paloalto TECHDOCS

VM 系列部署指南

Version 11.0



docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2021-2022 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

November 14, 2022

Table of Contents

关于 VM 系列防火墙 15
VM 系列部署 16
高可用性中的 VM 系列 18
升级 VM 系列防火墙 20
升级 PAN-OS 软件版本（独立版本） 20
升级 PAN-OS 软件版本（HA 对） 23
使用 Panorama 升级 PAN-OS 软件版本 27
升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列） 29
升级 VM 系列型号 35
升级 HA 对中的 VM 系列型号 36
将 VM 系列防火墙降级到上一版本 37
VM 系列插件 39
在防火墙上配置 VM 系列插件 39
升级 VM 系列插件 40
在 VM 系列防火墙上启用 Jumbo 帧 43
虚拟机监控程序分配的 MAC 地址 45
发布用于监控的自定义 PAN-OS 指标 47
用于访问 VM 系列防火墙上外部服务的接口 49
PacketMMAP 和 DPDK 驱动程序支持 50
在 VM 系列上启用 NUMA 性能优化 52
在 VM 系列防火墙上启用 ZRAM。 54
授权 VM 系列防火墙许可证 55
VM 系列防火墙许可 56
许可证类型 56
灵活 vCPU 和固定型号许可 57
灵活 vCPU 和固定型号部署 59
创建支持帐户 60
VM 系列防火墙的序列号和 CPU ID 格式 61
使用基于 Panorama 的软件防火墙许可证管理 62
软件 NGFW 积分 67
基于层和内存的最大限制 70
激活积分 79
创建部署配置文件 80

©2024 Palo Alto Networks, Inc.

管理部署配置文件 82
注册 VM 系列防火墙（软件 NGFW 积分） 83
配置 Panorama 86
将 Panorama 迁移到软件 NGFW 许可证 87
传输积分 91
续订软件 NGFW 积分合同 93
停用许可证（软件 NGFW 积分） 94
解除非正常终止防火墙的许可 96
设置许可的 vCPU 数量 97
自定义数据平面核心 98
将防火墙迁移到灵活 VM 系列许可证 99
软件 NGFW 许可 API 103
VM 系列型号 112
VM 系列系统要求 113
CPU 超额认购 115
VM-50 Lite 模式 116
VM 系列型号许可证类型 117
激活 VM 系列型号许可证 128
注册 VM 系列防火墙 134
在 VM 系列防火墙上安装设备证书 137
在 BYOL 和 PAYG 许可证之间切换 139
在 VM 系列型号许可证之间切换 140
停用许可证 143
更新 VM 系列防火墙许可证包 149
基于型号的许可 API 150
许可证到期后会发生什么？ 158
云安全服务提供商许可证 (CSSP) 161
获取 CSSP 许可证包的身份验证码 161
使用 CSSP 授权代码注册 VM 系列防火墙 162
为注册的 VM 系列防火墙添加最终用户信息 163
在 ESXi 服务器上设置 VM 系列防火墙 167
在 VMware vSphere 虚拟机监控程序 (ESXi) 上支持的部署 168
ESXi 系统上 VM 系列的要求和限制 169
ESXi 系统上 VM 系列的要求 169
ESXi 系统上 VM 系列的限制 170
在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙 171

©2024 Palo Alto Networks, Inc.

规划适用于ESXi的 VM 系列的接口 171
在 ESXi 服务器上设置 VM 系列防火墙 172
在 ESXi 上对 VM 系列防火墙执行初始配置 175
添加额外磁盘空间至 VM 系列防火墙 176
通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具 178
使用 vMotion 在主机之间移动 VM 系列防火墙 179
使用 VM 系列 CLI 在 ESXi 上交换管理接口 180
vCenter 上的 VM 监控 181
关于 VMware vCenter上的 VM 监控 181
安装适用于 VMware vCenter 的 Panorama 插件 182
为 VMware vCenter 配置 Panorama 插件 183
排除 ESXi 部署的故障 186
基本故障排除 186
安装问题 186
许可问题 188
连接问题 188
ESXi 的 VM 系列性能调整 190
在 ESXi 上安装 NIC 驱动程序 190
在 ESXi 上启用 DPDK 191
在 ESXi 上启用 SR-IOV 191
使用 SR-IOV 启用 ESXi VLAN 访问模式 192
在 ESXi 上启用 NIC 的多队列支持 194
VNF 性能调整 194

在 vCloud Air 上设置 VM 系列防火墙 207

关于 vCloud Air 上的 VM 系列防火墙 208
vCloud Air 上支持的部署 209
在 vCloud Air 上部署 VM 系列防火墙 210

在 VMware NSX-T 上设置 VM 系列防火墙 219

在 VMware NSX-T 上设置 VM 系列防火墙（北向南） 220
VMware NSX-T 上支持的 VM 系列防火墙部署（北向南） 220
NSX-T 上 VM 系列防火墙的组件（北向南） 220
在 NSX-T 上部署 VM 系列防火墙（北向南） 222
将安全策略从 NSX-V 扩展到 NSX-T 235
在 NSX-T 上设置 VM 系列防火墙（东向西） 237
NSX-T 上 VM 系列防火墙的组件（东向西） 237

©2024 Palo Alto Networks, Inc.

NSX-T 集成上的 VM 系列防火墙（东向西）.....238
VMware NSX-T 上支持的 VM 系列防火墙部署（东向西）.....240
使用以操作为中心的工作流程部署 VM 系列.....241
使用以安全为中心的工作流程部署 VM 系列.....260
从 Panorama 中删除服务定义.....291
从 NSX-T 操作上的 VM 系列迁移到以安全为中心的部署.....292
将安全策略从 NSX-V 扩展到 NSX-T.....299
使用就地迁移将 VM 系列从 NSX-V 迁移到 NSX-T.....301
在 AWS 上设置 VM 系列防火墙.....309
关于 AWS 上的 VM 系列防火墙.....310
AWS EC2 实例类型.....310
AWS GovCloud 上的 VM 系列防火墙.....310
AWS China 上的 VM 系列防火墙.....311
AWS Outposts 上的 VM 系列防火墙.....311
AWS 术语.....311
管理接口映射以用于 Amazon ELB.....314
在 AWS 上调整 VM 系列防火墙性能.....315
AWS 上支持的部署.....317
在 AWS 上部署 VM 系列防火墙.....320
获取 AMI.....320
AWS VPC 中 VM 系列防火墙的规划工作表.....324
在 AWS 上启动 VM 系列防火墙.....326
在 AWS Outpost 上启动 VM 系列防火墙.....334
创建自定义 Amazon 机器映像 (AMI).....342
在 AWS上 加密 VM 系列防火墙的 EBS 卷.....345
使用 VM 系列防火墙 CLI 以交换管理接口.....346
在 VM 系列防火墙上启用 CloudWatch 监控.....346
AWS 中的 Panorama Orchestrated 部署.....351
准备编排 AWS 部署.....353
在 AWS 中编排 VM 系列防火墙部署.....357
查看部署状态.....364
流量和配置.....366
VM 系列与 AWS 网关负载均衡器集成.....374
手动将 VM 系列与负载均衡器集成.....376
VM 系列自动扩展组与 AWS 网关负载均衡器.....390
AWS 上 VM 系列防火墙的高可用性.....404

©2024 Palo Alto Networks, Inc.

AWS 上 HA 的概述 404
HA 的 IAM 角色 405
HA 链接 408
检测信号轮询和呼叫消息 408
设备优先级和抢先 408
高可用性计时器 409
使用辅助 IP 在 AWS 上配置主动/被动 HA 409
使用接口移动在 AWS 上配置主动/被动 HA 415
在 AWS 上迁移主动/被动 HA 420
使用 AWS 机密管理器存储 VM 系列证书 426
用例：保护 AWS 云中的 EC2 实例 428
用例：使用动态地址组保护 VPC 中的新 EC2 实例 443
用例：VM 系列防火墙作为 AWS 上的 GlobalProtect 网关 448
GlobalProtect 基础架构的组件 448
在 AWS 上部署 GlobalProtect 网关 449
AWS 上的资源监控 451
在 Panorama 上使用 AWS 插件进行 AWS 资源监控 451
在 Panorama 上设置用于 VM 监控的 AWS 插件 451
使用 Amazon ELB 服务自动扩展 VM 系列防火墙 466
适用于 AWS 版本 2.0 的 VM 系列自动扩展模板 468
适用于 AWS 版本 2.1 的 VM 系列自动扩展模板 491
在 AWS VPC 上监控的属性列表 512
监控 AWS VPC 所需的 IAM 权限 513
在 KVM 上设置 VM 系列防火墙 515
KVM 上的 VM 系列防火墙—要求和先决条件 516
用于在网络上连接 VM 系列防火墙的选项 517
KVM 上 VM 系列防火墙的先决条件 518
在 KVM 上支持的部署 523
保护单个主机上的流量 523
保护 Linux 主机之间的流量 523
在 KVM 上安装 VM 系列防火墙 525
使用 Virt-Manager 安装 VM 系列防火墙 525
在 ISO 安装 VM 系列防火墙 532
使用 VM 系列 CLI 在 KVM 上交换管理接口 534
启用使用 SCSI 控制器 534
验证 VM 系列防火墙上网络接口排序的 PCI-ID 535

©2024 Palo Alto Networks, Inc.

KVM 的 VM 系列性能调整 537
在 Ubuntu 16.04.1 LTS 上安装 KVM 和 Open vSwitch 537
在 KVM 上启用 Open vSwitch 537
将 Open vSwitch 与 DPDK 集成 538
在 KVM 上启用 SR-IOV 543
使用 SR-IOV 启用 VLAN 访问模式 544
在 KVM 上启用 NIC 的多队列支持 545
在 KVM 上的 NUMA 节点中隔离 CPU 资源 545
智能流量分流 547
智能流量分流要求 548
智能流量分流接口 549
高可用性 550
配置软件直通 552
安装 BlueField-2 DPU 552
安装 VM 系列防火墙 553
启用虚拟功能 553
检查 BlueField-2 DPU 系统 554
安装或升级 BlueField 引导流软件 555
安装或升级 Debian 软件包 557
运行智能流量分流 558
Bluefield-2 DPU 故障排除 560
PAN-OS 故障排除 560
参考资料 563

在 Hyper-V 上设置 VM 系列防火墙 565

Hyper-V 上支持的部署 566
保护单个 Hyper-V 主机上的流量 566
保护跨多个 Hyper-V 主机的流量 566
Hyper-V 上的系统要求 568
Linux 集成服务 569
在 Hyper-V 上安装 VM 系列防火墙 570
准备工作 570
在 Hyper-V 上调整 VM 系列防火墙的性能 571
使用 Hyper-V 管理器在 Hyper-V 主机上设置 VM 系列防火墙 571
使用 PowerShell 在 Hyper-V 主机上设置 VM 系列防火墙 573
在 VM 系列防火墙上执行初始配置 574

©2024 Palo Alto Networks, Inc.

在 Azure 上设置 VM 系列防火墙 577
关于 Azure 上的 VM 系列防火墙 578
Azure 网络和 VM 系列防火墙 578
Azure 安全中心集成 579
Azure 上的 VM 系列防火墙模板 580
Azure 上对 VM 系列的最低系统要求 581
支持 Azure 上 VM 系列的高可用性 582
VM 系列在 Azure 上的服务主体权限 582
Azure 上支持的部署 586
从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板） 587
从 Azure China Marketplace 部署 VM 系列防火墙（解决方案模板） 596
Azure 中的 Panorama 编排部署 602
准备编排部署 604
在 Azure 中编排 VM 系列防火墙部署 608
使用 Azure 网关负载均衡器部署 VM 系列 617
为 Azure 创建自定义 VM 系列映像 626
使用 Azure 安全中心建议保护您的工作负载 628
基于 Azure 安全中心建议部署 VM 系列防火墙 628
从 Azure 安全中心连接现有 VM 系列防火墙 629
使用 Panorama 转发日志到 Azure 安全中心 631
在 Azure Stack 中部署 VM 系列防火墙 634
在 VM 系列防火墙上启用 Azure Application Insights 638
在 Azure 上监控 641
关于在 Azure 上监控 641
在 Panorama 上设置用于监控的 Azure 插件 641
使用 Azure 上 Panorama 插件监控的属性 649
在 Azure 上设置主动/被动 HA 652
在 Azure 上设置主动/被动 HA（北向南和东向西流量） 653
在 Azure 上设置主动/被动 HA（仅限东向西流量） 665
使用 Azure 密钥保管库存储 VM 系列证书 678
使用 ARM 模板部署 VM 系列防火墙 681
部署 VM 系列和 Azure 应用程序网关模板 685
VM 系列和 Azure 应用程序网关模板 685
开始使用 VM 系列和 Azure 应用程序网关模板 687
在 Azure 上保护 Kubernetes 服务 695
适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？ 695

©2024 Palo Alto Networks, Inc.

保护 AKS 集群 699

在 OpenStack 上设置 VM 系列防火墙 711

OpenStack 中的 VM 系列部署 712

基本网关 712

服务链和服务扩展 712

面向 OpenStack 解决方案的 VM 系列组件 714

基本网关部署的热量模板 716

服务链和服务扩展的 Heat 模板 719

虚拟网络 720

虚拟机 720

服务模板 721

服务实例 721

IPAM 722

服务政策 722

警报 723

在基本网关部署中安装 VM 系列防火墙 725

使用服务链或扩展来安装 VM 系列防火墙 728

在 Google Cloud Platform 上设置 VM 系列防火墙 731

关于 Google Cloud Platform 上 VM 系列防火墙 732

Google Cloud Platform 和 VM 系列防火墙 732

对 VM 系列的最低系统要求 732

Google Cloud Platform 上支持的部署 734

Internet 网关 734

分段网关 734

混合云 IPSec VPN 735

为 Google Cloud Platform 创建自定义 VM 系列防火墙映像 736

在 Google Public Cloud 上准备设置 VM 系列防火墙 739

一般要求 739

在 Panorama 上安装 VM 系列插件 740

安装适用于 GCP 的 Panorama 插件 740

准备从 GCP Marketplace 进行部署 741

在 Google Cloud Platform 上部署 VM 系列防火墙 749

从 Google Cloud Platform Marketplace 部署 VM 系列防火墙 749

用于 Google Cloud Launcher 负载均衡的管理接口交换 753

使用 VM 系列防火墙 CLI 以交换管理接口 755

 ©2024 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用 Google Stackdriver 监控 756
在 Google Cloud Platform (GCP) 上启用 VM 监控以跟踪 VM 更改 758
使用动态地址组保护 VPC 中的安全实例 760
使用自定义模板或 gcloud CLI 部署 VM 系列防火墙 762
使用适用于 GCP 的 Panorama 插件进行 VM 监控 764
使用适用于 GCP 的 Panorama 插件配置 VM 监控 764
在 Google Cloud Platform 上自动扩展 VM 系列防火墙 771
适用于 Google Cloud Platform 的自动扩展组件 771
部署 GCP 自动扩展模板 783

在 Cisco ENCS 网络中设置 VM 系列防火墙 809

计划 Cisco ENCS 部署 810
为 Cisco ENCS 准备 VM 系列防火墙映像 812
从图形用户界面转换 qcow2 文件 812
从命令行界面转换 qcow2 文件 814
在 Cisco ENCS 上部署 VM 系列防火墙 817

在 Oracle Cloud Infrastructure 上设置 VM 系列防火墙 821

OCI 形状类型 822
OCI 上支持的部署 823
准备在 OCI 上设置 VM 系列防火墙 824
从 Oracle Cloud Marketplace 部署 VM 系列防火墙 827
在 OCI 上配置主动/被动 HA 832

在 Alibaba Cloud 上设置 VM 系列防火墙 841

Alibaba Cloud 上的 VM 系列防火墙 842
Alibaba Cloud 上 VM 系列防火墙的最低系统要求 843
VM 系列防火墙软件要求 843
VM 系列防火墙的 Alibaba Cloud 实例类型建议 843
Alibaba Cloud CLI 843
准备在 Alibaba Cloud 上部署 VM 系列防火墙 844
选择许可证和计划网络 844
准备使用 Aliyun 命令行界面 844
在 Alibaba Cloud 上部署 VM 系列防火墙 846
创建 VPC 并配置网络 846
创建和配置 VM 系列防火墙 849
确保 Alibaba Cloud 的北向南流量安全 853

©2024 Palo Alto Networks, Inc.

在 Alibaba Cloud 上配置负载均衡 856

在 Cisco ACI 中设置防火墙 859

Palo Alto Networks 防火墙与 Cisco ACI 集成 860

Service Graph 模板 861

多上下文部署 861

准备您的 ACI 环境进行集成 862

在网络策略模式下将防火墙与 Cisco ACI 集成 863

在网络策略模式下部署防火墙以保护东向西向流量 863

部署防火墙以在网络策略模式下保护北向南流量 879

Cisco ACI 中的端点监控 896

安装适用于 Cisco ACI 的 Panorama 插件 897

配置 Cisco ACI 插件 898

适用于 Cisco ACI 仪表盘的 Panorama 插件 902

在 Cisco CSP 上设置 VM 系列防火墙 907

Cisco CSP 上的 VM 系列要求 908

在 Cisco CSP 上部署 VM 系列防火墙 909

Cisco TrustSec 的端点监控 911

适用于 Cisco TrustSec 的 Panorama 插件 912

批量同步 912

PubSub 913

动态地址与静态地址的区别 913

安装适用于 Cisco TrustSec 的 Panorama 插件 915

配置适用于 Cisco TrustSec 的 Panorama 插件 916

排除适用于 Cisco TrustSec 的 Panorama 插件故障 924

插件状态命令 924

调试命令 924

调试日志 925

在 Nutanix AHV 上设置 VM 系列防火墙 927

Nutanix 上的 VM 监控 928

关于 Nutanix 上的 VM 监控 928

安装适用于 Nutanix 的 Panorama 插件 929

配置适用于 Nutanix 的 Panorama 插件 929

引导 VM 系列防火墙 935

©2024 Palo Alto Networks, Inc.

选择引导方法 936
基本配置 937
完整配置 941
VM 系列防火墙引导工作流程 942
引导数据包 944
引导数据包结构 944
引导数据包交付 944
引导配置文件 946
init-cfg.txt 946
bootstrap.xml 946
在 Panorama 上生成 VM 身份验证密钥 948
创建 init-cfg.txt 文件 950
init-cfg.txt 文件组件 951
init-cfg.txt 示例文件 954
创建 bootstrap.xml 文件 957
准备引导许可证 958
准备引导数据包 959
在 AWS 上引导 VM 系列防火墙 961
在 Azure 上引导 VM 系列防火墙 965
在 ESXi 上引导 VM 系列防火墙 969
使用 ISO 文件在 ESXi 上引导 VM 系列防火墙 969
使用块存储设备在 ESXi 上引导 VM 系列防火墙 969
在 Google Cloud Platform 上引导 VM 系列防火墙 971
在 Hyper-V 上引导 VM 系列防火墙 973
使用 ISO 文件在 Hyper-V 上引导 VM 系列防火墙 973
使用块存储设备在Hyper-V上引导 VM 系列防火墙 973
在 KVM 上引导 VM 系列防火墙 976
使用 ISO 文件在 KVM 上引导 VM 系列防火墙 976
使用块存储设备在 KVM 上引导 VM 系列防火墙 977
验证引导完成 978
引导错误 979

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

关于 VM 系列防火墙

Palo Alto Networks VM 系列防火墙是虚拟化形式的 Palo Alto Networks 下一代防火墙。该防火墙适用于虚拟化或云环境，它可在其中保护东向西和北向南流量，并确保其安全。

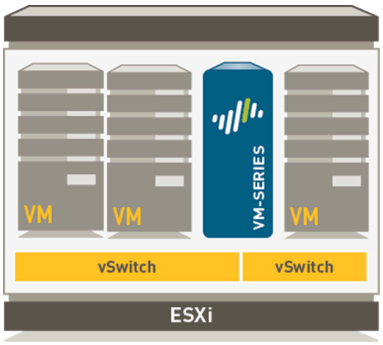
- VM 系列部署
- 高可用性中的 VM 系列
- 升级 VM 系列防火墙
- VM 系列插件
- 在 VM 系列防火墙上启用 Jumbo 帧
- 虚拟机监控程序分配的 MAC 地址
- 发布用于监控的自定义 PAN-OS 指标
- 用于访问 VM 系列防火墙上外部服务的接口
- PacketMMAP 和 DPDK 驱动程序支持
- 在 VM 系列上启用 NUMA 性能优化
- 在 VM 系列防火墙上启用 ZRAM。

VM 系列部署

VM 系列防火墙可在以下平台上部署：

- 用于 **VMware vSphere** 虚拟机监控程序 **(ESXi)** 的 **VM** 系列和 **vCloud Air**

  您可以在 VMware ESXi 上将任何 VM 系列型号部署为来宾机器；最适合需要虚拟组成因素的云和网络。

  有关详情，请参阅 在 ESXi 服务器上设置 VM 系列防火墙 和 在vCloud Air上设置 VM 系列防火墙。

- **VMware NSX-T** 上的 **VM** 系列

  您可以在 NSX-T 环境中部署 VM-100、VM-300、VM-500 或 VM-700。

  有关详细信息，请参阅 在 VMware NSX-T 上设置 VM 系列防火墙（北向南）。

- 用于 **Amazon Web** 服务 **(AWS)** 的 **VM** 系列

  您可以在 AWS 云上的 EC2 实例上部署除 VM-50 之外的任何 VM 系列型号。

  有关详细信息，请参阅在 AWS上 设置 VM 系列防火墙。

- 面向 **Google Cloud Platform** 的 **VM** 系列

  您可以在 Google Compute Engine 实例上部署除 VM-50 和 VM-50 Lite 之外的任何 VM 系列型号。有关详细信息，请参阅 在 Google Cloud Platform 上设置 VM 系列防火墙。

- 面向内核虚拟化模块 **(KVM)** 的 **VM** 系列

  您可以在运行 KVM 虚拟机监控程序的 Linux 服务器上部署任何 VM 系列型号。有关详细信息，请参阅在 KVM 上 设置 VM 系列防火墙。

- 面向 **Microsoft Hyper-V** 的 **VM** 系列

  您可以在已启用 Hyper-V 角色插件的 Windows Server 2012 R2 服务器上部署任何 VM 系列型号，也可以在单独的 Hyper-V 2012 R2 服务器上部署。有关详细信息，请参阅在 Hyper-V 上 设置 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

- 面向 **Microsoft Azure** 的 **VM** 系列

  您可以在 Azure VNet 上部署除 VM-50 之外的任何 VM 系列型号。

  有关详细信息，请参阅在 Azure 上 设置 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

高可用性中的 VM 系列

高可用性 (HA) 是一种配置，在该配置中，两个防火墙结合成组，且其配置保持同步，从而防止网络上出现单点故障。防火墙对等端之间的检测信号连接可以确保当某个对等端关闭时提供无缝故障转移。在由两台设备组成的集群中设置防火墙可以提供冗余，并且可以确保业务连续性。在 VM 系列防火墙上的 HA 配置中，必须部署在同一类型的虚拟机监控程序上，分配相同的硬件资源（如 CPU 内核/网络接口），且具有相同的许可/订阅集。有关在 Palo Alto Networks 防火墙上的 HA 的一般信息，请参阅高可用性。

VM 系列防火墙支持状态主动/被动或主动/主动高可用性，同时支持会话和配置同步。某些私有云虚拟机监控程序上的虚拟线路和第 3 层部署中支持主动/主动部署，并且仅在每个防火墙需要其自己的路由实例，并且您随时在两个防火墙外有完整实时的冗余时才推荐。要将 VM 系列防火墙配置为 HA 对，请参阅配置主动/被动 HA 和配置主动/主动 HA。

如果要在公共云中部署 VM 系列防火墙（例如在 Amazon Web Services (AWS) 或 Azure 上），则可以使用传统的主动/被动 HA 配置；请参阅 AWS 上 VM 系列防火墙的高可用性和在 Azure 上设置主动/被动 HA。或者，由于与私有数据中心相比，资源或区域冗余在云基础架构中构建的方式的内在差异，可以利用本机云服务和构建最大化正常运行时间的弹性架构，请参阅

- AWS — 使用 Amazon ELB 自动扩展 VM 系列防火墙，以在 VPC 中的两个或更多可用性区域中部署多个防火墙。
- Azure — VM 系列和 Azure 应用程序网关模板参数。

支持的功能/链接	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
主动/被动 HA	是	是	是	否	是	是	是	否	是
主动/主动 HA	是	是	否	否	否	是	否	否	否
HA 1	是	是	是	否	是	是	是	是	是
HA2 —（会话同步和保持活动）	是	是	是	否	是	是	是	是	是
HA3	是	是	否	否	否	是	否	否	否

GCP 上对 *VM* 系列的 *HA1* 和 *HA2* 支持需要 *PAN-OS 10.0x* 或更高版本和 *VM-Series* 插件 *2.0.5* 或更高版本。

通过 NSX-T 功能（称为服务运行状况检查），可以在 NSX-T (E/W) 上实现 VM 系列防火墙的高可用性。此 NSX-T 功能可以让您在服务实例失败时模拟高可用性。使用 VM 系列防火墙配置时，如果 VM 系列服务实例失败，则定向到该防火墙的所有流量都将重定向到集群中的另一个防火墙实

©2024 Palo Alto Networks, Inc.

例（对于服务集群部署）或另一个主机上的防火墙实例（对于基于主机的部署）。有关更多信息，请参阅 NSX-T (E/W) 上 VM 系列防火墙的在 Panorama 上配置服务定义。

©2024 Palo Alto Networks, Inc.

升级 VM 系列防火墙

通过升级 PAN-OS 版本或 VM 系列型号，您可以添加有助于改进防火墙的安全功能和性能的最新功能和缺陷修复。

独立 PAN-OS 版本就是这样；PAN-OS 的常规版本可以安装在所有 Palo Alto Networks 防火墙上。PAN-OS XFR 版本仅适用于 VM 系列防火墙，并且可以包括针对 VM 系列防火墙的新功能和缺陷修复。如果在 VM 系列防火墙上安装 PAN-OS XFR 映像，则比安装的软件版本更旧的 PAN-OS 版本不提供新功能和缺陷修复。

由于 XFR 映像包括 VM 系列防火墙的特定功能和缺陷修复，因此如果您升级到 XFR 版本，则必须保持 XFR 版本以保留 XFR 特定功能，直到下一个 PAN-OS 主要版本发行；XFR 中提供的所有缺陷修复和功能都将累积到下一个 PAN-OS 主要版本。

- 升级 PAN-OS 软件版本（独立版本）
- 升级 PAN-OS 软件版本（HA 对）
- 使用 Panorama 升级 PAN-OS 软件版本
- 升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列）
- 升级 VM 系列型号
- 升级 HA 对中的 VM 系列型号
- 将 VM 系列防火墙降级到上一版本

有关安装 VM 系列防火墙的说明，请参阅 VM 系列部署。

升级前验证防火墙型号的 VM 系列系统要求。如果防火墙的存储空间小于 *5.5GB*，则系统容量（会话、规则、安全区域、地址对象等的数量）将限制为 *VM-50 Lite* 的容量。

升级 PAN-OS 软件版本（独立版本）

查看新功能、解决的问题和已知问题，然后使用以下程序升级不在 HA 配置中的防火墙。

为避免影响流量，计划在中断时间段内进行升级。确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。

STEP 1 | 验证是否有足够的硬件资源可用于 VM 系列防火墙。

要查看每个 VM 系列型号的资源需求，请参阅 VM 系列系统要求。在继续升级过程之前分配其他硬件资源；在每个虚拟机监控程序上分配额外硬件资源的过程各不相同。

如果 VM 系列防火墙没有该模型所需的资源，则默认为与 VM-50 相关联的容量。

©2024 Palo Alto Networks, Inc.

STEP 2 | 从 Web 界面中，导航到 **Device**（设备） > **Licenses**（许可证），确保您拥有正确的 VM 系列防火墙许可证，同时确保该许可证已被激活。

在 VM 系列防火墙独立版本中，导航到 **Device**（设备） > **Support**（支持），并确保已经激活支持许可证。

STEP 3 | 保存当前配置文件的备份。



尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Export named configuration snapshot**（导出已命名的配置快照）。
2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。
3. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 4 | 如果您已启用 User-ID，则在升级后防火墙将清除当前 IP 地址到用户名和组映射，以便可以使用 User-ID 源中的属性重新填充这些映射。要估计环境重新填充映射所需的时间，请在防火墙上运行以下 CLI 命令。

- 对于 IP 地址到用户名映射：
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- 对于组映射：**`show user group-mapping statistics`**

STEP 5 | 确保防火墙运行最新的内容发行版本。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后查看当前安装的 **Applications**（应用程序）或 **Applications and Threats**（应用程序和威胁）内容发行版本。
2. 如果防火墙未运行所需的最低内容发行版本或 PAN-OS 所需的更高版本，请 **Check Now**（立即检查）以获取可用更新的列表。
3. 找到并 **Download**（下载）所需的内容发行版本。

   成功下载内容更新文件后，该内容发行版本的 Action（操作）列中的链接从 **Download**（下载）更改为 **Install**（安装）。
4. **Install**（安装）更新。

©2024 Palo Alto Networks, Inc.

STEP 6 | 升级 VM 系列插件。

1. 在升级之前，请查看最新的发行说明，以获取有关新 VM 系列插件是否会影响您的环境的详细信息。

   例如，假设新的 VM 系列插件版本仅包含 AWS 功能。要利用这些新功能，您必须在 AWS 上更新 VM 系列防火墙实例上的插件。

   不要安装不适用于您的环境的升级。

2. 登录 VM 系列防火墙，检查仪表盘以查看插件版本。
3. 选择 **Device**（设备）> **Plugins**（插件）以查看插件版本。使用 **Check Now**（立即检查）以检查更新。
4. 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。

STEP 7 | 升级 PAN-OS。

如果防火墙无法从管理端口访问 *Internet*，则您可以从 Palo Alto Networks 客户支持门户下载软件映像，然后手动将其 ***Upload***（上传）到防火墙。

1. 选择 **Device**（设备）> **Software**（软件），然后单击 **Check Now**（立即检查）以显示最新的 PAN-OS 更新。
2. 找到并 **Download**（下载）目标 PAN-OS 版本。
3. 在下载映像后（或者，对于手动升级，在上传映像后），请 **Install**（安装）映像。
4. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），然后单击 **Reboot Device**（重启设备）。

   此时，防火墙将清除 *User-ID* 映射，然后连接到 *User-ID* 源以重新填充映射。
5. 如果您已启用 User-ID，请使用以下 CLI 命令在允许流量之前验证防火墙是否已重新填充 IP 地址到用户名和组映射。
   - **`show user ip-user-mapping all`**
   - **`show user group list`**
6. 如果您是第一次升级到 XFR 版本，请重复此步骤以升级到相应的 XFR 版本。

STEP 8 | 验证防火墙是否正在传递流量。

选择 **Monitor**（监控）> **Session Browser**（会话浏览器），然后验证是否显示新的会话。

©2024 Palo Alto Networks, Inc.

升级 PAN-OS 软件版本（HA 对）

使用以下程序在高可用性 (HA) 配置中升级防火墙对。此程序适用于主动/被动和主动/主动配置。

当您在高可用性 (HA) 配置中更新防火墙时，为了避免出现停机，一次只应更新一台高可用性对等：对于主动/主动防火墙，首先升级哪个对等并不重要（为简单起见，此程序介绍了首先如何升级主动-辅助对等）。对于主动/被动防火墙，您必须首先升级被动对等，挂起主动对等（故障转移），更新主动对等，然后再使该对等恢复为运行状态（故障恢复）。为了防止在升级 HA 对等期间发生故障转移，您必须确保在继续升级之前禁用抢占行为。您只需要禁用对中一个对等的抢占行为。

为避免影响流量，计划在中断时间段内进行升级。确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。

STEP 1 | 验证是否有足够的硬件资源可用于 VM 系列防火墙。

要查看每个 VM 系列型号的资源需求，请参阅 VM 系列系统要求。在继续升级过程之前分配其他硬件资源；在每个虚拟机监控程序上分配额外硬件资源的过程各不相同。

如果 VM 系列防火墙没有该模型所需的资源，则默认为与 VM-50 相关联的容量。

STEP 2 | 从 Web 界面中，导航到 **Device**（设备） > **Licenses**（许可证），确保您拥有正确的 VM 系列防火墙许可证，同时确保该许可证已被激活。

在 VM 系列防火墙独立版本中，导航到 **Device**（设备） > **Support**（支持），并确保已经激活支持许可证。

STEP 3 | 保存当前配置文件的备份。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

对该对中的每个防火墙执行以下步骤：

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Export named configuration snapshot**（导出已命名的配置快照）。
2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。
3. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

©2024 Palo Alto Networks, Inc.

STEP 4 | 如果您已启用 User-ID，则在升级后防火墙将清除当前 IP 地址到用户名和组映射，以便可以使用 User-ID 源中的属性重新填充这些映射。要估计环境重新填充映射所需的时间，请在防火墙上运行以下 CLI 命令。

- 对于 IP 地址到用户名映射：
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- 对于组映射：**`show user group-mapping statistics`**

STEP 5 | 确保 HA 对中的每个防火墙都运行最新的内容发行版本。

请参阅发行说明以了解您必须为 PAN-OS 10.2 版本安装的最低内容发行版本。请确保遵循应用程序和威胁内容更新的最佳实践。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后选择 **Applications**（应用程序）或 **Applications and Threats**（应用程序和威胁）以确定当前安装的更新。
2. 如果防火墙未运行所需的最低内容发行版本或安装软件版本所需的更高版本，请 **Check Now**（立即检查）以获取可用更新的列表。
3. 找到并 **Download**（下载）所需的内容发行版本。

   成功下载内容更新文件后，该内容发行版本的 Action（操作）列中的链接从 **Download**（下载）更改为 **Install**（安装）。
4. **Install**（安装）更新。您必须在两个对等上安装更新。

STEP 6 | 升级 VM 系列插件。

1. 在升级之前，请查看最新的发行说明，以获取有关新 VM 系列插件是否会影响您的环境的详细信息。

   例如，假设新的 VM 系列插件版本仅包含 AWS 功能。要利用这些新功能，您必须在 AWS 上更新 VM 系列防火墙实例上的插件。

   不要安装不适用于您的环境的升级。
2. 登录 VM 系列防火墙，检查仪表盘以查看插件版本。
3. 选择 **Device**（设备） > **Plugins**（插件）以查看插件版本。使用 **Check Now**（立即检查）以检查更新。
4. 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。

   在 HA 对中的 VM 系列防火墙上安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

©2024 Palo Alto Networks, Inc.

STEP 7 | 在每个对中的第一个对等上禁用抢占行为。您只需要在 HA 对中的一个防火墙上禁用此设置，但在继续升级之前确保提交成功。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 如果已启用，则禁用（取消选择）**Preemptive**（抢先）设置，然后单击 **OK**（确定）。
3. **Commit**（提交）更改。

STEP 8 | 在第一个对等上安装 PAN-OS 版本。

要最大限度减少主动/被动配置的停机时间，请首先升级被动对等。对于主动/主动配置，请首先升级辅助对等。作为最佳做法，如果您使用主动/主动配置，我们建议您在同一维护时间段内升级两个对等。



如果要在升级之前测试该 *HA* 是否正常运行，请首先考虑升级主动/被动配置中的主动对等，以确保在发生故障转移时不会发生任何事件。

1. 在第一个对等上，选择 **Device**（设备） > **Software**（软件），然后单击 **Check Now**（立即检查）以获取最新更新。
2. 找到并 **Download**（下载）目标 PAN-OS 版本。



如果防火墙无法从管理接口访问 *Internet*，则您可以从 Palo Alto Networks 支持门户下载软件映像，然后手动将其 ***Upload***（上传）到防火墙。

3. 在下载映像后（或者，对于手动升级，在上传映像后），请 **Install**（安装）映像。
4. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。
5. 设备完成重新启动后，在 **Dashboard**（仪表盘）上查看高可用性小部件，并验证刚升级的设备在 HA 配置中是否仍是被动或主动辅助对等。

©2024 Palo Alto Networks, Inc.

STEP 9 | 在第二个对等上安装 PAN-OS 版本。

1. （仅限主动/被动配置）挂起主动对等，以便 HA 故障转移至您刚升级的对等。
   1. 在主动对等上，选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然后单击 **Suspend local device**（挂起本地设备）。
   2. 在 **Dashboard**（仪表盘）上查看高可用性小部件，并验证状态是否变为 **Passive**（被动）。
   3. 在其他对等上，验证其状态是否为主动或正在传递流量（**Monitor**（监控） > **Session Browser**（会话浏览器））。
2. 在第二个对等上，选择 **Device**（设备） > **Software**（软件），然后单击 **Check Now**（立即检查）以获取最新更新。
3. 找到并 **Download**（下载）目标 PAN-OS 版本。
4. 下载映像后，请 **Install**（安装）。
5. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。
6. （仅限主动/被动配置）在刚升级的对等的 CLI 中，运行以下命令使防火墙再次运行：
   `request high-availability state functional`

STEP 10 | 验证两个对等是否按预期传递流量。

在主动/被动配置中，仅主动对等应传递流量；两个对等应在主动/主动配置中传递流量。

运行以下 CLI 命令以确认升级成功：

- （仅限主动对等）要验证主动对等是否正在传递流量，请运行 **`show session all`** 命令。
- 要验证会话同步，请运行 **`show high-availability interface ha2`** 命令，并确保 CPU 表中的硬件接口计数器按如下方式增加：
  - 在主动/被动配置中，只有主动对等显示传输的数据包；被动对等将仅显示接收的数据包。

    如果启用了 *HA2 keep-alive*，则被动对等上的硬件接口计数器将同时显示传输和接收的数据包。发生这种情况是因为 *HA2 keep-alive* 是双向的，这意味着两个对等都会发送 *HA2 keep-alive* 数据包。
  - 在主动/主动配置中，您会看到这两个对等上收到的数据包和传输的数据包。

STEP 11 | 如果在升级之前禁用抢占行为，请立即重新启用。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 选择 **Preemptive**（抢占），然后单击 **OK**（确定）。
3. **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

使用 Panorama 升级 PAN-OS 软件版本

使用以下程序升级 Panorama 管理的防火墙。此程序适用于独立防火墙和部署在高可用性 (HA) 配置中的防火墙。

如果 *Panorama* 无法直接连接到更新服务器，请按照当 Panorama 未连接 Internet 时将更新部署到防火墙程序进行操作，以便您可以手动将映像下载到 *Panorama*，然后将映像分发到防火墙。

更新 Panorama 的防火墙前，必须：

- 确保 Panorama 运行的 PAN-OS 版本与更新到的版本相同或，高于更新到的版本。在将托管防火墙升级到此版本之前，您必须将 Panorama 及其日志收集器升级到 9.1。此外，在将日志收集器升级到 9.1 时，由于日志记录基础架构的变化，因此您必须同时升级所有日志收集器。
- 在将 Panorama 升级到 9.1 时，您需要计划最多六个小时的扩展维护时间段。此版本包括重大的基础架构变化，这意味着 Panorama 升级将需要比以前版本更长的时间。
- 确保防火墙已连接至可靠的电源。升级时断电可能导致防火墙无法使用。

STEP 1 | 在升级 Panorama 后，将配置提交并推送到您计划升级的防火墙。

STEP 2 | 验证是否有足够的硬件资源可用于 VM 系列防火墙。

要查看每个 VM 系列型号的资源需求，请参阅 VM 系列系统要求。在继续升级过程之前分配其他硬件资源；在每个虚拟机监控程序上分配额外硬件资源的过程各不相同。

如果 VM 系列防火墙没有该模型所需的资源，则默认为与 VM-50 相关联的容量。

STEP 3 | 从 Web 界面中，导航到 **Device**（设备） > **Licenses**（许可证），确保您拥有正确的 VM 系列防火墙许可证，同时确保该许可证已被激活。

在 VM 系列防火墙独立版本中，导航到 **Device**（设备） > **Support**（支持），并确保已经激活支持许可证。

STEP 4 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。

尽管防火墙自动创建配置备份，但最佳做法是在升级之前创建备份并通过外部方式将其保存。

1. 从 Panorama Web 界面选择 **Panorama** > **Setup**（设置） > **Operations**（操作），然后单击 **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）以生成和导出 Panorama 和每个托管防火墙的最新配置备份。
2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

©2024 Palo Alto Networks, Inc.

STEP 5 | 更新计划更新的防火墙上的内容发行版本。

要了解 PAN-OS 10.2 所需的最低内容发行版本，请参阅发行说明。在将内容更新到 Panorama 到托管防火墙时，必须遵循应用程序和威胁更新的最佳实践。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新），然后 **Check Now**（立即检查）最近更新。如果有更新可用，Action（操作）列会显示 **Download**（下载）链接。
2. 如果尚未安装，请 **Download**（下载）最新内容发行版本。
3. 单击 **Install**（安装）并选择要在其中安装更新的防火墙，然后单击 **OK**（确定）。如果更新 HA 防火墙，则必须更新两个对等的内容。

STEP 6 | （仅限 HA 防火墙更新）如果将要更新作为 HA 对组成部分的防火墙，请禁用抢占行为。您仅需要禁用每个 HA 对上每个防火墙的此设置。

1. 选择 **Device**（设备） > **High Availability**（高可用性），然后编辑 **Election Settings**（选择设置）。
2. 如果已启用，则禁用（取消选择）**Preemptive**（抢先）设置，然后单击 **OK**（确定）。
3. **Commit**（提交）更改。必须确保已成功提交，然后才能进行更新。

STEP 7 | 下载目标 PAN-OS 版本映像。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件），然后 **Check Now**（立即检查）最新发行版本。
2. **Download**（下载）您正在升级的发行版本的防火墙特定文件。您必须下载您打算升级的每个防火墙型号（或防火墙系列）的单个安装文件。

STEP 8 | 在防火墙上安装 PAN-OS 软件更新。

1. 单击与想要更新的防火墙型号匹配的操作列中的 **Install**（安装） 。
2. 在部署软件文件对话框，选择想要升级的所有防火墙。要减少停机时间，请仅在每个 HA 对中选择一个对等。对于主动/被动对，选择主动对等；对于主动/主动对，选择主动-辅助对等。
3. （仅限 HA 防火墙升级）请勿选择 **Group HA Peers**（组 **HA** 对等）。
4. 选择**Reboot device after install**（在安装之后重新启动设备）。
5. 要开始更新，请单击 **OK**（确定）。
6. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。
7. 防火墙重启后，请选择**Panorama** > **Managed Devices**（托管设备），然后验证用于已更新的防火墙的软件版本是否是 9.1.0。此外，还检验已更新的任何被动防火墙的 HA 状态是否仍为被动。

©2024 Palo Alto Networks, Inc.

STEP 9 | （仅限 HA 防火墙更新）更新每个 HA 对中的第二个 HA 对等。

1. （仅限主动/被动升级）挂起您正在升级的每个主动/被动对中的主动设备。
   1. 切换上下文至主动防火墙。
   2. 在 **Dashboard**（仪表盘）的高可用性小部件中，验证 **Local**（本地）防火墙状态是否是 **Active**（主动），**Peer**（对等）是否是 **Passive**（被动））。
   3. 选择 **Device**（设备） > **High Availability**（高可用性） > **Operational Commands**（操作命令） > **Suspend local device**（挂起本地设备）。
   4. 返回至 **Dashboard**（仪表盘）上的高可用性小部件，然后检验 **Local**（本地）是否已更改为 **Passive**（被动），**Peer**（对等）是否已更改为 **Active**（主动）。
2. 返回至 Panorama 上下文，然后选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件）。
3. 单击与正在更新的 HA 对中防火墙型号匹配的操作列中的 **Install**（安装）。
4. 在部署软件文件对话框，选择想要升级的所有防火墙。此时，仅选择刚升级的 HA 防火墙的对等。
5. 请勿选择 **Group HA Peers**（组高可用性对等）。
6. 选择**Reboot device after install**（在安装之后重新启动设备）。
7. 要开始更新，请单击 **OK**（确定）。
8. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作）和 **Reboot Device**（重启设备）。
9. （（仅限主动/被动升级）在刚升级的对等的 CLI 中，运行以下命令使防火墙再次运行：
   ```
   request high-availability state functional
   ```

STEP 10 | （仅限 PAN-OS XFR 升级）通过重复步骤 8 和步骤 9，将第一个对等和第二个对等升级至 PAN-OS XFR。

STEP 11 | 验证每个托管防火墙上运行的软件和内容发行版本。

1. 在 Panorama 上选择 **Panorama** > **Managed Devices**（托管设备）。
2. 找到防火墙并检查表格中的内容和软件版本。

   对于 HA 防火墙，您还可以验证每个对等的 HA 状态是否符合预期。

STEP 12 | （仅限 HA 防火墙升级）如果您在升级之前禁用其中一个 HA 防火墙的抢占，请编辑 **Election Settings**（选择设置）（**Device**（设备） > **High Availability**（高可用性）），并重新启用该防火墙的 **Preemptive**（抢占）设置，然后 **Commit**（提交）更改。

升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列）

选择最适合您部署的升级方法。

©2024 Palo Alto Networks, Inc.

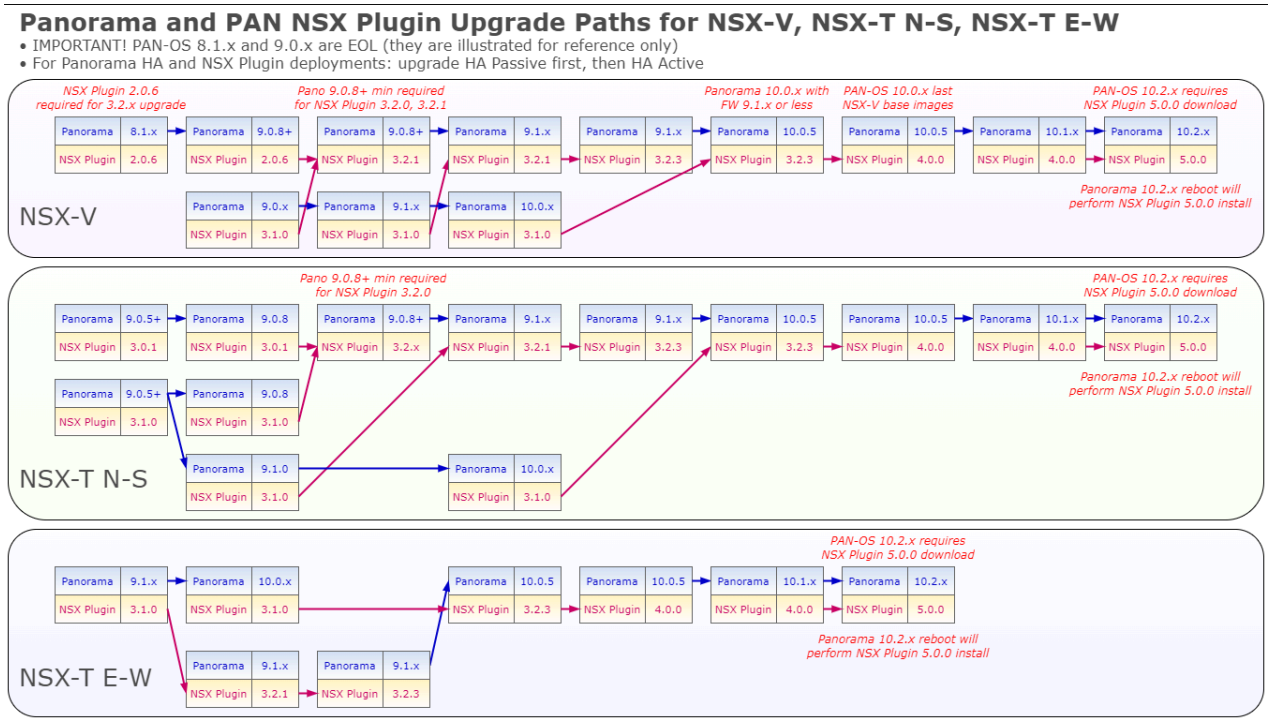
- 在维护窗口期间升级 NSX 的 VM 系列 — 使用此选项可在维护窗口期间升级 VM 系列防火墙，而无需更改服务定义中的 OVF URL。
- 在不中断流量的情况下升级 NSX 的 VM 系列 — 使用此选项升级 VM 系列防火墙而不中断对来宾 VM 的服务或更改服务定义中的 OVF URL。

下图显示了目前支持的适用于 VMware NSX 的 Panorama 和 Panorama 插件组合，以及成功升级需要遵循的升级路径。

- 下面的每个方框都代表一个受支持的组合。
- 在 HA 对中升级适用于 NSX 的 Panorama 插件或 Panorama 时，请先升级被动 Panorama 对等，然后升级主动 HA 对等。

在升级用于 VMware NSX 部署的 VM 系列之前，请查看下面所示的升级路径以了解升级步骤，从而找到最适合您的环境的插件和 PAN-OS 组件。

©2024 Palo Alto Networks, Inc.



在维护窗口期间升级 NSX 的 VM 系列

对于 VM 系列 NSX 版本防火墙，可以在防火墙上使用 Panorama 升级软件版本。

STEP 1 | 查看用于 VMware NSX 的 VM 系列升级路径。

STEP 2 | 将额外的硬件资源分配给 VM 系列防火墙。

验证是否有足够的硬件资源可用于 VM 系列防火墙。要查看每个 VM 系列型号的新资源需求，请参阅 VM 系列系统要求。分配额外的硬件资源，然后继续升级。每个虚拟机监控程序上分配额外硬件资源的过程都不相同。

©2024 Palo Alto Networks, Inc.

STEP 3 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。



尽管防火墙将自动创建配置文件的备份，但最佳实践是在升级和存储在外部设备之前创建备份。

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），并单击 **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）。该选项用于手动生成和导出 Panoram 和各托管设备的配置备份的最新版本。
2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 4 | 请参阅发行说明以确认 PAN-OS 版本所需的内容发行版本。

计划升级的防火墙必须运行 PAN-OS 版本所需的内容发行版本。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新）。
2. 检查最新更新。单击立即检查（位于窗口的左下角）以检查最新更新。操作列中的链接指示是否有更新可用。如果有版本可用，将会显示 **Download**（下载）链接。
3. 单击 **Download**（下载），下载选中的版本。成功下载后，**Action**（操作）列中的链接将从**Download**（下载）更改为**Install**（安装）。
4. 单击 **Install**（安装）并选择要在其中安装更新的设备。安装完成时，将在 **Currently Installed**（当前已安装）列中显示复选标记。

STEP 5 | 将软件更新部署到选定防火墙。



如果已使用高可用性配置防火墙，请确保取消选中 ***Group HA Peers***（对高可用性对等分组）复选框，并一次升级一个高可用性对等。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件）。
2. 检查最新更新。单击 **Check Now**（立即检查）（位于窗口的左下角）以检查最新更新。**Action**（操作）列中的链接指示是否有更新可用。
3. 检查 **File Name**（文件名称），然后单击 **Download**（下载）。验证您下载的软件版本与网络中部署的防火墙型号匹配。成功下载后，**Action**（操作）列中的链接将从**Download**（下载）更改为**Install**（安装）。
4. 单击 **Install**（安装）并选择要在其中安装软件版本的设备。
5. 选择 **Reboot device after install**（在安装之后重新启动设备），然后单击 **OK**（确定）。
6. 如果已使用高可用性配置设备，则取消选中 **Group HA Peers**（对高可用性对等分组）复选框，并一次升级一个高可用性对等。

STEP 6 | 验证每个托管设备上运行的软件和内容发行版本。

1. 选择 **Panorama** > **Managed Devices**（托管设备）。
2. 找到设备并检查表格中的内容和软件版本。

©2024 Palo Alto Networks, Inc.

在不中断流量的情况下升级 NSX 的 VM 系列

使用以下过程升级 VMware NSX 环境中 PAN-OS 版本的 VM 系列防火墙。此过程运行您通过将 VM 迁移到不同的 ESXi 主机执行 PAN-OS 升级，而不会中断流量。

STEP 1 | 查看用于 VMware NSX 的 VM 系列升级路径。

STEP 2 | 将当前配置文件的备份保存在计划要升级的每个托管防火墙上。



尽管防火墙将自动创建配置文件的备份，但最佳实践是在升级和存储在外部设备之前创建备份。

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），并单击 **Export Panorama and devices config bundle**（导出 **Panorama** 和设备配置包）。该选项用于手动生成和导出 Panoram 和各托管设备的配置备份的最新版本。
2. 将导出的文件保存到防火墙外部的位置。如果升级出现问题，您可以使用此备份还原配置。

STEP 3 | 请参阅发行说明以确认 PAN-OS 版本所需的内容发行版本。

计划升级的防火墙必须运行 PAN-OS 版本所需的内容发行版本。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Dynamic Updates**（动态更新）。
2. 检查最新更新。单击立即检查（位于窗口的左下角）以检查最新更新。操作列中的链接指示是否有更新可用。如果有版本可用，将会显示 **Download**（下载）链接。
3. 单击 **Download**（下载），下载选中的版本。成功下载后，**Action**（操作）列中的链接将从**Download**（下载）更改为**Install**（安装）。
4. 单击 **Install**（安装）并选择要在其中安装更新的设备。安装完成时，将在 **Currently Installed**（当前已安装）列中显示复选标记。

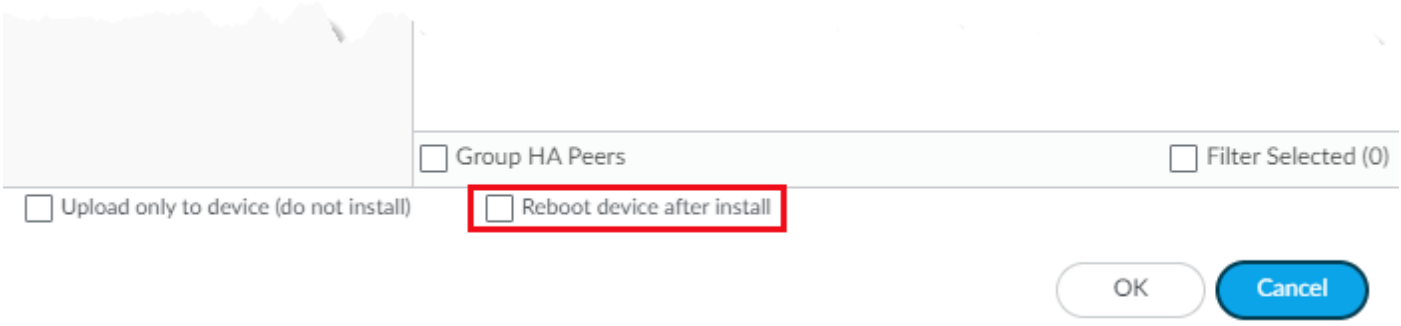
©2024 Palo Alto Networks, Inc.

STEP 4 | 将 PAN-OS 映像下载到集群中的所有 VM 系列防火墙。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Device Deployment**（设备部署） > **Software**（软件）。
3. 单击 **Refresh**（刷新）查看最新的软件版本，同时检查 **Release Notes**（发行说明）以查看版本中的更改说明和安装软件的迁移路径。
4. 单击 **Download**（下载）以检索该软件，然后单击 **Install**（安装）。

   安装新的软件映像后，请勿重新启动 *VM* 系列防火墙。

5. 选择要升级的托管设备。
6. 取消选择 **Reboot device after install**（在安装之后重新启动设备）复选框。



7. 单击 **OK**（确定）。

STEP 5 | 升级集群中是一个 ESXi 主机上的 VM 系列防火墙。

1. 登录到 vCenter。
2. 选择 **Hosts and Clusters**（主机和集群）。
3. 右键单击主机，并选择 **Maintenance Mode**（维护模式） > **Enter Maintenance Mode**（进入维护模式）。
4. 从主机（自动或主动）迁移除 VM 系列防火墙之外的所有 VM。
5. 关闭 VM 系列防火墙。这应该在主机上输入维护模式时自动发生。
6. （可选）在继续升级过程之前，为 VM 系列防火墙分配额外的 CPU 或内存。

   验证是否有足够的硬件资源可用于 VM 系列防火墙。要查看每个 VM 系列型号的新资源需求，请参阅 VM 系列型号。
7. 右键单击主机，并选择 **Maintenance Mode**（维护模式） > **Exit Maintenance Mode**（退出维护模式）。退出维护模式将导致 NSX ESX Agent Manager (EAM) 启动 VM 系列防火墙。防火墙使用新的 PAN-OS 版本重新启动。
8. 将所有 VM（自动或手动）迁移回原始主机。

STEP 6 | 为每个 ESXi 主机上每个 VM 系列防火墙重复此步骤。

©2024 Palo Alto Networks, Inc.

STEP 7 | 验证每个托管设备上运行的软件和内容发行版本。

1. 选择 **Panorama** > **Managed Devices**（托管设备）。
2. 找到设备并检查表格中的内容和软件版本。

升级 VM 系列型号

VM 系列防火墙的许可过程会使用 UUID 和 CPU ID 生成每个 VM 系列防火墙的唯一序列号。因此，在生成许可证时，此许可证会映射到 VM 系列防火墙的特定实例中，并且不能修改。

如果处于以下情况，请使用本部分中的说明：

- 从评估许可证迁移到生产许可证。
- 升级型号以便获得更大的容量。例如，您想要从 VM-100 升级到 VM-300 型号。

- 升级容量可能会重新启动防火墙上的一些关键进程。建议使用 *HA* 配置以尽量减少服务中断；要升级 *HA* 对上的容量，请参阅升级 HA 对中的 VM 系列型号。
- 在私有云或公共云部署中，如果防火墙已获得 *BYOL* 选项的许可，则您必须在更改实例类型或 *VM* 类型之前停用您的 VM。升级型号或实例会更改 *UUID* 和 *CPU ID*，因此，在以下情况下，您必须应用许可证。

STEP 1 | 将额外的硬件资源分配给 VM 系列防火墙。

在启动容量升级之前，您必须验证是否有足够的硬件资源可用于 VM 系列防火墙以支持新容量。每个虚拟机监控程序上分配额外硬件资源的过程都不相同。

要检查新 VM 系列型号的硬件要求，请参阅 VM 系列型号。

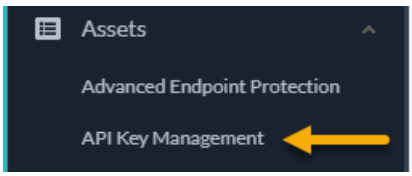
虽然容量升级不需要重新启动 VM 系列防火墙，但需要关闭虚拟机以更改硬件分配。

STEP 2 | 从客户支持门户检索许可证 API 密钥。

1. 登录到客户支持门户。

   确保您使用的是您用于注册初始许可证的相同帐户。

2. 在左侧菜单中，选择 **Assets**（资产）> **API Key Management**（**API** 密钥管理）。
3. 复制 API 密钥。



©2024 Palo Alto Networks, Inc.

STEP 3 | 在防火墙上，使用 CLI 安装上一步中复制的 API 密钥。

```
request license api-key set key <key>
```

STEP 4 | （如果可以访问 Internet）在 **Device**（设备） > **Setup**（设置） > **Service**（服务）上启用防火墙以 **Verify Update Server identity**（验证更新服务器标识）。

STEP 5 | **Commit**（提交）更改。确保防火墙上具有本地配置的用户。如果配置超过非许可的 PA-VM 对象限制，则在停用后 Panorama 推送的用户可能不可用。

STEP 6 | 升级容量。

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

- （访问 Internet）从许可证服务器检索许可证密钥 — 如果您已在客户支持门户上激活许可证，请使用此选项。
- （访问 Internet）使用授权代码 — 使用此选项升级为许可证使用授权代码的 VM 系列容量，该许可证之前在支持门户上为激活。系统提示时，输入 **Authorization Code**（授权代码），然后单击 **OK**（确定）。
- （无法访问 Internet）手动上传许可证密钥 — 如果防火墙无法通过 Internet 连接到客户支持门户，请使用此选项。从可以访问 Internet 的计算机登录 CSP，下载许可证密钥文件，将其传输到与防火墙处于同一网络的计算机，然后将其上传到防火墙。

STEP 7 | 验证防火墙已成功获得许可。

在 **Device**（设备） > **Licenses**（许可证）页面上，验证是否已成功激活许可证。

升级 HA 对中的 VM 系列型号

升级 VM 系列防火墙可以增加防火墙的容量。容量根据 VM 系列防火墙最适合处理的会话、规则、安全区域、地址对象、IPSec VPN 隧道和 SSL VPN 隧道的数量定义。当您在 VM 系列防火墙上应用新容量许可证时，型号及相关的容量将在防火墙上实施。

在升级之前，请验证防火墙型号的 VM 系列系统要求。如果防火墙的存储空间小于 *5.5GB*，则防火墙上的容量（会话、规则、安全区域、地址对象等的数量）将限制为 *VM-50 Lite* 的容量。

该过程类似于升级处于 HA 配置中的一对基于硬件的防火墙。在容量升级过程中，如果启用了会话同步，则会继续进行会话同步。当您在高可用性 (HA) 配置中更新防火墙时，为了避免出现停机，一次只应更新一台高可用性对等。

©2024 Palo Alto Networks, Inc.

在升级过程中，不要对防火墙执行配置更改。在升级过程中，当检测到容量不匹配时会自动禁用配置同步，并在两个 *HA* 对等机具有匹配的容量许可证时重新启用配置同步。

如果 *HA* 对中的防火墙具有不同的主要软件版本（如 *9.1* 和 *9.0*）和不同的容量，则两个设备都将进入 *Suspended HA*（*HA* 挂起）状态。因此，建议您在升级容量之前确保两个防火墙都运行相同版本的 *PAN-OS*。

STEP 1 | 升级被动防火墙上的容量许可证。

按照以下过程升级 VM 系列型号。

在此被动对等上重新启动某些进程后，指示板上将显示新的 VM 系列型号。由于与活动对等的容量不匹配，现在，升级后的对等处于无效状态。

如果已启用会话同步，请在继续下一步之前验证会话是否在 HA 对等之间同步。要验证会话同步，请运行 **`show high-availability interface ha2`** 命令并确保 CPU 表上的硬件接口计数器按如下方式递增：

- 在主动/被动配置中，只有主动对等显示传输的数据包，而被动设备将仅显示接收的数据包。

  如果启用了 HA2 keep-alive，则被动对等上的硬件接口计数器将同时显示传输和接收数据包。发生这种情况是因为 HA2 保持活动状态是双向的，这意味着两个对等都会发送 HA2 保持活动的数据包。
- 在主动/主动配置中，您会看到这两个对等上收到的数据包和传输的数据包。

STEP 2 | 升级主动防火墙上的容量许可证。

按照程序升级 VM 系列型号。

关键流程重新启动后，新的 VM 系列型号将显示在仪表盘上。被动防火墙变为活动状态，并且该对等（以前活动的防火墙）从初始状态转变为 HA 对中的被动对等。

将 VM 系列防火墙降级到上一版本

使用以下工作流程以还原在升级到其他功能版本之前正在运行的配置。自升级以来所做的任何更改都将丢失。因此，请务必备份当前配置，这样您可以在返回较新版本时还原这些更改。

使用以下过程降级到上一版本。

STEP 1 | 保存当前配置文件的备份。

尽管防火墙将自动创建配置文件的备份，但最佳做法是在升级和存储在外部设备之前创建备份。

1. **Export named configuration snapshot**（导出已命名的配置快照）（**Device**（设备）> **Setup**（设置）> **Operations**（操作））。
2. 选择包含正在运行的配置（如 **running-config.xml**）的 XML 文件，并单击 **OK**（确定）导出配置文件。

©2024 Palo Alto Networks, Inc.

3. 将导出的文件保存到防火墙外部的位置。如果降级出现问题，您可以使用此备份还原配置。

STEP 2 | 安装上一功能版本映像。

升级到新版本时，将创建自动保存版本。

1. **Check Now**（立即检查）（**Device**（设备） > **Software**（软件））可用的映像。
2. 找到您要降级的映像。如果尚未下载映像，请 **Download**（下载）。
3. 下载完成后，请 **Install**（安装）映像。
4. **Select a Config File for Downgrading**（选择用于降级的配置文件），防火墙将会在重启设备后加载该文件。在大多数情况下，您应选择在从现在正在降级的版本升级时自动保存的配置。例如，如果您正在运行 PAN-OS 9.1 并降级到 PAN-OS 9.0.3，则应选择 `autosave-9.0.3`。
5. 安装成功完成后，请使用以下方法之一重新启动：
   - 如果提示重新启动，请单击 **Yes**（是）。
   - 如果未提示重启，请转到 Device Operations（设备操作）（**Device**（设备） > **Setup**（设置） > **Operations**（操作）），然后 **Reboot Device**（重启设备）。

©2024 Palo Alto Networks, Inc.

VM 系列插件

VM 系列防火墙包括 VM 系列插件，这是一种内置插件架构，可与公共云提供商或私有云虚拟机监控程序集成。VM 系列插件可以独立于 PAN-OS 进行手动升级，使 PaloAltoNetworks® 能够加速新功能、修复，或与新的云提供商或虚拟机监控程序集成的发布。

通过 VM 系列插件，您可以管理 VM 系列防火墙与支持的公共云平台（AWS、GCP 和 Azure）之间的特定于云的交互。该插件可以将自定义指标发布到云监控服务（例如 AWS CloudWatch），从公共云环境引导，配置用户凭据预配信息，以及在 PAN-OS 上无缝更新云库或代理。

VM 系列插件不管理 *VM* 系列防火墙和基于硬件的防火墙共有的功能。例如，*VM* 监控不是 *VM* 系列插件的一部分，因为它是一个核心 *PAN-OS* 功能，可帮助您在 *VM* 系列防火墙和基于硬件的防火墙的虚拟机工作负载上一致地实施策略。

VM 系列插件无法管理 Panorama 插件。有关 *VM* 系列插件和 *Panorama* 插件之间的区别，请参阅 VM 系列插件和 Panorama 插件。

VM 系列插件是一个内置组件，可以升级或降级，但不能删除。每个 PAN-OS 版本都包含与 PAN-OS 软件版本对应的特定 VM 系列插件版本。当您降级到较早的 PAN-OS 软件版本时，插件版本将降级为与 PAN-OS 版本兼容的版本。您可以在虚拟防火墙上本地升级或降级 VM 系列插件，或者从 Panorama 集中管理插件版本。

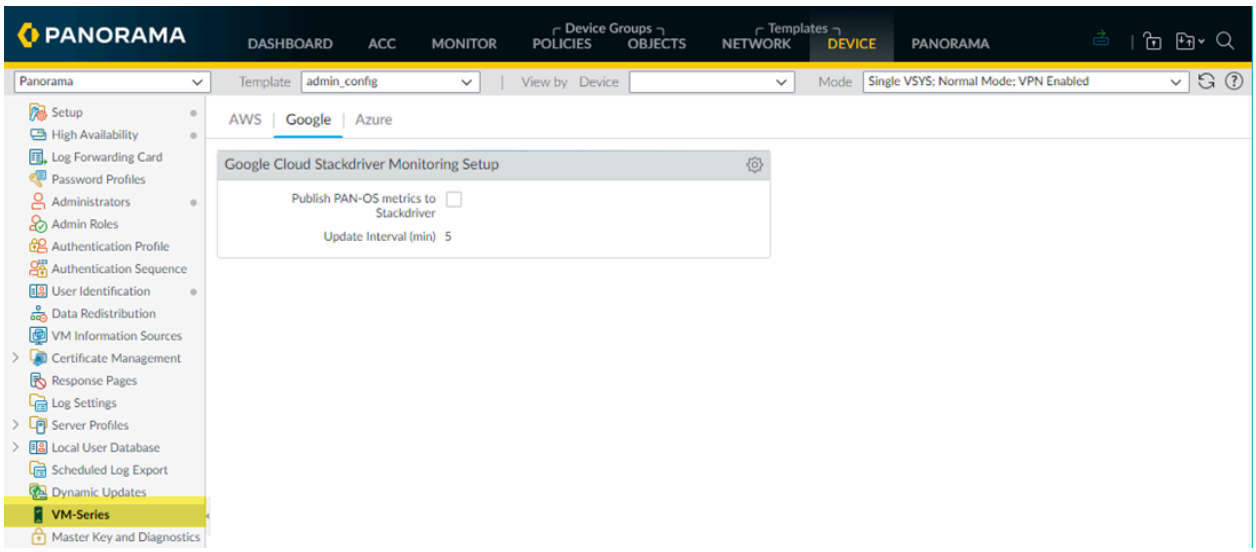
要使 Panorama 能够管理 VM 系列插件版本本身，或者发布托管防火墙的特定于云的指标，您必须在 Panorama 上手动安装 VM 系列插件，如 Panorama 插件中所述。

- 在防火墙上配置 VM 系列插件
- 升级 VM 系列插件

在防火墙上配置 VM 系列插件

选择 **Device**（设备） > **VM-Series**（**VM** 系列），为部署此 VM 系列防火墙实例的云提供商配置插件集成。

©2024 Palo Alto Networks, Inc.



如果防火墙部署在没有公共接口的虚拟机管理程序或云（例如 VMware ESXi）上，则该选项卡将命名为“VM 系列”并显示常规消息。

升级 VM 系列插件

当独立于 PAN-OS 发布插件更新时，您可以从 VM 系列防火墙（如软件或内容更新）或引导程序文件中独立升级插件版本。

每个插件版本都提供 PAN-OS 兼容性信息，且包含一个或多个云环境的新功能或错误修复。

STEP 1 | 在升级之前，请查看最新的发行说明，以获取有关新 VM 系列插件是否会影响您的环境的详细信息。

例如，假设新的 VM 系列插件版本仅包含 AWS 功能。要利用这些新功能，您必须在 AWS 上更新 VM 系列防火墙实例上的插件。

不要安装不适用于您的环境的升级。

仅 *PAN-OS 10.2.0* 中支持 *VM* 系列 *3.0.0* 插件。

©2024 Palo Alto Networks, Inc.

STEP 2 | 登录 VM 系列防火墙，检查仪表盘以查看插件版本。

System Mode	panorama
Software Version	10.0.2
Application Version	8335-6370 (10/26/20)
Device Dictionary Version	10-238 (10/30/20)
Time	Mon Nov 2 17:29:10 2020
Uptime	7 days, 0:31:54
Plugin Azure	azure-2.0.3
Plugin Interconnect	interconnect-1.0.2
Plugin SD WAN plugin	sd_wan-1.0.3
Plugin Cisco TrustSec Monitoring Plugin	cisco_trustsec-1.0.2
Plugin VM series	vm_series-2.0.1
Plugin AWS	aws-3.0.0

STEP 3 | 选择 **Panorama** > **Plugins**（插件），然后在搜索字段中键入 **`vm_series`**。

选择 **Check Now**（立即检查）以查看可用版本。

STEP 4 | 选择 VM 系列插件版本，然后单击 **Download**（下载）。

vm_series 1743 / 1600

FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL
Name: vm_series							
vm_series-1.0.5	1.0.5	Built-in	15M			Download	Release Notes
vm_series-2.0.0	2.0.0	Built-in	9M	✓		Install Delete	
vm_series-2.0.1	2.0.1	Built-in	9M	✓		Install Delete	
vm_series-2.0.2	2.0.2	Built-in	9M	✓	✓	Remove Config Uninstall	

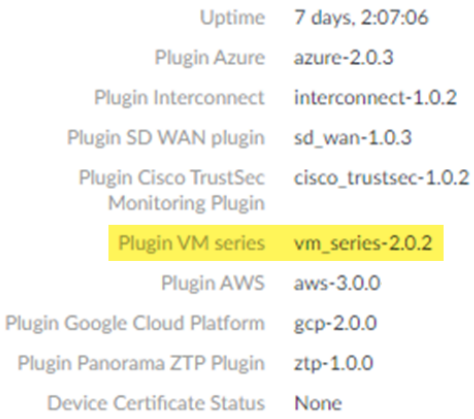
Check Now Upload

STEP 5 | 下载完成后，单击 **Actions**（操作）列中的 **Install**（安装）。

防火墙自动卸载之前安装的插件版本。

©2024 Palo Alto Networks, Inc.

STEP 6 | 查看 **Dashboard**（仪表盘）以验证插件是否成功升级。



 ©2024 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用 Jumbo 帧

在默认情况下，第 3 层接口上发送的数据包的最大传输单元 (MTU) 大小为 1500 字节。根据每个接口的具体情况，可将此大小手动设置为 512-1500 字节之间的任何大小。一些配置要求 Ethernet 帧具备大小超过 1500 字节的 MTU。这便称为 Jumbo 帧。

如需在防火墙上使用 Jumbo 帧，您必须特定启用全球级的 Jumbo 帧。如启用，则会将所有第 3 层接口的 MTU 大小默认设置为 9192 字节。此默认值可被重新设置为 512-9216 字节之间的任何值。

设置全球 Jumbo 帧大小后，它将成为所有在接口配置水平上未明确设定 MTU 值的第 3 层接口的默认值。如果您只想在某些接口上交换 Jumbo 帧，那么这可能会出现问题。在此情况下，您必须在每个您不想使用默认值的第 3 层接口上设置 MTU 值。

以下流程描述了如何在防火墙上启用 Jumbo 帧，为所有第 3 层接口设置默认的 MTU 值，然后再为特定接口设置不同的值。

VM 系列防火墙实例使用多个 *NUMA* 节点部署，在启用 *Jumbo* 帧支持时以 *PacketMMAP* 模式出现。您必须禁用 *Jumbo* 帧支持才能在使用多个 *NUMA* 节点部署的 *VM* 系列防火墙实例上使用 *DPDK*。

STEP 1 | 启用 Jumbo 帧并设置默认的全球 MTU 值。

1. 选择 **Device**（设备） > **Setup**（设置） > **Session**（会话），然后编辑 Session Settings（会话设置）部分。
2. 选择 **Enable Jumbo Frame**（启用 **Jumbo** 帧）。
3. 输入 **Global MTU**（全球 **MTU**）的值。

   默认值是 9192。可接受值的范围是：512 - 9216。
4. 单击 **OK**（确定）。

   之后将显示一条消息，提示您启用或禁用 Jumbo Frame 模式需要进行重启且第 3 层接口要继承 **Global MTU**（全球 **MTU**）值。
5. 单击 **Yes**（是）。

   之后将显示一条消息，提示您已启用 Jumbo Frame 支持，而如需激活此更改，则需重启设备。
6. 单击 **OK**（确定）。
7. 单击 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 设置第 3 层接口的 MTU 值并重启防火墙。

为此接口设置的值将替代全球 *MTU* 值。

1. 选择 **Network**（网络） > **Interfaces**（接口）。
2. 选择第 3 层 **Interface type**（接口类型）的接口。
3. 选择 **Advanced**（高级） > **Other Info**（其他信息）。
4. 输入 **MTU** 的值。

   默认值是 9192。可接受值的范围是：512 - 9216。
5. 单击 **OK**（确定）。
6. 单击 **Commit**（提交）。
7. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后选择 **Reboot Device**（重启设备）。

©2024 Palo Alto Networks, Inc.

虚拟机监控程序分配的 MAC 地址

默认情况下，VM 系列防火墙使用主机/虚拟机监控程序将 MAC 地址分配给物理接口，以通过第 3 层接口部署 VM 系列防火墙上。然后，防火墙会在其 ARP 响应中使用虚拟机监控程序分配的 MAC 地址。这一功能可使 VMware vSwitch 等非学习型交换机将流量转发至防火墙上的数据面板接口，而无需在 vSwitch 上启用混杂模式。如果混杂模式和虚拟机监控程序分配的 MAC 地址均未启用，那么，当主机检测到接口的目标 MAC 地址与主机分配的 MAC 地址不匹配时，它会丢弃帧。



没有选项可启用或禁用在 *AWS* 和 *Azure* 上使用虚拟机监控程序分配的 *MAC* 地址。它在两个平台上默认启用，不能被禁用。

如果使用第 2 层接口、虚拟线路或旁接接口模式部署 VM 系列防火墙，必须在防火墙所连接的虚拟交换机上启用混杂模式。使用虚拟机监控程序分配的 MAC 地址仅适用于第 3 层接口模式下的部署，其中防火墙一般作为来宾虚拟机的默认网关。

如果已在 VM 系列防火墙上启用虚拟机监控程序分配的 MAC 地址功能，请记住以下要求：

- 接口上的 **IPv6** 地址 — 在主动/被动 HA 配置（请参阅 高可用性中的 VM 系列）中，使用 IPv6 地址的第 3 层接口不得使用 EUI-64 生成的地址作为接口标识符（接口 ID）。因为，如果 EUI-64 使用接口的 48 字节 MAC 地址来推导此接口的 IPv6 地址，则 IP 地址将不是静态地址。如果在故障转移时，托管 VM 系列防火墙的硬件发生更改，这将使 HA 对等的 IP 地址发生更改，进而导致 HA 故障。
- 租借 **IP** 地址 — 当 MAC 地址更改时，DHCP 客户端、DHCP 中继和 PPPoE 接口可能会重新租借 IP 地址，因为原始 IP 地址租借可能已终止。
- **MAC** 地址和 **Gratuitous ARP**— 就 MAC 寻址而言，在高可用性配置中，使用虚拟机监控程序分配的 MAC 地址的 VM 系列防火墙会表现出与硬件设备不同的行为。硬件防火墙使用 HA 对中设备之间自生成的浮动 MAC 地址，而在各数据面板接口（如 eth 1/1）上使用的唯一 MAC 地址将被 HA 对等上数据面板接口通用的虚拟 MAC 地址所替代。您在 HA 中的 VM 系列防火墙上启用虚拟机监控程序分配的 MAC 地址后，虚拟 MAC 地址将不再被使用。各 HA 对等上的数据面板接口均为虚拟机监控程序指定的唯一接口。

  鉴于各数据面板接口具有唯一的 MAC 地址，当发生故障转移时，当前活动的 VM 系列防火墙必须发送 Gratuitous ARP，以便邻近设备能够了解已更新的 MAC/IP 地址对。因此，如需启用有状态故障转移，网络设备不得阻止或忽略 Gratuitous ARP；必要时，请确保在 Internet 设备上禁用反向 ARP 配置功能。

要配置 VM 系列防火墙以使用主机/虚拟机监控程序提供的接口 MAC 地址，请执行以下步骤。

STEP 1 | 选择 **Device**（设备） > **Management**（管理） > **Setup**（设置） > **General Settings**（常规设置）。

STEP 2 | 单击 **Edit**（编辑）图标。

©2024 Palo Alto Networks, Inc.

STEP 3 | 选中选项以 **Use Hypervisor Assigned MAC Address**（使用虚拟机监控程序分配的 **MAC** 地址）。

当 MAC 地址发生更改时，防火墙将生成系统日志以记录此转换，同时接口将生成 Gratuitous ARP。

STEP 4 | 单击 **OK**（确定）。

STEP 5 | 在防火墙上 **Commit**（提交）更改。您无需重启防火墙。

©2024 Palo Alto Networks, Inc.

发布用于监控的自定义 PAN-OS 指标

防火墙本身将以下指标发布到 AWS® CloudWatch、Azure® Application Insights 和 Google® Stackdriver 等公共云中的监控系统。通过这些指标，您可以评估防火墙性能和使用模式，从而设置警报，并采取措施以自动化启动或终止 VM 系列防火墙实例等事件。因为这些指标通过防火墙上的内容更新予以发布，因此，必须具备启用 VM 系列防火墙上此功能所需的最低内容发行版本。

指标	说明
数据面 **CPU** 利用率 **(%)**	监控数据面板 CPU 使用情况，并测量防火墙上的流量负载。
数据面数据包缓冲区利用率 **(%)**	监控数据面板缓冲区使用情况，并测量缓冲区利用率。如果流量突然激增，监控缓冲区利用率允许您确保防火墙不会耗尽数据面板缓冲区，从而丢弃数据包。
GlobalProtect™ 网关活动隧道	监控部署为 GlobalProtect 网关的防火墙上活动的 GlobalProtect 会话数量。如果此 VM 系列防火墙作为 VPN 网关以保护远程用户，请使用此指标。检查数据表以获取支持您防火墙型号的最大活动隧道数。
GlobalProtect 网关隧道利用率 **(%)**	监控网关上的活动 GlobalProtect 隧道，并测量隧道利用率。如果此 VM 系列防火墙作为 VPN 网关以保护远程用户，请使用此指标。
panSessionConnectionsPerSecond	监控每秒新连接建立速率。
panSessionThroughputKbps	监控吞吐量（以 Kbps 为单位）。
panSessionThroughputPps	监控每秒数据包数量。
活动会话	监控防火墙上活动的会话总数。活动会话是流查找表上的会话，根据策略要求将检查和转发数据包。
会话利用率 **(%)**	监控当前活动的 TCP、UDP、ICMP 和 SSL 会话，数据包速率，新连接建立速率，以及防火墙吞吐量，以确定会话利用率。
SSL 代理利用率 **(%)**	监控客户端的 SSL 转发代理会话的 SSL/TLS 解密百分比。

要发布这些指标，请参阅：

- 在 VM 系列防火墙上启用 CloudWatch 监控

©2024 Palo Alto Networks, Inc.

- 在 VM 系列防火墙上启用 Azure Application Insights
- 在 VM 系列防火墙上启用 Google Stackdriver Monitoring

©2024 Palo Alto Networks, Inc.

用于访问 VM 系列防火墙上外部服务的接口

要访问 Palo Alto Networks 服务器以检索许可证、软件和内容更新，并发布自定义 PAN-OS 或在您的配置中检索用于监控虚拟机的 IP 地址和标记映射，除另有说明外，VM 系列防火墙应使用管理接口。要使用数据面板接口，而非支持的管理接口，必须设置指定防火墙可用于访问服务器或服务的数据平面接口的服务路由。

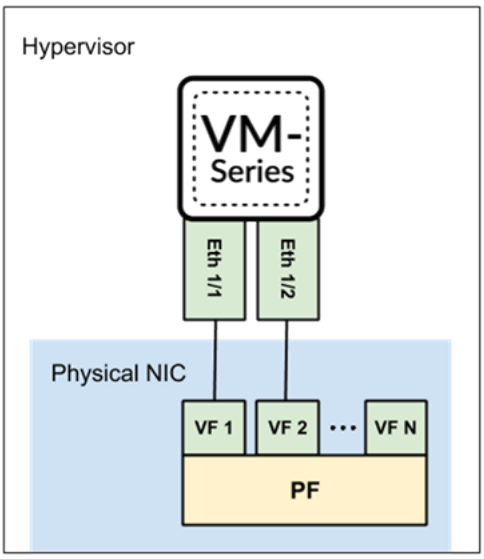
访问服务器或服务	**VM** 系列防火墙上使用的接口
许可	仅管理接口
软件更新	管理接口或服务路由
从云存储位置（如 AWS S3 存储桶、Azure 存储文件服务或 Google 存储桶）引导	仅管理接口（交换接口时包括） 如果您的 *bootstrap.xml* 文件包括许可证授权代码，则无法使用服务路由。要为防火墙授予许可，必须使用管理接口。
将 PAN-OS 指标发布到云监控服务，如 AWS CloudWatch、Azure Application Insights 或 Google Stackdriver	仅管理接口（交换接口时包括）
VM 监控	管理接口或服务路由

©2024 Palo Alto Networks, Inc.

PacketMMAP 和 DPDK 驱动程序支持

单根输入/输出虚拟化 (SR-IOV) 依赖于 VM 系列防火墙上虚拟功能 (VF) 驱动程序与主机（虚拟机监控程序）上物理功能 (PF) 驱动程序之间的通信。主机使用 PF 驱动程序与其物理 NIC 进行通信，VM 系列防火墙使用 VF 驱动程序与 PF 驱动程序进行通信。

下图是该概念的可视化示例。



SR-IOV

为什么使用 SR-IOV？SR-IOV 是一种数据包加速技术，能让虚拟机直接从 NIC 访问数据包。相反，当使用虚拟交换机时，主机将处理数据包，通过虚拟交换机发送数据包，然后虚拟机接收其数据包。

在兼容性矩阵中，PacketMMAP 驱动程序版本列出了 VM 系列防火墙上的主机版本和本机驱动程序版本。例如，主机上的 i40e 和防火墙上的 i40e（用于 PCI-passthrough）和 i40evf（用于 SR-IOV）。

对于 SR-IOV，考虑使用 i40e PF 驱动程序的 NIC。主机通过 i40e 驱动程序与 NIC 进行通信。VM 系列防火墙可以使用其 VF 驱动程序 (i40evf) 直接与主机的 PF 驱动程序进行通信。这可以让 VM 系列防火墙直接访问，从而提高数据包处理速度。要确保兼容性，请安装比本机 PF 驱动程序版本更高的主机 PF 驱动程序版本。

PCI-Passthrough

为什么 VM 系列防火墙具有本机 PF 驱动程序？如在网络上附加 VM 系列的选项中所述，当使用 PCI-passthrough 时，NIC 是为 VM 系列防火墙所保留，因此主机（或主机上的其他来宾）无法访问 NIC。在 PCI-passthrough 配置中，VM 系列防火墙使用其本机 PF 驱动程序直接与主机 NIC 进行通信。

请参阅 PacketMMAP 驱动程序版本列表，以确定要在主机上安装的 PF 驱动程序版本。安装高于 VM 系列防火墙本机 PF 驱动程序的 PF 版本。

©2024 Palo Alto Networks, Inc.

对于 PCI-Passthrough，请参阅在 ESXi 上启用 SR-IOV 和在 KVM 上启用 SR-IOV。

DPDK

PAN-OS 具有两种数据包处理模式：DPDK（默认）和 MMAP；在 VM 系列防火墙上每种模式都有一个相应的本机驱动程序。例如，如果防火墙处于 DPDK 模式，则防火墙使用 DPDK i40evf 驱动程序版本与主机的 i40e 驱动程序进行通信（使用 SR-IOV 时）。或者，如果防火墙处于 Packet MMAP 模式，则防火墙将使用其他 i40evf 驱动程序版本与主机的 i40e 驱动程序进行通信。

您可以在主机（虚拟机监控程序）或来宾（VM 系列防火墙）上启用 DPDK。同时启用两种模式可获取最佳结果。

- 使用 DPDK 编译 OVS 是在主机上启用 DPDK 的一部分。

  请参阅在主机上配置 OVS 和 DPDK。
- VM 系列 DPDK 在 VM 系列防火墙上启用本机 DPDK 驱动程序，因此无需在主机上启用 DPDK，但建议同时启用以获取最佳性能。

©2024 Palo Alto Networks, Inc.

在 VM 系列上启用 NUMA 性能优化

要提高 VM 系列防火墙的性能，您可以启用非一致性内存访问 (NUMA) 性能优化。启用 NUMA 性能优化后，VM 系列防火墙数据平面使用连接到 NUMA 节点 0 的 vCPU。VM 系列防火墙数据平面仅使用属于 NUMA 节点 0 的 vCPU。VM 系列管理平面使用核心 0，而 VM 系列数据平面则使用 NUMA 节点 0 上的其他 vCPU。此功能需要 PAN-OS 10.1.1 或更高版本和 VM 系列插件 2.1.1 或更高版本。

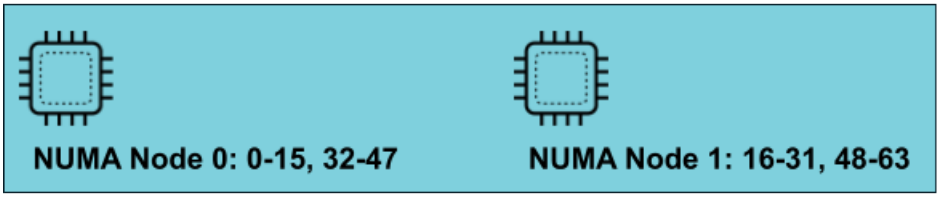
默认情况下，在 PAN-OS 10.1 中禁用 NUMA 性能优化。

如果您的设备在两个 NUMA 节点上包含 64 个核心，则在未启用 NUMA 性能优化时，VM 系列防火墙使用的数据平面 vCPU 可能位于不同的节点上，这会影响性能。例如，如果您的系统按照以下示例进行组织，则可以部署具有总共 32 个核心和 24 个数据平面核心的 VM 系列防火墙。

如果未启用 NUMA 性能优化，则 VM 系列防火墙在节点 0 上使用核心 1 到 15，在节点 1 上使用核心 16 到 24，因为系统按数字顺序分配核心，而不考虑节点位置。启用 NUMA 性能优化后，VM 系列仅使用节点 0 上的核心，本示例中为核心 1 到 15 和核心 33 到 39，不管数字顺序如何。将数据平面未使用的任何核心都分配给管理平面。

对于自定义数据平面核心设置，使用 NUMA 性能优化时，NUMA 设置优先。例如，对于启用了 NUMA 性能优化且数据平面核心设置为 47 的 64 CPU VM，NUMA 设置优先。

如果分配给 *VM* 系列防火墙的核心数量超过节点 *0* 上的 *vCPU* 数量，则 *VM* 系列使用节点 *0* 上的所有核心，而不使用其他节点的任何核心。例如，如果您为 *VM* 系列防火墙分配 *30* 个核心，但节点 *0* 只有 *24* 个核心，则 *VM* 系列防火墙仅将节点 *0* 上的 *24* 个核心用于数据平面。



STEP 1 | 登录 VM 系列 CLI。

STEP 2 | 执行以下命令。

```
request plugins vm_series numa-perf-optimize enable on
Previous NUMA performance optimization:None
Requested NUMA performance optimization:Enabled
Please reboot the PA-VM.
```

STEP 3 | 重新启动完成后，登录 VM 系列 CLI 并验证是否启用 NUMA 性能优化。

```
show plugins vm_series numa-perf-optimize
NUMA performance optimization:Enabled
```


©2024 Palo Alto Networks, Inc.

STEP 4 | 验证数据平面核心数。

```
show plugins vm_series dp-cores
```

```
Current DP cores:31 configured custom DP cores:47 (Current total
cores:64)
```

STEP 5 | 要禁用 NUMA 性能优化，请使用以下命令。此命令要求您重新启动 VM 系列防火墙。

```
request plugins vm_series numa-perf-optimize enable off
```


©2024 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用 ZRAM。

如果 VM 系列防火墙遇到内存不足的情况，您可以启用 ZRAM 以提高内存使用率。ZRAM 也称为 compcache（压缩缓存），是 Linux 内核模块，用于在 RAM 中创建压缩块设备。启用后，ZRAM 用作交换磁盘并允许更快交换 I/O，因为它驻留在 RAM 中。

完成以下步骤以启用 ZRAM。

STEP 1 | 登录 VM 系列 CLI。

STEP 2 | 使用以下 CLI 命令查找 VM 上的总内存。

```
grep pattern “KiB Mem :” mp-log mp-monitor.log
```

```
KiB Mem :9202656 total, 566504 free, 3475840 used, 5160312 buff/
cache KiB Mem :9202656 total, 497112 free, 3481944 used, 5223600
 buff/cache KiB Mem :9202656 total, 511744 free, 3466768 used,
 5224144 buff/cache KiB Mem :9202656 total, 511668 free, 3466340
 used, 5224648 buff/cache KiB Mem :9202656 total, 512124 free,
 3465700 used, 5224832 buff/cache KiB Mem :9202656 total, 511436
 free, 3465976 used, 5225244 buff/cache KiB Mem :9202656 total,
 510984 free, 3465944 used, 5225728 buff/cache
```

STEP 3 | 将上述总内存从 KB 转换为 MB。例如：

9202656 / 1024 = 8987 MB

记下总内存值（以 MB 为单位）。您将在下一步中需要此值。

STEP 4 | 使用以下两个 CLI 命令启用 ZRAM。

```
debug software kernelcfg zram-swap enable
```

```
debug software kernelcfg zram-swap modify host-mem-threshold <total-
memory-in-MB>
```

STEP 5 | 重新启动 VM 系列防火墙。

STEP 6 | 验证是否启用 ZRAM。

```
debug software kernelcfg zram-swap show config
```


©2024 Palo Alto Networks, Inc.

授权 VM 系列防火墙许可证

VM 系列防火墙支持两种许可证类型（BYOL 和 PayGo）和两种不同的许可型号：软件新一代防火墙积分（软件 NGFW），用于您使用部署配置文件指定的灵活配置；固定 VM 系列型号配置。此外，这两种许可型号还可以许可安全服务和其他功能。

如果您是授权的 CSSP 合作伙伴，请参阅云安全服务提供商许可证 (CSSP) 获取与您有关的信息。

有关创建支持帐户和管理许可证的详细信息，请参阅以下主题：

- VM 系列防火墙许可
- 创建支持帐户
- VM 系列防火墙的序列号和 CPU ID 格式
- 使用基于 Panorama 的软件防火墙许可证管理
- 软件 NGFW 积分
- VM 系列型号
- 云安全服务提供商许可证 (CSSP)

VM 系列防火墙许可

本章比较了以下许可证信息：

- 许可证类型：BYOL 与 PayGo
- 灵活 vCPU 和固定型号许可：灵活 vCPU 与固定型号
- 灵活 vCPU 和固定型号部署：灵活和固定型号的部署步骤摘要。

许可证类型

不可再购买新容量许可证（非软件 *NGFW* 积分）。但是，您可以为容量（永久和基于期限）许可证续订一 *(1)* 年。

目前，Palo Alto Networks 支持两种许可证类型：自带许可证 (BYOL) 和 PAYG（现收现付，也称为 PayGo）。

类型	说明
BYOL	软件 NGFW 积分 — 在运行所有 PAN-OS 版本的 VM 系列防火墙上可用。运行 PAN-OS 版本 10.0.4 及更高版本的 VM 系列防火墙可提供高级功能和更大的灵活性。灵活许可证成本基于 vCPU 数量、您启用的安全服务以及您是选择配置 Panorama 来管理防火墙还是充当日志收集器。 有关详细说明，请参阅软件 NGFW 积分。
BYOL	VM 系列型号许可证 — 适用于所有 PAN-OS 版本。vCPU 的数量根据您选择的 VM 系列型号固定。 灵活 *vCPU* 适用于 *PAN-OS 10.0.4* 及更高版本，支持高级功能和更多 *vCPU*。 容量许可证成本基于 VM 系列型号、设备内存、存储成本和支持权利。用于管理防火墙的安全服务和 Panorama 部署是额外成本。容量许可证类型为： • **VM** 系列企业许可协议（多型号 **ELA**） — VM 系列防火墙的为期一年或三年的综合许可协议。个人许可证可以包括型号、安全服务、支持权利和 Panorama 的可选设备管理许可证。 多型号 ELA 采用令牌池，您可以从中分配令牌以许可 VM 系列防火墙。（令牌池是 ELA 独有，与软件 NGFW 积分池不同。） • 具有支持权利和/或安全服务套餐 1 或套餐 2 的永久 VM 系列型号容量许可证。 • 具有支持权利和您选择的安全服务的期限防火墙容量许可证。

©2024 Palo Alto Networks, Inc.

类型	说明
PayGo	从公共云市场（例如 AWS、Azure 或 GCP）或云安全服务提供商 (CSSP) 购买。在您的提供商支持的 PAN OS 版本上可用。 在 9.1.1 之前的 PAN-OS 版本上，PayGo 仅支持 VM 系列 VM-300 型号。对于 PAN-OS 9.1.1 及更高版本，PayGo 可以支持固定型号。支持传统的 VM 型号，例如 VM-100、VM-300、VM-500 和 VM-700。

灵活 vCPU 和固定型号许可

灵活 vCPU 软件 NGFW 许可和固定 vCPU VM 系列型号许可有什么区别？它们为不同的项目收费，以不同的方式提供资助。下表提供了快速比较和指向更多详细信息的链接。

	灵活 **vCPU**	**VM** 系列型号（固定 **vCPU**）
说明	成本基于 vCPU 的数量和所选的安全服务。 除了消耗的 vCPU 之外，Panorama 没有任何其他成本。 您购买的可重复使用的软件 NGFW 积分将在预定期限结束时到期。激活积分后，您可以将其分成积分池。 要使用您的配额，请选择一个信用配置文件并创建一个或多个部署配置文件。选择自己的防火墙即平台组件组合：VM 系列 vCPU、安全服务、用于管理或专用日志收集的虚拟 Panorama 以及支持权利。使用配置文件部署的所有防火墙都使用同一授权代码许可，您可以从部署配置文件进行管理。	成本基于 VM 系列型号容量许可证、设备内存和存储。Panorama 和安全服务要单独购买。 • VM 系列企业许可协议（多型号 ELA） — VM 系列防火墙的为期一年或三年的综合许可协议。 多型号 ELA 采用令牌池，您可以从中分配令牌以许可 VM 系列防火墙。 • 具有支持权利和/或安全服务套餐 1 或套餐 2 的永久 VM 系列型号容量许可证。 • 具有支持权利和您选择的安全服务的期限防火墙容量许可证。
激活	需要激活电子邮件。激活和注册自动进行。	需要激活电子邮件和激活后的单独注册步骤。
安全服务	威胁预防、DNS 安全、GlobalProtect、WildFire、URL 筛选、SD-WAN、DLP 和其他可用服务。	套餐 **1**：威胁预防和高级支持权利。 套餐 **2**：威胁预防、DNS 安全、GlobalProtect、WildFire、URL 筛选、SD-WAN、DLP 和高级支持权利。

©2024 Palo Alto Networks, Inc.

	灵活 vCPU	VM 系列型号（固定 vCPU）
	创建部署配置文件时，您可以选择安全服务的任意组合。您可以随时从配置文件中添加或删除安全服务。	
PAN-OS 版本	多达 64 个灵活 vCPU 和高级服务选项，适用于运行 10.0.4 及更高版本的防火墙。	您可以在任何 PAN-OS 版本上部署 VM 系列型号（固定 vCPU）。
资金	允许您使用防火墙即平台组件的可重用积分。 购买积分后，您必须激活积分，并将其与贵组织的特定帐户相关联。激活的积分为您可以从中创建部署配置文件的积分池提供资金。 部署防火墙后，将会消耗积分。停用防火墙后，将会释放积分并将其返回您的积分池以供进一步使用。	• 多型号 ELA：令牌。 • 具有支持权利和/或安全服务套餐 1 或套餐 2 的永久 VM 系列型号容量许可证。您在购买时确定配置。除非您购买新的许可证，否则您无法更改配置。 • 具有支持权利和您选择的安全服务的期限防火墙容量许可证。
部署配置	灵活。可以随时更改部署配置文件。对配置文件的更改会传播到共享部署配置文件授权代码的所有防火墙。	VM 系列型号的容量不会改变，但是，如果您有 ELA，则可以添加安全服务。 永久许可证和短期许可证需提前配置和付费，并且不会改变。
部署	积分激活后，为特定环境或用例（例如“保护我的 NSX 环境”）创建部署配置文件，并配置防火墙 vCPU、安全服务和可选虚拟 Panorama。您可以随时创建任意数量的部署配置文件并对其进行自定义。 您必须有客户支持门户角色积分管理员（仅适用于帐户管理）才能激活和管理软件 NGFW 积分。	接受 VM 系列 ELA。创建和配置 VM 系列防火墙。激活模型许可证并注册防火墙。
Panorama	创建部署配置文件时，您可以选择添加 Panorama 进行管理，或作为使用部署配置文件的防火墙的专用日志收集器。此 Panorama 可以管理使用部署配置文件的共享授权代码部署的防火墙。	Panorama 是一项单独的费用。物理或虚拟 Panorama 可用于防火墙管理或日志收集。

©2024 Palo Alto Networks, Inc.

	灵活 vCPU	VM 系列型号（固定 vCPU）
升级或降级	如果 VM 系列防火墙或 Panorama 能够访问 Internet，则会将对部署配置文件的更改自动应用于防火墙。 如果防火墙无法访问 Internet，请手动停止防火墙。在 Assets（资产）> Software NGFW Credits（软件 NGFW 积分）中更改部署配置文件，在 CSP 中下载许可证密钥并将其传输到 VM，从 CSP 获取配置文件并将其传输到 VM，然后重新启动 VM 并应用许可证。 在任何一种情况下，您都无需重新启动防火墙。	更改为不同的型号需要更改许可证并重新启动。

灵活 vCPU 和固定型号部署

以下清单比较了软件 NGFW 积分和 VM 系列型号许可方法的部署过程。

灵活 vCPU	固定 vCPU（VM 系列型号）
1. 创建支持帐户. 2. 激活积分. 贵组织可以使用多个帐户来代表不同的成本中心。在注册期间，您应将积分购买与帐户相关联。 3. 创建部署配置文件. 4. 在 Alibaba、AWS、Azure、Cisco ACI、Cisco CSP、Cisco ENCS、ESXi、Google Cloud Platform、Hyper-V、KVM、OpenStack 上部署 VM 系列防火墙。Oracle 云基础架构、vCloud Air、NSX-T 或 NSX-V 5. 在 VM 系列防火墙上安装设备证书（适用于站点许可证，例如 Cortex Data Lake 和 Auto Focus。）	1. 创建支持帐户. 2. 激活 VM 系列型号许可证. 3. 注册 VM 系列防火墙. 4. 在 Alibaba、AWS、Azure、Cisco ACI、Cisco CSP、Cisco ENCS、ESXi、Google Cloud Platform、Hyper-V、KVM、OpenStack 上部署 VM 系列防火墙。Oracle 云基础架构、vCloud Air、NSX-T 或 NSX-V。 5. 在 VM 系列防火墙上安装设备证书（适用于站点许可证，例如 Cortex Data Lake 和 Auto Focus。）

©2024 Palo Alto Networks, Inc.

创建支持帐户

您需要支持帐户才能登录客户支持门户 (CSP)。您必须登录才能激活和管理软件 NGFW 积分、访问软件更新或通过 Palo Alto Networks 技术支持打开案例。支持帐户可让您查看并管理您通过 Palo Alto Networks 注册的所有资产，包括设备、许可证和订阅等。

除目前在 AWS 上提供的基于使用的许可证之外，对于所有许可选项，您均需配备支持帐户，以便下载安装 VM 系列防火墙所需的软件包。

如果您已有支持帐户，则可以下载并安装 VM 系列防火墙软件，然后继续注册 VM 系列防火墙。

STEP 1 | 转到 https://support.paloaltonetworks.com/UserAccount/PreRegister。

STEP 2 | 输入要与支持帐户相关联的公司电子邮件地址。

STEP 3 | 在以下选项中选择一项，再将详细信息填入用户注册表：

对于 AWS 上基于使用的许可证

1. 单击 **Register your Amazon Web Services VM-Series Instance**（注册 **Amazon Web** 服务 **VM** 系列实例）。
2. 在 AWS 管理控制台上，找到 AWS 实例 ID、AWS 产品代码，以及您部署防火墙的 AWS 区域。
3. 填入其他详细信息。

对于所有其他许可证

1. 单击 **Register device using Serial Number or Authorization Code**（使用序列号或授权代码注册设备）。
2. 输入容量授权代码和销售订单号或客户 ID。
3. 填入其他详细信息。

STEP 4 | **Submit**（提交）表单。您将收到一封电子邮件，其中包含激活您的用户帐户的链接。

完成激活帐户的步骤。帐户经验证后，注册即完成，之后您便可登录到支持门户。

©2024 Palo Alto Networks, Inc.

VM 系列防火墙的序列号和 CPU ID 格式

启动 VM 系列防火墙实例时，防火墙的每个实例都使用防火墙的 CPU ID 和序列号进行唯一标识。CPU ID 格式和序列号包括有关 VM 系列防火墙的每个实例的虚拟机监控程序和许可证类型的信息。

- 凭借 VM 系列防火墙的基于使用情况的许可模式，启动时防火墙会生成序列号和 CPU ID，并使用这些详细信息面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。。
- 使用 BYOL 型号，您可以在客户支持门户 (CSP) 上注册 VM 系列防火墙固定型号或具有灵活许可证的 VM 系列防火墙。
  - 对于可直接访问 Internet 的防火墙，您可以将防火墙代码应用于防火墙，以生成包含序列号的许可证文件。
  - 对于处于脱机状态的防火墙，您必须使用 CSP 输入 CPU ID、UUID 和授权代码，以生成包含序列号的许可证文件。然后，您可以在防火墙上安装许可证。

许可证类型	序列号	CPU ID
BYOL	15 位，全部为数字 示例：0071 **51** 345678909	<Hypervisor>:<ActualCPUID> 示例：**ESX**:12345678
PAYG	15 位，字母数字 示例：**4** DE0YTAYOGMYYTN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> 示例： **AWSMP**:1234567890abcdef0:6kxdw3bbmdeda 3o6i1ggqt4km:us-west1

©2024 Palo Alto Networks, Inc.

使用基于 Panorama 的软件防火墙许可证管理

Panorama 软件防火墙许可证插件允许您在 VM 系列防火墙连接到 Panorama 时自动许可。如果 VM 系列防火墙位于部署外围，并且未与 Palo Alto Networks 许可服务器建立连接，则软件防火墙许可证插件通过使用 Panorama 许可 VM 系列防火墙，从而简化许可证激活过程。

此外，软件防火墙许可证插件简化了环境中 VM 系列防火墙的许可证激活和停用，在该环境中可使用自动扩展和自动化部署和删除防火墙以应对云中的变化。



此插件不支持现收现付 *(PAYG)* 许可证。



请勿使用软件防火墙许可证插件许可适用于 *VMware NSX* 的 *VM* 系列防火墙。适用于 *VMware NSX* 的 *Panorama* 插件可自动许可部署在 *NSX* 和 *NSX-T* 中的 *VM* 系列防火墙

。

此外，请勿使用此插件许可设备组中部署的防火墙，包括在 *NSX-T* 中部署的 *VM* 系列防火墙的实例。

要安装 Panorama 软件防火墙许可证插件，您必须使用 Panorama 10.0.0 或更高版本和 VM 系列插件 2.0.4 或更高版本。您的 VM 系列防火墙必须运行 PAN-OS 9.1.0 或更高版本。



适用于 *Azure* 的 *VM* 系列防火墙需要 *VM* 系列插件 *2.0.8* 或更高版本。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

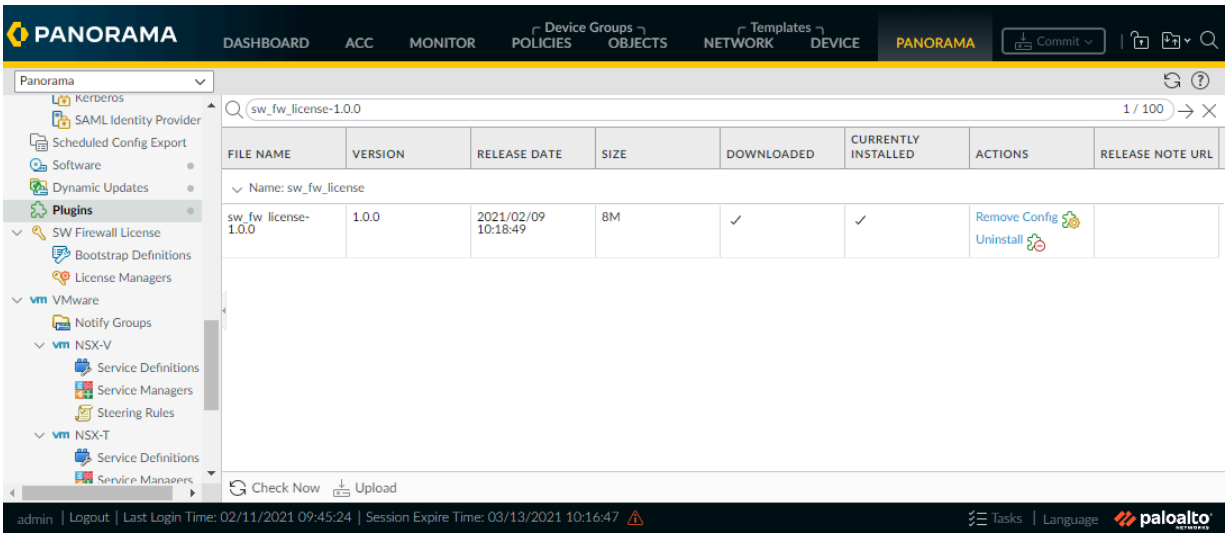
所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

©2024 Palo Alto Networks, Inc.

STEP 1 | 安装适用于 Panorama 的软件防火墙许可证插件。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Plugins**（插件）。
3. 单击 **Check Now**（立即检查）以获取可用插件列表。
4. 搜索 sw_fw_license 以找到插件。
5. 选择 **Download**（下载）并 **Install**（安装）软件许可插件。

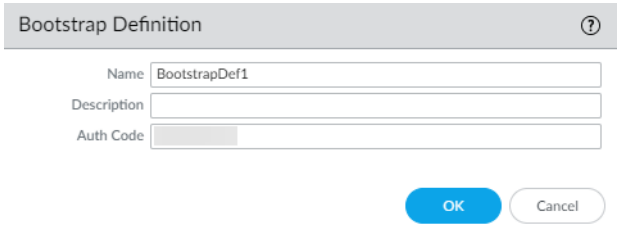
安装成功后，Panorama 将刷新，**Panorama** 选项卡上会显示软件许可插件。



©2024 Palo Alto Networks, Inc.

STEP 2 | 配置引导定义。

1. 选择 **Panorama** > **SW Firewall License**（软件防火墙许可证） > **Bootstrap Definitions**（引导定义）。
2. 单击添加。
3. 输入描述性 **Name**（名称）以标识引导定义。
4. （可选）输入引导定义的 **Description**（说明）。
5. 输入在连接到 Panorama 时用于许可 VM 系列防火墙的 **Auth Code**（授权代码）。
6. 单击 **OK**（确定）。



STEP 3 | 配置许可证管理器。

1. 选择 **Panorama** > **SW Firewall License**（软件防火墙许可证） > **License Managers**（许可证管理器）。
2. 单击添加。
3. 输入识别许可证管理器的描述性 **Name**（名称）。
4. （可选）输入许可证管理器的 **Description**（说明）。
5. 从下拉列表中选择 **Device Group**（设备组）。当使用许可证管理器引导的 VM 系列防火墙连接到 Panorama 时，会将其放置在指定的设备组中。
6. 从下拉列表中选择 **Template Stack**（模板堆栈）。当使用许可证管理器引导的 VM 系列防火墙连接到 Panorama 时，会将其放置在指定的模板堆栈中。
7. 在 **Auto Deactivate**（自动停用）字段中，指定 Panorama 在停用已断开连接的 VM 系列防火墙的许可证之前等待的时间（以小时为单位）。如果您选择 **Never**（从不），则

©2024 Palo Alto Networks, Inc.

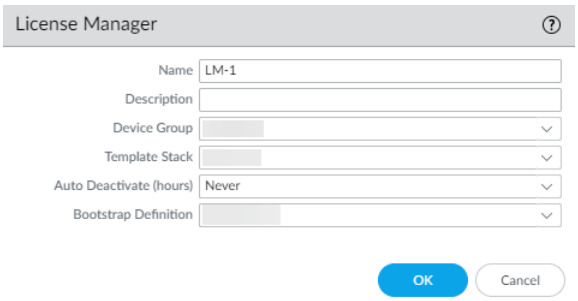
Panorama 不会停用已断开连接的 VM 系列防火墙。默认情况下，将 Auto Deactivate（自动停用）设置为 Never（从不）。您可以将停用时间设置为 1 至 24（以小时为单位）。

在解除之前，请使用以下命令设置 API 密钥：

```
request license api-key set key <key>
```

配置自动停用时间间隔后，除了断开的防火墙外，插件还可能解除已停止的 *VM* 系列防火墙的许可证。

8. 从下拉列表中选择 **Bootstrap Definition**（引导定义）。选定引导定义指定 Panorama 用来许可与许可证管理器相关联的 VM 系列防火墙的授权代码。
9. 单击 **OK**（确定）。
10. **Commit**（提交）更改。



STEP 4 | （可选）为引导 VM 系列防火墙创建 `init-cfg.txt` 文件。配置许可证管理器后，您可以在部署 VM 系列防火墙时复制并粘贴 Panorama 生成的引导参数。根据您的部署，显示的参数可能是下图所示参数的子集。例如，如果 Panorama 设备部署在公共云中，则引导参数将不包括 Panorama 的公共 IP 地址。在这种情况下，您必须在 `init-cfg.txt` 文件中手动输入公共 IP 地址。Panorama 将始终生成身份验证密钥和 **`plugin-op-commands=panorama-licensing-mode-on`**，以用于 `init-cfg.txt` 文件。

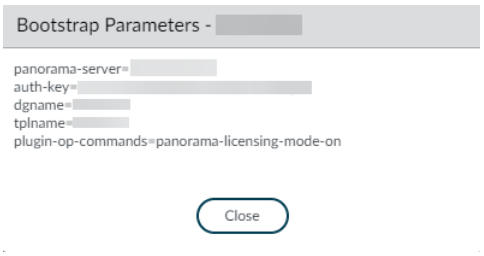
此处显示的身份验证密钥由 Panorama 生成，用于对连接到 Panorama 的 VM 系列防火墙进行身份验证。此外，将使用此身份验证密钥，而不是您可能在 Panorama 上生成并添加到 init-cfg.txt 文件的 VM 身份验证密钥。

如果您使用 *init-cfg.txt* 文件中此处显示的身份验证密钥，请不要使用手动生成的 *VM* 身份验证密钥。

1. 选择 **Panorama** > **SW Firewall License**（软件防火墙许可证） > **License Managers**（许可证管理器）。
2. 在给定许可证管理器的操作列中，单击 **Show Bootstrap Parameters**（显示引导参数）。
3. 复制显示的信息并将其粘贴到文本编辑器中，以创建用于引导的 `init-cfg.txt` 文件。

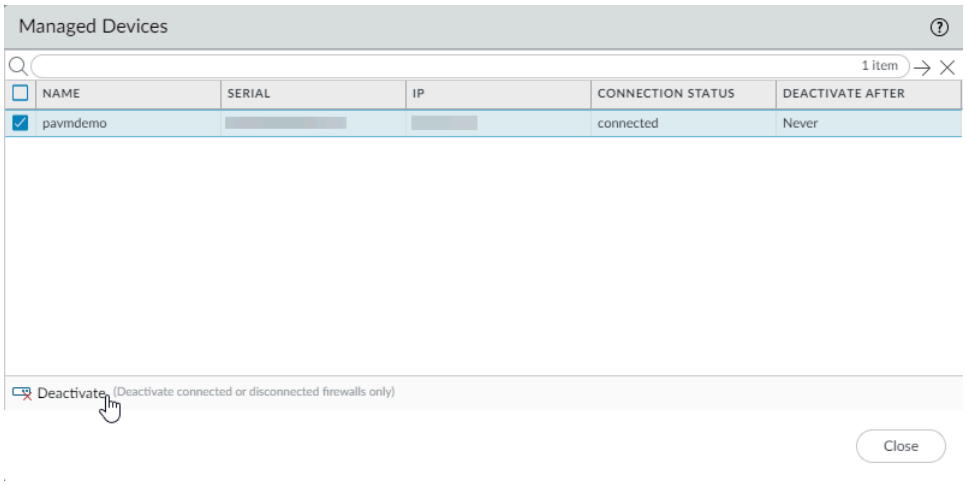
©2024 Palo Alto Networks, Inc.

4. 完成后，单击 **Close**（关闭）。



STEP 5 | （可选）查看和停用托管 VM 系列防火墙。在 **Show Devices**（显示设备）对话框中，您可以查看与给定许可证管理器相关联的设备。您可以查看名称、序列号、管理 IP 地址、连接状态以及 Panorama 等待停用断开连接的防火墙的时间。此外，您可以手动停用托管 VM 系列防火墙的许可证。

1. 选择 **Panorama** > **SW Firewall License**（软件防火墙许可证） > **License Managers**（许可证管理器）。
2. 在给定许可证管理器的操作列中，单击 **Show Devices**（显示设备）。
3. 要手动停用已连接或断开连接（但尚未停用）的托管 VM 系列防火墙，请选择一个或多个列出的 VM 系列防火墙，然后单击 **Deactivate**（停用）。



STEP 6 | （可选）验证 Panorama 是否已完成必要的 API 调用以许可连接的防火墙。

1. 登录 Panorama 命令行界面。
2. 执行以下命令。

```
show plugins sw_fw_license panorama-api-requests
```


©2024 Palo Alto Networks, Inc.

软件 NGFW 积分

软件 NGFW 积分可用于资助软件 NGFW（VM 系列和 CN 系列）、云交付安全服务 (CDSS) 或具有或不具有 Internet 访问权限的网络（例如，气隙网络）中的虚拟 Panorama 设备。

创建部署配置文件，根据 PAN OS 版本、每个防火墙的 vCPU 数量、部署配置文件支持的防火墙总数、Panorama 管理或日志收集以及安全服务配置一个或多个防火墙。使用部署配置文件创建的所有 VM 共享同一授权代码。

- 固定 vCPU — 与所有 PAN-OS 版本兼容。基于VM 系列型号和安全服务套餐。更改型号或服务选项需要新的许可证。
- 灵活 vCPU — 选择灵活数量的 vCPU，并灵活选择安全服务。您可以修改部署配置文件以添加或减少 vCPU 的数量，添加可用的新服务或删除服务。部署配置文件的最大 vCPU 数为 64。

软件 NGFW 积分是基于期限的。可以将期限定义为 1 到 5 年之间的任何时间。分配和未分配的积分在商定的期限结束后到期。您可以为积分池购买额外积分，但到期日期必须与目标池相同。使用软件 NGFW 积分估算器计算并获取部署配置文件的积分。

如果您可以通过 Internet 连接到许可证服务器且停止使用防火墙、安全服务或 Panorama 部署，则分配给该资源的积分将退还到积分池，并且可以重新分配给新资源。

如果您无法访问 Internet 且无法连接到 Palo Alto Networks 更新服务器（例如，在气隙网络中），则可以从其用户界面或 Panorama 本地管理 VM 系列防火墙。然后，您的管理员必须登录客户支持门户以返回许可证令牌，以便可以重复使用资金。

使用下面的支持虚拟机监控程序表和后面的数据平面上的 **vCPU** 总数表，以确保为所选数量的 vCPU 分配必要的硬件资源。

等级	内存
第 1 级	4.5 GB、5 GB、5 GB、5.5 GB、6 GB、6.5 GB、7 GB、8 GB
第 2 级	9 GB、10 GB、12 GB、14 GB、16 GB、18 GB
第 3 级	20 GB、24 GB、28 GB、32 GB、36 GB、40 GB、44 GB、48 GB、52 GB、56 GB、60 GB、64 GB
第 4 级	128 GB

内存配置文件	支持的虚拟机监控程序	最小硬盘驱动器
第 1 级	ESXi、Hyper-V、KVM	• 使用 4.5 GB 内存：32GB（启动时 60GB）

©2024 Palo Alto Networks, Inc.

内存配置文件	支持的虚拟机监控程序	最小硬盘驱动器
（4.5GB、5 GB、5.5GB、6GB 内存）		• 60GB
第 1 级	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T	60GB
第 2 级	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T	60GB
第 3 级	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	60GB
第 4 级	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	60GB

对于上面列出的所有内存配置文件，最小 vCPU 数为 2。

第 *1* 级需要至少 *32GB* 的硬盘空间。但是，由于 *VM* 系列基本映像对所有 *vCPU* 组合都通用，因此您必须分配 *60GB* 的硬盘空间，直到您许可具有 *4.5GB* 内存的 *VM* 系列防火墙。

为了达到最佳性能，所有必需的核心应该可以在一个 *CPU* 插槽上使用。

默认情况下，除非分配四个或更少的 vCPU，否则管理平面和数据平面 vCPU 的分配比例为 1 比 3。此外，最大数据平面 vCPU 与分配的内存相关联，如下表所述。例如，如果为 VM 系列防火墙分配 16 个 vCPU，则会将 4 个 vCPU 分配给管理平面，并将 12 个 vCPU 分配给数据平面。如果 VM 系列防火墙有 20 个 vCPU 和 20GB 内存，则会将 12 个 vCPU 分配给数据平面，而将剩余的 vCPU 分配给管理平面。

或者，您可以使用 VM 系列防火墙 CLI 进行自定义数据平面核心。这样，您可以指定分配给 VM 系列防火墙上数据平面的 vCPU 数量。

无论内存配置文件如何，内核总数（管理平面和数据平面）的最大数量均为 *64*。

©2024 Palo Alto Networks, Inc.

第 1 层	4.5 GB	5 GB	5.5 GB	6 GB	6.5 GB	7 GB	8 GB
默认数据平面 vCPU	1	1	1	1	2	2	2
默认管理平面 vCPU	1	1	1	1	2	2	2

第 2 级	9 GB	10 GB	12 GB	14 GB	16 GB	18 GB	20 GB
默认数据平面 vCPU	4	4	4	4	12	12	12
默认管理平面 vCPU	2	2	2	2	4	4	4

第 3 层	20 GB	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB	48 GB	52 GB	56 GB	64 GB
默认数据平面 vCPU	12	12	12	12	12	12	12	12	12	24	47
默认管理平面 vCPU	4	4	4	4	4	4	4	4	4	8	17

第 4 层	121 - 128 GB
默认数据平面 vCPU	47
默认管理平面 vCPU	17

继续执行软件 NGFW 任务：

- 基于层和内存的最大限制
- 激活积分
- 创建部署配置文件
- 管理部署配置文件
- 注册 VM 系列防火墙（软件 NGFW 积分）
- 配置 Panorama
- 将 Panorama 迁移到软件 NGFW 许可证
- 传输积分
- 续订软件 NGFW 积分合同

©2024 Palo Alto Networks, Inc.

- 停用许可证（软件 NGFW 积分）
- 解除非正常终止防火墙的许可
- 设置许可的 vCPU 数量
- 自定义数据平面核心
- 将防火墙迁移到灵活 VM 系列许可证
- 软件 NGFW 许可 API

基于层和内存的最大限制

下表基于分配的内存或层级提供了单个 VM 系列防火墙部署可以创建、存储、管理或交互的特定对象或资源的最大数量。这些限制适用于使用由软件 NGFW 积分资助的许可证的 VM 系列防火墙。

对于内存扩展，内存增量分为四层，分别代表 VM 系列防火墙的配置容量。无论分配给 VM 系列防火墙实例的内存容量是多少，内存容量所在的层级都决定非会话值的限制，例如安全规则、地址对象、安全配置文件等。

内存配置文件和 vCPU 总数决定自动分配给管理平面和数据平面的核心数量。此外，您可以选择自定义数据平面核心的分布。

如果为许可使用的是软件 NGFW 积分，则可以选择支持以下一个或多个资源要求的内存配置文件：

• 地址分配 • App-ID • EDL • GlobalProtect 客户端 VPN • GlobalProtect 无客户端 VPN • 高可用性	• 接口 • IPSec VPN • 第二层转发 • 多播 • NAT • 对象（地址和服务）	• 数量 • QoS • 路由 • 安全配置文件 • 安全区域数 • 会话	• SSL 解密 • URL 筛选 • User-ID • 虚拟路由器 • 虚拟系统 • 虚拟线路

会话

第 1 层	4.5 GB	5 GB	5.5 GB	6 GB	6.5 GB	7 GB	8 GB
最大会话数（IPv4 或 IPv6）	25,000	40,000	50,000	100，000	200，000	300，000	500，000
最大默认数据平面 vCPU	1	1	1	1	2	2	2

©2024 Palo Alto Networks, Inc.

第 2 级	9 GB	10 GB	12 GB	14 GB	16 GB	18 GB	20 GB
最大会话数（IPv4 或 IPv6）	600,000	800,000	1,000,000	1,200,000	1,800,000	2,000,000	2,800,000
最大默认数据平面 vCPU	4	4	4	4	12	12	12

第 3 层	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB
最大会话数（IPv4 或 IPv6）	3,600,000	4,400,000	5,200,000	6,000,000	6,800,000	6,800,000
最大默认数据平面 vCPU	12	12	12	12	12	12

第 3 层（续）	48 GB	52 GB	56 GB	64 GB
最大会话数（IPv4 或 IPv6）	7,600,000	8,400,000	9,200,000	10,000,000
最大默认数据平面 vCPU	12	12	24	47

第 4 层	121 - 128 GB
最大会话数（IPv4 或 IPv6）	14,000,000
最大默认数据平面 vCPU	47

数量

功能	第 1 层	第 2 级	第 3 层	第 4 层
安全规则	1,500	10,000	20,000	65,000
安全规则时间表	256	256	256	256
NAT 规则	3,000	8,000	15,000	16,000
解密规则	1，000	1，000	2,000	5,000

©2024 Palo Alto Networks, Inc.

功能	第 1 层	第 2 级	第 3 层	第 4 层
应用覆盖规则	1，000	1，000	2,000	4,000
隧道内容检测规则	100	500	2,000	8,500
SD-WAN 规则	100	300	300	1，000
基于策略的转发规则	100	500	2,000	2,000
强制网络门户规则	1，000	1，000	2,000	8,000
DoS 保护规则	1，000	1，000	1，000	2,000

安全区域数

功能	第 1 层	第 2 级	第 3 层	第 4 层
最大安全区域	40	200	200	17,000

对象（地址和服务）

功能	第 1 层	第 2 级	第 3 层	第 4 层
地址对象	10,000	20,000	40,000	160,000
地址组	1，000	2，500	4,000	80,000
每个地址组的成员数	2，500	2，500	2，500	2，500
服务对象	2,000	2,000	5,000	12,000
服务组	500	250	500	6,000
每个服务组的成员数	500	500	500	2，500
FQDN 地址对象	2,000	2,000	2,000	6,144
最大 DAG IP 地址数*（系统范围容量）	2，500	300，000	300,500	500，000
每个 IP 地址的标签数	32	32	32	64

©2024 Palo Alto Networks, Inc.

*使用 AppMix 事务启用的 App-ID 和 User-ID 功能衡量防火墙吞吐量。

安全配置文件

功能	第 1 层	第 2 级	第 3 层	第 4 层
安全配置文件	375	750	750	750

App-ID

功能	第 1 层	第 2 级	第 3 层	第 4 层
自定义 App-ID 签名	6,000	6,000	6,000	6,000
共享自定义 App-ID	512	512	512	512
自定义 App-ID （特定虚拟系统）	6,416	6,416	6,416	6,416

User-ID

功能	第 1 层	第 2 级	第 3 层	第 4 层
IP-User 映射（管理平面）	524,288	524,288	524,288	524,288
IP-User 映射（数据平面）	64,000	512,000	512,000	512,000
策略中使用的活动和唯一组（LDAP 组、XML API 组和动态用户组的集合）。*	1，000	10,000	10,000	10,000
User-ID 客户端数	100	100	100	100
User-ID 监控服务器数	100	100	100	100
终端服务器客户端数	400	2,000	2，500	2，500
每个用户的标签数* （PAN-OS 9.1 及更高版本）	32	32	32	32

*使用 AppMix 事务启用的 App-ID 和 User-ID 功能衡量防火墙吞吐量。

©2024 Palo Alto Networks, Inc.

SSL 解密

功能	第 1 层	第 2 级	第 3 层	第 4 层
最大 SSL 入站证书数	1，000	1，000	1，000	4,000
SSL 证书缓存 （转发客户端）	128	4,000	8,000	32,000
最大并发解密会话数	6,400	50,000	100，000	2,000,000
SSL 端口镜像	是	是	是	是
SSL 解密代理	否	否	是	是
支持 HSM	是	是	是	是

URL 筛选

功能	第 1 层	第 2 级	第 3 层	第 4 层
允许列表、阻止列表和自定义类别的总条目	25,000	25,000	100，000	100，000
最大自定义类别数	2,849	2,849	2,849	2,849
最大自定义类别数（特定虚拟系统）	500	500	500	500
URL 筛选的数据平面缓存大小	90,000	90,000	250,000	250,000
管理平面动态缓存大小	100，000	100，000	600,000	900,000

EDL

功能	第 1 层	第 2 级	第 3 层	第 4 层
最大自定义列表数	30	30	30	30
每个系统的最大 IP 地址数	50,000	50,000	50,000	150,000
每个系统的最大 DNS 域数	50,000	2,000,000	2,000,00	4,000,000
每个系统的最大 URL 数	50,000	100，000	100，000	250,000

©2024 Palo Alto Networks, Inc.

功能	第 1 层	第 2 级	第 3 层	第 4 层
最短检查间隔（分钟）	5	5	5	5

接口

功能	第 1 层	第 2 级	第 3 层	第 4 层
管理 - 带外	NA	NA	NA	NA
管理 - 10/100/1000 高可用性	NA	NA	NA	NA
管理 - 40Gbps 高可用性	NA	NA	NA	NA
管理 - 10Gbps 高可用性	NA	NA	NA	NA
流量 - 10/100/1000	NA	NA	NA	NA
流量 - 100/1000/10000	NA	NA	NA	NA
流量 - 1Gbps SFP	NA	NA	NA	NA
流量 - 10Gbps SFP+	NA	NA	NA	NA
流量 - 40/100Gbps QSFP+/QSFP28	NA	NA	NA	NA
每个设备的 802.1q 标签数	4,094	4,094	4,094	4,094
每个物理接口的 802.1q 标签数	4,094	4,094	4,094	4,094
最大接口数（逻辑和物理）	2,048	4,096	4,096	4,096
最大聚合接口数	NA	NA	NA	NA
最大 SD-WAN 虚拟接口数	300	1，000	1，000	1，000

虚拟路由器

功能	第 1 层	第 2 级	第 3 层	第 4 层
虚拟路由器数	3	20	125	225

©2024 Palo Alto Networks, Inc.

虚拟线路

功能	第 1 层	第 2 级	第 3 层	第 4 层
虚拟线路	12	12	12	12

虚拟系统

功能	第 1 层	第 2 级	第 3 层	第 4 层
基本虚拟系统数	1	1	1	1
最大虚拟系统数 超过基本虚拟系统容量的虚拟系统容量需要额外许可证	NA	NA	NA	NA

路由

功能	第 1 层	第 2 级	第 3 层	第 4 层
IPv4 转发表大小* （跨虚拟路由器共享的条目）	5,000	32,000	100，000	待添加
IPv6 转发表大小* （跨虚拟路由器共享的条目）	5,000	32,000	100，000	待添加
系统总转发表大小	5,000	32,000	100，000	待添加
每个虚拟路由器的最大路由映射数量	50	50	50	待添加
最大路由对端数（取决于协议）	500	1，000	1，000	待添加
静态条目 - DNS 代理	1,024	1,024	1,024	待添加
双向转发检测 (BFD) 会话数	128	1,024	1,024	待添加

*使用 AppMix 事务启用的 App-ID 和 User-ID 功能衡量防火墙吞吐量。

©2024 Palo Alto Networks, Inc.

第二层转发

功能	第 1 层	第 2 级	第 3 层	第 4 层
每个设备的 ARP 表大小	2，500	32,000	128,000	132,000
IPv6 邻居表大小	2，500	32,000	128,000	132,000
每个设备的 MAC 表大小	2，500	32,000	128,000	132,000
每个广播域的最大 ARP 条目数	2，500	32,000	128,000	132,000
每个广播域的最大 MAC 条目数	2，500	32,000	128,000	132,000

NAT

功能	第 1 层	第 2 级	第 3 层	第 4 层
NAT 规则总容量	3,000	8,000	8,000	待添加
最大 NAT 规则数（静态）* （将静态 NAT 规则配置为全容量要求不使用其他 NAT 规则类型。）	3,000	8,000	8,000	待添加
最大 NAT 规则数 (DIP)* （将静态 DIP NAT 规则配置为全容量要求不使用其他 NAT 规则类型。）	2,000	8,000	8,000	待添加
最大 NAT 规则数 (DIPP)	400	2,000	2,000	待添加
最大转换 IP 容量 (DIP)	128,000	160,000	160,000	待添加
最大转换 IP 容量 (DIPP)* （DIPP 转换 IP 容量与 DIPP 池超额订阅值成正比。此处显示的容量基于 1 倍的超额订阅值。）	400	2,000	2,000	待添加
默认 DIPP 池超额订阅* （跨并发会话重用源 IP 地址和源端口）	2	8	8	待添加

*使用 AppMix 事务启用的 App-ID 和 User-ID 功能衡量防火墙吞吐量。

©2024 Palo Alto Networks, Inc.

地址分配

功能	第 1 层	第 2 级	第 3 层	第 4 层
DHCP 服务器数	3	20	125	待添加
DHCP 中继* （最大容量表示 DHCP 服务器和 DHCP 中继的总和）	500	500	500	待添加
最大分配地址数	64,000	64,000	64,000	待添加

*使用 AppMix 事务启用的 App-ID 和 User-ID 功能衡量防火墙吞吐量。

高可用性

功能	第 1 层	第 2 级	第 3 层	第 4 层
支持的设备数	2	2	2	2
最大虚拟地址数	128	32	128	待添加

QoS

功能	第 1 层	第 2 级	第 3 层	第 4 层
QoS 策略数	500	2,000	4,000	待添加
支持 QoS 的物理接口数	6	12	12	12
每个物理接口的明文节点数	31	63	63	63
按策略选择 DSCP 标记	是	是	是	是
支持的子接口数	NA	NA	NA	NA

IPSec VPN

功能	第 1 层	第 2 级	第 3 层	第 4 层
Max IKE 对端	1，000	1，000	2,000	待添加

©2024 Palo Alto Networks, Inc.

功能	第 1 层	第 2 级	第 3 层	第 4 层
站点到站点（带有代理 ID）	1，000	4,000	8,000	待添加
SD-WAN IPSec 隧道数	1，000	1，000	2,000	待添加

GlobalProtect 客户端 VPN

功能	第 1 层	第 2 级	第 3 层	第 4 层
最大隧道数（SSL、IPSec 和带 XAUTH 的 IKE）	500	6,000	12,000	待添加

GlobalProtect 无客户端 VPN

功能	第 1 层	第 2 级	第 3 层	第 4 层
最大 SSL 隧道数	100	1,200	2，500	25,000

多播

功能	第 1 层	第 2 级	第 3 层	第 4 层
复制（出口接口）	100	100	100	待添加
路由	2,000	4,000	4,000	待添加

激活积分

在贵组织内，您可以创建多个帐户，每个帐户都有不同的用途。在激活过程中，您只能为每个默认积分池选择一个帐户。一旦积分池处于活动状态，则授予积分管理员角色的用户就可以为部署分配积分，甚至可以将积分传输到其他积分池。

如果您有现有 CSP 帐户并且是超级用户或管理员，系统会自动将信用管理员角色添加到您的配置文件中。如果您没有现有帐户，CSP 会自动为您创建一个帐户，并将积分管理员角色添加到您的配置文件中。

您（购买者）会收到一封电子邮件，其中详细说明了订阅、积分池 ID、订阅开始和结束日期、购买的积分数量以及默认积分池的说明（请参阅VM 系列防火墙许可中的“默认积分池”）。

保护此电子邮件以备将来参考。

©2024 Palo Alto Networks, Inc.

STEP 1 | 在电子邮件中，单击 **Start Activation**（开始激活）以查看可用的积分池。

STEP 2 | 选择要激活的积分池。您可以使用搜索字段按帐号或用户名筛选帐户列表。

如果您已购买多个积分池（请参阅软件 NGFW 积分），系统会自动将其选定。复选标记表示登录积分的激活链接。

系统会提示您进行身份验证或登录。

如果您取消选择积分池，您会看到一个提醒，提示您如果要激活这些积分，则必须返回电子邮件并单击 ***Start Activation***（开始激活）链接。

STEP 3 | 选择 **Start Activation**（开始激活）。

STEP 4 | 选择支持帐户（您可以按帐号或姓名进行搜索）。

STEP 5 | 选择默认积分池。

STEP 6 | 选择 **Deposit Credits**（存款积分）。

您会看到一条提示存款成功的消息。

STEP 7 | （可选）如果这是您第一次激活积分，则系统会显示 **Create Deployment Profile**（创建部署配置文件）对话框。

继续阅读创建部署配置文件。

创建部署配置文件

要创建部署配置文件，您必须拥有客户支持门户帐户 (CSP) 并访问激活的积分池。

在开始之前，估计将使用部署配置文件中的配置的防火墙数量。您无需一次部署所有防火墙。

STEP 1 | 如果您已有积分池，请登录帐户，然后从仪表盘中选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分） > **Create Deployment Profile**（创建部署配置文件）。

如果您刚刚激活积分池，系统会显示 **Create Deployment Profile**（创建部署配置文件）表单。

1. 选择 VM 系列防火墙类型。
2. 选择 PAN-OS 版本。
   - **Fixed Models**（固定型号）(VM 系列型号)
   - **Flexible vCPUs**（**PAN-OS 10.0.4** 及更高版本）
3. 单击 **Next**（下一步）。

©2024 Palo Alto Networks, Inc.

STEP 2 | VM 系列配置文件。

1. **Profile Name**（配置文件名称）。

   命名配置文件。

2. **Number of Firewalls**（防火墙数量）。

   假设您有足够的积分，请输入此配置文件部署的防火墙数量。您无需一次部署所有防火墙。

3. **Firewall Model**（防火墙型号）：

   选择 VM 系列型号。

   Planned vCPU/Firewall（规划的 **vCPU**/防火墙）（PAN-OS 10.0.4 或更高版本）。

   输入每个防火墙的 vCPU 数量。

   安全用例： 选择用例。

4. **Customize Subscriptions**（自定义订阅）。

   选择用例后，您可以添加或删除安全服务。

5. （可选）**Use Credits to Enable VM Panorama**（使用积分启用 **VM Panorama**）。

   选择 Panorama 用例 — 管理和/或日志收集器。

STEP 3 | （可选）将鼠标悬停在 **Protect more, save more**（保护更多，储蓄更多）后面的问号上方，以查看您的积分分配如何影响储蓄。

STEP 4 | 单击 **Calculate Estimated Cost**（计算估计成本）以查看积分总数和部署前可用的积分数量。

（可选）将鼠标悬停在估计值后面的问号上方以查看每个组成部分的积分明细。

STEP 5 | **Create the Deployment Profile**（创建部署配置文件）。

您可能需要等待几秒钟，配置文件才会出现在 **Current Deployment Profiles**（当前部署配置文件）选项卡列表中。在分配完成之前，**Credits Consumed/Allocated**（消耗/分配的积分）列显示 0 和 **Update Pending**（更新挂起）。滚动到底部并转到最后一页以查找您的配置文件。

要稍后查看部署配置文件，请单击父积分池上的 **Details**（详细信息）按钮，然后选择 **Current Deployment Profiles**（当前部署配置文件）选项卡。

- 请记下最右侧配置文件的授权代码；软件 NGFW 积分授权代码以 D 开头。
- 在分配完成之前，**Credits Consumed/Allocated**（消耗/分配的积分）列显示 0 和 **Update Pending**（更新挂起）。
- **Audit Trail**（审核线索）选项卡显示您管理的 **Credit Transactions**（积分交易）和 **Deployment Profiles**（部署配置文件）。您还可以在此选项卡中按时间搜索配置文件。

  使用搜索框查找您的配置文件，然后展开该行以查看您在创建配置文件时指定的配置。

©2024 Palo Alto Networks, Inc.

管理部署配置文件

创建部署配置文件后，您可以对其进行编辑、复制或删除。此外，您可以将部署配置文件从一个积分池转移到另一个积分池。

- 编辑部署配置文件
- 克隆部署配置文件
- 转移部署配置文件
- 删除部署配置文件

编辑部署配置文件

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）按钮。

STEP 2 | 选择 **Current Deployment Profiles**（当前部署配置文件）选项卡。

STEP 3 | 选择最右侧的垂直省略号（More Options（更多选项）），然后选择 **Edit Profile**（编辑配置文件）。

STEP 4 | 进行更改并选择 **Update Deployment Profile**（更新部署配置文件）。

STEP 5 | 选择 **Audit Trail**（审核线索）选项卡，然后使用搜索框查找您的配置文件。

使用搜索框查找您的配置文件，然后展开该行以查看您在创建配置文件时指定的配置。

克隆部署配置文件

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）按钮。

STEP 2 | 选择最右侧的垂直省略号（More Options（更多选项）），然后选择 **Clone Profile**（克隆配置文件）。

STEP 3 | 更改配置文件名称，进行任何其他更改，然后选择 **Create Deployment Profile**（创建部署配置文件）。

STEP 4 | 选择 **Audit Trail**（审核线索）选项卡，然后使用搜索框查找您的配置文件。

展开该行以查看您克隆的配置。这是新配置，具有不同的配置文件名称和授权代码。

转移部署配置文件

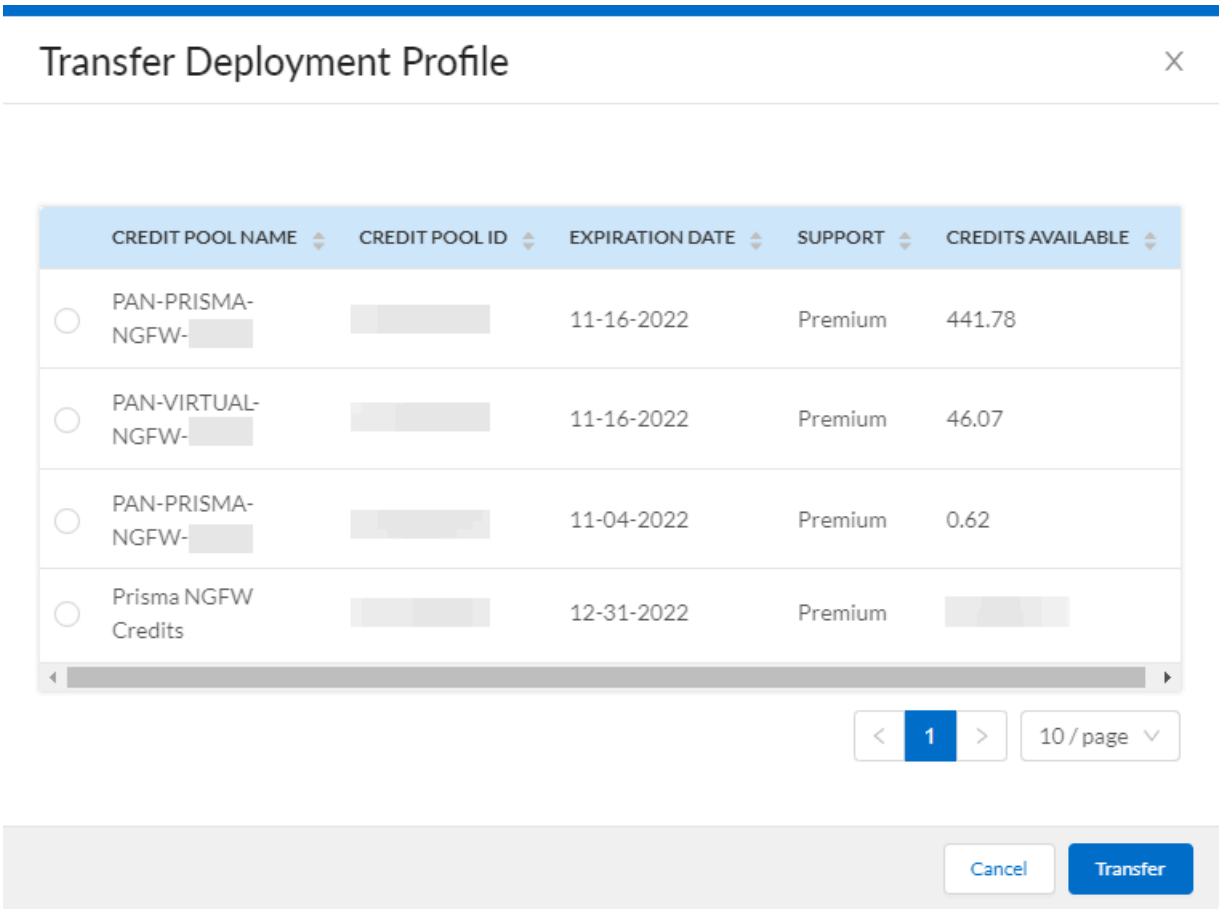
按以下步骤将部署配置文件从一个积分池转移到另一个积分池。

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）按钮。

STEP 2 | 在最右侧选择垂直省略号（更多选项），然后选择 **Transfer Profile**（转移配置文件）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 选择目标积分池，然后单击 **Transfer**（转移）。



删除部署配置文件

在删除部署配置文件之前，您必须在使用部署配置文件的任何防火墙上停用许可证（软件 NGFW 积分），然后停用 VM。

STEP 1 | 选择 **Assets**（资产）> **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）按钮。

STEP 2 | 选择最右侧的垂直省略号（More Options（更多选项）），然后选择 **Delete**（删除）。

注册 VM 系列防火墙（软件 NGFW 积分）

注册需要访问 Palo Alto Networks 客户支持门户 (CSP) 和支持帐户。如有必要，请创建帐户。

在激活过程中，管理员会激活积分池并存入积分。创建部署配置文件时，系统会为所有用户创建授权代码。完成以下过程之一以启动注册。

- 设备可以访问 CSP
- 设备无法访问 CSP

©2024 Palo Alto Networks, Inc.

如果防火墙能够连接到 **CSP**，请使用以下步骤：

1. 使用您的帐户凭据登录 CSP。
2. 选择 **Assets**（资产） > **Software NFGW Credits**（软件 **NFGW** 积分）。

   找到您的积分池并查看 **Details**（详细信息）。
3. 查看 **Current Deployment Profiles**（当前部署配置文件）并选择（或创建）一个配置文件。

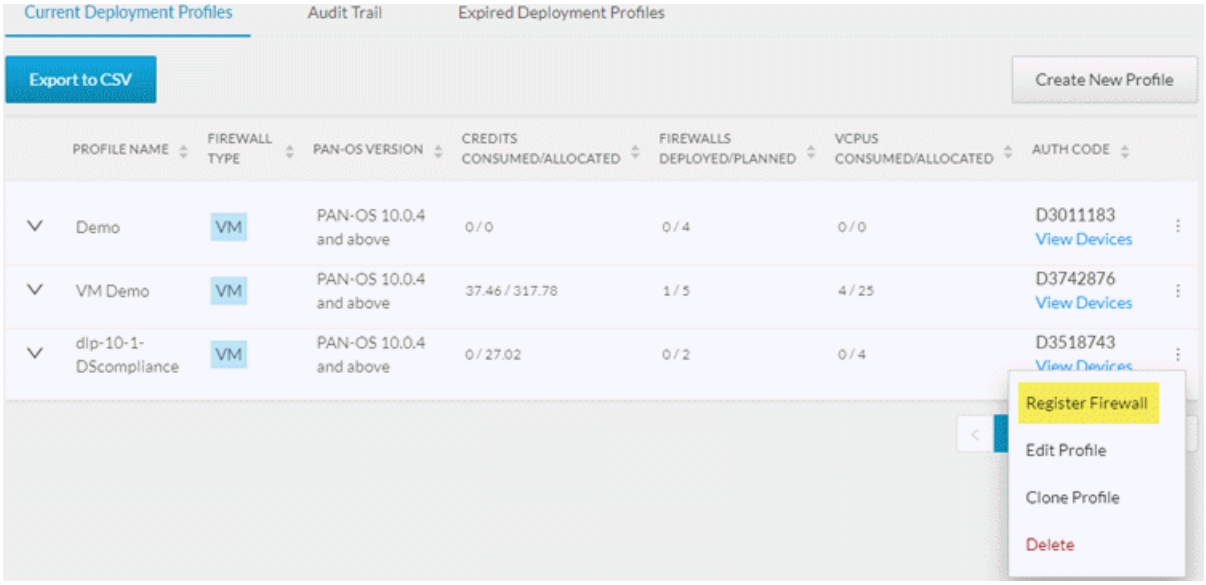
   您将使用此配置文件中的授权代码来许可使用它创建的任何防火墙。灵活防火墙许可证的授权代码以字母 D 开头。
4. 登录到 VM 系列防火墙 Web 接口。
5. 验证 Palo Alto Networks 更新服务器配置。
   1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）。
   2. 确认 **Update Server**（更新服务器）设置为 `updates.paloaltonetworks.com`。
   3. 确认已选择 **Verify Update Server Identity**（验证更新服务器标识）。
6. 选择**Device**（设备） > **Licenses**（许可证）。
   1. 选择 **Activate feature using authorization code**（使用授权代码激活功能）。
   2. 输入部署配置文件中的 VM 系列授权代码。
   3. 单击 **OK**（确定）以确认许可证升级。防火墙与 Palo Alto Networks 更新服务器建立连接，并根据 VM 系列型号使用防火墙所需的令牌。
7. 确认 **Dashboard**（仪表盘）显示有效的序列号，并且 **PA-VM** 许可证显示在 **Device**（设备） > **Licenses**（许可证）选项卡中。
8. 验证防火墙是否已在 CSP 上注册：
   - 选择 **Assets**（资产） > **Software NFGW Credits**（软件 **NFGW** 积分）
   - “授权代码”列，**View Devices**（查看设备）并找到部署的序列号。
   - 在积分池中，消耗的积分、部署的防火墙和使用的 vCPU 会增加，从而反映您的部署情况。

©2024 Palo Alto Networks, Inc.

如果防火墙无法连接到 **CSP**，请执行以下步骤：

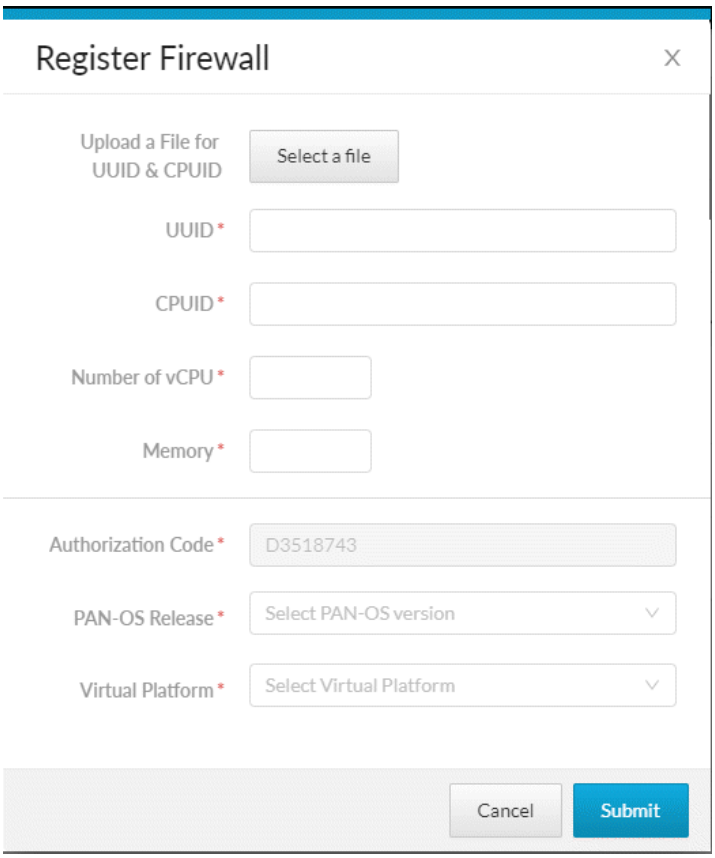
此工作流会将防火墙添加到支持数据库中。由于防火墙无法连接到许可证服务器，因此您必须手动将许可证从 CSP 传递到防火墙。

1. 使用您的帐户凭证登录 CSP。
2. 选择新的配置文件，然后选择垂直省略号（“更多”选项）并 **Register Firewall**（注册防火墙）。



这将打开设备注册表单。输入防火墙的信息，然后单击 **Submit**（提交）：

©2024 Palo Alto Networks, Inc.



这会将防火墙与配置文件及其授权代码相关联，并分配序列号。

3. 单击 **View Devices**（查看设备）以查看 **Software NGFW Devices**（软件 **NGFW** 设备）中的关联设备。

   在 **License**（许可证）列中，将每个许可证密钥下载到可以安全地将文件传输到防火墙的位置。

4. 登录防火墙并选择 **Device**（设备） > **Licenses**（许可证）。

   许可证密钥必须通过 *Web* 界面安装。防火墙不支持通过 *SCP* 或 *FTP* 安装许可证密钥。

   - 单击 **Manually upload license key**（手动上传许可证密钥）。
   - 确认 Dashboard（仪表盘）显示有效的序列号，并且 **PA-VM** 许可证显示在 **Device**（设备） > **Licenses**（许可证）选项卡中。

配置 Panorama

此选项仅在创建部署配置文件时选择 Panorama 才可见。如有必要，您可以编辑配置文件。

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）按钮。

©2024 Palo Alto Networks, Inc.

STEP 2 | 选择最右侧的垂直省略号（More Options（更多选项）），然后选择 **Provision Panorama**（配置 **Panorama**）和 **Provision**（配置）。您会看到为当前部署配置文件配置的防火墙列表。

这将创建 Panorama，分配序列号和型号类型 PAN-PRA-1000-CP，并将 Panorama 注册为资产。您刚才配置的 Panorama 是列出的最后一个 Panorama。请注意，授权代码以 F 开头（因此与部署配置文件不同），但到期日期与配置文件的积分池相同。

复制序列号。

STEP 3 | 在部署配置文件中 **View Devices**（查看设备），然后在 Software NGFW Devices（软件 NGFW 设备）页面上选择 **Panorama**。系统将显示所有软件 NGFW Panorama。

使用复制的序列号按序列号 **Search By**（搜索）。

您还可以选择 **Assets**（资产） > **Software NGFW Devices**（软件 **NGFW** 设备），并使用复制的序列号按序列号 **Search By**（搜索）。

STEP 4 | 设置 Panorama 虚拟设备后，将序列号添加到 Panorama。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Setup**（设置） > **Management**（管理） > **General Settings**（常规设置），并单击 **Edit**（编辑）图标。
3. 在 **Serial Number**（序列号）字段中输入从 CSP 复制的序列号。
4. 单击 **OK**（确定）保存更改。
5. Commit（提交）配置更改。

   选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

将 Panorama 迁移到软件 NGFW 许可证

您可以将 VM-ELA 或永久虚拟 Panorama 许可迁移到软件新一代防火墙（软件 NGFW）许可。

- 迁移可访问 CSP 的 Panorama
- 迁移可以访问 CSP 的 Panorama HA 对
- 将无法访问 CSP 的独立 Panorama 迁移到灵活许可证
- 将无法访问 CSP 的 HA 对迁移到灵活许可证

迁移可访问 CSP 的 Panorama

完成以下过程，将 VM-ELA 或永久虚拟 Panorama 许可证迁移到软件 NGFW 许可证。通过此迁移，您可以将现有 Panorama 设备移动到软件 NGFW 许可证而不会中断服务，同时保留现有的序列号。由于您的序列号不会发生更改，因此，这会保留您的日志和现有策略。

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）链接。

©2024 Palo Alto Networks, Inc.

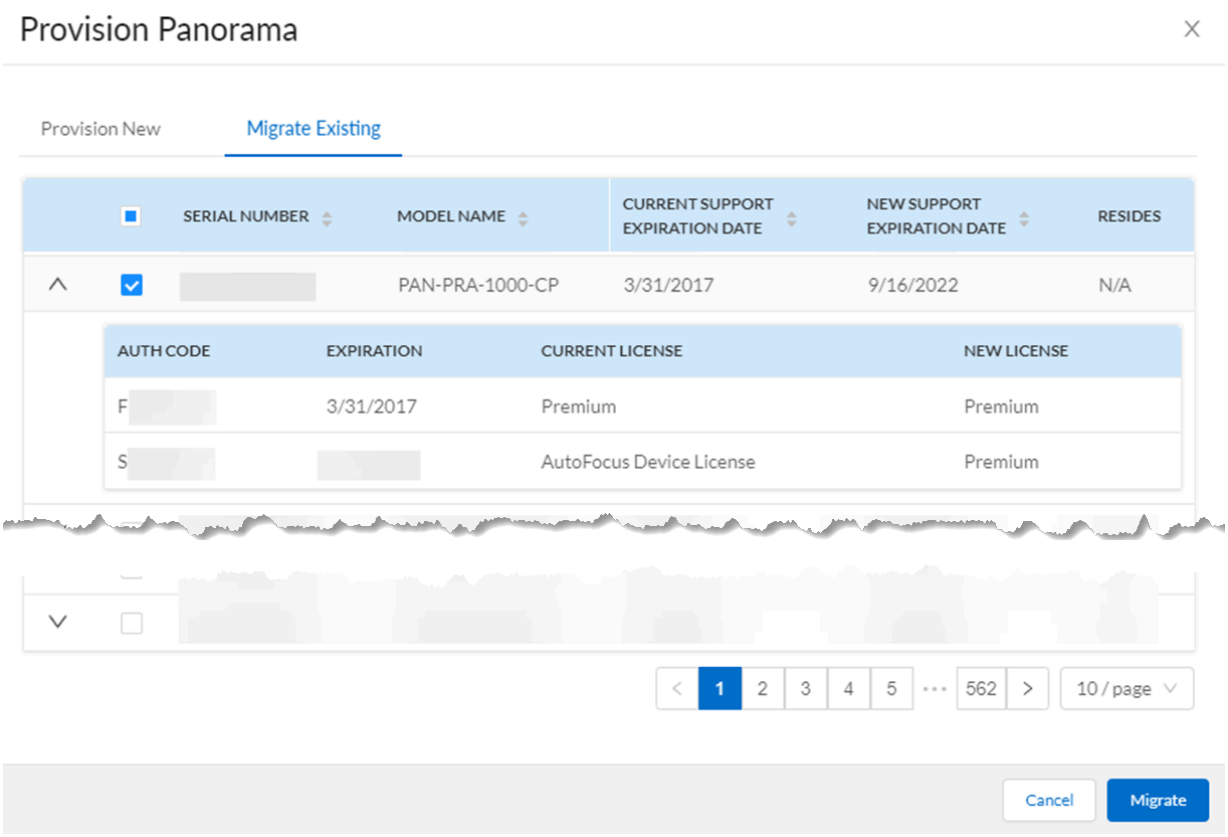
STEP 2 | 选择最右侧的垂直省略号（“更多”选项）并选择 **Provision Panorama**（配置 **Panorama**），然后单击 **Migrate Existing**（迁移现有）。

CSP 会显示与您的帐户关联的所有虚拟 Panorama 设备。

STEP 3 | 选择要迁移的每个虚拟 Panorama 的复选框。

STEP 4 | 单击 **Migrate**（迁移）。

验证 **Current Support Expiration Date**（当前支持到期日期）是否已更新。此外，您可以展开每一行以查看应用到所选 Panorama 的各许可证。



迁移可以访问 CSP 的 Panorama HA 对

完成以下过程，将具有 VM-ELA 或永久许可证的 HA 对迁移到软件 NGFW 许可。通过此迁移，您可以将现有 Panorama 设备移动到软件 NGFW 许可证而不会中断服务，同时保留现有的序列号。由于您的序列号不会发生更改，因此，这会保留您的日志和现有策略。

©2024 Palo Alto Networks, Inc.

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建配置文件的积分池上的 **Details**（详细信息）链接。

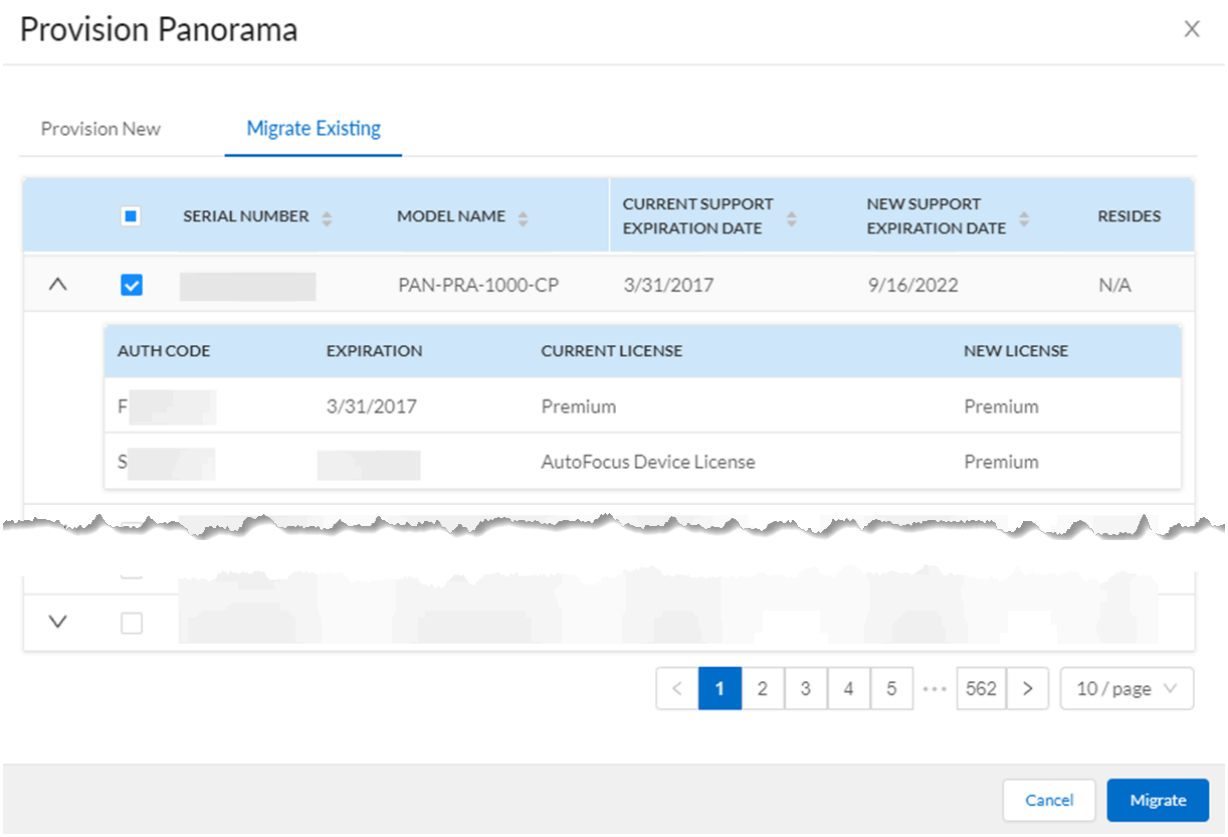
STEP 2 | 选择最右侧的垂直省略号（“更多”选项）并选择 **Provision Panorama**（配置 **Panorama**），然后单击 **Migrate Existing**（迁移现有）。

CSP 会显示与您的帐户关联的所有虚拟 Panorama 设备。

STEP 3 | 选择要迁移的每个虚拟 Panorama 的复选框。

STEP 4 | 选择 **Migrate**（迁移）。

验证 **Current Support Expiration Date**（当前支持到期日期）是否已更新。此外，您可以展开每一行以查看应用到所选 Panorama 的各许可证。



 ©2024 Palo Alto Networks, Inc.

将无法访问 CSP 的独立 Panorama 迁移到灵活许可证

完成以下过程，将 VM-ELA 或永久虚拟 Panorama 许可证迁移到软件 NGFW 许可证，即使您的 Panorama 无法访问 CSP 也是如此。在没有 CSP 的情况下进行迁移需要更改序列号，但是，它允许将 Panorama 设备迁移到软件 NGFW 许可证，同时保留现有策略。

Panorama 支持的最低版本是 *8.1*。如果必须升级 *PAN-OS*，请在开始迁移过程之前执行此操作。如果要管理使用灵活 *vCPU* 和高级服务的防火墙，*PAN-OS* 版本必须为 *10.0.4* 或更高版本。

STEP 1 | 在 Panorama 上，根据需要进行升级，并记下序列号和当前支持到期日期。

STEP 2 | 在 CSP 中，选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击积分池上的 **Details**（详细信息）链接。选择部署配置文件，或者创建一个配置文件。

STEP 3 | 选择最右侧的垂直省略号（“更多”选项），然后选择 **Provision Panorama**（配置 **Panorama**）和 **Migrate Existing**（迁移现有）。

CSP 会显示与您的帐户关联的所有虚拟 Panorama 设备。

STEP 4 | 选中要迁移的每个虚拟 Panorama，然后选择 **Migrate**（迁移）。

STEP 5 | 在 Panorama 上，将序列号替换为在 CSP 中配置的 Panorama 中的序列号。等待一分钟，然后刷新页面。

STEP 6 | 在 CSP 中，选择配置的 Panorama，然后下载所有许可证（支持许可证、管理许可证），如果部署配置文件包含，还包括作为日志管理器的 Panorama。

将许可证安全传递到您的 Panorama。

STEP 7 | 上传所有软件 NGFW 许可证。

STEP 8 | 验证 **Current Support Expiration Date**（当前支持到期日期）是否已更新。此外，您可以展开每一行以查看应用到所选 Panorama 的支持许可证和/或日志记录许可证。

将无法访问 CSP 的 HA 对迁移到灵活许可证

当 HA 对无法与 CSP 通信时，请使用此过程。此过程将启动故障转移。

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击积分池上的 **Details**（详细信息）按钮。

STEP 2 | 选择最右侧的垂直省略号（“更多”选项）），然后选择 **Provision Panorama**（配置 **Panorama**）。

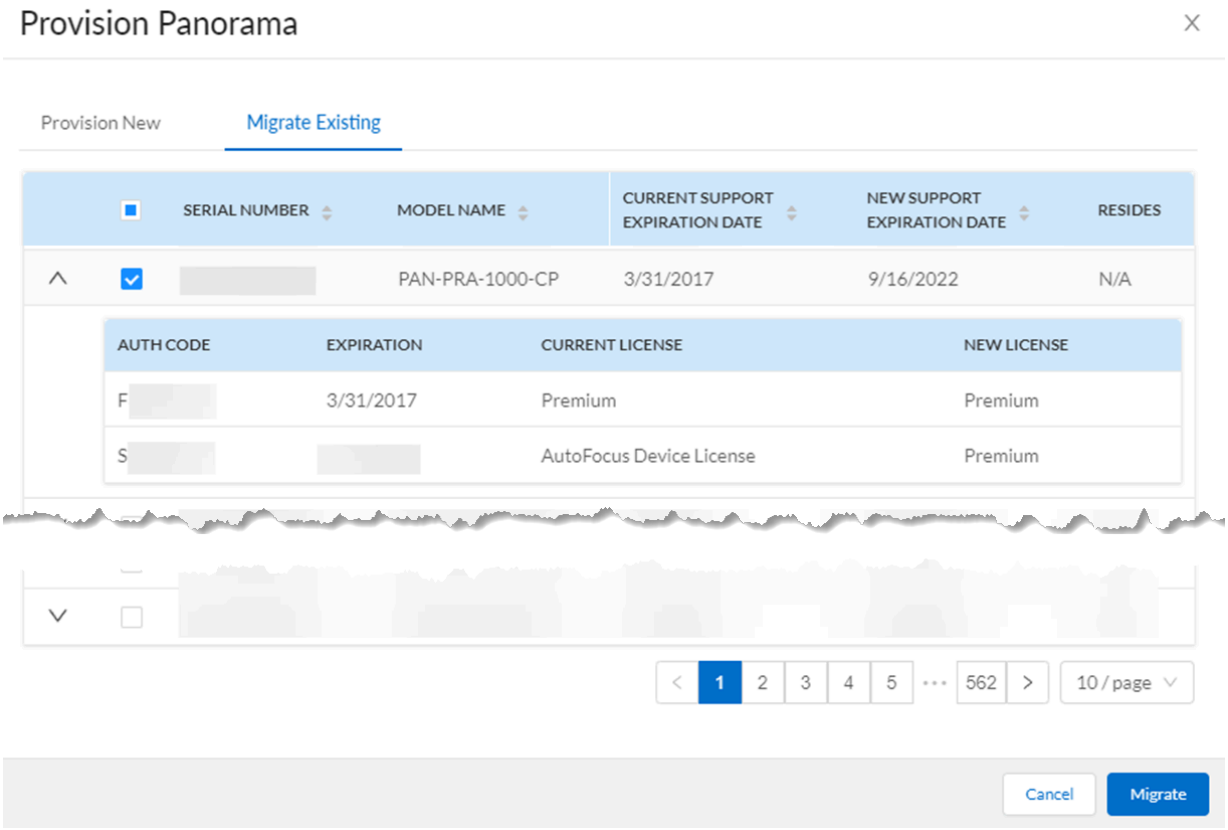
CSP 显示与当前支持帐户关联的所有虚拟 Panorama 设备。

©2024 Palo Alto Networks, Inc.

STEP 3 | 选择 **Provision New**（配置新的），然后选中要迁移的每个虚拟 Panorama 的复选框，然后选择 **Migrate**（迁移）。

迁移的 Panorama 显示为软件 NGFW 设备。

STEP 4 | 验证 **Current Support Expiration Date**（当前支持到期日期）是否已更新。此外，您可以展开每一行以查看应用到所选 Panorama 的各个许可证。



传输积分

从客户支持门户 (CSP)，将积分转移到同一帐户下的积分池（同一合同下的不同积分池）中，或者转移到您可以访问的不同帐户下的积分池中。

积分必须在同一合同（父/子）内的资金池之间转移。

- 不同的 CSP 帐户
- 此帐户中的不同积分池

©2024 Palo Alto Networks, Inc.

不同的 CSP 帐户

STEP 1 | 登录您的 CSP 帐户。

STEP 2 | 选择 **Assets**（资产）> **Software NGFW Credits**（软件 **NGFW** 积分）。

- 识别源积分池并记下积分池 ID。
- 识别目标积分池并记下积分池 ID。

  如果目标在不同帐户中，请从左上角的 **Current Account**（当前帐户）下拉列表中选择，然后选择 **Assets**（资产）> **Software NGFW Credits**（软件 **NGFW** 积分）。找到目标并记录积分类型和积分池 ID。

STEP 3 | 转到源积分池，然后单击左下角的 **Transfer Credits**（传输积分）。

STEP 4 | 选择不同的 CSP 帐户。

1. **Transfer to**（传输到）— 选择帐户名称。
2. **As credit type**（作为积分类型）— 选择积分类型。此时，源类型和目标类型必须相同。
3. **Credit Pool ID#**（积分池 **ID** 号）— 选择积分池 ID 号。

   如果目标帐户没有任何所选类型的积分池，则 CSP 会提示您创建积分池。
4. **Amount to transfer**（传输数量）— 输入传输数量。

STEP 5 | 选择 **Update Credits**（更新积分）。

您可能需要稍等片刻或刷新屏幕才能看到更改。

STEP 6 | 要查看积分池中的积分交易，请选择 **Details**（详细信息），然后选择 **Audit Trail**（审核线索）。

此帐户中的不同积分池

STEP 1 | 登录您的 CSP 帐户。

STEP 2 | 选择 **Assets**（资产）> **Software NGFW Credits**（软件 **NGFW** 积分）。

- 识别目标积分池并记下积分池 ID。
- 如果没有您指定类型的目标积分池，则系统会提示您创建新的积分池。

STEP 3 | 转到源积分池，然后选择左下角的 **Transfer Credits**（传输积分）。

STEP 4 | 选择 **Different Pool in this Account**（此帐户中的不同积分池）。

1. **New credit type**（新积分类型）— 选择积分类型。此时，源类型和目标类型必须相同。
2. **Credit Pool ID#**（积分池 **ID** 号）— 选择积分池 ID 号。

   如果目标帐户没有任何所选类型的积分池，则 CSP 会提示您创建积分池。
3. **Amount to transfer**（传输数量）— 输入传输数量。

©2024 Palo Alto Networks, Inc.

STEP 5 | 选择 **Update Credits**（更新积分）。

您可能需要稍等片刻或刷新屏幕才能看到更改。

STEP 6 | 要查看积分池中的积分交易，请选择 **Details**（详细信息），然后选择 **Audit Trail**（审核线索）。

如果您想在积分池之间转移积分，则两个积分池的到期日期必须相同。

续订软件 NGFW 积分合同

当部署配置文件过期时，它会从“当前部署配置文件”选项卡移到“续订配置文件”选项卡中。但是，如果续订合同而积分额度等于或大于续订前的积分额度，则部署配置文件会自动移回到“当前部署配置文件”选项卡下，无需采取进一步的操作。如果在续订时减少积分池中的积分数量，则必须使用新的积分数量手动续订部署配置文件。在“续订配置文件”选项卡下，您可以在不中断 VM 系列防火墙操作的情况下续订任何部署配置文件。在部署配置文件过期并移至“续订配置文件”选项卡中后，您有 30 天时间来续订配置文件。任何未在 30 天内续订的部署配置文件都会移至“过期的部署配置文件”选项卡下。如需更多信息，请参阅 许可证到期后会发生什么？。

续订后，您可能会发现新的配置文件与之前的部署配置文件有所不同。现在，*“Prisma NGFW* 积分”与“虚拟 *NGFW* 积分”积分池都称为“软件 *NGFW* 积分”积分池。此外，由于产品定价模型的变化，您的积分池中的积分数量可能会在续订后发生变化。

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

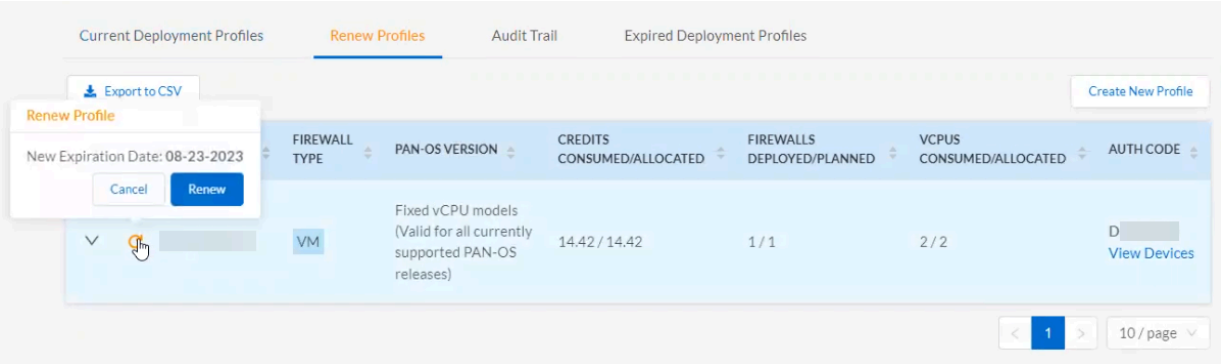
STEP 2 | 选择 **Assests**（评估） > **Software NGFW Credits**（软件 **NGFW** 积分）。

STEP 3 | 找到要续订的部署配置文件，然后单击 **Details**（详细信息）。

STEP 4 | 选择 **Renew Profiles**（续订配置文件）。

©2024 Palo Alto Networks, Inc.

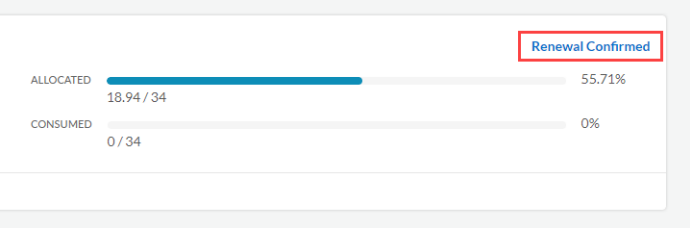
STEP 5 | 单击“续订”图标，然后单击 **Renew**（续订）以进行确认。



STEP 6 | 验证部署配置文件是否已续订成功。

1. 单击 **Current Deployment Profiles**（当前部署配置文件）。
2. 确认续订的部署配置文件显示正常。

   此外，您可以返回“软件 NGFW 指示板”来查看您的积分池。续订成功后，积分池会显示 **Renewal Confirmed**（已确认续订）。此消息将一直保留到续订的软件 NGFW 积分到期日期。



停用许可证（软件 NGFW 积分）

在删除防火墙（或托管防火墙的 VM）之前，您必须停用 CSP 的任何许可证，否则许可证积分将无法返回到您的积分池。

当您通过 Internet 访问许可服务器时，停用 CSP 上的防火墙会自动删除许可证，并将剩余积分返回到部署配置文件。停用许可证后，您必须删除防火墙，否则它将继续消耗积分。

如果您无法访问 Internet，则必须从防火墙导出许可证令牌。然后，在 CSP 中开始停用并上传令牌（或粘贴令牌文本）以完成停用。

- 允许访问 Internet
- 无互联网接入
- 无法访问 Internet - Panorama 管理

©2024 Palo Alto Networks, Inc.

直接访问 Internet。

1. 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后单击用于创建部署配置文件的积分池上的 **Details**（详细信息）按钮。
2. 找到您的部署配置文件，并在最右侧选择垂直省略号（More Options（更多选项）），然后选择 **Deactivate Firewall**（停用防火墙）。
3. 选择您要停用的防火墙，然后选择 **Deactivate Firewall**（停用防火墙）。

无法访问 Internet。

1. 登录防火墙 Web 界面，然后选择 **Device**（设备） > **Licenses**（许可证）。
2. 在 License Management（许可证管理）部分中，选择 **Deactivate VM**（停用 **VM**）。

   验证要在防火墙上停用的许可证/权利列表。
3. 选择 **Complete Manually**（手动完成）以开始停用。

   单击导出许可证令牌链接以将令牌许可证保存到客户端。令牌文件名如下所示：`20150128_1307_dact_lic.01282015.130737.tok`

   此时，已在防火墙上停用许可证，但尚未将积分返回积分池。
4. 使用令牌文件将更改注册到许可服务器：
   1. 登录到 Palo Alto Networks 客户支持网站。
   2. 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码） > **Deactivate License(s)**（停用许可证）.

   在停用许可证表单中，粘贴令牌文本，或将令牌复制到可以访问 Internet 的计算机，然后将令牌文件上传到 CSP 以完成许可证删除。
5. 删除虚拟机

©2024 Palo Alto Networks, Inc.

无法访问 Internet — Panorama 管理

1. 登录到 Panorama Web 界面，然后选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证）。
2. 选择 **Deactivate VMs**（停用 **VM**），然后选择您要停用的 VM 系列防火墙。
3. 选择 **Complete Manually**（手动完成）以导出令牌文件。
4. 单击导出许可证令牌链接以保存令牌文件。令牌文件名如下所示：20150128_1307_dact_lic.01282015.130737.tok

   如果导出成功，系统会显示完成消息，并且防火墙会自动重新启动。
5. 使用令牌文件将更改注册到许可服务器。
   1. 登录到 Palo Alto Networks 客户支持网站。
   2. 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码） > **Deactivate License(s)**（停用许可证）.

   在停用许可证表单中，粘贴令牌文本，或将令牌复制到可以访问 Internet 的计算机，然后将令牌文件上传到 CSP 以完成许可证删除。
6. （可选）删除已停用的 VM 系列防火墙，将其作为 Panorama 上的托管设备。

   您可以创建单独的设备组并将其分配给防火墙，而不是删除已停用的防火墙。

   1. 选择 **Panorama** > **Managed Devices**（Panorama > 受管设备）。
   2. 选择您停用的防火墙，然后单击 **Delete**（删除）。

解除非正常终止防火墙的许可

您可以通过客户支持门户解除失去访问权限或意外终止的防火墙的许可。例如，如果管理程序崩溃，或者意外删除了防火墙而又无法再登录到该防火墙，请完成以下过程以取消该防火墙的许可并释放软件 NGFW 积分，以供将来使用。

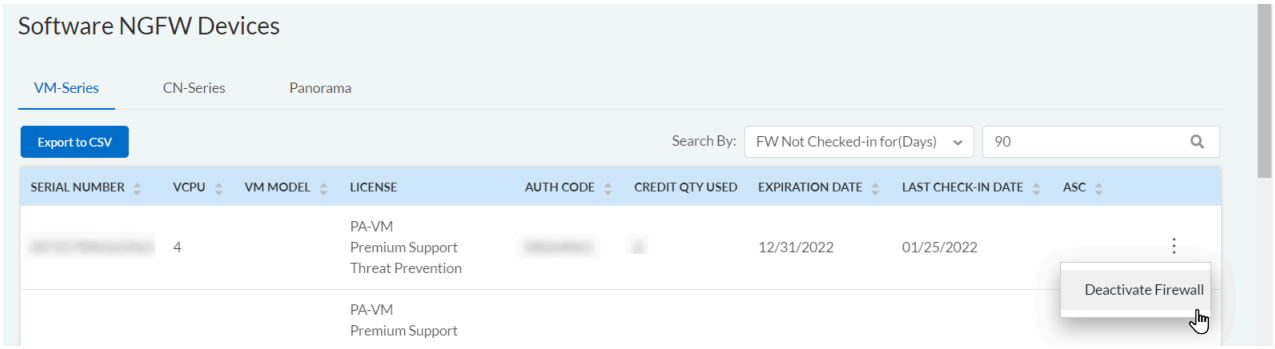
STEP 1 | 登录到客户支持门户。

STEP 2 | 选择 **Software NGFW Devices**（软件 **NGFW** 设备）。

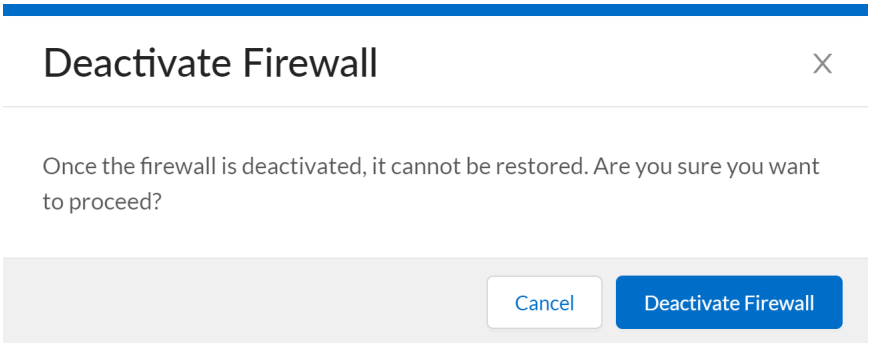
STEP 3 | 从 **Search By**（搜索依据）下拉列表中选择 **FW Not Checked-in for**（**FW** 未签入天数），然后输入要搜索的天数。

©2024 Palo Alto Networks, Inc.

STEP 4 | 要解除防火墙许可，请单击右侧的更多选项（垂直的三个点），然后单击 **Deactivate Firewall**（停用防火墙）。



STEP 5 | 单击 **Deactivate Firewall**（停用防火墙）以确认停用所选防火墙。停用防火墙后，积分将返还到积分池。



设置许可的 vCPU 数量

使用软件 NGFW 配额（而不是许可所选计算实例上可用的所有 vCPU）时，您可以指定许可的 vCPU 数量。这样，您可以使用更大的计算实例，而不会消耗不必要的软件 NGFW 配额。

此功能需要 *VM* 系列插件 *2.1.4* 或更高版本。

您可以使用 bootstrap plugin op 命令或 VM 系列防火墙 CLI 指定要许可的 vCPU 数量。

- 要在引导 VM 系列防火墙时设置核心数量，请将以下命令添加到 init-cfg.txt 文件中。

  plugin-op-commands=set-cores:<number-of-cores>

  例如：

  plugin-op-commands=set-cores:4

©2024 Palo Alto Networks, Inc.

- 要在已部署的 VM 系列防火墙上设置核心数量，请使用以下 CLI 命令。

  request plugins vm_series set-cores cores <number-of-cores>

  例如：

  request plugins vm_series set-cores cores 16

  您必须重新启动 VM 系列防火墙，此更改才会生效。

自定义数据平面核心

如软件 NGFW 积分中所述，当使用软件 NGFW 积分部署防火墙时，内存配置文件和 vCPU 总数决定自动分配给管理平面和数据平面的核心数量。在大多数情况下，默认配置运行正常。

自定义数据平面核心是一项可选功能，允许您通过两种方式自定义数据平面核心的数量：

- 在初始部署期间，使用 `init-cfg.txt` 文件引导参数 **plugin-op-commands=set-dp-cores:<#-cores>**。请参阅init-cfg.txt 文件组件。
- 从部署的防火墙中，使用 VM 系列 CLI 命令 **request plugins vm_series dp-cores <#-cores>**。此过程概述如下。

通常，您可以增加数据平面核心的数量（这会减少管理平面核心的数量）以提高性能。数据平面核心自定义不需要更改部署配置文件或其他积分，因为 vCPU 的总数保持不变。

- 运行 PAN-OS 10.1 或更高版本的防火墙支持数据平面核心自定义，该防火墙已获得 10.0.4 及更高版本的软件 NGFW 积分池许可。
- 以下插件不支持数据平面核心自定义：
  - NSX-T
  - 智能流量分流

按照以下步骤自定义 VM 系列防火墙上的数据平面核心。

STEP 1 | 登录 VM 系列防火墙并查看核心数量。

```
admin@PA-VM(active)>show plugins vm_series dp-cores
Device current DP cores:13 (Total cores:18)
```

STEP 2 | 更改数据平面核心的数量。

请注意，您至少必须拥有一个管理平面核心，核心太少会影响性能。

在本示例中，我们将数据平面核心增加到 14 个。

```
admin@PA-VM(active)>request plugins vm_series dp-cores 14
Device current DP cores:14 (Total cores:18)
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 重新启动 VM 系列防火墙。

选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后单击 **Reboot Device**（重新引导设备）。

STEP 4 | 使用 **`show plugins vm_series dp-cores`** 验证数据平面核心数量是否已更改。

将防火墙迁移到灵活 VM 系列许可证

您可以将 VM 系列防火墙永久许可证或 ELA 许可证迁移到灵活 VM 系列防火墙许可证（使用软件 NGFW 积分资助）。通过 Panorama，您可以同时在单个防火墙或多个防火墙上切换许可证。

使用此过程从评估许可证迁移到非评估积分池授权代码，而不会造成服务中断。

完成以下过程之一以迁移您的许可证。

- 可访问 CSP 的独立防火墙
- 独立防火墙，无法访问 CSP
- 可访问 CSP 的 Panorama 托管防火墙
- 无法访问 CSP 的 Panorama 托管防火墙
- 无法访问 CSP 的 Panorama 托管防火墙和 Panorama
- 验证迁移

可访问 CSP 的独立防火墙

此过程不会中断通过防火墙的流量。

STEP 1 | 登录到 VM 系列防火墙 Web 接口。

STEP 2 | 验证 Palo Alto Networks 更新服务器配置。

1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）。
2. 确认 **Update Server**（更新服务器）设置为 `updates.paloaltonetworks.com`。
3. 确认已选择 **Verify Update Server Identity**（验证更新服务器标识）。

STEP 3 | 登录 CSP 并创建部署配置文件。如果您要迁移的许可证适用于具有 ELA 许可证或永久许可证的 VM 系列防火墙，则在为灵活许可证创建软件 NGFW 部署配置文件时，您必须选择 **Fixed Models**（固定型号）并使用相同的 VM 系列型号和 vCPU 数量。

您将使用此配置文件中的授权代码。灵活防火墙许可证的授权代码以字母 D 开头，如下所示。

©2024 Palo Alto Networks, Inc.

STEP 4 | 选择 **Device** > **Licenses**（设备 > 许可证）。

如果当前的 VM 系列型号与您要迁移到的 VM 系列型号不同，请选择 **Upgrade VM Capacity**（升级 **VM** 容量）链接。

如果 VM 系列型号在迁移前后相同，请选择 **Activate feature using authorization code**（使用授权代码激活功能）链接。

STEP 5 | 输入新部署配置文件中的 VM 系列授权代码。

STEP 6 | 单击 **OK**（确定）以确认许可证升级。防火墙与 Palo Alto Networks 更新服务器建立连接，并根据 VM 系列型号使用防火墙所需的令牌。

STEP 7 | （可选）验证迁移。

STEP 8 | 为部署中的每个 VM 系列防火墙重复此步骤。

独立防火墙，无法访问 CSP

迁移无法访问 CSP 的防火墙的许可证。

STEP 1 | 如有必要，请在 VM 系列防火墙上安装许可证 API 密钥。

STEP 2 | 使用 CLI 以使用手动模式停用固定型号许可证。

STEP 3 | 从防火墙停用 VM 使用手动过程，然后登录 CSP 并使用令牌文件停用 VM。

STEP 4 | 在 CSP 中，创建部署配置文件 与之前的固定型号许可证具有相同的 VM 系列型号、vCPU 数量和安全订阅。您将使用此配置文件中的授权代码。

STEP 5 | 选择新的配置文件并单击垂直省略号，然后选择 **Register Firewall**（注册防火墙）。

1. 输入 VM 和防火墙信息，然后选择 **Submit**（提交）。这会将防火墙与配置文件及其授权代码相关联，并分配序列号。
2. 单击 **View Devices**（查看设备）以查看 **Software NGFW Devices**（软件 **NGFW** 设备）中的关联设备。
3. 在 **License**（许可证）列中，将许可证密钥下载到可以安全地将文件传输到主机的位置。

STEP 6 | 在防火墙上，选择 **Device**（设备） > **Licenses**（许可证）。

许可证密钥必须通过 *Web* 界面安装。防火墙不支持通过 *SCP* 或 *FTP* 安装许可证密钥。

STEP 7 | 单击 **Manually Upload License**（手动上传许可证），并输入许可证密钥。

STEP 8 | 确认 **Dashboard**（仪表盘）显示有效的序列号，并且 **PA-VM** 许可证显示在 **Device**（设备） > **Licenses**（许可证）选项卡中。

STEP 9 | （可选）验证迁移。

©2024 Palo Alto Networks, Inc.

可访问 CSP 的 Panorama 托管防火墙

在 Panorama 托管防火墙上从固定许可证迁移到灵活许可证。

STEP 1 | 在开始之前，请确保在防火墙上安装许可证 API 密钥。

STEP 2 | 登录到 Panorama Web 界面。

STEP 3 | 验证防火墙的 Palo Alto Networks 更新服务器配置。

1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）。
2. 确认 **Update Server**（更新服务器）设置为 `updates.paloaltonetworks.com`。
3. 确认已选择 **Verify Update Server Identity**（验证更新服务器标识）。

STEP 4 | 如果未这样操作，请为新许可证创建部署配置文件。为迁移的 Panorama 生成新的授权代码需要此配置文件。

STEP 5 | 检索 VM 系列授权代码。灵活许可证的防火墙授权代码以字母 F 开头，如下所示。

STEP 6 | 应用新的授权代码。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证）和 **Activate**（激活）。
2. 输入 VM 系列授权代码。
3. 使用筛选器选择要许可的托管防火墙。
4. 对于每个防火墙，在 **Auth Code**（授权代码）列中输入授权代码。
5. **Activate**（激活）以确认许可证升级。Panorama 与 Palo Alto Networks 更新服务器建立连接，并根据 VM 系列型号、vCPU 数量和选定服务使用防火墙所需的令牌。

STEP 7 | （可选）。

无法访问 CSP 的 Panorama 托管防火墙

迁移无法访问 CSP 的 Panorama 托管 VM 系列防火墙。

STEP 1 | 在开始之前，请确保在防火墙上安装许可证 API 密钥。

STEP 2 | **Panorama** 无法访问 **Internet** — 迁移离线 Panorama 托管防火墙上的许可证。

STEP 3 | 从 Panorama 停用 VM 使用手动过程，然后登录 CSP 并使用令牌文件停用 VM。

STEP 4 | 在 CSP 中，创建部署配置文件 与固定型号许可证具有相同的 VM 系列型号、vCPU 数量、安全订阅和 Panorama。您将使用此配置文件中的授权代码。

©2024 Palo Alto Networks, Inc.

STEP 5 | 选择新的配置文件并单击垂直省略号，然后选择 **Register Firewall**（注册防火墙）。

1. 输入 VM 和防火墙信息，然后选择 **Submit**（提交）。这会将防火墙与配置文件及其授权代码相关联，并分配序列号。
2. 单击 **View Devices**（查看设备）以查看 **Software NGFW Devices**（软件 **NGFW** 设备）中的关联设备。
3. 在 **License**（许可证）列中，将许可证密钥下载到可以安全地将文件传输到主机的位置。

STEP 6 | 应用新的授权代码。

1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证），然后单击 **Activate**（激活）。
2. 使用筛选器选择要许可的托管防火墙。
3. 在每个防火墙的 **Auth Code**（授权代码）列中输入部署配置文件中的授权代码。
4. 单击 **Activate**（激活）以确认许可证升级。Panorama 与 Palo Alto Networks 更新服务器建立连接，并根据 VM 系列型号、vCPU 数量和选定服务使用防火墙所需的令牌。

STEP 7 | （可选）验证迁移。

无法访问 CSP 的 Panorama 托管防火墙和 Panorama

当 Panorama 和托管防火墙都无法访问 CSP 时，迁移托管防火墙上的许可证。

STEP 1 | 如有必要，请在 VM 系列防火墙上安装许可证 API 密钥。

STEP 2 | 使用 CLI 以使用手动模式停用固定型号许可证。

STEP 3 | 从防火墙停用 VM 使用手动过程，然后登录 CSP 并使用令牌文件停用 VM。

STEP 4 | 在 CSP 中，创建部署配置文件 与之前的固定型号许可证具有相同的 VM 系列型号、vCPU 数量和安全订阅。您将使用此配置文件中的授权代码。

STEP 5 | 选择新的配置文件并单击垂直省略号，然后选择 **Register Firewall**（注册防火墙）。

1. 输入 VM 和防火墙信息，然后选择 **Submit**（提交）。这会将防火墙与配置文件及其授权代码相关联，并分配序列号。
2. 单击 **View Devices**（查看设备）以查看 **Software NGFW Devices**（软件 **NGFW** 设备）中的关联设备。
3. 在 **License**（许可证）列中，将许可证密钥下载到可以安全地将文件传输到主机的位置。

STEP 6 | 在防火墙上，选择 **Device**（设备） > **Licenses**（许可证）。

许可证密钥必须通过 *Web* 界面安装。防火墙不支持通过 *SCP* 或 *FTP* 安装许可证密钥。

STEP 7 | 单击 **Manually Upload License**（手动上传许可证），并输入许可证密钥。

©2024 Palo Alto Networks, Inc.

STEP 8 | 确认 **Dashboard**（仪表盘）显示有效的序列号，并且 **PA-VM** 许可证显示在 **Device**（设备）> **Licenses**（许可证）选项卡中。

STEP 9 | （可选）验证迁移。

验证迁移

验证许可证迁移是否成功。

STEP 1 | 在设备上，检查许可证到期日期以验证许可证是否已成功更新。

STEP 2 | 验证在部署配置文件中启用的所有订阅是否已应用于您的设备。

STEP 3 | 在 CSP 上，根据您的积分池匹配验证分配的预期积分数量和消耗的积分数量。

STEP 4 | 在 CSP 上，验证关联的令牌或许可证数量是否已返回您之前的授权代码。

软件 NGFW 许可 API

使用软件 NGFW 许可 API 创建和管理积分池授权代码，检索附加到授权代码的积分池，VM 系列防火墙上的所有基于模型的许可证。此外，许可 API 可让您许可无法直接访问 Internet 且无法访问 Palo Alto Networks 许可服务器的防火墙。您可以手动管理许可证或使用自定义脚本或编排服务自动许可。

要使用 API，每个支持帐户都会获得一个唯一的客户端 ID 和客户端机密。使用与您的客户支持帐户相关联的客户端 ID 和客户端机密来生成访问令牌。每个 API 调用都必须包含访问令牌以验证对许可服务器的请求。通过身份验证后，许可服务器将会以 json 格式（内容类型应用程序/json）发送响应。

- 获取软件 NGFW API 身份验证令牌
- 使用许可 API 管理部署配置文件
- 使用许可 API 创建部署配置文件
- 使用许可 API 更新部署配置文件

获取软件 NGFW API 身份验证令牌

要通过客户支持门户进行身份验证，您必须在所有 API 调用的标题中提供 OAuth 令牌。此令牌与您的 Palo Alto Networks 客户支持帐户相关联，必须在进行任何其他 API 调用之前生成。

联系销售代表，获取您的 *client_id* 和 *client_secret*。

生成令牌后，从 API 响应中复制整个令牌，以便在其他软件 NGFW API 中使用。

请求主题参数：**client_id**、**client_secret**、**grant_type=client_credentials**、**scope=fwflex-service**

©2024 Palo Alto Networks, Inc.

grant_type 的值必须是 ***client_credentials***，***scope*** 的值必须是 ***fwflex-service***。

请求方法：POST

URL：https://identity.paloaltonetworks.com/as/introspect.oauth2

使用 **JSON** 进行初始许可证激活时的示例请求：

```
curl --location --request POST 'https://
identity.paloaltonetworks.com/as/token.oauth2' \ --data-urlencode
 'client_id=customer-clientid-1' \ --data-urlencode 'client_secret='
 \ --data-urlencode 'grant_type=client_credentials' \ --data-
urlencode 'scope=fwflex-service'
```

示例 **API** 响应：

```
{ "access_token":eyJhifQ.eyJzY29wZSI6WyJmd2ZsZXgtc2VydmljZSJdLCJjbGllbnRfaWQiOi
fgZA6XPbHaml5fLpXOtsQ_IkmnxeDnJmcF-
K3akxgalQ8RA3GutHnKGoIX_JhYGqREHwHiWwgVm3ahK58ygCJDBb3z4BpOtTAnkejCp9k2ke1a4d_u
 "token_type":"Bearer" "expires_in":7199 }
```

使用许可 API 管理部署配置文件

使用以下 API 检索有关现有部署配置文件的信息或删除不再使用的部署配置文件。

- 获取所有积分池
- 通过积分池 ID 获取积分池
- 获取积分池中的所有部署配置文件
- 获取部署配置文件
- 删除部署配置文件

获取所有积分池

使用此 API 检索有关与 CSP 帐户相关联的所有积分池的信息。

标头参数：**token**

请求方法：入

URL：https://api.paloaltonetworks.com/tms/v1/creditPool

示例 **API** 请求：

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/creditPool' \ --header 'token: <your-token>'
```

示例 **API** 响应：

```
{ "data": [ { "creditPoolId":31586#####, "poolName":"Software NGFW
 Credits", "supportType":"Platinum", "expirationDate":"02/07/2026",
 "totalCredits":27.84, "creditsAllocated":0.0, "creditsConsumed":0.0,
```


©2024 Palo Alto Networks, Inc.

```
 "creditsAvailable":27.84 }, { "creditPoolId":99394#####,
 "poolName":"Software NGFW Credits", "supportType":"Premium",
 "expirationDate":"10/27/2023", "totalCredits":47.0,
 "creditsAllocated":13.68, "creditsConsumed":0.0,
 "creditsAvailable":33.32 }, { "creditPoolId":90775#####,
 "poolName":"Software NGFW Credits", "supportType":"Premium
Partner", "expirationDate":"04/13/2025", "totalCredits":34.0,
 "creditsAllocated":0.0, "creditsConsumed":0.0,
 "creditsAvailable":34.0 } ] }
```

通过积分池 **ID** 获取积分池

标头参数：**token**

路径参数：**creditPoolId**

请求方法：入

URL：**https://api.paloaltonetworks.com/tms/v1/creditPool/{creditPoolId}**

示例 **API** 请求：

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/creditPool/<creditPoolId>' \ --header 'token: <your-token>'
```

示例 **API** 响应：

```
{ "data": { "creditPoolId":97101#####, "poolName":"Software NGFW
 Credits", "supportType":"Premium", "expirationDate":"02/20/2026",
 "totalCredits":194.0, "creditsAllocated":172.75,
 "creditsConsumed":43.94, "creditsAvailable":21.25 } }
```

获取积分池中的所有部署配置文件

使用此 API 获取特定部署配置文件的详细信息。

标头参数：**token**

路径参数：**creditPoolId**

请求方法：入

URL：**https://api.paloaltonetworks.com/tms/v1/creditPool/{creditPoolId}/
deploymentProfile**

示例 **API** 请求：

```
curl --location --request GET 'https://api.paloaltonetworks.com/
tms/v1/creditPool/<creditPoolId>/deploymentProfile' \ --header
 'token:<your-token>'
```

示例 **API** 响应：

```
{ "data": [ { "profileName":"Credit Pool 1",
 "dAuthCode":"D#######", "type":"VM", "panOsVersion":"10.0.4_or-
above", "creditsAllocated":41.860000610351562,
```

 ©2024 Palo Alto Networks, Inc.

```
 "creditsConsumed":20.930000305175781, "vCpuConsumed":2,
 "vCpuAllocated":4, "fWsDeployed":1, "fWsPlanned":2,
 "status":"Updated" }, { "profileName":"Credit Pool 2",
 "dAuthCode":"D#######", "type":"VM", "panOsVersion":"10.0.3_or-
below", "creditsAllocated":32.200000762939453, "creditsConsumed":0.0,
 "vCpuConsumed":0, "vCpuAllocated":4, "fWsDeployed":0,
 "fWsPlanned":2, "status":"Created" } ] }
```

获取部署配置文件

使用此 API 获取特定部署配置文件的详细信息。

标头参数：**token**

路径参数：**authCode**

请求方法：入

URL: **https://api.paloaltonetworks.com/tms/v1/deploymentProfile/{authCode}**

示例 **API** 请求：

```
curl --location --request GET 'https://api.paloaltonetworks.com/tms/
v1/deploymentProfile/<authCode>' \ --header 'token:<your-token>'
```

示例 **API** 响应：

```
{ "data": { "profileName": "deployment-profile-1",
 "dAuthCode":"D#######", "type":"VM", "panOsVersion":"10.0.3_or-
below", "creditsAllocated":43.7, "creditsConsumed":0.0,
 "vCpuConsumed":0, "vCpuAllocated":8, "fWsDeployed":0,
 "fWsPlanned":1, "status":"Updated" } } }
```

删除部署配置文件

使用此 API 删除特定的部署配置文件。

标头参数：**token**

路径参数：**authCode**

请求方法：DELETE

URL：**https://api.paloaltonetworks.com/v1/deployment-profile/auth-code/{auth-code}**

示例 **API** 请求：

```
curl --location --request DELETE 'https://api.paloaltonetworks.com//
tms/v1/deploymentProfile/<authCode>' \ --header 'token:<your-token>'
```

示例 **API** 响应：

```
{ "isDeleted": true, "dAuthcode":"D#######", "message":"Deleted" }
```

 ©2024 Palo Alto Networks, Inc.

使用许可 API 创建部署配置文件

标头参数：`token`

请求主体参数：`creditPoolId`、`name`、`type`、`panOs`、`firewallQuantity`、`vCpuQuantity`、`panorama` 和 `subs`

请求方法：POST

网址：**`https://api.paloaltonetworks.com/tms/v1/deploymentProfile`**

使用以下 API 创建新的部署配置文件，从而使用软件 NGFW 积分为 VM 系列和 CN 系列防火墙授予许可。API 响应返回将用于为防火墙授予许可的软件 NGFW 授权代码。

参数	说明
`creditPoolId` 这是必需参数。	该署配置文件使用在此处输入的 ID 编号以添加到积分池中。
名称	部署配置文件名称。
类型 这是必需参数。	对于 VM 系列，请输入 **`vm`**。
`panOs`	对于灵活的 vCPU VM 系列防火墙，请输入 **`10.0.4_or_above`**。 对于固定型号 VM 系列防火墙，请输入 **`10.0.3_or-below`**
`firewallQuantity` 这是必需参数。	防火墙数量。该值必须大于零 (0)。
`vCpuQuantity`	每个防火墙的计划 vCPU 数量。 如果将 **`type`** 设置为 VM-Flex，那么这是一个必需的参数。此外，vCPU 值必须大于零 (0) 且小于或等于 64。
`vmModel`	在为固定模型 VM 系列防火墙创建部署配置文件时需要此参数。 • 对于 VM-50，请输入 **`50`**。 • 对于 VM-100，请输入 **`100`**。 • 对于 VM-300，请输入 **`300`**。

©2024 Palo Alto Networks, Inc.

参数	说明
	• 对于 VM-500，请输入 **500**。 • 对于 VM-700，请输入 **700**。
panorama	通过此参数可使用软件 NGFW 积分来启用 Panorama。使用 **PAN** 启用 Panorama 或 **DLC**，从而将 Panorama 作为专用日志收集器。
subscriptions	指定要添加到部署配置文件的订阅。您可以输入多个订阅，但有一些限制。 • 威胁防御 (TP) • 高级威胁防护 (ATP) • URL 过滤 (URL4) • Advanced URL Filtering (AURL) • DNS (DNS) • Global Protect (GP) • DLP (DLP) • Wildfire (WF) • Advanced Wildfire (AWF) • SD-WAN (SDWAN) • 智能流量分流（ITO） • Web 代理 (WP) 如果将 **panOsVersion** 留空，则此字段是为必填字段。

示例 **API** 请求：

```
curl --location --request POST 'https://api.paloaltonetworks.com/
tms/v1/deploymentProfile' \ --header 'token: <your-token>'
 \ --header 'Content-Type: application/json' \ --data-raw
 '{ "creditPoolId":97101#####, "name":"3-16-1", "type":"VM",
 "panOS":"10.0.4_or-above", "firewallQuantity":1, "vCpuQuantity":2,
 "panorama": [ "Management", "LogCollector" ], "subscriptions":
 [ "DNS", "GP", "DLP" ] }'
```

示例 **API** 响应：

```
{ "profileId":29###, "authCode":"D#######", "success": true,
 "message":"Deployment profile saved successfully." }
```


©2024 Palo Alto Networks, Inc.

响应返回完整的授权代码。

使用许可 API 更新部署配置文件

路径参数：`authCode`

标头参数：`token`

请求主体参数：`creditPoolId`、`name`、`type`、`panOs`、`firewallQuantity`、`vCpuQuantity`、`panorama` 和 `subs`

请求方法：修补程序

URL：`https://api.paloaltonetworks.com/tms/v1/deploymentProfile/{authCode}`

使用以下 API 更新现有部署配置文件，从而使用软件 NGFW 积分为 VM 系列和 CN 系列防火墙授予许可。

参数	说明
`creditPoolId` 这是必需参数。	拥有正在更新的部署配置文件的积分池的信用池 ID。
名称	部署配置文件名称。如果提供名称，则必须是 CSP 帐户中唯一的名称。
类型 这是必需参数。	对于 VM 系列，输入 **`vm`**。
`panOs`	对于灵活的 vCPU VM 系列防火墙，请输入 **`10.0.4_or_above`**。 对于固定型号 VM 系列防火墙，请输入 **`10.0.3_or-below`**
`firewallQuantity` 这是必需参数。	防火墙数量。该值必须大于零 (0)。
`vCpuQuantity`	每个防火墙的计划 vCPU 数量。 如果将 **`type`** 设置为 VM-Flex，那么这是一个必需的参数。此外，vCPU 值必须大于零 (0) 且小于或等于 64。

©2024 Palo Alto Networks, Inc.

参数	说明
`vmModel`	在为固定模型 VM 系列防火墙创建部署配置文件时需要此参数。 • 对于 VM-50，请输入 **`50`**。 • 对于 VM-100，请输入 **`100`**。 • 对于 VM-300，请输入 **`300`**。 • 对于 VM-500，请输入 **`500`**。 • 对于 VM-700，请输入 **`700`**。
`panorama`	通过此参数可使用软件 NGFW 积分来启用 Panorama。使用 **`PAN`** 启用 Panorama 或 **`DLC`**，从而将 Panorama 作为专用日志收集器。
`subscriptions`	指定要添加到部署配置文件的订阅。您可以输入多个订阅，但有一些限制。 • 威胁防御 (TP) • 高级威胁防护 (ATP) • URL 过滤 (URL4) • Advanced URL Filtering (AURL) • DNS (DNS) • Global Protect (GP) • DLP (DLP) • Wildfire (WF) • Advanced Wildfire (AWF) • SD-WAN (SDWAN) • 智能流量分流（ITO） • Web 代理 (WP) 如果将 **`panOsVersion`** 留空，则此字段是为必填字段。

部署配置文件更新 **JSON** 的示例请求：

```
curl --location --request PATCH 'https://
apitest.paloaltonetworks.com/tms/v1/deploymentProfile/D7984130' \ --
header 'token: <your-token>' \ --header 'Content-Type: application/
json' \ --data-raw '{ "creditPoolId":97101#####, "name":"3-15-3",
 "type":"VM", "panOS":"10.0.4_or-above", "firewallQuantity":1,
```


©2024 Palo Alto Networks, Inc.

```
 "vCpuQuantity":2, "panorama": [ "LogCollector" ], "subscriptions":
 [ "URL4", "AIOPS" ] }'
```

示例 **API** 响应：

```
{ "profileId":29###, "authCode":"D#######", "success": true,
 "message":"Deployment profile saved successfully." }
```

响应返回完整的授权代码。

©2024 Palo Alto Networks, Inc.

VM 系列型号

VM 系列防火墙在以下固定 vCPU 型号中可用 — VM-50、VM-100、VM-200、VM-300、VM-500、VM-700 和 VM-1000-HV。这些型号适用于所有支持的 PAN-OS 版本，除非下面另有说明。用于部署 VM 系列防火墙的软件包（*.xva*、*.ova* 或 *.vhdx* 文件）对所有型号都适用。

您可以将固定型号 *ELA* 或永久许可证迁移为灵活许可证，同时保留固定型号，也可以将许可证替换为灵活 *vCPU* 许可证。要比较许可方法，请参阅VM 系列防火墙许可。

- 所有型号均可在 VMware ESXi 和 vCloud Air、KVM、Microsoft Hyper-V、Cisco ACI、Cisco ENCS 和 Cisco CSP 上部署为来宾虚拟机。
- 在公共云环境（Amazon Web Services、Azure、Google Cloud Platform、Oracle Cloud Infrastructure、Alibaba Cloud）中支持除 VM-50 之外的所有型号。
- 对于 VMware NSX，仅支持 VM-100、VM-200、VM-300、VM-500 和 VM-1000-HV 防火墙。

当您在 VM 系列防火墙上应用容量许可证时，型号及相关的容量将在防火墙上实施。容量根据 VM 系列防火墙最适合处理的会话、规则、安全区域、地址对象、IPSec VPN 隧道和 SSL VPN 隧道的数量定义。为确保您购买了适合您网络要求的正确型号，请通过下表了解各型号的最大容量以及基于型号的容量差异：

模型	会话	安全规则	动态 **IP** 地址	安全区域数	**IPSec VPN** 隧道	**SSL VPN** 隧道
VM-50	50,000	• 250 • 200（Lite 模式）	1,000	15	• 250 • 25（Lite 模式）	• 250 • 25（Lite 模式）
VM-100 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300 VM-1000-HV	800,000	10,000	100,000	40	2,000	2,000
VM-500	2,000,000	10,000	100,000	200	4,000	6,000
VM-700	10,000,000	20,000	100,000	200	8,000	12,000

©2024 Palo Alto Networks, Inc.

有关您可以在其中部署 VM 系列防火墙的平台的信息，请参阅 VM 系列部署。有关 VM 系列防火墙型号的更多信息，请参阅 Palo Alto Networks 防火墙比较工具。您也可以查看一般信息关于 VM 系列防火墙。

- VM 系列系统要求
- CPU 超额认购
- VM-50 Lite 模式
- VM 系列型号许可证类型
- 激活 VM 系列型号许可证
- 注册 VM 系列防火墙
- 在 VM 系列防火墙上安装设备证书
- 在 BYOL 和 PAYG 许可证之间切换
- 在 VM 系列型号许可证之间切换
- 停用许可证
- 更新 VM 系列防火墙许可证包
- 基于型号的许可 API

VM 系列系统要求

VM 系列防火墙的每个实例都需要最少的资源分配 — 主机服务器上的 CPU、内存和磁盘空间的数量。使用下表验证您是否为 VM 系列型号或内存配置文件分配必要的硬件资源。

PAN-OS 11.0 添加了其他特性和功能，因而需要更多内存。要提供与 PAN-OS 10.2 之前的版本相同的会话规模，需要增加最小内存分配。如果没有从 PAN-OS 11.0 之前的配置增加最小内存，则会减小最大会话规模。

VM 系列型号	支持的虚拟机监控程序	支持的 **VCPU**	最小内存	通过 **GTP** 启用最小内存	最小硬盘驱动器	最大（旧）会话计数	**PAN-OS 10.2** 中的扩展会话*	旧会话计数的建议内存
VM-50	ESXi、Hyper-V、KVM	2	• 5.5GB • 4.5GB（Lite 模式）	• 6GB • 5GB（Lite 模式）	32 GB（启动时 60GB）	• 65,000 • 50,000（Lite 模式）	• 50,000 • 25,000（Lite 模式）	• 6GB • 5.5GB（Lite
VM-100	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba	2	6.5GB	7.5GB	60GB	250,000	200，000	7GB

©2024 Palo Alto Networks, Inc.

VM 系列型号	支持的虚拟机监控程序	支持的 VCPU	最小内存	通过 GTP 启用最小内存	最小硬盘驱动器	最大（旧）会话计数	PAN-OS 10.2 中的扩展会话*	旧会话计数的建议内存
	Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-100) *Azure 上的 VM-100 需要 4 个 vCPU。*							
VM-300	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-300)	2、4	9GB**	10GB	60GB	800,000	600,000	10GB
VM-500	AWS、Azure、Cisco ACI、Cisco CSP、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、NSX-T	2、4、8	16GB	20GB	60GB	2,000,000	1,800,000	18GB
VM-700	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco	2、4、8、16	56GB	64GB	60GB	10,000,000	10,000,000	56GB

©2024 Palo Alto Networks, Inc.

VM 系列型号	支持的虚拟机监控程序	支持的 VCPU	最小内存	通过 GTP 启用最小内存	最小硬盘驱动器	最大（旧）会话计数	PAN-OS 10.2 中的扩展会话*	旧会话计数的建议内存
	ACI、Cisco CSP、NSX-T							

*固定型号 VM 系列防火墙，其许可证由软件 NGFW 积分提供资助。

**在 PAN-OS 10.2 中，9GB 空间可能不够，具体取决于防火墙上使用的功能集或功能集组合（例如 GTP 或高性能功能）。如果您遇到与内存资源相关的问题，请将内存增加到 11GB，从而满足某些功能或功能组合的额外内存需求。

您可以在 VM-50 上启用 Lite 模式。Lite 模式是用于资源有限环境中的替代操作模式。有关详细信息，请参阅 VM-50 Lite 模式。

为了达到最佳性能，所有必需的内核应该可以在一个 *CPU* 插槽上使用。

对于操作，*VM-50* 防火墙至少需要 *32GB* 的硬盘空间。但是，由于 *VM* 系列基本映像对所有型号都是通用的，因此您必须分配 *60GB* 的硬盘空间，直到您许可 *VM-50*。

分配给管理层的 vCPU 数量和分配给数据平面的 vCPU 数量取决于分配给 VM 系列防火墙的 vCPU 总数。如果分配的 vCPU 数量多于许可证正式支持的 vCPU 数量，则会将任何其他 vCPU 分配给管理层。

总 vCPU 数量	管理层 vCPU 数量	数据面 vCPU 数量
2	1	1
4	2	2
8	2	6
16	4	12

CPU 超额认购

VM 系列防火墙支持所有型号的 CPU 超额订阅。CPU 超额订阅允许您在运行于 x86 架构的虚拟机监控程序上部署更高密度的 VM 系列防火墙。按照所需的 CPU 分配，可以部署两个 (2:1) 到五个 (5:1) VM 系列防火墙。规划部署时，请使用以下公式计算硬件可支持的 VM 系列防火墙数量。

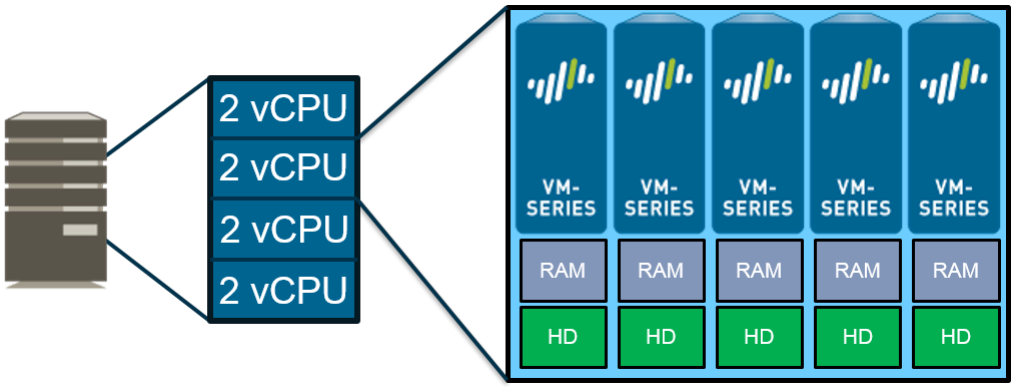
（总 CPU 数量 x OVERUB 比率）/每个防火墙的 CPU 数 = VM 系列防火墙的总数量

©2024 Palo Alto Networks, Inc.

例如，以 5:1 的比例，具有 16 个物理 CPU 和至少 180GB 内存 (40 × 4.5GB) 的主机可以支持多达 40 个实例到 VM-50。每个 VM-50 需要两个 vCPU，并且可将五个 VM-50 关联到每对 vCPU。

（16 个 CPU × 5）/2 = 40 个 VM-50 防火墙

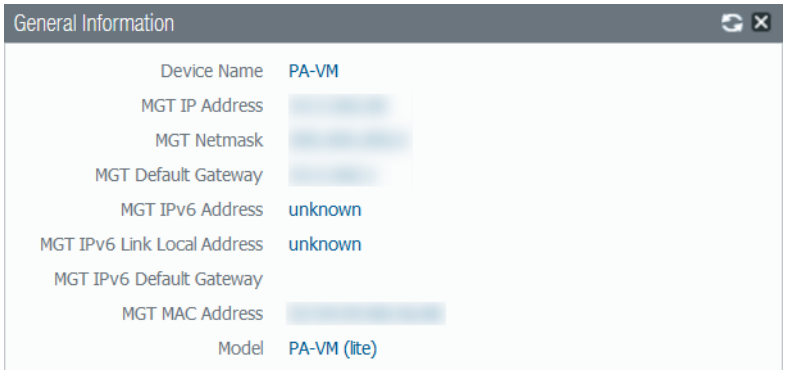
除最低 VM 系列系统要求以外，不需要额外的配置来利用超额订阅。正常部署 VM 系列防火墙并自动发生资源超额订阅。规划部署时，请考虑其他功能，如虚拟交换机和主机上需要自己的硬件资源的来宾计算机。



VM-50 Lite 模式

标准 VM-50 虽然是 VM 系列中的最小型号，但却需要比某些环境中更多的资源。VM-50 Lite 模式可在硬件资源受限的环境中提供备选方法。与标准 VM-50 需要 5.5GB 内存相比，VM-50 Lite 只需要 4.5GB 内存。VM-50 Lite 使用与标准 VM-50 相同的许可证，但在分配 4.5GB RAM 时以 Lite 模式启动。

- 在高可用性部署中，两个 *VM* 系列防火墙均必须作为 *VM-50 Lite* 来获取许可，以避免出现容量不匹配问题。如果出现容量许可证不匹配，则认定 *VM-50*（非 *Lite*）拥有较高的容量，而 *VM-50* 在 *VM-50 Lite* 仍正常运行时变得无法运行。
- *VM-50 Lite* 不支持 *Jumbo* 帧；*VM-50* 和 *VM-50 Lite* 不支持 *WildFire* 内联 *ML*。



©2024 Palo Alto Networks, Inc.

VM 系列型号许可证类型

不可再购买新容量许可证（非软件 *NGFW* 积分）。但是，您可以为容量（永久和基于期限）许可证续订一 *(1)* 年。

以下许可证和订阅均适用于 VM 系列防火墙：

- 容量许可证 — VM 系列防火墙需要基本许可证，又称容量许可证，以在防火墙上启用型号（VM-50、VM-100、VM-200、VM300、VM-500、VM-700 或 VM-1000-HV）及相关的容量。容量许可证包含在一个数据包中，可以是永久，也可以是有限的：
  - 永久许可证 — 无过期日期的许可证，拥有此许可证，即可无限期地以许可容量使用 VM 系列防火墙。永久许可证仅适用于 VM 系列容量许可。
  - 固定期限许可证 — 拥有固定期限许可证，即可在一段指定时期内使用 VM 系列防火墙。此种许可证有过期日期，您需要在其过期前进行更新。固定期限许可证适用于容量许可、支持授权和订阅。
- **VM** 系列 **ELA** — 对于高速成长的企业，VM 系列企业许可协议（VM 系列 ELA）提供固定价格的许可证选项，允许使用 BYOL 无限制部署 VM 系列防火墙。提供一年和三年期的 ELA 协议，在协议有效期间，内容无调整。

  VM 系列 ELA 有两个优势：
  - 如果在 2018 年 12 月 4 日之前购买了 VM 系列 ELA，则可以使用旧版 VM 系列 ELA，其中包括您在任何支持的虚拟机监控程序或公共云环境中选择的单个 VM 系列型号。凭借此 ELA，您可以获得用于 VM 系列防火墙每个实例的容量、支持、GlobalProtect、PAN-DB URL 筛选、威胁预防、WildFire 订阅的单一许可证授权代码。您还可以无限制地部署 Panorama 虚拟设备，其中每个部署包含 1000 个防火墙的设备管理许可证。

    Palo Alto Networks 于 2019 年 4 月 16 日开始逐步淘汰旧版 VM 系列 ELA。将现有企业的帐户迁移到多模型 ELA 时，支持代表将通知现有企业许可证客户。许可证令牌将根据 VM 系列防火墙订购协议进行分发 — 不需要执行其他操作来继续运行防火墙。如果要管理 VM 系列 ELA 许可证令牌，则必须指定一名 ELA 管理员。Palo Alto Networks 客户支持门户 (CSP) 上只有超级用户角色才能分配 ELA 管理员。
  - 在 2018 年 12 月 4 日之后购买VM 系列企业许可协议（多型号 ELA）（作为新购买或作为旧版 VM 系列 ELA 的回购）称为多模型 VM 系列 ELA，其中包括大多数 VM 系列防火墙产品组合以及 GlobalProtect、PAN-DB URL 筛选、威胁防护、WildFire 订阅和支持权利。您还可以无限制地部署 Panorama 虚拟设备，其中包含每个部署的 1000 个防火墙的设备管理许可证。

面向公共云的 VM 系列防火墙许可证

AWS、Azure 和 Google Cloud Platform 使用相同的 VM 系列防火墙许可证策略。有许多不同的许可证类别（请参阅 许可证类型 — VM 系列防火墙），有自带许可证和即用即付两种许可证方法：

©2024 Palo Alto Networks, Inc.

- 自带许可证 **(BYOL)** — 从合作伙伴、经销商处购买的许可证，或直接从 Palo Alto Networks 购买的许可证。BYOL 支持单容量许可证、支持许可证和订阅包。
  - 对于单个 BYOL 许可证，您必须在部署 VM 系列防火墙后应用授权代码。
  - BYOL 许可证包拥有可以包含在引导数据包中的单个授权代码（请参阅引导 VM 系列防火墙）。启动防火墙时，包中包含的所有订阅都将获得许可。

  OCI GovCloud 上 VM 系列防火墙的 BYOL 许可证需要 FIPS 和非 FIPS 模式的 PAN-OS 10.1.2 或更高版本。

- 即用即付 **(PAYG)**—也称为基于使用情况或按使用付费许可证。可从云提供商购买 PAYG 许可证：
  - AWS：从 AWS Marketplace 购买。支持按小时和按年 PAYG 选项。
  - Azure：从 Azure Marketplace 购买。支持按小时 PAYG 选项。
  - Google Cloud Platform：从 Google Cloud Platform Marketplace 购买。Google Cloud Platform 支持按分钟现收现付制 (PAYG) 选项。
  - Oracle 云基础架构：（PAN-OS 10.0.3 或更高版本）从 Oracle Cloud Marketplace 购买。

  OCI PAYG 许可证上的 VM 系列不支持 VM-100。

  在 PAYG 许可证包中，一旦完成了部署，防火墙即可获得许可并可供使用；您无需接收授权代码。当您停止或终止云控制台的防火墙时，PAYG 许可证将被暂停或终止。

  PAYG 许可证根据分配给实例的硬件应用 VM 系列容量许可证，PAYG 实例检查可用于实例的硬件资源数量，并为可用资源应用允许的最大 VM 系列防火墙容量许可证。例如，如果实例具有 2 个 vCPU 和 16GB 内存，根据 vCPU 的数量应用 VM-100 容量许可证。但是，如果实例具有 16 个 vCPU 和 16GB 内存，根据内存量应用 VM-500 容量许可证。有关 VM 系列模型资源要求的详细信息，请参阅 VM 系列系统要求。

  最初部署运行 *PAN-OS 9.1.2* 的 *PAYG* 防火墙实例不支持降级 *PAN-OS*。可以将在 *PAN-OS 9.1.2* 之前部署的防火墙实例降级到 *PAN-OS* 的更旧版本。

  PAYG 按如下方式绑定：

许可证功能	套餐 **1**	套餐 **2**	套餐 **3**
VM 系列防火墙容量许可证	VM-100、VM-300、VM-500、VM-700	VM-100、VM-300、VM-500、VM-700	VM-100、VM-300、VM-500、VM
高级支持	✓	✓	✓
威胁阻止（AV、IPS 和恶意软件预防）	✓	✓	
GlobalProtect		✓	✓

©2024 Palo Alto Networks, Inc.

许可证功能	套餐 1	套餐 2	套餐 3
PAN-DB URL Filtering		✓	
WildFire		✓	✓
DNS 安全		✓	✓
高级 URL 筛选			✓
高级威胁预防			✓

使用 *VM* 系列防火墙 *CLI* 查看应用的 *PAYG* 许可证时，命令 ***show system info*** 显示的值与命令 ***request license info*** 显示的输出不同。对于 *PAN OS* 版本 *9.1.1* 及更旧版本，命令 ***request license info*** 始终将型号显示为 *VM-300*，无论已应用的 *VM* 系列型号如何。

您不能在 PAYG 和 BYOL 许可证之间切换。要从 PAYG 转到 BYOL，请联系您的 Palo Alto Networks 渠道合作伙伴或销售代表购买 BYOL 许可证并获取可用于许可防火墙的 BYOL 授权代码。如果您已经部署了防火墙并希望切换许可证，请参阅在 BYOL 和 PAYG 许可证之间切换。

如果您有 *VM* 系列防火墙的评估版本，并且希望将其转换为同一许可证类型（*BYOL* 至 *BYOL*）的完全许可（购买）副本，则可以停用评估许可证并激活已购买的许可证。有关说明，请参阅升级 VM 系列防火墙。

VM 系列企业许可协议（多型号 ELA）

VM 系列企业许可协议（VM 系列 ELA）是一年或三年的综合许可协议，通过此协议，您可以购买 VM 系列防火墙，以及 GlobalProtect、PAN-DB URL 筛选、威胁防御、WildFire 和 DNS 安全订阅。它还包括 Panorama 的支持权利和设备管理许可证。多模型 VM 系列 ELA 通过单一合同提供简化的许可证管理，允许您部署满足企业安全需求的任何型号的 VM 系列防火墙。

购买多型号 VM 系列 ELA 时，您可以预测在订购期限内需要的防火墙数量。根据您的预测和适合未来增长的额外分配，您在客户支持门户 (CSP) 上的帐户将获得许可令牌池，允许您部署任何型号的 VM 系列防火墙。根据防火墙型号和部署的防火墙数量，将从可用的许可证令牌池中扣除指定数量的令牌。从您的帐户中提取的令牌是根据每个防火墙模型的值计算的：

- VM-50 — 10 个令牌
- VM-100 — 25 个令牌
- VM-300 — 50 个令牌
- VM-500 — 140 个令牌
- VM-700 — 300 个令牌

使用 VM 系列 ELA 时，在期限结束时没有任何应对措施，这意味着即使您部署的防火墙多于原始预测，也不会追溯性收费。因此，为了平衡灵活性和问责制，VM 系列 ELA 使用条款包括有限和无限期限，解释了如何在需要时使用令牌和部署防火墙。有关详细信息，请参阅 ELA 条款和条

©2024 Palo Alto Networks, Inc.

件。使用 VM 系列 ELA 部署的 VM 系列防火墙没有永久许可证，并且在期限到期时，您必须续订协议以扩展支持权利和继续访问防火墙上的软件及内容发布更新。

通过 CSP 上的 ELA 管理员角色，您可以使用自己的 CSP 帐户在属于不同部门的其他管理员之间传输或拆分许可令牌。此共享使企业中的其他管理员可以按需部署 VM 系列防火墙，只要他们在各自的 CSP 帐户中具有令牌即可。邀请其他管理员共享 ELA 令牌并部署符合企业安全需求的任何 VM 系列防火墙模型，请参阅 管理 VM 系列 ELA 许可证令牌。如果要根据不断变化的组织需求重新分配令牌，您还可以回收令牌以从 VM 系列 ELA 中删除 CSP 帐户。

观看 VM 系列多型号 ELA 视频

- 管理 VM 系列 ELA 许可证令牌
- 接受 VM 系列 ELA

管理 **VM** 系列 **ELA** 许可证令牌

凭借 VM 系列企业许可协议（多型号 ELA）（VM 系列 ELA），您可以灵活地签订单一合同，以便与企业中的其他管理员共享。您必须有 Palo Alto Networks 客户支持门户 (CSP) 上的超级用户角色才能激活 ELA，并且在激活 ELA 授权代码后，您将继承 CSP 上的 ELA 管理员角色。

使用 ELA 管理员角色，您可以管理可用于部署协议中包含的 VM 系列防火墙和订阅的许可证令牌池。您可以邀请其他管理员共享 VM 系列 ELA 令牌，为每个管理员授予哪些型号以及 VM 系列防火墙可用的实例数，以及从 VM 系列 ELA 中删除 CSP 帐户。根据您为每个被授予者分配的内容，他们会收到特定数量的令牌，然后可以使用这些令牌来部署 VM 系列防火墙。

额外的购买和授权不会直接增加 *CSP* 帐户中可用的 *VM* 系列防火墙的数量；相反，*ELA* 许可证令牌被添加到 *VM* 系列 *ELA* 令牌池中。*ELA* 许可证令牌随后可由 *ELA* 管理员分配给给定的 *CSP* 帐户，以增加可用的 *VM* 系列防火墙的数量。

STEP 1 | （仅限旧版 VM 系列 ELA 客户）指定 ELA 管理员来管理令牌。

已迁移到多型号 ELA 的现有企业许可证客户必须指定 ELA 管理员来管理 VM 系列 ELA 许可证令牌。转换后，不需要其他操作来继续运行防火墙，但是，在分配 ELA 管理员之前，您将无法（重新）分配令牌来部署防火墙。只有在 CSP 上具有超级用户角色的管理员才能指定 ELA 管理员，而 ELA 管理员又可以管理令牌或向其他管理员授予令牌。

1. 登录到 Palo Alto Networks CSP。
2. 选择 **Members**（成员） > **Manage Users**（管理用户）。
3. 单击 操作（**Actions**）下的铅笔图标，以编辑要为其分配 ELA 管理员角色的用户。
4. 选择 **ELA Administrator**（**ELA** 管理员），然后单击复选标记以将新角色添加到所选用户。
5. 继续转到步骤 3。

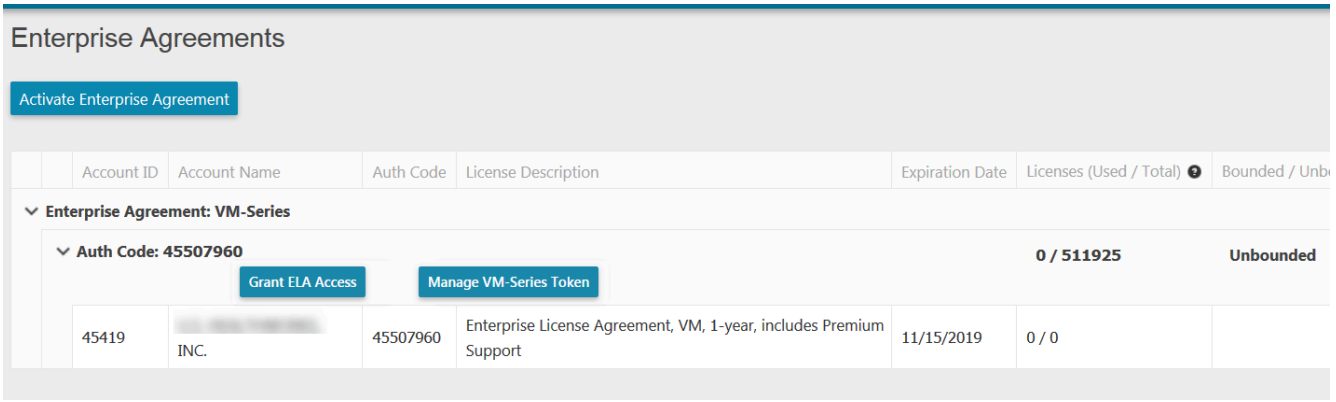
©2024 Palo Alto Networks, Inc.

STEP 2 | 激活 ELA 授权代码。

激活 ELA 的管理用户在 CSP 上继承了 ELA 管理员和超级用户角色，并且能够管理令牌或将令牌授予其他管理员。

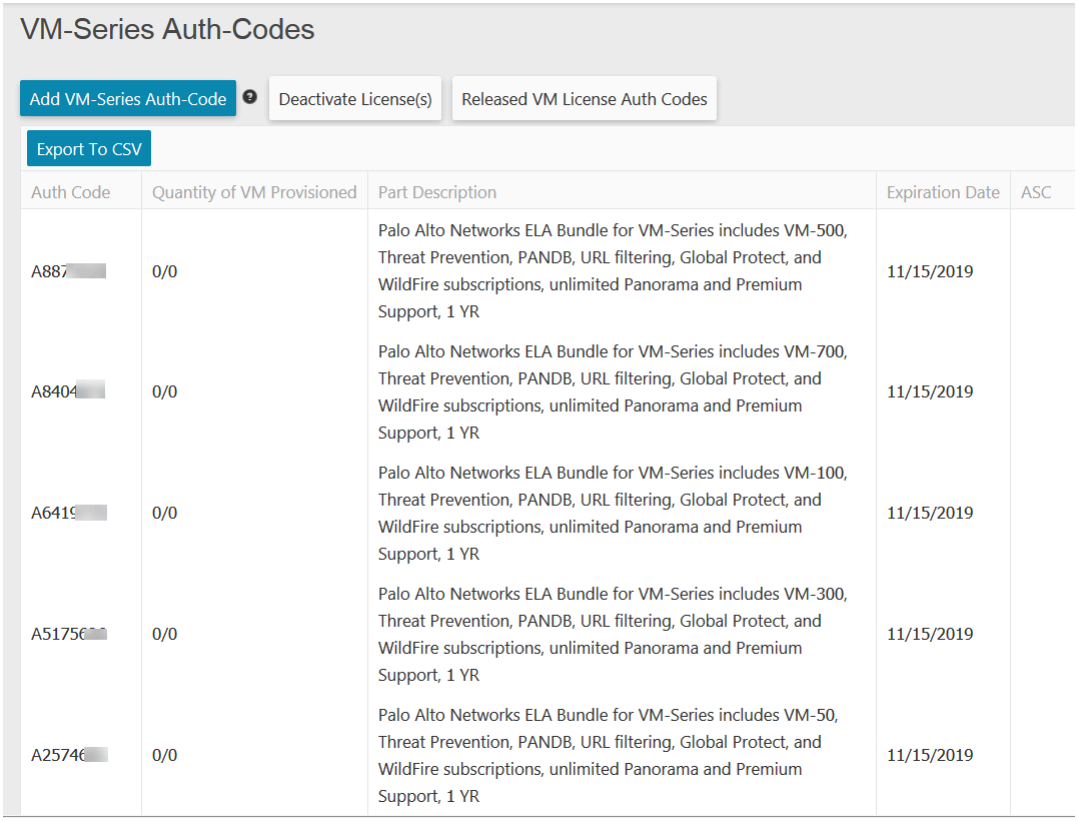
1. 登录到 Palo Alto Networks CSP。
2. 选择 **Assets**（资产） > **Enterprise Agreements**（企业协议） > **Activate Enterprise Agreement**（激活企业协议）。
3. 输入 **Authorization code**（授权代码）并 **Agree and Submit**（同意并提交）EULA。

   验证授权代码是否已在企业协议下注册到您的帐户：VM 系列。该页面显示授权代码、帐户 ID、帐户名称、许可证说明、过期日期、您拥有的许可证数量（已用/总计），以及在协议的限定和无限定期限内可以部署的数量。



4. 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码），以查看用于部署 VM 系列防火墙的每个型号以及 ELA 附带的关联订阅的授权代码。

©2024 Palo Alto Networks, Inc.



VM-Series Auth-Codes

Add VM-Series Auth-Code | Deactivate License(s) | Released VM License Auth Codes

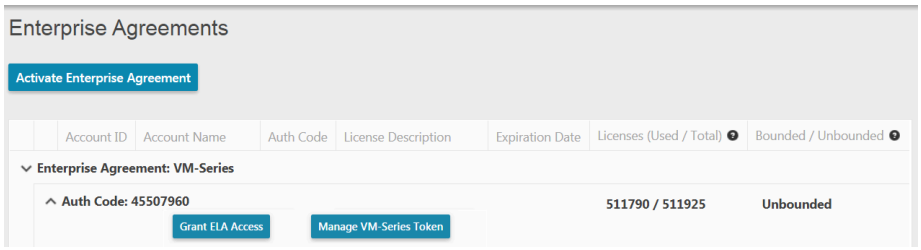
Export To CSV

Auth Code	Quantity of VM Provisioned	Part Description	Expiration Date	ASC
A887	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-500, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A8404	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-700, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A6419	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-100, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A51756	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-300, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A25746	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-50, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	

©2024 Palo Alto Networks, Inc.

STEP 3 | 授予 ELA 访问企业中其他管理员的权限。

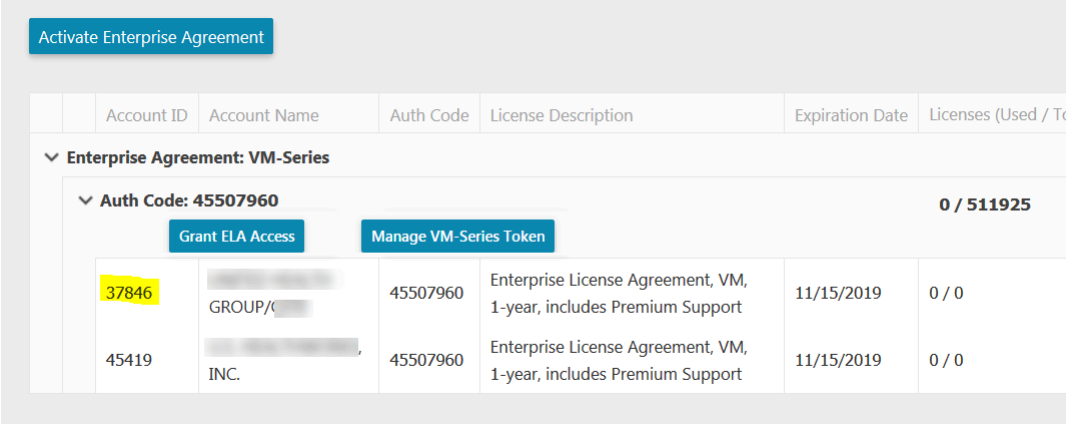
此功能允许您与企业或部门中的其他管理员共享 VM 系列 ELA，以便他们可以按需部署 VM 系列防火墙。作为 ELA 管理员，您可以授予对在 CSP 上使用电子邮件地址注册的其他用户的访问权限。



1. 在 **Assets**（资产）> **Enterprise Agreements**（企业协议）中，选择 **Grant ELA Access**（授予 **ELA** 访问权限）。
2. 输入要邀请的管理员的 **Destination Email**（目标电子邮件地址）。

   您在上面输入的目标电子邮件地址必须是具有超级用户角色的 CSP 上的注册用户，以便他们可以登录并接受授权。如果电子邮件地址未在 CSP 上注册，则必须先在 **Members**（成员）> **Create New User**（创建新用户）上为用户创建一个新帐户。
3. 选择 **Notify User**（通知用户），将通知电子邮件发送到您输入的电子邮件地址。

   收件人必须登录到 CSP 以接受 VM 系列 ELA。收件人接受授权后，帐户 ID 在 **Assets**（资产）> **Enterprise Agreements**（企业协议）上可用，如下面的屏幕截图所示。

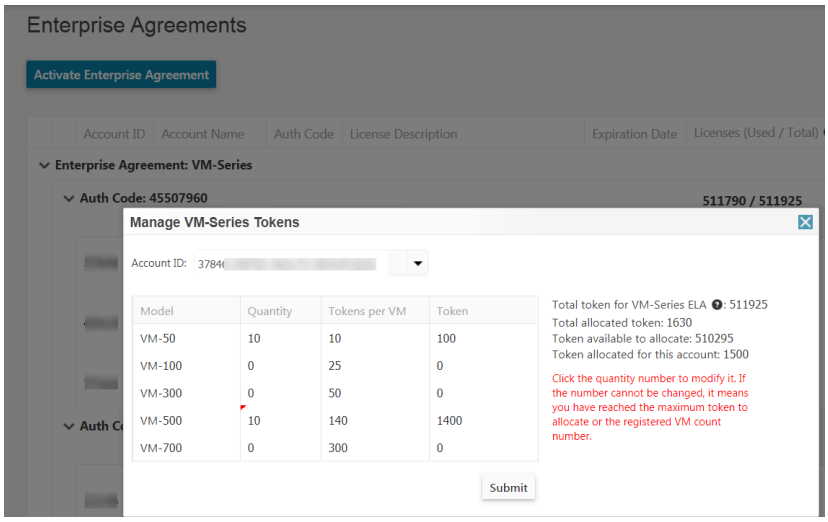


©2024 Palo Alto Networks, Inc.

STEP 4 | 为防火墙部署分配令牌。

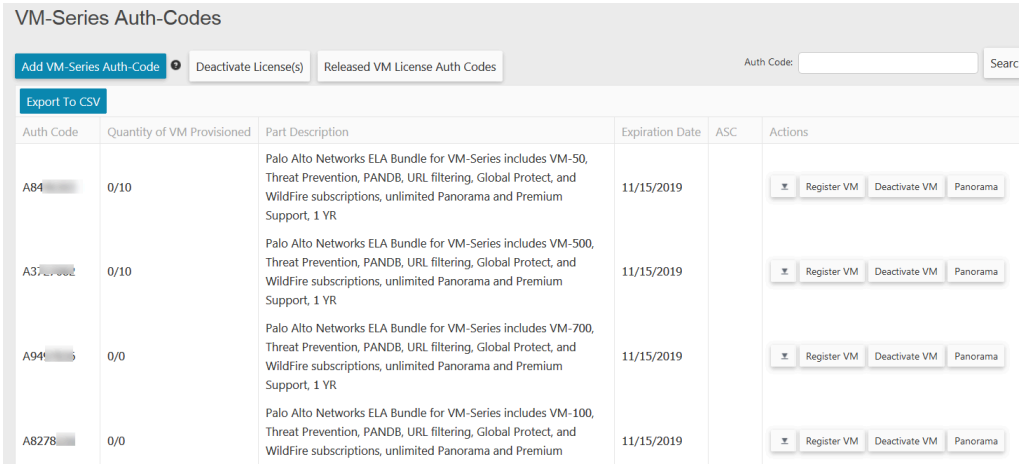
1. 选择 **Assets**（资产）> **Enterprise Agreements**（企业协议）> **Manage VM-Series Tokens**（管理 **VM** 系列令牌）。

   对于每个帐户 ID，您可以按模型指定要分配的防火墙数。根据数量和防火墙模型，自动计算令牌数量并可供使用。在此示例中，您允许 VM -50和 VM -500 的各 10 个实例。



2. 验证是否在帐户中存放了准确数量的防火墙实例。

   选择 **Assets**（资产）> **VM-Series Auth-Code**（**VM** 系列授权代码）以确认分配的授权代码。在此示例中，该帐户能够为 VM -50和 VM -500 中的每一个配置 10 个实例。当收件人部署防火墙时，会从总可用池中扣除令牌数，并且您可以查看已配置的防火墙实例的数量，作为为其分配的总数量的比率。随着安全需求的发展，只要您有可用的令牌，您就可以灵活地分配更多数量并允许访问不同的 VM 系列防火墙模型。



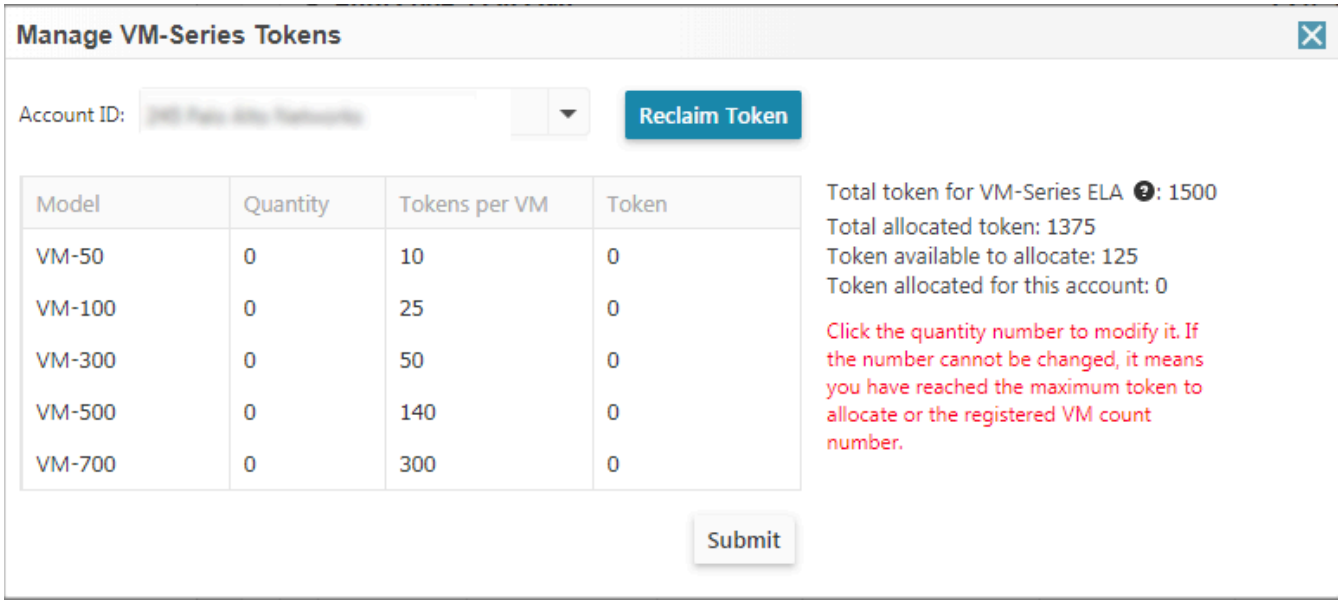
 ©2024 Palo Alto Networks, Inc.

STEP 5 | 从 VM 系列 ELA 中删除 CSP 帐户以回收令牌。

您无法回收分配给 *CSP* 帐户的部分令牌。通过回收令牌，您将从 *VM* 系列 *ELA* 中删除整个 *CSP* 帐户，并将所有关联的令牌重新分配到令牌池。

1. 验证 VM 系列防火墙是否未使用与要删除的 CSP 帐户关联的所有令牌。根据需要停用 VM 系列防火墙以配置令牌以进行删除。
2. 选择 **Assets**（资产） > **Enterprise Agreements**（企业协议）> **Manage VM-Series Token**（管理 **VM** 系列令牌）。

   选择要从中回收令牌的帐户 ID，然后单击 **Reclaim Token**（回收令牌）。如果令牌可用于回收，您将收到成功删除的确认。



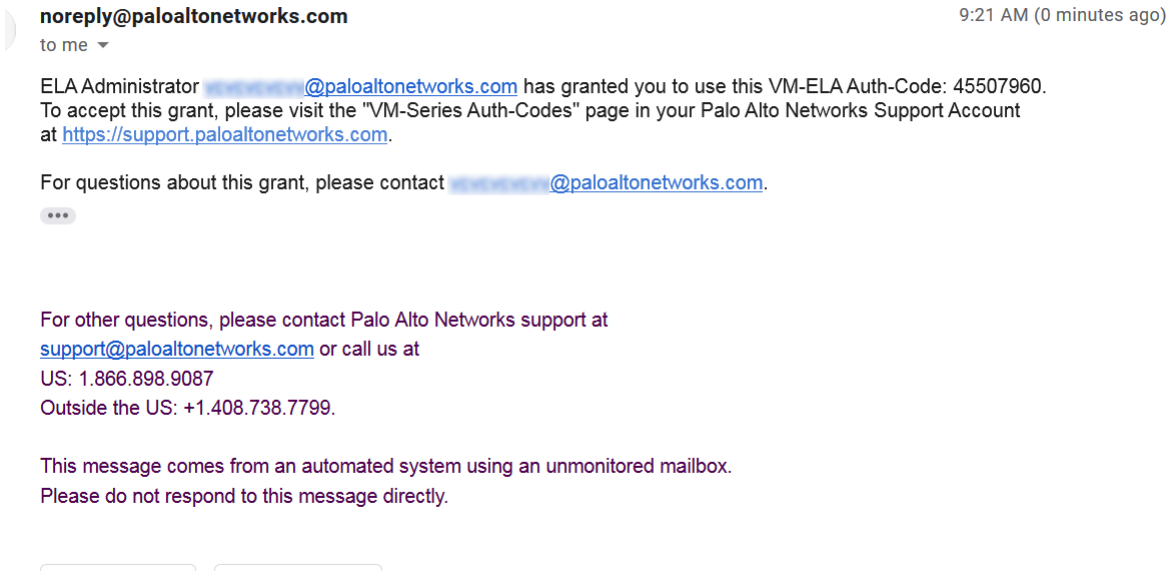
接受 VM 系列 ELA

如果您的企业购买了 VM 系列 ELA，您的 ELA 管理员可以邀请您共享合同并共享许可令牌池，以便您可以访问 VM 系列防火墙验证码，以便您按需部署 VM 系列防火墙。当您收到访问 VM 系列 ELA 的授权时，您会收到一封电子邮件通知，其中包含登录 Palo Alto Networks 客户支持门户 (CSP) 的链接，您必须同意并接受使用条款。在您接受 ELA 使用条款后，ELA 管理员可以分配哪些 VM 系列防火墙型号以及您有权使用多少个;相应数量的 VM 系列 ELA 令牌存入您的帐户。

©2024 Palo Alto Networks, Inc.

STEP 1 | 检查您的电子邮件收件箱以获取授权通知。

该通知包括邀请您共享 VM 系列 ELA 的 ELA 管理员的电子邮件地址。



noreply@paloaltonetworks.com 9:21 AM (0 minutes ago)

to me

ELA Administrator [redacted]@paloaltonetworks.com has granted you to use this VM-ELA Auth-Code: 45507960.
To accept this grant, please visit the "VM-Series Auth-Codes" page in your Palo Alto Networks Support Account at https://support.paloaltonetworks.com.

For questions about this grant, please contact [redacted]@paloaltonetworks.com.

For other questions, please contact Palo Alto Networks support at
support@paloaltonetworks.com or call us at
US: 1.866.898.9087
Outside the US: +1.408.738.7799.

This message comes from an automated system using an unmonitored mailbox.
Please do not respond to this message directly.

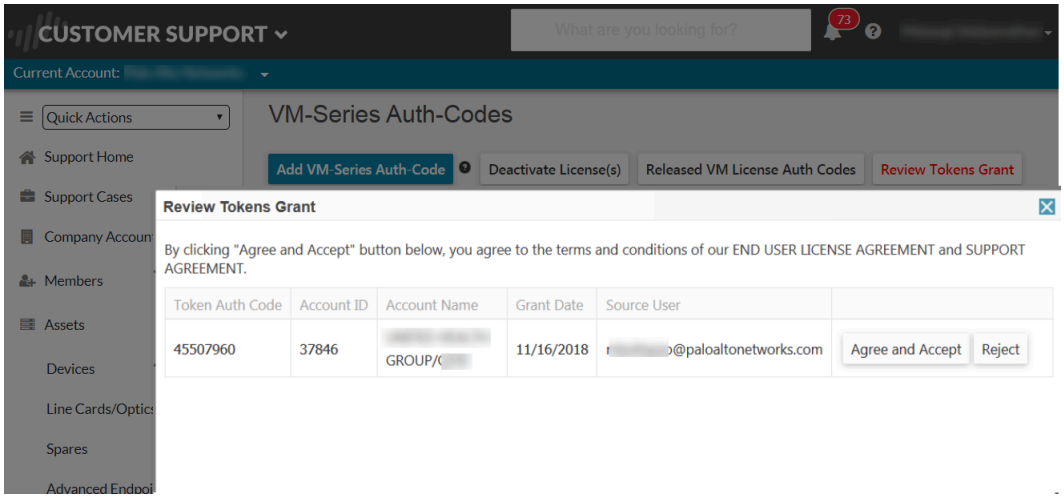
©2024 Palo Alto Networks, Inc.

STEP 2 | 接受授予。

您必须先检查条款并接受 EULA 和支持协议，ELA 管理员才能分配令牌，以便您部署 VM 系列防火墙。

1. 登录到 Palo Alto CSP。
2. 选择 **VM-Series Auth Codes**（**VM** 系列授权代码）以 **Review Tokens Grant**（检查令牌授予）。

   您必须“同意且接受 EULA”并支持接受授予的协议。如果拒绝，则向您提供授予的 ELA 管理员会收到您拒绝授予的电子邮件通知。请务必让 ELA 管理员知道您已接受授权，以便他/她可以为您分配可以部署的 VM 系列防火墙型号和数量。



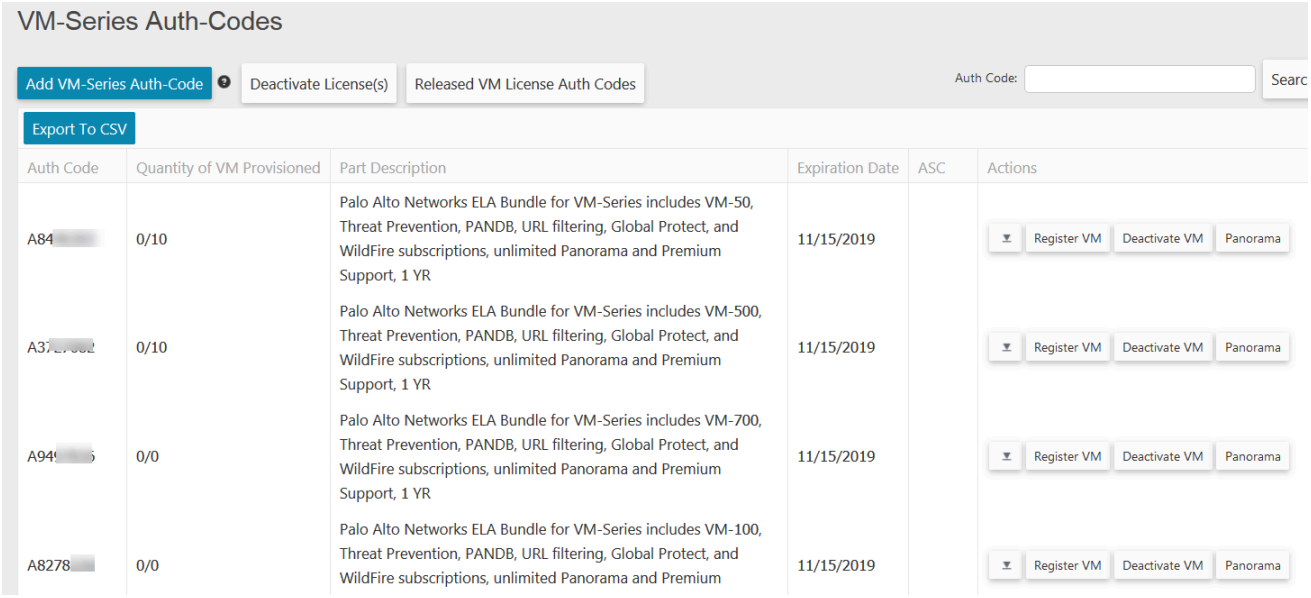
如果您属于 *CSP* 上的多个帐户，并且意外地接受了错误帐户的授权，则必须请求 *ELA* 管理员重新向您发送授权。接受正确帐户的授权之前，请勿开始使用授权代码配置防火墙。

STEP 3 | 验证为您分配了哪些 VM 系列型号以及分配的数量。

在 ELA 管理员分配 VM 系列防火墙模型和您可以配置的实例数量后，您可以选择 **Assets**（资产）> **VM-Series Auth Codes**（**VM** 系列授权代码）以查看哪些模型以及为您分配了多少模

©2024 Palo Alto Networks, Inc.

型。例如，以下屏幕截图中的授权显示了授权代码，可让您分别部署 VM-50 和 VM-500 的 10 个实例。



在部署防火墙并将其注册到 CSP 时，配置的防火墙数量会增加。该 **Quantity of VM Provisioned**（配置的 **VM** 数量）以显示每个型号的预配比和总可用比。

激活 VM 系列型号许可证

要在 VM 系列防火墙上激活许可证，必须已部署此 VM 系列防火墙，并已完成初始配置。要部署防火墙，请参阅 VM 系列部署。

将本节中的说明用于所有的 BYOL 模式，包括 AWS、 Azure 和 Google Public Cloud。对于公共云中基于使用情况的许可证，您无须激活许可证。您必须 面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）以激活您的高级支持权利。

对于 *AWS Marketplace* 中基于使用情况的 *VM* 系列防火墙模型，支持具有短和长 *AWS* 实例 *ID* 的实例。

在 VM 系列防火墙上激活许可证之前，此防火墙没有序列号，数据面板接口的 MAC 地址不唯一，并且仅支持最小数量的会话。由于在授权防火墙许可证之前 MAC 地址不唯一，为防止出现重叠 MAC 地址所致的问题，请确保您没有多个未经许可的 VM 系列防火墙。

在激活许可证时，许可服务器会使用虚拟机的 UUID 和 CPU ID 生成 VM 系列防火墙的唯一序列号。容量授权代码与序列号一起用于验证您的授权。

VM 系列防火墙 ***License***（许可证）选项卡显示所有许可证模型的标准 *VM-300* 许可证文件。要查找特定许可证模型信息，请在用户界面中查看系统信息，或使用 *CLI* 查看 ***`system info`***。

在您授权 *VM* 系列防火墙许可证之后，如需删除并重新部署 *VM* 系列防火墙，请确保在防火墙上停用许可证。停用许可证可让您传输活动许可证至 *VM* 系列防火墙的新实例，而无需技术支持部门提供协助。

©2024 Palo Alto Networks, Inc.

- 激活 VM 系列防火墙的许可证（独立版本）
- 激活 VMware NSX 的 VM 系列防火墙的许可证（独立版本）
- 排查许可证激活问题

激活 VM 系列防火墙的许可证（独立版本）

如果您尚未选择使用订阅捆绑软件的引导工作流程，则必须部署 VM 系列防火墙并完成初始配置，然后才能激活 VM 系列防火墙上的许可证。

- 直接访问 Internet
- 无互联网接入

直接访问 Internet

要激活许可证，必须使用 IP 地址、子网掩码、默认网关和 DNS 服务器 IP 地址配置防火墙。

防火墙必须具有有效的 DNS 配置并具有网络连接才能访问 Palo Alto Networks 许可服务器。

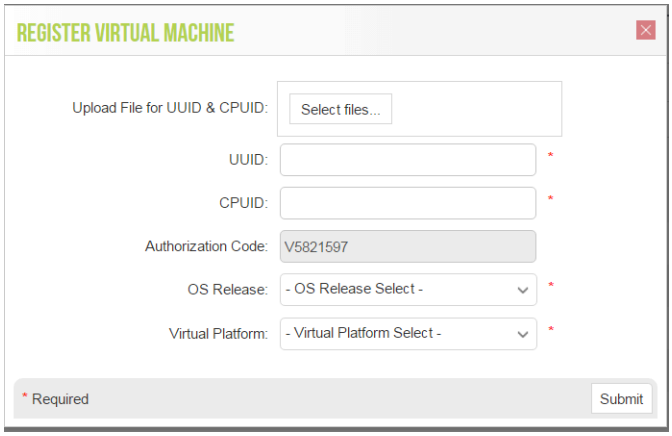
1. 选择 **Device**（设备） > **Licenses**（许可证），然后选择 **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）链接。
2. 防火墙将连接到更新服务器 (updates.paloaltonetworks.com)，并下载许可证，然后自动重新启动。
3. 重新登录到 Web 界面，并确认 **Dashboard**（仪表盘）显示有效的序列号。如果显示 **Unknown**（未知）一词，则表示此设备未经许可。
4. 在 **Device**（设备） > **Licenses**（许可证）上，验证 **PA-VM** 许可证是否已添加到此设备上。

   如果您看到错误消息，请检查排查许可证激活问题。

©2024 Palo Alto Networks, Inc.

无法访问 Internet

1. 选择 **Device**（设备）> **Licenses**（许可证），然后单击 **Activate Feature using Auth Code**（使用授权代码激活功能）链接。
2. 单击 **Download Authorization File**（下载授权文件），然后在客户端机器上下载 **authorizationfile.txt**。
3. 将 **authorizationfile.txt** 复制到有权访问 Internet 的计算机上，并登录到支持门户。单击 **My VM-Series Auth-Codes**（我的 **VM** 系列授权代码）链接，并从列表中选择适用的授权代码，然后单击 **Register VM**（注册 **VM**）链接。
4. 在 **Register Virtual Machine**（注册虚拟机）选项卡上，上传授权文件。选择已部署防火墙的 PAN-OS 版本和虚拟机监控程序，以完成注册过程。VM 系列防火墙的序列号将附加到您的帐户记录中。



5. 导航到 **Assets**（资产）> **My Devices**（我的设备），并搜索刚注册的 VM 系列设备，然后单击 **PA-VM** 链接。这样，可将 VM 系列许可证密钥下载到客户端机器上。
6. 将许可证密钥复制到可以访问 VM 系列防火墙 Web 界面的机器上，并导航到 **Device**（设备）> **Licenses**（许可证）。

   许可证密钥必须通过 *Web* 界面安装。防火墙不支持通过 *SCP* 或 *FTP* 安装许可证密钥。
7. 单击 **Manually Upload License**（手动上传许可证）链接，并输入许可证密钥。在防火墙上激活容量许可证后，设备将重新启动。
8. 登录到设备，并确认 **Dashboard**（仪表盘）显示有效的序列号，并且 **PA-VM** 许可证显示在 **Device**（设备）> **Licenses**（许可证）选项卡中。

激活 VMware NSX 的 VM 系列防火墙的许可证（独立版本）

在 Panorama 可直接访问 Internet 时，Panorama 将充当 VM 系列 VMware NSX 版防火墙的集中管理点，并且许可证激活过程自动启动。Panorama 会连接至 Palo Alto Networks 更新服务器以检索许可证，而且在新的 VM 系列 NSX 版防火墙部署时，将会与 Panorama 进行通信，以获得许可证。如果 Panorama 未连接到 Internet，您需要手动许可 VM 系列防火墙的每个实例，以便防火墙连接至 Panorama。

©2024 Palo Alto Networks, Inc.

对于此集成解决方案，授权代码（如 PAN-VM-1000-HV-SUB-BND-NSX2）包括威胁阻止、URL 筛选和 WildFire 订阅的许可证以及请求期间的高级支持。

要激活许可证，您必须完成以下任务：

- 将授权代码注册到支持帐户。如果不注册授权代码，许可服务器将无法创建许可证。
- 在 Panorama 的服务定义中输入授权代码。在 Panorama 上，选择 **VMWare Service Manager**，以将 **Authorization Code**（授权代码）添加到 **VMware Service Definition**（**VMware** 服务定义）中。



如果您已购买评估授权代码，可以使用为期 *30* 天或 *60* 天的 *VM-1000-HV* 容量许可证最多授权 *5* 个 *VM* 系列防火墙许可证。由于此解决方案可让您在每个 *ESXi* 主机上部署一个 *VM* 系列防火墙，因此在使用评估许可证时 *ESXi* 集群最多可以包括 *5* 个 *ESXi* 主机。

以下许可证激活流程为手动流程。如果您具有自定义脚本或协调服务，则可以使用许可证 API 自动检索 VM 系列防火墙的许可证流程。

- 当 Panorama 可以访问 Internet 时，在 NSX 上的 VM 系列防火墙上激活许可证
- 当 Panorama 无法访问 Internet 时，在 NSX 上的 VM 系列防火墙上激活许可证
- 排查许可证激活问题

当 **Panorama** 可以访问 **Internet** 时，在 **NSX** 上的 **VM** 系列防火墙上激活许可证

当Panorama有权访问 Internet 时，请完成以下过程以激活适用于 NSX 的 VM 系列防火墙。

STEP 1 | 验证 VM 系列防火墙已连接到 Panorama。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Managed Devices**（托管设备），并检查防火墙是否显示为 Connected（已连接）。

STEP 2 | 验证每个防火墙已获得许可。

选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证），并验证 Panorama 已匹配了授权代码并将许可证用于每个防火墙。

如果未看到许可证，则单击 **Refresh**（刷新）。选择要检索订阅许可证的 VM 系列防火墙，并单击 **OK**（确定）。

当 **Panorama** 无法访问 **Internet** 时，在 **NSX** 上的 **VM** 系列防火墙上激活许可证

当 Panorama 无法访问 Internet 时，请完成以下程序以激活VM 系列防火墙 NSX 版。

STEP 1 | 找到 VM 系列防火墙的 CPU ID 和 UUID。

1. 从 vCenter 服务器上，获得防火墙的 IP 地址。
2. 登录到 Web 界面并选择 **Dashboard**（仪表盘）。
3. 从常规信息小部件中获得 **CPU ID** 和 **UUID**。

©2024 Palo Alto Networks, Inc.

STEP 2 | 激活授权代码并生成许可证密钥。

1. 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。如果需要新帐户，请参阅创建支持帐户。
2. 选择 **Assets**（资产） > **VM-Series Auth Codes**（**VM** 系列授权代码），然后单击 **Add VM-Series Auth Codes**（添加 **VM** 系列授权代码）以输入授权代码。
3. 在您刚刚注册的授权代码相对应的一行中，选择 **Register VM**（注册 **VM**），输入防火墙的 CPU ID 和 UUID，然后单击 **Submit**（提交）。门户将会为防火墙生成一个序列号。
4. 选择 **Assets**（资产） > **Devices**（设备），然后搜索该序列号。
5. 单击操作栏的链接，将每个密钥下载到您的便携式计算机上。除订阅许可证密钥外，您还必须获取容量许可证和支持许可证密钥。

STEP 3 | 将密钥上传到防火墙。

1. 登录到防火墙 Web 界面。
2. 选择 **Device**（设备） > **Licenses**（许可证），然后选择 **Manually upload license key**（手动上传许可证密钥）。
3. 单击 **Browse**（浏览）选择一个密钥，然后单击 **OK**（确定）在防火墙上安装许可证。

   首先安装容量许可证密钥文件 *(pa-vm.key)*。使用了容量许可证密钥之后，*VM* 系列防火墙将会重新启动。在重新启动时，防火墙将会具有一个序列号，您可以使用该序列号将防火墙注册为 *Panorama* 上的托管设备。
4. 重复该流程，将每个密钥安装到防火墙上。
5. 选择 **Dashboard**（仪表盘）并验证您可以在常规信息小部件中看到 **Serial #**（序列号）。

STEP 4 | 添加 Panorama 上防火墙的序列号。

选择 **Panorama** > **Managed Devices**（托管设备），然后单击 **Add**（添加），以输入 NSX 的 VM 系列防火墙的序列号。此时，防火墙应能连接到 Panorama，以便获得其配置和策略规则。

排查许可证激活问题

本部分介绍了激活许可证的一些最常见问题。

许可没有足够内存的 PA-VM 会导致类似如下的错误：

```
Server error : failed key check :Resource check failed.Memory
 needed:6.5GB, allocated memory:4.8GB
```

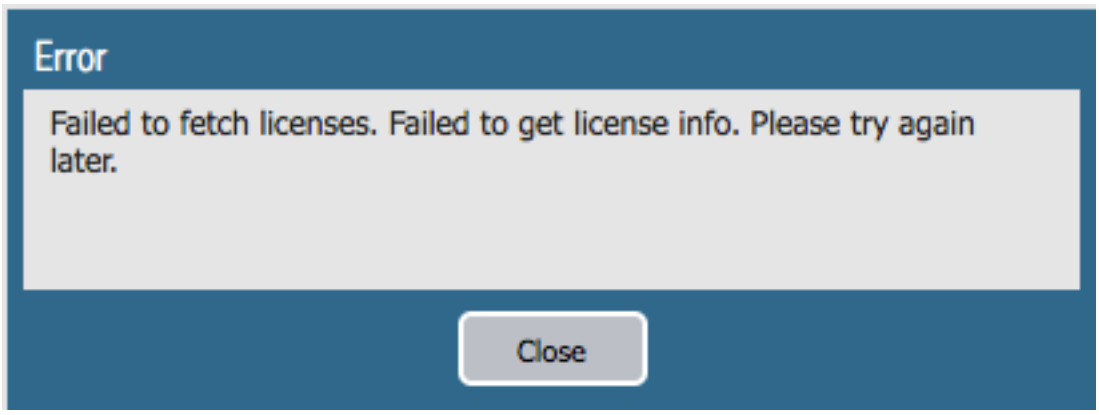
要解决此问题，请提供许可证所需的额外内存，并使用命令 **request license fetch** 提取许可证。

如果您使用任何其他命令，提取许可证将失败并显示以下错误：

```
Server error : failed to fetch license:Cannot apply a provisioning
 license feature to an already provisioned device.
```

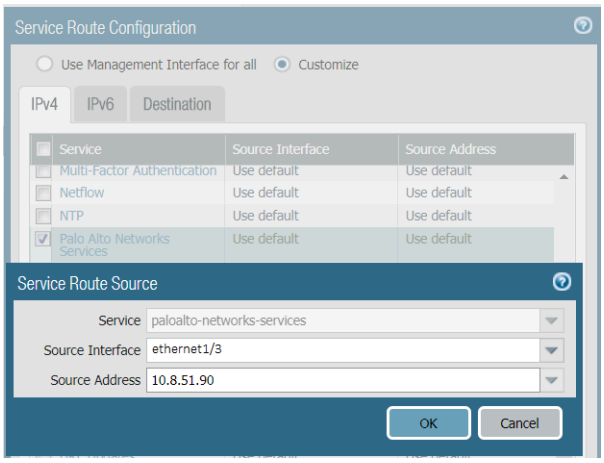

©2024 Palo Alto Networks, Inc.

如果您看到读取的错误 **Failed to fetch licenses**（无法提取许可证）。无法获取许可证信息。请稍后再试或显示通用通信错误消息。



验证以下内容：

- 防火墙能否使用服务路由将流量路由到 Palo Alto Networks 服务器？默认情况下，防火墙使用管理接口访问服务器。如果您计划使用数据平面界面，请确保已经设置了一个服务路由。



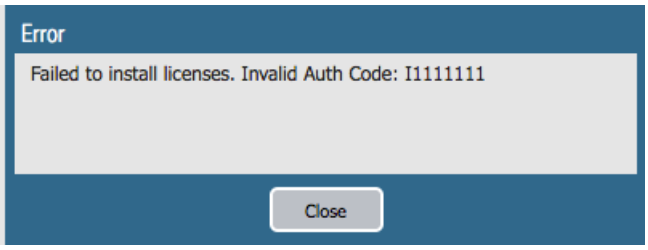
- 路由通过 Internet 工作？SSH 进入防火墙并 Ping 一个可公开访问的 IP 地址，如 4.2.2.2。如果您正在使用数据面界面，请务必使用源选项。例如：ping count 3 source 10.0.1.1 host 4.2.2.2.
- DNS 设置正确吗？SSH 进入防火墙并 Ping一个 DNS 名称，如 google.com。例如：

