应用程序（Active Directory 服务器、HTTP、DNS 等）通信。
设备组	从下拉列表中选择设备组。所选设备组确定应用于控制规则的安全策略。必须将设备组与 NSX 服务定义相关联。
安全策略	自动生成的控制规则基于的安全策略规则。

© 2019 Palo Alto Networks, Inc.

Panorama > Log Ingestion Profile（日志提取配置文件）

使用日志提取配置文件可让 Panorama 接收外部源的日志。在 PAN-OS 8.0.0 中，Panorama（在 Panorama 模式下）可充当 Syslog 接收器，使用 Syslog 提取陷阱 ESM 服务器中的日志。系统支持新的外部日志源，并且新陷阱 ESM 版本的更新将通过内容更新进行推送。

要启用日志提取，必须在陷阱 ESM 服务器上将 Panorama 配置为 Syslog 接收器，在 Panorama 上定义日志提取配置文件，然后将此日志提取配置文件附加到日志收集器组中。

要添加新的外部 Syslog 提取配置文件，请添加配置文件，并按下表所述配置设置。

字段	说明
名称	输入外部 Syslog 提取配置文件的名称。最多可以添加 255 个配置文件。
源名称	输入发送日志的外部源的名称或 IP 地址。在一个配置文件内最多可以添加 4 个日志源。
端口	输入通过网络可访问 Panorama 的端口，此端口将用于通信和侦听。 对于陷阱 ESM，在 23000-23999 范围之间选择一个值。必须在陷阱 ESM 上配置相同的端口号，Panorama 和 ESM 之间才能通信。
传输	选择 TCP、UDP 或 SSL。如果选择 SSL，为确保安全 syslog 通信，必须在 Panorama > Managed Collectors（受管收集器）> General（常规）中配置入站证书。
外部日志类型	从下拉列表中选择日志类型。
版本	从下拉列表中选择版本。

使用 Monitor（监控）> External Logs（外部日志）可查看从陷阱 ESM 服务器提取到 Panorama 的日志的信息。

© 2019 Palo Alto Networks, Inc.

Panorama > Log Settings（日志设置）

使用 **Log Settings**（日志设置）页面可将以下类型的日志转发到外部服务：

- Panorama 管理服务器（在 Panorama 模式下的 M 系列设备或 Panorama 虚拟设备）在本地生成的系统、配置、User-ID 和关联日志。
- 在传统模式下，Panorama 虚拟设备在本地生成的或从防火墙收集的所有类型的日志。

对于防火墙发送到日志收集器的日志，需完成日志收集器配置，才能将其转发到外部服务。

在开始之前，必须先为外部服务定义服务器配置文件（请参阅 Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱）、Device（设备）> Server Profiles（服务器配置文件）> Syslog、Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件）和 Device（设备）> Server Profiles（服务器配置文件）> HTTP）。然后添加一个或多个匹配列表配置文件，并按下表所述配置设置。

匹配列表配置文件设置	说明
名称	输入标识匹配列表配置文件的名称（最多 31 个字符）。
Filter（筛选器）	默认情况下，Panorama 会转发要添加匹配列表配置文件的相应类型的所有日志。要转发日志的子集，请打开下拉列表，并选择现有过滤器，或选择 **Filter Builder**（过滤器生成器）以添加新的过滤器。对于新过滤器中的每个查询，指定以下字段并 **Add**（添加）查询： • **Connector**（连接符）— 为查询选择逻辑连接符 (and/or)。如果想要应用逻辑否定，则选择 **Negate**（求反）。例如，要避免从不可信区域转发日志，可选择 **Negate**（求反），选择 **Zone**（区域）作为 Attribute（属性），选择 **equal**（等于）作为 Operator（运算符），然后在 Value（值）列中输入不可信区域的名称。 • **Attribute**（属性）— 选择日志属性。这些选项取决于日志类型。 • **Operator**（运算符）— 选择确定属性是否适用的标准（如 **equal**（等于））。这些可用选项取决于日志类型。 • **Value**（值）— 指定要匹配的查询的属性值。 要显示或导出与过滤器匹配的日志，请选择 **View Filtered Logs**（查看过滤的日志）。此选项卡提供与 **Monitoring**（监控）选项卡页面相同的选项（如**Monitoring**（监控）> **Logs**（日志）> **Traffic**（通信））。
说明	输入说明（最多 1,024 个字符），解释此匹配列表配置文件的用途。
SNMP	添加一个或多个 SNMP 陷阱服务器配置文件，以便以 SNMP 陷阱形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> SNMP Trap（SNMP 陷阱））。
email	添加一个或多个电子邮件服务器配置文件，以便以电子邮件通知形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Email（电子邮件））。
Syslog	添加一个或多个 Syslog 服务器配置文件，以便以 syslog 消息形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> Syslog）。

