VM 系列部署指南

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

April 13, 2020

Table of Contents

关于 VM 系列防火墙 11
VM 系列型号 12
VM 系列系统要求 12
CPU 超额认购 14
VM-50 Lite 模式 14
VM 系列部署 16
高可用性中的 VM 系列 18
升级 VM 系列防火墙 19
升级 PAN-OS 软件版本（独立版本） 19
升级 PAN-OS 软件版本（HA 对） 21
使用 Panorama 升级 PAN-OS 软件版本 24
升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列） 26
升级 VM 系列型号 31
升级 HA 对中的 VM 系列型号 33
将 VM 系列防火墙降级到上一版本 34
VM 系列插件 35
在防火墙上配置 VM 系列插件 35
升级 VM 系列插件 36
在 VM 系列防火墙上启用巨帧 (Jumbo Frame) 39
虚拟机监控程序分配的 MAC 地址 40
发布用于监控的自定义 PAN-OS 指标 41
用于访问 VM 系列防火墙上外部服务的接口 42

授权 VM 系列防火墙许可证 43
许可证类型 — VM 系列防火墙 44
适用于 NSX 许可证的 VM 系列防火墙 45
面向公共云的 VM 系列防火墙许可证 45
VM 系列企业许可协议（多型号 ELA） 46
VM 系列防火墙的序列号和 CPU ID 格式 53
创建支持帐户 54
注册 VM 系列防火墙 55
注册 VM 系列防火墙（使用授权代码） 55
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）。 55
在 BYOL 和 PAYG 许可证之间切换 57
在公共云上从旧版 PAYG 列表切换 58
切换 VM 系列许可证 59
更新 VM 系列防火墙许可证包 61
激活许可证 63
激活 VM 系列防火墙的许可证（独立版本） 63
激活 VMware NSX 的 VM 系列防火墙的许可证（独立版本） 64
停用许可证 68
安装许可证停用API密钥 68
使用 CLI 停用功能许可证或订阅 69
停用 VM 70
授权 API 许可证 74
管理许可证 API 密钥 74
使用许可证 API 75
许可证 API 错误代码 77
云安全服务提供商许可证 (CSSP) 78

获取 CSSP 许可证包的身份验证码 78
使用 CSSP 身份验证代码注册 VM 系列防火墙 78
为注册的 VM 系列防火墙添加最终用户信息 79

在 ESXi 服务器上设置 VM 系列防火墙 83
在 VMware vSphere 虚拟机监控程序 (ESXi) 上支持的部署 84
ESXi 系统上 VM 系列的要求和限制 85
ESXi 系统上的 VM 系列要求 85
ESXi 系统上 VM 系列的限制 85
在 VMware vSphere 虚拟机监控程序 (ESXi) 上安装 VM 系列防火墙 87
规划适用于ESXi的 VM 系列的接口 87
在 ESXi 服务器上设置 VM 系列防火墙 88
在 ESXi 上对 VM 系列防火墙执行初始配置 90
添加额外磁盘空间至 VM 系列防火墙 91
通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具 92
vCenter 上的 VM 监控 95
关于 VM ware vCenter上的 VM 监控 95
安装适用于 VMware vCenter 的 Panorama 插件 96
为 VMware vCenter 配置 Panorama 插件 96
排除 ESXi 部署的故障 99
基本故障排除 99
安装问题 99
许可问题 101
连接问题 101
ESXi 的 VM 系列性能调整 103
在 ESXi 上安装 NIC 驱动程序 103
在 ESXi 上启用 DPDK 104
在 ESXi 上启用 SR-IOV 105
在 ESXi 上启用 NIC 的多队列支持 105

在 vCloud Air 上设置 VM 系列防火墙 107
关于 vCloud Air 上的 VM 系列防火墙 108
vCloud Air 上支持的部署 109
在 vCloud Air 上部署 VM 系列防火墙 110

在 VMware NSX 上设置 VM 系列防火墙 115
在 VMware NSX-V 上设置 VM 系列防火墙 116
VM 系列 NSX-V 版防火墙概述 116
NSX-V 部署清单上的 VM 系列防火墙 122
安装 VMware NSX 插件 124
将 VM 系列防火墙注册为 NSX-V Manager 上的服务 125
部署 VM 系列防火墙 132
创建安全组和控制规则 140
将安全策略应用于 VM 系列防火墙 144
控制来自不运行 VMware 工具的来宾的流量 148
VM 系列防火墙 NSX-V 版上的多 NSX Manager 支持是什么？ 148
动态隔离感染的来宾 152
将以操作为中心的配置迁移到以安全为中心的配置 155
用例：共享的计算基础架构和安全策略 158
用例：专用计算基础架构上的共享安全策略 162
动态地址组 — 将信息从 NSX-V Manager 中继到 Panorama 167

在 VMware NSX-T 上设置 VM 系列防火墙（北向南）..... 172
VMware NSX-T 上支持的 VM 系列防火墙部署（北向南）.....172
NSX-T 上 VM 系列防火墙的组件（北向南）.....172
在 NSX-T 上部署 VM 系列防火墙（北向南）.....173
在 NSX-T 上设置 VM 系列防火墙（东向西）..... 186
NSX-T 上 VM 系列防火墙的组件（东向西）.....186
NSX-T 集成上的 VM 系列防火墙（东向西）.....187
VMware NSX-T 上支持的 VM 系列防火墙部署（东向西）.....188
在 NSX-T 上部署 VM 系列防火墙（东向西）.....189

在 AWS 上设置 VM 系列防火墙.....203
关于 AWS 上的 VM 系列防火墙.....204
AWS EC2 实例类型..... 204
AWS GovCloud 上的 VM 系列防火墙..... 204
AWS China 上的 VM 系列防火墙.....204
AWS Outposts 上的 VM 系列防火墙..... 205
AWS 术语.....205
管理接口映射以用于 Amazon ELB.....207
AWS 的 VM 系列性能调整.....208
AWS 上支持的部署..... 209
在 AWS 上部署 VM 系列防火墙.....211
获取 AMI..... 211
AWS VPC 中 VM 系列防火墙的规划工作表..... 215
在 AWS 上启动 VM 系列防火墙.....217
在 AWS Outpost 上启动 VM 系列防火墙.....222
创建自定义 Amazon 机器映像 (AMI).....227
在 AWS上 加密 VM 系列防火墙的 EBS 卷.....229
使用 VM 系列防火墙 CLI 以交换管理接口.....231
在 VM 系列防火墙上启用 CloudWatch 监控..... 231
AWS 上的 VM 系列防火墙启动和运行状况日志..... 235
AWS 上 VM 系列防火墙的高可用性.....240
AWS 上 HA 的概述..... 240
HA 的 IAM 角色.....241
HA 链接..... 242
检测信号轮询和呼叫消息.....242
设备优先级和抢先..... 243
高可用性计时器..... 243
在 AWS 上配置主动/被动 HA..... 243
用例：保护 AWS 云中的 EC2 实例.....247
用例：使用动态地址组保护 VPC 中的新 EC2 实例.....257
用例：VM 系列防火墙作为 AWS 上的 GlobalProtect 网关..... 260
GlobalProtect 基础架构的组件.....260
在 AWS 上部署 GlobalProtect 网关..... 261
AWS 上的 VM 监控..... 262
使用 Panorama 上的 AWS 插件进行 VM 监控..... 263
在 Panorama 上设置用于 VM 监控的 AWS 插件.....263
使用 Amazon ELB 服务自动扩展 VM 系列防火墙.....273
适用于 AWS 版本 2.0 的 VM 系列自动扩展模板.....274
适用于 AWS 版本 2.1 的 VM 系列自动扩展模板.....299
在 AWS VPC 上监控的属性列表.....322
监控 AWS VPC 所需的 IAM 权限.....323

在 KVM 上设置 VM 系列防火墙.....325
KVM 上的 VM 系列防火墙—要求和先决条件.....326
用于在网络上连接 VM 系列防火墙的选项.....327
KVM 上 VM 系列防火墙的先决条件.....327
在 KVM 上支持的部署.....329
保护单个主机上的流量.....329
保护 Linux 主机之间的流量.....329
在 KVM 上安装 VM 系列防火墙.....331
使用 Virt-Manager 安装 VM 系列防火墙.....331
在 ISO 安装 VM 系列防火墙.....336
启用使用 SCSI 控制器.....340
验证 VM 系列防火墙上网络接口排序的 PCI-ID.....341
KVM 的 VM 系列性能调整.....342
在 Ubuntu 16.04.1 LTS 上安装 KVM 和 Open vSwitch.....342
在 KVM 上启用 Open vSwitch.....342
将 Open vSwitch 与 DPDK 集成.....343
在 KVM 上启用 SR-IOV.....347
使用 SR-IOV 启用 VLAN 访问模式.....348
在 KVM 上启用 NIC 的多队列支持.....349
在 KVM 上的 NUMA 节点中隔离 CPU 资源.....349

在 Hyper-V 上设置 VM 系列防火墙.....351
Hyper-V 上支持的部署.....352
保护单个 Hyper-V 主机上的流量.....352
保护跨多个 Hyper-V 主机的流量.....352
Hyper-V 上的系统要求.....354
Linux 集成服务.....355
在 Hyper-V 上安装 VM 系列防火墙.....356
准备工作.....356
在 Hyper-V 上调整 VM 系列防火墙的性能.....356
使用 Hyper-V 管理器在 Hyper-V 主机上设置 VM 系列防火墙.....357
使用 PowerShell 在 Hyper-V 主机上设置 VM 系列防火墙.....358
在 VM 系列防火墙上执行初始配置.....359

在 Azure 上设置 VM 系列防火墙.....363
关于 Azure 上的 VM 系列防火墙.....364
Azure 网络和 VM 系列防火墙.....364
Azure 安全中心集成.....364
Azure 上的 VM 系列防火墙模板.....366
Azure 上对 VM 系列的最低系统要求.....367
支持 Azure 上 VM 系列的高可用性.....367
VM 系列在 Azure 上的服务主体权限.....367
Azure 上支持的部署.....369
从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）.....370
从 Azure China Marketplace 部署 VM 系列防火墙（解决方案模板）.....377
使用 Azure 安全中心建议保护您的工作负载.....381
基于 Azure 安全中心建议部署 VM 系列防火墙。.....381
从 Azure 安全中心连接现有 VM 系列防火墙.....382
使用 Panorama 转发日志到 Azure 安全中心.....383
在 Azure Stack 中部署 VM 系列防火墙.....386

在 VM 系列防火墙上启用 Azure 应用程序见解 389
Azure 上的 VM 监控 391
关于 Azure 上的 VM 监控 391
在 Panorama 上设置用于 VM 监控的 Azure 插件 391
使用 Azure 上 Panorama 插件监控的属性 395
在 Azure 上设置主动/被动 HA 397
在 Azure 上设置主动/被动 HA（北向南和东向西流量） 397
在 Azure 上设置主动/被动 HA（仅限东向西流量） 404
使用 ARM 模板部署 VM 系列防火墙 413
部署 VM 系列和Azure应用程序网关模板 416
VM 系列和 Azure 应用程序网关模板 416
开始使用 VM 系列和 Azure 应用程序网关模板 417
在 Azure 上自动扩展 VM 系列防火墙 424
在 Azure 上自动扩展 — 组件和规划清单 424
Azure 自动扩展部署用例 427
在 Azure 上自动扩展 — 工作原理 428
部署 Azure 自动扩展模板 429
Azure 自动扩展模板中的参数 439
在 Azure 上保护 Kubernetes 服务 443
适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？ 443
保护 AKS 集群 446

在 Google Cloud Platform 上设置 VM 系列防火墙 457
关于 Google Cloud Platform 上 VM 系列防火墙 458
Google Cloud Platform 和 VM 系列防火墙 458
对 VM 系列的最低系统要求 458
Google Cloud Platform 上支持的部署 460
Internet 网关 460
分段网关 460
混合云 IPSec VPN 461
在 Google Public Cloud 上准备设置 VM 系列防火墙 462
Google Cloud Platform (GCP) 帐户规划 462
虚拟私有云 (VPC) 网络规划 465
网络接口规划 465
从 Google Cloud Platform Marketplace 部署 VM 系列防火墙 467
用于 Google Cloud Launcher 负载均衡的管理接口交换 469
使用 VM 系列防火墙 CLI 以交换管理接口 470
使用自定义模板或 gcloud CLI 部署 VM 系列防火墙 472
在 VM 系列防火墙上启用 Google Stackdriver 监控 473
Google Stackdriver 权限 473
启动 Google Stackdriver 473
在 Google Cloud Platform (GCP) 上启用 VM 监控以跟踪 VM 更改 475
使用动态地址组保护 VPC 中的安全实例 477
在 Google Kubernetes 引擎群集中保护 Kubernetes 服务 479
使用适用于 Panorama 的 Google Cloud Platform 插件保护 Google Kubernetes 引擎服务 479
使用示例 Terraform 模板部署 Kubernetes 服务 481
为 Google Kubernetes 引擎配置 Google Cloud Platform 插件 485

在 Cisco ENCS 网络中设置 VM 系列防火墙 491
计划 Cisco ENCS 部署 492
为 Cisco ENCS 准备 VM 系列防火墙映像 494

从图形用户界面转换 qcow2 文件 494
从命令行界面转换 qcow2 文件 496
在 Cisco ENCS 上部署 VM 系列防火墙 500

在 Oracle Cloud Infrastructure 上设置 VM 系列防火墙 503
OCI 形状类型 504
OCI 上支持的部署 505
准备在 OCI 上设置 VM 系列防火墙 506
从 Oracle Cloud Marketplace 部署 VM 系列防火墙 509
在 OCI 上配置主动/被动 HA 513

在 Alibaba Cloud 上设置 VM 系列防火墙 519
Alibaba Cloud 上的 VM 系列防火墙 520
Alibaba Cloud 上 VM 系列防火墙的最低系统要求 521
VM 系列防火墙软件要求 521
VM 系列防火墙的 Alibaba Cloud 实例类型建议 521
Alibaba Cloud CLI 521
准备在 Alibaba Cloud 上部署 VM 系列防火墙 522
选择许可证和计划网络 522
在 Alibaba Cloud 控制台中创建自定义映像 522
准备使用 Aliyun 命令行界面 525
在 Alibaba Cloud 上部署 VM 系列防火墙 527
创建 VPC 并配置网络 527
创建和配置 VM 系列防火墙 529
确保 Alibaba Cloud 的北向南流量安全 531
在 Alibaba Cloud 上配置负载均衡 535

在 Cisco ACI 中设置防火墙 537
Palo Alto Networks 防火墙与 Cisco ACI 集成 538
Service Graph 模板 539
多上下文部署 539
准备您的 ACI 环境进行集成 540
在网络策略模式下将防火墙与 Cisco ACI 集成 541
在网络策略模式下部署防火墙以保护东向西向流量 541
部署防火墙以在网络策略模式下保护北向南流量 554
Cisco ACI 中的端点监控 567
安装适用于 Cisco ACI 的 Panorama 插件 568
配置 Cisco ACI 插件 568
适用于 Cisco ACI 仪表板的 Panorama 插件 571

在 Cisco CSP 上设置 VM 系列防火墙 575
Cisco CSP 上的 VM 系列要求 576
在 Cisco CSP 上部署 VM 系列防火墙 577

Cisco TrustSec 的端点监控 579
适用于 Cisco TrustSec 的 Panorama 插件 580
安装适用于 Cisco TrustSec 的 Panorama 插件 581
配置适用于 Cisco TrustSec 的 Panorama 插件 582

在 Nutanix AHV 上设置 VM 系列防火墙.....587
Nutanix 上的 VM 监控.....588
关于 Nutanix 上的 VM 监控.....588
安装适用于 Nutanix 的 Panorama 插件.....589
配置适用于 Nutanix 的 Panorama 插件.....589

引导 VM 系列防火墙.....593
VM 系列防火墙引导工作流程.....594
引导数据包.....595
引导配置文件.....596
在 Panorama 上生成 VM 身份验证密钥.....597
创建 init-cfg.txt 文件.....599
init-cfg.txt 文件组件.....600
init-cfg.txt 示例文件.....601
创建 bootstrap.xml 文件.....603
准备引导许可证.....604
准备引导包.....605
在 AWS 上引导 VM 系列防火墙.....607
在 Azure 上引导 VM 系列防火墙.....609
在 ESXi 上引导 VM 系列防火墙.....611
使用 ISO 文件在 ESXi 上引导 VM 系列防火墙.....611
使用块存储设备在 ESXi 上引导 VM 系列防火墙.....611
在 Google Cloud Platform 上引导 VM 系列防火墙.....613
在 Hyper-V 上引导 VM 系列防火墙.....614
使用 ISO 文件在 Hyper-V 上引导 VM 系列防火墙.....614
使用块存储设备在Hyper-V上引导 VM 系列防火墙.....614
在 KVM 上引导 VM 系列防火墙.....616
使用 ISO 文件在 KVM 上引导 VM 系列防火墙.....616
使用块存储设备在 KVM 上引导 VM 系列防火墙.....616
验证引导完成.....618
引导错误.....619

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 系列型号
> 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 系列防火墙上启用巨帧 (Jumbo Frame)
> 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

VM 系列型号

VM 系列防火墙的型号包括 — VM-50、VM-100、VM-200、VM-300、VM-500、VM-700 和 VM-1000-HV。

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

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

除 *VM-50* 和 *VM-100* 以外，所有 *VM* 系列型号都支持随 *PAN-OS 9.1.0* 发行的 SD-WAN 功能。

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 系列型号分配了必要的硬件资源。

© 2019 Palo Alto Networks, Inc.

VM 系列型号	支持的管理程序	支持的 vCPU	最小内存	最小硬盘驱动器
VM-50	ESXi、Hyper-V、KVM	2	• 5.5GB • 4.5GB（Lite 模式）	32 GB（启动时 60GB）
VM-100 VM-200	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、NSX-V、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS NSX-T (VM-100)	2、4	6.5GB	60GB
VM-300 VM-1000-HV	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、NSX-V、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-300)	2、4	9GB	60GB
VM-500	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、NSX-V、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	2、4、8	16GB	60GB
VM-700	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	2、4、8、16	56GB	60GB

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。更多有关 Lite 模式的信息，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*。

© 2019 Palo Alto Networks, Inc.

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

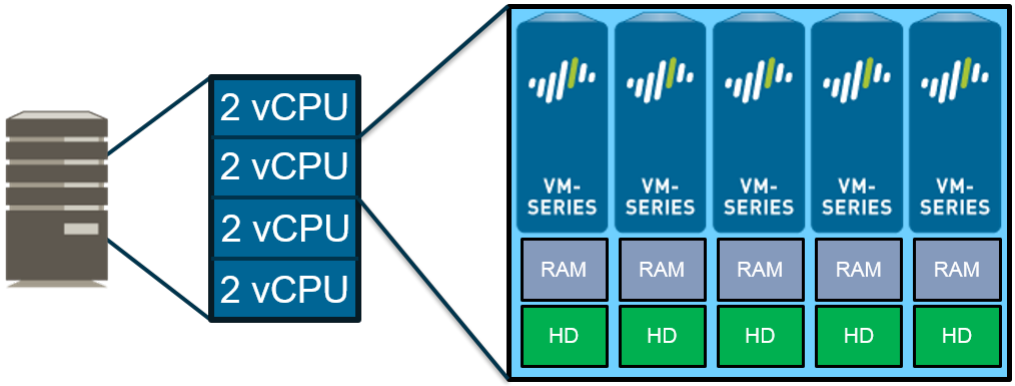
VM 系列防火墙支持所有型号的 CPU 超额订阅。CPU 超额订阅允许您在运行于 x86 架构的虚拟机管理程序上部署更高密度的 VM 系列防火墙。按照所需的 CPU 分配，可以部署两个 (2:1) 到五个 (5:1) VM 系列防火墙。规划部署时，请使用以下公式计算硬件可支持的 VM 系列防火墙数量。

（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

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。



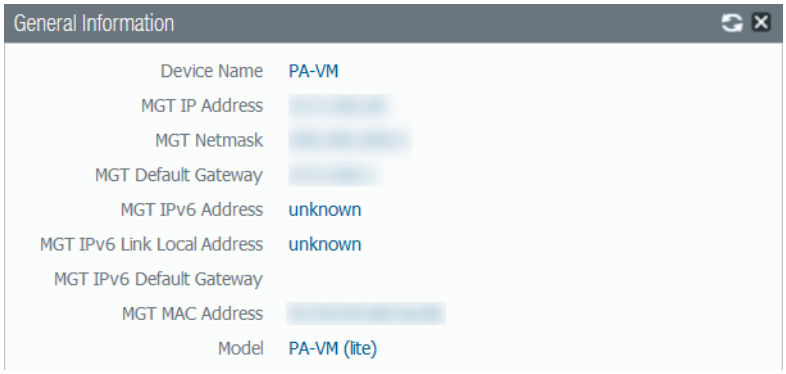
VM-50 Lite 模式

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 不支持巨型帧。

© 2019 Palo Alto Networks, Inc.



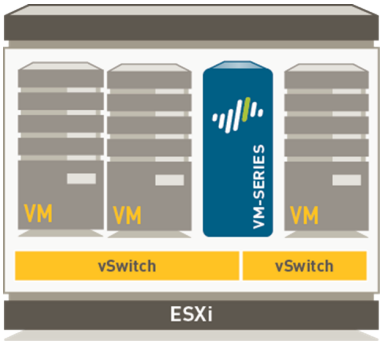
© 2019 Palo Alto Networks, Inc.

VM 系列部署

VM 系列防火墙可在以下平台上部署：

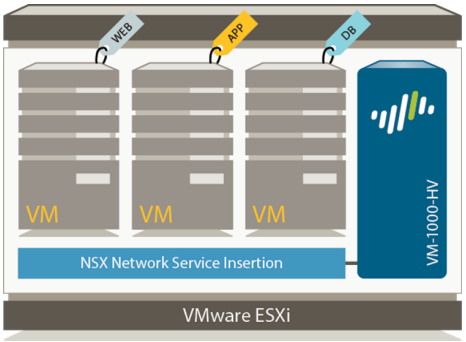
- 用于 **VMware vSphere** 虚拟机监控程序 **(ESXi)** 的 **VM** 系列和 **vCloud Air**

  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-V** 上的 **VM** 系列

  VM-100、VM-200、VM-300、VM-500 或 VM-1000-HV 可与 VMware NSX 和 Panorama 一起部署为网络自检服务。此部署最适合用于检测东向西流量，并且也可以确保北向南流量安全。



  有关详细信息，请参阅在 VMware NSX-V 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 Marketplace 上部署 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

© 2019 Palo Alto Networks, Inc.

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。

- 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。

© 2019 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群集中设置防火墙可以提供冗余，并且可以确保业务连续性。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。某些私有云管理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	否	是
HA2 —（会话同步和保持活动）	是	是	是	否	是	是	是	否	是
HA3	是	是	否	否	否	是	否	否	否

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。

© 2019 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；在每个管理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。

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）。

© 2019 Palo Alto Networks, Inc.

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。

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“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接口访问互联网，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）。

© 2019 Palo Alto Networks, Inc.

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。

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设备：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；在每个管理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。

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。

© 2019 Palo Alto Networks, Inc.

- 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 9.1 发行产品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“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，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，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。

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。如果要升级到 XFR 版本，请安装与 XFR 版本相对应的版本。

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。

© 2019 Palo Alto Networks, Inc.

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互联网，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**（仪表板）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。

STEP 9 | 在第二个对等上安装 PAN-OS 版本。如果要升级到 XFR 版本，请安装与 XFR 版本相对应的版本。

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**（仪表板）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）在刚升级的对端设备的 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 表上的硬件接口计数器增加如下：
  - 在主动/被动配置中，仅主动对等会显示传输的数据包；被动对等将只会显示收到的数据包。

    如果启用 *HA2* 保持活动状态，被动对等上的硬件接口计数器将同时显示发送和接收数据包。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，您将会看到这两个对等上收到的数据包和传输的数据包。

STEP 12 | 如果在升级之前禁用抢占行为，请立即重新启用。

© 2019 Palo Alto Networks, Inc.

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。

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 未连接互联网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；在每个管理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受管防火墙上。

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 和每个受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。

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 9.1 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 到受管防火墙时，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，“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。

© 2019 Palo Alto Networks, Inc.

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，则必须更新两个对端设备的内容。

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 对中选择一个对端设备。对于主动/被动对，选择主动对端设备；对于主动/主动对，选择主动-辅助对端设备。
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。

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**（对端设备）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**（对端设备）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 防火墙的对端设备。
5. 请勿选择 **Group HA Peers**（组高可用性对端设备）。
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，请单击是。

© 2019 Palo Alto Networks, Inc.

- 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）在刚升级的对端设备的 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 | 验证每个受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**（受管设备）。
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端设备的 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。

- 在维护窗口期间升级 NSX 的 VM 系列— 使用此选项在维护窗口期间升级 VM 系列防火墙，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，无需中断来宾 VM 中的服务，或是更改服务定义中的 OVF URL。
- 通过更改 OVF URL 升级 NSX 的 VM 系列— 使用此选项通过更改服务定义中的 OVF URL 来升级 VM 系列防火墙。

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 | 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。每个管理程序上分配额外硬件资源的过程都不相同。

STEP 2 | 将当前配置文件的备份保存在计划要升级的每个受管防火墙上。

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 和各受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。

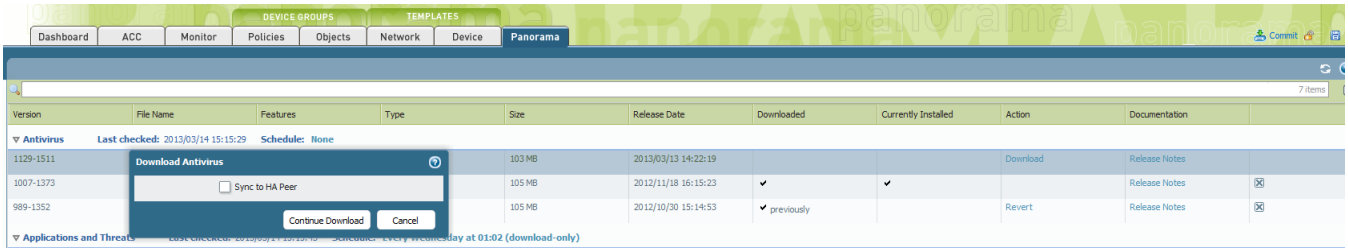
STEP 3 | 请参阅发行说明以确认 PAN-OS 版本所需的内容发行版本。

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）。

© 2019 Palo Alto Networks, Inc.

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。

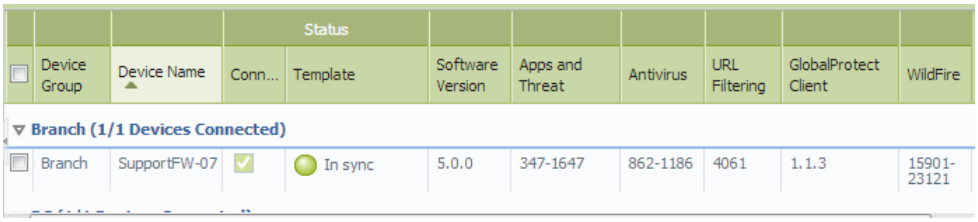
STEP 4 | 将软件更新部署到选定防火墙。

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设备。

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设备。

STEP 5 | 验证每个受管设备上运行的软件和内容发行版本。

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



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 | 将当前配置文件的备份保存在计划要升级的每个受管防火墙上。

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。

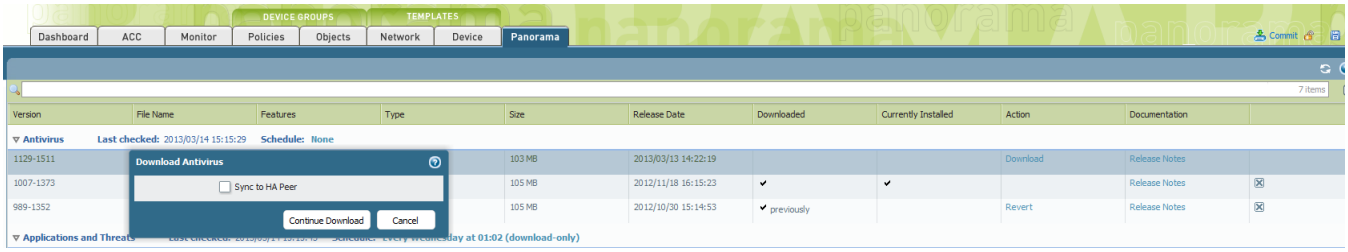
© 2019 Palo Alto Networks, Inc.

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 和各受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 2 | 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。

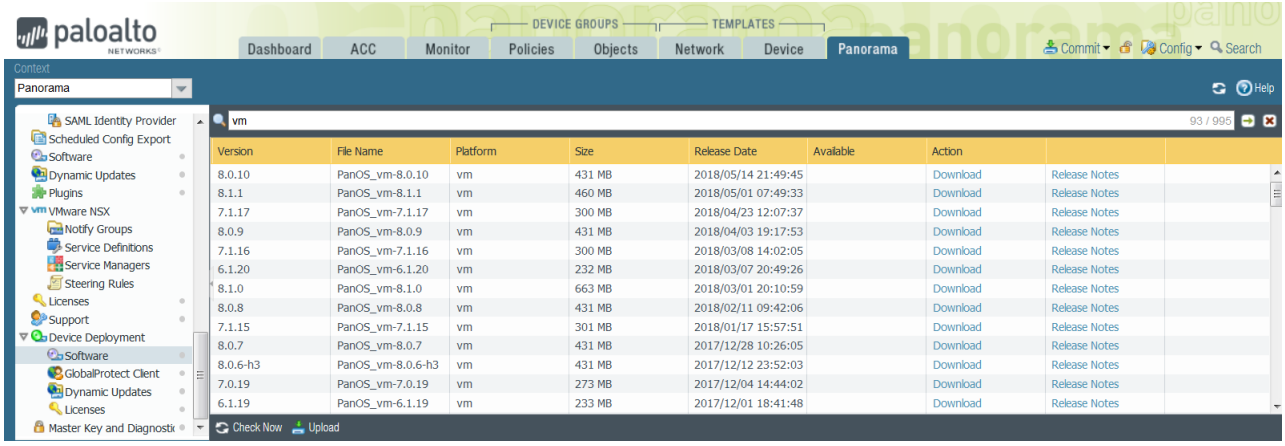
1. 选择 **Panorama** > **Device Deployment**（设备部署）> **Dynamic Updates**（动态更新）。
2. 检查最新更新。单击立即检查（位于窗口的左下角）以检查最新更新。操作列中的链接指示是否有更新可用。如果有版本可用，将会显示 **Download**（下载）链接。



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 3 | 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。

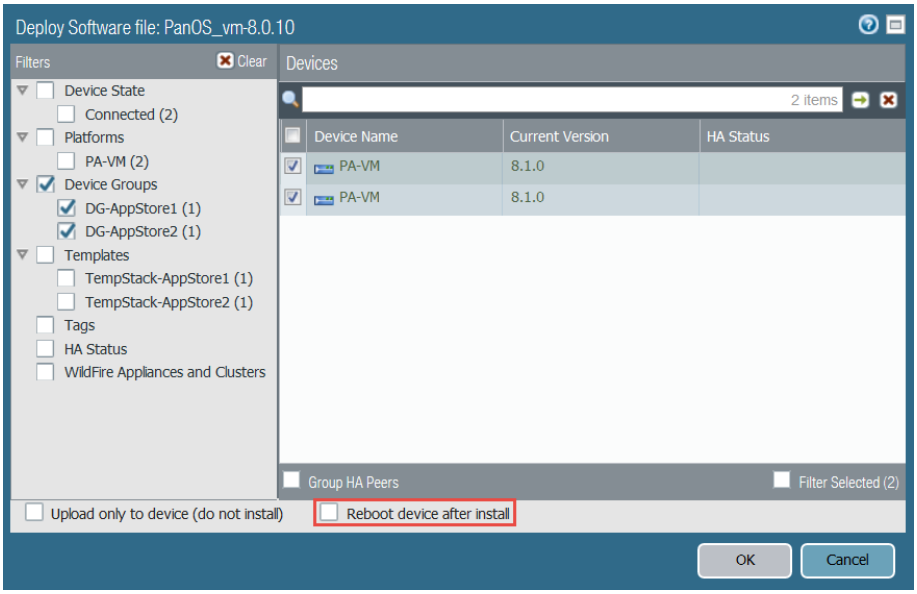


4. 单击 **Download**（下载）以检索该软件，然后单击 **Install**（安装）。

安装新的软件映像后，请勿重新启动 *VM* 系列防火墙。

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

© 2019 Palo Alto Networks, Inc.



7. 单击 **OK**（确定）。

STEP 4 | 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 系列系统要求。
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 5 | 为每个 ESXi 主机上每个 VM 系列防火墙重复此步骤。

STEP 6 | 验证每个受管设备上运行的软件和内容发行版本。

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

通过更改 *OVF URL* 升级 *NSX* 的 *VM* 系列

您可以通过更改服务定义中的 OVF URL 升级适用于 NSX 的 PAN-OS 版本 VM 系列防火墙。如果不更改 OVF URL，则将来部署的任何防火墙均将运行当前安装的 PAN-OS 版本，且需要进行额外升级。更改服务定义要求您重新部署防火墙，从而导致服务中断。因此，Palo Alto Networks 建议您在维护窗口期间执行此升级。

STEP 1 | 保存计划要升级的防火墙的当前配置文件备份。

© 2019 Palo Alto Networks, Inc.

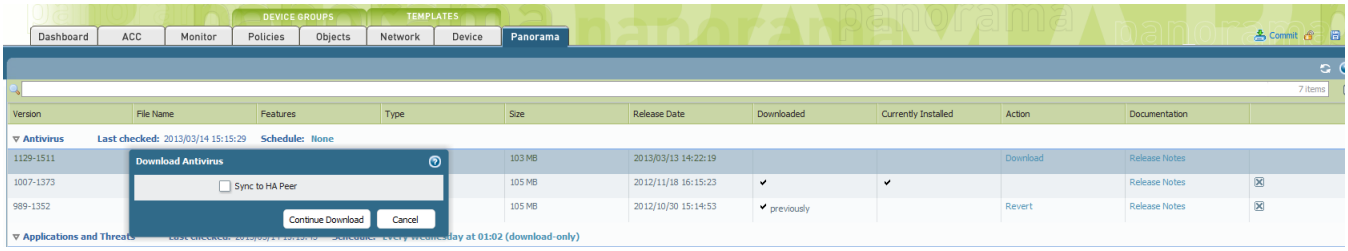
虽然防火墙将自动创建配置文件的备份，但还是在升级和存储在外部设备之前创建备份。

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 和各受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 2 | 请参阅发行说明以确认新的 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 3 | 下载新的 PAN-OS 基本映像文件。

1. 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。

选择与计划部署的 *VM* 系列型号相匹配的 *ovf* 文件。对于 *VM-200*，请使用 *vm100.ovf*。对于 *VM-1000-HV*，请使用 *vm300.ovf*。

2. 解压缩映像文件，以提取并将 .ovf、 mf 和 .vmdk 文件保存到可以访问 NSX Manager的目录。将所有三个文件存放在同一个目录。这些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。

STEP 4 | 添加新的 OVF URL 到服务定义配置。

1. 选择 **Panorama** > **VMware NSX** > **Service Definitions**（服务定义)，并选择要编辑的服务定义。
2. 在 **VM-Series OVF URL**（**VM** 系列 **OVF URL**）中，添加承载新的 ovf 文件的 Web 服务器的位置。http 和 https 均为支持协议。例如，输入 https://acme.com/software/PA-VM-NSX.9.1.0.ovf。

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* 群集中的 *VM* 系列防火墙上使用不同的 *PAN-OS* 版本。

。

3. 单击 **OK**（确定）。
4. 选择 **Commit**（提交）> **Commit to Panorama**（提交到 **Panorama**）> **Commit**（提交）。

   更改 OVF URL 并将其提交到 Panorama 会导致 NSX Manager上的配置不匹配。在 vCenter 中，您必须解决不匹配问题，才能重新部署与服务定义关联的防火墙。

© 2019 Palo Alto Networks, Inc.

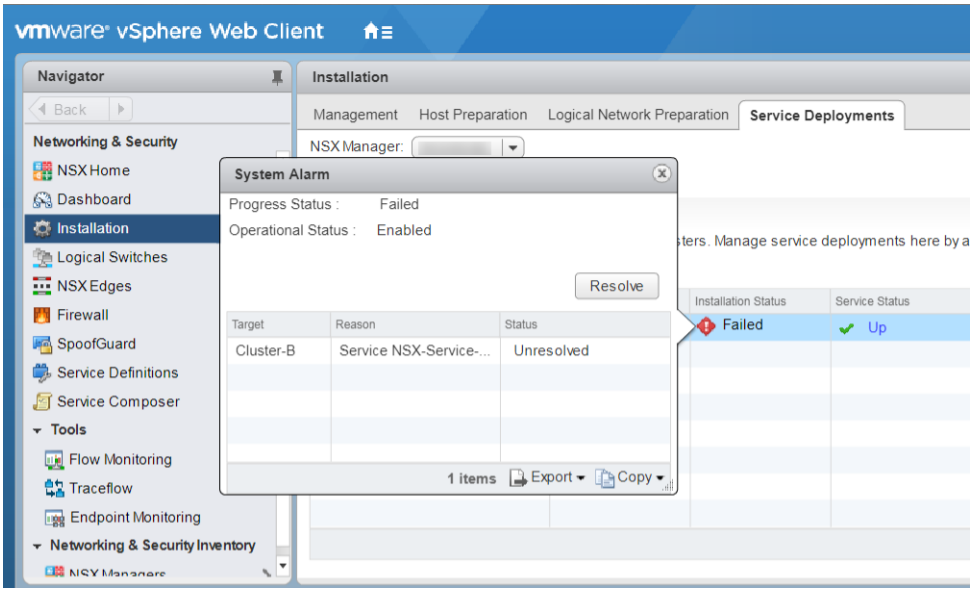
STEP 5 | 手动停用适用于 NSX 的VM 系列许可证。通过 Panorama CLI 或 Web 界面完成此任务。

- 使用 **`request license deactivate keyfeatures <name> mode manual`** CLI 命令使用 CLI 停用功能许可证或订阅。
- 要停用适用于 NSX 的 VM 系列许可证，则选择 **Complete Manually**（手动完成）（而非 **Continue**（继续）），然后按照步骤手动停用许可证。

STEP 6 | 重新部署防火墙。重新部署防火墙将中断穿过防火墙的任何流量。

1. 登录到 vSphere。
2. 选择 **Network & Security**（网络和安全）> **Installation**（安装）> **Service Deployments**（服务部署）。
3. 单击安装状态列的 **Failed**（已失败）图标以显示系统警报窗口。
4. 单击 **Resolve**（解决）。单击解决将重新部署带新 ovf 的防火墙。

重新部署防火墙将中断重定向到防火墙的任何流量。



STEP 7 | 验证防火墙重新部署是否已成功。

1. 选择 **Network & Security**（网络和安全）> **Installation**（安装）> **Service Deployments**（服务部署）。
2. 验证安装状态现在是否显示为成功。

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。

- 容量升级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。

© 2019 Palo Alto Networks, Inc.

- 在公共云部署中，如果使用 *BYOL* 选项许可防火墙，则必须在更改实例类型或 *VM* 类型之前停用 VM，然后在完成型号或实例升级后在防火墙上再次应用许可证。更改实例类型时，由于防火墙具有新的 *UUID* 和 *CPU ID*，因此现有许可证不再有效。

STEP 1 | 将额外的硬件资源分配给 VM 系列防火墙。

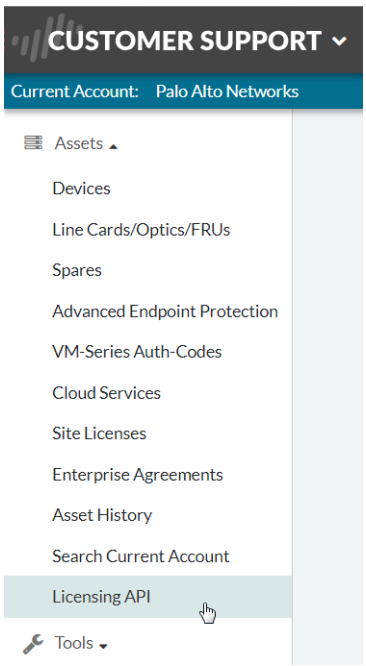
在启动容量升级之前，您必须验证是否有足够的硬件资源可用于 VM 系列防火墙以支持新容量。每个管理程序上分配额外硬件资源的过程都不相同。

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停用 API 密钥。

1. 登录到客户支持门户。
2. 从转到下拉列表中选择 **License API**（许可证 **API**）。
3. 复制 API 密钥。



确保您使用的是您用于注册初始许可证的相同帐户。

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 | 在 **Device**（设备）> **Setup**（设置）> **Service**（服务）上启用防火墙 **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：

© 2019 Palo Alto Networks, Inc.

- **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）— 如果您已在客户支持门户上激活您的许可证，则使用此选项。
- 手动上传许可证密钥 — 如果您的防火墙无法连接到 Palo Alto Networks 客户支持网站，请使用此选项。在此情况下，必须在具有 Internet 连接的计算机上从支持站点下载许可证密钥文件，然后上传到该防火墙。
- **Use an authorization code**（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）。

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。

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设备。

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。

按照程序升级 VM 系列型号。

在此被动对等上重新启动一些进程后，新的 VM 系列型号将显示在仪表盘上。这升级的对等现在是无功能状态，因为它与主动对等的容量不匹配。

如果您已启用会话同步，请在继续执行下一步之前验证会话是否跨 HA 对等同步。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增加如下：

- 在主动/被动配置中，仅主动对等会显示传输的数据包，被动设备只会显示收到的数据包。

  如果启用 HA2 保持活动状态，被动对等上的硬件接口计数器将同时显示发送和接收数据包。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，您将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。

© 2019 Palo Alto Networks, Inc.

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。
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）。

© 2019 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管理程序集成。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管理程序集成的发布。

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。

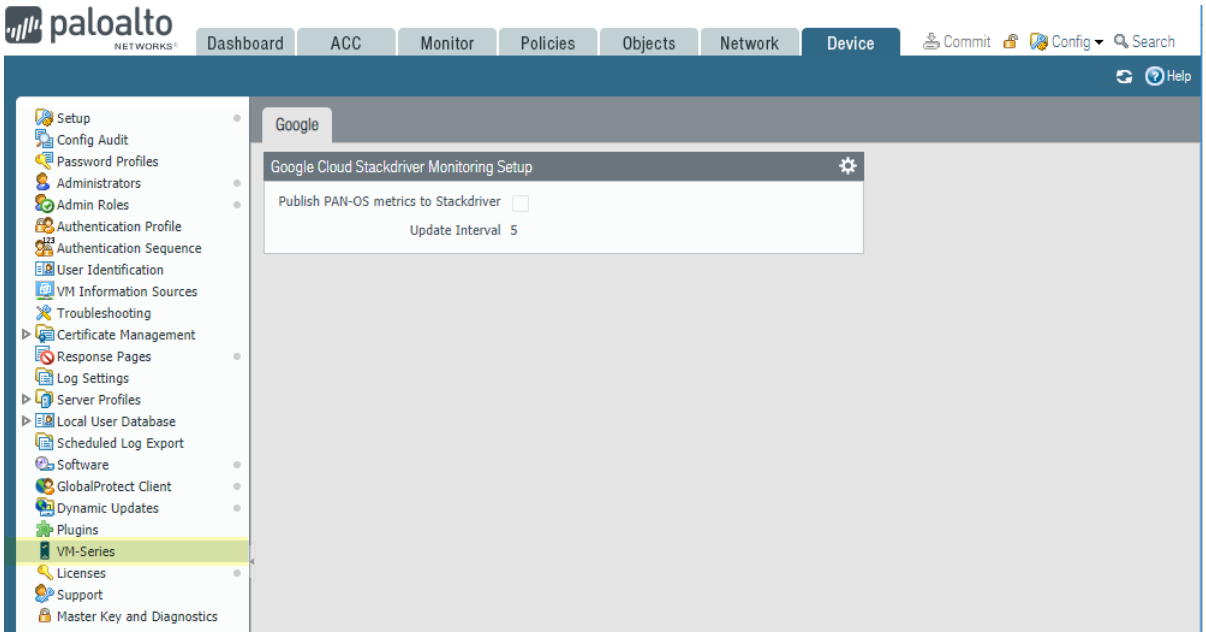
VM 系列插件是一个内置组件，可以升级或降级，但不能删除。每个 PAN-OS 版本都包含与 PAN-OS 软件版本对应的特定 VM 系列插件版本。当您降级到较早的 PAN-OS 软件版本时，插件版本将降级为与 PAN-OS 版本兼容的版本。您可以在虚拟防火墙上本地升级或降级 VM 系列插件，或者从 Panorama 集中管理插件版本。

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 VM 系列防火墙实例的云提供商配置插件集成。



如果防火墙部署在没有公共接口的管理程序或云（例如，VMware ESXi）上，则该选项卡将命名为 VM-Series 并显示一般消息。

© 2019 Palo Alto Networks, Inc.

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。

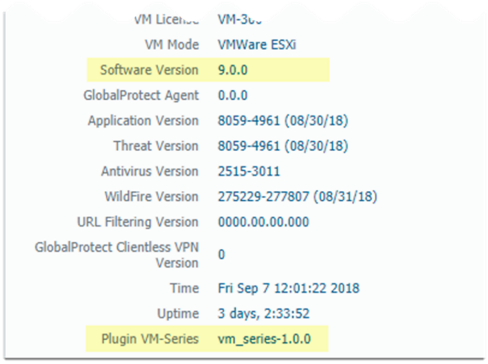
每个插件版本都提供 PAN-OS 兼容性信息，且包含一个或多个云环境的新功能或错误修复。

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。

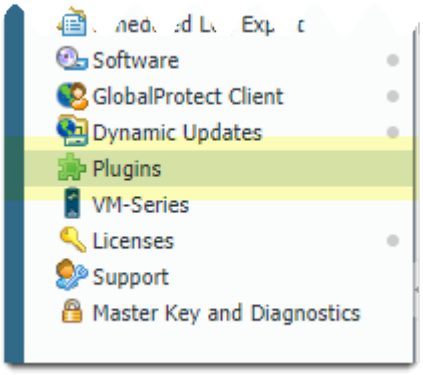
例如，假设新的 VM 系列插件版本仅包含 AWS 功能。要利用这些新功能，您必须在 AWS 上更新 VM 系列防火墙实例上的插件。

不要安装不适用于您的环境的升级。

STEP 2 | 登录 VM 系列防火墙，检查仪表盘以查看插件版本。



STEP 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。



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

© 2019 Palo Alto Networks, Inc.

Name	Version	Release Date	Size	Downloaded	Currently Installed	Actions	Releas
ame: vm_series							
eries-1.0.5	1.0.5	2019/09/10 18:11:21	15M	✔		Install Delete	
eries-1.0.0	1.0.0	2019/02/05 15:47:32	15M	✔	✔		
ame: vm_series-1.0.2							
eries-1.0.2	1.0.2	2019/04/07 09:42:26	15M			Download	Releas
ame: vm_series-1.0.3							
eries-1.0.3	1.0.3	2019/05/06 16:11:35	15M			Download	Releas
ame: vm_series-1.0.4							
eries-1.0.4	1.0.4	2019/07/09 15:08:08	15M			Download	Releas
ame: vm_series-1.0.6							
eries-1.0.6	1.0.6	2019/10/03 09:05:09	15M			Download	Releas
ame: vm_series-1.0.7							
eries-1.0.7	1.0.7	2019/11/05 16:15:15	15M			Download	Releas

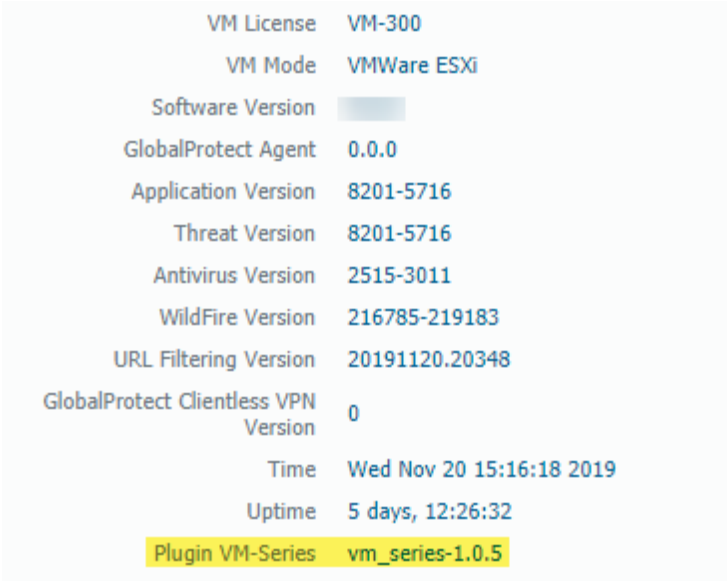
heck Now Upload

STEP 5 | 下载完成后，单击 **Install**（安装）。防火墙自动卸载之前安装的插件版本。

Name	Version	Release Date	Size	Downloaded	Currently Installed	Actions	Releas
ame: vm_series							
eries-1.0.5	1.0.5	2019/09/10 18:11:21	15M	✔		Install Delete	
eries-1.0.0	1.0.0	2019/02/05 15:47:32	15M	✔	✔		

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

© 2019 Palo Alto Networks, Inc.



© 2019 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用巨帧 (Jumbo Frame)

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 Frames（巨帧）。

如需在防火墙上使用 Jumbo Frames，您必须特定启用全球级的 Jumbo Frames。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 Frames 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 Frames，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 Frames，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。

STEP 1 | 启用 Jumbo Frames 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“会话设置”部分。
2. 选择 **Enable Jumbo Frame**（启用巨帧）。
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）。

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）。

© 2019 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/管理程序向物理接口分配的 MAC 地址，并在通过第 3 层接口部署的 VM 系列防火墙上使用该 MAC 地址。然后，防火墙会在其 ARP 响应中使用管理程序分配的 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。如果混杂模式和管理程序分配的 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* 上使用管理程序分配的 *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。使用管理程序分配的 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。

如果在 VM 系列防火墙上启用了管理程序分配的 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（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 对等设备的 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，使用管理程序分配的 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 对等设备上数据面板接口通用的虚拟 MAC 地址所替代。您在 HA 中的 VM 系列防火墙上启用管理程序分配的 MAC 地址后，虚拟 MAC 地址将不再被使用。各 HA 对等设备上的数据面板接口均为管理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，Internet 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/管理程序提供的接口 MAC 地址，请执行以下步骤。

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

STEP 2 | 禁用（清除）选项以 **Use Hypervisor Assigned MAC Address**（使用管理程序分配的 **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 3 | 在防火墙上 **Commit**（提交）更改。您无需重启防火墙。

© 2019 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
- 在 VM 系列防火墙上启用 Azure 应用程序见解
- 在 VM 系列防火墙上启用 Google Stackdriver 监控

© 2019 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用于访问服务器或服务的数据面板接口的 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 AWS S3 存储桶、Azure 存储文件服务、或 Google 存储桶等云存储位置进行引导	仅管理接口，包括交换接口的时间 如果 *bootstrap.xml* 包含许可证 *authcodes*，则无法使用服务路由。要许可防火墙，必须使用管理接口。
发布到 AWS CloudWatch、Azure Application Insights 和 Google Stackdriver 等云监控系统的 PAN-OS 指标	仅管理接口，包括交换接口的时间
VM 监控	管理接口或服务路由

授权 *VM* 系列防火墙许可证

您必须激活购买的服务的许可证以保护您的网络，然后才能开始使用 VM 系列防火墙保护东向西和北向南网络通信。

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。

了解有关创建支持帐户和激活许可证的详情：

- 许可证类型 — VM 系列防火墙
- VM 系列防火墙的序列号和 CPU ID 格式
- 创建支持帐户
- 注册 VM 系列防火墙
- 在 BYOL 和 PAYG 许可证之间切换
- 切换 VM 系列许可证
- 更新 VM 系列防火墙许可证包
- 激活许可证
- 停用许可证（释放属于防火墙的许可证）
- 授权 API 许可证
- 云安全服务提供商许可证 (CSSP)

许可证类型 — VM 系列防火墙

可以将 VM 系列防火墙许可证设为自带许可证 (BYOL)、即付即用 (PAYG) 或具有企业许可协议 (VM-ELA) 的证书。PAYG 是基于使用情况的选项，在用于受支持公共云平台的 marketplace 上提供。BYOL 和 VM 系列 ELA 可用于任何 VM 系列防火墙。您可以从合作伙伴、经销商或直接从 Palo Alto Networks 购买这些许可证类型。

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。
- 支持 — 除容量许可证外，您还需要支持授权，以便获取技术支持和软件更新。使用许可证绑定，可以包含高级支持权利。如果您需要 USG 支持，则必须在 AWSGov Cloud 和 Azure Government 上购买 BYOL。
- 订阅套餐 — 这些订阅可让您实施一系列的策略，确保在网络上安全启用应用程序和内容。例如，通过订阅 Treat Prevention，您可以获得内容更新，其中包括恶意软件检测相关的最新威胁信息。您可以从三种许可证套餐中进行选择：
  - 基本套餐包括 VM 系列容量许可证和高级支持授权。
  - 套餐 1 包括 VM 系列容量许可证、威胁防御许可证和高级支持授权。
  - 套餐 2 包括 VM 系列容量许可证和整套许可证（包含威胁防御、DNS 安全、GlobalProtect、WildFire、PAN-DB URL 筛选），以及高级支持授权。

  对于许可证套餐，有关更新选项，请参阅更新 VM 系列防火墙许可证包。如果需要在更新时间表之前添加更多的 VM 系列防火墙，则请与您的合作伙伴、经销商或 Palo Alto Networks 代表联系。
- **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管理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 将于 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。如果您要管理 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。

© 2019 Palo Alto Networks, Inc.

适用于 NSX 许可证的 VM 系列防火墙

如需在 VMware 集成 NSX 解决方案中自动执行 VM 系列 NSX 版防火墙的配置和许可，您可选用两种许可绑定：

- 一种套餐包括 VM 系列容量许可证（仅限 VM-100、VM-200、VM-300、VM-500 或 VM-1000-HV），威胁防御许可证和高级支持授权。
- 另一种套餐包括 VM 系列容量许可证（仅限 VM-100, VM-200、VM-300、VM-500 或 VM-1000-HV）和整套许可证（包括 Threat Prevention、GlobalProtect、WildFire、PAN-DB URL 筛选、DNS 安全），以及高级支持授权。

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：

- 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。
- 即用即付 **(PAYG)**—也称为基于使用情况或按使用付费许可证。以下配置支持 PAYG 许可型号：
  - PAN-OS 9.1.1，具有 VM 系列插件版本 1.0.9 和 1.0.10。
  - PAN-OS 9.1.2，具有 VM 系列插件版本 1.0.11 和更高版本。

  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。

  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。如果您要使用更新的 PAYG 列表，该列表根据实例类型上的可用资源自动选择 VM 系列型号，请参阅在公共云上从旧版 PAYG 列表切换中的说明。

  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 系列型号资源要求的更多信息，请参阅 VM 系列系统要求。

  - *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`***。
  - 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
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

© 2019 Palo Alto Networks, Inc.

许可证功能	套餐 1	套餐 2
Premium 支持	✓	✓
威胁阻止（AV、IPS 和恶意软件预防）	✓	✓
GlobalProtect		✓
PAN-DB URL Filtering		✓
WildFire		✓
DNS 安全		✓

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 令牌
- VM — 100-25 令牌
- VM — 300-50 令牌
- VM — 500-140 令牌
- VM — 700-300 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。参阅 管理 VM 系列 ELA 许可证令牌 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。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。

以下视频提供了 VM 系列多模型 ELA 的演练。

© 2019 Palo Alto Networks, Inc.

管理 *VM* 系列 *ELA* 许可证令牌

VM 系列企业许可协议（多型号 ELA）（VM 系列 ELA）使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。

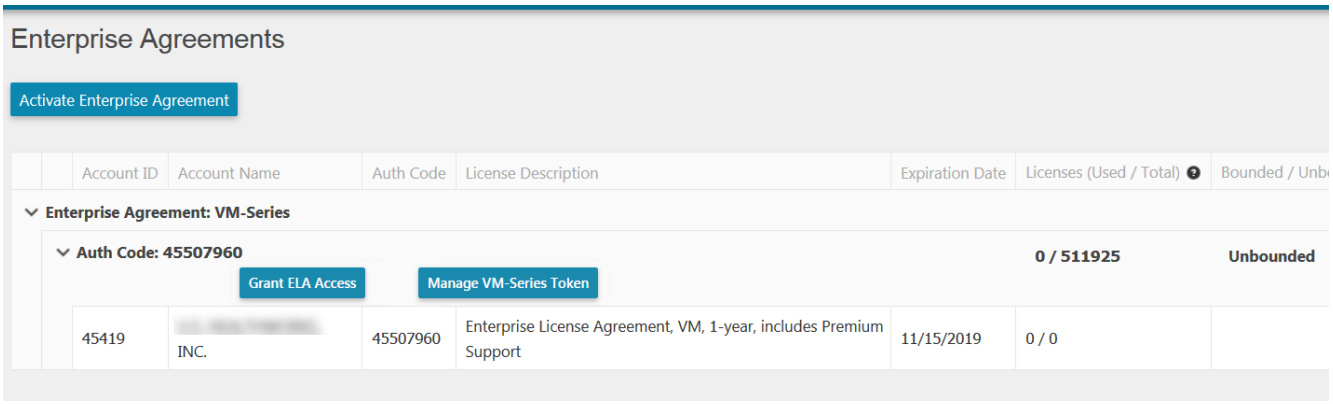
1. 登录到 Palo Alto Networks CSP。
2. 选择 **Members**（成员）> **Manage Users**（管理用户）。
3. 单击 操作（**Actions**）下的铅笔图标，以编辑要为其分配 ELA 管理员角色的用户。
4. 选择 **ELA Administrator**（**ELA** 管理员），然后单击复选标记以将新角色添加到所选用户。
5. 继续转到步骤 3。

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。

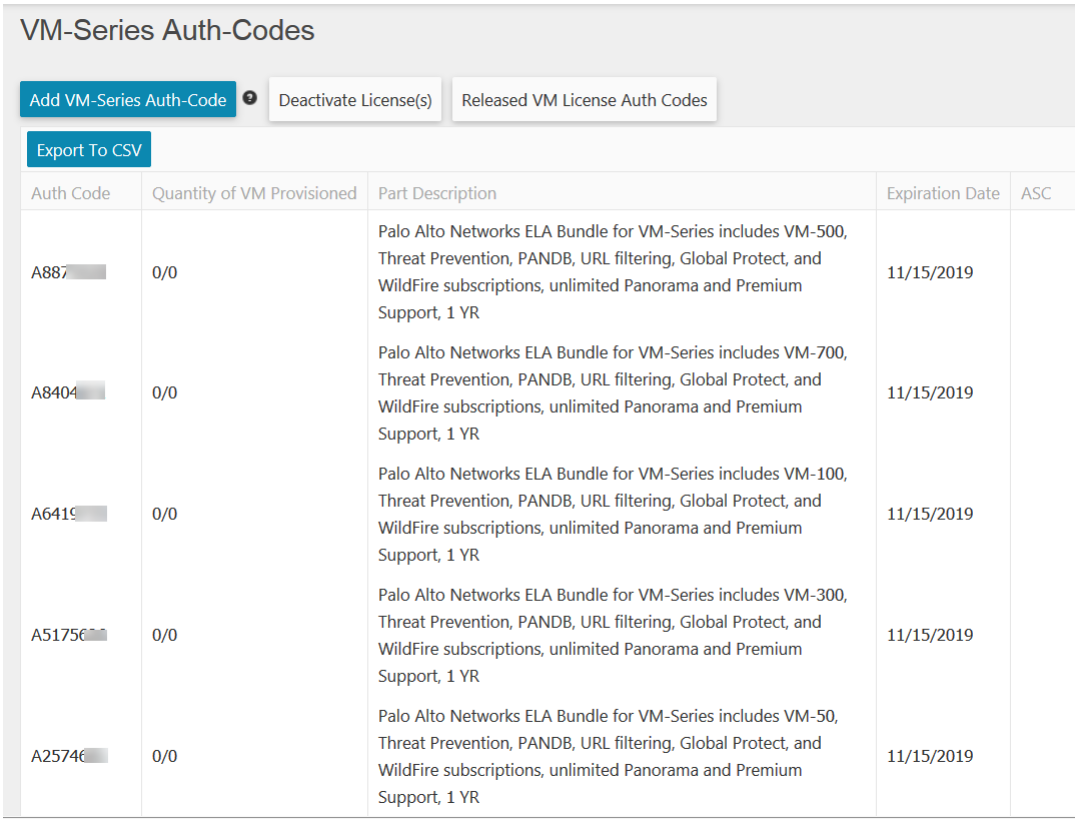
1. 登录到 Palo Alto Networks CSP。
2. 选择 **Assets**（资产）> **Enterprise Agreements**（企业协议）> **Activate Enterprise Agreement**（激活企业协议）。
3. 输入 **Authorization code**（授权代码）并 **Agree and Submit**（同意并提交）EULA。

   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。该页面显示身份验证代码、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），以及在协议的有界和无界期限内可以部署的数量。



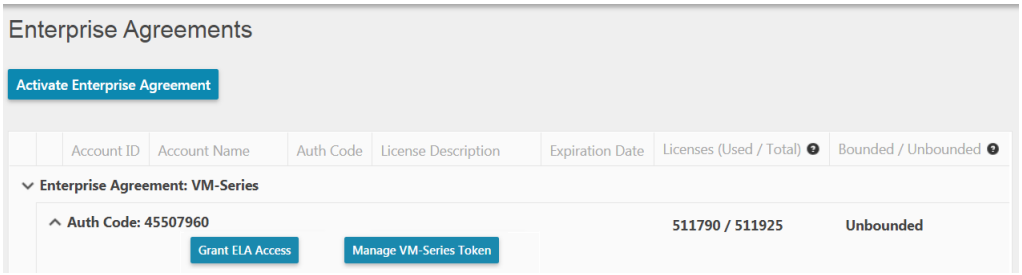
4. 选择 **Assets**（资产）> **VM-Series Auth-Codes**（**VM** 系列身份验证代码），以查看用于部署 VM 系列防火墙的每个型号以及 ELA 附带的关联订阅的授权代码。

© 2019 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。

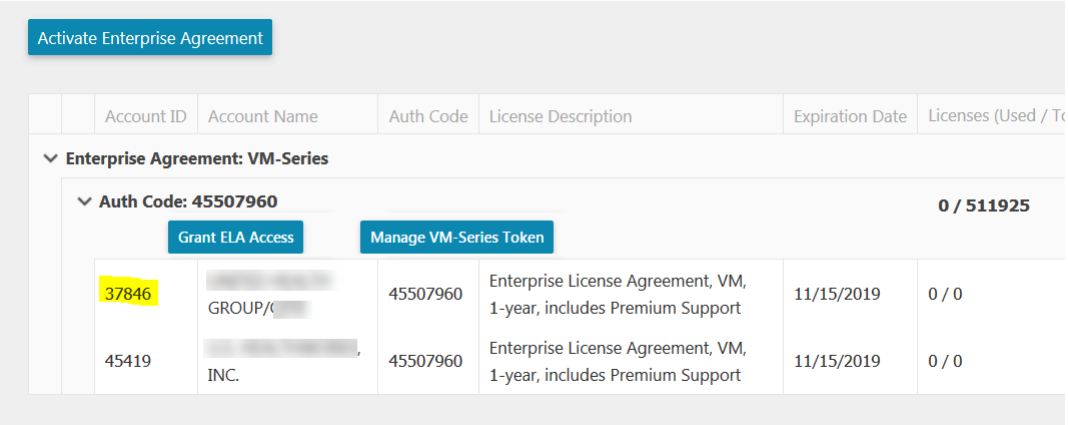


1. 在 **Assets**（资产）> **Enterprise Agreements**（企业协议）中，选择 **Grant ELA Access**（授予 **ELA** 访问权限）。
2. 输入要邀请的管理员的 **Destination Email**（目标电子邮件地址）。

   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。

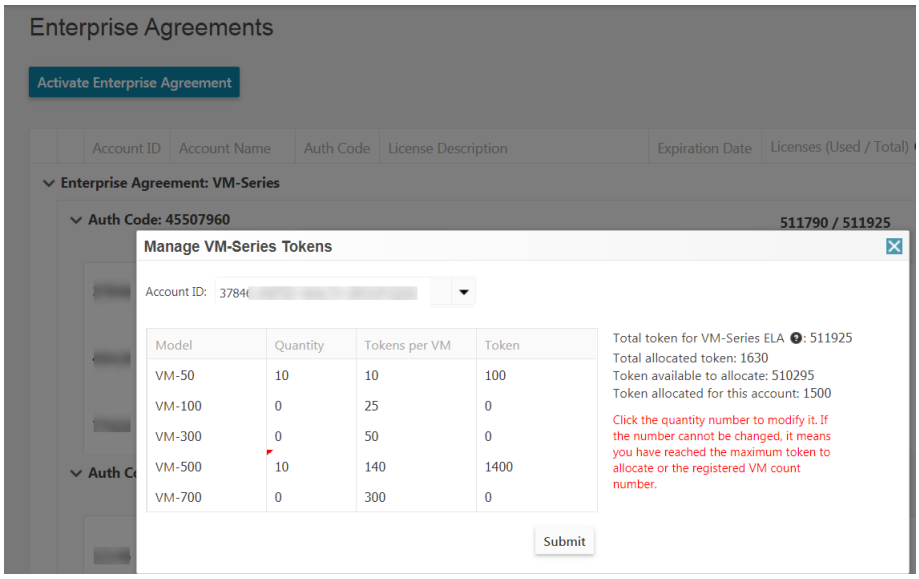
© 2019 Palo Alto Networks, Inc.



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）。

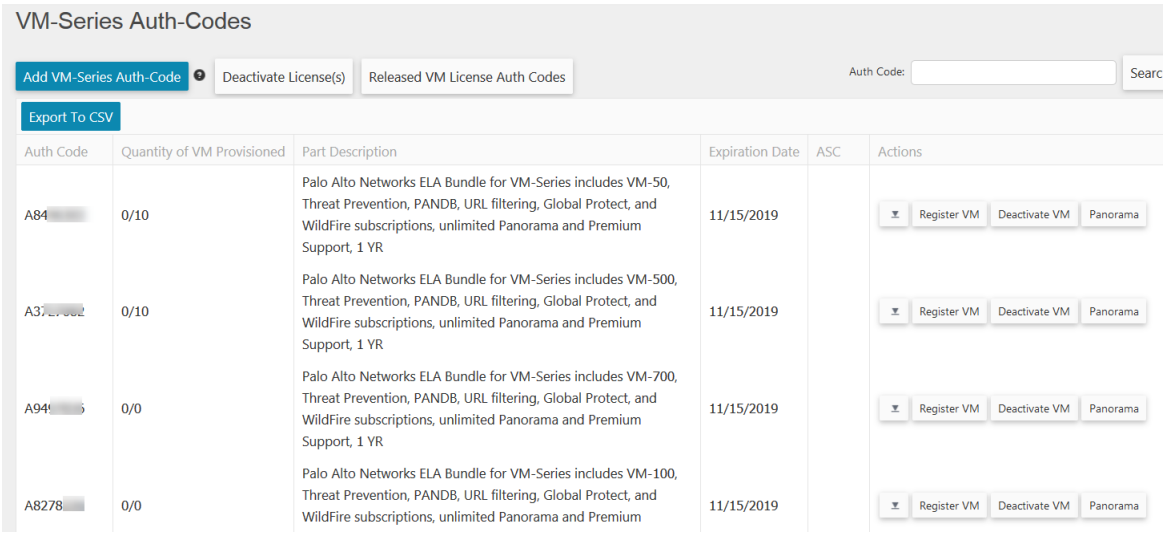
   对于每个帐户 ID，您可以按模型指定要分配的防火墙数。根据数量和防火墙模型，自动计算令牌数量并可供使用。在此示例中，您允许 VM -50和 VM -500 各 10 个实例。



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 系列身份验证代码）以确认分配的身份验证代码。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。

© 2019 Palo Alto Networks, Inc.

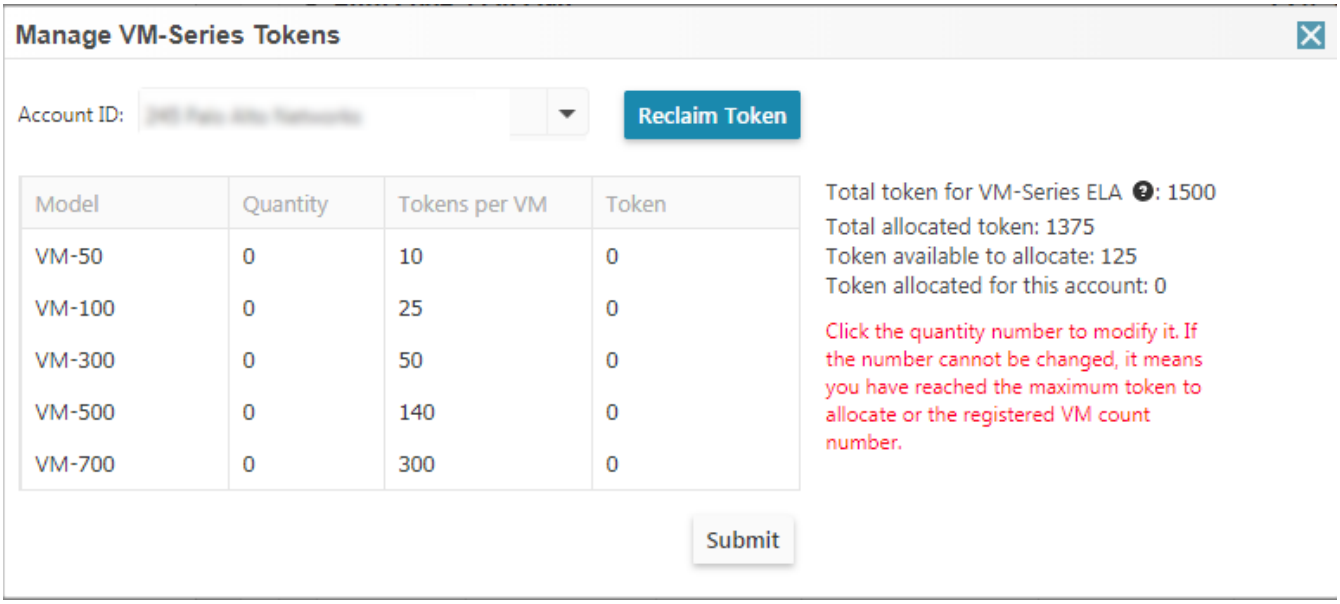


STEP 5 | 从 VM 系列 ELA 中删除 CSP 帐户以回收令牌。

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*

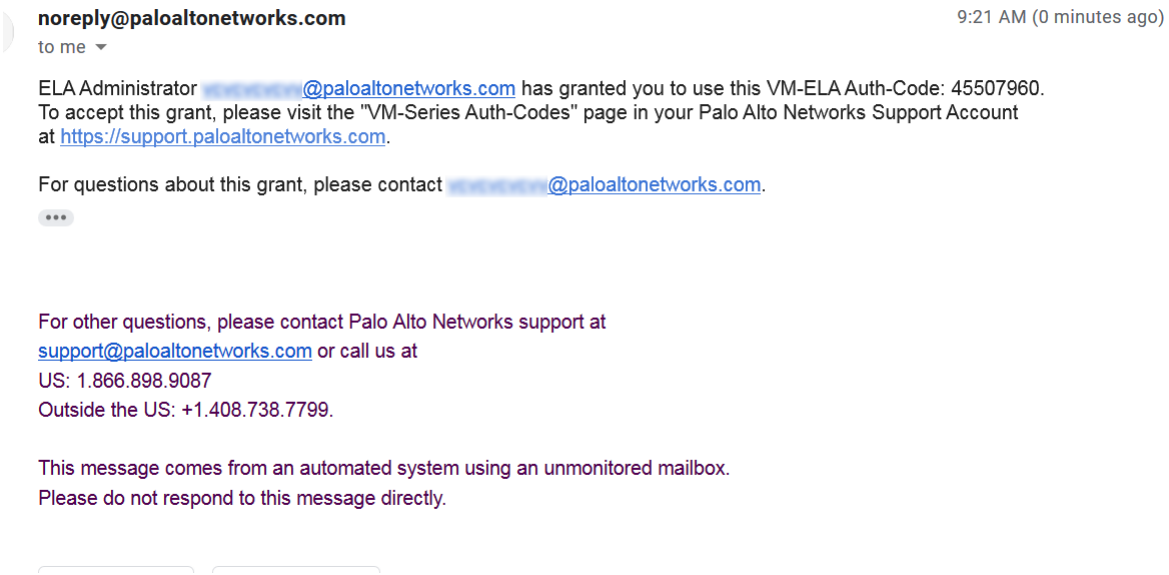
如果您的企业购买了 VM 系列 ELA，您的 ELA 管理员可以邀请您共享合同并共享许可令牌池，以便您可以访问 VM 系列防火墙验证码，以便您按需部署 VM 系列防火墙。当您收到访问 VM 系列 ELA 的授权时，您

© 2019 Palo Alto Networks, Inc.

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。

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。

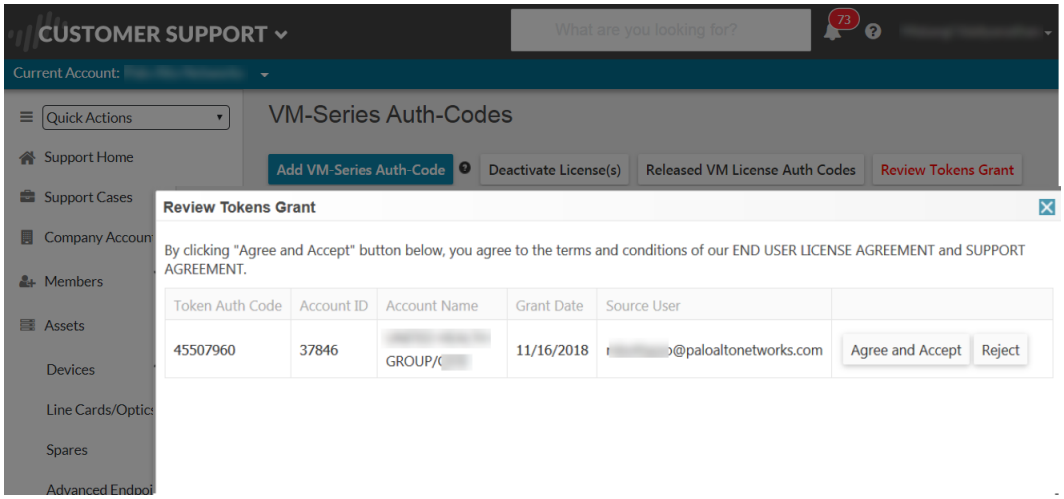


STEP 2 | 接受授予。

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** 系列身份验证代码）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。确保让 ELA 管理员知道您已接受授权，以便他/她可以分配您可以部署的 VM 系列防火墙型号和数量。

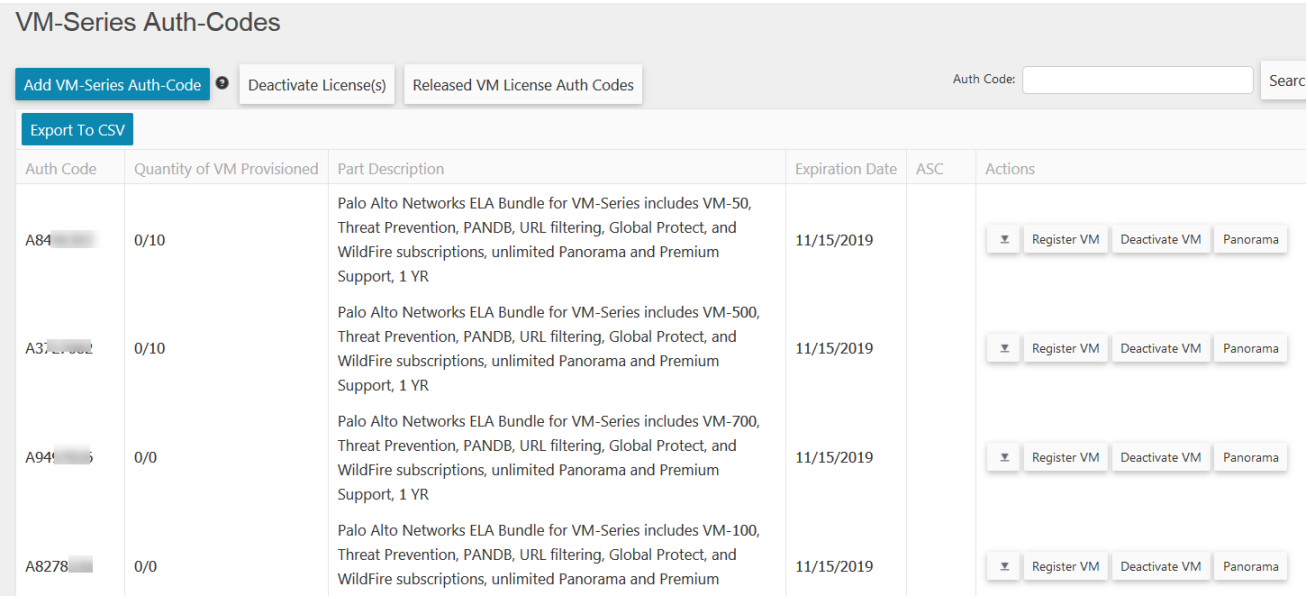


如果您属于 *CSP* 上的多个帐户且意外接受授予错误帐户，则必须请求 *ELA* 管理员重新授予您。接受正确帐户中的授权之前，请勿开始使用授权代码配置防火墙。

© 2019 Palo Alto Networks, Inc.

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** 系列身份验证代码）以查看哪些模型以及为您分配了多少模型。例如，以下屏幕截图中的授权显示了auth代码，使您可以部署 VM -50和 VM -500中的每个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。

© 2019 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 和序列号的格式包括有关 VM 系列防火墙的每个实例的管理程序和许可证类型的信息。

- 借助 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在 AWS 和 Azure 中注册 VM 系列防火墙的基于使用情况的模型（无认证代码）。
- 有了 BYOL 模型，您必须在客户支持门户 (CSP) 上注册 VM 系列防火墙（使用授权代码）。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并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**:1234567890abcdef0:6kxdw3bbmdeda3o6i1ggqt4km:us-west1

© 2019 Palo Alto Networks, Inc.

创建支持帐户

如需访问软件更新、获取技术支持或借助 Palo Alto Networks 技术支持打开案例，则您需要配备支持帐户。

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。此外，支持帐户还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、订阅等等。

如果已有支持帐户，请继续注册 VM 系列防火墙。

STEP 1 | 转到 https://www.paloaltonetworks.com/support/tabs/overview.html。

STEP 2 | 单击 **Register**（注册）链接（页面底部），并输入公司电子邮件地址，以关联支持帐户。

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。

© 2019 Palo Alto Networks, Inc.

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，其中包含有一个 VM 系列容量许可证授权代码、支持授权代码（例如 PAN-SVC-PREM-VM-100 SKU）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。

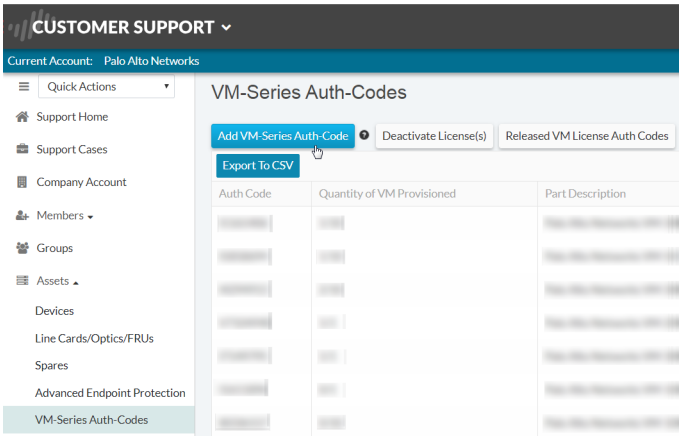
- 注册 VM 系列防火墙（使用授权代码）
- 面向公共云注册 VM 系列防火墙的基于使用情况的模式（无授权代码）。

注册 VM 系列防火墙（使用授权代码）

完成以下过程以使用身份验证码注册 VM 系列防火墙。

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 **Assests**（资产）> **VM-Series Auth-Codes**（**VM** 系列授权代码）> **Add VM-Series Auth-Code**（添加 **VM** 系列授权代码）。



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

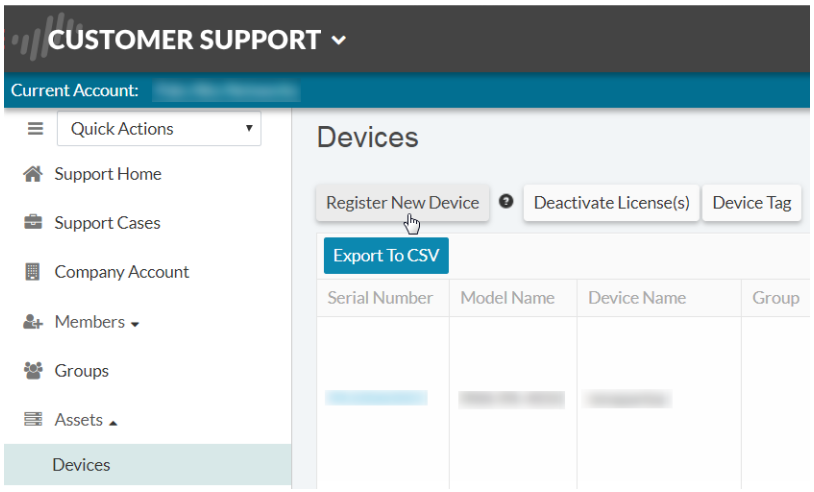
您可以跟踪已部署的 VM 系列防火墙的数量和仍可用于针对每个授权代码使用的许可证的数量。在使用所有可用许可证时，授权代码不会显示在 VM 系列授权代码页面上。要查看已部署的所有资产，请选择 **Assets**（资产）> **Devices**（设备）。

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）。

在开始注册过程之前，请登录到 VM 系列防火墙并从仪表盘记下序列号和 CPU ID（UUID 是可选的）。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 登录到 Palo Alto Networks 客户支持网站后，在 **Assets**（资产）选项卡上，单击 **Device**（设备）> **Register New Device**（注册新设备）。

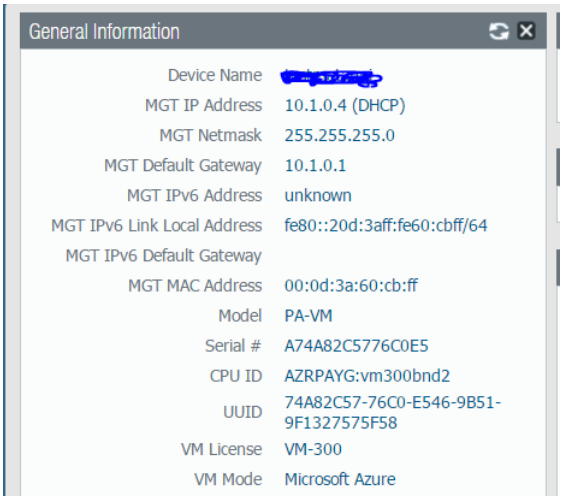


STEP 2 | 选择 **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace**（注册从公共云市场购买的基于使用情况的 **VM** 系列许可证模式）或云安全服务提供商 (CSSP)。

STEP 3 | 选择您的 **Cloud Marketplace**（云端市场）供应商并 **Submit**（提交）。

STEP 4 | 输入 VM 系列防火墙的 **Serial #**（序列号）、**CPU ID** 和 **UUID**。

例如，从 Azure 上的 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 5 | **Agree and Submit**（同意并提交）接受 EULA 并注册防火墙。

STEP 6 | 验证所购买许可证上的详情与支持门户 **Assets**（资产）页面上显示的详情是否一致。

© 2019 Palo Alto Networks, Inc.

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。

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。

© 2019 Palo Alto Networks, Inc.

在公共云上从旧版 PAYG 列表切换

从 PAN-OS 9.1.2 开始，公共云市场（AWS、Azure 和 GCP）上的 VM 系列即用即付 (PAYG) 产品可支持 VM-100、VM-300、VM-500 和 VM-700 型号。列表根据所选实例类型的资源可用性应用 VM 系列型号，以确保最佳利用可用资源。

尽管您可以继续使用从传统 PAYG 列表启动的（VM-300 的）实例，如果您要使用新列表启动新防火墙以便更好地优化资源，请按照以下说明在现有防火墙上保存和导出配置，并使用新 PAYG 列表部署新防火墙，然后在新防火墙上还原配置。

即使在将 *PAN-OS* 升级到 *9.1.2* 或更高版本后，使用传统 *PAYG* 列表启动的实例也仅限于 *VM-300* 型号。要选择其他支持的型号，您必须使用当前 *PAYG* 列表启动实例。

如果您使用 *AWS* 上的传统 *PAYG* 列表进行年度订阅，则在订阅期结束时该列表将转换为每小时订阅。要使用年度订阅选项，您必须使用当前 *PAYG* 列表，并且不能续订传统 *PAYG* 列表。

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。

STEP 2 | 使用当前 PAYG 列表部署新防火墙并进行注册。

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。

   需要 VM 系列插件 1.0.11 或更高版本。
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）。

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。

STEP 4 | 更新云平台上的所有路由表条目，以将流量指向新部署的防火墙。

© 2019 Palo Alto Networks, Inc.

切换 VM 系列许可证

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。您可以从 Panorama 同时在单个防火墙或多个防火墙上切换许可证。完成以下过程之一以执行以下许可证更改之一：

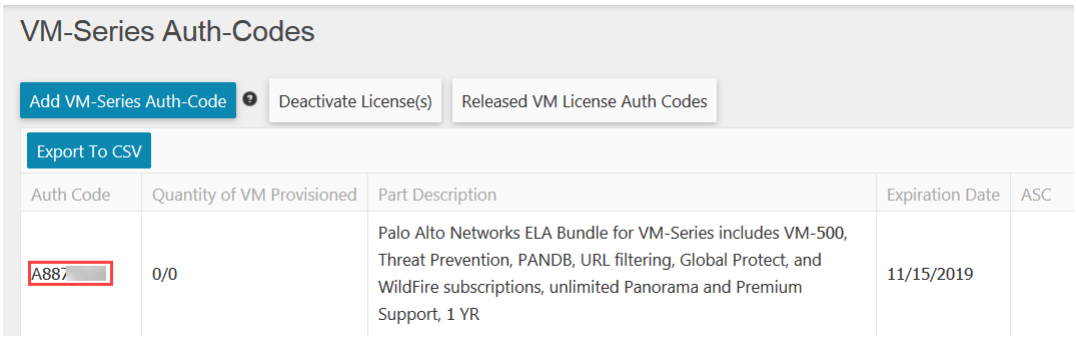
- 订阅套餐 1 到订阅套餐 2
- 订阅套餐 1 或 2 到 ELA
- 订阅套餐或 ELA 的容量许可

不要使用此程序在 *PAYG* 和 *BYOL* 之间切换。有关详细信息，请参阅在 BYOL 和 PAYG 许可证之间切换。

在切换到 ELA 许可证之前，必须分配等于当前部署的 VM 系列防火墙数量的足够令牌。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，激活 ELA 授权代码。

     请勿使用 *ELA* 授权代码激活单个 *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* 系列身份验证代码）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。

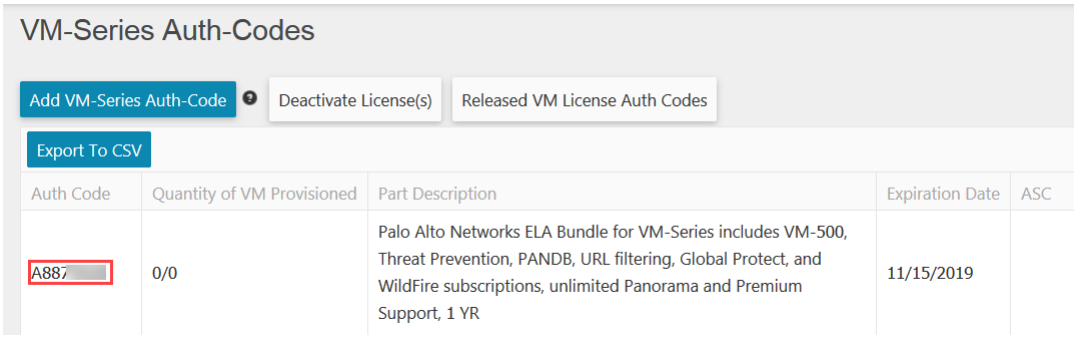
     1. 请选择 **Device**（设备）> **Licenses**（许可证），然后选择 **Activate feature using authorization code**（使用授权代码激活功能）链接。
     2. 输入 VM 系列授权代码。
     3. 单击 **OK**（确定）以确认许可证升级。防火墙与 Palo Alto Networks 更新服务器联系，并根据 VM 系列型号使用防火墙所需的令牌。
     4. 通过检查许可证到期日期验证许可证是否已成功更新。
  5. 为部署中的每个 VM 系列防火墙重复此步骤。

- 使用 Panorama 在受管防火墙上切换许可证。

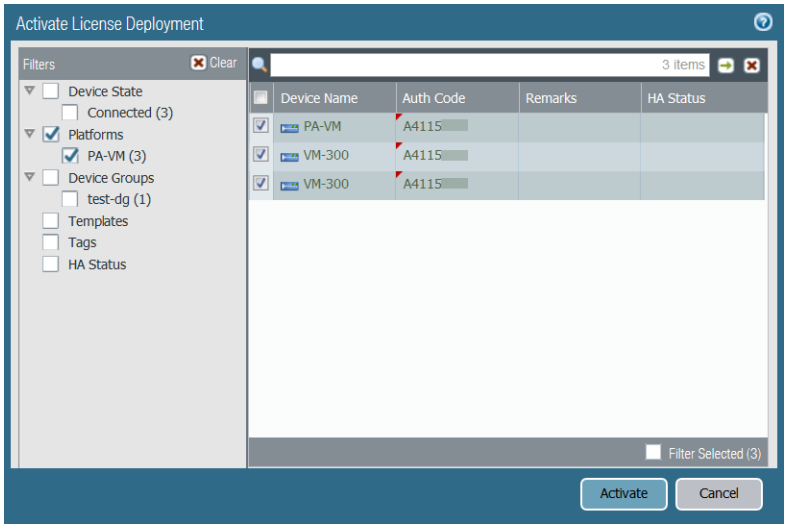
© 2019 Palo Alto Networks, Inc.

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

   请勿使用 *ELA* 授权代码激活单个 *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* 系列身份验证代码）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**（身份验证代码）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。



   6. 通过检查许可证到期日期验证许可证是否已成功更新。

© 2019 Palo Alto Networks, Inc.

更新 VM 系列防火墙许可证包

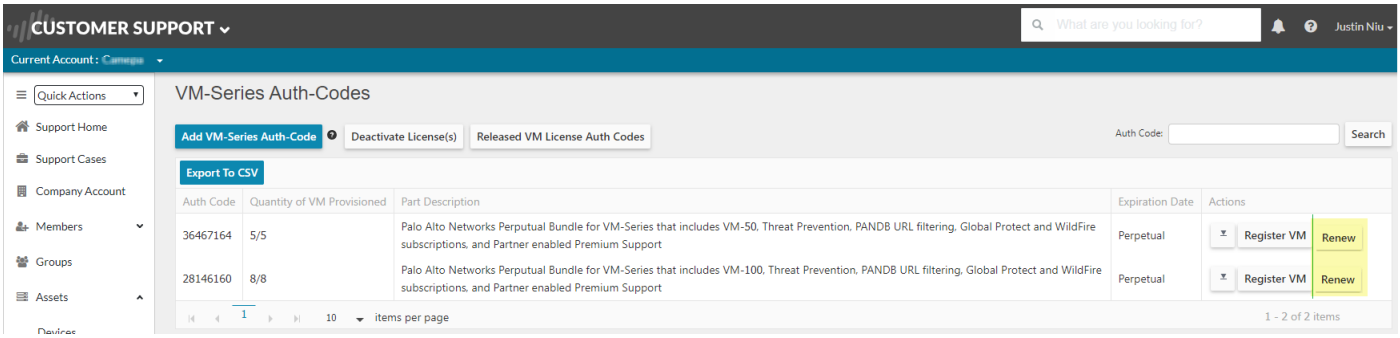
当 VM 系列防火墙包许可证需要更新时，可以登陆到 Palo Alto Networks 客户支持门户，并调整许可证数量以满足您的部署需求。更新时，可以查看您的使用趋势，并根据您未来的需求，从下列选项进行选择：

- **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。

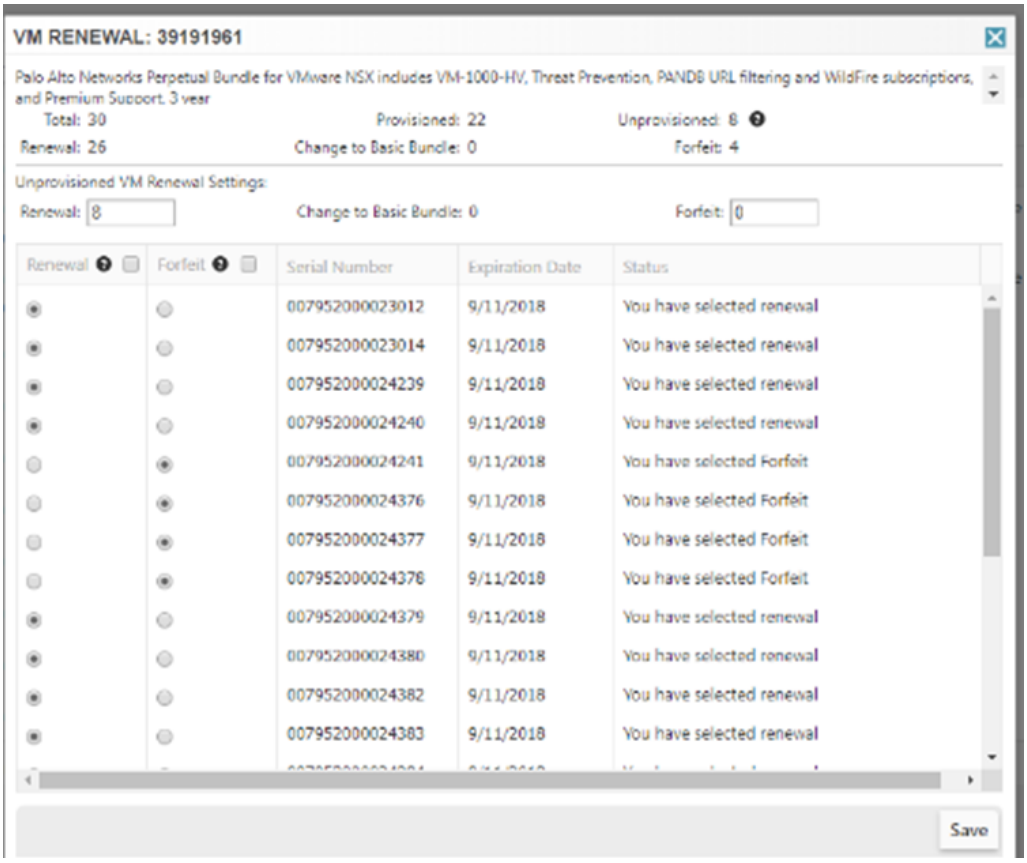
Renew（更新）选项显示适用于更新的授权代码。



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。如果您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。

© 2019 Palo Alto Networks, Inc.