```
warby@warbylan> ping count 3 source 10.0.1.1 host google.com
PING google.com (216.58.195.78) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=1 ttl=55 time=11.6 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=2 ttl=55 time=11.9 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=3 ttl=55 time=11.5 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 11.586/11.721/11.975/0.200 ms
```


©2024 Palo Alto Networks, Inc.

如果您看到一个读取授权代码的错误：



验证以下内容：

- 您已正确输入授权代码。
- 您已在支持门户上将授权代码注册至您的帐户。
- 您的授权代码尚未达到 VM 系列防火墙的最大供应容量。
  - 对于旧许可证，请登录 CSP 并选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码）。
  - 对于软件 NGFW 积分，如果您知道部署配置文件，请登录 CSP 并选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），找到您的配置文件，然后单击 **Details**（详细信息）。

    您还可以选择 **Assets**（资产） > **Software NGFW Devices**（软件 **NGFW** 设备），并通过授权代码进行搜索。

注册 VM 系列防火墙

在购买 VM 系列防火墙时，您会收到一封电子邮件，其中包含 VM 系列型号容量许可证的授权代码、支持授权代码以及一个或多个用于订阅许可证的授权代码。要使用授权代码，您必须在 Palo Alto Networks 客户支持网站上将授权代码注册到支持帐户。在 VMware 集成 NSX 解决方案的情况下，电子邮件包含一个绑定 VM 系列型号的一个或多个实例的容量许可证的授权代码、支持授权以及一个或多个订阅许可证。

对于 AWS、Azure 或 Google Cloud Platform 等公共云上的基于使用情况的许可证，您将不会收到授权代码。不过，要通过 Palo Alto Networks 激活您的高级支持授权，您必须在 Palo Alto Networks 客户支持网站上创建支持帐户并注册 VM 系列防火墙。

使用此部分的说明通过您的支持帐户注册容量授权代码或防火墙：

- 注册 VM 系列防火墙（软件 NGFW 积分）
- 注册 VM 系列防火墙（使用授权代码）
- 面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。

注册 **VM** 系列防火墙（使用授权代码）

完成以下过程以使用授权代码注册 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。如果需要，请创建一个支持帐户。

STEP 2 | 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码） > **Add VM-Series Auth-Code**（添加 **VM** 授权代码）。

STEP 3 | 在 **Add VM-Series Auth-Code**（添加 **VM** 系列授权代码）字段中，输入通过电子邮件收到的容量授权代码，然后单击最右侧的复选标记以保存输入。页面上将显示注册到支持帐户的授权代码的列表。

您可以跟踪已部署的 VM 系列防火墙的数量和仍可用于针对每个授权代码使用的许可证的数量。在使用所有可用许可证时，授权代码不会显示在 VM 系列授权代码页面上。要查看已部署的所有资产，请选择 **Assets**（资产） > **Devices**（设备）。

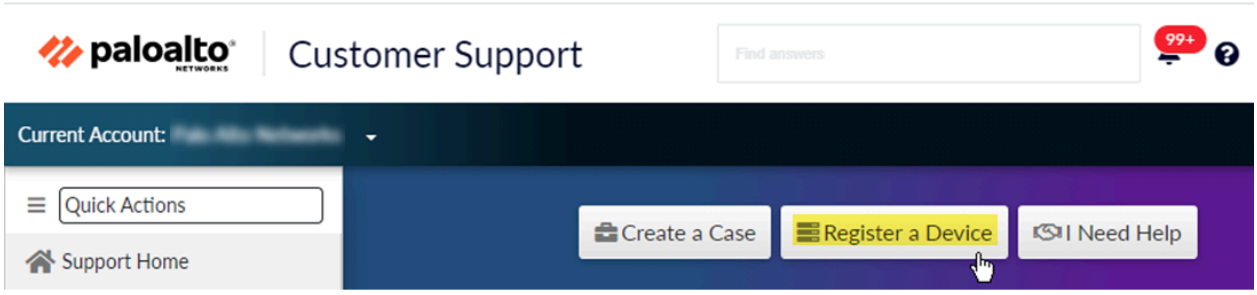
面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。

要在 Palo Alto Networks 客户支持门户 (CSP) 上注册基于使用情况的防火墙，您可以使用自动注册或手动注册。通过自动注册基于使用情况的防火墙，您可以在启动防火墙后立即进行无缝注册，并访问与 CSP 帐户相关联的网站许可证授权。有关详细信息，请参阅在 VM 系列防火墙上安装设备证书。

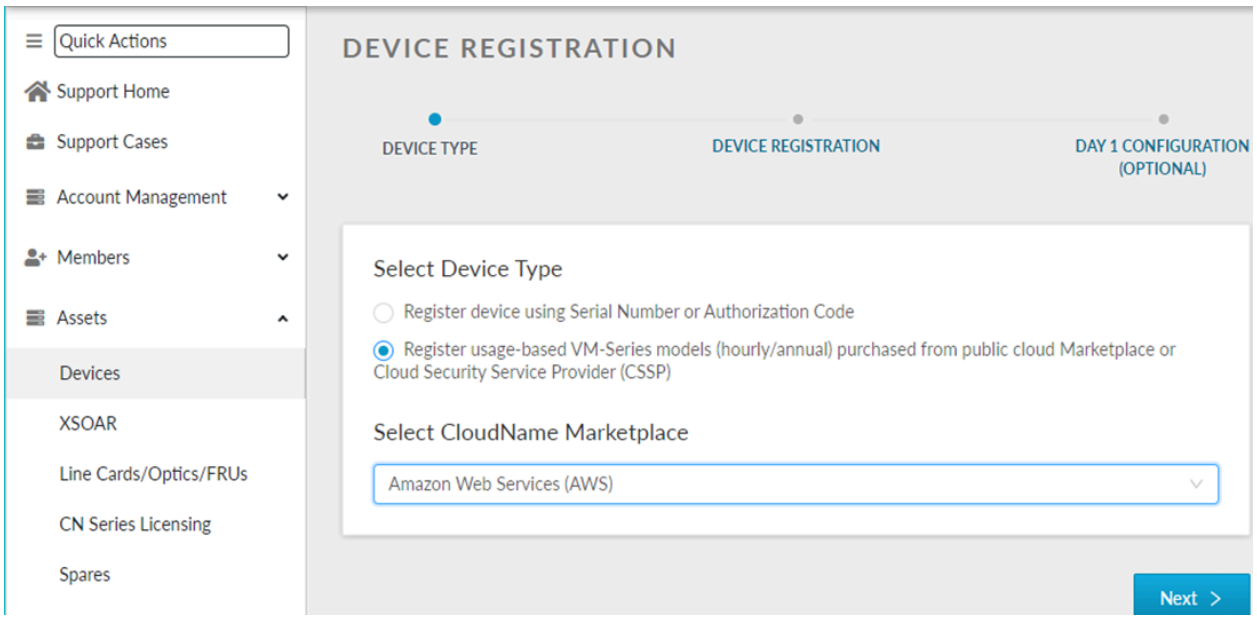
使用以下工作流程以手动注册 VM 系列防火墙。在开始手动注册过程之前，请登录 VM 系列防火墙并从仪表盘记下序列号和 CPU ID（UUID 为可选）。

©2024 Palo Alto Networks, Inc.

STEP 1 | 登录 Palo Alto Networks 客户支持网站，然后单击 **Assets**（资产）> **Devices**（设备）> **Register New Devices**（注册新设备）。



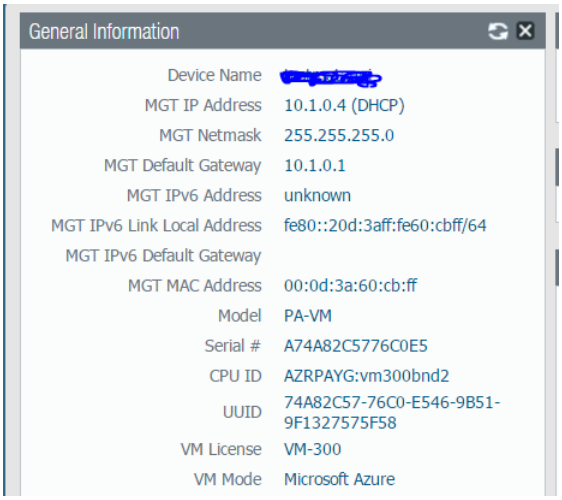
1. 选择 **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace or Cloud Security Service Provider (CSSP)**（注册从公共云市场或云安全服务提供商 **(CSSP)** 购买的基于使用情况的 **VM** 系列型号（每小时/每年））。
2. 选择您的 **Cloud Marketplace**（云市场）供应商，然后单击 **Next**（下一步）。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 输入 VM 系列防火墙的 **Serial #**（序列号）、**CPU ID** 和 **UUID**。

例如，在 VM 的 VM 系列防火墙的仪表盘中，您将看到以下信息。



如果您打算离线使用防火墙，请选择 ***Offline***（离线）复选框并输入您打算使用的 *PAN-OS* 版本。

STEP 3 | **Agree and Submit**（同意并提交）接受 EULA 并注册防火墙。

STEP 4 | 验证您购买的许可证的详细信息是否显示在 CSP **Assets**（资产）页面上。

在 VM 系列防火墙上安装设备证书

防火墙需要设备证书才能检索网站许可证授权和安全访问云服务，例如 WildFire、AutoFocus 和 Cortex Data Lake。可以通过两种方法将网站许可证应用于 VM 系列防火墙：一次性密码和自动注册 PIN。每个密码或 PIN 都是在客户支持门户 (CSP) 上生成，并且对于 Palo Alto Networks 支持帐户都是唯一。使用方法取决于用于部署防火墙的许可证类型以及防火墙是否由 Panorama 管理。

- 一次性密码 - 对于已向 Palo Alto Networks 许可服务器注册的 VM 系列防火墙，必须在客户支持门户上生成一次性密码并将其应用于 VM 系列防火墙。对于小型非托管部署中具有 BYOL 或 ELA 许可证的 VM 系列防火墙，以及 Panorama 托管的手动部署的 VM 系列防火墙，请使用此方法。
- 注册 PIN — 此方法用于在初次启动时将网站许可证应用于 VM 系列防火墙。无论许可证类型怎样，对于在启动时使用基于使用情况的 PAYG 许可证或任何类型的自动部署进行引导的 VM 系列防火墙，请使用此方法。通过自动注册 PIN，您可以在启动时自动向 CSP 注册基于使用情况的防火墙，并检索站点许可证。

对于 NSX-T 上的 VM 系列防火墙，您可以将自动注册 PIN 添加到服务定义配置中，以便在初始启动时由防火墙获取设备证书。有关详细信息，请参阅 NSX-T（北向南）和 NSX-T（东向西）的服务定义配置。如果您将之前部署的防火墙升级到支持设备证书的 PAN-OS 版本，则可以使用一次性密码将设备证书分别应用于这些防火墙。

©2024 Palo Alto Networks, Inc.

一次性密码和自动注册 PIN 必须在过期之前使用。如果没有在过期之前使用，则必须返回 CSP 以生成新的一次性密码。

启用防火墙以在启动时自动检索网站许可证。

防火墙需要设备证书才能获取网站许可证授权并安全访问云服务。要在启动防火墙时检索网站许可证，必须在引导数据包的 /license 文件夹中包含授权代码，在 init-cfg.txt 文件中添加自动注册 PIN ID 和值并将其放在 /config 文件夹中。添加自动注册 PIN ID 和值还可以在 VM 系列防火墙上自动注册 PAYG 或基于使用情况的实例。

1. 登录到客户支持门户 (CSP)。
2. 生成 VM 系列注册 PIN。

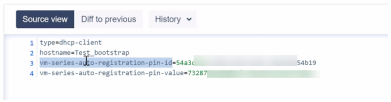
   选择 **Assets**（资产） > **Device Certificates**（设备证书） > **Generate Registration PIN**（生成注册 **PIN**）。保存 PIN ID 和值。确保在 PIN 过期之前启动防火墙。

3. 在 init-cfg.txt 文件中添加注册 PIN ID 和值。

   除了必需的参数外，还必须包括：

   ```
   vm-series-auto-registration-pin-id=
   ```

   ```
   vm-series-auto-registration-pin-value=
   ```

4. 登录到防火墙，并确认可以在防火墙上看到网站许可证。

©2024 Palo Alto Networks, Inc.

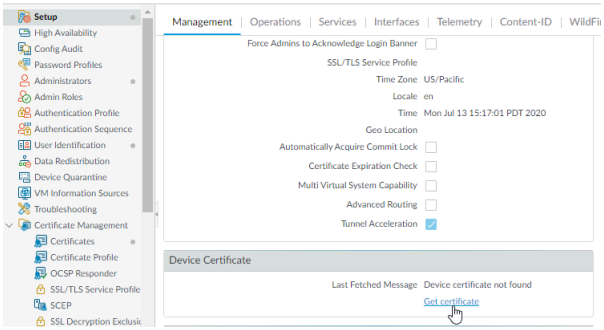
生成一次性密码 (OTP)，并在防火墙上手动检索设备证书。

防火墙需要此设备证书才能获取网站许可证授权并安全访问云服务。

1. 登录到客户支持门户。

   如果尚未注册，请注册您的 VM 系列防火墙。
2. 选择 **Assets**（资产） > **Device Certificates**（设备证书） > **Generate OTP**（生成 **OTP**）。
3. 从列表中选择防火墙以 **Generate OTP**（生成 **OTP**）。
4. 登录到防火墙，并检索设备证书。

   选择 **Setup**（设置） > **Management**（管理） > **Device Certificate**（设备证书），然后选择 **Get Certificate**（获取证书）



5. 确认已获取设备证书，并且可以在防火墙上看到网站许可证。

如果使用 Panorama 管理 VM 系列防火墙，请参阅在托管防火墙上安装设备证书。

在 BYOL 和 PAYG 许可证之间切换

VM 系列防火墙无法在 BYOL 和 PAYG 许可选项之间进行转换。如果您已经在 AWS、Azure 或 Google Cloud Platform 中使用 PAYG 或 BYOL 选项部署和配置 VM 系列防火墙，并且现在要切换到其他选项，请使用以下说明在现有防火墙上保存和导出配置，部署新的防火墙，然后恢复新防火墙上的配置。

STEP 1 | 保存当前配置文件的备份并将其存储到外部服务器。

1. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），单击 **Export named configuration snapshot**（导出已命名配置快照）。
2. 选择包含正在运行的配置（如 running-config.xml）的 XML 文件，并单击 **OK**（确定）导出配置文件。
3. 将导出的文件保存到防火墙外部的位置。

©2024 Palo Alto Networks, Inc.

STEP 2 | 根据需要部署新防火墙并注册或激活许可证。

对于新的 PAYG 实例：

1. 在 AWS、Azure 或 Google Cloud Platform 市场中，选择要部署的 PAYG 许可包的软件映像。
2. 在 AWS、Azure 或 Google 公共云中部署新的 VM 系列防火墙。请参阅 在 AWS 上设置 VM 系列防火墙、在 Azure 上设置 VM 系列防火墙或 在 Google Cloud Platform 上设置 VM 系列防火墙。
3. 面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。

对于新的 BYOL 实例：

1. 请联系您的销售代表或经销商购买 BYOL 许可证，并获取可用于许可防火墙的 BYOL 授权代码。
2. 注册 VM 系列防火墙（使用授权代码）。
3. 在 AWS 或 Azure 公共云中部署新的 VM 系列防火墙。请参阅在 AWS 上设置 VM 系列防火墙、在 Azure 上设置 VM 系列防火墙或在 Google Cloud Platform 上设置 VM 系列防火墙。
4. 激活 VM 系列防火墙的许可证（独立版本）。

STEP 3 | 在新部署的防火墙上，恢复您导出的配置。

1. 访问新部署的防火墙的 Web 界面。
2. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），并单击 **Import named configuration snapshot**（导入已命名配置快照），Browse（浏览）至位于外部主机的配置文件，单击 **OK**（确定）。
3. 单击 **Load named configuration snapshot**（加载已命名配置快照），选择您导入的配置文件 **Name**（名称），单击 **OK**（确定）。
4. 单击 **Commit**（提交）以使用您刚刚导入的快照覆写正在运行的配置。
5. 在删除防火墙或停用被替换的防火墙上的许可证之前，请验证新防火墙上的配置是否与要更换的防火墙相匹配。

在 VM 系列型号许可证之间切换

您可以使用 BYOL 选项切换当前部署的 VM 系列防火墙的许可证。例如，您可以从订阅套餐转移到企业许可协议 (ELA)，反之亦然，而不会中断通过防火墙的流量。您还可以从 Panorama 同时在单个防火墙或多个防火墙上切换许可证。

不要使用此过程在 *PAYG* 和 *BYOL* 之间切换 *ELA* 或永久许可证。如需更多信息，请参阅 在 BYOL 和 PAYG 许可证之间切换。

完成以下过程之一以执行以下许可证更改之一：

- 订阅套餐 1 到订阅套餐 2

©2024 Palo Alto Networks, Inc.

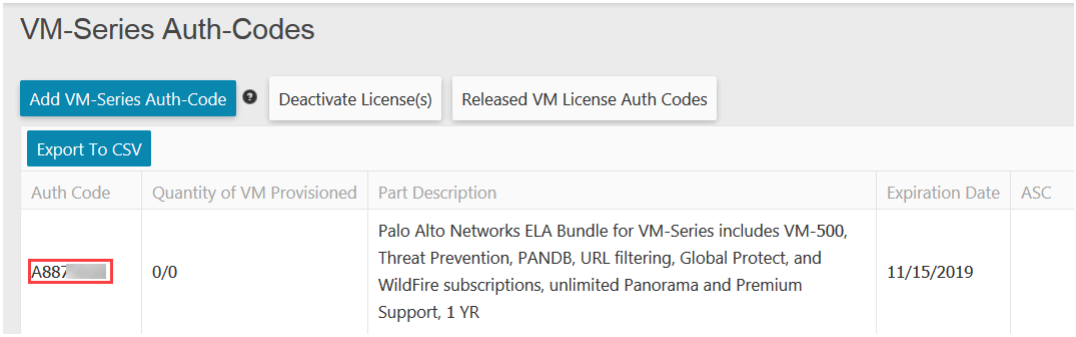
- 订阅套餐 1 或 2 到 ELA
- 订阅套餐或 ELA 的容量许可

在切换到 ELA 许可证之前，您必须分配足够令牌以支持当前部署的 VM 系列防火墙数量。有关每个 VM 系列型号所需的令牌的详细信息，请参阅 VM 系列企业许可协议（多型号 ELA）。

在独立防火墙上切换许可证。

1. 注册授权代码。
   - 对于订阅套餐，注册新授权代码。
   - 对于 ELA，请激活 ELA 授权代码。

   不要使用 *ELA* 授权代码来激活单个 *VM* 系列防火墙。注册 *ELA* 后，使用 *VM* 系列型号授权代码激活各个防火墙。在客户支持门户网站上，您可以在 ***Assets***（资产） > ***VM-Series Auth-Codes***（***VM*** 系列授权代码）下找到这些授权代码。
2. 登录到 VM 系列防火墙 Web 接口。
3. 验证 Palo Alto Networks 更新服务器配置。
   1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）。
   2. 确认 **Update Server**（更新服务器）设置为 updates.paloaltonetworks.com。
   3. 确认已选中 **Update Server Identity**（更新服务器标识）。
4. 应用 VM 系列授权代码。ELA 的防火墙授权代码以字母 A 开头，如下所示。

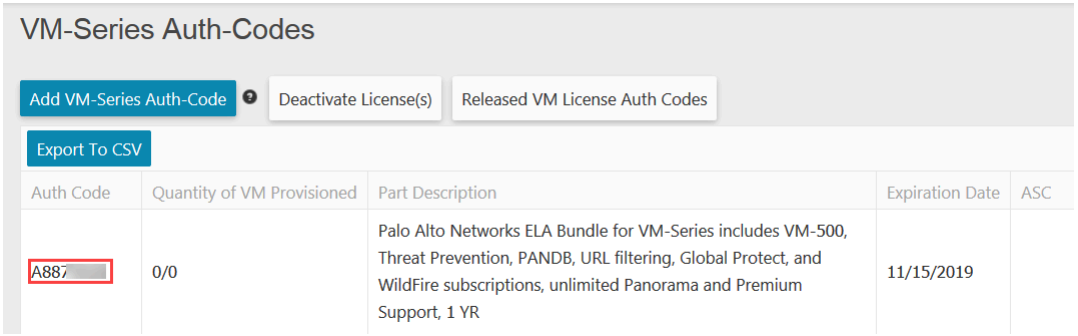
   1. 请选择 **Device**（设备） > **Licenses**（许可证），然后选择 **Activate feature using authorization code**（使用授权代码激活功能）链接。
   2. 输入 VM 系列授权代码。
   3. 单击 **OK**（确定）以确认许可证升级。防火墙与 Palo Alto Networks 更新服务器联系，并根据 VM 系列型号使用防火墙所需的令牌。
   4. 通过检查许可证到期日期验证许可证是否已成功更新。
5. 为部署中的每个 VM 系列防火墙重复此步骤。

©2024 Palo Alto Networks, Inc.

使用 Panorama 在托管防火墙上切换许可证。

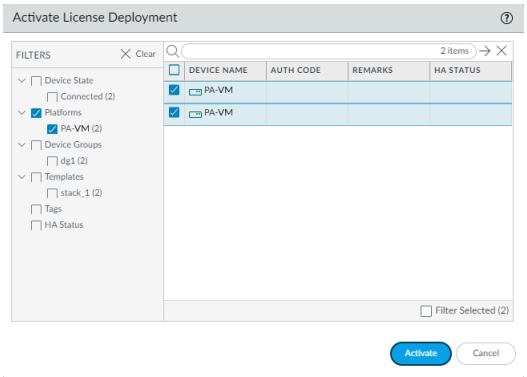
1. 注册授权代码。
   - 对于订阅套餐，注册新授权代码。
   - 对于 ELA，请激活 ELA 授权代码。

   不要使用 *ELA* 授权代码来激活单个 *VM* 系列防火墙。注册 *ELA* 后，使用 *VM* 系列型号授权代码激活各个防火墙。在客户支持门户网站上，您可以在 ***Assets***（资产） > ***VM-Series Auth-Codes***（*VM* 系列授权代码）下找到这些授权代码。
2. 登录到 Panorama Web 界面。
3. 验证防火墙的 Palo Alto Networks 更新服务器配置。
   1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）。
   2. 确认 **Update Server**（更新服务器）设置为 updates.paloaltonetworks.com。
   3. 确认已选中 **Update Server Identity**（更新服务器标识）。
4. 应用 VM 系列授权代码。ELA 的防火墙授权代码以字母 A 开头，如下所示。



   1. 选择 **Panorama** > **Device Deployment**（设备部署） > **Licenses**（许可证），然后单击 **Activate**（激活）。
   2. 输入 VM 系列授权代码。
   3. 使用筛选器选择要许可的托管防火墙。
   4. 对于每个防火墙，在 **Auth Code**（授权代码）列中输入授权代码。
   5. 单击 **Activate**（激活）以确认许可证升级。Panorama 与 Palo Alto Networks 更新服务器联系，并根据 VM 系列型号使用防火墙所需的令牌。

©2024 Palo Alto Networks, Inc.



6. 通过检查许可证到期日期验证许可证是否已成功更新。

停用许可证

许可证停用流程可让您启用许可证自管理。无论是想要移除某个防火墙（基于硬件的防火墙或 VM 系列防火墙）的一个或多个活动许可证或订阅，还是想要停用 VM 系列防火墙并撤回所有的活动许可证和订阅，均需启动防火墙或 Panorama 上的停用流程（而非 Palo Alto Networks 客户支持网站上的流程）。

要成功停用许可证，您必须安装许可证停用API密钥并启用更新服务器身份验证（默认情况下处于启用状态）。PAN-OS使用此停用API密钥进行认证，并与所有更新许可证服务进行身份认证。如果防火墙和许可证服务器之间没有连接，则停用 API 是关键，且无需手动停用许可证。

如果防火墙/Panorama 可访问 Internet，与 Palo Alto Networks 许可服务器进行通信，则只需单击按钮即可自动完成许可证删除流程。如果防火墙/Panorama 没有 Internet 访问权限，您必须通过两步流程来手动完成此过程。第一步，从防火墙或 Panorama 生成并导出许可证令牌文件（包含已停用密钥的相关信息）。第二步，登录到 Palo Alto Networks 客户支持网站后，上传令牌文件，以断开许可证密钥与防火墙之间的关联。

- 使用 CLI 停用功能许可证或订阅
- 停用 VM

使用 CLI 停用功能许可证或订阅

如果您已在防火墙上安装许可证/订阅，且需要重新将此许可证分配至其他防火墙，您可以停用单个许可证，然后在其他防火墙上重新使用相同的授权代码，而无需技术支持部门提供协助。此功能仅在 CLI 中受支持，并且在运行 PAN-OS 的物理和虚拟设备上均受支持。此过程通常与固定型号永久许可证或 ELA 许可证一起使用。

- 允许访问 Internet（自动模式）
- 无法访问 Internet（手动模式）

允许访问 **Internet**（自动模式）

STEP 1 | 在防火墙上登录到 CLI。

©2024 Palo Alto Networks, Inc.

STEP 2 | 查看您要停用的功能的许可证密钥名称。

```
request license deactivate key features
```

STEP 3 | 停用许可证或订阅。

使用自动模式删除许可证密钥。

```
request license deactivate key features <name> mode auto
```

名称为许可证密钥文件的完整名称。例如：

```
admin@vmPAN2> request license deactivate key features <name>
```

```
WildFire_License_2015_01_28_I5820573.key mode auto007200002599
 WildFire License Success Successfully removed license keys
```

无法访问 **Internet**（手动模式）

使用手动模式删除许可证密钥，并为基于型号的许可证生成许可证令牌。此过程假定您已在防火墙上安装许可证 API 密钥。

STEP 1 | 在防火墙上登录到 CLI。

STEP 2 | 查看您要停用的功能的许可证密钥名称。

```
request license deactivate key features
```

STEP 3 | 从命令行手动停用许可证。

```
request license deactivate key features <name> mode manual
```

例如：

```
admin@PA-VM> request license deactivate key features
```

```
PAN_DB_URL_Filtering_2015_01_28_I6134084.key mode manual
 Successfully removed license keys dact_lic.01282015.100502.tok
```

令牌文件使用格式为 `dact_lic.timestamp.tok`，其中时间戳格式为 `dmmyyyy.hrminsec`。

STEP 4 | 验证是否已生成令牌文件。

```
show -token-files
```


©2024 Palo Alto Networks, Inc.

STEP 5 | 导出令牌文件。

在一行中输入以下命令：

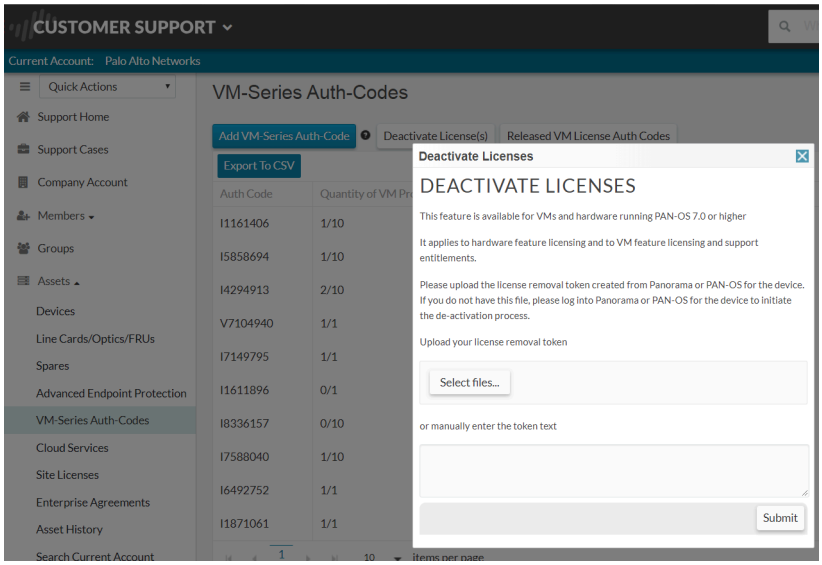
```
scp export license-token-file to <username@serverIP>
from <token_filename>
```

例如：

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

STEP 6 | 登录 Palo Alto Networks 客户支持门户。

1. 在 **Assets**（资产）选项卡上，单击 **Deactivate License(s)**（停用许可证）链接。
2. 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码），然后选择 **Deactivate License(s)**（停用许可证）。
3. 上传令牌文件以完成停用。



停用 VM

当您不再需要 VM 系列防火墙的 BYOL 实例时，您可以从防火墙或 Panorama 的 Web 界面、CLI 或 XML API 释放所有的活动许可证（例如订阅许可证、基于型号的容量许可证和支持授权）。许可证会退回到您的帐户，然后您可以对 VM 系列防火墙的不同实例应用相同的授权代码。

停用 VM 后，会移除所有的许可/授权，且会使 VM 系列防火墙置于非授权状态；防火墙将不再具有序列号，且仅支持最小数量的会话。由于防火墙上的配置仍旧完整，因此您可以在需要时重新应用一系列许可，并在防火墙上恢复所有功能。

©2024 Palo Alto Networks, Inc.

在删除 *VM* 系列防火墙之前，请务必停用许可证。如果在删除防火墙之前未停用许可证，可采用以下两种方式处理：

由 ***Panorama*** 托管 — 通过 *Panorama* 停用许可证。

不由 ***Panorama*** 托管 — 联系 Palo Alto Networks 客户支持以获取停用帮助。

- 从防火墙停用 VM
- 从 Panorama 停用 VM

从防火墙停用 **VM**

完成以下过程以便从防火墙停用 VM 许可证。

STEP 1 | 登录到防火墙 Web 界面，然后选择 **Device**（设备） > **Licenses**（许可证）。

STEP 2 | 在 License Management（许可证管理）部分中，选择 **Deactivate VM**（停用 **VM**）。

此选项仅适用于 VM，不适用于物理防火墙。

STEP 3 | 验证要在防火墙上停用的许可证/权利列表。

STEP 4 | 选择以下任一选项开始停用 VM：

- （通过 Internet 访问 Palo Alto Networks 许可服务器）选择 **Continue**（继续）。

  系统会提示您重新启动防火墙；重新启动后，将停用许可证。

- （无法访问 Internet）— 选择 **Complete Manually**（手动完成）。

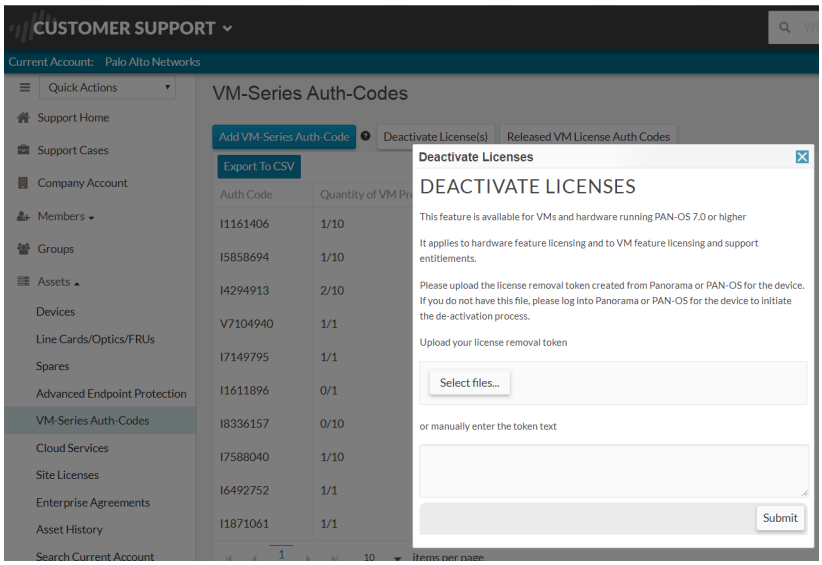
  单击 **Export license token**（导出许可证令牌）链接，可将令牌文件保存到本地计算机。以下是令牌文件名示例：20150128_1307_dact_lic.01282015.130737.tok

  系统会提示您重新启动防火墙；重新启动后，将停用许可证。

©2024 Palo Alto Networks, Inc.

STEP 5 | （手动过程 — 无法访问 Internet）使用令牌文件将更改注册到许可服务器：

1. 登录到 Palo Alto Networks 客户支持网站。
2. 选择 **Assets**（资产）> **VM-Series Auth-Codes**（**VM** 系列授权代码）> **Deactivate License(s)**（停用许可证）。
3. 登录到 Palo Alto Networks 客户支持网站后，上传令牌文件，以完成停用。

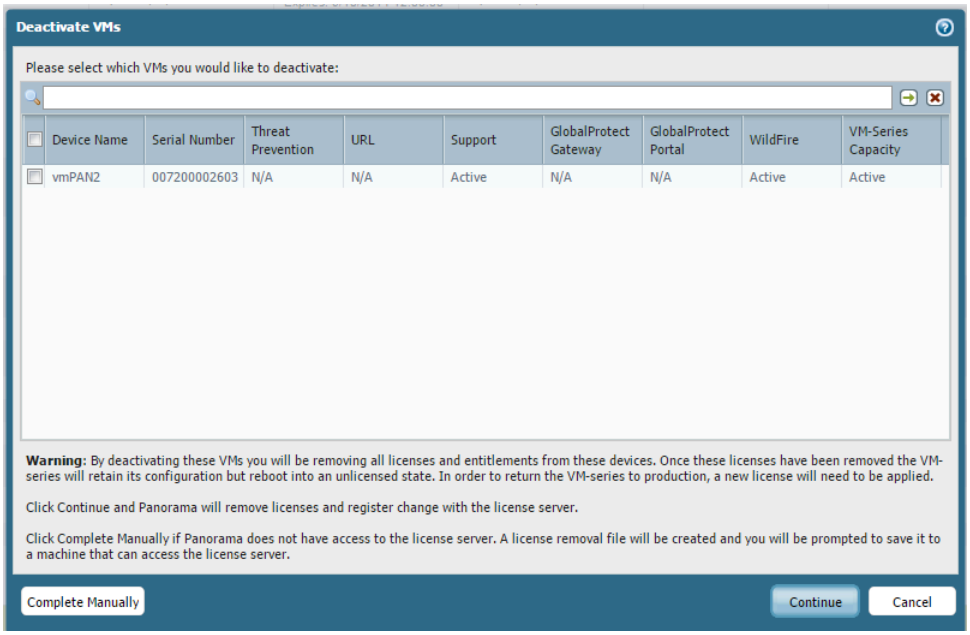


从 **Panorama** 停用 **VM**

完成以下过程以从 Panorama 停用 VM 许可证。

STEP 1 | 登录到 Panorama Web 界面，然后选择 **Panorama** > **Device Deployment**（设备部署）> **Licenses**（许可证）。

STEP 2 | 单击 **Deactivate VMs**（停用 **VM**），选择您想要停用的 VM 系列防火墙。



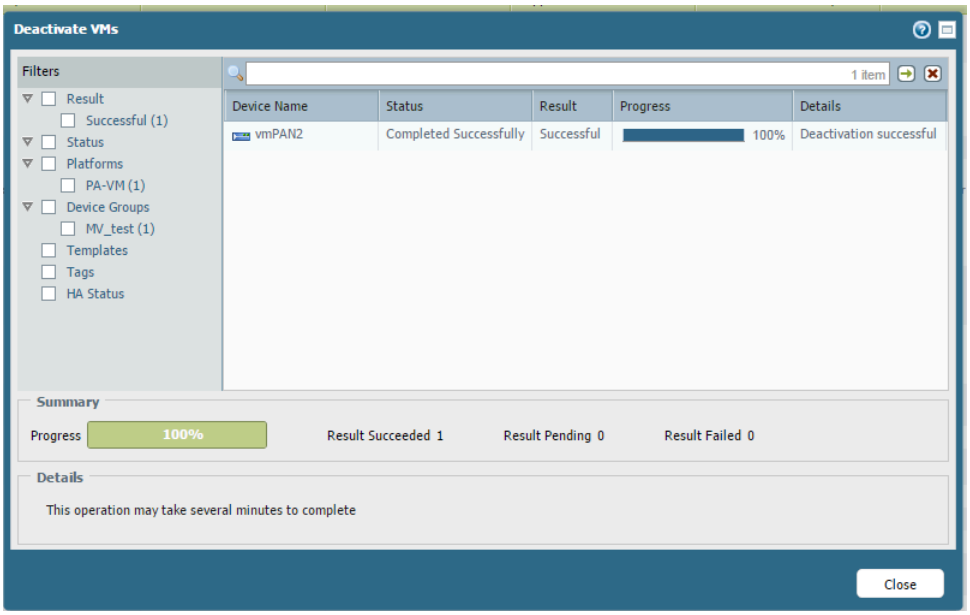
 ©2024 Palo Alto Networks, Inc.

STEP 3 | 选择以下任一选项开始停用 VM：

- 如果 Panorama 可直接与 Palo Alto Networks 许可服务器通信且可注册更改，请单击 **Continue**（继续）。要验证是否已在防火墙上停用许可证，请选择 **Refresh on Panorama**（在 **Panorama** 上刷新）> **Device Deployment**（设备管理）> **Licenses**（许可证）。此时，防火墙将会自动重启。
- **Complete Manually**（手动完成）— 如果 Panorama 无法访问 Internet，则 Panorama 将生成令牌文件。

  单击 **Export license token**（导出许可证令牌）链接，可将令牌文件保存到本地计算机。以下是令牌文件名示例：20150128_1307_dact_lic.01282015.130737.tok

  屏幕上将显示成功完成消息，随即自动重新启动防火墙。



STEP 4 | （仅限手动过程 — 无法访问 Internet）使用令牌文件将更改注册到许可服务器。

1. 登录到 Palo Alto Networks 客户支持网站。
2. 选择 **Assets**（资产）> **VM-Series Auth-Codes**（**VM** 系列授权代码）> **Deactivate License(s)**（停用许可证）。
3. 上传令牌文件以完成停用。

STEP 5 | 删除已停用的 VM 系列防火墙，将其作为 Panorama 上的托管设备。

1. 选择 **Panorama** > **Managed Devices**（托管设备）。
2. 从托管设备列表中选择已停用的防火墙，然后单击 **Delete**（删除）。

除删除防火墙外，您还可根据个人意愿选择创建一个独立的设备组，并将已停用的 *VM* 系列防火墙分配至此设备组。

©2024 Palo Alto Networks, Inc.

更新 VM 系列防火墙许可证包

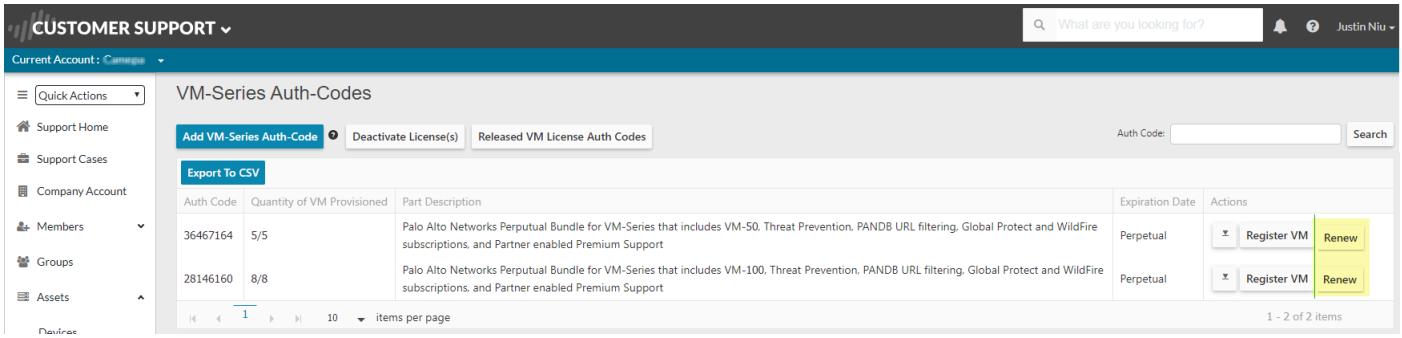
当 VM 系列防火墙包许可证需要更新时，可以登陆到 Palo Alto Networks 客户支持门户，并调整许可证数量以满足您的部署需求。更新时，可以查看您的使用趋势，并根据您未来的需求，从下列选项进行选择：

- **Renew**（更新）— 您可以原样更新所有许可证，或是增加或减少许可证数量。如果减少所需的许可证数量，则必须选择未更新的防火墙基本包，否则将放弃不进行更新的选项。如果增加许可证数量，则将其他许可证添加到现有授权代码中。
- **Change to Basic Bundle**（更改为基本包） — 如果拥有一个包含订阅的 VM 系列包 1 或包 2，则可以更改为包含永久容量许可证且支持权利的基本包。切换到基本包时，可以保留先前购买的 VM 系列防火墙型号。当前部署且已关联至现有授权代码的所有防火墙将继续运行，且支持权利将具有新的到期日。对于任何未设置的防火墙，您将收到一个可用于部署新实例的授权代码。
- **Forfeit**（放弃）— 放弃不再需要的许可证。如果已部署不再需要更新的防火墙，则需要选择想要停止更新的实例序列号。可以通过当前安装的软件和内容版本使用这些防火墙实例，但您的订阅和支持权利将不再有效。要放弃尚未配置的 VM 系列防火墙的许可证，只需选择要放弃的数量即可。

STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持门户。

STEP 2 | 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码），找到想要更新的授权代码。

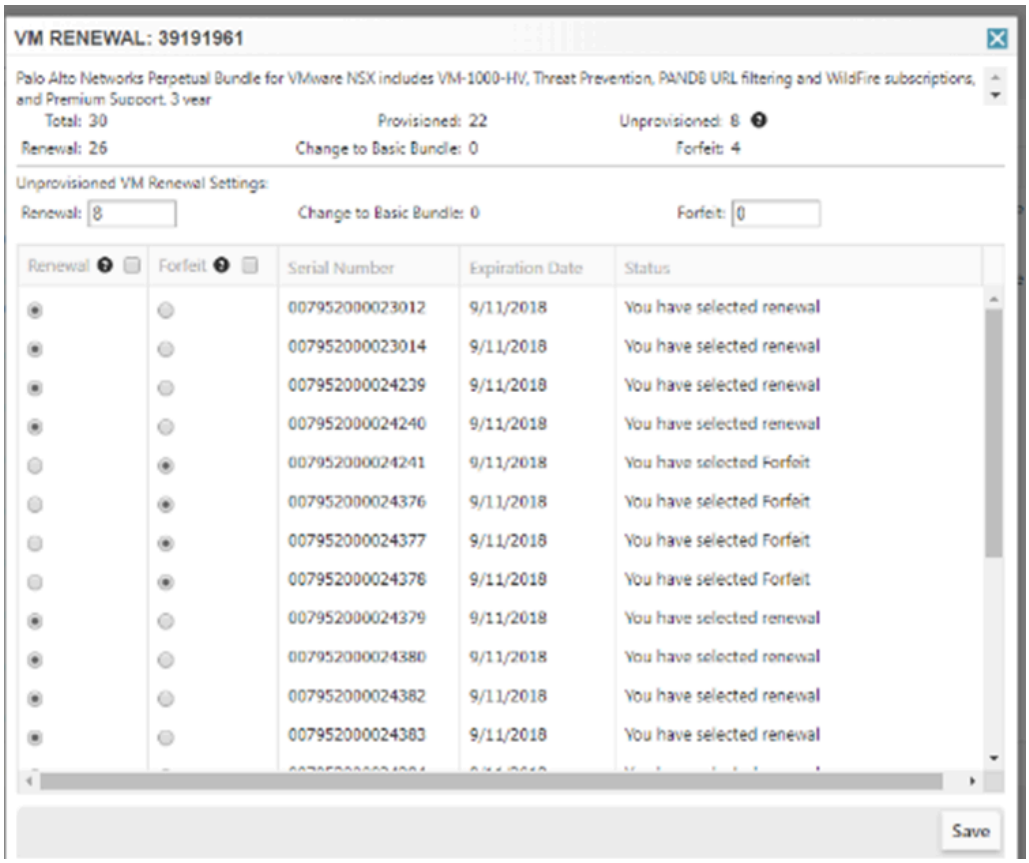
Renew（续订）选项显示适用于续订的授权代码。



©2024 Palo Alto Networks, Inc.

STEP 3 | 单击 **Renew**（更新）链接，选择 **Renew**（更新）、**Change to Basic Bundle**（更改为基本包）或 **Forfeit**（放弃）的序列号。

如果已配置防火墙，请在与序列号对应的行中选择适当的选项。如果有未设置的防火墙实例，请选择在 **Unprovisioned VM Renewal Settings**（未预配置的 **VM** 续订设置）下选择的每个续订选项的数量。



STEP 4 | **Save**（保存）更改。

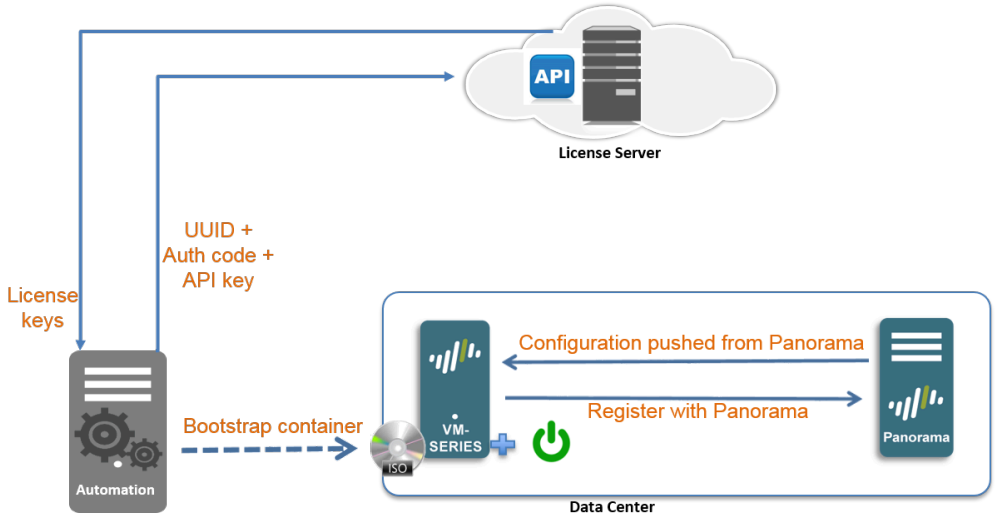
您将在屏幕上收到确认信息，确认您的更改已提交进行处理。提交更改后，如果再次选择续订，则可以针对每个序列号查看请求的状态。如果续订处理已开始，并且需要进行其他修订，则无法保存更改。如需帮助，您可以通过 renewals@paloaltonetworks.com 与续订团队联系。

基于型号的许可 API

使用基于型号的许可 API 注册授权代码，检索附加到授权代码的许可证，续订许可证或停用 VM 系列防火墙上基于型号的许可证。此外，许可 API 可让您许可无法直接访问 Internet 且无法访问 Palo Alto Networks 许可服务器的防火墙。您可以手动管理许可证或使用自定义脚本或编排服务自动许可。

您还可以使用 Panorama 软件防火墙许可证插件许可任务，包括离线许可。插件需要 *Panorama 10.0.0* 或更高版本以及 *VM* 系列插件 *2.0.4* 或更高版本，并且您的托管 *VM* 系列防火墙必须运行 *PAN-OS 9.1.0* 或更高版本和 *VM* 系列插件 *2.0.4* 或更高版本；适用于 *Azure* 的 *VM* 系列防火墙需要 *VM* 系列插件 *2.0.8*。

©2024 Palo Alto Networks, Inc.



对于基于型号的许可证，您还可以使用 API 查看授权代码的详细信息，以便跟踪与某个授权代码或授权代码套餐相关的未使用许可证的数量，进而对多个防火墙实例进行许可。授权代码包中包括 VM 系列型号、订阅和支持，这些均采用易于订购的单一格式；您可以重复使用该授权代码包，以便在部署 VM 系列防火墙时对其进行许可。

为了使用该 API，每个支持帐户都分配有一个独特的密钥。每次 API 调用都是一次 POST 请求，且该请求必须包含 API 密钥，以便认证对许可证服务器的请求。通过身份验证后，许可服务器将会以 json 格式（内容类型应用程序/json）发送响应。

- 安装许可证 API 密钥
- 管理许可证 API 密钥
- 使用许可证 API
- 许可证 API 错误代码

安装许可证 **API** 密钥

许可证 API 密钥可用于激活、更改或停用许可证。此过程适用于 VM 系列防火墙或 Panorama 部署。

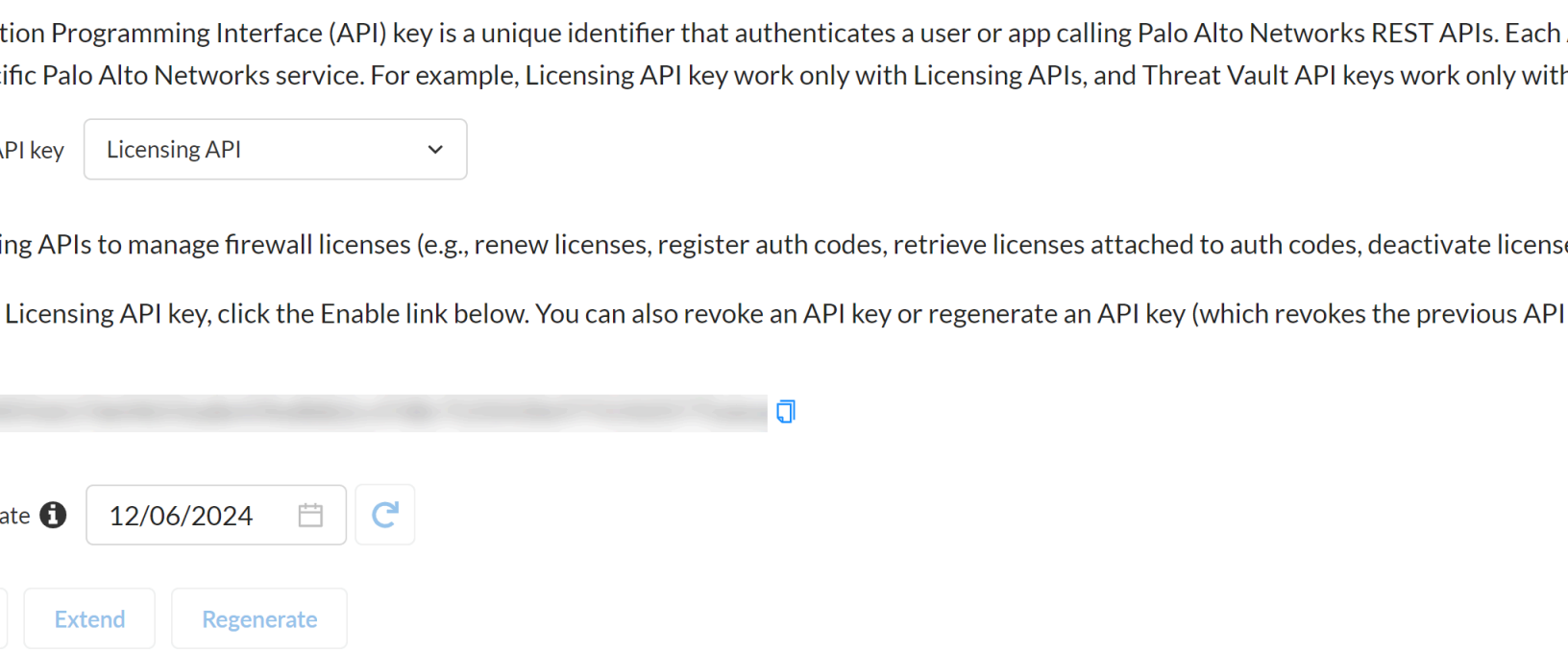
您必须具有超级用户权限才能从客户支持门户检索许可证 API 密钥，并使用 CLI 在防火墙或 Panorama 上安装密钥。

在 Panorama 上安装许可证 API 密钥时，Panorama 会将 API 密钥推送到其托管设备。如果托管设备已安装 API 密钥，则 Panorama 会使用新密钥覆盖旧的 API 密钥。

©2024 Palo Alto Networks, Inc.

STEP 1 | 从客户支持门户检索许可证 API 密钥。

1. 登录到客户支持门户。
2. 选择 **Assets**（资产）> **Licensing API**（许可证 **API**）。
3. 复制 API 密钥。



STEP 2 | 使用 CLI 安装在上一步中复制的 API 密钥。将密钥粘贴到请求中：

```
request license api-key set key <key>
```

STEP 3 | （可选）要替换许可证停用 API 密钥，请使用以下 CLI 命令删除已安装的 API 密钥。

```
request license api-key delete
```

如果您删除 API 密钥，则必须先安装另一个许可证停用密钥，然后才能停用许可证。

管理许可证 API 密钥

要获得使用授权 API 所需的 API 密钥，您的帐户必须在支持门户上拥有超级用户权限。您可以使用同一密钥激活和停用许可证。

API 密钥的过期日期与支持帐户中最新订阅的日期相同。如果续订当前订阅且需要重置 API 密钥的过期日期，则可以重新生成密钥（并使用新密钥替换现有密钥，不管在何处使用），或者联系 Palo Alto Networks，以便帮助您扩展现有 API 密钥的期限。

©2024 Palo Alto Networks, Inc.

STEP 1 | 获取许可证 API 密钥。

1. 使用具有超级用户权限的帐户登录到 Palo Alto Networks 支持门户。
2. 选择 **Assets**（资产） > **API Key Management**（**API** 密钥管理）。
3. 单击 **Enable**（启用）以查看密钥，并 复制密钥以供使用。一旦生成密钥，该密钥就会启用，直到您重新生成或禁用密钥。

STEP 2 | 重新生成或调用 API 密钥。

1. 您可以生成一个新 API 密钥或调用密钥的使用。
   - 单击 **Regenerate**（重新生成），以生成一个新密钥。如果您怀疑 API 密钥可能已泄露，则可以生成新密钥。自动重新生成新密钥会使旧密钥失效。
   - 如果您不再打算使用此密钥，则选择 **Disable**（禁用）。禁用 API 密钥将会予以调用。

使用许可证 API

访问许可 API 的基本 URI 是 https://api.paloaltonetworks.com/api/license；根据您要执行的任务（例如激活许可证，停用许可证或跟踪许可证使用情况），URL 将会更改。

API 请求必须使用 HTTP POST 方法，并且必须将 API 密钥包含在 apikey HTTP 请求标头中，并使用 `content-type application/x-www-form-urlencoded` 将请求参数作为 URL 编码的表单数据传递。

API 版本是可选的，可以包含以下值 — 0或1。如果指定，它必须包含在 `version` HTTP 请求标头。当前的 API 版本是 1；如果您未指定版本或指定版本 0，则请求将使用当前的 API 版本。

所有的 API 响应均采用 json 格式。

在开始之前，获取您的许可 API 密钥并将其复制到您的本地驱动器。在执行以下任何任务之前，必须执行这一步：

- 激活许可证
- 停用许可证
- 跟踪许可证使用情况

激活许可证

标题：apikey

参数：`uuid`、`cpuid`、`authCode`、`memory`、`serialNumber` 和 `vCPU`

URL：`https://api.paloaltonetworks.com/api/license/activate`

无论 PAN-OS 版本怎样，参数 uuid、cpuid、authCode 和 serialNumber 适用于所有 VM 系列许可证。

可选参数 `memory` 和 `vCPU` 仅适用于灵活的 vCPU（PAN-OS 10.0.4 及更高版本）。

©2024 Palo Alto Networks, Inc.

- 对于初始许可证激活，请在 API 请求中提供参数。例如：

```
curl -i -H
 "apikey:a103e3065360acc5e01666fb9335964fcfe668100666db6f3ff43d4544de0###"
 --data-urlencode cpuid=AWS:57060500FFFBE### --data-urlencode
 uuid=EC2278FF-F0CB-45E2-343B-E97984BAC### --data-urlencode
 authCode=D3521### --data-urlencode vcpu=4 --data-urlencode
 memory=8388608 https://api.paloaltonetworks.com/api/license/
activate
```

- 如果您在初始许可证激活期间未保存许可证密钥或遇到网络连接问题，您可以检索以前激活的防火墙的许可证。

  在 API 请求中，请提供 `cpuid` 和 `uuid`，或提供防火墙的 `serialNumber`。

使用 **Crul** 进行初始许可证激活时的示例请求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode cpuid=51060400FFFBAB1F
 --data-urlencode uuid=564D0E5F-3F22-5FAD-DA58-47352C6229FF --data-
urlencode authCode=I7115398 https://api.paloaltonetworks.com/api/
license/activate
```

示例 **API** 响应：

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureFi--eld":"Premium","feature_descField":"24
 x 7 phone support; advanced replacement
 hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","errmsgField":null,
 "typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/
 "vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":nul
 "mac_countField":null,"drrField":null,"expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP",
 "featureField":"Threat Prevention","feature_descField":"Threat
 Prevention","keyField":"NqaXoaFG+9qj0t9Vu7FBMizDArj
+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl\n2qJhNq3kwXBDxn181z3nrUOsQd/
eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b\ndZBRH5AQjPoaON7xZ46VMFovOR
+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==\n","auth_codeField":"",
 "errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03T08:18:41",
 "startDateField":"5/29/2016","vm_capacityField":null,"uuidField":null,
 "cpuidField":null,"mac_baseField":null,"mac_countField":null,"drrField":null,
 "expirationField":"8/29/2016 12:00:00
 AM","PropertyChanged":null} ...<truncated>
```


©2024 Palo Alto Networks, Inc.

响应中的 *feature_Field* 用于指示在 *keyField* 中的密钥类型。将每个密钥复制到文本文件中，并以 *.key* 的扩展名保存。因为密钥为 *json* 格式，所以没有换行符。如果分析程序需要，请确保将其转换为换行符。确保对每个密钥进行适当命名，并将其保存在引导数据包的 */license* 文件夹中。可以按照密钥类型保存授权代码，例如可采用以下命名：*I3306691_1pa-vm.key*（适于容量许可证密钥）、*I3306691_1threat.key*（适于 *Threat Prevention* 许可证密钥）、*I3306691_1wildfire.key*（适于 *WildFire* 订阅许可证密钥）。

使用 **Curl** 检索以前激活的许可证的示例 **API** 请求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 serialNumber=007200006142 https://api.paloaltonetworks.com/api/
license/activate
```

示例 **API** 响应：

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureField":"Premium","feature_descField":"24
 x 7 phone support; advanced replacement
 hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","errmsgField":null,
 "typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/
 "vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":nul
 "mac_countField":null,"drrField":null, "expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP",
 "featureField":"Threat Prevention","feature_descField":"Threat
 Prevention","keyField":"NqaXoaFG+9qj0t9Vu7FBMizDArj
+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl\n2qJhNq3kwXBDxn181z3nrUOsQd/
eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b\ndZBRH5AQjPoaON7xZ46VMFovOR
+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUB",
 "regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2016","vm_capacity
 "mac_countField":null,"drrField":null,"expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null} ...<truncated>
```

停用许可证

URL：https://api.paloaltonetworks.com/api/license/deactivate

参数：encryptedToken

要停用未直接连接到 Internet 的防火墙的许可证，您必须在防火墙上本地生成许可证令牌文件，然后在 API 请求中使用该令牌文件。有关生成许可证令牌文件的详细信息，请参阅停用 VM，停用许可证（软件 NGFW 积分）以及使用 CLI 停用功能许可证或订阅。

©2024 Palo Alto Networks, Inc.

标题：apikey

请求：https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>

使用 **Crul** 停用许可证时的示例 **API** 请求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 encryptedtoken@dact_lic.05022016.100036.tok https://
api.paloaltonetworks.com/api/license/deactivate
```

示例 **API** 响应：

```
[{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nu
 {"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
 "successField":"Y","errorField":null,"isBundleField":null,
 "PropertyChanged":null}]$
```

跟踪许可证使用情况

URL：**https://api.paloaltonetworks.com/api/license/get**

参数：authCode

标题：apikey

请求：https://api.paloaltonetworks.com/api/license/get?authCode=<authcode>

使用 **Crul** 追踪许可证使用时的示例 **API** 请求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode authcode=I9875031
 https://api.paloaltonetworks.com/api/license/get
```

示例 **API** 响应：

```
HTTP/1.1 200 OK Date:Thu, 05 May 2016 20:07:16 GMT Content-Length:182
 {"AuthCode":"I9875031","UsedCount":4,"TotalVMCount":10,"UsedDeviceDetails":
[{"UUID":"420006BD-113D-081B-F500-2E7811BE80C
 9","CPUID":"D7060200FFFBAB1F","SerialNumber":"007200006142"}]}.....
```

许可证 **API** 错误代码

许可证服务器会返回的 HTTP 错误代码如下所示：

- 200 成功
- 400 错误

©2024 Palo Alto Networks, Inc.

- 401 API 密钥无效
- 500 服务器错误

©2024 Palo Alto Networks, Inc.

许可证到期后会发生什么？

Palo Alto Networks VM 系列防火墙许可证和订阅为防火墙提供附加功能和/或访问 Palo Alto Networks 云交付设备的权限。当许可证到期前 30 天内，系统日志中每天都会显示一条警告消息，直到订阅续订或到期为止。许可证过期后，一些订阅仍继续以有限容量运行，而另一些则完全停止运行。下面介绍了每个订阅到期后会发生的事件。

许可证确切的到期时间是次日凌晨 *12:00 (GMT)*。例如，如果您的许可证预计在 *1/20* 结束，则您在当天剩余时间内仍能使用该功能。从新一天 *1/21* 日的凌晨 *12:00 (GMT)* 开始，许可证将处于到期状态。无论防火墙上配置的时区如何，所有与许可证相关的功能均按格林威治标准时间 *(GMT)* 运行。

（*Panorama* 许可证）如果支持许可证已过期，*Panorama* 仍可以管理防火墙并收集日志，但软件更新和内容更新将不可用。*Panorama* 上的软件和内容版本必须与受管防火墙上的软件和内容版本相同，或者高于后者，否则会出现错误。有关详细信息，请参阅 Panorama、日志收集器、防火墙和 WildFire 的版本兼容性。

许可证：	到期行为
VM-SERIES	您仍能： 您可以继续配置和使用在许可证到期之前部署的防火墙，而会话容量不会发生变化。防火墙不会自动重启和导致流量中断。 但是，如果防火墙因任何原因重新启动，则会进入未许可状态。虽然未获得许可，但支持的会话数限制为 1200。其他管理平面功能或配置选项不受限制。
威胁防护	系统日志中出现警报，指示许可证已到期。 您仍能： • 除非您已手动安装或是作为自动安排的一部分安装有一个仅适用于应用程序的新内容更新，否则，请使用在许可证到期时安装的签名。如果这样操作，更新将删除您现有的威胁签名，且您将再也无法获得对这些签名的保护。 • 使用并修改自定义 App-ID™ 和威胁签名。 您再也不能： • 安装新签名。 • 将签名滚回到先前版本。
DNS 安全	您仍能： • 使用本地 DNS 签名，前提是您拥有有效的威胁防护许可证。

©2024 Palo Alto Networks, Inc.

许可证：	到期行为
	您再也不能： • 获取新的 DNS 签名。
高级 URL 过滤 / URL 过滤	您仍能： • 使用自定义 URL 类别实施策略。 • 使用许可证到期时已保存在本地缓存中的 PAN-DB 类别实施策略。 您再也不能： • 获取缓存的 PAN-DB 类别更新。 • 连接到 PAN-DB URL 过滤数据库。 • 获取未缓存的 URL 的 PAN-DB 类别。 • 使用高级 URL 过滤实时分析 URL 请求。
WildFire	您仍能： • 转发 PE 进行分析。 • 每隔 24-48 小时获取签名更新一次，前提是您拥有有效的威胁防护订阅。 您再也不能： • 通过 WildFire 公共云和私有云每隔 5 分钟获取更新一次。 • 转发 APK、Flash 文件、PDF、Microsoft Office 文件、Java Applets、Java 文件（.jar 和 .class）以及 SMTP 和 POP3 电子邮件消息中包含的 HTTP/HTTPS 电子邮件链接等高级文件类型。 • 使用 WildFire API。 • 使用 WildFire 设备托管 WildFire 私有云或 WildFire 混合云。
AutoFocus	您仍能： • 在三个月宽限期内将外部动态列表与 AutoFocus 数据一起使用。 您再也不能： • 访问 AutoFocus 门户。 • 查看 AutoFocus 情报摘要以监控日志或 ACC 构件。
Cortex 数据湖	您仍能：

©2024 Palo Alto Networks, Inc.

许可证：	到期行为
	• 在日志数据被删除后拥有 30 天的宽限期保存此数据。 • 在 30 天宽限期结束后转发日志到 Cortex 数据湖。
GlobalProtect	您仍能： • 使用适用于运行 Windows 和 macOS 的端点的应用程序。 • 配置单个或多个内部/外部网关。 您再也不能： • 访问适用于运行 iOS、Android、Chrome OS 和 Windows 10 UWP 的 Linux OS 应用程序和移动应用程序。 • 使用适用于外部网关的 IPv6。 • 运行 HIP 检查。 • 使用 无客户端 VPN。 • 根据目的域、客户端进程和视频流应用程序强制拆分隧道。
支持	您再也不能： • 接收软件更新。 • 下载 VM 映像。 • 受益于技术支持。

©2024 Palo Alto Networks, Inc.

云安全服务提供商许可证 (CSSP)

Palo Alto Networks CSSP 合作伙伴计划允许服务提供商将安全作为服务或作为托管应用程序提供给其最终客户。Palo Alto Networks 为授权云安全服务提供商 (CSSP) 合作伙伴提供的许可证产品与企业用户的产品有所不同。

对于 CSSP 合作伙伴，Palo Alto Networks 支持与预订和支持捆绑在一起的 VM 系列防火墙的基于使用情况的模型。CSSP 合作伙伴可以将基于期限的容量许可证与 VM 系列型号结合使用，从而可选择威胁预防、URL 筛选，AutoFocus、GlobalProtect 和 WildFire 的订阅许可证，并提供访问技术支持和软件更新的权利。如果您计划在 HA 配置中部署防火墙，则可以购买具有成本效益的高可用性选项。

- 获取 CSSP 许可证包的身份验证码
- 使用 CSSP 授权代码注册 VM 系列防火墙
- 为注册的 VM 系列防火墙添加最终用户信息

获取 CSSP 许可证包的身份验证码

要成为 CSSP 合作伙伴，您必须注册 Palo Alto Networks CSSP 合作伙伴计划。有关注册 CSSP 计划的信息，请联系您的 Palo Alto Networks 渠道业务经理。如果您已注册，Palo Alto Network 支持门户会提供允许您选择许可证包、跟踪许可证使用情况并应用许可证权利的工具。

许可证包是以下选项的组合：

- 使用条款 — 按使用付费的选项为小时、每月、1 年和 3 年。
- VM 系列防火墙型号 — VM-100、VM-200、VM-300 和 VM-1000-HV，可为您提供型号和与每个型号相关的容量。
- 订阅包 — 三个选项为基本、包 1 和包 2。基本选项不包括任何订阅；包 1 拥有威胁预防许可证，包括 IPS、AV、恶意软件预防；包 2 拥有威胁预防（包括 IPS、AV、恶意软件预防）、DNS 安全、GlobalProtect、WildFire 和 PAN-DB URL 筛选许可证。
- 支持级别 — 高级支持或后台支持。
- 冗余防火墙 — 该选项为高可用性 (HA) 或无 HA。如果您计划部署一对冗余防火墙，则此选项是一个经济实惠的选项。

例如，提供的 PAN-VM-300-SP-PREM-BND1-YU 是一个为期一年的软件包，其中包括具有高级支持和订阅包 1 的 VM-300。每个软件包最多支持 10,000 个 VM 系列防火墙实例。

在您选择许可证包后，您会收到一封包含授权代码的电子邮件；执行过程可能需要长达 48 小时。

STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。如果需要新帐户，请参阅创建支持帐户。

STEP 2 | 选择 **CSSP** > **Order History**（订单历史记录）查看注册到您的支持帐户的授权代码。

在部署防火墙时，您必须针对授权代码注册防火墙的每个实例。

©2024 Palo Alto Networks, Inc.

使用 CSSP 授权代码注册 VM 系列防火墙

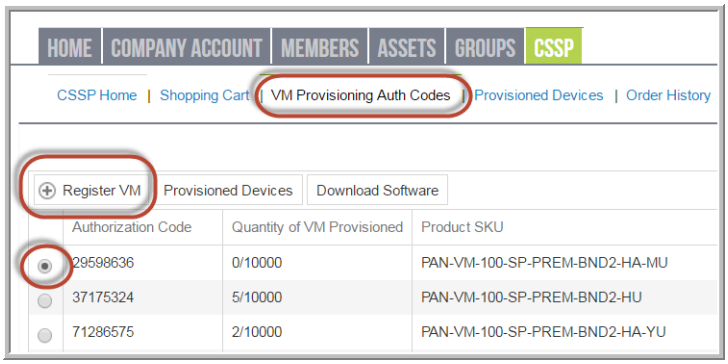
要在 VM 系列防火墙上激活许可证，必须已部署此 VM 系列防火墙，并已完成初始配置。作为 CSSP 合作伙伴，您可以选择以下选项来注册防火墙：

- API —使用许可 API，如果您有自定义脚本或编排服务。凭借此选项，防火墙不需要直接访问 Internet。
- 引导程序 - 使用此选项可以自动配置防火墙并在首次引导时对其进行许可。参阅引导 VM 系列防火墙。
- 防火墙 Web 界面 — 您可以使用防火墙 Web 界面激活 VM 系列防火墙的许可证（独立版本）。此工作流程适用于带或不带Internet访问的防火墙。
- 客户支持门户 — 使用此选项在Palo Alto Networks客户支持门户上手动注册防火墙，如下所示。

STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。如果需要新帐户，请参阅创建支持帐户。

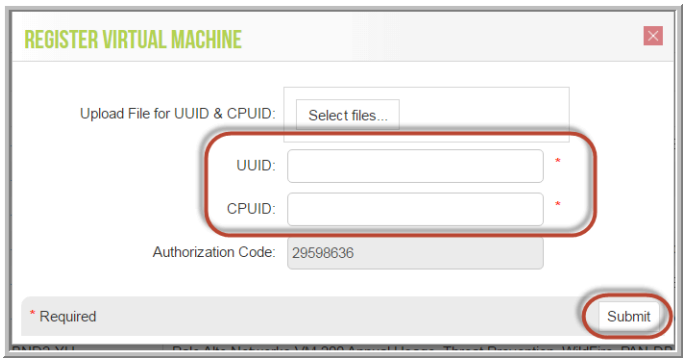
STEP 2 | 选择 **CSSP** > **Order History**（订单历史记录）查看注册到您的支持帐户的授权代码。

STEP 3 | 选择 **CSSP** > **VM Provisioning Auth Codes**（**VM** 预配置授权代码），选择一个 **Authorization Code**（授权代码）并单击 **Register VM**（注册 **VM**）。



©2024 Palo Alto Networks, Inc.

STEP 4 | 输入 **UUID** 和 **CPUID** 的虚拟机实例并单击 **Submit**（提交）。门户将会为防火墙生成一个序列号。



您可以跟踪已部署的 *VM* 系列防火墙的数量和仍可用于针对每个授权代码使用的许可证的数量。要查看根据特定授权代码注册的所有防火墙数量，请选择 ***CSSP*** > ***VM Provisioning Auth Codes***（***VM*** 预配置授权代码），然后选择一个 ***Authorization Code***（授权代码）并单击 ***Provisioned Devices***（已配置设备）。

为注册的 VM 系列防火墙添加最终用户信息

对于 CSSP 许可证持有者，在注册防火墙后，可以使用 Palo Alto Networks 支持门户或许可 API 将 VM 系列防火墙的序列号与为其配置防火墙的客户链接。

- 为注册的 VM 系列防火墙添加最终客户信息（客户支持门户）。支持门户使用用户名和密码进行身份验证。
- 为注册的 VM 系列防火墙 (API) 添加最终客户信息。API 使用许可 API 密钥进行身份验证。

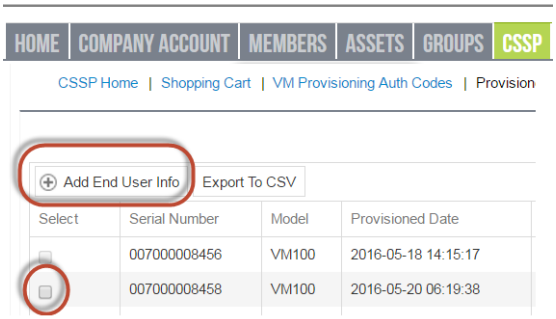
为注册的 VM 系列防火墙添加最终用户信息（客户支持门户）

通过客户支持门户完成以下过程，为已注册的防火墙添加最终用户信息。

STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。

STEP 2 | 选择 **CSSP** > **Provisioned Devices**（配置的设备）。

STEP 3 | 选择 **Serial Number**（序列号），然后单击 **Add End User Info**（添加最终用户信息）。

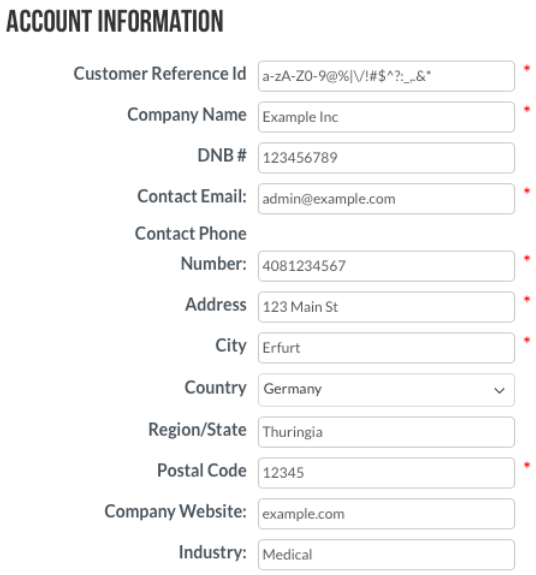


©2024 Palo Alto Networks, Inc.

STEP 4 | 按如下为客户输入 **Account Information**（帐户信息）。

- 客户参考 ID：必需
- 公司名称：必需
- DNB #：数据通用编号系统 (D-U-N-S) 编号
- 联系人电子邮件：必需，最终用户电子邮件地址
- 联系人电话号码：最终用户电话号码
- address:必需，最终用户地址
- 国家/地区：必需，ISO 2 个字母国家代码
- 城市：必需，最终用户城市名称
- 地区/国家：需要;对于美国和加拿大，您必须输入一个 ISO 2 个字母的细分代码;对于所有其他国家，任何文本字符串都是有效的
- 邮政编码：必需，最终用户邮政编码
- 公司网站：最终用户网站网址
- 行业：最终用户行业类型，例如网络或咨询

单击 **Submit**（提交）保存详细信息。



添加帐户信息后，您可以找到注册给客户的所有防火墙。在 ***Search Existing End User***（搜索现有最终用户），输入客户*ID*或客户名称并单击 ***Search***（搜索） 找到为客户提供的所有防火墙。

为注册的 VM 系列防火墙 (API) 添加最终客户信息

访问 API 的 URL 为 https://api.paloaltonetworks.com/api/license/ReportEndUserInfo。

API 请求必须使用 HTTP POST 方法，并且必须包括包含 API 密钥的 HTTP 请求标头并将内容类型指定为 JSON。API 响应采用 JSON 格式。

©2024 Palo Alto Networks, Inc.

STEP 1 | 获取许可证 API 密钥。

STEP 2 | 使用 ReportEndUserInfo API 为注册到 CSSP 的 VM 系列防火墙添加最终用户信息。

URL: **`https://api.paloaltonetworks.com/api/license/ReportEndUserInfo`**

标头：

- 内容类型：application/json
- apiKey：*API* 密钥

参数：

- `SerialNumbers`：必需，提供至少一个有效的防火墙序列号
- `CustomerReferenceId`：必需
- `CompanyName`：必需，最终用户公司名称
- `DnBNumber`：数据通用编号系统 (D-U-N-S) 编号
- `PhoneNumber`：最终用户电话号码
- `EndUserContactEmail`：必需，最终用户电子邮件地址
- `Address`:必需，最终用户地址
- `Country`:必需，ISO 2 个字母国家代码
- `City`:必需，最终用户城市名称
- `Region/State`:必需；对于美国和加拿大，必须输入 ISO 2 个字母细分代码；对于所有其他国家/地区，可输入任何大小写字母字符串
- `PostalCode`：必需，最终用户邮政编码
- `Industry`:最终用户行业类型，例如网络或咨询
- `WebSite`：最终用户网站网址
- `CreatedBy`：系统或个人提交此信息

使用 **Curl** 为注册的 **VM** 系列防火墙添加最终用户信息的示例请求：

```
curl -X POST "http://api.paloaltonetworks.com/
api/license/ReportEndUserInfo" \-H "Content-Type:
 application/json" \-H "apikey: your_key_here" \--data-raw
 '{ "SerialNumbers": ["0001A101234"], "CustomerAccountId":12345,
 "CompanyName":"ExampleInc", "DnBNumber":"123456789",
 "Address":"123 Main St", "City":"Sunnydale", "Region":"CA",
 "State":"CA", "Country":"US", "PostalCode":"12345",
 "Industry":"Medical", "PhoneNumber":"4081234567", "WebSite":
```


©2024 Palo Alto Networks, Inc.

```
 "example.com", "EndUserContactEmail": "admin@example.com",
 "CreatedBy":"Jane Doe"}'
```

示例 **API** 响应：

```
"{"Message":"End User Information Updated Successfully"}"
```

如果您收到错误，请参阅许可 API 错误代码。

©2024 Palo Alto Networks, Inc.

在 ESXi 服务器上设置 VM 系列防火墙

使用开放式虚拟化联盟 (OVA) 格式分发 VM 系列防火墙，这是打包和部署虚拟机的标准方法。您可以在能够运行 VMware ESXi 的任何 x86 设备上安装此解决方案。

为部署 VM 系列防火墙，您必须熟悉 VMware 和 vSphere（包括 vSphere 网络）、ESXi 主机设置和配置以及来宾虚拟机部署。

如果要自动化部署 VM 系列防火墙的过程，您可以使用最佳配置和策略创建一个黄金标准模板，然后使用 vSphere API 和 PAN-OS XML API 在您的网络中快速部署新的 VM 系列防火墙。

请参阅以下主题获取相关信息：

- 在 VMware vSphere 虚拟机监控程序 (ESXi) 上支持的部署
- ESXi 系统上 VM 系列的要求和限制
- 在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙
- vCenter 上的 VM 监控
- 排除 ESXi 部署的故障
- ESXi 的 VM 系列性能调整

在 VMware vSphere 虚拟机监控程序 (ESXi) 上支持的部署

您可以在 ESXi 服务器上部署 VM 系列防火墙的一个或多个实例。是否将 VM 系列防火墙放入网络中取决于您的拓扑。选择以下选项（对于不使用 VMware NSX 的环境）：

- 每个 **ESXi** 主机一个 **VM** 系列防火墙 — 在退出物理网络的主机之前，ESXi 主机上的每个 VM 服务器都会通过此防火墙。VM 服务器通过标准虚拟交换机连接到防火墙。来宾服务器没有其他网络连接，因此该防火墙可监控和控制离开 ESXi 主机的所有流量。此用例的一个变化因素是，还需要所有流量通过此防火墙流动，包括同一 ESXi 主机上的服务器到服务器流量（东向西流量）。
- 每个虚拟网络一个 **VM** 系列防火墙 — 为每个虚拟网络部署一个 VM 系列防火墙。如果对您的网络进行了相应的设计，以使一个或多个 ESXi 主机拥有一组属于内部网络的虚拟机，一组属于外部网络的虚拟机，以及一组属于 DMZ 的虚拟机，则可部署一个 VM 系列防火墙来保护每组的服务器。如果某个组或虚拟网络不与任何其他虚拟网络共享虚拟交换机或端口组，则与主机之内或之间的所有其他虚拟网络完全隔离。由于没有任何其他网络的其他物理或虚拟路径，每个虚拟网络中的服务器必须使用防火墙才能与任何其他网络通信。防火墙可以监控和控制离开连接到每个虚拟网络的（标准或分布式）虚拟交换机的所有流量。
- 混合环境—物理和虚拟主机都需要使用。VM 系列防火墙可以替代传统聚合位置的物理防火墙设备。混合环境可以获得用于所有设备的通用服务器平台的优势，并取消硬件和软件升级依赖关系。

继续使用 ESXi 系统上 VM 系列的要求和限制和 在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

ESXi 系统上 VM 系列的要求和限制

本部分列出了 VMware vSphere 虚拟机监控程序 (ESXi) 上 VM 系列防火墙的要求和限制。要部署 VM 系列防火墙，请参阅 在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙。

- ESXi 系统上 VM 系列的要求
- ESXi 系统上 VM 系列的限制

ESXi 系统上 VM 系列的要求

您可以在 ESXi 服务器上创建和部署 VM 系列防火墙的多个实例。在 ESXi 服务器上，由于此防火墙的每个实例都需要最低资源配置（CPU、内存和磁盘空间的数量），请确保符合下面的规范，从而保证最佳性能。

VM 系列防火墙有下列要求：

- 主机 CPU 必须为带有虚拟化扩展的 X86 Intel 或 AMD CPU。
- 有关 ESXi 的支持版本，请参阅兼容性矩阵。对 vmx 版本的支持基于用于部署 VM 系列防火墙的 OVA，并且无法修改此版本。升级或降级 VM 系列软件版本不会更改启动时启用的 vmx 版本。
- 有关 VM 系列型号的最低硬件要求，请参阅 VM 系列系统要求。
- 至少要有两个网络接口 (vNIC)。一个是用于管理接口的专用 vNIC，另一个用于数据接口。您随后可以为数据流量最多添加八个额外的 vNIC。对于其他接口，应在 ESXi 服务器上使用 VLAN 来宾标记 (VGT) 或在防火墙上配置子接口。

  虚拟机监控程序分配的 MAC 地址默认情况下处于启用状态。vSphere 为 VM 系列防火墙的每个数据平面接口分配唯一的 vNIC MAC 地址。如果禁用虚拟机监控程序分配的 MAC 地址，则 VM 系列防火墙会从其自己的池中为每个接口分配一个 MAC 地址。因为这会导致每个接口上的 MAC 地址不同，因此，您必须在防火墙数据面板接口附加的虚拟交换机端口组上启用混杂模式，从而允许防火墙接收帧（请参阅 在 ESXi 服务器上设置 VM 系列防火墙）。如果既未启用混杂模式，也未启用虚拟机监控程序分配的 MAC 地址，则防火墙将不会收到任何流量。这是因为当帧的目标 MAC 地址和 vNIC MAC 地址不匹配时，vSphere 无法将帧转发至虚拟机。
- ESXi 上的 VM 系列防火墙上默认启用数据平面开发套件 (DPDK)。有关 DPDK 的更多信息，请参阅在 ESXi 上启用 DPDK。

©2024 Palo Alto Networks, Inc.

- 为了实现 VM 系列防火墙的最佳性能，您可以在部署 VM 系列防火墙之前对主机进行以下调整。请参阅适用于 ESXi 的 VM 系列的性能调整了解更多信息。
  - 启用 **DPDK**。DPDK 允许主机绕过 Linux 内核来更快地处理数据包。相反，使用驱动程序和 DPDK 库执行与 NIC 的交互。
  - 启用 **SR-IOV**。单根 I/O 虚拟化 (SR-IOV) 允许单个根端口下的单个 PCIe 物理设备看起来像是虚拟机监控程序或来宾的多个单独的物理设备。

    请勿在启用 SR-IOV 的物理端口上配置 vSwitch。要与网络上的主机或其他虚拟机进行通信，VM 系列防火墙必须能够独占访问此接口上的物理端口和关联的虚拟功能 (VF)。
  - 启用 **NIC** 的多队列支持。多队列允许网络性能随着 vCPU 的数量而扩展，并通过创建多个 TX 和 RX 队列允许并行数据包处理。

ESXi 系统上 VM 系列的限制

VM 系列防火墙的功能和 Palo Alto Networks 硬件防火墙功能非常类似，但是有以下限制：

- 切勿在 ESXi 的 VM 系列上使用 VMware 快照功能。快照功能可能对性能造成影响，进而导致间歇性、不一致的数据包丢失。请参阅使用快照功能的 VMware 最佳方案推荐。

  如果需要配置备份，则使用 Panorama 或使用防火墙上的 **Export named configuration snapshot**（导出已命名的配置快照）（Device（设备）> Set up（设置）> Operations（操作））。使用 **Export named configuration snapshot**（导出已命名的配置快照）导出防火墙的活动配置 (`running-config.xml`)，并允许将其保存在任何网络位置。
- 推荐专用的 CPU 核心。
- ESXi 上的 VM 系列防火墙不支持高可用性 (HA) 链接监控。使用路径监控来验证至目标 IP 地址或下个中继段 IP 地址的连接性。
- 总共可以配置最多 10 个端口；这是 VMware 限制。其中一个端口用于管理流量，最多 9 个端口可用于数据流量。
- 仅支持 vmxnet3 驱动程序。
- 不支持虚拟系统。
- 如果 ESXi 主机具有同构 CPU 配置，则在 6.5、6.7 和 7.0 上支持 VM 系列防火墙的 vMotion。要在 vSphere 6.5 或 6.7 上安装 使用 vMotion 在主机之间移动 VM 系列防火墙，您需要 PAN-OS 9.1.6 及更高版本。
- 必须在连接到 VM 系列防火墙上的第 2 层和 vwire 接口的 ESXi vSwitch 端口组上启用伪造传输和混杂模式。
- 要在 ESXi 上将 PCI 设备与 VM 系列防火墙配合使用，映射 I/O (MMIO) 的内存必须低于 4GB。您可以在服务器的 BIOS 中禁用 4GB 以上的 MMIO。这是 ESXi 限制。
- 如果使用 ESXi 7.0，则在将 VF 附加到具有 PCI 设备直通功能的虚拟机时不显示接口。

©2024 Palo Alto Networks, Inc.

在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙

要安装 VM 系列防火墙，您必须拥有开放式虚拟化联盟 (OVA) 格式模板的访问权。使用在订单履行电子邮件中收到的授权代码注册您的 VM 系列防火墙，并下载 OVA 模板。OVA 模板是一个包含三种文件类型的 zip 压缩文件：

- .mf:包含数据包中各个文件的 SHA-1 摘要的 OVF 清单文件
- .ovf:包含数据包及其内容的所有元数据的 OVF 描述符文件
- .vmdk:包含防火墙虚拟化版本的磁盘映像文件

完成以下任务以在 ESXi 上安装和配置 VM 系列防火墙。

- 规划适用于ESXi的 VM 系列的接口
- 在 ESXi 服务器上设置 VM 系列防火墙
- 在 ESXi 上对 VM 系列防火墙执行初始配置
- （可选）添加额外的磁盘空间至 VM 系列防火墙
- 通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具
- 使用 vMotion 在主机之间移动 VM 系列防火墙
- 使用 VM 系列 CLI 在 ESXi 上交换管理接口

规划适用于ESXi的 VM 系列的接口

通过规划 VM 系列防火墙vNIC和接口的映射，可以避免重新启动和配置问题。下表介绍了在ESXi上启用全部10个vNIC时，VMware vNIC和 VM 系列接口之间的默认映射。

VMware vNIC	VM 系列接口
1	Ethernet 1/0 (mgmt)
2	Ethernet 1/1 (eth1)
3	Ethernet 1/2 (eth2)
4	Ethernet 1/3 (eth3)
5	Ethernet 1/4 (eth4)
6	Ethernet 1/5 (eth5)
7	Ethernet 1/6 (eth6)

©2024 Palo Alto Networks, Inc.

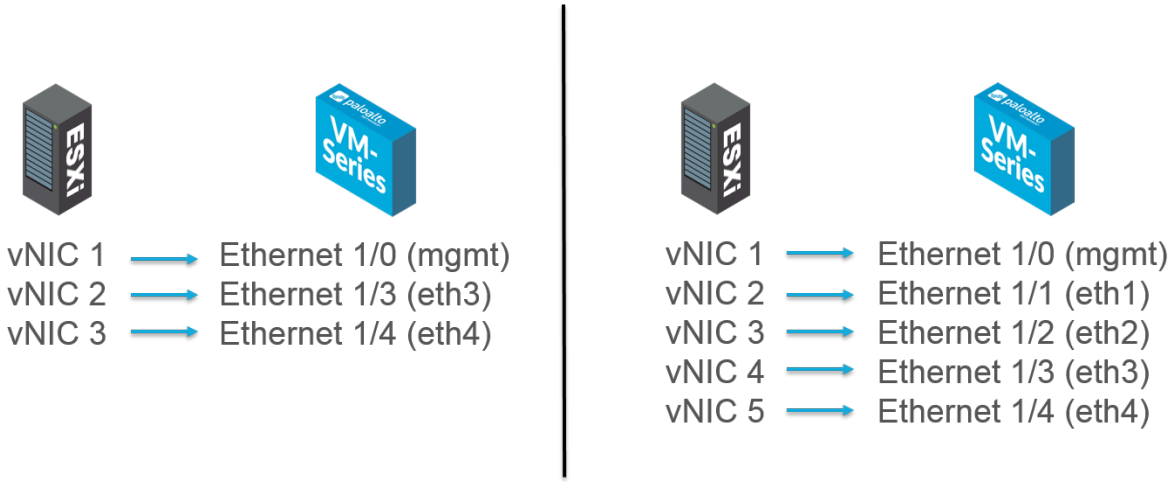
VMware vNIC	VM 系列接口
8	Ethernet 1/7 (eth7)
9	Ethernet 1/8 (eth8)
10	Ethernet 1/9 (eth9)

无论您在ESXi上添加哪个vNIC， VM 系列防火墙上的映射都保持不变。您在防火墙上激活的接口将始终占用 ESXi 上的下一个可用 vNIC。

在下图中，VM 系列防火墙上的 eth3 和 eth4 分别与 ESXi 上的 vNIC 2 和 3 配对，且未映射 eth1 和 eth2，如左图所示。

如果要在保留当前映射时添加两个额外的接口，请激活 vNICs 4 和 5，并重新启动防火墙。因为接口在最后映射接口之后添加，因此将保留现有 vNIC 映射。

如果激活 VM 系列防火墙上的 eth1 和 eth2，接口将会重新排序（如右图所示），从而导致映射不匹配，进而影响流量。



要避免前面示例中描述的问题，您可以执行以下操作：

- 首次配置 ESXi 主机时，激活第一个之外的所有九个 vNIC。在启动 VM 系列防火墙之前，将所有 9 个 vNIC 添加为占位符，可让您使用任何 VM 系列接口，而不管其顺序如何。
- 如果激活所有 vNIC，添加额外接口将无须重新启动。由于 ESXi 上每个 vNIC 都要求您选择一个网络，因此可以将空端口组创建为网络占位符。
- 请勿移除 VM 系列防火墙 vNIC 以避免映射不匹配。

在 ESXi 服务器上设置 VM 系列防火墙

使用这些说明在（独立）ESXi 服务器上部署 VM 系列防火墙。有关部署 VM 系列 NSX 版防火墙，请参阅在 VMware NSX-T 上设置 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | 下载 OVA 文件。

注册您的 VM 系列防火墙，并从 Palo Alto Networks 客户支持网站上获得 OVA 文件。

此 *OVA* 文件包含基本安装。完成基本安装后，您必须从支持门户下载最新 *PAN-OS* 版本并安装。这样可确保您在创建基本映像后拥有已实施的最新修补程序。有关说明，请参阅升级 PAN-OS 软件版本（独立版本）。

STEP 2 | 在部署 OVA 文件前，设置 VM 系列防火墙所需的标准虚拟交换机或分布式虚拟交换机。

如果您正在使用第 *3* 层接口部署 *VM* 系列防火墙，则防火墙默认使用虚拟机监控程序分配的 MAC 地址 默认。如果选择禁用虚拟机监控程序分配的 *MAC* 地址，或是如果真通过第 *2* 层、虚拟线路或旁接接口部署防火墙，则必须配置（设置为 ***Accept***（接受））附加到 *VM* 系列防火墙的任何虚拟交换机，以便运行下列模式：混杂模式、*MAC* 地址更改和伪造传输。

配置标准虚拟交换机或分布式虚拟交换机以接收 VM 系列防火墙的帧。

标准虚拟交换机

1. 导航至 **Home**（主页）> **Hosts and Clusters**（主机和集群），然后选择主机。
2. 单击 **Configure**（配置）选项卡并查看 **Virtual Switches**（虚拟交换机）。对于每个 VM 系列防火墙附加的虚拟交换机，单击 **Properties**（属性）。
3. 突出显示与虚拟交换机对应的端口组，并单击 **Edit Settings**（编辑设置）。在 vSwitch 属性中，单击 **Security**（安全）选项卡，并将 **Promiscuous Mode**（混杂模式）、**MAC Address Changes**（**MAC** 地址更改）和 **Forged Transmits**（伪造传输）设置为 **Accept**（接受），然后单击 **OK**（确定）。此更改将传播到虚拟交换机上的所有端口组。

分布式虚拟交换机

1. 选择 **Home**（主页）> **Networking**（网络）。选择分布式虚拟交换机，并突出显示想要编辑的 **Distributed Port Group**（分布式端口组）。
2. 单击 **Edit Settings**（编辑设置），选择 **Policies**（策略）> **Security**（安全），然后将 **Promiscuous Mode**（混杂模式）、**MAC Address Changes**（**MAC** 地址更改）和 **Forged Transmits**（伪造传输）设置为 **Accept**（接受），并单击 **OK**（确定）。

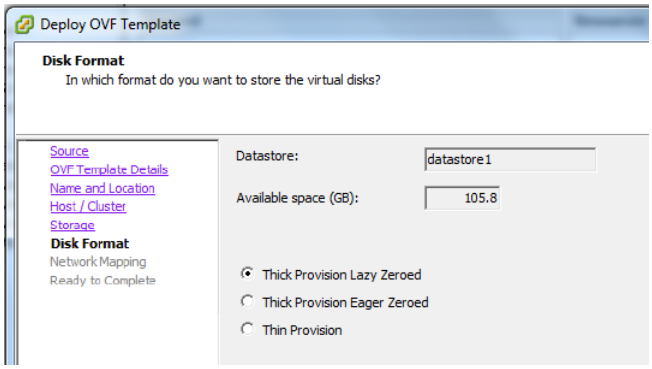
©2024 Palo Alto Networks, Inc.

STEP 3 | 部署 OVA。

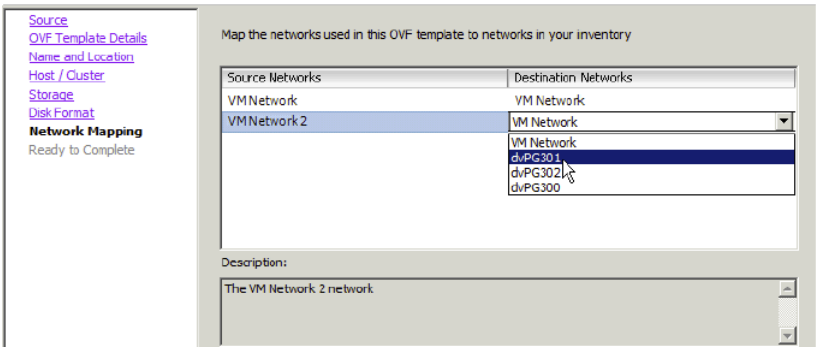
如果将其他接口 *(vNIC)* 添加到 *VM* 系列防火墙，必须重新启动防火墙，因为在启动时检测到新接口。要减少重新启动防火墙的需要，请在初始部署或维护窗口期间激活接口。

要查看安装进度，请监控 ***Recent Tasks***（最近的任务）列表。

1. 使用 vSphere Client 登录 vCenter。如有需要，还可以直接转到目标 ESXi 主机。
2. 从 vSphere Web 客户端转至 **Hosts and Clusters**（主机和集群），右键单击您的主机，然后选择 **Deploy OVF Template**（部署 **OVF** 模板）。
3. 浏览到您之前下载的 OVA 文件。选择文件，然后单击 **Next**（下一步）。查看模板详细信息，然后再次单击 **Next**（下一步）。
4. 命名 VM 系列防火墙实例，并在 **Inventory Location**（目录位置）窗口中选择数据中心和文件夹，然后单击 **Next**（下一步）
5. 选择 VM 系列防火墙的 ESXi 主机，然后单击 **Next**（下一步）。
6. 选择用于 VM 系列防火墙的数据存储，然后单击 **Next**（下一步）。
7. 保留数据存储设置的默认设置，然后单击 **Next**（下一步）。默认设置是 **Thick Provision Lazy Zeroed**。

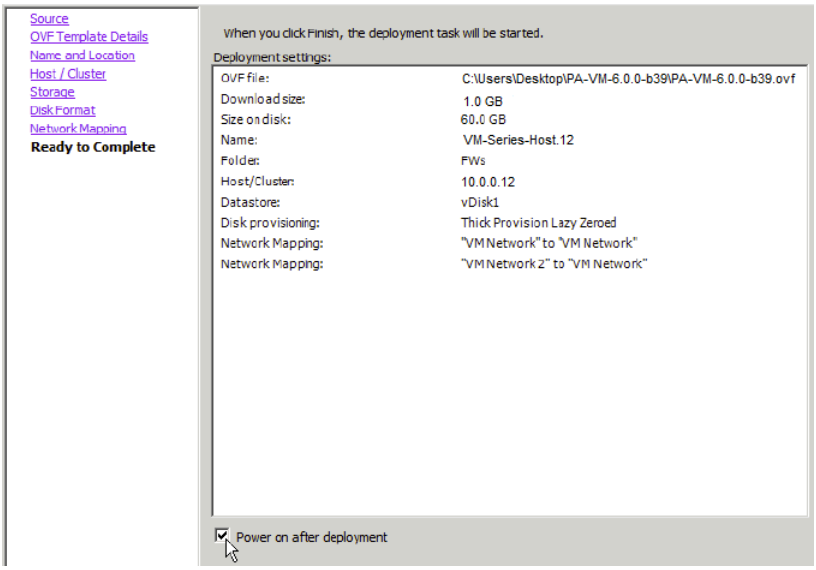


8. 选择用于两个初始 vNIC 的网络。第一个 vNIC 用于管理接口，第二个 vNIC 用于首个数据端口。请确保 **Source Networks**（源网络）映射到正确的 **Destination Networks**（目标网络）。



 ©2024 Palo Alto Networks, Inc.

9. 查看详细信息，选中 **Power on after deployment**（部署后开机），然后单击 **Next**（下一步）。



10. 完成部署后，单击 **Summary**（摘要）选项卡查看当前状态。

在 ESXi 上对 VM 系列防火墙执行初始配置

使用 ESXi 服务器上的虚拟设备控制台设置对 VM 系列防火墙的网络访问权限。默认情况下，VM 系列防火墙使用 DHCP 获取管理接口的 IP 地址，但是，您还可以分配静态 IP 地址。完成初始配置后，访问 Web 界面以完成进一步的配置任务。如果让 Panorama 进行集中管理，有关使用 Panorama 管理设备的信息，请参阅《Panorama 管理员指南》。

如果您正在使用引导来执行 ESXi 上 VM 系列防火墙的配置，请参阅在 ESXi 上引导 VM 系列防火墙。

有关引导的一般信息，请参阅引导 VM 系列防火墙。

STEP 1 | 从网络管理员处收集必要的信息。

- MGT 端口的 IP 地址
- 子网掩码
- 默认网关
- DNS 服务器 IP 地址

STEP 2 | 访问 VM 系列防火墙的控制台。

1. 在此 VM 系列防火墙的 ESXi 服务器上，选择 **Console**（控制台）选项卡，或右键单击此 VM 系列防火墙并选择 **Open Console**（打开控制台）。
2. 按 Enter 键访问登录屏幕。
3. 输入登录的默认用户名/密码 (admin/admin)。
4. 输入 **`configure`**（配置）以切换到“Configuration（配置）”模式。

©2024 Palo Alto Networks, Inc.

STEP 3 | 配置管理接口的网络访问设置。

输入以下命令：

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> 网络掩码 <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | 提交您所做的更改，并退出配置模式。

输入 **commit**。

输入 **exit**。

STEP 5 | 验证防火墙管理所需外部服务（例如 Palo Alto Networks 更新服务器）的网络访问权限。

1. 使用 ping 实用程序验证是否能联网到 Palo Alto Networks 更新服务器，如以下示例所示。验证是否发生 DNS 解析，响应中是否包含更新服务器的 IP 地址（更新服务器不响应 ping 请求）。 验证 DNS 解析后，按 Ctrl+C 键以停止 ping 请求。

   ```
   admin@PA-220 > ping host updates.paloaltonetworks.com
   ```

   ```
   PING updates.paloaltonetworks.com (10.101.16.13) 56(84)
    bytes of data.From 192.168.1.1 icmp_seq=1 Destination Host
    Unreachable From 192.168.1.1 icmp_seq=2 Destination Host
    Unreachable From 192.168.1.1 icmp_seq=3 Destination Host
    Unreachable From 192.168.1.1 icmp_seq=4 Destination Host
    Unreachable
   ```

2. 使用以下 CLI 命令从 Palo Alto Networks 更新服务器检索关于防火墙支持授权的信息：请求支持检查，如果网络畅通，则更新服务器响应防火墙的支持状态。

STEP 6 | 在开始测试 VM 系列防火墙之前，应用容量授权代码并检索许可证。

未经许可的 VM 系列防火墙最多可以处理约 1230 个并发会话。根据环境，可能很快就会达到会话限制，从而导致不可预测的结果。

添加额外磁盘空间至 VM 系列防火墙

默认情况下，VM 系列防火墙需要 60GB 的虚拟磁盘，其中 21GB 用于日志记录。

- 对于大型部署，使用 Panorama 汇总来自所有下一代防火墙的数据并监控网络上的所有通信。Panorama 提供集中式日志记录和报告。

©2024 Palo Alto Networks, Inc.

- 在无需使用 Panorama 的小型部署中，您可以添加新的虚拟磁盘，以增加日志存储容量。新的虚拟磁盘可以支持 60GB 至 2TB 的日志存储容量。此任务如下所述。

  当配置虚拟设备以使用虚拟磁盘时，*VM* 系列防火墙不再存储日志。如果设备丢失与虚拟磁盘的连接，日志可能会于故障存在期间丢失。必要时，请在提供 *RAID* 冗余的数据存储上放置新创建的虚拟磁盘。*RAID10* 为具有大量日志记录特性的设备提供了最佳写入性能。

STEP 1 | 关闭 VM 系列防火墙。

STEP 2 | 在 ESXi 服务器上，将虚拟磁盘添加至防火墙。

1. 在 ESXi 服务器上选择 VM 系列防火墙。
2. 单击 **Edit Settings**（编辑设置）。
3. 单击 **Add**（添加）启动“添加硬件”向导，并在弹出时选择以下选项：
   1. 对于硬件类型，请选择 **Hard Disk**（硬盘）。
   2. 选择 **Create a new virtual disk**（新建虚拟磁盘）。
   3. 选择 **SCSI** 作为虚拟磁盘类型。
   4. 选择 **Thick provisioning**（密集配置）磁盘格式。
   5. 在位置字段中，选择 **Store with the virtual machine option**（使用虚拟机选项存储）。数据存储不必位于 ESXi 服务器上。
   6. 验证设置是否正确，并单击 **Finish**（完成）退出向导。新磁盘随后将添加到虚拟机设备列表中。

STEP 3 | 启动防火墙。

首次使用时，启动防火墙会初始化虚拟磁盘。完成初始化流程所需的时间随着新虚拟磁盘的大小不同而不同。

新虚拟磁盘被初始化并准备好后，PAN-OS 将会把所有来自现有磁盘的日志移至新虚拟磁盘。随即，新日志条目将会被写入此新虚拟磁盘。

PAN-OS 还会生成记录新磁盘的系统日志条目。

如果您重新使用之前用于存储 *PAN-OS* 日志的虚拟磁盘，那么所有来自现有磁盘的日志均被覆盖。

STEP 4 | 验证新虚拟磁盘的大小。

1. 选择 **Device**（设备） > **Setup**（设置） > **Management**（管理）。
2. 在“记录和报告设置”部分，验证 **Log Storage**（日志存储）容量是否正确显示新的磁盘容量。

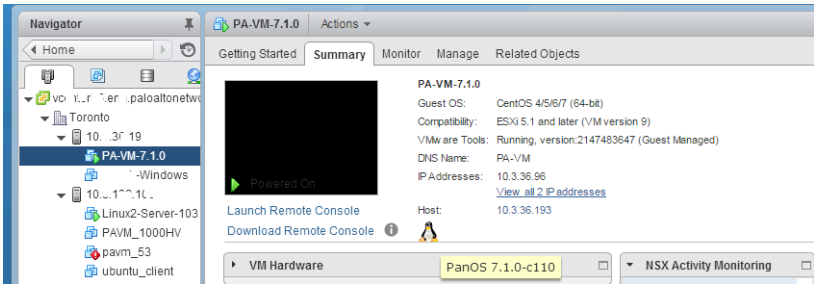
©2024 Palo Alto Networks, Inc.

通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具

VMware 工具使用程序从 vCenter 服务器和 vCloud Director 改进 VM 系列防火墙的管理。VMware 与 VM 系列防火墙的软件映射绑定在一起，所有更新均通过新的 OVF 映像提供。您无法使用 vCenter 服务器或 vCloud Director 安装或更新 VMware 工具。

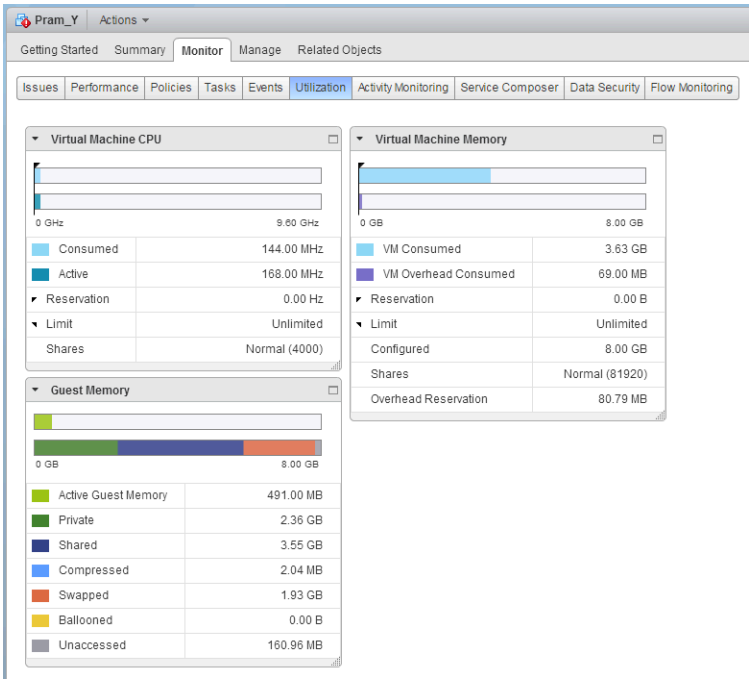
查看管理接口上的 IP 地址以及防火墙和 Panorama 上的软件版本。

在 vCenter 服务器上的 Hosts and Cluster（主机和集群）部分，选择防火墙或 Panorama 并在 **Summary**（摘要）选项卡上查看分配至管理接口的 IP 地址以及当前所安装的软件版本的信息。



查看硬盘、内存和 CPU 的资源利用指标。使用这些指标启用 vCenter 服务器上的警报。

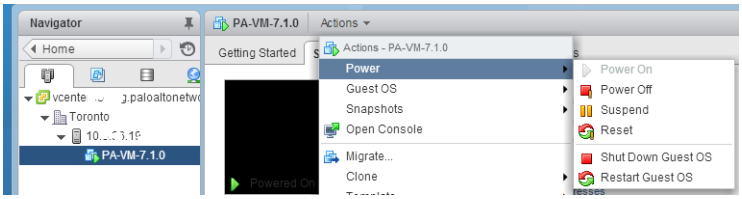
在 vCenter 服务器上的 Hosts and Cluster（主机和集群）部分，选择防火墙或 Panorama 并在 **Monitor**（监控） > **Utilization**（利用）选项卡上查看硬盘、内存和 CPU 使用情况的信息。



 ©2024 Palo Alto Networks, Inc.

关闭或重启 vCenter 服务器上的防火墙和 Panorama。

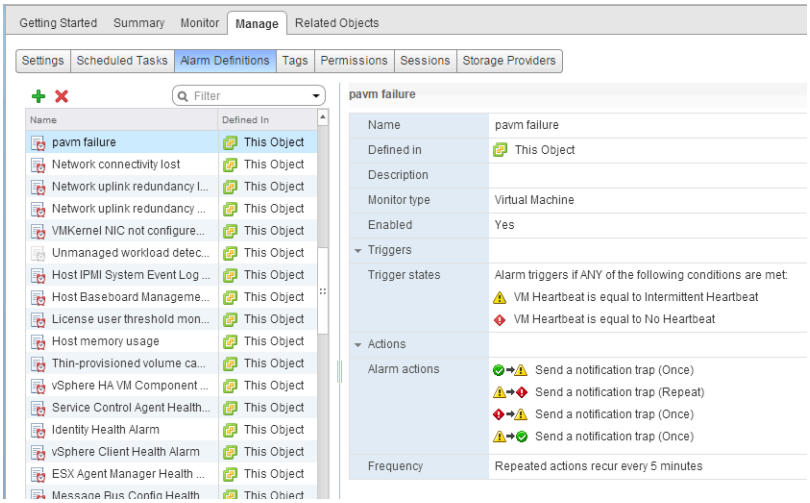
在 vCenter 服务器上的 Hosts and Cluster（主机和集群）部分，选择防火墙或 Panorama 并选择 **Actions**（操作） > **Power**（电源）下拉列表。



创建您希望获得通知的事件的警报定义，或创建您希望为其指定自动操作的事件的警报定义。

有关创建警报定义的详细信息，请参阅 VMware 文档。

在 vCenter 服务器上的 Hosts and Cluster（主机和集群）部分，选择防火墙或 Panorama 并选择 **Manage**（管理） > **Alarm Definitions**（警报定义），以添加一个新的触发器，并指定达到某个阈值时进行的操作。例如：当在指定持续时间内检测信号丢失时，或者内存资源使用率超过阈值时。以下屏幕快照所示即为如何使用通知实现防火墙或 Panorama 上的检测信号监控。



使用 vMotion 在主机之间移动 VM 系列防火墙

要在使用 vMotion 在 VMware ESXi 上具有同构 CPU 配置的 ESXi 主机之间移动 VM 系列防火墙时保持流量，必须在 vMotion 期间使用 PAN-OS CLI 暂停 VM 系列防火墙的内部检测信号监控。您可以指定暂停检测信号监控的时间（以分钟为单位）。最多可以将检测信号监控暂停 60 分钟。当暂停间隔结束或您故意结束暂停间隔，则检测信号监控将恢复。

如果 ESXi 主机具有同构 CPU 配置，则在 6.5、6.7 和 7.0 上支持 VM 系列防火墙的 vMotion。

如果运行 *vSphere 7.0* 或更高版本，则在使用 *vMotion* 时不需要运行这些命令。

STEP 1 | 登录到 VM 系列防火墙 CLI。

©2024 Palo Alto Networks, Inc.

STEP 2 | 使用以下命令设置检测信号监控暂停间隔。一旦执行命令，暂停就开始。如果 vMotion 所用时间比预期更长，则可以重新运行此命令以设置一个更长的新间隔，该间隔从再次执行命令时开始。

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

您可以使用以下命令查看暂停间隔中的剩余时间。

```
request system heartbeat-pause show interval
```

STEP 3 | （可选）如果在暂停间隔过去之前完成 vMotion，则可以通过将间隔设置为零 (0) 以结束暂停。

```
request system heartbeat-pause set interval 0
```

使用 VM 系列 CLI 在 ESXi 上交换管理接口

默认情况下，VM 系列防火墙分配第一个接口 (eth0) 作为管理接口。但是，在某些部署中，必须将第一个接口预映射到公共 IP 地址。因此，必须将管理接口分配给不同的接口。将公共 IP 地址分配给管理接口存在安全风险。

此过程需要 VM 系列插件 2.0.7 或更高版本。

或者，作为 init-cfg.txt 文件组件的一部分，您可以在引导时启用管理接口交换。

STEP 1 | 登录到 VM 系列防火墙 CLI，然后输入以下命令：

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | 确认希望交换接口，然后将 eth1 数据面板接口用作管理接口。

STEP 3 | 重启防火墙，以使交换操作成效。使用以下命令：

```
request restart system
```

STEP 4 | 验证接口交换已完成。使用以下命令：

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```


©2024 Palo Alto Networks, Inc.

vCenter 上的 VM 监控

安装并配置 VMware vCenter 的 Panorama 插件，以检索 vCenter 环境中来宾的 IP 地址，并使用该信息来构建使用动态地址组的策略。

适用于 *VMware vCenter* 的 *Panorama* 插件不支持代理服务器。

- 关于 VMware vCenter上的 VM 监控
- 安装适用于 VMware vCenter 的 Panorama 插件
- 为 VMware vCenter 配置 Panorama 插件

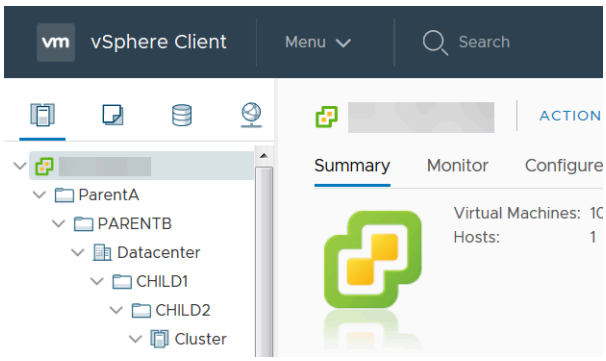
关于 VMware vCenter上的 VM 监控

适用于 VMware vCenter 的 Panorama 插件提供了使用动态地址组为您的 vCenter 环境构建策略的工具。动态地址组允许您创建自动适应环境变化的策略，例如添加或删除来宾虚拟机。VMware vCenter 插件监控 vCenter 环境中的更改，并与 Panorama 共享信息。

该插件处理从 vCenter 接收的信息，并将其转换为 Panorama 上的一组标记，您可以将其用作匹配条件，以便为动态地址组分配 IP 地址。每个标记都有前缀，用于说明虚拟机上方的层次结构。

在本例中，Panorama 中的每个标记均以如下所示的前缀开头。每个标记都包括 vCenter 名称、数据中心名称和集群名称；如果 vCenter 层次结构中有文件夹，则标记将包括文件夹名称。标记中对象的顺序与 vCenter 层次结构中的顺序匹配。

vcenter.<vcenter-name>_ParentA_ParentB_Datacenter_CHILD1_CHILD2_Cluster_<tag>



适用于 *VMware vCenter* 的 *Panorama* 插件不支持与 *vApp* 和资源池关联的标记。

标签以下面的格式显示在 Panorama 中：

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vmname.<vm-name>**— 此标记根据 VM 名称映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_guestos.<guest-os>**— 此标记根据来宾操作系统映射虚拟机 IP 地址。

©2024 Palo Alto Networks, Inc.

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_annotation.<annotation>**— 此标记根据注释映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vlanId.<vlan-ID>**— 此标记根据 VLAN ID 映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_host-ip.<host-ip>**— 此标记根据主机 IP 地址映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_<tag-category>.<user-defined-tag>**— 此标记根据在 vCenter 中创建的用户定义的标记映射虚拟机 IP 地址。

> 该插件每个 *VM* 最多支持 *16* 个用户定义的标记。超出 *16* 的任何用户定义标签都不会被处理。

vCenter 的 Panorama 插件无法处理长度超过 128 个字符的标记；这包括字母，数字和特殊字符。vCenter 对象名称中的空格将替换为正斜杠。此外，Panorama 在 vCenter VM 名称和注释中不支持非 ASCII 特殊字符或以下特殊字符 — ’ **<>&**”。Panorama 会删除包含不支持字符的标记。

要检索端点 IP 地址到标记映射信息，必须为虚拟环境中的每个 vCenter 配置监控定义。监控定义指定允许 Panorama 连接到 vCenter 的用户名和密码。它还指定了包含 Panorama 推送标记的防火墙的设备组和相应的通知组。配置监控定义并且 VM ware vCenter 的 Panorama 插件检索标记后，您可以创建 DAG 并将标记添加为匹配条件。

安装适用于 VMware vCenter 的 Panorama 插件

要开始监控 vCenter 上的端点，请下载并安装适用于 VMware vCenter 的 Panorama 插件。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 HA 对中的 Panorama 上安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

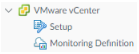
©2024 Palo Alto Networks, Inc.

STEP 1 | 选择 **Panorama** > **Plugins**（插件）。

STEP 2 | 选择 **Upload**（上传）并单击 **Browse**（浏览）以找到插件文件。

STEP 3 | 单击 **OK**（确定）以完成上传。

STEP 4 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。



为 VMware vCenter 配置 Panorama 插件

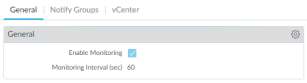
安装插件后，请完成以下过程以在 Panorama 和 vCenter 之间建立连接。

对于在 vCenter 环境中监控虚拟机的插件，您必须已安装 VMware 工具。在 vCenter 中，VM 的 IP 地址不可从外部检索；它们只能通过 VMware 工具查看。此外，插件需要本机只读权限才能从 vCenter 检索 IP 地址信息。

STEP 1 | 登录到 Panorama Web 界面。

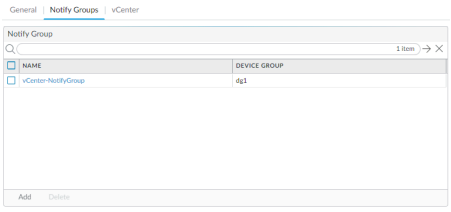
STEP 2 | 启用监控并设置监控间隔。

1. 选择 **Panorama** > **VMware vCenter** > **Setup**（设置） > **General**（常规）。
2. 选择 **Enable Monitoring**（启用监控）。这样即可监控部署中的所有 vCenter。
3. 以秒为单位设置 **Monitoring Interval**（监控间隔）。监控间隔是 Panorama 从 vCenter 检索更新的网络信息的频率。默认值为 60 秒，范围为 60 至 84600 秒。



STEP 3 | 创建通知组。

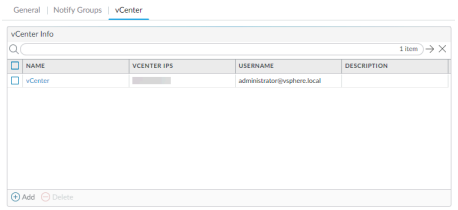
1. 选择 **Panorama** > **VMware vCenter** > **Setup**（设置） > **Notify Groups**（通知组）。
2. 单击 **Add**（添加）。
3. 输入通知组的描述性 **Name**（名称）。
4. 在 vCenter 部署中选择设备组。



©2024 Palo Alto Networks, Inc.

STEP 4 | 添加 vCenter 信息。适用于 VMware vCenter 的 Panorama 插件最多支持 16 个 vCenter 实例。

1. 选择 **Panorama** > **VMware vCenter** > **Setup**（设置） > **vCenter**。
2. 输入 vCenter 的描述性 **Name**（名称）。
3. 输入 vCenter 和端口的 IP 地址或 FQDN（如果适用）。
4. 输入 vCenter 用户名。
5. 输入并确认 vCenter 密码。
6. 单击 **Validate**（验证）以确认 Panorama 可以使用您输入的登录凭据连接到 vCenter。
7. 单击 **OK**（确定）。



STEP 5 | 最多配置 16 个监控定义。

只能将一个 *vCenter* 实例分配给一个 *Monitoring Definition*（监控定义）。

1. 选择 **Panorama** > **VMware vCenter** > **Monitoring Definition**（监控定义），然后单击 **Add**（添加）。
2. 输入用于标识使用此定义的 vCenter 的描述性 **Name**（名称），也可选择输入说明。
3. 选择 **vCenter** 和 **Notify Group**（通知组）。
4. 单击 **OK**（确定）。



STEP 6 | **Commit**（提交）更改。

STEP 7 | 验证是否可以在 Panorama 上查看 VM 信息，并定义动态地址组的匹配条件。

在匹配条件中使用多个标记时，您必须使用 *OR* 运算符；使用 *AND* 运算符无效。

某些浏览器扩展程序可能会阻止 *Panorama* 与 *vCenter* 之间的 *API* 调用，从而阻止 *Panorama* 接收匹配条件。如果 *Panorama* 未显示匹配条件且您正在使用浏览器扩展程序，请禁用扩展程序和同步动态对象以填充 *Panorama* 可用的标记。

©2024 Palo Alto Networks, Inc.

STEP 8 | 验证 VM 中的地址是否已添加到 DAG。

1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
2. 在 DAG 的地址列中单击 **More**（更多）。

   Panorama 根据指定的匹配条件显示添加到 DAG 的 IP 地址列表。

STEP 9 | 在策略中使用动态地址组。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），然后为策略输入 **Name**（名称）和 **Description**（说明）。
3. 添加 **Sources Zone**（源区域）来指定产生流量的区域。
4. 添加流量于其中终止的 **Destination Zone**（目标区域）。
5. 对于 **Destination Address**（目标地址），选择刚创建的动态地址组。
6. 为流量指定操作 — **Allow**（允许）或 **Deny**（拒绝），并可选地将默认安全配置文件附加至规则。
7. 重复步骤 1 至 6 来创建另一个策略规则。
8. 单击 **Commit**（提交）。

STEP 10 | 您可以通过同步动态对象随时从 vCenter 更新动态对象。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启用应用程序。

1. 选择 **Panorama** > **VMware vCenter** > **Monitoring Definition**（监控定义）。
2. 单击 **Synchronize Dynamic Objects**（同步动态对象）。

STEP 11 | 如果 vCenter 部署中的防火墙重新启动或与 Panorama 断开连接，则防火墙与适用于 vCenter 的 Panorama 插件不同步，也不会接收更新。防火墙重新连接 Panorama 后，您必须手动同步 Panorama 和防火墙。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令。

   ```
   admin@Panorama> request plugins vmware_vcenter sync
   ```


©2024 Palo Alto Networks, Inc.

排除 ESXi 部署的故障

VM 系列防火墙的许多故障排除步骤和 PAN-OS 硬件版本的故障排除步骤非常相似。出现问题时，您应检查接口计数器和系统日志文件，同时，如有必要，请使用调试程序创建捕获。

以下各节介绍如何排除某些常见问题：

- 基本故障排除
- 安装问题
- 许可问题
- 连接问题

基本故障排除



有关网络故障排除工具的建议

让独立的故障排除工作站在虚拟化环境中捕获流量或提供测试数据包很有用。通过从头开始构建安装了通用故障排除工具的全新操作系统可提供帮助，这些工具包括 *tcpdump*、*nmap*、*hping*、*traceroute*、*iperf*、*tcpedit*、*netcat* 等。随后可以关闭此机器，并将其转变为模板。每次需要这些工具时，可以将此故障排除客户端（虚拟机）快速部署到相关虚拟交换机，并使用它隔离网络问题。在测试完成后，可以简单丢弃此实例，在下次需要时，可再次使用此模板。

有关防火墙的相关性能问题，请先检查防火墙 Web 界面中的仪表盘。要查看警报或者创建技术支持或统计转储文件，请导航到**Device**（设备）> **Support**（支持）。

有关 vSphere 客户端中的信息，请转到 **Home**（主页）> **Inventory**（目录）> **VMs and Templates**（**VM** 和模板），选择 VM 系列防火墙示实例，然后单击 **Summary**（摘要）选项卡。在 **Resources**（资源）下，检查所用的内存、CPU 和存储空间的统计信息。有关资源历史记录，请单击 **Performance**（性能）选项卡，然后监控一定时间内的资源消耗。

安装问题

- 部署 OVA 的相关问题
- 防火墙为什么会引导至维护模式？
- 如何修改 VM-1000-HV 许可证的基本映像文件？

部署 **OVA** 的相关问题

- VM 系列防火墙以 zip 压缩文件的方式交付，其格式为开放式虚拟化联盟 (OVA) 格式，可扩展为三个文件。

  如果您在部署 OVA 映像时遇到问题，必须对三个文件实施解压缩，并可以进行访问。必要时，再次下载并压缩 OVA 映像。

©2024 Palo Alto Networks, Inc.

- OVA 映像中的虚拟磁盘约 1GB。必须出现在运行 vSphere 客户端的计算机上，或是必须可作为 OVA 映像的 URL 进行访问。
  - 请确保 vSphere 客户端计算机和目标 ESXi 主机之间的网络连接延迟低，且带宽充足。如果连接不佳，OVA 部署可能需要数小时才能完成，或者会出现超时和失败。

    如果将映像托管在与 ESXi 主机的同一网络中的设备上，则可以最大限度地减少此问题。
  - 此路径中的任何防火墙均允许从 vSphere 客户端到 ESXi 主机的 TCP 端口 902 和 443。
- ESX 6.5.0a 内置 4887370 将每个插槽限制为 2 CPU 内核。如果部署 VM-300、VM-500 或 VM-700 到您想要为每个插槽分配大于 2 个的 vCPU，请参阅 VMware KB: https://kb.vmware.com/s/article/53354 寻求解决方法。

防火墙为什么会引导至维护模式？

如果已购买 VM-1000-HV 许可证，并在独立模式下在 VMware ESXi 服务器上部署 VM 系列防火墙，则必须向 VM 系列型号分配符合最低要求的内存。

要避免在维护模式下引导，必须修改基本映像文件（请参阅如何修改 VM-1000-HV 许可证的基本映像文件？），或者在启动 VM 系列防火墙以前编辑 ESXi 主机或 vCenter 服务器上的设置 。

此外，验证接口是否为 VMXnet3。将接口类型设置为任何其他格式会导致防火墙启动进入维护模式。

如何修改 **VM-1000-HV** 许可证的基本映像文件？

如果已购买 VM-1000-HV 许可证，并在 VMware ESXi 服务器上独立模式下部署 VM 系列防火墙，可使用以下说明修改 VM 系列防火墙基本映像文件（.ova 或 .xva）中定义的以下属性。

重要信息：修改非下文列出的值会让基本映像文件失效。

STEP 1 | 使用文本编辑工具（例如记事本）打开基本映像文件，例如 7.0.0。

STEP 2 | 搜索 4096，并将分配的内存更改为 5012（即 5 GB），如下所示：

```
<Item> <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
 <rasd:Description>Memory Size</rasd:Description>
 <rasd:ElementName>4096MB of memory</rasd:ElementName>
 <rasd:InstanceID>2</rasd:InstanceID> <rasd:ResourceType>4</
rasd:ResourceType> <rasd:VirtualQuantity>4096</
rasd:VirtualQuantity> <Item> <rasd:AllocationUnits>byte
 * 2^20</rasd:AllocationUnits> <rasd:Description>Memory
 Size</rasd:Description> <rasd:ElementName>5120MB
 of memory</rasd:ElementName> <rasd:InstanceID>2</
rasd:InstanceID> <rasd:ResourceType>5</rasd:ResourceType>
 <rasd:VirtualQuantity>5120</rasd:VirtualQuantity>
```

STEP 3 | 根据部署需要将分配的虚拟 CPU 核心数量从 2 更改为 4 或 8：

```
<Item> <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
 <rasd:Description>Number of Virtual CPUs</rasd:Description>
```


©2024 Palo Alto Networks, Inc.

```
 <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
 <rasd:InstanceID>1</rasd:InstanceID> <rasd:ResourceType>3</
rasd:ResourceType> <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
 <vmw:CoresPerSocket ova:required="false">2</vmw:CoresPerSocket>
 </Item> <Item> <rasd:AllocationUnits>hertz * 10^6</
rasd:AllocationUnits> <rasd:Description>Number of Virtual
 CPUs</rasd:Description> <rasd:ElementName>4 virtual CPU(s)</
rasd:ElementName> <rasd:InstanceID>1</rasd:InstanceID>
 <rasd:ResourceType>3</rasd:ResourceType> <rasd:VirtualQuantity>4</
rasd:VirtualQuantity> <vmw:CoresPerSocket ova:required="false">2</
vmw:CoresPerSocket> </Item>
```

或者，您可以部署此防火墙，并在开启此 VM 系列防火墙之前，直接在 ESXi 主机或 vCenter 服务器上编辑内存和虚拟 CPU 分配。

许可问题

- 为什么我不能申请支持或功能许可证？
- 为什么我克隆的 VM 系列防火墙没有有效的许可证？
- 移动 VM 系列防火墙是否会导致许可证失效？

为什么我不能申请支持或功能许可证？

您是否已在 VM 系列防火墙上申请功能授权代码？在激活支持或功能许可证之前，必须申请功能授权代码，设备才能获取序列号。需要使用此序列号才能在 VM 系列防火墙上激活其他许可证。

为什么我克隆的 VM 系列防火墙没有有效的许可证？

VMware 会向每个虚拟机（包括 VM 系列防火墙）分配唯一的 UUID。因此，当克隆 VM 系列防火墙时，会将新 UUID 分配给它。由于 VM 系列防火墙每个实例的序列号和许可证均已与 UUID 绑定，因此克隆许可的 VM 系列防火墙将导致新防火墙的许可证无效。您将需要使用新的授权代码在新部署的防火墙上激活许可证。必须应用容量授权代码和新的支持许可证，才能在 VM 系列防火墙上获取完整的功能、支持和软件升级。

移动 VM 系列防火墙是否会导致许可证失效？

如果将 VM 系列防火墙从一个主机手动移动到其他主机，请确保选择 **This guest was moved**（此来宾已移动）选项以防止许可证失效。

连接问题

- 为什么 VM 系列防火墙未收到任何网络流量？

为什么 VM 系列防火墙未收到任何网络流量？

在 VM 系列防火墙上，检查流量日志（**Monitor**（监控）> **Logs**（日志））。如果日志为空，请使用以下 CLI 命令在 VM 系列防火墙的界面上查看数据包：

©2024 Palo Alto Networks, Inc.

```
show counter global filter delta yes Global
 counters:Elapsed time since last sampling:594.544 seconds
 ---------------------------------------------------------------------------
 Total counters shown:0
 ---------------------------------------------------------------------------
```

在 vSphere 环境中，检查以下问题：

- 检查端口组，并确认防火墙和虚拟机都在正确的端口组上

  确保正确映射以下接口。

  网络适配器 1 = 管理

  网络适配器 2 = Ethernet1/1

  网络适配器 3 = Ethernet1/2

  对每个虚拟机检查设置，以验证接口是否已映射到正确的端口组。

- 验证是对每个端口组还是对整个交换机启用混杂模式，或是您已配置此防火墙，以便使用虚拟机监控程序分配的 MAC 地址。

  由于数据平面 PAN-OS MAC 地址与 vSphere 分配的 vNIC MAC 地址不同，因此端口组（或整个 vSwitch）必须处于混杂模式，而如未启用虚拟机监控程序分配的 MAC 地址，请执行以下操作：

  - 检查 vSphere 上的 VLAN 设置。

    对 vSphere 端口组使用 VLAN 设置有两个目的：首先确定哪些端口组共享第 2 层域，然后确定是否标记上行链路端口 (802.1Q)。

  - 检查物理交换机端口设置

    如果在带有上行链路端口的端口组上指定 VLAN ID，则 vSphere 使用 802.1Q 标记出站帧。此标记必须与物理交换机上的配置一致，否则流量将无法通过。

    如果是使用分布式虚拟交换机 (vDS)，请检查端口统计信息；标准交换机不提供任何端口统计信息

©2024 Palo Alto Networks, Inc.

ESXi 的 VM 系列性能调整

适用于 ESXi 的 VM 系列防火墙是一款高性能设备，但可能需要调整虚拟机监控程序才能取得最佳效果。本节介绍了一些有助于实现 VM 系列防火墙最佳性能的最佳实践和建议。为获得最佳性能，建议使用 ESXi 6.0.0.0 或更高版本。

- 在 ESXi 上安装 NIC 驱动程序
- 在 ESXi 上启用 DPDK
- 在 ESXi 上启用 SR-IOV
- 使用 SR-IOV 启用 ESXi VLAN 访问模式
- 在 ESXi 上启用 NIC 的多队列支持
- VNF 性能调整

在 ESXi 上安装 NIC 驱动程序

要获得最佳性能，请使用带有 Intel 10GB 网络接口的 SR-IOV，这需要 ixgbe 4.4.1 驱动程序为每个接口支持多个队列。

STEP 1 | 获取 ESXi 主机上的网络接口列表。

1. 登录到 ESXi 主机 CLI。
2. 使用以下命令返回网络接口列表：

```
$ esxcli network nic list
```

STEP 2 | 确定特定接口的驱动程序版本。

您也可以使用 **ethtool** 或 **esxcli** 确定当前安装的驱动程序版本。以下示例使用 vNIC4 并返回驱动程序版本 3.21.6。

- ethtool—**ethtool -l *<nic-name>***

```
$ ethtool -I vNIC4 driver: ixgbe version:3.21.6iov firmware-
version:0x80000389 bus-info:0000:04:00.0
```

- esxcli—**esxcli network nic get -n *<nic-name>***

```
$ esxcli network nic get -n vNIC4 Advertised Auto Negotiation:
 true Advertised Link Modes:Auto Negotiation: true Cable
 Type:Current Message Level:7 Driver Info:Bus Info:0000:04:00.0
 Driver: ixgbe Firmware Version:0x80000389 Version:3.21.6iov Link
 Detected: false Link Status:Down Name: vNIC4 PHYAddress:0 Pause
 Autonegotiate: true Pause RX: true Pause TX: true Supported
 Ports:FIBRE Supports Auto Negotiation: true Supports Pause: true
 Supports Wakeon: false Transceiver: external Wakeon:None
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 安装新的驱动程序。

1. 从 VMware 网站下载 4.4.1 驱动程序。将内容压缩到本地目录，并找到驱动程序的 .zip 或 .vib 文件。
2. 在 ESXi 主机数据存储中创建新的文件夹。
3. 将压缩的本地 .zip 或 .vib 文件复制到 EXSi 主机数据存储的新文件夹中。
4. 在 ESXi 主机上启用维护模式。
5. 使用以下命令之一安装新驱动程序，-d 用于 .zip 文件，-v 用于 .vib 文件。
   - `$ esxcli software vib install -d <path to driver .zip file>`
   - `$ esxcli software vib install -v <path to driver .vib file>`

   必须指定前往 .zip 或 .vib 文件的绝对路径。例如：

   ```
   $ esxcli software vib install -d "/vmfs/volumes/
   Datastore/DirectoryName/DriverName.zip"
   ```
6. 验证 VIB 安装情况。

   ```
   $ esxcli software vib list
   ```
7. 重启 ESXi 主机。

在 ESXi 上启用 DPDK

数据面开发套件 (DPDK) 通过提高网络接口卡 (NIC) 数据包处理速度增强 VM 系列防火墙性能。在 VM 系列防火墙上，在 ESXi 上默认启用 DPDK。

要利用 DPDK，您必须将 NIC 与 DPDK 驱动程序版本中提到的支持 DPDK 驱动程序之一结合使用：

如果您禁用 DPDK，则 NIC 使用 PacketMMap 而不是 DPDK。可以使用 **`set system setting dpdk-pkt-io off`** 命令禁用 DPDK。

请参阅 PAN-OS 版本的 ESXi 虚拟机监控程序支持和 PacketMMAP 和 DPDK 驱动程序支持的兼容性矩阵。

在 ESXi 上启用 SR-IOV

单根 I/O 虚拟化 (SR-IOV) 允许单个根端口下的单个 PCIe 物理设备看起来像是虚拟机监控程序或来宾的多个单独的物理设备。通过在 SR-IOV NIC 上启用虚拟功能设备并修改 vCenter 中的来宾设置以启用 SR-IOV。

适用于 ESXi 的 VM 系列上的 SR-IOV 需要 PacketMMAP 驱动程序版本中提到的 Intel NIC 驱动程序之一。请参阅 PAN-OS 版本的 SR-IOV 和 DPDK 驱动程序支持的兼容性矩阵。

可以通过两种方法在 ESXi 上启用 SR-IOV。

©2024 Palo Alto Networks, Inc.

- **SR-IOV passthrough** — 通过此方法，您可以在 SR-IOV NIC 上启用虚拟功能设备，并在 vCenter 中修改来宾设置，从而添加 SR-IOV VF 接口作为适配器类型“SR-IOV Passthrough”。请参阅将虚拟功能作为SR-IOV Passthrough 适配器添加到虚拟机。

  对于 PAN-OS 8.1.2 及更高版本，此方法是首选，可让您将 SR-IOV PF 添加到 vSwitch 或 DvSwitch。

- **PCI Adaptor**（**PCI** 适配器）— 对于 PAN-OS 8.0 至 8.1.1，此方法是首选。您可以查看《8.1 部署指南》的在 ESXi 上启用 SR-IOV 中的 PCI 适配器工作流程。

  PCI 适配器方法的局限性在于，您无法在启用 SR-IOV 的物理端口上配置 vSwitch。VM 系列防火墙必须能够独占访问此接口上的物理端口和关联的虚拟功能 (VF)，以便可以与网络上的主机或其他虚拟机进行通信。请参阅在 vSphere Web Client 上添加 PCI 设备。

使用 SR-IOV 启用 ESXi VLAN 访问模式

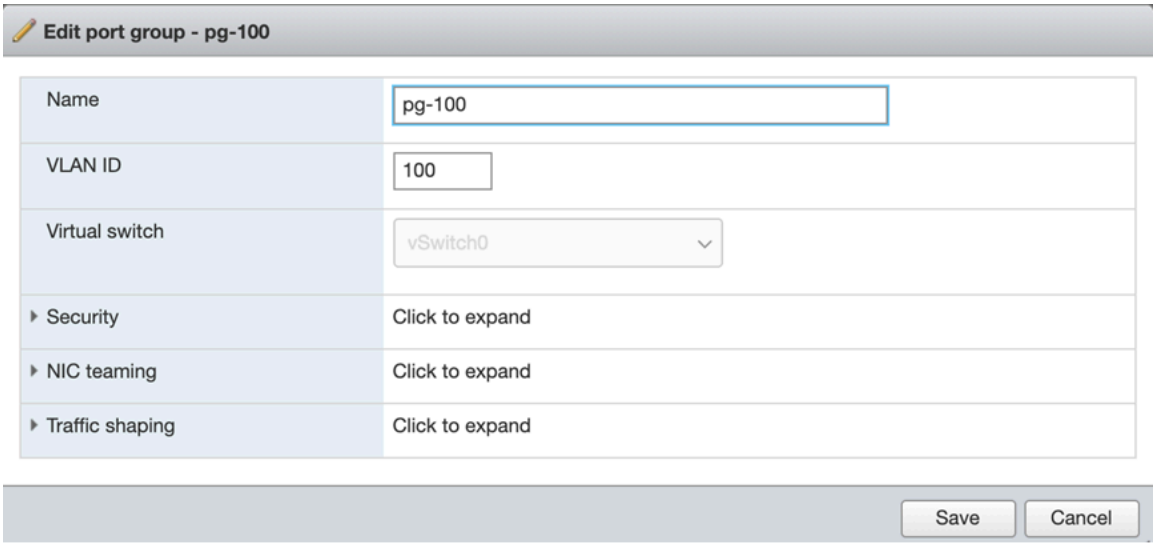
ESXi 上的 VM 系列防火墙可以在 VLAN 访问模式下运行，以支持将其部署作为虚拟网络功能 (VNF) 的用例，该功能可在多租户云/数据中心环境中提供安全即服务。在 VLAN 访问模式下，每个 VNF 都具有适用于每个网络的专用虚拟网络接口 (VNI)，并在不使用 VLAN 标记的情况下将数据包发送到 SR-IOV 虚拟功能 (VF)/从 SR-IOV 虚拟功能 (VF) 接收数据包；您必须在主机虚拟机监控程序的物理和虚拟功能上启用此功能。然后，在 VM 系列防火墙上启用 VLAN 访问模式后，防火墙可以在不使用 VLAN 标记的情况下在其所有数据平面接口之间发送和接收流量。此外，如果您已配置 QoS 策略，则防火墙可以在访问接口上强制执行 QoS，并在多租户部署中提供不同的流量处理。

默认情况下，*ESXi* 上的 *VM* 系列防火墙在 *VLAN* 中继模式下运行。

©2024 Palo Alto Networks, Inc.

STEP 1 | 在主机系统上，将物理和虚拟功能设置为在 VLAN 访问模式下运行。

1. 单击 VMware Host Client 清单中的 **Networking**（网络），然后单击 **Port groups**（端口组）。
2. 在要编辑的列表中，右键单击端口组并选择 **Edit settings**（编辑设置）。输入新的端口组 **Name**（名称）。输入新的 **VLAN ID**。



如需在 *VM* 系列防火墙上获得最佳性能，请确保：

- 启用 *CPU* 定位。
- 如果您已配置 *IPSec Tunnels*（*IPSec* 隧道），请 *Disable Replay Protection*（禁用重播保护）。

  在防火墙 *Web* 界面上，选择 ***Network***（网络） > ***IPSec Tunnels***（***IPSec*** 隧道）以选择 *IPSec* 隧道并单击 ***General***（常规），然后选择 ***Show Advanced Options***（显示高级选项）并清除 ***Enable Replay Protection***（启用重播保护）。

STEP 2 | 在 VM 系列防火墙上访问 CLI。

STEP 3 | 启用 VLAN 访问模式。

```
request plugins vm-series vlan-mode access-mode on
```

on 启用 VLAN 访问模式；要使用 VLAN 中继模式，请输入 **request plugins vm-series vlan-mode access-mode off**。

STEP 4 | 重启防火墙。

```
request restart system
```

STEP 5 | 验证 VLAN 模式配置。

```
show plugins vm-series vlan-mode
```


©2024 Palo Alto Networks, Inc.

在 ESXi 上启用 NIC 的多队列支持

多队列允许网络性能随着 vCPU 的数量而扩展，并通过创建多个 TX 和 RX 队列允许并行数据包处理。修改 .vmx 文件或访问 Advanced Settings（高级设置）以启用多队列。

STEP 1 | 启用多队列。

1. 打开 .vmx 文件。
2. 添加以下参数：

```
ethernetX.pnicFeatures = “4”
```

STEP 2 | 启用接收端扩展 (RSS)。

1. 登录到 ESXi 主机上的 CLI。
2. 执行以下命令：

```
$ vmkload_mod -u ixgbe $ vmkload_mod ixgbe RSS=”4,4,4,4,4,4”
```

STEP 3 | 为获得最佳性能，请为每个 ethernet/vSwitch 设备分配额外的 CPU 线程。这受 ESXi 主机上可用的备用 CPU 资源数量限制。

1. 打开 .vmx 文件。
2. 添加以下参数：

```
ethernetX.ctxPerDev = “1”
```

VNF 性能调整

本主题提供有关 VM 系列部署的 VNF 调整指南。您可以参考该指南为 VM 系列部署选择某些参数设置。在尝试调整之前，您应熟悉在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙的步骤，包括如何配置调整参数和属性。

本指南可能不适用于超出针对 *SD-WAN*、*MSSP* 或 *CSSP* 用例的白盒或灰盒环境以外的 *VM* 系列部署。

VM 系列是一种高性能设备，能够提供各种尺寸，具体取决于大小、虚拟机监控程序占用空间及其在私有云或公共云中的部署位置。

全局和主机级别配置更改会影响同一主机上运行的其他 VM。您应考虑任何折衷方案，并谨慎选择最适合部署的参数。

- ESXi 调整参数
- 用例
- 参考资料

©2024 Palo Alto Networks, Inc.

ESXi 调整参数

要在 VM 系列上实现最佳性能，您可以调整硬件、虚拟机监控程序和网络 I/O 参数。

此处提到的参数并不适用于每个部署模型。

- BIOS 设置
- 物理设置
- 虚拟 NIC 设置
- NUMA 和资源注意事项

BIOS 设置

本节建议可以增强 VM 系列防火墙性能的 BIOS 电源管理、超线程和 Intel VT-D 设置，并用 BIOS 配置示例作为总结。

- 电源管理
- 超线程
- Intel Virtualization Technology for Directed I/O
- BIOS 配置示例

电源管理

对于延迟敏感的应用程序，任何形式的电源管理都会增加空闲系统（以几种省电模式之一）对外部事件作出响应的路径的延迟。VMware 建议将 BIOS 电源管理设置设置为“静态高性能”（无操作系统控制的电源管理），从而有效禁用任何形式的主动电源管理。具有 Intel Nehalem 类及更高版本 CPU（Intel Xeon 55xx 及更高版本）的服务器提供了两个其他电源管理选项：C-states 和 Intel Turbo Boost。

启用 C-states 可能会增加内存延迟，因此不建议用于低延迟工作负载。即使是增强型 C-states（也称为 C1E）也会引入更长的延迟，以将 CPU 从暂停（空闲）状态唤醒到全功率状态。VMware 建议在 BIOS 中禁用 C1E，以进一步缩减延迟。

- 对于 HP，请将电源调节器模式设置为静态高性能模式，并禁用 QPI 处理器、C-states 支持和 C1E 支持。
- 对于 Dell，请将电源管理模式、CPU 电源和性能管理设置为最高性能。

要考虑的另一个参数是 P-states。出于性能方面的考虑，请在 BIOS 中禁用 P-states 设置。

Intel Turbo Boost 可能会在一段时间内导致性能变化。为了获得一致的确定性性能，请禁用 Turbo Boost。

超线程

如果硬件和 BIOS 支持超线程，则 ESXi 会在主机上自动启用超线程。为了从 VM 系列防火墙获得最佳性能，请在 ESXi 主机上禁用超线程。

©2024 Palo Alto Networks, Inc.

如果部署环境允许启用超线程，请确保从可以访问 PCI 设备的同一 NUMA/Socket 节点保留 VM 系列防火墙的所有 CPU 资源。

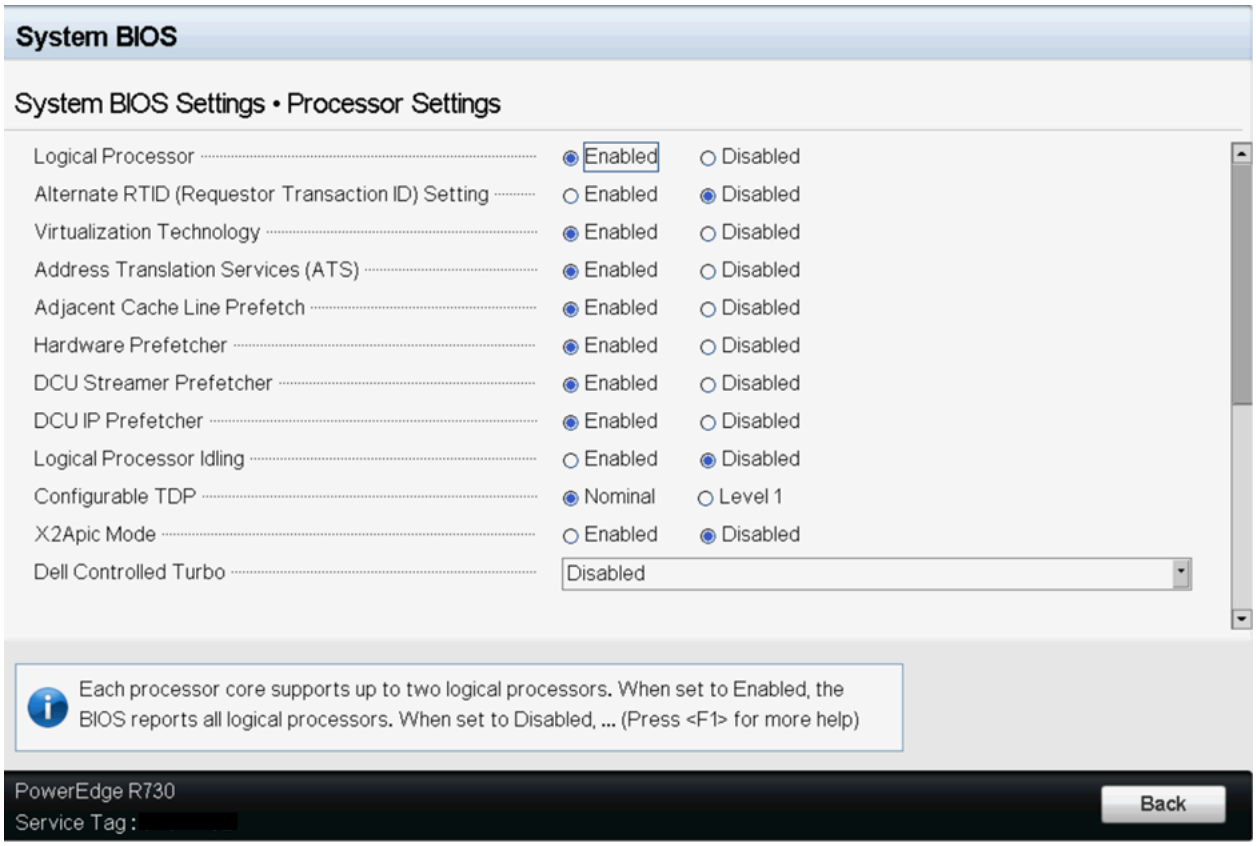
通常，配置 PA-VM 作为单个 NUMA VM。有关更多详细信息，请参阅NUMA 和资源注意事项。

Intel Virtualization Technology for Directed I/O

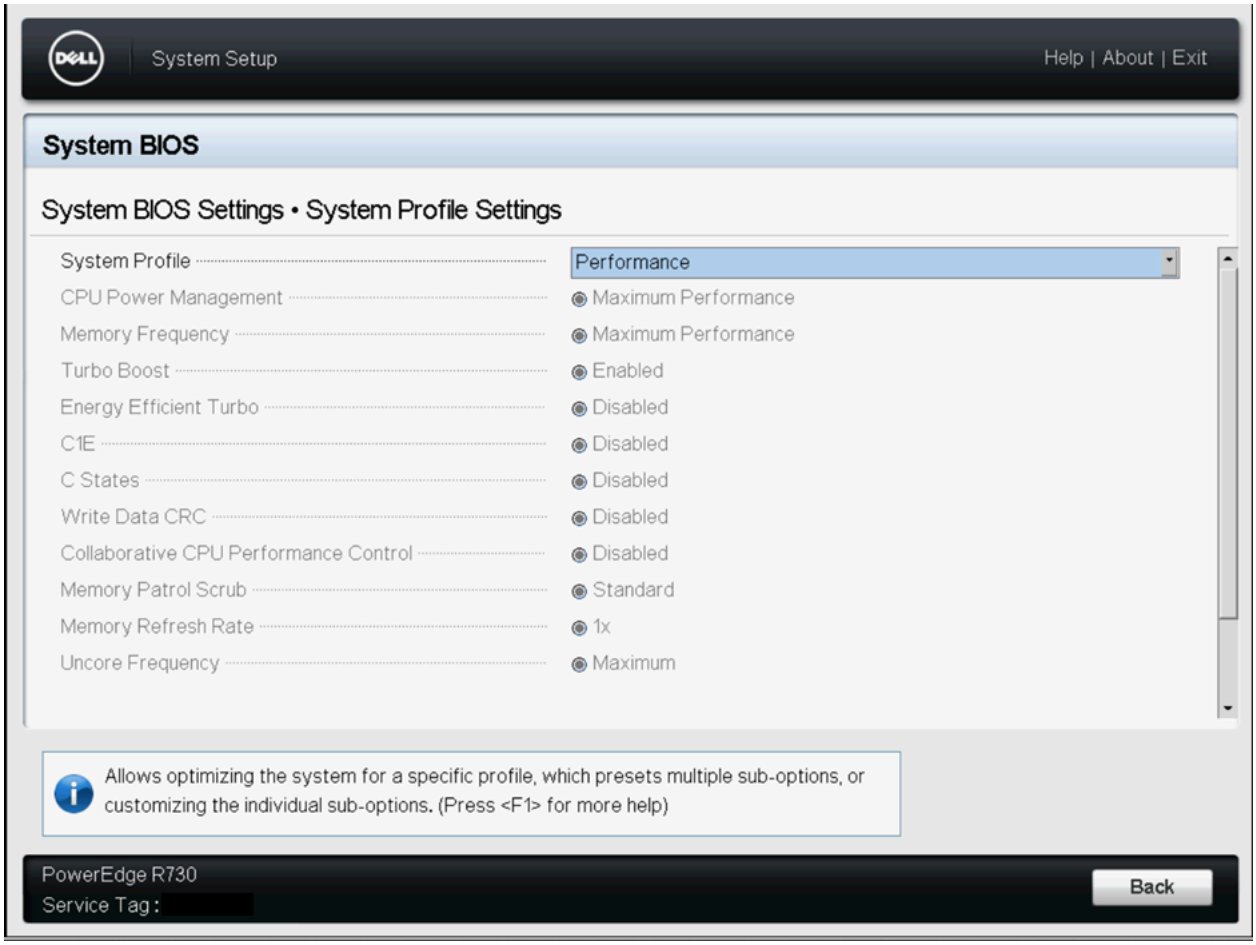
Intel Virtualization Technology for Directed I/O (Intel VT-D) 允许将 LAN 卡专用于来宾系统，从而实现比仿真 LAN 卡更高的网络性能。在 BIOS 上启用此功能。如果您计划利用 SR-IOV 提高性能（推荐），请启用 SRI-OV BIOS 设置。

BIOS 配置示例

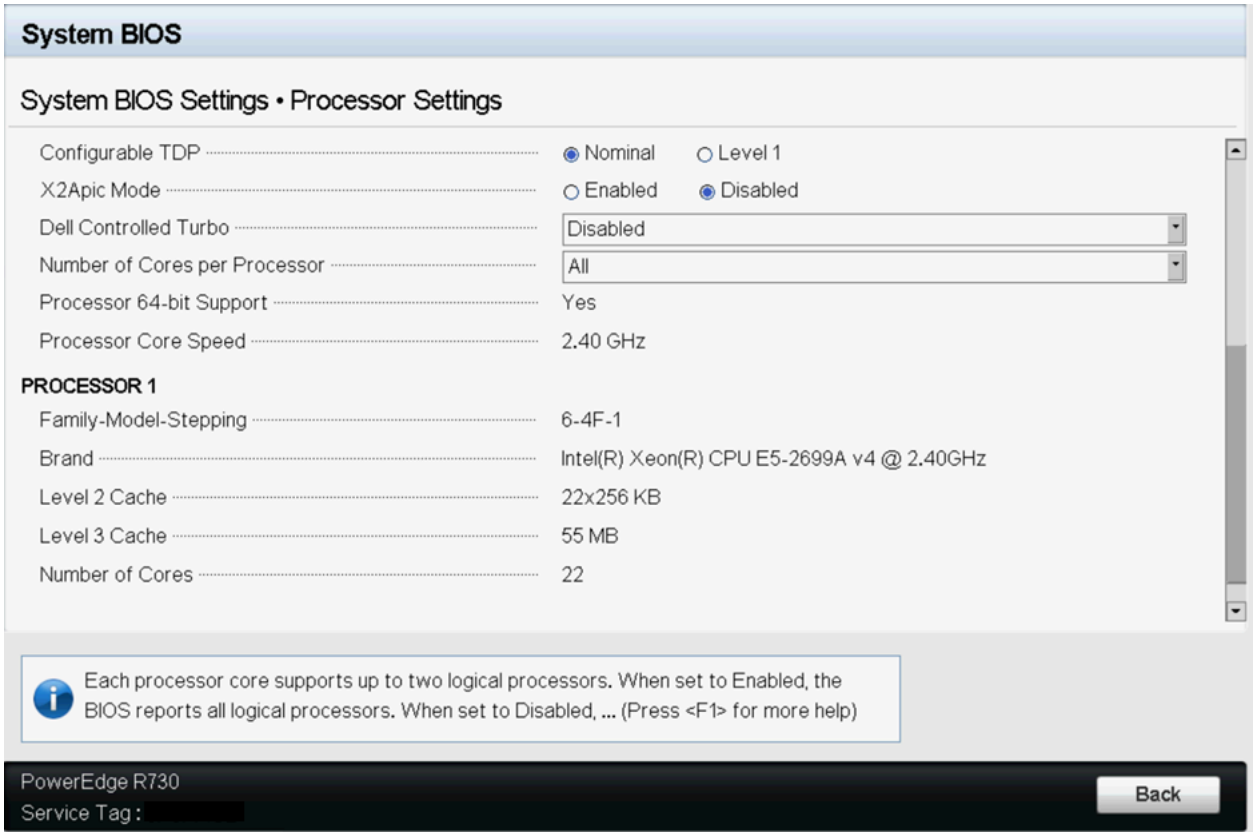
以下屏幕截图显示了 Dell BIOS 的系统配置文件设置和处理器设置。



©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.



物理设置

大部分 1GbE 或 10GbE 网络接口卡 (NIC) 支持称为中断裁决或中断限制的功能，该功能可将从 NIC 到主机的中断合并在一起，从而不会使主机变得惊慌失措，并且能够花费所有 CPU 周期来处理中断。但是，对于延迟敏感的工作负载，NIC 延迟收到的数据包或已在网络上成功发送的数据包的中断交付时间，就是增加工作负载的延迟的时间。为了在 PA-VM 上获得最佳性能，请禁用中断裁决。例如，按如下所示在 ESXi 主机上禁用物理 NIC 中断裁决：

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0"
```

- 传输队列
- 队列配对

传输队列

ESXi 上行链路 pNIC 层还可维护排队等待传输的数据包的软件 Tx 队列，默认可存储 500 个数据包。如果工作负载是 I/O 密集型且包含大量的传输数据包突发，则此队列可能会溢出，从而导致数据包在上行链路层中丢弃。使用以下 ESXi 命令，可以将 Tx 队列大小最多增加到 10,000 个数据包：

```
# esxcli system settings advanced set -i 10000 -o /Net/
MaxNetifTxQueueLen
```


©2024 Palo Alto Networks, Inc.

根据 ESXi 主机上使用的物理 NIC 和特定的 ESXi 驱动程序版本，有时可能会在 pNIC 驱动程序中丢弃数据包，因为 pNIC 上的传输环路太小且已被填满。大部分 pNIC 驱动程序允许使用以下命令增加传输环路的大小：

```
# ethtool -G vmnic0 tx 4096
```

此命令可将 Tx 环路大小增加到 4096 个条目。您可以使用以下命令确定能为特定 pNIC 驱动程序设置的最大大小，以及当前有效的 Tx 环路大小：

```
# ethtool -g vmnic0
```

```
Ring parameters for vmnic0:Pre-set maximums:RX:4096 RX Mini:0 RX
 Jumbo:0 TX:4096 Current hardware settings:RX:512 RX Mini:0 RX
 Jumbo:0 TX:4096
```

队列配对

某些 pNIC 驱动程序（例如 Intel 的 ixgbe 和 Broadcom 的 bnx2x）也支持“队列配对”，这表明接收线程 (NetPoll) 的 ESXi 上行链路层也将处理配对传输队列中传输数据包的完成情况。对于某些传输繁重的工作负载，这可能会导致处理传输完成情况的延迟，从而导致 vNIC 的传输环路用完传输其他数据包的空间，并强制来宾操作系统中的 vNIC 驱动程序丢弃数据包。

在 ESXi 主机上为所有 pNIC 禁用队列配对会创建一个单独的线程，用于处理 pNIC 传输完成情况。因此，应及时处理传输完成情况，从而释放 vNIC 传输环路中的空间以传输其他数据包。

您可以使用以下 ESXi 命令禁用队列配对：

```
# esxcli system settings advanced set -o /Net/
NetNetqRxQueueFeatPairEnable -i 0
```

为使此命令生效，必须重新启动 ESXi 主机。

如果在专用主机上使用 *VM-700* 的 *PCI-passthrough*，则无需对 *NIC/NIC* 驱动程序进行性能调整。但是，这种部署模式并不常见。

虚拟 **NIC** 设置

如果可能，请使用 SR-IOV 获取最佳性能，如以下主题所述：

- SR-IOV
- VMXNET3/vSwitch 和虚拟中断合并
- 在 Intel x710/x520 上启用多队列支持

SR-IOV

- 更改 SR-IOV 驱动程序的模块参数需要重新启动 ESXi 主机。

 ©2024 Palo Alto Networks, Inc.

- 按如下所示在 ESXi 主机上禁用物理 NIC 中断裁决：

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0 “
```

- 如果启用多队列支持，则还必须为驱动程序启用接收方缩放 (RSS)。
  - 要启用 RSS，请将端口值设置为 4。
  - 用以逗号分隔的字符串指定端口。

  示例 — 设置 3 个 NIC，每个 NIC 带 2 个端口。

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=” 4,4,4,4,4,4”
```

```
$ vmkload_mod ixgbe RSS=” 4,4,4,4,4,4”
```

  示例 — 为单个端口设置 RSS：

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=” 0,4,0,0,0,0”
```

VMXNET3/vSwitch 和虚拟中断合并

默认情况下，VMXNET3 支持中断合并算法（出于与物理 NIC 实现中断裁决相同的原因）。为了避免中断过多而使主机系统崩溃，因此需要收集数据包并为多个数据包生成一个中断，这称为中断合并。

中断合并是指在发出硬中断之前，网络接口接收的流量总量，或收到流量后经过的时间总量。由于内核停止（或“中断”）正在运行的任务以处理来自硬件的中断请求，因此中断太快或太频繁都会导致系统性能下降。如果不能尽快丢弃 NIC 的流量，则中断太晚可能会导致流量丢失 — 更多流量到达，将覆盖仍在等待内核接收的先前流量。要通过 vSphere Web Client 禁用此功能，请转至 **VM Settings**（**VM** 设置） > **Options**（选项） > **Advanced General**（高级常规） > **Configuration Parameters**（配置参数），然后使用值 **`disabled`** 为 **`ethernetX.coalescingScheme`** 添加一个条目。

要在主机上为所有虚拟 NIC 禁用虚拟中断合并（这会影响所有 VM，而不仅仅是对延迟敏感的 VM），请设置高级网络性能选项。转至 **Configuration**（配置） > **Advanced Settings**（高级设置） > **Net**（网络），然后将 **`CoalesceDefaultOn`** 设置为 **`0`**（禁用）。

在 **Intel x710/x520** 上启用多队列支持

使用具有多队列支持的 ixgbe 驱动程序版本的 ESXi 6.0.0 或更高版本。请参阅兼容性矩阵中的 SR-IOV 驱动程序版本。Modify the `.vmx` file or access **Advanced Settings** to enable multiqueue support:

```
ethernetX.pnicFeatures = “4”
```


©2024 Palo Alto Networks, Inc.

To set multi-core affinity so a vSwitch can exceed 300K PPS, set:

```
ethernetX.pnicFeatures = "4" ethernetX.ctxPerDev = "1"
```

Setting **ethernetX.ctxPerDev = “1”**, is like a binary flag (set to 1 to enable).该二进制标志添加一个 CPU 线程来仅处理来自 **ethernetX** 端口的流量，这会导致提高流量调度性能。

NUMA 和资源注意事项

NUMA 是指非一致性内存访问。多核处理器具有复杂的设计。为了解决此类系统中的性能问题，您需要了解所有 NUMA 和 CPU Pinning 的细微差别。需要注意以下几个重要方面：

- 线程在哪些核心上运行？（如果已用超线程，请参阅超线程）
- vCPU 在哪些核心上运行？（相关性）
- 物理 NIC 卡安装在哪个 NUMA 插槽中？
- 内存分配在哪里？（NUMA 影响）

  在任何套接字上运行的线程都有一个统一的内存空间，因此它们可以读取/写入其他套接字本地的内存。
- 节点上的不同套接字之间共享内存吗？
- 与访问本地内存相比，访问不同套接字上的内存需要花费更多时间。

  当线程过多访问其他 NUMA 域中的内存时，就会出现 MUMA 影响。为了避免跨 NUMA 问题，应避免套接字 0 通信与套接字 1 通信之间的快速通道互联 (QPi)。

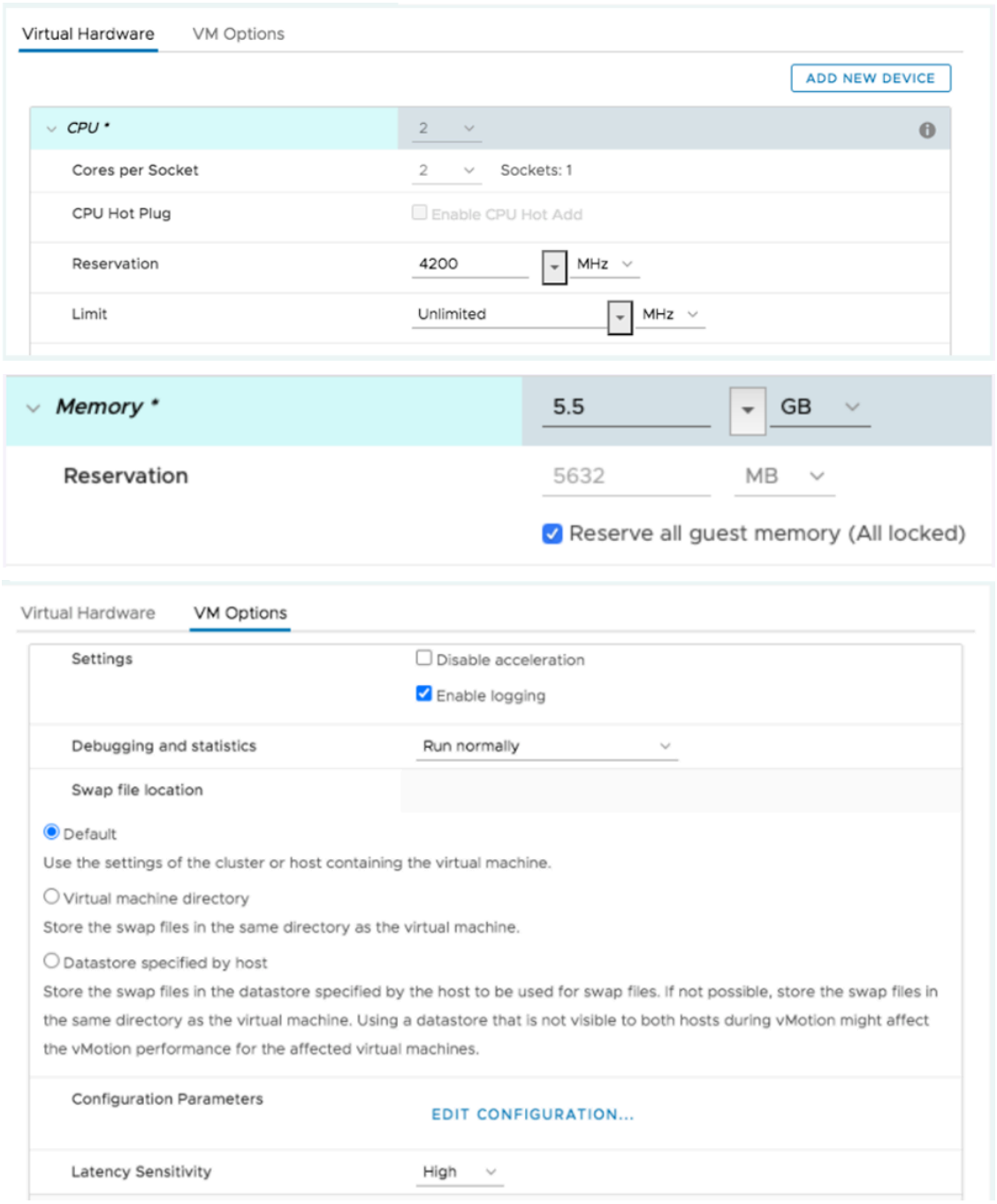
对于延迟敏感的 VM（例如 PA-VM），与 ESXi 主机上的物理 CPU（处理器）数量相比，VMware 建议不要过量使用 vCPU。例如，如果主机具有 8 个 CPU 内核，则将 VM 的 vCPU 数量限制为 7。这可确保 ESXi VMkernel 调度程序有更大的机会将 vCPU 放置在与其他调度环境不兼容的 pCPU 上，例如其他 VM 或 ESXi 帮助程序环境的 vCPU。最好是确保分配给 VM 的 vCPU 数量不超过 VM 中消耗活动 CPU 的进程或线程的数量。

为了获得最佳性能，应将所有 vCPU 安排在同一 NUMA 节点上，并且所有 VM 内存应适合并从与该 NUMA 节点相连的本地物理内存中分配出来。可以使用 VM 设置 **numa.nodeAffinity=0, 1, …** 更改此设置，其中 0 和 1 等是套接字号。

要确保 VM 能够独占访问 CPU 资源，请将“延迟敏感度”设置为“高”。为使新设置生效，必须将 VM CPU 保留设置为最大，应保留内存，并且必须将 CPU 限制设置为无限制。

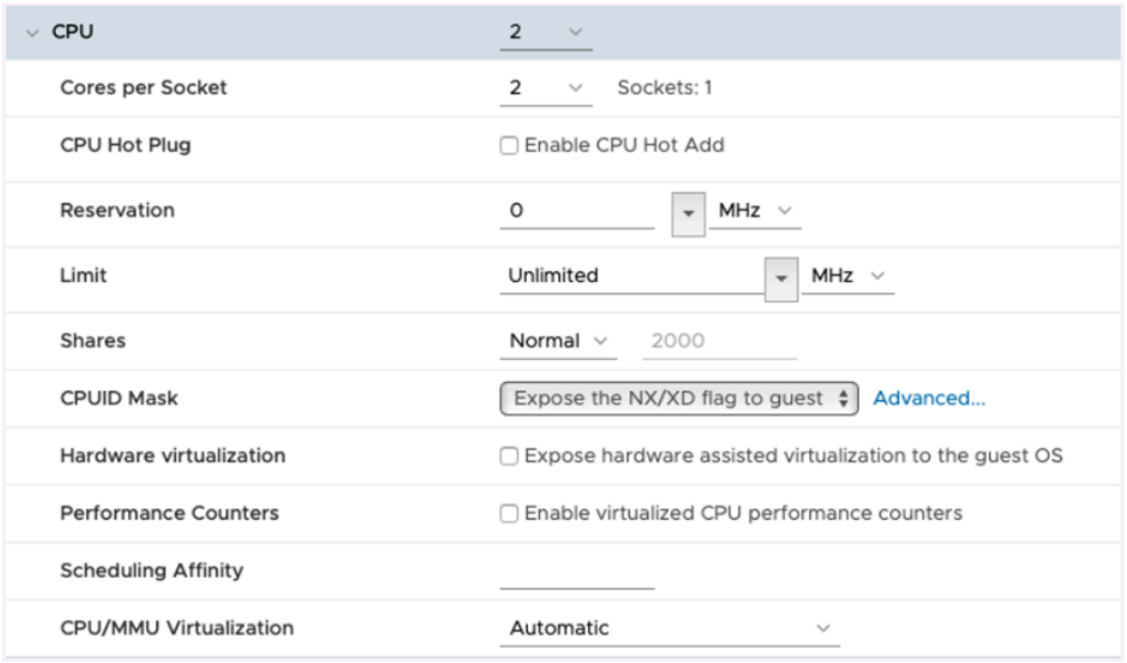
- 在较新版本中，使用 vSphere Web Client 将“VM 延迟敏感度”选项设置为“高”（默认值为“正常”）。
- 在较旧版本中，将 **sched.cpu.latencySensitivity** 设置为“高”。

©2024 Palo Alto Networks, Inc.



此外，还可以使用 VM 设置 **Host Affinity**（主机相关性）将 VM 的 vCPU 固定到主机 CPU 内核，这样永远就不会将其调度到其他内核。使用主机相关性时，请记住 NUMA 和超线程。如果过度使用系统，请避免设置主机相关性。有关更多详细信息，请参阅 CPU 相关性的潜在问题。

©2024 Palo Alto Networks, Inc.



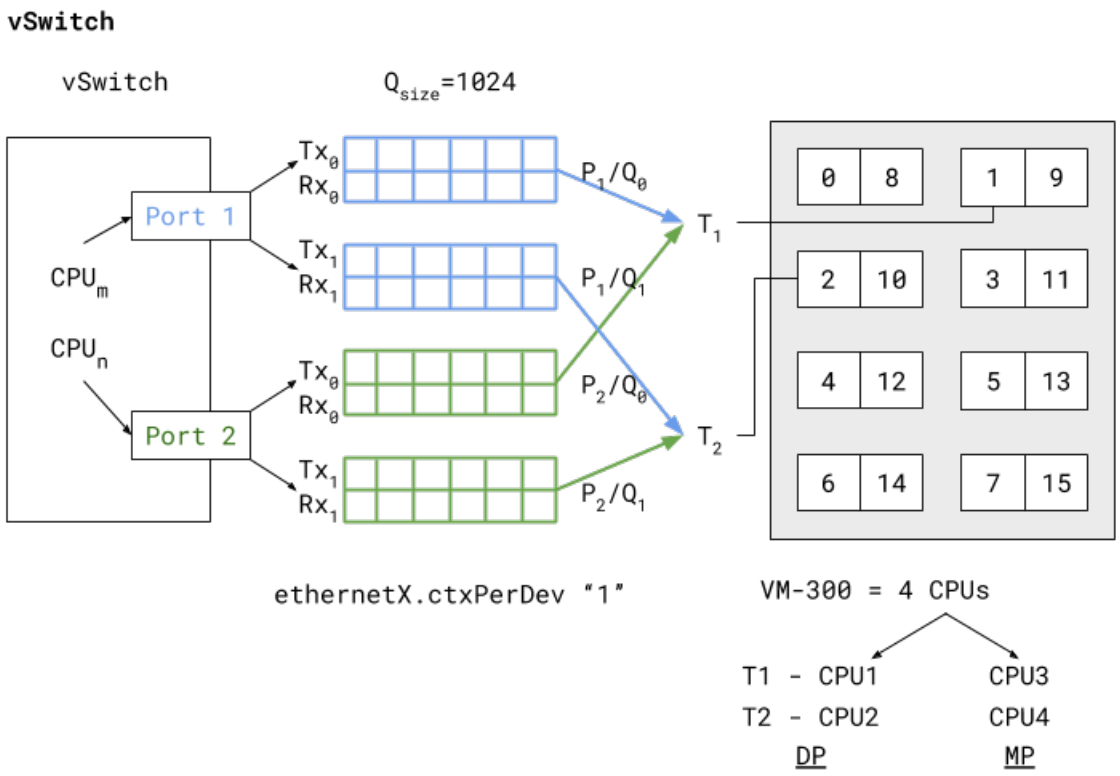
实施调整参数后，使用 esxtop 或 CPU 图表检查 VM 的 CPU Ready (%RDY) 和 Co Stop (%CSTP)。这两个值都应接近 0%，以确保可以独占访问 CPU 资源。您也可以使用 esxtop 检查 NUMA 使用情况，并确保 VM 的内存资源不会在 NUMA 节点之间扩散。有关更多详细信息，请参阅解释 esxtop 统计信息。

用例

用例 **1**：**vSwitch** 部署

下图显示了 ESXi 主机上的 PA-VM 部署，其中数据端口“端口 1”和“端口 2”链接到 PA-VM 的 eth1 和 eth2。每个端口托管两个队列对（例如，Tx0/Rx0 和 Tx1/Rx1），或已启用多队列。

©2024 Palo Alto Networks, Inc.



启用多队列和 RSS 以负载均衡发送到多个队列或从多个队列接收的数据包可提高处理性能。根据 vCPU 到端口/队列映射的内部逻辑（在本例中），从 P1/Q0 和 P2/Q0 到达和发送的数据包由在 vCPU1 上运行（即固定）的数据平面任务 T1 处理。数据平面任务 T2 遵循类似的关联，如上面的 vSwitch 部署图所示。

这两个数据平面任务在 vCPU1 和 vCPU2 上运行，并且它们是非同级 CPU（意味着在启用超线程时无法共享同一内核）。这意味着即使启用超线程，也可以将任务分配固定到不同的内核以实现高性能。同样，这些数据平面任务 vCPU 都属于同一 NUMA 节点（或套按字），以避免出现与 NUMA 相关的性能问题。

可以通过增加队列大小，并将 vCPU 或线程专用于调度往返于这些端口的流量的端口，从而解决其他两个性能瓶颈。增加队列大小 (Qsize) 可容纳大量的突发流量，并防止突发流量下的数据包丢弃。在端口级数据包处理中添加专用 CPU 线程 (**`ethernetX.ctxPerDev = 1`**) 将允许以更高的速率处理流量，从而提高流量吞吐量以达到线路速率。

PA-VM 数据包处理技术也可以决定性能，可以将其设置为 DPDK 或 PacketMMAP。DPDK 使用轮询模式驱动程序（取决于驱动程序类型）不断轮询队列中收到的数据包，这可以导致更高的吞吐量性能。根据轮询周期，数据包会观察到延迟。如果轮询是连续的（即从 PANOS CLI 设置繁忙轮询），则数据平面任务的 vCPU 利用率将为 100%，但可以产生最佳性能。在内部，软件使用毫秒级轮询时间来防止不必要地利用 CPU 资源。

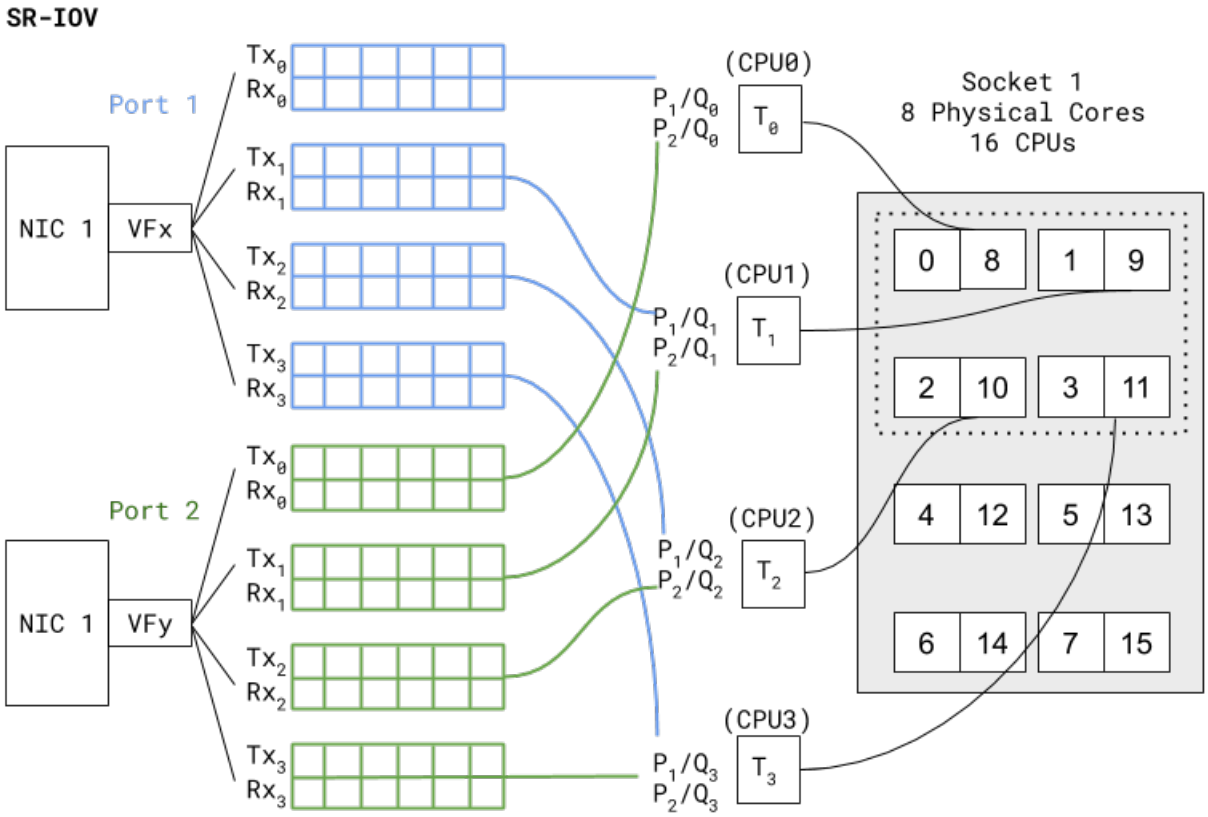
另一方面，PacketMMAP 的性能比 DPDK 低，但它可以与任何网络级驱动程序一起使用。对于 DPDK，vSwitch 驱动程序必须支持 DPDK。PacketMMAP 处理端口接收数据包并将其放入接收队列时引发的中断。对于每个数据包或数据包组，这意味着都会引发中断，并且会将数据包从接收队列排出以进行处理。这可减少数据包处理的延迟，但会降低吞吐量，因为每次都必须处理中断，从

©2024 Palo Alto Networks, Inc.

而导致更高的 CPU 开销。通常，PacketMMAP 将具有比 DPDK 更低的数据包处理延迟（无需修改繁忙轮询设置）。

用例 **2**：**SR-IOV** 部署

下面的 SR-IOV 部署图显示了与 vSwitch 用例类似的 PAVM 部署，但在 SR-IOV 模式下。



在 SR-IOV 中，兼容的物理 NIC 端口（表现为物理功能）实质上被划分为多个接口（表现为虚拟功能）。上图显示了 NIC1 Port1 具有一个名为 VFX 的 VF，关联该 VF 作为 PAVM 数据平面接口之一，例如 eth1。为 Port2 VF 与 PAVM eth2 创建类似的关联。数据包处理链类似于 vSwitch 环境中的部署链。唯一区别是 SR-IOV VF 驱动程序应与 PAN-OS 中使用的驱动程序兼容。此外，由于没有内部 vSwitch（在主机中）交换流量，因此无需设置用于从端口调度流量的专用线程（也就是说，在此设置中不需要 **`ethernetX.ctxPerDev = 1`**）。与 SR-IOV 和 DPDK 配合使用，将产生比 vSwitch 用例更高的数据包处理性能。

参考资料

- 调整 VMware vCloud NFV 以处理数据密集型工作负载
- vSphere 中 Telco 和 NFV 工作负载性能调整的最佳实践
- CPU 相关性的潜在问题
- 解释 esxtop 统计信息

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 vCloud Air 上设置 VM 系列防火墙

可以使用 vCloud Air 门户从 vCloud Director 门户或使用 vCloud Air API 在 vCloud Air 上的虚拟数据中心 (vDC) 中部署 VM 系列防火墙。

- 关于 vCloud Air 上的 VM 系列防火墙
- vCloud Air 上支持的部署
- 在 vCloud Air 上部署 VM 系列防火墙

关于 vCloud Air 上的 VM 系列防火墙

您可使用 vCloud Air 门户或通过 vCloud Director 门户在 VMware vCloud Air 的虚拟数据中心 (vDC) 中部署 VM 系列防火墙。随即对所有物理和 VM 系列防火墙进行集中管理，同时您可使用现有的 Panorama 或在内部/vCloud Air 上部署新 Panorama。

在 vCloud Air 上部署 VM 系列防火墙，需满足以下条件：

- ESXi 版本的软件映像，这是一个开放式虚拟化联盟 (OVA) 文件，可从 Palo Alto Networks 客户支持站点下载。目前，vCloud Air 市场未托管此软件映像。

  为高效部署 VM 系列防火墙，请在 vApp 中纳入防火墙软件映像。vApp 是预配置虚拟设备（虚拟机和操作系统映像）的容器，且将作为单个对象进行管理。例如，如果您的 vApp 包括一组多层应用程序和 VM 系列防火墙，则您每次部署此 vApp 时，VM 系列防火墙会自动保护随 vApp 一同部署的 Web 服务器和数据库服务器。
- 在自带许可证 (BYOL) 模式下，从合作伙伴、经销商或直接从 Palo Alto Networks 购买的许可证和订阅；在 vCloud Air 上，针对 VM 系列防火墙的基于使用的许可证不可用。
- 鉴于在 vCloud Air 上施加的安全限制，最好使用第 3 层接口来部署 vCloud Air 上的 VM 系列防火墙，同时必须启用此类接口使用虚拟机监控程序分配的 MAC 地址。如果您未启用虚拟机监控程序分配的 MAC 地址，VMware vSwitch 将无法转发流量至 VM 系列防火墙上的数据面板接口，因为 vCloud Air 上的 vSwitch 不支持混杂模式或 MAC 伪造传输。不可使用旁接接口、第 2 层接口或虚拟线路接口部署 VM 系列防火墙。

仅可在主动/被动高可用性配置中部署 vCloud Air 上的 VM 系列防火墙。但是，vCloud Air 上的 VM 系列防火墙不支持为托管于 vCloud Air 上的虚拟机配置的 VM 监控功能。

如需了解有关 vCloud Air 的一切信息，请参阅 VMware vCloud Air 文档。

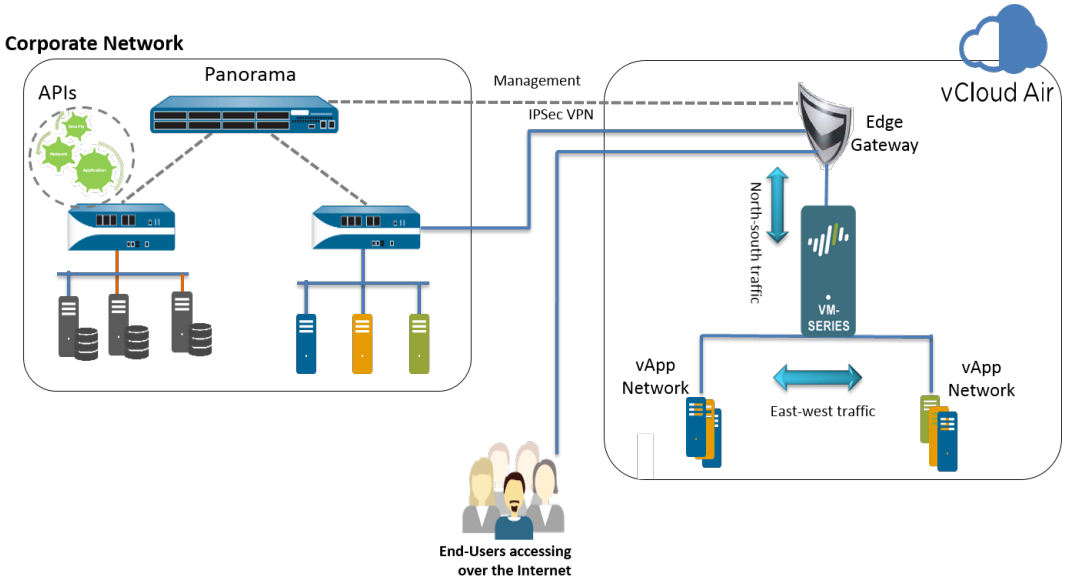
©2024 Palo Alto Networks, Inc.

vCloud Air 上支持的部署

如需安全启用应用程序，请阻止已知和未知的威胁，而如需与环境变更速度保持一致，您可采用以下方法通过第 3 层接口在 vCloud Air 上部署 VM 系列防火墙：

- 保护虚拟数据中心边界 — 将 VM 系列防火墙部署为连接 vCloud Air 上已独立、已路由网络的虚拟机。在此部署中，防火墙将保护所有遍历 vCloud Air 上基础架构的北向南流量。
- 设置混合云 — 将您的数据中心和专有云拓展至 vCloud Air 上，然后使用 VPN 连接，实现企业网络和数据中心之间的通信。在此部署中，VM 系列防火墙将使用 IPSec 进行流量加密并保护访问云的用户。
- 保护 **vDC** 中应用程序子网之间的流量 — 为提高安全性，请通过创建应用程序层来划分网络并隔离流量，然后部署 VM 系列防火墙以防止子网和应用程序层之间的侧向威胁。

以下说明整合了所有三种部署场景且包括 Panorama 的相关内容。借助 Panorama 可简化策略更新，集中进行策略管理，并实现集中日志记录和报告。



©2024 Palo Alto Networks, Inc.

在 vCloud Air 上部署 VM 系列防火墙

使用本节中的说明，在 vCloud Air 上通过按需或专用型 vDC 部署 VM 系列防火墙。本流程假定您已设置您的 vDC（包括允许流量进入和流出 vDC 所需的网关），以及通过 vDC 路由管理流量和数据所需的网络。

STEP 1 | 从 Palo Alto Networks 客户支持网站获取 VM 系列 OVA 映像；vCloud Air Marketplace 目前不托管软件映像。

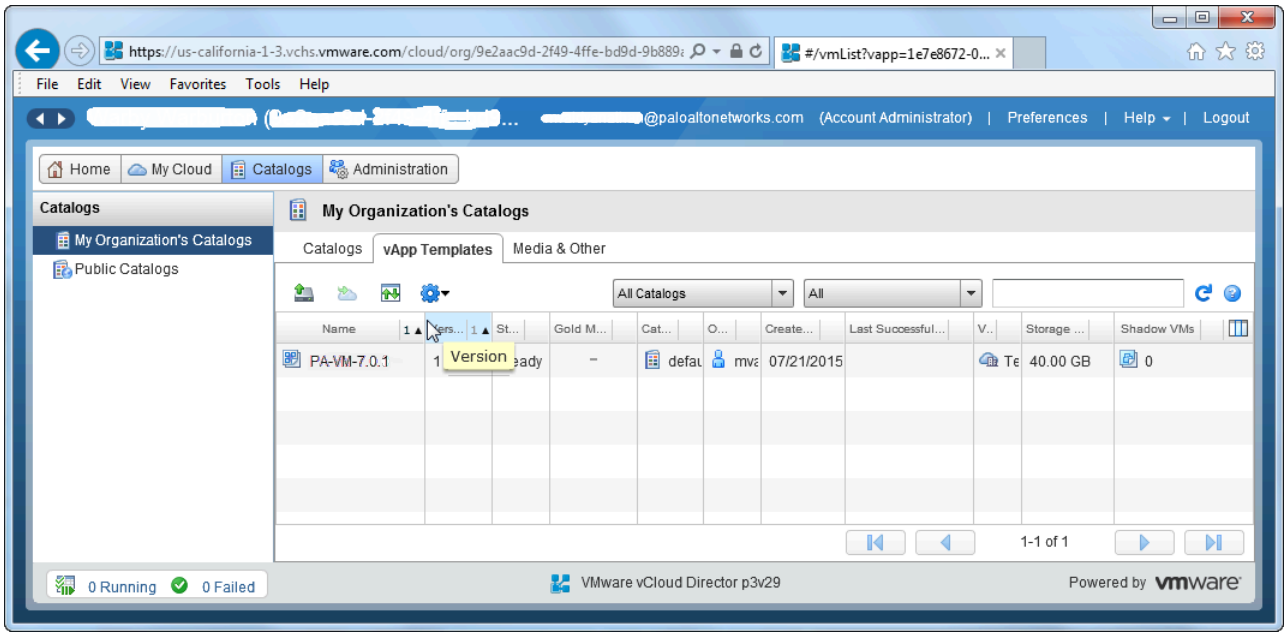
1. 转到：www.paloaltonetworks.com/services/support.html.
2. 按 **PAN-OS for VM-Series Base Images**（用于 **VM** 系列基本映像的 **PAN-OS**）进行筛选并下载 OVA 映像。例如，PA-VM-ESX-9.1.0.ova。

STEP 2 | 从 OVA 映像中提取开放式虚拟化格式 (OVF) 文件，并将该 OVF 文件导入到您的 vCloud Air 编录中。

在从 OVA 映像中提取文件时，确保将所有文件（包括 .mf、.ovf 和 .vmdk 格式）放置在同一目录中。

有关从 OVA 映像中提取 OVF 文件的说明，请参阅 VMware 文档：https://www.vmware.com/support/developer/ovf/#sthash.WUp55ZyE.dpuf

在导入 OVF 文件时，VM 系列防火墙的软件映像列于 **My Organization’ s Catalogs**（我的组织编录）中。



©2024 Palo Alto Networks, Inc.

STEP 3 | 选择您的工作流。

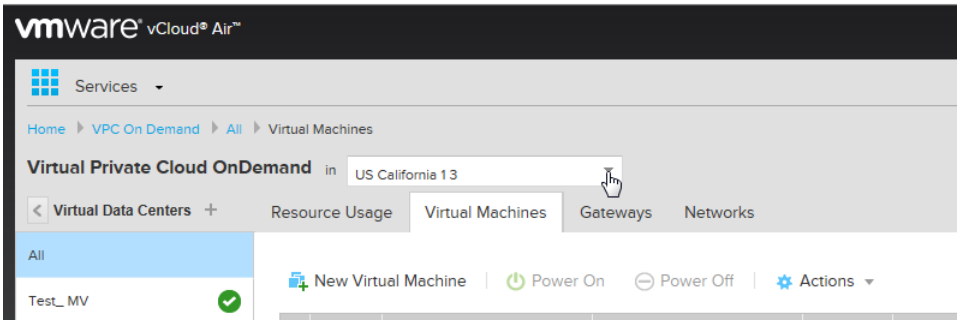
vApp 是一个模板集，适用于所有包含虚拟机及操作系统映像的预配置虚拟设备。

- 如果您想创建包含 VM 系列防火墙的新 vDC 和新 vApp，请转到步骤 4。
- 如果您已部署 vDC 且已配备 vApp，现在希望将 VM 系列防火墙添加至 vApp 以保护流量，请转到步骤 5

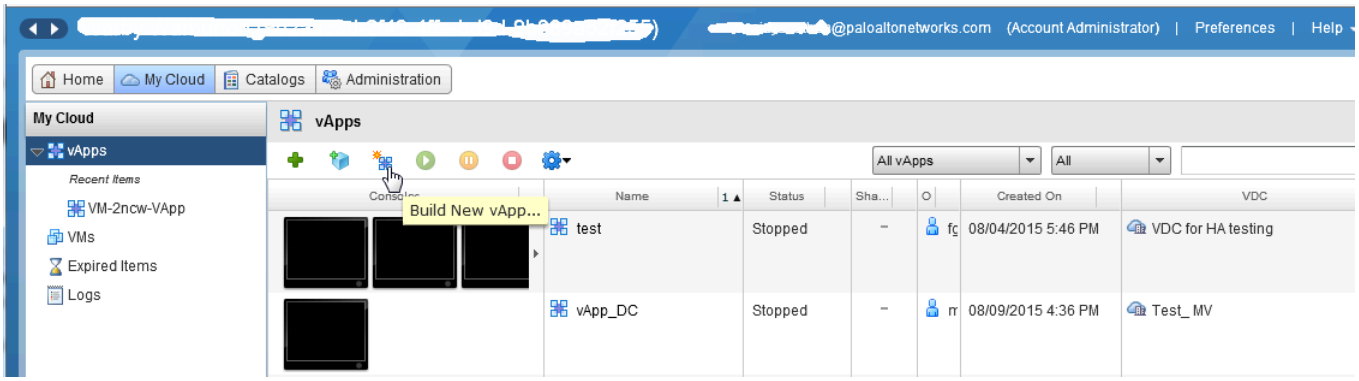
©2024 Palo Alto Networks, Inc.

STEP 4 | 创建包含 VM 系列防火墙的 vDC 和 vApp。

1. 登录到 vCloud Air。
2. 选择 **VPC OnDemand**，然后选择希望部署 VM 系列防火墙的位置。



3. 选择 **Virtual Data Centers**（虚拟数据中心），然后单击 **+** 以添加新虚拟数据中心。
4. 选择 vDC，右键单击并选择 **Manage Catalogs in vCloud Director**（管理 **vCloud Director** 中的编录）。您将重定向至 vCloud Director 的 Web 接口。
5. 创建含有一个或多个虚拟机（包括 VM 系列防火墙在内）的新 vApp：
   1. 选择 **My Cloud**（我的云）> **vApp**，然后单击 **Build New vApp**（构建新 **vApp**）。



   2. 选择 **Name and Location**（名称和位置），然后选择此 vApp 将在其中运行的**Virtual Datacenter**（虚拟数据中心）。默认情况下，运行时间和存储的 **Leases**（租借）不会过期，且 vApp 不会自动关闭。
   3. 添加虚拟机。要从 **Look in:**（查看：）下拉列表中添加 VM 系列防火墙，请选择 **My Organization's Catalog**（我的组织编录），然后选择映像并单击 **Add**（添加）。单击 **Next**（下一步）。
   4. 配置 **Resources**（资源）以指定部署虚拟机后的存储策略。VM 系列防火墙使用 **Standard**（标准）选项。
   5. 配置 **Virtual Machines**（虚拟机）。命名各虚拟机，然后选择希望其连接的网络。您必须将 NIC 0（用于管理访问）连接至默认路由网络；NIC 1 用于数据流量。您可稍后再添加其他 NIC。
   6. 验证设置，然后单击 **Finish**（完成）。
   7. 继续转到步骤 6。

©2024 Palo Alto Networks, Inc.

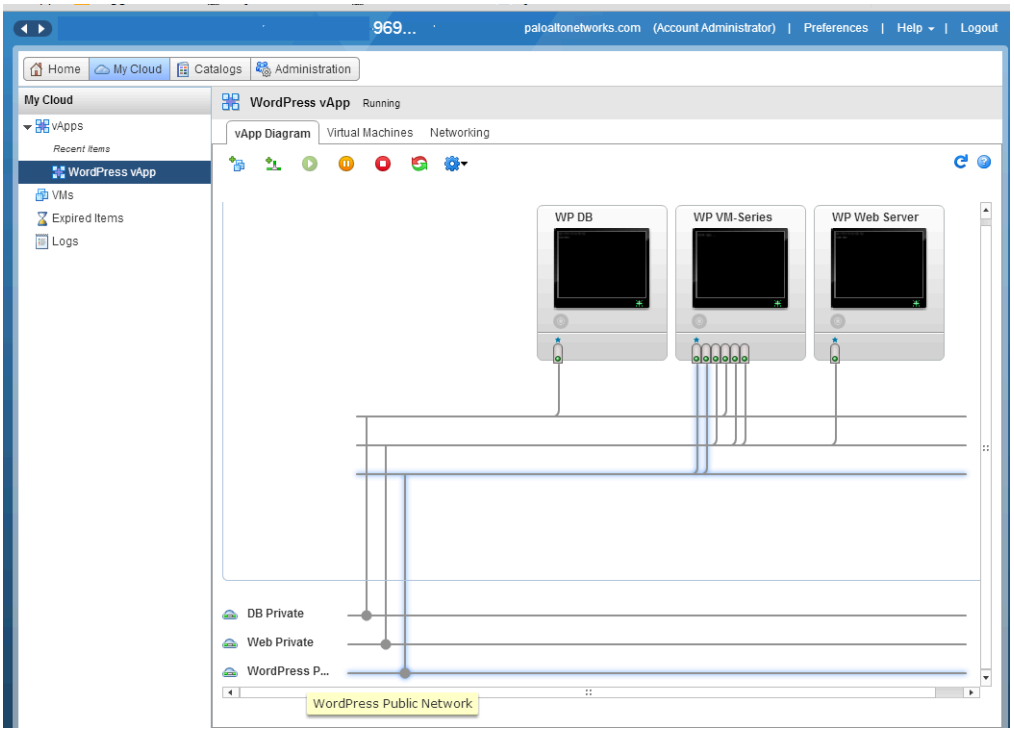
STEP 5 | 将 VM 系列防火墙添加到 vApp 中。

1. 登录到 vCloud Air。
2. 从左窗格中选择您现有的**Virtual Data Center**（虚拟数据中心），右键单击并选择 **Manage Catalogs in vCloud Directorr**（管理 **vCloud Director** 中的编录）。您将重定向至 vCloud Director 的 Web 接口。
3. 选择 **My Cloud**（我的云） > **vApp**，然后单击要将 VM 防火墙纳入其中的 vApp 的 **Name**（名称）。
4. 打开 vApp（双击名称），选择 **Virtual Machines**（虚拟机），然后单击 ✚ 以添加虚拟机。
   1. 在 **Look in:**（查看：）下拉列表中，选择 **My Organization’s Catalog**（我的组织编录），然后选择 VM 系列防火墙映像并单击 **Add**（添加）。单击 **Next**（下一步）。
   2. 单击 **Next**（下一步）以跳过 **Configure Resources**（配置资源）。VM 系列防火墙使用 **Standard**（标准）选项，您无需修改存储策略。
   3. 为防火墙和管理访问 **(NIC 0)** 输入 **Name**（名称），选择默认路由网络和 **IP Mode**（**IP** 模式）— 静态或 DHCP。您可以配置 NIC 1 并在步骤 6 中添加额外的 NIC。单击 **Next**（下一步）。
   4. 验证此 vApp 如何连接至 vDC（此 vApp 中虚拟机的网关地址和网络掩码）。
   5. 验证已添加 VM 系列防火墙，然后单击 **Finish**（完成）。
   6. 继续转到步骤 6。

©2024 Palo Alto Networks, Inc.

STEP 6 | 根据部署要求，将 VM 系列防火墙的数据接口连接至已隔离或已路由的网络。

1. 在 vCloud Director 中，选择 **My Cloud**（我的云）> **vApp**，然后选择刚才创建或编辑的 vApp。
2. 选择 **Virtual Machines**（虚拟机），然后选择 VM 系列防火墙。再右键单击并选择 **Properties**（属性）。
3. 选择 **Hardware**（硬件），滚动至“NIC”部分，然后选择 **NIC 1**。
4. 根据您的连接所需流入 VM 系列防火墙的数据流量，将数据平面网络接口附加至 vApp 网络或组织的 VDC 网络。如需创建新网络，请执行以下操作：
   1. 在 Network（网络）下拉列表中，单击 **Add Network**（添加网络）。
   2. 选择 **Network Type**（网络类型）并为其提供一个名称，然后单击 **OK**（确定）。
   3. 验证新网络是否已附加至接口。
5. 如需将其他 NIC 添加至防火墙，请单击 **Add**（添加），然后重复执行上述步骤 4 中的操作。您最多可附加 7 个数据面板接口至 VM 系列防火墙。
6. 验证 VM 系列防火墙的管理接口是否已附加至 vDC 上的默认路由子网，且至少一个数据面板接口已连接至已路由或已独立的网络。
   1. 选择 **My Cloud**（我的云）> **vApp**，然后双击刚才编辑的 vApp 的 **Name**（名称）。
   2. 在 **vApp Diagram**（**vApp** 图）中验证网络连接。

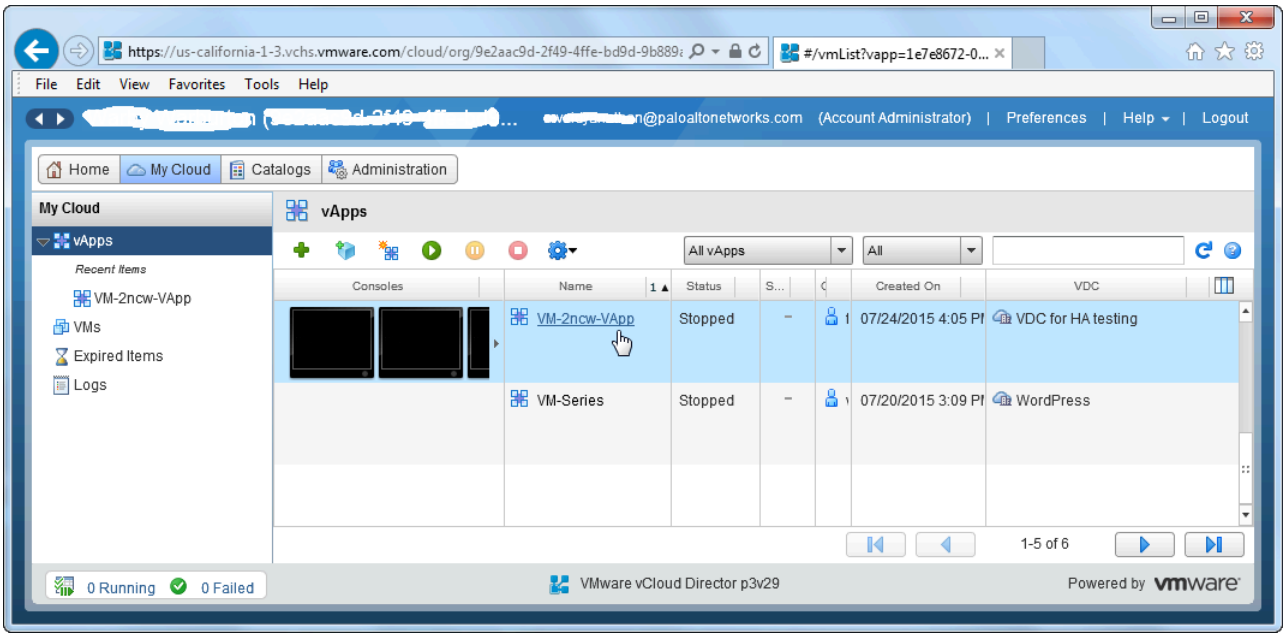


 ©2024 Palo Alto Networks, Inc.

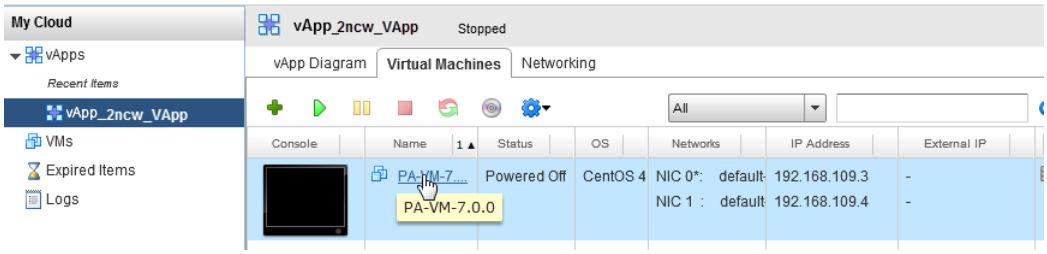
STEP 7 | （可选）编辑为 VM 系列防火墙分配的硬件资源。

仅当您需要分配额外的 CPU、内存或硬盘至防火墙时，才需进行此操作。

1. 选择 **My Cloud**（我的云）> **vApp**，然后双击刚才部署的 vApp 的 **Name**（名称）。



2. 选择 **Virtual Machine**（虚拟机），单击 VM 系列防火墙的 **Name**（名称）以访问虚拟机属性。



3. 为 VM 系列防火墙添加额外的 **Hardware**（硬件）资源：
   - 有关 VM 系列型号的最低 vCPU、内存和磁盘要求，请参阅 VM 系列系统要求。
   - NIC：1 个管理接口，外加至多 7 个数据面板接口。

STEP 8 | 启动 VM 系列防火墙。

STEP 9 | 为 VM 系列防火墙管理接口配置 IP 地址。

在 ESXi 上对 VM 系列防火墙执行初始配置。

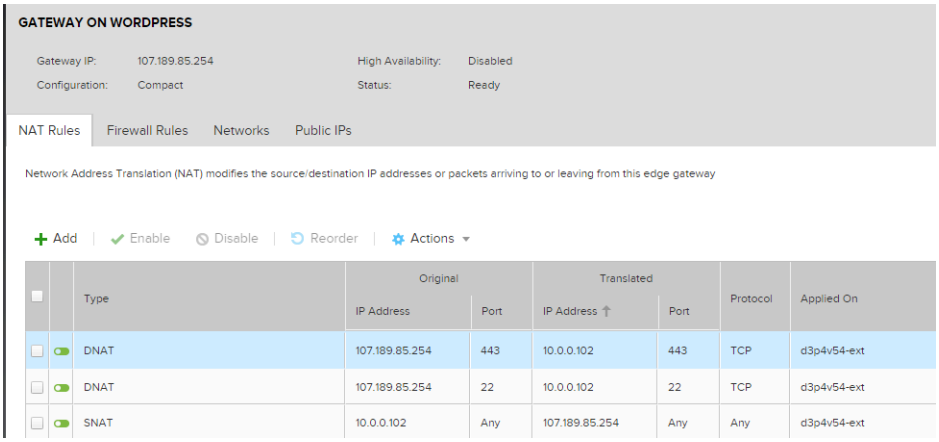
vCloud Air 上的 VM 系列防火墙支持 VMware 工具，您可以通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具查看 VM 系列防火墙的管理 IP 地址。

©2024 Palo Alto Networks, Inc.

STEP 10 | 在 vCloud Air 边缘网关上定义 NAT 规则，为 VM 系列防火墙启用 Internet 访问。

1. 选择 **Virtual Data Centers**（虚拟数据中心）> **Gateways**（网关），然后选择网关并双击以添加 **NAT Rules**（**NAT** 规则）。
2. 创建两个 DNAT 规则。一个用于允许 SSH 访问，另一个用于 HTTPS 访问 VM 系列防火墙上的管理端口的 IP 地址。
3. 创建 SNAT 规则用于为所有从 VM 系列防火墙上的管理端口对内部 IP 地址发起的流量转换内源 IP 地址。

如需发送、接收来自防火墙上的数据面板接口的流量，您必须在 *vCloud Air* 边缘网关上创建其他 *DNAT* 和 *SNAT* 规则。



STEP 11 | 登录防火墙的 Web 界面。

在本示例中，Web 界面的 URL 为 https://107.189.85.254

边缘网关上的 NAT 规则会将外部 IP 地址和端口 107.189.85.254:443 转换至专用 IP 地址和端口 10.0.0.102:443。

STEP 12 | 在防火墙上添加授权代码以激活许可证。

激活许可证。

STEP 13 | 配置 VM 系列防火墙以使用虚拟机监控程序分配的 MAC 地址。

虚拟机监控程序分配的 MAC 地址

©2024 Palo Alto Networks, Inc.

STEP 14 | 配置数据面板网络接口作为第 3 层接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - 接口类型：**Layer3**
   - 选择 **Config**（配置）选项卡，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，选择 **Security Zone**（安全区域）下拉列表中的 **New Zone**（新建区域）。定义新区域（如 untrust），然后单击 **OK**（确定）。
   - 选择 **IPv4**，分配静态 IP 地址。
   - 选择 **Advanced**（高级） > **Other Info**（其他信息），展开 **Management Profile**（管理配置文件）下拉列表，然后选择 **New Management Profile**（新建管理配置文件）。
   - 输入配置文件的 **Name**（名称）（如 allow_ping），并从允许的服务列表中选择 Ping，然后单击 **OK**（确定）。
   - 要保存接口配置，请单击 **OK**（确定）。
3. 对于各附加接口，请重复执行此流程。
4. 单击 **Commit**（提交）以保存更改。

 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 VMware NSX-T 上设置 VM 系列防火墙

VM 系列防火墙可以部署在 VMware NSX-T 上以保护南向北和东向西流量。

- 在 VMware NSX-T 上设置 VM 系列防火墙（北向南）
- 在 NSX-T 上设置 VM 系列防火墙（东向西）

在 VMware NSX-T 上设置 VM 系列防火墙（北向南）

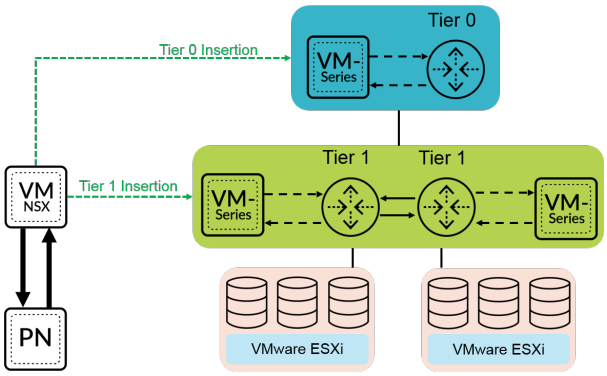
VMware NSX-T 上的 VM 系列防火墙将 Palo Alto 下一代防火墙和 Panorama 与 ESXi 主机服务器集成在一起，为 NSX-T 软件定义数据中心中的所有北向南流量提供全面的可见性和安全应用程序支持。

以下主题提供有关 VMware NSX-T 上 VM 系列防火墙的信息：

- VMware NSX-T 上支持的 VM 系列防火墙部署（北向南）
- NSX-T 上 VM 系列防火墙的组件（北向南）
- 在 NSX-T 上部署 VM 系列防火墙（北向南）
- 将安全策略从 NSX-V 扩展到 NSX-T

VMware NSX-T 上支持的 VM 系列防火墙部署（北向南）

您可以将一个或多个 VM 系列防火墙实例部署为 VM ware NSX-T 数据中心中的合作伙伴服务。将 VM 系列防火墙连接到任何第 0 层或第 1 层逻辑路由器，以保护北向南流量。您可以将 VM 系列防火墙部署为独立服务实例，也可以将两个防火墙部署在高可用性 (HA) 对中。Panorama 管理与 NSX-T Manager 和 NSX-T 软件定义数据中心中部署的 VM 系列防火墙的连接。



- 第 0 层插入 — 第 0 层插入 将 VM 系列防火墙部署到第 0 层逻辑路由器，该路由器处理逻辑和物理网络之间的流量。部署具有第 0 层插入的 VM 系列防火墙时，NSX-T Manager 使用您在 Panorama 上配置的部署信息将防火墙连接到虚拟线路模式的第 0 层逻辑路由器。
- 第 1 层插入 — 第 1 层插入将 VM 系列防火墙部署到第 1 层逻辑路由器，该路由器提供到段的下行链路连接和到 0 层逻辑路由器的上行链路连接。NSX-T Manager 将部署了第 1 层插入的 VM 系列防火墙连接到虚拟线路模式的第 1 层逻辑路由器。

部署防火墙后，您可以配置流量重定向规则，以便在穿过第 0 层或第 1 层路由器时将流量发送到 VM 系列防火墙。您在 Panorama 上配置的安全策略规则将推送到托管 VM 系列防火墙，然后应用于通过防火墙的流量。

NSX-T 上 VM 系列防火墙的组件（北向南）

下表显示了 Palo Alto Networks 和 VMware NSX-T 联合解决方案的组件。

©2024 Palo Alto Networks, Inc.

VMware 组件	
vCenter/ESXi	vCenter 服务器是 vSphere 套件的集中式管理工具。ESXi 是支持计算虚拟化的虚拟机管理程序。 请参阅 VMware 的兼容性列表，了解 vCenter 与 NSX-T 版本的兼容性。
NSX-T Manager	VMware NSX-T Data Center 2.4.0 及更高版本必须使用 vCenter 服务器进行安装和注册。需要使用 NSX -TManager 才能在 ESXi 集群内的 ESXi 主机上部署 VM 系列防火墙。

Palo Alto Networks 组件	
PAN-OS	部署 VM 系列 NSX-T 版防火墙需要 VM 系列基本映像 (PA-VM-NST-9.1.zip)。 在 ESXi 服务器上部署 NSX 的 VM 系列防火墙的最低系统要求取决于 VM 系列型号。有关 VM 系列型号的最低硬件要求，请参阅VM 系列型号。
Panorama Panorama 必须运行与用于管理防火墙的版本相同或更高的版本。	VM 系列 NSX-T 版防火墙需要 Panorama 9.1 或更高版本。 Panorama 是 Palo Alto Networks 下一代防火墙的集中式管理工具。在此解决方案中，Panorama 协同 NSX-T Manager 一起部署、许可和集中管理 NSX-T 的 VM 系列防火墙的配置和策略。 Panorama 必须连接到 NSX-T Manager、VM 系列防火墙和 Palo Alto Networks 更新服务器。 有关部署 Panorama 设备的信息，请参阅 Panorama 管理员指南。
适用于 VMware NSX 的 Panorama 插件	3.0.0 或更高版本
VM 系列插件	1.0.6 或更高版本
VM 系列防火墙	• 软件 NGFW 积分：多达 64 个 vCPU • 模型：VM-100、VM-300、VM-500 和 VM-700

©2024 Palo Alto Networks, Inc.

在 NSX-T 上部署 VM 系列防火墙（北向南）

完成以下任务以使用 VM 系列防火墙保护 NSX-T 环境中的北向南流量。

对于以下过程，请参阅 *NSX-T Manager 3.0*

。

- 安装适用于 VMware NSX 的 Panorama 插件
- 启用 NSX-T Manager 与 Panorama 之间的通信
- 在 Panorama 上创建模板堆栈和设备组
- 在 Panorama 上配置服务定义
- 部署 VM 系列防火墙
- 将流量定向到 VM 系列防火墙
- 将安全策略应用到 VM 系列 NSX-T 版防火墙
- 使用 vMotion 在主机之间移动 VM 系列防火墙

安装适用于 **VMware NSX** 的 **Panorama** 插件

下载和安装适用于 VMware NSX 的 Panorama 插件。安装或升级插件之前，请参阅兼容性矩阵。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 Panorama HA 对中安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 选择 **Panorama** > **Plugins**（插件）。安装或升级插件之前，请参阅兼容性矩阵。

©2024 Palo Alto Networks, Inc.

STEP 2 | 选择**Check Now**（立即检查）以检索可用的更新列表。

STEP 3 | 在操作列中选择 **Download**（下载）以下载插件。

STEP 4 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

启用 NSX-T Manager 与 Panorama 之间的通信

完成以下过程可启用 Panorama 与 NSX-T Manager 之间的通信。您最多可以将 Panorama 连接到 16 个 NSX-T Manager。如果您要将 Panorama 连接到多个 NSX-T Manager，则必须仔细规划设备组层次结构和模板堆栈，并考虑它们如何与部署所需的其他组件进行交互。服务定义引用设备组和模板堆栈，并将该信息推送到相关 ESXi 集群中的防火墙。

STEP 1 | （可选）对于 Panorama 与 NSX-T Manager 之间的通信，绕过代理服务器设置，在 Panorama 下配置 **Panorama** > **Setup**（设置） > **Services**（服务） > **Proxy Server**（代理服务器）。此命令允许 Panorama 与 NSX-T Manager 直接通信，同时保持其他服务的代理通信。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令以启用或禁用代理绕过。

   ```
   admin@Panorama> request plugins vmware_nsx global proxy bypass {yes | no}
   ```

   选择 **Yes**（是）可启用代理绕过，选择 **No**（否）可禁用代理绕过。默认将此选项设置为 **No**（否）。

STEP 2 | 登录到 Panorama Web 界面。

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

STEP 3 | 设置对 NSX-T Manager 的访问权限。对连接 Panorama 的每个 NSX-T Manager 重复执行此程序。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器），然后单击 **Add**（添加）。
2. 输入 NSX-T Manager 的描述性 **Name**（名称）。
3. （可选）添加 NSX-T Manager 的 **Description**（说明）。
4. 输入用于访问 NSX-T Manager 的 **NSX Manager URL** — NSX-T Manager 集群虚拟 IP 地址或 FQDN。
5. 输入 **NSX Manager Login**（**NSX Manager** 登录）凭据（用户名和密码），以使 Panorama 可以对 NSX-T Manager 执行身份验证。
6. 单击 **OK**（确定）。

如果更改 *NSX-T Manager* 登录密码，则必须立即更新 *Panorama* 上的密码。密码错误会中断 *Panorama* 与 *NSX-T Manager* 之间的连接。

©2024 Palo Alto Networks, Inc.

STEP 4 | 将更改提交到 Panorama。

单击 **Commit**（提交） 和 **Commit to Panorama**（提交到 **Panorama**）。

STEP 5 | 验证 Panorama 上的连接状态。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器）。
2. 验证 **Status**（状态）列中的消息。

   连接成功时，状态显示为 **Registered**（已注册）。这表示 Panorama 与 NSX-T Manager 处于同步状态。

   失败状态消息为：

   - **No connection**（无连接）：无法连接到 NSX-T Manager 或建立与 NSX-T Manager 的网络连接。
   - **Invalid Credentials**（无效凭据）：访问凭据（用户名和/或密码）不正确。
   - **Out of sync**（不同步）：Panorama 上定义的配置设置与 NSX-T Manager 上定义的不同。单击该链接了解失败的具体原因。例如，NSX-T 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-T Manager 上的服务定义。在 Panorama 和 NSX-T Manager 未同步之前，您无法在 Panorama 上添加新的服务定义。
   - **Connection Disabled**（连接已禁用）：手动禁用 Panorama 与 NSX-T Manager 之间的连接。

在 Panorama 上创建模板堆栈和设备组

要使用 Panorama 在 NSX-T 上管理 VM 系列防火墙，这些防火墙必须属于某设备组和模板堆栈。设备组可让您将需要相似策略和对象的防火墙组合为一个逻辑单位；在 Panorama 上可使用 **Objects**（对象）和 **Policies**（策略）选项卡定义此配置。使用模板堆栈来配置 VM 系列防火墙在网络上运行所需的设置；在 Panorama 上可使用 **Device**（设备）和 **Network**（网络）选项卡定义此配置。NSX-T 配置中使用的每个模板堆栈都必须与服务定义相关联。

部署在 NSX-T 中的防火墙具有采用 Virtual Wire 模式配置的两个默认区域和两个接口。Ethernet1/1 是 **south**（南）区域的一部分，ethernet1/2 是 **north**（北）区域的一部分。要将策略规则从 Panorama 推送到托管防火墙，您必须在 Panorama 的相应模板堆栈中配置与防火墙上的区域和接口匹配的区域和接口。

STEP 1 | 添加设备组或设备组层级。

1. 选择 **Panorama** > **Device Groups**（设备组），然后单击 **Add**（添加）。您还可以创建一个设备组层级。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识设备组。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

©2024 Palo Alto Networks, Inc.

STEP 2 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识模板。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

STEP 3 | 创建模板堆栈。

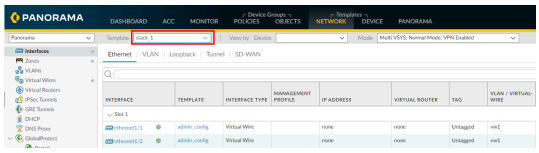
1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add Stack**（添加堆栈）。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识模板。
3. 单击 **Add**（添加）以添加您之前创建的模板。
4. 单击 **OK**（确定）。
5. 单击 **Commit**（提交），然后选择 **Commit to Panorama**（提交到 **Panorama**）以将更改保存到 Panorama 上正在运行的配置。

STEP 4 | 配置 Virtual Wire、接口和区域。确保从下面显示的下拉列表中选择正确的模板。您创建的对象必须满足以下条件：

如果您更改默认 *Virtual Wire* 或区域名称，则 *Panorama* 上的 *Virtual Wire* 和区域必须与防火墙上使用的名称匹配。

- 使用 **ethernet1/1** 和 **ethernet1/2**。
- Virtual Wire 对象名为 **vw1**。
- 第一个区域名为 **south**（南），类型为 **virtual-wire**，并包含 **ethernet1/1**。
- 第二个区域名为 **north**（北），类型为 **virtual-wire**，并包含 **ethernet1/2**。

为部署中的每个模板重复此过程。



STEP 5 | 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

©2024 Palo Alto Networks, Inc.

STEP 6 | 更新模板堆栈的 DNS 和 NTP 服务器信息。如果您在部署中使用设备证书，则必须完成此步骤。这是确保在 NSX-T 环境中部署的防火墙具有访问设备证书服务器所需的正确 DNS 信息所必需的。

1. 验证您是否从 **Template**（模板）下拉列表中指定正确的模板堆栈。
2. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后单击 **Edit**（编辑）图标。
3. 在 Services（服务）选项卡上，输入 **Primary DNS Server**（主 **DNS** 服务器）和 **Secondary DNS Server**（辅助 **DNS** 服务器）的 IP 地址。
4. 在 NTP 选项卡上，输入 **NTP Server**（**NTP** 服务器）的 IP 地址。
5. 单击 **OK**（确定）。
6. 将更改 **Commit**（提交）到 Panorama。

在 Panorama 上配置服务定义

服务定义用于指定在 NSX-T 数据中心环境中安装的 VM 系列防火墙的配置。服务定义必须包括设备组、模板堆栈和 OVF URL。

STEP 1 | 添加一个新的服务定义。

在 *Panorama* 上，您最多可创建 *32* 个服务定义。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（服务定义）。
2. 选择 **Add**（添加）以创建新服务定义。
3. 输入服务定义的描述性 **Name**（名称）。
4. （可选）添加 **Description**（说明），用以识别将通过该服务定义进行部署的 VM 系列防火墙的功能或目的。

STEP 2 | 为该服务定义分配一个设备组和模板堆栈。

确保 在 Panorama 上创建模板堆栈和设备组。

由于使用此解决方案部署的防火墙将在 Panorama 中集中管理，因此必须指定防火墙所属的 **Device Group**（设备组）和 **Template Stack**（模板堆栈）。使用该服务定义部署的所有防火墙均属于指定的模板堆栈和设备组。

1. 在 **Device Group**（设备组）下拉列表中选择设备组或设备组层级。
2. 选择 **Template**（模板）下拉列表中的模板堆栈。

   您无法重复使用已在另一个服务定义中分配给某个服务定义的模板堆栈或设备组。

©2024 Palo Alto Networks, Inc.

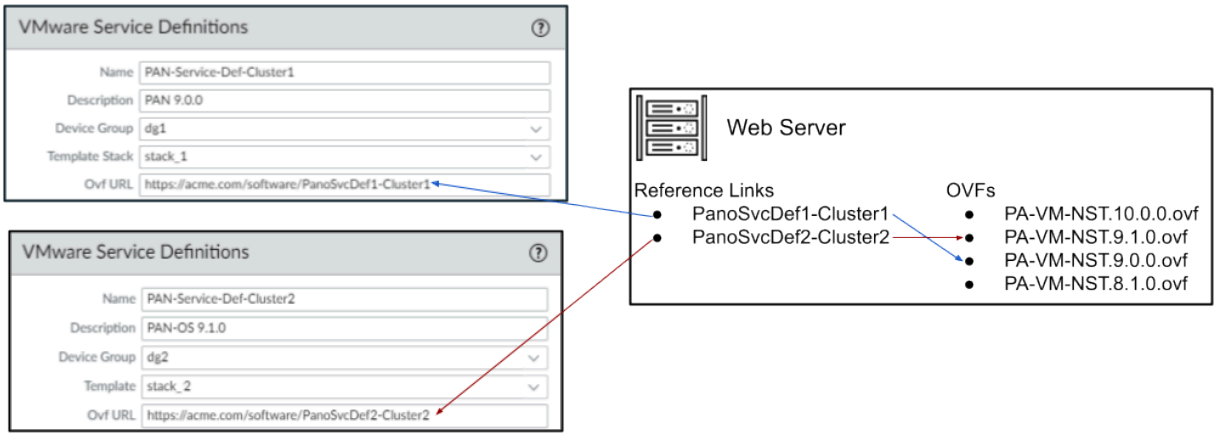
STEP 3 | 指定 OVF 文件的位置。

下载 zip 文件，将其解压缩以提取并将.ovf，mf 和 .vmdk 文件保存到同一目录。ovf 和 vmdk 文件均用于部署防火墙的每个实例。

如果需要，可以修改服务器的安全设置，以便下载文件类型。例如，在 IIS 服务器上，可以修改 Mime Types （Mime 类型）配置；在 Apache 服务器上，可以编辑 .htaccess 文件。

在 *VM* 系列防火墙的 *NSX* 服务部署成功后，请勿更改 *Panorama* 服务定义 *OVF* 路径。在成功部署 *VM* 系列防火墙后更改 *OVF* 路径可能会导致 *NSX* 服务部署失败。您可以在 *NSX-T Manager* 中解决此故障，但这可能会导致要重新部署所有 *VM* 系列防火墙。

建议您使用可扩展的 OVF 路径名称，并允许您在不影响部署的防火墙的情况下更改基本映像。请勿使用诸如 **https://acme.com/software/PA-VM-NST.9.1.0.ovf** 之类的路径，而是使用诸如 **https://acme.com/software/PanoSvcDef1-Cluster1.ovf** 之类的路径。使用静态路径引用可消除将来更改 OVF 路径的任何需要。建议您为部署中的每个 Panorama 服务定义（vSphere 集群）创建一个路径，并根据需要更改 Web 服务器上的 PAN-OS 基础映像引用。



在 **OVF URL** 中，添加托管 ovf 文件的 Web 服务器的位置。http 和 https 均为支持协议。

Panorama 必须与 *Web* 服务器建立网络连接才能检索 *OVF* 文件。

对于各个服务定义，您可以使用相同的 ovf 版本，也可以使用不同的版本。如果对各个服务定义使用不同的 ovf 版本，则可以在不同 ESXi 集群中的 VM 系列防火墙上使用不同的 PAN-OS 版本。

STEP 4 | 为您的防火墙选择 **North South**（北向南）作为 **Insertion Type**（插入类型）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 要在 NSX Manager 部署 VM 系列防火墙时自动检索设备证书，请配置设备证书。

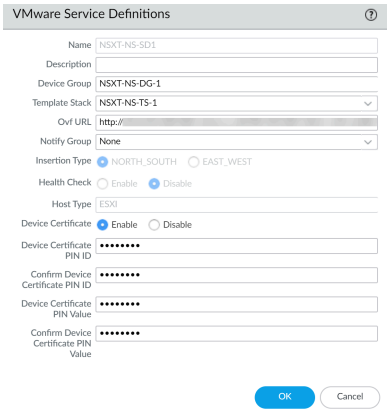
启用此选项可将设备证书应用于新部署的 VM 系列防火墙。只有在使用支持设备证书的基本映像 OVF 部署防火墙时才使用此选项。Panorama 将设备证书信息作为服务定义的一部分推送到 NSX Manager。在 NSX 中部署新防火墙时，启动时将会在防火墙上安装设备证书。

有关支持 VMware NSX 上 VM 系列防火墙的设备证书的 OVF 列表，请参阅 Palo Alto Networks 兼容性矩阵。

如果您的 OVF 支持设备证书，无论您是否使用设备证书，则都必须启用设备证书。如果 OVF 不支持设备证书，请禁用此选项。

1. 如果您尚未安装设备证书，请登录到客户支持门户，并生成注册 PIN 和 PIN ID。
2. 在 **Device Certificate**（设备证书）下，单击 **Enable**（启用）。
3. 复制 PIN ID，然后在 **Device Certificate PIN ID**（设备证书 **PIN ID**）字段中输入该 PIN ID。
4. 在 **Confirm Device Certificate PIN ID**（确认设备证书 **PIN ID**）字段中重新输入该 PIN ID。
5. 复制 PIN 值，然后在 **Device Certificate PIN Value**（设备证书 **PIN** 值）字段中输入该 PIN 值。
6. 在 **Confirm Device Certificate PIN Value**（确认设备证书 **PIN** 值）字段中重新输入该 PIN 值。

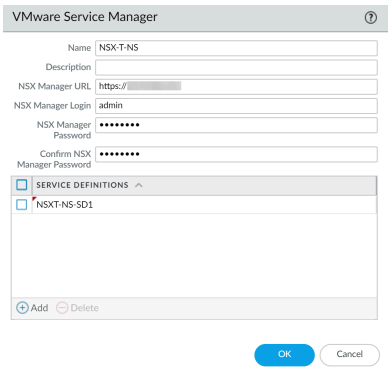
STEP 6 | 单击 **OK**（确定）保存服务定义。



 ©2024 Palo Alto Networks, Inc.

STEP 7 | 将服务定义附加到服务管理器。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Manager**（服务管理器），然后单击服务管理器名称的链接。
2. 在服务定义下，单击 **Add**（添加） 并从下拉列表中选择您的服务定义。
3. 单击 **OK**（确定）。

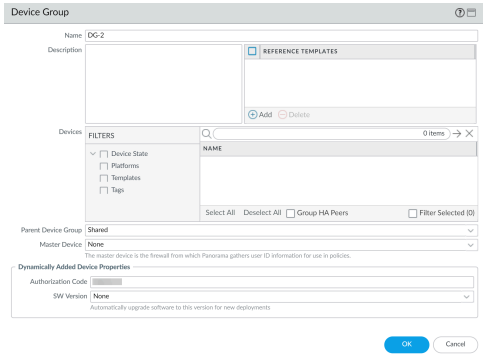


STEP 8 | 将授权代码添加到防火墙的许可证中。

1. 选择 **Panorama** > **Device Groups**（设备组），并选择与刚才创建的服务定义关联的设备组。
2. 在 **Dynamically Added Device Properties**（动态添加的设备属性）下，将您收到的授权代码添加到订单履行电子邮件中，并且可选择性地从 **SW Version**（软件版本）下拉列表中选择 None（无）。

   在 NSX-T 上部署新防火墙时，它将自动添加到设备组，并使用您提供的授权代码进行许可，以及升级到您指定的 PAN-OS 版本。

   在支持门户上，您可以查看经授权部署的防火墙的总数量，以及所用许可证的数量与授权代码启用的许可证的总数量的比率。



STEP 9 | **Commit to Panorama**（提交到 **Panorama**）。

STEP 10 | 在 NSX-T Manager 上，验证服务定义是否可用。

选择 **System**（系统） > **Service Deployments**（服务部署） > **Catalog**（目录）。服务定义作为 NSX-T Manager 上的服务实例列出。

©2024 Palo Alto Networks, Inc.

部署 VM 系列防火墙

完成 Panorama 上的配置后，执行以下过程以在 NSX-T 数据中心中启动 VM 系列防火墙。

在高可用性中的 NSX-T 上部署 VM 系列防火墙后，会将两个防火墙部署到同一设备组和模板堆栈。

STEP 1 | 登录到 NSX-T Manager。

STEP 2 | 选择 **System**（系统） > **Service Deployments**（服务部署） > **Deployment**（部署）。

STEP 3 | 从 **Partner Service**（合作伙伴服务）下拉列表中选择服务定义。

STEP 4 | 单击 **Deploy Service**（部署服务）。

STEP 5 | 输入 VM 系列防火墙的描述性 **Service Deployment Name**（服务部署名称）。

STEP 6 | 在 **Attachment Points**（附加点）下选择第 0 层或第 1 层路由器。NSX-T Manager 将 VM 系列防火墙连接到选定的路由器，并将通过该路由器的流量重定向到 VM 系列防火墙以进行检查。您必须选择未附加服务插入的路由器。

STEP 7 | 选择 **Compute Manager**（计算管理器）。计算管理器是管理数据中心的 vCenter 服务器。

STEP 8 | 选择 **Cluster**（集群）。您可以在不包含任何边缘传输节点的任何集群上部署 VM 系列防火墙。

STEP 9 | 选择 **Datastore**（数据存储）。

STEP 10 | 配置您的网络设置。

1. 在 **Networks**（网络）列中，单击 **Edit Details**（编辑详细信息）。
2. 选择 **Primary Interface Network**（主接口网络）。
3. 输入 **Primary Interface IP**（主接口 **IP** 地址）。
4. 输入 **Primary Gateway Address**（主网关地址）。
5. 输入 **Primary Subnet Mask**（主子网掩码）。
6. 单击 **Save**（保存）。

STEP 11 | NSX-T Manager 会根据您选择的合作伙伴服务预先填写 **Deployment Specification**（部署规范）和 **Deployment Template**（部署模板）。

STEP 12 | 将 **Failure Policy**（故障策略）设置为允许或阻止。故障策略定义了 NSX-T Manager 如何处理在防火墙不可用时定向到 VM 系列防火墙的流量。

STEP 13 | 选择 VM 系列防火墙的 **Deployment Mode**（部署模式） — 独立或高可用性。If you have an edge node cluster and select High Availability, NSX-T Manager will deploy an additional VM-Series firewall on the standby edge node in addition to the firewall deployed on the active edge node.

STEP 14 | 单击 **Save**（保存）以部署 VM 系列防火墙。

 ©2024 Palo Alto Networks, Inc.

STEP 15 | 验证防火墙是否连接到 Panorama。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要）。
3. 确认已在正确的设备组下列出您的防火墙，并且 **Device State**（设备状态）显示 **Connected**（已连接）。

   对于 NSX-T (N-S) 部署，VM 系列防火墙的设备名称在 Panorama 上显示为 **PA-VM:<nsx.clusterid>**，对于 NSX-T (E-W) 部署，则显示为 **PA-VM:<nsx.servicevmid>**。

STEP 16 | 为 VM 系列防火墙上的管理员帐户设置安全密码。

每个 VM 系列防火墙都使用默认用户名和密码 (admin/admin) 来进行初始登录。首次登录时，系统会提示设置一个更安全的新密码。新密码至少包含 8 个字符，其中至少 1 个小写字母和 1 个大写字母以及 1 个数字或特殊字符。

通过 Panorama 可单独更新每个防火墙的密码，也可以一次性更新所有防火墙的密码。

- **Panorama** — 在 Panorama 上，您可以更改模板中所有防火墙的默认密码或删除管理员用户并创建新的用户名和密码。
  1. 登录到 Panorama。
  2. 选择 **Device**（设备） > **Administrators**（管理员），然后选择 **admin** 用户。
  3. **Delete**（删除）用户，或单击用户并输入新密码。
  4. 如果更改了密码，请单击 **OK**（确定）。
  5. 选择 **Commit**（提交） > **Push to Devices**（推送到设备） > **Edit Selections**（编辑选择） > **Force Template Values**（强制模板值）。
  6. 单击 **OK**（确定）。
- 防火墙 — 必须在每个 VM 系列防火墙上重复此过程。
  1. 使用默认用户名和密码登录 VM 系列防火墙。
  2. 按照提示重置密码。

将流量定向到 VM 系列防火墙

完成以下过程以将流量定向到 VM 系列防火墙。对于北向南流量，重定向规则默认无状态且无法更改。此外，NSX-T 将自动为返回流量创建相应的自反规则。

在 HA 模式下为 NSX-T 北向南流量部署 VM 系列防火墙时，必须为两个 HA 对等创建流量重定向规则。此外，还必须为主动对等第一和被动对等第二创建流量重定向规则。

自反规则不会显示在 *NSX-T Web* 界面中。

STEP 1 | 登录到 NSX-T Manager。

STEP 2 | 验证您处于 **Policy**（策略）模式下。

©2024 Palo Alto Networks, Inc.

STEP 3 | 选择 **Security**（安全） > **North South Security**（北向南安全） > **Network Introspection (N-S)**（网络自检 **(N-S)**）。

STEP 4 | 单击 **Add Policy**（添加策略）。

STEP 5 | 输入策略的描述性 **Name**（名称）。

STEP 6 | 从 **Redirect To**（重定向到）下拉列表中选择 VM 系列防火墙服务实例。NSX-T Manager 将根据您选择的服务实例自动填充 **Applied To**（应用到）字段。

STEP 7 | 选择新创建的策略。

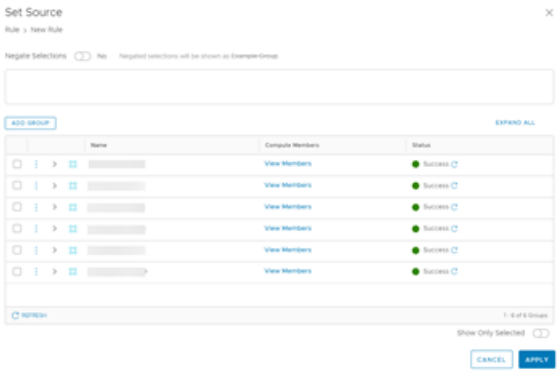
STEP 8 | 单击 **Add Rule**（添加规则）。

如果 *NSX-T* 环境在主动待机 *HA* 中具有边缘节点，则必须为每个边缘节点创建重定向规则。在发生故障转移时，*NSX-T* 不会自动将重定向规则应用于待机节点。

STEP 9 | 单击 **Name**（名称）字段，然后输入规则的描述性名称。

STEP 10 | 默认情况下，源设置为 Any（任何）。完成以下步骤以指定其他源。

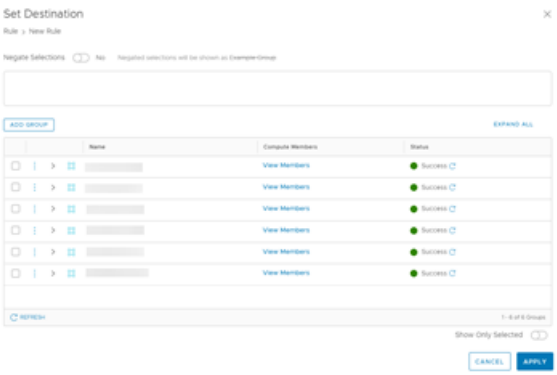
1. 单击 **Source**（源）列中的编辑按钮。
2. 选择一个或多个要设置为 Source（源）的组，或单击 Add Group（添加组）以创建新组。
3. 单击 **Apply**（应用）。



 ©2024 Palo Alto Networks, Inc.

STEP 11 | 默认情况下，目标设置为 Any（任何）。完成以下步骤以指定其他目标。

1. 单击 **Destination**（目标）列中的编辑按钮。
2. 选择一个或多个要设置为 Destination（目标）的组，或单击 Add Group（添加组）以创建新组。
3. 单击 **Apply**（应用）。



STEP 12 | 默认情况下，任何服务都会重定向到防火墙。完成以下步骤以指定某些服务和协议。

1. 单击 **Services**（服务）列中的编辑按钮。
2. 选择一个或多个要设置为 Services（服务）的组，或单击 Add Service（添加服务）以创建新服务。
3. 单击 **Apply**（应用）。

STEP 13 | 从 **Action**（操作）下拉列表中选择 **Redirect**（重定向），将流量发送到 VM 系列防火墙。

STEP 14 | **Enable**（启用）规则。NSX-T Manager 会发布您刚创建的重定向规则，并自动为返回流量创建自反规则。自反规则不会显示在 NSX-T Manager Web 界面中。



STEP 15 | 如果在 HA 中部署 VM 系列防火墙，请为被动 HA 对等创建另一个规则。

如果未将返回流量定向到 *VM* 系列防火墙，请为返回流量手动配置流量重定向规则。

将安全策略应用到 VM 系列 NSX-T 版防火墙

现在，您已部署 VM 系列防火墙并创建了将流量发送到防火墙的流量重定向规则，您可以使用 Panorama 集中管理 VM 系列防火墙上的安全策略规则。

STEP 1 | 登录到 Panorama。

©2024 Palo Alto Networks, Inc.

STEP 2 | 创建安全策略规则。

默认情况下，防火墙会创建允许双向转发检测 *(BFD)* 的规则，不会创建阻止 *BFD* 的规则。如果阻止 *BFD*，*NSX-T* 会认为防火墙不可用。

1. 选择 **Policies**（策略） > **Security**（安全） > **Prerules**（预订规则）。
2. 选择在在 Panorama 上创建模板堆栈和设备组中为 NSX-T 上管理 VM 系列防火墙而创建的 **Device Group**（设备组）。
3. 单击 **Add**（添加），然后为规则输入 **Name**（名称）和 **Description**（说明）。在本示例中，安全规则允许 WebFrontEnd 服务器和应用程序服务器之间的所有流量。
4. 选择 **Source Zone**（源区域）和 **Destination Zone**（目标区域）。
5. 对于 **Source Address**（源地址）和 **Destination Address**（目标地址），选择或键入地址、静态地址组或区域。

   NSX-T 上的 *VM* 系列防火墙不支持北向南流量的动态地址组。

6. 选择允许的 **Application**（应用程序）。在本例中，我们创建 **Application Group**（应用程序组），其中包含已组合在一起的一组静态特定应用程序。
   1. 单击 **Add**（添加），然后选择 **New Application Group**（新建应用程序组）。
   2. 单击 **Add**（添加）以选择要包含到组中的应用程序。
   3. 单击 **OK**（确定）以创建应用程序组。
7. 为流量指定操作（**Allow**（允许）或 **Deny**（拒绝）），（可选）在 Profiles（配置文件）下为防病毒、防间谍软件和漏洞保护附加默认安全配置文件。
8. 单击 **Commit**（提交），然后选择 **Commit to Panorama**（提交到 **Panorama**）。单击 **OK**（确定）。

STEP 3 | 将策略应用到 VM 系列 NSX-T 版防火墙。

1. 单击 **Commit**（提交） > **Push to Devices**（推送到设备） > **Edit Selections**（编辑选择）。
2. 选择设备组，然后单击 **OK**（确定）。
3. 选择 **Force Template Values**（强制模板值）。默认情况下，Panorama 不会使用 Panorama 上共享名称的对象覆盖防火墙上的对象。您必须选择 Force Template Values（强制模板值）以将策略推送到托管防火墙。
4. 单击 **Yes**（是）以确认强制模板值。
5. 单击 **OK**（确定）。
6. 验证提交是否成功。

STEP 4 | （可选）使用模板推送网络的基本配置和设备配置，例如 DNS 服务器、NTP 服务器、Syslog 服务器和登录提示。

有关使用模板的信息，请参阅《Panorama 管理员指南》。

 ©2024 Palo Alto Networks, Inc.

使用 vMotion 在主机之间移动 VM 系列防火墙

要在使用 vMotion 在 VMware NSX-T 中具有同构 CPU 配置的 ESXi 主机之间移动 VM 系列防火墙时保持流量，必须在 vMotion 期间使用 PAN-OS CLI 暂停 VM 系列防火墙的内部检测信号监控。您可以指定暂停检测信号监控的时间（以分钟为单位）。最多可以将检测信号监控暂停 60 分钟。当暂停间隔结束或您故意结束暂停间隔，则检测信号监控将恢复。

如果 ESXi 主机具有同构 CPU 配置，则在 6.5、6.7 和 7.0 上支持 VM 系列防火墙的 vMotion。

如果运行 *vSphere 7.0* 或更高版本，则在使用 *vMotion* 移动 *VM* 系列防火墙时不需要执行此过程。

STEP 1 | 登录到 VM 系列防火墙 CLI。

STEP 2 | 使用以下命令设置检测信号监控暂停间隔。一旦执行命令，暂停就开始。如果 vMotion 所用时间比预期更长，则可以重新运行此命令以设置一个更长的新间隔，该间隔从再次执行命令时开始。

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

您可以使用以下命令查看暂停间隔中的剩余时间。

```
request system heartbeat-pause show interval
```

STEP 3 | （可选）如果在暂停间隔过去之前完成 vMotion，则可以通过将间隔设置为零 (0) 以结束暂停。

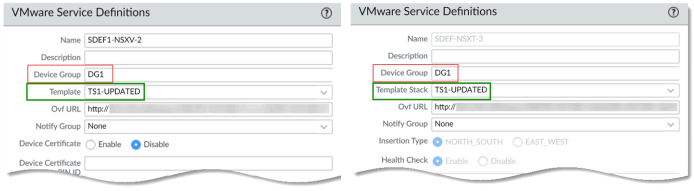
```
request system heartbeat-pause set interval 0
```

将安全策略从 NSX-V 扩展到 NSX-T

如果您要从 NSX-V 部署迁移到 NSX-T 部署，或将 NSX-T 部署与 NSX-V 部署进行组合，则可以将现有安全策略从 NSX-V 扩展到 NSX-T，而无需重新创建安全策略规则。这可以通过利用现有设备组并在 NSX-V 和 NSX-T 服务定义之间进行共享来实现。将安全策略迁移到 NSX-T 后，您可以继续为 NSX-V 使用 VM 系列或删除 NSX-V 部署。

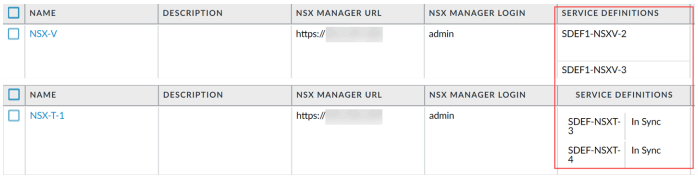
STEP 1 | 安装适用于 VMware NSX 的 Panorama 插件 3.2.0 或更高版本。在升级之前，请参阅适用于 VMware NSX 3.2.0 的Panorama 插件发行说明。

STEP 2 | 为部署中的每个 NSX-V 服务定义定义 NSX-T 服务定义。不创建新的设备组；而是使用现有的 NSX-V 设备组。使用现有设备组，您可以将 NSX-V 上使用的同一安全策略规则应用于 NSX-T 上部署的 VM 系列防火墙。如果您拥有引用特定区域的策略，请将同一模板堆栈从 NSX-V 服务定义添加到 NSX-T 服务定义。此外，如果设备组引用特定模板，请确保选择包括该设备组中引用的模板的模板堆栈。



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 配置 NSX-T 服务管理器，并将 NSX-T 服务定义与服务管理器相关联。

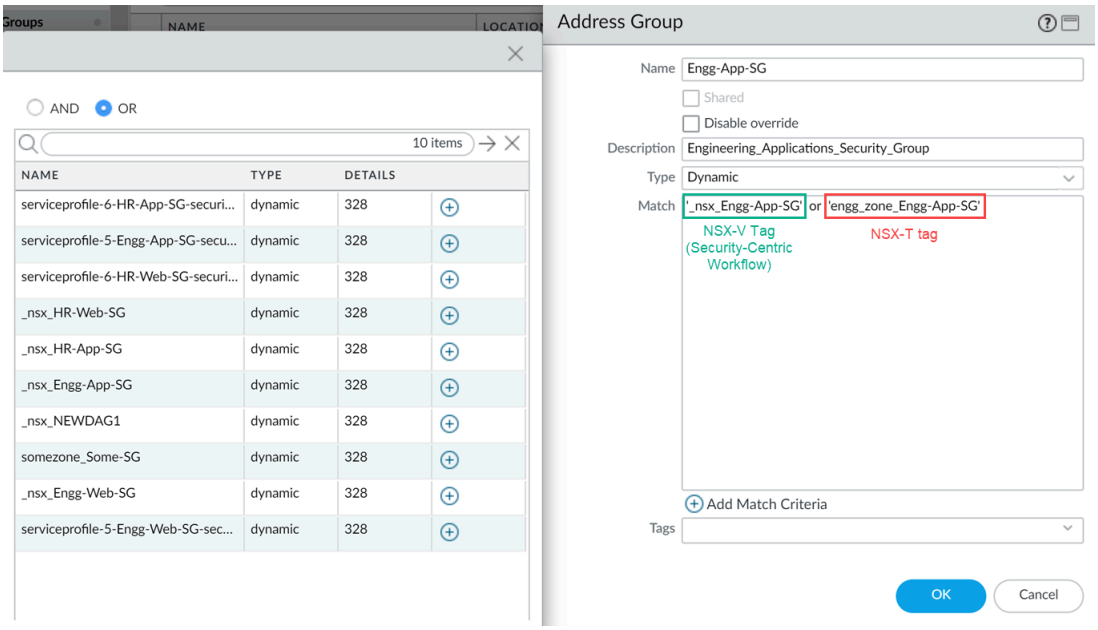


STEP 4 | 准备 NSX-T 环境并部署 VM 系列防火墙。在启动 VM 系列防火墙之前，您必须创建安全组、服务链和流量重定向策略。

- 在 NSX-T 上部署 VM 系列防火墙（北向南）
- 使用以操作为中心的工作流程部署 VM 系列

STEP 5 | 将 NSX-T 标记添加到现有的动态地址组。

1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
2. 单击现有 NSX-V 动态地址组的名称。
3. 单击 **Add Match Criteria**（添加匹配条件）以显示 NSX-V 和 NSX-T 的标记。
4. 将 NSX-T 标记添加到动态地址组。确保在标记之间使用 **OR** 运算符。
5. 添加所有必需的标记后，单击 **OK**（确定）。
6. **Commit**（提交）更改。



STEP 6 | 将 VM 工作负载成功从 NSX-V 迁移到 NSX-T 后，如果您计划停止使用 NSX-V，则可以从动态地址组删除 NSX-V 标记。从适用于 NSX 的 Panorama 插件删除所有与 NSX-V 相关的信息，以及从 NSX-V Manager 删除 VM 系列防火墙配置后，将取消注册所有 NSX-V 标记和相应的 IP 地址。

©2024 Palo Alto Networks, Inc.

在 NSX-T 上设置 VM 系列防火墙（东向西）

VMware NSX-T 上的 VM 系列防火墙将 Palo Alto 下一代防火墙和 Panorama 与 ESXi 主机服务器集成在一起，为 NSX-T 软件定义数据中心中的所有东向西流量提供全面的可见性和安全应用程序支持。

- NSX-T 上 VM 系列防火墙的组件（东向西）
- NSX-T 集成上的 VM 系列防火墙（东向西）
- VMware NSX-T 上支持的 VM 系列防火墙部署（东向西）
- 使用以操作为中心的工作流程部署 VM 系列
- 使用以安全为中心的工作流程部署 VM 系列
- 从 Panorama 中删除服务定义
- 从 NSX-T 操作上的 VM 系列迁移到以安全为中心的部署
- 将安全策略从 NSX-V 扩展到 NSX-T
- 使用就地迁移将 VM 系列从 NSX-V 迁移到 NSX-T

NSX-T 上 VM 系列防火墙的组件（东向西）

下表显示了 Palo Alto Networks 和 VMware NSX-T（东向西）联合解决方案的组件。

VMware 组件	
vCenter/ESXi	vCenter 服务器是 vSphere 套件的集中式管理工具。ESXi 是支持计算虚拟化的虚拟机管理程序。 请参阅 VMware 的兼容性列表，了解 vCenter 与 NSX-T 版本的兼容性。
NSX-T Manager	VMware NSX-T Data Center 2.5.0 及更高版本必须使用 vCenter 服务器进行安装和注册。需要使用 NSX -TManager 才能在 ESXi 集群内的 ESXi 主机上部署 VM 系列防火墙。

Palo Alto Networks 组件	
PAN-OS	PAN-OS 10.1.x 及更高版本。 在 NSX-T 上部署 VM 系列防火墙需要 VM 系列基本映像，例如 PA-VM-NST-10.1.0zip。

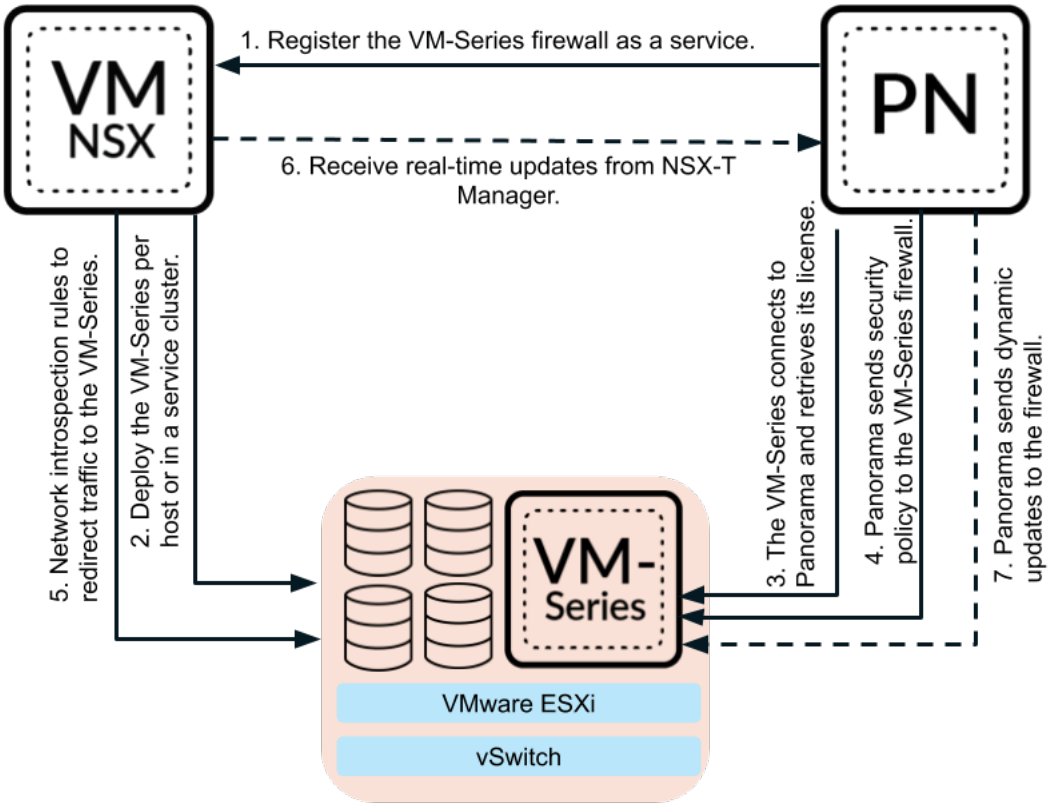
©2024 Palo Alto Networks, Inc.

Palo Alto Networks 组件	
	在 ESXi 服务器上部署 NSX 的 VM 系列防火墙的最低系统要求取决于 VM 系列型号。有关 VM 系列型号的最低硬件要求，请参阅VM 系列型号。
Panorama Panorama 必须运行与用于管理防火墙的版本相同或更高的版本。	NSX-T 上的 VM 系列防火墙要求运行 10.1.0 的防火墙需要 Panorama 10.1.0 及更高版本 Panorama 是 Palo Alto Networks 下一代防火墙的集中式管理工具。在此解决方案中，Panorama 协同 NSX-T Manager 一起部署、许可和集中管理 NSX-T 的 VM 系列防火墙的配置和策略。 Panorama 必须连接到 NSX-T Manager、VM 系列防火墙和 Palo Alto Networks 更新服务器。 有关部署 Panorama 设备的信息，请参阅《11.0 Panorama 管理员指南》。
适用于 VMware NSX 的 Panorama 插件	3.1.0 或更高版本 4.0.0 或更高版本，用于以安全为中心的工作流程
VM 系列插件	1.0.8 或更高版本
VM 系列防火墙型号	VM-100、VM-300、VM-500 和 VM-700 支持 NSX-T。 在 *NSX-T* 上部署 *VM* 系列防火墙之前，请确保您有足够的硬件资源支持所选部署模式（服务集群或每个主机）中的 *VM* 系列防火墙数量。这在部署大型防火墙（例如 *VM-700*）时至关重要。

NSX-T 集成上的 VM 系列防火墙（东向西）

NSX-T Manager、vCenter、Panorama 和 VM 系列防火墙可以共同协作解决 NSX-T 数据中心的安全挑战。

©2024 Palo Alto Networks, Inc.



1. 将 **VM** 系列防火墙注册为服务 — 使用 Panorama 连接到 VMware NSX-T Manager。Panorama 使用 NSX-T API 与 NSX-T Manager 通信，并建立双向通信。在 Panorama 上，您可以通过输入 NSX-T Manager 的 IP 地址、用户名和密码配置服务管理器，以启动通信。

   与 NSX-T Manager 建立通信后，可以配置服务定义。服务定义包括 VM 系列防火墙基本映像的位置，许可 VM 系列防火墙所需的授权代码，以及防火墙所属的设备组和模板堆栈。

   此外，NSX-T Manager 使用此连接通过 Panorama 发送有关 NSX-T 环境中变化的更新。
2. 在每个主机或服务集群中部署 **VM** 系列防火墙 — NSX-T Manager 使用在服务定义中从 Panorama 推送的信息部署 VM 系列防火墙。选择要部署 VM 系列防火墙的位置（在服务集群中或每个 ESXi 主机上），以及 NSX-T 如何为 VM 系列防火墙提供管理 IP 地址（DHCP 或静态 IP）。当防火墙启动时，NSX-T Manager 的 API 会将 VM 系列防火墙连接到虚拟机监控程序，以便可以从 vSwitch 接收流量。

©2024 Palo Alto Networks, Inc.

3. **VM** 系列防火墙连接到 **Panorama** — VM 系列防火墙然后连接到 Panorama 以获取其许可证。Panorama 从 Palo Alto Networks 更新服务器获取许可证，并将其发送到防火墙。防火墙获取其许可证后，将重新启动并返回序列号。

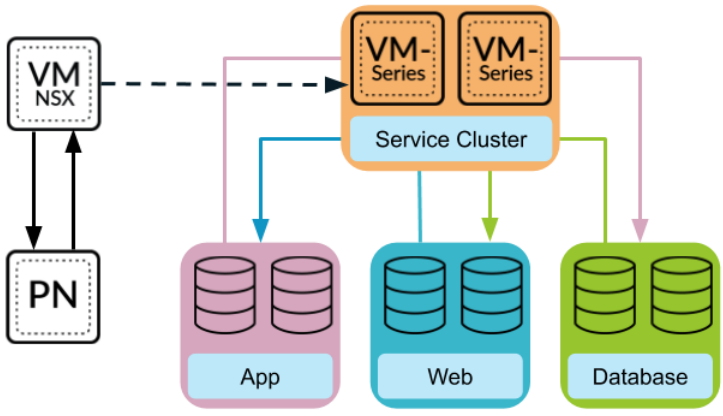
   如果 *Panorama* 无法访问 *Internet*，则无法获取许可证并将其推送到防火墙，因此您必须分别手动许可每个防火墙。如果 *VM* 系列防火墙无法访问 *Internet*，则必须手动将序列号添加到 *Panorama* 以将其注册为托管设备，以便 *Panorama* 可以推送模板堆栈、设备组和其他配置信息。有关详细信息，请参阅激活 VMware NSX 的 VM 系列防火墙的许可证（独立版本）。

4. **Panorama** 将安全策略发送到 **VM** 系列防火墙 — 防火墙重新连接到 Panorama 后，也会将其添加到在服务定义中定义的设备组和模板堆栈，并且 Panorama 将适当的安全策略推送到该防火墙。现在，防火墙已准备就绪，可以保护 NSX-T 数据中心中的流量。
5. 创建网络自检规则以将流量重定向到 **VM** 系列防火墙 — 在 NSX-T Manager 上，创建服务链和网络自检规则，以重定向 NSX-T 数据中心中的流量。
6. 从 **NSX-T Manager** 发送实时更新 — NSX-T Manager 将有关虚拟环境变化的实时更新发送到 Panorama。这些更新包括将流量发送到 VM 系列防火墙的组中虚拟机的组成员和 IP 地址的变化。
7. **Panorama** 发送动态更新 — 当 Panorama 从 NSX-T Manager 接收更新时，将从其托管 VM 系列防火墙发送这些更新。Panorama 根据您确定的条件将虚拟机放入动态地址组，并将动态地址组成员信息推送到防火墙。这可以让防火墙将正确的安全策略应用到流向和来自 NSX-T 数据中心中虚拟机的流量。

VMware NSX-T 上支持的 VM 系列防火墙部署（东向西）

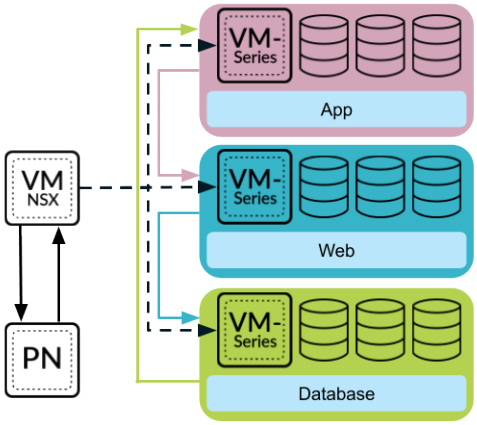
您可以将一个或多个 VM 系列防火墙实例部署为 VMware NSX-T 数据中心中的合作伙伴服务，以保护东向西流量并执行微分段。要配置 VM 系列防火墙以执行微分段，您可以将防火墙部署在服务集群或每个主机中。

- 服务集群 — 在集群部署中，所有 VM 系列防火墙都安装在单个集群中。VM 与组之间的流量重定向到 VM 系列集群以进行策略检查和实施，然后继续定向到其目标。配置集群部署时，您可以在集群内指定特定主机，也可以选择 **Any**（任何），然后让 NSX-T 选择主机。



©2024 Palo Alto Networks, Inc.

- 基于主机 — 在每个主机部署中，VM 系列防火墙的实例安装在 ESXi 集群中的每个主机上。本地防火墙会检查同一主机上来宾之间的流量，因此它不需要离开主机进行检查。在到达 vSwitch 之前，防火墙会检查离开主机的流量。



部署防火墙后，您可以配置将流量发送到 VM 系列防火墙的流量重定向规则。您在 Panorama 上配置的安全策略规则将推送到托管 VM 系列防火墙，然后应用于通过防火墙的流量。

要在 VMware NSX-T 上部署 VM 系列防火墙，您可以使用两个工作流程选项 — 以操作为中心和以安全为中心的部署。

- 以操作为中心 — 在以操作为中心的工作流程中，部署过程的某些部分在 Panorama 上执行，其余部分在 NSX-T Manager 上执行。在 Panorama 上，您必须先启用 Panorama 和 NSX-T Manager 之间的通信，然后配置服务定义并启动 VM 系列防火墙。然后，您必须登录 NSX-T Manager 以通过创建服务链和控制规则来继续配置。要完成 VM 系列部署，您必须返回 Panorama 以创建安全策略。
- 以安全为中心 — 在以安全为中心的工作流程中，您可以将 Panorama 用作单一管理平台来控制和管理安全操作。您可以从 Panorama 完成整个部署工作流程。适用于 VMware NSX 的 Panorama 插件将配置推送到 NSX-T Manager，以创建服务链和控制规则。

为便于使用，建议您为 NSX-T 上的 VM 系列部署选择一个部署工作流程。但是，适用于 VMware NSX-T 的 VM 系列防火墙支持在同一个插件上使用两个工作流程。

使用以操作为中心的工作流程部署 VM 系列

完成以下任务以部署 VM 系列防火墙保护 NSX-T 数据中心中的东向西流量。

- 安装适用于 VMware NSX 的 Panorama 插件
- 启用 NSX-T Manager 与 Panorama 之间的通信
- 在 Panorama 上创建模板堆栈和设备组
- 在 Panorama 上配置服务定义
- 在 NSX-T 上启动 VM 系列防火墙（东向西）
- 添加服务链
- 将流量定向到 VM 系列防火墙

©2024 Palo Alto Networks, Inc.

- 将安全策略应用到 NSX-T 上的 VM 系列防火墙（东向西）
- 使用 vMotion 在主机之间移动 VM 系列防火墙

安装适用于 VMware NSX 的 Panorama 插件

下载和安装适用于 VMware NSX 的 Panorama 插件。安装或升级插件之前，请参阅兼容性矩阵。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 Panorama HA 对中安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 选择 **Panorama** > **Plugins**（插件）。

STEP 2 | 选择**Check Now**（立即检查）以检索可用的更新列表。

STEP 3 | 在操作列中选择 **Download**（下载）以下载插件。

STEP 4 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

启用 NSX-T Manager 与 Panorama 之间的通信

完成以下过程可启用 Panorama 与 NSX-T Manager 之间的通信。您最多可以将 Panorama 连接到 16 个 NSX-T Manager。如果您要将 Panorama 连接到多个 NSX-T Manager，则必须仔细规划设备组层次结构和模板堆栈，并考虑它们如何与部署所需的其他组件进行交互。服务定义引用设备组和模板堆栈，并将该信息推送到相关 ESXi 集群中的防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | （可选）对于 Panorama 与 NSX-T Manager 之间的通信，绕过代理服务器设置，在 Panorama 下配置 **Panorama** > **Setup**（设置） > **Services**（服务） > **Proxy Server**（代理服务器）。此命令允许 Panorama 与 NSX-T Manager 直接通信，同时保持其他服务的代理通信。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令以启用或禁用代理绕过。

   ```
   admin@Panorama> request plugins vmware_nsx global proxy bypass
   {yes | no}
   ```

   选择 **Yes**（是）可启用代理绕过，选择 **No**（否）可禁用代理绕过。默认将此选项设置为 **No**（否）。

STEP 2 | 登录到 Panorama Web 界面。

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

STEP 3 | 设置对 NSX-T Manager 的访问权限。对连接 Panorama 的每个 NSX-T Manager 重复执行此程序。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器），然后单击 **Add**（添加）。
2. 输入 NSX-T Manager 的描述性 **Name**（名称）。
3. （可选）添加 NSX-T Manager 的 **Description**（说明）。
4. 输入用于访问 NSX-T Manager 的 **NSX Manager URL** — NSX-T Manager 集群虚拟 IP 地址或 FQDN。
5. 输入 **NSX Manager Login**（**NSX Manager** 登录）凭据（用户名和密码），以使 Panorama 可以对 NSX-T Manager 执行身份验证。
6. 单击 **OK**（确定）。



如果更改 *NSX-T Manager* 登录密码，则必须立即更新 *Panorama* 上的密码。密码错误会中断 *Panorama* 与 *NSX-T Manager* 之间的连接。

STEP 4 | 将更改提交到 Panorama。

单击 **Commit**（提交） 和 **Commit to Panorama**（提交到 **Panorama**）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 验证 Panorama 上的连接状态。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器）。
2. 验证 **Status**（状态）列中的消息。

   连接成功时，状态显示为 **Registered**（已注册）。这表示 Panorama 与 NSX-T Manager 处于同步状态。

   失败状态消息为：

   - **No connection**（无连接）：无法连接到 NSX-T Manager 或建立与 NSX-T Manager 的网络连接。
   - **Invalid Credentials**（无效凭据）：访问凭据（用户名和/或密码）不正确。
   - **Out of sync**（不同步）：Panorama 上定义的配置设置与 NSX-T Manager 上定义的不同。单击该链接了解失败的具体原因。例如，NSX-T 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-T Manager 上的服务定义。在 Panorama 和 NSX-T Manager 未同步之前，您无法在 Panorama 上添加新的服务定义。
   - **Connection Disabled**（连接已禁用）：手动禁用 Panorama 与 NSX-T Manager 之间的连接。

在 Panorama 上创建模板堆栈和设备组

要使用 Panorama 管理适用于 NSX-T 的 VM 系列防火墙，这些防火墙必须属于某设备组和属于模板堆栈成员的模板。设备组可让您将需要相似策略和对象的防火墙组合为一个逻辑单位；在 Panorama 上可使用 **Objects**（对象）和 **Policies**（策略）选项卡定义此配置。使用模板堆栈来配置 VM 系列防火墙在网络和关联资源上运行所需的设置；在 Panorama 上可使用 **Device**（设备）和 **Network**（网络）选项卡定义此配置。并且在 Panorama 上的 NSX-T 配置中使用的区域的每个模板堆栈都必须与服务定义关联；您至少必须在模板中创建一个区域，以便 NSX-T Manager 可以将流量重定向到 VM 系列防火墙。

Panorama 可以同时支持 NSX-T 北向南和 NSX-T 东向西的部署。建议您为 NSX-T 北向南和 NSX-T 东向西配置单独的设备组、模板堆栈和服务定义。

STEP 1 | 添加设备组或设备组层级。

1. 选择 **Panorama** > **Device Groups**（设备组），然后单击 **Add**（添加）。您还可以创建一个设备组层级。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识设备组。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

©2024 Palo Alto Networks, Inc.

STEP 2 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识模板。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

STEP 3 | 创建模板堆栈。

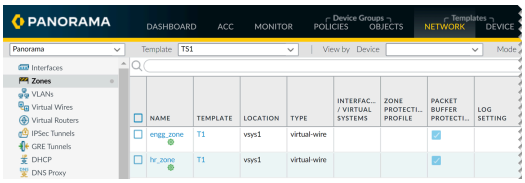
1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add Stack**（添加堆栈）。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识模板。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），然后选择 **Commit to Panorama**（提交到 **Panorama**）以将更改保存到 Panorama 上正在运行的配置。

STEP 4 | 为每个模板创建区域。

每个区域都映射到 NSX-T Manager 上的服务配置文件。要符合条件，区域必须是虚拟线路类型，并且是一个与服务定义关联的模板。

每个模板最多可以添加 32 个区域。

1. 选择 **Network**（网络） > **Zones**（区域）。
2. 选择 **Template**（模板）下拉列表中的正确模板。
3. 选择 **Add**（添加），然后输入区域 **Name**（名称）。
4. 将接口 **Type**（类型）设置为 **Virtual Wire**（虚拟线路）。
5. 单击 **OK**（确定）。
6. 验证区域已附加至正确的模板。



7. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

   Panorama 在提交时为每个合格区域在 NSX-T Manager 上创建相应的服务配置文件。

©2024 Palo Alto Networks, Inc.

STEP 5 | 更新模板堆栈的 DNS 和 NTP 服务器信息。如果您在部署中使用设备证书，则必须完成此步骤。这是确保在 NSX-T 环境中部署的防火墙具有访问设备证书服务器所需的正确 DNS 信息所必需的。

1. 验证您是否从 **Template**（模板）下拉列表中指定正确的模板堆栈。
2. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后单击 **Edit**（编辑）图标。
3. 在 Services（服务）选项卡上，输入 **Primary DNS Server**（主 **DNS** 服务器）和 **Secondary DNS Server**（辅助 **DNS** 服务器）的 IP 地址。
4. 在 NTP 选项卡上，输入 **NTP Server**（**NTP** 服务器）的 IP 地址。
5. 单击 **OK**（确定）。
6. 将更改 **Commit**（提交）到 Panorama。

在 Panorama 上配置服务定义

服务定义用于指定在 NSX-T 数据中心环境中安装的 VM 系列防火墙的配置。服务定义必须包括设备组、模板堆栈和 OVF URL。

STEP 1 | （可选）配置通知组

通过指定应该通知在虚拟环境中发生更改的设备组来创建通知组。指定设备组中包含的防火墙会收到其中来宾 VM 的安全组和 IP 地址的实时更新。这些防火墙可使用此更新确定构成策略中所引用动态地址组的成员的最新列表

1. 选择 **Panorama** > **VMware** > **Notify Group**（通知组），然后单击 **Add**（添加）。
2. 为通知组指定一个描述性 **Name**（名称）。
3. 选择应该通知虚拟环境变化的所有设备组的框。如果某个设备组没有可用的复选框，则设备组将借由设备组层次结构被自动纳入。
4. 单击 **OK**（确定）。

STEP 2 | 添加一个新的服务定义。

在 *Panorama* 上，您最多可创建 *32* 个服务定义。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（服务定义）。
2. 选择 **Add**（添加）以创建新服务定义。
3. 输入服务定义的描述性 **Name**（名称）。
4. （可选）添加一个 **Description**（说明），用以识别将通过该服务定义进行部署的 VM 系列防火墙的功能或目的。

©2024 Palo Alto Networks, Inc.

STEP 3 | 为该服务定义分配一个设备组和模板堆栈。

确保 在 Panorama 上创建模板堆栈和设备组。

由于使用此解决方案部署的防火墙将在 Panorama 中集中管理，因此必须指定防火墙所属的 **Device Group**（设备组）和 **Template Stack**（模板堆栈）。使用该服务定义部署的所有防火墙均属于指定的模板堆栈和设备组。

1. 在 **Device Group**（设备组）下拉列表中选择设备组或设备组层级。
2. 选择 **Template**（模板）下拉列表中的模板堆栈。

   您无法重复使用已在另一个服务定义中分配给某个服务定义的模板堆栈或设备组。

STEP 4 | 指定 OVF 文件的位置。

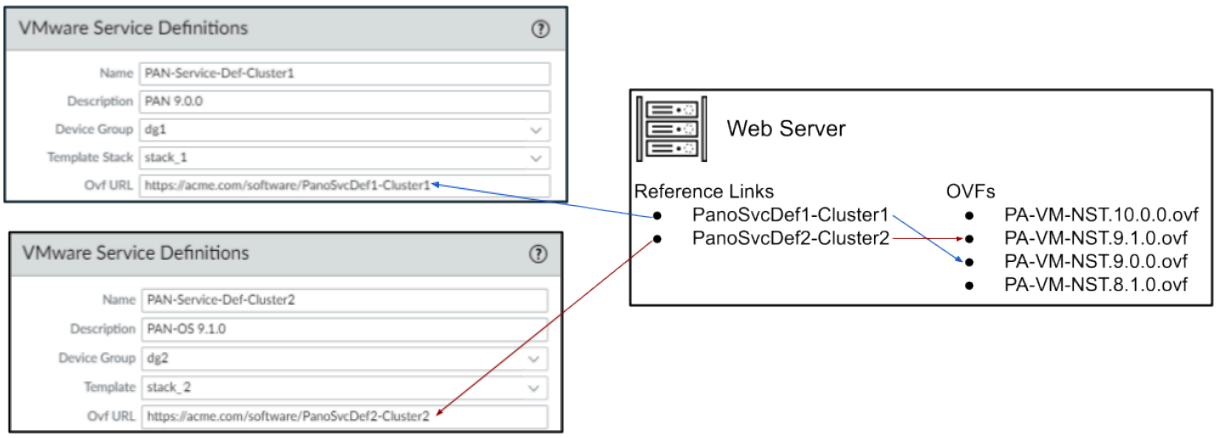
下载 zip 文件，将其解压缩以提取并将.ovf，mf 和 .vmdk 文件保存到同一目录。ovf 和 vmdk 文件均用于部署防火墙的每个实例。

在 *VM* 系列防火墙的 *NSX* 服务部署成功后，请勿更改 *Panorama* 服务定义 *OVF* 路径。在成功部署 *VM* 系列防火墙后更改 *OVF* 路径可能会导致 *NSX* 服务部署失败。您可以在 *NSX-T Manager* 中解决此故障，但这可能会导致要重新部署所有 *VM* 系列防火墙。

建议您使用可扩展的 OVF 路径名称，并允许您在不影响部署的防火墙的情况下更改基本映像。请勿使用诸如 **https://acme.com/software/PA-VM-NST.9.1.0.ovf** 之类的路径，而是使用诸如 **https://acme.com/software/PanoSvcDef1-Cluster1.ovf** 之类的路径。使用静态路径引用可消除将

©2024 Palo Alto Networks, Inc.

来更改 OVF 路径的任何需要。建议您为部署中的每个 Panorama 服务定义（vSphere 集群）创建一个路径，并根据需要更改 Web 服务器上的 PAN-OS 基础映像引用。



在 **OVF URL** 中，添加托管 ovf 文件的 Web 服务器的位置。http 和 https 均为支持协议。

对于各个服务定义，您可以使用相同的 ovf 版本，也可以使用不同的版本。如果对各个服务定义使用不同的 ovf 版本，则可以在不同 ESXi 集群中的 VM 系列防火墙上使用不同的 PAN-OS 版本。

STEP 5 | （可选）选择 **Notify Group**（通知组）。

STEP 6 | 为您的防火墙选择 **East West**（东向西）作为 **Insertion Type**（插入类型）。

STEP 7 | （可选）启用 **Health Check**（运行状况检查）。默认情况下，在适用于 VMware NSX 3.2.0 及更高版本的 Panorama 插件中启用运行状况检查。在插件的较旧版本中，默认禁用运行状况检查。此 NSX-T 功能也称为服务运行状况检查，可让您在服务实例失败时模拟高可用性。使用 VM 系列防火墙配置时，如果 VM 系列服务实例失败，则定向到该防火墙的所有流量都将重定向到集群中的另一个防火墙实例（对于服务集群部署）或另一个主机上的防火墙实例（对于基于主机的部署）。

在 *NSX-T* 中提交和部署 *VM* 系列防火墙后，您无法在服务定义中禁用或启用 *Health Check*（运行状况检查）。尝试在 *Health Check*（运行状况检查）配置中提交更改将返回提交失败。要更改此设置，您必须删除并重新创建服务定义，然后重新部署 *VM* 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 8 | 要在 NSX Manager 部署 VM 系列防火墙时自动检索设备证书，请配置设备证书。

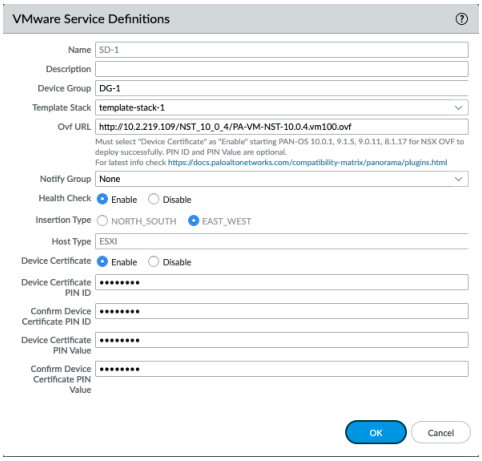
启用此选项可将设备证书应用于新部署的 VM 系列防火墙。只有在使用支持设备证书的基本映像 OVF 部署防火墙时才使用此选项。Panorama 将设备证书信息作为服务定义的一部分推送到 NSX Manager。在 NSX 中部署新防火墙时，启动时将会在防火墙上安装设备证书。

有关支持 VMware NSX 上 VM 系列防火墙的设备证书的 OVF 列表，请参阅 Palo Alto Networks 兼容性矩阵。

如果您的 OVF 支持设备证书，无论您是否使用设备证书，则都必须 **Enable**（启用）设备证书。如果 OVF 不支持设备证书，请禁用此选项。

1. 如果您尚未安装设备证书，请登录到客户支持门户，并生成注册 PIN 和 PIN ID。
2. 在 **Device Certificate**（设备证书）下，单击 **Enable**（启用）。
3. 复制 PIN ID，然后在 **Device Certificate PIN ID**（设备证书 **PIN ID**）字段中输入该 PIN ID。
4. 在 **Confirm Device Certificate PIN ID**（确认设备证书 **PIN ID**）字段中重新输入该 PIN ID。
5. 复制 PIN 值，然后在 **Device Certificate PIN Value**（设备证书 **PIN** 值）字段中输入该 PIN 值。
6. 在 **Confirm Device Certificate PIN Value**（确认设备证书 **PIN** 值）字段中重新输入该 PIN 值。

STEP 9 | 单击 **OK**（确定）保存服务定义。

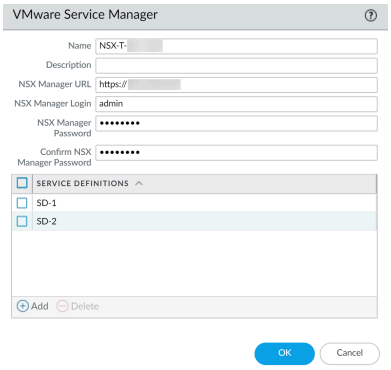


 ©2024 Palo Alto Networks, Inc.