© 2019 Palo Alto Networks, Inc.

匹配列表配置文件设置	说明
Http	添加一个或多个 HTTP 服务器配置文件，以便以 HTTP 请求形式转发日志（请参阅 Device（设备）> Server Profiles（服务器配置文件）> HTTP）。
内置操作	除系统日志和配置日志以外，所有日志类型都允许配置操作。 • 添加一项操作，并输入描述操作的名称。 • 选择要标记的 IP 地址 — **Source Address**（源地址）或 **Destination Address**（目标地址）。 • 选择操作 — **Add Tag**（添加标记）或 **Remove Tag**（删除标记）。 • 选择是将标记分发到此设备上的本地 User-ID 代理，还是分发到远程 User-ID 代理。 • 要将标记分发到远程设备 **User-ID** 代理，请选择启用转发功能的 HTTP 服务器配置文件。 • 配置要设置的 IP 标记**Timeout**（超时）（以分钟为单位），即，维护 IP 地址到标记映射的时间量。设置超时为 0，意味着 IP 标记映射未超时（范围为 0-43200（30 天），默认为 0）。 您只能使用*Add Tag*（添加标记）配置超时。 • 输入或选择要应用或从目标源或目标 IP 地址删除的 **Tags**（标记）。在关联日志和 HIP 匹配日志中，只能标记源 IP 地址。

© 2019 Palo Alto Networks, Inc.

Panorama > Server Profiles（服务器配置文件）> SCP

- Panorama > Server Profiles（服务器配置文件）> SCP

选择 **Panorama** > **Server Profiles**（服务器配置文件）> **SCP**以配置安全复制协议(SCP)服务器的设置，从而在网络上安全复制并传输文件，这样，就可以自动下载并在受管防火墙、日志收集器以及受物理隔离 Panorama™ 管理服务器管理的 WildFire® 设备上安装内容更新。

SCP 服务器设置	说明
名称	输入名称以标识服务器配置文件（最多 31 个字符）。名称区分大小写，且必须是唯一的。仅可使用字母、数字、空格、连字符和下划线。
服务器	输入服务器 IP 地址或 FQDN。
端口	输入文件传输服务器端口（范围为 1–65,535；默认为 22）。
用户名	输入用于访问 SCP 服务器的用户名。
密码 确认密码	输入用于访问 SCP 服务器的用户名的密码（区分大小写）。

© 2019 Palo Alto Networks, Inc.

Panorama > Scheduled Config Export（计划配置导出）

要调度 Panorama 和防火墙上所有运行配置的导出，请添加导出任务，并按下表所述配置设置。

如果 *Panorama* 具有高可用性 *(HA)* 配置，则您必须在每个对端设备上执行以下说明以确保在故障转移后计划导出能够继续。*Panorama* 不会在高可用性对端设备之间同步计划配置。