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。

© 2019 Palo Alto Networks, Inc.

激活许可证

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。

- 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。

- 如果您的 VM 系列防火墙拥有直接 Internet 访问权。

  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。

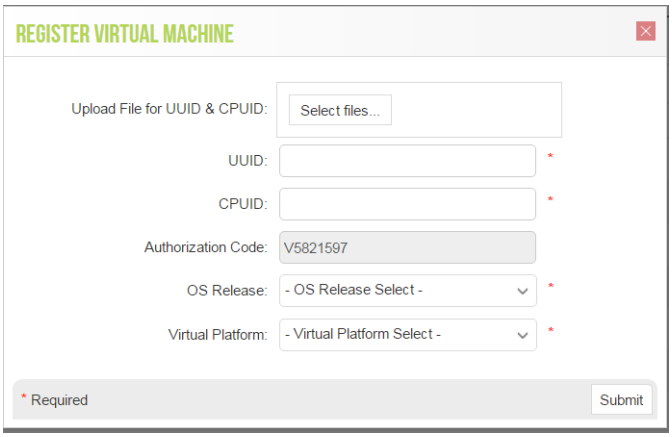
  1. 请选择 **Device**（设备）> **Licenses**（许可证），然后选择 **Activate feature using authorization code**（使用身份验证代码激活功能）链接。
  2. 输入在支持门户上注册的容量授权代码。防火墙将连接到更新服务器 (updates.paloaltonetworks.com)，并下载许可证，然后自动重新启动。
  3. 重新登录到 Web 界面，并确认 **Dashboard**（仪表盘）显示有效的序列号。如果显示**Unknown**（未知）一词，则表示此设备未经许可。
  4. 在 **Device**（设备）> **Licenses**（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。

- 如果您的 VM 系列防火墙没有 Internet 访问权。

© 2019 Palo Alto Networks, Inc.

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 版本和管理程序，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。有关为 NSX 部署 VM 系列防火墙的组件和要求的概述，请参阅 VM 系列NSX防火墙概述。

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。

© 2019 Palo Alto Networks, Inc.

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* 群集最多可以包括 *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

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**（受管设备），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**。

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），并单击 **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 并单击 **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）并搜索该序列号。
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。除了订阅许可证密钥之外，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），并选择 **Manually upload license key**（手上上传许可证密钥）。
3. 单击 **Browse**（浏览）选择一个密钥，并单击 **OK**（确定）在防火墙上安装许可证。

© 2019 Palo Alto Networks, Inc.

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* 上的受管设备。

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）。

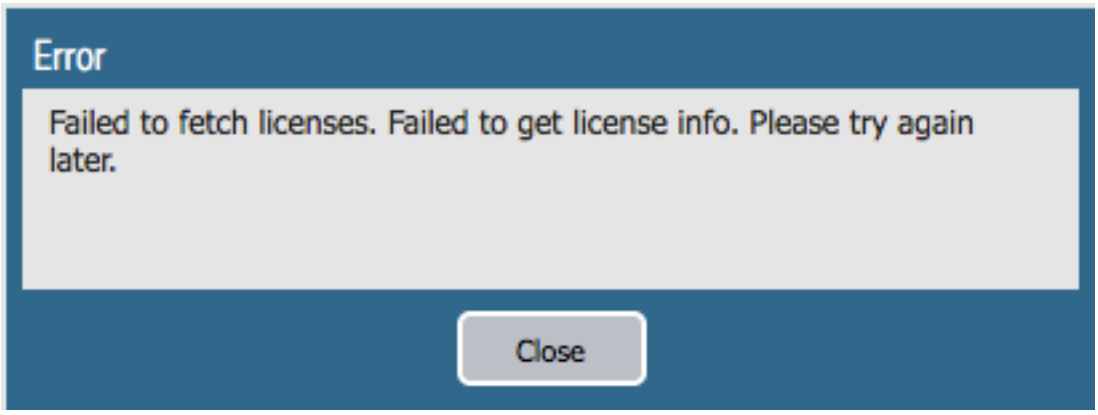
STEP 4 | 添加 Panorama 上防火墙的序列号。

选择 **Panorama** > **Managed Devices**（受管设备），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

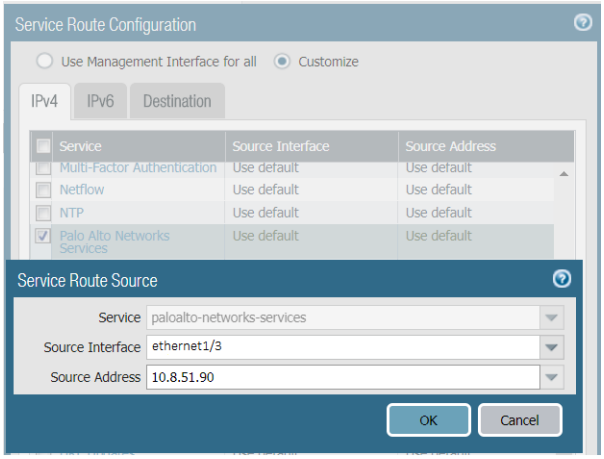
本部分介绍了激活许可证的一些最常见问题。

- 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。



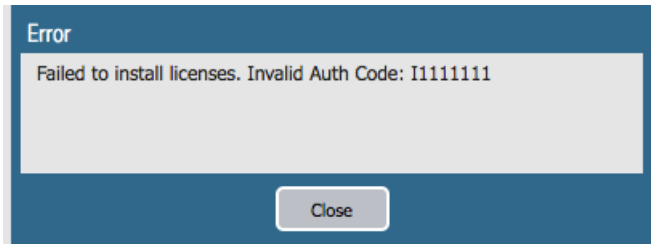
- 路由通过 Internet 工作？SSH 进入防火墙并 Ping 一个可公开访问的 IP 地址，如 4.2.2.2。如果您正在使用数据面界面，请务必使用源选项。例如：ping count 3 source 10.0.1.1 host 4.2.2.2.
- DNS 设置正确吗？SSH 进入防火墙并 Ping一个 DNS 名称，如 google.com。例如：

© 2019 Palo Alto Networks, Inc.

```
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

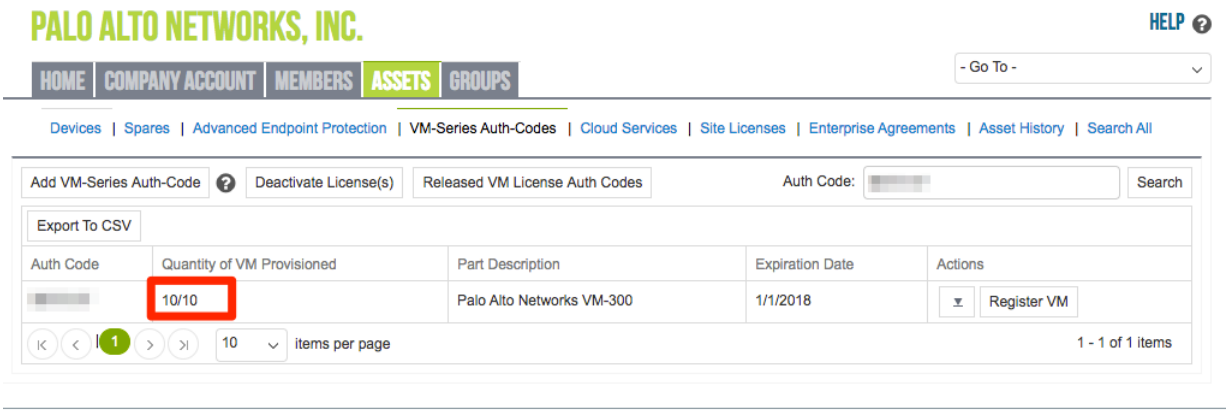
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 11.586/11.721/11.975/0.200 ms
```

- 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。



© 2019 Palo Alto Networks, Inc.

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。

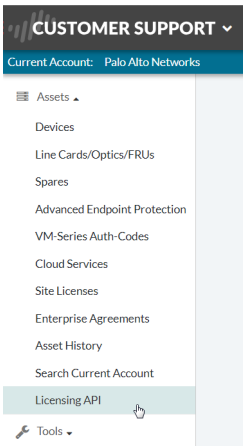
- 安装许可证停用API密钥
- 使用 CLI 停用功能许可证或订阅
- 停用 VM

安装许可证停用API密钥

从客户支持门户中检索您的许可证 API 密钥，并使用 CLI 在防火墙和 Panorama 上进行安装。您必须在防火墙或 Panorama 上拥有超级用户权限才能安装许可证 API 密钥。在 Panorama 上安装许可证 API 密钥时，Panorama 会将 API 密钥推送到其受管设备。如果受管设备已安装 API 密钥，则 Panorama 会使用新密钥覆盖旧的 API 密钥。

STEP 1 | 从客户支持门户检索许可证停用 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。

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

STEP 3 | 安装许可证停用 API 密钥后，请按正常方式停用 VM。

停用 VM 系列许可证需要重新启动软件。

STEP 4 | 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。

© 2019 Palo Alto Networks, Inc.

request license api-key delete

要在删除 API 密钥后停用 VM 系列防火墙，您必须安装新的 API 密钥。

使用 CLI 停用功能许可证或订阅

如果您无意中在防火墙上安装了许可证/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验证代码，而无需技术支持部门提供协助。仅在 CLI 上支持此功能；基于硬件的防火墙和 VM 系列防火墙上均支持此流程。

STEP 1 | 在防火墙上登录到 CLI。

STEP 2 | （仅限直接 Internet 访问）查看需停用功能的许可证密钥文件的名称。

request license deactivate key features ?

STEP 3 | （只能直接上网）停用许可或订阅。

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

其中，名称为许可证密钥文件的全名。

例如：

```
admin@vmPAN2> request license deactivate key features
 WildFire_License_2015_01_28_I5820573.key mode auto007200002599

WildFire License Success

Successfully removed license keys
```

STEP 4 | （没有直接 Internet 访问时）查看需停用功能的许可证密钥文件的名称。

request license deactivate key features

STEP 5 | （当没有直接的Internet访问）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
```

令牌文件所用格式为“*dact_lic.timestamp.tok*”，其中时间戳的格式为“*dmmyyyy.hrminsec*”。

STEP 6 | 验证是否已生成令牌文件。

show license-token-files

STEP 7 | 导出令牌文件至 SCP 或 TFTP 服务器，再将其保存至您的计算机。

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

© 2019 Palo Alto Networks, Inc.

例如：

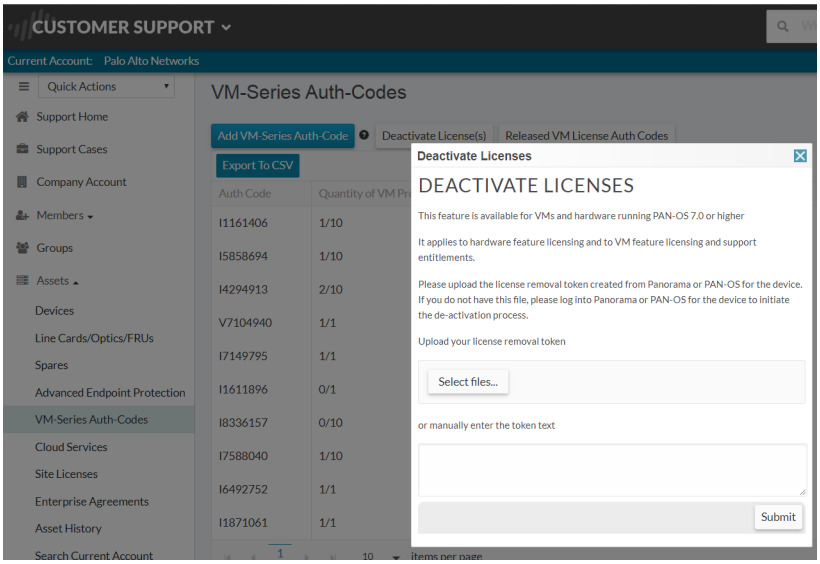
```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

STEP 8 | 登录到 Palo Alto Networks 客户支持网站。

STEP 9 | 在 **Assets**（资产）选项卡上单击 **Deactivate License(s)**（停用许可证）链接。

STEP 10 | 选择 **Assets**（资产） > **VM-Series Auth-Codes**（**VM** 系列授权代码） > **Deactivate License(s)**（停用许可证）.

STEP 11 | 登录到 Palo Alto Networks 客户支持网站后，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，您可以使用防火墙或 Panorama 上的 Web 界面、CLI 或 XML API 释放所有的活动许可证，如订阅许可、VM 容量许可和支持授权等。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。

在删除 *VM* 系列防火墙前，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：

- 如果设备由 *Panorama* 管理，您可以通过 *Panorama* 停用许可证。
- 如果设备并非由 *Panorama* 管理，则必须联系 Palo Alto Networks 客户支持。

- 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。

© 2019 Palo Alto Networks, Inc.

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

STEP 2 | 在许可证管理部分，选择 **Deactivate VM**（停用 VM）。

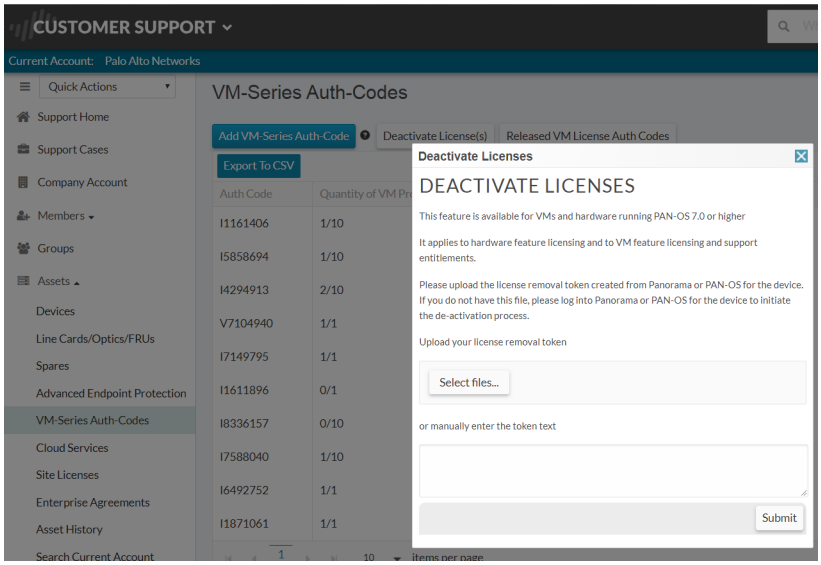
STEP 3 | 验证在防火墙上停用的许可证/授权列表。

STEP 4 | 选择以下任一选项开始停用 VM：

- 如果防火墙能直接与 Palo Alto Networks 许可服务器进行通信，单击 **Continue**（继续）。此时会提示您重启防火墙，重启后，许可证将会被停用。
- 如果 VM 系列防火墙无法访问 Internet，请单击 **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。例如，令牌文件可命名为 20150128_1307_dact_lic.01282015.130737.tok。此时会提示您重启防火墙，重启后，许可证将会被停用。

STEP 5 | （仅适用于手动流程）如需在许可服务器上注册更改，需完成以下任务：

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。



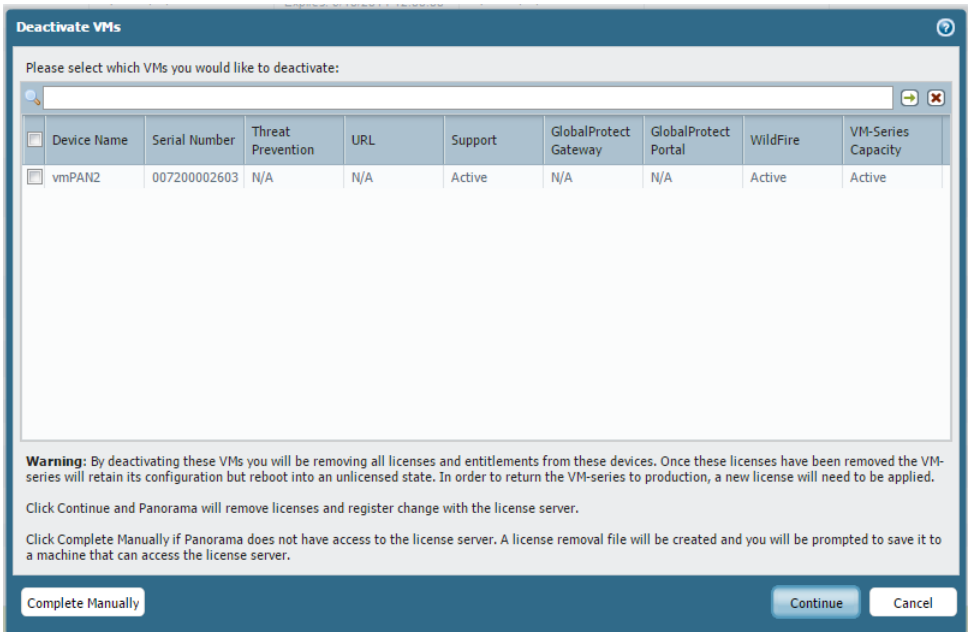
从 *Panorama* 停用 *VM*

完成以下过程以便从 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）。

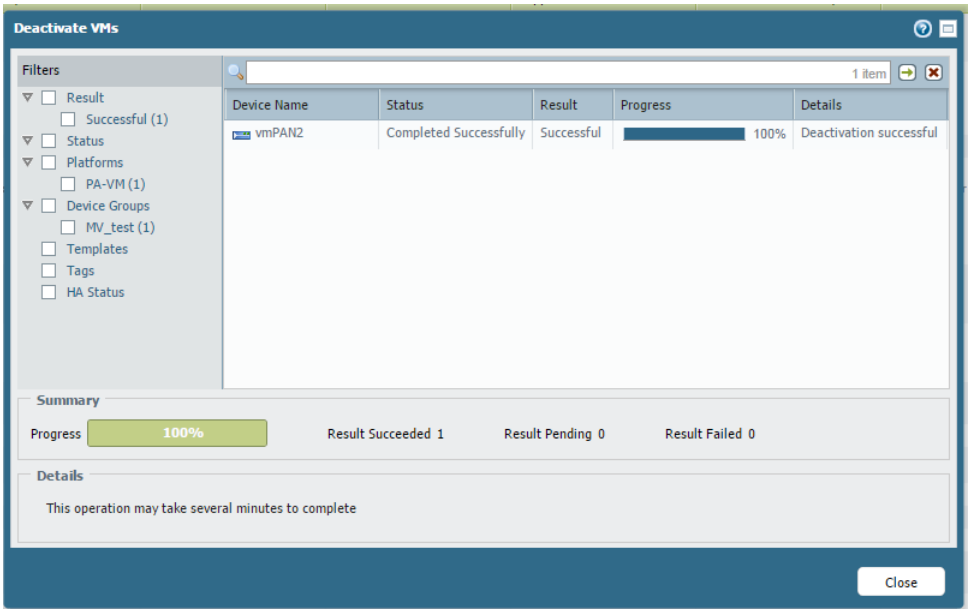
STEP 2 | 单击 **Deactivate VMs**（停用 **VM**），选择您想要停用的 VM 系列防火墙。

© 2019 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）。如需验证是否已在防火墙上停用许可证，请依次单击 **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。Panorama 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。屏幕上将显示“成功完成”消息，随即防火墙将自动重启。



STEP 4 | （仅限手动流程）如需使用令牌文件通过许可服务器注册更改，请参阅上述此步骤。

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

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

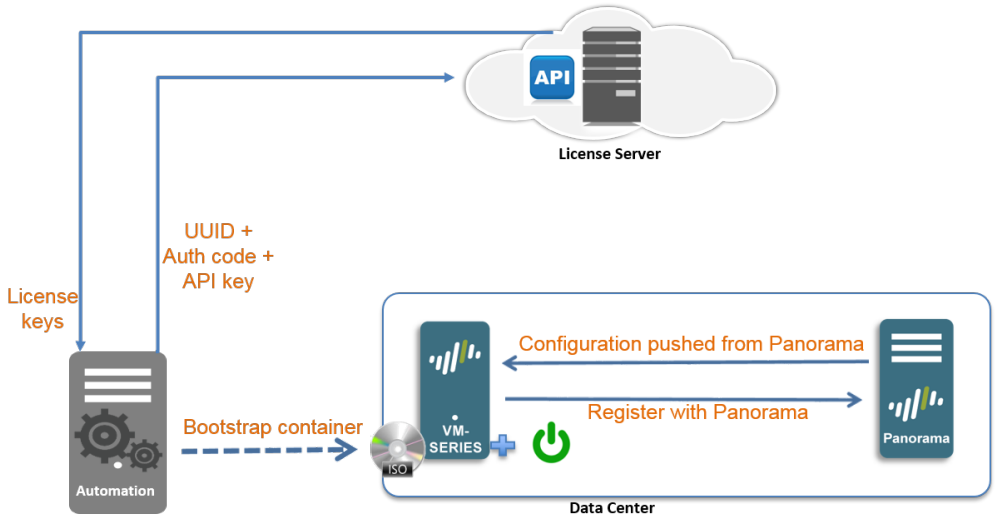
© 2019 Palo Alto Networks, Inc.

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。

© 2019 Palo Alto Networks, Inc.

授权 API 许可证

为了确保成功许可未直接连接到 Internet 的许可证防火墙，Palo Alto Networks 会提供一个许可证 API。您可以使用该带有自定义脚本或协调服务的 API 注册授权代码、检索与授权代码相关的许可证、续订许可证，或停用 VM 系列防火墙上的所有许可证（停用 VM）。



通过该 API，您还可以查看授权代码的详情，以便跟踪与某个授权代码或授权代码包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。认证后，许可证服务器将会以 json 的格式（内容类型 应用程序/json）发送响应。

- 管理许可证 API 密钥
- 使用许可证 API
- 许可证 API 错误代码

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。

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。

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. 从 —**Go To**—（—转到—）下拉列表中选择 **Licensing API**（许可 **API**）。
3. 单击 **Enable**（启用）以查看您的密钥，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。如果您怀疑某个 API 密钥可能出现损坏，则可以生成一个新密钥，之后旧密钥将自动失效。

© 2019 Palo Alto Networks, Inc.

- 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，获取许可证 API 密钥。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

URL：**`https://api.paloaltonetworks.com/api/license/activate`**

参数： uuid、cpuid、authCode 和 serialNumber。

使用上述参数完成以下步骤：

- 在初次或初始许可证激活时，需在 API 请求中提供 cpuid、uuid 和授权代码。
- 如果在初始许可证激活过程中，您没有保存许可证密钥或出现网络连接问题，因此需要再次检索之前已激活防火墙的许可证，则可以在 API 请求中提供 cpuid 和 uuid，或者在 API 请求中提供防火墙的序列号。

标题：apikey

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":"2016-06-03T
 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
```


© 2019 Palo Alto Networks, Inc.

```
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03T
 12:00:00 AM","PropertyChanged":null}
...<truncated>
```


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。由于密钥采用的是 *json* 格式，因此没有换行符；如果您的分析程序需要，则必须将其转化为换行符格式。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":"2016-06-03T
 "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":"2016-06-03T
 12:00:00 AM","PropertyChanged":null}
```


...<truncated>

停用许可证

URL：**`https://api.paloaltonetworks.com/api/license/deactivate`**

参数：加密令牌

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 要么 使用CLI停用功能许可或订阅。

标题：apikey

请求：https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>

© 2019 Palo Alto Networks, Inc.

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":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"","successFiel
```

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
- 401 API 密钥无效
- 500 服务器错误

© 2019 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 身份验证代码注册 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，您会收到一封包含身份验证代码的电子邮件；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身份验证代码代码。

在部署防火墙时，您必须针对身份验证代码注册防火墙的每个实例。

使用 CSSP 身份验证代码注册 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：

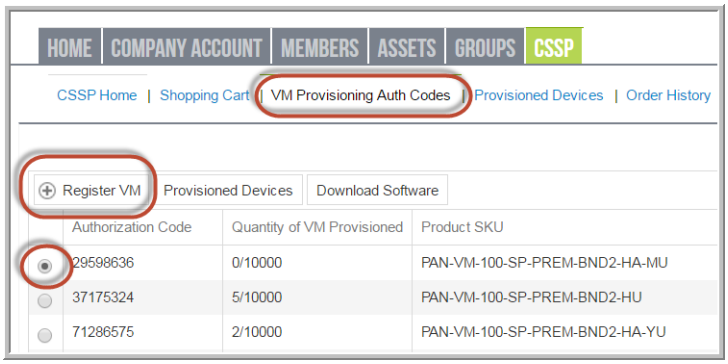
- API —使用许可 API，如果您有自定义脚本或编排服务。凭借此选项，防火墙不需要直接访问 Internet。
- 引导程序 - 使用此选项可以自动配置防火墙并在首次引导时对其进行许可。参阅引导 VM 系列防火墙。
- 防火墙 Web 界面 — 您可以使用防火墙 Web 界面激活 VM 系列防火墙的许可证（独立版本）。此工作流程适用于带或不带Internet访问的防火墙。
- 客户支持门户 — 使用此选项在Palo Alto Networks客户支持门户上手动注册防火墙，如下所示。

© 2019 Palo Alto Networks, Inc.

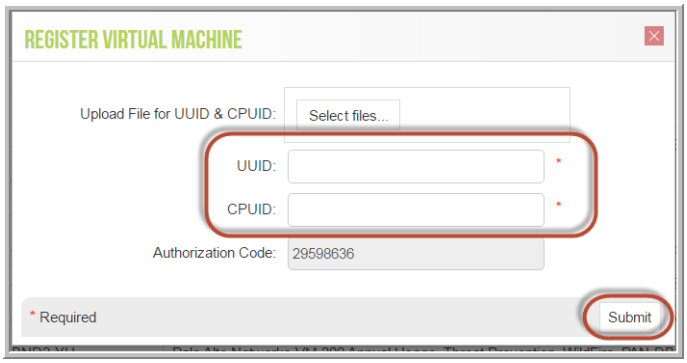
STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。如果需要新帐户，请参阅创建支持帐户。

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身份验证代码代码。

STEP 3 | 选择 **CSSP** > **VM Provisioning Auth Codes**（VM 预配置身份验证代码），选择一个 **Authorization Code**（授权代码）并单击 **Register VM**（注册 VM）。



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* 预配置身份验证代码），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）

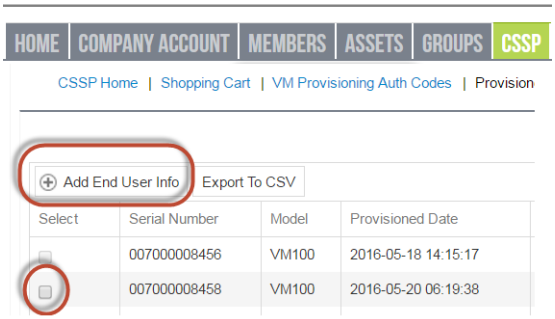
通过客户支持门户完成以下过程，为已注册的防火墙添加最终用户信息。

STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持网站。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 选择 **CSSP** > **Provisioned Devices**（配置的设备）。

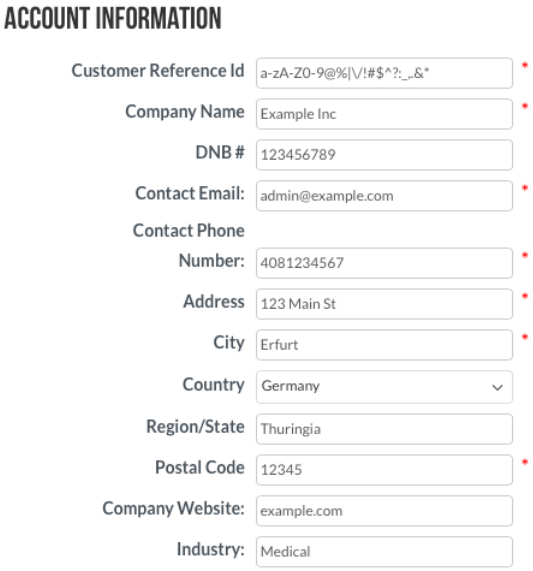
STEP 3 | 选择 **Serial Number**（序列号）并单击 **Add End User Info**（添加最终用户信息）。



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。

© 2019 Palo Alto Networks, Inc.

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。

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": "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。

© 2019 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。有关详细信息，请参阅文章：《VM 系列数据中心自动化》。

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
- 在 ESXi 服务器上设置 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，因此该防火墙可监视和控制离开 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。防火墙可以监视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。

© 2019 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 系统上的 VM 系列要求
- ESXi 系统上 VM 系列的限制

ESXi 系统上的 VM 系列要求

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。
- 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。

  管理程序分配的 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。如果禁用管理程序分配的 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，也未启用管理程序分配的 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。
- 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管理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。

© 2019 Palo Alto Networks, Inc.

- 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。
- 不支持 VM 系列防火墙的 vMotion。不过，VM 系列防火墙可确保已迁移至新目标主机的客户端虚拟机的安全，前提是源主机和目标主机均为来宾虚拟机为实现网络连接所用的全部 vSphere 分布式交换机的成员。
- 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。

© 2019 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

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)
8	Ethernet 1/7 (eth7)
9	Ethernet 1/8 (eth8)
10	Ethernet 1/9 (eth9)

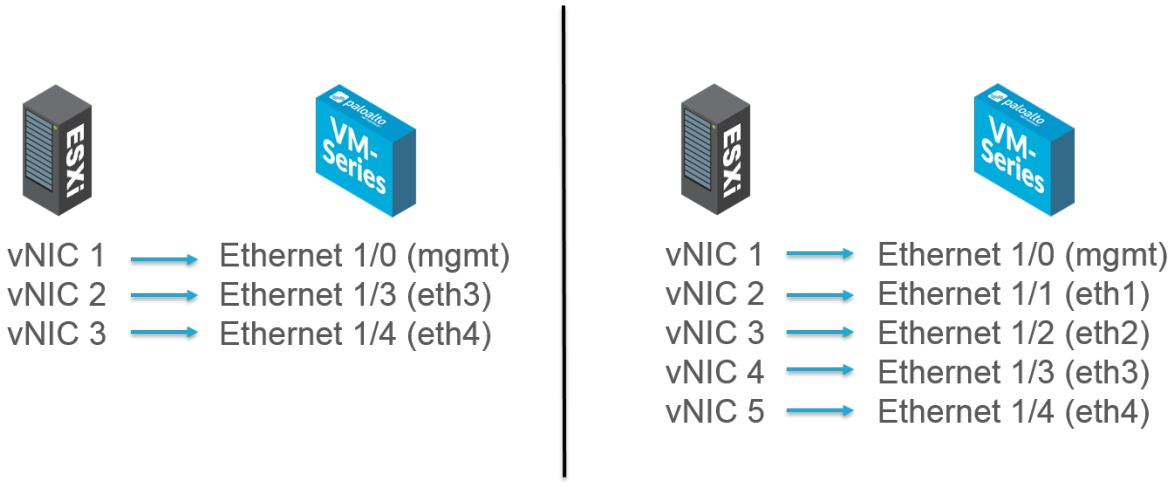
无论您在ESXi上添加哪个vNIC， VM 系列防火墙上的映射都保持不变。您在防火墙上激活的接口将始终占用 ESXi 上的下一个可用 vNIC。

© 2019 Palo Alto Networks, Inc.

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 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 上设置 VM 系列防火墙。

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。如果选择禁用管理程序分配的 *MAC* 地址，或是如果真通过第二层、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。

© 2019 Palo Alto Networks, Inc.

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

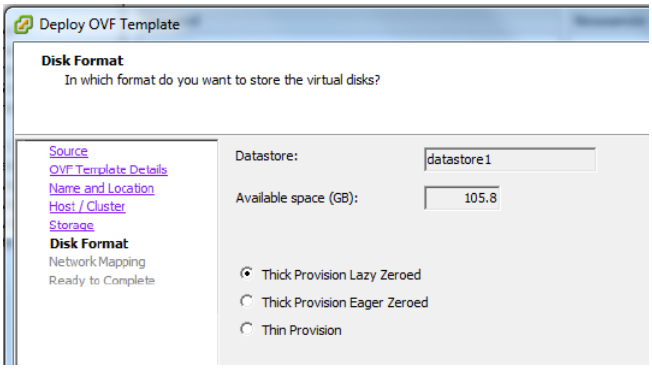
1. 选择 **Home**（主页）> **Networking**（网络）。选择分布式虚拟交换机，并突出显示想要编辑的 **Distributed Port Group**（分布式端口组）。
2. 单击 **Edit Settings**（编辑设置），选择 **Policies**（策略）> **Security**（安全），然后将 **Promiscuous Mode**（混杂模式）、**MAC Address Changes**（MAC 地址更改）和 **Forged Transmits**（伪造传输）设置为 **Accept**（接受），并单击 **OK**（确定）。

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。

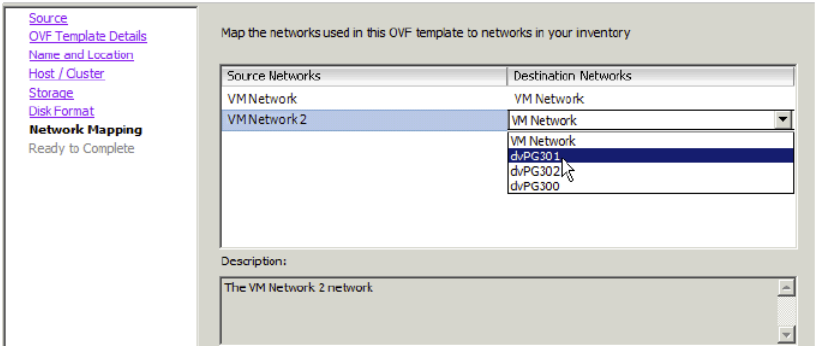
要查看安装进度，请监控 *Recent Tasks*（最近的任务）列表。

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. 浏览找到在1中下载的 OVA 文件，选定该文件，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**。

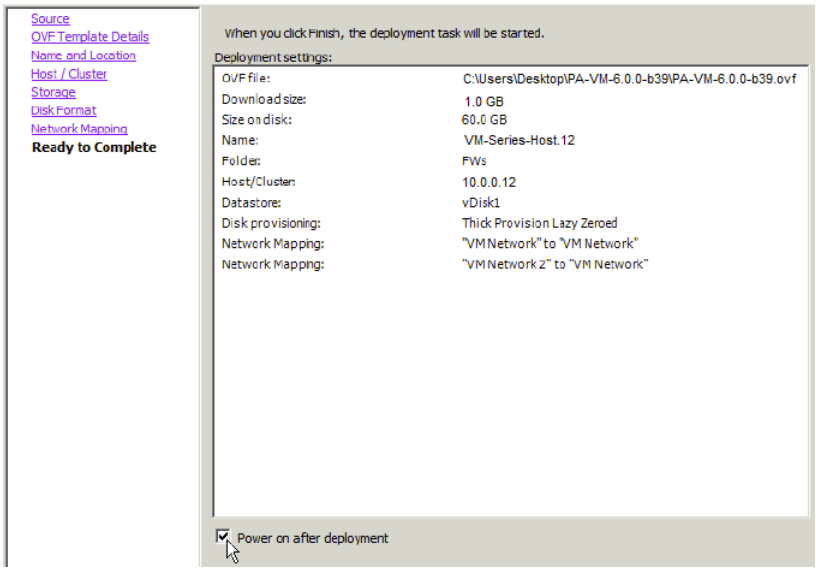


8. 选择用于两个初始 vNIC 的网络。第一个 vNIC 用于管理接口，第二个 vNIC 用于首个数据端口。请确保 **Source Networks**（源网络）映射到正确的 **Destination Networks**（目标网络）。

© 2019 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)。

© 2019 Palo Alto Networks, Inc.

4. 输入 **configure**（配置）以切换到“Configuration（配置）”模式。

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> netmask <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 40GB 的虚拟磁盘，其中 17GB 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视网络上的所有通信。Panorama 提供集中式日志记录和报告。
- 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 40GB-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。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 在 ESXi 服务器上，将虚拟磁盘添加至防火墙。

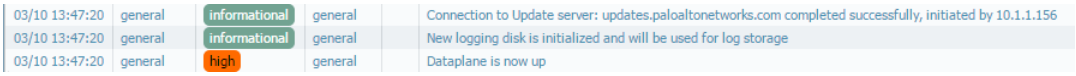
1. 在 ESXi 服务器上选择 VM 系列防火墙。
2. 单击 **Edit Settings**（编辑设置）。
3. 单击 **Add**（添加）启动“添加硬件”向导，并在弹出时选择以下选项：
    1. 对于硬件类型，请选择 **Hard Disk**（硬盘）。
    2. 选择 **Create a new virtual disk**（新建虚拟磁盘）。
    3. 选择 **SCSI** 作为虚拟磁盘类型。
    4. 选择 **Thick provisioning**（密集配置）磁盘格式。
    5. 在位置字段中，选择 **Store with the virtual machine 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。

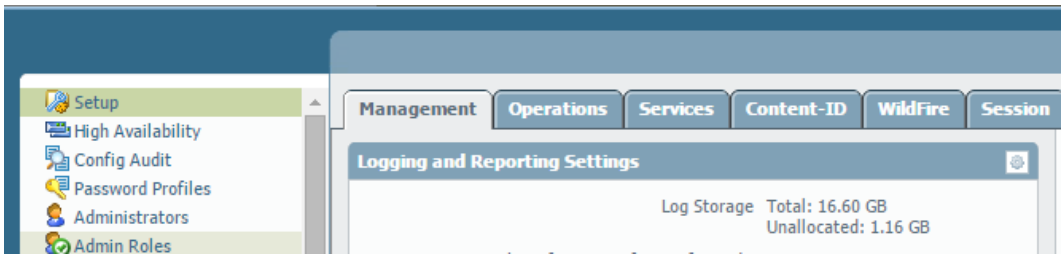
PAN-OS 还会生成记录新磁盘的系统日志条目。



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。



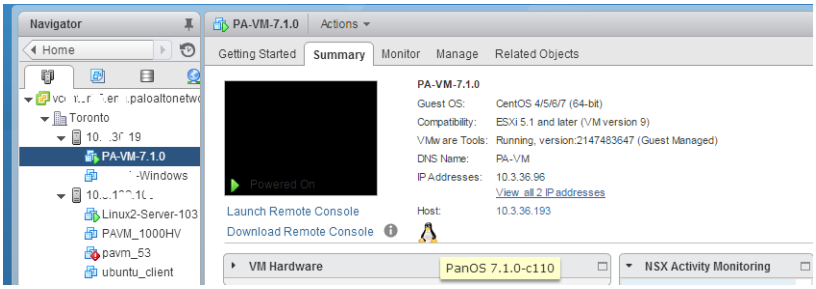
通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具

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。

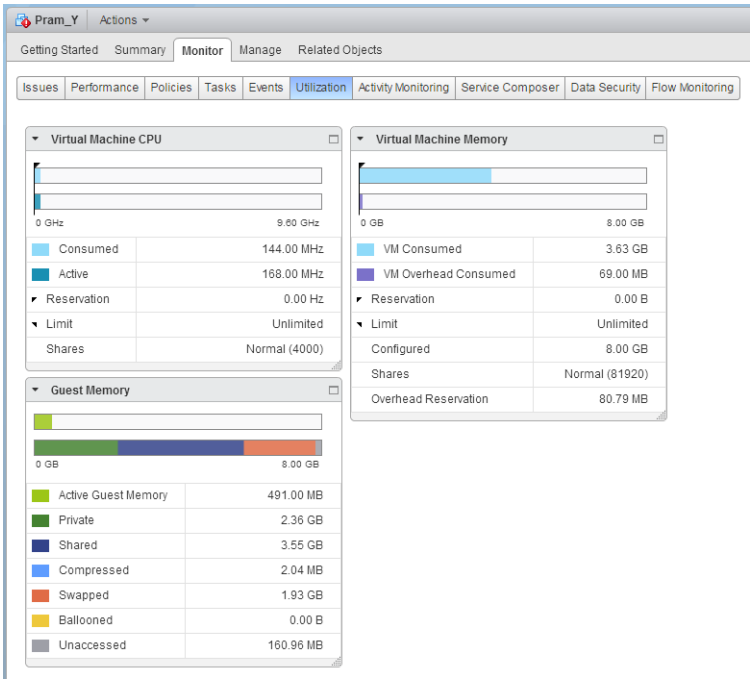
  在 vCenter 服务器上的“Hosts and Cluster（主机和集群）”部分，选择防火墙或 Panorama 并在 **Summary**（摘要）选项卡上查看分配至管理接口的 IP 地址以及当前所安装的软件版本的信息。

© 2019 Palo Alto Networks, Inc.



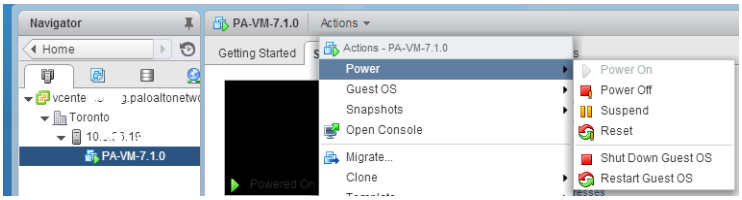
- 查看硬盘、内存和 CPU 的资源利用指标。使用这些指标启用 vCenter 服务器上的警报。

  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。



- 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。



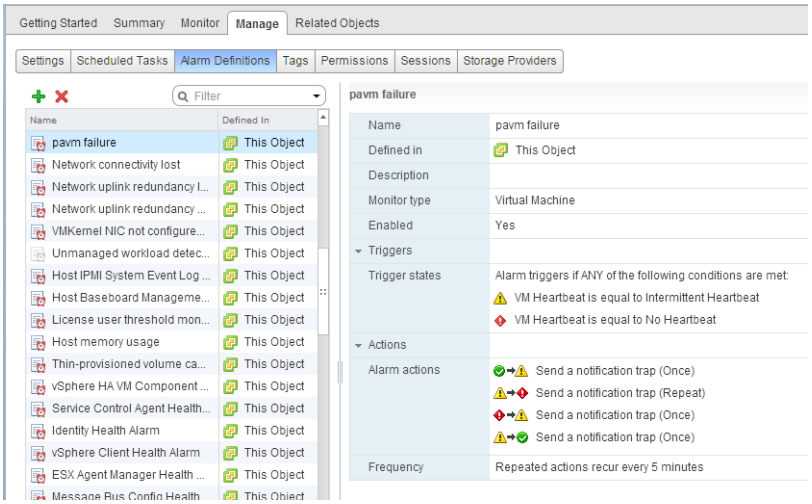
- 创建您希望获得通知的事件的警报定义，或创建您希望为其指定自动操作的事件的警报定义。

  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

© 2019 Palo Alto Networks, Inc.

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。



© 2019 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 VM ware 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

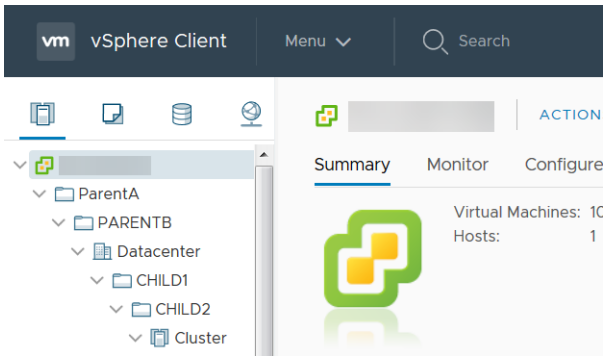
关于 VM ware vCenter上的 VM 监控

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 插件监视 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>** — 此标记基于 VM 名称映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_guestos.<guest-os>** — 此标记基于来宾操作系统映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_annotation.<annotation>** — 此标记基于注释映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vlanId.<vlan-ID>** — 此标记基于 VLAN ID 映射虚拟机 IP 地址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_host-ip.<host-ip>** — 此标记基于主机 IP 地址映射虚拟机 IP 地址。

© 2019 Palo Alto Networks, Inc.

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_<tag-category>.<user-defined-tag>** — 此标记基于用户在 vCenter 中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

要开始监视 vCenter 上的端点，请下载并安装适用于 VMware vCenter 的 Panorama 插件。

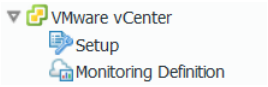
如果拥有 Panorama HA 配置，则在每个 Panorama 对等设备上重复此安装过程。在 HA 对中的 Panorama 上安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

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"操作"列中单击 **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

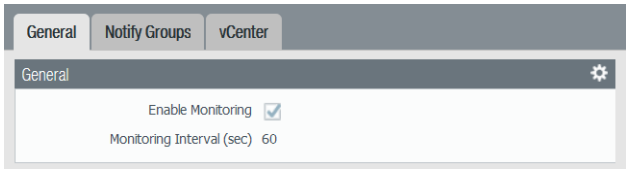
安装插件后，请完成以下过程以在 Panorama 和 vCenter 之间建立连接。

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。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 启用监控并设置监控间隔。

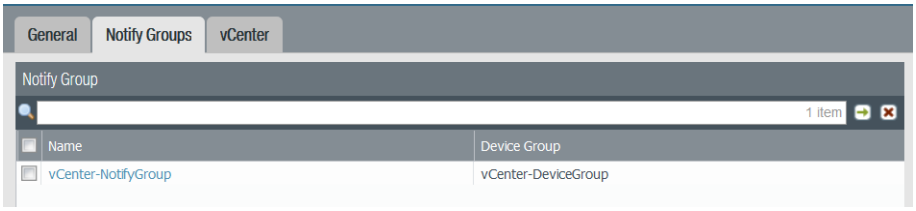
1. 选择 **Panorama** > **VMware vCenter** > **Setup**（设置）> **General**（常规）。
2. 选择 **Enable Monitoring**（启用监控）。这样即可监视部署中的所有 vCenter。
3. 以秒为单位设置 **Monitoring Interval**（监控间隔）。监视时间间隔是 Panorama 从 vCenter 检索更新的网络信息的频率。默认值为 60 秒，范围为 60 至 84600 秒。



© 2019 Palo Alto Networks, Inc.

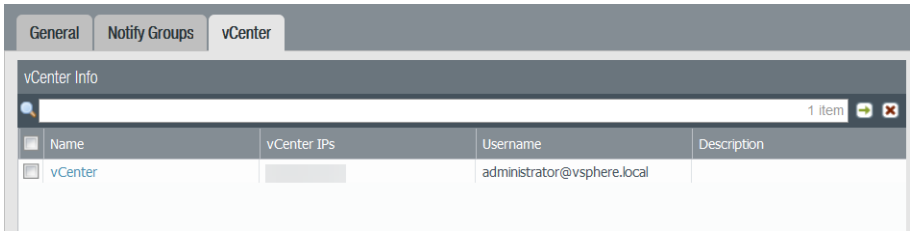
STEP 3 | 创建通知组。

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。



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。

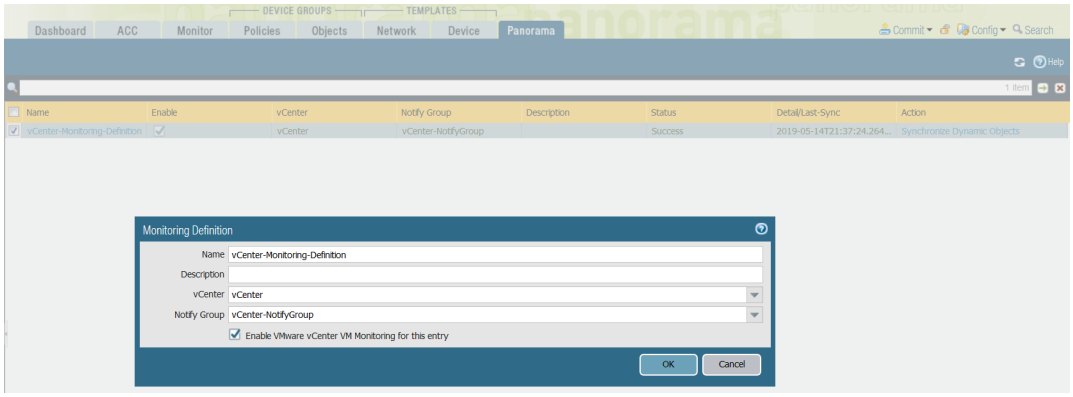
1. 选择 **Panorama** > **VMware vCenter** > **Setup**（设置） > **vCenter**。
2. 输入 vCenter 的描述性 **Name**（名称）。
3. 输入 vCenter 和端口的 IP 地址或 FQDN（如果适用）。
4. 输入 vCenter 用户名。
5. 输入并确认 vCenter 密码。
6. 单击 **Validate**（验证）以确认 Panorama 可以使用您输入的登录凭据连接到 vCenter。
7. 单击 **OK**（确定）。



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）并单击 **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）。



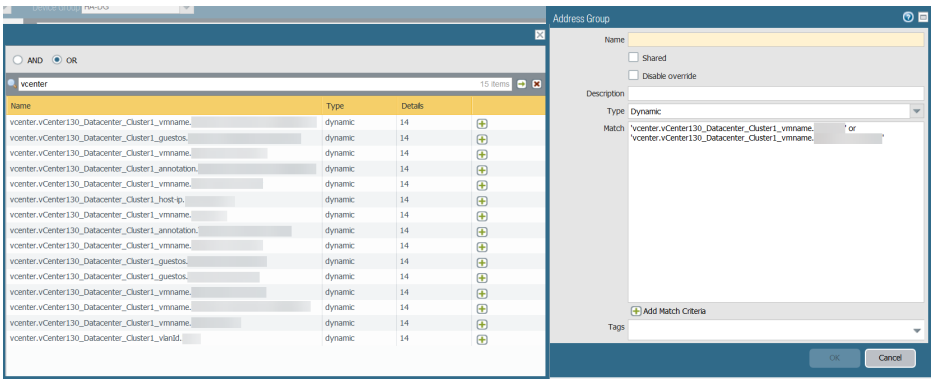
© 2019 Palo Alto Networks, Inc.

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。



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
```


© 2019 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，然后监视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。
- 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，则 OVA 部署可能会耗费数小时，或超时并且失败。

    如果将映像托管在与 ESXi 主机相同的网络中的设备上，则可以减少此问题。
  - 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。

© 2019 Palo Alto Networks, Inc.

- 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 5120（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>
        <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>
```


© 2019 Palo Alto Networks, Inc.

```
        <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：

```
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

© 2019 Palo Alto Networks, Inc.

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，而如未启用管理程序分配的 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

© 2019 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，但可能需要调整管理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
- 在 ESXi 上启用 NIC 的多队列支持

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
```


© 2019 Palo Alto Networks, Inc.

```
    Supported Ports: FIBRE
    Supports Auto Negotiation: true
    Supports Pause: true
    Supports Wakeon: false
    Transceiver: external
    Wakeon: None
```

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。

所有数据接口必须使用相同的驱动程序支持 *DPDK*。

要利用 DPDK，必须使用具有以下驱动程序之一的 NIC：

支持的驱动程序	
虚拟驱动程序	VMXNET3
Intel 驱动程序	ixgbe、ixgbevf、i40e、i40evf

如果禁用 DPDK，则 NIC 使用数据包 mmap 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 管理程序支持和 SR-IOV 和 DPDK 驱动程序支持的兼容性矩阵。

© 2019 Palo Alto Networks, Inc.

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管理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 需要以下 Intel NIC 驱动程序之一：i40/i40e、i40evf、ixgbe 或 ixgbevf。请参阅 PAN-OS 版本的 SR-IOV 和 DPDK 驱动程序支持的兼容性矩阵。

完成以下步骤以启用 SR-IOV。

STEP 1 | 启用 SR-IOV NIC 上的虚拟功能 (VF)。max_vfs 是物理端口上允许的最大虚拟功能数。最大限制取决于 ESXi 主机、适配器和服务器配置支持的 VF 数。请参阅驱动程序文档。

1. 登录到 ESXi 主机 CLI。
2. 使用以下命令指定每个端口的 VF (max_vfs) 最大数。

```
$ esxcli system
module parameters set -m <nic_driver> -p “max_vfs=<n>”
```

如果您有使用相同驱动程序的多端口 NIC 或多个 NIC，则必须指定以逗号分隔的 max_vfs 值列表。您可以按照 PCI 总线上 NIC 端口的顺序列出数字，其中，每个数字对应于物理端口上启用的 VF 数。例如，对于 ixgbe，您可以指定：

```
$ esxcli
system module parameters set -m ixgbe -p "max_vfs=8,8,8"
```

3. 启用 VF 设备后，关闭所有 VM（包括 vCenter 服务器应用程序），并重启 ESXi 主机。

STEP 2 | 修改 vCenter 中的来宾设置。

1. 登录到 vCenter 并选择您的 VM 系列防火墙客户机。
2. 选择 **Manage**（管理）> **Settings**（设置）> **VM Hardware**（虚拟机硬件）和 **Edit**（编辑）硬件设置。
3. 选择 **Virtual Hardware**（虚拟硬件）。
4. 从**New device**（新设备）下拉菜单中选择 **PCI Device**（**PCI** 设备）并单击 **Add**（添加）。
5. 编辑添加的 PCI 设备的设置，选择对应于可用虚拟功能设备的 PCI ID。

STEP 3 | 重启 ESXi 主机，以使更改生效。

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：

© 2019 Palo Alto Networks, Inc.

```
$ 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"
```

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管理程序分配的 MAC 地址。如果您未启用管理程序分配的 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。

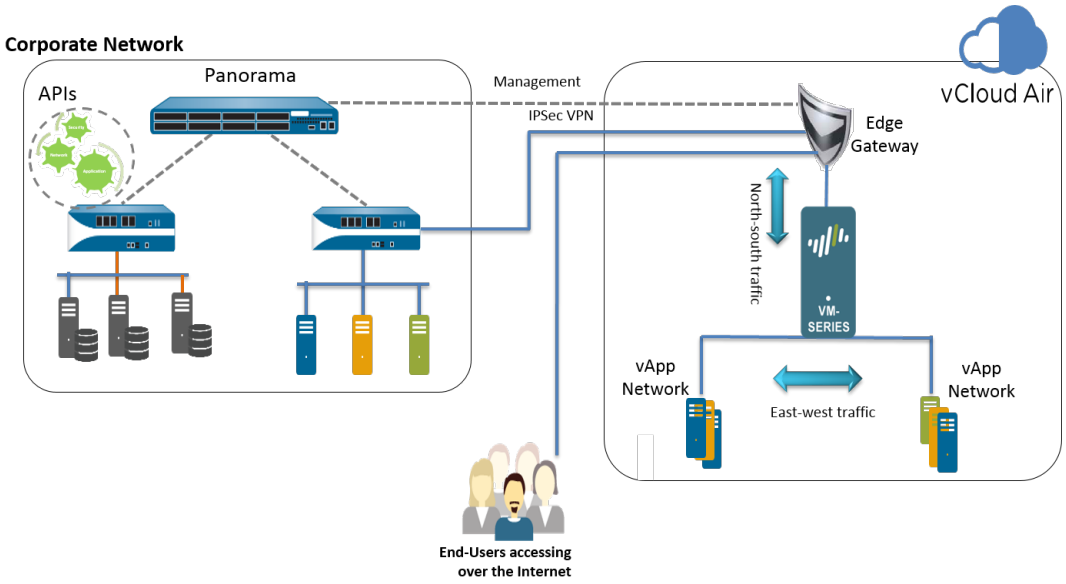
© 2019 Palo Alto Networks, Inc.

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 即可简化策略更新，集中进行策略管理，并实现集中日志记录和报告。



© 2019 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。

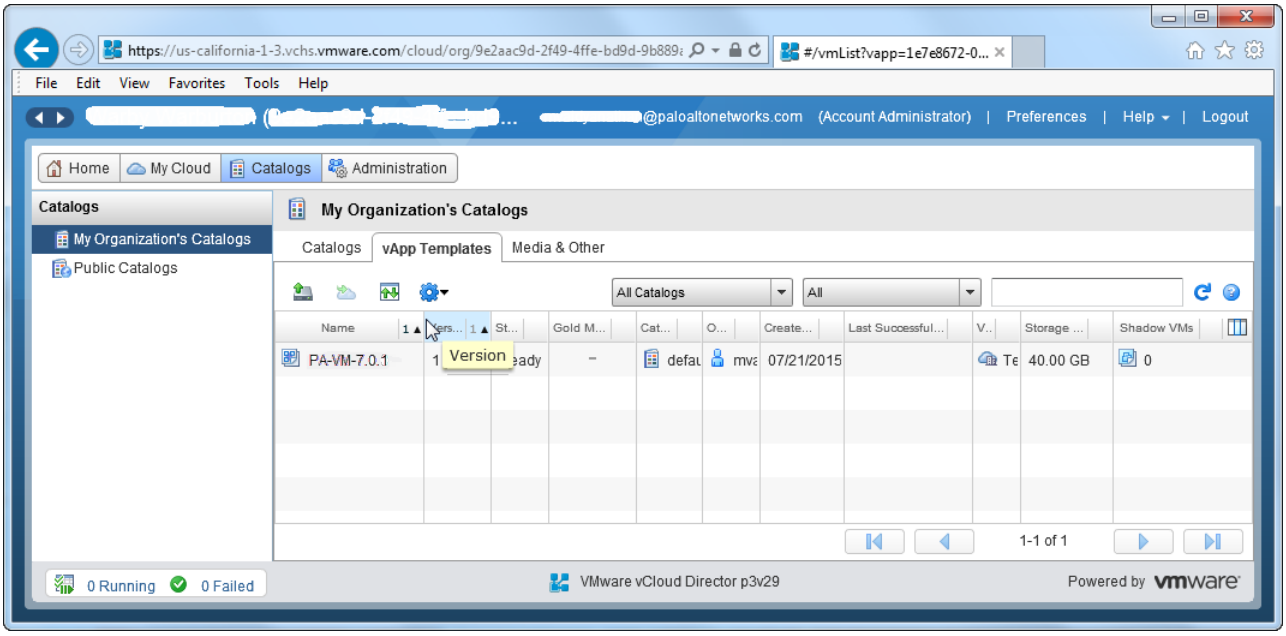
1. 转到：www.paloaltonetworks.com/services/support.html.
2. 按 **PAN-OS for VM-Series Base Images**（用于 VM 系列基本映像的 PAN-OS）进行筛选并下载 OVA 映像。例如，PA-VM-ESX-9.1.0.ova。

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。



STEP 3 | 选择您的工作流。

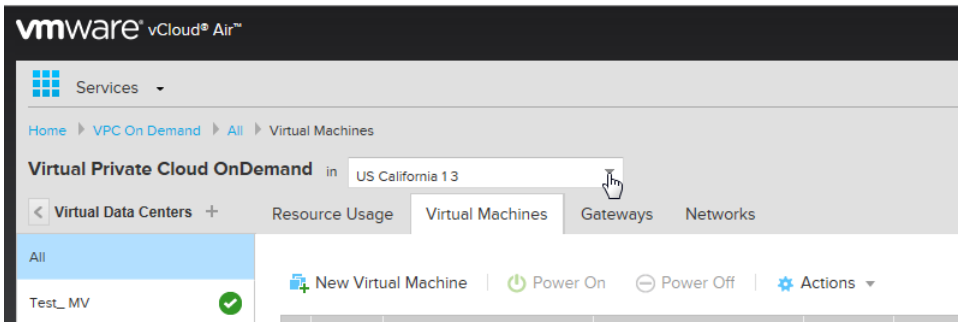
vApp 是一个模板集，适用于所有包含虚拟机及操作系统映像的预配置虚拟设备。

- 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。

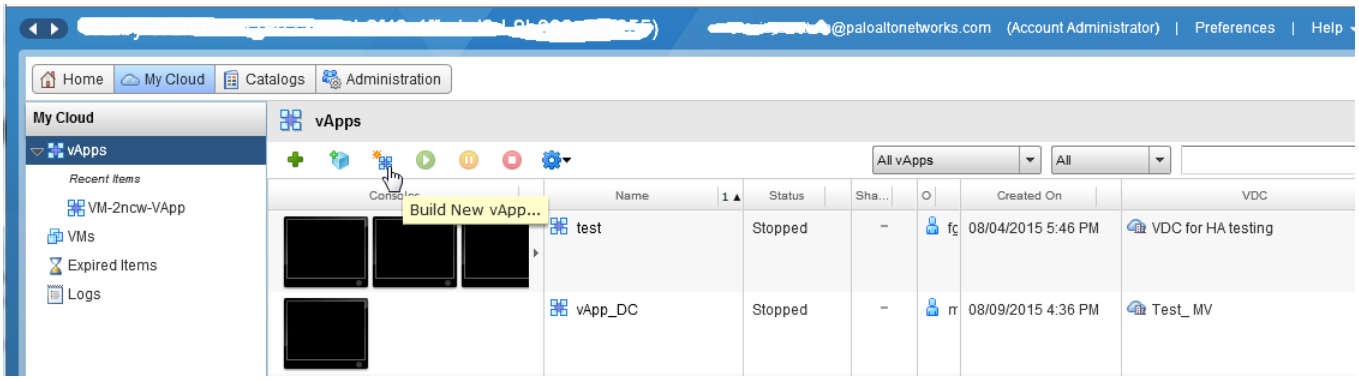
STEP 4 | 创建包含 VM 系列防火墙的 vDC 和 vApp。

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。

© 2019 Palo Alto Networks, Inc.



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）> **vApps**，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。

STEP 5 | 将 VM 系列防火墙添加到 vApp 中。

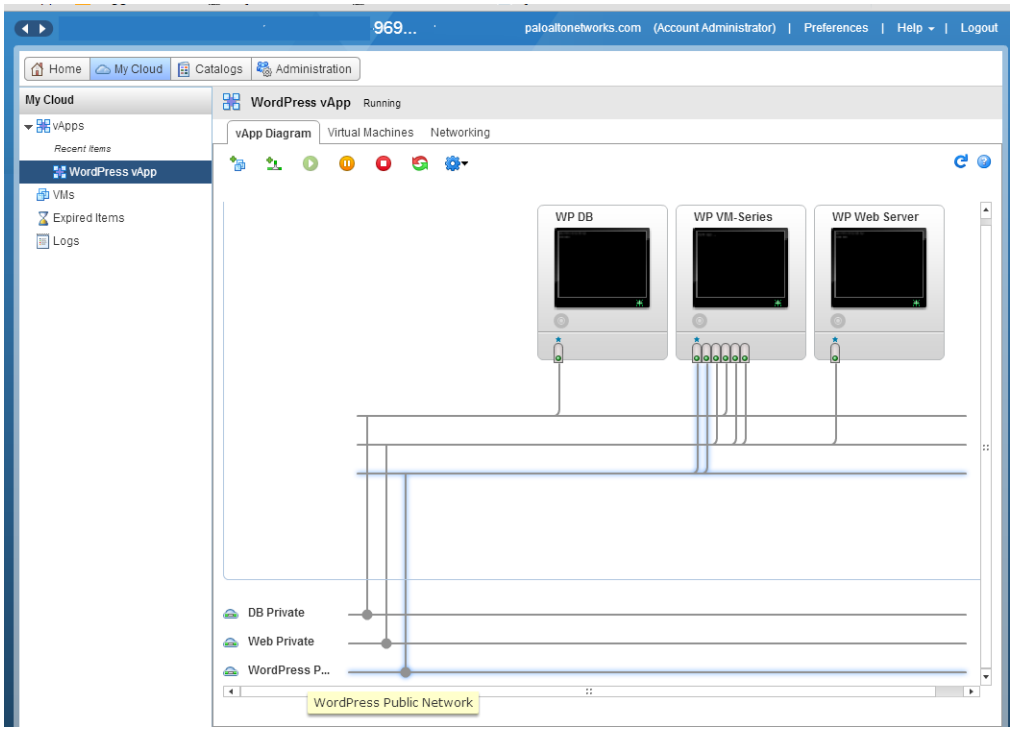
1. 登录到 vCloud Air。
2. 从左窗格中选择您现有的**Virtual Data Center**（虚拟数据中心），右键单击并选择 **Manage Catalogs in vCloud Directorr**（管理 vCloud Director 中的编录）。您将重定向至 vCloud Director 的 Web 接口。
3. 选择 **My Cloud**（我的云）> **vApps**，然后单击要将 VM 防火墙纳入其中的 vApp 的 **Name**（名称）。
4. 打开 vApp（双击名称），选择 **Virtual Machines**（虚拟机），然后单击 ✚ 以添加虚拟机。
   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）。

© 2019 Palo Alto Networks, Inc.

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。

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）> **vApps**，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，将数据面板网络接口附加至 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）> **vApps**，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。

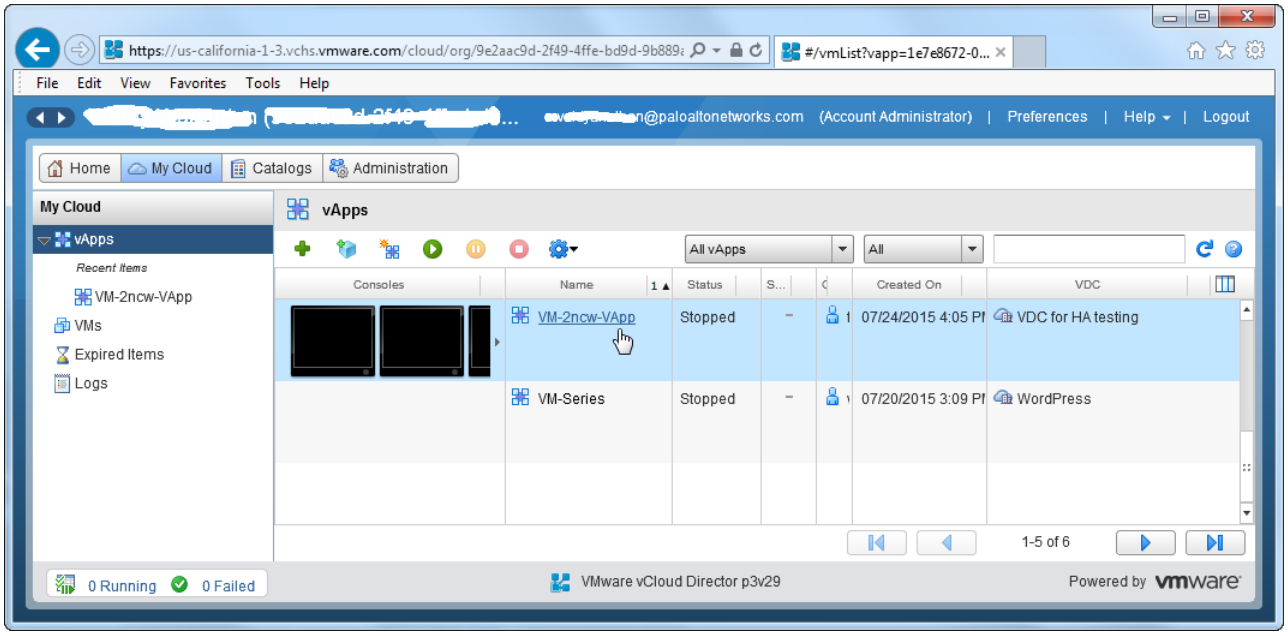


STEP 7 | （可选）编辑为 VM 系列防火墙分配的硬件资源。

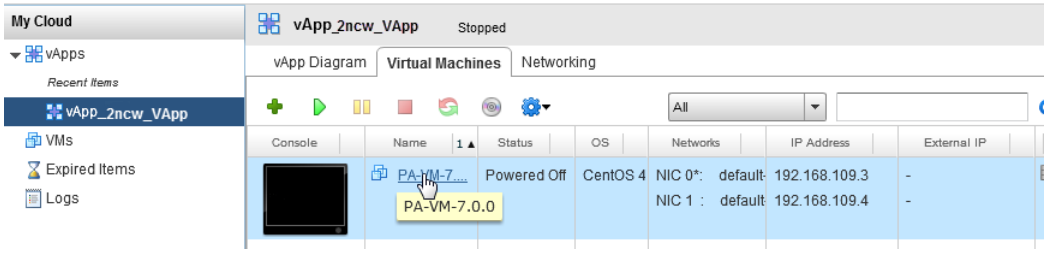
仅当您需要分配额外的 CPU、内存或硬盘至防火墙时，才需进行此操作。

© 2019 Palo Alto Networks, Inc.

1. 选择 **My Cloud**（我的云）> **vApps**，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。

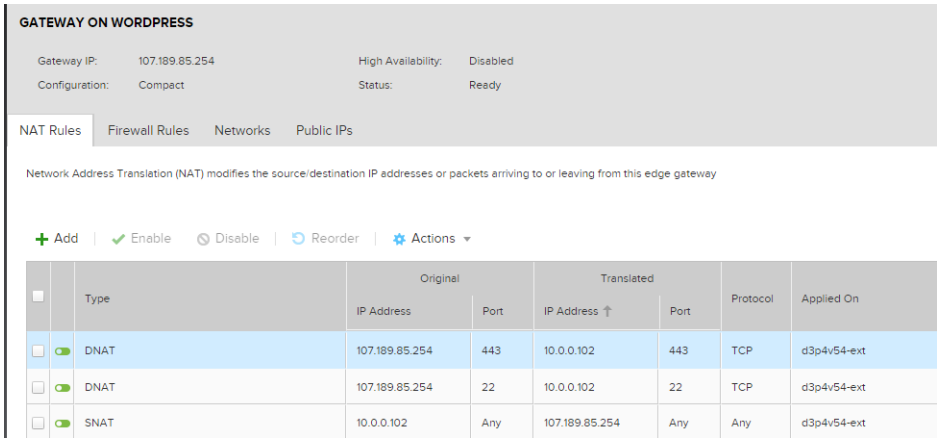
vCloud Air 上的 VM 系列防火墙支持 VMware 工具，您可以通过 ESXi 和 vCloud Air 使用 VM 系列防火墙的 VMware 工具查看 VM 系列防火墙的管理 IP 地址。

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。

© 2019 Palo Alto Networks, Inc.



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 系列防火墙以使用管理程序分配的 MAC 地址。

虚拟机监控程序分配的 MAC 地址

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：
   - **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，选择 **New Zone**（安全区域）下拉列表中的 **Security Zone**（新区域）。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。

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

在 *VMware NSX* 上设置 *VM* 系列防火墙

VM 系列防火墙可以部署在 VMware 网络虚拟化解决方案的两个版本中 — NSX-V 和 NSX-T。

> 在 VMware NSX-V 上设置 VM 系列防火墙
> 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-V 上设置 VM 系列防火墙

VM 系列 VMware NSX-V 版防火墙由 Palo Alto Networks 和 VMware 共同开发。此解决方案使用 NetX API 通过 VMware ESXi 服务器集成 Palo Alto Networks 下一代防火墙和 Panorama，以全面监视所有数据中心流量（包括主机内虚拟机通信），并对其启用安全应用程序。

以下主题提供有关 VM 系列 NSX-V 版防火墙的信息：

- VM 系列 NSX-V 版防火墙概述
- NSX-V 部署清单上的 VM 系列防火墙
- 安装 VMware NSX 插件
- 将 VM 系列防火墙注册为 NSX-V Manager 上的服务
- 部署 VM 系列防火墙
- 创建安全组和控制规则
- 将安全策略应用于 VM 系列防火墙
- 控制来自不运行 VMware 工具的来宾的流量
- #unique_131/unique_131_Connect_42_id17ADHJ00IPQ
- 动态隔离感染的来宾
- 将以操作为中心的配置迁移到以安全为中心的配置
- 用例：共享计算基础架构和共享安全策略
- 用例：专用计算基础架构上的共享安全策略
- 动态地址组 — 将信息从 NSX-V Manager 中继到 Panorama

VM 系列 NSX-V 版防火墙概述

NSX-V（VMware 为软件定义的数据中心 (SDDC) 设计的网络和安全平台）能够将 Palo Alto Networks 防火墙部署为 ESXi 服务器群集上的服务。*SDDC* 一词是 VMware 术语，指的是基础架构（计算资源、网络和存储）使用 VMware NSX-V 虚拟化的数据中心。

为适应灵活的 SDDC 中的变化，NSX-V 版 VM 系列防火墙简化了部署 Palo Alto Networks 下一代防火墙和继续强制 SDDC 中东向西流量的安全性和合规性的过程。有关 VM 系列 NSX-V 版的详细信息，请参阅以下主题：

- 适用于 NSX-V 解决方案的 VM 系列防火墙有哪些组件？
- VM 系列防火墙 NSX-V 版解决方案中的组件如何共同协作？
- 适用于 NSX-V 解决方案的 VM 系列防火墙有哪些优势？
- VM 系列防火墙 NSX-V 版上的多租户支持是什么？

适用于 *NSX-V* 解决方案的 *VM* 系列防火墙有哪些组件？

下表显示了 Palo Alto Networks 和 VMware 联合解决方案的组件。下列主题详细介绍了各个组件：

- vCenter 服务器
- NSX-V Manager
- Panorama
- VM 系列防火墙 NSX-V 版
- 网络通信使用的端口/协议

VMware 组件	
vCenter 服务器	vCenter 服务器是 vSphere 套件的集中式管理工具。

© 2019 Palo Alto Networks, Inc.

VMware 组件	
NSX-V Manager	VMware 的网络和安全平台必须使用 vCenter 服务器进行安装和注册。需要使用 NSX-V Manager 才能在 ESXi 群集内的 ESXi 主机上部署 VM 系列防火墙。
ESXi 服务器	ESXi 是启用计算虚拟化的虚拟机监控程序。

有关支持的软件版本，请参阅 Palo Alto Networks 兼容性矩阵。

Palo Alto Networks 组件	
PAN-OS	VM 系列基本映像 (PA-VM-NSX-9.1.zip) 使用 PAN-OS 9.1 为 NSX-V 部署 VM 系列防火墙。 在 ESXi 服务器上部署 NSX-V 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 系列系统要求。
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。	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-V Manager 一起部署、许可和集中管理 NSX-V 的 VM 系列防火墙（配置和策略）。 Panorama 必须连接到 NSX-V Manager、vCenter 服务器、VM 系列防火墙，Palo Alto Networks 才能更新服务器。 Panorama 所需的资源取决于 Panorama 将运行的模式：旧版或 Panorama（推荐）。Panorama 的新安装在 Panorama 模式下运行。升级到 9.1 前在传统模式下运行的 Panorama 安装在升级到 9.1 后仍处于传统模式。有关与每种模式相关的模式和要求的更多信息，请参阅设置 Panorama 虚拟设备。 在 Panorama 模式下，根据 Panorama 的日志存储容量设置内存、CPU 数量和存储空间： • 2TB 存储空间 — 8 个 CPU 和 16GB 内存 • 4TB 存储空间 — 8 个 CPU 和 32GB 内存 • 6 到 8TB 存储空间 — 12 个 CPU 和 32GB 内存 • 10 到 16TB 存储空间 — 12 个 CPU 和 64GB 内存 • 18 到 24TB 存储空间 — 16 个 CPU 和 64GB 内存 • 系统磁盘空间：81GB • 日志存储容量：2TB 至 24TB 在传统模式下，根据 Panorama 管理的防火墙数量设置内存和内核数量： • 1 到 10 个防火墙：4 核和 4GB • 11 到 50 个防火墙：8 核和 8GB 内存 • 51 到 1,000 个防火墙：8 核和 16GB 内存 • 系统磁盘空间：52GB • 日志存储容量：11Gb（系统磁盘上的默认日志存储）设置为 8TB（如果添加虚拟日志记录磁盘）
VM 系列防火墙 NSX-V 版	VM-100、VM-200、VM-300、VM-500 和 VM-1000-HV 支持 NSX-V。

© 2019 Palo Alto Networks, Inc.

vCenter 服务器

需要使用 vCenter 服务器才能在数据中心中管理 NSX-V Manager 和 ESXi 主机。此共同的解决方案要求在 vCenter 服务器上将 ESXi 主机组织为一个或多个群集，并且必须将 ESXi 主机连接到分布式虚拟交换机。

有关群集、分布式虚拟交换机、DRS 和 vCenter 服务器的信息，请参阅 VMware 文档：http://www.vmware.com/support/vcenter-server.html

NSX-V Manager

NSX-V 是 VMware 的网络虚拟化平台，已与 vSphere 完全集成。NSX-V 防火墙和服务组合系统是 NSX-V Manager 的主要功能。NSX-V 防火墙是一个逻辑防火墙，可让您将网络和安全服务附加到虚拟机，而服务组合系统可让您对虚拟机分组，并创建策略将流量重定向到 VM 系列防火墙（称为 NSX-V Manager 上的 Palo Alto Networks NGFW 服务）。

Panorama

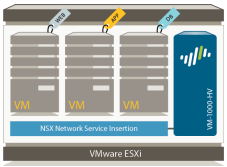
Panorama 用于将 NSX-V 版 VM 系列防火墙注册为 NSX-V Manager 上的 *Palo Alto Networks NGFW* 服务。在 NSX-V Manager 上注册 Palo Alto Networks NGFW 服务可让 NSX-V Manager 在 ESXi 群集中的每个 ESXi 主机上部署 NSX-V 版 VM 系列防火墙。

Panorama 充当 VM 系列 NSX 版防火墙的集中管理点。在 NSX-V 中部署新的 VM 系列防火墙后，它可与 Panorama 通信以获取许可证，并从 Panorama 接收其配置/策略。在 Panorama 中，可以使用设备组和模板堆栈来集中管理 VM 系列防火墙的所有配置元素、策略和动态地址组。此解决方案中基于 REST 的 XML API 集成可让 Panorama 与 NSX-V Manager 和 VM 系列防火墙同步，以便使用动态地址组，以及在虚拟化环境和安全实施之间共享上下文。有关更多信息，请参阅 使用动态地址组实施策略。

VM 系列防火墙 NSX-V 版

VM 系列 NSX-V 版防火墙是在 ESXi 虚拟机监控程序上部署的 VM 系列防火墙。使用 NetX API 集成可自动化在 ESXi 虚拟机监控程序上直接安装 VM 系列防火墙的过程，并且可让此虚拟机监控程序将流量转发到 VM 系列防火墙，而无需使用 vSwitch 配置；因此，不需要更改此虚拟网络拓扑。

VM 系列 NSX-V 版防火墙仅支持虚拟线路接口。在此版本中，Ethernet 1/1 和 Ethernet 1/2 通过虚拟线路绑定在一起，并使用 NetX 数据面板 API 与虚拟机监控程序通信。VM 系列 NSX-V 版防火墙既不需要也不支持第 2 层或第 3 层接口，因此防火墙不会执行任何交换或路由操作。为了启用多租户环境中的流量分离，您可以创建其他区域，这些区域在内部映射到专利虚拟线路接口、ethernet 1/1 和 ethernet 1/2 上的虚拟线路子接口对。



网络通信使用的端口/协议

要启用部署 VM 系列 NSX-V 版防火墙所需的网络通信，必须使用以下协议/端口和应用程序。

- **Panorama** — 要获得软件更新和动态更新，Panorama 在 TCP/443 上使用 SSL 访问 updates.paloaltonetworks.com；此 URL 利用 CDN 基础架构。如果需要单个 IP 地址，使用 staticupdates.paloaltonetworks.com。更新的 App-ID 为 paloalto-updates。

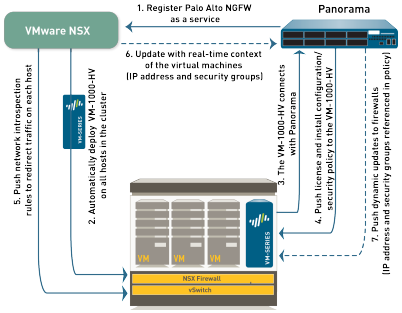
  NSX-V Manager 和 Panorama 在 TCP/443 上使用 SSL 进行通信。
- **VM 系列 NSX-V** 版防火墙 — 如果计划使用 WildFire，VM 系列防火墙必须能够使用端口 443 访问 wildfire.paloaltonetworks.com。这是一个 SSL 连接，且 App-ID 为 paloalto-wildfire-cloud。

  VM 系列防火墙上的管理接口使用 SSL 通过 TCP/3978 与 Panorama 进行通信。
- **vCenter** 服务器 — vCenter 服务器必须能够访问托管 VM 系列 OVA 的部署 Web 服务器。默认情况下，端口为 TCP/80 或 App-ID 为 web-browsing。

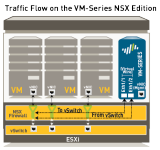
© 2019 Palo Alto Networks, Inc.

VM 系列防火墙 *NSX-V* 版解决方案中的组件如何共同协作？

为符合软件定义的数据中心中的安全性质询要求，NSX-V Manager、ESXi 服务器和 Panorama 需要协调工作才能自动执行 VM 系列防火墙部署。



1. 注册 **Palo Alto Networks NGFW** 服务 — 第一步是在 NSX-V Manager 上将 Palo Alto Networks NGFW 注册为服务。在此注册过程中，将使用 NetX 管理面板 API 启用 Panorama 和 NSX-V Manager 之间的双向通信。使用 IP 地址和访问凭据配置 Panorama，以建立连接，并在 NSX-V Manager 上注册 Palo Alto Networks NGFW 服务。服务配置包括部署 VM 系列 NSX-V 版防火墙所需的 VM 系列基本映像的访问 URL、取回许可证使用的授权代码以及 VM 系列防火墙所属的设备组和模板堆栈。NSX-V Manager 使用此管理面板连接与 Panorama 共享虚拟环境变更更新。
2. 从 **NSX-V** 自动部署 **VM** 系列 — NSX-V Manager 在注册期间通过指定 URL 收集 VM 系列基本映像，并在 ESXi 群集中的每个 ESXi 主机上安装 VM 系列防火墙的实例。在静态管理 IP 池或 DHCP 服务（在 NSX-V Manager 上定义的）中，将管理 IP 地址分配给 VM 系列防火墙，并将 Panorama IP 地址提供给此防火墙。当此防火墙启动时，NetX 数据面板集成 API 会将此 VM 系列防火墙连接到虚拟机监控程序，以便从 vSwitch 接收流量。



3. 在 **VM** 系列防火墙和**Panorama**之间建立通信- VM 系列防火墙然后启动到Panorama的连接以获取其许可证。Panorama 从更新服务器中取回许可证，并将其推送到防火墙。VM 系列防火墙接收许可证，并使用有效的序列号重新启动。

   如果您的 *Panorama* 处于离线状态，这表示其没有直接连接到*Internet*来检索许可证和推送到防火墙，您必须手动许可每个防火墙。如果 *VM* 系列防火墙没有 Internet 访问权限，您必须将防火墙的序列号添加到 *Panorama* 中，以便将其注册为一台受管设备，以便您可以从 *Panorama* 中推送相应的模板堆栈和设备组设置。
4. 从 **Panorama** 安装配置/策略到 **VM** 系列防火墙 — VM 系列防火墙与 Panorama 重新连接并提供其序列号。Panorama 现在将此防火墙添加到在服务定义过程中定义的设备组和模板堆栈，并将配置和策略规则推送到此防火墙。此 VM 系列防火墙现可用作安全虚拟机，您可进一步配置它，以在网络中安全启用应用程序。
5. 将流量重定向规则推送到 **NSX-V Manager** — 创建安全组，并定义网络自检规则，以便指定流向 VM 系列防火墙的流量的源来宾。请参阅综合策略规则了解详情。

   为确保来宾的流量转向 *VM* 系列防火墙，您必须在每位来宾上安装*VMware Tools*。如果未安装 *VMware Tools*，则 *NSXNSX-V Manager* 不知道该来宾虚拟机的 *IP* 地址，因此无法将流量转向 *VM* 系列防火墙。有关详细信息，请参阅控制来自不运行 VMware 工具的来宾的流量。如果您运行的是 *NSX-V Manager 6.2.4* 或更高版本，则不需要这样做。
6. 从 **NSX-V Manager** 接收实时更新 — NSX-V Manager 将虚拟环境变更的实时更新发送到 Panorama。这些更新包括重定向到 VM 系列防火墙的流量的源安全组中来宾的安全组和 IP 地址信息。请参阅综合策略规则了解详情。

© 2019 Palo Alto Networks, Inc.

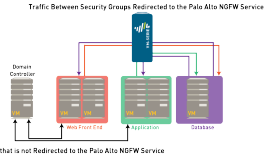
7. 使用策略中的动态地址组并将动态更新从 **Panorama** 推送到 **VM** 系列防火墙 — 在 Panorama 上，使用安全组的实时更新创建动态地址组，将它们绑定到安全策略，然后将这些策略推送到 VM 系列防火墙。此设备组中的每个 VM 系列防火墙均有相同的策略集，并且现经完全编制用以保护 SDDC。有关详细信息，请参阅使用动态地址组实施策略。

集成策略规则

Panorama 作为单点配置，为 NSX-V Manager 提供将来宾虚拟机的流量重定向到 VM 系列防火墙所需的上下文信息。流量导向规则在 Panorama 上定义并推送到 NSX-V Manager；这些决定了集群中哪些客户端将流向 Palo Alto Networks NGFW 服务的流量。在 Panorama 上也定义了安全实施规则，并将其推送到 VM 系列防火墙，以获取转向 Palo Alto Networks NGFW 服务的流量。

- 控制规则 — 每台 ESXi 主机上用于定向来宾流量的规则在 Panorama 上定义，并由 NSX-V Manager 作为合作伙伴安全服务规则应用。

  对于需要 VM 系列防火墙检查和保护的流量，在 Panorama 上创建的控制规则允许您将流量重定向到 Palo Alto Networks NGFW 服务。此流量随后流向 VM 系列防火墙，在转到虚拟交换机之前，先由 VM 系列防火墙处理。



  不需要 VM 系列防火墙检查的流量（例如网络数据备份或流到内部域控制器的流量）不需要重定向到 VM 系列防火墙，可以发送到虚拟交换机进行进一步处理。
- 在 **Panorama** 上集中管理并应用于 **VM** 系列防火墙的规则 — 这些下一代防火墙规则均应用于 VM 系列防火墙。这些规则通过模板堆栈和设备组在 Panorama 上集中定义和管理，并被推送到 VM 系列防火墙。VM 系列防火墙随后通过在源/目标 IP 地址中进行匹配来实施安全策略（使用动态地址组可让防火墙实时填充组成员），并将流量转发到 NSX-V 防火墙的筛选器。

  要了解 NSX-V Manager 和 Panorama 如何与 SDDC 中的变更保持同步，并确保 VM 系列防火墙一致地实施策略，请参阅使用动态地址组实施策略。

使用动态地址组实施策略

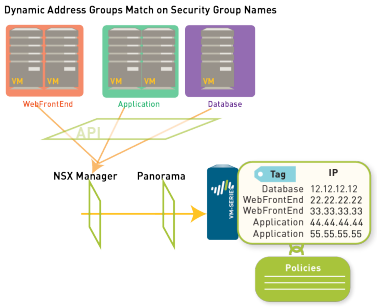
与其他版本的 VM 系列防火墙不同，由于两个虚拟线路接口（及其子接口）都属于同一区域，VM 系列 NSX-V 版防火墙会使用动态地址组作为其流量分段机制。VM 系列 NSX-V 版防火墙的安全策略规则必须具有相同的源区域和目标区域，因此，若要实施不同的流量处理，您需使用动态地址组作为安全策略规则中的源对象或目标对象。

由于 IP 地址会在数据中心环境下不断变化，动态地址组可实现安全策略内源和/或目标地址的自动引用。在出现地址变更（添加、删除或移动）时，静态地址对象必须在配置中进行手动更新和提交，与静态地址对象不同，动态地址组可根据变更自动改写。

对于在属于 NSX-V 配置的设备组中创建，并使用匹配条件 **_nsx_*<dynamic address group name>*** 配置的任何动态地址组，会触发在 NSX-V Manager 中的相应安全组中触发创建。在带有多个客户或租户的 ESXi 群集中，凭借 NSX-V Manager 上的服务配置文件（Panorama 上的区域）的安全组筛选功能，您可以在虚拟环境中不同安全组出现 IP 地址交叠时强制执行策略。

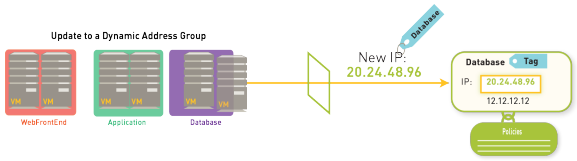
例如，如果 Web 应用程序有多层架构，则在 Panorama 上为 WebFrontEnd 服务器、应用程序服务器和数据库服务器创建三个动态地址组。在 Panorama 上提交这些更改时，会触发在 NSX-V Manager 上创建三个相应的安全组。

© 2019 Palo Alto Networks, Inc.



在 NSX-V Manager 上，您可以将来宾虚拟机添加到相应的安全组。然后，您可以在安全策略中将动态地址组用作源/目标对象，定义允许遍历这些服务器的应用程序，然后将这些规则推送到 VM 系列防火墙。

每次在 ESXi 群集或更新/创建的安全组中添加或修改来宾时，NSX-V Manager 都会通过 PAN-OS 基于 REST 的 XML API 使用 IP 地址和来宾所属的安全组更新 Panorama。要跟踪信息流，请参阅 动态地址组 — 从 NSX Manager 到 Panorama 的信息中继。



为确保每个安全组的名称唯一，*vCenter* 服务器会将受管对象引用 *(MOB) ID* 分配给您为安全组定义的名称。在 *Panorama* 上用于显示安全组名称的语法为 *serviceprofileid-specified_name-securitygroup-number; for example, serviceprofile13-WebFrontEnd-securitygroup-47*。

当 Panorama 收到 API 通知时，它会验证/更新每个来宾的 IP 地址和该来宾所属的安全组和服务配置文件。然后，Panorama 将这些实时更新推送到设备组中包含的所有防火墙，并在 Panorama 上的服务管理器配置中通知设备组。

在每个防火墙上，引用这些动态地址组的所有策略规则均在运行时更新。由于防火墙会对安全组标记进行匹配以确定动态地址组的成员，因此您不需要修改或更新在虚拟环境中更改的策略。防火墙会匹配这些标记以找到每个动态地址组的当前成员，并会将安全策略应用于该组包含的源/目标 IP 地址。

适用于 *NSX-V* 解决方案的 *VM* 系列防火墙有哪些优势？

适用于 VMware NSX-V 的 VM 系列防火墙侧重于保护软件定义的数据中心内的东向西通信。部署此防火墙具有以下优点：

- 更牢固的集中式管理 — 使用此解决方案部署的防火墙由 Panorama（Palo Alto Networks 集中管理工具）授权许可和管理。Panorama 作为与 NSX-V 集成的单点配置。它为 NSX-V Manager 提供将流量重定向到 VM 系列防火墙，以进行检查和执行所需的信息。使用 Panorama 管理边界防火墙和数据中心防火墙（基于硬件的防火墙和虚拟防火墙）可让您集中策略管理，并在整个网络的策略实施中保持灵活性和一致性。
- 自动部署 — NSX-V Manager 自动执行提供下一代防火墙安全服务的过程，并且此 VM 系列防火墙允许透明化安全实施。在将新的 ESXi 主机添加到群集中时，将自动部署、配置新的 VM 系列防火墙，并且新的 VM 系列防火墙可用于立即实施策略，而无需任何手动干预。此自动工作流程可让您与数据中心的虚拟机部署保持同步。防火墙上的虚拟机监控程序模式可让您无需重新配置端口/vSwitch/网络拓扑；由于每个 ESXi 主机都有此防火墙的实例，因此流量不需要遍历网络或回传，以便检查和一致实施策略。
- 在共享和专用计算基础架构中轻松管理租户 — 这种集成有助于实现防火墙配置方面的灵活性，包括处理多个区域的流量分段，定义每个租户或子租户的共享或特定策略集，还包括租户或子租户之间 IP 地址交叠的处理支持。无论是采用共享式群集，因而需要定义租户特定策略并从逻辑上隔离每个租户（或子租户）的流量，还是针对每个租户采用专用群集，该解决方案都可满足您在防火墙配置方面的需求。在托管多个租户工作负载的群集中，如果您需要为每个租户采用专用的 VM 系列防火墙实例，您可以在 ESXi

© 2019 Palo Alto Networks, Inc.

群集中的每个主机上部署多个 VM 系列防火墙实例。有关详细信息，请参阅VM 系列防火墙 NSX-V 版上的多租户支持是什么？

- 虚拟环境和动态安全的安全实施之间的集成更紧密 — 动态地址组可感知虚拟机/应用程序的变更，并确保安全策略与网络变更如影随形。此感知功能可在灵活的环境中监视和保护应用程序。

总而言之，此解决方案可确保以最低管理开销保护虚拟网络的动态性。您可以更快、更有效、更安全地成功部署应用程序。

VM 系列防火墙 *NSX-V* 版上的多租户支持是什么？

VM 系列防火墙上的多租户支持可让您确保多个租户或多个子租户的安全。租户是指一个客户或组织，例如 Palo Alto Networks。子租户是组织内部的一个部门或业务单元，例如营销、会计或人力资源部门等。为了确保多个租户的安全，Parorama 提供了一种灵活的方式，以便您针对每个租户创建多个安全策略集，并创建多个区域来隔离来自每个子租户的流量，并将流量重定向至适当配置的 VM 系列防火墙。您还可以在 ESXi 群集中的每个主机上部署多个 VM 系列防火墙实例。

Panorama 和受管的 *VM* 系列防火墙必须运行 *PAN-OS 7.1* 或更高版本才能支持多租户。

要部署多租户解决方案，请在 Panorama 上创建一个或多个服务定义和服务配置文件区域。Panorama 上的服务定义用于指定使用一个设备组和一个模板堆栈的 VM 系列防火墙的配置。这意味着使用一个服务定义部署的 VM 系列防火墙的每个实例均采用一个通用的策略规则集，用于确保 ESXi 群集中租户和子租户的安全。

Panorama 模板堆栈内的服务配置文件区域用于通过虚拟线路子接口对来自每个子租户的流量进行分段。在创建新服务配置文件区域时，Panorama 会将区域作为模板堆栈配置的一部分推送至防火墙，然后防火墙会自动创建一对虚拟线路子接口，例如 ethernet1/1.3 和 etherent 1/2.3，确保防火墙可以为某个子租户隔离流量。由于模板堆栈最多可支持 32 个子接口对，您可以从逻辑上隔离流量并最多保护 32 个子租户。

Panorama 会将每个服务定义注册为 NSX-V Manager上的服务定义，并将每个服务配置文件区域注册为相应服务定义中的服务配置文件。此外，在您通过 NSX-V Manager部署服务定义时，会在 ESXi 群集的每个主机上部署 VM 系列防火墙的一个实例。您还可以使用在 Panorama 定义和在 NSX-V Manager 上应用的操作规则来指定哪些流量会基于 NSX-V 安全组被重定向至 VM 系列防火墙，以及会基于服务配置文件被重定向至哪个租户或子租户。

根据您的具体需求，您可以选择下列一种多租户选项：

- 带有共享 **VM** 系列防火墙的共享群集 — 多个租户共享群集和 VM 系列防火墙。在群集中的每个主机上部署 VM 系列防火墙单个实例。若要分离来自每个租户的流量，您可以为每个租户创建一个区域，并定义单个通用的策略集，以确保所有租户虚拟机的安全。请参阅用例：共享计算基础架构和共享安全策略。
- 带有专用 **VM** 系列防火墙的专用群集 — 单个租户占用整个群集，在群集内的每个主机上部署单个 VM 系列防火墙实例。在这种部署中，租户可以拥有单个区域和单个策略集，或者租户也可以为需要流量分离的子租户配置多个区域（每个子租户对应一个区域），并配置带有基于区域的规则的单个策略集，用于确保每个子租户的流量安全。用例：专用计算基础架构上的共享安全策略。
- 带有专用 **VM** 系列防火墙的共享群集 — 多个租户共享群集，并在群集内的每个主机上部署多个 VM 系列防火墙实例，确保每个租户拥有一个专用的 VM 系列防火墙实例。这种部署可在共享的基础架构上为每个租户提供可扩展性和更好的性能。基于每个租户的需求，您可以为群集定义两个或两个以上的服务定义。

  在部署 VM 系列防火墙的多个实例时，您必须确保每个 ESXi 主机均具有充足的 CPU、内存和硬盘资源，以便支持 VM 系列防火墙以及在其上运行的其他虚拟机。

NSX-V 部署清单上的 VM 系列防火墙

要为 NSX-V 部署 VM 系列防火墙，请使用以下工作流程：

© 2019 Palo Alto Networks, Inc.