STEP 10 | 将服务定义附加到服务管理器。

您无法在多个服务管理器中使用服务定义。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Manager**（服务管理器），然后单击服务管理器名称的链接。
2. 在服务定义下，单击 **Add**（添加） 并从下拉列表中选择您的服务定义。
3. 单击 **OK**（确定）。

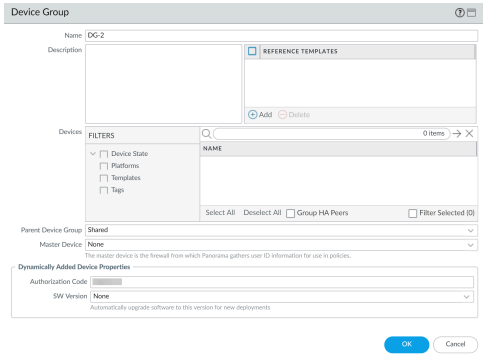


STEP 11 | 将授权代码添加到防火墙的许可证中。

1. 选择 **Panorama** > **Device Groups**（设备组），并选择与刚才创建的服务定义关联的设备组。
2. 在 **Dynamically Added Device Properties**（动态添加的设备属性）下，将您收到的授权代码添加到订单履行电子邮件中，并且可选择性地从 **SW Version**（软件版本）下拉列表中选择 None（无）。

   在 NSX-T 上部署新防火墙时，它将自动添加到设备组，并使用您提供的授权代码进行许可，以及升级到您指定的 PAN-OS 版本。

   在支持门户上，您可以查看经授权部署的防火墙的总数量，以及所用许可证的数量与授权代码启用的许可证的总数量的比率。



STEP 12 | **Commit to Panorama**（提交到 **Panorama**）。

©2024 Palo Alto Networks, Inc.

STEP 13 | 在 NSX-T Manager 上，验证服务定义是否可用。

选择 **System**（系统） > **Service Deployments**（服务部署） > **Catalog**（目录）。服务定义作为 NSX-T Manager 上的服务实例列出。

在 NSX-T 上启动 VM 系列防火墙（东向西）

完成以下过程，以部署 VM 系列防火墙作为 NSX-T 环境中的服务。作为服务定义的一部分，**Deployment Specification**（部署规范）和 **Deployment Template**（部署模板）字段自动使用从 Panorama 推送的信息填充。

不要编辑 *Deployment Attributes*（部署属性）下的任何设置。这些值是从 *Panorama* 导入的，更改它们可能会导致部署失败。

STEP 1 | 登录到 NSX-T Manager。

STEP 2 | 选择 **System**（系统） > **Service Deployments**（服务部署） > **Deployment**（部署）。

STEP 3 | 从 **Partner Service**（合作伙伴服务）下拉列表中选择服务定义。

STEP 4 | 单击 **Deploy Service**（部署服务）。

STEP 5 | 输入服务部署的描述性 **Name**（名称）。

STEP 6 | 选择 **Compute Manager**（计算管理器）(vCenter)。

STEP 7 | 选择 **Deployment Type**（部署类型）— **Clustered**（集群）或 **Host Based**（基于主机）。

STEP 8 | 如果选择 **Clustered**（集群）作为 **Deployment Type**（部署类型），请输入 **Clustered Deployment Count**（集群部署计数）以指定要在集群上部署的 VM 系列防火墙实例的数量。

STEP 9 | 如果要在集群部署中启动 VM 系列防火墙，请选择 **Host**（主机）。从 **Host**（主机）下拉列表中选择特定主机，或选择 **Any**（任何）以允许 NSX-T Manager 选择主机。此选项在 **Per Host**（每个主机）部署中显示为灰色。

STEP 10 | 选择 **Data Store**（数据存储）作为 VM 系列防火墙的存储库。在集群部署中，如果您选择 **Any**（任何）以选择主机，请选择共享数据存储，或如果您已指定特定主机，请选择本地数据存储。

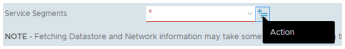
STEP 11 | 配置 **Networks**（网络）设置。

1. 在 Networks（网络）列中，单击 **Set**（设置）。
2. 选择 **Network**（网络）作为 **eth0 - Management Nic**（**eth0** — 管理 **Nic**）。
3. 选择 **Network Type**（网络类型）— DHCP 或静态 IP 池。如果选择静态 IP 池，请选择 **IP Pool**（**IP** 池）。
4. 检查 **eth1 - Data-1 Nic**。
5. 单击 **Save**（保存）。

©2024 Palo Alto Networks, Inc.

STEP 12 | 选择或配置 **Service Segment**（服务段）。要配置服务段，请完成以下过程。

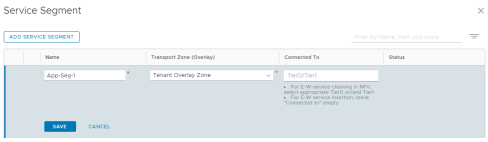
1. 单击 **Service Segments**（服务段）列中的 **Action**（操作）。



2. 单击 **Add Service Segment**（添加服务段）。
3. 输入描述性的 **Name**（名称）。
4. 选择 **Transport Zone (Overlay)**（传输区域（覆盖））。

   VM 系列防火墙必须附加到 *Overlay* 传输区域。来宾 *VM* 可以附加到 *VLAN* 或 *Overlay* 传输区域。托管来宾 *VM* 和 *VM* 系列的传输节点必须配置 *Overlay* 传输区域。

5. 单击 **Save**（保存）并 **Close**（关闭）。



STEP 13 | 选择将在其中部署服务的 **Cluster**（集群）。您必须选择包含 **NSX Configuration**（**NSX** 配置）的集群。

STEP 14 | 单击 **Save**（保存）。

STEP 15 | 验证防火墙部署是否已成功。

1. 选择 **System**（系统） > **Service Deployments**（服务部署） > **Service Instances**（服务实例）。
2. 确认已列出您的防火墙，并且 **Deployment Status**（部署状态）显示 **Up**（启动）。

STEP 16 | 验证防火墙是否连接到 Panorama。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要）。
3. 确认已在正确的设备组下列出您的防火墙，并且 **Device State**（设备状态）显示 **Connected**（已连接）。

   对于 NSX-T (N-S) 部署，VM 系列防火墙的设备名称在 Panorama 上显示为 **PA-VM:<nsx.clusterid>**，对于 NSX-T (E-W) 部署，则显示为 **PA-VM:<nsx.servicevmid>**。

©2024 Palo Alto Networks, Inc.

STEP 17 | 为 VM 系列防火墙上的管理员帐户设置安全密码。

每个 VM 系列防火墙都使用默认用户名和密码 (admin/admin) 来进行初始登录。首次登录时，系统会提示设置一个更安全的新密码。新密码至少包含 8 个字符，其中至少 1 个小写字母和 1 个大写字母以及 1 个数字或特殊字符。

通过 Panorama 可单独更新每个防火墙的密码，也可以一次性更新所有防火墙的密码。

- **Panorama** — 在 Panorama 上，您可以更改模板中所有防火墙的默认密码或删除管理员用户并创建新的用户名和密码。
  1. 登录到 Panorama。
  2. 选择 **Device**（设备） > **Administrators**（管理员），然后选择 **admin** 用户。
  3. **Delete**（删除）用户，或单击用户并输入新密码。
  4. 如果更改了密码，请单击 **OK**（确定）。
  5. 选择 **Commit**（提交） > **Push to Devices**（推送到设备） > **Edit Selections**（编辑选择） > **Force Template Values**（强制模板值）。
  6. 单击 **OK**（确定）。
- 防火墙 — 必须在每个 VM 系列防火墙上重复此过程。
  1. 使用默认用户名和密码登录 VM 系列防火墙。
  2. 按照提示重置密码。

添加服务链

服务链是按逻辑顺序设置的一组服务。当将流量重定向到服务链时，它将按照您配置的顺序在每个服务中移动。

STEP 1 | 选择 **Security**（安全） > **Network Introspection Settings**（网络自检设置） > **Service Chains**（服务链） > **Add Chain**（添加链）。

STEP 2 | 输入服务链的描述性 **Name**（名称）和 **Description**（说明）（可选）。

STEP 3 | 选择在部署 VM 系列防火墙时应用的 **Service Segment**（服务段）。

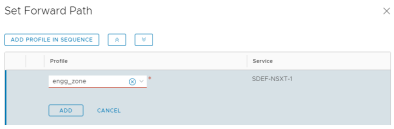
©2024 Palo Alto Networks, Inc.

STEP 4 | 设置转发路径。服务链是服务配置文件的逻辑顺序，因此流量将按照您指定为转发路径的顺序在服务中移动。

1. 选择 **Set Forward Path**（设置转发路径） > **Add Profile in Sequence**（按顺序添加配置文件）。
2. 选择服务配置文件。服务列根据您选择的服务配置文件自动填充。
3. 单击 **Add**（添加）。
4. （可选）如果 NSX-T 环境中还有其他合作伙伴服务配置文件，请单击 **Add Profile in Sequence**（按顺序添加配置文件）以将它们添加到此服务链。

   您只能为每个服务定义选择一个服务配置文件。

5. 添加服务配置文件完成后，单击 **Save**（保存）。



STEP 5 | 在 Reverse Path（反向路径）列中，选择 **Inverse Forward**（反向转发）**Path**（路径）以使返回流量按照相反顺序在服务链中移动。

STEP 6 | （可选）如果您已选择其他合作伙伴服务配置文件，请设置反向路径。

您必须选择与在 *Forward Path*（转发路径）中设置相同的 *VM* 系列服务配置文件。

1. 选择 **Set Reverse Path**（设置反向路径） > **Add Profile in Sequence**（按顺序添加配置文件）。
2. 选择服务配置文件。服务列根据您选择的服务配置文件自动填充。
3. 单击 **Add**（添加）。
4. （可选）如果 NSX-T 环境中还有其他服务配置文件，请单击 **Add Profile in Sequence**（按顺序添加配置文件）以将它们添加到此服务链。
5. 添加服务配置文件完成后，单击 **Save**（保存）。

STEP 7 | 设置 **Failure Policy**（失败策略）— **Allow**（允许）或 **Block**（阻止）。这可以定义服务配置文件失败时 NSX-T 执行的操作。

STEP 8 | 单击 **Save**（保存）。

将流量定向到 VM 系列防火墙

配置策略规则以将流量虚拟机或虚拟机组定向到 VM 系列防火墙。

STEP 1 | 选择 **Security**（安全） > **Network Introspection (E-W)**（网络自检 **(E-W)**） > **Rules**（规则） > **Add Policy**（添加策略）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 单击 **New Policy**（新建策略）为策略指定一个描述性名称。

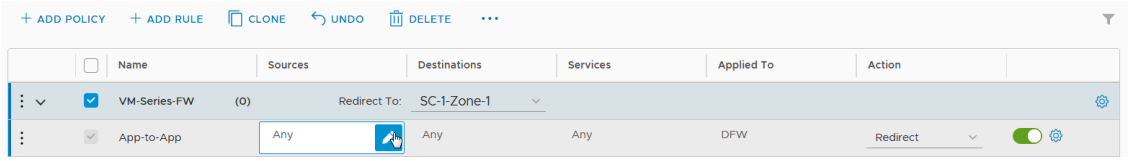
STEP 3 | 从 **Redirect To**（重定向到）下拉列表中选择服务链。

STEP 4 | 选择策略，然后单击 **Add Rule**（添加规则）。

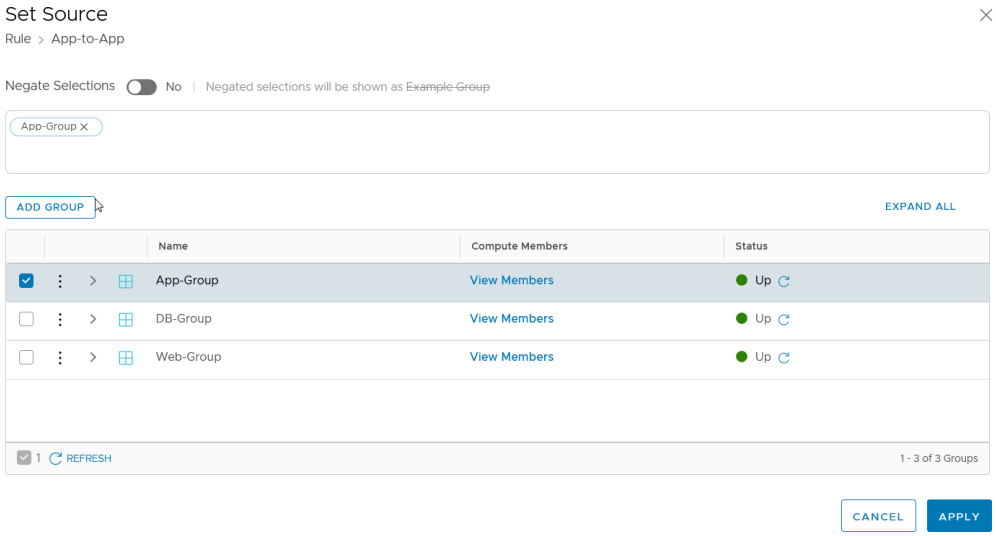
STEP 5 | 单击 **New Rule**（新建规则）为规则指定一个描述性名称。

STEP 6 | 选择源。

1. 单击源列中的铅笔图标以选择虚拟机的源组。



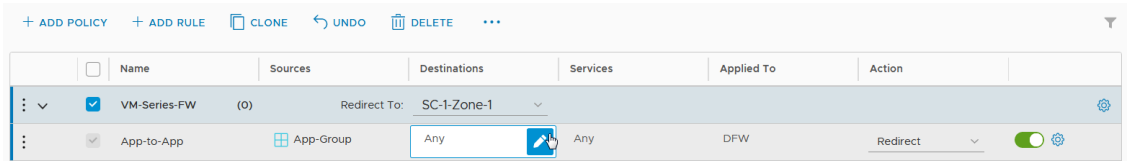
2. 选择源组或组。
3. 单击 **Apply**（应用）。



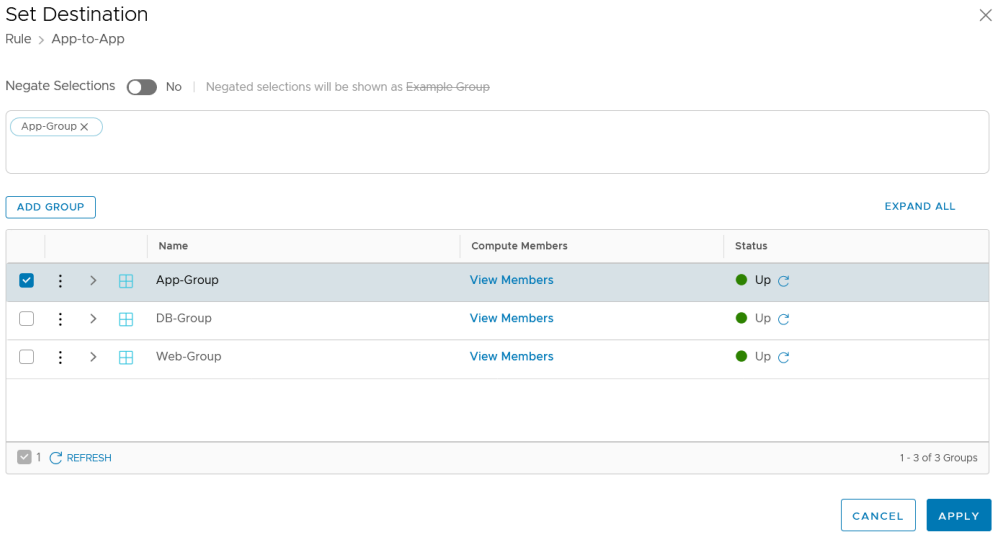
©2024 Palo Alto Networks, Inc.

STEP 7 | 选择 **Destination**（目标）。

1. 单击目标列中的铅笔图标以选择虚拟机的源组。



2. 选择目标组或组。
3. 单击 **Apply**（应用）。



STEP 8 | （可选）选择将要应用规则的 **Services**（服务）。

STEP 9 | 在 **Applied To**（应用到）字段中选择以下选项之一：

- 选择 **DFW** 以将规则应用到连接到逻辑交换机的所有虚拟 NIC。
- 选择 **Groups**（组）以将规则应用到指定组或组中成员虚拟机的虚拟 NIC。

STEP 10 | 选择 **Action**（操作）— **Redirect**（重定向）或 **Do Not Redirect**（不重定向）。

STEP 11 | 单击 **Publish**（发布）。

STEP 12 | 重复此过程以创建其他策略或规则。

将安全策略应用到 NSX-T 上的 VM 系列防火墙（东向西）

现在您已在 NSX-T Manager 上创建重定向规则，现在可以使用 Panorama 在 VM 系列防火墙上集中管理策略。

要集中管理策略，请将动态地址组作为源或目标地址附加到安全策略，并将其推送到防火墙；防火墙可以动态检索每个安全组包含的虚拟机的 IP 地址，以强制指定组中的虚拟机为源或目标地址的流量遵循规则。

©2024 Palo Alto Networks, Inc.

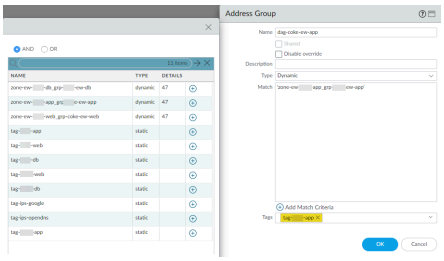
STEP 1 | 登录到 Panorama。

STEP 2 | 创建动态地址组。

1. 选择 **Object**（对象） > **Address Groups**（地址组）。
2. 从 **Device Group**（设备组）下拉列表中选择为了在 NSX-T 防火墙上管理 VM 系列而创建的设备组。
3. 单击 **Add**（添加），然后为动态地址组输入 **Name**（名称）和 **Description**（说明）。
4. 选择 **Dynamic**（动态）作为 **Type**（类型）。
5. 将匹配条件添加到动态地址组。

   某些浏览器扩展程序可能会阻止 *Panorama* 与 *NSX-T* 之间的 *API* 调用，从而阻止 *Panorama* 接收匹配条件。如果 *Panorama* 未显示匹配条件且您正在使用浏览器扩展程序，请禁用扩展程序和同步动态对象以填充 *Panorama* 可用的标记。
6. 单击 **Add Match Criteria**（添加匹配条件）。
7. 选择 **And** 或 **Or** 运算符，并单击安全组名称旁边的加号 (+) 图标，将其添加到动态地址组。

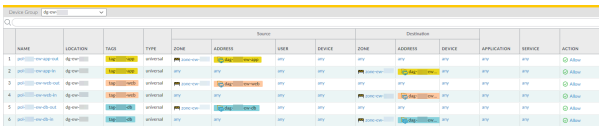
   匹配条件对话框中显示的安全组源自您在 *NSX-T Manager* 上定义的组。此时仅安全策略中引用的组和流量重定向到 *VM* 系列防火墙的源安全组可用。



8. 单击 **OK**（确定）。
9. 重复这些步骤可创建部署所需的适当数量的动态地址组。
10. **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 3 | 创建安全策略规则。



1. 选择 **Policies**（策略） > **Security**（安全） > **Prerules**（预订规则）。
2. 选择在在 Panorama 上创建模板堆栈和设备组中为 NSX-T 上管理 VM 系列防火墙而创建的 **Device Group**（设备组）。
3. 单击 **Add**（添加），然后为规则输入 **Name**（名称）和 **Description**（说明）。在本示例中，安全规则允许 WebFrontEnd 服务器和应用程序服务器之间的所有流量。
4. 选择 **Source Zone**（源区域）和 **Destination Zone**（目标区域）。两栏中的区域名称必须一致。
5. 对于 **Source Address**（源地址）和 **Destination Address**（目标地址），选择或键入地址、地址组或区域。在本例中，我们选择地址组，即您之前创建的动态地址组。
6. 选择允许的 **Application**（应用程序）。在本例中，我们创建 **Application Group**（应用程序组），其中包含已组合在一起的一组静态特定应用程序。
   1. 单击 **Add**（添加），然后选择 **New Application Group**（新建应用程序组）。
   2. 单击 **Add**（添加）以选择要包含到组中的应用程序。
   3. 单击 **OK**（确定）以创建应用程序组。
7. 为流量指定操作（**Allow**（允许）或 **Deny**（拒绝）），（可选）在 Profiles（配置文件）下为防病毒、防间谍软件和漏洞保护附加默认安全配置文件。
8. 重复上面的步骤，以创建相关策略规则。
9. 单击 **Commit**（提交），选择 **Panorama** 作为提交类型。单击 **OK**（确定）。

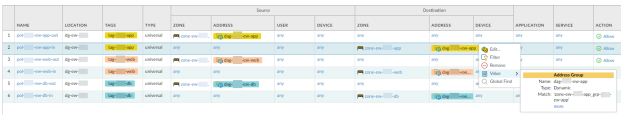
STEP 4 | 将策略应用到适用于 NSX-T 的 VM 系列防火墙。

1. 单击 **Commit**（提交），选择 **Device Groups**（设备组）作为提交类型。
2. 选择设备组（在本例中选择 NSX-T 设备组），然后单击 **OK**（确定）。
3. 验证提交是否成功。

©2024 Palo Alto Networks, Inc.

STEP 5 | 在 VM 系列防火墙上验证是否已填充动态地址组的成员。

1. 在 Panorama 上，切换设备上下文以启动策略推送到的防火墙的 Web 界面。
2. 在 VM 系列防火墙上，选择 **Policies**（策略）> **Security**（安全），然后选择规则。
3. 选择地址组链接旁的下拉箭头，然后选择 **Inspect**（检查）。您还可以验证匹配条件是否准确。



4. 单击 **more**（更多）链接，然后验证是否显示已注册 IP 地址列表。

   将对属于此地址组，并在此显示的所有 IP 地址实施策略。

STEP 6 | （可选）使用模板推送网络的基本配置和设备配置，例如 DNS 服务器、NTP 服务器、Syslog 服务器和登录提示。

有关使用模板的信息，请参阅《Panorama 管理员指南》。

STEP 7 | 创建一个区域保护配置文件，并将其连接到区域。

区域保护配置文件不仅可提供泛滥攻击保护，且可有效防止端口扫描和基于数据包的攻击。通过这种方式，您可以保护数据中心内虚拟机之间的层内和层间流量，以及以数据中心内的虚拟机（工作负载）为目标的来自Internet的流量。

1. 选择您的 **Template**（模板）。
2. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），以添加并配置新的配置文件。
3. 选择 **Network**（网络）> **Zones**（区域），单击所列的默认区域，然后在 **Zone Protection Profile**（区域保护配置文件）下拉列表中选择配置文件。

STEP 8 | 创建 DoS 保护配置文件并将其附加至 DoS 保护策略规则。

1. 选择您的 **Device Group**（设备组）。
2. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **DoS Protection**（**DoS** 保护），以添加并配置新的配置文件。
   - 分类的配置文件将允许创建可应用于单源 IP 的阈值。例如，您可为与策略相匹配的 IP 地址配置最大会话率，然后在触发阈值时，封禁单个 IP 地址。
   - 使用聚合配置文件可为所有与策略相匹配的数据包创建最大会话率。此阈值适用于所有已合并 IP 地址的新会话率。一旦触发此阈值，将影响与策略相匹配的所有流量。
3. 在 **Policy**（策略）> **DoS Protection**（**DoS** 保护）中创建新的 DoS 保护策略规则，然后将新配置文件附加至此策略规则。

使用 vMotion 在主机之间移动 VM 系列防火墙

要在使用 vMotion 在 VMware NSX-T 中具有同构 CPU 配置的 ESXi 主机之间移动 VM 系列防火墙时保持流量，必须在 vMotion 期间使用 PAN-OS CLI 暂停 VM 系列防火墙的内部检测信号监控。您

 ©2024 Palo Alto Networks, Inc.

可以指定暂停检测信号监控的时间（以分钟为单位）。最多可以将检测信号监控暂停 60 分钟。当暂停间隔结束或您故意结束暂停间隔，则检测信号监控将恢复。

如果 ESXi 主机具有同构 CPU 配置，则在 6.5、6.7 和 7.0 上支持 VM 系列防火墙的 vMotion。

如果运行 *vSphere 7.0* 或更高版本，则在使用 *vMotion* 移动 *VM* 系列防火墙时不需要执行此过程。

STEP 1 | 登录到 VM 系列防火墙 CLI。

STEP 2 | 使用以下命令设置检测信号监控暂停间隔。一旦执行命令，暂停就开始。如果 vMotion 所用时间比预期更长，则可以重新运行此命令以设置一个更长的新间隔，该间隔从再次执行命令时开始。

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

您可以使用以下命令查看暂停间隔中的剩余时间。

```
request system heartbeat-pause show interval
```

STEP 3 | （可选）如果在暂停间隔过去之前完成 vMotion，则可以通过将间隔设置为零 (0) 以结束暂停。

```
request system heartbeat-pause set interval 0
```

使用以安全为中心的工作流程部署 VM 系列

您可以使用以安全为中心的工作流程从 Panorama 为 NSX-T 控制和管理 VM 系列防火墙。您无需访问 NSX-T Manager 即可创建服务链和控制规则；但是，仍必须在 NSX-T Manager 上创建服务部署。

- 安装适用于 VMware NSX 的 Panorama 插件
- 启用 NSX-T Manager 与 Panorama 之间的通信
- 在 Panorama 上创建模板堆栈和设备组
- 在 Panorama 上配置服务定义
- 在 NSX-T 上启动 VM 系列防火墙（东向西）
- 创建动态地址组
- 创建安全策略
- 创建动态地址组成员资格条件
- 生成控制策略
- 生成控制规则

安装适用于 VMware NSX 的 Panorama 插件

下载和安装适用于 VMware NSX 的 Panorama 插件。安装或升级插件之前，请参阅兼容性矩阵。

©2024 Palo Alto Networks, Inc.

以安全为中心的部署工作流程需要适用于 *VMware NSX 4.0.0* 的 *Panorama* 插件。此外，您必须从适用于 *VMware NSX 3.2.x* 的 *Panorama* 插件升级到插件 *4.0.0*。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 Panorama HA 对中安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 选择 **Panorama** > **Plugins**（插件）。

STEP 2 | 选择**Check Now**（立即检查）以检索可用的更新列表。

STEP 3 | 在操作列中选择 **Download**（下载）以下载插件。

STEP 4 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

启用 NSX-T Manager 与 Panorama 之间的通信

完成以下过程可启用 Panorama 与 NSX-T Manager 之间的通信。您最多可以将 Panorama 连接到 16 个 NSX-T Manager。如果您要将 Panorama 连接到多个 NSX-T Manager，则必须仔细规划设备组层次结构和模板堆栈，并考虑它们如何与部署所需的其他组件进行交互。服务定义引用设备组和模板堆栈，并将该信息推送到相关 ESXi 集群中的防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | （可选）对于 Panorama 与 NSX-T Manager 之间的通信，绕过代理服务器设置，在 Panorama 下配置 **Panorama** > **Setup**（设置） > **Services**（服务） > **Proxy Server**（代理服务器）。

此命令允许 Panorama 与 NSX-T Manager 直接通信，同时保持其他服务的代理通信。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令以启用或禁用代理绕过。

   ```
   admin@Panorama> request plugins vmware_nsx global proxy bypass
   {yes | no}
   ```

   选择 **Yes**（是）可启用代理绕过，选择 **No**（否）可禁用代理绕过。默认将此选项设置为 **No**（否）。

STEP 2 | 登录到 Panorama Web 界面。

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

STEP 3 | 设置对 NSX-T Manager 的访问权限。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器），然后单击 **Add**（添加）。
2. 输入 NSX-T Manager 的描述性 **Name**（名称）。
3. （可选）添加 NSX-T Manager 的 **Description**（说明）。
4. 输入用于访问 NSX-T Manager 的 **NSX Manager URL** — NSX-T Manager 集群虚拟 IP 地址或 FQDN。
5. 输入 **NSX Manager Login**（**NSX Manager** 登录）凭据（用户名和密码），以使 Panorama 可以对 NSX-T Manager 执行身份验证。
6. 单击 **OK**（确定）。
7. 对连接 Panorama 的每个 NSX-T Manager 重复执行此程序。



如果更改 *NSX-T Manager* 登录密码，则必须立即更新 *Panorama* 上的密码。密码错误会中断 *Panorama* 与 *NSX-T Manager* 之间的连接。

STEP 4 | 将更改提交到 Panorama。

单击 **Commit**（提交） 和 **Commit to Panorama**（提交到 **Panorama**）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 验证 Panorama 上的连接状态。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器）。
2. 验证 **Status**（状态）列中的消息。

   连接成功时，状态显示为 **Registered**（已注册）。这表示 Panorama 与 NSX-T Manager 处于同步状态。

   失败状态消息为：

   - **No connection**（无连接）：无法连接到 NSX-T Manager 或建立与 NSX-T Manager 的网络连接。
   - **Invalid Credentials**（无效凭据）：访问凭据（用户名和/或密码）不正确。
   - **Out of sync**（不同步）：Panorama 上定义的配置设置与 NSX-T Manager 上定义的不同。单击该链接了解失败的具体原因。例如，NSX-T 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-T Manager 上的服务定义。在 Panorama 和 NSX-T Manager 未同步之前，您无法在 Panorama 上添加新的服务定义。
   - **Connection Disabled**（连接已禁用）：手动禁用 Panorama 与 NSX-T Manager 之间的连接。

在 Panorama 上创建模板堆栈和设备组

要使用 Panorama 管理适用于 NSX-T 的 VM 系列防火墙，这些防火墙必须属于某设备组和属于模板堆栈成员的模板。设备组可让您将需要相似策略和对象的防火墙组合为一个逻辑单位；在 Panorama 上可使用 **Objects**（对象）和 **Policies**（策略）选项卡定义此配置。使用模板堆栈来配置 VM 系列防火墙在网络和关联资源上运行所需的设置；在 Panorama 上可使用 **Device**（设备）和 **Network**（网络）选项卡定义此配置。在 Panorama 上的 NSX-T 配置中使用的区域的每个模板堆栈都必须与稍后将创建的服务定义相关联；您至少必须在模板中创建一个区域，以便 NSX-T Manager 可以将流量重定向到 VM 系列防火墙。稍后，您将设备组和模板与 NSX-T 部署相关联以创建服务定义。

Panorama 可以同时支持 NSX-T 北向南和 NSX-T 东向西的部署。您必须为 NSX-T 北向南和 NSX-T 东向西配置单独的设备组、模板堆栈和服务定义。

STEP 1 | 添加设备组或设备组层级。

1. 选择 **Panorama** > **Device Groups**（设备组），然后单击 **Add**（添加）。您还可以创建一个设备组层级。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识设备组。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

©2024 Palo Alto Networks, Inc.

STEP 2 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识模板。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

STEP 3 | 创建模板堆栈并添加新创建的模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add Stack**（添加堆栈）。
2. 输入唯一的 **Name**（名称）和 **Descriptio**（说明）**n**，以标识模板堆栈。
3. 在 **Templates**（模板）下，单击 **Add**（添加），然后从下拉列表中选择在步骤 2 中创建的模板。
4. 单击 **OK**（确定）。
5. 单击 **Commit**（提交），然后选择 **Commit to Panorama**（提交到 **Panorama**）以将更改保存到 Panorama 上正在运行的配置。

STEP 4 | 为每个模板创建区域。

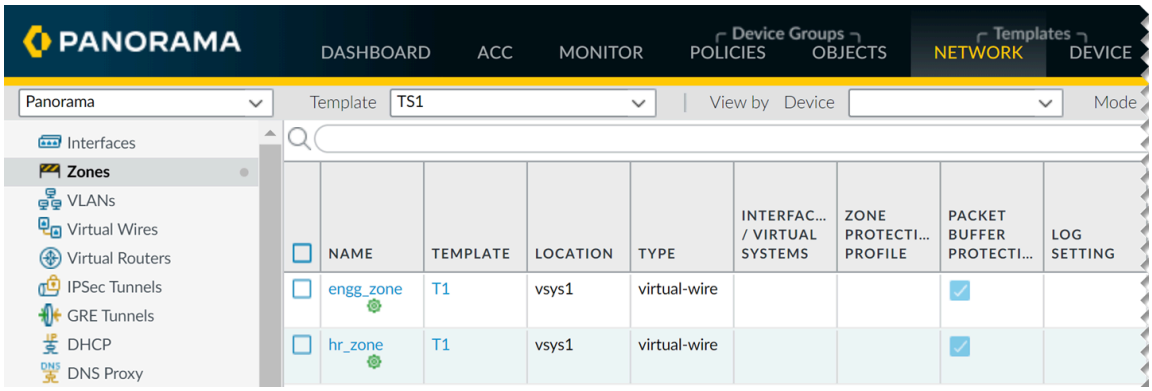
适用于 VMware NSX 的 Panorama 插件将每个区域映射到 NSX-T Manager 上的服务配置文件。为了符合条件，区域必须是虚拟线路类型，并且是要与服务定义相关联的模板的一部分；有关

 ©2024 Palo Alto Networks, Inc.

详细信息，请参阅在 Panorama 上配置服务定义。在大多数用例中，单个区域就已足够。但是，您必须为多租户创建多个区域

每个模板最多可以添加 32 个区域。

1. 选择 **Network**（网络）> **Zones**（区域）。
2. 选择 **Template**（模板）下拉列表中的正确模板。
3. 选择 **Add**（添加），然后输入区域 **Name**（名称）。
4. 将接口 **Type**（类型）设置为 **Virtual Wire**（虚拟线路）。
5. 单击 **OK**（确定）。
6. 验证区域已附加至正确的模板。



7. 单击 **Commit**（提交），选择 **Panorama** 作为 **Commit Type**（提交类型），以便将更改保存到 Panorama 上正在运行的配置。

STEP 5 | 更新模板堆栈的 DNS 和 NTP 服务器信息。如果您在部署中使用设备证书，则必须完成此步骤。这是确保在 NSX-T 环境中部署的防火墙具有访问设备证书服务器所需的正确 DNS 信息所必需的。

1. 验证您是否从 **Template**（模板）下拉列表中指定正确的模板堆栈。
2. 选择 **Device**（设备）> **Setup**（设置）> **Services**（服务），然后单击 **Edit**（编辑）图标。
3. 在 Services（服务）选项卡上，输入 **Primary DNS Server**（主 **DNS** 服务器）和 **Secondary DNS Server**（辅助 **DNS** 服务器）的 IP 地址。
4. 在 NTP 选项卡上，输入 **NTP Server**（**NTP** 服务器）的 IP 地址。
5. 单击 **OK**（确定）。
6. 将更改 **Commit**（提交）到 Panorama。

在 **Panorama** 上配置服务定义

服务定义可让您将 VM 系列防火墙注册为 NSX-T Manager 上的合作伙伴安全服务。服务定义必须包括设备组、模板堆栈和 OVF URL。

©2024 Palo Alto Networks, Inc.

STEP 1 | （可选）配置通知组

通过指定应该通知在虚拟环境中发生更改的设备组来创建通知组。指定设备组中包含的防火墙会收到其中来宾 VM 的安全组和 IP 地址的实时更新。这些防火墙可使用此更新确定构成策略中所引用动态地址组的成员的最新列表。

1. 选择 **Panorama** > **VMware** > **Notify Group**（通知组），然后单击 **Add**（添加）。
2. 为通知组指定一个描述性 **Name**（名称）。
3. 选择应该通知虚拟环境变化的所有设备组的框。如果某个设备组没有可用的复选框，则设备组将借由设备组层次结构被自动纳入。
4. 单击 **OK**（确定）。

STEP 2 | 添加一个新的服务定义。

在 *Panorama* 上，您最多可创建 *32* 个服务定义。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（服务定义）。
2. 选择 **Add**（添加）以创建新服务定义。
3. 输入服务定义的描述性 **Name**（名称）。
4. （可选）添加一个 **Description**（说明），用以识别将通过该服务定义进行部署的 VM 系列防火墙的功能或目的。

STEP 3 | 为该服务定义分配一个设备组和模板堆栈。

确保 在 Panorama 上创建模板堆栈和设备组。

由于使用此解决方案部署的防火墙将在 Panorama 中集中管理，因此必须指定防火墙所属的 **Device Group**（设备组）和 **Template Stack**（模板堆栈）。使用该服务定义部署的所有防火墙均属于指定的模板堆栈和设备组。

1. 在 **Device Group**（设备组）下拉列表中选择设备组或设备组层级。
2. 选择 **Template**（模板）下拉列表中的模板堆栈。

   您无法重复使用已在另一个服务定义中分配给某个服务定义的模板堆栈或设备组。

©2024 Palo Alto Networks, Inc.

STEP 4 | 指定 OVF 文件的位置。

下载 zip 文件，将其解压缩以提取并将.ovf，mf 和 .vmdk 文件保存到同一目录。ovf 和 vmdk 文件均用于部署防火墙的每个实例。

在 *VM* 系列防火墙的 *NSX* 服务部署成功后，请勿更改 *Panorama* 服务定义 *OVF* 路径。在成功部署 *VM* 系列防火墙后更改 *OVF* 路径可能会导致 *NSX* 服务部署失败。您可以在 *NSX-T Manager* 中解决此故障，但这可能会导致要重新部署所有 *VM* 系列防火墙。

在 **OVF URL** 中，添加托管 ovf 文件的 Web 服务器的位置。http 和 https 均为支持协议。

对于各个服务定义，您可以使用相同的 ovf 版本，也可以使用不同的版本。如果对各个服务定义使用不同的 ovf 版本，则可以在不同 ESXi 集群中的 VM 系列防火墙上使用不同的 PAN-OS 版本。

STEP 5 | （可选）选择 **Notify Group**（通知组）。

STEP 6 | 为您的防火墙选择 **East West**（东向西）作为 **Insertion Type**（插入类型）。

STEP 7 | （可选）启用 **Health Check**（运行状况检查）。

默认启用运行状况检查。此 NSX-T 功能也称为服务运行状况检查，可让您在服务实例失败时模拟高可用性。使用 VM 系列防火墙配置时，如果 VM 系列服务实例失败，则定向到该防火墙的所有流量都将重定向到集群中的另一个防火墙实例（对于服务集群部署）或另一个主机上的防火墙实例（对于基于主机的部署）。

在 *NSX-T* 中提交和部署 *VM* 系列防火墙后，您无法在服务定义中禁用或启用 *Health Check*（运行状况检查）。尝试在 *Health Check*（运行状况检查）配置中提交更改将返回提交失败。要更改此设置，您必须删除并重新创建服务定义，然后重新部署 *VM* 系列防火墙。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 要在 NSX Manager 部署 VM 系列防火墙时自动检索设备证书，请配置设备证书。

启用此选项可将设备证书应用于新部署的 VM 系列防火墙。只有在使用支持设备证书的基本映像 OVF 部署防火墙时才使用此选项。Panorama 将设备证书信息作为服务定义的一部分推送到 NSX Manager。在 NSX 中部署新防火墙时，启动时将会在防火墙上安装设备证书。

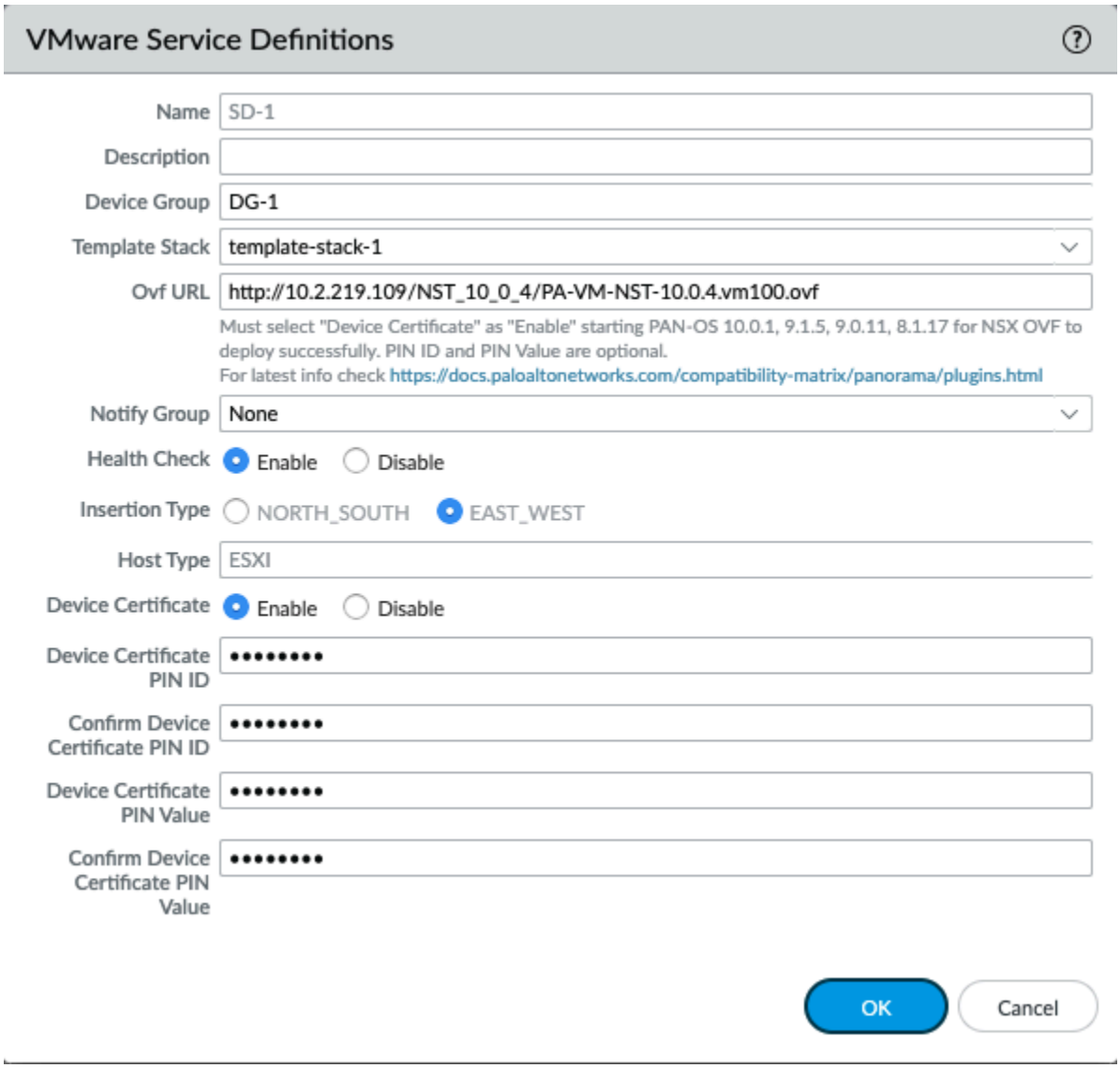
有关支持 VMware NSX 上 VM 系列防火墙的设备证书的 OVF 列表，请参阅 Palo Alto Networks 兼容性矩阵。

如果您的 OVF 支持设备证书，无论您是否使用设备证书，则都必须启用设备证书。如果 OVF 不支持设备证书，请禁用此选项。

1. 如果您尚未安装设备证书，请登录到客户支持门户，并生成注册 PIN 和 PIN ID。
2. 在 **Device Certificate**（设备证书）下，单击 **Enable**（启用）。
3. 复制 PIN ID，然后在 **Device Certificate PIN ID**（设备证书 **PIN ID**）字段中输入该 PIN ID。
4. 在 **Confirm Device Certificate PIN ID**（确认设备证书 **PIN ID**）字段中重新输入该 PIN ID。
5. 复制 PIN 值，然后在 **Device Certificate PIN Value**（设备证书 **PIN** 值）字段中输入该 PIN 值。
6. 在 **Confirm Device Certificate PIN Value**（确认设备证书 **PIN** 值）字段中重新输入该 PIN 值。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 单击 **OK**（确定）保存服务定义。

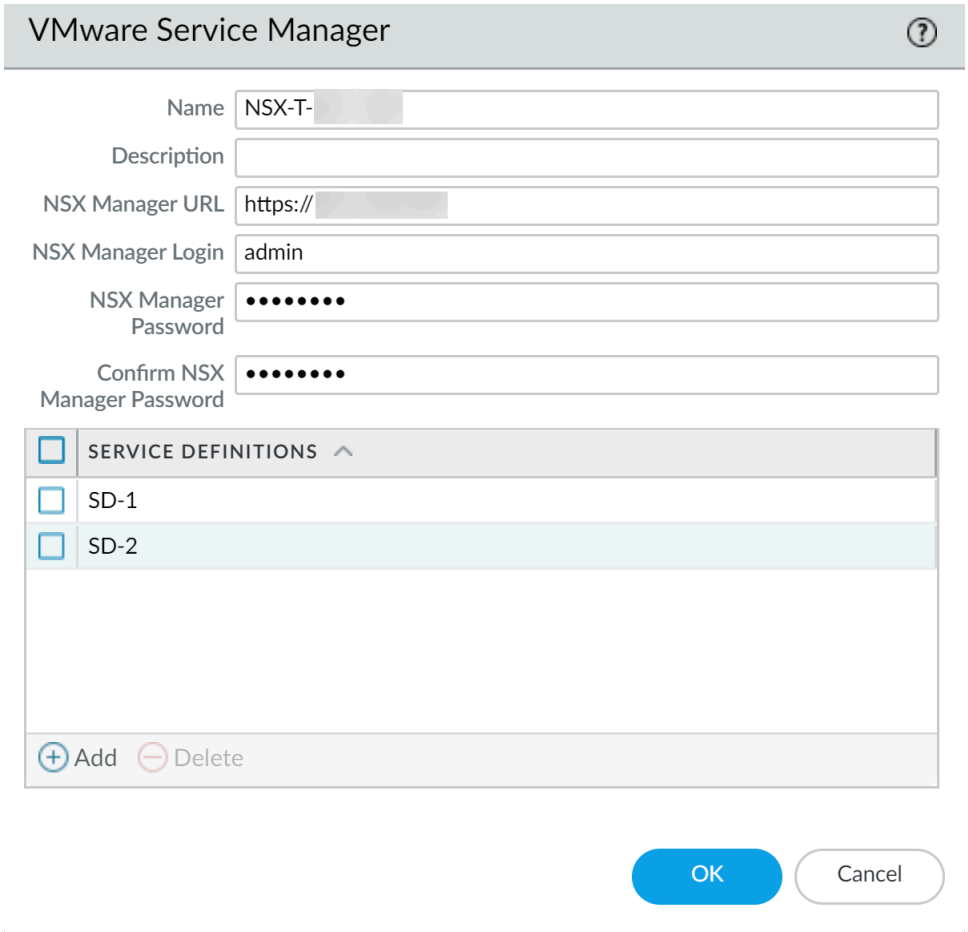


 ©2024 Palo Alto Networks, Inc.

STEP 10 | 将服务定义附加到服务管理器。

您无法在多个服务管理器中使用服务定义。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Manager**（服务管理器），然后单击服务管理器名称的链接。
2. 在服务定义下，单击 **Add**（添加） 并从下拉列表中选择您的服务定义。
3. 单击 **OK**（确定）。



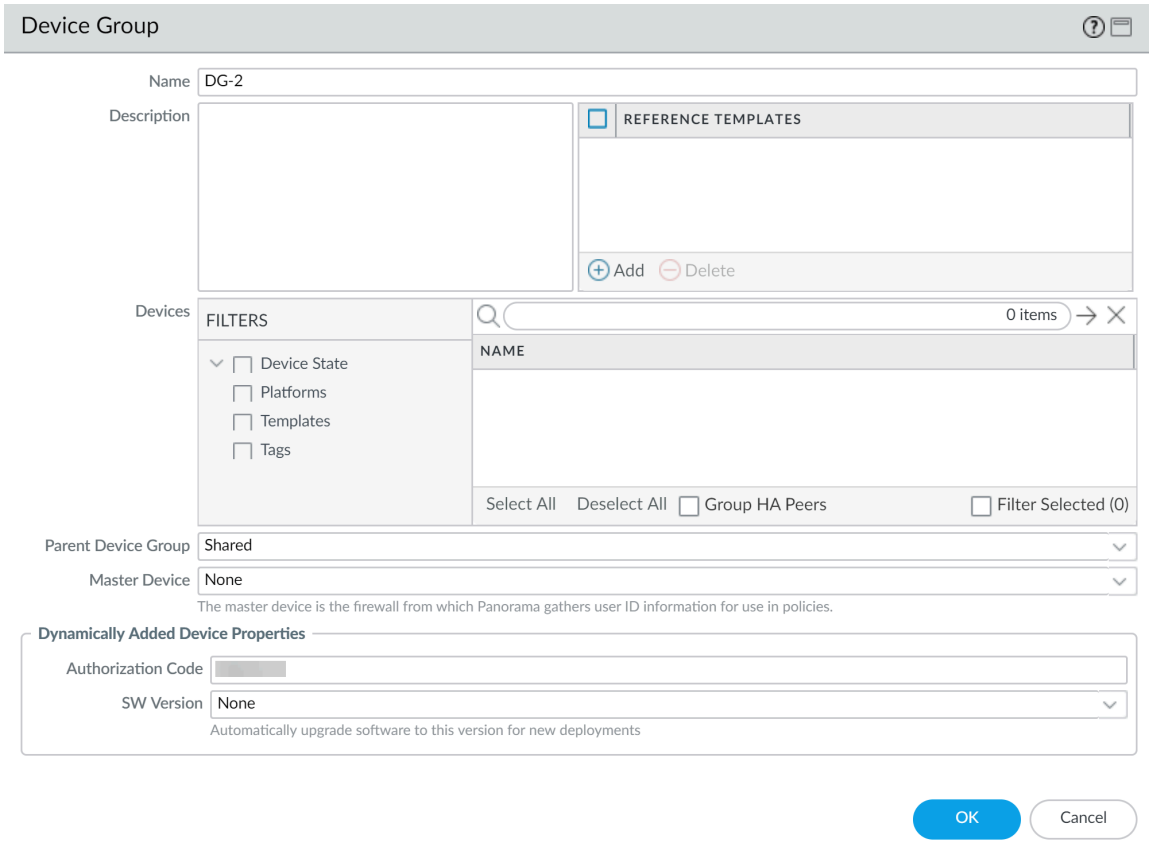
©2024 Palo Alto Networks, Inc.

STEP 11 | 将授权代码添加到防火墙的许可证中。

1. 选择 **Panorama** > **Device Groups**（设备组），并选择与刚才创建的服务定义关联的设备组。
2. 在 **Dynamically Added Device Properties**（动态添加的设备属性）下，将您收到的授权代码添加到订单履行电子邮件中，并且可选择性地从 **SW Version**（软件版本）下拉列表中选择 None（无）。

   在 NSX-T 上部署新防火墙时，它将自动添加到设备组，并使用您提供的授权代码进行许可，以及升级到您指定的 PAN-OS 版本。

   在支持门户上，您可以查看经授权部署的防火墙的总数量，以及所用许可证的数量与授权代码启用的许可证的总数量的比率。



STEP 12 | **Commit to Panorama**（提交到 **Panorama**）。

©2024 Palo Alto Networks, Inc.

STEP 13 | 在 NSX-T Manager 上，验证服务定义是否可用。

选择 **System**（系统） > **Service Deployments**（服务部署） > **Catalog**（目录）。服务定义作为 NSX-T Manager 上的服务实例列出。

在 NSX-T 上启动 VM 系列防火墙（东向西）

完成以下过程，以部署 VM 系列防火墙作为 NSX-T 环境中的服务。作为服务定义的一部分，**Deployment Specification**（部署规范）和 **Deployment Template**（部署模板）字段自动使用从 Panorama 推送的信息填充。

不要编辑 *Deployment Attributes*（部署属性）下的任何设置。这些值是从 *Panorama* 导入的，更改它们可能会导致部署失败。

STEP 1 | 登录到 NSX-T Manager。

STEP 2 | 选择 **System**（系统） > **Service Deployments**（服务部署） > **Deployment**（部署）。

STEP 3 | 从 **Partner Service**（合作伙伴服务）下拉列表中选择服务定义。

STEP 4 | 单击 **Deploy Service**（部署服务）。

STEP 5 | 输入服务部署的描述性 **Name**（名称）。

STEP 6 | 选择 **Compute Manager**（计算管理器）(vCenter)。

STEP 7 | 选择 **Deployment Type**（部署类型）— **Clustered**（集群）或 **Host Based**（基于主机）。

STEP 8 | 如果选择 **Clustered**（集群）作为 **Deployment Type**（部署类型），请输入 **Clustered Deployment Count**（集群部署计数）以指定要在集群上部署的 VM 系列防火墙实例的数量。

STEP 9 | 如果要在集群部署中启动 VM 系列防火墙，请选择 **Host**（主机）。从 **Host**（主机）下拉列表中选择特定主机，或选择 **Any**（任何）以允许 NSX-T Manager 选择主机。此选项在 **Host Based**（基于主机）部署中显示为灰色。

STEP 10 | 选择 **Data Store**（数据存储）作为 VM 系列防火墙的存储库。在集群部署中，如果您选择 **Any**（任何）以选择主机，请选择共享数据存储，或如果您已指定特定主机，请选择本地数据存储。

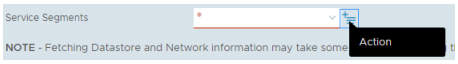
©2024 Palo Alto Networks, Inc.

STEP 11 | 配置 **Networks**（网络）设置。

1. 在 Networks（网络）列中，单击 **Set**（设置）。
2. 选择 **Network**（网络）作为 **eth0 - Management Nic**（**eth0** — 管理 **Nic**）。
3. 选择 **Network Type**（网络类型）— DHCP 或静态 IP 池。如果选择静态 IP 池，请选择 **IP Pool**（**IP** 池）。
4. 检查 **eth1 - Data-1 Nic**。
5. 验证是否已检查两个接口。
6. 单击 **Save**（保存）。

STEP 12 | 选择或配置 **Service Segment**（服务段）。要配置服务段，请完成以下过程。

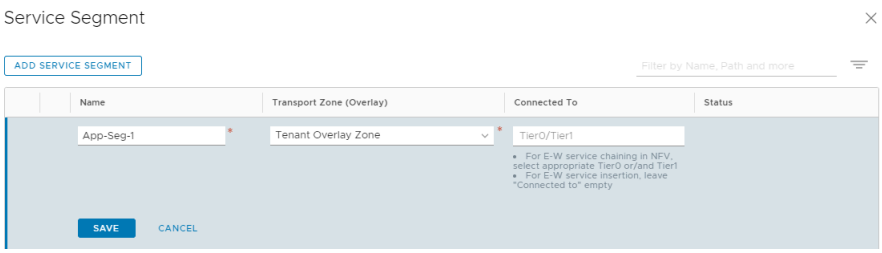
1. 单击 **Service Segments**（服务段）列中的 **Action**（操作）。



2. 单击 **Add Service Segment**（添加服务段）。
3. 输入描述性的 **Name**（名称）。
4. 选择 **Transport Zone (Overlay)**（传输区域（覆盖））。

> *VM* 系列防火墙必须附加到 *Overlay* 传输区域。来宾 *VM* 可以附加到 *VLAN* 或 *Overlay* 传输区域。托管来宾 *VM* 和 *VM* 系列的传输节点必须配置 *Overlay* 传输区域。

5. 单击 **Save**（保存）并 **Close**（关闭）。



STEP 13 | 选择将在其中部署服务的 **Cluster**（集群）。您必须选择包含 **NSX Configuration**（**NSX** 配置）的集群。

STEP 14 | 单击 **Save**（保存）。

STEP 15 | 验证防火墙部署是否已成功。

1. 选择 **System**（系统） > **Service Deployments**（服务部署） > **Service Instances**（服务实例）。
2. 确认已列出您的防火墙，并且 **Deployment Status**（部署状态）显示 **Up**（启动）。

©2024 Palo Alto Networks, Inc.

STEP 16 | 验证防火墙是否连接到 Panorama。

1. 登录到 Panorama。
2. 选择 **Panorama** > **Managed Devices**（托管设备） > **Summary**（摘要）。
3. 确认已在正确的设备组下列出您的防火墙，并且 **Device State**（设备状态）显示 **Connected**（已连接）。

   对于 NSX-T (N-S) 部署，VM 系列防火墙的设备名称在 Panorama 上显示为 **PA-VM:<nsx.clusterid>**，对于 NSX-T (E-W) 部署，则显示为 **PA-VM:<nsx.servicevmid>**。

STEP 17 | 为 VM 系列防火墙上的管理员帐户设置安全密码。

每个 VM 系列防火墙都使用默认用户名和密码 (admin/admin) 来进行初始登录。首次登录时，系统会提示设置一个更安全的新密码。新密码至少包含 8 个字符，其中至少 1 个小写字母和 1 个大写字母以及 1 个数字或特殊字符。

通过 Panorama 可单独更新每个防火墙的密码，也可以一次性更新所有防火墙的密码。

- **Panorama** — 在 Panorama 上，您可以更改模板中所有防火墙的默认密码或删除管理员用户并创建新的用户名和密码。
  1. 登录到 Panorama。
  2. 选择 **Device**（设备） > **Administrators**（管理员），然后选择 **admin** 用户。
  3. **Delete**（删除）用户，或单击用户并输入新密码。
  4. 如果更改了密码，请单击 **OK**（确定）。
  5. 选择 **Commit**（提交） > **Push to Devices**（推送到设备） > **Edit Selections**（编辑选择） > **Force Template Values**（强制模板值）。
  6. 单击 **OK**（确定）。
- 防火墙 — 必须在每个 VM 系列防火墙上重复此过程。
  1. 使用默认用户名和密码登录 VM 系列防火墙。
  2. 按照提示重置密码。

创建动态地址组

安全组是一个逻辑容器，可组合集群中多个 ESXi 主机中的来宾。创建符合正确条件并提交更改的动态地址组时，NSX-T Manager 上将创建相应的安全组。需要创建安全组来管理和保护来宾的安全。

要使动态地址组成为 NSX-T 上的安全组，您必须按以下格式在动态地址组中添加匹配条件：‘**_nsxt_<dynamic-address-group-name>**’。匹配条件中添加的动态地址名称必须与动态地址组名称完全匹配。例如，名为应用程序的动态地址组必须包含匹配条件‘**_nsxt_applications**’。此外，您必须在服务定义的设备组中包含动态地址组，该服务定义是服务管理器的一部分并已提交。

从动态地址组创建的每个安全组都采用以下格式：**<service-def-name>_<dynamic-address-group-name>**。例如，**ServiceDef1_applications**。

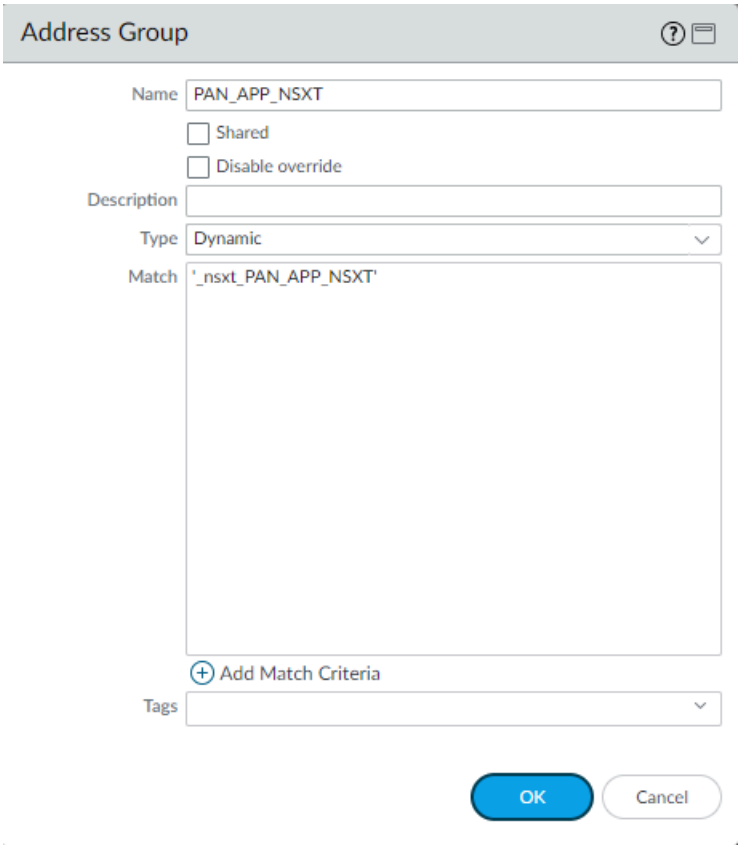
 ©2024 Palo Alto Networks, Inc.

在 *Panorama* 上配置的每个设备组中，您创建的每个动态地址组必须具有唯一名称。

STEP 1 | 为您的部署所需的每个安全组配置一个动态地址组。

1. 选择 **Object**（对象） > **Address Groups**（地址组）。
2. 验证您是否在与 NSX-T 服务定义相关联的设备组中配置动态地址组。
3. 单击 **Add**（添加），然后为地址组输入 **Name**（名称）和 **Description**（说明）。
4. 选择 **Dynamic**（动态）作为 **Type**（类型）。
5. 定义匹配条件。

   要使动态地址组成为 *NSX-T Manager* 中的安全组，匹配条件字符串必须用单引号括起来，前缀为 *_nsxt_*，后跟地址组的确切名称。例如，***'_nsxt_PAN_APP_NSX'***。
6. 对于需要的每个安全组，请重复执行此流程。



STEP 2 | **Commit**（提交）更改。

创建安全策略

创建将用于自动生成在控制策略中使用的控制规则的安全策略规则。

当您生成控制规则时，可以选择根据前导规则、后导规则或全部规则生成控制规则。如果选择“全部”，则适用于 NSX 的 VMware 插件将为前导规则和后导规则中的每个适用安全创建一个控制规

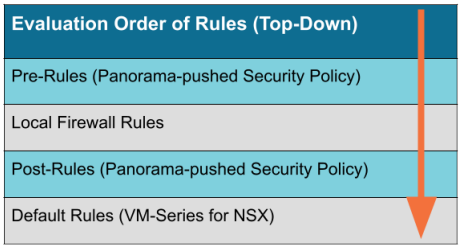
 ©2024 Palo Alto Networks, Inc.

则。这可能会导致创建不必要的控制规则，并使得管理规则变得更加困难。为了帮助轻松地将控制规则与安全规则区分开来，您可以创建控制规则作为后导规则，并创建安全规则作为前导规则。

要根据在 Panorama 上创建的安全规则自动生成控制规则，安全规则必须满足以下条件：

- 属于注册到 NSX-T Service Manager 的父或子设备组。
- 是区域内策略，仅包含一个区域。
- 不包含为规则配置的静态地址组、IP 范围或子网掩码。

决定在 Panorama 中定义 NSX-T 控制规则（前导规则或后导规则）的位置时，请考虑将在 Panorama 上创建的安全策略规则和 NSX-T 控制规则的数量，以及这些规则应用于流量的顺序。前导规则先于后导规则应用于流量。



- 前导规则 — 您可以使用 Panorama 前导规则库来定义 NSX-T 控制规则和 VM 系列防火墙安全策略规则。如果在同一规则库中定义安全规则和控制规则，则必须考虑安全规则相对于控制规则的顺序。如果您拥有包含控制规则和安全策略规则的大型规则库，则在扩展过程中管理这两种类型的规则可能会变得困难。
- 后导规则 — 将用于检查和实施的安全策略规则与用于生成 NSX-T 控制规则的安全规则区分开来，可以帮助您使用大量规则在部署中进行扩展。自动生成控制规则时，插件会为指定规则库中满足必要条件的每个规则生成控制规则。因此，通过将这两种类型的规则区分开来，您可以防止无意中生成无关的控制规则。建议使用控制规则的后导规则库；尤其是在具有大量安全策略规则的部署中。

您在安全规则中指定的源和目标动态地址组。自动生成控制规则时，规则的应用位置（NSX-T 分布式防火墙或安全组）取决于您在配置安全规则时指定的源和目标。如果为源或目标选择任何，则 NSX-T Manager 会将控制规则应用于分布式防火墙。如果为源和目标选择动态地址组，则会将控制规则应用于这些安全组中的来宾虚拟机。如果您手动创建控制规则，则可以指定应用控制规则的安全组。

确保用于定义控制规则的安全策略不包括配置的动态地址组，该动态地址组作为以操作为中心的部署工作流程的一部分。如果不包含，则会将控制规则的源和目标作为任意源和任意目标推送到 NSX-T Manager。这可能会影响 NSX-T 环境中的流量。

如果您禁用将用于自动生成控制规则的安全规则，则也将禁用控制规则。

- 使用前导规则库定义 NSX-T 控制规则
- 使用后导规则库定义 NSX-T 控制规则
- 将安全策略应用到 NSX-T 上的 VM 系列防火墙（东向西）

©2024 Palo Alto Networks, Inc.

使用前导规则库定义 **NSX-T** 控制规则

以下过程介绍了如何创建将用于生成 NSX-T 控制规则的安全策略规则，以及如何创建 Panorama 将推送到 VM 系列防火墙以进行流量检查和执行的安全策略。

如果您不了解规则在 NSX-T Manager 以及 VM 系列防火墙和 Panorama 上的工作原理，请不要应用流量重定向策略。VM 系列防火墙上的默认策略设置为全部拒绝流量，这表示将丢弃重定向到 VM 系列防火墙的所有流量。

在关联的设备组中创建安全策略规则。对于每个安全规则，将规则类型设置为 Intrazone，在关联模板堆栈中选择一个区域，然后选择动态地址组作为源和目标。在 Panorama 中创建合格的安全策略有助于在控制规则生成和 Panorama 中的提交时，在 NSX-T Manager 上创建相应的控制规则。

STEP 1 | 在 Panorama 中，选择 **Policies**（政策） > **Security**（安全） > **Pre Rules**（操作规则）。

STEP 2 | 单击 **Add**（添加），并输入安全策略规则的 **Name**（名称）和 **Description**（说明）。

STEP 3 | 验证您是否在与 NSX-T 服务定义相关联的设备组中配置安全规则。

STEP 4 | 将规则类型设置为 **intrazone (Devices with PAN-OS 6.1 or later)**（区域内（带有**PAN-OS 6.1**或更高版本的设备））。

STEP 5 | 在 Source（源）选项卡中，将源区域设置为与服务定义关联的模板堆栈中的区域。然后选择您之前创建的动态地址组（NSX-T 安全组）作为源地址。不要将任何静态地址组，IP 范围或网络掩码添加为源地址。

STEP 6 | 在 Destination（目标）选项卡中，Panorama 不允许您设置目标区域，因为您将规则类型设置为区域内。然后选择您之前创建的动态地址组（NSX-T 安全组）作为目标地址。不要将任何静态地址组，IP 范围或网络掩码添加为目标地址。

STEP 7 | 单击 **OK**（确定）。

STEP 8 | 对于所需的每项控制规则，请重复步骤 1 到 7。

STEP 9 | **Commit**（提交）更改。

STEP 10 | 将安全策略应用到 NSX-T 上的 VM 系列防火墙（东向西）.

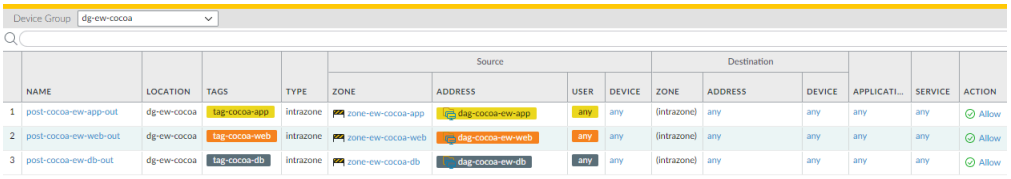
使用后导规则库定义 **NSX-T** 控制规则

在 post 规则库中创建安全策略规则以定义 NSX-T 控制规则。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建安全策略规则。

1. 在 Panorama 中，选择 **Policies**（策略） > **Security**（安全） > **Post Rules**（后导规则）。
2. 验证是否在与 NSX-T 服务定义相关联的设备组中配置安全规则。
3. 单击要编辑的安全策略规则的名称。
4. 将规则类型设置为 **intrazone (Devices with PAN-OS 6.1 or later)**（区域内（带有**PAN-OS 6.1**或更高版本的设备））。
5. 在 Source（源）选项卡中，将源区域设置为与服务定义关联的模板堆栈中的区域。然后，选择您之前创建的动态地址组作为源地址。不要将任何静态地址组，IP 范围或网络掩码添加为源地址。
6. 在 Destination（目标）选项卡中，Panorama 不允许您设置目标区域，因为您将规则类型设置为区域内。然后，选择您之前创建的动态地址组作为目标地址。不要将任何静态地址组，IP 范围或网络掩码添加为目标地址。
7. 单击 **OK**（确定）。
8. 对于所需的每项控制规则，请重复步骤 1 到 7。



STEP 2 | 将更改 **Commit**（提交）到 Panorama。

STEP 3 | 将安全策略规则应用于 VM 系列 NSX-T EW SEC 中心防火墙。

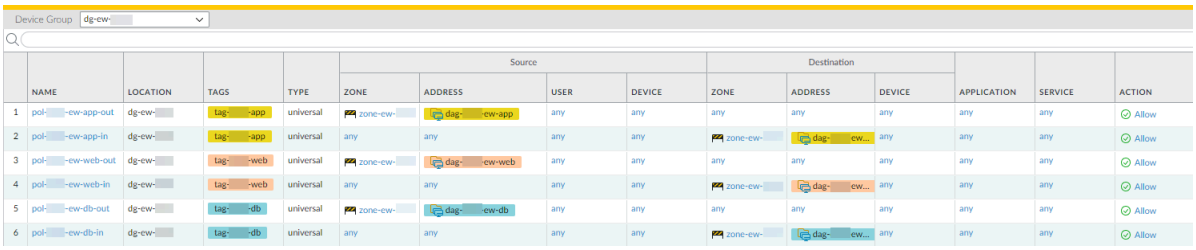
将安全策略应用到 **NSX-T** 上的 **VM** 系列防火墙（东向西）

既然您已定义控制规则，现在可以使用 Panorama 集中管理 VM 系列防火墙上的策略。

要集中管理策略，请将动态地址组作为源或目标地址附加到安全策略，并将其推送到防火墙；防火墙可以动态检索每个安全组包含的虚拟机的 IP 地址，以强制指定组中的虚拟机为源或目标地址的流量遵循规则。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建安全策略规则。



1. 选择 **Policies**（策略） > **Security**（安全） > **Prerules**（预订规则）。
2. 选择在在 Panorama 上创建模板堆栈和设备组中为 NSX-T 上管理 VM 系列防火墙而创建的 **Device Group**（设备组）。
3. 单击 **Add**（添加），然后为规则输入 **Name**（名称）和 **Description**（说明）。在本示例中，安全规则允许 WebFrontEnd 服务器和应用程序服务器之间的所有流量。
4. 选择 **Source Zone**（源区域）和 **Destination Zone**（目标区域）。两栏中的区域名称必须一致。
5. 对于 **Source Address**（源地址）和 **Destination Address**（目标地址），选择或键入地址、地址组或区域。在本例中，我们选择地址组，即您之前创建的动态地址组。
6. 选择允许的 **Application**（应用程序）。在本例中，我们创建 **Application Group**（应用程序组），其中包含已组合在一起的一组静态特定应用程序。
   1. 单击 **Add**（添加），然后选择 **New Application Group**（新建应用程序组）。
   2. 单击 **Add**（添加）以选择要包含到组中的应用程序。
   3. 单击 **OK**（确定）以创建应用程序组。
7. 为流量指定操作（**Allow**（允许）或 **Deny**（拒绝）），（可选）在 Profiles（配置文件）下为防病毒、防间谍软件和漏洞保护附加默认安全配置文件。
8. 重复上面的步骤，以创建相关策略规则。
9. 单击 **Commit**（提交），选择 **Panorama** 作为提交类型。单击 **OK**（确定）。

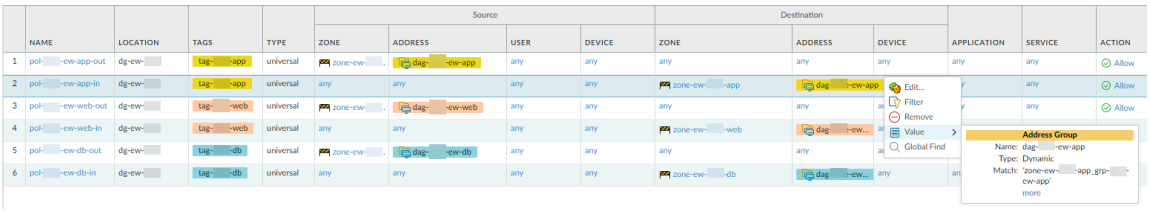
STEP 2 | 将策略应用到适用于 NSX-T 的 VM 系列防火墙。

1. 单击 **Commit**（提交），选择 **Device Groups**（设备组）作为提交类型。
2. 选择设备组（在本例中选择 NSX-T 设备组），然后单击 **OK**（确定）。
3. 验证提交是否成功。

©2024 Palo Alto Networks, Inc.

STEP 3 | 在 VM 系列防火墙上验证是否已填充动态地址组的成员。

1. 在 Panorama 上，切换设备上下文以启动策略推送到的防火墙的 Web 界面。
2. 在 VM 系列防火墙上，选择 **Policies**（策略）> **Security**（安全），然后选择规则。
3. 选择地址组链接旁的下拉箭头，然后选择 **Inspect**（检查）。您还可以验证匹配条件是否准确。



4. 单击 **more**（更多）链接，然后验证是否显示已注册 IP 地址列表。

   将对属于此地址组，并在此显示的所有 IP 地址实施策略。

STEP 4 | （可选）使用模板推送网络的基本配置和设备配置，例如 DNS 服务器、NTP 服务器、Syslog 服务器和登录提示。

有关使用模板的信息，请参阅《Panorama 管理员指南》。

STEP 5 | 创建一个区域保护配置文件，并将其连接到区域。

区域保护配置文件不仅可提供泛滥攻击保护，且可有效防止端口扫描和基于数据包的攻击。通过这种方式，您可以保护数据中心内虚拟机之间的层内和层间流量，以及以数据中心内的虚拟机（工作负载）为目标的来自Internet的流量。

1. 选择您的 **Template**（模板）。
2. 选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **Zone Protection**（区域保护），以添加并配置新的配置文件。
3. 选择 **Network**（网络）> **Zones**（区域），单击所列的默认区域，然后在 **Zone Protection Profile**（区域保护配置文件）下拉列表中选择配置文件。

STEP 6 | 创建 DoS 保护配置文件并将其附加至 DoS 保护策略规则。

1. 选择您的 **Device Group**（设备组）。
2. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **DoS Protection**（**DoS** 保护），以添加并配置新的配置文件。
   - 分类的配置文件将允许创建可应用于单源 IP 的阈值。例如，您可为与策略相匹配的 IP 地址配置最大会话率，然后在触发阈值时，封禁单个 IP 地址。
   - 使用聚合配置文件可为所有与策略相匹配的数据包创建最大会话率。此阈值适用于所有已合并 IP 地址的新会话率。一旦触发此阈值，将影响与策略相匹配的所有流量。
3. 在 **Policy**（策略）> **DoS Protection**（**DoS** 保护）中创建新的 DoS 保护策略规则，然后将新配置文件附加至此策略规则。

©2024 Palo Alto Networks, Inc.

创建动态地址组成员资格条件

在 NSX-T 中，您可以在适用于 NSX 的 Panorama 插件中为属于 NSX-T 安全组（动态地址组）的虚拟机和 IP 地址集配置成员资格条件。对于每个动态地址组，您必须指定服务定义并最多定义五个匹配条件，每个条件最多包含五个匹配规则。

您在插件上创建此成员资格条件，然后将其推送到 *NSX-T Manager*。但是，这不会将成员资格条件应用于部署中的来宾虚拟机。您必须在 *NSX-T Manager* 中定义成员资格数据（例如标签），并将其应用到您的来宾虚拟机。

适用于 NSX-T 的 Panorama 插件根据两种成员资格类型（虚拟机或 IP 地址集）识别并对虚拟机进行分类的规则。下表列出了可用于每个成员类型的键和运算符。

成员类型	密钥	运算符
IP 地址集	标记	等于
虚拟机	• 标记 • 名称 • 操作系统名称 • 计算机名称	• 等于 • 包含 • 开头为 • 结尾为 • 不等于（不适用于标签键）

只能在 *Panorama* 上更改成员资格条件；不能在 *NSX-T Manager* 上更改。如果您在 *NSX-T Manager* 上更改，则适用于 *VMware NSX* 的 *Panorama* 插件会将服务定义显示为不同步。您可以单击 ***Out-of-Sync***（不同步）链接以查看不同步状态的特定原因。如果成员资格条件更改是原因，请单击 ***NSX-T Config-Sync***（***NSX*** 配置同步）执行配置同步。

STEP 1 | 选择 **Panorama** > **VMware** > **NSX-T** > **Membership Criteria**（成员资格条件） > **Add**（添加）。

要添加或修改至少包含一个动态地址组的服务定义的成员资格条件，您可以单击服务定义名称而不是单击 **Add**（添加）。

STEP 2 | 从 **Name**（名称）中为成员资格条件选择服务定义。所选服务定义必须具有 East_West 插入类型，并用作以安全为中心的部署的一部分。

STEP 3 | 单击 **Add**（添加）以指定动态地址组。

STEP 4 | 从下拉列表中选择 **Dynamic Address Group**（动态地址组）。下拉列表列出了与指定服务定义相关联的动态地址组。

插件用户界面显示在 *Panorama* 上配置的动态和静态地址组。配置成员资格条件时，请注意不要意外选择静态地址组。

©2024 Palo Alto Networks, Inc.

STEP 5 | 单击 **Add**（添加）以定义与所选动态地址组关联的条件。

STEP 6 | 输入 **Criteria**（条件）的描述性名称。

STEP 7 | 单击 **Add**（添加）以定义规则。

STEP 8 | 定义规则。您最多可以创建五个规则。

1. 输入规则的描述性名称。
2. 选择 **Member Type**（成员类型）- 虚拟机或 IP 地址集。
3. 选择 **Key**（键）- 标签、名称、操作系统名称、计算机名称。
4. 选择 **Operator**（运算符）- 等于、包含、开头为、结尾为、不等于。
5. 输入 **Value**（值）。

   如果将 Key（键）设置为 Tag（标签），则 Value（值）为 Tag（标签）。插件用户界面未列出标签，因此您必须使用 Panorama CLI（使用 NSX-T Manager 3.0.0 及更高版本）。

   ```
   request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
   ```

6. （可选）输入 **Scope**（作用域）。作用域仅适用于键 **Tag**（标签）。作用域是应用于 NSX-T 中对象标签的可选值。作用域在 NSX-T Manager 上定义。例如，如果您根据操作

©2024 Palo Alto Networks, Inc.

系统标记虚拟机，则可以为 Windows、Linux 和 MacOS 创建标签，然后将每个标签的作用域设置为 OS。

要查看标签和作用域，请使用 Panorama CLI（使用 NSX-T Manager 3.0.0 及更高版本）。

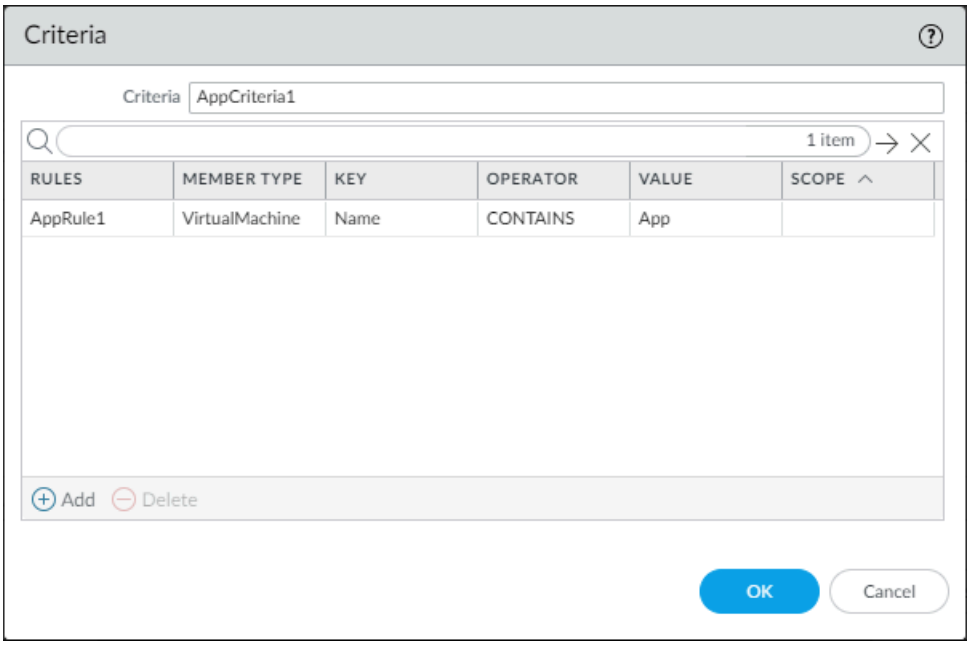
执行以下命令以查看标签列表。

```
request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
```

执行以下命令以查看与指定标签相关联的作用域。

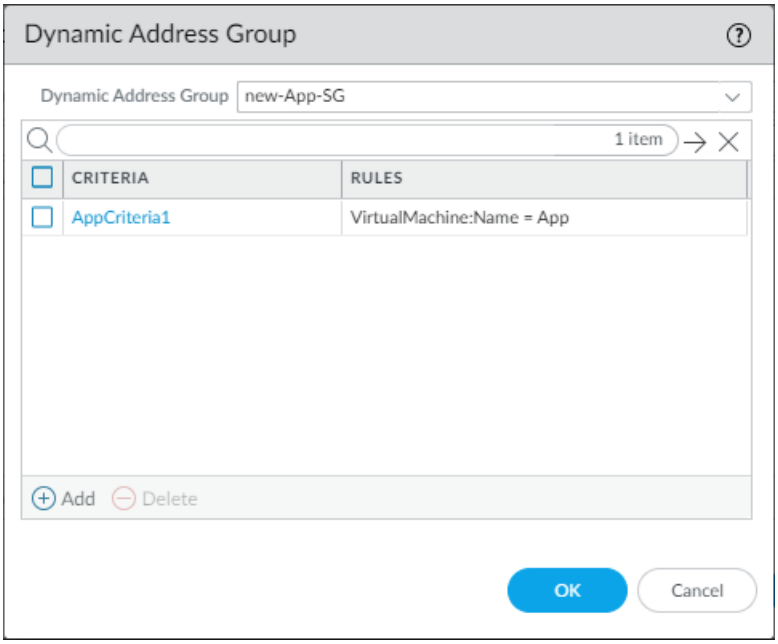
```
request plugins vmware_nsx nsx_t nsxt-scope tag <tag_value> service-definition <SD-name>
```

7. 单击 **OK**（确定）。
8. （可选）单击 **Add**（添加）以创建其他（最多五个）规则。

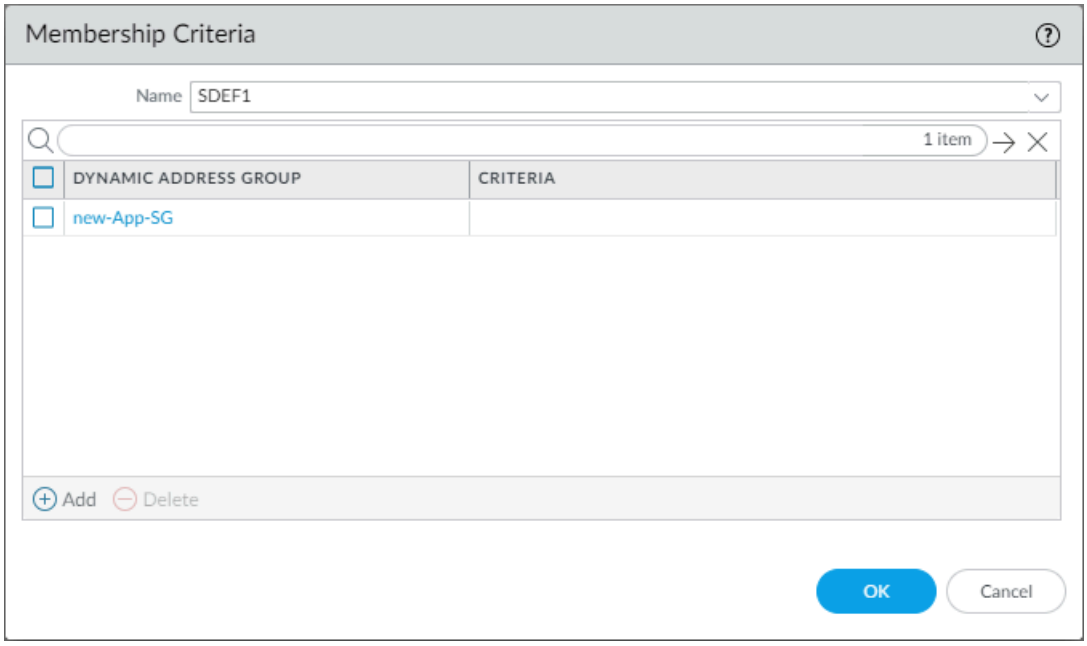


©2024 Palo Alto Networks, Inc.

STEP 9 | 在 Dynamic Address Group（动态地址组）窗口中，单击 **OK**（确定）以完成，或单击 **Add**（添加）以创建其他条件（最多五个）和规则。



STEP 10 | 在 Membership Criteria（成员资格条件）窗口中，单击 **OK**（确定）以完成，或单击 **Add**（添加）以指定其他动态地址组。



生成控制策略

NSX-T 使用控制策略来定义将流量控制到的服务链。您可以手动创建控制策略，也可以自动生成控制策略。

©2024 Palo Alto Networks, Inc.

自动生成控制策略时，适用于 VMware NSX-T 的 Panorama 插件会为每个指定的服务管理器和相关联的服务定义创建控制策略。默认情况下，TCP 严格已禁用，并将失败策略设置为允许。自动生成的策略使用 **auto_<service-def-name>_<zone-name>_steering_policy** 命名格式。

启用 TCP 严格后，防火墙会强制执行三次握手的要求。如果防火墙在会话中间获取流量（例如，由于非对称流量）且未检测到三次握手，则将丢弃会话。有关详细信息，请参阅 VMware NSX-T 文档。

失败策略定义防火墙发生故障时流量会发生什么情况。如果您选择 Allow（允许），则流量将继续到达其目标。如果您选择 Block（阻止），则将丢弃流量。

此外，您可以选择所有服务管理器而不是特定服务管理器。如果任何服务管理器包含以操作为中心的服务定义，则不建议选择 **All**（全部）。插件将为与以操作为中心的服务定义相关联的每个区域创建控制策略，然后将其推送到 NSX-T Manager。如果您选择 **All**（全部），请验证自动生成控制策略时选择的服务管理器是否仅包含以安全为中心的服务定义。

如果您自动生成控制策略，则还必须自动生成控制规则。如果您手动创建控制策略，则还必须手动创建控制规则。

- 自动生成控制策略
- 手动创建控制策略

只能在 *Panorama* 上更改控制策略；不能在 *NSX-T Manager* 上更改。如果您在 *NSX-T Manager* 上更改，则适用于 *VMware NSX* 的 *Panorama* 插件会将服务定义显示为不同步。您可以单击 ***Out-of-Sync***（不同步）链接以查看不同步状态的特定原因。如果控制策略更改是原因，请单击 ***NSX-T Config-Sync***（***NSX-T*** 配置同步）执行配置同步。

自动生成控制策略

使用以下过程自动生成控制策略。

以下步骤用于指定服务管理器，而不是选择 ***All***（全部）。

STEP 1 | 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Policy**（策略）。

STEP 2 | 单击 **Auto Generate**（自动生成）。

STEP 3 | 对于 **Service Managers**（服务管理器），请选择 **Select**（选择）。

如果您选择 ***All***（全部）而不是特定服务管理器，则插件将为与配置中的每个服务管理器相关联的每个服务定义生成控制策略。此外，请确保所选服务管理器包含以安全为中心的服务定义。

STEP 4 | 单击 **Add**（添加）以选择服务管理器。

STEP 5 | 从下拉列表中选择 **Service Manager**（服务管理器）。

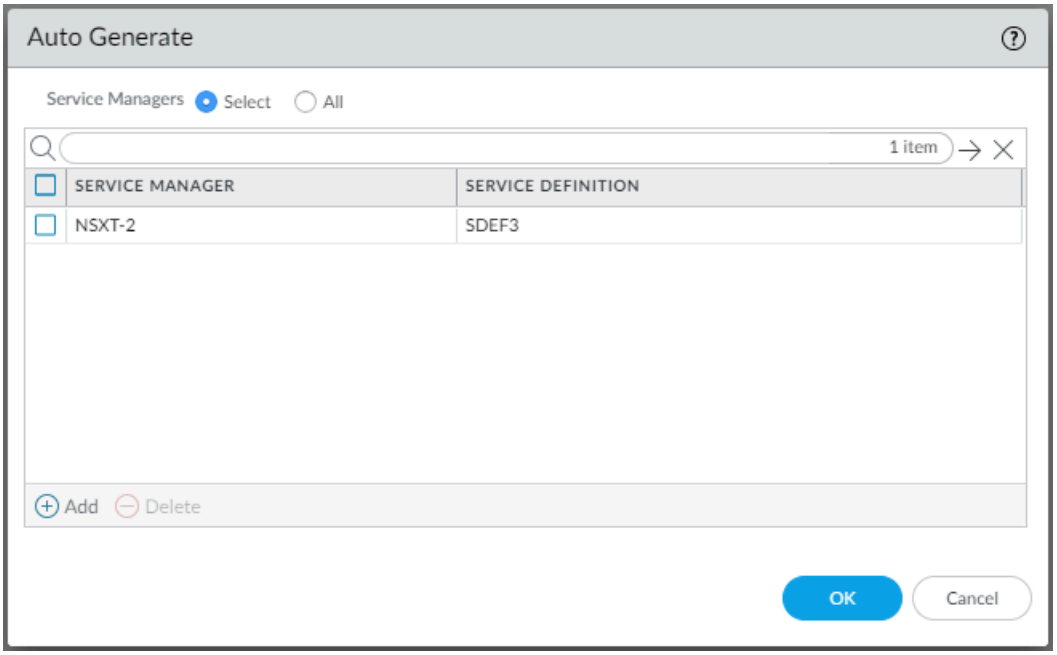
©2024 Palo Alto Networks, Inc.

STEP 6 | 单击 **Add**（添加）以选择服务定义。

STEP 7 | 从下拉列表中选择服务定义。

STEP 8 | 单击 **OK**（确定），然后再次单击 **OK**（确定）。

STEP 9 | 将更改 **Commit**（提交）到 Panorama。



手动创建控制策略

使用以下过程手动创建控制策略。

STEP 1 | 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Policy**（策略）。

STEP 2 | 单击 **Add**（添加）。

STEP 3 | 输入控制策略的描述性 **Name**（名称）。

控制策略不能包含任何空格。

STEP 4 | 从下拉列表中选择 **Service Definition**（服务定义）。

STEP 5 | 从下拉列表中选择 **Service Chain**（服务链）。

STEP 6 | （可选）启用 **TCP Strict**（**TCP** 严格）。该选项在默认情况下已禁用。

STEP 7 | 选择 **Failure Policy**（失败策略）— **Allow**（允许）或 **Block**（阻止）。默认设置为 Allow（允许）。

©2024 Palo Alto Networks, Inc.

STEP 8 | 单击 **OK**（确定）。

STEP 9 | 将更改 **Commit**（提交）到 Panorama。



生成控制规则

控制规则在控制策略中定义。规则定义流量的源和目标、自检服务、应用规则的 NSX-T 对象以及流量重定向策略。您可以手动创建控制规则或自动生成控制规则。

在生成或创建控制规则之前，您必须生成或创建控制策略。

要根据在 Panorama 上创建的安全规则自动生成控制规则，安全规则必须满足以下条件：

- 属于注册到 NSX-T Service Manager 的父或子设备组。
- 是区域内策略，仅包含一个区域。
- 不包含为规则配置的静态地址组、IP 范围或子网掩码。

自动生成的控制规则使用 **auto_<device-group-name>_<device-group-rule-name>** 命名格式。

默认情况下，在未指定 NSX 服务的情况下配置自动生成的控制规则。此外，将 NSX 流量方向设置为输入输出，禁用日志记录，IP 协议为 ipv4-ipv6，并将操作设置为重定向。自动生成规则后，您可以更新控制以更改默认值。

此外，您可以选择所有服务管理器而不是特定服务管理器。不建议选择 **All**（全部）。

如果您自动生成控制策略，则还必须自动生成控制规则。如果您手动创建控制策略，则还必须手动创建控制规则。

- 自动生成控制规则
- 手动创建控制规则

只能在 *Panorama* 上更改控制规则；不能在 *NSX-T Manager* 上更改。如果您在 *NSX-T Manager* 上更改，则适用于 *VMware NSX* 的 *Panorama* 插件会将服务定义显示为不同步。您可以单击 ***Out-of-Sync***（不同步）链接以查看不同步状态的特定原因。如果控制规则更改是原因，请单击 ***NSX-T Config-Sync***（***NSX-T*** 配置同步）执行配置同步。

©2024 Palo Alto Networks, Inc.

自动生成控制规则

使用以下过程自动生成控制规则。

自动生成控制规则时，规则的应用位置（NSX-T 分布式防火墙或安全组）取决于您在配置安全规则时指定的源和目标。如果为源或目标选择 **Any**（任何），则 NSX-T Manager 会将控制规则应用于分布式防火墙。如果为源和目标选择动态地址组，则会将控制规则应用于这些安全组中的来宾虚拟机。

如果您对设备组配置进行任何更改，而这些更改也是控制规则配置的一部分，例如映射到控制规则中的 Applied To（应用到）设置的源和目标地址组，则必须再次自动生成控制规则以使更改生效。

以下步骤用于指定服务管理器，而不是选择 ***All***（全部）。

STEP 1 | 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Rule**（规则）。

STEP 2 | 单击 **Auto Generate**（自动生成）。

STEP 3 | 从下拉列表中选择安全规则的类型 — **All**（全部）、仅 **Pre Rulebase**（前导规则库）或仅 **Post Rulebase**（后导规则库）。安全规则从以下步骤中指定的服务定义中提取。

如果您重新生成控制规则，则删除所有当前规则，并根据所选规则库创建新规则。如果您最初使用前导规则库创建控制规则，然后使用后导规则库重新生成控制规则，则只会保留后导规则库控制规则。

STEP 4 | 对于 **Type**（类型），请选择 **Select**（选择）。

STEP 5 | 单击 **Add**（添加）以指定 **Service Manager**（服务管理器）和 **Service Definition**（服务定义）。

STEP 6 | 从下拉列表中选择 **Service Manager**（服务管理器）。

STEP 7 | 单击 **Add**（添加）以选择服务定义。

STEP 8 | 单击 **OK**（确定）。

STEP 9 | 单击 **OK**（确定）以完成，或单击 **Add**（添加）以指定其他服务管理器和服务定义。

©2024 Palo Alto Networks, Inc.

STEP 10 | （可选）单击自动生成的规则以修改以下默认选项。

如果您重新生成控制规则，则将覆盖您对先前生成的控制规则所做的任何更改。

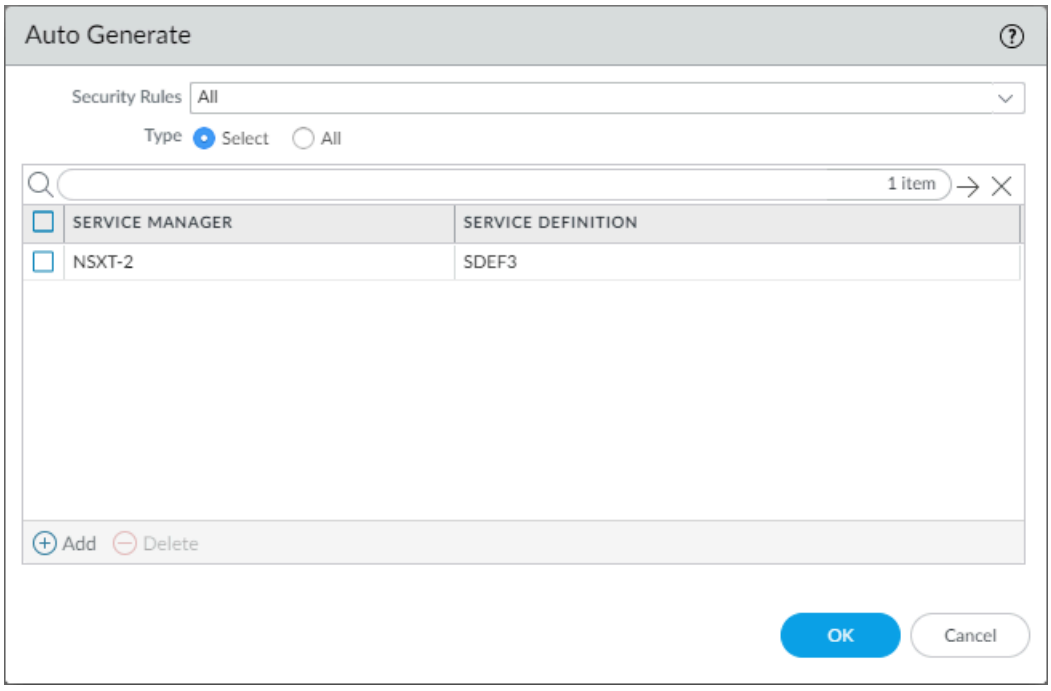
- 启用 NSX-T **Logging**（日志记录）。
- 单击 **Add**（添加）以指定 **NSX Services**（**NSX** 服务），例如 Active Directory Server、HTTPS、DNS 等。
- **Disable**（禁用）规则。如果您禁用控制规则，但启用相应的安全规则（**Device Group**（设备组）> **Policies**（策略）> **Security**（安全）），则也将启用控制规则。
- **Applied to**（应用于）允许您更改应用控制规则的位置 - **DFW** 或 **Security Group**（安全组）。

STEP 11 | 清理不需要或不正确的控制规则。

例如，如果您的设备组在与 NSX-T 控制规则相同的规则库中包含安全规则，则插件会根据这些非 NSX-T 安全规则生成安全规则。由于这些规则不引用 NSX-T 动态地址组，因此会在 NSX-T Manager 中将这些规则的源和目标设置为 Any（任何）。这种情况可能会影响 NSX-T Manager 定向流量的方式。为避免这种情况，您必须手动删除不正确的控制规则。

1. 选择不正确的控制规则。
2. 单击 **Delete**（删除）。
3. 单击 **Yes**（是）以确认删除。

STEP 12 | **Commit**（提交）您的配置以将其推送到 NSX-T Manager。



©2024 Palo Alto Networks, Inc.

手动创建控制规则

使用以下过程手动创建控制规则。

STEP 1 | 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Rule**（规则）。

STEP 2 | 单击 **Add**（添加）。

STEP 3 | 输入控制规则的描述性 **Name**（名称）。

控制规则不能包含任何空格。

STEP 4 | 从下拉列表中选择 **Steering Policy**（控制策略）。

STEP 5 | 从下拉列表中选择 **Device Group**（设备组）。

STEP 6 | 从下拉列表中选择 **Security Rule**（安全规则）。

安全规则下拉列表显示服务定义的所有设备组的所有安全规则中的规则。确保选择合适的安全规则。

STEP 7 | 指定 **Action**（操作）— **Redirect**（重定向）或 **Do Not Redirect**（不重定向）。

STEP 8 | （可选）启用 NSX-T **Logging**（日志记录）。

STEP 9 | 指定 **IP Protocol**（**IP** 协议）— **ipv4-ipv6**、**ipv4** 或 **ipv6**。

STEP 10 | 指定 **NSX Traffic Direction**（**NSX** 流量方向）— **in-out**（输入输出）、**in**（输入）或 **out**（输出）。

STEP 11 | （可选）单击 Add（添加）以指定 **NSX Services**（**NSX** 服务），例如 Active Directory Server、HTTPS、DNS 等。

不支持以下 *ALG* 服务：*FTP*、*TFTP*、*ORACLE_TNS*、*SUN_RPC_TCP*、*SUN_RPC_UDP*、*MS_RPC_TCP*、*MS_RPC_UDP*

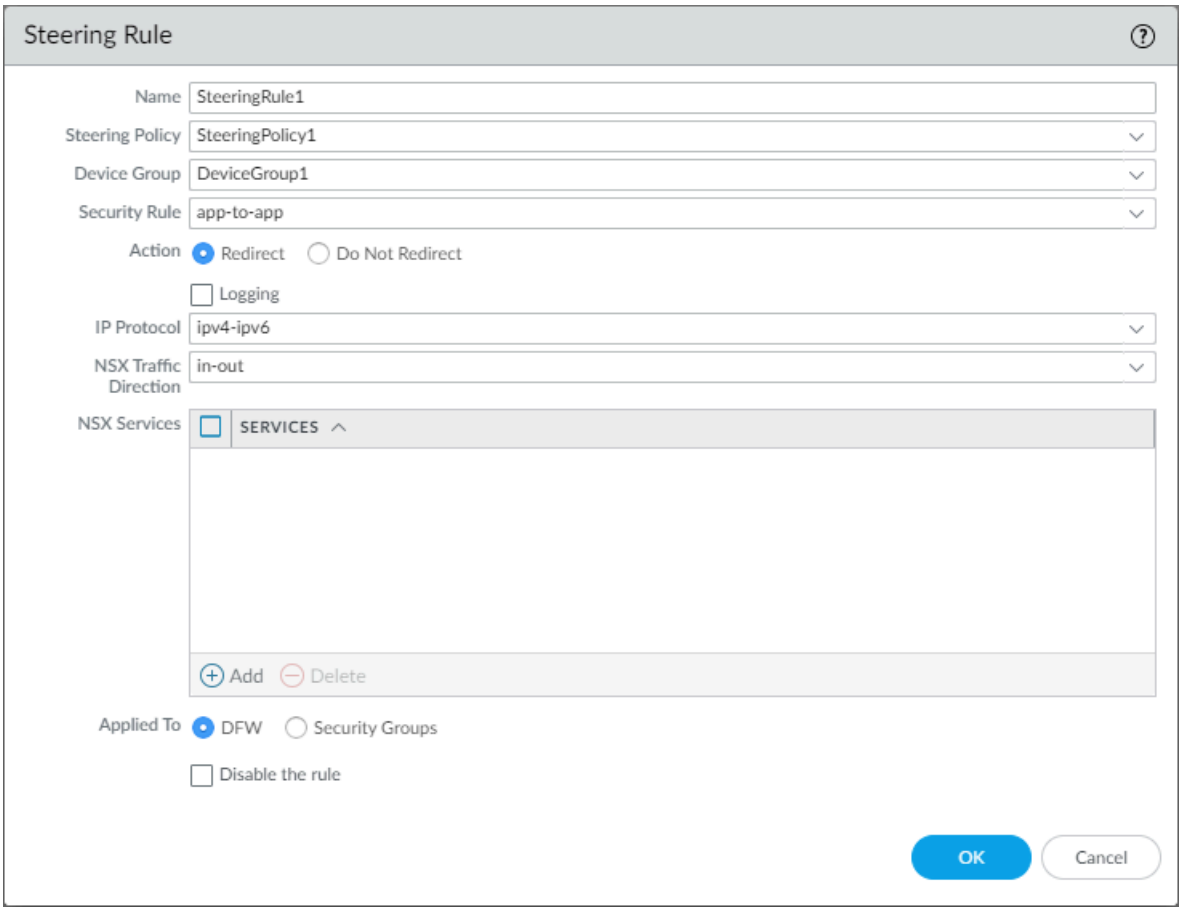
STEP 12 | **Applied To**（应用于）— **DFW** 或 **Security Groups**（安全组）。您可以选择一个或多个安全组。安全组从 Panorama 上配置的动态地址组创建。安全组名称的格式为 **<servicedefinition>_<dynamic-address-group>**。如果您选择 DFW，则将控制规则应用于所有来宾 VM，无论其安全成员如何。

STEP 13 | （可选）禁用规则。

STEP 14 | 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 15 | **Commit**（提交）您的配置以将其推送到 NSX-T Manager。



从 Panorama 中删除服务定义

完成以下过程以从 Panorama 上的 NSX-T 配置中删除服务定义。

STEP 1 | 登录到 Panorama。

STEP 2 | 对于以安全为中心的部署，请删除与要删除的服务定义相关联的控制规则和控制策略。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Rules**（规则）。
2. 选择要删除的控制规则。
3. 单击 **Delete**（删除）。
4. 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Policy**（策略）。
5. 选择要删除的控制策略。
6. 单击 **Delete**（删除）。

STEP 3 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 4 | 删除 NSX-T 中部署的与要删除的服务定义相关联的 VM 系列防火墙。

STEP 5 | 删除与服务定义相关联的成员资格条件。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Membership Criteria**（成员资格条件）。
2. 选择要删除的条件。
3. 单击 **Delete**（删除）。

STEP 6 | 取消服务定义与其相关联的服务管理器的链接。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服务管理器）。
2. 单击服务管理器名称。
3. 选择服务定义。
4. 单击 **Delete**（删除）。
5. 单击 **OK**（确定）。

STEP 7 | 将更改 **Commit**（提交）到 Panorama。

从 NSX-T 操作上的 VM 系列迁移到以安全为中心的部署

使用以下过程将以操作为中心的 NSX-T 部署迁移到以安全为中心的 NSX-T 部署。

STEP 1 | 登录到 Panorama。

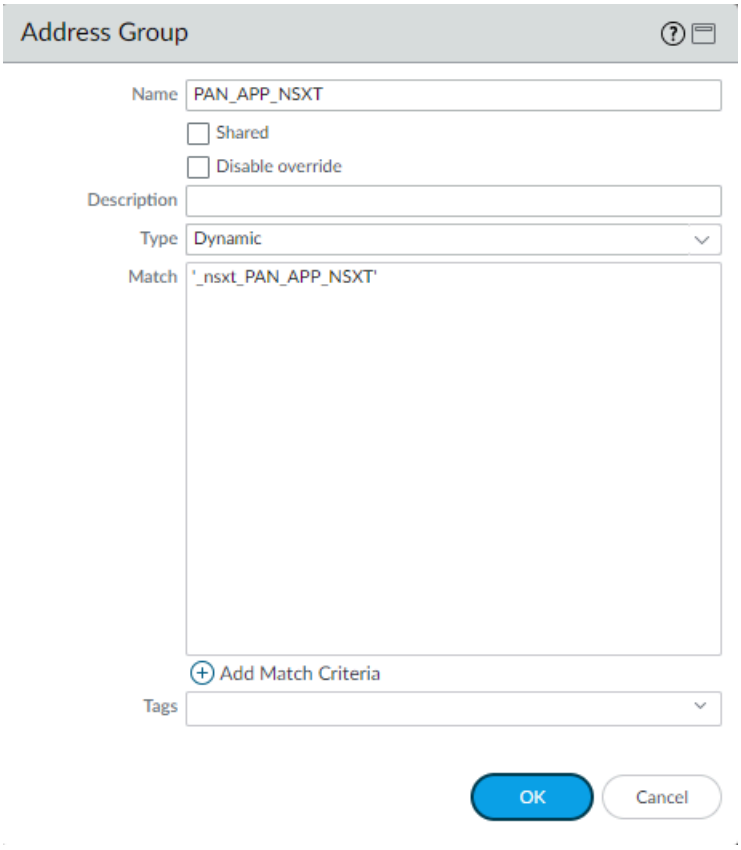
 ©2024 Palo Alto Networks, Inc.

STEP 2 | 修改动态地址组的匹配条件，以遵循以安全为中心的部署所需的格式。

1. 选择 **Object**（对象） > **Address Groups**（地址组）。
2. 验证您是否在与 NSX-T 服务定义相关联的设备组中配置动态地址组。
3. 单击之前创建的 NSX-T 动态地址组的名称。
4. 编辑匹配条件。

   要使动态地址组成为 *NSX-T Manager* 中的安全组，匹配条件字符串必须用单引号括起来，前缀为 *_nsxt_*，后跟地址组的确切名称。例如，***'_nsxt_PAN_APP_NSX'***。

5. 对于需要的每个安全组，请重复执行此流程。



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 将安全规则设置为区域内的 NSX-T 控制规则。

1. 在 Panorama 中，选择 **Policies**（政策） > **Security**（安全） > **Pre Rules**（操作规则）。
2. 验证您是否在与 NSX-T 服务定义相关联的设备组中配置安全规则。
3. 单击 **Add**（添加），并输入安全策略规则的 **Name**（名称）和 **Description**（说明）。
4. 将规则类型设置为 **intrazone (Devices with PAN-OS 6.1 or later)**（区域内（带有**PAN-OS 6.1**或更高版本的设备））。
5. 在 Source（源）选项卡中，将源区域设置为与服务定义关联的模板堆栈中的区域。然后，选择您之前创建的动态地址组作为源地址。不要将任何静态地址组，IP 范围或网络掩码添加为源地址。
6. 在 Destination（目标）选项卡中，Panorama 不允许您设置目标区域，因为您将规则类型设置为区域内。然后，选择您之前创建的动态地址组作为目标地址。不要将任何静态地址组，IP 范围或网络掩码添加为目标地址。
7. 单击 **OK**（确定）。
8. 对于所需的每项控制规则，请重复步骤 1 到 7。
9. **Commit**（提交）更改。

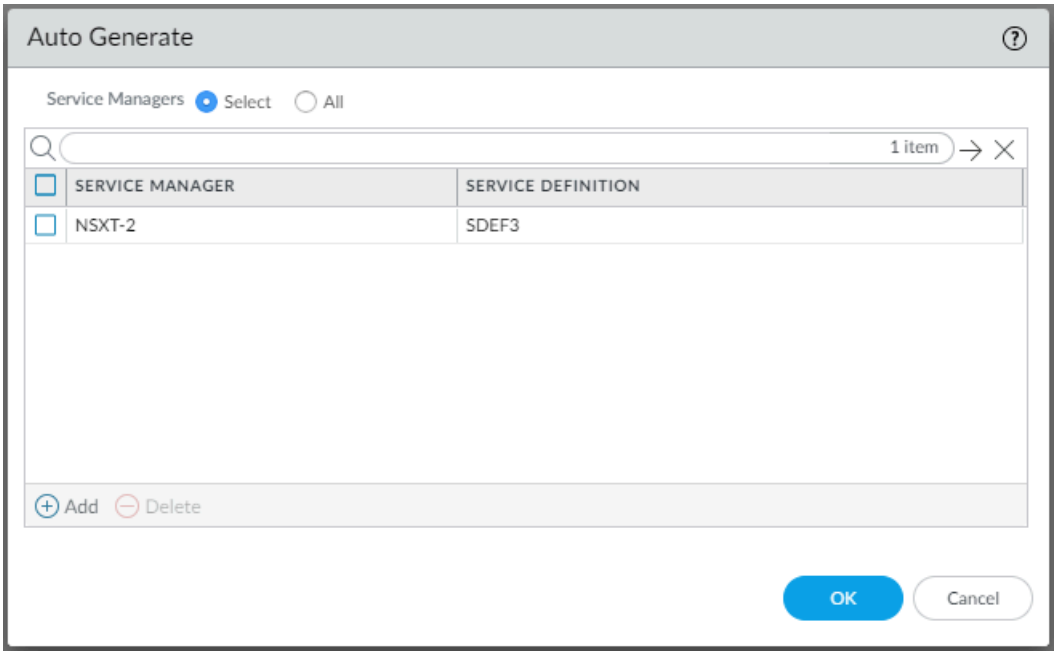
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 自动生成新的控制策略。

以下步骤用于指定服务管理器，而不是选择 **All**（全部）。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Policy**（策略）。
2. 单击 **Auto Generate**（自动生成）。
3. 对于 **Service Managers**（服务管理器），请选择 **Select**（选择）。

   如果您选择 ***All***（全部）而不是特定服务管理器，则插件将为与配置中的每个服务管理器相关联的每个服务定义生成控制策略。
4. 单击 **Add**（添加）以选择服务管理器。
5. 从下拉列表中选择 **Service Manager**（服务管理器）。
6. 单击 **Add**（添加）以选择服务定义。
7. 从下拉列表中选择服务定义。
8. 单击 **OK**（确定），然后再次单击 **OK**（确定）。



9. **Commit**（提交）更改。

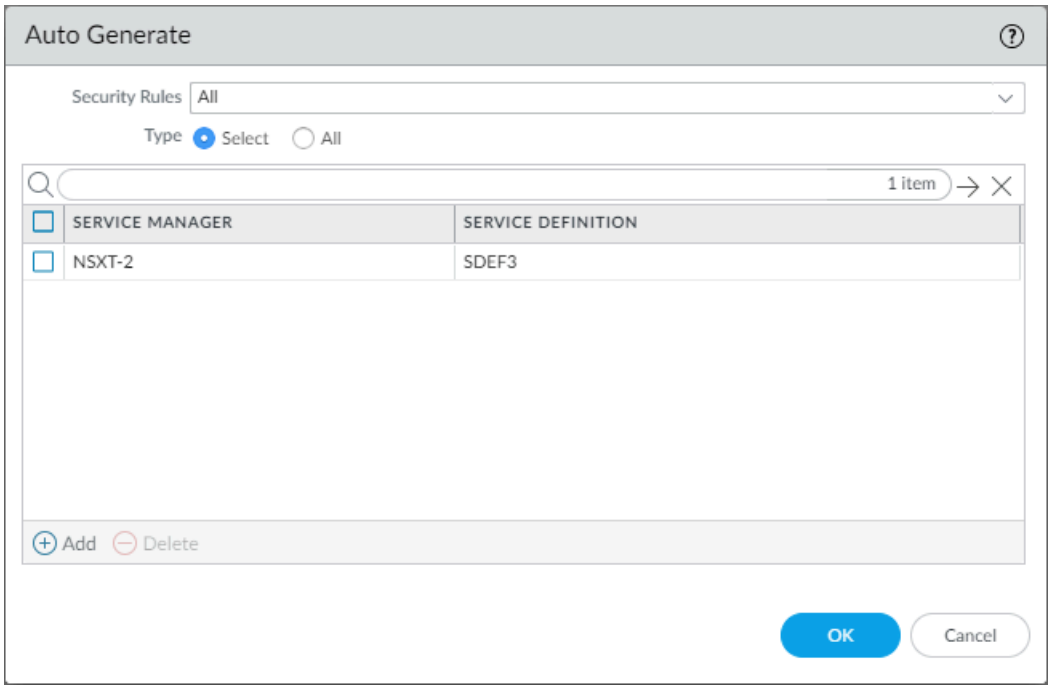
©2024 Palo Alto Networks, Inc.

STEP 5 | 自动生成新的控制规则。

如果您自动生成控制策略，则还必须自动生成控制规则。如果您手动创建控制策略，则还必须手动创建控制规则。

以下步骤用于指定服务管理器，而不是选择 ***All***（全部）。

1. 选择 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（网络自检） > **Rule**（规则）。
2. 单击 **Auto Generate**（自动生成）。
3. 从下拉列表中选择安全规则的类型 — **All**（全部）、仅 **Pre Rulebase**（前导规则库）或仅 **Post Rulebase**（后导规则库）。安全规则从以下步骤中指定的服务定义中提取。
4. 对于 **Type**（类型），请选择 **Select**（选择）。
5. 单击 Add（添加）以指定 **Service Manager**（服务管理器）和 **Service Definition**（服务定义）。
6. 从下拉列表中选择 **Service Manager**（服务管理器）。
7. 单击 **Add**（添加）以选择服务定义。
8. 单击 **OK**（确定）。
9. 单击 **OK**（确定）以完成，或单击 **Add**（添加）以指定其他服务管理器和服务定义。
10. （可选）单击自动生成的规则以修改默认选项。



STEP 6 | 创建动态地址组成员资格条件.

STEP 7 | 将更改 **Commit**（提交）到 Panorama。

©2024 Palo Alto Networks, Inc.

STEP 8 | 从 NSX-T Manager 中删除以操作为中心的控制规则。

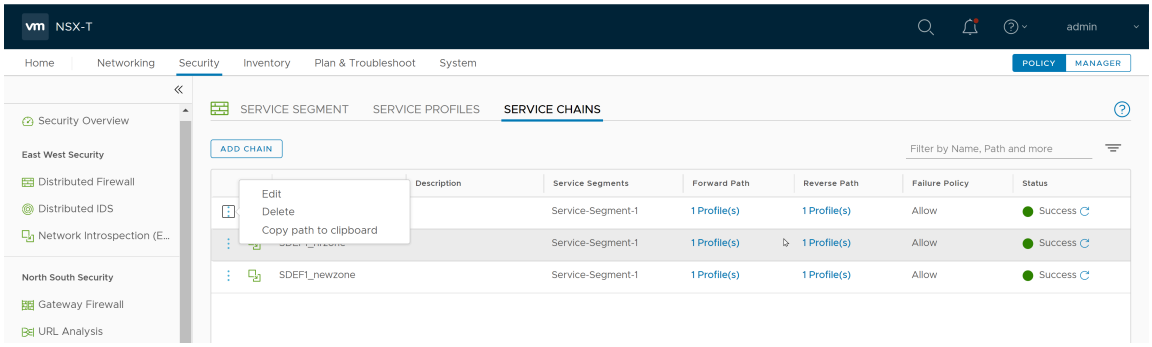
1. 登录到 NSX-T Manager。
2. 选择 **Security**（安全） > **Network Introspection (E-W)**（网络自检 **(E-W)**） > **Rules**（规则）。
3. 选择每个以操作为中心的控制规则。
4. 单击 **Delete**（删除）。

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 从 NSX-T Manager 中删除以操作为中心的服务链。

1. 登录到 NSX-T Manager。
2. 选择 **Security**（安全） > **Network Introspection Settings**（网络自检设置） > **Service Chains**（服务链）。
3. 单击垂直省略号。
4. 单击 **Delete**（删除）。

 ©2024 Palo Alto Networks, Inc.



将安全策略从 NSX-V 扩展到 NSX-T

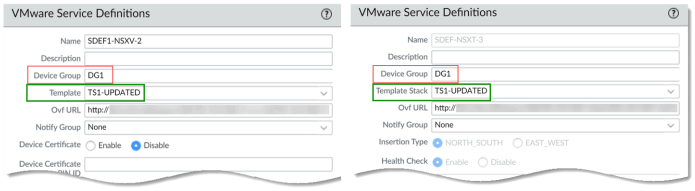
如果您要从 NSX-V 部署迁移到 NSX-T 部署，或将 NSX-T 部署与 NSX-V 部署进行组合，则可以将现有安全策略从 NSX-V 扩展到 NSX-T，而无需重新创建安全策略规则。这可以通过利用现有设备

©2024 Palo Alto Networks, Inc.

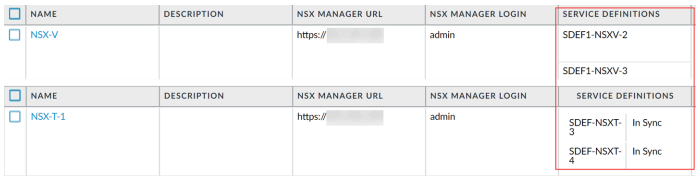
组并在 NSX-V 和 NSX-T 服务定义之间进行共享来实现。将安全策略迁移到 NSX-T 后，您可以继续为 NSX-V 使用 VM 系列或删除 NSX-V 部署。

STEP 1 | 安装适用于 VMware NSX 的 Panorama 插件 3.2.0 或更高版本。在升级之前，请参阅适用于 VMware NSX 3.2.0 的Panorama 插件发行说明。

STEP 2 | 为部署中的每个 NSX-V 服务定义定义 NSX-T 服务定义。不创建新的设备组；而是使用现有的 NSX-V 设备组。使用现有设备组，您可以将 NSX-V 上使用的同一安全策略规则应用于 NSX-T 上部署的 VM 系列防火墙。如果您拥有引用特定区域的策略，请将同一模板堆栈从 NSX-V 服务定义添加到 NSX-T 服务定义。此外，如果设备组引用特定模板，请确保选择包括该设备组中引用的模板的模板堆栈。



STEP 3 | 配置 NSX-T 服务管理器，并将 NSX-T 服务定义与服务管理器相关联。



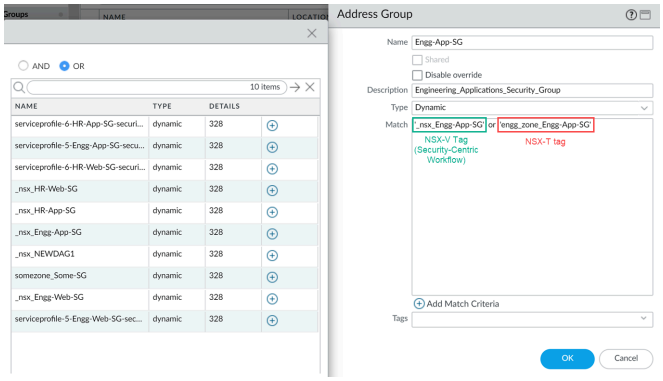
STEP 4 | 准备 NSX-T 环境并部署 VM 系列防火墙。在启动 VM 系列防火墙之前，您必须创建安全组、服务链和流量重定向策略。

- 在 NSX-T 上部署 VM 系列防火墙（北向南）
- 使用以操作为中心的工作流程部署 VM 系列

©2024 Palo Alto Networks, Inc.

STEP 5 | 将 NSX-T 标记添加到现有的动态地址组。

1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
2. 单击现有 NSX-V 动态地址组的名称。
3. 单击 **Add Match Criteria**（添加匹配条件）以显示 NSX-V 和 NSX-T 的标记。
4. 将 NSX-T 标记添加到动态地址组。确保在标记之间使用 **OR** 运算符。
5. 添加所有必需的标记后，单击 **OK**（确定）。
6. **Commit**（提交）更改。



STEP 6 | 将 VM 工作负载成功从 NSX-V 迁移到 NSX-T 后，如果您计划停止使用 NSX-V，则可以从动态地址组删除 NSX-V 标记。从适用于 NSX 的 Panorama 插件删除所有与 NSX-V 相关的信息，以及从 NSX-V Manager 删除 VM 系列防火墙配置后，将取消注册所有 NSX-V 标记和相应的 IP 地址。

使用就地迁移将 VM 系列从 NSX-V 迁移到 NSX-T

完成以下过程，以将 VM 系列防火墙配置从 NSX-V 迁移到 NSX-T。通过迁移配置，您可以重用已在 Panorama 上配置的策略和动态地址组。此过程涉及 VMware 文档中发布的信息和流程，以及 PAN 特定的步骤。

此过程仅支持以操作为中心的 NSX-V 部署。部署意味着将流量重定向到 VM 系列防火墙的策略规则是在 NSX-V Manager（而非 Panorama）中所创建。

此过程需要 *NSX-T Manager 3.1.0* 或更高版本。

建议在执行此迁移时计划安全停机时间。

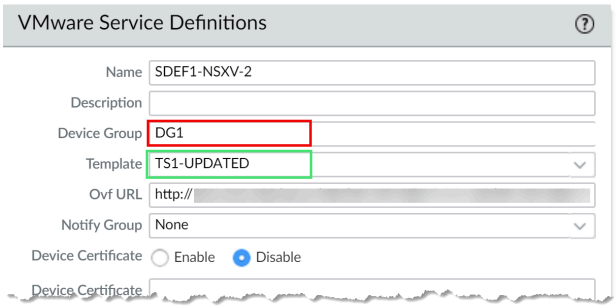
STEP 1 | 根据 VMware 所述的步骤，为迁移准备 NSX-V 和 NSX-T 环境。

STEP 2 | 安装适用于 VMware NSX 的 Panorama 插件 3.2.0 或更高版本。在升级之前，请参阅适用于 VMware NSX 3.2.0 的Panorama 插件发行说明。

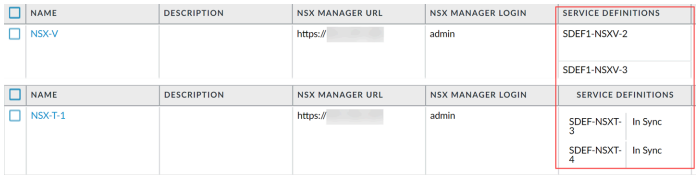
STEP 3 | 启用 NSX-T Manager 与 Panorama 之间的通信.

©2024 Palo Alto Networks, Inc.

STEP 4 | 为部署中的每个 NSX-V 服务定义定义 NSX-T 服务定义。不创建新的设备组；而是使用现有的 NSX-V 设备组。使用现有设备组，您可以将 NSX-V 上使用的同一安全策略规则应用于 NSX-T 上部署的 VM 系列防火墙。如果您拥有引用特定区域的策略，请将同一模板堆栈从 NSX-V 服务定义添加到 NSX-T 服务定义。此外，如果设备组引用特定模板，请确保选择包括该设备组中引用的模板的模板堆栈。



STEP 5 | 配置 NSX-T 服务管理器，并将 NSX-T 服务定义与服务管理器相关联。



STEP 6 | 验证 NSX-T Manager 上是否存在 NSX-T 配置。

1. 登录到 NSX-T Manager。
2. 选择 **System**（系统） > **Service Deployments**（服务部署） > **Catalog**（目录）。
3. 确认已列出 NSX-T 服务定义。
4. 选择 **Security**（安全） > **Network Introspection Settings**（网络自检设置） > **Service Profiles**（服务配置文件）。
5. 确认已列出与 NSX-T 模板相关联的区域。

STEP 7 | 如果尚未执行此操作，请在 NSX-T Manager 中添加计算管理器。确认注册状态和连接状态正常后，请继续执行下面的步骤。

STEP 8 | 将 NSX-V 配置导入 NSX-T。

©2024 Palo Alto Networks, Inc.

STEP 9 | 从 NSX-V 卸载服务实例。



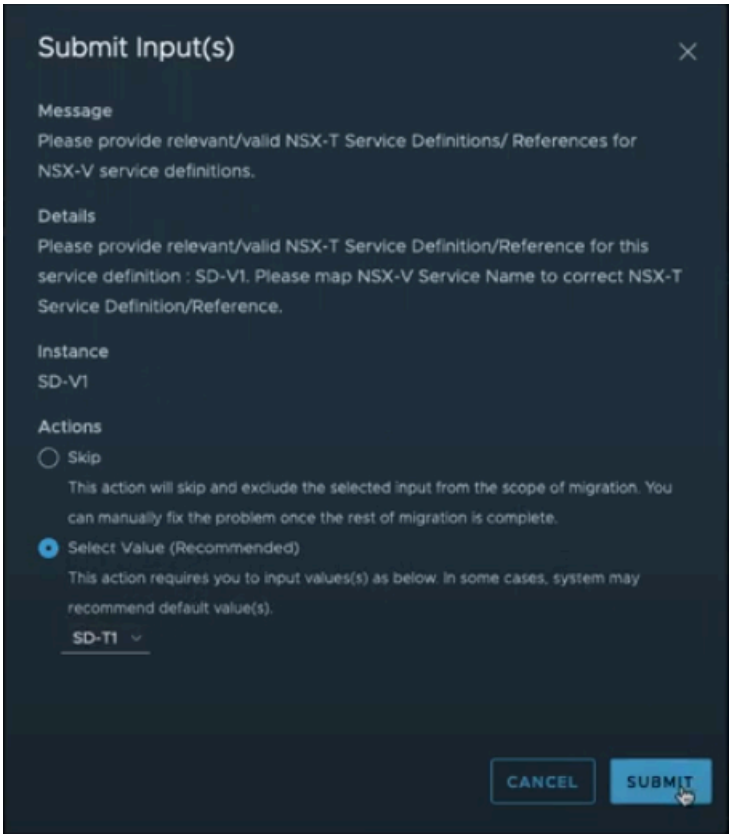
此步骤将可能会导致流量中断。

1. 登录到 vSphere 客户端。
2. 选择 **Installation and Upgrade**（安装和升级） > **Service Deployment**（服务部署）。
3. 选择服务部署。
4. 单击 **Delete**（删除）。
5. 单击 **Delete**（删除）以确认。

©2024 Palo Alto Networks, Inc.

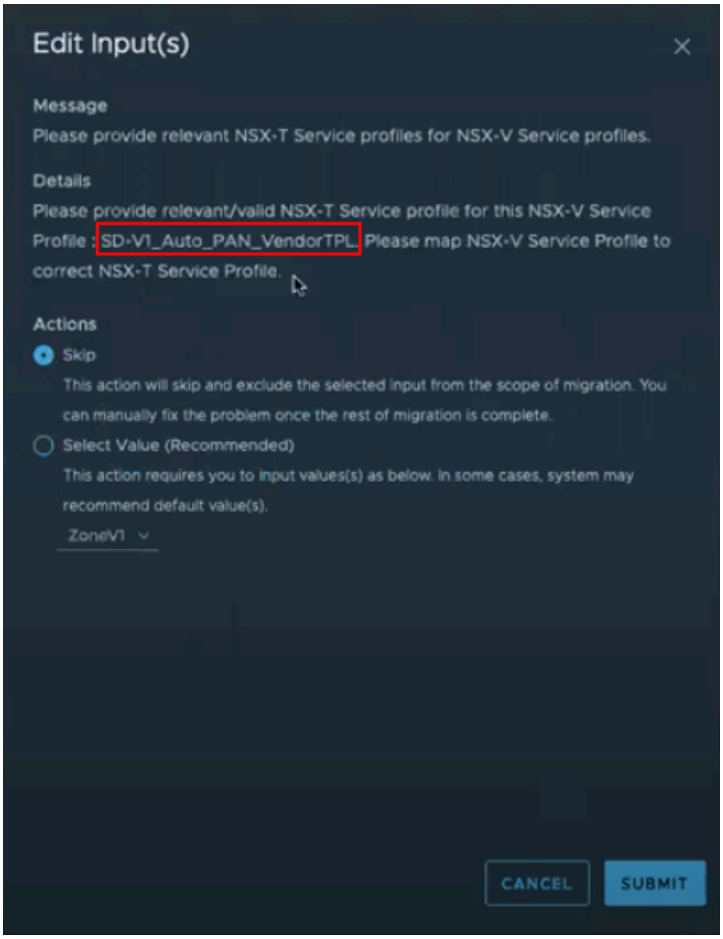
STEP 10 | 在 NSX-T Manager 上解决配置问题。解决配置问题时，您必须执行特定操作以迁移 VM 系列防火墙配置。在大多数情况下，您可以接受 NSX-T Manager 提出的建议。

1. 解决服务插入配置问题时，请验证您是否已选择之前在 Panorama 上为 NSX-T 上的 VM 系列配置的正确服务定义。



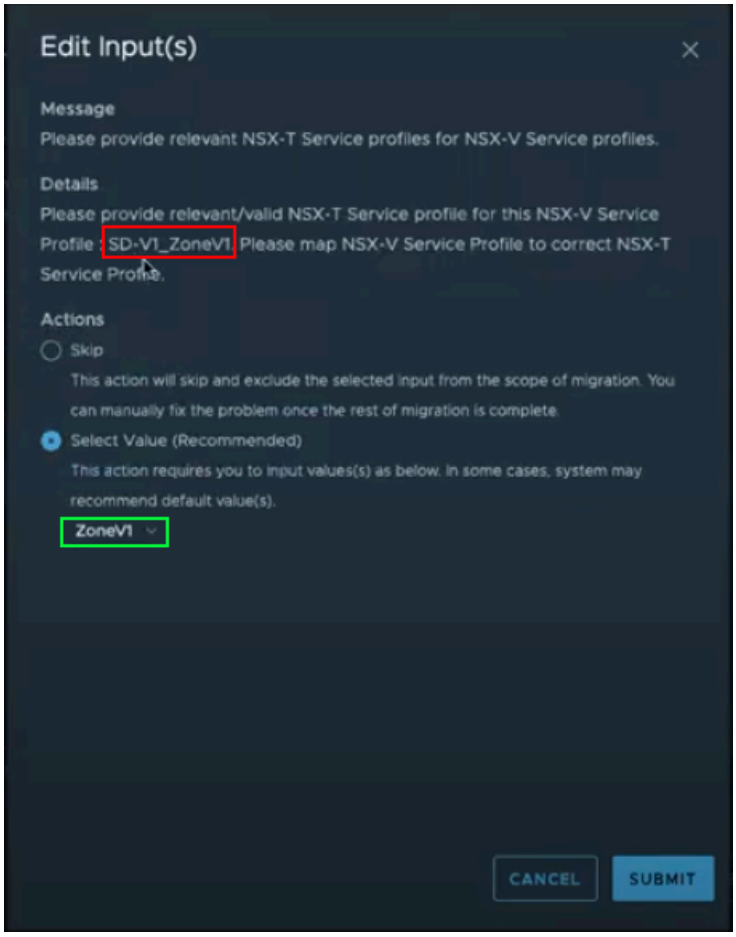
2. 继续解决剩余配置问题。
3. 在移至 **Migrate Configuration**（迁移配置）之前，将会要求您提供用于服务插入的传输区域。
4. 将 NSX-V 上的服务配置文件映射到 NSX-T 上的相应服务配置文件。
    1. 可以跳过 Auto_PAN_VendorTPL。

 ©2024 Palo Alto Networks, Inc.



2. 将 NSX-T 服务配置文件映射到相应的 NSX-V 服务配置文件。

 ©2024 Palo Alto Networks, Inc.



STEP 11 | 迁移配置。

STEP 12 | 确认您的配置已成功迁移。

1. 选择 **Inventory**（清单）> **Groups**（组）以验证 IP 集和安全组是否存在。您可以单击安全组名称，以查看正确的 IP 地址是安全组的一部分。
2. 选择 **Security**（安全）> **Network Introspection Settings**（网络自检设置）> **Service Segment**（服务段），以确认已创建服务段。
3. 选择 **Security**（安全）> **Network Introspection Settings**（网络自检设置）> **Service Chains**（服务链），以确认已创建服务链。单击 Forward Path（转发路径）和 Reverse Path（反向路径）列中的 Profiles（配置文件）链接以查看服务配置文件。
4. 选择 **Security**（安全）> **Network Introspection (E-W)**（网络自检 **(E-W)**），以确认已创建流量重定向规则，可将流量定向到 VM 系列防火墙的服务配置文件。

STEP 13 | 如果适用，请修改和迁移边缘。

STEP 14 | 配置和迁移您的主机。

©2024 Palo Alto Networks, Inc.

STEP 15 | 将 NSX-T 标记添加到现有的动态地址组。

1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
2. 单击现有 NSX-V 动态地址组的名称。
3. 单击 **Add Match Criteria**（添加匹配条件）以显示 NSX-V 和 NSX-T 的标记。
4. 将 NSX-T 标记添加到动态地址组。如果选择不删除 NSX-V 标记，请确保在标记之间使用 **OR** 运算符。
5. 添加所有必需的标记后，单击 **OK**（确定）。
6. **Commit**（提交）更改。

STEP 16 | 在 NSX-T 上启动 VM 系列防火墙（东向西）.您无需创建新的服务段；而是选择在迁移过程中创建的服务段。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 AWS 上设置 VM 系列防火墙

可以在 Amazon Web 服务 (AWS) 公共云和 AWS GovCloud 上部署 VM 系列防火墙。然后，可以配置 VM 系列防火墙保护访问在 EC2 实例上部署并置于 AWS 上虚拟私有云 (VPC) 的应用程序。

- 关于 AWS 上的 VM 系列防火墙
- AWS 上支持的部署
- 在 AWS 上部署 VM 系列防火墙
- VM 系列与 AWS 网关负载均衡器集成
- AWS 上 VM 系列防火墙的高可用性
- 用例：保护 AWS 云中的 EC2 实例
- 用例：使用动态地址组保护 VPC 中的新 EC2 实例
- 用例：VM 系列防火墙作为 AWS 上的 GlobalProtect 网关
- AWS 上的 VM 监控
- 在 AWS VPC 上监控的属性列表

关于 AWS 上的 VM 系列防火墙

Amazon Web 服务 (AWS) 是一种公共云服务，能够让您在由 Amazon 管理的共享基础架构上运行应用程序。可以在不同 AWS 区域的可扩展计算容量或 EC2 实例上部署这些应用程序，并由用户通过 Internet 进行访问。

为了网络一致性和轻松管理 EC2 实例，Amazon 提供了虚拟私有云 (VPC)。VPC 从 AWS 公共云中分配，并从私人网络空间分配 CIDR 块 (RFC 1918)。在 VPC 中，您可以根据需要细分公共/私有子网，并在这些子网内的 EC2 实例上部署应用程序。然后，为了能够访问 VPC 内的应用程序，您可以在 EC2 实例上部署 VM 系列防火墙。最后，可以配置 VM 系列防火墙保护流向和来自 VPC 内 EC2 实例的流量。

VM 系列防火墙适用于 AWS 公共云和 AWS GovCloud。公共 AWS 和 AWS GovCloud 中的 VM 系列防火墙支持自带许可证 (BYOL) 模式和以小时计的即用即付 (PAYG) 模式，后者为基于使用情况的许可模式，可从 AWS Marketplace 获取。关于许可证详细信息，请参阅 面向公共云的 VM 系列防火墙许可证。

- AWS EC2 实例类型
- AWS GovCloud 上的 VM 系列防火墙
- AWS China 上的 VM 系列防火墙
- AWS Outposts 上的 VM 系列防火墙
- AWS 术语
- 管理接口映射以用于 Amazon ELB
- 在 AWS 上调整 VM 系列防火墙性能

AWS EC2 实例类型

有关支持的实例类型，请参阅 EC2 实例上的 VM 系列型号。

您可以在 AWS 实例大小上部署 VM 系列防火墙，并使用比最低 VM 系列系统要求更多的资源。如果您为 VM 系列防火墙型号选择较大的实例大小，尽管防火墙只使用表中所示的最大 vCPU 内核和内存，但它可利用 AWS 提供的更快的网络性能。如果您要更改使用 BYOL 选项许可的 VM 系列防火墙上的实例类型，必须在切换实例类型之前停用 VM 以确保许可证有效。请参阅升级 VM 系列型号以了解原因。

有关在 AWS 上调整 VM 系列防火墙大小的指导，请参阅此文章。

AWS GovCloud 上的 VM 系列防火墙

AWS GovCloud 是一种独立的 AWS 区域，该区域符合美国政府机构和客户在法规符合性方面的要求。

©2024 Palo Alto Networks, Inc.

为保护 AWS GovCloud（美国）区域中含各类受控非密信息 (CUI) 数据及可公用政府主导数据的工作负载，VM 系列防火墙在标准 AWS 公共云及 AWS GovCloud 上提供同样强大的安全功能。AWS GovCloud 上的 VM 系列防火墙和标准 AWS 公共云均支持相同的功能。

请参阅 AWS GovCloud 上的 AMI 到 在 AWS 上部署 VM 系列防火墙。

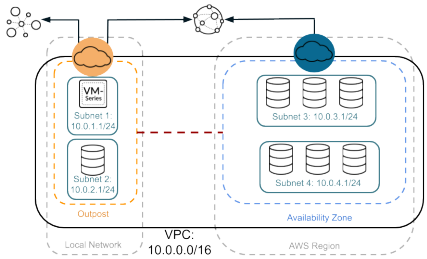
AWS China 上的 VM 系列防火墙

VM 系列防火墙在 AWS China Marketplace 带有 BYOL 选项，并在 AWS China（北京）和 AWS China（宁夏）地区提供。您必须拥有独立于您的全球 AWS 帐户的 AWS China 帐户才能访问此映像并在 AWS China 上使用 AWS 资源 。

请务必先查看 VM 系列系统要求，然后 在 AWS 上启动 VM 系列防火墙。

AWS Outposts 上的 VM 系列防火墙

要为本地工作负载提供与 AWS Cloud 中的工作负载相同级别的安全，您可以在本地位置 AWS Outposts 机架的 AWS 上安装 VM 系列防火墙。使用适用于 AWS 地区的 AWS Marketplace BYOL AMI，在 AWS Outposts 子网中部署 VM 系列防火墙实例。



要在 Palo Alto Networks 客户支持网站上创建支持帐户并注册 VM 系列防火墙，从而通过 Palo Alto Networks 激活支持授权，请参阅注册 VM 系列防火墙（使用授权代码）。

AWS 术语

本文档假定您熟悉在 AWS VPC 上设置网络和配置。下面简短回顾了本文档中引用的 AWS 术语（有些定义是直接从 AWS 词汇中采用），目的是为本节中使用的术语提供上下文：

术语	说明
EC2	弹性计算云 一种 Web 服务，能够让您在 Amazon 的数据中心启动和管理 Linux/UNIX 和 Windows 服务器实例。
AMI	Amazon 机器映像 AMI 提供了启动实例（即云中的虚拟服务器）所需的信息。

©2024 Palo Alto Networks, Inc.

术语	说明
	VM 系列 AMI 是一种加密的机器映像，包括在 EC2 实例上实例化 VM 系列防火墙所需的操作系统。
ELB	弹性负载均衡 ELB 是一种 Amazon Web 服务，该服务可通过跨多个弹性计算云 (EC2) 实例的路由来实现应用程序在可用性及可扩展性方面的提升。ELB 会检测不正常的 EC2 实例，再将流量重新路由到正常实例，直到不正常实例还原为止。ELB 只能将流量发送到下一个跃点负载均衡 EC2 实例的主接口。所以，要在 AWS 上通过 VM 系列防火墙使用 ELB，防火墙必须能够使用数据面板流量的主接口。
ENI	弹性网络接口 可以将其他网络接口附加到 EC2 实例。ENI 可以包括主要专用 IP 地址、一个或多个次要专用 IP 地址、公共 IP 地址、弹性 IP 地址（可选）、MAC 地址、指定安全组成员、说明和源/目标检查标记。
EC2 实例的 IP 地址类型	EC2 实例可以有不同的 IP 地址类型。 • 公共 IP 地址：可以通过 Internet 路由的 IP 地址。 • 专用 IP 地址：位于在 RFC 1918 中定义的专用 IP 地址范围的 IP 地址。您可以选择手动分配 IP 地址，也可以选择在启动 EC2 实例的子网的 CIDR 块范围内自动分配 IP 地址。 如果您手动分配 IP 地址，Amazon 将保留每个子网中的前四 (4) 个 IP 地址和最后一 (1) 个 IP 地址，以用于 IP 联网目的。 • 弹性 IP 地址 (EIP)：一种在 Amazon EC2 或 Amazon VPC 中分配的静态 IP 地址，然后可以将其附加到实例。弹性 IP 地址与您的帐户相关联，而与特定实例不相关联。它们具有弹性，因为您可以根据需求的变化轻松分配、附加、分离和释放它们。 公共子网中的实例可以有专用 IP 地址、公共 IP 地址和弹性 IP 地址 (EIP)；专用子网中的实例可以有专用 IP 地址，也可以有 EIP。
实例类型	Amazon 定义的规范，用于规定实例的内存，CPU、存储容量和每小时成本。已经为标准应用程序设计了一些实例类型，而为 CPU 密集型和内存密集型的应用程序等设计了其他实例类型。
VPC	虚拟私有云 由共享公共安全和互连的基础架构、平台和应用程序服务填充的弹性网络。

©2024 Palo Alto Networks, Inc.

术语	说明
IGW	Amazon 提供的 Internet 网关。 用于将网络连接到 Internet。您可以将 VPC 以外的 IP 地址的流量路由到 Internet 网关。
IAM 角色	标识和访问管理 在 AWS 上实现高可用性 VM 系列防火墙的必备要求。IAM 角色定义了在承担该角色后应用程序可使用的 API 操作和资源。在故障转移的情况下，IAM 角色可使 VM 系列防火墙安全地发出 API 请求，以将数据面板接口从主动对等切换至被动对等。 IAM 角色也是实施 VM 监控所必须的。请参阅在 AWS VPC 上监控的属性列表。
子网	可以将 VPC 的 IP 地址范围的分段附加到 EC2 实例。您可以根据安全和操作需求将 EC2 实例分组到子网。 您可以使用两种类型的子网： • 私有子网：不能通过 Internet 访问此子网中的 EC2 实例。 • 公共子网：可以将 Internet 网关附加到公共子网，且可以通过 Internet 访问此子网中的 EC2 实例。
安全组	可以将安全组附加到 ENI，且它用于指定允许在接口上建立入站/出站连接的协议、端口和 IP 地址范围的列表。 在 *AWS VPC* 中，安全组和网络 *ACL* 用于控制入站和出站流量；安全组规定了对于 *EC2* 实例的访问，而网络 *ACL* 规定了对于子网的访问。由于您是部署 *VM* 系列防火墙，因此需要在安全组中设置更宽松的规则，并允许防火墙在 *VPC* 中安全启用应用程序。
路由表	一组路由规则，用于控制离开与路由表相关联的任何子网的流量。只能将子网与一个路由表相关联。
密钥对	一组安全凭据，用来以电子方式证明您的身份。密钥对包含一个私钥和一个公钥。在启动 VM 系列防火墙时，您必须为 VM 系列防火墙生成密钥对或选择现有的密钥对。在维护模式下访问防火墙需要使用私钥。
CloudWatch	Amazon CloudWatch 是一项监控服务，可让您收集和跟踪 AWS 上 VM 系列防火墙的指标。启用后，防火墙会使用 AWS API 将本机 PAN-OS 指标发布到 CloudWatch。

©2024 Palo Alto Networks, Inc.

管理接口映射以用于 Amazon ELB

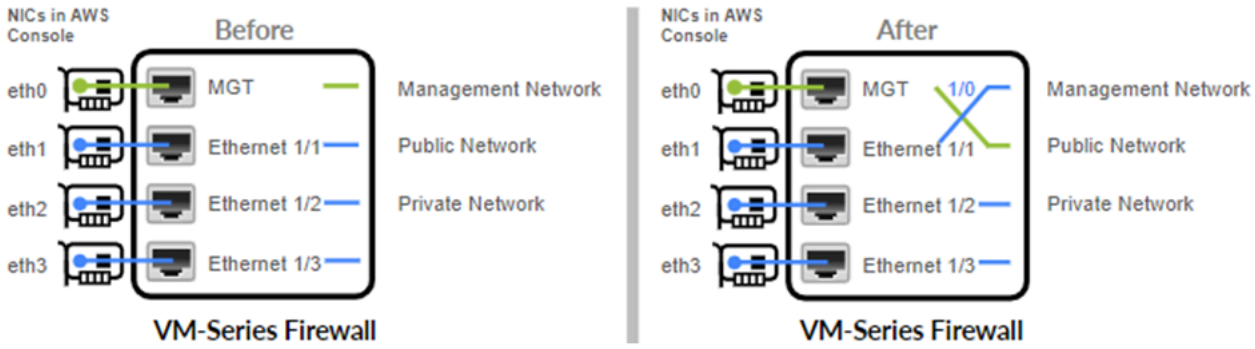
默认情况下，弹性网络接口 (ENI) eth0 会映射到防火墙上的 MGT 接口，而 ENI eth1 则会映射到防火墙上的 ethernet 1/1。由于 ELB 只能将流量发送到下一个跃点负载均衡 EC2 实例的主接口，所以 VM 系列防火墙必须能够使用数据面板流量的主接口。

在以下场景中，VM 系列防火墙位于 Amazon ELB 服务的下游，可以接收主接口上的数据面板流量（如需了解拓扑图，请参阅 使用 Amazon ELB 服务自动扩展 VM 系列防火墙）：

- VM 系列防火墙正在保护直接出站到 Internet 的流量，且无需使用返回到企业网络的 VPN 链接或 Direct Connect 链接。
- 当每个防火墙有且仅有一个后端服务器（如 Web 服务器等）时，VM 系列防火墙保护面向 Internet 的应用程序。VM 系列防火墙和 Web 服务器能够以成对方式在 ELB 下游进行线性扩展。

目前，对于需要 *ELB* 夹层式部署以向外扩展防火墙及应用程序层 *EC2* 实例的用例，交换管理接口将无法让用户以无缝方式部署 *ELB* 解决方案。交换管理接口仅可部分解决与 *ELB* 集成的问题。

要使防火墙能够收发 eth0 而非 eth1 上的数据面板流量，则必须交换防火墙内 ENI 的映射，以使 ENI eth0 映射到 ethernet 1/1，而 ENI eth1 则映射到防火墙上的 MGT 接口，具体如下所示。



如果可能，配置防火墙或定义策略规则之前，交换管理接口。

交换映射到上述接口的方式可使 ELB 将流量分配并路由到 VM 系列防火墙的正常实例，这些防火墙位于 AWS 上相同或不同的可用性区域，以便提升系统容量和容错性。

仅当 VM 系列防火墙部署在 Amazon ELB 服务后时，才需要进行接口交换。如果您的要求是在传统的高可用性设置中部署 VM 系列防火墙，则无需配置本节描述的接口交换。继续阅读AWS 上 VM 系列防火墙的高可用性。

要交换接口，以下选项可供选择：

- 启动时 — 启动防火墙时，可输入 AWS 管理控制台上的 **User data**（用户数据） 字段或 CLI 中输入 **`mgmt-interface-swap=enable`** 命令（请参阅在 AWS 上启动 VM 系列防火墙），或者在自举配置中加入新的 **`mgmt-interface-swap`** 操作命令。

©2024 Palo Alto Networks, Inc.

- 启动后 — 启动防火墙后，在防火墙上使用 VM 系列防火墙 CLI 交换管理界面（**set system setting mgmt-interface-swap enable yes** 操作命令）。

  - 为了防止在防火墙上出现不可预测的行为，选择一种能够持续指定接口交换设置的方法，可利用引导配置中防火墙上的 *CLI*，或使用 *AWS* 控制台上的 *Amazon EC2* ***User data***（用户数据）字段。
  - 确保您拥有 *AWS* 控制台（管理控制台或 *CLI*）的访问权限，以便查看 *eth1* 接口的 *IP* 地址。同时也要验证 *AWS* 安全组规则是否允许与新管理接口建立连接（*HTTPS* 或 *SSH*）。
  - 如果您已在交换接口前配置防火墙或定义策略规则，请检查 *eth0* 或 *eth1* 的任何 *IP* 地址变更是否会对策略规则造成影响。

在 AWS 上调整 VM 系列防火墙性能

以下配置会影响性能：

- PAN-OS 版本 9.0.3 及更低版本支持 AWS C5 和 M5 实例类型，这些实例类型默认具有对 SR-IOV 模式的弹性网络适配器支持。有关更多详细信息，请参阅弹性网络适配器 – Amazon EC2 的高性能网络接口。
- 默认情况下，PAN-OS 版本 9.0.4 及更高版本可为 C5 和 M5 实例类型提供 DPDK 支持。当防火墙处于 DPDK 模式时，将使用 DPDK 驱动程序。有关支持的驱动程序列表，请参阅 VM 系列防火墙上的 PacketMMAP 和 PDK 驱动程序以及官方 DPDK 发行说明。
- 要从 IETF RFC 8926 (Geneve) 封装和提高的吞吐量中受益，请升级到 PAN-OS 10.0.2 或更高版本，并参阅 VM 系列与 AWS 网关负载均衡器集成。

使用 VM 系列 CLI 查看您的 DPDK 设置或启用打包的 I/O。

查看防火墙上的 DPDK 配置

STEP 1 | 登录 VM 系列防火墙 CLI。

STEP 2 | 查看您的 DPDK 配置。如果启用 DPDK，则输出如下：

```
> show system setting dpdk-pkt-io on
```

```
Device current Packet IO mode:DPDK Device DPDK Packet IO capable:
 yes Device default Packet IO mode:DPDK
```

启用 DPDK 打包的 I/O

STEP 1 | 登录 VM 系列防火墙 CLI

STEP 2 | 启用 DPDK：

```
> set system setting dpdk-pkt-io on
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 重新启动设备。

在防火墙上，选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），然后选择 **Reboot Device**（重新启动设备）。

©2024 Palo Alto Networks, Inc.

AWS 上支持的部署

VM 系列防火墙可保护流向和来自 AWS 虚拟私有云 (VPC) 内 EC2 实例的入站和出站流量。由于 AWS VPC 仅支持 IP 网络（第 3 层网络功能），因此只能使用第 3 层接口部署 VM 系列防火墙。

- 部署 VM 系列防火墙可以保护在 AWS 虚拟私有云中托管的 EC2 实例。

  如果您在 AWS 云中托管应用程序，可以为通过 Internet 访问这些应用程序的用户部署 VM 系列防火墙保护和安全启用应用程序。例如，下图显示了在 Internet 网关连接到的边缘子网中部署的 VM 系列防火墙。在私有子网中部署的应用程序不能直接访问 Internet。

  当用户需要访问私有子网中的应用程序时，在验证安全策略和确认目标 NAT 后，防火墙接收请求并将其引导至相应的应用程序。在返回路径上，防火墙接收流量、应用安全策略并使用源 NAT 将内容传送给用户。请参阅用例：保护 AWS 云中的 EC2 实例。

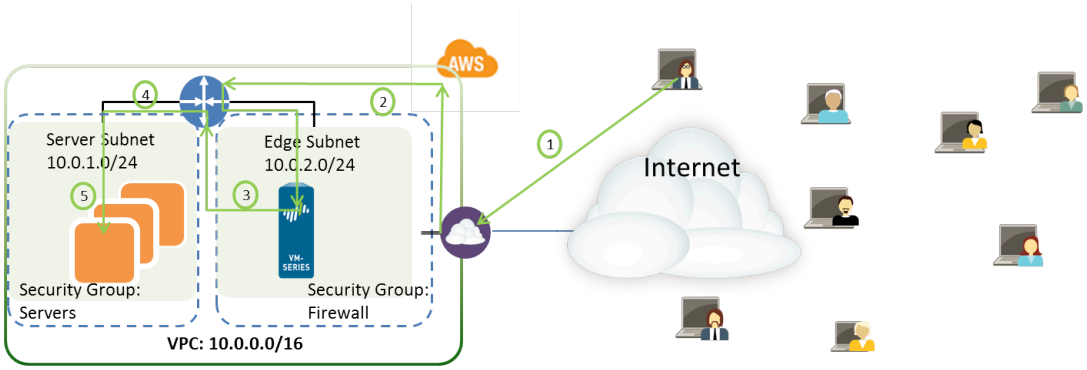


图 **1:** 用于 **EC2** 实例的 **VM** 系列

- 部署 VM 系列防火墙便于访问企业网络和 AWS 虚拟私有云中 EC2 实例之间的 VPN。

  要使用在 AWS 云中部署的应用程序连接企业网络，可以配置防火墙作为 IPSec VPN 隧道的终止点。该 VPN 隧道可以让网络上的用户安全访问云中的应用程序。

  对于集中管理，须在整个网络中一致执行策略；对于集中日志记录和报告，您也可以在企业网络中部署 Panorama。如果您需要设置对于多个 VPC 的 VPN 访问，使用 Panorama 可让您按区域对防火墙进行分组并进行轻松管理。

©2024 Palo Alto Networks, Inc.

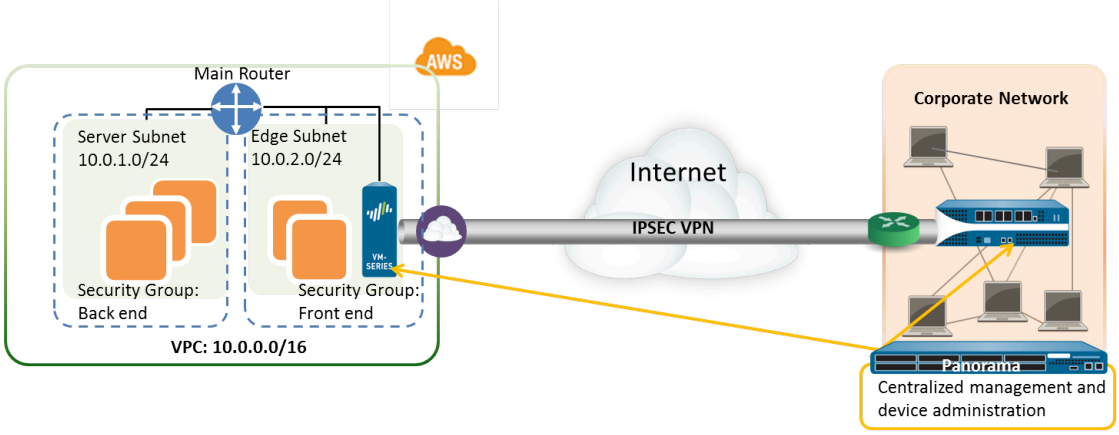


图 **2:** 用于 **VPN** 访问的 **VM** 系列

- 部署 VM 系列防火墙作为 GlobalProtect 网关保护使用笔记本电脑的远程用户进行访问。可以将笔记本电脑上的 GlobalProtect 代理连接到网关，并且网关可根据请求建立与企业网络的 VPN 连接或将请求路由到 Internet。要在移动设备（使用 GlobalProtect 应用）上为用户执行安全合规性，必须结合使用 GlobalProtect 网关和 GlobalProtect Mobile Security Manager。GlobalProtect Mobile Security Manager 可确保通过使用与企业应用程序和网络结合使用的设备设置和帐户信息管理和配置移动设备。

  针对上述各用例，您均可采用主动/被动高可用性 *(HA)* 对的方式部署 *VM* 系列防火墙。有关以 *HA* 方式设置 *VM* 系列防火墙的相关信息，请参阅 用例：使用动态地址组保护 VPC 中的新 EC2 实例。

- 利用 Amazon 弹性负载均衡 (ELB) 服务部署 VM 系列防火墙，以便防火墙能够在以下场景中（VM 系列防火墙位于 Amazon ELB 下游）接收主接口上的数据面板流量：
  - VM 系列防火墙正在保护直接出站到 Internet 的流量，且无需使用返回到企业网络的 VPN 链接或 Direct Connect 链接。
  - 当每个防火墙有且仅有一个后端服务器（如 Web 服务器等）时，VM 系列防火墙保护面向 Internet 的应用程序。VM 系列防火墙和 Web 服务器能够以成对方式在 ELB 下游进行线性扩展。

  如果您想 使用 Amazon ELB 服务自动扩展 VM 系列防火墙，请使用 GitHub 存储库中提供的 CloudFormation 模板将 ELS 三明治拓扑结构中的 VM 系列部署到面向 Internet 的传统 ELB 以及内部经典负载均衡器或内部应用程序负载均衡器（内部 ELB）。

©2024 Palo Alto Networks, Inc.

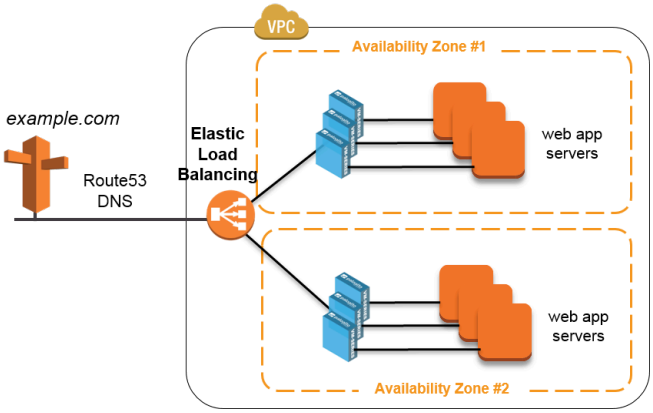


图 **3: VM** 系列与 **ELB**

如果防火墙位于 *ELB* 前方，则无法配置防火墙以收发 *eth0* 上的数据面板流量。*VM* 系列防火墙必须置于 *Amazon ELB* 的下游。

您也可以 使用 VM 系列防火墙CLI交换管理界面 或者在启动时启用它。有关详细信息，请参阅管理接口映射以用于 Amazon ELB。

如果您想部署负载均衡器三明治拓扑结构，请参阅 使用 Amazon ELB 服务自动扩展 VM 系列防火墙。

除 *Palo Alto Networks* 官方支持政策覆盖的上述链接外，*Palo Alto Networks* 还在 Palo Alto Networks GitHub 存储库中提供社区支持模板，从而搜索可用解决方案以快速启动 *AWS* 上的云自动化和扩展。有关可让您保护 *VPC* 之间，*VPC* 与本地/混合云资源之间的流量，以及保护到 *Internet* 的出站流量的集线器和订阅 *VPC* 部署，请参阅 AWS Transit VPC。

©2024 Palo Alto Networks, Inc.

在 AWS 上部署 VM 系列防火墙

- 获取 AMI
- AWS VPC 中 VM 系列防火墙的规划工作表
- 在 AWS 上启动 VM 系列防火墙
- 在 AWS Outpost 上启动 VM 系列防火墙
- 创建自定义 Amazon 机器映像 (AMI)
- 在 AWS上 加密 VM 系列防火墙的 EBS 卷
- 使用 VM 系列防火墙 CLI 以交换管理接口
- 在 VM 系列防火墙上启用 CloudWatch 监控

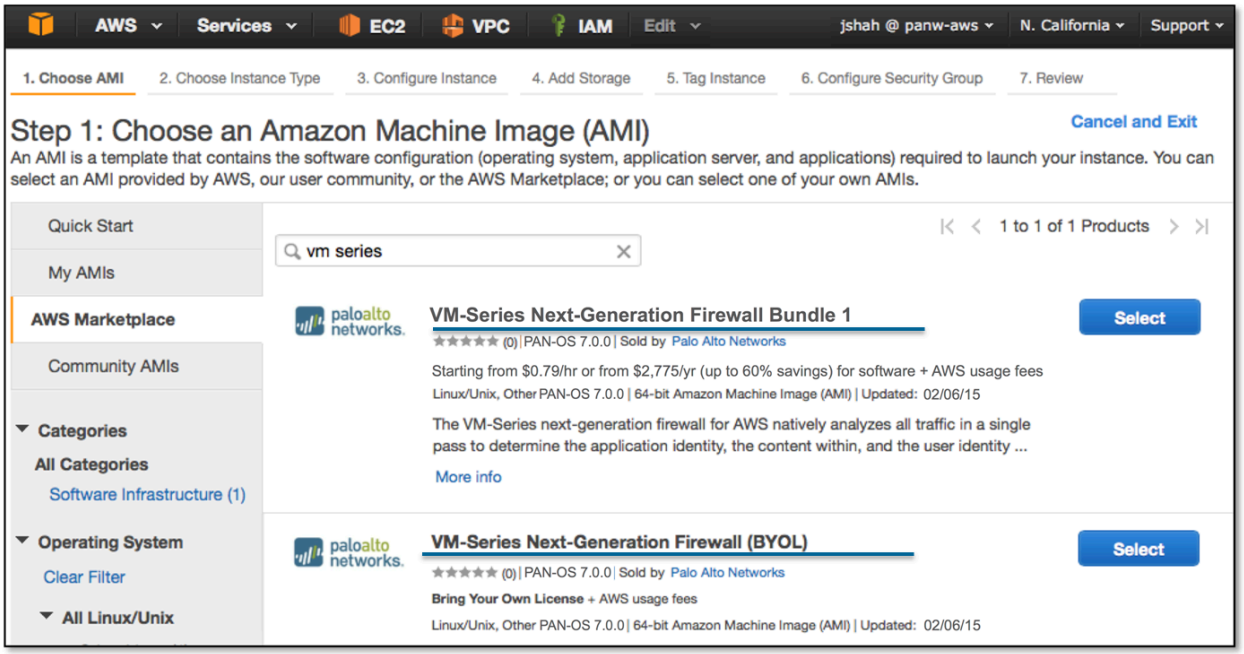
获取 AMI

从相应的 Marketplace 获取 AWS 公共云和 AWS GovCloud 的 Amazon 机器映像。

- AWS 公共云中的 AMI
- AWS GovCloud 上的 AMI
- 获取 VM 系列防火墙 Amazon 机器映像 (AMI) ID

AWS 公共云中的 AMI

对于自带许可 (BYOL) 和基于使用的价格选项，VM 系列防火墙的 AMI 在 AWS Marketplace 中均有提供。



©2024 Palo Alto Networks, Inc.

如需购买含 BYOL 选项的许可证，请联系 Palo Alto Networks 销售工程师或分销商。

AWS GovCloud 上的 AMI

AWS GovCloud Marketplace 上提供 VM 系列防火墙自带许可证 (BYOL) 模式和基于使用的模式。

您可以通过 GovCloud 帐户搜索 Palo Alto Networks，查找 Marketplace 上 VM 系列防火墙的 AMI。启动防火墙之前，务必查看受支持的 EC2 实例类型。有关详细信息，请参阅在 AWS上 启动 VM 系列防火墙。

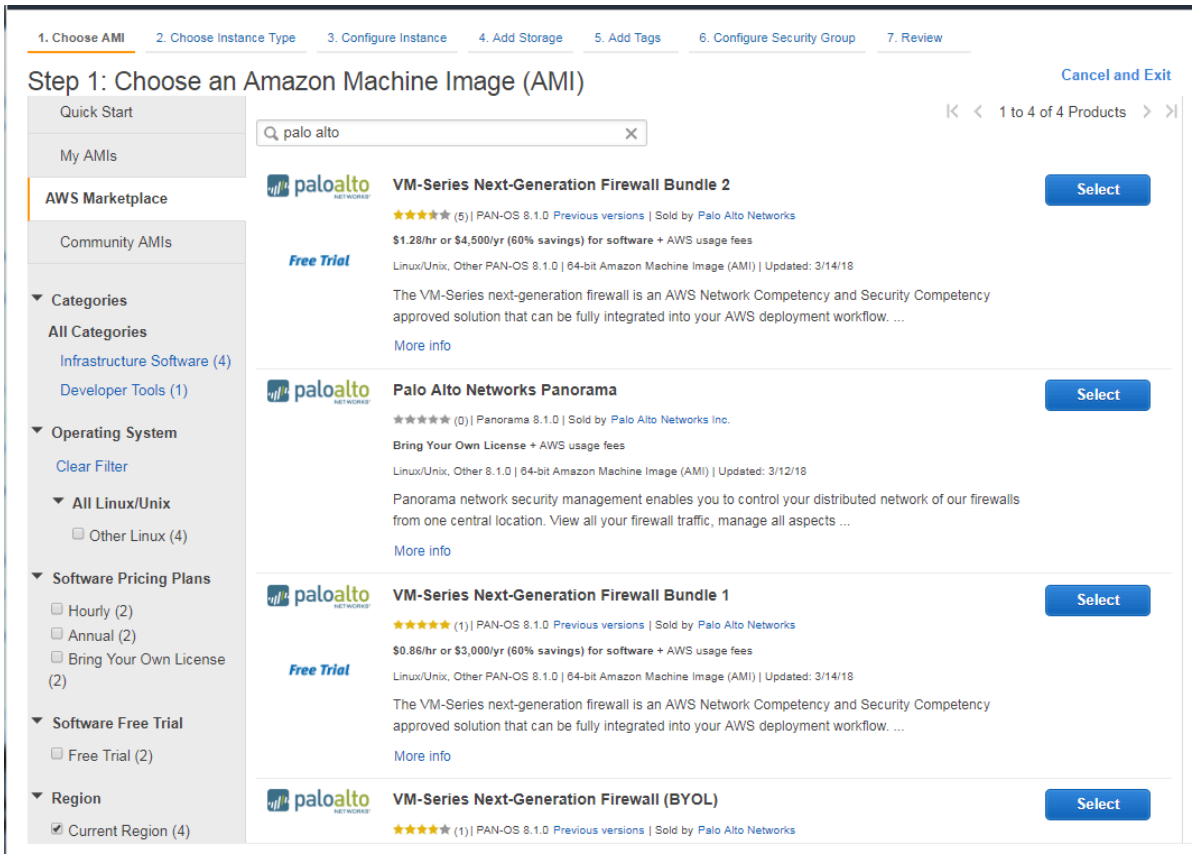


表 **1:** 查看 **AWS** 上 **VM** 系列防火墙的系统要求和限制

要求	详细信息
EC2 实例类型	您选择的EC2实例类型必须符合 VM 系列系统要求 对于 VM 系列防火墙型号。如果在不符合这些要求的 EC2 实例类型上部署 VM 系列防火墙，防火墙将会在启动时进入维护模式。 为支持 *AWS* 的 *VM* 监控和高可用性，*VM* 系列防火墙必须能够在防火墙管理接口与 *AWS API* 端点（如 *ec2.us-west-2.amazonaws.com*）之间无任何代理服务器的情况下，直接访问 *AWS API* 服务端点。

©2024 Palo Alto Networks, Inc.

要求	详细信息
Amazon 弹性块存储 (EBS)	VM 系列防火墙必须使用 Amazon 弹性块存储 (EBS) 卷进行存储。EBS 优化可以为 Amazon EBS I/O 提供优化的配置堆栈和其他专用容量。
网络	由于 AWS 仅支持第 3 层网络功能，因此只能使用第 3 层接口部署 VM 系列防火墙。在 AWS VPC 中部署的 VM 系列防火墙不支持第 2 层接口、Virtual Wire、VLAN 和子接口。
接口	最多可以为数据流量支持八个接口 — 一个管理接口和最多七个弹性网络接口 (ENI)。VM 系列防火墙不支持 ENI 的热附件；要检测添加或移除 ENI，您必须重新启动防火墙。 您选择的 *EC2* 实例类型确定了可以启用的 *ENI* 的总数。例如，*c3.8xlarge* 可支持八 *(8)* 个 *ENI*。
支持授权和许可证	对于自带许可证模型，需要支持帐户和有效的 VM 系列许可证才能获取在 AWS VPC 中安装 VM 系列防火墙所需的 Amazon 机器映像 (AMI) 文件。必须从 Palo Alto Networks 购买 VM 系列防火墙所需的许可证，如容量许可证、支持许可证和威胁防御订阅、URL 筛选和 WildFire 等。要购买部署所需的许可证，请联系您的销售代表。请参阅面向公共云的 VM 系列防火墙许可证。 对于基于使用的许可证模型，按小时和按年度的定价捆绑可直接通过 AWS 进行购买和付费。但您必须使用 Palo Alto Networks 来注册您的支持授权。有关详细信息，请参阅面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。

获取 VM 系列防火墙 Amazon 机器映像 (AMI) ID

使用以下说明找到与您想要启动 VM 系列防火墙的 PAN-OS 版本、许可证类型和 AWS 区域匹配的 VM 系列防火墙的 AMI ID。

STEP 1 | 在用于检索 AMI ID 的客户端上安装 AWS CLI，并使用您的 AWS 凭据登录。

有关安装 CLI 的说明，请参阅 AWS 文档。

©2024 Palo Alto Networks, Inc.

STEP 2 | 使用以下 CLI 命令查找 AMI-ID。

```
aws ec2 describe-images --filters "Name=product-
code,Values=<license-type-value>" Name=name,Values=PA-VM-AWS*<PAN-
OS-version>*  --region <region> --output json
```

您需要使用如下所示的相关信息替换尖括号 <> 中的值：

- 对每种许可证类型使用 VM 系列产品代码。值为：
  - Bundle 1—

    ```
    e9yfvyj3uag5uo5j2hjikv74n
    ```

  - Bundle 2—

    ```
    hd44w1chf26uv4p52cdynb2o
    ```

  - BYOL—

    ```
    6njl1pau431dv1qxipg63mvah
    ```

- 使用 PAN-OS 版本 — 10.0。如果 PAN-OS 版本中有多个功能版本，则会列出所有 AMI-ID。例如，在 9.0.x 中，您可以查看 PAN-OS 版本 9.0、9.0.3.xfr、9.0.5.xfr 和 9.0.6 的 AMI ID 列表，也可以使用所需的 PAN-OS 版本的 AMI-ID。
- 获取 AWS 区域详细信息：https://docs.aws.amazon.com/general/latest/gr/rande.html。

例如：要查找在美国加利福尼亚地区适用于 PAN-OS 10.0.0 VM 系列套餐 1 的 AMI ID，CLI 命令为：

```
 aws ec2 describe-images --filters "Name=product-
code,Values=e9yfvyj3uag5uo5j2hjikv74n" "Name=name,Values=PA-VM-
AWS*10.0*"  --region us-west-1 --output json
```

输出为：

```
 { "ProductCodes": [ { "ProductCodeId":
 "e9yfvyj3uag5uo5j2hjikv74n", "ProductCodeType":
 "marketplace" } ], "VirtualizationType": "hvm",
 "Hypervisor": "xen", "ImageOwnerAlias": "aws-marketplace",
 "EnaSupport": true, "SriovNetSupport": "simple",
 "ImageId": "ami-06f7a63d7481d0ded", "State": "available",
 "BlockDeviceMappings": [ { "DeviceName": "/dev/xvda", "Ebs":
 { "SnapshotId": "snap-0009036179b39824b", "DeleteOnTermination":
 false, "VolumeType": "gp2", "VolumeSize":60, "Encrypted":
 false } } ], "Architecture": "x86_64", "ImageLocation":
 "aws-marketplace/PA-VM-AWS-10.0.0-f1260463-68e1-4bfb-
bf2e-075c2664c1d7-ami-06f7a63d7481d0ded.1", "RootDeviceType":
 "ebs", "OwnerId":"679593333241", "RootDeviceName": "/dev/
xvda", "CreationDate":"2020-07-20T12:45:22.000Z", "Public":
```


©2024 Palo Alto Networks, Inc.

```
 true, "ImageType": "machine", "Name":"PA-VM-AWS-10.0.0-
f1260463-68e1-4bfb-bf2e-075c2664c1d7-ami-06f7a63d7481d0ded.1" }
```

您也可以输出为表格格式。例如，要查看 PAN-OS 10.0.2 的 AMI for BYOL 映像：

```
aws ec2 describe-images --filters "Name=product-
code,Values=6njl1pau431dv1qxipg63mvah" "Name=name,Values=PA-VM-
AWS*10.0.2*" --region us-west-1 --output table --query "Images[*].
{Name:Name,AMI:ImageId,State:State}"
```

```
-----------------------------------------------------------------------------
 DescribeImages |+----------------------
+-----------------------------------------------------------------------------
+-------------+| AMI | Name | State |+----------------------
+-----------------------------------------------------------------------------
+-------------+| ami-037b90bd9b630f594| PA-VM-
AWS-10.0.2-7064e142-2859-40a4-ab62-8b0996b842e9-
ami-07a0e94019f2a2001.4 | available |+----------------------
+-----------------------------------------------------------------------------
+-------------+
```

AWS VPC 中 VM 系列防火墙的规划工作表

为了便于部署，应计划 VPC 内的子网和要在每个子网内部署的 EC2 实例。在开始部署之前，使用下表核对在 VPC 中将 VM 系列防火墙部署和插入流量所需的网络信息：

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

配置项	值
VPC CIDR	
安全组	
子网（公共）CIDR	
子网（专用）CIDR	
子网（公共）路由表	
子网（专用）路由表	
安全组 • 访问防火墙的管理规则 (eth0/0) • 访问防火墙的数据面板接口规则	

©2024 Palo Alto Networks, Inc.

配置项	值
• 访问分配给应用服务器的接口规则。	
ELB 下游的 VM 系列防火墙	
EC2 实例 1（VM 系列防火墙） 附加到公共子网的数据面板接口唯一需要的 *EIP*。	子网： 实例类型： 管理接口 IP： 管理接口 EIP： 数据面板接口 eth1/1 • 专用 IP： • EIP（如果需要）： • 安全组： 数据面板接口 eth1/2 • 专用 IP： • EIP（如果需要）： • 安全组：
EC2 实例 2（要保护的应用程序） 对于要部署的其他应用程序重复这些值集合。	子网： 实例类型： 管理接口 IP： 默认网关： 数据面板接口 1 • 专用 IP：
HA 的必要条件	如果在高可用性（主动/被动）配置中部署 VM 系列防火墙，则必须确保满足以下条件： • 部署实例时创建 IAM 角色并将该角色分配给 VM 系列防火墙。请参阅 HA 的 IAM 角色。 • 在相同的 AWS 可用性区域中部署 HA 对等。 • HA 对等中的主动防火墙必须至少有 3 个 ENI：两个数据面板接口和一个管理接口。

©2024 Palo Alto Networks, Inc.

配置项	值
	HA 对中的被动防火墙必须有一个用于管理的 ENI，一个发挥数据面板接口功能的 ENI，同时需要将数据面板接口配置为 HA2 接口。 切勿附加其他数据面板接口至 *HA* 对中的被动防火墙。在故障转移的情况下，数据面板接口将以先分离后附加的方式，从之前的主动防火墙移动至当前的主动防火墙（之前为被动）。

在 AWS 上启动 VM 系列防火墙

如果您还没有向您的支持帐户注册已在订单履行电子邮件中收到的功能验证代码，请参阅注册 VM 系列防火墙。注册后，可以使用 Marketplace 中发布的 AMI 部署 VM 系列防火墙或在 WS VPC 中创建自定义 Amazon 机器映像 (AMI)，如下所述：

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 访问 AWS 控制台。

登录到 AWS 控制台，然后选择 EC2 仪表盘。

©2024 Palo Alto Networks, Inc.

STEP 2 | 设置网络需要的 VPC。

无论是在现有 VPC 中启动 VM 系列防火墙还是创建新的 VPC，VM 系列防火墙必须能够接收来自 EC2 实例的流量，并在 VPC 和 Internet 之间执行入站和出站通信。

有关创建 VPC 和设置进行访问的说明，请参阅 AWS VPC 文档。

如需包含完整工作流程的示例，请参阅用例：保护 AWS 云中的 EC2 实例。

1. 创建新的 VPC 或使用现有的 VPC。请参阅《AWS 入门指南》文档。
2. 验证是否已适当定义网络和安全组件。
   - 启用与 Internet 的通信。默认 VPC 包括 Internet 网关，如果在默认子网中安装 VM 系列防火墙，则该防火墙必须能够访问 Internet。
   - 创建子网。子网是分配给可以在其中启动 EC2 实例的 VPC 的 IP 地址范围的分段。VM 系列防火墙必须属于公共子网，这样可以配置它以访问 Internet。
   - 根据需要创建安全组管理来自 EC2 实例/子网的入站和出站流量。
   - 将路由添加到专用子网的路由表，以确保可以通过 VPC 中的子网和安全组路由流量（如适用）。
3. 如果希望在 HA 中部署两个 VM 系列防火墙，则必须先定义 HA 的 IAM 角色，然后才能在 AWS 上配置主动/被动 HA。
4. （可选）如果您正在使用引导来执行 VM 系列防火墙的配置，请参阅在 AWS 中引导 VM 系列防火墙。有关引导的更多信息，请参阅引导 VM 系列防火墙和选择引导方法。

©2024 Palo Alto Networks, Inc.

STEP 3 | 启动 VM 系列防火墙。

尽管您可在启动时添加其他网络接口 *(ENI)* 至 *VM* 系列防火墙，但 *AWS* 仍会在您重启防火墙时针对管理接口发布自动分配的公共 *IP* 地址。因此，为确保与管理接口之间的连接性，您必须先为其分配一个弹性 *IP* 地址，之后再向防火墙附加其他接口。

如果您希望保存 EIP 地址，则可分配一个 EIP 地址至 eth 1/1 接口，然后将此接口作为管理流量和数据流量的共用接口。如需限制在 eth 1/1 接口上允许执行的服务或可登陆至此接口的 IP 地址，请附加管理配置文件至此接口。

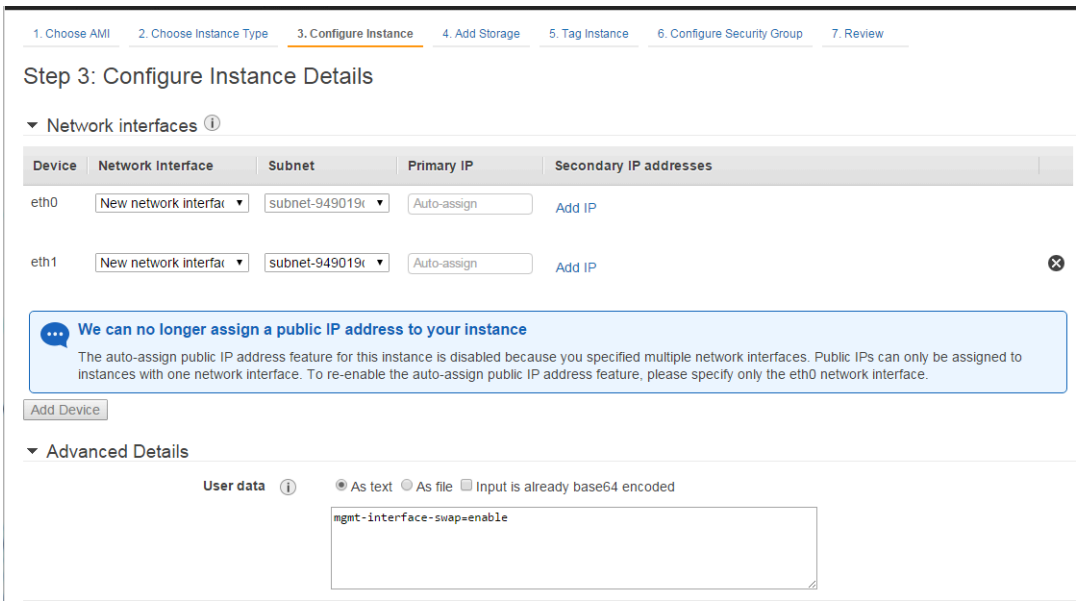
1. 在 EC2 仪表盘上，单击 **Launch Instance**（启动实例）。
2. 选择 VM 系列 AMI。要获得 AMI，请参阅获得 AMI。
3. 在 EC2 实例上启动 VM 系列防火墙。
   1. 对于防火墙所需的资源分配，请选择 **EC2 instance type**（**EC2** 实例类型），然后单击 **Next**（下一步）。请参阅 VM 系列系统要求，以满足资源需求。
   2. 选择 VPC。
   3. 选择将要附加 VM 系列管理接口的公共子网。
   4. 选择**Automatically assign a public IP address**（自动分配公共 **IP** 地址）。这可让您获取 VM 系列防火墙管理接口的可公共访问 IP 地址。

      稍后，您可以将弹性 IP 地址附加到管理接口；与在终止实例时与防火墙解除相关联的公共 IP 地址不同，弹性 IP 地址可提供持久性且可以重新附加到 VM 系列防火墙的新的（或更换）实例，而不需要重新配置 IP 地址，无论您可能在何处引用。
   5. 选择 **Launch as an EBS-optimized instance**（启动作为 **EBS** 优化实例）。
   6. 使用 ELB 为部署添加另一个网络接口，以便交换防火墙上的管理和数据接口。交换接口至少需要两个 ENI（eth0 和 eth1）。
      - 展开 Network Interfaces（网络接口）部分，然后单击 **Add Device**（添加设备）以添加其他网络接口。

        确保 VPC 具备一个以上的子网，以便在启动时可添加其他 ENI。

        如果仅使用一个 *ENI* 启动防火墙：
        - 接口交换命令将使防火墙启动进入维护模式。
        - 添加第二个 *ENI* 时，必须重新启动防火墙。
      - 展开 Advanced Details（高级详细信息）部分，然后在 **User data**（用户数据）字段中输入 **`mgmt-interface-swap=enable`** 作为启动期间执行接口交换的文本。

©2024 Palo Alto Networks, Inc.



Bootstrap Package（引导数据包）— 如果使用引导数据包引导防火墙，还可以在 **mgmt-interface-swap=enable** 后面输入分号分隔符，然后输入 **vmseries-bootstrap-aws-s3bucket=<bucketname>**。

User Data（用户数据）— 如果使用用户数据引导防火墙，可以在 **mgmt-interface-swap=enable** 后面输入分号分隔符，然后根据输入基本配置作为用户数据（公共云）输入其他键值对。

AWS Secret（**AWS** 机密）— 如果使用 AWS 密钥引导防火墙，可以在 **mgmt-interface-swap=enable** 后面输入分号分隔符，然后输入密钥名称作为键值对，如在 AWS 上引导 VM 系列防火墙中的步骤 3 所述。例如：

7. 接受默认 **Storage**（存储）设置。该防火墙使用卷类型 SSD (gp2)。

   第一次访问防火墙需要使用此密钥对。同样，在维护模式下访问防火墙也需要使用此密钥对。

8. （可选）**Tagging**（标记）。添加一个或多个标记来创建您自己的元数据，用以识别 VM 系列防火墙并对其进行分组。例如，添加带 **Value**（值）的 **Name**（名称）标记可帮助您记忆已交换到此 VM 系列防火墙的 ENI 接口。
9. 选择现有 **Security Group**（安全组）或创建新安全组。此安全组用于限制访问防火墙的管理接口。至少考虑对管理接口启用 HTTPS 和 SSH 访问权限。
10. 如果出现提示，选择设置的相应 **SSD** 选项。
11. 选择 **Review and Launch**（查看并启动）。查看您的选择是否正确，然后单击 **Launch**（启动）。
12. 选择现有的密钥对或创建新的密钥对，并确认密钥免责声明。
13. 下载并将私钥保存到安全位置；文件扩展名为 `.pem`。如果丢失，则将无法重新生成此密钥。

©2024 Palo Alto Networks, Inc.

启动 VM 系列防火墙需要 5 至 7 分钟。您可以在 EC2 仪表盘上查看进程。进程完成后，VM 系列防火墙将会显示在 EC2 仪表盘的 **Instances**（实例）页面上。

STEP 4 | 配置防火墙的新管理密码。

在 *VM* 系列防火墙 *CLI* 上，您必须先配置唯一的管理密码，然后才能访问防火墙的 *Web* 界面。要登录到 *CLI*，您需要可用于启动防火墙的私钥。

1. 在 VM 系列防火墙的命令行界面 (CLI) 中使用 SSH 的公共 IP 地址。您将需要在3 中使用或创建的私钥才能访问 CLI。

   如果您已添加其他 *ENI* 支持使用 *ELB* 进行部署，则必须先为 *ENI* 创建和分配弹性 *IP* 地址才能访问 *CLI*，请参阅6。

   如果您正在使用 PuTTY 访问 SSH，则您必须将 .pem 格式转换为 .ppk 格式。参阅 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

2. 输入以下命令以登录到防火墙：

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*

3. 使用以下命令并按照屏幕上的提示配置新密码：

   配置

   set mgt-config users admin password

4. 如果存在需激活的 BYOL，请对 DNS 服务器的 IP 地址进行设置，以使防火墙可访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

   set deviceconfig system dns-setting servers primary *<ip_address>*

5. 使用以下命令提交您所做的更改：

   commit

6. 终止 SSH 会话。

STEP 5 | 关闭 VM 系列防火墙。

1. 在 EC2 仪表盘上，选择 **Instances**（实例）。
2. 从列表中选择 VM 系列防火墙，然后单击 **Actions**（操作）> **Stop**（停止）。

STEP 6 | 创建并分配弹性 IP 地址 (EIP) 至用于对防火墙进行管理访问的 ENI，然后重启 VM 系列防火墙。

1. 选择 **Elastic IPs**（弹性 **IP**），并单击 **Allocate New Address**（分配新地址）。
2. 选择 **EC2-VPC**，并单击 **Yes, Allocate**（是，分配）。
3. 选择新分配的 EIP，并单击 **Associate Address**（关联地址）。
4. 选择 **Network Interface**（网络接口）和与之相关联的 **Private IP address**（专用 **IP** 地址），然后单击 **Yes, Associate**（是，关联）。

©2024 Palo Alto Networks, Inc.

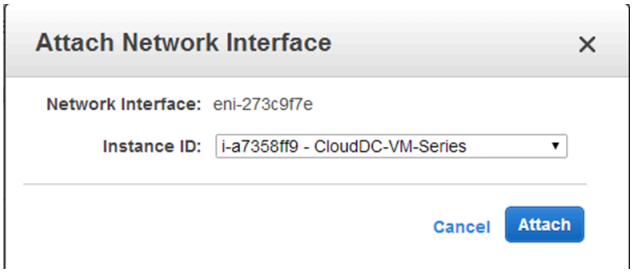
STEP 7 | 创建虚拟网络接口并将接口附加到 VM 系列防火墙。虚拟网络接口在 AWS 上称为弹性网络接口 (ENI)，并且在防火墙上可以用作数据面板网络接口。这些接口都用于处理流向/来自防火墙的数据流量。

您至少需要两个可使流量传入/出防火墙的 ENI。您最多可以添加七个 ENI 来处理 VM 系列防火墙的数据流量；检查 EC2 实例类型以确认它可以支持的最大接口数量。

1. 在 EC2 仪表盘上，选择 **Network Interfaces**（网络接口），然后单击 **Create Network Interface**（创建网络接口）。
2. 输入隧道的描述性名称。
3. 选择子网。使用子网 ID 以确保您已选择正确的子网。您只能将 ENI 附加到同一子网中的实例。
4. 输入要分配给接口的**Private IP**（专用 **IP**）地址或选择**Auto-assign**（自动分配）以自动分配选定子网中可用 IP 地址内的 IP 地址。
5. 选择 **Security group**（安全组）以控制访问数据面板网络接口。
6. 单击**Yes, Create**（是，创建）。



7. 要将 ENI 附加到 VM 系列防火墙，选择刚创建的接口，然后单击 **Attach**（附加）。



8. 选择 VM 系列防火墙的 **Instance ID**（实例 **ID**），然后单击 **Attach**（附加）。
9. 重复上述步骤可创建多个 ENI 并将其附加到防火墙。

STEP 8 | 在 VM 系列防火墙上激活许可证（基于使用的许可证模型无需进行此操作）。

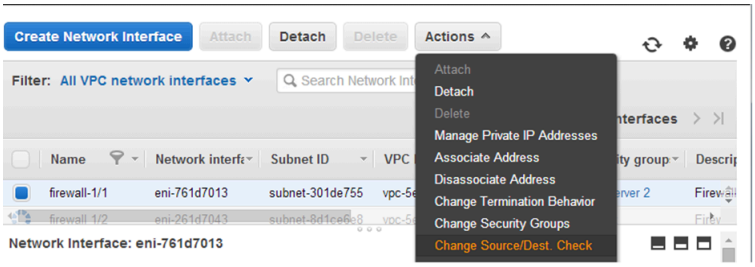
在 *AWS* 管理控制台上不执行此任务。激活许可证需要访问 *Palo Alto Networks* 支持门户和 *VM* 系列防火墙的 *Web* 界面。

请参阅激活许可证。

©2024 Palo Alto Networks, Inc.

STEP 9 | 在每个防火墙数据面板网络接口上禁用源/目标检查。禁用该选项可让接口处理不是以分配给网络接口的 IP 地址为目标的网络流量。

1. 在 EC2 仪表盘上，选择 **Network Interfaces**（网络接口）选项卡中的网络接口（如 eth1/1）。
2. 在 **Action**（操作）下拉列表中，选择 **Change Source/Dest.Check**（更改源/目标检查）。



3. 单击 **Disabled**（已禁用）并 **Save**（保存）您的更改。
4. 对每个防火墙数据面板接口重复步骤 1-3。

©2024 Palo Alto Networks, Inc.

STEP 10 | 配置数据面板网络接口作为防火墙上的第 3 层接口。

有关配置示例，请参阅步骤 14 到 17（在用例：保护 AWS 云中的 EC2 实例。

在 *VPC* 内的应用服务器上，定义防火墙的数据面板网络接口作为默认网关。

1. 在 Web 浏览器中使用安全连接 (https)，通过初始配置期间分配的 EIP 地址和密码登录 (https://<Elastic_IP address>)。您将看到证书警告；这属于正常情况。继续浏览网页。
2. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
3. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 VM_Series_untrust），然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **Static**（静态）或 **DHCP Client**（**DHCP** 客户端）。

     如果使用 **Static**（静态）选项，请单击 IP 部分中的 **Add**（添加），然后输入接口的 IP 地址和网络掩码，如 10.0.0.10/24。

     确保 IP 地址与之前分配的 ENI IP 地址相匹配。

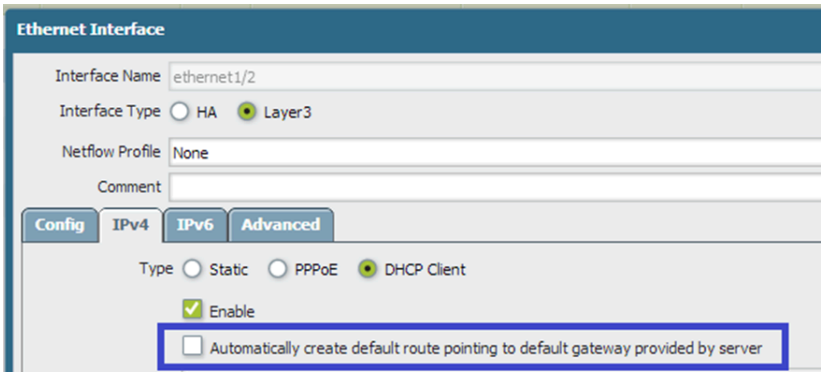
     如果使用 DHCP，选择 **DHCP Client**（**DHCP** 客户端）；将会自动获取在 AWS 管理控制台上分配给 ENI 的专用 IP 地址。
4. 单击 **ethernet 1/2** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 安全区域：VM_Series_trust
   - **IP Address**（**IP** 地址）：选择 **Static**（静态）或 **DHCP Client**（**DHCP** 客户端）单选按钮。

     对于静态，单击 IP 部分中的 **Add**（添加），然后输入接口的 IP 地址和网络掩码。确保 IP 地址与之前分配的附加 ENI IP 地址相匹配。
5. 单击 **Commit**（提交）。验证各接口的链接状态是否正常。



对于 *DHCP*，取消选中 ***Automatically create default route to default gateway provided by server***（自动创建指向服务器所提供的默认网关的默认路由）复选框。对于附加到 *VPC* 中私有子网的接口，禁用该选项可确保由此接口处理的流量不会直接流向 *VPC* 上的 *Internet* 网关。

©2024 Palo Alto Networks, Inc.



STEP 11 | 创建 NAT 规则以允许来自在 VPC 中部署的服务器的入站或出站流量。

1. 在防火墙的 Web 界面上选择 **Policies**（策略） > **NAT**。
2. 创建 NAT 规则以允许流量从防火墙的数据面板网络接口流向 VPC 的 Web 服务器接口。
3. 创建 NAT 规则以允许出站访问从 Web 服务器流向 Internet 的流量。

STEP 12 | 创建安全策略以允许/拒绝流向/来自在 VPC 中部署的服务器的流量。

1. 在防火墙的 Web 界面上选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），然后指定要执行限制的区域、应用程序和日志记录选项，并审核遍历网络的流量。

STEP 13 | 在防火墙上提交更改。

单击 **Commit**（提交）。

STEP 14 | 确认 VM 系列防火墙正在保护流量且 NAT 规则已生效。

1. 在防火墙的 Web 界面上选择 **Monitor**（监控） > **Logs**（日志） > **Traffic**（流量）。
2. 查看日志以确保应用程序遍历与实施的安全策略相匹配的网络。

在 AWS Outpost 上启动 VM 系列防火墙

完成此过程，在 AWS Ouptost 机架上部署 VM 系列防火墙。如果您还没有向您的支持帐户注册已在订单履行电子邮件中收到的功能验证代码，请参阅注册 VM 系列防火墙。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 访问 AWS Outpost 控制台。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 扩展 VPC 以包括 AWS Outpost 机架。

VM 系列防火墙必须能够接收来自 EC2 实例的流量，并在 VPC 和 Internet 之间执行入站和出站通信。

有关将 Outpost 连接到 VPC 的说明，请参阅 AWS Outpost 文档。

1. 验证是否已适当定义网络和安全组件。
   - 启用与 Internet 的通信。Outpost 需要本地网关才能连接到本地 LAN 和 Internet。
   - 创建 Outpost 子网。
   - 根据需要创建安全组管理来自 EC2 实例/子网的入站和出站流量。
   - 将路由添加到专用子网的路由表，以确保可以通过 VPC 中的子网和安全组路由流量（如适用）。
2. 如果希望在 HA 中部署两个 VM 系列防火墙，则必须先定义 HA 的 IAM 角色，然后才能配置 AWS 上 VM 系列防火墙的高可用性。
3. （可选）如果使用引导执行 VM 系列防火墙的配置，请参阅在 AWS 上引导 VM 系列防火墙。有关引导的更多信息，请参阅引导 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 3 | 启动 VM 系列防火墙。

尽管您可在启动时添加其他网络接口 *(ENI)* 至 *VM* 系列防火墙，但 *AWS* 仍会在您重启防火墙时针对管理接口发布自动分配的公共 *IP* 地址。因此，为确保与管理接口之间的连接性，您必须先为其分配一个弹性 *IP* 地址，之后再向防火墙附加其他接口。

如果您希望保存 EIP 地址，则可分配一个 EIP 地址至 eth 1/1 接口，然后将此接口作为管理流量和数据流量的共用接口。如需限制在 eth 1/1 接口上允许执行的服务或可登陆至此接口的 IP 地址，请附加管理配置文件至此接口。

1. 在 EC2 仪表盘上，单击 **Launch Instance**（启动实例）。
2. 选择 VM 系列 AMI。要获得 AMI，请参阅获得 AMI。
3. 在 EC2 实例上启动 VM 系列防火墙。
   1. 对于防火墙所需的资源分配，请选择 **EC2 instance type**（**EC2** 实例类型），然后单击 **Next**（下一步）。请参阅 VM 系列系统要求，以满足资源需求。
   2. 选择 VPC。
   3. 选择将要附加 VM 系列管理接口的 Outpost 上的公共子网。
   4. 选择**Automatically assign a public IP address**（自动分配公共 **IP** 地址）。这可让您获取 VM 系列防火墙管理接口的可公共访问 IP 地址。

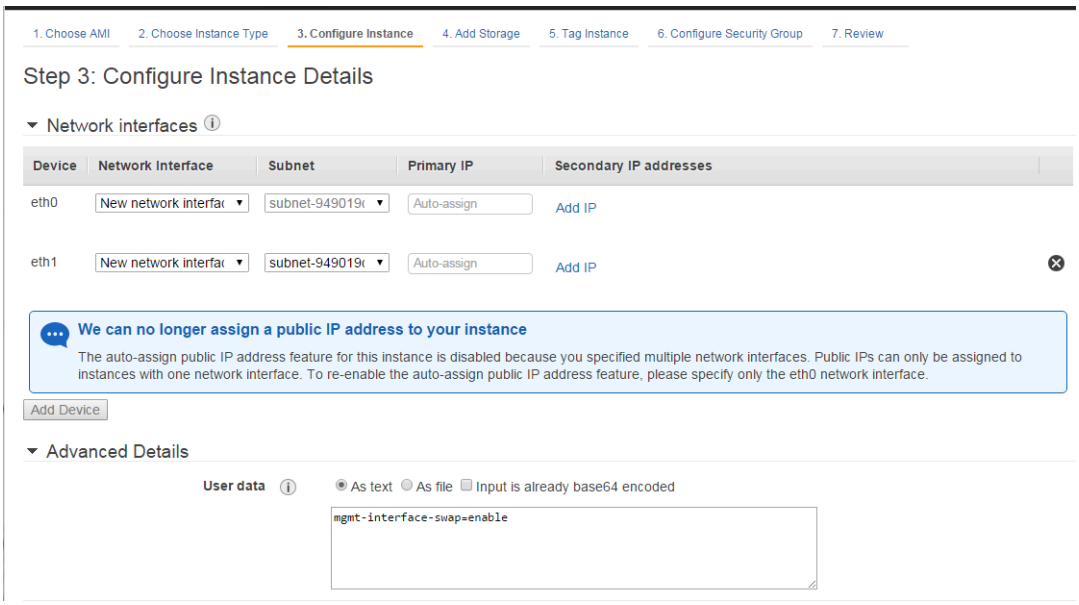
      稍后，您可以将弹性 IP 地址附加到管理接口；与在终止实例时与防火墙解除相关联的公共 IP 地址不同，弹性 IP 地址可提供持久性且可以重新附加到 VM 系列防火墙的新的（或更换）实例，而不需要重新配置 IP 地址，无论您可能在何处引用。
   5. 选择 **Launch as an EBS-optimized instance**（启动作为 **EBS** 优化实例）。
   6. 使用 ELB 为部署添加另一个网络接口，以便交换防火墙上的管理和数据接口。交换接口至少需要两个 ENI（eth0 和 eth1）。
      - 展开 Network Interfaces（网络接口）部分，然后单击 **Add Device**（添加设备）以添加其他网络接口。

        确保 VPC 具备一个以上的子网，以便在启动时可添加其他 ENI。

        如果仅使用一个 *ENI* 启动防火墙：
        - 接口交换命令将使防火墙启动进入维护模式。
        - 添加第二个 *ENI* 时，必须重新启动防火墙。
      - 展开高级详情部分，在用户数据字段中输入 **`mgmt-interface-swap=enable`**，以作为启动期间执行接口交换的文本。

        如果正在引导防火墙，也可以在 ***`mgmt-interface-swap=enable`*** 后输入一个逗号分隔符，然后输入 ***`vmseries-bootstrap-aws-s3bucket=<bucketname>`***。

©2024 Palo Alto Networks, Inc.



7. 接受默认 **Storage**（存储）设置。该防火墙使用卷类型 SSD (gp2)

   第一次访问防火墙需要使用此密钥对。同样，在维护模式下访问防火墙也需要使用此密钥对。

8. （可选）**Tagging**（标记）。添加一个或多个标记来创建您自己的元数据，用以识别 VM 系列防火墙并对其进行分组。例如，添加带 **Value**（值）的 **Name**（名称）标记可帮助您记忆已交换到此 VM 系列防火墙的 ENI 接口。
9. 选择现有 **Security Group**（安全组）或创建新安全组。此安全组用于限制访问防火墙的管理接口。至少考虑对管理接口启用 HTTPS 和 SSH 访问权限。
10. 如果出现提示，选择设置的相应 **SSD** 选项。
11. 选择 **Review and Launch**（查看并启动）。查看您的选择是否正确，然后单击 **Launch**（启动）。
12. 选择现有的密钥对或创建新的密钥对，并确认密钥免责声明。
13. 下载并将私钥保存到安全位置；文件扩展名为 `.pem`。如果丢失，则将无法重新生成此密钥。

    启动 VM 系列防火墙需要 5 至 7 分钟。您可以在 EC2 仪表盘上查看进程。进程完成后，VM 系列防火墙将会显示在 EC2 仪表盘的 **Instances**（实例）页面上。

©2024 Palo Alto Networks, Inc.

STEP 4 | 配置防火墙的新管理密码。

在 *VM* 系列防火墙 *CLI* 上，您必须先配置唯一的管理密码，然后才能访问防火墙的 *Web* 界面。要登录到 *CLI*，您需要可用于启动防火墙的私钥。

1. 在 VM 系列防火墙的命令行界面 (CLI) 中使用 SSH 的公共 IP 地址。您将需要在3 中使用或创建的私钥才能访问 CLI。

   如果您已添加其他 *ENI* 支持使用 *ELB* 进行部署，则必须先为 *ENI* 创建和分配弹性 *IP* 地址才能访问 *CLI*，请参阅6。

   如果您正在使用 PuTTY 访问 SSH，则您必须将 .pem 格式转换为 .ppk 格式。参阅 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

2. 输入以下命令以登录到防火墙：

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*

3. 使用以下命令并按照屏幕上的提示配置新密码：

   配置

   set mgt-config users admin password

4. 如果存在需激活的 BYOL，请对 DNS 服务器的 IP 地址进行设置，以使防火墙可访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

   set deviceconfig system dns-setting servers primary *<ip_address>*

5. 使用以下命令提交您所做的更改：

   commit

6. 终止 SSH 会话。

STEP 5 | 关闭 VM 系列防火墙。

1. 在 EC2 仪表盘上，选择 **Instances**（实例）。
2. 从列表中选择 VM 系列防火墙，然后单击 **Actions**（操作） > **Stop**（停止）。

STEP 6 | 创建并分配弹性 IP 地址 (EIP) 至用于对防火墙进行管理访问的 ENI，然后重启 VM 系列防火墙。

1. 选择 **Elastic IPs**（弹性 **IP**），并单击 **Allocate New Address**（分配新地址）。
2. 选择 **EC2-VPC**，并单击 **Yes, Allocate**（是，分配）。
3. 选择新分配的 EIP，并单击 **Associate Address**（关联地址）。
4. 选择 **Network Interface**（网络接口）和与之相关联的 **Private IP address**（专用 **IP** 地址），然后单击 **Yes, Associate**（是，关联）。

©2024 Palo Alto Networks, Inc.

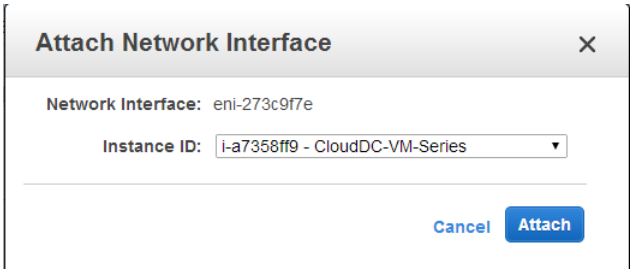
STEP 7 | 创建虚拟网络接口并将接口附加到 VM 系列防火墙。虚拟网络接口在 AWS 上称为弹性网络接口 (ENI)，并且在防火墙上可以用作数据面板网络接口。这些接口都用于处理流向/来自防火墙的数据流量。

您至少需要两个可使流量传入/出防火墙的 ENI。您最多可以添加七个 ENI 来处理 VM 系列防火墙的数据流量；检查 EC2 实例类型以确认它可以支持的最大接口数量。

1. 在 EC2 仪表盘上，选择 **Network Interfaces**（网络接口），然后单击 **Create Network Interface**（创建网络接口）。
2. 输入隧道的描述性名称。
3. 选择子网。使用子网 ID 以确保您已选择正确的子网。您只能将 ENI 附加到同一子网中的实例。
4. 输入要分配给接口的**Private IP**（专用 **IP**）地址或选择**Auto-assign**（自动分配）以自动分配选定子网中可用 IP 地址内的 IP 地址。
5. 选择 **Security group**（安全组）以控制访问数据面板网络接口。
6. 单击**Yes, Create**（是，创建）。



7. 要将 ENI 附加到 VM 系列防火墙，选择刚创建的接口，然后单击 **Attach**（附加）。



8. 选择 VM 系列防火墙的 **Instance ID**（实例 **ID**），然后单击 **Attach**（附加）。
9. 重复上述步骤可创建多个 ENI 并将其附加到防火墙。

STEP 8 | 在 VM 系列防火墙上激活许可证（基于使用的许可证模型无需进行此操作）。

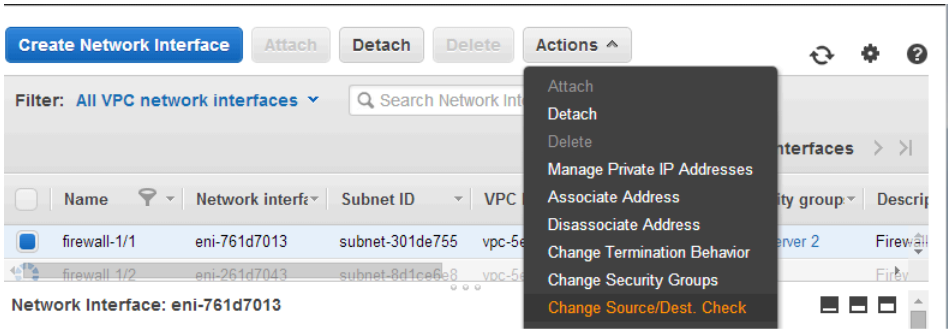
在 *AWS* 管理控制台上不执行此任务。激活许可证需要访问 *Palo Alto Networks* 支持门户和 *VM* 系列防火墙的 *Web* 界面。

请参阅激活许可证。

©2024 Palo Alto Networks, Inc.

STEP 9 | 在每个防火墙数据面板网络接口上禁用源/目标检查。禁用该选项可让接口处理不是以分配给网络接口的 IP 地址为目标的网络流量。

1. 在 EC2 仪表盘上，选择 **Network Interfaces**（网络接口）选项卡中的网络接口（如 eth1/1）。
2. 在 **Action**（操作）下拉列表中，选择 **Change Source/Dest.Check**（更改源/目标检查）。



3. 单击 **Disabled**（已禁用）并 **Save**（保存）您的更改。
4. 对每个防火墙数据面板接口重复步骤 1-3。

©2024 Palo Alto Networks, Inc.

STEP 10 | 配置数据面板网络接口作为防火墙上的第 3 层接口。

有关配置示例，请参阅步骤 14 到 17（在用例：保护 AWS 云中的 EC2 实例。

在 *VPC* 内的应用服务器上，定义防火墙的数据面板网络接口作为默认网关。

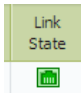
1. 在 Web 浏览器中使用安全连接 (https)，通过初始配置期间分配的 EIP 地址和密码登录 (https://<Elastic_IP address>)。您将看到证书警告；这属于正常情况。继续浏览网页。
2. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
3. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 VM_Series_untrust），然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **Static**（静态）或 **DHCP Client**（**DHCP** 客户端）。

     如果使用 **Static**（静态）选项，请单击 IP 部分中的 **Add**（添加），然后输入接口的 IP 地址和网络掩码，如 10.0.0.10/24。

     确保 IP 地址与之前分配的 ENI IP 地址相匹配。

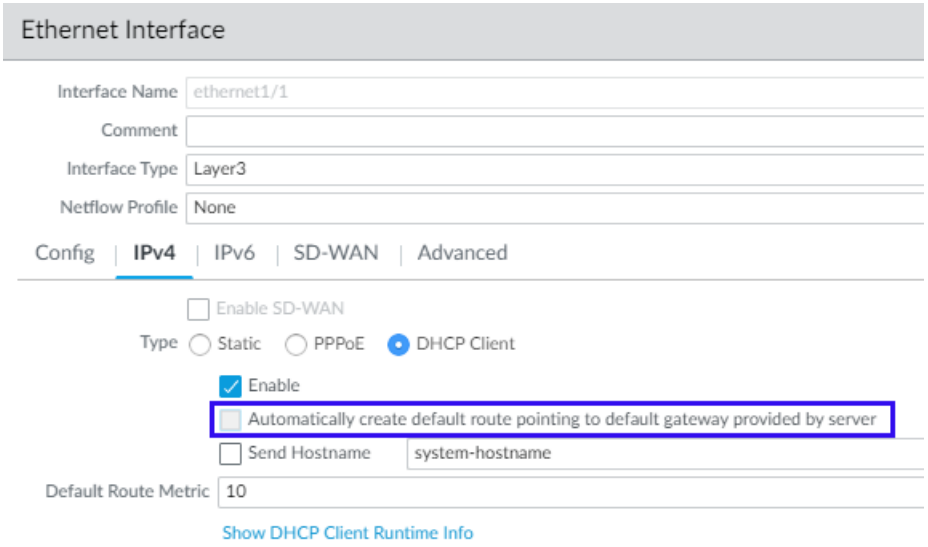
     如果使用 DHCP，选择 **DHCP Client**（**DHCP** 客户端）；将会自动获取在 AWS 管理控制台上分配给 ENI 的专用 IP 地址。
4. 单击 **ethernet 1/2** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 安全区域：VM_Series_trust
   - **IP Address**（**IP** 地址）：选择 **Static**（静态）或 **DHCP Client**（**DHCP** 客户端）单选按钮。

     对于静态，单击 IP 部分中的 **Add**（添加），然后输入接口的 IP 地址和网络掩码。确保 IP 地址与之前分配的附加 ENI IP 地址相匹配。
5. 单击 **Commit**（提交）。验证各接口的链接状态是否正常。



对于 *DHCP*，取消选中 ***Automatically create default route to default gateway provided by server***（自动创建指向服务器所提供的默认网关的默认路由）复选框。对于附加到 *VPC* 中私有子网的接口，禁用该选项可确保由此接口处理的流量不会直接流向 *VPC* 上的 *Internet* 网关。

©2024 Palo Alto Networks, Inc.



STEP 11 | 创建 NAT 规则以允许来自在 VPC 中部署的服务器的入站或出站流量。

1. 在防火墙的 Web 界面上选择 **Policies**（策略）> **NAT**。
2. 创建 NAT 规则以允许流量从防火墙的数据面板网络接口流向 VPC 的 Web 服务器接口。
3. 创建 NAT 规则以允许出站访问从 Web 服务器流向 Internet 的流量。

STEP 12 | 创建安全策略以允许/拒绝流向/来自在 VPC 中部署的服务器的流量。

1. 在防火墙的 Web 界面上选择 **Policies**（策略）> **Security**（安全）。
2. 单击 **Add**（添加），然后指定要执行限制的区域、应用程序和日志记录选项，并审核遍历网络的流量。

STEP 13 | 在防火墙上提交更改。

单击 **Commit**（提交）。

STEP 14 | 确认 VM 系列防火墙正在保护流量且 NAT 规则已生效。

1. 在防火墙的 Web 界面上选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）。
2. 查看日志以确保应用程序遍历与实施的安全策略相匹配的网络。

创建自定义 Amazon 机器映像 (AMI)

自定义 VM 系列 AMI 提供了一致性和灵活性，可以让您使用自己希望在网络上使用的 PAN-OS 版本部署 VM 系列防火墙，而不是仅限于使用发布到公共 AWS Marketplace 或 AWS GovCloud Marketplace 的 AMI。使用自定义 AMI 可加快使用您选择的 PAN-OS 版本部署防火墙的过程，因为它可以减少使用在 AWS 公共或 AWS GovCloud Marketplace 上发布的 AMI 配置防火墙的时间，然后执行软件升级来获得您已获得资格或想要在您的网络上使用的 PAN-OS 版本。

©2024 Palo Alto Networks, Inc.

您可以使用 BYOL、套餐 1 或套餐 2 许可证创建自定义 AMI。创建自定义 AMI 的过程要求从防火墙中删除所有配置，并将其重置为出厂默认设置，因此，在此工作流程中，您将从 AWS Marketplace 启动新的防火墙实例，而不是使用您完全配置的现有防火墙。

在使用防火墙的 *BYOL* 版本创建自定义 *AMI* 时，必须先在防火墙上激活许可证，以便可以访问和下载 *PAN-OS* 软件更新来升级防火墙，然后在将防火墙重置为出厂默认设置和创建自定义 *AMI* 之前停用防火墙上的许可证。如果未取消激活许可证，则会丢失在此防火墙实例上应用的许可证。

STEP 1 | 从 Marketplace 启动 VM 系列防火墙。

请参阅3

STEP 2 | （仅限 BYOL）激活许可证。

STEP 3 | 安装软件更新并将防火墙升级到计划使用的 PAN-OS 版本。

STEP 4 | （仅限 BYOL）停用许可证。

STEP 5 | 执行私有数据重置。

重置私有数据会删除所有日志并恢复默认配置。

不会擦除系统盘，因此，步骤 4 中的内容更新是完整的。

1. 访问防火墙 CLI。
2. 删除所有日志并恢复默认配置。

```
request system private-data-reset
```

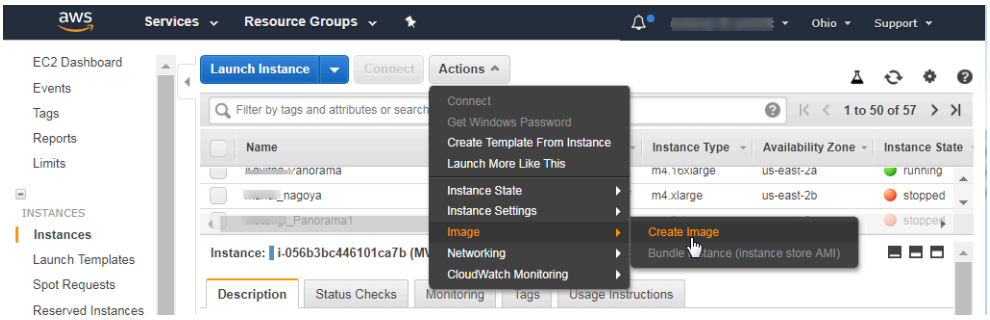
输入 **y** 以确认。

防火墙重新启动以初始化默认配置。

©2024 Palo Alto Networks, Inc.

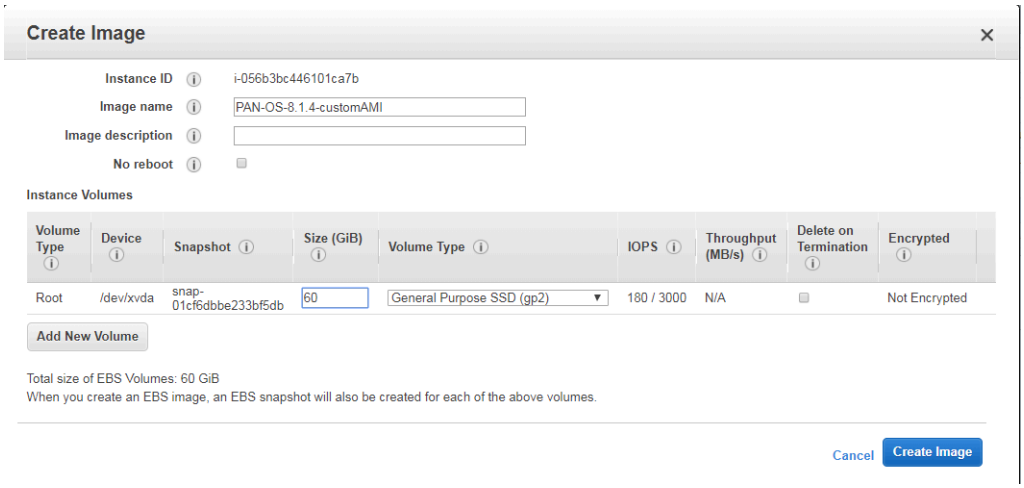
STEP 6 | 创建自定义 AMI。

1. 登录到 AWS 控制台，然后选择 EC2 仪表盘。
2. **Stop**（停止）VM 系列防火墙。
3. 选择 VM 系列防火墙实例，然后单击 **Image**（映像） > **Create Image**（创建映像）。



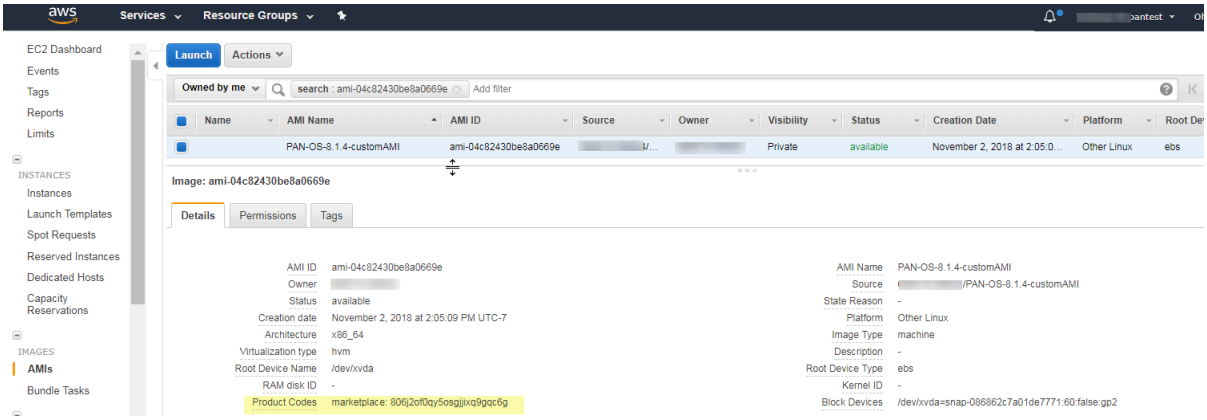
4. 输入自定义映像名称，然后单击 **Create Image**（创建映像）。

   最低要求 60GB 的磁盘空间。



5. 验证是否已创建自定义 AMI 且具有正确的产品代码。
   1. 在 EC2 仪表盘上，选择 **AMI**。
   2. 选择刚才创建的 AMI。根据选择的是具有 BYOL、套餐 1 或套餐 2 许可证选项的 AMI，您可以在详细信息中看到以下产品代码之一：
      - BYOL — 6njl1pau431dv1qxipg63mvah
      - 套餐 1 — 6kxdw3bbmdeda3o6i1ggqt4km
      - 套餐 2 — 806j2of0qy5osgjjixq9gqc6g

©2024 Palo Alto Networks, Inc.



STEP 7 | 在 AWS上 加密 VM 系列防火墙的 EBS 卷.

STEP 8 | 配置防火墙上的管理密码。

请参阅4

在 AWS上 加密 VM 系列防火墙的 EBS 卷

EBS 加密适用于所有 AWS EC2 实例类型，您可以在其上部署 VM 系列防火墙。要在 AWS 上的 VM 系列防火墙上安全地存储数据，您必须首先创建在 AWS 公共或 GovCloud Marketplace 上发布的 AMI 的副本，或者使用自定义 AMI，然后使用 AWS 密钥管理服务 (KMS) 上的客户主密钥 (CMK) 加密 EBS 卷。您可以使用 AWS 帐户的默认主密钥或之前使用 AWS 密钥管理服务创建的任何 CMK，以及 EBS KMS 进行交互以确保数据安全。

STEP 1 | 创建一个 AWS 上的加密密钥，如果您要使用帐户的默认主密钥，请跳过此步骤。

您将使用此密钥加密防火墙上的 EBS 卷。请注意，密钥是特定于区域的。

STEP 2 | 使用密钥加密防火墙上的 EBS 卷。

您必须创建要加密的 AMI 副本。您可以复制在 AWS 公共或 GovCloud Marketplace 上发布的 AMI，或使用自定义 AMI (创建自定义 Amazon 机器映像 (AMI))。

1. 在 EC2 仪表盘上，选择 AMI 并 **Copy AMI**（复制 **AMI**）。

2. 设置 AMI 的详细信息。
   确保选中 **Encrypt target EBS snapshots**（加密目标 **EBS** 快照）。

3. 选择加密密钥和 **Copy AMI**（复制 **AMI**）以创建加密的 EBS 快照。

4. 选择 **EC2 Dashboard**（**EC2** 仪表盘） > **Snapshots**（快照）以验证使用在上面选择的密钥加密 EBS 快照。

©2024 Palo Alto Networks, Inc.

使用 VM 系列防火墙 CLI 以交换管理接口

如果没有在部署防火墙时将管理接口 (MGT) 与数据面板接口 (ethernet 1/1) 互换，您可以使用 CLI 以使防火墙能在启动后接收主接口上的数据面板流量。

STEP 1 | 完成在 AWS 上启动 VM 系列防火墙中所述的步骤 1 到 7。

继续之前，验证防火墙是否至少有两个 *ENI*（*eth0* 和 *eth1*）。如果仅用一个 *ENI* 启动防火墙，接口交换命令可能使防火墙启动到维护模式。

STEP 2 | 在 EC2 仪表盘上查看 eth1 接口的 IP 地址，验证 AWS 安全组规则是否允许与新管理接口 (eth1) 建立连接（HTTPS 和 SSH）。

STEP 3 | 登录到 VM 系列防火墙 CLI，然后输入以下命令：

```
set system setting mgmt-interface-swap enable yes
```

STEP 4 | 确认希望交换接口，然后将 eth1 数据面板接口用作管理接口。

STEP 5 | 重启防火墙，以使交换操作成效。使用以下命令：

```
request restart system
```

STEP 6 | 验证接口交换已完成。使用以下命令：

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```

在 VM 系列防火墙上启用 CloudWatch 监控

AWS 上的 VM 系列防火墙可以将本机 PAN-OS 指标发布到 AWS CloudWatch，您可以用来监控防火墙。通过这些指标，您可以评估可用于启动或终止 VM 系列防火墙实例的性能和使用模式。

防火墙使用 AWS API 将指标发布到命名空间，该命名空间是在其中以指定间隔收集指标的 AWS 上的位置。当您配置防火墙以将指标发布到 AWS CloudWatch 时，可以在两个命名空间中查看指标 — 主要命名空间，用于收集并汇总配置为使用命名空间的所有实例的选定指标；辅助命名空间，使用后缀 `_dimensions` 自动创建的命名空间，可让您使用主机名和 AWS 实例 ID 元数据（或维度）筛选指标，并了解各个 VM 系列防火墙的使用情况和性能。

您可以在 CloudWatch 中监控指标或创建自动扩展策略以触发警报，并在监控的指标达到阈值时采取相关操作以手动部署防火墙的新实例。请参考有关最佳实践的 AWS CloudWatch 和自动扩展组 (ASG) 文档，了解设置扩展或缩小操作的警报条件。

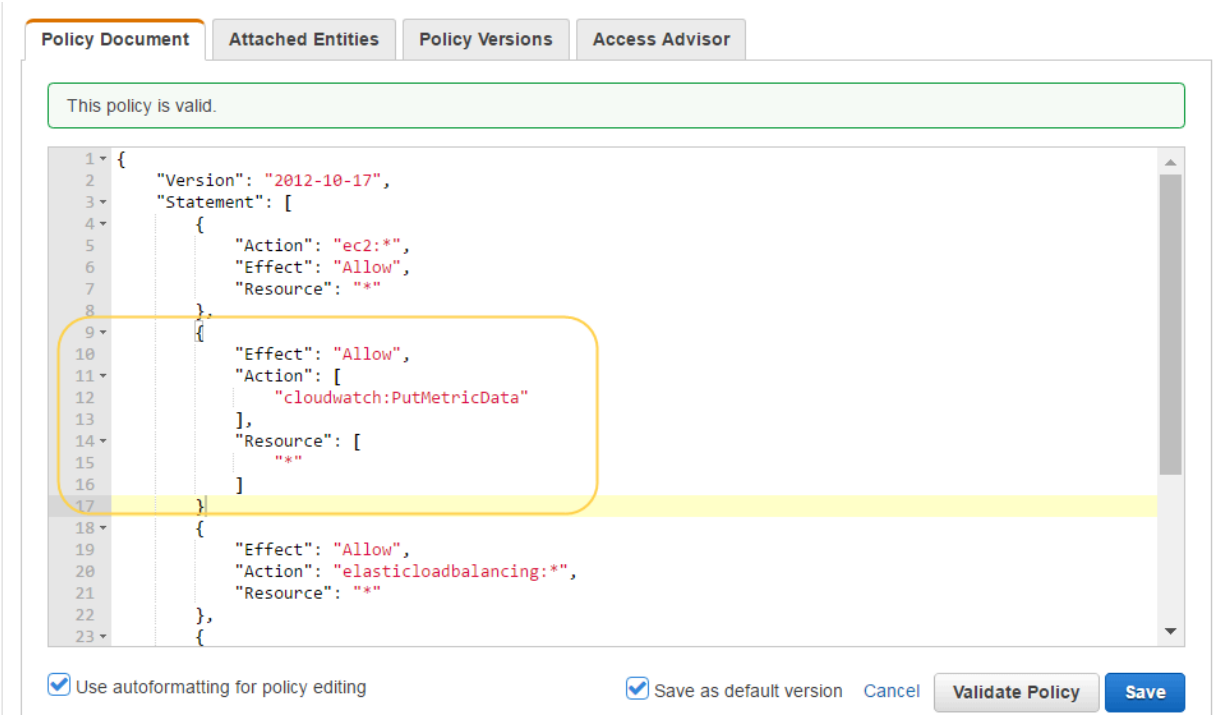
有关发布到 CloudWatch 上的 PAN-OS 指标详细信息，请参阅 发布用于监控的自定义 PAN-OS 指标。

©2024 Palo Alto Networks, Inc.

STEP 1 | 为用于在 AWS 上部署 VM 系列防火墙的 AWS 身份识别及访问管理 (IAM) 用户角色分配适当的权限。

无论是启动 VM 系列防火墙的新实例还是升级 AWS 上现有 VM 系列防火墙，与实例相关联的 IAM 角色都必须拥有将指标发布到 CloudWatch 的权利。

1. 在 AWS 控制台上，选择 IAM。
2. 编辑 IAM 角色以授予以下权限：



您可以在此处复制和粘贴权限：

```
 { "Version":"2012-10-17", "Statement": [ { "Effect":"Allow",
"Action": [ "cloudwatch:PutMetricData" ], "Resource":
[ "*" ] } ] }
```


©2024 Palo Alto Networks, Inc.

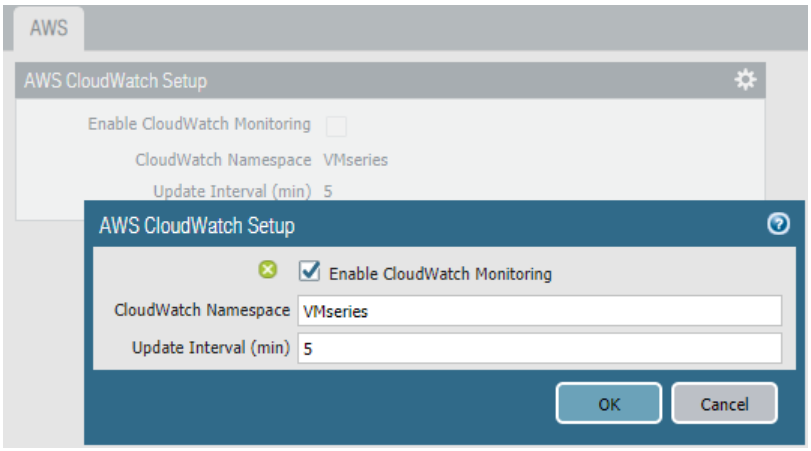
STEP 2 | 在 AWS 上的 VM 系列防火墙上启用 CloudWatch。

1. 登录到 VM 系列防火墙的 Web 界面。
2. 选择 **Device**（设备）> **VM-Series**（**VM** 系列）。
3. 在 AWS CloudWatch Setup（AWS CloudWatch 设置）中，单击 **Edit**（编辑）()，然后选择 **Enable CloudWatch Monitoring**（启用 **CloudWatch** 监控）。

   1. 输入防火墙可以发布指标的 **CloudWatch Namespace**（**CloudWatch** 命名空间）。命名空间不能以 **AWS** 为开头。

      HA 对或自动扩展部署中所有 VM 系列防火墙的汇总指标都将发布到您在上面输入的命名空间中。通过自动创建后缀为 `_dimensions` 的命名空间，您可以使用附加到防火墙的主机名或 AWS 实例 ID 元数据筛选和查看特定 VM 系列防火墙的指标。

   2. 将 **Update interval**（更新间隔）设置为 1-60 分钟之间的值。这是防火墙将指标发布到 CloudWatch 的频率。默认值为 5 分钟。



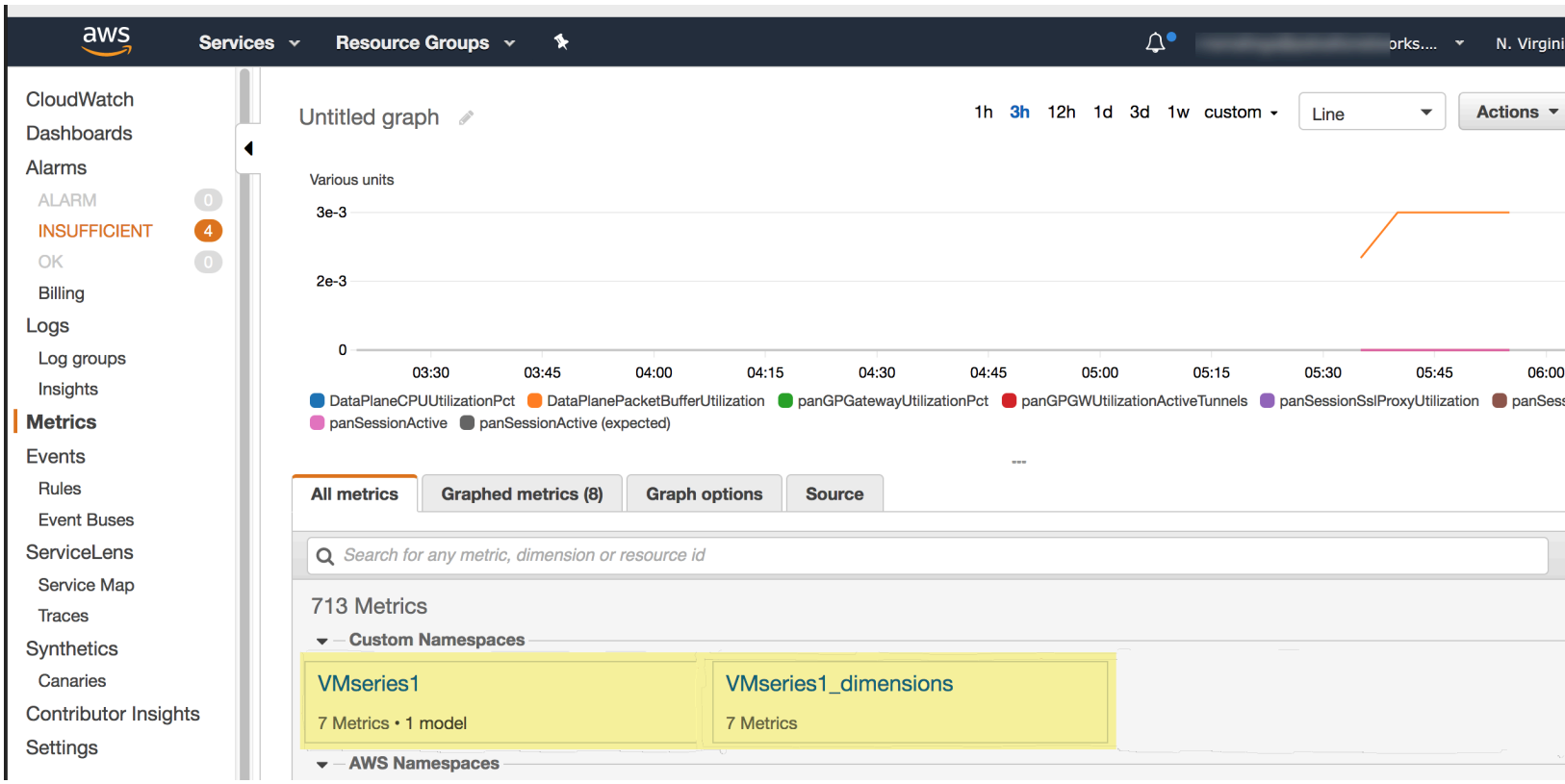
4. **Commit**（提交）更改。

   在防火墙开始将指标发布到 CloudWatch 之前，您无法为 PAN-OS 指标配置警报。

©2024 Palo Alto Networks, Inc.

STEP 3 | 确认您可以在 CloudWatch 上查看指标。

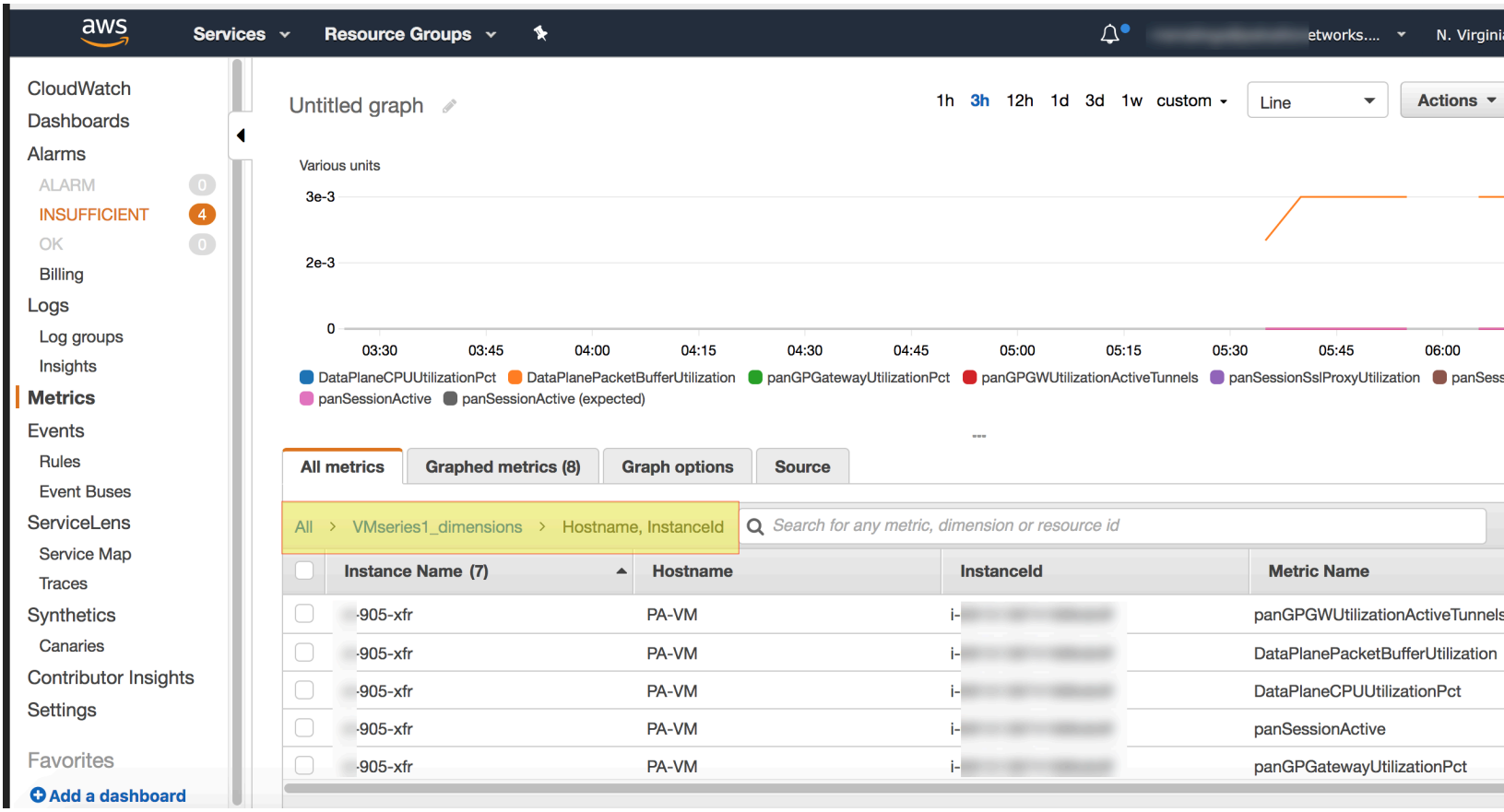
1. 在 AWS 控制台上，选择 **CloudWatch** > **Metrics**（指标）按类别查看 CloudWatch 指标。
2. 从 Custom Metrics（自定义指标）下拉列表中选择命名空间。



3. 确认您可以在查看列表中看到 PAN-OS 指标。

   要按特定防火墙的主机名或 AWS 实例 ID 进行筛选，请选择 `_dimensions`。

 ©2024 Palo Alto Networks, Inc.



STEP 4 | 在 CloudWatch 上配置 PAN-OS 指标的警报和操作。

请参考 AWS 文档：http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

包含引导配置的 VM 系列防火墙大约需要 7 至 9 分钟才能提供服务。因此，下面是一些关于如何设置触发 VM 系列防火墙自动扩展的警报的示例：

- 如果已将 2 个 VM 系列防火墙实例部署为 GlobalProtect 网关以保护远程用户，请使用 GlobalProtect 网关活动通道指标。您可以配置当活动隧道数大于 300 个达到 15 分钟时的警报，也可以部署引导和配置作为 GlobalProtect 网关的 2 个 VM 系列防火墙实例。
- 如果您使用防火墙保护 AWS 中的工作负载，请使用会话利用率指标根据资源使用情况缩小或扩展防火墙。您可以配置当会话利用率指标大于 60# 达到 15 分钟时的警报，以部署 1 个 VM 系列防火墙实例。相反，如果会话利用率低于 50# 达到 30分钟，则终止 VM 系列防火墙实例。

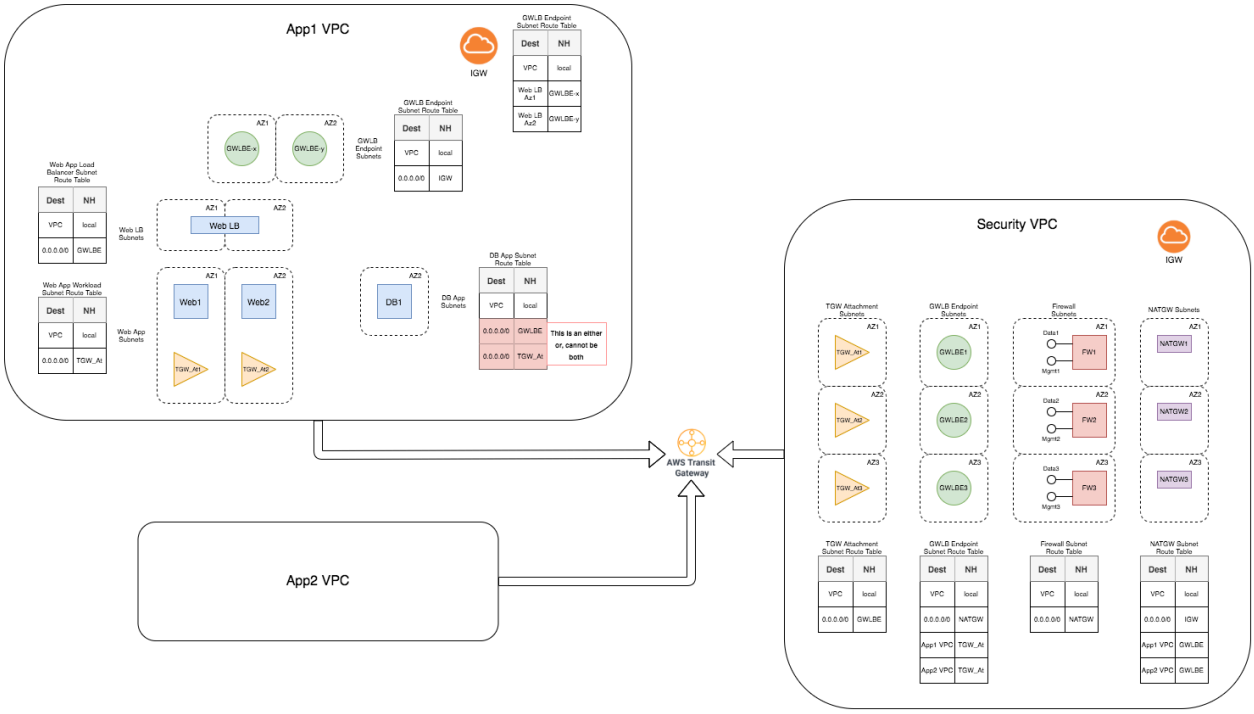
©2024 Palo Alto Networks, Inc.

AWS 中的 Panorama Orchestrated 部署

使用适用于 AWS 3.0.1 或更高版本的 Panorama 插件在 AWS 中编排 VM 系列防火墙部署，并为托管防火墙启用安全策略。AWS Orchestration 设计为一种即插即用型号，适用于在 AWS 中设置安全部署。它通过将所有配置集中到 Panorama 上的一个屏幕中，简化了现有网关负载均衡器 (GWLB) 解决方案的部署。Panorama 允许您使用插件管理部署和资源配置。该插件还通过生成所需的基线配置执行防火墙管理，以获得部署的流量。配置策略时，该插件将为所有流量协议提供入站、出站和东西向流量服务。使用此插件可配置、部署和管理您的安全部署。

下图突出显示了安全 VPC 部署的拓扑结构。在这里，将所有安全资源部署到插件托管的安全 VPC。利用 GWLB 解决方案将流量从应用程序重定向到防火墙堆栈。

©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

作为 AWS 云上基础设施设置的一部分，该插件使用 GWLB 端点、防火墙以及 NAT 网关子网和路由表创建安全 VPC。该插件不会创建 AWS 中转网关 (TGW)。

VM 系列防火墙可检查在 VPC 之间路由的流量。

源自应用程序 VPC 的入站流量通过 IGW 流入，然后根据边缘路由重定向到 GWLB 端点。为了进行检查，流量会通过 GWLB 端点进入安全 VPC 中的防火墙。完成检查后，流量将回到 GWLB 端点并定向到原应用程序。

对于出站和东西向流量，该解决方案需要利用 TGW。创建 TGW 时，该插件会在安全 VPC 中创建 TGW 附件和路由表。您必须将应用程序 VPC 连接到在安全 VPC 配置中使用的 TGW。还必须通过将路由添加到与工作负载子网相关联的路由表中，从而将出站和东向西流量定向到 TGW。您必须修改应用程序 VPC 附件路由表才能将东向西和出站流量定向到安全 VPC 附件。

该插件会监控 TGW 附件，以了解新添加和删除的 VPC 附件。当插件检测到现有或新附件时，它会在安全 VPC 中进行必要的更改，以确保在将流量发送回 TGW 之前，防火墙会检查进入 TGW 的流量。这些更改包括将路由添加到 NAT 网关路由表，从而将出站流量定向回 GWLB 端点，然后定向到 GWLB 端点路由表，以便在完成检查后将流量返回到 TGW。该插件会更新 TGW 附件路由表，以确保将从安全 VPC 返回到 TGW 的流量发送到正确的应用程序附件。来自应用程序 VPC 的流量会通过路由定向到 TGW。当流量到达安全 VPC 中的 TGW 附件时，附件路由表会将流量发送到安全 VPC。在安全 VPC 中，流量会被定向到现有的 GWLB 端点，然后被定向到防火墙来进行检查。出站流量通过 NAT 网关流出到原始目标地址。东西向流量将被发送回 TGW，路由表会在其中将流量定向到原始目标地址。

- 准备编排 AWS 部署
- 在 AWS 中编排 VM 系列防火墙部署
- 查看部署状态
- 流量和配置

准备编排 AWS 部署

在 AWS 上编排 VM 系列防火墙之前，请在 AWS 和 Panorama 上完成以下任务。

- **AWS**
  - AWS 上 Panorama 编排的部署需要两个可用区域（最多支持六个可用区域）。
  - 为具有编程访问权限和必要权限的特定 AWS 帐户创建 AWS 用户或实例配置文件，从而允许该插件在安全 VPC 上创建资源。

    对于安全帐户 — 具有用户或实例配置文件的 AWS 帐户，该帐户具有启动 AWS 资源的必要权限，例如 VPC、VM 实例、AWS 负载均衡器、NAT 网关和端点。插件需要现有用户或实例配置文件具有以下权限集才能声明 IAM 角色有效。单击 **Security Account**（安全帐户）下的 CFT 超链接可创建具有以下权限的策略。

```
"Statement":[ { "Effect":"Allow", "Action": "ec2:*", "Resource":
 "*" }, { "Effect":"Allow", "Action": "elasticloadbalancing:*",
 "Resource": "*" }, { "Effect":"Allow", "Action":
 "cloudwatch:*", "Resource": "*" }, { "Effect":"Allow", "Action":
```

 ©2024 Palo Alto Networks, Inc.

```
"autoscaling:*", "Resource": "*" }, { "Effect":"Allow",
"Action": "sts:assumerole", "Resource": "*" },
{ "Effect":"Allow", "Action": "cloudformation:*", "Resource":
"*" }, { "Effect":"Allow", "Action": [ "iam:Get*", "iam:List*",
"iam:PassRole" ], "Resource": "*" }, { "Effect":"Allow",
"Action": "ram:*", "Resource": "*" } ] },
```

以下细化权限可满足您的要求和安全权限。这些权限提供从插件进行 API 调用的详细说明。这些权限经过细化，支持从安全 VPC 和跨帐户应用程序 VPC 的 CFT 和插件后端代码调用的每个操作。

以下权限未在适用于 *Panorama 3.0.1* 版本的 *AWS* 插件中实现，因为详细权限列表超出 *AWS* 策略大小限制。对于内联策略，您可以为用户、角色或组添加任意数量的策略，但每个实体的总策略大小不能超过以下限制 — 用户策略大小不能超过 *2048* 个字符、角色策略大小不能超过 *10240* 个字符、组策略大小不能超过 *5120* 个字符。由于这些限制和后端验证时间，您必须使用上述权限。

```
{ "Version":"2012-10-17", "Statement":
 [ { "Sid":"VisualEditor0", "Effect":"Allow",
 "Action": [ "ec2:AuthorizeSecurityGroupIngress",
 "cloudwatch:PutMetricData", "ec2:Describe*",
 "cloudwatch:DeleteAlarms", "autoscaling:DescribePolicies",
 "ec2:DeleteVpcEndpoints", "ec2:AttachInternetGateway",
 "ec2:AcceptTransitGatewayVpcAttachment",
 "autoscaling:ExecutePolicy", "ec2:DeleteRouteTable",
 "sts:GetSessionToken", "cloudformation:DescribeStackEvents",
 "ec2:RevokeSecurityGroupEgress", "ec2:CreateRoute",
 "ec2:CreateInternetGateway", "cloudformation:UpdateStack",
 "ec2:DeleteInternetGateway", "iam:ListRolePolicies",
 "autoscaling:TerminateInstanceInAutoScalingGroup",
 "iam:ListPolicies", "ec2:DisassociateTransitGatewayRouteTable",
 "iam:GetRole", "iam:GetPolicy", "ec2:CreateTags",
 "elasticloadbalancing:CreateTargetGroup",
 "ec2:RunInstances", "ec2:DisassociateRouteTable",
 "ec2:CreateVpcEndpointServiceConfiguration",
 "ec2:CreateTransitGatewayRoute",
 "ec2:CreateTransitGatewayVpcAttachment",
 "elasticloadbalancing:DescribeAccountLimits",
 "elasticloadbalancing:AddTags", "cloudformation:DeleteStack",
 "cloudwatch:DescribeAlarms", "ec2:DeleteNatGateway",
 "ram:AssociateResourceShare",
 "autoscaling:DeleteAutoScalingGroup", "ec2:CreateSubnet",
 "elasticloadbalancing:ModifyLoadBalancerAttributes",
 "iam:GetRolePolicy", "ec2:ModifyVpcEndpoint",
 "ec2:DisassociateAddress",
 "autoscaling:DescribeAutoScalingInstances",
 "ec2:ModifyVpcEndpointServicePermissions",
 "ec2:CreateNatGateway", "ec2:CreateVpc",
 "ec2:ModifySubnetAttribute", "iam:PassRole",
 "autoscaling:DescribeScalingActivities",
 "sts:DecodeAuthorizationMessage",
 "autoscaling:DescribeLoadBalancerTargetGroups",
 "iam:ListAttachedGroupPolicies",
 "ec2:DeleteLaunchTemplateVersions", "sts:GetServiceBearerToken",
```


©2024 Palo Alto Networks, Inc.

```
"iam:ListAccessKeys", "ram:DisassociateResourceShare",
"ec2:ReleaseAddress", "ec2:DeleteLaunchTemplate",
"elasticloadbalancing:CreateLoadBalancer",
"ec2:AcceptVpcEndpointConnections", "iam:ListGroupPolicies",
"iam:ListRoles", "elasticloadbalancing:DeleteTargetGroup",
"ram:AssociateResourceSharePermission",
"ec2:CreateLaunchTemplate",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DeleteListener",
"ram:UpdateResourceShare", "iam:GetPolicyVersion",
"ec2:DeleteSubnet", "ec2:ModifyVpcEndpointServiceConfiguration",
"ec2:CreateTransitGatewayRouteTable",
"ec2:ModifyTransitGateway",
"cloudformation:DescribeStackResource",
"ec2:AssociateRouteTable",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DescribeLoadBalancers",
"logs:CreateLogStream", "ec2:GetLaunchTemplateData",
"ec2:DeleteTransitGatewayVpcAttachment",
"autoscaling:DescribeAutoScalingGroups",
"iam:ListAttachedRolePolicies", "logs:GetLogEvents",
"autoscaling:UpdateAutoScalingGroup",
"ec2:AssociateTransitGatewayRouteTable",
"elasticloadbalancing:ModifyTargetGroupAttributes",
"autoscaling:SetDesiredCapacity",
"cloudformation:DescribeStackResources", "ec2:CreateRouteTable",
"ec2:DetachInternetGateway", "cloudformation:DescribeStacks",
"ec2:DeleteTransitGatewayRouteTable", "sts:AssumeRole",
"ec2:DeleteTransitGatewayRoute", "iam:GetUserPolicy",
"iam:ListGroupsForUser", "ec2:DeleteVpc", "iam:GetGroupPolicy",
"ec2:AssociateAddress", "autoscaling:CreateAutoScalingGroup",
"ram:AcceptResourceShareInvitation",
"ec2:DeleteTags", "logs:DescribeLogStreams",
"ec2:DeleteVpcEndpointServiceConfigurations",
"autoscaling:DeletePolicy", "elasticloadbalancing:RemoveTags",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:DescribeListeners",
"autoscaling:PutScalingPolicy", "ec2:CreateSecurityGroup",
"iam:ListAttachedUserPolicies", "ec2:ModifyVpcAttribute",
"ec2:ModifyInstanceAttribute",
"ec2:GetTransitGatewayRouteTableAssociations",
"ram:DeleteResourceShare", "ec2:AuthorizeSecurityGroupEgress",
"ec2:ModifyTransitGatewayVpcAttachment",
"iam:GetInstanceProfile",
"ram:DisassociateResourceSharePermission",
"elasticloadbalancing:DescribeTags", "ec2:DeleteRoute",
"iam:ListUserPolicies", "logs:PutLogEvents",
"ec2:AllocateAddress", "ec2:CreateLaunchTemplateVersion",
"cloudwatch:PutMetricAlarm", "cloudformation:CreateStack",
"ec2:CreateVpcEndpoint", "ec2:DeleteSecurityGroup",
"ec2:StartVpcEndpointServicePrivateDnsVerification",
```


©2024 Palo Alto Networks, Inc.