调度配置导出设置	说明
名称	输入标识配置导出作业的名称（最多 31 个字符）。名称区分大小写，且必须是唯一的。只能使用字母、数字、连字符和下划线。
说明	输入可选说明。
启用	选择此选项可导出作业。
已计划的导出开始时间(每天)	指定时间以开始导出（24 小时制，格式为 HH:MM）。
协议	选择用于将日志从 Panorama 导出到远程主机的协议。安全复制 (**SCP**) 是一种安全协议，但 **FTP** 不是。
主机名	输入目标 SCP 或 FTP 服务器的 IP 地址或主机名。
端口	输入目标服务器上的端口号。
路径	在将存储导出配置的目标服务器上，指定文件夹或目录的路径。 例如，如果配置包存储于名为 Panorama 顶层文件夹下的“exported_config”文件夹中，则各服务器类型的语法为： • SCP 服务器： /Panorama/exported_config • FTP 服务器： //Panorama/exported_config 以下字符：**.**（句点）、**+**、**{** 和 **}**、**/**、**-**、**_**、**0-9**、**a-z** 和 **A-Z**。文件 **Path**（路径）中不支持空格。
启用 FTP 被动模式	选中此选项可使用 FTP 被动模式。
用户名	指定访问目标系统所需的用户名。
密码/确认密码	指定访问目标系统所需的密码。 使用的密码长度最长不超过 15 个字符。如果超过 15 个字符，测试 SCP 连接将显示错误，因为防火墙在尝试连接到 SCP 服务器时加密密码，且加密密码的长度最多只能为 63 个字符。
测试 SCP 服务器连接	选择此选项可测试 Panorama 和 SCP 主机/服务器之间的通信。 要实现数据的安全传输，必须验证并接受 SCP 服务器的主机密钥。接受主机密钥后才能建立连接。如果 Panorama 具有高可用性配置，则您必须在

© 2019 Palo Alto Networks, Inc.

调度配置导出设置	说明
	每个高可用性对端设备上执行此验证，从而使得每个高可用性对端设备都可以接受 SCP 服务器的主机密钥。

© 2019 Palo Alto Networks, Inc.

Panorama > Software（软件）

使用此页面管理 Panorama 管理服务器上的 Panorama 软件更新。

- 管理 Panorama 软件更新
- 显示 Panorama 软件更新信息

管理 Panorama 软件更新

选择 **Panorama** > **Software**（软件）可执行下表中所述的任务。

默认情况下，*Panorama* 管理服务器最多可保存两个软件更新。为给新版软件留出存储空间，服务器将自动删除最早的版本。您可以更改 Panorama 保存的软件映像数量，并手动删除映像以释放空间。

请参阅安装 Panorama 的内容和软件更新，了解有关版本兼容性的重要信息。

任务	说明
立即检查	如果 Panorama 可以访问互联网，请单击 **Check Now**（立即检查）以显示最新的更新信息（请参阅显示 Panorama 软件更新信息）。 如果 Panorama 无法访问外部网络，请使用浏览器访问软件更新站点，以获取更新信息。
上传	若要在 Panorama 无法访问互联网时上传软件映像，请使用浏览器访问软件更新站点，找到所需的版本，然后将软件映像下载到 Panorama 可以访问的计算机，选择 **Panorama** > **Software**（软件），单击 **Upload**（上传）、**Browse**（浏览）并选择软件映像，然后单击 **OK**（确定）。上传结束后，已下载列将显示一个复选标记，且操作列显示 **Install**（安装）。
下载	如果 Panorama 可以访问互联网，请单击所需版本 Action（操作）列中的 **Download**（下载）。下载完成后，已下载列将显示一个复选标记。
安装	**Install**（安装）（Action（操作）列）软件映像。安装完成后，Panorama 将在重启时将您注销。 *Panorama* 定期执行文件系统完整性检查 *(FSCK)*，以防止 *Panorama* 系统文件损坏。此检查在八次重新启动后或在最后一次文件系统完整性检查 *(FSCK)* 执行 *90* 天后发生。如果正在运行文件系统完整性检查，将会在 *Web* 界面和 *SSH* 登录屏幕上显示一则警告，提示在完成该操作前您将无法进行登录。完成此过程的时间随存储系统大小而变化；对于较大的存储系统，可能需要数小时之后才可以登录回 *Panorama*。要查看进度，请设置 *Panorama* 的控制台访问。
发行说明	如果 Panorama 可以访问互联网，则您可以访问所需软件版本的 **Release Notes**（发行说明），并查看版本更改、修复、已知问题、兼容性问题和默认行为更改。 如果 Panorama 无法访问互联网，请使用浏览器访问软件更新站点并下载合适的软件版本。
☒	如果您不再需要某软件映像或想要释放空间以便存储更多映像，请将其删除。