- 步骤 **1**：设置组件 — 要为 NSX-V 部署 VM 系列防火墙，请设置以下组件（参阅 适用于 NSX-V 解决方案的 VM 系列防火墙有哪些组件？）：
  - 设置 vCenter 服务器，使用 vCenter 服务器安装和注册 NSX-V Manager。

    如果尚未设置虚拟机，并且未将 ESXi 主机分为多个群集，请参阅相关 VMware 文档了解有关设置 vSphere 环境的说明。此文档不会引导您完成设置此解决方案 VMware 组件的过程。

    除非启用大量接收负载，否则切勿修改 *vSphere* 基础架构中虚拟分布式交换机 *(vDS)* 上的默认 *MTU* 值（*1500* 字节）。将 *MTU* 的值修改为任何其他值会导致 *VM* 系列 *NSX-V* 版防火墙出现丢包的情况。
  - 升级 Panorama。如果不熟悉 Panorama，请参阅 Panorama 文档了解有关设置和升级 Panorama 的说明。如果选择将以操作为中心的配置迁移到以安全为中心的配置格式，请参阅将以操作为中心的配置迁移到以安全为中心的配置。
  - 配置 SSL/TLS 服务配置文件。如果您运行的是 NSX-V Manager 6.2.3 或更低版本，则必须配置允许 TLSv1.0 并将其应用于 Panorama 管理接口的 SSL/TLS 服务配置文件。如果您运行的是 NSX Manager-V 6.2.4 或更高版本，则不需要 SSL/TLS 服务配置文件。
  - 安装 VMware NSX 插件。
  - 安装许可证停用 API 密钥。删除 NSX-V Manager 上的 Palo Alto Networks 服务部署会自动触发停用许可证。停用 API 密钥是成功禁用 VM 系列许可证所必需的。
  - 在 Web 服务器上下载并保存 VM 系列 NSX-V 版防火墙的 ovf 模板。ovf 模板必须与您的 VM 系列型号匹配。如果使用 VM-200，请选择 VM-100 ovf。如果使用 VM-1000-HV，请选择 VM-300 ovf。

    NSX-V Manager 必须具有此 Web 服务器的网络访问权限，才能根据需要部署 VM 系列防火墙。您不能在 Panorama 上托管 ovf 模板。

    请为 *ova* 文件名提供一个未包含版本号的通用名。通过使用通用命名规则（如 ***https://acme.com/software/PA-VM-NSX.ova***），您将能在每次更新版本可用时覆盖此 *ova*。
  - 在支持门户上使用支持帐户注册 VM 系列 NSX-V 版防火墙的容量授权代码。有关详情，请参阅升级 VM 系列防火墙。
- 步骤 **2**：注册 — 配置 Panorama 以将 VM 系列防火墙注册为 NSX-V Manager 上的服务。注册后，VM 系列防火墙将添加到网络服务列表中，NSX-V Manager 以透明方式将这些网络服务部署为服务。授权防火墙许可证和配置防火墙还需要在 Panorama 和 NSX-V Manager 之间建立连接。
  - （在 Panorama 上）创建服务管理器以启用 Panorama 和 NSX-V Manager 之间的通信。
  - （在 Panorama 上）创建服务定义。如果您从更早的版本升级，将会自动迁移现有的服务定义。有关详细信息，请参阅默认行为更改。
- 步骤 **3**：部署 **VM** 系列防火墙 — 在使用 NSX-V 部署 VM 系列防火墙之前，群集中的每台主机必须具有部署防火墙所需的必要 NSX-V 组件。
  - （在 NSX-V Manager 上）定义 IP 地址池。将定义范围中的 IP 地址分配给 VM 系列防火墙每个实例的管理接口。

    NSX-V Manager 使用 *IP* 地址作为控制流量流向 *VM* 系列防火墙的匹配条件。如果来宾虚拟机上未安装 *VMware* 工具，请参阅引导来自未运行 VMware 工具的来宾的流量。如果您运行的是 *NSX-V Manager 6.2.4* 或更高版本，则不需要这样做。
  - （在 NSX-V Manager 上）准备用于 VM 系列防火墙的 ESXi 主机。
  - （在 NSX-V Manager 上）部署 VM 系列防火墙。NSX-V Manager 会在群集中的每个 ESXi 主机上自动部署一个 VM 系列防火墙。
  - （在 NSX-V Manager 上）将 VM 添加到相关安全组。
  - （在 Panorama 上）将策略应用于 VM 系列防火墙。在 Panorama 中，可以定义策略，将其推送到所有 VM 系列防火墙，并对其集中管理。此集中式管理机制可让您以最少管理干预措施保护来宾/应用程序。

© 2019 Palo Alto Networks, Inc.

- 步骤 4：创建安全组和控制规则 — 您如何选择部署安全组，并且指导规则取决于您的部署重点是以安全为中心还是以操作为中心。

  在以安全为中心的部署中，安全管理员在 Panorama 中创建安全组和导向规则。您可以从现有的安全策略集和指定的源组和目标组集开始。任何新的动态部署的应用程序都符合 Panorama 上定义的预定义安全策略。Panorama 将这些命名组推送到 NSX-V Manager，虚拟化管理员在其中挑选组名并定义将哪些虚拟机放入其中。

  在以操作为中心的部署中，安全组由虚拟化管理员根据需要对 VM 工作负载进行分类和分类来定义。在这种情况下，安全组在 NSX-V Manager 中定义并填充。在 NSX-V Manager 中创建的安全组必须与 Panorama 上的动态地址组关联，后者在部署防火墙后完成。在这种情况下，先部署 NSX-V 基本功能，然后再添加 VM 系列防火墙。

  在继续之前，您必须决定以安全为中心还是以运营为中心的部署适合 NSX-V 环境。本文档介绍了以安全为中心的部署过程。

  以安全为中心 — 创建指定 VM 系列防火墙配置的服务定义，创建动态地址组，并创建策略将流量重定向到 VM 系列防火墙。请参阅在以安全为中心的部署中创建安全组和指导规则。

  - （在 Panorama 上）设置映射到 NSX-V Manager 上的安全组的动态地址组。安全组可组合指定来宾/应用程序，以便将策略应用于该组。
  - （在 Panorama 上）创建安全策略规则以将流量重定向到 Palo Alto Networks 服务配置文件。

  运营中心 —（在 NSX-V Manager 上）创建安全组和策略以将流量重定向到 VM 系列防火墙。请参阅在以操作为中心的部署中创建安全组和控制规则。

  - （在 NSX-V Manager 上）设置安全组。安全组可组合指定来宾/应用程序，以便将策略应用于该组。
  - （在 NSX-V Manager 上）创建 NSX-V 版防火墙策略以将流量重定向到 Palo Alto Networks 服务配置文件。
- 步骤 5：监控和维持网络安全 — Panorama 可提供网络流量的综合图形视图。使用 Panorama 上的可见性工具，包括应用程序命令中心 (ACC)、日志和报告生成功能。利用这些工具可以集中分析、调查和报告全部网络活动，识别有潜在安全影响的区域，并将它们转化为安全应用程序启用策略。有关详细信息，请参阅《Panorama 管理员指南》。

以下附加任务不是主要 VM 系列 NSX-V 部署过程的必需部分，只有在部署需要时才应完成。

- 升级软件版本 — 升级 VM 系列 NSX-V 版防火墙时，您必须首先升级 Panorama，然后才能进行防火墙升级。要升级防火墙，请参阅 升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列）。

  - 对于在防火墙上升级 *PAN-OS* 版本，请勿在 *Panorama* > *VMware Service Manager* 中修改 *VM-Series OVA URL*（*VM* 系列 *OVA URL*）。
  - 切勿在 *VM* 系列 *NSX-V* 版防火墙上使用 *VMware* 快照功能。快照可能会影响性能并导致间歇性和不一致的数据包丢失。请参阅 *VMware* 使用快照的最佳实践建议。如果需要配置备份，则使用 Panorama 或防火墙上的 *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）即可在防火墙上导出活动配置 *(running-config.xml)*，且可使您能将其保存在任何网络位置。
- 将以操作为中心的配置迁移到以安全为中心的配置 — 如果将用于 NSX-V 部署的以操作为中心的现有 VM 系列防火墙进行升级，并打算继续使用以安全为中心的工作流程，请将以操作为中心的配置迁移到以安全为中心的配置。

如果需要从 NSX-V 部署中重新安装或删除 VM 系列，请参阅 如何从 VMware NSX-V 中删除 VM 系列集成知识库文章。

安装 VMware NSX 插件

要为 NSX 解决方案部署 VM 系列，必须在 Panorama 上安装 VMware NSX 插件。

© 2019 Palo Alto Networks, Inc.

如果当前安装了另一个版本的插件，请选择 *Install*（安装）将其删除，然后安装选定的版本。

STEP 1 | 下载插件。

1. 选择**Panorama** > **Plugins**（插件）。
2. 选择**Check Now**（立即检查）以检索可用的更新列表。
3. 在操作列中选择 **Download**（下载）以下载插件。
4. 选择插件的版本并在“操作”列中单击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

在 HA 对中的 Panorama 上安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，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。

STEP 2 | 如果要升级您当前版本的 VMware NSX 插件，请完成手动配置同步。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Managers**（服务管理器）。
2. 在 Action 列中选择 **NSX Config-Sync**（**NSX** 配置同步）。
3. 单击 **Yes**（是）。
4. 同步完成时，请单击 **OK**（确定）。

将 VM 系列防火墙注册为 NSX-V Manager 上的服务

您需要启用 Panorama 与 NSX-V Manager 之间的通信，然后在 NSX-V Manager 上将 VM 系列防火墙注册为服务。注册后，VM 系列防火墙将添加到网络服务列表中，NSX-V Manager 以透明方式将这些网络服务部署为服务。

- 启用 NSX-V Manager 与 Panorama 之间的通信
- 在 Panorama 上创建模板和设备组
- 在 Panorama 上创建服务定义

启用 *NSX-V Manager* 与 *Panorama* 之间的通信

要自动配置 NSX-V 的 VM 系列防火墙，请启用 NSX-V Manager 与 Panorama 之间的通信。此设置是一次性设置，并且仅当 NSX-V Manager 的 IP 地址更改或超出部署 VM 系列防火墙的容量许可证限制时，才需要修改此设置。

STEP 1 | （可选）对于 Panorama 与 NSX-V 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-V Manager 直接通信，同时保持其他服务的代理通信。此功能需要适用于 VMware NSX 2.0.5 的 Panorama 插件。

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。

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-V Manager 的访问权限。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Managers**（服务管理器），然后单击 **Add**（添加）。
2. 输入**Service Manager Name**（服务管理器名称）。

© 2019 Palo Alto Networks, Inc.

在 NSX-V Manager 上，此名称显示在 **Networking & Security**（网络和安全）> **Service Definitions**（服务定义）> **Service Managers**（服务管理器）上的服务管理器列中。

3. （可选）添加将 VM 系列防火墙标识为服务的 **Description**（说明）。
4. 输入用于访问 NSX-V Manager 的 **NSX Manager URL**（IP 地址或 FQDN）。
5. 输入 **NSX Manager Login**（**NSX Manager** 登录）凭据 — NSX Manager 上企业管理员角色的用户名和密码。这可以让 Panorama 通过 NSX-V Manager 进行身份验证。

   NSX-V Manager 帐户密码不支持特殊字符 *(&)*。如果密码包含 # 符号，则 *Panorama* 与 *NSX-V Manager* 之间的连接会失败。

   如果更改 *NSX-V 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* 和 *NSX-V Manager* 之间的连接。从与 *NSX-V Manager* 断开连接开始，*Panorama* 就再也不会收到有关部署更改的更新。
6. 单击 **OK**（确定）。

STEP 4 | 将更改提交到 Panorama。

选择 **Commit**（提交）和提交类型：**Panorama**。

STEP 5 | 验证 Panorama 上的连接状态。

Name	Description	NSX Manager URL	NSX Manager Login	Service Definitions	Status	Last Dynamic Update	Action
PAN-SERVICE-MANAGER		[redacted]	admin	PAN-SD-1	Registered	-	Synchronize Dynamic Objects NSX Config-Sync

要查看 Panorama 与 NSX-V Manager 之间的连接状态。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Managers**（服务管理器）。
2. 验证 **Status**（状态）列中的消息。

   连接成功时，状态显示为已注册。这表示，Panorama 和 NSX-V Manager 处于同步状态，并且 VM 系列防火墙已注册为 NSX-V Manager 上的服务。

   失败状态消息为：

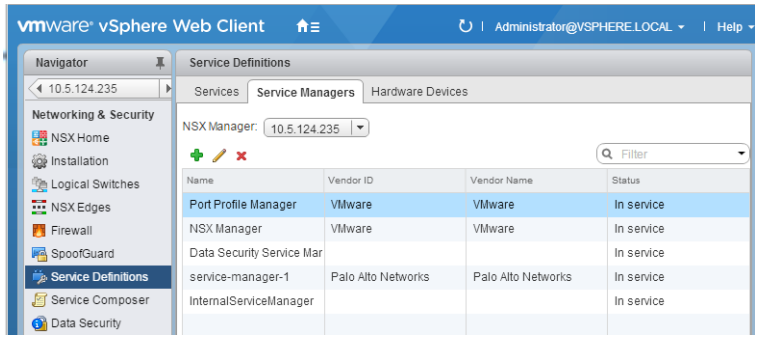
   - **Not connected**（未连接）：无法连接到 NSX-V Manager 或建立与 NSX-V Manager 的网络连接。
   - 无效凭据：访问凭据（用户名和/或密码）不正确。
   - **Out of sync**（不同步）：Panorama 上定义的配置设置与 NSX-V Manager 上定义的不同。单击该链接了解失败的具体原因。例如，NSX-V Manager 可能具有某项服务定义，其名称与 Panorama 上定义的名称相同。要修复此错误，请使用错误消息中列出的服务定义名称，以验证 NSX-V Manager 上的服务定义。在 Panorama 和 NSX-V Manager 未同步之前，您无法在 Panorama 上添加新的服务定义。
   - **No service/ No service profile**（无服务/无服务配置文件）：表示 NSX-V Manager 上的配置不完整。

   如果进行更改并需要手动同步，请参阅 9

STEP 6 | 验证防火墙是否已注册为 NSX-V Manager 上的服务。

1. 在 vSphere Web 客户端上，选择 **Networking & Security**（网络和安全）> **Service Definitions**（服务定义）> **Service Managers**（服务管理器）。

© 2019 Palo Alto Networks, Inc.



2. 验证 **Palo Alto Networks** 是否显示在可用于安装的服务列表中。

STEP 7 | 如果您运行的是 VMware NSX 插件 2.0.4 或更高版本，则可以将 Panorama 配置为自动将动态对象与 NSX-V Manager同步，就像发布 **Synchronize Dynamic Objects**（同步动态对象）一样。默认情况下，DAG 同步间隔处于禁用状态，且值设置为零 (0)。要启用 DAG 同步，请设置 1小时到 72 小时之间的时间间隔。将值设置为零会禁用 DAG 同步。要配置或禁用间隔，请完成以下过程。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令。

   request plugins vmware_nsx nsx_v dag-sync-interval interval <interval-in-hours>

   您可以使用以下 show 命令查看配置的值。

   show plugins vmware_nsx nsx_v dag-sync-interval

STEP 8 | （可选）在包含数万个 IP 地址的大型 NSX-V 环境中，允许 Panorama 有足够的时间从 NSX-V Manager 检索 IP 地址更新至关重要。您现在可以配置 Panorama 可以从 NSX-V Manager 检索更新的时间（最多 10 分钟）。默认情况下，Panorama 从 NSX-V Manager 获取 IP 地址更新时会等待最多两分钟（120 秒）。但是，如果 Panorama 在分配的两分钟内未检索到所有 IP 地址更新，则 Panorama 会超时且更新失败。

您可以通过 Panorama 错误日志确定是否遇到 cURL 调用失败。cURL 调用失败返回以下消息。

```
2019-05-23 06:50:15.780 -0700 ERROR: Curl call to NSX Manager failed
```

完成以下过程以增加 Panorama 必理更新的时间。此功能需要适用于 VMware NSX 2.0.5 的 Panorama 插件。

1. 登录到 Panorama 命令行界面。
2. 执行以下命令以设置 cURL 调用超时。您可以将超时设置为 30 秒到 600 秒（10 分钟）。

   admin@Panorama> request plugins vmware_nsx global curl-timeout timeout <seconds>

   如果 *Panorama* 是 *HA* 对的一部分，请在主动和被动 *Panorama* 对等上配置相同的超时值。

在 *Panorama* 上创建模板、模板堆栈和设备组

要使用 Panorama 管理 VM 系列 NSX-V 版防火墙，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。

© 2019 Palo Alto Networks, Inc.

并且在 Panorama 上的 NSX-V 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-V Manager 可以将流量重定向到 VM 系列防火墙。

属于与 NSX 相关的模板的每个虚拟线路区域均可作为 NSX-V Manager 上的服务组成系统的服务配置文件予以提供。在 Panorama 上创建与 NSX 相关的区域时，Panorama 会将区域作为模板堆栈配置的一部分推送至防火墙，然后防火墙会自动创建一对虚拟线路子接口，例如 ethernet1/1.3 和 etherent 1/2.3，以便为租户或子租户隔离流量。在防火墙上，您可以创建安全组和控制规则，以保护映射到区域且到达虚拟线路子接口对上的流量。

如果不熟悉 Panorama，请参阅《Panorama 管理员指南》了解有关设置 Panorama 的说明。

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）。

   在部署和配置防火墙后，这些防火墙将在 **Panorama** > **Managed Devices**（受管设备）下显示，并将在设备组中列出。
4. 单击 提交（**Commit**），选择 **Panorama** 作为 提交类型（**Commit Type**），以便将更改保存到 Panorama 上正在运行的配置。

STEP 2 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 输入唯一的名称和说明，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 | 添加模板堆栈。

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 **Descriptio**（说明）**n**，以标识模板堆栈。
3. 在模板下单击 **Add**（添加），然后选择在上面创建的模板。
4. 单击 **OK**（确定）。
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。

STEP 4 | 为每个模板创建区域。

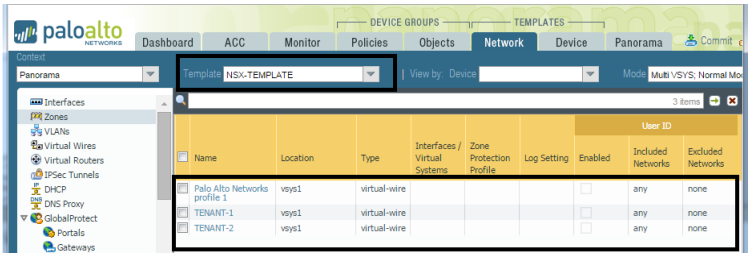
每个区域都映射到 NSX-V Manager 上的服务配置文件。要符合条件，区域必须是虚拟线路类型，并且是一个与服务定义关联的模板。

对于单租户部署，创建一个区域。如具备多租户部署，请为每个子租户创建一个区域。

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。

© 2019 Palo Alto Networks, Inc.



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-V Manager 上创建相应的服务配置文件。

在 *Panorama* 上创建服务定义

服务定义用于指定在 ESXi 群集中每个主机上安装的 VM 系列防火墙的配置。服务定义必须包括设备组、部署 VM 系列防火墙所用的许可证授权代码，以及带有一个或多个 NSX-V 服务配置文件区域的模板堆栈。通常，您会为 ESXi 群集中的 VM 系列防火墙创建一个服务定义。如果您拥有不同的 ESXi 群集，而且这些群集具有需要 VM 系列防火墙以不同方式来处理流量的工作负载，您可以在 Panorama 上创建多个服务定义。

在 Panorama 提交过程中，每个服务定义均会在 NSX-V Manager 上注册。在 NSX-V Manager 上注册的过程中，NetX API 实施会使每个区域（在模板堆栈中定义的区域）可供流量重定向使用。在部署 VM 系列防火墙时，您可以选择相应防火墙的配置文件名称，即您希望将其作为从 NSX-V 安全组中的对象重定向流量时的目标位置的防火墙。之后，经过适当配置的防火墙会检查流量，并通过属于 NSX-V 安全组的虚拟机执行策略。

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** > **NSX-V** > **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-V** > **Service Definitions**（服务定义）。
2. 选择 **Add**（添加）以创建新服务定义。服务定义名称最多允许 40 个字符。

   在 NSX-V Manager 上，此服务定义名称显示在**Networking & Security**（网络和安全）> **Service Definitions**（服务定义）> **Services**（服务）上的服务列中。
3. （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。

确保为每个模板堆栈创建区域。

© 2019 Palo Alto Networks, Inc.

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。这两个文件都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 OVF URL** 中，添加承载 ovf 文件的 Web 服务器的位置。http 和 https 均为支持协议。例如，输入 **https://acme.com/software/PA-VM-NSX.9.1.0.ovf**

选择与计划部署的 *VM* 系列型号相匹配的 *ovf* 文件。对于 *VM-200*，请使用 *vm100.ovf*。对于 *VM-1000-HV*，请使用 *vm300.ovf*。

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 群集中的 VM 系列防火墙上使用不同的 PAN-OS 版本。

STEP 5 | （可选）选择一个通知组。

为在虚拟环境和安全环境之间创建感知上下文，确保将策略一致地应用于流向防火墙的所有流量，选择需要在虚拟环境发生变化时使其接收通知的设备组。

在 **Notify Device Groups**（通知设备组）下拉列表中选择您希望启用通知的每个设备组。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。

指定设备组中包含的防火墙会收到安全组和 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。

STEP 6 | 保存服务定义并将其附加到服务管理器。

1. 单击 **OK**（确定）。
2. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Manager**（服务管理器），然后单击服务管理器名称的链接。
3. 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。
4. 单击 **OK**（确定）。
5. 选择 **Commit**（提交）和提交类型：**Panorama**。

   提交更改后，每个服务定义将会在 NSX-V Manager 上被注册为安全服务。

STEP 7 | 将授权代码添加到防火墙的许可证中。

授权代码必须适用于 *VM* 系列型号 *NSX* 包；例如，*PAN-VM-300-PERP- BND-NSX*。

验证订购量/容量是否足以支持您需要在网络中部署的防火墙数量。

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。

© 2019 Palo Alto Networks, Inc.

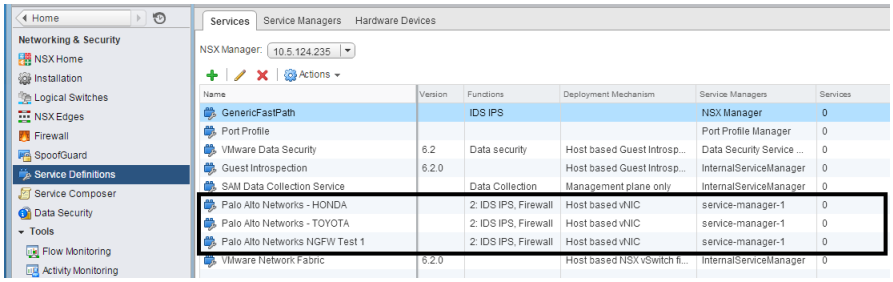
2. 在“动态添加设备属性”下，将您收到的授权代码添加到您的订单履行电子邮件中，并从“软件版本”下拉列表中选择一个 PAN-OS 软件版本。

   在 NSX-V 下部署新防火墙并将其添加到选定设备组时，将应用授权代码并将防火墙升级到选择版本的 PAN-OS。

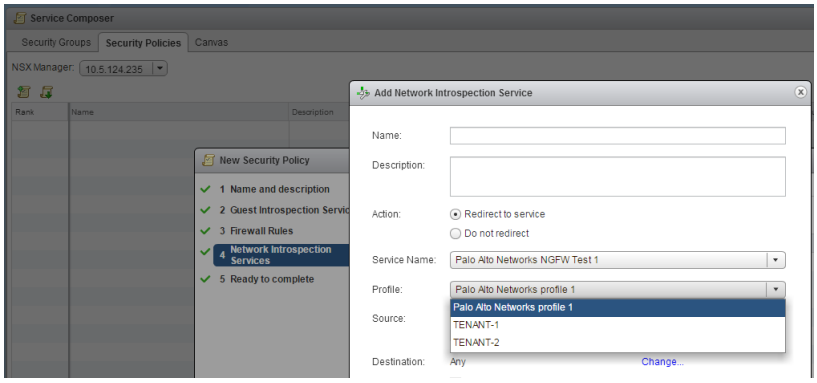
   在支持门户上，您可以查看经授权部署的防火墙的总数量，以及所用许可证的数量与授权代码启用的许可证的总数量的比率。
3. 同步 Panorama 与 NSX-V Manager 之间的配置。
   1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Managers**（服务管理器）。
   2. 在操作列中选择 **NSX Config-Sync**（**NSX** 配置同步）。
   3. 单击 **Yes**（是）以确认同步。

STEP 8 | 验证您在 Panorama 上定义的服务定义和 NSX-V 服务配置文件已在 NSX-V Manager 上进行了注册。

1. 在 NSX-V Manager 上，要验证服务定义的可用性，选择 **Networking & Security**（网络和安全）> **Service Definitions**（定义）> **Services**（服务）。服务定义作为 NSX-V Manager 上的一项服务被列出。



2. 要验证区域在 NSX-V Manager 上的可用性：
   1. 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Policies**（安全策略），然后单击 **Create Security Policy**（创建安全策略）。
   2. 选择 **Network Introspection Services**（网络自检服务），然后单击 **Add**（添加）。
   3. 在 **Service Name**（服务名称）下拉列表中，选择您已在之前步骤中验证过的 Palo Alto Networks 服务。
   4. 在 **Profile**（配置文件）下拉列表中，验证您可以查看您针对 Panorama 上的服务定义所定义的所有区域。



STEP 9 | （可选）同步 Panorama 和 NSX-V Manager 之间的配置。

如果添加或更新在 Panorama 上配置的服务定义，请在 **Panorama** > **VMware** > **NSX-V** > **Service Managers**（服务管理器）下的 Action（操作）列中选择 **NSX Config Sync**（**NSX** 配置同步），以在 NSX-V Manager 上同步更改。

© 2019 Palo Alto Networks, Inc.

如果 *Panorama* 上存在任何待决提交，该链接将变得不可用。

如果同步失败，查看详细信息，了解是在 Panorama 上还是 NSX-V Manager 上解决错误。举例来说，如果您删除了 Panorama 上的某个服务定义，但由于该服务定义已被 NSX-V Manager 上的某个规则所引用，导致其无法从 NSX-V Manager 上删除，同步将会失败，同时给出失败原因的错误消息。

部署 VM 系列防火墙

将 VM 系列防火墙注册为 NSX-V Manager 上的服务 (Palo Alto Networks NGFW)，并创建安全组和操作规则后，请在 NSX-V Manager 上完成以下任务。

- 定义 IP 地址池（（仅在未针对 DHCP 配备管理接口时需要）
- 准备用于 VM 系列防火墙的 ESXi 主机
- 部署 Palo Alto Networks NGFW 服务
- 启用大容量接收卸载

vSphere/NSX-V 环境中客户端虚拟机的 *vMotion* 的支持

当客户端 *VM* 从群集中的一个主机虚拟化移动到另一主机时，目标主机的 *NSX-V* 分布式防火墙会将所有的新会话引导至目标主机上的 *VM* 系列防火墙。为了确保所有的活动（现有会话）在客户段虚拟化移动过程中不发生中断，*NSX-V Manager* 会就现有的允许会话对 *VM* 系列防火墙进行轮询，然后与目标主机上 *NSX-V* 分布式防火墙共享这些会话。原 *VM* 系列防火墙允许的所有现有会话也将会被目标主机上的 *NSX-V* 分布式防火墙（筛选模块）所允许，而无需引导至目标主机 *VM* 系列防火墙，以防出现会话丢失。

VM 系列防火墙作为服务在群集中的每个主机上运行，因此从来都不会被虚拟化移动。

定义 *IP* 地址池

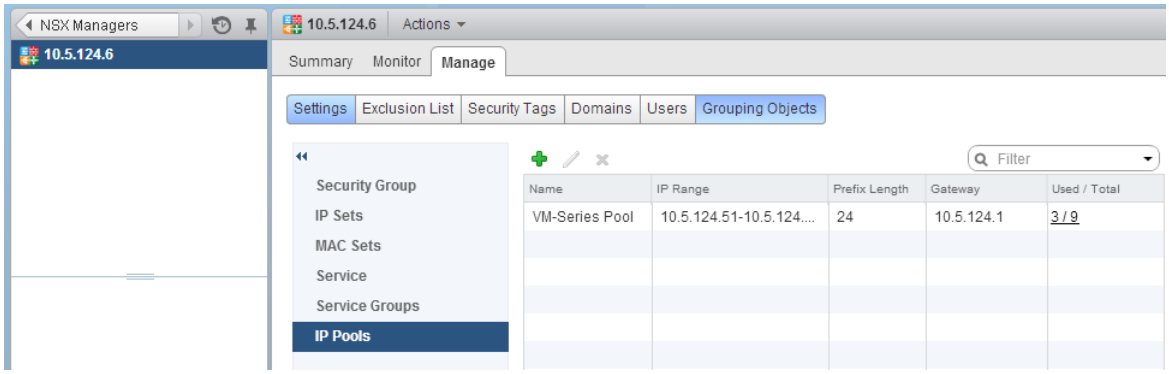
您可以配置 VM 系列防火墙上的管理接口，以便使用来自静态 IP 池的 IP 地址或使其成为一个 DHCP 客户端。

如果您选择使用 IP 池（为建立对 VM 系列防火墙的管理访问而预留的静态 IP 地址范围），则在 NSX-V Manager 部署新的 VM 系列防火墙时，该范围内的第一个可用 IP 地址将会被分配至防火墙的管理接口。

STEP 1 | 在 **Networking & Security Inventory**（网络和安全目录）中，选择 **NSX Manager**，然后双击以打开 NSX-V Manager 的配置详细信息。

STEP 2 | 选择 **Manage**（管理）> **Grouping Objects**（分组对象）> **IP Pools**（IP 池）。

STEP 3 | 单击 **Add IP Pool**（添加 IP 池），并指定屏幕中请求的网络访问权限详细信息，包括要用于 Palo Alto Networks NGFW 的静态 IP 地址的范围。

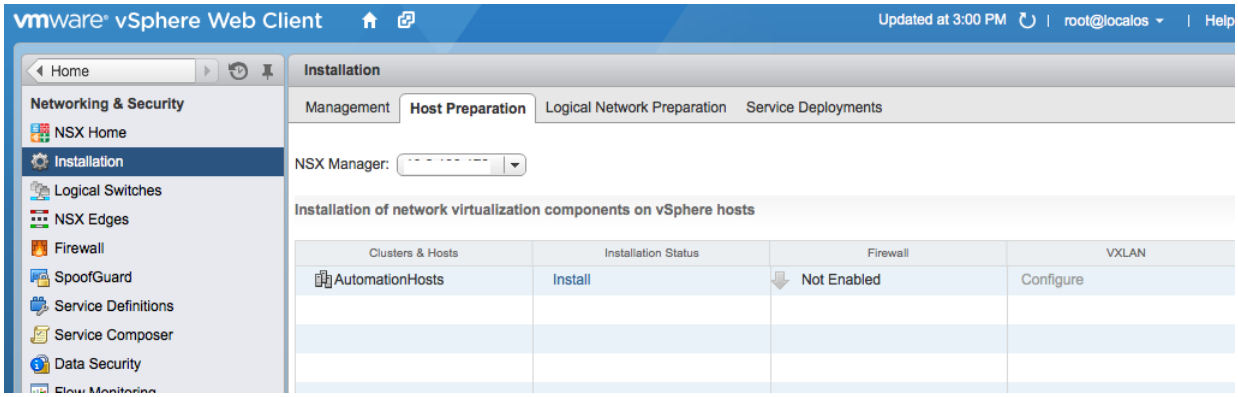


© 2019 Palo Alto Networks, Inc.

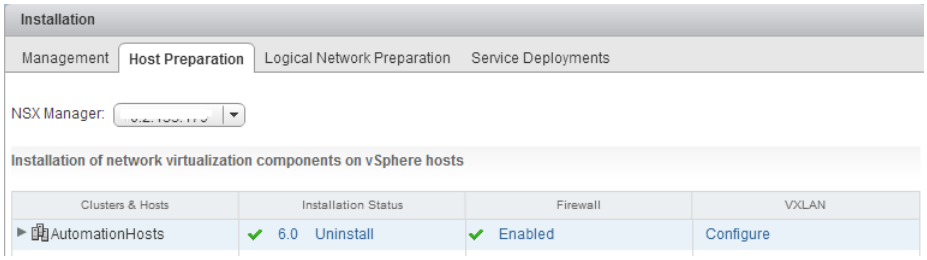
准备用于 *VM* 系列防火墙的 *ESXi* 主机

在部署 VM 系列防火墙之前，群集中的每个主机必须具有必需的 NSX-V 组件，以便 NSX-V 防火墙和 VM 系列防火墙共同协作。NSX-V Manager 将安装部署 VM 系列防火墙所需的组件 — Ethernet 适配器模块 (.eam) 和 SDK。

STEP 1 | 在 NSX-V Manager 上，选择 **Networking and Security**（网络和安全）> **Installation**（安装）> **Host Preparation**（主机准备）。

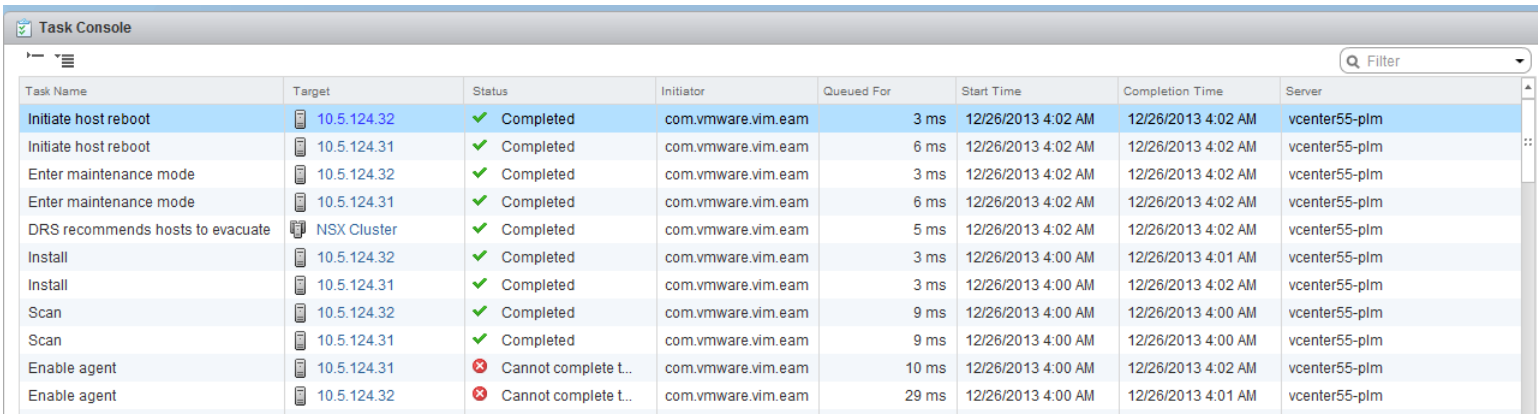


STEP 2 | 单击 **Install**（安装），然后验证安装状态是否为成功。



当新 *ESXi* 主机添加到群集中时，此过程自动执行，并且必需的 *NSX-V* 组件将自动安装到 *ESXi* 主机上的每个来宾上。

STEP 3 | 如果安装状态为未就绪或在屏幕上显示一个警告，则单击**Resolve**（解析）链接。要监控重新安装尝试的进度，请单击**More Tasks**（更多任务）链接，并查询以下任务是否成功完成：



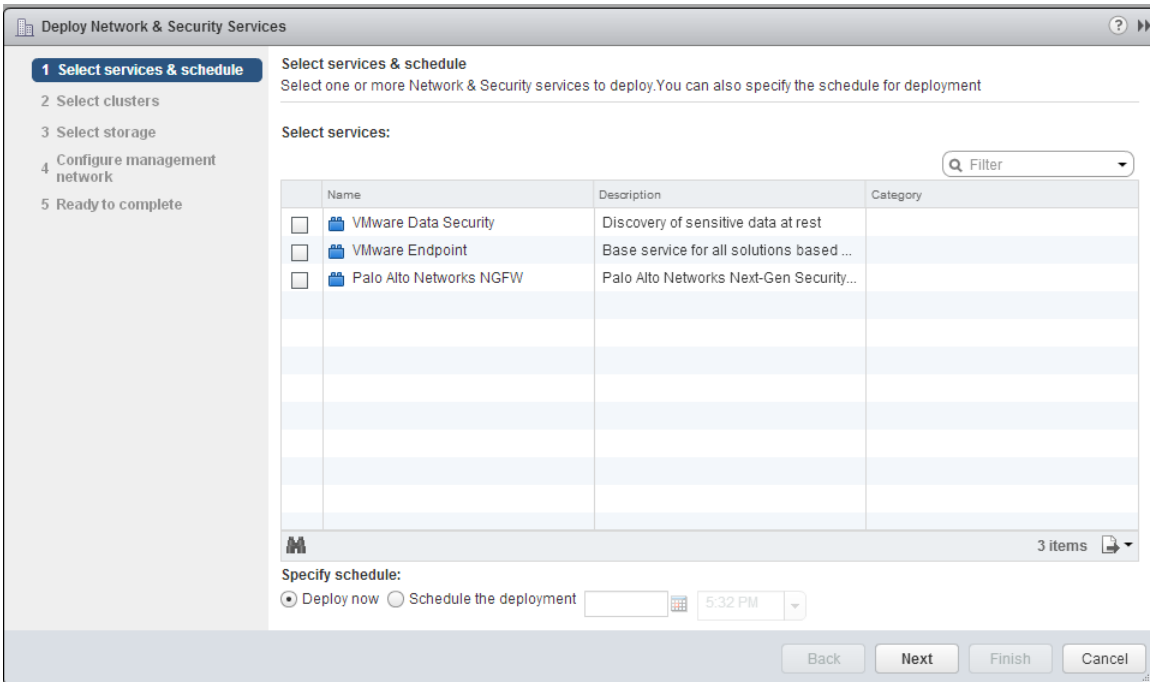
部署 *Palo Alto Networks NGFW* 服务

使用以下步骤自动执行在指定群集的每个 ESXi 主机上部署 VM 系列防火墙 NSX-V 版实例的过程。

© 2019 Palo Alto Networks, Inc.

STEP 1 | 选择 **Networking and Security**（网络和安全）> **Installation**（安装）> **Service Deployments**（服务部署）。

STEP 2 | 单击 **New Service Deployment**（新服务部署）（绿色加号图标），然后选择您想要部署的 Palo Alto Networks 下一代防火墙的服务定义，在本示例中，即：**Palo Alto Networks NGFW** 服务。单击 **Next**（下一步）。

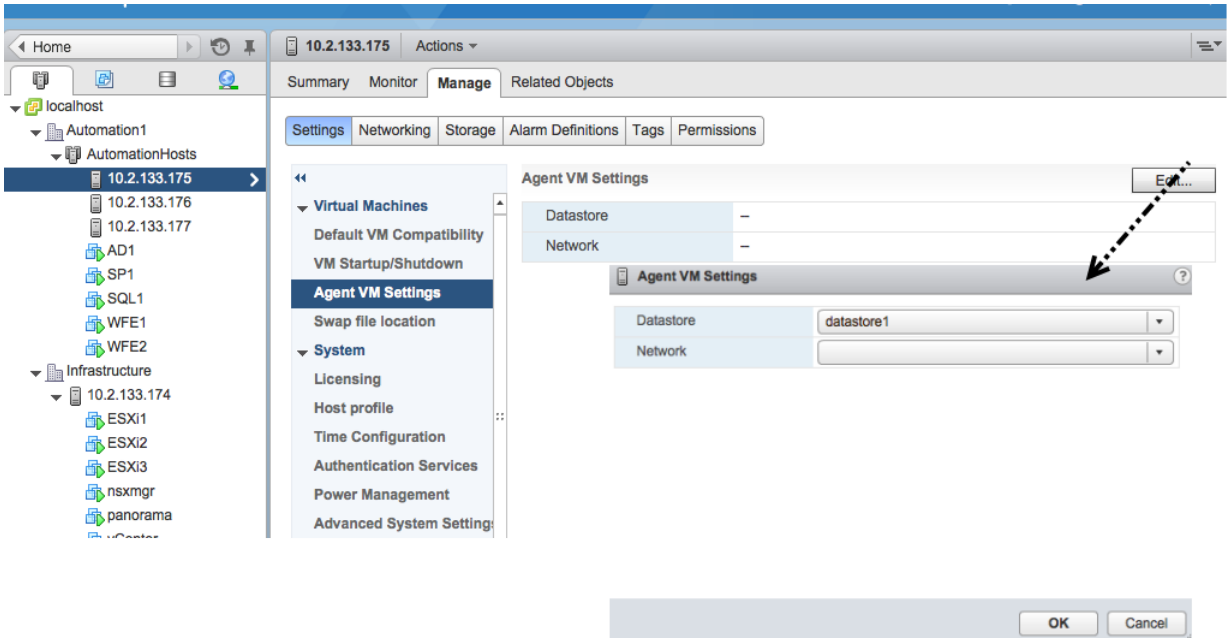


STEP 3 | 选择 **Datacenter**（数据中心）和将部署服务的群集。防火墙的一个实例将被部署到所选群集的每个主机上。

STEP 4 | 选择分配防火墙的磁盘空间所用的数据存储。根据您的部署选择以下选项之一：

- 如果已为群集分配共享存储，则选择一个可用的共享数据存储。
- 如果尚未为群集分配共享存储，则选择 **Specified-on-host** 选项。请务必在群集中的每个 ESXi 主机上选择存储。并且选择用于 VM 系列防火墙上的管理流量的网络。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 选择为防火墙提供管理网络流量访问权限的端口组。

STEP 6 | 选择 IP 地址池分配。

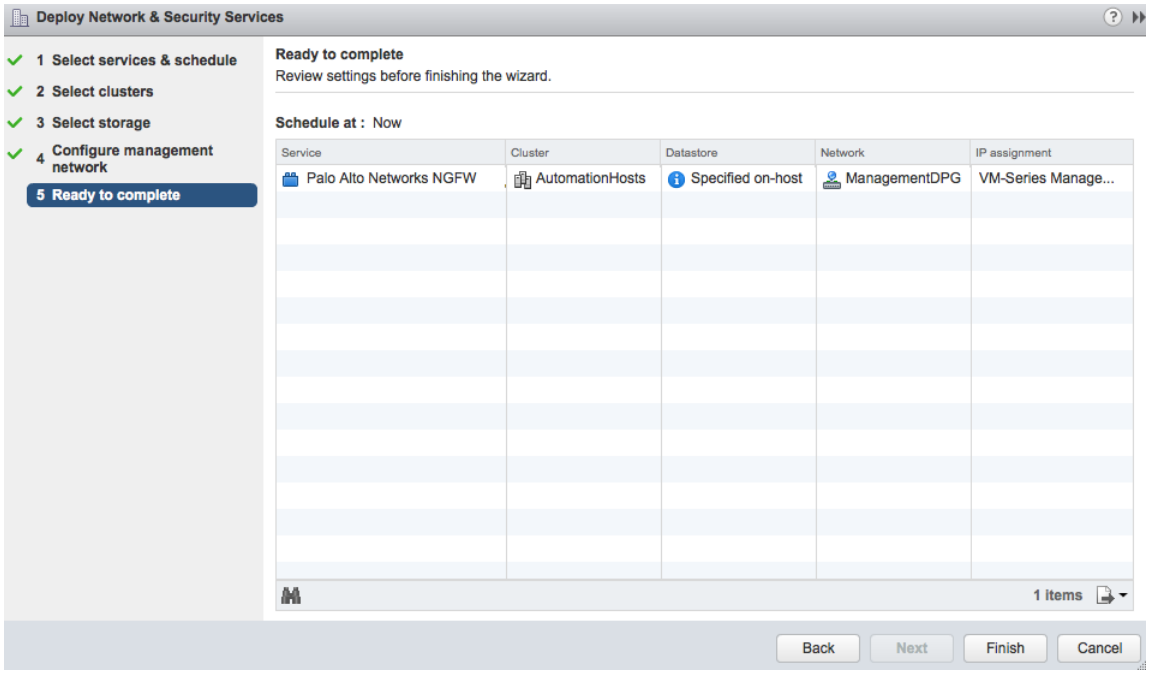
- **Use IP Pool**（使用 **IP** 池）（定义 IP 地址池），在部署时从中为每个防火墙分配管理 IP 地址。
- **Use DHCP**（使用 **DHCP**），使用管理接口上的 DHCP。

如果使用*IP*池，则在部署时，*Panorama*上 *VM* 系列防火墙的显示名称将包含*ESXi*主机的主机名。例如：*PA-VM:10.5.1.120.*

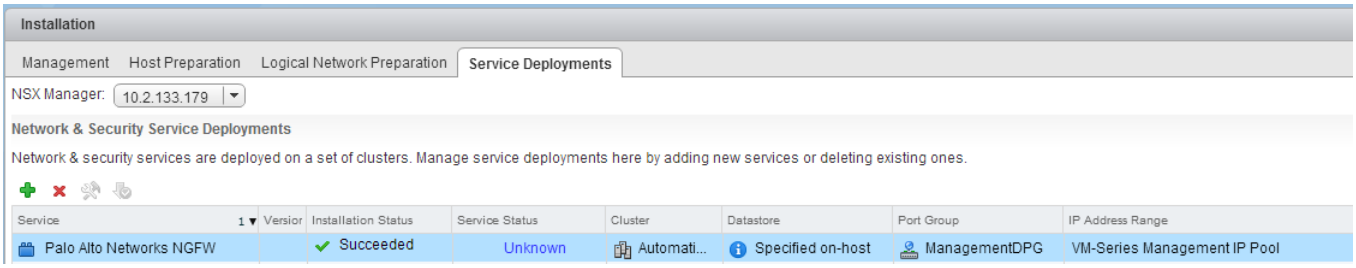
如果使用DHCP，则 VM 系列防火墙的显示名称不包含ESXi主机的名称。

STEP 7 | 检查配置，然后单击 **Finish**（完成）。

© 2019 Palo Alto Networks, Inc.



STEP 8 | 验证 NSX-V Manager 是否将 **Installation Status**（安装状态）报告为 **Successful**（成功）。此过程需要一段时间；在 vCenter 上单击 **More tasks**（更多任务）链接可监控安装进度。



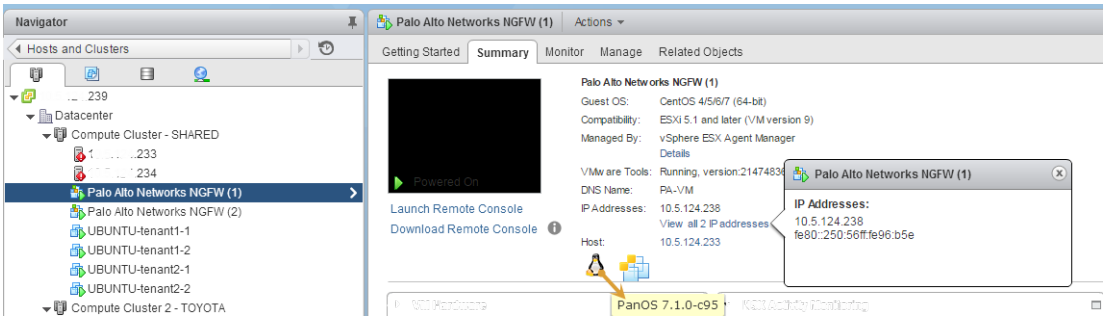
如果 *VM* 系列安装失败，则会在安装状态列上显示错误消息。您还可以使用 *NSX-V Manager* 上的 *Tasks*（任务）选项卡和 *Log Browser*（日志浏览器）查看失败的详细信息，有关故障排除步骤，请参阅 *VMware* 文档。

STEP 9 | 验证是否已成功部署防火墙。

1. 在 vCenter 服务器中，选择 **Hosts and Clusters**（主机和群集）以检查群集中的每个主机是否有一个防火墙实例。
2. 直接通过 vCenter 服务器查看管理 IP 地址和防火墙上运行的 PAN-OS 版本。VMware 工具与 PAN-OS 软件映像绑定，在您启动 VM 系列防火墙时会自动启用。

   借助 VMware 工具，您可以查看硬盘、内存和 CPU 的资源利用指标，然后使用这些指标启用 vCenter 服务器上的警报或操作。通过检测信号，您可以验证防火墙处于活动状态，且可以触发操作来确保高可用性。您还可以通过 vCenter 上的关机功能正常关闭和重启防火墙。

© 2019 Palo Alto Networks, Inc.

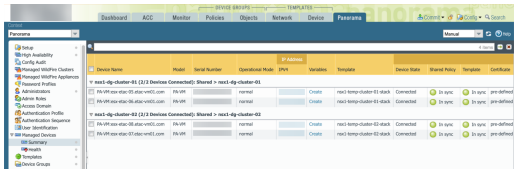


STEP 10 | 访问 Panorama Web 界面以确保 VM 系列防火墙已与 Panorama 连接和同步。

1. 选择 **Panorama** > **Managed Devices**（受管设备）以验证是否已连接和同步这些防火墙。

   如果防火墙从IP池获取其IP地址，那么 **Display Name**（显示名称）防火墙包括部署它的ESXi服务器的主机名，例如 PA-VM：ESX1.Sydney。如果防火墙获得 DHCP 分配的 IP 地址，则不会显示 ESXi 服务器的主机名。

   如果 *ESXi* 服务器的主机名长度超过 *32* 个字符，则该主机名将不会显示在 *Panorama* 中。相反，仅显示 *PA-VM*。



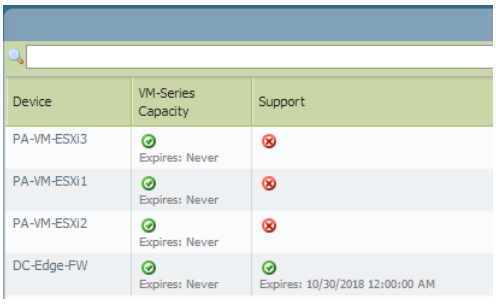
2. 单击 Commit（提交），选择 **Panorama** 作为提交类型。

   需要 *Panorama* 定期提交才能确保 *Panorama* 将设备序列号保存到配置中。如果在不提交更改的情况下重新启动 *Panorama*，则受管设备不会重新连接到 *Panorama*；虽然设备组将显示设备列表，但这些设备不会显示在 *Panorama* > *Managed Devices*（受管设备）中。

STEP 11 | 验证是否已应用容量许可证，并应用已购买的所有额外的许可证。至少必须激活每个防火墙上的支持许可证。

如果 *Panorama* 不能访问 *Internet*（脱机），您必须手动许可每个防火墙，然后将防火墙的序列号添加到 *Panorama* 中，以便将其注册为一台受管设备，之后可以从 *Panorama* 中推送相应的模板堆栈和设备组设置。请参阅激活适用于 VMware NSX 的 VM 系列防火墙的许可证，了解更多信息。

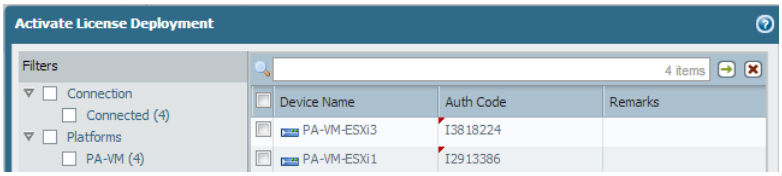
1. 选择 **Panorama** > **Device Deployment**（设备部署）> **Licenses**（许可证）以验证是否已应用 VM 系列容量许可证。



2. 在 VM 系列防火墙上应用额外的许可证：

© 2019 Palo Alto Networks, Inc.

- 在 **Panorama** > **Device Deployment**（设备部署）> **Licenses**（许可证）上单击 **Activate**（激活）。
- 查找或筛选防火墙，在 **Auth Code**（授权代码）列中，输入激活许可证的授权代码。对于每个防火墙，一次只能输入一个授权代码。

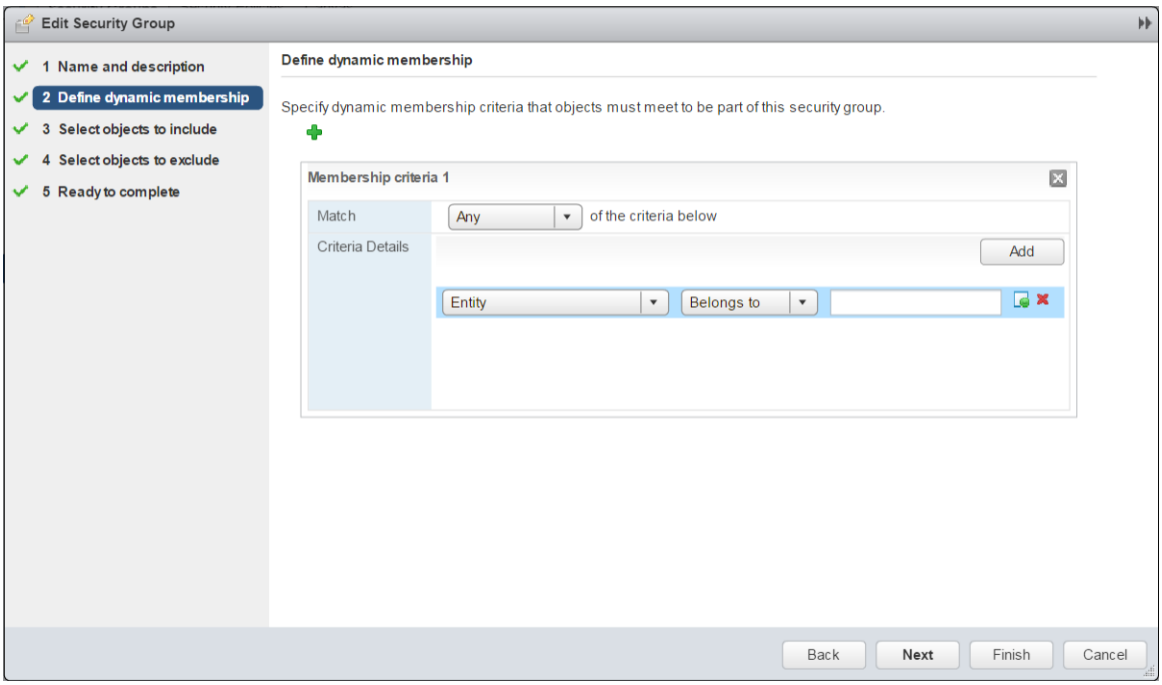


3. 单击激活，验证许可证激活结果是否成功。

STEP 12 | （可选）在 VM 系列防火墙上升级 PAN-OS 版本，请参阅升级 PAN-OS 软件版本（适用于 NSX 的 VM 系列）。

STEP 13 | 将来宾虚拟机添加到正确的安全组，以便将这些虚拟机的流量重定向到 VM 系列防火墙。

1. 登录到 vCenter。
2. 选择 **Networking & Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组）。
3. 突出显示要分配来宾虚拟机的安全组，然后单击 编辑安全组 图标。
4. 选择 **Define dynamic membership**（定义动态成员）并单击 + 图标。
5. 单击 **Add**（添加）。
6. 定义来宾虚拟机必须符合所选安全组的一部分的动态成员资格条件。您使用的标准取决于您的网络部署。例如，您可以选择由实体（例如逻辑交换机或分布式端口组）分组 VM。



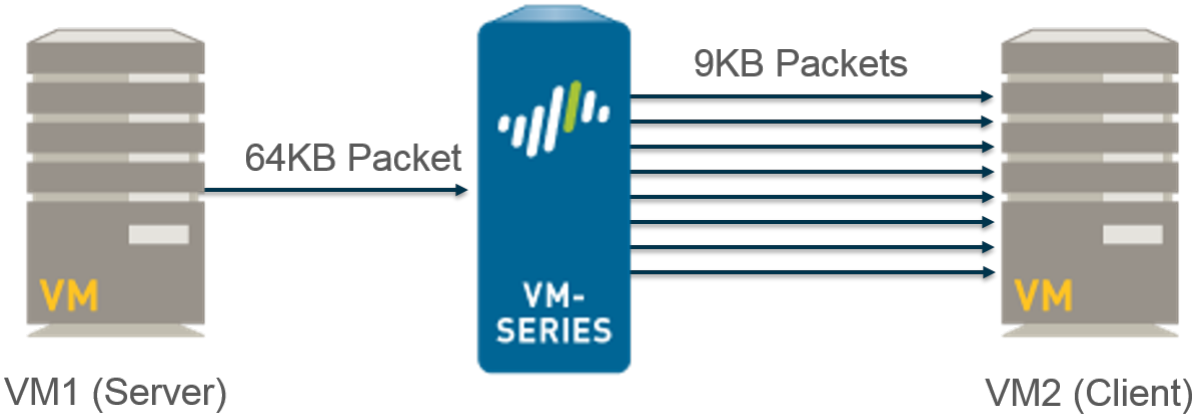
7. 单击 **Finish**（完成）。
8. 对于应将其流量重定向到 VM 系列防火墙的每个安全组重复此过程。

启用大容量接收卸载

大容量接收卸载 (LRO) 是一种通过降低 CPU 开销来增加高带宽网络连接上入站吞吐量的技术。如果没有 LRO，防火墙会丢弃大于配置的最大传输单元 MTU 的数据包，当防火墙启用巨型帧时，最大数量为 9216

© 2019 Palo Alto Networks, Inc.

字节。启用 LRO 后，防火墙将接收最大为 64KB 的数据包，并且不丢弃大于配置的 MTU 的数据包。相反，它将较大的数据包分割成 9000 个字节的较小数据块。例如，如果 VM1 向 VM2 发送 64KB 数据包，数据包被分成八段。



默认情况下，在新的 NSX-V 部署和升级时，LRO 处于禁用状态。您可以启用或禁用 LRO 并通过 CLI 查看 LRO 状态。在 VM 系列防火墙上启用LRO会自动启用巨型帧。此外，必须在 VM 系列防火墙主机上的VMXNET3网络适配器上启用LRO和TCP分段卸载（TSO）。

STEP 1 | 验证主机上是否启用了大容量接收卸载和 TCP 分段卸载。

有关主机上的 LRO 和 TSO 的信息，请参阅 VMware vSphere 文档。

1. 登录到 vSphere 并导航到您的主机。
2. 选择 管理 > 设置 > 系统 > 高级系统设置。
3. 找到以下参数并验证它们的值是否设置为 1。1 表示该参数在 VMXNET3 适配器上启用。
   - 对于 LRO—Net.Vmxnet3HwLRO
   - 对于 TSO—Net.UseHwTSO 和 Net.UseHwTSO6

STEP 2 | 在 VM 系列防火墙上启用 LRO。

1. 访问防火墙 CLI。
2. 使用以下命令启用 LRO：

```
admin@PA-VM> set system setting lro enable
```

3. 使用以下命令重启防火墙：

```
> request restart system
```

4. 使用以下命令验证 LRO 是否已启用：

```
admin@PA-VM> show system setting lro
Device LRO mode:                          on
Current device mtu size:                  9192
```

可以使用 ***set system setting lro disable*** 命令禁用 *LRO*。

© 2019 Palo Alto Networks, Inc.

创建安全组和控制规则

以下主题介绍如何创建安全组和策略以将流量引导至 VM 系列防火墙。按照下面的链接匹配您的部署流程 — 以安全为中心或以操作为中心。

- 在以安全为中心的部署中创建安全组和指导规则
- 在以操作为中心的部署中创建安全组和控制规则

在以安全为中心的部署中创建安全组和指导规则

以下主题介绍如何在 Panorama 上创建策略以将流量引导至 VM 系列防火墙。要使 VM 系列防火墙保护流量，必须完成以下任务：

- 在 Panorama 上设置动态地址组
- 在 Panorama 上创建控制规则

在 **Panorama** 上设置动态地址组

安全组是一个逻辑容器，可组合群集中多个 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-V Manager 上将创建相应的安全组。创建管理和保护来宾所要求的安全组；要了解安全组如何支持策略实施，请参阅使用动态地址组实施策略。

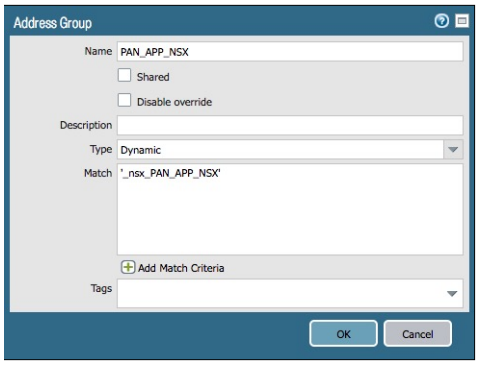
STEP 1 | 为您的部署所需的每个安全组配置一个动态地址组。

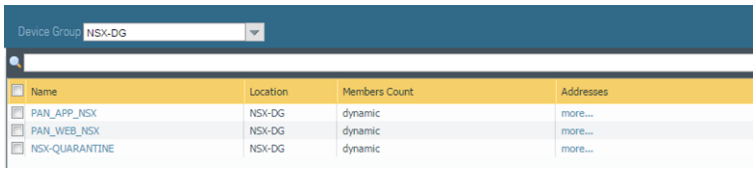
适用于 *VMware NSX-V* 的 *VM* 系列不支持共享动态地址组。

1. 选择 **Object**（对象）> **Address Groups**（地址组）。
2. 验证您是否在与 NSX-V 服务定义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-V 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*_nsx_*，后跟地址组的确切名称。例如，**'_nsx_PAN_APP_NSX'**。

6. 对于需要的每个安全组，请重复执行此流程。

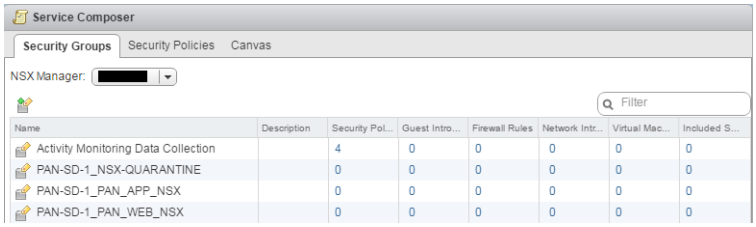




STEP 2 | 验证是否在 NSX-V Manager 上创建了相应的安全组。

© 2019 Palo Alto Networks, Inc.

1. 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组）。
2. 验证您的动态地址组是否在安全组列表中显示为安全组。每个安全组都以您的服务定义作为前缀，后跟一个下划线和动态地址组名称。



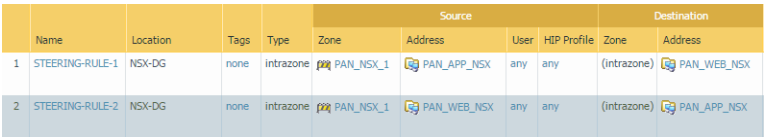
在 **Panorama** 上创建控制规则

如果您不了解规则在 NSX-V Manager 上以及在 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。要在 Panorama 上创建策略，并将其推送到 VM 系列防火墙，请参阅将策略应用于 VM 系列防火墙。

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-V Manager 上创建相应的控制规则。

STEP 1 | 创建安全策略。

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-V 服务定义关联的设备组中配置动态地址组。
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-V 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。
6. 在“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-V 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。
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。

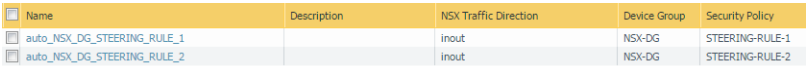


STEP 2 | 生成控制规则。

Panorama 为每个符合条件的安全策略规则生成一个控制规则。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Steering Rules**（控制规则）。
2. 选择 **Auto-Generate Steering Rules**（自动生成控制规则）。

   Panorama 将根据服务定义中附加的设备组中的合格安全策略规则填充控制规则列表。



3. （可选）修改 NSX-V 流量方向并将 NSX-V 服务添加到控制规则。

© 2019 Palo Alto Networks, Inc.

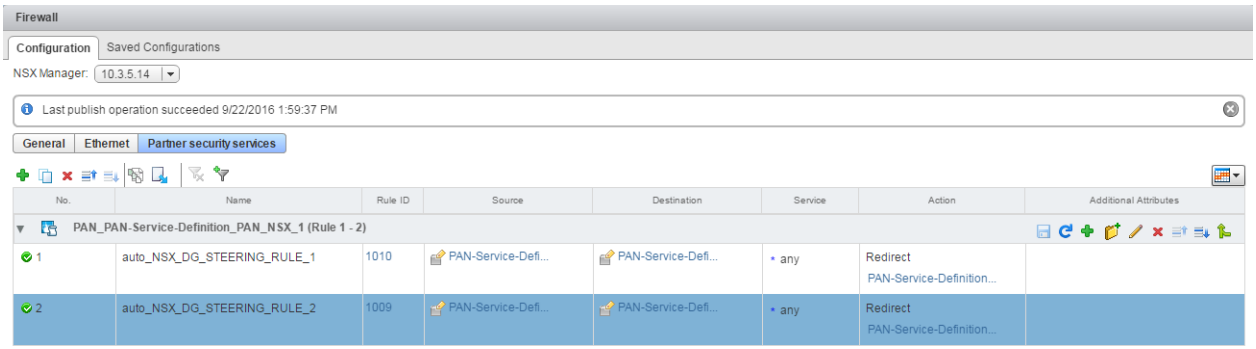
默认情况下，NSX-V 流量方向设置为 **inout**（进出）并且没有选择 NSX-V 服务。如果未指定 NSX-V 服务，则任何类型的流量都会重定向到 VM 系列防火墙。

1. 选择要修改的自动生成控制。
2. 要更改通讯方向，请从 **NSX Traffic Direction**（**NSX** 流量方向）下拉菜单中选择方向。
3. 在 NSX 服务下单击 **Add**（添加）并从 **Services**（服务）下拉菜单中选择服务。重复此步骤可添加其他服务。
4. 单击 **OK**（确定）。

4. 如果您已删除任何控制规则，请单击 **Auto-Generate Steering Rules**（自动生成控制规则），然后提交更改。
5. **Commit**（提交）更改。

STEP 3 | 验证是否在 NSX-V Manager 上创建了相应的流量控制规则。

1. 选择 **Network and Security**（网络和安全）> **Firewall**（防火墙）> **Configuration**（配置）> **Partner Security Services**（合作伙伴安全服务）。
2. 确认您在 Panorama 上创建的流量控制规则已列出。



在以操作为中心的部署中创建安全组和控制规则

在以操作为中心的部署中，您可以在 NSX-V Manager 而不是 Panorama 上创建安全组和流量重定向规则。然后，您在 Panorama 上配置的安全规则强制重定向到 VM 系列防火墙。在以操作为中心的部署中部署适用于 NSX-V 的 VM 系列防火墙时，请完成以下任务：

- #unique_159/unique_159_Connect_42_id17ADFI002L3
- #unique_160/unique_160_Connect_42_id17ADFI0H04S

在 **NSX-V Manager** 上设置安全组

安全组是一个逻辑容器，可组合群集中多个 ESXi 主机中的来宾。创建管理和保护来宾所要求的安全组；要了解安全组如何支持策略实施，请参阅使用动态地址组实施策略。

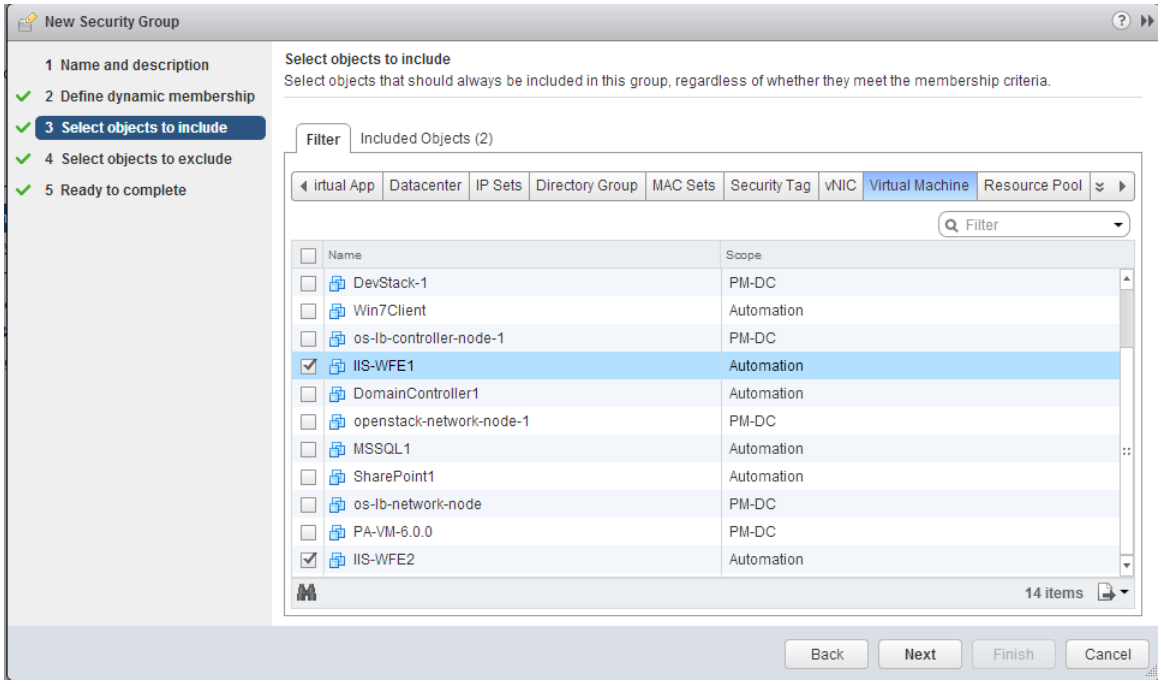
STEP 1 | 登录到 vSphere 用户界面。

STEP 2 | 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组），然后添加 **New Security Group**（新安全组）。

STEP 3 | 添加 **Name**（名称）和**Description**（说明）。在 Panorama 上定义动态地址组时，此名称将显示在匹配条件列表中。

STEP 4 | 选择构成安全组的来宾。您可以动态或静态添加成员。您可以通过匹配安全标记（推荐）**Define Dynamic Membership**（动态定义成员）或静态 **Select the Objects to Include**（选择包含的对象）。在以下屏幕截图中，已使用 **Objects Type:Virtual Machine**（对象类型：虚拟机）选项选择属于安全组的来宾。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 检查详细信息，然后单击 **OK**（确定）以创建安全组。

在**NSX-V Manager**上创建控制规则

如果您不了解规则在 NSX-V Manager 上以及在 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。要在 Panorama 上创建策略，并将其推送到 VM 系列防火墙，请参阅将安全策略应用于 VM 系列防火墙。

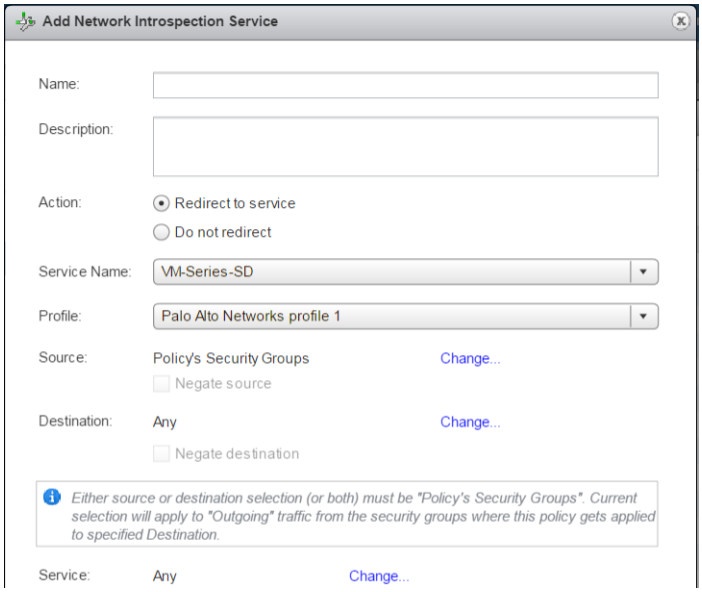
STEP 1 | 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Policies**（安全策略），然后单击 **Create Security Policy**（创建安全策略）()。

STEP 2 | 添加规则 **Name**（名称）。

STEP 3 | 添加网络自检服务。

1. 选择 **Network Introspection Service**（网络反省服务）并单击绿色加号图标。
2. **Name**（名称）网络内省服务并添加一个 **Description**（描述）。
3. 选择 **Redirect to Service**（重定向到服务）在行动。
4. 在服务名称下选择您的服务定义。
5. 在配置文件下选择服务配置文件。
6. 选择一个 **Source**（资源）和 **Destination**（目的地）。默认情况下，流量源设置为策略的安全组。该选项动态地包含应用此策略的所有安全组。或者，您可以选择将来自任何源的流量重定向到防火墙，或指定某些安全组。但是，vSphere 要求将 Source 或 Destination（或两者）设置为 Policy 的安全组。如果您为目标选择任意或特定安全组，则必须将源设置为策略的安全组。
7. （可选）选择要重定向到防火墙的特定网络服务。如果您选择任何服务或服务，则所有其他流量都不会重定向到防火墙。
8. 单击 **OK**（确定）。
9. 重复步骤 1 至 6 以添加其他网络自检服务。
10. 单击 **Finish**（完成）以保存您的配置。

© 2019 Palo Alto Networks, Inc.



STEP 4 | 将重定向策略应用于安全组。

1. 通过单击安全策略以突出显示。
2. 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Policies**（安全策略），然后单击 Apply Security Policy（应用安全策略）()。
3. 通过检查所有适当的区域来应用重定向规则。
4. 单击 **OK**（确定）。

将安全策略应用于 VM 系列防火墙

现在您已在 Panorama 上创建了控制规则并将其推送到 NSX-V Manager，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。

STEP 1 | 登录到 Panorama。

STEP 2 | （仅限以操作为中心的部署）创建动态地址组。

跳过此步骤以进行以安全为中心的部署。如果要执行以安全为中心的部署，则表示已创建动态地址组。

在 NSX-V Manager 上创建安全重定向规则后，Panorama 上将提供安全策略中引用的安全组的名称。

适用于 *VMware NSX-V* 的 *VM* 系列不支持共享动态地址组。

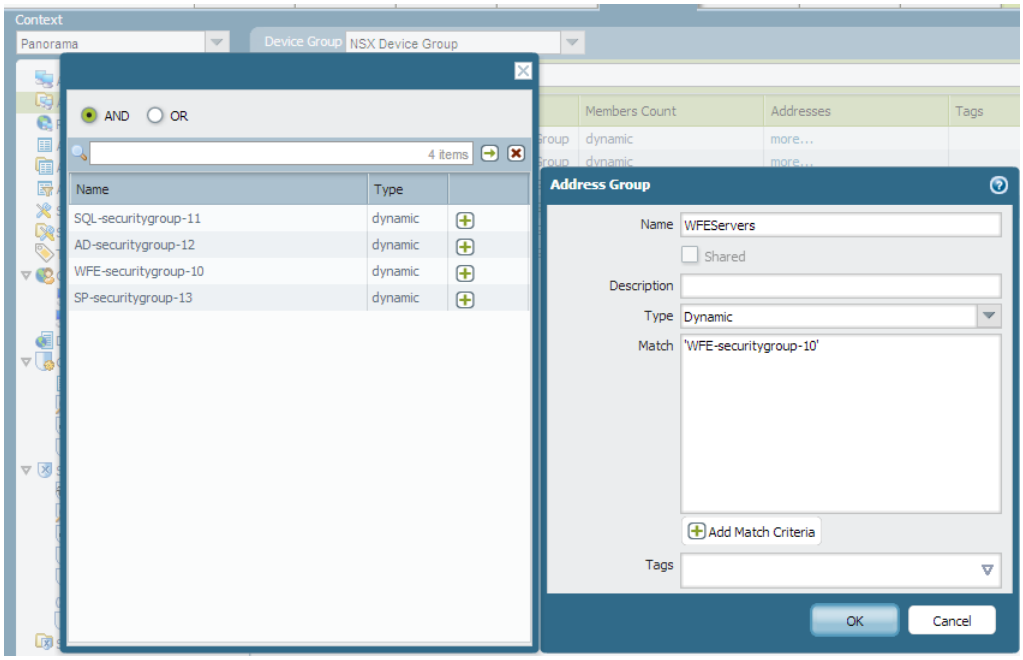
1. 选择 **Object**（对象）> **Address Groups**（地址组）。
2. 从 **Device Group**（设备组）下拉列表中选择为了在 NSX-V 防火墙上管理 VM 系列而创建的设备组。
3. 单击 **Add**（添加），然后为动态地址组输入 **Name**（名称）和 **Description**（说明）。
4. 选择 **Dynamic**（动态）作为 **Type**（类型）。
5. 将匹配条件添加到动态地址组。

© 2019 Palo Alto Networks, Inc.

某些浏览器扩展程序可能会阻止 *Panorama* 与 *NSX-V* 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。

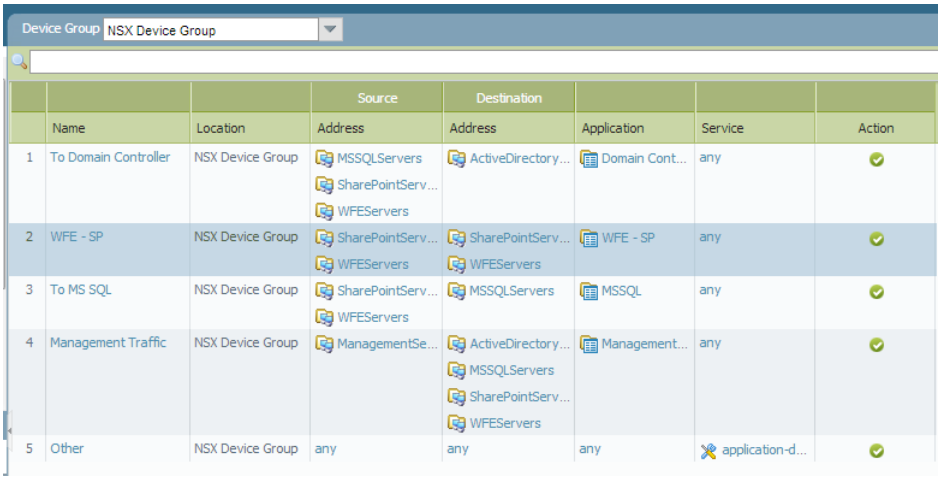
6. 单击 **Add Match Criteria**（添加匹配条件）。
7. 选择 **And** 或 **Or** 运算符，并单击安全组名称旁边的加号 (+) 图标，将其添加到动态地址组。

显示在匹配条件对话框中的安全组派生自在 *Distributed Firewall Partner Security Service*（分布式防火墙合作伙伴安全服务）或 *NSX-V Manager* 上的 *Service Composer*（服务组合系统）中定义的组。此时仅安全策略中引用的安全组和流量重定向到 *VM* 系列防火墙的源安全组可用。



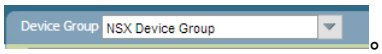
8. 单击 **OK**（确定）。
9. 重复这些步骤可创建部署所需的适当数量的动态地址组。
10. **Commit**（提交）更改。

STEP 3 | 创建安全策略规则。



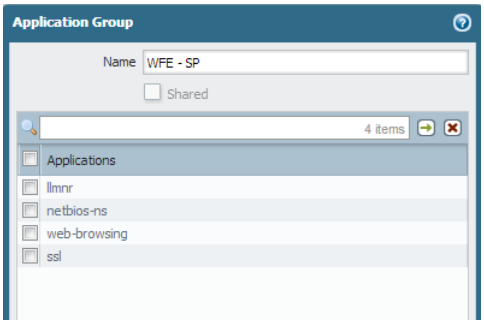
1. 选择 **Policies**（策略）> **Security**（安全）> **Prerules**（预订规则）。

© 2019 Palo Alto Networks, Inc.

2. 选择在将 VM 系列防火墙注册为 NSX-V Manager 上的服务中为 NSX-V 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。

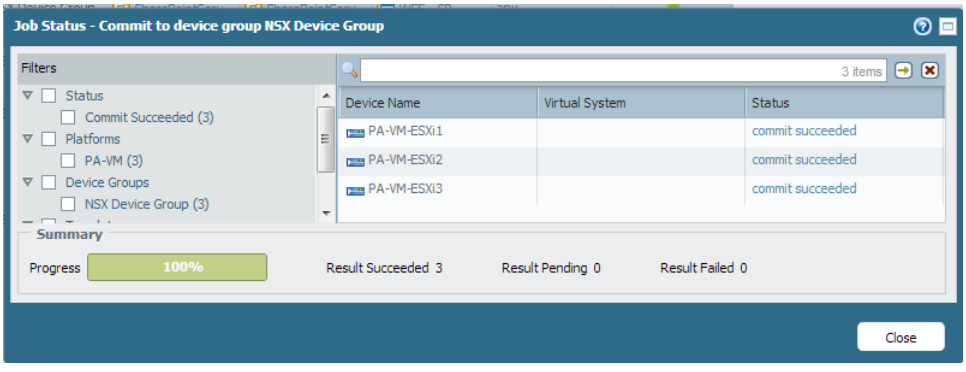
6. 选择允许的 **Application**（应用程序）。在本例中，我们创建 **Application Group**（应用程序组），其中包含已组合在一起的一组静态特定应用程序。
   1. 单击 **Add**（添加），然后选择 **New Application Group**（新建应用程序组）。
   2. 单击 **Add**（添加）以选择要包含到组中的应用程序。在本示例中，我们选择以下应用程序：
   3. 单击 **OK**（确定）以创建应用程序组。



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 VM 系列 NSX-V 版防火墙。

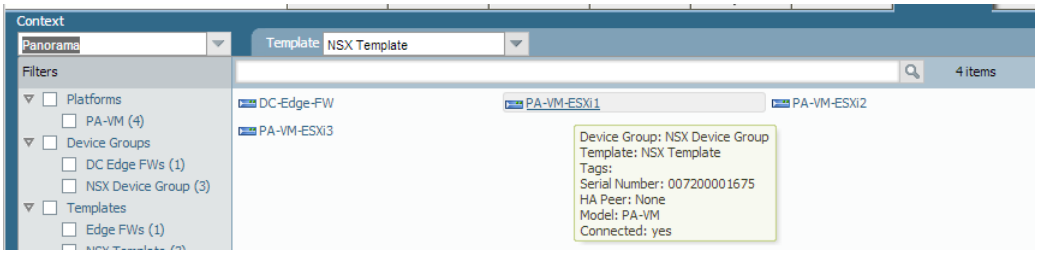
1. 单击 **Commit**（提交），选择 **Device Groups**（设备组）作为提交类型。
2. 选择设备组（在本例中选择 NSX-V 设备组），然后单击 **OK**（确定）。
3. 验证提交是否成功。



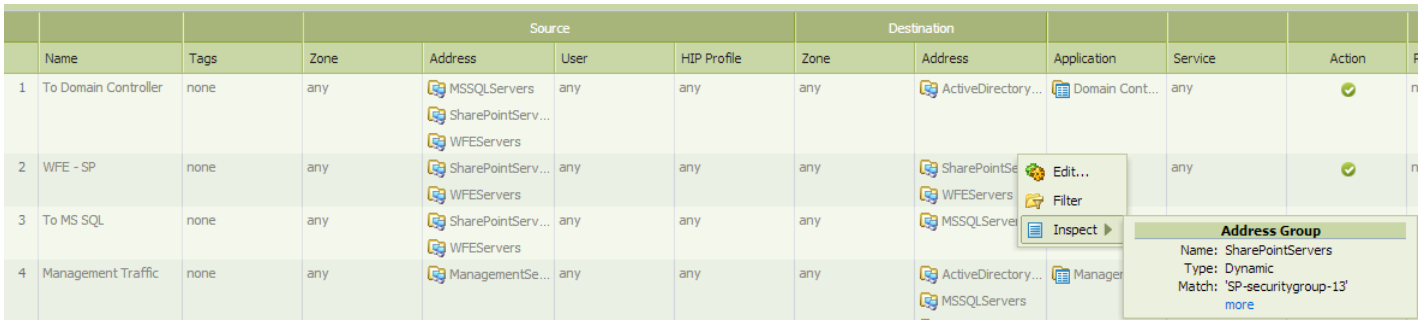
STEP 5 | 在 VM 系列防火墙上验证是否已填充动态地址组的成员。

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。

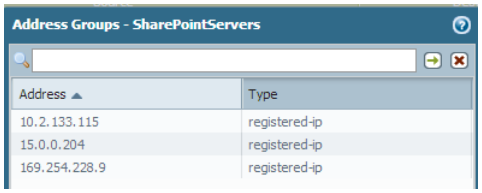
© 2019 Palo Alto Networks, Inc.



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。

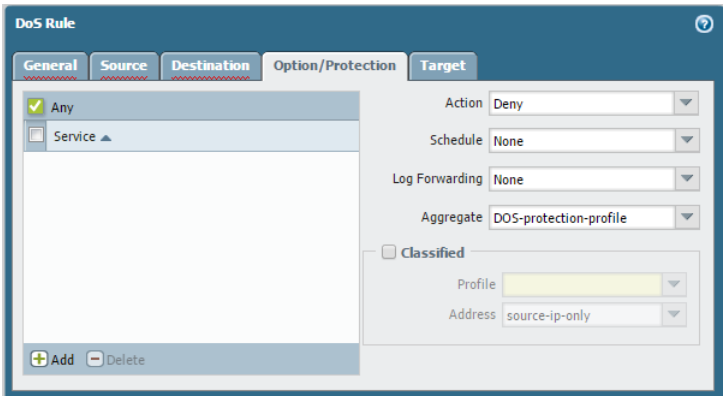
STEP 8 | 创建 DoS 保护配置文件并将其附加至 DoS 保护策略规则。

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。

© 2019 Palo Alto Networks, Inc.

- 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。



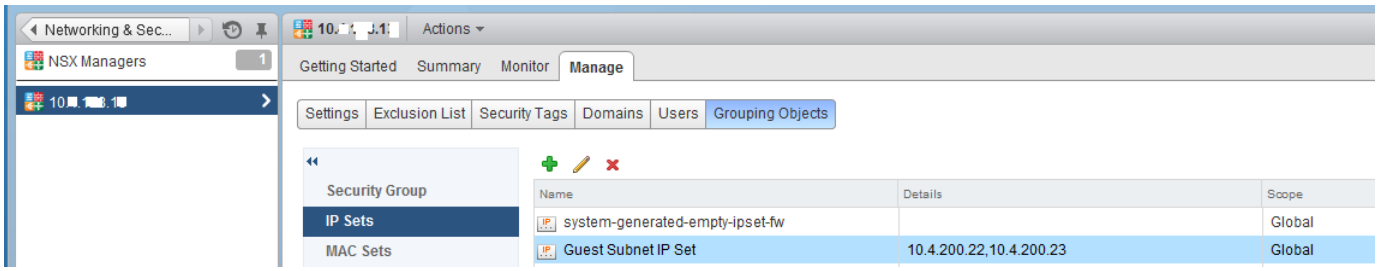
控制来自不运行 VMware 工具的来宾的流量

VMware 工具包含一个实用程序，可让 NSX-V Manager 收集在群集中运行的各个来宾的 IP 地址。NSX-V Manager 使用 IP 地址作为控制流量流向 VM 系列防火墙的匹配条件。如果在各个来宾上没有安装 VMware 工具，则来宾的 IP 地址不适用于 NSX-V Manager 且无法控制流量流向 VM 系列防火墙。

以下步骤可让您手动设置来宾而不使用 VMware 工具，这样可以让 VM 系列防火墙管理来自各个来宾的流量。

STEP 1 | 创建包括由 VM 系列防火墙保护的来宾的 IP 地址集。此 IP 地址集将用作下述步骤 2 中 NSX-V 分布式防火墙规则的源对象或目标对象。

1. 选择 **NSX Manager** > **Manage**（管理）> **Grouping Objects**（分组对象）> **IP Sets**（**IP** 地址集）。
2. 单击 **Add**（添加），并输入没有安装 VMware 工具且需要 VM 系列防火墙保护的各个来宾的 IP 地址。使用逗号分隔单个 IP 地址；IP 范围或子网无效。



STEP 2 | 将 IP 地址集附加到 NSX-V 上的安全组以执行策略。

1. 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组）。
2. 选择 **Select objects to include**（选择包含的对象）> **IP Sets**（**IP** 地址集），然后添加要包含的 IP 地址集对象。

VM 系列防火墙 NSX-V 版上的多 NSX Manager 支持是什么？

VM 系列防火墙 NSX-V 版上的多 NSX Manager 支持允许您将单个 Panorama 连接到运行单个 vCenter 服务器的多个 NSX-V Manager。使用单个 Panorama 可让您管理通用对象和策略并在多个 vCenter 服务器之间同步它们。您现在可以在一个位置配置和管理多个 NSX-V Manager，从而无需在多台 Panorama 服务器上多次复制常用配置。

© 2019 Palo Alto Networks, Inc.

- 计划您的多 NSX 部署
- 在多 NSX Manager 环境中部署 VM 系列防火墙

计划您的多 *NSX* 部署

您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。

- 配置您的设备组—设备组是根据需要相似策略配置的共同点对防火墙进行分组的逻辑单元。每个服务定义都需要一个设备组，每个设备组只能在一个服务定义中被引用。

  设备组从设备组层次结构中的设备组上继承策略规则和对象设置。这使您可以在父设备组中配置通用或共享设置，并在子设备组或孙设备组中设置唯一设置。默认情况下，Panorama 具有共享设备组，并且共享设备组中的任何配置都会推送到所有设备组。在配置任何策略规则或对象设置时，请确认您已选择正确的设备组。

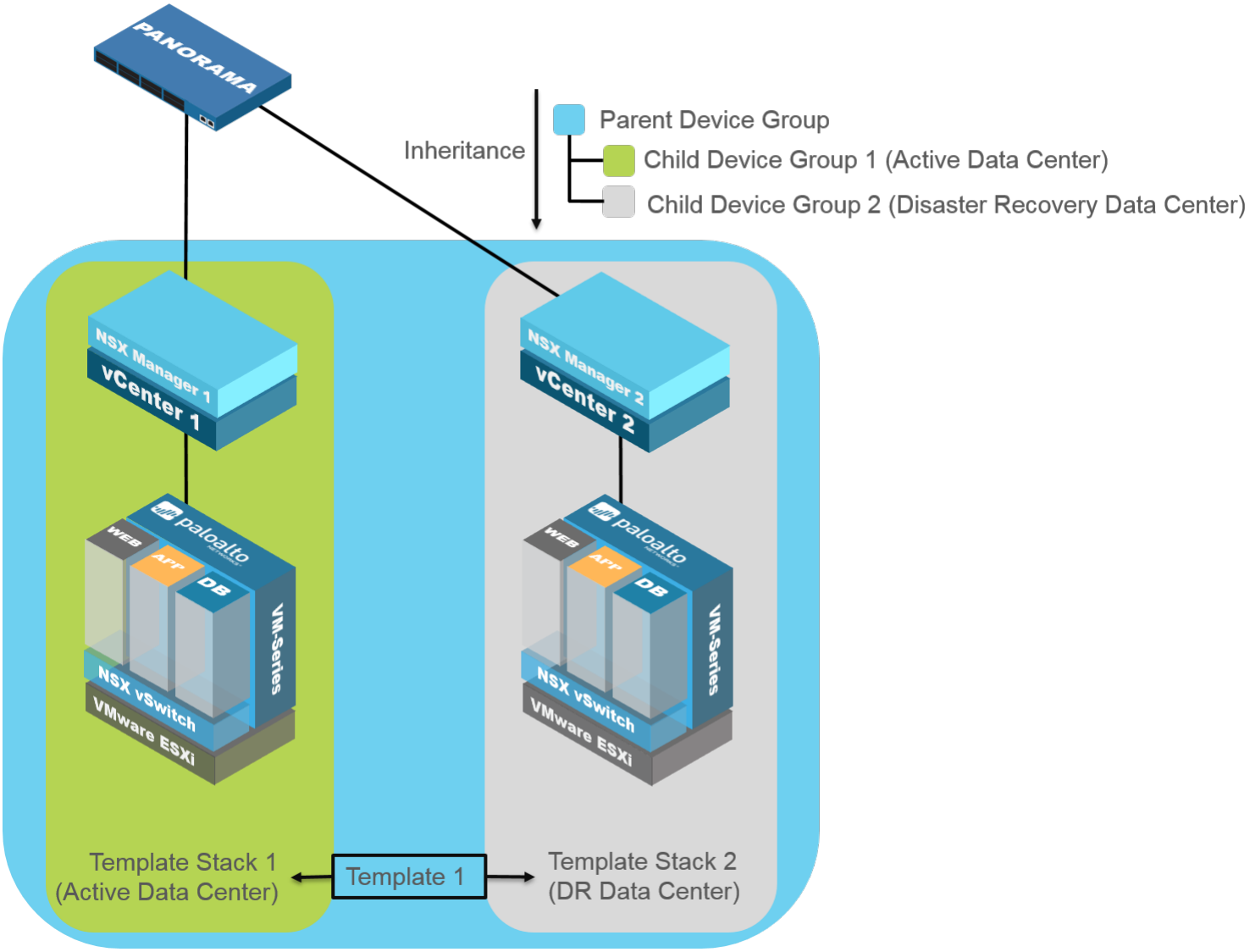
  有关配置和管理设备组的信息，请参阅 Panorama 管理员指南中的管理设备组。
- 配置您的模板堆栈 — 模板堆栈包含使防火墙能够连接到您的网络的设置，例如接口和区域配置。每个服务定义都需要一个模板堆栈，每个模板堆栈只能在一个服务定义中被引用。

  将模板堆栈分配给服务定义时，请考虑堆栈中模板的优先级，以确保将正确的配置推送到正确的防火墙。如果堆栈中的模板包含重叠配置，则优先级较高的模板优先，下层模板中的相同设置将被忽略。因此，请确保 NSX-V Manager 特有的模板配置在分配给该 NSX-V Manager 服务定义的模板堆栈中具有更高的优先级。

  有关配置和管理模板堆栈的信息，请参阅 Panorama 管理员指南中的管理模板和模板堆栈。
- 创建服务定义 — 服务定义用于指定在 ESXi 集群中每个主机上安装的 VM 系列防火墙的配置。每个单独的 NSX-V Manager 配置至少需要一个服务定义。服务管理器可以有多个服务定义，但每个服务定义只能由一个设备组和一个模板堆栈。将设备组或模板堆栈分配给服务定义后，您将无法再为将来服务定义选择该设备组或模板堆栈。

例如，在灾难恢复部署方案中，您需要为每个数据中心创建相同的设备组。由于数据中心的所有策略规则和对象都相同，因此您可以在单个设备组中执行所有配置。但是，您不能在两个服务定义中使用相同的设备组。为确保每个数据中心都获得相同的策略规则，请为具有通用配置的设备组下的每个数据中心创建一个子设备组。这些子设备组不需要任何自己的配置，因为它们从父设备组继承 VM 系列防火墙所需的所有内容。并且因为每个数据中心都是相同的，请在模板中配置您的网络设置（模板 1）。为每个数据中心创建一个模板堆栈并将模板 1 分配给每个堆栈。

© 2019 Palo Alto Networks, Inc.