```
 "ec2:ModifyLaunchTemplate", "iam:ListUsers",
 "ram:CreateResourceShare" ], "Resource": "*" } ] }
```

对于应用程序帐户 — 除安全帐户（托管 TGW 或需要保护的应用程序）以外的 AWS 帐户。在此帐户中，必须创建具有以下权限的 RoleARN。

```
{ "Version":"2012-10-17", "Statement": [ { "Action":
 [ "ec2:Describe*", "ec2:DisassociateTransitGatewayRouteTable",
 "ec2:CreateTransitGatewayRoute",
 "ec2:CreateTransitGatewayRouteTable",
 "ec2:AssociateTransitGatewayRouteTable",
 "ec2:DeleteTransitGatewayRouteTable",
 "ec2:DeleteTransitGatewayRoute",
 "ec2:GetTransitGatewayRouteTableAssociations" ], "Resource":
 "*", "Effect":"Allow" }, { "Action": [ "iam:Get*",
 "iam:List*" ], "Resource": "*", "Effect":"Allow" } ] }
```

- **Dedicated CIDR block**（专用 **CIDR** 块）— 为安全 VPC 保留的 CIDR 块。插件管理此 CIDR 块，并用来为安全 VPC 启动防火墙、负载均衡器和其他部署资源。
- **AWS** 中转网关 — 创建 TGW 并确保所选 AWS 用户有权限配置 TGW 资源。

- **Panorama**
  - 适用于 **AWS** 的 **Panorama** 插件 — 版本 3.0.1 或更高版本。
  - **VM-Series Plugin**（**VM** 系列插件）— 版本 2.0.6 或更高版本。
  - **PanOS** — 版本 10.0.5 或更高版本。
  - 创建在 Panorama 上配置的有效许可证 API 密钥，用于取消防火墙的许可。
  - 在 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Roles**（**IAM** 角色）下的插件上创建 IAM 角色。此配置需要与您在 AWS 帐户中创建的用户相关联的访问密钥和秘密密钥。

在 Panorama 中为 AWS 插件配置 IAM 角色

使用 AWS 插件版本 3.0.1 或更高版本，您可以使用 IAM 角色支持 Panorama 在 AWS 帐户中部署的资源上进行身份验证和检索元数据。如果 Panorama 未部署在 AWS 上，您有两种选择。您可以为 AWS 帐户提供长期 IAM 凭据，也可以在 AWS 上设置 Assume 角色，从而允许访问同一 AWS 帐户或跨帐户中的已定义 AWS 资源。建议将承担角色作为更安全的选项。

STEP 1 | 要验证为安全 VPC 创建的 AWS 用户凭据，请转到 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Roles**（**IAM** 角色）。

STEP 2 | 单击 **Add**（添加），然后在 **Security Account Detail**（安全帐户详细信息）下输入以下详细信息。

- 输入 IAM 角色的名称和可选说明。
- 输入 AWS 访问密钥和秘密密钥以验证权限。重新输入秘密密钥以确认秘密访问密钥。
- 选择帐户类型 — **Instance Profile**（实例配置文件）或 **AWS Account Credentials**（**AWS** 帐户凭据）。如果 Panorama 部署在 AWS 上，您可以选择将具有正确权限的实例配置文件附

©2024 Palo Alto Networks, Inc.

加到 Panorama，或在 Panorama 上添加与 IAM 角色相关联的凭据。如果 Panorama 不是部署在 AWS 上，则必须在 Panorama 上输入 IAM 角色的凭据。

STEP 3 | 在 **Application Account Details**（应用程序帐户详细信息）下，搜索并选择所需的 RoleARN，为安全帐户提供访问应用程序 VPC 中资源的有效权限。

为便于识别，监视和部署的有效性状态采用颜色编码。

- 有效（绿色） — 表示机密密钥和访问密钥有效。此外，为应用程序帐户访问输入的所有 RoleARN 都具有执行必要操作的有效权限。
- 部分有效（橙色v — 表示机密密钥和访问密钥有效，但为应用程序帐户访问输入的一个或多个 RoleARN 没有执行必要操作的有效权限。单击状态超链接以打开 IAM，并查看哪些特定 RoleARN 不符合要求。
- 无效（红色） — 表示输入的机密密钥和访问密钥无效或没有执行必要操作的权限。
- 需要提交（灰色）— 表示角色需要提交。
- 正在验证（灰色）— 表示插件正在尝试连接到 AWS 来检查必要的要求。如果此状态持续几秒钟，请验证是否已建立与 AWS 的连接。

只有状态为绿色或橙色的 IAM 角色才能进行进一步的部署配置。

在 AWS 中编排 VM 系列防火墙部署

完成以下过程，在 AWS 中协调 VM 系列防火墙的部署。

在代理后部署时，不支持在 *AWS* 上使用实例配置文件进行 *Panorama* 部署。

STEP 1 | 登录 Panorama Web 界面。

STEP 2 | 安装适用于 AWS 3.0.1 或更高版本的 Panorama 插件。

要将 *AWS* 的 *Panorama* 插件升级到 *3.0.1* 版，必须先将该插件升级到 *2.0.2* 版。安装 *AWS* 插件版本 *3.0.1* 后，您无法降级到 *2.0.x* 或更低版本。

如果拥有 *Panorama HA* 配置，则在每个 *Panorama* 对等上重复安装/升级过程。

如果当前已安装适用于任何云平台的 *Panorama* 插件，则安装（或卸载）其他插件需要重新启动 *Panorama*，以便提交更改。

STEP 3 | 在 Panorama 中为 AWS 插件配置 IAM 角色

STEP 4 | 选择 **Panorama** > **Plugins**（插件） > **AWS** > **Deployments**（部署）以 **Add**（添加）新部署。

©2024 Palo Alto Networks, Inc.

STEP 5 | 在 **General**（常规）选项卡中输入部署的常规详细信息。

- 输入 **Name**（名称）和可选 **Description**（说明）以标识 Panorama 和 AWS 云中的部署。
- 从下拉列表中选择 **IAM Role**（**IAM** 角色）。该列表显示具有有效或部分有效部署权限的 IAM 角色。

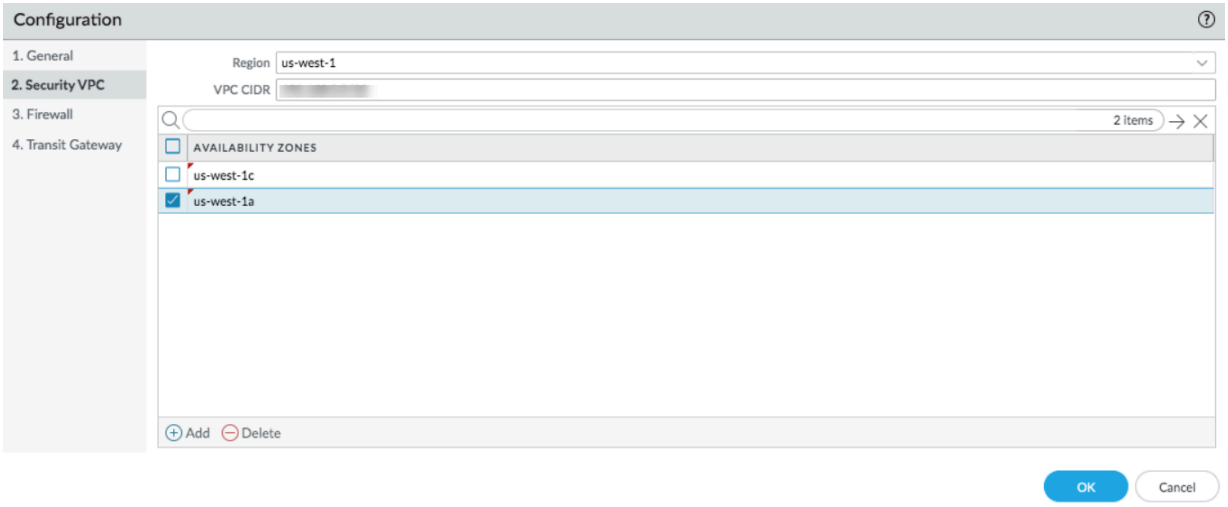
> 创建 *IAM* 角色并将其添加到部署后，您可以编辑 *IAM* 中的信息（例如机密密钥和访问密钥）。但是，您无法编辑 *IAM* 角色的名称。要更改名称，您必须删除 *IAM* 并重新创建一个。



 ©2024 Palo Alto Networks, Inc.

STEP 6 | 在 **Security VPC**（安全 **VPC**）选项卡中输入与安全 VPC 相关的信息。

- 选择您打算在其中启动部署的 AWS **Region**（区域）。该列表根据所选 IAM 角色显示区域。
- 输入 **VPC CIDR** 值以在安全 VPC 中创建资源。此 CIDR 将由 AWS 插件托管。
- 从预填充列表中选择两个或多个 **Availability Zones**（可用性区域），并遵循与 AWS 中相同的映射。此列表根据您选择的区域填充。



STEP 7 | 选择 **Firewall**（防火墙） > **Image**（映像）并输入以下详细信息。

- **License Type**（许可证类型）— 提供了标准许可证类型 **Bring Your Own License**（自带许可证）(BYOL)、**Pay As you Go-Marketplace-Bundle1**（现收现付市场套餐 **1**）和 **Pay As you Go-Marketplace-Bundle2**（现收现付市场套餐 **2**）作为下拉列表中的选项（基于所选区域）。如果选择 **Bring Your Own License**（自带许可证），请准备好输入许可证身份验证代码。

  现收现付套装 *1* 和套装 *2* 不能与 *AMI* 自定义映像一起使用。

- （可选 — 仅在选择 **Bring Your Own License**（自带许可证）许可证类型时才会显示）**License Authcode**（许可证授权代码）— 输入 BYOL 许可证的授权代码。此授权代码确定 **Instance Type**（实例类型）下拉列表中显示的实例类型。

©2024 Palo Alto Networks, Inc.

- **Instance Type**（实例类型）— 从支持的实例类型下拉列表中进行选择。此列表源自许可证授权代码。
- **Image Type**（映像类型）— 选择 Marketplace 映像或自定义映像。

  如果选择 **Marketplace Image**（**Marketplace** 映像），请从下拉列表中选择配置安全 VPC 时所选的区域内支持的 **PanOS** 版本 10.0.5 或更高版本。

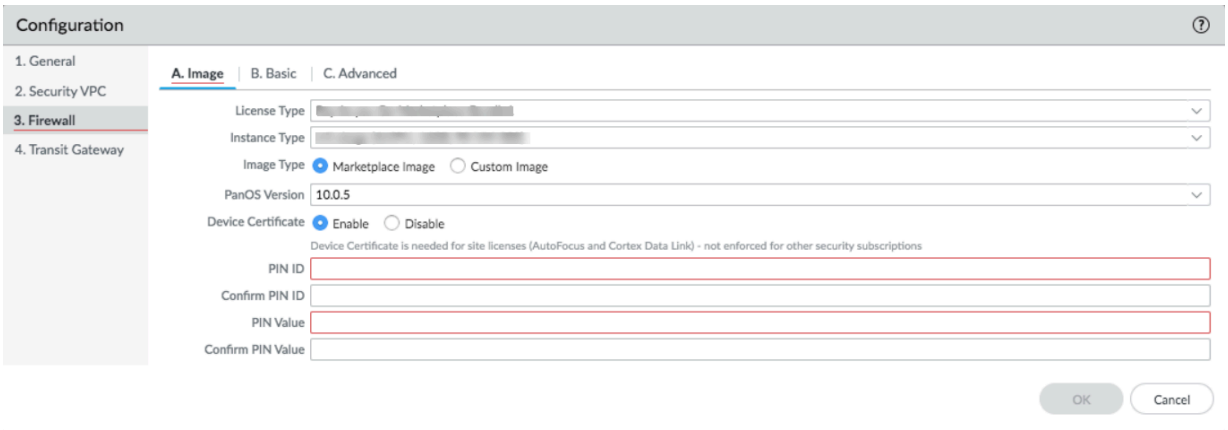
  如果选择 **Custom Image**（自定义映像），请输入 Amazon Machine Image (AMI) ID，然后选择 PanOS 版本 10.0.5 或更高版本。
- **Device Certificate**（设备证书）— 设备证书在客户支持门户上生成，用于检索 AutoFocus 或 Cortex Data Link 的站点许可证授权。如果未使用这些许可证，请选择 **Disable**（禁用）。要配置设备证书 PIN，请选择 **Enable**（启用）并输入以下信息：

  PIN ID— 输入 PIN ID。

  Confirm PIN ID（去人 **PIN ID**）— 再次输入 PIN ID。

  PIN Value（**PIN** 值）— 输入 PIN。

  Confirm VM PIN Value（确认 **VM PIN** 值）— 再次输入 PIN 值。



©2024 Palo Alto Networks, Inc.

STEP 8 | 选择 **Firewall**（防火墙）> **Basic**（基本），然后输入以下详细信息。

- **AWS Key Name**（**AWS** 密钥名称）— 部署防火墙后用于登录防火墙的 SSH 密钥的名称。此密钥引导防火墙，可用于在防火墙启动并运行时进行调试。
- **Existing Device Group**（现有设备组）— 如果您选择 **No**（否），则插件创建设备组名称的格式。如果您选择 **Yes**（是），则从下拉列表中选择现有 **Device Group**（设备组）。
- **Primary Panorama IP**（主要 **Panorama IP** 地址）— 您正在使用的 Panorama IP 地址。该下拉列表列出了管理接口上的公共和专用 IP 地址。从下拉列表中选择 IP 地址。

  如果您在代理后部署 *Panorama*，则必须在 ***Panorama*** > ***Setup***（设置）> ***Interfaces***（接口）下手动输入主要 *Panorama* 的公共 *IP* 地址。
- **Secondary Panorama IP**（辅助 **Panorama IP** 地址）— 如果使用 Panorama HA，则下拉列表中会显示辅助设备管理接口上的 IP 地址。从下拉列表中选择 IP 地址。

  如果辅助 *Panorama* 有公有 *IP* 地址，则可能不会出现在下拉列表中。在这种情况下，必须手动添加辅助 *Panorama* 的 *IP* 地址。
- **Min Firewalls**（最小防火墙数量）— 自动扩展组 (ASG) 中的最小防火墙数量。值介于 1 和 25 之间。
- **Max Firewalls**（最大防火墙数量）— ASG 中的最大防火墙数量。值介于 2 和 25 之间。
- **FirewallInstanceARN** — 在下拉列表中，选择在与防火墙实例相关联的 AWS 云上创建的 Assume RoleARN，以发布自动扩展指标。该下拉列表仅显示在 **Setup**（设置）> **IAM Roles**（**IAM** 角色）页面上输入的 RoleARN。



 ©2024 Palo Alto Networks, Inc.

STEP 9 | （可选）选择 **Firewall**（防火墙） > **Advanced**（高级），然后输入以下详细信息。

- **Autoscaling Metric**（自动扩展指标）— 从下拉列表中选择指标：数据平面 CPU 利用率百分比（默认）、活动会话、数据平面数据包缓冲区利用率百分比或会话利用率百分比。
- **Scale In Threshold**（缩小阈值）— 选择缩小阈值的值。该值取决于所选指标。
- **Scale Out Threshold**（扩大阈值）— 选择扩大阈值的值。该值取决于所选指标。
- **Scale Out Threshold**（扩大阈值）— 选择扩大阈值的值。该值取决于所选指标。
- **Jumbo Frame**（**Jumbo** 帧）— 默认禁用。您只能在准备初始部署时启用此选项。选择 **Enable**（启用）可在防火墙上启用巨型帧支持。



 ©2024 Palo Alto Networks, Inc.

STEP 10 | 选择是否连接到 **Transit Gateway**（中转网关）以处理跨安全 VPC 和应用程序 VPC 的流量路由。

- 选择您是否要 **Connect to TGW**（连接到 **TGW**）。如果选择 **Yes**（是），请准备好输入要连接安全 VPC 的 TGW ID。

  此配置仅适用于出站或东西向流量。

- （可选）选择要附加安全 VPC 的 **TGW ID**。

  如果要跨帐户使用它们，则必须共享 *TGW*。您可以在 *AWS* 上使用 ***Resource Access Manager***（资源访问管理器）*(RAM)* 共享中转网关。根据 *TGW* 所在的帐户创建 *RAM*。

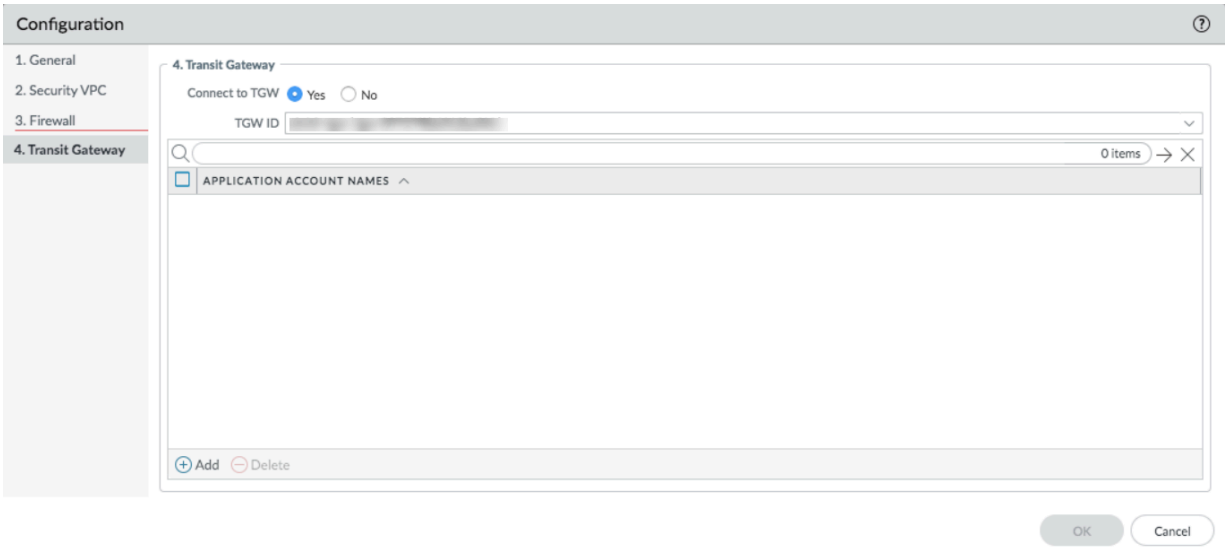
- 选择 **Application Account Names**（应用程序帐户名称）。如果 TGW 和安全 VPC 位于同一帐户中，请选择要与其共享 TGW 的应用程序帐户。该插件可在安全帐户中创建 RAM，以在所选应用程序帐户之间共享 TGW。您必须在此处选择的帐户上接受 RAM 邀请。

  如果 *TGW* 和安全 *VPC* 位于同一帐户中，则选择要共享 *TGW* 的应用程序帐户。如果 *TGW* 位于应用程序帐户下，请确保在 *RAM* 上共享 *TGW*。

  如果 TGW 在应用程序帐户（安全帐户除外）中：

  1. 确保与安全帐户共享 TGW。
  2. 使用 **Setup**（设置）> **IAM Roles**（**IAM** 角色）> **Application Account Details**（应用程序详细信息）下的 CFT 超链接。在 CFT 中，您可以为上述 TGW 创建 RAM。
  3. 在安全帐户中，请确保转到 AWS 控制台中的 RAM，并接受共享 TGW 的请求。

©2024 Palo Alto Networks, Inc.



STEP 11 | **Commit**（提交）以添加部署并推送到防火墙。

查看部署状态

如果 **Deployment Status**（部署状态）列中有条目，请单击超链接以查看部署详细信息。

可能的状态消息包括：

- **Commit changes**（提交更改）— 首次添加部署，但尚未提交更改。

  必须提交部署的每个配置更改，以便插件可以接受您的更改。

- **Deploying**（部署）— 插件正在部署或更新部署。有关详细信息，请单击超链接以查看详细状态。
- **Failure**（失败）— 部署已失败。单击超链接并查看安全堆栈的 **Detailed Status**（详细状态）。
- **Not Deployed**（未部署）— 插件已准备好部署配置，但尚未开始部署。
- **Success**（成功）— 插件已成功部署安全堆栈，且防火墙已连接到 Panorama。防火墙可以传递流量。

©2024 Palo Alto Networks, Inc.

- **Warning**（警告）— 部署已成功完成，但部署的外部操作已失败。例如，系统会显示以下消息：

  ```
  FWs have not connected after 20 minutes of the deployment completing.
  ```

  单击超链接并查看安全堆栈。

部署完成后，插件允许您修改某个参数子集。更改完成后，您必须在单击 **Redeploy**（重新部署）按钮之前进行提交。进行更新时，插件会确保 Panorama 配置已创建且准确无误。它会重新部署 CFT 以应用更改，并附加或分离配置的 TGW（如果此配置已修改）。

- **Deploy**（部署）— 提交初始配置后，选择 **Deploy**（部署）以启动部署。
- **Redeploy**（重新部署）— 修改部署并提交更改，然后选择 **Redeploy**（重新部署）。

  您必须提交对部署所做的更改，然后单击 ***Redeploy***（重新部署）。

- **Undeploy**（取消部署）— 删除部署，但保留配置以便日后可以重新部署。

要删除现有部署及其配置，请检查部署，然后选择 ***Deployment***（部署）页面底部的 ***Delete***（删除）。

详细状态

要访问 **Detailed Status**（详细状态），请单击 **Deployment Status**（部署状态）列中的超链接。您可以从详细状态中了解在何处应用配置、查看堆栈失败的错误消息或在部署时查看部署状态。

- **Name**（名称）— 部署名称。
- **Status**（状态）— 有关每种状态的说明，请参阅 Deployment Status（部署状态）。
- **Detail**（详细信息）— 有关在 **Deployment Status**（部署状态）中选择的部署的详细信息。例如，如果部署成功，则系统会显示部署的日期和时间；或者，如果堆栈失败，则系统会显示错误消息。
- **Policy Device Group**（策略设备组）— 插件可以为您的部署创建策略设备组，您也可以选择现有设备组作为特定部署的策略设备组。
- **Config Device Group**（配置设备组）— 插件创建配置设备组作为策略设备组的子项。插件将部署的配置信息放在配置设备组中，以确保在删除部署后策略设备组保持不变。

  请不要将策略信息放在配置设备组中。

- **Template Stack**（模板堆栈）— 显示与 VM 系列防火墙相关联的模板堆栈。将任何自定义配置都应用于此模板堆栈。
- **External IP**（外部 **IP**）— 显示安全 VPC 中 NAT 网关的公共 IP 地址，每个可用区一个地址。出站公共 IP 地址用于来自部署的所有出站流量，以及来自 VM 系列防火墙管理接口的出站流量。

  要允许防火墙连接到 *Panorama*，出站公共 *IP* 地址必须在 *Panorama* 安全组中列入白名单。

©2024 Palo Alto Networks, Inc.

- **CloudFormation Link**（**CloudFormation** 链接）— 此链接用于打开 AWS 控制台，以在 CloudFormation 服务部分中显示当前堆栈。您可以查看部署堆栈的位置并调试部署的问题。
- **CloudWatch Link**（**CloudWatch** 链接）— 此链接用于打开 AWS 控制台，以显示与防火墙相关的 **PaloAltoNetworkFirewalls** 日志和日志组。
- **AutoScalingGroup Link**（**AutoScalingGroup** 链接）— 此链接用于打开 AWS 控制台，以显示与部署相关联的 ASG 的详细信息和 ASG 下的实例列表。您可以通过 **CloudWatch Link**（**CloudWatch** 链接）查看与这些实例相关联的日志。
- **Endpoint Service Name**（端点服务名称）— 作为部署的一部分创建的 GWLB 端点名称。例如，com.amazonaws.vpce.us-east-1.vpce-svc-0d00ebcb0000dc000。
- **Cloudformation Stack Name**（**Cloudformation** 堆栈名称）— 例如，mynw-aws2-virgexstdg0-c0b0f。

流量和配置

插件用于部署和管理安全 VPC。该插件根据在 AWS Transit Gateway 上发现的附件更新安全 VPC 路由表。

入站流量

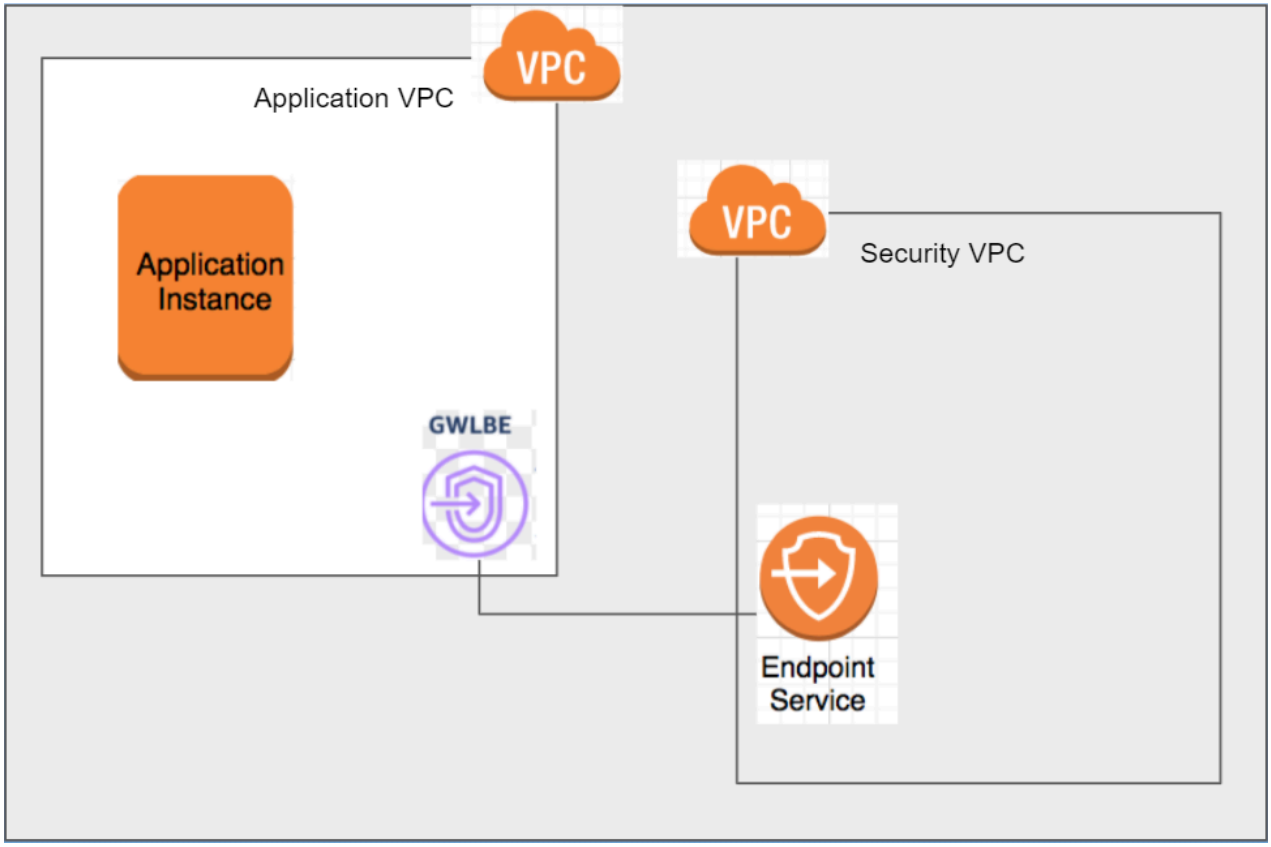
表 **2:** 入站流量组合

	应用程序	流量类型
1	在安全帐户中	入站
2	在应用程序帐户中	跨出站

用例：入站流量 - 应用程序在安全帐户中

插件在安全帐户上创建 VPC 服务端点。GWLB 端点必须与 VPC 端点服务相关联。

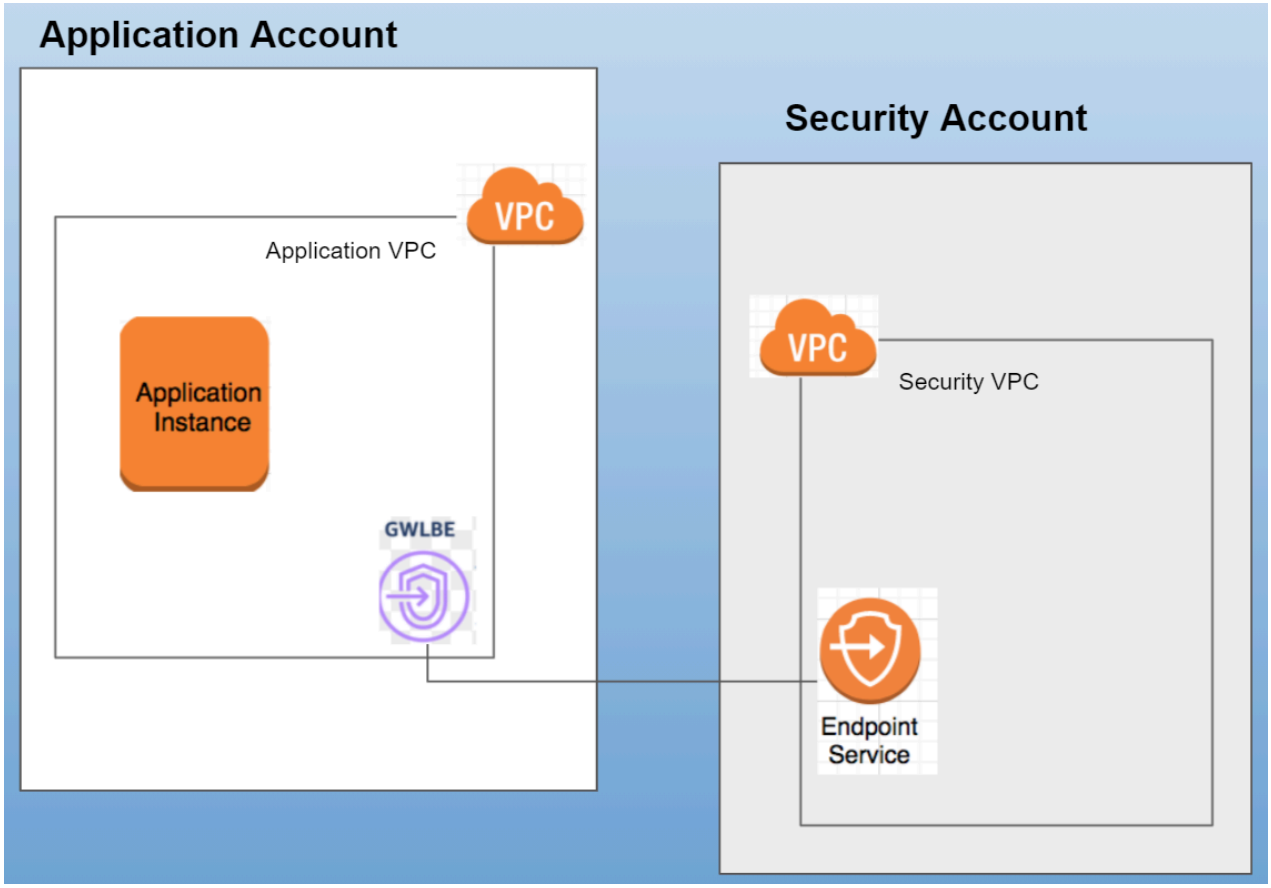
©2024 Palo Alto Networks, Inc.



用例：入站流量 - 应用程序在其他应用程序帐户中

如果应用程序位于其他帐户中，在 AWS 控制台的导航窗格中，选择 **Endpoint Services**（端点服务），然后选择端点服务。选择 **Actions**（操作） > **Add Principal**（添加主体）以允许主体。例如，**`arn:aws:iam::AccountNumber:root`**。GWLB 端点必须与 VPC 端点服务相关联。

©2024 Palo Alto Networks, Inc.



出站和东向西流量

表 **3:** 出站流量组合

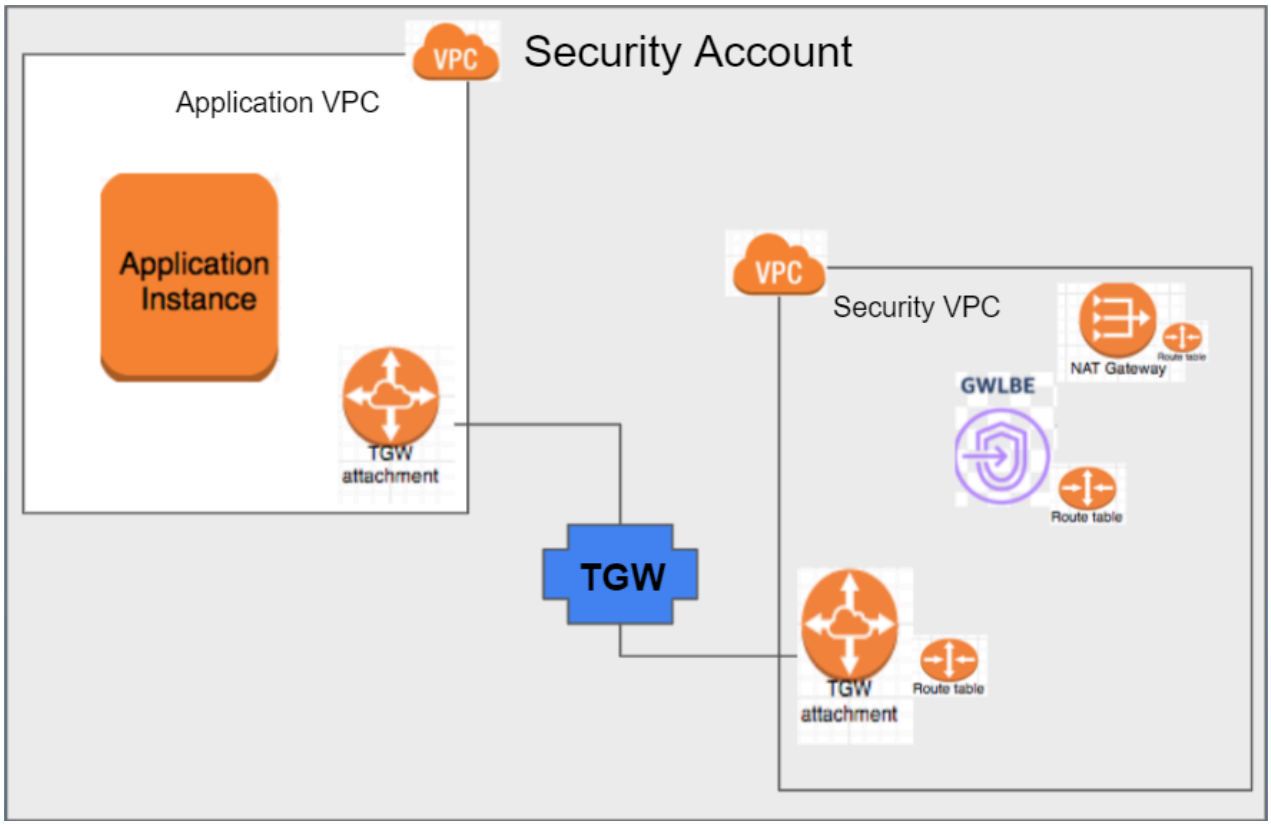
	中转网关	应用程序	流量类型
1	在安全帐户中	在安全帐户中	出站
2	在安全帐户中	在应用程序帐户中	出站
3	在应用程序帐户中	在应用程序帐户中	跨出站

©2024 Palo Alto Networks, Inc.

	中转网关	应用程序	流量类型
4	在应用程序帐户中	在安全帐户中	跨出站

用例：出站流量 - 中转网关和应用程序在安全帐户中

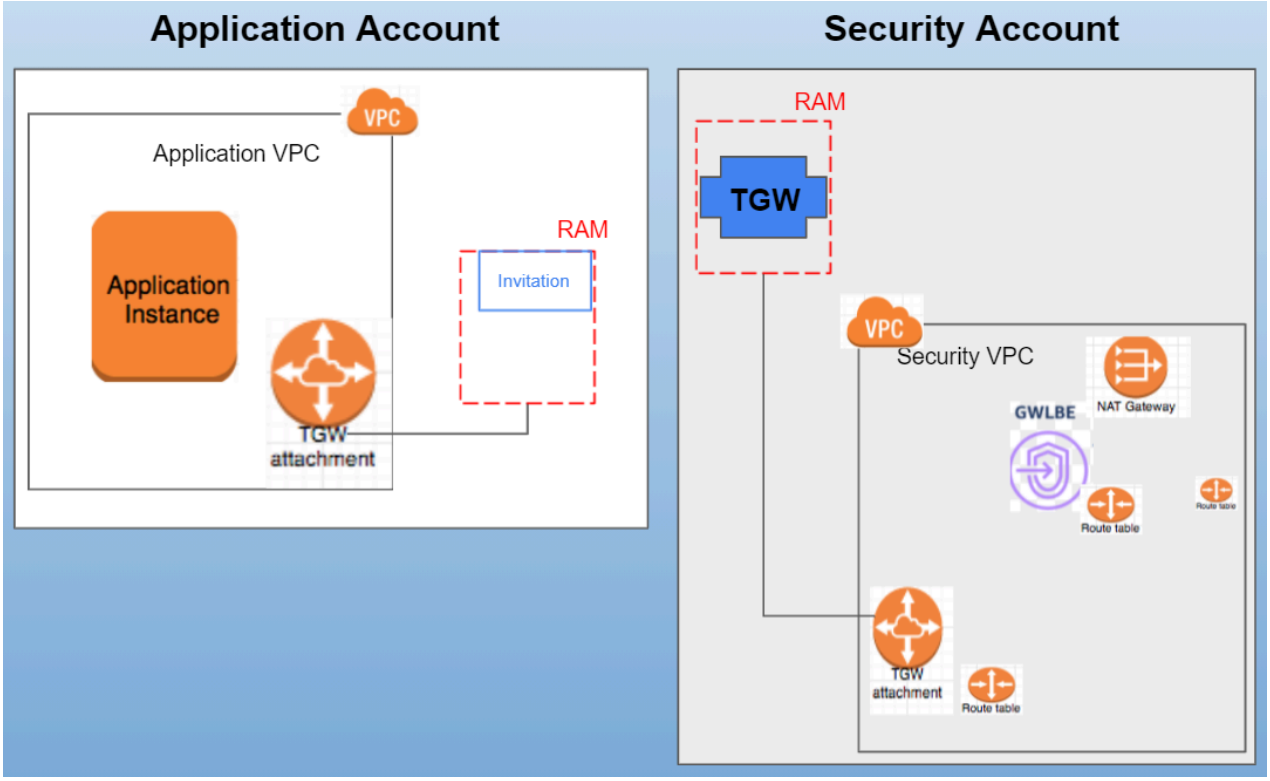
插件扫描配置的 TGW 上的附件。当插件检测到现有或新附件时，它会对安全 VPC 组件进行必要的路由表修改。



用例：出站流量 - 中转网关在安全帐户中，应用程序在应用程序帐户中

如果 TGW 位于安全帐户中，为了保护不在安全帐户中的应用程序，将在 AWS 控制台中使用资源访问管理器 (RAM) 在这些应用程序之间共享 TGW。您可以从插件用户界面中选择要与其共享 TGW 的帐户。当部署处于 **Deploying**（正在部署）状态时，监控应用程序帐户上的 RAM 以获取共享资源的邀请。

©2024 Palo Alto Networks, Inc.



用例：出站流量 - 中转网关和应用程序在应用程序帐户中

如果 TGW 是应用程序帐户，则必须使用 RAM 将其与安全帐户共享。要创建 TGW 附件和路由表，必须将此帐户的 ROLearn 添加到用于此部署的 IAM 中。使用 **Setup**（设置）> **Application Account**（应用程序帐户）下的 CFT 超链接来配置应用程序帐户先决条件。

©2024 Palo Alto Networks, Inc.

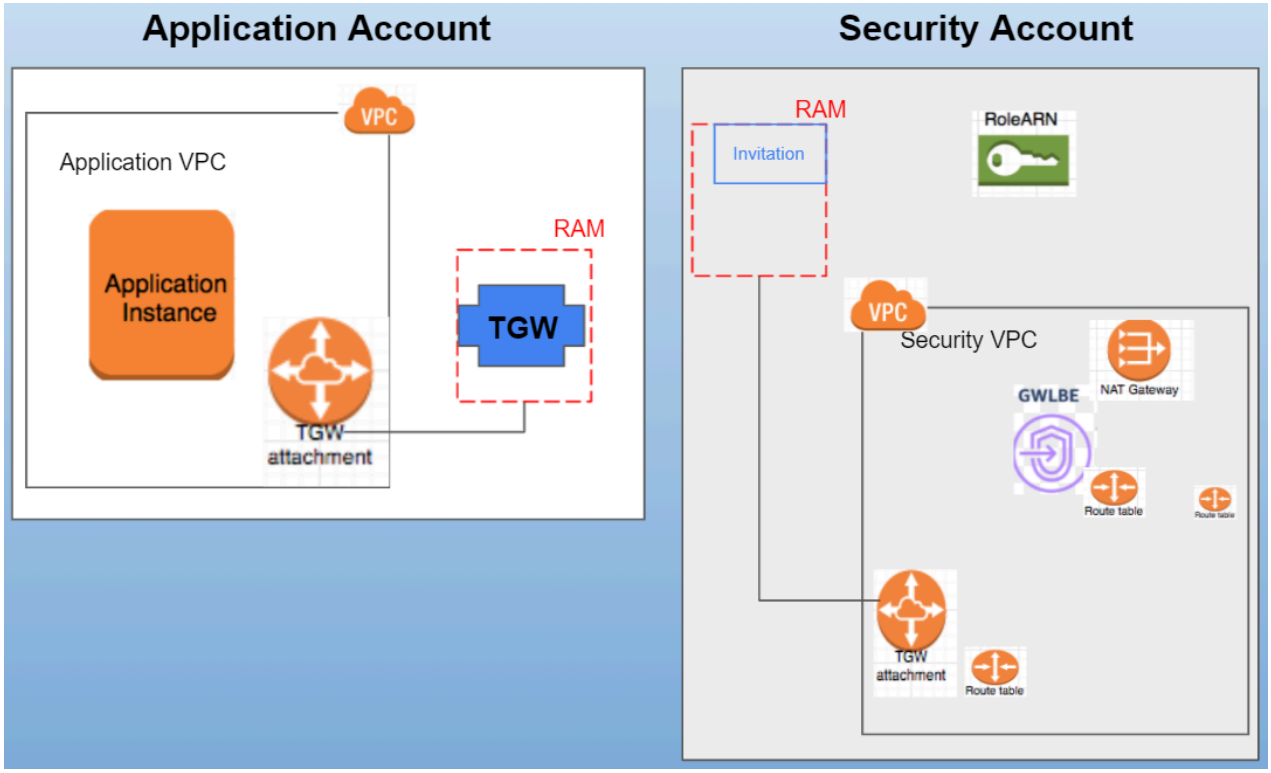


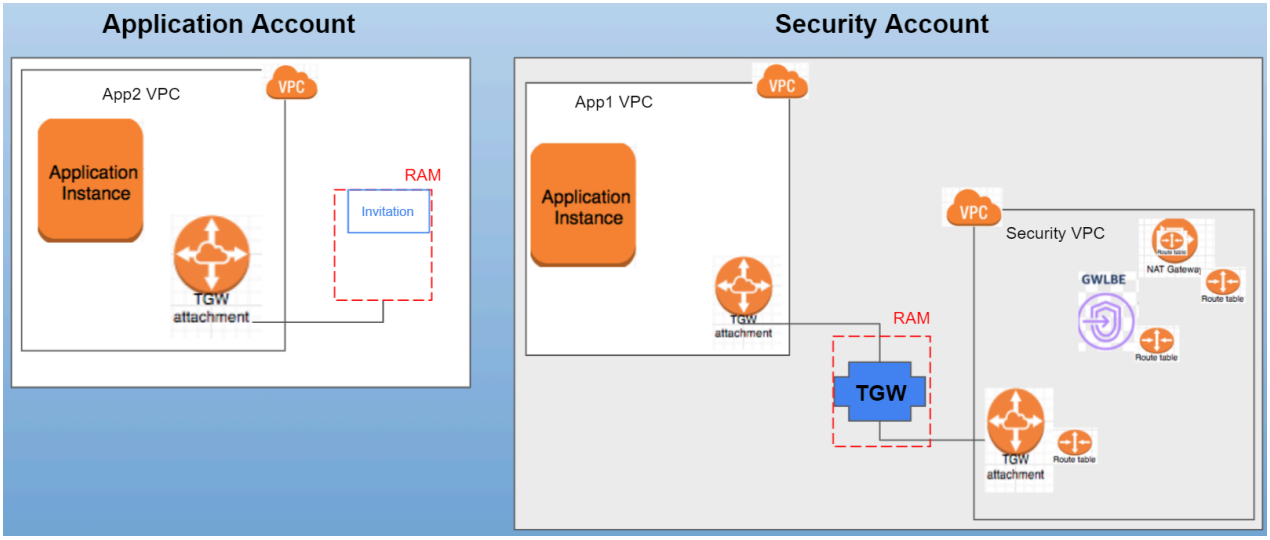
表 **4:** 东向西流量组合

	中转网关	应用程序 **1**	应用程序 **2**	流量类型
1	在安全帐户中	在安全帐户中	在安全帐户中	东向西
2（多帐户应用程序）	在安全帐户中	在安全帐户中	在应用程序帐户中	东向西
3	在应用程序帐户中	在应用程序帐户中	在应用程序帐户中	跨东向西
4（多帐户应用程序）	在应用程序帐户中	在应用程序帐户中	在安全帐户中	跨东向西

用例：东向西流量 - 中转网关和应用程序 **1** 在安全帐户中，应用程序 **2** 在安全帐户中

©2024 Palo Alto Networks, Inc.

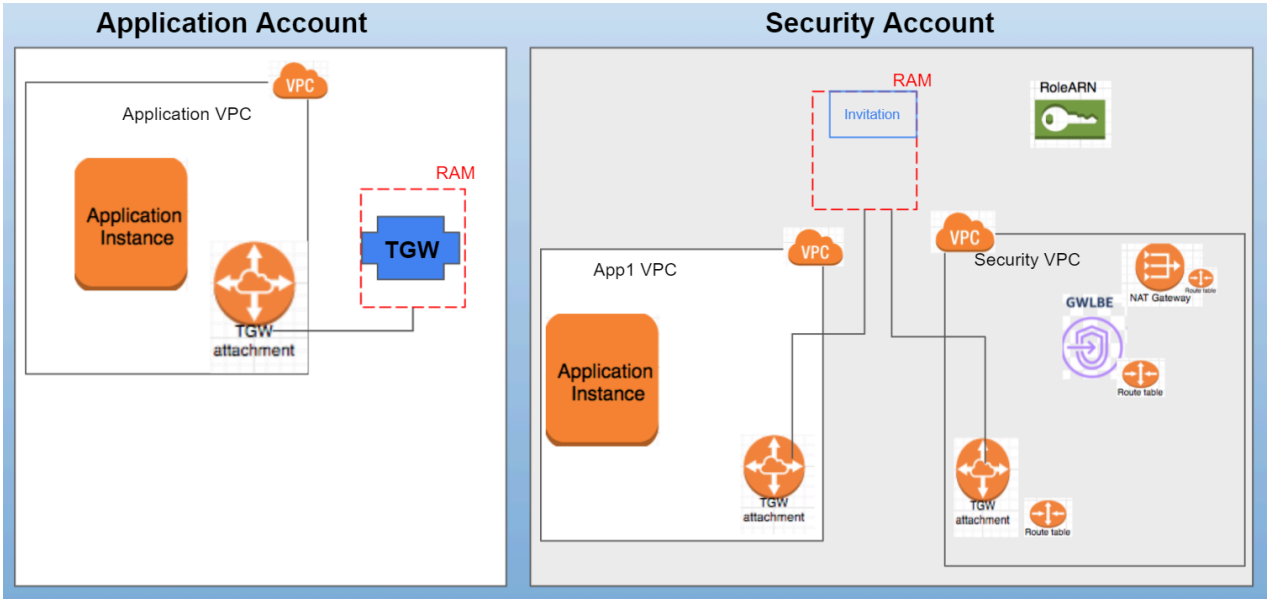
如果 TGW 位于安全帐户中，为了保护不在安全帐户中的应用程序，将在 AWS 控制台中使用资源访问管理器 (RAM) 在这些应用程序之间共享 TGW。您可以从插件用户界面中选择要与其共享 TGW 的帐户。当部署处于 **Deploying**（正在部署）状态时，监控应用程序帐户上的 RAM 以获取共享资源的邀请。



用例：东向西流量 - 中转网关和应用程序 **1** 在应用程序帐户中，应用程序 **2** 在安全帐户中

如果 TGW 是应用程序帐户，则必须使用 RAM 将其与安全帐户共享。要创建 TGW 附件和路由表，必须将此帐户的 ROLearn 添加到用于此部署的 IAM 中。使用 设置 > 应用程序帐户 下的 CFT 超链接来配置应用程序帐户先决条件。

©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

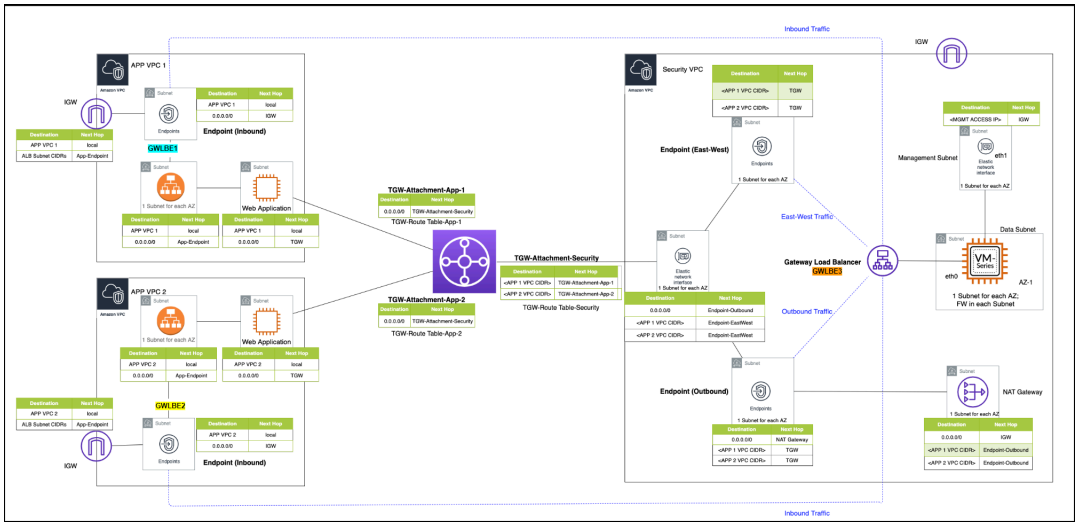
VM 系列与 AWS 网关负载均衡器集成

AWS 网关负载均衡器 (GWLB) 是一项 AWS 托管服务，用于部署一堆 VM 系列防火墙，并以水平可扩展和容错的方式运行。然后，您可以将带有防火墙堆栈的 AWS GWLB 作为 VPC 端点服务公开，以进行流量检查和威胁保护。通过为 VPC 端点服务创建网关负载均衡器端点 (GWLBE)，您可以轻松地在应用程序的出站、东向西和入站流量路径中插入自动扩展 VM 系列防火墙堆栈。VM 系列防火墙和 GWLB 使用 GENEVE 封装保持流量数据包标头和负载完整，从而为应用程序提供源身份的完整可见性。

VM 系列防火墙在 *GWLB* 后面部署时支持解密，用于转发和入站用例，包括使用 *DHE/ECDHE* 密码的 *TLS1.2* 和 *TLS1.3*。

在 *GWLB* 后面部署 *VM* 系列防火墙需要配置 AWS 中转网关。

下图介绍 GWLB 与 VM 系列的集成如何简化了 AWS 中转网关 (TGW) 环境。您可以将集中式安全 VPC 附加到中转网关。集中式安全 VPC 包括用于在 VM 系列防火墙之间扩展和均衡负载流量的 GWLB。



要确保 VM 系列防火墙可以检查在 VPC 附件之间路由的流量，您必须在中转网关 VPC 附件上为包含 VM 系列防火墙的安全 VPC 启用设备模式。您可以使用以下命令启用装置模式：

```
modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 <value> --options ApplianceModeSupport=enable
```

有关更多说明，请参阅启用设备模式。

这可确保对称路由双向流量 — 将请求和响应流量定向到防火墙 VPC 中的同一网关端点，并且 GWLB 将一致保持对同一 VM 系列防火墙进行检查，然后将流量继续路由到正确的目标。

与 GWLB 一起部署时，您可以使用 VM 系列防火墙来保护：

©2024 Palo Alto Networks, Inc.

- 入站流量 — 来自 VPC 外部并前往应用程序 VPC 中资源的流量，例如 Web 服务器。VM 系列防火墙可防止恶意软件和漏洞以 AWS 安全组允许的流量进入网络。
- 出站流量 — 来自应用程序内并前往 Internet 上外部资源的流量。VM 系列防火墙可通过确保将应用程序 VPC 中的工作负载连接到允许的服务（例如 Windows Update）和允许的 URL 类别，并防止敏感信息的数据泄露来保护出站流量。此外，VM 系列安全配置文件可防止恶意软件和漏洞以返回流量进入网络。
- 东向西流量 — 在中转网关环境中，东向西流量是指 VPC 之间的流量，例如两个不同应用程序 VPC 中源和目标工作负载之间的流量。VM 系列防火墙可保护东向西流量，以防止恶意软件传播。

要保护应用程序 VPC 的入站流量，请执行以下操作：

1. 创建在分支 VPC 中关联了单独子网的 GWLBE 终端节点（上图中的 GWLBE1 和 GWLBE2）。确保在应用程序 VPC 中具有用于 GWLB 终端节点、ALB 以及应用程序和中转网关附件的单独子网。
2. 在应用程序 VPC 中添加路由表（除 VPC 本地路由外），如下所示：
    1. 具有 IGW 边缘关联的路由表 - 添加指定为 ALB 且目标为 GWLBE 的路由。
    2. 具有 ALB 子网关联的路由表 - 添加指定为 0.0.0.0/0 且目标为 GWLBE 的路由。
    3. 具有 GWLBE 子网关联的路由表 - 添加指定为 0.0.0.0/0 且目标为 IGW 的路由。

添加这些路由后，到达 VPC IGW 的入站流量将路由到 GWLBE。GWLBE 将流量转发到 GWLB，后者又将流量发送到安全 VPC 中的 VM 系列防火墙，以便进行检查。防火墙将请求流量发送回应用程序 VPC GWLBE，然后通过 ALB 将流量转发到应用程序。此请求的响应流量由 ALB 发送到应用程序 GWLBE，接着，应用程序 GWLBE 将流量发送到 GWLB。GWLB 依次将流量发送到 VM 系列防火墙。检查响应流量后，防火墙将响应流量发送回应用程序 GWLBE，后者又将流量发送到 IGW。

要保护应用程序 VPC 的出站流量，请执行以下操作：

1. 在集中式防火墙 VPC 中创建一个 GWLBE（上图中的 GWLBE3）。确保在安全 VPC 中具有用于 GWLB 终端节点、中转网关附件、NAT 网关的单独子网。
2. 在安全 VPC 中创建 NAT 网关。

©2024 Palo Alto Networks, Inc.

3. 按如下方式添加路由表：
   1. 具有应用程序子网关联的路由表 - 添加指定为 0.0.0.0/0 且目标为 TGW 的路由。这是对 VPC 本地路由的补充。
   2. VPC 中的路由表：
      - 具有 TGW 连接子网关联的路由表 - 除 VPC 本地路由外，还要添加指定为 0.0.0.0/0 且目标为 GWLBE3 的路由。
      - 具有 GWLBE 子网关联的路由表 - 除 VPC 本地路由外，还要添加指定为 0.0.0.0/0 且目标为 NAT 网关的路由。添加指定为 TGW 的应用程序 VPC CIDR 的路由。
      - 具有 NAT 网关子网关联的路由表 - 除 VPC 本地路由外，还要添加指定为 0.0.0.0/0 且目标为 IGW 的路由。添加目标为 GWLBE3 的应用程序 VPC CIDR 的路由。
   3. 添加中转网关路由表，如下所示：
      - 具有 App1-1 VPC TGW-附件关联的路由表 - 将具有附件 ID 的指定为 0.0.0.0/0 的网关添加为安全 VPC TGW 附件。
      - 具有 App2-2 VPC TGW-附件关联的路由表 - 将具有附件 ID 且指定为 0.0.0.0/0 的网关添加为安全 VPC TGW 附件。
      - 具有安全 VPC TGW-附件关联的路由表 - (a) 将具有附件 ID 且指定为 App-1 VPC CIDR 的网关添加为 Application-1 VPC TGW 附件。(b) 将具有附件 ID 且指定为 App-2 VPC CIDR 的网关添加为 Application-2 VPC TGW 附件。

   完成此配置后，从应用程序 (App1) 发起的出站流量将发送到 TGW，而 TGW 会将其转发到安全 VPC 子网。接着，将流量路由到安全 GWLBE (GWLBE3)，后者会将流量发送到 VM 系列防火墙，以便通过 GWLB 进行检查。检查后，VM 系列防火墙将流量发送回 GWLBE3，GWLBE3 将流量转发到 NAT 网关，而 NAT 网关则通过 IGW 发送流量。同样，响应流量通过 NAT 网关传递到 GWLBE3、VM 系列防火墙和 TGW，然后将其路由回应用程序。

   东西向流量也按上述步骤中所述的路由和配置进行管理。当流量从 App1 发送到 App2 时，流量通过 TGW 传递，而 TGW 会将流量路由到 GWLBE3。GWLBE3 通过 GWLB 将流量转发到 VM 系列防火墙。检查后，VM 系列防火墙将数据包发送回 GWLBE3。然后，GWLBE3 通过 TGW 将数据包转发到 App2。从 App-2 到 App-1 的响应流量将按照相反的路径传送。

   建议将所有子网放在同一个可用性区域中，以免产生跨可用性区域的流量费用。

手动将 VM 系列与负载均衡器集成

请参阅以下主题，以手动将 VM 系列防火墙与 AWS 网关负载均衡器集成。

- 启用 VM 系列与 AWS 网关负载均衡器集成
- 手动将 VM 系列与负载均衡器集成
- （可选）将 VPC 端点与 VM 系列接口关联
- （可选）在 AWS 上为 VM 系列启用覆盖路由

©2024 Palo Alto Networks, Inc.

启用 VM 系列与 AWS 网关负载均衡器集成

将 VM 系列防火墙与 GWLB 集成后，首先必须启用 VM 系列防火墙以正确处理由 GWLB 端点重定向到防火墙的流量。您可以使用 VM 系列防火墙 CLI，通过 VM 系列引导数据包或 AWS 控制台中的用户数据字段启用此功能。

使用 GWLB 部署 VM 系列防火墙要求：

- PAN-OS 10.0.2 或更高版本
- VM 系列插件 2.0.2 或更高版本
- Panorama 10.0.2 或更高版本（如果使用 Panorama 管理防火墙）

下表列出了使用 VPC 端点启用 GWLB 流量检查所需的命令。可以在引导 init-cfg.txt 文件或 AWS 控制台的用户数据字段中使用这些操作命令。

引导参数	CLI 命令	说明
op-command-modes=mgmt-interface-swap	op-command-modes=mgmt-interface-swap 此命令要求重新启动防火墙才能生效。	交换 eth0 和 eth1。默认情况下，GWLB 仅将流量发送到其目标实例的 Eth0。通过交换，Eth0 会变成数据接口，而 eth1 则会变成管理接口。
plugin-op-commands=aws-gwlb-inspect:enable	request plugins vm_series aws gwlb inspect enable <yes/no>	启用 VM 系列防火墙以处理通过 GWLB 的流量。

手动将 VM 系列与负载均衡器集成

完成以下过程，以手动将 AWS 上的 VM 系列防火墙与 GWLB 集成。

如果在引导时通过用户数据将 *VPC* 端点关联到接口或子接口，并且 *bootstrap.xml* 文件不包含接口配置，则可以在防火墙启动后配置接口。

STEP 1 | 设置安全 VPC。有关创建安全 VPC 的更多信息，请参阅 AWS 文档。

- 创建两个子网 — 一个用于管理，另一个用于数据。
- 创建两个安全组 — 一个用于防火墙管理，另一个用于数据。
- 管理子网安全组应允许 HTTPS 和 SSH 进行管理访问。
- 确保数据 VPC 中的安全组允许 GENEVE 封装数据包（UDP 端口 6081）。
- 如果您的部署包括中转网关和将在 VPC 之间移动的流量，则必须在安全 VPC 附件上启用设备模式。

GWLB 的目标组无法使用 *HTTP* 进行运行状况检查，因为 *VM* 系列防火墙不允许使用不安全的协议进行访问，而是使用其他协议，例如 *HTTPS* 或 *TCP*。

©2024 Palo Alto Networks, Inc.

STEP 2 | 启动 VM 系列防火墙。

1. 在 EC2 仪表盘上，单击 **Launch Instance**（启动实例）。
2. 选择 Palo Alto VM 系列 AMI。要获得 AMI，请参阅获得 AMI。
3. 在 EC2 实例上启动 VM 系列防火墙。
   1. 对于防火墙所需的资源分配，请选择 **EC2 instance type**（**EC2** 实例类型），然后单击 **Next**（下一步）。有关资源要求，请参阅 VM 系列系统要求。
   2. 选择安全 VPC。
   3. 选择要附加到 eth0 的数据子网。
   4. 接口交换后，为 eth1 添加另一个网络接口充当管理接口。交换接口至少需要两个 ENI（eth0 和 eth1）。
      - 展开“网络接口”部分，然后单击 **Add Device**（添加设备）以添加另一个网络接口，并将管理子网配置到此接口。

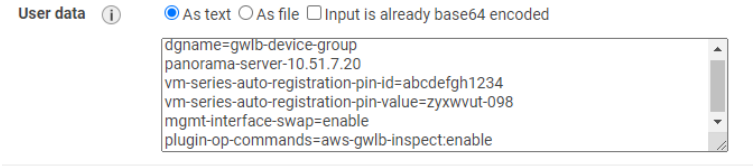
        确保 VPC 具备一个以上的子网，以便在启动时可添加其他 ENI。

        如果仅使用一个 *ENI* 启动防火墙：
        - 接口交换命令将使防火墙启动进入维护模式。
        - 添加第二个 *ENI* 时，必须重新启动防火墙。
      - 展开 Advanced Details（高级详细信息）部分，然后在 **User data**（用户数据）字段中输入作为启动期间执行接口交换的文本。

        `mgmt-interface-swap=enable`

        `plugin-op-commands=aws-gwlb-inspect:enable`

        如果您将目标类型设置为 *VM* 系列防火墙上特定接口的 *IP* 地址，则无需启用管理接口交换。

   5. 接受默认 **Storage**（存储）设置。该防火墙使用卷类型 SSD (gp2)。
   6. 如果出现提示，选择设置的相应 **SSD** 选项。
   7. （可选）**Tagging**（标记）。添加一个或多个标记来创建您自己的元数据，用以识别 VM 系列防火墙并对其进行分组。例如，添加带 **Value**（值）的 **Name**（名称）标记可帮助您记忆已交换到此 VM 系列防火墙的 ENI 接口。
   8. 为 eth0（数据接口）选择数据 **Security Group**（安全组）。在 UDP 端口 6081 上启用流量。

      如果启用对防火墙的运行状况检查，则无法使用 HTTP。而是使用其他协议，例如 HTTPS 或 TCP。

©2024 Palo Alto Networks, Inc.

9. 选择 **Review and Launch**（查看并启动）。查看您的选择是否正确，然后单击 **Launch**（启动）。
10. 选择现有的密钥对或创建新的密钥对，并确认密钥免责声明。

    第一次访问防火墙需要使用此密钥对。同样，在维护模式下访问防火墙也需要使用此密钥对。
11. 下载并将私钥保存到安全位置；文件扩展名为 `.pem`。如果丢失，则将无法重新生成此密钥。

    启动 VM 系列防火墙需要 5 至 7 分钟。您可以在 EC2 仪表盘上查看进程。进程完成后，VM 系列防火墙将会显示在 EC2 仪表盘的 **Instances**（实例）页面上。

STEP 3 | 将管理安全组附加到 eth1（管理接口）。允许 SSH 和 HTTPS。有关更多信息，请参阅 AWS 文档。

STEP 4 | 创建弹性 IP 地址 (EIP) 并将其分配给用于对防火墙进行管理访问 (eth1) 的 ENI。

1. 选择 **Elastic IPs**（弹性 **IP**），并单击 **Allocate New Address**（分配新地址）。
2. 选择 **EC2-VPC**，并单击 **Yes, Allocate**（是，分配）。
3. 选择新分配的 EIP，并单击 **Associate Address**（关联地址）。
4. 选择 **Network Interface**（网络接口）和与之相关联的 **Private IP address**（专用 **IP** 地址），然后单击 **Yes, Associate**（是，关联）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 配置防火墙的新管理密码。

在 *VM* 系列防火墙 *CLI* 上，您必须先配置唯一的管理密码，然后才能访问防火墙的 *Web* 界面。要登录到 *CLI*，您需要可用于启动防火墙的私钥。

1. 使用 EIP 通过 SSH 访问 VM 系列防火墙的命令行界面 (CLI)。您将需要在上面使用或创建的私钥，并使用用户名 **admin**（管理员）访问 CLI。

   如果您正在使用 PuTTY 访问 SSH，则您必须将 .pem 格式转换为 .ppk 格式。参阅 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

2. 输入以下命令以登录到防火墙：

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*

3. 使用以下命令并按照屏幕上的提示配置新密码：

   配置

   set mgt-config users admin password

4. 如果存在需激活的 BYOL，请对 DNS 服务器的 IP 地址进行设置，以使防火墙可访问 Palo Alto Networks 许可服务器。输入以下命令，设置 DNS 服务器的 IP 地址：

   set deviceconfig system dns-setting servers primary *<ip_address>*

5. 使用以下命令提交您所做的更改：

   commit

6. 终止 SSH 会话。

©2024 Palo Alto Networks, Inc.

STEP 6 | 配置数据平面网络接口作为防火墙上的第 3 层接口。

在 *VPC* 内的应用服务器上，定义防火墙的数据面板网络接口作为默认网关。

1. 在 Web 浏览器中使用安全连接 (https)，通过初始配置期间分配的 EIP 地址和密码登录 (https://<Elastic_IP address>)。您将看到证书警告；这属于正常情况。继续浏览网页。
2. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
3. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认虚拟路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义一个新区域，并将其余字段保留为默认值，然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **DHCP Client**（**DHCP** 客户端）。

     如果使用 DHCP，选择 **DHCP Client**（**DHCP** 客户端）；将会自动获取在 AWS 管理控制台上分配给 ENI 的专用 IP 地址。
   - 在“高级”选项卡上，创建管理配置文件以在创建管理配置文件的过程中启用 HTTP 服务，并允许来自 GWLB 的运行状况检查探测。
   - （可选）在 IPv6 选项卡上，选择**Enable IPv6 on this Interface**（在此接口上启用 **IPv6**），然后选择 **DHCPv6 Client**（**DHCPv6** 客户端）。

     作为 *AWS Dualstack* 的一部分，*GWLB* 后适用于 *AWS* 的 *VM* 系列仅支持 *IPv6*，这意味着客户端使用 *IPv4* 和 *IPv6* 地址与负载均衡器通信。不支持 *IPv6*。

     此外，必须创建允许 *IPv6* 流量的安全策略。
4. 单击 **Commit**（提交）。验证此接口的链接状态是否正常。

STEP 7 | 创建安全策略以允许/拒绝流量。

由于 *VM* 系列在与 *GWLB* 集成时将流量视为区域内流量，因此默认的区域内规则将允许所有流量。对于与任何其他安全策略规则不匹配的流量，最佳做法是利用拒绝操作覆盖默认的区域内规则。

1. 在防火墙的 Web 界面上选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），然后指定要执行限制的安全区域、应用程序和日志记录选项，并审核遍历网络的流量。

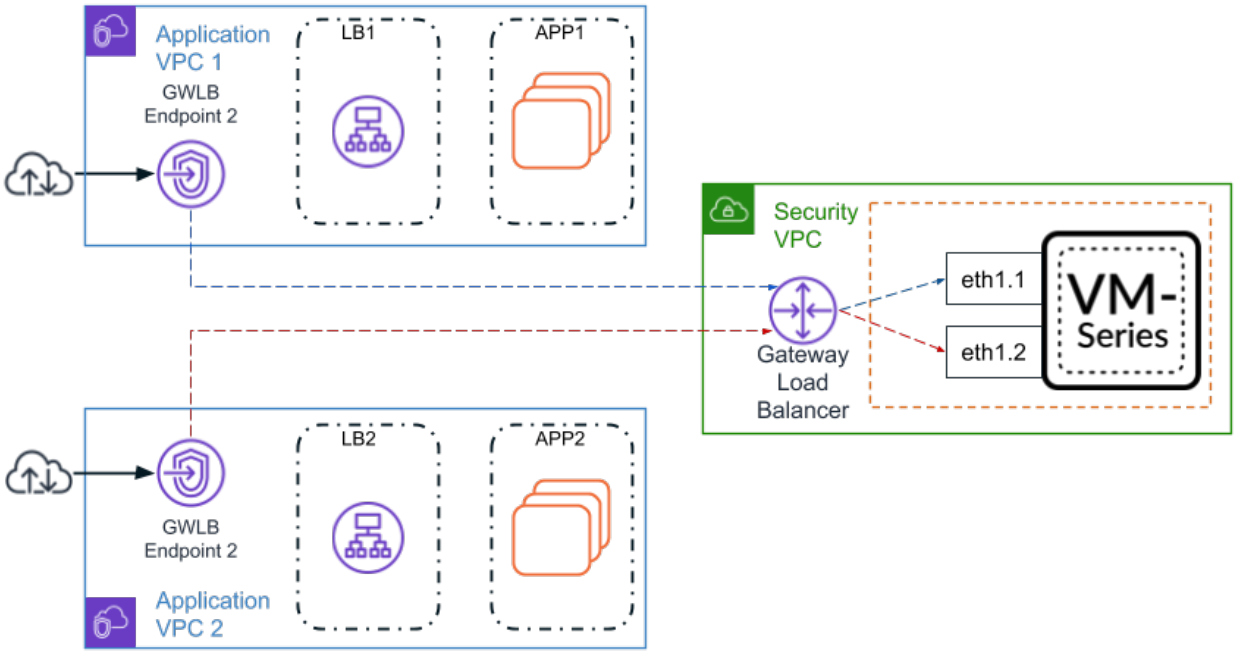
STEP 8 | 在防火墙上 **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

将 VPC 端点与 VM 系列接口关联

您可以将一个或多个 VPC 端点与 VM 系列防火墙的接口或子接口关联。您可以通过将单个 VPC 中的所有端口关联到防火墙上的同一子接口来提供一致的策略实施。或者，如果部署中的 VPC 具有重叠的 IP 地址，则可以将不同 VPC 中的端点与不同子接口关联以区分策略实施。

要将 *VM* 系列防火墙与 *GWLB* 集成，不需要将 *VPC* 端点与接口或子接口关联。



您可以使用以下方法配置接口并将 VPC 与防火墙接口关联：

- 将接口配置包含在 `bootstrap.xml` 文件中，并将关联命令作为 `init-cfg.txt` 文件或 AWS 用户数据的一部分。
- 部署防火墙后，手动配置接口，并使用防火墙 CLI 将 VPC 与接口关联。

您可以将多个 VPC 端口关联到 VM 系列防火墙上的单个接口。但是，您必须分别关联每个 VPC 端点。例如，要将 VPC 端点 1 和 VPC 端点 2 与子接口 ethernet1/1.2 关联，必须为每个 VPC 端点分别执行关联命令。

下表介绍了用于将 VPC 端点与接口关联的命令。您可以在 `init-cfg.txt` 文件或 AWS 用户数据中包含该操作命令。

引导参数	CLI 命令	说明
plugin-op-commands= aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>	request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>	将 VPC 端点与防火墙上的接口或子接口关联。已将指定接口分配给安全区域。

©2024 Palo Alto Networks, Inc.

引导参数	CLI 命令	说明
—	request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>	解除 VPC 端点与防火墙上接口或子接口的关联。已将指定接口分配给安全区域。
—	show plugins vm_series aws gwlb	显示与 GWLB 部署相关的防火墙的操作状态。它不显示防火墙配置。 例如，如果您配置与不存在的接口关联，则该关联已配置，但不是操作状态的一部分。因此，它不会显示。

当使用引导 init-cfg.txt 文件或 AWS 用户数据关联 VPC 端点时，您可以一起列出多个接口或子接口。所有命令都必须在以逗号分隔的列表中的一行中，且不能有空格，如下例所示。

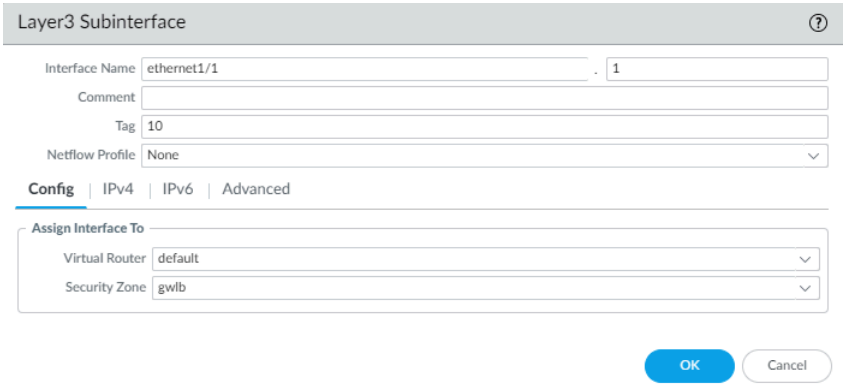
```
plugin-op-commands=aws-gwlb-inspect:enable,aws-gwlb-associate-
vpce:vpce-0913731043b5c0ebc@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-08207ccb4cb23a1de@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-07b66cca88821d6e1@ethernet1/1.2,aws-gwlb-associate-
vpce:vpce-0a9a583fdb928492b@ethernet1/1.3
```

如果使用子接口来隔离流量，请为每个 VPC 端点创建一个子接口并将其与 VPC 端点关联。

©2024 Palo Alto Networks, Inc.

STEP 1 | 配置子接口。

1. 登录到防火墙 Web 界面。
2. 选择 **Network**（网络）> **Interface**（接口）。
3. 突出显示 **ethernet1/1**，然后单击 **Add Subinterface**（添加子接口）。
4. 输入数字后缀（1 至 9,999）以标识子接口。
5. 输入该子接口的 **VLAN** 标记（1 至 4,094）。该字段为必填字段，但未使用 VLAN。
6. 选择 **Virtual Router**（虚拟路由器）作为默认设置。
7. 选择 **Security Zone**（安全区域）。
8. 在 **IPv4** 选项卡上，将 **Type**（类型）设置为 **DHCP Client**（**DHCP** 客户端）。
9. 单击 **OK**（确定）。
10. 对于每个 VPC 端点，请重复执行此命令。



STEP 2 | 将接口与 VPC 端点关联。

1. 登录至防火墙 CLI。
2. 执行以下命令：

   request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>

   例如：

   request plugins vm_series aws gwlb associate vpc-endpoint vpce-02c4e6g8ha97h7e39 interface ethernet1/1.4

   您可以在 *AWS* 控制台中找到 *VPC* 端点 *ID*。

3. 对于每个接口和 VPC 端点关联，请重复执行此命令。

STEP 3 | 验证与 VPC 端点关联的接口。

show plugins vm_series aws gwlb

```
GWLB enabled:True Overlay Routing:False
 ------------------------------------------------------------ VPC
```

 ©2024 Palo Alto Networks, Inc.

```
endpoint Interface
------------------------------------------------------------------
vpce-0aeb1a919bd4ae609 ethernet1/1.1 vpce-0294375bfe413f04a
ethernet1/1.2
```

STEP 4 | 如果需要，您可以使用以下命令解除 VPC 端点与接口的关联。

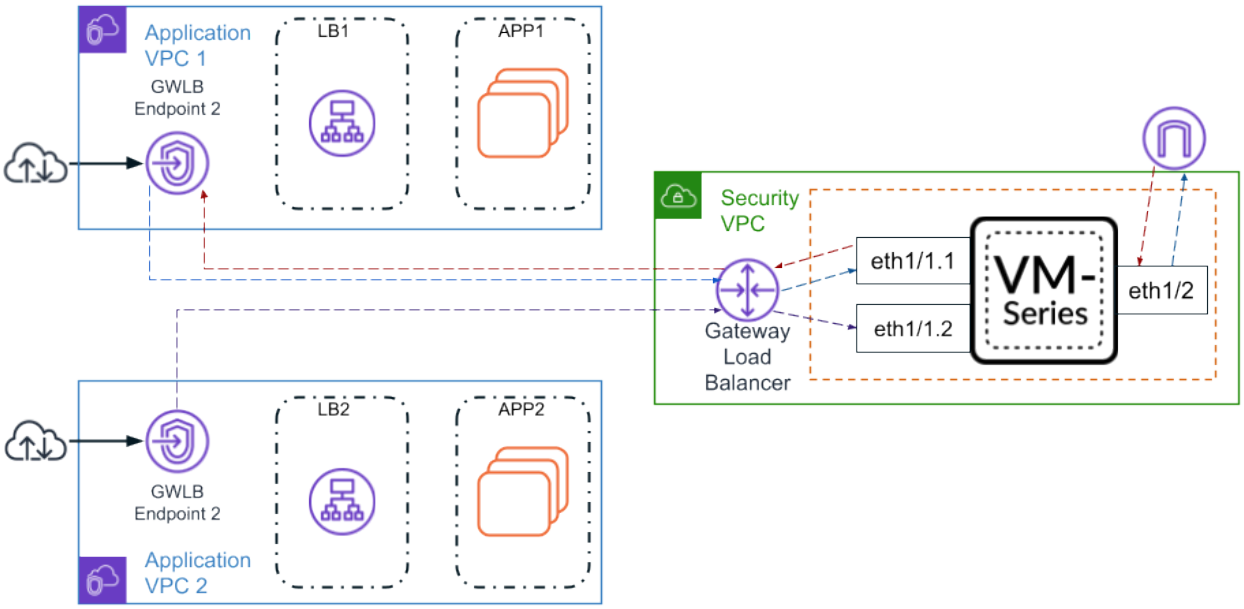
```
request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-
id> interface <subinterface>
```

在 AWS 上为 VM 系列启用覆盖路由

覆盖路由需要 *PAN-OS 10.0.5* 或更高版本。

在 VM 系列防火墙集成中使用覆盖路由，AWS GWLB 允许您使用双区域策略来检查离开（传出）AWS 环境的流量。这允许数据包通过与其进入时不同的接口离开 VM 系列防火墙。

配置覆盖路由后，防火墙能够执行第 3 层路由查找数据包的内部标头。如果目标与入口接口相同，则正常定向数据包。将会话中的所有未来数据包视为 vwire；好像未启用覆盖路由。如果将数据包定向到出站目标，则防火墙会解封装数据包，并将数据包转发到 IGW 或 NAT 网关。当数据包返回时，防火墙重新应用封装。



使用以下过程启用覆盖路由。

STEP 1 | 在开始之前，请确保为可信和不可信接口创建不同的子网。

STEP 2 | 手动将 VM 系列与负载均衡器集成.

©2024 Palo Alto Networks, Inc.

STEP 3 | （可选）将 VPC 端点与 VM 系列接口关联。

STEP 4 | 使用覆盖路由 CLI 命令。如果您在 AWS user-data 或 init-cfg.txt 引导文件中包含覆盖路由 Op 命令，则不需要此 CLI 命令。

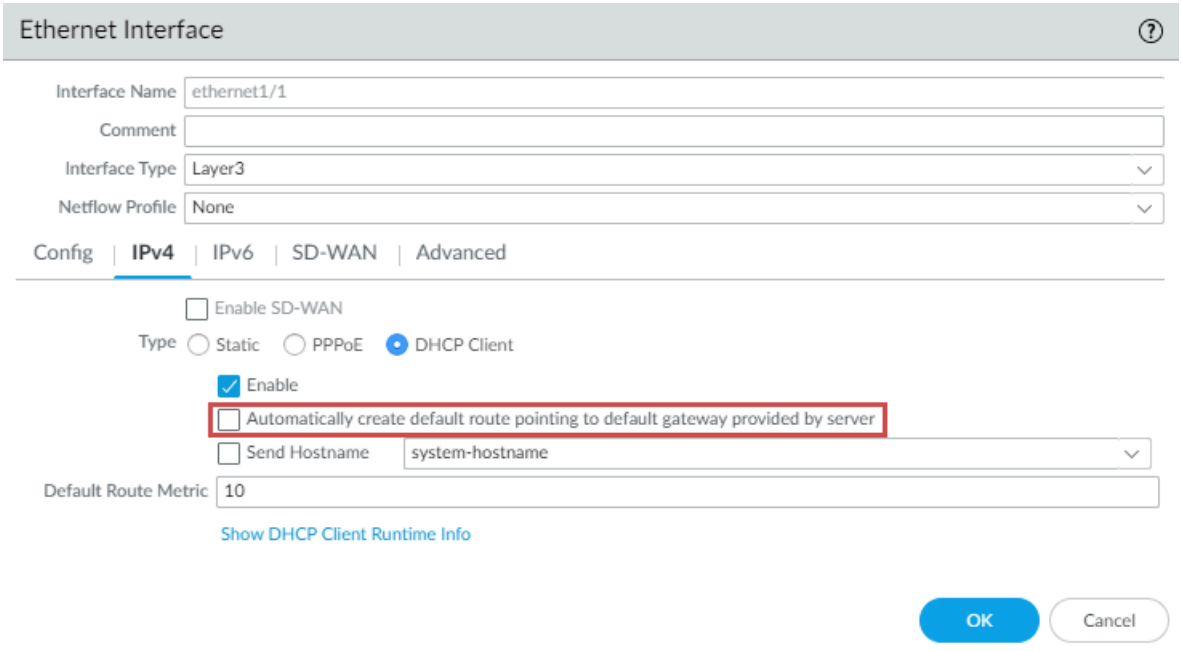
1. 登录防火墙命令行界面。
2. 执行以下命令。

```
request plugins vm_series aws gwlb overlay-routing enable yes
```

STEP 5 | 登录到防火墙 Web 界面。

STEP 6 | 在可信（入口）接口上禁用 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器提供的默认网关的默认路由）。

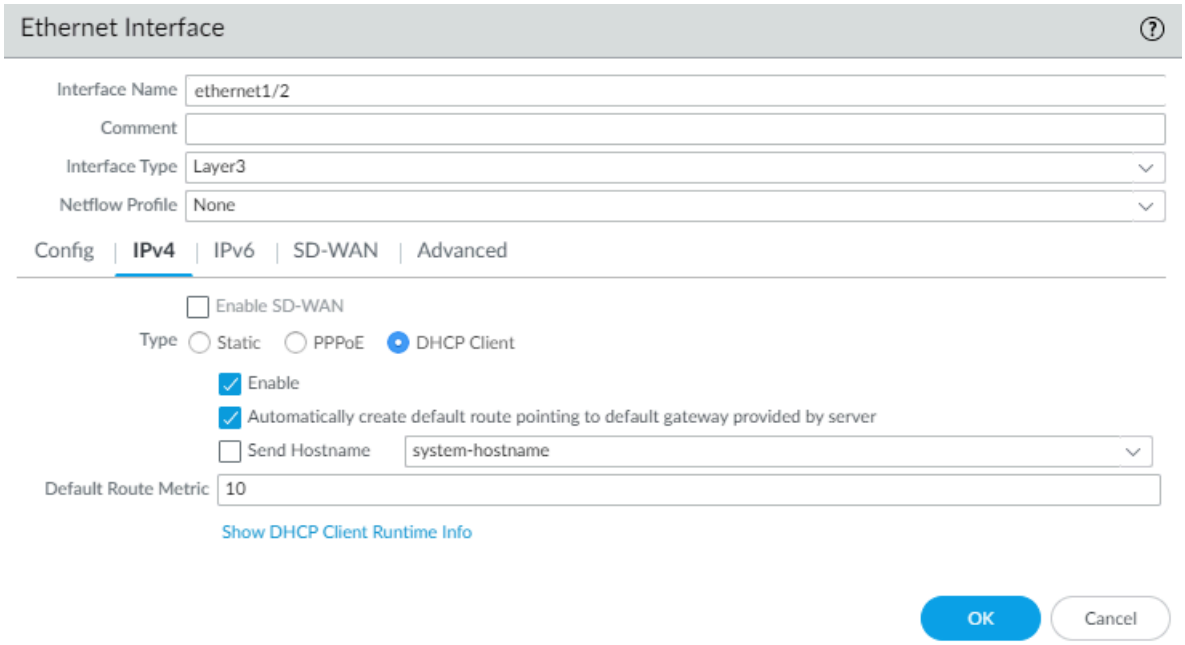
1. 选择 **Network**（网络 ） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 单击可信接口，然后单击 IPv4 选项卡。
3. 取消选择 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器提供的默认网关的默认路由）。
4. 单击 OK（确定）。



©2024 Palo Alto Networks, Inc.

STEP 7 | 配置接口 Ethernet1/2。

1. 选择 **Network**（网络 ）> **Interfaces**（接口）> **Ethernet**（以太网）。
2. 选择 **Interface Type**（接口类型）— **Layer 3**（第 **3** 层）。
3. 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。此区域将充当不可信区域，并将出站流量定向到安全 VPC 之外。定义新区域，例如 VM-Series-untrust，然后单击 **OK**（确定）。
4. 在 **IPv4** 选项卡上，选择 **DHCP Client**（**DHCP** 客户端）。
5. 选择 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器提供的默认网关的默认路由）。
6. 单击 **OK**（确定）。



 ©2024 Palo Alto Networks, Inc.

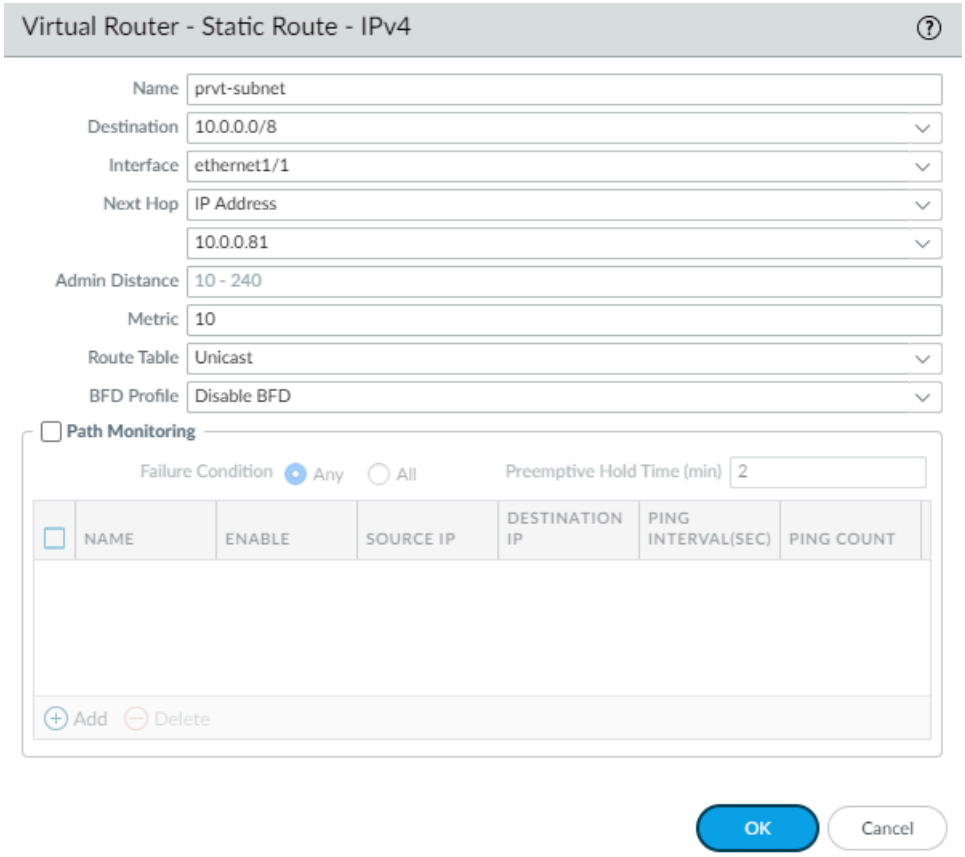
STEP 8 | 配置虚拟路由器。

1. 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器） > **Add**（添加）。
2. 输入虚拟路由器的描述性 **Name**（名称）。
3. 在 **Interfaces**（接口）下，**Add**（添加）Ethernet1/1、Ethernet1/1 下的任何子接口和 Ethernet1/2。
4. 单击 **Static Routes**（静态路由） > **Add**（添加）。
   1. 输入静态路由的描述性名称。
   2. 作为 **Destination**（目标），输入应用程序 VPC 子网的专用 IP 地址。
   3. 从 **Interface**（接口）下拉列表中选择可信（入口）接口。
   4. 对于 **Next Hop**（下一个跃点），选择 IP Address（IP 地址），然后输入可信接口的网关 IP 地址。您可以在 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网） > **Dynamic-DHCP Client**（动态 **DHCP** 客户端）上找到网关 IP 地址。



   5. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.



5. 确保静态路由可以访问部署中的所有应用程序 VPC。您可以创建一些大型聚合路由（涵盖所有 RFC1918）或应用程序 VPC 特定路由。如果您使用子接口，则无需路由回子接口。出口检查仅查找匹配的接口而不是匹配的子接口。
6. 单击 **OK**（确定）。

STEP 9 | 为出站 Ethernet1/2 的流量创建 NAT 策略。

1. 选择 **Policies**（策略） > **NAT** > **Add**（添加）。
2. 输入 NAT 策略规则的描述性 **Name**（名称）。
3. 从 **NAT Type**（**NAT** 类型）下拉列表中选择 **ipv4**。
4. 在 **Original Packet**（原始数据包）选项卡，将 **Source Zone**（源区域）设置为任何，并将 **Destination Zone**（目标区域）设置为不可信（出口）区域。
5. 在 **Translated Packet**（已转换数据包）选项卡上，设置以下参数。
   - 转换类型：动态 IP 和端口
   - 地址类型：接口地址
   - 接口：从下拉列表中选择不可信（出口）端口。
   - IP 地址：None
6. 单击 **OK**（确定）。

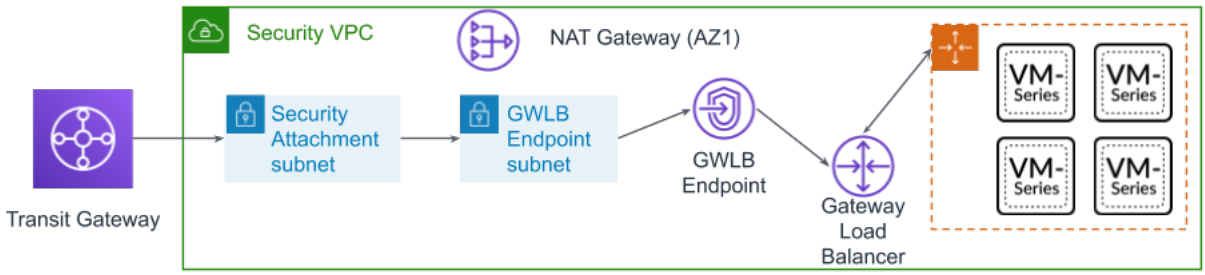
©2024 Palo Alto Networks, Inc.

STEP 10 | **Commit**（提交）更改。

VM 系列自动扩展组与 AWS 网关负载均衡器

Palo Alto Networks 自动扩展适用于 AWS 的模板可帮助您将 VM 系列防火墙与 GWLB 集成并配置，以保护在 AWS 中部署的应用程序。这些模板利用 AWS 可扩展性功能独立和自动扩展在 AWS 中部署的 VM 系列防火墙，以满足应用程序工作负载资源需求的激增。

这些模板是社区支持模板。



该解决方案提供安全 VPC 模板和应用程序模板。安全 VPC 模板可为每个可用性区域部署 VM 系列防火墙自动扩展组、GWLB、GWLBE、GWLBE 子网、安全附件子网和 NAT 网关。您可以从 Palo Alto Networks GitHub 存储库下载 CloudFormation 模板。

与 AWS GWLB 集成的 VM 系列自动扩展模板包含以下构建基块：

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

构建基块	说明
PAN 组件	• 运行版本 10.0.2 或更高版本的 Panorama • PAN-OS 10.0.2 或更高版本 • Panorama 上安装的 VM 系列插件版本 2.0.2 或更高版本
防火墙模板 （社区支持模板）	根据您选择的可用性区域 (AZ) 数，`firewall-new-vpc-v3.0.template` 可部署以下内容： 该模板最多支持四个可用性区域。 • 用于 Lambda 管理的子网、中转网关附件、GWLB 端点、NAT 网关和可信子网。 • 每个子网的路由表 • 中转网关附件和路由表

©2024 Palo Alto Networks, Inc.

构建基块	说明
	• NAT 和 Internet 网关 • 在每个可用性区域中，带一个 VM 系列防火墙的自动扩展组。 • 在每个可用性区域中，一个 GWLB 和 GWLB 端点。 防火墙模板的 VPC CIDR 应大于 /23。 由于生产环境中的诸多变化，包括但不限于特定数量的组件，例如子网、可用性区域、路由表和安全组，因此您必须在新 VPC 中部署 `firewall-new-vpc-v3.0.template`。  适用于 *AWS* 的 *VM* 系列自动扩展模板未部署中转网关或 *Panorama*。您必须先部署中转网关和 *Panorama*，然后才能启动 *firewall-new-vpc-v3.0.template*。
应用程序模板 （社区支持模板）	根据您选择的可用性区域 (AZ) 数，`panw-aws-app-v3.0.template` 可部署以下内容：  该模板最多支持四个可用性区域。 • 用于 Lambda 管理的子网、中转网关附件、GWLB 端点、应用程序负载均衡器。 • 每个子网的路由表，以及与 Internet 网关相关联以将入站流量定向到 GWLB 端点的入站路由表。 • 一个应用程序负载均衡器 • 一个 Internet 网关 • 在每个可用性区域中，带一个 Ubuntu 实例的自动扩展组。 应用程序模板的 VPC CIDR 应大于 /23。  应用程序模板旨在用作验证安全模板的示例。
Lambda 函数	AWS Lambda 提供强大的事件驱动自动化，无需复杂的编排软件。除部署上面行中所述的组件外，`firewall-new-vpc-v3.0.template` 还执行以下功能： • 在防火墙启动或终止时添加或删除接口 (ENI)。 • 在删除堆栈或终止实例时删除所有关联资源。 • 当发生缩小事件时删除作为 Panorama 托管设备的防火墙。 • 当缩小事件导致防火墙终止时停用许可证。

©2024 Palo Alto Networks, Inc.

构建基块	说明
	• 定期监控中转网关是否有新的附件或分离，并在安全 VPC 中相应更新路由表。
引导文件 GitHub 存储库中提供的 bootstrap.xml 文件仅用于测试和评估。对于生产部署，您必须在启动之前修改 bootstrap.xml 中的示例凭证。	此解决方案需要 init-cfg.txt 文件和 bootstrap.xml 文件，以便 VM 系列防火墙具有处理流量的基本配置。 • `init-cfg.txt` 文件包含 mgmt-interface-swap 操作命令，以使防火墙能够在其主接口 (eth0) 上接收数据平面流量。此自动扩展解决方案需要交换数据平面和管理界面，以使 GWLB 能够将 Web 流量转发到 VM 系列防火墙的自动扩展层。 • `bootstrap.xml` 文件为防火墙网络接口启用基本连接，并允许防火墙连接到与启动模板时输入的堆栈名称相匹配的 AWS CloudWatch 命名空间。

如果您需要从 *AWS* 删除这些模板，请始终先删除应用程序模板。尝试删除防火墙模板可能会导致删除失败。

- 启动模板之前
- 启动防火墙模板
- 启动应用程序模板

启动模板之前

在启动模板以将 VM 系列防火墙自动扩展组与 AWS GWLB 集成之前，您必须完成以下过程。

©2024 Palo Alto Networks, Inc.

STEP 1 | 开始之前，请确保您具备下列条件。

- 获取支持部署可能需要的防火墙数量的套餐的授权代码。您必须将此授权代码保存在名为 `authcodes`（无扩展名）的文本文件中，并把 `authcodes` 文件放在引导数据包的 `/license` 文件夹中。
- 从 GitHub 存储库下载启动 VM 系列网关负载均衡器模板所需的文件。
- 创建一个中转网关。该中转网关连接您的安全和应用程序 VPC。
  - 记下中转网关 ID；稍后在部署模板时将需要使用该 ID。
  - 您必须将 0.0.0.0/0 路由添加到指向安全附件的应用程序附件路由表，以保护东向西和出站流量。
  - 确保禁用 **Default route table association**（默认路由表关联）和 **Default route table propagation**（默认路由表传播）。
- 对于防火墙和应用程序模板，建议的 VPC CIDR 应大于 /23。

网关 *GWLB* 的目标组无法使用 *HTTP* 进行运行状况检查，因为 *VM* 系列防火墙不允许使用不安全的协议进行访问，而是使用 *HTTPS* 或 *TCP* 协议。

STEP 2 | 部署运行版本 10.0.2 的 Panorama，并配置以下内容。

Panorama 必须允许 AWS 公共 IP 地址。VM 系列防火墙使用模板创建的 NAT 网关的外部 IP 地址访问 Panorama。

STEP 3 | 在 Panorama 上下载并安装 VM 系列插件。

1. 选择 **Panorama** > **Plugins**（插件），然后使用 **Check Now**（立即检查）查找新的插件数据包。VM 系列插件名称为 `vm_series`。
2. 请参阅插件版本说明，以确定哪个版本提供的升级对您有用。
3. 选择插件的版本，并在 Action（操作）列中选择 **Download**（下载）。
4. 单击 Action（操作）列中的 **Install**（安装）。安装完成后，Panorama 会提醒您。
5. 要查看插件，请选择 **Device**（设备）> **VM-Series**（**VM** 系列）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 配置模板。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
   1. 输入描述性的 **Name**（名称）。
   2. 单击 **OK**（确定）。
3. 配置虚拟路由器。
   1. 选择**Network**（网络） > **Virtual Routers**（虚拟路由器）。
   2. 确保已从 **Template**（模板）下拉列表中选择您在上面创建的模板。
   3. 单击 **Add**（添加）。
   4. 使用以下格式命名虚拟路由器：VR-<tempstackname>。
   5. 在虚拟路由器上启用 ECMP。
   6. 单击 **OK**（确定）。
4. 配置接口并创建区域。
   1. 选择 **Network**（网络） > **Interfaces**（接口），然后单击 **Add Interface**（添加接口）。
   2. 选择 **Slot 1**（插槽 **1**），然后选择接口名称（例如，ethernet 1/1）。
   3. 将 **Interface Type**（接口类型）设置为第 3 层。
   4. 在 **Config**（配置）选项卡上，选择 **Security Zone**（安全区域）下拉列表中的 **New Zone**（新建区域）。在区域对话框中，定义新区域的 **Name**（名称），例如 Internet，然后单击 **OK**（确定）。
   5. 在 **Virtual Router**（虚拟路由器）下拉列表中，选择您在上面创建的虚拟路由器。
   6. 选择 **IPv4**，然后单击 **DHCP Client**（**DHCP** 客户端）。
   7. 单击 **OK**（确定）。
5. 允许管理配置文件，允许上面创建的接口上的 HTTPS 以支持运行状态检查。
   1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **Interface Mgmt**（接口管理），然后单击 **Add**（添加）。
   2. 选择接口允许管理流量的协议：**Ping**、**Telnet**、**SSH**、**HTTP**、**HTTP OCSP**、**HTTPS** 或 **SNMP**。

      请勿启用 ***HTTP***或 ***Telnet***，因为这些协议会以明文形式传输，不安全。
6. 为接口分配一个接口管理配置文件。
   1. 选择 **Network**（网络） > **Interfaces**（接口），选择接口类型（**Ethernet**（以太网）、**VLAN**、**Loopback**（回环）或 **Tunnel**（隧道）），并选择接口。
   2. 选择 **Advanced**（高级） > **Other info**（其他信息），然后选择添加的接口 **Management Profile**（管理配置文件）。
   3. 单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

7. 配置 DNS 服务器和 FQDN 刷新时间。
   1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务），然后单击 Edit（编辑）图标。
   2. 将 **Primary DNS Server**（主 **DNS** 服务器）设置为 169.254.169.253。这是 AWS DNS 地址。
   3. 将 **Minimum FQDN Refresh Time**（最短 **FQDN** 刷新时间）设置为 60 秒。
   4. 单击 **OK**（确定）。
8. **Commit**（提交）更改。必须在执行下一步之前执行此操作。
9. 创建管理员。
   1. 选择**Device**（设备） > **Administrators**（管理员）。
   2. 输入 **`pandemo`** 作为 **Name**（名称）。
   3. 将 **Password**（密码）设置为 **`demopassword`** 并 **Confirm**（确认）。
   4. 单击 **OK**（确定）。
10. **Commit**（提交）更改。

STEP 5 | 配置模板堆栈并将模板添加到模板堆栈。

1. 选择 **Panorama** > **Templates**（模板），然后 **Add Stack**（添加堆栈）。
2. 输入唯一的**Name**（名称）以标识该堆栈。
3. 单击 **Add**（添加）并选择模板。
4. 单击 **OK**（确定）以保存模板堆栈。

STEP 6 | 创建 **Device Group**（设备组）。

1. 选择 **Panorama** > **Device Groups**（设备组）。
2. 单击添加。
3. 输入描述性的 **Name**（名称）。
4. 单击 **OK**（确定）。
5. 添加允许所有安全前导规则。
   1. 确保已从 **Device Group**（设备组）下拉列表中选择您在上面创建的设备组。
   2. 选择 **Policies**（策略） > **Security**（安全） > **Pre Rules**（前导规则），然后单击 **Add**（添加）。
   3. 输入描述性的 **Name**（名称）。
   4. 在 **Source**（源）、**User**（用户）、**Destination**（目标）、**Application**（应用程序）和 **Service/URL Category**（服务/**URL** 类别）下，选择 Any（任何）。
   5. 在 **Actions**（操作）下，选择 **Allow**（允许）。
   6. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 7 | 将防火墙的许可证停用 API 密钥添加到 Panorama。

1. 登录到客户支持门户。
2. 选择 **Assets**（资产） > **API Key Management**（**API** 密钥管理）。
3. 复制 API 密钥。
4. 使用 CLI 安装在上一步中复制的 API 密钥。

   request license api-key set key *<key>*

STEP 8 | 部署 Panorama 后，您必须按以下说明在 AWS 的 Panorama 安全组上打开以下端口。

- 端口 **443 (HTTPS)** — 初始部署防火墙模板后，保持 HTTPS 开放，以便 Lambda 可以连接到 Panorama。

  保护端口 443 时，您可以指定允许连接的 IP 地址范围，以及分配给 NAT 网关的 EIP。部署中的 NAT 网关数取决于您配置的可用性区域数。要在 AWS 中查找 NAT 网关 EIP，请转到 **VPC** > **NAT Gateways**（**NAT** 网关）。请注意 HTTPS 安全组的 EIP 信息。

  此外，要允许 Panorama 在删除堆栈后释放防火墙许可证，必须允许来自部署防火墙模板的区域的 CIDR 范围的流量。您可以在此链接中找到所在区域的 CIDR 范围。
- 端口 **3978** — 端口 3978 必须能够从任何 IP 地址接收流量。

启动防火墙模板

此工作流程介绍了如何部署防火墙模板。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 修改 `init-cfg.txt` 文件并将其上传到 `/config` 文件夹。

由于您使用 Panorama 来引导 VM 系列防火墙，所以，您的 `init-cfg.txt` 文件需要按如下修改。不需要 `bootstrap.xml` 文件。

确保使用上面在 init-cfg.txt 文件中创建的设备组和模板名称。

```
type=dhcp-client ip-address= default-gateway= netmask=
 ipv6-address= ipv6-default-gateway= hostname= vm-auth-key=
 panorama-server= panorama-server-2= tplname= dgname= dhcp-
send-hostname=yes dhcp-send-client-id=yes dhcp-accept-server-
hostname=yesdhcp-accept-server-domain=yes plugin-op-commands=aws-
gwlb-inspect:enable
```

Your init-cfg.txt file must include **`plugin-op-commands=aws-gwlb-inspect:enable`**。将 VM 系列防火墙与 GWLB 集成时，这是必需的。

您必须将设备证书自动注册 PIN 添加到 init-cfg.txt 文件，才能在部署 VM 系列防火墙实例时自动安装设备证书。

©2024 Palo Alto Networks, Inc.

STEP 2 | 将许可证认证码添加到引导软件包的 `/license` 文件夹中。

1. 使用文本编辑器创建名为 **`authcodes`**（无扩展名）的新文本文件。
2. 将 BYOL 许可证的授权代码添加到此文件，然后保存。授权代码必须代表一个代码包，且必须支持部署可能需要的防火墙数量。如果使用单个授权代码，而非代码包，防火墙只会检索文件中第一个授权代码的许可证密钥。

STEP 3 | 上传防火墙模板的 Lambda 代码 (`panw-aws.zip`) 和应用程序模板 (`app.zip`) 到 S3 存储桶。您可以使用与引导所使用的相同的 S3 存储桶。

如果应用程序堆栈由与防火墙不同的帐户管理，请使用应用程序帐户在与防火墙模板相同的 AWS 区域中创建另一个 S3 存储桶，并复制 `app.zip` 到该 S3 存储桶。

STEP 4 | 选择防火墙模板。

1. 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。
2. 选择从 Git 存储库**Upload**（上传）最新的防火墙模板，从而选择部署模板启动的资源的防火墙模板。单击 Open（打开）和 Next（下一步）。
3. 指定 Stack name（堆栈名称）。堆栈名称允许您唯一标识使用此模板部署的所有资源。

STEP 5 | 输入堆栈的描述性 **Name**（名称）。名称必须在 28 个字符以内。

STEP 6 | 配置 VPC 的参数。

1. 输入可用性区域数，然后从可用性区域下拉列表中选择地区。
2. 为 VM 系列防火墙查找并输入 AMI ID。确保 AMI ID 与您选择使用的 AWS 区域、PAN-OS 版本和 BYOL 或 PAYG 许可选项相匹配。有关更多信息，请参阅获取 Amazon 机器映像 ID。
3. 选择 EC2 **Key pair**（密钥对）（从下拉菜单中）启动防火墙。要登录防火墙，您必须提供此密钥对的名称以及与其关联的私钥。
4. 如果您要 **Enable Debug Log**（启用调试日志），请选择 **Yes**（是）。启用调试日志会生成详细列出的日志，以帮助解决部署问题。这些日志是使用堆栈名称生成的，并保存在 AWS CloudWatch 中。

默认情况下，模板使用 CPU 利用率作为 VM 系列防火墙的扩展参数。 自定义 PAN-OS 指标会自动发布到与之前指定的堆栈名称匹配的 CloudWatch 命名空间。

STEP 7 | 指定 Amazon S3 存储桶的名称。

1. 输入包含引导程序包的 S3 存储桶的名称。

   如果引导桶未正确设置，或者输入的存储桶名称不正确，则引导进程将失败，并且您无法登录到防火墙。对负载均衡器的运行状况检查也失败。
2. 输入包含 panw-aws.zip 文件的 S3 存储桶的名称。如前所述，对于 Bootstrap 和 Lambda 代码，您可以使用一个 S3 存储桶。

©2024 Palo Alto Networks, Inc.

STEP 8 | 指定启用 API 访问防火墙和 Panorama 的密钥。

1. 输入防火墙必须用来验证 API 调用的密钥。默认密钥基于示例示例文件，您只能将其用于测试和评估。对于生产部署，您必须为 API 调用创建单独的 PAN-OS 登录并生成关联的密钥。
2. 请输入 API 密钥以允许 AWS Lambda 对 Panorama 进行 API 调用。对于生产部署，您应该为 API 调用创建一个单独的登录并生成关联的密钥。

STEP 9 | 添加您的 AWS 帐号。您必须提供用于部署连接到 GWLB 的所有 VPC 的帐号。添加这些值作为以逗号分隔的列表。部署模板后，您可以添加其他帐号。

要找到您的帐号，单击 AWS 控制台右上角的 AWS 用户名，然后选择 **My Security Credentials**（我的安全凭据）。

STEP 10 | 输入中转网关 ID。保护东向西流量和出站流量需要中转网关 ID。如果未输入中转网关 ID，则模板假设入站流量只能由与 GWLB 集成的防火墙检查。

STEP 11 | 输入安全 VPC 的 CIDR。

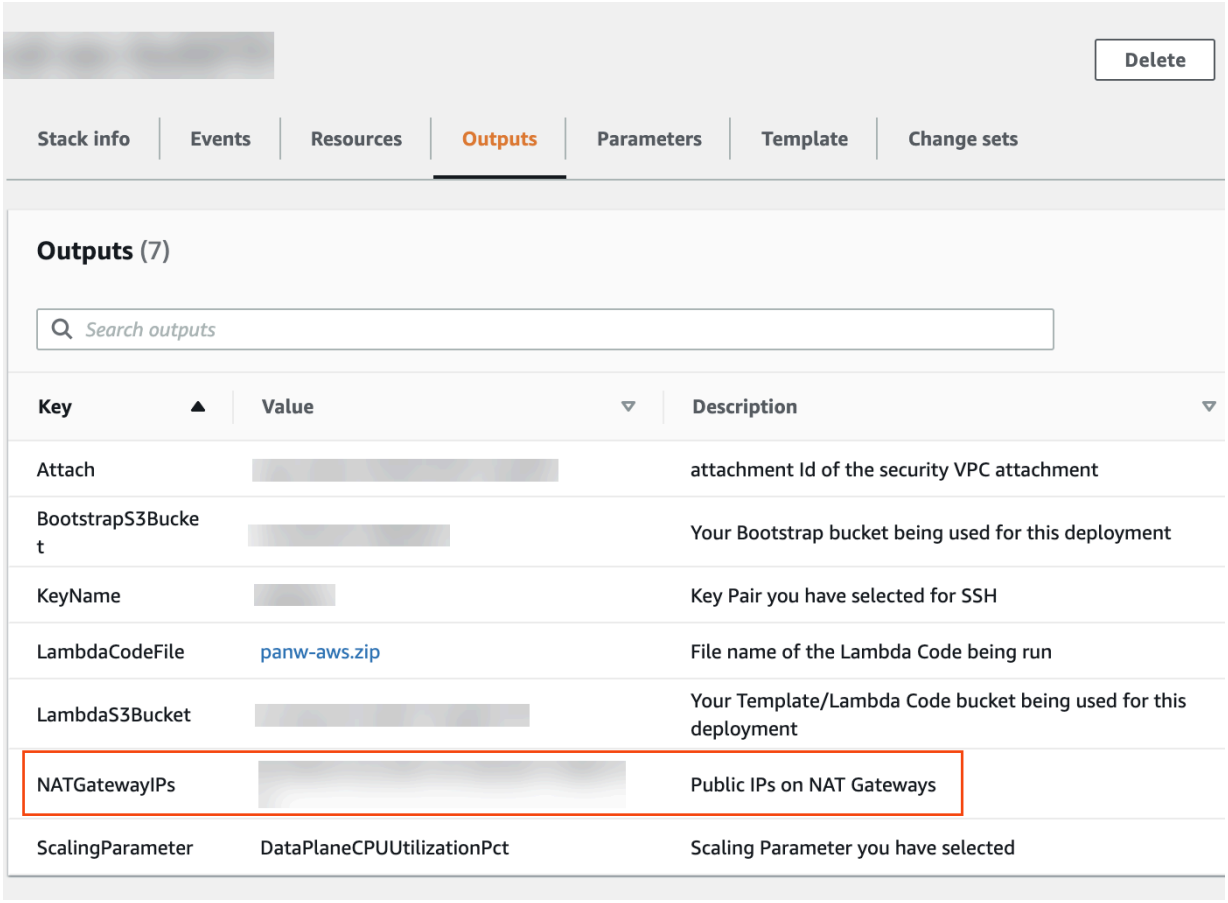
STEP 12 | 查看模板设置并启动模板。

1. 选择 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我承认此模板可能会导致 **AWS CloudFormation** 创建 **IAM** 资源）。
2. 单击 **Create**（创建）以启动模板。显示 CREATE_IN_PROGRESS 事件。
3. 成功部署时，状态会更新到 CREATE_COMPLETE。

STEP 13 | 验证模板是否启动了所有必需的资源。

©2024 Palo Alto Networks, Inc.

STEP 14 | 创建允许部署 Panorama 设备的安全组上的 NAT 网关 IP 地址的规则。允许防火墙连接到 Panorama 需要该规则。您可以在 CFT 安全堆栈输出中找到 NAT 网关 IP 地址列表。



 ©2024 Palo Alto Networks, Inc.

1. 访问 AWS VPC 控制台。
2. 在导航窗格中选择 **Security Groups**（安全组）。
3. 选择部署 Panorama 的安全组。
4. 选择 **Actions**（操作） > **Edit Inbound Rules**（编辑入站规则） > **Add rule**（添加规则）。
5. 对于端口范围 3978 的自定义 TCP 规则，添加允许 NAT 网关 IP 地址的规则。
6. 单击 **Save rules**（保存规则）。

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	

启动应用程序模板

完成以下过程以启动应用程序模板。

STEP 1 | 创建一个从中启动应用程序模板的 S3 存储桶。

- 如果是跨帐户部署，请创建新存储桶。
- 如果有一个帐户，则可以创建新的存储桶或使用之前创建的 S3 存储桶（您可以为所有部署使用一个存储桶）。

STEP 2 | 将 app.zip 文件上传到 S3 存储桶。

STEP 3 | 选择要启动的应用程序启动模板。

1. 在 AWS 管理控制台上，选择 **CloudFormation** > **CreateStack**（创建堆栈）。
2. 选择 Upload a template to Amazon S3（将模板上传到 Amazon S3），选择应用程序模板，将模板自动的资源部署到与防火墙相同的 VPC 中，或者将资源部署到不同的 VPC 中。单击 **Open**（打开）和 **Next**（下一步）。
3. 指定 Stack name（堆栈名称）。堆栈名称允许您唯一标识使用此模板部署的所有资源。

STEP 4 | 在“选择 AZ 列表”中选择设置将跨越的可用性区域 (AZ)。

©2024 Palo Alto Networks, Inc.

STEP 5 | 输入描述性的 **VPC Name**（**VPC** 名称）。

STEP 6 | 配置 Lambda 的参数。

1. 输入存储 app.zip 的 S3 存储桶名称。
2. 输入 zip 文件名。

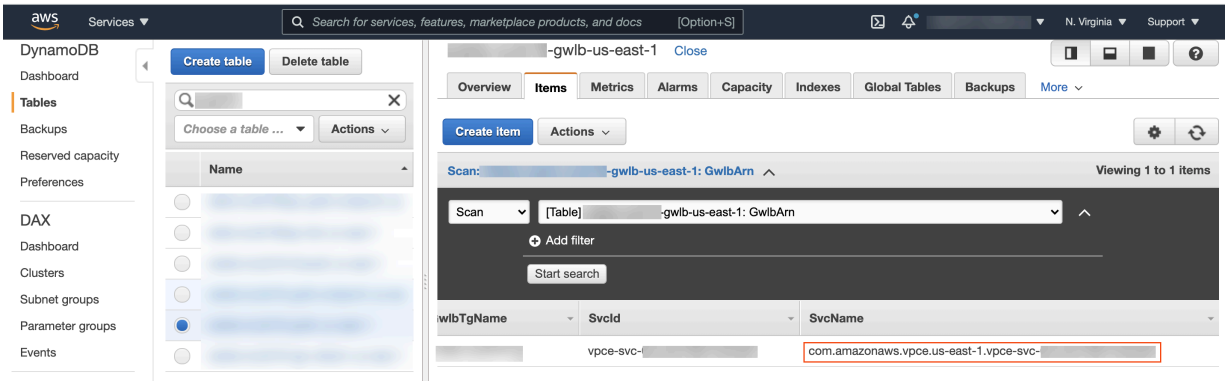
STEP 7 | 选择此模板启动的 Ubuntu Web 服务器的 EC2 实例类型。

STEP 8 | 输入您的 Amazon EC2 密钥对。

©2024 Palo Alto Networks, Inc.

STEP 9 | 输入安全 VPC 中 GWLB 端点的服务配置名称（服务名称）。

1. 在 AWS 控制台中，从 **Services**（服务）下拉列表中选择 **DynamoDB**。
2. 选择 **Tables**（表）并找到您的安全 VPC 表。表名将为 <stack name>-gwlb-<region>。例如：cft-deployment-gwlb-us-east-1。
3. 单击 Items（项目）选项卡，然后复制服务名称。
4. 将服务名称粘贴到应用程序模板配置参数中。



©2024 Palo Alto Networks, Inc.

STEP 10 | 输入中转网关 ID。这与您在部署防火墙模板之前创建的中转网关相同。

STEP 11 | 查看模板设置并启动模板。

STEP 12 | 部署应用程序后，您必须将路由添加到中转网关路由表，以启用东向西和出站流量检查。

1. 登录到 AWS VPC 控制台。
2. 选择 **Transit Gateway Route Tables**（中转网关路由表），然后选择您的中转网关路由表。此路由表由模板创建，名为 **<app-stack-name>-<region>-PANWAppAttRt**。
3. 选择 **Routes**（路由），然后单击 **Create static route**（创建静态路由）。
4. 在 **CIDR** 字段中输入 0.0.0.0/0。
5. 在 **Choose attachment**（选择附件）下拉列表中，选择 VM 系列防火墙 VPC 附件。
6. 单击 **Create static route**（创建静态路由）。

STEP 13 | （可选）创建堡垒主机（也称为跳转盒）以访问应用程序模板创建的 Web 服务器。

1. 在应用程序 VPC 中创建面向公众的子网。
2. 将路由添加到从 IP 地址到 Internet 网关的此子网。
3. 在具有公共 IP 地址的公共子网中创建新的 EC2 实例。
4. 为此 EC2 实例创建安全组，该安全组允许从 IP 地址进行 SSH。

©2024 Palo Alto Networks, Inc.

AWS 上 VM 系列防火墙的高可用性

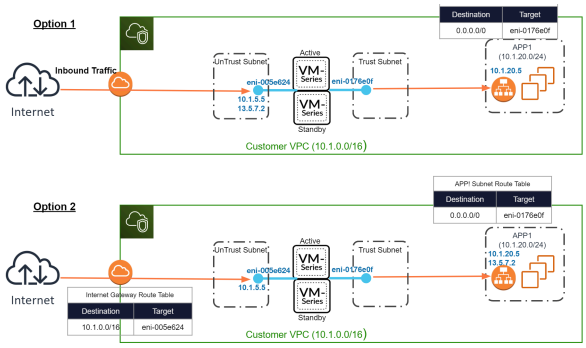
AWS 上的 VM 系列防火墙仅支持主动/被动 HA；如果已使用 Amazon 弹性负载均衡 (ELB) 部署，则它不支持 HA（在这种情况下，ELB 会提供故障转移功能）。

- AWS 上 HA 的概述
- HA 的 IAM 角色
- HA 链接
- 检测信号轮询和呼叫消息
- 设备优先级和抢先
- 高可用性计时器
- 使用辅助 IP 在 AWS 上配置主动/被动 HA
- 使用接口移动在 AWS 上配置主动/被动 HA
- 在 AWS 上迁移主动/被动 HA

AWS 上 HA 的概述

为确保冗余，您可采用主动/被动高可用性 (HA) 配置方式在 AWS 中部署 VM 系列防火墙。主动对等将与相同配置的被动对等持续同步其配置和会话信息。上述两个设备之间的脉动连接可确保在主动设备关闭时实现故障转移。可以通过使用两个选项在 HA 中的 AWS 上部署 VM 系列防火墙：辅助 IP 移动和数据平面接口 (ENI) 移动。

要确保到面向 Internet 的应用程序的所有流量都通过防火墙，您有两种选择。您可以在 VM 系列防火墙的不可信接口（上图中的 E1/2）上配置应用程序的公用 IP 地址，也可以配置 AWS 入口路由。AWS 入口路由功能可让您将路由表与 AWS Internet 网关相关联，并添加路由规则以通过 VM 系列防火墙重定向应用程序流量。该重定向可确保所有 Internet 流量都通过防火墙，而无需重新配置应用程序端点。



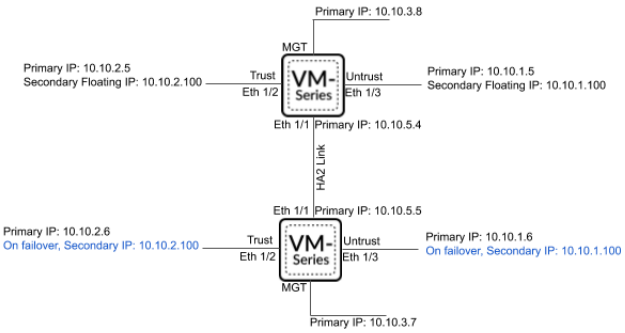
辅助 IP 地址移动

当主动对等出现故障时，被动对等会检测到此故障并变成主动对等。此外，还会触发对 AWS 基础架构的 API 调用，以将配置的辅助 IP 地址从出现故障的对等的数据平面接口移动到自身。另外，AWS 更新路由表以确保将流量定向到主动防火墙实例。这两个操作可确保故障转移后恢复入

©2024 Palo Alto Networks, Inc.

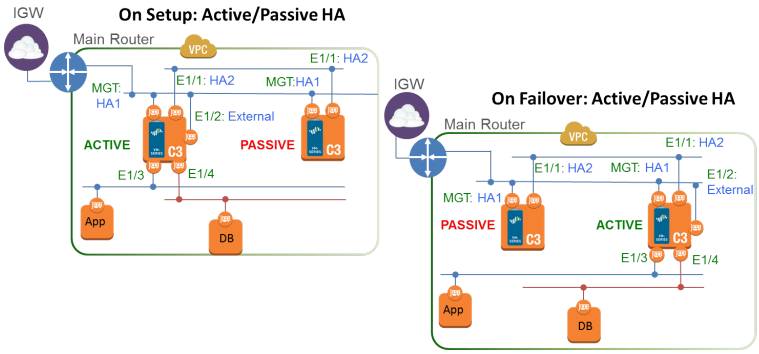
站和出站流量会话。使用该选项，您可以利用 DPDK 提高 VM 系列防火墙实例的性能，并提供比接口移动 HA 更好的故障转移时间，同时支持接口移动提供的所有功能。

辅助 *IP* 移动 *HA* 需要 *VM* 系列插件 *2.0.1* 或更高版本。



数据平面接口移动

当主动对等出现故障时，被动对等会检测到故障并变成主动对等。此外，还会触发对 AWS 基础架构的 API 调用，以将所有数据平面接口 (ENI) 从出现故障的对等移动到自身。



HA 的 IAM 角色

AWS 要求所有 API 请求必须使用由其发布的凭证进行加密签名。要为部署为 HA 对的 VM 系列防火墙启用 API 权限，必须创建一个策略，然后将该策略附加到 AWS 身份识别及访问管理 (IAM) 服务中的角色。相关角色必须在启动时附加到 VM 系列防火墙。该策略授予 IAM 角色权限，使其能够在触发故障转移时启动将接口或辅助 IP 地址从主动对等移动到被动对等所需的 API 操作。

有关创建策略的详细说明，请参阅关于创建客户管理策略的 AWS 文档。有关创建 IAM 角色、定义哪些帐户/AWS 服务可承担此角色、定义承担此角色时应用程序可使用哪些 API 操作和资源的详细说明，请参阅关于《Amazon EC2 的 IAM 角色》的 AWS 文档。

在 AWS 控制台中配置的 IAM 策略必须具备针对以下操作和资源的权限（基本要求）：

©2024 Palo Alto Networks, Inc.

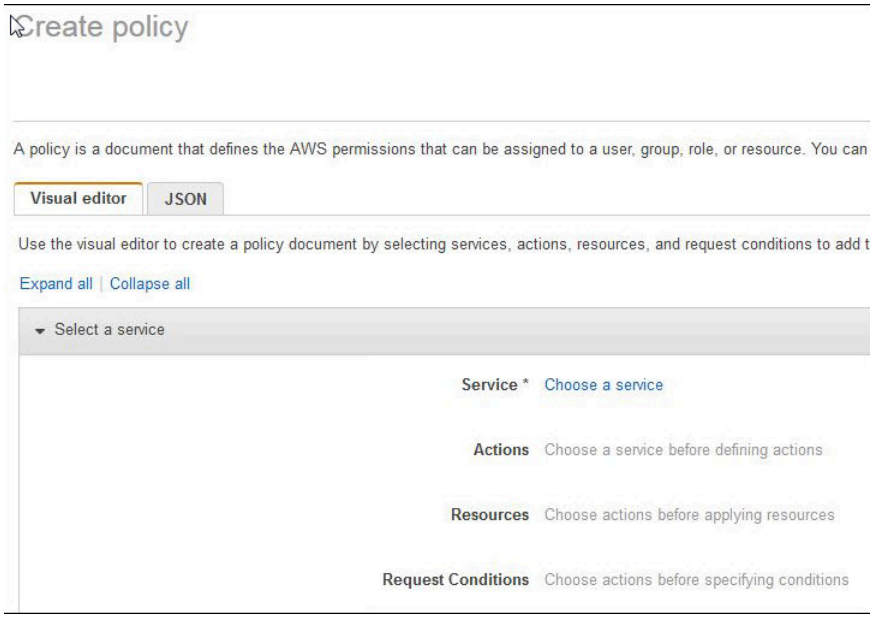
要启用 *HA*，您需要以下 *IAM* 操作、权限和资源。要启用 *AWS Cloudwatch* 监控，请参阅在 VM 系列防火墙上启用 CloudWatch 监控 所需的 *IAM* 操作。

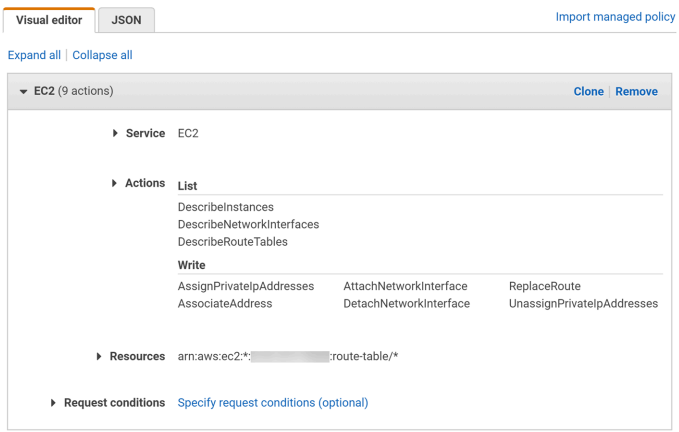
IAM 操作、权限或资源	说明	接口移动	辅助 **IP** 地址移动
AttachNetworkInterface	用于允许将 ENI 附加到实例。	✓	✓
DescribeNetworkInterfaces	用于提取 ENI 参数以将接口附加到实例。	✓	✓
DetachNetworkInterface	用于允许从 EC2 实例分离 ENI。	✓	✓
DescribeInstances	用于允许在 VPC 中的 EC2 实例上获取信息。	✓	✓
AssociateAddress	用于允许将与辅助 IP 地址关联的公共 IP 地址从被动接口移动到主动接口。		✓
AssignPrivateIpAddresses	用于允许将辅助 IP 地址和关联的公共 IP 地址分配至被动对等上的接口。		✓
DescribeRouteTables	用于允许检索与 VM 系列防火墙实例关联的所有路由表。		✓
ReplaceRoute	用于允许更新 AWS 路由表条目。		✓
GetPolicyVersion	用于允许检索 AWS 策略版本信息。		✓
GetPolicy	用于允许检索 AWS 策略信息。		✓
ListAttachedRolePolicies	用于允许检索附加到指定 IAM 角色的所有托管策略列表。		✓
ListRolePolicies	用于允许检索指定 IAM 角色中嵌入的内联策略名称列表。		✓
GetRolePolicy	用于允许检索指定 IAM 角色中嵌入的指定内联策略。		✓

©2024 Palo Alto Networks, Inc.

IAM 操作、权限或资源	说明	接口移动	辅助 IP 地址移动
策略	用于允许访问 IAM 策略 Amazon 资源名称 (ARN)。		✓
角色	用于允许访问 IAM 角色 ARN。		✓
route-table	用于允许访问路由表 Amazon 资源名称 (ARN)，以便在发生故障转移后进行更新。		✓
通配符 (*)	在 ARN 字段中，使用 * 作为通配符。	✓	✓

以下屏幕截图显示了针对辅助 IP HA 的上述 IAM 角色进行的访问管理设置：





©2024 Palo Alto Networks, Inc.

接口移动 HA 所需的最低权限为：

{ "Version":"2012-10-17", "Statement":[{ "Sid":"VisualEditor0", "Effect":"Allow", "Action": ["ec2:AttachNetworkInterface", "ec2:DetachNetworkInterface", "ec2:DescribeInstances", "ec2:DescribeNetworkInterfaces"], "Resource":"*" }]}

辅助 IP 地址移动 HA 所需的最低权限为：

{ "Statement": [{ "Action": ["ec2:AttachNetworkInterface", "ec2:DetachNetworkInterface", "ec2:DescribeInstances", "ec2:DescribeNetworkInterfaces", "ec2:AssignPrivateIpAddresses", "ec2:AssociateAddress", "ec2:DescribeRouteTables"], "Effect":"Allow", "Resource": ["*"], "Sid":"VisualEditor0" }, { "Action": "ec2:ReplaceRoute", "Effect":"Allow", "Resource": "arn:aws:ec2:*:*:route-table/*", "Sid":"VisualEditor1" }], "Version":"2012-10-17"}

HA 链接

HA 对中的设备使用 HA 链接来同步数据并维护状态信息。在 AWS 上，VM 系列防火墙使用以下端口：

- 控制链接 — HA1 链接用于交换呼叫消息、检测信号和 HA 状态信息，以及路由和 User-ID 信息的管理面板同步。此链接还用于同步主动或被动设备与其对等端上的配置更改。

  使用管理端口进行 HA1 链接操作。使用 TCP 端口 28769 和 28260 进行明文通信；使用端口 28 进行加密通信 (SSH over TCP)。
- 数据链接 — HA2 链接用于在 HA 对中的设备之间同步会话、转发表、IPSec 安全关联和 ARP 表。HA2 链接上的数据流始终是单向的（HA2 保持活动状态除外）；它从主动设备流动到被动设备。

  必须将 Ethernet1/1 分配为 HA2 链接；这是在 HA 中在 AWS 上部署 VM 系列防火墙所必需的。可以将 HA 数据链接配置为使用 IP（协议号 99）或 UDP（端口 29281）进行传输。

AWS 上的 VM 系列防火墙不支持 HA1 或 HA2 的备份链接。

检测信号轮询和呼叫消息

防火墙使用呼叫消息和检测信号来验证对等设备是否有响应、是否可操作。呼叫消息以配置的呼叫间隔从一个对等端发送到另一个对等端，以验证设备的状态。检测信号是通过控制链接对 HA 对等端进行的 ICMP ping 操作，对等端响应 ping 操作以确定该设备已连接并且有响应。有关触发故障转移的 HA 计时器的详细信息，请参阅高可用性计时器。（VM 系列防火墙与 PA-5200 系列防火墙的高可用性计时器相同）。

设备优先级和抢先

可以为 HA 对中的设备分配设备优先级值，以在故障转移时指示优先选择哪台设备来承担主动角色并管理通信。如果您需要使用 HA 对中的特定设备来主动保护通信安全，则必须在两个防火墙上启用抢先行为，并为每台设备分配一个设备优先级值。具有较低数值，从而具有较高优先级的设备将被指定为主动设备，管理网络上的所有通信。另一台设备处于被动状态，它将同步主动设备的配置和状态信息，以便随时准备在主动设备发生故障时转换为主动状态。

 ©2024 Palo Alto Networks, Inc.

默认情况下，抢先行为在防火墙上是禁用的，并且必须在两台设备上同时启用。启用后，抢先行为将允许具有较高优先级（较低数值）的防火墙在从故障中修复后恢复为主动角色。当发生抢先行为时，该事件会记录在系统日志中。

不建议在 *AWS* 上的 *VM* 系列防火墙中为 *HA* 执行抢先行为。

高可用性计时器

高可用性 (HA) 计时器用于检测防火墙故障和触发故障转移。要降低配置高可用性计时器的复杂性，您可以从以下三个配置文件中进行选择：**Recommended**（建议）、**Aggressive**（积极）和 **Advanced**（高级）。对于特定的防火墙平台，这些配置文件会自动填写最佳高可用性计时器值，从而更快地执行高可用性部署。

对于典型的故障转移计时器设置，使用 **Recommended**（建议）的配置文件；对于更快的故障转移计时器设置，使用 **Aggressive**（积极）的配置文件。**Advanced**（高级）配置文件可用于自定义适合您的网络需求的计时器值。

AWS 中 **VM** 系列的高可用性计时器	建议/积极配置文件的默认值
提升持有时间	2000/500 ms
呼叫间隔	8000/8000 ms
检测信号间隔	2000/1000 ms
最大翻动数	3/3
抢先持有时间	1/1 min
监控失败持续时间	0/0 ms
额外主设备持续时间	500/500 ms

使用辅助 IP 在 AWS 上配置主动/被动 HA

完成以下过程，以部署新的 VM 系列防火墙作为具有辅助 IP 地址的 HA 对。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2024 Palo Alto Networks, Inc.

STEP 1 | 在为 HA 对部署 VM 系列防火墙之前，请确保执行以下操作：

- 参阅 VPC 规划工作表，以确保 VPC 已为 VM 系列防火墙做好准备。
- 辅助 IP 移动 HA 需要 VM 系列插件 2.0.1 或更高版本。
- 在相同的 AWS 可用性区域中部署两个 HA 对等。

  从 VM 系列插件 2.0.3 开始，您可以在不同的可用性区域中部署 HA 对等。虽然不推荐这种类型的部署，但是它受支持。
- 创建 IAM 角色，然后在部署实例时将该角色分配至 VM 系列防火墙。
- 主动和被动防火墙至少必须具有四个接口 — 管理接口、HA2 接口、不可信接口和可信接口。此外，主动防火墙上的可信和不可信接口必须分配辅助 IP 地址。

  必须将管理接口用作 HA1 接口。
- 验证是否已适当定义网络和安全组件。
  - 启用与 Internet 的通信。默认 VPC 包括 Internet 网关，如果在默认子网中安装 VM 系列防火墙，则该防火墙必须能够访问 Internet。
  - 创建子网。子网是分配给可以在其中启动 EC2 实例的 VPC 的 IP 地址范围的分段。VM 系列防火墙必须属于公共子网，这样可以配置它以访问 Internet。
  - 创建一个包含防火墙数据接口的数据安全组。此外，将安全配置为允许所有流量 (0.0.0.0/0)，因此安全由防火墙强制执行。在故障转移过程中维护现有会话需要执行此操作。
  - 将路由添加到专用子网的路由表，以确保可以通过 VPC 中的子网和安全组路由流量（如适用）。
- 如果您引导防火墙，请创建包含所需引导文件的必需 S3 存储桶。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在 AWS 上部署 VM 系列防火墙。

1. 如果 VM 系列防火墙未安装 VM 系列插件 2.0.1 或更高版本，请先更新插件，然后再继续。
2. 在每个 HA 对等上将 ethernet 1/1 接口配置为 HA2 接口。
   1. 打开 Amazon EC2 控制台。
   2. 选择 Network Interface（网络接口），然后选择您的网络接口。
   3. 选择 **Actions**（操作） > **Manage IP Addresses**（管理 **IP** 地址）。
   4. 将字段留空以允许 AWS 动态分配 IP 地址，或输入 VM 系列防火墙的子网范围内的 IP 地址。
   5. 单击 **Yes**（是）和 **Update**（更新）。
   6. 选择 **Actions**（操作） > **Change Source/Dest.Check**（更改源/目标检查），然后选择 **Disable**（禁用）。
   7. 在第二个（被动）HA 对等上重复此过程。
3. 将辅助 IP 地址添加到第一个（主动）HA 对等上的数据平面接口。
   1. 选择 **Network Interface**（网络接口），然后选择您的网络接口。
   2. 选择 **Actions**（操作） > **Manage IP Addresses**（管理 **IP** 地址） > **IPv4 Addresses**（**IPv4** 地址） > **Assign new IP**（分配新的 **IP** 地址）。
   3. 将字段留空以允许 AWS 动态分配 IP 地址，或输入 VM 系列防火墙的子网范围内的 IP 地址。
   4. 单击 **Yes**（是）和 **Update**（更新）。
4. 将主实例上的弹性（公共）IP 地址与活动对等的不信任接口相关联。
   1. 选择 **Elastic IPs**（弹性 **IP** 地址），然后选择要关联的弹性 IP 地址。
   2. 选择 **Actions**（操作） > **Associate Elastic IP**（关联弹性 **IP** 地址）。
   3. 在 **Resource Type**（资源类型）下，选择 **Network Interface**（网络接口）。
   4. 选择要与弹性 IP 地址相关联的网络接口。
   5. 单击 **Associate**（关联）。
5. 对于出站流量检查，在子网路由表中添加一个条目，以将下一个跃点设置为防火墙可信接口。
   1. 选择 **VPC** > **Route Tables**（路由表）。
   2. 选择您的子网路由表。
   3. 选择 **Actions**（操作） > **Edit routes**（编辑路由） > **Add route**（添加路由）。
   4. 输入 **Destination**（目标）CIDR 块或 IP 地址。
   5. 对于 **Target**（目标），输入防火墙可信接口的网络接口。
   6. 单击 **Save routes**（保存路由）。

©2024 Palo Alto Networks, Inc.

6. 要使用 AWS 入口路由，请创建一个路由表，并将 Internet 网关与其相关联。然后添加一个条目，并将下一个跃点设置为主动防火墙不可信接口。
   1. 选择 **Route Tables**（路由表）> **Create route table**（创建路由表）。
   2. （可选）输入路由表的描述性 **Name tag**（名称标签）。
   3. 单击 **Create**（创建）。
   4. 单击路由表，然后选择 **Actions**（操作）> **Edit edge associations**（编辑边缘关联）。
   5. 选择 **Internet gateways**（**Internet** 网关），然后选择 VPC Internet 网关。
   6. 单击 **Save**（保存）。
   7. 单击路由表，然后选择 **Actions**（操作）> **Edit routes**（编辑路由）。
   8. 对于 **Target**（目标），选择 **Network Interface**（网络接口），然后选择主动防火墙的不可信接口。
   9. 单击 **Save routes**（保存路由）。

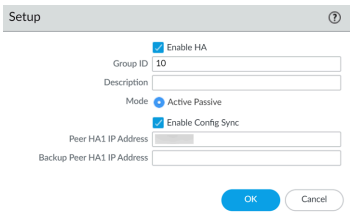
STEP 3 | 配置防火墙上的接口。您必须为不可信和可信接口配置 HA2 数据链路和至少两个第 3 层接口。在第一个 HA 对等上完成此工作流程，然后在第二个 HA 对等上重复这些步骤。

1. 登录到防火墙 Web 界面。
2. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后单击不可信接口。在本例中，HA2 接口为 1/1，可信接口为 ethernet 1/2，不可信接口为 ethernet 1/3。
3. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**HA**
4. 单击 **ethernet 1/2** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 trust-zone），然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **DHCP Client**（**DHCP** 客户端）。
   - 选中 **Enable**（启用）。
   - 在不可信接口上，选中 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）。该选项指示防火墙针对默认网关创建静态路由。
   - 对于 ethernet 1/3 接口，重复这些步骤。
5. 在被动对等上，重复上述步骤。

©2024 Palo Alto Networks, Inc.

STEP 4 | 启用 HA。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规）。
2. 编辑 Setup（设置）设置。
3. 在 **Peer HA1 IP address**（对等 **HA1 IP** 地址）字段中输入被动对等的专用 IP 地址。
4. 单击 **OK**（确定）。



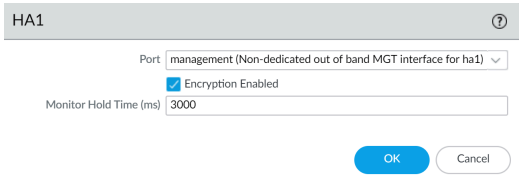
5. 编辑 **Election Settings**（选择设置）以将特定防火墙指定为主动对等。在主动防火墙上输入较低的数字 **Device Priority**（设备优先级）值。如果两个防火墙具有相同的设备优先级值，则在 HA1 控制链路上具有最低 MAC 值的防火墙将变为主动防火墙。

   建议不启用抢占行为。

6. 单击 **OK**（确定）。
7. **Commit**（提交）更改。
8. 在被动对等上，重复上述步骤。

STEP 5 | 将控制链接 (HA1) 设为使用管理端口。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规），然后编辑控制链接 (HA1) 部分。

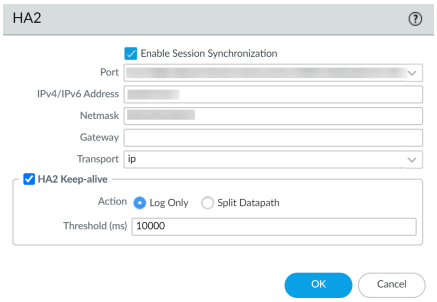


2. （可选）选择 **Encryption Enabled**（启用加密），以便保护对等之间的 HA 通信。如需启用加密，您必须从设备中导出 HA 密钥并将其导入对等设备。
   1. 选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书）。
   2. 选择 **Export HA key**（导出 **HA** 密钥）。将高可用性密钥保存到对等设备可以访问的网络位置。
   3. 在对等设备上，导航到 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书），然后选择 **Import HA key**（导入 **HA** 密钥）以浏览到您保存密钥的位置并将密钥导入对等设备。

©2024 Palo Alto Networks, Inc.

STEP 6 | 将数据链接 (HA2) 设为使用 ethernet1/1。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后编辑数据链接 (HA2) 部分。
2. 选择 **Port**（端口）ethernet1/1。
3. 输入 ethernet1/1 的 IP 地址。此 IP 地址必须与在 EC2 仪表盘上分配至 ENI 的 IP 地址相同。
4. 输入**Netmask**（子网掩码）。
5. 当 HA1 接口处于单独的子网上时，输入 **Gateway**（网关）IP 地址。
6. 选择用于 **Transport**（传输）的 **IP** 或 **UDP**。需要第 3 层传输时，请使用 **IP**（IP 协议号为 99）。如果想要防火墙对整个数据包，而非仅对标头计算校验（如 IP 选项一样），请选择 **UDP**（UDP 端口为 29281）。



7. （可选）修改 **HA2 Keep-alive**（**HA2** 保持活动状态）数据包的 **Threshold**（阈值）。在默认情况下，将启用 **HA2 Keep-alive**（**HA2** 保持活动状态）以监控对等之间的 HA2 数据链接。如果发生故障且超过此阈值（默认情况下为 10000 ms），则会执行已定义的操作。在发生 HA2 保持活动状态故障时，一条关键的系统日志消息将随之生成。

> 您可以在 *HA* 对的两台设备或仅在一台设备上配置 ***HA2 keep-alive***（***HA2*** 保持活动状态）选项。如果您仅在一台设备上启用此选项，则仅此一台设备会发送“保持活动状态”消息。

©2024 Palo Alto Networks, Inc.

STEP 7 | 在完成两个防火墙的配置 HA 后，验证防火墙是否已在主动/被动 HA 中配对。

1. 访问两个防火墙上的 **Dashboard**（仪表盘），并查看高可用性小部件。
2. 在主动 HA 对等上，单击 **Sync to peer**（同步到对等）。
3. 确认防火墙已配对并同步。
   - 在被动防火墙上：本地防火墙的状态应显示 **Passive**（被动），并且 **Running Config**（运行配置）应显示为 Synchronized（已同步）。
   - 在主动防火墙上：本地防火墙的状态应显示 **Active**（主动），并且 **Running Config**（运行配置）应显示为 Synchronized（已同步）。
4. 在防火墙命令行界面中，执行以下命令：
   - 验证故障转移就绪情况：

     ```
     show plugins vm_series aws ha state
     ```
   - 显示辅助 IP 映射：

     ```
     show plugins vm_series aws ha ips
     ```

使用接口移动在 AWS 上配置主动/被动 HA

完成以下过程，以使用接口移动模式配置主动-被动 HA。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2024 Palo Alto Networks, Inc.

STEP 1 | 确保已满足以下先决条件。

对于在 AWS 云中以 HA 方式部署两个 VM 系列防火墙，必须确保已满足以下条件：

- 在 EC2 实例上启动 VM 系列防火墙时，选择已创建的 IAM 角色，且不可将此角色分配至已运行的实例。请参阅 IAM Roles for HA（HA 的 IAM 角色）。

  有关创建 IAM 角色，定义哪些帐户或 AWS 服务可承担此角色，定义承担此角色时应用程序可使用哪些 API 操作和资源的详细说明，请参阅 AWS documentation（AWS 文档）。

- 在接口移动 HA 部署中，AWS 上的 VM 系列防火墙不支持 DPDK。如果防火墙上已安装 VM 系列插件 2.0.1 或更高版本，则您必须禁用 DPDK。

  禁用 DPDK 要求防火墙重新启动。如果您使用引导来部署 VM 系列防火墙，则可以通过使用 **op-cmd-dpdk-pkt-io=off** 禁用 initi-cfg.txt 文件中的 DPDK 以避免重新启动防火墙。如需更多信息，请参阅 在 AWS 上引导 VM 系列防火墙。

- HA 对中的活动防火墙必须至少有三个 ENI：两个数据平面接口和一个管理接口。

  HA 对中的被动防火墙，必须有一个用于管理的 ENI，一个用作数据平面接口的 ENI；您可以将数据平面接口配置为 HA2 接口。

  不要将其他数据平面接口附加到 *HA* 对中的被动防火墙。在故障转移的情况下，数据面板接口将以先分离后附加的方式，从之前的主动防火墙移动至当前的主动防火墙（之前为被动）。

- 必须在相同的 AWS 可用性区域中部署 HA 对等。虽然跨 AWS 可用性区域的 VM 系列 HA 不是推荐的解决方案，但是它受支持。

STEP 2 | 在 AWS 上启动 VM 系列防火墙。

STEP 3 | （VM 系列插件 2.0.1 或更高版本）在主动和被动防火墙上禁用 DPDK。默认已启用 DPDK，并且接口移动 HA 模式不支持 DPDK，因此您必须将其禁用；启用 Packet MMAP。

1. 登录到被动防火墙 CLI。
2. 使用以下命令禁用 DPDK。执行此命令重新启动防火墙。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

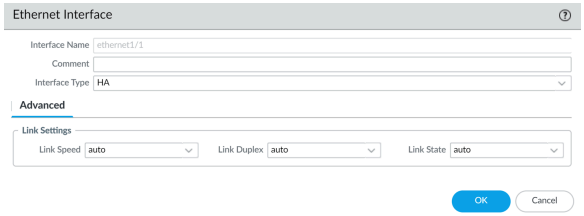
STEP 4 | 启用 HA。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后编辑 Setup（设置）部分。
2. 选择 **Enable HA**（启用 **HA**）。

©2024 Palo Alto Networks, Inc.

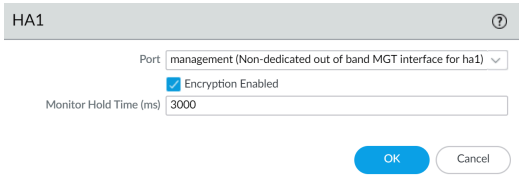
STEP 5 | 配置 ethernet 1/1 为 HA 接口。此接口必须被用于 HA2 通信。

1. 选择 **Network**（网络） > **Interfaces**（接口）。
2. 确认 ethernet1/1 上的链接状态正常。
3. 单击 ethernet1/1 的链接，将 **Interface Type**（接口类型）设置为 HA。



STEP 6 | 将控制链接 (HA1) 设为使用管理端口。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规），然后编辑控制链接 (HA1) 部分。

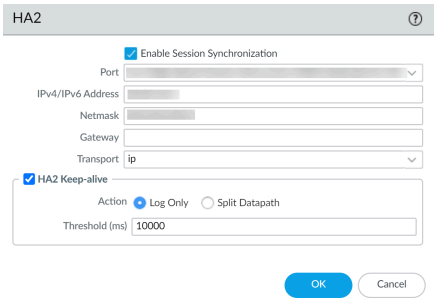


2. （可选）选择 **Encryption Enabled**（启用加密），以便保护对等之间的 HA 通信。如需启用加密，您必须从设备中导出 HA 密钥并将其导入对等设备。
   1. 选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书）。
   2. 选择 **Export HA key**（导出 **HA** 密钥）。将高可用性密钥保存到对等设备可以访问的网络位置。
   3. 在对等设备上，导航到 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书），然后选择 **Import HA key**（导入 **HA** 密钥）以浏览到您保存密钥的位置并将密钥导入对等设备。

©2024 Palo Alto Networks, Inc.

STEP 7 | 将数据链接 (HA2) 设为使用 ethernet1/1。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规），然后编辑数据链接 (HA2) 部分。
2. 选择 **Port**（端口）ethernet1/1。
3. 输入 ethernet1/1 的 IP 地址。此 IP 地址必须与在 EC2 仪表盘上分配至 ENI 的 IP 地址相同。
4. 输入**Netmask**（子网掩码）。
5. 当 HA1 接口处于单独的子网上时，输入 **Gateway**（网关）IP 地址。
6. 选择用于 **Transport**（传输）的 **IP** 或 **UDP**。需要第 3 层传输时，请使用 **IP**（IP 协议号为 99）。如果想要防火墙对整个数据包，而非仅对标头计算校验（如 IP 选项一样），请选择 **UDP**（UDP 端口为 29281）。



7. （可选）修改 **HA2 Keep-alive**（**HA2** 保持活动状态）数据包的 **Threshold**（阈值）。在默认情况下，将启用 **HA2 Keep-alive**（**HA2** 保持活动状态）以监控对等之间的 HA2 数据链接。如果发生故障且超过此阈值（默认情况下为 10000 ms），则会执行已定义的操作。在发生 HA2 保持活动状态故障时，一条关键的系统日志消息将随之生成。

   您可以在 *HA* 对的两台设备或仅在一台设备上配置 ***HA2 keep-alive***（***HA2*** 保持活动状态）选项。如果您仅在一台设备上启用此选项，则仅此一台设备会发送“保持活动状态”消息。

©2024 Palo Alto Networks, Inc.

STEP 8 | 设置设备优先级并启用抢先。

如果您希望确保特定设备为首选主动设备，请使用此设置。有关详细信息，请参阅设备优先级和抢先。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规），然后编辑 Election Settings（选择设置）部分。
2. 在 **Device Priority**（设备优先级）中设置数值。确保在要分配较高优先级的设备上设置较低的数值。

   如果两个防火墙具有相同的设备优先级值，则在 *HA1* 控制链接上具有最低 *MAC* 地址的防火墙将变为主动设备。
3. 选择 **Preemptive**（抢先）。

   必须同时在主动和被动设备上启用抢先。
4. 修改故障转移计时器。默认情况下，高可用性计时器配置文件设置为 **Recommended**（建议）配置文件，并且适用于最佳高可用性部署。

STEP 9 | （可选）修改触发故障转移之前的等待时间。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规），然后编辑 Active/Passive Settings（主动/被动设置）。
2. 将 **Monitor fail hold up time**（监控故障持续时间）修改为 1-60 分钟之间的一个值（默认值为 1 分钟）。此为防火墙在链接故障后将保持活动状态的时间间隔。使用此设置可避免因邻近设备偶然翻动而触发的 HA 故障转移。

STEP 10 | 配置 HA 对等的 IP 地址。

1. 选择 **Device**（设备） > **High Availability**（高可用性） > **General**（常规），然后编辑 Setup（设置）部分。
2. 在对等上输入 HA1 端口的 IP 地址。此为分配至管理接口 (ethernet 0/0) 的 IP 地址，也是其他防火墙上的 HA1 链接。
3. 将 **Group ID**（组 **ID**）设置为 1 至 63 之间的数值。尽管此数值不会在 AWS 上的 VW 系列防火墙上使用，但不可将此字段留空。

STEP 11 | 配置其他对等。

在 HA 对端上，重复步骤 3 到 9。

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 在完成两台设备的配置后，验证设备是否已在主动/被动 HA 中配对。

1. 访问两台设备上的 **Dashboard**（仪表盘），并查看 **High Availability**（高可用性）小部件。
2. 在主动设备上，单击 **Sync to peer**（同步到对等）链接。
3. 确认设备已配对并同步，如下所示：
   - 在被动设备上：本地设备的状态应显示 **passive**（被动），并且配置为 **synchronized**（已同步）。
   - 在主动设备上：本地设备的状态应显示 **active**（主动），并且配置为 **synchronized**（已同步）。

STEP 13 | 验证是否已正确发生故障转移。

1. 验证 HA 模式。

   ```
   show plugins vm_series aws ha failover-mode
   ```
2. 验证已将数据包 IO 模式设置为 Packet MMAP。

   ```
   show system setting dpdk-pkt-io
   ```
3. 关闭主动 HA 对等。
   1. 在 EC2 仪表盘上，选择 **Instances**（实例）。
   2. 从列表中选择 VM 系列防火墙，然后单击 **Actions**（操作） > **Stop**（停止）。
4. 检查被动对等是否已承担主动对等的角色，且数据面板接口已移至当前的主动 HA 对等。

在 AWS 上迁移主动/被动 HA

支持两种可用性模式，如果部署需要，则可以在每种模式之间迁移。由于接口移动模式不支持 DPDK，因此必须在 VM 系列防火墙上将其禁用，然后再完成迁移。禁用 DPDK 要求重新启动 VM 系列防火墙，这将会影响主动防火墙上的所有流量会话。

- 在 AWS 上将主动/被动 HA 迁移到辅助 IP 模式
- 在 AWS 上将主动/被动 HA 迁移到接口移动模式

在 AWS 上将主动/被动 HA 迁移到辅助 IP 模式

完成以下过程，以将现有的 VM 系列防火墙 HA 对从接口移动 HA 迁移到辅助 IP HA。

辅助 *IP* 移动 *HA* 需要 *VM* 系列插件 *2.0.1* 或更高版本。

STEP 1 | 在被动 HA 对等上升级 VM 系列插件，然后在主动对等上进行升级。

©2024 Palo Alto Networks, Inc.

STEP 2 | 为主动对等上的所有数据接口创建辅助 IP 地址。

1. 登录到 AWS EC2 控制台。
2. 选择 **Network Interface**（网络接口），然后选择您的网络接口。
3. 选择 **Actions**（操作） > **Manage IP Addresses**（管理 **IP** 地址） > **IPv4 Addresses**（**IPv4** 地址） > **Assign new IP**（分配新的 **IP** 地址）。
4. 将字段留空以允许 AWS 动态分配 IP 地址，或输入 VM 系列防火墙的子网范围内的 IP 地址。
5. 单击 **Yes**（是）和 **Update**（更新）。

STEP 3 | 将辅助弹性（公共）IP 地址与主动对等的不可信接口相关联。

1. 登录到 AWS EC2 控制台。
2. 选择 **Elastic IPs**（弹性 **IP** 地址），然后选择要关联的弹性 IP 地址。
3. 选择 **Actions**（操作） > **Associate Elastic IP**（关联弹性 **IP** 地址）。
4. 在 **Resource Type**（资源类型）下，选择 **Network Interface**（网络接口）。
5. 选择要与弹性 IP 地址相关联的网络接口。
6. 单击 **Associate**（关联）。

STEP 4 | 创建指向包含可信接口的子网的路由表。

1. 选择 **Route Tables**（路由表） > **Create route table**（创建路由表）。
2. （可选）输入路由表的描述性 **Name tag**（名称标签）。
3. 选择您的 **VPC**。
4. 单击 **Create**（创建）。
5. 选择 **Subnet Associations**（子网关联） > **Edit subnet associations**（编辑子网关联）。
6. 选中包含可信接口的子网的 **Associate**（关联）复选框。
7. 单击 **Save**（保存）。

STEP 5 | 使用迁移到辅助 IP 移动 HA 所需的其他操作和权限更新 IAM 角色。

IAM 操作、权限或资源	说明
AssociateAddress	用于允许将与辅助 IP 地址关联的公共 IP 地址从被动接口移动到主动接口。
AssignPrivateIpAddresses	用于允许将辅助 IP 地址和关联的公共 IP 地址从被动接口移动到主动接口。
UnassignPrivateIpAddress	用于允许取消将辅助 IP 地址和关联的公共 IP 地址分配至主动对等上的接口。

©2024 Palo Alto Networks, Inc.

IAM 操作、权限或资源	说明
DescribeRouteTables	用于允许检索与 VM 系列防火墙实例关联的所有路由表。
ReplaceRoute	用于允许更新 AWS 路由表条目。
GetPolicyVersion	用于允许检索 AWS 策略版本信息。
GetPolicy	用于允许检索 AWS 策略信息。
ListAttachedRolePolicies	用于允许检索附加到指定 IAM 角色的所有托管策略列表。
ListRolePolicies	用于允许检索指定 IAM 角色中嵌入的内联策略名称列表。
GetRolePolicy	用于允许检索指定 IAM 角色中嵌入的指定内联策略。
策略	用于允许访问 IAM 策略 Amazon 资源名称 (ARN)。
角色	用于允许访问 IAM 角色 ARN。
route-table	用于允许访问路由表 ARN。
通配符 (*)	在 ARN 字段中，使用 * 作为通配符。

©2024 Palo Alto Networks, Inc.

STEP 6 | 在与主动防火墙数据接口相同的子网中的被动防火墙上创建新接口 (ENI)。

不要将辅助 *IP* 地址分配至这些新接口。

1. 打开 Amazon EC2 控制台。
2. 选择 **Network Interfaces**（网络接口） > **Create Network Interfaces**（创建网络接口）。
3. 输入新接口的描述性 **Name**（名称）。
4. 在 **Subnet**（子网）下，选择主动防火墙的不可信接口的子网。
5. 在 **Private IP**（专用 **IP** 地址）下，将字段留空以允许 AWS 动态分配 IP 地址，或输入主动防火墙不可信接口的子网范围内的 IP 地址。
6. 在 **Security groups**（安全组）下，选择一个或多个安全组。
7. 选择 **Yes**（是），然后选择 **Create**（创建）。
8. 选择 **Actions**（操作） > **Change Source/Dest.Check**（更改源/目标检查），然后选择 **Disable**（禁用）。
9. 对于主动防火墙可信接口的子网，请重复执行这些步骤。

STEP 7 | 将新的 ENI 附加到被动防火墙实例。您必须按照正确的顺序将这些 ENI 附加到被动防火墙，因为辅助 IP HA 方法基于 AWS 分配的网络接口索引。例如，如果主动防火墙上的 eth1/2 是子网 A 的一部分，eth1/3 是子网 B 的一部分，则必须附加既是子网 A 的一部分又是子网 B 的一部分的接口。在本例中，AWS 将索引值 2 分配给 eth1/2，将索引值 3 分配给 eth1/3。必须维护此索引才能成功进行故障转移。

1. 要附加上面创建的 ENI，选择您创建的不可信接口，然后单击 **Attach**（附加）。
2. 选择被动防火墙的实例 ID，然后单击 **Attach**（附加）。
3. 对于可信接口，请重复执行这些步骤。

STEP 8 | 登录到被动防火墙，并设置接口以通过 DHCP 获取其 IP 地址。

1. 登录到被动 VM 系列防火墙 Web 接口。
2. 选择 **Network**（网络） > **Interfaces**（接口）。
3. 单击第一个数据接口。
4. 选择 **IPv4**。
5. 选择 **DHCP Client**（**DHCP** 客户端）。
6. 仅限在不可信接口上，选择 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）。
7. 单击 OK（确定）。
8. 对于每个数据接口，请重复执行此过程。

©2024 Palo Alto Networks, Inc.

STEP 9 | 如果您已在 VM 系列防火墙上配置引用数据接口的专用 IP 地址的任何 NAT 策略，则必须更新这些策略以引用新分配的辅助 IP 地址。

1. 访问主动 VM 系列防火墙的 Web 界面。
2. 选择 **Policies**（策略） > **NAT**。
3. 单击要修改的 NAT 策略规则，然后单击 **Translated Packet**（转换后的数据包）。
4. 在 **Translated Address**（转换后的数据包）下，单击 Add（添加），然后输入在 AWS 中创建的辅助 IP 地址。
5. 删除主 IP 地址。
6. 单击 **OK**（确定）。
7. 根据需要重复执行这些步骤。
8. **Commit**（提交）更改。

STEP 10 | 启用辅助 IP HA 故障转移模式。

1. 在主动对等上访问 VM 系列防火墙 CLI。
2. 执行以下命令。

   ```
   request plugins vm_series aws ha failover-mode secondary-ip
   ```
3. 提交更改。
4. 通过执行以下命令确认 HA 模式。

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. 在被动对等上重复执行此命令。

STEP 11 | 在完成两个防火墙的配置 HA 后，验证防火墙是否已在主动/被动 HA 中配对。

1. 访问两个防火墙上的 **Dashboard**（仪表盘），并查看高可用性小部件。
2. 在主动 HA 对等上，单击 **Sync to peer**（同步到对等）。
3. 确认防火墙已配对并同步。
   - 在被动防火墙上：本地防火墙的状态应显示 **Passive**（被动），并且 **Running Config**（运行配置）应显示为 Synchronized（已同步）。
   - 在主动防火墙上：本地防火墙的状态应显示 **Active**（主动），并且 **Running Config**（运行配置）应显示为 Synchronized（已同步）。
4. 在防火墙命令行界面中，执行以下命令：
   - 验证故障转移就绪情况：

     ```
     show plugins vm_series aws ha state
     ```
   - 显示辅助 IP 映射：

     ```
     show plugins vm_series aws ha ips
     ```


©2024 Palo Alto Networks, Inc.

在 AWS 上将主动/被动 HA 迁移到接口移动模式

完成以下过程，以将现有的 VM 系列防火墙 HA 对从辅助 IP HA 迁移到接口移动 HA。

STEP 1 | 支持在被动 HA 对等上禁用 DPDK。接口移动 HA 模式不支持 DPDK，因此您必须将其禁用；启用 Packet MMAP。

1. 登录到被动防火墙 CLI。
2. 使用以下命令禁用 DPDK。执行此命令重新启动防火墙。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 2 | 支持在主动 HA 对等上禁用 DPDK。

1. 登录到主动防火墙 CLI。
2. 使用以下命令禁用 DPDK。执行此命令重新启动防火墙。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

   重新启动防火墙将会影响流量。

STEP 3 | 在主动对等上将 HA 模式从辅助 IP 模式更改为接口移动模式。

1. 在主动对等上访问 VM 系列防火墙 CLI。
2. 执行以下命令。

   ```
   request plugins vm_series aws ha failover-mode interface-move
   ```
3. 提交更改。
4. 通过执行以下命令确认 HA 模式。

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. 在被动对等上重复执行此命令。

STEP 4 | 从被动防火墙实例删除数据接口。

1. 登录到 AWS EC2 控制台。
2. 选择 **Network Interfaces**（网络接口）。
3. 选择被动防火墙实例上的数据接口，然后单击 **Delete**（删除）。
4. 在 **Delete Network Interface**（删除网络接口）窗口中，单击 **Yes, Delete**（是，删除）。
5. 对于被动防火墙实例上的每个数据接口，请重复执行此过程。

©2024 Palo Alto Networks, Inc.

使用 AWS 机密管理器存储 VM 系列证书

您可以集成云原生密钥管理器来存储证书。用于证书的私钥不存储在防火墙的硬盘上，从而消除了安全问题。管理员在云存储中保留证书和私钥。防火墙使用 AWS 机密管理器从云存储中检索证书和私钥，并将其用于解密和 IPSec 等功能。

仅支持 *VM* 系列防火墙通过 *AWS* 机密管理器启用证书检索。如果使用 *AWS* 机密管理器证书，则无法降级到早期版本的 *PAN-OS*。

对于出站和入站解密，将证书上传到原生密钥管理器并向 NGFW 提供所需的访问权限。

公共云上的 NGFW 可使用 AWS 机密管理器来存储证书。在这种情况下，请使用 PAN-OS 或 CLI 为相同的实例配置所需的访问管理策略。

对于使用自动缩放的环境，实例在检索到必要证书并准备好解密流量的状态下启动，无需额外的手动配置。

在云中更新证书时，必须将其作为新证书重新导入防火墙中。您必须将 IAM 角色分配给一个实例，从而使该实例能够从 AWS 机密管理器存储中检索证书。IAM 角色必须具有从 AWS 机密管理器获取机密的权限。

当主密钥发生更改时，将删除所有证书，然后在提交时重新获取。当配置同步到 *HA* 下的被动防火墙时，证书由被动防火墙上的管理守护程序自动下载。结果是不会同步证书。

STEP 1 | 在 AWS 管理控制台中创建 IAM 角色，或者选择之前创建的角色。使用的 IAM 角色必须具有读/写权限

STEP 2 | 在 AWS 控制台的 **Instances**（实例）部分选择 **IAM Role**（**IAM** 角色）策略以查看 **Secrets Manager**（机密管理器）。

STEP 3 | 在 **Permissions**（权限）选项卡中，选择 **Secrets Manager**（机密管理器）。您将使用此屏幕查看公钥和私钥。

STEP 4 | 在 **Secrets**（机密）屏幕中，选择与 IAM 角色相关联的机密文件的名称。

STEP 5 | 在 **Secret**（机密）字段中，选择 **Key/value**（键/值）以显示私钥和公钥。两个键应相同。此外，私钥或公钥必须与 AWS 在机密管理器中期望的格式相匹配。如果格式不匹配，则密钥检索会失败。

Rotation configuration（轮换配置）选项必须是 **Disabled**（禁用）。不支持此功能。

STEP 6 | 返回到资源组并选择 VM 系列防火墙。单击 **Identity**（标识）> **User Assigned**（分配的用户）并添加 **Managed Identity**（托管标识）。

STEP 7 | 返回机密管理器并选择 **Certificates**（证书）。导入证书。

©2024 Palo Alto Networks, Inc.

STEP 8 | 登录到 VM 系列防火墙。

STEP 9 | 选择 **Device**（设备）> **Certificate**（证书）**Management**（管理）> **Certificates**（证书）> **Import**（导入）。

STEP 10 | 在 **Cloud**（云）下，输入证书名称并设置文件格式。

STEP 11 | 选择 **Cloud**（云），从 **Cloud Platform**（云平台）下拉列表中选择 **AWS**：

1. 输入 **Certificate Name**（证书名称）；从 **AWS Secrets Manager**（**AWS** 机密管理器）> **Secrets**（机密）中的 **Certificate Name**（证书名称）字段中复制证书名称。
2. 选择 **AWS** 作为 **Cloud Platform**（云平台）。
3. 输入 **Cloud Secret Name**（云机密名称）；从 **AWS Secrets Manager**（**AWS** 机密管理器）> **Secrets**（机密）中的 **Secret Name** （机密名称）字段中复制机密名称。
4. 您可以在证书信息屏幕中指定 **Algorithm**（算法）。为配置选择算法 **RSA** 或 **Elliptical Curve DSA**（椭圆曲线 **DSA**）。默认情况下，算法设置为使用 **RSA**。配置证书以使用 转发信任证书、转发不信任证书或信任的根 **CA**。您也可以选择证书的所有算法。
5. 单击 **OK**（确定）。
6. 提交更改。

STEP 12 | 验证证书是否添加成功：

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
2. 随即会列出新证书。

证书详细信息不会显示在 **Certificates**（证书）

屏幕中。要在 CLI 中查看此信息，请使用命令：

```
show shared certificate
```

<cert-name>

证书详细信息不会显示在 **Certificates**（证书）

屏幕中。要在 CLI 中查看此信息，请使用命令：

```
show shared certificate
```

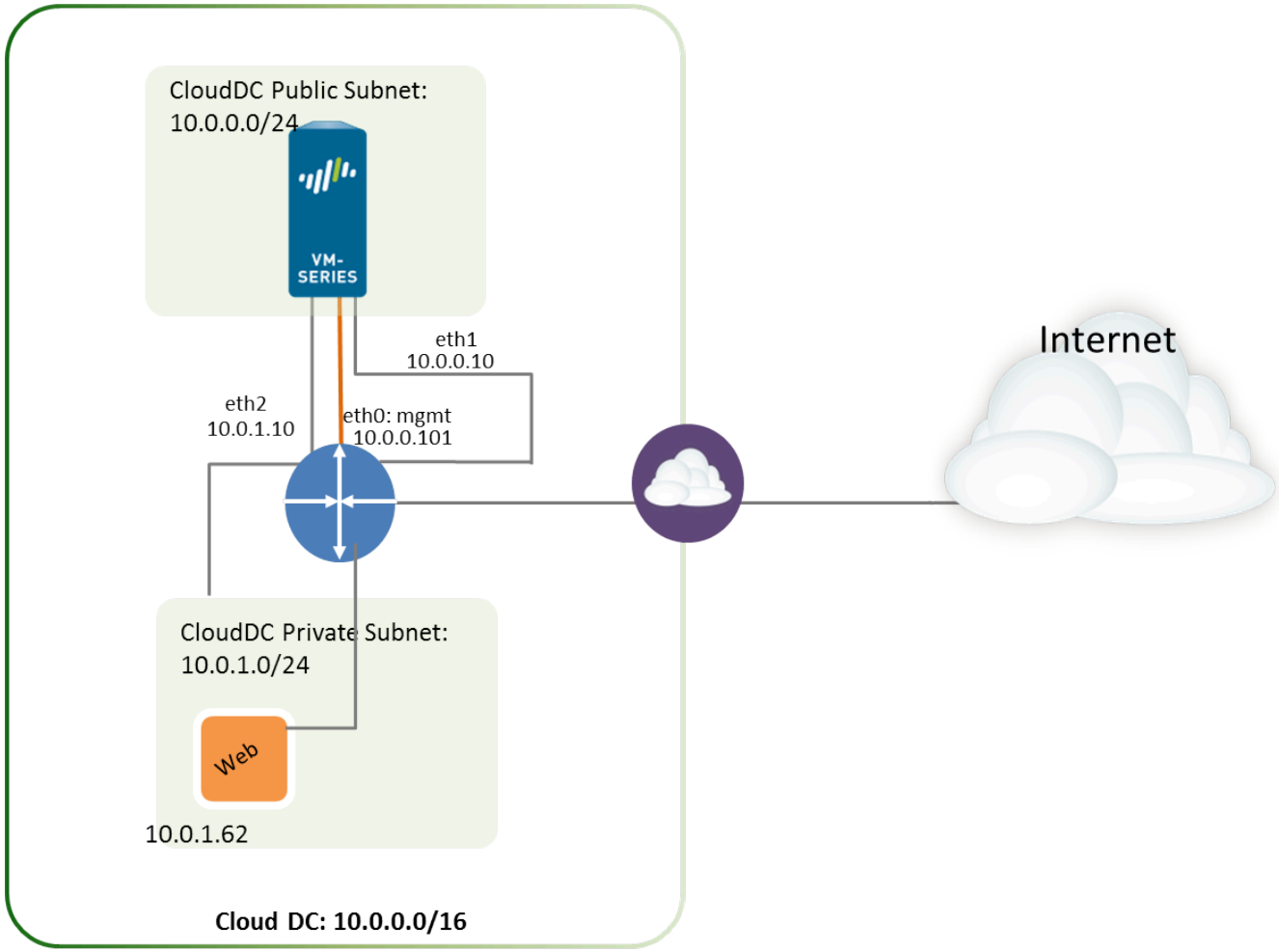
<cert-name>

您可以在 Panorama 中确认证书集成的配置。在设备证书窗口中确定是否使用了证书。请记住，由于数据未存储在运行配置（硬盘驱动器）中，因此，**Device Certificates**（设备证书）表中的所有字段均为空，**Usage**（使用情况）字段（如果已配置）和 **Cloud Secret Name**（云机密名称）除外。

©2024 Palo Alto Networks, Inc.

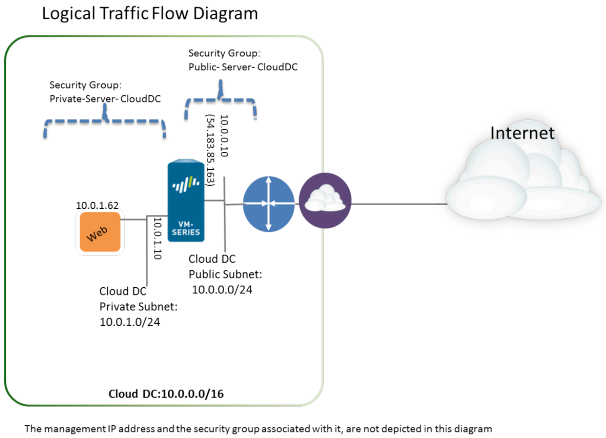
用例：保护 AWS 云中的 EC2 实例

在本示例中，VPC 部署于拥有两个 /24 子网的 10.0.0.0/16 网络中：10.0.0.0/24 和 10.0.1.0/24。可以在其中附加 Internet 网关的 10.0.0.0/24 子网中启用 VM 系列防火墙。10.0.1.0/24 子网是一个私有子网，将用于托管需要由 VM 系列防火墙保护的 EC2 实例；此私有子网中的任何服务器都使用可路由 IP 地址（即弹性 IP 地址）的 NAT 访问 Internet。使用WS VPC 中 VM 系列防火墙的规划工作表规划 VPC 中的设计；记录 EC2 实例的子网范围、网络接口和相关联的 IP 地址以及安全组，将会使设置流程变得更轻松和有效。



下图说明了流量流向/来自 Internet 中 Web 服务器的逻辑流程。已将流向/来自 Web 服务器的流量发送到附加到私有子网的 VM 系列防火墙的数据接口。防火墙应用策略和进程传入/传出来自/流向 VPC 的 Internet 网关的流量。该图还显示了已附加数据接口的安全组。

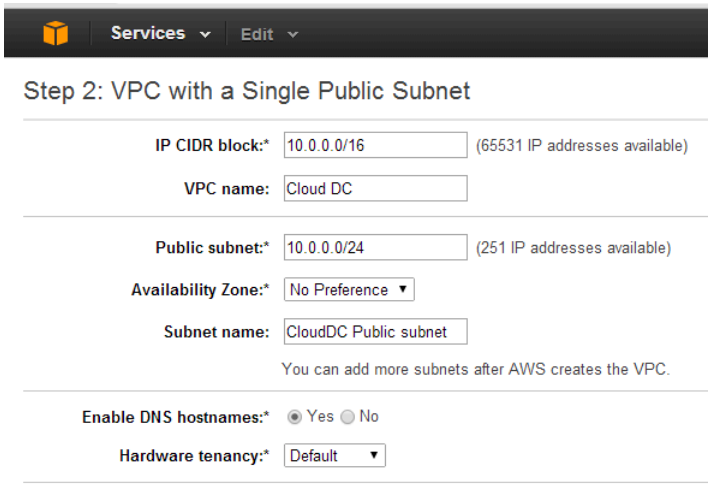
©2024 Palo Alto Networks, Inc.



STEP 1 | 使用公共子网创建新的 VPC（或选择现有的 VPC）。

1. 登录到 AWS 控制台，然后选择 **VPC** 仪表盘。
2. 确认您已选择正确的地理区域（AWS 区域）。将会在目前选定的区域中部署 VPC。
3. 选择 **Start VPC Wizard**（启动 **VPC** 向导），并选择 **VPC with a Single Public Subnet**（拥有单个公共子网的 **VPC**）。

   在本示例中，VPC 的 IP CIDR 块为 10.0.0.0/16，VPC 名称为 Cloud DC；公共子网为 10.0.0.0/24，子网名称为 Cloud DC 公共子网。创建 VPC 后，您将会创建私有子网。



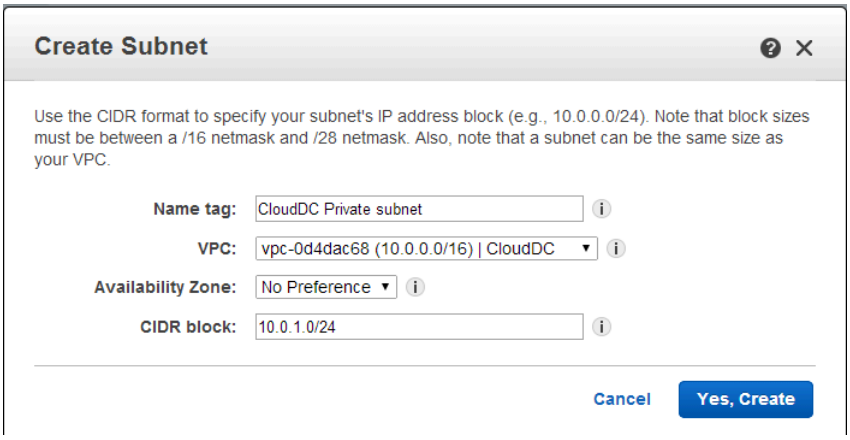
4. 单击 **Create VPC**（创建 VPC）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 创建私有子网。

选择 **Subnets**（子网），并单击 **Create Subnet**（创建子网）。填写所需的信息。

在本示例中，子网的 **Name tag**（名称标记）为 Web/DB Server Subnet，在 Cloud Datacenter VPC 中创建和分配的 CIDR 块为 10.0.1.0/24。



©2024 Palo Alto Networks, Inc.

STEP 3 | 为每个子网创建新的路由表。

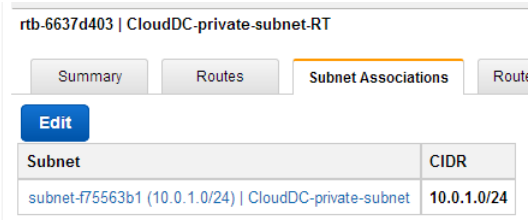
尽管已经在 *VPC* 中自动创建主路由表，但我们建议您创建新的路由表，而不是修改默认路由表。

要直接出站来自每个子网的流量，您稍后可以在此工作流程中将与每个子网相关联的路由添加到路由表。

1. 选择 **Route Tables**（路由表）> **Create Route Table**（创建路由表）。
2. 添加 **Name**（名称）（如 CloudDC-public-subnet-RT），选择在步骤 1 中创建的 **VPC**，然后单击 **Yes, Create**（是，创建）。
3. 选择路由表，单击 **Subnet Associations**（子网关联）并选择公共子网。



4. 选择 **Create Route Table**（创建路由表）。
5. 添加 **Name**（名称）（如 CloudDC-private-subnet-RT），选择在步骤 1 中创建的 **VPC**，然后单击 **Yes, Create**（是，创建）。
6. 选择路由表，单击 **Subnet Associations**（子网关联）并选择私有子网。



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 创建安全组以限制对于 VPC 中 EC2 实例的入站/出站 Internet 访问。

默认情况下，AWS 不允许在不属于同一安全组的接口之间进行通信。

选择 **Security Groups**（安全组），并单击 **Create Security Group**（创建安全组）按钮。在本示例中，我们使用以下规则为入站访问创建三个安全组：

- CloudDC-Management 指定可以连接到 VM 系列防火墙的管理接口的协议和源 IP 地址。至少需要指定 SSH 和 HTTPS。在本示例中，我们在附加到安全组的网络接口上启用 SSH、ICMP、HTTP 和 HTTPS。

  会将 VM 系列防火墙的管理接口 (eth 0/0) 分配给 CloudDC-management-sg。

- Public-Server-CloudDC 指定可以在 VPC 内通过 HTTP、FTP 和 SSH 连接的源 IP 地址。该安全组允许来自外部网络的流量流向防火墙。

  VM 系列防火墙的数据面板接口 eth1/1 将分配给 Public-Server-CloudDC。

- Private-Server-CloudDC 拥有非常有限的访问权限。它只允许位于同一子网中的其他 EC2 实例进行互相通信，以及与 VM 系列防火墙进行通信。

  VM 系列防火墙的数据面板接口 eth1/2 和私有子网中的应用程序将附加到安全组。

  以下屏幕截图显示了本用例的安全组。

Name tag	Group ID	Group Name	VPC	Description
CloudDC-private-subnet-sg	sg-6c32c409	Private-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	For Private Servers to comm...
CloudDC-public-subnet-sg	sg-6832c40d	Public-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	External Traffic to VM-Series
CloudDC-management-sg	sg-9735c3f2	CloudDC-Managment	vpc-0d4dac68 (10.0.0.0/16) |...	CloudDC-Management
	sg-1035c375	default	vpc-0d4dac68 (10.0.0.0/16) |...	default VPC security group

STEP 5 | 部署 VM 系列防火墙。

在初始启动时，只能将主网络接口用作要为防火墙附加和配置的管理接口。在步骤 6 中将会添加用于处理数据流量所需的网络接口。

请参阅在 AWS 上启动 VM 系列防火墙中所述的步骤 3。

©2024 Palo Alto Networks, Inc.

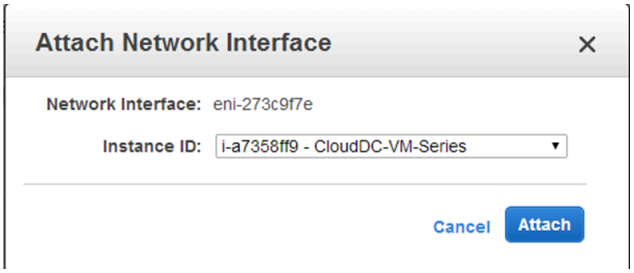
STEP 6 | 创建虚拟网络接口（称为弹性网络接口 (ENI)）并将其附加到 VM 系列防火墙。这些 ENI 都用于处理流向/来自防火墙的数据流量。

1. 在 EC2 仪表盘上，选择 **Network Interfaces**（网络接口），然后单击 **Create Network Interface**（创建网络接口）。
2. 输入隧道的描述性名称。
3. 选择子网。使用子网 ID 以确保您已选择正确的子网。您只能将 ENI 附加到同一子网中的实例。
4. 输入要分配给接口的 **Private IP**（专用 **IP**）地址或选择 **Auto-assign**（自动分配）以自动分配选定子网中可用 IP 地址内的 IP 地址。
5. 选择 **Security group**（安全组）以控制访问网络接口。
6. 单击**Yes, Create**（是，创建）。

   在本示例中，我们创建具有以下配置的两个接口：

Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	CloudDC-VM-Series-Trust	i-a7358ff9

   - 对于 Eth1/1 (VM-Series-Untrust)
     - 子网：10.0.0.0/24
     - 专用 IP：10.0.0.10
     - 安全组：Public-Server-CloudDC
   - 对于 Eth1/2 (VM-Series-Trust)
     - 子网：10.0.1.0/24
     - 专用 IP：10.0.1.10
     - 安全组：Private-Server-CloudDC
7. 要将 ENI 附加到 VM 系列防火墙，选择刚创建的接口，然后单击 **Attach**（附加）。



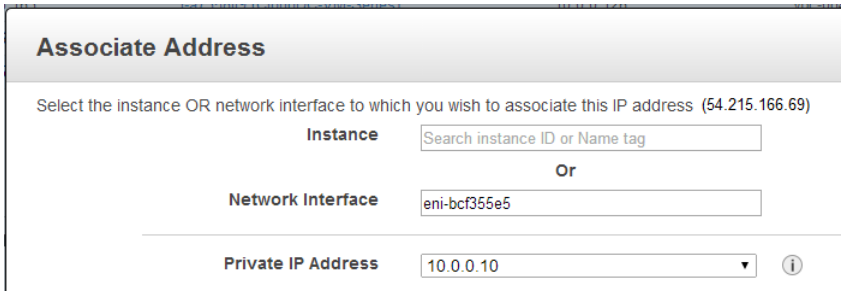
8. 选择 VM 系列防火墙的 **Instance ID**（实例 **ID**），然后单击 **Attach**（附加）。
9. 要附加其他网络接口，请重复步骤 7 和 8。

©2024 Palo Alto Networks, Inc.

STEP 7 | 创建弹性 IP 地址并将其附加到需要直接访问 Internet 的防火墙数据面板网络接口。

在本示例中，给 VM-Series_Untrust 分配了一个 EIP。与接口相关联的 EIP 是私有子网中 Web 服务器的可公共访问 IP 地址。

1. 选择 **Elastic IPs**（弹性 **IP**），然后单击 **Allocate New Address**（分配新地址）。
2. 选择 **EC2-VPC**，并单击 **Yes, Allocate**（是，分配）。
3. 选择新分配的 EIP，并单击 **Associate Address**（关联地址）。
4. 选择 **Network Interface**（网络接口）和与接口相关联的 **Private IP address**（专用 **IP** 地址），然后单击 **Yes, Associate**（是，关联）。



在本示例中，配置为：

Address	Instance	Private IP Address	Scope	Public DNS
54.183.85.163	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.126	vpc-0d4dac68	ec2-54-183-85-163.us-west-...
54.215.166.69	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.10	vpc-0d4dac68	ec2-54-215-166-69.us-west-...

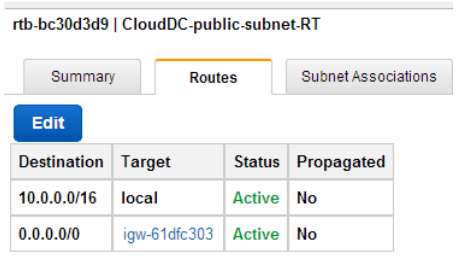
STEP 8 | 在附加到 VM 系列防火墙的每个网络接口上禁用源/目标检查。禁用此属性允许接口处理不是以其 IP 地址为目标的网络流量。

1. 在 **Network Interfaces**（网络接口）选项卡中选择网络接口。
2. 在 **Action**（操作）下拉列表中，选择 **Change Source/Dest.Check**（更改源/目标检查）。
3. 单击 **Disabled**（已禁用）并 **Save**（保存）您的更改。
4. 在本示例中，对于其他网络接口 firewall-1/2，请重复步骤 1-3。

©2024 Palo Alto Networks, Inc.

STEP 9 | 在与公共子网相关联的路由表中（从步骤 3 开始），将默认路由添加到 VPC 的 Internet 网关。

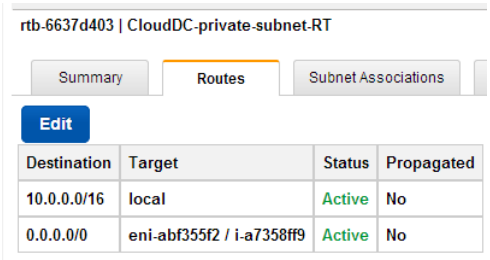
1. 在 VPC 仪表盘上，选择 **Route Tables**（路由表），并找到与公共子网相关联的路由表。
2. 选择路由表，选择 **Routes**（路由），并单击 **Edit**（编辑）。
3. 添加路由以将数据包从此子网转发到 Internet 网关。在本例中，0.0.0.0 表示来自/流向此子网的所有流量都将使用已附加到 VPC 的 Internet 网关。



STEP 10 | 在与私有子网相关联的路由表中，添加默认路由以将流量发送到 VM 系列防火墙。

添加该路由可以将来自此私有子网的 EC2 实例的流量转发到 VM 系列防火墙。

1. 在 VPC 仪表盘上，选择 **Route Tables**（路由表），并找到与私有子网相关联的路由表。
2. 选择路由表，选择 **Routes**（路由），并单击 **Edit**（编辑）。
3. 添加路由以将数据包从此子网转发到驻留在同一子网的 VM 系列防火墙网络接口。在本示例中，0.0.0.0/0 表示来自/流向此子网的所有流量都将使用 VM 系列防火墙上的 eni-abf355f2（ethernet 1/2，即 CloudDC-VM-Series-Trust）。



对于在私有子网的 *EC2* 实例上部署的每个 *Web* 或数据库服务器，您还必须定义 *VM* 系列防火墙的 *IP* 地址的默认路由，以便将防火墙作为该服务器的默认网关。

在 VM 系列防火墙上执行步骤 11 到 16。

©2024 Palo Alto Networks, Inc.

STEP 11 | 配置防火墙的新管理密码。

访问防火墙的命令行界面和更改默认管理密码需要使用的 *SSH* 工具（如 *PuTTY*）。如果不使用 *SSH* 工具，则无法访问 *Web* 界面和更改默认密码。

1. 在防火墙上配置公共 IP 地址时，可以使用 SSH 工具访问 VM 系列防火墙的命令行界面 (CLI)。

   您将需要在 AWS 上启动 VM 系列防火墙中所述的步骤 3-12 中使用或创建的私钥才能访问 CLI。
2. 输入以下命令以登录到防火墙：

   ssh-i *<private_key_name>* admin@*<public-ip_address>*
3. 使用以下命令并按照屏幕上的提示配置新密码：

   配置

   set mgt-config users admin password

   提交
4. 终止 SSH 会话。

STEP 12 | 访问 VM 系列防火墙的 Web 界面。

打开 Web 浏览器，输入管理接口的 EIP。例如：https://54.183.85.163

STEP 13 | 在 VM 系列防火墙上激活许可证。仅对于 BYOL 许可证需进行此操作，而基于使用的许可证则会自动被激活。

请参阅激活许可证。

©2024 Palo Alto Networks, Inc.

STEP 14 | 在 VM 系列防火墙上，配置防火墙的数据面板网络接口作为第 3 层接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 选择 **Config**（配置）选项卡，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 New Zone（新建区域）。定义新区域（如 untrust），然后单击 OK（确定）。
   - 选择 IPv4，并选择 **DHCP Client**（**DHCP** 客户端）；系统会自动获取在 AWS 管理控制台中分配给网络接口的专用 IP 地址。
   - 在 **Advanced**（高级） > **Other Info**（其他信息）选项卡上，展开 Management Profile（管理配置文件）下拉列表，然后选择 **New Management Profile**（新建管理配置文件）。
   - 输入配置文件的 **Name**（名称）（如 allow_ping），并从 Permitted Services（允许的服务）列表中选择 **Ping**，然后单击 **OK**（确定）。
   - 要保存接口配置，请单击 **OK**（确定）。
3. 单击 **ethernet 1/2** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 选择 **Config**（配置）选项卡，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 trust），然后单击 **OK**（确定）。
   - 选择 **IPv4**，然后选择 **DHCP Client**（**DHCP** 客户端）。
   - 在 **IPv4** 选项卡上，取消选中 **Automatically create default route to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）复选框。对于附加到 VPC 中私有子网的接口，禁用该选项可确保由此接口处理的流量不会直接流向 VPC 上的 IGW。
   - 在 **Advanced**（高级） > **Other Info**（其他信息）选项卡上，展开“管理配置文件”下拉列表，然后选择先前创建的 allow_ping 配置文件。
   - 单击 **OK**（确定）以保存接口配置。
4. 单击 **Commit**（提交）以保存更改。验证此接口的链接状态是否正常  。 如果链路状态不正常，必须重新启动防火墙。

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	allow_ping		Dynamic-DHCP Client	default	untrust
ethernet1/2	Layer3	allow_ping		Dynamic-DHCP Client	default	trust

©2024 Palo Alto Networks, Inc.

STEP 15 | 在 VM 系列防火墙上，创建目标 NAT 和源 NAT 规则以允许流向/来自在 VPC 中部署的应用程序的入站/出站流量。

1. 选择 **Policies**（策略） > **NAT**。
2. 创建目标 NAT 规则以控制从防火墙流向 Web 服务器的流量。
   1. 单击 **Add**（添加），然后输入规则的名称。例如，NAT2WebServer。
   2. 在 **Original Packet**（原始数据包）选项卡中，作出以下选择：
      - **Source Zone**（源区域）：untrust（流量起源的区域）
      - **Destination Zone**（目标区域）：untrust（将防火墙数据面板接口与 Web 服务器的 EIP 进行相关联的区域。）
      - **Source Address**（源地址）：任何
      - **Destination Address**（目标地址）：10.0.0.10
      - 在 **Translated Packet**（转换后的数据包）选项卡中，选中 Destination Address Translation（目标地址转换）复选框，然后将 **Translated Address**（转换后的地址）设置为 10.0.1.62，该地址是 Web 服务器的专用 IP 地址。
   3. 单击 **OK**（确定）。

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62

3. 创建源 NAT 规则以允许从 Web 服务器流向 Internet 的出站流量。
   1. 单击 **Add**（添加），然后输入规则的名称。例如，NAT2External。
   2. 在 **Original Packet**（原始数据包）选项卡中，作出以下选择：
      - **Source Zone**（源区域）：trust（流量起源的区域）
      - **Destination Zone**（目标区域）：untrust（将防火墙数据面板接口与 Web 服务器的 EIP 进行相关联的区域。）
      - **Source Address**（源地址）：任何
      - **Destination Address**（目标地址）：任何
   3. 在 **Translated Packet**（转换后的数据包）选项卡中，在 Source Address Translation（源地址转换）部分中作出以下选择：
      - **Translation Type**（转换类型）：动态 IP 和端口
      - **Address Type**（地址类型）：转换后的地址
      - 转换后的地址：10.0.0.10（untrust 区域中的防火墙数据面板接口。）
   4. 单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62
2	NAT2External	none	trust	untrust	any	any	any	any	dynamic-ip-and-port 10.0.0.10	none

4. 单击 **Commit**（提交）以保存 NAT 策略。

©2024 Palo Alto Networks, Inc.

STEP 16 | 在 VM 系列防火墙上，创建安全策略用于管理流量。

不是使用 *Web* 服务器的静态 *IP* 地址，而是使用动态地址组。动态地址组可让您创建自动适应变化的策略，这样您就不需要在子网中启动其他 *Web* 服务器时更新策略。有关详情，请参阅用例：使用动态地址组保护 VPC 中的新 EC2 实例。

1. 选择 **Policies**（策略） > **Security**（安全）。

   在本示例中，我们拥有四个规则。第一个规则允许对于防火墙流量的管理访问，第二个规则允许 Web 服务器的入站流量，第三个规则允许对于 Web 服务器的 Internet 访问，第四个规则允许我们修改预定义的 intrazone-default 规则以记录拒绝的所有流量。

2. 创建规则以允许对于防火墙的管理访问。

   1. 单击 **Add**（添加），然后输入规则的 **Name**（名称）。确认 **Rule Type**（规则类型）为 universal。
   2. 在 **Source**（源）选项卡中，添加 untrust 作为 **Source Zone**（源区域）。
   3. 在 **Destination**（目标）选项卡中，添加 trust 作为 **Destination Zone**（目标区域）。
   4. 在 **Applications**（应用程序）选项卡中，**Add**（添加）ping 和 ssh。
   5. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 Allow（允许）。
   6. 单击 **OK**（确定）。

	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
1	AllowManagement	universal	untrust	any	trust	ping ssh	application-default	✓	none	

3. 创建规则以允许 Web 服务器的入站流量。

   1. 单击 **Add**（添加），并输入规则的 **Name**（名称），然后确认 **Rule Type**（规则类型）为 universal。
   2. 在 **Source**（源）选项卡中，添加 untrust 作为 **Source Zone**（源区域）。
   3. 在 **Destination**（目标）选项卡中，添加 trust 作为 **Destination Zone**（目标区域）。
   4. 在 **Applications**（应用程序）选项卡中，**Add**（添加）web-browsing。
   5. 在 **Service/URL Category**（服务/URL 类别）选项卡中，确认已将服务设置为 application-default。
   6. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 Allow（允许）。
   7. 在 **Actions**（操作）选项卡的 Profile Settings（配置文件设置）部分中，选择 **Profiles**（配置文件），然后附加防病毒软件、反间谍软件和漏洞保护的默认配置文件。
   8. 单击 **OK**（确定）。

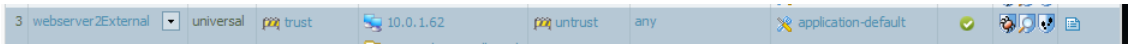
2	AllowWebAccess	universal	untrust	any	trust	web-browsing	application-default	✓		

4. 创建规则以允许对于 Web 服务器的 Internet 访问。

   1. 单击 **Add**（添加），并输入规则的 **Name**（名称），然后确认 Rule Type（规则类型）为 universal。

©2024 Palo Alto Networks, Inc.

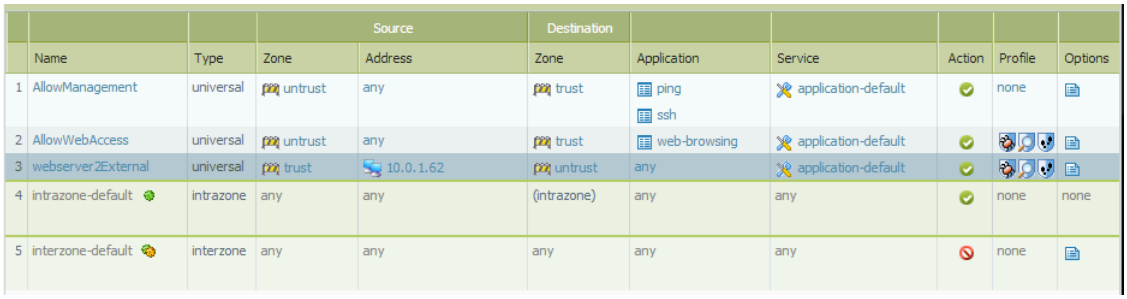
2. 在 **Source**（源）选项卡中，添加 trust 作为 **Source Zone**（源区域）。
3. 在 **Source**（源）选项卡的 Source Address（源地址）部分中，添加 10.0.1.62 作为 Web 服务器的 IP 地址。
4. 在 **Destination**（目标）选项卡中，添加 untrust 作为 **Destination Zone**（目标区域）。
5. 在 **Service/URL Category**（服务/**URL** 类别）选项卡中，确认已将服务设置为 **application-default**。
6. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 Allow（允许）。
7. 在 **Actions**（操作）选项卡的 Profile Settings（配置文件设置）部分中，选择 **Profiles**（配置文件），然后附加防病毒软件、反间谍软件和漏洞保护的默认配置文件。
8. 单击 **OK**（确定）。



5. 编辑 interzone-default 规则以记录拒绝的所有流量。当没有任何明确定义的其他规则与不同区域之间的流量相匹配时，评估此预定义的区域间规则。
   1. 选择 **interzone-default** 规则，并单击 **verride**（替代）。
   2. 在 **Actions**（操作）选项卡中，选择 **Log at session end**（在会话结束时记录）。
   3. 单击 **OK**（确定）。



6. 查看在防火墙上定义的整组安全规则。
7. 单击 **Commit**（提交）以保存策略。

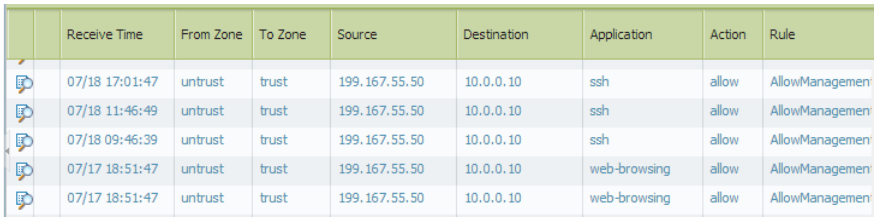


 ©2024 Palo Alto Networks, Inc.

STEP 17 | 确认 VM 系列防火墙正在保护流量。

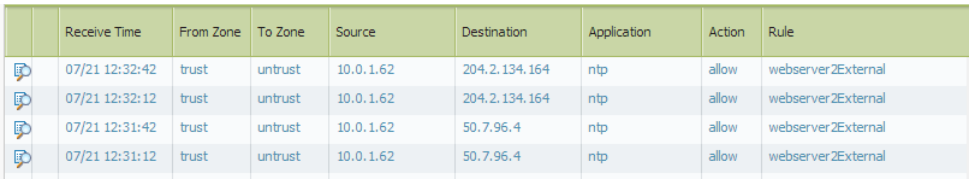
1. 启动 Web 浏览器，然后输入 Web 服务器的 IP 地址。
2. 登录到 VM 系列防火墙的 Web 界面，并确认您可以在 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）中查看会话的流量日志。

   - Web 服务器的入站流量（到达 AWS VPC 中的 EC2 实例）：



		Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
		07/18 17:01:47	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
		07/18 11:46:49	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
		07/18 09:46:39	untrust	trust	199.167.55.50	10.0.0.10	ssh	allow	AllowManagemen
		07/17 18:51:47	untrust	trust	199.167.55.50	10.0.0.10	web-browsing	allow	AllowManagemen
		07/17 18:51:47	untrust	trust	199.167.55.50	10.0.0.10	web-browsing	allow	AllowManagemen

   - Web 服务器的出站流量（AWS VPC 中的 EC2 实例）：



		Receive Time	From Zone	To Zone	Source	Destination	Application	Action	Rule
		07/21 12:32:42	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
		07/21 12:32:12	trust	untrust	10.0.1.62	204.2.134.164	ntp	allow	webserver2External
		07/21 12:31:42	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External
		07/21 12:31:12	trust	untrust	10.0.1.62	50.7.96.4	ntp	allow	webserver2External

   您已经成功部署 VM 系列防火墙作为云网关#

©2024 Palo Alto Networks, Inc.

用例：使用动态地址组保护 VPC 中的新 EC2 实例

在根据需要启动新的 EC2 实例的动态环境（如 AWS-VPC）中，管理安全策略的管理开销可能会很高。在安全策略中使用动态地址组可以灵活地防止服务中断或出现保护方面的差距。

在本示例中，您可以使用防火墙上的 VM 信息源来监控 VPC，并在安全策略中使用动态地址组发现和保护 EC2 实例。启动 EC2 实例时，动态地址组将核对与为组成员所定义的条件相匹配的所有实例的 IP 地址，然后为组应用安全策略。在本示例中，安全策略允许 Internet 访问组的所有成员。



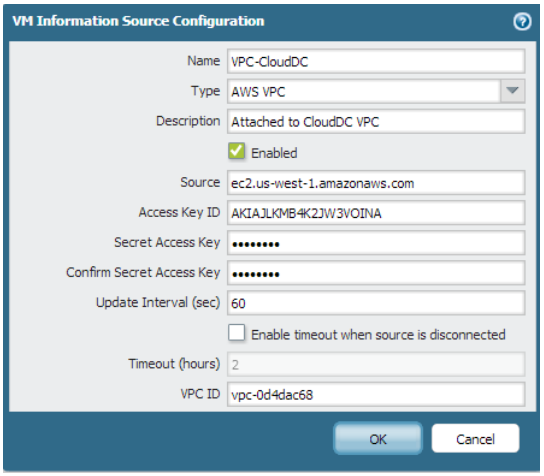
您可以选择使用 *Panorama* 作为与 *VPC* 通信的中心点，而不是使用防火墙上的 *VM* 信息源。您可以使用 *Panorama* 上的 *AWS* 插件来检索 *IP* 地址到标记映射，并在配置通知的防火墙上注册信息。有关此选项的更多详细信息，请参阅使用 Panorama 上的 AWS 插件进行 VM 监控。

以下部分中的此工作流程假设您已创建 AWS VPC，并且已在 EC2 实例上部署 VM 系列防火墙和一些应用程序。有关为 VM 系列防火墙设置 VPC 的说明，请参阅用例：保护 AWS 云中的 EC2 实例。

©2024 Palo Alto Networks, Inc.

STEP 1 | 配置防火墙以监控 VPC。

1. 选择 **Device**（设备）> **VM Information Sources**（**VM** 信息源）。
2. 单击**Add**（添加），并输入以下信息：
   1. **Name**（名称）用于标识要监控的 VPC。例如，VPC-CloudDC。
   2. 将 **Type**（类型）设置为 AWS VPC。
   3. 在 **Source**（源）选项卡中，输入 VPC 的 URI。语法是 **ec2.*<your_region>*.amazonaws.com**
   4. 将防火墙数字签名 API 调用模式所需的凭据添加到 AWS 服务。您需要以下信息：
      - **Access Key ID**（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。
      - **Secret Access Key**（机密访问密钥）：输入密码并确认输入。
   5. （可选）将 **Update interval**（更新间隔）修改为 5 至 600 秒之间的值。默认情况下，防火墙会每隔 5 秒轮询一次。每隔 60 秒将对 API 调用进行排队和检索，从而更新需要的时间可能最长为 60 秒加上配置的轮询间隔。



   6. 输入在 AWS 管理控制台的 VPC 仪表盘上显示的 **VPC ID**。
   7. 单击**OK**（确定）并**Commit**（提交）更改。
   8. 验证连接 **Status**（状态）是否显示为 已连接。

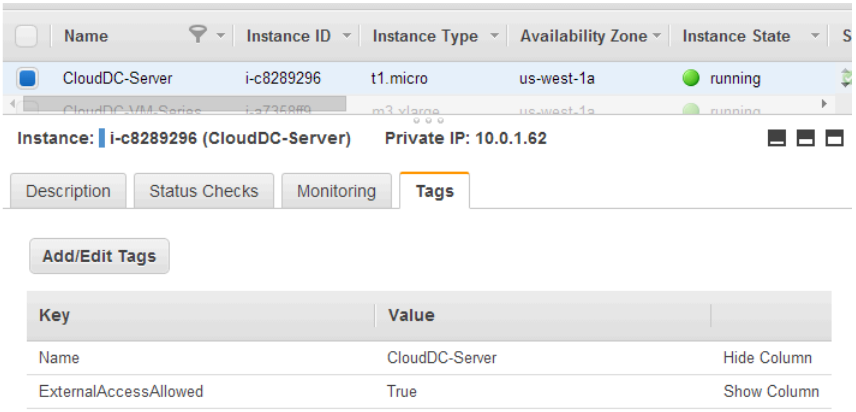
 ©2024 Palo Alto Networks, Inc.

STEP 2 | 标记 VPC 中的 EC2 实例。

有关 VM 系列防火墙可以监控的标记的列表，请参阅在 AWS VPC 上监控的属性列表。

标记是一个名称-值对。您可以在 AWS 管理控制台的 EC2 仪表盘上标记 EC2 实例，或者使用 AWS API 或 AWS CLI 标记 EC2 实例。

在本示例中，我们使用 EC2 仪表盘添加标记：

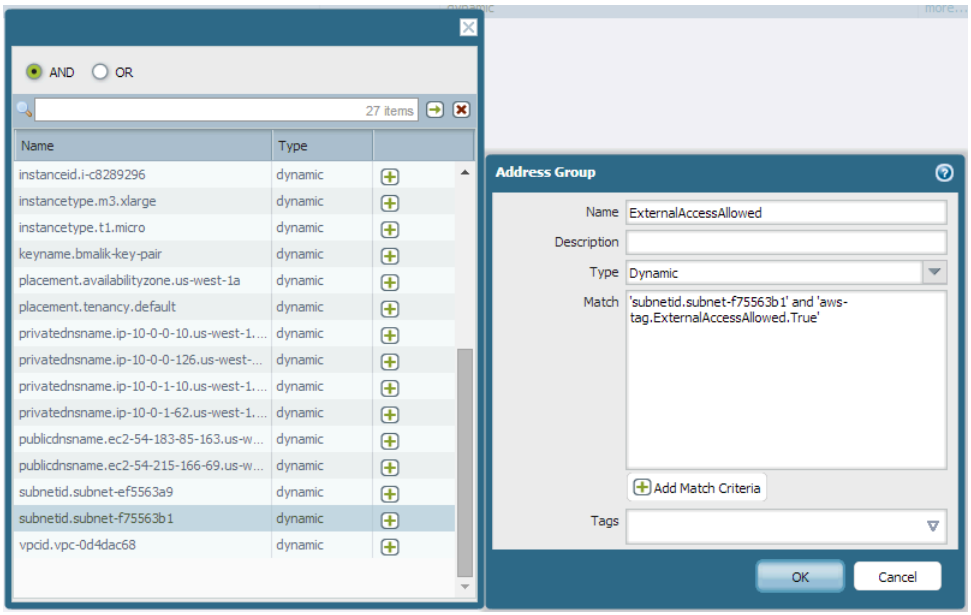


 ©2024 Palo Alto Networks, Inc.

STEP 3 | 在防火墙上创建动态地址组。

查看教程观看功能的大视图。

1. 选择 **Object**（对象） > **Address Groups**（地址组）。
2. 单击 **Add**（添加），然后为地址组输入 **Name**（名称）和 **Description**（说明）。
3. 选择 **Dynamic**（动态）作为 **Type**（类型）。
4. 定义匹配条件。
   1. 单击 **Add Match Criteria**（添加匹配条件），然后选择 **And** 运算符。
   2. 选择用于筛选或进行匹配的属性。在本示例中，我们选择刚创建的 ExternalAccessAllowed 标记和 VPC 私有子网的子网 ID。



5. 单击 **OK**（确定）。
6. 单击 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 在安全策略中使用动态地址组。

创建规则以允许对于属于动态地址组（称为 ExternalServerAccess）的所有 Web 服务器的 Internet 访问。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），并输入规则的 **Name**（名称），然后确认 **Rule Type**（规则类型）为 universal。
3. 在 **Source**（源）选项卡中，添加 trust 作为 **Source Zone**（源区域）。
4. 在 **Source**（源）选项卡的 Source Address（源地址）部分中，**Add**（添加）刚创建的 ExternalServerAccess 组。
5. 在 **Destination**（目标）选项卡中，添加 untrust 作为 **Destination Zone**（目标区域）。
6. 在 **Service/URL Category**（服务/URL 类别）选项卡中，确认已将服务设置为 **application-default**。
7. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 Allow（允许）。
8. 在 **Actions**（操作）选项卡的 Profile Settings（配置文件设置）部分中，选择 **Profiles**（配置文件），然后附加防病毒软件、反间谍软件和漏洞保护的默认配置文件。
9. 单击 **OK**（确定）。

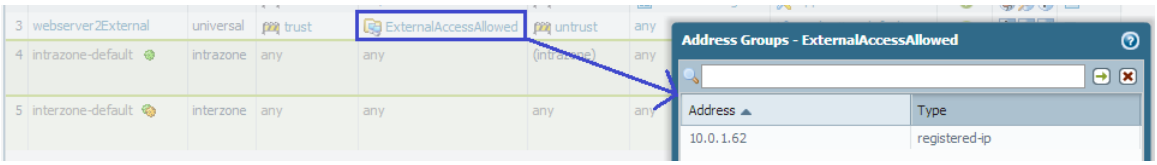


10. 单击 **Commit**（提交）。

STEP 5 | 在防火墙上验证是否已填充动态地址组的成员。

将对属于此地址组，并在此显示的所有 IP 地址实施策略。

1. 选择 **Policies**（策略） > **Security**（安全），并选择规则。
2. 选择地址组链接旁的下拉箭头，然后选择 **Inspect**（检查）。您还可以验证匹配条件是否准确。
3. 单击 **more**（更多）链接，然后验证是否显示已注册 IP 地址列表。



 ©2024 Palo Alto Networks, Inc.

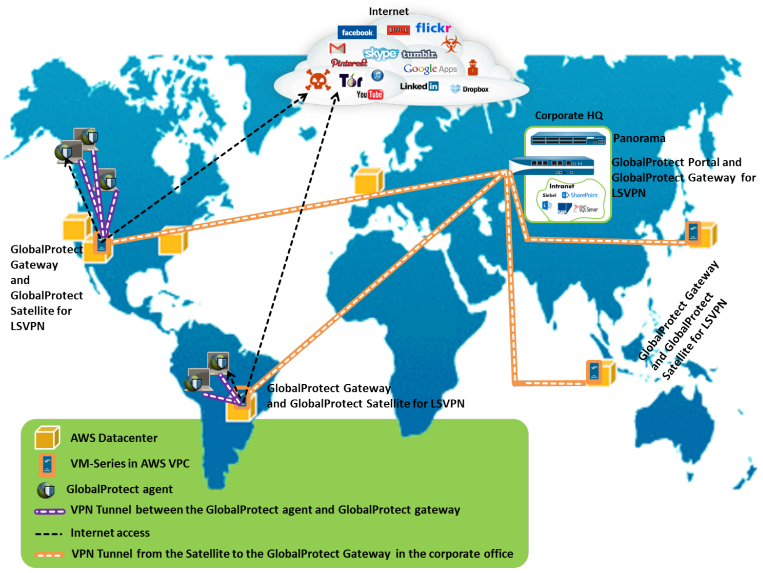
用例：VM 系列防火墙作为 AWS 上的 GlobalProtect 网关

保护移动用户免遭威胁和危险的应用程序攻击通常是采购和设置安全性和 IT 基础架构的复杂混合，不仅要确保在全球的多个地点满足拥有足够的带宽和正常运行时间要求，而且还需将其控制在预算以内。

AWS 上的 VM 系列防火墙融合了一致可靠地保护您尚未列出地区的移动用户所使用设备需要的安全性和 IT 物流。通过在 AWS 云中部署 VM 系列防火墙，您可以使用自己的资源在任何区域中快速和轻松地部署 GlobalProtect™ 网关，而不需要使用设置此基础架构通常所需的费用或 IT 物流。

为了最大限度减少延迟，应选择最靠近用户的 AWS 区域、在 EC2 实例上部署 VM 系列防火墙并配置防火墙作为 GlobalProtect 网关。使用此解决方案，AWS 云中的 GlobalProtect 网关可以为 Internet 流量执行安全策略，因此不需要回传流向企业网络的流量。此外，为了访问企业网络中的资源，AWS 上的 VM 系列防火墙可以利用 LSVPN 功能建立返回到企业网络中防火墙的 IPSec 隧道。

为了便于部署和集中管理此分布式基础架构，可以使用 Panorama 配置在此解决方案中使用的 GlobalProtect 组件。或者，如需确保在网络上安全使用移动设备（如智能手机、平板电脑等），也可以使用 Mobile Security Manager 配置和管理移动设备。



- GlobalProtect 基础架构的组件
- 在 AWS 上部署 GlobalProtect 网关

GlobalProtect 基础架构的组件

要阻止危险的应用程序和保护移动用户免遭恶意软件攻击，您必须设置 GlobalProtect 基础架构，包括 GlobalProtect 门户、GlobalProtect 网关和 GlobalProtect 应用。此外，为了访问企业资源，您还必须使用 LSVPN（星型 VPN 部署）设置 AWS 上 VM 系列防火墙与公司总部中防火墙之间的 IPSec VPN 连接。

©2024 Palo Alto Networks, Inc.

- 同时，在允许访问企业应用程序和资源的每个最终用户系统上安装 GlobalProtect 代理/应用。首先将代理连接到门户以获取有关网关的信息，然后建立与最近的 GlobalProtect 网关的安全 VPN 连接。最终用户系统和网关之间的 VPN 连接可以确保数据隐私。
- GlobalProtect 门户提供了针对 GlobalProtect 基础架构的管理功能。每个最终用户端系统都会从门户收到配置信息，包括可用网关的相关信息以及连接到 GlobalProtect 网关时可能需要的任何客户端证书的相关信息。在此用例中，GlobalProtect 门户是一个在公司总部中部署的基于硬件的防火墙。
- GlobalProtect 网关根据应用程序、用户、内容、设备和设备状态提供移动威胁防御和实施策略。在此用例中，可以将 AWS 上的 VM 系列防火墙用作 GlobalProtect 网关。GlobalProtect 网关扫描恶意软件和其他威胁的每个用户请求，并且如果策略允许，它将会通过 IPSec 隧道（至 LSVPN 网关）将请求发送到 Internet 或企业网络。
- 对于 LSVPN，您必须配置 GlobalProtect 门户、LSVPN 的 GlobalProtect 网关（中心型）和 GlobalProtect 卫星（辐射型）。

  在本用例中，在企业办公室中部署基于硬件的防火墙作为 GlobalProtect 门户和 LSVPN 网关。已经配置 AWS 上的 VM 系列防火墙作为 GlobalProtect 卫星。另外，也已经配置 GlobalProtect 卫星和网关以建立可在网关上终止的 IPSec 隧道。当移动用户请求驻留在企业网络中的应用程序或资源时，VM 系列防火墙通过 IPSec 隧道路由请求。

在 AWS 上部署 GlobalProtect 网关

为了保护移动用户，除在 AWS 上部署和配置 GlobalProtect 网关以外，您还需要设置此集成解决方案所需的其他组件。下表包括建议的工作流程：

在 AWS 上部署 VM 系列防火墙。

请参阅在 AWS 上部署 VM 系列防火墙。

在公司总部配置防火墙。

在本用例中，已配置防火墙作为 GlobalProtect 门户和 LSVPN 网关。

- 配置 lobalProtectportal。
- 为 LSVPN 配置 GlobalProtectportal。
- 配置门户以验证 LSVPN 卫星。
- 为 LSVPN 配置 GlobalProtect 网关。

©2024 Palo Alto Networks, Inc.

在 Panorama 上设置模板用来配置 AWS 上的 VM 系列防火墙作为 GlobalProtect 网关和 LSVPN 卫星。

要轻松管理此分布式部署，使用 Panorama 配置 AWS 上的防火墙。

- 在 Panorama 上创建模板。

然后，使用以下链接定义模板中的配置。

- 配置防火墙作为 GlobalProtect 网关。
- 准备卫星加入 LSVPN。

在 Panorama 上创建设备组以定义网络访问策略和 Internet 访问规则，并将它们应用到 AWS 上的防火墙。

请参阅创建设备组。

将模板和设备组应用到 AWS 上的 VM 系列防火墙，并确认已正确配置防火墙。

部署 GlobalProtect 客户端软件。

每个最终用户系统都需要 GlobalProtect 代理或应用连接到 GlobalProtect 网关。

请参阅部署 GlobalProtect 客户端软件。

©2024 Palo Alto Networks, Inc.

AWS 上的资源监控

在 AWS 公共云中部署或终止资源时，可以使用 AWS 的 Panorama 插件或使用防火墙上的 AWS 资源信息源对这些工作负载统一执行安全策略。有关 Panorama 插件版本信息，请参阅兼容性矩阵。

用于 AWS 的 Panorama 插件为扩展而构建，允许最多可监控 AWS 公共云上的 1000 个 AWS VPC。您可以通过此插件将 Panorama 用作轮询 AWS 帐户标记的锚，然后将元数据（IP 地址到标记映射）分发到设备组中的许多防火墙。因为 Panorama 与您的 AWS 帐户进行通信以检索 AWS 资源信息，因此，您可以简化云环境中使用的 API 调用数量。使用 Panorama 和 AWS 插件时，可以集中检索标记和安全策略管理，确保混合和云端本地架构使用的策略一致。请参阅在 Panorama 上使用 AWS 插件监控 AWS 资源。

如果您没有 Panorama 或是您的部署更简单，且需要监控 10 个或更少的 VPC，则可以使用防火墙（硬件或 VM 系列防火墙）上的 VM 信息源监控您的 AWS 工作负载。您可以在动态地址组内使用防火墙检索到的元数据，并引用至安全策略，确保 VM 工作负载在其启动或关闭且 IP 地址频繁更改时的安全。请参阅用例：使用动态地址组保护 VPC 中的新 EC2 实例。

在 Panorama 上使用 AWS 插件进行 AWS 资源监控

在 AWS 公共云中部署或终止资源时，需要一种同步更新 Palo Alto Networks® 防火墙上安全策略的方法，以便确保这些 EC2 实例的安全。要从 Panorama 启用此功能，必须在 Panorama 上安装 AWS 插件，并在 Panorama 和 AWS VPC 之间启用 API 通信。然后，Panorama 可以收集用作 AWS 资源标签的预定义属性集（或元数据元素集），并将信息注册到您的 Palo Alto Networks® 防火墙。当您在动态地址组内引用这些标记，并将其与安全策略规则内的标记进行匹配时，可以在 AWS 帐户内部署的所有资产中统一执行该策略。

- 在 Panorama 上设置用于监控的 AWS 插件
- 在 AWS VPC 上监控的属性列表

在 Panorama 上设置用于 VM 监控的 AWS 插件

要找到组织在 AWS 公共云中部署的所有虚拟机工作负载，则必须在 Panorama 上安装 AWS 插件，并配置促使 Panorama 对 AWS VPC 进行身份验证且检索工作负载上的 VM 信息的监控定义。Panorama 检索正在运行的 VM IP 地址（即，公共 IP 地址以及主要和次要专用 IP 地址）和关联标记。有关 Panorama 支持的元数据元素列表，请参阅在 AWS VPC 上监控的属性列表。

Panorama 获得属性后，将虚拟机信息从 Panorama 推送到防火墙，因此，必须将防火墙（硬件或 VM 系列）添加为 Panorama 上的托管设备，并将防火墙分组到一个或多个设备组。然后，可以指定属于通知组的设备组，这是监控定义的配置元素，Panorama 可用于注册从 AWS 检索到的 IP 地址到标记映射。

最后，要在 EC2 实例中统一实施安全策略，则必须设置动态地址组，并在用于允许或拒绝流向 VM IP 地址的流量的策略规则中加以引用。为了从 Panorama 集中简化您的配置，管理策略和对象，您可以在 Panorama 上定义动态地址组和安全策略规则，并将其推送到防火墙，而不是对每个防火墙上的动态地址组和安全策略规则进行本地管理。

©2024 Palo Alto Networks, Inc.

AWS 插件版本 *3.0.1* 或更高版本用于监控 *AWS* 公共云、*AWS GovCloud* 和 *AWS China* 上最多 *1000* 个 *VPC* 的 *EC2* 实例。但是，由于无法将 *Panorama* 部署在 *AWS China* 上，因此 *IAM* 角色不支持 *AWS China* 上的实例配置文件；您必须提供 *AWS* 凭据。

- 规划 AWS 上的 VM 监控清单
- Panorama 的 IAM 角色和权限
- 安装或升级 AWS 插件
- 配置用于 VM 监控的 AWS 插件

规划 AWS 上的 VM 监控清单

要使 Panorama 与 AWS API 交互，并收集 EC2 实例上的信息，则需要创建一个 IAM 角色，并将用于授予 AWS 身份验证以及访问 VPC 内 EC2 实例所需权限的策略进行分配。您可以添加 100 个 IAM 角色来管理 Panorama 上的最多 1000 个 VPC。

- 收集 VPC ID。
- 标记 AWS 上的 EC2 实例。您可以在 AWS 管理控制台的 EC2 仪表盘上标记（定义名称值对）EC2 实例，或者使用 AWS API 或 AWS CLI 标记（定义一个名称值对）EC2 实例。有关受支持的属性，请参阅在 AWS VPC 上监控的属性列表。
- 检查要启用监控的 VPC 上的重复 IP 地址。如果在 AWS VPC 中存在重复 IP 地址，则元数据将附加在一起或交换，这可能会导致策略执行出现意外结果。

  重复的 *IP* 地址写入可以从 *Panorama* 上的 *CLI* 访问的 *plugin_aws_ret.log* 文件。

- 查看 Panorama 和托管防火墙的要求：
  - 系统最低要求 — Panorama 虚拟设备或基于硬件的 Panorama 设备。

Panorama 最低要求				
系统资源	内存	CPU 数量	监控的 VPC 数量	注册的标记数量
	16GB	4	1-100	带有 AWS 插件 v2.0（或更高版本）的 Panorama 9.1 已经过测试，可检索每个具有 13 个标记的 10,000 个 IP 地址，或每个具有 25 个标记的 5000 个 IP 地址，并将它们成功注册到设备组中包含的防火墙。对于每个 EC2 实例，每个标记的长度（包括名称和值）假设为 64 个字节。例如，EC2 实例名称标记为 aws.ec2.tag.Name.prod-web-app-4523-lvss6j。
	32 GB	8	100-500	
	64 GB	16	500-1000	

©2024 Palo Alto Networks, Inc.

Panorama 最低要求	
Panorama 操作系统版本	10.0.5 或更高版本
AWS 插件版本	3.0.1 或更高版本
许可证	Panorama 上用于管理防火墙的有效支持许可证和设备管理许可证。 下一代防火墙必须具有有效的支持许可证。
在 EC2 实例上检索元数据的角色和权限	请参阅Panorama 的 IAM 角色和权限

- 必须在 Panorama 上添加防火墙作为托管设备，并创建设备组，这样，您可以配置 Panorama 以将检索到的 VM 信息通知这些组。设备组可以包括 VM 系列防火墙或是硬件防火墙上的虚拟系统。
- 如果 Panorama 设备具有高可用性配置，则必须手动在两个 Panorama 对等上安装相同版本的 AWS 插件。此外，如果您使用实例配置文件，必须将相同的实例配置文件附加到两个 Panorama 对等。

  您只能在 *Panorama* 主动对等上配置 *AWS* 插件。提交时，配置同步到 *Panorama* 被动对等。仅 *Panorama* 主动对等轮询用于 *VM* 监控的 *AWS* 帐户。
- 设置 Panorama 数字签名 API 调用模式所需的凭据/权限用于 AWS 服务。

  您可以选择是否要提供支持访问每个 AWS 帐户中的资源的长期凭据（访问密钥 ID 和机密访问密钥），或者设置AWS 上的假定角色，从而允许访问同一 AWS 帐户或跨帐户中定义的 AWS 资源。使用“假定角色”，您必须设置可信关系并在创建角色时定义权限。这在跨帐户部署中非常有用，因为在这种情况下，查询帐户没有权限查看或处理来自查询帐户的数据。要使 Panorama 插件成功通过 VPC 验证并检索标记，您必须配置“假定角色”，从而将 AWS Security Token Service (STS) API 用于任何 AWS 服务。查询帐户中的用户必须具有 STS 权限才能查询“假定角色”，并获取临时安全凭证来访问资源。如果 Panorama 部署在 AWS 上，您可以选择使用实例配置文件，而不是为 IAM 角色提供 AWS 凭据。实例配置文件包括 Panorama 以数字方式签名对 AWS 服务的 API 调用所需的角色信息和关联凭据。有关更多详细信息，请参阅Panorama 的 IAM 角色和权限。

Panorama 的 IAM 角色和权限

使用 AWS 插件，您可以使用 IAM 角色或实例配置文件支持 Panorama 在 AWS 帐户中部署的资源上进行身份验证和检索元数据。

- 如果 Panorama 未部署在 AWS 上，您有两种选择。您可以为要监控的 AWS 帐户提供长期 IAM 凭据，也可以在 AWS 上设置承担角色以允许访问同一 AWS 帐户或跨帐户中的已定义 AWS 资源。建议将承担角色作为更安全的选项。

©2024 Palo Alto Networks, Inc.

- 在 AWS 上部署 Panorama 时，除上面所列的两个选项以外，您还可以添加允许将 IAM 角色传递给 EC2 实例的实例配置文件。您可以使用将所有监控资源和 Panorama 托管在同一帐户中的实例配置文件，或具有 Panorama 和监控资源部署在不同 AWS 帐户之间进行跨帐户访问的承担角色的实例配置文件。如果您使用实例配置文件，则无需在 Panorama 上输入 AWS 凭据。

选项 **1**：具有长期凭据的 **IAM** 角色	
所需的角色和权限	与具有要监控的 VPC/EC2 实例的 AWS 帐户相关联的 AWS 凭据。 与具有长期凭据的 IAM 角色相关联的最低权限的 JSON 格式如下所示： `{ “Version”:“2012-10-17", “Statement”: [ { “Sid”:“VisualEditor0”, “Effect”:“Allow”, “Action”: [ “elasticloadbalancing:DescribeLoadBalancerAttributes”, “elastic ], “Resource”: “*” } ] }`
Panorama 上的输入	在 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Role**（**IAM** 角色）中，为用户输入 **Access Key ID**（访问密钥 **ID**）和 **Secret Access Key**（机密访问密钥）。
选项 **2**：具有 **Assume** 角色的 **IAM** 角色	

所需的角色和权限	尽管您可以使用此选项监控同一或跨帐户中的 VPC，但建议您使用此选项通过承担允许访问可正常访问的资源的角色进行跨帐户访问。
	要从其他帐户承担角色，AWS 帐户必须受该角色信任，并在其信任策略中将其定义为可信实体。此外，要访问其他帐户中的角色的用户必须拥有包含指定角色 ARN 的安全令牌服务 (STS) 访问权限的策略。
	在要监控的帐户 **1** 上：
	• 创建具有所需权限的 IAM 角色。对于 VM 监控，您需要以下权限。
	`{ “Version”:“2012-10-17", “Statement”: [ { “Sid”:“VisualEditor0”, “Effect”:“Allow”, “Action”: [ “elasticloadbalancing:DescribeLoadBalancerAttributes”, “elast ], “Resource”: “*” } ] }`
	• 复制角色 ARN。
	• 创建用户，并添加帐户 2 的帐户 ID 作为可信实体。这可以让帐户 2 拥有使用此角色访问帐户 1 中资源的权限。
	在需要访问帐户 **1** 的帐户 **2** 上
	• 附加具有 STS 权限的以下策略，并修改角色 ARN 以匹配您在帐户 1 中创建的角色。
	`{ "Version":"2012-10-17", "Statement": { "Effect": “Allow", "Action": "sts:AssumeRole",`

©2024 Palo Alto Networks, Inc.

	`"Resource":"arn:aws:iam::012347211234:role/ PAN-OS-assume-role" } }`
Panorama 上的输入	• 在 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Role**（**IAM** 角色）中，为帐户 2 上的用户输入 **Access Key ID**（访问密钥 **ID**）和 **Secret Access Key**（机密访问密钥）。 • 在 **Panorama** > **Plugins**（插件） > **AWS** > **Monitoring Definitions**（监控定义）中，输入要监控的 AWS 帐户 1 的 **Role ARN**（角色 **ARN**）。
选项 **3**：实例配置文件	
所需的角色和权限	仅当 Panorama 作为 EC2 实例部署在 AWS 上时 请注意，使用 *AWS* 管理控制台创建 *IAM* 角色时，控制台会自动创建与该角色同名的实例配置文件。由于角色和实例配置文件具有相同的名称，因此，使用 *IAM* 角色启动 *Panorama*（*EC2* 实例）时，同名实例配置文件将与其建立关联。 当 Panorama 与要监控的资源全部位于一个 AWS 帐户中时。 使用 AmazonEC2ReadOnlyAccess 创建 IAM 角色。
Panorama 上的输入	在 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Role**（**IAM** 角色）中，选择 **Instance Profile**（实例配置文件）作为选项。
选项 **4**：具有 **Assume** 角色的实例配置文件	
所需的角色和权限	当要监控的 Panorama 和资源部署在不同的 AWS 帐户中时，请使用具有承担角色的实例配置文件。 对于 Panorama HA，请确保将相同的实例配置文件附加到两个 Panorama 对等。 在已部署 **EC2** 实例的帐户 **1** 上： • 创建 IAM 角色。 • 对于此角色，添加在其中将 Panorama 部署作为可信实体的 AWS 帐户 ID（帐户 2）。 • 为 VM 监控附加上面详细介绍的 JSON 策略。 • 复制角色 ARN。Panorama 需要此角色才能检索 EC2 实例或 EKS 集群上的元数据。 在已部署 **Panorama** 的帐户 **2** 上： • 创建 IAM 角色并附加 JSON 策略（包含从帐户 1 获得的 STS 策略和源 ARN）。 • 对于要监控的每个其他 AWS 帐户，复制同一 STS 策略并修改角色 ARN。

©2024 Palo Alto Networks, Inc.

Panorama 上的输入	• 在 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Role**（**IAM** 角色）中，选择 **Instance Profile**（实例配置文件）作为选项。 • 在 **Panorama** > **Plugins**（插件） > **AWS** > **Monitoring Definitions**（监控定义）中，输入要监控的 AWS 帐户的 **Role ARN**（角色 **ARN**）。 例如，在本例中为帐户 1。

安装或升级 AWS 插件

要开始在 AWS 上监控 EC2 实例，请参阅适用于 AWS 的 Panorama 插件的兼容性矩阵和支持 VM 监控所需的 VM 系列插件版本。

要将适用于 AWS 的早期 Panorama 插件升级到更高版本（例如，从 1.0 版升级到 4.0 版），您必须先升级到最新版本（当前为 4.0）所需的 Panorama 和 VM 系列插件版本，然后按照下面的指示安装以执行升级。

安装最新的 *AWS* 插件（例如 *v4.0*）后，无法降级到更早的版本（例如 *v2.0*）。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复安装/升级过程。

在计划的维护时间段内安装或卸载插件。

如果当前已安装适用于任何云平台的 Panorama 插件，则安装（或卸载）其他插件需要重新启动 Panorama，以便提交更改。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

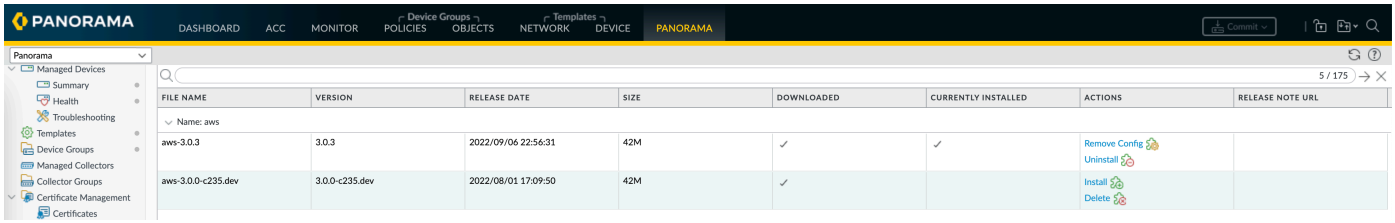
  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

©2024 Palo Alto Networks, Inc.

STEP 1 | 登录到 Panorama Web 界面，选择 **Panorama** > **Plugins**（插件），然后单击 **Check Now**（立即检查）以获取支持 VM 监控的 **AWS** 插件版本。



STEP 2 | **Download and Install**（下载并安装）插件。

安装成功后，Panorama 将刷新并在 **Panorama** > **Plugins**（插件）选项卡上显示 AWS 插件。

在 *Panorama* ***Dashboard***（仪表盘）上，您可以在 *General Information*（常规信息）小部件上验证安装的适用于 *AWS* 版本的 *Panorama* 插件。

STEP 3 | （HA 中的 Panorama）**Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。

如果 Panorama 在 HA 中，可以将更改提交到 Panorama 配置，以确保在发生故障转移时标记已注册到 Panorama 对等。

配置用于 VM 监控的 AWS 插件

要开始监控 AWS 公共云部署中的虚拟机，则必须在安装 AWS 插件之后创建监控定义。此定义指定有权在想要监控的 AWS VPC 中访问 EC2 实例的 IAM 角色，以及包含 Panorama 将检索的所有 IP 地址到标记映射推送到的防火墙的通知组。为了实施策略，必须随后创建动态地址组，并在安全策略中加以引用。您可通过动态地址组筛选想要匹配的标记，这样，防火墙可以根据每个标记获取注册的公共和专用 IP 地址，然后基于定义的策略规则允许或拒绝往返于工作负载的流量。

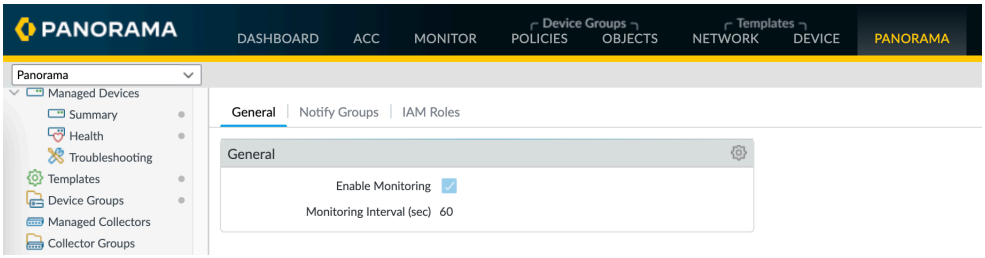
STEP 1 | 登录到 Panorama Web 界面。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在 AWS 上设置以下对象，以启用 VM 监控。

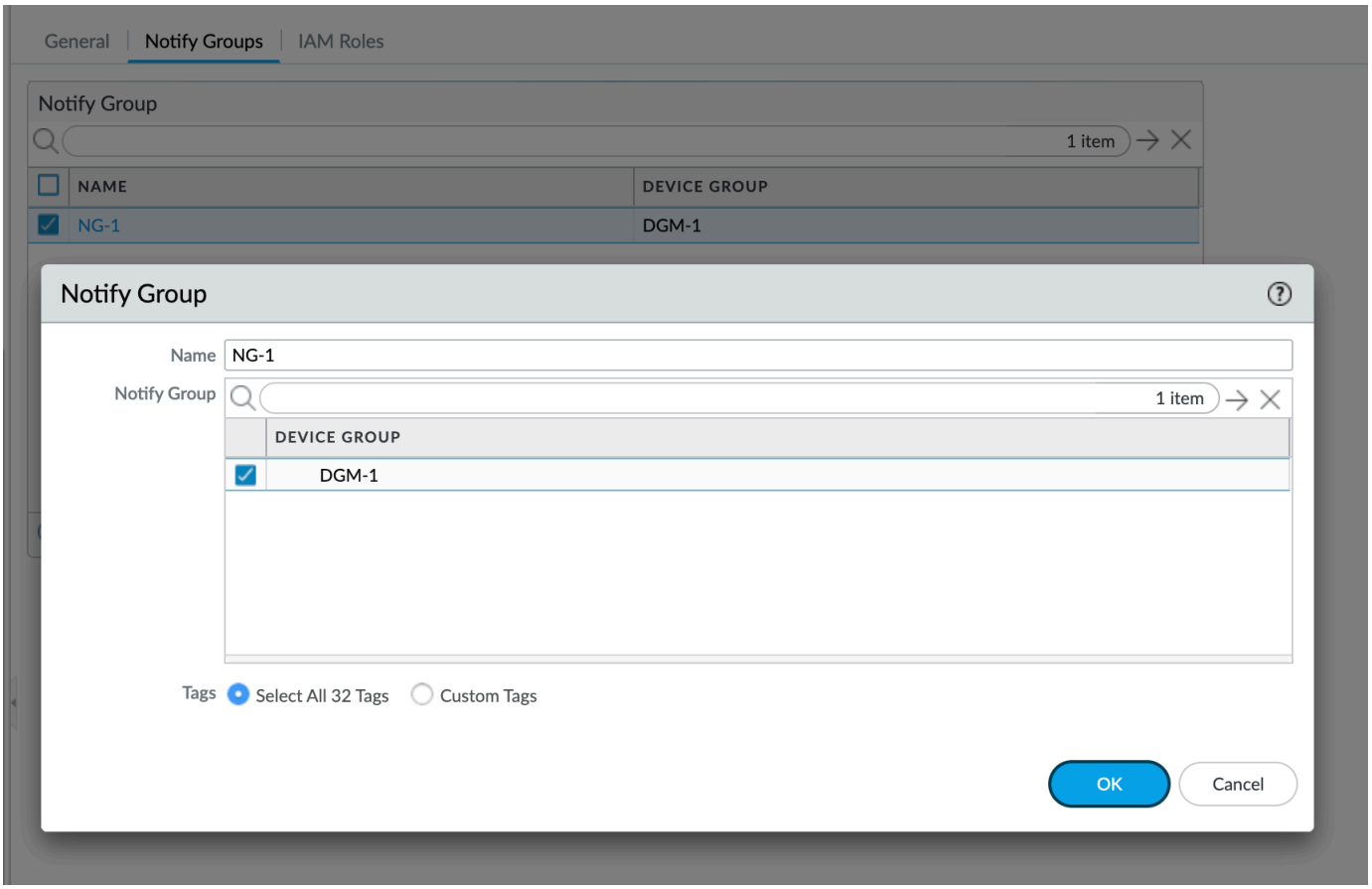
- 验证插件上是否启用监控。必须为 Panorama 启用此设置，以便与 AWS 公共云进行通信，从而进行 VM 监控。

  Enable Monitoring（启用监控）复选框位于 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **General**（常规）上。



- 添加通知组。

1. 选择 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **Notify Groups**（通知组） > **Add**（添加）。



2. 输入用于标识 Panorama 将检索到的 VM 信息推送到的防火墙组的 **Name**（名称）。
3. 选择作为防火墙或虚拟系统组的 **Device Groups**（设备组），以便 Panorama 将其从 AWS VPC 检索到的 VM 信息（IP 地址到标记映射）推送到该组。这些防火墙可使用此更新确

©2024 Palo Alto Networks, Inc.

定构成策略中所引用动态地址组的成员的最新列表。如果使用适用于 Azure 和 AWS 的 Panorama 插件，则可以使用来自两种环境的标记定位相同的防火墙或虚拟系统。

仔细考虑您的设备组。

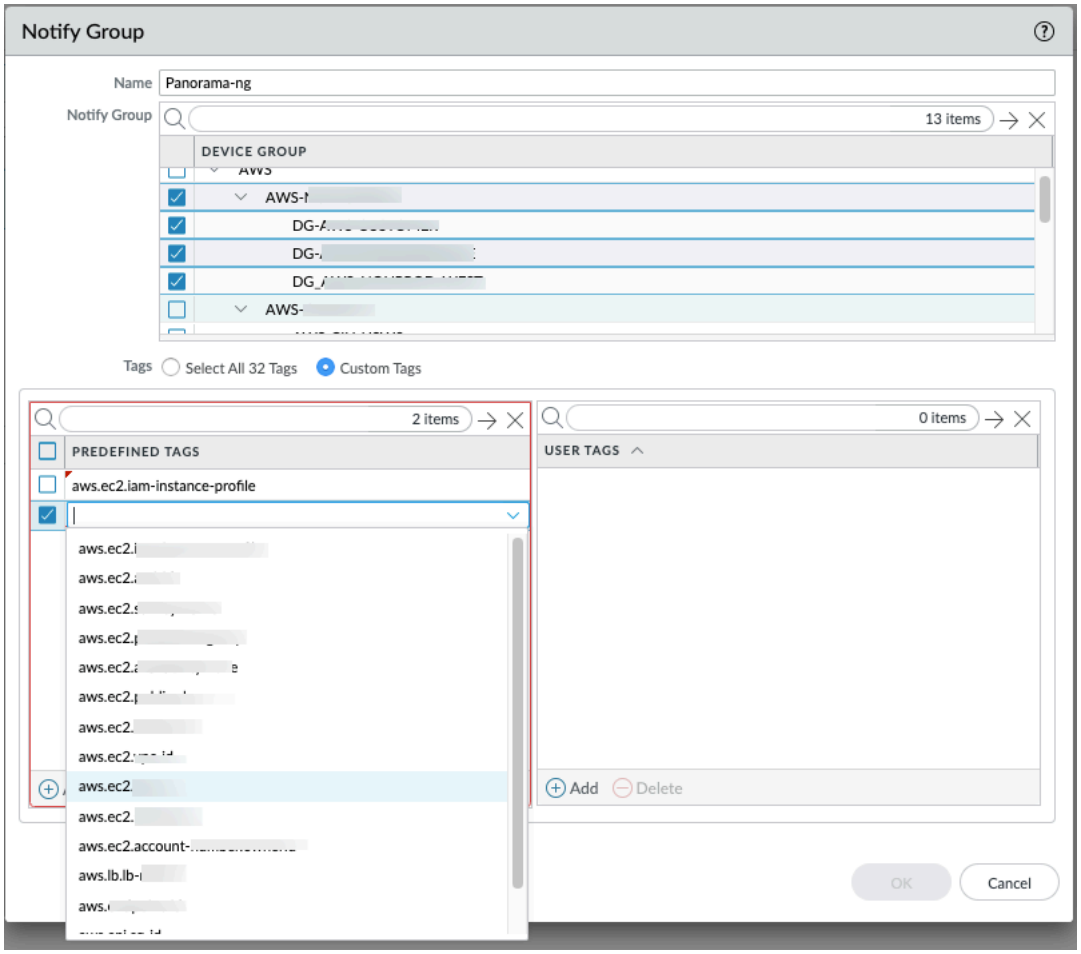
- 因为监控定义仅包括一个通知组，因此必须选中通知组内所有的相关设备组。如果想要取消注册 *Panorama* 已推送到通知组内防火墙的标记，则必须删除监控定义。
- 要将标记注册到启用用于多个虚拟系统的防火墙上的所有虚拟系统，则必须将每个虚拟系统添加到 *Panorama* 上的单独设备组，并分配设备组到通知组。如果您将所有虚拟系统分配到一个设备组，则 *Panorama* 仅将标记注册到防火墙上的一个虚拟系统。

4. 选择要从 AWS VPC 检索的标记。

   您可以 **Select All 32 Tags**（选择全部 **32** 个标记）（默认）或选择您想要为您的实例检索的 **Custom Tags**（自定义标记）。使用 Custom Tags（自定义标记）选项，您可以 **Add**（添加）要在安全策略中用作匹配条件的预定义标记和用户定义标记。如果要监控大

©2024 Palo Alto Networks, Inc.

量 EC2 实例，减少检索的标记数可确保在 Panorama 上更有效地使用 CPU 和内存容量。如需某些指导，请参阅规划 AWS 上的 VM 监控清单。

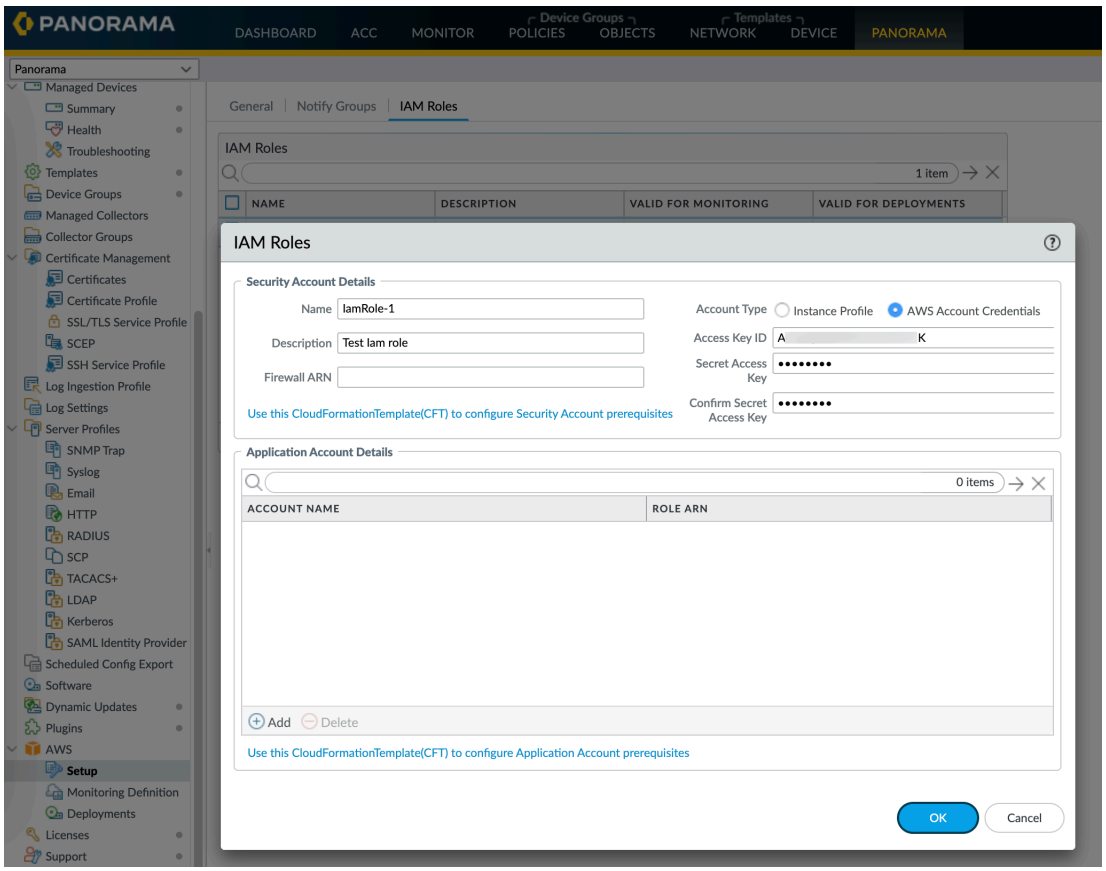


- 添加 IAM 角色。

  IAM 角色是允许您授权以便 Panorama 可以代表您向 AWS 资源（部署为 EC2 实例的虚拟机）发出服务请求的实体。

  1. 选择 **Panorama** > **Plugins**（插件） > **AWS** > **Setup**（设置） > **IAM Role**（**IAM** 角色） > **Add**（添加）。

©2024 Palo Alto Networks, Inc.



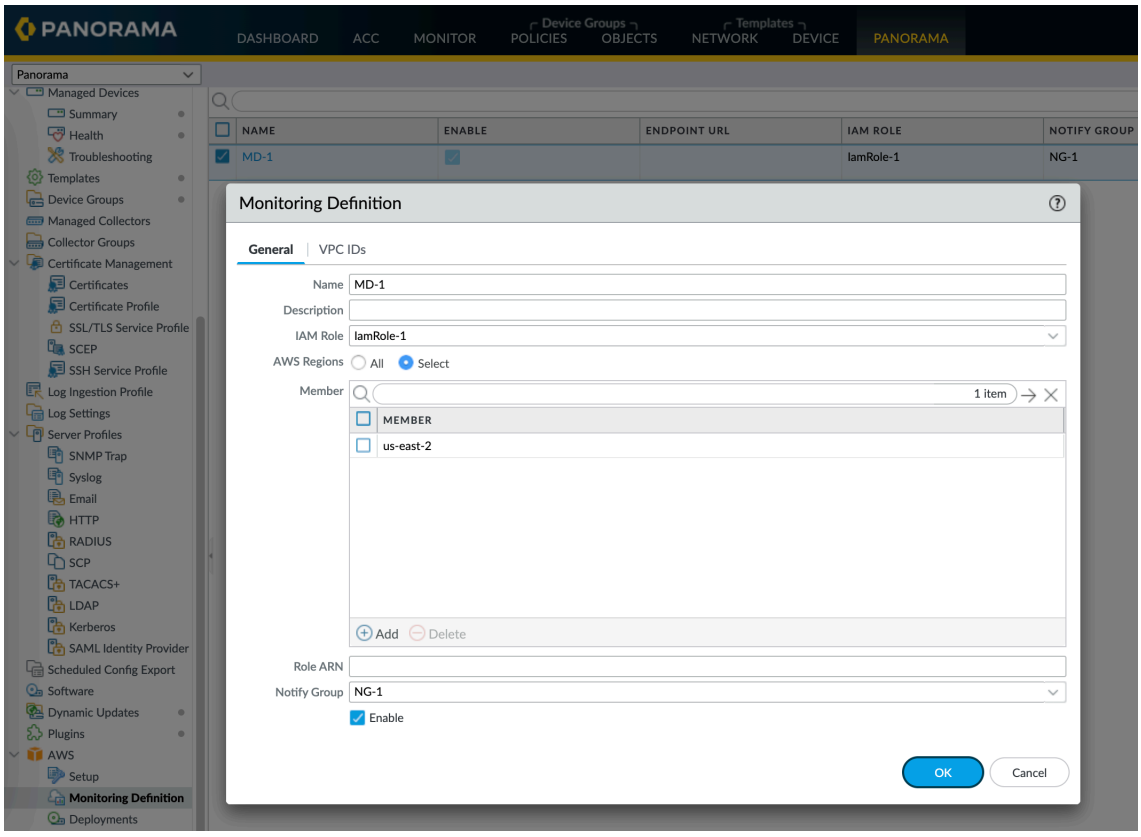
2. 输入标识 IAM 角色的 **Name**（名称），也可选择输入 **Description**（说明）。
3. 选择 Account Type（帐户类型）— **Instance Profile**（实例配置文件）或 **AWS Account Credentials**（**AWS** 帐户凭据）。如果 Panorama 部署在 AWS 上，您可以选择将具有正确权限的实例配置文件附加到 Panorama，或在 Panorama 上添加与 IAM 角色相关联的凭据。如果 Panorama 不是部署在 AWS 上，则必须在 Panorama 上输入 IAM 角色的凭据。
4. （仅限 AWS 帐户凭据）输入 **Secret Access Key**（机密访问密钥），然后重新输入以确认，然后单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 为要监控的每个 VPC 创建 **Monitoring Definition**（监控定义）。

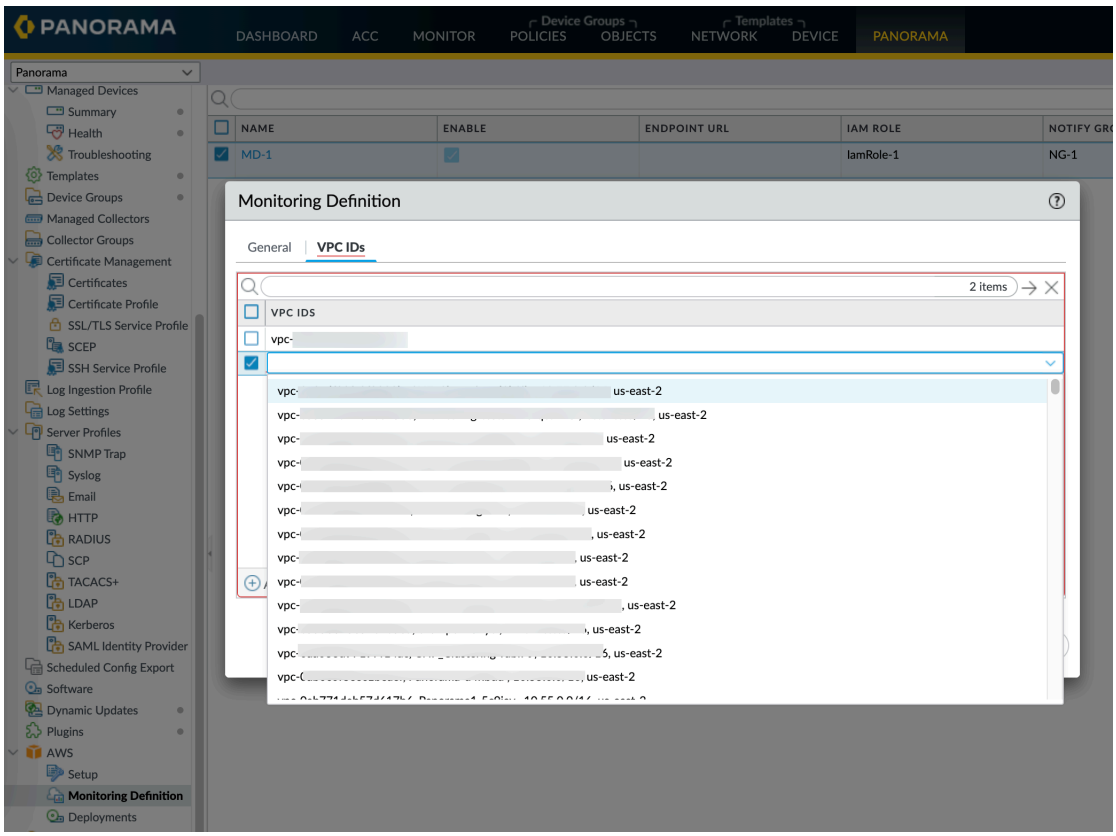
添加新的监控定义时，它将默认启用。

- 选择 **Panorama** > **Plugins**（插件） > **AWS** > **Monitoring Definition**（监控定义） > **General**（常规），从而 **Add**（添加）新定义。
- 输入用于标识使用此定义的 AWS VPC 的 **Name**（名称），也可选择输入 **Description**（说明）。
- 从 AWS 管理控制台上的 VPC 仪表盘选择 **IAM Role**（**IAM** 角色），**Add**（添加） **VPC ID**，以及 **Notify Group**（通知组）。
- 选择 **AWS Regions**（**AWS** 区域）：
  - **All**（全部）— 选择所有 AWS 区域。
  - **Select**（选择）— 选择特定的 AWS 区域。从 **Member**（成员）搜索栏搜索 AWS 区域或 **Add**（添加）新区域。
- （可选） 输入 **Role ARN**（角色 **ARN**），如果您已使用有权使用 AWS STS API 访问相同帐户或跨帐户的 AWS 资源的临时凭据设置角色链接和 IAM 角色。角色 ARN 必须属于要监控的 VPC。
- 选择 **Notify Group**（通知组）并 **Enable**（启用）监控。



- 在 **VPC ID** 选项卡上，从 AWS 管理控制台上的 VPC 指示板添加 VPC ID。

©2024 Palo Alto Networks, Inc.



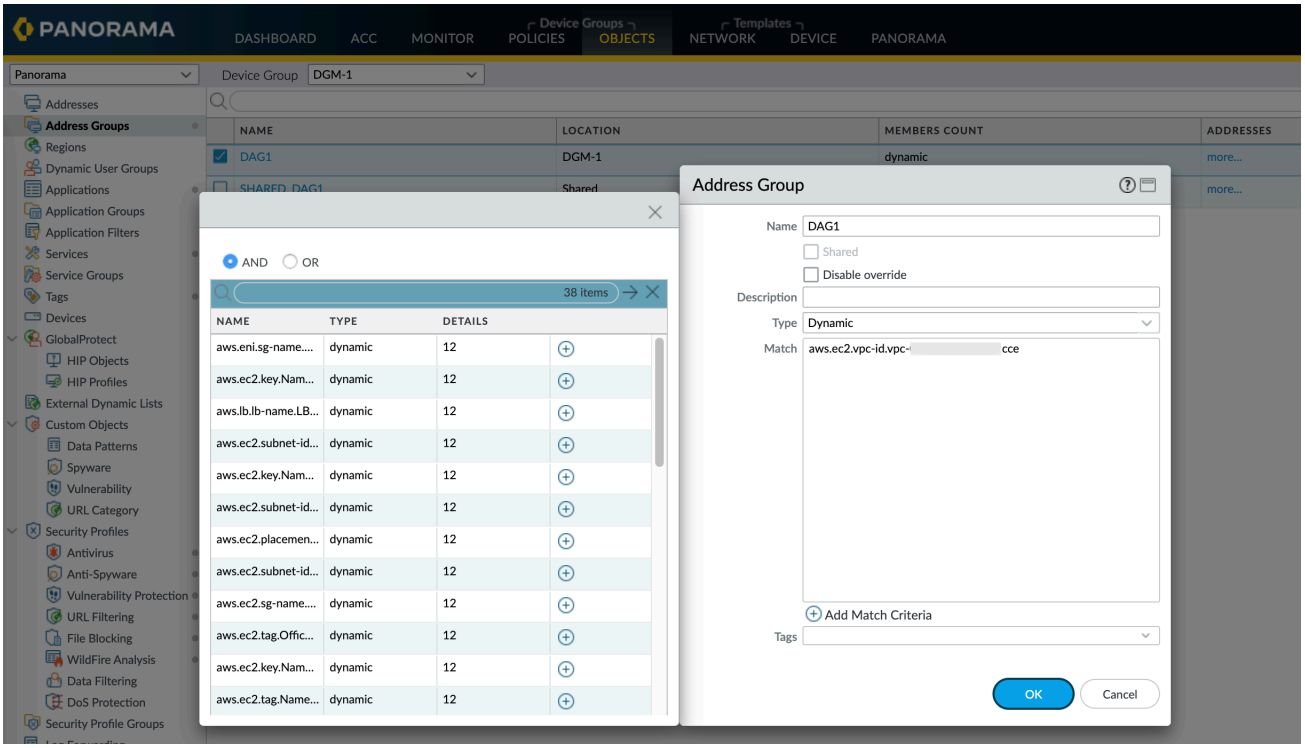
STEP 4 | 在 Panorama 上 **Commit**（提交）更改。

验证监控定义的状态是否显示为成功。如果失败，则验证是否输入正确的 AWS VPC ID，并为授权访问提供正确的密钥和 ID。

单击 ***Validate***（验证）以确认 *Panorama* 可以使用 *IAM* 角色和密钥进行身份验证，并与您在上面输入的 *AWS VPC* 进行通信。

©2024 Palo Alto Networks, Inc.

STEP 5 | 验证是否可以在 Panorama 上查看 VM 信息，并定义动态地址组的匹配条件。



在 *HA* 故障转移时，新激活的 *Panorama* 尝试重新连接到 *AWS* 云，并检索所有监控定义的标记。如果 *Panorama* 无法重新连接到已配置和启用的任一监视定义，*Panorama* 会生成系统日志消息

```
Unable to process accounts after HA switch-over; user-intervention required
```

。如果发生这种情况，您必须登录 *Panorama* 并验证监视定义，从而解决无效凭据或删除无效帐户。虽然 *Panorama* 从 *AWS* 云断开连接，但在故障转移之前检索用于监控定义的所有标记仍将保留，且防火墙可以继续在该 *IP* 地址列表上执行策略。只有当您删除监控定义时，*Panorama* 才会删除所有与帐户相关联的标记。最佳实践是，要监控此问题，您可以从 *Panorama* 配置面向操作的日志转发到 HTTP 定义，这样，您可以立即采取行动。

©2024 Palo Alto Networks, Inc.

STEP 6 | 知道在哪里可以找到与 Panorama 上的 AWS 插件相关的日志以进行故障排除。

- 使用 CLI 命令 **less plugins-log** 查看所有可用日志的列表

  less plugins-log plugin_aws_ret.log 显示与 IP 地址和标记检索相关的日志。

  less plugins-log plugin_aws_proc.log 显示与处理注册 IP 地址和标记相关的日志。

  less plugins-log plugin_aws.log 显示与 AWS 插件配置和守护进程相关的日志。

将 **show plugins aws vm-mon-status** 用作监控定义的状态。

```
admin@Panorama> show plugins aws vm-mon-status Mon-
Def Name VPC Status Last Updated Time Error Msg
 ------------------------------------------------------------------------------
 MD-Ins-Prof-ARN vpc-07986b091 Success 2019-12-02T10:24:56.007000
 MD-gov vpc-7ea1cf1a Success 2019-12-02T10:24:56.008000 MD-IAM-ARN
 vpc-025a83c123 Success 2019-12-02T10:24:56.012000
```


©2024 Palo Alto Networks, Inc.

使用 Amazon ELB 服务自动扩展 VM 系列防火墙

Palo Alto Networks 自动扩展适用于 AWS 的模板可帮助您配置和部署 VM 系列防火墙，以保护在 AWS 中部署的应用程序。这些模板利用 AWS 可扩展性功能独立和自动扩展在 AWS 中部署的 VM 系列防火墙，以满足应用程序工作负载资源需求的激增。

- VM 系列自动化功能包括 PAN-OS API 和引导（使用 2.0 版本的引导文件和 2.1 版本的 Panorama）。
- AWS 自动化技术包括用于 AWS 服务的 CloudFormation 模板和脚本，例如 Lambda、自动扩展组 (ASG)、弹性负载均衡 (ELB)、S3 和 SNS。

这些模板可在 Palo Alto Networks GitHub AWS 中的自动扩展 VM 系列防火墙的存储库中获得：

- 版本 2.0 提供防火墙模板和应用程序模板。这些模板和支持脚本在单个虚拟私有云 (VPC) 或多个 VPC 中部署 VM 系列防火墙、面向 Internet 的防火墙、内部防火墙和应用程序 ASG。

  在 2.0 版本中，Palo Alto Networks 支持防火墙模板，而应用程序模板由社区支持。有关部署详细信息，请参阅适用于 AWS 版本 2.0 的 VM 系列自动扩展模板。
- 版本 2.1 添加了对在单个 VPC 中部署的支持，并添加了对负载均衡器三明治拓扑结构的支持。该拓扑结构可让您将 VM 系列防火墙部署到前端 VPC，并将后端应用程序部署到 VPC 对等或 AWS PrivateLink 连接的一个或多个应用程序 VPC 中。

  在 2.1 版本中，您可以在 VPC 中实施应用程序负载均衡器 (ALB) 和网络负载均衡器 (NLB)。2.1 版本包括两个防火墙模板和五个应用程序模板。有关部署详细信息，请参阅适用于 AWS 版本 2.1 的 VM 系列自动扩展模板。

如果有现有模板部署，则不存在迁移过程。

下表比较了每个模板版本的一些高级功能。

功能/要求	版本 **2.0**	版本 **2.1**
在 Panorama 模式下，Panorama 运行 PAN-OS 9.0.1 或更高版本。	（可选）如果选择使用 Panorama，则必须在 VM 系列防火墙 VPC 和应用程序 VPC 之间配置 VPC 对等。对等的流量会传输到公共 Internet 上。	（必须）部署 2.1 版本的模板。

©2024 Palo Alto Networks, Inc.

功能/要求	版本 **2.0**	版本 **2.1**
在高可用性 *(HA)* 配置中，不支持 *Panorama*。		在 *Panorama* 上，必须手动安装 *VM* 系列插件，从而使 *VM* 系列防火墙能够发布用于自动扩展的 *PAN-OS* 指标。
引导	S3存储桶中的 `Bootstrap.xml` 配置文件。	Panorama 的 `init-cfg.txt` 文件。
Palo Alto Networks S3 存储桶示例	使用自己的 S3 存储桶或使用 panw-aws-autoscale-v20-us-west-2 中的示例。	使用自己的 S3 存储桶进行部署。
单个 VPC 或单独的 VPC（中心辐射型）	是	是
新 VPC	是	是
现有 VPC（棕色字段）	否	是
每个 VPC 的可用性区域	2	2-4
外部负载均衡器	仅限 ALB	ALB 或 NLB
内部负载均衡器	仅限 NLB	ALB 或 NLB
VM 系列防火墙 VPC 和后端服务器的 AWS PrivateLink。	否	是

有关模板的详细信息，请参阅：

- 适用于 AWS 版本 2.0 的 VM 系列自动扩展模板
- 适用于 AWS 版本 2.1 的 VM 系列自动扩展模板

©2024 Palo Alto Networks, Inc.

适用于 AWS 版本 2.0 的 VM 系列自动扩展模板

为了帮助您管理增加的应用程序规模，2.0 版的自动扩展 VM 系列防火墙模板提供了可简化部署的集线器和分线架构。该版本的解决方案提供了两个模板，可在单个 AWS 帐户和多个 AWS 帐户中支持单个和多个 VPC 部署。

- 防火墙模板 — 防火墙模板跨两个可用性区域 (AZ) 在自动扩展组内部署应用程序负载均衡器 (ALB) 和 VM 系列防火墙。这种面向 Internet 的应用程序负载均衡器可分配跨 VM 池系列防火墙进入 VPC 的流量。VM 系列防火墙自动发布启用自动扩展的自定义 PAN-OS 指标。

  Palo Alto Networks 正式支持防火墙模板，并且通过有效的支持权利，您可以向 Palo Alto Networks 技术支持请求帮助。

  以下应用程序模板部署上图中描述的网络负载均衡器。

- 应用程序模板 — 应用程序模板在每个 AZ 中使用 Web 服务器部署网络负载均衡器 (NLB) 和一个自动扩展组 (ASG)。

  应用程序模板受社区支持。此模板作为示例提供，以帮助您开始使用基本 Web 应用程序。对于生产环境，请使用您自己的应用程序模板或自定义此模板以满足您的要求。

通过这些模板，您可以使用面向 Internet 的应用程序负载均稀器和内部网络负载均稀器部署负载均衡器三明治拓扑结构。面向 Internet 的 ELB 可通过 Internet 访问，并分发跨 VM 池系列防火墙进入 VPC 的流量。防火墙随后使用 NAT 策略将流量路由到内部网络负载均衡器，后者将流量分发到网络或应用程序服务器的自动扩展层。VM 系列防火墙能够将自定义 PAN-OS 指标发布到 AWS CloudWatch，您可以监控 VM 系列防火墙上的运行状况和资源负载，然后使用该信息在防火墙上的适当 ASG 上触发自动扩展事件。

- 适用于 AWS (v2.0) 的 VM 系列自动扩展模板具有哪些组件？
- 适用于 AWS (v2.0) 的 VM 系列自动扩展模板如何启用动态扩展？
- 规划适用于 AWS (v2.0) 的 VM 系列自动扩展模板
- 在启动前自定义防火墙模板 (v2.0)
- 启动适用于 AWS 的 VM 系列自动扩展模板 (v2.0)
- 自定义 Bootstrap.xml 文件 (v2.0)
- AWS 更新与 VM 系列自动扩展模板 (v2.0)
- 修改管理帐户和更新堆栈

适用于 **AWS (v2.0)** 的 **VM** 系列自动扩展模板具有哪些组件？

AWS 的 VM 系列自动扩展模板包含以下构建基块：

©2024 Palo Alto Networks, Inc.

构建基块	说明
防火墙模板 （Palo Alto Networks 官方支持模板）	`firewall-v2.0.template` 部署具有跨这些 AZ 进行流量路由所需的子网、路由表、AWS NAT 网关、两个可用性区域 (AZ) 和安全组的新 VPC。此版本 2.0 模板还在每个 AZ 中部署外部 ALB 和带有 VM 系列防火墙的 ASG。 由于生产环境中的诸多变化，包括但不限于特定数量的组件，例如子网、可用性区域、路由表和安全组，因此您必须在新 VPC 中部署 `firewall-v2.0.template`。 适用于 *AWS* 的 *VM* 系列自动扩展模板不会部署 *Panorama*，*Panorama* 是可选的。*Panorama* 提供了简化的政策管理和集中可见性。如果要使用 *Panorama* 来管理解决方案所部署的 *VM* 系列防火墙，则可以在公司网络内使用 *M* 系列设备或 *Panorama* 虚拟设备，也可以在 *AWS* 上使用 *Panorama* 虚拟设备。 此解决方案包括一个 AWS NAT 网关，防火墙使用该网关发起用于检索更新的出站请求，连接到 Panorama 并将度量标准发布到 AWS CloudWatch。
应用程序模板 （社区支持模板）	应用程序模板在每个 AZ 中部署 NLB 和带有 Web 服务器的 ASG。由于 NLB 具有每个 AZ 的唯一 IP 地址，并且防火墙上的 NAT 策略规则必须引用单个 IP 地址，因此两个 AZ 中的每一个都有一个 ASG。ASG 中的所有防火墙都使用相同的配置。 2.0 版本的自动扩展解决方案包含两个应用程序模板： • `panw_aws_nlb-v2.0.template` 允许您在与部署防火墙模板（同一 AWS 帐户）相同的 VPC 中部署应用程序模板资源。 • `panw_aws_nlb_vpcv-2.0.template` 允许您使用同一 AWS 帐户或多个 AWS 帐户在独立的 VPC 中部署应用程序模板资源。
Lambda 函数	AWS Lambda 提供强大的事件驱动自动化，无需复杂的编排软件。在 `firewall-v2.0.template` 中，AWS Lambda 监控简单队列服务 (SQS) 以了解发布到队列的 NLB。当 Lambda 函数检测到新的 NLB 时，它会创建一个新的 NAT 策略规则并将其应用于 ASG 内的 VM 系列防火墙。防火墙对每个应用都有 NAT 策略规则，防火墙使用 NAT 策略规则（将端口映射到 NLB IP 地址）将流量转发到应用程序 Web 服务器前面的 NLB。 您需要创建安全策略规则以允许或拒绝部署的应用程序通信。示例 *`bootstrap.xml`* 文件不包含任何安全策略规则。您应使用 *Panorama* 集中管理防火墙并简化创建安全策略规则。

©2024 Palo Alto Networks, Inc.

构建基块	说明
	您还可以使用其他功能： • 在防火墙启动或终止时添加或删除接口 (ENI)。 • 在删除堆栈或终止实例时删除所有关联资源。 • 当发生缩小事件时删除作为 Panorama 托管设备的防火墙。 • 当缩小事件导致防火墙终止时停用 BYOL 许可证。 要了解更多关于 Lambda 函数的信息，请参阅 **http://paloaltonetworks-aws-autoscale-2-0.readthedocs.io/en/latest/**
引导文件 GitHub 存储库中提供的 bootstrap.xml 文件仅用于测试和评估。对于生产部署，您必须在启动之前修改 bootstrap.xml 中的示例凭证。	此解决方案需要 init-cfg.txt 文件和 bootstrap.xml 文件，以便 VM 系列防火墙具有处理流量的基本配置。 • `init-cfg.txt` 文件包含 mgmt-interface-swap 操作命令，以使防火墙能够在其主接口 (eth0) 上接收数据平面流量。此自动扩展解决方案需要交换数据平面和管理界面，以使 ALB 能够将 Web 流量转发到 VM 系列防火墙的自动扩展层。有关详细信息，请参阅管理接口映射以用于 Amazon ELB。 • `bootstrap.xml` 文件为防火墙网络接口启用基本连接，并允许防火墙连接到与启动模板时输入的堆栈名称相匹配的 AWS CloudWatch 命名空间。

要部署解决方案，请参阅为 AWS (v2.0) 启动 VM 系列自动扩展模板。

AWS（v2.0 和 v2.1）的 VM 系列自动扩展模板如何启用动态扩展？

VM 系列防火墙使用基于自定义 PAN-OS 指标的自动扩展模板部署的 VM 系列防火墙进行缩小和扩展。VM 系列防火墙本地将这些指标发布到 Amazon CloudWatch 控制台，并根据您选择作为扩展参数的指标，您可以定义 CloudWatch 警报和策略动态部署或终止实例以管理您的 AWS 部署中的应用程序流量。

防火墙以五分钟（默认）将指标发布到 AWS CloudWatch。当监控的指标达到定义时间间隔的配置阈值时，CloudWatch 会触发警报并启动自动扩展事件。

当自动扩展事件触发新防火墙的部署时，新实例在启动时引导并且 AWS Lambda 功能使用 NAT 策略规则配置防火墙。为每个应用程序创建 NAT 策略规则，并且该规则引用部署中每个网络负载均衡器的 IP 地址。当应用程序负载均衡器收到请求时，它会将请求转发到指定 TCP 端口上的防火墙。随后，防火墙检查流量并将其转发到相应的网络负载均衡器，然后将该请求转发到其目标组中的 Web 服务器。

规划 AWS (v2.0 和 v2.1) 的 VM 系列自动扩展模板

此清单中的项目是您为实施此解决方案必须执行的操作和选择。

©2024 Palo Alto Networks, Inc.

模板 **v2.0** 和 **v2.1** 的规划清单	
❑ 验证部署 VM 系列自动扩展模板的要求。	自动扩展模板需要 AWS Lambda 和 S3 签名版本 2 或 4，并且可以部署运行支持的 PAN-OS 版本的 VM 系列防火墙。您需要查看支持的区域和 AMI ID 列表，作为防火墙模板中的输入。
❑ 为 IAM 用户角色分配适当的权限。	部署 VM 系列自动扩展模板的用户必须具有管理权限或具有在中列出的权限 IAM-policy.json 成功启动该解决方案。将此文件的权限复制并粘贴到新的 IAM 策略中，然后将该策略附加到新的或现有的 IAM 角色。 对于跨帐户部署，要访问不同 AWS 帐户中的资源，部署应用程序模板的用户的 IAM 角色必须具有完整的 SQS 访问权限和可信关系，授权她写入属于 SQS 队列到防火墙模板。
❑ 收集跨帐户部署所需的详细信息。	对于防火墙模板和应用程序模板属于不同帐户的部署，承载防火墙模板资源的帐户为可信帐户，其他拥有应用程序模板资源的 AWS 帐户为受可信帐户。要在跨帐户部署中启动应用程序模板，您需要以下信息： • 跨帐户角色您正在部署应用程序模板的帐户的 Amazon 资源名称 (ARN)。 • 您在创建授予对可信帐户的完整 SQS 访问权限的 IAM 角色时定义的外部 ID。 • 计划启动应用程序模板的每个 AWS 帐户的 10 位帐号。因为承载防火墙模板资源的帐户充当可信帐户，拥有应用程序模板用户需要的资源，所以需要列出每个可以访问防火墙资源的受可信帐户的帐号。
❑ 在 Palo Alto Networks 支持门户上创建支持帐户（如果未创建）。	您可以选择 BYOL 或 PAYG 许可证。 • 对于 BYOL，您必须在启动 VM 系列自动扩展模板之前向 Palo Alto Networks 支持帐户注册授权代码，并使用引导数据包中的授权代码文件名将授权代码添加到 `/license` 文件夹中。有关详细信息，请参阅为 AWS (v2.0) 启动 VM 系列自动扩展模板或启动防火墙模板 (v2.1)。 • 对于 PAYG，您必须注册 VM 系列防火墙以激活您的支持权利。
❑ （仅适用于 PAYG）查看并接受最终用户许可协议 (EULA)。 如果您是首次在 AWS 帐户中启动 VM 系列防火墙，	在 AWS Marketplace 中，搜索 Palo Alto Networks，然后选择要使用的套餐。如果未接受计划使用的套餐的 EULA，则无法部署 VM 系列防火墙。 • 例如，搜索 **VM** 系列新一代防火墙套餐 **2**。

©2024 Palo Alto Networks, Inc.

模板 **v2.0** 和 **v2.1** 的规划清单	
则必须执行此操作。	• 单击 **Continue**（继续），然后选择 **Manual Launch**（手动启动）。查看协议，然后单击 **Accept Software Terms**（接受软件条款）以接受 EULA。 现在可以关闭浏览器。
❑ 决定是否打算针对 AWS Lambda、Python 脚本和模板使用公共 S3 存储桶或专用 S3 存储桶。	Palo Alto Networks 提供 支持地区 列表内所有 AWS 区域的公共 S3 存储桶。这些 S3 存储桶包含您需要的所有模板、AWS Lambda 代码和引导文件。 *Palo Alto Networks* 建议仅在公共 *S3* 存储桶中使用引导文件来评估此解决方案。对于生产部署，您必须为引导数据包创建专用 *S3* 存储桶。 S3 存储桶的命名约定是 `panw-aws-autoscale-v20-<region_name>`。例如，AWS Oregon 地区的存储桶是 panw-aws-autoscale-v20-us-west-2。 要使用您的专有 S3 存储桶，您必须下载模板、AWS Lambda 代码和引导文件，并将其复制到您的专有 S3 存储桶。您可以将防火墙模板和应用程序模板的所有必需文件放在一个 S3 存储桶中，或将它们放在单独的 S3 存储桶中。

©2024 Palo Alto Networks, Inc.

模板 **v2.0** 和 **v2.1** 的规划清单	
❑ 下载模板、AWS Lambda 代码和引导文件。	• 从 GitHub 存储库获取用于部署防火墙模板（应用程序负载均衡器和 VM 系列防火墙）的文件。 不要在 *VM* 系列自动扩展模板版本中混用和匹配文件。 • 模板和 Lambda 代码： • panw-aws.zip • firewall-v2.X.template • 引导文件： • init-cfg.txt • bootstrap.xml 与此解决方案捆绑在一起的 bootstrap.xml 文件旨在帮助您开始使用，仅提供用于测试和评估。对于生产部署，您必须在启动之前修改 bootstrap.xml。 • iam-policy：部署 VM 系列自动扩展模板的用户必须具有此文件中列出的管理权限或权限才能成功启动此解决方案。 该防火墙模板由 *Palo Alto Networks* 技术支持部门提供支持。 • 从 GitHub 存储库版本 2.0 或 2.1 获取用于部署 NLB 和 Web 服务器的文件。 • 模板： • pan_aws_nlb-2.X.template — 使用此模板在与部署防火墙模板（同一 AWS 帐户）相同的 VPC 中部署应用程序模板资源。 • pan_aws_nlb_vpc-2.X.template — 使用此模板在不同的 VPC 中部署应用程序模板资源。只要您具有支持跨帐户部署的适当权限，该模板就允许您在相同的AWS帐户或不同的AWS帐户内部署资源。 • pan_nlb_lambda.template — 创建 AWS 网络负载均衡器，用于多路复用流量以注册扩展的后端 Web 服务器。 • Lambda 代码和 Python 脚本。
❑ 为您的生产环境自定义 bootstrap.xml 文件。	为确保您的生产环境安全，您必须为生产部署 自定义 Bootstrap.xml 文件（具有唯一管理用户名和密码）。默认的用户名和密码为 pandemo/demopassword。您还可以借此机会创建具有接口、区域和安全策略规则的最佳防火墙配置，以满足您的应用程序安全需求。

©2024 Palo Alto Networks, Inc.

模板 **v2.0** 和 **v2.1** 的规划清单	
❑ 决定是否要使用 Panorama 进行集中式日志记录、报告和防火墙管理。	Panorama 是一个管理方便的选项，也是管理防火墙的最佳实践。不需要管理此解决方案中部署的 VM 系列防火墙的自动扩展层。 如果要使用 Panorama，可以在 AWS 上使用 Panorama 虚拟设备，也可以在公司网络中使用 M 系列设备或 Panorama 虚拟设备。 *Panorama* 必须处于 *Panorama* 模式，而非仅管理模式。 要使用 Panorama 成功注册防火墙，您必须收集以下详细信息： • Panorama的API密钥 — 为了让AWS Lambda可以向Panorama发出API请求，您必须在启动 VM 系列自动扩展模板时提供API密钥。作为最佳实践，在生产部署中，应该为 API 调用创建单独的管理帐户，并 生成关联的 API 密钥。 • PanoramaIP地址 — 您必须在配置 (init-cfg.txt) 文件中包含IP地址。防火墙必须能够从 VPC 访问此IP地址；为确保安全连接，请使用直接连接链路或 IPSec 隧道。 • VM 身份验证密钥 — 允许 Panorama 对防火墙进行验证，以便它可以将每个防火墙添加为托管设备。您必须将此密钥包含在配置 (init-cfg.txt) 文件中。 部署生命周期必须提供 VM 验证密钥。没有连接请求中的有效密钥，VM 系列防火墙将无法注册Panorama。有关密钥的详细信息，请参阅 在 Panorama 上生成 VM 身份验证密钥。 • 模板堆栈名称和要将防火墙分配到的设备组名称 — 必须首先添加一个模板并将其分配给模板堆栈，创建一个设备组 在 Panorama 上，然后在配置 (init-cfg.txt) 文件中包含模板堆栈名称和设备组名称。 为了降低使用弹性 *IP* 地址的成本和规模限制，防火墙不包含公共 *IP*。如果您未使用 *Panorama* 管理防火墙，则必须部署跳转服务器（具有 *EIP* 地址的堡垒主机），该服务器连接到 *VPC* 内的 *Untrust* 子网，以启用对 *VM* 系列防火墙的 *SSH* 和/或 *HTTPS* 访问。默认情况下，此解决方案包括一个 *AWS NAT* 网关，防火墙使用该网关发起用于检索更新的出站请求，连接到 *Panorama* 并将度量标准发布到 *AWS CloudWatch*。
入门	启动适用于 AWS 的 VM 系列自动扩展模板 (v2.0)。

©2024 Palo Alto Networks, Inc.

在启动前自定义防火墙模板（v2.0 和 v2.1）

为了简化部署工作流程，防火墙显示有限的参数集，在启动模板时需要为其提供输入。如果您想要查看和自定义模板中包含的其他选项，可以使用文本编辑工具（如记事本或 Visual Studio Code），为 AWS v2.0 或 2.1 启动 VM 系列自动扩展模板之前指定想要的值。

使用下表查看允许您为 AWS 部署自动扩展防火墙模板进行自定义的参数列表。通过您购买的支持选项，从列表中修改参数属于 Palo Alto Networks 的官方支持政策。

参数	说明	默认值
VPC 的 CIDR 块	您想要用于 VPC 的 IP 地址空间。 您在下面修改的子网必须属于此 *VPC CIDR* 块，并且是唯一的。	192.168.0.0/16
管理子网 CIDR 块	用逗号分隔的防火墙管理子网的 CIDR 块列表。	192.168.0.0/24, 192.168.10.0/24
不可信子网 CIDR 块	用逗号分隔的不可信子网的 CIDR 块列表。	192.168.1.0/24, 192.168.11.0/24
可信子网 CIDR 块	用逗号分隔的可信子网的 CIDR 块列表。	192.168.2.0/24, 192.168.12.0/24
NAT 网关子网 CIDR 块	用逗号分隔的 AWS NAT 网关的 CIDR 块列表。	192.168.100.0/24, 192.168.101.0/24
Lambda 子网 CIDR 块	用逗号分隔的 Lambda 功能的 CIDR 块列表。	192.168.200.0/24, 192.168.201.0/24
防火墙实例大小	AWS 实例类型和大小，您需要为您的部署中的 VM 系列防火墙。	M4.xlarge
选择您的扩展参数	该模板将以下所有指标发布到 AWS CloudWatch： • CPU — 数据平面 CPU 利用率	数据面板 CPU 利用率

©2024 Palo Alto Networks, Inc.

参数	说明	默认值
您无需修改模板的扩展参数。您可以设置 AWS CloudWatch 警报在 *AWS* 控制台上为您要触发自动调节的一个或多个自定义 *PAN-OS* 指标。	• AS — 活动会话数 • SU — 会话利用率 • SSPU—SSL 代理利用率 • GPU — GlobalProtect 网关利用率 • GPAT — GlobalProtect 网关利用活动隧道数 • DPB — 数据平面数据包缓冲区利用率	
选择扩展周期的秒数	应用平均统计量的时间段，以秒为单位。必须是 60 的倍数。	900
最大 VM 系列实例	自动扩展组中的 VM 系列防火墙的最大数量。	3
最小 VM 系列实例	自动扩展组中最小数量的 VM 系列防火墙。	1
ScaleDown 阈值（以百分比/值表示）	触发放大事件的值。	20
ScaleUp 阈值（以百分比/值表示）	触发缩减事件的值。	80

启动适用于 AWS 的 VM 系列自动扩展模板 (v2.0)

您可以选择将防火墙模板部署到一个 VPC 中，并将示例应用程序模板部署在与部署防火墙的 VPC 相同的 VPC 中，或放入不同的 VPC 中。

如果您想要保护的应用程序属于单独的 AWS 帐户，则示例应用程序模板包含对跨帐户部署的支持。该解决方案支持中心辐射架构，您可以在一个 AWS 帐户中部署防火墙模板，并将其用作集线器来保护属于相同或不同 AWS 帐户的应用程序（散点）。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

- 启动 VM 系列防火墙模板
- 启动应用程序模板
- （仅在部署多个内部负载均衡器时才需要）为 ELB 服务启用流量（v2.0 和 v2.1）

©2024 Palo Alto Networks, Inc.

启动 VM 系列防火墙模板

此工作流程将告诉您如何使用防火墙模板部署应用程序负载均衡器和 VM 系列防火墙。

此防火墙模板包含一个 *AWS NAT* 网关，防火墙用来启动用于检索更新的出站请求，连接到 *Panorama* 以及将指标发布到 *AWS CloudWatch*。如果您未使用 *Panorama* 管理防火墙，则必须部署跳转服务器（具有 *EIP* 地址的堡垒主机），该服务器连接到 *VPC* 内的 *Untrust* 子网，以启用对 *VM* 系列防火墙的 *SSH* 和/或 *HTTPS* 访问。此跳转服务器是必需的，因为 *VM* 系列防火墙上的管理界面仅具有私有 *IP* 地址。

STEP 1 | 审核检查清单计划 AWS 的 VM 系列自动扩展模板 (v 2.0)。

确保已完成以下任务：

- （仅限 PAYG）审核并接受您计划使用的 PAYG 套餐的 EULA。
- （仅限 BYOL）获得授权代码。您需要在引导数据包的 /license 文件夹中输入此授权代码。
- 下载启动 VM 系列自动扩展模板所需的文件 GitHub 存储库。

©2024 Palo Alto Networks, Inc.

STEP 2 | 修改 init-cfg.txt 文件。您必须将设备证书自动注册 PIN 添加到 init-cfg.txt 文件，才能在部署 VM 系列防火墙实例时自动安装设备证书。

vm-series-auto-registration-id=

vm-series-auto-registration-pin-value=

要了解更多详细信息，请阅读有关引导过程和 init-cfg.txt 文件的信息。

如果您使用 Panorama 来管理防火墙，请完成以下任务：

1. 在 Panorama 上生成 VM 身份验证密钥.防火墙必须在 Panorama 的连接请求中包含有效的密钥。将密钥的使用期限设置为 8760 小时（1 年）。
2. 使用文本编辑器（如记事本）打开 init-cfg.txt 文件。确保不要更改格式，否则会导致部署 VM 系列自动扩展模板失败。以“名称 — 值”对的形式添加以下信息：
   - 主要 Panorama 的 IP 地址和可选的辅助 Panorama。输入：

     panorama-server=

     panorama-server-2=
   - 指定您希望为其分配防火墙的模板堆栈名称和设备组。输入：

     tplname=

     dgname=
   - VM 身份验证密钥。输入：

     vm-auth-key=
3. 验证没有删除 AWS 上 VM 系列防火墙的交换管理接口 (mgmt) 和数据面接口 (ethernet 1/1) 的名称。例如，文件必须包含“名称 — 值”对，如下所示：

   op-command-modes=mgmt-interface-swap

   vm-auth-key=755036225328715

   panorama-server=10.5.107.20

   panorama-server-2=10.5.107.21

   tplname=FINANCE_TG4

   dgname=finance_dg
4. 保存并关闭此文件。

STEP 3 | （仅限 BYOL）将许可证认证码添加到引导软件包的 /license 文件夹中。有关详细信息，请参阅准备引导数据包。

1. 用文本编辑器（如记事本）创建一个新的 .txt 文件。
2. 将您的 BYOL 许可证的授权代码添加到该文件中，并保存带授权代码的文件（无文件扩展），然后将其上传到 /license 文件夹。授权代码必须支持部署可能需要的防火墙数量。您必须使用授权代码包，而不是单个授权代码，确保防火墙能够同时获取与防火墙相关的

©2024 Palo Alto Networks, Inc.

所有许可证密钥。如果您使用单个授权代码，而非代码包，防火墙只会检索文件中第一个授权代码对应的许可证密钥。

STEP 4 | 更改 bootstrap.xml 文件中定义的 VM 系列防火墙管理员帐户的默认凭据。

在生产环境中使用 VM 系列自动扩展模板时需要。

GitHub 存储库中的 bootstrap.xml 文件仅用于测试和评估。对于生产部署，您必须在启动前自定义 Bootstrap.xml 文件 (v2.0)。

©2024 Palo Alto Networks, Inc.

STEP 5 | 准备 Amazon Simple Storage (S3) 存储桶，以便将 VM 系列自动扩展模板启动到生产环境。

确保在计划部署模板的相同区域中创建 *S3* 存储桶；仅提供公用 *S3* 存储桶中托管的引导文件，以便您更轻松地评估模板。

1. 为引导文件创建一个新的 S3 存储桶。
   1. 登录到 AWS 管理控制台，然后打开 S3 仪表盘。
   2. 单击 **Create Bucket**（创建存储桶）。
   3. 输入 **Bucket Name**（存储同名称）和 **Region**（地区），然后单击 **Create**（创建）。存储区必须位于 S3 根级别。因为您无法指定引导文件位置的路径，因此如果您嵌套存储桶，引导将会失败。
2. 将引导文件上传到 S3 存储桶。引导文件夹必须位于 S3 存储桶的根文件夹中。
   1. 单击存储桶的名称，然后单击 **Create folder**（创建文件夹）。
   2. 为引导创建以下文件夹结构。
   3. 单击链接打开 **config** 文件夹。
   4. 选择 **Actions**（操作） > **Upload**（上传）和**Add Files**（添加文件），浏览以选择 init-cfg.txt 文件和 bootstrap.xml 文件，然后单击 **Open**（打开）。
   5. 单击 **Start Upload**（开始上传）将文件添加到配置文件夹。该文件夹只能包含两个文件：init-cfg.txt 和 bootstrap.xml。
   6. （仅限 BYOL）单击链接打开 **license**（许可证）文件夹并上传带有授权 VM 系列防火墙所需的授权代码的 txt 文件。
3. 将 AWS Lambda 代码（panw-aws.zip 文件）上传到 S3 存储桶。在此示例中，AWS Lambda 代码与引导程序包位于相同的 S3 存储桶中。
   1. 单击存储桶名称。
   2. 单击 **Add Files**（添加文件）以选择 panw-aws.zip 文件，请单击 **Open**（打开）。
   3. 单击 **Start Upload**（开始上传）以将 zip 文件添加到 S3 存储桶。

STEP 6 | 选择防火墙模板。

如果您需要在启动前自定义防火墙模板 (v2.0)，请现在做，并选择修改后的模板。

1. 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。
2. 选择 **Upload a template to Amazon S3**（将模板上传到 **Amazon S3**），选择 firewall-v2.0.template 并单击 **Open**（打开）和 **Next**（下一个）。
3. 指定 **Stack name**（堆栈名称）。堆栈名称允许您唯一标识此模板部署的所有资源。

©2024 Palo Alto Networks, Inc.

STEP 7 | 配置 VPC 的参数。

1. 输入参数 **VPC Configuration**（**VPC** 配置），如下：
   1. 输入 **VPCName**。
   2. 选择您的设置跨越的两个可用性区域 **Select two AZs**（选择两个 **AZ**）。

STEP 8 | 选择 VM 系列防火墙的首选项。

1. 为 VM 系列防火墙查找 AMI ID 并输入它。确保 AMI ID 与您选择使用的 AWS 区域、PAN-OS 版本和 BYOL 或 PAYG 许可选项相匹配。
2. 选择 EC2 **Key pair**（密钥对）（从下拉菜单中）启动防火墙。要登录防火墙，您必须提供此密钥对的名称以及与其关联的私钥。
3. 限制 SSH 访问防火墙的管理界面。确保提供与专用管理 IP 地址或网络相对应的 CIDR 块。不要将允许的源网络范围设置得比所需的大，并且不要将允许的源配置为 0.0.0.0/0。在将模板配置到模板上之前验证您的 IP 地址，以确保您不会锁定自己。
4. 如果您要 **Enable Debug Log**（启用调试日志），请选择 **Yes**（是）。启用调试日志会生成详细列出的日志，以帮助解决部署问题。这些日志是使用堆栈名称生成的，并保存在 AWS CloudWatch 中。

默认情况下，模板使用 CPU 利用率作为 VM 系列防火墙的扩展参数。自定义 PAN-OS 指标会自动发布到与您之前指定的堆栈名称匹配的 CloudWatch 命名空间。

STEP 9 | 指定 Amazon S3 存储桶的名称。

您可以使用一个 *S3* 存储桶作为引导程序包和 *zip* 文件。

1. 输入包含引导程序包的 S3 存储桶的名称。

   如果引导桶未正确设置，或者输入的存储桶名称不正确，则引导进程将失败，并且您无法登录到防火墙。对负载均衡器的运行状况检查也失败。
2. 输入包含 panw-aws.zip 文件的 S3 存储桶的名称。

©2024 Palo Alto Networks, Inc.

STEP 10 | 指定启用 API 访问防火墙和 Panorama 的密钥。

1. 输入防火墙必须用来验证 API 调用的密钥。默认密钥基于示例 bootstrap.xml 文件，您只能将其用于测试和评估。对于生产部署，您必须为 API 调用创建单独的 PAN-OS 登录并生成关联的密钥。
2. 如果您使用 Panorama 进行集中管理，请输入 API 密钥以允许 AWS Lambda 对 Panorama 进行 API 调用。对于生产部署，您应该为 API 调用创建一个单独的登录并生成关联的密钥。
3. 复制并粘贴您的帐户的许可证停用 API 密钥。在发生伸缩事件时，需要此密钥才能成功禁用防火墙上的许可证。要获得此密钥：
   1. 登录到客户支持门户。
   2. 选择 **Assets**（资产） > **API Key Management**（**API** 密钥管理）。
   3. 复制 API 密钥。

STEP 11 | 输入应用程序负载均衡器的名称。

STEP 12 | （可选）应用标签来识别与 VM 系列自动扩展模板关联的资源。

添加“名称 — 值”对来识别和分类此堆栈中的资源。

STEP 13 | 查看模板设置并启动模板。

1. 选择 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我承认此模板可能会导致 **AWS CloudFormation** 创建 **IAM** 资源）。
2. 单击 **Create**（创建）以启动模板。显示 CREATE_IN_PROGRESS 事件。
3. 成功部署时，状态会更新到 CREATE_COMPLETE。

除非您定制了模板，否则 VM 系列自动扩展模板将启动一个 ASG，其中每个 AZ 中包含一个位于应用程序负载均衡器后的 VM 系列防火墙。

STEP 14 | 验证模板是否启动了所有必需的资源。

1. 在 AWS 管理控制台上，选择堆栈名称以查看资源列表的 **Output**（输出）。
2. 在 EC2 仪表盘上，选择 **Auto Scaling Groups**（自动扩展组）。验证在每个 AZ 中，每个 ASG 具有一个防火墙的 VM 系列防火墙有一个 ASG。ASG 名称前缀包含堆栈名称。
3. 登录到 VM 系列防火墙。您必须部署跳转服务器或使用 Panorama 访问防火墙上的 Web 界面。

- 防火墙启动并可用于处理流量可能需要长达 *20* 分钟的时间。
- 完成测试或生产部署时，确保停止收费的唯一方法是彻底删除堆栈。关闭实例或将 *ASG* 最大值更改为 *0* 还不够。

©2024 Palo Alto Networks, Inc.

STEP 15 | 保存以下信息。部署应用程序模板时，您需要提供这些值作为输入。

- 每个 AZ 中的 NAT 网关的 IP 地址。如果将应用程序部署在不同的 VPC 中，则需要此 IP 地址来限制对 Web 服务器的 HTTP 访问。指定此 IP 地址可确保防火墙确保在不同的 VPC 中访问您的应用程序，并且任何人都无法绕过防火墙直接访问 Web 服务器。如果您未输入 NAT 网关 IP 地址，示例应用程序模板 (panw_aws_nlb_vpc-2.0.template) 会显示模板验证错误；您必须以逗号分隔列表的方式输入 IP 地址。
- 网络负载均衡器 SQS URL。防火墙堆栈中的 AWS Lambda 功能监控此队列，以便它可以了解您部署的任何网络负载均衡器，并在 VM 系列防火墙上创建 NAT 策略规则（每个应用程序一个），使防火墙可以将流量发送到网络负载均衡器 IP 地址。

启动应用程序模板

应用程序模板允许您完成三明治拓扑结构，并提供应用程序目标以便您可以评估自动扩展解决方案。此应用程序模板在使用防火墙模板部署的 VM 系列防火墙自动扩展组后面部署网络负载均衡器和一对 Web 服务器。此模板中的 Web 服务器具有公共 IP 地址，可直接出站访问以检索软件更新。使用此模板评估解决方案，但构建自己的模板以部署到生产中。对于自定义模板，请确保启用应用程序模板和防火墙模板之间的 SQS 消息传递。

在启动应用程序模板时，您必须根据是否要将应用程序模板部署在部署防火墙模板的相同 VPC (panw_aws_nlb-2.0.template) 中或在单独的 VPC 中进行选择 (panw_aws_nlb_vpc-2.0.template)。对于单独的 VPC，该模板为跨帐户部署提供支持。跨帐户部署要求您创建 IAM 角色并启用可信的 AWS 帐户和受可信的 AWS 帐户之间的权限和可信关系，并且在启动模板时需要输入帐户信息作为输入。

STEP 1 | （仅适用于跨帐户部署）创建 IAM 角色。参考 AWS 文档。

此角色授予对属于不同 AWS 帐户的用户的访问权限。该用户需要权限才能访问防火墙模板中的简单队列服务 (SQS) 资源。防火墙使用此队列来了解您部署的每个网络负载均衡器，以便它可以创建 NAT 策略以将流量发送到网络负载均衡器后面的 Web 服务器。

- 对于 **Account ID**（帐户**ID**），键入要部署应用程序模板的帐户的 AWS 帐户 ID。通过指定该帐户 ID，您可以授予访问您帐户中承载防火墙模板资源的资源的权限。
- 选择 **Require external ID**（需要外部 **ID**），并输入一个共享密钥的值。指定外部 ID 允许用户只有在请求包含正确的值时才承担角色。
- 选择 **Permissons**（权限）以允许 **Amazon SQS Full Access**（**Amazon SQS** 完全访问）。

STEP 2 | 使用 Palo Alto Networks 公共 S3 存储桶或准备您的私有 (S3) 存储桶以启动应用程序模板。

1. 创建一个包含所有文件的 zip 文件 GitHub 存储库，不包括下面屏幕截图中名为 nlb.zip 的三个 .template 文件。
2. 将 zip 文件上传到先前创建的 S3 存储桶或新的存储桶。
3. 将 pan_nlb_lambda 模板复制到您将 nlb.zip 文件复制到的同一个存储桶中。

©2024 Palo Alto Networks, Inc.

STEP 3 | 选择要启动的应用程序模板。

1. 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。
2. 选择 **Upload a template to Amazon S3**（将模板上传到 **Amazon S3**），选择 panw_aws_nlb-2.0.template 来部署模板在与防火墙相同的 VPC 内启动的资源，或选择 panw_aws_nlb_vpc-2.0.template 来将资源部署到不同的 VPC。单击 **Open**（打开）和 **Next**（下一步）。
3. 指定 **Stack name**（堆栈名称）。堆栈名称允许您唯一标识使用此模板部署的所有资源。

STEP 4 | 配置 VPC 和网络负载均衡器的参数。

1. 选择两个可用性区域，您的设置将跨越 **Select list of AZ**（选择 **AZ** 列表）。如果您在同一个 VPC 内部署，请确保选择与防火墙模板相同的可用性区域。
2. 输入 **CIDR Block for the VPC**（**VPC** 的 **CIDR** 块）。默认 CIDR 为 192.168.0.0/16。
3. （仅当您使用 panw_aws_nlb-2.0.template 在同一个 VPC 中部署应用程序时）

   选择与每个 AZ 中的防火墙上的可信子网关联的 **VPC ID** 和 **Subnet IDs**（子网 **ID**）。网络负载均衡器连接到防火墙上的可信子网，以完成负载均衡器夹层式拓扑。
4. 输入网络负载均衡器的名称。

STEP 5 | 配置 AWS Lambda 的参数。

1. 输入存储 nlb.zip 和 pan_nlb_lambda.template 的 S3 存储桶名称。
2. 输入 pan_nlb_lambda.template 的名称和 zip 文件名称。
3. 粘贴您之前复制的 SQS URL。
4. 输入一个唯一的 **TableName**（表名）。此表存储部署中与网络负载均衡器关联的应用程序的端口和 IP 地址的映射。

   当您删除应用程序堆栈时，该表被删除。因此，如果网络负载均衡器的多个实例写入同一个表并删除该表，则防火墙上的 NAT 规则将无法正常运行，并且应用程序流量可能不准确地转发给错误的端口/网络负载均衡器。

STEP 6 | 修改 Web 服务器 EC2 实例类型以满足部署需求。

STEP 7 | 选择启动 Web 服务器的 EC2 **Key pair**（密钥对）（从下拉菜单中）。要登录到 Web 服务器，您必须提供密钥对名称和与其关联的私钥。

©2024 Palo Alto Networks, Inc.

STEP 8 | （仅当您使用 panw_aws_nlb_vpc-2.0.template 时）锁定对 Web 服务器的访问。

1. 限制 **SSH From**（**SSH** 来自）访问 Web 服务器。只有您在此处列出的 IP 地址才能登录到 Web 服务器。
2. 限制对 Web 服务器的 HTTP 访问。从防火墙模板输出中输入 NAT 网关的公共 IP 地址，且必须使用逗号分隔 IP 地址。通过输入 NAT 网关 IP 地址，您可以确保应用程序服务器的所有 Web 通信都受到 VM 系列防火墙的保护。

STEP 9 | （仅当您使用 panw_aws_nlb_vpc-2.0.template 时）配置其他参数需要在不同的 VPC 中启动应用程序模板堆栈。

1. 如果您在与防火墙模板相同的 AWS 帐户中部署此应用程序模板，选择 SameAccount **true**，并将交叉帐户角色和外部 ID 留空；对于跨帐户部署，选择 **false**。

   对于跨帐户部署，为 **CrossAccountRole** 请输入该帐户的 Amazon 资源编号 (ARN)，以及您在 （仅用于跨帐户部署）创建 IAM 角色中定义的 **ExternalId**（外部 **ID**）。请参阅 AWS 文档。从在AWS管理控制台上的 **Support**（支持） > **Support Center**（支持中心）可以从中获得 ARN。
2. 输入您要在其中部署应用程序模板资源 **VPC Name**（**VPC** 名称）。
3. 可选为网络负载均衡器的管理子网更改 **NLBSubnetIPBlocks**。

STEP 10 | 查看模板设置并启动模板。

STEP 11 | 验证网络负载均衡器已部署并处于就绪状态。

STEP 12 | 获得应用程序负载均衡器的 **DNS name**（**DNS** 名称），并将其输入到 Web 浏览器。

例如：http://MVpublic-elb-123456789.us-east-2.elb.amazonaws.com/

当网页显示时，您已成功启动自动扩展模板。

STEP 13 | 验证每个防火墙对每个网络负载均衡器的 IP 地址都有 NAT 策略规则。

当您部署应用程序模板以启动网络负载均衡器和 Web 服务器对的另一个实例时，防火墙会了解为下一个网络负载均衡器实例分配的端口并创建另一个 NAT 策略规则。因此，如果您部署应用程序模板三次，防火墙对等口 81、82 和 83 有三个 NAT 策略规则。

STEP 14 | 如果您不止一次启动了应用程序模板，则需要为 ELB 服务启用流量。

为 **ELB** 服务启用流量（**v2.0** 和 **v2.1**）

如果在部署中添加第二个或额外的内部负载均衡器，则必须完成其他配置，以便内部负载均衡器、VM 系列防火墙自动扩展组和 Web 服务器可以报告为正常运行，并且流量负载均衡利用您的全部 AWS 资源。

©2024 Palo Alto Networks, Inc.

在 *v2.0* 中，*ILB* 只能是网络负载均衡器。在 *v2.1* 中，*ILB* 可以是应用程序负载均衡器或网络负载均衡器。

STEP 1 | 在 AWS 管理控制台上，验证 DynamoDB 表上为每个网络均衡器分配的端口。

在启动新的内部负载均衡器时，应用程序模板必须将 SQS 消息发送到您在启动模板时作为输入提供的 SQS URL。防火墙模板中的 AWS Lambda 功能监控 SQS 并将端口映射添加到防火墙模板的 DynamoDB 表。从端口 81 开始，为您部署的每个额外内部负载均衡器分配的端口将增加 1。因此，第二个内部负载均衡器使用端口 82，第三个端口使用端口 83。

1. 选择 AWS 管理控制台上的 **DynamoDB** 服务。
2. 选择 **Tables**（表），然后单击与防火墙模板的堆栈名称匹配的表。例如，MV-CFT20-firewall-us-east-2。

   在“项目”列表中，查看发布到与防火墙模板关联的 SQS 的内部负载均衡器使用的端口。

STEP 2 | 创建目标组。内部负载均衡器使用您为目标组中服务器指定的端口和协议向注册目标发送请求。

添加新目标组时，请使用在 DynamoDB 表上验证的端口信息。

STEP 3 | 在内部负载均衡器上编辑侦听器规则，将请求路由到目标 Web 服务器中。

1. 在 AWS 管理控制台上，在 Load Balancing（负载均衡）部分中选择 **Load Balancers**（负载均衡器），然后选择与您的堆栈名称匹配的内部负载均衡器。
2. 选择 **View/edit rules**（查看/编辑规则），修改监听器的规则。
3. 选择 **View/edit rules**（查看/编辑规则），并添加基于路径的路由以将流量转发到您在上面定义的目标组，如下所示：

STEP 4 | 将目标组连接到 VM 系列防火墙自动扩展组。

1. 在 Auto Scaling（自动扩展）部分中选择 **Auto Scaling Groups**（自动扩展组），然后选择一个与堆栈名称匹配的自动扩展组。
2. 选择 **Details**（细节） > **Edit**（编辑），并从 **Target Groups**（目标组）下拉列表中选择新的目标组。

©2024 Palo Alto Networks, Inc.

STEP 5 | 登录到应用程序模板部署的每个 Web 服务器，使用目标组名称创建一个新目录，并将 index.html 文件复制到目录中。在设置 index.html 文件的路径之前，此 Web 服务器的运行状况检查报告为不健康。

```
sudo su
cd/var/www/html
mkdir <target-groupname>
cp index.html <target-groupname>
```

STEP 6 | 验证 Web 服务器的监控状态。

选择 **Auto Scaling Groups**（自动扩展组），并使用应用程序堆栈名称来查找 Web 服务器自动扩展组，从而验证 Web 服务器是否报告健康。

自定义 Bootstrap.xml 文件 (v2.0)

GitHub 存储库中提供的 bootstrap.xml 文件为防火墙管理员使用默认的用户名和密码。在生产环境中部署 VM 系列自动扩展模板之前，您至少必须为 VM 系列防火墙上的管理帐户创建唯一的用户名和密码。或者，您可以使用区域、策略规则和安全配置文件完全配置防火墙并导出黄金配置快照。然后，您可以将此配置快照用作生产环境的 bootstrap.xml 文件。

您可以通过两种方法自定义用于生产环境的 bootstrap.xml 文件：

- 选项 **1**：使用 GitHub 存储库中提供的引导文件在 AWS 上启动 VM 系列防火墙，修改防火墙配置并导出配置以为 VM 系列防火墙自动扩展模板创建新的 bootstrap.xml 文件。请参阅使用 GitHub 引导文件作为种子。
- 选项 **2**：在 AWS 上启动新的 VM 系列防火墙而不使用引导文件，添加 NAT 策略规则以确保 VM 系列防火墙正确处理流量，并导出配置以为 VM 系列防火墙自动扩展模板创建新的 bootstrap.xml 文件。请参阅从头开始创建新的引导文件。

> 如果您已经部署该模板，现在需要更改管理用户的凭据或添加新的管理用户并更新模板堆栈，请参阅修改管理帐户和更新堆栈。

从头开始创建一个新的引导文件

使用支持的 PAN-OS 版本的 AMI 在 AWS 上启动新的 VM 系列防火墙（有关 Panorama 插件，请参阅兼容性矩阵），而无需使用示例 bootstrap.xml 文件，并导出配置以创建新的 bootstrap.xml 文件以用于 VM 系列自动扩展模板 v2.0。

STEP 1 | 在 AWS 上部署 VM 系列防火墙（无需执行故障排除），并在 VM 系列防火墙的命令行界面 (CLI) 上使用 SSH 的公共 IP 地址。您需要为防火墙配置新管理密码。

STEP 2 | 登录到防火墙 Web 界面。

STEP 3 | （可选）配置防火墙。您可以配置数据面板接口、区域和策略规则。

STEP 4 | 在防火墙上 **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 5 | 导出配置文件，并将其命名为 **`bootstrap.xml`**。（**Device**（设备） > **Setup**（设置） > **Operation**（操作） > **Export Named Configuration Snapshot**（导出已命名的配置快照））。

STEP 6 | 从 GitHub 存储库下载 bootstrap.xml 文件，使用文本编辑工具打开，并复制第 353 至 356 行。这些行定义 AWS CloudWatch 命名空间，以便防火墙发布防火墙自动扩展所需的自定义 PAN-OS 指标。

STEP 7 | 编辑您之前导出的配置文件以包含 AWS CloudWatch 信息。

搜索 `</management>` 并将第 353 行到第 356 行粘贴到 `</management>`。

STEP 8 | 删除管理接口配置。

1. 搜索 `</service>` 并删除后面的 ip-address、netmask 和 default-gateway。
2. 搜索 `</type>` 并删除后面的 ip-address、netmask、default-gateway 和 public-key。

STEP 9 | 保存文件。您现在可以继续 为 AWS (v2.0) 启动 VM 系列自动扩展模板。

使用 **GitHub** 引导文件作为种子

使用 GitHub 存储库中提供的引导文件从 AWS Marketplace 中的 AWS 上启动 VM 系列防火墙，修改生产环境的防火墙配置。然后，导出配置以创建现在可用于 VM 系列自动扩展模板的新 bootstrap.xml 文件。

STEP 1 | 要启动防火墙，请参阅在 AWS 上引导 VM 系列防火墙。

STEP 2 | 添加弹性网络接口 (ENI) 并将弹性IP地址 (EIP) 与其关联，以便您可以访问 VM 系列防火墙上的 Web 界面。有关详细信息，请参阅在 AWS 上启动 VM 系列防火墙。

STEP 3 | 使用 EIP 地址以 admin 作为用户名和密码登录防火墙 Web 界面。

STEP 4 | 为管理用户帐户添加安全密码（**Device**（设备） > **Local User Database**（本地用户数据库） > **Users**（用户））。

STEP 5 | （可选）配置防火墙以保护您的生产环境。

STEP 6 | 在防火墙上 **Commit**（提交）更改。

STEP 7 | 为管理员帐户生成新 API 密钥。将此新密钥复制到新文件。启动 VM 系列自动扩展模板时，您需要输入此 API 密钥；AWS 服务使用 API 密钥来部署防火墙并发布用于自动扩展的指标。

STEP 8 | 导出配置文件，并将其另存为 **`bootstrap.xml`**。（**Device**（设备） > **Setup**（设置） > **Operation**（操作） > **Export Named Configuration Snapshot**（导出已命名的配置快照））。

STEP 9 | 使用文本编辑工具打开 bootstrap.xml 文件并删除管理接口配置。

 ©2024 Palo Alto Networks, Inc.

STEP 10 | （如果您导出 PAN-OS 8.0 配置，则为必需）确保用于验证 Palo Alto Networks 服务器的设置已禁用。查找 `<server-verification>no</server-verification>`。

STEP 11 | 如果值为 `yes`，将其更改为 **`no`**。

STEP 12 | 保存文件。您现在可以继续 为 AWS (v2.0) 启动 VM 系列自动扩展模板。

应用程序模板和防火墙模板之间的 SQS 消息传递

因此，使用 firewall-v2.0.template 部署的 VM 系列防火墙可以检测流量并将其发送到要自动分配传入流量的网络负载均衡器，防火墙模板包含一个 Lambda 函数，该函数可监控简单队列服务消息。该消息允许 Lambda 函数了解新的网络负载均衡器，然后在防火墙上自动创建 NAT 策略规则，以将流量发送到网络负载均衡器的 IP 地址。为了在 AWS 基础架构内正确路由流量，该消息还必须包括 DNS、VPC ID 和网络负载均衡器所属的 AZ 的基本信息。

如果您正在构建自己的应用程序模板，则必须设置应用程序模板以将两种类型的消息发布到 SQS URL，VM 系列自动扩展模板 2.0 版中的防火墙模板使用该模板来了解它必须使用的网络负载均衡器在您的环境中分配流量：

- ADD-NLB 消息，用于在新的网络负载均衡器可用时通知防火墙。
- DEL-NLB 消息，用于在网络负载均衡器终止并不再可用时通知防火墙。

每种消息类型的以下示例均包括示例值。您需要使用符合您的部署的值修改这些消息。

ADD-NLB 消息

```
msg_add_nlb= { 'MSG-TYPE':'ADD-NLB', 'AVAIL-ZONES': [{'NLB-
IP':'192.168.2.101', 'ZONE-NAME':'us-east-2a', 'SUBNET-ID':
 'subnet-2a566243'}, {'NLB-IP':'192.168.12.101', 'ZONE-NAME':'us-
east-2b', 'SUBNET-ID': 'subnet-2a566243 '}], 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', 'VPC-ID':
 'vpc-42ba9f2b', 'NLB-NAME': 'publicelb1' }
```

DEL-NLB 消息

```
msg_del_nlb= { 'MSG-TYPE':'DEL-NLB', 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', }
```

有关如何将消息发送到 Amazon SQS 队列的详细信息，请参阅 AWS 文档，或在示例应用程序模板包中查看 **describe_nlb_dns.py**，以查看应用程序模板如何构造消息。

AWS 更新与 VM 系列自动扩展模板 (v2.0)

堆栈更新允许您修改 VM 系列自动扩展模板 (firewall-v2.0.template) 部署的资源。不要删除现有的部署并重新部署解决方案，而是使用堆栈更新来修改以下参数：

- 许可证 — 从 BYOL 切换到 PAYG，反之亦然，或从一个 PAYG 包切换到另一个。

©2024 Palo Alto Networks, Inc.

- 其他堆栈资源 — 更改启动配置参数，例如您的自动扩展组的 Amazon 机器映像 (AMI) ID、AWS 实例类型、密钥对。您还可以更新与防火墙上的管理用户帐户关联的 API 密钥。

  通过更改 *AMI-ID*，您可以使用不同的 *PAN-OS* 版本部署 *VM* 系列防火墙的新实例。

在部署 VM 系列自动扩展模板时，会自动为您创建自动扩展组和启动配置。启动配置是自动扩展组用于启动 EC2 实例的模板，它为您的自动扩展组指定参数，例如 AMI ID、实例类型、密钥对。要使用更新后的参数启动 VM 系列防火墙，必须先更新堆栈，然后删除每个 AZ 中现有的自动扩展组。要防止服务中断，请首先删除一个 AZ 中的自动扩展组，然后等待新的防火墙实例使用更新的堆栈参数启动。然后，验证在继续完成其他 AZ 中的更改之前，防火墙已经继承了您所做的更新。

对于关键应用程序，在维护窗口期间执行堆栈更新。

您可以直接更新堆栈或创建更改集。本文档中的工作流程将引导您完成手动堆栈更新。

STEP 1 | 在 AWS CloudFormation 控制台中，选择您要更新并选择的父堆栈 **Actions**（操作） > **Update Stack**（更新堆栈）。

STEP 2 | 修改您想要更新的资源。

- PAN-OS 版本 — 要修改 PAN-OS 版本，为您要使用的版本查找 AMI ID 并输入 ID。
- 许可证选项 — 从 BYOL 切换到 PAYG 或跨 PAYG 套餐 1 和 2。

如果您切换到 BYOL，请确保将身份验证包含在引导程序包中（请参阅步骤 3 和 5）。

如果您在 PAYG 套餐版本 1 和 2 之间切换，查找 AMI ID 用于 VM 系列防火墙。

- 其他堆栈资源 — 您可以修改堆栈资源的 AMI ID、实例类型、安全组、密钥对或与防火墙上的管理用户帐户关联的 API 密钥。

如果您创建新的管理用户帐户或修改防火墙上现有管理员的凭据，为了更新该堆栈并使用更新的 API 密钥部署新防火墙，您需要按照修改管理帐户和更新堆栈。

STEP 3 | 确认通知并查看更改并单击 **Update**（更新）启动堆栈更新。

STEP 4 | 在 **EC2 dashboard**（**EC2** 仪表盘） > **Auto Scaling Groups**（自动扩展组），并选择一个 AZ 来删除 ASG。

删除 ASG 会自动触发重新部署新 ASG 的过程。新 ASG 中的防火墙使用更新后的堆叠配置。

STEP 5 | 验证是否使用更新的参数在新的 ASG 中启动 VM 系列防火墙。

使用分阶段推出流程，您可以彻底测试新的 ASG 并确保火管正确地处理流量。然后等待一小时，然后继续下一个 ASG。

©2024 Palo Alto Networks, Inc.

STEP 6 | 重复步骤 4 和 5 以替换其他 AZ 中的 ASG。

修改管理帐户和更新堆栈 (v2.0)

如果您已经部署了该模板，并且现在要更改管理帐户的密码或在 VM 系列防火墙上创建新的管理用户帐户，则必须生成新的 API 密钥并使用新的 API 密钥更新模板堆栈管理用户帐户。为了确保使用更新的管理用户帐户配置新防火墙实例，需要导出防火墙配置并将其重命名为 bootstrap.xml，然后将其上传到 VM 系列 AutoScaling 模板使用的 S3 引导文件夹。

STEP 1 | 登录到防火墙的 Web 界面并更改现有管理用户的凭证或创建新帐户。

STEP 2 | 生成 API 密钥。

STEP 3 | 导出当前正在运行的配置并将其重命名为 bootstrap.xml。

STEP 4 | 将此 bootstrap.xml 文件上传到 S3 引导文件夹；请参阅自定义 Bootstrap.xml 文件 (v2.0)。

STEP 5 | 更新堆栈中的 API 密钥以确保新启动的防火墙拥有更新后的管理员帐户。

请参阅 AWS 的堆栈更新与 VM 系列自动扩展模板 (v2.0)。

适用于 AWS 版本 2.1 的 VM 系列自动扩展模板

通过 VM 系列自动扩展模板，您可以部署 VM 系列防火墙的单个自动扩展组 (ASG)，以保护从 Internet 到 AWS 上的应用程序工作负载的入站流量。您可以在单个 VPC 中部署 VM 系列防火墙 ASG 和应用程序工作负载，如下所示。

您还可以将防火墙 ASG 部署在集中式 VPC 中，将应用程序工作负载部署在同一区域内的单独 VPC 中，形成集线器和分支架构，如下所示。

借助中心和分支架构，您可以简化为许多应用程序，VPC 或帐户的 AWS 部署提供集中安全性和连接性。这种架构可以提高灵活性。您的网络安全管理员可以管理防火墙 VPC，DevOps 管理员或应用程序开发人员可以管理应用程序 VPC。

确保应用程序 *VPC* 连接到没有 *Internet* 网关 *(IGW)* 的防火墙 *VPC*，并使用连续监控和安全合规性服务，例如 Prisma 公共云。

您可以使用单个 AWS 帐户或多个 AWS 帐户来监控和保护 VPC 与 Internet 之间的流量。在单个 VPC 中集中防火墙可以降低具有多个 VPC 和/或多个帐户的部署的成本。

为了提供保护应用程序工作负载的灵活性，2.1 版本允许您为面向 VM 系列防火墙 ASG 的外部负载均衡器以及面向应用程序负载的内部负载均衡器 (ILB) 部署应用程序负载均衡器或网络负载均衡器。

©2024 Palo Alto Networks, Inc.

当应用程序负载均衡器面向应用程序工作负载时，您可以使用 VPC 对等将防火墙 VPC 连接到应用程序 VPC。当 NLB 面向应用程序工作负载时，您可以使用 VPC 对等或 AWS 专用链接来连接防火墙和应用程序 VPC，如下所述：

防火墙 **VPC LB**（外部）	应用程序 **VPC LB**（内部）	连接方法
ALB	NLB	AWS 专用链接
NLB	NLB	AWS 专用链接
NLB	ALB	VPC 对等
ALB	ALB	VPC 对等

如果部署在单个 VPC 中，则可以使用上表中的所有负载均衡组合。

您可以在绿色字段（新 VPC 和应用程序）和棕色字段（现有 VPC 和应用程序）用例中部署模板。

模板	新	现有
防火墙	firewall-new-vpc-v2.1.template panw-aws-same-vpc-v2.1.template	firewall-existing-vpc-v2.1.template panw-aws-same-vpc-v2.1.template
应用程序	panw-aws-nlb-new-vpc-v2.1.template panw-aws-alb-new-vpc-v2.1.template	panw-aws-alb-existing-vpc-v2.1.template panw-aws-nlb-existing-vpc-v2.1.template

适用于 **AWS (v2.1)** 的 **VM** 系列自动扩展模板具有哪些组件？

AWS 的 VM 系列自动扩展模板包含以下构建基块。

- VM 系列防火墙模板
- 应用程序模板
- Lambda 函数
- Panorama
- 引导文件

VM 系列防火墙模板

防火墙模板在跨越至少两个可用性区域 (AZ) 的自动扩展组中部署面向 Internet 的外部负载均衡器和 VM 系列防火墙。外部负载均衡器在 VM 系列防火墙池中分配传入的 VPC 流量。它可以是应用程序负载均衡器 (ALB) 或网络负载均衡器 (NLB)。VM 系列防火墙自动发布启用自动扩展的自定义 PAN-OS 指标。

©2024 Palo Alto Networks, Inc.

模板	说明
firewall-new-vpc-v2.1.template	在新的 VPC 中部署具有两到四个可用性区域的防火墙堆栈。
firewall-existing-vpc-v2.1.template	在现有 VPC 中部署具有 2 到 4 个可用性区域的防火墙堆栈。 要在现有 VPC 中部署，您必须输入： • VPC ID • Internet 网关 ID。这是一个现有网关。 • 管理、不可信、可信、NAT 网关和 Lambda 子网的子网 CIDR 列表。该模板使用 CIDR 创建这些子网。 如果您选择创建新的 ELB，该模板会将防火墙 ASG 连接到 ELB 后端池。如果使用现有 ELB，则必须手动将防火墙 ASG 连接到现有负载均衡器后端。

有关这些参数的详细信息，请参阅在启动前自定义防火墙模板（v2.0 和 v2.1）。

应用程序模板

应用程序模板在每个可用性区域 (AZ) 中使用 Web 服务器部署内部负载均衡器 (ILB) 和一个自动扩展组。

模板	说明
panw-aws-same-vpc-v2.1.template	在与防火墙 VPC 相同的 VPC 中部署应用程序。您可以选择网络或应用程序负载均衡器。
panw-aws-alb-new-vpc-v2.1.template	使用 ALB 作为内部负载均衡器，并在防火墙 VPC 和应用程序 VPC 之间使用 VPC 对等，在新的 VPC 中部署应用程序。支持同帐户和跨帐户部署。 您必须提供以下参数： • 中心帐户 ID • 适用于 VPC 对等的中心 VPC ID • 中心 VPC 信任子网 CIDR。建立 VPC 对等后，模板将使用这些 CIDR 构建路由表（每个可用性区域一个 CIDR）。 • StsAssumeRoleARN（SQS 访问的 Hub 模板的输出）

©2024 Palo Alto Networks, Inc.

模板	说明
panw-aws-nlb-new-vpc-v2.1.template	新 VPC 中部署应用程序，使用 NLB 作为内部负载均衡器在，并在防火墙 VPC 和应用程序 VPC 之间使用 NLB 端点服务/接口进行通信。 您必须提供这些参数。 • 中心帐户 ID • StsAssumeRoleARN（SQS 访问的 Hub 模板的输出）
panw-aws-alb-existing-vpc-v2.1.template	在现有应用程序 VPC 中部署 ALB。您必须提供应用程序的 VPC ID 和现有的子网 ID。 此模板在应用程序 VPC 中部署负载均衡器并建立 Lambda 资源。您必须从任何现有负载均衡器分离目标工作负载，并将其连接到新的负载均衡器。
panw-aws-nlb-existing-vpc-v2.1.template	在现有应用程序 VPC 中部署 NLB。新 VPC 中部署应用程序，使用 NLB 作为内部负载均衡器在，并在防火墙 VPC 和应用程序 VPC 之间使用 NLB 端点服务/接口进行通信。

Lambda 函数

AWS Lambda 提供强大的事件驱动自动化，无需复杂的编排软件。AWS Lambda 监控简单队列服务 (SQS) 以了解发布到队列的负载均衡器（ALB 或 NLB）。当 Lambda 函数检测到新的负载均衡器时，它会创建一个新的 NAT 策略规则并将其应用于 ASG 内的 VM 系列防火墙。防火墙对每个应用都有 NAT 策略规则，防火墙使用 NAT 策略规则（将端口映射到负载均衡器 IP 地址）将流量转发到应用程序 Web 服务器前面的负载均衡器。

Lambda 函数还会删除 Lambda 添加到 Panorama 中的设备组和模板堆栈的所有配置项。这包括推送到 VM 系列防火墙的 NAT 规则、地址对象和静态路由。Lambda 函数也处理取消许可证。

要了解有关 Lambda 函数的详细信息，请参阅 **Palo Alto Networks AWS** 自动扩展文档。

Panorama

您必须在 Panorama 模式下安装 Panorama 管理服务器才能配置自动扩展 v2.1。

Panorama 管理服务器从单一位置提供对多个 Palo Alto Networks 下一代防火墙的集中监控和管理。Panorama 可让您监督遍历网络的所有应用程序、用户和内容，然后利用收集的信息创建应用程序启用策略来保护和控制网络。如果您不熟悉 Panorama，请参阅 Panorama 管理员指南。

托管防火墙使用 `init-config.txt` 文件进行引导。GitHub 存储库中包含一个示例文件，以便在现有 Panorama 中创建模板堆栈和设备组时复制配置。

©2024 Palo Alto Networks, Inc.

在 *Panorama* 中创建的不可信和可信区域必须全部为小写。

在 Panorama 中，您必须使用 DHCP 配置网络接口。

- 只有 eth1/1 应自动创建默认路由可信和非可信区域。
- 安全策略区域命名为 `untrust` 和 `trust`。

  所有区域名称必须为小写

- 模板配置名为 `pandemo` 的管理员帐户和密码 `demopassword`。
- 使用命名约定 VR-<*TemplateStackName*> 创建虚拟路由器。在虚拟路由器 ECMP 选项卡上，启用 ECMP。
- 要在 Panorama 上设置 DNS 服务器地址，请选择 **Device**（设备）> **Setup**（设置）> **Services**（服务）。将 **Primary DNS Server**（主 **DNS** 服务器）设置为 169.254.169.253，将 **Secondary DNS Server**（辅助 **DNS** 服务器）设置为 8.8.8.8，并将 **FQDN Refresh Time (sec)**（**FQDN** 刷新时间（秒））设置为 60。Panorama 需要 AWS DNS 服务器 IP 地址来解析 AWS 上内部负载均衡器的 FQDN。FQDN 刷新时间是 Panorama 提交新检测到的内部负载均衡器的间隔。

应用程序模板启动后，Lambda 将在 Panorama 中填充以下内容：

- NAT 政策
- 应用程序模板中 LB 的地址对象
- 虚拟路由器中的静态路由
- Tcp81 服务对象

V2.1 防火墙模板包含一个 AWS NAT 网关，防火墙用来启动用于检索更新的出站请求，连接到 Panorama 以及将指标发布到 AWS CloudWatch。NAT 网关还为每个区域附加了弹性 IP 地址。

您需要以下 Panorama 资源才能使用 AWS 的自动扩展模板。

Panorama API 密钥	您需要 Panorama API 密钥才能对 API 进行身份验证。Lambda 使用您的 API 密钥自动配置模板和设备组选项。要生成 API 密钥，请参阅获取 API 密钥。
Panorama 许可证停用密钥	该模板需要许可证停用 API 密钥，并启用“验证更新服务器标识”以从 Panorama 中停用许可证密钥。您要从 Palo Alto 客户支持门户获取许可证取消激活密钥，如安装许可证 API 密钥中所述。
Panorama VM-Auth-Key	您需要一个 vm-auth-key 来启用引导的防火墙，以连接到 Panorama 和接收其引导程序配置。请参阅在 Panorama 上生成 VM 身份验证密钥。

©2024 Palo Alto Networks, Inc.

Panorama 管理界面访问	• 端口 **443 (HTTPS)** — 初始部署防火墙模板后，保持 HTTPS 开放，以便 Lambda 可以连接到 Panorama。等待在 Panorama 中收到以下连接确认： 保护端口 443 时，您可以指定允许连接的 IP 地址范围，以及分配给 NAT 网关的 EIP。有两个 NAT 网关和与之关联的 EIP。要在 AWS 中查找 NAT 网关 EIP，请转到 **VPC** > **NAT Gateways**（**NAT** 网关）。请注意 HTTPS 安全组的 EIP 信息。 • 端口 **3978** — 端口 3978 必须能够从任何 IP 地址接收流量。

引导文件

GitHub 自动扩展存储库包括一个 `init-cfg.txt` 文件，以便 VM 系列防火墙具有以下基本配置：

- 执行接口交换以便 VM 系列防火墙的不可信流量为 eth0 使用 AWS ENI。
- 与 Panorama 通信以进行设备组和模板配置。

自动扩展 GitHub 存储库具有入门的基本配置。该自动扩展解决方案需要交换数据平面和管理界面，以使负载均衡器能够将 Web 流量转发到 VM 系列防火墙的自动扩展层。有关使用 Amazon ELB 进行管理接口映射的详细信息，如管理接口映射以用于 Amazon ELB 中所述。

规划部署 AWS 的 VM 系列自动扩展模板 (v2.1)

在开始部署之前，请查看以下资源。

- 有关模板功能和帐户规划的概述，请参阅使用 Amazon ELB 服务自动扩展 VM 系列防火墙。
- 在启动前自定义防火墙模板（v2.0 和 v2.1）.本主题中的基本参数适用于所有模板版本。
- AWS（v2.0 和 v2.1）的 VM 系列自动扩展模板如何启用动态扩展？

  这些概念适用于所有模板版本。

启动防火墙模板 (v2.1)

您可以选择在同一 VPC 或单独的 VPC 中部署防火墙和应用程序模板。

该模板支持中心辐射型架构，您可以在一个 AWS 帐户中部署防火墙模板，并将其用作中心来保护属于相同或不同 AWS 帐户的应用程序（辐射）。

此工作流程将告诉您如何使用防火墙模板部署外部负载均衡器和 VM 系列防火墙。在启动此模板之前，必须在 Panorama 上配置 vm-auth-key。

©2024 Palo Alto Networks, Inc.

STEP 1 | 在 规划部署 AWS 的 VM 系列自动扩展模板 (v2.1) 和 规划 AWS (v2.0 和 v2.1) 的 VM 系列自动扩展模板 中查看检查清单。

验证已完成以下任务：

- （仅限 PAYG）审核并接受您计划使用的 PAYG 套餐的 EULA。
- （仅适用于 BYOL）获取支持部署可能需要的防火墙数量的套餐的授权代码。您必须将此授权代码保存在名为 `authcodes`（无扩展名）的文本文件中，并把 `authcodes` 文件放在引导数据包的 `/license` 文件夹中。

  如果您使用单个授权代码，而非代码包，防火墙只会检索文件中第一个授权代码的许可证密钥。
- 从 GitHub 存储库下载启动 VM 系列自动扩展模板 v2.1 模板所需的文件。

©2024 Palo Alto Networks, Inc.

STEP 2 | 修改 `init-cfg.txt` 文件并将其上传到 `/config` 文件夹。

由于您使用 Panorama 来引导 VM 系列防火墙，所以您的 `init-cfg.txt` 文件应按如下修改。无需 `bootstrap.xml` 文件。

```
type=dhcp-client
```

```
ip-address=
```

```
default-gateway=
```

```
netmask=
```

```
ipv6-address=
```

```
ipv6-default-gateway=
```

```
hostname=
```

```
vm-auth-key=
```

```
panorama-server=
```

```
panorama-server-2=
```

```
tplname=AWS-tmplspoke1
```

```
dgname=AWS-dgspoke1
```

```
dns-primary=169.254.169.253
```

```
dns-secondary=8.8.8.8
```

```
op-command-modes=mgmt-interface-swap
```

```
dhcp-send-hostname=yes
```


©2024 Palo Alto Networks, Inc.