© 2019 Palo Alto Networks, Inc.

显示 Panorama 软件更新信息

选择 **Panorama** > **Software**（软件）可显示以下信息。要显示来自 Palo Alto Networks 的最新信息，请单击 **Check Now**（立即检查）。

软件和内容更新信息	说明
版本	Panorama 软件版本
大小	软件映像的大小（兆字节）。
发布日期	Palo Alto Networks 发布更新的日期和时间。
可用	说明此映像是否可用于安装。
当前已安装	一个选中标记，说明已安装所选更新。
操作	说明适用于映像的操作（**Download**（下载）、**Install**（安装）或 **Reinstall**（重装））。
发行说明	单击 **Release Notes**（发行说明）可访问所需软件版本的发行说明，并查看版本更改、修复、已知问题、兼容性问题和默认行为更改。
☒	如果不再需要某更新或要释放空间用于更多下载或上传，请将其删除。

© 2019 Palo Alto Networks, Inc.

Panorama > Device Deployment（设备部署）

您可使用 Panorama 将软件和内容更新部署到多个防火墙和日志收集器，并管理防火墙许可证。

您在查找什么内容？	请参阅：
将软件和内容更新部署到防火墙和日志收集器。	管理软件和内容更新
查看已安装的软件和内容更新，或可用于下载和安装的软件和内容更新。	显示软件和内容更新信息
调度防火墙和日志收集器的自动内容更新	调度动态内容更新
从 Panorama 恢复一个或多个防火墙的内容版本。	从 Panorama 恢复内容版本
查看、激活、停用和刷新许可证。 查看防火墙许可证的状态。	管理防火墙许可证
了解更多？	管理许可证和更新。

管理软件和内容更新

- Panorama > Device Deployment（设备部署）> Software（软件）

Panorama 可以为将软件和内容更新部署到防火墙和日志收集器提供以下选项。

要减少管理 *(MGT)* 接口的流量，您可以配置 *Panorama* 使用单独的接口部署更新（请参阅 Panorama > Setup（设置）> Interfaces（接口））。

Panorama 设备部署选项	说明
下载	如需在 Panorama 连接到 Internet 时部署软件或内容更新，请 **Download**（下载）此更新。下载完成后，Available（可用）列将显示“Downloaded（已下载）”。之后，您可以： • 安装 PAN-OS/Panorama 软件更新或内容更新。 • 激活 GlobalProtect™ 应用程序或 SSL VPN 客户端软件更新。
升级	如果 BrightCloud URL 过滤的内容更新可用，请单击 **Upgrade**（升级）。升级成功后，您可在防火墙上安装更新。
安装	下载或上传 PAN-OS 软件、Panorama 软件或内容更新后，请单击 Action（操作）列中的 **Install**（安装），然后选择： • **Devices**（设备）— 选择要安装更新的防火墙或日志收集器。如果列表过长，请使用 Filters（过滤器）。选择 **Group HA Peers**（分组高可用性对端），以对属于高可用性

© 2019 Palo Alto Networks, Inc.