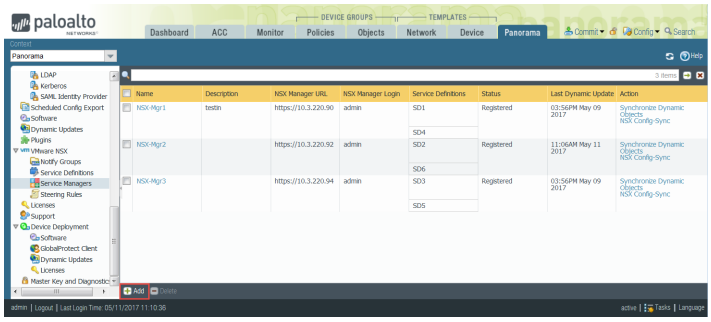
在多 *NSX Manager* 环境中部署 *VM* 系列防火墙

无论您是部署单个 NSX-V Manager 还是多 NSX Manager 环境，在继续使用 Panorama 设置下一个 NSX-V Manager 之前，请设置 NSX-V Manager 与 Panorama 之间的连接。

STEP 1 | 安装 VMware NSX 插件 2.0 版本，因为它允许您最多连接 16 个 NSX-V Manager。对于 Panorama 上的 NSX-V 配置，此版本的插件允许您为 VM 系列防火墙添加多个服务管理器。

STEP 2 | #unique_151/unique_151_Connect_42_id17ADEL00MNX。

© 2019 Palo Alto Networks, Inc.

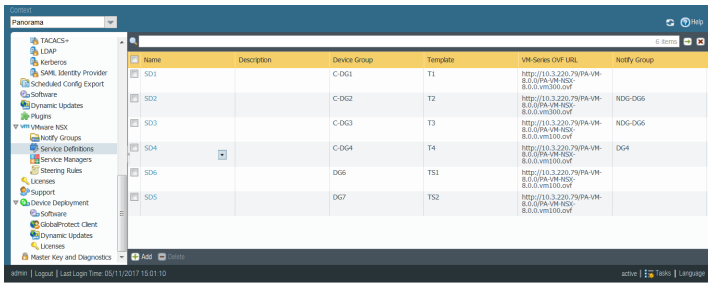


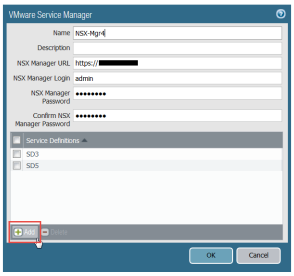
STEP 3 | 在 Panorama 上创建模板和设备组.设备组和模板堆栈将安全策略和网络设置推送到每个 ESXi 群集中的 VM 系列防火墙。

配置策略规则和对象时，请确认您已选择正确的设备组。

在配置网络和设备设置时，请确认您已选择正确的模板堆栈。

STEP 4 | 在 Panorama 上创建服务定义 并将它们附加到服务管理器。每个服务定义都可以引用一个设备组和一个模板堆栈。Panorama 在所有服务管理器中最多支持 32 个服务定义。





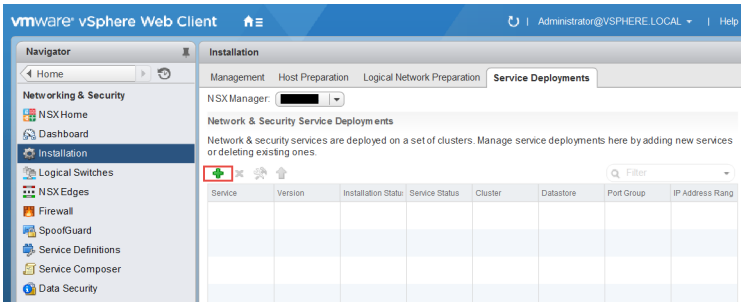
STEP 5 | 配置动态地址组或安全组，并将流量重定向到 VM 系列防火墙。

- 对于以安全为中心的部署 在 Panorama 上设置动态地址组 和 在 Panorama 上创建控制规则。
- 对于以操作为中心的部署在 NSX-V Manager 上设置安全组和在NSX-V Manager上创建控制规则。

确认您选择了正确的设备组，以便将正确的控制规则发送到相应的 NSX-V Manager。

STEP 6 | 使用相关的服务定义在每个 ESXi 集群上部署 Palo Alto Networks NGFW 服务。

© 2019 Palo Alto Networks, Inc.



STEP 7 | 对于每个 NSX-V Manager，请重复执行此流程。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Managers**（服务管理器），然后单击 **Add**（添加）。
2. 启用 NSX-V Manager 与 Panorama 之间的通信。

动态隔离感染的来宾

PAN-OS 中的威胁和流量日志包括 NSX-V 部署中来宾虚拟机的源或目标通用唯一标识符 (UUID)。这使得 NSX-V 的 VM 系列可以支持使用 NSX-V 安全标记标记的来宾虚拟机。在来宾 VM 的 UUID 现在包含在日志事件后，基于筛选的日志事件的防火墙可以通过 NSX-V Manager API 标记受影响的来宾 VM。这允许在 NSX-V 环境中自动定位被感染的虚拟机。然后，NSX-V 可以将所有关联的 UUID 置于策略下，以隔离网络其余部分的这些虚拟机。

Panorama 在 HTTP 服务器配置文件中包含用于威胁和流量日志的预定义负载格式。这些有效负载格式对应于 NSX -V 中的预定义安全标记。在威胁或流量日志中找到来宾虚拟机后，Panorama 会向 NSX-V Manager 发出 API 调用，通知 NSX-V Manager 使用 HTTP 服务器配置文件中指定的标记来标记来宾虚拟机。标记来宾虚拟机后，NSX-V Manager 将标记的来宾虚拟机动态移动到隔离安全组中，该组将来宾虚拟机置于隔离区动态地址组中。

STEP 1 | 确认在 Panorama 上已安装内容更新版本 636 或更高版本。

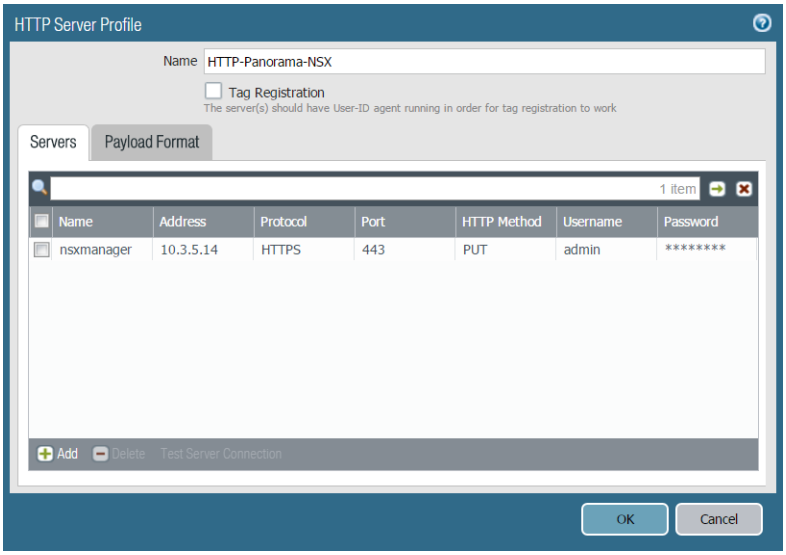
STEP 2 | 创建一个动态地址组作为您的隔离区动态地址组。

Name	Location	Members Count
PAN_APP_NSX	NSX-DG	dynamic
PAN_WEB_NSX	NSX-DG	dynamic
NSX-QUARANTINE	NSX-DG	dynamic

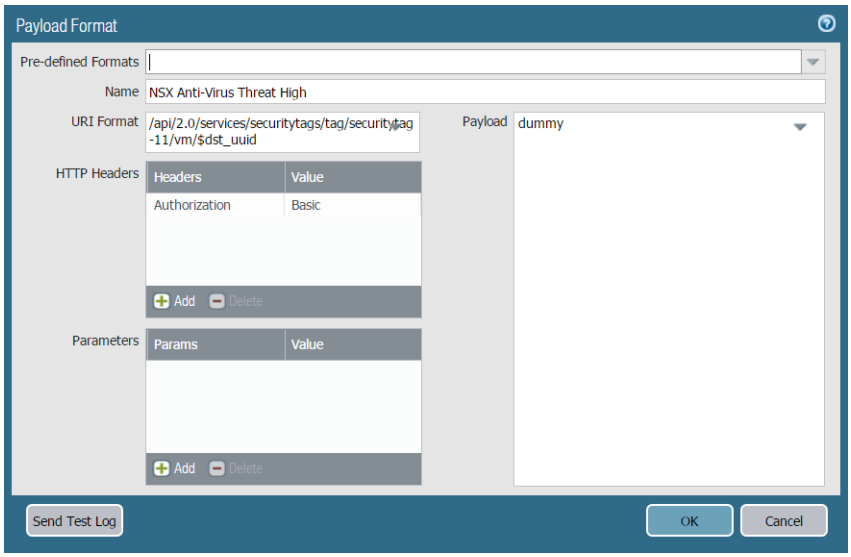
STEP 3 | 创建 HTTP 服务器配置文件以将 API 调用发送到 NSX-V Manager。

1. 选择 **Panorama** > **Server Profiles**（服务器配置文件）> **HTTP**，并 **Add**（添加）新的 HTTP 服务器配置文件。
2. 输入描述性的 **Name**（名称）。
3. 选择 **Add**（添加）以提供 NSX-V Manager 的详细信息。
4. 输入 NSX-V Manager 的 **Name**（名称）。
5. 输入 NSX-V Manager 的 **IP Address**（IP 地址）。
6. 选择协议（HTTP 或 HTTPS）。默认端口分别为 80 或 443。
7. 在 HTTP Method（HTTP 方法）列下选择 PUT。
8. 输入 NSX-V Manager 的用户名和密码。

© 2019 Palo Alto Networks, Inc.



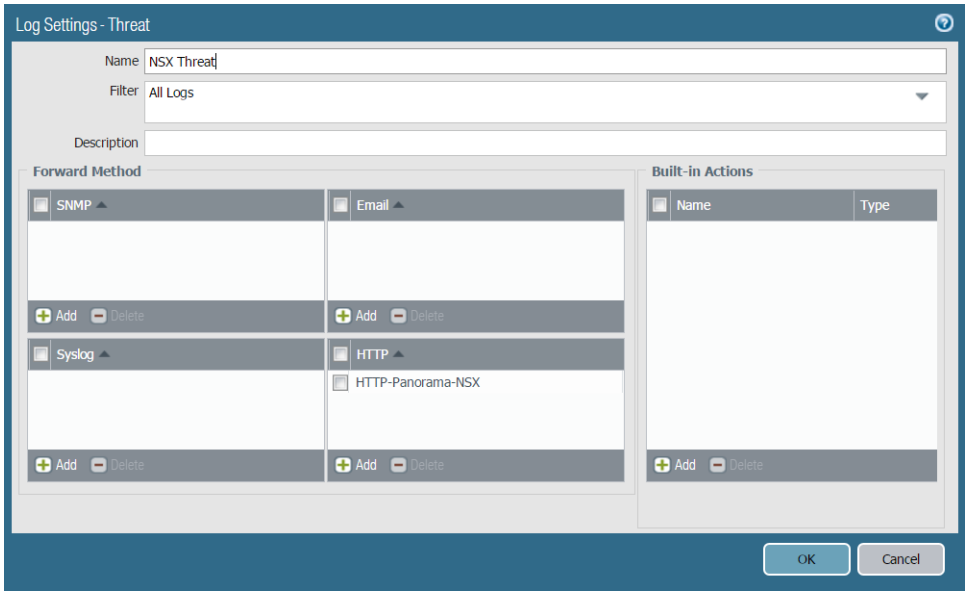
9. 选择 **Payload Format**（有效负载格式）并从 Pre-defined Formats（预定义格式）下拉列表中选择 NSX-V 有效负载格式。这将使用正确的信息填充 URI Format（URI 格式）、HTTP Headers（HTTP 标头）和 Payload（有效负载）字段以将 HTTP API 调用发送到 NSX-V Manager。此外，所选格式将 NSX-V Manager 应用到受感染的来宾虚拟机的安全标记。在下面的示例中，选择与 NSX-V Manager 上的 **ANTI_VIRUS.VirusFound.threat=**高安全标记对应的 **NSX-V** 防病毒威胁高。



STEP 4 | 定义 Panorama 将日志转发到 NSX -VManager 时的匹配条件，并附加要使用的 HTTP 服务器配置文件。

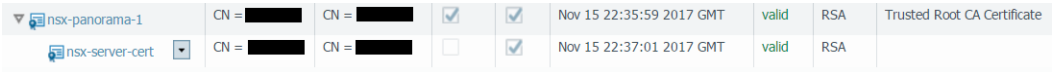
1. 为威胁或流量日志选择 **Panorama** > **Collector Groups**（收集器组）> **Collector Log Forwarding**（收集器日志转发）。
2. 单击 **Traffic**（流量）或 **Threat**（威胁）和 **Add**（添加）。
3. 输入新日志设置的描述性名称。
4. （可选）在 Filter（筛选器）下，您可以添加筛选器（如严重性）以缩小转发到 NSX-V Manager 的日志。如果选择 All Logs（所有日志），则符合 HTTP 服务器配置文件中设置的条件的所有威胁或通信日志都会发送到 NSX-V Manager。
5. 单击 HTTP 下的 **Add**（添加）并选择在步骤 3 中配置的 HTTP 服务器配置文件。
6. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.



STEP 5 | 为 Panorama 配置 NSX -V服务器证书以将日志转发到 NSX-V Manager。

1. 选择 **Panorama** > **Certificate Management**（证书管理）> **Certificates**（证书）。
2. 使用 CN = Panorama 的 IP 地址创建根 CA 证书。
3. 使用“CN = NSX-V Manager”的 IP 地址创建签名证书。
4. 不使用私钥以 PEM 格式导出根 CA 证书。
5. 使用私钥以 PEM 格式导出签名证书。



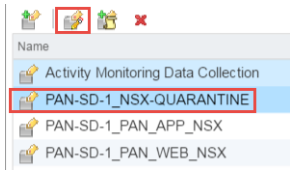
6. 使用诸如 OpenSSL 之类的工具将导出的证书合并成单个 PEM 文件以上传到 NSX-V Manager。在 OpenSSL 中使用以下命令完成此步骤。

```
cat cert_NSX_Root_CA.crt
cert_NSX_Signed1.pem > cert_NSX_cert_chain.pem
openssl pkcs12 -export -in cert_NSX_cert_chain.pem -out cert_NSX_cert.p12
```

7. 登录到 NSX-V Manager 并选择 **Manage Appliance Settings**（管理设备设置）> **SSL Certificates**（SSL 证书）> **Upload PKC#12 Keystore**（上传 **PKC # 12** 密钥库）。单击 **Choose File**（选择文件），找到您在上一步中创建的 p12 文件，然后单击 **Import**（导入）。

STEP 6 | 将安全组与 vCenter 中的安全标记关联。

1. 登录到 vCenter。
2. 选择 **Networking & Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组）。
3. 选择与之前创建的隔离区动态地址组相对应的安全组，然后单击 **Edit Security Group**（编辑安全组）。

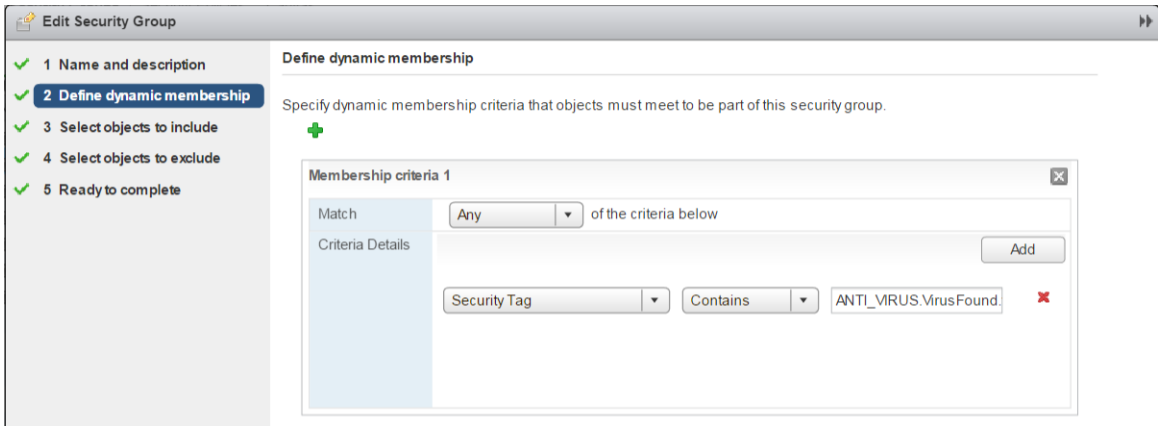


4. 选择 Define dynamic membership（定义动态成员）并单击 + 图标。
5. 单击 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

6. 将条件详细信息设置为 Security Tag Contains（安全标记包含），然后输入与您在步骤 3 中选择的 NSX 有效负载格式相对应的 NSX-V 安全标记。每个预定义的 NSX-V 有效负载格式都对应于一个 NSX-V 安全标记。要查看 NSX-V 中的 NSX-V 安全标记，请选择 **Networking & Security**（网络和安全）> **NSX-V Managers** > **NSX Manager IP** > **Manage**（管理）> **Security Tags**（安全标记）。

   在本示例中，在 HTTP 服务器配置文件中使用 **NSX-V** 防病毒威胁高，因此在此处使用的 NSX-V 安全标记是 **ANTI_VIRUS.VirusFound.threat=高**。
7. 单击 Finish（完成）。



STEP 7 | 在从隔离区中删除清除的来宾 VM 后，请手动从 NSX-V 中的来宾 VM 中删除 NSX-V 安全标记。

1. 登录到 vCenter。
2. 选择 **VMs and Templates**（**VM** 和模板）并选择隔离的来宾。
3. 选择 **Summary**（摘要）> **Security Tags**（安全标记）> **Manage**（管理）。
4. 取消选择隔离安全组使用的安全标记，然后单击 OK（确定）。
5. 刷新页面，隔离安全将不再列在 **Summary**（摘要）> **Security Group Membership**（安全组成员）下方。

在从隔离区中删除来宾 VM 后，威胁和流量日志中的源和目标 UUID 字段可能为空。运行 NSX-V 6.2.3 或更早版本或 NSX-V 操作规则不使用 inout 方向时可能会发生这种情况。您可以通过将 NSX-V 升级到 6.2.4 解决此问题，或在 **Panorama** > **VMware** > **NSX-V** > **Service Manager**（服务管理器）下发出 NSX 配置同步并重新启动 PA-VM 解决此问题。

将以操作为中心的配置迁移到以安全为中心的配置

完成以下步骤将以操作为中心的配置迁移到以安全为中心的格式。不需要此迁移。VMware NSX-V 的 VM 系列防火墙支持两种风格的配置。但是，不推荐在同一部署中使用两种风格的配置。

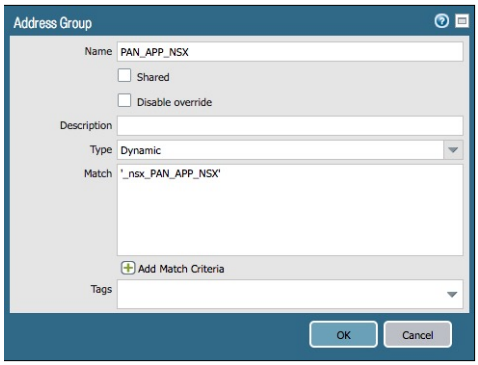
STEP 1 | 升级 Panorama。

STEP 2 | 更新动态地址组中的匹配标准格式。

1. 选择 **Objects**（对象）> **Address Groups**（地址组），然后单击第一个动态地址组的链接名称。
2. 删除现有的匹配条件条目。
3. 按以下格式输入新的匹配条件：

```
'_nsx_<dynamic-address-group-name>'
```

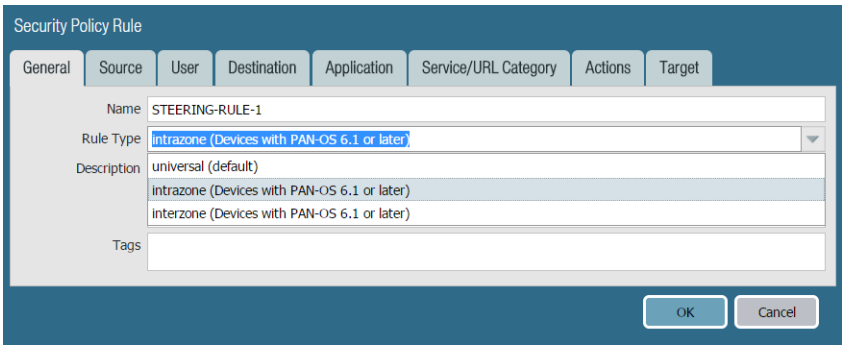

© 2019 Palo Alto Networks, Inc.



4. 单击 **OK**（确定）。
5. 对于每个动态地址组，请重复执行此流程。

STEP 3 | 将用作 NSX-V 控制规则的安全政策更改为内部区域。

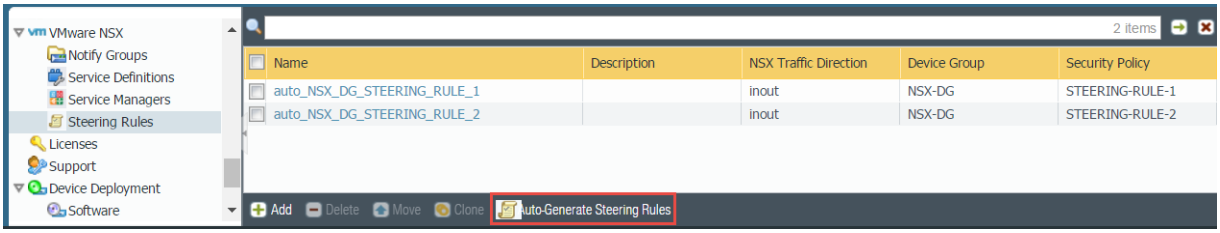
1. 选择 **Policies**（策略）> **Security**（安全）> **Pre Rules**（操作规则），然后单击第一个安全策略规则的链接名称。
2. 在常规选项卡上，更改 **Rule Type**（规则类型）为区域内。



3. 单击 **OK**（确定）。
4. 对于每个安全策略规则，请重复执行此流程。

STEP 4 | 生成新的控制规则。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Steering Rules**（控制规则）。
2. 单击 **Auto-Generate Steering Rules**（自动生成控制规则）。



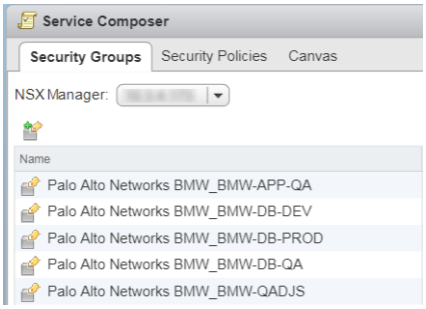
STEP 5 | **Commit**（提交）更改。

当您提交更改时，Panorama 会将更新推送到 NSX-V Manager。

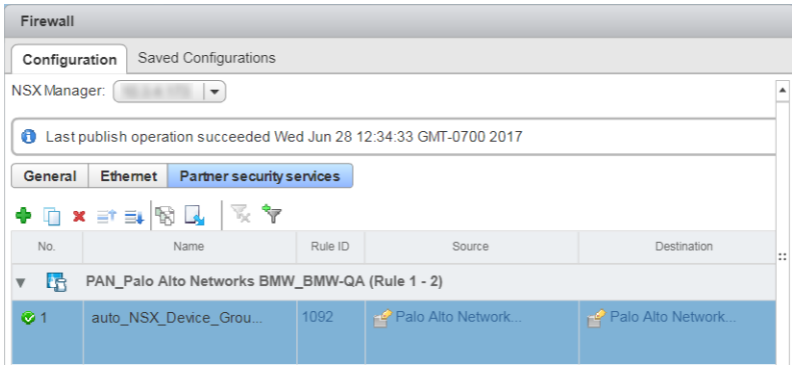
1. 验证 NSX-V Manager 是否创建了新的安全组。
   1. 登录到 vCenter 并选择 **Networking & Security** >（网络和安全）**Security Groups**（安全组）。
   2. 新安全组（映射到更新后的动态地址组）应以下列格式显示：

      <service-definition-name> - <dynamic-address-group-name>

© 2019 Palo Alto Networks, Inc.



2. 验证 NSX-V Manager 是否创建了新的控制规则。
   1. 选择 **Networking & Security**（网络和安全）> **Firewall**（防火墙）> **Configuration**（配置）> **Partner security services**（合作伙伴安全服务）。
   2. 新的控制规则（映射到您在 Panorama 上创建的安全策略规则）在旧控制规则的上方列出。



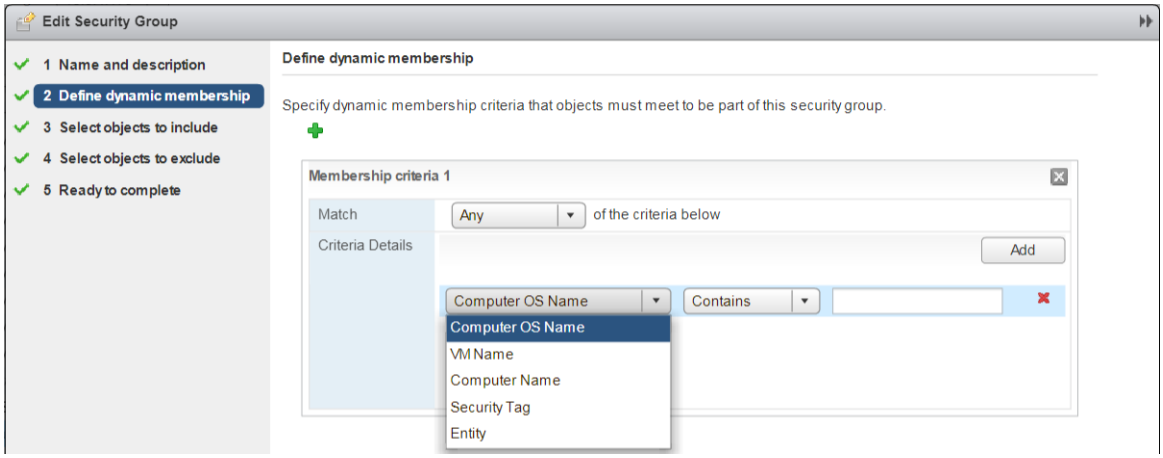
STEP 6 | 为新创建的安全组添加匹配条件，以确保您的 VM 放置在正确的安全组中。

有两种方法可以完成此任务 — 从新安全组中的旧安全组重新创建匹配条件，或将旧安全组嵌套到新安全组中。

要从旧安全组重新创建匹配条件，请完成以下过程。

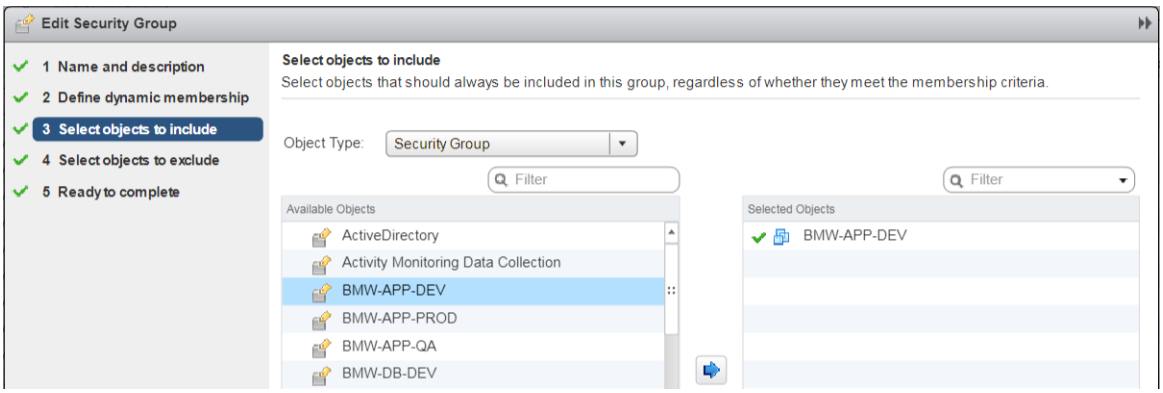
1. 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组）。
2. 单击一个新的安全组并选择 **Edit Security Group**（编辑安全组）。
3. 选择 **Define dynamic membership**（定义动态成员资格）并单击加号图标。
4. 在相应的旧安全组中添加相同的匹配条件。
5. 对于每个新的安全组，请重复执行此流程。
6. 删除旧的安全组。

© 2019 Palo Alto Networks, Inc.



要将旧安全组嵌套到新安全组中，请完成以下过程。在此方法中，旧安全组中的 VM 将添加到新安全组。此外，任何符合旧安全组条件的新 VM 都会自动添加到新安全组。

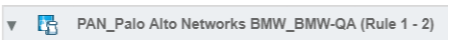
1. 选择 **Networking and Security**（网络和安全）> **Service Composer**（服务组合系统）> **Security Groups**（安全组）。
2. 单击一个新的安全组并选择 **Edit Security Group**（编辑安全组）。
3. 选择 **Define dynamic membership**（选择要包含的对象）。
4. 选择 **Security Group**（安全组）对象类型。
5. 在可用对象下选择相应的旧安全组，然后通过单击右箭头图标将其移至选定对象。
6. 单击 **Finish**（完成）。



STEP 7 | 从 vCenter 中删除旧的控制规则。

1. 选择 **Networking & Security**（网络和安全）> **Firewall**（防火墙）> **Configuration**（配置）>（合作伙伴安全服务）。
2. 删除旧的控制规则。注意不要删除由以安全为中心的工作流程创建的 Palo Alto Networks 规则。这些控制规则部分使用以下命名约定。

   <service-definition-name> - <dynamic-address-group-name>

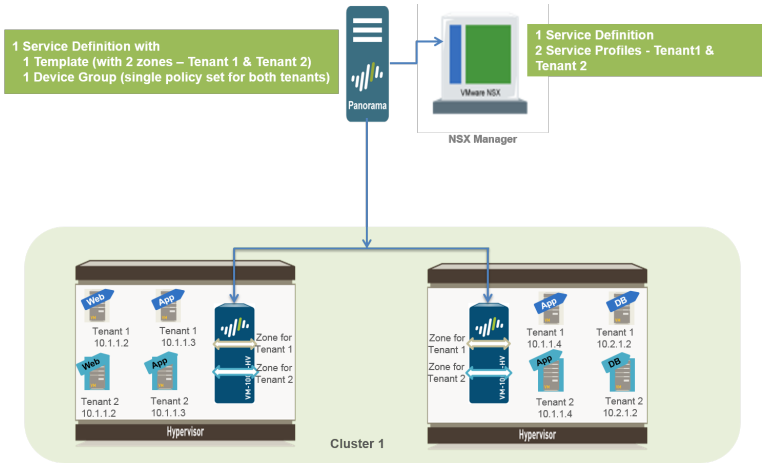


用例：共享的计算基础架构和安全策略

该用例允许您以逻辑的方式隔离来自两个租户的流量，这两个租户共享一个 ESXi 群集，且具有通用的安全策略集。若要隔离来自每个租户的流量，您需要使用一个包含有两个区域的模板堆栈创建一个服务定义。通过基于区域的流量分离，您可以在属于单独租户的虚拟机之间的流量通过防火墙时，对其加以区分。防火墙能够基于在 NSX-V Manager 上创建的服务配置文件和安全组区分租户虚拟机之间的流量，这些服务配置文

© 2019 Palo Alto Networks, Inc.

件和安全组可作为防火墙上动态地址组的匹配标准。因此，即便出现 IP 地址重叠，您也可以分离每个租户的流量，使用基于区域的策略规则（源区域和目标区域必须相同）和动态地址组确保每个租户虚拟机的安全。

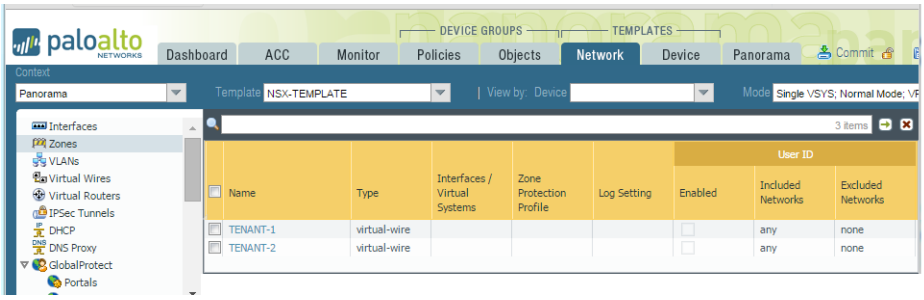


STEP 1 | 启用 NSX-V Manager 与 Panorama 之间的通信。

该任务为一次性任务，如果未启用 NSX-V Manager 与 Panorama 之间的访问权限，将必须执行该任务。

STEP 2 | 在 Panorama 上创建模板和设备组.

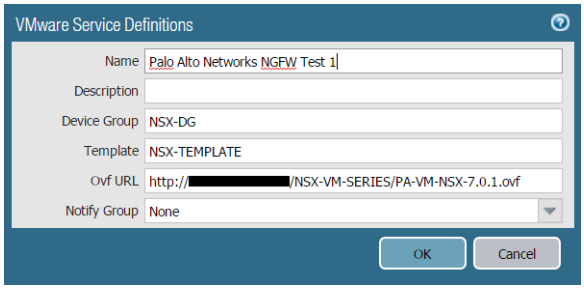
1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Templates**（模板），以添加模板堆栈。该用例中使用了一个名为 NSX-Template 的模板堆栈。
3. 选择 **Panorama** > **Device Groups**（设备组），然后添加设备组。该用例中使用了一个名为 NSX-DG 的设备组。
4. 在模板堆栈中创建两个区域。若要隔离每个租户的流量，您需要在本用例中使用两个区域。
    1. 选择 **Network**（网络）> **Zones**（区域）。
    2. 选择 **Template**（模板）下拉列表中正确的模板堆栈。
    3. 选择 **Add**（添加），然后输入区域 **Name**（名称）。例如，**Tenant1**。
    4. 将接口 **Type**（类型）设置为 **Virtual Wire**（虚拟线路）。
    5. 单击 **OK**（确定）。
    6. 重复上述步骤添加另一个区域，例如 **Tenant2**。
    7. 验证区域是否已附加至正确的模板堆栈。



STEP 3 | 在 Panorama 上创建服务定义。

1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Definitions**（服务定义）。
2. 选择 **Add**（添加）并填写详细信息。

© 2019 Palo Alto Networks, Inc.



3. 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 4 | 创建安全组和操作规则。

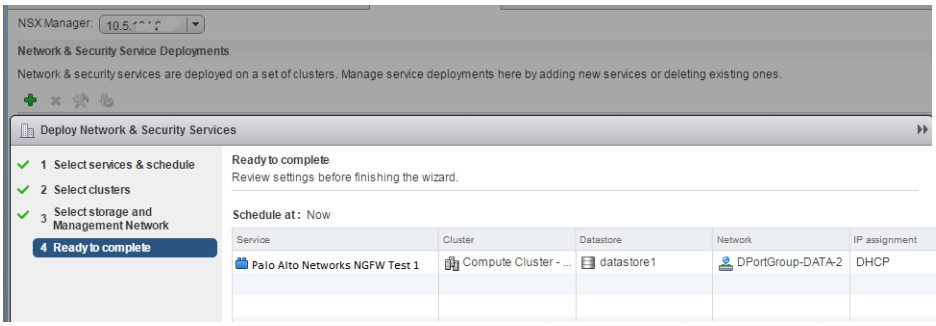
1. 选择 **Objects**（对象）> **Address Groups**（地址组）和 在 Panorama 上设置动态地址组为每个租户的虚拟机。例如，在该用例中，每个租户拥有两个安全组；一个安全组用于 Web 服务器，而另一个安全组用于应用程序服务器。
2. 选择 **Policies**（策略）> **Security**（安全）> **Pre Rules**（前导规则），以设置将流量发送到 VM 系列防火墙的安全策略规则。
3. 选择 **Panorama** > **VMware** > **NSX-V** > **Steering Rules**（控制规则），然后单击 **Auto-Generate Steering Rules**（自动生成控制规则）。
4. **Commit**（提交）更改

STEP 5 | 准备用于 VM 系列防火墙的 ESXi 主机。

群集中的 ESXi 主机必须具有必需的 NSX-V 组件，以便 NSX-V 防火墙和 VM 系列防火墙共同协作。NSX-V Manager 将安装部署 VM 系列防火墙所需的组件 — Ethernet 适配器模块 (.eam) 和 SDK。

STEP 6 | 部署 Palo Alto Networks NGFW 服务。

1. 选择 **Networking and Security**（网络和安全）> **Installation**（安装）> **Service Deployments**（服务部署）。
2. 单击 **New Service Deployment**（新服务部署）（绿色加号图标），然后选择您想要部署的 Palo Alto Networks 下一代防火墙的服务定义，在本示例中，即：**Palo Alto Networks NGFW Test 1**，确保您的选择中包含您想要向其部署防火墙的适当 ESXi 群集，然后单击 **Finish**（完成）。

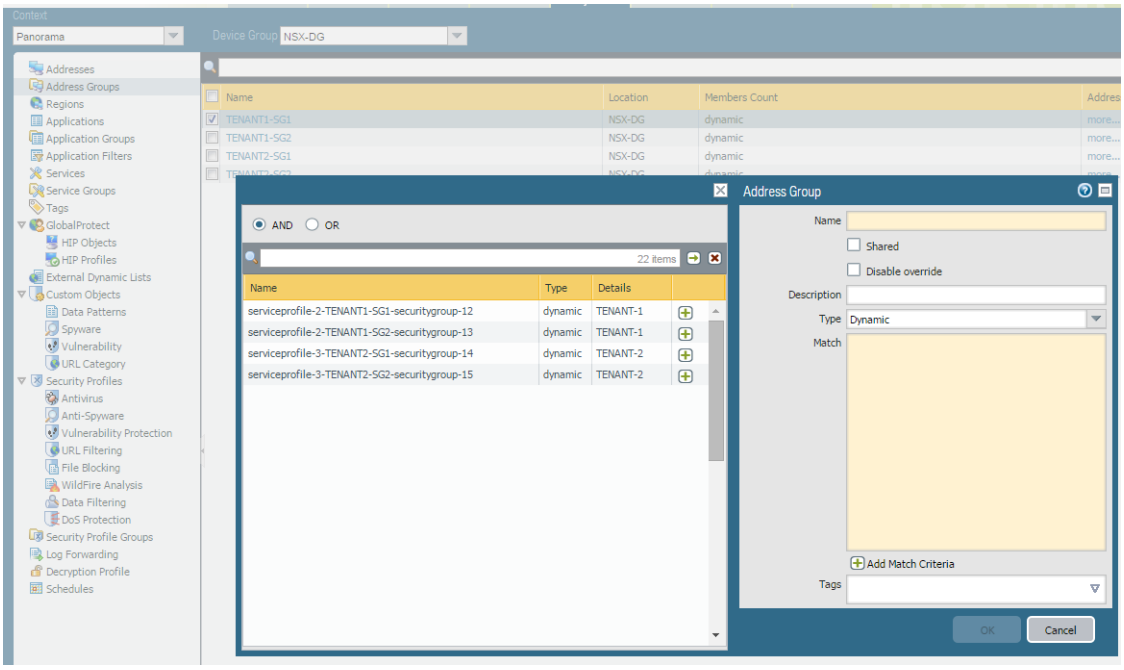


3. 验证 NSX-V Manager 是否将 **Installation Status**（安装状态）报告为 **Successful**（成功）。
4. 验证是否已成功部署 VM 系列防火墙。
    1. 在 vCenter 服务器中，选择 **Hosts and Clusters**（主机和群集）以检查群集中的每个主机是否有一个防火墙实例。
    2. 直接通过 vCenter 服务器查看管理 IP 地址和防火墙上运行的 PAN-OS 版本。VMware 工具与 PAN-OS 软件映像绑定，在您启动 VM 系列防火墙时会自动启用。

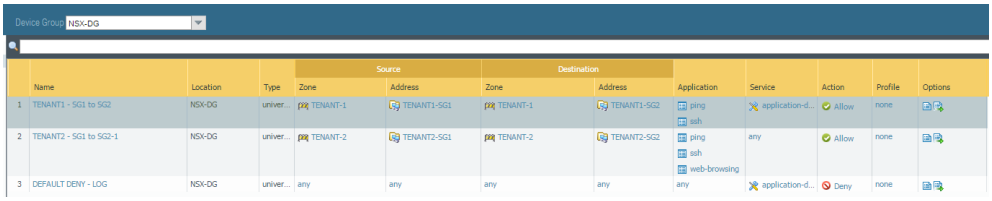
STEP 7 | 将安全策略应用于 VM 系列防火墙。

© 2019 Palo Alto Networks, Inc.

1. 为 Panorama 上的每个租户创建动态地址组。与 NSX-V Manager 上所定义安全组的名称匹配的动态地址组。
   1. 在 Panorama 上，选择 **Objects**（对象）> **Address Groups**（地址组）。
   2. 从下拉列表中选择正确的 **Device Group**（设备组），然后单击 **Add**（添加）。
   3. 为地址组添加一个 **Name**（名称），并将类型设置为 **Dynamic**（动态），并 **Add Match Criteria**（添加匹配标准）。验证您为每个租户选择了正确的标记，标记中包括服务配置文件 ID、安全组名称和安全组 ID。举例来说，该用例中有四个动态地址组：



2. 在 Panorama 上，创建安全策略规则并使用动态地址组作为安全策略规则中的源地址对象或目标地址对象，然后将其推送至防火墙。
   1. 选择 **Policies**（策略）> **Security**（安全）> **Prerules**（预定规则），然后单击 **Add**（添加）。
   2. 为每个租户创建规则。该用例具有以下策略规则：



3. 单击 Commit（提交），选择 Device Groups（设备组）作为 Commit Type（提交类型）。选择设备组（在本例中选择 NSX-DG 设备组），然后单击 OK（确定）。

STEP 8 | 验证来自每个租户的流量均已确保安全。

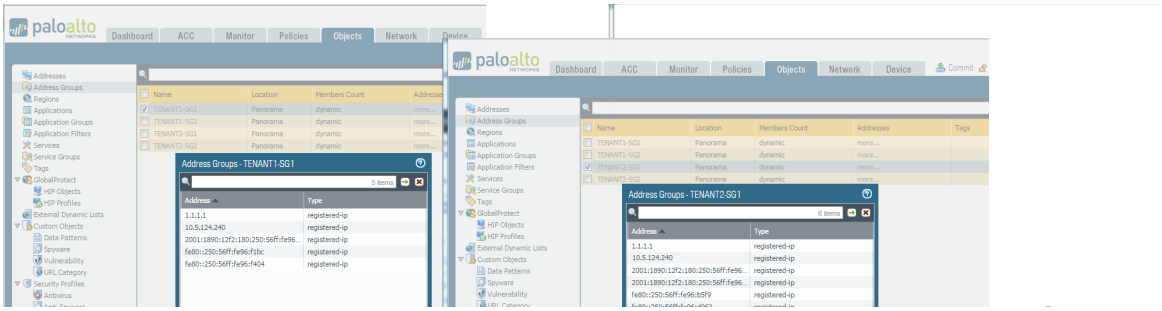
1. 登录到防火墙上的 CLI，然后输入以下命令查看防火墙上的子接口：

```
show interface all
total configured hardware interfaces: 2
name id    speed/duplex/state        mac address
--------------------------------------------------
ethernet1/1              16    auto/auto/up d4:f4:be:c6:af:10
ethernet1/2              17    auto/auto/up d4:f4:be:c6:af:11
aggregation groups: 0
total configured logical interfaces: 6
```


© 2019 Palo Alto Networks, Inc.

```
name                 id vsys zone          forwarding
-------------------- ----- ---- ------------------
ethernet1/1          16    1                vwire:ethernet1/2
ethernet1/1.3        4099  1    TENANT-1    vwire:ethernet1/2.3
ethernet1/1.4         4100   1   TENANT-2      vwire:ethernet1/2.4
ethernet1/2           17    1 vwire:ethernet1/1
ethernet1/2.3        4355  1    TENANT-1 vwire:ethernet1/1.3
ethernet1/2.4         4356  1 TENANT-2 vwire:ethernet1/1.4
```

2. 在 VM 系列防火墙的 Web 界面上，选择 **Objects**（对象）> **Address Groups**（地址组），并验证您可以查看每个动态地址组成员的 IP 地址。以下所示为两个租户之间动态地址组中的重复 IP 地址。



3. 查看 **ACC**，然后选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）。筛选区域名称，以确保来自每个租户虚拟机的流量均为安全流量。

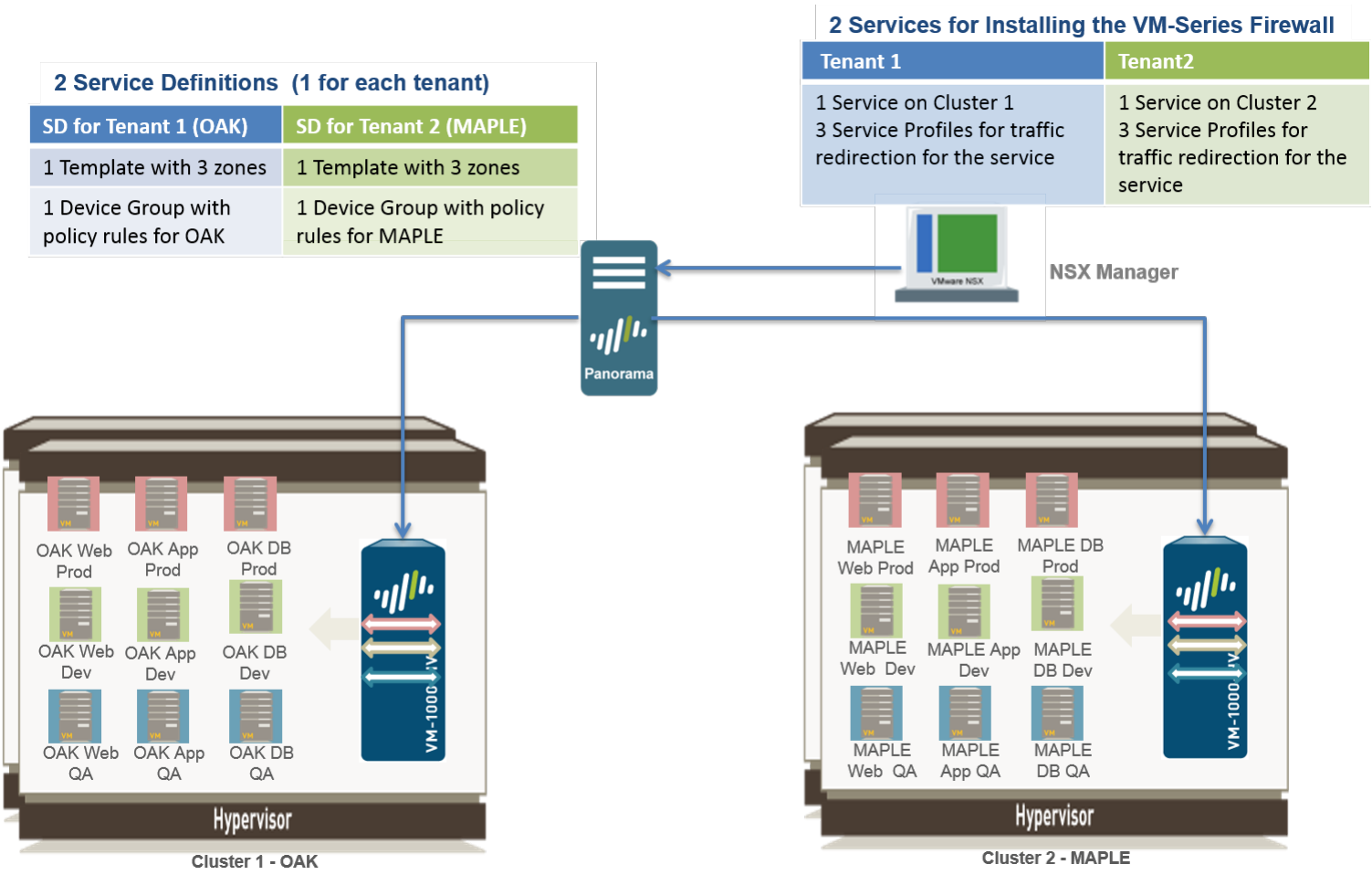
用例：专用计算基础架构上的共享安全策略

如果您是一个托管服务提供商，需要确保一个大型企业（租户）及其多个部门（子租户）的安全，而且每个租户均需要专用的计算基础架构和安全策略规则，则您需要为每个租户创建一个服务定义。

在本用例中，每个租户（Oak 和 Maple）均具有一个专用的 ESXi 集群。每个租户均拥有多个子租户（Dev、QA 和 Prod），其工作负载部署在群集上。您需要定义两个服务定义，以确保每个租户的 VM 系列防火墙均具有针对各自 ESXi 群集的安全策略。每个租户的服务定义包括多个区域（带有相应的虚拟线路子接口对），用于隔离来自每个子租户的流量。每个区域均映射到 NSX-V Manager 上的服务配置文件，以便防火墙区分来自每个子租户虚拟机的流量，以及在针对租户的通用策略规则集范围内执行基于区域的安全策略规则。通过结合使用基于区域的策略和动态地址组，您还可以保护可能存在重叠网络进而存在重复 IP 地址的子租户。为了识别分配至每个子租户的虚拟机并确保策略的成功执行，NSX-V Manager 提供了虚拟机所属的服务配置文件和安全组，以此作为 Panorama 上动态地址组的匹配标准。有关更多信息，请参阅 使用动态地址组实施策略。

您还可以使用 Panorama 上的访问域配置基于角色的访问控制。通过访问域，您可以控制特定设备组（以实现对策略和对象的管理）和模板堆栈（以实现对网络和设备设置的管理）的管理访问，确保每个租户管理员可以管理其 VM 系列防火墙的配置。此外，通过基于角色的访问，可以确保仅有各自的租户可以查看其日志。

© 2019 Palo Alto Networks, Inc.



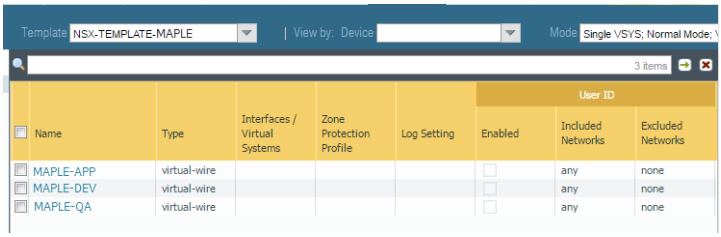
STEP 1 | 启用 NSX-V Manager 与 Panorama 之间的通信。

该任务为一次性任务，如果未启用 NSX-V Manager 与 Panorama 之间的访问权限，将必须执行该任务。

STEP 2 | 在 Panorama 上创建模板和设备组.

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Templates**（模板），以添加模板堆栈。该用例中具有两个模板堆栈，名称分别为 NSX-Template-MAPLE 和 NSX-Template-OAK。
3. 选择 **Panorama** > **Device Groups**（设备组），然后添加设备组。该用例中具有两个设备组，名称分别为 NSX-DG-OAK 和 NSX-DG-MAPLE。
4. 在每个模板堆栈中创建 NSX-V 服务配置文件区域。若要隔离本用例中每个租户的流量，您需要为每个租户配置三个区域。
    1. 选择 **Network**（网络）> **Zones**（区域）。
    2. 选择 **Template**（模板）下拉列表中正确的模板堆栈。
    3. 选择 **Add**（添加），然后输入区域 **Name**（名称）。例如，**Tenant1**。
    4. 将接口 **Type**（类型）设置为 **Virtual Wire**（虚拟线路）。
    5. 单击 **OK**（确定）。
    6. 重复上述步骤 a-e，为每个子租户添加其他区域。
    7. 验证区域是否已附加至正确的模板堆栈。

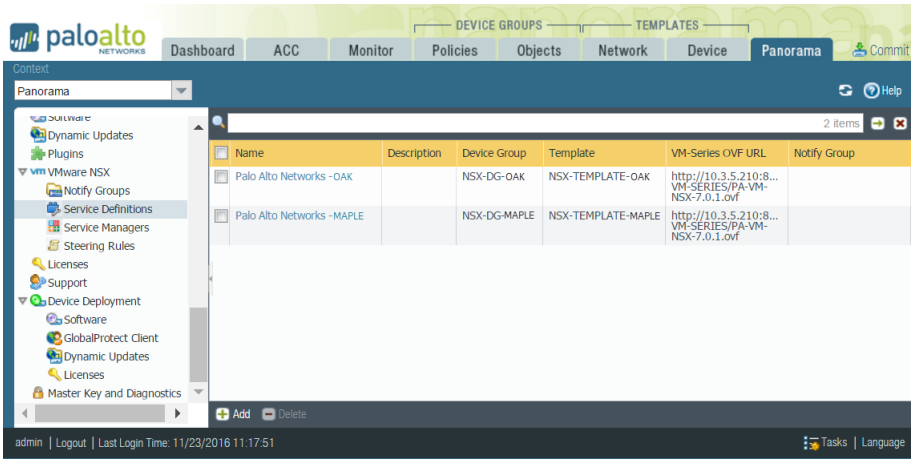
© 2019 Palo Alto Networks, Inc.



5. 在每个其他模板堆栈中创建 NSX 服务配置文件区域。

STEP 3 | 在 Panorama 上创建服务定义。

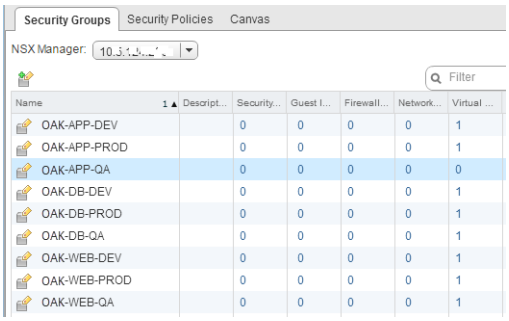
1. 选择 **Panorama** > **VMware** > **NSX-V** > **Service Definitions**（服务定义）。
2. 选择添加。填写每个租户服务定义的详细信息。在本示例中，两个服务定义分别为：Palo Alto Networks - Maple 和 Palo Alto Networks - Oak。



3. 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。

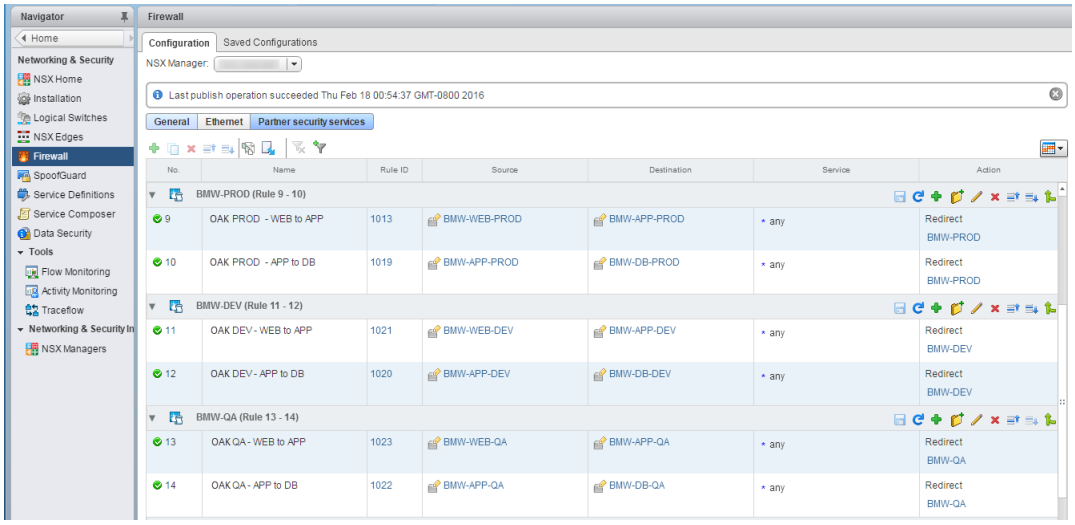
STEP 4 | 创建安全组和操作规则。

1. 选择 **Objects**（对象）> **Address Groups**（地址组）和 在 Panorama 上设置动态地址组为每个租户的虚拟机。例如，在该用例中，每个租户拥有两个安全组；一个安全组用于 Web 服务器，而另一个安全组用于应用程序服务器。



2. 选择 **Policies**（策略）> **Security**（安全）> **Pre Rules**（前导规则），以设置将流量发送到 VM 系列防火墙的安全策略规则。
3. 选择 **Panorama** > **VMware** > **NSX-V** > **Steering Rules**（控制规则），然后单击 **Auto-Generate Steering Rules**（自动生成控制规则）。
4. **Commit**（提交）更改

© 2019 Palo Alto Networks, Inc.

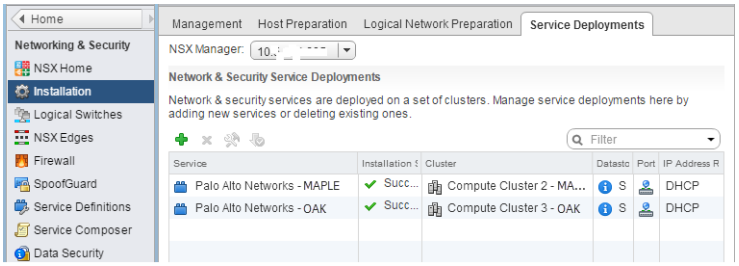


STEP 5 | 准备用于 VM 系列防火墙的 ESXi 主机

群集中的 ESXi 主机必须具有必需的 NSX-V 组件，以便 NSX-V 防火墙和 VM 系列防火墙共同协作。NSX-V Manager 将安装部署 VM 系列防火墙所需的组件 — Ethernet 适配器模块 (.eam) 和 SDK。

STEP 6 | 部署 Palo Alto Networks NGFW 服务

1. 选择 **Networking and Security**（网络和安全）> **Installation**（安装）> **Service Deployments**（服务部署）。
2. 单击 **New Service Deployment**（新服务部署）（绿色加号图标），然后选择您想要部署的 Palo Alto Networks 下一代防火墙的服务定义，在本示例中，即：**Palo Alto Networks NGFW Test 1** ，确认您的选择，然后单击 **Finish**（完成）。
3. 验证 NSX-V Manager 是否将 **Installation Status**（安装状态）报告为 **Successful**（成功）。

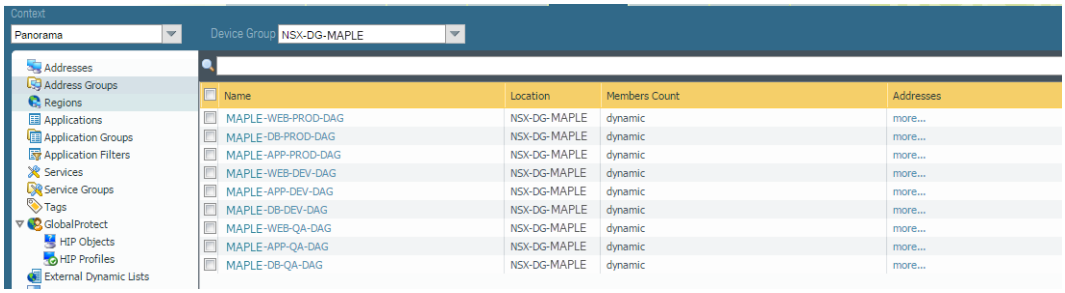


4. 验证是否已成功部署 VM 系列防火墙。
    1. 在 vCenter 服务器中，选择 **Hosts and Clusters**（主机和群集）以检查每个群集中的每个主机是否有一个防火墙实例。
    2. 直接通过 vCenter 服务器查看管理 IP 地址和防火墙上运行的 PAN-OS 版本。VMware 工具与 PAN-OS 软件映像绑定，在您启动 VM 系列防火墙时会自动启用。

STEP 7 | 将安全策略应用于 VM 系列防火墙

1. 为 Panorama 上的每个子租户创建动态地址组。与 NSX-V Manager 上所定义安全组的名称匹配的动态地址组。
    1. 在 Panorama 上，选择 **Objects**（对象）> **Address Groups**（地址组）。
    2. 从下拉列表中选择一个 **Device Group**（设备组），然后单击 **Add**（添加）。
    3. 为地址组添加一个 **Name**（名称），并将类型设置为 **Dynamic**（动态），并 **Add Match Criteria**（添加匹配标准）。为了便于管理这些动态地址组，可以使用与 NSX-V Manager 上的安全组相同的动态地址组名称。

© 2019 Palo Alto Networks, Inc.

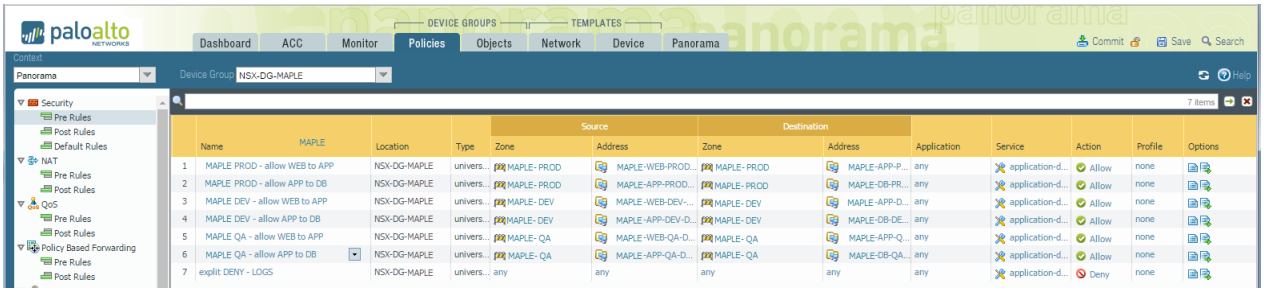


4. 为其他租户（在本示例中即：Oak）的子租户创建动态地址组。

2. 在 Panorama 上，创建安全策略并使用动态地址组作为安全策略规则中的源地址对象或目标地址对象，然后将其推送至防火墙。

   1. 选择 **Policies**（策略）> **Security**（安全）> **Pre Rules**（前导规则）。
   2. 从下拉列表中选择一个 **Device Group**（设备组），然后单击 **Add**（添加）。
   3. 为每个子租户创建规则。确保策略规则中的源区域和目标区域保持相同。若要确保仅允许在服务器上运行的应用程序，则仅允许应用程序默认端口上的服务。

      对于租户 Maple，该用例具有以下策略规则：



3. 从下拉列表中选择其他 **Device Group**（设备组），并为其他租户（在本示例中即：Oak）的子租户创建安全策略。
4. 单击 Commit（提交），选择 Device Groups（设备组）作为 Commit Type（提交类型）。选择设备组（在本例中选择 NSX-DG-OAK 和 NSX-DG-MAPLE 设备组），然后单击确定。

   提交后，会将安全策略推送至属于每个设备组的防火墙，之后这些防火墙将会对由 NSX-V Manager 重定向的流量执行这些策略。

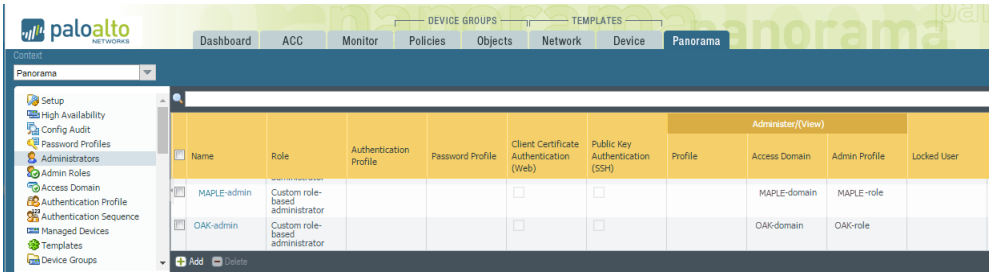
STEP 8 | 验证来自每个租户的流量均已确保安全。

1. 在 Panorama 上，转到 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量）和**Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），以查看流量日志和威胁日志。选择某个租户的设备组，并按区域名称对其进行排序，以完整查看来自每个子租户的流量。
2. 在 Panorama 上，使用 ACC 查看威胁的流量模式及可执行信息。使用小部件和筛选器与 ACC 上的数据进行交互。
3. 在 VM 系列防火墙上，选择 **Objects**（对象）> **Address Groups**（地址组），然后查看每个动态地址组成员的 IP 地址。

© 2019 Palo Alto Networks, Inc.

STEP 9 | （可选）为租户管理员启用基于角色的访问，以管理 VM 系列防火墙的配置和策略。

1. 创建访问域。通过访问域，您可以限制特定设备组和模板堆栈的管理访问。在本示例中，您创建了两个访问域，用于限制对各自租户的设备组和模板堆栈的访问。
2. 为 **Device Group and Template**（设备组和模板）角色配置管理角色，并允许管理员管理访问域。之后，管理员仅可管理属于访问域的防火墙。
3. 创建一个管理帐户，并将该帐户关联到访问域和管理角色。

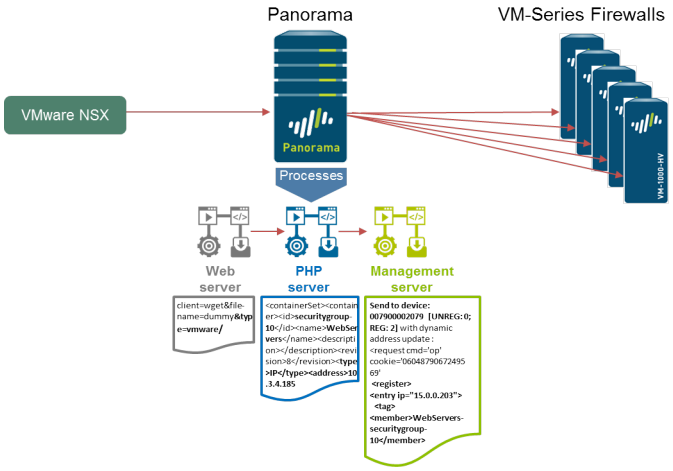


动态地址组 — 将信息从 NSX-V Manager 中继到 Panorama

要在 VM 系列和 NSX-V 集成数据中心执行安全策略，Panorama 必须能够获得有关虚拟环境变化的信息。当部署、更改或删除新虚拟机时，NSX-V Manager 会告知 Panorama 从 NSX-V Manager 上的安全组添加和移除 IP 地址。然后，Panorama 反过来将此信息推送到 VM 系列防火墙。在与此信息匹配的防火墙策略中引用的动态地址组可确定属于该组的成员。此过程可以让防火墙执行上下文感知的安全策略，从而保护流向和来自这些虚拟机的流量。有关动态地址组的详细信息，请参阅使用动态地址组的策略执行。

下图说明了如何将信息从 NSX-V Manager 中继到 Panorama。

© 2019 Palo Alto Networks, Inc.



要了解此过程，需要在将新服务器添加到安全组时跟踪从 NSX-V Manager 发送到 Panorama 的信息更新。使用在本示例的各个阶段的输出中突出显示的元素，对失败的过程进行故障排除。

STEP 1 | 要实时查看更新，需要登录到 Panorama 命令行界面。

登录到 Panorama 命令行界面。

STEP 2 | 验证是否已将来自 NSX-V Manager 的请求路由到 Panorama 上的 Web 服务器。

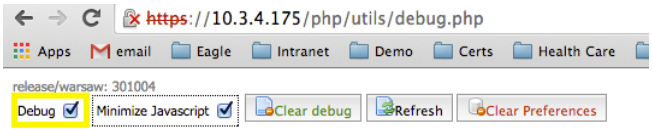
要在 NSX-V 安全组更新期间检查 Panorama 上的 webserver-log，使用以下命令：

```
admin@Panorama> tail follow yes webserver-log cmsaccess.log
127.0.0.1 - - [Wed Dec 03 14:24:11 2014 PST] "POST /unauth/php/
RestApiAuthenticator.php HTTP/1.1" 200 433
127.0.0.1 - - [Wed Dec 03 14:24:11 2014 PST] "PUT /api/index.php?
client=wget&file-name=dummy&type=vmware/vmware/2.0/si/serviceprofile/
serviceprofile-1/containerset HTTP/1.0" 200 446
```

如果输出不包括上述元素，检查是否出现路由问题。从 *NSX-V Manager Ping Panorama*，并检查可能会阻止 *NSX-V Manager* 和 *Panorama* 之间通信的 *ACL* 或其他网络安全设备。

STEP 3 | 验证是否由 Panorama 上的 PHP 守护进程解析请求。

1. 使用以下 URL 启用调试：**https://<Panorama_IP>/php/utils/debug.php**



2. 在命令行界面中，输入以下命令以查看 PHP 服务器生成的日志：

```
admin@Panorama> tail follow yes mp-log php.debug.log
[2014/12/03 14:24:11]
<request cmd="op" cookie="0604879067249569" refresh="no">
  <operations xml="yes">
    <show>
      <cli>
...
   <request>
      <partner>
        <vmware-service-manager>
          <update>
```


© 2019 Palo Alto Networks, Inc.

```
            <method>PUT</method>
            <type>update</type>
            <username>_vsm_admin</username>
           <password>4006474760514053</password>
<url>/vmware/2.0/si/serviceprofile/serviceprofile-1/containerset</url>
            <data><![CDATA[
<containerSet><container><id>securitygroup-10</id><name>WebServers</
name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</
address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</
address></container></containerSet>]]></data>
```

```
</update>
        </vmware-service-manager>
      </partner>
    </request>
  </operations>
</request>
```

STEP 4 | 通过 Panorama 上的管理服务器处理信息。

1. 在管理服务器上使用以下命令启用调试：

```
admin@Panorama> debug management-server on debug
```

2. 输入以下命令以查看 configd 日志生成的日志：

```
admin@Panorama> tail follow yes mp-log configd.log
```

3. 在输出中，检查从 PHP 守护进程中继到管理服务器守护进程的更新。

```
2014-12-03 14:24:11.143 -0800 debug:
 pan_job_progress_monitor(pan_job_mgr.c:3694): job-monitor:
 updated 0 jobs.....2014-12-03 14:24:11.641 -0800 debug:
 recursive_add_params(pan_op_ctxt.c:158): > 'url'='/vmware/2.0/si/
serviceprofile/serviceprofile-1/containerset'
2014-12-03 14:24:11.641 -0800 debug:
 recursive_add_params(pan_op_ctxt.c:158): > 'data'='
<containerSet><container><id>securitygroup-10</id><name>WebServers</
name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</
address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</
address></container></containerSet>'
2014-12-03 14:24:11.641 -0800 Received vshield update: PUT /vmware/2.0/si/
serviceprofile/serviceprofile-1/containerset
Received dynamic address update from VSM:
<request cmd='op' cookie='0604879067249569' client="xmlapi"><operations
 xml='yes'><request>
    <partner>
        <vmware-service-manager>
            <update>
                <method>PUT</method>
        <type>update</type>
<username>_vsm_admin</username>
<password>4006474760514053</password><url>/vmware/2.0/si/serviceprofile/
serviceprofile-1/containerset</url><data><![CDATA[
<containerSet><container><id>securitygroup-10</id><name>WebServers</
name><description></description><revision>8</revision><type>IP</type><address>10.3.4.185</
```


© 2019 Palo Alto Networks, Inc.

```
address><address>10.3.4.186</address><address>15.0.0.203</address><address>15.0.0.202</
address></container></containerSet>]]>
```

```
</data></update>
```

4. 查找 IP 地址和安全组标记的列表

```
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip:
10.3.4.185
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag:
WebServers-securitygroup-10
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip:
15.0.0.202
2014-12-03 14:24:11.646 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag:
WebServers-securitygroup-10
pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag:
DomainControllers-securitygroup-16
2014-12-03 14:24:11.647 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip:
15.0.0.201
2014-12-03 14:24:11.648 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag:
SQLServers-securitygroup-11
2014-12-03 14:24:11.665 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag:
SharePointServers-securitygroup-13
2014-12-03 14:24:11.665 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3721): ip:
10.3.4.187
2014-12-03 14:24:11.665 -0800 debug:
 pan_cfg_mongo_sel_ip_taglist_by_tag_rev(src_cms/
pan_cfg_mongo_tables.c:3738): tag:
SharePointServers-securitygroup-13
...
```

5. 最后，验证是否已将更新从管理服务器守护进程中继到受管防火墙。

```
Send to device: 007900002079 [UNREG: 0; REG: 2] with dynamic address
 update : <request cmd='op' cookie='0604879067249569' target-....
 <register>
<entry ip="15.0.0.203">
  <tag>
<member>WebServers-securitygroup-10</member>
```


© 2019 Palo Alto Networks, Inc.

```
  </tag>
</entry>
<entry ip="10.3.4.186">
  <tag>
<member>WebServers-securitygroup-10</member>
  </tag>
</entry>
</register>
```


© 2019 Palo Alto Networks, Inc.

在 VMware NSX-T 上设置 VM 系列防火墙（北向南）

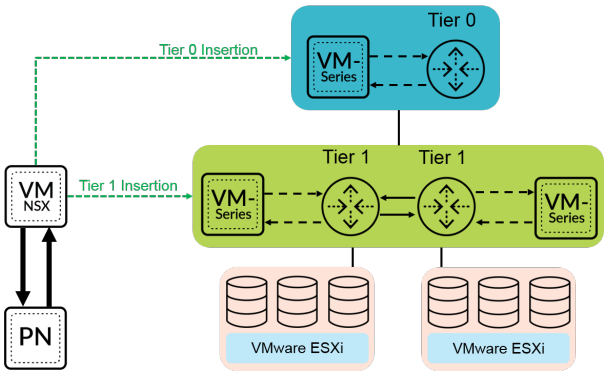
VMware NSX-T 上的 VM 系列防火墙将 Palo Alto 下一代防火墙和 Panorama 与 ESXi 主机服务器集成在一起，为 NSX-T 软件定义数据中心中的所有北向南流量提供全面的可见性和安全应用程序支持。

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）

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。

VMware 组件	
vCenter/ESXi	vCenter 服务器是 vSphere 套件的集中式管理工具。ESXi 是启用计算虚拟化的虚拟机监控程序。

© 2019 Palo Alto Networks, Inc.

VMware 组件	
	有关 vCenter 与 NSX-T 版本的兼容性，请参阅 VMware 的兼容性矩阵。
NSX-T Manager	VMware NSX-T Data Center 2.4.0 和更高版本必须使用 vCenter 服务器进行安装和注册。需要使用 NSX - TManager 才能在 ESXi 群集内的 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（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。

- 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

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。

© 2019 Palo Alto Networks, Inc.

如果拥有 Panorama HA 配置，则在每个 Panorama 对等设备上重复此安装过程。在 Panorama HA 对中安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，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。

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。

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“操作”列中单击 **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 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**）。

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。

© 2019 Palo Alto Networks, Inc.

连接成功时，状态显示为已注册。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 提交（**Commit**），选择 **Panorama** 作为 提交类型（**Commit Type**），以便将更改保存到 Panorama 上正在运行的配置。

STEP 2 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 输入唯一的名称和说明，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. 输入唯一的名称和说明，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。

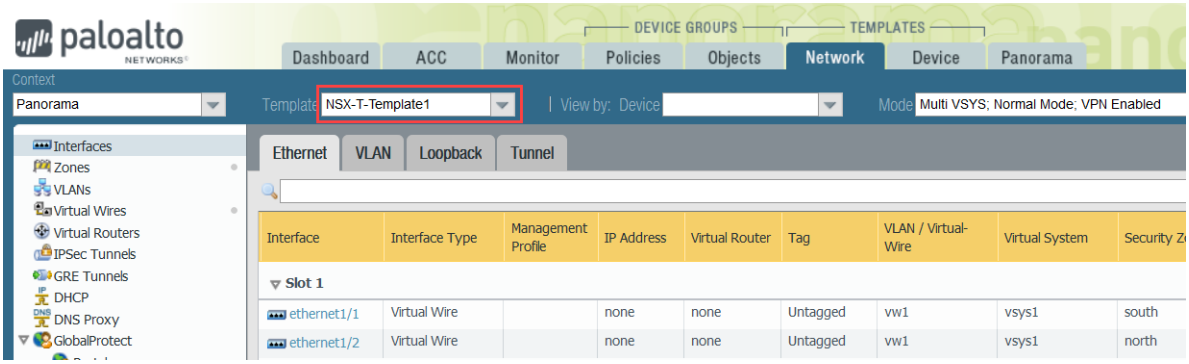
STEP 4 | 配置 Virtual Wire、接口和区域。确保从下面显示的下拉列表中选择正确的模板。您创建的对象必须满足以下条件：

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。

© 2019 Palo Alto Networks, Inc.

- 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。

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 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。

STEP 3 | 指定 OVF 文件的位置。

© 2019 Palo Alto Networks, Inc.

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。

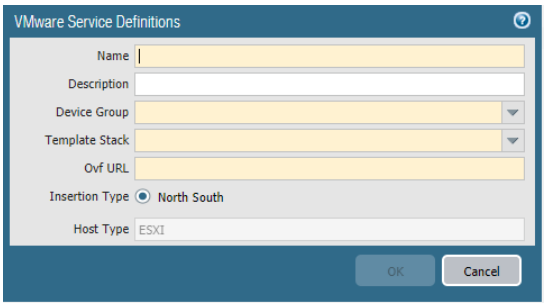
如果需要，可以修改服务器的安全设置，以便下载文件类型。例如，在 IIS 服务器上，可以修改 Mime Types（Mime 类型）配置；在 Apache 服务器上，可以编辑 .htaccess 文件。

在 **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。例如，输入 **https://acme.com/software/PA-VM-NST.9.1.0.ovf**

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 群集中的 VM 系列防火墙上使用不同的 PAN-OS 版本。

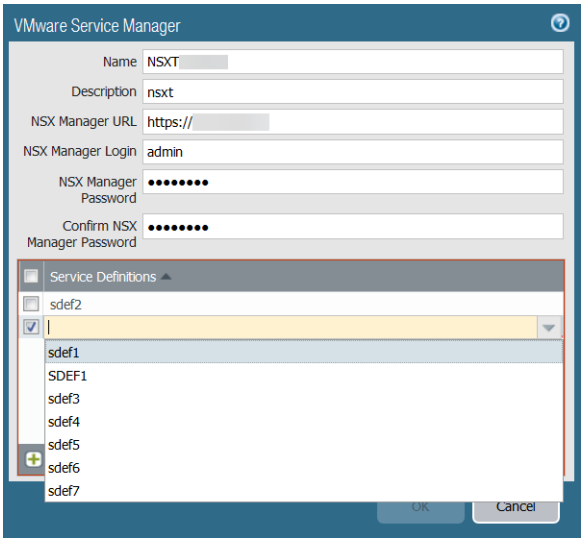
STEP 4 | 为您的防火墙选择 **North South**（北向南）作为 **Insertion Type**（插入类型）。

STEP 5 | 单击 **OK**（确定）保存服务定义。



STEP 6 | 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）。



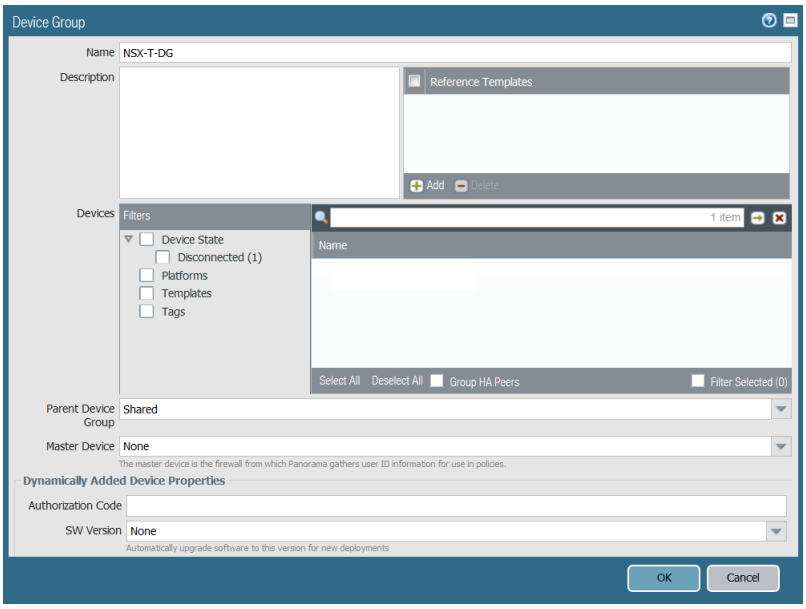
STEP 7 | 将授权代码添加到防火墙的许可证中。

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）。

© 2019 Palo Alto Networks, Inc.

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 8 | **Commit to Panorama**（提交到 **Panorama**）。

STEP 9 | 在 NSX-T Manager 上，验证服务定义是否可用。

选择 **Advanced Networking & Security**（高级网络和安全）> **Partner Services**（合作伙伴服务）> **Catalog**（目录）。服务定义作为 NSX-T Manager 上的服务实例列出。

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。

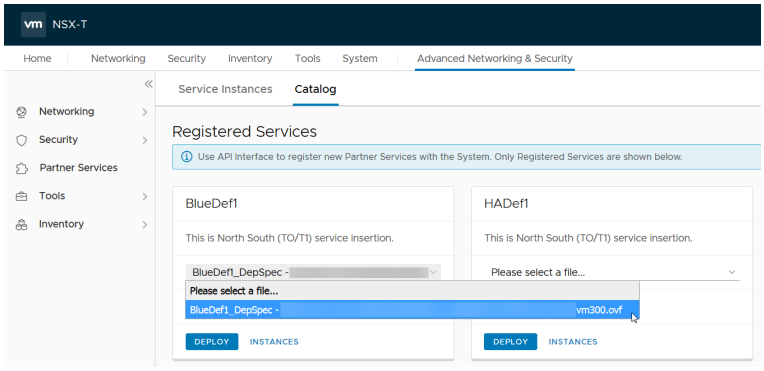
STEP 1 | 登录 NSX-T Manager。

STEP 2 | 选择 **Advanced Networking & Security**（高级网络和安全）> **Partner Services**（合作伙伴服务）> **Catalog**（目录）。

STEP 3 | 选择与要部署的服务定义匹配的 **Registered Service**（注册服务）。

STEP 4 | 从“已注册服务”条目的下拉列表中选择 VM 系列防火墙映像。

© 2019 Palo Alto Networks, Inc.

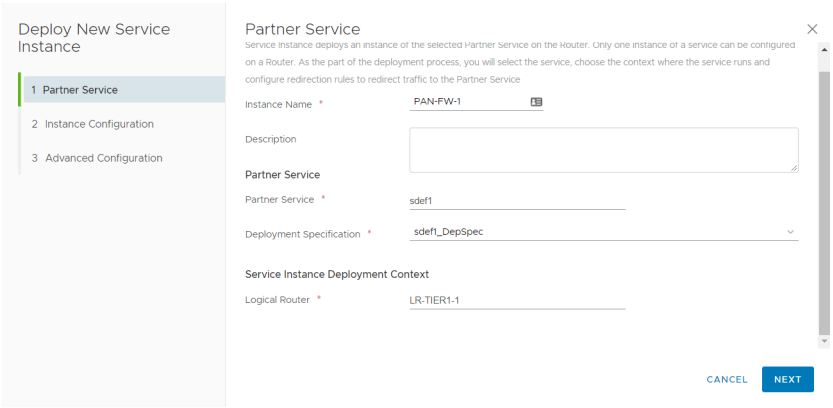


STEP 5 | 在要用于启动防火墙的服务定义的注册服务下单击 **Deploy**（部署）。

STEP 6 | 单击 **Proceed**（继续）。

STEP 7 | 输入合作伙伴服务详情。此信息告诉 NSX-T Manager 在部署 VM 系列防火墙时使用哪个合作伙伴服务和逻辑路由器。

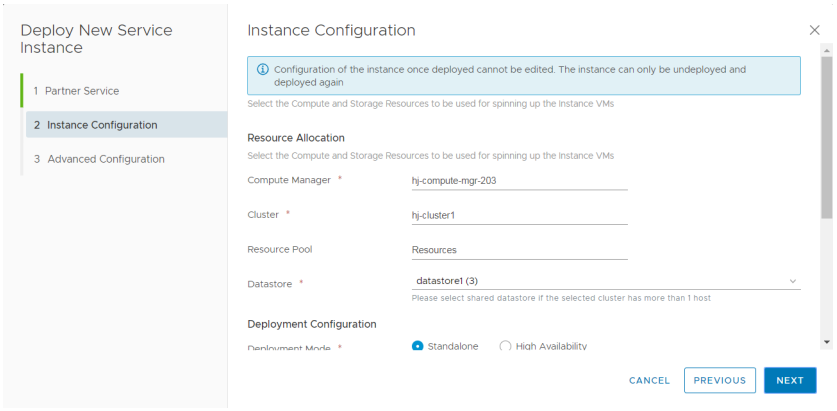
1. 输入 VM 系列防火墙的描述性 **Instance Name**（实例名称）。
2. NSX-T Manager 预先填写 **Partner Service**（合作伙伴服务）字段。选择合作伙伴服务会填写 **Deployment Specification**（部署规范）字段。
3. 单击 **Logical Router**（逻辑路由器）字段并选择第 0 层或第 1 层路由器。NSX-T Manager 将 VM 系列防火墙连接到选定的路由器，并将通过该路由器的流量重定向到 VM 系列防火墙以进行检查。您必须选择未附加服务插入的路由器。
4. 单击 **Next**（下一步）。



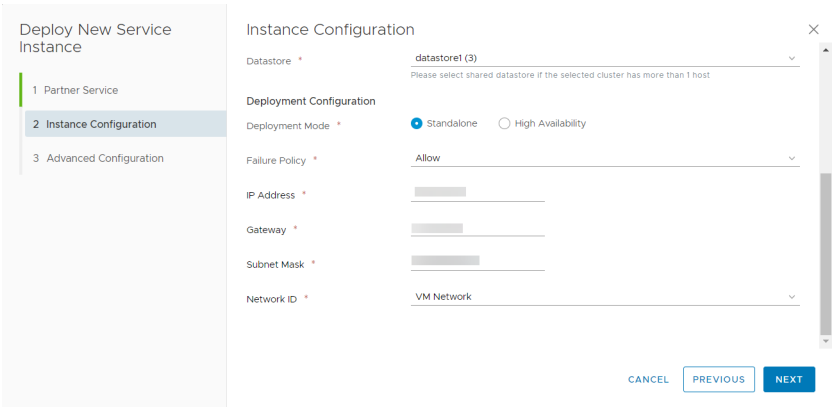
STEP 8 | 配置资源和存储设置。

1. 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。
2. 选择 **Cluster**（群集）。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。
3. （可选）如果已在 vCenter 服务器上创建任何资源池，请选择资源池。
4. 选择 **Datastore**（数据存储）。

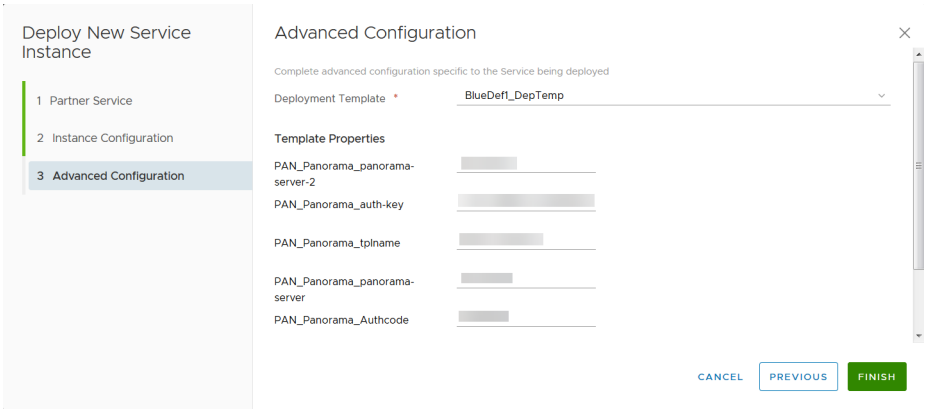
© 2019 Palo Alto Networks, Inc.



5. 选择 VM 系列防火墙的 **Deployment Mode**（部署模式）— 独立或高可用性。
6. 将 **Failure Policy**（故障政策）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。
7. 输入 VM 系列防火墙管理端口的 **IP Address**（IP 地址）、**Gateway**（网关）、**Subnet Mask**（子网掩码）和 **Network ID**（网络 ID）。
8. 如果要在 HA 模式下部署 VM 系列防火墙，请对辅助防火墙实例重复上一步。
9. 单击 **Next**（下一步）。



STEP 9 | 单击 **Deployment Template**（部署模板）字段并选择部署模板。选择部署模板会自动填充模板属性。不要编辑 **Template Property**（模板属性）设置。



STEP 10 | 单击 **Finish**（完成）以部署 VM 系列防火墙。

© 2019 Palo Alto Networks, Inc.

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。

自反规则不会显示在 *NSX-T Web* 界面中。

STEP 1 | 登录 NSX-T Manager。

STEP 2 | 选择 **Advanced Networking & Security**（高级网络和安全）> **Partner Services**（合作伙伴服务）> **Service Instances**（服务实例）。

STEP 3 | 选择服务实例，然后单击 **Traffic Redirection**（流量重定向）。

STEP 4 | 单击第一条默认重定向规则。

STEP 5 | 单击 **Add Section**（添加段），然后从下拉列表中选择 **Add Section Above**（添加上面的段）。

STEP 6 | 输入描述性 **Section Name**（段名称）。

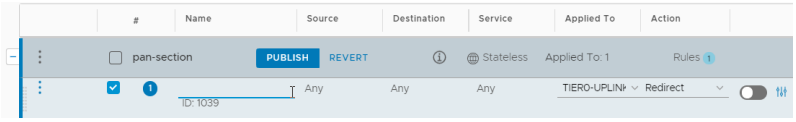
STEP 7 | 单击 **OK**（确定）。

STEP 8 | 选择新创建的段。

STEP 9 | 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。

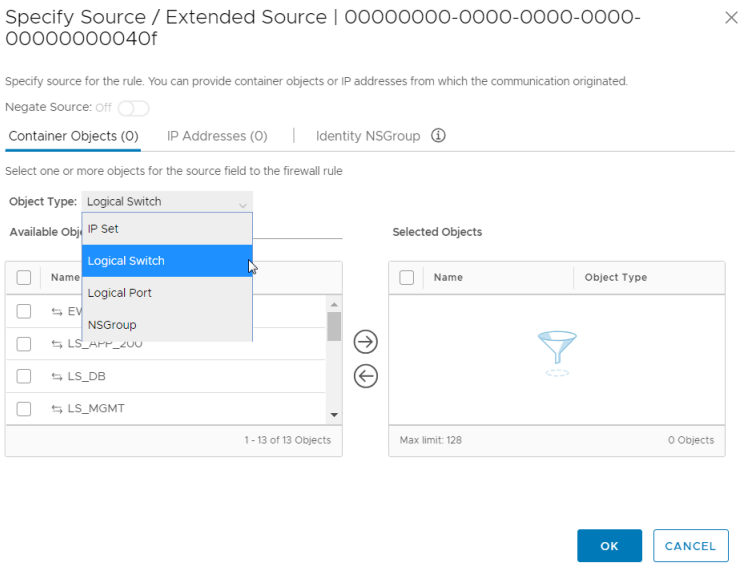
STEP 10 | 单击 **Name**（名称）字段，然后输入规则的描述性名称。



STEP 11 | 默认情况下，源设置为 Any（任何）。完成以下步骤以指定其他源。

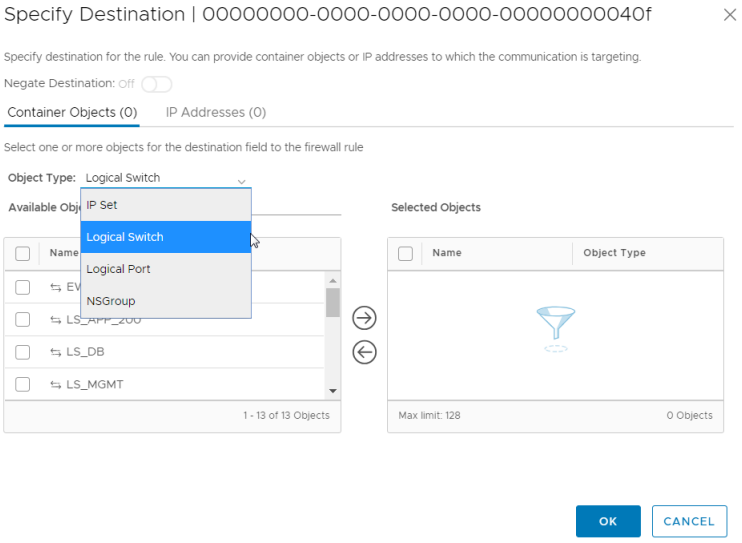
1. 在源列中单击编辑按钮 ( )，然后单击 **Edit Rule Source/Extended Source**（编辑规则源/扩展源）。
2. 要指定容器对象，请单击 **Container Objects**（容器对象）。
    1. 从下拉列表中选择 **Object Type**（对象类型）。
    2. 选择一个 **Available Objects**（可用对象）。
    3. 将所选对象移动到“选定对象”列。
3. 要指定 IP 地址，请单击 **IP Addresses**（IP 地址）。
    1. 单击 **Add**（添加）。
    2. 输入 IP 地址或 IP 地址范围。
4. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.