```
dhcp-send-client-id=yes
```

```
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
```

```
vm-series-auto-registration-id=
```

```
vm-series-auto-registration-pin-value=
```

验证是否存在 **`op-command-modes=mgmt-interface-swap`**。这是在 AWS 上的 VM 系列防火墙上交换管理接口 (mgmt) 和数据面接口 (ethernet 1/1) 的命令。使用 AWS DNS 服务器 IP 地址 169.254.169.253 可以更快地解析加载负载均衡器 DNS 名称。

您必须将设备证书自动注册 PIN 添加到 init-cfg.txt 文件，才能在部署 VM 系列防火墙实例时自动安装设备证书。

STEP 3 | （仅限 BYOL）将许可证授权代码添加到引导软件包的 `/license` 文件夹中。

1. 使用文本编辑器创建名为 **`authcodes`**（无扩展名）的新文本文件。
2. 将 BYOL 许可证的授权代码添加到此文件，然后保存。授权代码必须代表一个代码包，且必须支持部署可能需要的防火墙数量。如果使用单个授权代码，而非代码包，防火墙只会检索文件中第一个授权代码的许可证密钥。

STEP 4 | 上传防火墙模板的 Lambda 代码 (`panw-AWS-ZIP`) 和应用程序模板 (`ilb.zip`) 到 S3 存储桶。您可以使用与引导所使用的相同的 S3 存储桶。

如果应用程序堆栈由与防火墙不同的帐户管理，请使用应用程序帐户在与防火墙模板相同的 AWS 区域中创建另一个 S3 存储桶，并复制 `ilb.zip` 到该 S3 存储桶。

STEP 5 | 选择防火墙模板。

1. 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。
2. 选择 Upload a template to Amazon S3（将模板上传到 Amazon S3），选择应用程序模板，将模板自动的资源部署到与防火墙相同的 VPC 中，或者将资源部署到不同的 VPC 中。单击 Open（打开）和 Next（下一步）。
3. 指定 Stack name（堆栈名称）。堆栈名称允许您唯一标识使用此模板部署的所有资源。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 配置 VPC 的参数。

1. 请务必选择至少两个可用性区域

2. 为 VM 系列防火墙查找并输入 AMI ID。确保 AMI ID 与您选择使用的 AWS 区域、PAN-OS 版本和 BYOL 或 PAYG 许可选项相匹配。
3. 选择 EC2 **Key pair**（密钥对）（从下拉菜单中）启动防火墙。要登录防火墙，您必须提供此密钥对的名称以及与其关联的私钥。
4. 对于 **SSH from field**（**SSH** 发件人字段），防火墙将由 Panorama 管理，并且没有管理界面的 EIP。但是，如果您决定分配 EIP，请配置将连接的 IP 地址范围。
5. 如果您要 **Enable Debug Log**（启用调试日志），请选择 **Yes**（是）。启用调试日志会生成详细列出的日志，以帮助解决部署问题。这些日志是使用堆栈名称生成的，并保存在 AWS CloudWatch 中。

默认情况下，模板使用 CPU 利用率作为 VM 系列防火墙的扩展参数。 自定义 PAN-OS 指标会自动发布到与之前指定的堆栈名称匹配的 CloudWatch 命名空间。

STEP 7 | 指定 Amazon S3 存储桶的名称。

1. 输入包含引导程序包的 S3 存储桶的名称。

   如果引导桶未正确设置，或者输入的存储桶名称不正确，则引导进程将失败，并且您无法登录到防火墙。对负载均衡器的运行状况检查也失败。
2. 输入包含 panw-aws.zip 文件的 S3 存储桶的名称。如前所述，对于 Bootstrap 和 Lambda 代码，您可以使用一个 S3 存储桶。

STEP 8 | 指定启用 API 访问防火墙和 Panorama 的密钥。

1. 输入防火墙必须用来验证 API 调用的密钥。默认密钥基于示例示例文件，您只能将其用于测试和评估。对于生产部署，您必须为 API 调用创建单独的 PAN-OS 登录并生成关联的密钥。
2. 请输入 API 密钥以允许 AWS Lambda 对 Panorama 进行 API 调用。对于生产部署，您应该为 API 调用创建一个单独的登录并生成关联的密钥。

STEP 9 | 输入应用程序负载均衡器的名称。

©2024 Palo Alto Networks, Inc.

STEP 10 | 查看模板设置并启动模板。

1. 选择 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我承认此模板可能会导致 **AWS CloudFormation** 创建 **IAM** 资源）。
2. 单击 **Create**（创建）以启动模板。显示 CREATE_IN_PROGRESS 事件。
3. 成功部署时，状态会更新到 CREATE_COMPLETE。

STEP 11 | 验证模板是否启动了所有必需的资源。

1. 在 EC2 仪表盘上，选择 Auto Scaling Groups（自动扩展组）。验证在每个 AZ 中，VM 系列防火墙有一个 ASG。ASG 名称前缀包含堆栈名称。
2. 在 AWS 管理控制台上，选择堆栈名称以查看资源列表的 Output（输出）。
3. 输出应类似于下图中的输出。
   - 记下网络负载均衡器队列名称。
   - 记下弹性负载均衡器公共 DNS 名称。

防火墙启动并可用于处理流量可能需要长达 *20* 分钟的时间。

完成测试或生产部署时，确保停止收费的唯一方法是彻底删除堆栈。关闭实例或将 *ASG* 最大值更改为 *0* 还不够。

STEP 12 | 保存以下防火墙模板信息。部署应用程序模板时，您需要提供这些值作为输入。

- 每个 **AZ** 中 **NAT** 网关的 **IP** 地址 — 您需要此 IP 地址来限制对 Panorama 的 HTTPS 访问，以便可以使用 NAT 网关的 EIP 的 Lambda 在需要时与 Panorama 通信。
- 网络负载均衡器 **SQS URL** — 防火墙堆栈中的 Lambda 函数监控此队列，以便它可以了解您部署的任何网络负载均衡器，并在 Panorama 中创建 NAT 策略规则（每个应用程序一个），从而使防火墙可以将流量发送到网络负载均衡器 IP 地址。

启动应用程序模板 (v2.1)

应用程序模板允许您完成三明治拓扑结构，并提供应用程序目标以便您可以评估自动扩展解决方案。此应用程序模板在使用防火墙模板部署的 VM 系列防火墙自动扩展组后面部署应用程序或网络负载均衡器和一对 Web 服务器。

使用此模板评估解决方案，但自定义自己的模板以部署到生产中。对于自定义模板，请确保启用应用程序模板与防火墙模板之间的 SQS 消息传递。

在启动应用程序模板时，您必须根据是将应用程序模板部署在部署防火墙模板的相同 VPC 中还是部署在单独的 VPC 中，从而选择模板。请参阅为 ELB 服务启用流量（v2.0 和 v2.1）。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建一个从中启动应用程序模板的 S3 存储桶。

- 如果是跨帐户部署，请创建新存储桶。
- 如果有一个帐户，则可以创建新的存储桶或使用之前创建的 S3 存储桶（您可以为所有部署使用一个存储桶）。

STEP 2 | 将 ilb.zip 文件上传到 S3 存储桶。

STEP 3 | 选择要启动的应用程序启动模板。

1. 在 AWS 管理控制台上，选择 **CloudFormation** > **CreateStack**（创建堆栈）。
2. 选择 Upload a template to Amazon S3（将模板上传到 Amazon S3），选择应用程序模板，将模板自动的资源部署到与防火墙相同的 VPC 中，或者将资源部署到不同的 VPC 中。单击 **Open**（打开）和 **Next**（下一步）。
3. 指定 Stack name（堆栈名称）。堆栈名称允许您唯一标识使用此模板部署的所有资源。

STEP 4 | 配置 VPC 和网络负载均衡器的参数。

1. 选择两个可用性区域，您的设置将跨越 Select list of AZ（选择 AZ 列表）。如果您在同一个 VPC 内部署，请确保选择与防火墙模板相同的可用性区域。
2. 如果部署到新 VPC，请输入 VPC 的 CIDR 块。默认 CIDR 为 192.168.0.0/16。
3. 如果部署到同一 VPC，您将选择以前的 VPC 并使用 Trust 子网。

STEP 5 | 选择负载均衡器类型。

STEP 6 | 配置 Lambda 的参数。

1. 输入存储 ilb.zip 的 S3 存储桶名称。
2. 输入 zip 文件名。
3. 粘贴您之前复制的 SQS URL。

STEP 7 | 修改 Web 服务器 EC2 实例类型以满足需求。

STEP 8 | 选择启动 Web 服务器的 EC2 密钥对（从下拉菜单中）。要登录到 Web 服务器，您必须提供密钥对名称和与其关联的私钥。

STEP 9 | 对于仅管理访问，选择要访问服务器的网络的 IP 地址。Web 流量来自启动防火墙模板时复制的 ELBDNS 名称。

STEP 10 | 查看模板设置并启动模板。

©2024 Palo Alto Networks, Inc.

STEP 11 | 完成应用程序模板后，最多可能需要 20 分钟才能生效。

1. 验证应用程序模板负载均衡器是否标记为活动。
2. 验证 Panorama 在设备组中是否具有 NAT 对象。
3. 验证 Panorama 在设备组中是否有地址对象。
4. 验证 Panorama 在模板堆栈中是否有静态路由。

STEP 12 | 获得应用程序负载均衡器的 DNS 名称并将其输入 Web 浏览器。

STEP 13 | 成功启动后，浏览器输出应如以下所示。

创建自定义 Amazon 机器映像 (v2.1)

自定义 VM 系列 AMI 提供了一致性和灵活性，可以让您使用自己希望在网络上使用的 PAN-OS 版本部署 VM 系列防火墙，而不是仅限于使用发布到公共 AWS Marketplace 或 AWS GovCloud Marketplace 的 AMI。使用自定义 AMI 可加快使用您选择的 PAN-OS 版本部署防火墙的过程，因为它可以减少使用在 AWS 公共或 AWS GovCloud Marketplace 上发布的 AMI 配置防火墙的时间，然后执行软件升级来获得您想要在您的网络上使用的 PAN-OS 版本。此外，您可以在自动扩展 VM 系列防火墙 CloudFormation 模板或已创建的任何其他模板中使用自定义 AMI。

您可以使用 BYOL、套餐 1 或套餐 2 许可证创建自定义 AMI。创建自定义 AMI 的过程要求从防火墙中删除所有配置，并执行私有数据重置，因此，在此工作流程中，您将从 AWS Marketplace 启动新的防火墙实例，而不是使用您完全配置的现有防火墙。

在使用防火墙的 *BYOL* 版本创建自定义 *AMI* 时，必须先在防火墙上激活许可证，以便可以访问和下载 *PAN-OS* 内容和软件更新来升级防火墙，然后在将执行私有数据重置和创建自定义 *AMI* 之前停用防火墙上的许可证。如果未取消激活许可证，则会丢失在此防火墙实例上应用的许可证。

STEP 1 | 从 Marketplace 启动 VM 系列防火墙。

参阅 Launch the VM-Series firewall（启动 VM 系列防火墙）。

STEP 2 | （仅限 BYOL）激活许可证。

STEP 3 | 在防火墙上安装最新内容。

STEP 4 | （仅限 BYOL）停用许可证。

©2024 Palo Alto Networks, Inc.

STEP 5 | 执行私有数据重置。

重置私有数据会删除所有日志并恢复默认配置。

不会擦除系统盘，因此，步骤 4 中的内容更新是完整的。

1. 访问防火墙 CLI。
2. 导出配置的副本。
3. 删除所有日志并恢复默认配置。

```
request system private-data-reset
```

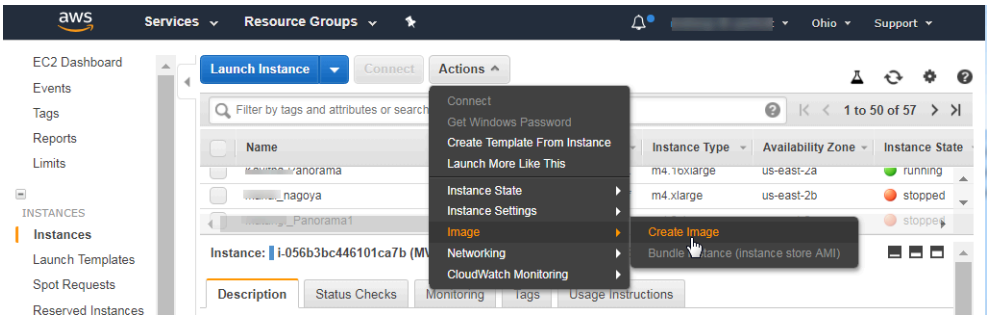
输入 **y** 以确认。

防火墙重新启动以初始化默认配置。

©2024 Palo Alto Networks, Inc.

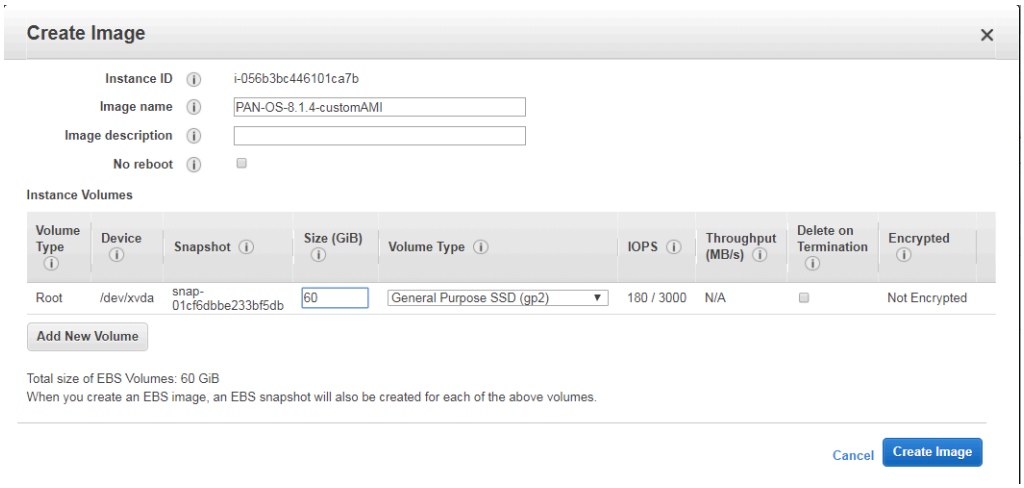
STEP 6 | 创建自定义 AMI。

1. 登录到 AWS 控制台，然后选择 EC2 仪表盘。
2. **Stop**（停止）VM 系列防火墙。
3. 选择 VM 系列防火墙实例，然后单击 **Image**（映像） > **Create Image**（创建映像）。



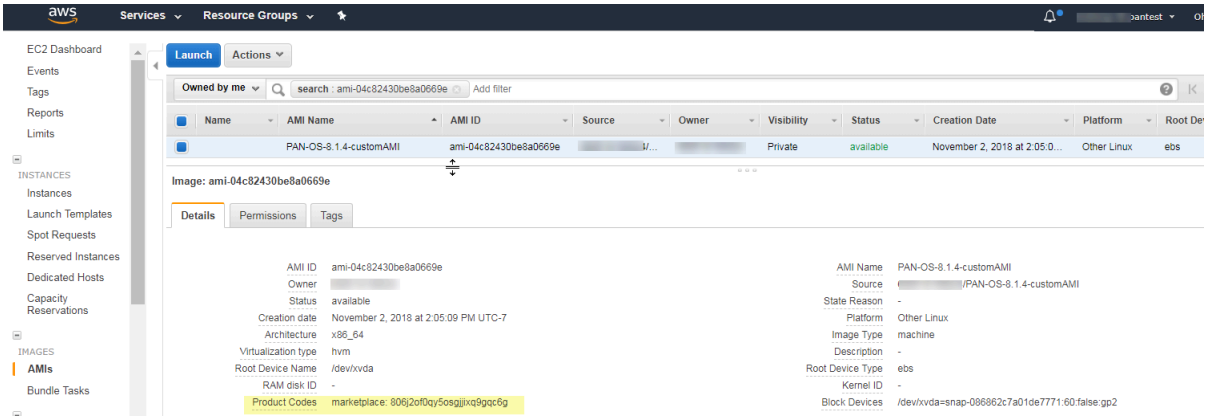
4. 输入自定义映像名称，然后单击 **Create Image**（创建映像）。

   最低要求 60GB 的磁盘空间。



5. 验证是否已创建自定义 AMI 且具有正确的产品代码。
   1. 在 EC2 仪表盘上，选择 **AMI**。
   2. 选择刚才创建的 AMI。根据选择的是具有 BYOL、套餐 1 或套餐 2 许可证选项的 AMI，您可以在详细信息中看到以下产品代码之一：
      - BYOL — 6njl1pau431dv1qxipg63mvah
      - 套餐 1 — 6kxdw3bbmdeda3o6i1ggqt4km
      - 套餐 2 — 806j2of0qy5osgjjixq9gqc6g

©2024 Palo Alto Networks, Inc.



STEP 7 | 在 AWS上 加密 VM 系列防火墙的 EBS 卷.

如果您计划将具有 EBS 加密的自定义 AMI 来进行使用 Amazon ELB 服务自动扩展 VM 系列防火墙部署，则必须使用 AWS 帐户的默认主密钥。

VM 系列自动扩展模板清理 (v2.1)

如果将模板部署为测试，请将其删除以节省资源和降低成本。

STEP 1 | 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。

STEP 2 | 找到先前启动的防火墙模板和应用程序模板，然后删除这两个模板。

有关删除模板堆栈的详细信息，请参阅“什么是 AWS CloudFormation？”

不删除模板堆栈会导致 *AWS* 收费。

应用程序模板和防火墙模板之间的 SQS 消息传递 (v2.1)

使用防火墙模板之一部署的 VM 系列防火墙可以检测流量并将流量发送到您希望自动分发传入流量的负载均衡器。为此，防火墙模板包含一个 Lambda 函数，用于监控消息的简单队列服务。该消息允许 Lambda 函数了解新的网络负载均衡器，然后在防火墙上自动创建 NAT 策略规则，以将流量发送到负载均衡器的 IP 地址。为了在 AWS 基础架构内正确路由流量，该消息还必须包括 DNS、VPC ID 和负载均衡器所属的 AZ 的基本信息。

如果您正在构建自己的应用程序模板，则必须设置应用程序模板以将 ADD 和 DEL 消息发布到 SQS URL。防火墙模板使用 SQS URL 来了解它在环境中必须将流量分发到的负载均衡器：

- ADD-NLB 消息，用于在新的网络负载均衡器可用时通知防火墙。
- DEL-NLB 消息，用于在网络负载均衡器终止并不再可用时通知防火墙。
- 当新的网络负载均衡器可用时通知防火墙的 ADD-ALB 消息。
- 当网络负载均衡器终止且不再可用时通知防火墙的 DEL-ALB 消息。

每种消息类型的以下示例均包括示例值。您需要使用符合部署的值来修改这些消息。

ADD-NLB 消息

©2024 Palo Alto Networks, Inc.

```
msg_add_nlb= {
       "MSG-TYPE":"ADD-NLB",
       "AVAIL-ZONES": [
       {
           "NLB-IP":"192.168.2.101",
           "ZONE-NAME":"us-east-2a",
           "SUBNET-ID": "subnet-2a566243"
       },
       {
           "NLB-IP":"192.168.12.101",
           "ZONE-NAME":"us-east-2b",
           "SUBNET-ID": "subnet-2a566243 "
       }
       ],
            "DNS-NAME": "publicelb1-2119989486.us-
east-2.elb.amazonaws.com",
           "VPC-ID": "vpc-42ba9f2b",
           "NLB-NAME": "publicelb1"
}
```


©2024 Palo Alto Networks, Inc.

DEL-NLB 消息

```
msg_del_nlb= {
 "MSG-TYPE":"DEL-NLB",
 "DNS-NAME": "publicelb1-2119989486.us-east-2.elb.amazonaws.com",
}
```

ADD-ALB

```
{ "AVAIL-ZONES": [
       {
           "SUBNET-CIDR":"172.32.0.0/24",
           "SUBNET-ID": "subnet-0953a3a8e2a8208a9",
           "ZONE-NAME": "us-east-2a"
       },
       {
           "SUBNET-CIDR":"172.32.2.0/24",
           "SUBNET-ID": "subnet-0a9602e4fb0d88baa",
           "ZONE-NAME": "us-east-2c"
       },
       {
           "SUBNET-CIDR":"172.32.1.0/24",
```

 ©2024 Palo Alto Networks, Inc.

```
            "SUBNET-ID": "subnet-0b31ed16f308b3c4d",

            "ZONE-NAME": "us-east-2b"

        }

    ],

    "VPC-PEERCONN-ID": "pcx-0538bb05dbe2e1b8e",

    "VPC-CIDR":"172.32.0.0/16",

    "ALB-NAME": "appILB-908-0",

    "ALB-ARN":"arn:aws:elasticloadbalancing:us-
east-2:018147215560:loadbalancer/app/appILB-908-0/1997ed20eeb5bcef",

    "VPC-ID": "vpc-0d9234597da6d9147",

    "MSG-TYPE":"ADD-ALB",

    "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"

}
```

DEL-ALB 消息

```
{

    "MSG-TYPE":"DEL-ALB",

    "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"

}
```

有关如何将消息发送到 Amazon SQS 队列的详细信息，请参阅 AWS 文档。

©2024 Palo Alto Networks, Inc.

AWS 更新与 VM 系列自动扩展模板 (v2.1)

通过堆栈更新，您可以修改 VM 系列自动扩展模板防火墙模板部署的资源。不要删除现有的部署并重新部署解决方案，而是使用堆栈更新来修改启动配置参数。

您可以修改 AWS 实例类型、自动扩展组的密钥对以及与防火墙上的管理员用户帐户关联的 API 密钥。

无需更新堆栈即可修改默认通知或创建自动扩展警报。请参阅 更改扩展参数和 CloudWatch 指标 (v2.1)。

部署 VM 系列自动扩展模板时，系统会自动创建自动扩展组和启动配置。启动配置是自动扩展组用于启动 EC2 实例的模板，它指定了实例类型，自动扩展组的密钥对或与防火墙上的管理用户帐户关联的 API 密钥等参数。

对于关键应用程序，请在维护时段内执行堆栈更新。

您可以直接更新堆栈或创建更改集。本文档中的工作流程将引导您完成手动堆栈更新。

STEP 1 | 在 AWS CloudFormation 控制台中，选择您要更新并选择的父堆栈 **Actions**（操作） > **Update Stack**（更新堆栈）。

STEP 2 | 修改您想要更新的资源。

您可以修改堆栈资源的实例类型、安全组、密钥对或与防火墙上的管理用户帐户关联的 API 密钥。

如果您创建新的管理用户帐户或修改防火墙上现有管理员的凭据，为了更新该堆栈并使用更新的 API 密钥部署新防火墙，您需要按照修改管理帐户 (v2.1) 中的工作流程操作。

STEP 3 | 确认通知并查看更改并单击 **Update**（更新）启动堆栈更新。

修改管理帐户 (v2.1)

如果您已经部署了该模板，并且现在要更改管理帐户的密码或在 VM 系列防火墙上创建新的管理用户帐户，则必须生成新的 API 密钥并使用新的 API 密钥更新模板堆栈管理用户帐户。

STEP 1 | 登录到防火墙的 Web 界面并更改现有管理用户的凭证或创建新帐户。

STEP 2 | 生成 API 密钥。

STEP 3 | 更新堆栈中的 API 密钥以确保新启动的防火墙拥有更新后的管理员帐户。

请参阅 AWS 的堆栈更新与 VM 系列自动扩展模板 (v2.0)。

©2024 Palo Alto Networks, Inc.

更改扩展参数和 CloudWatch 指标 (v2.1)

此任务描述如何使用自定义 PAN-OS 指标作为扩展参数来触发自动扩展操作。

当您启动防火墙模板时，模板创建一个名称空间，其中包含可用于定义自动扩展操作的扩展和扩展策略。策略名称包括命名空间，如下所示：

- <Custom Namespace>-scalein - Remove 1 instance
- <Custom Namespace>-scaleout - Add 1 instance

每个 PAN-OS 指标都有一个默认通知，您可以删除并替换为自动扩展操作。对于每个度量标准，请创建两个操作：一个用于确定何时添加 VM 系列防火墙，另一个用于确定何时删除 VM 系列防火墙。

STEP 1 | 在 AWS 中，选择 **Services**（服务） > **CloudWatch** > **Metrics**（指标）。

STEP 2 | 选择一个 **Custom Namespace**（自定义命名空间）链接，并选择指标链接以查看 自定义 PAN-OS 指标。

STEP 3 | 选中一个框以选择指标，然后选择 **Graphed metrics**（图表指标）标签。

1. 在 **Statistics**（统计信息）列中，选择统计条件（例如平均值，最小值和最大值）并选择时间段。
2. 在 **Actions**（操作）列中，选择铃声（创建闹钟）。

STEP 4 | 定义一个警报，在 CPU 利用率达到或低于您设置的标准时，在您设置的时间范围内删除防火墙。

1. 选择 **Edit**（编辑）以更改图表标题。
2. 在 **Alarm details**（警报详细信息）下，填写 **Name**（名称）和 **Description**（说明），选择一个运算符，并设置最小值以维护当前实例。如果未维护最小值，则删除实例。
3. 在 **Actions**（操作）下，**Delete**（删除）默认通知。
4. 选择 **+AutoScaling Action**（+自动扩展操作）。
   - 使用 **From the**（来自）列表以选择命名空间。
   - 从 **Take this action**（执行此操作），选择要删除实例的策略。
5. 选择 **Create Alarm**（创建警报）。

STEP 5 | 创建第二个警报，在 CPU 利用率达到或超过您设置的标准时添加防火墙。

STEP 6 | 要查看警报，请选择 **Services**（服务） > **CloudWatch** > **Alarms**（警报）。

要从此窗口编辑警报，请选中警报旁边的框并选择 **Action**（操作） > **Edit**（编辑）。

©2024 Palo Alto Networks, Inc.

在 AWS VPC 上监控的属性列表

在 AWS VPC 中配置或修改虚拟机时，有两种方法可以监控这些实例，并检索用作动态地址组内匹配条件的标记。

- **VM** 信息源 — 在下一代防火墙上，您最多可以监控共计 32 个标记，包括 14 个预定义和 18 个用户定义的表项值对（标记）。
- **Panorama** 上的 **AWS** 插件 — AWS 的 Panorama 插件允许您将 Panorama 连接到公共云上的 AWS APC，并检索虚拟机的“IP 地址到标记”映射。然后，Panorama 将 VM 信息注册到您配置用于通知的 Palo Alto Networks® 托管防火墙。使用插件后，Panorama 最多可为每个虚拟机检索共计 32 个标记，包括 11 个预定义标记和最多 21 个用户定义的标记。



标记值（包括名称和值）的最大长度必须为 *116* 个字符或更少。如果标记的长度超过 *116* 个字符，则 *Panorama* 无法检索标记，并将其注册到防火墙上。

AWS-VPC 所监控的属性		防火墙上的 **VM** 信息源	**Panorama** 上的 **AWS** 插件
AMI ID	ImageId.<ImageId string>	是	是
架构	Architecture.<Architecture string>	是	否
可用性区域	AvailabilityZone.<string>	是	是
来宾操作系统	GuestOS.<guest OS name>	是	否
IAM 实例配置文件	Iam-instance-profile.<instanceProfileArn>	否	是
实例 ID	InstanceId.<InstanceId string>	是	否
实例状态	InstanceState.<instance state>	是	否
实例类型	InstanceType.<instance type>	是	否
密钥名称	KeyName.<KeyName string>	是	是
所有者 ID 此属性的值从 ENI 获取。	Account-number.<OwnerId>	否	是
位置 租户、组名称	Placement.Tenancy.<string> Placement.GroupName.<string>	是	是

©2024 Palo Alto Networks, Inc.

AWS-VPC 所监控的属性		防火墙上的 VM 信息源	Panorama 上的 AWS 插件
私有 DNS 名称	PrivateDnsName.<Private DNS Name>	是	否
公共 DNS 名称	PublicDnsName.<Public DNS Name>	是	是
子网 ID	SubnetID.<subnetID string>	是	是
安全组 ID	Sg-id.<sg-xxxx>	否	是
安全组名称	Sg-name.<SecurityGroupName>	否	是
VPC ID	VpcId.<VpcId string>	是	是
标记（键，值）	aws-tag.<key>.<value>	是； 最多支持 18 个用户定义的标记。用户定义的标记按字母顺序排序，且前 18 个标记可用于防火墙。	是； 最多支持 21 个用户定义的标记。用户定义的标记按字母顺序排序，且前 21 个标记可用于 Panorama 和防火墙。

监控 AWS VPC 所需的 IAM 权限

为了启用 VM 监控，绑定至 AWS 访问密钥和机密访问密钥的用户 的 AWS 登录凭证必须具备以上所列属性的权限。这些权限可使防火墙发起 API 调用，以监控 AWS VPC 中的虚拟机。

与用户相关联的 IAM 策略必须具备全球只读访问权限（如 AmazonEC2ReadOnlyAccess），或必须包含对所有受监控属性的独立权限。以下 IAM 策略示例列出了启动 API 操作对 AWS VPC 中的资源进行监控所需的权限：

```
{ “Version”:“2012-10-17", “Statement”:
 [ { “Sid”:“VisualEditor0”, “Effect”:“Allow”, “Action”:
 [ “elasticloadbalancing:DescribeLoadBalancerAttributes”, “elasticloadbalanci
 ], “Resource”: “*” } ] }
```


©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 KVM 上设置 VM 系列防火墙

基于内核的虚拟机 (KVM) 是一个用于运行 Linux 分布的服务器的开源虚拟化模块。可以在运行 KVM 虚拟机监控程序的 Linux 服务器上部署 VM 系列防火墙。

本指南假设您拥有使用 Linux 的现有 IT 基础架构，且拥有使用 Linux/Linux 工具的基础知识。相关说明仅适用于在 KVM 上部署 VM 系列防火墙。

- KVM 上的 VM 系列防火墙—要求和先决条件
- 在 KVM 上支持的部署
- 在 KVM 上安装 VM 系列防火墙
- KVM 的 VM 系列性能调整
- 智能流量分流

KVM 上的 VM 系列防火墙—要求和先决条件

- 用于在网络上连接 VM 系列防火墙的选项
- KVM 上 VM 系列防火墙的先决条件

表 **5: KVM** 系统上 **VM** 系列的要求

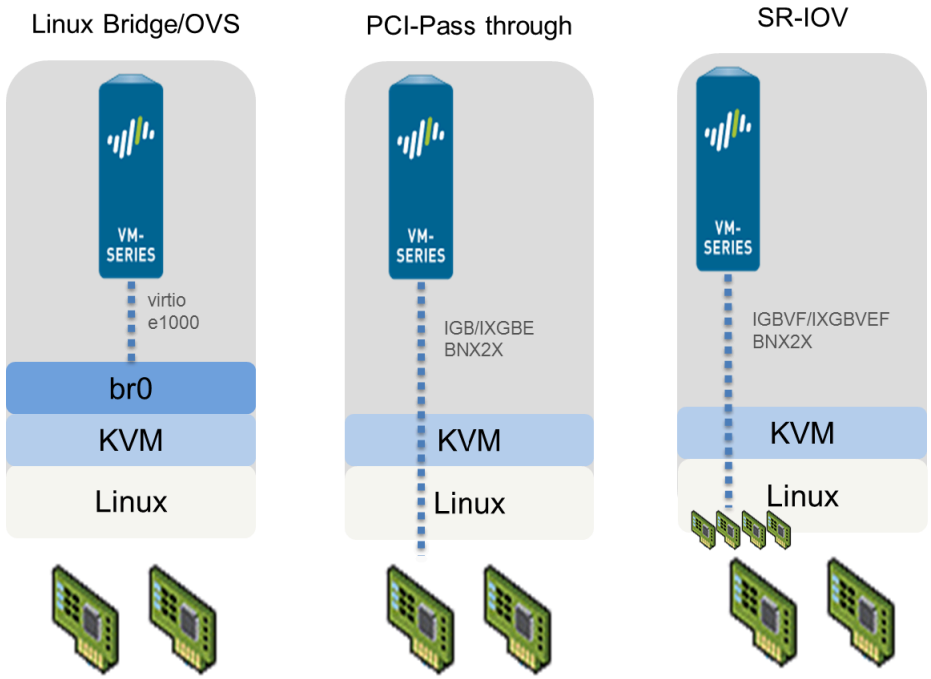
要求	说明
硬件资源	有关 VM 系列型号的最低硬件要求，请参阅 VM 系列系统要求。
软件版本	请参阅兼容性矩阵中支持的 KVM 软件版本。
SR-IOV 驱动程序	请参阅兼容性矩阵中的 PacketMMAP 驱动程序版本。
DPDK 驱动程序	请参阅兼容性列表中的 DPDK 驱动程序版本。 如果您在 KVM 上使用 VM 系列上支持的 NIC 驱动程序之一，则默认启用 DPDK。
网络接口 — 网络接口卡和软件网桥	KVM 上的 VM 系列防火墙最多支持 25 个接口 — 1 个管理接口和最多 24 个用于数据流量的网络接口。 在 KVM 上部署的 VM 系列防火墙支持基于软件的虚拟交换机（如 Linux 网桥或 Open vSwitch 网桥），并且可直接连接到 PCI passthrough 或 SR-IOV 功能适配器。 如果计划使用 PCI-passthrough 或 SR-IOV 建立连接，则不能在用于 SR-IOV 或 PCI-passthrough 的物理端口上配置 vSwitch。要与网络上的主机以及其他虚拟机进行通信，VM 系列防火墙必须能够独占访问此接口上的物理端口和关联的虚拟功能 (VF)。 • 在 Linux 网桥和 OVS 上，支持 e1000 和 Virtio 驱动程序；不支持默认驱动程序 rtl8139。

©2024 Palo Alto Networks, Inc.

要求	说明

	• 对于 PCI passthrough/SR-IOV 支持，已经为下列网卡测试 VM 系列防火墙：
	  • 基于 Intel 82576 的 1G NIC：在所有支持的 Linux 分布上都支持 SR-IOV；支持 PCI-passthrough。
	  • 基于 Intel 82599 的 10G NIC：在所有支持的 Linux 分布上都支持 SR-IOV；支持 PCI-passthrough。
	  • Intel X710 10G NIC：在所有支持的 Linux 分布上都支持 SR-IOV；支持 PCI-passthrough
	  • Intel X722 10G NIC：在所有支持的 Linux 分布上都支持 SR-IOV；支持 PCI-passthrough
	  • 基于 Broadcom 57112 和 578xx 的 10G NIC：在所有支持的 Linux 分布上都支持 SR-IOV；不支持 PCI-passthrough。
	  • Mellanox ConnectX5 10G/25G/50G/100G NIC：在所有支持的 Linux 分布上都支持 SR-IOV。
	  • 请参阅兼容性矩阵中的 PacketMMAP 驱动程序版本。
	
	必须配置分配给 *VM* 系列防火墙的 *SR-IOV* 功能接口作为第 *3* 层接口或高可用性接口。

用于在网络上连接 VM 系列防火墙的选项



 ©2024 Palo Alto Networks, Inc.

- 使用 Linux 网桥或 OVS，数据流量可使用软件网桥连接到同一主机上的来宾。对于外部连接，数据流量使用已连接到网桥的物理接口。
- 使用 PCI passthrough，数据流量在来宾与已连接到来宾的物理接口之间直接传递。将接口连接到来宾后，该接口不可用于主机或主机上的其他来宾。
- 使用 SR-IOV，数据流量在来宾与已连接到来宾的虚拟功能之间直接传递。

KVM 上 VM 系列防火墙的先决条件

在 Linux 服务器上安装 VM 系列防火墙之前，请仔细阅读以下各节：

- 准备 Linux 服务器
- 准备部署 VM 系列防火墙

准备 Linux 服务器

在 KVM 上安装 VM 系列防火墙之前，请确认您已安装能够正常运行的 Linux 环境，并且网络基础架构支持选定部署所需的连接。

- 验证 Linux 支持
- 验证网络基础架构
- 安装 Mellanox 软件工具
- 在适用于 KVM 的 VM 系列防火墙上为 Mellanox CX5 NIC 启用虚拟功能
- 验证主机配置

验证 Linux 支持

确认您拥有支持安装的正确环境。

- ☐ 检查 Linux 分布版本。有关支持的版本列表，请参阅兼容性矩阵中的适用于 KVM 的 VM 系列。
- ☐ 确认您已安装并配置创建和管理虚拟机所需的 KVM 工具和软件包，如 Libvirt。
- ☐ 如果您要使用 SCSI 磁盘控制器访问 VM 系列防火墙用来存储数据的磁盘，必须使用 virsh 将 virtio-scsi 控制器连接到 VM 系列防火墙。然后，您可以编辑 VM 系列防火墙的 XML 模板以使用 virtio-scsi 控制器。有关说明，请参阅启用使用 SCSI 控制器。

  Ubuntu 12.04 上的 *KVM* 不支持 *virtio-scsi* 控制器。

验证网络基础架构

确认您已设置用于控制来宾与 VM 系列防火墙之间流量以及用于连接到外部服务器或 Internet 的网络基础架构。可以使用 Linux 网桥、Open vSwitch、PCI passthrough 或 SR-IOV 功能网卡连接 VM 系列防火墙。

- ☐ 确保您计划使用的每个接口的链路状态均正常，有时必须手动使接口状态变成正常。

©2024 Palo Alto Networks, Inc.

- 如果使用 Linux 网桥或 OVS，确认您已设置将流量发送到防火墙/接收来自防火墙的流量所需的网桥。如果未设置，创建网桥并在开始安装防火墙之前确认网桥能够正常使用。
- 如果使用 SR-IOV 或 PCI-passthrough，确认所有接口的 PCI ID。要查看列表，使用以下命令：

  Virsh nodedev-list –tree

  请参阅验证 VM 系列防火墙上网络接口排序的 PCI-ID。
- 如果使用 SR-IOV 或 PCI-passthrough，确认已在 BIOS 中启用虚拟化扩展 (VT-d/IOMMU)。例如，要启用 IOMMU，必须在 `/etc/grub.conf` 中定义 `intel_iommu=on`。有关说明，请参阅系统供应商提供的文档。
- 如果使用 PCI-passthrough，确保 VM 系列防火墙对计划要连接的接口具有唯一的访问权限。

  要允许独占访问，您必须从 Linux 服务器手动分离接口。

  Virsh nodedev-detach *<pci id of interface>*

  例如：

  Virsh nodedev-detach pci_0000_07_10_0

  在某些情况下，您可能需要编辑 `/etc/libvirt/qemu.conf` 并取消对 `relaxed_acs_check = 1` 的注释。
- 如果使用 SR-IOV，确认已为计划在网卡上使用的每个端口启用虚拟功能。使用 SR-IOV，可以将一个 Ethernet 端口（物理功能）细分成多个虚拟功能。可以将来宾映射到一个或多个虚拟功能。

  按如下所示启用虚拟功能：

  1. 在此位置创建一个新文件：`/etc/modprobe.d/`
  2. 使用 vi 编辑文件以使功能更持久：

     vim /etc/modprobe.d/igb.conf
  3. 启用所需的虚拟功能数量：

     options igb max_vfs=4

     保存更改和重新启动 Linux 服务器后，上例中的每个接口（或物理功能）都将拥有 4 个虚拟功能。

  有关支持的实际虚拟功能数的详细信息和启用虚拟功能的说明，请参阅网络供应商提供的文档。

安装 **Mellanox** 软件工具

如果使用 Mellanox CX5 卡，请在主机上安装 Mellanox 软件工具。在安装之前，确认 Linux 支持和网络基础架构。

STEP 1 | 在主机上，从以下链接下载适用于操作系统版本的 Mellanox OpenFabric Enterprise Distribution for Linux (MLNX_OFED) 的软件包：

https://www.mellanox.com/products/infiniband-drivers/linux/mlnx_ofed

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 运行安装命令：

```
mlnxofedinstall
```

如果您已安装所有必备软件包，则上述命令将安装所有 MLNX_OFED 软件包。继续执行步骤 3。

如果您的环境没有安装所需的软件包，则安装程序会列出必须安装的所有软件包。安装软件包后，重新运行安装命令，然后继续执行步骤 3。

STEP 3 | 重新启动主机。

STEP 4 | 检查 Mellanox 软件工具的状态。

```
# mst status MST modules:
 ------------------------------------------------------------------
   MST PCI module is not loaded   MST PCI
 configuration module loaded MST devices:
 ------------------------------------------------------------------ /
dev/mst/mt4121_pciconf0     - PCI configuration cycles access.
         domain:bus:dev.fn=0000:3b:00.0 addr.reg=88 data.reg=92
         Chip revision is:00
```

STEP 5 | 确保 PCI 列表中已更新 Mellanox：

```
# lspci | grep Mellanox 3b:00.0 Ethernet controller:Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex] 3b:00.1 Ethernet
 controller:Mellanox Technologies MT28800 Family [ConnectX-5 Ex]
```

在适用于 KVM 的 VM 系列防火墙上为 Mellanox CX5 NIC 启用虚拟功能

在 Mellanox Cx5 NIC 上启用虚拟功能之前，请安装 Mellanox 软件工具。

STEP 1 | 确保已启动 Mellanox 软件工具 (mst)。

©2024 Palo Alto Networks, Inc.

STEP 2 | 启用所需的虚拟功能数量。例如：

```
mlxconfig -d /dev/mst/mt4121_pciconf0 set SRIOV_EN=1 NUM_OF_VFS=4
```

保存更改和重新启动 Linux 服务器后，上例中的每个接口（或物理功能）都将拥有 4 个虚拟功能。有关支持的实际虚拟功能数的详细信息和启用虚拟功能的说明，请参阅网络供应商提供的文档。

首次在 *Mellanox Cx5 NIC* 上启用虚拟功能时，系统可能会显示以下错误消息：

```
[ 1429.841162] mlx5_core 0000:3b:00.1:
 mlx5_port_module_event:1025:(pid 0):Port module
 event[error]: module 1, Cable error, One or more network
 ports have been powered down due to insufficient/
unadvertised power on the PCIe slot.请参阅该卡片的用户手册，以了解电源规格或联系 Mellanox 支持团队
```

要解决该问题，请在 *Linux* 服务器上输入以下命令序列：

```
# mlxconfig -d <dev> set ADVANCED_POWER_SETTINGS=1 #
 mlxconfig -d <dev> set DISABLE_SLOT_POWER_LIMITER=1 #
 reboot
```

STEP 3 | 检查虚拟功能的状态。

```
# cat /sys/class/net/enp59s0f1/device/sriov_numvfs
```

（可选）如果虚拟功能设置不正确（状态为 0 或为空），请运行以下命令：

```
# echo 4 > /sys/class/net/enp59s0f1/device/sriov_numvfs
```

STEP 4 | 列出 PCI 设备以准确匹配 Mellanox 的各个物理功能所加载的虚拟功能数：

```
# lspci | grep Mellanox 3b:00.0 Ethernet controller:Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex] 3b:00.1 Ethernet
 controller:Mellanox Technologies MT28800 Family [ConnectX-5
 Ex] 3b:00.2 Ethernet controller:Mellanox Technologies MT28800
 Family [ConnectX-5 Ex Virtual Function] 3b:00.3 Ethernet
 controller:Mellanox Technologies MT28800 Family [ConnectX-5
 Ex Virtual Function] 3b:00.4 Ethernet controller:Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex Virtual Function]
 3b:00.5 Ethernet controller:Mellanox Technologies MT28800
 Family [ConnectX-5 Ex Virtual Function] 3b:00.6 Ethernet
 controller:Mellanox Technologies MT28800 Family [ConnectX-5
 Ex Virtual Function] 3b:00.7 Ethernet controller:Mellanox
 Technologies MT28800 Family [ConnectX-5 Ex Virtual Function]
```

 ©2024 Palo Alto Networks, Inc.

```
3b:01.0 Ethernet controller:Mellanox Technologies MT28800
Family [ConnectX-5 Ex Virtual Function] 3b:01.1 Ethernet
controller:Mellanox Technologies MT28800 Family [ConnectX-5 Ex
Virtual Function]
```

验证主机配置

配置主机以获得最大的 VM 系列性能。有关配置下面每个选项的信息，请参阅适用于 KVM 的 VM 系列性能调整。

- 启用 **DPDK**。DPDK 允许主机绕过 Linux 内核来更快地处理数据包。相反，使用驱动程序和 DPDK 库执行与 NIC 的交互。在 VM 系列防火墙中使用 DPDK 需要 Open vSwitch。
- 启用 **SR-IOV**。单根 I/O 虚拟化 (SR-IOV) 允许单个根端口下的单个 PCIe 物理设备看起来像是虚拟机监控程序或来宾的多个单独的物理设备。
- 启用 **NIC** 的多队列支持。多队列 virtio-net 允许网络性能随 vCPU 的数量扩展，并通过创建多个 TX 和 RX 队列来支持并行数据包处理。
- 隔离 **NUMA** 节点中的 **CPU** 资源。通过将来宾虚拟机的 CPU 资源隔离到单个非统一内存访问 (NUMA) 节点，您可以提高 KVM 上 VM 系列的性能。

准备部署 VM 系列防火墙

- 购买 VM 系列防火墙型号，并在 Palo Alto Networks 客户支持网站上注册授权代码。请参阅创建支持帐户和注册 VM 系列防火墙。
- 获取 qcow2 映像并将其保存 Linux 服务器上。作为最佳实践，应将映像复制到以下文件夹： /var/lib/libvirt/qemu/images.

  如果计划部署 VM 系列防火墙的多个实例，应准备所需的映像副本数。由于 VM 系列防火墙的每个实例都保持与用于部署防火墙的 .qcow2 映像的链接，因此为防止出现任何数据损坏问题，必须确保每个映像都是独立的且由防火墙的一个实例使用。

©2024 Palo Alto Networks, Inc.

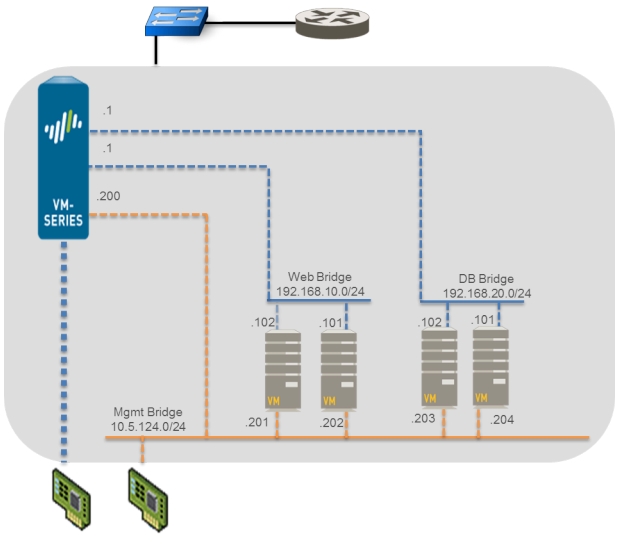
在 KVM 上支持的部署

您可以在一个 Linux 主机（单租户）上部署 VM 系列防火墙的一个实例或在 Linux 主机上部署 VM 系列防火墙的多个实例。可以使用 Virtual Wire、第 2 层或第 3 层接口部署 VM 系列防火墙。如果您计划在 VM 系列防火墙上使用 SR-IOV 功能接口，则只能将接口配置作为第 3 层接口。

- 保护单个主机上的流量
- 保护 Linux 主机之间的流量

保护单个主机上的流量

要保护 Linux 服务器上各来宾之间的东向西流量，可以使用 Virtual Wire、第 2 层或第 3 层接口部署 VM 系列防火墙。下图显示了具有第 3 层接口的防火墙，其中已经使用 Linux 网桥连接服务器上的防火墙和其他来宾。在此部署中，通过防火墙路由 Web 服务器和数据库服务器之间的所有流量；只能通过网桥处理数据库服务器或 Web 服务器之间的流量，而不能通过防火墙路由。

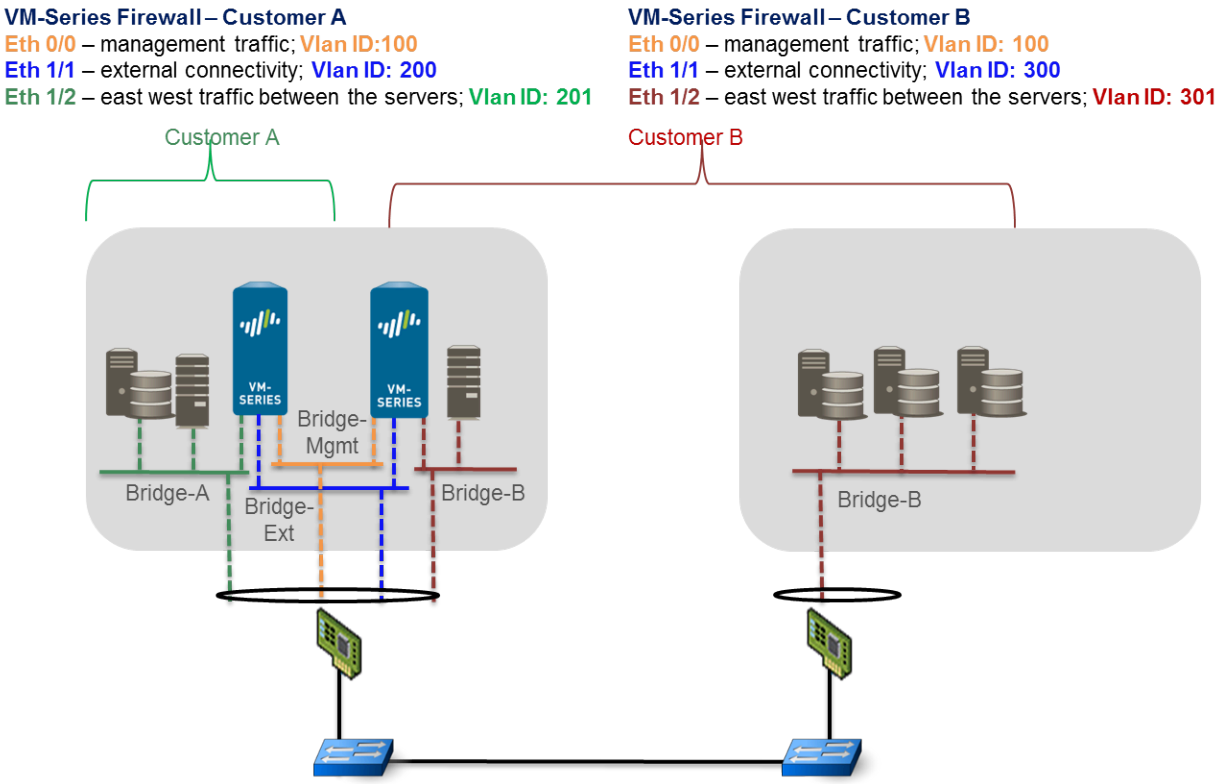


保护 Linux 主机之间的流量

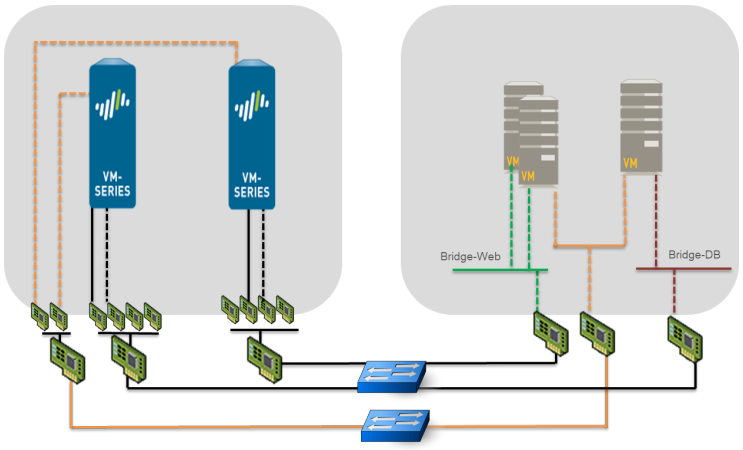
要保护您的工作负载，可以在 Linux 主机上部署多个 VM 系列防火墙实例。例如，如果要为单独的部门或客户隔离流量，可以使用 VLAN 标记

逻辑隔离网络流量，并将其路由到相应的 VM 系列防火墙。在下例中，一个 Linux 主机为两个客户（客户 A 和客户 B）托管 VM 系列防火墙，而客户 B 的工作负载分布在两个服务器上。为隔离流量并将其引导至为每个客户配置的 VM 系列防火墙，可以使用 VLAN。

©2024 Palo Alto Networks, Inc.



在此部署的另一种不同形式中，已设置使用高可用性部署的两个 VM 系列防火墙。在下图中，使用 SR-IOV 功能适配器在 Linux 服务器上部署 VM 系列防火墙。使用 SR-IOV，可以将一个 Ethernet 端口（物理功能）细分成多个虚拟功能。已将每个虚拟功能附加到配置作为第 3 层接口的 VM 系列防火墙。高可用性对等中的主动对等保护从在不同 Linux 服务器上部署的来宾向其路由的流量。



©2024 Palo Alto Networks, Inc.

在 KVM 上安装 VM 系列防火墙

用于管理 KVM 的 libvirt API 包括一系列工具，可让您创建和管理虚拟机。要在 KVM 上安装 VM 系列防火墙，可以使用下列任意方法。

- virt-manager — 使用 virt-manager 虚拟机管理器部署 VM 系列。Virt-manager 提供了一个方便的向导来帮助您完成安装过程。
- virsh — 使用 KVM 命令行部署 VM 系列。创建一个定义虚拟机实例的 XML 文件和定义防火墙的初始配置设置的引导程序 XML 文件。将 ISO 映像作为 CD-ROM 装载，然后安装防火墙。
- virt-install — 使用 KVM 命令行部署 VM 系列防火墙的另一个选项。使用此选项创建 VM 系列防火墙的定义并安装。

本文档提供了使用 virt-manager 和 virsh 在 KVM 上安装 VM 系列防火墙的步骤。

- 使用 Virt-Manager 安装 VM 系列防火墙
- 在 ISO 安装 VM 系列防火墙
- 使用 VM 系列 CLI 在 KVM 上交换管理接口
- 启用使用 SCSI 控制器
- 验证 VM 系列防火墙上网络接口排序的 PCI-ID

使用 Virt-Manager 安装 VM 系列防火墙

按照以下过程使用 virt-manager 在运行 KVM 或 RHEL 的服务器上安装 VM 系列防火墙。

- 在 KVM 主机上设置 VM 系列防火墙
- 在 KVM 上执行 VM 系列防火墙的初始配置

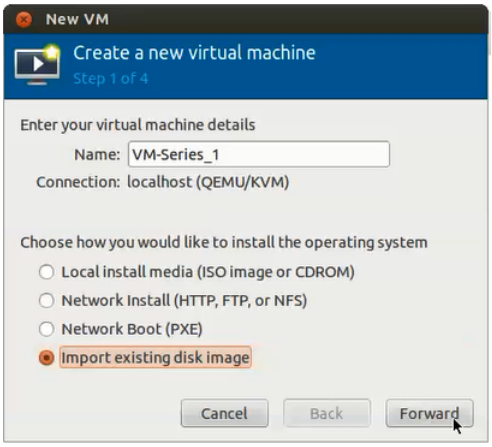
在 **KVM** 主机上设置 **VM** 系列防火墙

使用以下说明为 VM 系列防火墙配置KVM主机。

©2024 Palo Alto Networks, Inc.

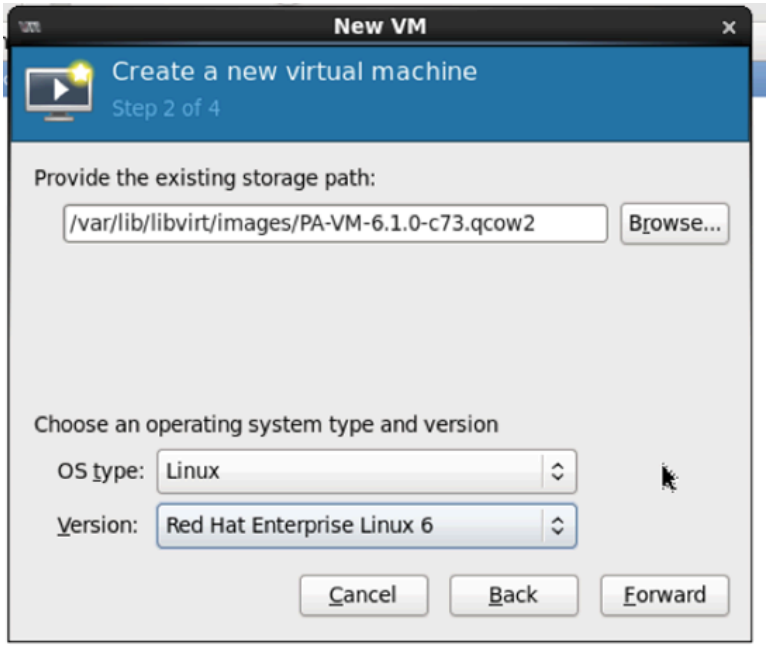
STEP 1 | 创建一个新的虚拟机并将用于KVM映像的 VM 系列防火墙添加到virt-mgr。

1. 在 Virt-manager 上，选择 **Create a new virtual machine**（创建新虚拟机）。
2. 添加 VM 系列防火墙的描述性 **Name**（名称）。



3. 选择 **Import existing disk image**（导入现有磁盘映像），浏览至映像，并设置 **OS Type**（操作系统类型）：Linux 和 **Version**（版本）：Red Hat Enterprise Linux 6。

   如果愿意，可以将“操作系统”和“版本”保留为“通用”。

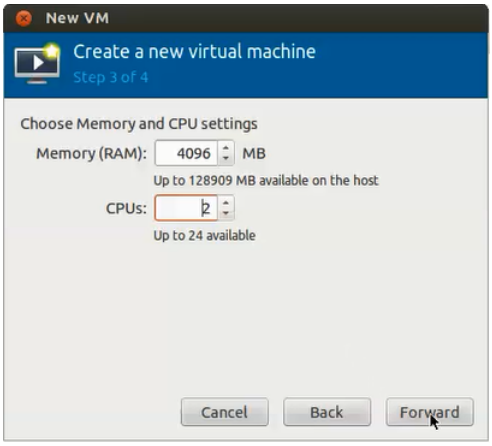


4. 添加数据接口的网络适配器：

 ©2024 Palo Alto Networks, Inc.

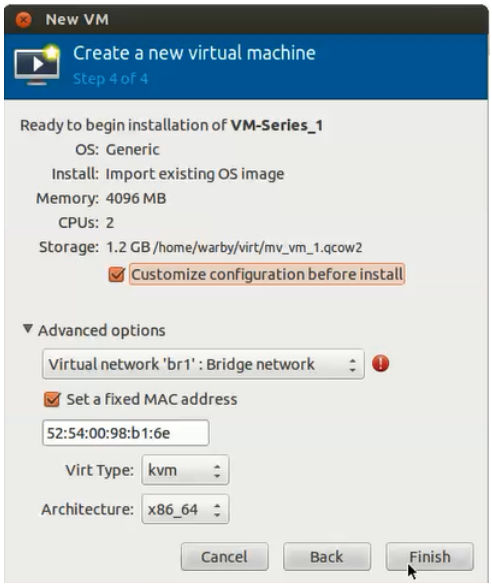
STEP 2 | 配置内存和 CPU 设置。

1. 根据您的 VM 系列型号的 VM 系列系统要求，将 **Memory**（内存）设置为最小内存。
2. 根据 VM 系列型号的VM 系列系统要求，将 **CPU** 设置为最小 CPU。



STEP 3 | 启用配置自定义并选择管理接口桥接。

1. 选择 **Customize configuration before install**（在安装之前自定义配置）。
2. 在“高级”选项下，选择管理接口的网桥，并接受默认设置。



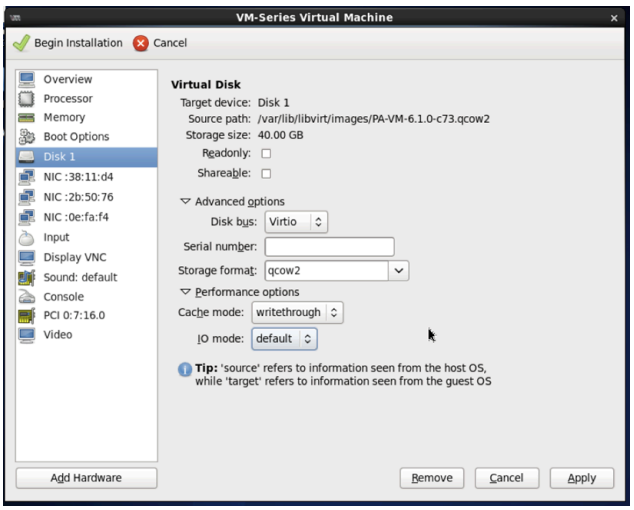
©2024 Palo Alto Networks, Inc.

STEP 4 | 配置虚拟磁盘设置。

1. 选择 **Disk**（磁盘），展开 Advanced（高级）选项并选择 **Storage format**（存储格式）— qcow2；**Disk Bus**（磁盘总线）— Virtio 或 IDE，具体取决于您的设置。

   如果要使用 *SCSI* 磁盘总线，请参阅 Enable the Use of a SCSI Controller（启用使用 SCSI 控制器）。

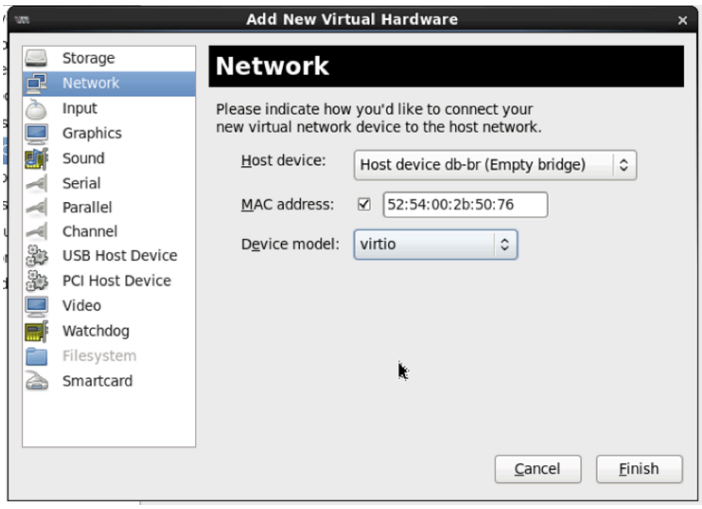
2. 展开“性能”选项，并将 **Cache mode**（高速缓存模式）设置为 **writethrough**。此设置缩短了安装时间和提高了在 VM 系列防火墙上执行的速度。



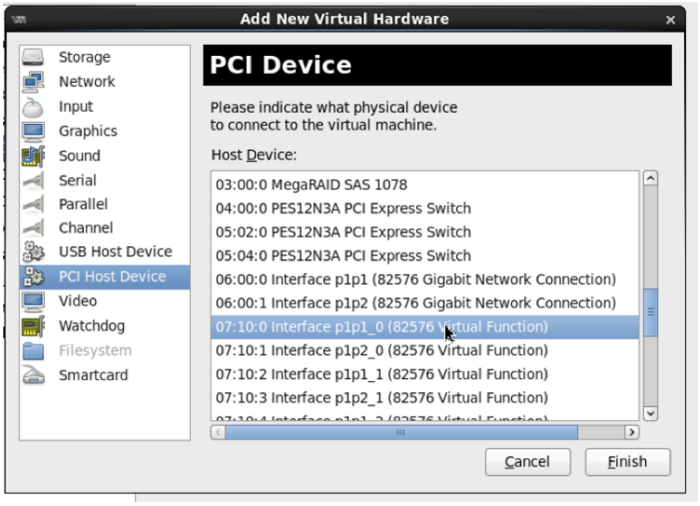
 ©2024 Palo Alto Networks, Inc.

STEP 5 | 配置网络适配器。

1. 如果使用软件网桥（如 Linux 网桥或 Open vSwitch），选择 **Add Hardware**（添加硬件）> **Network**（网络）。
2. 对于 **Host Device**（主机设备），输入网桥的名称或从下拉列表中选择。
3. 要指定驱动程序，将 **Device Model**（设备型号）设置为 e-1000 或 virtio。这些是唯一支持的虚拟接口类型。



4. 对于 PCI-passthrough 或 SR-IOV 功能设备，选择 **Add Hardware**（添加硬件） > **PCI Host Device**（**PCI** 主机设备）



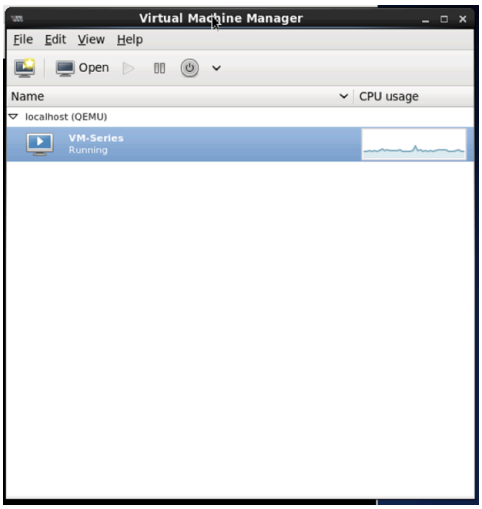
。

5. 在 **Host Device**（主机设备）列表中，选择网卡或虚拟功能上的接口。
6. 单击应用或完成。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 单击 **Begin Installation**（开始安装）Begin Installation。完成安装需要等待 5-7 分钟。

默认情况下，在 *etc/libvirt/qemu* 中创建并存储 *VM* 系列防火墙的 *XML* 模板。



STEP 7 | （可选）引导 VM 系列防火墙

如果您正在使用引导来执行 KVM 上 VM 系列防火墙的配置，请参阅在 KVM 中引导 VM 系列防火墙。有关引导的更多信息，请参阅 引导 VM 系列防火墙。

STEP 8 | 配置管理接口的网络访问设置。

1. 打开与控制台的连接。
2. 使用用户名/密码登录到防火墙：admin/admin。
3. 使用以下命令进入配置模式：

   ```
   配置
   ```

4. 使用以下命令配置管理接口：

   1. ```
      set deviceconfig system type static
      ```
   2. ```
      set deviceconfig system ip-address <Firewall-IP>
       netmask <netmask> default-gateway <gateway-IP> dns-setting
       servers primary <DNS-IP>
      ```

      其中 <*Firewall-IP*> 是您想要分配给管理接口的 IP 地址，<*netmask*> 是子网掩码，<*gateway-IP*> 是网关的 IP 地址，<*DNS-IP*> 是 DNS 服务器的 IP 地址。
   3. ```
      提交
      ```


©2024 Palo Alto Networks, Inc.
      ```

STEP 9 | 确认已将主机上的端口映像到 VM 系列防火墙上的接口。为了验证 Linux 主机上的接口顺序，请参阅 验证 VM 系列防火墙上网络接口排序的 PCI-ID。

为了确保由正确的接口处理流量，使用以下命令来确定要将主机上的哪些端口映射到 VM 系列防火墙上的端口。

```
admin@PAN-VM> debug show vm-series interfaces all Phoenix_interface
 Base-OS_port Base-OS_MAC PCI-ID mgt                                eth0
 52:54:00:d7:91:52 0000:00:03.0 Ethernet1/1 eth1 52:54:00:fe:8c:80
 0000:00:06.0 Ethernet1/2 eth2 0e:c6:6b:b4:72:06 0000:00:07.0
 Ethernet1/3 eth3 06:1b:a5:7e:a5:78 0000:00:08.0 Ethernet1/4 eth4
 26:a9:26:54:27:a1 0000:00:09.0 Ethernet1/5 eth5 52:54:00:f4:62:13
 0000:00:11.0
```

STEP 10 | 访问 VM 系列防火墙的 Web 接口和配置接口，并定义安全规则和 NAT 规则来安全启用要保护的应用程序。

请参阅《PAN-OS 管理员指南》。

在 KVM 上执行 VM 系列防火墙的初始配置

使用 KVM 服务器上的虚拟设备控制台设置对 VM 系列防火墙的网络访问权限。默认情况下， VM 系列防火墙使用DHCP获取管理接口的IP地址。但是，您可以分配静态 IP 地址。完成初始配置后，访问 Web 界面以完成进一步的配置任务。如果使用 Panorama 进行集中管理，请参阅《Panorama 管理员指南》，了解有关使用 Panorama 管理设备的详细信息。

如果要使用引导在 KVM 上执行 VM 系列防火墙的配置，请参阅在 KVM 上引导 VM 系列防火墙。

有关引导的一般信息，请参阅引导 VM 系列防火墙。

STEP 1 | 从网络管理员处收集必要的信息。

- MGT 端口的 IP 地址
- 子网掩码
- 默认网关
- DNS 服务器 IP 地址

STEP 2 | 访问 VM 系列防火墙的控制台。

1. 在此 VM 系列防火墙的 KVM 服务器上，选择 **Console**（控制台）选项卡，或右键单击此 VM 系列防火墙并选择 **Open Console**（打开控制台）。
2. 按 Enter 键访问登录屏幕。
3. 输入登录的默认用户名/密码 (admin/admin)。
4. 输入 **`configure`**（配置）以切换到“Configuration（配置）”模式。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 配置管理接口的网络访问设置。

输入以下命令：

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> 网络掩码 <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | 提交您所做的更改，并退出配置模式。

输入 **commit**。

输入 **exit**。

在 ISO 安装 VM 系列防火墙

手动创建 VM 系列防火墙的 XML 定义，然后使用 virsh 将定义作为 ISO 导入。Virsh 是一个功能强大的工具，可让您完全管理虚拟机。

- 使用 ISO 文件部署 VM 系列防火墙
- VM 系列防火墙的 XML 文件示例

使用 ISO 文件部署 VM 系列防火墙

如果要在启动时将脚本传递到 VM 系列防火墙，可以使用 ISO 文件安装 CD-ROM。ISO 文件可让您定义引导 XML 文件，包括防火墙的管理端口的初始配置参数。VM 系列防火墙会在第一次启动时检查 **bootstrap-networkconfig.xml** 文件，并使用在其中定义的值。

如果在解析引导文件时出现一个错误，*VM* 系列防火墙将拒绝此文件中的所有配置并使用默认值启动。

STEP 1 | 创建 XML 文件并将其定义为虚拟机实例。

有关示例文件，请参阅 VM 系列防火墙的 XML 文件示例。

在本示例中，VM 系列防火墙称为 PAN_Firewall_DC1。

例如：

```
user-PowerEdge-R510:~/kvm_script$ sudo vi /etc/libvirt/qemu/
PAN_Firewall_DC1.xml user-PowerEdge-R510:~/kvm_script$ sudo
 virsh define/etc/libvirt/qemu/PAN_Firewall_DC1.xml Domain
 PAN_Firewall_DC1_bootstp defined from /etc/libvirt/qemu/
PAN_Firewall_DC1.xml user-PowerEdge-R510:~/kvm_script$
 sudo virsh -q attach-interface PAN_Firewall_DC1_bootstp
 bridge br1 --model=virtio --persistent user-PowerEdge-
R510:~/kvm_script$ virsh list --all Id Name State
 ---------------------------------------------- -
 PAN_Firewall_DC1_bootstp shut off
```


©2024 Palo Alto Networks, Inc.

STEP 2 | 创建引导 XML 文件。

您可以在此文件中定义初始配置参数并将其命名为 bootstrap-networkconfig。

如果不想包括参数（如 *panorama-server-secondary*），可以从文件中删除整行。如果要将 *IP* 地址字段留空，将不会成功解析文件。

使用下例作为 bootstrap-networkconfig 文件的模板。bootstrap-networkconfig 文件只能包括以下参数：

```
<vm-initcfg> <hostname>VM_ABC_Company</hostname> <ip-
address>10.5.132.162</ip-address> <netmask>255.255.254.0</
netmask> <default-gateway>10.5.132.1</default-gateway> <dns-
primary>10.44.2.10</dns-primary> <dns-secondary>8.8.8.8</dns-
secondary> <panorama-server-primary>10.5.133.4</panorama-server-
primary> <panorama-server-secondary>10.5.133.5</panorama-server-
secondary> </vm-initcfg>
```

STEP 3 | 创建 ISO 文件。在本示例中，我们使用 mkisofs。

将 *ISO* 文件保存在映像目录 *(/var/lib/libvirt/image)* 或 *qemu* 目录 *(/etc/libvirt/qemu)* 中，以确保防火墙拥有对 *ISO* 文件的读取权限。

例如：

```
# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -
allow-lowercase -allow-multidot -o <iso-filename> bootstrap-
networkconfig.xml
```

STEP 4 | 将 ISO 文件附加到 CD-ROM。

例如：

```
# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --
mode readonly –persistent\
```

VM 系列防火墙的 XML 文件示例

```
<?xml version="1.0"?> <domain type="kvm"> <name>PAN_Firewall_DC1</
name> <memory>4194304</memory> <currentMemory>4194304</currentMemory>
 <vcpu placement="static">2</vcpu> <os> <type arch="x86_64">hvm</
type> <boot dev="hd"/> </os> <features> <acpi/> <apic/> <pae/> </
features> <clock offset="utc"/> <on_poweroff>destroy</on_poweroff>
 <on_reboot>restart</on_reboot> <on_crash>restart</on_crash>
 <devices> <emulator>/usr/libexec/qemu-kvm</emulator> <disk
 type="file" device="disk"> <driver type="qcow2" name="qemu"/>
 <source file="/var/lib/libvirt/images/panos-kvm.qcow2"/> <target
 dev="vda" bus="virtio"/> </disk> <controller type="usb" index="0"/
> <controller type="ide" index="0"/> <controller type="scsi"
 index="0"/> <serial type="pty"> <source path="/dev/pts/1"/> <target
```


©2024 Palo Alto Networks, Inc.

```
 port="0"/> <alias name="serial0"/> </serial> <console type="pty"
 tty="/dev/pts/1"> <source path="/dev/pts/1"/> <target type="serial"
 port="0"/> <alias name="serial0"/> </console> <input type="mouse"
 bus="ps2"/> <graphics type="vnc" port="5900" autoport="yes"/> </
devices> </domain>
```

如需修改在 *VM* 系列防火墙上分配的 *vCPU* 的数量，请在样本 *XML* 文件的此行中将 *vCPU* 数从 *“2”* 改为 *“4”* 或 *“8”*：

```
<vcpu placement="static">2</vcpu>
```

使用 VM 系列 CLI 在 KVM 上交换管理接口

默认情况下，VM 系列防火墙分配第一个接口 (eth0) 作为管理接口。但是，在某些部署中，必须将第一个接口预映射到公共 IP 地址。因此，必须将管理接口分配给不同的接口。将公共 IP 地址分配给管理接口存在安全风险。

或者，作为 init-cfg.txt 文件组件的一部分，您可以在引导时启用管理接口交换。

STEP 1 | 登录到 VM 系列防火墙 CLI，然后输入以下命令：

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | 确认希望交换接口，然后将 eth1 数据面板接口用作管理接口。

STEP 3 | 重启防火墙，以使交换操作成效。使用以下命令：

```
request restart system
```

STEP 4 | 验证接口交换已完成。使用以下命令：

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```

启用使用 SCSI 控制器

如果您希望 VM 系列防火墙使用磁盘总线型 SCSI 访问虚拟磁盘，可以使用以下说明将 virtio scsi 控制器附加到防火墙，然后启用使用 virtio-scsi 控制器。

Ubuntu 12.04 上的 *KVM* 不支持 *virtio-scsi* 控制器；只能在运行 *RHEL* 或 *CentOS* 的 *VM* 系列防火墙上启用 *virtio-scsi* 控制器。

此过程需要 *virsh*，因为 *Virt-manager* 不支持 *virtio-scsi* 控制器。

STEP 1 | 创建用于 SCSI 控制器的 XML 文件。在本示例中，将其称为 virt-scsi.xml。

 ©2024 Palo Alto Networks, Inc.

```
[root@localhost~]# cat /root/virt-scsi.xml <controller type='scsi'
 index='0' model='virtio-scsi'> <address type='pci' domain='0x0000'
 bus='0x00' slot='0x0b'function='0x0'/> </controller>
```

确保用于 *virtio-scsi* 控制器的插槽不会与其他设备发生冲突。

STEP 2 | 将此控制器与 VM 系列防火墙的 XML 模板相关联。

```
[root@localhost~]# virsh attach-device --config <VM-Series_name> /
root/virt-scsi.xml Device attached successfully
```

STEP 3 | 启用防火墙使用 SCSI 控制器。

```
[root@localhost~]# virsh attach-disk <VM-Series_name>/var/
lib/libvirt/images/PA-VM-6.1.0-c73.qcow2 sda --cache none --
persistent Disk attached successfully
```

STEP 4 | 编辑 VM 系列防火墙的 XML 模板。在 XML 模板中，必须更改防火墙使用的目标磁盘和磁盘总线。

默认情况下，*XML* 模板存储在 *etc/libvirt/qemu* 中。

```
<disk type='file' device='disk'> <driver name='qemu' type='qcow2'
 cache='writeback'/> <source file='/var/lib/libvirt/images/PA-
VM-7.0.0-c73.qcow2'/> <target dev='sda' bus='scsi'/> <address
 type='drive' controller='0' bus='0' target='0' unit='0'/> </disk>
```

验证 VM 系列防火墙上网络接口排序的 PCI-ID

无论您是使用虚拟接口（Linux/OVS 网桥）还是使用 PCI 设备（PCI-passthrough 或 SR-IOV 功能适配器）连接到 VM 系列防火墙，VM 系列防火墙都会将接口视为 PCI 设备。在 VM 系列防火墙上将根据 PCI-ID 分配接口，其中 PCI-ID 是一个结合了接口的总线、设备或插槽和功能的值。接口从最低 PCI-ID 开始排序，这意味着将防火墙的管理接口 (eth0) 分配给具有最低 PCI-ID 的接口。

假设您向 VM 系列防火墙分配四个接口，三个虚拟接口为 virtio 和 e1000 类型，第四个接口为 PCI 设备。要查看每个接口的 PCI-ID，请在 Linux 主机上输入命令 **virsh dumpxml $ domain *<name of the VM-Series firewall>***，以便查看附加到 VM 系列防火墙的接口列表。在输出中，检查以下网络配置：

```
<interface type='bridge'> <mac address='52:54:00:d7:91:52'/> <source
 bridge='mgmt-br'/> <model type='virtio'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x03' function='0x0'/> </interface>
 <interface type='bridge'> <mac address='52:54:00:f4:62:13'/>
 <source bridge='br8'/> <model type='e1000'/> <address type='pci'
```

 ©2024 Palo Alto Networks, Inc.

```
 domain='0x0000' bus='0x00' slot='0x10' function='0x0'/> </interface>
 <interface type='bridge'> <mac address='52:54:00:fe:8c:80'/>
 <source bridge='br8'/> <model type='e1000'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x06' function='0x0'/> </interface>
 <hostdev mode='subsystem' type='pci' managed='yes'> <source>
 <address domain='0x0000' bus='0x08' slot='0x10' function='0x1'/> </
source> <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
 function='0x0'/> </hostdev>
```

在这种情况下，每个防火墙的 PCI-ID 如下：

- 第一个虚拟接口 PCI-ID 为 00:03:00
- 第二个虚拟接口 PCI-ID 为 00:10:00
- 第三个虚拟接口 PCI-ID 为 00:06:00
- 第四个接口 PCI-ID 为 00:07:00

因此，在 VM 系列防火墙上，分配 PCI-ID 为 00:03:00 的接口作为 eth0（管理接口）、分配 PCI-ID 为 00:06:00 的接口作为 eth1 (ethernet1/1)、分配 PCI-ID 为 00:07:00 的接口作为 eth2 (ethernet1/2) 并分配 PCI-ID 为 00:10:00 的接口作为 eth3 (ethernet1/3)。

©2024 Palo Alto Networks, Inc.

KVM 的 VM 系列性能调整

用于 KVM 的 VM 系列防火墙是一款高性能设备，但可能需要调整虚拟机监控程序以获得最佳结果。本节介绍了一些有助于实现 VM 系列防火墙最佳性能的最佳实践和建议。

默认情况下，KVM 使用 Linux 网桥进行虚拟机联网。但是，虚拟环境中的最佳性能是通过专用 I/O 接口（PCI passthrough 或 SR-IOV）实现的。如果需要虚拟交换机，请使用性能优化的虚拟交换机（例如带有 DPDK 的 Open vSwitch）。

- 在 Ubuntu 16.04.1 LTS 上安装 KVM 和 Open vSwitch
- 在 KVM 上启用 Open vSwitch
- 将 Open vSwitch 与 DPDK 集成
- 在 KVM 上启用 SR-IOV
- 使用 SR-IOV 启用 VLAN 访问模式
- 在 KVM 上启用 NIC 的多队列支持
- 在 KVM 上的 NUMA 节点中隔离 CPU 资源

在 Ubuntu 16.04.1 LTS 上安装 KVM 和 Open vSwitch

为便于安装，推荐使用 Ubuntu 16.04.1 LTS 作为 KVM 虚拟机监控程序平台。

STEP 1 | 安装 KVM 和 OVS。

1. 登录到 Ubuntu CLI。
2. 执行以下命令：

```
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder
 bridge-utils $ sudo apt-get install openvswitch-switch
```

STEP 2 | 检查并比较相关数据包的版本。

执行以下命令：

```
$ virsh --version 1.3.1 $ libvirtd --version libvirtd (libvirt)
 1.3.1 $ /usr/bin/qemu-system-x86_64 --version QEMU emulator
 version 2.5.0 (Debian 1:2.5+dfsg-5ubuntu10.6), Copyright (c)
 2003-2008 Fabrice Bellard $ ovs-vsctl --version ovs-vsctl (Open
 vSwitch) 2.5.0 Compiled Mar 10 2016 14:16:49 DB Schema 7.12.1
```

在 KVM 上启用 Open vSwitch

通过修改来宾 XML 定义网络设置启用 OVS。

修改来宾 XML 定义，如下所示。

©2024 Palo Alto Networks, Inc.

```
[...] <interface type='bridge'> <mac address='52:54:00:fb:00:01'/>
 <source bridge='ovsbr0'/> <virtualport type='openvswitch'/> <model
 type='virtio'/> <address type='pci' domain='0x0000' bus='0x00'
 slot='0x03' function='0x0'/> </interface> [...]
```

将 Open vSwitch 与 DPDK 集成

要将 Open vSwitch (OVS) 与 DPDK 集成，必须安装所需的组件，然后配置 OVS。在 KVM 的 VM 系列防火墙上默认启用 DPDK。

- 在 Ubuntu 上安装 QEMU、DPDK 和 OVS
- 在主机上配置 OVS 和 DPDK
- 编辑 VM 系列防火墙配置文件

在 Ubuntu 上安装 QEMU、DPDK 和 OVS

在 OVS 上启用 DPDK 之前，必须安装 QEMU 2.5.0、DPDK 2.2.0 和 OVS 2.5.1。完成以下过程以安装组件。

STEP 1 | 登录到 KVM 主机 CLI。

STEP 2 | 通过执行以下命令安装 QEMU 2.5.0：

```
apt-get install build-essential gcc pkg-config glib-2.0 libglib2.0-
dev libsdl1.2-dev libaio-dev libcap-dev libattr1-dev libpixman-1-
dev apt-get build-dep qemu apt-get install qemu-kvm libvirt-bin
 wget http://wiki.qemu.org/download/qemu-2.5.0.tar.bz2 tar xjvf
 qemu-2.5.0.tar.bz2 cd qemu-2.5.0 ./configure make make install
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 安装 dpdk-2.2.0。

1. 执行以下命令：

```
wget http://dpdk.org/browse/dpdk/snapshot/dpdk-2.2.0.tar.gz
 tar xzvf dpdk-2.2.0.tar.gz cd dpdk-2.2.0 vi config/
common_linuxapp
```

2. 将 `CONFIG_RTE_APP_TEST=y` 更改为 **`CONFIG_RTE_APP_TEST=n`**
3. 将 `CONFIG_RTE_BUILD_COMBINE_LIBS=n` 更改为 **`CONFIG_RTE_BUILD_COMBINE_LIBS=y`**
4. 执行以下命令：

```
vi GNUmakefile
```

5. 将 `ROOTDIRS-y := lib drivers app` 更改为 **`ROOTDIRS-y := lib drivers`**
6. 执行以下命令：

```
make install T=x86_64-native-linuxapp-gcc
```

STEP 4 | 通过执行以下命令安装 OVS 2.5.1：

```
wget http://openvswitch.org/releases/openvswitch-2.5.1.tar.gz
 tar xzvf openvswitch-2.5.1.tar.gz cd openvswitch-2.5.1 ./
configure –with-dpdk=”/root/dpdk-2.2.0/x86_64-native-linuxapp-
gcc/” make make install
```

在主机上配置 OVS 和 DPDK

安装必要的组件以支持 OVS 和 DPDK 后，必须将主机配置为使用 OVS 和 DPDK。

STEP 1 | 登录到 KVM 主机 CLI。

STEP 2 | 如果要替换或重新配置现有的 OVS-DPDK 设置，请执行以下命令重置以前的任何配置。对每个接口重复执行以下命令。

```
rm /usr/local/var/run/openvswitch/<interface-name>
```

STEP 3 | 配置 OVS 的初始大页面。

```
echo 16384 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```


©2024 Palo Alto Networks, Inc.

STEP 4 | 为 QEMU 装载大页面：

```
mkdir /dev/hugepages mkdir /dev/hugepages/libvirt mkdir /dev/
hugepages/libvirt/qemu mount -t hugetlbfs hugetlbfs /dev/hugepages/
libvirt/qemu
```

STEP 5 | 使用以下命令终止任何当前存在的 OVS 守护进程。

```
killall ovsdb-server ovs-vswitchd
```

STEP 6 | 为 OVS 守护进程创建目录。

```
mkdir -p /usr/local/etc/openvswitch
mkdir -p /usr/local/var/run/openvswitch
```

STEP 7 | 清除旧的目录。

```
rm -f /var/run/openvswitch/vhost-user*
rm -f /usr/local/etc/openvswitch/conf.db
```

STEP 8 | 初始化配置数据库。

```
ovsdb-tool create /usr/local/etc/openvswitch/conf.db\
/usr/local/share/openvswitch/vswitch.ovsschema
```

STEP 9 | 创建 OVS DB 服务器。

```
ovsdb-server --remote=punix:/usr/local/var/run/openvswitch/
db.sock \ --remote=db:Open_vSwitch,Open_vSwitch,manager_options
 \ --private-key=db:Open_vSwitch,SSL,private_key \ --
certificate=db:Open_vSwitch,SSL,certificate \ --bootstrap-ca-
cert=db:Open_vSwitch,SSL,ca_cert \ --pidfile --detach
```

STEP 10 | 初始化 OVS。

```
ovs-vsctl --no-wait init
```

STEP 11 | 启动数据库服务器。

```
export DB_SOCK=/usr/local/var/run/openvswitch/db.sock
```

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 安装 DPDK 的 igb_uio 模块（网络设备驱动程序）。

```
cd ~/dpdk-2.2.0/x86_64-native-linuxapp-gcc/kmod modprobe uio insmod
 igb_uio.ko cd ~/dpdk-2.2.0/tools/
```

STEP 13 | 使用 PCI-ID 或接口名称在接口上启用 DPDK。

```
./dpdk_nic_bind.py --bind=igb_uio <your first data interface>
./dpdk_nic_bind.py --bind=igb_uio <your second data interface>
```

STEP 14 | 在 DPDK 模式下启动 OVS 守护进程。您可以更改 ovs-vswitchd 的核心数量。通过将 -c 0x1 更改为 -c 0x3，可以让两个内核运行此守护程序。

```
ovs-vswitchd --dpdk -c 0x3 -n 4 -- unix:$DB_SOCK --pidfile --
detach
echo 50000 > /sys/kernel/mm/hugepages/hugepages-2048kB/
nr_hugepages
```

STEP 15 | 创建 OVS 桥并将端口连接到 OVS 桥。

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
 datapath_type=netdev
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
ovs-vsctl add-br ovs-br1 -- set bridge ovs-br1
 datapath_type=netdev
ovs-vsctl add-port ovs-br1 dpdk1 -- set Interface dpdk1 type=dpdk
```

STEP 16 | 为 OVS 创建 DPDK vhost 用户端口。

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
 type=dpdkvhostuser
ovs-vsctl add-port ovs-br1 vhost-user2 -- set Interface vhost-user2
 type=dpdkvhostuser
```

STEP 17 | 设置主机使用的 NIC 的硬件队列数量。

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=8
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-txqs=8
```

STEP 18 | 设置用于 OVS 的 CPU 掩码。

```
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0xffff
```

 ©2024 Palo Alto Networks, Inc.

STEP 19 | 为 DPDK vhost 用户端口设置必要的权限。在下面的示例中，777 用于提供读取、写入和可执行权限。

```
chmod 777 /usr/local/var/run/openvswitch/vhost-user1
chmod 777 /usr/local/var/run/openvswitch/vhost-user2
chmod 777 /dev/hugepages/libvirt/qemu
```

编辑 VM 系列防火墙配置文件

编辑 VM 系列防火墙 XML 配置文件以支持 OVS 和 DPDK。您可以在部署 VM 系列防火墙后访问 XML 配置文件。如果在部署防火墙后执行此操作，请确保在进行任何更改之前关闭防火墙。下面的值是示例，每个参数的值将根据您的 VM 系列防火墙型号而有所不同。

STEP 1 | 登录到 KVM 主机 CLI。

STEP 2 | 编辑 VM 系列防火墙的 XML 配置文件。

1. 使用 **virsh edit $<*your-vm-series-name*>** 打开 XML 配置文件。
2. 为大页面设置内存支持。确保提供足够的内存支持您在主机上部署的 VM 系列防火墙型号。请参阅 VM 系列系统要求了解更多信息。

```
<memory unit='KiB'>12582912</memory> <currentMemory
 unit='KiB'>6291456</currentMemory> <memoryBacking>
 <hugepages/>
```

3. 为 VM 设置必要的 CPU 标志。

```
<cpu mode='host-model'>
```

4. 启用虚拟机和主机之间的内存共享。

```
<numa> <cell id='0' cpus='0,2,4,6' memory='6291456'
 unit='KiB' memAccess='shared'/> <cell id='1' cpus='1,3,5,7'
 memory='6291456' unit='KiB' memAccess='shared'/> </numa>
```

5. 将 DPDK vhost 用户端口设置为 VM 系列防火墙的网络接口。另外，请设置主机提供给 VM 系列防火墙的 virtio 虚拟队列的数量。

```
<interface type='vhostuser'> <mac address='52:54:00:36:83:70'/
> <source type='unix' path='/usr/local/var/run/openvswitch/
vhost-user1' mode='client'/> <model type='virtio'/>
 <driver name=’ vhost’  queues=’ 8’ /> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x04' function='0x0'/
> </interface> <interface type='vhostuser'> <mac
 address='52:54:00:30:d7:94'/> <source type='unix' path='/
usr/local/var/run/openvswitch/vhost-user2' mode='client'/>
 <model type='virtio'/> <driver name=’ vhost’  qeueus=’ 8’ >
 <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
 function='0x0'/> </interface>
```


©2024 Palo Alto Networks, Inc.

在 KVM 上启用 SR-IOV

单根 I/O 虚拟化 (SR-IOV) 允许单个根端口下的单个 PCIe 物理设备看起来像是虚拟机监控程序或来宾的多个单独的物理设备。要在 KVM 来宾上启用 SR-IOV，请定义与物理 NIC 关联的虚拟功能 (VF) 设备池，并自动将池中的 VF 设备分配给 PCI ID。

对于具有 Intel 10GB 网络接口（ixgbe 驱动程序）的 SR-IOV，驱动程序版本必须为 4.2.5 或更高版本才能支持每个 NIC 接口的多个队列。请参阅 PAN-OS 版本的 PacketMMAP 和 DPDK 驱动程序支持的兼容性矩阵。

STEP 1 | 为 VF 池定义一个网络。

1. 生成一个包含类似以下示例的文本的 XML 文件。将 `pf dev` 的值更改为与您的 SR-IOV 设备的物理功能对应的 `ethdev`。

```
<network> <name>passthrough</name> <forward mode='hostdev'
 managed='yes'> <pf dev='eth3'/> </forward> </network>
```

2. 保存 XML 文件。
3. 执行以下命令：

```
$ virsh net-define <path to network XML file>  $ virsh net-
autostart passthrough $ virsh net-start passthrough
```

STEP 2 | 要确保在 DPDK 模式下启动 VM 系列防火墙，可编辑 KVM 虚拟机监控程序上的来宾 VM XML 配置以添加以下内容：

```
<cpu mode='host-passthrough' check='none'/>
```

这可以确保显示 CPU 标志。

要验证 VM 上显示的 CPU 标志，可执行以下命令：

```
cat /proc/cpuinfo
```

在安装 DPDK 18.11 的 PAN-OS 11.0 或更高版本的 `flags` 输出中，您需要 `AVX` 或 `AES` 和 `SSE` 标志。

STEP 3 | 在定义和启动网络后，修改来宾 XML 定义以指定网络。

```
<interface type='network'> <source network='passthrough'> </
interface>
```

当来宾启动时，VF 会自动分配给来宾。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 将多播 MAC 地址添加到防火墙。

启用 SR-IOV 后，PF 会筛选多播流量。此筛选会导致依赖于多播的应用程序（如 OSPF）失败。要防止此筛选，必须使用下列命令将多播 MAC 地址手动添加到主机：

```
#ip maddress add <multicast-mac> dev <interface-name>
```

使用 SR-IOV 启用 VLAN 访问模式

KVM 上的 VM 系列防火墙可以在 VLAN 访问模式下运行，以支持将其部署作为虚拟网络功能 (VNF) 的用例，该功能可在多租户云/数据中心环境中提供安全即服务。在 VLAN 访问模式下，每个 VNF 都具有适用于每个网络的专用虚拟网络接口 (VNI)，并在不使用 VLAN 标记的情况下将数据包发送到 SR-IOV 虚拟功能 (VF)/从 SR-IOV 虚拟功能 (VF) 接收数据包；您必须在主机虚拟机监控程序的物理和虚拟功能上启用此功能。然后，在 VM 系列防火墙上启用 VLAN 访问模式后，防火墙可以在不使用 VLAN 标记的情况下在其所有数据平面接口之间发送和接收流量。此外，如果您已配置 QoS 策略，则防火墙可以在访问接口上强制执行 QoS，并在多租户部署中提供不同的流量处理。

默认情况下，*KVM* 上的 *VM* 系列防火墙在 *VLAN* 中继模式下运行。

STEP 1 | 在主机系统上，将物理和虚拟功能设置为在 VLAN 访问模式下运行。

ip link set [inf_name] vf [vf_num] vlan [vlan_id]。

如需在 *VM* 系列防火墙上获得最佳性能，请确保：

- 启用 *CPU* 定位。请参阅在 KVM 上的 NUMA 节点中隔离 CPU 资源。
- 如果您已配置 *IPSec Tunnels*（*IPSec* 隧道），请 *Disable Replay Protection*（禁用重播保护）。

  在防火墙 *Web* 界面上，选择 ***Network***（网络） > ***IPSec Tunnels***（***IPSec*** 隧道）以选择 *IPSec* 隧道并单击 ***General***（常规），然后选择 ***Show Advanced Options***（显示高级选项）并清除 ***Enable Replay Protection***（启用重播保护）。

STEP 2 | 在 VM 系列防火墙上访问 CLI。

STEP 3 | 启用 VLAN 访问模式。

request plugins vm-series vlan-mode access-mode on

on 启用 VLAN 访问模式；要使用 VLAN 中继模式，请输入 **request plugins vm-series vlan-mode access-mode off**。

STEP 4 | 重启防火墙。

输入 **request restart system**。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 验证 VLAN 模式配置。

```
show plugins vm-series vlan-mode
```

在 KVM 上启用 NIC 的多队列支持

修改来宾 XML 定义以启用多队列 virtio-net。多队列 virtio-net 允许网络性能随 vCPU 的数量扩展，并通过创建多个 TX 和 RX 队列来支持并行数据包处理。

修改来宾 XML 定义。对于 N，插入 1 到 256 的值以指定队列数。为获得最佳结果，请将队列数与虚拟机上配置的数据面内核数相匹配。

```
<interface type='network'> <source network='default'/> <model
 type='virtio'/> <driver name='vhost' queues='N'/> </interface>
```

在 KVM 上的 NUMA 节点中隔离 CPU 资源

通过将来宾虚拟机的 CPU 资源隔离到单个非统一内存访问 (NUMA) 节点，您可以提高 KVM 上 VM 系列的性能。在 KVM 上，您可以查看 NUMA 拓扑 **virsh**。以下示例来自双节点 NUMA 系统：

STEP 1 | 查看 NUMA 拓扑。在下面的例子中，有两个 NUMA 节点（套接字），每个节点都有一个启用超线程的四核 CPU。所有的偶数编号的 CPU ID 属于一个节点，所有的奇数编号的 CPU ID 属于另一个节点。

```
% virsh capabilities <…> <topology> <cells num='2'> <cell
 id='0'> <memory unit='KiB'>33027228</memory> <pages unit='KiB'
 size='4'>8256807</pages> <pages unit='KiB' size='2048'>0</
pages> <distances> <sibling id='0' value='10'/> <sibling
 id='1' value='20'/> </distances> <cpus num='8'> <cpu id='0'
 socket_id='1' core_id='0' siblings='0,8'/> <cpu id='2'
 socket_id='1' core_id='1' siblings='2,10'/> <cpu id='4'
 socket_id='1' core_id='2' siblings='4,12'/> <cpu id='6'
 socket_id='1' core_id='3' siblings='6,14'/> <cpu id='8'
 socket_id='1' core_id='0' siblings='0,8'/> <cpu id='10'
 socket_id='1' core_id='1' siblings='2,10'/> <cpu id='12'
 socket_id='1' core_id='2' siblings='4,12'/> <cpu id='14'
 socket_id='1' core_id='3' siblings='6,14'/> </cpus> </cell> <cell
 id='1'> <memory unit='KiB'>32933812</memory> <pages unit='KiB'
 size='4'>8233453</pages> <pages unit='KiB' size='2048'>0</
pages> <distances> <sibling id='0' value='20'/> <sibling id='1'
 value='10'/> </distances> <cpus num='8'> <cpu id='1' socket_id='0'
 core_id='0' siblings='1,9'/> <cpu id='3' socket_id='0' core_id='1'
 siblings='3,11'/> <cpu id='5' socket_id='0' core_id='2'
 siblings='5,13'/> <cpu id='7' socket_id='0' core_id='3'
 siblings='7,15'/> <cpu id='9' socket_id='0' core_id='0'
 siblings='1,9'/> <cpu id='11' socket_id='0' core_id='1'
 siblings='3,11'/> <cpu id='13' socket_id='0' core_id='2'
 siblings='5,13'/> <cpu id='15' socket_id='0' core_id='3'
 siblings='7,15'/> </cpus> </cell> </cells>
```


©2024 Palo Alto Networks, Inc.

STEP 2 | 将 KVM 来宾虚拟机中的 vCPU 绑定到特定物理 vCPU，请使用 **cpuset** 来宾 xml 定义中的属性。在本例中，所有 8 个 vCPU 都固定在第一个 NUMA 节点中的物理 CPU 上。如果您不希望明确固定 vCPU，则可以省略 **cputune** 块，在这种情况下，所有 vCPU 将被固定到 cpuset 中指定的 CPU 范围，但不会被明确映射。

```
<vcpu cpuset='0,2,4,6,8,10,12,14'>8</vcpu> <cputune> <vcpupin
 vcpu='0' cpuset='0'/> <vcpupin vcpu='1' cpuset='2'/> <vcpupin
 vcpu='2' cpuset='4'/> <vcpupin vcpu='3' cpuset='6'/> <vcpupin
 vcpu='4' cpuset='8'/> <vcpupin vcpu='5' cpuset='10'/> <vcpupin
 vcpu='6' cpuset='12'/> <vcpupin vcpu='7' cpuset='14'/> </cputune>
```


©2024 Palo Alto Networks, Inc.

智能流量分流

智能流量分流 (ITO) 服务会将流量的前几个数据包路由到防火墙进行检查，以确定是应检查还是分流流量中的其余数据包。此决策基于策略或是否可以检查流量（例如，无法检查加密流量）通过仅检查可从安全检查中受益的流，可大大减少防火墙上的总体负载，并在不牺牲安全性的情况下提高 VM 系列防火墙性能。

使用软件直通技术实现智能分流

如果环境不支持流量引擎硬件来执行 ITO，则可以将 Panorama 虚拟设备配置为实现软件直通以模仿流量引擎在硬件支持环境中使用的功能。为了支持此功能，Pan-OS 支持的设备（包括 VM 系列防火墙）的流量优化已更新，包括对会话密钥合并方式的更改。

软件直通为内部会话流量利用 *GTPU*。使用 *GTPU*，内部会话完成 *L7* 数据包检查，然后遵循现有的软件直通数据路径。它会绕过不必要的操作，并利用缓存来完成操作。

基于 **DPU** 的智能分流

智能流量分流是 VM 系列防火墙安全订阅，在使用 NVIDIA BlueField-2 DPU 进行配置后，可以提高 VM 系列防火墙的容量吞吐量。VM 系列防火墙和 BlueField-2 DPU 必须安装在运行 Ubuntu 18.04、内核版本为 4.15.0-20 的 x86 物理主机上。VM 系列防火墙必须以虚拟线路模式部署。

当前 NVIDIA BlueField-2 DPU 可扩展性限制如下：

- 会话表容量：500,000 个会话
- 会话表更新率：7000 个会话/秒
- 每秒连接数：20,000
- 分流发夹速率：1500 字节数据包约 90 Gbps

如果分流到 BlueField-2 DPU 的流量超过每秒 7,000 个会话，或者分流会话表已满，则流量仍会流经 VM 系列防火墙并进行检查。当每秒会话数降至 7,000 个以下时，将恢复向 Bluefield-2 DPU 的智能流量分流。

在具有相同配置的物理主机上运行的 VM 系列防火墙支持主动/被动 HA。

智能流量分流不支持加速老化会话设置。

- 智能流量分流要求
- 智能流量分流接口
- 高可用性
- 配置软件直通
- 安装 BlueField-2 DPU
- 安装 VM 系列防火墙

©2024 Palo Alto Networks, Inc.

- 检查 BlueField-2 DPU 系统
- 启用虚拟功能
- 安装或升级 BlueField 引导流软件
- 安装或升级 Debian 软件包
- 运行智能流量分流
- Bluefield-2 DPU 故障排除
- PAN-OS 故障排除
- 参考资料

智能流量分流要求

ITO 要求在同一台 x86 物理主机上安装一个 VM 系列防火墙和一个 BlueField-2 DPU。VM 系列防火墙支持主动/被动高可用性。



您只能在每台主机上部署一个 *VM* 系列防火墙和一个 *BlueField-2 DPU*。

- 具有 2 个可用 100GB/s 端口的网络交换机（4 个用于 HA）。

  如果您要使用 VLAN，请确保交换机能够正常使用。
- X86 物理主机硬件要求。
  - 最少 120GB 的可用内存（64GB 用于服务器/56GB 用于 VM 系列防火墙）
  - 至少 18 个物理核心
  - Bluefield-2 SmartNIC MBF2M516A-CEEOT，在 PCI-e 插槽 3 或 4 中安装两个 100Gb/s 端口。
  - 按照 NVIDIA BlueField 以太网 DPU 用户指南的建议，BlueField2 DPU 上的每个端口都使用经过认证的 100GigE SFP。
- X86 主机软件要求：
  - Ubuntu 18.04，内核版本 4.15.0-20。
  - Bluefield 二进制引导流版本：5.3-1.0.0.1

    接受最终用户许可协议以开始下载。

©2024 Palo Alto Networks, Inc.

- VM 系列防火墙的虚拟机。
  - PAN-OS 11.0 或更高版本。
  - VM 系列插件 2.1.0 或更高版本。
  - 要许可智能流量分流，请为 10.0.4 及更高版本创建软件 NGFW 部署配置文件，其中至少包含 18 个 vCPU 和智能流量分流服务。配置文件可以包括其他安全服务。

    使用 PAN-OS 10.1.1 或更高版本和 VM 系列插件 2.1.1 或更高版本，要许可智能流量分流，请为 10.0.4 及更高版本创建软件 NGFW 部署配置文件，其中至少包含六 (6) 个 vCPU 和智能流量分流服务。配置文件可以包括其他安全服务。

智能流量分流接口

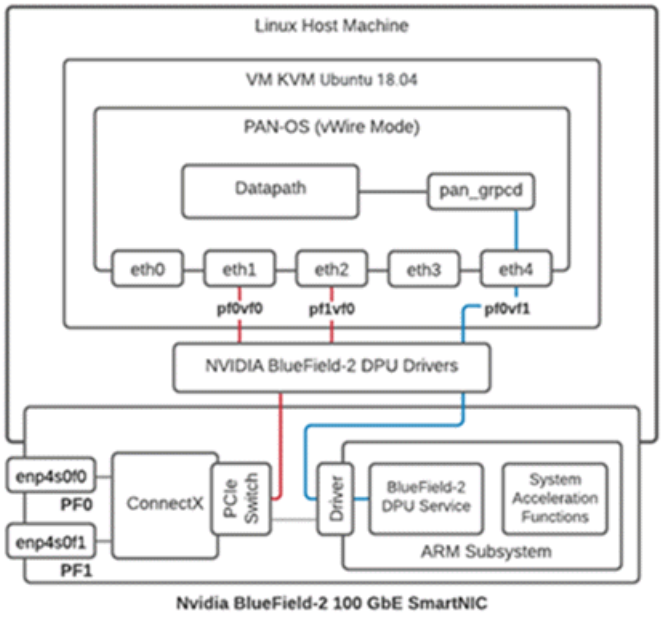
智能流量分流部署可连接三种类型的接口：

- PAN-OS 虚拟接口：
  - eth0：管理接口
  - eth1、eth2：数据平面
  - eth3：HA 接口
  - eth4：gRPC 接口
- BlueField-2 DPU 物理接口（从主机操作系统创建）。
- 用于 BlueField-2 DPU 100GB 端口（从主机操作系统创建）的主机物理接口。

通过在物理主机上创建的 SR-IOV 虚拟功能 (VF)，您可以将 PAN-OS 接口连接到 BlueField-2 DPU（参阅启用虚拟功能）。

在下图中，两个 Bluefield-2 DPU 端口显示为物理功能 PF0 和 PF1。从主机端可以观察到这些 PF 为 enp4s0f0 和 enp4s0f1，并分为多个 VF 用于 SR-IOV 功能。

©2024 Palo Alto Networks, Inc.



- 每个 PF 的第一个 VF 必须是数据端口 (eth1:pf0vf0)。
- gRPC 客户端/服务器接口的控制通道需要额外的VF (eth4:pf0v1)。
- 主机端的 VF 如下所示：
  - enp4s0f0 在 BlueField-2 DPU 上用 pf0vf0 和 pf1vf0 表示，用于数据。
  - enp4s0f1 用 pf0vf1 表示，用于 gRPC 控制流量。

高可用性

在物理主机上以 Vwire 模式部署的一对 VM 系列防火墙支持主动/被动 HA。

- 必须将防火墙安装在如智能流量分流要求中所述配置了 BlueField-2 DPU 的物理主机上。
- 对于 HA2 接口（参阅主动数据包流和被动数据包流中的图），在两台主机上使用同一 Mellanox 接口（cx-3、cx-4 或 cx-5）。
- （可选）要支持流量交换，主机必须位于单独的 VLAN 中，以便您可以使用 VLAN 标记来选择主要主机，如保护 Linux 主机之间的流量中所述。

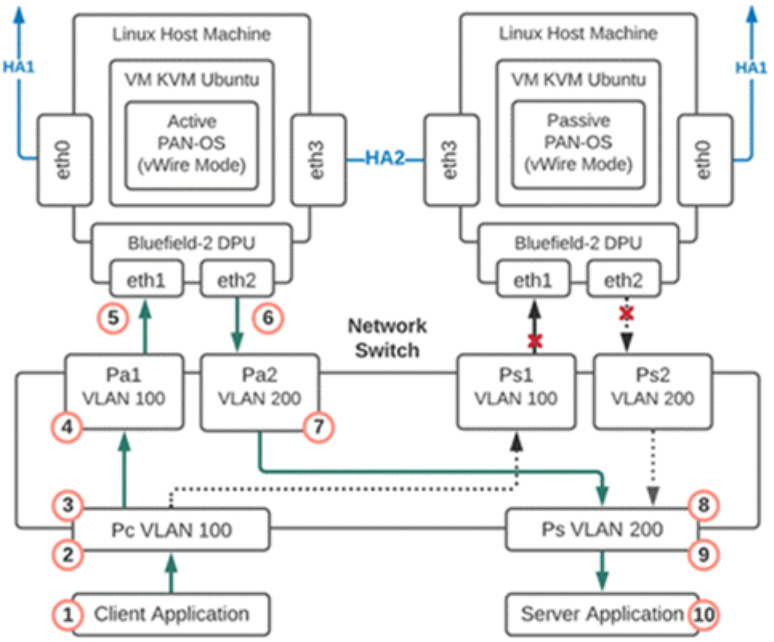
ITO H/A 专注于 VM 系列防火墙可用性。每个防火墙维护一个会话表，每个 BlueField-2 DPU 维护一个流量表。HA 配置同步活动会话表，确保在运行时将其镜像到被动防火墙。会话表存储需要检查和标记为分流的会话。

HA 使用 PAN-OS 接口 eth3，该接口位于 VM 系列防火墙的 NIC 上。Eth3 用于选择主动防火墙，并在主动/被动对上同步 VM 系列防火墙会话表。

主动数据包流

下图逐步介绍了使用可选 VLAN 配置的 HA 配置的主动数据包流。

©2024 Palo Alto Networks, Inc.



1. 数据包从客户端应用程序发送到网络交换机。
2. 数据包到达交换机端口，该端口被编程为将 VLAN 100 标签添加到数据包。
3. 由于端口 Ps1 的接口因防火墙处于被动模式而关闭，因此标记的数据包只能进入端口 Pa1。
4. 数据包到达端口 Pa1，并从数据包中删除 VLAN 100，然后将数据包传送到防火墙接口 eth1。
5. 防火墙以 vWire 模式运行，因此数据包由防火墙处理，然后从防火墙接口 eth2 发出。
6. 数据包到达端口 Pa2，并添加 VLAN 200。
7. 由于另一个 VLAN 200 端口 Ps2 关闭，因此数据包从端口 Pa2 发出，只能传送到端口 Ps。
8. 数据包到达端口 Ps，并删除 VLAN 200 标签。
9. 数据包从端口 Ps 发出，不带任何 VLAN 标签。
10. 数据包传送到服务器。

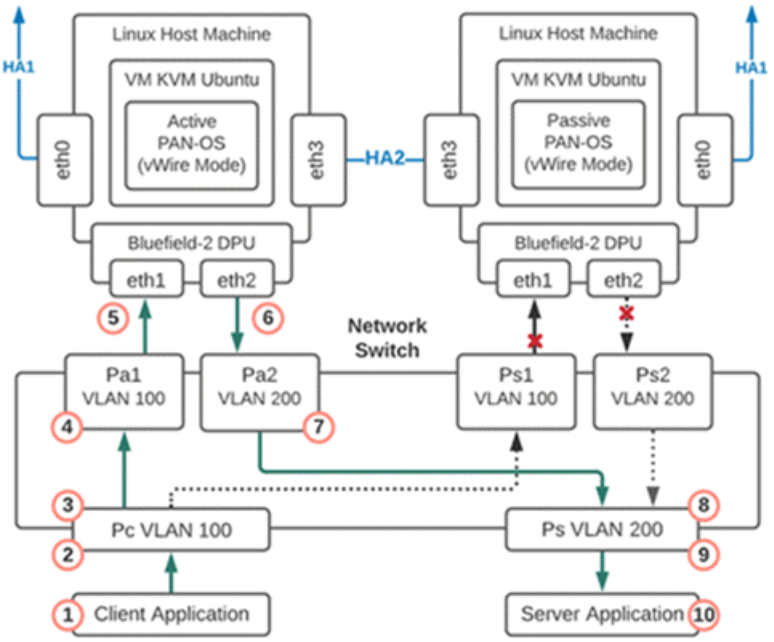
故障转移事件

当收到来自主动 VM 系列防火墙的通知或被动防火墙检测到主动系列防火墙没有响应时，就会发生故障转移事件。发生这种情况时，与端口 Pa1 和 Pa2 的网络连接将断开，与端口 Ps1 和 Ps2 的网络连接变为活动状态。

被动数据包流

当 VM 系列防火墙处于被动状态时，被动成员上的 BlueField-2 DPU 处于活动状态，但在进行故障转移并且共置的 VM 系列防火墙变为活动状态之前不会传递流量。下图逐步介绍了使用可选 VLAN 配置的 HA 配置的被动数据包流。

©2024 Palo Alto Networks, Inc.



1. 数据包从客户端应用程序发送到网络交换机。
2. 数据包到达交换机端口，该端口被编程为将 VLAN 100 标签添加到数据包。
3. 标记的数据包只能进入端口 Ps1，因为端口 Pa1 的接口已关闭，并且该防火墙现在已从被动状态变为主动状态。
4. 数据包到达端口 Ps1，并从数据包中删除 VLAN 100，然后将数据包传送到防火墙接口 eth1。
5. 防火墙以 vWire 模式运行，因此数据包由防火墙处理，然后从防火墙接口 eth2 发出。
6. 数据包到达端口 Ps2，并添加 VLAN 200。
7. 由于另一个 VLAN 200 端口 Pa2 关闭，因此数据包从端口 Ps2 发出，只能传送到端口 Ps。
8. 数据包到达端口 Ps，并删除 VLAN 200 标签。
9. 数据包从端口 Ps 发出，不带任何 VLAN 标签。
10. 数据包传送到服务器。

配置软件直通

使用命令行界面在 VM 系列防火墙上配置软件直通。

1. 以管理员身份访问 VM 系列防火墙。
2. 使用 CLI 命令 `set session sw-cut-thru yes` 启用软件直通。要禁用软件直通，请输入 `set session sw-cut-thru no`。

安装 BlueField-2 DPU

在安装 VM 系列防火墙之前，请在物理主机上安装 BlueField-2 DPU。有关 BlueField-2 DPU 的信息，请参阅软件文档：NVIDIA BLUEFIELD DPU 系列软件 V3.5.0.11563 文档。

1. 按照 NVIDIA BlueField 以太网 DPU 用户指南中的说明在主机上安装 BlueField-2 DPU。

©2024 Palo Alto Networks, Inc.

2. 按照 NVIDIA BlueField-2 DPU 软件快速入门指南安装 BlueField 驱动程序。

安装 VM 系列防火墙

VM 系列防火墙上的 KVM 标准安装就是安装 PAN-OS。请按照以下部分中的安装步骤进行操作。

- KVM 上的 VM 系列防火墙—要求和先决条件
- 使用 Virt-Manager 安装 VM 系列防火墙 或 在 ISO 安装 VM 系列防火墙

启用虚拟功能

按照 智能流量分流接口 虚拟功能 (VF) 中所述，将 PAN-OS 接口连接到 BlueField-2 DPU。

每个端口的最多虚拟功能 VF 数为 2。您总共需要三个虚拟功能：两个用于数据路径，一个用于管理接口。

STEP 1 | 在主机上启用虚拟功能。

- 默认情况下，BlueField-2 DPU 将第一个 VF 用于数据路径，即以下示例中的 enp4s0f0v0 和 enp4s0f1v0。
- 另一个 VF enp4s0f0v1 用于 BlueField-2 卡上运行的服务的管理接口（不要与 VM 系列防火墙管理接口混淆）。

$ **cat /sys/class/net/enp4s0f0/device/sriov_totalvfs**

```
8
```

$ echo 2 > **/sys/class/net/enp4s0f0/device/sriov_numvfs**

$ **cat /sys/class/net/enp4s0f1/device/sriov_totalvfs**

```
8
```

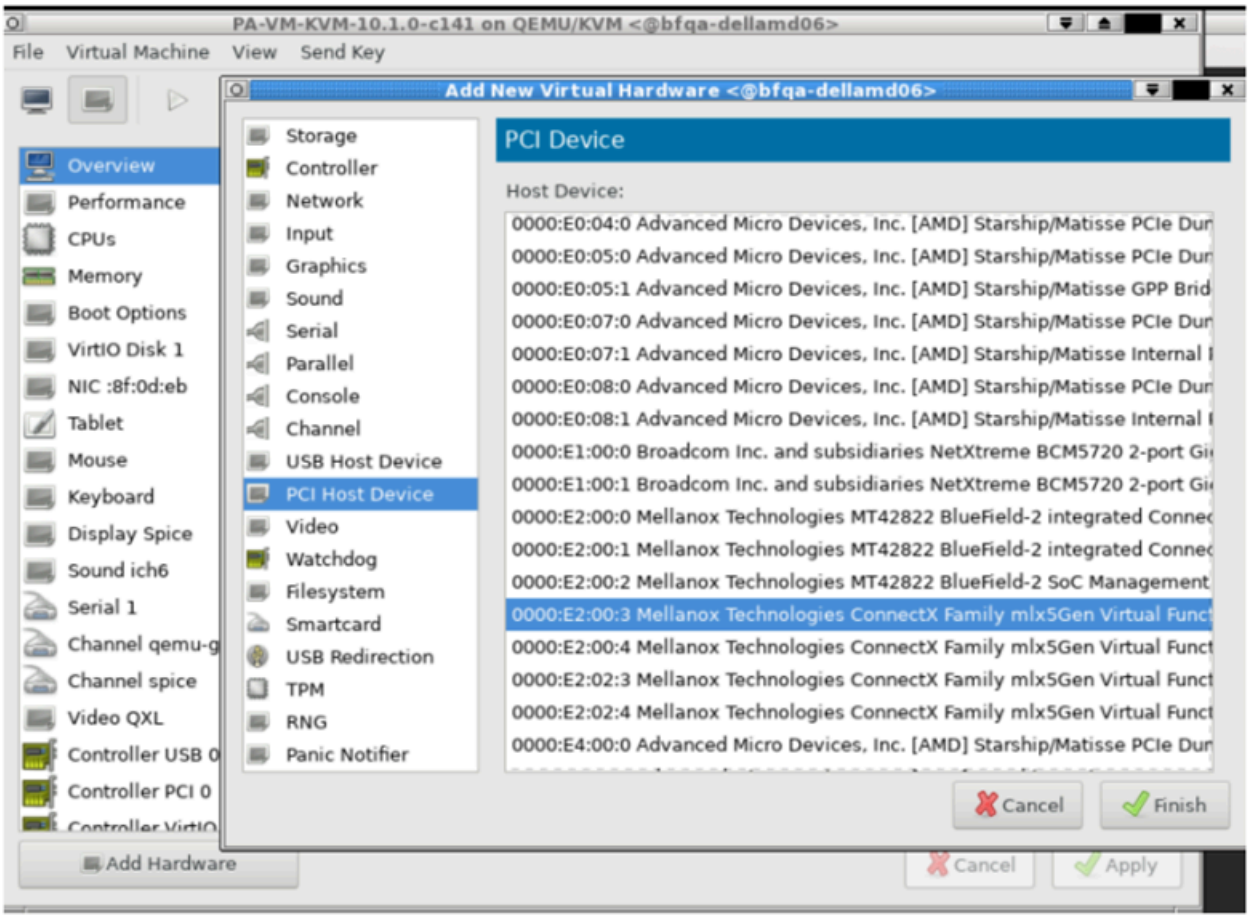
$ echo 2 > **/sys/class/net/enp4s0f1/device/sriov_numvfs**

©2024 Palo Alto Networks, Inc.

STEP 2 | 从 KVM 虚拟机监控程序将 VF 分配给 VM 系列防火墙。

除非将 *VF* 分配给 *VM*，否则来宾 *PAN-OS* 将无法启动。

1. 关闭 VM。
2. 在 KVM 上，使用 virt-manager 将 VF 添加到 VM。
   - 选择 Add Hardware（添加硬件），选择 PF1 的 VF0，然后单击 Finish（完成）。
   - 选择 Add Hardware（添加硬件），选择 PF0 的 VF0，然后单击 Finish（完成）。
   - 选择 Add Hardware（添加硬件），选择 PF0 的 VF1，然后单击 Finish（完成）。



检查 BlueField-2 DPU 系统

在主机上安装 Rshim 驱动程序后，BlueField-2 DPU 首先与主机通信。Rshim 提供一个 tty 接口（可通过 minicom 访问）和一个名为 tmfifo_net0 的网络接口。使用 tmfifo_net0 接口，您可以从主机通过 SSH 连接到 BlueField-2 DPU。Rshim 驱动程序在 x86 虚拟机监控程序操作系统上运行，实际上 OFED 安装默认安装 Rshim 驱动程序。

©2024 Palo Alto Networks, Inc.

STEP 1 | 登录主机。

```
$ ssh user@<host-ip-address>
```

```
$ password:
```

STEP 2 | 如果 Rshim 驱动程序的主机网络接口没有 IP 地址，则必须创建 IP 地址。

```
$ ip addr add dev tmfifo_net0 192.168.100.1/24
```

STEP 3 | 从主机登录 BlueField-2 DPU 子系统。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password: ubuntu
```

如果您是第一次登录，系统会提示您用新密码替换默认密码。

STEP 4 | 更改 BlueField-2 DPU 上的默认密码。

用初始用户名 **ubuntu** 和密码 **ubuntu** 登录 BlueField-2 DPU。

登录后，系统会提示您设置新密码。

```
WARNING:Your password has expired.You must change your password now
 and login again!Changing password for ubuntu.Current password:
 ***** New password: ***** Retype new password: ***** passwd:
 password updated successfully
```

注销并使用新密码登录。

STEP 5 | 检查软件版本。

```
$ ofed_info -s
```

这应该返回以下版本或更高版本：

```
$ MLNX_OFED_LINUX-5.3-0.3.3
```

STEP 6 | 检查 Bluefield 2 DPU 是否处于正确的模式。

正确的模式是嵌入式 CPU 功能所有权模式。有关检查和配置模式的说明，请参阅嵌入式 CPU 功能所有权模式文档。

安装或升级 BlueField 引导流软件

请按照以下步骤操作，以确保您拥有适用于 BlueField-2 DPU 的最新 Bluefield 引导流 (BFB) 软件。BFB 包括 BlueField 操作系统和其他软件，例如驱动程序和网络接口。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 将 BFB 软件包下载到适用于 BlueField-2 DPU 的物理主机。

从 NVIDIA 网站获取在 DPI ARM 核心上运行的操作系统的最新版本驱动程序 — 您必须接受最终用户许可协议才能下载。

STEP 2 | 从物理主机上的 Rshim 引导位置安装 BFB。

请注意，下面的文件名（以 **DOCA** 开头，以 **.bfb** 结尾的字符串）不包含空格。在一行中输入以下命令。

```
$ cat DOCA_v1.0_BlueField_OS_Ubuntu_20.04-5.3-1.0.0.0-3.6.0.11699-1-aarch64.bfb > /dev/rshim0/boot
```

STEP 3 | 登录 BlueField-2 DPU。

使用在检查 BlueField-2 DPU 系统中创建的新密码。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 4 | 在 BlueField-2 DPU 上应用固件升级。

在一行中输入以下命令。

```
$ sudo /opt/mellanox/mlnx-fw-updater/firmware/mlxfwmanager_sriov_dis_aarch64_41686
```

STEP 5 | 重启系统电源。

注销 BlueField-2 DPU 并返回 Linux 主机。

```
$ ipmitool chassis power cycle
```

STEP 6 | 登录 BlueField-2 DPU。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 7 | 在 BlueField-2 DPU 上启动 opof（打开分流）服务。目前，opof 是一项独立服务。

在启动 *opof* 之前，*VF* 必须存在。请参阅启用虚拟功能。

```
$ opof_setup
$ service opof restart
```

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 验证 opof 服务是否正常运行。

```
$ service opof status
```

安装或升级 Debian 软件包

如果 Debian 软件包版本低于 1.0.4，则必须升级。

STEP 1 | 在 BlueField-2 DPU 上，检查 opof 软件包的版本。

```
$ opov-v
```

如果版本低于 1.0.4，则必须升级。

STEP 2 | 为软件包添加 NViIDIA 存储库。

```
$ cd /etc/apt/sources.list.d
```

在一行中输入每个 `wget` 命令。URL 中不能包含任何空格：

```
wget https://linux.mellanox.com/public/repo/doca/1.0/ubuntu20.04/
doca.list
```

```
wget -qO - https://linux.mellanox.com/public/repo/doca/1.0/
ubuntu20.04/aarch64/GPG-KEY-Mellanox.pub | sudo apt-key add -
```

```
$ apt update
```

STEP 3 | 在 BlueField-2 DPU 上，检查存储库中的 Debian 软件包。

```
$ apt search opof
```

```
Sorting...Done Full Text Search...Done opof/now 1.0.4 arm64
 [installed,local] Nvidia Firewall Open Offload Daemon
```

STEP 4 | 在 ARM 上，卸载过时的 Debian 软件包。

```
$ apt remove opof
```

STEP 5 | 安装新的 Debian 软件包。

```
$ apt install opof
```

STEP 6 | 设置并重新启动 opof 服务。

```
$ opof_setup
```

```
$ service opof restart
```

STEP 7 | 验证 opof 服务是否正常运行。

```
$ service opof status
```

 ©2024 Palo Alto Networks, Inc.

运行智能流量分流

此解决方案需要订阅智能流量分流软件和至少 18 个物理核心才能获得最佳性能/吞吐量。默认情况下，PAN-OS 为智能流量分流分配 2 个核心，为管理进程分配 4 个核心，为数据平面处理分配其余 12 个核心。

- 在 VM 系列防火墙上设置智能流量分流
- 在 BlueField-2 DPU 上设置智能流量分流服务
- 启动或重新启动智能流量分流服务
- 获取服务状态和运行状况

在 VM 系列防火墙上设置智能流量分流

按照以下步骤在 PAN-OS 上启用智能流量分流。

STEP 1 | 启动 PAN-OS VM。这假定您已经创建 VM 实例，并且正在重新启动该实例。

```
$ virsh start <vm-name>
```

STEP 2 | 使用 SSH 登录 VM 系列防火墙管理接口。

```
$ ssh admin@<panos-management-IP-address>
```

```
$ admin@PA-VM>
```

STEP 3 | 验证是否已安装并许可智能流量分流。

```
admin@PA-VM> show intelligent-traffic-offload
```

```
Intelligent Traffic Offload:  Configuration             :Enabled
   Operation Enabled        :True   Min number packet        :8
   Min Rate                 :95   TCP ageing                :12-
   UDP ageing               :20
```

`Configuration:Enabled` 表示已许可智能流量分流。

`Operation Enabled:True` 表示已重新启动的配置设备。

STEP 4 | 启用智能流量分流。

使用以下命令启用 ITO，而无需重新启动系统。

```
admin@PA-VM> set session offload yes
```

您还可以使用 **set session offload no** 禁用 ITO，而无需重新启动系统。

©2024 Palo Alto Networks, Inc.

STEP 5 | 验证智能流量分流。

admin@PA-VM> **show session info | match offload**

```
Hardware session offloading:True Hardware UDP session
 offloading:True
```

要查看全局计数器，请使用以下命令：

admin@PA-VM> **show counter global | match flow_offload**

有关输出组织和每个计数器说明的详细信息，请参阅会话计数器。

在 BlueField-2 DPU 上设置智能流量分流服务

必须按照在 VM 系列防火墙上设置智能流量分流中所述构建服务。

STEP 1 | 从主机登录 BlueField-2 DPU 复合体。

$ **ssh ubuntu@192.168.100.2**

```
$ password: ubuntu $ ubuntu> sudo -i
```

STEP 2 | 在 BlueField-2 DPU 操作系统中设置初步配置。

root@bf2SmartNIC:~# **opof_setup**

```
[ INFO ] No num of hugepages specified, use 2048 [ INFO ] No gRPC
 port specified, use pf0vf1 Configure ovs fallback Configure grpc
 for pf0vf1 Reserved 2048*2MB hugepages
```

启动或重新启动智能流量分流服务

如果 ITO 服务在 DPU 上运行，则该服务可能会自动启动。要检查状态，请运行以下命令：

$ service opof status

如果 opof 服务未运行，请输入以下命令启动控制器：

$ service opof start

要重新启动服务，请运行以下命令：

$ service opof restart

获取服务状态和运行状况

使用 opof 获取服务状态和运行状况。每个命令都有自己的命令行帮助，例如：**$ opof -h**

- 查询会话：

  $ opof query -i <session_id>

 ©2024 Palo Alto Networks, Inc.

- 查询服务分流统计信息：

  $ opof stats

Bluefield-2 DPU 故障排除

使用以下步骤重启系统电源。

1. 要重启系统电源，请注销 BlueField-2 DPU 并返回 Linux 主机操作系统。

   $ ipmitool chassis power cycle
2. 如果重启电源后接口没有出现，请登录 BlueField-2 DPU 并输入：

   $ /sbin/mlnx_bf_configure
3. 返回主机操作系统并输入：

   $ sudo /etc/init.d/openibd restart

PAN-OS 故障排除

验证流量

数据流量可以从客户端生成，并通过服务器的智能流量分流设置消耗。IPERF3 可用于生成流量，如运行 IPERF3 测试中所讨论。启动流量后，将流量的前几个数据包发送到 PA-VM，由 PA-VM 决定是否需要分流流量。

必须定义应用程序覆盖策略以识别要分流的流量。TCP 流量在控制数据包上设置 FIN/RST 标记，并将其发送到 PA-VM。当 PA-VM 决定分流流量时，使用 show session all 显示分流的流量。使用 **show session id <flowID>** 提供有关流量状态的信息。分流的流量状态为 `Offload: yes`。

当流量的后续数据包处于分流状态并通过 BlueField-2 DPU 时，流量计数器不会更新。流量完成后，分流服务将触发老化计时器（从 CLI 配置的 TCP 老化）。计时器到期后，服务会收集更新的流量统计信息并将其发送到 VM 系列防火墙。然后，防火墙会更新其流量会话计数器，并且 **show session id <flowID>** 会返回更新的值。

会话计数器

使用以下命令查看会话计数器。

admin@PA-VM > **show counter global | match flow_offload**

每个计数器的输出列为：

计数器名称 | 值 | 速率 | 严重性 | 类别 | 方面 | 说明。

- 值 — 自系统启动以来出现的次数。
- 速率 — 计数器更改的频率。
- 严重性 — 信息、警告、丢弃。用于技术支持。
- 类别 — 流量（会话的一个组成部分）。

 ©2024 Palo Alto Networks, Inc.

- 方面 — 整个流量的分流。

计数器名称	说明
flow_offload_rcv_cpu	分流会话时 CPU 收到的数据包数
flow_offload_session_update	需要更新会话的次数
flow_offload_session_insert	在分流设备中插入的会话数
flow_offload_session_delete	从分流设备中删除的会话数
flow_offload_delete_msg_failed	发送给 GRPC 失败的 del 消息数
flow_offload_add_msg_failed	发送给 GRPC 失败的会话消息数
flow_offload_session_verify	发送给分流设备的验证消息数
flow_offload_verify_msg_failed	发送给 GRPC 失败的验证消息数
flow_offload_update_session_stat	HW 表示流量老化
flow_offload_missing_session_stat	找不到统计信息的会话
flow_offload_invalid_session	分流无效的会话 ID
flow_offload_del_session_fail	分流删除无效的会话
flow_offload_add_session_fail	分流添加会话失败
flow_offload_get_session_fail	分流获取会话失败
flow_offload_grpc_fail	分流 grpc 调用失败
flow_offload_active_session	活动分流会话数
flow_offload_aged_session	老化分流会话数
flow_offload_session	分流会话数

运行 IPERF3 测试

Iperf3 是一个可选的简单应用程序，用于生成可有效运行数据流量测试的流量。要将服务器作为服务运行，请使用 **`iperf3 -s -D`**。默认情况下，应用程序需要 TCP/UDP 目标端口 5201 上的数据包，但可以更改端口。

©2024 Palo Alto Networks, Inc.

- 单流量 — 对于单个 iperf3 流量，请输入：

```
iperf3 -c <server-ip-address> -t 60
```

- 多流量 — 要在 60 秒持续时间内启动 20 个并发流量，请输入：

```
iperf3 -c <ip of server> -P 20 -t 60
```

验证智能流量分流

您可以使用 VM 系列防火墙日志验证防火墙上运行的 ITO 客户端与 BlueField-2 DPU 上的分流服务之间的连接。成功分流的预期日志输出如下。

admin@auto-pavm> **less mp-log pan_grpcd.log**

```
[PD] dec free list 0xe0ff022000 RS LIB INIT in DP! pan_fec_app_init:
 fec_data 0xe0feef1088, maxentries 120 [FEC] enc free list
 0xe0feef1100, dec free list 0xe0feef10b8 Creating dp grpc ring buf
 Initializing dp grpc ring buf Mapping flow data memory Found offload
 parameters Heart beat found 1 Established connection to offload
 device
```

OPOF 故障排除

您还可以查看分流服务日志以验证连接：

root@linux:~# **service opof status**

```
● opof.service - Nvidia Firewall Intelligent Traffic Offload Daemon
 Loaded: loaded (/etc/systemd/system/opof.service; disabled; vendor
 preset: enabled) Active: active (running) since Fri 2021-05-21
 18:40:38 UTC; 3h 48min ago Docs: file:/opt/mellanox/opof/README.md
 Process:163906 ExecStartPre=/usr/sbin/opof_pre_check (code=exited,
 status=0/SUCCESS) Main PID:163922 (nv_opof) Tasks:30 (limit:19085)
 Memory:50.7M CGroup: /system.slice/opof.service └─163922 /
usr/sbin/nv_opof -n 1 -a 0000:03:00.0,representor=[0] -a
 0000:03:00.1,representor=[0] May 21 18:40:38 localhost.localdomain
 nv_opof[163922]:EAL:Probe PCI driver: mlx5_pci (15b3:a2d6)
 device:0000:03:00.0 (socket 0) May 21 18:40:38 localhost.localdomain
 nv_opof[163922]:EAL:Invalid NUMA socket, default to 0 May 21
 18:40:38 localhost.localdomain nv_opof[163922]:EAL:Probe PCI
 driver: mlx5_pci (15b3:a2d6) device:0000:03:00.0 (socket 0) May
 21 18:40:38 localhost.localdomain nv_opof[163922]:EAL:Invalid
 NUMA socket, default to 0 May 21 18:40:38 localhost.localdomain
 nv_opof[163922]:EAL:Probe PCI driver: mlx5_pci (15b3:a2d6)
 device:0000:03:00.1 (socket 0) May 21 18:40:38 localhost.localdomain
 nv_opof[163922]:EAL:Invalid NUMA socket, default to 0 May 21
 18:40:38 localhost.localdomain nv_opof[163922]:EAL:Probe PCI driver:
 mlx5_pci (15b3:a2d6) device:0000:03:00.1 (socket 0) May 21 18:40:39
 localhost.localdomain nv_opof[163922]:EAL:No legacy callbacks,
 legacy socket not created May 21 18:40:39 localhost.localdomain
 nv_opof[163922]:EAL:No legacy callbacks, legacy socket not created
```


©2024 Palo Alto Networks, Inc.

```
May 21 18:40:42 localhost.localdomain nv_opof[163922]:Server
listening on:169.254.33.51:3443
```

日志可显示智能流量分流 `server listening on` IP 地址与 VM 系列防火墙 PA-VM 进行通信，您可以看到 VF 和 DPDK 参数的其他详细信息。此外，还附有添加分流的 TCP 流量的日志。

参考资料

- NVIDIA BlueField 以太网 DPU 用户指南
- NVIDIA BLUEFIELD DPU 系列软件 V3.5.0.11563 文档
- Nvidia DPU 智能流量分流守护进程
- OpenOffload gRPC GITHUB
- PAN-OS 管理员指南

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 Hyper-V 上设置 VM 系列防火墙

VM 系列防火墙可在运行 Microsoft Hyper-V 的服务器上部署。Hyper-V 可作为一个单独的虚拟机监控程序进行打包，也可作为 Windows Server 的插件/角色。

- Hyper-V 上支持的部署
- Hyper-V 上的系统要求
- Linux 集成服务
- 在 Hyper-V 上安装 VM 系列防火墙

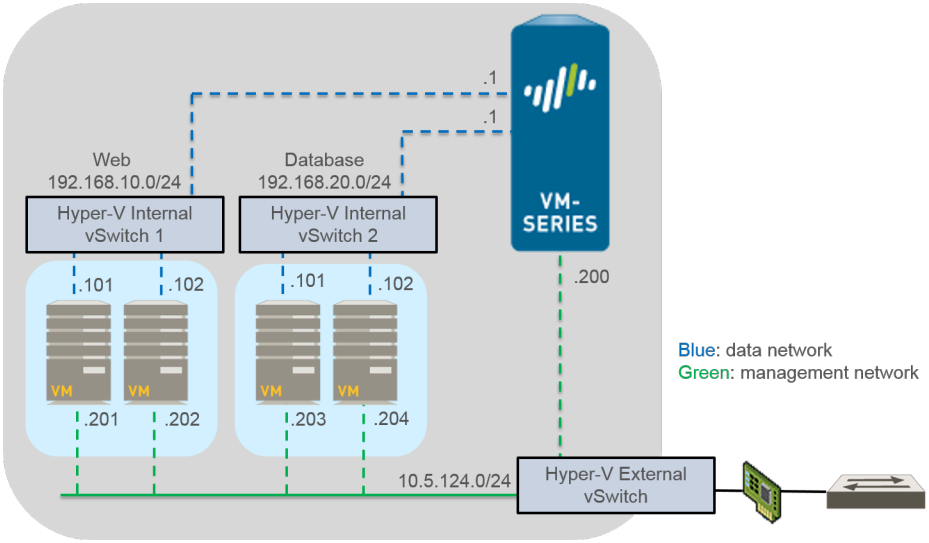
Hyper-V 上支持的部署

您可以在运行 Hyper-V 的主机上部署一个或多个 VM 系列防火墙实例。VM 系列防火墙的具体部署位置取决于您的网络拓扑。VM 系列防火墙支持分接接口、虚拟线路、第 2 层和第 3 层部署模式。

- 保护单个 Hyper-V 主机上的流量
- 保护跨多个 Hyper-V 主机的流量

保护单个 Hyper-V 主机上的流量

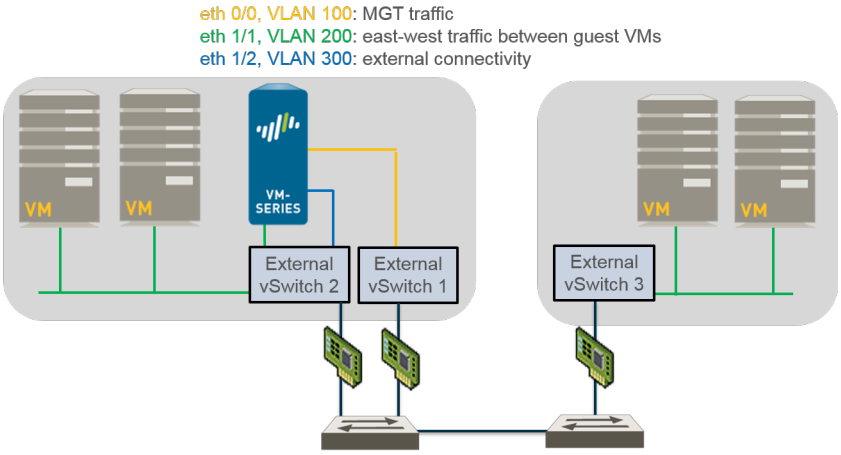
VM 系列防火墙可部署在单个 Hyper-V 主机和其他客户端 VM 上。在下述示例中，VM 系列防火墙拥有一个第 3 层接口，而 VM 系列防火墙和其他客户端 VM 通过 Hyper-V vSwitch 实现连接。Web 服务器和数据库服务器之间的所有流量都会通过防火墙路由。仅通过数据库服务器或仅通过 Web 服务器的流量将由外部 vSwitch 处理，且不会通过防火墙。



保护跨多个 Hyper-V 主机的流量

您可以通过部署 VM 系列防火墙来保护多个 Hyper-V 主机的流量。在下述示例中，VM 系列防火墙采用第 2 层接口模式部署，用以保护进出客户端 VM 的流量。单个 VM 系列防火墙可保护分布在两个 Hyper-V 主机之间的 4 个客户端 VM 之间的流量。VLAN 标记用于逻辑隔离流量并将其定向至防火墙。此外，可通过将管理流量放置在其自身的外部 vSwitch 上的方法将其与其他所有流量解耦。

©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

Hyper-V 上的系统要求

VM 系列防火墙在 Hyper-V 主机上的最低资源分配应确保符合下述要求，以实现最优性能。

- 主机 CPU 必须为带虚拟化扩展的 64 位 x86 Intel 或 AMD CPU。
- 有关 VM 系列型号的最低硬件要求，请参阅 VM 系列系统要求。
- 至少要有两个网络适配器。VM 系列防火墙支持合成网络适配器，此类适配器可提供优于仿真网络适配器的性能。Hyper-V 最多可支持 8 个合成网络适配器。
- 有关支持的 Windows Server 版本，请参阅兼容矩阵。

  Hyper-V Server 未配备原生图形用户界面；所有的配置均通过 PowerShell 完成。但是，可以使用在远程计算机上运行的 Hyper-V 管理器对防火墙进行管理。如果使用 Hyper-V 角色插件，则可以使用 Hyper-V 管理器或 PowerShell 管理防火墙。
- VM 系列防火墙支持 SR-IOV/PCI-Passthrough。

  DPDK 仅支持 *Nvidia/Mellanox(Mlx5) SRIOV* 设备。不支持使用 *SR-IOV* 的中继模式。

©2024 Palo Alto Networks, Inc.

Linux 集成服务

Linux 集成服务 (LIS) 是一个驱动程序和服务包，可用于增强 Hyper-V 上基于 Linlux 的虚拟机的性能。VM 系列防火墙支持以下服务，以改善主机与虚拟机之间的集成：

- 正常关闭 — 允许您通过 Hyper-V 管理接口正常关闭 VM 系列防火墙，而无需登录到客户机。
- **Hyper-V** 管理器的检测信号 — 通过 Hyper-V 管理接口提供客户端 VM 运行状态的检测信号监控。
- 防火墙管理 **IP** 地址的可视性 — 允许您使用 Hyper-V 管理器查看为防火墙上的管理接口而分配的 IP 地址。

©2024 Palo Alto Networks, Inc.

在 Hyper-V 上安装 VM 系列防火墙

您可以按照本节中的说明在 Hpyer-V 主机上部署 VM 系列防火墙。若要下载 VHDX 映像文件并在 Hyper-V 主机上安装 VM 系列防火墙，需要 Palo Alto Networks 支持帐户以及有效的 VM 系列许可证。如果您还没有向您的支持帐户注册功能验证代码（您已在订单履行电子邮件中收到），请参阅注册 VM 系列防火墙。在注册完成后，继续以下任务：

- 准备工作
- 在 Hyper-V 上调整 VM 系列防火墙的性能
- 使用 Hyper-V 管理器在 Hyper-V 主机上设置 VM 系列防火墙
- 使用 PowerShell 在 Hyper-V 主机上设置 VM 系列防火墙
- 在 VM 系列防火墙上执行初始配置

准备工作

在安装和配置 VM 系列防火墙之前，在配置 VM 系列防火墙时根据需要了解并考虑以下各项：

- 虚拟交换机类型
- MAC 地址假冒

虚拟交换机类型

在安装 VM 系列防火墙之前，您必须创建提供外部连接实现管理访问所需的 vSwitch，以及实现将由防火墙提供安全保护的虚拟机进出流量的路由所需的 vSwitch。Hyper-V 允许您创建三种类型的 vSwitch：

- 外部 **vSwitch** — 绑定至物理网络适配器，为 vSwitch 提供物理网络访问。
- 内部 **vSwitch** — 传输虚拟机与 Hyper-V 主机之间的流量。该类 vSwitch 不提供与物理网络的连接。
- 私有 **vSwitch** — 仅传输 Hyper-V 主机上虚拟机之间的流量。

VM 系列防火墙的管理需要使用外部 vSwitch。连接至 VM 系列防火墙的其他 vSwitch 可以是任何类型，具体取决于您的网络拓扑。

MAC 地址假冒

如果您使用第 3 层模式中启用的接口部署 VM 系列防火墙，需确保使用由虚拟机监控程序分配的 MAC 地址，确保虚拟机监控程序和防火墙可以适当地处理数据包。或者，您可以使用 Hyper-V 管理器针对防火墙上的每个数据面板接口启用虚拟网络适配器上的 MAC 地址假冒。有关详细信息，请参阅虚拟机监控程序分配的 MAC 地址。

如果您使用第 2 层模式或虚拟线路模式中启用的接口部署 VM 系列防火墙，则必须针对防火墙上的每个数据面板接口启用 Hyper-V 中虚拟网络适配器上的 MAC 地址假冒。该项设置旨在确保：当源 MAC 地址与出站接口的 MAC 地址不符时，虚拟网络适配器不会丢失由 VM 系列防火墙发送的数据包。

©2024 Palo Alto Networks, Inc.

在 Hyper-V 上调整 VM 系列防火墙的性能

适用于 Hyper-V 的 VM 系列防火墙是一款高性能设备，但可能需要调整虚拟机监控程序才能取得最佳效果。本节介绍了一些有助于实现 VM 系列防火墙最佳性能的最佳实践和建议。

- 禁用虚拟机队列
- 隔离 NUMA 节点中的 CPU 资源

禁用虚拟机队列

Palo Alto Networks 建议禁用 Hyper-V 主机上所有 NIC 的虚拟机队列 (VMQ)。此选项容易出现配置错误，并且在启用时可能导致网络性能下降。

STEP 1 | 登录到 Hyper-V 管理器并选择您的 VM。

STEP 2 | 选择 **Settings**（设置） > **Hardware**（硬件） > **Network Adapter**（网络适配器） > **Hardware Acceleration**（硬件加速）。

STEP 3 | 在虚拟机队列下，取消选择 **Enable virtual machine queue**（启用虚拟机队列）。

STEP 4 | 单击 **Apply**（应用）保存更改，然后单击 **OK**（确定）退出虚拟机设置。

隔离 NUMA 节点中的 CPU 资源

通过将来宾虚拟机的 CPU 资源隔离到单个非统一内存访问 (NUMA) 节点，您可以提高 Hyper-V 的 VM 系列的性能。通过选择，您可以在 Hyper-V 管理器中查看虚拟机的 NUMA 设置 **Settings**（设置） > **Hardware**（硬件） > **Processor**（处理器） > **NUMA**。

使用 Hyper-V 管理器在 Hyper-V 主机上设置 VM 系列防火墙

按照以下说明使用 Hyper-V 管理器在 Hyper-V 上部署 VM 系列防火墙。

STEP 1 | 下载 VHDX 文件。

注册您的 VM 系列防火墙，并获取 VHDX 文件。

1. 转到 https://www.paloaltonetworks.com/services/support。
2. 按 **PAN-OS for VM-Series Base Images**（用于 **VM** 系列基本映像的 **PAN-OS**）进行筛选并下载 VHDX 文件。例如，PA-VM-HPV-7.1.0.vhdx。

STEP 2 | 设置所需的任何 vSwitch。

若要创建一个 vSwitch：

1. 在 Hyper-V 管理器中，选择主机，然后选择 **Action**（操作） > **Virtual Switch Manager**（虚拟交换机管理器），以打开虚拟交换机管理器窗口。
2. 在 **Create virtual switch**（创建虚拟交换机）窗口中，选择 vSwitch 的类型（外部、内部或私有），然后单击 **Create Virtual Switch**（创建虚拟交换机）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 安装防火墙。

1. 在 Hyper-V 管理器中，选择主机，然后选择 **Action**（操作） > **New**（新建） > **Virtual Machine**（虚拟机）。在新建虚拟机向导中配置以下设置：
   1. 为 VM 系列防火墙选择 **Name**（名称）和 **Location**（位置）。VM 系列防火墙会在指定位置存储 VHDX 文件。
   2. 选择 **Generation 1**（第 **1** 代）。该选项为默认选项，也是唯一支持的版本。
   3. 对于 **Startup Memory**（启动内存），根据 VM 系列型号的 VM 系列系统要求分配内存。

      切勿启用动态内存；*VM* 系列防火墙需要静态内存分配。

   4. 配置 **Networking**（网络）。选择一个外部 vSwitch，以连接防火墙上的管理接口。
   5. 若要连接 **Virtual Hard Disk**（虚拟硬盘），选择 **Use an existing virtual hard disk**（使用现有虚拟硬盘），并浏览到您之前下载的 VHDX 文件。
   6. 检查摘要，然后单击 **Finish**（完成）。
2. 为防火墙分配虚拟 CPU。
   1. 选择创建的 VM，然后导航至 **Action**（操作） > **Settings**（设置）。
   2. 选择 **Processor**（处理器），并根据 VM 系列型号的 VM 系列系统要求输入 CPU 的最小数量。
   3. 单击 **OK**（确定）。

STEP 4 | 对于防火墙上的数据面板接口，至少连接一个网络适配器。

1. 选择 **Settings**（设置） > **Hardware**（硬件） > **Add Hardware**（添加硬件），然后选择网络适配器的 **Hardware type**（硬件类型）。

   不支持传统网络适配器和 *SR-IOV*。若选择这两种适配器，防火墙将会以维护模式启动。

2. 单击 **OK**（确定）。

STEP 5 | （可选）如果您未通过虚拟机监控程序分配的 MAC 地址使用第 3 层模式，则启用 Hyper-V 上的 MAC 地址假冒。

1. 双击数据面板虚拟网络适配器，并单击 **Advanced Settings**（高级设置）。
2. 单击 **Enable MAC address spoofing**（启用 **MAC** 地址假冒）复选框，然后单击 **Apply**（运用）。

STEP 6 | 启动防火墙。

从 **Virtual Machines**（虚拟机）列表中选择防火墙，然后导航至 **Action**（操作） > **Start**（启动）以启动防火墙。

©2024 Palo Alto Networks, Inc.

使用 PowerShell 在 Hyper-V 主机上设置 VM 系列防火墙

按照以下说明使用 PowerShell 管理器在 Hyper-V 上部署 VM 系列防火墙。

STEP 1 | 下载 VHDX 文件。

注册您的 VM 系列防火墙，并获取 VHDX 文件。

1. 转到 https://www.paloaltonetworks.com/services/support。
2. 按 **PAN-OS for VM-Series Base Images**（用于 **VM** 系列基本映像的 **PAN-OS**）进行筛选并下载 VHDX 文件。例如，PA-VM-HPV-7.1.0.vhdx。

STEP 2 | 设置所需的任何 vSwitch。

使用以下命令创建 vSwitch。命名 vSwitch 并选择一个交换机类型。

```
> New-VMSwitch -Name <"switch-name"> -SwitchType <switch-type>
```

STEP 3 | 安装 VM 系列防火墙。

1. 创建新的虚拟机并根据 VM 系列型号的 VM 系列系统要求设置内存。

   ```
   > NEW-VM -Name <vm-name> -MemoryStartupBytes 4GB -
   VHDPath <file-path-to-vhdx>
   ```

2. 根据 VM 系列型号的 VM 系列系统要求设置处理器数量。

   ```
   > SET-VMProcessor  -VMName <vm-name>  -Count 2
   ```

STEP 4 | 对于防火墙上的管理接口，至少连接一个网络适配器。

将在 VM 创建过程中创建的默认网络适配器连接到管理 vSwitch。

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-
adapter-name"> -SwitchName <"management-vswitch">
```

STEP 5 | （可选）如果您未通过虚拟机监控程序分配的 MAC 地址使用第 3 层模式，则启用 Hyper-V 上的 MAC 地址假冒。

```
> Set-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-
name"> -MacAddressSpoofing On
```

STEP 6 | 启动防火墙。

例如：

```
> Start-VM -vmname <vm-name>
```


©2024 Palo Alto Networks, Inc.

在 VM 系列防火墙上执行初始配置

使用下述说明对您的 VM 系列防火墙执行初始配置。默认情况下， VM 系列防火墙使用DHCP获取管理接口的IP地址。但是，您可以分配静态 IP 地址。完成初始配置后，访问 Web 界面以完成进一步的配置任务。如果让 Panorama 进行集中管理，有关使用 Panorama 管理设备的信息，请参阅《Panorama 管理员指南》。

如果您正在使用引导来执行 Hyper-V 上 VM 系列防火墙的配置，请参阅在 Hyper-V 上引导 VM 系列防火墙。有关引导的一般信息，请参阅引导 VM 系列防火墙。

STEP 1 | 从网络管理员处收集必要的信息。

- 管理端口 IP 地址
- 子网掩码
- 默认网关
- DNS 服务器 IP 地址

STEP 2 | 访问 VM 系列防火墙的控制台。

1. 在 Hyper-V 管理器中，选择 VM 系列防火墙，然后在操作列表中单击 **Connect**（连接）。
2. 使用默认的用户名和密码登录到防火墙：**admin/admin**
3. 通过运行以下命令进入配置模式：**configure**

STEP 3 | 配置管理接口的网络访问设置。

输入以下命令：

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> 网络掩码 <netmask>
default-gateway <gateway-IP> dns-settingservers primary <DNS-IP>
```

其中 <*Firewall-IP*> 是您想要分配给管理接口的 IP 地址，<*netmask*> 是子网掩码，<*gateway-IP*> 是网关的 IP 地址，<*DNS-IP*> 是 DNS 服务器的 IP 地址。

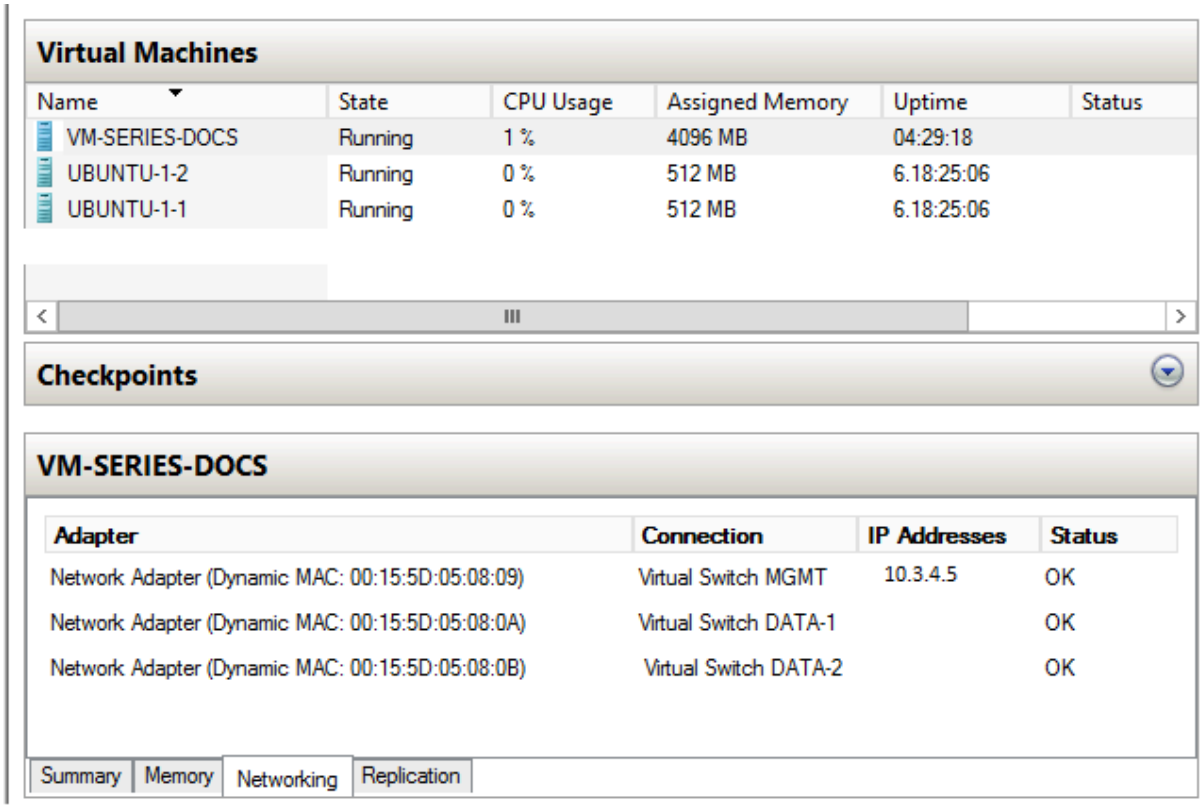
STEP 4 | 提交您所做的更改，并退出配置模式。

1. 输入 **commit**。
2. 输入 **exit**。

©2024 Palo Alto Networks, Inc.

STEP 5 | 验证您可以通过 Hyper-V 管理器查看管理接口 IP 地址。

1. 从 **Virtual Machines**（虚拟机）列表中选择 VM 系列防火墙。
2. 选择 **Networking**（网络）。列表中显示的第一个网络适配器用于防火墙的管理访问；列表中的其他适配器用作防火墙上的数据面板接口。



STEP 6 | 验证防火墙管理所需外部服务（例如 Palo Alto Networks 更新服务器）的网络访问权限。

1. 使用 ping 实用程序验证是否能联网到 Palo Alto Networks 更新服务器，如以下示例所示。验证是否发生 DNS 解析，响应中是否包含更新服务器的 IP 地址；更新服务器不响应 ping 请求。

```
admin@PA-220 > ping host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84)
 bytes of data.From 192.168.1.1 icmp_seq=1 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=2 Destination Host
 Unreachable From 192.168.1.1 icmp_seq=3 Destination Host
```


©2024 Palo Alto Networks, Inc.

```
Unreachable From 192.168.1.1 icmp_seq=4 Destination Host
Unreachable
```

验证 *DNS* 解析后，按 *Ctrl+C* 键以停止 *ping* 请求。

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

```
request support check
```

如果网络畅通，更新服务器响应防火墙的支持状态。

STEP 7 | （可选）验证您的 VM 系列防火墙的 Jumbo 帧配置未超过 Hyper-V 上支持的最大 MTU。

在启用 Jumbo 帧的情况下，VM 系列防火墙的默认 MTU 大小为 9216 字节。不过，Hyper-V 主机上的物理网络适配器所支持的最大 MTU 为 9000 或 9014 字节，具体取决于网络适配器的容量。若要验证 Hyper-V 上的已配置 MTU：

1. 在 Windows Server 2012 R2 中，打开 **Control Panel**（控制面板），然后导航到 **Network and Internet**（网络和 **Internet**）> **Network and Sharing Center**（网络和共享中心）> **View network status and tasks**（查看网络状态和任务）。
2. 单击列表中的网络适配器或虚拟交换机。
3. 单击 **Properties**（属性）。
4. 单击 **Configure**（配置）。
5. 在 Advanced（高级）选项卡上，从列表中选择 **Jumbo Packet**（**Jumbo** 帧数据包）。
6. 从 Value（值）下拉菜单中选择 9000 或 9014 字节。
7. 单击 **OK**（确定）。

如果已在 Hyper-V 上启用 Jumbo 帧，请在 VM 系列防火墙上启用 Jumbo 帧，并将 MTU 大小设置成与 Hyper-V 主机的配置相符。

STEP 8 | 访问 VM 系列防火墙的 Web 接口和配置接口，并定义安全规则和 NAT 规则来安全启用要保护的应用程序。

请参阅《PAN-OS 管理员指南》。

©2024 Palo Alto Networks, Inc.

在 Azure 上设置 VM 系列防火墙

作为 Azure Marketplace 虚拟机，Azure 上的 VM 系列防火墙可提供 Palo Alto Networks 下一代防火墙的安全功能。VM 系列防火墙提供一整套安全功能，确保虚拟机工作负载和数据得到保护。防火墙启用的功能不同于本机安全功能，例如安全组、Web 应用程序防火墙和本机基于端口的防火墙。

在 Azure 上，VM 系列防火墙适用于自带许可证 (BYOL) 模式，或以小时计的即用即付 (PAYG) 模式。借助 Microsoft Azure，您可以通过部署防火墙来保护云中虚拟网络内的工作负载，以便部署公共云解决方案，或通过扩展预置型 IT 基础架构创建混合云解决方案。

- 关于 Azure 上的 VM 系列防火墙
- Azure 上支持的部署
- 从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）
- 从 Azure China Marketplace 部署 VM 系列防火墙（解决方案模板）
- Azure 中的 Panorama 编排部署
- 为 Azure 创建自定义 VM 系列映像
- 使用 Azure 安全中心建议保护您的工作负载
- 在 Azure Stack 中部署 VM 系列防火墙
- 在 VM 系列防火墙上启用 Azure 应用程序见解
- Azure 上的 VM 监控
- 在 Azure 上设置主动/被动 HA
- 使用 ARM 模板部署 VM 系列防火墙
- 部署 VM 系列和 Azure 应用程序网关模板
- 在 Azure 上保护 Kubernetes 服务

关于 Azure 上的 VM 系列防火墙

Azure 上的 VM 系列防火墙必须使用资源管理器部署模式部署在虚拟网络 (Vnet) 中。您可以在标准 Azure 公共云、Azure China 和 Azure Government 上部署 VM 系列防火墙，包括 Azure Government 上的 DoD，用于满足 DoD Impact Level 5 数据和 FedRAMP 高标准的安全要求。

市场上用于 Azure 公共云、Azure Government 和 Azure DoD 区域的 VM 系列防火墙支持自带许可证 (BYOL) 模型和以小时计的即用即付 (PAYG) 选项（基于使用情况的许可）。有关许可证详细信息，请参阅许可证类型 — VM 系列防火墙，并参阅支持的 Azure 区域（可在其中部署 VM 系列防火墙）列表。

对于 Azure China，VM 系列防火墙仅提供 BYOL 选项。有关工作流程，请参阅从 Azure China Marketplace 部署 VM 系列防火墙（解决方案模板）。

此外，还可以在 Azure Stack 中部署 VM 系列防火墙，这是一种您可以用于启用组织数据中心 Azure 服务的 Microsoft 专有云解决方案，您可以通过 Azure Stack 构建混合云解决方案，将您的 Azure 公共部署与您的预置型 Azure Stack 设置统一起来。可以从 Azure Marketplace 下载 VM 系列防火墙 BYOL 产品，并将其提供给 Azure Stack 上的租户。有关说明，请参阅在 Azure Stack上部署 VM 系列防火墙。

- Azure 网络和 VM 系列防火墙
- Azure 安全中心集成
- Azure 上的 VM 系列防火墙模板
- Azure 上对 VM 系列的最低系统要求
- 支持 Azure 上 VM 系列的高可用性

Azure 网络和 VM 系列防火墙

Azure VNet 基础架构不需要虚拟机在各个子网中拥有网络接口。该基础架构包含有内部路由表（称为系统路由），可直接连接 VNet 内的所有虚拟机，以便将流量自动转发至任意子网中的虚拟机。对于不在 VNet 内的目标 IP 地址，在已配置的情况下，流量将发送至默认 Internet 网关或 VPN 网关。为了通过 VM 系列防火墙路由流量，您必须创建用户定义路由 (UDR)，为离开子网的流量指定下一个跃点。此路由将迫使以其他子网为目标的流量进入 VM 系列防火墙，而非使用系统路由直接访问其他子网中的虚拟机。例如，在具备 Web 层和数据库层的双层式应用程序中，您可以设置 UDR，以通过 VM 系列防火墙将来自 Web 子网的流量定向至数据库子网。

在 *Azure* 上，*UDR* 仅适用于离开子网的流量。您不能通过创建用户定义路由来指定流量从 *Internet* 进入子网的方式，或将流量路由至子网内的虚拟机。您可以通过 *UDR* 直接将出站流量流向 *VM* 系列防火墙的接口，始终确保防火墙也能安全地将流量输送到 *Internet*。

有关与 *Microsoft Azure* 相关的文档，请参阅 https://azure.microsoft.com/en-us/documentation/。

©2024 Palo Alto Networks, Inc.

Azure Marketplace 可提供用于部署 VM 系列防火墙的解决方案模板，该模板包含有三个网络接口。要在 Azure 上设置主动/被动 HA，您需要为 HA2 链路添加一个额外的接口。如需自定义上述模板，请使用 GitHub 存储库中提供的 ARM 模板。

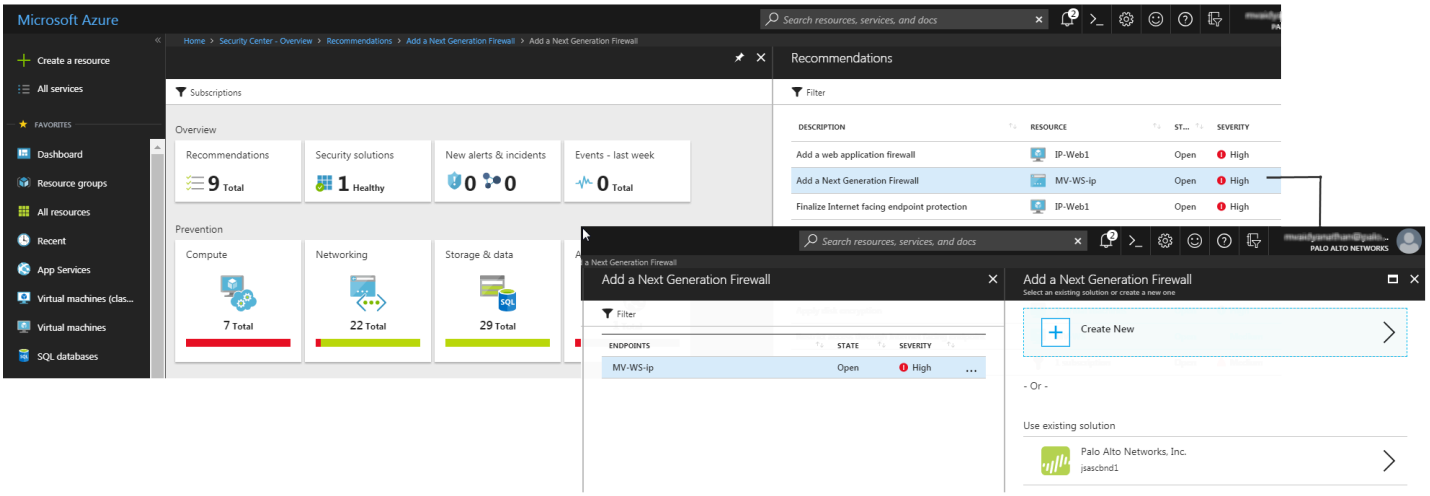
Azure 安全中心集成

Microsoft 已弃用 Azure 安全中心对合作伙伴解决方案的支持，并将其替换为 Azure Sentinel。

VM 系列防火墙与 Azure 安全中心集成，以提供用于监控和警告 Azure 工作负载安全状态的统一视图。在 Azure 安全中心，VM 系列防火墙可以充当合作伙伴安全解决方案，保护您的 Azure 工作负载免受威胁，并缩短公共云中在保护业务和知识产品方面的任何差距。要启用此集成并将日志作为安全警报直接显示在 Azure 安全中心仪表盘上，Azure 上的 VM 系列防火墙应包含一个日志转发配置文件。

首先，您需要启用 Azure 应用程序上的 Azure 安全中心。然后，可通过两种方式启用此集成：

- 根据 **Azure** 安全中心指示板上的建议部署 **VM** 系列防火墙。



当 Azure 安全中心仪表盘建议您部署 VM 系列防火墙来保护暴露于 Internet 的工作负载时，您可以仅在新的资源组或空的现有资源组内部署防火墙。这是因为 Azure 目前限制您在现有资源组内部署多个 NIC 设备。因此，部署 VM 系列防火墙后，必须手动将其配置为位于需要保护的工作负载的流量路径中。

从 Azure 安全中心部署防火墙时，防火墙将通过三个网络接口（管理、面向外部（不信任）和面向内部（信任））启动，还有一个用户定义的路由 (UDR)，用于将所有出站流量从信任子网发送到防火墙上的信任接口，以便防火墙始终检查连接到 Internet 的通信。在使用默认防病毒、防间谍软件和漏洞保护配置文件对流量进行检测后，默认配置可包括两个示例安全策略规则：默认出站规则和默认入站规则。前者允许所有来自可信区域的流量流向应用程序默认端口的不可信区域，而后者允许所有来自不可信区域的 Web 浏览流量流向可信区域。此外，防火墙还将入站或出站规则拦截的所有文件发送至 WildFire 公共云进行分析。两种规则均包含一个 URL 筛选配置文件，可阻止通往 URL 类别侵犯版权、动态 DNS、极端、恶意软件、网络钓鱼

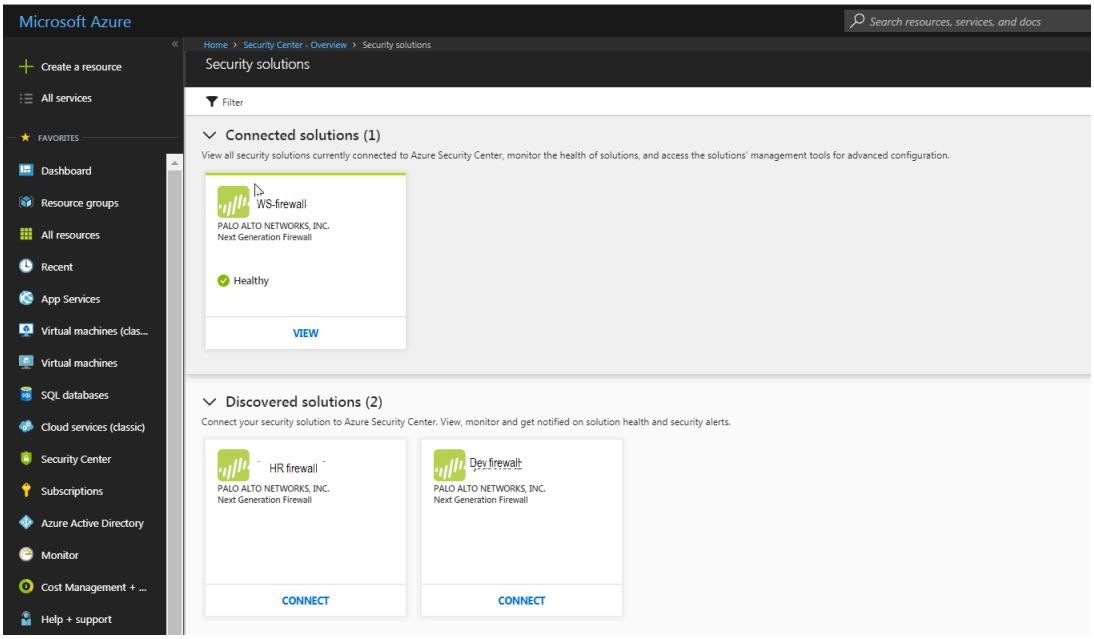
©2024 Palo Alto Networks, Inc.

和未知的所有流量。除了这些安全配置文件外，还启用了两个安全策略规则，以便在会话结束时进行记录，并将威胁和 WildFire 提交日志作为安全警报转发到 Azure 安全中心指示板。

要切实利用此集成，并在要保护的工作负载所在的同一资源组中基于 Azure 安全中心建议部署 VM 系列防火墙，您可以使用公开到 Internet 的公共 IP 地址暂存工作负载。当 Azure 安全中心检测到安全风险时，会触发部署下一代防火墙的建议，然后，您可以在新的资源组内部署 VM 系列防火墙，以便稍后在其中添加工作负载。然后，您必须删除分阶段执行的工作负载，以触发建议。

- 选择已部署用于保护工作负载安全的 **VM** 系列防火墙。如果拥有 Azure 安全中心订阅标准层，Azure 安全中心会发现从 Azure Marketplace 部署或是采用 Azure CLI、PowerShell 或 ARM 模板自定义部署的所有现有 VM 系列防火墙，并予以显示。Azure 订阅中的防火墙分组在 Azure 安全中心指示板上的安全解决方案下。

  Microsoft Azure 不支持使用免费套餐订阅发现现有防火墙。



要从 Azure 安全中心连接现有 VM 系列防火墙，必须设置 Linux 虚拟机并配置 Syslog 转发，才能将通用事件格式的防火墙日志作为警报转发到 Azure 安全中心。通过其他配置可启用监控所有 Azure 资产的单一平台视图。

转发大量日志到 *Azure* 安全中心可能会导致额外的订阅成本。

Azure 上的 VM 系列防火墙模板

您可以使用模板在 Azure 上部署 VM 系列防火墙。Palo Alto Networks 提供两种模板：解决方案模板和 ARM 模板。

- **Solution Templates in the Azure Marketplace**（**Azure Marketplace** 中的解决方案模板）— 借助 Azure Marketplace 提供的此种解决方案模板，您可以使用 Azure 门户来部署 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

您可以使用已有的资源组和存储帐户（或新建资源组和存储帐户）来为所有区域（Azure China 除外）部署具备以下默认设置的 VM 系列防火墙：

- VNet CIDR 10.8.0.0/16；您可以将 CIDR 自定义为不同的专用 IP 地址范围。
- 3 个子网 — 10.8.0.0/24（管理）、10.8.1.0/24（不可信）、10.8.2.0/24（可信）
- 3 个网络接口（每个子网各一个）。如果自定义 VNet CIDR，子网范围会映射到所作更改。

要使用解决方案模板，请参阅从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板），对于 Azure China，请参阅从 Azure China Marketplace 部署 VM 系列防火墙（解决方案模板）。

- **ARM Templates in the GitHub Repository**（GitHub 存储库中的 ARM 模板）— 除基于 Marketplace 的部署之外，Palo Alto Networks 还在 GitHub 存储库中提供 Azure Resource Manager 模板，用以简化在 Azure 上部署 VM 系列防火墙的流程。
  - 使用 ARM 模板部署 VM 系列防火墙— 基本 ARM 模板包含有两个 JSON 文件（一个 Template 文件，一个 Parameters 文件），用以帮助您部署防火墙，并通过单一协调运作提供 VNet 内的所有资源。这些模板“按原样尽最大努力”提供，支持策略。

    如果要使用 *Azure CLI* 定位 *Palo Alto Networks* 提供的所有映像，您需要以下详细信息来完成此命令（显示 *vm-image* 列表）：
    - 发行商：*paloaltonetworks*
    - 产品：*vmseries-flex*
    - *SKU*：*byol*、套餐 *1*、套餐 *2*
    - 版本：*10.0.0* 或最新版本
  - 部署 VM 系列和 Azure 应用程序网关模板以支持横向扩展安全体系结构，该体系结构可在一对（外部和内部）Azure 负载均衡器 VM 系列和 Azure 应用程序网关之间使用两个 VM 系列防火墙来保护面向 Internet 的 Web 应用程序。此模板目前不适用于 Azure China。
  - 使用 ARM 模板将 VM 系列防火墙部署到现有资源组，例如，当您想要在 Azure 上设置主动/被动 HA时。

除 Palo Alto Networks 官方支持政策覆盖的上述 ARM 模板外，Palo Alto Networks 还在 Palo Alto Networks GitHub 存储库中提供社区支持模板，从而搜索可用解决方案以快速启动 Azure 上的云自动化和扩展。

Azure 上对 VM 系列的最低系统要求

您只能在 Azure 资源管理器 (ARM) 模式下部署 VM 系列防火墙；不支持经典模式（基于服务管理的部署）。Azure 上的 VM 系列防火墙必须满足以下要求：

- 以下类型的 Azure Linux VM — 支持的型号。

  这些类型包括对加速网络 (SR-IOV) 的支持。

©2024 Palo Alto Networks, Inc.

- 有关部署 VM 系列防火墙所需的内存、磁盘和 CPU 内核，请参阅 VM 系列系统要求。

  出于日志记录用途，您最多可以额外添加 40GB 至 8TB 的磁盘空间。如果可用，VM 系列防火墙会使用 Azure 托管磁盘；它不使用 Azure 为某些实例类型提供的临时磁盘。
- 最多八个网络接口 (NIC)。一个主接口用于管理访问，最多七个接口用于数据流量。

  在 Azure 上，由于虚拟机不需要各子网中设有网络接口，您可以设置三个网络接口（一个用于管理流量，另外两个用于数据面流量）的 VM 系列防火墙。要在防火墙上创建基于区域的策略规则，除管理接口外，您还需要至少两个数据面板接口，以便将一个数据面板接口分配给可信区域，另一个分配给不可信区域。对于 HA 部署，HA 对等之间的 HA2 链路需要另一个接口。

  由于 Azure VNet 属于第 3 层网络，所以 Azure 上的 VM 系列防火墙只支持第 3 层接口。

支持 Azure 上 VM 系列的高可用性

为了确保可用性，您可以使用会话同步或使用扩展架构在传统配置中在 Azure 上设置主动/被动 HA。该扩展架构使用云端本地负载均衡器（例如 Azure 应用网关或 Azure 负载均衡器）横向扩展架构将流量分配到一组健康的防火墙实例中。有关详细信息，请参阅 部署 VM 系列和 Azure 应用程序网关模板。

VM 系列在 Azure 上的服务主体权限

为了使 Panorama 与 Azure API 进行交互并收集有关工作负载的信息，您需要创建 Azure Active Directory 应用程序和服务主体，该主体具有使用 Azure AD 进行身份验证并访问订阅中的资源所需的权限。

要创建 Active Directory 应用程序和服务主体，请按照如何：使用门户创建可以访问资源的 Azure AD 应用程序和服务主体中的说明执行操作。在应用程序生成过程中，执行某个步骤以“将应用程序分配给角色”，并将“读取者”的 IAM 角色分配给应用程序。

如果您没有创建并注册 AD 应用程序所需的权限，请要求 AD 或订阅管理员创建服务主体。

注册应用程序后，记录以下值，以便稍后可以在适用于 Azure 的 Panorama 插件中输入：

- 应用程序 ID
- 密钥（在创建密钥时记录；一旦离开页面，该密钥将不可见）。
- 租户 ID

权限

下表列出了所需的最低内置角色和精细权限（如果要自定义角色）。

要支持	权限
Azure 高可用性	请参阅在 Azure 上设置主动/被动 HA。

©2024 Palo Alto Networks, Inc.

要支持	权限
Azure Application Insights 在 VM 系列防火墙上启用 Azure Application Insights	“Microsoft.Authorization/*/read”, “Microsoft.Network/networkInterfaces/*”, “Microsoft.Network/networkSecurityGroups/*”, “Microsoft.Network/virtualNetworks/*”, “Microsoft.Compute/virtualMachines/read”
Azure 监控 在 Panorama 上设置用于监控的 Azure 插件	对于服务主体，要求最低角色为 **Reader**（读取者）。或者，你可以添加以下自定义权限： “Microsoft.Compute/virtualMachines/read”、 “Microsoft.Network/networkInterfaces/read”、 “Microsoft.Network/virtualNetworks/read”、 “Microsoft.Network/virtualNetworks/subnets/read”、 “Microsoft.Network/applicationGateways/read”、 “Microsoft.Network/locations/serviceTags/read”、 "Microsoft.Network/loadBalancers/read"、 "Microsoft.Network/publicIPAddresses/read"、 "Microsoft.Resources/subscriptions/resourcegroups/read"
Panorama 编排部署 创建自定义角色并将其与 Active Directory 关联	“Microsoft.Resources/subscriptions/resourcegroups/*”, “Microsoft.Resources/deployments/write”, “Microsoft.Resources/deployments/operationStatuses/read”, “Microsoft.Resources/deployments/read”, “Microsoft.Resources/deployments/delete”
	"Microsoft.Network/publicIPPrefixes/write", "Microsoft.Network/publicIPPrefixes/read", "Microsoft.Network/publicIPPrefixes/delete", "Microsoft.Network/publicIPAddresses/write",

©2024 Palo Alto Networks, Inc.

要支持	权限
	"Microsoft.Network/publicIPAddresses/read", "Microsoft.Network/publicIPAddresses/delete", "Microsoft.Network/publicIPAddresses/join/action",
	"Microsoft.Network/natGateways/write", "Microsoft.Network/natGateways/read", "Microsoft.Network/natGateways/delete", "Microsoft.Network/natGateways/join/action",
	"Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/delete", "Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/delete", "Microsoft.Network/virtualNetworks/subnets/join/action",
	"Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
	"Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Network/networkSecurityGroups/join/action",
	"Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/probes/join/action",

©2024 Palo Alto Networks, Inc.

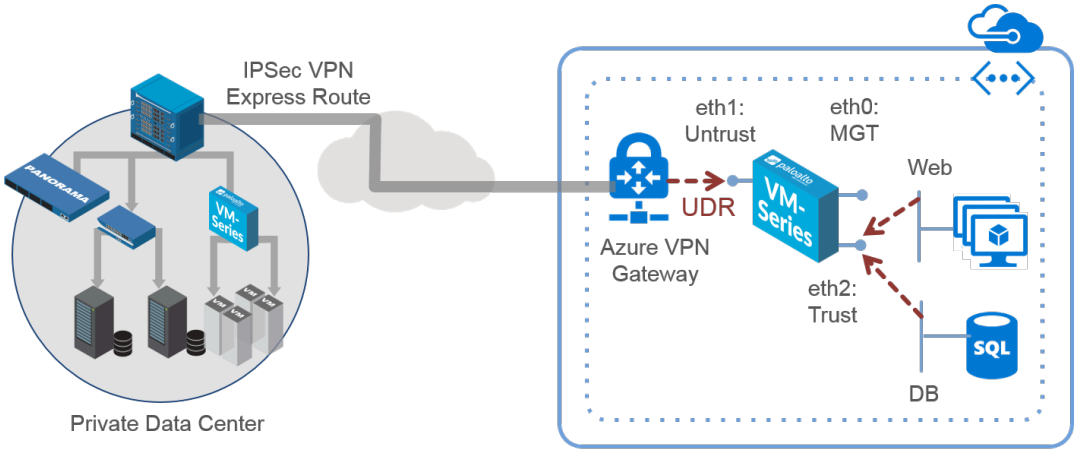
要支持	权限
	"Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
	"Microsoft.Network/locations/serviceTags/read",
	"Microsoft.Network/applicationGateways/read", "Microsoft.Network/networkInterfaces/read",
	"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Compute/virtualMachineScaleSets/read", "Microsoft.Compute/virtualMachineScaleSets/delete", "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
	"Microsoft.Compute/virtualMachines/read",
	"Microsoft.Compute/images/read",
	"Microsoft.insights/components/write", "Microsoft.insights/components/read", "Microsoft.insights/components/delete",
	"Microsoft.insights/autoscalesettings/write"

©2024 Palo Alto Networks, Inc.

Azure 上支持的部署

使用 Azure 上的 VM 系列防火墙保护以下场景中网络用户：

- **Hybrid and VNet to VNet** — 借助 Azure 上的 VM 系列防火墙，您可以安全地使用 IPSec 和 ExpressRoute 将物理数据中心/私有云扩展到 Azure 上。如果已对网络进行分段并在各个 VNet 中部署了工作负载，您可以利用允许应用程序流量的 IPSec 隧道和策略来保护在各个 VNet 之间流动的流量，从而提高数据中心安全。



- **Inter-Subnet** — 此 VM 系列防火墙可位于 VNet 中服务器的上游，并保护多层架构中应用程序之间子网间流量免于遭受横向威胁。
- **Gateway** — 此 VM 系列防火墙可作为 VNet 网关保护 Azure 虚拟网络 (VNet)中面向 Internet 的部署。此 VM 系列防火墙可保护以 VNet 中服务器为目标的流量，还可保护多层架构中应用程序之间子网间流量免于遭受横向威胁。
- **GlobalProtect** — 支持使用 Azure 基础架构快速、简便地将 VM 系列防火墙部署为 GlobalProtect™，并将网关安全策略扩展到远程用户和设备，不论位置如何。

您可以继续从 Azure Marketplace（解决方案模板）部署 VM 系列防火墙，在 Azure 堆栈上部署 VM 系列防火墙或在 Azure 中编排 VM 系列防火墙部署。

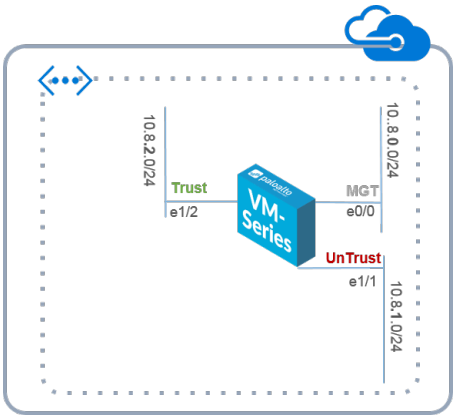
您还可以了解有关用于部署防火墙的 Azure 上的 VM 系列防火墙模板的更多信息。

有关引导的更多信息，请参阅在 Azure 上引导 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）

以下说明展示如何部署 Azure® Marketplace 和 Azure Government Marketplace 中提供的 VM 系列防火墙解决方案模板。要使用 GitHub 存储库中提供的自定义 Azure Resource Manager (ARM) 模板，请参阅使用 ARM 模板部署 VM 系列防火墙。



All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 设置 Azure 帐户。

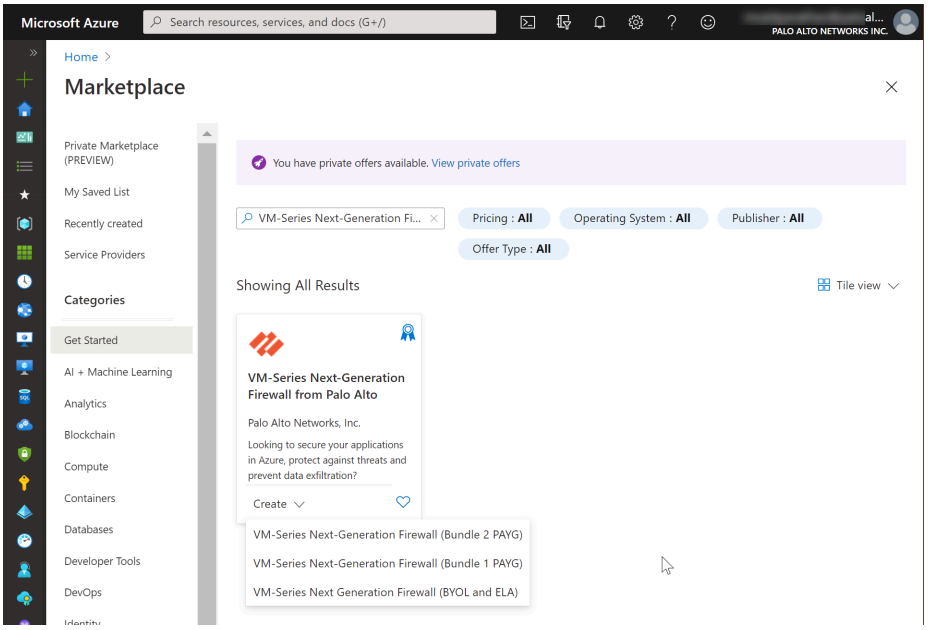
1. 如果还没有帐户，请创建一个 Microsoft® 帐户。
2. 使用 Microsoft 帐户凭据登录到 Azure 门户 (**`https://portal.azure.com`** 或 **`https://portal.azure.us`**)。

   如果正在使用试订，您可能需要打开一个支持请求（***Help + Support***（帮助 + 支持） > ***New Support Request***（新建支持请求））以增加已分配 *VM* 核心的配额。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在 Azure Marketplace 中找到 VM 系列解决方案模板。

1. 选择 **Marketplace** > **Virtual Machines**（虚拟机）。
2. 搜索 Palo Alto Networks®，将显示 VM 系列防火墙的产品列表。对于自带许可证 (BYOL) 和即用即付 (PAYG) 模式的区别，请参阅 面向公共云的 VM 系列防火墙许可证。



3. 选择产品以 **Create**（创建）新的 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 3 | 部署防火墙。

1. 配置防火墙的基本设置。
   1. 选择所需的 Azure **Subscription**（订阅）。
   2. 创建新资源组，或选择空的现有资源组。此资源组将用于存放与此部署中的 VM 系列防火墙相关联的所有资源。

      Azure 已删除此选项，以选择用于启动多个网络结构控制器 *(NIC)* 的 *Marketplace* 解决方案的现有资源组。要将防火墙部署到现有资源组中，请使用 GitHub 存储库中的 *ARM* 模板或您自己的自定义 *ARM* 模板。
   3. 选择您在其中部署防火墙的 Azure **Region**（地区）。
   4. 输入防火墙管理员的 **Username**（用户名）。
   5. 选择 **Authentication type**（身份验证类型）— 密码或 SSH 公钥。

      如果您计划在 *FIPS-CC* 操作模式下使用防火墙，则必须启用 *SSH* 密钥身份验证。尽管您可以使用用户名和密码部署 *VM* 系列防火墙，但在将操作模式更改为 *FIPS-CC* 后，就无法使用用户名和密码进行身份验证。重置为 *FIPS-CC* 模式后，必须使用 *SSH* 密钥登录，然后才可以配置随后将用于登录到防火墙 *Web* 界面的用户名和密码。有关创建 *SSH* 密钥的详细信息，请参阅 Azure 文档。
   6. 输入 **Password**（密码）（不超过 31 个字符）或复制粘贴 **SSH public key**（**SSH** 公钥）以确保对防火墙进行管理访问的安全。
2. 配置网络。
   1. 选择现有 Azure 虚拟网络 (VNet) 或创建新的虚拟网络，并输入 VNet 的 IP 地址。无类域间路由 (CIDR) 的默认 IP 地址为 10.8.0.0/16。
   2. 配置网络接口的子网。

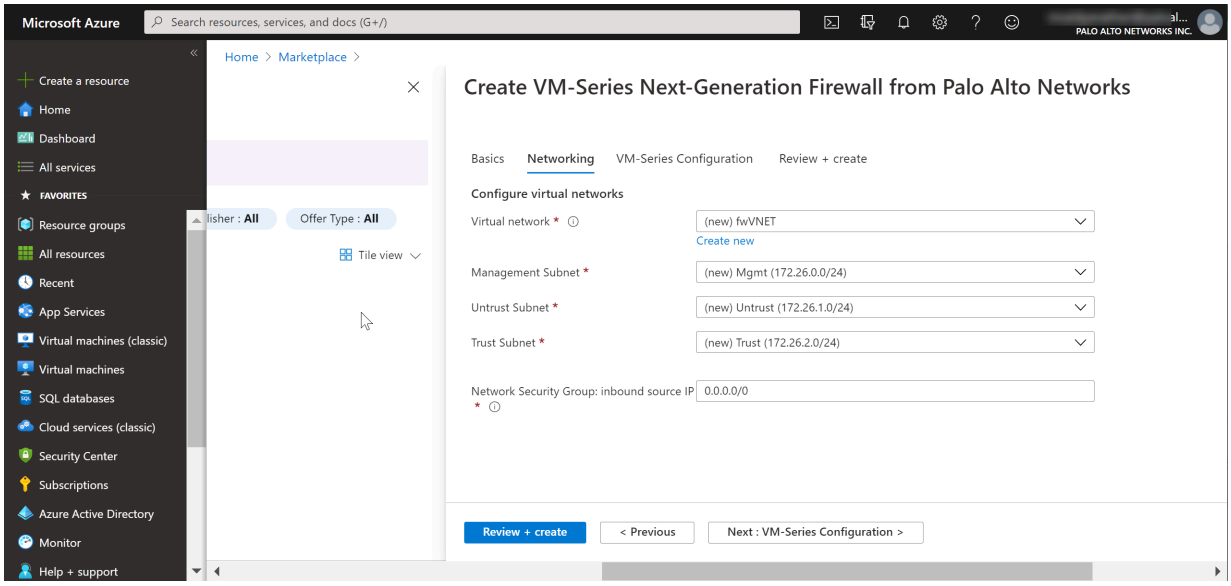
      如果使用默认子网，则必须检查配置。如果使用现有 VNet，则必须设置三个子网，分别用于管理、可信和不可信接口。如果您创建新的 VNet，请检验或更改每个子网的前

©2024 Palo Alto Networks, Inc.

缀。管理子网的默认子网为 10.8.0.0/24，不可信子网的默认子网为 10.8.1.0/24，可信子网的默认子网为 10.8.2.0/24。

3. 输入能够访问 VNet 的源 IP 地址或 IP 范围（包括 CIDR 块）。**Network Security Group: inbound source IP**（网络安全组：入站源 **IP**）让您能够限制 Azure VNet 的入站访问。

   限制对防火墙的访问。确保提供与专用管理 *IP* 地址或网络相对应的 *CIDR* 块。不要将允许的源网络范围设置得比所需的大，并且不要将允许的源配置为 *0.0.0.0/0*。在将其配置到模板上之前验证您的 *IP* 地址，以确保您不会锁定自己。



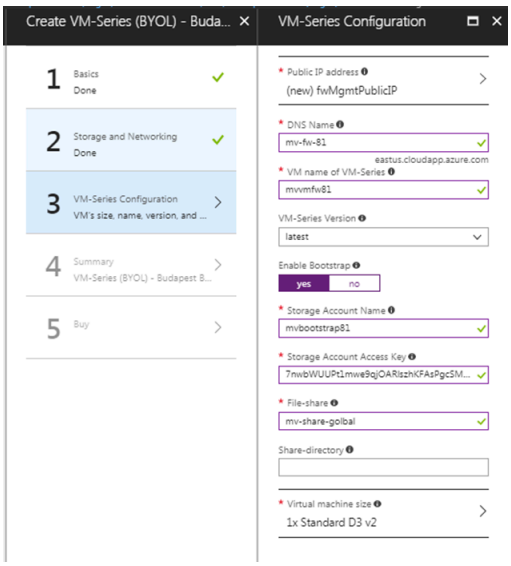
3. 定义防火墙管理访问。

   1. 使用默认变量（新变量 wMgmtPublicIP）将 **Public IP address**（公共 **IP** 地址）分配给防火墙的管理接口 (`eth0`)。

      管理界面不支持 *Azure* 加速网络。

   2. 输入前缀，以使用 DNS 名称访问防火墙。您必须将输入的前缀与屏幕上显示的后缀相组合，以便访问防火墙的 Web 界面。例如：***<yourname><your-region>*.cloudapp.azure.com**
   3. 选择最新的 **VM-Series Version**（**VM** 系列版本）。
   4. 输入显示名称，以识别资源组内的 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

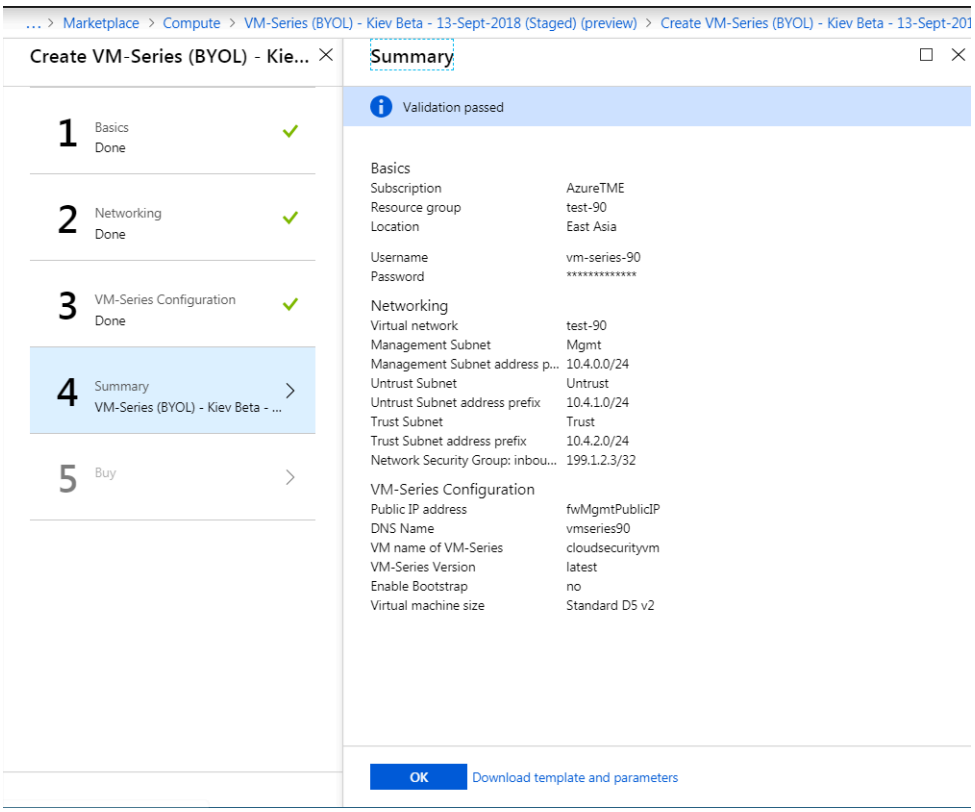


4. 添加信息以在启动时配置防火墙。请参阅在 Azure 上引导 VM 系列防火墙。

   1. 选择 **yes**（是）以 **Enable Bootstrap**（启动应用）。
   2. 输入包含 引导数据包 的 **Storage Account Name**（存储帐户名称）。
   3. 输入 **Storage Account Access Key**（存储帐户访问密钥）。防火墙需要此访问密钥以对存储帐户进行身份验证，并访问其中的文件。
   4. 添加已上传且用于引导防火墙所需的文件的**File share name**（文件共享名称）。存储帐户必须与防火墙部署在同一区域，必须具有正确的引导用文件夹结构。
   5. 根据您的需求，选择 Azure 虚拟机层和规模。使用 **Change size**（更改大小）链接查看支持的实例类型，并检查 Azure 上 VM 系列的最低系统要求。

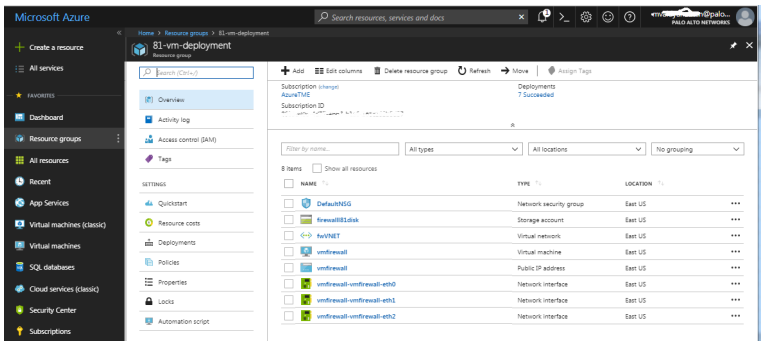
5. 查看摘要，然后单击 **OK**（确定）。然后，接受使用条款和隐私政策，并 **Create**（创建）以启动防火墙。

©2024 Palo Alto Networks, Inc.



6. 确认您已成功部署 VM 系列防火墙。

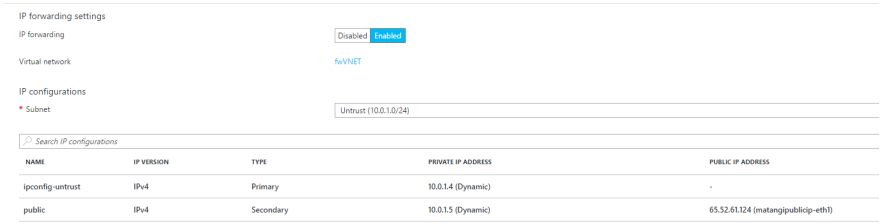
   1. 选择 **Dashboard**（仪表盘）> **Resource Groups**（资源组），然后选择资源组。
   2. 关于已成功部署的资源的详细信息状态，请选择您的资源组，并查看 **Overview**（概述）。



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 为 VM 系列防火墙的不可信接口附加一个公共IP地址。当您创建一个新的公共 IP 地址时，您可以从 Microsoft 拥有的 IP 地址块中获得一个，所以您不能选择一个特定的 IP 地址。您可以分配给接口的最大公共 IP 地址数量取决于您的 Azure 订阅。

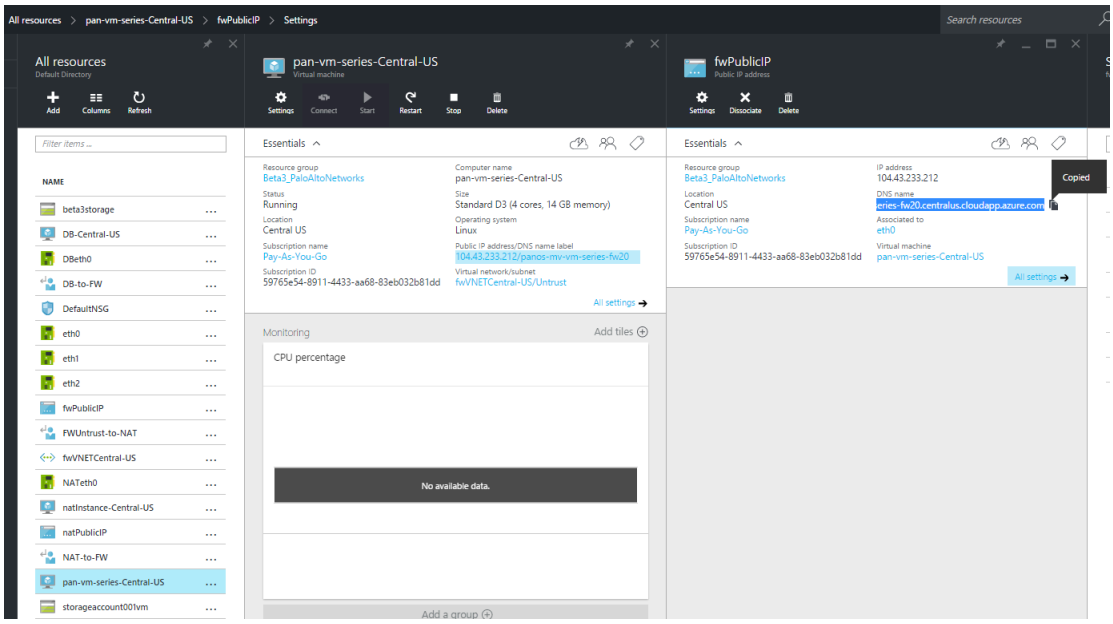
1. 在 Azure 门户上，选择要为其添加公共 IP 地址的网络接口（例如 **eth1**接口）。
2. 选择 **IP Configurations**（**IP** 配置）> **Add**（添加），并为公共 IP 地址选择 **Enabled**（启用）。创建一个新的公共 IP 地址或选择一个可用的 IP 地址。
3. 验证您是否可以查看与该接口关联的辅助 IP 地址。



将辅助 *IP* 地址附加到网络接口时，*VM* 系列防火墙不会自动获取分配给该接口的专用*IP*地址。您将需要使用 *VM* 系列防火墙 *Web* 界面手动配置专用 *IP* 地址。请参阅配置数据面板网络接口作为防火墙上的第 3 层接口。

STEP 5 | 登录防火墙的 Web 界面。

1. 在 Azure 门户的 **All Resources**（所有资源）中，选择 VM 系列防火墙并查看防火墙的完整 DNS 名称。



1. 使用 Web 浏览器提供的安全连接 (https) 登录到防火墙的 DNS 名称。
2. 输入您在 parameters 文件中定义的用户名密码。您将看到证书警告，但这是正常现象，请继续前往网页。

©2024 Palo Alto Networks, Inc.

STEP 6 | 在 VM 系列防火墙上激活许可证。

对于 **BYOL** 版本

1. 创建支持帐户。
2. 注册 VM 系列防火墙（使用授权代码）。
3. 在防火墙 Web 界面上，选择 **Device**（设备） > **Licenses**（许可证），然后选择 **Activate feature using authentication code**（使用授权代码激活功能）。
4. 输入在支持门户上注册的容量授权代码 (*auth-code*)。防火墙将连接到更新服务器 (`updates.paloaltonetworks.com`)，并下载许可证，然后自动重新启动。
5. 返回登录到 Web 界面，然后在 **Dashboard**（仪表盘）上确认以下各项：
   - 有效序列号显示于 **Serial#**（序列号）中。

     如果显示 `Unknown`一词，则表示此设备未经许可。要查看防火墙上的流量日志，您必须安装有效的容量许可证。
   - **VM Mode**（**VM** 模式）显示为 Microsoft Azure。

对于 **PAYG** 版本

1. 创建支持帐户。
2. 面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。

STEP 7 | 配置数据面板网络接口作为防火墙上的第 3 层接口。

如果您在一台服务器上托管多个具有不同IP地址和SSL证书的网站或服务，则可能需要在 VM 系列防火墙接口上配置多个IP地址。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
2. 单击 **ethernet 1/1** 并按如下所述配置：
   - 设置 **Interface Type**（接口类型）为**Layer3**（第三层）（默认）。
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 此外，在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义名为 **`UnTrust`** 的新区域，然后单击 **OK**（确定）。
   - 如果您打算在接口上仅分配一个 IP 地址，请在 **IPv4** 选项卡中选择 **DHCP Client**（**DHCP** 客户端）— 防火墙将自动获取在 ARM 模板中分配的专用 IP 地址。如

©2024 Palo Alto Networks, Inc.

果您打算分配多个 IP 地址，请选择 **Static**（静态）并手动输入分配给 Azure 门户上接口的主要 IP 地址和辅助 IP 地址。

- 禁用（取消选择） **Automatically create default route to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由），确保此接口处理的流量不会直接流向 VNet 的默认网关。

3. 单击 **ethernet 1/2** 并按如下所述配置：
   - 设置 **Interface Type**（接口类型）为**Layer3**（第三层）（默认）。
   - 将 **Security Zone**（安全区域）设置为 **Trust**（可信）。
   - 设置 **IP address**（**IP** 地址）**DHCP Client**（**DHCP** 客户端）或 **Static**（静态）。
   - 禁用（取消选择）**Automatically create default route to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由），确保此接口处理的流量不会直接流向 VNet 的默认网关。
4. **Commit**（提交）更改，并确认接口链路状态为 up（工作中）。
5. 在防火墙需要路由的任何网络的 VM 系列防火墙虚拟路由器上添加静态路由。

   例如，要添加默认路由到防火墙保护的服务器的目标子网：
   - 选择 **Network**（网络） > **Virtual Router**（虚拟路由器） > **default**（默认） >
   - 选择 **Static Routes**（静态路由） > **IPv4**，并为目标服务器添加下一个跃点 IP 地址。您可以设置 x.x.x.1 为所有流量的下一个跃点 IP 地址（从接口 ethernet1/1 发往 0.0.0.0/0）。

STEP 8 | 为特定部署配置防火墙。

- 网关 — 在不可信区域上游部署第三方负载均衡器。
- **Hybrid** 和 **Inter-VNet** — 在不可信区域上游部署 Azure VPN 网关或 NAT 虚拟机。
- **Inter-Subnet** — 在 VM 系列防火墙上，添加区域之间的安全策略规则以允许基于附加到可信接口的子网流量。
- **GlobalProtect™** — 在不可信区域上游部署 NAT 虚拟机。

STEP 9 | 将流量定向到 VM 系列防火墙。

1. 为确保 VM 系列防火墙保护 Azure 资源组内的所有流量，请在防火墙上配置静态路由。
2. 配置用户定义路由以通过 VM 系列防火墙上的接口定向所有流量。请参阅有关 UDR 的 Azure 文档了解详细信息。

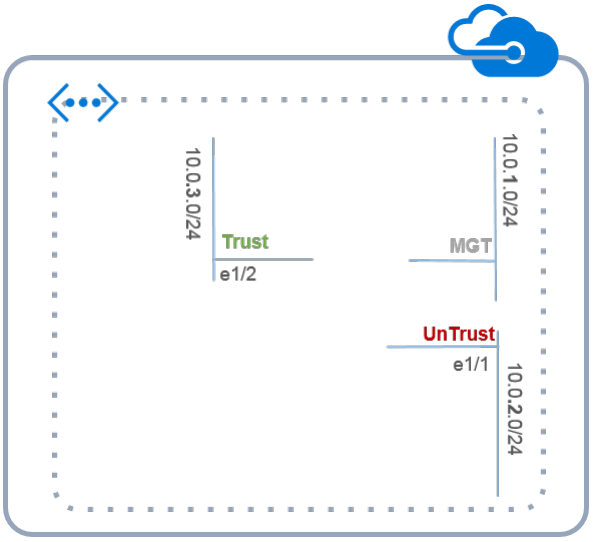
   内部子网上的用户定义路由必须发送通过可信接口的所有流量。不可信侧的用户定义路由将定向通过 VM 系列防火墙上不可信接口的 所有 Internet 流量。Internet 发出的流量可能来自 Azure 应用程序网关或 Azure 负载均衡器，或在采用混合部署连接预置型网络与 Azure 云的情况下，此流量也可能来自 Azure VPN 网关。

STEP 10 | 要发布 PAN-OS® 指标到 Azure Application Insights，请参阅在 VM 系列防火墙上启用 Azure Application Insights。

 ©2024 Palo Alto Networks, Inc.

从 Azure China Marketplace 部署 VM 系列防火墙（解决方案模板）

以下说明将向您展示如何部署 Azure China Marketplace 中提供的 VM 系列防火墙解决方案模板。Azure China Marketplace仅支持 VM 系列防火墙的BYOL模型。您可以将防火墙部署到空的现有资源组或新的资源组中。模板中的默认VNet是10.0.0.0/16，并且它部署了一个 VM 系列防火墙，它具有3个网络接口，一个管理接口和两个数据平面接口，如下所示。要使用GitHub存储库中可用的可定制ARM模板，请参阅 使用ARM模板部署 VM 系列防火墙。



All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 设置 Azure 帐户。

1. 创建 Microsoft 帐户。
2. 使用 Microsoft 帐户凭据登录到 Azure 门户 (**`https://portal.azure.com`**)。

   如果正在使用试订，您可能需要打开一个支持请求（***Help + Support***（帮助 + 支持） > ***New Support Request***（新建支持请求））以增加已分配 *VM* 核心的配额。

©2024 Palo Alto Networks, Inc.

STEP 2 | 在 Azure Marketplace 中找到 VM 系列解决方案模板。

1. 在 Azure China Marketplace 上搜索 Palo Alto Networks (https://market.azure.cn)。显示 VM 系列防火墙的不同PAN-OS版本的产品。



2. 选择一种产品，然后单击 **Immediate deployment of**（立即部署）。

©2024 Palo Alto Networks, Inc.

STEP 3 | 部署防火墙。

1. 选择所需的 Azure **Subscription**（订阅）。
2. 选择存放与此部署中的 VM 系列防火墙相关联的所有资源的资源组。

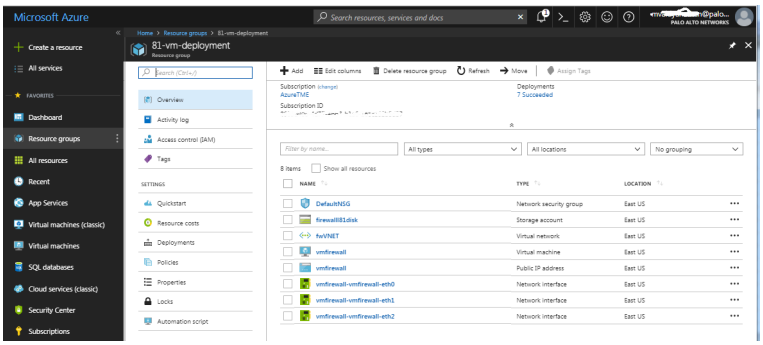
   您可以将 *VM* 系列防火墙部署到新的资源组或空的现有资源组中。要将防火墙部署到具有其他资源的现有资源组中，请使用 GitHub 存储库中的 *ARM* 模板或您自己的自定义 *ARM* 模板。确保现有资源与您在 *ARM* 模板中提供的参数值相匹配。

   1. 如果您创建新的资源组，请为该资源组输入一个名称，并选择您想要部署防火墙的 Azure China 区域。
   2. 如果选择现有资源组，请为该资源组选择 Azure China 区域，然后选择完整部署。
3. 配置防火墙的基本设置。
   1. 输入现有帐户的存储帐户名称或创建一个新帐户。
   2. 输入要将防火墙vhd映像复制并保存到的blob存储容器的名称。
   3. 输入用于访问防火墙管理接口 (eth0) 上公共 IP 地址的 DNS 名称。要访问防火墙的 Web 界面，必须将输入的前缀与后缀组合在一起，例如，<yourDNSname><china_region>.cloudapp.azure.com。
   4. 输入防火墙管理员的 **Username**（用户名）。
   5. 输入 **Password**（密码）以保护对防火墙的管理访问。
   6. 根据您的需求，选择 Azure 虚拟机层和规模。请参阅 Azure 上对 VM 系列的最低系统要求。
   7. 输入 **VmName**，这是识别资源组内的 VM 系列防火墙的显示名称。
   8. 使用 **PublicIPAddressName** 标记资源组中的防火墙管理接口。Microsoft Azure 将使用此名称定义的 DNS 名称进行绑定，以便您可以从公共 Internet 访问防火墙上的管理界面。
   9. 输入 **VirtualNetworkName** 以识别 VNet。VNet 的默认 IP **Address Prefix**（地址前缀）是10.0.0.0/16。您可以更改此设置以满足您的 IP 寻址需求。
   10. 配置网络接口的子网。如果使用现有 VNet，则必须定义三个子网，分别为：管理子网、可信子网和不可信子网。如果您创建新的 VNet，请检验或更改每个子网的前缀。

©2024 Palo Alto Networks, Inc.

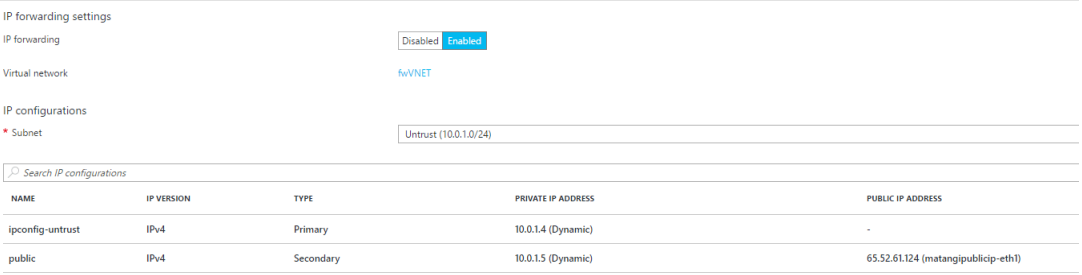
默认子网是 10.0.1.0/24、10.0.2.0/24 和 10.0.3.0/24。您可以根据需要将这些子网分配给管理、可信和非可信接口。

4. 查看摘要，接受使用条款和隐私政策，然后单击 **Immediate deployment**（立即部署）以部署防火墙。部署可能需要 20 分钟，您可以使用页面上的链接来检验进度。
5. 确认您已成功部署 VM 系列防火墙。
   1. 使用 Microsoft 帐户凭据登录到 Azure China 门户 (https://portal.azure.cn)。
   2. 选择 **Dashboard**（仪表盘） > **Resource Groups**（资源组），然后选择所需的资源组。
   3. 选择 **All Settings**（所有设置） > **Deployments**（部署） > **Deployment History**（部署历史记录）以了解详细状态



STEP 4 | 为 VM 系列防火墙的不可信接口附加一个公共IP地址。这使您可以从公共 Internet 访问界面，并可用于任何面向 Internet 的应用程序或服务。

1. 在 Azure 门户上，选择要为其添加公共 IP 地址的网络接口。例如 eth1 接口。
2. 选择 **IP Configurations**（**IP** 配置） > **Add**（添加）并为公共IP地址选择 **Enabled**（启用）。创建一个新的公共 IP 地址或选择一个可用的 IP 地址。
3. 验证您是否可以查看与该接口关联的辅助 IP 地址。



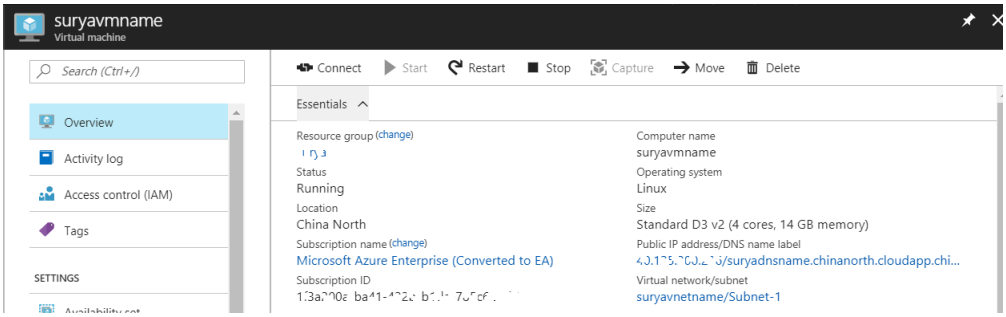
将辅助 *IP* 地址附加到网络接口时，*VM* 系列防火墙不会自动获取分配给该接口的专用*IP*地址。您将需要使用 *VM* 系列防火墙 *Web* 界面手动配置专用 *IP* 地址。请参阅配置数据面板网络接口作为防火墙上的第 3 层接口。

Azure上的 VM 系列防火墙上的每个接口都可以具有一个动态（默认）或静态私有 IP 地址以及与之关联的多个公共 IP 地址（静态或动态）。您可以分配给接口的最大公共 IP 地址数量取决于您的 Azure 订阅。当您创建一个新的公共 IP 地址时，您可以从微软拥有的 IP 地址块中获得一个，所以您不能选择一个特定的 IP 地址。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 登录防火墙的 Web 界面。

1. 在 Azure 门户的 **All Resources**（所有资源）中，选择 VM 系列防火墙并查看防火墙的完整 DNS 名称。



2. 使用 Web 浏览器提供的安全连接 (https) 登录到防火墙的 DNS 名称。
3. 输入之前定义的用户名/密码。您将看到证书警告；这属于正常情况。继续浏览网页。

STEP 6 | 在 VM 系列防火墙上激活许可证。

1. 创建支持帐户。
2. 注册 VM 系列防火墙（使用授权代码）。
3. 在防火墙 Web 界面上，选择 **Device**（设备）> **Licenses**（许可证），然后选择 **Activate feature using authentication code**（使用授权代码激活功能）。
4. 输入在支持门户上注册的容量授权代码。防火墙将连接到更新服务器 (updates.paloaltonetworks.com)，并下载许可证，然后自动重新启动。
5. 返回登录到 Web 界面，然后在 **Dashboard**（仪表盘）上确认以下各项：
   - 有效序列号显示于 **Serial#**（序列号）中。

     如果显示“Unknown（未知）”一词，则表示此设备未经许可。要查看防火墙上的流量日志，您必须安装有效的容量许可证。
   - **VM Mode**（**VM** 模式）显示为 Microsoft Azure。

STEP 7 | 配置数据面板网络接口作为防火墙上的第 3 层接口。

如果您在一台服务器上托管多个具有不同IP地址和SSL证书的网站或服务，则可能需要在 VM 系列防火墙接口上配置多个IP地址。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。
2. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：Layer3（默认）。
   - 在配置选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 New Zone（新建区域）。定义“UnTrust”新区域，然后单击 OK（确定）。
   - 如果您打算在接口上仅分配一个 IP 地址，请在 **IPv4** 选项卡中选择 **DHCP Client**（**DHCP** 客户端）。在 ARM 中分配的专用 IP 地址将被自动获取。如果您打算

 ©2024 Palo Alto Networks, Inc.

分配多个 IP 地址，请选择 **Static**（静态）并手动输入分配给 Azure 门户上接口的主要 IP 地址和辅助 IP 地址。

- 取消选中 **Automatically create default route to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）复选框。禁用此选项可确保此接口处理的流量不会直接流向 Vnet 中的默认网关。

3. 单击 **ethernet 1/2** 的链路并按如下所述配置：
   - 设置 **Interface Type**（接口类型）为第 3 层（默认）。
   - **Security Zone**（安全区域）：可信
   - **IP Address**（**IP** 地址）：选择 **DHCP Client**（**DHCP** 客户端）或 **Static**（静态）。
   - 取消选中 **Automatically create default route to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）复选框。禁用此选项可确保此接口处理的流量不会直接流向 Vnet 中的默认网关。
4. 单击 **Commit**（提交）。确认接口链路状态为“up（工作中）”。

STEP 8 | 为特定部署配置防火墙。

- 网关 — 在“UnTrust（不可信）”区域上游，部署第三方负载均衡器或。
- Hybrid and Inter-VNet — 在“UnTrust（不可信）”区域上游，部署 Azure VPN 网关或 NAT 虚拟机。
- Inter-Subnet — 在此系列防火墙上，添加区域之间的安全策略规则以允许基于附加到“Trust（可信）”接口的子网流量。
- GlobalProtect — 在“UnTrust（不可信）”区域上游，部署 NAT 虚拟机。

STEP 9 | 将流量定向到 VM 系列防火墙。

1. 为确保 VM 系列防火墙保护 Azure 资源组内的所有流量，请在防火墙上配置静态路由。
2. 配置UDR以通过 VM 系列防火墙上的接口定向所有流量。请参阅有关 UDR 的 Azure 文档了解详细信息。

   内部子网上的 UDR 必须发送通过“Trust（可信）”接口的所有流量。“UnTrust（不可信）”侧的 UDR 将定向所有来自 Internet 流量通过 VM 系列防火墙上的“UnTrust（不可信）”接口。Internet 发出的流量可能来自 Azure 应用程序网关或 Azure 负载均衡器，或在采用混合部署连接预置型网络与 Azure 云的情况下，此流量也可能来自 Azure VPN 网关。

©2024 Palo Alto Networks, Inc.

Azure 中的 Panorama 编排部署

适用于 Azure 的 Panorama 插件可在 Azure 云中集中部署、配置和监控您的安全态势。它可以在 Azure 网络中编排 VM 系列部署，以便您可以为托管防火墙启用安全策略。该插件链接到 Azure ARM 部署和 Azure 监视器页面，可提供对 VM 系列防火墙的部署状态、使用情况和性能的了解。

在 Azure 中，该插件可编排 Azure 资源的部署，例如负载均衡器、子网和 NAT 网关，以及 VM 系列防火墙自动扩展集。在 Panorama 中，该插件自动配置 Panorama 设备组、模板堆栈和 NAT 策略。它读取 Azure 资源中的标记，然后在一组防火墙上集中启用基于标记的策略。

Panorama 插件可以在 Azure 环境中的一个或多个区域中编排部署。部署可以包含中心堆栈或入站堆栈，或者同时包含两者，具体取决于需要为部署保护的流量：

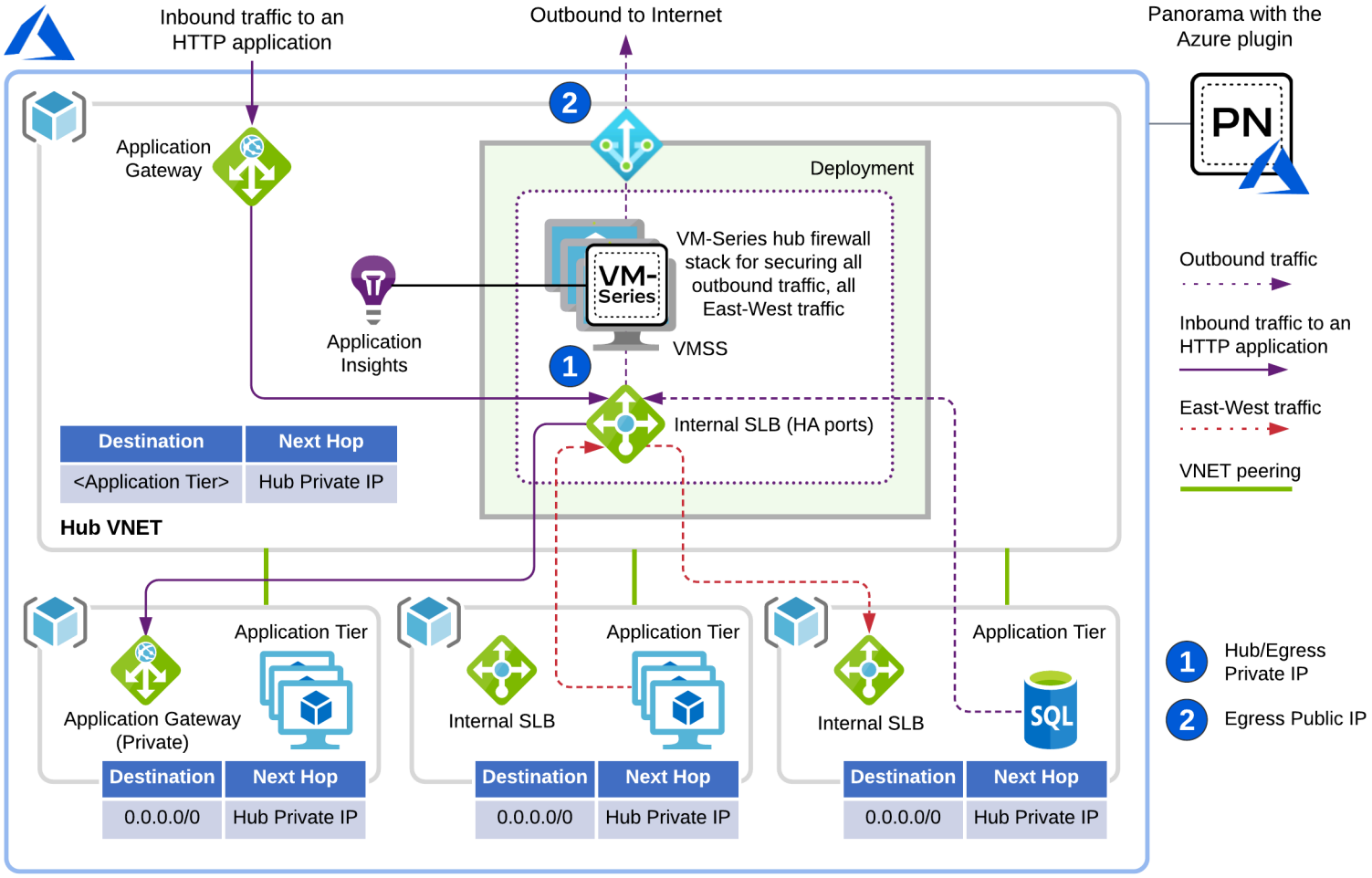
- 中心防火墙堆栈可保护应用程序工作负载之间的出站流量和东向西流量。
- 入站防火墙堆栈可保护往返于面向公众的应用程序的流量。

您可以配置每个堆栈中的防火墙数量。您可以选择在部署中配置静态数量的防火墙，也可以配置 VMSS 用于扩展的范围。部署中的这两个堆栈都可以创建 VM 系列防火墙的 VMSS，并且每个堆栈最多可以扩展到 25 个防火墙。

中心堆栈

部署使用中心堆栈，并利用 Azure 内部标准负载均衡器（具有 HA 端口）在一组防火墙之间扩展和加载均衡器。然后，您可以使用标准负载均衡器的专用 IP 地址（**2**，下图中的“中心/出口专用 IP”）将流量路由到防火墙，以进行检查和威胁保护。中心堆栈可保护应用程序的出站流量和东向西流量。

©2024 Palo Alto Networks, Inc.



要保护出站流量和东向西流量，请在应用程序 VNET 中添加路由规则，以将流量重定向到中心堆栈进行检查。

入站堆栈

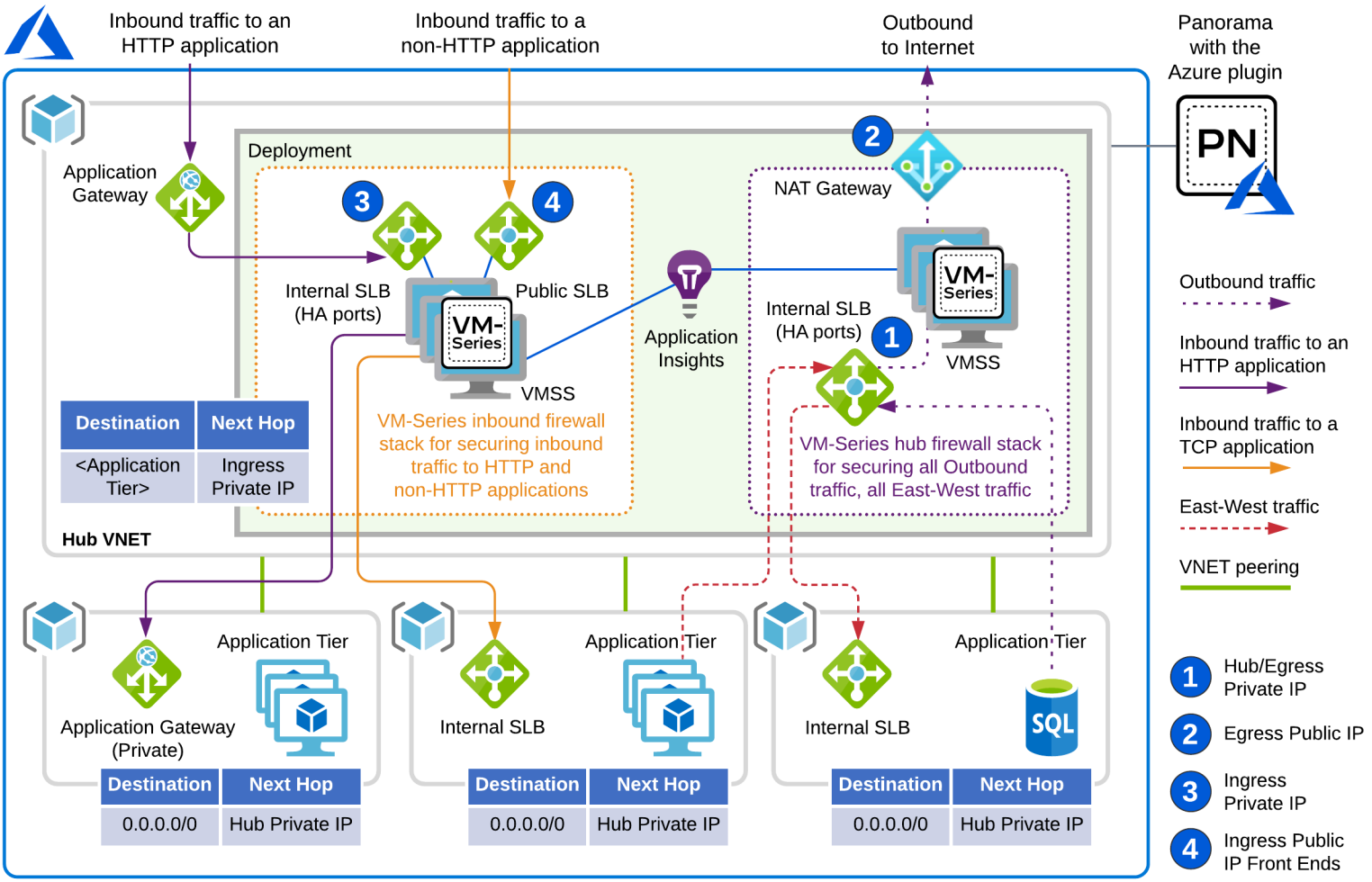
入站防火墙堆栈可独立扩展，并为应用程序的入站流量增加可见性和安全性。

每个入站堆栈最多可以保护 *10* 个应用程序。

要保护入站 HTTP 流量，请在应用程序网关的子网路由表中添加 UDR，以将所有流量路由到入站堆栈（**3**，下图中的入口专用 IP 地址）。要保护非 HTTP 入站流量，请使用 Panorama 插件为应用程序端点创建前端条目（**4**，下图中的入口公共 IP 前端）。要启用检查，Panorama 插件会在 Azure 公共标准负载均衡器上自动创建负载均衡器规则，并在防火墙上自动创建 NAT 规则。

如果您只有 HTTP/HTTPS 入站流量，则可以省去入站堆栈，并仅使用中心堆栈保护该流量。

©2024 Palo Alto Networks, Inc.



请参阅 准备编排部署 和 在 Azure 中编排 VM 系列防火墙部署。

准备编排部署

在 Azure 上编排 VM 系列防火墙之前，请完成以下任务。

- 配置前提条件
- 编排权限
- 创建自定义角色并将其与 Active Directory 关联
- 查找 Azure 目录域名

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

配置前提条件

在 Panorama 和 Azure 上完成以下基本任务。

©2024 Palo Alto Networks, Inc.

- Azure
  - 创建服务主体以启用插件进行 API 调用。
  - 计划专用于 VM 系列防火墙 Transit VNet 的 CIDR 块。该插件管理此 CIDR 块，用于部署初始防火墙 VNet，并作为将来对新模板堆栈的升级。

    最小 CIDR 范围为 /22。
- Panorama
  - 确保您已在 Panorama 上配置有效的许可证 API 密钥。这能够让插件管理解除对缩减自动扩展事件的许可。请参阅安装许可证停用 API 密钥。
  - 在 Panorama 上安装最新版本的 VM 系列插件，可允许将 Application Insights 配置添加到模板堆栈。
- 合格的 Azure 区域

  所有支持 VM 系列防火墙的区域都支持 Panorama 编排部署。以下地区已获得资格；如果您在未列出的区域部署并遇到问题，请联系支持人员。
  - 美国西部
  - 美国西部 2
  - 美国中北部
  - 美国东部
  - 美国东部 2
  - 西欧
  - 德国中西部
  - 阿联酋北部
  - 西印度
  - 澳大利亚东南部

规划部署时，请注意，如果您目前运行适用于 Azure 版本 2.x 的 Panorama 插件，则不允许升级到当前版本。与此同时，一旦安装当前版本，不允许将插件降级到版本 2.x。请参阅兼容性矩阵中适用于 Azure 的 Panorama 插件。

编排权限

以下是一个具有模板部署者角色权限的 JSON 文件示例。在 **AssignableScopes** 部分中，包括所有必须查询的相关订阅，包括在其中部署部署的订阅，以及包含与现有保护资源的 VM 系列防火墙 VNet 对等的应用程序 VNET 的每个订阅。

```
{ "Name":"Template Deployment", "IsCustom": true,
 "Description":"Manage template deployments.",    "Actions":
 [ "Microsoft.Resources/subscriptions/resourcegroups/*",
 "Microsoft.Resources/deployments/write", "Microsoft.Resources/
deployments/operationStatuses/read", "Microsoft.Resources/
deployments/read", "Microsoft.Resources/deployments/delete",
```


©2024 Palo Alto Networks, Inc.