Panorama 设备部署选项	说明
	(HA) 对端的防火墙进行分组。此选项可让您轻松确定拥有高可用性配置的防火墙。如需仅显示特定的防火墙或日志收集器，则可将其选中，然后选择 **Filter Selected**（已选择过滤器）。 • **Upload only to device**（仅上传到设备）（仅限软件）— 选择此选项可在不自动安装软件的情况下加载软件。您必须手动安装软件。 • **Reboot device after install**（安装后重启设备）（仅限软件）— 选择此选项可指定安装过程自动重新启动防火墙或日志收集器。只有在重启后才能完成安装。 • **Disable new apps in content update**（禁用内容更新中的新应用程序）（仅限应用程序和威胁）— 选择此选项可在最近一次更新安装后进行更新时禁用相关的应用程序。这不仅能防止最新威胁的攻击，还能确保您在准备任何策略更新后启用应用程序的灵活性。然后，要启用应用程序，请登录到防火墙，选择 **Device**（设备）> **Dynamic Updates**（动态更新），单击 Features（功能）列中的 **Apps**（应用程序）以显示新应用程序，然后单击要启用的各应用程序的 **Enable/Disable**（启用/禁用）。 还可以选择 *Panorama* > *Managed Devices*（受管设备）以安装防火墙软件和内容更新，也可以选择 *Panorama* > *Managed Collectors*（受管收集器）以安装专用日志收集器的软件更新。
Activate	下载或上传 GlobalProtect 应用程序软件更新后，请单击 Action（操作）列中的 **Activate**（激活），然后按以下说明选择各个选项： • **Devices**（设备）— 选择要激活更新的防火墙。如果列表过长，请使用 Filters（过滤器）。选择 **Group HA Peers**（分组高可用性对端），以对属于高可用性 (HA) 对端的防火墙进行分组。此选项可让您轻松确定拥有高可用性配置的防火墙。要仅显示特定防火墙，则可选中防火墙，然后选中 **Filter Selected**（已选择过滤器）。 • **Upload only to device**（仅上传至设备）— 如果您不想 PAN-OS 自动激活已上传的映像，则可选择此选项。您必须登录防火墙，然后将其激活。
发行说明	单击 **Release Notes**（发行说明）可访问所需软件版本的发行说明，并查看版本更改、修复、已知问题、兼容性问题和默认行为更改。
文档	单击 **Documentation**（文档）可访问所需内容版本的发行说明。
☒	如果不再需要某软件或内容更新，或要释放空间用于更多下载或上传，请将其删除。
立即检查	**Check Now**（立即检查）可显示软件和内容更新信息。
上传	要在 Panorama 未连接到互联网时部署软件或内容更新，请从软件更新或动态更新站点将更新下载到计算机，选择与更新类型相对应的 **Panorama** > **Device Deployment**（设备部署）页面，单击 **Upload**（上传），选择更新 **Type**（类型）（仅限内容更新），选择已上传的文件，然后单击 **OK**（确定）。然后，安装或激活更新的步骤取决于类型： • **PAN-OS or Panorama software**（**PAN-OS** 或 **Panorama** 软件）—上传结束后，已下载列将显示一个复选标记，且操作列显示 **Install**（安装）。 • **GlobalProtect Client or SSL VPN Client software**（**GlobalProtect** 客户端或 **SSL VPN** 客户端软件）— 从文件激活。 • **Dynamic updates**（动态更新）— 从文件安装。
从文件安装	上传内容更新后，请单击 **Install from File**（从文件安装），选择内容 **Type**（类型），选择此更新的文件名，然后选择防火墙或日志收集器。

© 2019 Palo Alto Networks, Inc.