STEP 12 | 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. 在目标列中单击编辑按钮 ( )，然后单击 **Edit Rule Destination**（编辑规则目标）。
2. 要指定容器对象，请单击 **Container Objects**（容器对象）。
    1. 从下拉列表中选择 **Object Type**（对象类型）。
    2. 选择一个 **Available Objects**（可用对象）。
    3. 将所选对象移动到“选定对象”列。
3. 要指定 IP 地址，请单击 **IP Addresses**（IP 地址）。
    1. 单击 **Add**（添加）。
    2. 输入 IP 地址或 IP 地址范围。
4. 单击 **OK**（确定）。

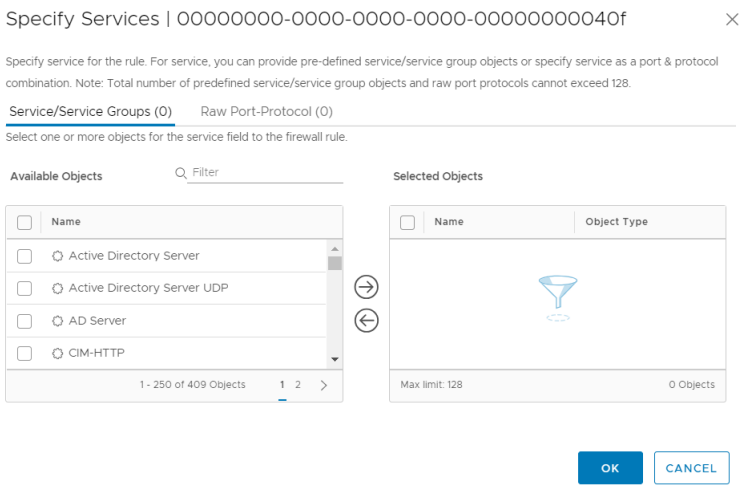


STEP 13 | 默认情况下，任何服务都会重定向到防火墙。完成以下步骤以指定某些服务和协议。

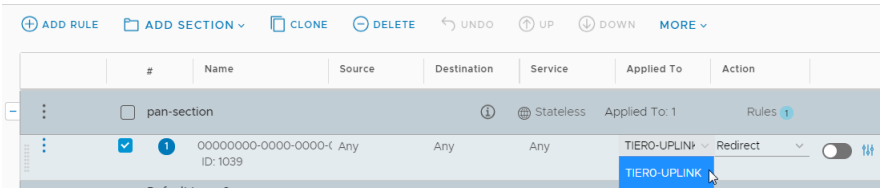
1. 在目标列中单击编辑按钮 ( )，然后单击 **Edit Rule Service**（编辑规则服务）。

© 2019 Palo Alto Networks, Inc.

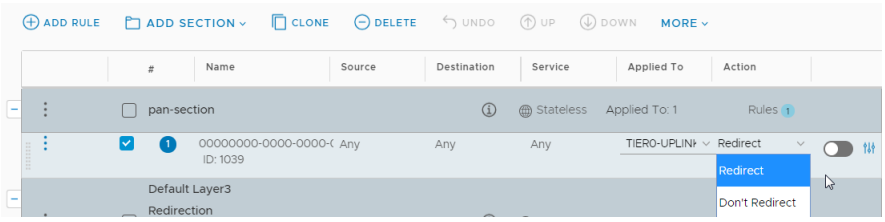
2. 要指定容器对象，请单击 **Service/Service Groups**（服务/服务组）。
    1. 选择任何 **Available Objects**（可用对象）。
    2. 将所选对象移动到“选定对象”列。
3. 要指定 IP 地址，请单击“Raw Port-Protocols（原始端口-协议）”。
    1. 单击 **Add**（添加）。
    2. 从下拉列表中选择 **Type of Service**（服务类型）。
    3. 从下拉列表中选择 **Protocol**（协议）。
    4. 根据选择的服务类型和协议，可能需要其他信息。填写任何其他字段。
    5. 单击 **OK**（确定）。
4. 单击 **OK**（确定）。



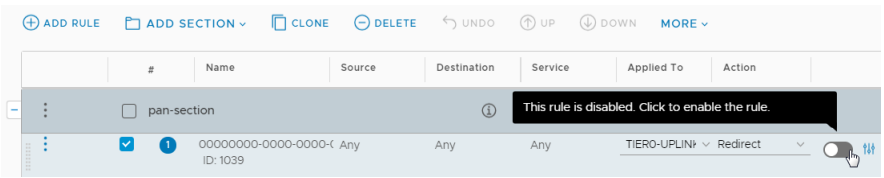
STEP 14 | 单击 **Applied To**（应用到）字段并从下拉列表中选择连接 VM 系列防火墙的路由器。



STEP 15 | 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 16 | **Enable**（启用）规则。



© 2019 Palo Alto Networks, Inc.

STEP 17 | 单击 **Publish**（发布）。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。

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。

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。

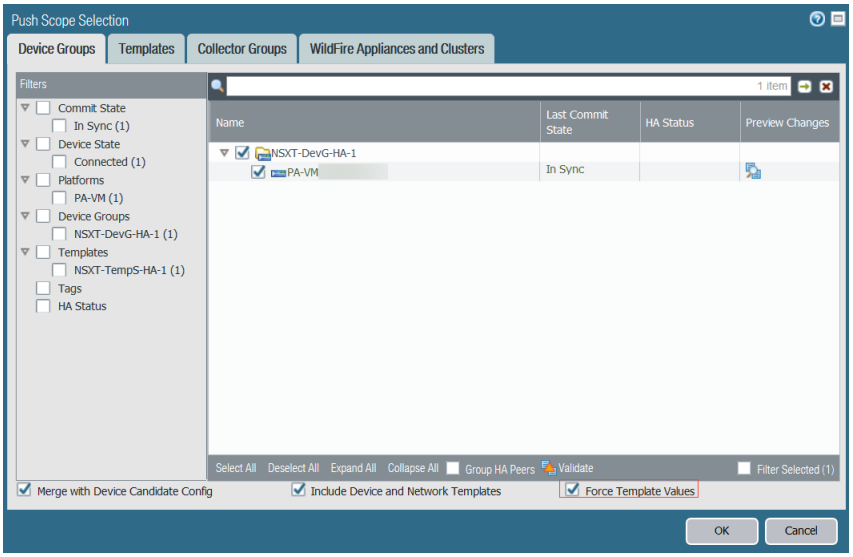
   NSX-T 上的 *VM* 系列防火墙不支持北向南流量的动态地址组。

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。

© 2019 Palo Alto Networks, Inc.



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》。

© 2019 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）
- 在 NSX-T 上部署 VM 系列防火墙（东向西）

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 是启用计算虚拟化的虚拟机监控程序。 有关 vCenter 与 NSX-T 版本的兼容性，请参阅 VMware 的兼容性矩阵。
NSX-T Manager	VMware NSX-T Data Center 2.5.0 和更高版本必须使用 vCenter 服务器进行安装和注册。需要使用 NSX - TManager 才能在 ESXi 群集内的 ESXi 主机上部署 VM 系列防火墙。

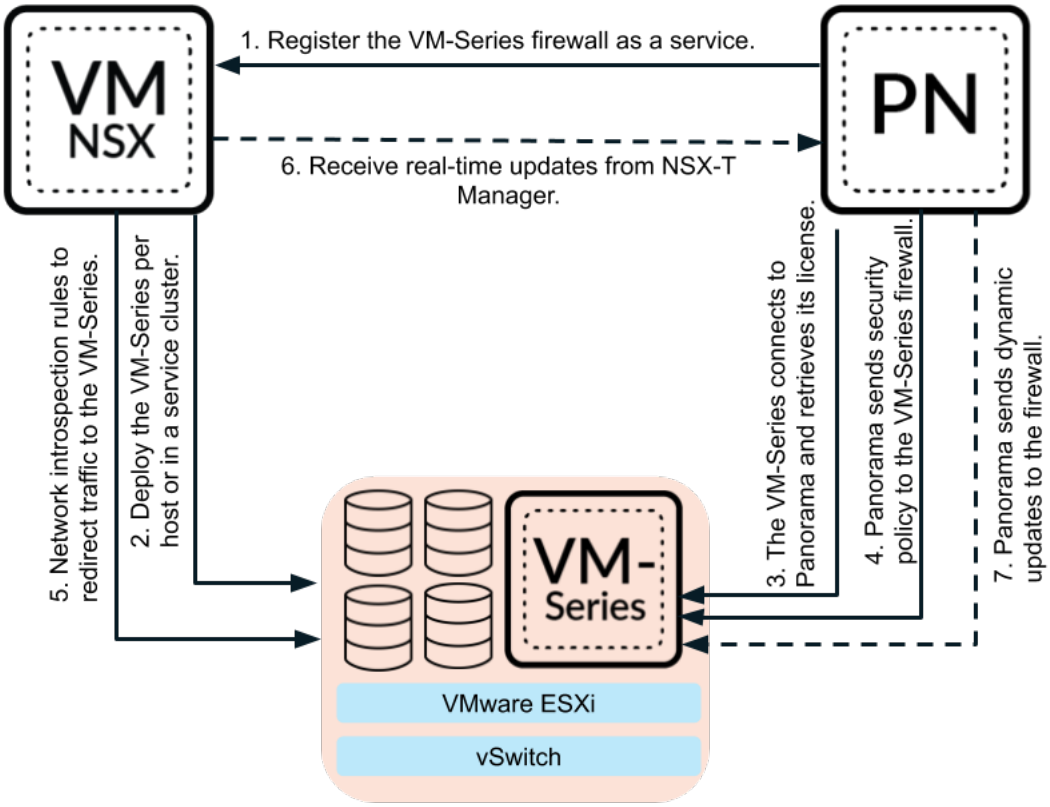
Palo Alto Networks 组件	
PAN-OS	PAN-OS 9.1.x 和更高版本。 在 NSX-T 上部署 VM 系列防火墙需要 VM 系列基本映像，例如 PA-VM-NST-9.1.0zip。 在 ESXi 服务器上部署 NSX 的 VM 系列防火墙的最低系统要求取决于 VM 系列型号。有关 VM 系列型号的最低硬件要求，请参阅 VM 系列型号。
Panorama Panorama 必须运行与用于管理防火墙的版本相同或更高的版本。	NSX-T 上的 VM 系列防火墙要求运行 9.1.0 的防火墙需要 Panorama 9.1.0 和更高版本 Panorama 是 Palo Alto 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 9.1 Panorama 管理员指南。
适用于 VMware NSX 的 Panorama 插件	3.1.0 或更高版本

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks 组件	
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。



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。

© 2019 Palo Alto Networks, Inc.

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。

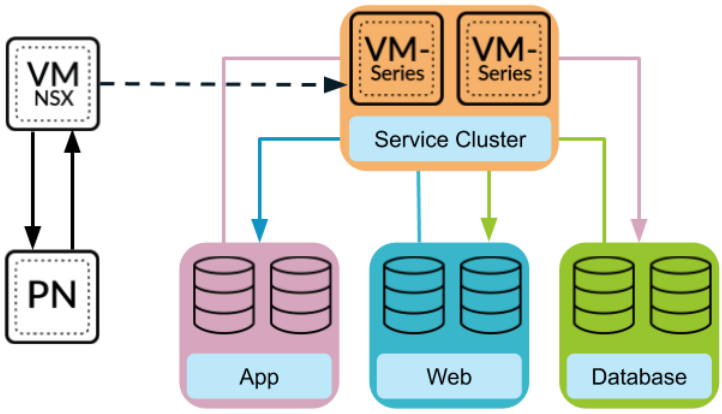
2. 在每个主机或服务集群中部署 **VM** 系列防火墙 — NSX-T Manager 使用在服务定义中从 Panorama 推送的信息部署 VM 系列防火墙。选择要部署 VM 系列防火墙的位置（在服务集群中或每个 ESXi 主机上），以及 NSX-T 如何为 VM 系列防火墙提供管理 IP 地址（DHCP 或静态 IP）。当防火墙启动时，NSX-T Manager 的 API 会将 VM 系列防火墙连接到管理程序，以便可以从 vSwitch 接收流量。
3. **VM** 系列防火墙连接到 **Panorama** — VM 系列防火墙然后连接到 Panorama 以获取其许可证。Panorama 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* 无法访问互联网，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互联网，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。有关更多信息，请参阅激活适用于 VMware NSX 的 VM 系列防火墙的许可证。
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）

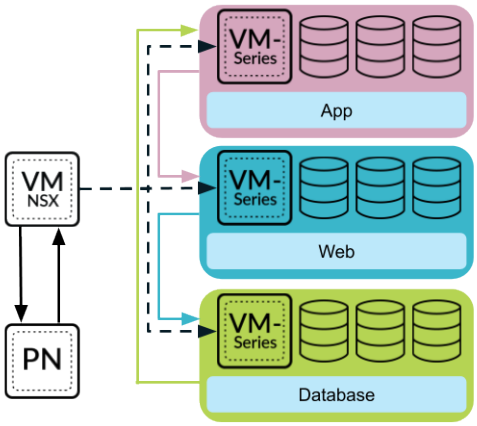
您可以将一个或多个 VM 系列防火墙实例部署为 VMware NSX-T 数据中心中的合作伙伴服务，以保护东向西流量并执行微分段。要配置 VM 系列防火墙以执行微分段，您可以将防火墙部署在服务集群或每个主机中。

- 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。



- 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。

© 2019 Palo Alto Networks, Inc.



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。

在 NSX-T 上部署 VM 系列防火墙（东向西）

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
- 将安全策略应用到 NSX-T 上的 VM 系列防火墙（东向西）
- 将流量定向到 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 对等设备上重复此安装过程。在 Panorama HA 对中安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，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。

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“操作”列中单击 **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。

© 2019 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 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**）。

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。

© 2019 Palo Alto Networks, Inc.

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 提交（**Commit**），选择 **Panorama** 作为 提交类型（**Commit Type**），以便将更改保存到 Panorama 上正在运行的配置。

STEP 2 | 添加模板。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add**（添加）。
2. 输入唯一的名称和说明，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。

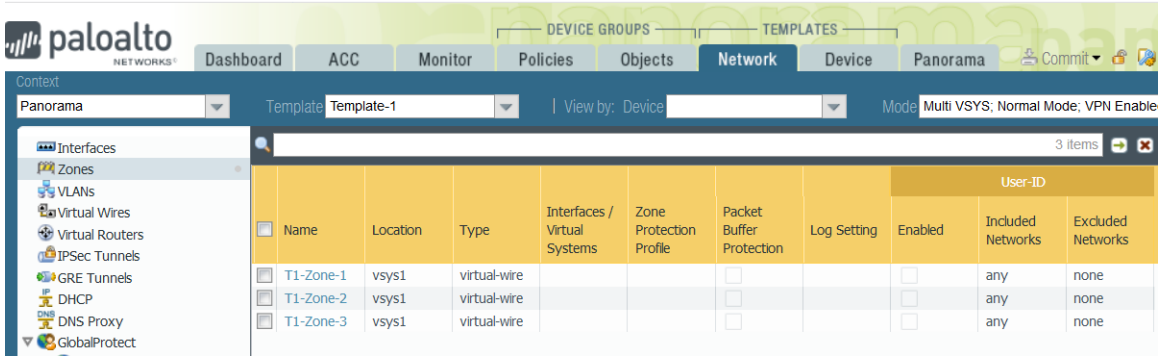
1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add Stack**（添加堆栈）。
2. 输入唯一的名称和说明，以标识模板。
3. 单击 **OK**（确定）。
4. 单击 **Commit**（提交），然后选择 **Commit to Panorama**（提交到 **Panorama**）以将更改保存到 Panorama 上正在运行的配置。

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。



© 2019 Palo Alto Networks, Inc.

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。

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。

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。

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 **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。例如，输入 **https://acme.com/software/PA-VM-NSX.9.1.0.ovf**

© 2019 Palo Alto Networks, Inc.

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 群集中的 VM 系列防火墙上使用不同的 PAN-OS 版本。

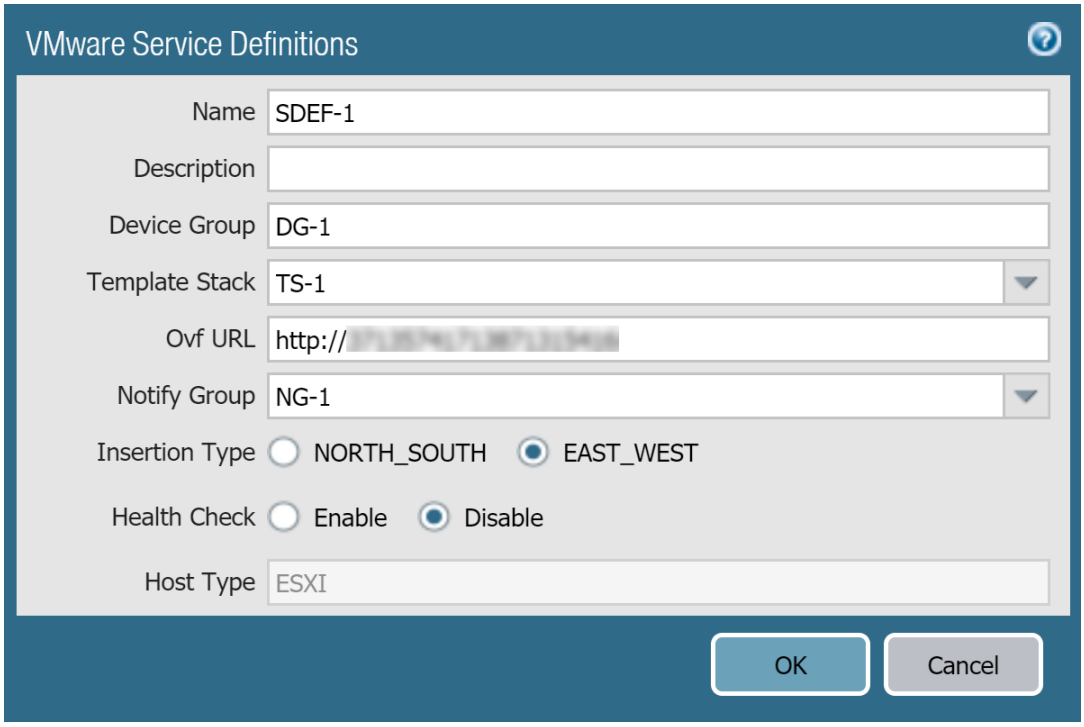
STEP 5 | （可选）选择 **Notify Group**（通知组）。

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。

STEP 8 | 单击 **OK**（确定）保存服务定义。

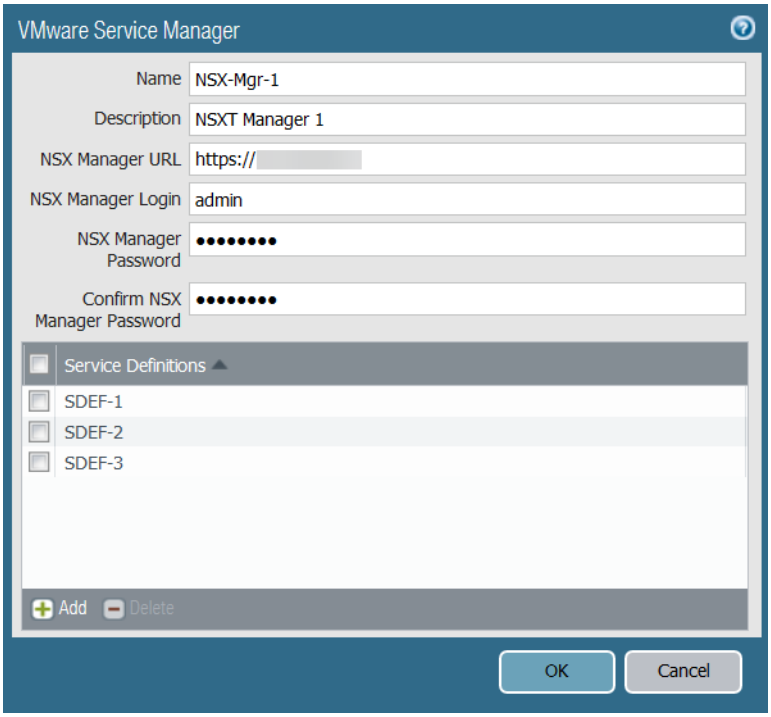


STEP 9 | 将服务定义附加到服务管理器。

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）。

© 2019 Palo Alto Networks, Inc.

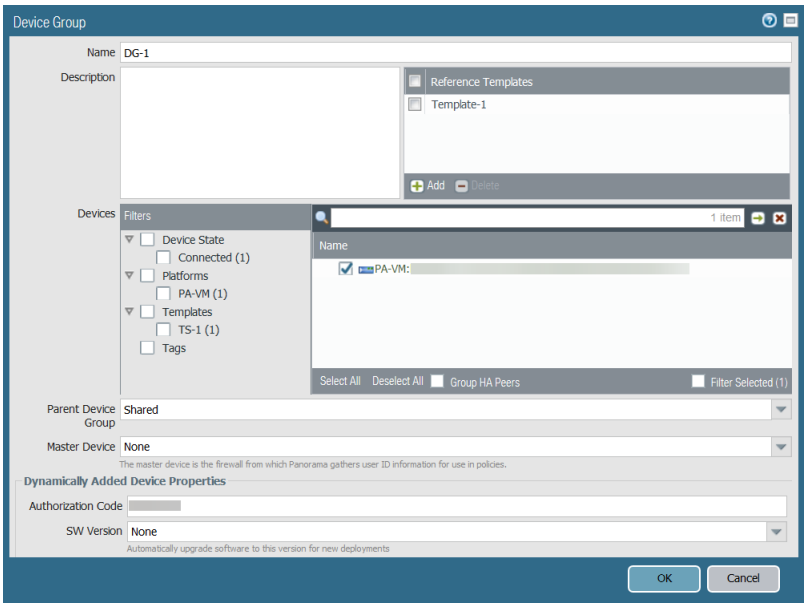


STEP 10 | 将授权代码添加到防火墙的许可证中。

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 11 | **Commit to Panorama**（提交到 **Panorama**）。

© 2019 Palo Alto Networks, Inc.

STEP 12 | 在 NSX-T Manager 上，验证服务定义是否可用。

选择 **Advanced Networking & Security**（高级网络和安全）> **Partner Services**（合作伙伴服务）> **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）。

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 8 | 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。

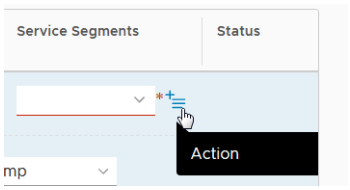
STEP 9 | 选择 **Data Store**（数据存储）作为 VM 系列防火墙的存储库。在集群部署中，如果您选择 **Any**（任何）以选择主机，请选择共享数据存储，或如果您已指定特定主机，请选择本地数据存储。

STEP 10 | 配置 **Networks**（网络）设置。

1. 在 Networks（网络）列中，单击 **Edit Details**（编辑详细信息）。
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）。

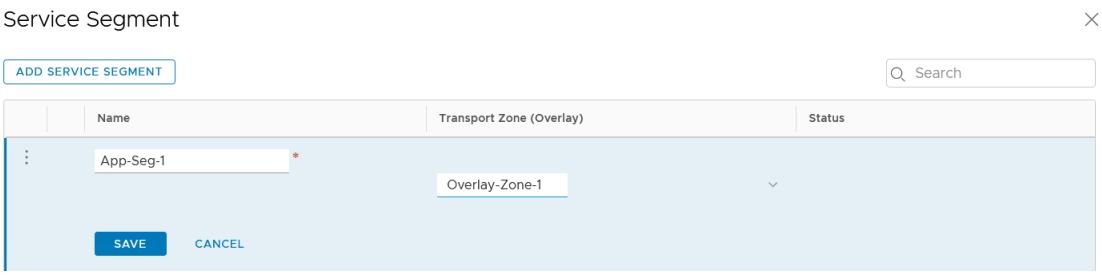
STEP 11 | 选择或配置 **Service Segment**（服务段）。要配置服务段，请完成以下过程。

1. 单击 **Service Segments**（服务段）列中的 **Action**（操作）。



© 2019 Palo Alto Networks, Inc.

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））。
5. 单击 **Save**（保存）并 **Close**（关闭）。



STEP 12 | 选择 **Deployment Type**（部署类型）— **Clustered**（集群）或 **Host Based**（基于主机）。

STEP 13 | 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 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**（受管设备）> **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）。

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 (E-W)**（网络自检 (E-W)）> **Service Chains**（服务链）> **Add Chain**（添加链）。

STEP 2 | 输入服务链的描述性 **Name**（名称）。

STEP 3 | 在 **System**（系统）> **Service Deployments**（服务部署）> **Deployment**（部署）> **Deploy Service**（部署服务）下，选择在部署 VM 系列防火墙服务时应用的 **Service Segment**（服务段）。

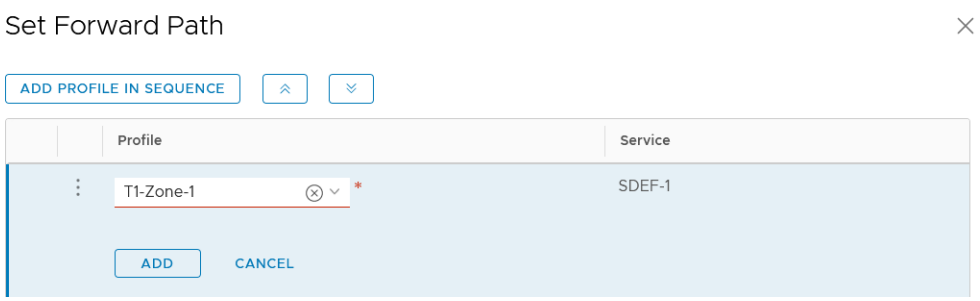
STEP 4 | 设置转发路径。服务链是服务配置文件的逻辑顺序，因此流量将按照您指定为转发路径的顺序在服务中移动。

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。

© 2019 Palo Alto Networks, Inc.

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）。

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。

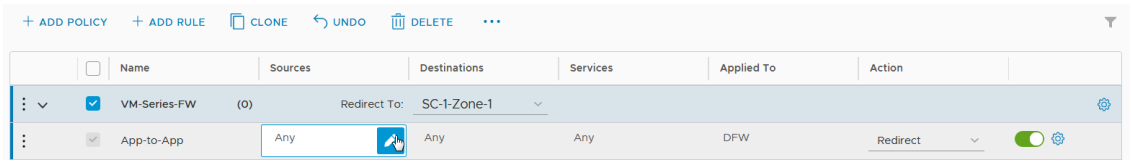
STEP 4 | 选择策略，然后单击 **Add Rule**（添加规则）。

STEP 5 | 单击 **New Rule**（新建规则）为规则指定一个描述性名称。

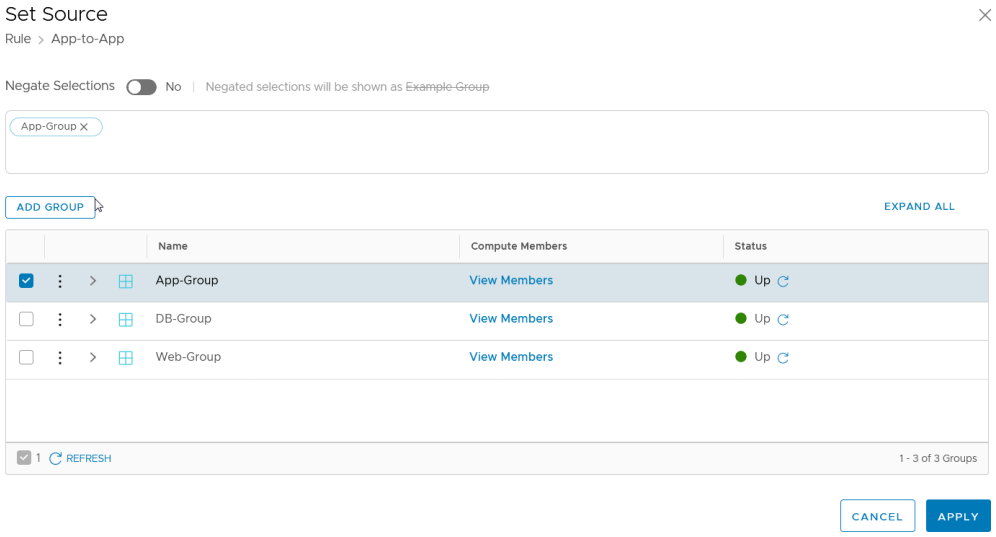
STEP 6 | 选择源。

1. 单击源列中的铅笔图标以选择虚拟机的源组。

© 2019 Palo Alto Networks, Inc.

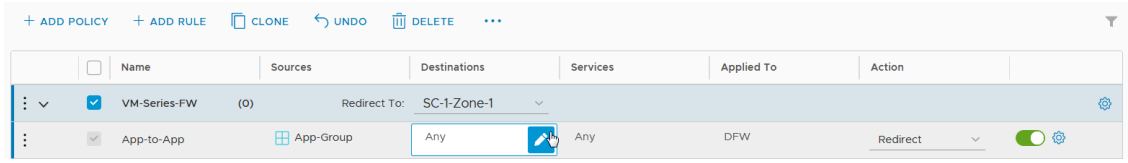


2. 选择源组或组。
3. 单击 **Apply**（应用）。

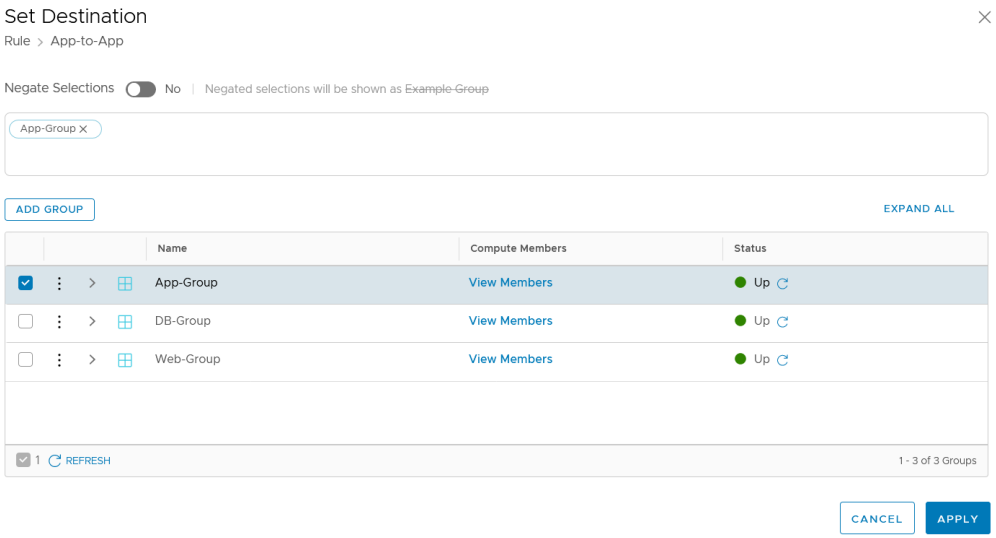


STEP 7 | 选择 **Destination**（目标）。

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）。



© 2019 Palo Alto Networks, Inc.

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。

STEP 1 | 登录到 Panorama。

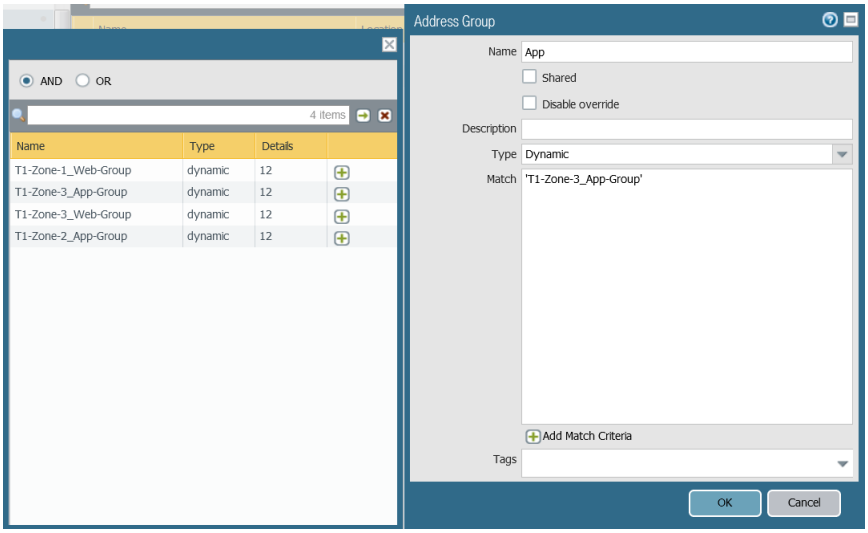
STEP 2 | 创建动态地址组。

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。

© 2019 Palo Alto Networks, Inc.



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。

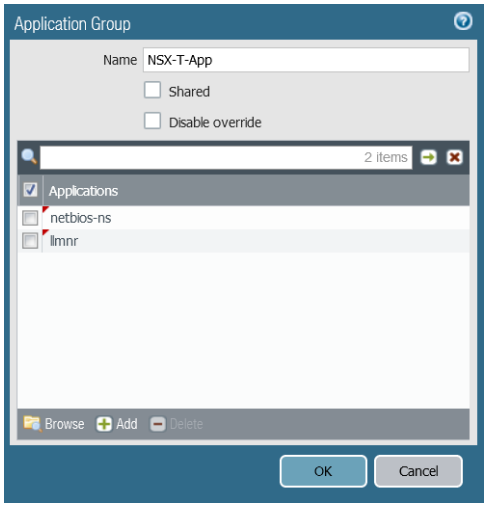
STEP 3 | 创建安全策略规则。

1. 选择 **Policies**（策略）> **Security**（安全）> **Prerules**（预订规则）。
2. 选择在将 VM 系列防火墙注册为 NSX-V Manager 上的服务中为 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。在本示例中，我们选择以下应用程序：
   3. 单击 **OK**（确定）以创建应用程序组。

© 2019 Palo Alto Networks, Inc.



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）。

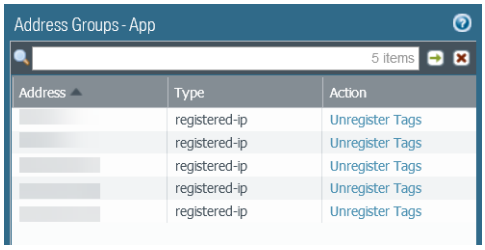
STEP 4 | 将策略应用到适用于 NSX-T 的 VM 系列防火墙。

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。

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。

© 2019 Palo Alto Networks, Inc.

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。

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
> 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
> 使用 Amazon ELB 服务自动扩展 VM 系列防火墙
> 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

AWS EC2 实例类型

VM 系列防火墙支持以下 Amazon EC2 实例类型 — C3、C4、C5、M3、M4、M5。

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。

C3、C4、M3、M4 实例类型同时支持 DPDK 和 SR-IOV 模式。DPDK 支持从 PAN-OS 9.0.3.xfr 开始提供。有关 PAN-OS 版本对 SR-IOV 和 DPDK 驱动程序的支持，请参阅 VM 系列防火墙上的 SR-IOV 和 DPDK 驱动程序。

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。

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

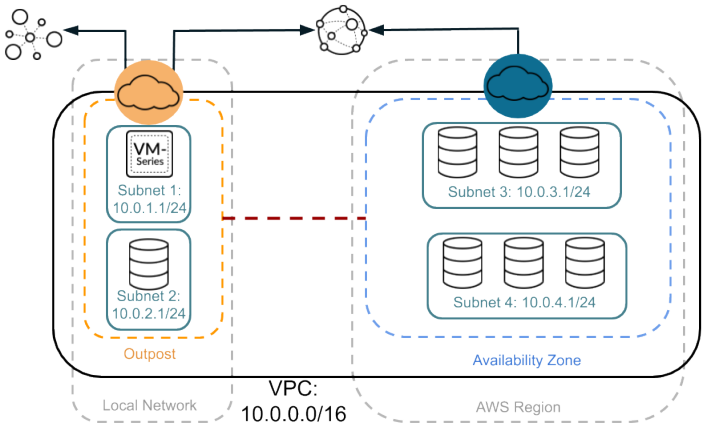
VM 系列防火墙在 AWS China Marketplace 带有 BYOL 选项，并在 AWS China（北京）和 AWS China（宁夏）地区提供。您必须拥有独立于您的全球 AWS 帐户的 AWS China 帐户才能访问此映像并在 AWS China 上使用 AWS 资源 。

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。

© 2019 Palo Alto Networks, Inc.

AWS Outposts 上的 VM 系列防火墙

您可以在本地位置的 AWS Outposts 机架上在 AWS 上安装 VM 系列防火墙。使用适用于 AWS 区域的市场 BYOL AMI，您可以在 AWS Outposts 子网中实例化 VM 系列防火墙实例。这可以让您为位于本地的工作负载提供与位于 AWS 云中的工作负载相同的安全级别。



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。 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 实例可以拥有不同的 IP 地址类型。

© 2019 Palo Alto Networks, Inc.

术语	说明
	• 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。您可以选择为在其中启动 EC2 实例的子网手动或自动分配位于 CIDR 块中范围的 IP 地址。 如果手动分配 IP 地址，Amazon 将保留每个子网中前四 (4) 个 IP 地址和最后一 (1) 个 IP 地址用于 IP 网络用途。 • 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。这些地址具有弹性，因为您可以轻松分配、附加、分离并根据需求变化释放。 公共子网中的实例可以拥有专用 IP 地址、公共 IP 地址和弹性 IP 地址 (EIP)；私有子网中的实例可以拥有专用 IP 地址和（可选）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。
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设备切换至被动对等设备。 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。

© 2019 Palo Alto Networks, Inc.

术语	说明
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。

管理接口映射以用于 Amazon ELB

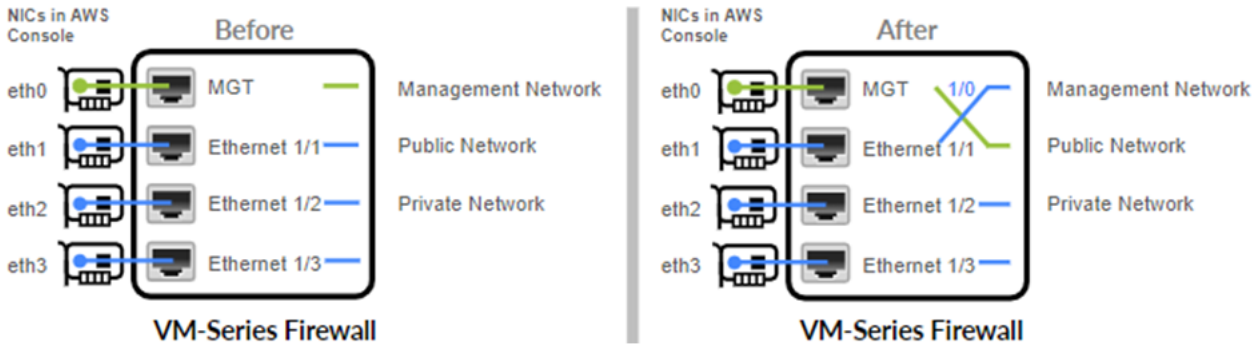
默认情况下，弹性网络接口 (ENI) eth0 会映射到防火墙上的 MGT 接口，而 ENI eth1 则会映射到防火墙上的 ethernet 1/1。由于 ELB 只能将流量发送到下一个跃点负载均衡 EC2 实例的主接口，所以 VM 系列防火墙必须能够使用数据面板流量的主接口。

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。

© 2019 Palo Alto Networks, Inc.

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。
- 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。

AWS 的 VM 系列性能调整

必须完成以下事项：

- 为部署选择正确的 AWS 实例类型。例如，因为 VM 系列防火墙需要具有 2 个或 4 个 vCPU 的 9G 内存，而实例类型仅支持 4 个 vCPU 和 7.5G 内存，因此您无法部署 c4.xlarge EC2 实例类型。

具有弹性网络适配器的 *C5* 和 *M5* 实例类型仅在 *PAN-OS 9.0.3* 和更早版本上支持 *SR-IOV* 模式。*DPDK* 支持从 *PAN-OS 9.0.3.xfr* 开始提供。

- 选择最符合部署需求的 VM 系列型号和 VM 系列防火墙许可证。有关尺寸调整的帮助，请参阅此文章。
- 使用 CLI 命令 **set system setting dpdk-pkt-io on** 启用 DPDK，或才在启动时引导防火墙以使用 DPDK（在 HA 配置的防火墙上部署时除外）。请参阅 init-cfg.txt 文件组件。

  有关 PAN-OS 版本对 SR-IOV 和 DPDK 驱动程序的支持，请参阅 VM 系列防火墙上的 SR-IOV 和 DPDK 驱动程序。

© 2019 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。

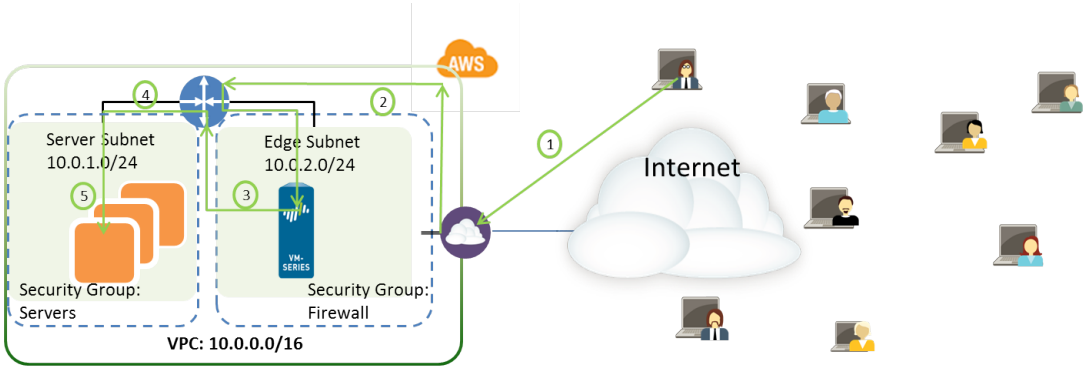


图 1: 用于 **EC2** 实例的 **VM** 系列

- 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。

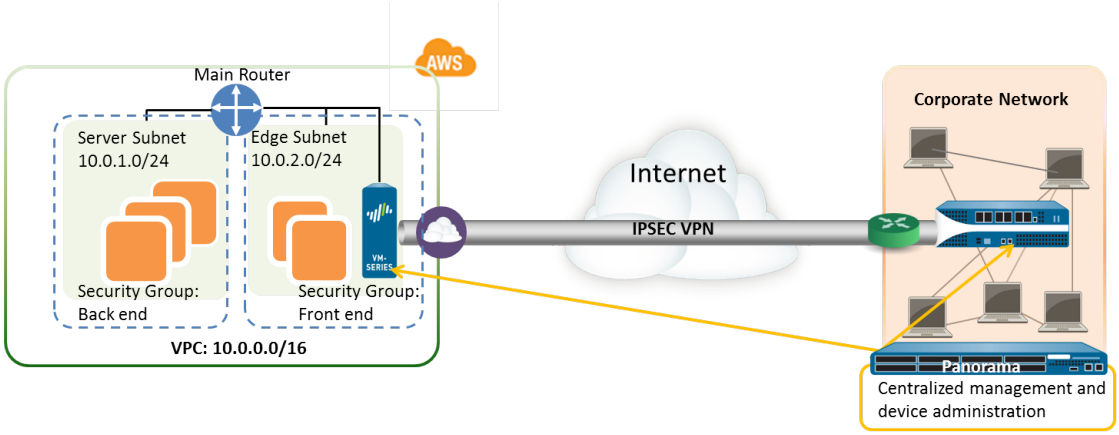


图 2: 用于 **VPN** 访问的 **VM** 系列

- 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

© 2019 Palo Alto Networks, Inc.

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）。

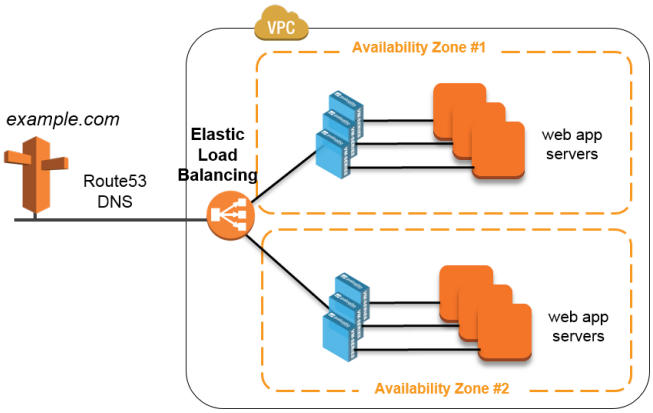


图 3: VM 系列与 ELB

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。

© 2019 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
- AWS 上的 VM 系列防火墙启动和运行状况日志

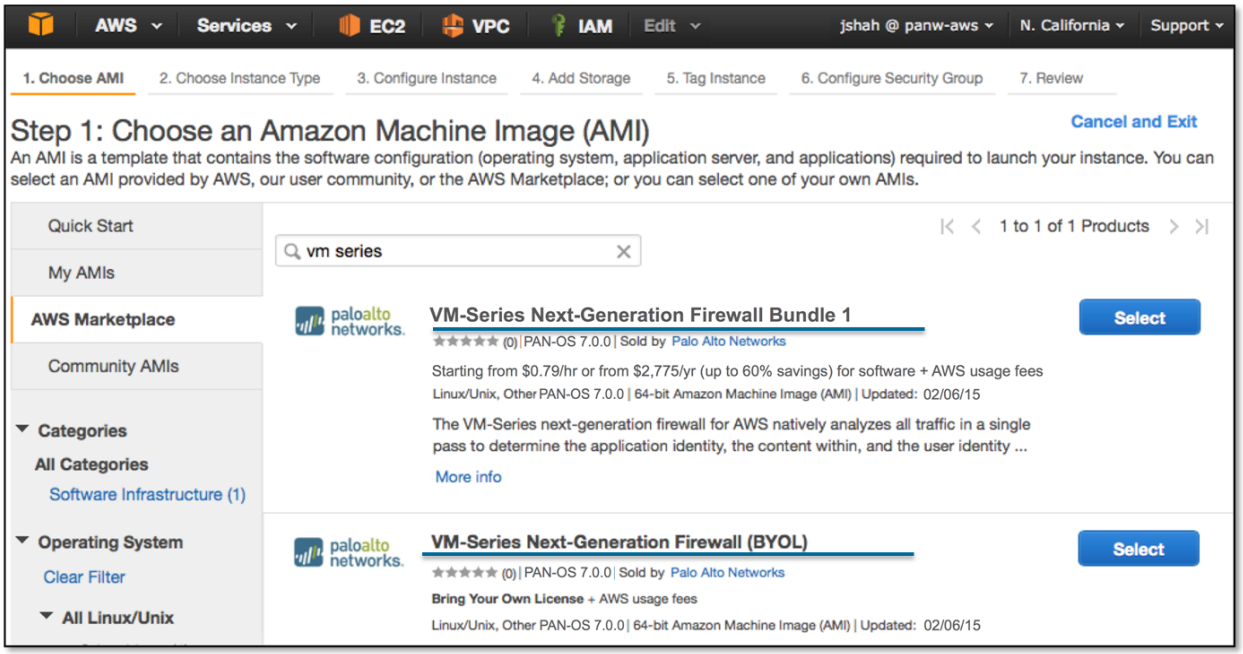
获取 AMI

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。



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 账户搜索 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。

© 2019 Palo Alto Networks, Inc.

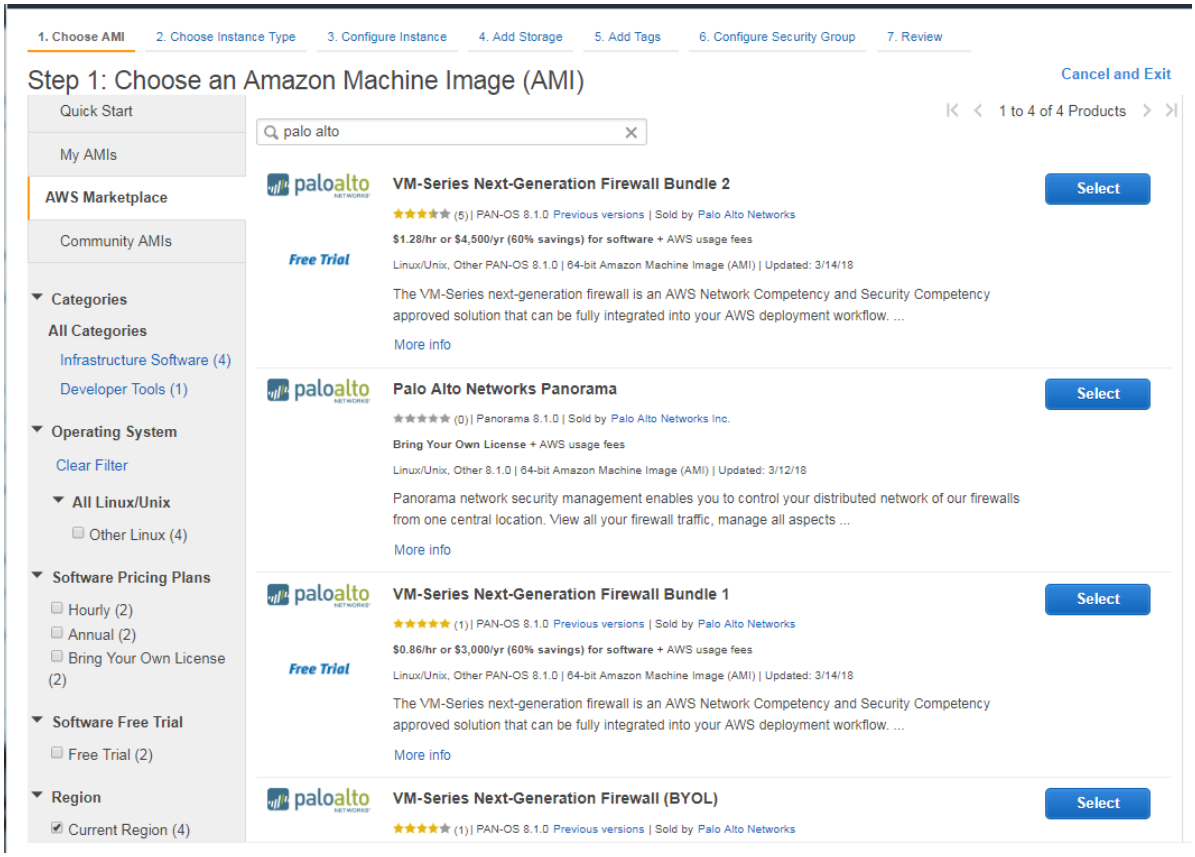


表 **1:** 查看 **AWS** 上 **VM** 系列防火墙的系统要求和限制

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。
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。

© 2019 Palo Alto Networks, Inc.

要求	详细信息
	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*

使用的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。

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：
  - 套餐 1 —

    ```
    e9yfvyj3uag5uo5j2hjikv74n
    ```

  - 套餐 2 —

    ```
    hd44w1chf26uv4p52cdynb2o
    ```

  - BYOL —

    ```
    6njl1pau431dv1qxipg63mvah
    ```


© 2019 Palo Alto Networks, Inc.

- 使用 PAN-OS 版本 — 8.1、9.0、9.1.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：要在美国加利福尼亚州区域找到适用于 PAN-OS 9.1.2 的 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*9.1*  --
region us-west-1 --output json
```

输出是：

```
{
    "ProductCodes": [
        {
            "ProductCodeId": "e9yfvyj3uag5uo5j2hjikv74n",
            "ProductCodeType": "marketplace"
        }
    ],
    "Description": "[Copied ami-0bca43c13aad118d7 from us-east-1]
PA-VM-AWS-9.1.2",
    "VirtualizationType": "hvm",
    "Hypervisor": "xen",
    "ImageOwnerAlias": "aws-marketplace",
    "EnaSupport": true,
    "SriovNetSupport": "simple",
    "ImageId": "ami-073032145e4357d41",
    "State": "available",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "SnapshotId": "snap-0009036179b39824b",
                "DeleteOnTermination": false,
                "VolumeType": "gp2",
```


© 2019 Palo Alto Networks, Inc.

```
                        "VolumeSize": 60,

                        "Encrypted": false

                    }

                }

            ],

            "Architecture": "x86_64",

            "ImageLocation": "aws-marketplace/PA-VM-AWS-9.1.2-
f1260463-68e1-4bfb-bf2e-075c2664c1d7-ami-0d106268bcff16e73.4",

            "RootDeviceType": "ebs",

            "OwnerId": "679593333241",

            "RootDeviceName": "/dev/xvda",

            "CreationDate": "2020-04-21T12:45:22.000Z",

            "Public": true,

            "ImageType": "machine",

            "Name": "PA-VM-AWS-9.1.2-f1260463-68e1-4bfb-bf2e-075c2664c1d7-
ami-0d106268bcff16e73.4"

        }
```


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：

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	

© 2019 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	如果您正在高可用性（主动/被动）配置中部署 VM 系列防火墙，则您必须确保以下条件： • 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。请参阅HA 的 IAM 角色。 • 在相同的 AWS 可用性区域中部署 HA 对等设备。 • HA 对等设备中的主动防火墙必须至少配备有 3 个 ENI：两个数据面板接口和一个管理接口。 在 HA 对中的被动防火墙必须配备有一个用于管理的 ENI，一个行使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）。

© 2019 Palo Alto Networks, Inc.

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：

STEP 1 | 访问 AWS 控制台。

登录到 AWS 控制台，然后选择 EC2 仪表盘。

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。

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。

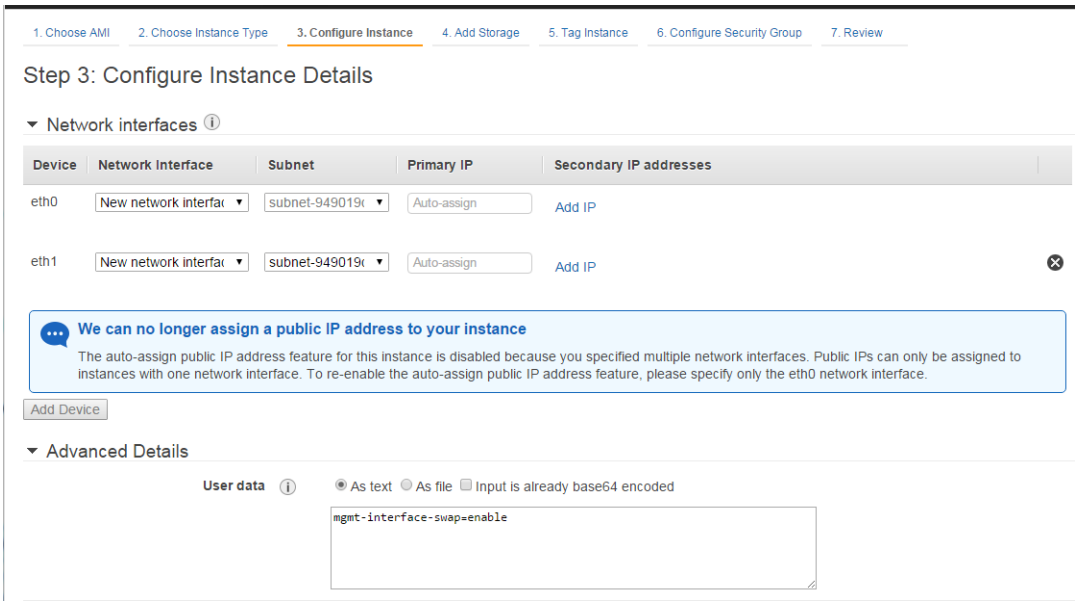
© 2019 Palo Alto Networks, Inc.

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。

     如果您正在引导防火墙，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>`***。



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**（名称）。
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 5-7 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。

© 2019 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。您将需要在步骤 3 中使用或创建的私钥才能访问命令行界面。

   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：

   ```
   configure
   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）。

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。

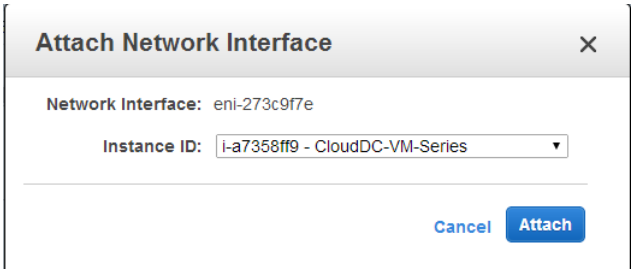
您至少需要两个可使流量传入/出防火墙的 ENI。您最多可以添加七个 ENI 来处理 VM 系列防火墙的数据流量；检查 EC2 实例类型以确认它可以支持的最大接口数量。

1. 在 EC2 仪表盘上，选择**Network Interfaces**（网络接口），并单击**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。

© 2019 Palo Alto Networks, Inc.

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，并单击**Attach**（附加）。



8. 选择 VM 系列防火墙的**Instance ID**（实例 ID），并单击**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。

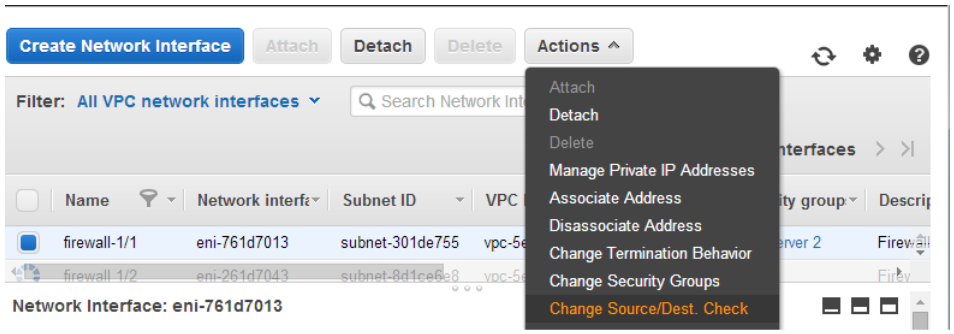
STEP 8 | 在 VM 系列防火墙上激活许可证（基于使用的许可证模型无需进行此操作）。

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。

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。

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。

© 2019 Palo Alto Networks, Inc.

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）。

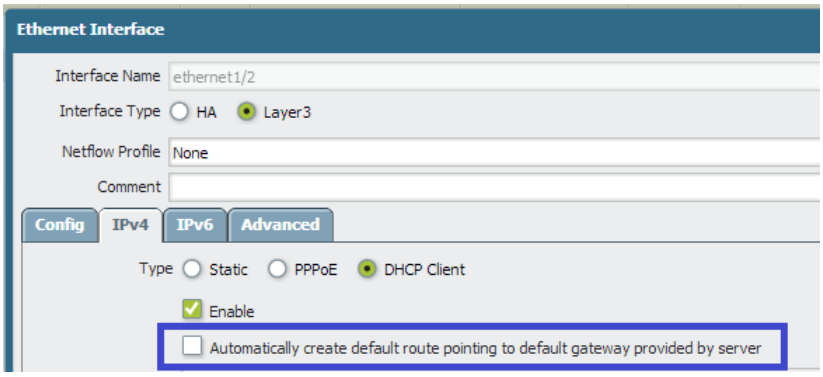
     如果使用 **Static**（静态）选项，请单击 IP 部分中的 **Add**（添加），然后输入接口的 IP 地址和网络掩码，如 10.0.0.10/24。

     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。



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。

© 2019 Palo Alto Networks, Inc.

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。

STEP 1 | 访问 AWS Outpost 控制台。

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，然后才能在 AWS 上配置主动/被动 HA。
3. （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。

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。

© 2019 Palo Alto Networks, Inc.

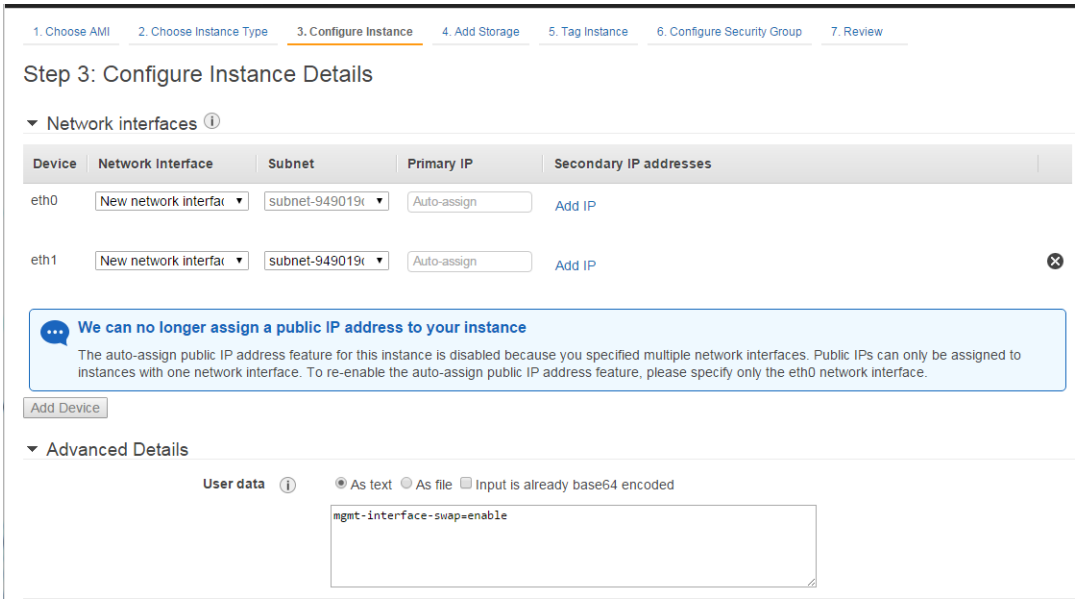
稍后，您可以将弹性 IP 地址附加到管理接口；与在终止实例时与防火墙解除相关联的公共 IP 地址不同，弹性 IP 地址可提供持久性且可以重新附加到 VM 系列防火墙的新的（或更换）实例，而不需要重新配置 IP 地址，无论您可能在何处引用。

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。

     如果您正在引导防火墙，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>`***。



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**（名称）。
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。

© 2019 Palo Alto Networks, Inc.

启动 VM 系列防火墙需要 5-7 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。您将需要在步骤 3 中使用或创建的私钥才能访问命令行界面。

   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：

   ```
   configure
   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）。

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。

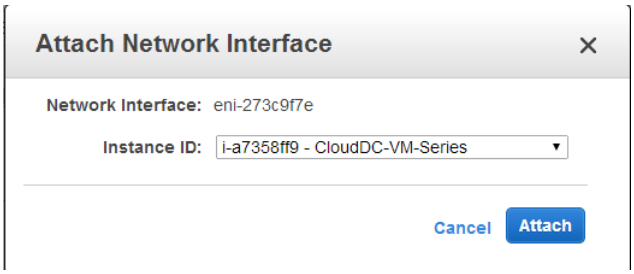
您至少需要两个可使流量传入/出防火墙的 ENI。您最多可以添加七个 ENI 来处理 VM 系列防火墙的数据流量；检查 EC2 实例类型以确认它可以支持的最大接口数量。

1. 在 EC2 仪表盘上，选择**Network Interfaces**（网络接口），并单击**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。

© 2019 Palo Alto Networks, Inc.

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，并单击**Attach**（附加）。



8. 选择 VM 系列防火墙的**Instance ID**（实例 ID），并单击**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。

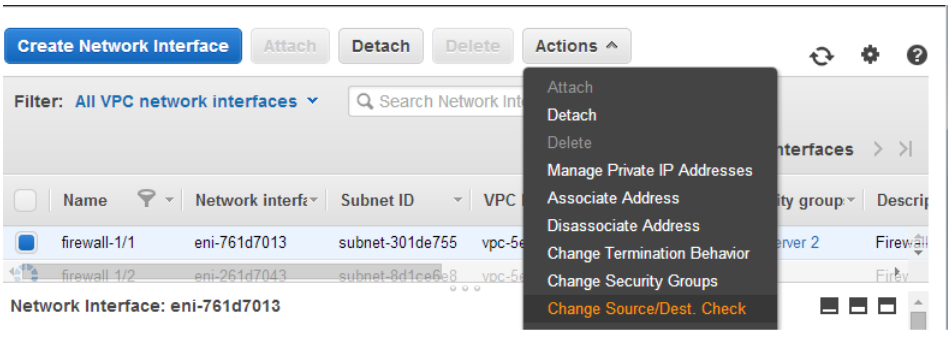
STEP 8 | 在 VM 系列防火墙上激活许可证（基于使用的许可证模型无需进行此操作）。

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。

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。

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。

© 2019 Palo Alto Networks, Inc.

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）。

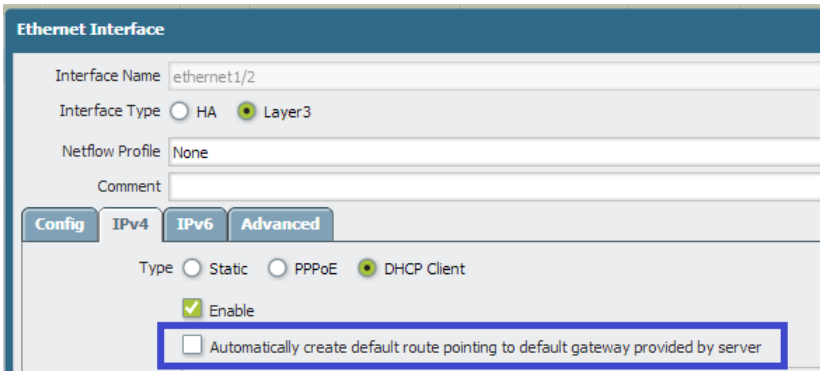
     如果使用 **Static**（静态）选项，请单击 IP 部分中的 **Add**（添加），然后输入接口的 IP 地址和网络掩码，如 10.0.0.10/24。

     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。



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。

© 2019 Palo Alto Networks, Inc.

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。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。

私有数据重置会删除所有日志并恢复默认配置。

系统磁盘未被擦除，因此步骤 4 中的内容更新完好无损。

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
```

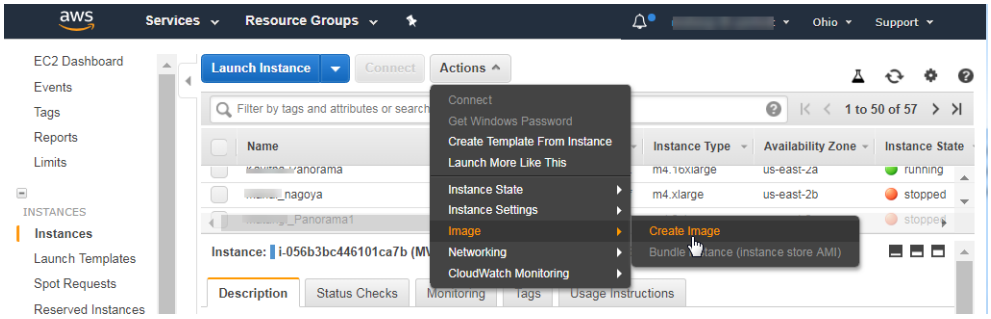

© 2019 Palo Alto Networks, Inc.

输入 ÿ 确认。

防火墙重新启动以初始化默认配置。

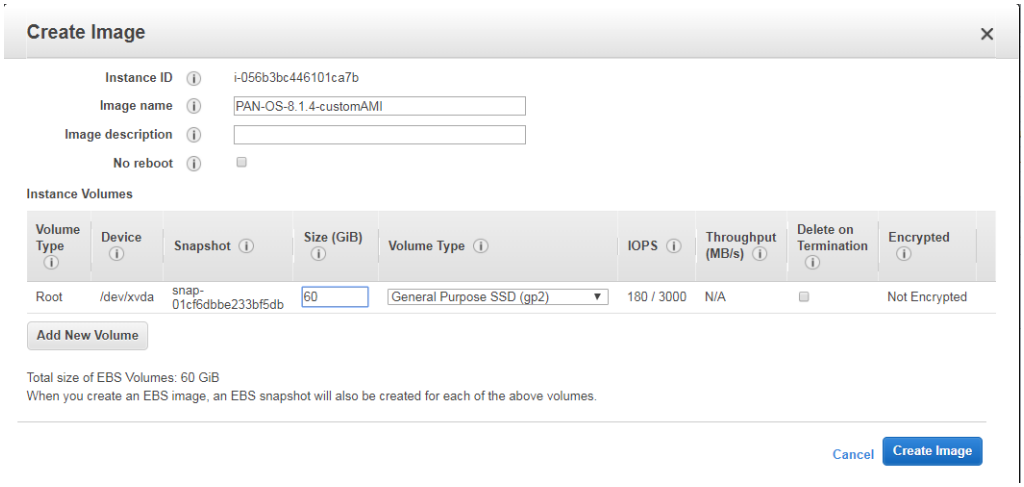
STEP 6 | 创建自定义 AMI。

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）。

   60GB 的磁盘空间是最低要求。

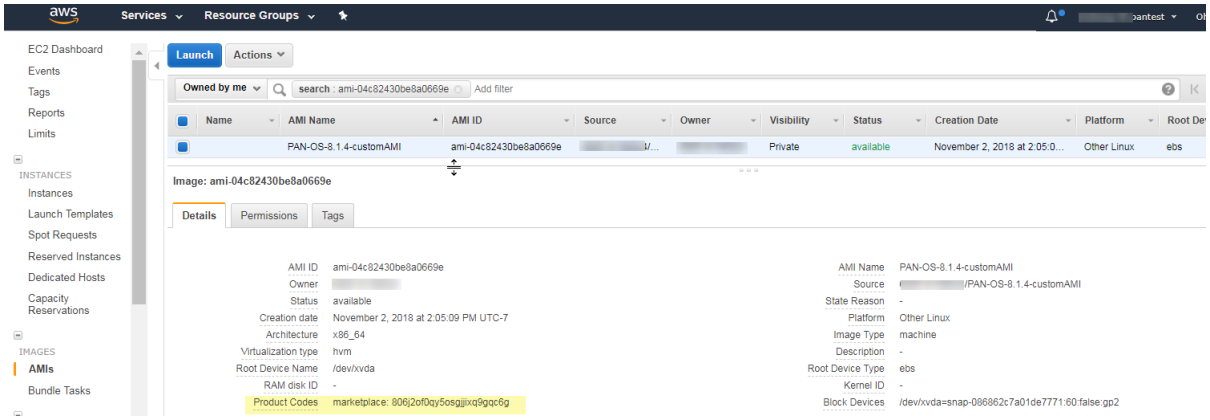


5. 验证是否已创建自定义 AMI 且具有正确的产品代码。

   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

© 2019 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 用于使用 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。

STEP 8 | 配置防火墙上的管理密码。

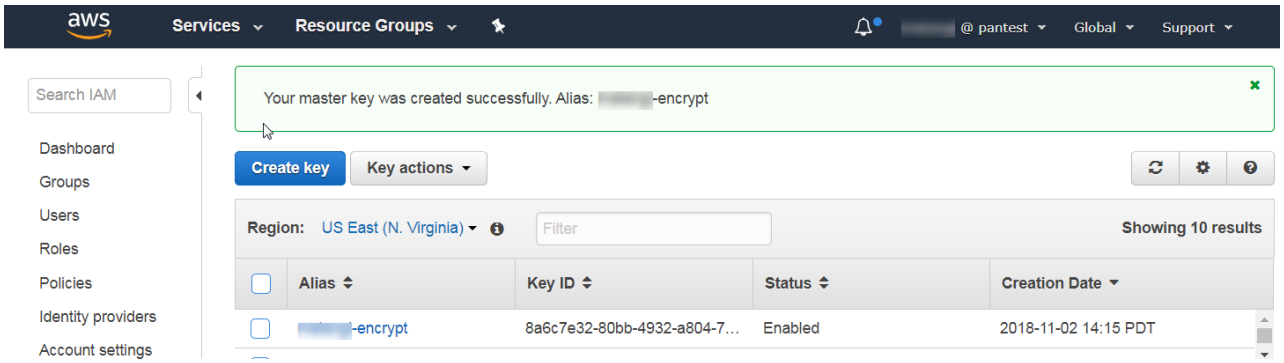
请参阅4

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。

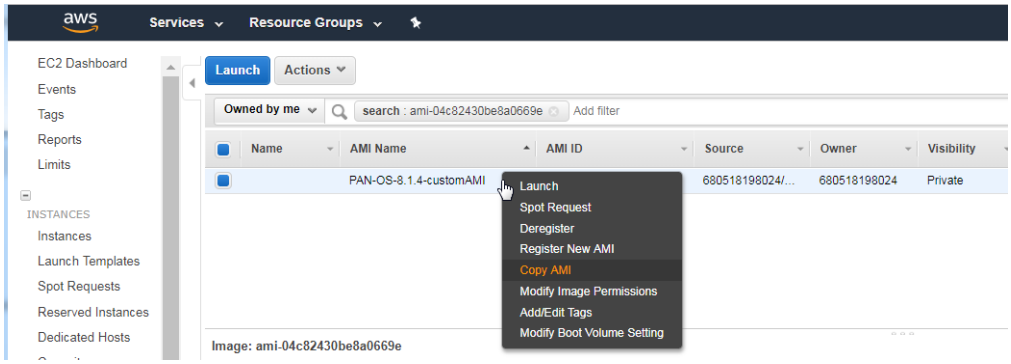


STEP 2 | 使用密钥加密防火墙上的 EBS 卷。

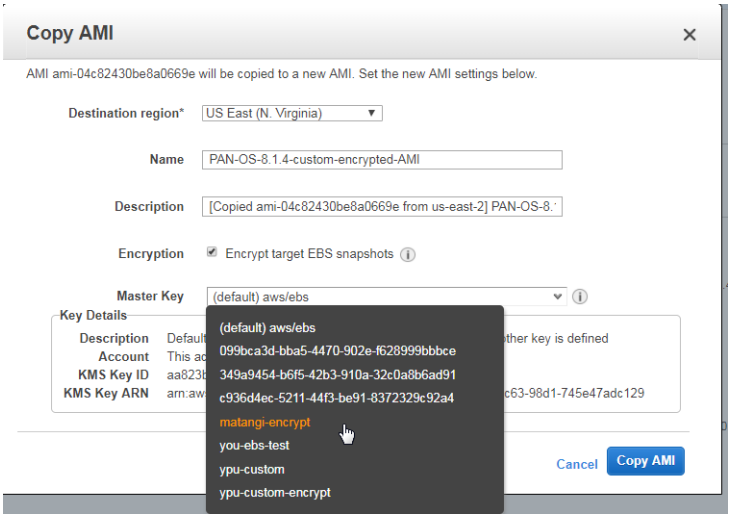
您必须创建要加密的 AMI 副本。您可以复制在 AWS 公共或 GovCloud Marketplace 上发布的 AMI，或使用自定义 AMI（创建自定义 Amazon 机器映像 (AMI)）。

1. 在 EC2 仪表盘上，选择 AMI 并 **Copy AMI**（复制 **AMI**）。

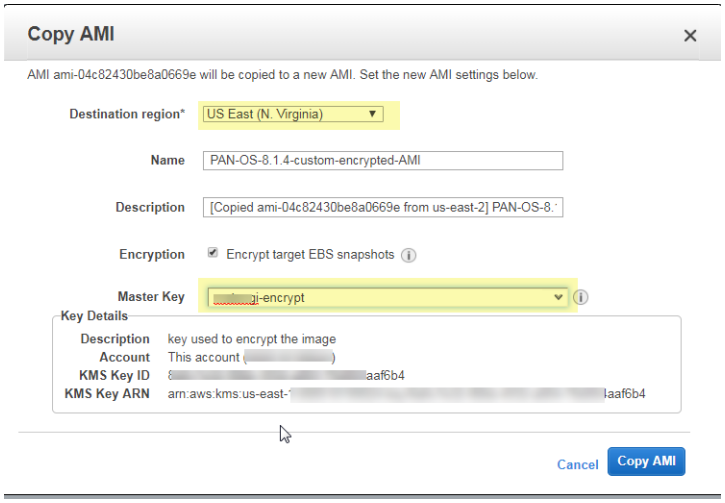
© 2019 Palo Alto Networks, Inc.



2. 设置 AMI 的详细信息。
   确保选中 **Encrypt target EBS snapshots**（加密目标 **EBS** 快照）。

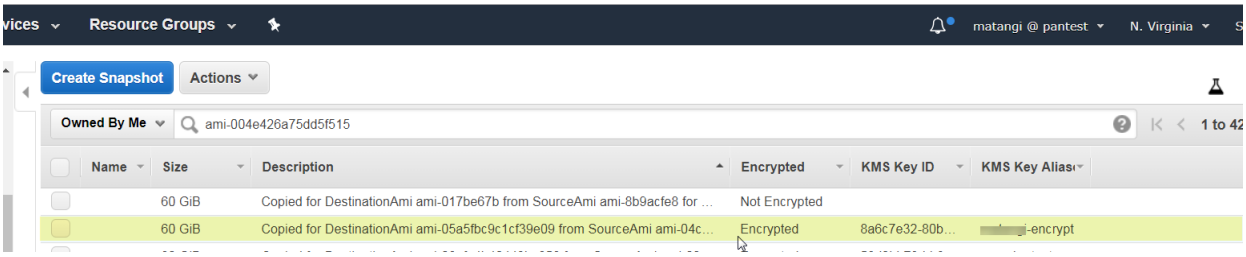


3. 选择加密密钥和 **Copy AMI**（复制 **AMI**）以创建加密的 EBS 快照。



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。

© 2019 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。

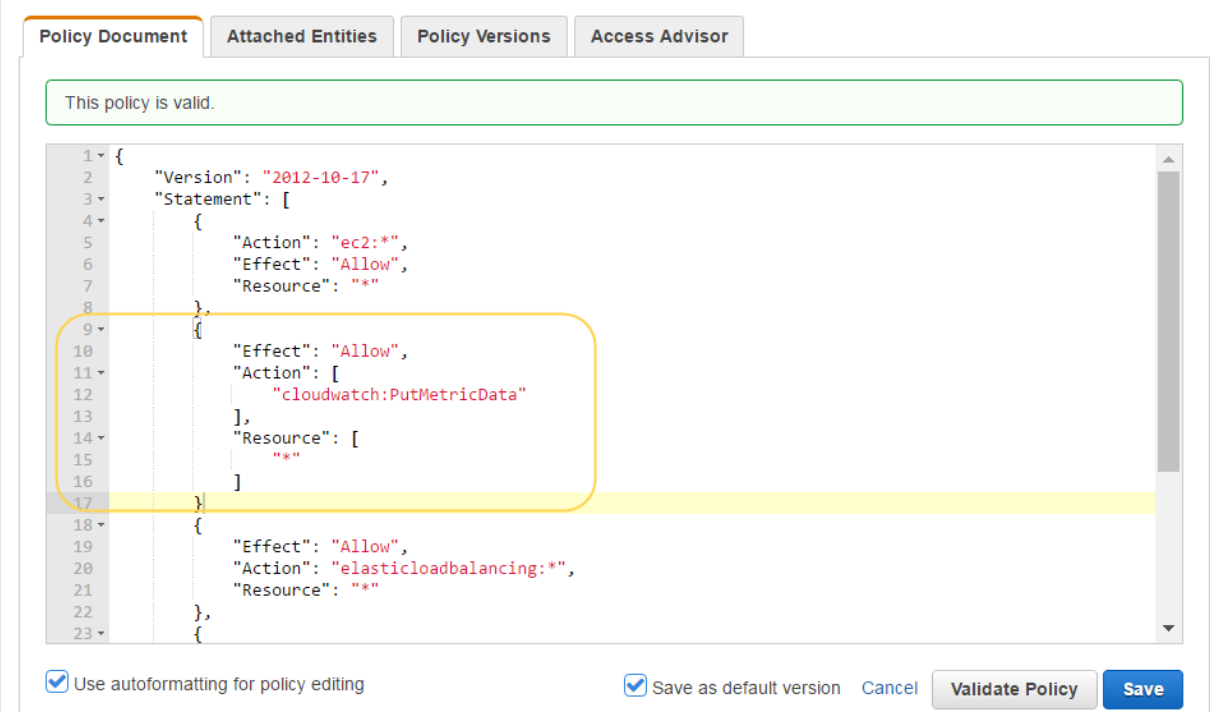
有关发布到 CloudWatch 上的 PAN-OS 指标详细信息，请参阅 发布用于监控的自定义 PAN-OS 指标。

© 2019 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": [
                 "*"
             ]
        }
    ]
}
```

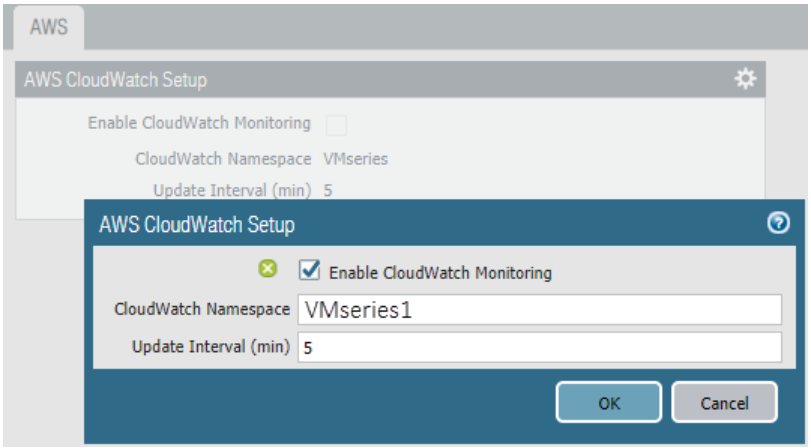
STEP 2 | 在 AWS 上的 VM 系列防火墙上启用 CloudWatch。

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）。

© 2019 Palo Alto Networks, Inc.

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。



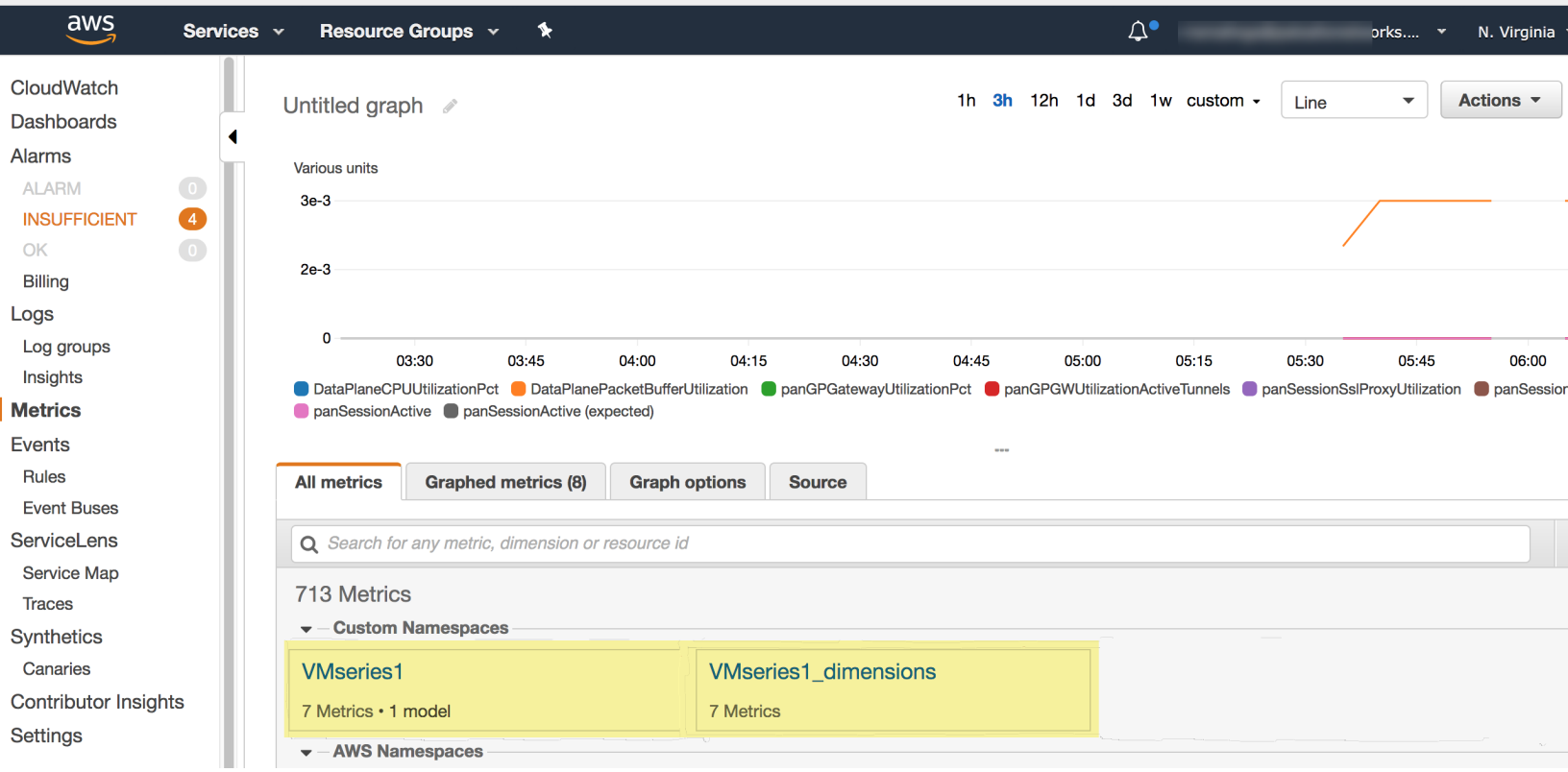
4. **Commit**（提交）更改。

   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。

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。

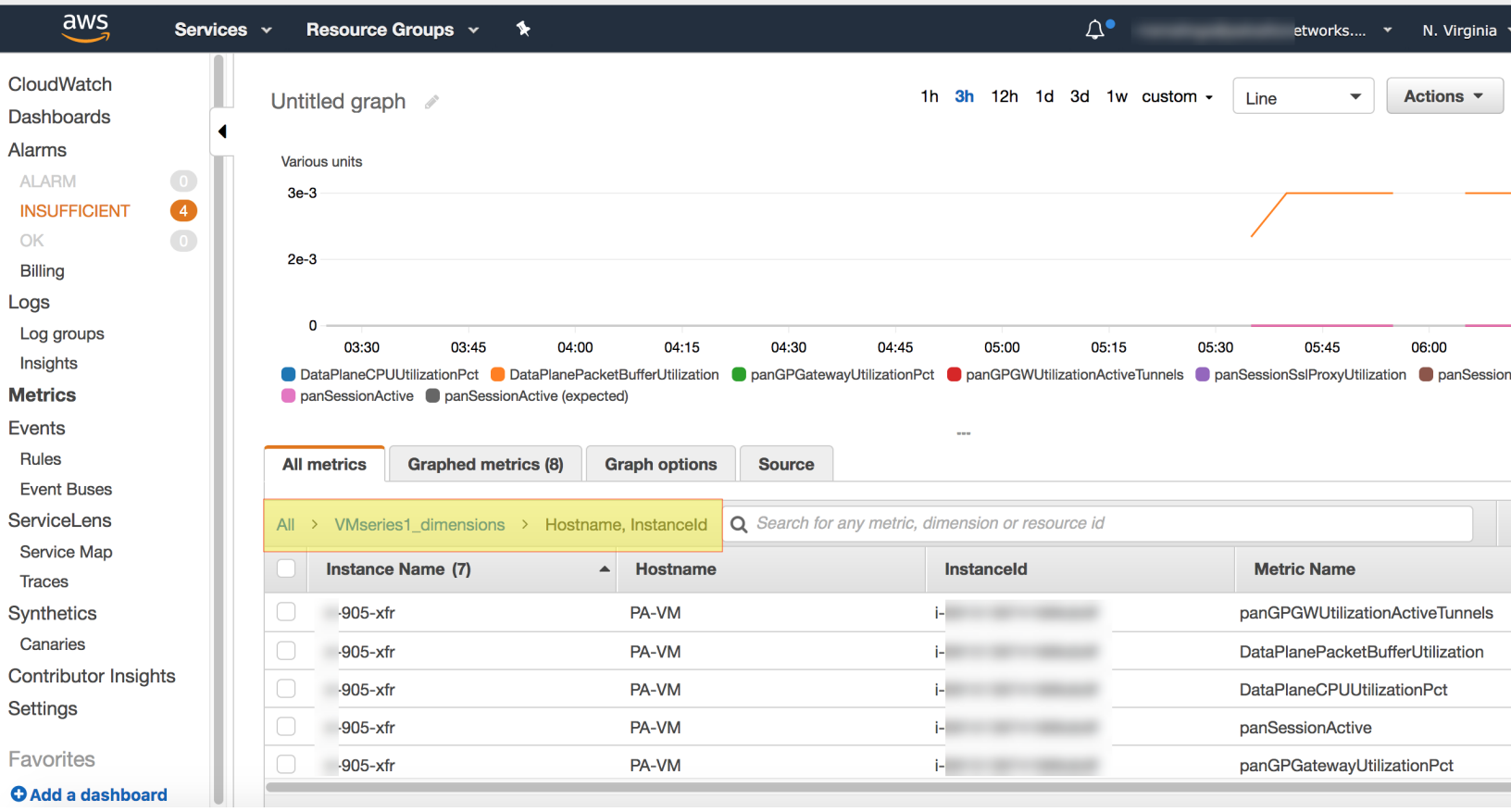
© 2019 Palo Alto Networks, Inc.



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`。

© 2019 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 7-9 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。

AWS 上的 VM 系列防火墙启动和运行状况日志

为了帮助调试部署问题，VM 系列防火墙可在系统启动期间提供系统日志。系统成功启动后，防火墙可以为系统事件生成状态消息，并且可以将系统资源的变化报告为运行状况。消息记录在 VM 系列防火墙控制台的 /dev/ttyS0 和 /dev/tty0 位置。

如果环境配置正确，则您还可以使用 AWS CloudWatch 服务查看 AWS 中部署的 VM 系列防火墙的日志。

- 在 CloudWatch 中查看 VM 系列防火墙日志
- VM 系列防火墙系统消息

© 2019 Palo Alto Networks, Inc.

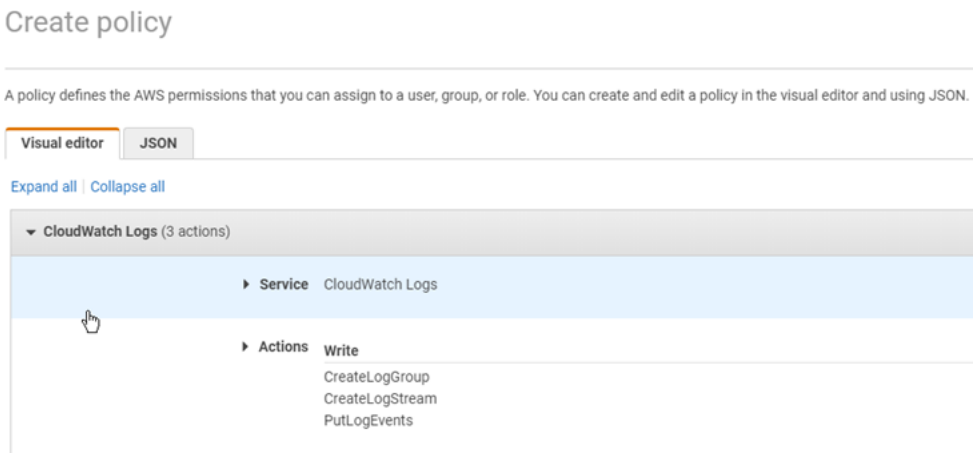
在 CloudWatch 中查看 VM 系列防火墙日志

要在 CloudWatch 中查看 VM 系列防火墙日志，防火墙至少必须运行支持系统消息的 VM 系列插件版本，如兼容性矩阵中所述。

- 确保 AWS 环境是最新的，并且 Boto3 可用。
- 您必须创建允许 VM 系列防火墙在 CloudWatch 中创建日志组和日志流的 IAM 角色和策略，并将日志事件写入日志流。

  为了确保 CloudWatch 可以显示 VM 系列防火墙日志，IAM 角色必须包括允许以下操作的策略：

  ```
  "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"
  ```



- 确保兼容性矩阵中指定的 VM 系列插件版本支持防火墙启动和运行状况日志。

VM 系列插件包括连接到 AWS CloudWatch 服务的日志记录脚本。

1. 该脚本创建日志组 **PaloAltoNetworksFirewalls**。部署中的所有 VM 系列防火墙实例都使用此日志组。
2. 该脚本创建 VM 系列防火墙特有的日志流。每个防火墙都将根据防火墙的实例 ID 配置 CloudWatch 拥有自己的日志流。
3. 记录事件后，将使用防火墙的日志流将日志消息和时间戳发送到日志组。

VM 系列防火墙系统消息

为了帮助调试，VM 系列防火墙可在系统启动期间提供系统消息。系统启动后，防火墙可以生成状态消息以报告系统运行状况。将始终报告关键运行状况事件或错误，并且您可以启用定期运行状况消息按选择的时间间隔记录系统状态。

- 消息格式
- 系统启动消息
- 运行状况状态消息
- 定期运行状况消息

消息格式

日志消息格式如下：

```
Log level :Resource :State :Details
```

- **Log level**（日志级别）
  - CRITICAL
  - ERROR
  - INFO

© 2019 Palo Alto Networks, Inc.

每个 CRITICAL 或 ERROR 事件在日志中都具有唯一 MSGID。如果您已用户定期运行状况消息，MSGID 可以帮助您区分新的 CRITICAL 或 ERROR 消息与之前未解决的问题。

```
Log level :Resource :State :MSGID :Details
```

运行状况状态 ERROR 将包含错误代码。例如：

```
ERROR :HA :DOWN :MSGID :HA status <>
```

- **Resource**（资源）
  - BOOTSTRAP
  - CONTENT
  - HA
  - INTERFACE
  - LICENSE
  - MGMTINTERFACE
  - PANORAMA
  - PANOS
  - PERIODIC_STATUS
  - SYSTEM
- **State**（状态）
  - START/READY
  - COMPLETE/FAIL
  - UP/DOWN
  - HEALTHY/UNHEALTHY
- **Details**（详细信息）— 详细信息通常从资源传递。

系统启动消息

下表根据系统启动事件按松散顺序排列。但是，顺序可以随着事件发生而改变。

- **Base OS start and network initialization**（基本操作系统启动和网络初始化）

  ```
  INFO :SYSTEM :START :Palo Alto Networks Firewall Initializing
  ```
- **PAN-OS bootstrap**（**PAN-OS** 引导）

  ```
  INFO :BOOTSTRAP :COMPLETE :Firewall Successfully Bootstrapped
  ```

  或者

  ```
  ERROR :BOOTSTRAP :FAIL :MSGID :Firewall bootstrap failureError - <>
  ```
- **Management interface swap**（管理接口交接）（如果适用）

  ```
  INFO :MGMTINTERFACE :COMPLETE :Firewall Interface Swap Configured
  ```

  或者

  ```
  ERROR :MGMTINTERFACE :MSGID :COMPLETE :Firewall Interface Swap failed <>
  ```
- **PAN-OS start**（**PAN-OS** 启动）

  ```
  INFO :PANOS :START :Firewall version <x,yz> Starting
  ```

  或者

  ```
  CRITICAL :PANOS :FAIL:MSGID :Firewall failed to start version <x,yz>

  INFO :SYSTEM :START :Palo Alto Networks Firewall Initializing
  ```
- **Load license**（加载许可证）

  ```
  INFO :LICENSE :COMPLETE :Firewall successfully licensed <model>
  ```


© 2019 Palo Alto Networks, Inc.

或者

```
CRITICAL :LICENSE :FAIL :MSGID :Firewall failed to license <reason>
```

- **Load content**（加载内容）

```
INFO :CONTENT :COMPLETE :Firewall content version <> loaded.
```

或者

```
ERROR :CONTENT :FAIL :MSGID :Firewall content version <> failed to load.
```

- **Dataplane processes up, and auto commit**（数据平面处理和自动提交）