```
 "Microsoft.Network/publicIPPrefixes/write", "Microsoft.Network/
publicIPPrefixes/read", "Microsoft.Network/publicIPPrefixes/delete",
 "Microsoft.Network/publicIPAddresses/write", "Microsoft.Network/
publicIPAddresses/read", "Microsoft.Network/publicIPAddresses/
delete", "Microsoft.Network/publicIPAddresses/join/action",
 "Microsoft.Network/natGateways/write", "Microsoft.Network/
natGateways/read", "Microsoft.Network/natGateways/delete",
 "Microsoft.Network/natGateways/join/action", "Microsoft.Network/
virtualNetworks/read", "Microsoft.Network/virtualNetworks/write",
 "Microsoft.Network/virtualNetworks/delete", "Microsoft.Network/
virtualNetworks/subnets/write", "Microsoft.Network/virtualNetworks/
subnets/read", "Microsoft.Network/virtualNetworks/subnets/
delete", "Microsoft.Network/virtualNetworks/subnets/join/action",
 "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/
read", "Microsoft.Network/networkSecurityGroups/write",
 "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/
networkSecurityGroups/delete", "Microsoft.Network/
networkSecurityGroups/join/action", "Microsoft.Network/loadBalancers/
write", "Microsoft.Network/loadBalancers/read", "Microsoft.Network/
loadBalancers/delete", "Microsoft.Network/loadBalancers/probes/join/
action", "Microsoft.Network/loadBalancers/backendAddressPools/join/
action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/
read", "Microsoft.Network/locations/serviceTags/read",
 "Microsoft.Network/applicationGateways/read", "Microsoft.Network/
networkInterfaces/read", "Microsoft.Compute/virtualMachineScaleSets/
write", "Microsoft.Compute/virtualMachineScaleSets/read",
 "Microsoft.Compute/virtualMachineScaleSets/delete",
 "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
 "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/images/
read", "Microsoft.insights/components/write", "Microsoft.insights/
components/read", "Microsoft.insights/components/delete",
 "Microsoft.insights/autoscalesettings/write" ] "NotActions": [ ],
 "AssignableScopes": [ "/subscriptions/{deployment-subscription}",
 "/subscriptions/{app1-subscription}", "/subscriptions/{app2-
subscription}", . . . ] }
```

创建自定义角色并将其与 **Active Directory** 关联

STEP 1 | 要在 Azure 中创建 Active Directory，导航到 Azure Active Directory，然后单击左侧的 **App Registrations**（应用程序注册）。使用插件所需的权限创建自定义角色。

下面包括一个 JSON 文件示例。

1. 单击 **Add**（添加）并提供名称。选择从上述 JSON 文件创建的角色，保留“将访问权限分配给”作为 Active Directory 用户，并选择在第一步中创建的 Active Directory，然后单击 Save（保存）。
2. 选择类型。

   不要修改 Redirect URI（重定向 URI）下的任何内容。

©2024 Palo Alto Networks, Inc.

STEP 2 | 使用插件所需的权限创建自定义角色。

请参阅编排权限。

1. 登录到 Azure CLI。

```
az login
```

2. 从编排权限中的文件创建自定义角色。

```
az 角色定义创建 — 角色定义 <role-json-file>
```

STEP 3 | 将角色与您在步骤 1 中创建的 Active Directory 关联。您可以使用控制台或 CLI。

在编排权限的自定义角色的 ***assignableScope*** 部分定义的每个订阅中，您必须重复执行此步骤。

控制台

1. 在 Azure 门户上，导航到 **Subscriptions**（订阅），然后选择您的订阅。
2. 选择左侧的 **Access Control (IAM)**（访问控制 **(IAM)**），然后选择顶栏中的 **Role Assignments**（角色分配）。
3. 选择 **Add**（添加），然后选择 **add role assignment**（添加角色分配）。
   - 选择在步骤 3 中创建的角色，然后保留“将访问权限分配给”作为 Active Directory 用户。
   - 选择在步骤 1 中创建的 Active Directory，然后单击 **Save**（保存）。

CLI：

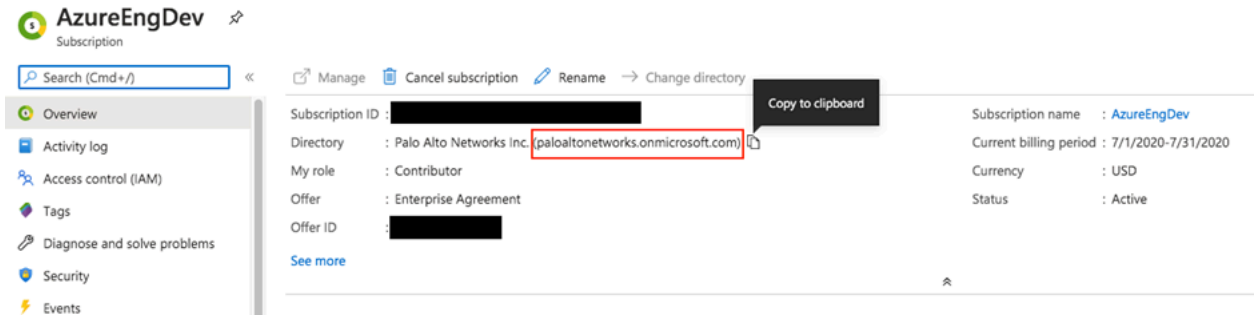
在以下命令中，**<role-name>** 是指示例 JSON 文件中的名称，在前面的示例中，则为 **Template Deployment**。

```
az ad sp create-for-rbac --name <name-of-service-principal> --role
 <role-name> --output json
```

查找 Azure 目录域名

为了让该插件提供指向 Azure 门户中 Azure 部署和 Application Insights 实例的链接，您必须标识订阅的目录域，如下所示：

 ©2024 Palo Alto Networks, Inc.



在 Azure 中编排 VM 系列防火墙部署

您最多可以创建十个编排部署。此外，每个编排部署最多支持 100 个前端应用程序。

不支持 *Azure China* 和 *Azure Government*。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建服务主体。

使用创建的服务主体凭据登录，以授予 Panorama 插件权限来进行必要的 API 调用，从而编排您的部署。

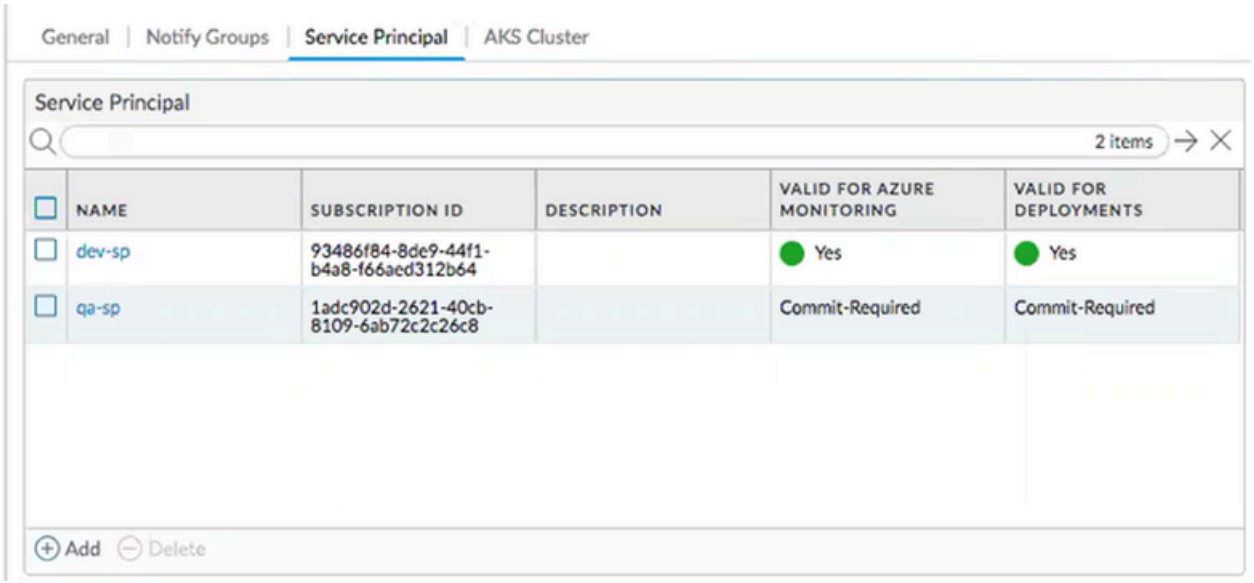
1. 选择 **Setup**（设置） > **Service Principal**（服务主体） > **Add**（添加）。
2. 输入标识服务帐户的 **Name**（名称），也可选择输入 **Description**（说明）。
3. 输入要监控的 Azure 订阅的 **Subscription ID**（订阅 **ID**）。

   您必须登录到 Azure 门户才能获取此订阅 ID。
4. 输入 **Client ID**（客户端 **ID**）。客户端 ID 是与 Azure Active Directory 应用程序相关联的应用程序 ID。
5. 输入 **Client Secret**（客户端机密），并重新输入以进行确认。
6. 输入 **Tenant ID**（租户 **ID**）。

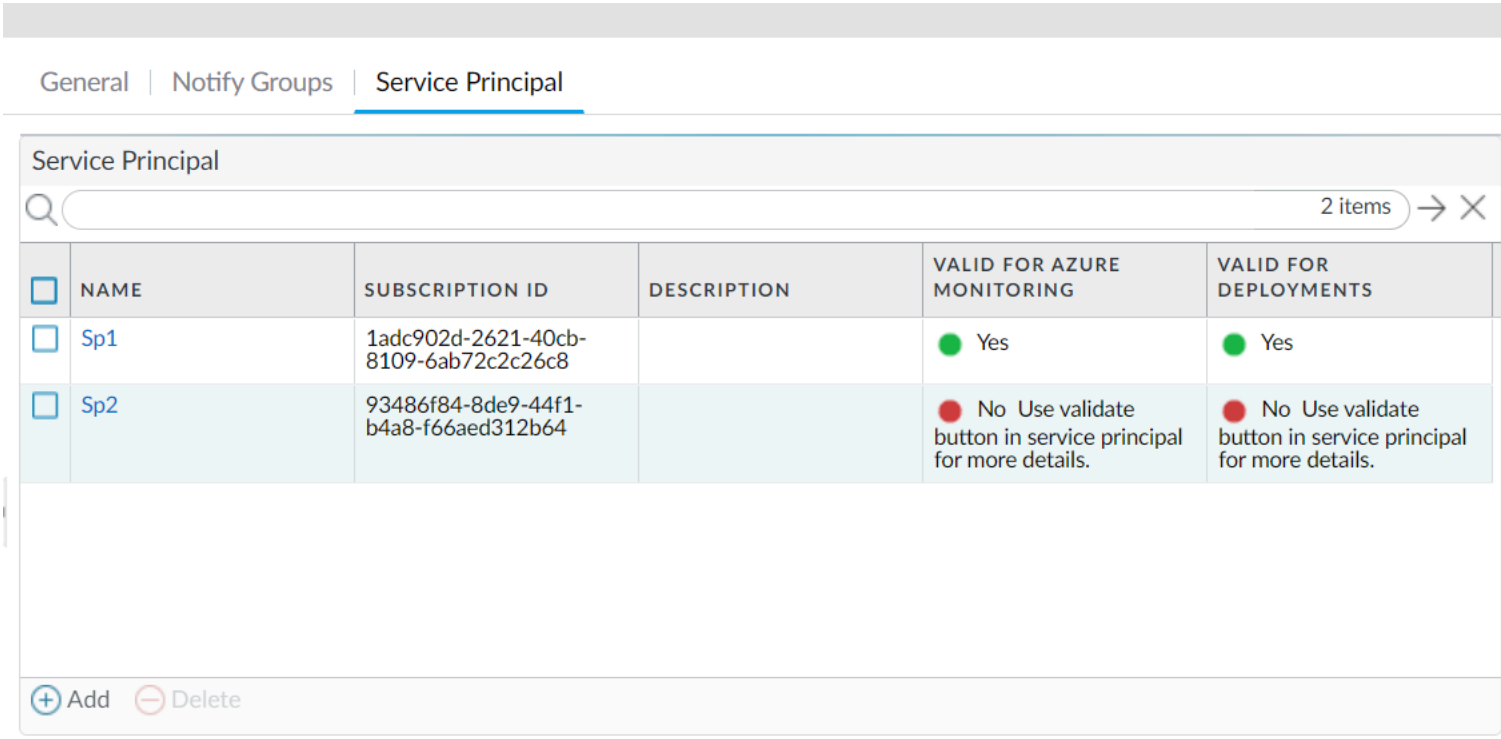
   租户 ID 是在设置 Active Directory 应用程序时保存的 Directory ID。
7. 单击 **Validate**（验证）以验证输入的密钥和 ID 是否有效，并且 Panorama 是否可以使用 API 与 Azure 订阅进行通信。

   验证最多可能需要一分钟的时间。您可以更新页面以检查进度。
8. 当服务主体有效时，请提交您的更改。

   提交可确保服务主体在配置部署时可用。



 ©2024 Palo Alto Networks, Inc.



©2024 Palo Alto Networks, Inc.

STEP 2 | 配置 Azure 部署。

1. 选择 **Deployments**（部署）并 **Add**（添加）配置。
2. 选择 **Build**（构建） > **General**（常规）。
   - 提供 **Name**（名称）和可选 **Description**（说明）。
   - 从下拉列表中选择服务主体。

     必须选择有效的服务主体才能启用 **Azure** 选项卡。

     如果看不到服务主体，请返回步骤 1 并确保服务主体有效且已提交。

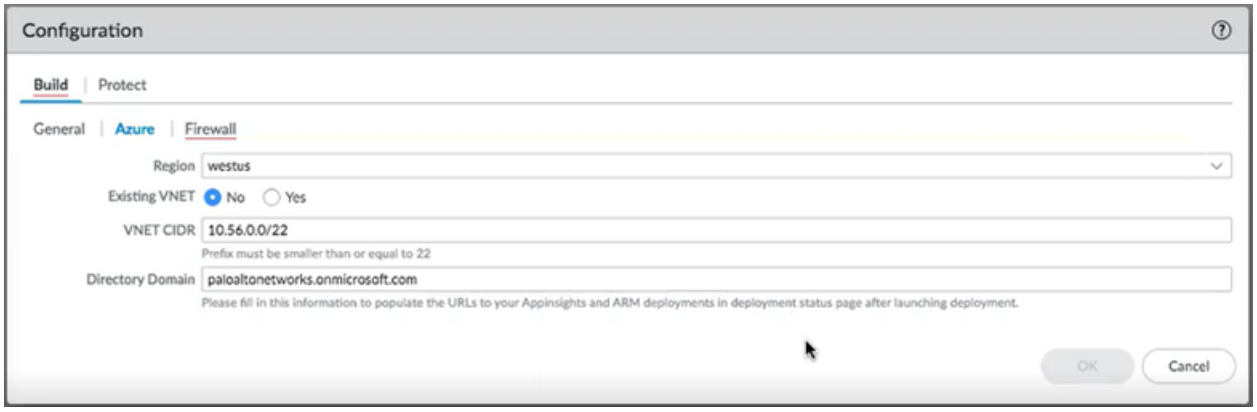


3. 在 **Build**（构建） > **Azure** 选项卡上，选择一个地区。

   下拉列表是动态的，列出了安装 Palo Alto Networks VM 系列下一代防火墙映像的所有地区。

   - **Existing VNET**（现有 **VNET**）。
     - 选择 **No**（否）以创建新 VNET。

       该插件使用 VNET CIDR 和目录域创建 VNET。
     - 选择 **Yes**（是）以指示现有 VNET。
   - **VNET CIDR** — 输入 CIDR 范围。前缀必须小于或等于 /22。例如，192.168.0.0/22。
   - **Directory Domain**（目录域）— 请参阅查找 Azure 目录域名。该字符串是订阅中所有资源的 URL 的一部分，有助于将插件链接到部署。

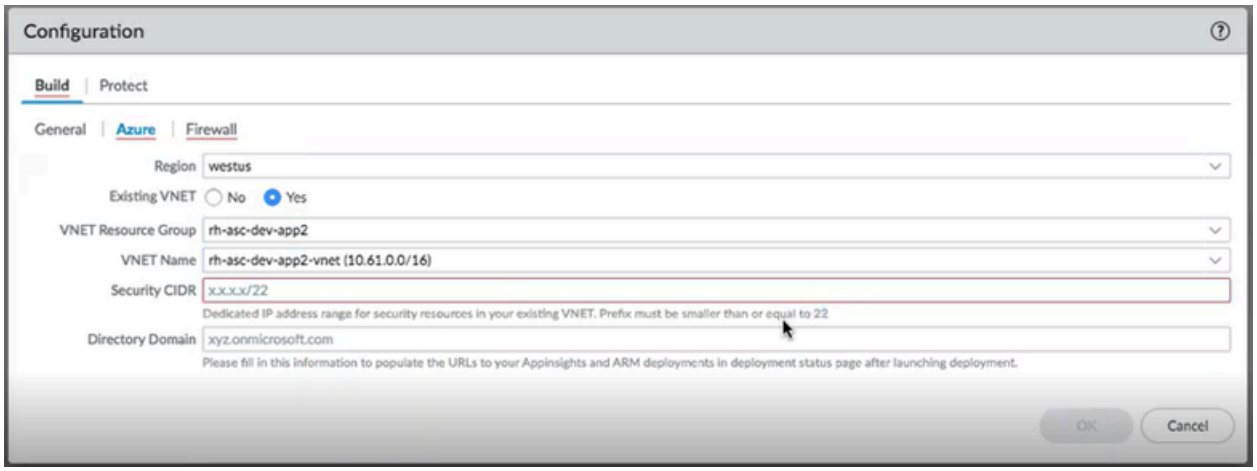


 ©2024 Palo Alto Networks, Inc.

如果选择 **Yes**（是），则插件会询问 VNET 资源组、VNET 名称、安全 CIDR 和目录域。

- **VNET Resource Group**（**VNET** 资源组）— 从所选地区的所有资源组列表中选择。
- **VNET Name**（**VNET** 名称）— 从所选资源组的 VNETS 列表中选择。
- **Security CIDR**（安全 **CIDR**）— 输入 CIDR 范围。前缀必须小于或等于 /22。例如，192.168.0.0/22。
- **Directory Domain**（目录域）— 请参阅查找 Azure 目录域名。该字符串是订阅中所有资源的 URL 的一部分，有助于将插件链接到部署。

VNET 资源组和 VNET 名称有助于插件找到现有 VNET。插件部署的所有内容都加入插件管理的资源组。



©2024 Palo Alto Networks, Inc.

STEP 3 | 为部署配置 VM 系列防火墙堆栈。

您可以部署中心堆栈以保护出站/东向西流量。此外，您还可以部署入站堆栈以保护入站流量。如果需要保护所有流量，也可以部署两个堆栈。

两个堆栈的配置参数相同。

- **License Type**（许可证类型）— 选择 BYOL、套餐 1 或套餐 2。
- **License Authcode**（许可证授权代码）—（仅限 BYOL）。输入在欢迎信中发送给您的授权代码。
- **VM Size**（**VM** 大小）
  - 该下拉列表显示与输入的授权代码相关的 VM 大小。
  - 套餐 1 或套餐 2 — 选择任意 VM 大小。

现有设备组 — 堆栈和部署中的设备组必须是唯一的。也就是说，每个部署中的每个堆栈都需要一个单独的专用设备组。

如果选择 **No**（否），则插件会创建一个设备组。

如果选择 **Yes**（是），请从下拉列表中选择一个现有设备组。

- **Min Firewalls**（最小防火墙数）— VMSS 的值介于 1 到 25 之间。
- **Max Firewall**（最大防火墙数）— VMSS 的值介于 1 到 25 之间。

©2024 Palo Alto Networks, Inc.

STEP 4 | 选择 **Build**（构建） > **Firewall**（防火墙） > **Basic**（基本），以配置两个堆栈共有的信息。

对于 **Image Type**（映像类型），选择 **Marketplace Image**（**Marketplace** 映像）或 **Custom Image**（自定义映像）。

- **Image Resource Group**（映像资源组）—（仅限自定义映像）选择包含自定义映像的资源组。对于自定义映像，该列表显示包含您在步骤 2.b 中选择的地区中映像的所有资源组。
- **Image**（映像）—（仅限自定义映像）下拉列表显示所选资源组中的所有映像。
- **Software Version**（软件版本）—（Marketplace 映像）仅显示有效的软件版本。有关最低 PAN-OS 版本，请参阅兼容性矩阵。
- **Username**（用户名）— 您创建的防火墙的管理员用户名。用户名对于 VM 系列防火墙和 Azure 必须是合法的。请参阅创建 VM 时用户名要求是什么？ 。
- **Password**（密码）— 您创建的防火墙的管理员密码。密码必须满足 VM 系列防火墙和 Azure 的字符和长度要求（31 个字符）。请参阅创建 VM 时密码要求是什么？ 。
- **Confirm Password**（确认密码）— 重新输入密码。
- **Primary Panorama IP**（主 **Panorama IP** 地址）— 指定防火墙启动时可用于连接到 Panorama 的 Panorama IP 地址。可以选择下拉列表中显示的公用或专用 IP 地址，或键入 Panorama IP 地址。
- **Secondary Panorama IP**（辅助 **Panorama IP** 地址）—（仅限 Panorama 在 HA 设置中时。）指定防火墙启动时可用于连接到 Panorama 的辅助 Panorama IP 地址。从下拉列表中选择或键入正确的 IP 地址。
- **Configure Device Certificate PIN**（配置设备证书 **PIN**）。由于以下值已经过加密，因此必须输入并确认每个值。
  - **Device Certificate PIN ID**（设备证书 **PIN ID**）— 设备证书 ID。
  - **Confirm Device Certificate PIN ID**（确认设备证书 **PIN ID**）
  - **Device Certificate PIN Value**（设备证书 **PIN** 值）— 证书 PIN 值。
  - **Confirm Device Certificate PIN Value**（确认设备证书 **PIN** 值）

STEP 5 | 选择 **Build**（构建） > **Firewall**（防火墙） > **Advanced**（高级）可选默认值。

选择 **Advanced**（高级）以编辑默认值。

- **Autoscaling Metric**（自动扩展指标）— 默认值为数据平面 CPU 使用率百分比。
- **Scale In Threshold**（缩小阈值）— 接受默认值或定义缩小阈值。
- **Scale Out Threshold**（扩大阈值）— 接受默认值或定义扩大阈值。
- **Jumbo Frame**（**Jumbo** 帧）— 默认禁用。

单击 **OK**（确定）并提交更改。刷新页面，直到系统显示 **Deploy**（部署）按钮，然后单击 **Deploy**（部署）以启动部署。部署启动后，会将相关信息写入 **Deployments**（部署）页面。

部署完成可能需要 *15* 至 *20* 分钟的时间。

©2024 Palo Alto Networks, Inc.

STEP 6 | 选择 **Azure** > **Deployments**（部署）以查看部署状态。

- Resource Group（资源组）列显示插件已创建的资源组。
- 防火墙的管理接口使用防火墙访问 IP 地址连接到 Panorama。您必须将此地址列入白名单，以确保防火墙可以连接至 Panorama 以获取所需的配置。

  如果在公共云中部署 *Panorama*，请确保将防火墙访问 *IP* 地址添加到 *Panorama* 安全组。

  请参阅用于 Panorama 的端口，以确定需要打开以允许流量的端口。
- 打开 **Deployment Status**（部署状态）列中的链接，以获取每个堆栈的更多详细信息。
  - **Hub-Stack**（中心堆栈）— 中心堆栈公用 IP 地址与部署摘要中的防火墙访问 IP 地址匹配，因为 NAT 网关对于来自部署的出口流量和来自防火墙的管理流量而言是相同的。

    应将所有出站和东向西流量路由到 **Egress Private IP**（出口专用 **IP** 地址）以进行检查。如果已配置 UDR，则可以将流量定向到该地址。
  - **Inbound-Stack**（入站堆栈）— 专用 IP 地址是防火墙前面的 Azure 内部负载均衡器上的地址。如果要配置 UDR，则可以将流量定向到该地址。
- 单击链接以查看 Azure 上的部署信息和 Application Insights。
- 部署详细信息将显示“成功”、“警告”和“失败”消息。

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 为后端 TCP/UDP 应用程序配置入站保护。

入站防火墙堆栈前面的公共负载均衡器是所有后端 UDP 或 TCP 应用程序的入口点。添加以下配置以允许插件管理必需的负载均衡器，并将防火墙配置路由到后端应用程序。

1. 选择 **Azure** > **Deployments**（部署），然后选择部署。
2. 选择 **Protect**（保护）选项卡，然后单击 **Add**（添加）。
3. 提供应用程序 **Name**（名称），然后选择 **Protocol**（协议）。

   输入保护详细信息：

   - **Frontend IP Type**（前端 **IP** 地址类型）— 选择新的公用 IP 地址、现有前端和现有公用 IP 地址之一。

     如果选择现有前端，则 **Frontend Name**（前端名称）会列出负载均衡器上的所有已知前端。
   - **Resource Group**（资源组）—（仅限现有公用 IP 地址）从下拉列表中选择所需前端 IP 地址所在的资源组。
   - IP Name（IP 地址名称）—（仅限现有公用 IP 地址） 用于将 IP 地址映射到负载均衡器上的前端，配置负载均衡器，并创建 NAT 规则。
   - **Frontend Port**（前端端口）— 添加应配置为在公共负载均衡器上接收流量的前端端口。
   - **Backend IP**（后端 **IP** 地址）— 添加后端应用程序的 IP 地址。
   - **Backend Port**（后端端口）— 添加后端应用程序期望在其上接收流量的端口。

   单击 **OK**（确定）。
4. **Commit**（提交）以在负载均衡器上添加配置，然后推送到防火墙。

 ©2024 Palo Alto Networks, Inc.

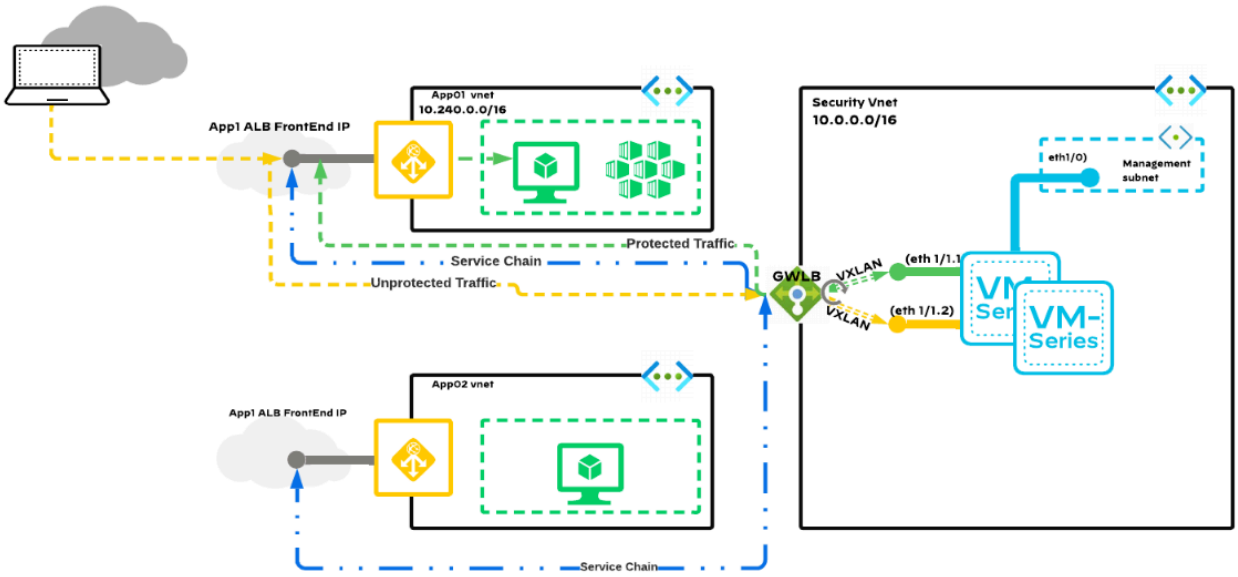
使用 Azure 网关负载均衡器部署 VM 系列

现在，您可以为 Azure 将 VM 系列防火墙与 Azure 网关负载均衡器 (GWLB) 集成。保护入站流量需要在流量传输到云中的目的地时完全了解流量源的标识。当 VM 系列防火墙部署在公共标准负载均衡器后时，入站流量的源 IP 地址将被替换为负载均衡器的 IP 地址。结果是会混淆应用程序源的标识。通过在 Azure GWLB 后部署 VM 系列防火墙，流量数据包标头和有效负载保持完好无损，这提供了源标识在传输到目的地时的完整可见性。启用 Azure GWLB 集成后，VM 系列使用 VXLAN 数据包来检查流量的内部数据包，并将策略应用到数据包。

当部署在 Azure GWLB 后时，VM 系列防火墙可以实施基于区域的安全策略。通过为 VNet 绑定流量分配信任区域并为 Internet 绑定流量分配不信任区域，您可以分割 VNet 绑定流量和 Internet 绑定流量。

通过此集成，您可以在所有支持的区域中将 VM 系列防火墙作为后端部署到 Azure GWLB。

©2024 Palo Alto Networks, Inc.



VM 系列防火墙与 *Azure GWLB* 集成需要 *PAN-OS 10.1.4* 或更高版本以及 *VM* 系列插件 *2.1.4* 或更高版本。

遵循最佳做法，不同 *VNet* 不要使用重叠的 *CIDR*。

STEP 1 | 使用 ARM 模板在 Azure GWLB 后部署 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 2 | （可选） 在步骤 1 中部署的 GWLB 后添加额外的 VM 系列防火墙实例。

1. 使用 Microsoft Azure CLI 创建 VM。

   在下面的示例命令中提供输入参数。

```
az vm create \ --resource-group <myResourceGroup> \ --
name <myPA-VM> \ --vnet-name secVnet \ --subnet Subnet-
mgmt \ --public-ip-sku Standard \ --size Standard_DS3_V2
 \ --nsg networkSecurityGroup1 \ --admin-username
 <username> \ --admin-password <password> \ --image
 paloaltonetworks:vmseries-flex:bundle1:10.1.4 \ --plan-
name bundle1 \ --plan-product vmseries-flex \ --plan-
publisher paloaltonetworks \ --custom-data "storage-
```

 ©2024 Palo Alto Networks, Inc.

```
account=<myStorageAccountName>,access-key=<myAccessKey>,file-
share=<FileName>,share-directory=<SharedDirectoryName>"
```

需要 *init-cfg.txt* 文件才能引导 *VM* 系列防火墙。该文件提供防火墙连接到网络所需的基本信息。*bootstrap* 文件夹中的 *init-cfg.txt* 文件包含以下信息。

- 使用默认端口部署解决方案：

  ```
  plugin-op-commands=azure-gwlb-inspect:enable
  ```

- 要使用自定义端口部署解决方案，如果自定义数据字段用于定义 *VNI ID* 和端口信息，请使用 *init-cfg.txt* 文件中的示例命令。您必须在 *800* 到 *1000* 的范围内定义内部和外部 *VNI* 标识符。

  ```
  plugin-op-commands=azure-gwlb-inspect:enable
  +internal-port-<internalport>+external-port-
  <externalport>+internal-vni-<internalvni>+external-
  vni-<internalvni>
  ```

  If you choose to use custom ports, use these sample commands to configure the GWLB.

  ```
  az network lb address-pool tunnel-interface
   add --resource-group <myResourceGroup> --lb-
  name <myGatewayLoadBalancer> --address-pool
   <myBackendPool> --type external --protocol
   vxlan --identifier <VNI> --port <port> az
   network lb address-pool tunnel-interface
   add --resource-group <myResourceGroup> --lb-
  name <myGatewayLoadBalancer> --address-pool
   <myBackendPool> --type internal --protocol vxlan
   --identifier <VNI> --port <port>
  ```

有关详细信息，请参阅 Azure 虚拟机上的自定义数据和 Cloud-init。

2. 在数据子网中创建 NIC。

   ```
   az network nic create -g <myResourceGroup> --vnet-name secVnet
    --subnet Subnet-data -n <myDataNIC> --accelerated-networking
    true --ip-forwarding true
   ```

3. 停止在步骤 1 中创建的 VM。

   ```
   az vm deallocate -n <myPA-VM> -g <myResourceGroup>
   ```


©2024 Palo Alto Networks, Inc.

4. 将步骤 2 中创建的 NIC 添加到 VM。

```
az vm nic add -g <myResourceGroup> --vm-name <myPA-VM> --nics
 <myDataNIC>
```

5. 将虚拟机加入 GWLB 后端地址池。

```
az network nic ip-config address-pool add --address-
pool BackendPool1 --ip-config-name ipconfig1 --nic-name
 <myDataNIC> --resource-group <myResourceGroup> --lb-name
 securityLB
```

6. 启动虚拟机。

```
az vm start -n <myPA-VM> -g <myResourceGroup>
```

7. 使用 SSH 连接到防火墙。在防火墙 CLI 中输入以下命令以验证是否已启用 GWLB。

```
show plugins vm_series azure gwlb
```

（可选）如果未引导防火墙，用户数据 将用于配置端口和 VNI ID。在防火墙 CLI 上使用以下示例命令启用或禁用 GWLB，配置自定义端口和 VNI ID，以及查看 GWLB 状态和端口/VNI ID 映射。



端口号和 *VNI ID* 必须与 *GWLB* 后端地址池中的 *ID* 相匹配。

```
request plugins vm_series azure gwlb inspect enable yes request
 plugins vm_series azure gwlb parameters internal-port 2000
```


©2024 Palo Alto Networks, Inc.

```
external-port 2001 internal-vni 800 external-vni 801 show plugins
vm_series azure gwlb
```

示例输出：

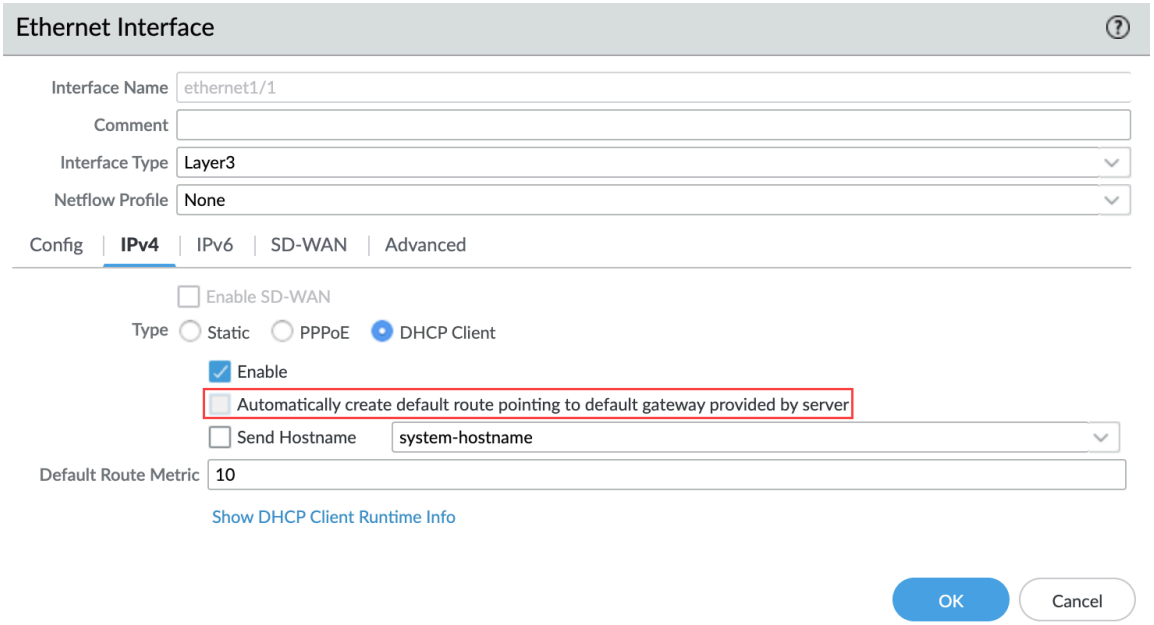
```
GWLB enabled :True Internal Tunnel Port:2000 Internal Tunnel
 VNI:800 External Tunnel Port:2001 External Tunnel VNI:801
```

（手动引导配置）如果您没有在步骤 1 或步骤 2.1 至 2.7 中使用 GWLB 引导 VM 系列防火墙，请执行以下手动过程。

1. 将数据平面网络接口配置为防火墙上的第 3 层接口。
   1. 在 VM 系列防火墙 Web 界面上，请选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
   2. 单击 **ethernet 1/1** 并按如下所述配置：
      - 将 **Interface Type**（接口类型）设置为 **Layer3**（默认）

        。
      - 在 **Config**（配置）选项卡上，将接口分配给虚拟路由器。
      - 此外，在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义内部和外部区域，然后单击 **OK**（确定）。
      - 在 **IPv4** 选项卡上，选择 **DHCP Client**（**DHCP** 客户端）。
      - 禁用 **Automatically create default route to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由），确保此接口处理的流量不会直接流向 VNet 的默认网关。

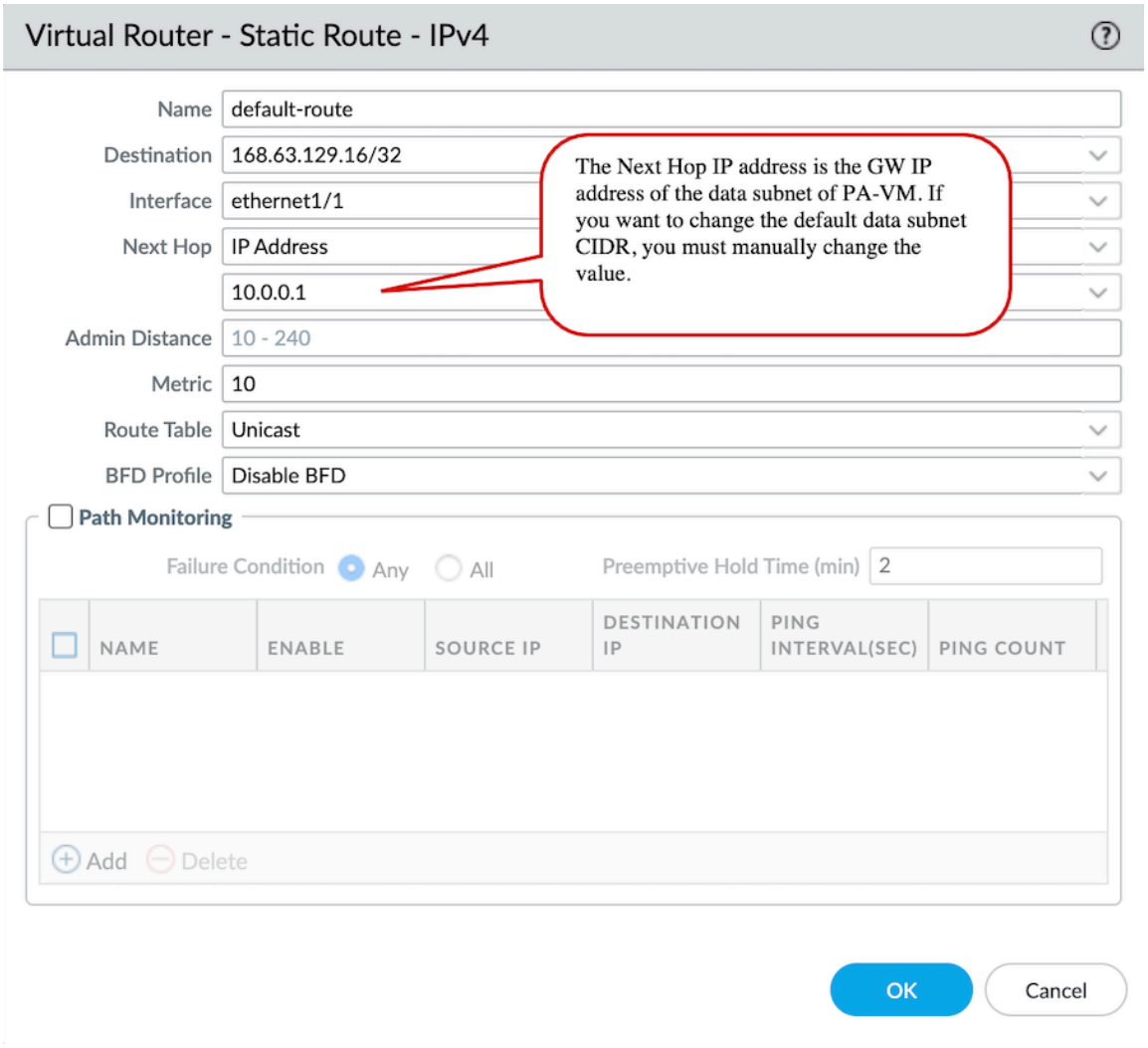
©2024 Palo Alto Networks, Inc.



3. 在 **Advanced**（高级）选项卡上，创建管理配置文件以允许防火墙接收运行状况检查。
4. **Commit**（提交）更改，并验证接口链路状态为“工作中”。

2. 在 VM 系列防火墙上创建静态路由。
   1. 在 VM 系列防火墙 Web 界面上，选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择与此数据接口相关联的虚拟路由器。
   2. 选择 **Static Routes**（静态路由）并单击 **Add**（添加）。
   3. 配置静态路由。

©2024 Palo Alto Networks, Inc.

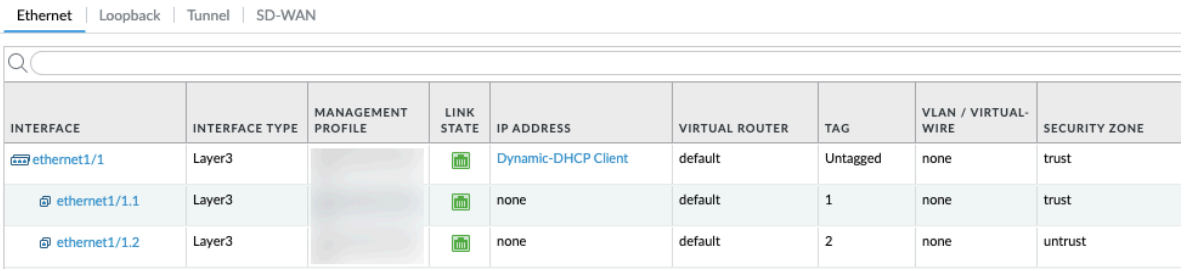


©2024 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。
5. **Commit**（提交）更改。

3. 在 eth1/1 下创建两个子接口以实施基于区域的安全策略。
   1. 在 VM 系列防火墙 Web 界面上，选择 **Network**（网络）> **Interface**（接口）。
   2. 突出显示 **ethernet1/1** 并单击 **Add Subinterface**（添加子接口）。
   3. 输入数字后缀（1 至 9,999）以标识子接口。
   4. 输入该子接口的 **VLAN Tag**（**VLAN** 标记）。这是必填字段，但不使用 VLAN。

      内部隧道的 *VNI ID*/端口映射到 *VLAN 1* 标记，外部隧道则映射到 *VLAN 2* 标记。*VLAN 1* 标记和 *VLAN 2* 标记必须始终分别映射到内部（信任）区域和外部（不信任）区域。
   5. 选择与数据接口相关联的 **Virtual Router**（虚拟路由器）。
   6. 选择 **Security Zone**（安全区域）。
   7. 在 **IPv4** 选项卡上，将 **Type**（类型）设置为 **DHCP Client**（**DHCP** 客户端）。
   8. 单击 **OK**（确定）。
   9. 对第二个子接口重复执行此命令。
   10. **Commit**（提交）更改。



©2024 Palo Alto Networks, Inc.

为 Azure 创建自定义 VM 系列映像

您可以创建稍后用于 Azure 部署的自定义 VM 系列防火墙映像。自定义映像可提供所需的灵活性和一致性，从而能够让您通过想要使用的 PAN-OS 版本部署 VM 系列防火墙，而不仅限于使用通过 Azure 市场获取的可用映像。此外，自定义映像可包含最新的内容和防病毒更新。

创建自定义映像需要在创建 VHD 之前删除所有私有数据，例如用户配置、用户、插件配置等。此外，要准备并创建自定义映像，请完成以下过程。

如果使用高级磁盘类型部署用于创建自定义映像的 *VM* 系列防火墙，则必须使用同一高级磁盘类型部署使用自定义映像部署的所有 *VM* 系列防火墙都。但是，如果您使用通过标准磁盘类型部署的防火墙创建映像，则可以使用标准磁盘类型或高级磁盘类型部署防火墙。

STEP 1 | 登录到 Azure。

STEP 2 | 从 Azure Marketplace 部署 VM 系列防火墙。

STEP 3 | （仅限 BYOL 许可证）激活您的许可证。

STEP 4 | 升级 VM 系列防火墙 到 PAN-OS 10.0.3。升级到 PAN-OS 10.0.3 还将 VM 系列插件升级到 2.0.3。

STEP 5 | 使用 Azure Marketplace 模板中提供的用户名和密码，通过 SSH 访问 VM 系列防火墙命令行界面。

STEP 6 | 验证 VM 系列防火墙具有正确的 PAN-OS、VM 系列插件、内容和防病毒版本。

```
show system info
```

如果使用 *PAN-OS 10.1*，请确保将 *VM* 系列插件升级到版本 *2.1.7* 或更高版本，如果使用 *PAN-OS 10.2.0*，请确保使用 *3.0.3* 或更高版本的 *VM* 系列插件。

STEP 7 | （仅限 BYOL 许可证）停用您的许可证。

STEP 8 | 在 VM 系列防火墙上执行私有数据重置。此命令要求重新启动防火墙。您必须等待 VM 系列防火墙重新启动完成才能继续；重新启动可能需要五至七分钟的时间。

```
request system private-data-reset
```


©2024 Palo Alto Networks, Inc.

STEP 9 | 从 VM 系列实例创建新的 VHD 映像。

1. 登录到 Azure CLI。
2. 验证您正在使用正确的订阅。

   ```
   az account set --subscription <subscription-id>
   ```
3. 执行以下命令以使 VM 具有通用性，从而可以为多个部署进行映像，并创建新的 VHD。

   ```
   az vm deallocate --resource-group <myResourceGroup> --name
   <myVM>
   ```

   ```
   az vm generalize --resource-group <myResourceGroup> --name
   <myVM>
   ```

STEP 10 | 从自定义映像创建新的 VM 系列防火墙。

```
az image create --resource-group <myResourceGroup> --name <myImage>
--source <resource-id-of-VM>
```

STEP 11 | 使用自定义映像部署 VM 系列防火墙后，请验证部署。

1. 您要使用从自定义映像启动 VM 时提供的凭据登录到防火墙。
2. 成功登录后，验证防火墙是否正在运行正确的 PAN-OS 版本，以及是否安装正确的内容和防病毒版本。

   ```
   show system info
   ```

STEP 12 | （可选）将自定义映像复制到另一个区域。

```
az image copy –source-resource-group <source-rg> –source-object-
name <pa-vm-image-name> –target-location <target-region> –target-
resource-group <destination-rg>
```

 ©2024 Palo Alto Networks, Inc.

使用 Azure 安全中心建议保护您的工作负载

Microsoft 已弃用 Azure 安全中心对合作伙伴解决方案的支持，并将其替换为 Azure Sentinel。

在为 Azure 安全中心启用的 Azure 订阅中部署新的工作负载时，Azure 安全中心可以使您通过两种方式保护这些工作负载。在一个工作流程中，Azure 安全中心建议您部署 VM 系列防火墙新实例以保护面向 Internet 的应用程序的工作负载。在另一个工作流程中，Azure 安全中心发现您在 Azure 订阅中部署的 VM 系列防火墙（合作伙伴安全解决方案），然后，您必须执行其他配置以将 VM 系列防火墙连接到 Azure 安全中心，这样您才能在仪表盘上查看警报。有关集成和每个工作流程的优缺点，请参阅 Azure 安全中心集成：

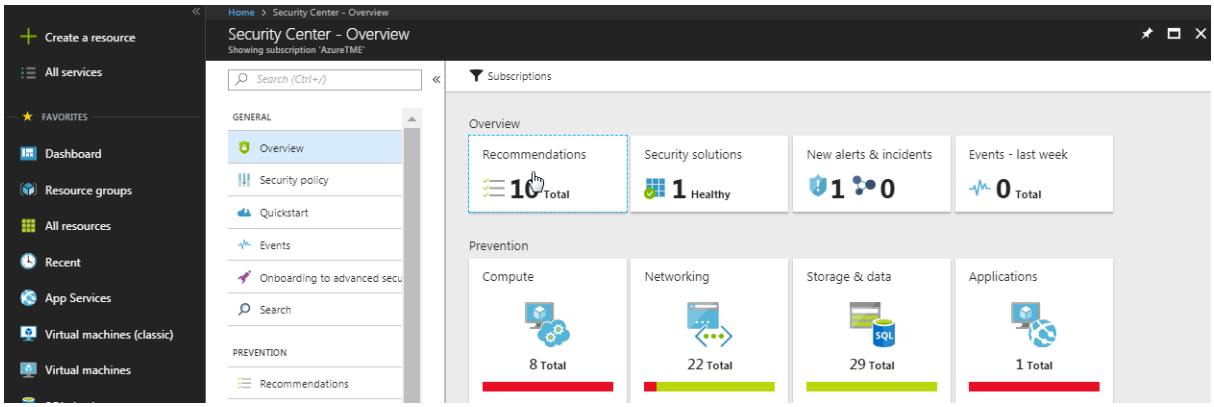
- 基于 Azure 安全中心建议部署 VM 系列防火墙
- 从 Azure 安全中心连接现有 VM 系列防火墙

基于 Azure 安全中心建议部署 VM 系列防火墙

Azure 安全中心扫描您的 Azure 资源，并为需要下一代防火墙的安全工作负载提供建议。此建议显示在仪表盘上，您可以随后从 Azure marketplace 部署新的 VM 系列防火实例，也可以使用 Azure CLI、 Powershell 或 ARM 模板。使用 Azure CLI、Powershell 或 ARM 模板实施的自定义部署的优点在于您可以将 VM 系列防火墙部署在与需要保护的工作负载相同的资源组中。使用 Azure marketplace 部署 VM 系列防火墙时，Azure 要求您仅将防火墙部署在新的资源组或是空的资源组。因此，随后，marketplace 部署要求您确保来自想要保护的工作负载的流量引导至不同资源组内的防火墙。

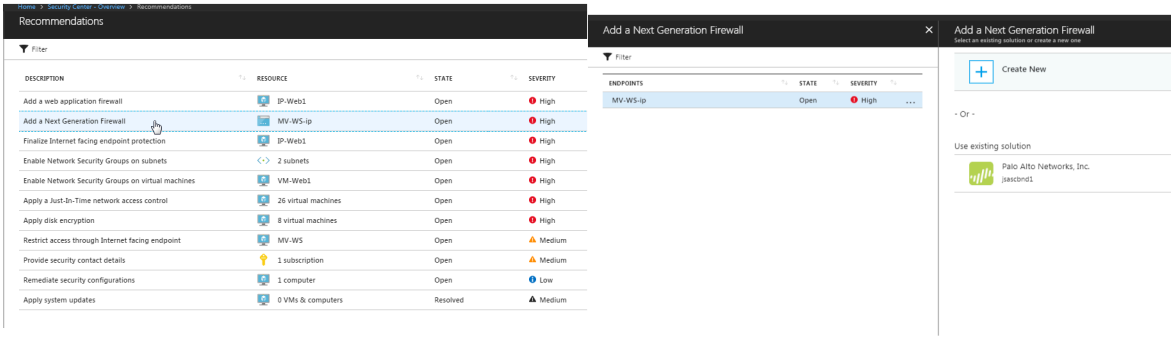
STEP 1 | 登录到 Azure 门户，并访问安全中心仪表盘。

STEP 2 | 选择 **Recommendations**（建议）。



 ©2024 Palo Alto Networks, Inc.

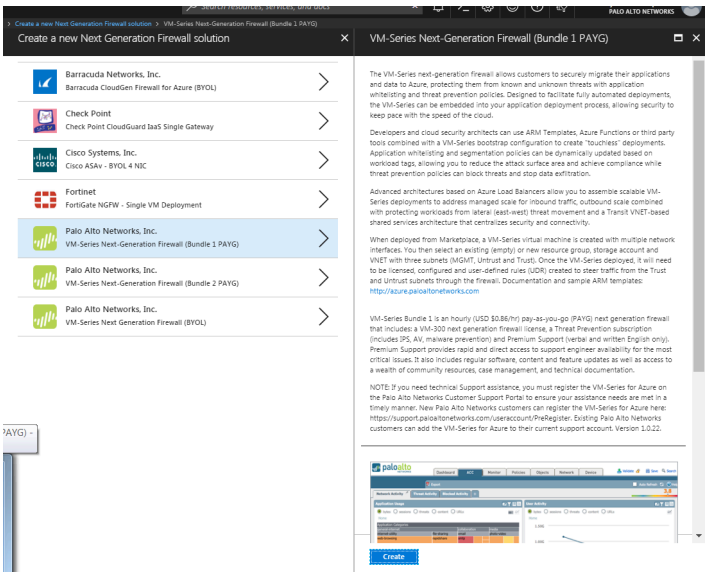
STEP 3 | 选择 **Add a Next Generation Firewall**（添加下一代防火墙），然后选择想要保护的工作负载。



STEP 4 | 选择是否想要部署 VM 系列防火墙新实例，还是使用 VM 系列防火墙现有实例。

要使用此工作流，请使用暴露于 Internet 的公共 IP 地址分段执行工作负载，并在新的资源组内部署一个 VM 系列防火墙实例。然后，删除分段执行的工作负载，并在已部署 VM 系列防火墙的资源组内部署生产工作负载。

- 若要 **Create New**（新建），请参阅从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）。
- 要 **Use existing solution**（使用现有解决方案），则选择之前部署的 VM 系列防火墙。



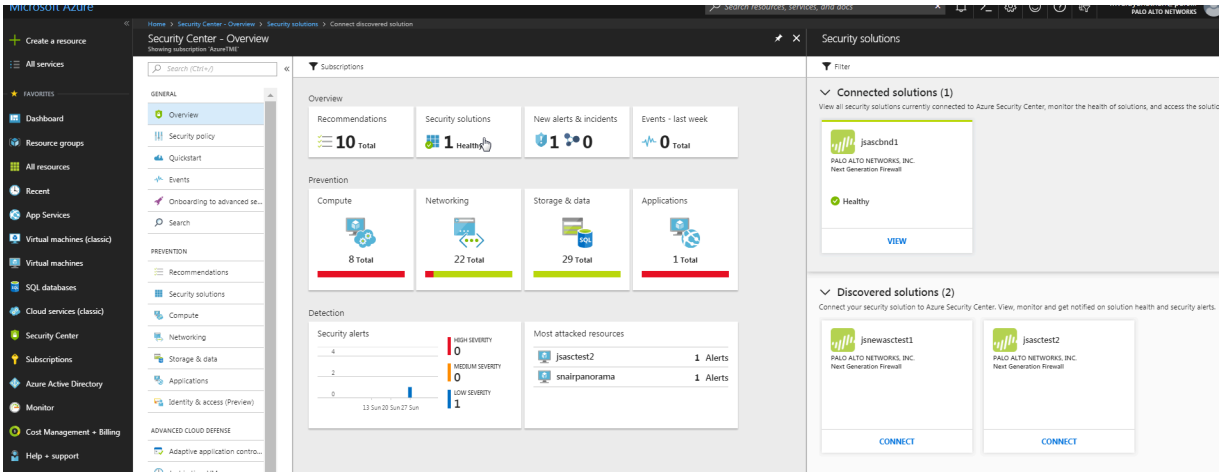
从 Azure 安全中心连接现有 VM 系列防火墙

当 Azure 安全中心检测到您已在 Azure 订阅中部署 VM 系列防火墙，则会将防火墙显示为安全解决方案。然后，您可以使用 Syslog 上的公共事件格式 (CEF) 将 VM 系列防火墙连接到安全中心，并查看安全中心仪表盘上显示为警报的防火墙日志。

STEP 1 | 登录到 Azure 门户，并访问安全中心仪表盘。

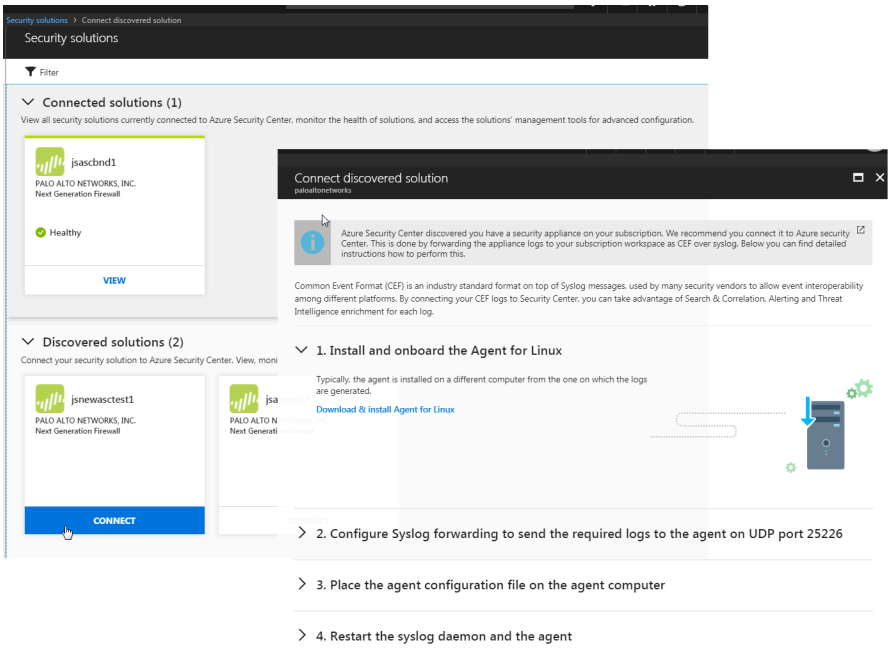
©2024 Palo Alto Networks, Inc.

STEP 2 | 选择安全解决方案以查看此 Azure 订阅内所有可用的 VM 系列防火墙。



STEP 3 | 展开发现的解决方案，并选择与要保护的工作负载相同的资源组内的 VM 系列防火墙实例，然后单击 **Connect**（连接）。

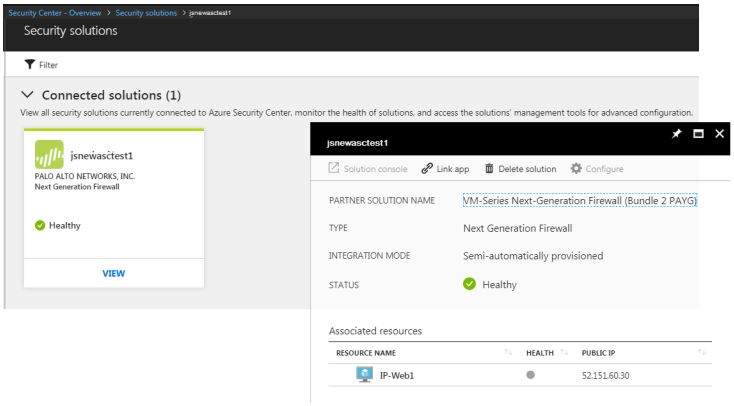
要查看安全中心仪表盘上显示为警报的防火墙日志，则需要按照屏幕上显示的四步流程执行。



©2024 Palo Alto Networks, Inc.

STEP 4 | VM 系列防火墙成功连接到安全中心后，VM 系列防火墙将出现在已连接的解决方案列表中。

单击查看以验证防火墙是否正在保护需要保护的工作负载。



使用 Panorama 转发日志到 Azure 安全中心

如果正在使用 Panorama 管理防火墙，则可以使用模板和设备组转发防火墙日志到 Azure 安全中心。使用默认的 Azure 安全中心日志转发，可将防火墙上生成的严重级别为低、中、高或关键的威胁和 WildFire 提交日志在 Azure 安全中心仪表盘上显示为安全警报。为此，您可以更有效地关注和分类警报，还可以设置粒度日志筛选器，以便仅转发您感兴趣的日志，或是仅转发高等严重性和关键性日志。此外，您还可以根据您的应用程序和安全需求，有选择性地将日志转发配置文件附加到少数安全策略规则。

要从 Panorama 启用 Azure 安全中心集成，则使用下列工作流程。

STEP 1 | 在 Panorama 上将防火墙添加为托管设备。

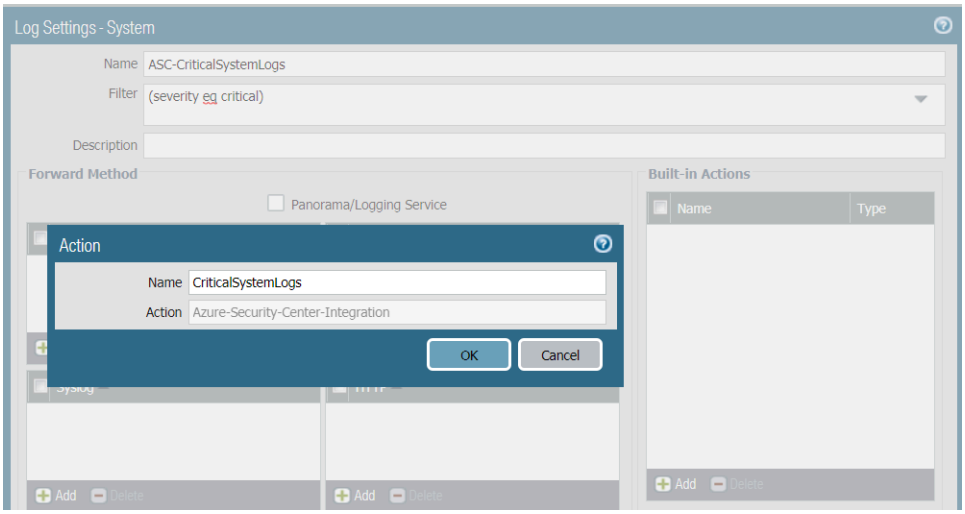
STEP 2 | 在 Panorama 上创建模板和设备组，以将日志转发设置推送到防火墙，从而转发日志到 Azure 安全中心。

©2024 Palo Alto Networks, Inc.

STEP 3 | 指定转发至日志记录服务的日志类型。

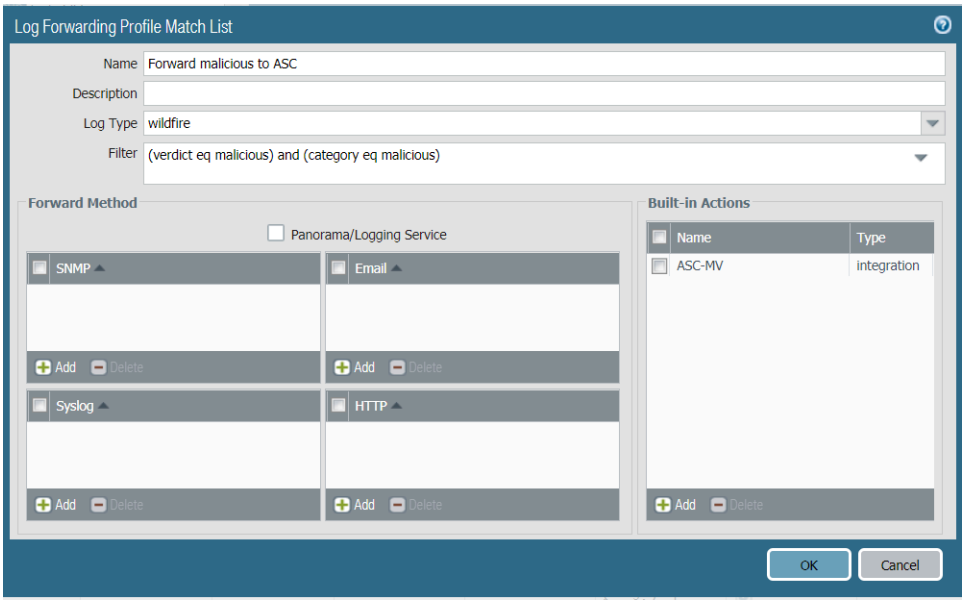
启用转发的方式取决于日志类型。对于基于策略匹配生成的日志，您可以使用设备组中的日志转发配置文件；而对于其他日志类型，则使用模板中的日志设置配置。

1. 配置系统、配置、User-ID 和 HIP 匹配日志转发。
   1. 选择 **Device**（设备）> **Log Settings**（日志设置）。
   2. 选择包含您想要转发日志到日志记录服务的防火墙 **Template**（模板）。
   3. 对于转发至日志记录服务的每种日志类型，请 **Add**（添加）匹配列表筛选器。为其指定 **Name**（名称），也可以定义一个 **Filter**（筛选器）。
   4. **Add**（添加）内置操作，然后输入 **Name**（名称）。Azure 安全中心集成将被自动选中.单击 **OK**（确定）。



   5. 单击 **OK**（确定）。
2. 配置策略匹配发生时生成的所有其他日志类型的转发，例如流量、威胁、WildFire 提交内容、URL 筛选、数据筛选和身份验证日志。要转发这些日志，您必须创建日志转发配置文件，并将其附加到想要转发日志所用的每个策略规则。
   1. 选择 **Device Group**（设备组），然后选择 **Objects**（对象）> **Log Forwarding**（日志转发）以 **Add**（添加）配置文件。在日志转发配置文件匹配列表，添加您想要转发的每种日志类型。
   2. 在内置操作中选择 **Add**（添加），以便在设备组中启用防火墙，从而将日志转发到 Azure 安全中心。

©2024 Palo Alto Networks, Inc.



3. 在您刚创建的设备组中创建基本安全策略规则，然后选择 **Actions**（操作）以附加您为转发日志所创建的日志转发配置文件到 Azure 安全中心。在防火墙具有接口、区域和基本安全策略之前，不会让任何流量通过，仅记录匹配安全策略的流量（默认）。
4. 对于您创建的每种规则，选择 **Actions**（操作），并选择允许防火墙转发日志到 Azure 安全中心的日志转发配置文件。

STEP 4 | 提交更改到 Panorama，并将其推送到您创建的模板和设备组。

STEP 5 | 验证防火墙日志是否正被转发到 Azure 安全中心。

1. 登录 Azure 门户，选择 **Azure Security Center**（**Azure** 安全中心）。
2. 检验您是否可以在 Azure 安全中心仪表盘上看到作为安全警报的防火墙日志。

©2024 Palo Alto Networks, Inc.

在 Azure Stack 中部署 VM 系列防火墙

您可以在 Azure Stack 中部署 VM 系列防火墙，以保护多层架构中应用程序之间的子网间流量，来自 Azure Stack 部署中服务器的出站流量。如果想要将 VM 系列防火墙用作保护发往 Azure Stack 部署中服务器的入站流量的网关，则必须在防火墙前面部署 NAT 设备，以接收入站流量并将其转发给防火墙。因为在 Azure Stack 上，您无法将公共 IP 地址分配给虚拟机的非主要接口（例如，VM 系列防火墙），因此，必须部署 NAT 设备。

Azure stack 上的 *VM* 系列防火墙不支持引导、*Azure Application Insights* 或 *Azure* 安全中心集成。

与公共 Azure 不同，您没有用于在 Azure Stack 中部署 VM 系列防火墙的解决方案模板。因此，必须使用 ARM 模板部署 VM 系列防火墙。首先，可以在 GitHub 上使用社区支持的 ARM 示例模板，然后开发自己的 ARM 模板用于生产部署。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 将 Markeplace 项目从 Azure 下载到 AzureStack。

要在 Azure Stack 中部署 VM 系列防火墙，则需要访问 VM 系列防火墙 PAN-OS 映像（8.1 或更高版本）的 BYOL 产品。您可以在连接的部署中将映像直接从 Azure Marketplace 下载到 Azure Stack。

STEP 2 | 访问 Azure Stack 门户。

您的 Azure Stack 运算符（服务提供商或组织内的管理员）应提供用于访问门户的正确 URL。

STEP 3 | 部署 VM 系列防火墙。

Azure Stack 不提供 VM 系列防火墙解决方案模板。因此，必须在 ARM 模板中引用上一步下载的映像以部署 VM 系列防火墙。首先，您可以在社区支持策略下部署 GitHub 上提供的 ARM 示例模板：

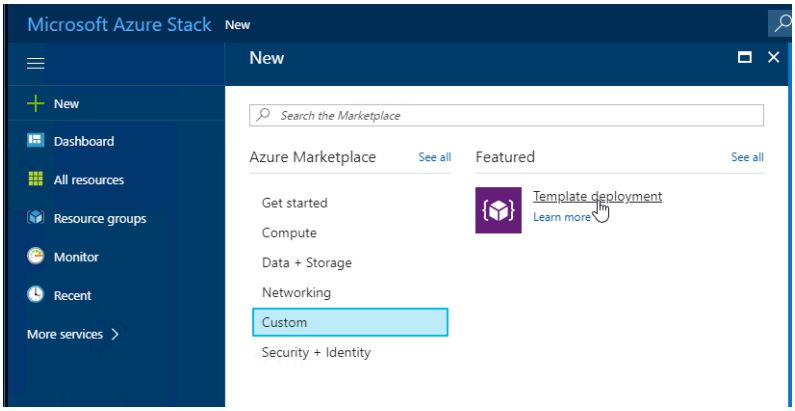
1. 获取 Azure Stack GitHub 模板示例。
   - 选择 azurestackdeploy.json 以查看内容。
   - 单击 Raw，并复制 JSON 文件的内容。
2. 部署 GitHub 示例模板。

   您可以将防火墙部署到空的现有资源组或新的资源组中。模板中的默认 VNet 是192.168.0.0/16，并且它部署了一个具有三个网络接口的 VM 系列防火墙，

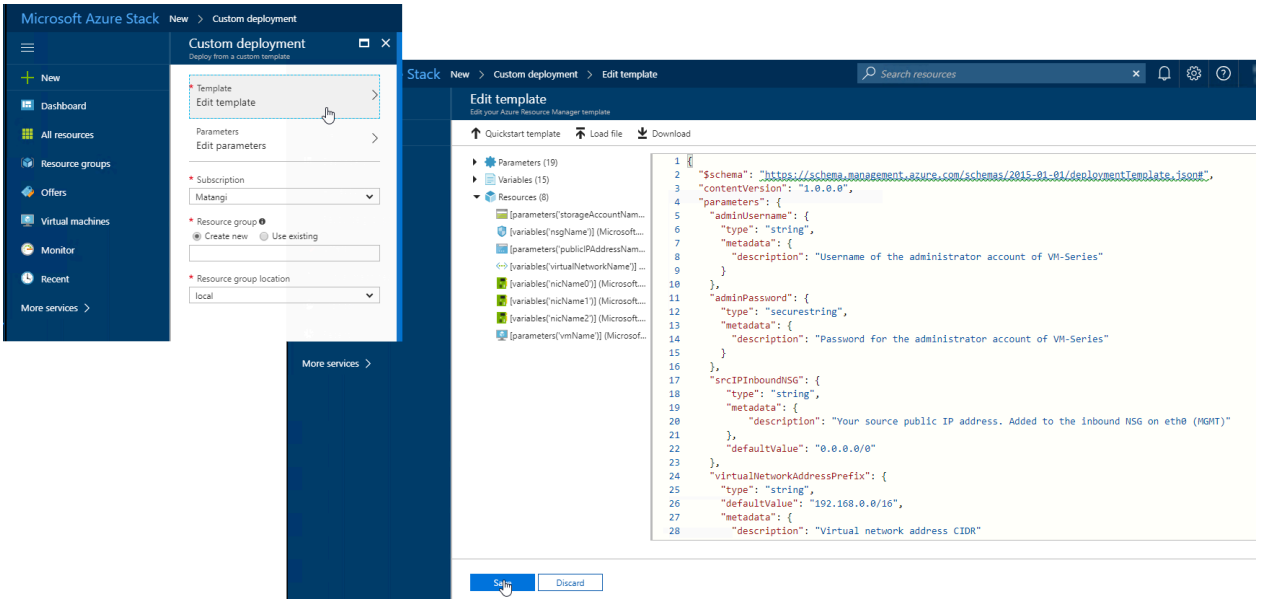
©2024 Palo Alto Networks, Inc.

即，192.168.0.0/24 子网上的一个管理接口以及 192.168.1.0/24 和 192.168.2.0/24 子网上的两个数据平面接口。可以根据需要自定义这些子网。

- 登录至 Azure Stack 门户。
- 选择 **New**（新建） > **Custom**（自定义） > **Template deployment**（模板部署）。

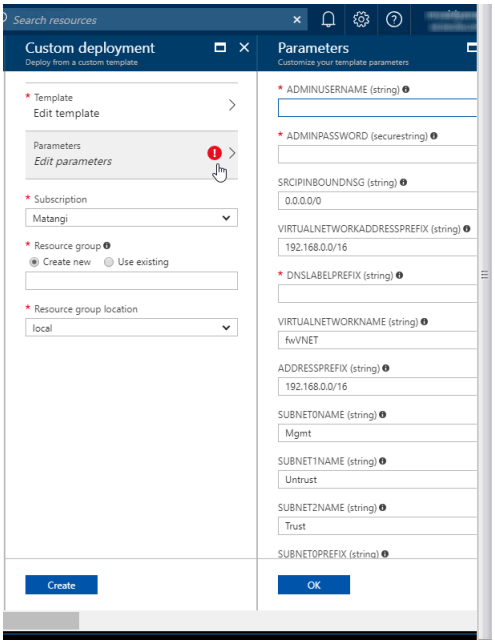


- **Edit template**（编辑模板），删除模板中所有现存内容，并粘贴先前复制的 JSON 模板内容，然后 **Save**（保存）。

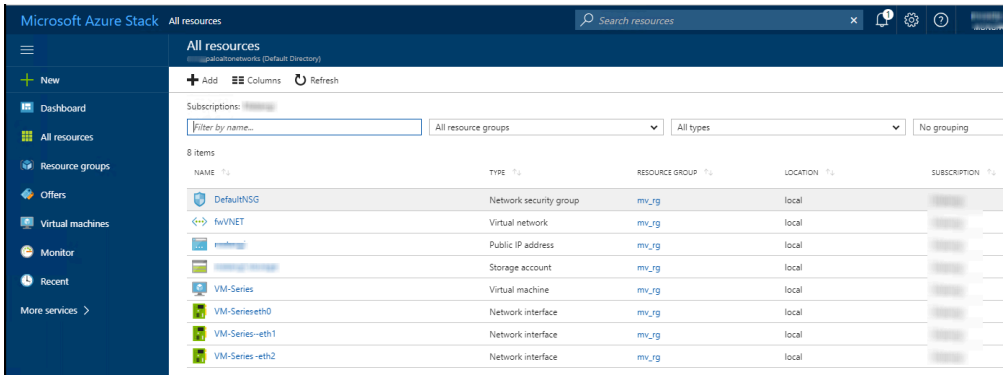


- **Edit parameters**（编辑参数），输入所需参数值，并在必要时修改默认值，然后单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.



- 选择想要使用的 **Subscription**（订阅），然后单击 **OK**（确定）。
- 选择为空的现有 **Resource Group**（资源组）或新建一个，然后单击 **OK**（确定）。
- 单击 **Create**（创建）。指示板上的新磁贴显示模板部署进度。



©2024 Palo Alto Networks, Inc.

STEP 4 | 后续步骤：

1. 登录防火墙的 Web 界面。

   使用 Web 浏览器提供的安全连接 (https) 登录到防火墙的 DNS 名称。输入之前定义的用户名/密码。您将看到证书警告；这属于正常情况。继续浏览网页。

2. 在 VM 系列防火墙上激活许可证。

   1. 创建支持帐户和注册 VM 系列防火墙（使用授权代码）。
   2. 在防火墙 Web 界面上，选择 **Device**（设备）> **Licenses**（许可证），然后选择 **Activate feature using authentication code**（使用授权代码激活功能）。
   3. 输入在支持门户上注册的容量授权代码。防火墙将连接到更新服务器 (updates.paloaltonetworks.com)，并下载许可证，然后自动重新启动。
   4. 重新登录到 **Dashboard**（仪表盘） Web 界面，并确认显示有效的 **Serial#**（序列号）。

      VM Mode（**VM** 模式）显示为 Microsoft Azure。

      如果显示“Unknown（未知）”一词，则表示此设备未经许可。要查看防火墙上的流量日志，您必须安装有效的容量许可证。

STEP 5 | 7

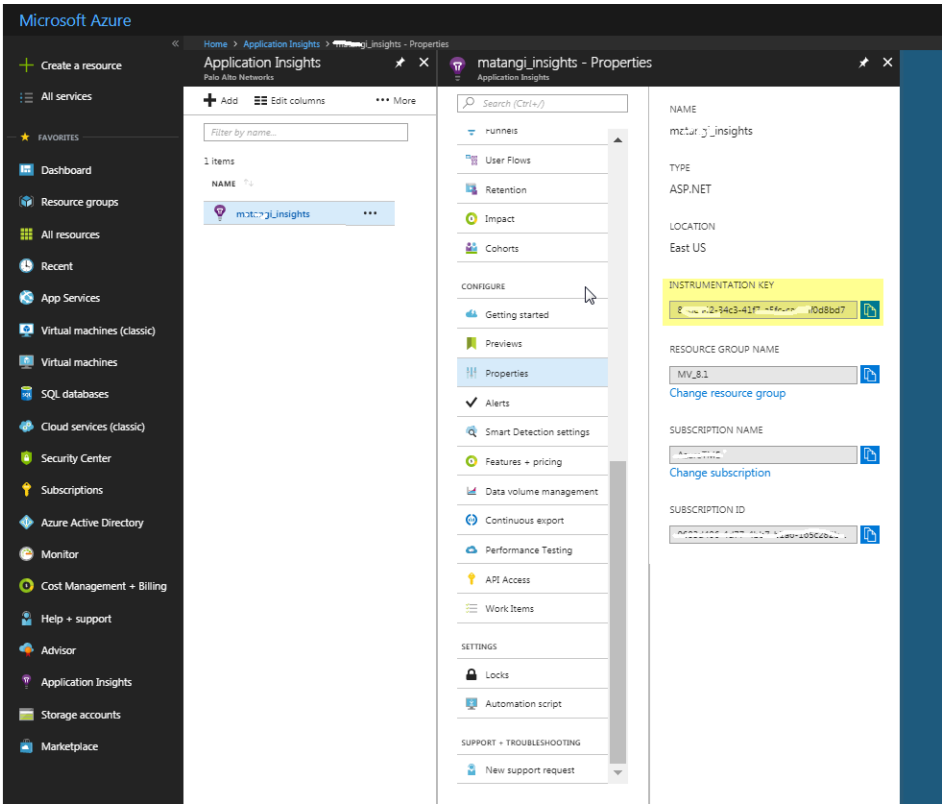
 ©2024 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用 Azure Application Insights

Azure 上的 VM 系列防火墙可以将自定义 PAN-OS 指标本身发布到您用于直接监控 Azure 门户中防火墙的 Azure Application Insights。通过这些指标，您可以评估用于设置警报的性能和使用模式，并采取行动以自动化用于启动或终止 VM 系列防火墙实例的事件。有关可用指标的说明，请参阅发布用于监控的自定义 PAN-OS 指标。

STEP 1 | 在 Azure 门户上创建 Application Insights实例以监控防火墙，并通过 **Configure**（配置）> **Properties**（属性）复制 **Instrumention Key**（检测密钥）。

防火墙需要使用此密钥以验证 Application Insights 实例，并向其发布指标。有关所需的权限，请参阅VM 系列在 Azure 上的服务主体权限。

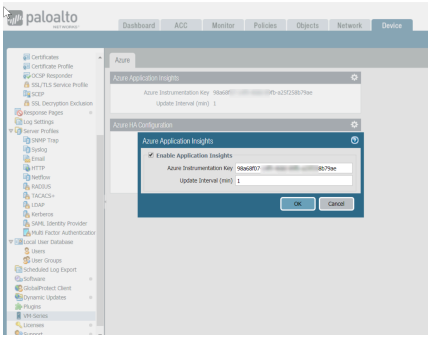


©2024 Palo Alto Networks, Inc.

STEP 2 | 启用防火墙以发布指标到您的 Application Insights 实例。

1. 登录到 Azure 上的 VM 系列防火墙。
2. 选择 **Device**（设备） > **VM-Series**（**VM** 系列） > **Azure**。
3. 编辑 **Azure Application Insights**（**Azure Application Insights**），然后输入之前复制的检测密钥。

   指标发布的默认间隔时间为 5 分钟。您可以将此时间更改为 1-60 分钟。



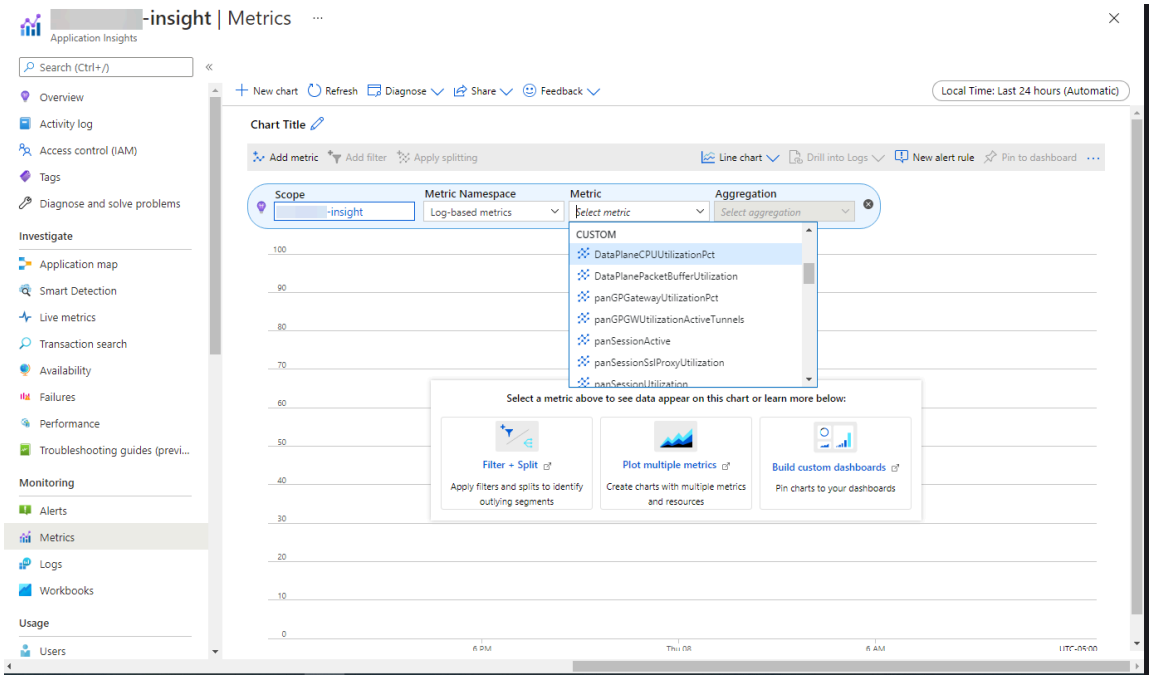
4. **Commit**（提交）更改。

   防火墙会生成一个系统日志，以记录 Azure Application Insights 身份验证成功或失败。

©2024 Palo Alto Networks, Inc.

STEP 3 | 检验您是否可以查看 Azure Application Insights 仪表盘上的指标。

1. 在 Azure 门户上，选择 Application Insights 实例，然后选择 **Monitoring**（监控） > **Metrics**（指标）以查看 PAN-OS 自定义指标。



2. 选择您想用于监控趋势和触发警报的指标。有关浏览 Application Insights 上指标的详细信息，请参阅 Microsoft Azure 文档。

 ©2024 Palo Alto Networks, Inc.

在 Azure 上监控

您可以通过 Microsoft® Azure® 上的监控动态更新安全策略规则，以便在 Azure 订阅中部署的所有资产上一致地实施安全策略。要启用此功能，需要安装适用于 Azure 的 Panorama 插件，并在 Panorama 和 Azure 订阅之间启用 API 通信。然后，Panorama 收集用于所有 Azure 资产的 IP 地址到标记映射，并将 Azure 资源信息推送或分发到 Palo Alto Networks® 防火墙。

- 关于在 Azure 上监控
- 在 Panorama 上设置用于监控的 Azure 插件
- 使用 Azure 上 Panorama 插件监控的属性

关于在 Azure 上监控

在 Azure 公共云中部署或终止虚拟机时，您可以使用适用于 Azure 的 Panorama 插件对这些工作负载统一执行安全策略。

用于 Azure 的 Panorama 插件为扩展而构建，允许最多可监控 Azure 公共云上的 100 个 Azure 订阅。您可以通过此插件将 Panorama 用作轮询订阅标记的锚，然后将元数据（IP 地址到标记映射）分发到设备组中的许多防火墙。因为 Panorama 与您的 Azure 订阅进行通信以检索 Azure 资源信息，因此您可以简化云环境中使用的 API 调用数量。虽然您可以在防火墙上本地定义安全策略，但使用 Panorama 和插件可以集中化安全策略管理，从而确保混合和云端本地架构使用的策略一致。

请参阅兼容性矩阵中的 Panorama 插件版本信息。

在 Panorama 上设置用于监控的 Azure 插件

要找到组织在 Azure 云中部署的所有工作负载，则必须在 Panorama 上安装 Azure 插件，并配置促使 Panorama 对 Azure 订阅进行身份验证且检索 Azure 工作负载上的信息的监控定义。Panorama 检索 Azure 资源的主要专用 IP 地址以及关联标记。有关 Panorama 支持的元数据元素列表，请参阅在 Azure 上使用 Panorama 插件监控的属性。

Panorama 获取属性后将资源信息从 Panorama 推送到防火墙，因此必须将防火墙（硬件或 VM 系列）添加为 Panorama 上的托管设备，并将防火墙分组到一个或多个设备组。然后，可以指定属于通知组的设备组，这是监控定义的配置元素，Panorama 可用于注册从 Azure 检索到的 IP 地址到标记映射。

最后，要在 Azure 工作负载中统一实施安全策略，则必须设置动态地址组，并在用于允许或拒绝流向 Azure 资源 IP 地址的流量的策略规则中加以引用。为了从 Panorama 集中简化您的配置，管理策略和对象，您可以在 Panorama 上定义动态地址组和安全策略规则，并将其推送到防火墙，而不是对每个防火墙上的动态地址组和安全策略规则进行本地管理。

Azure 插件专用于监控 *Azure* 公共云上的 *Azure* 资源。不支持 *Azure Government* 或 *Azure China*。

©2024 Palo Alto Networks, Inc.

- 规划采用 Azure 插件进行的 VM 监控列表
- 安装 Azure 插件
- 配置用于监控的 Azure 插件

规划采用 **Azure** 插件进行的监控列表

- 设置 Active Directory 应用程序和服务主体以启用 API 访问。对于与 Azure API 进行交互并在工作负载上收集信息的 Panorama，则需要创建 Azure Active Directory 服务主体。此服务主体拥有对 Azure AD 进行身份验证并访问订阅内资源的所需权限。

  要完成此设置，您必须拥有通过 Azure AD 租户注册应用程序，并将此应用程序分配给订阅中角色的权限。如果没有所需权限，请要求 Azure AD 或订阅管理员创建一个具有读取者 IAM 角色或 VM 系列在 Azure 上的服务主体权限中指定的自定义权限的服务主体。
- 对于服务主体而言，订阅 ID 必须是唯一的。Panorama 运行您仅使用一个服务主体来监控 Azure 订阅。您最多可以监控 100 个 Azure 订阅，其中包含 100 个服务主体资源。从 Panorama Azure 插件版本 3.2.0 开始，您可以监视多达 500 个 Azure 订阅。请注意下表中所述的处理时间。

	订阅数				
	100	**200**	**300**	**400**	**500**
系统资源利用率	• CPU：22% • 内存：0.025 MB	• CPU：23.8% • 内存：0.025 MB	• CPU：31.8% • 内存：0.025 MB	• CPU：28.6% • 内存：0.025 MB	• CPU：39.2% • 内存：0.025 MB
处理所有监视定义的平均时间	1 小时 15 分钟	2 小时 30 分钟	3 小时 30 分钟	4 小时	5 小时
平均标记更新处理时间	5 分钟	10 分钟	15 分钟	20 分钟	25 分钟

上表中的信息是在具有 *8* 个 *vCPU* 和 *32 GB* 内存的实例上获取的。

©2024 Palo Alto Networks, Inc.

- Panorama 最多可以将 8000 个 IP 地址到标记映射推送到分配给设备组的防火墙或虚拟系统。查看 Panorama 和托管防火墙的要求：
  - 最低系统要求（请参阅兼容性矩阵中的 Panorama 插件信息）：

    运行 Panorama 8.1.3 或更高版本的 Panorama 虚拟设备或基于硬件的 Panorama 设备，具有用于管理防火墙的有效支持许可证和设备管理许可证。

    运行 PAN-OS 8.0 或 8.1 的许可的下一代防火墙。
  - 必须在 Panorama 上添加防火墙作为托管设备，并创建设备组，这样，您可以配置 Panorama 以将检索到的信息通知这些组。设备组可以包括 VM 系列防火墙或是硬件防火墙上的虚拟系统。
  - Panorama 插件可以检索并注册的标记数如下所示：

    在管理运行 PAN-OS 8.1.3 或更低版本的防火墙的 Panorama 8.1.3 或更高版本上，设备组中包含的防火墙或虚拟系统可以具有每个包含 10 个标记的 7000 个 IP 地址，或每个包含 15 个标记的 6500 个 IP 地址。

    在管理运行 PAN-OS 8.0.x 的防火墙的 Panorama 8.1.3 或更高版本上，共计 2500 个 IP 地址，每个地址包含 10 个标记。
    - 如果 Panorama 设备具有高可用性配置，则必须手动在两个 Panorama 对等上安装相同版本的 Azure 插件。

      您只能在 *Panorama* 主动对等上配置 *Azure* 插件。提交时，配置同步到 *Panorama* 被动对等。仅 *Panorama* 主动对等轮询您为监控配置的 *Azure* 订阅。

安装 **Azure** 插件

要开始监控 Azure 上的监控，则需要在 Panorama 上下载并安装 Azure 插件。如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。

如果当前有安装好的 *Panorama* 插件，则安装（或卸载）两一个插件的过程需要使用 *Panorama* 重启才能提交更改。因此，在规划的维护窗口安装其他插件以允许重启。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件

©2024 Palo Alto Networks, Inc.

- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

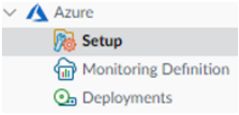
  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 登录到 Panorama Web 界面，选择 **Panorama** > **Plugins**（插件），然后单击 **Check Now**（立即检查）以获取可用的插件列表。

STEP 2 | 选择 **Download**（下载），然后 **Install**（安装）插件。

安装成功后，Panorama 将刷新，**Panorama**选项卡上会显示 Azure 插件。



STEP 3 | 重新启动 Panorama。

选择 **Panorama** > **Setup**（设置） > **Operations**（操作） > **Reboot Panorama**（重新启动 **Panorama**）

配置用于监控的 Azure 插件

要开始监控 Azure 公共云部署中的资源，则必须在安装 Azure 插件之后创建监控定义。此定义指定有权在想要监控的 Azure 订阅中访问资源的服务主体，以及包含 Panorama 将检索的所有 IP 地址到标记映射推送到的防火墙的通知组。为了实施策略，必须随后创建动态地址组，并在安全策略中加以引用。您可通过动态地址组筛选想要匹配的标记，这样，防火墙可以获取注册用于标记的主要专用 IP 地址，然后基于定义的策略规则允许或拒绝往返于工作负载之间的流量。

STEP 1 | 登录到 Panorama Web 界面。

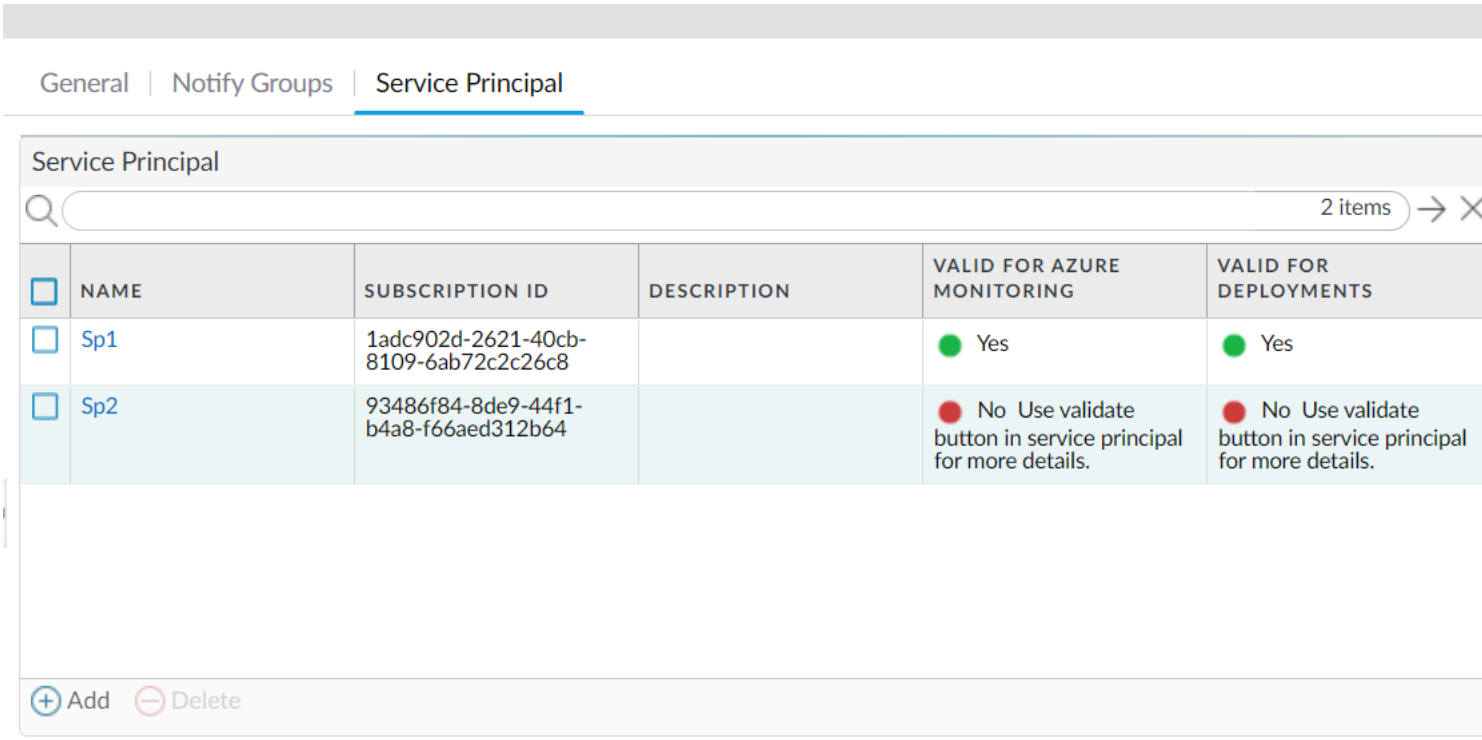
 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在 Azure 上设置用于启动监控的以下对象。

- 添加服务主体。

  服务主体是您在 Azure 门户上创建的服务帐户。此帐户可添加到 Azure AD，且有一定的权限，可访问和监控 Azure 订阅中的资源。

  1. 选择 **Panorama** > **Plugins**（插件） > **Azure** > **Setup**（设置） > **Service Principal**（服务主体） > **Add**（添加）。

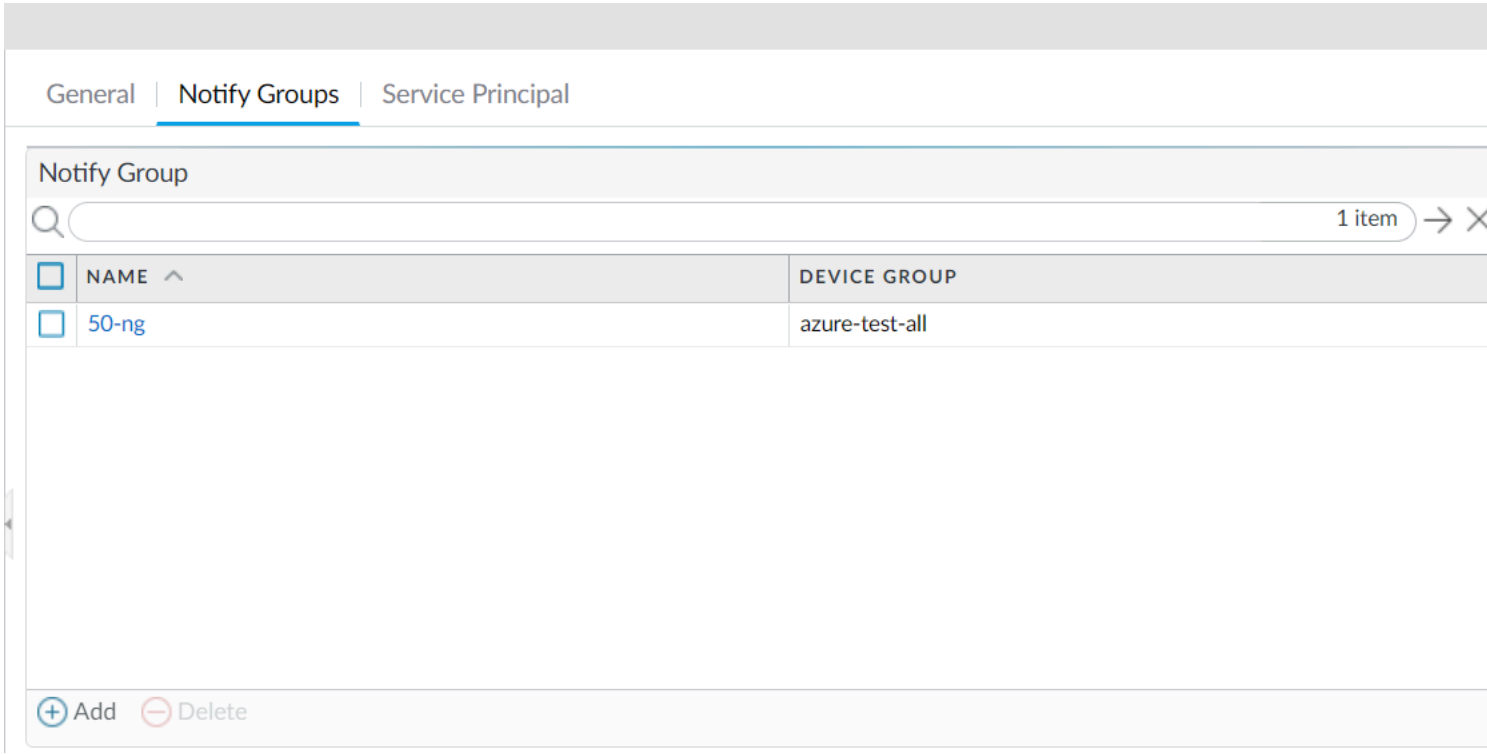


  2. 输入标识服务帐户的 **Name**（名称），也可选择输入 **Description**（说明）。
  3. 输入想要监控的 Azure 订阅的 **Subscription ID**（订阅 **ID**）。您必须登录到您的 Azure 门户才能获取此订阅 ID。
  4. 输入 **Client Secret**（客户端密钥），并重新输入以进行确认。
  5. 输入 **Tenant ID**（租户 **ID**）。租户 ID 是您在设置 Active Directory 应用程序时保存的 Directory ID。
  6. 单击 **Validate**（验证）以验证输入的密钥和 ID 是否有效，Panorama 是否可以通过 API 与 Azure 订阅进行通信。

- 添加通知组。

  1. 选择 **Panorama** > **Plugins**（插件） > **Azure** > **Setup**（设置） > **Notify Groups**（通知组） > **Add**（添加）。

©2024 Palo Alto Networks, Inc.



2. 输入用于标识 Panorama 向其推送检索的信息的防火墙组的 **Name**（名称），也可选择输入 **Description**（说明）。
3. 选择作为防火墙或虚拟系统组的 **Device Groups**（设备组），以便 Panorama 将其从 Azure 订阅检索的信息（IP 地址到标记映射）推送到该组。这些防火墙可使用此更新确定构成策略中所引用动态地址组的成员的最新列表。

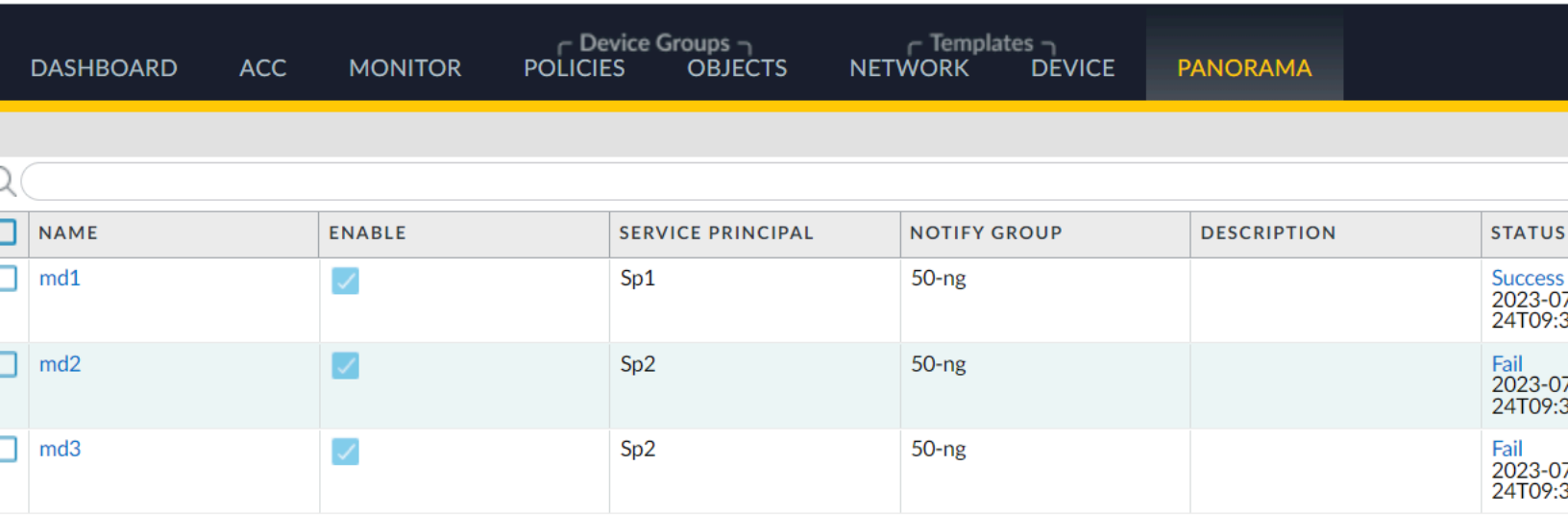
   仔细考虑您的设备组。

   - 因为监控定义仅包括一个通知组，因此必须选中通知组内所有的相关设备组。如果想要注册 Panorama 已推送到通知组内防火墙的标记，则必须删除监控定义。
   - 要将标记注册到启用用于多个虚拟系统的防火墙上的所有虚拟系统，则必须将每个虚拟系统添加到 Panorama 上的单独设备组，并分配设备组到通知组。如果将所有虚拟系统分配到一个设备组，则 Panorama 仅将标记注册到一个虚拟系统中。
4. 验证插件上是否启用监控。必须为 Panorama 启用此设置，以便与 Azure 公共云进行通信，从而进行监控。

   Enable Monitoring（启用监控）复选框位于 **Panorama** > **Plugins**（插件） > **Azure** > **Setup**（设置） > **General**（常规）上。

©2024 Palo Alto Networks, Inc.

STEP 3 | 创建 **Monitoring Definition**（监控定义）。



添加新的监视定义时，默认情况下将启用该定义。

- 选择 **Panorama** > **Plugins**（插件） > **Azure** > **Monitoring Definition**（监视定义），以便 **Add**（添加）新定义。
- 输入用于标识使用此定义的 Azure 订阅的 **Name**（名称），也可选择输入 **Description**（说明）。
- 选择 **Service Principal**（服务主体）和 **Notify Group**（通知组）。

  Panorama 需要您在服务主体配置中指定的密钥和 ID 才能生成 Azure Bearer 令牌。此令牌可在 API 调用标头中使用，以便收集工作负载上的信息。

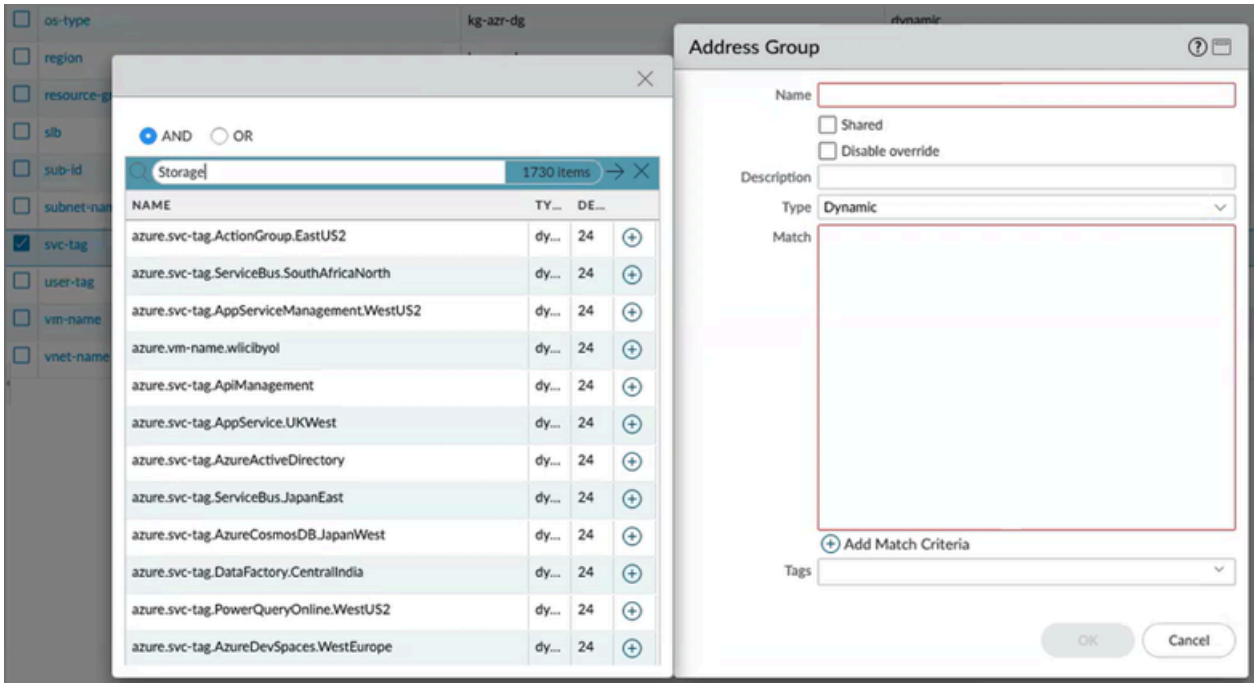
STEP 4 | 在 Panorama 上 **Commit**（提交）更改。

验证监控定义的状态是否显示为成功。如果失败，则验证是否输入正确的 Azure 订阅 ID，并为服务主体提供正确的密钥和 ID。

©2024 Palo Alto Networks, Inc.

STEP 5 | 验证是否可以在 Panorama 上查看信息，并定义动态地址组的匹配条件。

某些浏览器扩展程序可能会阻止 *Panorama* 与 *Azure* 之间的 *API* 调用，从而阻止 *Panorama* 接收匹配条件。如果 *Panorama* 未显示匹配条件且您正在使用浏览器扩展程序，请禁用扩展程序和同步动态对象以填充 *Panorama* 可用的标记。



在 *HA* 故障转移时，新激活的 *Panorama* 尝试重新连接到 *Azure* 云，并检索所有监控定义的标记。如果重新连接一个监视定义时出现错误，*Panorama* 会生成系统日志消息：

```
Unable to process subscriptions after HA switch-over;
 user-intervention required。
```

看到此错误时，您必须登录到 *Panorama* 并解决问题，例如删除无效的订阅或提供有效的凭据，然后提交更改，以便 *Panorama* 重新连接并检索所有监控定义的标记。即使 *Panorama* 从 *Azure* 云断开连接，防火墙也拥有在故障转移前已检索到的所有标记列表，并继续在该 *IP* 地址列表上执行策略。只有当您删除监控定义时，*Panorama* 才会删除所有与订阅相关联的标记。最佳实践是，要监控此问题，可以从 *Panorama* 配置面向操作的日志转发到 HTTP 定义，这样，您可以立即采取行动。

©2024 Palo Alto Networks, Inc.

使用 Azure 上 Panorama 插件监控的属性

使用 Azure 的 Panorama 插件时，Panorama 在 Microsoft® Azure® 部署中的虚拟机上收集以下元数据元素或属性集。Panorama 最多可为每个 VM 检索共计 32 个标记，包括 11 个预定义标记和最多 21 个用户定义的标记。

标记的最大长度为 *127* 个字符。如果标记的长度超过 *127* 个字符，则 *Panorama* 无法检索标记，并将其注册到防火墙上。此外，标记不得包含非 *ASCII* 特殊字符，例如 *{* 或 *"*。

在适用于 Azure 版本的所有 Panorama 插件上监控以下属性。

虚拟机

VM 监控	示例
VM 名称	azure-tag.vm-name.web_server1
网络安全组名称	azure-tag.nsg-name.myNSG
OS 类型	azure-tag.os-type.Linux
OS 发行商	azure-tag.os-publisher.Canonical
OS 产品	azure-tag.os-offer.UbuntuServer
OS SKU	azure-tag.os-sku.14.04.5-LTS
子网	azure-tag.subnet.webtier
VNet	azure-tag.vnet.untrustnet
Azure 区域	azure-tag.region.east-us
资源组名称	azure-tag.resource-group.myResourceGroup
订阅 **ID**	azure.sub-id.93486f84-8de9-44f1-b4a8-f66aed312b64
用户定义的标记 最多支持 21 个用户定义的标记。用户定义的标记按字母顺序排序，且前 21 个标记可用于 Panorama 和防火墙。	azure-tag.mytag.value

负载均衡器

 ©2024 Palo Alto Networks, Inc.

Azure 版本 3.0 或更高版本上的 Panorama 插件支持每个应用程序网关和标准负载均衡器（公用和专用 IP 地址）的标签。每个负载均衡器都具有资源组、负载均衡器和区域的预定义标记，并且最多支持 21 个特定于负载均衡的用户定义的标记。

负载均衡器标记	示例
负载均衡器	azure.<type>.myLoadBalancer
Azure 区域	azure-tag.region.east-us
资源组名称	azure-tag.resource-group.myResourceGroup
用户定义的标记 最多支持 21 个用户定义的标记。用户定义的标记按字母顺序排序，且前 21 个标记可用于 Panorama 和防火墙。	azure-tag.mytag.value

子网**/VNET**

Azure 版本 3.0 或更高版本上的 Panorama 插件支持订阅中每个子网和 VNET 的标记。每个子网和 VNET 标记都与整个 IP CIDR 范围关联，因此您可以根据 CIDR 范围而不是单个 IP 地址创建策略。该插件查询订阅中的每个子网和 VNET，并为其创建标记。

子网和 **VNET** 标记	示例
子网名称	azure.subnet-name.web
VNET 名称	azure.vnet-name.myvnet

服务标记监控

Azure 版本 3.0 上的 Panorama 插件支持服务标记。

Azure 服务标记可简化 Azure 虚拟机和 Azure 虚拟网络的安全性，因为您可以将网络访问限制为仅要使用的 Azure 服务。服务标记表示特定 Azure 服务的一组 IP 地址前缀。例如，一个标记可以表示所有存储 IP 地址。

该插件每天进行一次 API 调用（上午 5:00，世界标准时间），以便从 Azure 门户检索所有服务标记，解析负载以形成 IP 服务映射，并将映射存储在插件数据库中。将映射传递到 configd，然后传递到 Panorama。如果 API 调用无法返回服务信息，则该插件将根据 **`service_tags_public.json`** 的内容形成 IP 服务映射。该插件日志将报告 IP 服务映射、每日检索或 JSON 文件的来源。

该插件还更新新安装插件、提交事件以及监控定义添加或删除的服务标记。

IP 服务映射示例如下所示：

©2024 Palo Alto Networks, Inc.

```
Service Name:AppServiceManagementazure.svc-tag.<service-name>Example:
     azure.svc-tag.AppServiceManagement.WestUS2 Public IP
 CIDRs:    13.166.40.0/26     54.179.89.0/18
```


©2024 Palo Alto Networks, Inc.

在 Azure 上设置主动/被动 HA

您可以采用主动/被动高可用性 (HA) 配置方式在 Azure 上配置一对 VM 系列防火墙。对于 Azure 上的 HA，您必须在同一 Azure 资源组中部署两个防火墙 HA 对等，并且必须在两个 HA 对等上安装相同版本的 VM 系列插件。

- 在 Azure 上设置主动/被动 HA（北向南和东向西流量） — 如果您在 Azure 基础架构上部署面向 Internet 的应用程序且需要保护北向南流量，则需要使用浮动 IP 地址保护发生故障转移时的流量。此浮动 IP 地址用于启动外部连接，始终附加到主动对端。在发生故障转移时，分离 IP 地址并将其重新附加到当前主动对等的过程可能需要几分钟。
- 在 Azure 上设置主动/被动 HA（仅限东向西流量） — 如果您的应用程序访问和安全要求包含在 Azure 基础架构中且只需要保护东向西流量，则不需要使用浮动 IP 地址。相反，HA 实施会自动重新配置 Azure 路由表中的 UDR，以提供更快的故障转移时间。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

要在 Azure 上的 VM 系列防火墙上启用高可用性，您必须创建包含下表中列出的权限的 Azure Active Directory 应用程序和服务主体。

Azure HA 类型	权限	角色范围
辅助 IP 地址移动 HA	**"Microsoft.Authorization/*/read""Microsoft.Compute/virtualMachines/read""Microsoft.Network/networkInterfaces/*""Microsoft.Network/networkSecurityGroups/*""Microsoft.Network/virtualNetworks/join/action""Microsoft.Network/virtualNetworks/subnets/join/action"** 仅当您已将公共 IP 地址分配给任何数据接口时才需要以下权限。建议使用标准 SKU 接口。 **"Microsoft.Network/publicIPAddresses/join/action""Microsoft.Network/publicIPAddresses/read""Microsoft.Network/publicIPAddresses/write"**	• 部署 VM 的虚拟网络 • 两个 VM 系列防火墙 • 两个 VM 系列防火墙的 NIC • 网络安全组 • VM 系列防火墙的公共 IP 地址

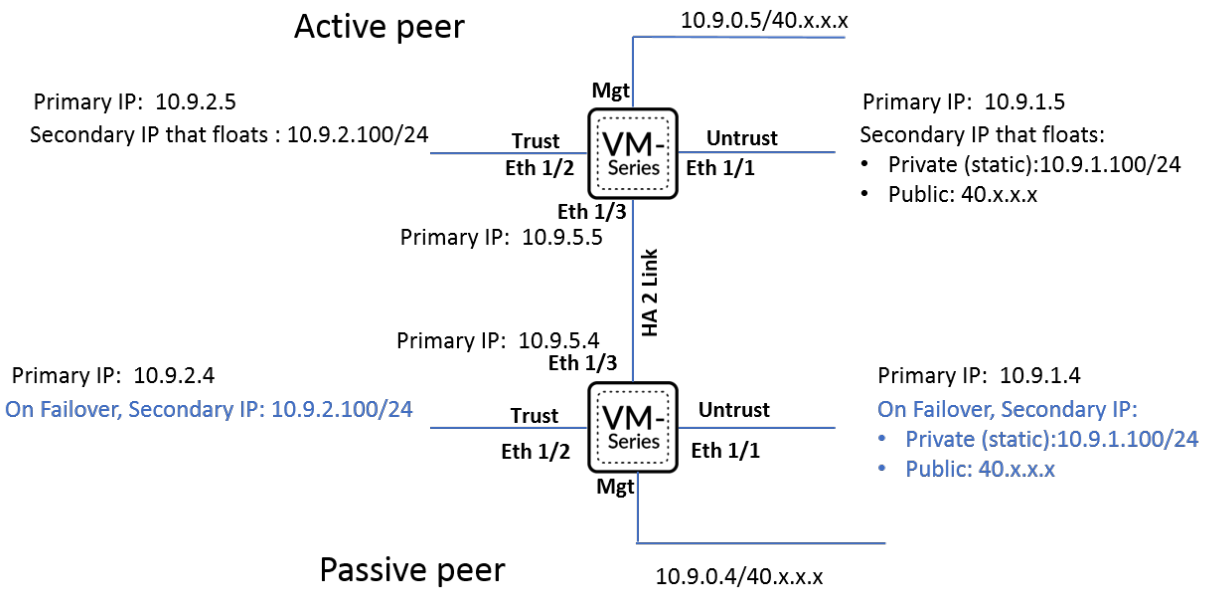
©2024 Palo Alto Networks, Inc.

Azure HA 类型	权限	角色范围
UDR HA	**"Microsoft.Authorization/*/read""Microsoft.Compute/virtualMachines/read""Microsift.Network/routeTables/*"**	• 两个 VM 系列防火墙 • 两个 VM 系列防火墙的 NIC • 与 UDRR 相关联的路由表
辅助 IP 地址移动和 UDRR	**"Microsoft.Authorization/*/read""Microsoft.Compute/virtualMachines/read""Microsoft.Network/networkInterfaces/*""Microsoft.Network/networkSecurityGroups/*""Microsoft.Network/routeTables/*""Microsift.Network/virtualNetworks/join/action""Microsoft.Network/virtualNetworks/subnets/join/action"** 仅当您已将公共 IP 地址分配给任何数据接口时才需要以下权限。建议使用标准 SKU 接口。 **"Microsoft.Network/publicIPAddresses/join/action""Microsoft.Network/publicIPAddresses/read""Microsoft.Network/publicIPAddresses/write"**	• 部署 VM 的虚拟网络 • 两个 VM 系列防火墙 • 两个 VM 系列防火墙的 NIC • 网络安全组 • VM 系列防火墙的公共 IP 地址 • 与 UDRR 相关联的路由表

在 Azure 上设置主动/被动 HA（北向南和东向西流量）

如果您要保护 Azure 基础架构中应用程序的北向南流量，请将此工作流程与可以从一个对等快速移动到另一个对等的浮动 IP 地址配合使用。由于无法在 Azure 上移动与防火墙主接口关联的 IP 地址，因此，需要分配可用作浮动 IP 地址的 辅助 IP 地址。当主动防火墙发生故障时，浮动 IP 地址会从活动防火墙移动到被动防火墙，以便被动防火墙一旦成为活动对等就可以无缝保护流量。除浮动 IP 地址外，HA 对等还需要 HA 链接 — 一个控制链路 (HA1) 和一个数据链路 (HA2) — 用于同步数据和维护状态信息。

©2024 Palo Alto Networks, Inc.



- 为启用 HA 设置防火墙
- 在 Azure 上的 VM 系列防火墙上配置主动/被动 HA

为启用 HA 设置防火墙

收集在 Azure 上的 VM 系列防火墙上配置 HA 的以下详细信息。

设置 Active Directory 应用程序和服务主题以启用编程 API 访问。

- 为了让防火墙与 Azure API 交互，需要创建 Azure Active Directory 服务主体。该服务主体具有对 Azure AD 进行身份验证和访问订阅中的资源的权限。要完成此设置，必须具有向 Azure AD 租户注册应用程序的权限，并将应用程序分配给订阅的角色。如果您没有所需权限，请要求 Azure AD 或订阅管理员创建服务主体。有关所需的权限，请参阅上表。复制以下详细信息以供稍后在此工作流程中使用：
  - 客户端 **ID** — 与 Active Directory 相关联的应用程序 ID（在 Azure 门户中，单击 **Home**（主页） > **Azure Active Directory** > **App registrations**（应用程序注册），然后选择应用程序并复制 ID）。
  - 租户 **ID** — 与 Active Directory 相关联的应用程序 ID（在 Azure 门户上，单击 **Home**（主页） > **Azure Active Directory** > **Properties**（属性） > **Directory ID**（目录 **ID**），然后选择应用程序并复制 ID）。
  - **Azure** 订阅 **ID** — 已部署防火墙的 Azure 订阅。您必须登录到您的 Azure 门户才能获取此订阅 ID。

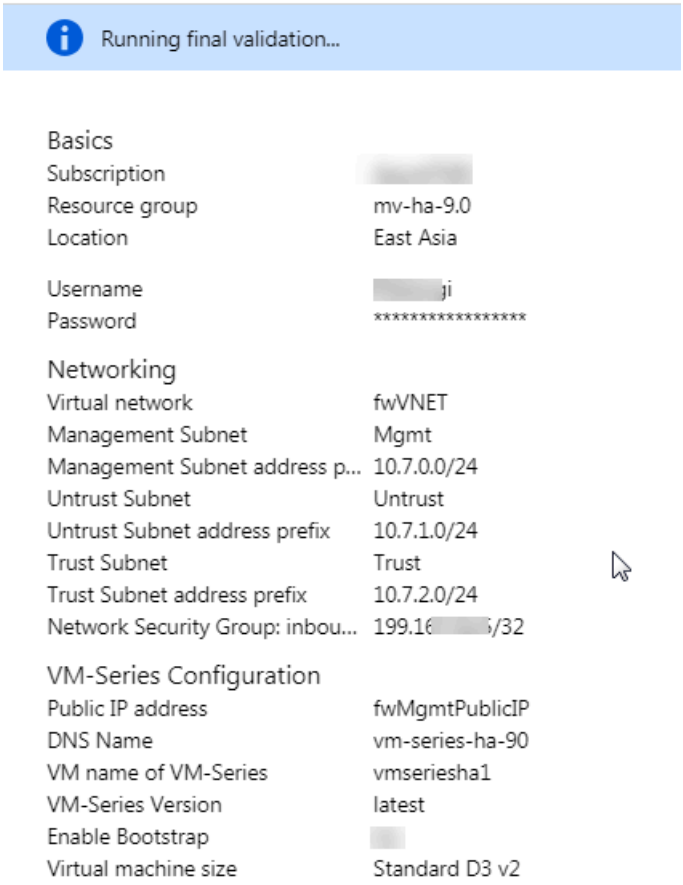
©2024 Palo Alto Networks, Inc.

- 资源组名称 — 已在其中部署要配置为 HA 对等的防火墙的资源组名称。两个防火墙必须位于同一资源组中。
- 密钥 — 与 Active Directory 应用程序相关联的身份验证密钥（在 Azure 门户中，单击 **Home**（主页） > **Azure Active Directory** > **Certificates & secrets**（证书和密钥），然后在 **Client secrets**（客户端密钥）下复制 **Value**（值）。如果您没有密钥，请先创建一个密钥，然后复制该值）。要以应用程序身份登录，必须同时提供密钥值和应用程序 ID。

了解在同一 Azure 资源组中部署 VM 系列防火墙所需的模板的位置。

对于 HA 配置，两个 HA 对等必须属于同一 Azure 资源组。如果从 Azure Marketplace 部署防火墙的第一个实例，则在将第二个防火墙实例部署到现有资源组的模板时，必须使用自定义 ARM 模板或 Palo Alto Networks 示例 GitHub 模板。您需要自定义模板或 Palo Alto Networks 示例模板的原因是 Azure 不支持将防火墙部署到非空资源组的功能。

复制第一个防火墙实例的部署信息。例如，



将 **VM Name of VM-Series**（**VM** 系列的 **VM** 名称）与防火墙 Web 界面上的 **Hostname**（主机名）匹配，如以上屏幕截图所示。在 **Device**（设备） > **Setup**（设置） > **Management**（管理）中必须添加相同的名称，因为防火墙的主机名用于触发故障转移。

©2024 Palo Alto Networks, Inc.

在 Azure 上的 VM 系列防火墙上规划网络接口配置。

要设置 HA，必须在同一 Azure 资源组中部署两个 HA 对等，并且两个防火墙必须具有相同数量的网络接口。每个 HA 对等至少需要四个网络接口：

- 管理界面 **(eth0)** — 与主接口关联的私有和公共 IP 地址。公共 IP 地址支持访问防火墙 Web 界面和 SSH 访问。

  对于主动/被动 HA 对等之间的控制链路通信，您可以使用管理接口上的专用 IP 接口作为 HA1 对等 IP 地址。如果需要专用的 HA1 接口，则必须在每个防火墙上附加一个额外的网络接口，这意味着每个防火墙上需要五个接口。
- **Untrust** 接口 **(eth1/1)** — 具有 /32 网络掩码的主要专用 IP 地址，以及具有专用 IP 地址（任何网络掩码）和公共 IP 地址的辅助 IP 配置。

  在故障转移时，当被动对等转换为主动状态时，与辅助 IP 配置相关联的公共 IP 地址将与先前的主动对等分离，并附加到现在的主动 HA 对等。
- 可信接口 **(eth1/2)** — 主要和次要专用 IP 地址。在故障转移时，当被动对等转换为主动状态时，辅助专用 IP 地址与先前的主动对等分离，并附加到现在的主动 HA 对等。
- **HA2 (eth 1/3)** — 主要专用 IP 地址。HA2 接口是 HA 对等用于同步会话、转发表、IPSec 安全关联和 ARP 表的数据链路。

接口	主动防火墙对等	被动防火墙对等	说明
可信	辅助 IP 地址	—	主动对等的可信接口需要可在故障转移时浮动到另一个对等的辅助 IP 配置。可信接口上的该辅助 IP 配置必须是专用 IP 地址，并具有它保护的服务器的网络掩码。在故障转移时，VM 系列插件调用 Azure API 以从活动对等分离此辅助专用 IP 地址，并将其附加到被动对等。将此 IP 地址附加到现在的主动对等可确保防火墙可以在不可信接口的浮动 IP 上接收流量，并将其发送到可信接口上的浮动 IP 以及工作负载。
不可信	辅助 IP 地址	—	防火墙的不可信接口需要辅助 IP 配置。该配置包括具有用于不可信子网的网络掩码的静态专用 IP 地址，以及用于通过 Internet 访问后端服务器或工作负载的公共 IP 地址。在故障转移时，VM 系列插件调用 Azure API 以从主动对等分离辅助 IP 配置，并在转换为主动状态之前将其附加到被动对等。此浮动辅助 IP 配置的过程使现在的主动防火墙能够继续处理发往工作负载的入站流量。

©2024 Palo Alto Networks, Inc.

接口	主动防火墙对等	被动防火墙对等	说明
HA2	从 Azure 管理控制台向防火墙添加 NIC。	从 Azure 管理控制台向防火墙添加 NIC。	在主动和被动对等上，添加专用 HA2 链路以启用会话同步。 HA1 的默认接口是管理接口，您可以选择使用管理接口，而不是向防火墙添加其他接口。要通过 HA2 链路启用数据流，您需要在 Azure 门户上添加其他网络接口，并在防火墙上配置 HA2 的接口。

在 **Azure** 上的 **VM** 系列防火墙上配置主动/被动 **HA**

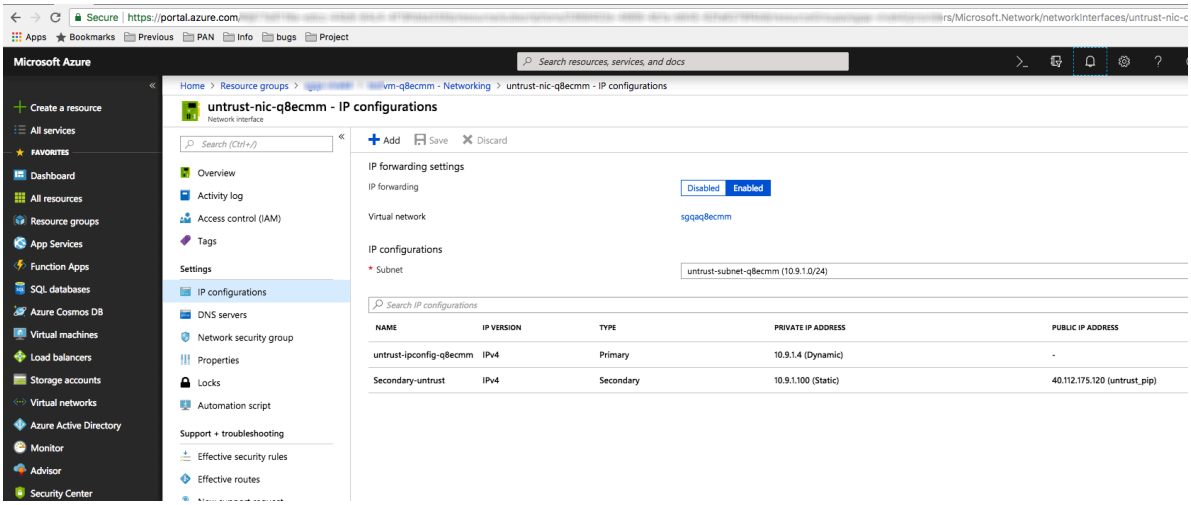
在此工作流程中，您使用 Azure Marketplace 中的 VM 系列防火墙解决方案模板部署 VM 系列防火墙的第一个实例，使用示例 GitHub 模板部署第二个防火墙实例。

与在 *HA* 配置中设置 *VM* 系列防火墙所需的 *Active Directory* 应用程序关联的身份验证密钥（客户端密钥）使用防火墙和 *Panorama* 上使用 *VM* 系列插件版本 *1.0.4* 进行加密。由于该密钥在 *VM* 系列插件版本 *1.0.4* 中加密，因此，必须在 *Panorama* 和托管 *VM* 系列防火墙上安装相同版本的插件，以便从 *Panorama* 集中管理防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | 使用解决方案模板部署 VM 系列防火墙并为 HA 设置网络接口。

1. 将辅助 IP 配置添加到防火墙上的不可信接口。

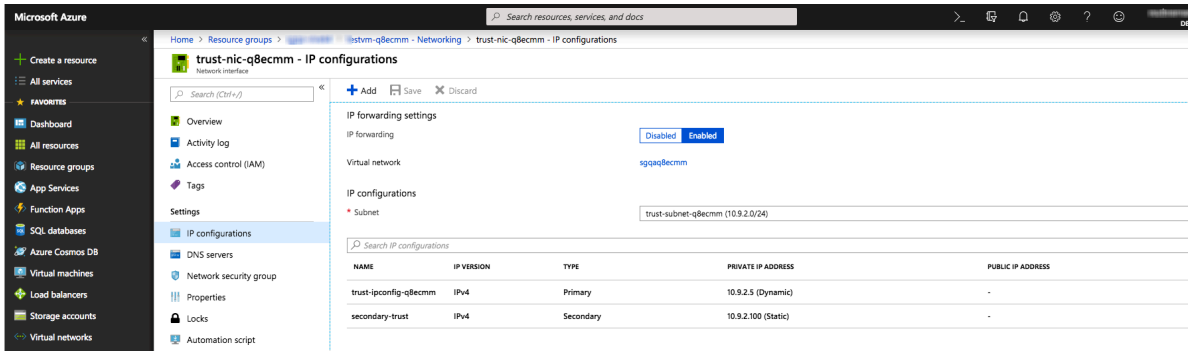


您必须将辅助 IP 配置（具有专用 IP 地址（任何网络掩码）和公共 IP 地址）附加到将指定为主动对等的防火墙。辅助 IP 配置始终与主动 HA 对等保持一致，并在发生故障转移时从一个对等移动到另一个对等。

在此工作流程中，该防火墙将被指定为主动对等。主动 HA 对等的设备优先级数值较低（在防火墙上作为 HA 配置的一部分配置），该值表示防火墙承担主动对等角色的优先级。

2. 将辅助 IP 配置添加到防火墙上的可信接口。

 ©2024 Palo Alto Networks, Inc.



可信接口的辅助 IP 配置仅需要静态专用 IP 地址。此 IP 地址在发生故障转移时从主动防火墙移动到被动防火墙，以便流量从不可信接口流向可信接口和防火墙保护的目标子网。

3. 为防火墙 HA 对等之间的 HA2 通信附加网络接口。
   1. 在虚拟网络中添加子网。
   2. 创建和连接防火墙的网络接口。
4. 在 Azure 上设置路由表。

   您的下一个跃点应指向浮动 IP 地址，如下所示：

 ©2024 Palo Alto Networks, Inc.

Routes

Search routes

Name	Address prefix	Next hop
database_server_to_frontend_server_route	10.9.3.0/24	10.9.2.100

Subnets

Search subnets

Name	Address range	Virtual network	Security group
database-server	10.9.4.0/24	vmq	-

Routes

Search routes

Name	Address prefix	Next hop
frontend_Server_to_Database_Server_route	10.9.4.0/24	10.9.1.100

Subnets

Search subnets

Name	Address range	Virtual network	Security group
frontend-server	10.9.3.0/24	vmq	-

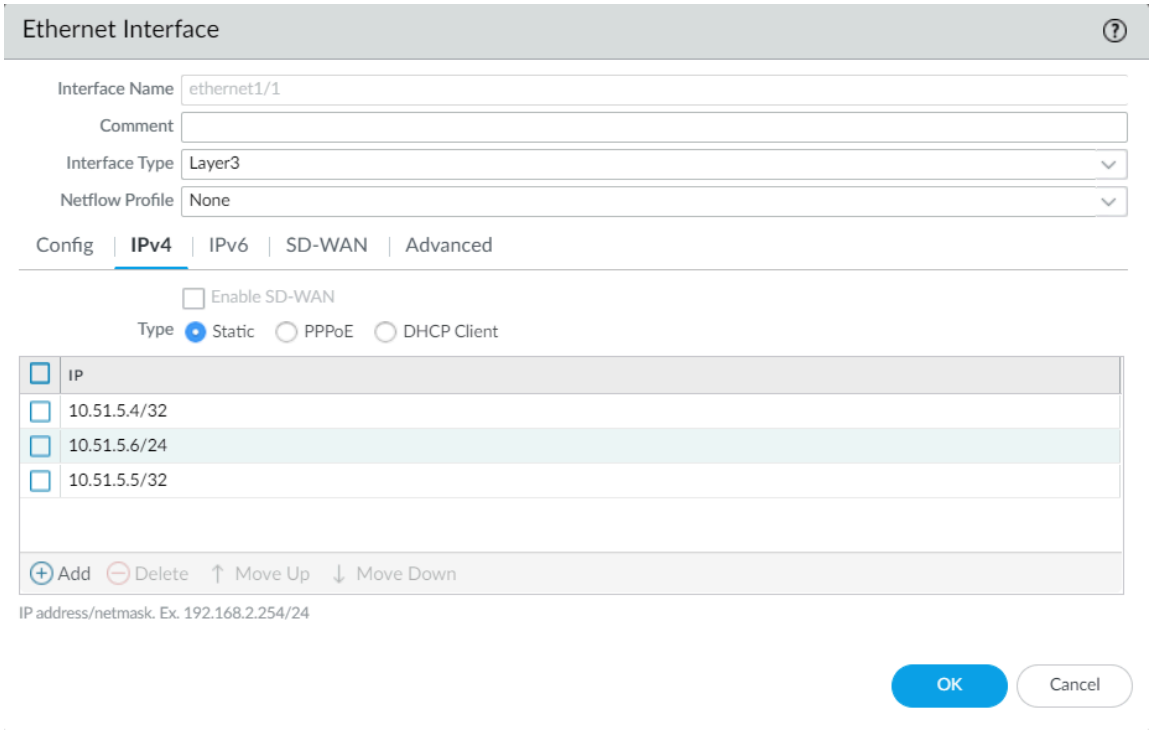
©2024 Palo Alto Networks, Inc.

STEP 2 | 配置防火墙上的接口。

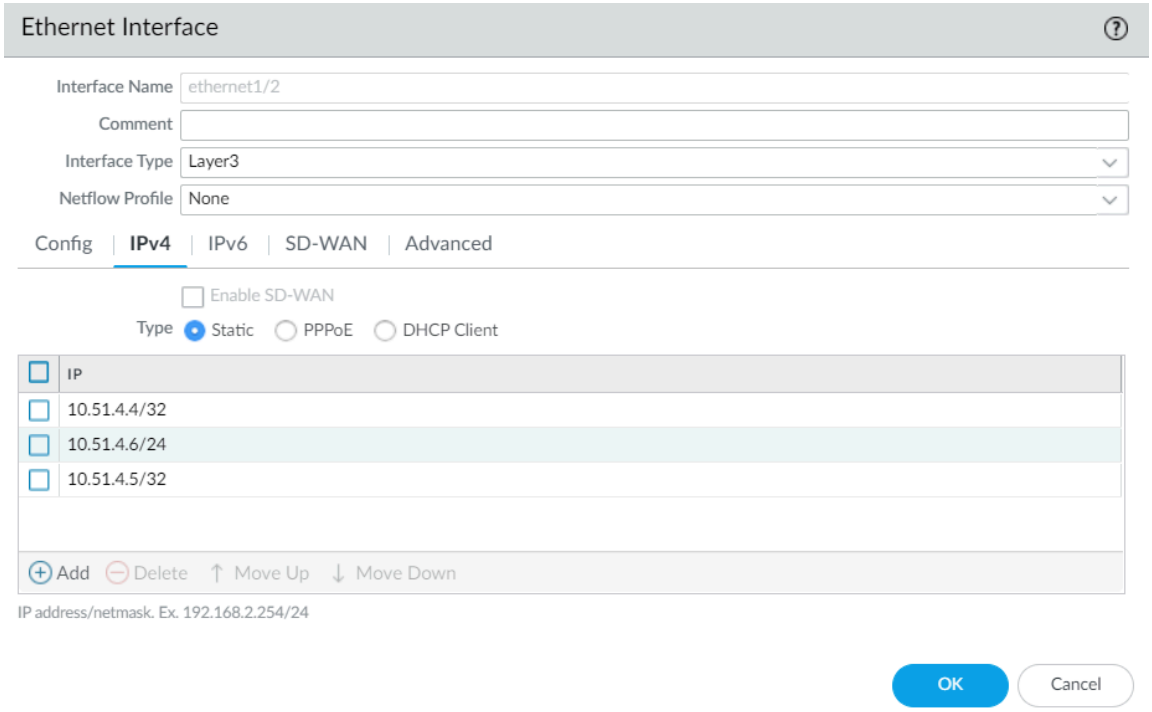
在部署和设置被动 HA 对等之前，请在主动 HA 对等上完成这些步骤。

1. 登录到防火墙 Web 界面。
2. 将 ethernet 1/1 配置为不可信接口，将 ethernet 1/2 配置为可信接口。

   选择 **Network**（网络） > **Interfaces**（接口）并按如下配置：



 ©2024 Palo Alto Networks, Inc.



3. 将 ethernet 1/3 配置为 HA 接口。

   要设置 HA2 链路，请选择接口并将 **Interface Type**（接口类型）设置为 **HA**。将链接速度和双工设置为自动。



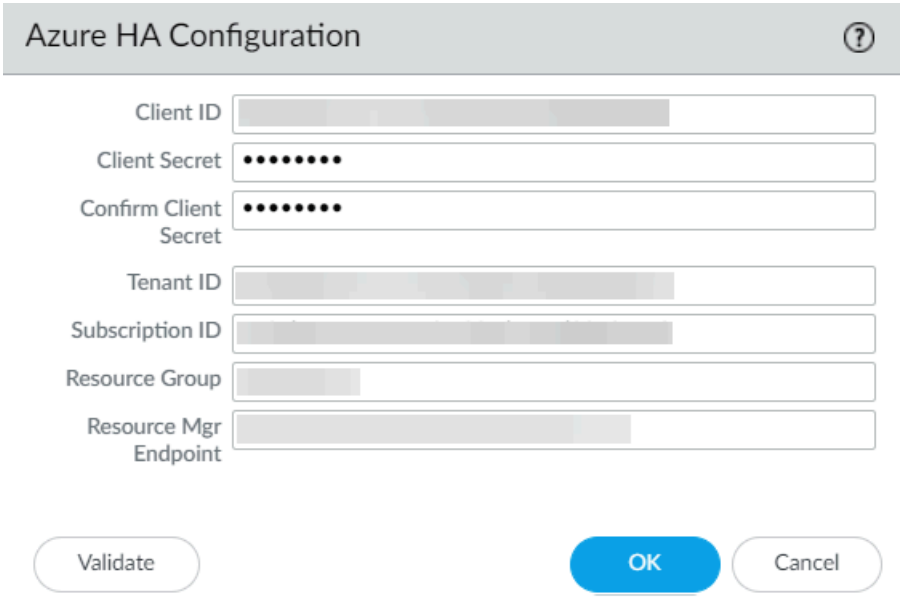
 ©2024 Palo Alto Networks, Inc.

STEP 3 | 配置 VM 系列插件以对已部署防火墙的 Azure 资源组进行身份验证。

在 VM 系列插件上设置 Azure HA 配置。

要加密客户端密钥，请使用 VM 系列插件版本 1.0.4 或更高版本。如果使用 Panorama 管理防火墙，则必须安装 VM 系列插件版本 1.0.4 或更高版本。

1. 选择 **Device**（设备）> **VM-Series**（**VM** 系列），以便在防火墙插件和 Azure 资源之间启用编程访问。



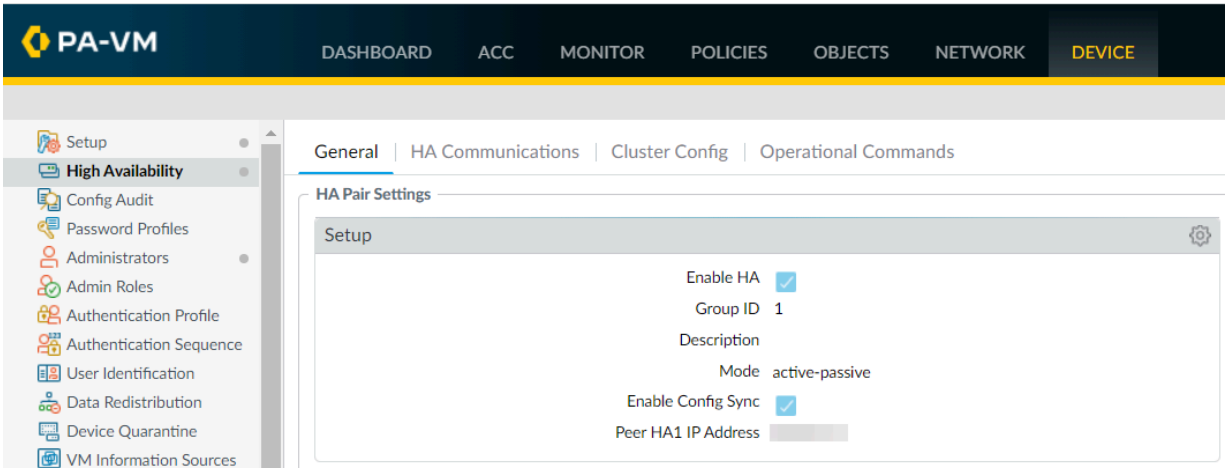
2. 输入 **Client ID**（客户端 **ID**）。客户端 ID 是与 Azure Active Directory 应用程序相关联的应用程序 ID。
3. 输入 **Client Secret**（客户端密钥），并重新输入以进行确认。
4. 输入 **Tenant ID**（租户 **ID**）。租户 ID 是您在设置 Active Directory 应用程序时保存的 Directory ID。
5. 输入想要监控的 Azure 订阅的 **Subscription ID**（订阅 **ID**）。
6. 输入 **Resource Group**（资源组）名称。
7. （仅适用于 Azure Stack 部署）输入 **Resource Mgr Endpoint**（资源管理端点）URL。该字段仅对于 Azure Stack 部署是必填字段。如果您使用的是常规 Azure 云部署，请勿在此字段中输入值；如果为常规 Azure 云部署指定资源管理终端节点 URL，则高可用性故障转移无法成功。

   此字段在 *VM* 系列插件 *2.1.2* 及更高版本上可用。

8. 单击 **Validate**（验证）以验证输入的密钥和 ID 是否有效，以及 VM 系列插件是否可以与使用 API 的 Azure 资源成功通信。

©2024 Palo Alto Networks, Inc.

STEP 4 | 启用 HA。



1. 选择 **Device**（设备） > **Setup**（设置） > **HA**。
2. 输入 **Peer HA1 IP address**（对等 **HA1 IP** 地址）作为被动对等的专用 IP 地址。
3. （可选）编辑控制链接 (HA1)。如果不计划使用管理接口作为控制链接且已添加其他接口（例如 ethernet 1/4），请编辑此部分以选择用于 HA1 通信的接口。
4. 编辑数据链路 (HA2) 以使用 **Port**（端口）ethernet 1/3，并添加此对等的 IP 地址和子网的 **Gateway**（网关）IP 地址。

STEP 5 | **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 在同一 Azure 资源组中设置被动 HA 对等。

1. 部署防火墙的第二个实例。
   - 从 GitHub 中下载自定义模板和参数文件。
   - 登录 Azure 门户。
   - 搜索 **Custom Template**（自定义模板）并选择 **Deploy from a custom template**（从自定义模板部署）。
   - 选择 **Build your own template in the editor**（在编辑器中构建自己的模板） > **Load file**（加载文件）。
   - 选择之前下载的 **azuredeploy.json** 并 **Save**（保存）。
   - 完成输入，同意条款并 **Purchase**（购买）。

     确保将以下输入与已部署的防火墙实例的输入相匹配 — Azure 订阅、资源组的名称、资源组的位置，要将防火墙部署到的现有 VNet 的名称，VNet CIDR、子网名称、子网 CIDR，并启动管理、可信和不可信子网的 IP 地址。
2. 重复步骤 1 和步骤 2 以设置接口，并将防火墙配置为被动 HA 对等。
3. 跳过步骤 3 并完成启用 HA（步骤 5）。根据情况在步骤 4 中修改此被动 HA 对等的 IP 地址。

STEP 7 | 在完成两个防火墙的配置后，验证防火墙是否已在主动/被动 HA 中配对。

1. 访问两个防火墙上的 **Dashboard**（仪表盘），并查看高可用性小部件。
2. 在主动防火墙上，单击 **Sync to peer**（同步到对等）链接。
3. 确认防火墙已配对并同步，如下所示：
   - 在被动防火墙上：本地防火墙的状态应显示 **Passive**（被动），并且 **Running Config**（运行配置）应显示为 **Synchronized**（已同步）。
   - 在主动防火墙上：本地防火墙的状态应显示为 **Active**（主动），并且 **Running Config**（运行配置）应显示为 **Synchronized**（已同步）。
4. 在被动对等上，验证 VM 系列插件配置现在是否已同步。

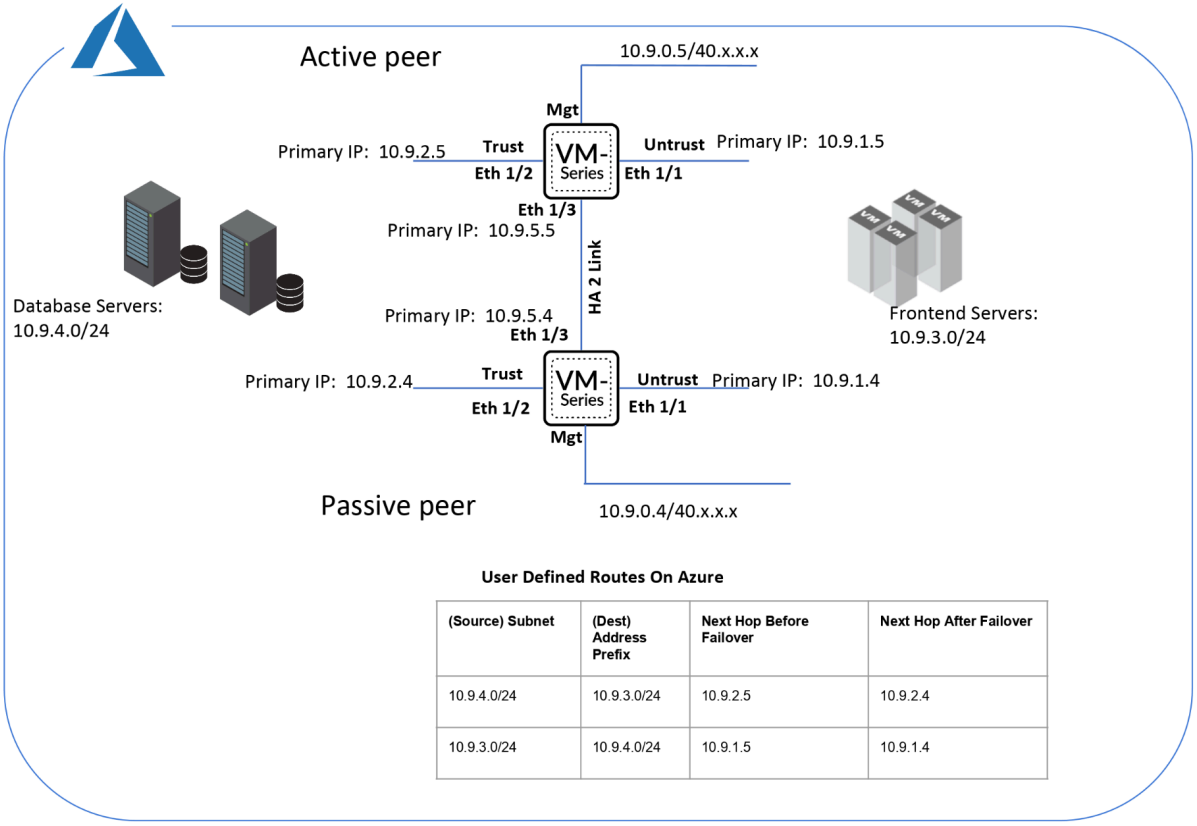
   选择 **Device**（设备） > **VM-Series**（**VM** 系列），并验证是否可以查看已在被动对等上忽略配置的 Azure HA 配置。

在 Azure 上设置主动/被动 HA（仅限东向西流量）

如果全部资源都部署在 Azure 基础架构中并且不需要为到 Azure VNet 的北向南流量强制执行安全，则可以在主动/被动高可用性 (HA) 配置中部署一对 VM 系列防火墙，而无需浮动 IP 地址。HA 对等仍将需要 HA 链接 — 一个控制链路 (HA1) 和一个数据链路 (HA2) — 用于同步数据和维护状态信息。

您必须拥有 VM 系列插件 1.0.9 版本或更高版本，并且必须在同一 Azure 资源组中部署两个防火墙 HA 对等。

©2024 Palo Alto Networks, Inc.



User Defined Routes On Azure

(Source) Subnet	(Dest) Address Prefix	Next Hop Before Failover	Next Hop After Failover
10.9.4.0/24	10.9.3.0/24	10.9.2.5	10.9.2.4
10.9.3.0/24	10.9.4.0/24	10.9.1.5	10.9.1.4

- 为启用 HA 设置防火墙
- 在 Azure 上的 VM 系列防火墙上配置主动/被动 HA

为启用 HA 设置防火墙

收集在 Azure 上的 VM 系列防火墙上配置 HA 的以下详细信息。

设置 Active Directory 应用程序和服务主题以启用编程 API 访问。

- 为了让防火墙与 Azure API 交互，需要创建 Azure Active Directory 服务主体。该服务主体具有对 Azure AD 进行身份验证和访问订阅中的资源的权限。要完成此设置，必须具有向 Azure AD 租户注册应用程序的权限，并将应用程序分配给订阅的角色。如果您没有所需权限，请要求 Azure AD 或订阅管理员创建服务主体。有关所需的权限，请参阅上表。复制以下详细信息以供稍后在此工作流程中使用：
  - 客户端 **ID** — 与 Active Directory 相关联的应用程序 ID（在 Azure 门户中，单击 **Home**（主页） > **Azure Active Directory** > **App registrations**（应用程序注册），然后选择应用程序并复制 ID）。

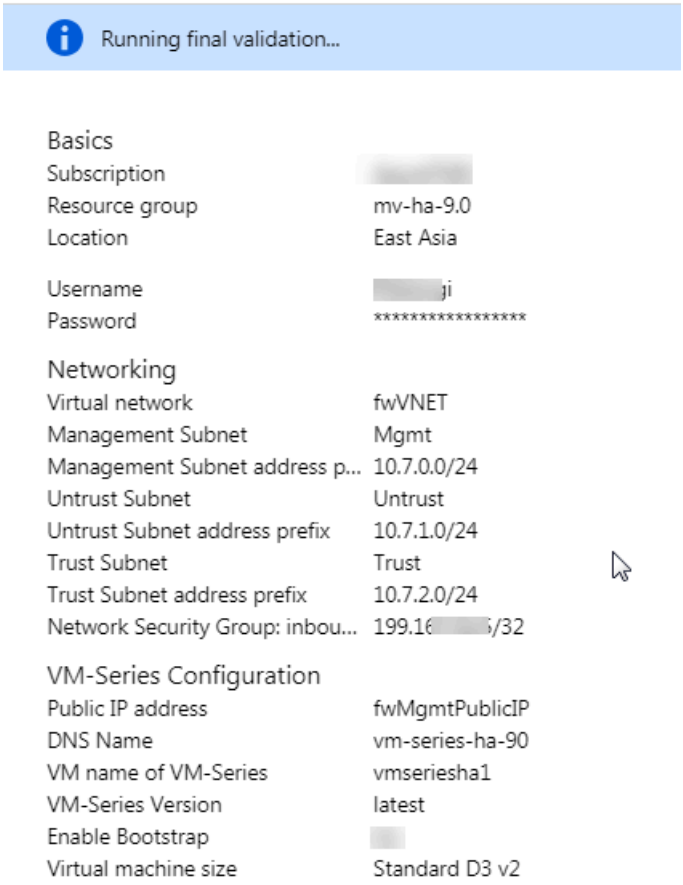
©2024 Palo Alto Networks, Inc.

- 租户 **ID** — 与 Active Directory 相关联的应用程序 ID（在 Azure 门户上，单击 **Home**（主页）> **Azure Active Directory** > **Properties**（属性）> **Directory ID**（目录 **ID**），然后选择应用程序并复制 ID）。
- **Azure** 订阅 **ID** — 已部署防火墙的 Azure 订阅。您必须登录到您的 Azure 门户才能获取此订阅 ID。
- 资源组名称 — 已在其中部署要配置为 HA 对等的防火墙的资源组名称。两个防火墙必须位于同一资源组中。
- 密钥 — 与 Active Directory 应用程序相关联的身份验证密钥（在 Azure 门户中，单击 **Home**（主页）> **Azure Active Directory** > **Certificates & secrets**（证书和密钥），然后在 **Client secrets**（客户端密钥）下复制 **Value**（值）。如果您没有密钥，请先创建一个密钥，然后复制该值）。要以应用程序身份登录，必须同时提供密钥值和应用程序 ID。

了解在同一 Azure 资源组中部署 VM 系列防火墙所需的模板的位置。

对于 HA 配置，两个 HA 对等必须属于同一 Azure 资源组。如果从 Azure Marketplace 部署防火墙的第一个实例，则在将第二个防火墙实例部署到现有资源组的模板时，必须使用自定义 ARM 模板或 Palo Alto Networks 示例 GitHub 模板。您需要自定义模板或 Palo Alto Networks 示例模板的原因是 Azure 不支持将防火墙部署到非空资源组的功能。

复制第一个防火墙实例的部署信息。例如，



 ©2024 Palo Alto Networks, Inc.

将 **VM Name of VM-Series**（**VM** 系列的 **VM** 名称）与防火墙 Web 界面上的 **Hostname**（主机名）匹配，如以上屏幕截图所示。在 **Device**（设备）> **Setup**（设置）> **Management**（管理）中必须添加相同的名称，因为防火墙的主机名用于触发故障转移。

在 Azure 上的 VM 系列防火墙上规划网络接口配置。

要设置 HA，必须在同一 Azure 资源组中部署两个 HA 对等，并且两个防火墙必须具有相同数量的网络接口。每个 HA 对等至少需要四个网络接口：

- 管理界面 **(eth0)** — 与主接口关联的私有和公共 IP 地址。公共 IP 地址支持访问防火墙 Web 界面和 SSH 访问。

  对于主动/被动 HA 对等之间的控制链路通信，您可以使用管理接口上的专用 IP 接口作为 HA1 对等 IP 地址。如果需要专用的 HA1 接口，则必须在每个防火墙上附加一个额外的网络接口，这意味着每个防火墙上需要五个接口。
- 不可信接口 **(eth1/1)** — 具有 /32 网络掩码的主要专用 IP 地址。

  发生故障转移时，当被动对等转换为主动状态后，VM 系列插件会自动将流量发送到被动对等的主要专用 IP 地址。Azure UDR 将启用流量流。
- 可信接口 **(eth1/2)** — 主要专用 IP 地址。发生故障转移时，当被动对等转换为主动状态后，VM 系列插件会自动将流量发送到被动对等的主要专用 IP 地址。
- **HA2 (eth 1/3)** — 主要专用 IP 地址。HA2 接口是 HA 对等用于同步会话、转发表、IPSec 安全关联和 ARP 表的数据链路。

接口	主动防火墙对等	被动防火墙对等	说明
HA2	从 Azure 管理控制台向防火墙添加 NIC。	从 Azure 管理控制台向防火墙添加 NIC。	在主动和被动对等上，添加专用 HA2 链路以启用会话同步。 HA1 的默认接口是管理接口，您可以选择使用管理接口，而不是向防火墙添加其他接口。要通过 HA2 链路启用数据流，您需要在 Azure 门户上添加其他网络接口，并在防火墙上配置 HA2 的接口。

在 **Azure** 上的 **VM** 系列防火墙上配置主动/被动 **HA**

在此工作流程中，您使用 Azure Marketplace 中的 VM 系列防火墙解决方案模板部署 VM 系列防火墙的第一个实例，使用示例 GitHub 模板部署第二个防火墙实例。

©2024 Palo Alto Networks, Inc.

与在 *HA* 配置中设置 *VM* 系列防火墙所需的 *Active Directory* 应用程序关联的身份验证密钥（客户端密钥）使用防火墙和 *Panorama* 上使用 *VM* 系列插件版本 *1.0.9* 进行加密。由于该密钥在 *VM* 系列插件版本 *1.0.9* 中加密，因此，必须在 *Panorama* 和托管 *VM* 系列防火墙上安装相同版本的插件，以便从 *Panorama* 集中管理防火墙。

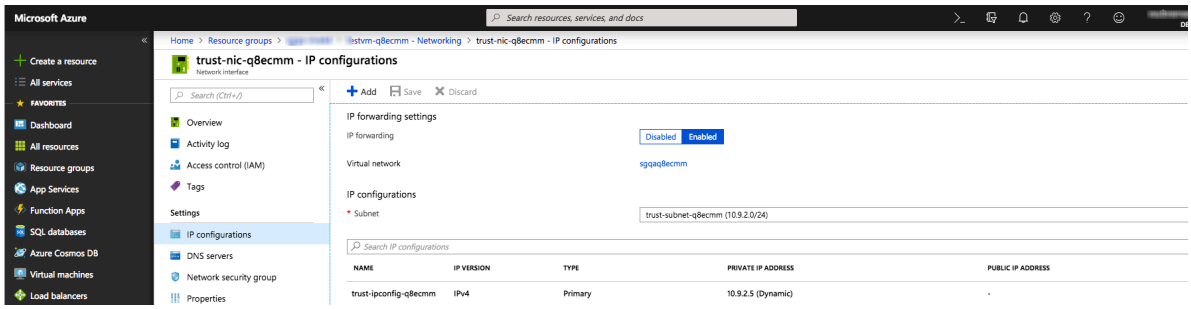
©2024 Palo Alto Networks, Inc.

STEP 1 | 使用解决方案模板部署 VM 系列防火墙并为 HA 设置网络接口。

为了保护 Azure VNet 中的东向西流量，您只需要可信和不可信防火墙接口的主要 IP 地址。发生故障转移时，UDR 会更改，并且路由会指向转换为主动状态的对等的主要 IP 地址。

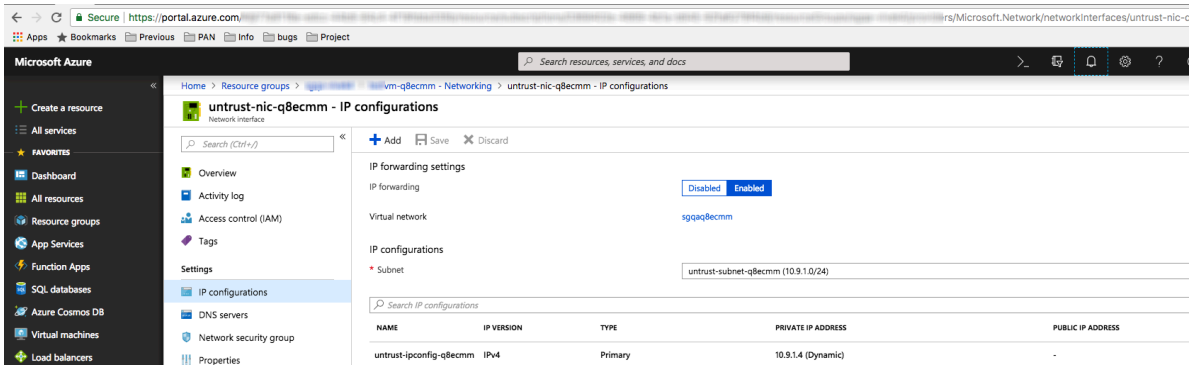
1. 将主 IP 配置添加到活动防火墙对等的信任接口。

   此工作流中会将该防火墙指定为活动对等。主动 HA 对等的设备优先级数值较低（在防火墙上作为 HA 配置的一部分配置），该值表示防火墙承担主动对等角色的优先级。



2. 将主要 IP 配置添加到主动防火墙对等的不可信接口。

 ©2024 Palo Alto Networks, Inc.



3. 在防火墙 HA 对等之间为 HA2 通信附加一个网络接口。
   1. 在虚拟网络中添加一个子网。
   2. 为防火墙 创建并附加一个网络接口。
4. 在 Azure 上设置路由表。

   为主动防火墙对等的可信和不可信接口的主要 IP 地址的下一个跃点创建路由。

   Example with Frontend Server to Database Server Route :

   Routes

   Search routes

Name	Address prefix	Next hop
frontend_Server_to_Database_Server_route	10.9.4.0/24	10.9.1.5

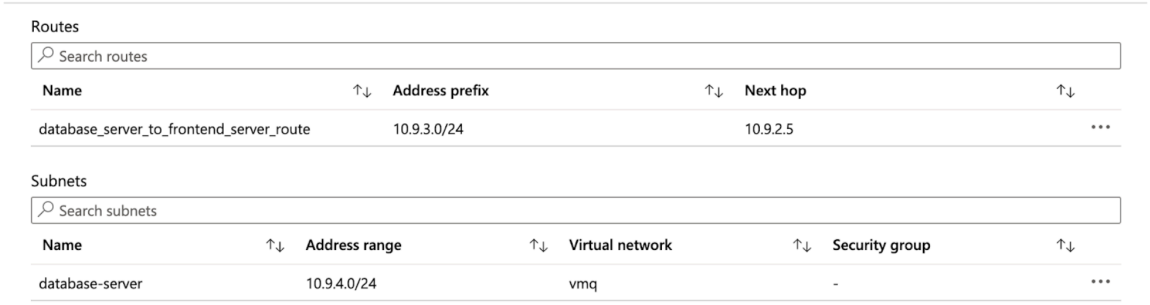
   Subnets

   Search subnets

Name	Address range	Virtual network	Security group
frontend-server	10.9.3.0/24	vmq	-

©2024 Palo Alto Networks, Inc.

Example with Database Server to Frontend Server route:



发生故障转移后，数据库服务器到前端服务器路由的下一个跃点将从 10.9.2.5 更改为 10.9.2.4。同样，前端服务器到数据库服务器路由的下一个跃点将从 10.9.1.5 更改为 10.9.1.4。

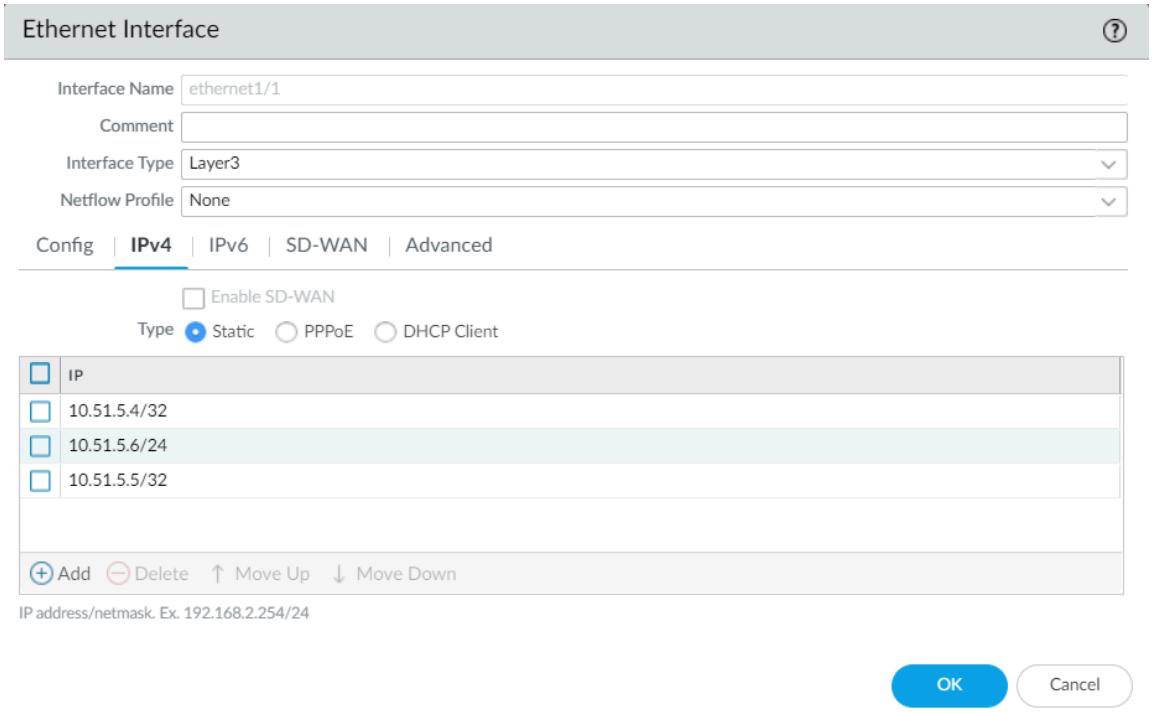
©2024 Palo Alto Networks, Inc.

STEP 2 | 配置防火墙上的接口。

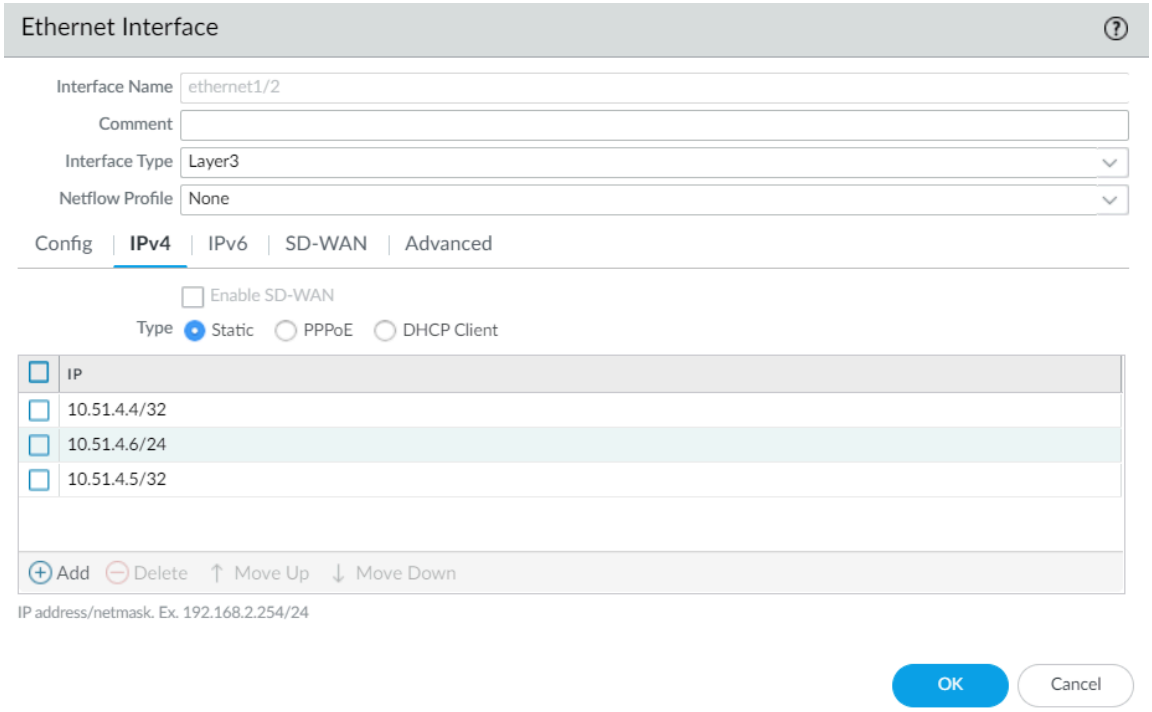
在部署和设置被动 HA 对等之前，请在主动 HA 对等上完成这些步骤。

1. 登录到防火墙 Web 界面。
2. 将 ethernet 1/1 配置为不可信接口，将 ethernet 1/2 配置为不可信接口。

   选择 **Network**（网络） > **Interfaces**（接口）并按如下配置：



 ©2024 Palo Alto Networks, Inc.



3. 将 ethernet 1/3 配置为 HA 接口。

   要设置 HA2 链路，请选择接口并将 **Interface Type**（接口类型）设置为 **HA**。将链接速度和双工设置为自动。



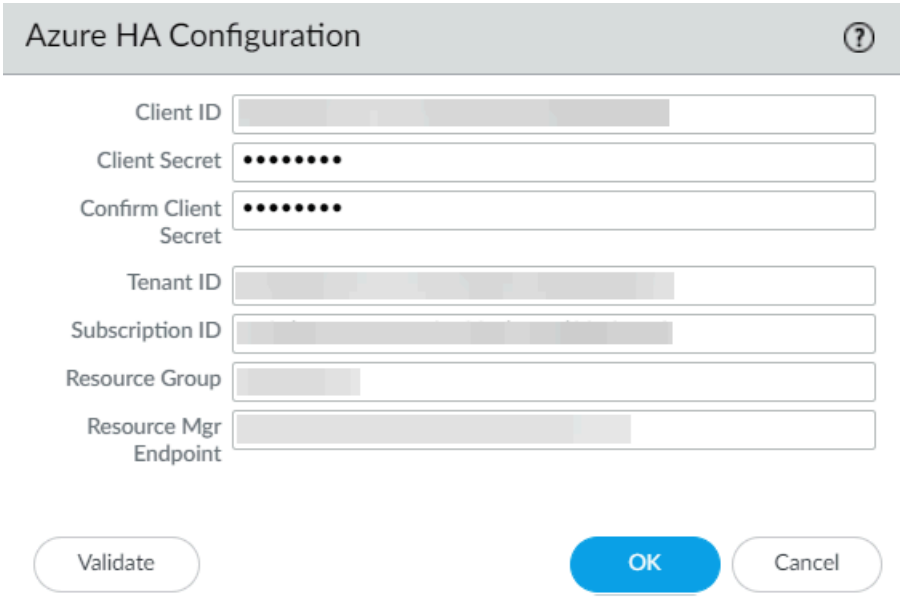
 ©2024 Palo Alto Networks, Inc.

STEP 3 | 配置 VM 系列插件以对已部署防火墙的 Azure 资源组进行身份验证。

在 VM 系列插件上设置 Azure HA 配置。

要加密客户端密钥，请使用 VM 系列插件版本 1.0.4 或更高版本。如果使用 Panorama 管理防火墙，则必须安装 VM 系列插件版本 1.0.4 或更高版本。

1. 选择 **Device**（设备）> **VM-Series**（**VM** 系列），以便在防火墙插件和 Azure 资源之间启用编程访问。



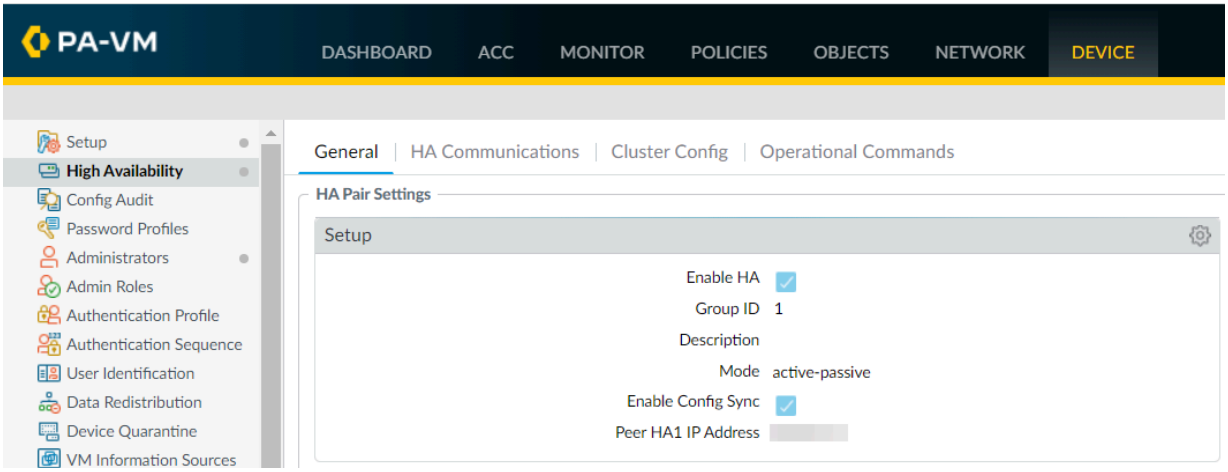
2. 输入 **Client ID**（客户端 **ID**）。客户端 ID 是与 Azure Active Directory 应用程序相关联的应用程序 ID。
3. 输入 **Client Secret**（客户端密钥），并重新输入以进行确认。
4. 输入 **Tenant ID**（租户 **ID**）。租户 ID 是您在设置 Active Directory 应用程序时保存的 Directory ID。
5. 输入想要监控的 Azure 订阅的 **Subscription ID**（订阅 **ID**）。
6. 输入 **Resource Group**（资源组）名称。
7. （仅适用于 Azure Stack 部署）输入 **Resource Mgr Endpoint**（资源管理端点）URL。

   此字段在 *VM* 系列插件 *2.1.2* 及更高版本上可用。

8. 单击 **Validate**（验证）以验证输入的密钥和 ID 是否有效，以及 VM 系列插件是否可以与使用 API 的 Azure 资源成功通信。

©2024 Palo Alto Networks, Inc.

STEP 4 | 启用 HA。



1. 选择 **Device**（设备） > **Setup**（设置） > **HA**。
2. 输入 **Peer HA1 IP address**（对等 **HA1 IP** 地址）作为被动对等的专用 IP 地址。
3. （可选）编辑控制链接 (HA1)。如果不计划使用管理接口作为控制链接且已添加其他接口（例如 ethernet 1/4），请编辑此部分以选择用于 HA1 通信的接口。
4. 编辑数据链路 (HA2) 以使用 **Port**（端口）ethernet 1/3，并添加此对等的 IP 地址和子网的 **Gateway**（网关）IP 地址。

STEP 5 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 6 | 在同一 Azure 资源组中设置被动 HA 对等。

1. 部署防火墙的第二个实例。
   - 从 GitHub 中下载自定义模板和参数文件。
   - 登录 Azure 门户。
   - 搜索 **Custom Template**（自定义模板）并选择 **Deploy from a custom template**（从自定义模板部署）。
   - 选择 **Build your own template in the editor**（在编辑器中构建自己的模板） > **Load file**（加载文件）。
   - 选择之前下载的 **azuredeploy.json** 并 **Save**（保存）。
   - 完成输入，同意条款并 **Purchase**（购买）。

     确保将以下输入与已部署的防火墙实例的输入相匹配 — Azure 订阅、资源组的名称、资源组的位置，要将防火墙部署到的现有 VNet 的名称，VNet CIDR、子网名称、子网 CIDR，并启动管理、可信和不可信子网的 IP 地址。
2. 重复步骤 1 和步骤 2 以设置接口，并将防火墙配置为被动 HA 对等。
3. 跳过步骤 3 并完成启用 HA（步骤 5）。根据情况在步骤 4 中修改此被动 HA 对等的 IP 地址。

STEP 7 | 在完成两个防火墙的配置后，验证防火墙是否已在主动/被动 HA 中配对。

1. 访问两个防火墙上的 **Dashboard**（仪表盘），并查看高可用性小部件。
2. 在主动防火墙上，单击 **Sync to peer**（同步到对等）链接。
3. 确认防火墙已配对并同步，如下所示：
   - 在被动防火墙上：本地防火墙的状态应显示 **Passive**（被动），并且 **Running Config**（运行配置）应显示为 **Synchronized**（已同步）。
   - 在主动防火墙上：本地防火墙的状态应显示为 **Active**（主动），并且 **Running Config**（运行配置）应显示为 **Synchronized**（已同步）。
4. 在被动对等上，验证 VM 系列插件配置现在是否已同步。

   选择 **Device**（设备） > **VM-Series**（**VM** 系列），并验证是否可以查看已在被动对等上忽略配置的 Azure HA 配置。

©2024 Palo Alto Networks, Inc.

使用 Azure 密钥保管库存储 VM 系列证书

您可以集成云原生密钥管理器来存储证书。用于证书的私钥不存储在防火墙的硬盘上，从而消除了安全问题。管理员在云存储中保留证书和私钥。防火墙使用 Azure 密钥保管库从云存储中检索证书和私钥，并将其用于解密和 IPSec 等功能。

仅支持 *VM* 系列防火墙通过 *Azure* 密钥保管库启用证书检索。如果使用密钥保管库证书，则不能降级到早期版本的 *PAN-OS*。

对于出站和入站解密，将证书上传到本机密钥管理器并向 NGFW 提供所需的访问权限。公共云上的 NGFW 可使用密钥保管库来存储证书。在这种情况下，请使用 PAN-OS 或 CLI 为相同的实例配置所需的访问管理策略。

对于使用自动缩放的环境，实例在检索到必要证书并准备好解密流量的状态下启动，无需额外的手动配置。

在云中更新证书时，必须将其作为新证书重新导入防火墙中。您必须将 IAM 角色分配给实例，从而使实例能够从 Azure 密钥保管库存储中检索证书。IAM 角色必须对 Azure 密钥保管库上的机密具有 **get** 权限。

您可以从密钥保管库的证书存储（而不是机密部分）检索证书。PEM 是唯一受支持的格式。不支持 PKCS12 或链式证书。

当主密钥发生更改时，将删除所有证书，然后在提交时重新获取。当配置同步到 *HA* 下的被动防火墙时，证书由被动防火墙上的管理守护程序自动下载。结果是不会同步证书。

STEP 1 | 下载证书。

STEP 2 | 在部署 VM 系列防火墙的同一资源组中的 Azure 上创建密钥保管库。使用以 PEM 格式存储证书（公钥和私钥）的密钥保管库。

以 **.pem** 格式将证书和私钥一起上传。

STEP 3 | 创建密钥保管库后，在 **Access Policies**（访问策略）下，单击 **Create**（创建）并添加托管标识。

STEP 4 | 返回到资源组并选择 VM 系列防火墙。单击 **Identity**（标识）> **User Assigned**（分配的用户）并添加 **Managed Identity**（托管标识）。

还必须向密钥保管库提供托管标识中的权限。

STEP 5 | 返回密钥保管库并选择 **Certificates**（证书）。导入证书 PEM 文件。

证书必须以 PEM 格式保存在 **Key Vault**（密钥保管库）> **Certificates**（证书）中。

STEP 6 | 登录到 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 7 | 选择 **Device**（设备）> **Certificate**（证书）**Management**（管理）> **Certificates**（证书）> **Import**（导入）。

如果要导入 **ECDSA** 证书，请修改私钥：

----Begin EC PRIVATE KEY----

&

----END EC PRIVATE KEY----

到

----BEGIN PRIVATE KEY----

&

----END PRIVATE KEY----

如果要导入 **PEM** 证书，请修改私钥：

----BEGIN PRIVATE KEY----

&

----END PRIVATE KEY----

STEP 8 | 在 **Cloud**（云）下，输入证书名称并将文件格式设置为 **PEM**。

STEP 9 | 选择 **Cloud**（云）作为 **Certificate Type**（证书类型），然后配置以下字段：

1. 输入 **Certificate Name**（证书名称）；从 Azure 门户中的密钥保管库复制证书名称。
2. 从 **Cloud Platform**（云平台）下拉列表中选择 **Azure**。
3. 输入 **Azure Key Vault URI**（**Azure** 密钥保管库 **URI**）以指定密钥保管库的位置；从 Azure 门户中的密钥保管库复制此 URI。
4. 输入 **Cloud Secret Name**（云机密名称）。这用于将证书存储在 Azure 密钥保管库中。
5. 您可以在证书信息屏幕中指定 **Algorithm**（算法）。为配置选择算法 **RSA** 或 **Elliptical Curve DSA**（椭圆曲线 **DSA**）。默认情况下，算法设置为使用 **RSA**。配置证书以使用 转发信任证书、转发不信任证书或信任的根 **CA**。您也可以选择证书的所有算法。
6. 单击 **OK**（确定）。
7. 提交更改。

 ©2024 Palo Alto Networks, Inc.

STEP 10 | 验证证书是否添加成功：

1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
2. 随即会列出新证书。

证书详细信息不会显示在 **Certificates**（证书）

屏幕中。要在 CLI 中查看此信息，请使用命令：

```
show shared certificate
```

<cert-name>

您可以在 Panorama 中确认证书集成的配置。在设备证书窗口中确定是否使用了证书。请记住，由于数据未存储在运行配置（硬盘驱动器）中，因此，**Device Certificates**（设备证书）表中的所有字段均为空，**Usage**（使用情况）字段（如果已配置）和 **Cloud Secret Name**（云机密名称）除外。

©2024 Palo Alto Networks, Inc.

使用 ARM 模板部署 VM 系列防火墙

除基于 Marketplace 的部署外，Palo Alto Networks 还提供托管示例 ARM 模板的 GitHub 存储库，您可以根据需求从中下载这些模板并进行自定义设置。ARM 模板为 JSON 文件，这些文件会对一些个人必备资源加以说明，包括网络接口、完整虚拟机，甚至带多个虚拟机的整个应用程序堆栈等。

ARM 模板适用于高级用户，Palo Alto Networks 在社区支持策略下提供 ARM 模板。要了解 ARM 模板的信息，请参阅有关 ARM 模板的 Microsoft 文档。

为简化所有必备资源的部署工作，双层示例模板 (https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample) 包含两个 json 文件：

- **Template File**（模板文件）— azureDeploy.json 为主资源文件，用以部署资源组内的所有组件。
- **Parameters File**（参数文件）— azureDeploy.parameters.json 为包含有所有必备参数的文件，这些参数有助于成功实现 VNet 中 VM 系列防火墙的部署。该文件中也包含有诸多详细信息，如虚拟机层和规模、用于防火墙的用户名和密码，以及用于防火墙的存储容器等。您可以针对 Azure VNet 部署对此文件进行自定义设置。

为了帮助您将防火墙部署为面向 Internet 的应用程序的网关，该模板提供了 VM 系列防火墙，数据库服务器和 Web 服务器。VNet 使用不可路由的专用 IP 地址空间 192.168.0.0/16。您可以通过修改模板来使用 172.16.0.0/12 或 10.0.0.0/8。

ARM 模板也提供必需的用户定义规则和 IP 转发标记，以使 VM 系列防火墙能够保护 Azure 资源组。对于此模板中包含 5 个子网 — Trust、Untrust、Web、DB 和 NAT，您拥有 5 个路由表，每个子网各一个，这些子网均设有用户定义规则，用以将流量路由至 VM 系列防火墙和 NAT 虚拟机。

对于此模板中包含四个子网 — Trust、Untrust、Web 和 DB，您拥有四个路由表，每个子网各一个，这些子网均有用户定义规则，用于将流量路由至 VM 系列防火墙。

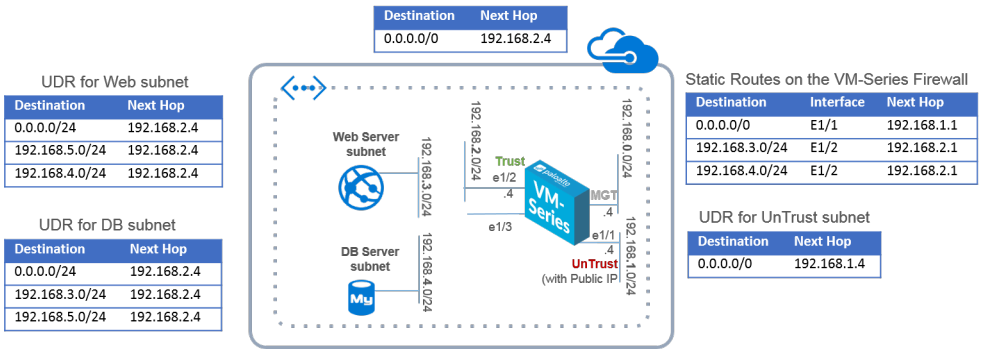


图 **4:** 使用 **ARM** 模板部署 **VM** 系列防火墙

STEP 1 | 下载 GitHub 存储库提供的 ARM 双层示例模板。

下载并保存文件至本地客户端：https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample

©2024 Palo Alto Networks, Inc.

STEP 2 | 在 Azure 上创建资源组。

1. 使用以下命令登录到 Azure CLI：**`az login`**

   如果您需要帮助，请参阅关于安装 CLI 的 Azure 文档，或者有关如何在 Azure Government 或 Azure China 上访问 CLI 的详细信息。

2. 创建资源组。

STEP 3 | 部署 ARM 模板。

1. 使用文本编辑器打开参数文件，然后修改部署的值：

   在 *Azure China*，您必须编辑承载部署 *VM* 系列防火墙所需的 *VHD* 映像的存储帐户的路径。在模板文件的变量部分中，找到调用的参数 ***userImageNameURI*** 并将该值替换为您保存 *VHD* 映像的位置。

2. 在已创建的资源组中部署模板。

   ```
   az deployment group create --name <YourResourceGroupName> --
   resource-group <YourResourceGroupName> --parameters ' @<path-
   to-template-parameter-azureDeploy.json>'
   ```

3. 通过 Azure CLI 检查部署进程/状态：

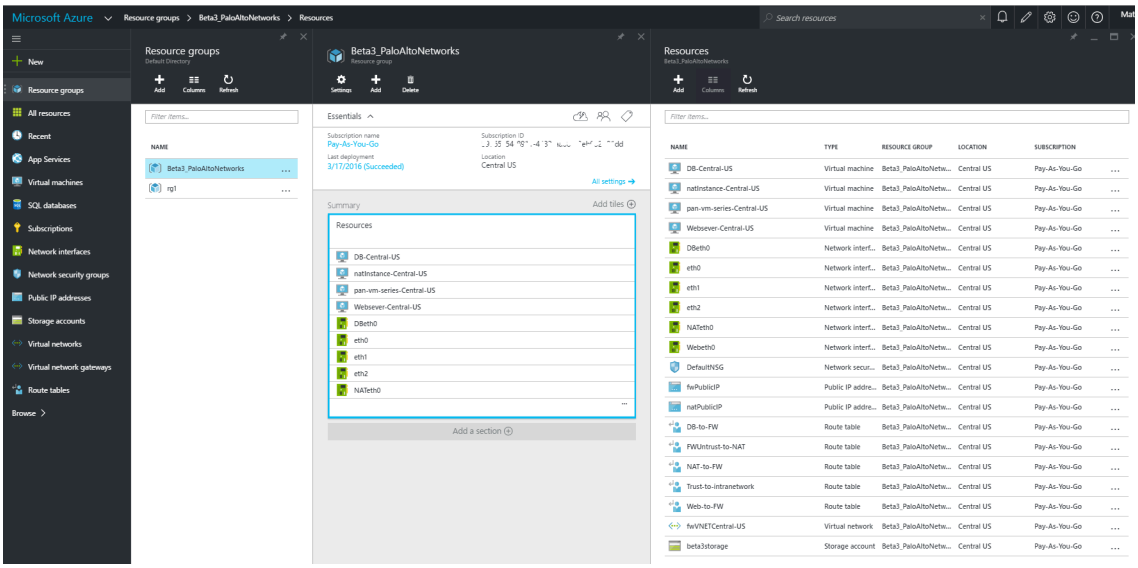
   ```
   azure deployment group show <YourResourceGroupName>
   ```


©2024 Palo Alto Networks, Inc.

成功部署模板后，会显示 `ProvisioningStateis Running`。

如果显示 *`ProvisioningStateis Failed`*，则必须在 *Azure* 门户的 ***Resource Group***（资源组） > ***Events***（事件）中检查是否存在错误。筛选出仅在最近一小时内发生的事件，选中最近的事件，然后单击查看具体错误。

4. 确认您已成功部署 VM 系列防火墙。
   1. 选择 **Dashboard**（仪表盘） > **Resource Groups**（资源组），然后选择所需的资源组。
   2. 选择 **All Settings**（所有设置） > **Deployments**（部署） > **Deployment History**（部署历史记录）以了解详细状态。



VNet 内的地址空间使用前缀 *“192.168”*，这在 *ARM* 模板中已作定义。

5. 将公有 IP 地址附加到防火墙上的不可信接口。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 将防火墙配置为 VNet 网关，用以保护面向 Internet 的部署。

1. 登录到防火墙上的管理接口 IP 地址。
2. 将数据面板接口配置为防火墙上的第 3 层接口（**Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网））。
3. 将静态规则添加到防火墙上的虚拟路由。在本示例中，要路由通过防火墙的流量，您需要防火墙上的 3 个静态路由（**Network**（网络） > **Virtual Routers**（虚拟路由器），选择路由器并单击 **Static Routes**（静态路由））：
   1. 将所有出站流量通过 UnTrust 区域 ethernet1/1 路由至位于 192.168.1.1 的 Azure 路由器。
   2. 将所有以 Web 服务器为目标的入站流量通过 Trust 区域 ethernet1/2 路由至位于 192.168.2.1 的 Azure 路由器。
   3. 将所有以数据库服务器子网为目标的入站流量通过 Trust 区域 ethernet1/2 路由至位于 192.168.2.1 的 Azure 路由器。
4. 创建安全策略规则（**Policies**（策略） > **Security**（安全）），以允许防火墙上的入站流量和出站流量。您也需要设置相应的安全策略规则，确保适当流量能够在 Web 服务器子网与数据库服务器子网之间往来通信。
5. 在防火墙上 **Commit**（提交）更改。
6. 确认 VM 系列防火墙正在保护流量（**Monitor**（监控） > **Logs**（日志） > **Traffic**（流量））。

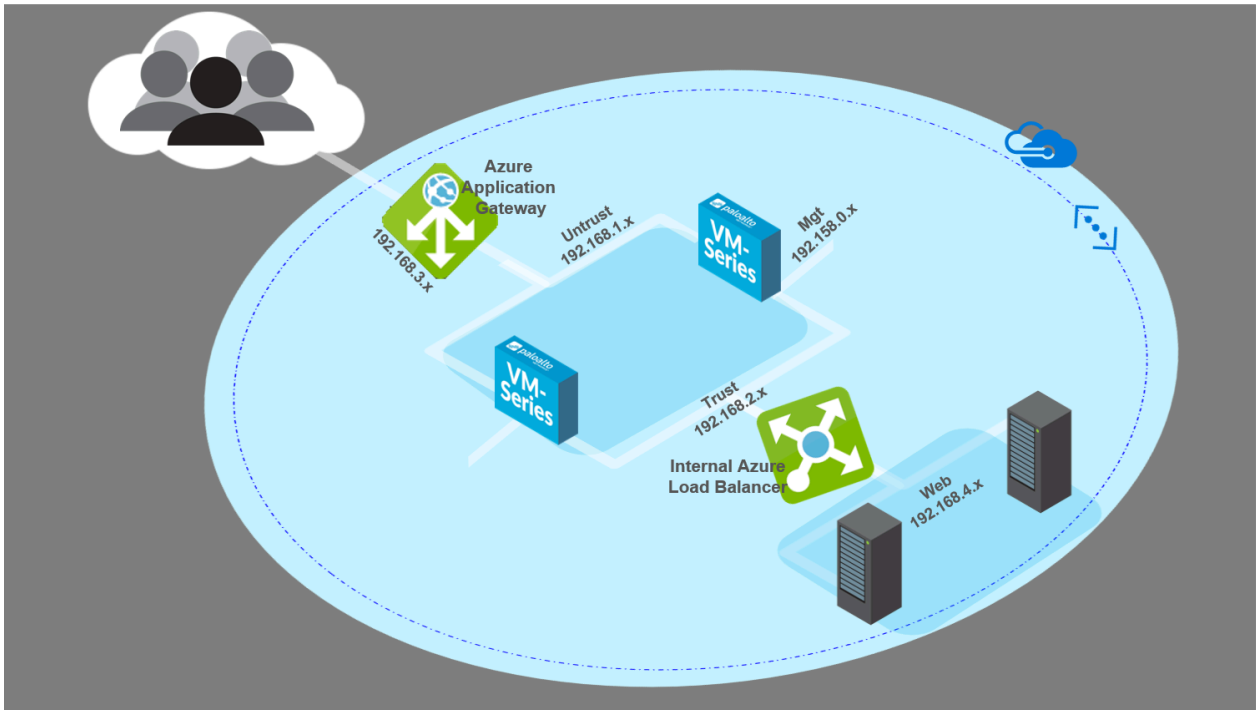
 ©2024 Palo Alto Networks, Inc.

部署 VM 系列和 Azure 应用程序网关模板

VM 系列和 Azure 应用程序网关模板是一款入门工具包，可用于部署 VM 系列防火墙以保护 Microsoft Azure 上的面向 Internet 部署的 Web 工作负载（目前不适用于 Azure China）。

该模板在一对（外部和内部）Azure 负载均衡器之间部署两个 VM 系列防火墙。外部负载均衡器是一个 Azure 应用程序网关，它是一个 HTTP（第 7 层）负载均衡器，也可作为面向 Internet 的网关，用于接收流量并通过 VM 系列防火墙将其分配到内部负载均衡器。内部负载均衡器是面向一对 Web 服务器的 Azure 负载均衡器（第 4 层）。该模板支持 VM 系列防火墙的 BYOL 和 Azure Marketplace 版本。

随着 Web 工作负载需求的增加以及您增加 Web 服务器层的容量，您可以手动部署其他 VM 系列防火墙来保护您的 Web 服务器层。



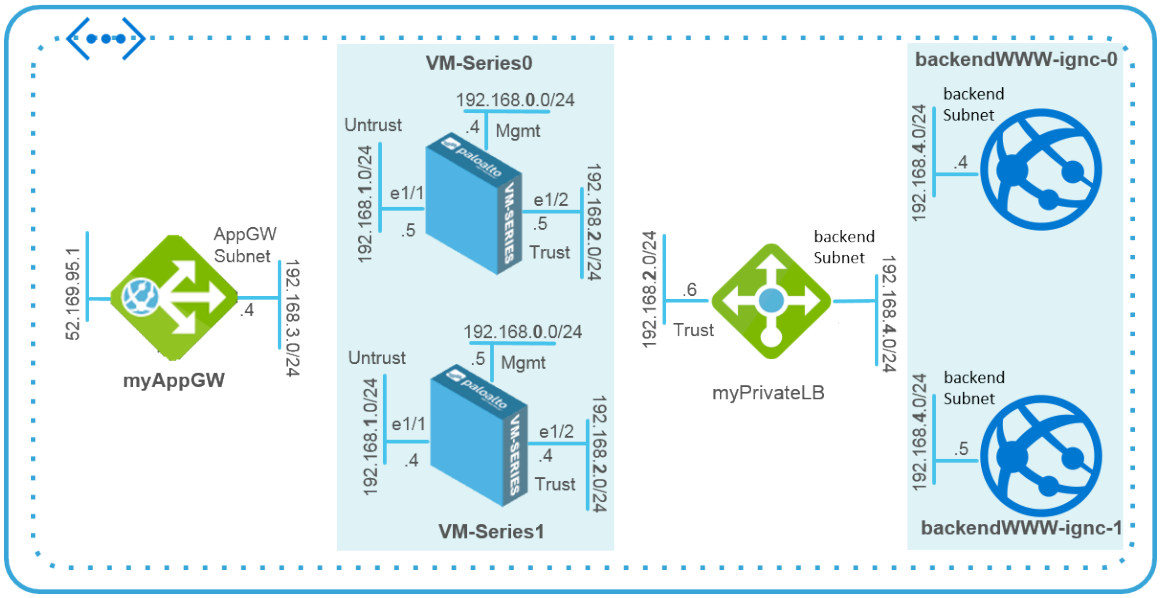
- VM 系列和 Azure 应用程序网关模板
- 开始使用 VM 系列和 Azure 应用程序网关模板

VM 系列和 Azure 应用程序网关模板

VM 系列和 Azure 应用程序网关模板将启动 Azure 应用程序网关（第 7 层负载均衡器）和 Azure（第 4 层）负载均衡器。在应用程序网关和负载均衡器之间嵌套的是可用性集中的一对 VM

©2024 Palo Alto Networks, Inc.

系列防火墙，以及在另一个可用性集中的 Ubuntu 上运行 Apache2 的一对示例 Web 服务器。可用性集提供了防止计划内和计划外停机的保护。以下拓扑图显示模板部署的资源：



您可以使用新的或现有的存储帐户和资源组来在 Azure 位置中部署此解决方案的所有资源。它不提供资源组名称和存储帐户名称的默认值，您必须输入相应地名称。虽然您可以创建新的或使用现有的 VNet，但该模板会使用 CIDR 块 192.168.0.0/16 创建一个名为 *vnet-FW* 的默认，并分配五个子网 (192.168.1.0/24 - 192.168.5.0/24) 来部署 Azure 应用程序网关、VM 系列防火、Azure 负载均衡器和 Web服务器。每个 VM 系列防火墙都部署有三个网络接口：管理子网中的 ethernet0/1 (192.168.0.0/24)，不可信子网中的 ethernet1/1 (192.168.1.0/24) 和可信子网中的 ethernet1/2 (192.168.2.0/24)。

该模板创建一个网络安全组 (NSG)，允许来自端口 80、443 和 22 上的任何源 IP 地址的入站流量。它还在其各自的可用性集中部署这对 VM 系列防火墙和 Web 服务器对，以确保在有计划或无计划的维护时段内至少有一个实例可用。每个可用性集都配置为使用三个故障域和五个更新域。

Azure 应用程序网关充当反向代理服务，它终止客户端连接并将请求转发到后端 Web 服务器。Azure 应用程序网关使用 HTTP 侦听器进行设置，并使用默认运行状况探测器来测试 VM 系列防火墙IP地址（对于 ethernet1/1）是否健康并可以接收流量。

该模板不提供自动扩展解决方案；您必须计划容量需求，然后为您的部署分配更多资源到 调整模板。

VM 系列防火墙未配置为接收并保护发往 Web 服务器的网络流量。因此，至少必须使用静态路由配置防火墙，以将流量从 VM 系列防火墙发送到默认路由器，配置目标 NAT 策略以将流量发送回负载均衡器的IP地址，并配置安全策略规则。NAT 策略规则还需要防火墙将响应从 Azure 应用程序网关上的 HTTP 侦听器发回到健康探测器。为了帮助您进行基本的防火墙配置，GitHub 存储库包含一个名为 *appgw-sample.xml* 的示例配置文件，您可以用它开始。

©2024 Palo Alto Networks, Inc.

开始使用 VM 系列和 Azure 应用程序网关模板

VM 系列 和 Azure 应用程序网关模板将启动部署和保护您的 Web 工作负载所需的全部资源，以便在 Microsoft Azure 上面向 Internet 的部署（不包括 Azure China）。本节详细介绍了如何部署模板，配置防火墙以发送和保护发往 Web 服务器的流量，并扩展此模板提供的功能和资源以满足部署需求。

- 将模板部署到 Azure
- VM 系列和 Azure 应用程序网关模板参数
- 示例配置文件
- 调整模板

将模板部署到 **Azure**

使用以下说明将模板部署到 Azure。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2024 Palo Alto Networks, Inc.

STEP 1 | 部署模板。

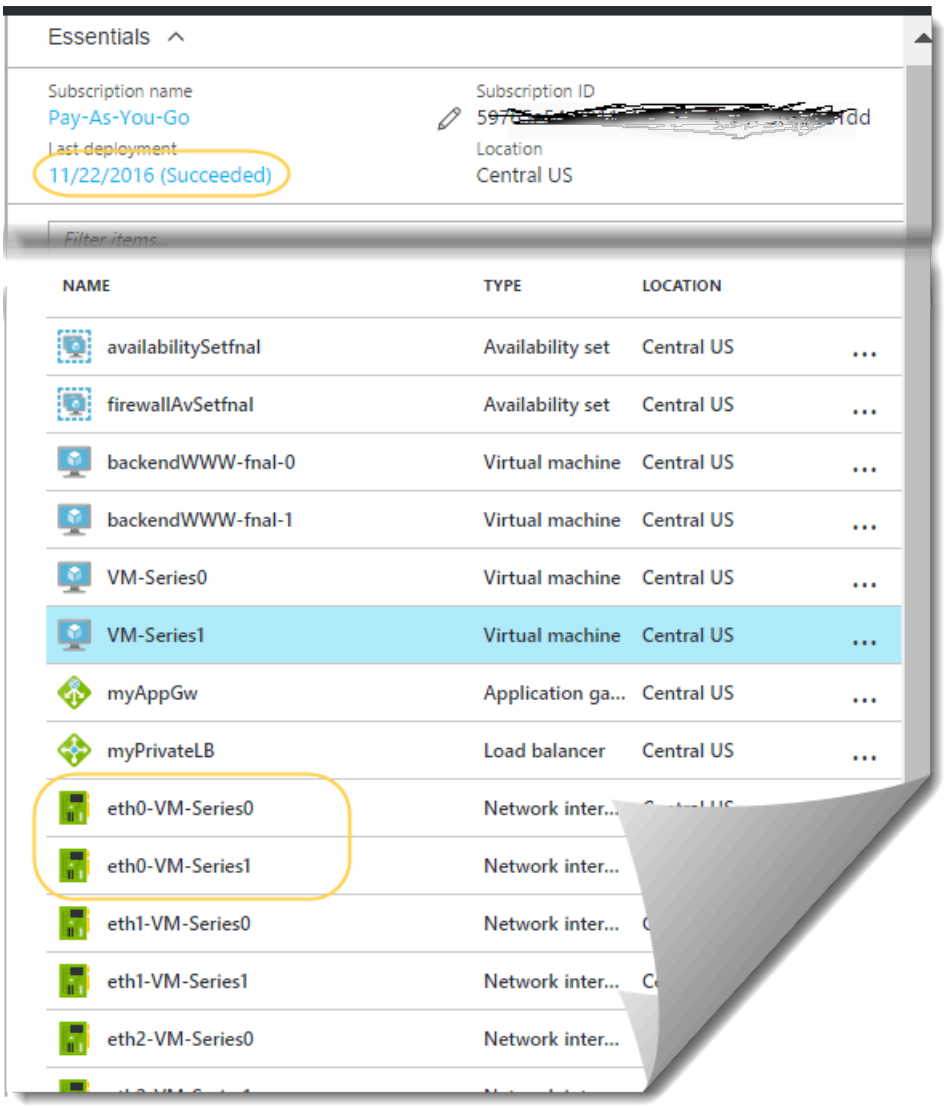
目前无法在 *Azure China* 中进行部署。

1. 从 https://github.com/PaloAltoNetworks/azure-applicationgateway访问模板
2. 单击 **Deploy to Azure**（部署到 **Azure**）。
3. 填写部署模板的详细信息。请参阅VM 系列和 Azure 应用程序网关模板参数，获取每个参数的说明和缺省值（如果有的话）。

   至少，您必须选择 **Azure Subscription**（**Azure** 订阅）、**Resource Group**（资源组）、**Location**（位置）、**Storage Account Name**（存储帐户名称） 和 VM 系列防火墙上的管理帐户的 **Username/password**（用户名/密码） 或 **SSH Key**（**SSH** 密钥）。
4. 单击 **Purchase**（购买）接受条款和条件并部署资源。

   如果出现验证错误，请单击以查看详细信息并修复错误。
5. 在Azure门户上，确认您已成功部署模板资源，包括 VM 系列防火墙。
   1. 选择 **Dashboard**（仪表盘） > **Resource Groups**（资源组），然后选择所需的资源组。
   2. 选择 **Overview**（概述）审查所有已部署的资源。应显示部署状态 **Succeeded**（成功）。

©2024 Palo Alto Networks, Inc.



3. 记下分配给的公共 IP 地址或 DNS 名称 **eth0-VM-Series0** 和 **eth0-VM-Series1** 访问 VM 系列防火墙的管理界面。

STEP 2 | 登录到防火墙。

1. 使用 Web 浏览器提供的安全连接 (https) 登录到防火墙的 eth0-VM-Series0 或 DNS 名称的 IP 地址。
2. 输入您在 parameters 文件中定义的用户名/密码。您将看到证书警告；这属于正常情况。继续浏览网页。

©2024 Palo Alto Networks, Inc.

STEP 3 | 配置 VM 系列防火墙。

您可以手动配置防火墙或导入GitHub 存储库中提供的 示例配置文件，并根据您的安全需求进行自定义。

- 手动配置防火墙- 您必须至少做到以下几点：

1. 将数据面板接口配置为防火墙上的第 3 层接口（**Network**（网络） > **Interfaces**（接口） > **Ethernet**）。
2. 将静态规则添加到防火墙上的虚拟路由器。此静态规则将防火墙的不可信接口 IP 地址指定为任何发往 ethernet1/1 的流量的下一跳地址。（**Network**（网络） > **Virtual Routers**（虚拟路由器），选择路由器并单击 **Static Routes**（静态路由））。
3. 创建安全策略规则（**Policies**（策略） > **Security**（安全）），以允许防火墙上的入站流量和出站流量。
4. 添加 NAT 策略（**Policies**（策略） > **NAT**）。您必须在防火墙上创建目标 NAT 和源 NAT 规则，以将流量发送到 Web 服务器并返回给发起请求的客户端。

   目标 NAT 规则适用于所有到达防火墙不可信接口的流量。此规则需要将数据包上的目标 IP 地址转换为内部负载均衡器的目标 IP 地址，以便所有通信都被引导至内部负载均衡器和后端 Web 服务器。

   源 NAT 规则适用于来自后端 Web 服务器的所有流量，并且指向防火墙上的不可信接口。此规则将源地址转换成防火墙上可信接口的 IP 地址。
5. **Commit**（提交）更改。

   - 导入示例配置文件：
6. 下载并将示例配置文件保存到您的本地客户端。
7. 选择 **Device**（设备） > **Setup**（设置） > **Operations**（操作），并单击 **Import named configuration snapshot**（导入已命名配置快照），**Browse**（浏览）到已保存到本地的示例配置文件，然后单击 **OK**（确定）。
8. 单击 **Load named configuration snapshot**（加载已命名配置快照），选择您导入的示例配置文件 **Name**（名称），单击 **OK**（确定）。
9. 更改地址对象的 IP 地址和静态路由以匹配您使用的 CIDR 块的 IP 地址。更新地址对象以使用 eth1-VM-Series0 和 eth1-VM-Series1 的专用 IP 地址。
10. 重要信息#创建一个新的管理员用户帐户。选择 **Device**（设备） > **Administrators**（管理员），并 **Add**（添加）帐户。
11. 修改 **Hostname**（主机名）在常规设置小部件中 **Device**（设备） > **Setup**（设置） > **Management**（管理）。
12. **Commit**（提交）您的更改并注销。提交将使用示例配置文件覆盖正在运行的配置并更新您刚创建的配置。提交时，覆盖部署模板时指定的主机名和管理员用户帐户。现在，您需要使用新的管理员用户帐户和密码登录。

    - 登录到防火墙 — 使用您创建的凭据，并删除作为示例配置文件一部分导入的p andemo 管理帐户。

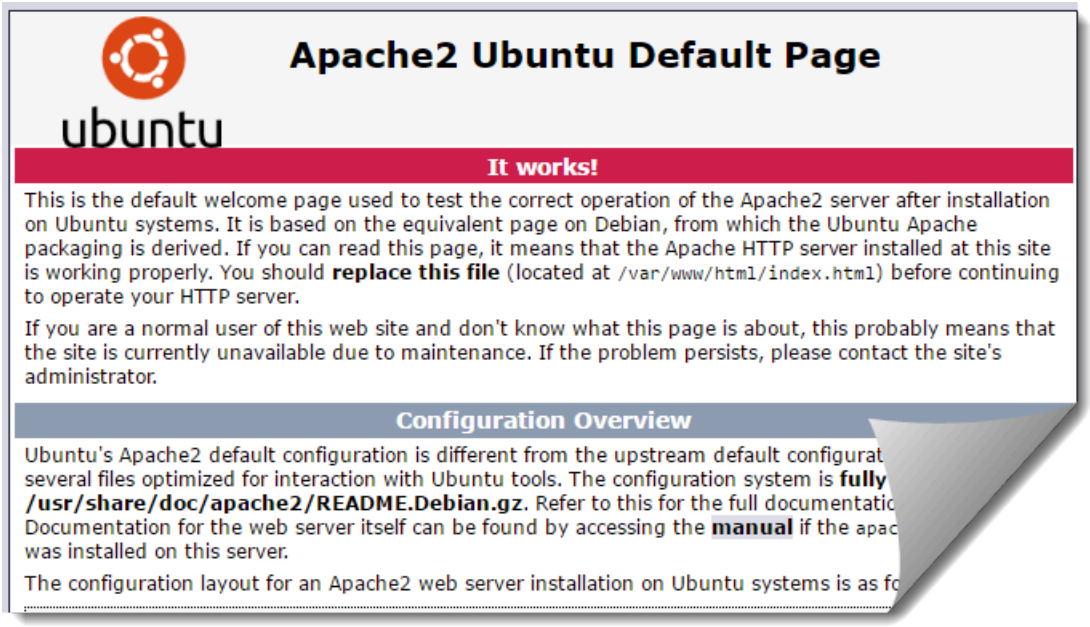
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 登录并配置 VM 系列防火墙的其他实例。

请参阅步骤 配置 VM 系列防火墙。

STEP 5 | 验证您是否已正确配置防火墙。

在 Web 浏览器中，使用 http 访问应用程序网关的 IP 地址或 DNS 名称。您应该能够查看默认的 Apache 2 Ubuntu 网页。



如果您已使用示例配置防火墙，请登录到防火墙，并在 **Monitor**（监控） > **Logs**（日志） > **Traffic**（流量）中查看会话开始时生成的流量日志。

VM 系列和 Azure 应用程序网关模板参数

下表列出了必需参数和可选参数以及默认值（如果有）。

参数	说明
资源组	创建新的或使用现有的（无默认值）。
订阅	您将使用 Azure 订阅类型来支付随模板部署的资源成本。
位置	选择要将模板部署到 Azure 的位置（无默认值）。
网络安全组	
网络安全组名称	网络安全组限制可以访问 VM 系列防火墙和 Web 服务器的源 IP 地址。 默认值：nsg-mgmt

©2024 Palo Alto Networks, Inc.

参数	说明
网络安全组入站 Src IP	可以登录模板部署的虚拟机管理端口的源 IP 地址。 默认值为 0.0.0.0/0，表示您可以从任何 IP 地址登录防火墙管理端口。
存储帐户	
存储帐户名称	新建或输入现有存储帐户的名称（无默认值）。该名称必须是全局唯一的。
存储帐户类型	在标准和高级存储与您的数据复制需求之间进行选择，以实现本地冗余、地理冗余和读取访问地理冗余。 默认选项是本地冗余存储 (LRS)。其他选项是标准 GRS、高级 LRS 和标准 RAGRS。
VNet	
虚拟网络	新建或输入现有 VNet 的名称。 VNet 的默认名称是 vnet-FW
虚拟网络地址前缀	192.168.0.0/16
Azure 应用程序网关	
应用程序网关名称	myAppGw
应用网关 DNS 名称	为 Azure 应用程序网关输入全局唯一的 DNS 名称。
应用程序网关子网名称和前缀	默认名称是 AppGWSubnet，子网前缀是 192.168.3.0/24。
Azure 负载均衡器和 Web 服务器	
内部负载均衡器名称	myPrivateLB
内部负载均衡器子网名称和前缀	默认名称是 backendSubnet，子网前缀是 192.168.4.0/24。
后端 Vm 大小	默认大小是 Azure VM 标准层 D1。使用模板中的下拉列表查看可用于后端 Web 服务器的其他 Azure VM 选项。
防火墙	

©2024 Palo Alto Networks, Inc.

参数	说明
防火墙型号	从 BYOL 或 PAYG 中选择（包 1或包 2，每个包包含 VM-300 和订阅集）。
防火墙 Vm 名称和大小	防火墙的默认名称是 VM 系列，默认大小是 Azure VM 标准层 D3 。 使用模板中的下拉列表查看可用于 VM 系列防火墙的其他Azure VM选项
管理子网名称和前缀	VM 系列防火墙的管理子网和此解决方案中部署的Web服务器。 默认名称是 Mgmt，子网前缀是 192.168.0.0/24。
Mgmt 公共 IP 地址名称	输入主机名以访问每个防火墙的管理界面。这些名称必须是全局唯一的。
可信的子网名称和前缀	VM 系列防火墙上的 eth1 / 1 所连接到的子网；此子网将 VM 系列防火墙连接到 Azure 应用程序网关。防火墙在 eth1/1上接收发往 Web 服务器的网络流量。 默认名称为可信，子网前缀为 192.168.2.0/24。
不可信的子网名称	VM 系列防火墙上的eth1 / 2所连接的子网。防火墙在此接口上接收返回和出站网络流量。 默认名称是不可信，子网前缀是 192.168.1.0/24。该名称必须是全局唯一的。
用户名	在 VM 系列防火墙和Web服务器上输入管理帐户的用户名。
身份验证类型	您必须输入密码进行身份验证或使用 SSH 公钥（无默认值）。

示例配置文件

为了帮助您入门，GitHub 存储库包含一个名为 *appgw-sample.xml* 的示例配置文件，其中包括以下规则/对象：

- 地址对象 — 两个地址对象，`firewall-untrust-IP` 和 `internal-load-balancer-IP`，您需要修改它以匹配设置中的 IP 地址。您需要修改这些地址对象以使用分配给 Azure 门户上的 eth1-VM-Series0 和 eth1-VM-Series1 的私有 IP 地址。
- 静态路由 — 防火墙上的默认虚拟路由器具有到 192.168.1.1 的静态路由，如果使用默认模板值，则此 IP 地址是准确的。如果您更改了 Untrust 子网 CIDR，则需要更新 IP 地址以符合您的设置。所有来自后端 Web 服务器的流量都是针对应用网关的，它使用此 IP 地址作为将数据包传送到防火墙上的不可信接口的下一跳。

©2024 Palo Alto Networks, Inc.

- **NAT** 策略规则 — NAT 策略规则启用目标 NAT 和源 NAT。
  - 目标 NAT 规则适用于所有到达防火墙非可信接口 (ethernet1/2) 的流量，这是防火墙 — 非可信 IP 地址对象。此规则将数据包上的目标IP地址转换为内部负载均衡器的目标 IP 地址，以便将所有流量导向内部负载均衡器，从而导向后端 Web 服务器。
  - 源 NAT 规则适用于来自后端 Web 服务器的所有流量，并且指向防火墙上的不可信网络接口。此规则将源地址转换为防火 (ethernet1/2) 上可信接口的 IP 地址。
- 安全策略规则 — 两个安全策略规则在示例配置文件中定义。第一条规则允许所有入站网页浏览流量，并在防火墙会话开始时生成日志。第二条规则阻止所有其他流量，并在防火墙的会话开始和结束时生成日志。您可以使用这些日志来监控此部署中到 Web 服务器的所有流量。
- 管理用户凭证— 示例配置文件包含登录到防火墙的用户名和密码，该防火墙设置为 pandemo/demopassword。导入示例配置后，您必须更改密码并将其设置为强大的自定义密码，或创建新的管理员帐户并删除 pandemo 帐户。

调整模板

随着您的需求的发展，您可以扩展容量需求并扩展您的部署方案的模板。您可以通过以下方式构建起始模板以满足您的计划容量需求：

- 在 Azure 应用程序网关后部署其他 VM 系列防火墙。您可以手动将更多 VM 系列防火墙安装到相同的可用性集中，或者启动新的可用性集并手动部署其他 VM 系列防火墙。
- 配置 VM 系列防火墙超出 GitHub 存储库中示例配置文件中提供的基本配置。
- 在 Azure 应用程序网关上启用 HTTPS 负载均衡（SSL 卸载）。有关详细信息，请参阅 Azure 文档。
- 添加或替换模板附带的示例 Web 服务器。

©2024 Palo Alto Networks, Inc.

在 Azure 上保护 Kubernetes 服务

要保护 Azure Kubernetes 服务，首先，您必须在 Panorama 上安装 Azure 插件，然后配置 Azure 在 Azure 上保护 Kubernetes 服务 部署。适用于 Panorama 的 Azure 插件支持基于标记的 VM 监控和在 Azure 上保护 Kubernetes 服务，保护 Azure Kubernetes 服务 (AKS) 集群的入站流量，以及监控来自 AKS 集群的出站流量。通过 Panorama 编排的部署，您可以利用 Azure 自动扩展指标以及缩小和扩展阈值，通过独立扩展 VM 系列防火墙来管理应用程序工作负载资源的突然激增的需求。

要保护 AKS 集群的入站流量，首先必须在 Azure 上保护 Kubernetes 服务。Panorama 编排的部署与在 Azure 上保护 Kubernetes 服务一起用于收集有关网络和资源的信息，然后为在 Azure 上保护 Kubernetes 服务部署创建 VM 系列防火墙的自动扩展层。请参阅 Palo Alto Networks 兼容性矩阵，以验证保护 AKS 集群所需的最低操作系统、插件和模板版本。

Palo Alto Networks 可提供 AKS 模板，用于在新的 Azure VNet 中部署 Azure Kubernetes 服务 (AKS) 集群。Panorama 上的 Azure 插件可帮助您建立连接，该连接可用于监控 Azure Kubernetes 集群工作负载，收集您已注释为“内部负载均衡器”的服务，以及创建可以在动态地址组中使用的标记。您可以利用 Panorama 动态地址组将安全策略应用到 AKS 集群上运行的服务的入站流量。

- 适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？
- 保护 AKS 集群

适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？

您可以使用 VM 系列防火墙保护 Azure Kubernetes 服务 (AKS) 集群的入站流量。VM 系列防火墙只能保护负载均衡器（例如 Azure 负载均衡器）公开的服务。此外，只能监控出站流量。

本章介绍了用来将适用于 Panorama 的 Azure 插件连接到 AKS 集群的不同组件。

- 要求
- 保护 AKS 集群的简单星型拓扑
- 用户定义的路由
- AKS 集群通信
- 具有 Kubernetes 标签的动态地址组

要求

该解决方案需要以下组件。有关最低版本要求，请参阅兼容性矩阵中的 Panorama 插件版本信息。

- VM 系列防火墙。
- Panorama — Panorama 版本必须与 VM 系列 PAN-OS 版本相同或更高。
- 适用于 Azure 的 Panorama 插件。
- Panorama 编排部署。

©2024 Palo Alto Networks, Inc.

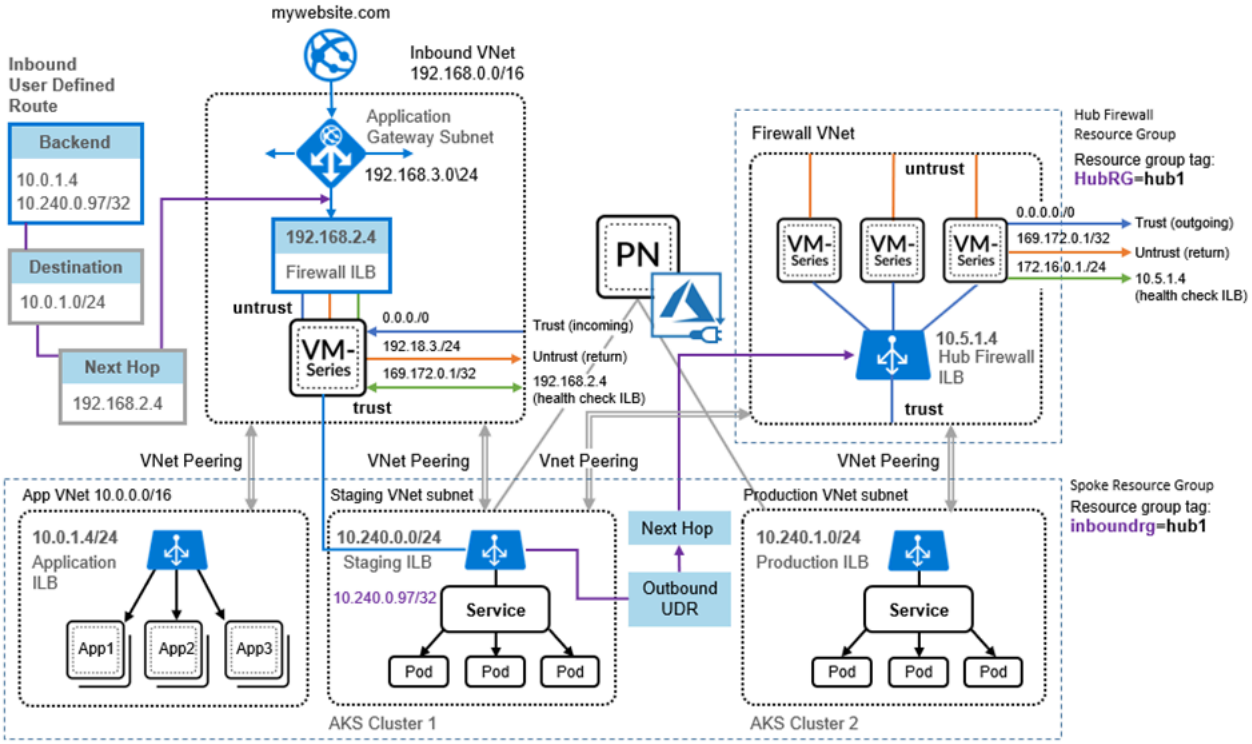
- Azure AKS 模板版本 1.0。此模板用于创建 AKS 群集。

  您必须为群集启用 AKS 高级网络 (CNI)。

  AKS 部署需要高级网络才能为中心辐射型 VNet 配置 VNet 对等（参阅 保护 AKS 集群的简单星型拓扑）。

保护 AKS 集群的简单星型拓扑

下图说明了保护 Azure AKS 集群的入站流量的自动扩展部署示例。请查看其中的一些组件。



- 自动扩展基础架构 — Azure 自动扩展模板可创建消息基础架构和基本星型体系结构。
- **AKS** 集群 — Palo Alto Networks AKS 模板可在新的 VNet 中创建 AKS 集群。如果指定星型资源组的名称，该模板将使用星型资源组名称标记 VNet 和 AKS 集群，以便可以通过适用于 Panorama 的 Azure 自动扩展插件发现资源组。适用于 Panorama 的 Azure 插件查询临时 ILB 上的服务 IP 地址，以了解 AKS 集群服务。

  只能将一个星型防火墙规模集与 *AKS* 集群相关联；如果您在单个 *AKS* 集群中公开多个服务，则必须由同一星型防火墙规模集提供保护。

  对于每个资源组，可创建基于子网的地址组。例如，在上图中，为 *10.240.0.0/24*（*AKS* 集群 *1*）创建地址组。

©2024 Palo Alto Networks, Inc.

- **VNet** 对等 — 您必须手动配置 VNET 对等才能与同一区域中的其他 VNet 进行通信。

  不支持跨区域对等。

  您可以使用其他自动化工具部署 *AKS* 集群。如果您在现有 *VNet*（例如中心防火墙 *VNet*）中部署，必须手动将 *VNet* 对等配置为入站和出站星型资源组，并使用资源组名称手动标记 *VNet* 和 *AKS* 集群。
- 用户定义的路由和规则 — 您必须手动配置用户定义的路由和规则（参阅用户定义的路由）。在上图中，可以根据 UDR 规则将传入流量重定向到防火墙 ILB 进行检查。您可以使用 Azure 用户定义的路由 (UDR) 规则，将退出 AKS 集群的出站流量重定向到中心防火墙 ILB。该解决方案假定允许所有作为 Kubernetes 编排的默认策略按原样运行，但是要应用策略，您可以使用允许列表或拒绝列表来允许或拒绝出站流量。

用户定义的路由

您必须手动创建用户定义的路由和路由规则，以控制入站流量或出站流量。

入站

在上图中，来自应用程序网关的入站流量被驱动到后端池，并根据 UDR 规则重定向到防火墙 ILB。例如，创建指向 VNet 子网的 UDR，以便将 Kubernetes 服务的流量指向防火墙 ILB。

出站

在中心防火墙规模集上，对于保护的每个 AKS 集群，您必须为集群子网 CIDR 创建静态路由，并且下一个跃点是中心 VNet 可信子网的网关地址。

AKS 集群的所有出站流量都将通过单个 UDR 规则定向到中心防火墙规则模板集。

AKS 集群通信

适用于 Azure 的 Panorama 插件只能与给定 AKS 集群的 AKS 控制器节点通信。对于出站 AKS 流量，下一个跃点是中心防火墙 ILB。由于出站流量受到监控，因此您必须允许所有流量。以下主题重点介绍了可帮助您建立连接的常见做法。请在规划网络和子网时谨记。

- 创建 AKS 集群身份验证
- 使用地址组标识流量
- 将子网地址组添加到顶级策略
- 对等工作负载和 AKS 集群 VNet 时防止应用程序中断

创建 **AKS** 集群身份验证

当在适用于 Panorama 的 Azure 插件中连接 AKS 集群时，您必须输入身份验证令牌。您可以使用 Kubernetes 命令执行以下步骤。

STEP 1 | 创建 ClusterRole。

©2024 Palo Alto Networks, Inc.

STEP 2 | 创建 ClusterRoleBinding。

1. 为 ClusterRoleBinding 创建 `.yaml` 文件。例如，创建名为 `crb.yaml` 的文本文件。

```
  apiVersion: rbac.authorization.k8s.io
   kind:ClusterRoleBinding   metadata:      name: default-
view   roleRef:     apiGroup: rbac.authorization.k8s.io
     kind:ClusterRole     name: view   subjects:   -
 kind:ServiceAccount   name: default   namespace: default
```

2. 使用 Azure Cloud Shell 以应用 `crb.yaml` 角色绑定。

   kubectl apply -f crb.yaml

3. 查看刚才创建的服务帐户。

   kubectl get serviceaccounts

STEP 3 | 将服务帐户凭据保存到 `.json` 文件。

1. 在本地计算机上，切换到要保存凭据的目录。
2. 使用 kubectl 命令创建令牌。

   MY_SA_TOKEN= ‘kubectl get serviceaccounts default -o jsonpath=’ {.secrets[0].name}’ ‘

3. 查看令牌名称。

   $ echo $MY_SA_TOKEN

4. 显示凭证。

   kubectl get secret $MY_SA_TOKEN -o json

在适用于 Panorama 的 Azure 插件中连接 AKS 集群时，您需要在步骤 3.d 中获得的令牌。

使用地址组标识流量

要为监控的出站流量创建一些粒度，请为 AKS 集群 VNet 子网专门创建地址组（例如，上图中的 10.240.0.97/32）。然后，您可以编写允许传入或传回流量的规则，而不是使用允许所有。

如果创建地址组，请小心保持 AKS 控制器与任何工作节点之间的通信。请参阅将子网地址组添加到顶级策略。

如果通信中断，则应用程序流量可能会丢失或应用程序部署可能会出现问题。

将子网地址组添加到顶级策略

要保持连接，地址组必须是 Panorama 中顶级策略的一部分。您可以配置集群地址组，也可以引导集群以配置集群地址组。

在配置 *VNet* 对等或用户定义的路由之前，将地址组添加顶级策略。

©2024 Palo Alto Networks, Inc.

对等工作负载和 **AKS** 集群 **VNet** 时防止应用程序中断

如果 AKS 集群与在单独的 VNet 中运行的 VM 工作负载共存，并且 VNet 与工作负载星型（入站）和中心（出站）同时对等，则您必须创建地址组以区分工作负载和 AKS 流量，并将地址组添加到顶级策略，如上所述。

具有 Kubernetes 标签的动态地址组

监控 AKS 集群资源时，Azure 插件为 AKS 服务自动生成以下 IP 标记。

```
aks.<aks cluster name>.<aks service name>
```

不会为节点、*Pod* 或其他资源生成标记。

如果 AKS 服务包含任何标签，则标记如下所示（每个标签一个服务）：

```
aks.<aks cluster name>.svc.<label>.<value>
```

如果您已为集群定义 labelSelector 标记，则插件将生成以下 IP 标记：

```
aks_<labelSelector>.<aks cluster name>.<aks service name>
```

保护 AKS 集群

要使 Panorama 能够连接到 Azure Kubernetes 服务 (AKS) 集群，您必须在 Panorama 上启用 Azure 插件与 AKS 集群建立连接。然后，您必须配置防火墙所属的设备组和模板，以便 Panorama 可以将配置对象和策略规则推送到托管防火墙。

- 准备工作
- 使用模板部署 AKS 集群
- 在适用于 Panorama 的 Azure 插件中连接 AKS 集群
- 设置 VNet 对等
- 将流量重定向到防火墙 ILB
- 将策略应用于相关的 AKS 服务
- 部署和保护 AKS 服务

准备工作

要保护 AKS 的安全，首先，您必须部署 GitHub 上提供的 Azure 自动扩展解决方案。

要保护在 Kubernetes 群集中作为服务运行的 Web 应用程序的安全，您必须规划 VNet、子网和 UDR。VM 系列防火墙和 Panorama 可为您提供 Kubernetes 服务的安全性和可见性。

- 查看“适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？”。

©2024 Palo Alto Networks, Inc.

- 您必须有 AKS 高级网络才能使用 Palo Alto Networks AKS 模板。
- 在部署 AKS 群集之前，您要设计 AKS 子网。查看 保护 AKS 集群的简单星型拓扑，并AKS 集群通信。
  - 该模板将创建单个 AKS 集群（服务），以作为示例。您必须指定 VNet、VNet 子网和服务的 CIDR 范围。CIDR 范围不能重叠
  - 根据您的要求调整子网大小。除非必要，请避免设置过大的范围，因为这可能会影响性能。
  - 请参阅 用户定义的路由。指定特定的 UDR 路由，而不是广泛的子网特定路由。
- 计划要如何对等 VNet。如果要对等 AKS 集群，请确保已阅读AKS 集群通信。
- 考虑要标识流量的方式。
  - 如果计划在出站 AKS 流量上使用地址组，请参阅将子网地址组添加到顶级策略。
  - 如果整个命名空间内的服务名称或标记中不是唯一的，请使用标签选择器筛选标记和命名空间，从而获得唯一的结果。

使用模板部署 AKS 集群

Azure AKS 模板是在新的 VNet 中配置集群的示例。

STEP 1 | 在 GitHub 上，转到 PaloAltoNetworks/azure-aks，并在存储库中找到构建包。

STEP 2 | 解压构建包。编辑 `azuredeploy.json` 和 `parameters.json` 文件进行自己的部署，然后保存。

STEP 3 | 发出以下 Azure CLI 命令以部署模板。

```
az group deployment validate --resource-group RG_NAME --template-
file azuredeploy.json --parameters @parameters.json
```

```
az group deployment create --name DEPLOYMENT_NAME --resource-
group RG_NAME --template-file azuredeploy.json --parameters
 @parameters.json
```

STEP 4 | 在 AKS 集群上部署应用程序或服务。

1. 注释服务 YAML 文件，以使类型为负载均衡器，并将其注释为 service.beta.kubernetes.io/azure-load-balancer-internal: "true"。例如：

```
  apiVersion: v1     kind:Service   metadata:
 name: azure-vote-front    labels:    service: "azure-
vote-front"    tier: "stagingapp"    annotations:
 service.beta.kubernetes.io/azure-load-balancer-internal:
 "true"   spec:    type:LoadBalancer ports: - port:80
 selector: app: azure-vote-front
```

2. 如果您还没有这样做，请在继续操作之前创建 AKS 集群身份验证。

©2024 Palo Alto Networks, Inc.

3. 在 AKS 集群上部署服务。

   例如，您可以通过以下 kubectl 命令部署应用程序：

   ```
   kubectl apply -f myapplication.yaml
   ```

   有关示例，请参阅：https://github.com/Azure-Samples/azure-voting-app-redis/blob/master/azure-vote-all-in-one-redis.yaml

4. 使用以下 kubectl 命令获取已部署服务的服务 IP 地址。

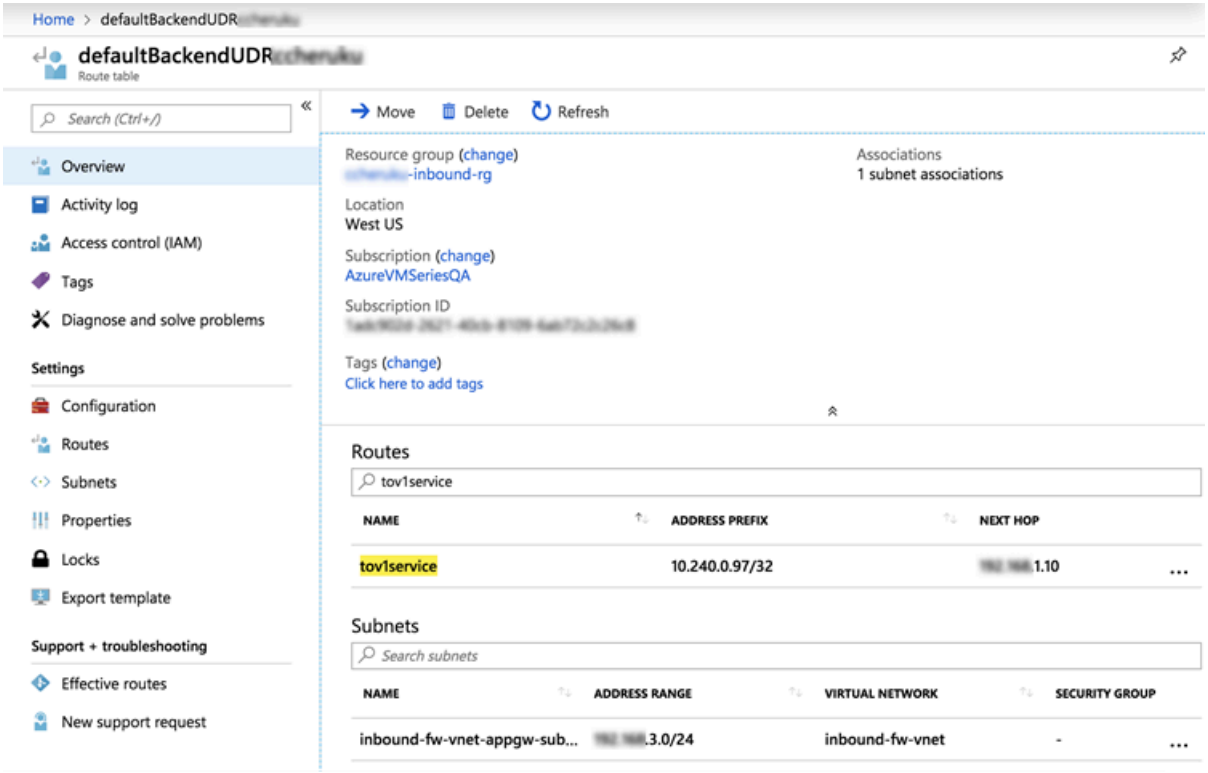
   ```
   kubectl get services -o wide
   ```

```
NAME              TYPE           CLUSTER-IP     EXTERNAL-IP   PORT(S)        AGE    SELECTOR
azure-vote-back   ClusterIP      10.0.77.21     <none>        6379/TCP       2d23h  app=azure-vote-back
azure-vote-front  LoadBalancer   10.0.18.189    10.240.0.97   80:31937/TCP   2d23h  app=azure-vote-front
kubernetes        ClusterIP      10.0.0.1       <none>        443/TCP        2d23h  <none>
```

   根据步骤 a 中的注释，EXTERNAL-IP 列中的 10.240.0.97 是 ILB 的 IP 地址。使用服务 IP 地址在 Azure 上创建用户定义的路由。

STEP 5 | 创建 UDR 规则以将服务指向应用程序网关后面的防火墙 ILB。

在 Azure 中，转到入站分支资源组，查看路由表并根据目标服务 IP 地址添加新路由。在以下屏幕截图中，tov1service **ADDRESS PREFIX**（地址前缀）列中的值为服务 IP 地址。



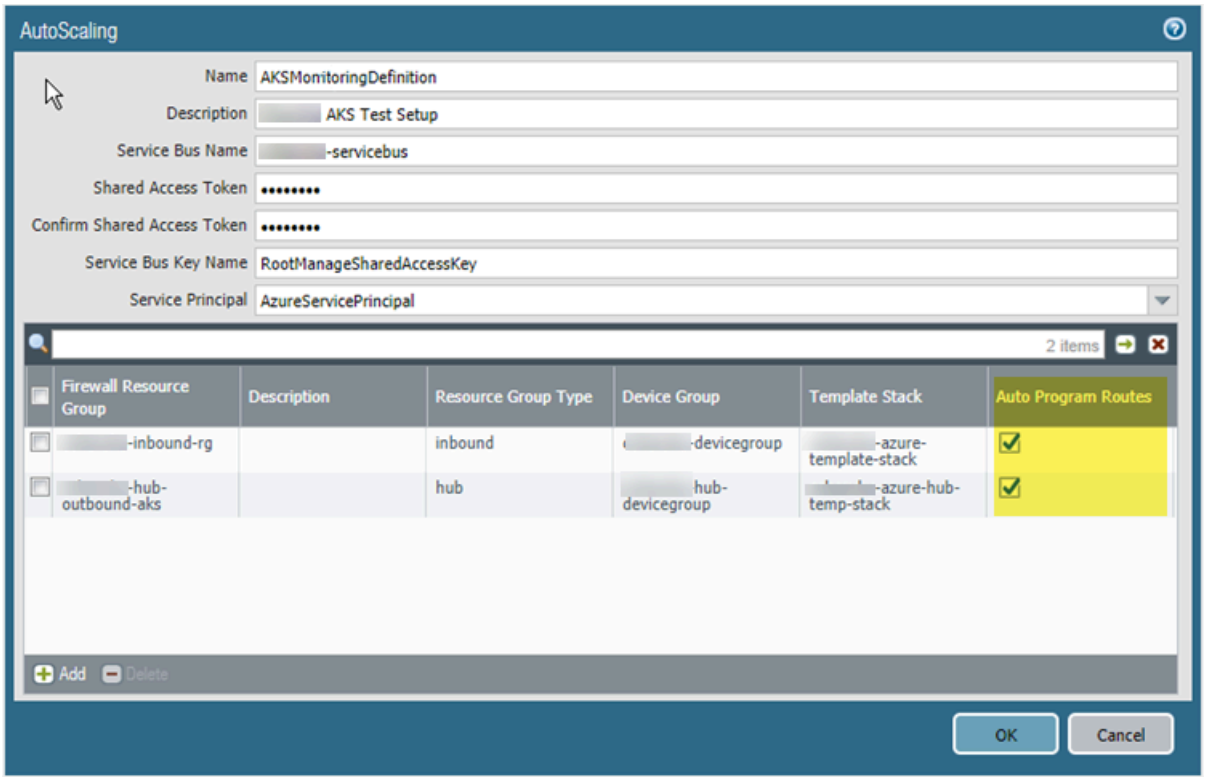
在适用于 **Panorama** 的 **Azure** 插件中连接 **AKS** 集群

该任务假设您已部署 Panorama 编排部署，并且已创建模板、模板堆栈和设备组。

©2024 Palo Alto Networks, Inc.

有关填写每个表单的更多信息，请参阅 Panorama 在线帮助。

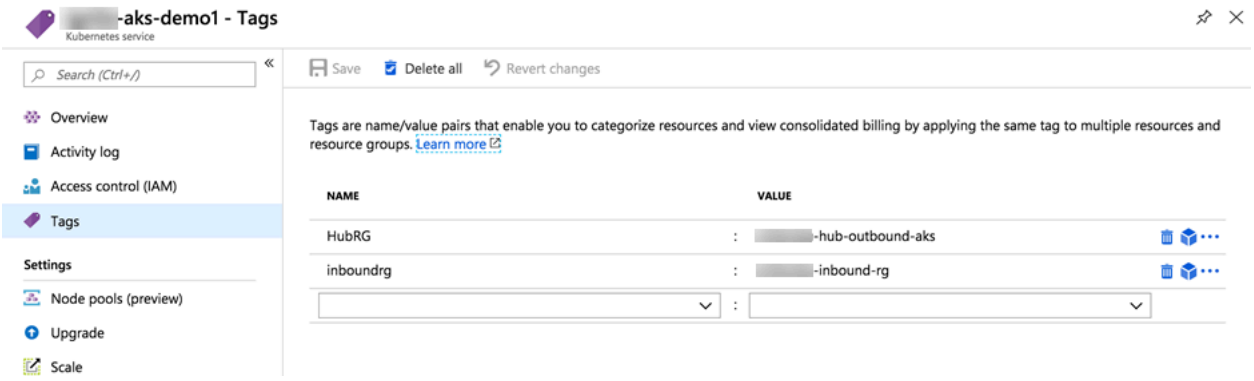
STEP 1 | 选择 **Panorama** > **Azure** > **Deployments**（部署），以查看您在配置部署时创建的监控定义。如下所示，如果已启用 **Auto Program Routes**（自动编程路由），则会为您编程防火墙路由。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在 AKS 中，标记资源组。标记是名称/值对。

1. 丢 **Home**（主页） > **Resource groups**（资源组），然后选择资源组。
2. 选择 **Tags**（标记）并定义名称/值对。如下图所示，标记名称必须是 inboundgrouprg 和 HubRG：
   - inboundgrouprg — 分支资源组名称
   - HubRG — 中心资源组名称



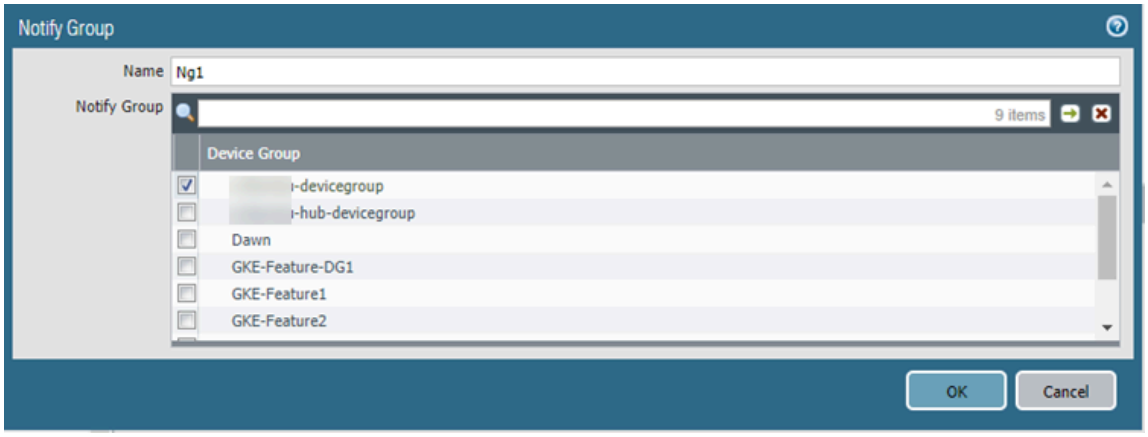
该模板将分支资源组的名称用作参数，并使用分支资源组名称标记 VNet 和 AKS 集群，以便适用于 Azure 的 Panorama 插件可以发现资源组。

该模板在单独的 *VNet* 中部署资源组。如果您在与分支防火墙集相同的 *VNet* 中手动部署 *AKS* 集群和服务，则必须手动为分支资源组名称创建标记。

©2024 Palo Alto Networks, Inc.

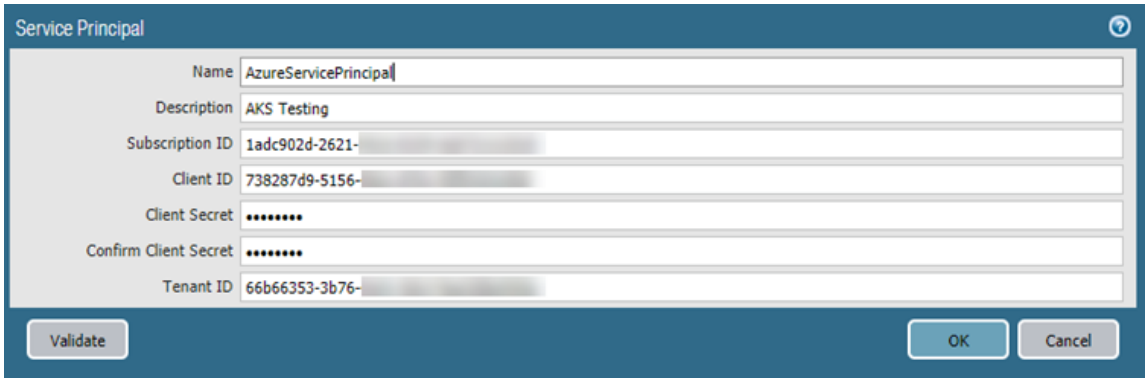
STEP 3 | 在 Panorama 中，选择 **Panorama** > **Azure** > **Setup**（设置）。

1. 在 **General**（常规）选项卡上，启用监控。
2. 在 **Notify Groups**（通知组）选项卡上，**Add**（添加）通知组并选择要通知的设备组。



3. 在 **Service Principal**（服务主体）选项卡上，**Add**（添加）并 **Validate**（验证）服务主体。

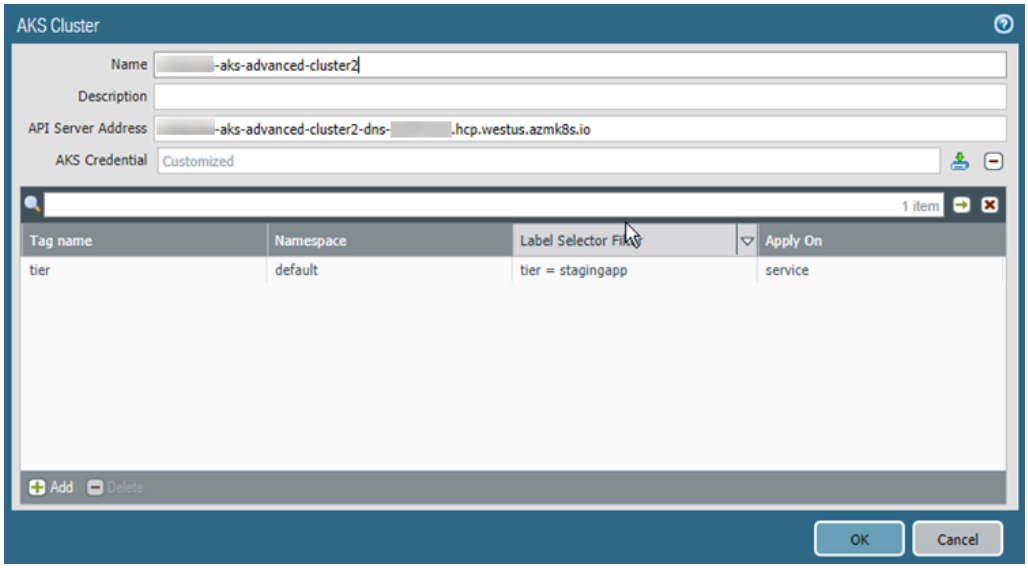
   使用您为编排部署创建的服务主体。



4. 在 **AKS Cluster**（**AKS** 集群）选项卡上，**Add**（添加）AKS 集群。
   - 输入 AKS 集群的确切名称。
   - 输入 API 服务器地址。要在 Azure 中查找地址，请查看 AKS 服务，然后选择 Overview（概述）。
   - 上传 AKS 凭据 JSON 文件（参阅创建 AKS 集群身份验证）。
5. 填写其余字段，然后 **Add**（添加）一个或多个标记。

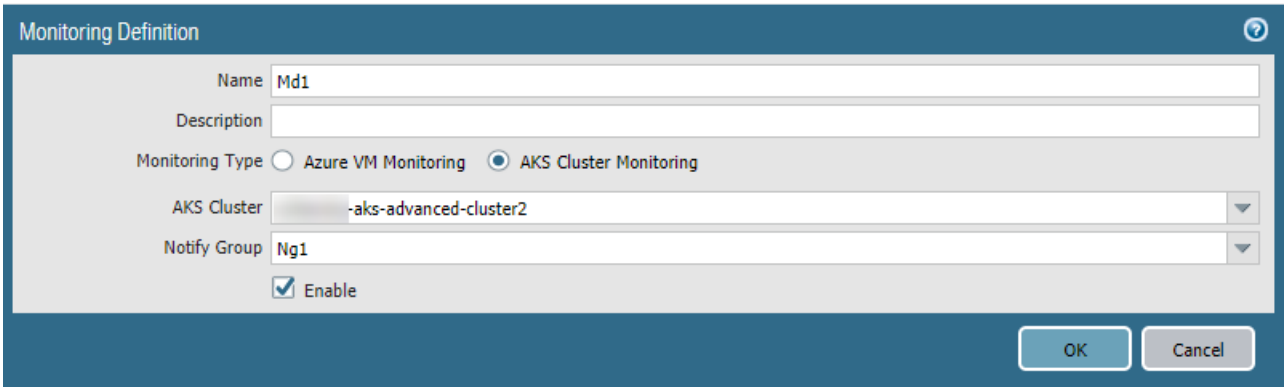
   如果服务名称或标记在整个命名空间中不是唯一，请使用标签选择器同时筛选标记和命名空间，以使其成为唯一。

©2024 Palo Alto Networks, Inc.



STEP 4 | 选择 **Panorama** > **Azure** > **Monitoring Definition**（监控定义）。

1. 添加监控定义。
2. 输入名称和说明，然后选择 **AKS Cluster Monitoring**（**AKS** 集群监控）。
3. 选择 **AKS Cluster**（**AKS** 集群）和 **Notify Group**（通知组），选中 **Enable**（启用），然后单击 **OK**（确定）。



设置 VNet 对等

如果您计划使用地址组标识流量，请确保在配置对等之前将子网地址组添加到顶级 Panorama 策略。

部署 AKS 集群后，从入站 VNet 到集群，以及从集群到防火墙 VNet 设置 VNet 对等。

将流量重定向到防火墙 ILB

您必须手动创建用户定义的路由 (UDR) 和路由规则，以将流量重定向到特定 ILB。有关示例，请参阅“适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？”中介绍入站 UDR 的示意图。

STEP 1 | 创建 URL 路由规则以将 Web 流量重定向到合适的后端池。

©2024 Palo Alto Networks, Inc.

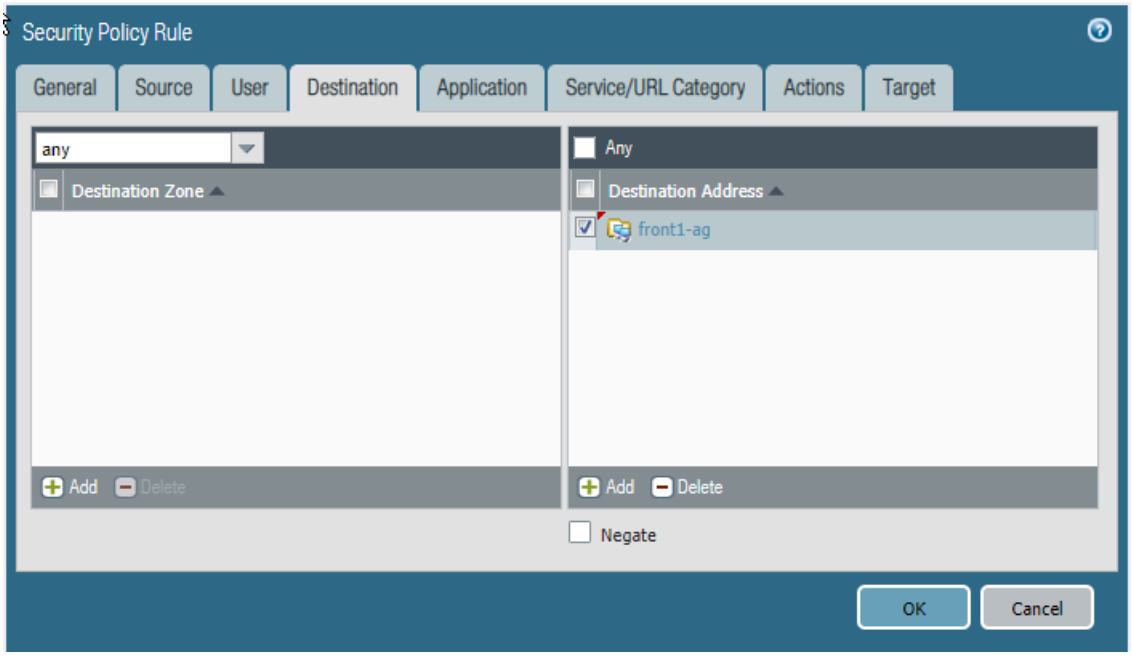
STEP 2 | 更新应用程序网关子网的 UDR 规则以添加服务 CIDR 的路由，下一个跃点是分支防火墙资源组中的入站防火墙负载均衡器。

将策略应用于相关的 AKS 服务

STEP 1 | 在 Panorama 中，选择 Policies（策略）。

STEP 2 | 在 **Device Group**（设备组）列表中，选择 AKS 服务的设备组。

STEP 3 | **Add**（添加）安全策略规则。填写表单，然后在 **Destination**（目标）选项卡上 **Add**（添加）目标地址或地址组。



部署和保护 AKS 服务

这些步骤概述了如何使用 VM 系列防火墙和适用于 Panorama 的 Azure 插件保护遍历 Kubernetes 服务的入站和出站流量。

STEP 1 | 在应用程序部署环境中，为应用程序创建 YAML 文件或使用已存在的文件。以下是应用程序 YAML 文件示例：

```
apiVersion: apps/v1 kind:Deployment metadata:   name: azure-
vote-back spec:   replicas:1   selector:     matchLabels:
       app: azure-vote-back   template:     metadata:       labels:
         app: azure-vote-back     spec:       containers:       -
 name: azure-vote-back         image: redis         resources:
           requests:             cpu:100m             memory:128Mi
           limits:             cpu:250m             memory:256Mi
         ports:         - containerPort:6379           name:
 redis --- apiVersion: v1 kind:Service metadata:   name: azure-
vote-back   labels:     service: backend spec:   ports:   -
 port:6379   selector:     app: azure-vote-back --- apiVersion:
```


©2024 Palo Alto Networks, Inc.