Panorama 设备部署选项	说明
从文件激活	上传 GlobalProtect 应用程序软件更新后，请单击 **Activate from File**（从文件激活），选择此更新的文件名，然后选择防火墙。
计划	选择此选项可计划动态内容更新。

显示软件和内容更新信息

- Panorama > Device Deployment（设备部署）> Software（软件）

选择 **Panorama** > **Device Deployment**（设备部署）> **Software**（软件），可显示目前已安装或可供下载和安装的 PAN-OS **Software**（软件）、**GlobalProtect Client**（**GlobalProtect** 客户端）软件和 **Dynamic Updates**（动态更新）（内容）。**Dynamic Updates**（动态更新）页面将按内容（防病毒软件、应用程序和威胁、URL 过滤、WildFire）来组织信息，并指明最近一次检查更新信息的日期和时间。要显示来自 Palo Alto Networks 的最新软件或内容信息，请单击 **Check Now**（立即检查）。

软件和内容更新信息	
版本	软件或内容更新的版本。
文件名	更新文件的名称。
平台	专为更新指定的防火墙或日志收集器型号。数字表示硬件防火墙型号（例如，7000 表示 PA-7000 系列防火墙）；vm 表示 VM 系列防火墙；m 表示 M 系列防火墙。
功能	（仅限内容）列出内容版本可能包含的签名类型。
类型	（仅限内容）表示下载包含的是完整数据库更新还是增量更新。
大小	更新文件的大小。
发布日期	Palo Alto Networks 发布更新的日期和时间。
可用	（仅限 PAN-OS 或 Panorama 软件）表示此更新已下载或已上传。
已下载	（仅限 SSL VPN 客户端软件、GlobalProtect 客户端软件或内容）选中标记表示此更新已下载。
操作	表示可对更新执行的操作：下载、升级、安装或激活。
文档	（仅限内容）提供访问所需内容版本发行说明的链接。
发行说明	（仅限内容）提供访问所需软件版本发行说明的链接。
☒	如果不再需要某更新或要释放空间用于更多下载或上传，请将其删除。

调度动态内容更新

- Panorama > 设备部署 > 动态更新

© 2019 Palo Alto Networks, Inc.

要调度更新的自动下载和安装，请单击 **Schedules**（调度），单击 **Add**（添加），并按下表所述配置设置。

动态更新调度设置	
名称	输入标识调度作业的名称（最多 31 个字符）。名称区分大小写，必须是唯一的，且只能包含字母、数字、连字符和下划线。
禁用	选中此选项可禁用调度的作业。
下载源	选择用于内容更新的下载源。您可以选择从 Palo Alto Networks **Updates Server**（更新服务器）或从 **SCP** 服务器下载内容更新。
SCP 配置文件（仅限 SCP）	选择要从中下载的配置的 SCP 配置文件。
SCP 路径（仅限 SCP）	输入要从中下载内容更新的 SCP 服务器上的特定路径。
类型	选择要调度的内容更新类型：**App**（应用程序）、**App and Threat**（应用程序和威胁）、**Antivirus**（防病毒软件）、**WildFire** 或 **URL Database**（**URL** 数据库）。
重复	选择 Panorama 检查更新服务器的时间间隔。重复选项因更新类型而异。
时间	对于 **Daily**（每天）更新，请选择 24 小时制的 **Time**（时间）。 对于 **Weekly**（每周）更新，请选择 **Day of week**（星期几）以及 24 小时制的 **Time**（时间）。
在内容更新中禁用新应用程序	仅当您将更新 **Type**（类型）设为 **App**（应用程序）或 **App and Threat**（应用程序和威胁），且将 **Action**（操作）设为 **Download and Install**（下载并安装）时，才能在内容更新中禁用新应用程序。 选中此选项，可在更新中禁用相对于上次安装的更新是新应用程序的应用程序。这不仅能防止最新威胁的攻击，还能确保您在准备任何策略更新后启用应用程序的灵活性。然后，要启用应用程序，请登录到防火墙，选择 **Device**（设备）> **Dynamic Updates**（动态更新），单击 Features（功能）列中的 **Apps**（应用程序）以显示新应用程序，然后单击要启用的各应用程序的 **Enable/Disable**（启用/禁用）。
操作	• **Download Only**（仅下载）— Panorama™ 将下载已调度的更新。您必须在防火墙和日志收集器上手动安装更新。 • **Download and Install**（下载并安装）— Panorama 将下载并自动安装已调度的更新。 • **Download and SCP**（下载和 **SCP**）—Panorama 将下载并传输内容更新数据包给特定 SCP 服务器。
设备	选择 **Devices**（设备），然后选择将接收已调度内容更新的防火墙。
日志收集器	选择 **Log Collectors**（日志收集器），然后选择将接收已调度内容更新的受管收集器。

从 Panorama 恢复内容版本

- Panorama > 设备部署 > 动态更新

© 2019 Palo Alto Networks, Inc.