```
INFO :COMMIT :COMPLETE :Auto-commit job successful.Firewall license -
<model>
```

或者

```
CRITICAL :COMMIT :FAIL:Auto-commit job failed <reason>.
```

- **Panorama registration, Panorama connected**（**Panorama** 注册，**Panorama** 已连接）（如果适用）

```
INFO :PANORAMA :COMPLETE:Connected to Panorama <IP>
```

或者

```
ERROR :PANORAMA :FAIL :MSGID:Failed to connect to Panorama <IP>
```

- **System ready and interfaces up**（系统就绪和接口启动）

```
INFO :SYSTEM :READY :Firewall ready to process traffic.Firewall license -
<model>
```

运行状况状态消息

运行状况消息将报告资源的状态。系统成功启动后，将所有系统运行状况事件设置为 UP，并报告后续状态变化。如消息格式中所述，运行状况状态 ERROR 消息将包含状态代码。在下面的消息示例中，<> 是状态代码的占位符。

如果管理员执行故意关闭，则不会报告关闭。

- **CloudLoggingConnectionFailed**

  如果没有 CloudWatch 日志（由于连接失败），您可以检查 PAN-OS 日志 `vm_cloud_logging.log`。

- **Data path interface failure**

  消息：`ERROR :INTERFACE :DOWN :MSGID :Interface <> went down`

- **HA interface failure**（**HA** 接口故障）— 此消息适用于单个防火墙；并不表明有关 HA 对的任何运行状况。例如，辅助防火墙关闭后，主要防火墙状态可以为 UP。

```
INFO :HA :UP :HA status <>
```

或者

```
ERROR :HA :DOWN :MSGID :HA status <>
```

- **Peer HA interface failure**（对等 **HA** 接口失败）— 此消息是 HA 对中的对等状态。

```
ERROR :PEER_HA :UP :Peer HA status <>
```

或者

```
ERROR :PEER_HA :DOWN :MSGID :Peer HA status <>
```

- **Panorama Connectivity**（**Panorama** 连接）

```
ERROR :PANORAMA :DOWN :MSGID :Lost Panorama <IP> connectivity
```


© 2019 Palo Alto Networks, Inc.

或者

```
INFO :PANORAMA :UP :Panorama <IP> connected
```

定期运行状况消息

如果运行状况没有发生变化，则您可以选择生成定期运行状况状态消息。默认情况下，云日志记录时间间隔为 0（无消息）。

例如，如果状态保持 Up，则消息为：

```
INFO :PERIODIC_STATUS :HEALTHY :All resources healthy
```

如果存在无法解决的运行状况故障，则定期运行状况状态消息将重新打印这些故障。如消息格式中所述，MSGID 可以帮助您在查看定期日志时区分错误。

```
INFO :PERIODIC_STATUS :UNHEALTHY :Resources unhealthy
```

```
ERROR :INTERFACE :DOWN :MSGID :Interface ethernet1/2 down
```

- **Set the periodic interval from 10 to 300 seconds**（将定期时间间隔设置为从 10 至 300 秒）
  - **CLI**：

    request plugins vm_series cloud-logging interval <seconds>
  - **XML API**：

```
api/?type=op&cmd=<request>
  <plugins>
    <vm_series>
      <cloud-logging>
        <interval>seconds</interval>
      </cloud-logging>
     </vm_series>
   </plugins>
</request>
```

- 显示云日志记录时间间隔 — 使用 CLI 显示当前时间间隔（以秒为单位）。

  show plugins vm_series cloud-logging interval
- 禁用定期日志记录 — 使用 CLI 关闭定期日志记录。

  request plugins vm_series cloud-logging interval 0

© 2019 Palo Alto Networks, Inc.

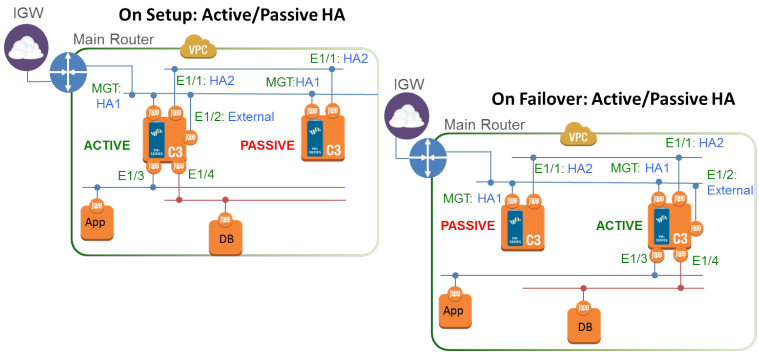
AWS 上 VM 系列防火墙的高可用性

AWS 上的 VM 系列防火墙仅支持主动/被动 HA；如果已使用 Amazon 弹性负载平衡 (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）。

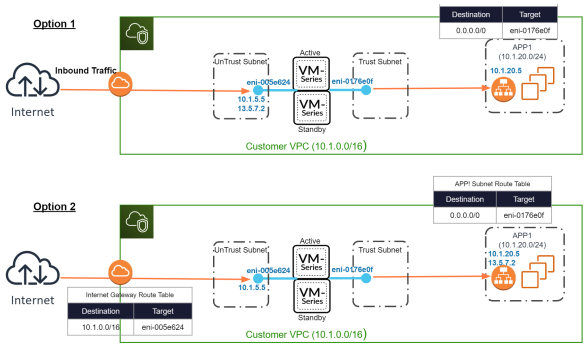
- AWS 上 HA 的概述
- HA 的 IAM 角色
- HA 链接
- 检测信号轮询和呼叫消息
- 设备优先级和抢先
- 高可用性计时器
- 在 AWS 上配置主动/被动 HA

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。主动对等设备将与相同配置的被动对等设备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。当被动对等设备检测到故障时，它将成为主动设备并触发 API 向 AWS 基础架构发出请求，以将所有数据面板接口 (ENI) 从已故障的对等设备移至其本身。故障转移时间可能从 20 秒至 1 分钟以上不等，具体取决于 AWS 基础架构的相应能力。



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。



© 2019 Palo Alto Networks, Inc.

HA 的 IAM 角色

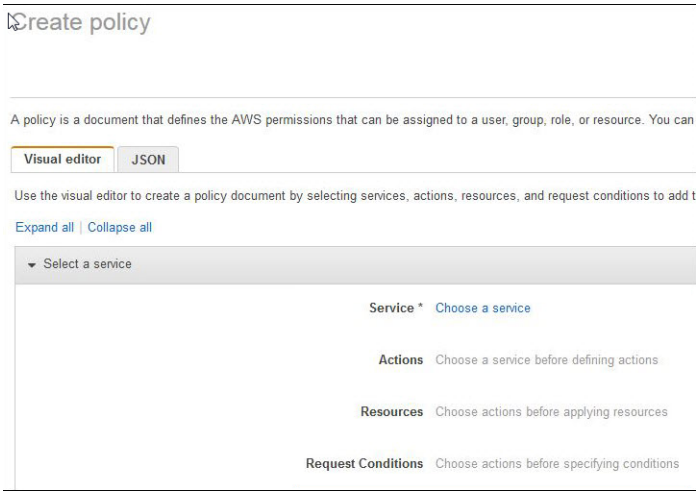
AWS 要求所有 API 请求必须使用由其发布的凭证进行加密签名。要为部署为 HA 对的 VM 系列防火墙启用 API 权限，必须创建一个策略，然后将该策略附加到 AWS 身份识别及访问管理 (IAM) 服务中的角色。相关角色必须在启动时附加到 VM 系列防火墙。该策略赋予 IAM 角色权限，使其能够在触发故障转移时将网络接口从 HA 对中的主动对等设备分离，然后附加到被动对等设备。

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。

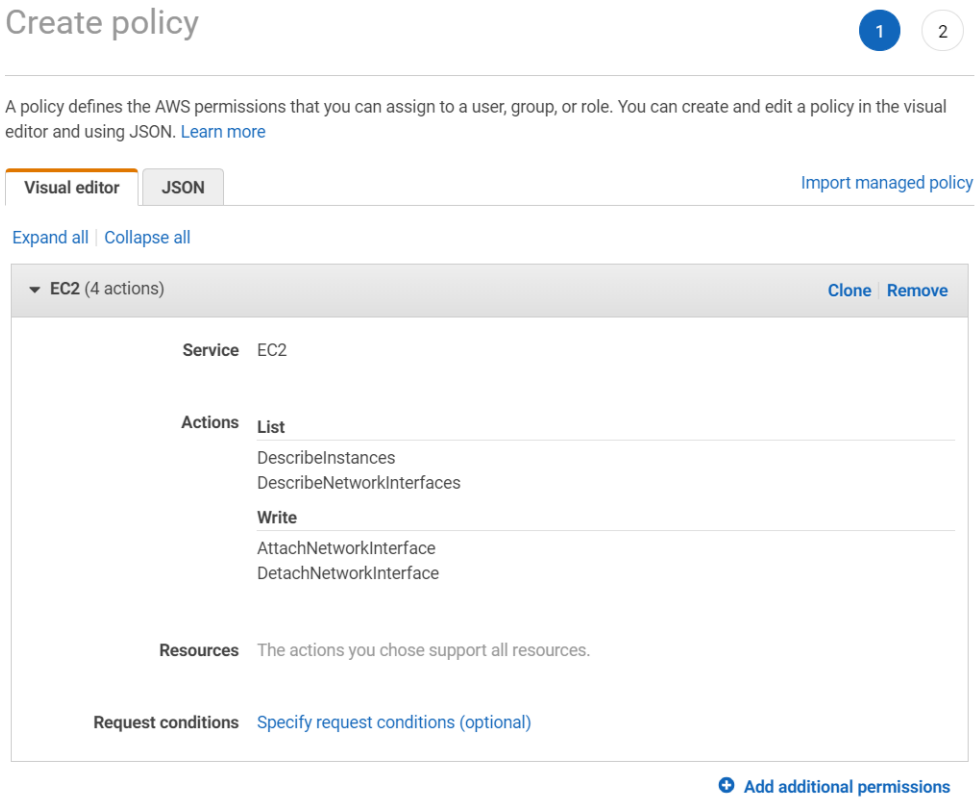
在 AWS 控制台中配置的 IAM 策略必须具备针对以下操作和资源的权限（基本要求）：

- AttachNetworkInterface — 用于允许附加 ENI 至实例。
- DescribeNetworkInterface — 用于提取 ENI 参数，以将接口附加至实例。
- 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。
- Wild card (*)— 在 Amazon 资源名称 (ARN) 字段中将 * 用作通配符。

以下屏幕截图显示了针对上述 IAM 角色进行的访问管理设置：



© 2019 Palo Alto Networks, Inc.



您需要的权限包括：`{"Version":"2012-10-17","Statement":[{"Sid":"VisualEditor0","Effect":"Allow","Action":["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstances","ec2:I"*"}]}`

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：

- **Control Link**（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)。
- **Data Link**（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（'93;HA2 保持活动状态'94;除外）；它从主动设备流动到被动设备。

  Ethernet1/1 必须被分配为 HA2 链接。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高可用性计时器的详细信息，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）。

© 2019 Palo Alto Networks, Inc.

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。

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。

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
监视失败持续时间	0/0 ms
额外主设备持续时间	500/500 ms

在 AWS 上配置主动/被动 HA

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。参阅 HA 的 IAM 角色。

  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 AWS 文档。
- 无法在 HA 配置中启用 DPDK。默认情况下，AWS 上的 VM 系列防火墙已禁用 DPDK，除非您手动启用它，否则无需将其禁用。
- HA 对等设备中的主动防火墙必须至少配备有 3 个 ENI：两个数据面板接口和一个管理接口。

© 2019 Palo Alto Networks, Inc.

在 HA 对中的被动防火墙必须配备有一个用于管理的 ENI，一个行使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）。

- 必须在相同的 AWS 可用性区域中部署 HA 对等设备。

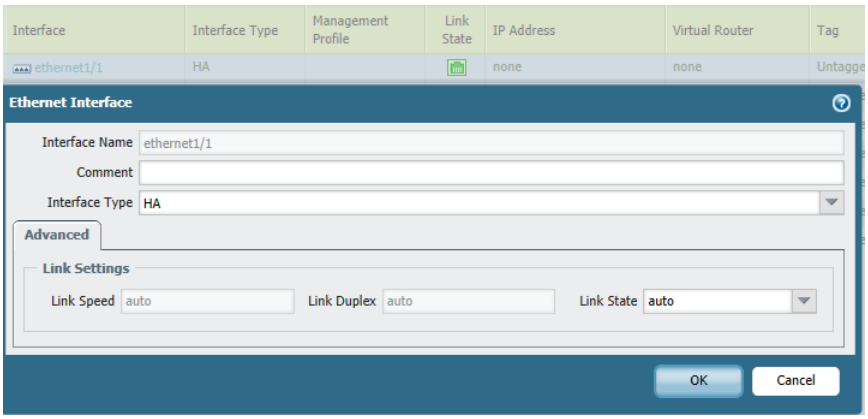
STEP 2 | 在 AWS 上启动 VM 系列防火墙。

STEP 3 | 启用 HA。

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置部分。
2. 选择 **Enable HA**（启用 **HA**）。

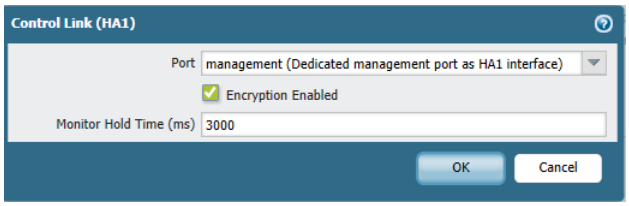
STEP 4 | 配置 ethernet 1/1 为 HA 接口。此接口必须被用于 HA2 通信。

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 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。

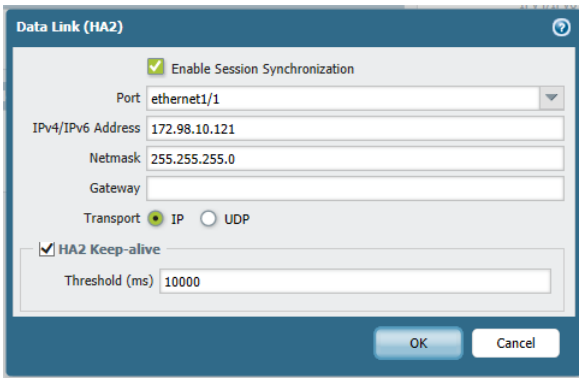


2. （可选）选择 **Encryption Enabled**（启用加密），以便保护对等设备之间的 HA 通信。如需启用加密，您必须从设备中导出 HA 密钥并将其导入对等设备。
   1. 选择 **Device**（设备）> **Certificate Management**（证书管理）> **Certificates**（证书）。
   2. 选择 **Export HA key**（导出 **HA** 密钥）。将高可用性密钥保存到对等设备可以访问的网络位置。
   3. 在对等设备上，导航到 **Device**（设备）> **Certificate Management**（证书管理）> **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。

STEP 6 | 将数据链接 (HA2) 设为使用 ethernet1/1。

© 2019 Palo Alto Networks, Inc.

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。

STEP 7 | 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 8 | （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**（监视故障持续时间）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 9 | 配置 HA 对等的 IP 地址。

© 2019 Palo Alto Networks, Inc.

1. 在 **Device**（设备）> **High Availability**（高可用性）> **General**（常规）中，编辑设置部分。
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）设为 1-63 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。

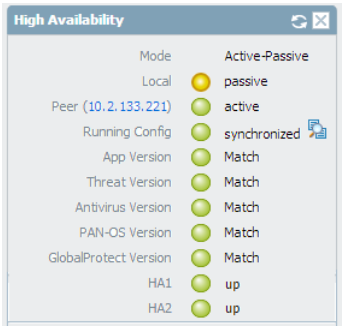
STEP 10 | 配置其他对等。

在 HA 对等上，重复执行步骤 3 至 9。

STEP 11 | 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）。



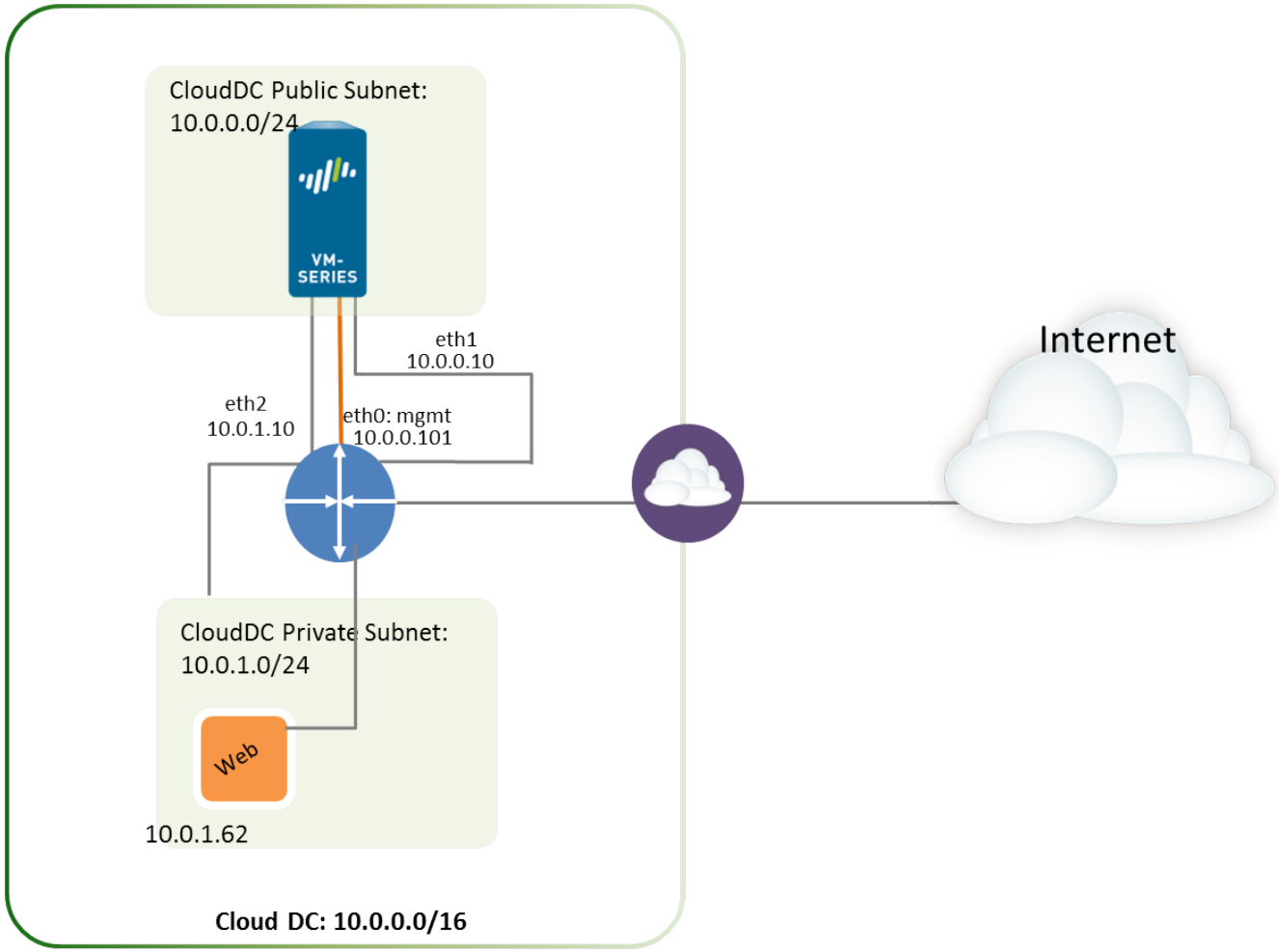
STEP 12 | 验证是否已正确发生故障转移。

1. 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）。
2. 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。

© 2019 Palo Alto Networks, Inc.

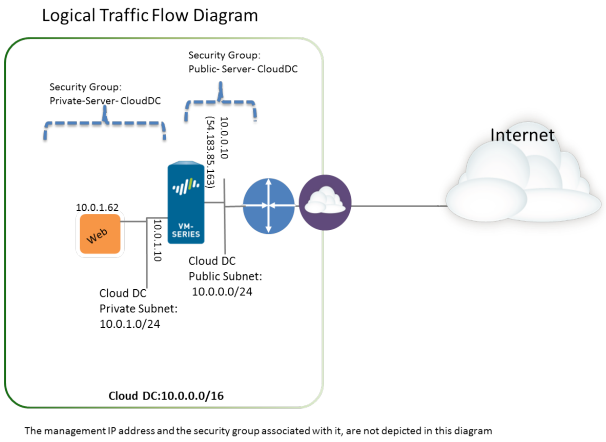
用例：保护 AWS 云中的 EC2 实例

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。

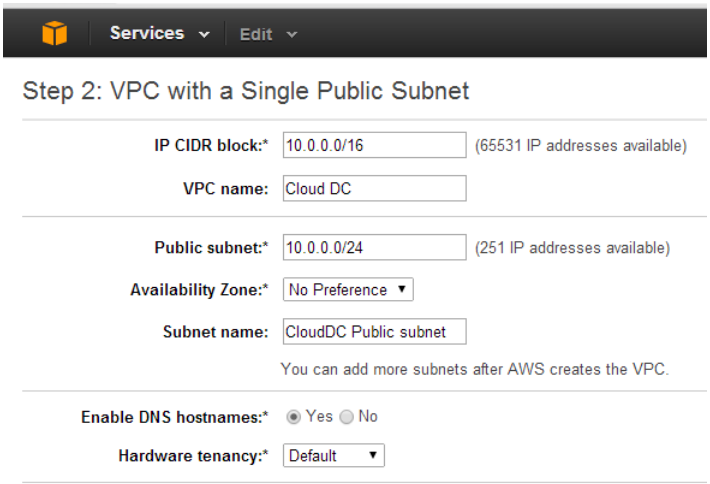
© 2019 Palo Alto Networks, Inc.



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。



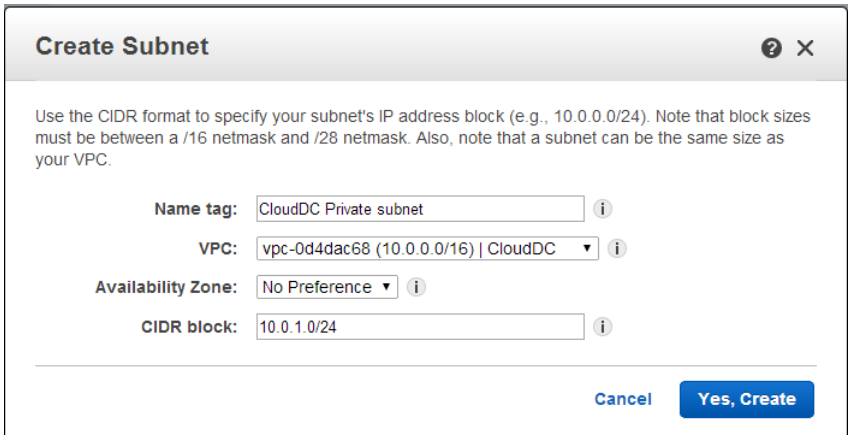
4. 单击 **Create VPC**（创建 VPC）。

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。

© 2019 Palo Alto Networks, Inc.

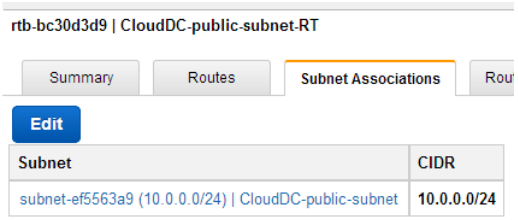


STEP 3 | 为每个子网创建新的路由表。

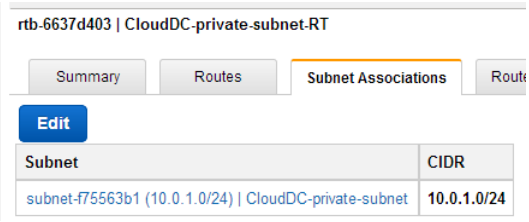
尽管已经在 *VPC* 中自动创建主路由表，但我们建议您创建新的路由表，而不是修改默认路由表。

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。



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：

© 2019 Palo Alto Networks, Inc.

- 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。

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），并单击**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：

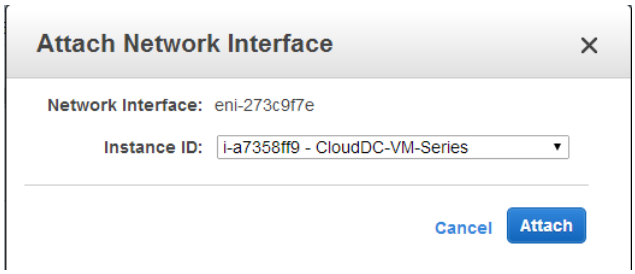
Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	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

© 2019 Palo Alto Networks, Inc.

- 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，并单击**Attach**（附加）。

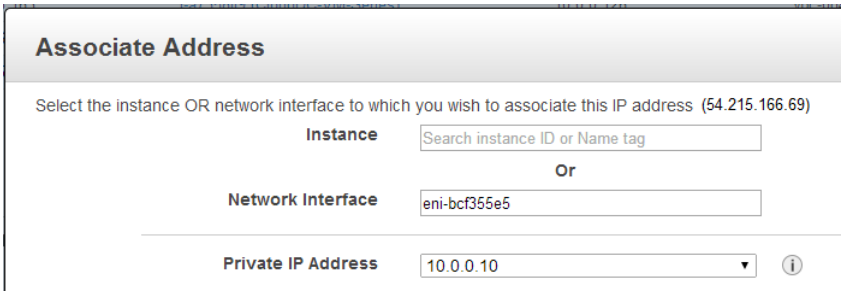


8. 选择 VM 系列防火墙的**Instance ID**（实例 ID），并单击**Attach**（附加）。
9. 要附加其他网络接口，请重复步骤 7 和 8。

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**），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-...

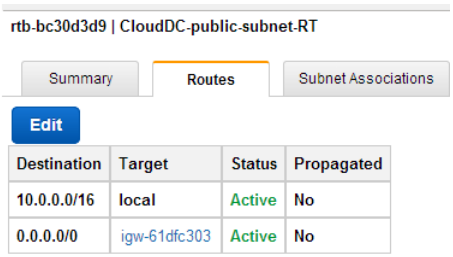
STEP 8 | 在附加到 VM 系列防火墙的每个网络接口上禁用源/目标检查。禁用此属性允许接口处理不是以其 IP 地址为目标的网络流量。

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。

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，0.0.0.0/0 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。

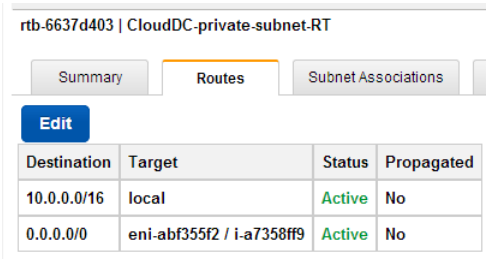
© 2019 Palo Alto Networks, Inc.



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。

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：

   ```
   configure
   set mgt-config users admin password
   commit
   ```
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。

© 2019 Palo Alto Networks, Inc.

请参阅激活许可证。

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“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

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

© 2019 Palo Alto Networks, Inc.

- 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“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）。

			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。

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）。

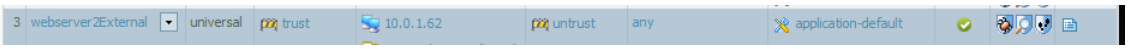
   在本示例中，我们拥有四个规则。第一个规则允许对于防火墙流量的管理访问，第二个规则允许 Web 服务器的入站流量，第三个规则允许对于 Web 服务器的 Internet 访问，第四个规则允许我们修改预定义的 intrazone-default 规则以记录拒绝的所有流量。
2. 创建规则以允许对于防火墙的管理访问。
   1. 单击 **Add**（添加），然后输入规则的 **Name**（名称）。确认 **Rule Type**（规则类型）为 universal。
   2. 在 **Source**（源）选项卡中，添加 untrust 作为 **Source Zone**（源区域）。
   3. 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“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	

© 2019 Palo Alto Networks, Inc.

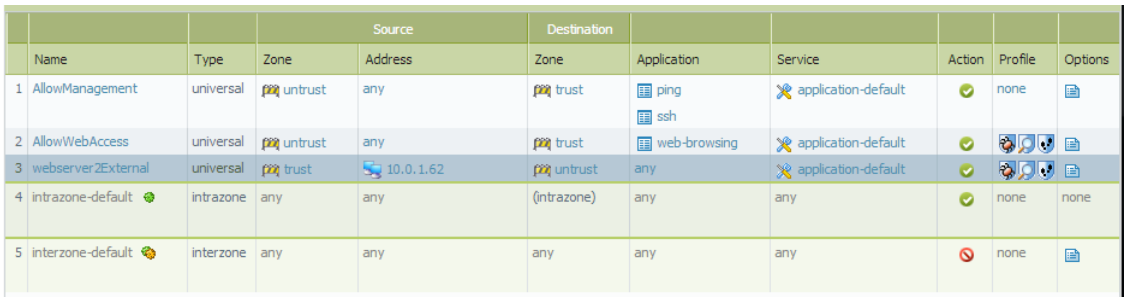
3. 创建规则以允许 Web 服务器的入站流量。
    1. 单击 **Add**（添加），并输入规则的 **Name**（名称），然后确认 **Rule Type**（规则类型）为 universal。
    2. 在 **Source**（源）选项卡中，添加 untrust 作为 **Source Zone**（源区域）。
    3. 在 **Destination**（目标）选项卡中，添加 trust 作为 **Destination Zone**（目标区域）。
    4. 在 **Applications**（应用程序）选项卡中，**Add**（添加）web-browsing。
    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“允许”。
    7. 在 **Actions**（操作）选项卡的“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）。

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。
    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“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“允许”。
    7. 在 **Actions**（操作）选项卡的“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。



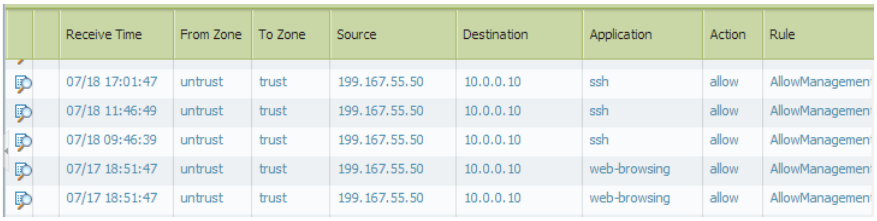
			Source		Destination					
	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
1	AllowManagement	universal	untrust	any	trust	ping ssh	application-default		none	
2	AllowWebAccess	universal	untrust	any	trust	web-browsing	application-default			
3	webserver2External	universal	trust	10.0.1.62	untrust	any	application-default			
4	intrazone-default	intrazone	any	any	(intrazone)	any	any		none	none
5	interzone-default	interzone	any	any	any	any	any		none	

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。

© 2019 Palo Alto Networks, Inc.

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！

© 2019 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。

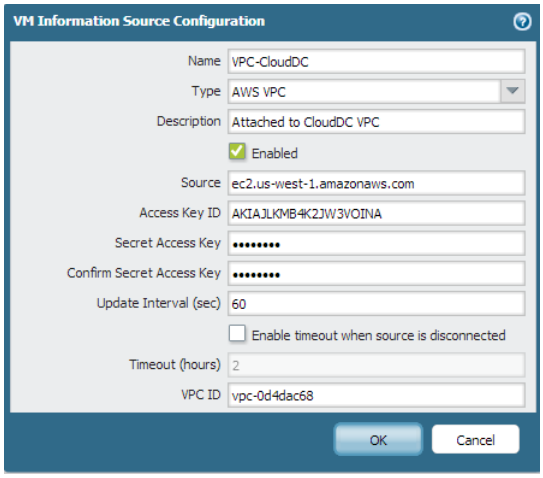
在本示例中，您可以使用防火墙上的 VM 信息源来监控 VPC，并在安全策略中使用动态地址组发现和保护 EC2 实例。启动 EC2 实例时，动态地址组将核对与为组成员所定义的条件相匹配的所有实例的 IP 地址，然后为组应用安全策略。在本示例中，安全策略允许 Internet 访问组的所有成员。

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。

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。语法为 **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**（秘密访问密钥）：输入密码并确认输入。
    5. （可选）将 **Update interval**（更新间隔）修改为 5-600 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。

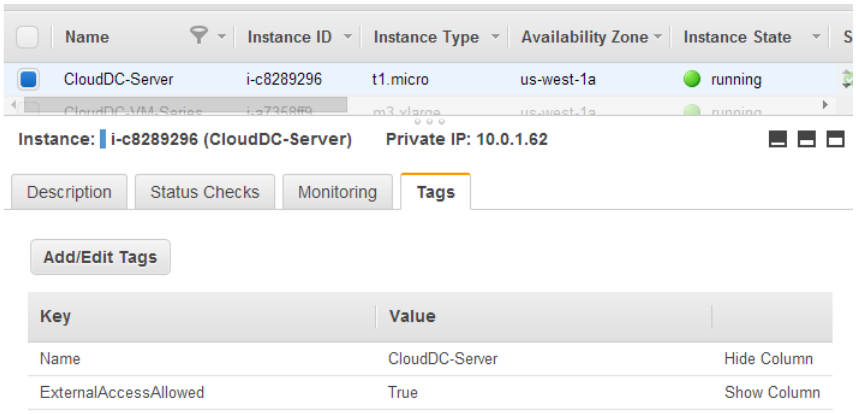
© 2019 Palo Alto Networks, Inc.

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。

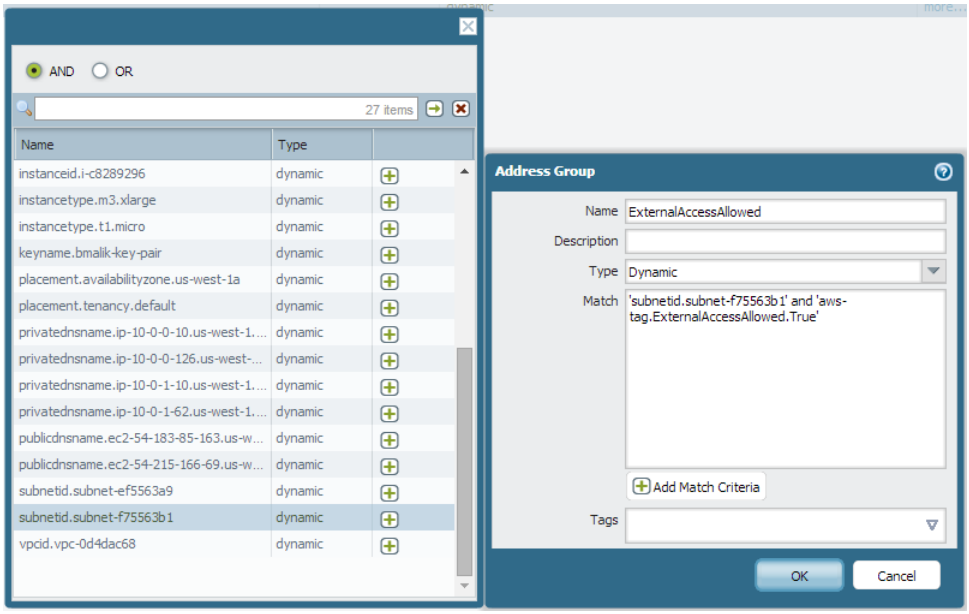
在本示例中，我们使用 EC2 仪表盘添加标记：



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）。

© 2019 Palo Alto Networks, Inc.

6. 单击 **Commit**（提交）。

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。

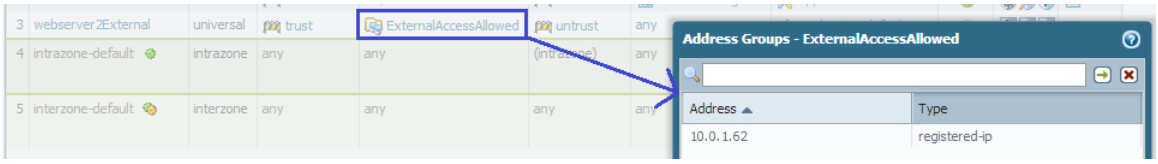
1. 选择 **Policies**（策略）> **Security**（安全）。
2. 单击 **Add**（添加），并输入规则的 **Name**（名称），然后确认 **Rule Type**（规则类型）为 universal。
3. 在 **Source**（源）选项卡中，添加 trust 作为 **Source Zone**（源区域）。
4. 在 **Source**（源）选项卡的“源地址”部分中，**Add**（添加）刚创建的 ExternalServerAccess 组。
5. 在 **Destination**（目标）选项卡中，添加 untrust 作为 **Destination 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“允许”。
8. 在 **Actions**（操作）选项卡的“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。



© 2019 Palo Alto Networks, Inc.

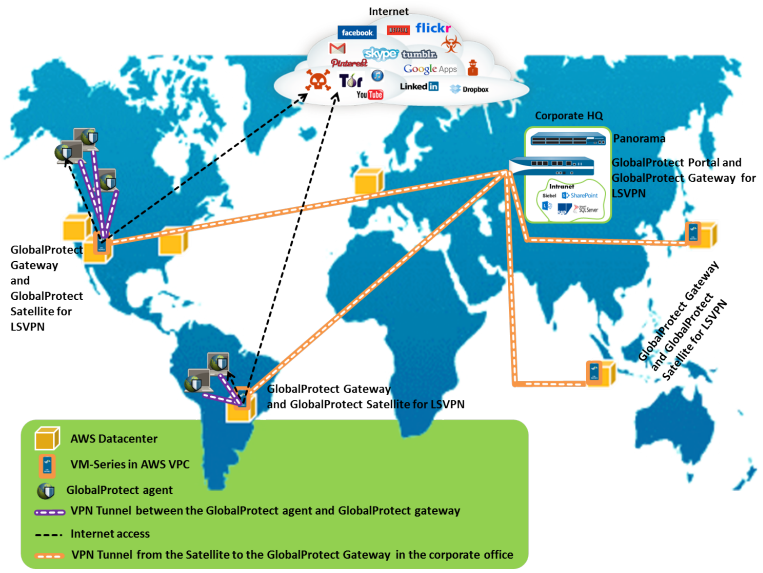
用例：VM 系列防火墙作为 AWS 上的 GlobalProtect 网关

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。

- 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。

© 2019 Palo Alto Networks, Inc.

- 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。

- 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。

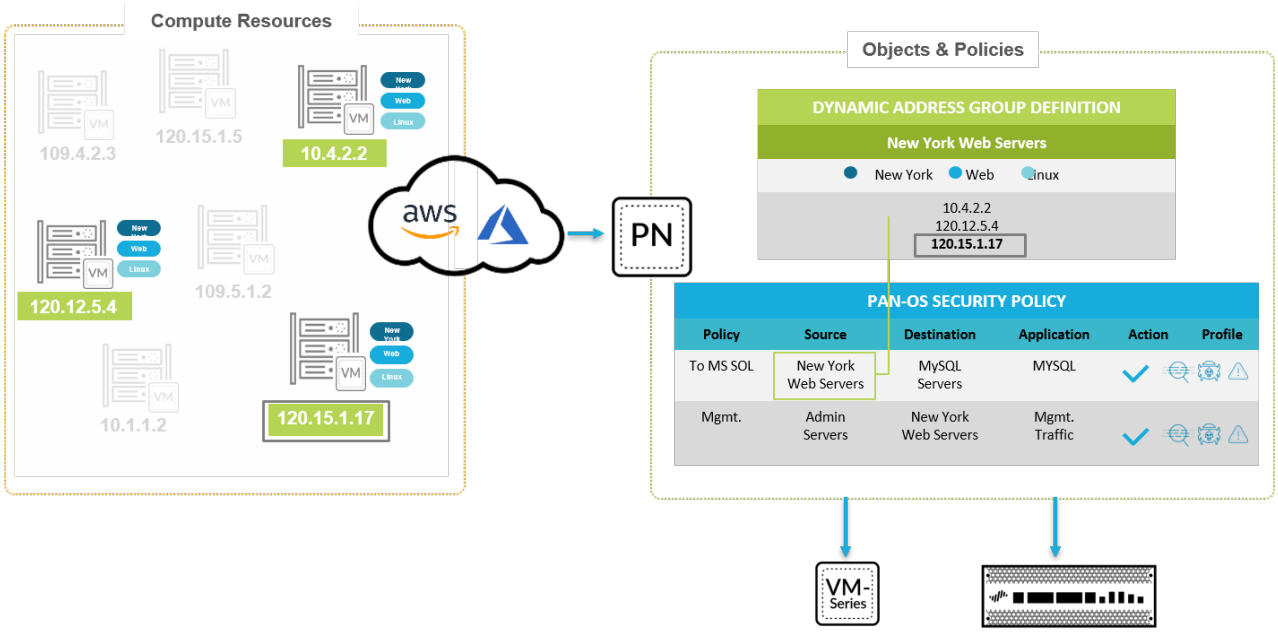
  请参阅部署 GlobalProtect 客户端软件。

© 2019 Palo Alto Networks, Inc.

AWS 上的 VM 监控

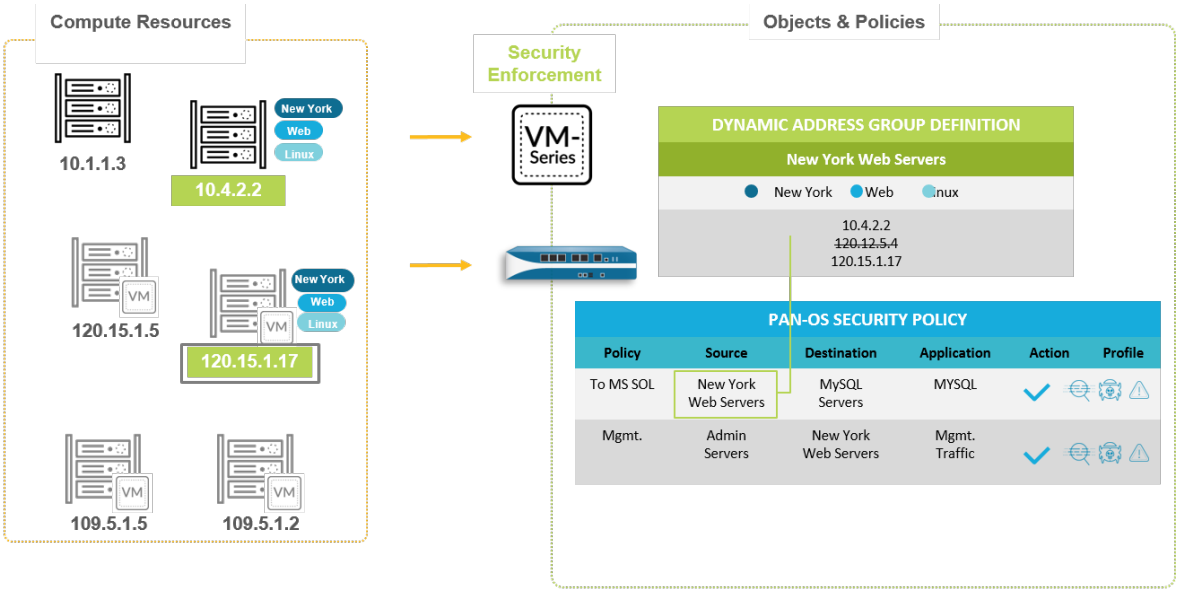
在 AWS 公共云中部署或终止虚拟机时，可以使用 AWS 的 Panorama 插件或使用防火墙上的 VM 信息源对这些工作负载统一执行安全策略。有关 Panorama 插件版本信息，请参阅兼容性矩阵。

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 VM 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。请参阅使用 Panorama 上的 AWS 插件进行 VM 监控。



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。

© 2019 Palo Alto Networks, Inc.



© 2019, Palo Alto Networks, Inc. All Rights Reserved.

使用 Panorama 上的 AWS 插件进行 VM 监控

在 AWS 公共云中部署或终止虚拟机时，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 EC2 实例标记的预定义属性集（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 VM 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 上的受管设备，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。

AWS 插件版本 2.0 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

© 2019 Palo Alto Networks, Inc.

- 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 和受管防火墙的要求：
  - 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 的 Panorama 9.1 或更高版本已经过测试，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	
Panorama 操作系统版本	9.1 或更高版本			
AWS 插件版本	2.0.0 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 上添加防火墙作为受管设备，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。

  确保作为在 Panorama 上未启用的设备组的一部分的防火墙可使用适用于 AWS 的 VM 信息源。启用 Panorama 插件以监控 AWS VPC 之前，您必须在这些防火墙上禁用适用于 AWS 的 VM 信息源，以避免与标记发生冲突并出现意外行为。

© 2019 Palo Alto Networks, Inc.

- 如果 Panorama 设备具有高可用性配置，则必须手动在两个 Panorama 对等设备上安装相同版本的 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* 主动对等设备上配置 *AWS* 插件。提交时，配置同步到 *Panorama* 被动对等设备。仅 *Panorama* 主动对等设备质询用于 *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 和秘密访问密钥），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 插件版本 2.0，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。
- 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**：**IAM** 角色与长期凭据	

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：
	<pre>{ "Path": "/", "UserName": "panorama_vm_programmatic",
	  "UserId": "AIDAIZXXXXCR5JPII4XYZ",
	  "Arn": "arn:aws:iam::412383210500:user/
	  panorama_vm_programmatic",
	  "CreateDate": "2018-07-06T19:14:31Z",
	  "GroupList": [],
	  "AttachedManagedPolicies":
	  [
	  { "PolicyName": "ReadOnlyAccess",
	  "PolicyArn": "arn:aws:iam::aws:policy/ReadOnlyAccess"
	  }
	  ]
	},</pre>

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**（秘密访问密钥）。
选项 **2**：**IAM** 角色与承担角色	

© 2019 Palo Alto Networks, Inc.

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 AmazonEC2ReadOnlyAccess。 • 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", "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**（秘密访问密钥）。 • 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	仅在将 Panorama 部署作为 AWS 上的 EC2 实例时 请注意，当使用 *AWS* 管理控制台创建 *IAM* 角色时，该控制台会自动创建名称与角色相同的实例配置文件。由于角色和实例配置文件具有相同的名称，因此当使用 *IAM* 角色启动浏览 *Panorama*（*EC2* 实例）时，具有相同名称的实例配置文件将会与其相关联。 当要监控的 Panorama 和资源都在一个 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**：实例配置文件与承担角色	
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：

© 2019 Palo Alto Networks, Inc.

	• 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。
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 版本 1.0.1 安装的 Panorama 插件升级到版本 2.0.x，您必须先升级到版本 2.0.x 所需的 Panorama 和 VM 系列插件版本，然后按照以下说明进行安装以执行升级。

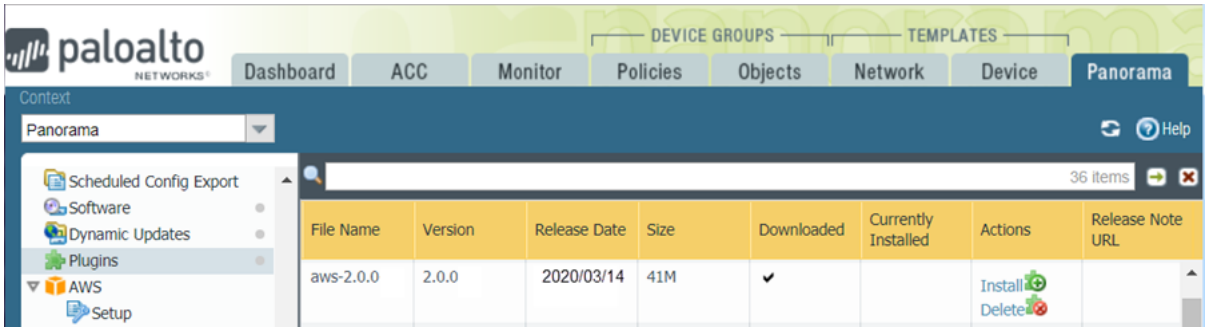
安装 *AWS* 插件 *v2.0* 后，您无法降级到 *v1.0*。

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。

如果您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。

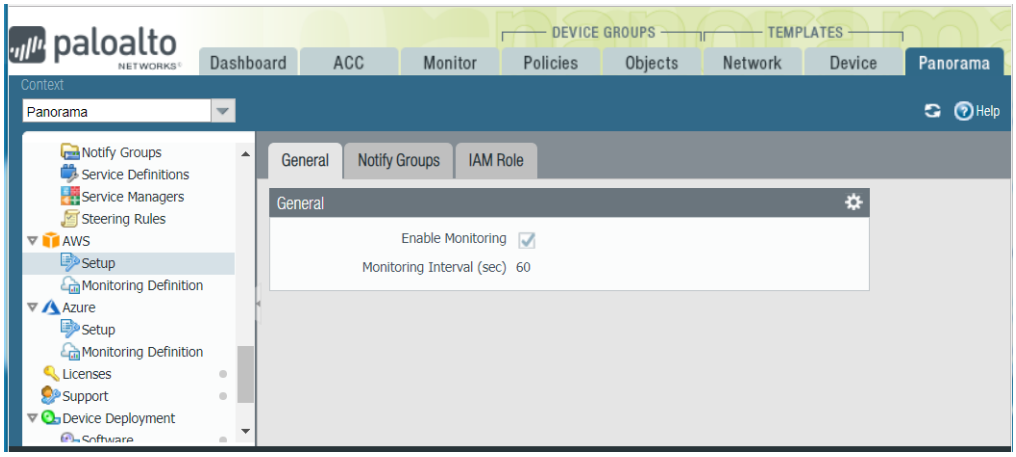
STEP 1 | 登录到 Panorama Web 界面，选择 **Panorama** > **Plugins**（插件），然后单击 **Check Now**（立即检查）以获取支持 VM 监控的 **AWS** 插件版本。



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。

© 2019 Palo Alto Networks, Inc.



在 *Panorama Dashboard*（仪表板）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。

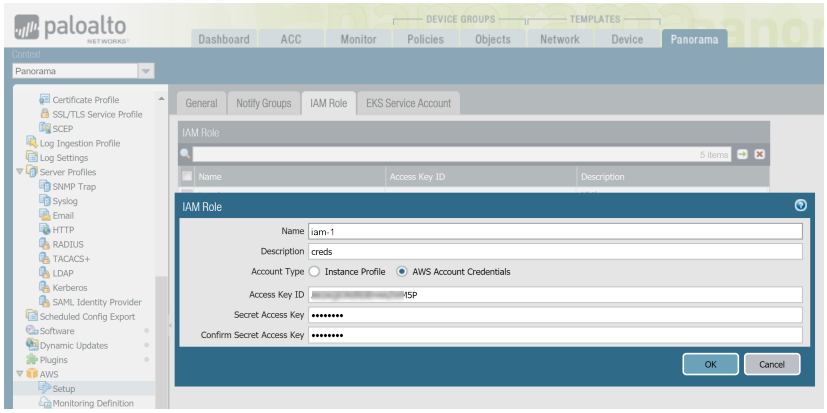
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 AWS 上设置以下对象，以启用 VM 监控。

- 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）。



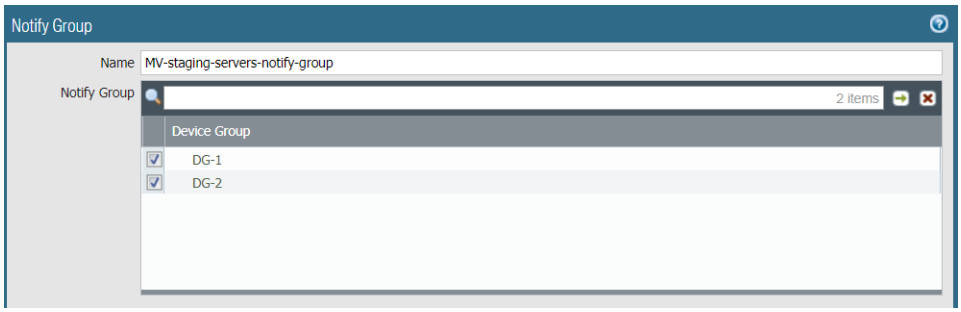
  2. 输入标识 IAM 角色的 **Name**（名称），也可选择输入 **Description**（说明）。

© 2019 Palo Alto Networks, Inc.

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**（秘密访问密钥），然后重新输入以确认，然后单击 **OK**（确定）。

- 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。

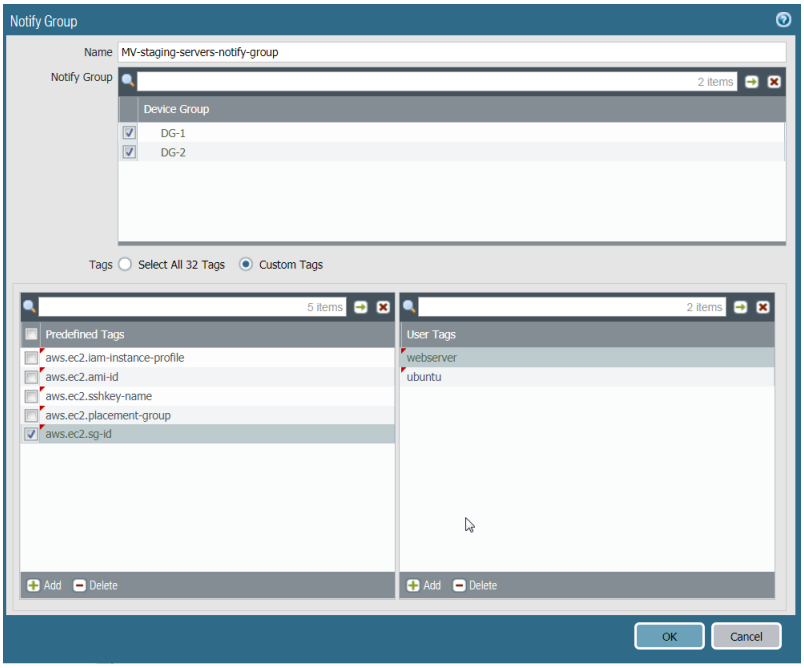
仔细考虑您的设备组。

- 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。

© 2019 Palo Alto Networks, Inc.



- 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。

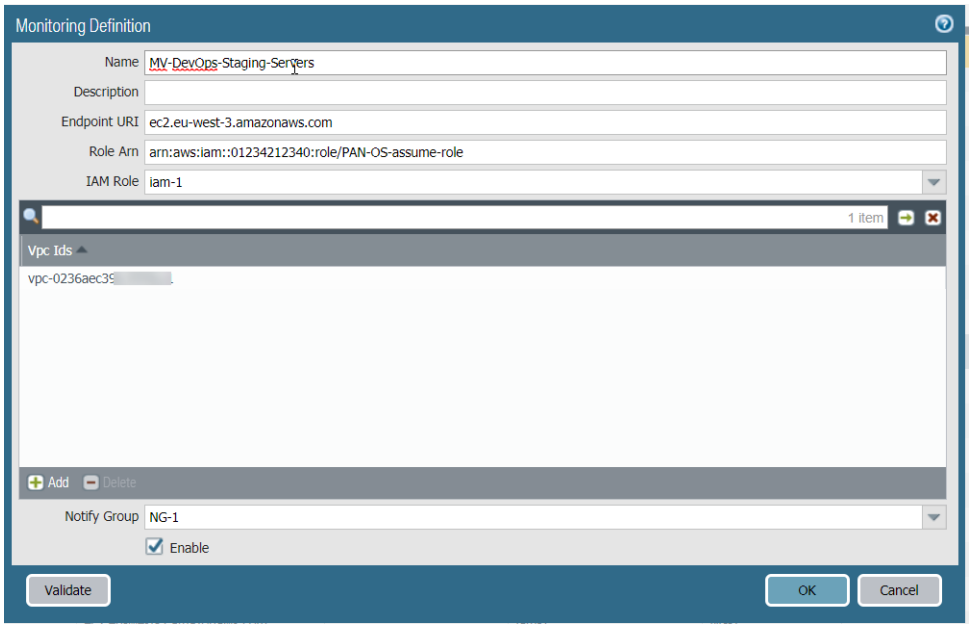
STEP 3 | 为要监控的每个 VPC 创建 **Monitoring Definition**（监控定义）。

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）以 **Add**（添加）新的定义。
- 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）。
- 输入 **Endpoint URI**（端点 **URI**）。语法为 ec2.<your_region>.amazonaws.com；

  对于 AWS China，语法为 ec2.<your region>.amazonaws.com.cn。
- （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。
- 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）。

© 2019 Palo Alto Networks, Inc.

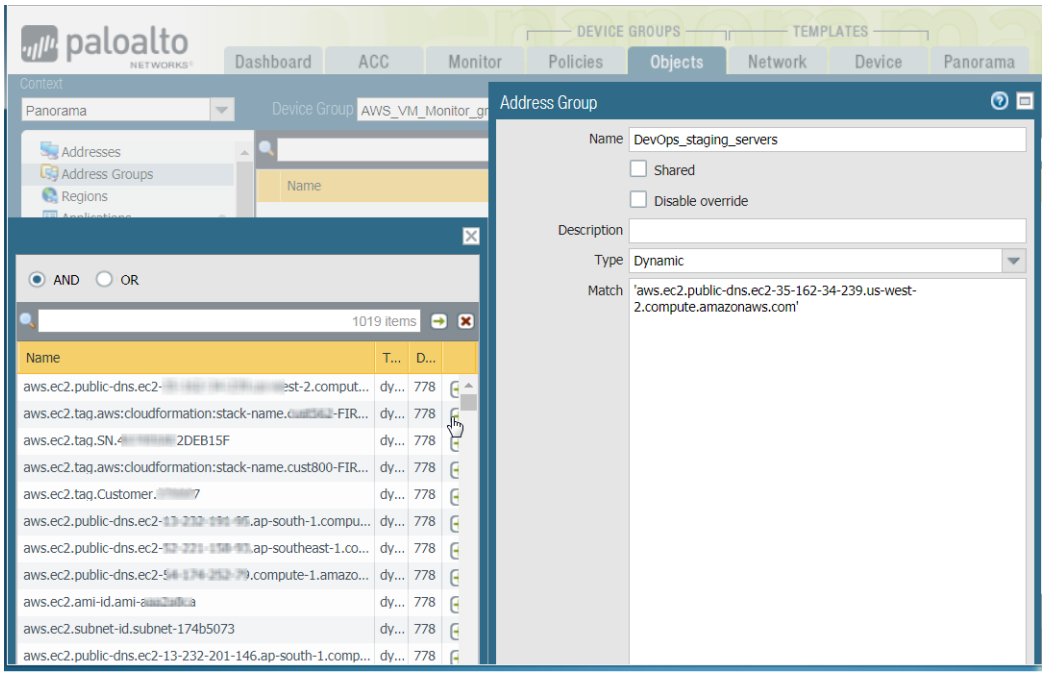


STEP 4 | 在 Panorama 上 **Commit**（提交）更改。

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。

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* 甚至无法重新连接至已配置和启用的其中一个监控定义，则 *Panorama* 生成系统日志消息

© 2019 Palo Alto Networks, Inc.

```
Unable to process accounts after HA switch-over; user-intervention
 required.
```

如果发生这种情况，则必须登录到 *Panorama*，并验证监控定义是否修复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。

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

  plugin_aws_ret.log 显示与 IP 地址和标记检索相关的日志。

  plugin_aws_proc.log 显示与处理注册 IP 地址和标记相关的日志。

  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
```


© 2019 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、面向互联网的防火墙、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。 在高可用性 *(HA)* 配置中，不支持 *Panorama*。	（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。 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。

© 2019 Palo Alto Networks, Inc.

功能/要求	版本 2.0	版本 2.1
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

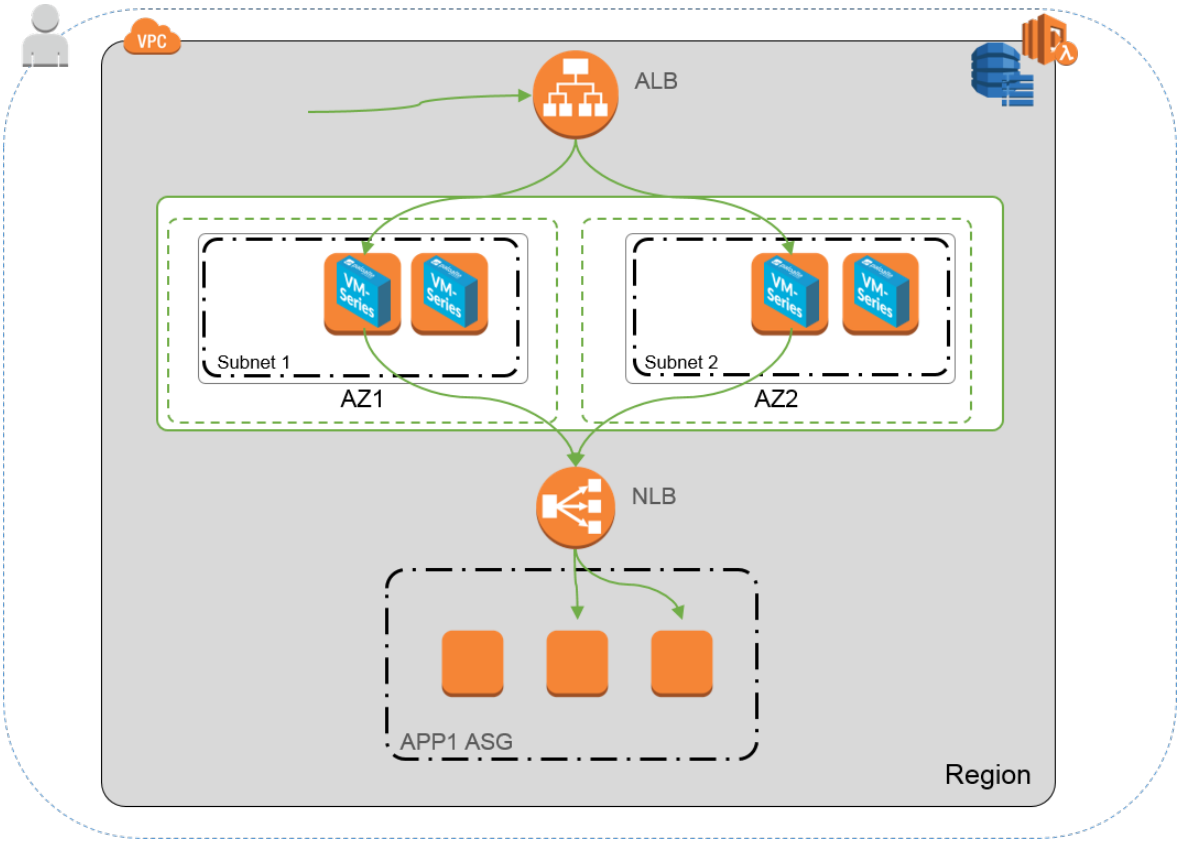
适用于 AWS 版本 2.0 的 VM 系列自动扩展模板

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区 (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。这种面向互联网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缩放的自定义 PAN-OS 指标。

  Palo Alto Networks 正式支持防火墙模板，并且拥有有效的支持权利，您可以请求 Palo Alto Networks 技术支持部门提供帮助。

© 2019 Palo Alto Networks, Inc.



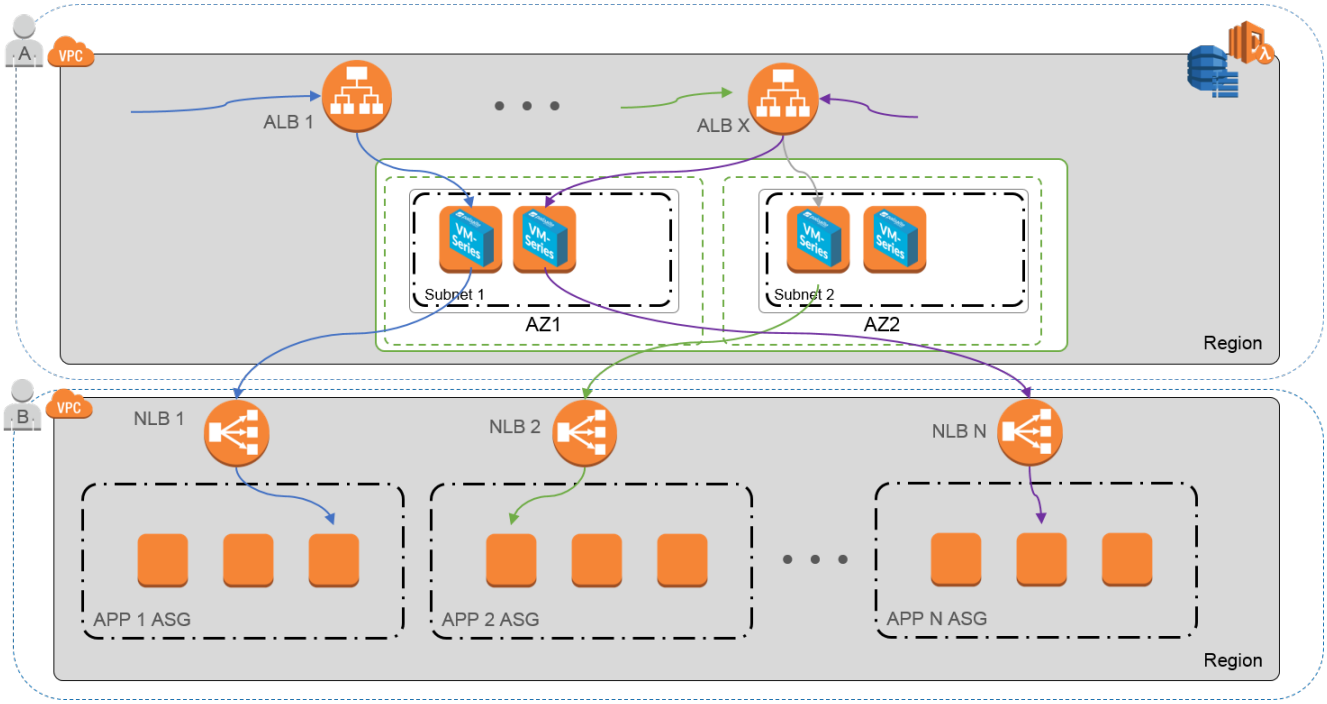
以下应用程序模板将部署上图中描述的网络负载均衡器。

- 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。

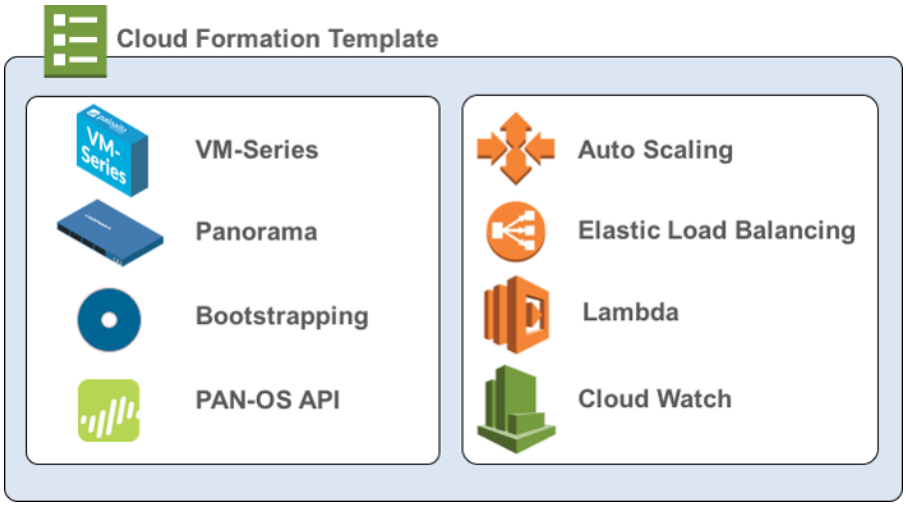
通过这些模板，您可以使用面向互联网的应用程序负载均稀器和内部网络负载均稀器部署负载均衡器三明治拓扑结构。面向互联网的 ELB 可通过互联网访问，并分发跨 VM 池系列防火墙进入 VPC 的流量。防火墙随后使用 NAT 策略将流量路由到内部网络负载均衡器，后者将流量分发到网络或应用程序服务器的自动扩展层。VM 系列防火墙能够将自定义 PAN-OS 指标发布到 AWS CloudWatch，您可以监控 VM 系列防火墙上的运行状况和资源负载，然后使用该信息在防火墙上的适当 ASG 上触发自动扩展事件。

© 2019 Palo Alto Networks, Inc.



- 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模块：

© 2019 Palo Alto Networks, Inc.

构建模块	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、两个可用区 (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、可用区、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。 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	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

© 2019 Palo Alto Networks, Inc.

构建模块	说明
部署，您必须在启动之前修改 bootstrap.xml 中的示例凭证。	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缩放？

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。

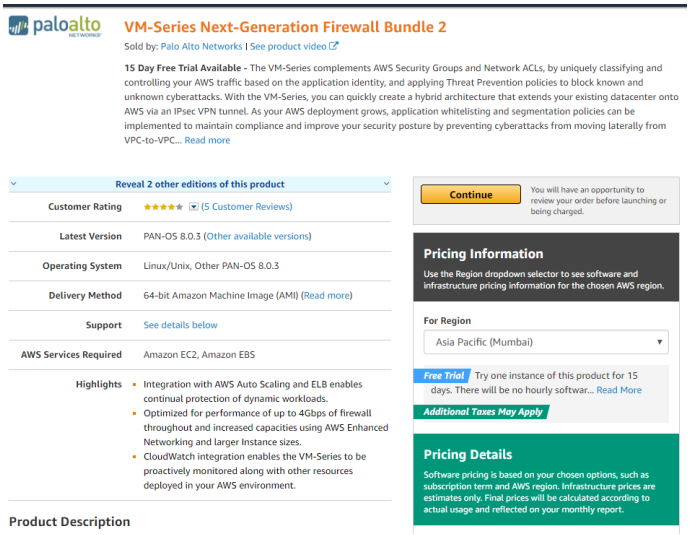
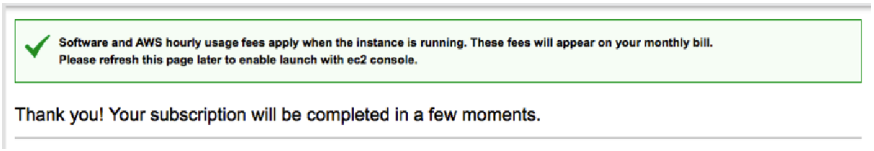
当自动扩展事件触发新防火墙的部署时，新实例在启动时引导并且 AWS Lambda 功能使用 NAT 策略规则配置防火墙。为每个应用程序创建 NAT 策略规则，并且该规则引用部署中每个网络负载均衡器的 IP 地址。当应用程序负载均衡器收到请求时，它会将请求转发到指定 TCP 端口上的防火墙。随后，防火墙检查流量并将其转发到相应的网络负载均衡器，然后将该请求转发到其目标组中的 Web 服务器。

规划 AWS 的 VM 系列自动缩放模板（v2.0 和 v2.1）

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。

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。	自动缩放模板需要 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。您需要查看清单 支持的区域和AMI ID，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	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

© 2019 Palo Alto Networks, Inc.

帐户（如果您还没有）。	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。
❑ （仅限 PAYG）审核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，那么这是必需的。	在 AWS Marketplace 中，搜索 Palo Alto Networks，然后选择您打算使用的套餐。如果您尚未接受计划使用的套餐的EULA，则 VM 系列防火墙将无法部署。 • 搜索 例如， **VM** 系列下一代防火墙套装**2**。  • 单击 **Continue**（继续），然后选择 **Manual Launch**（手动启动）。查看协议并单击 **Accept Software Terms**（接受软件条款）以接受 EULA。  您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 存储区的命名约定是 `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。
❑ 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。

© 2019 Palo Alto Networks, Inc.

模板 v2.0 和 v2.1 的规划清单	

	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。
❑ 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。

© 2019 Palo Alto Networks, Inc.

模板 v2.0 和 v2.1 的规划清单	
	• 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验证密钥 — 允许Panorama验证防火墙，以便它可以将每个防火墙添加为受管设备。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)。

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

© 2019 Palo Alto Networks, Inc.

参数	说明	默认值
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 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。	该模板将所有以下指标发布到 AWS CloudWatch： • CPU—数据面板 CPU 利用率 • AS—活动会话 • SU—会话利用率 • SSPU—SSL 代理利用率 • GPU—GlobalProtect 网关利用率 • GPAT—GlobalProtect 网关利用率活动隧道 • DPB—数据面板数据包缓冲区利用率	数据面板 CPU 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	自动缩放组中的 VM 系列防火墙的最大数量。	3
最小 VM 系列实例	自动缩放组中最小数量的 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）。

- 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）

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

© 2019 Palo Alto Networks, Inc.

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 文件夹中输入此身份验证代码。
- 下载启动 VM 系列自动扩展模板所需的文件 GitHub 存储库。

STEP 2 | （可选）修改 init-cfg.txt 文件。

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

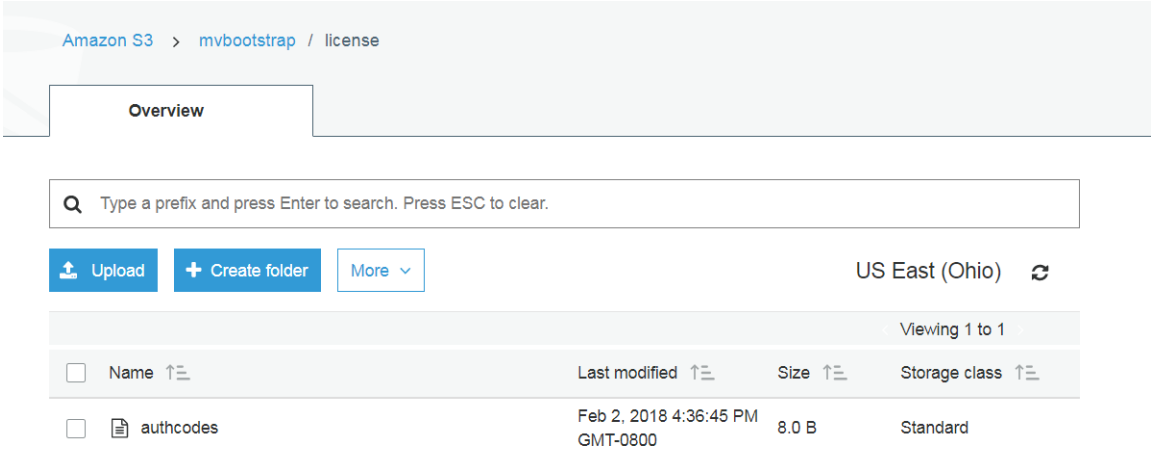
   tplname=FINANCE_TG4

   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。身份验证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。

© 2019 Palo Alto Networks, Inc.



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。

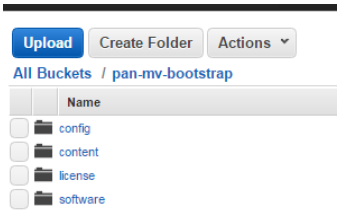
在生产环境中使用 VM 系列自动扩展模板时需要。

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)。

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。

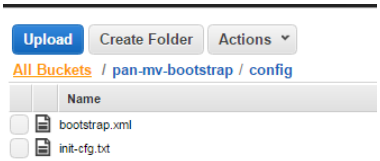
确保在计划部署模板的相同区域中创建 *S3* 存储桶；仅提供公用 *S3* 存储桶中托管的引导文件，以便您更轻松地评估模板。

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**（区域），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。

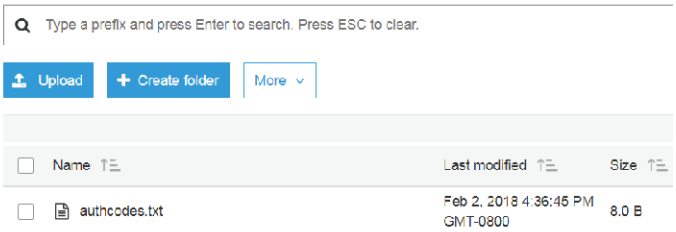


    3. 单击链接打开 **config** 文件夹。
    4. 选择 **Actions**（操作）> **Upload**（上传）和**Add Files**（添加文件），浏览以选择 init-cfg.txt 文件和 bootstrap.xml 文件，然后单击 **Open**（打开）。
    5. 单击 **Start Upload**（开始上传）将文件添加到配置文件夹。该文件夹只能包含两个文件：init-cfg.txt 和 bootstrap.xml。

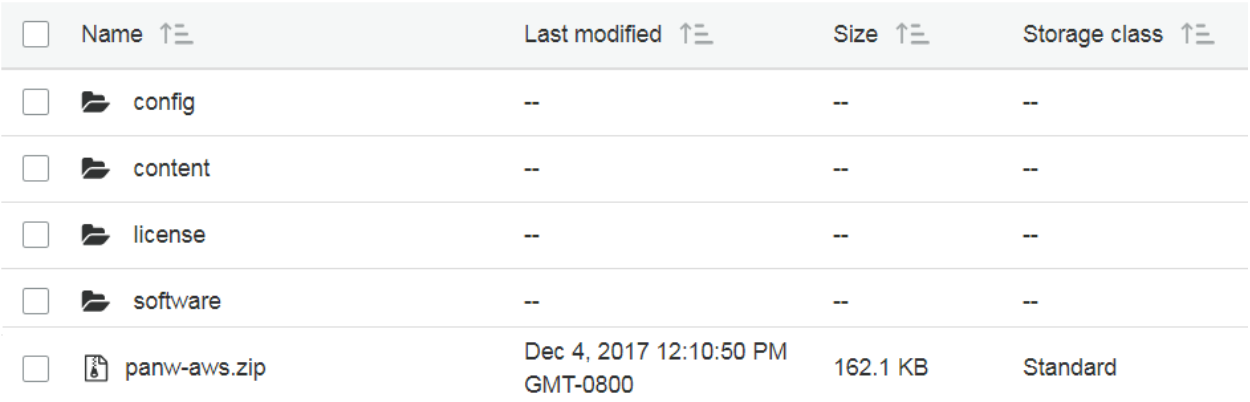
© 2019 Palo Alto Networks, Inc.



6. （仅限 BYOL）单击链接打开 **license** 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。

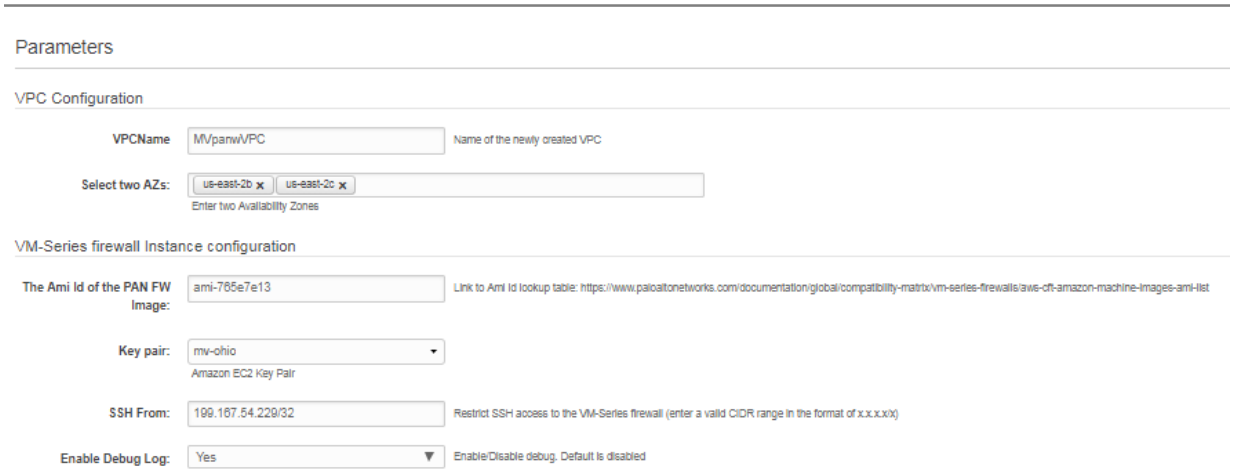
1. 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。
2. 选择 **Upload a template to Amazon S3**（将模板上传到 **Amazon S3**），选择 firewall-v2.0.template 并单击 **Open**（打开）和 **Next**（下一个）。
3. 指定 **Stack name**（堆栈名称）。堆栈名称允许您唯一标识此模板部署的所有资源。

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区域 **Select two AZs**（选择两个 **AZ**）。

STEP 8 | 选择 VM 系列防火墙的首选项。

© 2019 Palo Alto Networks, Inc.

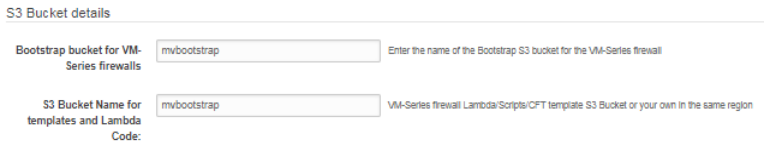


1. 为 VM 系列防火墙查找 AMI ID 并输入它。确保 AMI ID 与您选择使用的 AWS 区域、PAN-OS 版本和 BYOL 或 PAYG 许可选项相匹配。
2. 选择 EC2 **Key pair**（密钥对）（从下拉菜单中）启动防火墙。要登录防火墙，您必须提供此密钥对的名称以及与其关联的私钥。
3. 限制 SSH 访问防火墙的管理界面。确保提供与专用管理IP地址或网络相对应的 CIDR 块。不要将允许的源网络范围设置得比所需的大，并且不要将允许的源配置为 0.0.0.0/0。在将模板配置到模板上之前验证您的 IP 地址，以确保您不会锁定自己。
4. 如果您要 **Enable Debug 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 系列防火墙的缩放参数。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。

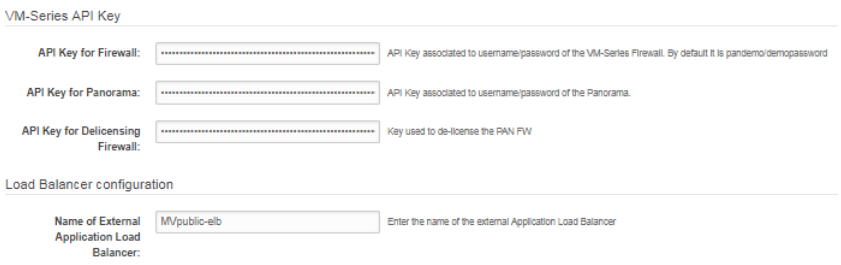
您可以使用一个 *S3* 存储桶作为引导程序包和 *zip* 文件。



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。

STEP 10 | 指定启用 API 访问防火墙和 Panorama 的密钥。



© 2019 Palo Alto Networks, Inc.

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. 从 **Go To**（转到）下拉列表中选择 **License API**（许可证 **API**）。
    3. 复制 API 密钥。

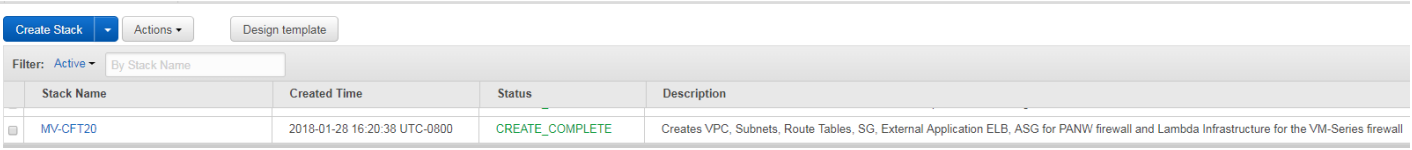
STEP 11 | 输入应用程序负载均衡器的名称。

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。

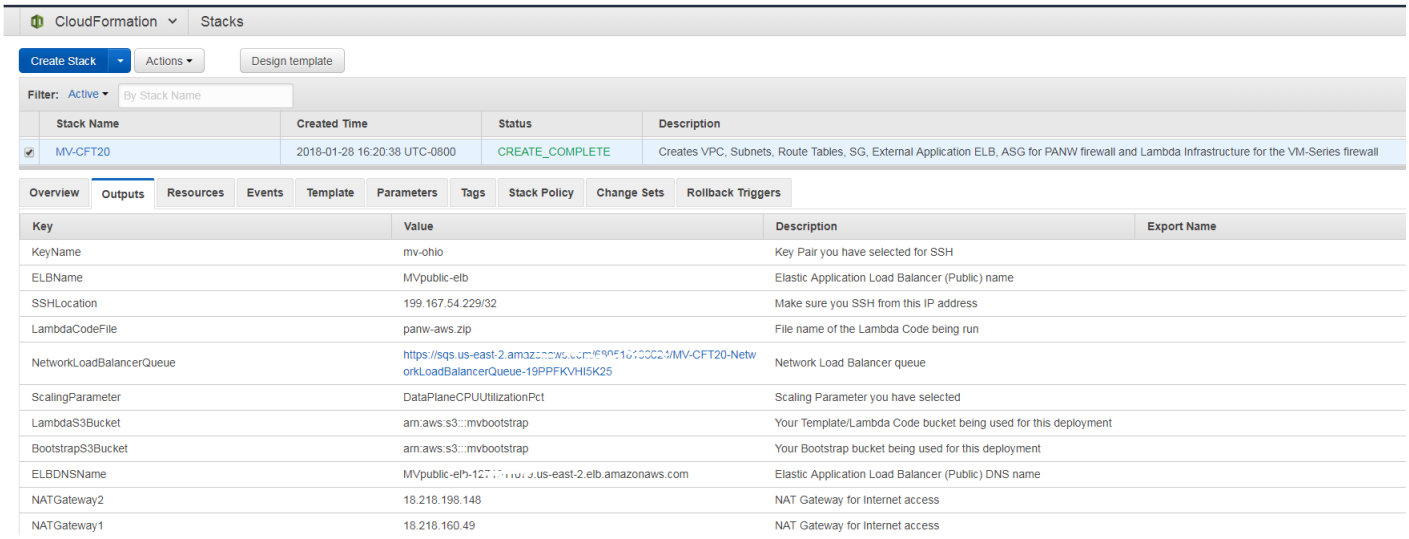
1. 选择 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我承认此模板可能会导致 **AWS CloudFormation** 创建 **IAM** 资源）。
2. 单击 **Create**（创建）以启动模板。显示 CREATE_IN_PROGRESS 事件。
3. 成功部署时，状态会更新到 CREATE_COMPLETE。



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。

© 2019 Palo Alto Networks, Inc.

- 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 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

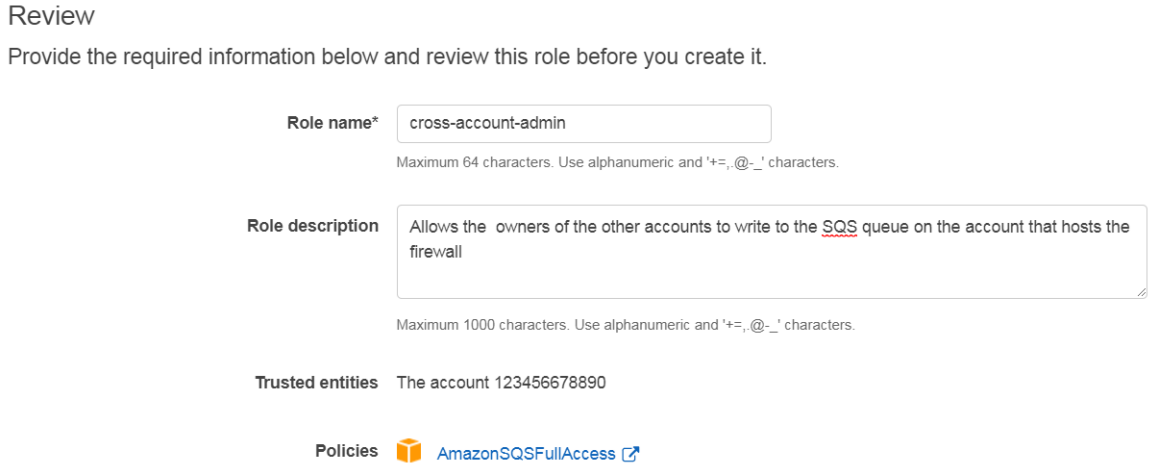
应用程序模板允许您完成三明治拓扑结构，并提供应用程序目标以便您可以评估自动扩展解决方案。此应用程序模板在使用防火墙模板部署的 VM 系列防火墙自动扩展组后面部署网络负载均衡器和一对 Web 服务器。此模板中的 Web 服务器具有公共 IP 地址，可直接出站访问以检索软件更新。使用此模板评估解决方案，但构建自己的模板以部署到生产中。对于自定义模板，请确保启用应用程序模板和防火墙模板之间的 SQS 消息传递。

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。

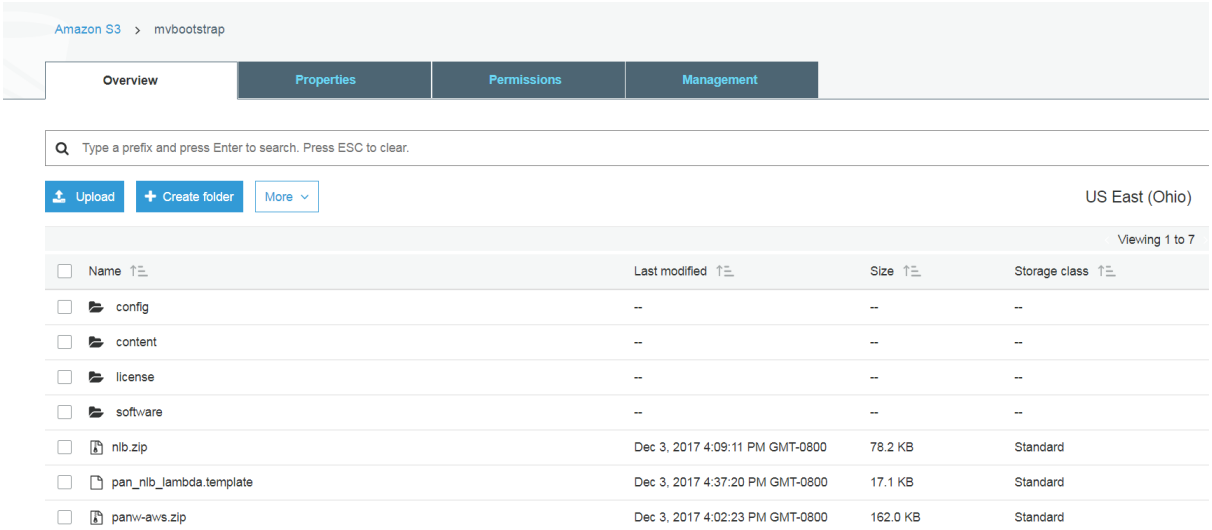
- 对于 **Account ID**（帐户**ID**），键入要部署应用程序模板的帐户的 AWS 帐户 ID。通过指定该帐户 ID，您可以授予访问您帐户中承载防火墙模板资源的资源的权限。
- 选择 **Require external ID**（需要外部 **ID**），并输入一个共享密钥的值。指定外部 ID 允许用户只有在请求包含正确的值时才承担角色。
- 选择 **PERMISSONS**（权限）以允许 **Amazon SQS Full Access**（**Amazon SQS** 完全访问）。



© 2019 Palo Alto Networks, Inc.

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。



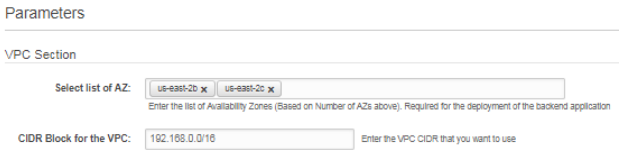
3. 将 pan_nlb_lambda 模板复制到您将 nlb.zip 文件复制到的同一个存储桶中。

STEP 3 | 选择要启动的应用程序模板。

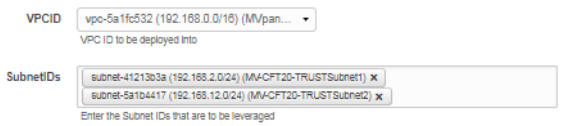
1. 在 AWS 管理控制台中，选择 **CloudFormation** > **Create Stack**（创建堆栈）。
2. 选择 **Upload a template to Amazon S3**（将模板上传到 **Amazon S3**），选择 panw_aws_nlb-2.0.template 来部署模板在与防火墙相同的 VPC 内启动的资源，或选择 panw_aws_nlb_vpc-2.0.template 来将资源部署到不同的 VPC。单击 **Open**（打开）和 **Next**（下一步）。
3. 指定 **Stack name**（堆栈名称）。堆栈名称允许您唯一标识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。

© 2019 Palo Alto Networks, Inc.

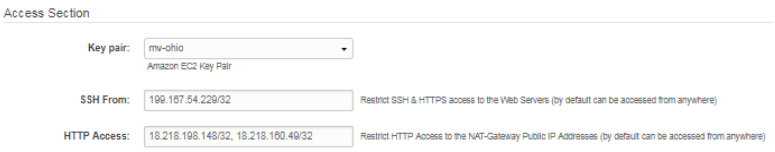
1. 输入存储 nlb.zip 和 pan_nlb_lambda.template 的 S3 存储桶名称。
2. 输入 pan_nlb_lambda.template 的名称和 zip 文件名称。
3. 粘贴您之前复制的 SQS URL。
4. 输入一个唯一的 **TableName**（表名）。此表存储部署中与网络负载均衡器关联的应用程序的端口和 IP 地址的映射。

   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。

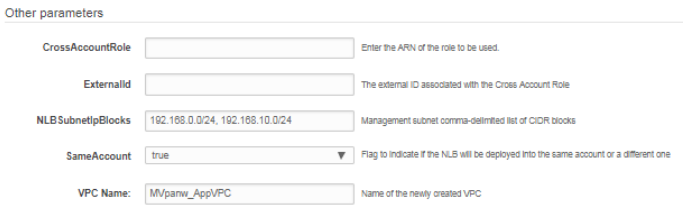
STEP 7 | 选择启动 Web 服务器的 EC2 **Key pair**（密钥对）（从下拉菜单中）。要登录到 Web 服务器，您必须提供密钥对名称和与其关联的私钥。

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。



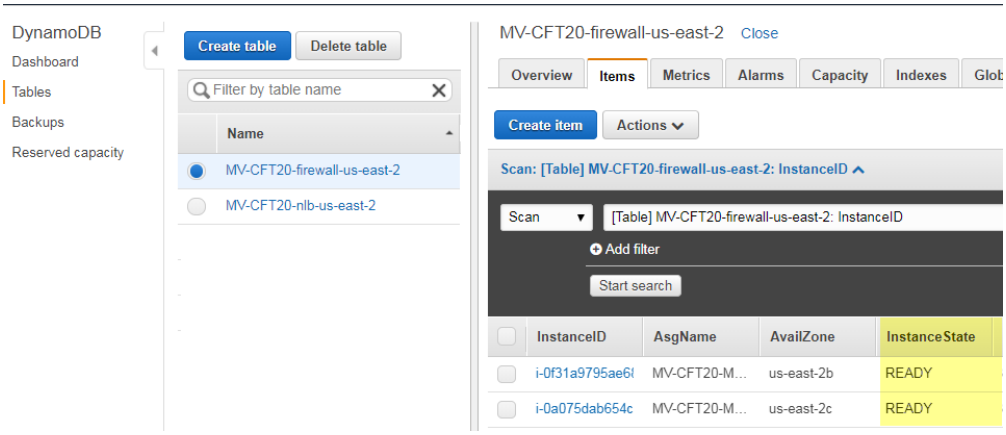
1. 如果您在与防火墙模板相同的 AWS 帐户中部署此应用程序模板，选择 SameAccount **true**，并将交叉帐户角色和外部 ID 留空；对于跨帐户部署，选择 **false**。

   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**。

© 2019 Palo Alto Networks, Inc.