```
 apps/v1 kind:Deployment metadata:   name: azure-vote-front spec:
   replicas:5   selector:     matchLabels:       app: azure-
vote-front   template:     metadata:       labels:         app:
 azure-vote-front     spec:       containers:       - name:
 azure-vote-front         image: microsoft/azure-vote-front:v1
         resources:           requests:             cpu:100m
             memory:128Mi           limits:             cpu:250m
             memory:256Mi         ports:         - containerPort:80
         env:          - name:REDIS           value: "azure-vote-
back" --- apiVersion: v1 kind:Service metadata:   name: azure-
vote-front   labels:     service: "azure-vote-front"     type:
 "production"     providesecurity: "yes"     a: "value"     b:
 "value"     c: "value"     tier: "stagingapp"   annotations:
     service.beta.kubernetes.io/azure-load-balancer-internal:
 "true" spec:   type:LoadBalancer   ports:   - port:80   selector:
     app: azure-vote-front
```

STEP 2 | 编辑 YAML 文件以标记 Kubernetes 服务。

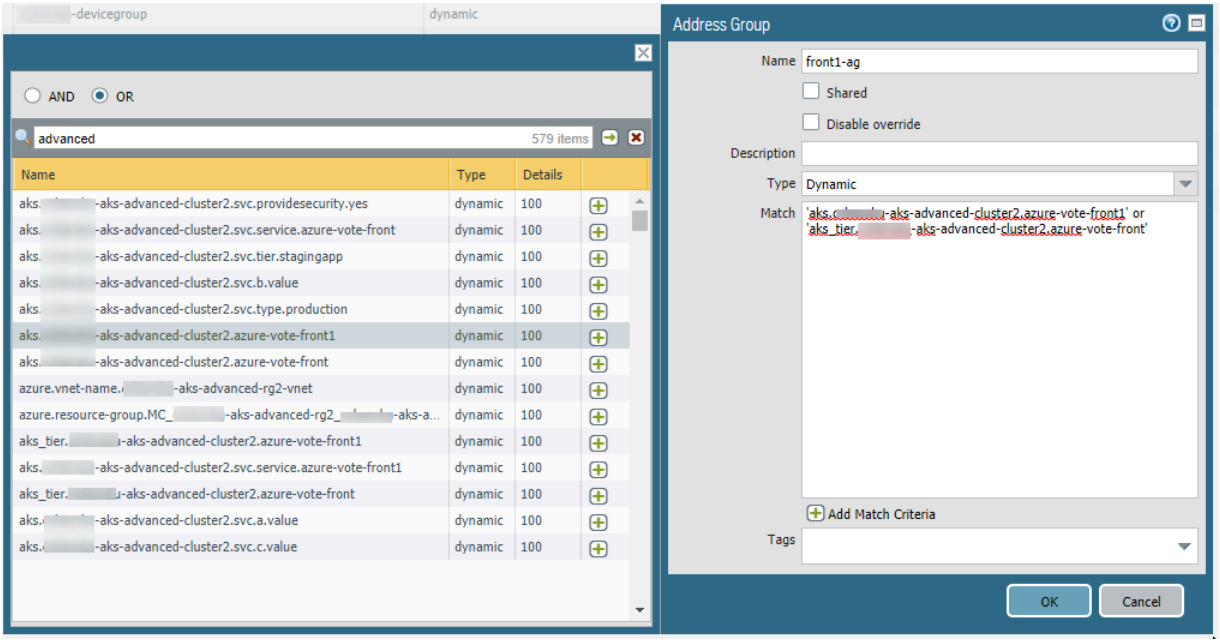
标签可支持您在使用适用于 AKS 的 Panorama 插件连接到集群时创建的相应标记到 IP 映射。例如，在上面的示例文件中，在服务元数据中查找应用程序标签。这些标签是：**azure-vote-back** 和 **azure-vote-front**。

STEP 3 | 在 AKS 集群中，应用 YAML 文件。

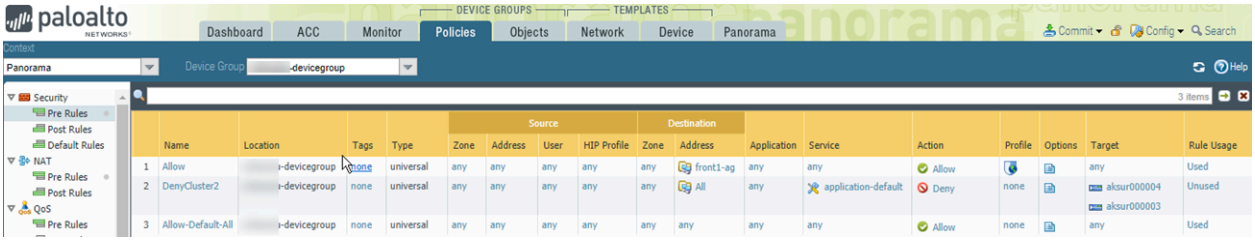
©2024 Palo Alto Networks, Inc.

STEP 4 | 在 Panorama 中，使用资源组标记创建地址组。

1. 在 **Objects**（对象）选项卡上，从 **Device Group**（设备组）列表中选择设备组。
2. 选择 **Address Groups**（地址组）并 **Add**（添加）地址组。
   1. 指定名称，然后选择 **Dynamic**（动态）类型。
   2. **Add**（添加）地址。添加操作将生成一个列出所有检测到的地址的窗口。填充列表可能需要几分钟的时间。
   3. 您可以选择一个或多个地址作为匹配条件。选择 AND 或 OR 作为条件关系。
   4. 如果您有多个地址，请在搜索框中输入一个字符串以筛选输出，如下图所示。
   5. 在地址列表中，单击 + 以将地址包括在地址组匹配条件中。
   6. 匹配条件完成后，单击 **OK**（确定）。



STEP 5 | 使用地址组显示策略。



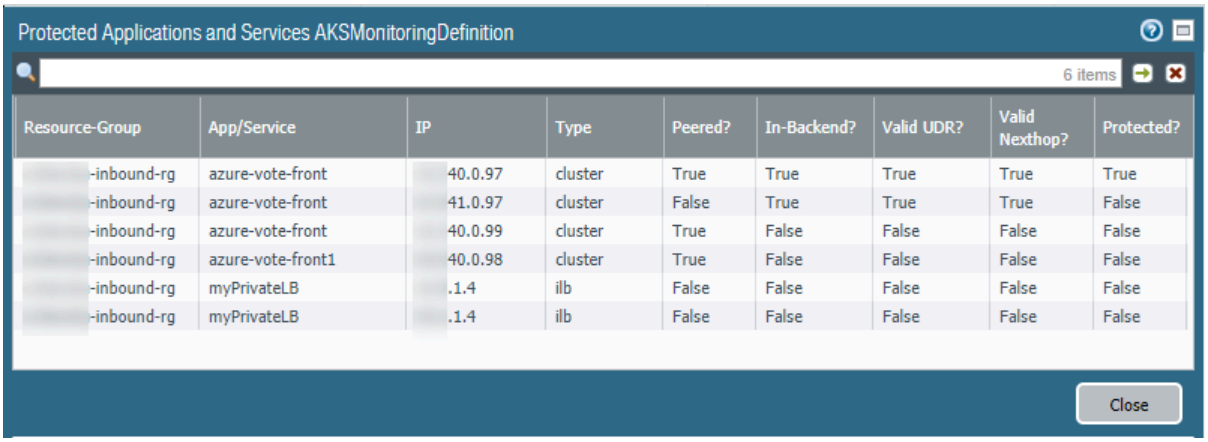
 ©2024 Palo Alto Networks, Inc.

STEP 6 | 查看保护的 AKS 服务。

在 **Panorama** > **Azure** > **Deployments**（部署）中查看监控定义，然后在 Action（操作）列中选择 **Protected Applications and Services**（保护的应用程序和服务）链接。

Protected?（保护？）列汇总了资源组的安全状态。填充该窗口可能需要几分钟的时间。如果您有多个资源组，请在搜索框中输入一个字符串以筛选输出。

此输出取决于 Azure 资源组配置；它不查询设备组或模板堆栈成员。



 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 OpenStack 上设置 VM 系列防火墙

通过适应于 OpenStack 的 VM 系列防火墙，您可以提供安全的应用程序交付以及网络安全、性能和可见性。

- 适用于 OpenStack 的 VM 系列防火墙
- 面向 OpenStack 解决方案的 VM 系列组件
- 基本网关部署的热量模板
- 服务链和服务扩展的 Heat 模板
- 在基本网关部署中安装 VM 系列防火墙
- 使用服务链或扩展来安装 VM 系列防火墙

OpenStack 中的 VM 系列部署

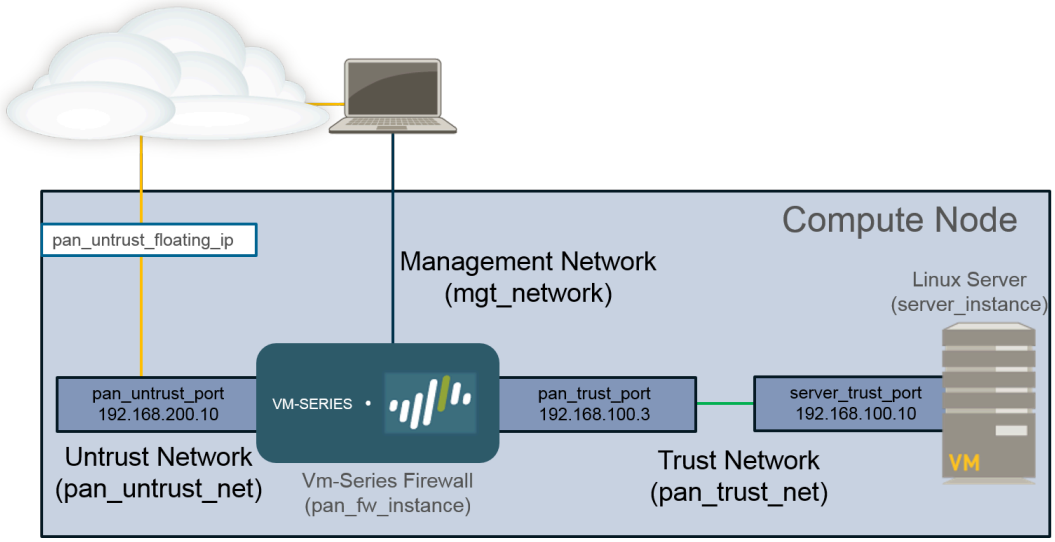
Palo Alto Networks 提供的 Heat Orchestration 模板允许您单独部署 VM 系列防火墙，通过服务链或通过服务扩展动态地部署。

- 基本网关
- 服务链和服务扩展

基本网关

用于 OpenStack 的 VM 系列防火墙允许您在 OpenStack 环境中的计算节点上运行的 KVM 虚拟机监控程序上部署 VM 系列防火墙。该解决方案使用 Heat 编排模板和引导来部署 VM 系列防火墙和 Linux 服务器。VM 系列防火墙通过检查进出服务器的流量来保护已部署的 Linux 服务器。示例引导程序文件允许 VM 系列防火墙使用基本配置进行引导，以处理流量。

这些 Heat 模板文件和引导程序文件结合在一起，创建了两个虚拟机，即 VM 系列防火墙和 Linux 服务器，其网络配置类似于下图所示。



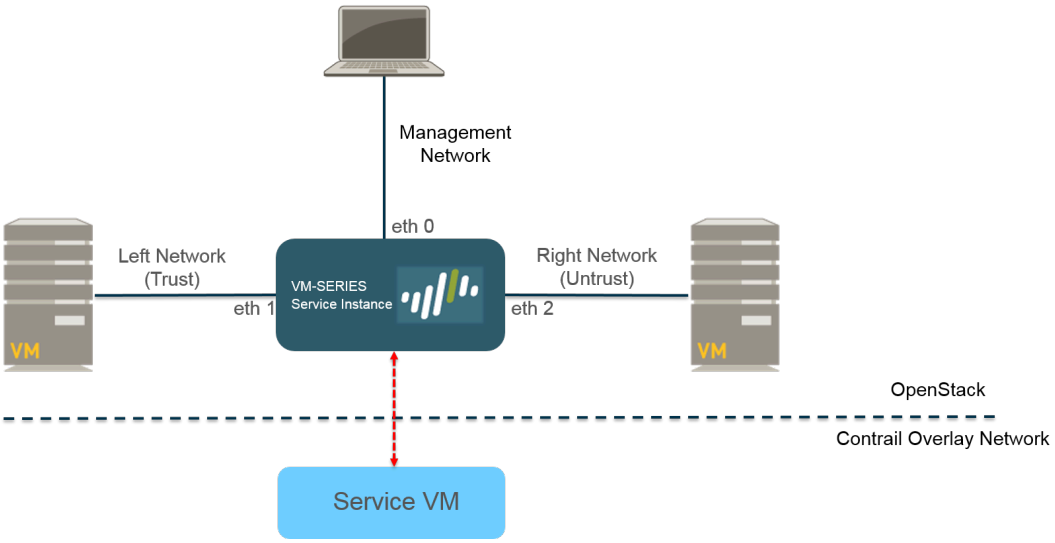
服务链和服务扩展

在 *OpenStack Queens* 上不支持通过服务链或服务扩展部署 *VM* 系列防火墙。

服务链是一种 Contrail 功能，可在您的 OpenStack 环境中将 VM 系列防火墙作为服务实例进行部署。服务链是服务虚拟机集，例如防火墙或负载均衡器，并且服务链中每个虚拟机都是服务实例。服务扩展允许您动态部署 VM 系列防火墙的其他实例。使用 CPU 利用率或 Ceilometer 收集的每秒传入字节数量，OpenStack 会部署或关闭 VM 系列防火墙的其他实例，以满足您网络的当前需求。

©2024 Palo Alto Networks, Inc.

OpenStack 解决方案中的 VM 系列防火墙利用 Heat 编排模板来配置和部署服务链和服务扩展所需的组件。Palo Alto networks 提供的 Heat 模板创建服务模板，服务实例和服务策略（将流量引导到 VM 系列防火墙），以在它们之间部署两台 Linux 服务器和 VM 系列防火墙服务实例。



©2024 Palo Alto Networks, Inc.

面向 OpenStack 解决方案的 VM 系列组件

OpenStack环境中的 VM 系列防火墙已通过以下组件进行测试。

组件	说明
软件	有关支持的软件版本的详细信息，请参阅兼容性矩阵。
VM 系列硬件资源	有关 VM 系列型号的最低硬件要求，请参阅 VM 系列系统要求。 在 OpenStack 中，风格定义了计算实例的 CPU、内存和存储容量。设置Heat模板时，请选择满足或超过 VM 系列型号硬件要求的计算风格。
Fuel Master	Fuel 是 OpenStack 的 Web UI 驱动部署和管理工具。
OpenStack 控制器	该节点运行大部分共享的 OpenStack 服务，例如 API 和计划。此外，Horizon UI 在此节点上运行。
OpenStack Compute	计算节点包含 OpenStack 部署中的虚拟机（包括 VM 系列防火墙）。容纳 VM 系列的计算节点必须符合以下标准： • 实例类型 OS :: Nova :: Server • 允许配置至少三个接口 • 接受 VM 系列qcow2映像 • 接受计算风格参数 将*OpenStack*计算节点安装在裸机服务器上，因为 *VM* 系列防火墙不支持嵌套虚拟化。
Contrail 控制器	Contrail 控制器节点是一个软件定义的网络控制器，用于虚拟化网络的管理、控制和分析。它为计算和网关节点提供路由信息。 另外，Contrail 控制器为服务链和服务扩展提供必要的支持。
Contrail 网关	Contrail 网关节点通过虚拟网络提供到外部网络的 IP 连接。来自虚拟机的 GRE 隧道上的 MPLS 终止于网关节点，其中数据包被解封并发送到 IP 网络上的目标。
Ceilometer（OpenStack 遥测）	对于 OpenStack 的 VM 系列防火墙，Ceilometer监控 CPU 利用率以进行服务扩展。当 CPU 利用率满足定义的阈值时，将部署或关闭 VM 系列防火墙的新服务实例。

©2024 Palo Alto Networks, Inc.

组件	说明
Heat Orchestration 模板文件	Palo Alto Networks为部署 VM 系列防火墙提供了一个示例 Heat 模板。该模板由主模板和环境模板组成。这些文件通过一个管理接口和两个数据接口实例化一个 VM 系列实例。 在基本网关部署中，模板通过一个接口实例化 Linux 服务器。服务器的接口连接到由模板创建的专用网络。 在服务链或服务扩展部署中，模板实例化两个 Linux 服务器，其中一个服务器连接到防火墙的每个数据接口。
VM 系列防火墙引导文件	VM 系列防火墙引导文件由 init-cfg.txt 文件，bootstrap.xml 文件和 VM 系列授权代码组成。与 Heat 模板文件一起，Palo Alto Networks 提供了一个示例 init-cfg.txt 和 bootstrap.xml 文件。您必须提供您自己的授权代码来授权您的 VM 系列防火墙并激活任何订阅。有关 VM 系列引导程序文件的更多信息，请参阅引导 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

基本网关部署的热量模板

热量模板文件包含以下四个文件，以帮助您在OpenStack中的KVM上启动 VM 系列防火墙。所有四个文件都需要部署 VM 系列防火墙和Linux服务器。

- **pan_basic_gw.yaml**- 定义创建的资源以支持计算节点上的 VM 系列防火墙和Linux服务器，例如接口和IP地址。
- **pan_basic_gw_env.yaml** — 定义 VM 系列防火墙和Linux服务器存在的环境。pan_basic_gw.yaml文件中的许多参数引用此文件中定义的参数，例如 VM 系列和Linux服务器的风格。
- **Init-cfg.txt**—包括在防火墙管理界面上启用 DHCP 的操作命令。
- **bootstrap.xml**- 为 VM 系列防火墙提供基本配置。bootstrap.xml 文件用于配置数据接口和 IP 地址。这些值必须与 pan_basic_gw.yaml 板文件中的相应值匹配。

  另外，bootstrap.xml 文件包含一个名为 untrust2trust 的 NAT 规则。此规则将服务器上的可信端口转换为 VM 系列防火墙的不可信端口。

您可以通过两种方法将引导文件传递到 OpenStack — 文件注入（个性文件）或用户数据。

从 *OpenStack Queens* 开始不再支持文件注入；您必须改用用户数据。

下表描述了 pan_basic_gw.yaml 模板文件创建的资源，并在适用时提供默认值。

资源	说明
pan_fw_instance	具有管理接口和两个数据接口的 VM 系列防火墙。
server_instance	具有单一接口的 Linux 服务器。
pan_trust_net	防火墙可信接口和服务器可信接口附加的内部网络连接。
pan_trust_subnet	子网连接到防火墙上的可信接口 (pan_trust_net)，并具有 CIDR 值 192.168.100.0/24。
pan_untrust_net	防火墙的不可信端口附加的不可信网络。
pan_untrust_subnet	子网连接到防火墙上的不可信接口 (pan_untrust_net)，并具有 CIDR 值 192.168.200.0/24。
allow_ssh_https_icmp_secgroup	允许端口 22 和 443 上 TCP 以及 ICMP 流量的安全组。
pan_untrust_port	以3层模式部署的 VM 系列防火墙的不可信端口。Heat 模板为该端口提供默认 IP 地址 192.168.200.10。

©2024 Palo Alto Networks, Inc.

资源	说明
	如果您在 Heat 模板中更改此 IP 地址，则必须更改 bootstrap.xml 文件中的 IP 地址。
pan_untrust_floating_ip	从 public_network 分配的浮动 IP 地址。
pan_untrust_floating_ip_assoc	这将 pan_untrust_floating_ip 关联到 pan_untrust_port。
pan_trust_port	VM 系列防火墙第3层模式的可信端口。
server_trust_port	Linux 服务器第 3 层模式的可信端口。Heat 模板为该端口提供默认 IP 地址 192.168.100.10。 如果您在 Heat 模板中更改此 IP 地址，则必须更改 bootstrap.xml 文件中的 IP 地址。

Pan_basic_gw.yaml 文件引用 pan_basic_gw_env.yaml 中的许多值来创建部署 VM 系列防火墙和 Linux 服务器所需的资源。Heat 模板环境文件包含以下参数。

参数	说明
mgmt_network	VM 系列防火墙管理接口连接到此参数中指定的网络。该模板不会创建管理网络;您必须在部署 Heat 模板之前创建它。默认值为 mgmt_ext_net。
public_network	OpenStack 集群和集群中虚拟机用于与外部或公共网络进行通信的地址。公共网络为公共端点提供虚拟 IP 地址，用于连接到 OpenStack 服务 API。该模板不会创建公共网络;您必须在部署 Heat 模板之前创建它。默认值为 public_net。
pan_image	此参数指定部署 VM 系列防火墙时由 Heat 模板使用的 VM 系列基本映像。默认值为 pa-vm-7.1.4。
pan_flavor	此参数定义分配给 VM 系列防火墙的硬件资源。默认值为 m1.medium。这个值符合在 KVM 上设置 VM 系列防火墙章节中所述的 VM 系列在 KVM 系统上的要求。
server_image	该参数告诉 Heat 模板哪个映像可用于 Linux 服务器。默认值为 Ubuntu-14.04。
server_flavor	该参数定义分配给 Linux 服务器的硬件资源。默认值为 m1.small。

©2024 Palo Alto Networks, Inc.

参数	说明
server_key	服务器密钥用于通过 ssh 访问 Linux 服务器。默认值为 server_key。您可以通过在环境文件中输入新的服务器密钥来更改此值。

©2024 Palo Alto Networks, Inc.

服务链和服务扩展的 Heat 模板

在 *OpenStack Queens* 上不支持通过服务链或服务扩展部署 *VM* 系列防火墙。

Heat 模板环境文件定义特定于通过服务链或服务扩展部署的 VM 系列防火墙实例的参数。在环境文件中定义的参数分为几个部分，描述如下。用于服务链的 Heat 模板有两个版本：vwire 和 L3；用于服务扩展的 Heat 模板只有一个版本。

服务链需要 Heat 模板文件和两个引导文件启动左侧和右侧网络中的 VM 系列防火墙服务实例和两个 Linux 服务器。

- 模板文件 — 此模板定义为支持 VM 系列防火墙和两个 Linux 服务器而创建的资源，例如接口和 IP 地址。
  - 适用于 VMWire 部署的 service_chaining_template_vm.yaml。
  - 适用于第 3 级部署的 service_chaining_template_L3.yaml。
  - 适用于服务扩展部署的service_scaling_template.yaml。
- 环境文件 — 该环境文件定义 VM 系列防火墙和 Linux 服务器所在的环境。该模板中的许多参数引用此文件中定义的参数，例如 VM 系列的特征和 Linux 服务器的名称。
  - 适用于 VMWire 部署的 service_chaining_env_vm.yaml。
  - 适用于第 3 级部署的 service_chaining_env_L3.yaml。
  - 适用于服务扩展部署的 service_scaling_env.yaml。
- **Service_instance.yaml** —（仅限服务扩展）这是一个嵌套的 Heat 模板，由 Service_Scaling_template.yaml 引用以部署服务实例。它提供部署服务实例以扩展事件的必要信息。
- **init-cfg.txt** — 提供引导 VM 系列防火墙所需的最少信息。所提供的 init-cfg.txt 仅包含在防火墙管理界面上启用 DHCP 的操作命令。
- **<file_name>_bootstrap.xml** — 为 VM 系列防火墙提供基本配置。bootstrap.xml 文件用于配置数据接口。这些值必须与 Heat 模板文件中的相应值匹配。

有关 init-cfg.txt 和 bootstrap.xml 文件的更多信息，请参阅引导配置文件。

以下表格介绍环境文件的参数。

- 虚拟网络
- 虚拟机
- 服务模板
- 服务实例
- IPAM
- 服务政策

©2024 Palo Alto Networks, Inc.

- 警报

虚拟网络

Heat 模板环境文件中的虚拟网络配置参数定义了连接 VM 系列防火墙和 Heat 模板部署的两台Linux服务器的虚拟网络。

虚拟网络 **(VN Config)**	
management_network	VM 系列防火墙管理接口连接到此参数中指定的网络。
left_vn 或 left_network	左侧虚拟网络的名称。
right_vn 或 right_network	右侧虚拟网络的名称。
left_vn_fqdn	左侧虚拟网络的完全限定域名。
right_vn_fqdn	右侧虚拟网络的完全限定域名。
route_target	编辑此值以使路由目标配置与您的外部网关匹配。

虚拟机

虚拟机参数定义了左侧和右侧的 Linux 服务器。端口元组的名称在此定义并由 Heat 模板引用。在 Contrail 中，端口元组是连接到同一虚拟机的有序虚拟网络接口集。您可以使用端口元组创建端口，并在创建服务实例时传递该信息。Heat 模板创建左端口、右端口和管理端口并将它们添加到端口元组中。端口元组然后链接到服务实例。当您使用 Heat 模板启动服务实例时，端口元组将服务虚拟机映射到在 OpenStack 中部署的虚拟机。

虚拟机（**VM** 配置）	
flavor	左侧和右侧虚拟机的风格。默认值为 m1.small。
left_vm_image 或 right_vm_image 或映像	左侧和右侧虚拟机的软件映像名称。更改此值以匹配您上传的映像的文件名。 缺省值是 TestVM，它是 OpenStack 提供的默认映像。
svm_name	将名称应用到 VM 系列防火墙。
left_vm_name 和 right_vm_name	左侧和右侧虚拟机的名称。

©2024 Palo Alto Networks, Inc.

虚拟机（**VM** 配置）	
port_tuple_name	两个 Linux 服务器和 VM 系列防火墙使用的端口元组的名称。
server_key	服务器密钥用于通过 SSH 访问虚拟机。默认值为 server_key。您可以通过在环境文件中输入新的服务器密钥来更改此值。

服务模板

服务模板定义服务实例的参数，例如软件映像、虚拟机风格、服务类型和接口。服务模板在域范围内配置，可用于指定域内所有项目。

服务模板（**ST** 配置）	
S_Tmp_name	服务模板的名称。
S_Tmp_version	服务模板版本。默认值是 2。不要更改此参数，因为需要服务模板版本 2 来支持端口元组。
S_Tmp_service_mode	服务模式是 VM 系列防火墙服务实例使用的网络模式。对于 L3 网络模板，默认值是网内的。对于虚拟线路模板，默认值是透明的。
S_Tmp_service_type	模板部署的服务类型。默认值是防火墙，部署 VM 系列防火墙时不应更改。
S_Tmp_image_name	此参数指定部署 VM 系列防火墙时由 Heat 模板使用的 VM 系列基本映像。编辑此参数以匹配上传到 OpenStack 环境的 VM 系列防火墙映像的名称。
S_Tmp_flavor	此参数定义分配给 VM 系列防火墙的硬件资源。默认值为 m1.large。
S_Tmp_interface_type_mgmt S_Tmp_interface_type_left S_Tmp_interface_type_right	这些参数定义管理、左侧和右侧接口的接口类型。
domain	此服务模板绑定的域。默认值为 default-domain。

服务实例

Heat 模板环境文件的服务实例部分提供了由 Heat 模板和服务模板部署的单个实例的名称。

©2024 Palo Alto Networks, Inc.

服务实例（SI 配置）	
S_Ins_name	服务实例名称。这是 Contrail 中 VM 系列防火墙实例的名称。
S_Ins_fq_name	服务实例的完全限定名称。

IPAM

IP 地址管理 (IPAM) 为服务实例的接口提供 IP 地址信息。更改这些参数以最适合您的环境。

IPAM（IPAM 配置）	
NetIPam_ip_prefix_mgmt	VM 系列防火墙上的管理接口的 IP 前缀。默认值为 172.2.0.0。
NetIPam_ip_prefix_len_mgmt	VM 系列防火墙上的管理接口的 IP 前缀长度。默认值为 /24。
NetIPam_ip_prefix_left	VM 系列防火墙上左侧接口的IP前缀。默认值是 10.10.1.0。
NetIPam_ip_prefix_len_left	VM 系列防火墙上左侧接口的IP前缀长度。默认值为 /24。
NetIPam_ip_prefix_right	VM 系列防火墙上正确接口的IP前缀。默认值是 10.10.2.0。
NetIPam_ip_prefix_len_right	VM 系列防火墙上正确接口的IP前缀长度。默认值为 /24。
NetIPam_addr_from_start_true	此参数确定如何将 IP 地址分配给上述子网上的 VM。如果为 true，则任何新 VM 都将采用下一个可用 IP 地址。如果为 false，则任何新虚拟机都会随机分配一个 IP 地址。默认值为 True。

服务政策

服务策略定义了流量重定向规则和策略，将流量从左侧虚拟机和右侧虚拟机之间传递到 VM 系列防火墙服务实例。

服务策略（策略配置）	
policy_name	Contrail 中的服务策略的名称通过 VM 系列防火墙重定向流量。对于 L3 模板，默认值为 PAN_SVM_policy-L3。对于虚拟线路模板，默认值为 PAN_SVM_policy-vw。
policy_fq_name	服务策略的完全限定名称。
simple_action	默认操作 Contrail 适用于去往 VM 系列防火墙服务实例的流量。默认值为 pass，因为 VM 系列防火墙会将自己的安全策略应用于流量。

©2024 Palo Alto Networks, Inc.

服务策略（策略配置）	
协议	Contrail 允许的协议传递给 VM 系列防火墙。默认值为 Any。
src_port_end 和 src_port_start	使用此参数指定应与策略规则关联的源端口。您可以输入单个端口，用逗号分隔的端口列表，或者以 <port>-<port> 形式输入一系列端口。 提供的 Heat 模板中的默认值为 -1；意味着任何源端口。
direction	此参数定义 Contrail 允许传递给 VM 系列防火墙的流量方向。默认值是 <> 或双向流量。
dst_port_end 和 dst_port_start	使用此参数指定应与策略规则关联的目标端口。您可以输入单个端口，用逗号分隔的端口列表，或者以 <port>-<port> 形式输入一系列端口。 提供的 Heat 模板中的默认值为-1;意思是任何目标端口。

警报

警报参数用于服务扩展，并且不包含在服务链环境文件中。这些参数定义了 Contrail 用于确定何时进行扩展的阈值。这组参数仅用于服务扩展 Heat 模板。

在冷却时间参数下配置的默认时间旨在让防火墙有足够的时间启动。如果更改冷却时间值，请为每个新的防火墙实例留有足够的启动时间。

警报	
meter_name	由 Ceilometer 监控的度量标准，并由收缩指示器用于确定何时应该部署或关闭额外的 VM 系列防火墙。Heat 模板使用 CPU 利用率或每秒字节数作为服务扩展的度量标准。
cooldown_initial	在启动初始服务实例之后，Contrail 在启动附加服务实例之前等待的时间。默认值为 1200 秒。
cooldown_scaleup	在第一次放大服务实例启动后，Contrail 在启动附加服务实例之间等待的时间。默认值为 1200 秒。
cooldown_scaledown	在第一个放大服务实例关闭后，Contrail 在关闭其他服务实例之间等待的时间。默认值为 1200 秒。
period_high	在触发警报之前，平均 CPU 负载计算为高的间隔。默认值为 300 秒。
period_low	在触发警报之前，平均 CPU 负载计算为低的间隔。默认值为 300 秒。
threshold_high	在启动放大事件之前，Contrail 引用的 CPU 利用率百分比或每秒字节数。默认值是 CPU 利用率 40# 或每秒 2800 字节。

©2024 Palo Alto Networks, Inc.

警报	
threshold_low	在启动缩减事件之前，Contrail 引用的CPU利用率百分比或每秒字节数。默认值是 CPU 利用率 20# 或每秒 12000 字节。

©2024 Palo Alto Networks, Inc.

在基本网关部署中安装 VM 系列防火墙

完成以下步骤以准备在 OpenStack 中部署 VM 系列防火墙所需的 Heat 模板，引导程序文件和软件映像。准备文件后，部署 VM 系列防火墙和 Linux 服务器。

STEP 1 | 下载 Heat 模板和引导文件。

从 GitHub 存储库下载 Heat 模板包。

STEP 2 | 下载 VM 系列基本映像。

1. 登录到 Palo Alto Networks 客户支持门户。
2. 选择 **Software Updates**（软件更新），然后从 **Filter By**（筛选条件）下拉列表中选择 **PAN-OS for VM-Series KVM Base Images**（用于 **VM** 系列 **KVM** 基本映像的 **PAN-OS**）。
3. 下载用于 KVM**qcow2** 文件的 VM 系列。

STEP 3 | 下载 Ubuntu 14.04 并将映像上传到 OpenStack 控制器。

Heat 模板需要用于启动 Linux 服务器的 Ubuntu 映像。

1. 下载 Ubuntu 14.04。
2. 登录到 Horizon UI。
3. 选择 **Project**（项目） > **Compute**（计算） > **Images**（映像） > **Create Image**（创建映像）。
4. **Name**（名称）Ubuntu 14.04 映像匹配 pan_basic_gw_env.yaml 文件中的参数。
5. 将映像源设置为 **Image File**（映像文件）。
6. 单击 **Choose File**（选择文件）并导航到您的 Ubuntu 映像文件。
7. 设置格式以匹配 Ubuntu 映像的文件格式。
8. 单击 **Create VPC**（创建 **VPC**）。

STEP 4 | 将用于 KVM 基础映像的 VM 系列上传到 OpenStack 控制器。

1. 登录到 Horizon UI。
2. 选择 **Project**（项目） > **Compute**（计算） > **Images**（映像） > **Create Image**（创建映像）。
3. **Name**（命名） 映像，以匹配 Heat 模板中的映像名称。
4. 将映像源设置为 **Image File**（映像文件）。
5. 单击 **Choose File**（选择文件）并导航到您的 VM 系列映像文件。
6. 将格式设置为 **QCOW2-QEMU Emulator**（**QCOW2-QEMU** 仿真器）。
7. 单击 **Create VPC**（创建 **VPC**）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 上传引导文件。您可以通过两种方法将引导文件传递到 OpenStack — 文件注入（个性文件）或用户数据。要使用用户数据传递引导文件，您必须将文件放置在 tar ball（.tgz 文件）中，并使用 base64 对 tar ball 进行编码。

从 *OpenStack Queens* 开始不再支持文件注入；您必须改用用户数据。

- 对于文件注入，您可以将 init-cfg.txt、bootstrap.xml 和您的 VM 系列授权代码上传到 OpenStack 控制器，或 OpenStack 控制器可以访问的 Web 服务器。
- 如果使用 **--user-data** 方法将引导数据包传递到 config-drive，则可以使用以下命令创建 tar ball，并使用 base64 对 tar ball（.tgz 文件）进行编码：

```
tar -cvzf <file-name>.tgz config/ license software content base64
 -i <in-file> -o <outfile>
```

STEP 6 | 编辑 pan_basic_gw.yaml 模板以指向引导文件和授权代码。

- 如果您使用个性文件，将文件路径或 Web 服务器地址指定为文件在个性下的位置。取消注释不使用的行。

```
  pan_fw_instance: type:OS::Nova::Server properties: image:
 { get_param: pan_image } flavor: { get_param: pan_flavor }
 networks: - network: { get_param: mgmt_network } - port:
 { get_resource: pan_untrust_port } - port: { get_resource:
 pan_trust_port } user_data_format:RAW config_drive: true
 personality: /config/init-cfg.txt: {get_file: "/opt/pan_bs/
init-cfg.txt"} # /config/init-cfg.txt: { get_file: "http://
web_server_name_ip/pan_bs/init-cfg.txt" } /config/bootstrap.xml:
 {get_file: "/opt/pan_bs/bootstrap.xml"} # /config/bootstrap.xml:
 { get_file: "http://web_server_name_ip/pan_bs/bootstrap.xml" } /
license/authcodes: {get_file: "/opt/pan_bs/authcodes"} # /
license/authcodes: {get_file: "http://web_server_name_ip/pan_bs/
authcodes"}
```

- 如果您使用用户数据，将文件路径或 Web 服务器地址指定为文件在 user_data 下的位置。如果您有多个

```
pan_fw_instance: type:OS::Nova::Server properties: image:
 { get_param: pan_image } flavor: { get_param: pan_flavor }
 networks: - port: { get_resource: mgmt_port } - port:
 { get_resource: pan_untrust_port } - port: { get_resource:
 pan_trust_port } user_data_format:RAW config_drive: true
 user_data: # get_file: http://10.0.2.100/pub/repository/panos/
images/openstack/userdata/boot.tgz get_file: /home/stack/newhot/
bootfiles.tgz
```


©2024 Palo Alto Networks, Inc.

STEP 7 | 编辑 pan_basic_gw_env.yaml 模板环境文件以适合您的环境。确保管理和公共网络值与您在 OpenStack 环境中创建的值相匹配。将 pan_image 设置为与您分配给 VM 系列基本映像文件的名称相匹配。您也可以在此处更改您的服务器密钥。

```
root@node-2:~# cat basic_gateway/pan_basic_gw_env.yaml parameters:
 mgmt_network: mgmt_ext_net public_network: public_net pan_image:
 pa-vm-image pan_flavor: m1.medium server_image:Ubuntu-14.04
 server_flavor: m1.small server_key: server_key
```

STEP 8 | 部署 Heat 模板。

1. 执行命令 **source openrc**
2. 执行 **heat stack-create *<stack-name>* -f *<template>* -e ./*<env-template>***

```
root@node-2:~# heat stack-create stack1 -f pan_basic_gw.yaml -e pan_basic_gw_env.yaml
+--------------------------------------+------------+--------------------+---------------------+--------------+
| id                                   | stack_name | stack_status       | creation_time       | updated_time |
+--------------------------------------+------------+--------------------+---------------------+--------------+
| ebe40f9d-2781-4bb2-b246-f15c761f9045 |   stack1   | CREATE_IN_PROGRESS | 2017-01-25T13:36:59 | None         |
+--------------------------------------+------------+--------------------+---------------------+--------------+
```

STEP 9 | 验证 VM 系列防火墙是否部署成功。

您可以使用以下命令来检查堆栈的创建状态。

- 使用 **heat stack-list** 检查堆栈状态
- 使用 **heat event-list** 查看堆栈创建期间发生的事件详细列表
- 使用 **heat stack-show** 查看堆栈的详细信息

STEP 10 | 验证 VM 系列防火墙是否正在双向检查访问 Linux 服务器的通信。

1. 登录到防火墙。
2. 选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）来查看 SSH 会话。

©2024 Palo Alto Networks, Inc.

使用服务链或扩展来安装 VM 系列防火墙

完成以下步骤以准备部署 VM 系列防火墙所需的 Heat 模板，引导程序文件和软件映像。准备文件后，部署 VM 系列防火墙服务和两台 Linux 服务器。

在 *OpenStack Queens* 上不支持通过服务链或服务扩展部署 *VM* 系列防火墙。

STEP 1 | 下载 Heat 模板和引导文件。

从 GitHub 存储库下载 Heat 模板包。

STEP 2 | 下载 VM 系列基本映像。

1. 登录到 Palo Alto Networks 客户支持门户。
2. 选择 **Software Updates**（软件更新），然后从 **Filter By**（筛选条件）下拉列表中选择 **PAN-OS for VM-Series KVM Base Images**（用于 **VM** 系列 **KVM** 基本映像的 **PAN-OS**）。
3. 下载用于 KVM**qcow2** 文件的 VM 系列。

STEP 3 | 下载 Ubuntu 14.04 并将映像上传到 OpenStack 控制器。

对于服务链，您可以使用 OpenStack 提供的名为 TestVM 的默认映像。使用 TestVM 时跳过此步骤。服务扩展需要 Ubuntu 映像。

1. 下载 Ubuntu 14.04。
2. 登录到 Horizon UI。
3. 选择 **Project**（项目） > **Compute**（计算） > **Images**（映像） > **Create Image**（创建映像）。
4. **Name**（名称）Ubuntu 14.04 映像匹配 pan_basic_gw_env.yaml 文件中的参数。
5. 将映像源设置为 **Image File**（映像文件）。
6. 单击 **Choose File**（选择文件）并导航到您的 Ubuntu 映像文件。
7. 设置格式以匹配 Ubuntu 映像的文件格式。
8. 单击 **Create VPC**（创建 **VPC**）。

使用 *Ubuntu* 映像时需要服务器密钥。确保服务器密钥已添加到环境文件中。

©2024 Palo Alto Networks, Inc.

STEP 4 | 将用于 KVM 基础映像的 VM 系列上传到 OpenStack 控制器。

1. 登录到 Horizon UI。
2. 选择 **Project**（项目） > **Compute**（计算） > **Images**（映像） > **Create Image**（创建映像）。
3. **Name**（命名） 映像，以匹配 Heat 模板中的映像名称。
4. 将映像源设置为 **Image File**（映像文件）。
5. 单击 **Choose File**（选择文件）并导航到您的 VM 系列映像文件。
6. 将格式设置为 **QCOW2-QEMU Emulator**（**QCOW2-QEMU** 仿真器）。
7. 单击 **Create VPC**（创建 **VPC**）。

STEP 5 | 上传引导文件。这些文件必须上传到这里描述的文件夹结构。Heat 模板使用此文件夹结构来定位引导程序文件。

1. 登录到 OpenStack 控制器。
2. 创建以下文件夹结构：

   /root/bootstrap/config/

   /root/bootstrap/license/
3. 使用 SCP 或 FTP，将 init-cfg.txt 和 bootstrap.xml 文件添加到 config 文件夹中，并将 VM 系列授权代码添加到许可证 license 中。

STEP 6 | 编辑模板环境文件以适合您的环境。验证环境文件中的映像名称是否与您上传文件时所用的名称相匹配。

```
parameters: # VN config management_network: 'mgmt_net'
 left_vn: 'left_net' right_vn: 'right_net' left_vn_fqdn:
 'default-domain:admin:left_net' right_vn_fqdn:
 'default-domain:admin:right_net' route_target:
 "target:64512:20000" # VM config flavor: 'm1.small'
 left_vm_image:'TestVM' right_vm_image:'TestVM'
 svm_name:'PAN_SVM_L3' left_vm_name:'Left_VM_L3'
 right_vm_name:'Right_VM_L3' port_tuple_name: 'port_tuple_L3'
 #ST Config S_Tmp_name:PAN_SVM_template_L3 S_Tmp_version:2
 S_Tmp_service_mode: 'in-network' S_Tmp_service_type: 'firewall'
 S_Tmp_image_name:'PA-VM-8.0.0' S_Tmp_flavor: 'm1.large'
 S_Tmp_interface_type_mgmt: 'management' S_Tmp_interface_type_left:
 'left' S_Tmp_interface_type_right: 'right' domain: 'default-
domain' # SI Config S_Ins_name:PAN_SVM_Instance_L3 S_Ins_fq_name:
 'default-domain:admin:PAN_SVM_Instance_L3' #IPAM Config
 NetIPam_ip_prefix_mgmt:'172.2.0.0' NetIPam_ip_prefix_len_mgmt:24
 NetIPam_ip_prefix_left:'10.10.1.0' NetIPam_ip_prefix_len_left:24
 NetIPam_ip_prefix_right:'10.10.2.0' NetIPam_ip_prefix_len_right:24
 NetIPam_addr_from_start_true: true #Policy Config
 policy_name:'PAN_SVM_policy-L3' policy_fq_name: 'default-
domain:admin:PAN_SVM_policy-L3' simple_action: 'pass' protocol:
 'any' src_port_end: -1 src_port_start: -1 direction: '< >'
 dst_port_end: -1 dst_port_start: -1
```


©2024 Palo Alto Networks, Inc.

STEP 7 | 编辑模板文件以指向引导文件和授权代码。在个性化模式下，指定文件路径。取消注释不使用的行。

```
Pan_Svm_instance: type:OS::Nova::Server depends_on:
 [ mgmt_InstanceIp, left_InstanceIp, right_InstanceIp ] properties:
 name: {get_param: svm_name } image: { get_param:S_Tmp_image_name }
 flavor: { get_param:S_Tmp_flavor } networks: - port:
 { get_resource: mgmt_VirtualMachineInterface } -
 port: { get_resource: left_VirtualMachineInterface } -
 port: { get_resource: right_VirtualMachineInterface }
 user_data_format:RAW config_drive: true personality: /config/
init-cfg.txt: {get_file: "/root/bootstrap/config/init-cfg.txt"}
 # /config/init-cfg.txt: { get_file: "http://10.4.1.21/op_test/
config/init-cfg.txt" } /config/bootstrap.xml: {get_file: "/
root/bootstrap/config/Service_Chaining_bootstrap_L3.xml"} # /
config/bootstrap.xml: { get_file: "http://10.4.1.21/op_test/
config/Service_Chaining_bootstrap_L3.xml" } # /license/authcodes:
 {get_file: "/root/bootstrap/license/authcodes"} # /license/
authcodes: {get_file: "http://10.4.1.21/op_test/license/authcodes"}
```

STEP 8 | 上传 Heat 模板文件。

1. 登录到 OpenStack 控制器。
2. 使用 SCP 或 FTP 添加热量模板文件和环境文件。

STEP 9 | 部署 Heat 模板。

1. 执行命令 **source openrc**
2. 执行 **heat stack-create *<stack-name>* -f *<template>* -e ./*<env-template>***

STEP 10 | 验证 VM 系列防火墙是否部署成功。

您可以使用以下命令来检查堆栈的创建状态。

- 使用 **heat stack-list** 检查堆栈状态
- 使用 **heat event-list** 查看堆栈创建期间发生的事件详细列表
- 使用 **heat stack-show** 查看堆栈的详细信息

STEP 11 | 验证 VM 系列防火墙是双向检查 Linux 服务器之间的流量。

1. 登录到防火墙。
2. 选择 **Monitor**（监控） > **Logs**（日志） > **Traffic**（流量）来查看 SSH 会话。

 ©2024 Palo Alto Networks, Inc.

在 Google Cloud Platform 上设置 VM 系列防火墙

您可以在 Google Cloud Platform 上的 Google Cloud Engine 实例中部署 VM 系列防火墙。

- Google Cloud Platform 上支持的部署
- 在 Google Public Cloud 上准备设置 VM 系列防火墙
- 在 Google Cloud Platform 上部署 VM 系列防火墙
- 使用适用于 GCP 的 Panorama 插件进行 VM 监控
- 在 Google Cloud Platform 上自动扩展 VM 系列防火墙

关于 Google Cloud Platform 上 VM 系列防火墙

VM 系列防火墙可将下一代防火墙的功能应用于 Google® Cloud Platform (GCP™)。

要提高性能， GCP 上的 VM 系列防火墙支持数据面开发套件 (DPDK) 库，并根据 VM 系列防火墙许可证和 Google Cloud Platform 虚拟机 (VM) 大小的特定组合提供快速的数据包处理，提高网络性能。

- Google Cloud Platform 和 VM 系列防火墙
- 对 VM 系列的最低系统要求

Google Cloud Platform 和 VM 系列防火墙

通过 VM 系列防火墙与 Google Cloud Platform (GCP) 的集成，可将 VM 系列防火墙部署为在 Google Compute Engine 实例上运行的虚拟机 (VM)。当从 Google Cloud Platform Marketplace 部署 VM 系列防火墙时，这一过程得到了简化。

VM 系列防火墙部署结束后，您可以配置以下可选服务：

- 在 VM 系列防火墙上启用 Google Stackdriver 监控 — 从防火墙将 PAN-OS 指标推送给 Google Stackdriver 服务。
- 在 Google Cloud Platform 上启用 VM 监控以跟踪 VM 更改 — 设置可以监控包含您的实例在内的特定 GCP 区域的 VM 信息源。受监控的 VM 元数据可以包含项目 ID 等 GCP 预定义属性，以及标签和网络标记等用户定义属性。

对 VM 系列的最低系统要求

必须选择公共云的 VM 系列防火墙许可证和许可证方法：自带许可证 (BYOL) 或即付即用 (PAYG)。要在 Google Compute Engine 实例上部署 VM 系列防火墙，必须选择支持许可证的 VM 系列系统要求的机器类型。

单个 Google Compute Engine 实例最多支持 8 个网络接口。如果想配置 8 个接口，请选择 n1-standard-8 或更大的机器类型。

容量	BYOL	套餐 1 和 2	
		PAYG	市场
VM-100 防火墙	✓		
VM-200 防火墙	✓		
VM-300 防火墙	✓	✓	✓

©2024 Palo Alto Networks, Inc.

容量	BYOL	套餐 1 和 2	
		PAYG	市场
VM-1000-HV 防火墙	✓		
VM-500 防火墙	✓		
VM-700 防火墙	✓		

VM 系列防火墙支持下面列出的预定义标准计算机类型。如果资源要求与您的 VM 系列防火墙许可证兼容，则可以选择性能较高的机器类型，或是创建您自己的自定义机器类型。

- n1-standard-4
- n1-standard-8
- n1-standard-16
- n2-standard-4
- n2-standard-8
- n2-standard-16
- n2-standard-32

自定义计算机类型：

- e2-standard-4
- e2-standard-8
- e2-standard-16
- e2-standard-32

©2024 Palo Alto Networks, Inc.

Google Cloud Platform 上支持的部署

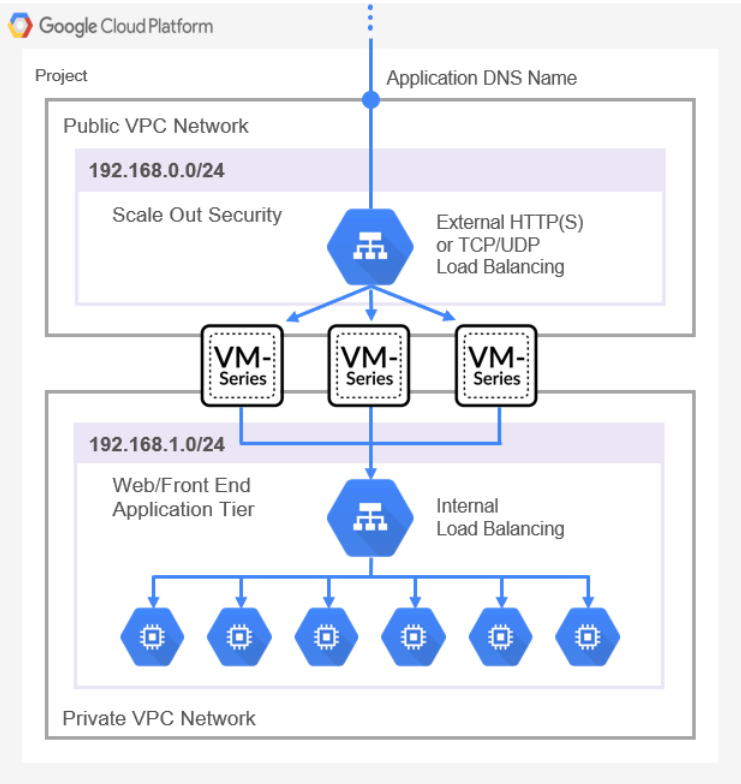
您可以在虚拟私有云 (VPC) 网络中的 Google® Compute Engine 实例上部署 VM 系列防火墙。部署类型包括：

- Internet 网关
- 分段网关
- 混合云 IPSec VPN

Internet 网关

VM 系列防火墙可以保护进出 internet 的北向南流量，从而保护应用程序免受已知和未知威胁。Google 项目最多可以包含五个 VPC 网络。有关 Internet 网关的典型示例，请参阅 Google 配置示例。

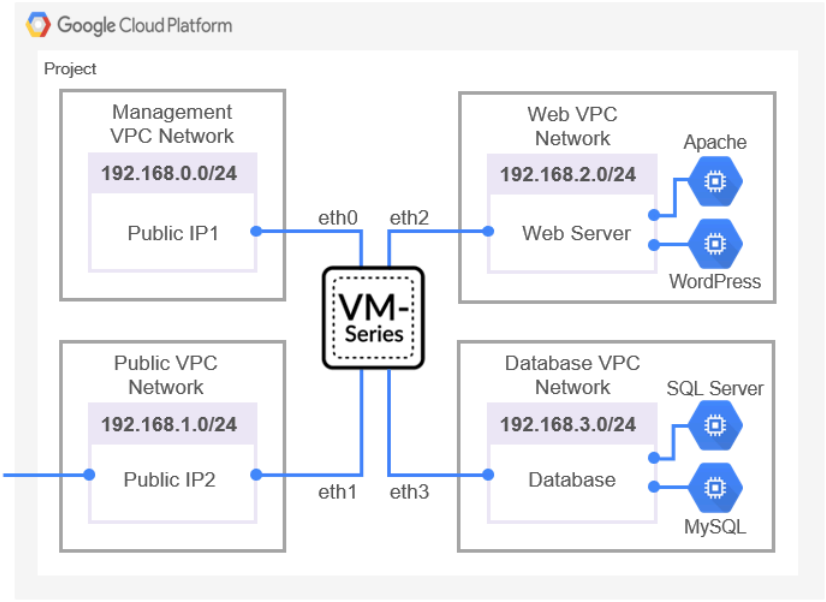
在公共云环境中，常见的做法是使用扩展架构（如下所示），而非性能更好的大型 VM。此架构（有时也称为三明治部署）可以避免单点故障，在必要时允许添加或移除防火墙。



分段网关

分段网关保护虚拟私有云 (VPC) 之间的东向西流量，确保数据保护合规性和应用程序的访问。下图显示的是保护北向南和东向西流量的防火墙。

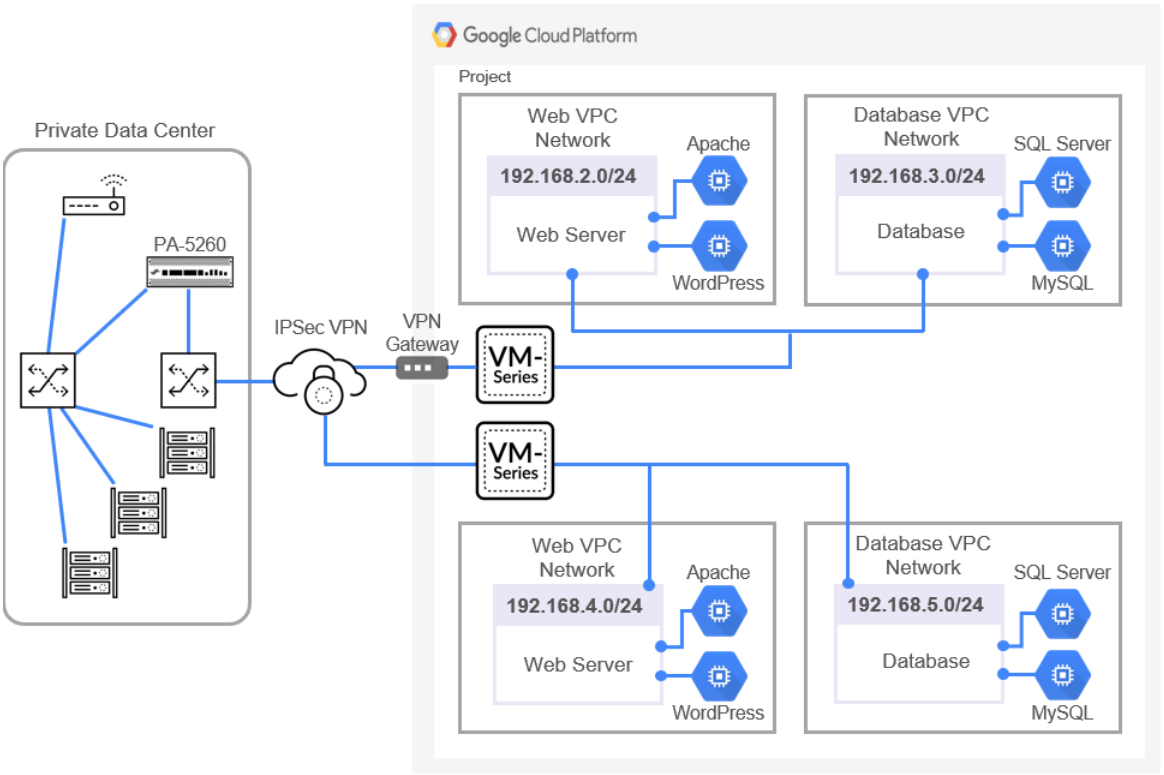
©2024 Palo Alto Networks, Inc.



混合云 IPSec VPN

VM 系列防火墙充当 IPSec VPN 终止点，从而保护 Google Cloud Platform (GCP) 上托管的应用程序进出通信的安全。

下图中部署显示的是从预置型网络到 GCP 上部署的 VM 系列防火墙之间的站点到站点 VPN，以及从预置型网络到 Google Cloud VPN 网关之间的 IPSec 连接。



©2024 Palo Alto Networks, Inc.

为 Google Cloud Platform 创建自定义 VM 系列防火墙映像

Palo Alto Networks 在 Google Cloud Platform (GCP) Marketplace 上发布 VM 系列防火墙基础映像版本或具有关键修复程序的次要版本（例如 PAN-OS 11.0）。从 GCP Marketplace 部署 VM 系列防火墙时，这些版本可用。但是，您可能需要部署早于或晚于 Marketplace 版本的 PAN-OS 版本。

要部署在 Marketplace 上未提供的 VM 系列防火墙版本，您可以使用 BYOL 许可证创建自定义 VM 系列防火墙映像。

从防火墙实例创建自定义防火墙的基本步骤如下：

- 从 GCP Marketplace 部署新的防火墙。
- 激活防火墙许可证，将所需的 PAN-OS 软件版本下载到防火墙，使用动态更新来更新 应用程序和威胁内容，然后停用防火墙许可证。
- 从 GCP 控制台执行私有数据重置。
- 从升级后的防火墙创建自定义映像。

STEP 1 | 在创建自定义映像之前，请查看您的帐户，为 VM 系列防火墙部署规划和创建网络，同时规划网络接口。

STEP 2 | 从 GCP Marketplace 部署 VM 系列防火墙。

您无法从现有防火墙创建映像。首先从 GCP Marketplace 确保自定义图像可以获得许可。

STEP 3 | （仅限 BYOL）激活许可证。

1. 选择 **Device**（设备） > **Licenses**（许可证）并激活许可证。

   许可完成后，防火墙将重新启动。

2. 登录到防火墙。

©2024 Palo Alto Networks, Inc.

STEP 4 | 升级到首选 PAN-OS 版本并安装软件更新。

1. 选择 **Device**（设备） > **Software**（软件） > **Check Now**（立即检查），并下载所需的 PAN-OS 版本。

   如果没有看到所需的版本，请按如下方式从 Palo Alto Networks 客户支持网站下载。

   1. 登录并选择 **Updates**（更新） > **Software Updates**（软件更新）。

      从 **Filter By**（筛选依据）列表中选择适用于 VM 系列的 PAN-OS 版本。
   2. 选择一个 PAN OS 版本并将其下载到本地计算机。
   3. 在 VM 系列防火墙上 **Select Device**（选择设备） > **Software**（软件）并将 PAN-OS 版本从本地计算机 **Upload**（上传）到设备。
2. 安装所选版本。
3. 升级 PAN OS 软件版本。
4. 选择 **Device**（设备） > **Dynamic Updates**（动态更新）并升级 **Applications and Threats**（应用程序和威胁）以及您想要包含在基本映像中的任何其他内容。

STEP 5 | （仅限 BYOL）从防火墙停用 VM。

如果未停用许可证，则会丢失在此防火墙实例上应用的许可证。

1. 选择 **Device**（设备） > **Licenses**（许可证）并在 **License Management**（许可证管理）下选择 **Deactivate VM**（停用 **VM**）。
2. 选择 **Complete Manually**（手动完成），然后 **Export**（导出）许可证令牌。
3. 返回 Palo Alto Networks 客户支持网站，选择 **Assets**（资产） > **VM** 系列授权代码 > **Deactivate License(s)**（停用许可证）并上传许可证令牌。

©2024 Palo Alto Networks, Inc.

STEP 6 | 执行私有数据重置。

重置私有数据会删除所有日志并恢复默认配置，

但不会擦除系统磁盘，因此，4 中的内容更新是完整的。

1. 访问防火墙 CLI 并使其保持活动状态。
2. 在 GCP 控制台中，从 VM 系列防火墙中删除 SSH 密钥。
    1. 选择 **Compute Engine** > **VM Instances**（**VM** 实例）并选择实例名称。
    2. 在 **Details**（详细信息）视图中，选择 **EDIT**（编辑）。
    3. 在 **SSH Keys**（**SSH** 密钥）下，单击 **Show and edit**（显示和编辑）链接，然后单击 **X** 以删除 SSH 密钥。
    4. **Save**（保存）更改。
3. （可选）导出配置的副本。
4. 在 CLI 中，请求重置私有数据。

    ```
    request system private-data-reset
    ```

    输入 **y** 以确认。

    防火墙重新启动以初始化默认配置。
5. 在 GCP 控制台中，选择 **Compute Engine** > **VM instances**（**VM** 实例）并 **STOP**（停止）防火墙。

STEP 7 | 在 GCP 控制台中创建自定义映像。

这些步骤基于创建、删除和弃用自定义映像。

1. 选择 **Compute Engine** > **Images**（映像） > **Create Image**（创建映像）。
2. 为映像命名并选择 **Google-managed key**（**Google** 管理的密钥）（参阅 Google 管理的加密密钥）。
3. 选择 **Disk**（磁盘） 作为来源，对于 **Source disk**（源磁盘），选择已停止的 VM 系列防火墙 VM，然后单击 **Create**（创建）。
4. （可选）映像完成后，单击 **Equivalent REST**（等效 **REST**）链接，然后从 **REST response**（**REST** 响应）中复制 selfLink。这是您需要的任何类型 CI/CD 流水线的 URI 链接。

    例如：`projects/my-vpc-vpcID/global/images/pa-vm-8-1-9`

    使用此链接直接指向映像，以便可以在模板或脚本中使用。例如：

    ```
    源映像：https://www.googleapis.com/compute/v1/projects/
    {{project}}/global/images/pa-vm-8-1-9}
    ```


©2024 Palo Alto Networks, Inc.

在 Google Public Cloud 上准备设置 VM 系列防火墙

从 Google Cloud Platform Marketplace 部署 VM 系列防火墙的过程需要完成一些准备任务。

如果使用 Google Marketplace 进行部署，则必须创建项目网络和子网，并提前为 VM 系列防火墙接口规划网络和 IP 地址分配。部署时，必须从现有网络和子网中进行选择。

规划您的部署时，请参阅以下主题：

- 一般要求
- 在 Panorama 上安装 VM 系列插件
- 安装适用于 GCP 的 Panorama 插件
- 准备从 GCP Marketplace 进行部署

一般要求

此清单中的组件通常用于部署直接或使用 Panorama 管理的 VM 系列防火墙。Panorama 插件的其他要求适用于多项服务，例如 Stackdriver 监控、VM 监控、自动扩展或保护 Kubernetes 部署。

请始终参阅公共云的 Panorama 插件兼容性矩阵信息。此版本需要以下软件：

- **GCP** 帐户 — 必须拥有包含链接电子邮件地址的 GCP 用户帐户，并且还必须知道该电子邮件地址的用户名和密码。
- **Google Cloud SDK** — 如果尚未安装，请安装 Google Cloud SDK，其中包括 Google Cloud API、gcloud 和其他命令行工具。您可以使用命令行界面部署防火墙模板和其他模板。
- **GCP** 上 **VM** 系列防火墙上的 **PAN-OS** — 可以从 Google Marketplace 获取运行 PAN-OS 版本的 VM 系列防火墙。
  - **VM** 系列防火墙 — 必须使用 Google Marketplace 的 Palo Alto Networks 映像，在 Google Cloud Platform 中部署要通过 Panorama 管理的 VM 系列防火墙。防火墙必须满足对 VM 系列的最低系统要求。
  - **VM** 系列防火墙 — 必须许可 VM 系列防火墙以获取序列号。添加 VM 系列防火墙作为 Panorama 托管设备需要使用序列号。如果您使用适用于 GCP 的 Panorama 插件部署 VM 系列防火墙，则必须提供 BYOL 授权代码。Google Marketplace 负责处理服务计费，但您部署的防火墙将直接与 Palo Alto Networks 许可服务器交互。
  - 防火墙上的 **VM** 系列插件 — 运行 PAN-OS 9.0 及更高版本的 VM 系列防火墙包括 VM 系列插件，该插件管理与公共云和私有云的集成。如兼容性矩阵所示，VM 系列插件具有与每个 PAN-OS 版本相对应的最低版本。

    升级主要 PAN-OS 版本时，将自动升级 VM 系列插件版本。对于次要版本，由您确定是否需要升级 VM 系列插件，如果需要，则执行手动升级。请参阅在 Panorama 上安装 VM 系列插件。

©2024 Palo Alto Networks, Inc.

- 在管理模式下运行的 **Panorama** — 运行与托管防火墙相同或更高版本的 PAN-OS 版本的 Panorama 物理或虚拟设备。不需要在 GCP 中部署虚拟实例。
  - 您必须拥有 Panorama 的许可版本。
  - Panorama 必须对部署要管理的 VM 的 VPC 具有网络访问权限。
  - 如果您计划管理在 GCP 中部署的 VM 或配置其他功能（例如自动扩展），则 PAN-OS 和 VM 系列插件版本必须满足公共云要求，以支持适用于 GCP 的 Panorama 插件。
  - Panorama 上的 VM 系列插件。请参阅在 Panorama 上安装 VM 系列插件
- 适用于 **GCP** 版本 **2.0.0** 的 **Panorama** 插件 — GCP 插件可管理许可、引导和配置使用 VM 监控或自动扩展模板部署防火墙所需的交互。GCP 插件与 VM 监控或自动扩展模板结合使用 Panorama 模板模板堆栈和设备组，对 NAT 规则进行编程以将流量定向到托管的 VM 系列防火墙。

  请参阅安装适用于 GCP 的 Panorama 插件。

在 Panorama 上安装 VM 系列插件

在 Panorama 上，安装或升级到支持您要配置的 GCP 功能的 VM 系列插件版本，如公共云兼容性矩阵表中所述。

初始安装 — 由于 VM 系列插件在 Panorama 上是可选插件，因此首次安装时，必须从支持门户下载 VM 系列插件，然后转到 **Panorama** > **Device Deployment**（设备部署） > **Plugins**（插件）进行上传和安装。

升级 — 转至 **Panorama** > **Device Deployment**（设备部署） > **Plugins**（插件），然后单击 **Check Now**（立即检查）。安装满足公共云兼容性矩阵表中要求的版本。

安装适用于 GCP 的 Panorama 插件

如果您要使用 Panorama 管理通过 Palo Alto Networks 模板创建的 VM 监控或自动扩展部署，则需要适用于 GCP 的 Panorama 插件。安装支持您要配置的 GCP 功能的所有版本，如公共云兼容性矩阵表中所述。

您不能将适用于 *GCP* 的 *Panorama* 插件从版本 *1.0.0* 升级到版本 *2.0.x*。如果已安装版本 *1.0.0*，请在安装版本 *2.0.x* 之前将其删除。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件

©2024 Palo Alto Networks, Inc.

- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 验证 Panorama 安装。

在 Panorama 上，确保 PAN-OS 版本满足支持 GCP 自动扩展的要求。

STEP 2 | 删除适用于 GCP 版本 1.0 的 Panorama 插件。

如果已安装适用于 GCP 版本 1.0 的 Panorama 插件，则必须将其删除。

STEP 3 | 安装适用于 GCP 的 Panorama 插件。

选择 **Panorama** > **Plugins**（插件），然后在搜索栏中键入 **gcp**。**Install**（安装）支持您要配置的功能的插件版本（请参阅公共云的兼容性矩阵表）。

安装后，您可以在 Panorama 仪表盘的 **General Information**（常规信息）列表中看到该插件。查看 **Panorama** > **Google Cloud Platform**，您会看到 **Setup**（设置）、**Monitoring Definition**（监控定义）和 **AutoScaling**（自动扩展）定义。

STEP 4 | （可选）如果 Panorama 设备具有高可用性配置，则必须手动在两个 Panorama 对等上安装相同版本的 Google 插件。

只能在 *Panorama* 主动对等上配置 *Google* 插件。提交后，配置同步到 *Panorama* 被动对等。仅 *Panorama* 主动对等轮询为 *VM* 监控配置的 *Google VM* 帐户。

准备从 GCP Marketplace 进行部署

查看这些要求，以确保您在 Google Compute Engine (GCE) 实例上使用 Google Marketplace 部署防火墙之前拥有正确的帐户和权限。

- 一般帐户和权限
- 可用 Google 资源
- Google 身份验证方法
- SSH 密钥对

©2024 Palo Alto Networks, Inc.

一般帐户和权限

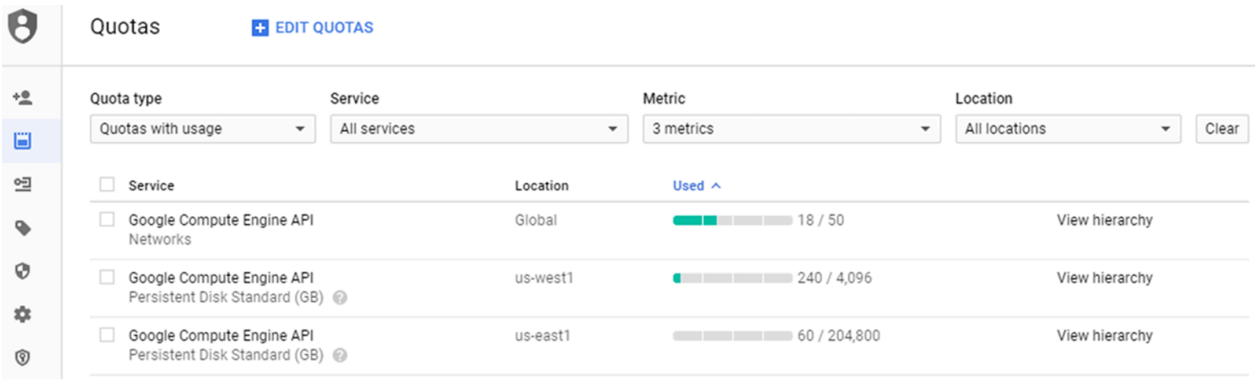
- 您以及您允许的任何用户均必须至少具有下列角色或等效的身份及访问管理 (IAM) 权限，以连接到 VM 系列防火墙：
  - 计算查看器 — 计算查看器允许您获取并列出 Compute Engine 资源，但无法读取存储在其中的数据。
  - 存储对象查看器 — 可让您在同一项目中使用 Google 存储桶进行引导。

  您组织中的用户可能具有比所需权限更宽松的 IAM 权限或预定义角色。确保适当限制 *VM* 系列防火墙的访问权限。

  您还可以限制服务帐户的访问权限，如Google 身份验证方法中所述。
- 监控指标编写器 — Stackdriver 所需。

可用 Google 资源

您的项目必须具有足够的资源以将 VM 系列防火墙部署为 Google Compute Engine 实例。如果部署 GCP Marketplace解决方案，以确定此解决方案是否部署除此防火墙外的其他 VM。在 Google Cloud 控制台中，选择 **IAM & admin**（**IAM** 和管理员）> **Quotas**（配额），以查看项目的资源配额以及所消耗的网络和磁盘空间。如果资源耗尽，则可以要求 Google 为您的组织分配更多的资源。



Google 身份验证方法

GCP 可采用多种方法连接到实例。您可以使用服务帐户或 SSH 密钥对进行身份验证。

©2024 Palo Alto Networks, Inc.

1. 服务帐户 — 服务帐户适用于应用程序或 VM，而不适用于最终用户。他们通常在您使用程序或脚本，或从 gcloug 命令行访问防火墙时用于控制访问。如果使用 Google 服务帐户对实例或应用程序进行验证，则必须知道此帐户的电子邮件地址。请参阅创建和管理服务帐户密钥。

   如果想要从项目外部（从其他项目或命令行）连接到 VM 系列防火墙，则必须使用服务帐户。例如，如果您想启用下一代物理防火墙监控 VM 系列防火墙，则必须将 VM 系列防火墙服务帐户息保存到 JSON 文件。在物理防火墙中，您可以在配置连接时上传文件。

   1. 选择 **IAM & Admin**（**IAM** 和管理员） > **Service accounts**（服务帐户），然后选择 **+Create Service Account**（+创建服务帐户）。

      输入服务帐户名称和说明，然后单击 **Create**（创建）。
   2. 从下拉菜单中选择角色类型，然后在右侧选择适当的访问级别。

      例如，选择 Project（项目）> Editor（编辑器）。您可以为服务帐户选择多个角色。完成后，单击 **Continue**（继续）。
   3. 向特定用户授予访问此服务帐户的权限。从右侧的 **Permissions**（权限）列中选择成员，以授予他们访问上一步中的角色的权限。

2. **SSH** 密钥 — 如果从 Marketplace 部署 VM 系列防火墙，则必须为 Google Compute Engine 实例元数据提供一个 RSA 格式的 Open SSH 密钥。

   部署时，*VM* 系列防火墙仅接受一个密钥。

   您可以在部署期间将公钥粘贴到 Marketplace 部署中，如 SSH 密钥对中所述。部署后，在防火墙内使用 SSH 私钥配置管理员帐户。要添加用户，请参阅管理防火墙管理员。

您可以通过多种方式进行身份验证：

- 为实例创建服务帐户 — 您可以为特定实例或实例组创建服务帐户，并授予特定权限，然后可以向用户授予这些权限。
- 使用项目的默认服务帐户 — 如果使用 Google Cloud Platform (GCP™) 控制台，则使用您的电子邮件地址登录，并可以根据项目管理员分配给帐户的任何权限或角色访问 GCE 实例。

  使用 Google Cloud Console 或 gcloud 命令行工具创建的每个 Google Compute Engine 实例都有一个默认服务帐户，其名称采用电子邮件地址格式：

  ```
  <project-number>-compute@developer.gserviceaccount.com
  ```

  要查看防火墙实例的服务帐户名称，请查看实例详细信息并滚动到底部（参阅 Compute Engine 默认服务帐户）。

  对于与 VM 系列防火墙相同的项目，默认服务帐户可以对其中的 VM 身份验证进行管理。访问范围允许防火墙启动对 Google Cloud 项目中 VM 的 API 调用。

©2024 Palo Alto Networks, Inc.

- 使用 **IAM** 权限和 **Google API** — 如果使用 Google SDK API 和 gcloud，则必须调用 API 进行身份验证。
  - 当想要从命令行管理防火墙，或是运行脚本以配置防火墙时，您通常会使用 Google SDK。
  - 如果您连接的虚拟机包含需要 Google API 的应用程序的自定义映像，则需要访问 Google API。

SSH 密钥对

从 Google Marketplace 部署 VM 系列防火墙时，您需要 SSH 密钥对通过 VM 系列防火墙进行身份验证。

根据密钥生成器文件创建密钥对。不得删除公钥文件。编辑引入非法字符的风险。

VM 系列防火墙以不同于 GCE 实例的方式管理身份验证。部署后，首先以 **admin** 用户身份登录。仅接受一次 VM 系列防火墙默认用户名。登录成功后，您可以设置 VM 系列 Web 界面的管理员用户名和密码（参阅从 Google Cloud Platform Marketplace 部署 VM 系列防火墙）。

Google Marketplace 部署界面中的 **SSH key**（**SSH** 密钥）字段显示以下占位符：

```
admin:ssh-rsa your-SSH-key
```

admin 是首次登录到系列防火墙所需的管理员用户名。当您从 Google Cloud Platform Marketplace 部署 VM 系列防火墙时，您可以在 Marketplace 字段中添加 **admin:** 前缀。

如果不能提供整个公钥，或是在将密码粘贴到 Marketplace **SSH key**（**SSH** 密钥）字段时发现您的密钥包含非法字符，则无法登录到 VM 系列防火墙。在 VM 系列防火墙内首次使用 SSH 时，公钥会传送到防火墙。

如果公钥已损坏，则必须删除部署并重新开始。将保留所有网络和子网，但必须重新创建防火墙规则。

STEP 1 | 创建 SSH 密钥对，并将 SSH 密钥对存储在查找 SSH 密钥中提到的操作系统默认位置。

- **Linux** 或 **MacOS** — 在 .ssh 目录中使用 `ssh-keygen` 创建密钥对。
- **Windows** — 使用 PuTTYgen 创建密钥对。

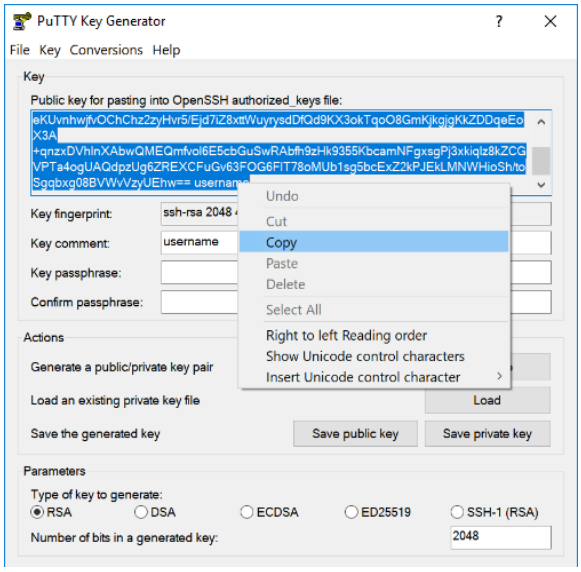
  Key comment（密钥注释）字段的内容与 VM 系列防火墙无关；您可以接受默认注释（密钥创建日期）或输入有助于您记住密钥对名称的注释。使用 **Save private key**（保存私钥）按钮将私钥存储在 .ssh 目录中。

©2024 Palo Alto Networks, Inc.

STEP 2 | 选择完整的公钥。

- **Linux** 或 **MacOS** — 在文本编辑器中打开公钥，然后复制公钥。
- **Windows** — 必须使用 PuTTY 密钥生成器查看公钥。启动 PuTTYgen，单击 **Load**（加载），然后浏览到保存在 .ssh 目录中的私钥。

  在 PuTTYgen 中向下滚动，确保选择整个密钥，右键单击，然后选择 Copy（复制）。



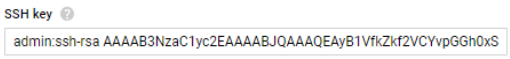
STEP 3 | 在 SSH 密钥字段中输入公钥，如下所述。

1. 在 Marketplace **SSH key**（**SSH** 密钥）字段，删除占位符文本和类型：

   `admin:`

   确保冒号后面没有多余的空格。

2. 在 **`admin:`** 之后插入光标，然后选择 **Paste as plain text**（粘贴为纯文本）。密钥必须在一行上，如下所示：

3. 将光标移动到密钥的末尾，添加一个空格，然后键入：**`admin`**。

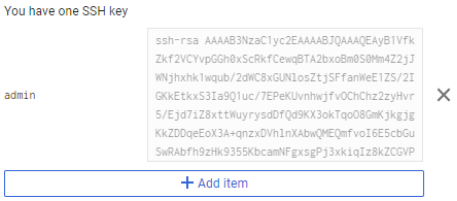
   SSH key（**SSH** 密钥）字段的最终内容必须为：

   `admin:ssh-rsa` [KEY] **`admin`**

©2024 Palo Alto Networks, Inc.

STEP 4 | 检查密钥。

部署后，在尝试登陆到防火墙之前，请查看管理实例，并检查密钥是否有换行符或多余空格：



如果密钥全部在一行上，并且格式为 **`admin:ssh-rsa`** [KEY] **`admin`**，则操作完成。

STEP 5 | （可选）如果出现错误，则必须更换密钥。

1. 单击 **X** 删除密钥，然后单击 **+ Add item**（+ 添加项目）。
2. 按照步骤 3 中所述输入密钥。现在，**SSH key**（**SSH** 密钥）字段必须显示：

   `admin:ssh-rsa` [KEY] **`admin`**
3. 单击 **Save**（保存） 以部署更新过的部署。
4. 重新检查密钥。

虚拟私有云 (VPC) 网络规划

在从 Google Marketplace 进行部署之前，制定 VPC 网络（称为网络）、子网（也称为子网）和 Google 防火墙规则的计划。首先，您必须创建网络和子网，然后才能开始从 Google Cloud Platform Marketplace 部署 VM 系列防火墙。

Marketplace 部署页面仅显示启动部署时存在的网络和子网。如果网络丢失，则必须退出部署，创建网络，然后从头开始。

- **VPC** 网络 — 您必须创建专用于每个 VM 系列防火墙网络接口的自定义网络。
  - 要根据 VM 系列防火墙许可证确定所需的网络接口数，请参阅 面向公共云的 VM 系列防火墙许可证。至少需要设置三个 VPC 网络和子网以启动 VM 系列防火墙。
  - GCP 项目具有包含预设配置和防火墙规则的默认网络；如果未使用，您可以删除默认网络。
  - 一个项目中默认最多有五个网络。GCP 管理员可以为您的项目请求其他网络。
  - 要连接到管理接口，必须创建允许访问的 GCP 防火墙规则。如果选择 **Enable GCP Firewall rule for connections to Management interface**（启用管理接口连接用 **GCP** 防火墙规则），然后为 **Source IP in GCP Firewall rule for connections to Management Interface**（管理接口连接用的 **GCP** 防火墙规则源 **IP**）提供 CIDR 块，则可以在部署时执行此操作。

    您的网络必须包含想要保护的所有实例。
- 子网 — Compute Engine 实例最多可在单个实例上支持八个第 3 层接口。管理、可信和不可信接口占据三个接口，您最多可以创建五个额外的数据平面接口。通常，数据平面接口代表应用程序网络。

©2024 Palo Alto Networks, Inc.

- **IP** 地址 — 您可以在创建接口子网时提供 IP 地址范围，并且可以选择在部署子网时启用外部地址。
  - 创建网络子网时，必须指定 IP 地址范围。该范围用于内部网络，因此，它不能与其他子网重叠。
  - 在部署期间，您可以选择在创建网络接口时启用外部 IP 地址。默认情况下，您可以获得一个临时 IP 地址。部署时，您不能提供保留的静态 IP 地址，但可以在完成部署时将临时地址升级为静态 IP 地址（参阅升级临时外部 IP 地址）。

网络接口规划

在 Google Cloud Platform Marketplace 上进行部署时，VM 系列防火墙默认部署有三个接口：管理层接口、不可信和可信数据平面接口。您可以定义其他数据平面实例，具体取决于 VM 上的可用计算资源；请参阅 面向公共云的 VM 系列防火墙许可证。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

在部署时，您可以有机会为这些接口命名。

接口顺序

使用 Marketplace 进行部署时，会预定义网络接口的顺序。管理接口映射至 eth0，不可信接口映射至 eth1，可信接口映射至 eth2。Marketplace 会使用此顺序，因为如果需要交换管理接口以进行负载均衡，必须将管理接口映射到 eth0，不可信接口映射到 eth1 可确保映射成功。

管理接口

您添加的第一个网络接口映射到防火墙上的 eth0，包含启用 IP 转发的选项。您可以使用此接口管理 VM 系列防火墙。通常，此接口具有一个外部 IP 地址。

只有当数据层接口附加到公共子网时才需要外部 *IP* 地址。创建时，您可以获得一个临时 *IP* 地址，稍后在部署结束后将其升级为静态 *IP* 地址；请参阅升级临时外部 IP 地址。

数据层接口（不可信，可信）

从 Marketplace 进行部署时，会预定义添加接口的顺序。

- 将不可信接口配置到管理接口的下游。此顺序表示不可信接口映射到 eth1。不可信接口通常会附加到公共子网，并具有一个外部 IP 地址。

  只有当数据层接口附加到公共子网时才需要外部 *IP* 地址。创建时，您可以获得一个临时 *IP* 地址，但您可以将其升级为静态 *IP* 地址；请参阅 升级临时外部 IP 地址。
- 可信接口紧随不可信接口，并映射到 eth2。可信网络通常不具有外部 IP 地址。可以将任何其他数据平面接口添加到可信接口的下游。

©2024 Palo Alto Networks, Inc.

其他数据面板接口

规划必须保护的应用程序（例如，Web 服务器，数据库）以及网络中其他应用程序接口。除用于启动防火墙所必需的三个接口外，您还可以创建最多五个其他数据平面接口。想要保护的应用程序必须位于连接到 VM 系列防火墙的网络中。

©2024 Palo Alto Networks, Inc.

在 Google Cloud Platform 上部署 VM 系列防火墙

要使用 GCP Marketplace 模板部署 VM 系列防火墙，首先必须为防火墙上的每个接口创建 VPC 网络。从 Google Marketplace 部署防火墙后，您可以登录到防火墙以调整配置，以便在 GCP VPC 配置中使用。您还可以启用监控功能，以便收集指标可改进资源管理的指标，或创建可自动适应应用程序环境中更改的安全策略规则。

- 从 Google Cloud Platform Marketplace 部署 VM 系列防火墙
- 用于 Google Cloud Launcher 负载均衡的管理接口交换
- 使用 VM 系列防火墙 CLI 以交换管理接口
- 在 VM 系列防火墙上启用 Google Stackdriver 监控
- 在 Google Cloud Platform (GCP) 上启用 VM 监控以跟踪 VM 更改
- 使用动态地址组保护 VPC 中的安全实例
- 使用自定义模板或 gcloud CLI 部署 VM 系列防火墙

从 Google Cloud Platform Marketplace 部署 VM 系列防火墙

您可以使用 Google® Cloud Platform Marketplace 在固定 vCPU 容量许可证 (VM 系列型号) 上部署 VM 系列防火墙。可从公共云获取的许可映像有：

- VM 系列下一代防火墙包 1
- VM 系列下一代防火墙包 2
- VM 系列下一代防火墙 (BYOL)

有关这些许可证选项的更多信息，请参阅从 Google Cloud Platform Marketplace 部署 VM 系列防火墙。

Marketplace 将通过至少一个管理接口和两个数据平面接口（可信和不可信）部署 VM 系列防火墙实例。您可以在您的虚拟私有云 (VPC) 中为最多五个 Google Compute Engine 实例添加额外的数据平面接口。

部署 VM 系列防火墙之前，必须在组织中创建或选择一个项目，然后创建将与防火墙相连接的任何网络和子网，如VPC 网络规划和网络接口规划所述。

您无法将多个网络接口附加到相同的 VPC 网络。创建的每个接口必须具有包含一个子网的专用网络。您的网络必须包含您创建的任何其他数据平面实例。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 选择引导方法.

©2024 Palo Alto Networks, Inc.

STEP 2 | 在 Marketplace 上找到 VM 系列防火墙列表。

1. 登录到 Google Cloud 控制台。
2. 从产品和服务菜单中选择 **Marketplace**。
3. 搜索 **VM** 系列。
4. 选择以下 VM 系列防火墙许可证选项之一。

STEP 3 | 单击 **Launch on Compute Engine**（在 **Compute Engine** 上启动）。

STEP 4 | 命名实例，并选择资源。

1. 输入 **Deployment Name**（部署名称）（此名称显示在部署管理器中）。此名称必须是唯一的，且不能与项目中的任何其他部署冲突。
2. 选择 **Zone**（区域）。有关支持区域列表，请参阅地区和区域。
3. 根据您的许可证的 VM 系列系统要求和 Google Cloud Platform 上 VM 系列防火墙的系统最低要求选择 **Machine Type**（机器类型）。

STEP 5 | 指定实例元数据。

Bootstrap Bucket（引导桶）和 **Interface Swap**（接口交换）会影响 VM 系列防火墙首次启动时的初始配置。

1. **Bootstrap Bucket**（引导桶）（可选）— 如果您计划使用引导文件，请输入存储桶的名称，或输入包含引导数据包的存储桶中文件夹的路径。您需要权限才能访问存储桶。例如：

   vmseries-bootstrap-gce-storagebucket=<bucketname>

   或者

   vmseries-bootstrap-gce-storagebucket=<bucketname/directoryname>

   如果您选择使用自定义元数据进行引导，请继续执行步骤 6。
2. **Interface Swap**（接口管理）（可选）— 在部署时交换管理接口 (eth0) 和第一个数据平面接口 (eth1)。接口交换仅在将 VM 系列防火墙部署在 Google Cloud Platform HTTP(S) 负载

©2024 Palo Alto Networks, Inc.

均衡后才有用。有关详细信息，请参阅用于 Google Cloud Launcher 负载均衡的管理接口交换。

3. **SSH key**（**SSH** 密钥） — 从 SSH 密钥对粘贴公钥。按照SSH 密钥对中的操作系统说明来创建、复制和粘贴密钥。Windows 用户必须查看 PuTTY 中的密钥，从用户界面进行复制，并将其粘贴到 Marketplace 部署。

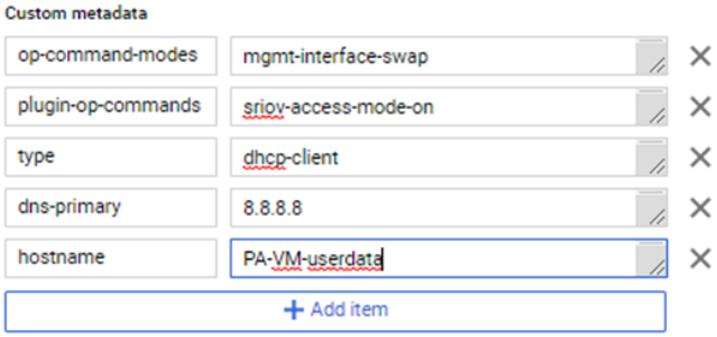
   如果密钥格式不正确，则 *VM* 系列防火墙不允许您登录，您必须删除此部署，并重新设置。

4. 单击 **More**（更多）以显示其他元数据选项。**blockProjectKeys**（阻止项目密钥）和 **enableSerialConsole**（启用串行控制台）是实例的属性；您可以在成功部署后更改这些元数据值。

   - **blockProjectKeys**（阻止项目密钥）（可选）— 如果阻止项目密钥，则只能使用您提供的 SSH 公共密钥来访问实例。
   - **enableSerialConsole**（启用串行控制台） （可选） — 通过与串行控制台交互，您可以监控实例创建，执行交互调试任务。

STEP 6 | 指定自定义元数据。

如果您选择使用自定义元数据进行引导，请添加您在步骤 5 中未添加的所有键值对。有关键值对列表，请参阅init-cfg.txt 文件组件。例如：



STEP 7 | 配置启动磁盘。

1. **Boot disk type**（启动磁盘类型）— 从 SSD 永久磁盘或标准永久磁盘选择。请参阅存储选项。
2. 输入 **Boot disk size**（启动磁盘大小）— 60GB 为最大值。您可以稍后编辑磁盘大小，但必须停止 VM 才能执行此操作。

©2024 Palo Alto Networks, Inc.

STEP 8 | 配置管理接口。

1. **Management VPC Network name**（管理 **VPC** 网络名称）— 选择现有网络
2. **Management Subnet name**（管理子网名称）— 选择现有子网。
3. **Enable External IP for Management interface**（启用管理接口外部 **IP**）（可选**nal)**（可选）— 如果启用此选项，您可以使用分配给 VM 系列防火墙管理接口的 IP 地址和 SSH 访问 VM 系列防火墙 Web 界面。
4. **Enable GCP Firewall rule for connections to Management interface**（启用管理接口连接用 **GCP** 防火墙规则）（可选）— 启动此选项后，可自动创建用于您提供的外部源 IP 地址的 GCP 防火墙允许规则。
5. **Source IP in GCP Firewall rule for connections to Management Interface**（管理接口连接用的 **GCP** 防火墙规则源 **IP**） — 如果 **Enable GCP Firewall rule for connections to Management interface**（启用管理接口连接用 **GCP** 防火墙规则），则输入源 IP 地址或 CIDR 块。
   - 请勿使用 0.0.0.0/0。确保提供与专用管理 IP 地址或网络相对应的 IP 地址或 CIDR 块。源网络范围不得大于必要的范围。
   - 验证地址，确保您不会锁定自己。

STEP 9 | 配置不可信的数据平面接口。

1. **Untrust VPC Network name**（不可信的 **VPC** 网络名称）— 选择现有网络。
2. **Untrust Subnet name**（不可信的子网名称）— 选择现有子网。
3. **Enable External IP for Untrust**（启用不可信的外部 **IP**）— 启用 GCP 以提供充当外部 IP 地址的临时 IP 地址。

STEP 10 | 配置可信的数据平面接口。

1. **Trust VPC Network name**（可信的 **VPC** 网络名称）— 选择现有网络。
2. **Trust Subnet name**（可信的子网名称）— 选择现有网络。
3. **Enable External IP for Trust**（启用可信的外部 **IP**）— 启用 GCP 以提供充当外部 IP 地址的临时 IP 地址。

STEP 11 | 配置其他接口。必须输入想要添加的数据平面接口数；默认为 0 （无）。部署页面始终显示另外五个编号为 4-8 的数据平面字段。

1. **Additional Dataplane interfaces**（其他数据平面接口）— 输入其他数据平面接口的数量。

   如果此数字为 *0*（默认），即使已填写接口字段，也会忽略编号为 *4-8* 的数据平面。例如，如果指定 *2*，然后填写三个接口的信息，则仅创建前两个。
2. **Additional Dataplane # VPC name**（其他数据平面 **# VPC** 名称）— 选择现有网络。
3. **Dataplane # Subnet name**（数据平面 # 子网名称）— 选择已存在的子网。
4. **Enable External IP for dataplane # interface**（启用数据平面 # 接口外部 **IP**）— 启用 GCP 以提供充当外部 IP 地址的临时 IP 地址。

©2024 Palo Alto Networks, Inc.

STEP 12 | **Deploy**（部署）实例。

STEP 13 | 使用 Google Cloud Deployment Manager查看和管理您的部署。

STEP 14 | 使用 CLI 更改防火墙上的管理员密码。

1. 从命令行登录到 VM 系列防火墙。在 SSH 工具中，连接至管理接口外部 IP，并指定私钥路径。

   Windows 用户：使用 PuTTY 连接到 VM 系列防火墙，并发出命令行指令。要指定私钥路径，请选择 **Connection**（连接） > **SSH** > **Auth**（授权）。在 **Private key file for authentication**（提供密钥文件进行身份验证）中：单击 **Browse**（浏览）以选择私钥。
2. 进入配置模式：

   ```
   VMfirewall> 配置
   ```
3. 输入以下命令：

   ```
   VMfirewall# set mgt-config users admin password
   ```
4. 输入并确认管理员的新密码。
5. 提交新密码：

   ```
   VMfirewall# 提交
   ```
6. 返回到命令模式：

   ```
   VMfirewall# exit
   ```
7. （可选）如果使用引导文件进行接口交换，则使用下列命令查看接口映射：

   ```
   VMfirewall> debug show vm-series interfaces all
   ```

STEP 15 | 访问 VM 系列防火墙 Web 界面。

1. 在浏览器中创建与管理接口 IP 地址的安全 (https) 连接。

   如果出现网络错误，则检查您是否拥有允许连接的 GCP 防火墙规则。
2. 出现提示时，输入用户名 (admin) 以及 CLI 中指定的管理员密码。
3. （可选） 如果引导结束，则检验引导完成。

   如果发现问题，则在 VM 系列防火墙上搜索日志信息。选择 **Monitor**（监控） > **System**（系统），并在手动搜索字段内输入 **`description contains 'bootstrap'`**，然后在结果中查找指示引导成功的消息。

登录防火墙后，可以添加管理员，并创建接口、区域、NAT 规则和策略规则，就像在物理防火墙上操作一样。

用于 Google Cloud Launcher 负载均衡的管理接口交换

由于内部负载均衡只能将流量发送到下一个跃点负载均衡 Google Compute Engine 实例的主接口，所以 VM 系列防火墙必须能够使用数据面板流量的 eth0。

©2024 Palo Alto Networks, Inc.

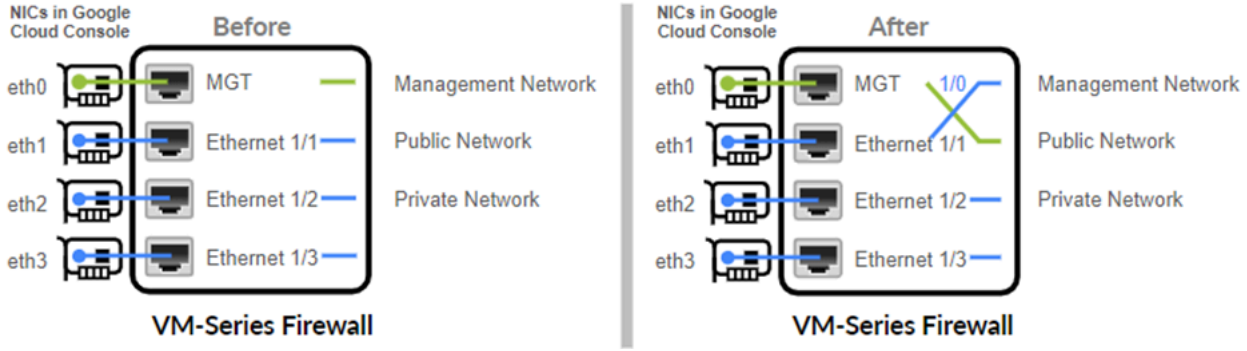
All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

如果 VM 系列防火墙位于 Google Cloud Platform 内部负载均衡接口的下游，则防火墙可以在 eth0 上接收数据面板流量。

- VM 系列防火墙保护直接出站到 Internet 的流量，且无需使用返回到企业网络的 VPN 链接或 Direct Connect 链接。
- 当每个防火墙有且仅有一个后端服务器（如 Web 服务器等）时，VM 系列防火墙保护面向 Internet 的应用程序。VM 系列防火墙和 Web 服务器能够以成对方式在 Google 内部负载均衡地址的下游进行线性扩展。

要使防火墙能够收发 eth0 而非 eth1 上的数据面板流量，则必须交换防火墙的内部负载均衡网络接口的映射，以使 eth0 映射到 ethernet 1/1，而 eth1 则映射到防火墙上的 MGT 接口。

如果可能，配置防火墙并定义策略规则之前，交换管理接口映射。



交换映射到上述接口的方式可使 Google Cloud Platform 将流量分配并路由到位于相同或不同区域的 VM 系列防火墙的正常实例。

交换管理接口

您可以在创建防火墙时交换接口，也可以在创建防火墙后进行配置。

创建时 — 部署 VM 系列防火墙时，您可以通过两种方式启用接口。

- Google Cloud 控制台 — 在创建实例表格中，在 **Metadata**（元数据）字段中输入表项值对，其中 **`mgmt-interface-swap`** 是表项，**`enable`** 是值。
- 引导文件 — 创建包含引导配置中 **`mgmt-interface-swap`** 操作命令的引导文件，如在 Google Cloud Platform 上引导 VM 系列防火墙中所述。在创建实例表格中，在 **Metadata**（元数据）字段输入表项值对，以启用引导选项。

从 **VM** 系列防火墙 — 登录到防火墙，并使用 VM 系列防火墙 CLI 以交换管理接口。在操作模式中，发出以下命令：

```
set system setting mgmt-interface-swap enable yes
```


©2024 Palo Alto Networks, Inc.

- 选择一种方法来指定接口交换设置 — 引导配置文件、防火墙 *CLI* 或 *Google Compute Engine* 实例 ***Metadata***（元数据）字段（从 *Google Cloud* 控制台访问）。使用一种方法可确保防火墙上的行为可预测。

  在 *Google Cloud Console* 中，您无法确认是否交换了 *eth0* 和 *eth1*。完成交换后，您必须记住，负载均衡在 *eth0* 上，而防火墙管理接口在 *eth1* 上，因此，您可以正确配置 *Google Cloud Platform* 负载均衡，并创建安全策略规则来确保一个或多个 *VM* 系列防火墙的负载均衡的安全。
- 如果在交换前已经配置了 *VM* 系列防火墙，请检查 *eth0* 和 *eth1* 的任何 *IP* 地址变更是否会对策略规则造成影响。

使用 VM 系列防火墙 CLI 以交换管理接口

仅当您的架构将 *VM* 系列防火墙放置在 *Google Cloud Platform* 内部负载均衡器下游时才需要执行此任务。

如果没有在部署防火墙时指定元数据以将管理接口 (MGT) 与数据面板接口互换，您可以使用 CLI 以使防火墙接收主接口上的数据面板流量。

STEP 1 | 从 Google Cloud Platform Marketplace 部署 VM 系列防火墙.

继续之前，验证防火墙是否至少有两个网络接口（*eth0* 和 *eth1*）。如果仅用一个接口启动防火墙，接口交换命令可能使防火墙启动到维护模式。

STEP 2 | 在 Google Cloud 控制台上查看 VM 实例详细信息，以检验 eth1 的网络接口 IP 地址，并验证是否所有安全规则军允许连接（HTTPS 和 SSH）到新管理接口 (eth1)。

STEP 3 | 登录到 VM 系列防火墙 CLI，然后输入以下命令：

```
set system setting mgmt-interface-swap enable yes
```

您可以通过命令行界面查看默认映射。输出与下列类似：

```
> debug show vm-series interfaces all Interface_name Base-
OS_port   mgt                eth0   Ethernet1/1      eth1
   Ethernet1/2      eth2
```

STEP 4 | 确认希望交换接口（将 eth1 数据面板接口用作管理接口）。

STEP 5 | 重启防火墙，以使交换操作成效：

```
request restart system
```

STEP 6 | 验证接口交换已完成：

```
debug show vm-series interfaces all
```


©2024 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用 Google Stackdriver 监控

Google® Compute Engine 实例上的 VM 系列防火墙可将自定义 PAN-OS 指标发布到 Google Stackdriver。您可以通过这些指标对性能和使用模式进行评估，从而管理您的防火墙资源。

- Google Stackdriver 权限
- 启动 Google Stackdriver

Google Stackdriver 权限

身份验证要求各不相同，这取决于您是否可以使用默认服务帐户进行身份验证，或是您是否需要使用 Google API 进行身份验证。

可以采用下列两种方式进行验证：

- 使用 **VM** 系列防火墙实例的默认服务帐户 — 如果使用 Google Cloud Platform (GCP™) 控制台，则使用您的电子邮件地址登录，并可以根据项目管理员分配的任何权限或角色访问实例。
- 使用 **IAM** 权限和 **Google API** — 如果使用 Google SDK API 和 gcloud，则必须调用 API 进行身份验证。当想要从命令行管理防火墙，或是运行脚本以配置防火墙时，您通常会使用 Google SDK。

使用 Google Cloud 控制台或 gcloud 命令行工具创建的每个 Google Compute Engine 实例都有一个其名称以电子邮件地址格式存在的默认服务帐户：

```
<project-number>-compute@developer.gserviceaccount.com
```

要查看防火墙实例的服务帐户名称，请查看实例详细情况，并滚动至底部（请参阅 Compute Engine 默认服务帐户）。

默认服务帐户可以管理身份验证，以便监控同一项目中用作 VM 系列防火墙的 VM。

- 访问范围允许防火墙启动 API 调用以监控 Google Cloud 项目中的 VM。
- 除非其中一个被监控的虚拟机包含需要 Google API 的应用程序的自定义映像， 否则无须访问 Google API。

如果想在不同项目中从物理防火墙或 VM 系列防火墙设置监控，则必须使用 Google API 进行身份验证。有两个前提条件：

- 必须安装 Google API。
- 您的帐户必须具有监控指标编写器和 Stackdriver 帐户查看器的角色。

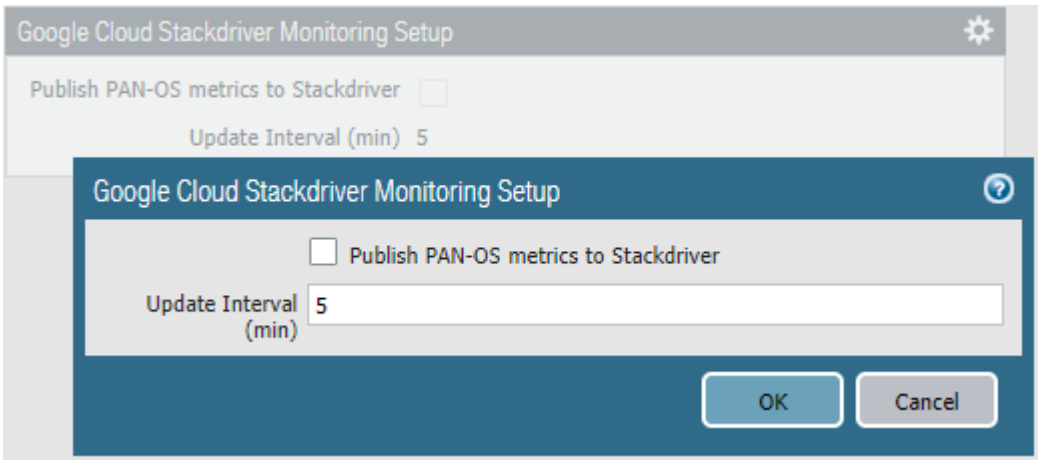
启动 Google Stackdriver

有关发布到 Google Stackdriver 上的 PAN-OS 指标的详细信息，请参阅 发布用于监控的自定义 PAN-OS 指标。

©2024 Palo Alto Networks, Inc.

STEP 1 | 在 Google Compute Engine 实例上将 PAN-OS 指标从 VM 系列防火墙发布到 Stackdriver。

1. 登录到 VM 系列防火墙的 Web 界面。
2. 选择 **Device**（设备）> **VM-Series**（**VM** 系列）。在 Google Cloud Stackdriver 监控设置上，单击**Edit** ( )。
   1. 选择 **Publish PAN-OS metrics to Stackdriver**（将 **PAN-OS** 指标发布到 **Stackdriver**）。



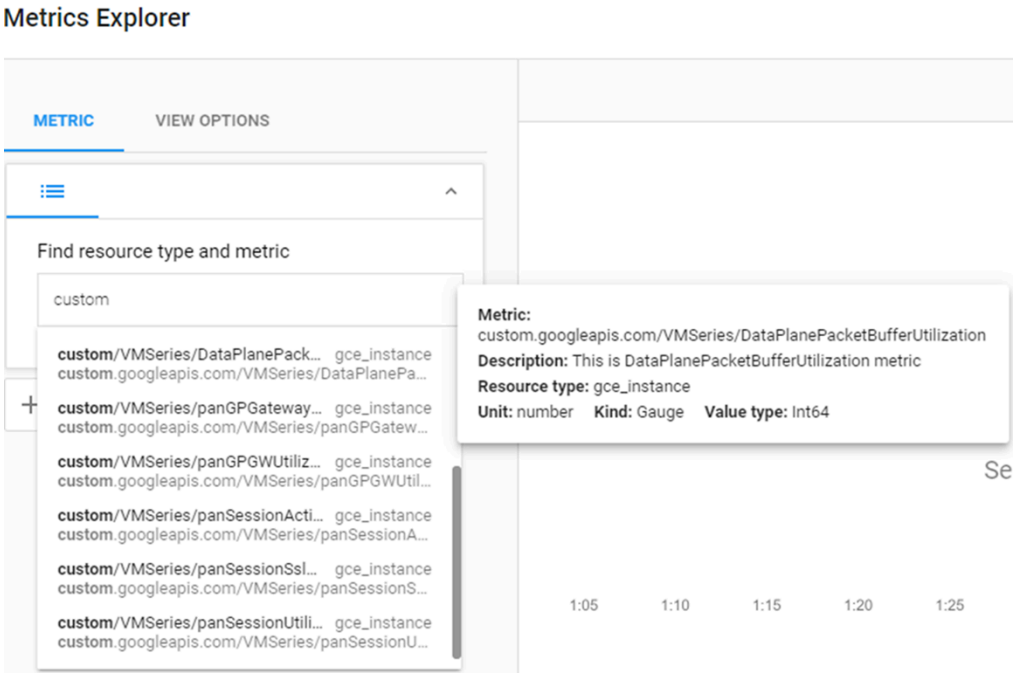
   2. 设置 **Update Interval**（更新间隔）（范围是 1 至 60 分钟，默认为 5 分钟）。这是防火墙将指标发布到 Stackdriver 的频率。
   3. 单击 **OK**（确定）。
3. **Commit**（提交）更改。

   等到防火墙开始将指标发布到 Stackdriver 之前，您无法为 PAN-OS 指标配置警报。

©2024 Palo Alto Networks, Inc.

STEP 2 | 确认您可以在 Stackdriver 上查看指标。

1. 在 Google Cloud 控制台上，选择 **Products and Services**（产品和服务）> **Monitoring**（监控）。
2. 在 Stackdriver 上选择 **Resources**（资源）> **Metrics Explorer**（指标浏览器）。
3. 在查找资源类型和指标部分，在搜索字段中输入 **`custom`** 以筛选 PAN-OS 指标。



STEP 3 | 在 Stackdriver 上配置 PAN-OS 指标的警报和操作。请参阅监控 Google Compute Engine 快速入门和 Stackdriver 警报简介。

在 Google Cloud Platform (GCP) 上启用 VM 监控以跟踪 VM 更改

您可以启用运行 PAN-OS 9.0（虚拟或物理）的任何防火墙，以监控 Google Compute Engine 实例上部署的应用程序工作负载。通过 VM 监控，您可以监控 VM 系列防火墙上的预定义元数据元素集或属性。在 PAN-OS 9.1 管理指南中，可以查看 Cloud Platform 中虚拟机上受监控的属性。

通过感知 Google VPC 内虚拟机的添加、移动或删除，您可以创建自动适应于应用程序环境中更改的安全策略规则。因为虚拟机已部署或移动，防火墙可以收集属性（或元数据元素）。您可以使用此元数据进行策略匹配，定义动态地址组（请参阅使用动态地址组保护 VPC 中实例的安全）。

在每个防火墙或具有多个虚拟系统的防火墙上每个虚拟系统上，您最多可配置 10 个 VM 信息源。此外，信息源还可以通过 Panorama 模板推送。

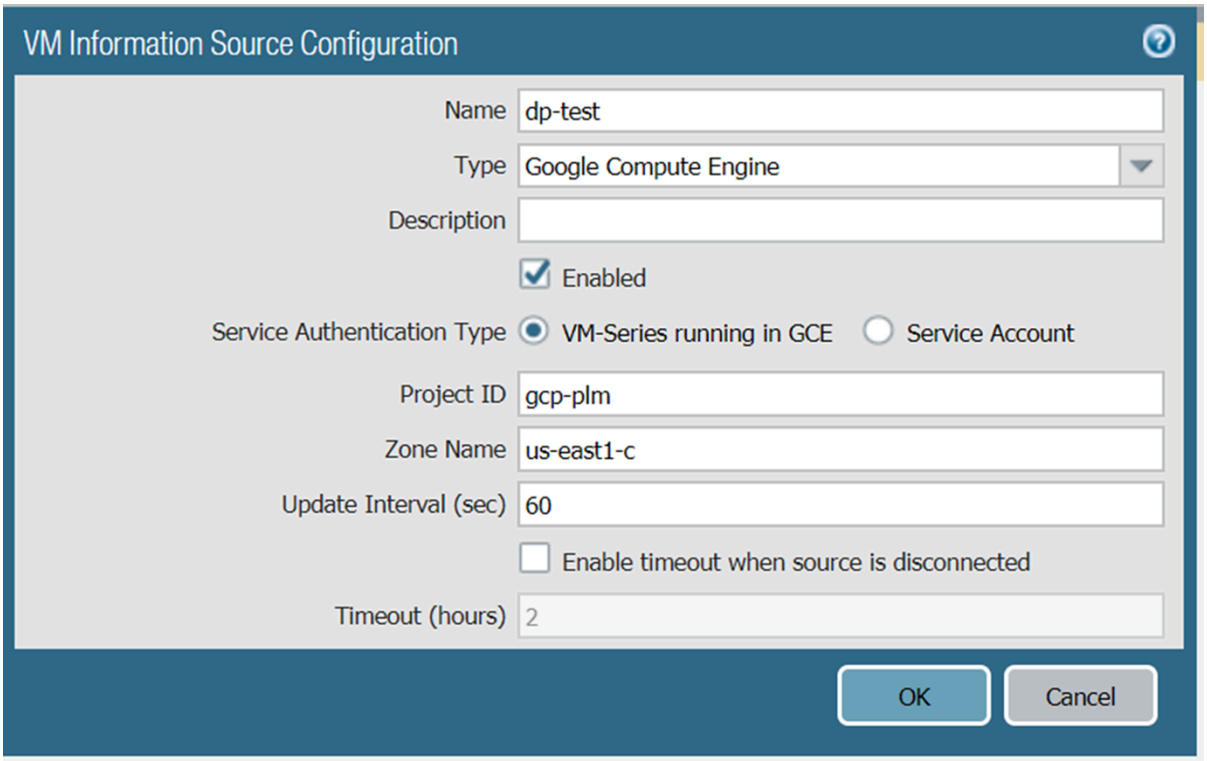
要执行 VM 监控，必须具有监控指标编写器的 IAM 角色。

STEP 1 | 登录到已部署的防火墙。

©2024 Palo Alto Networks, Inc.

STEP 2 | 启用 VM 监控。

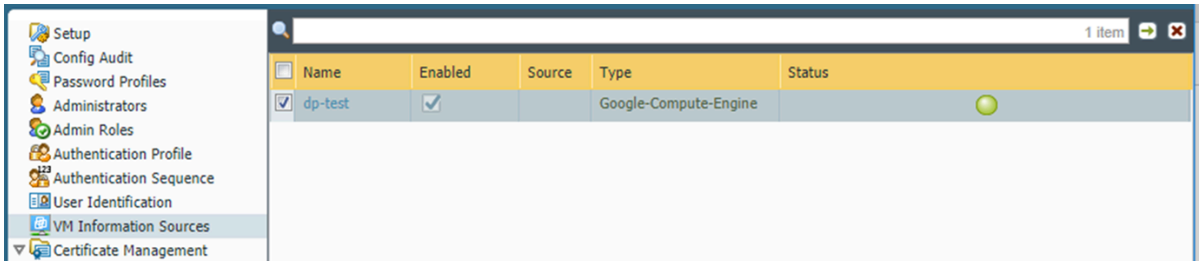
1. 选择 **Device**（设备）> **VM Information Sources**（**VM** 信息源）。
2. **Add**（添加）VM 信息源，并输入以下信息：
   - 指定用于标识要监控的实例的 **Name**（名称）。
   - 选择 Google Compute Engine **Type**（类型）。
   - 选择 **Enabled**（启用）。
   - 选择 **Service Authentication Type**（服务身份验证类型）。
     - 如果选择 **VM-Series running in GCE**（**GCE** 中运行的 **VM** 系列），则使用创建实例时生成的默认服务帐户进行身份验证。这是实例元数据的一部分。
     - 如果想要从当前项目之外的防火墙进行监控，则选择 **Service Account**（服务帐户）。必须上传 JSON 格式的服务帐户凭据。请参阅创建和管理服务帐户密钥。
   - （可选）将 **Update interval**（更新间隔）修改为 5-600 秒之间的值。默认情况下，防火墙会每隔 5 秒轮询一次。每隔 60 秒将对 API 调用进行排队和检索，从而更新需要的时间可能最长为 60 秒加上配置的轮询间隔。



   - （可选）要在超时之前更改小时数，则选择 **Enable timeout when the source is disconnected**（源断开后启用超时），并在连接到受监控源的连接关闭时输入超时（小时）（范围是 2-10；默认为 2）。

     如果防火墙无法访问主机且已达到指定限制，防火墙关闭与源的连接。
   - 单击 **OK**（确定）并 **Commit**（提交）更改。

 ©2024 Palo Alto Networks, Inc.



STEP 3 | 验证连接状态。

如果连接状态为挂起或断开，则检查源是否正常工作，并且防火墙能够访问源。如果您使用管理 (MGT) 之外的端口与受监控的源通信，则必须更改服务路由（选择 **Device**（设备） > **Setup**（设置） > **Services**（服务），单击 **Service Route Configuration**（服务路由配置）并修改 **VM Monitor**（**VM** 监控）服务的 **Source Interface**（源接口））。

使用动态地址组保护 VPC 中的安全实例

在根据需要启动新实例的动态环境（如 Google® Cloud Platform）中，管理安全策略的管理开销可能会很高。使用在策略中使用动态地址组可以灵活地防止服务中断或出现保护方面的差距。

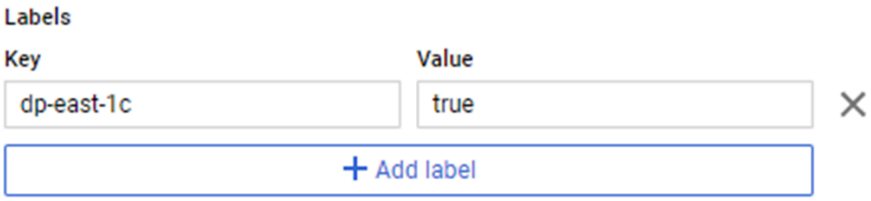
此工作流程的前提是：假定您已部署 VM 系列防火墙，在实例上配置一些应用程序，且已启用 Google Stackdriver 监控。

STEP 1 | 配置防火墙以监控 VPC。

STEP 2 | 标记 VPC 中的实例。

标签是一个名称-值对。您可以在 Google Cloud 工作台、Google API 调用或 Google Cloud Shell 中标记资源。在此任务中，我们标记实例；但是，标签可以应用于多种资源，如标记资源中所述。

您还可以从实例浏览器添加标签。

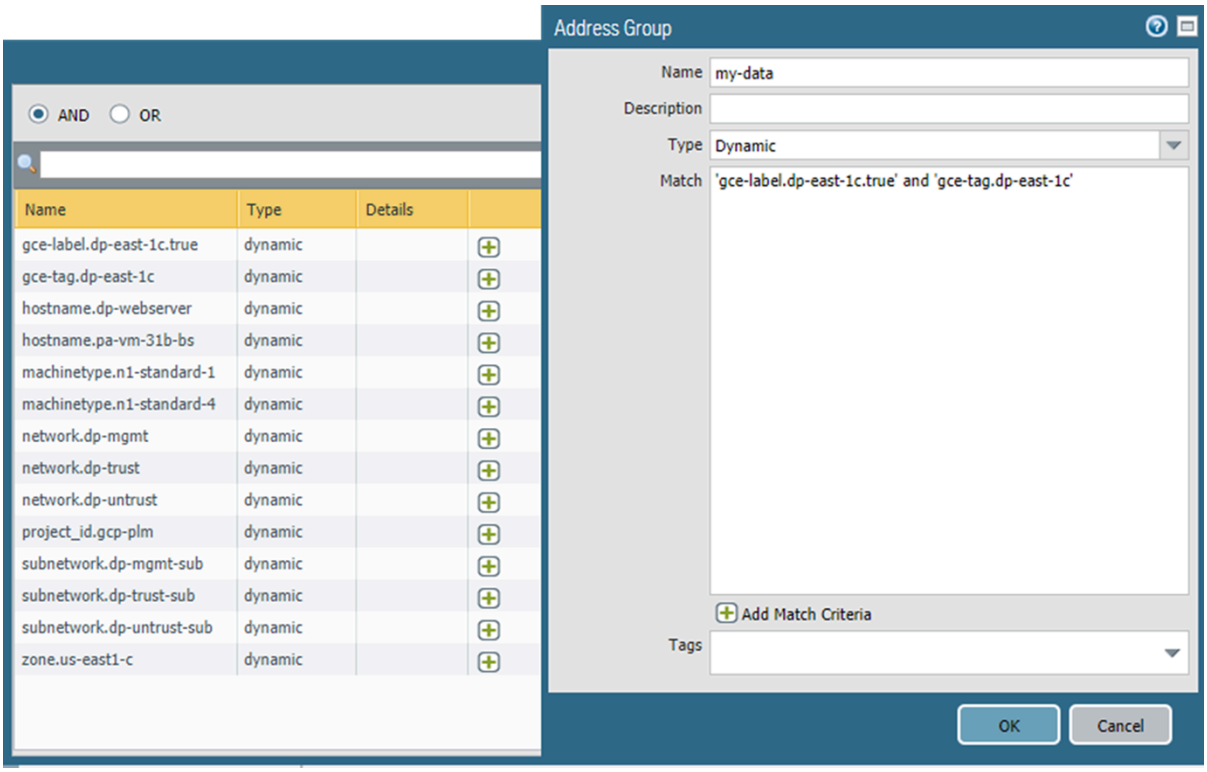


您可以创建标签来支持您的策略，以对安全策略有用的方式区分资源。

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 在防火墙上创建动态地址组。

1. 选择 **Object**（对象） > **Address Groups**（地址组）。
2. **Add**（添加）动态地址组，并指定 **Name**（名称）和 **Description**（说明）。
3. 设置 **Type**（类型）为**Dynamic**（动态）。
4. 定义匹配条件。
   1. **Add Match Criteria**（添加匹配条件），然后选择 **And** 运算符。
   2. 选择用于筛选或进行匹配的属性。



5. 单击 **OK**（确定）。
6. 单击 **Commit**（提交）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 在安全策略规则中使用动态地址组。

创建规则以允许对于属于动态地址组（称为 my-data）的所有 Web 服务器的 Internet 访问。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. **Add**（添加）规则和规则 **Name**（名称），然后确认 **Rule Type**（规则类型）为 `universal`。
3. 在 **Source**（源）选项卡中，添加 trust 作为 **Source Zone**（源区域）。
4. 在源地址部分，**Add**（添加）新的 my-data 组。
5. 在 **Destination**（目标）选项卡中，添加 untrust 作为 **Destination Zone**（目标区域）。
6. 在 **Service/URL Category**（服务/**URL** 类别）选项卡中，确认已将服务设置为 **application-default**。
7. 在 **Actions**（操作）选项卡中，将 **Action**（操作）设置为 Allow（允许）。
8. 在配置文件设置中，将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件），然后附加防病毒软件、反间谍软件和漏洞保护的默认配置文件。
9. 单击 **OK**（确定）。
10. 单击 **Commit**（提交）。

STEP 5 | 在防火墙上验证是否已填充动态地址组的成员。

将对属于此地址组并在此显示的所有 IP 地址实施策略。

1. 选择 **Policies**（策略） > **Security**（安全），并选择规则。
2. 从下拉列表中选择 **Inspect**（检查）。您还可以验证匹配条件是否准确。
3. 单击 **More**（更多）以验证是否显示已注册 IP 地址列表。

使用自定义模板或 gcloud CLI 部署 VM 系列防火墙

可在 **paloaltonetworksgcp-public** 项目中使用在 Google Cloud Platform Marketplace 上发布的官方 VM 系列映像。如果想要从 **gcloud** 命令行调用，或是在已写入或调整的模板内调用这些映像，则必须知道这些映像的路径。

- BYOL：vmseries-byol-<*version*>
- PAYG 套餐 1：vmseries-bundle1-<*version*>
- PAYG 套餐 2：vmseries-bundle2-<*version*>

使用 gcloud CLI 查找当前映像名称和项目：

```
gcloud compute images list --project paloaltonetworksgcp-public
 --no-standard-images   NAME PROJECT FAMILY DEPRECATED STATUS
 vmseries-bundle1-810 paloaltonetworksgcp-public READY   vmseries-
bundle2-810 paloaltonetworksgcp-public READY   vmseries-byol-810
 paloaltonetworksgcp-public READY
```

添加 **--uri** 标志以查看映像路径：

©2024 Palo Alto Networks, Inc.

```
gcloud compute images list --project paloaltonetworksgcp-public
 --no-standard-images --uri
```

```
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-
public   /global/images/vmseries-bundle1-810   https://
www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public
   /global/images/vmseries-bundle2-810   https://www.googleapis.com/
compute/v1/projects/paloaltonetworksgcp-public   /global/images/
vmseries-byol-810
```

例如，从 https://github.com/PaloAltoNetworks 下载 gcp-two-tier 模板。

此模板将包含 PAN-OS 版本的映像名称与 URL 路径区分开。在 `two-tier-template.py` 中，*image* 变量需要映像名称；例如：*vmseries-byol-810*。`vm-series-template.py` 使用 *COMPUTE_URL_BASE* 和 *sourceImage* 的值构建路径。

©2024 Palo Alto Networks, Inc.

使用适用于 GCP 的 Panorama 插件进行 VM 监控

使用适用于 Google Cloud Platform (GCP) 版本 2.0.0 的 Panorama 插件，您可以创建通过 GCP 项目进行身份验证的 VM 监控配置，并监控 VM 系列防火墙和其中部署的其他 VM。建立与项目的连接后，该插件可以检索 Panorama 和 GCP 资产之间的 IP 地址到标记通信。标记可以是预定义属性，VM 的用户定义的标签和用户定义的网络标记（参阅查看并创建标记）。

适用于 GCP 的 Panorama 插件从运行的 VM 检索内部和外部 IP 地址，并定期从连接的 GCP VPC 中的 VM 检索 IP 地址到标记映射。

您可以使用标记将 VM 组织到动态地址组中，然后在允许或拒绝到特定 VM IP 地址的流量的安全策略规则中引用标记。要一致地实施安全策略，您随后可以将规则推送到 VM 系列防火墙。

- 使用适用于 GCP 的 Panorama 插件配置 VM 监控

使用适用于 GCP 的 Panorama 插件配置 VM 监控

本主题介绍了准备 GCP 资产以进行 VM 监控和查看所需的 Panorama 元素的步骤，并介绍了如何在适用于 Google Cloud Platform (GCP) 的 Panorama 插件上配置 VM 监控。

- 配置 GCP 资产以进行 VM 监控
- 查看并创建标记
- 使用适用于 GCP 的 Panorama 插件配置 VM 监控
  - 准备 Panorama 以配置 VM 监控
  - 设置 VM 监控

配置 **GCP** 资产以进行 **VM** 监控

您可以监控从 GCP 市场部署的 VM 系列防火墙，使用自动扩展防火墙模板部署的防火墙，从 GCP 控制台或 gcloud 命令行创建的 GCE 实例，或者在 GCP 中部署的虚拟机。如果您从 Google Marketplace 部署 PAN-OS VM，请按照在 Google Cloud Platform 上设置 VM 系列防火墙中的说明进行操作。

查看 **IAM** 角色

确保您具备 VM 监控任务的以下最低权限：

- 在 GCP 控制台中，为您的项目创建一个服务帐户，并向项目所有者或编辑者授予权限。

  无法自动创建服务帐户。如果您没有创建服务帐户的权限，则可以要求管理员创建服务帐户，并为您分配相应的角色。
- 查看您的服务帐户：只读。
- 查看从 Google Marketplace 部署的 PAN-OS VM：计算查看器。
- 将用户定义的标签分配给实例：项目所有者、编辑者或实例管理员。

©2024 Palo Alto Networks, Inc.

创建服务帐户

在 Panorama 上使用 GCP 插件配置 VM 监控之前，您必须使用 GCP 控制台创建服务帐户，这些服务帐户可授予访问 GCP 项目、其中部署的 VM 系列防火墙、您希望 Panorama 管理的任何其他 VM，以及相关网络和子网的权限。适用于 Panorama 的 GCP 插件检索 Google 资产的预定义属性、用户定义的 VM 标签和用户定义的网络标记。

在 GCP 版本 3.1.0 或更高版本的 Panorama 插件的共享 VPC 设置中，您可以为主机项目创建服务帐户，并授予对服务项目的权限。有关更多信息，请参阅 在 GCP 中创建跨项目服务帐户。必须在监视定义中使用此服务帐户凭据来检索多个附加服务项目的标记。

每个项目都拥有一个在创建项目时自动创建的默认服务帐户。如果您专门为 VM 监控创建一个单独的服务帐户，则可以更好地控制用户及其角色。您最多可以为每个项目配置 100 个服务帐户。

STEP 1 | 在 Google Cloud Platform 控制台中，选择要监控的项目。

STEP 2 | 选择 **IAM & Admin**（**IAM** 和管理员）> **Service accounts**（服务帐户），然后选择 **+Create Service Account**（+创建服务帐户）。

输入服务帐户名称和说明，然后单击 **Create**（创建）。

STEP 3 | 从下拉菜单中选择角色类型，然后在右侧选择适当的访问级别。

例如，选择 Project（项目）> Editor（编辑器）。您可以为服务帐户选择多个角色。

完成后，单击 **Continue**（继续）。

STEP 4 | 向特定用户授予访问此服务帐户的权限。从右侧的 **Permissions**（权限）列中选择成员，以授予他们访问上一步中的角色的权限。

STEP 5 | （可选）单击 **+CREATE KEY**（+创建密钥）以创建用来通过 Google Cloud CLI 进行身份验证的凭据，以访问 VM 系列防火墙、网络以及与此服务帐户相关联的其他 VM。

将会自动下载该密钥，请确保将其存储在安全的位置。生成的私钥的 JSON 格式如下：

```
{ "type": "service_account", "project_id": "gcp-xxx",
 "private_key_id":"252e1e7a2e9c84b5d4dbb6195b1de074594b6499",
 "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDAd0i
+RMKCtrsO\n4KHnzTAPrgoBjRgpjyNcvQmdUqHr\n-----END PRIVATE
 KEY-----\n", "client_email": "dlp-vm-monit-svc-acct@gcp-
xxx.iam.gserviceaccount.com", "client_id":"108932514695821539229",
 "auth_uri": "https://accounts.google.com/o/oauth2/auth",
 "token_uri": "https://oauth2.googleapis.com/token",
 "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/
v1/certs", "client_x509_cert_url": "https://www.googleapis.com/
robot/v1/metadata/x509/dlp-vm-monit-svc-acct%40gcp-
xxx.iam.gserviceaccount.com" }
```

查看并创建标记

“标记”是预定义属性、用户定义的标签和用户定义的网络标记的总称。

 ©2024 Palo Alto Networks, Inc.

- 将会自动为 Google VM 创建预定义标记（属性）。配置 VM 监控时，您可以选择监控所有 8 个预定义属性，也可以创建要监控的自定义属性列表。
- 您可以为 VM 标签和网络标记定义自己的标记。

标记 VM 和网络，以便您可以标识并对其进行分组，从而构造规则以实施安全策略。您可以标记在 Google 项目中部署的所有 VM，例如 VM 系列防火墙、Web 服务器、应用程序服务器或负载均衡器。

- 标记必须与 VM 相关联，这也适用于网络和子网。
- 如果有多个 IP 地址与实例相关联（例如，如果您标记 VM 系列防火墙可信和不可信接口），则 Panorama 会生成多组标记信息。

Panorama 插件可以检索和注册的标记总数，取决于 Panorama 运行的 PAN-OS 版本和托管 VM 系列防火墙的版本。

Google 区域、Google 地区、VPC 名称和子网名称用于标记 VM 上具有特定于网络接口的多个接口的网络接口。

预定义属性

适用于 Panorama 的 Google Cloud Platform 插件可从任何托管 VM 检索以下预定义属性：

- 项目 **ID** — 例如：google.project-id.myProjectId。

  要在 Google 控制台上查找项目信息，请选择您的项目，然后选择 **IAM & Admin**（**IAM** 和管理员）> **Settings**（设置）。
- 服务帐户 — 服务帐户格式为电子邮件。例如：google.svc-accnt.sa-name@project-id.iam.gserviceaccount.com。

  要查找服务帐户，请查看 VM 实例详细信息。
- **VPC** 名称 — 托管 VM 的 VPC 网络的名称。例如：google.vpc-name.myvnet。
- 子网名称 — 您为托管 VM 接口创建的子网的名称。例如，对于 VM 系列防火墙不可信接口，您为不可信接口创建的子网的名称：google.subnet-name-untrust.web。
- **OS SKU** — 您在部署托管 VM 时选择的操作系统。例如：google.os-sku.centos-7。

  如果 *VM* 使用自定义映像，则不支持此属性。
- **Google** 区域 — 您在部署 VM 时选择的区域。例如：google.zone.us-east1-c。
- **Google** 地区 — 地区包含您所选择的区域。例如：google.region.us-east1。
- 实例组名称 — 例如：google.instance-group.myInstanceGroup。要在 Google 控制台中查看或创建实例组，请选择 **Compute Engine** > **Instance Group**（实例组）。

用户定义的标签

Panorama 最多使用 16 个用户定义的标签。如果标签超过 16 个，Panorama 会按字母顺序对用户定义的标签进行排序，并使用前 16 个标记。

©2024 Palo Alto Networks, Inc.

查看 Google 对标签键值对的要求：键的最小长度为 1 个字符，最大长度为 63 个字符，并且不能为空。值可以为空，并且最大长度为 63 个字符。

要在 GCP 控制台中创建或查看标签，请转到**Compute Engine** > **VM Instances**（**VM** 实例），然后选择 **Show Info Panel**（显示信息面板）。选择一个或多个 VM，然后在 **Info**（信息）面板中选择 **Labels**（标签）。单击 **+Add a label**（+添加标签），添加键和值，然后单击 **Save**（保存）。

用户定义的网络标记

Panorama 最多使用 8 个用户定义的网络标记，如果标记超过 8 个，Panorama 会按字母顺序对用户定义的网络标记进行排序，并使用前 8 个标记。

请注意，Google 对网络标记的限制如下：

- 每个网络标记的最大长度为 63 个字符。
- 您可以使用小写字母、数字和破折号；标记必须以小写字母开头，并以数字或小写字母结尾。

要在 GCP 控制台中创建或查看网络标记，请转到**Compute Engine** > **VM Instances**（**VM** 实例），然后选择一个实例。**Edit**（编辑）实例，并向下滚动到 **Network Tags**（网络标记），输入标记（用逗号分隔），然后单击 **Save**（保存）。请参阅配置网络标记。

使用适用于 GCP 的 Panorama 插件配置 VM 监控

标记 GCP 资产并创建服务帐户后，使资产可用于 Panorama，以便您设置 VM 监控。

准备 **Panorama** 以配置 **VM** 监控

请按照以下步骤，启用 Panorama 以管理和监控 GCP 资产。GCP 中部署的任何 VM 都可以是 Panorama 中的托管设备。

STEP 1 | 在 Panorama 中，添加与 GCP 项目相关联的 VM 系列防火墙和其他 VM 作为托管设备。

STEP 2 | 添加设备组并为其分配托管设备。设备组是一组您要作为组进行管理的防火墙或虚拟系统。

一个 *VM* 只能是一个设备组的成员。仔细计划您的设备组。

STEP 3 | 添加模板。命名模板并接受默认 VPC。

STEP 4 | 添加模板堆栈。**Add**（添加）堆栈，**Add**（添加）您刚创建的模板，然后选择您的设备。

STEP 5 | 提交更改。

设置 **VM** 监控

STEP 1 | 如果未安装，请安装适用于 GCP 的 Panorama 插件。

STEP 2 | 登录到 Panorama Web 界面，然后选择**Panorama** > **Google Cloud Platform**。

©2024 Palo Alto Networks, Inc.

STEP 3 | 设置 VM 监控。

1. 配置常规设置。
   1. 选择 **Panorama** > **Google Cloud Platform** > **Setup**（设置） > **General**（常规）。要编辑设置，请单击齿轮。
      - 选中 **Enable Monitoring**（启用监控）以允许对配置服务帐户的所有项目进行 VM 监控。
      - 输入 **Monitoring Interval**（监控间隔）（以秒为单位）。这是标签检索事件之间的时间长度。
2. **Add**（添加）通知组。通知组是 Panorama 会向其推送 IP 地址到标记的映射和更新的设备组列表。

   一个项目只能有一个通知组。

   1. 选择 **Panorama** > **Google Cloud Platform** > **Setup**（设置） > **Notify Groups**（通知组），然后单击 **Add**（添加）。
   2. 输入用于标记 Panorama 向其推送检索的 VM 信息（IP 地址到标记的映射）的防火墙组的 **Name**（名称）。
   3. 选择 Panorama 将向其推送从项目检索的 VM 信息（IP 地址到标记的映射）的 **Device Groups**（设备组）。VM 系列防火墙使用更新来确定安全策略中引用的动态地址组的当前成员列表。

      仔细计划您的设备组。

   4. 选择预定义标记或自定义标记。
      - **Select All 8 Predefined Tags**（选择所有 **8** 个预定义标记）— 选择此选项可选择所有预定义属性（标记）。
      - **Custom Tags**（自定义标记）— 选择此选项可为预定义属性、用户定义的标签和用户定义的网络标记创建标记列表。
   5. - 确保在单个通知组中包含所有相关的设备组。
      - 如果您想要注册 Panorama 已推送到通知组内防火墙的标记，则必须删除监控定义。

 ©2024 Palo Alto Networks, Inc.

- 要将标记注册到启用用于多个虚拟系统的防火墙上的所有虚拟系统，则必须将每个虚拟系统添加到 Panorama 上的单独设备组，并分配设备组到通知组。如果您将所有虚拟系统分配到一个设备组，则 Panorama 仅将标记注册到一个虚拟系统中。

3. 添加 GCP 服务帐户凭据。
   - 命名服务帐户凭据。
   - （可选）输入服务帐户的说明。
   - **Browse**（浏览）以上传您在创建服务帐户时生成的 JSON 文件。

   在共享 VPC 设置中，您需要为主机项目创建服务帐户，并为服务项目授予权限。您可以在 GCP 插件中使用这些服务帐户。这样就可以检索属于附加到主机项目的服务项目的标记

   您必须使用 *Panorama Web* 界面，并且不能使用 *CLI* 添加服务帐户。

   您只能为一个凭据使用一个服务帐户，并且不能从单个 *JSON* 文件创建多个凭据。

添加服务帐户凭据后，您可以从 Panorama 命令行验证凭据：

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

STEP 4 | 创建 **Monitoring Definition**（监控定义）。

监控定义包含项目和通知组的服务帐户凭据。将监控项目中的所有网络资产，并将检索的标记推送到监控定义中列出的设备组。添加新的监控定义时，它将默认启用。

一个项目只能有一个监控定义，并且一个监控定义只能包含一个通知组。

1. 选择 **Panorama** > **Google Cloud Platform** > **Monitoring Definition**（监控定义），然后单击 Add（添加）。
2. **Name**（命名）监控定义。
3. 输入您监控的项目和资产的可选 **Description**（说明）。
4. 选择您在上一步中创建的 **Service Account**（服务帐户）凭据。
5. 选择 **Notify Group**（通知组）。
6. 对与该服务帐户相关联的元素 **Enable**（启用）监控。

STEP 5 | 在 Panorama 上 **Commit**（提交）更改。

验证监控定义的状态是否显示为成功。如果失败，则验证是否输入正确的项目 ID，并为服务提供正确的密钥和 ID。

©2024 Palo Alto Networks, Inc.

STEP 6 | 验证是否可以在 Panorama 上查看 VM 信息，并定义动态地址组的匹配条件。

在 HA 故障转移时，Panorama 会第二次尝试重新连接到 Google Cloud Platform，并检索所有监控定义的标记。如果重新连接一个监视定义时出现错误，Panorama 会生成一条系统日志消息：

```
HA 切换后无法处理订阅；需要用户干预。
```

如果看到此错误，请在 Panorama 中修复问题。例如，删除无效订阅或提供有效凭据，提交更改以促使 Panorama 重新连接，并检索所有监控定义的标记。

即使 *Panorama* 与 *Google Cloud Platform* 断开连接，防火墙也拥有在故障转移前已检索到的所有标记列表，并继续在该 *IP* 地址列表上执行策略。删除监控定义后，*Panorama* 会删除与注册 *VM* 相关联的所有标记。最佳实践是从 *Panorama* 配置面向操作的日志转发到 HTTP 定义，以便您可以立即采取行动。

©2024 Palo Alto Networks, Inc.

在 Google Cloud Platform 上自动扩展 VM 系列防火墙

适用于 Google Cloud Platform (GCP) 版本 2.0.0 的 Panorama 插件有助于您在 GCP 中部署 VM 系列防火墙，并启用 Panorama 管理 VM 系列防火墙以保护 GCP 中的 VM 监控或自动扩展部署。使用 Panorama 的集中策略和防火墙管理可提高管理和维护分布式网络防火墙的运营效率。

通过 Panorama 维护 GCP 托管实例组，您可以创建保护和控制网络的应用程序启用策略。

自动扩展部署支持使用共享 VPC 网络配置或 VPC 网络对等在包含共享 VPC 网络和 VM 系列防火墙的主机项目，以及在包含基于 VM 或基于容器的应用程序部署（Kubernetes 集群）的服务项目中创建公共 VPC 网络。Palo Alto networks 提供模板以帮助您在主机项目中部署 VM 系列防火墙，并在服务项目中部署可选的应用程序示例。

BYOL 和 PAYG 许可证可用于 VM 系列防火墙。许可过程中，VM 系列防火墙实例直接与 Palo Alto Networks 许可证服务器进行通信。

如果您选择 BYOL，则部署可以停用许可证实例以响应缩减事件。如果在适用于 GCP 的 Panorama 插件中配置 VM 系列防火墙的部署信息，并且自动删除防火墙，则 Panorama 将检测防火墙状态并自动注销防火墙。

- 适用于 Google Cloud Platform 的自动扩展组件
- 部署 GCP 自动扩展模板 2

适用于 Google Cloud Platform 的自动扩展组件

典型的 GCP 自动扩展部署使用主机项目和服务项目，并在两者之间形成公用的 VPC 网络。适用于 GCP 的 Panorama 插件可以使用主机和服务 VPC 在单个项目中保护自动扩展部署，或者在 共享 VPC 或对等 VPC 网络配置的主机和服务项目中保护自动扩展部署，其中主机项目包含 VM 系列防火墙和共享 VPC 网络，服务项目包含应用程序部署。如果将应用程序部署在 Kubernetes 集群中，则需要对等 VPC。

- 自动扩展要求
- 准备部署自动扩展模板

自动扩展要求

- 一般要求 — 确保您的环境满足基本要求。
- 适用于 **GCP** 的 **Panorama** 插件 — 如果未安装，请安装适用于 GCP 的 Panorama 插件。

  如果您之前已安装适用于 *GCP* 版本 *1.0.0* 的 *Panorama* 插件，请在安装 *2.0.X* 之前将其删除。否则，您将无法升级。
- **Palo Alto Networks** 自动扩展模板版本 **1.0** — Palo Alto Networks 提供了在主机项目中部署 VM 系列防火墙实例以及在服务项目中配置和部署应用程序示例的模板。有关模板的更多信息，请参阅关于自动扩展模板。

  从 GitHub 下载模板。该 Zip 文件包含分别用于防火墙和应用程序模板的 Zip 文件。

©2024 Palo Alto Networks, Inc.

准备部署自动扩展模板

在部署自动扩展模板之前，请完成以下任务。

- 准备主机项目和所需的服务帐户
- 获取许可证 API 密钥
- 配置适用于 GCP 的 Panorama 插件以保护自动扩展部署
- 准备用于自动扩展的 VM 系列防火墙引导数据包

准备主机项目和所需的服务帐户

您需要主机项目和服务项目才能形成支持防火墙和应用程序模板的共享 VPC 拓扑。您可以创建一个新主机项目或准备一个现有项目作为主机。

要设置共享 VPC，组织管理员必须向主机项目管理员授予共享 VPC 管理员角色。共享 VPC 管理员可以启用一个项目作为主机，并向服务项目管理员授予服务项目管理员角色。请查看有关管理员和 IAM 角色的 GCP 文档。

STEP 1 | 在 GCP 控制台中，创建一个 GCP 项目作为主机。如果您要使用现有项目，请跳到下一步。

要创建新项目，请选择您的组织或 **No organization**（没有组织），单击 **New Project**（新建项目），然后填写项目信息。请注意，这是您 **EDIT**（编辑）项目 ID 的唯一机会。

必须已安装且配置 *Google Cloud SDK*，以便您可以从 *CLI* 通过主机项目进行身份验证。您将使用命令行界面部署防火墙模板和应用程序模板，并将服务项目附加到主机项目。

©2024 Palo Alto Networks, Inc.

STEP 2 | 启用自动扩展所需的 API 和服务。所需的 API 是：

- Cloud Pub/Sub API
- Cloud Deployment Manager API
- Cloud Storage API
- Compute Engine API
- Google Compute Engine Instance Group Manager API
- Google Compute Engine Instance Group Updater API
- Google Compute Engine Instance Groups API
- Kubernetes Engine API
- Stackdriver API
- Stackdriver Logging API
- Stackdriver Monitoring API

您可以从 GCP 控制台或 GCP CLI 启用 API，如下所示。

从 **GCP** 控制台启用 **API**

1. 选择主机项目，然后从 Navigation（导航）菜单选择 **APIs & Services**（**API** 和服务）。
2. 搜索并查看所需的每个 API。
3. **ENABLE**（启用）所有不显示“API 已启用”状态的 API。

从 **CLI** 控制台启用 **API**

1. 在 CLI 中，查看您的配置以确保位于正确的项目中。

```
gcloud config list
```

如果不是，请按如下所示设置项目：

```
gcloud config set project <project-name>
```

2. 发出以下命令以启用所需的 API。

```
gcloud services enable pubsub.googleapis.com gcloud
 services enable deploymentmanager.googleapis.com
 gcloud services enable storage-component.googleapis.com
 gcloud services enable compute.googleapis.com gcloud
 services enable replicapool.googleapis.com gcloud
 services enable replicapoolupdater.googleapis.com gcloud
 services enable resourceviews.googleapis.com gcloud
 services enable container.googleapis.com gcloud services
 enable stackdriver.googleapis.com gcloud services
```


©2024 Palo Alto Networks, Inc.

```
enable logging.googleapis.com gcloud services enable
monitoring.googleapis.com
```

3. 确认已启用所需的 API。

```
gcloud services list --enabled
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 创建用于部署 VM 系列防火墙的服务帐户，并分配自动扩展或 Kubernetes 集群所需的 IAM 角色。

配置防火墙模板时，您可以将此服务帐户的电子邮件地址添加到 VM 系列防火墙 `.yaml` 文件中。在主机项目中，模板使用此服务帐户的凭据创建具有子网的主机 VPC，在 VPC 中部署 VM 系列防火墙，配置 Stackdriver 自定义指标以及创建 Pub/Sub 主题等。

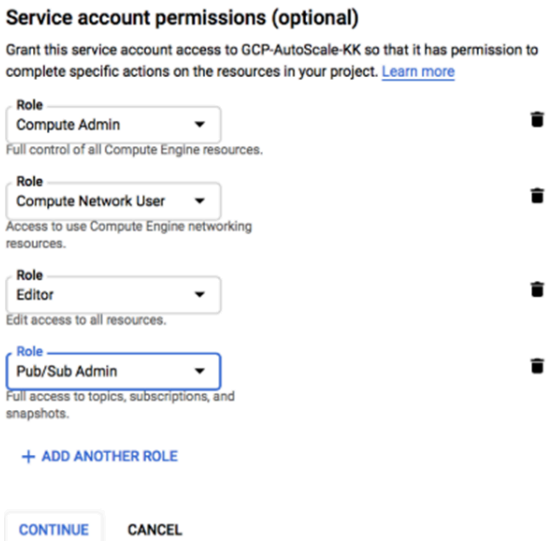
1. 在 GCP 控制台中，选择**IAM & Admin**（**IAM** 和管理员）> **Service accounts**（服务帐户），然后选择 **+CREATE SERVICE ACCOUNT**（+创建服务帐户）。

   填写服务帐户详细信息，然后单击 **CREATE**（创建）。

2. 授予服务帐户权限以自动扩展此项目中的资源。

   从下拉菜单中选择角色类型，然后在右侧选择适当的访问级别。例如，选择 Project（项目）> Editor（编辑器）。您可以为服务帐户选择多个角色。

   - Compute Engine > 计算管理员
   - Compute Engine > 计算网络用户
   - Pub/Sub > 管理员
   - 监控 > 监控指标编写器
   - Stackdriver > Stackdriver 帐户编辑器
   - 存储 > 存储管理员
   - （仅限 GKE）Kubernetes > Kubernetes Engine 集群管理员
   - （仅限 GKE）Kubernetes > Kubernetes Engine 查看者

   添加角色完成后，请单击 **Continue**（继续）。

3. 单击 **+CREATE KEY**（+创建密钥）为主机服务帐户创建密钥。

   - （可选）添加电子邮件地址以授权其他用户或管理员访问此服务帐户。
   - 单击 JSON 以 JSON 格式下载私钥。

©2024 Palo Alto Networks, Inc.

- 将密钥存储在安全位置。部署 GCP 自动扩展模板时将需要此密钥。

4. 单击 **DONE**（完成）。

STEP 4 | 创建 Panorama 管理员可以用来与该主机项目进行交互的服务帐户。

1. 在 GCP 控制台中，选择 **IAM & Admin**（**IAM** 和管理员）> **Service accounts**（服务帐户），然后选择 **+CREATE SERVICE ACCOUNT**（+创建服务帐户）。
2. 填写服务帐户详细信息，然后单击 **CREATE**（创建）。
3. 授予服务帐户访问权限。

   从下拉菜单中选择角色类型，然后在右侧选择适当的访问级别。例如，选择 Project（项目）> Editor（编辑器）。您可以为服务帐户选择多个角色。

   - Compute Engine > 计算查看者
   - Deployment Manager > 查看者
   - Pub/Sub > 管理员

   单击 **CONTINUE**（继续）。
4. 单击 **+CREATE KEY**（+创建密钥）为主机服务帐户创建密钥。
   - （可选）添加电子邮件地址以授权其他用户或管理员访问此服务帐户。
   - 选择 JSON 以 JSON 格式下载私钥。
   - 将密钥存储在安全位置。配置适用于 GCP 的 Panorama 插件以保护自动扩展部署时将需要此密钥。

STEP 5 | （可选）在 CLI 中，确保您可以与新的主机项目进行通信。

1. 将项目设置为您刚创建的主机项目。

   ```
   gcloud set project <your-autoscale-host-project-name>
   ```
2. 创建用于自动扩展的配置。除非您禁用激活，否则将自动激活新配置。

   ```
   gcloud config configurations create <CONFIGURATION_NAME> gcloud config list
   ```

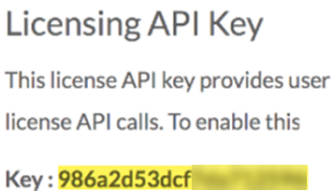
获取许可证 **API** 密钥

您需要许可证 API 密钥，以便 Panorama 可以在 GCP 中许可和取消许可托管资产。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 登录到支持门户，并选择**Assets**（资产） > **Licensing API**（许可证 **API**），然后单击 **Enable**（启用）。系统将显示密钥。

只有超级用户才能查看“启用”链接以生成此密钥。请参阅如何启用、重新生成、扩展许可证 API 密钥。



STEP 2 | 选择并复制密钥。

STEP 3 | 在 CLI 中，使用 SSH 登录 Panorama，然后发出以下命令，以将 <key> 替换为从支持门户复制的 API 密钥：

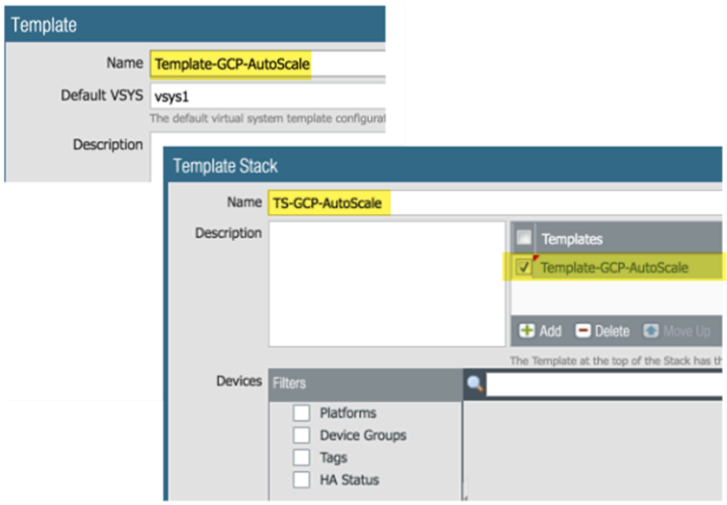
```
request license api-key set key <key>
```

```
API 密钥设置成功
```

配置适用于 **GCP** 的 **Panorama** 插件以保护自动扩展部署

在 Panorama 中，创建资产以支持自动扩展防火墙部署。

STEP 1 | 创建一个模板和一个包括该模板的模板堆栈，然后 **Commit**（提交）更改。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 在 **Network**（网络）上下文中，选择模板或模板堆栈。选择 **Virtual Routers**（虚拟路由器），然后 **Add**（添加）虚拟路由器。

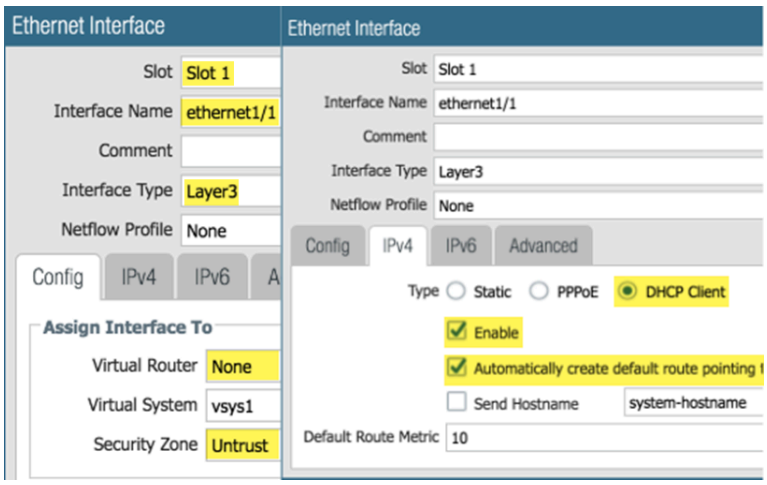
防火墙模板创建静态路由时，会将它们添加到此虚拟路由器。

仅定义一个用于自动扩展部署的路由器。



STEP 3 | 在 **Network**（网络）上下文中，选择您创建的模板，然后选择 **Interfaces**（接口）和 **Add Interface**（添加接口）。

- 在 Config（配置）选项卡上，选择一个插槽，并选择 **Interface name**（接口名称），然后选择第 3 层 **Interface Type**（接口类型）。在 **Security Zone**（安全区域）菜单中，选择 **New Zone**（新建区域），并将区域命名为“不可信”，然后单击 **OK**（确定）。
- 在 **IPv4** 选项卡上，启用 **DHCP Client**（**DHCP** 客户端）和 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）（默认已启用），然后单击 **OK**（确定）。



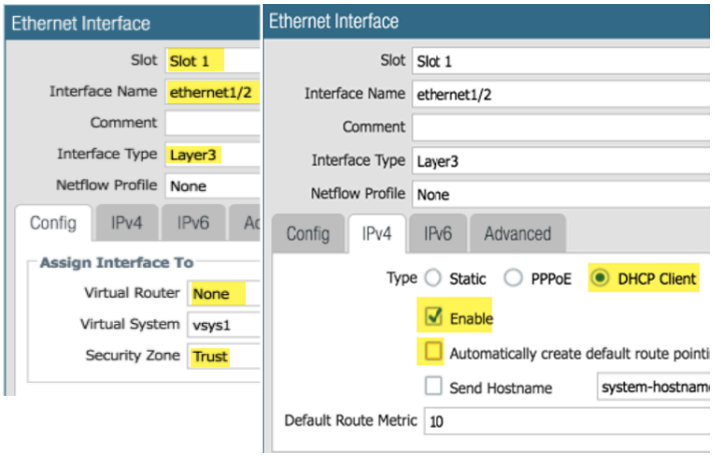
STEP 4 | 添加 ethernet1/2（信任）第 3 层接口。

- 在 Config（配置）选项卡上，选择与上一步相同的插槽，并选择 **Interface name**（接口名称）(ethernet1/2)，然后选择第 3 层 **Interface Type**（接口类型）。在 **Security Zone**（安全区

©2024 Palo Alto Networks, Inc.

域）菜单中，选择 **New Zone**（新建区域），并将区域命名为“可信”，然后单击 **OK**（确定）。

- 在 **IPv4** 选项卡上，启用 **DHCP Client**（**DHCP** 客户端），并禁用 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由），然后单击 **OK**（确定）。



STEP 5 | 返回模板堆栈和先前创建的虚拟路由器。将不可信和可信接口（ethernet1/1 和 ethernet1/2）放置在虚拟路由器中，然后单击 **OK**（确定）。

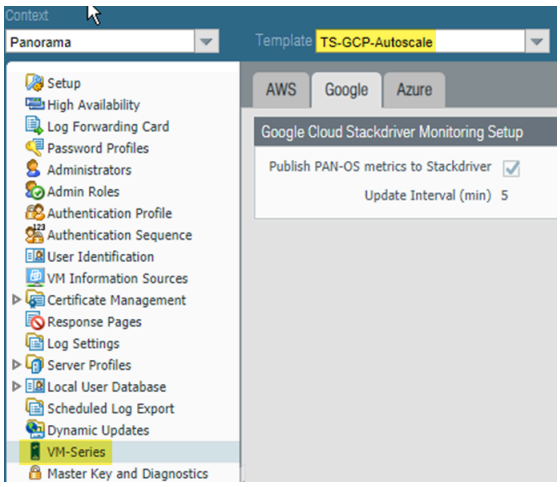


 ©2024 Palo Alto Networks, Inc.

STEP 6 | 为自动扩展部署配置 Stackdriver。

您必须在 Panorama 上拥有 VM 系列插件才能配置 Stackdriver。

1. 在 **Device**（设备）上下文中，从 Template（模板）下拉菜单中选择您之前创建的模板堆栈。
2. 选择 **Device**（设备）> **VM-Series**（**VM** 系列）> **Google**，然后单击 Edit（编辑）齿轮 ( )。启用 **Publish PAN-OS metrics to Stackdriver**（将 **PAN-OS** 指标发布到 **Stackdriver**）。



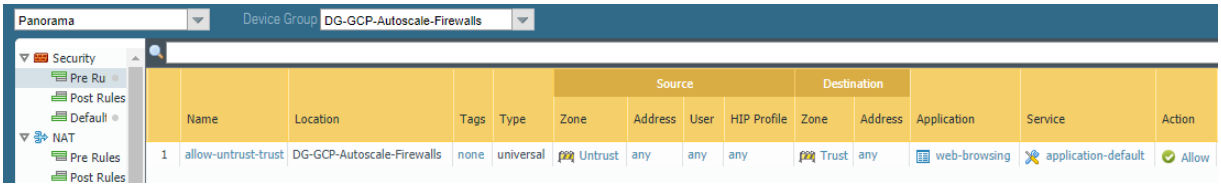
3. 提交更改。

STEP 7 | 创建一个引用您在步骤 1 中创建的模板或模板堆栈的设备组。

该设备组将包含您使用防火墙模板创建的 VM 系列防火墙。

1. 添加一个允许 Web 浏览流量从“不可信”变成“可信”的安全策略。

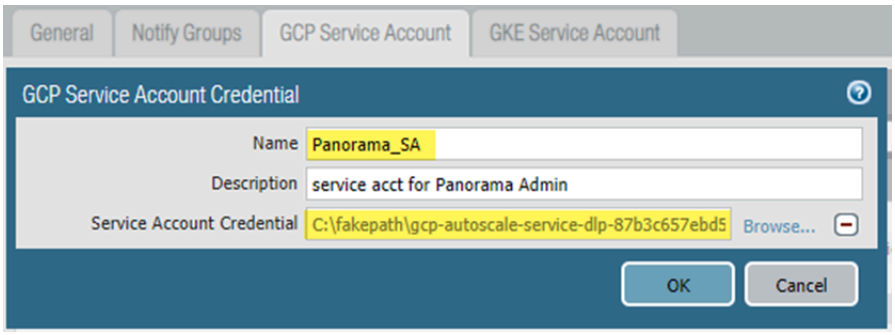
   在 Policies（策略）上下文中，选择您刚创建的设备组。选择 **Security**（安全）> **Pre Rules**（前导规则），然后 **Add**（添加）以下安全策略。



 ©2024 Palo Alto Networks, Inc.

STEP 8 | 为主机项目设置 GCP 服务帐户。

1. 在 Panorama 上下文中，展开 Google Cloud Platform，选择 **Setup**（设置），然后单击 **Add**（添加）。
2. 提供您在步骤 4 中创建的主机服务帐户的名称和说明。
3. 上传您在步骤 4.4 中创建的 JSON 凭据文件。

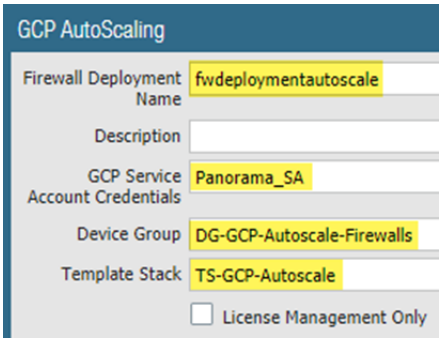


添加服务帐户凭据后，您可以从 Panorama 命令行验证凭据（不能从 Web 界面验证）：

```
request plugins gcp validate-service-account
 gcp_service_account <svc-acct-credential-name>
```

STEP 9 | 在适用于 GCP 的 Panorama 插件上设置自动扩展。

1. 在 Panorama 上下文中，展开 Google Cloud Platform，选择 AutoScaling（自动扩展），然后单击 **Add**（添加）。
2. 提供防火墙部署名称和部署的可选说明。
3. 对于 GCP 服务帐户凭据，提供步骤 8 中的 GCP 服务帐户名称。



4. 选择您在步骤 7 中创建的设备组，以及您在步骤 1 中创建的模板堆栈。
5. 禁用 **License Management Only**（仅限许可证管理）以确保流量安全。

STEP 10 | 提交更改。

准备用于自动扩展的 **VM** 系列防火墙引导数据包

引导过程中，防火墙的初始请求提供了主机 IP 地址和序列号，以及 VM 身份验证密钥，因此 Panorama 可以验证 VM 身份验证密钥，并添加防火墙作为托管设备。然后，Panorama 可以将防火墙分配至相应的设备组和模板，以便您可以使用 Panorama 集中配置和管理防火墙。

©2024 Palo Alto Networks, Inc.

在这种情况下，您必须在 Panorama 上生成 VM 身份验证密钥，并将该密钥包含在用于引导的 init-cfg.txt 文件中。通过 VM 身份验证密钥，Panorama 可以对新引导的 VM 系列防火墙进行身份验证。引导数据包必须包含。

- 在 /config 目录中，包含 Panorama IP 地址的 init-cfg.txt 文件
- 在 /license 目录中，VM 身份验证密钥位于名为 authcodes 的文件中。

  根据不同的情况，密钥的生命周期在 1 小时到 8760 小时（1 年）不等。指定的时间到期后，密钥将会过期；如果 VM 系列防火墙的连接请求中没有有效的身份验证密钥，Panorama 将不会对其进行注册。

STEP 1 | 使用在 Google Cloud Platform 上引导 VM 系列防火墙所需的文件夹设置Google 存储桶。您可以为这些文件夹使用现有的引导数据包或创建新的引导数据包。

STEP 2 | 编辑 `init-cfg.txt` 示例文件中的值，以根据您的环境自定义文件。

防火墙模板包含 `init-cfg.txt` 示例文件。

参数	值	注释
type	dhcp-client	
主机名：	<pa-vm>	您在准备主机项目时分配的可选名称。只有在特定主机为必需且 dhcp-send-hostname 为“否”时才需要。
vm-auth-key	<vmauthkey>	在添加防火墙作为托管设备之前，Panorama 必须验证的密钥。请参阅在 Panorama 上生成 VM 身份验证密钥。
panorama-	<panorama-ip>	在配置适用于 GCP 的 Panorama 插件以保护自动扩展部署中配置的 Panorama 管理设备的 IP 地址。
tplname	<template-stack-name>	在配置适用于 GCP 的 Panorama 插件以保护自动扩展部署中创建的模板堆栈。
dgname	<dg-name>	您在适用于 GCP 的 Panorama 插件中创建的设备组的名称。
dns-primary		主 DNS 服务器。
dns-secondary		辅助 DNS 服务器。

©2024 Palo Alto Networks, Inc.

参数	值	注释
dhcp-send-hostname	是	保持原样。
dhcp-send-client-id	是	保持原样。
dhcp-accept-server-hostname	是	保持原样。
dhcp-accept-server-domain	是	保持原样。

STEP 3 | 将您编辑的 `init-cfg.txt` 文件上传到引导数据包中的 `/config` 文件夹。

STEP 4 | 如果您使用 BYOL，请创建一个名为 `authcodes` 的文本文件（无扩展名），添加授权代码，然后将该文件上传到 `/license` 文件夹。

部署 GCP 自动扩展模板

- 关于自动扩展模板
- 部署防火墙模板
- 准备服务项目
- 配置共享 VPC
- 部署应用程序模板
- 登录新应用程序
- GKE 服务模板示例

关于自动扩展模板

可从 https://github.com/PaloAltoNetworks/GCP-AutoScaling 下载 Palo Alto Networks 自动扩展模板。该 Zip 文件包含分别用于防火墙和应用程序模板的 Zip 文件。每个 Zip 文件都是一个包含几个文件的模板目录，但您只需要编辑 YAML 文件。

- 防火墙模板
- 应用程序模板

防火墙模板

防火墙目录文件可创建 VM 系列防火墙和其他部署资源。它们可为 VM 系列防火墙创建新网络和常见子网：管理、不可信和可信。此外，它们还可部署 Cloud Pub/Sub 消息服务，以将信息从 GCP 中继到适用于 GCP 的 Panorama 插件。使用此基础架构，该插件可利用动态地址组对路由到 GCP 上运行的服务的入站流量应用安全策略，并使用自动扩展指标部署 VM 系列防火墙，以满足应用程序工作负载资源的增长需求，或清除不再需要的防火墙。

要配置负载均衡器，请编辑外部应用程序负载均衡器 (ALB) 或网络负载均衡器 (NLB) 的 `.yaml` 文件。

©2024 Palo Alto Networks, Inc.

- **ALB**（HTTP 外部负载均衡器）

  要自定义 ALB，请编辑 `vm-series-fw-alb.yaml`。

  HTTP 外部负载均衡器是基于代理的负载均衡器，可对来自 Internet 的入站流量执行 SNAT 和 DNAT。HTTP 负载均衡器旨在仅支持 80 和 8080 TCP 端口。

  要在负载均衡器夹层式架构中使用 HTTP 负载均衡器支持多个应用程序，我们可以使用 GCP HTTP 负载均衡器 *urlMap* 和 *namedPort* 将不同的 URL 映射到负载均衡器中的不同端口。反过来，VM 系列防火墙可以将端口转换为不同的应用程序，每个应用程序都由一个内部负载均衡器表示。

- **NLB**（TCP 负载均衡器）

  要自定义 NLB，请编辑 `vm-series-fw-nlb.yaml`。

  TCP 负载均衡器是基于非代理的负载均衡器，这意味着它不能对来自 Internet 的入站流量执行 NATing。

  GCP 中的 TCP 负载均衡器允许通过任意端口添加多个前端 IP 地址，从而可以支持多个应用程序。

  TCP 负载均衡器的另一个优点是已保留原始客户端 IP 地址，非常适合用于某些应用程序。

应用程序模板

应用程序目录可提供一个应用程序示例。您可以配置和部署内部负载均衡器 (ILB) 以使应用程序服务器能够订阅 Pub/Sub 服务，并与 VM 系列防火墙和 Panorama 上的 GCP 插件进行通信。

要自定义应用程序模板，请编辑 `apps.yaml`，如部署防火墙模板和应用程序模板中所述。

部署防火墙模板

从主机项目编辑防火墙模板。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2024 Palo Alto Networks, Inc.

STEP 1 | 编辑 `vm-series-fw-nlb.yaml` 或 `vm-series-fw-alb.yaml` 环境变量以反映您的云环境。

此工作流程中的示例适用于 NLB。有关模板参数的进一步说明，请参阅 vm-series-fw-nlb.yaml 和vm-series-fw-alb.yaml。

```
properties:     region: us-east1     zones:     -us-east1-b     #
 Do not modify the lb-type field.     lb-type: nlb     cloud-nat:
 yes     forwarding-rule-port:80
```

```
# Only one app is allowed     urlPath-namedPort-maps:     -
 appName: app1
```

```
# ssh key PUBLIC:     - optional
```

自动扩展防火墙模板要求您输入一个值，用单引号括起来，并在密钥前加上 **admin:**，后跟一个空格。这与 Google Marketplace 模板使用的约定相同，如 SSH 密钥对中所述。例如：

```
    sshkey: 'admin: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDe0gJHd8okxPGWXsmdTdcZBJNI6ONT/NSz6INs2CNtKW
[redacted]
oTKXL8t0SRnOKaKV73NR5KnfpsNfwGxG8aQtEkeMCZIxX+6WOnRf/N4K3
yourname@[redacted].paloaltonetworks.local'
```

```
    bootstrap-bucket: bootstrap-autoscale
```

```
    image: vmseries-byol-814     machine-type: n1-standard-4
```

对于服务帐户，提供您先前（步骤 3）创建的主机项目服务帐户的电子邮件地址。

```
     service-account: sa-pan@gcp-autoscale-
kk.iam.gserviceaccount.com
```

fw-instance-tag 值将是部署中的托管实例组名称。

```
     fw-instance-tag: vm-series-fw
```

选择一个指标以进行自动扩展。可能的值为：panSessionActive、panSessionUtilization、DataPlaneCPUUtilizationPct、DataPlanePacketBufferUtilization 或 panSessionUtilization。

```
metric: custom.googleapis.com/VMSeries/panSessionActive
```


©2024 Palo Alto Networks, Inc.

```
max-size:2 min-size:1 target-type:GAUGE util-target:100
```

```
# Greenfield deployment mgmt-network-cidr:172.22.2.0/24 untrust-
network-cidr:172.22.1.0/24 trust-network-cidr:172.22.3.0/24 mgmt-
network-access-source-range: - 199.167.54.229/32 - 199.167.52.5/32
 mgmt-network-access-ports: - 22 - 443
```

STEP 2 | 部署防火墙模板。

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

记下部署后 CLI 打印的输出：子网名称、部署名称和 Panorama Pub/Sub 主题名称。您需要使用这些值配置共享 VPC 和应用程序模板部署。

必须在适用于 GCP 自动扩展定义的 Panorama 插件中配置防火墙部署名称。

准备服务项目

为应用程序创建单独的服务项目，或选择现有项目。

要了解有关共享 VPC 中主机项目和服务项目的更多信息，请参阅共享 VPC 概述，并查看管理员和 IAM 角色。主机项目管理员必须具有适当的角色才能设置共享 VPC，并使应用程序项目成为主机项目的服务项目。请参阅设置共享 VPC 中的说明。

©2024 Palo Alto Networks, Inc.

STEP 1 | 从 GCP 控制台或 CLI 启用服务项目 API。

所需的 API 是：

- Cloud Deployment Manager API
- Cloud Pub/Sub API
- 计算引擎 API

从 **GCP** 控制台启用 **API**

1. 选择服务项目，然后从 Navigation（导航）菜单选择 **APIs & Services**（**API** 和服务）。
2. 搜索并查看所需的每个 API。
3. **ENABLE**（启用）所有不显示“API 已启用”状态的 API。

从 **CLI** 控制台启用 **API**

1. 在 CLI 中，查看您的配置以确保位于正确的项目中。

```
gcloud config list
```

如果不是，请按如下所示设置项目：

```
gcloud config set project <project-name>
```

2. 发出以下命令以启用所需的 API。

```
gcloud services enable deploymentmanager.googleapis.com gcloud
 services enable pubsub.googleapis.com gcloud services enable
 compute.googleapis.com
```

3. 确认已启用所需的 API。

```
gcloud services list --enabled
```

STEP 2 | 使应用程序项目成为主机项目的服务项目。

添加服务/应用程序项目管理员的服务帐户作为具有以下角色的主机项目成员：

- 计算网络用户
- Pub/Sub 管理员

STEP 3 | 选择 VPC 配置。

- 如果服务项目将共享主机项目中的网络，请继续配置共享 VPC。
- 如果服务项目本身有用于应用程序部署的 VPC 网络，请继续配置对等 VPC。

©2024 Palo Alto Networks, Inc.

配置共享 VPC

在主机项目中部署防火墙模板后，请配置支持应用程序的服务项目。拥有共享 VPC 凭据的管理员可从主机项目执行这些任务。要了解有关共享 VPC 上下文中主机项目和服务项目的更多信息，请参阅共享 VPC 概述。

STEP 1 | 使用部署防火墙模板时创建的可信 VPC 创建共享 VPC。

设置主机（防火墙）项目的共享 VPC：

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

STEP 2 | 将服务/应用程序项目附加到主机项目。

```
gcloud compute shared-vpc associated-projects add
[SERVICE_PROJECT_ID]--host-project [HOST_PROJECT_ID]
```

其他选项可用于仅共享特定子网，而不共享主机项目中的所有子网。

STEP 3 | 如果要使用应用程序模板示例部署应用程序，请继续部署应用程序模板。

如果已部署应用程序，并且要在自动扩展部署中保护应用程序，请转至手动将应用程序登录到现有的自动扩展部署。

如果已在 GKE 集群中部署服务，请继续在共享 VPC 中登录 GKE 集群。

配置对等 VPC

必须在两个 VPC 之间建立 VPC 网络对等连接。如果 VPC 在两个不同的项目中，则必须在两个项目中创建连接。

STEP 1 | 在主机项目中，将防火墙部署的可信 VPC 网络与应用程序 VPC 进行对等。

```
gcloud beta compute networks peerings create [PEERING-NAME] \
     --network=[MY-LOCAL-NETWORK] \     --peer-project [SERVICE-
PROJECT-ID] \     --peer-network [PEER-NETWORK-NAME] \    [--
import-custom-routes] \    [--export-custom-routes]
```

STEP 2 | 在服务项目中，将应用程序部署的可信 VPC 网络与防火墙部署的可信 VPC 网络进行对等。

```
gcloud beta compute networks peerings create [PEERING-NAME] \
     --network=[MY-LOCAL-NETWORK] \     --peer-project [HOST-
PROJECT-ID] \     --peer-network [PEER-NETWORK-NAME] \    [--
import-custom-routes] \     [--export-custom-routes]
```

STEP 3 | 如果要使用应用程序模板示例部署应用程序，请继续部署应用程序模板。

如果已部署应用程序，并且要在自动扩展部署中保护应用程序，请转至手动将应用程序登录到现有的自动扩展部署。

如果已在 GKE 集群中部署服务，请继续在对等 VPC 中登录 GKE 集群。

©2024 Palo Alto Networks, Inc.

部署应用程序模板

服务项目管理员从服务项目部署应用程序模板。

STEP 1 | 创建单独的应用程序项目（服务项目）来署应用程序（参阅准备服务项目）。

STEP 2 | 准备 `apps.yaml` 文件，如 apps.yaml 中所述。

STEP 3 | 使用应用程序模板部署新应用程序，并为命名端口定义标签。

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

继续阅读在适用于 GCP 的 Panorama 插件上查看登录的应用程序。

登录新应用程序

使用应用程序模板部署应用程序时，它负责与主机项目建立连接。您可以使用应用程序模板来保护未部署的应用程序，前提是已使用准备服务项目中所述的功能在服务项目中部署这些应用程序模板。

- 手动将应用程序登录到现有的自动扩展部署
- 登录 GKE 集群

手动将应用程序登录到现有的自动扩展部署

要保护使用外部负载均衡器部署的应用程序和自动扩展的 VM 系列防火墙部署，请遵循以下步骤。对于登录的每个应用程序，必须提供应用程序名称、命名端口和路径。

STEP 1 | 准备将新的命名端口和 URL 路径添加到在部署防火墙模板时创建的 HTTP 外部负载均衡器。

STEP 2 | 使用其他服务名称和端口值更新所有实例组命名端口。以下示例登录应用程序 `app2` 和 `app3`。

```
gcloud compute instance-groups set-named-ports fw-template2-fw-igm-
us-east1-b --zone us-east1-b --named-ports=app1:80,app2:81,app3:82
 gcloud compute instance-groups set-named-ports fw-
template2-fw-igm-us-east1-c --zone us-east1-c --named-
ports=app1:80,app2:81,app3:82
```

STEP 3 | 创建新的 http-health-check。

```
gcloud compute backend-services create fw-template2-backend-app3 --
protocol="HTTP" --port-name=app3 --http-health-checks=fw-template2-
healthcheck-app3 --load-balancing-scheme="EXTERNAL" --global
```


©2024 Palo Alto Networks, Inc.

STEP 4 | 使用先前在 HTTP 外部负载均衡器上创建的端口名称创建新的后端服务。

```
gcloud compute backend-services create fw-template2-backend-app3 --
protocol="HTTP" --port-name=app3 --http-health-checks=fw-template2-
healthcheck-app3 --load-balancing-scheme="EXTERNAL" --global
```

检查以查看新的后端服务是否可见。

```
gcloud compute backend-services list
```

STEP 5 | 编辑 URL 映射并添加新的路径规则。例如：

```
- paths:     - /app3     - /app3/*service:     https://
www.googleapis.com/compute/v1/projects/<project-name>/global/
backendServices/fw-template2-backend-app3
```

```
gcloud compute url-maps edit fw-template2-ext-loadbalancer
```

STEP 6 | 要使用 VM 系列防火墙保护此应用程序，请通过 gcloud CLI 手动触发 Pub/Sub 消息。这会将消息发送到在防火墙模板中创建的主题。

```
gcloud pubsub topics publish   projects/topics/hj-asg-891ca3-gcp-
pavmqa-panorama-apps-deployment   --attribute ilb-ip=172.22.9.34,
     app-deployment-name=hj-asg-891ca3-app1,     ilb-port=80,
     named-port=81,     network-cidr=172.22.9.0/24,     fw-
deployment-name=hj-asg-891ca3,     host-project=gcp-pavmqa,
     type=ADD-APP   --message "ADD-APP"
```

STEP 7 | 在适用于 GCP 的 Panorama 插件上查看登录的应用程序.

STEP 8 | （可选）要更新应用程序属性，例如 ilb-ip、ilb-port 或 named-port，请发出 pubsub 命令：

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment   --attribute
 ilb-ip=172.22.9.34,     app-deployment-name=hj-asg-891ca3-
app1,     ilb-port=80,     named-port=81,     network-
cidr=172.22.9.0/24,     fw-deployment-name=hj-asg-891ca3,     host-
project=gcp-pavmqa,     type=UPDATE-APP   --message "UPDATE-APP"
```

STEP 9 | （可选）要停止保护应用程序，请发出以下命令：

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment   --attribute ilb-
ip=172.22.3.20,app-deployment-name=fw-templ-3-app-1,     ilb-
port=80,     named-port=80,     fw-deployment-name=hj-asg-891ca3,
     type=DEL-APP   --message "DEL-APP"
```


©2024 Palo Alto Networks, Inc.

登录 **GKE** 集群

要登录私有 GKE 集群，适用于 Panorama 的 GCP 插件需要以下信息。

- 在 GCP 中，将集群的 ELB 前端向 GKE 服务公开，以便 VM 系列防火墙可以获取服务的命名端口信息。
- 集群 API 服务器地址。
- 集群在其中部署的服务的服务帐户凭据的格式为 JSON。

GKE 集群名称不得超过 *24* 个字符。这可确保如果在对等 *VPC* 配置中部署自动扩展，则静态路由名称不超过 *31* 个字符。

- 在共享 VPC 中登录 GKE 集群
- 在对等 VPC 中登录 GKE 集群
- 在适用于 GCP 的 Panorama 插件上查看登录的应用程序
- 从 CLI 查看部署状态

在共享 *VPC* 中登录 *GKE* 集群

要登录 GKE 集群，必须与服务项目共享主机项目可信网络 VPC。请参阅配置共享 VPC。

出于安全原因，在自动扩展部署中仅应使用专用集群。请参阅创建专用集群。

STEP 1 | 设置主机项目 ID。

```
gcloud config set project [HOST_PROJECT_ID]
```

STEP 2 | （可选）设置集群的计算区域或地区。

如果集群是区域集群，请输入以下内容：

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

如果集群是地区集群，请输入以下内容：

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | 在主机项目中，更新可信 VPC 子网中的辅助范围。

```
gcloud compute networks subnets update [TRUST_SUBNETWORK_NAME]   --
add-secondary-ranges   [PODS_IP_RANGE_NAME] = [POD_RANGE_CIDR],
   [SERVICE_IP_RANGE_NAME]=[SERVICE_RANGE_CIDR]
```

Pod 和服务 *IP* 范围必须在以下范围内：*10.0.0.0/8*、*172.16.0.0/12* 或 *192.168.0.0/16*，并且不能与子网中的现有 *IP* 范围冲突。

©2024 Palo Alto Networks, Inc.

STEP 4 | 在服务项目中，在共享 VPC 中创建专用集群。

1. 设置服务项目 ID。

```
gcloud config set project [SERVicE_PROJECT_ID]
```

2. 在共享 VPC 中创建专用集群。

```
gcloud container clusters create  [CLUSTER_NAME]   --project
 [SERVICE_PROJECT_ID]   --zone=[ZONE_NAME]   --enable-
ip-alias   --enable-private-nodes   --network projects/
[HOST_PROJECT_ID]/global/networks/[NETWORK_NAME]   --
subnetwork projects/[HOST_PROJECT_ID]/regions/[REGION_NAME] /
subnetworks/[TRUST_SUBNETWORK_NAME]   --cluster-secondary-
range-name=[PODS_IP_RANGE_NAME]   --services-secondary-
range-name=[SERVICE_IP_RANGE_NAME]   --master-ipv4-
cidr=[MASTER_IPV4_CIDR]   --enable-master-authorized-networks
   --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
   [MY_MANAGEMENT_IP/32]
```

STEP 5 | 检查当前集群上下文。

```
kubectl config current-context
```

STEP 6 | 检查所有集群上下文。

```
kubectl config get-context
```

STEP 7 | 更改为另一个集群。

```
kubectl config use-context [CONTEXT_NAME]
```

如果您在 GCP 控制台中创建集群，将生成 kubeconfig 条目：

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 8 | 在 `.yaml` 文件中创建集群角色，例如 `gke_cluster_role.yaml`。

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind:ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 9 | 应用集群角色。

```
kubectl apply -f gke_cluster_role.yaml
```

 ©2024 Palo Alto Networks, Inc.

STEP 10 | 在 `.yaml` 文件中创建集群角色绑定，例如 `gke_cluster_role_binding.yaml`。

```
kind:ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:   -
 kind:ServiceAccount     name: [SERVICEACCOUNT_NAME]     namespace:
 default roleRef:   kind:ClusterRole   name: gke-plugin-role
   apiGroup: rbac.authorization.k8s.io
```

STEP 11 | 应用集群角色绑定。

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 12 | 创建服务帐户。

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 13 | 以 JSON 格式导出服务帐户机密令牌。

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json > [FILE_NAME].json
```

STEP 14 | 获取 API 服务器地址。

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

STEP 15 | 在适用于 GCP 的 Panorama 插件上，添加服务帐户信息。

选择 **Panorama** > **Google Cloud Platform** > **Setup**（设置）。

命名凭据，输入说明，然后输入步骤 14 中的 **API server address**（**API** 服务器地址）；对于 **GKE** 服务帐户凭据，请上传在步骤 13 中导出的 JSON 文件。

添加服务帐户凭据后，您可以从 Panorama 命令行验证凭据（不能从 Web 界面验证）：

```
request plugins gcp validate-service-account gke_service_account
 <svc-acct-credential-name>
```

 ©2024 Palo Alto Networks, Inc.

STEP 16 | 在适用于 GCP 的 Panorama 插件上设置自动扩展。

1. 在 Panorama 上下文中，展开 Google Cloud Platform，选择 AutoScaling（自动扩展），然后单击 **Add**（添加）。
2. 提供 **Firewall Deployment Name**（防火墙部署名称）和部署的可选说明。
3. 对于 **GCP Service Account Credential**（**GCP** 服务帐户凭据），请提供在 准备主机项目和所需的服务帐户 中（步骤 4）创建的 GCP 服务帐户名称。
4. 选择在配置 Panorama 插件时创建的设备组和模板堆栈。
5. 禁用 **License Management Only**（仅限许可证管理）以确保流量安全。
6. 输入确切的 **GKE Cluster Name**（**GKE** 集群名称）。
7. （可选）输入 GKE 集群的 **Description**（说明）。
8. 输入 GKE 集群的 **Network CIDR**（网络 **CIDR**）。
9. 选择与 GKE 集群对应的 **GKE Service Account**（**GKE** 服务帐户）。

STEP 17 | 提交更改。

STEP 18 | （可选）根据使用 GKE 服务模板示例创建和部署服务模板，或者在 GCP 控制台中部署 GKE 服务。

在对等 *VPC* 中登录 *GKE* 集群

要登录 GKE 集群，您必须在主机项目中创建服务 VPC 并将其与防火墙可信网络进行对等，如配置对等 VPC 中所述。

出于安全原因，在自动扩展部署中仅应使用专用集群。请参阅创建专用集群。

STEP 1 | 设置项目 ID。

```
gcloud config set project [PROJECT_ID]
```

STEP 2 | 设置集群的计算区域或地区。

如果集群是区域集群，请输入以下内容：

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

如果集群是地区集群，请输入以下内容：

```
gcloud config set compute/region [COMPUTE_REGION]
```

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 使用 Pod 和服务的辅助 IP 地址范围更新服务项目 VPC 网络。

```
gcloud compute networks subnets update [GKE_PEERED_VPC_SUBNETWORK]
 --region=[REGION] --add-secondary-ranges PODS_IP_RANGE_NAME=[ip
 cidr], SERVICE_IP_RANGE_NAME=[ip cidr]
```

STEP 4 | 启用 Cloud NAT。

部署专用集群时需要 *Cloud NAT*。

```
gcloud compute routers create [ROUTER_NAME]   --network
 [NETWORK_NAME]   --region [REGION_NAME]
```

```
gcloud compute routers nats create [NAT_CONFIG_NAME]   --router-
region [REGION_NAME]   --router [ROUTER_NAME]   --nat-all-subnet-
ip-ranges   --auto-allocate-nat-external-ip
```

STEP 5 | 在服务 VPC 中创建一个新的专用集群。

```
gcloud container clusters create [CLUSTER_NAME]   --
project [SERVICE_PROJECT_ID]   --zone=[ZONE_NAME]   --
enable-ip-alias   --network [NETWORK_NAME]   --subnetwork
 [SUBNETWORK_NAME]   --enable-private-nodes   --cluster-
secondary-range-name=[PODS_IP_RANGE_NAME]   --services-
secondary-range-name=[SERVICE_IP_RANGE_NAME]   --master-ipv4-
cidr=[MASTER_IPV4_CIDR]   --enable-master-authorized-networks
   --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
   [MY_MANAGEMENT_IP/32]
```

STEP 6 | 检查当前集群上下文。

```
kubectl config current-context
```

STEP 7 | 检查所有集群上下文。

```
kubectl config get-context
```

STEP 8 | 更改为另一个集群。

```
kubectl config use-context [CONTEXT_NAME]
```

如果您在 GCP 控制台中创建集群，将生成 kubeconfig 条目：

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 在 `.yaml` 文件中创建集群角色，例如 `gke_cluster_role.yaml`。

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind:ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 10 | 应用集群角色。

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 11 | 在 `.yaml` 文件中创建集群角色绑定，例如 `gke_cluster_role_binding.yaml`。

```
kind:ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:   -
 kind:ServiceAccount     name: [SERVICEACCOUNT_NAME]     namespace:
 default roleRef:   kind:ClusterRole   name: gke-plugin-role
   apiGroup: rbac.authorization.k8s.io
```

STEP 12 | 应用集群角色绑定。

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 13 | 创建服务帐户。

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 14 | 以 JSON 格式导出服务帐户机密令牌。

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json >[FILE_NAME].json
```

STEP 15 | 获取 API 服务器地址。

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

 ©2024 Palo Alto Networks, Inc.

STEP 16 | 在适用于 GCP 的 Panorama 插件上，添加服务帐户信息。

选择 **Panorama** > **Google Cloud Platform** > **Setup**（设置）。

命名凭据，并输入步骤 15 中的 **API server address**（**API** 服务器地址），然后上传在步骤 14 中导出的 JSON 文件。

添加服务帐户凭据后，您可以从 Panorama 命令行验证凭据：

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

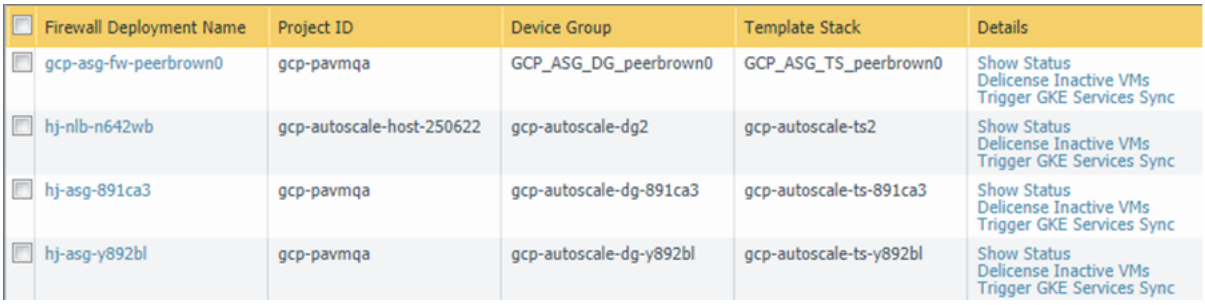
STEP 17 | 在适用于 GCP 的 Panorama 插件上设置自动扩展。

1. 在 Panorama 上下文中，展开 Google Cloud Platform，选择 AutoScaling（自动扩展），然后单击 **Add**（添加）。
2. 提供 **Firewall Deployment Name**（防火墙部署名称）和部署的可选说明。
3. 对于 **GCP Service Account Credential**（**GCP** 服务帐户凭据），请提供步骤 16 中的 GCP 服务帐户名称。
4. 选择在配置 Panorama 插件时创建的设备组和模板堆栈。
5. 禁用 **License Management Only**（仅限许可证管理）以确保流量安全。
6. 输入确切的 **GKE Cluster Name**（**GKE** 集群名称）。
7. （可选）输入 GKE 集群的 **Description**（说明）。
8. 输入 GKE 集群的 **Network CIDR**（网络 **CIDR**）。
9. 选择与 GKE 集群对应的 **GKE Service Account**（**GKE** 服务帐户）。

STEP 18 | （可选）在服务项目中，根据使用 GKE 服务模板示例创建和部署 GKE 模板，或者使用 GCP 控制台部署 GKE 服务。登录 GKE 集群

在适用于 *GCP* 的 *Panorama* 插件上查看登录的应用程序

选择 **Panorama** > **Google Cloud Platform** > **Autoscaling**（自动扩展），以查看登录的应用程序。**Details**（详细信息）列只有在您拥有登录的应用程序时才可见。

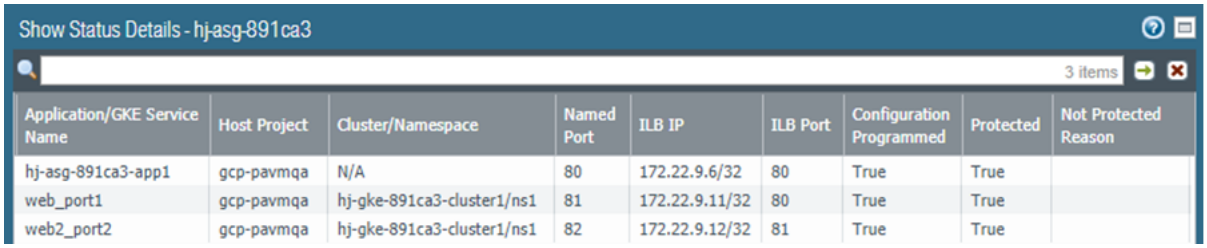


Firewall Deployment Name	Project ID	Device Group	Template Stack	Details
gcp-asg-fw-peerbrown0	gcp-pavmqa	GCP_ASG_DG_peerbrown0	GCP_ASG_TS_peerbrown0	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-nlb-n642wb	gcp-autoscale-host-250622	gcp-autoscale-dg2	gcp-autoscale-ts2	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-891ca3	gcp-pavmqa	gcp-autoscale-dg-891ca3	gcp-autoscale-ts-891ca3	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-y892bl	gcp-pavmqa	gcp-autoscale-dg-y892bl	gcp-autoscale-ts-y892bl	Show Status Delicense Inactive VMs Trigger GKE Services Sync

Details（详细信息）列中的每个链接都将触发一个操作。

©2024 Palo Alto Networks, Inc.

- 显示状态 — 查看登录到 GCP VM 系列防火墙部署的应用程序的详细信息。



Application/GKE Service Name	Host Project	Cluster/Namespace	Named Port	ILB IP	ILB Port	Configuration Programmed	Protected	Not Protected Reason
hj-asg-891ca3-app1	gcp-pavmqa	N/A	80	172.22.9.6/32	80	True	True	
web_port1	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	81	172.22.9.11/32	80	True	True	
web2_port2	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	82	172.22.9.12/32	81	True	True	

以下字段会显示从所选部署获取的信息。您已在 Pub/Sub 消息中或通过 GKE 集群服务轮询指定这些值。

- **Application/GKE Service Name**（应用程序/**GKE** 服务名称）— 应用程序部署名称，或 GKE 服务的名称。
- **Host Project**（主机项目）— 主机项目的名称。
- **Cluster/Namespace**（集群/命名空间）— GKE 集群名称，后跟命名空间，例如 **`mycluster/namespace9`**。
- **Named Port**（命名端口）— 分配给服务的命名端口的端口。
- **ILB IP** — ILB IP 地址。
- **ILB Port**（**ILB** 端口）— ILB 端口号。

  对于自动扩展应用程序，此属性是 `apps.yaml` 中的 **`ilb-port`**。

  对于保护 GKE 集群，此值是 GKE 集群的端口号，如用于集群中部署服务的 `.yaml` 文件中所指定。
- **Configuration Programmed**（配置编程）— 如果存在 NAT 规则，则为 True；否则为 False。
- **Protected**（保护）— 如果成功登录应用程序，则为 True；否则为 False。如果为 False，请参阅 **Not Protected Reason**（未保护原因）列以获取说明。
- **Not Protected Reason**（未保护原因）— 如果 **Protected**（保护）为 False，则会显示未保护应用程序的原因。一些常见的原因是：
  - **Configuration Programmed**（配置编程）— 如果存在 NAT 规则，则为 True；否则为 False。
  - **Protected**（保护）— 如果成功登录应用程序，则为 True；否则为 False。如果为 False，请参阅 **Not Protected Reason**（未保护原因）列以获取说明。
  - **Not Protected Reason**（未保护原因）— 如果 **Protected**（保护）为 False，则会显示未保护应用程序的原因。一些常见的原因是：
    - 在 GKE 集群中部署了 UDP 服务。
    - 指定了已使用的命名端口。一个应用程序只能侦听一个特定命名端口。
    - 已选择 **License management only**（仅限许可证管理）选项，因此，我们无法对配置进行编程。
    - 找不到与 GKE 服务匹配的标签。

©2024 Palo Alto Networks, Inc.

- 解除许可非活动 **VM** — 回答 **Yes**（是）以触发非活动 VM 的解除许可功能。
- 触发 **GKE** 服务同步 — 回答 **Yes**（是）以轮询集群中运行的服务，并在必要时对 NAT、地址、服务对象和静态路由进行编程。默认情况下，Panorama 将在上一次轮询完成后 10 分钟自动进行轮询。

从 *CLI* 查看部署状态

您可以使用 Panorama CLI 管理部署的应用程序。命令行操作与在适用于 GCP 的 Panorama 插件上查看登录的应用程序中所述的操作类似。在以下命令中，**autoscaling_name** 是您在自动扩展配置中输入的防火墙部署名称。

- 列出登录（保护）的应用程序。

```
show plugins gcp show-protected-apps autoscaling_name <fw-deployment-name>
```

- 在指定的部署中触发防火墙的解除许可功能。

```
request plugins gcp force-delicensing autoscaling_name <fw-deployment-name>
```

- 对于 GKE 部署，强制插件读取 Pub/Sub 消息，并同步根据 Pub/Sub 消息编程的 NAT 规则。

```
request plugins gcp gke-service-discovery autoscaling_name <fw-deployment-name>
```

适用于 GCP 的自动扩展模板中的参数

您可以从 https://github.com/PaloAltoNetworks/GCP-AutoScaling 下载模板 `.zip` 文件。该 `.zip` 文件包含支持网络负载均衡器和应用程序负载均衡器配置的防火墙模板，以及应用程序模板的目录。

模板 YAML 文件具有以下常规格式：

```
#Copyright and license information     :     :
 imports:                        <do not change>     :     : resources:
     -name: vm-series-fw         <do not change>     -type:vm-series-
fw.py    <do not change
    -properties:
    :
    :
outputs:                       <do not change>     :     :
```

在所有 `.yaml` 文件中，您可以为部署自定义 `resources` 属性。请不要在 `imports` 或 `outputs` 部分中进行任何更改。

- 防火墙模板
- 应用程序模板

©2024 Palo Alto Networks, Inc.

防火墙模板

以下各节详细介绍 NLB 和 ALB `.yaml` 文件中的参数。

- vm-series-fw-nlb.yaml
- vm-series-fw-alb.yaml

vm-series-fw-nlb.yaml

在 `vm-series-fw-nlb.yaml` 模板中，编辑 `-properties`。

参数	示例值	注释
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	如果可以，请按如下所示列出多个区域： zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	nlb	请勿更改。
cloud-nat	是	请勿更改。
forwarding-rule-port	80	80 或 8080
urlPath-namedPort-maps-appname	`urlPath-namedPort-maps -MyApplication`	输入应用程序名称。
sshkey	'admin:ssh-rsa <PASTE KEY>'	查看 SSH 密钥对。用单引号括起来，键入 **admin:**，后跟一个空格，然后粘贴您的密钥。这与 Google Marketplace 模板使用的约定相同。
bootstrap-bucket	bootstrap-autoscale	包含引导文件的 GCP 存储桶的名称。
image	vm-series-byol-814	Google Marketplace 目前可提供的 BYOL 映像。 如果使用 PAYG 或其他许可证模型，则映像可能会有所不同。

©2024 Palo Alto Networks, Inc.

参数	示例值	注释
machine-type	n1-standard-4	n1-standard-4 是 BYOL 的默认值。 如果您的许可证允许，则可以使用 对 VM 系列的最低系统要求 中的任何计算机类型。
service-account		主机项目的唯一服务帐户名称。
fw-instance-tag	vm-series-fw	您在 GCP 中提供的实例标记。
metric	custom.googleapis.com/VMSeries/panSessionActive	VM 系列的自定义 API 路径，以及所选自动缩放指标。 仅提供以下指标之一。 `panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	GAUGE 是目前唯一的有效值。
util-target	100	
要部署 VM 系列防火墙，您需要适用于防火墙的管理、不可信和可信接口的专用网络和子网。填写有关绿色字段部署（配置模板以创建新网络）或棕色字段部署（使用现有网络）的信息。同时，请确保删除或注释掉未使用的网络部署参数。		
绿色字段部署：输入值可为防火墙创建管理、不可信和可信网络和子网。		
mgmt-network-cidr	172.22.2.0/24	
untrust-network-cidr	172.22.1.0/24	
trust-network-cidr	172.22.3.0/24	

©2024 Palo Alto Networks, Inc.

参数	示例值	注释
mgmt-network-access-source-range- <permitted-ip-range>	`mgmt-network-access-source-range - <permitted-ip-range-1> - <permitted-ip-range-2>`	
mgmt-network-access-ports- <port-number>	`mgmt-network-access-ports - 22 - 443`	
棕色字段部署：输入每个现有网络或子网的名称。		
mgmt-network	my-mgmt-network	
mgmt-subnet	my-mgmt-subnet	
trust-network	my-trust-network	
trust-subnet	my-trust-subnet	
untrust-network	my-untrust-network	
untrust-subnet	my-untrust-subnet	

vm-series-fw-alb.yaml

在 `vm-series-fw-alb.yaml` 模板中，编辑 `-properties`。

参数	示例值	注释
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	如果可以，请按如下所示列出多个区域： zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	alb	请勿更改。
cloud-nat	是	请勿更改。
forwarding-rule-port	80	80
connection-draining-timeout	300	超时值（以秒为单位）。

©2024 Palo Alto Networks, Inc.

参数	示例值	注释
`urlPath-namedPort-maps: - appname: namedPort: urlMapPaths: - '/app1' - '/app1/*'`	`urlPath-namedPort-maps: - appName: app1 namedPort:80 urlMapPaths: - '/app1' - '/app1/*' - appName: app2 namedPort:81 urlMapPaths: - '/app2' - '/app2/*'`	列出应用程序和相应的命名端口。
sshkey	'admin:ssh-rsa <PASTE KEY>'	查看 SSH 密钥对。用单引号括起来，键入 **admin:**，后跟一个空格，然后粘贴您的密钥。这与 Google Marketplace 模板使用的约定相同。
bootstrap-bucket	bootstrap-bucket-name	包含引导文件的 GCP 存储桶的名称。
image	vm-series-byol-814	Google Marketplace 目前可提供的 BYOL 映像。 如果使用 PAYG 或其他许可证模型，则映像可能会有所不同。
machine-type	n1-standard-4	n1-standard-4 是 BYOL 的默认值。 如果您的许可证允许，则可以使用 对 VM 系列的最低系统要求 中的任何计算机类型。
service-account	服务项目的唯一服务帐户名称。	
fw-instance-tag	vm-series-fw	您在 GCP 中提供的实例标记。
metric	custom.googleapis.com/VMSeries/panSessionActive	VM 系列的自定义 API 路径，以及所选自动缩放指标。 仅提供以下指标之一。 `panSessionActive panSessionUtilization DataPlaneCPUUtilizationP`

©2024 Palo Alto Networks, Inc.

参数	示例值	注释
		`ct DataPlanePacketBuf ferUtilization panSes sionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	GAUGE 是目前唯一的有效值。
util-target	100	输入自动扩展的目标利用率目标值。
绿色字段部署：输入值可为防火墙创建管理、不可信和可信网络和子网。		
mgmt-network-cidr	192.168.12.0/24	
untrust-network-cidr	192.168.11.0/24	
trust-network-cidr	192.168.11.0/24	
mgmt-network-access-source-range- <permitted-ip-range>	`mgmt-network-access-source-range- <permitted-ip-range-1>- <permitted-ip-range-2>`	
mgmt-network-access-ports-<port-number>	`mgmt-network-access-ports- 22- 443`	
棕色字段部署：输入每个现有网络或子网的名称。		
mgmt-network	existing-vpc-mgmt	
mgmt-subnet	existing-subnet-mgmt	
trust-network	existing-vpc-trust	
trust-subnet	existing-subnet-trust	
untrust-network	existing-vpc-untrust	
untrust-subnet	existing-subnet-untrust	

应用程序模板
apps.yaml

应用程序模板在主机项目（包含 VM 系列防火墙）和服务项目（包含防火墙部署保护的应用程序或服务）之间创建连接。

©2024 Palo Alto Networks, Inc.

参数	示例值	注释
host-project	your-host-project-name	包含 VM 系列防火墙部署的项目的名称。
fw-deployment-name	my-vm-series-firewall-name	
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	如果可以，请按如下所示列出多个区域： `zones- us-central1-a - us-central1-b- us-central1-c- us-central1-f`
app-machine-type	n1-standard-2	运行应用程序或服务的 VM 的机器类型。如果许可证允许，则可以使用对 VM 系列的最低系统要求中的任何机器类型。
app-instance-tag	web-app-vm	您已在 GCP 中应用此标记（标签）。
sshkey	'admin:ssh-rsa <PASTE KEY>'	查看 SSH 密钥对。用单引号括起来，键入 **admin:**，后跟一个空格，然后粘贴您的密钥。这与 Google Marketplace 模板使用的约定相同。
trust-network	<project-name>/<vpc-network-name>	对于共享 VPC，<project-name> 是主机项目名称。 对于对等 VPC，<project-name> 是服务项目名称。
trust-subnet	<project-name>/<subnet-name>	对于共享 VPC，<project-name> 是主机项目名称。 对于对等 VPC，<project-name> 是服务项目名称。
trust-subnet-cidr	10.2.0.0/24	对于绿色字段部署，参数值为主机项目可信子网 CIDR（防

©2024 Palo Alto Networks, Inc.

参数	示例值	注释
		火墙模板中的 trust-network-cidr 参数）。 对于棕色字段部署，参数值为可信网络 CIDR。
vm-series-fw-template-topic	<pubsub-topic>	输入防火墙部署创建的主题名称。应用程序模板将消息发布到主题，以对防火墙配置进行编程以转发流量。
ilb-port	80	输入应用程序的 internal-load-balancer-port 输出的端口号。
urlPath-namedPort	83	输入 urlPath-namedPort 输出的端口号。

GKE 服务模板示例

这些模板示例演示如何配置 GKE 服务，以使其受 VM 系列防火墙保护。有关创建集群服务的基础知识，请参阅创建专用集群。

- 使用 GKE 服务模板示例
- gke_cluster_role.yaml
- gke_cluster_role_binding.yaml
- web-deployment.yaml
- web-service.yaml
- web-deployment-v2.yaml
- web-service-v2.yaml
- 服务中的多个端口

使用 **GKE** 服务模板示例

您可以根据后面 `.yaml` 文件中的内容示例创建服务模板。通常，您将创建一个 `.yaml` 文件。

要通过 VM 系列防火墙提供保护，必须将集群中的服务标记为“panw-named-port=<named_port>”，如 web-service.yaml 或 web-service-v2.yaml 中所示。

1. 部署 `.yaml` 文件，如下所示：

```
kubectl apply -f [FILE_NAME].yaml
```


©2024 Palo Alto Networks, Inc.

2. 配置 VPC 部署。
   - 在共享 VPC 部署中，在共享 VPC 中启动 GKE 集群，如配置共享 VPC 中所述。
   - 在对等 VPC 部署中，将 GKE 集群 VPC 与主机项目可信网络进行对等。请参阅配置对等 VPC。



部署后，您可以删除服务模板 *.yaml* 文件中部署的所有服务，如下所示：

```
kubectl delete -f [FILE_NAME].yaml
```

gke_cluster_role.yaml

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind:ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

gke_cluster_role_binding.yaml

```
kind:ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:
   - kind:ServiceAccount     name: hj-gke-891ca3-cluster1-sa
     namespace: default roleRef:   kind:ClusterRole   name: gke-
plugin-role   apiGroup: rbac.authorization.k8s.io
```

web-deployment.yaml

```
apiVersion: extensions/v1beta1 kind:Deployment metadata:   name:
 web   namespace: default spec:   selector:    matchLabels:     run:
 web   template:    metadata:     labels:       run: web    spec:
     containers:     - image: gcr.io/google-samples/hello-app:1.0
       imagePullPolicy:IfNotPresent       name: web       ports:
       - containerPort:8080        protocol:  TCP
```

web-service.yaml

```
apiVersion: v1 kind:Service metadata:   name: web   namespace:
 default   annotations:     cloud.google.com/load-balancer-
type:"Internal"   labels:     panw-named-port-port1:"80" spec:
   ports:   # the port that this service should serve on   - name:
 port1     port:80     protocol:TCP     targetPort:8080   selector:
     run: web   type:LoadBalancer
```

web-deployment-v2.yaml

```
apiVersion: extensions/v1beta1 kind:Deployment metadata:   name: web2
   namespace: default spec:   selector:     matchLabels:       run:
 web2   template:     metadata:       labels:         run: web2
     spec:       containers:       - image: gcr.io/google-samples/
```


©2024 Palo Alto Networks, Inc.

```
hello-app:2.0          imagePullPolicy:IfNotPresent          name: web2
         ports:          - containerPort:8080           protocol:TCP
```

web-service-v2.yaml

```
apiVersion: v1   kind:Service   metadata:     name: web2
     namespace: default     annotations:       cloud.google.com/
load-balancer-type:"Internal"     labels:       panw-named-
port-port2:"81"   spec:     ports:     # the port that this
 service should serve on      - name: port2       port:81
       protocol:TCP       targetPort:8080     selector:       run:
 web2     type:LoadBalancer
```

服务中的多个端口

对于一个服务中的多个端口，请编辑标签，并以 panw-named-port-<*service-spec-port-name*> 格式映射目标端口名称和编号，如下例所示。

```
apiVersion: v1 kind:Service metadata:   name: carts   annotations:
     cloud.google.com/load-balancer-type:"Internal"   labels:
     panw-named-port-carts-http:"6082"     panw-named-port-carts-
https:"6083"   namespace: default spec:   type:LoadBalancer   ports:
   # the port that this service should serve on   - name: carts-http
     protocol:TCP     port:80     targetPort:80   - name: carts-
https     protocol:TCP     port:443     targetPort:443   selector:
     name: carts
```


©2024 Palo Alto Networks, Inc.

在 Cisco ENCS 网络中设置 VM 系列防火墙

如果您已使用 Cisco 5400 系列企业网络计算系统 (ENCS) 设备虚拟化分支机构或远程办公室的基于设备的传统网络基础架构，则可以使用企业 NFV 基础架构软件 (NFVIS) 在您的 Cisco 网络中部署 VM 系列防火墙。VM 系列防火墙用作具有下一代防火墙功能的虚拟网络功能 (VNF)，可安全启用所有应用程序，并保护您的分支机构或远程办公室用户和网络免遭威胁。

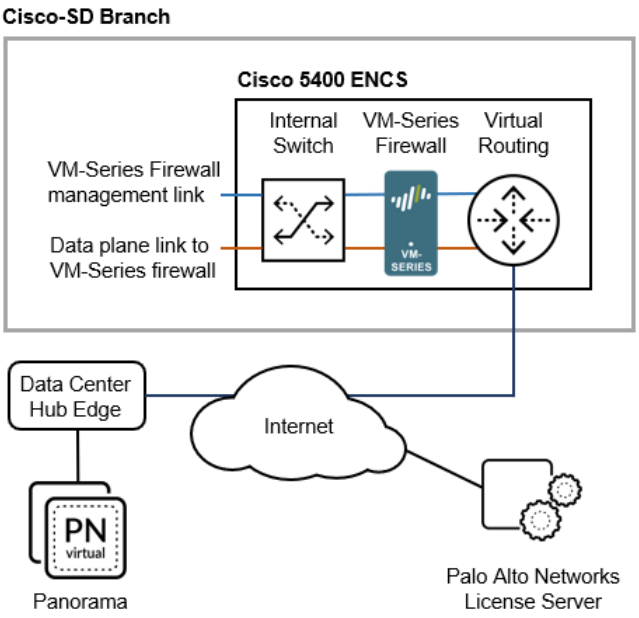
Cisco 企业网络计算系统 (ENCS) 设备与 Cisco 集成服务虚拟路由器 (ISRV) 和 NFVIS 软件相结合，以支持软件定义分支 (SD-Branch) 网络基础架构。

- 计划 Cisco ENCS 部署
- 为 Cisco ENCS 准备 VM 系列防火墙映像
- 在 Cisco ENCS 上部署 VM 系列防火墙

计划 Cisco ENCS 部署

在 Cisco SD-Branch 中，将 Cisco 系列防火墙作为 VNF 部署在 Cisco ENCS 设备上，该 VNF 提供下一代防火墙功能，以保护分支机构的应用程序和用户。您可以在虚拟线路，第 2 层或第 3 层部署以及高可用性配置中部署防火墙。

要管理 VM 系列防火墙，可以在本地或云中部署 Panorama 设备。以下拓扑显示了分支边缘的 VM 系列防火墙。



Cisco ENCS 要求

有关支持的 NFVIS 版本和硬件平台，请参阅 Palo Alto Networks 兼容性矩阵。

- 在 NFVIS 中，建立网络和桥接。
  - 创建虚拟 NIC 并将其连接到虚拟网桥，以便 ENCS 设备可以控制通过 VM 系列防火墙的流量。

    在 Cisco ENCS 设备上，VM 系列防火墙最多支持 8 个数据平面接口。

    Cisco ENCS 上 *VM* 系列防火墙的数据平面接口仅支持 *Virtio* 模式；不支持 *ENCS SR-IOV* 和 *PCI passthrough* 模式。
  - 为 VM 系列防火墙管理访问设置网络连接。如果您使用的是 Panorama，请确保 Panorama 具有网络访问权限以管理您部署的防火墙。
- Python 2.7。如果使用命令行进行转换，则在本地计算机上是必需的。

©2024 Palo Alto Networks, Inc.

VM 系列防火墙和 **Panorama** 要求

- VM 系列防火墙 — 推荐使用 VM-50 和 VM-100。如果 ENCS 硬件具有足够的资源可分配给 VM 系列防火墙，则还支持 VM-300、VM-500和 VM-700。要确保 Cisco ENCS 设备具有足够的资源来支持所选 VM 系列型号，请参阅 VM 系列系统要求。
  - 用于 PAN-OS 9.1 或更高版本的 qcow2 文件（用于 VM 系列 KVM 基本映像的 PAN-OS）。请参阅从图形用户界面转换 qcow2 文件中的步骤 2，或从命令行界面转换 qcow2 文件中的步骤 2。
  - VM 系列防火墙容量许可证和订阅授权代码，可满足您的要求。请参阅VM 系列型号许可证类型。您可以在 NFVIS 用户界面中输入验证码，或者在 conversion 文件夹中的 **`authcodes`** 文本文件中包含身份验证代码，如从命令行界面转换 qcow2 文件中的步骤 4 所述。
  - 使用 PAN-OS 9.1，Cisco ENCS 上的 VM 系列防火墙默认支持启用 DPDK 模式的 Virtio。
- Panorama 硬件或虚拟设备。虽然您可以在 Cisco SD-Branch 网络中部署单个 VM 系列防火墙，使用 Panorama 在许多分支机构中部署防火墙并集中管理它们更为常见。
  - Panorama 版本 9.1 或更高版本。版本必须与 VM 系列防火墙上的版本相同或更高。
  - 在Panorama上生成 VM 身份验证密钥。此密钥允许 VM 系列防火墙使用 Panorama 进行身份验证。

©2024 Palo Alto Networks, Inc.

为 Cisco ENCS 准备 VM 系列防火墙映像

您可以从 NFVIS 图形用户界面或命令行界面转换 PAN-OS qcow2 文件。

- 从图形用户界面转换 qcow2 文件
- 从命令行界面转换 qcow2 文件

从图形用户界面转换 qcow2 文件

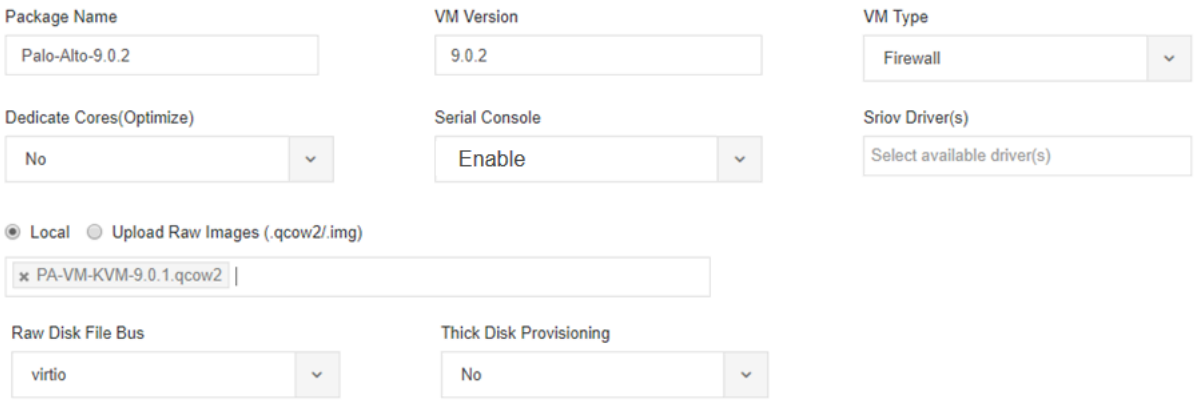
使用 NFVIS 图形用户界面输入映像打包和引导信息。

STEP 1 | 在 NFVIS 中，转到 **VM Life Cycle**（**VM** 生命周期）> **Image Repository**（映像存储库）> **Image Packaging**（映像打包）。

STEP 2 | 填写包信息，如下所示，提供您自己的值。

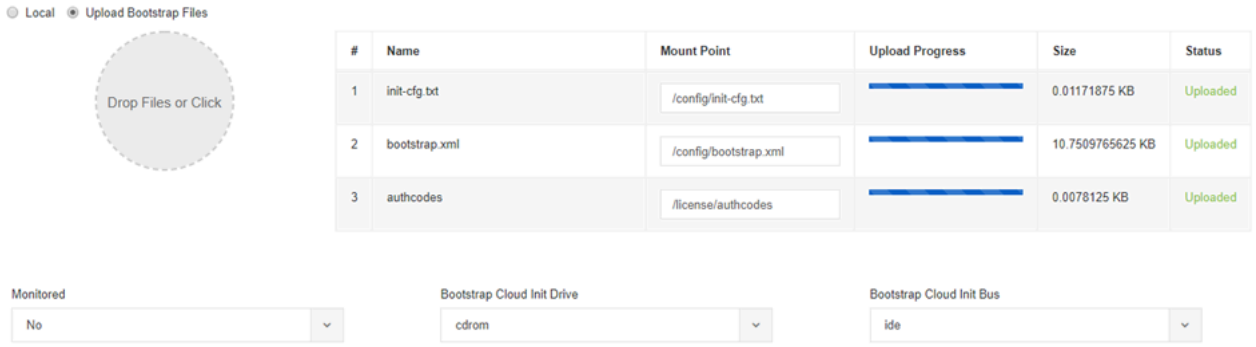
1. 输入 **Package Name**（数据包名称）和 **VM Version**（**VM** 版本），对于 **VM Type**（**VM** 类型），选择 **Firewall**（防火墙）。
2. **Enable**（启用）**Serial Console**（串行控制台）。
3. 将 **Sriov Driver(s)**（**Sriov** 驱动器）字段留空，因为不支持 SR-IOV。
4. 选择 **Local**（本地）以选择之前上传的 qcow2 文件，或单击 **Upload Raw Images**（上传原始映像）以上传 qcow2 文件。
   - 登录到 Palo Alto Networks 客户支持门户。

     如果您还没有这样做，请创建一个支持帐户并注册 VM 系列防火墙。
   - 选择 **Support**（支持）> **Software Updates**（软件更新），并从 **Filter By**（筛选条件）下拉列表中，选择 **Pan OS for VM-Series KVM Base Image**（用于 **VM** 系列 **KVM** 基本映像的 **PAN-OS**），例如，版本 9.1。
   - 下载 qcow2 映像。

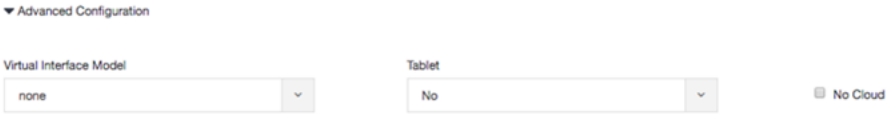


©2024 Palo Alto Networks, Inc.

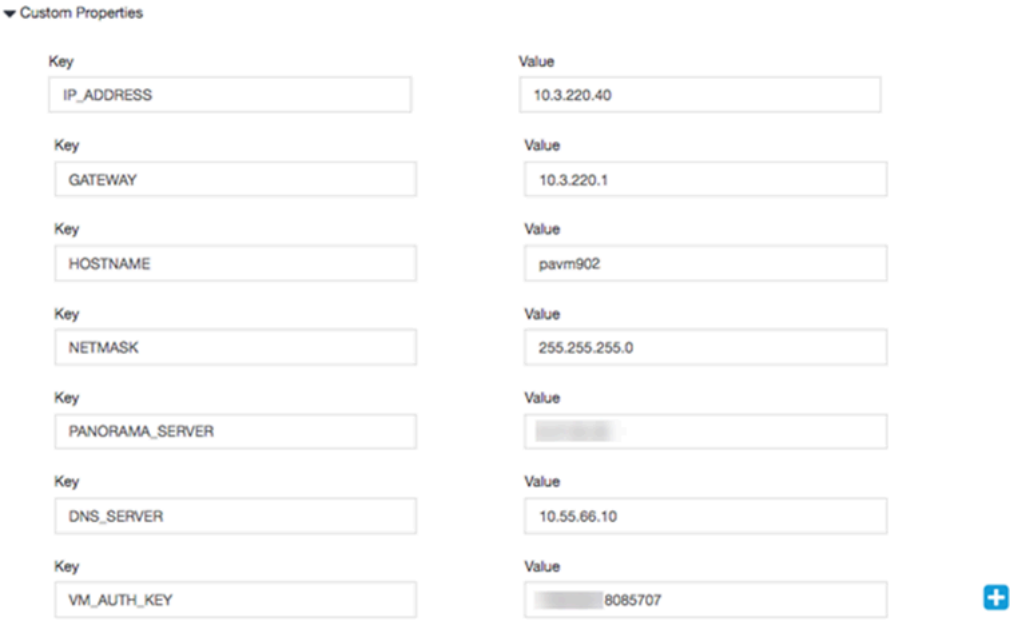
STEP 3 | 上传引导文件。



STEP 4 | 设置 **Advanced Configuration**（高级配置）。



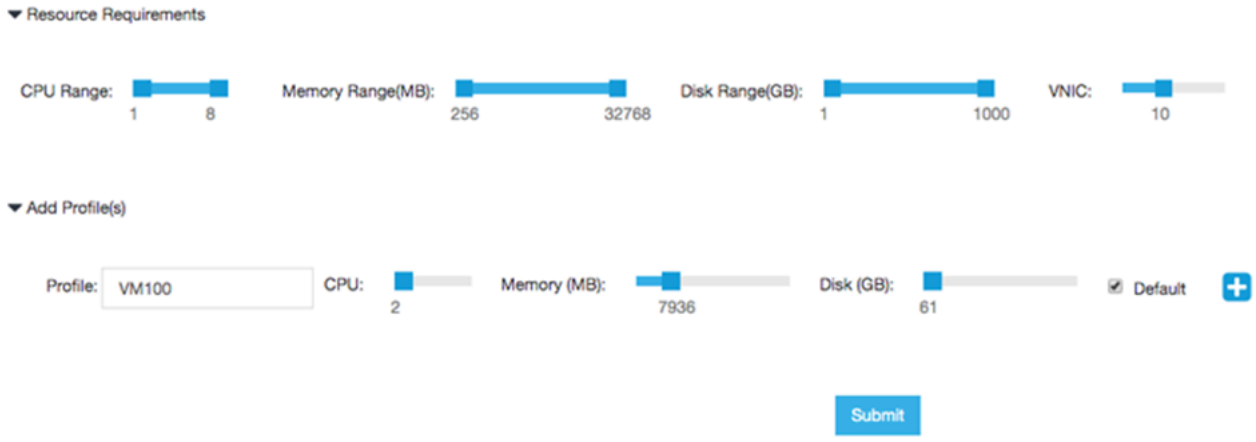
STEP 5 | 输入 **Custom Properties**（自定义属性）的值。



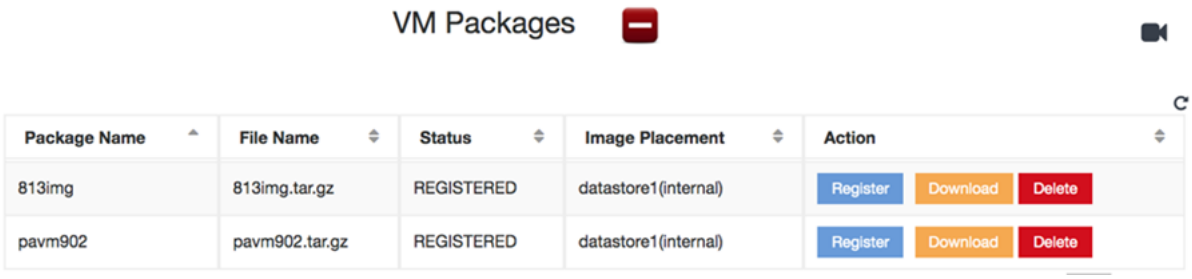
 ©2024 Palo Alto Networks, Inc.

STEP 6 | 设置资源要求的值并选择“默认”配置文件，或为当前配置添加配置文件。

单击 **Submit**（提交）以保存数据包。



STEP 7 | 单击 **Register**（注册）以注册新映像。



从命令行界面转换 qcow2 文件

要从命令行界面创建引导程序文件，请创建文件 `image_properties_template.xml`，然后使用 VM Image Packaging 实用程序以创建 `.tar` 文件，您将使用此文件转换 `nfvpt.py` 脚本。输出是可以从 NFVIS 用户界面上传的 `tar.gz` 文件。

STEP 1 | 在您要下载的本地计算机（转换文件夹）上创建或选择一个文件夹，并保存将 VM 系列防火墙 qcow2 映像转换为 Cisco ENCS 格式所需的文件。

STEP 2 | 获取 VM 系列防火墙 qcow2 映像。

1. 登录到 Palo Alto Networks 客户支持门户。

   如果您还没有这样做，请创建一个支持帐户并注册 VM 系列防火墙。
2. 选择 **Support**（支持） > **Software Updates**（软件更新），并从 **Filter By**（筛选条件）下拉列表中，选择 **Pan OS for VM-Series KVM Base Image**（用于 **VM** 系列 **KVM** 基本映像的 **PAN-OS**），例如，版本 9.1。
3. 将 qcow2 映像下载到转换文件夹。

©2024 Palo Alto Networks, Inc.

STEP 3 | 在转换文件夹中创建以下 init-cfg.txt 文件。

```
type=static ip-address=${IP_ADDRESS} default-gateway=${GATEWAY}
 netmask=${NETMASK} ipv6-address=  ipv6-default-gateway=
 hostname=${HOSTNAME} vm-auth-key=${VM_AUTH_KEY} panorama-server=
${PANORAMA_SERVER} panorama-server-2=  tplname=  dgname=  dns-
primary=${DNS_SERVER} dns-secondary=  op-command-modes=jumbo-
frame, mgmt-interface-swap** dhcp-send-hostname=yes dhcp-send-
client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes
```

STEP 4 | 创建一个名为 authcodes的文本文件（无扩展名），并输入 VM 系列防火墙容量和订阅的授权代码。将文件保存在转换文件夹中。

STEP 5 | 在转换文件夹中创建以下 image_properties_template.xml 文件，并为部署提供值：

```
<image_properties> <vnf_type>FIREWALL</vnf_type>
 <name>pafw</name> <version>9.1.0</version> <bootup_time>-1</
bootup_time> <root_file_disk_bus>virtio</root_file_disk_bus>
 <root_image_disk_format>qcow2</root_image_disk_format>
 <vcpu_min>2</vcpu_min> <vcpu_max>8</vcpu_max>
 <memory_mb_min>4096</memory_mb_min> <memory_mb_max>16384</
memory_mb_max> <vnic_max>8</vnic_max> <root_disk_gb_min>32</
root_disk_gb_min> <root_disk_gb_max>60</root_disk_gb_max>
 <console_type_serial>true</console_type_serial>
 <sriov_supported>true</sriov_supported> <pcie_supported>false</
pcie_supported> <monitoring_supported>false</monitoring_supported>
 <monitoring_methods>ICMPPing</monitoring_methods>
 <low_latency>true</low_latency> <privileged_vm>true</
privileged_vm> <custom_property> <HOSTNAME> </HOSTNAME> </
custom_property> <custom_property> <IP_ADDRESS> </IP_ADDRESS>
 </custom_property> <custom_property> <NETMASK> </NETMASK>
 </custom_property> <custom_property> <GATEWAY> </GATEWAY>
 </custom_property> <custom_property> <PANORAMA_SERVER> </
PANORAMA_SERVER> </custom_property> <custom_property> <DNS_SERVER>
 </DNS_SERVER> </custom_property> <custom_property> <VM_AUTH_KEY>
 </VM_AUTH_KEY> </custom_property> <default_profile>VM-50</
default_profile> <profiles> <profile> <name>VM-50</name>
 <description>VM-50 profile</description> <vcpus>2</
vcpus> <memory_mb>5120</memory_mb> <root_disk_mb>60000</
root_disk_mb> </profile> <profile> <name>VM-100-n-200</name>
 <description>VM-100 and VM-200 profile</description> <vcpus>2</
vcpus> <memory_mb>7168</memory_mb> <root_disk_mb>60000</
root_disk_mb> </profile> <profile> <name>VM-300</name>
 <description>VM-300 profile</description> <vcpus>2</vcpus>
 <memory_mb>9216</memory_mb> <root_disk_mb>60000</root_disk_mb> </
profile> <profile> <name>VM-1000-HV</name> <description>VM-1000-
HV profile</description> <vcpus>4</vcpus> <memory_mb>9216</
memory_mb> <root_disk_mb>60000</root_disk_mb> </profile>
 <profile> <name>VM-500</name> <description>VM-500 profile</
description> <vcpus>4</vcpus> <memory_mb>16384</memory_mb>
 <root_disk_mb>60000</root_disk_mb> </profile> </profiles>
 <cdrom>true</cdrom> <bootstrap_file_1>/config/init-cfg.txt</
bootstrap_file_1> <bootstrap_file_2>/config/bootstrap.xml</
```

 ©2024 Palo Alto Networks, Inc.

```
bootstrap_file_2> <bootstrap_file_3>/license/authcodes</
bootstrap_file_3> </image_properties>
```

STEP 6 | 下载映像打包实用程序。

1. 登录企业 NFVIS 用户界面并选择 **VM Life Cycle**（**VM** 生命周期） > **Image Repository**（映像存储库）。
2. 单击 **Browse Datastore**（浏览数据存储）选项卡，然后导航到 **Data**（数据） > **intdatastore** > **Uploads**（上传） > **vmpackagingutility**。
3. 下载 `nfvisvmpackagingtool.tar` 到转换文件夹。
4. 解压文件：

```
tar -xvf nfvisvmpackagingtool.tar
```

STEP 7 | 在包含 qcow2 （即 `init-config.txt` 和 `authcodes` 文件）的转换文件夹中，运行 `nfvpt.py` 脚本。参阅 `nfvpt.py` 映像打包实用工具文档。

以下示例创建映像文件 Palo-Alto-9.1.0 和 VM-100 配置文件。选项是以空格分隔的（为了清晰起见，示例在单独一行显示选项），自定义选项是带有冒号分隔符的键值对。

```
./nfvpt.py -o Palo-Alto-9.1.0 -i PA-VM-KVM-9.1.0.qcow2 -n
 PAN902 -t FIREWALL -r 9.1.0 --monitored false --privileged
 true --bootstrap /config/init-cfg.txt:init-cfg.txt,/license/
authcodes:authcodes --min_vcpu 2 --max_vcpu 8 --min_mem 4096
 --max_mem 16384 --min_disk 10 --max_disk 70 --vnic_max 8 --
optimize true --console_type_serial true --profile VM-100,"VM-100
 profile",2,7168,61440 --default_profile VM-100 --custom
 HOSTNAME:hello --custom IP_ADDRESS:10.2.218.24 --custom
 NETMASK:255.255.255.0 --custom GATEWAY:10.2.218.1 --custom
 DNS_SERVER:10.55.66.10 --custom PANORAMA_SERVER:0.10.10.0 --custom
 VM_AUTH_KEY:123451234512345
```

STEP 8 | 上传转换后的映像。

1. 在 NFVIS 用户界面中，选择 **VM Life Cycle**（**VM** 生命周期） > **Image Repository**（映像存储库），然后单击蓝色图像图标以显示 **Drop Files or Click**（拖放文件或单击）圆圈。
2. 将转换后的文件拖到圆圈中，或单击以浏览并选择文件。
3. 在“状态”列中，单击 **Start**（开始）。

   上传完成后，将注册映像，您上传的文件将显示在 **Image Registration**（映像注册）标签的 **Images**（映像）列表。

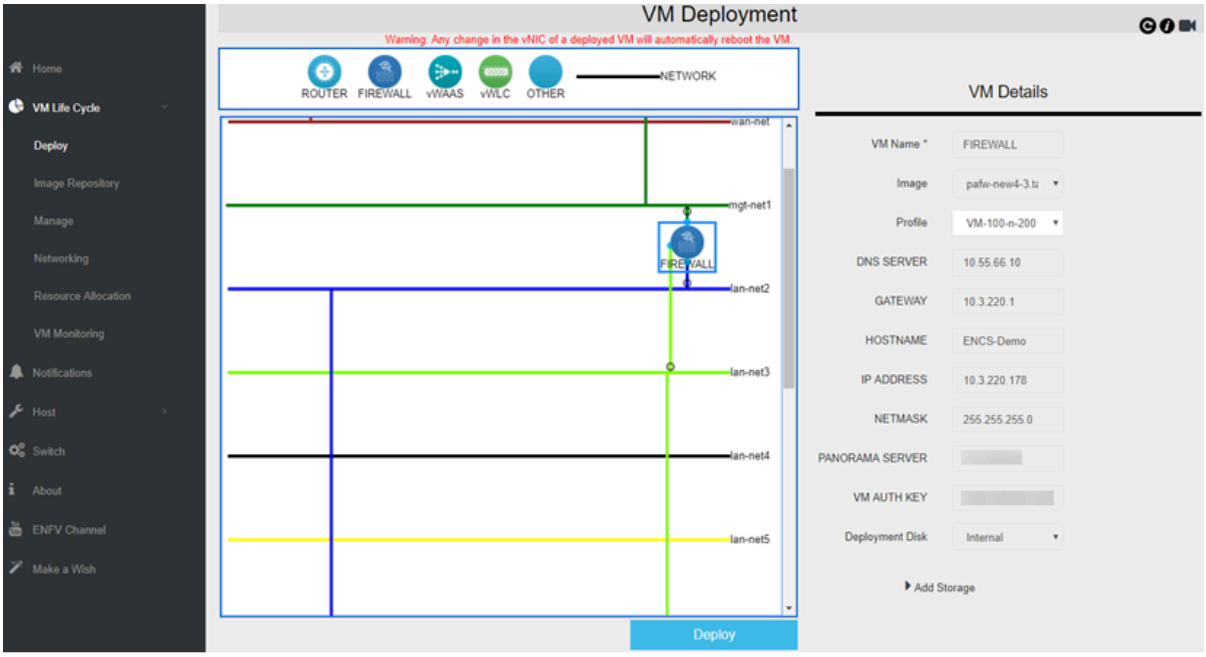
 ©2024 Palo Alto Networks, Inc.

在 Cisco ENCS 上部署 VM 系列防火墙

在开始部署防火墙之前，请确保已创建网络连接，以便管理对 VM 系列防火墙的访问。如果您使用的是 Panorama，请确保 Panorama 具有与防火墙的管理连接。

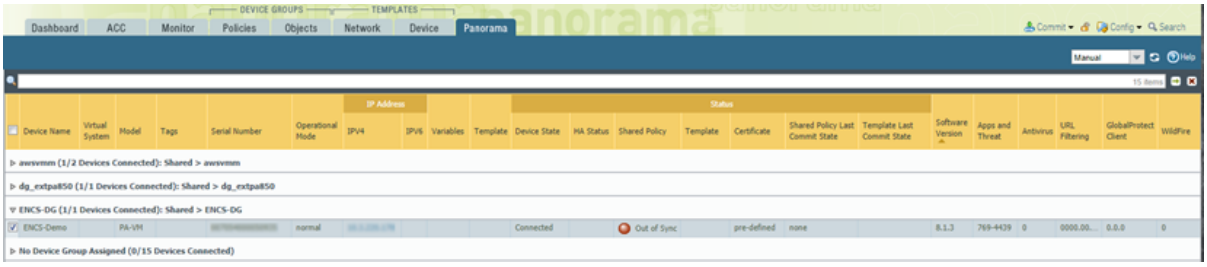
STEP 1 | 部署 VM 系列防火墙。

1. 在 Enterprise NFVIS 中，单击 **VM Life Cycle**（**VM** 生命周期）> **Deploy**（部署）。
2. 将防火墙图标拖放到适当的网络中。在本示例中，防火墙连接到管理网络和 LAN 网络。



3. **Deploy**（部署）VM 系列防火墙。

   如果使用 Panorama 管理防火墙，则防火墙显示为 **Panorama** > **Managed Devices**（托管设备）> **Summary**（摘要）上显示为 **Connected**（已连接）。如果防火墙未连接到 Panorama，请检查是否提供了正确的 Panorama IP 地址，以及设备是否可以通过网络进行通信。

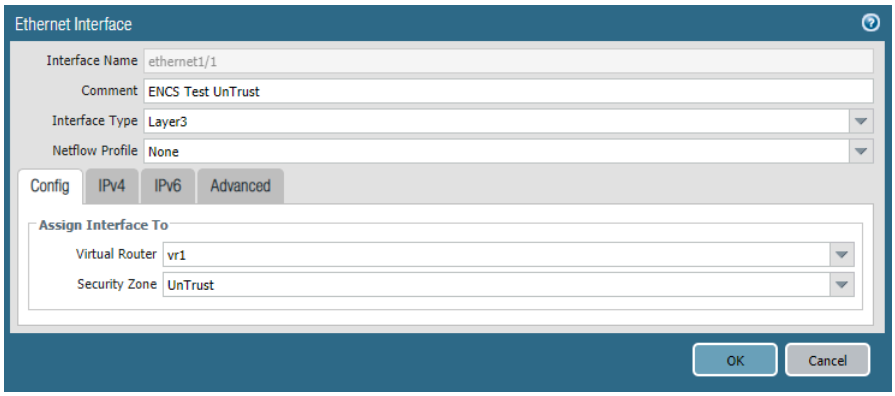


 ©2024 Palo Alto Networks, Inc.

STEP 2 | 配置 VM 系列防火墙数据面接口。

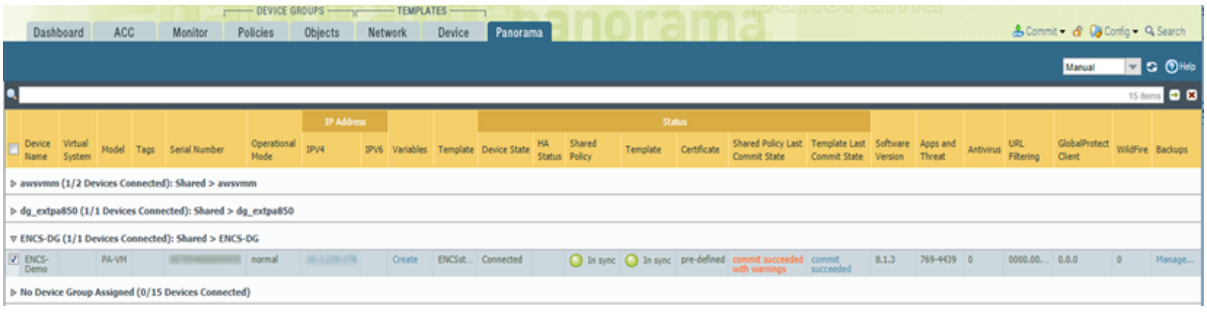
请参阅 Configure a Layer 3 Interface（配置第 3 层接口），Configure a Layer 2 Interface（配置第 2 层接口）或 Configure Virtual Wires（配置虚拟线路）。如果使用 Panorama，以下步骤将说明如何为第 3 层部署配置防火墙。

1. 添加模板并将防火墙分配到模板。
2. 选择 **Network**（网络），然后在 Template（模板）下拉列表中选择创建的模板。
3. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。
4. 单击 **ethernet 1/1** 并按如下所述配置：
   - 将 **Interface Type**（接口类型）设置为 **Layer3**（第 **3** 层）。
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 此外，在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。例如，定义名为 **`UnTrust`** 的新区域，然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **DHCP Client**（**DHCP** 客户端）或 **Static**（静态）。如果选择静态，请输入 IP 地址。



5. 对每个网络接口重复 b-e。
6. **Commit**（提交）> **Commit and Push**（提交并推送）以将所有配置更改提交到 Panorama 和托管防火墙。

   确认防火墙接口的链路状态正常。

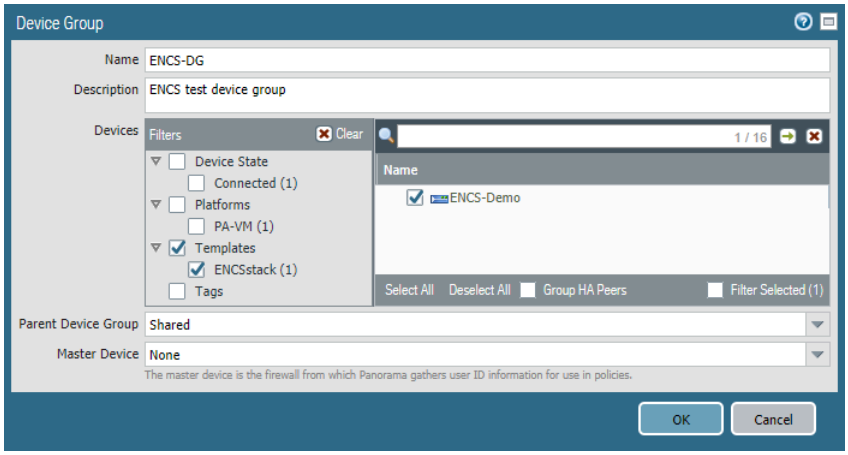


 ©2024 Palo Alto Networks, Inc.

STEP 3 | 配置安全策略以安全启用网络上的应用程序和用户。

如果使用 Panorama，以下步骤将说明如何使用设备组集中管理托管防火墙的策略规则。

1. 添加设备组并将托管防火墙分配到设备组。



2. 为设备组配置安全政策。

STEP 4 | 验证 VM 系列防火墙正在保护网络上的流量。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 Oracle Cloud Infrastructure 上设置 VM 系列防火墙

在 Oracle 云基础架构 (OCI) 云上部署 VM 系列防火墙。凭借 OCI 上的 VM 系列，您可以保护和分割工作负载，防止高级威胁，并在迁移到云时提高应用程序的可见性。

OCI 是一种公共云计算服务，让您能够在 Oracle 提供的高可用性托管环境中运行应用程序。您可以部署 VM 系列防火墙以保护运行 OCI 环境的应用程序和服务。

- OCI 形状类型
- OCI 上支持的部署
- 准备在 OCI 上设置 VM 系列防火墙
- 从 Oracle Cloud Marketplace 部署 VM 系列防火墙
- 在 OCI 上配置主动/被动 HA

OCI 形状类型

VM 系列防火墙支持以下 OCI VM 形状。有关 VM 形状的详细信息，请参阅 Oracle 云基础架构文档。

VM 系列型号	最小 OCI 形状
• VM-100 • 基于软件 NFGW 积分的 VM 系列	VM.Standard2.4
• VM-300 • 基于软件 NFGW 积分的 VM 系列	VM.Standard2.4
• VM-500 • 基于软件 NFGW 积分的 VM 系列	VM.Standard2.8
• VM-700 • 基于软件 NFGW 积分的 VM 系列	VM.Standard2.16
• VM-100、VM-300、VM-500 和 VM-700 • 基于软件 NFGW 积分的 VM 系列	VM.Optimized3.Flex VM.Standard3.Flex

您可以使用比最低 VM 系列系统要求更多的资源在 OCI 实例上部署 VM 系列防火墙。如果为 VM 系列防火墙型号选择更大的形状大小。虽然防火墙仅使用系统要求页面上列出的最大 vCPU 核心和内存，但它确实利用了较大形状提供的更快的网络性能。

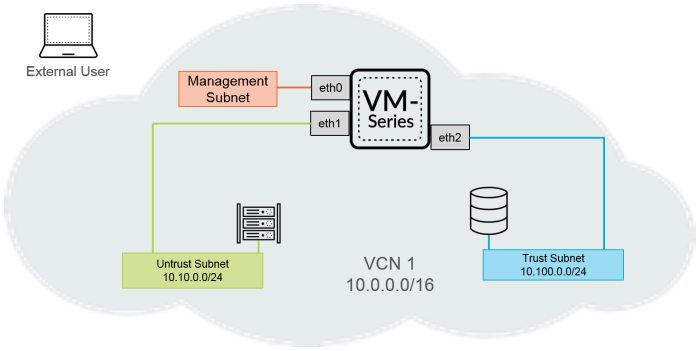
©2024 Palo Alto Networks, Inc.

OCI 上支持的部署

使用 OCI 上的 VM 系列防火墙保护以下场景中云环境：

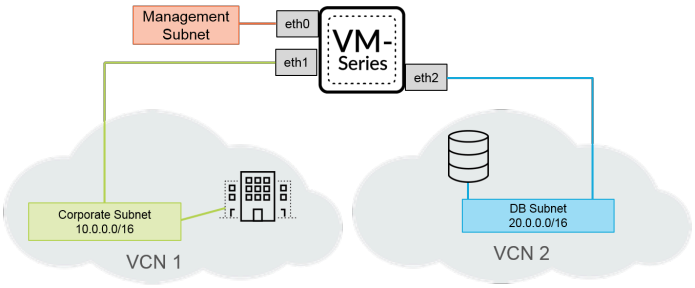
- 北向南流量 — 您可以使用 VM 系列防火墙来保护从不受可信的来源进入云网络的流量或退出云网络以访问不受可信的来源的流量。对于任一类型的流量，您必须在防火墙上的虚拟云网络 (VCN) 和 NAT 策略规则中配置路由表规则。

  在此示例中，出站流量正在退出 VCN 中的可信子网。您必须将源地址转换策略配置到公共 IP 地址和将该流量重定向到防火墙的路由表规则。路由规则将传出流量指向 VCN 的可信子网中的防火墙接口。当防火墙收到此流量时，它会对流量执行源地址转换，并应用您已配置的任何其他安全策略。



- VCN 间流量（东向西）— VM 系列防火墙允许您在 VCN 之间保护云环境中的流量。每个子网必须属于不同的 VCN，因为默认情况下，没有路由规则用于启用 VCN 内的流量。在此方案中，您在连接到每个 VCN 中的子网的防火墙上配置接口。

  在下面的示例中，可信子网中的用户想要访问 DB 子网中的数据。在 OCI 上配置到达 DB Subnet CIDR 下一跃点的路由，该路由指向 VM 系列防火墙上的可信子网网络接口。



有关更多信息，请参阅通过 Palo Alto Networks VM 系列防火墙使用灵活网络保护工作负载。

©2024 Palo Alto Networks, Inc.

准备在 OCI 上设置 VM 系列防火墙

在 Oracle Cloud Infrastructure 上部署 VM 系列防火墙的过程需要完成准备任务。

- 虚拟去网络
- SSH 密钥
- 初始配置用户数据

虚拟去网络

虚拟云网络 (VCN) 是您在 OCI 环境中设置的虚拟专用网络。要在 OCI 中部署 VM 系列防火墙，VCN 必须至少具有三个用于管理接口的虚拟网络接口卡 (VNIC) 和两个数据接口。

OCI 使用一系列路由表从 VCN 发送流量，并将一个路由表添加到每个子网。子网是 VCN 的一个部分。如果未指定路由表，则子网使用 VCN 的默认路由表。每个路由表规则为与 CIDR 匹配的任何流量指定目标 CIDR 块和下一个跃点（目标）。如果目标 IP 地址在 VCN 的指定 CIDR 块之外，OCI 仅使用子网的路由表；在 VCN 中启用流量不需要路由规则。并且，如果流量具有重叠规则，则 OCI 使用路由表中最具体的规则来路由流量。

如果没有与尝试离开 *VCN* 的流量匹配的路由规则，则流量将被丢弃。

每个子网都需要一个路由表，一旦您将路由表添加到子网，就无法更改它。但是，您可以在创建路由表后添加，删除或编辑规则。

SSH 密钥

您首次必须创建 SSH 密钥对才能登录到防火墙。您首次不能使用默认的用户名和密码访问防火墙。防火墙首次启动后，您必须通过 CLI 访问防火墙，并创建新的用户名和密码。

1. 创建 SSH 密钥对，并将 SSH 密钥对存储在操作系统的默认位置。
   - 在 Linux 或 MacOS 中，使用 `ssh-keygen` 在 .ssh 目录中创建密钥对。
   - 在 Windows 中，使用 PuTTYgen 创建密钥对。

     Key comment（密钥注释）字段的内容与 VM 系列防火墙无关；您可以接受默认注释（密钥创建日期）或输入有助于您记住密钥对名称的注释。使用 **Save private key**（保存私钥）按钮将私钥存储在 .ssh 目录中。

©2024 Palo Alto Networks, Inc.

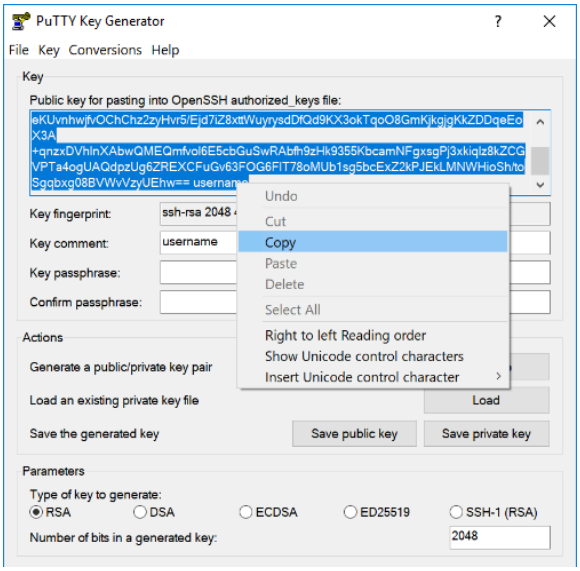
2. 选择完整的公钥。

   - Linux 或 MacOS

     ：在文本编辑器中打开公钥并复制该公钥。

   - Windows：必须使用 PuTTY 密钥生成器查看公钥。启动 PuTTYgen，单击 Load（加载），然后浏览到保存在 .ssh 目录中的私钥。

     在 PuTTYgen 中向下滚动，确保选择整个密钥，右键单击，然后选择 Copy（复制）。



初始配置用户数据

设置 VM 系列防火墙实例时，您必须提供以下引导参数。OCI 使用此信息执行防火墙的初始配置，这样可以为防火墙提供主机名和许可证，并将防火墙连接到 Panorama（如果适用）。

只有在您拥有 *Panorama* 设备并且想要使用 *Panorama* 管理 *VM* 系列防火墙时与 *Panorama* 相关的字段才是必填字段。

字段	说明
hostname=	防火墙的主机名称。
vm-auth-key=	虚拟机身份验证密钥用于将防火墙注册到 Panorama。
panorama-server=	Panorama 主服务器的 IPv4 或 IPv6 地址。该字段不是必填字段，但建议填写，以便集中管理防火墙。
panorama-server-2=	Panorama 辅助服务器的 IPv4 或 IPv6 地址。该字段非必填字段，但建议予以填写。

©2024 Palo Alto Networks, Inc.

字段	说明
tplname=	Panorama 模板堆栈名称。如果您添加 Panorama 服务器 IP 地址，作为最佳实践，请在 Panorama 上将防火墙分配到模板堆栈，并在此字段中输入模板堆栈名称，以便集中管理配置设置并将其推送到防火墙。
dgname=	Panorama 设备组名称。如果添加 Panorama 服务器 IP 地址，作为最佳实践，请在 Panorama 上创建设备组，并在该字段中输入设备组名称，以便按逻辑将防火墙分组并将策略规则推送到防火墙。
authcodes=	用于通过 Palo Alto Networks 许可服务器许可 VM 系列防火墙。
op-command-modes=jumbo-frame	用于在 VM 系列防火墙上启用 Jumbo 帧模式。由于 OCI 默认以 Jumbo 帧模式部署 VM 实例，因此建议您在 Jumbo 帧模式下启动 VM 系列防火墙以实现最佳吞吐量。

将引导参数按以下格式粘贴到 OCI 控制台中。

hostname=<*fw-hostname*>

vm-auth-key=<*auth-key*>

panorama-server=<*panorama-ip*>

panorama-server-2=<*panorama2-ip*>

tplname=<*template-stack-name*>

dgname=<*device-group-name*>

authocodes=<*firewall-authcode*>

op-command-modes=jumbo-frame

©2024 Palo Alto Networks, Inc.

从 Oracle Cloud Marketplace 部署 VM 系列防火墙

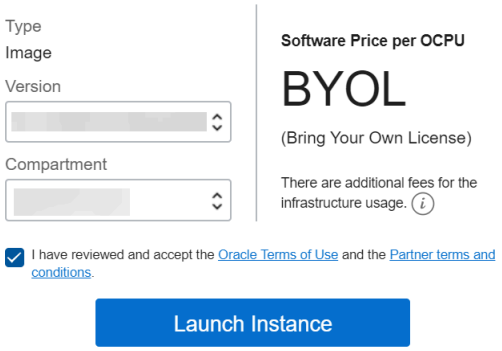
完成以下过程，在 OCI 中从 Oracle Cloud Marketplace 部署 VM 系列防火墙。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 登录到 Oracle Cloud Marketplace。

STEP 2 | 在 Oracle Cloud Marketplace 中找到 VM 系列防火墙应用程序。

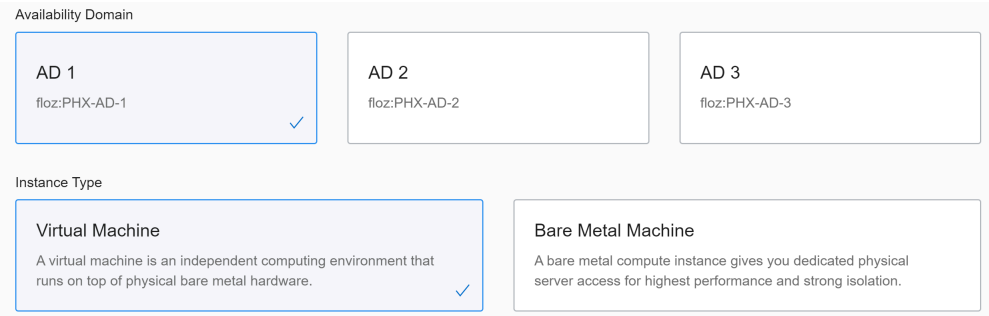
1. 搜索 Palo Alto Networks，将显示 VM 系列防火墙的产品列表。
2. 选择一个产品。
3. 单击 **Get App**（获取应用程序）。
4. 选择 **Region**（区域），然后单击 **Sign In**（登录）。
5. 选择 **Version**（版本）和 **Compartment**（区段）。
6. 接受 Oracle 和合作伙伴条款。
7. 单击 **Launch Instance**（启动实例）。



STEP 3 | 输入 VM 系列防火墙实例的描述性 **Name**（名称）。

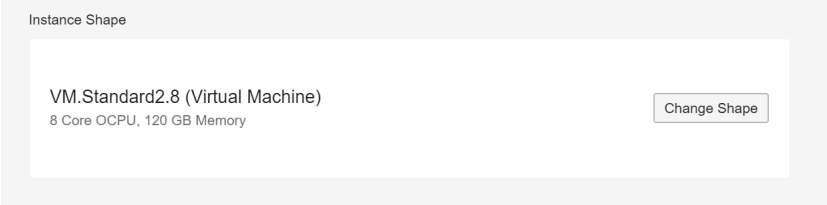
STEP 4 | 选择 **Availability Domain**（可用性域）。

STEP 5 | 在 **Shape Type**（形状类型）下选择 **Virtual Machine**（虚拟机）。



©2024 Palo Alto Networks, Inc.

STEP 6 | 选择具有 VM 系列防火墙模型所需的 CPU 数量、RAM 数量和接口数量的形状。有关不同计算形状提供的数量资源，请参阅计算形状。有关各 VM 系列防火墙型号所需的资源的详细信息，请参阅 VM 系列系统要求。



STEP 7 | 在 Networking（网络）下，为管理接口选择 **Virtual cloud network compartment**（虚拟云网络区段），**Virtual cloud network**（虚拟云网络），**Subnet compartment**（子网区段）和 **Subnet**（子网）。创建 VM 系列防火墙实例时，您只能添加一个实例。您稍后可以添加其他接口。

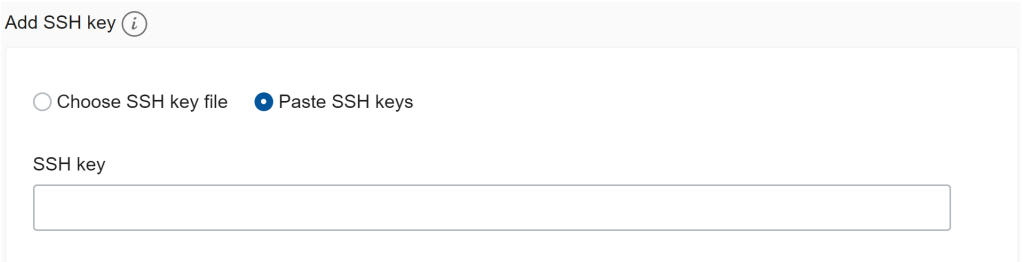


STEP 8 | （可选）将启动卷设置为大于默认大小的大小。默认情况下，将启动卷设置为 60GB。如果需要更大的启动卷以支持诸如附加日志等功能，请完成此过程。

1. 选择 **Custom boot volume size (in GB)**（自定义启动卷大小（以 **GB** 为单位））。
2. 输入 60 或更大的数字。60GB 是 VM 系列防火墙要求的最小硬盘驱动器大小。

STEP 9 | 添加 SSH 密钥。

1. 在 **Add SSH Key**（添加 **SSH** 密钥）下，选择 **Paste SSH Key**（粘贴 **SSH** 密钥）。
2. 将 SSH 密钥粘贴到提供的字段中。



©2024 Palo Alto Networks, Inc.

STEP 10 | 添加引导参数。

1. 单击 **Show Advanced Options**（显示高级选项）。
2. 在 **User data**（用户数据）下，选择 **Paste cloud-init script**（粘贴 **cloud-init** 脚本）。
3. 将 boostrap parameters（引导参数）粘贴到提供的字段中。

   hostname=<*fw-hostname*>

   vm-auth-key=<*auth-key*>

   panorama-server=<*panorama-ip*>

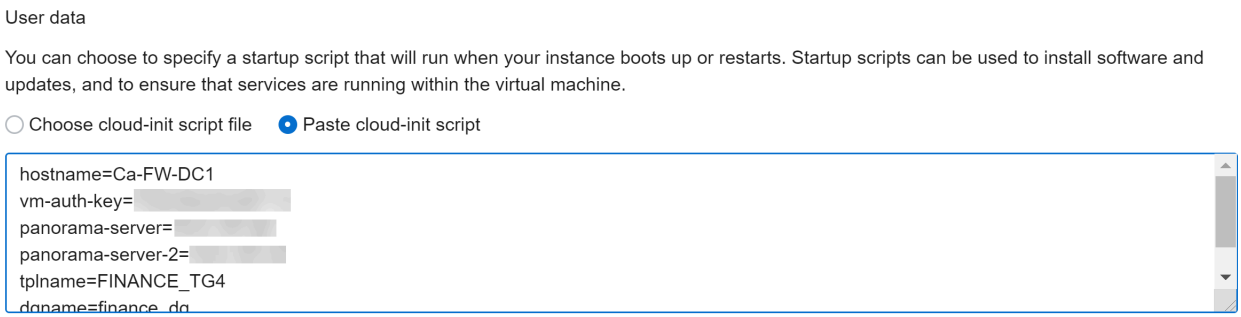
   panorama-server-2=<*panorama2-ip*>

   tplname=<*template-stack-name*>

   dgname=<*device-group-name*>

   authcodes=<*firewall-authcode*>

   op-command-modes=jumbo-frame



STEP 11 | 单击 **Create**（创建）。

启动 VM 系列防火墙后，OCI 将创建主 VNIC 并将其附加到实例。此 VNIC 驻留在实例网络设置中指定的子网中，并连接到 VM 系列防火墙的管理接口。

STEP 12 | 配置防火墙的新管理密码。

1. 在 VM 系列防火墙的命令行界面 (CLI) 中使用 SSH 的管理 IP 地址。
2. 输入以下命令以登录到防火墙：

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. 使用以下命令并按照屏幕上的提示配置新密码：

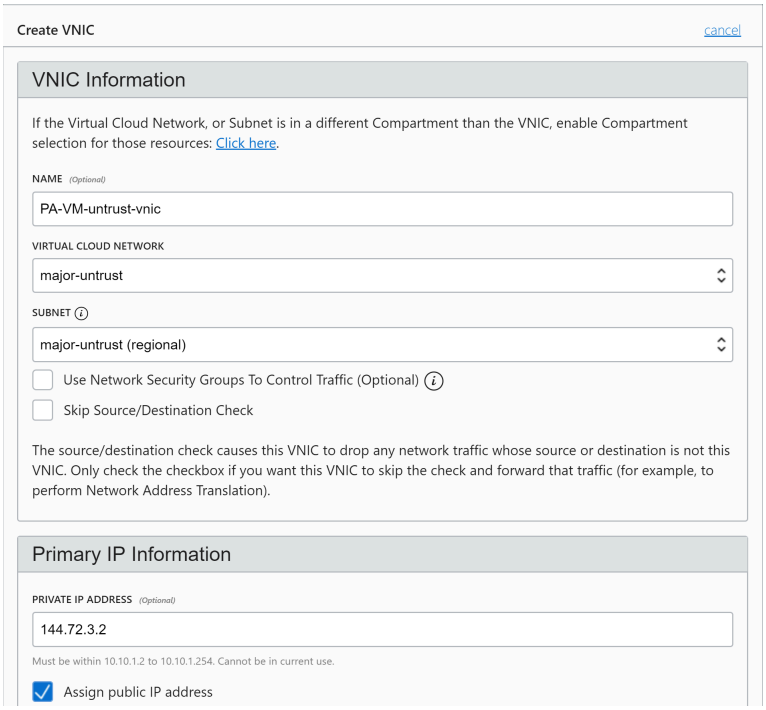
   配置

   set mgt-config users admin password

 ©2024 Palo Alto Networks, Inc.

STEP 13 | 将 vNIC 附加到每个数据接口的 VM 系列防火墙实例。您至少必须将两个数据接口附加到防火墙实例 — 不可信和可信。

1. 选择新启动的 VM 系列防火墙实例并选择 **Attached VNICs**（附加的 **VNIC**） > **Create VNIC**（创建 **VNIC**）。
2. 输入 vNIC 的描述性 **Name**（名称）。
3. 从 **Virtual Cloud Network**（虚拟云网络）下拉列表中选择 VCN。
4. 从 **Subnet**（子网）下拉列表中选择子网。
5. 指定一个 **Private IP Address**（专用 **IP** 地址）。仅在您希望为 vNIC 选择特定 IP 时才需要这样做。如果未指定 IP，OCI 将从分配给子网的 CIDR 块中分配 IP 地址。
6. 为面向公众的 vNIC（例如不可信子网）选择 **Assign Public IP Address**（分配公共 **IP** 地址）。
7. 单击 **Create VPC**（创建 **VPC**）。
8. 对部署所需的每个 vNIC 重复此过程。



 ©2024 Palo Alto Networks, Inc.

STEP 14 | 配置数据面板网络接口作为防火墙上的第 3 层接口。

1. 登录到防火墙。
2. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
3. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 untrust-zone），然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **Static**（静态）。
   - 在 IP 部分单击 **Add**（添加），然后输入接口的 IP 地址和网络掩码。确保 IP 地址与分配给 VCN 中相应子网的 IP 地址相匹配。例如，如果将此接口添加到不可信区域，请确保分配 VCN 中配置的不可信 vNIC IP 地址。
4. 对 VCN 中配置的每个 vNIC 重复此过程（管理 vNIC 除外）。

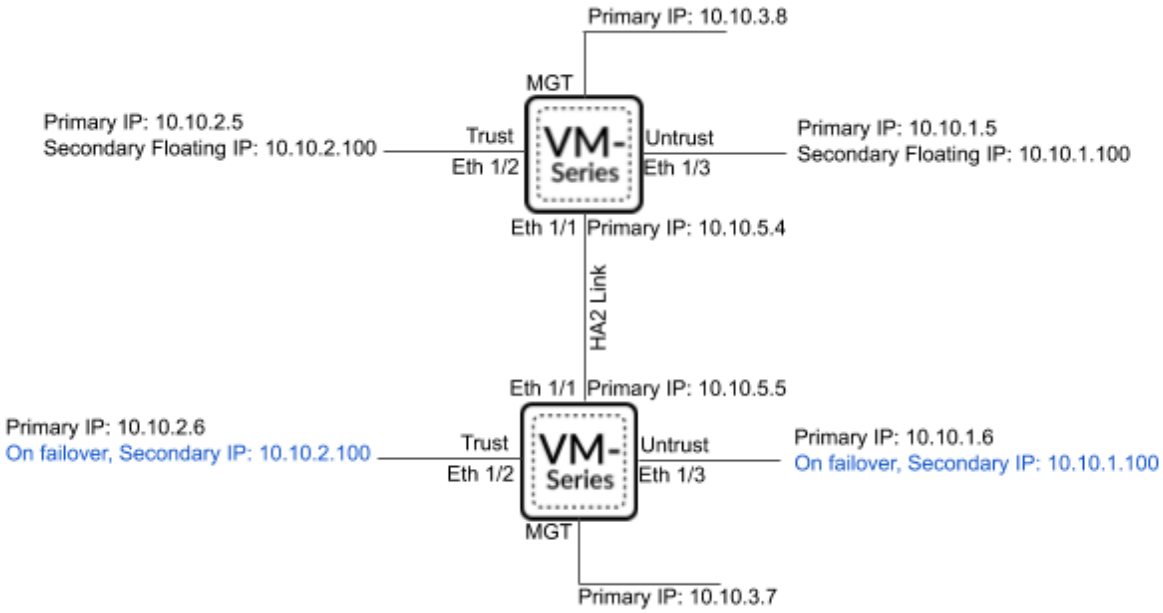
始终只删除接口列表底部的接口。以错误的顺序删除防火墙接口会导致防火墙与 *OCI* 之间的接口不匹配。例如，假设您有五个数据接口，然后删除防火墙上的接口 *2* 并在底部添加一个新接口。重新启动防火墙后，新添加的接口将取代删除的接口 *2*，而不是占据列表底部的位置。

©2024 Palo Alto Networks, Inc.

在 OCI 上配置主动/被动 HA

您可以采用主动/被动高可用性 (HA) 配置方式在 OCI 上配置一对 VM 系列防火墙。为了确保 OCI 上 HA 设置的正常运行时间，您必须创建一个可以快速从一个对等移动到另一个对等的辅助浮动 IP 地址。当主动防火墙发生故障时，浮动 IP 地址会从活动防火墙移动到被动防火墙，以便被动防火墙一旦成为活动对等就可以无缝保护流量。除浮动 IP 地址外，HA 对等还需要 HA 链接 — 一个控制链路 (HA1) 和一个数据链路 (HA2) — 用于同步数据和维护状态信息。

FIPS 模式下 *OCI* 的 *VM* 系列防火墙不支持高可用性。



要允许防火墙在发生故障转移后移动到浮动 IP 地址，您必须将防火墙实例放置在 OCI 上的动态组中。动态组可让您将防火墙实例作为主要参与者进行分组，并创建策略以允许动态组中的实例根据 OCI 服务进行 API 调用。您可以使用匹配规则将 HA 对等实例添加到动态组，然后创建策略以允许可以从一个 VNIC 移动到另一个 VNIC 的浮动 IP 地址。

HA 对中的两个 VM 系列防火墙必须具有相同数量的网络接口。每个防火墙至少需要四个接口 — 管理、不可信、可信和 HA。您可以根据部署要求配置其他数据接口。

- 管理接口 — 与主要接口相关联的专用和公用 IP 地址。您可以将管理接口上的专用 IP 地址用作对等之间 HA1 接口的 IP 地址。如果需要专用 HA 接口，必须将其他接口附加到每个防火墙，每个防火墙总共五个接口。
- 不可信和可信接口 — 主动 HA 对等上的每个数据接口都需要一个主要 IP 地址和一个辅助 IP 地址。在发生故障转移时，当被动 HA 对等转换为主动状态时，辅助专用 IP 地址与先前的主动对等分离，并附加到现在的主动 HA 对等。

©2024 Palo Alto Networks, Inc.

- **HA2** 接口 — 此接口在每个 HA 对等上都拥有一个专用 IP 地址。HA2 接口是 HA 对等用于同步会话、转发表、IPsec 安全关联和 ARP 表的数据链路。

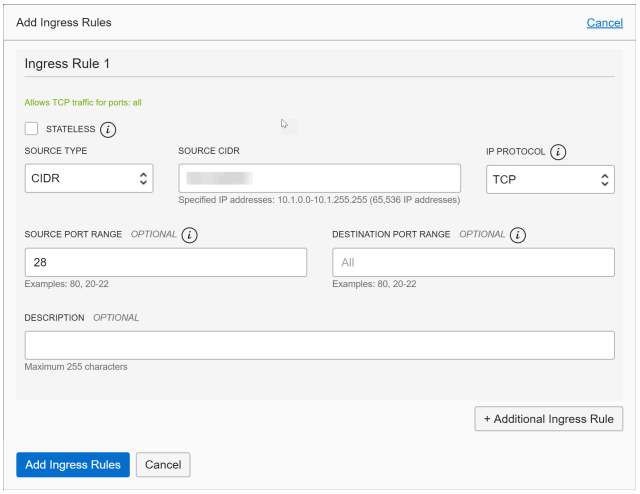
STEP 1 | 从 Oracle Cloud Marketplace 部署 VM 系列防火墙并为 HA 设置网络接口。

1. （可选）在每个 HA 对等上配置专用 HA1 接口。
    1. 在 OCI 控制台中，选择 **Compute**（计算）> **Instances**（实例），然后单击主动对等实例的名称。
    2. 选择 **Attached VNICs**（附加的 **VNIC**），然后单击 **Create VNIC**（创建 **VNIC**）。
    3. 输入 HA1 接口的描述性名称。
    4. 选择 VCN 和子网。
    5. 输入专用 IP 地址。
    6. 单击 **Create VPC**（创建 **VPC**）。
    7. 在被动对等实例上重复此过程。
2. 在每个 HA 对等上配置 HA2 接口。
    1. 在 OCI 控制台中，选择 **Compute**（计算）> **Instances**（实例），然后单击主动对等实例的名称。
    2. 选择 **Attached VNICs**（附加的 **VNIC**），然后单击 **Create VNIC**（创建 **VNIC**）。
    3. 输入 HA2 接口的描述性名称。
    4. 选择 VCN 和子网。HA2 接口应与数据接口位于单独的子网中。
    5. 输入专用 IP 地址。
    6. 单击 **Create VPC**（创建 **VPC**）。
    7. 在被动对等实例上重复此过程。
3. 将辅助 IP 地址添加到主动对等上的数据平面接口。
    1. 在 OCI 控制台中，选择 **Compute**（计算）> **Instances**（实例），然后单击主动对等实例的名称。
    2. 选择 **Attached VNICs**（附加的 **VNIC**），然后单击不可信 VNIC。
    3. 选择 **IP Addresses**（**IP** 地址），然后单击 **Assign Private IP Address**（分配专用 **IP** 地址）。
    4. 输入 IP 地址，然后单击 **Assign**（分配）。
    5. 对主动对等上的每个数据平面接口重复此过程。

©2024 Palo Alto Networks, Inc.

STEP 2 | 创建安全规则以允许 HA 对等同步数据并维护状态信息。默认情况下，OCI 仅允许 ICMP 流量。您必须打开必需的 HA 端口。

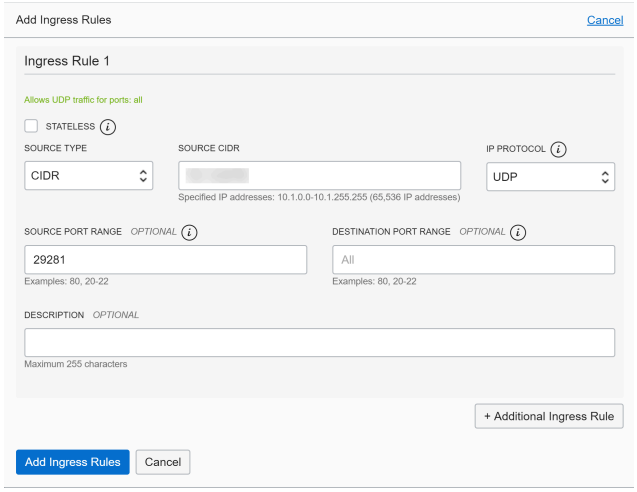
1. 然后，您需要打开 HA1 接口的端口。
    1. 在 OCI 控制台中，选择 **Networking**（网络） > **Virtual Cloud Networks**（虚拟云网络），然后选择 VCN。
    2. 选择 **Subnets**（子网），然后选择包含 HA1 接口的子网。
    3. 选择 **Security Lists**（安全列表），然后单击默认安全列表进行编辑。
    4. 单击 **Add Ingress Rule**（添加入口规则）。
    5. 输入包括 HA 对等 HA1 端口 IP 地址的 **Source CIDR**（源 **CIDR**）。
    6. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **TCP**。
    7. 单击 **+Additional Ingress Rule**（+其他入口规则）。您需要为 TCP 端口 28260 和 28769 创建两个其他规则。
    8. 如果在 VM 系列防火墙上为 HA1 链路启用加密，则应为 ICMP 和 TCP 端口 28 创建其他规则。
    9. 单击 **Add Ingress Rule**（添加入口规则）。



2. 打开 HA2 接口的端口。
    1. 在 OCI 控制台中，选择 **Networking**（网络） > **Virtual Cloud Networks**（虚拟云网络），然后选择 VCN。
    2. 选择 **Subnets**（子网），然后选择包含 HA2 接口的子网。
    3. 选择 **Security Lists**（安全列表），然后单击默认安全列表进行编辑。
    4. 单击 **Add Ingress Rule**（添加入口规则）。
    5. 输入包括 HA 对等 HA2 端口 IP 地址的 **Source CIDR**（源 **CIDR**）。
    6. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **UDP** 或 **IP**。
    7. 如果传输模式为 UDP，请在 **Source Port Name**（源端口名称）中输入 **29281**。如果传输模式为 IP，请在 **Source Port Name**（源端口名称）中输入 **99**。

©2024 Palo Alto Networks, Inc.

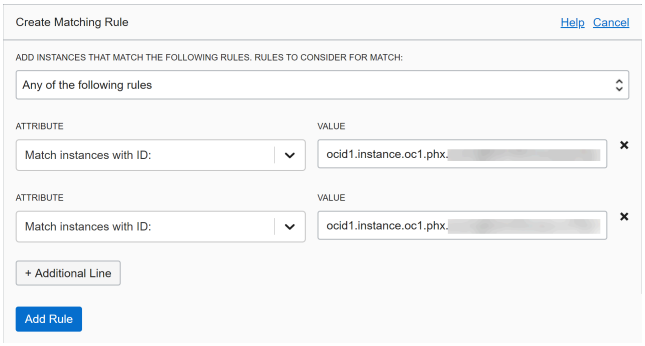
8. 单击 **Add Ingress Rule**（添加入口规则）。



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 将两个 HA 对等添加到动态组，并创建允许 HA 对等移动浮动 IP 地址的策略。您必须拥有每个 HA 对等实例的 OCID 才能构建动态组匹配规则，因此必须将这些规则传递到规则构建器中。

1. 创建动态组。
   1. 在 OCI 控制台中，选择 **Identity**（标识） > **Dynamic Groups**（动态组） > **Create Dynamic Group**（创建动态组）。
   2. 输入动态组的描述性 **Name**（名称）。
   3. 单击 **Rule Builder**（规则构建器）。
   4. 从第一个下拉列表中选择 **Any of the following rules**（以下任何规则）。
   5. 从 **Attributes**（属性）下拉列表中选择 **Match instances with ID:**（匹配具有 **ID** 的实例：），然后将其中一个对等 OCID 复制到 **Value**（值）字段中。
   6. 单击 **+Additional Line**（+其他行）。
   7. 从 **Attributes**（属性）下拉列表中选择 **Match instances with ID:**（匹配具有 **ID** 的实例：），然后将另一个对等 OCID 复制到 **Value**（值）字段中。
   8. 单击 **Add Rule**（添加规则）。

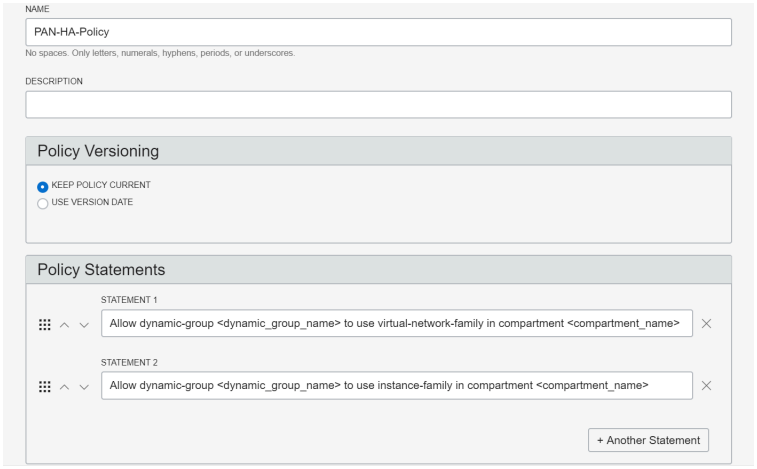


   9. 单击 **Create Dynamic Group**（创建动态组）。
2. 创建策略规则。
   1. 在 OCI 控制台中，选择 **Identity**（标识） > **Policies**（策略） > **Create Policy**（创建策略）。
   2. 输入策略的描述性 **Name**（名称）。
   3. 输入第一个策略声明。

      Allow dynamic-group *<dynamic_group_name>* to use virtual-network-family in compartment *<compartment_name>*
   4. 单击 **+Another Statement**（+另一个声明）。
   5. 输入第二个策略声明。

      Allow dynamic-group *<dynamic_group_name>* to use instance-family in compartment *<compartment_name>*
   6. 单击 **Create**（创建）。

©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 配置防火墙上的接口。您必须为不可信和可信接口配置 HA2 数据链路和至少两个第 3 层接口。在第一个 HA 对等上完成此工作流程，然后在第二个 HA 对等上重复这些步骤。

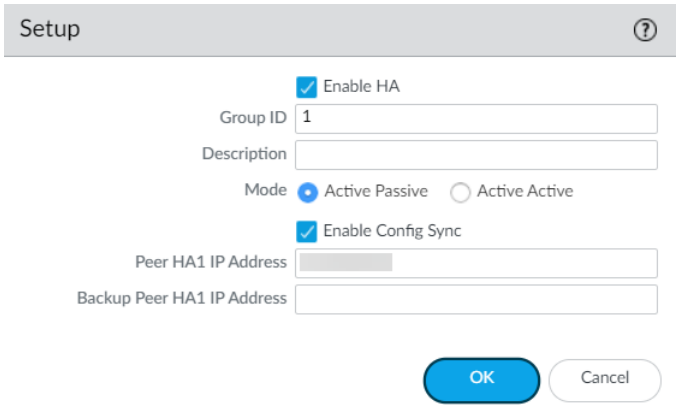
1. 登录到防火墙 Web 界面。
2. （可选）如果您将管理接口用作 HA1 接口，则必须将接口 IP 类型设置为静态并配置 DNS 服务器。
   1. 选择 **Device**（设备） > **Setup**（设置） > **Interfaces**（接口） > **Management**（管理）。
   2. 将 **IP Type**（**IP** 类型）设置为 **Static**（静态）。
   3. 输入 VM 系列防火墙实例的主要 VNIC 的专用 **IP address**（**IP** 地址）。
   4. 单击 **OK**（确定）。
   5. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务）。
   6. 单击 **Edit**（编辑）。
   7. 输入 **Primary DNS Server**（主 **DNS** 服务器）的 IP 地址。
   8. 单击 **OK**（确定）。
   9. **Commit**（提交）更改。
3. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后单击不可信接口。在本例中，HA2 接口为 1/1，可信接口为 ethernet 1/2，不可信接口为 ethernet 1/3。
4. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**HA**
5. 单击 **ethernet 1/2** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 trust-zone），然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **Static**（静态）。
   - 在 IP 部分单击 **Add**（添加），然后输入接口的主要 IP 地址和网络掩码。确保 IP 地址与分配给 VCN 中相应子网的 IP 地址相匹配。例如，如果将此接口添加到可信区域，请确保分配 VCN 中配置的可信 vNIC IP 地址。
   - 在 IP 部分中单击 **Add**（添加），然后输入辅助浮动 IP 地址和网络掩码。
6. 单击 **ethernet 1/3** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 untrust-zone），然后单击 **OK**（确定）。
   - 在 **IPv4** 选项卡上，选择 **Static**（静态）。

©2024 Palo Alto Networks, Inc.

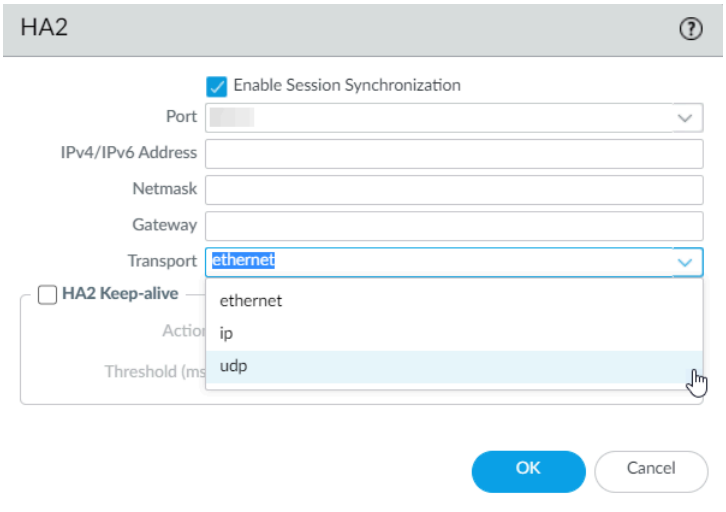
- 在 IP 部分单击 **Add**（添加），然后输入接口的主要 IP 地址和网络掩码。确保 IP 地址与分配给 VCN 中相应子网的 IP 地址相匹配。例如，如果将此接口添加到不可信区域，请确保分配 VCN 中配置的不可信 vNIC IP 地址。
- 在 IP 部分中单击 **Add**（添加），然后输入辅助浮动 IP 地址和网络掩码。

STEP 5 | 启用 HA。

1. 选择 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）。
2. 编辑 Setup（设置）设置。
3. 在 **Peer HA1 IP address**（对等 **HA1 IP** 地址）字段中输入被动对等的专用 IP 地址。
4. 单击 **OK**（确定）。



5. （可选）编辑控制链路 (HA1)。如果不计划使用管理接口作为控制链接且已添加其他接口（例如 ethernet 1/4），请编辑此部分以选择用于 HA1 通信的接口。
6. 编辑数据链路 (HA2) 以使用 **Port**（端口）ethernet 1/1，并添加主动对等的 IP 地址和子网的 **Gateway**（网关）IP 地址。
7. 从 Transport（传输）下拉列表中选择 **IP** 或 **UDP**。不支持以太网。



8. 单击 **OK**（确定）。

 ©2024 Palo Alto Networks, Inc.

STEP 6 | **Commit**（提交）更改。

STEP 7 | 在被动 HA 对等上重复步骤 4 和步骤 5。

STEP 8 | 在完成两个防火墙的配置 HA 后，验证防火墙是否已在主动/被动 HA 中配对。

1. 访问两个防火墙上的 **Dashboard**（仪表盘），并查看高可用性小部件。
2. 在主动 HA 对等上，单击 **Sync to peer**（同步到对等）。
3. 确认防火墙已配对并同步。
   - 在被动防火墙上：本地防火墙的状态应显示 **Passive**（被动），并且 **Running Config**（运行配置）应显示为 Synchronized（已同步）。
   - 在主动防火墙上：本地防火墙的状态应显示 **Active**（主动），并且 **Running Config**（运行配置）应显示为 Synchronized（已同步）。

©2024 Palo Alto Networks, Inc.

在 Alibaba Cloud 上设置 VM 系列防火墙

在 Alibaba Cloud 上部署 VM 系列防火墙可以保护您在 Alibaba Cloud 中创建的网络。您可以部署 VM 系列防火墙来保护面向 Internet 的应用程序和混合云部署。

- Alibaba Cloud 上的 VM 系列防火墙
- Alibaba Cloud 上 VM 系列防火墙的最低系统要求
- 准备在 Alibaba Cloud 上部署 VM 系列防火墙
- 在 Alibaba Cloud 上部署 VM 系列防火墙

Alibaba Cloud 上的 VM 系列防火墙

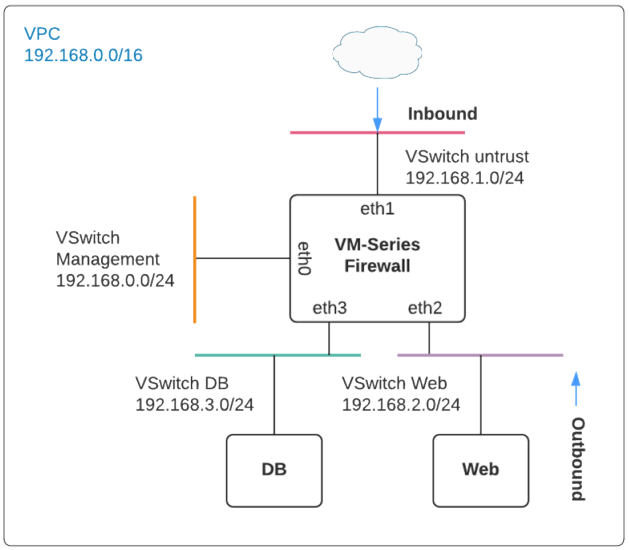
您可以部署 VM 系列防火墙以保护 Alibaba Cloud 中的入站和出站北向南流量。

不支持在同一 *VPC* 中保护东向西流量，因为 *Alibaba Cloud* 不支持子网路由。

当您选择有足够资源的 Alibaba Cloud 实例时，Alibaba Cloud 上的 VM 系列防火墙在 KVM 虚拟机监控程序上运行，并且支持多达 8 个网络接口（请参阅Alibaba Cloud 上 VM 系列防火墙的最低系统要求）。

Alibaba Cloud 上的 VM 系列防火墙在 Alibaba Cloud 国际区域和中国大陆上支持 BYOL 许可证和 VM 系列 ELA。目前不支持 PAYG 许可证。

在 Alibaba Cloud 中，VPC 可逻辑隔离虚拟网络。创建 VPC 后，您可以创建 VSwitch 以进一步细分虚拟专用网络，如下图所示。要保护入站流量，必须在防火墙上配置 DNAT 和 SNAT。



来自 VPC 外部客户端的入站流量将进入 VM 系列防火墙不可信接口。防火墙检查流量并通过可信接口将其发送到应用程序。从应用程序返回的流量必须通过 VM 系列防火墙可信接口，防火墙在该接口上检查返回流量并通过不可信接口将其发送出去。

出站流量通常来自外部应用程序。通常，会将面向 VPC 内的流量的 Internet 路由到 NAT 网关（附有 EIP）。为此，请在 VPC 路由表中添加默认网关路由，并将应用程序子网的 VM 系列防火墙 IP 地址设置为下一个跃点。使用不可信接口 IP 配置 SNAT，以确保来自 Internet 的流量通过 VM 系列防火墙返回。

有关配置示例，请参阅确保 Alibaba Cloud 的北向南流量安全。

©2024 Palo Alto Networks, Inc.

Alibaba Cloud 上 VM 系列防火墙的最低系统要求

在 Alibaba Cloud 上，您可以在 KVM 虚拟机监控程序上部署 VM 系列防火墙（参阅VM 系列部署）。

- VM 系列防火墙软件要求
- VM 系列防火墙的 Alibaba Cloud 实例类型建议
- Alibaba Cloud CLI

VM 系列防火墙软件要求

确保您拥有在 Alibaba Cloud 上完成 VM 系列部署所需的软件和许可证。

- 要在 Alibaba Cloud 上部署 VM 系列防火墙，您必须使用从 Alibaba Marketplace 获取的 VM 系列映像。该映像包含 PAN-OS 版本 10.0.3 和 VM 系列插件版本 2.0.3。
- 在部署之前，请选择 VM 系列 ELA 或 BYOL 许可证、容量许可证和订阅套餐。请参阅VM 系列型号许可证类型。
- 您必须能够通过 SSH 登录到 VM 系列防火墙以完成部署。如果您的操作系统不支持 SSH，请安装第三方软件，例如 Putty。

VM 系列防火墙的 Alibaba Cloud 实例类型建议

在创建 VM 系列防火墙之前，您必须选择支持适用于您的 VM 系列型号最低系统要求的弹性计算服务 (ECS) 实例类型。检查实例类型文档以确保 ECS 实例类型具有保护网络配置的资源。

VM 系列型号	弹性计算服务实例类型
VM-100，软件 NGFW 积分	ecs.g5.xlarge、ecs.sn2ne.xlarge、ecs.g7ne.xlarge
VM-300，软件 NGFW 积分	ecs.g5.xlarge、ecs.sn2ne.xlarge、ecs.g7ne.2xlarge
VM-500，软件 NGFW 积分	ecs.g5.2xlarge, ecs.sn2ne.2xlarge, ecs.g7ne.2xlarge
VM-700软件 NGFW 积分	ecs.g5.4xlarge、ecs.sn2ne.4xlarge、ecs.g7ne.4xlarge
软件 NGFW 积分	g7ne 实例系列

Alibaba Cloud CLI

Aliyun 版本 3.0.4 或更高版本。请参阅准备使用 Aliyun 命令行界面。

©2024 Palo Alto Networks, Inc.

准备在 Alibaba Cloud 上部署 VM 系列防火墙

此任务使用 Aliyun CLI 为 VM 系列防火墙创建 VPC 和 VSwitch，但是，您应该在开始之前规划网络。评估要保护的应用程序，并确定部署 VM 系列防火墙以检查和保护北向南流量的位置。

- 选择许可证和计划网络
- 准备使用 Aliyun 命令行界面

选择许可证和计划网络

评估保护所需的应用程序并创建允许 VM 系列防火墙检查入站和出站应用程序流量的网络。

STEP 1 | 规划和设计 VPC。

1. 为您的 VPC 和 VSwitch 规划网络，包括 CIDR 块。

   有关示例过程，请参阅创建 VPC 并配置网络。
2. 规划 IP 地址。如果需要特定的地址或地址范围，请参阅弹性 IP 地址用户指南。
3. 规划安全组织。

STEP 2 | 评估您的应用程序和网络配置，并计算保护应用程序和网络所需的防火墙容量。

STEP 3 | 获取 VM 系列防火墙许可证。

虽然您不需要许可证来安装 VM 系列防火墙（您可以在安装后激活许可证），但您必须在部署防火墙之前选择合适的 VM 系列型号和 ECS 实例类型。

1. 选择一个 VM 系列型号。

   VM 系列防火墙最多支持 *8* 个接口，前提是 *VM* 系列型号和 *Alibaba Cloud* 实例有足够的资源。您可以使用型号

   使用所选的 VM 系列型号 来选择 VM 系列防火墙的 Alibaba Cloud 实例类型建议 之一。
2. 选择满足您的需求的 VM 系列容量许可证。
3. 购买 BYOL 订阅套餐（如果还没有）。您会收到 VM 系列订阅的授权代码，并且必须在部署过程中提供该授权代码。

STEP 4 | 规划如何配置 Alibaba 帐户和权限以访问 VM 系列防火墙。首先，请参阅安全常见问题解答，然后了解有关实例 RAM 角色的更多信息。

准备使用 Aliyun 命令行界面

本章将重点介绍 ECS 控制台，但是，您在 ECS 控制台中执行的所有操作都可以从 Aliyun 命令行界面完成。如果您想使用 VM 系列防火墙来保护 Alibaba Cloud 上的负载均衡，则需要 CLI。

安装和配置最新版本的 Aliyun，则需要 Alibaba Cloud 命令行界面。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建一个 AccessKey，并将访问密钥 ID 和密钥保存在安全位置。

STEP 2 | 从 https://github.com/aliyun/aliyun-cli 下载 Aliyun 的 支持版本。

STEP 3 | 安装 Aliyun。

STEP 4 | 配置 Alibaba Cloud。

配置会提示输入访问密钥信息和其他信息。

如果部署使用存储桶，则地区必须与存储桶的地区匹配。

```
aliyun configure Configuring profile '' in '' authenticate
 mode...Access Key Id [*************8rq]: *************8rq
 Access Key Secret [***************************tM2]:
 ***************************tM2 Default Region Id [us-west-1]:
 us-west-1 Default Output Format [json]: json (Only support
 json)) Default Language [zh|en] en: en Saving profile[] ...Done.
 available regions: ...
```


©2024 Palo Alto Networks, Inc.

在 Alibaba Cloud 上部署 VM 系列防火墙

VM 系列防火墙假设至少有三个接口：管理、不可信和可信。创建 Alibaba Cloud VPC 时，它在逻辑上是隔离的。要将虚拟专用网络划分为子网，可以创建 vSwitch，每个都有自己的 CIDR 块。由于 VM 系列防火墙具有多个接口，因此，可以检查所有子网上的流量。

通常，外部入站流量遇到 VM 系列防火墙的不可信接口。防火墙检查入站流量并通过可信接口将其发送到应用程序。应用程序的返回流量进入防火墙的可信接口，防火墙在该接口上检查返回流量并通过不可信接口将其发送出去。

以下任务演示如何使用控制台创建 VM 系列防火墙基础架构。

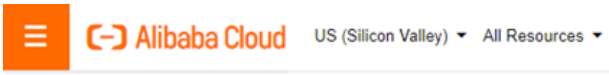
- 创建 VPC 并配置网络
- 创建和配置 VM 系列防火墙
- 确保 Alibaba Cloud 的北向南流量安全
- 在 Alibaba Cloud 上配置负载均衡

创建 VPC 并配置网络

使用 Alibaba Cloud 控制台创建 VPC、VSwitch、安全组和安全组规则。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 打开 VPC 控制台并从菜单中选择所在的区域。请注意，您选择的区域必须提供 Palo Alto Networks 支持的实例类型之一。



STEP 2 | 在 Alibaba Cloud 控制台主页上，选择**Products and Services**（产品和服务） > **Networking**（网络） > **Virtual Private Cloud**（虚拟私有云）。

STEP 3 | **Create a VPC**（创建 **VPC**）。

在此步骤中，您将创建一个 VPC 和管理、不可信和可信 VSwitch。ECS 控制台使用相同的形式创建 VPC 和交换机。

1. 选择 **Create VPC**（创建 **VPC**）。

   指定 VPC 名称、IPv4 CIDR 块和描述。请参阅创建 VPC。

属性	值
名称	您的选择。
IPV4 CIDR 块	您的选择。请参阅 CIDR 块常见问题解答。

©2024 Palo Alto Networks, Inc.

属性	值
资源组	您的选择。

2. 选择 **Create VSwitch**（创建 **VSwitch**）。
   - 命名 VSwitch 为 **`Management`**。
   - 选择 **Zone**（区域），指定 **IPv4 CIDR Block**（**IPv4 CIDR** 块）（该块是您为 VPC 指定的块的子网），然后指定 **Description**（说明）。
   - 单击底部的 **Add**（添加）以添加其他 VSwitch（请勿单击 **OK**（确定），直到您已添加所有 VSwitch）。

   请参阅创建 VSwitch。
3. 以相同的方式 **Add**（添加）不可信 VSwitch。
4. **Add**（添加）可信 VSwitch。
5. 单击 **OK**（确定）。

   查看 VPC 详细信息并进行任何更改，然后单击 **Complete**（完成）。

STEP 4 | 创建安全组和安全组规则。

- 在 Alibaba Cloud 控制台主页上，选择**Elastic Compute Service**（弹性计算服务） > **Networking & Security**（网络和安全） > **Security Groups**（安全组）。
- 单击右上角的 **Create Security Group**（创建安全组）。

1. 创建管理安全组。

   请参阅创建安全组以填写以下字段。

属性	值
模板	自定义
安全组名称	管理
安全组类型	基础
网络类型	VPC
VPC	选择之前创建的 VPC。

©2024 Palo Alto Networks, Inc.

属性	值
资源组	您的选择。

- 填写表单，然后单击 **OK**（确定）。

  ECS 控制台会提示为此安全组创建规则。此任务介绍可用于启动 VM 系列防火墙的一些基本安全组规则。您可以创建更多规则来强制执行网络安全要求。

2. 选择 **Create Rules Now**（立即创建规则），然后为 HTTPS 和 SSH 创建规则。

   选择 Inbound（入站）选项卡，然后单击 **Add Security Group Rule**（添加安全组规则）。

   - 创建入站规则以允许此安全组中的 HTTPS。例如：

属性	值
规则方向	入站
操作	允许
协议类型	HTTPS (443)
优先级	100
授权类型	请参阅添加安全组规则。
授权对象	

   - 单击 **Add Security Group Rule**（添加安全组规则）以创建入站规则，从而允许在管理接口上使用 SSH。

属性	值
规则方向	入站
操作	允许
协议类型	自定义 TCP
端口范围	1/65535
授权类型	请参阅添加安全组规则。
授权对象	

   单击 **OK**（确定），然后选择 **Back**（返回）以返回安全组页面。

©2024 Palo Alto Networks, Inc.

3. 选择 **Create Security Group**（创建安全组）并创建不可信安全组。

   出现提示时，为不可信安全组创建规则。

属性	值
规则方向	入站
操作	允许
协议类型	自定义 TCP
端口范围	1/65535
优先级	100
授权类型	请参阅添加安全组规则。
授权对象	

   单击 **OK**（确定），然后选择 **Back**（返回）以返回安全组页面。

4. 创建可信安全组。

   出现提示时，单击 **Add Security Group Rule**（添加安全组规则），然后复制不可信规则。

   继续阅读创建和配置 VM 系列防火墙。

创建和配置 VM 系列防火墙

此任务使用 ECS 控制台创建至少具有三个接口的 VM 系列防火墙实例：管理、不可信和可信。默认情况下，ECS 实例支持单个 NIC，并自动为其附加弹性网络接口 (ENI)。要支持 VM 系列防火墙，必须单独创建不可信和可信弹性网络接口 (ENI) 并将它们附加到您的实例。

STEP 1 | 在 Alibaba Cloud 控制台主页上，选择**Elastic Compute Service**（弹性计算服务） > **Instances & Images**（实例和映像） > **Instances**（实例），然后单击右上角的 **Create Instance**（创建实例）。

STEP 2 | 选择 **Custom Launch**（自定义启动）。

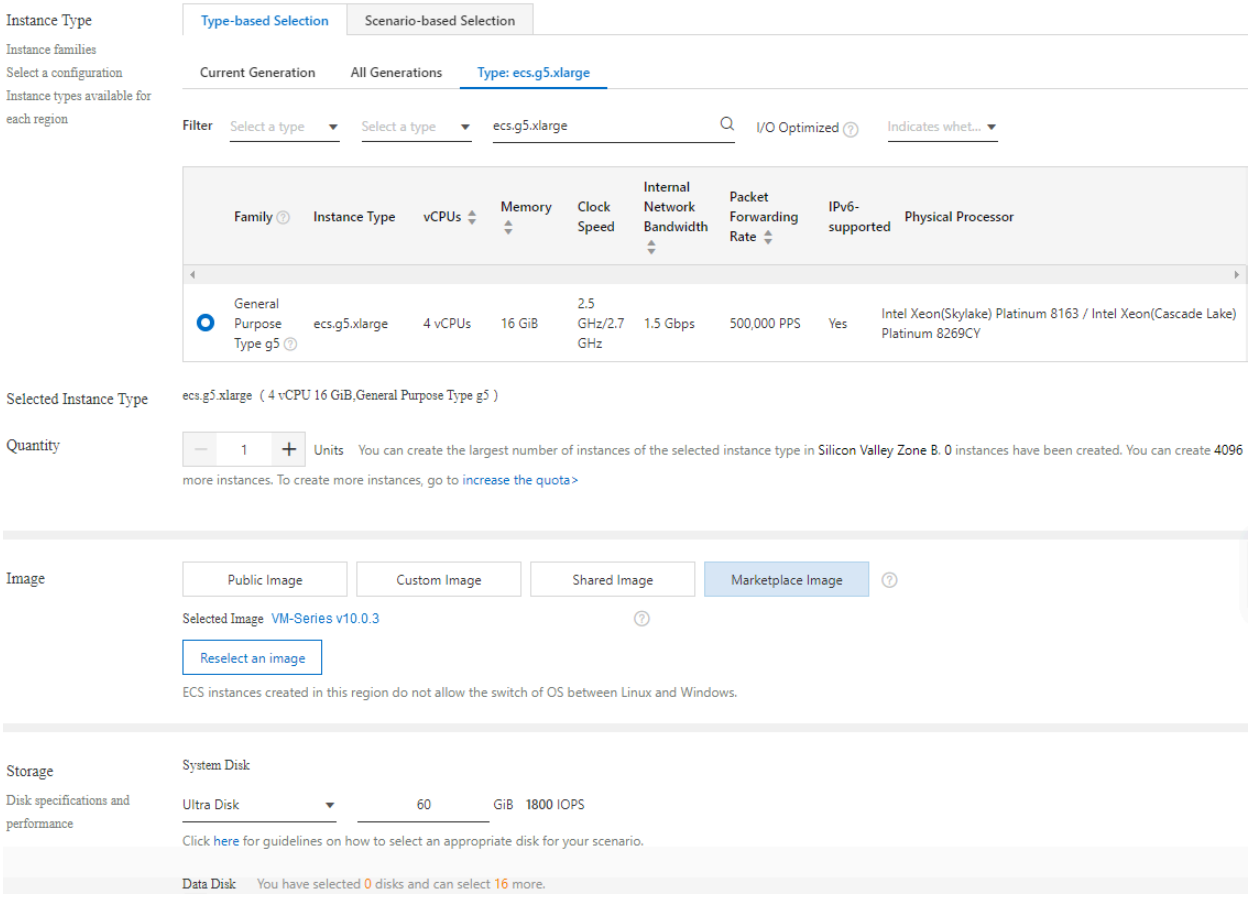
STEP 3 | 基本配置。

1. 填写以下值。例如：

属性	值
计费方式	订阅。

©2024 Palo Alto Networks, Inc.

属性	值
区域	您的选择。您也可以选择地区。您选择的区域必须提供所需的实例类型之一。
实例类型	VM 系列防火墙的 Alibaba Cloud 实例类型建议中的一种类型。您可以使用基于类型的选择来搜索实例类型。
映像	选择 **Marketplace Image**（**Marketplace** 映像），然后在 Alibaba Marketplace 中搜索“VM 系列”。该映像组合了 OS 和 VM 系列防火墙。
存储	选择磁盘类型并指定 60 GB。
快照	您的选择。
持续时间	您的选择。



2. 选择 **Next:Networking**（下一步：网络）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 在 Networking（网络）页面上，提供以下值。

1. 网络（选择 VPC）。
   - 选择在创建 VPC 并配置网络 中创建的 VPC。
   - 选择管理 VSwitch。
2. 公共 IP 地址。

   如果没有公共 IP 地址，可以启用 **Assign Public IP address**（分配公共 **IP** 地址），系统将分配一个地址。如果必须使用特定 IP 地址或特定范围内的地址，则可以请求自定义 IP 地址。请参阅弹性 IP 地址用户指南。
3. 安全组。

   选择管理安全组。
4. 弹性网络接口。

   管理界面已附加到 eth0。
5. 选择 **Next:System Configurations**（下一步：系统配置）。

STEP 5 | 在 System Configurations（系统配置）页面上，填写以下值。

1. 登录凭据：选择 **Key Pair**（密钥对）。

   不支持密码身份验证。
2. 命名 VM 系列防火墙实例并提供主机名。

   完成所有更正。

   选择 **Preview**（预览）以查看到目前的设置。
3. 关注 **Advanced (based or instance RAM roles or cloud-init)**（高级（基于或实例 **RAM** 角色或 **cloud-init**）），然后单击 **Show**（显示）。
   - RAM 角色为可选。
   - 在 User Data（用户数据）字段中，输入基本引导信息作为键值对，用换行符分隔。请参阅输入基本配置作为用户数据（公共云）。例如，在 **User Data**（用户数据）字段中输入以下内容。

```
type=dhcp-client hostname=Ca-FW-DC1 vm-auth-
key=7550362253**** panorama-server=10.*.*.20 panorama-
server-2=10.*.*.21 tplname=FINANCE_TG4 dgname=finance_dg op-
cmd-dpdk-pkt-io=on dhcp-send-hostname=yes dhcp-send-client-
id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes authcodes=I7115398 vm-series-auto-registration-
```


©2024 Palo Alto Networks, Inc.

```
pin-id=abcdefgh1234**** vm-series-auto-registration-pin-
value=zyxwvut-0987****
```

> ***op-command-modes*** *(mgmt-interface-swap and jumbo frame)* 不支持 *Alibaba Cloud*。
>
> ***op-cmd-dpdk-pkt-io=on*** 支持 *DPDK*。如果要指定 *PacketMMAP*，请指定 *op-cmd-dpdk-pkt-io=off*。

分组为可选。在订购之前，请选择 **Preview**（预览）以查看配置。

STEP 6 | 查看服务条款，然后选择 **Create Order**（创建订单）以创建 VM 系列防火墙实例。

查看采购订单，然后选择 **Subscribe**（订阅）。

STEP 7 | 在控制台主页上，选择 > **Elastic Compute Service**（弹性计算服务） > **Networks and Security**（网络和安全） > **ENI**，然后选择 **Create ENI**（创建 **ENI**）。为不可信和可信接口创建弹性网络接口。

1. 创建不可信 ENI。

   在 **Actions**（操作）列中，选择 **Bind to Instance**（绑定到实例），然后选择您刚创建的实例。

2. 创建可信 ENI 并将其绑定到实例。

STEP 8 | 分配弹性 IP (EIP) 地址。

为 VM 系列防火墙管理界面和不可信网络接口分配 EIP 地址。在此示例中，可信接口未向 Internet 公开，因此，您不需要第三个 IP 地址。

如果您已有两个 EIP，请转到下一步。

1. 将 EIP 与 VM 系列防火墙管理接口相关联。
2. 将 EIP 与 VM 系列防火墙不可信网络接口关联。

   您连接的第二个接口将分配给 VM 系列防火墙上的网络接口 1。

STEP 9 | 重新启动实例以附加新的网络接口。

在实例列表中，选择实例并选择 **Manage**（管理），然后选择右上角的 **Restart**（重新启动）。

STEP 10 | 使用安全密钥通过 SSH 登录到 VM 系列防火墙，并设置管理员密码：

```
developer1$ ssh -i dev1-vpc1.pem admin@18.***.145.153
 Welcome admin. admin> configure Entering configuration
 mode [edit] admin# set mgt-config users admin password
 Enter password:<password>Confirm password:<password> [edit]
 admin# commit
```

STEP 11 | 访问 VM 系列防火墙 Web 界面。

打开 Web 浏览器，输入管理接口的 EIP。

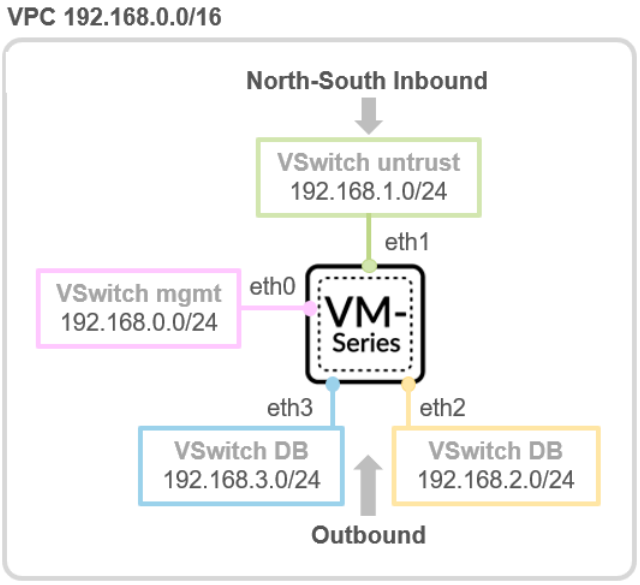
©2024 Palo Alto Networks, Inc.