从 Panorama 将一个或多个防火墙的应用程序、应用程序和威胁、防病毒软件、WildFire 以及 WildFire 内容更新的内容版本快速 **Revert**（恢复）为先前安装的内容版本。您将要恢复到的内容版本必须低于防火墙上当前安装的版本。可在运行 8.1 的 Panorama 上恢复内容。只要防火墙上的恢复功能在本地可用，就可以恢复防火墙上的内容。

字段	说明
Filter（筛选器）	筛选想要恢复内容的设备。可以按以下项筛选： • 设备状态 • 平台 • 设备组 • 模板 • 标记 • HA 状态 • 软件版本 (PAN-OS) • 当前内容版本
设备	选择要恢复的一个或多个设备。显示以下设备信息： • 设备名称 — 防火墙的名称。 • 当前版本 — 设备上安装的当前内容版本。如果未安装内容版本，列将显示为 0。 • 先前版本（内容）— 在运行 PAN 8.1 或更高版本的防火墙上先前安装的内容版本。如果先前未安装任何内容版本或者防火墙正在运行的 PAN-OS 版本低于 8.1，则列将为空。 • 软件版本 — 设备上安装的当前 PAN-OS 版本。 • HA 状态 — 显示 HA 对中的 HA 状态。如果设备不在 HA 对中，则列将为空。
分组 HA 对	选中此复选框以对 HA 对端分组。

选择要恢复的设备后，请单击 **OK**（确定）。

管理防火墙许可证

- Panorama > Device Deployment（设备部署）> Licenses（许可证）

选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证）可执行以下任务：

- 更新不具备互联网直接访问权限的防火墙的许可证 — 单击 Refresh（刷新）。
- 在防火墙上激活许可证 — 要激活防火墙上的许可证，请单击 **Activate**（激活），选择防火墙，然后在 Auth Code（授权码）列中输入 Palo Alto Networks 为防火墙提供的授权码。
- 停用安装在 VM 系列防火墙上的所有许可证和订阅/授权 — 请单击 **Deactivate VMs**（停用 **VM**），选择防火墙（列表将仅显示运行 PAN-OS 7.0 或更新版本的防火墙），然后单击以下选项中的一项：
  - **Continue**（继续）— 停用许可证并自动将更改注册到许可服务器。许可证被退回到您的帐户，且可供重复使用。
  - **Complete Manually**（手动完成）— 生成令牌文件。如果 Panorama 无法直接访问 Internet，可以使用此选项。如需完成停用过程，您必须登录支持门户，选择 **Assets**（资产），单击 **Deactivate License(s)**（停用许可证），上传令牌文件，然后单击 **Submit**（提交）。完成上述操作后，将会停用过程。

© 2019 Palo Alto Networks, Inc.

您还可以查看受管防火墙的当前许可证状态。对于可直接访问互联网的防火墙，Panorama 将使用许可服务器自动执行每日签到、检索许可证更新和续期，并将其推送到防火墙。签到采用硬编码，时间设定在凌晨 1-2 点；您不可更改此时间安排。

防火墙许可证信息	
设备	防火墙名称。
虚拟系统	表示防火墙是否支持多个虚拟系统。
威胁防护	表示许可证的状态是活动、不活动，还是已过期（也会指明过期日期）。
网址	
支持	
GlobalProtect 网关	
GlobalProtect 网络门户	
WildFire	
虚拟器系列容量	表示此设备是否为 VM 系列防火墙。