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。

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。

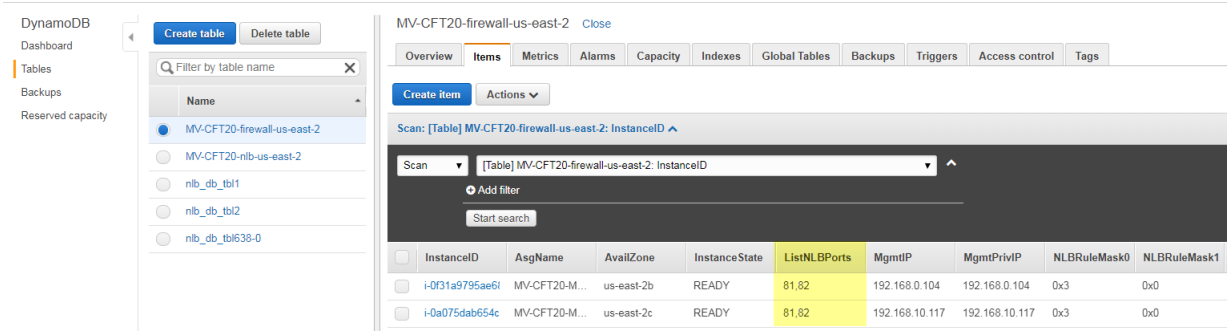
STEP 1 | 在 AWS 管理控制台上，验证 DynamoDB 表上为每个网络均衡器分配的端口。

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。

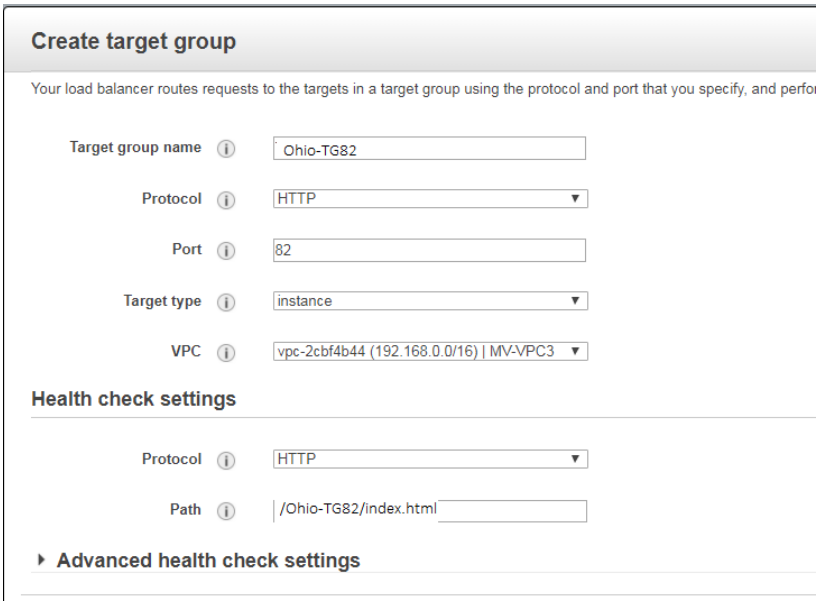
© 2019 Palo Alto Networks, Inc.

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。

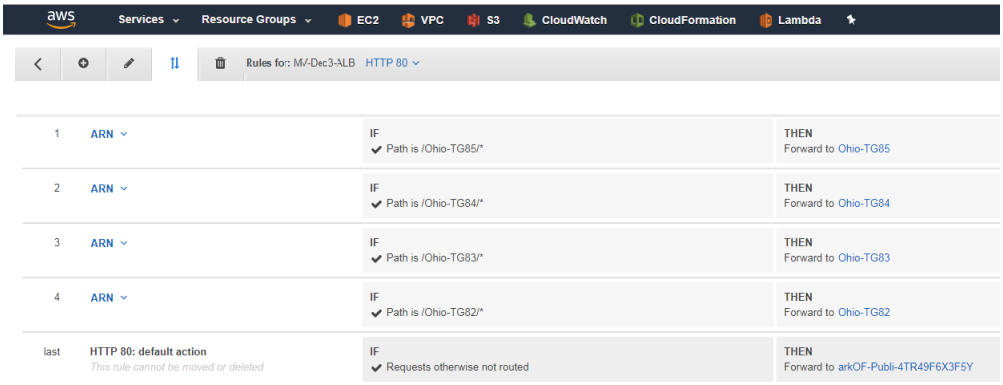
添加新目标组时，请使用您在 DynamoDB 表上验证的端口信息。



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“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：

© 2019 Palo Alto Networks, Inc.



STEP 4 | 将目标组连接到 VM 系列防火墙自动扩展组。

1. 在“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缩放组。
2. 选择 **Details**（细节）> **Edit**（编辑），并从 **Target Groups**（目标群体）下拉列表中选择新的目标组。

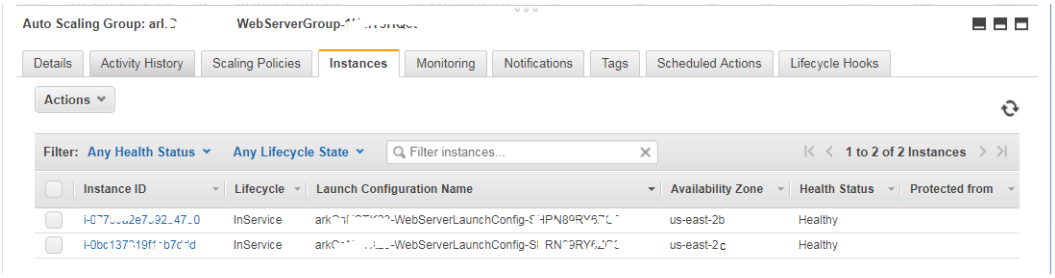
STEP 5 | 登录到应用程序模板部署的每个 Web 服务器，使用目标组名称创建一个新目录，并将 index.html 文件复制到目录中。在设置 index.html 文件的路径之前，此 Web 服务器的运行状况检查报告为不健康。

```
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，以验证 Web 服务器是否报告健康。

© 2019 Palo Alto Networks, Inc.



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。

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>` 之后粘贴行 353 至 356 `</management>`。

© 2019 Palo Alto Networks, Inc.

```
352            </management>
353            <aws-cloudwatch>
354              <enabled>yes</enabled>
355              <name>autoscale-default-panw-asg-name</name>
356            </aws-cloudwatch>
357          </setting>
```

STEP 8 | 删除管理接口配置。

1. 搜索 `</service>` 并删除后面的 ip-address、netmask 和默认网关。
2. 搜索 `</type>` 并删除后面的 ip-address、netmask、默认网关和公钥。

```
326          </service>
327          <ip-address>192.168.10.16</ip-address>
328          <netmask>255.255.255.0</netmask>
329          <default-gateway>192.168.10.1</default-gateway>
330          <hostname>PA-VM</hostname>
331        </system>
332        <setting>
333          <config>
334            <rematch>yes</rematch>
335          </config>
336          <management>
337            <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
338            <initcfg>
339              <type>
340                <dhcp-client>
341                  <send-hostname>yes</send-hostname>
342                  <send-client-id>no</send-client-id>
343                  <accept-dhcp-hostname>no</accept-dhcp-hostname>
344                  <accept-dhcp-domain>no</accept-dhcp-domain>
345                </dhcp-client>
346              </type>
347              <ip-address>192.168.10.16</ip-address>
348              <netmask>255.255.255.0</netmask>
349              <default-gateway>192.168.10.1</default-gateway>
350              <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJVeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXlLczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTR</public-key>
351            </initcfg>
352          </management>
```

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缩放的指标。

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。

© 2019 Palo Alto Networks, Inc.

```
        </service>
        <ip-address>192.168.10.16</ip-address>
        <netmask>255.255.255.0</netmask>
        <default-gateway>192.168.10.1</default-gateway>
        <hostname>PA-VM</hostname>
      </system>
      <setting>
        <config>
          <rematch>yes</rematch>
        </config>
        <management>
          <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
          <initcfg>
            <type>
              <dhcp-client>
                <send-hostname>yes</send-hostname>
                <send-client-id>no</send-client-id>
                <accept-dhcp-hostname>no</accept-dhcp-hostname>
                <accept-dhcp-domain>no</accept-dhcp-domain>
              </dhcp-client>
            </type>
            <ip-address>192.168.10.16</ip-address>
            <netmask>255.255.255.0</netmask>
            <default-gateway>192.168.10.1</default-gateway>
            <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJ4dldEaHFHWQ3'
            VEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXllczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTRnhZdDdXUlFY
          </initcfg>
        </management>
```

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。

© 2019 Palo Alto Networks, Inc.

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。
- 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。

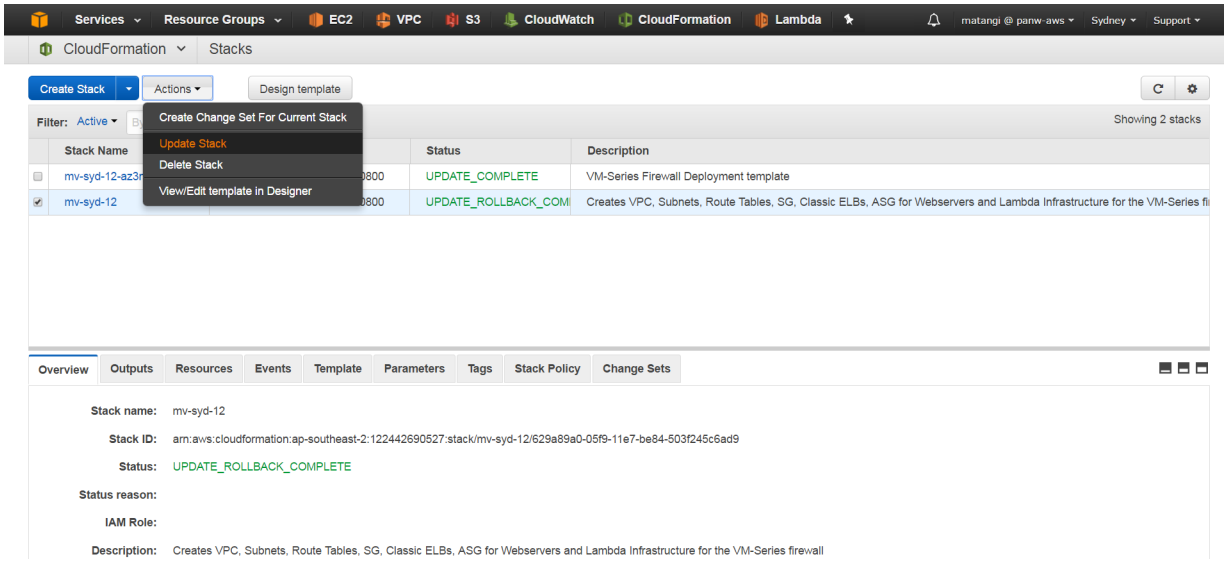
通过更改 *AMI-ID*，您可以使用不同的 *PAN-OS* 版本部署 *VM* 系列防火墙的新实例。

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 中现有的自动缩放组。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）。

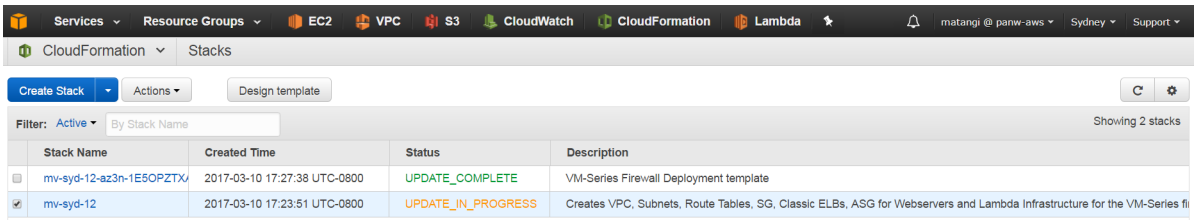
如果您在 PAYG 套餐版本 1 和 2 之间切换，查找 AMI ID 用于 VM 系列防火墙。

- 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。

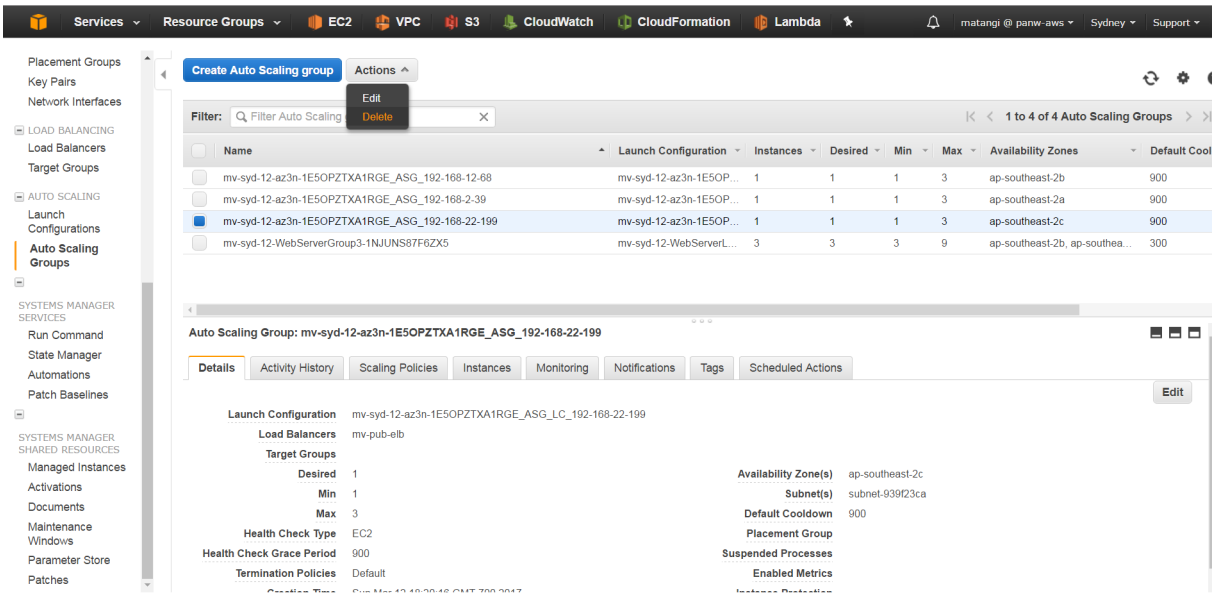
© 2019 Palo Alto Networks, Inc.

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。

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)。

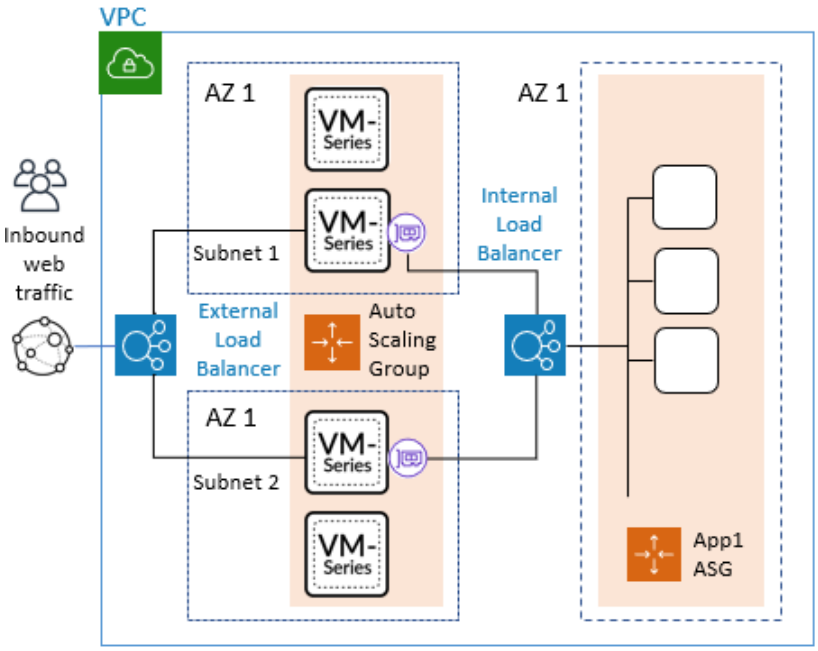
© 2019 Palo Alto Networks, Inc.

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。

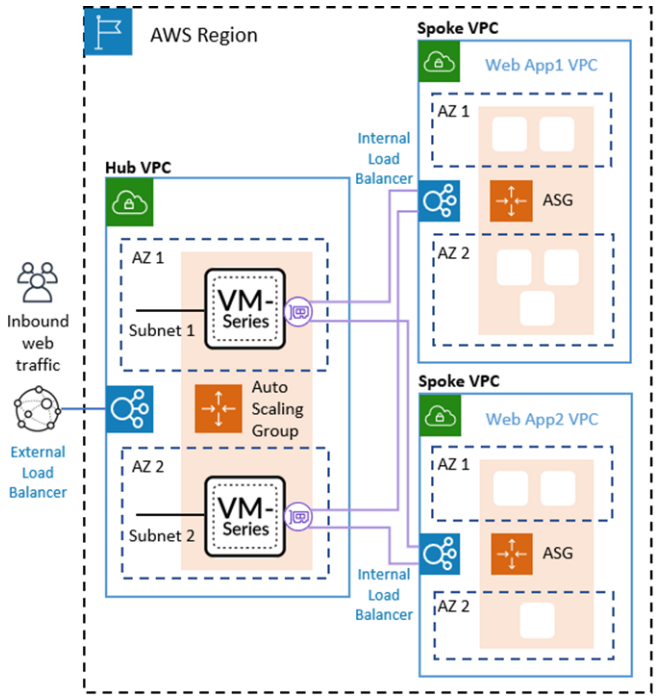
请参阅 AWS 的堆栈更新与 VM 系列自动扩展模板 (v2.0)。

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。



© 2019 Palo Alto Networks, Inc.

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*，并使用连续监视和安全合规性服务，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。

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平衡组合。

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模块。

- VM 系列防火墙模板
- 应用程序模板
- Lambda 函数
- Panorama
- 引导文件

© 2019 Palo Alto Networks, Inc.

VM 系列防火墙模板

防火墙模板在跨越至少两个可用区 (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缩放的自定义 PAN-OS 指标。

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区的防火墙堆栈。
firewall-existing-vpc-v2.1.template	在现有 VPC 中部署具有两到四个可用区的防火墙堆栈。 要在现有 VPC 中部署，您必须输入： • VPC ID • Internet 网关 ID。这是一个现有的网关。 • 子网 CIDR 列出了管理、不可信、可信、NAT 网关和 Lambda 子网。该模板使用 CIDR 来创建这些子网。 如果选择创建新 ELB，则模板会将防火墙 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	在新的 VPC 中部署应用程序，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。支持相同的帐户和跨帐户部署。 您必须提供以下参数： • 中心帐户 ID • VPC 对等的中心 VPC ID • 中心 VPC 可信子网 CIDR。建立 VPC 对等后，模板将这些用于路由表构建，每个可用区域一个 CIDR。 • StsAssumeRoleARN（SQS 访问的 Hub 模板的输出）
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。

© 2019 Palo Alto Networks, Inc.

模板	说明
	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。

受管防火墙使用 `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。

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时间间隔。

应用程序模板启动后，Lambda 将在 Panorama 中填充以下内容：

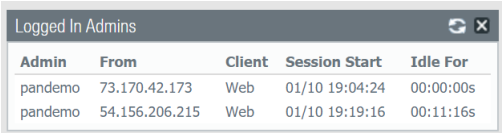
- NAT 政策
- 应用程序模板中 LB 的地址对象
- 虚拟路由器中的静态路由

© 2019 Palo Alto Networks, Inc.

- 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。许可证取消激活密钥应从 Palo Alto 客户支持门户获取，如安装许可证停用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。
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：  Logged In Admins Admin From Client Session Start Idle For pandemo 73.170.42.173 Web 01/10 19:04:24 00:00:00s pandemo 54.156.206.215 Web 01/10 19:19:16 00:11:16s 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缩放？

  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。

© 2019 Palo Alto Networks, Inc.

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。

STEP 1 | 在 规划部署 AWS 的 VM 系列自动扩展模板 (v2.1) 和 规划 AWS 的 VM 系列自动缩放模板（v2.0 和 v2.1）中审查检查清单。

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身份验证代码。您必须将此身份验证代码保存在名为 `authcodes`（没有扩展名）的文本文件中，并把 `authcodes` 文件放在引导数据包的 `/license` 文件夹中。

  如果您使用单个身份验证代码，而非代码包，防火墙只会检索文件中第一个身份验证代码的许可证密钥。
- 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。

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
```


© 2019 Palo Alto Networks, Inc.

```
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
```

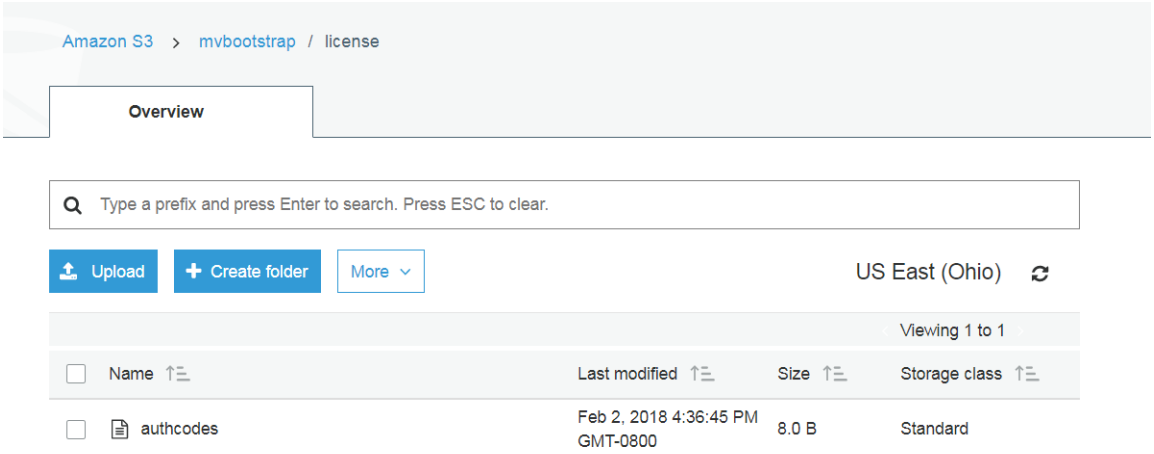
```
dhcp-send-client-id=yes
```

```
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
```

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。

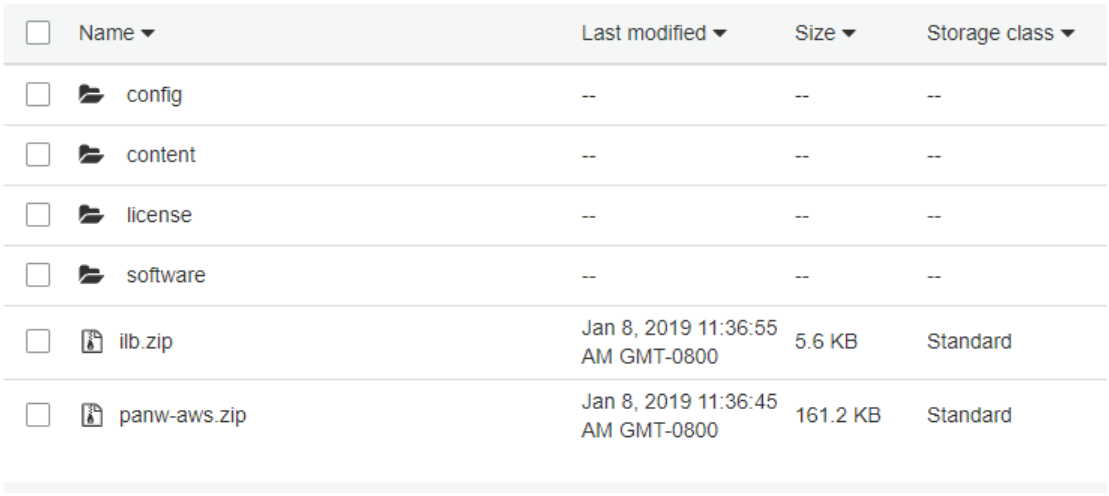
STEP 3 | （仅限 BYOL）将许可证身份验证代码添加到引导软件包的 **/license** 文件夹中。

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 许可证的身份验证代码添加到此文件，然后保存。身份验证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。如果使用单个身份验证代码，而非代码包，防火墙只会检索文件中第一个身份验证代码的许可证密钥。



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。

© 2019 Palo Alto Networks, Inc.



Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
ilb.zip	Jan 8, 2019 11:36:55 AM GMT-0800	5.6 KB	Standard
panw-aws.zip	Jan 8, 2019 11:36:45 AM GMT-0800	161.2 KB	Standard

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。

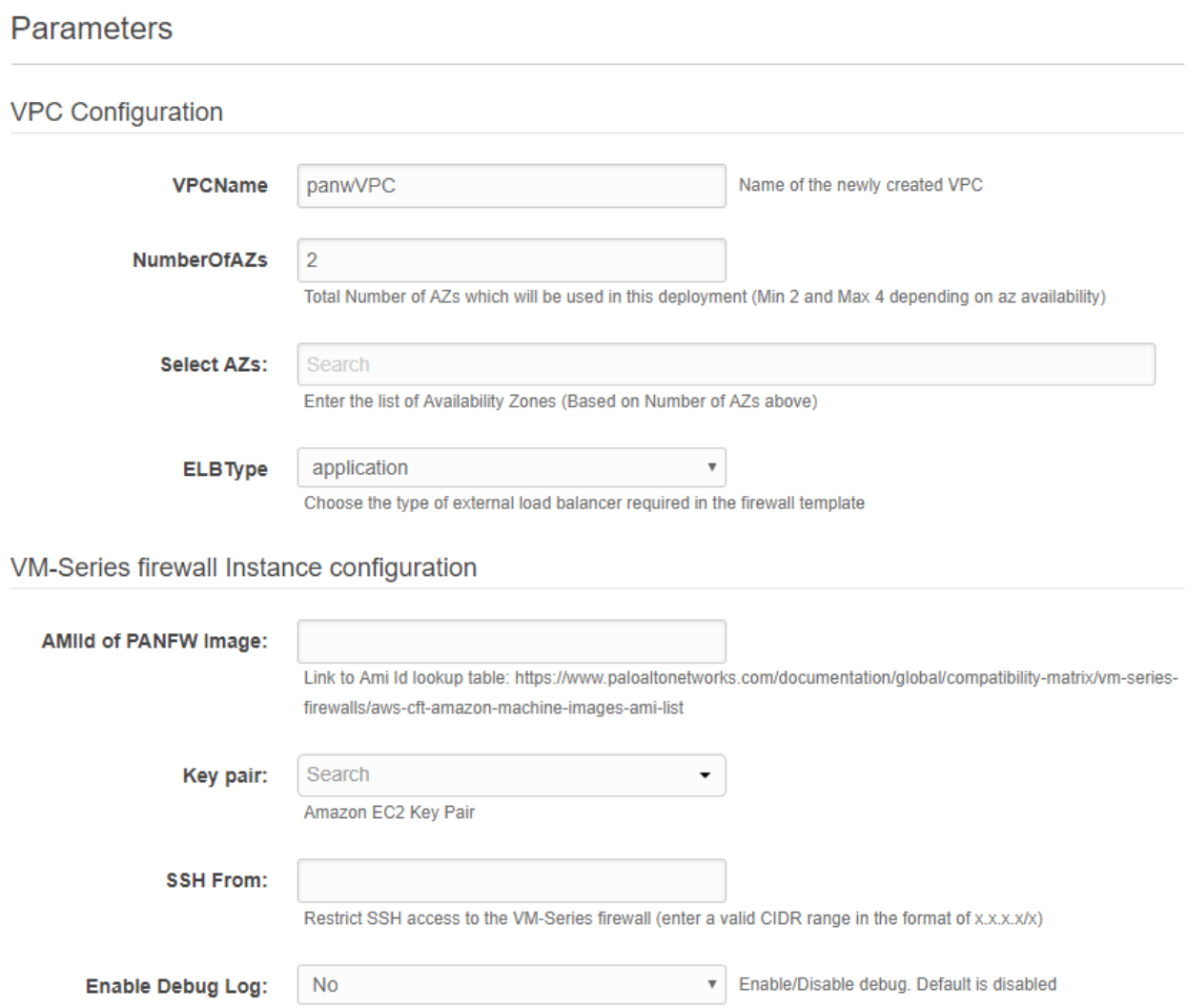
STEP 5 | 选择防火墙模板。

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。

STEP 6 | 配置 VPC 的参数。

1. 请务必选择至少两个可用区域

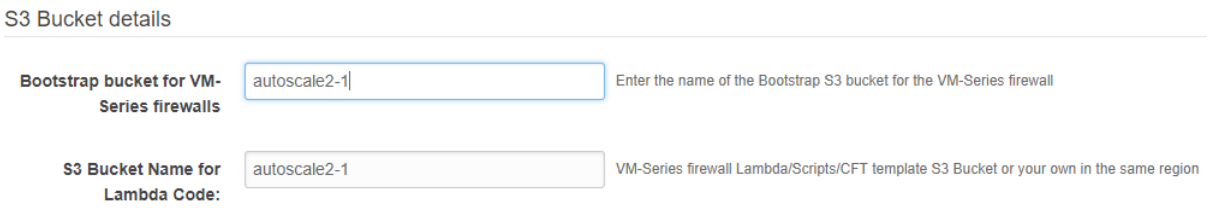
© 2019 Palo Alto Networks, Inc.



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 系列防火墙的缩放参数。 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。

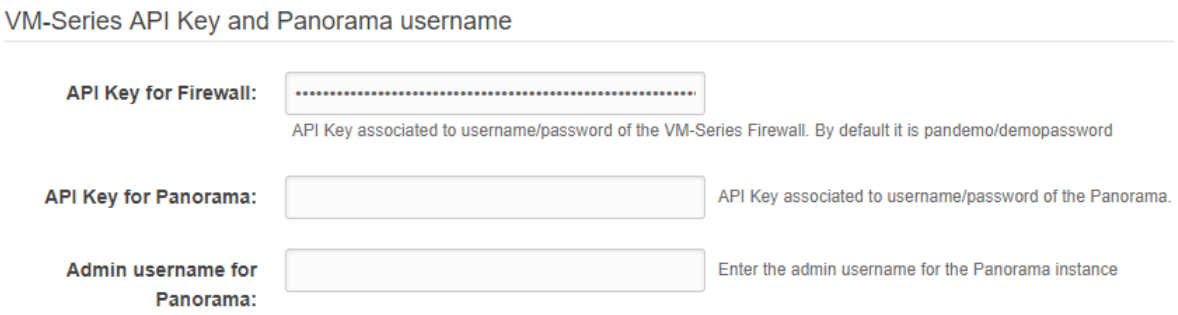


© 2019 Palo Alto Networks, Inc.

1. 输入包含引导程序包的 S3 存储桶的名称。

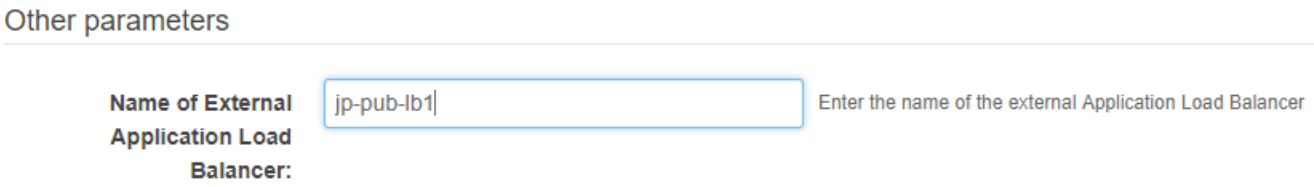
   如果引导桶未正确设置，或者输入的存储桶名称不正确，则引导进程将失败，并且您无法登录到防火墙。对负载均衡器的运行状况检查也失败。
2. 输入包含 panw-aws.zip 文件的 S3 存储桶的名称。如前所述，对于 Bootstrap 和 Lambda 代码，您可以使用一个 S3 存储桶。

STEP 8 | 指定启用 API 访问防火墙和 Panorama 的密钥。



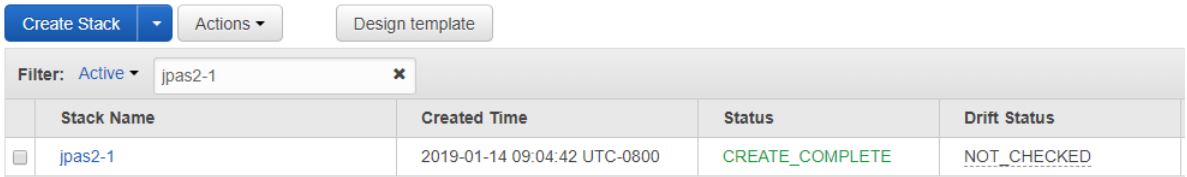
1. 输入防火墙必须用来验证 API 调用的密钥。默认密钥基于示例示例文件，您只能将其用于测试和评估。对于生产部署，您必须为 API 调用创建单独的 PAN-OS 登录并生成关联的密钥。
2. 请输入 API 密钥以允许 AWS Lambda 对 Panorama 进行 API 调用。对于生产部署，您应该为 API 调用创建一个单独的登录并生成关联的密钥。

STEP 9 | 输入应用程序负载均衡器的名称。



STEP 10 | 查看模板设置并启动模板。

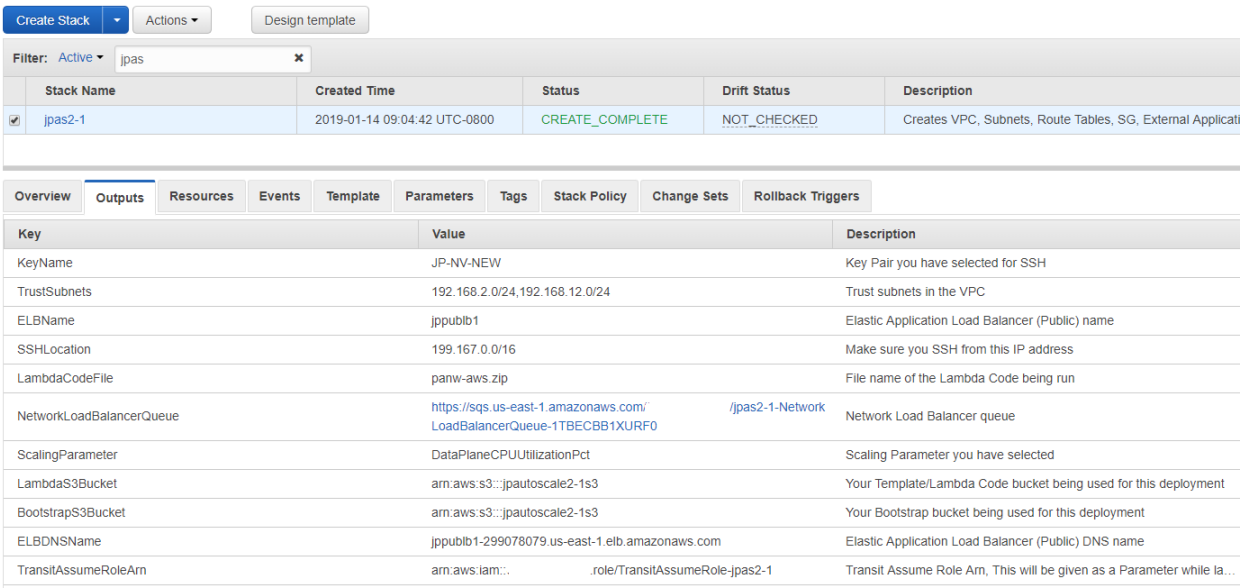
1. 选择 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我承认此模板可能会导致 **AWS CloudFormation** 创建 **IAM** 资源）。
2. 单击 **Create**（创建）以启动模板。显示 CREATE_IN_PROGRESS 事件。
3. 成功部署时，状态会更新到 CREATE_COMPLETE。



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。

© 2019 Palo Alto Networks, Inc.



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 函数监视此队列，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。

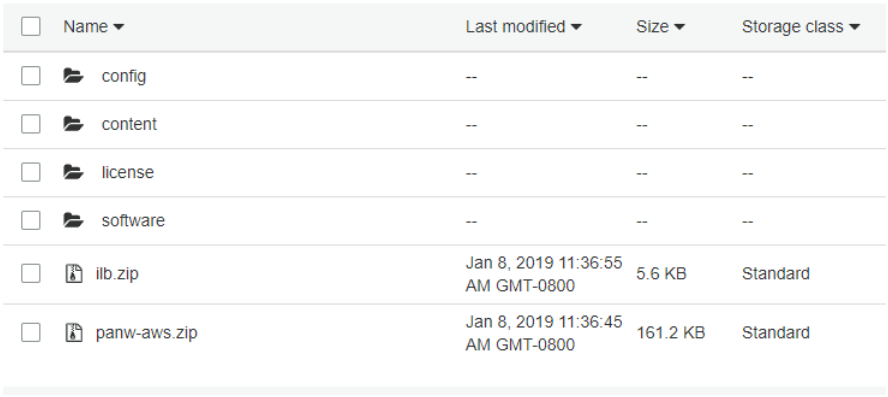
在启动应用程序模板时，您必须根据是将应用程序模板部署在部署防火墙模板的相同 VPC 中还是部署在单独的 VPC 中，从而选择模板。请参阅为 ELB 服务启用流量（v2.0 和 v2.1）。

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。

© 2019 Palo Alto Networks, Inc.

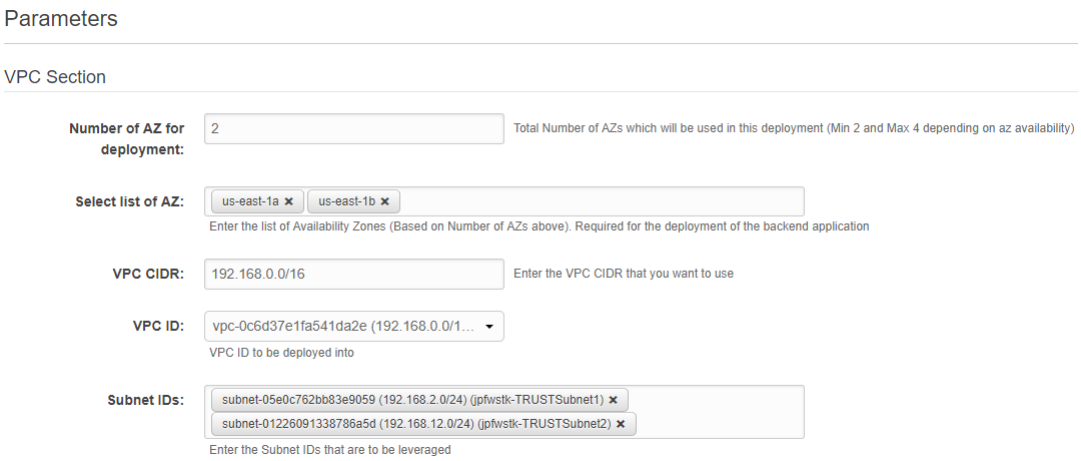


STEP 3 | 选择要启动的应用程序启动模板。

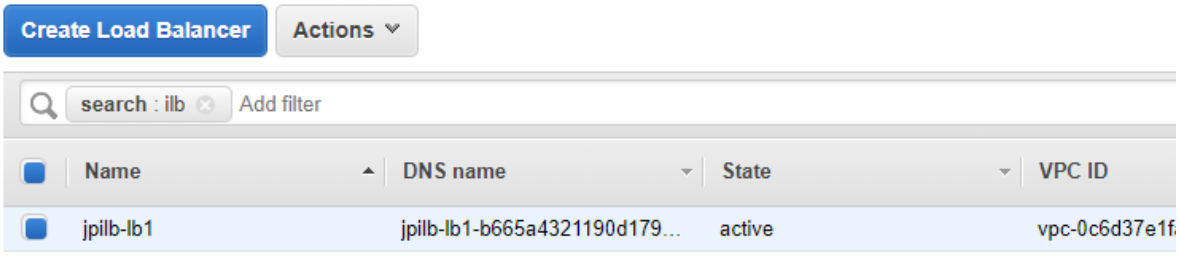
1. 在 AWS 管理控制台上，选择 **CloudFormation** > **CreateStack**。
2. 选择 Upload a template to Amazon S3（将模板上传到 Amazon S3），选择应用程序模板，将模板自动的资源部署到与防火墙相同的 VPC 中，或者将资源部署到不同的 VPC 中。单击 **Open**（打开）和 **Next**（下一步）。
3. 指定 Stack name（堆栈名称）。堆栈名称允许您唯一标识使用此模板部署的所有资源。

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。



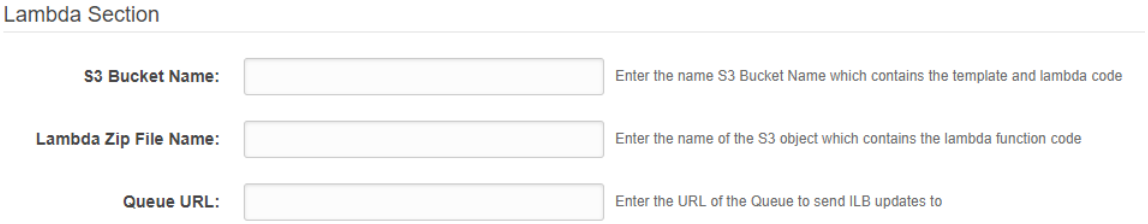
STEP 5 | 选择负载均衡器类型。



STEP 6 | 配置 Lambda 的参数。

© 2019 Palo Alto Networks, Inc.

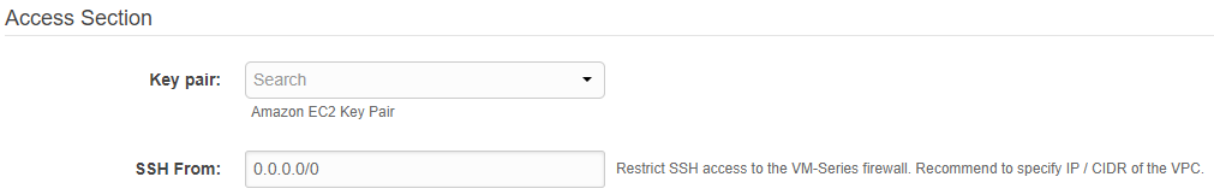
1. 输入存储 ilb.zip 的 S3 存储桶名称。
2. 输入 zip 文件名称。
3. 粘贴您之前复制的 SQS URL。



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。

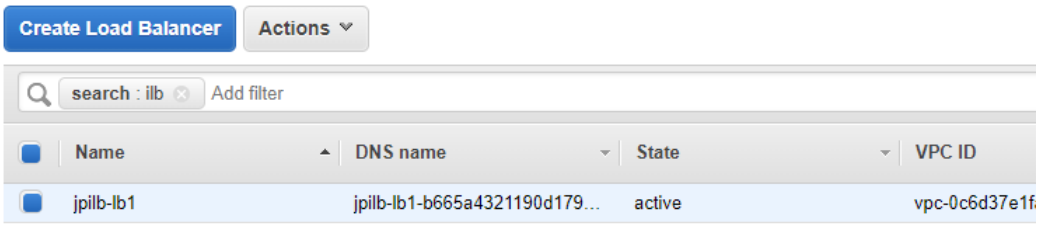
STEP 9 | 对于仅管理访问，选择要访问服务器的网络的 IP 地址。Web 流量来自启动防火墙模板时复制的 ELBDNS 名称。



STEP 10 | 查看模板设置并启动模板。

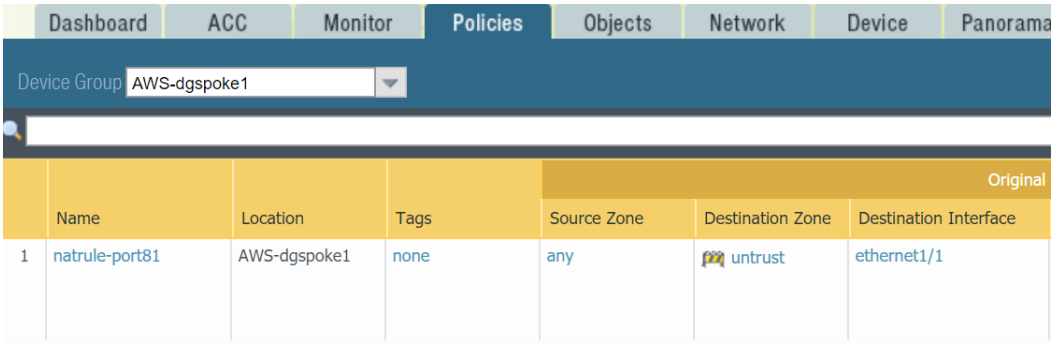
STEP 11 | 完成应用程序模板后，最多可能需要 20 分钟才能生效。

1. 验证应用程序模板负载均衡器是否标记为活动。

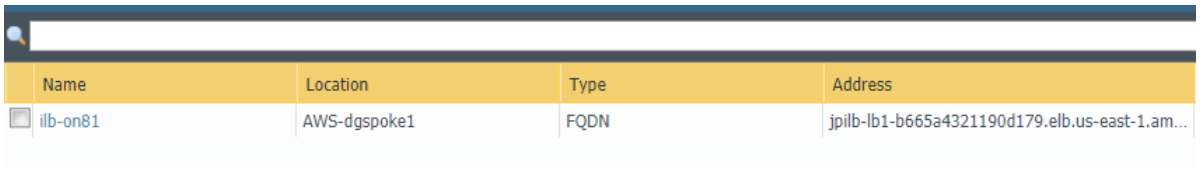


2. 验证 Panorama 在设备组中是否具有 NAT 对象。

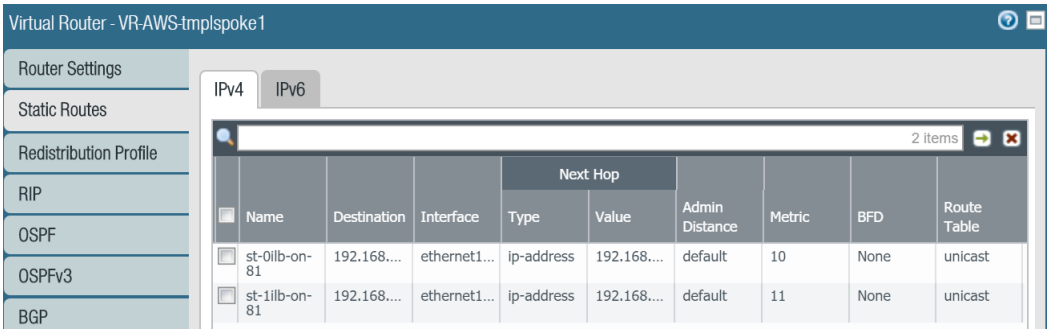
© 2019 Palo Alto Networks, Inc.



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。

Congratulations, you have successfully launched VM-Series ASG CloudFormation. This file is coming from Webserver Region: us-east-1

StackID: arn:aws:cloudformation:us-east-1: :stack/jpappstk1/1c197cb0-18f4-11e9-b92e-0ab87eb901cc

StackName: jpappstk1

© 2019 Palo Alto Networks, Inc.

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 | 配置防火墙上的管理密码。

参阅配置防火墙的新管理密码。

STEP 3 | （仅限 BYOL）激活许可证。

STEP 4 | 在防火墙上安装最新内容。

STEP 5 | （仅限 BYOL）停用许可证。

STEP 6 | 执行私有数据重置。

私有数据重置会删除所有日志并恢复默认配置。

系统磁盘未被擦除，因此第 4 步的内容更新完好无损。

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
```

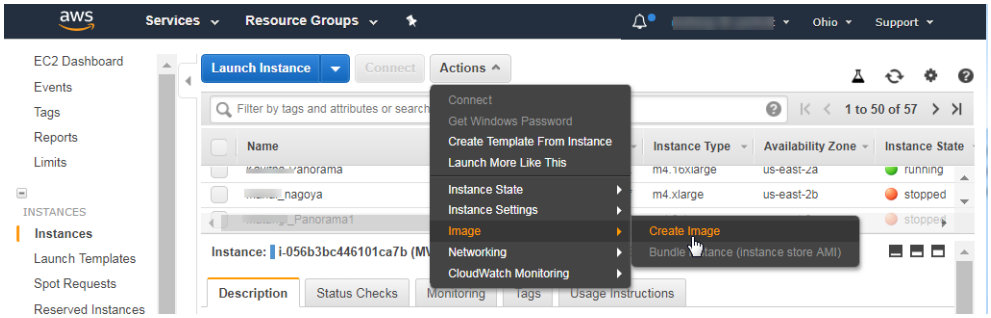
输入 **ÿ** 确认。

防火墙重新启动以初始化默认配置。

STEP 7 | 创建自定义 AMI。

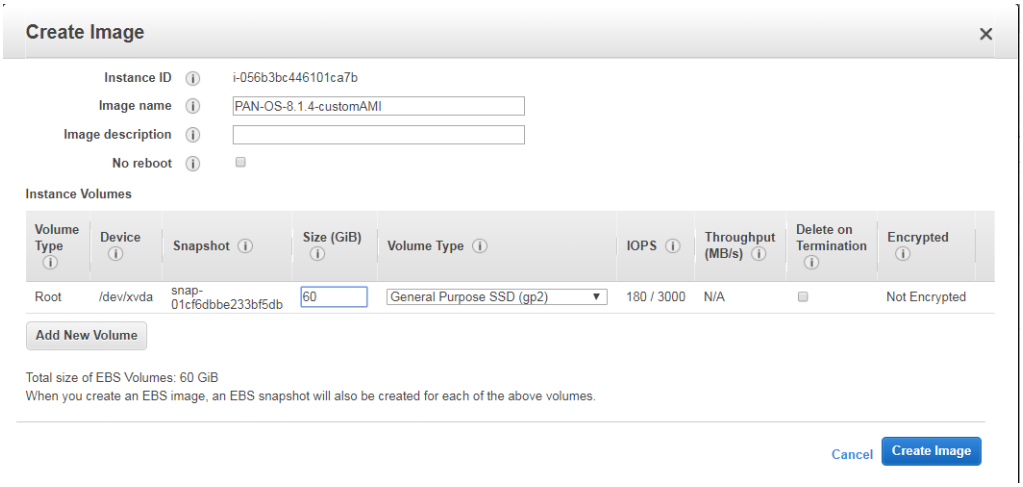
1. 登录到 AWS 控制台，然后选择 EC2 仪表盘。
2. **Stop**（停止）VM 系列防火墙。
3. 选择 VM 系列防火墙实例，然后单击 **Image**（映像）> **Create Image**（创建映像）。

© 2019 Palo Alto Networks, Inc.



4. 输入自定义映像名称，然后单击 **Create Image**（创建映像）。

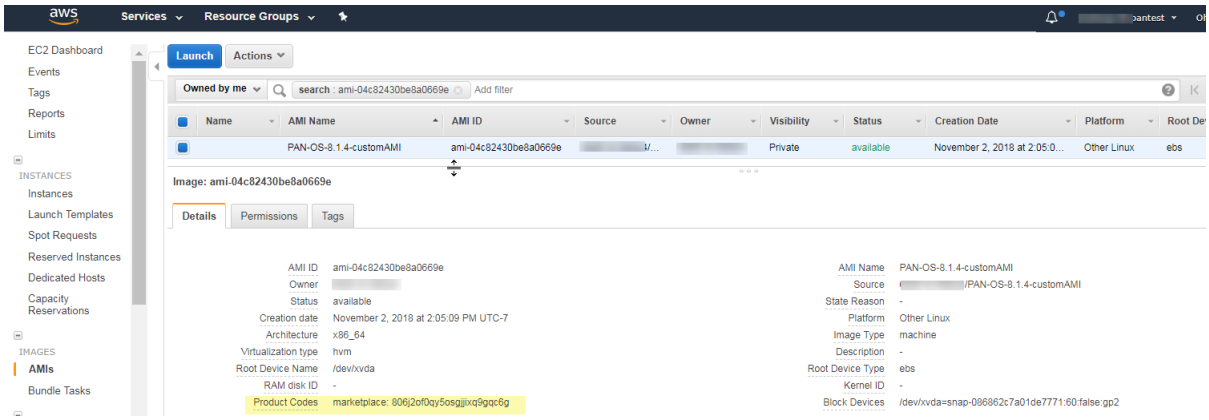
   60GB 的磁盘空间是最低要求。



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



STEP 8 | 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 用于使用 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。

© 2019 Palo Alto Networks, Inc.

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

```
msg_add_nlb= {

        "MSG-TYPE": "ADD-NLB",

        "AVAIL-ZONES": [

        {

            "NLB-IP":"192.168.2.101",

            "ZONE-NAME":"us-east-2a",

            "SUBNET-ID": "subnet-2a566243"

        },
```


© 2019 Palo Alto Networks, Inc.

```
        {
            "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",
}
```

ADD-ALB

```
{   "AVAIL-ZONES": [
        {
            "SUBNET-CIDR": "172.32.0.0/24",
            "SUBNET-ID": "subnet-0953a3a8e2a8208a9",
```


© 2019 Palo Alto Networks, Inc.

```
            "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",
            "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",
```


© 2019 Palo Alto Networks, Inc.

```
    "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。

AWS 更新与 VM 系列自动扩展模板 (v2.1)

堆栈更新允许您修改 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用户帐户相关联的 API 密钥。

要修改默认通知或创建自动扩展警报，您不必更新堆栈。请参阅更改扩展参数和 CloudWatch 指标 (v2.1)。

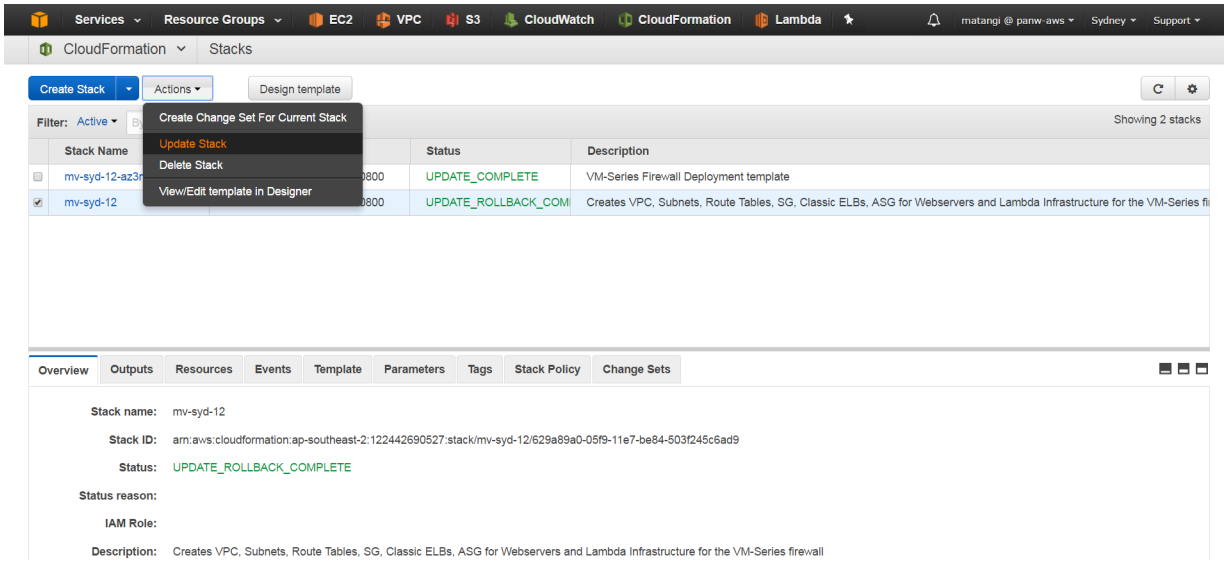
在部署 VM 系列自动扩展模板时，会自动为您创建自动扩展组和启动配置。启动配置是自动扩展组用于启动 EC2 实例的模板，它用于指定参数，例如实例类型、自动扩展组的密钥对或与防火墙上的管理用户帐户关联的 API 密钥。

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）。

© 2019 Palo Alto Networks, Inc.

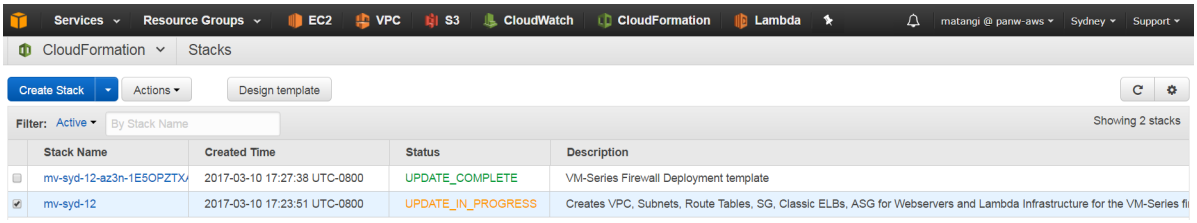


STEP 2 | 修改您想要更新的资源。

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)。

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缩放操作。

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：

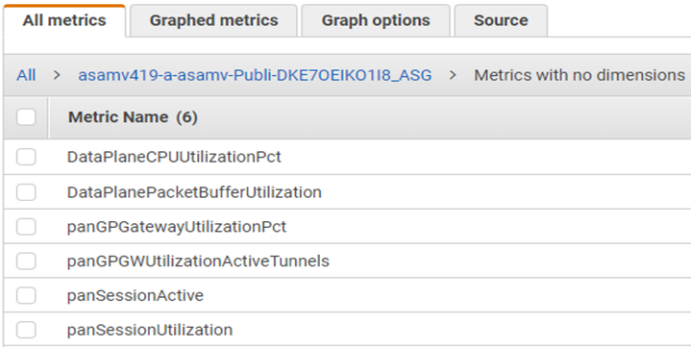
- <自定义命名空间> -scalein - 删除 1 个实例
- <自定义命名空间> -scaleout - 添加 1 个实例

© 2019 Palo Alto Networks, Inc.

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缩放操作。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。

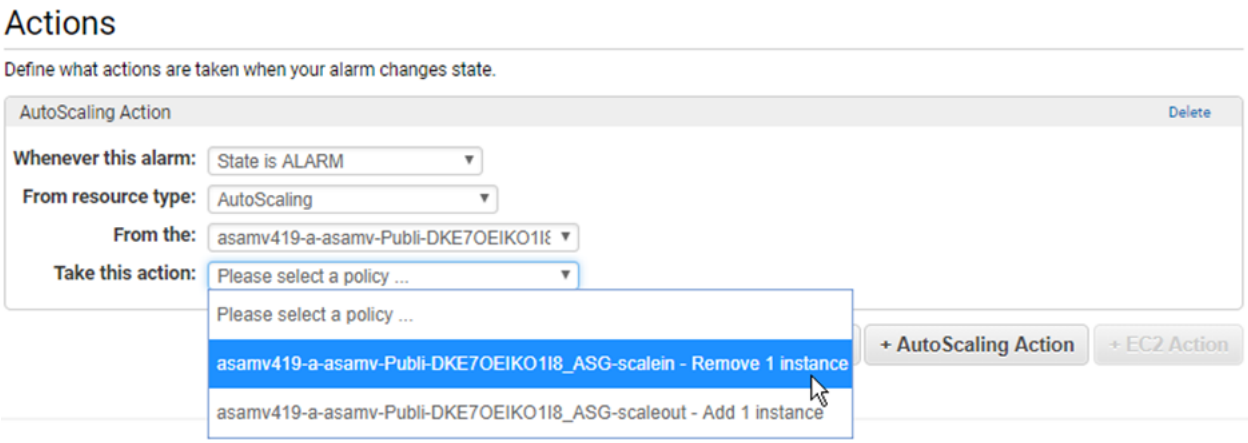


STEP 3 | 选中一个框以选择指标，然后选择 **Graphed metrics**（图表指标）标签。

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。

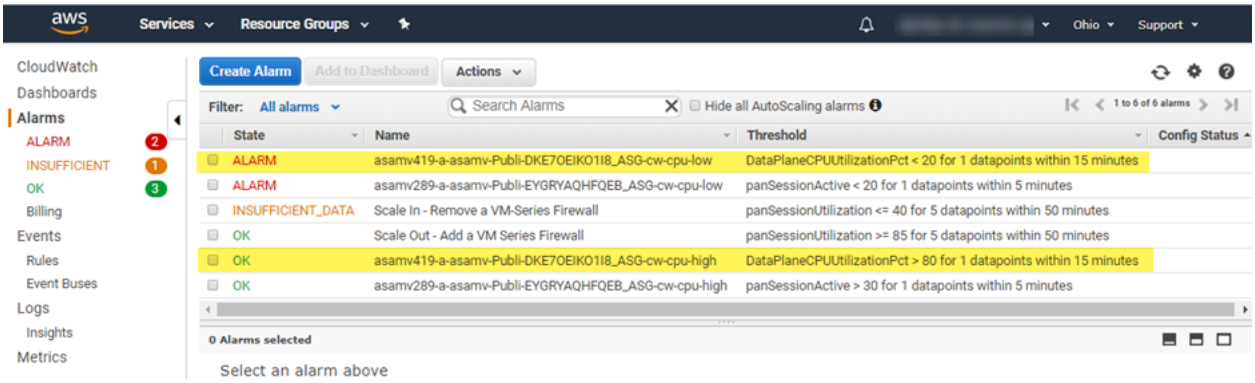


5. 选择 **Create Alarm**（创建警报）。

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）。

© 2019 Palo Alto Networks, Inc.



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）。

© 2019 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 — Microsoft 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® 受管防火墙。使用插件后，Panorama 最多可为每个虚拟机检索共计 32 个标记，包括 11 个预定义标记和最多 21 个用户定义的标记。

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
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

© 2019 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
安全组名称	Sg-name.<SecurityGroupName>	否	是
VPC ID	VpcId.<VpcId string>	是	是
标记（密钥，值）	aws-tag.<key>.<value>	Yes; 最多可支持 18 个用户定义标记。用户定义的标记按字母顺序排序，且前 18 个标记可用于防火墙。	Yes; 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 访问密钥和秘密访问密钥的用户 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": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeKeyPairs",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs"
            ],
            "Resource": [
                "*"
            ]
}
    ]
}
```


© 2019 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

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

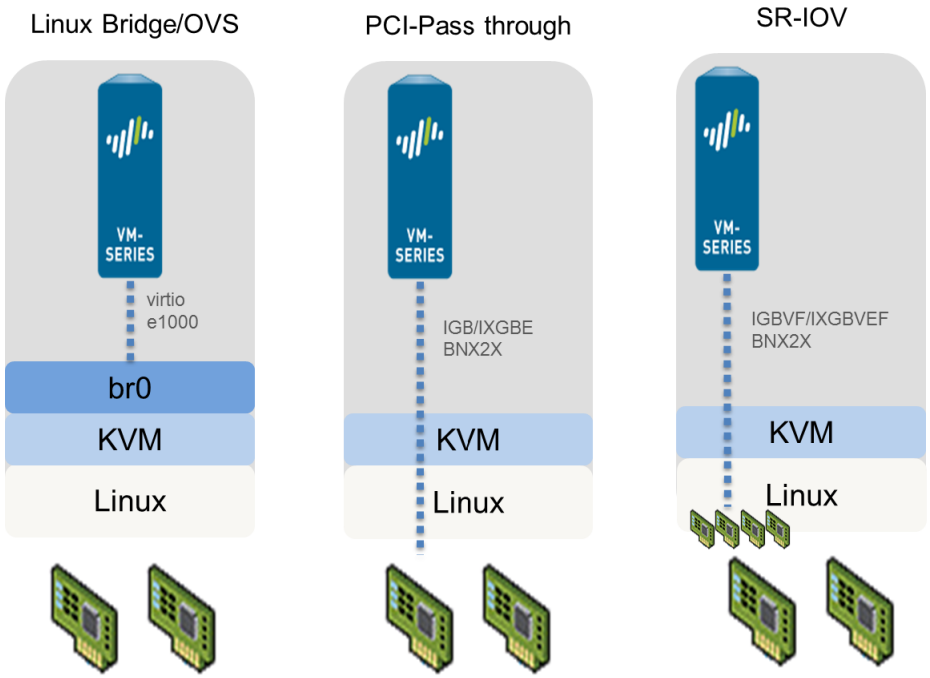
表 2: KVM 系统上 VM 系列的要求

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 VM 系列防火墙上的 SR-IOV 和 DPDK 驱动程序。
DPDK 驱动程序	请参阅兼容性矩阵中 VM 系列防火墙上的 SR-IOV 和 DPDK 驱动程序。 如果使用以下 NIC 驱动程序之一，在默认情况下，KVM 上的 VM 系列防火墙上启用 DPDK： • 虚拟驱动程序：virtio • NIC 驱动程序：ixgbe、ixgbevf、i40e、i40evf

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。
	• 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
	  • 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。
	  • 驱动程序：igb；ixgbe；bnx2x
	  • 驱动程序：igbvf；ixgbevf；bnx2x
	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。

© 2019 Palo Alto Networks, Inc.

用于在网络上连接 VM 系列防火墙的选项



- 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

- ❑ 检查 Linux 分布版本。有关受支持版本的列表，请参阅 KVM 系统上 VM 系列的要求。
- ❑ 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。

- ❑ 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。
  - 确保您计划使用的所有接口的链路状态均正常，有时必须手动使其状态变成正常。
  - 确认所有接口的 PCI ID。要查看列表，使用命令：**`Virsh nodedev-list –tree`**

© 2019 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 PCI-passthrough 或 SR-IOV，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，必须手动将接口与 Linux 服务器分开；有关说明，请参阅网卡供应商提供的文档。

  要从服务器手动分开接口，使用命令：

  `Virsh nodedev-detach <pci id of interface>`

  例如：**`pci_0000_07_10_0`**

  在某些情况下，在 /etc/libvirt/qemu.conf 中，可能需要取消对 `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。

  要启用虚拟功能，需要：

  1.在此位置创建一个新文件： /etc/modprobe.d/

  2.使用 vi 编辑器修改文件使功能更持久：vim /etc/modprobe.d/igb.conf

  3.启用虚拟功能所需的数量：options igb max_vfs=4

  在保存更改和重新启动 Linux 服务器后，本示例中的每个接口（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。

- ❑ 配置主机以获得最大的 VM 系列性能。有关配置每个选项的信息，请参阅 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管理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。
  - 在 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。

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。

© 2019 Palo Alto Networks, Inc.

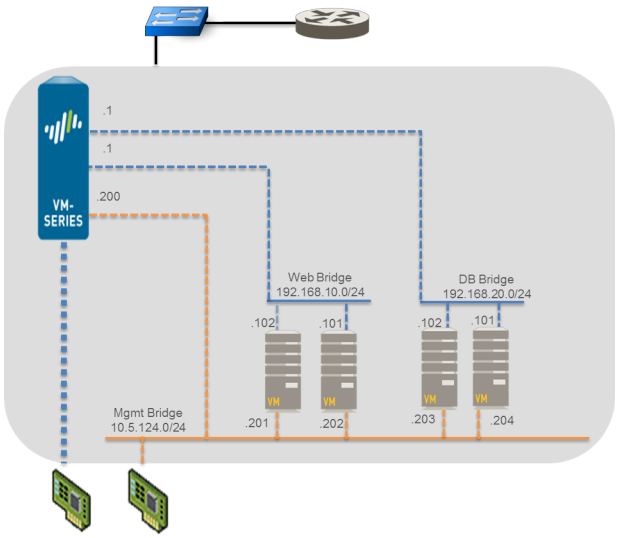
在 KVM 上支持的部署

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。

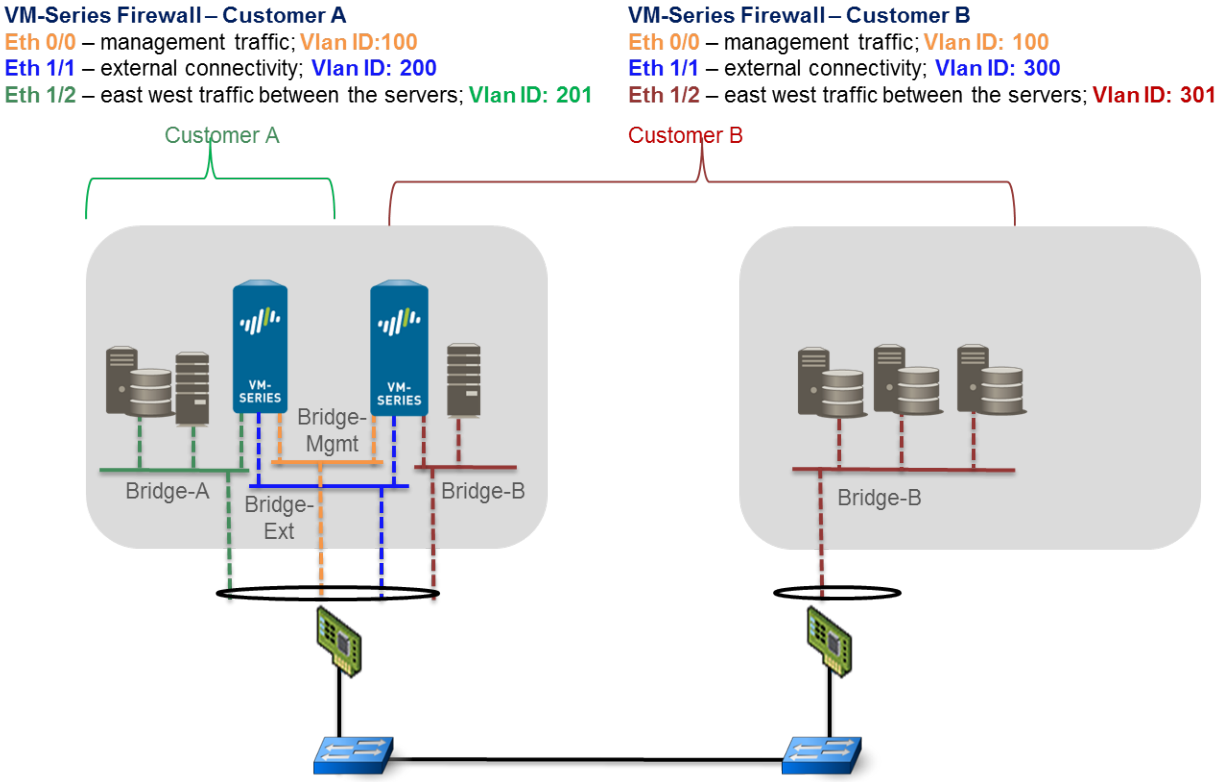


保护 Linux 主机之间的流量

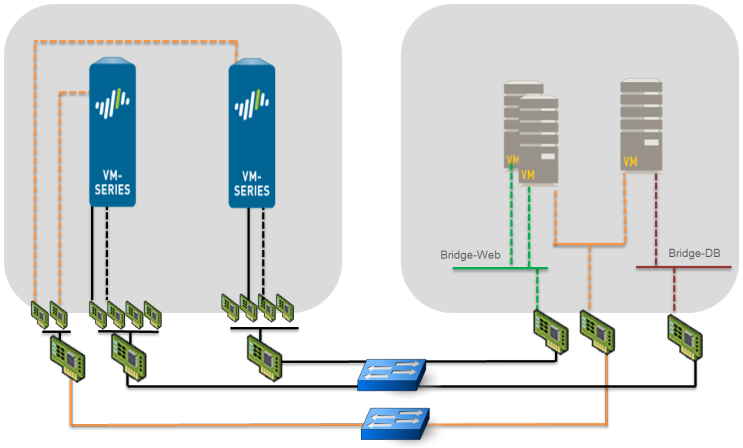
要保护您的工作负载，可以在 Linux 主机上部署多个 VM 系列防火墙实例。例如，如果要为单独的部门或客户隔离流量，可以使用 VLAN 标记

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。

© 2019 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。高可用性对等设备中的主动对等设备保护从在不同 Linux 服务器上部署的来宾向其路由的流量。



© 2019 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 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。

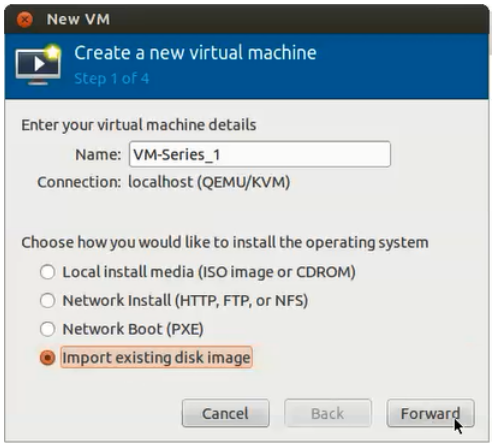
- 在 KVM 主机上设置 VM 系列防火墙
- 在 KVM 上执行 VM 系列防火墙的初始配置

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。

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。

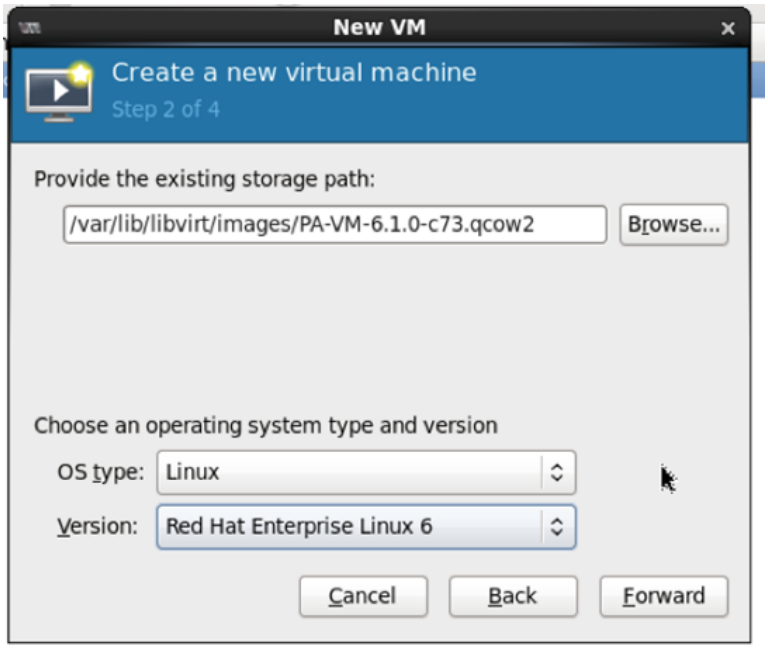
1. 在 Virt-manager 上，选择 **Create a new virtual machine**（创建新虚拟机）。
2. 添加 VM 系列防火墙的描述性 **Name**（名称）。



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”。

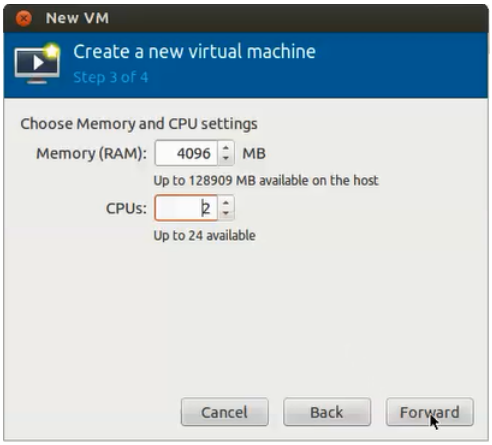
© 2019 Palo Alto Networks, Inc.



4. 添加数据接口的网络适配器：

STEP 2 | 配置内存和 CPU 设置。

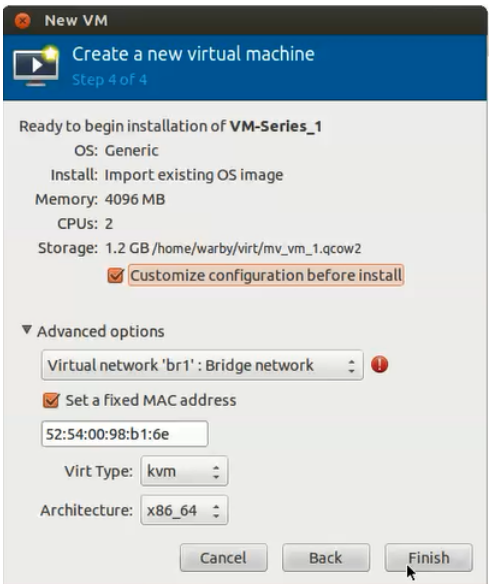
1. 根据您的 VM 系列型号的 VM 系列系统要求设置 **Memory**（内存）为最小内存。
2. 根据您的 VM 系列型号的 VM 系列系统要求设置 **CPU** 为最小 CPU 数量。



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。

© 2019 Palo Alto Networks, Inc.

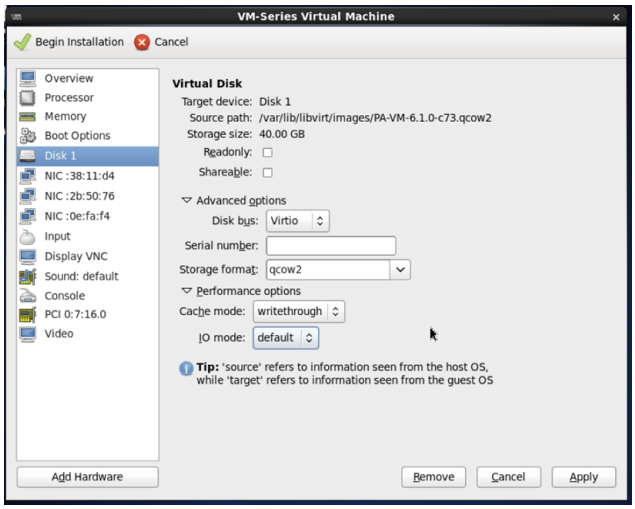


STEP 4 | 配置虚拟磁盘设置。

1. 选择 **Disk**（磁盘），展开“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。

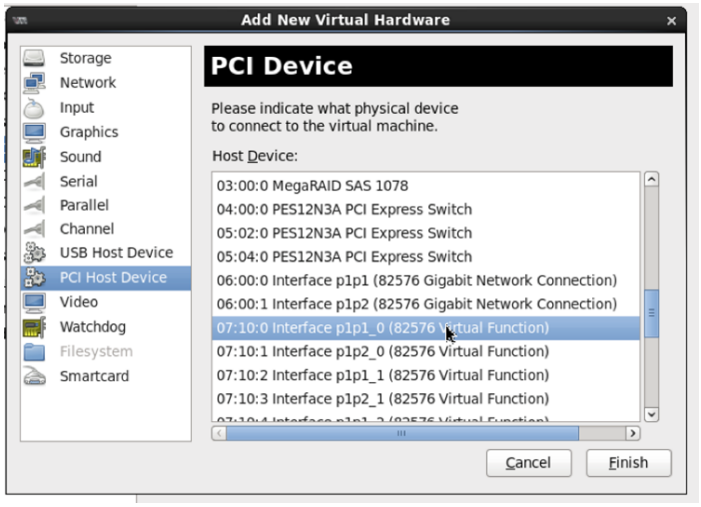


STEP 5 | 配置网络适配器。

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。

© 2019 Palo Alto Networks, Inc.

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）



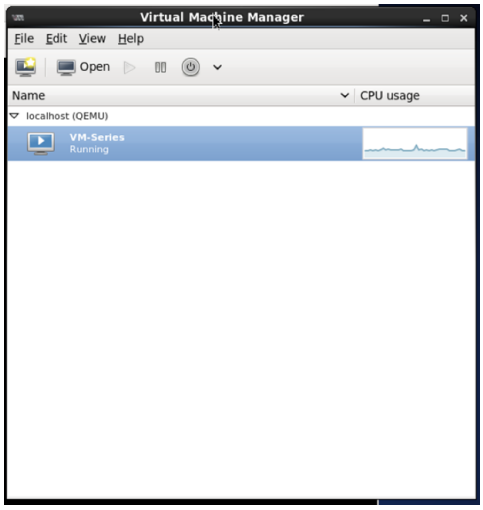
。

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。

STEP 6 | 单击 **Begin Installation**（开始安装） 。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。

© 2019 Palo Alto Networks, Inc.



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：

```
configure
```

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>* 是要分配给管理接口的 IP 地址，*<netmask>* 是子网掩码，*<gateway-IP>* 是网络网关的 IP 地址，*<DNS-IP>* 是 DNS 服务器的 IP 地址。

3. ```
   commit
   ```

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
```


© 2019 Palo Alto Networks, Inc.
```

```
Ethernet1/5              eth5          52:54:00:f4:62:13 0000:00:10.0
```

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。如果让 Panorama 进行集中管理，有关使用 Panorama 管理设备的更多信息，请参阅《Panorama 管理员指南》。

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。

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> netmask <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

© 2019 Palo Alto Networks, Inc.

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
```

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：

© 2019 Palo Alto Networks, Inc.

```
# 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 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>
```


© 2019 Palo Alto Networks, Inc.

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>
```


© 2019 Palo Alto Networks, Inc.

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。

```
[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>
```


© 2019 Palo Alto Networks, Inc.

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 系列防火墙的接口的列表。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' 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)。

© 2019 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，但可能需要调整管理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 直通或 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 管理程序平台。

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。

```
[...]
    <interface type='bridge'>
```


© 2019 Palo Alto Networks, Inc.

```
      <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
```

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：

© 2019 Palo Alto Networks, Inc.

```
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
```

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
```


© 2019 Palo Alto Networks, Inc.

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
```

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。

© 2019 Palo Alto Networks, Inc.

```
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
```

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'/>
```


© 2019 Palo Alto Networks, Inc.

```
    </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>
```

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管理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 SR-IOV 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 -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 管理程序上的来宾 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。

© 2019 Palo Alto Networks, Inc.

要验证 VM 上显示的 CPU 标志，可执行以下命令：

cat /proc/cpuinfo

在 flags 输出中，查找以下标志：

- 对于带有 DPDK 1.11 版本的 PAN-OS 9.1，需要 AVX，或 AES 和 SSE。
- 对于带有 DPDK 18.11 版本的 PAN-OS 9.1，需要 AVX 或 SSE。

STEP 3 | 定义和启动网络后，可修改 KVM 管理程序上的来宾 VM 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。

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；您必须在主机管理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

© 2019 Palo Alto Networks, Inc.

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**。

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>
```


© 2019 Palo Alto Networks, Inc.

```
      <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>
```

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>
```

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 可作为一个单独的管理程序进行打包，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

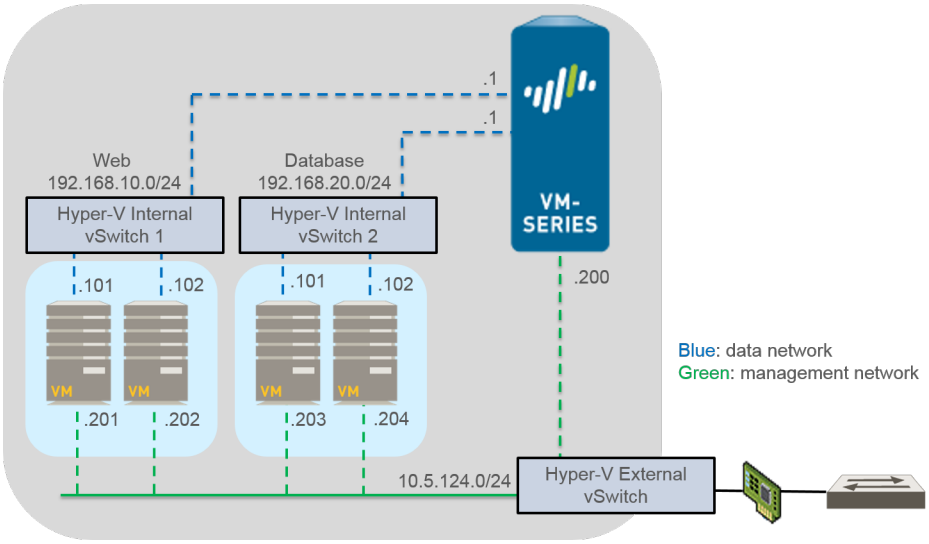
Hyper-V 上支持的部署

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

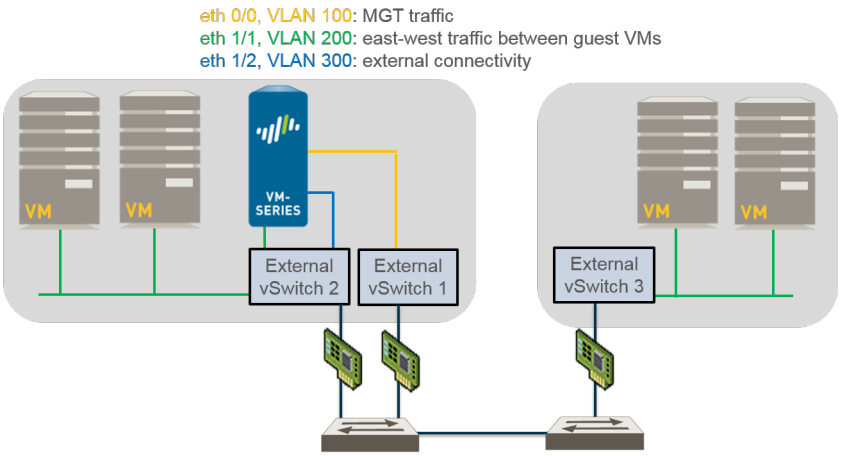
VM 系列防火墙可部署在单个 Hyper-V 主机和其他客户端 VM 上。在下述示例中，VM 系列防火墙拥有一个第 3 层接口，而 VM 系列防火墙和其他客户端 VM 通过 Hyper-V vSwitch 实现连接。Web 服务器和数据库服务器之间的所有流量都会通过防火墙路由。仅通过数据库服务器或仅通过 Web 服务器的流量将由外部 vSwitch 处理，且不会通过防火墙。



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。

© 2019 Palo Alto Networks, Inc.



© 2019 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 系列防火墙不支持传统网络适配器或 SR-IOV/PCI-Passthrough。

© 2019 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。

© 2019 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，需确保使用由管理程序分配的 MAC 地址，确保管理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。

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，但可能需要调整管理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。

© 2019 Palo Alto Networks, Inc.

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）。

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 系列防火墙选择一个 **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**（联网）。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。

© 2019 Palo Alto Networks, Inc.

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）如果您未通过管理程序分配的 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。

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。

© 2019 Palo Alto Networks, Inc.

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-name">
 -SwitchName <"management-vswitch">
```

STEP 5 | （可选）如果您未通过管理程序分配的 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>
```

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> netmask <netmask>
default-gateway <gateway-IP> dns-settingservers primary <DNS-IP>
```

其中，*<Firewall-IP>* 是要分配给管理接口的 IP 地址，*<netmask>* 是子网掩码，*<gateway-IP>* 是网络网关的 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。

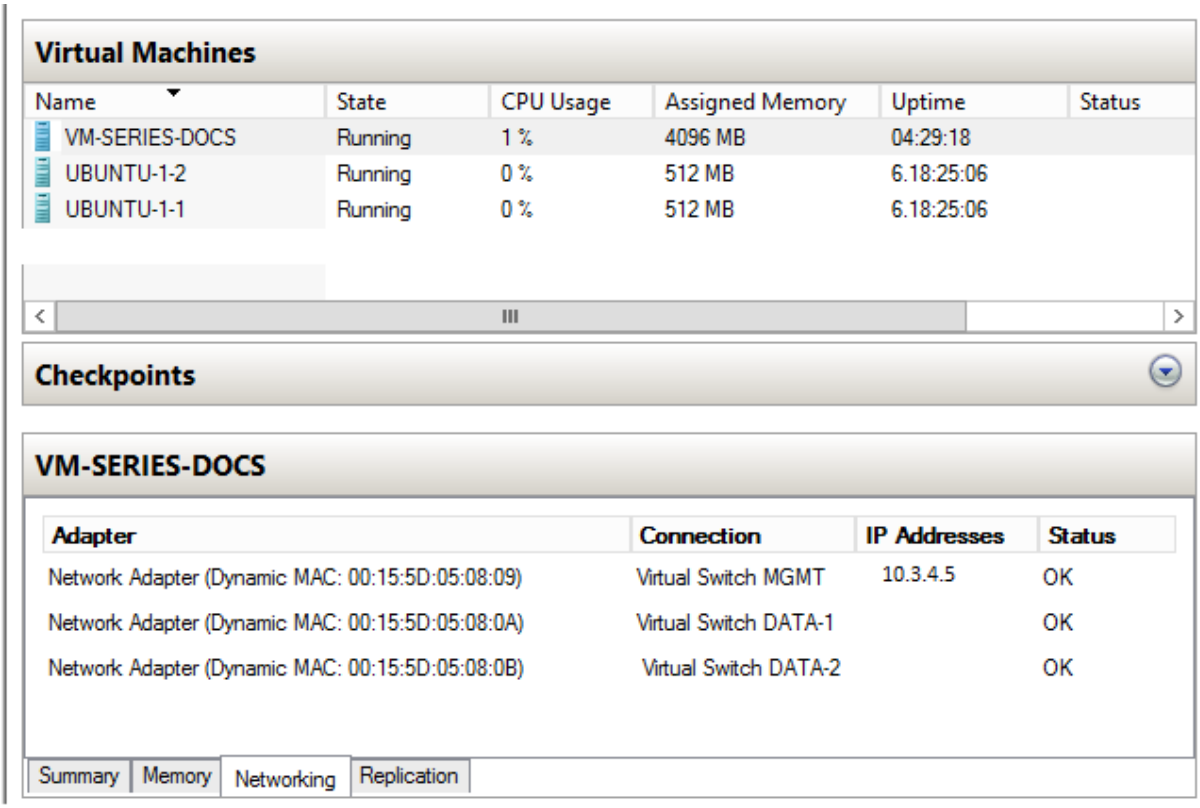
1. 输入 **commit**。

© 2019 Palo Alto Networks, Inc.