确保 Alibaba Cloud 的北向南流量安全

创建 VPC 后，您可以创建 VSwitch 以将虚拟专用网络划分为子网。此示例包含具有 CIDR 192.168.0.0/16 的 VPC；您可以输入自己的值。四个 VSwitch 创建四个子网。

VSwitch 名称	接口	示例 CIDR
mgmt	eth0	192.168.0.0/24
不可信	eth1	192.168.1.0/24
web	eth2	192.168.2.0/24
db	eth3	192.168.3.0/24

在下图中，VM 系列防火墙可以连接到两个可信子网：Web 和 DB。当外部客户端访问 VM 系列防火墙的不可信接口时，将启动入站流量。防火墙检查流量并将其发送到应用程序。例如，防火墙通过可信接口将流量发送到 Web 服务器。从 Web 服务器返回的流量必须到达 VM 系列防火墙的可信接口。防火墙检查返回流量，并通过不可信接口发送出去。



要保护入站流量，必须在防火墙上配置 DNAT 和 SNAT。

STEP 1 | 为入站流量创建 NAT 规则。

以下是入站流量保护的 NAT 规则示例。

```
            <nat> <rules> <entry name="inbound_web"> <source-
translation> <dynamic-ip-and-port> <interface-address>
 <interface>ethernet1/2</interface> </interface-address>
 </dynamic-ip-and-port> </source-translation> <destination-
translation> <translated-address>web_server</translated-address>
 </destination-translation> <to> <member>untrust</member> </to>
```


©2024 Palo Alto Networks, Inc.

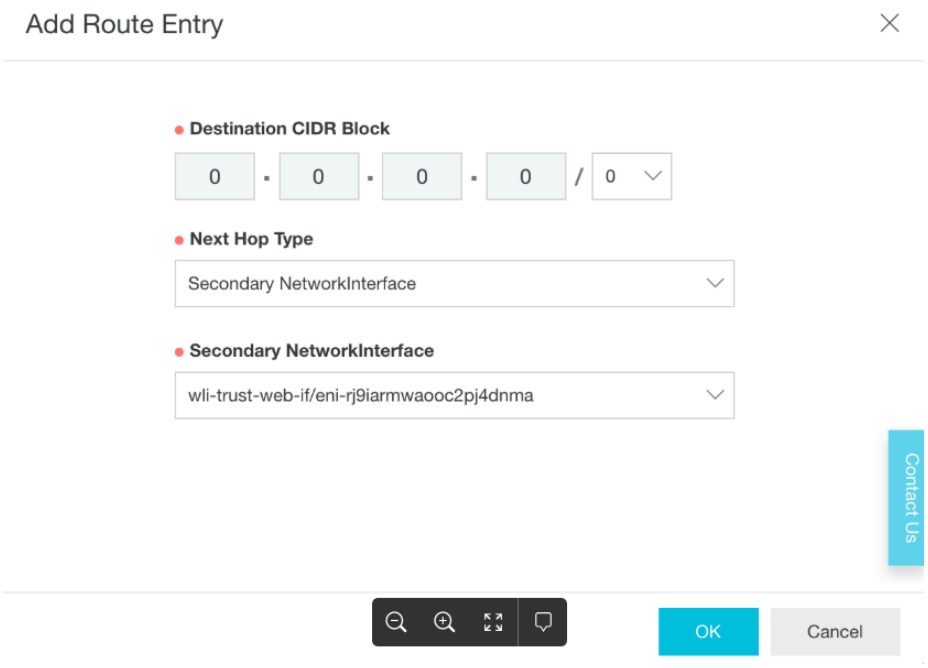
```
 <from> <member>any</member> </from> <source> <member>any</member>
 </source> <destination> <member>fw_untrust</member> </destination>
 <service>any</service> <to-interface>ethernet1/1</to-interface>
 </entry> </rules> </nat> <address> <entry name="fw_untrust"> <ip-
netmask>192.168.1.4</ip-netmask> </entry> <entry name="fw_trust">
 <ip-netmask>192.168.2.201</ip-netmask> </entry> <entry
 name="web_server"> <ip-netmask>192.168.2.203</ip-netmask> </entry>
 </address>
```


©2024 Palo Alto Networks, Inc.

STEP 2 | 保护出站流量。

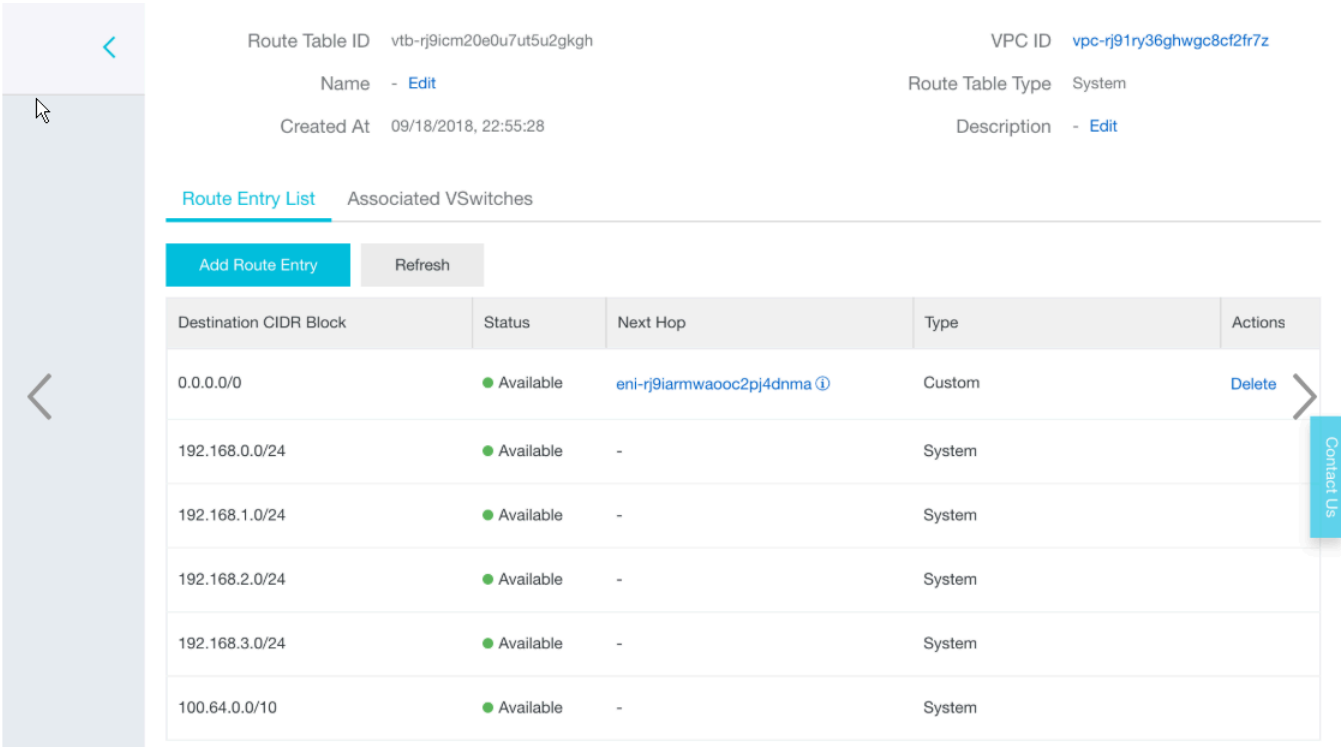
如上图所示，应用程序启动出站流量。例如，Web 服务器必须运行 **`yum install`** 以更新 rpm 数据包。通常，面向 VPC 内的流量的 Internet 被路由到 NAT 网关（附有 EIP）。要保护出站流量，必须强制出站流量通过 VM 系列防火墙。

1. 在 VPC 路由表中添加默认网关路由，并在 Web 服务器的子网中将防火墙 IP 设置为下一个跃点。



2. 在路由表中查看您的条目。

 ©2024 Palo Alto Networks, Inc.



3. 使用不可信接口 IP 配置 SNAT 规则，以确保从 Internet 返回的流量通过 VM 系列防火墙。

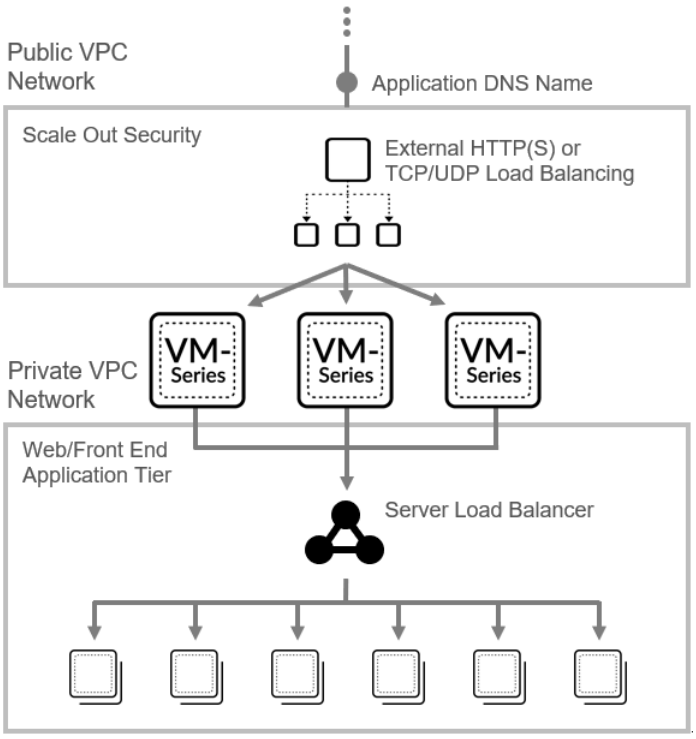
   这是一个 SNAT 配置示例。

```
            <nat> <rules> <entry name="outbound_web">
 <source-translation> <dynamic-ip-and-port> <interface-
address> <interface>ethernet1/1</interface> </interface-
address> </dynamic-ip-and-port> </source-translation> <to>
 <member>untrust</member> </to> <from> <member>trust</member>
 </from> <source> <member>any</member> </source> <destination>
 <member>any</member> </destination> <service>any</service>
 <to-interface>any</to-interface> </entry> </rules> </nat>
```

在 Alibaba Cloud 上配置负载均衡

在 Alibaba Cloud，您可以在负载均衡器三明治配置中部署 VM 系列防火墙，其中防火墙部署在公共网络和专用网络之间，如下所示。

©2024 Palo Alto Networks, Inc.



在创建 VPC 并配置网络中，您创建了不可信和可信 ENI，并将它们作为辅助 ENI 附加到 VM 系列防火墙实例。

使用控制台向 Alibaba 服务器负载均衡器 (SLB) 添加多个后端服务器时，SLB 将流量发送到下一个跃点后端服务器的主 ENI。由于主要 ENI 是管理接口，因此流量必须转到不可信接口（辅助 ENI）进行检查。

要确保 Internet 流量进入数据平面接口而不是管理接口，请使用 Alibaba CLI 将 VM 系列防火墙不可信 ENI 连接到 SLB 实例。

您必须安装 Aliyun 命令行界面才能使用以下 *CLI* 命令。

STEP 1 | 为负载均衡器三明治配置创建公共和专用 VPC，并部署 VM 系列防火墙。

剩下的步骤是您可以根据环境调整的示例 CLI 命令。

STEP 2 | 创建负载均衡器。

```
slb CreateLoadBalancer --RegionId us-west-1 --LoadBalancerName
 wli-slb --VpcId vpc-rj91ry36ghwgc8cf2fr7z --LoadBalancerSpec
 slb.s1.small --AddressType internet --MasterZoneId us-
west-1a --SlaveZoneId us-west-1b { "NetworkType": "classic",
 "LoadBalancerName": "**********", "Address": "**********,
 "ResourceGroupId": "rg-***********ofi", "RequestId":"0B8BA2AA-
E837-****-****-B82A8A1D5FBB", "AddressIPVersion": "ipv4",
 "LoadBalancerId": "lb-*****************mvz", "VSwitchId": "",
 "VpcId": "vpc-*****************r7z" }
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 添加后端服务器。

使用 *CLI* 一次添加一个接口。添加接口的顺序决定了哪个 *NIC* 接收接口。

```
aliyun slb AddBackendServers --LoadBalancerId lb-
**********************mvz --BackendServers '[ { "ServerId":"eni-
**********************bzw", "Type":"eni","Weight":"100" } ]'
```

STEP 4 | 创建一个执行运行状况检查的 HTTP 侦听器。

```
aliyun slb CreateLoadBalancerHTTPListener --LoadBalancerId lb-
**********************mvz --ListenerPort 80 --StickySession on --
HealthCheck on --HealthCheckURI '/'
```


©2024 Palo Alto Networks, Inc.

在 Cisco ACI 中设置防火墙

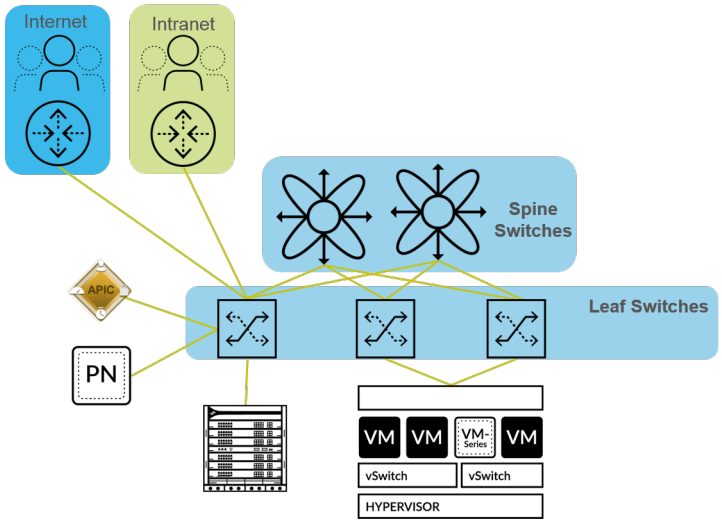
Palo Alto Networks 将服务与 Cisco 以应用为中心的基础架构 (ACI) 集成在一起。ACI 是一种软件定义网络 (SDN) 解决方案，可轻松部署新的工作负载和网络服务。使用名为 Cisco 应用策略基础设施控制器 (APIC) 的 SDN 控制器，您可以在端点组 (EPG) 之间部署防火墙服务。EPG 充当应用程序或应用程序层的容器。在 EPG 之间放置防火墙时，防火墙上配置的安全策略可确保 EPG 之间的通信。APIC 为管理整个数据中心的网络拓扑结构，网络策略和连接提供了一个单一的平台，并支持插入 L4-L7 设备，如基于硬件或 VM 系列的防火墙。Panorama 是集中安全管理所必需的。

- Palo Alto Networks 防火墙与 Cisco ACI 集成
- 准备您的 ACI 环境进行集成
- 在网络策略模式下将防火墙与 Cisco ACI 集成
- Cisco ACI 中的端点监控

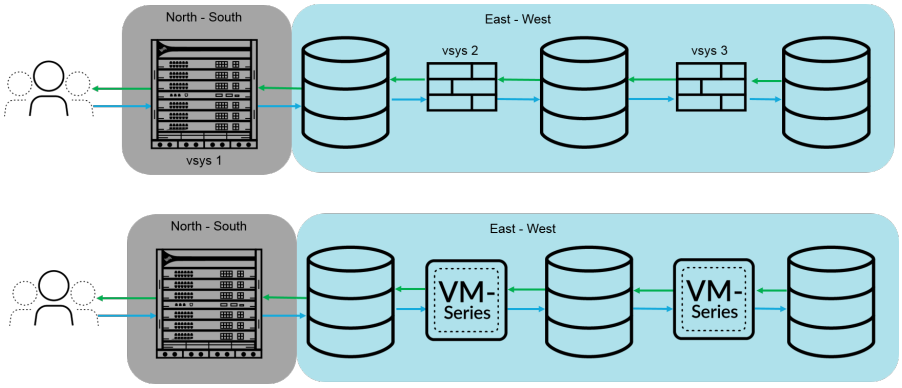
Palo Alto Networks 防火墙与 Cisco ACI 集成

Palo Alto Networks 与 Cisco ACI 的集成允许您在 EPG 之间插入防火墙作为第 4 层到第 7 层服务。然后，防火墙确保这些 EPG 内应用层之间的东向西向流量或用户与应用程序之间的北向南流量。

下图显示包含集成 Palo Alto Network 防火墙的物理 ACI 部署示例。ACI Fabric 中所有的实体都连接到叶子交换机，而那些叶子交换机连接到较大的主干交换机。当用户访问应用程序时，ACI 结构将流量移动到正确的目标。为了保护应用层之间的流量，网络管理员在每个 EPG 之间插入 Palo Alto Networks 防火墙作为 L4 到 L7 的服务，并创建服务图定义 L4 到 L7 设备提供的服务。



防火墙服务部署完成后，现在流量逻辑流向如下所示。与应用程序中的最终用户和每个层进行通信，而不管每个实体在何处或如何物理连接到网络。



当防火墙与 Cisco ACI 集成时，流量将通过基于策略的重定向 (PBR) 发送到防火墙。另外，防火墙的配置与 APIC 的配置是完全独立的。网络策略模式不依赖于防火墙与 APIC 之间的任何其他配置集成，因此它为防火墙的配置和部署提供了更大的灵活性。

对于东向西流量，在防火墙的 ACI 结构中定义网桥域和子网。配置使用 PBR 将流量发送到防火墙的 EPG 之间的合同。PBR 根据包含防火墙 IP 和 MAC 地址的策略将流量转发到防火墙。防火墙接口始终处于第 3 层模式，并接收流量和将其路由回 ACI 结构。您可以为使用者和提供者连接配置单独的接口，也可以为入口和出口流量配置单个接口。本文档中的过程使用单个接口，因为它简化

©2024 Palo Alto Networks, Inc.

了集成；您无需配置同样数量的接口、IP地址或 VLAN。但是，使用单个接口时，不能在定义安全策略时使用区域信息，必须修改防火墙上的默认区域内策略以拒绝流量。

对于北向南流量，必须使用名为 L3Out 的专用策略。L3Out 包含租户连接到外部路由设备和访问外部网络所需的信息。L3Out 连接包含外部网络 EPG，表示可通过 L3Out 策略访问的网络。正如 L3Out 可以将所有外部网络分组到单个 EPG 中一样，您可以使用 vzAny 对象 ACI 来表示 VRF 中的所有 EPG。使用 vzAny 对象简化了出站流量合同的应用，因为每当有新的 EPG 添加到 VRF 时，都会自动应用合同。在这种情况下，外部网络提供合同，vzAny 对象（所有内部 EPG）使用合同。

以下部分介绍有关构成下一代防火墙和 Cisco ACI 之间集成的组件和概念的其他详细信息。

- Service Graph 模板
- 多上下文部署

Service Graph 模板

防火墙通过服务图部署在 Cisco ACI 中。服务图允许您将第 4 层 - 第 7 层设备（如防火墙）集成到流量流中，而无需将 L4-L7 设备作为 ACI 结构中服务器的默认网关。

防火墙在 ACI 结构中表示为 L4-L7 设备，您可以在 APIC 中将其配置为设备集群。将部署为 HA 对的单个防火墙或两个防火墙配置为设备集群。每个设备集群都有一个或多个逻辑接口，用于描述设备集群的接口信息，并使用物理或虚拟机监视器 (VMM) 域中的 VLAN 映射成员防火墙的路径。

Service Graph 模板定义插入到 EPG 之间的流量流中的防火墙设备集群。此外，Service Graph 模板定义防火墙的集成方式以及分配给消费者和提供商 EPG 的逻辑接口。创建 Service Graph 模板后，将其分配给 EPG 和合同。由于 Service Graph 模板与特定 EPG 或合同无关，因此，您可以在多个 EPG 之间重复使用。APIC 随后通过将 Service Graph 模板连接到 EPG 之间的桥接域来部署 Service Graph 模板。

多上下文部署

Cisco ACI 集成支持将物理防火墙划分为由 ACI 作为单独防火墙管理的上下文。在防火墙上，这些上下文是防火墙上的虚拟系统 (vsys)，每个防火墙都被许可支持一定数量的 vsys 实例。在 ACI 中部署多 vsys 防火墙时，您必须在租户中配置机箱管理器并将其分配给防火墙服务。

©2024 Palo Alto Networks, Inc.

准备您的 ACI 环境进行集成

在将防火墙与设备包集成之前，您必须完成以下步骤以准备 Cisco ACI 环境。

STEP 1 | 部署 Panorama。

STEP 2 | 部署防火墙。

- 物理防火墙 — 将防火墙的带外管理端口连接到一个叶子交换机端口，并将至少一个防火墙数据接口连接到交换机。物理防火墙上的防火墙接口配置有 VLAN，以确保连接到正确的网络。根据 平台特定的安装指南部署防火墙。
- VM 系列防火墙 — 为 VM 系列防火墙配置虚拟硬件时，请为管理接口设置端口组。连接到网络的每个 VM 系列防火墙都需要自己的虚拟NIC。部署 VM 系列防火墙 基于您的虚拟机监控程序。

STEP 3 | 在每个防火墙和 Panorama 上配置管理 IP 地址。

执行初始配置：

- 基于硬件的防火墙
- VM 系列防火墙
- Panorama

STEP 4 | 添加防火墙到 Panorama，作为托管设备。

STEP 5 | 在您的防火墙上安装功能许可证。

- 寄存器和激活许可证在您的物理防火墙上。
- VM 系列防火墙上的注册表和激活 VM 系列型号许可证。
- 使用 Panorama管理防火墙许可证。

STEP 6 | 建立 Cisco ACI 结构和管理连接。

作为此配置的一部分，创建一个物理域和 VLAN 名称空间。确保任何物理防火墙的数据接口都是物理域的一部分。

STEP 7 | 创建一个 Cisco ACI VMM 域配置文件。

如果您正在使用虚拟机或 VM 系列防火墙，请为VMware vSphere环境创建虚拟机监控器 (VMM) 域配置文件。VMM 域指定 vSphere 与 ACI 结构之间的连接策略。

©2024 Palo Alto Networks, Inc.

在网络策略模式下将防火墙与 Cisco ACI 集成

在网络策略模式下，通过使用基于策略的重定向到单个逻辑 HA 接口，将高可用性 (HA) 中的一对防火墙集成到东向西或北向南流量中。分别配置防火墙和 ACI 结构，防火墙上的地址对象映射到 ACI 结构中的 EPG。

您可以使用网络策略模式部署 Palo Alto Networks 防火墙以保护东向西向或北向南流量。

- 在网络策略模式下部署防火墙以保护东向西向流量
- 部署防火墙以在网络策略模式下保护北向南流量

在网络策略模式下部署防火墙以保护东向西向流量

以下过程介绍如何使用具有基于策略的重定向的非托管模式部署 Palo Alto Networks 防火墙以保护 Cisco ACI 环境中的东向西向流量。此过程假定您已完成以下操作：

- 防火墙可以运行并连接到 Cisco ACI 环境中的叶子交换机。此外，APIC 必须能够访问每个防火墙的管理接口。
- 防火墙以主动/被动 HA 模式部署。此过程不包括 HA 网络设置，并假设您已提前完成此操作。

要保护东向西流量，在防火墙的 ACI 结构中定义网桥域和子网。配置使用 PBR 将流量发送到防火墙的 EPG 之间的合同。PBR 根据包含防火墙 IP 和 MAC 地址的策略将流量转发到防火墙。防火墙接口始终处于第 3 层模式，并接收流量和将其路由回 ACI 结构。您可以为使用者和提供者连接配置单独的接口，也可以为入口和出口流量配置单个接口。本文档中的过程使用单个接口，因为它简化了集成；您无需配置同样数量的接口、IP地址或 VLAN。但是，使用单个接口时，不能在定义安全策略时使用区域信息，必须修改防火墙上的默认区域内策略以拒绝流量。

此过程以单臂模式部署防火墙。在单臂模式下，流量通过单个接口进入和退出防火墙。此通用防火墙接口用于服务图模板中的使用者和提供者接口。使用单个接口可以减少必须配置的 IP 地址，VLAN 和接口的数量，从而简化与防火墙的集成。但是，单臂部署模型是区域内，因此您无法使用区域信息来定义安全策略。

在防火墙上：

- 创建虚拟路由器和安全区域
- 配置网络接口
- 配置静态默认路由
- 为 EPG 创建地址对象
- 创建安全策略规则

在 Cisco APIC 上：

- 创建 VLAN 池和域
- 为东向西向流量配置 LLDP 和 LACP 的接口策略
- 建立防火墙与 ACI 结构之间的连接

©2024 Palo Alto Networks, Inc.

- 创建 VRF 和桥接域
- 创建 L4-L7 设备
- 创建基于策略的重定向
- 创建和应用 Service Graph 模板

创建虚拟路由器和安全区域

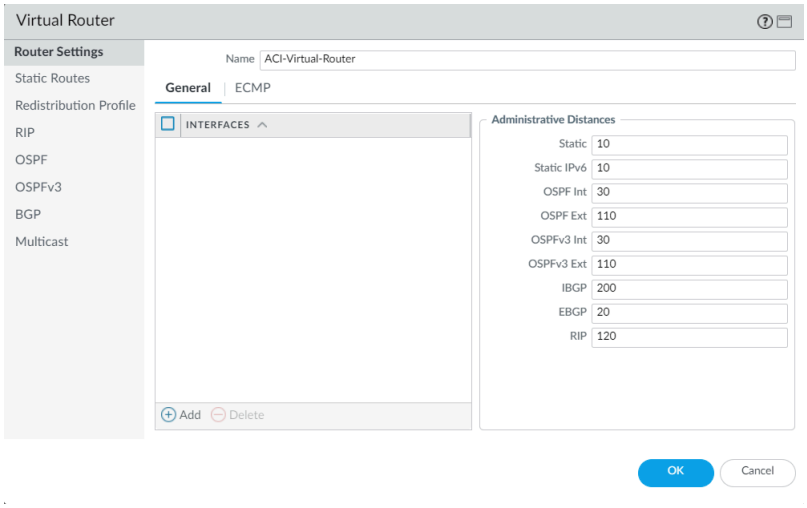
在防火墙上为租户的每个 VRF 配置虚拟路由器和区域。

STEP 1 | 登录到防火墙。

STEP 2 | 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后单击 **Add**（添加）。

STEP 3 | 输入虚拟路由器的描述性 **Name**（名称）。

STEP 4 | 单击 **OK**（确定）。



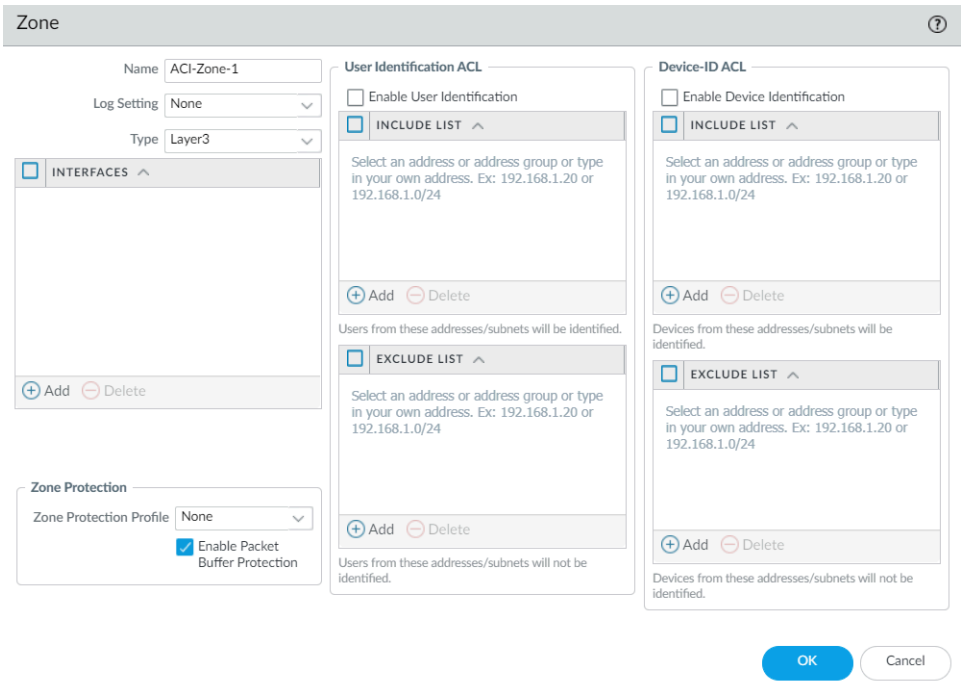
STEP 5 | 选择 **Network**（网络） > **Zones**（区域），然后单击 **Add**（添加）。

STEP 6 | 输入区域的描述性 **Name**（名称）。

STEP 7 | 从 **Type**（类型）下拉列表中选择 Layer 3（第 3 层）。

©2024 Palo Alto Networks, Inc.

STEP 8 | 单击 **OK**（确定）。



STEP 9 | **Commit**（提交）更改。

配置网络接口

配置将防火墙连接到 ACI 叶子交换机的以太网接口。此配置中使用的 VLAN ID 号应该是分配给 ACI 中防火墙的 VLAN 池的成员。

VM 系列防火墙不支持聚合以太网组。

STEP 1 | 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后单击 **Add Aggregate Group**（添加聚合组）。

STEP 2 | 在第二个 **Interface Name**（接口名称）字段中输入聚合组的编号。

STEP 3 | 从 **Interface Type**（接口类型）下拉列表中选择 Layer 3（第 3 层）。

STEP 4 | 选择 **LACP** 选项卡，然后单击 **Enable LACP**（启用 **LACP**）。

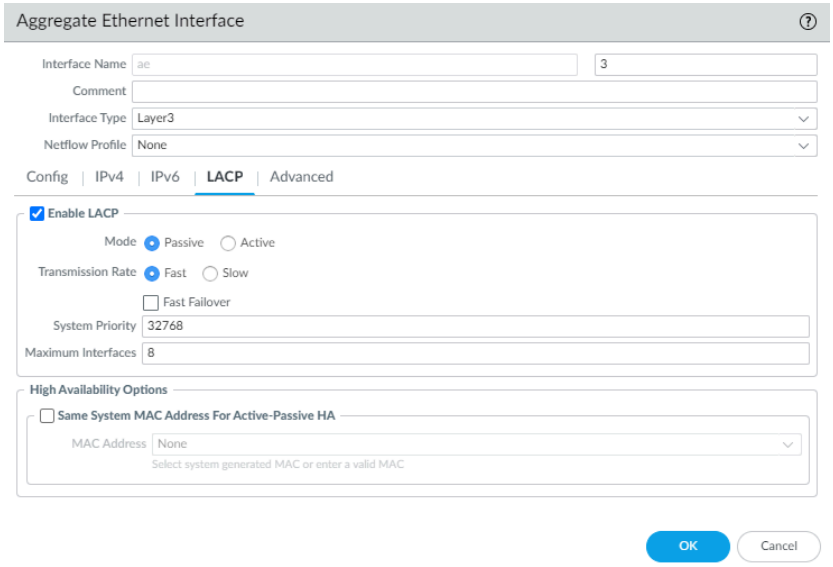
STEP 5 | 选择 **Fast**（快速）作为 **Transmission Rate**（传输速率）。

STEP 6 | 在“高可用性选项”下，选择 **Enable in HA Passive State**（在 **HA** 被动状态下启用）。

不要选择 ***Same System MAC Address for Active-Passive HA***（为主动-被动 ***HA*** 使用相同的系统 ***MAC*** 地址）。此选项使防火墙对显示为交换机的单个设备，因此，流量将流向两个防火墙而不仅仅是主动防火墙。

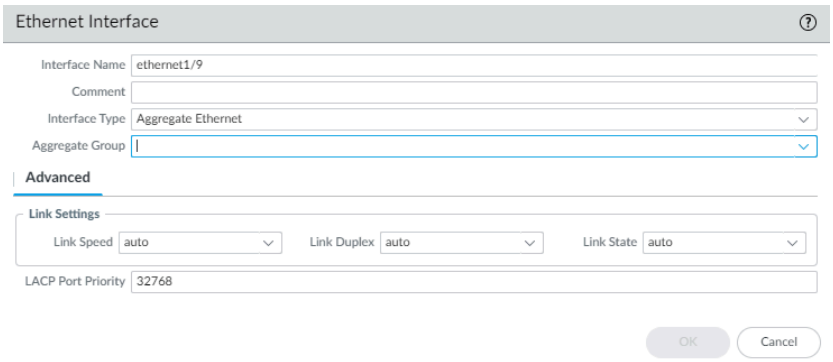
©2024 Palo Alto Networks, Inc.

STEP 7 | 单击 **OK**（确定）。



STEP 8 | 单击以太网接口的名称进行配置，并将其添加到聚合组。

1. 从 Interface Type（接口类型）下拉列表中选择 **Aggregate Ethernet**（聚合以太网）。
2. 选择在聚合以太网组配置中定义的接口。
3. 单击 **OK**（确定）。
4. 对聚合以太网组的每个其他成员接口重复此步骤。



©2024 Palo Alto Networks, Inc.

STEP 9 | 在租户和 VRF 的聚合以太网接口上添加子接口。

1. 选择聚合以太网组的行，然后单击 **Add Subinterface**（添加子接口）。
2. 在第二个 **Interface Name**（接口名称）字段中，输入标识子接口的数字后缀。
3. 在 **Tag**（标记）字段中，输入子接口的 VLAN 标记。
4. 从 **Virtual Router**（虚拟路由器）下拉列表中选择之前配置的虚拟路由器。
5. 从 **Zone**（区域）下拉列表中选择之前配置的区域。
6. 选择 **IPv4** 选项卡。
7. 选择 **Static**（静态）类型。
8. 单击 **Add**（添加）并以 CIDR 表示法输入子接口 IP 地址和网络掩码。
9. 单击 **OK**（确定）。

配置静态默认路由

配置静态默认路由，将以太网子接口的流量引导到子网路由器。

STEP 1 | 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），并单击之前在此步骤中创建的虚拟路由器。

STEP 2 | 选择 **Static Routes**（静态路由） > **IPv4**，然后单击 **Add**（添加）。

STEP 3 | 输入描述性的 **Name**（名称）。

STEP 4 | 在 **Destination**（目标）字段中输入 0.0.0.0/0。

STEP 5 | 从 **Interface**（接口）在下拉列表中，选择之前在此过程中创建的聚合以太网组。

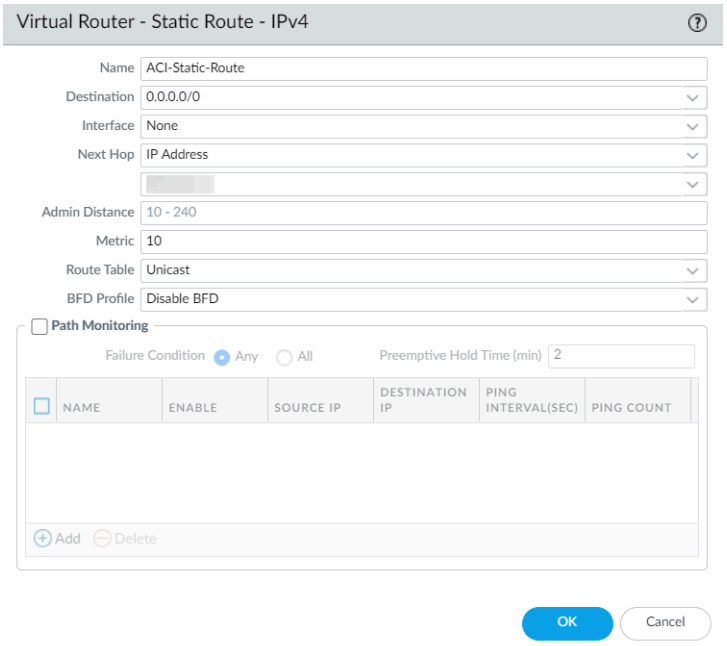
STEP 6 | 从 **Next Hop**（下一个跃点）下拉列表中中选择 IP 地址，并输入下一个跃点路由器的 IP 地址。

STEP 7 | 单击 **OK**（确定）。

STEP 8 | 再次单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

STEP 9 | **Commit**（提交）更改。



为 EPG 创建地址对象

您必须定义地址对象并将其映射到要在安全策略中使用的端点 (EPG)。地址组是使用端点 IP 地址范围将安全组映射到一组服务器的最佳方法。为每个 EPG 创建一个地址对象。

STEP 1 | 选择 **Objects**（对象） > **Address**（地址），然后单击 **Add**（添加）。

STEP 2 | 输入地址对象的描述性名称。

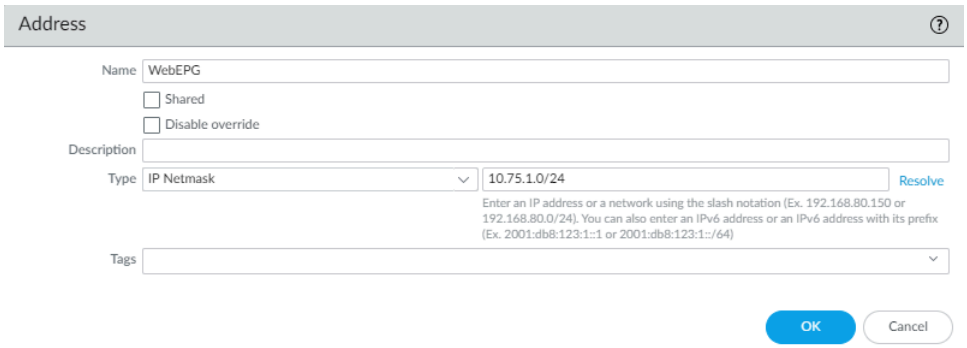
STEP 3 | 从 **Type**（类型）下拉列表中选择 IP 网络掩码。

STEP 4 | 输入 IP 网络掩码。

STEP 5 | 单击 **OK**（确定）。

STEP 6 | 对于每个 EPG，请重复执行此流程。

STEP 7 | **Commit**（提交）更改。



 ©2024 Palo Alto Networks, Inc.

创建安全策略规则

创建安全策略规则以控制在 EPG 之间移动的流量。默认情况下，防火墙允许所有域内流量。因此，由于 EPG 在同一区域中，所以允许这些 EPG 之间的所有 EPG。在创建新规则之前，您将默认的区域内规则从“允许”更改为“拒绝”。

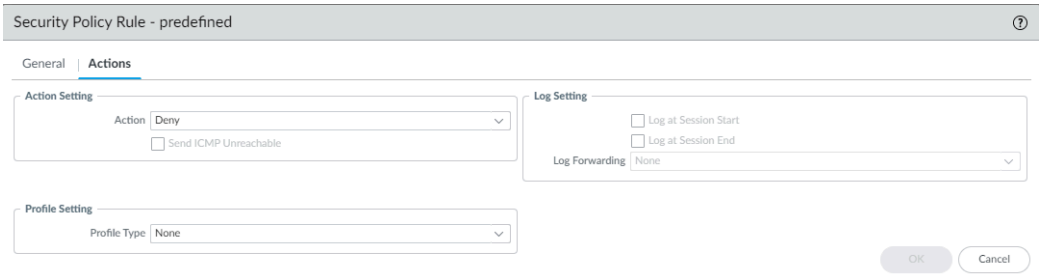
STEP 1 | 选择 **Policies**（策略） > **Security**（安全）。

STEP 2 | 单击“区域内默认”以突出显示该行并单击 **Override**（覆盖）。

STEP 3 | 选择 **Actions**（操作）选项卡。

STEP 4 | 从 **Action**（操作）下拉列表中选择 Deny（拒绝）。

STEP 5 | 单击 **OK**（确定）。



STEP 6 | 根据需要，使用为 EPG 创建的地址对象和区域配置其他安全政策规则。

创建 VLAN 池和域

将接口连接到 EPG 的 ACI 基础架构时，配置将用于为防火墙分配 VLAN 的 VLAN 池。防火墙的 VLAN 池应具有静态 VLAN 范围。

为防火墙配置专用域。需要使用防火墙域将 VLAN 映射到 EPG。为物理防火墙创建物理域，并为 VM 系列防火墙创建 VMM 域。

STEP 1 | 创建 VLAN 池。

1. 登录到 APIC。
2. 选择 **Fabric**（结构） > **Access Policies**（访问策略） > **Pools**（池） > **VLAN**。
3. 右键单击 **VLAN**，然后选择 **Create VLAN Pool**（创建 **VLAN** 池）。
4. 输入 VLAN 池的描述性 **Name**（名称）。
5. 为分配模式选择 **Dynamic Allocation**（动态分配）。
6. 单击 **Encap Blocks**（**Encap** 块）右侧的加号 (+) 按钮。
7. 在 **VLAN Range**（**VLAN** 范围）字段中输入 VLAN 范围。
8. 从 Allocation Mode（分配模式）下拉列表中选择 **Static Allocation**（静态分配）。
9. 单击 **OK**（确定）。
10. 单击 **Submit**（提交）。

©2024 Palo Alto Networks, Inc.

STEP 2 | （Physical firewall only（仅限物理防火墙））创建物理域。

1. 选择 **Fabric**（结构） > **Access Policies**（访问策略） > **Physical and External Domains**（物理和外部域） > **Physical Domains**（物理域）。
2. 右键单击 **Physical Domain**（物理域），然后选择 **Create Physical Domain**（创建物理域）。
3. 输入物理域的描述性 **Name**（名称）。
4. 从 VLAN Pool（VLAN 池）列表中选择在上一过程中创建的 VLAN 池。
5. 单击 **Submit**（提交）。

STEP 3 | （VM-Series firewall only（仅限 VM 系列防火墙））创建 VMM 域。

1. 选择 **Virtual Networking**（虚拟网络） > **VMM Domains**（**VMM** 域） > **VMware**。
2. 右键单击 **VMware**，然后选择 **Create vCenter Domain**（创建 **vCenter** 域）。
3. 输入 VMM 域的描述性 **Name**（名称）。
4. 从 **Virtual Switch**（虚拟交换机）下拉列表中选择 **VMware vSphere Distributed Switch**（**VMware vSphere** 分布式交换机）。
5. 从 **Encapsulation**（封装）下拉列表中选择 **VLAN**。
6. 从 **VLAN Pool**（**VLAN** 池）下拉列表中选择 VLAN 池。
7. 单击 **vCenter Credentials**（**vCenter** 凭据）右侧的加号 (+) 按钮。
8. 输入描述性的 **Profile Name**（配置文件名称）和您的 vCenter 登录信息。
9. 单击 **vCenter** 右侧的加号 (+) 按钮。
10. 输入描述性的 **Name**（名称）。
11. 从 Type（类型）下拉列表中选择 vCenter。
12. 在 **P/Hostname**（**IP/**主机名）下输入 vCenter IP 地址。
13. 从 **Associated Credential**（相关联的凭据）下拉列表中选择刚才创建的 vCenter 凭据配置文件。
14. 单击 **Submit**（提交）。

为东向西向流量配置 LLDP 和 LACP 的接口策略

创建在连接到防火墙的 ACI 接口上启用 LLDP 和 LACP 的策略。

LLDP 是转发在 ACI 环境中正常工作所必需的；ACI 不会在叶子交换机上部署子网路由器接口，除非它检测到交换机上需要端点的端点。LLDP 有助于确定是否需要子网路由器接口。

LACP 可在链路故障时提供更高的弹性和恢复速度。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建 LLDP 接口策略。

1. 选择 **Fabric**（结构）> **Access Policies**（访问策略）> **Interface Policies**（接口策略）> **Policies**（策略）> **LLDP Interface** （**LLDP** 接口）。
2. 右键单击 **LLDP Interface**（**LLDP** 接口），然后选择 **Create LLDP Interface Policy**（创建 **LLDP** 接口策略）。
3. 输入 LLDP 接口策略的描述性 **Name**（名称）。
4. 为 **Receive State**（接收状态）选择 **Enabled**（启用）。
5. 为 **Transmit State**（传输状态）选择 **Enabled**（启用）。
6. 单击 **Submit**（提交）。

STEP 2 | 创建端口通道策略以启用 LACP。

1. 选择 **Fabric**（结构）> **Access Policies**（访问策略）> **Interface Policies**（接口策略）> **Policies**（策略）> **Port Channel**（端口信道）。
2. 右键单击 **Port Channel**（端口信道），然后选择 **Create Port Channel Policy**（创建端口信道策略）。
3. 输入端口信道策略的描述性 **Name**（名称）。
4. 从 **Mode**（模式）下拉列表中选择 **LACP Active**（**LACP** 主动）。
5. 单击 **Submit**（提交）。

建立防火墙与 ACI 结构之间的连接

使用您在此过程中先前在防火墙上配置的以太网接口（或聚合以太网组），通过 VPC 连接将防火墙连接到叶子交换机。将接口或接口连接到叶子交换机上的相同端口。

STEP 1 | 选择 **Fabric**（结构）> **Access Policies**（访问策略）> **Quick Start**（快速入门）。

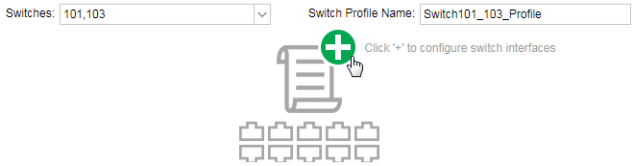
STEP 2 | 单击 **Configure an interface, PC, and VPC**（配置接口、**PC** 和 **VPC**）。

STEP 3 | 单击绿色和白色加号 (+)。



STEP 4 | 从 **Switches**（交换机）下拉列表中选择防火墙所连接的叶子交换机。

STEP 5 | 单击绿色和白色加号 (+)。



 ©2024 Palo Alto Networks, Inc.

STEP 6 | 选择 VPC 作为 **Interface Type**（接口类型）。

STEP 7 | 在 **Interfaces**（接口）字段中，输入防火墙连接到叶子交换机的接口编号。

STEP 8 | 在 **Interface Selector Name**（接口选择器名称）字段中输入描述性名称。

STEP 9 | 从 **LLDP Policy**（**LLDP** 策略）下拉列表中选择 **LLDP-Enabled**（**LLDP** 启用）。

STEP 10 | 从 **Port Channel Policy**（端口通道策略）下拉列表中选择 **LACP Active**（**LACP** 主动）。

STEP 11 | 从 **Attached Device Type**（附加设备类型） 下拉列表中，为物理防火墙选择 **Bare Metal**（裸机），或者为 VM 系列选择 **ESX Hosts**（**ESX** 主机）。

STEP 12 | 为 **Domain**（域）选择 **Choose One**（选择一个）。

STEP 13 | 从 **Domain**（域）下拉列表中选择之前在此过程中创建的物理域或 VMM 域。

STEP 14 | 单击 **Save**（保存）。

STEP 15 | 单击 **Save**（保存），然后 **Submit**（提交）。

STEP 16 | 为 HA 对中的第二个防火墙重复此过程。

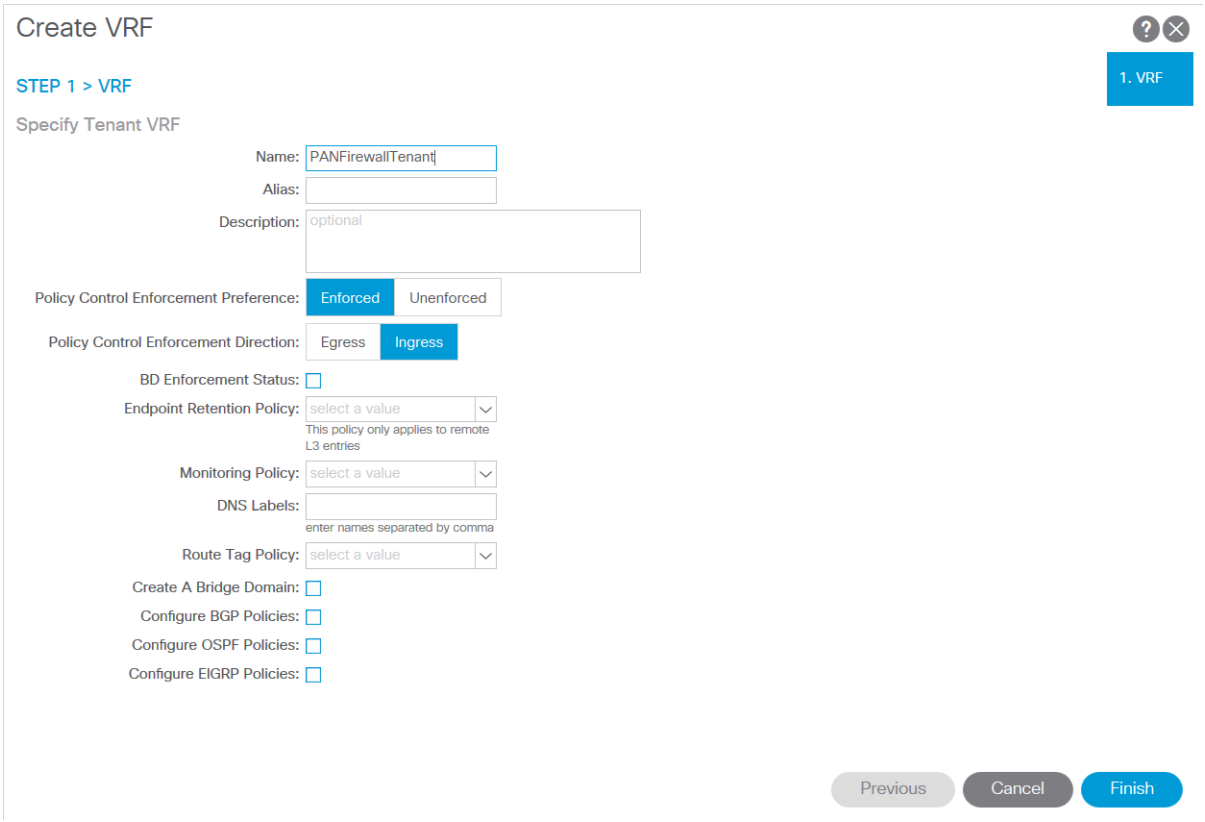
创建 **VRF** 和桥接域

租户的所有网桥域和子网都需要 VRF。在此示例中，您将为防火墙和端点创建单个通用 VRF。然后为防火墙配置专用网桥域并禁用数据平面学习。要在桥接域中使用基于策略的重定向，需要禁用数据平面学习。

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 创建一个 VRF。

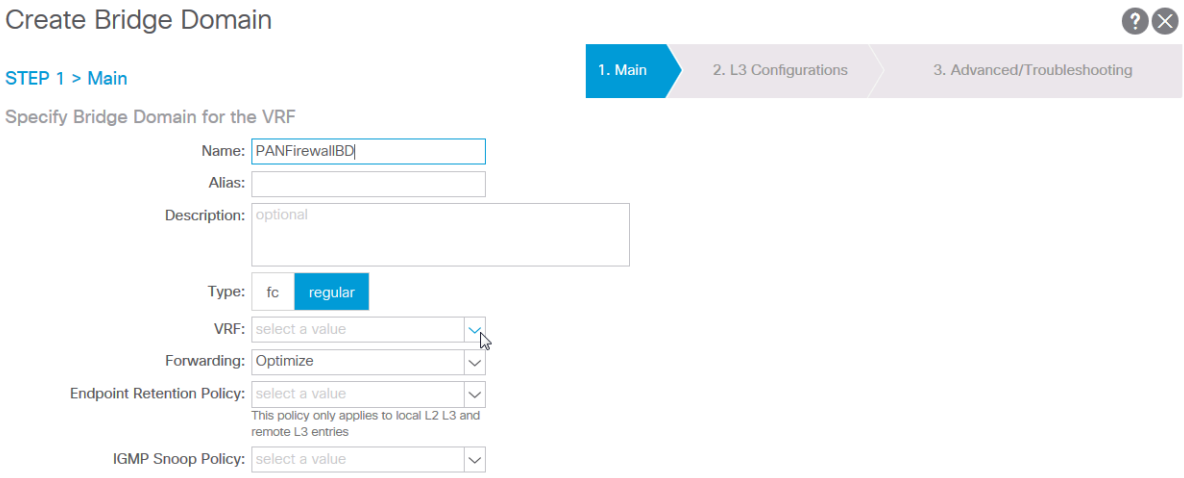
1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Networking**（网络）> **VRF**。
3. 右键单击 **VRF**，然后选择 **Create VRF**（创建 **VRF**）。
4. 输入 VRF 的描述性 **Name**（名称）。
5. 清除 **Create A Bridge Domain**（创建桥接域）复选框。
6. 单击 **Finish**（完成）。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 为防火墙创建桥接域。

1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Networking**（网络） > **Bridge Domains**（桥接域）。
3. 右键单击 **Bridge Domains**（桥接域），然后选择 **Create Bridge Domain**（创建桥接域）。
4. 输入桥接域的描述性 **Name**（名称）。
5. 从 **VRF** 下拉列表中选择在上一过程中创建的 VRF。
6. 单击 **Next**（下一步）。



创建 L4-L7 设备

您必须将防火墙定义为 APIC 中的 L4-L7 设备，以便 ACI 可以将其插入到流量流中。您可以将 APIC 中的 L4-L7 设备配置为设备集群，该集群是表示单个防火墙或充当单个设备的防火墙 HA 对的构造。设备集群具有一个或多个逻辑接口，这些接口使用物理域中的 VLAN 定义成员防火墙的路径。

STEP 1 | 在 **Tenants**（租户）选项卡上双击租户名称。

STEP 2 | 选择 **Services**（服务） > **L4-L7** > **Devices**（设备）。

STEP 3 | 右键单击 **Devices**（设备），然后选择 **Create L4-L7 Device**（创建 **L4-L7** 设备）。

STEP 4 | 清除 **Managed**（托管）选项卡。

STEP 5 | 输入 L4-L7 的描述性 **Name**（名称）。

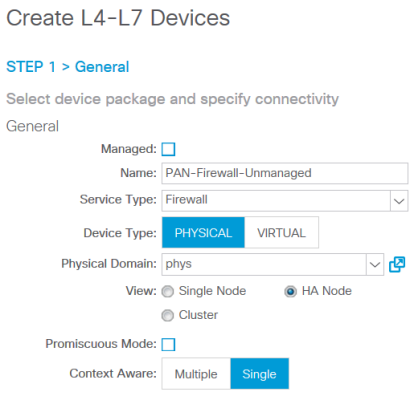
STEP 6 | 从 **Service Type**（服务类型）下拉列表中选择 **Firewall**（防火墙）。

STEP 7 | 在 **Device Type**（设备类型）下拉列表中，为物理防火墙选择 **Physical**（物理），为 VM 系列防火墙选择 **Virtual**（虚拟）。

STEP 8 | 从 **Domain**（域）下拉列表中选择之前创建的物理或 VMM。

©2024 Palo Alto Networks, Inc.

STEP 9 | 为 **View**（视图）选择 HA 节点。



STEP 10 | 在 **Device 1**（设备 **1**）下，单击 **Device Interfaces**（设备接口）右侧的加号 (+) 图标。

STEP 11 | 输入该接口的描述性 **Name**（名称）。

STEP 12 | 在 **Path**（路径）下，选择 HA 对中主要防火墙的路径。

STEP 13 | 单击 **Update**（更新）。

STEP 14 | 在 **Device 2**（设备 **2**）下，单击 **Device Interfaces**（设备接口）右侧的加号 (+) 图标。

STEP 15 | 输入该接口的描述性 **Name**（名称）。

STEP 16 | 在 **Path**（路径）下，选择 HA 对中辅助防火墙的路径。

STEP 17 | 单击 **Update**（更新）。

STEP 18 | 在 **Cluster**（集群）下，单击 **Cluster Interfaces**（集群接口）右侧的加号 (+) 图标。

STEP 19 | 输入集群的描述性 **Name**（名称）。

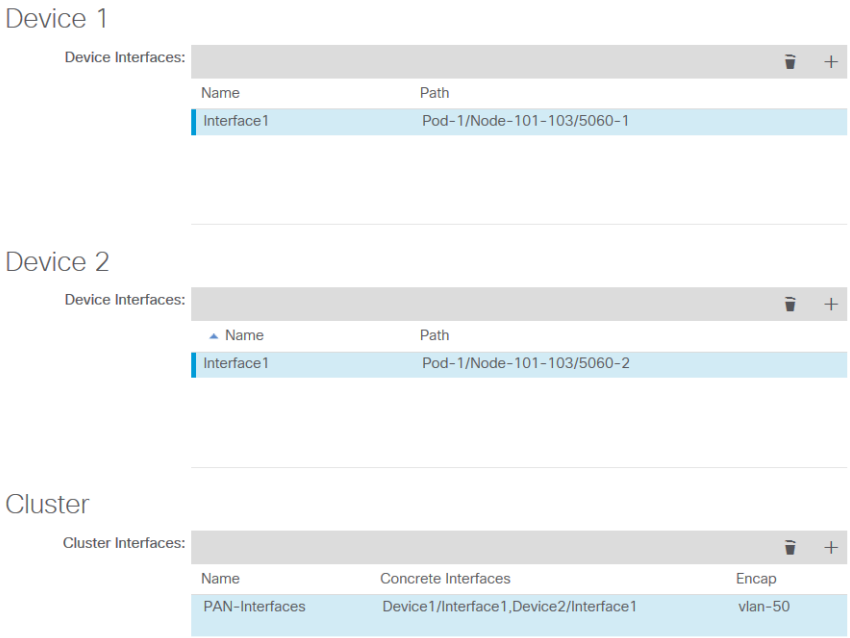
STEP 20 | 从 **Concrete Interfaces**（具体接口）下的列表中选择在上面配置的两个接口。APIC 要求配置两个接口。但是，由于防火墙与 ACI 结构之间只有一个连接，因此，只使用其中一个接口。

STEP 21 | 在 **Encap**（封装）下，从之前创建的静态 VLAN 池中输入 VLAN。流量将重定向到此处分配的 VLAN 上的防火墙。

STEP 22 | 单击 **Update**（更新）。

©2024 Palo Alto Networks, Inc.

STEP 23 | 单击 **Finish**（完成）。



创建基于策略的重定向

配置基于策略的重定向，将 EPG 之间的流量发送到防火墙。基于策略的重定向利用防火墙上接口的 MAC 地址。在 APIC 上配置 PBR 设置之前，必须从防火墙获取 MAC 地址。

STEP 1 | 获取防火墙的 MAC 地址。

1. 登录到防火墙 CLI。
2. 使用 **`command show interface all`** 显示已配置接口的 MAC 地址。
3. 复制将接收重定向流量的接口的 MAC 地址。

STEP 2 | 创建 L4-L7 基于策略的重定向。

1. 登录 APIC。
2. 在 **Tenants**（租户）选项卡上双击租户名称。
3. 选择 **Policies**（策略） > **Protocol**（协议） > **L4-L7 Policy Based Redirect**（基于 **L4-L7** 策略的重定向）。
4. 右键单击 **L4-L7 Policy Based Redirect**（基于 **L4-L7** 策略的重定向），然后选择 **Create L4-L7 Policy Based Redirect**（创建基于 **L4-L7** 策略的重定向）。
5. 输入基于策略的重定向的描述性 **Name**（名称）。
6. 单击 **Destinations**（目标）右侧的加号 (+) 图标。
7. 在 **IP** 字段中，输入将接收重定向流量的接口的 IP 地址。
8. 在 **MAC** 字段中，输入从防火墙 CLI 复制的 MAC 地址。
9. 单击 **OK**（确定）。
10. 单击 **Submit**（提交）。

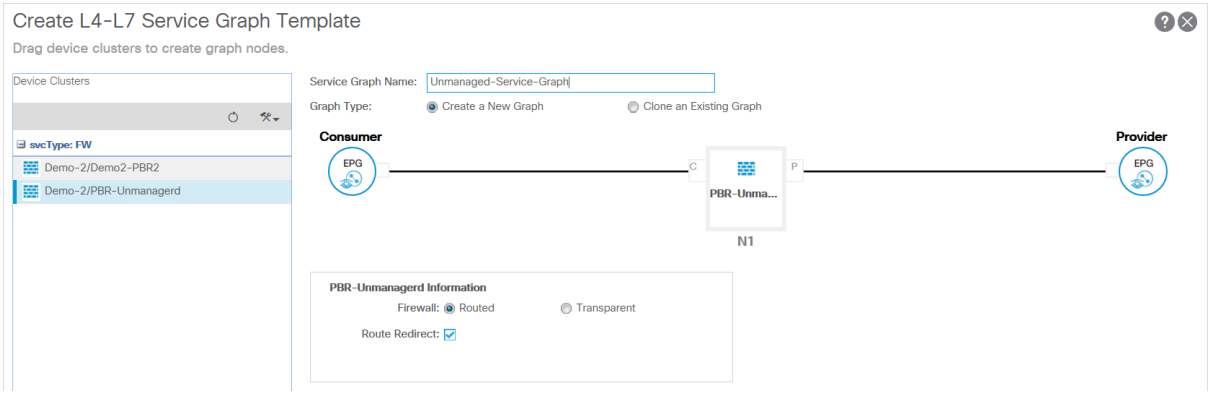
©2024 Palo Alto Networks, Inc.

创建和应用 **Service Graph** 模板

创建 Service Graph 模板，该模板使用代表基于策略的重定向集成中的防火墙的设备集群。创建服务图表后，您必须将其应用于 EPG 以保护流量。合同和合同筛选规则定义可以转发到防火墙的流量。

STEP 1 | 创建 Service Graph 模板。

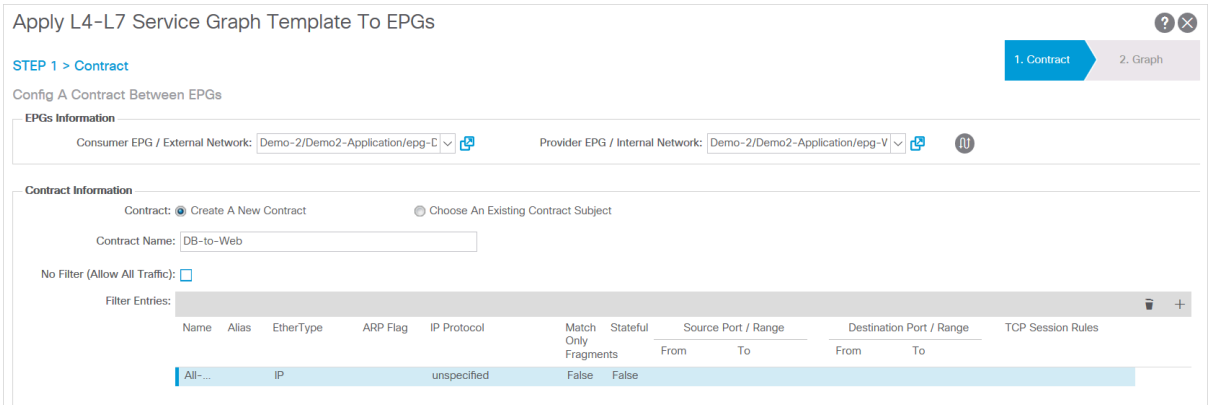
1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Services**（服务） > **L4-L7** > **L4-L7 Service Graph Templates**（**L4-L7 Service Graph** 模板）。
3. 右键单击 **L4-L7 Service Graph Template**（**L4-L7 Service Graph** 模板）并选择 **Create L4-L7 Service Graph Template**（创建 **L4-L7 Service Graph** 模板）。
4. 为 Service Graph 模板输入描述性 **Graph Name**（图表名称）。
5. 选择 **Create a New One**（创建新模板）作为 **Graph Type**（图表类型）。
6. 单击并拖动您在上一过程中在消费者和提供者 EPG 之间创建的 L4-L7 设备。
7. 对于 **Firewall**（防火墙），选择 **Routed**（路由）。
8. 选择 **Routed Redirect**（路由重定向）。
9. 单击 **Submit**（提交）。



 ©2024 Palo Alto Networks, Inc.

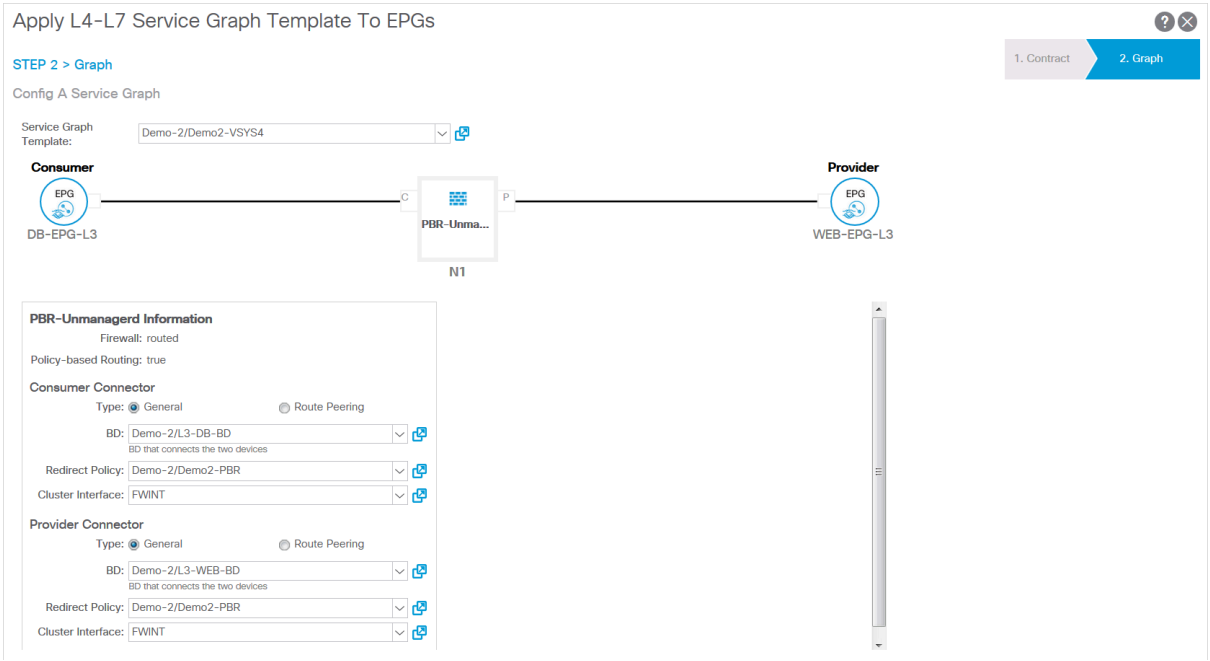
STEP 2 | 应用 Service Graph 模板。

1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Services**（服务）> **L4-L7**。
3. 在 **EPGs Information**（**EPG** 信息）面板中，从 **Consumer EPG**（消费者 **EPG**）和 **Provider EPG**（提供商 **EPG**）下拉列表中选择消费者和提供商 EPG。
4. 选择 **Create a New Contract**（创建新合同）。
5. 输入描述性 **Contract Name**（合同名称）。
6. 清除“无筛选器”**(Allow All Traffic)**（允许所有流量）。建议不要使用此选项。要允许 EPG 之间的所有流量重定向到防火墙，建议您创建一个筛选器来执行此操作。
7. 单击 **Filter Entries**（筛选条目）右侧的加号 (+) 图标。
8. 创建规则以定义允许在 EPG 之间传递并重定向到防火墙的流量。
9. 单击 **Next**（下一步）。



10. 从 **Service Graph Template**（**Service Graph** 模板）下拉列表中选择在上一过程中创建的服务图模板。
11. 在使用者和提供商窗格中，从 **BD** 下拉列表中选择包含防火墙的桥接域。
12. 从 **Redirect Policy**（重定向政策）下拉菜单中选择之前创建的基于策略的重定向。
13. 从 **Cluster Interface**（集群接口）下拉菜单中选择使用 L4-L7 设备创建的集群接口。

©2024 Palo Alto Networks, Inc.



部署防火墙以在网络策略模式下保护北向南流量

使用网络策略模式，使用基于策略的重定向的非托管模式保护进入和退出数据中心的北向南流量。此过程假定您已完成以下操作：

- 防火墙可以运行并连接到 Cisco ACI 环境中的叶子交换机。此外，APIC 必须能够访问每个防火墙的管理接口。
- 防火墙以主动/被动 HA 模式部署。此过程不包括 HA 网络设置，并假设您已提前完成此操作。

要建立与 ACI 结构外部网络的外部连接，必须配置 L3Out。L3Out 是一项专用策略，包含将外部路由设备连接到租户所需的参数。此外，L3Out 包含外部 EPG（在 APIC UI 中称为外部网络），表示可通过 L3Out 访问的网络。外部 EPG 不会动态填充并遵循零可信模型，因此您必须在 EPG 中定义网络。要使配置更容易，您可以配置 0.0.0.0/0 的网络，以将所有网络分配给外部 EPG。

要保护入站流量，请将 HA 对中的防火墙或防火墙连接到边界交换机。边界交换机是叶子交换机，提供到外部路由器的第 3 层连接。防火墙使用开放式最短路径优先 (OSPF) 协议与边界叶子交换机对等，该协议在 vPC 对中的每个叶子交换机上配置，并使用交换机虚拟接口 (SVI) 与防火墙通信。在防火墙上，您可以配置专用于连接到数据中心的接口的虚拟路由器。此外，此程序包括

对于出站流量，防火墙使用 OSPF 将外部网络通告给边界交换机。另外，外部网络 EPG 被配置为允许防火墙通告的所有网络进入该 EPG。您在 vzAny 托管对象和外部网络 EPG 之间创建合同，以允许来自 VRF 内任何 EPG 的流量通过防火墙到达外部网络。vzAny 托管对象允许您将VRF中的所有 EPG 合并为一个或多个合同，而不是为每个 EPG 创建单独的合同。在 vzAny 管理对象中收集的 EPG 使用外部 EPG 提供的联系。

与服务管理器模式不同，管理是否单独完成 ACI 基础架构和防火墙。

在 APIC 上 —

 ©2024 Palo Alto Networks, Inc.

- 创建 VLAN 池和外部路由域
- 为北向南流量配置 LLDP 和 LACP 的接口策略
- 创建外部路由网络
- 配置子网以通告外部防火墙
- 创建出站合同
- 创建入站 Web 合同
- 将出站和入站合同应用到 EPG

在防火墙上 —

- 为北向南流量创建虚拟路由器和安全区域
- 配置网络接口
- 配置路由重新分发和 OSPF
- 为外部连接配置 NAT

创建 **VLAN** 池和外部路由域

将接口连接到基础架构时，创建 VLAN 池以将 VLAN 分配给防火墙，从而支持 ACI 结构中的 EPG。应为防火墙使用静态 VLAN 范围。

此外，必须创建物理域以将 VLAN 映射到 EPG。以下过程将创建专用于防火墙的物理域。

STEP 1 | 创建 VLAN 池。

1. 登录到 APIC。
2. 选择 **Fabric**（结构） > **Access Policies**（访问策略） > **Pools**（池） > **VLAN**。
3. 右键单击 **VLAN**，然后选择 **Create VLAN Pool**（创建 **VLAN** 池）。
4. 输入 VLAN 池的描述性 **Name**（名称）。
5. 为分配模式选择 **Dynamic Allocation**（动态分配）。
6. 单击 **Encap Blocks**（**Encap** 块）右侧的加号 (+) 按钮。
7. 在 **VLAN Range**（**VLAN** 范围）字段中输入 VLAN 范围。
8. 从 Allocation Mode（分配模式）下拉列表中选择 **Static Allocation**（静态分配）。
9. 单击 **OK**（确定）。
10. 单击 **Submit**（提交）。

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 创建外部路由域。

1. 选择 **Fabric**（结构） > **Access Policies**（访问策略） > **Physical and External Domains**（物理和外部域） > **External Domains**（外部域）。
2. 右键单击 **External Routed Domain**（外部路由域），然后选择 **Create Layer 3 Domain**（创建第 **3** 层域）。
3. 输入物理域的描述性 **Name**（名称）。
4. 从 VLAN Pool（VLAN 池）列表中选择在上一过程中创建的 VLAN 池。
5. 单击 **Submit**（提交）。

为北向南流量配置 LLDP 和 LACP 的接口策略

创建在连接到防火墙的 ACI 接口上启用 LLDP 和 LACP 的策略。

LLDP 是转发在 ACI 环境中正常工作所必需的；ACI 不会在叶子交换机上部署子网路由器接口，除非它检测到交换机上需要端点的端点。LLDP 有助于确定是否需要子网路由器接口。

LACP 可在链路故障时提供更高的弹性和恢复速度。

STEP 1 | 创建 LLDP 接口策略。

1. 选择 **Fabric**（结构） > **Access Policies**（访问策略） > **Interface Policies**（接口策略） > **Policies**（策略） > **LLDP Interface** （**LLDP** 接口）。
2. 右键单击 **LLDP Interface**（**LLDP** 接口），然后选择 **Create LLDP Interface Policy**（创建 **LLDP** 接口策略）。
3. 输入 LLDP 接口策略的描述性 **Name**（名称）。
4. 为 **Receive State**（接收状态）选择 **Enabled**（启用）。
5. 为 **Transmit State**（传输状态）选择 **Enabled**（启用）。
6. 单击 **Submit**（提交）。

STEP 2 | 创建端口通道策略以启用 LACP。

1. 选择 **Fabric**（结构） > **Access Policies**（访问策略） > **Interface Policies**（接口策略） > **Policies**（策略） > **Port Channel**（端口信道）。
2. 右键单击 **Port Channel**（端口信道），然后选择 **Create Port Channel Policy**（创建端口信道策略）。
3. 输入端口信道策略的描述性 **Name**（名称）。
4. 从 **Mode**（模式）下拉列表中选择 **LACP Active**（**LACP** 主动）。
5. 单击 **Submit**（提交）。

创建外部路由网络

防火墙将 IP 路由信息传递到第 3 层上的 ACI OSPF 网络。ACI 在叶子交换机上使用交换机虚拟接口 (SVI)，每个交换机上都有一个 IP 地址，用于连接弹性。使用 OSPF 创建第 3 层路由网络以与防火墙建立对等。

©2024 Palo Alto Networks, Inc.

STEP 1 | 在 **Tenants**（租户）选项卡上双击租户名称。

STEP 2 | 选择 **Networking**（网络） > **External Routed Networks**（外部路由网络）。

STEP 3 | 右键单击 **External Routed Networks**（外部路由网络）并选择 **Create Routed Outside**（创建外部路由）。

STEP 4 | 输入 **External Routed Network**（外部路由网络）的描述性 **Name**（名称）。

STEP 5 | 从 **VRF**下拉列表中选择具有外部连接的 VRF。

STEP 6 | 从 **External Routed Domain**（外部路由域）下拉列表中选择之前创建的外部路由域。

STEP 7 | 选择 **OSPF**。

STEP 8 | 输入一个 **OSPF Area ID**（**OSPF** 区域 **ID**）。区域 ID 可以用十进制数或点分十进制形式表示。例如，区域 1 与区域 0.0.0.1 相同，或区域 271 与区域 0.0.1.15 相同。区域 ID 范围是 0 (0.0.0.0) 到 4294967295 (255.255.255.255)。

STEP 9 | 为 **OSPF Area Type**（**OSPF** 区域类型）选择 **Regular Area**（常规区域）。

STEP 10 | 单击 **Nodes and Interface Profiles**（节点和接口配置文件）右侧的加号 (+) 按钮以创建带一个节点的节点配置文件，该节点用于连接到防火墙的边界页交换机。

STEP 11 | 输入 **Node Profile**（节点配置文件）的描述性 **Name**（名称）。

STEP 12 | 将节点附加到节点配置文件。

1. 单击 **Nodes**（节点）右侧的加号 (+) 按钮。随即打开 **Select Node**（选择节点）窗口。
2. 从 **Node ID**（节点 **ID**）下拉列表中选择防火墙连接的节点。
3. 在 **Router ID**（路由器 **ID**）中输入连接到叶子交换机的路由器的 IP 地址。
4. 单击 **OK**（确定）。
5. 单击 **Nodes and Interface Profiles**（节点和接口配置文件）右侧的加号 (+) 按钮。
6. 输入 **Node Profile**（节点配置文件）的描述性 **Name**（名称）。
7. 单击 **Nodes**（节点）右侧的加号 (+) 按钮。随即打开 **Select Node**（选择节点）窗口。
8. 从 **Node ID**（节点 **ID**）下拉列表中选择连接到节点的辅助 HA 防火墙。
9. 在 **Router ID**（路由器 **ID**）中输入连接到第二个叶子交换机的路由器的 IP 地址。
10. 单击 **OK**（确定）。

©2024 Palo Alto Networks, Inc.

STEP 13 | 为节点配置文件附加 OSPF 接口配置文件。

1. 输入 OSPF 接口配置文件的描述性 **Name**（名称）。
2. 单击 **Next**（下一步）。
3. 从 OSPF 策略下拉列表中选择 **Create OSPF Interface Policy**（创建 **OSPF** 接口策略）。
4. 输入 OSPF 接口策略的描述性 **Name**（名称）。
5. 选择 **MTU Ignore**（**MTU** 忽略）。
6. 单击 **Submit**（提交）。
7. 单击 **Next**（下一步）。
8. 单击 **SVI**。
9. 单击 **SVI Interfaces**（**SVI** 接口）右侧的加号 (+) 按钮。随即打开 **Select SVI**（选择 **SVI**）窗口。
10. 单击 **Virtual Port Channel**（虚拟端口通道）。
11. 选择防火墙连接到叶子交换机的端口和端口通道接口的路径。
12. 在 **ENCAP**中，输入第 3 层外部配置文件的 VLAN 封装。
13. 为模式选择 **Trunk**（中继）。
14. 在 **Side A IPv4 Primary Address**（**A** 端 **IPv4** 主要地址）字段中，输入附加到第 3 层外部配置文件的路径的主 IP 地址。
15. 在 **Side B IPv4 Primary Address**（**B** 端 **IPv4** 主要地址）字段中，输入附加到第 3 层外部配置文件的路径的辅助 IP 地址。
16. 单击 **OK**（确定）。

STEP 14 | 单击 **OK**（确定）以关闭“创建接口配置文件”窗口。

STEP 15 | 单击 **OK**（确定）以关闭“创建节点配置文件”窗口。

STEP 16 | 单击 **Next**（下一步）。

STEP 17 | 单击 **External EPG Networks**（外部 **EPG** 网络）右侧的加号 (+) 按钮。此操作将打开 **Create Routed Outside**（创建外部路由）窗口。

STEP 18 | 输入外部网络的描述性 **Name**（名称）。

STEP 19 | 将子网添加到外部网络。

1. 单击 **Subnets**（子网）右侧的加号 (+) 按钮。
2. 输入子网默认网关的 IP 地址和掩码。
3. 选择 **Export Route Control Subnet**（导出路由控制子网）。
4. 选择 **External Subnets for External EPG**（外部 **EPG** 的外部子网）。
5. 单击 **OK**（确定）。

STEP 20 | 单击 **Finish**（完成）。

 ©2024 Palo Alto Networks, Inc.

配置子网以通告外部防火墙

默认情况下，不会将 ACI 结构中的子网公布到外部网络。您必须配置要在外部公布的子网。

STEP 1 | 在 **Tenants**（租户）选项卡上双击租户名称。

STEP 2 | 选择 **Networking**（网络） > **Bridge Domains**（桥接域） > **<your bridge domain>**。

STEP 3 | 单击 **L3 Configurations**（**L3** 配置）。

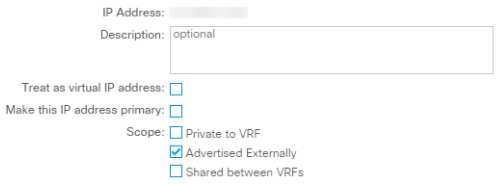
STEP 4 | 单击 **Associated L3 Outs**（关联的 **L3** 输出）右侧的加号 (+) 按钮。

STEP 5 | 从中 **L3 Out**（**L3** 输出）下拉列表中选择在上一过程中创建的第 3 层外部路由网络连接。

STEP 6 | 单击 **Update**（更新）。

STEP 7 | 选择 **Networking**（网络） > **Bridge Domains**（桥接域） > **<your bridge domain>** > **Subnets**（子网） > **<externally advertised subnet>**。

STEP 8 | 将范围设置为 **Advertised Externally**（向外部公布）。



STEP 9 | 单击 **Submit**（提交）。

创建出站合同

使用允许 DNS、NTP、HTTP 和 HTTPS 流量的筛选器创建合同。您将使用此合同允许 VRF 中的所有端点到达外部网络，但限制发送到防火墙的流量。

STEP 1 | 在 **Tenants**（租户）选项卡上双击租户名称。

STEP 2 | 选择 **Contracts**（合同） > **Filters**（筛选器）

STEP 3 | 右键单击 **Filters**（筛选器），然后选择 **Create Filter**（创建筛选器）。

STEP 4 | 输入筛选器的描述性 **Name**（名称）。

©2024 Palo Alto Networks, Inc.

STEP 5 | 为 UDP 流量创建筛选条目。

1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **UDP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **UDP**。
5. 从 **Destination Port From**（目标端口来源）下拉列表中选择 **DNS**。
6. 单击 **Update**（更新）。

STEP 6 | 为 TCP 流量创建筛选条目。

1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **TCP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **TCP**。
5. 从 **Destination Port From**（目标端口来源）下拉列表中选择 **DNS**。
6. 单击 **Update**（更新）。

STEP 7 | 为 NTP 流量创建筛选条目。

1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **NTP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **UDP**。
5. 在 **Destination Port From**（目标端口来源）字段中，输入 123。
6. 单击 **Update**（更新）。

STEP 8 | 为 HTTP 流量创建筛选条目。

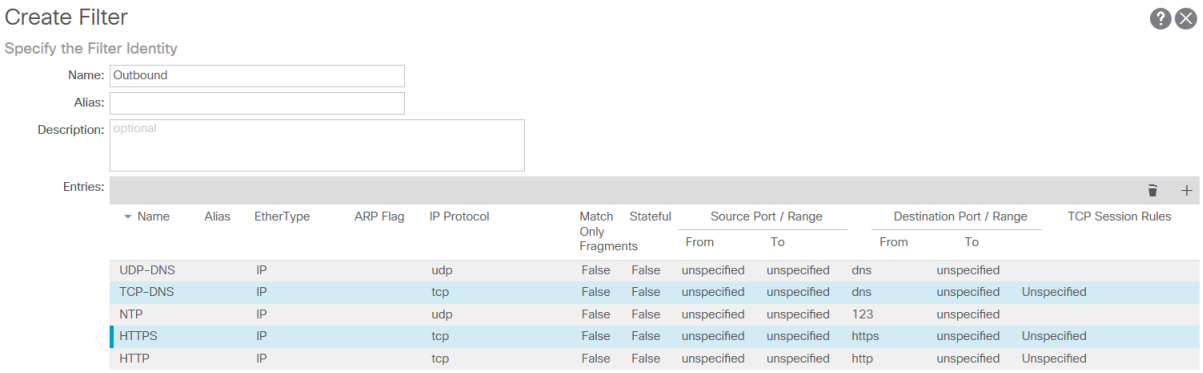
1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **HTTP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **TCP**。
5. 从 **Destination Port From**（目标端口来源）下拉列表中选择 **http**。
6. 单击 **Update**（更新）。

©2024 Palo Alto Networks, Inc.

STEP 9 | 为 HTTPS 流量创建筛选条目。

1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **HTTP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **TCP**。
5. 从 **Destination Port From**（目标端口来源）下拉列表中选择 **https**。
6. 单击 **Update**（更新）。

STEP 10 | 单击 **Submit**（提交）。



STEP 11 | 为出站流量创建合同。

1. 在 **Tenants**（租户）选项卡，双击租户名称并选择 **Contracts**（合同）。
2. 右键单击 **Contracts**（合同）并选择 **Create Contract**（创建合同）。
3. 输入 **Contract**（合同）的描述性 **Name**（名称）。
4. 单击 **Subjects**（主题）右侧的加号 (+) 按钮。
5. 输入 **Subject**（主题）的描述性 **Name**（名称）。
6. 在筛选器链下，单击 **Filters**（筛选器）右侧的加号 (+) 按钮。
7. 从下拉列表中选择之前创建的筛选器。
8. 单击 **OK**（确定）。

STEP 12 | 单击 **Submit**（提交）。

创建入站 Web 合同

您还必须创建合同和筛选器，以允许入站流量到达防火墙后面的服务器。以下过程描述了创建合同和筛选器的过程，这些筛选器允许 HTTP 和 HTTPS Web 流量访问防火墙后面的资源。

STEP 1 | 在 **Tenants**（租户）选项卡上双击租户名称。

STEP 2 | 选择 **Contracts**（合同） > **Filters**（筛选器）

STEP 3 | 右键单击 **Filters**（筛选器），然后选择 **Create Filter**（创建筛选器）。

©2024 Palo Alto Networks, Inc.

STEP 4 | 输入筛选器的描述性 **Name**（名称）。

STEP 5 | 为 HTTP 流量创建筛选条目。

1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **HTTP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **TCP**。
5. 从 **Destination Port From**（目标端口来源）下拉列表中选择 **http**。
6. 单击 **Update**（更新）。

STEP 6 | 为 HTTPS 流量创建筛选条目。

1. 单击 **Entries**（条目）右侧的加号 (+) 按钮。
2. 输入 **TCP** 筛选器的描述性 **Name**（名称）。
3. 从 **EtherType** 下拉列表中选择 **IP**。
4. 从 **IP Protocol**（**IP** 协议）下拉列表中选择 **TCP**。
5. 从 **Destination Port From**（目标端口来源）下拉列表中选择 **https**。
6. 单击 **Update**（更新）。

STEP 7 | 单击 **Submit**（提交）。

STEP 8 | 为入站 Web 流量创建合同。

1. 在 **Tenants**（租户）选项卡，双击租户名称并选择 **Contracts**（合同）。
2. 右键单击 **Contracts**（合同）并选择 **Create Contract**（创建合同）。
3. 输入 **Contract**（合同）的描述性 **Name**（名称）。
4. 单击 **Subjects**（主题）右侧的加号 (+) 按钮。
5. 输入 **Subject**（主题）的描述性 **Name**（名称）。
6. 在筛选器链下，单击 **Filters**（筛选器）右侧的加号 (+) 按钮。
7. 从下拉列表中选择之前创建的筛选器。
8. 单击 **OK**（确定）。

STEP 9 | 单击 **Submit**（提交）。

将出站和入站合同应用到 EPG

现在，您必须将入站和出站合同应用于相应的 EPG。

对于 VRF 内的所有 EPG（EPG 集合），为了将流量发送到外部目标，每个内部 EPG 必须与外部 EPG 签订合同。通常，您需要在每个内部 EPG 和外部 EPG 之间创建单独的合同。但是，使用 vzAny 对象，您可以动态地将相同的合同应用于所有 EPG。EPG 集使用合同，外部 EPG 提供合同。您可以在合同中配置特定的流量配置文件，或将所有流量发送到防火墙，并允许它控制离开数据中心的流量。此外，任何加入 VRF 的新 EPG 都会自动将合同应用于它。

©2024 Palo Alto Networks, Inc.

应用入站合同，以便内部 EPG 是提供者，外部 EPG 是消费者。流向内部 EPG 的流量将根据合同进行检查，然后根据需要由防火墙进一步确保任何允许的流量。

STEP 1 | 将出站合同应用于 VRF 中的所有 EPG。

1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Networking**（网络） > **VRF** > **<you VRF>** > **EPG Collection for VRF**（**VRF** 的 **EPG** 集合）。
3. 单击 **Consumed Contracts**（消耗的合同）右侧的加号 (+) 按钮。
4. 从 **Name**（名称）下拉列表中选择出站合同。
5. 单击 **Update**（更新）。
6. 选择 **Networking**（网络） > **External Routed Networks**（外部路由网络） > **<your external routed network>** > **Networks**（网络） > **External**（外部）。
7. 单击 **Provided Contracts**（提供的合同）右侧的加号 (+) 按钮。
8. 从 **Name**（名称）下拉列表中选择出站合同。
9. 单击 **Update**（更新）。

STEP 2 | 应用入站合同，以便内部 EPG 将其提供给外部 EPG。

1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Application Profiles**（应用程序配置文件） > **<your application profile>** > **Application EPGs**（应用程序 **EPG**） > **<your application EPG>** > **Contracts**（合同）。
3. 右键单击 **Contracts**（合同）并选择 **Add Provided Contract**（添加提供的合同）。
4. 从 **Contract**（合同）下拉列表中选择入站合同。
5. 单击 **Submit**（提交）。
6. 在同一租户上，选择 **Networking**（网络） > **External Routed Networks**（外部路由网络） > **<your external routed network>** > **Networks**（网络） > **External**（外部）。
7. 在 Contracts（合同）选项卡上，单击 **Consumed Contracts**（消耗的合同）右侧的加号 (+) 按钮。
8. 从 **Name**（名称）下拉列表中选择入站合同。
9. 单击 **Update**（更新）。

为北向南流量创建虚拟路由器和安全区域

在防火墙上创建虚拟路由器和安全区域，以匹配 ACI 上的租户和 VRF。

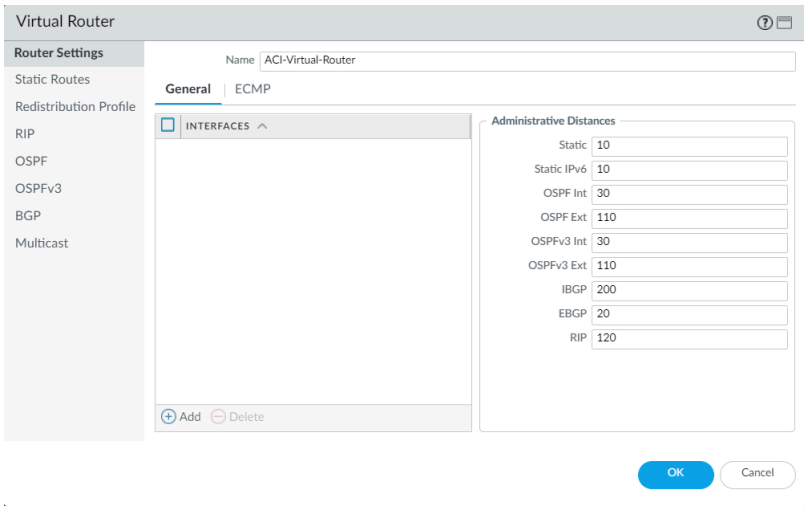
STEP 1 | 登录到防火墙。

STEP 2 | 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后单击 **Add**（添加）。

STEP 3 | 输入虚拟路由器的描述性 **Name**（名称）。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 单击 **OK**（确定）。

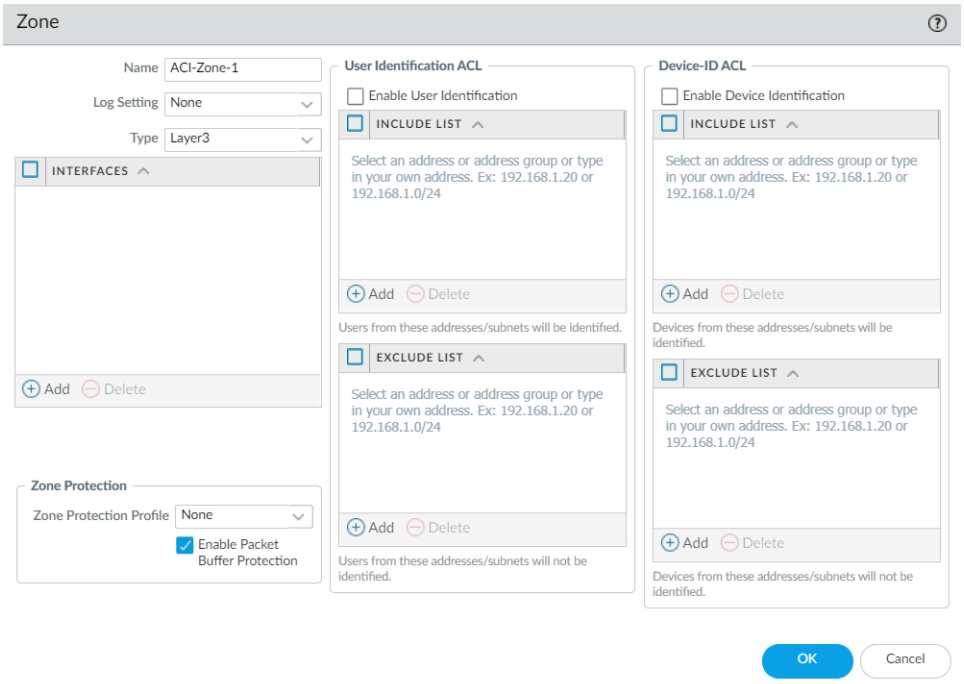


STEP 5 | 选择 **Network**（网络） > **Zones**（区域），然后单击 **Add**（添加）。

STEP 6 | 输入区域的描述性 **Name**（名称）。

STEP 7 | 从 **Type**（类型）下拉列表中选择 Layer 3（第 3 层）。

STEP 8 | 单击 **OK**（确定）。



STEP 9 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

配置网络接口

配置防火墙用于连接 ACI 叶子交换机的聚合以太网接口、成员接口和子接口。如果您使用的是 VM 系列防火墙，请使用离散接口而不是聚合接口。

VM 系列防火墙不支持聚合以太网组。

STEP 1 | 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后单击 **Add Aggregate Group**（添加聚合组）。

STEP 2 | 在第二个 **Interface Name**（接口名称）字段中输入聚合组的编号。

STEP 3 | 从 **Interface Type**（接口类型）下拉列表中选择 Layer 3（第 3 层）。

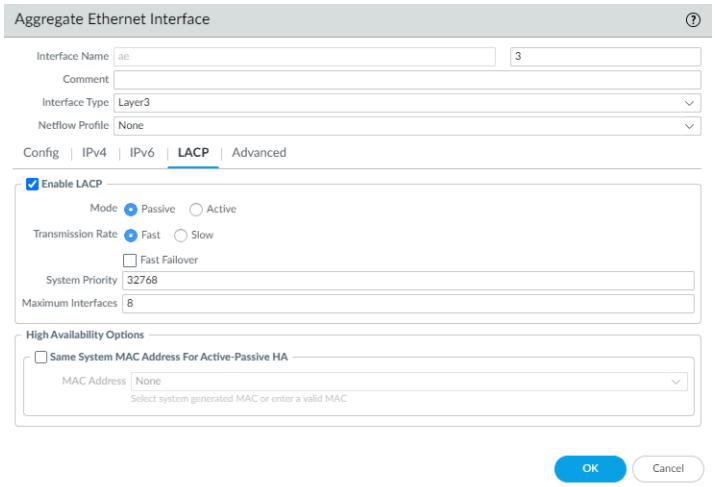
STEP 4 | 选择 **LACP** 选项卡，然后单击 **Enable LACP**（启用 **LACP**）。

STEP 5 | 选择 **Fast**（快速）作为 **Transmission Rate**（传输速率）。

STEP 6 | 在“高可用性选项”下，选择 **Enable in HA Passive State**（在 **HA** 被动状态下启用）。

不要选择 ***Same System MAC Address for Active-Passive HA***（为主动-被动 ***HA*** 使用相同的系统 ***MAC*** 地址）。此选项使防火墙对显示为交换机的单个设备，因此，流量将流向两个防火墙而不仅仅是主动防火墙。

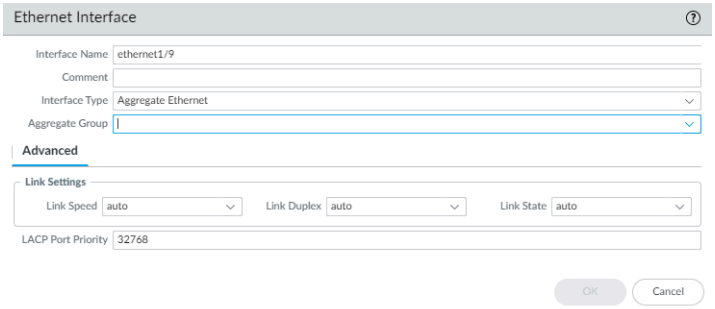
STEP 7 | 单击 **OK**（确定）。



©2024 Palo Alto Networks, Inc.

STEP 8 | 单击以太网接口的名称进行配置，并将其添加到聚合组。

1. 从 Interface Type（接口类型）下拉列表中选择 **Aggregate Ethernet**（聚合以太网）。
2. 选择在聚合以太网组配置中定义的接口。
3. 单击 **OK**（确定）。
4. 对聚合以太网组的每个其他成员接口重复此步骤。



STEP 9 | 在租户和 VRF 的聚合以太网接口上添加子接口。

1. 选择聚合以太网组的行，然后单击 **Add Subinterface**（添加子接口）。
2. 在第二个 **Interface Name**（接口名称）字段中，输入标识子接口的数字后缀。
3. 在 **Tag**（标记）字段中，输入子接口的 VLAN 标记。
4. 从 **Virtual Router**（虚拟路由器）下拉列表中选择之前配置的虚拟路由器。
5. 从 **Zone**（区域）下拉列表中选择之前配置的区域。
6. 选择 **IPv4** 选项卡。
7. 选择 **Static**（静态）类型。
8. 单击 **Add**（添加）并以 CIDR 表示法输入子接口 IP 地址和网络掩码。
9. 单击 **OK**（确定）。

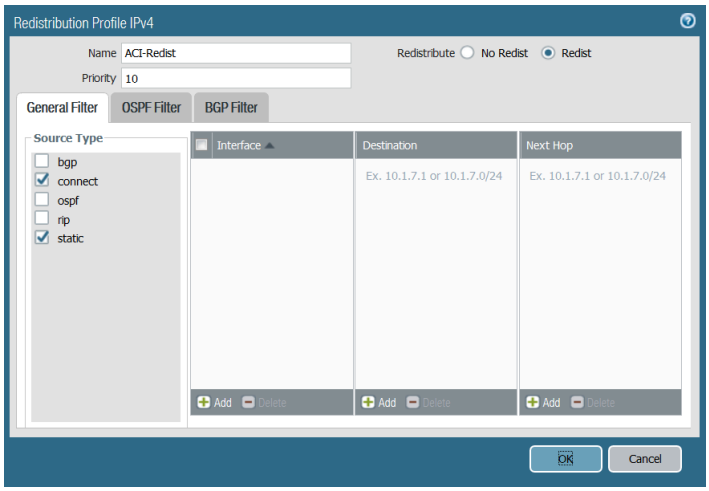
配置路由重新分发和 OSPF

配置路由重新分发，使防火墙的路由信息可用于连接到叶子交换机的面向外部的路由器。然后在防火墙上配置 OSPF，并分配路由器 ID、区号和接口以形成邻接关系。

©2024 Palo Alto Networks, Inc.

STEP 1 | 配置路由重新分发。

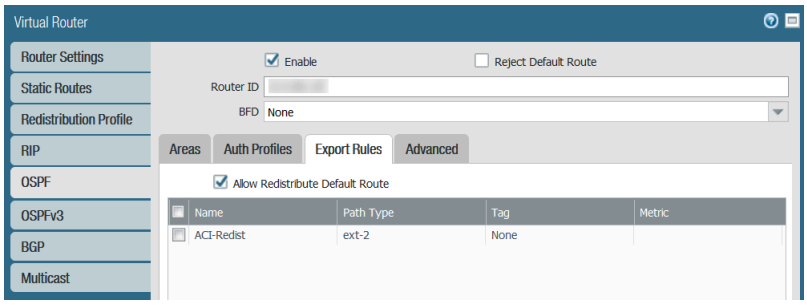
1. 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后单击之前创建的虚拟路由器。
2. 选择 **Redistribution Profile**（重新分发配置文件） > **IPv4** > **Add**（添加）。
3. 输入重新分发配置文件的描述性 **Name**（名称）。
4. 输入优先级。
5. 对于 **Redistribute**（重新分发），请选择 **Redist**（重新分发）。
6. 在 **General Filters**（常规筛选器）下选中 **Connect**（连接）和 **Static**（静态）。
7. 单击 **OK**（确定）。



 ©2024 Palo Alto Networks, Inc.

STEP 2 | 配置 OSPF。

1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后单击之前创建的虚拟路由器。
2. 选择 **Router Settings**（路由器设置）> **ECMP**，然后选择 **Enable**（启用）。
3. 选择 **OSPF**，然后选择 **Enable**（启用）。
4. 输入 OSPF **Router ID**（路由器 **ID**）。
5. 在 **Area**（区域）下，单击 **Add**（添加）。
6. 输入 **Area ID**（区域 **ID**）。该值必须与在 APIC 上创建外部路由网络时分配的值匹配。在防火墙上，必须以点分十进制形式输入。例如，如果您在 APIC 中输入的区域 ID 为 10，则防火墙上的等效值为 0.0.0.10。
7. 选择 **Interface**（接口）> **Add**（添加）。
8. 进入连接外部网络 EPG 的界面，然后单击 **OK**（确定）。
9. 选择 **Export Rules**（导出规则）> **Add**（添加）。
10. 从 **Name**（名称）下拉列表中选择重新分发配置文件，然后单击 **OK**（确定）。
11. 选择 **Allow Redistribute Default Route**（允许在分发默认路由）。
12. 单击 **OK**（确定）。



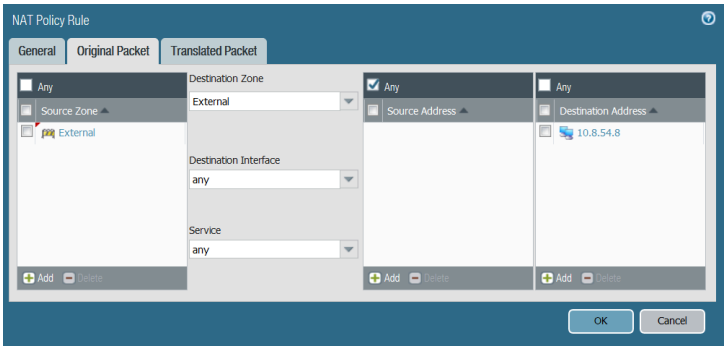
为外部连接配置 NAT

如果防火墙具有用于连接到数据中心外部网络的外部接口，则只需配置 NAT。虽然不需要 NAT，但您可以使用此过程将数据中心的专用 IP 地址转换为外部的公共 IP 地址。为了让流量进入数据中心 EPG 内部的服务器，开始通过配置地址转换来设置 NAT。然后配置 NAT 策略，将来自任何 EPG 的出站流量的源地址转换为外部接口 IP 地址。

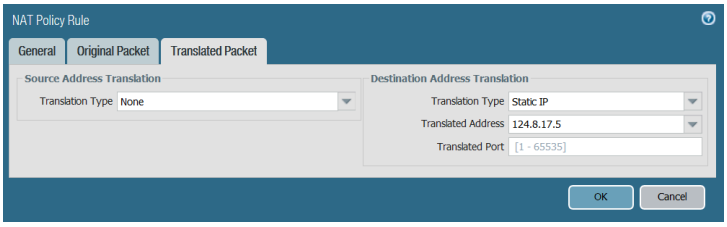
©2024 Palo Alto Networks, Inc.

STEP 1 | 为进入数据中心的 EPG 的流量配置地址转换。

1. 选择 **Policies**（策略）> **NAT**，然后单击 **Add**（添加）。
2. 输入 NAT 策略规则的描述性 **Name**（名称）。
3. 选择 **Original Packet**（原始数据包），然后单击 **Source Zone**（源区域）下的 **Add**（添加）。
4. 从下拉列表中选择源区域。
5. 从 **Destination Zone**（目标区域）下拉列表中选择目标区域。
6. 为 **Source Address**（源地址）选择 **Any**（任何）。
7. 在 **Destination Address**（目标地址）下单击 **Add**（添加）并输入外部 IP 地址。



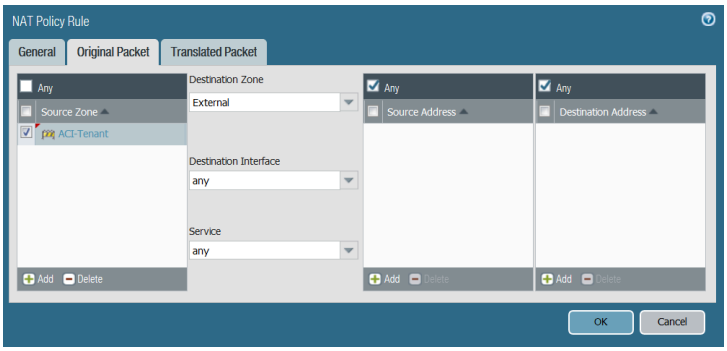
8. 在 **Translated Packet**（转换数据包）选项卡上，选择 **Destination Address Translation**（目标地址转换）下的 **Translation Type**（转换类型）。
9. 从 **Translated Address**（转换地址）下拉列表中选择一个地址。
10. 单击 **OK**（确定）。



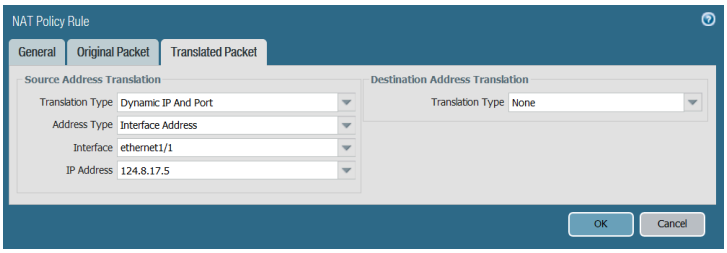
 ©2024 Palo Alto Networks, Inc.

STEP 2 | 配置出站流量的地址转换。

1. 选择 **Policies**（策略）> **NAT**，然后单击 **Add**（添加）。
2. 输入出站 NAT 策略的描述性 **Name**（名称）。
3. 选择 **Original Packet**（原始数据包），然后单击 **Source Zone**（源区域）下的 **Add**（添加）。
4. 选择与您的 ACI 租户和 VRF 匹配的区域。
5. 从 **Destination Zone**（目标区域）下拉列表中选择外部区域。



6. 在 **Translated Packet**（转换数据包）选项卡上，选择 **Source Address Translation**（源地址转换）下的 **Translation Type**（转换类型）。
7. 输入其他所需的地址信息。
8. 单击 **OK**（确定）。



STEP 3 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

Cisco ACI 中的端点监控

适用于 Panorama 的 Cisco ACI 插件允许您使用动态地址组为 Cisco ACI 构建安全策略。该插件监控 Cisco ACI 环境中应用程序策略基础架构控制器 (APIC) 结构的更改，并与 Panorama 共享该信息。安装了 Cisco ACI 插件的每个 Panorama 最多可支持 16 个 APIC 集群。每个监控定义都有一个集群和一个通知组。

Cisco ACI 插件可以监控的端点数量取决于分配给 Panorama 的内存量。如果您有 Panorama 虚拟设备，请确保为环境中的端点分配必要的内存量。有关准备虚拟 Panorama 的详细信息，请参阅 Panorama 管理员指南。

Panorama 内存	端点
8GB	10,000
16GB	20,000

Cisco ACI 插件处理端点信息并将其转换为一组标记，这些标记可用作在动态地址组中放置 IP 地址的匹配条件。标签按以下格式构建：

cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.{epg_<EPG> | uepg_<micro-EPG>}

- **cisco.cl_<cluster>** — 此标记将 IP 地址分组到基于 Cisco ACI 集群的动态地址组中，并显示集群的名称。
- **cisco.cl_<cluster>.tn_<tenant>** — 此标记将 IP 地址分组到基于租户的动态地址组中，并显示集群和租户的名称。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>** — 此标记将 IP 地址分组到基于应用程序配置文件的动态地址组中，并显示集群、租户和应用程序配置文件的名称。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.epg_<EPG>** — 此标记根据 EPG 将 IP 地址分组到动态地址组中，并显示群集、租户、应用程序配置文件和 EPG 的名称。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.uepg_<micro-EPG>** — 此标记根据 micro-EPG 将 IP 地址分组到动态地址组中，并显示群集、租户、应用程序配置文件和 micro-EPG 的名称。
- **cisco.cl_<cluster>.tn_<tenant>.l2out_<L2-external-endpoint>** — 此标记将 IP 地址分组到基于第 2 层外部端点的动态地址组中，并显示集群、租户和第 2 层外部端点的名称。
- **cisco.cl_<cluster>.tn_<tenant>.bd_<bridge-domain>.subnet_<subnet>** — 此标记根据子网将 IP 地址分组到动态地址组中，并显示群集、租户、网桥域和子网的名称。

要检索端点 IP 地址到标记映射信息，必须为 Cisco ACI 环境中的每个 APIC 结构配置监控定义。监控定义指定允许 Panorama 连接到 APIC 的用户名和密码。它还指定了包含 Panorama 推送标记的防火墙的设备组和相应的通知组。配置监控定义并且 Cisco ACI 插件检索标签后，您可以创建动态地址组并将标签添加为匹配条件。

Cisco ACI 插件使用两个间隔从 APIC 检索信息。第一个是监控间隔。

©2024 Palo Alto Networks, Inc.

- 监控间隔 — 监控间间隔是插件在查询结构中的更改之前等待的时间。如果未发生更改，则监控间隔将重置。如果检测到更改，则插件会在重置监控间隔之前处理更改。默认监控间隔为 60 秒。您可以将监控间隔设置为 60 秒到一天（86,400 秒）。
- 完全同步间隔 — 完全同步间隔是插件在从所有结构更新动态对象之前等待的时间量，无论发生任何更改。即使监控间隔遗漏了更改事件，这也可确保插件与结构同步。默认完全同步间隔为 10 分钟。您可以将完全同步间隔设置为 600 秒（10 分钟）和 86,400 秒（一天）。

  您必须通过 Panorama CLI 配置完全同步间隔。

如果将监控间隔的值配置为大于完全同步间隔的值，则会忽略完全同步间隔，并在每个监控间隔执行完全同步。

如果 Panorama 失去与 APIC 的连接，Panorama 将尝试重新连接五次。在五次尝试失败后，Panorama 停止监控集群中的更改并在系统日志中显示重新连接尝试。要恢复并再次开始监视群集，必须在 Panorama 上执行提交。

- 安装适用于 Cisco ACI 的 Panorama 插件
- 配置 Cisco ACI 插件
- 适用于 Cisco ACI 仪表盘的 Panorama 插件

安装适用于 Cisco ACI 的 Panorama 插件

要开始使用 Cisco ACI 进行端点监控，请在 Panorama 上下载并安装 Cisco ACI 插件。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 HA 对中的 Panorama 上安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

©2024 Palo Alto Networks, Inc.

STEP 1 | 验证虚拟 Panorama 是否有足够的存储空间来支持 ACI 环境中的数字端点。

STEP 2 | 选择 **Panorama** > **Plugins**（插件）。

STEP 3 | 选择**Check Now**（立即检查）以检索可用的更新列表。

STEP 4 | 在操作列中选择 **Download**（下载）以下载插件。

STEP 5 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。



配置 Cisco ACI 插件

安装插件后，必须设置监控间隔，配置通知组，并在 Panorama 与 APIC 结构之间建立连接。

STEP 1 | （可选）配置完全同步间隔。

1. 登录到 Panorama 命令行界面。
2. 进入配置模式。

   admin@Panorama> configure
3. 使用以下命令设置完全同步间隔。默认时间为 600 秒（10 分钟）。范围为 600 至 86,400 秒（1 天）。

   admin@Panorama# **set plugins cisco full-sync-interval <interval-in-seconds>**

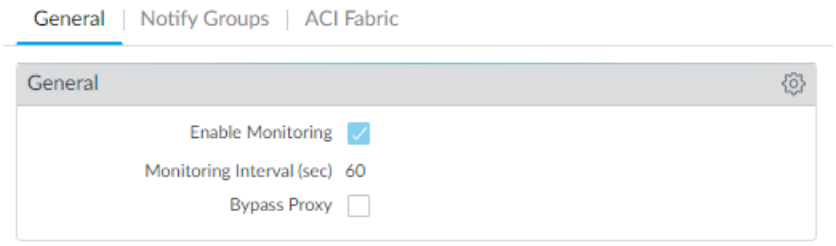
STEP 2 | 登录到 Panorama Web 界面。

STEP 3 | 必须在 Panorama 上添加防火墙作为托管设备，并创建设备组，这样，您可以配置 Panorama 以将检索到的 VM 信息通知这些组。设备组可以包括 VM 系列防火墙或是硬件防火墙上的虚拟系统。

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 启用监控，设置监控间隔，然后启用绕过代理。

1. 选择 **Panorama** > **Cisco ACI** > **Setup**（设置） > **General**（常规）。
2. 选择 **Enable Monitoring**（启用监控）。这样可以监控部署中的所有集群。
3. 以秒为单位设置 **Monitoring Interval**（监控间隔）。监控间隔是 Panorama 从 APIC 检索更新的网络信息的频率。默认值为 60 秒；范围从 60 到 86,400 秒（1 天）。
4. （可选）对于 Panorama 与 APIC 之间的通信，选择绕过代理服务器设置，在 Panorama 下配置 **Panorama** > **Setup**（设置） > **Services**（服务） > **Proxy Server**（代理服务器）。这可允许 Panorama 与 APIC 直接进行通信，同时保持其他服务的代理通信。



STEP 5 | 创建通知组。

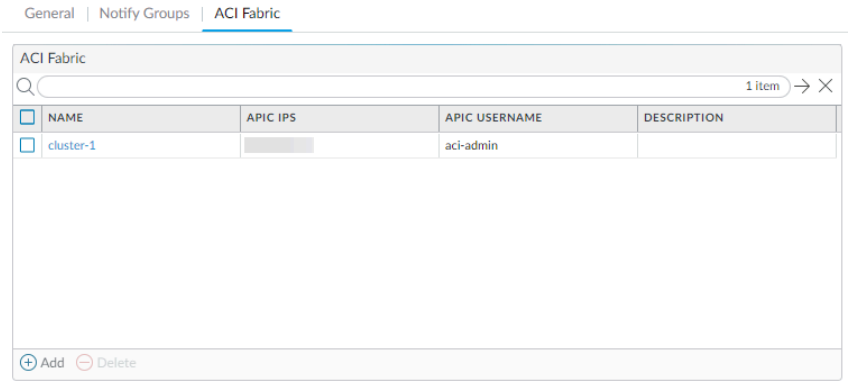
1. 选择 **Panorama** > **Cisco ACI** > **Setup**（设置） > **Notify Groups**（通知组）。
2. 单击 **Add**（添加）。
3. 输入通知组的描述性 **Name**（名称）。
4. 在 ACI 部署中选择设备组。

©2024 Palo Alto Networks, Inc.

STEP 6 | 添加 ACI 结构信息。

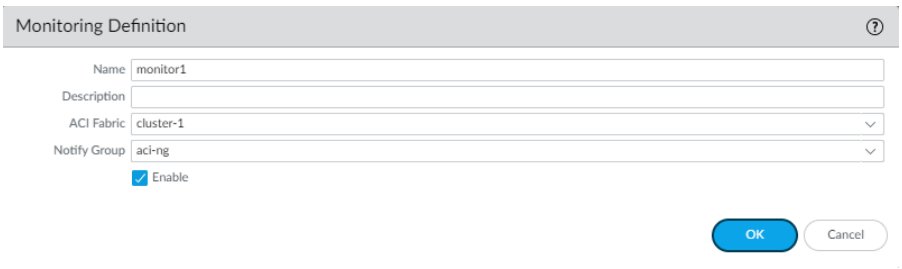
1. 选择 **Panorama** > **Cisco ACI** > **Setup**（设置） > **ACI Fabric**（**ACI** 结构）。
2. 输入集群的描述性 **Name**（名称）。
3. 以逗号分隔列表的形式输入集群中每个 APIC 的 IP 地址或 FQDN。

   使用 *FQDN* 时，请勿在 *URL* 中包含 *https://*。
4. 输入 APIC 用户名。
5. 输入并确认 APIC 密码。
6. 单击 **OK**（确定）。



STEP 7 | 配置监控定义。

1. 选择 **Panorama** > **Cisco ACI** > **Monitoring Definition**（监控）并单击 **Add**（添加）。
2. 输入用于标识使用此定义的 Cisco ACI 集群的描述性 **Name**（名称），也可选择输入说明。
3. 选择 **Cluster Info**（集群信息）和 **Notify Group**（通知组）。
4. 单击 **OK**（确定）。



STEP 8 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 9 | 验证是否可以在 Panorama 上查看 EPG 信息，并定义动态地址组的匹配条件。

某些浏览器扩展程序可能会阻止 *Panorama* 与 *APIC* 之间的 *API* 调用，从而阻止 *Panorama* 接收匹配条件。如果 *Panorama* 未显示匹配条件且您正在使用浏览器扩展程序，请禁用扩展程序和同步动态对象以填充 *Panorama* 可用的标记。

Panorama 不会立即处理新的监控定义和填充动态地址可用的匹配条件。在验证 *EPG* 信息之前，您应等待配置的监控间隔的持续时间。

STEP 10 | 确认 EPG 中的地址已添加到动态地址组中。

1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
2. 在动态地址组的地址列中单击 **More**（更多）。

   Panorama 根据指定的匹配条件显示添加到动态地址组的 IP 地址列表。

STEP 11 | 在策略中使用动态地址组。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），然后为策略输入 **Name**（名称）和 **Description**（说明）。
3. 添加 **Sources Zone**（源区域）来指定产生流量的区域。
4. 添加流量于其中终止的 **Destination Zone**（目标区域）。
5. 对于 **Destination Address**（目标地址），选择刚创建的动态地址组。
6. 为流量指定操作 — **Allow**（允许）或 **Deny**（拒绝），并可选地将默认安全配置文件附加至规则。
7. 重复步骤 1 至 6 来创建另一个策略规则。
8. 单击 **Commit**（提交）。

   有关详细信息，请参阅在策略中使用动态地址组。

©2024 Palo Alto Networks, Inc.

STEP 12 | 您可以通过同步动态对象随时更新 APIC 中的动态对象。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启用应用程序。

1. 选择 **Panorama** > **Cisco ACI** > **Monitoring Definition**（监控定义）。
2. 单击 **Synchronize Dynamic Objects**（同步动态对象）。

在 *HA* 故障转移时，新激活的 *Panorama* 尝试重新连接到 *APIC*，并检索所有监控定义的标记。如果重新连接至甚至一个监控定义时也发生错误，*Panorama* 会生成系统日志消息

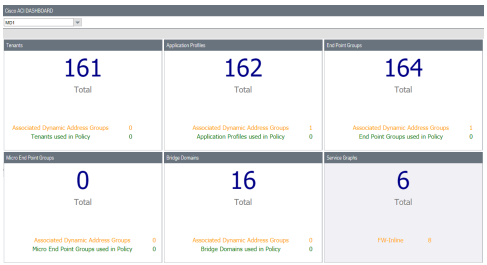
HA 切换后无法处理订阅；需要用户干预。

看到此错误后，必须登录到 *Panorama* 修复此问题。例如，删除 *APIC IP* 或提供有效凭据，提交更改以促使 *Panorama* 重新连接，并检索所有监控定义的标记。即使 *Panorama* 从 *APIC* 断开连接，防火墙也拥有在故障转移前已检索到的所有标记列表，并继续在该 *IP* 地址列表上执行策略。如果在解决故障转移错误之前执行提交，则新激活的 *Panorama* 将不会推送任何 *“IP* 到标记”映射信息并从防火墙清除映射信息。最佳实践是，要监控此问题，可以从 *Panorama* 配置面向操作的日志转发到 HTTP 定义，这样，您可以立即采取行动。

适用于 Cisco ACI 仪表盘的 Panorama 插件

适用于 Cisco ACI 仪表盘的 Panorama 插件概述了插件监控的 ACI 基础架构。仪表盘包含两个页面：第一个页面提供了插件在一组可单击磁贴上监控的各种对象的概述；单击磁贴进入第二个页面，该页面提供了有关磁贴上显示的对象的更多信息。

安装插件后，您可以通过选择 **Panorama** > **Cisco ACI** > **Dashboard**（仪表盘）访问仪表盘。



仪表盘仅查询和统计在 *Panorama* 上配置的前导规则安全策略；不包括后续规则、默认规则或 *NAT* 规则。

仪表盘磁贴	说明
Tenant Tags（租户标记）	显示从 APIC 检索的 Panorama 租户总数。此外，还显示与租户相关联的动态地址组数和策略中使用的租户数。 单击磁贴可深入分析并查看以下列。

©2024 Palo Alto Networks, Inc.

仪表盘磁贴	说明
如果在 *APIC* 上租户的运行状况得分为零 *(0)*，则 *Panorama* 不会检索有关该租户的信息。因此，*Panorama* 上的租户数可能与 *APIC* 上的总数不符。	• **Tenant Name**（租户名称）— 列出 Panorama 检索的所有租户。 • **Tenant Tag**（租户标记）— 与每个租户相关联的 Panorama 标记。 • **Dynamic Address Group**（动态地址组）— 显示与所列标记相关联的动态地址组。 • **In Policy**（在策略中）— 显示是否在策略中使用列出的动态地址组。
Application Profiles（应用程序配置文件）	显示从 APIC 检索的 Panorama 应用程序配置文件总数。此外，还显示与应用程序配置文件相关联的动态地址组数和策略中使用的应用程序配置文件数。 单击磁贴可深入分析并查看以下列。 • **Application Profile Name**（应用程序配置文件名称）— 列出 Panorama 检索的所有应用程序配置文件。 • **Tenant Name**（租户名称）— 显示与列出的应用程序配置文件相关联的租户。 • **Application Profile Tag**（应用程序配置文件标记）— 与每个应用程序配置文件相关联的 Panorama 标记。 • **Dynamic Address Group**（动态地址组）— 显示与所列标记相关联的动态地址组。

©2024 Palo Alto Networks, Inc.

仪表盘磁贴	说明
	• **In Policy**（在策略中）— 显示是否在策略中使用列出的动态地址组。
End Point Groups（端点组）	显示从 APIC 检索的 Panorama 端点组 (EPG) 总数。此外，还显示与 EPG 相关联的动态地址组数和策略中使用的 EPG 数。 单击磁贴可深入分析并查看以下列。 • **EPG Name**（**EPG** 名称）— 列出 Panorama 检索的所有 EPG。 • **Application Profile Name**（应用程序配置文件名称）— 列出与应用程序配置文件相关联的 EPG。 • **Tenant Name**（租户名称）— 显示与列出的应用程序配置文件相关联的租户。 • **EPG Tag**（**EPG** 标记）— 与每个 EPG 相关联的 Panorama 标记。 • **Dynamic Address Group**（动态地址组）— 显示与所列标记相关联的动态地址组。 • **In Policy**（在策略中）— 显示是否在策略中使用列出的动态地址组。
Micro End Point Groups（微端点组）	显示从 APIC 检索的 Panorama 微端点组 (EPG) 总数。此外，还显示与微 EPG 相关联的动态地址组数和策略中使用的微 EPG 数。 单击磁贴可深入分析并查看以下列。 • **Micro EPG Name**（微 **EPG** 名称）— 列出 Panorama 检索的所有 EPG。 • **Application Profile Name**（应用程序配置文件名称）— 列出与应用程序配置文件相关联的微 EPG。 • **Tenant Tag**（租户标记）— 显示与列出的应用程序配置文件相关联的租户。 • **Micro EPG Tag**（微 **EPG** 标记）— 与每个微 EPG 相关联的 Panorama 标记。 • **Dynamic Address Group**（动态地址组）— 显示与所列标记相关联的动态地址组。 • **In Policy**（在策略中）— 显示是否在策略中使用列出的动态地址组。
Bridge Domains（桥接域）	显示从 APIC 检索的 Panorama 桥接域总数。此外，还显示与桥接域相关联的动态地址组数和策略中使用的桥接域数。 单击磁贴可深入分析并查看以下列。 • **Bridge Domain Name**（桥接域名称）— 列出 Panorama 检索的所有桥接域。 • **Tenant Name**（租户名称）— 显示与列出的桥接域相关联的租户。

©2024 Palo Alto Networks, Inc.

仪表盘磁贴	说明
	• **Bridge Domain Tag**（桥接域标记）— 与每个桥接域相关联的 Panorama 标记。 • **Dynamic Address Group**（动态地址组）— 显示与所列标记相关联的动态地址组。 • **In Policy**（在策略中）— 显示是否在策略中使用列出的动态地址组。
Service Graphs（服务图）	显示插件监控的服务图总数，以及与监控的服务图一致的防火墙数。 单击磁贴可深入分析并查看以下列。 • **Service Graph Name**（服务图名称）— 列出 Panorama 检索的所有服务图。 • **Producer EPG**（制作者 **EPG**）— 显示与服务图相关联的制作者 EPG。 • **FW InLine** — 显示与服务图相关联的防火墙。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 Cisco CSP 上设置 VM 系列防火墙

您可以将 VM 系列防火墙作为网络虚拟服务部署到 Cisco Cloud Security Platform (CSP) 上。由于 Cisco CSP 是 RHEL KVM 平台，因此使用 KVM 基本映像的 VM 系列防火墙部署 VM 系列防火墙。

凭借 Cisco CSP 上的 VM 系列防火墙，您可以保护工作负载，防止高级威胁，并提高对虚拟网络上应用程序的可视性。

- Cisco CSP 上的 VM 系列要求
- 在 Cisco CSP 上部署 VM 系列防火墙

Cisco CSP 上的 VM 系列要求

您可以在 Cisco CSP 的 VM 系列防火墙上创建和部署多个实例（作为独立实例或作为 HA 对）。

VM 系列防火墙有下列要求：

- 有关 CSP 和 PAN-OS 的支持版本，请参阅兼容性矩阵。
- 将 引导数据包 转换为 ISO 文件
- 有关 VM 系列型号的最低硬件要求，请参阅 VM 系列系统要求。
- 至少要有两个网络接口 (vNIC)。一个是用于管理接口的专用 vNIC，另一个用于数据接口。您随后可以为数据流量最多添加八个额外的 vNIC。
- Cisco CSP 上的 VM 系列防火墙支持除 VM-50 之外的所有 VM 系列型号。
- 仅 SR-IOV 和数据包 MMAP 模式；不支持 DPDK。

©2024 Palo Alto Networks, Inc.

在 Cisco CSP 上部署 VM 系列防火墙

完成以下过程，在 Cisco CSP 上部署 VM 系列防火墙。

STEP 1 | 从客户支持门户下载 VM 系列 qcow2 基本映像文件。

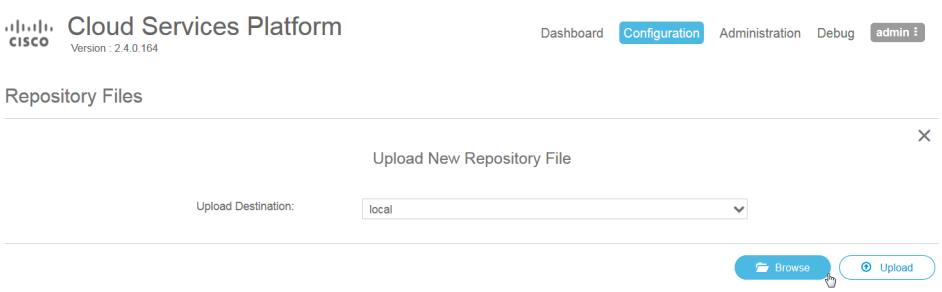
STEP 2 | 为 VM 系列防火墙创建引导 ISO 文件。

1. 为您的 VM 系列防火墙创建引导数据包。
2. 使用首选工具创建包含引导程序包的 ISO 文件。

STEP 3 | 登录到 Cisco CSP Web 界面。

STEP 4 | 上传 VM 系列防火墙 qcow2 映像和 ISO 文件。

1. 选择 **Configuration**（配置） > **Repository**（存储库）。
2. 单击加号 (+) 图标。
3. 单击 **Browse**（浏览）并导航到 qcow2 文件。
4. 单击 **Upload**（上传）。
5. 单击 **Browse**（浏览）并导航到 ISO 文件。
6. 单击 **Upload**（上传）。



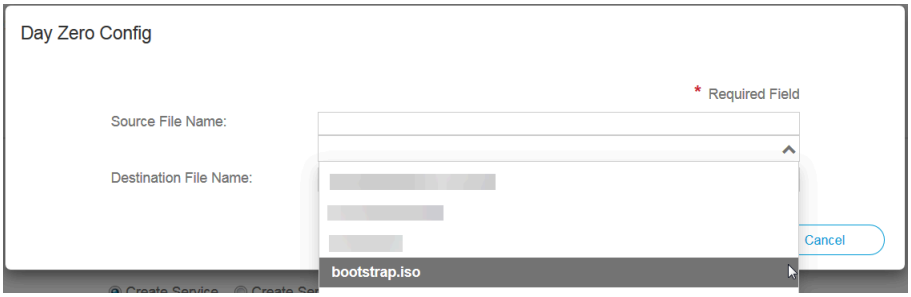
©2024 Palo Alto Networks, Inc.

STEP 5 | 创建 VM 系列防火墙服务。

1. 输入 VM 系列防火墙的描述性 **Name**（名称）。
2. 从下拉列表中选择 **Target Host Name**（目标主机名）。
3. 从 **Image Name**（映像名称）下拉列表中选择上传的 qcow2 文件。



4. 选择 Day Zero Config（零日配置）。
   1. 单击 **Day Zero Config**（零日配置）加号 (+) 图标。
   2. 从 **Source File Name**（源文件名）下拉列表中选择引导程序 ISO 文件。
   3. 单击 **Submit**（提交）。



5. 为 VM 系列防火墙模型分配所需的核心数和内存数。
6. 添加足够的 vNIC 以支持引导 ISO 文件中配置的 VM 系列接口的数量。

有关创建和部署服务实例的详细信息，请参阅Cisco Cloud Service Platform 文档。

STEP 6 | 完成引导过程后，使用引导 ISO 文件中指定的管理 IP 地址登录 VM 系列防火墙。

防火墙应该启动并根据您在引导程序包中定义的参数进行配置。

©2024 Palo Alto Networks, Inc.

Cisco TrustSec 的端点监控

安装和配置适用于 Cisco TrustSec 的 Panorama 插件以检索环境中端点的 IP 地址，并使用动态地址组为这些端点构建安全策略。

- 适用于 Cisco TrustSec 的 Panorama 插件
- 安装适用于 Cisco TrustSec 的 Panorama 插件
- 配置适用于 Cisco TrustSec 的 Panorama 插件
- 排除适用于 Cisco TrustSec 的 Panorama 插件故障

适用于 Cisco TrustSec 的 Panorama 插件

凭借适用于 Cisco TrustSec 的 Panorama 插件，您可以使用动态或静态地址组为 TrustSec 环境创建安全策略。该插件监控 TrustSec 安全组中的变更，以及将该信息注册到 Panorama 并将 IP 信息转发到防火墙，因此 Panorama 可以将正确的策略应用于相应的端点。适用于 Cisco TrustSec 的 Panorama 插件最多支持 16 个 pxGrid (Cisco ISE) 服务器。

Panorama 插件处理端点信息并将其转换为一组标记，您可以将这些标记用作在动态地址组中放置 IP 地址的匹配条件。Panorama 将为 pxGrid 服务器上的每个安全组标记 (SGT) 创建一个标记。标签按以下格式构建：

cts.svr_<pxgrid-server-name>.sgt_<SGT-name>

要检索端点 IP 地址到标记映射信息，必须为环境中的每个 pxGrid 服务器配置监控定义。pxGrid 服务器配置指定用户名和密码，并由允许 Panorama 连接到 pxGrid 服务器的监控定义引用。此外，您可以配置插件以使用 Panorama 上的证书配置文件验证 pxGrid 服务器的身份。它还指定了包含 Panorama 推送标记的防火墙的设备组和相应的通知组。配置监控定义并且插件检索标记后，您可以创建 DAG 并将标记添加为匹配条件。

适用于 Cisco TrustSec 版本 1.0.2 及更高版本的 Panorama 插件支持批量同步和 PubSub 监控模式。该插件会根据 Panorama 版本选择模式：如果 Panorama 版本低于 10.0.0，则选择批量同步模式；如果 Panorama 版本为 10.0.0 及更高版本，则选择 PubSub 模式。用户界面会显示默认监控模式的配置选项。

- 批量同步
- PubSub

批量同步

批量同步模式使用两个间隔从 pxGrid 服务器检索信息 — 监控间隔和完全同步间隔。如果低于 10.0.0 的 Panorama 版本上已安装适用于 Cisco TrustSec 版本 1.0.2 或更高版本的 Panorama 插件，则批量同步模式为默认模式。低于 10.0.0 的 Panorama 版本支持每 10 秒配置一次 IP 选项卡更新。

- 监控间隔 — 监控间隔是插件在查询更改之前等待的时间。如果未发生更改，则监控间隔将重置。如果发生更改，则插件会在重置监控间隔之前处理更改。默认监控间隔为 60 秒。您可以将监控间隔设置为 10 秒到 1 天（86,400 秒）。

  安装适用于 *Cisco TrustSec 1.0.0* 的 *Panorama* 插件时，最小监控间隔为 *30* 秒。

- 完全同步间隔 — 完全同步间隔是插件在从所有 pxGrid 服务器更新动态对象之前等待的时间量，无论发生任何更改。即使监控间隔遗漏了更改事件，这也可确保插件与 pxGrid 服务器同步。您可以将完全同步间隔设置为 600 秒（10 分钟）到 86,400 秒（一天）。您必须从 Panorama CLI 配置完全同步间隔。

如果监控间隔大于完全同步间隔，则会忽略完全同步间隔，并在每个监控间隔执行完全同步。

©2024 Palo Alto Networks, Inc.

PubSub

PubSub 模式直接从 Cisco ISE 服务器（订阅守护程序）监控通知，解析 IP 标记，并将相关信息发送到标记处理守护程序 (tag-proc)。如果 Panorama 版本 10.0.0 或更高版本上已安装适用于 Cisco TrustSec 版本 1.0.2 或更高版本的 Panorama 插件，则 PubSub 模式为默认模式。Panorama 版本 10.0.0 或更高版本支持每 100 毫秒配置一次 IP 选项卡更新。

- 推送间隔 — 推送间隔是两次推送之间的时间量。如果上一次推送花费太多时间，则下一次推送将在上一次推送完成后立即触发。最小推送间隔为 100 毫秒（0 秒），最大推送间隔为 60 秒。默认推送间隔为 0 秒。
- 启用完全同步 — 启用此选项可触发完整更新。如果启用完全同步，则可以设置完全同步间隔。默认为 no（否）。
- 完全同步间隔 — 完全同步间隔是插件在从所有 pxGrid 服务器更新动态对象之前等待的时间量，无论发生任何更改。默认完全同步间隔为 10 分钟。您可以将完全同步间隔设置为 600 秒（10 分钟）到 86,400 秒（一天）。您必须从 Panorama CLI 配置完全同步间隔。
- 重新连接间隔 — 初始重新连接间隔为 1 秒，如果先前的重新连接失败，则重新连接间隔将翻倍。最大重新连接间隔为 64 秒，重新连接尝试次数没有限制。

动态地址与静态地址的区别

您可以使用 Cisco TrustSec 的 Panorama 插件来创建使用动态或静态地址组的安全策略。从 Cisco ISE 服务器收到的映射在被 Panorama 插件框架处理之前进行转换。此转换（表示自定义标记）基于 pxGrid 服务器名称和收到的 SGT：

```
cts.svr_<server-name>.sgt_<SGT-name>
```

SGT 名称在 Cisco ISE 服务器中有三种表示方法：

- 字符串 — 例如，BYOD。
- 十进制数字 — 例如，15。
- 十六进制数字 — 例如，000F。

SGT 名称的格式取决于 SGT 的类型：

- 动态 SGT 使用的 **com.cisco.ise.session** 服务以字符串格式返回标签。此格式可用于将匹配条件配置为：

  ```
  cts.svr_<server-name>.sgt_BYOD
  ```

- 静态 SGT 使用的 **com.cisco.ise.sxp** 服务以十进制格式返回标签。因此，静态 SGT 的匹配条件是：

  ```
  cts.svr_<server-name>.sgt_15
  ```


©2024 Palo Alto Networks, Inc.

您可以在同一地址组中同时包含动态和静态 SGT，但是，匹配条件必须包含两种格式：

```
cts.svr_<server-name>.sgt_BYOD
```

或者

```
cts.svr_<server-name>.sgt.15
```

 ©2024 Palo Alto Networks, Inc.

安装适用于 Cisco TrustSec 的 Panorama 插件

要开始使用 Cisco TrustSec 进行端点监控，请在 Panorama 上下载并安装 Cisco TrustSec 插件。要将插件版本与 Panorama 版本相关联，请参阅兼容性矩阵中的 Panorama 插件。

Cisco TrustSec 插件升级或降级都需要提交。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 HA 对中的 Panorama 设备上安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push yes
  ```

  您可以通过执行以下命令来取消此命令：

  ```
  request plugins dau plugin-name <plugin-name> unblock-device-push no
  ```

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 选择 **Panorama** > **Plugins**（插件）。

STEP 2 | 单击 **Check Now**（立即检查）以获取插件的最新版本。

STEP 3 | 在操作列中选择 **Download**（下载）以下载插件。

STEP 4 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

©2024 Palo Alto Networks, Inc.

配置适用于 Cisco TrustSec 的 Panorama 插件

安装插件后，您还必须将通知组分配给 Cisco TrustSec 插件配置。通知组是设备组的列表，其中包括 Panorama 应向其推送从 pxGrid 服务器检索的所有标记的防火墙。

每个已安装 Cisco TrustSec 插件的 Panorama 最多可以支持 16 个 pxGrid 服务器和 16 个监控定义。每个监控定义都有一个 pxGrid 服务器和一个通知组。

以下配置说明涵盖批量同步和PubSub监控模式；根据监控模式，某些用户界面功能已启用或可见。

STEP 1 | 如果要从默认 600 秒（10 分钟）更改完全同步间隔，请进行配置。

1. 登录到 Panorama 命令行界面。
2. 进入配置模式。

   ```
   admin@Panorama> configure
   ```
3. 使用以下命令设置完全同步间隔。范围为 600 至 86,400 秒（1 天）。

   ```
   admin@Panorama# set plugins cisco_trustsec full-sync-interval
   <interval-in-seconds>
   ```

STEP 2 | 登录到 Panorama Web 界面。

STEP 3 | 必须在 Panorama 上添加防火墙作为托管设备，并创建设备组，这样，您可以配置 Panorama 以将检索到的 VM 信息通知这些组。设备组可以包括 VM 系列防火墙或是硬件防火墙上的虚拟系统。

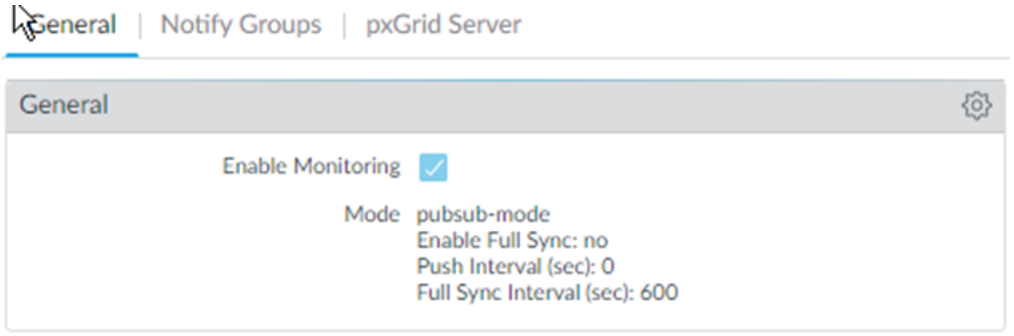
©2024 Palo Alto Networks, Inc.

STEP 4 | 配置 Cisco TrustSec 监控。

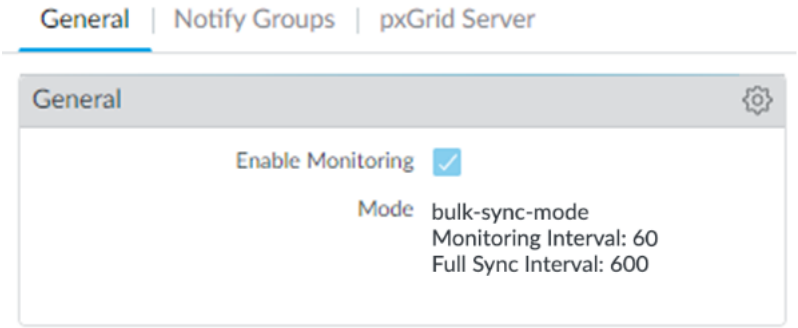
1. 选择 **Panorama** > **Cisco TrustSec** > **Setup**（设置） > **General**（常规）。

   默认启用 **Enable Cisco TrustSec Monitoring**（启用 **Cisco TrustSec** 监控）。这样可以监控部署中的所有集群。

   如果在 Panorama 10.0.0 或更高版本上安装适用于 Cisco TrustSec 的 Panorama 插件为 1.0.2 或更高版本，则用户界面将选择 PubSub 监控模式：

   如果在 Panorama 10.0.0 之前的版本中安装，则该插件会选择批量同步模式：

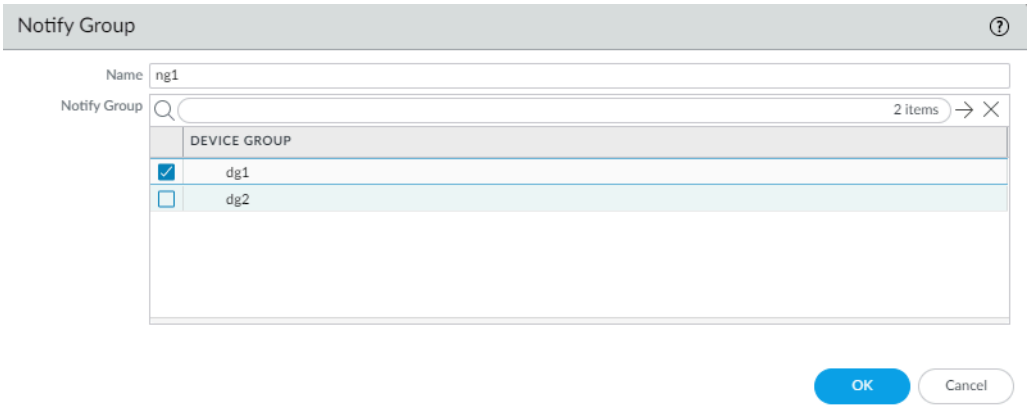
2. 单击齿轮以编辑设置参数。

   - 推送间隔（仅限 PubSub）— 最小为 0 秒，最大为 60 秒，默认值为 0（100 毫秒）。
   - 启用完全同步（仅限 PubSub，可选）— 选择该选项可启用完全同步。默认为 no（否）。
   - 完全同步间隔。
     - PubSub — 如果选择 Enable Full Sync（启用完全同步），则可以设置完全同步间隔（以秒为单位）。范围为 600 秒至 86400 秒（一天），默认值为 600 秒。
     - 批量同步 — 在批量同步模式下默认启用。范围为 600 秒至 86400 秒（一天），默认值为 600 秒。
   - 监控间隔（仅限批量同步）— 10 秒至 86400 秒，默认值为 60 秒 — 设置 Panorama 向 pxGrid 服务器查询端点地址信息的轮询间隔。这是监控事件结束与下一个事件开始之间的时间段。

©2024 Palo Alto Networks, Inc.

STEP 5 | 创建通知组。

1. 选择 **Panorama** > **Cisco TrustSec** > **Setup**（设置） > **Notify Groups**（通知组）。
2. 单击 **Add**（添加）。
3. 输入通知组的描述性 **Name**（名称）。
4. 选择先前创建的设备组。



STEP 6 | （可选）如果启用 pxGrid 服务器的服务器身份验证，请在 Panorama 上配置证书配置文件。

STEP 7 | 创建、激活和核准 pxGrid 客户端名称和客户端密码。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令以创建客户端名称。
   - 如果您拥有证书配置文件，请按如下所示创建客户端名称：

     admin@Panorama> request plugins cisco_trustsec create-account client-name <client-name> host <ise-server-ip>
   - 如果您跳过步骤 6 且没有证书，请输入：

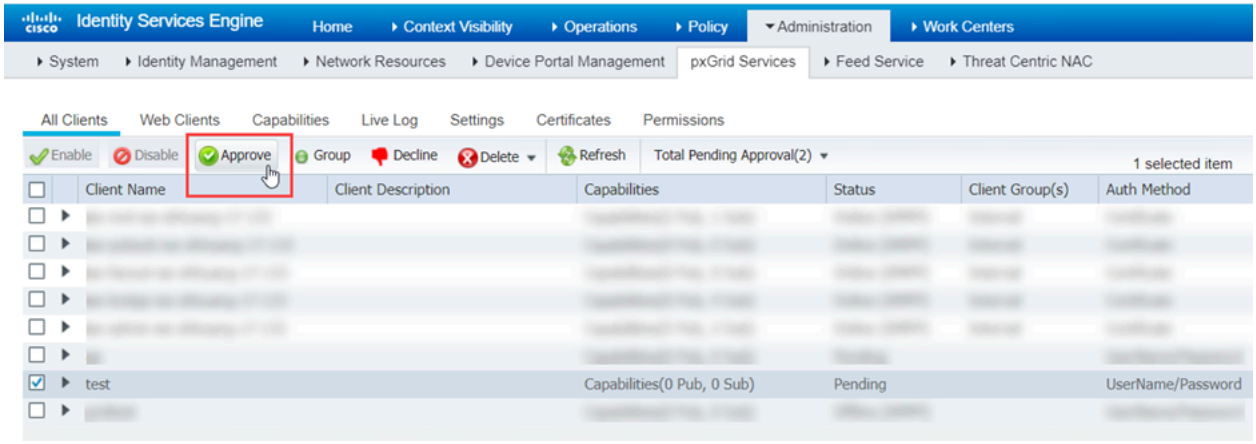
     request plugins cisco_trustsec create-account server-cert-verification-enabled no client-name <client-name>host <host-name>
3. 执行以下命令以创建客户端名称。

```
admin@Panorama> request plugins cisco_trustsec create-
account client-name test host 10.10.10.15 AccountCreate in
 progress...AccountCreate successful.   client nodename:
 test client password:PmVKBmPgf63Hypq AccountActivate in
```


©2024 Palo Alto Networks, Inc.

```
progress...AccountActivate successful.Please approve the
account on the server.
```

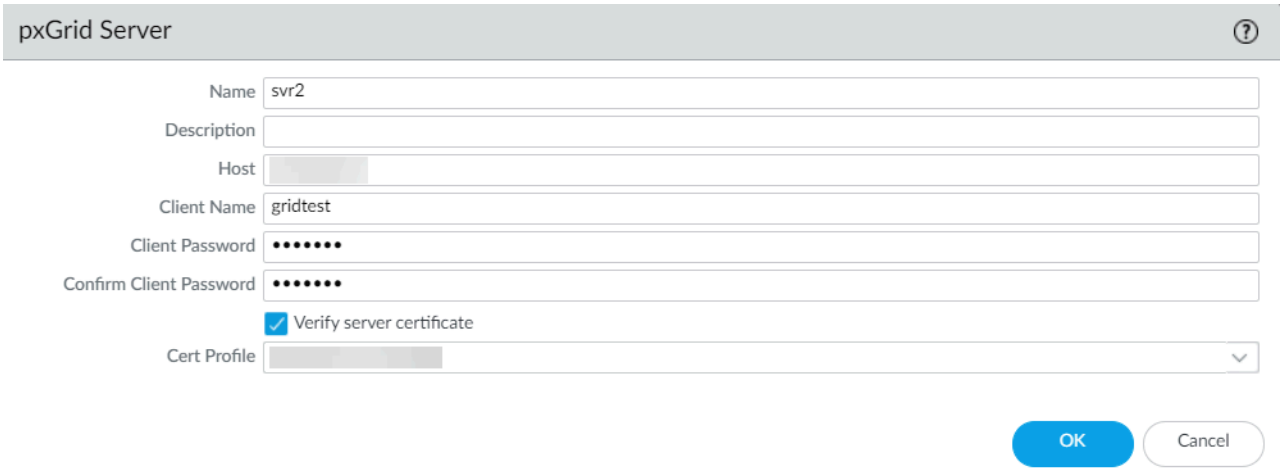
4. 登录到 Cisco ISE 服务器以核准帐户。
5. 选择 **Administration**（管理）> **pxGrid Services**（**pxGrid** 服务）> **All Clients**（所有客户端）。
6. 选择在 Panorama 上创建的客户端名称。
7. 单击 **Approve**（核准）。



©2024 Palo Alto Networks, Inc.

STEP 8 | 添加 pxGrid 服务器信息。适用于 Cisco TrustSec 的 Panorama 插件最多支持 16 个 pxGrid (Cisco ISE) 服务器。

1. 选择 **Panorama** > **Cisco TrustSec** > **Setup**（设置） > **pxGrid Server**（**pxGrid** 服务器）。
2. 输入 pxGrid 服务器的描述性 **Name**（名称）。
3. 在 **Host**（主机）字段中，输入 pxGrid 服务器的 IP 地址或 FQDN。
4. 输入在上一步中创建的客户端名称。
5. 输入并确认在上一步中生成的客户端密码。
6. 验证 pxGrid 服务器身份。
   1. 选择 **Verify server certificate**（验证服务器证书）。
   2. 从 **Cert Profile**（证书配置文件）下拉列表中选择证书配置文件。
7. 单击 **OK**（确定）。



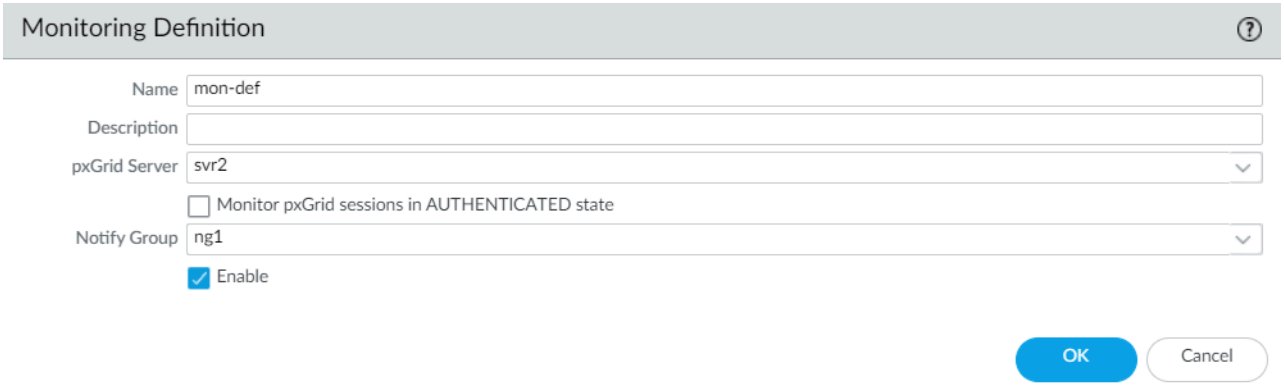
STEP 9 | 配置监控定义。

1. 选择 **Panorama** > **Cisco TrustSec** > **Monitoring Definition**（监控定义），然后单击 **Add**（添加）。
2. 输入描述性 **Name**（名称），也可以输入 **Description**（说明）以标识监控定义。
3. 选择 **pxGrid Server**（**pxGrid Server**（**pxGrid** 服务器）。
4. （可选）将 Panorama 设置为 **Monitor pxGrid sessions in AUTHENTICATED state**（在“身份验证”状态下监控 **pxGrid** 会话）。默认情况下，Panorama 从处于“已开

©2024 Palo Alto Networks, Inc.

始”状态的会话中检索 IP 标签映射。如果存在相应的记帐开始数据包，则 ISE 会话将处于“已开始”状态。如果会话不存在任何记帐开始数据包，则会话状态为“身份验证”。

5. 选择 **Notify Group**（通知组）。
6. 单击 **OK**（确定）。



STEP 10 | **Commit**（提交）更改。

STEP 11 | 创建活动 ISE 会话，以便 Panorama 可以了解动态或静态地址组定义的 SGT 标签。要创建活动会话，请使用 ISE 对设备进行身份验证。

Panorama 不会在 ISE 上收集默认 SGT 标签。

©2024 Palo Alto Networks, Inc.

STEP 12 | 创建动态或静态地址组并验证是否已添加地址。

1. 选择 **Object**（对象） > **Address Groups**（地址组）。
2. 从 **Device Group**（设备组）下拉列表中，选择创建用于监控 Cisco TrustSec 环境中的端点的设备组。
3. 单击 **Add**（添加），然后为地址组输入 **Name**（名称）和 **Description**（说明）。

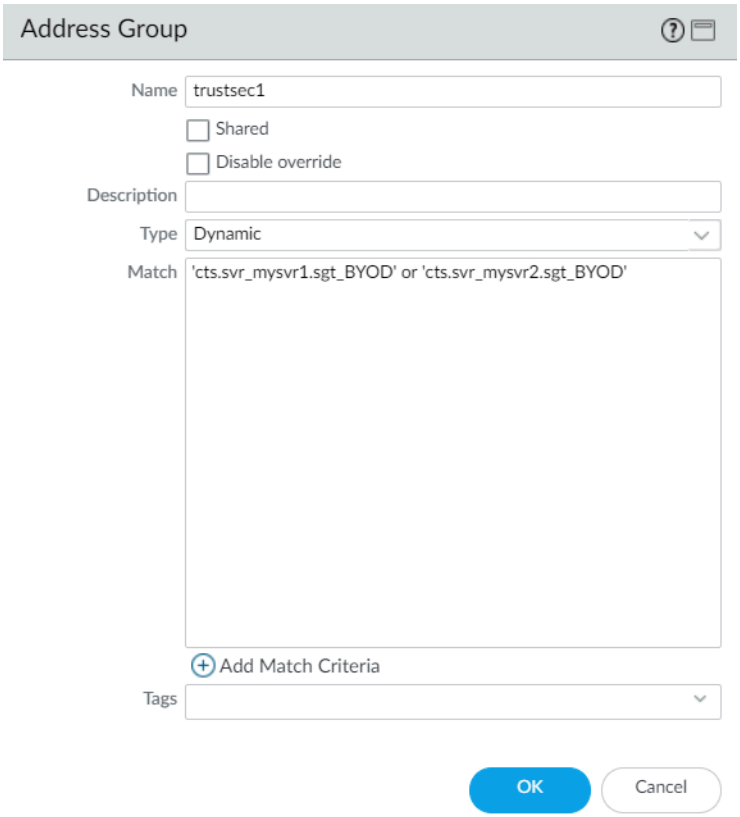
   动态地址组命名约定为：**`cts.svr_<server-name>.sgt_<SGT-name>`**

   静态组的命名约定为：

   `cts.svr_<server-name>.sgt_<SGT-decimal number>`
4. 选择 **Dynamic**（动态）或 **Static**（静态）作为 **Type**（类型）。
5. 单击 **Add Match Criteria**（添加匹配条件）。
6. 选择 **And** 或 **Or** 运算符，并单击安全组名称旁边的加号 (+) 图标，将其添加到动态地址组。

   Panorama 只能显示从活动会话了解的安全组标签。实时会话中的安全组标签显示在匹配条件列表中。
7. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
8. 在动态地址组的地址列中单击 **More**（更多）。

   Panorama 根据指定的匹配条件显示添加到动态地址组的 IP 地址列表。



 ©2024 Palo Alto Networks, Inc.

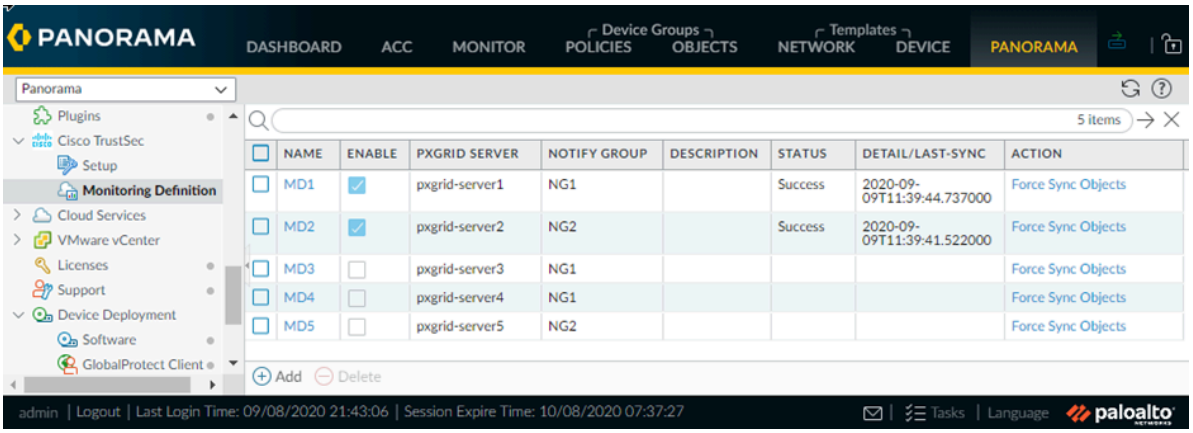
STEP 13 | 在策略中使用动态地址组。

动态地址组为空，直到将其附加到策略。除非策略正在使用它，否则您不会在动态地址组中看到任何 *IP* 地址。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），然后为策略输入 **Name**（名称）和 **Description**（说明）。
3. 添加 **Sources Zone**（源区域）来指定产生流量的区域。
4. 添加流量于其中终止的 **Destination Zone**（目标区域）。
5. 对于 **Destination Address**（目标地址），选择刚创建的动态地址组。
6. 为流量指定操作 — **Allow**（允许）或 **Deny**（拒绝），并可选地将默认安全配置文件附加至规则。
7. 重复步骤 1 至 6 来创建另一个策略规则。
8. 单击 **Commit**（提交）。

STEP 14 | （可选）通过同步对象，您可以随时更新 pxGrid 服务器中的对象。同步对象使您能够维护虚拟环境中关于变化的上下文，还允许您通过自动更新策略规则中使用的动态地址组来启用应用程序。

1. 选择 **Panorama** > **Cisco TrustSec** > **Monitoring Definition**（监控定义）。
2. 单击 **Synchronize Dynamic Objects**（同步动态对象）。



 ©2024 Palo Alto Networks, Inc.

排除适用于 Cisco TrustSec 的 Panorama 插件故障

- 插件状态命令
- 调试命令
- 调试日志

插件状态命令

- 清除计数器：

```
clear plugins cisco_trustsec counters
```

- 显示监视器状态：

```
show plugins cisco_trustsec status
```

- 显示计数器：

```
show plugins cisco_trustsec counters
```

调试命令

- 检查动态地址组中的 IP 地址。

```
show object registered-ip tag <tag>
```

```
show object registered-ip all
```

- 从服务器获取 IP 地址的标记。获取的 IP 地址标记映射记录在 `plugin_cisco_trustsec.log` 中。不会将任何 IP 地址标记映射推送到与服务器相关联的通知组。如果失败，则不重试。

```
debug plugins cisco_trustsec query pxgrid-server $server-name ip
 $ip-address
```

- 强制与服务器同步，然后将映射推送到配置的进程。如果失败，则不重试。

```
request plugins cisco_trustsec synchronize-dynamic-objects name
 $server-name
```


©2024 Palo Alto Networks, Inc.

- 强制与所有服务器同步，然后将映射推送到配置的进程。如果失败，则不重试。

```
request plugins cisco_trustsec synchronize-dynamic-objects all
```

- 强制将映射从配置的进程同步到 VM 系列防火墙。如果失败，则不重试。

```
request plugins cisco_trustsec sync
```

调试日志

日志位于磁盘上的以下位置：

```
/opt/plugins/var/log/pan/plugin_cisco_trustsec.log /opt/plugins/
var/log/pan/plugin_cisco_trustsec_sub.log /opt/plugins/var/
log/pan/plugin_cisco_trustsec_ret.log /opt/plugins/var/log/pan/
plugin_cisco_trustsec_proc.log
```

日志文件的大小限制（由 Panorama 设备上安装的所有插件共享）为 10MB。日志文件可以接受 93,000 次会话登录。如果配置日志轮转，则备份日志可以支持 186,000 次会话登录。

- 更改插件调试级别。

```
request plugins debug level $level plugin-name cisco_trustsec
```

  - **off**（关）：没有调试日志。
  - **low**（低）：仅转储基本调试日志。
  - **medium**（中）：转储详细的调试日志。
  - **high**（高）：转储所有调试日志，包括与服务器的请求/响应消息。
- 将日志合并到一个日志文件：

```
request plugins cisco_trustsec merge-logs
```

- 在 CLI 中显示调试日志：
  - 在低于 10.0.0 的 Panorama 版本上安装 Cisco TrustSec 插件版本 1.0.2 或更高版本：

```
tail mp-log plugin_cisco_trustsec_merged.log
```

  - 在 Panorama 版本 10.0.0 或更高版本上安装 Cisco TrustSec 插件版本 1.0.2 或更高版本：

```
tail follow yes plugins-log
```


©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

在 Nutanix AHV 上设置 VM 系列防火墙

通过适用于 Nutanix AHV 的 VM 系列防火墙，您可以在能够运行 Nutanix Acropolis Hypervisor 的设备上部署 VM 系列防火墙。如果您使用 Panorama 管理 Nutanix AHV 上的 VM 系列防火墙，则可以使用适用于 Nutanix 的 Panorama 插件执行 VM 监控。这可以让您动态通知 Nutanix 环境中的防火墙变更，并确保在虚拟机加入网络时为其应用策略。

- 在 Nutanix AHV 上部署 VM 系列防火墙
- Nutanix 上的 VM 监控

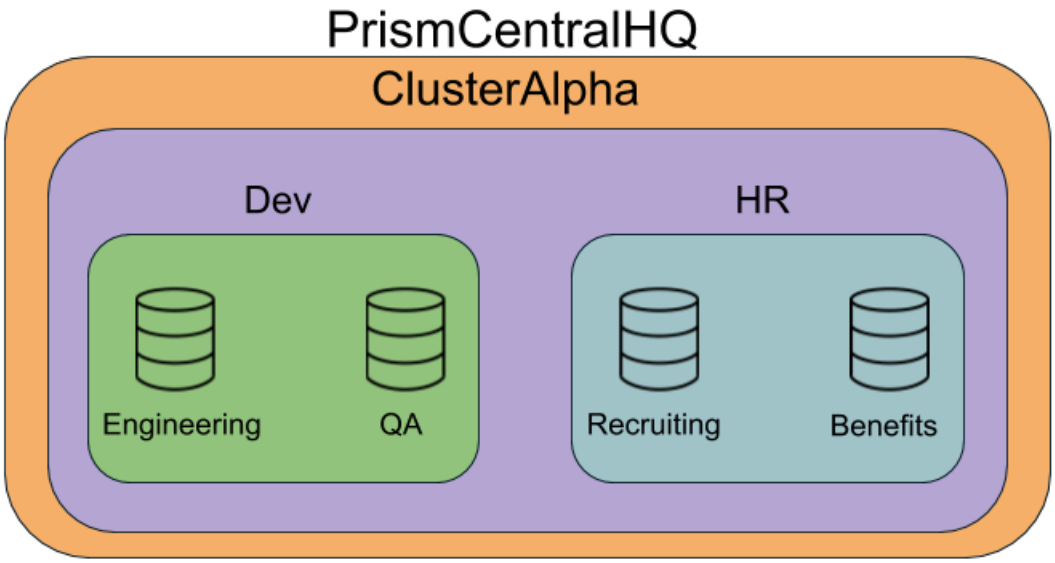
Nutanix 上的 VM 监控

安装和配置适用于 Nutanix 的 Panorama 插件，以监控 Nutanix 环境中的变化并使用动态地址组构建策略。

- 关于 Nutanix 上的 VM 监控
- 安装适用于 Nutanix 的 Panorama 插件
- 配置适用于 Nutanix 的 Panorama 插件

关于 Nutanix 上的 VM 监控

适用于 Nutanix 的 Panorama 插件通过监控 Nutanix 环境中的虚拟机来促进使用动态地址组。Prism Central 按类别对 Nutanix 环境中的实体进行分组，并按值进一步筛选。Panorama 根据您在 Prism Central 中定义的类别和值创建标记。将虚拟机放入类别中并为其分配值后，Panorama 会将相应的标记应用于虚拟机的 IP 地址。然后，您可以通过使用标记作为 Panorama 中动态地址组的匹配条件来创建安全策略。



在上例中，我们有两个类别（Dev 和 HR），每个类别中都有两个值。并且，这两个类别都位于 Prism Central 中的集群内。开始监控 Nutanix 环境后，Panorama 将使用值、类别、集群和 Prism Central 形成标记。当您查看动态地址组的匹配条件时，标记将按以下格式列出。

ntnx.PC-<prism-central-name>.CL-<cluster-name>.<category>.<value>

通过使用上例中的信息，Panorama 可以创建以下标记。

```
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.Engineering
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.QA
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Recruiting
```


©2024 Palo Alto Networks, Inc.

```
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Benefits
```

为了保护这些类别中的这些工作负载，可以在动态地址组中使用诸如此类的标记作为匹配条件。然后，您可以在安全策略规则中使用动态地址组作为源和目标地址组。虚拟机加入动态地址组后，将自动应用您创建的策略。

安装适用于 Nutanix 的 Panorama 插件

要开始监控 Nutanix 上的端点，请下载并安装适用于 Nutanix 的 Panorama 插件。

如果拥有 Panorama HA 配置，则在每个 Panorama 对等上重复此安装过程。在 HA 对中的 Panorama 上安装插件时，请在主动对等之前将该插件安装在被动对等上。在被动对等上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

如果在高可用性对中安装了独立的 Panorama 设备或两台 Panorama 设备，并且安装了多个插件，那么，如果未配置一个或多个插件，则可能不会收到更新的 IP 标记信息。这是因为 Panorama 不会将 IP 标记信息转发到未配置的插件。此外，如果一个或多个 Panorama 插件的状态不是“已注册”或“成功”（每个插件的正常状态不同），则可能会出现此问题。继续或执行下述命令之前，请确保插件处于正常状态。

如果遇到此问题，可使用两种解决方法：

- 卸载未配置的一个或多个插件。建议不要安装不计划立即配置的插件
- 您可以使用以下命令来解决此问题。对每个 Panorama 实例上的各未配置插件执行以下命令，以防止 Panorama 等待发送更新。否则，防火墙可能会丢失一些 IP 标记信息。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以通过执行以下命令来取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

所述命令在重启后不会持久执行，对于任何后续重启，您必须再次执行命令。对于 HA 对中的 Panorama，必须在每个 Panorama 上执行命令。

STEP 1 | 登录到 Panorama 用户界面。

STEP 2 | 选择 **Panorama** > **Plugins**（插件）。

STEP 3 | 选择**Check Now**（立即检查）以检索可用的更新列表。

STEP 4 | 在操作列中选择 **Download**（下载）以下载插件。

STEP 5 | 选择插件的版本并在 Action（操作）列中点击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

配置适用于 Nutanix 的 Panorama 插件

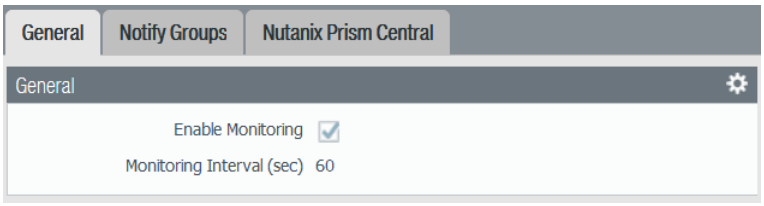
安装插件后，请完成以下过程以在 Panorama 和 Prism Central 之间建立连接。

STEP 1 | 登录到 Panorama Web 界面。

 ©2024 Palo Alto Networks, Inc.

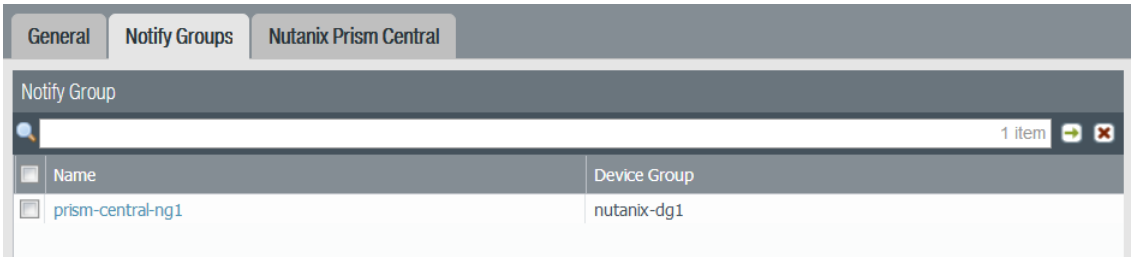
STEP 2 | 启用监控并设置监控间隔。

1. 选择 **Panorama** > **Nutanix** > **Setup**（设置） > **General**（常规）。
2. 选择 **Enable Monitoring**（启用监控）。
3. 以秒为单位设置 **Monitoring Interval**（监控间隔）。监控间隔是 Panorama 从 Prism Central 检索更新的网络信息的频率。



STEP 3 | 创建通知组。

1. 选择 **Panorama** > **Nutanix** > **Setup**（设置） > **Notify Groups**（通知组）。
2. 单击 **Add**（添加）。
3. 输入通知组的描述性 **Name**（名称）。
4. 在 Nutanix 部署中选择设备组。



©2024 Palo Alto Networks, Inc.

STEP 4 | 添加 Prism Central 信息。

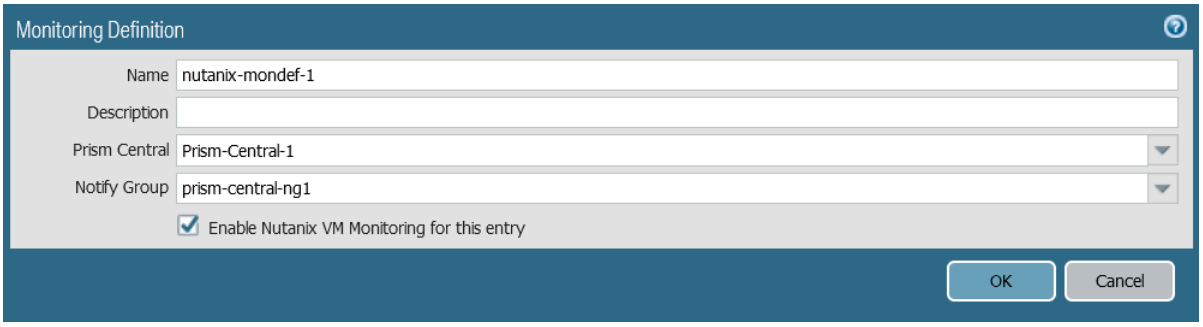
1. 选择 **Panorama** > **Nutanix** > **Setup**（设置） > **Nutanix Prism Central**。
2. 单击 **Add**（添加）。
3. 输入 Prism Central 的描述性 **Name**（名称）。
4. 输入 Prism Central 的 IP 地址或 FQDN。
5. 输入 Prism Central 用户名。
6. 输入并确认 Prism Central 密码。
7. 单击 **Validate**（验证）以确认您已正确输入 Prism Central 凭据。

   如果单击 *OK*（确定）后返回 *Nutanix Prism Central Info*（*Nutanix Prism Central* 信息）窗口，则单击 *Validate*（验证）按钮可返回凭据验证错误消息。这是预期的行为。尽管 *Panorama* 在密码字段中显示点，但该字段为空；即使 *Panorama* 已成功连接到 *Prism Central*，这也会导致验证失败。
8. 单击 **OK**（确定）。



STEP 5 | 配置监控定义。

1. 选择 **Panorama** > **Nutanix** > **Monitoring Definition**（监控定义），然后单击 **Add**（添加）。
2. 输入用于标识使用此定义的 Prism Central 的描述性 **Name**（名称），也可选择输入说明。
3. 选择 **Prism Central** 和 **Notify Group**（通知组）。
4. 单击 **OK**（确定）。

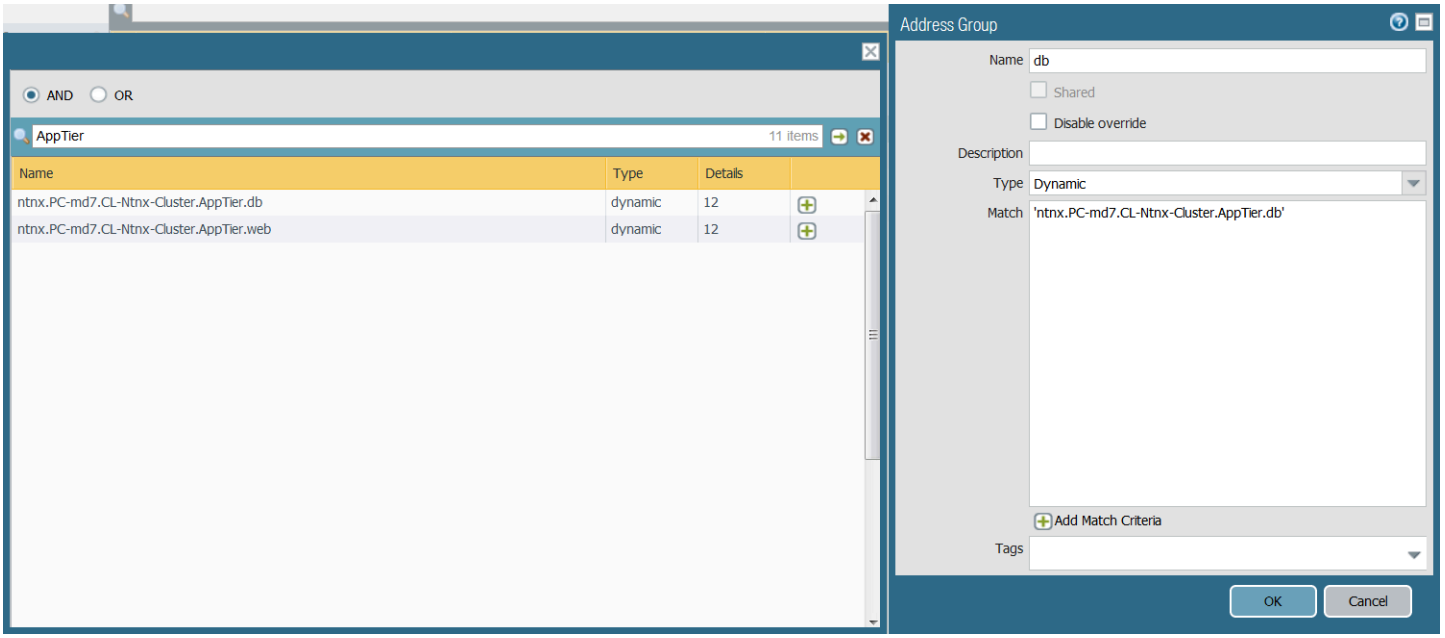


STEP 6 | **Commit**（提交）更改。

©2024 Palo Alto Networks, Inc.

STEP 7 | 验证是否可以在 Panorama 上查看 VM 信息，并定义动态地址组的匹配条件。

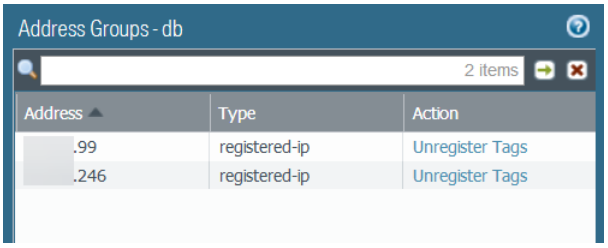
1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组），然后单击 **Add**（添加）。
2. 输入动态地址组的描述性 **Name**（名称）。
3. 从 Type（类型）下拉列表中选择 **Dynamic**（动态）。
4. 单击 **Add Match Criteria**（添加匹配条件）。您可将动态标记选择为匹配条件来填充组成员。选择 **And** 或 **Or** 运算符以及您想要筛选或排除的属性，然后单击 **OK**（确定）。
5. **Commit**（提交）更改。



STEP 8 | 确认 VM 中的地址已添加到动态地址组中。

1. 选择 **Panorama** > **Objects**（对象） > **Address Groups**（地址组）。
2. 在动态地址组的地址列中单击 **More**（更多）。

   Panorama 根据指定的匹配条件显示添加到动态地址组的 IP 地址列表。



©2024 Palo Alto Networks, Inc.

STEP 9 | 在策略中使用动态地址组。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 单击 **Add**（添加），然后为策略输入 **Name**（名称）和 **Description**（说明）。
3. 添加 **Sources Zone**（源区域）来指定产生流量的区域。
4. 添加流量于其中终止的 **Destination Zone**（目标区域）。
5. 对于 **Destination Address**（目标地址），选择刚创建的动态地址组。
6. 为流量指定操作 — **Allow**（允许）或 **Deny**（拒绝），并可选地将默认安全配置文件附加至规则。
7. 重复步骤 1 至 6 来创建另一个策略规则。
8. 单击 **Commit**（提交）。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

引导 VM 系列防火墙

通过引导功能，您可以创建一个可重复的简化流程，以便在您的网络上部署新的 VM 系列防火墙；具体来说，该功能允许您为网络创建一个带有模型配置的数据包，然后使用该数据包在任何位置部署 VM 系列防火墙。

您可以使用完整配置引导防火墙，以便在启动时对防火墙进行完全配置，也可以从基本配置开始 — 用来引导防火墙，然后注册到 Panorama 以完成配置的最小初始配置。

如果您选择基本配置且要在 AWS、Azure 或 GCP 上部署时，则可以使用引导数据包和 `init-cfg.txt` 文件。或者，您可以使用用户数据进行引导。在启动 VM 系列防火墙时，无需在文件中提供引导配置参数，而是在 AWS 或 GCP 用户界面中将它们作为键值对直接输入。Azure 具有类似的流程，您可以通过该流程从 Azure CLI 访问的模板或其他文本文件中提供引导参数。

如果您创建引导数据包，则可以从外部设备（例如虚拟磁盘、虚拟 CD-ROM 或云存储设备（例如存储桶）交付。

- 选择引导方法
- VM 系列防火墙引导工作流程
- 引导数据包
- 引导配置文件
- 在 Panorama 上生成 VM 身份验证密钥
- 创建 init-cfg.txt 文件
- 创建 bootstrap.xml 文件
- 准备引导许可证
- 准备引导数据包
- 在 AWS 上引导 VM 系列防火墙
- 在 Azure 上引导 VM 系列防火墙
- 在 ESXi 上引导 VM 系列防火墙
- 在 Google Cloud Platform 上引导 VM 系列防火墙
- 在 Hyper-V 上引导 VM 系列防火墙
- 在 KVM 上引导 VM 系列防火墙
- 验证引导完成
- 引导错误

选择引导方法

您可以使用基本配置或完整配置引导 VM 系列防火墙。

完整配置使用引导数据包，并包含在启动时完全配置防火墙所需的所有内容。这包含配置参数（init-cfg.txt 文件中）、内容更新和软件版本。完整配置可以同时包含 init-cfg.txt 和 bootstrap.xml 文件。

配置方法	配置位置	注释
在引导数据包的 /config/bootstrap.xml 中指定完整配置信息。	公共云存储 AWS S3 存储桶、Azure 存储帐户或 Google 存储桶。	• 存储桶中的完整引导数据包。 • 需要云存储和 IAM 角色才能访问它。

基本配置是能让您启动、许可和注册 VM 系列防火墙的最小配置。基本配置不支持插件、内容、软件映像或 bootstrap.xml。

启动防火墙后，您可以与 Panorama 建立连接以完成配置，或登录到防火墙以手动更新内容和软件。下表简要对比了可以存储和访问基本配置的三种方式：

配置方法	配置位置	注释
init-cfg.txt 将基本配置参数作为键值对存储在引导数据包的 config/init-cfg.txt 中。	公共云存储 • AWS S3 存储桶 • Azure 存储帐户 • GCP 存储桶	• 需要云存储和 IAM 角色才能访问它。还必须向 Panorama 管理员授予访问存储桶的权限。
用户数据 在公共云用户界面中输入配置参数作为键值对。	**VM** 实例 • Alibaba：用户数据 • AWS：用户数据 • Azure：自定义数据 • GCP：GCP 元数据 • Oracle 云基础架构：用户数据	• 初始配置参数存储在 VM 中。 • 无需单独的存储和关联的 IAM 角色。
AWS 密钥管理器 在 AWS 密钥管理器中输入配置参数作为键值对。	在 AWS 密钥管理器中加密。	• 您需要 IAM 角色才能创建密钥。可以向其他人授予获取密钥的权限。

©2024 Palo Alto Networks, Inc.

配置方法	配置位置	注释
		• 要获取密钥，请使用用户数据传递密钥名称。

请参阅 VM 系列防火墙引导工作流程，以比较基本配置和完整配置的工作流程。

- 基本配置
- 完整配置

基本配置

基本配置包含初始配置和许可证。您可以使用引导数据包传递初始配置的键值对，也可以输入引导参数键值对作为用户数据。

如果您不使用 Panorama，则可以使用初始配置引导防火墙，然后登录并手动完成配置。如果您使用 Panorama，则初始配置必须包含 Panorama 服务器 IP 地址和 VM 身份验证密钥的引导参数，以便引导防火墙可以注册到 Panorama 并完成完整配置。

- 将基本配置添加到引导数据包
- 输入基本配置作为用户数据（公共云）
- 在 AWS 密钥管理器中保存基本配置

将基本配置添加到引导数据包

初始配置是最小配置，您可以用来启动、许可和注册 VM 系列防火墙，以及与 Panorama 建立连接（如果适用）。您可以在引导数据包中交付配置 (init-cfg.txt)。

输入基本配置作为用户数据（公共云）

当您从公共云用户界面部署 VM 系列防火墙时，可以在启动/部署过程中输入配置参数作为用户数据。如果您有足够的权限从云帐户部署防火墙，并访问 Panorama（如果您正在使用），则可以跳过创建引导数据包，创建配置文件，以及与云存储相关的其他引导任务（存储桶、IAM 角色或授予外部存储访问权限的服务帐户）。

配置参数包含init-cfg.txt 文件组件中的值和以下仅用作用户数据的附加值：

- **authcodes** — 用于注册 VM 系列防火墙。例如，**authcodes=I7115398**。
- **mgmt-interface-swap** — 当 VM 系列防火墙位于 AWS 或 GCP 部署中的负载均衡器背后时，用于交换管理接口。例如，**mgmt-interface-swap=enable**。

您可以直接在 Alibaba、AWS、GCP 或 OCI 用户界面中输入配置参数作为键值对。此外，您还可以从文本文件或云原生模板定义配置，例如 AWS Cloud Formation 模板、Azure ARM 模板、GCP YAML 文件或 Terraform 模板。

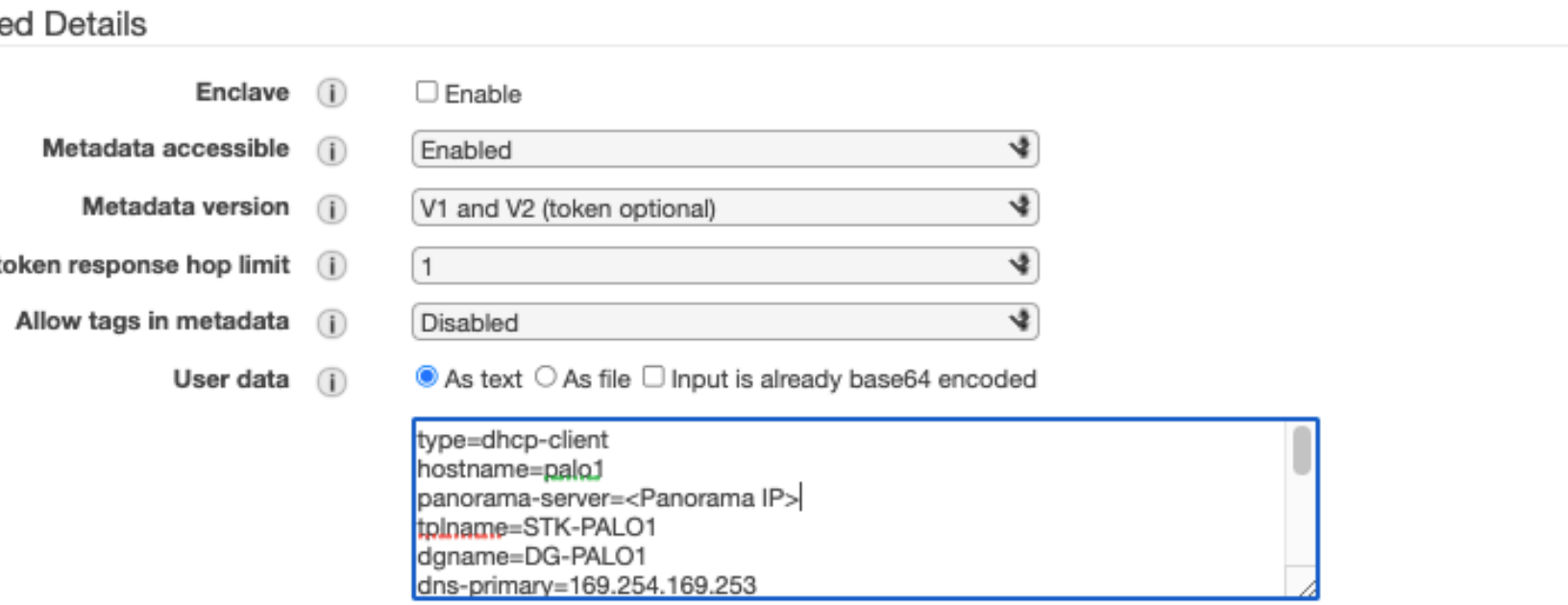
每个云对用户数据都有不同的条款，并在引导参数之间使用不同的分隔符。

©2024 Palo Alto Networks, Inc.

- **Alibaba Cloud** 用户数据 — 对每个参数使用换行符 (\n)，如果参数具有多个选项，请使用逗号分隔。
- **AWS** 用户数据 — 使用分号或换行符 (\n)。如果参数具有多个选项，请使用逗号分隔选项。例如：

```
  type=dhcp-client hostname=palo1 panorama-server=<PANORAMA-1 IP>
 panorama-server-2=<PANORAMA-2 IP> tplname=STK-NGFW-01 dgname=DG-
NGFW-01 dns-primary=169.254.169.253 dns-secondary=8.8.8.8 op-
command-modes=mgmt-interface-swap dhcp-send-hostname=yes dhcp-send-
client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes vm-auth-key= <YOUR AUTH KEY HERE> authcodes= <<YOUR AUTH
 CODE HERE>
```

如果您选择在 AWS 密钥管理器中保存基本配置，请在用户数据字段中输入密钥名称作为键值对。例如：



- **Azure** 自定义数据 — 使用分号。如果参数具有多个选项，请使用逗号分隔选项。例如：

```
type=dhcp-client; op-command-modes=jumbo-frame; plugin-op-
commands=numa-perf-optimize:enable,set-dp-cores:30 vm-series-auto-
registration-pin-id=abcdefgh1234****; vm-series-auto-registration-
pin-value=zyxwvut-0987****
```


©2024 Palo Alto Networks, Inc.

- **GCP** 自定义元数据 — 在文件（例如 YAML 文件或 Terraform 模板）中，对每个参数使用换行符 (\n)，如果参数具有多个选项，请使用逗号分隔选项。例如：

```
type=dhcp-client op-command-modes=mgmt-interface-swap,jumbo-frame
 plugin-op-commands=numa-perf-optimize:enable,set-dp-cores:30 vm-
series-auto-registration-pin-id=abcdefgh1234**** vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

- **Oracle** 云基础架构用户数据 — 对每个参数使用换行符 (\n)，如果参数具有多个选项，请使用逗号分隔。

在 AWS 密钥管理器中保存基本配置

您可以使用 AWS 密钥管理器将基本配置存储为密钥，然后使用用户数据通过存储在密钥中的参数引导 VM。要执行此任务，您需要具有使用密钥管理器的权限。

- 密钥创建者必须具有完整的密钥管理器管理员权限。密钥管理器管理员可以允许其他人使用密钥，如 AWS 密钥管理器的身份验证和访问控制中所述。

  例如，以下策略语句允许您获取密钥值：

```
{ "Version":"2012-10-17", { "Effect":"Allow",
 "Action": "secretsmanager:GetSecretValue", "Resource":
 "arn:aws:secretsmanager:us-east-1:688382******:secret:My_bts-
******" } }
```

  请参阅您可以在适用于 AWS 密钥管理器的 IAM 策略或密钥策略中使用的操作、资源和上下文密钥，以查看需要许可的操作，例如列出、获取和旋转密钥。

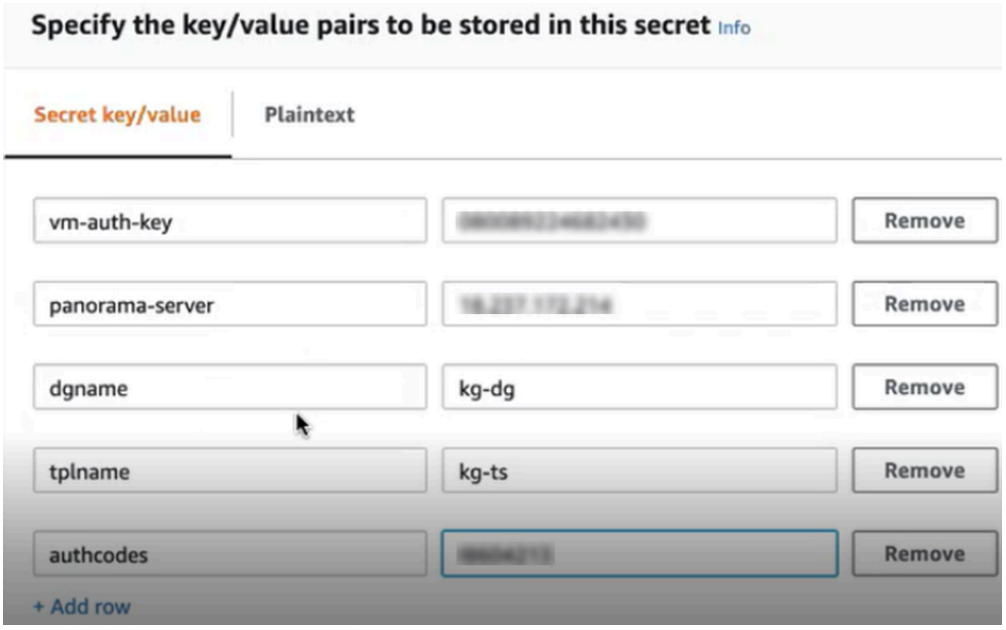
- （可选）要对密钥进行加密，您可以使用 AWS 密钥管理器的 DefaultEncryptionKey。

STEP 1 | 登录到 AWS 控制台，然后在 Security, Identity and Compliance（安全、身份和合规性）下，选择 **Secrets Manager**（密钥管理器），然后选择 **Store a new secret**（存储新密钥）。

©2024 Palo Alto Networks, Inc.

STEP 2 | 选择 **other type of secrets**（其他类型的密钥）。

1. 输入键值对以定义基本配置。



不能将 ***mgmt-interface-swap*** 用作 *AWS* 密钥中的键值对。输入格式必须为：***op-command-modes=mgmt-interface-swap***

2. 选择 DefaultEncryptionKey，然后单击 **Next**（下一步）。

STEP 3 | 提供密钥名称和说明。

1. 编辑资源权限以便安全地在 AWS 帐户之间访问密钥。例如：

```
{ "Version":"2012-10-17", "Statement":
 [ { "Sid":"VisualEditor0", "Effect":"Allow", "Action":
 "s3:ListBucket", "Resource": "arn:aws:s3:::sn-
bootstrap" }, { "Sid":"VisualEditor1", "Effect":"Allow",
 "Action": "s3:GetObject", "Resource": "arn:aws:s3:::sn-
bootstrap/*" }, { "Effect":"Allow", "Action":
 "secretsmanager:GetSecretValue", "Resource":
 "arn:aws:secretsmanager:us-east-1:688382******:
 secret:My_bootstrap" } ] }
```

2. （可选）您可以从命令行检查密钥（如果您具有权限）。例如：

```
# aws secretsmanager get-secret-value --secret-id My_bootstrap
 { "ARN": "arn:aws:secretsmanager:us-east-1:688382******:
 secret:My_bootstrap", "Name":"My_bootstrap",
 "VersionId":"01b6853d-e187-479f-**********", "SecretString":
 "{\"mgmt-interface-swap\":\"enable\", \"vm-auth-key\":\"AAA
\",\"panorama-server\":\"10.*.*.1\", \"panorama-server-2\":
\"10.*.*.2\",\"dgname\":\"dg-s0000h\", \"tplname\":\"tpl-
santosh\",\"license-authcode\":\"AAAA\"}", "VersionStages":
 [ "AWSCURRENT" ], "CreatedDate":1581018411.847 }
```


©2024 Palo Alto Networks, Inc.

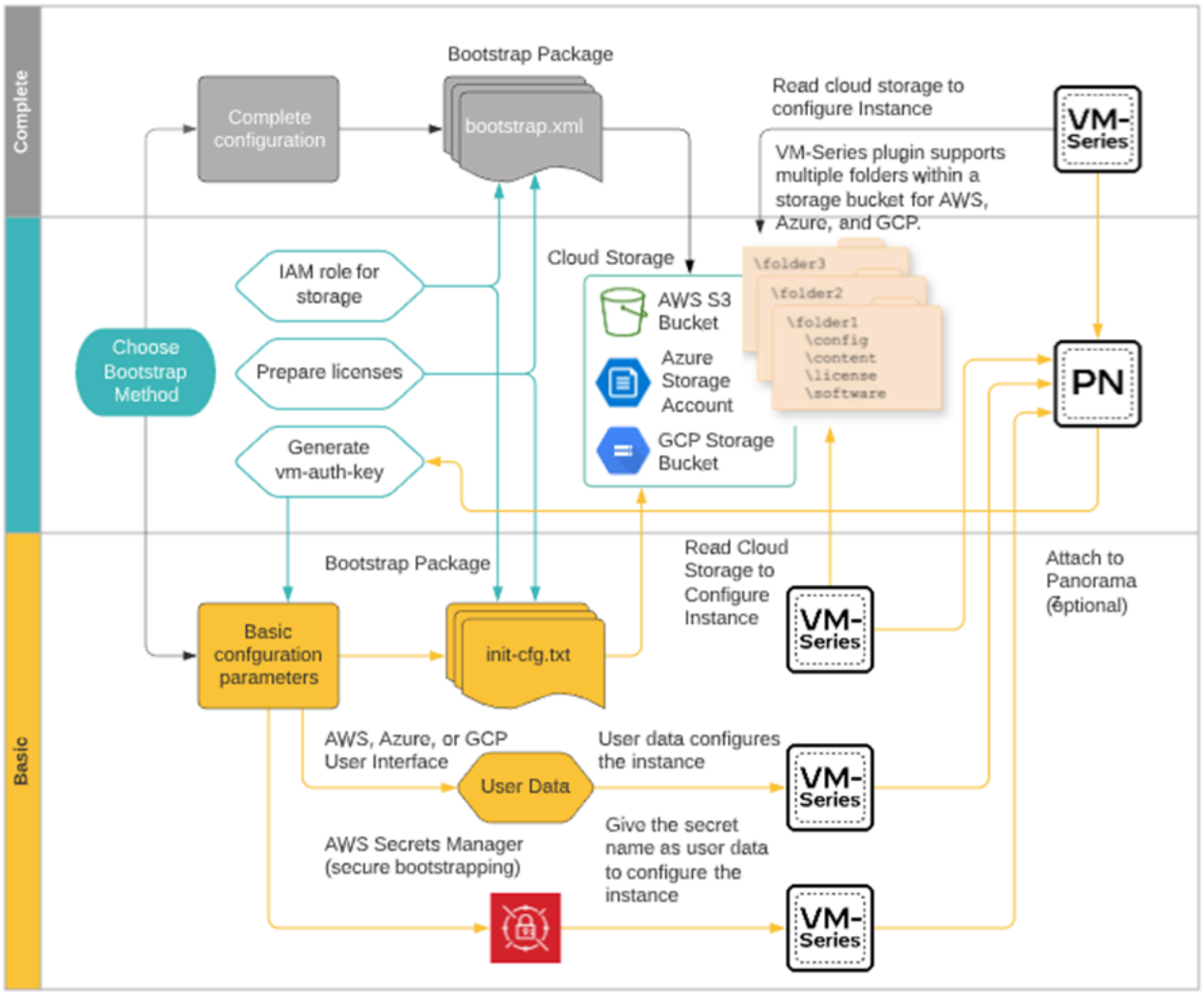
完整配置

完整配置可确保在启动时对防火墙进行完全配置。bootstrap.xml 文件包含 VM 系列插件的初始配置、许可证、软件、内容和版本。您可以手动创建 `bootstrap.xml`，也可以导出现有配置，如创建 bootstrap.xml 文件中所述。

©2024 Palo Alto Networks, Inc.

VM 系列防火墙引导工作流程

使用以下工作流程引导 VM 系列防火墙。有关完整和基本引导过程的概述，请参见下图。



STEP 1 | （可选）出于安全考虑，您只要在防火墙处于出厂默认配置的状态下方可对其进行引导。如果要使用引导数据包引导之前已配置的 VM 系列防火墙，可以将防火墙重置为出厂默认设置。

STEP 2 | 选择引导方法。

在熟悉引导数据包后，请评估是要使用完整配置，还是要使用基本配置，也可以选择使用 Panorama 管理引导的防火墙。

如果选择基本配置，请决定是使用引导数据包，还是输入配置参数作为用户数据中的键值对。

STEP 3 | （可选）如果您要使用 Panorama 管理引导的 VM 系列防火墙，则在 Panorama 上生成 VM 授权密钥。您必须在 `init-cfg.txt` 文件中包含此密钥 (**`vm-auth-key`**)，或输入键值对作为用户数据。

©2024 Palo Alto Networks, Inc.

STEP 4 | 准备引导许可证。

许可证检索机制只能使用 VM 系列管理界面。不支持服务路由，因为它们发生在检索许可证之后。

STEP 5 | 如果选择基本配置，并计划使用用户数据进行引导，请跳至步骤 7。

如果您计划使用基本配置和引导数据包，请创建 init-cfg.txt 文件，并准备引导数据包。

如果选择完整配置，请创建 bootstrap.xml 文件，并准备完整引导数据包。

STEP 6 | 准备引导数据包，然后将引导数据包保存为适用于虚拟机监控程序的相应交付格式。

STEP 7 | 引导 VM 系列防火墙。

- 在 AWS 上引导 VM 系列防火墙
- 在 Azure 上引导 VM 系列防火墙
- 在 ESXi 上引导 VM 系列防火墙
- 在 Google Cloud Platform 上引导 VM 系列防火墙
- 在 Hyper-V 上引导 VM 系列防火墙
- 在 KVM 上引导 VM 系列防火墙

STEP 8 | 验证引导完成。

©2024 Palo Alto Networks, Inc.

引导数据包

只有在防火墙处于出厂默认配置下且为首次启动时，引导流程才会启动。

- 引导数据包结构
- 引导数据包交付

引导数据包结构

引导数据包必须包含 `/config`、`/license`、`/software` 和 `/content` 文件夹，即使为空文件夹。`/plugins` 文件夹为可选。例如，请参阅准备引导数据包。

- **/config** 文件夹 — 包含有配置文件。该文件夹用于存放两个文件：`init-cfg.txt` 和 `bootstrap.xml`。有关详细信息，请参阅引导配置文件。

  如果您通过引导在 *Panorama* 中预先注册 *VM* 系列防火墙，则必须在 *Panorama* 上生成一个 *VM* 授权密钥，并将其包含在 *`init-cfg.txt`* 文件的密钥中。请参阅在 Panorama 上生成 VM 身份验证密钥。

- **/license** 文件夹 — 包含有您将要在防火墙上激活的许可证和订阅的许可证密钥或授权代码。如果防火墙未连接 Internet，则您必须手动从 Palo Alto Networks 支持门户获取许可证密钥，或使用许可证 API 获取密钥，然后将每个密钥保存在该文件夹中。有关详细信息，请参阅准备引导许可证。

  您必须在其中保存授权代码包，而不是保存单个授权代码，确保防火墙或协调服务能够同时获取与防火墙相关的所有许可证密钥。如果您使用单个授权代码，而非代码包，防火墙将只会检索文件中第一个授权代码对应的许可证密钥。

- **/software** 文件夹 — 包含有将新配备的 VM 系列防火墙升级至适于您的网络的 PAN-OS 版本所需的软件映像。其中必须包含当前版本与您希望将 VM 系列防火墙升级到的最终 PAN-OS 软件版本之间的所有中间版本。请参阅兼容性矩阵中的 VM 系列防火墙虚拟机监控程序支持。
- **/content** 文件夹 — 包含有应用程序和威胁升级、WildFire 更新以及确保 VM 系列防火墙上的有效订阅所需的 BrightCloud URL 筛选数据库。其中必须包含所需 PAN-OS 版本所需的最低内容版本。如果您没有与 PAN-OS 版本相关联的所需最低内容版本，则 VM 系列防火墙将无法完成软件升级。
- **/Plugins** 文件夹 — 可选文件夹包含单个 VM 系列插件映像。

引导数据包交付

在将引导数据包交付至 VM 系列防火墙所用的文件类型取决于虚拟机监控程序。使用下表可以确定虚拟机监控程序或云供应商支持的文件类型。

©2024 Palo Alto Networks, Inc.

引导用外部设备（引导数据包格式）	AWS	Azure	ESXi	Google	Hyper-V	KVM
CD-ROM（ISO 映像）	—	—	是	—	是	是
块存储设备	—	—	是	—	是	是
存储帐户	—	是	—	—	—	—
存储桶	是	—	—	是	—	—

在将存储设备连接到防火墙时，防火墙会扫描是否存在引导数据包；如果存在，防火墙将使用该引导数据包中定义的设置。

如果文件中包含有一个 Panorama 服务器 IP 地址，防火墙将会连接到 Panorama。如果防火墙已连接到 Internet，它将会连接到许可证服务器，以更新 UUID 并获得许可证密钥和订阅。然后，将添加防火墙作为 Palo Alto Networks 支持门户中的资产。如果防火墙未连接到 Internet，则您可以使用引导数据包中的许可证密钥，也可以连接至 Panorama 以检索适当的许可证并将其部署到托管防火墙。

©2024 Palo Alto Networks, Inc.

引导配置文件

引导数据包必须在 `config/init-cfg.txt` 文件中包含基本配置。完整配置（在 `/config/bootstrap.xml` 文件中）为可选。

将 `init-cfg.txt` 文件和 `bootstrap.xml` 文件同时包含在引导数据包中之后，防火墙将合并这两个文件的配置，并且如果有任何设置重叠，防火墙将使用 `init-cfg.txt` 文件中定义的值。

- init-cfg.txt
- bootstrap.xml

init-cfg.txt

该文件包含配置防火墙上的管理接口所需的基本信息，例如 IP 地址类型（静态或 DHCP）、IP 地址（仅 IPv4 或 IPv4 和 IPv6）、网络掩码和默认网关。DNS 服务器 IP 地址、Panorama IP 地址以及设备组和模板堆栈参数为可选项。

您可以使用通用名称 `init-cfg.txt`，或者您可以在文件名中加上每个防火墙的 UUID 或序列号前缀，使文件名更为具体化（例如：`0008C100105-init-cfg.txt`）。

防火墙启动时，它会搜索与其 UUID 或序列号匹配的文本文件；如果找不到该文件，将使用通用文件名 `init-cfg.txt` 进行搜索。有关示例文件，请参阅创建 init-cfg.txt 文件。

如果使用 *Panorama* 管理引导的 *VM* 系列防火墙：

- 您必须在 *Panorama* 上生成 *VM* 身份验证密钥，并将该密钥包含在 *`init-cfg.txt`* 文件中。有关更多信息，请参阅在 Panorama 上生成 VM 身份验证密钥。
- 管理防火墙的 *Panorama* 设备必须处于 *Panorama* 模式。如果在仅管理模式使用 *Panorama* 设备，因为仅管理模式的 *Panorama* 防火墙日志没有可以存储防火墙日志的日志收集器组，因此防火墙日志被丢弃。

bootstrap.xml

可选的 `bootstrap.xml` 文件包含防火墙的完整配置。如果您不使用 Panorama 集中管理防火墙，则 `bootstrap.xml` 文件提供一种自动部署在启动时配置的防火墙过程的方法。

您可以手动定义配置，也可以从现有防火墙中导出正在运行的配置 (`running-config.xml`)，然后将该文件另存为 `bootstrap.xml`。如果您导出 `bootstrap.xml` 文件，请确保从与部署相同的平台或虚拟机监控程序上部署的防火墙中导出 XML 文件。请参阅创建 bootstrap.xml 文件。

©2024 Palo Alto Networks, Inc.

为确保使用 *init-cfg.txt** 和 *bootstrap.xml* 文件成功引导高级路由，请在 * *init-cfg.txt** 和 *bootstrap.xml* 中启用高级路由。不在两个文件中启用高级路由可能会导致环境不稳定；例如，如果使用 ***show advanced routing route***，输出表明高级路由已启用，但命令 ***show deviceconfig setting*** 表明高级路由未启用。此外，高级路由不会完全正常工作，可能会以提交失败而结束。如果设置处于上述状态，要启用高级路由，请在配置 ***set deviceconfig setting advanced-routing yes*** 后重新启动 *VM* 系列防火墙

。

©2024 Palo Alto Networks, Inc.

在 Panorama 上生成 VM 身份验证密钥

如果您想要使用 Panorama 来管理正在引导的 VM 系列防火墙，您必须在 Panorama 上生成一个 VM 身份验证密钥，并将该密钥包含在基本配置文件 init-cfg.txt 中。通过 VM 身份验证密钥，Panorama 可以对新引导的 VM 系列防火墙进行身份验证。因此，要使用 Panorama 管理防火墙，基本配置文件中必须包含 Panorama 的 IP 地址及 VM 身份验证密钥，并且引导数据包的 /license 文件夹中必须包含许可证授权代码。之后，防火墙会在其初始连接请求中将 IP 地址、序列号和 VM 身份验证密钥提供给 Panorama，以便 Panorama 验证 VM 身份验证密钥的有效性，并将防火墙添加为托管设备。如果您在基本配置文件中提供了设备组和模板，Panorama 会将防火墙分配至相应的设备组和模板，以便使用 Panorama 集成配置和管理防火墙。

根据不同的情况，密钥的生命周期在 1 小时到 8760 小时（1 年）不等。指定的时间到期后，密钥将会过期；如果 VM 系列防火墙的连接请求中没有有效的身份验证密钥，Panorama 将不会对其进行注册。

STEP 1 | 登录到 Panorama CLI 或访问 API：

- 在 CLI 中，使用以下运行命令：

  ```
  request bootstrap vm-auth-key generate lifetime <1-8760>
  ```

  举例来说，若要生成一个有效期为 24 小时的密钥，则输入以下命令：

  ```
  request bootstrap vm-auth-key generate lifetime 24
  VM auth key 755036225328715 generated.Expires at:2015/12/29
   12:03:52
  ```

- 在该 API 中，使用以下 URL：

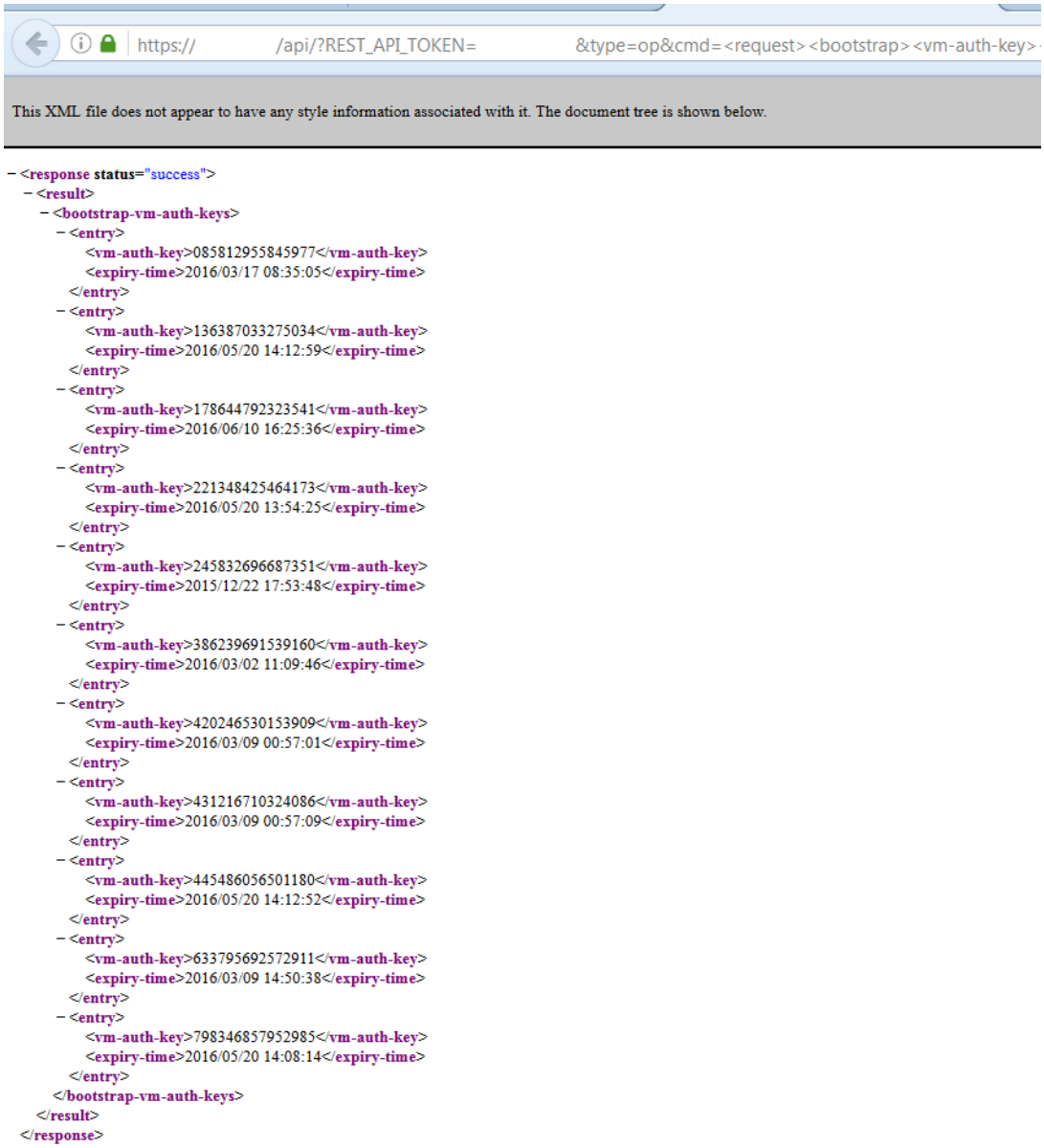
  ```
  https://<Panorama_IP_address>/api/?
  type=op&cmd=<request><bootstrap><vm-auth-
  key><generate><lifetime><number-of-hours></lifetime></generate></
  vm-auth-key></bootstrap></request>
  ```

  其中 lifetime 是指 VM 身份验证密钥保持有效的小时数。

©2024 Palo Alto Networks, Inc.

STEP 2 | 验证您在 Panorama 上生成的 VM 身份验证密钥的有效期。确保该有效期具有足够的时间，以便完成防火墙在 Panorama 上的注册。

```
https://<Panorama_IP_address>/api/?
type=op&cmd=<request><bootstrap><vm-auth-key><show></show></vm-
auth-key></bootstrap></request>
```



STEP 3 | 将生成的 VM 身份验证密钥添加到基本配置文件 init-cfg.txt 中。请参阅创建 init-cfg.txt 文件

 ©2024 Palo Alto Networks, Inc.

创建 init-cfg.txt 文件

需要 `init-cfg.txt` 文件才能引导 VM 系列防火墙。该文件提供防火墙连接到网络所需的基本信息。

- init-cfg.txt 文件组件
- init-cfg.txt 示例文件

完成以下过程以创建 `init-cfg.txt` 文件。

STEP 1 | 创建一个新的文本文件。

使用 Notepad、EditPad 或其他纯文本编辑器创建一个新的文本文件。

STEP 2 | 针对防火墙上的管理接口，添加基本网络配置。

如果文件中缺失任何所需的参数，防火墙将会退出引导流程，并使用默认的 *IP* 地址 *192.168.1.1* 启动。您可以查看防火墙上的系统日志，以检测引导出现故障的原因。有关错误，请参阅许可证 API。

每个字段中的键值之间没有空格。切勿在其中添加空格，否则将会导致在 *mgmtsrvr* 侧的解析过程中出现故障。

- 若要使用静态 IP 地址配置管理接口，您必须指定 IP 地址、地址类型、默认网关和网络掩码。IPv4 地址为必填字段，IPv6 地址是可选字段。有关语法，请参阅示例 init-cfg.txt 文件。
- 若要将管理接口配置为 DHCP 客户端，则只能指定地址类型。如果在管理接口上启用了 DHCP 客户端，防火墙将会忽略 IP 地址、默认网关、网络掩码、IPv6 地址以及文件中定义的 IPv6 默认网关值。有关语法，请参阅示例 init-cfg.txt 文件。

在管理接口上启用 DHCP 时，防火墙将会采用 DHCP 分配的 IP 地址，而且可通过网络进行访问。您可以通过仪表盘上的常规信息小部件查看 DHCP 分配的 IP 地址，或者通过 CLI 命令 **`show system info`**。不过，默认静态管理 IP 地址 192.168.1.1 会保留在防火墙上的运行配置 (**`show config running`**) 中。该静态 IP 地址可确保在防火墙的 DHCP 访问丢失时，您能够随时恢复防火墙的连接。

STEP 3 | 添加 VM 身份验证密钥，以在 Panorama 上注册 VM 系列防火墙。

要在 Panorama 上添加 VM 系列防火墙，必须将在 Panorama 上生成的 VM 身份验证密钥添加到基本配置文件 (`init-cfg.txt`) 中。有关生成密钥的详细信息，请参阅在 Panorama 上生成 VM 身份验证密钥。

STEP 4 | 添加访问 Panorama 的详细信息。

- 添加 Panorama 主服务器和辅助服务器的 IP 地址。
- 指定您希望为其分配防火墙的模板和设备组。

©2024 Palo Alto Networks, Inc.

STEP 5 | （推荐）添加 VM 系列注册 PIN 和值用于安装设备证书。

如果您要在启动时在 VM 系列防火墙上安装设备证书，则必须在 CSP 上生成 VM 系列注册 PIN ID 和值，并将其包含在 `init-cfg.txt` 文件中。该 PIN 和值也适用于使用 PAYG 许可证的所有网站许可证。

STEP 6 | （可选）包括防火墙的其他参数。

- 添加 DNS 主服务器和辅助服务器的 IP 地址。
- 添加防火墙的主机名称。
- 启用 Jumbo 帧或多个虚拟系统（或两者）
- 为 AWS 或 GCP 上的 VM 系列防火墙启用管理接口交换 (mgmt) 和数据平面接口交换 (ethernet 1/1)。有关更改管理接口的更多信息，请参阅Management Interface Mapping for Use with Amazon ELB（管理接口映射以用于 Amazon ELB）或用于 Google Cloud Launcher 负载均衡的管理接口交换。
- 启用或禁用 DPDK。

init-cfg.txt 文件组件

下表介绍了 `init-cfg.txt` 文件中的引导参数。

字段	说明
type=	管理 IP 地址的类型：静态或 dhcp 客户端。此为必填字段。
ip-address=	IPv4 地址。如果 IP 地址的类型为“dhcp 客户端”，则忽略该字段。如果是静态类型，则需要 IPv4 地址；ipv6-address 字段是可选的，可包含在内。 对于 AWS 和 Azure 上的 VM 系列防火墙，您无法指定管理 IP 地址和网络掩码配置。一旦定义了此类配置，防火墙将会忽略您指定的值。
default-gateway=	管理接口的 IPv4 默认网关。如果 IP 地址的类型为“dhcp 客户端”，则忽略该字段。如果类型为“静态”且使用了 ip-address 字段，则必须填写该字段。
netmask=	IPv4 网络掩码。如果 IP 地址的类型为“dhcp 客户端”，则忽略该字段。如果类型为“静态”且使用了 ip-address 字段，则必须填写该字段。
ipv6-address=	（可选）管理接口的 IPv6 地址和 / 前缀长度。如果 IP 地址的类型为“dhcp 客户端”，则忽略该字段。如果是静态类型，则可以与 ip-address 字段一起制定此字段，ip-address 是必填字段。

©2024 Palo Alto Networks, Inc.

字段	说明
ipv6-default-gateway=	管理接口的 IPv6 默认网关。如果 IP 地址的类型为“dhcp 客户端”，则忽略该字段。如果类型为“静态”且使用了 ipv6-address 字段，则必须填写该字段。
hostname=	防火墙的主机名称。
panorama-server=	Panorama 主服务器的 IPv4 或 IPv6 地址。该字段不是必填字段，但建议填写，以便集中管理防火墙。
panorama-server-2=	Panorama 辅助服务器的 IPv4 或 IPv6 地址。该字段非必填字段，但建议予以填写。
tplname=	Panorama 模板堆栈名称。如果您添加 Panorama 服务器 IP 地址，作为最佳实践，请在 Panorama 上将防火墙分配到模板堆栈，并在此字段中输入模板堆栈名称，以便集中管理配置设置并将其推送到防火墙。
dgname=	Panorama 设备组名称。如果添加 Panorama 服务器 IP 地址，作为最佳实践，请在 Panorama 上创建设备组，并在该字段中输入设备组名称，以便按逻辑将防火墙分组并将策略规则推送到防火墙。
cgname=	Panorama 收集器组名称。如果您要引导防火墙将日志发送到 Panorama 收集器组，则必须先在 Panorama 上配置收集器组，然后配置防火墙将日志转发到 Panorama。 在 M 系列设备上，已预定义默认收集器组，并且已经包含本地日志收集器作为成员。在 Panorama 虚拟设备上，您必须添加收集器组并添加本地日志收集器作为成员。
dns-primary=	DNS 主服务器的 IPv4 或 IPv6 地址。
dns-secondary=	DNS 辅助服务器的 IPv4 或 IPv6 地址。
vm-auth-key=	Panorama 的虚拟机身份验证密钥（参阅在 Panorama 上生成 VM 身份验证密钥）。在引导硬件防火墙时，会忽略该字段。
op-command-modes=	允许的值包括：multi-vsys、jumbo-frame、mgmt-interface-swap。如果输入了多个值，需使用空格或逗号相互隔开。 • **multi-vsys** — （仅适于基于硬件的防火墙）启用多个虚拟系统。 • **jumbo-frame** — 启用第 3 层所有接口的默认 MTU 大小，设置为 9192 字节。

©2024 Palo Alto Networks, Inc.

字段	说明
	• **mgmt-interface-swap** —（仅适于 AWS、Google、ESXi 和 KVM 中的 VM 系列防火墙）用于在部署防火墙时使用数据面板接口 (ethernet 1/1) 交换管理接口 (MGT)。有关详细信息，请参阅 • 管理接口映射以用于 Amazon ELB • 用于 Google Cloud Launcher 负载均衡的管理接口交换 • 使用 VM 系列 CLI 在 ESXi 上交换管理接口 • 使用 VM 系列 CLI 在 KVM 上交换管理接口
op-cmd-dpdk-pkt-io=	**on** 或 **off** 值可让您在防火墙支持 DPDK 的环境中启用或禁用数据平面开发工具包 (DPDK)。DPDK 允许主机绕过 Linux 内核来更快地处理数据包；与 NIC 的交互使用驱动程序和 DPDK 库执行。
plugin-op-commands=	指定 VM 系列插件操作命令。 必须在一个逗号分隔的列表中输入多个命令，逗号之间不能有空格。 • **sriov-access-mode-on** — 此命令仅适用于 ESXi 和 KVM 虚拟机监控程序中的 VM 系列防火墙。 仅限 KVM，如果您启用 **sriov-access-mode-on**，请不要启用 **op-command-modes=jumbo-frame**。 • **aws-gwlb-inspect:enable**—Enables VM 系列与 AWS 网关负载均衡器集成. • **aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>** — 支持访问防火墙上的将 VPC 端点与 VM 系列接口关联或子接口。已将指定接口分配给安全区域。 • **aws-gwlb-overlay-routing:enable** — 与 AWS GWLB 集成时使用此命令在 AWS 上为 VM 系列启用覆盖路由。 • **set-dp-cores:<#-cores>** — 为运行使用软件 NGFW 许可证部署的 PAN-OS 11.0 或更高版本的 VM 系列防火墙自定义数据平面 vCPU 的数量。NSX-T 不支持此选项。有关详细信息，请参阅自定义数据平面核心。 • **numa-perf-optimize:enable** — 在已安装 VM 系列插件 2.1.2 或更高版本的 VM 系列防火墙上启用 NUMA 性能优化。有关详细信息，请参阅在 VM 系列上启用 NUMA 性能优化。 • **advance-routing:enable** — 启用高级路由。为确保使用 init-cfg.txt* 和 bootstrap.xml 文件成功引导高级路由，请在 * init-cfg.txt*

©2024 Palo Alto Networks, Inc.

字段	说明
	和 bootstrap.xml 中启用高级路由。不在两个文件中启用高级路由可能会导致环境不稳定；例如，如果使用 **show advanced routing route**，输出表明高级路由已启用，但命令 **show deviceconfig setting** 表明高级路由未启用。此外，高级路由不会完全正常工作，可能会以提交失败而结束。如果设置处于上述状态，要启用高级路由，请在配置 **set deviceconfig setting advanced-routing yes** 后重新启动 VM 系列防火墙。
dhcp-send-hostname=	来自 DHCP 服务器的值，包括 yes 和 no。若为 yes，防火墙会发送其主机名称到 DHCP 服务器。只有在 IP 地址的类型为“dhcp 客户端”时，才需要填写该字段。
dhcp-send-client-id=	来自 DHCP 服务器的值，包括 yes 和 no。若为 yes，防火墙会发送其客户端 ID 到 DHCP 服务器。只有在 IP 地址的类型为“dhcp 客户端”时，才需要填写该字段。
dhcp-accept-server-hostname=	来自 DHCP 服务器的值，包括 yes 和 no。若为 yes，防火墙会接收来自 DHCP 服务器的主机名称。只有在 IP 地址的类型为“dhcp 客户端”时，才需要填写该字段。
dhcp-accept-server-domain=	来自 DHCP 服务器的值，包括 yes 和 no。若为 yes，防火墙会接收来自 DHCP 服务器的 DNS 服务器。只有在 IP 地址的类型为“dhcp 客户端”时，才需要填写该字段。
vm-series-auto-registration-pin-id 和 vm-series-auto-registration-pin-value	VM 系列注册 PIN ID 和值用于在 VM 系列防火墙上安装设备证书。此外，PIN ID 和值还能让您在防火墙的 PAYG 实例上自动激活 AutoFocus 和 Cortex Data Lake 的网站许可证。 您必须在 Palo Alto Networks CSP 上生成此注册 PIN ID 和值。有关生成 PIN ID 和值的信息，请参阅在 VM 系列防火墙上安装设备证书。

init-cfg.txt 示例文件

以下基本配置文件示例显示了文件中支持的所有参数；粗体所示为必需参数。

示例 **init-cfg.txt** 文件（静态 **IP** 地址）	**init-cfg.txt** 文件示例（**DHCP** 客户端）
type=static	**type=dhcp-client**
ip-address=10.*.*.19	ip-address=
default-gateway=10.*.*.1	default-gateway=
netmask=255.255.255.0	netmask=

©2024 Palo Alto Networks, Inc.

示例 **init-cfg.txt** 文件（静态 **IP** 地址）	**init-cfg.txt** 文件示例（**DHCP** 客户端）
ipv6-address=2001:400:f00::1/64	ipv6-address=
ipv6-default-gateway=2001:400:f00::2*	ipv6-default-gateway=
hostname=Ca-FW-DC1	hostname=Ca-FW-DC1
vm-auth-key=7550362253****	vm-auth-key=7550362253****
panorama-server=10.*.*.20	panorama-server=10.*.*.20
panorama-server-2=10.*.*.21	panorama-server-2=10.*.*.21
tplname=FINANCE_TG4	tplname=FINANCE_TG4
dgname=finance_dg	dgname=finance_dg
dns-primary=10.5.6.6	dns-primary=10.5.6.6
dns-secondary=10.5.6.7	dns-secondary=10.5.6.7
op-command-modes=jumbo-frame,mgmt-interface-swap**	op-command-modes=jumbo-frame,mgmt-interface-swap**
op-cmd-dpdk-pkt-io=***	op-cmd-dpdk-pkt-io=***
plugin-op-commands=	plugin-op-commands=
dhcp-send-hostname=no	dhcp-send-hostname=yes
dhcp-send-client-id=no	dhcp-send-client-id=yes
dhcp-accept-server-hostname=no	dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=no	dhcp-accept-server-domain=yes
vm-series-auto-registration-pin-id=abcdefgh1234**	**vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987**	**vm-series-auto-registration-pin-value=zyxwvut-0987****

©2024 Palo Alto Networks, Inc.

对于 *AWS* 上的 *VM* 系列防火墙，您无法指定管理 *IP* 地址和网络掩码配置。一旦定义此类配置，防火墙将会忽略您指定的值；这是因为 *AWS* 使用后端元数据文件来分配管理 *IP* 地址和网络掩码。

*如果包含 *IPv6* 地址，则需要 *IPv6* 默认网关。

***`mgmt-interface-swap`* 运行命令仅适用于 *AWS* 或 *GCP* 上的 *VM* 系列防火墙。

****`op-cmd-dpdk-pkt-io=off`* 用于在 *ESXi*、*KVM* 和 *GCP* 上的 *VM* 系列防火墙上禁用 *DPDK*（默认情况下已启用 *DPDK*）。

*****对于两个用例，*`vm-series-auto-registration-pin-id`* 和 *`vm-series-auto-registration-pin-value`* 为必需：

- 使用 *VM* 系列防火墙的即用即付 *(PAYG)* 许可证选项激活网站许可证 — *AutoFocus* 或 *Cortex Data Lake*。
- 在 *VM* 系列防火墙上检索并安装设备证书。

©2024 Palo Alto Networks, Inc.

创建 bootstrap.xml 文件

使用以下说明从与目标部署相同的平台或虚拟机监控程序上运行的防火墙导出配置。

STEP 1 | 从防火墙中导出配置文件。

1. 选择**Device**（设备） > **Setup**（设置） > **Operations**（操作）。
2. 选择要导出的配置文件。
   - 要导出运行的配置，在 Configuration Management（配置管理）部分中，选择 **Export named configuration snapshot**（导出已命名的配置快照）并从下拉列表中选择 **running config.xml**（运行 **config.xml**）。
   - 要导出之前版本的防火墙配置，在 Configuration Management（配置管理）部分中，选择 **Export configuration version**（导出配置版本）并在下拉列表中选择适当的配置版本。

STEP 2 | 重命名配置文件并保存。

1. 将文件重命名为 `bootstrap.xml`。

   若要确保引导流程成功，必须确保文件名的精确匹配（区分大小写）。
2. 将 `bootstrap.xml` 文件保存在与 `init-cfg.txt` 文件相同的位置。

©2024 Palo Alto Networks, Inc.

准备引导许可证

若要在引导流程中许可防火墙，您必须购买授权代码，并在开始引导前在 Palo Alto Networks 支持门户上注册许可证和订阅。

对于运行 BYOL 的 VM 系列防火墙（不适于基于使用情况的许可证 — PAYG），您必须拥有一个授权代码包，其中包括容量授权代码、支持订阅和所需的其他任何订阅。准备引导所需许可证的过程取决于防火墙在引导时是否可以访问 Internet：

- 直接 Internet 访问 — 防火墙直接连接至 Internet。
- 间接 Internet 访问 — 防火墙由 Panorama 管理，Panorama 可直接访问 Internet，而且能够代表防火墙获取许可证密钥。
- 无 Internet 访问 — 防火墙使用协调服务或由自定义脚本代表防火墙获取许可证密钥。

  对于带有 Internet 访问的 VM 系列防火墙。

  当您准备引导数据包时，输入 `/license` 文件夹中的授权代码。

  对于带有间接 Internet 访问的 VM 系列防火墙。

  1. 在 Palo Alto Networks 支持门户上注册授权代码。
     1. 转至支持门户并登录，然后选择 **Assets**（资产） > **Register New Device**（注册新设备） > **Register device using Serial Number or Authorization Code**（使用序列号或授权代码注册设备）。
     2. 按注册 VM 系列防火墙的步骤操作。
     3. 单击 **Submit**（提交）。
  2. 在 Palo Alto Networks 支持门户上激活授权代码，以生成许可证密钥。
     1. 转至支持门户并登录，然后选择 **Assets**（资产）选项卡。
     2. 对于每个序列号，单击 **Action**（操作）链接。
     3. 选择 **Activate Auth-Code**（激活授权代码）按钮。
     4. 输入 **Authorization code**（授权代码）并单击 **Agree**（同意）和 **Submit**（提交）。
     5. 下载许可证密钥并将其保存到本地文件夹。
     6. 继续准备引导数据包；您必须将下载至 `\license` 文件夹的许可密钥添加到引导数据包中。

  对于自定义脚本或可代表防火墙访问 Internet 的协调服务。

  脚本或服务必须从防火墙部署所在的虚拟机监控程序获取 CPU ID 和 UUID，并通过 CPU ID、UUID、API 密钥和授权代码访问 Palo Alto Networks 支持门户，以获取所需的密钥。请参阅基于型号的许可 API。

©2024 Palo Alto Networks, Inc.

准备引导数据包

在 AWS、Azure 或 GCP 上，您可以在公共云存储中创建引导数据包。

- VM 系列插件版本 1.0.13 及更早版本，以及版本 2.0.0 和 2.0.1 都支持每个存储桶的引导数据包。
- VM 系列插件版本 2.0.2 及更高版本也支持公共云存储桶中的子文件夹。您可以在存储桶中创建多个文件夹和子文件夹，每个文件夹和子文件夹都可以包含一个引导数据包。通常，文件夹代表一组 VM 的配置，例如 Panorama 设备组。

  要访问引导数据包，请指定引导文件夹的完整路径。例如：`my-storage/my-firewalls/bootstrap-2020-10-15`

使用下列过程准备引导数据包。

STEP 1 | 创建引导数据包的顶级目录结构。

在本地客户端或笔记本电脑上，或在公共云存储桶中创建以下文件夹：

```
/config
/content
/software
/license
/plugins
```

您可以将文件夹留空，但必须创建 **`/config`**, **`/license`**、**`/software`** 和 **`/content`** 文件夹。**`/plugins`** 文件夹为可选，只有在升级独立于 PAN-OS 版本的 VM 系列插件时才需要。

请勿在引导结构中放置任何其他文件或文件夹。添加其他文件或文件夹将导致引导失败。

```
/my-storage                          /my-firewalls
       /internal     /external             /config        /config
         /content       /content           /license       /license
         /plugins       /plugins           /software      /software
```

STEP 2 | 在每个文件夹中添加内容。

有关该过程的概述，请参阅引导数据包。有关 **`/config`** 文件夹中的文件的详细信息，请参阅引导配置文件。

```
/config
  0008C100105-init-cfg.txt
  0008C100107-init-cfg.txt
  bootstrap.xml
/content
  panupv2-all-contents-488-2590
  panup-all-antivirus-1494-1969
  panup-all-wildfire-54746-61460
/software
```

 ©2024 Palo Alto Networks, Inc.

```
  PanOS_vm-10.0.0
/license
  authcodes
  0001A100110-url3.key
  0001A100110-threats.key
  0001A100110-url3-wildfire.key
/plugins
  vm_series-2.0.2
```

- 如果将密钥保存到 *license* 文件夹，则可以使用对您适用，但文件名中保留 *..key* 扩展名的文件命名约定。对于授权代码，请创建一个名为 *authcodes* 的文本文件（没有文件扩展名），将授权代码添加到该文件，并将其保存到 *license* 文件夹中。
- 请使用授权代码包，而不是单个授权代码，确保防火墙或协调服务能够同时获取与防火墙相关的所有许可证密钥。如果您使用单个授权代码，而非代码包，防火墙将只会检索文件中第一个授权代码对应的许可证密钥。
- 在 */plugins* 文件夹中，只支持一个 *VM* 系列插件二进制文件。不要提供多个插件版本。

STEP 3 | 创建引导数据包。

对于 VM 系列防火墙，为您的虚拟机监控程序创建格式适当的映像。请参阅引导数据包交付。

©2024 Palo Alto Networks, Inc.

在 AWS 上引导 VM 系列防火墙

STEP 1 | 选择引导方法。

- 要将基本配置添加到引导数据包，请继续执行步骤 2。
- 要输入基本配置作为用户数据或使用用户数据从 AWS 密钥获取基本配置，请继续执行步骤 3。

STEP 2 | 准备 S3 存储桶和 IAM 角色，以启用读取访问。

要使用文件进行引导，您必须熟悉完成该流程所需的 AWS S3 和 IAM 权限。有关创建策略的详细说明，请参阅关于创建客户管理策略的 AWS 文档。

VM 系列防火墙的管理界面必须能够访问S3存储桶以完成引导。您可以为管理接口分配公共 IP 地址或弹性 IP 地址，以便可以通过 Internet 访问 S3 存储桶。或者，如果您希望在VPC和S3存储桶之间创建专用连接，并且不希望在防火墙管理界面上启用Internet访问，请在与S3存储区相同的区域创建AWS VPC端点。有关更多信息，请参阅设置 VPC 端点的 AWS 文档。

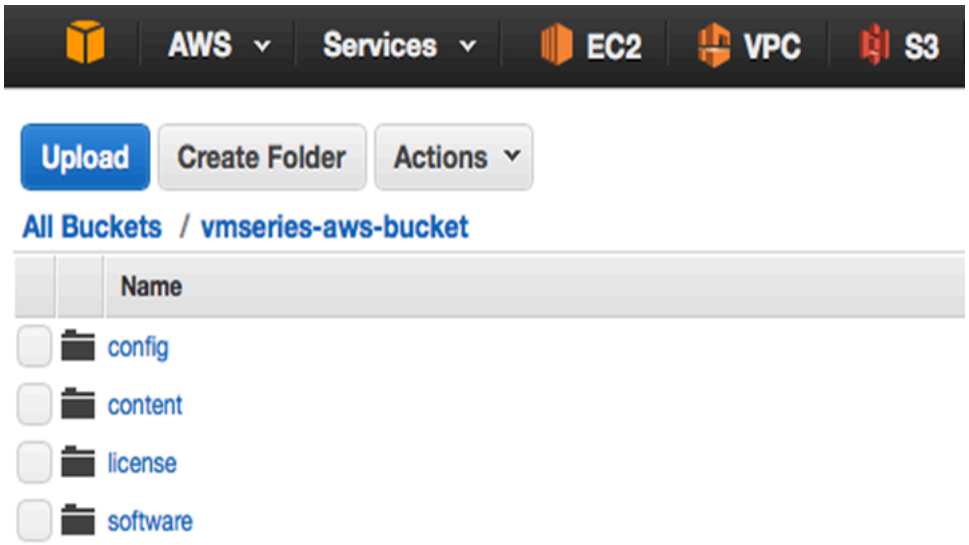
1. 使用内联策略创建 IAM 角色，以启用 S3 桶的读取访问 [ListBucket, GetObject]。有关创建 IAM 角色、定义哪些帐户/AWS 服务可承担此角色、定义承担此角色时应用程序可使用哪些 API 操作和资源的详细说明，请参阅关于《Amazon EC2 的 IAM 角色》的 AWS 文档。在启动 VM 系列防火墙时，您必须连接该角色，以启用对 S3 桶及其中所含的对象，确保可成功完成引导。
2. 在 AWS 控制台上，创建一个 Amazon 简单存储服务 (S3) 存储桶，或者在现有 S3 存储桶中创建一个子目录。

   本例中的 S3 存储桶 vmseries-aws-bucket 位于所有存储桶根文件夹级别。

```
{    "Version":"2012-10-17",    "Statement":
 [    {       "Effect":"Allow",       "Action":
 ["s3:ListBucket"],       "Resource":
 ["arn:aws:s3:::<bucketname>"]    },
    {       "Effect":"Allow",       "Action":
 ["s3:GetObject"],       "Resource":
 ["arn:aws:s3:::<bucketname>/*"]       }    ] }
```


©2024 Palo Alto Networks, Inc.

3. 在 S3 存储桶中创建文件夹，如准备引导数据包中所述。
   - 直接在 S3 存储桶中创建结构。



   - （可选）在每个文件夹中添加内容。您可以将文件夹留空，但必须创建所有 \config、\content、\license 和 \software 文件夹。\plugins 文件夹为可选。

> 如果在 *Amazon S3* 中启用了记录功能，将会自动在 *S3* 桶中创建名为 *Logs* 的文件夹。*Logs* 文件夹可帮助您解决 *S3* 桶访问相关的问题。

©2024 Palo Alto Networks, Inc.

STEP 3 | 在 AWS 上启动 VM 系列防火墙。选择以下选项之一。

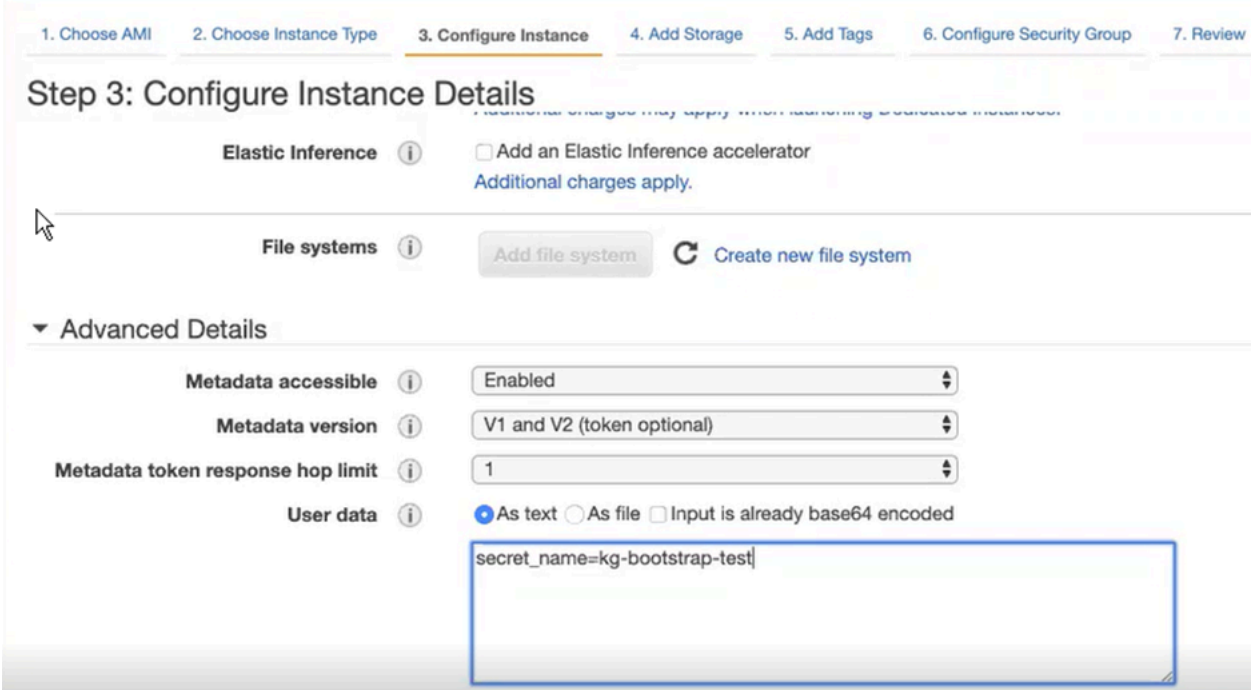
- **`init-cfg.txt`** — 如果您使用文件配置防火墙，请附加您在步骤 2.1 中创建的 IAM 角色，展开 **Advanced Details**（高级详细信息）部分，然后在 **User Data**（用户数据）字段中指定 S3 存储桶、目录或子目录的路径。例如，

  ```
  vmseries-bootstrap-aws-s3bucket=<bucketname>
  ```

  或者

  ```
  vmseries-bootstrap-aws-s3bucket=<bucketname/directoryname>
  ```

- 用户数据 — 如果您使用用户数据配置防火墙，请展开 **Advanced Details**（高级详细信息）部分，然后在 **User Data**（用户数据）字段中输入初始引导参数，如输入基本配置作为用户数据（公共云）中所述。
- **AWS** 机密管理器 — 如果您按在 AWS 密钥管理器中保存基本配置中所述存储基本配置，请展开 **Advanced Details**（高级详细信息）部分，然后在 **User Data**（用户数据）字段中选择 **As text**（作为文本），并输入机密名称作为键值对。例如：

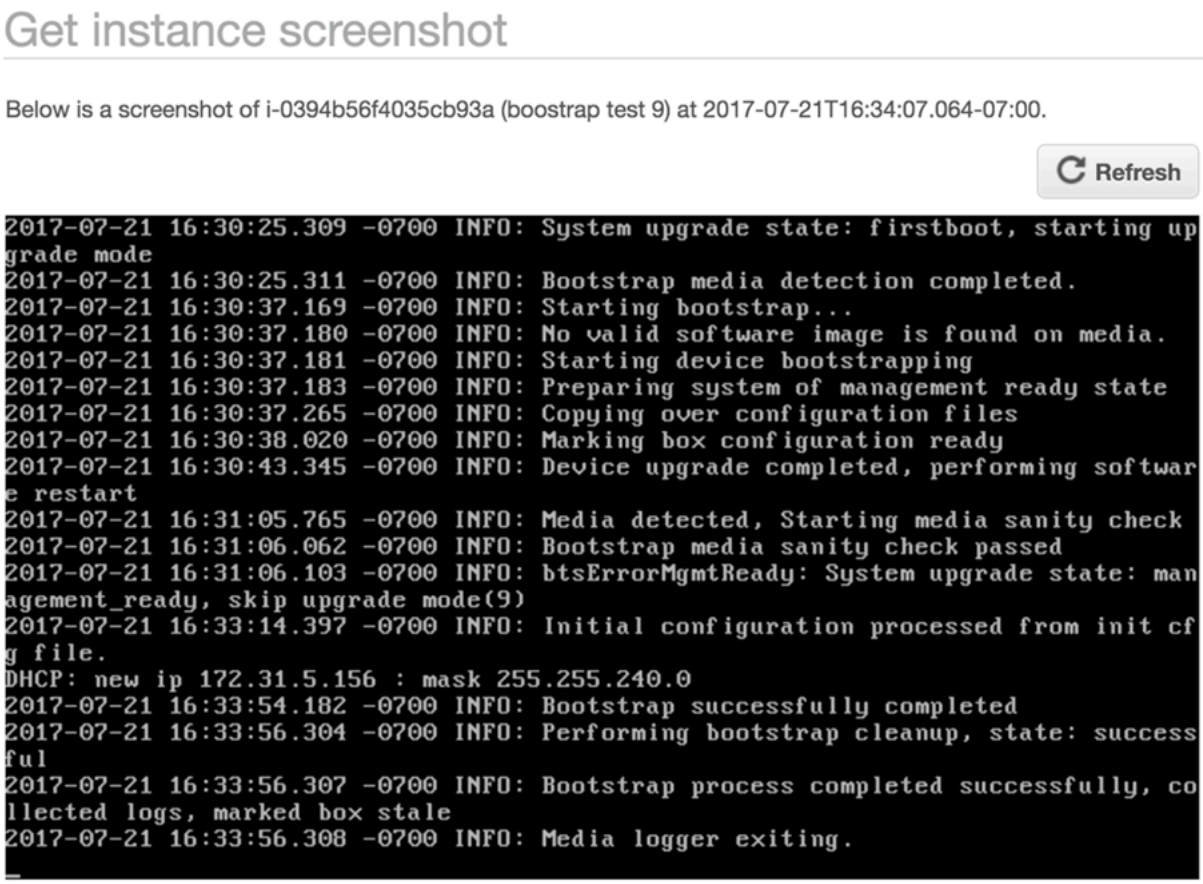


选择 **Review and Launch**（查看并启动）。有关详细信息，请参阅在 AWS 上启动 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 4 | 验证引导完成。在AWS管理控制台上选择防火墙实例并选择 **Actions**（操作） > **Instance Settings**（实例设置） > **Get Instance Screenshot**（获取实例屏幕截图）。

- 屏幕截图显示了正在进行的引导。成功的引导如下所示：



- 如果您使用 S3 存储桶，但 S3 存储桶没有正确的权限或 S3 存储桶中没有全部四个文件夹，则会显示以下错误消息：



 ©2024 Palo Alto Networks, Inc.

在 Azure 上引导 VM 系列防火墙

Azure 上的 VM 系列防火墙支持用于引导的 *Azure* 文件服务。

STEP 1 | 选择引导方法。

- 要将基本配置添加到引导数据包，请继续执行步骤 2。

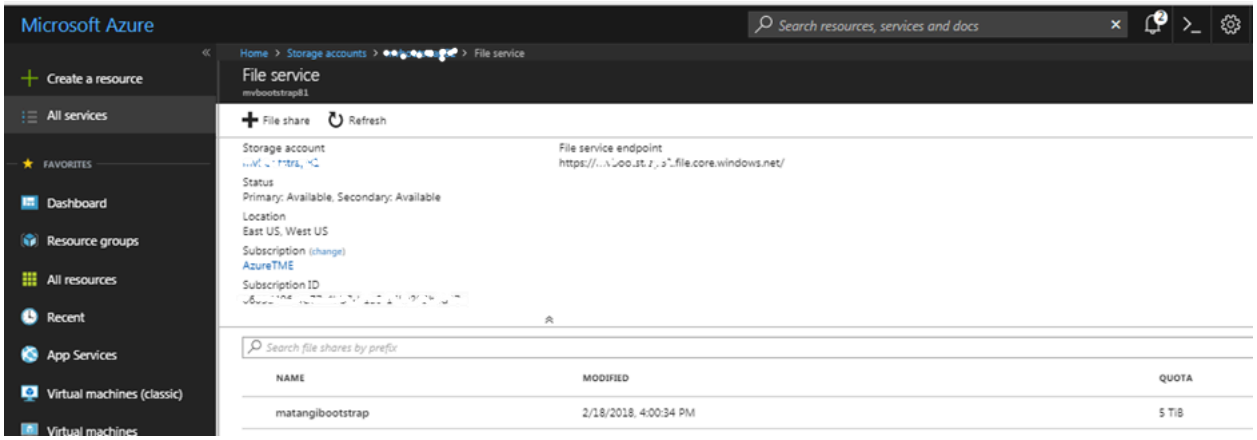
  要管理 Azure 上 VM 系列防火墙的引导数据包，必须熟悉 Azure 上的存储帐户，并知道如何创建包含引导数据包所需的文件夹结构的文件共享和目录对象。因为托管文件的存储帐户可以同时访问这些 Azure 文件，因此，您可以在多个虚拟机上共享 Azure 文件，以将防火墙作为存储帐户部署在相同的区域。

  VM 系列防火墙的管理界面必须能够访问包含引导数据包的文件共享，以完成引导。
- 要输入基本配置作为用户数据（公共云），请继续执行步骤 3.2。

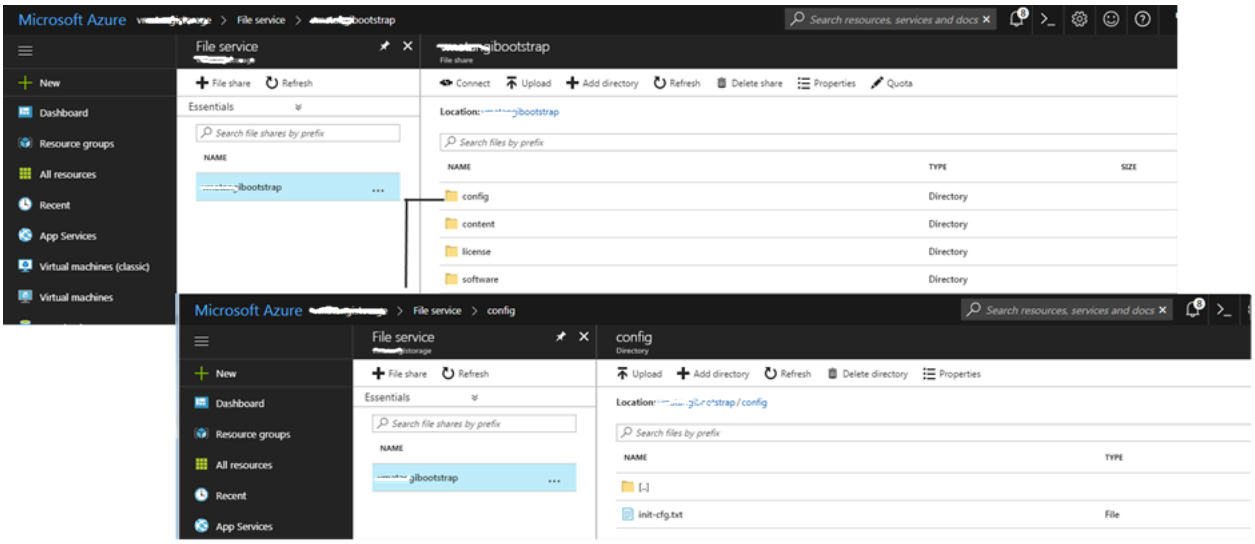
©2024 Palo Alto Networks, Inc.

STEP 2 | 在 Azure 文件服务内设置引导数据包。

1. 在 Azure 门户上选择或创建存储帐户。
2. 在 Azure 文件服务内创建文件共享。



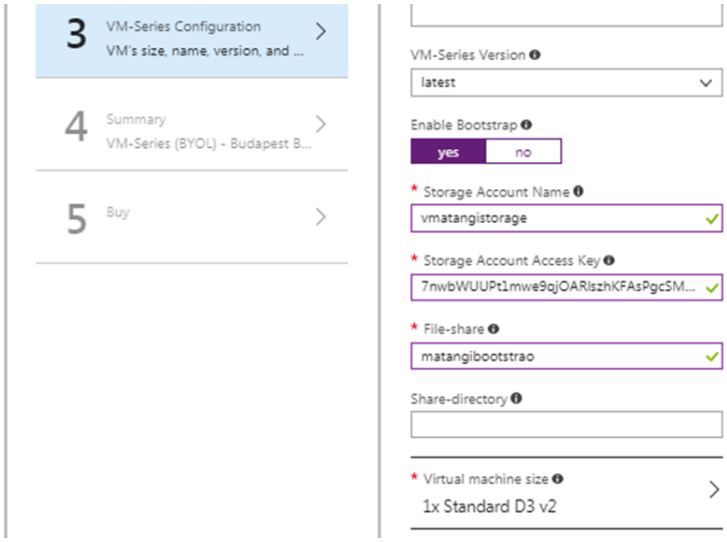
3. 在存储帐户中创建文件夹。
   - 直接在根文件夹中为引导数据包创建顶层目录结构，并为每个引导配置创建一个子文件夹。
   - 在每个文件夹中添加内容文件夹。您可以将文件夹留空，但必须在父文件夹中创建所有四个文件夹（config、license、software 和 content 文件夹）。在下面的屏幕截图中，您会看到，`config` 文件夹用于已上传的 `init-cfg.txt`文件。



©2024 Palo Alto Networks, Inc.

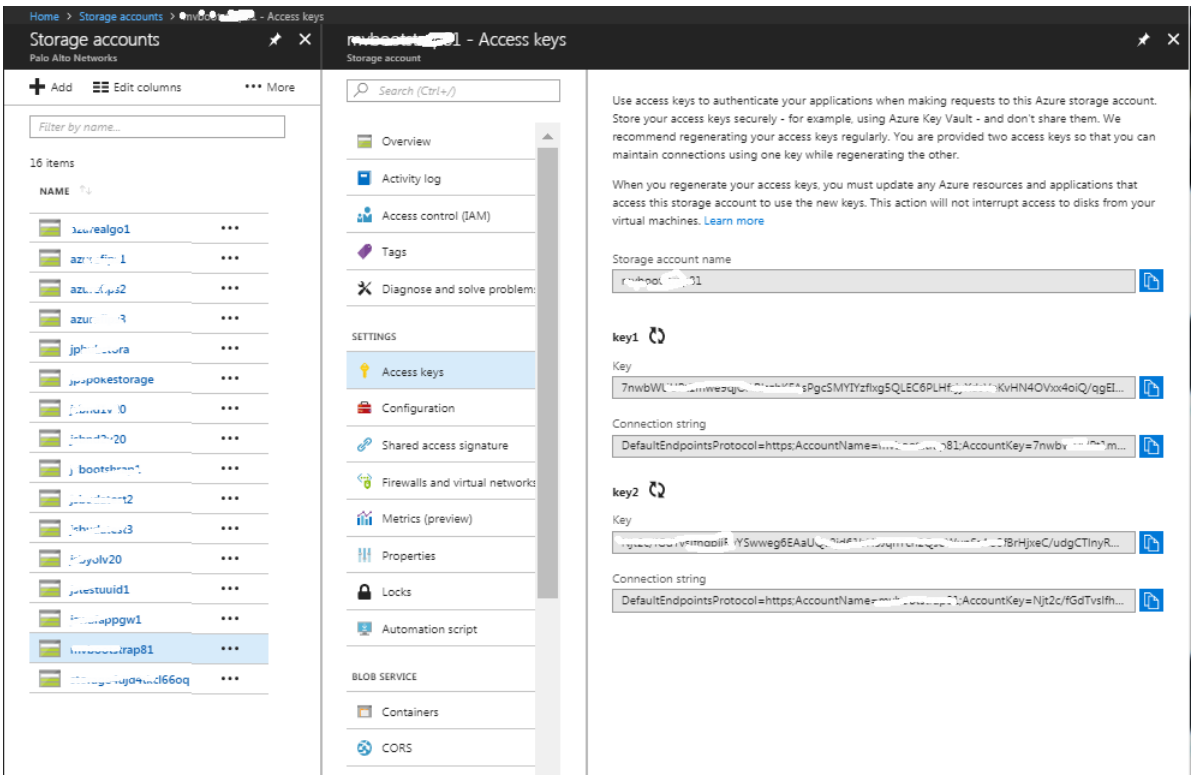
STEP 3 | 从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）。

- 如果您使用文件配置防火墙，请继续执行步骤 3.1。
- 如果您使用自定义数据配置防火墙，请继续执行步骤 3.2。



1. 如果您选择使用引导数据包，请选择 **Enable Bootstrap:Yes**（启用引导：是），并提供所需信息以访问包含引导文件的文件共享。
    1. 存储帐户名称 — 这是一个您可以在其中创建引导文件夹的文件共享 Azure 存储帐户。
    2. 存储帐户访问密钥 — 防火墙需要此访问密钥以对存储帐户进行身份验证，并访问其中的文件。要复制此访问密钥，请选择存储帐户名称，然后选择 **Settings**（设置）> **Access Keys**（访问密钥）。

©2024 Palo Alto Networks, Inc.



3. 文件共享 — 包含引导数据包的文件共享名称。
4. （可选）共享目录 — 文件共享中子文件夹的路径。如果您拥有可用作不同设置的引导配置的存储库公共文件共享，则可以使用共享目录创建文件夹层次结构，并访问公共文件共享中一组特定的子文件夹。

2. 输入配置参数作为自定义数据。有关键值对，请参阅输入基本配置作为用户数据（公共云）。每个键值对之间用分号分隔。例如：

```
type=dhcp-client; op-command-modes=jumbo-frame; vm-series-
auto-registration-pin-id=abcdefgh1234****; vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

使用在 Azure 虚拟机上自定义数据和 Cloud-Init 中的方法之一提供自定义数据。

STEP 4 | 验证引导完成。

©2024 Palo Alto Networks, Inc.

在 ESXi 上引导 VM 系列防火墙

您可以使用 ISO 映像或虚拟硬盘引导 VM 系列防火墙。

- 使用 ISO 文件在 ESXi 上引导 VM 系列防火墙
- 使用块存储设备在 ESXi 上引导 VM 系列防火墙

使用 ISO 文件在 ESXi 上引导 VM 系列防火墙

按照以下说明使用 ISO 在 ESXi 服务器上引导 VM 系列防火墙。

STEP 1 | 创建一个 ISO 映像，并将其上传到虚拟机文件系统 (VMFS) 存储设备，或上传到网络文件系统 (NFS) 卷。

1. 准备引导数据包.
2. 创建一个 ISO 映像。在创建映像时，您可以针对不同的客户端操作系统选择使用不同的工具。
3. 将 ISO 映像上传到可供 ESX/ESXI 主机访问的 VMFS 数据存储设备或 NFS 数据卷。

STEP 2 | 部署防火墙。

1. 在 ESXi 服务器上设置 VM 系列防火墙.

   默认情况下，防火墙会部署两个网络接口，一个用于管理流量，另一个用于数据流量。确保防火墙上的第一个以太网接口（即管理接口）连接到专为设备管理而分配的虚拟交换机端口组。
2. 切勿关闭防火墙。

STEP 3 | 将引导映像连接到防火墙。

1. 从 **Inventory**（目录）列表中选择 VM 系列防火墙。
2. 单击 **Edit Settings**（编辑设置），然后选择 **Virtual Hardware**（编辑设置）。
3. 在 **CD DVD drive**（**CD DVD** 驱动器）下拉列表中选择 **Datastore iso file**（数据存储 **iso** 文件），然后**browse**（浏览）ISO 映像。
4. 启动防火墙。此时，防火墙将会开始引导流程，该流程将需要几分钟的时间。之后，控制台上将会显示引导成功或失败的状态消息。
5. 验证引导完成.

使用块存储设备在 ESXi 上引导 VM 系列防火墙

按照以下说明使用块存储设备在 ESXi 服务器上引导 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建引导数据包和虚拟硬盘。

1. 创建引导数据包。
2. 部署 Linux 虚拟机。
3. 在 Linux 机器上，准备引导数据包。您可以将文件夹留空，但必须创建所有的四个文件夹。
4. 将一个容量少于 39 GB 的新硬盘连接到该 Linux 虚拟机。
5. 对该磁盘进行分区，并将文件系统格式化为 ext3。
6. 为新文件系统创建一个目录，并将磁盘安装到 Linux 虚拟机上。
7. 将引导数据包的内容复制到磁盘。
8. 拆下磁盘。
9. 从 Linux 虚拟机中分离磁盘。记下描述您创建的引导磁盘的磁盘文件；它显示数据存储区名称和磁盘路径。此外，不要选中从数据存储删除文件复选框；这样做会删除磁盘。

STEP 2 | 部署防火墙。

1. 在 ESXi 服务器上设置 VM 系列防火墙.
2. 切勿关闭防火墙。

STEP 3 | 将引导数据包连接到防火墙。

1. 从目录列表中选择 VM 系列防火墙。
2. 单击 **Edit Settings**（编辑设置），然后选择 **Virtual Hardware**（编辑设置）。
3. 从新建设备下拉列表中选择 **Existing Hard Disk**（现有硬盘）。根据前面提到的数据存储和路径选择引导磁盘。
4. 启动防火墙。此时，防火墙将会开始引导流程，该流程将需要几分钟的时间。之后，控制台上将会显示引导成功或失败的状态消息。
5. 验证引导完成.

©2024 Palo Alto Networks, Inc.

在 Google Cloud Platform 上引导 VM 系列防火墙

STEP 1 | 选择引导方法。

STEP 2 | 登录到 Google Cloud 控制台。

- 要将基本配置添加到引导数据包，请按准备引导数据包中所述创建引导文件，然后继续执行步骤 3。
- 要输入基本配置作为自定义元数据，请跳至步骤 4。

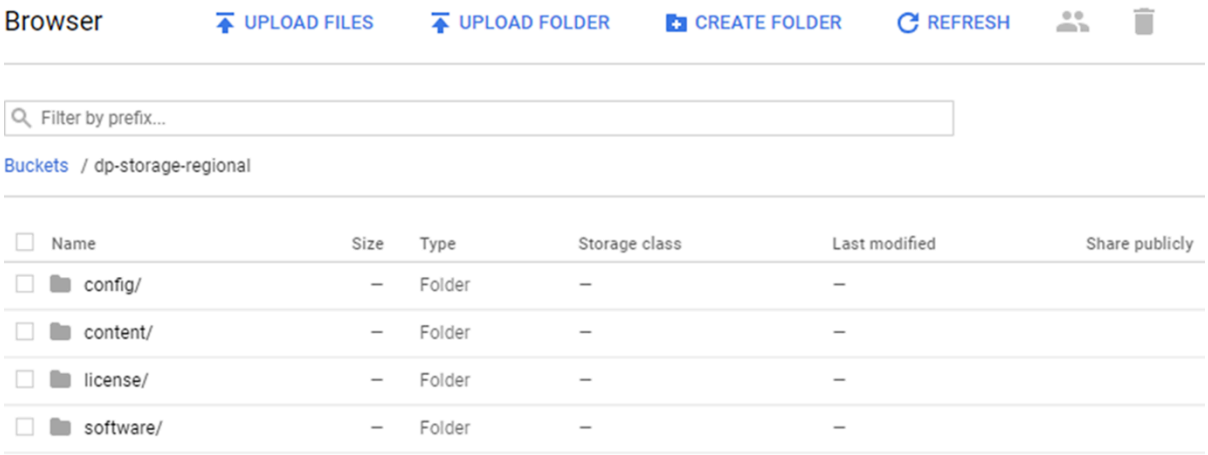
STEP 3 | 选择**Storage**（存储） > **Browser**（浏览），并单击 **Create Bucket**（创建存储桶）。

当您从 Google Cloud Platform Marketplace 部署 VM 系列防火墙时，可以使用此存储桶引导防火墙。

如果打算在同一项目中使用 Google 存储桶进行引导，则必须具有 devstorage.read_only IAM 权限。

您可以在顶层创建并填充存储桶，也可以在其中创建带有子文件夹的存储桶，以便多个引导数据包可以共享同一个存储桶。

1. 输入桶名称，选择默认存储类别，然后选择位置。请注意，存储桶的位置必须与您指定用于 compute engine 实例的区域兼容。
2. 单击 **Create**（创建）。
3. 在存储浏览中，单击存储桶名称以打开它。
4. 单击 **Create Folder**（创建文件夹），并命名文件夹为 `config`。单击 **Create**（创建）。
5. 重复为`content`、`license`和`software`创建文件夹的过程，如下所述。即使文件夹为空，所有文件夹均必须存在。



6. （可选）如果您已创建 **`init-cfg.txt`** 文件，则打开 `config` 文件夹。单击 **Upload Files**（上传文件），浏览以选择您的 **`init-cfg.txt`** 文件，然后单击 **Open**（打开）。
7. 打开 `license` 文件夹，然后上传 **`authcodes`** 文件。
8. 继续，直到所有引导文件均上传完毕。

©2024 Palo Alto Networks, Inc.

STEP 4 | 添加初始配置参数作为元数据。**Add**（添加）每个键值对，如输入基本配置作为用户数据（公共云）中所述。

STEP 5 | 有关部署详细信息，请参阅从 Google Cloud Platform Marketplace 部署 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

在 Hyper-V 上引导 VM 系列防火墙

您可以使用 ISO 映像或虚拟硬盘引导 VM 系列防火墙。

- 使用 ISO 文件在 Hyper-V 上引导 VM 系列防火墙
- 使用块存储设备在Hyper-V上引导 VM 系列防火墙

使用 ISO 文件在 Hyper-V 上引导 VM 系列防火墙

按以下说明使用 ISO 在 Hyper-V 服务器上引导 VM 系列防火墙。

STEP 1 | 创建一个 ISO 映像。

1. 准备引导数据包.
2. 创建一个 ISO 映像。在创建映像时，您可以针对不同的客户端操作系统选择使用不同的工具。
3. 将 ISO 映像上传到可供 Hyper-V 主机访问的位置。

STEP 2 | 部署防火墙。

1. 使用 Hyper-V 管理器在 Hyper-V 主机上设置 VM 系列防火墙.

   默认情况下，防火墙会部署两个网络接口，一个用于管理流量，另一个用于数据流量。确保防火墙上的第一个以太网接口（即管理接口）连接到专为设备管理分配的 vSwitch。
2. 切勿关闭防火墙。

STEP 3 | 将引导映像连接到防火墙。

1. 在 Hyper-V 管理器中，从 **Virtual Machines**（虚拟机）列表中选择 VM 系列防火墙。
2. 单击 **Settings**（设置） > **Hardware**（硬件） > **IDE Controller**（**IDE** 控制器） > **DVD Drive**（**DVD** 驱动器）。

   如果您有多个 *DVD* 驱动器，则必须将 *ISO* 映像应用于第一个驱动器。
3. 在 Media（媒介）窗口中，单击 **Image file**（映像文件）单选按钮。
4. 单击 **Browse**（映像文件），然后选择上传的 ISO 映像。
5. 单击 **Apply**（应用）和 **OK**（确定），以退出虚拟机设置。
6. 启动防火墙。此时，防火墙将会开始引导流程，该流程将需要几分钟的时间。之后，控制台上将会显示引导成功或失败的状态消息。
7. 验证引导完成.

使用块存储设备在Hyper-V上引导 VM 系列防火墙

按照以下说明使用块存储设备在 Hyper-V 服务器上引导 VM 系列防火墙。

©2024 Palo Alto Networks, Inc.

STEP 1 | 创建引导数据包和虚拟硬盘。

1. 部署 Linux 虚拟机。
2. 在 Linux 机器上，准备引导数据包。您可以将文件夹留空，但必须创建所有的四个文件夹。
3. 将一个容量少于 39 GB 的新硬盘连接到该 Linux 虚拟机。
    1. Linux 虚拟机电源。
    2. 在 Hyper-V 中，从 Virtual Machines（虚拟机）列表中选择 Linux 虚拟机。
    3. 选择 **Settings**（设置） > **Hardware**（硬件） > **IDE Controller**（**IDE** 控制器）。
    4. 选择 **Hard Drive**（硬盘驱动器），然后单击 **Add**（添加）。
    5. 选择 **Virtual Hard Disk**（虚拟硬盘），然后单击 **New**（新建）。
    6. 按照屏幕上的说明创建新的 VHD。请注意新 VHD 的名称和路径。
    7. 单击 **Apply**（应用）和 **OK**（确定），以退出虚拟机设置。
    8. 开启 Linux 虚拟机。
4. 连接到 Linux 虚拟机的 CLI。
5. 对该磁盘进行分区，并将文件系统格式化为 ext3。
6. 为新文件系统创建一个目录，并将磁盘安装到 Linux 虚拟机上。
7. 将引导数据包的内容复制到磁盘。
8. 拆下磁盘。
9. 从 Linux 虚拟机中分离磁盘。
    1. Linux 虚拟机电源。
    2. 从虚拟机列表中选择 Linux 虚拟机。
    3. 选择 **Settings**（设置） > **Hardware**（硬件） > **IDE Controller**（**IDE** 控制器）。
    4. 选择您创建的 VHD。
    5. 单击 **Remove**（移除）。这会分离 VHD，但不会将其删除。

STEP 2 | 部署防火墙。

1. 使用 Hyper-V 管理器在 Hyper-V 主机上设置 VM 系列防火墙.
2. 切勿关闭防火墙。

©2024 Palo Alto Networks, Inc.

STEP 3 | 将引导磁盘映像连接到防火墙。

1. 从虚拟机列表中选择防火墙。
2. 选择 **Settings**（设置） > **Hardware**（硬件） > **IDE Controller**（**IDE** 控制器）。
3. 选择 **Hard Drive**（硬盘驱动器），然后单击 **Add**（添加）。
4. 选择 **Virtual Hard Disk**（虚拟硬盘），然后单击 **Browse**（浏览）。
5. 浏览到您创建的引导VHD，选择它，然后单击 **Open**（打开）。
6. 单击 **Apply**（应用）和 **OK**（确定），以退出虚拟机设置。
7. 启动防火墙。此时，防火墙将会开始引导流程，该流程将需要几分钟的时间。之后，控制台上将会显示引导成功或失败的状态消息。
8. 验证引导完成.

©2024 Palo Alto Networks, Inc.

在 KVM 上引导 VM 系列防火墙

您可以使用 ISO 映像或虚拟硬盘在 KVM 上引导 VM 系列防火墙。

- 使用 ISO 文件在 KVM 上引导 VM 系列防火墙
- 使用块存储设备在 KVM 上引导 VM 系列防火墙

使用 ISO 文件在 KVM 上引导 VM 系列防火墙

按照以下说明使用 ISO 在 KVM 服务器上引导 VM 系列防火墙。

STEP 1 | 创建一个 ISO 映像。

1. 准备引导数据包。
2. 创建一个 ISO 映像。在创建映像时，您可以针对不同的客户端操作系统选择使用不同的工具。
3. 将 ISO 映像上传到可供 KVM 主机访问的位置。

STEP 2 | 部署防火墙。

1. 在 KVM 上安装 VM 系列防火墙。

   默认情况下，防火墙会部署两个网络接口，一个用于管理流量，另一个用于数据流量。确保防火墙上的第一个以太网接口（即管理接口）连接到专为设备管理而分配的虚拟交换机端口组。
2. 切勿关闭防火墙。

STEP 3 | 将引导映像连接到防火墙。

1. 在 virt 管理器中，双击 VM 系列防火墙以打开控制台。
2. 导航至 **View**（视图） > **Details**（详情），查看 VM 硬件的详情。
3. 单击 **Add HardwareChoose Storage Volume**（添加 **HardwareChoose** 存储卷），打开 Add New Virtual Hardware（添加新虚拟硬件）菜单。
4. 将设备类型更改为 IDE CDROM。
5. 单击 **Select managed or other existing storage**（选择托管或其他已有存储）单选按钮，然后单击 **Browse**（浏览）。找到您创建的 ISO 映像，然后单击 **Choose VolumeChoose Storage Volume**。
6. 单击 **FinishChoose Storage Volume**，退出 Add New Virtual Hardware（添加新虚拟硬件）菜单。
7. 导航至 **Virtual Machine**（虚拟机） > **Run**（运行），打开防火墙。此时，防火墙将会开始引导流程，该流程将需要几分钟的时间。之后，控制台上将会显示引导成功或失败的状态消息。
8. 验证引导完成。

©2024 Palo Alto Networks, Inc.

使用块存储设备在 KVM 上引导 VM 系列防火墙

按照以下说明使用块存储设备在 KVM 服务器上引导 VM 系列防火墙。

STEP 1 | 创建引导数据包和虚拟硬盘。

1. 创建引导数据包。
2. 创建一个小于 39 GB 的新磁盘映像，对磁盘进行分区，并将文件系统格式化为 ext3。根据客户端操作系统，用于完成此过程的工具可能各不相同。
3. 安装磁盘映像文件，并将准备好的引导数据包复制到磁盘映像文件。
4. 将引导数据包的内容复制到磁盘。
5. 拆下磁盘映像。
6. 将磁盘映像文件上传到可供 KVM 主机访问的位置。

STEP 2 | 部署防火墙。

1. 在 KVM 上安装 VM 系列防火墙。
2. 切勿关闭防火墙。

STEP 3 | 将引导磁盘映像连接到防火墙。

1. 在 virt-manager 中，双击 VM 系列防火墙以打开控制台。
2. 选择 **View**（视图） > **Details**（详细信息），查看 VM 硬件详细信息。
3. 单击 **Add HardwareChoose Storage Volume**（添加 **HardwareChoose** 存储卷），打开 Add New Virtual Hardware（添加新虚拟硬件）菜单。
4. 选择 **Storage**（存储）并选择 **Select or create custom storage**（选择或创建自定义存储）。
5. 单击 **Manage**（管理）按钮打开 **Choose Storage Volume**（选择存储卷）对话框，然后选择您之前创建的磁盘映像文件。
6. 单击 Choose Volume（选择卷）。
7. 确保设备类型是磁盘设备，并且不要更改总线类型。
8. 单击 Finish（完成）。
9. 启动防火墙。此时，防火墙将会开始引导流程，该流程将需要几分钟的时间。之后，控制台上将会显示引导成功或失败的状态消息。
10. 验证引导完成。

©2024 Palo Alto Networks, Inc.

验证引导完成

引导期间，您可在控制台上查看基本状态日志，并确认引导流程已完成。

STEP 1 | 如果 `init-cfg.txt` 文件中包含 **`panorama-server`**、**`tplname`** 和 **`dgname`**，则检查 Panorama 托管设备、设备组和模板名称。

STEP 2 | 验证一般系统设置和配置。进入 Web 界面，然后选择 **Dashboard**（仪表盘）> **Widgets**（小部件）> **System**（系统），或使用 CLI 运行命令 **`show system info`** 和 **`showconfig running`**。

STEP 3 | 验证许可证的安装情况。选择 **Device**（设备）> **Licenses**（许可证），或使用 CLI 运行命令 **`request license info`**。

STEP 4 | 如果您已配置 Panorama，则可通过 Panorama 管理内容及软件版本。如果您未配置 Panorama，则可使用 Web 界面管理内容及软件版本。

©2024 Palo Alto Networks, Inc.

引导错误

如果您在引导流程中收到了错误消息，请参阅下表了解详细信息。

错误消息（严重程度）	原因
启动映像错误（高）	• 未检测到具有引导程序包的外部设备。 或者 • 从外部设备上的映像启动时发生严重错误。引导流程已中止。
外部设备上无引导配置文件（高）	外部设备没有引导配置文件。
引导配置文件中强制网络信息所需参数错误或缺失（高）	引导所需的网络参数不正确或缺失。此时，错误消息会列出导出引导失败的相关值，包括 IP address（IP 地址）、netmask（网络掩码）、default gateway（默认网关）。
无法为文件 <license-key-filename> 安装许可证密钥（高）	无法运用许可证密钥。该错误表示所用的许可证密钥无效。输出包括无法运用的许可证密钥的名称。
使用授权代码 <authcode> 安装许可证密钥失败（高）	无法运用许可证授权代码。该错误表示所用的许可证授权代码无效。输出包括无法运用的许可证授权代码的名称。
内容更新提交失败（高）	内容更新运用失败。
已成功通过给定的数据包准备了 USB 媒介（提示性）	引导映像已在 USB 闪存设备上成功编译。<username>：已成功使用程序包 <bundlename> 准备 USB
成功引导（提示性）	已使用引导配置文件成功配备了防火墙。输出包括所安装的许可证密钥以及引导配置的文件名。在 VM 系列防火墙上，还会显示 PAN-OS 版本和内容更新版本。

了解有关引导数据包以及如何准备引导数据包的详细信息。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.