2. 输入 **exit**。

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**（联网）。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 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
```


© 2019 Palo Alto Networks, Inc.

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 系列防火墙的巨帧配置未超过 Hyper-V 上支持的最大 MTU。

在启用巨帧的情况下，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**（巨帧数据包）。
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 上启用巨帧，请在 VM 系列防火墙上启用巨帧，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》。

© 2019 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）
> 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 上自动扩展 VM 系列防火墙
> 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/。

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

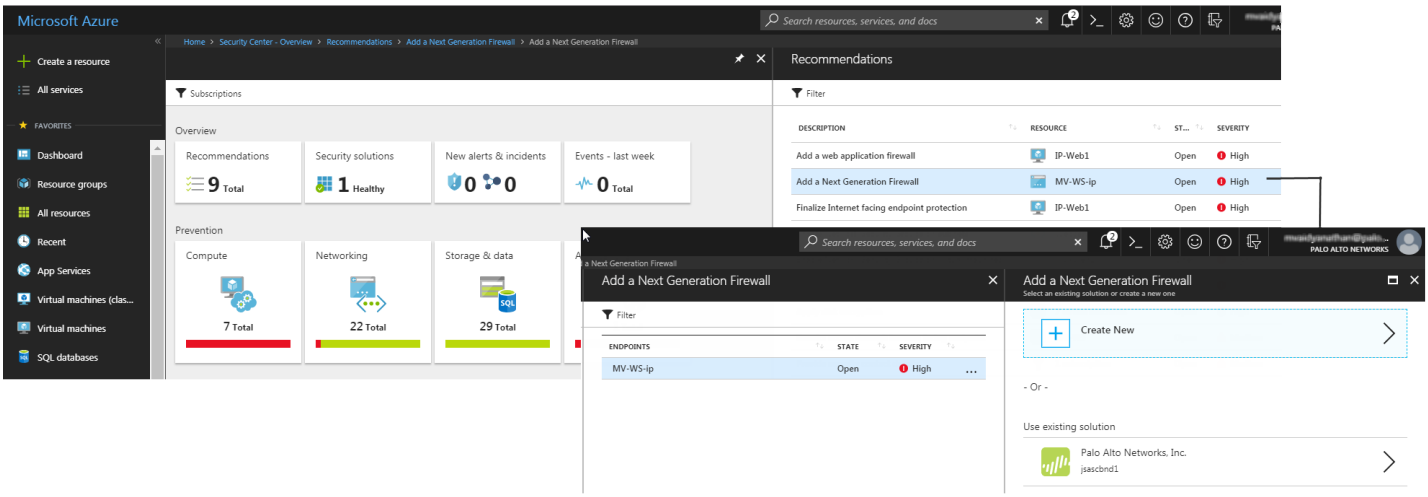
Microsoft 已弃用 Azure 安全中心对合作伙伴解决方案的支持，并将其替换为 Azure Sentinel。

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：

© 2019 Palo Alto Networks, Inc.

- 基于 **Azure** 安全中心仪表盘上的建议部署 **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需要保护的工作负载的流量路径。

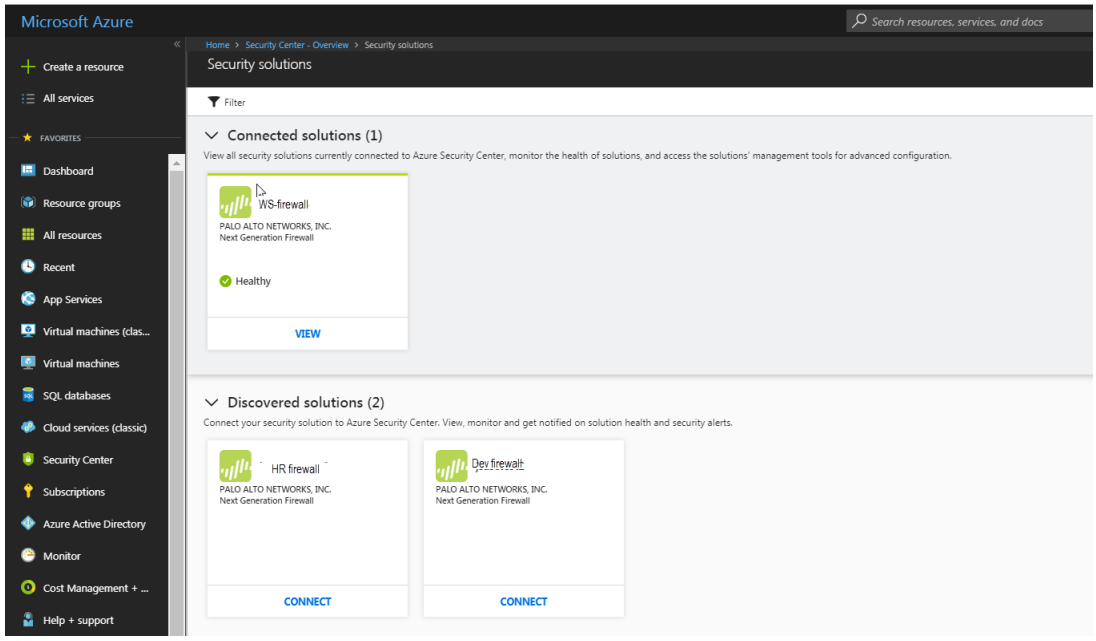
当您部署 Azure 安全中心的防火墙时，此防火墙通过三个网络接口以及用户定义路由 (UDR) 启用。这三个网络接口为管理接口、面向外部的接口（不可信）和面向内部的接口（可信）。用户定义路由将来自可信子网的出站流量发送至防火墙上可信接口，以便防火墙始终检测 Internet 入站流量。在使用默认防病毒、防间谍软件和漏洞保护配置文件对流量进行检测后，默认配置可包括两个示例安全策略规则：默认出站规则和默认入站规则。前者允许所有来自可信区域的流量流向应用程序默认端口的不可信区域，而后者允许所有来自不可信区域的 Web 浏览流量流向可信区域。此外，防火墙还将入站或出站规则拦截的所有文件发送至 WildFire 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、网络钓鱼和未知的所有流量。除了这些安全配置文件，还可启用这两种安全策略规则在会话结束时记录日志，并将威胁和 WildFire 提交日志作为安全警报转发给 Azure 安全中心仪表盘。

要实际使用此集成并在相同的资源组内基于 Azure 安全中心建议部署 VM 系列防火墙。作为想要保护的工作负载，则可以使用暴露于互联网的公共 IP 地址分阶段执行工作负载。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 订阅中的防火墙在 Azure 安全中心仪表盘上的安全解决方案中进行分组。

  Microsoft Azure 不支持使用免费层订阅发现现有防火墙。

© 2019 Palo Alto Networks, Inc.



要从 Azure 安全中心连接现有 VM 系列防火墙，则必须设置 Linux 虚拟机，并配置 Syslog 转发，以转发作为警报的公共事件格式的防火墙日志到 Azure 安全中心。通过其他配置，可启用一个单一的平台视图，以监控所有 Azure 资产。

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。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*

© 2019 Palo Alto Networks, Inc.

- 产品：*vmseries1*
- *SKU*：*byol*、*bundle1*、*bundle 2*
- 版本：*9.0.0*、*8.1.0*、*8.0.0*、*7.1.1* 或更高版本

- 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：
  - Standard_D3_v2（默认）
  - Standard_D4_v2
  - Standard_D5_v2
  - Standard_D4_v3
  - Standard_D16_v3
  - Standard_DS3_v2
  - Standard_DS4_v2
  - Standard_DS5_v2

  这些类型包括对加速网络 (SR-IOV) 的支持。
- 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

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。如果您没有所需权限，请要求 Azure AD 或订阅管理员创建服务主体。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）。

© 2019 Palo Alto Networks, Inc.

要支持	权限

Azure 高可用性在 Azure 上设置主动/被动 HA	`Microsoft.Authorization/*/read`
	`Microsoft.Network/networkInterfaces/*`
	`Microsoft.Network/networkSecurityGroups/*`
	`Microsoft.Network/virtualNetworks/*`
	`Microsoft.Compute/virtualMachines/read`

Azure Application Insights在 VM 系列防火墙上启用 Azure 应用程序见解	`Microsoft.Authorization/*/read`
	`Microsoft.Network/networkInterfaces/*`
	`Microsoft.Network/networkSecurityGroups/*`
	`Microsoft.Network/virtualNetworks/*`
	`Microsoft.Compute/virtualMachines/read`

Azure 自动扩展在 Azure 上自动扩展 VM 系列防火墙	需要服务主体的最低 **Contributor**（贡献者）角色。或者，您可以添加以下自定义权限：
	`Microsoft.Network/virtualNetworks/read`
	`Microsoft.Network/routeTables/read`
	`Microsoft.Network/loadBalancers/read`
	`Microsoft.Insights/components/read`
	`Microsoft.Network/publicIPAddresses/read`
	`Microsoft.Network/applicationGateways/read`
	`Microsoft.Compute/virtualMachineScaleSets/read`
	`Microsoft.Insights/autoscalesettings/read`

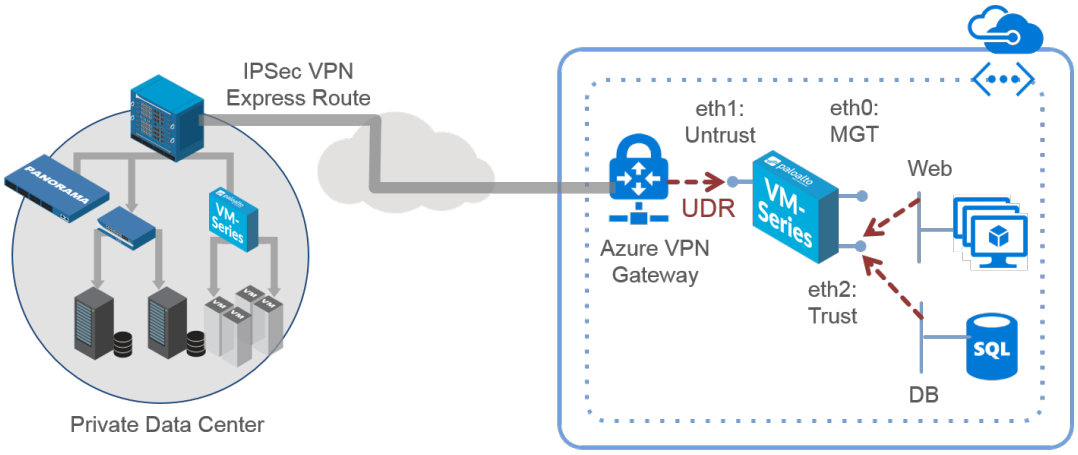
Azure VM 监控在 Panorama 上设置用于 VM 监控的 Azure 插件	需要服务主体的最低 **Reader**（读取者）角色。或者，您可以添加以下自定义权限：
	`Microsoft.Compute/virtualMachines/read`
	`Microsoft.Network/networkInterfaces/read`
	`Microsoft.Network/virtualNetworks/read`

© 2019 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 IPSec 隧道和应用程序允许列表策略来保护在各个 VNet 之间流动的流量，从而提高数据中心安全。



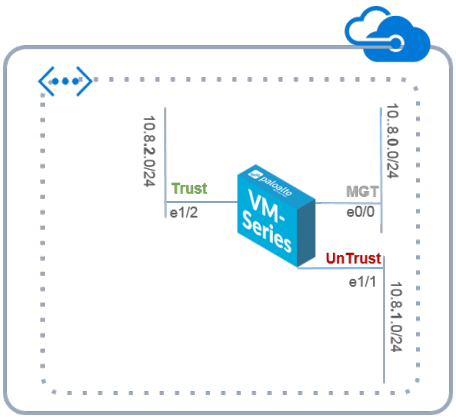
- **Inter-Subnet** — 此 VM 系列防火墙可位于 VNet 中服务器的上游，并保护多层架构中应用程序之间子网间流量免于遭受横向威胁。
- **Gateway** — 此 VM 系列防火墙可作为 VNet 网关保护 Azure 虚拟网络 (VNet)中面向 Internet 的部署。此 VM 系列防火墙可保护以 VNet 中服务器为目标的流量，还可保护多层架构中应用程序之间子网间流量免于遭受横向威胁。
- **GlobalProtect** — 支持使用 Azure 基础架构快速、简便地将 VM 系列防火墙部署为 GlobalProtect™，并将网关安全策略扩展到远程用户和设备，不论位置如何。

您可以继续从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）或在 Azure Stack 中部署 VM 系列防火墙，并根据部署需求配置防火墙，或是了解可以用于部署防火墙的 Azure 上的 VM 系列防火墙模板。有关引导的更多信息，请参阅在 Azure 上引导 VM 系列防火墙。

© 2019 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。



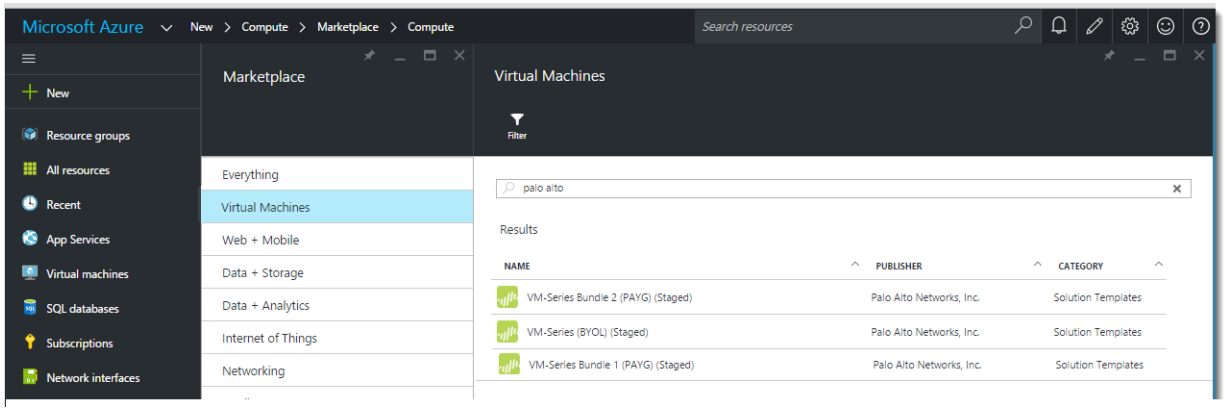
STEP 1 | 设置 Azure 帐户。

1. 如果一个都未就绪，请创建 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。

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，并 **Create**（创建）新的 VM 系列防火墙。

STEP 3 | 部署防火墙。

1. 配置防火墙的基本设置。

© 2019 Palo Alto Networks, Inc.

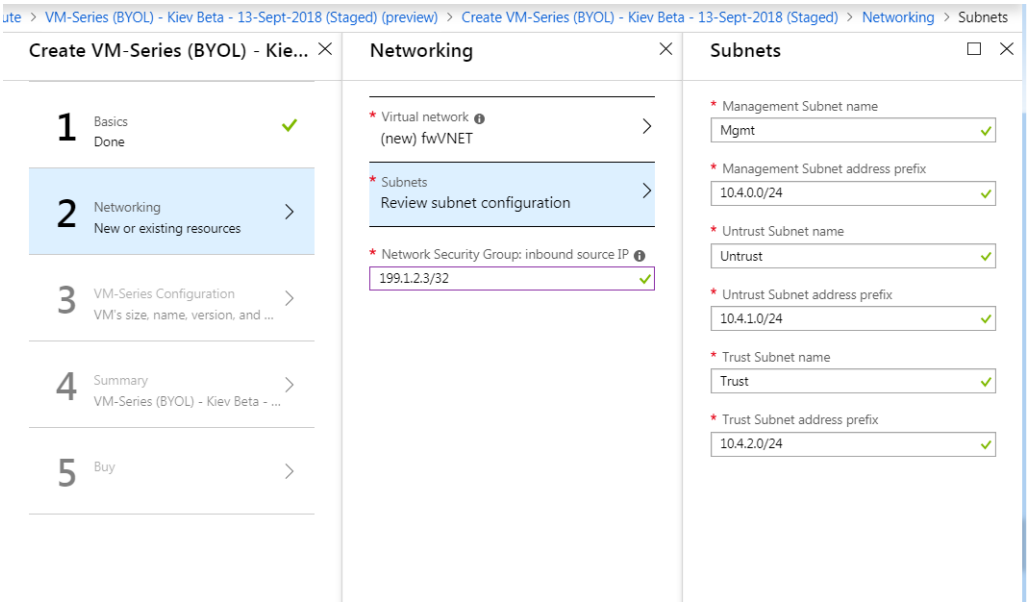
1. 输入防火墙管理员的 **Username**（订阅）。
2. 输入 **Password**（密码）（不超过 31 个字符）或复制粘贴 **SSH public key**（**SSH** 公钥）以确保对防火墙进行管理访问的安全。
3. 选择所需的 Azure **Subscription**（订阅）。
4. 创建新资源组，或选择空的现有资源组。此资源组将用于存放与此部署中的 VM 系列防火墙相关联的所有资源。

   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。
5. 选择 Azure **Location**（位置）。此为当前部署防火墙的区域。

2. 配置联网。
   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。

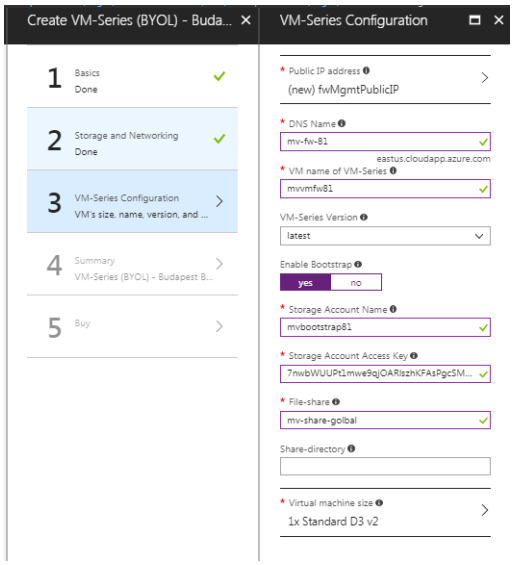


3. 定义防火墙管理访问。
   1. 使用默认变量（新变量 wMgmtPublicIP）将 **Public IP address**（公共 **IP** 地址）分配给防火墙的管理接口 (`eth0`)。

      管理界面不支持 *Azure* 加速网络。

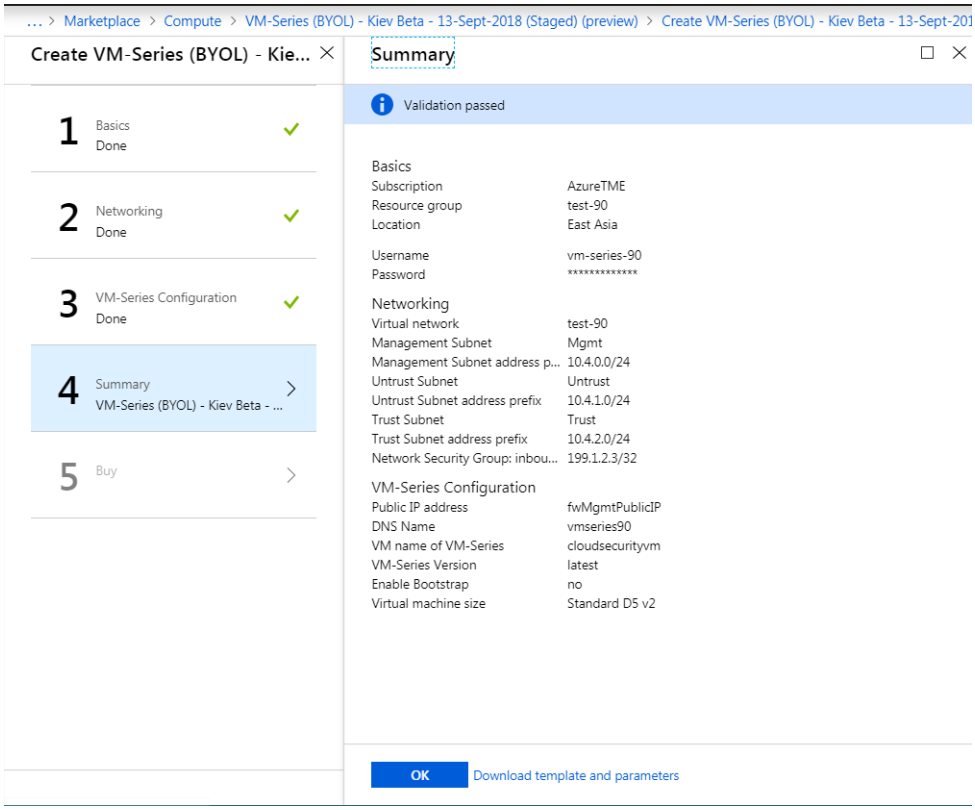
© 2019 Palo Alto Networks, Inc.

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。

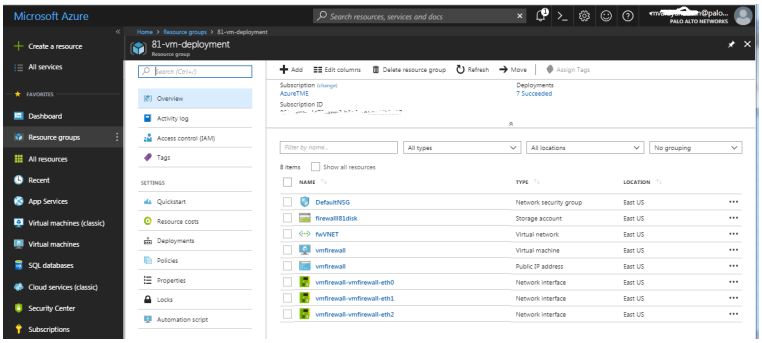


4. 添加信息以在启动时配置防火墙。请参阅在 Azure 上引导 VM 系列防火墙。
   1. 选择 **yes**（是）以 **Enable Bootstrap**（启动应用）。
   2. 输入包含引导数据包的 **Storage Account Name**（存储帐户名称）。
   3. 输入 **Storage Account Access Key**（存储帐户访问密钥）。防火墙需要此访问密钥以对存储帐户进行身份验证，并访问其中的文件。
   4. 添加已上传且用于引导防火墙所需的文件的**File share name**（文件共享名称）。存储帐户必须与防火墙部署在同一区域，必须具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。

© 2019 Palo Alto Networks, Inc.



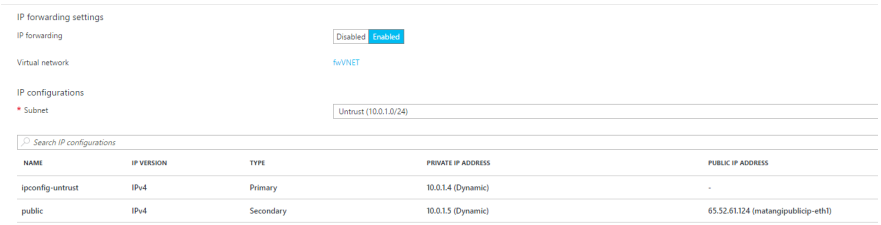
6. 确认您已成功部署 VM 系列防火墙。
   1. 选择 **Dashboard**（仪表盘）> **Resource Groups**（资源组），然后选择资源组。
   2. 关于已成功部署的资源的详细信息状态，请选择您的资源组，并查看 **Overview**（概述）。



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。

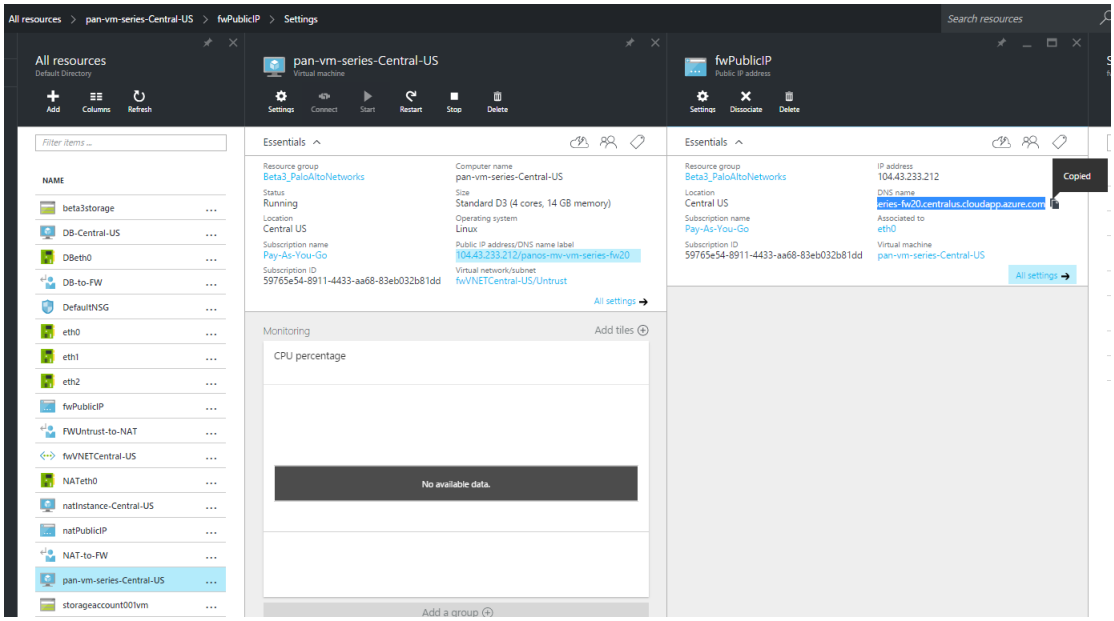
© 2019 Palo Alto Networks, Inc.



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。

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**（使用身份验证代码激活功能）。
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。

© 2019 Palo Alto Networks, Inc.

- **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

© 2019 Palo Alto Networks, Inc.

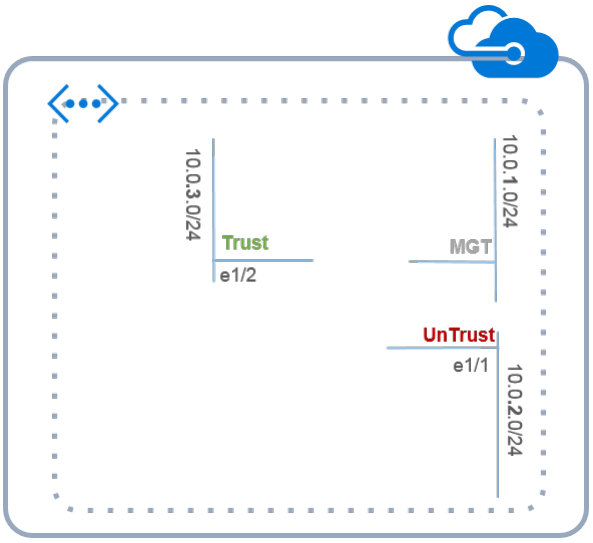
关或 Azure 负载均衡器，或在采用混合部署连接预置型网络与 Azure 云的情况下，此流量也可能来自 Azure VPN 网关。

STEP 10 | 要发布 PAN-OS® 指标到 Azure 应用程序见解，请参阅在 VM 系列防火墙上启用 Azure 应用程序见解。

© 2019 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。



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。

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）。

STEP 3 | 部署防火墙。

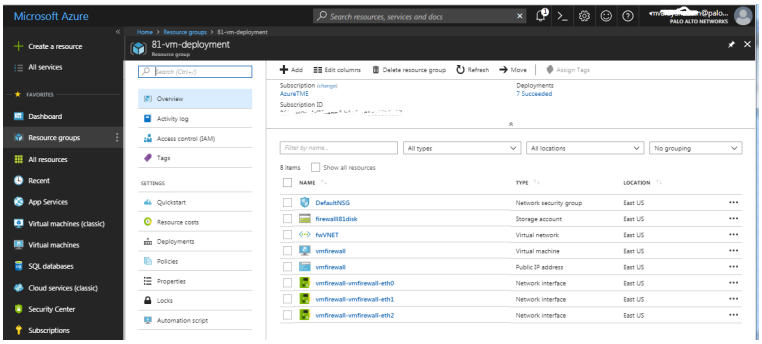
1. 选择所需的 Azure **Subscription**（订阅）。
2. 选择存放与此部署中的 VM 系列防火墙相关联的所有资源的资源组。

© 2019 Palo Alto Networks, Inc.

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。

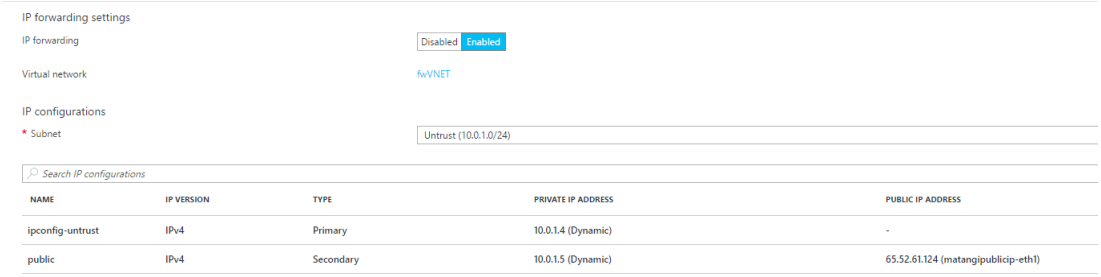
3. 配置防火墙的基本设置。
   1. 输入现有帐户的存储帐户名称或创建一个新帐户。
   2. 输入要将防火墙vhd映像复制并保存到的blob存储容器的名称。
   3. 输入用于访问防火墙管理接口 (eth0) 上公共 IP 地址的 DNS 名称。例如，要访问防火墙的Web界面，必须将输入的前缀与后缀组合在一起 <yourDNSname><china_region>.cloudapp.azure.com。
   4. 输入防火墙管理员的 **Username**（订阅）。
   5. 输入 **Password**（密码）以保护对防火墙的管理访问。
   6. 根据您的需求，选择 Azure 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。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。

© 2019 Palo Alto Networks, Inc.

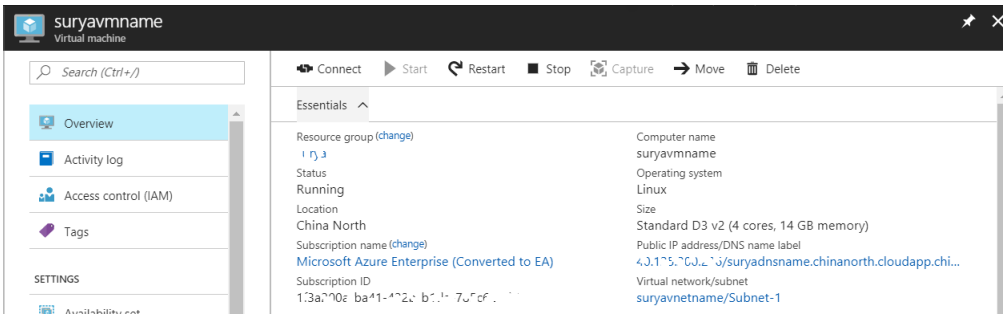


将辅助*IP*地址附加到网络接口时，*VM* 系列防火墙不会自动获取分配给该接口的专用*IP*地址。您将需要使用 *VM* 系列防火墙*Web*界面手动配置专用*IP*地址。请参阅配置数据面板网络接口作为防火墙上的第 3 层接口。

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。

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**（使用身份验证代码激活功能）。
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。

© 2019 Palo Alto Networks, Inc.

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）为第三层（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。

© 2019 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：

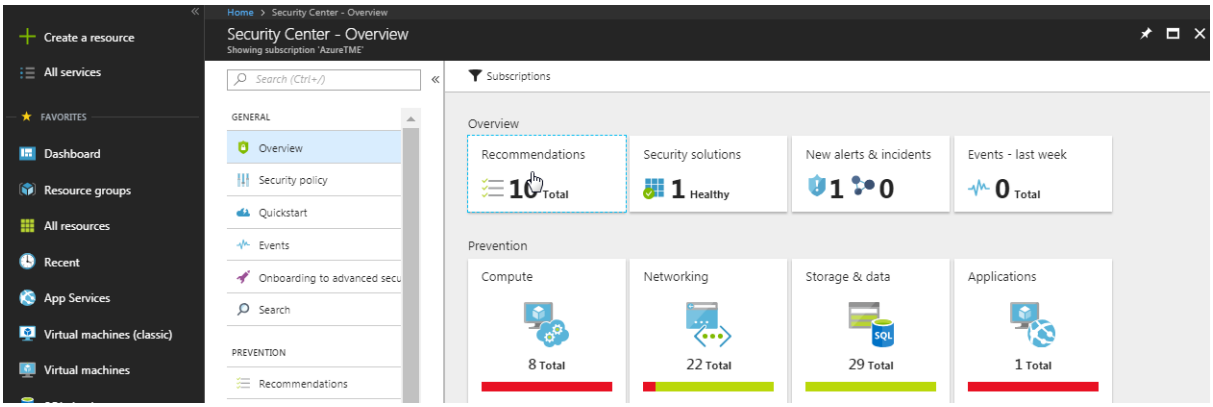
- 基于 Azure 安全中心建议部署 VM 系列防火墙
- 从 Azure 安全中心连接现有 VM 系列防火墙

基于 Azure 安全中心建议部署 VM 系列防火墙。

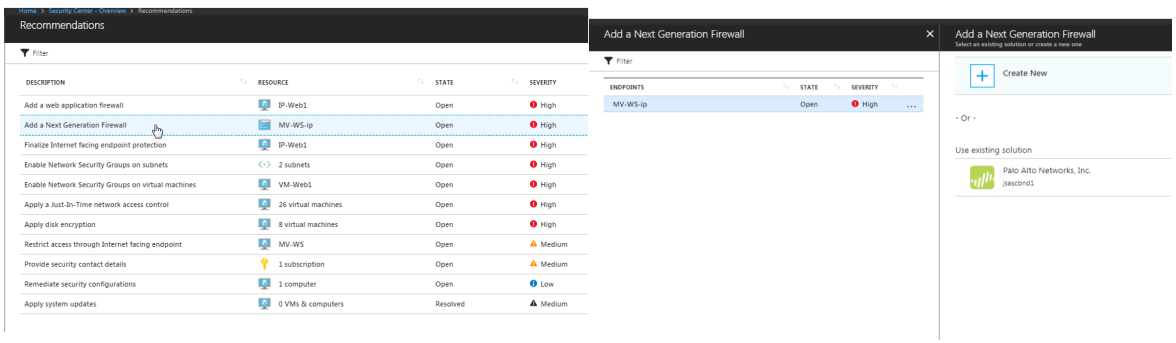
Azure 安全中心扫描您的 Azure 资源，并为需要下一代防火墙的安全工作负载提供建议。此建议显示在仪表盘上，您可以随后从 Azure marketplace 部署新的 VM 系列防火实例，也可以使用 Azure CLI、 Powershell 或 ARM 模板。使用 Azure CLI、Powershell 或 ARM 模板实施的自定义部署的优点在于您可以将 VM 系列防火墙部署在与需要保护的工作负载相同的资源组中。使用 Azure marketplace 部署 VM 系列防火墙时，Azure 要求您仅将防火墙部署在新的资源组或是空的资源组。因此，随后，marketplace 部署要求您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）。



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。

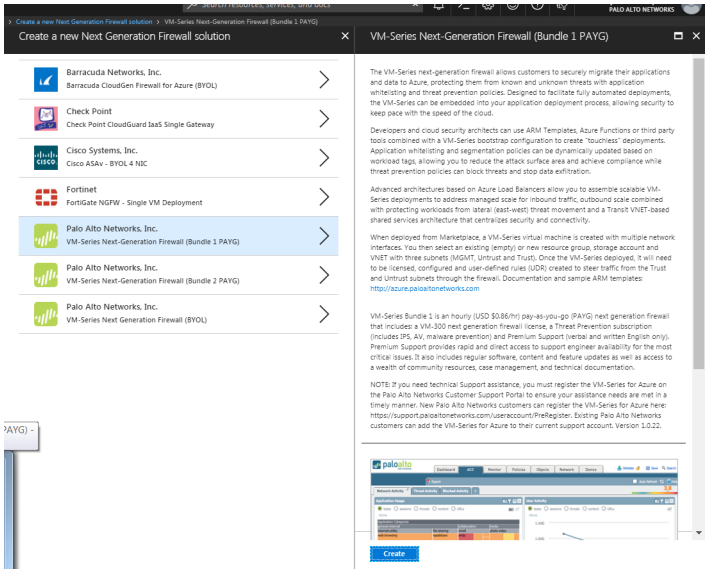


© 2019 Palo Alto Networks, Inc.

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。

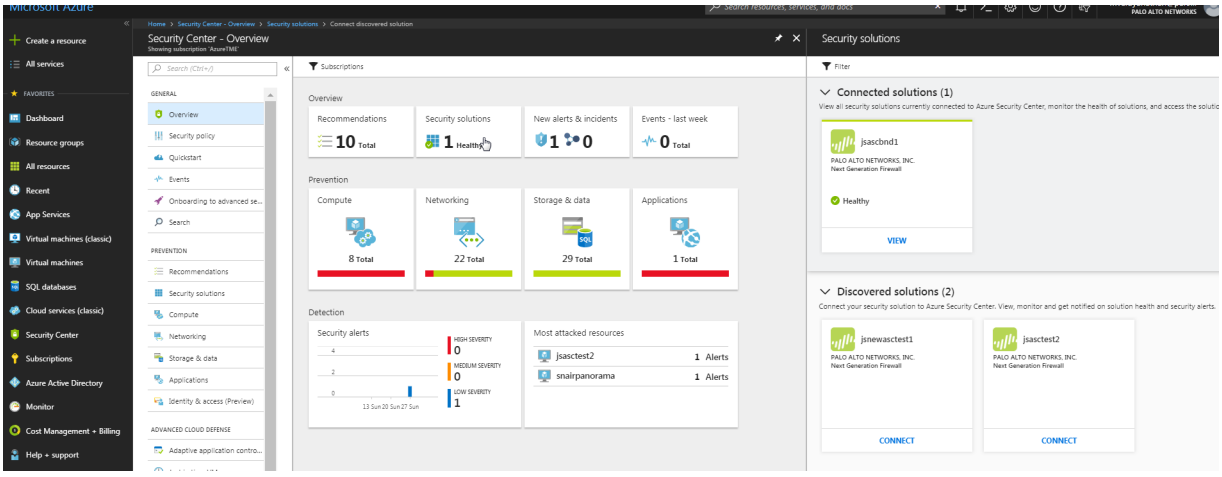


从 Azure 安全中心连接现有 VM 系列防火墙

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。

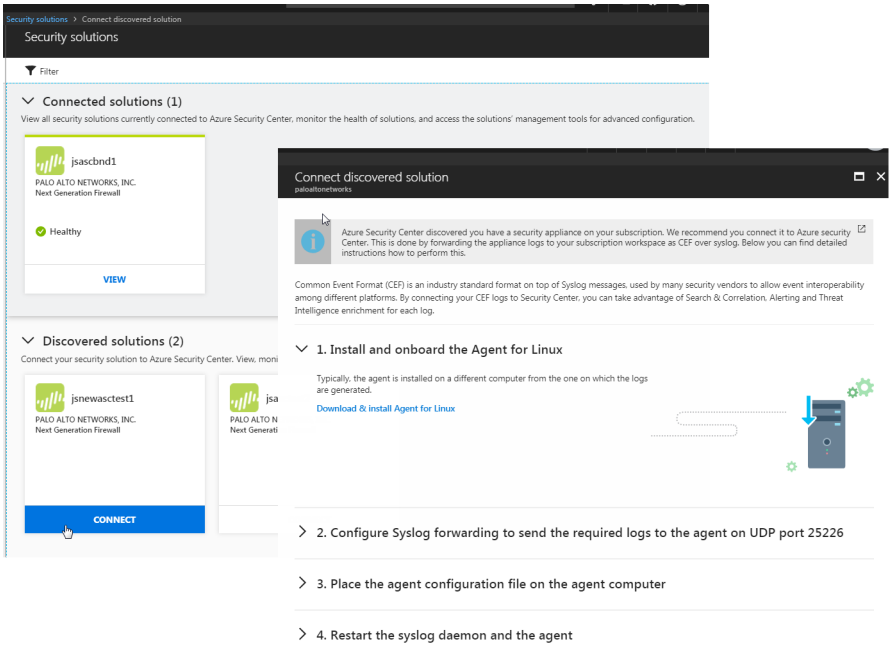
STEP 2 | 选择安全解决方案以查看此 Azure 订阅内所有可用的 VM 系列防火墙。



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）。

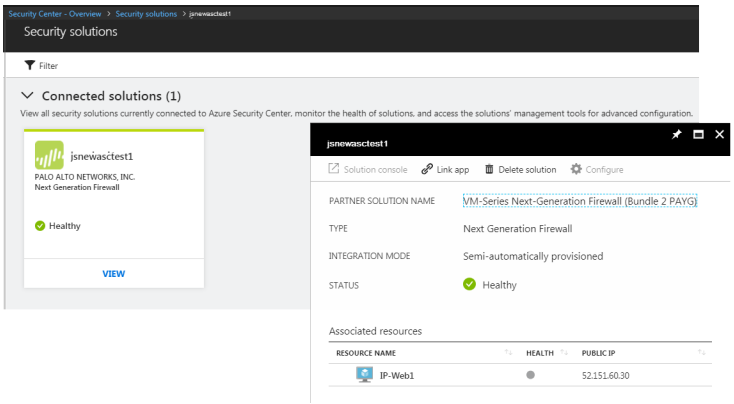
© 2019 Palo Alto Networks, Inc.

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。



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 上将防火墙添加为受管设备。

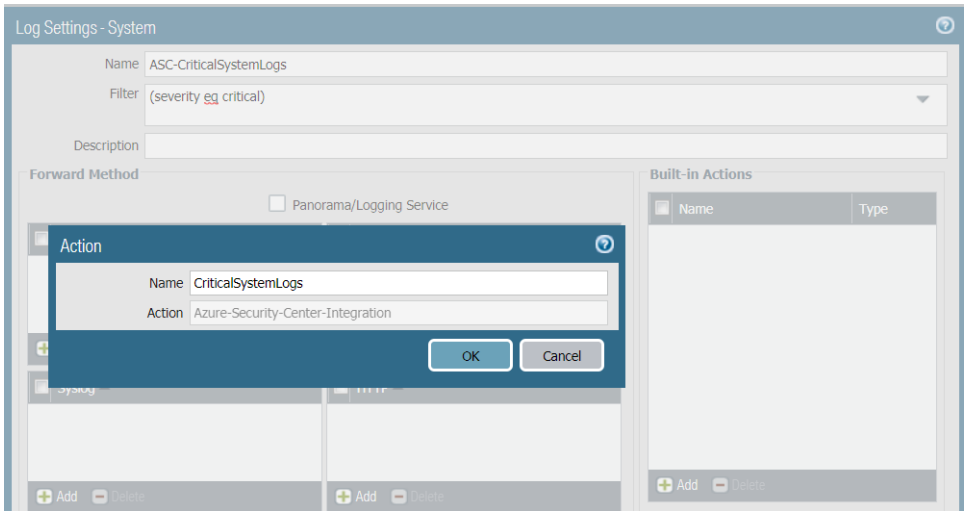
STEP 2 | 在 Panorama 上创建模板和设备组，以将日志转发设置推送到防火墙，从而转发日志到 Azure 安全中心。

© 2019 Palo Alto Networks, Inc.

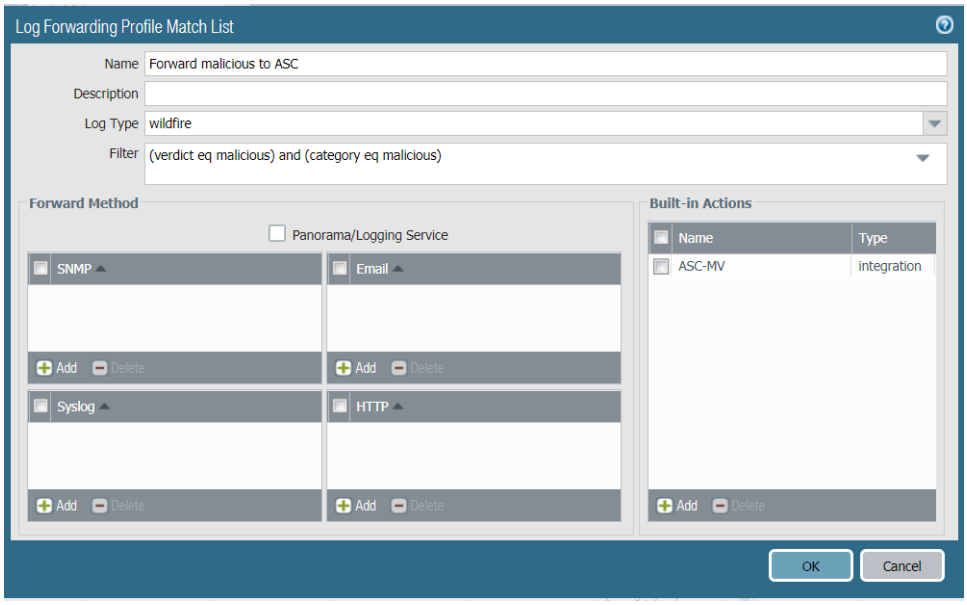
STEP 3 | 指定转发至日志记录服务的日志类型。

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），以启用设备组中的防火墙转发日志到 Azure 安全中心。



© 2019 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。

© 2019 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。

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。

Azure stack 上的 *VM* 系列防火墙不支持引导、*Azure* 应用程序见解或 *Azure* 安全中心集成。

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。

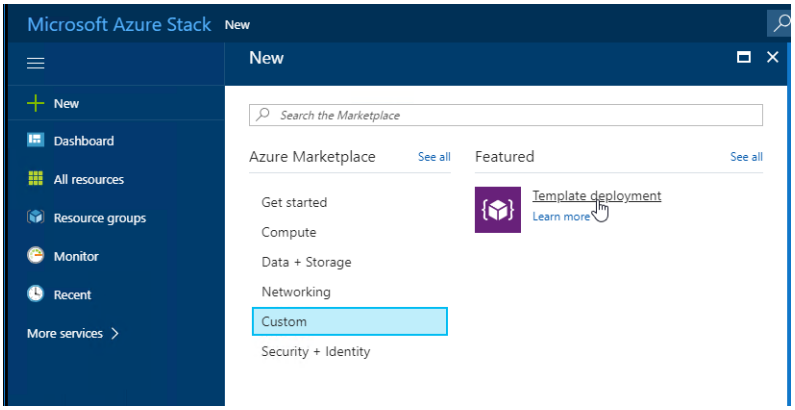
STEP 3 | 部署 VM 系列防火墙。

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。

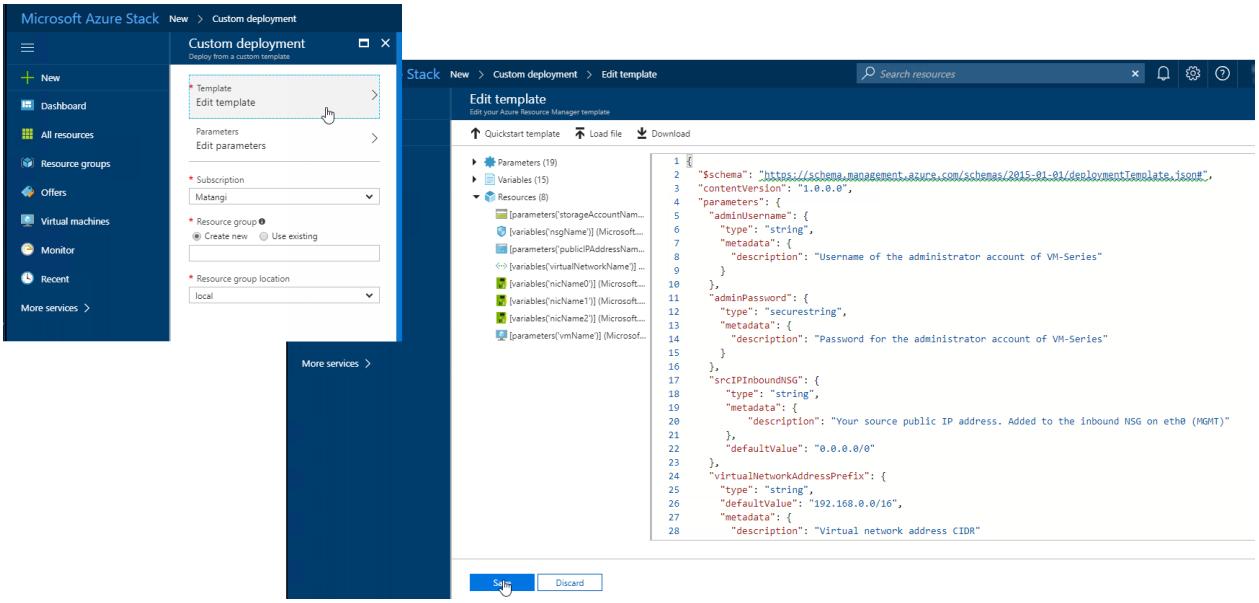
   您可以将防火墙部署到空的现有资源组或新的资源组中。模板中的默认 VNet 是192.168.0.0/16，并且它部署了一个具有三个网络接口的 VM 系列防火墙，即，192.168.0.0/24 子网上的一个管理接口以及 192.168.1.0/24 和 192.168.2.0/24 子网上的两个数据平面接口。可以根据需要自定义这些子网。

   - 登录至 Azure Stack 门户。
   - 选择 **New**（新建）> **Custom**（自定义）> **Template deployment**（模板部署）。

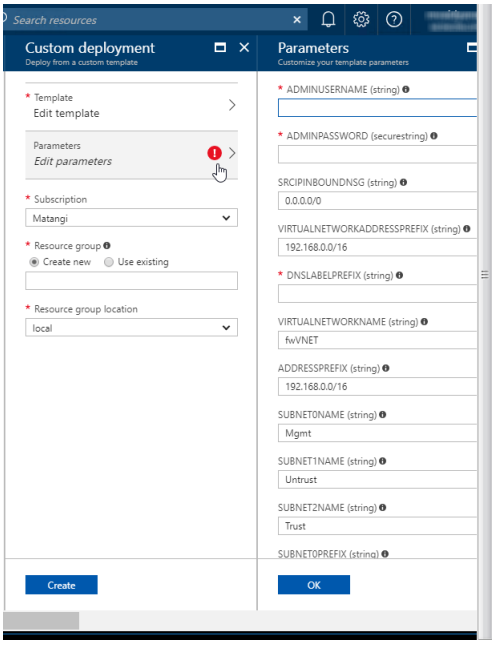


   - **Edit template**（编辑模板），删除模板中所有现存内容，并粘贴先前复制的 JSON 模板内容，然后 **Save**（保持）。

© 2019 Palo Alto Networks, Inc.

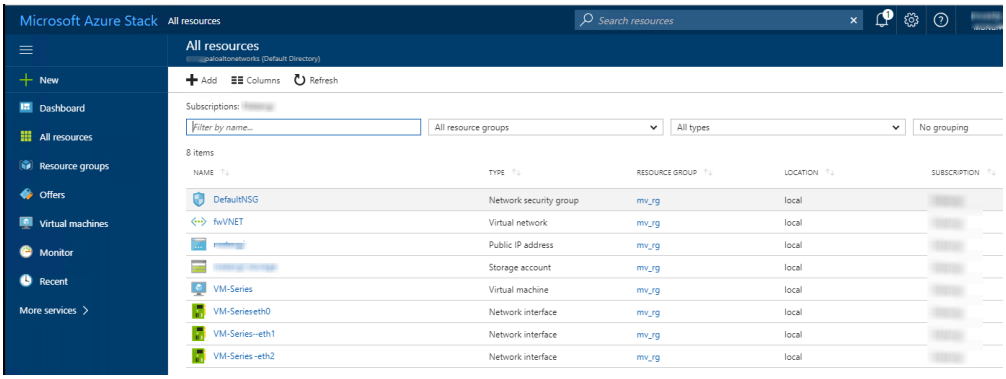


- **Edit parameters**（编辑参数），输入所需参数值，并在必要时修改默认值，然后单击 **OK**（确定）。



- 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）。仪表盘上的新磁贴显示模板部署进度。

© 2019 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**（使用身份验证代码激活功能）。
   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

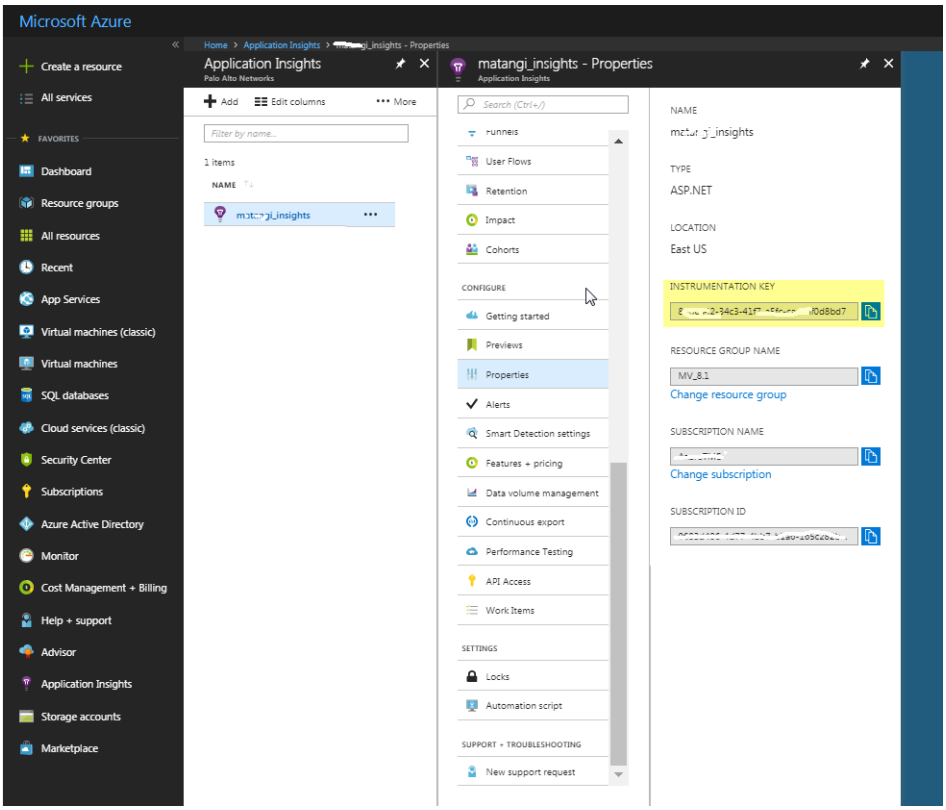
© 2019 Palo Alto Networks, Inc.

在 VM 系列防火墙上启用 Azure 应用程序见解

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 应用程序见解。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 应用程序见解实例以监控防火墙，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应用程序见解实例，并向其发布指标。确保查看 VM 系列在 Azure 上的服务主体权限中服务主体所需的权限。

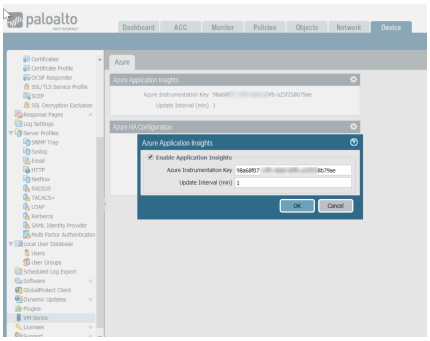


STEP 2 | 启用防火墙以发布指标到您的应用程序见解实例。

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** 应用程序见解），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。

© 2019 Palo Alto Networks, Inc.

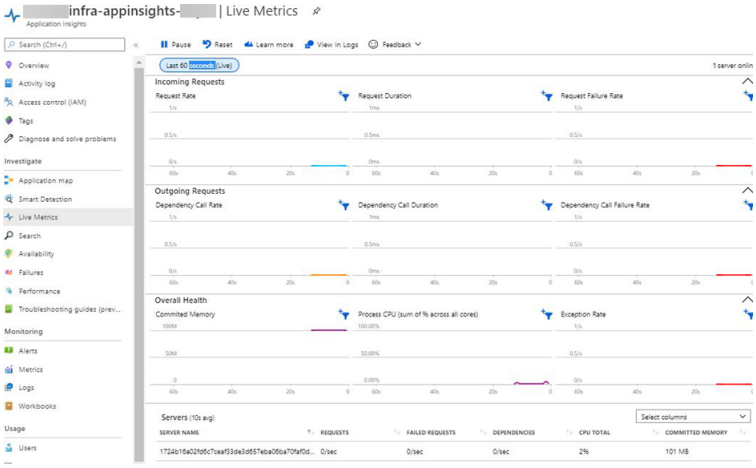


4. **Commit**（提交）更改。

   防火墙会生成一个系统日志，以记录 Azure 应用程序见解验证成功或失败。

STEP 3 | 检验您是否可以查看 Azure 应用程序见解仪表盘上的指标。

1. 在 Azure 门户上选择应用程序见解实例，然后选择 **Overview**（概述）> **Metrics Explorer**（指标浏览器）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。有关浏览应用程序见解上指标的详细信息，请参阅 Microsoft Azure 文档。

© 2019 Palo Alto Networks, Inc.

Azure 上的 VM 监控

您可以通过 Microsoft® Azure® 上的 VM 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。要从启用此功能，必须在 Panorama 上安装 Azure 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 VM 信息推送或分发到 Palo Alto Networks® 防火墙。

- 关于 Azure 上的 VM 监控
- 在 Panorama 上设置用于 VM 监控的 Azure 插件
- 使用 Azure 上 Panorama 插件监控的属性

关于 Azure 上的 VM 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 VM 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 VM 监控的 Azure 插件

要找到组织在 Azure 云中部署的所有虚拟机工作负载，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 VM 信息的监控定义。Panorama 检索 VM 的主要专有 IP 地址（即，停止和运行）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 上的受管设备，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 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。

Azure 插件专用于监控 *Azure* 公共云上的 *VM*。版本 *1.0* 不支持 *Azure Government* 或 *Azure China*。

- 规划采用 Azure 插件进行的 VM 监控列表
- 安装 Azure 插件
- 配置用于 VM 监控的 Azure 插件

规划采用 *Azure* 插件进行的 *VM* 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。

© 2019 Palo Alto Networks, Inc.

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。如果您没有所需权限，请要求 Azure AD 或订阅管理员创建一个具有读取器 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。
- 如果使用适用于 Azure 和 AWS 的 Panorama 插件，则无法使用来自两种环境的标记定位相同的防火墙或虚拟系统。确保您添加到用于 AWS 和 Azure 的监控定义的设备组无重叠。
- 如果使用适用于 Azure 和 AWS 的 Panorama 插件，则无法使用来自两种环境的标记定位相同的防火墙或虚拟系统。确保您添加到用于 AWS 和 Azure 的监控定义的设备组无重叠。
- 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 和受管防火墙的要求：
  - 最低系统要求（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 上添加防火墙作为受管设备，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。
  - 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 对等设备上安装相同版本的 Azure 插件。

      您只能在 *Panorama* 主动对等设备上配置 *Azure* 插件。提交时，配置同步到 *Panorama* 被动对等设备。仅 *Panorama* 主动对等设备质询用于 *VM* 监控的 *Azure* 订阅。

安装 *Azure* 插件

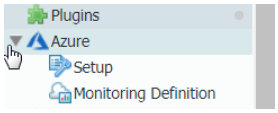
要开始监控 Azure 上的 VM 监控，则需要在 Panorama 上下载并安装 Azure 插件。如果拥有 Panorama HA 配置，则在每个 Panorama 对等设备上重复此安装过程。

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。

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。

© 2019 Palo Alto Networks, Inc.

选择 **Panorama** > **Setup**（设置） > **Operations**（操作） > **Reboot Panorama**（重新启动 **Panorama**）

配置用于 *VM* 监控的 *Azure* 插件

要开始监控 Azure 公共云部署中的虚拟机，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。

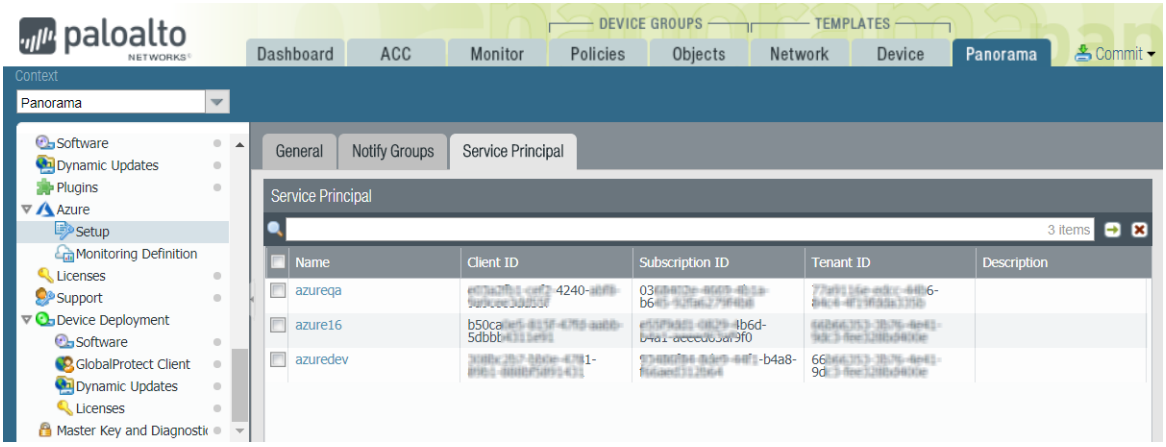
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Azure 上设置用于启动 VM 监控的以下对象。

- 添加服务主体。

  服务主体是您在 Azure 门户上创建的服务账户。此账户可添加到 Azure AD，且有一定的权限，可访问和监控 Azure 订阅中的资源。

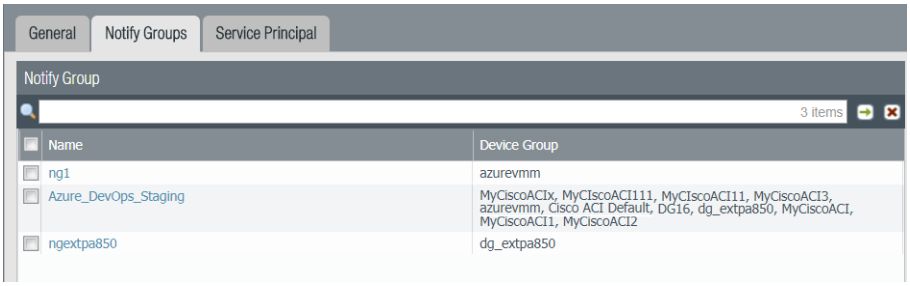
  1. 选择 **Panorama** > **Plugins**（插件） > **Azure** > **Setup**（设置） > **Service Principal**（服务主体） > **Add**（添加）。



  2. 输入标识服务账户的 **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）。



© 2019 Palo Alto Networks, Inc.

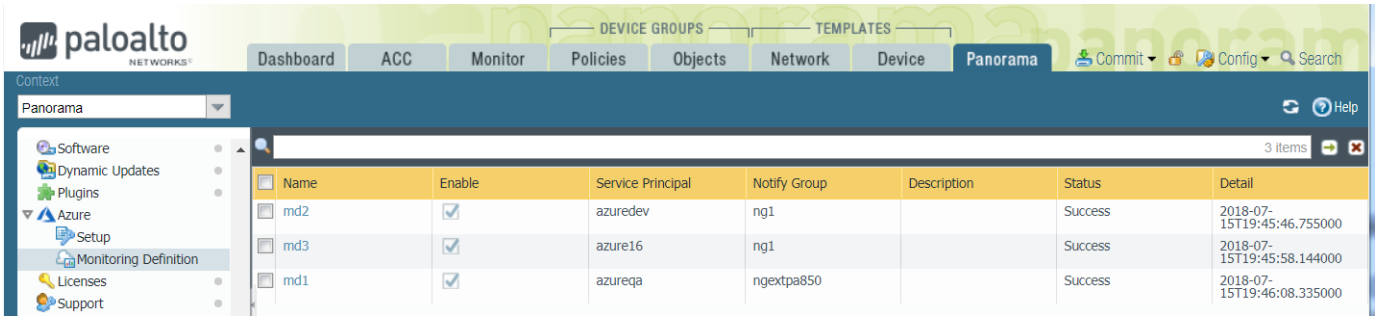
2. 输入用于标识 Panorama 推送检索到的 VM 信息到其的防火墙组的 **Name**（名称），也可选择输入 **Description**（说明）。
3. 选择作为防火墙或虚拟系统组的 **Device Groups**（设备组），以便 Panorama 将其从 Azure 订阅检索到的 VM 信息（IP 地址到标记映射）推送到该组。这些防火墙可使用此更新确定构成策略中所引用动态地址组的成员的最新列表。

   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 VM 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。

STEP 3 | 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） > **Azure** > **Monitoring Definition**（监控定义）以 **Add**（添加）新的定义。
- 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 以生成 Azure Bearer 令牌。此令牌可在 API 调用标头中使用，以收集工作负载上的信息。

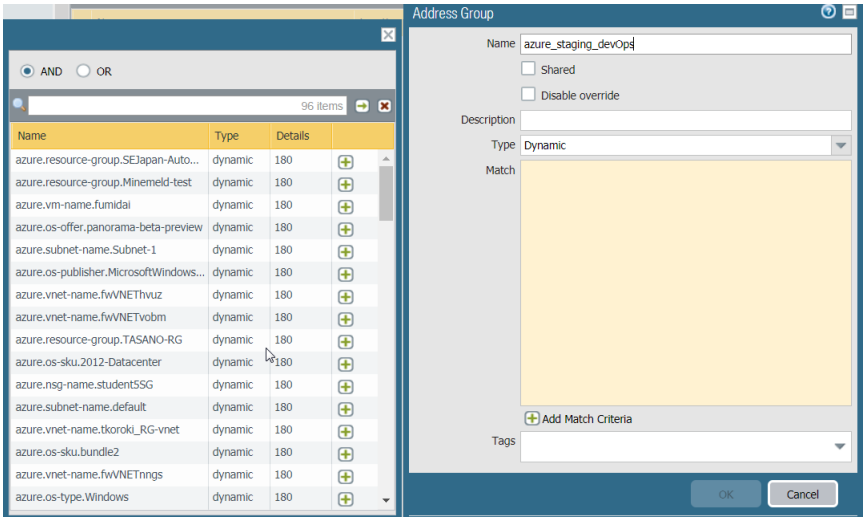
STEP 4 | 在 Panorama 上 **Commit**（提交）更改。

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。

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。

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。

© 2019 Palo Alto Networks, Inc.



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

```
Unable to process subscriptions after HA switch-over; user-intervention required.
```

看到此错误后，必须登录到 *Panorama* 修复此问题。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* 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。

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 "。

受监控的属性	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

© 2019 Palo Alto Networks, Inc.

受监控的属性	示例
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

© 2019 Palo Alto Networks, Inc.

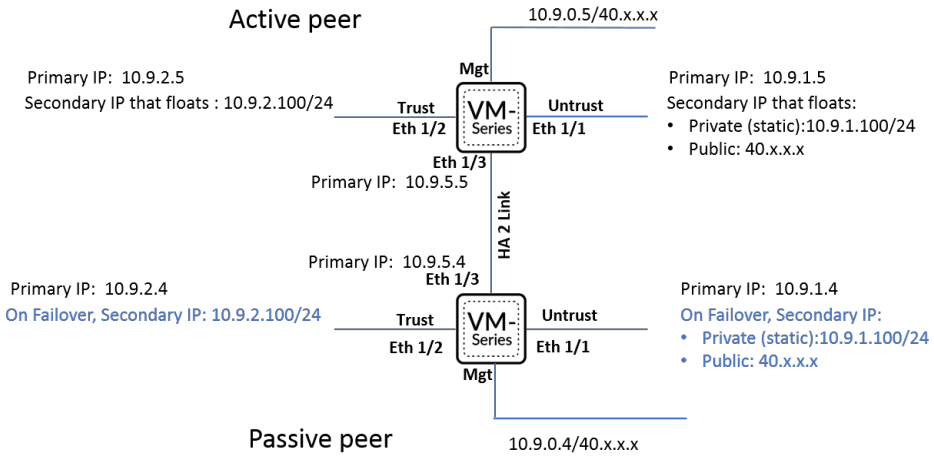
在 Azure 上设置主动/被动 HA

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互联网的应用程序并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 基础架构中并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。

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。除了浮动 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。



- 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 或订阅管理员创建一个具有VM 系列在 Azure 上的服务主体权限中指定的权限的服务主体。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 关联的应用程序 ID（**Azure Active Directory** > **App registrations**（应用程序注册），选择应用程序并复制 ID）。

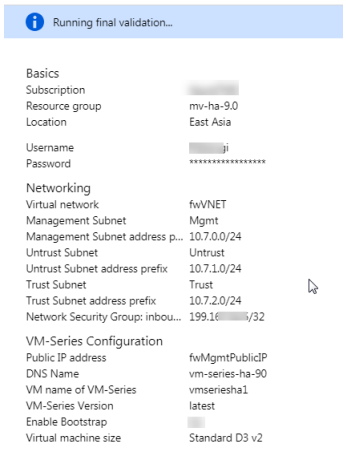
© 2019 Palo Alto Networks, Inc.

- 租户 **ID** — 目录 ID（Azure 门户网站上的 **Azure Active Directory** > **Properties**（属性） > **Directory ID**（目录 **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。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。

- 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。

© 2019 Palo Alto Networks, Inc.

- **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。
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*

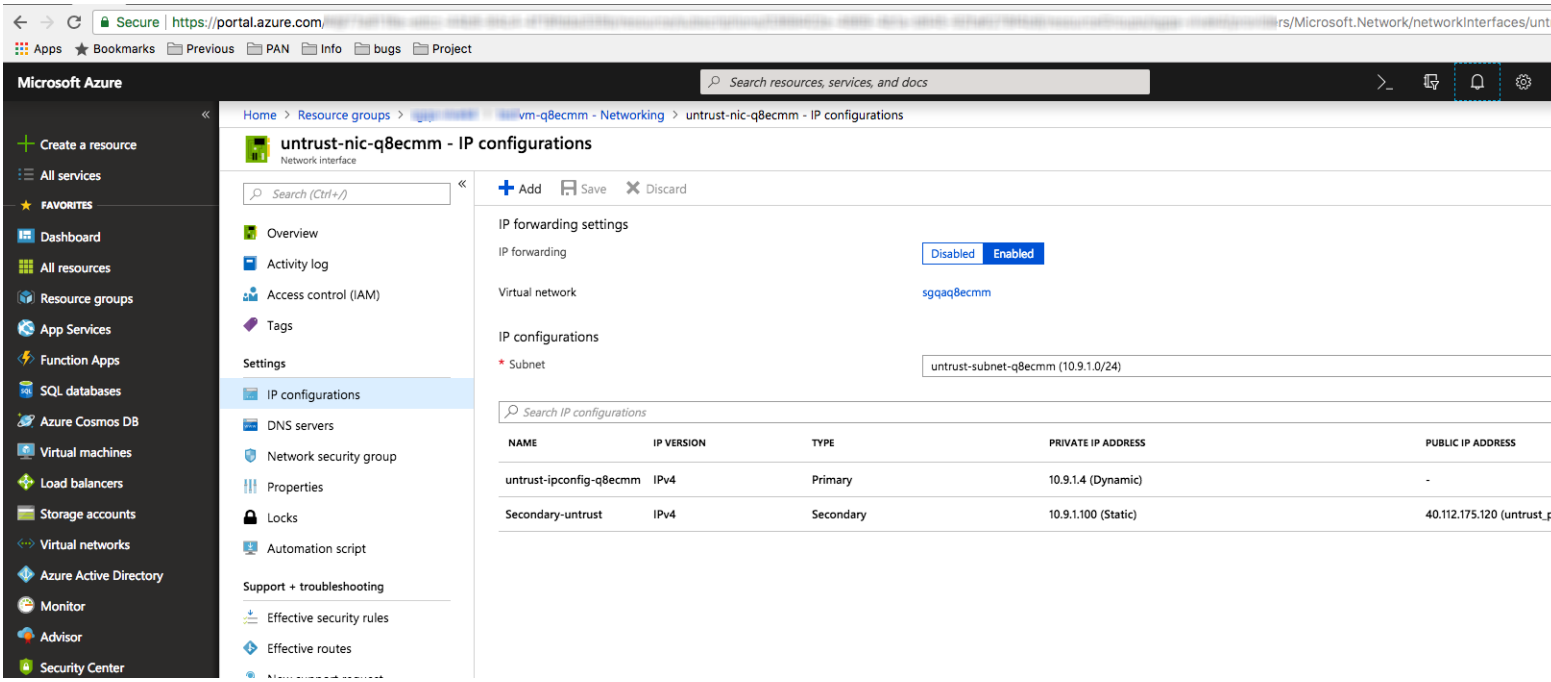
在此工作流程中，您使用 Azure Marketplace 中的 VM 系列防火墙解决方案模板部署 VM 系列防火墙的第一个实例，使用示例 GitHub 模板部署第二个防火墙实例。

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。

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。

© 2019 Palo Alto Networks, Inc.

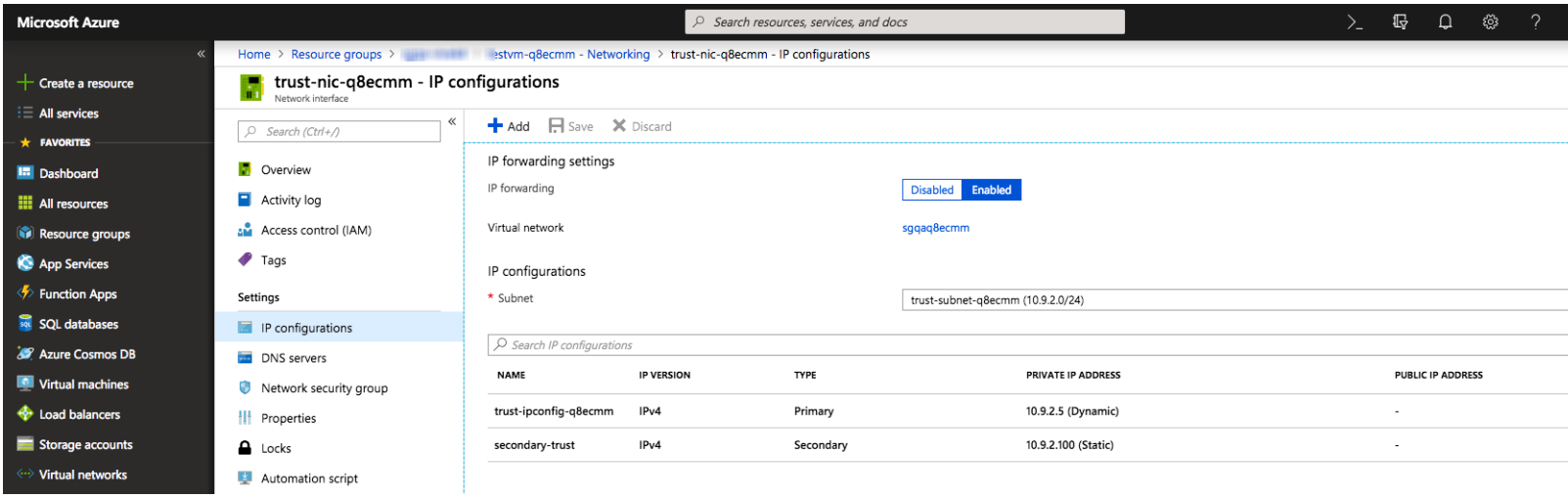
1. 将辅助 IP 配置添加到防火墙上的不可信接口。



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。



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：

© 2019 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

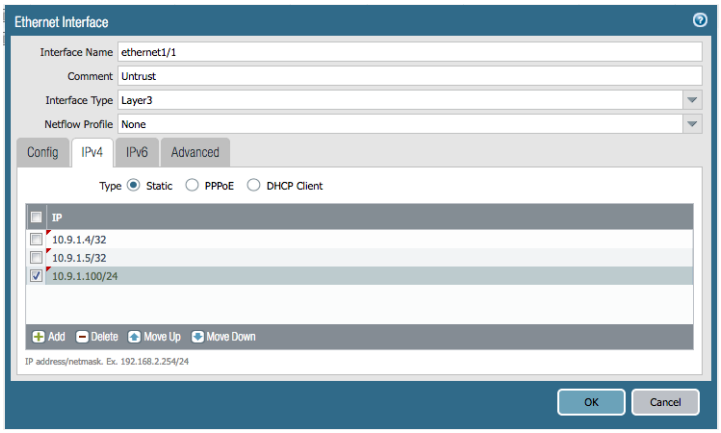
Name	Address range	Virtual network	Security group
frontend-server	10.9.3.0/24	vmq	-

STEP 2 | 配置防火墙上的接口。

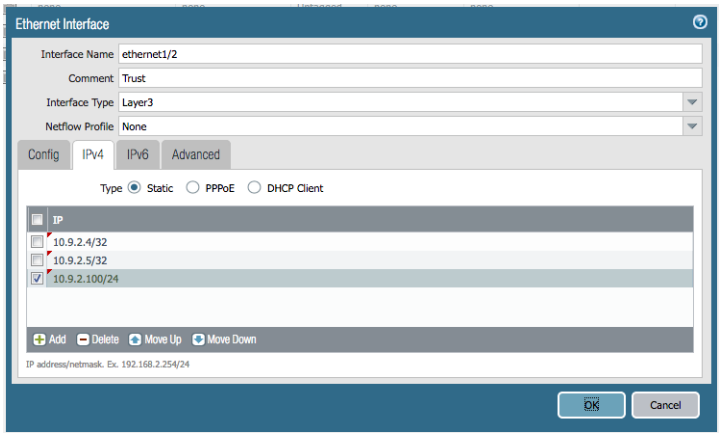
在部署和设置被动 HA 对等之前，请在主动 HA 对等上完成这些步骤。

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：

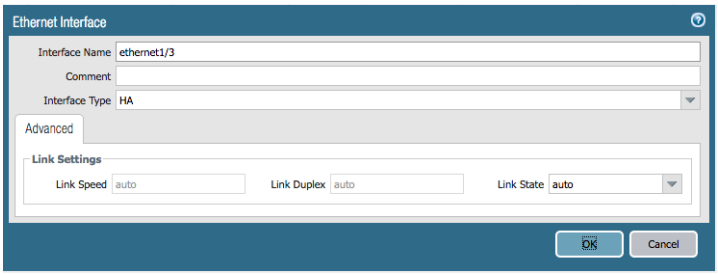


© 2019 Palo Alto Networks, Inc.



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。

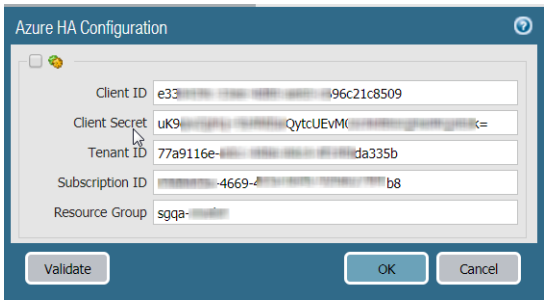


STEP 3 | 配置 VM 系列插件以对已部署防火墙的 Azure 资源组进行身份验证。

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。

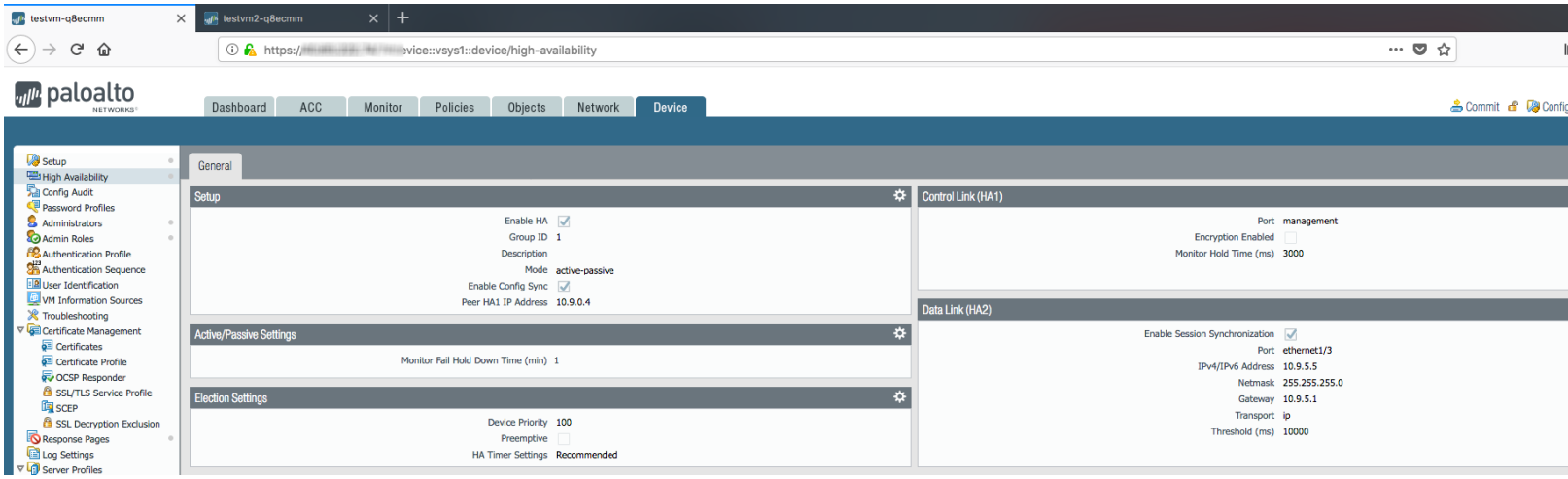
1. 选择 **Device**（设备）> **VM-Series**（**VM** 系列），以便在防火墙插件和 Azure 资源之间启用编程访问。



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. 输入想要监控的 Azure 订阅的 **Subscription ID**（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，以及 VM 系列插件是否可以与使用 API 的 Azure 资源成功通信。

STEP 4 | 启用 HA。

© 2019 Palo Alto Networks, Inc.



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。

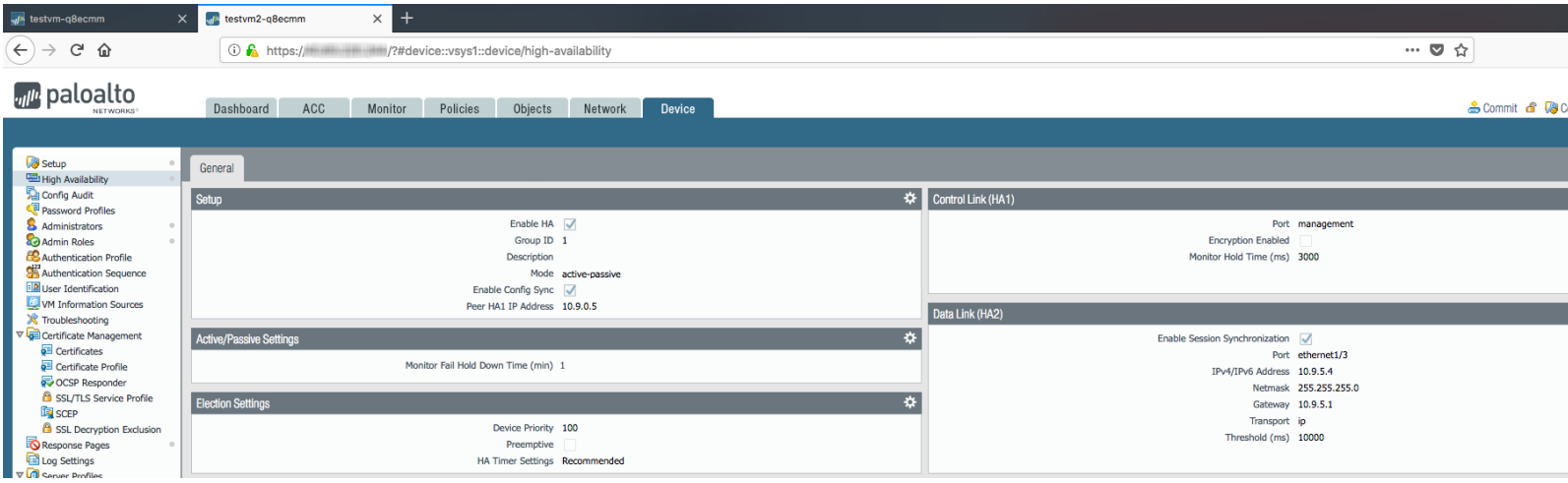
STEP 5 | **Commit**（提交）更改。

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）。

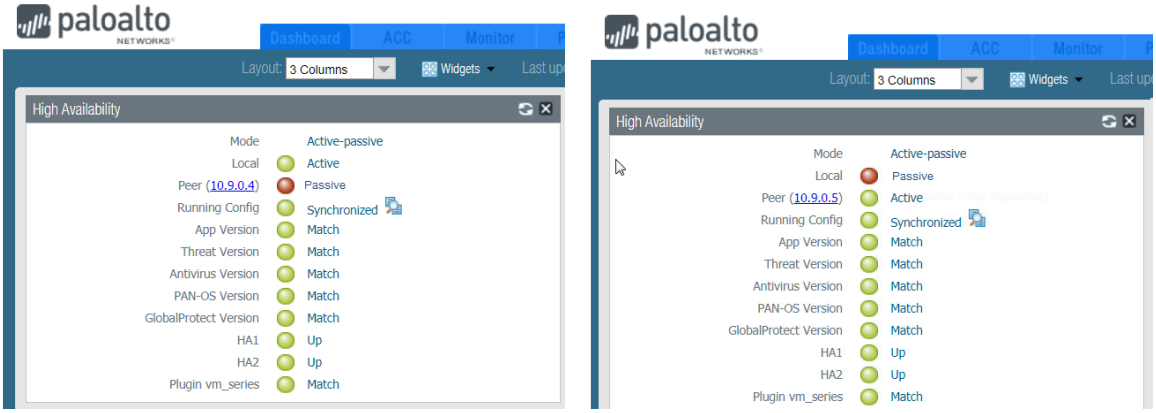
     确保将以下输入与已部署的防火墙实例的输入相匹配 — Azure 订阅、资源组的名称、资源组的位置，要将防火墙部署到的现有 VNet 的名称，VNet CIDR、子网名称、子网 CIDR，并启动管理、可信和不可信子网的 IP 地址。
2. 重复步骤 1 和步骤 2 以设置接口，并将防火墙配置为被动 HA 对等。
3. 跳过步骤 3 并完成启用 HA（步骤 5）。根据情况在步骤 4 中修改此被动 HA 对等的 IP 地址。

© 2019 Palo Alto Networks, Inc.



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**（仪表板），并查看高可用性小部件。
2. 在主动防火墙上，单击 **Sync to peer**（同步到对等）链接。
3. 确认防火墙已配对并同步，如下所示：



- 在被动防火墙上：本地防火墙的状态应显示 **Passive**（被动），并且 **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。

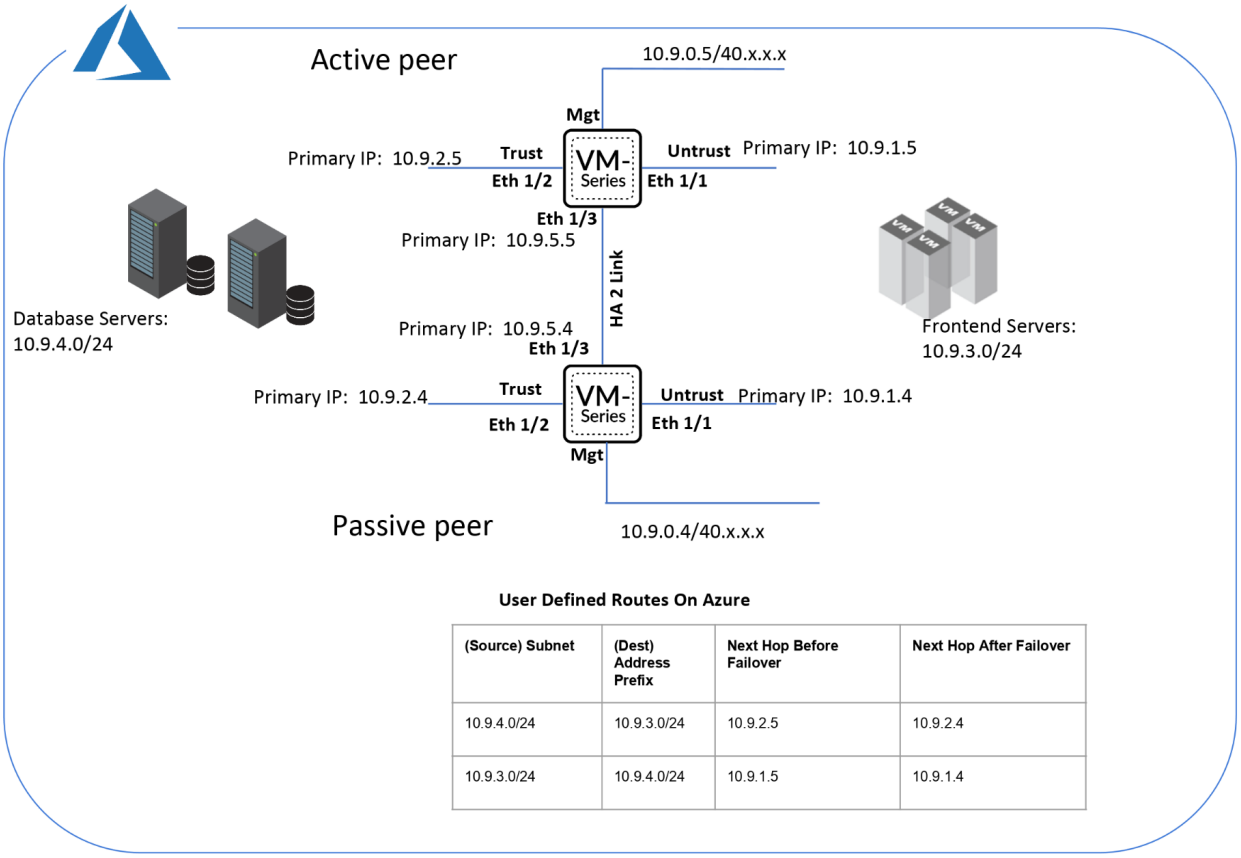
   选择 **Device**（设备）> **VM-Series**（**VM** 系列），并验证是否可以查看已在被动对等上忽略配置的 Azure HA 配置。

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。

© 2019 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

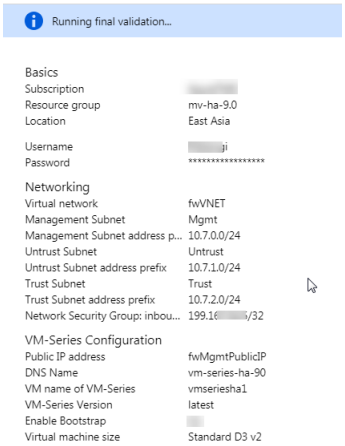
收集在 Azure 上的 VM 系列防火墙上配置 HA 的以下详细信息。

- 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 或订阅管理员创建一个具有VM 系列在 Azure 上的服务主体权限中指定的权限的服务主体。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 关联的应用程序 ID（**Azure Active Directory** > **App registrations**（应用程序注册），选择应用程序并复制 ID）。
    - 租户 **ID** — 目录 ID（Azure 门户网站上的 **Azure Active Directory** > **Properties**（属性） > **Directory ID**（目录 **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。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。

© 2019 Palo Alto Networks, Inc.

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。

- 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

© 2019 Palo Alto Networks, Inc.

接口	主动防火墙对等	被动防火墙对等	说明
			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。

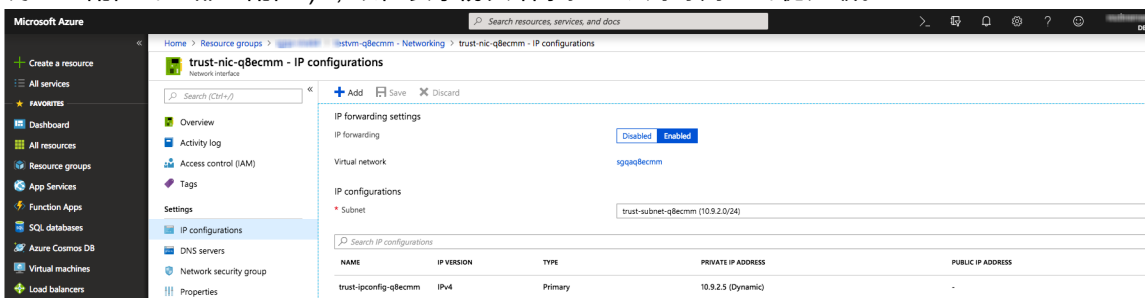
与在 *HA* 配置中设置 *VM* 系列防火墙所需的 *Active Directory* 应用程序关联的身份验证密钥（客户端密钥）使用防火墙和 *Panorama* 上使用 *VM* 系列插件版本 *1.0.9* 进行加密。由于该密钥在 *VM* 系列插件版本 *1.0.9* 中加密，因此，必须在 *Panorama* 和托管 *VM* 系列防火墙上安装相同版本的插件，以便从 *Panorama* 集中管理防火墙。

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。

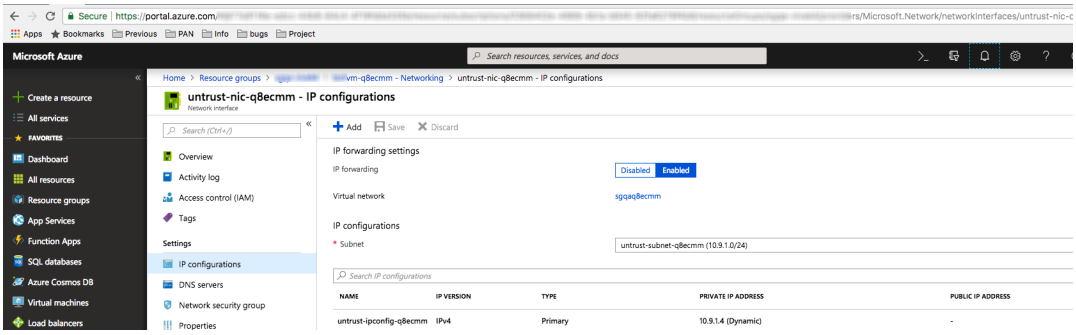
为了保护 Azure VNet 中的东向西流量，您只需要可信和不可信防火墙接口的主要 IP 地址。发生故障转移时，UDR 会更改，并且路由会指向转换为主动状态的对等的主要 IP 地址。

1. 将主要 IP 配置添加到主动防火墙对等的可信接口。

   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. 将主要 IP 配置添加到主动防火墙对等的不可信接口。

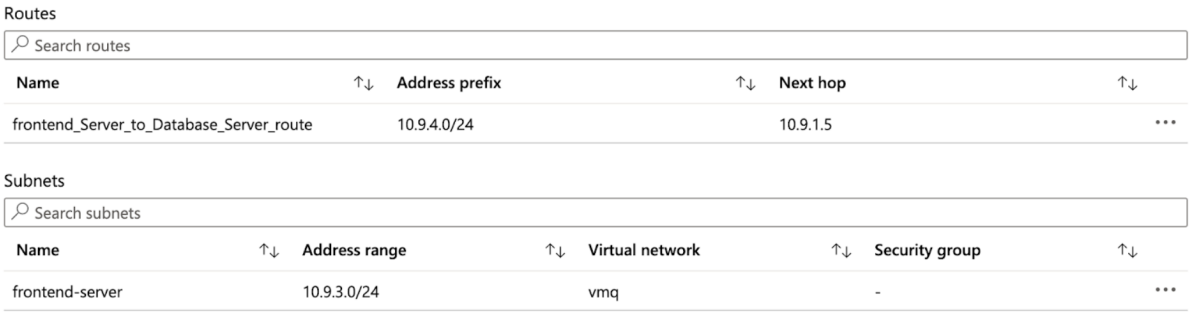


3. 为防火墙 HA 对等之间的 HA2 通信附加网络接口。
   1. 在虚拟网络中添加子网。
   2. 创建和连接防火墙的网络接口。
4. 在 Azure 上设置路由表。

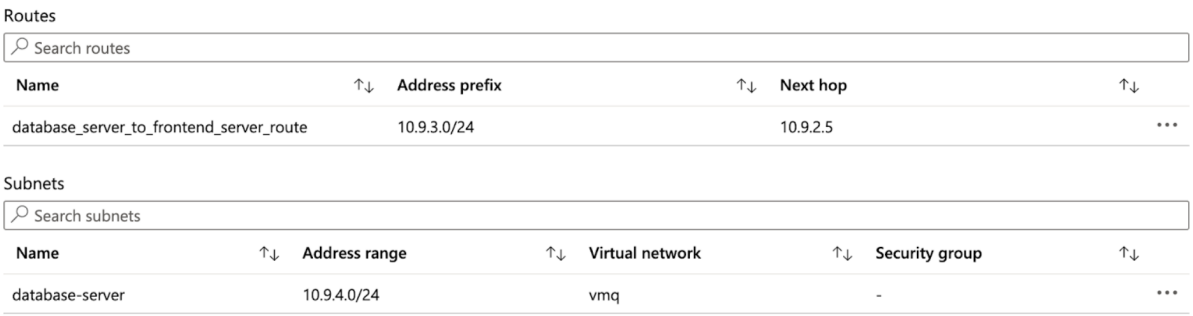
   创建到主动防火墙对等的可信和不可信接口的主要 IP 地址的下一个跃点的路由。

© 2019 Palo Alto Networks, Inc.

Example with Frontend Server to Database Server Route :



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。

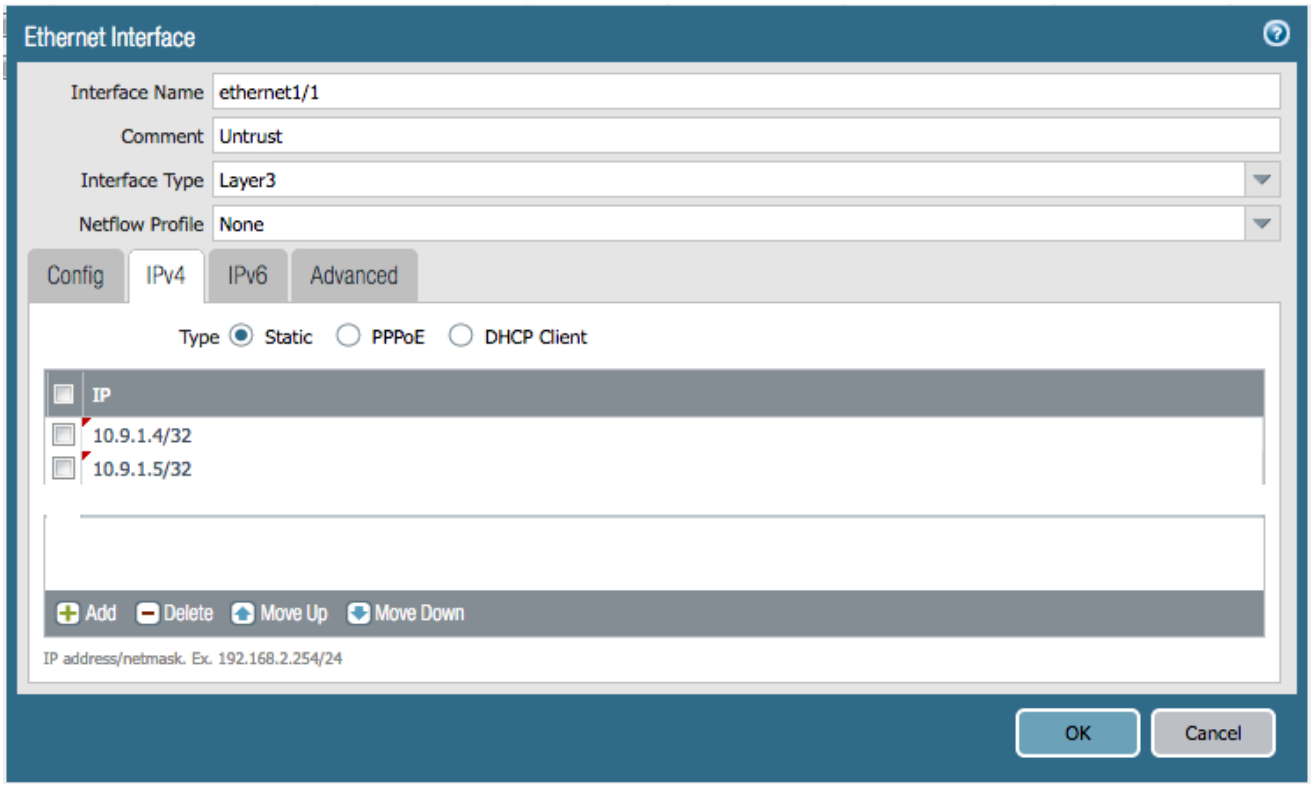
STEP 2 | 配置防火墙上的接口。

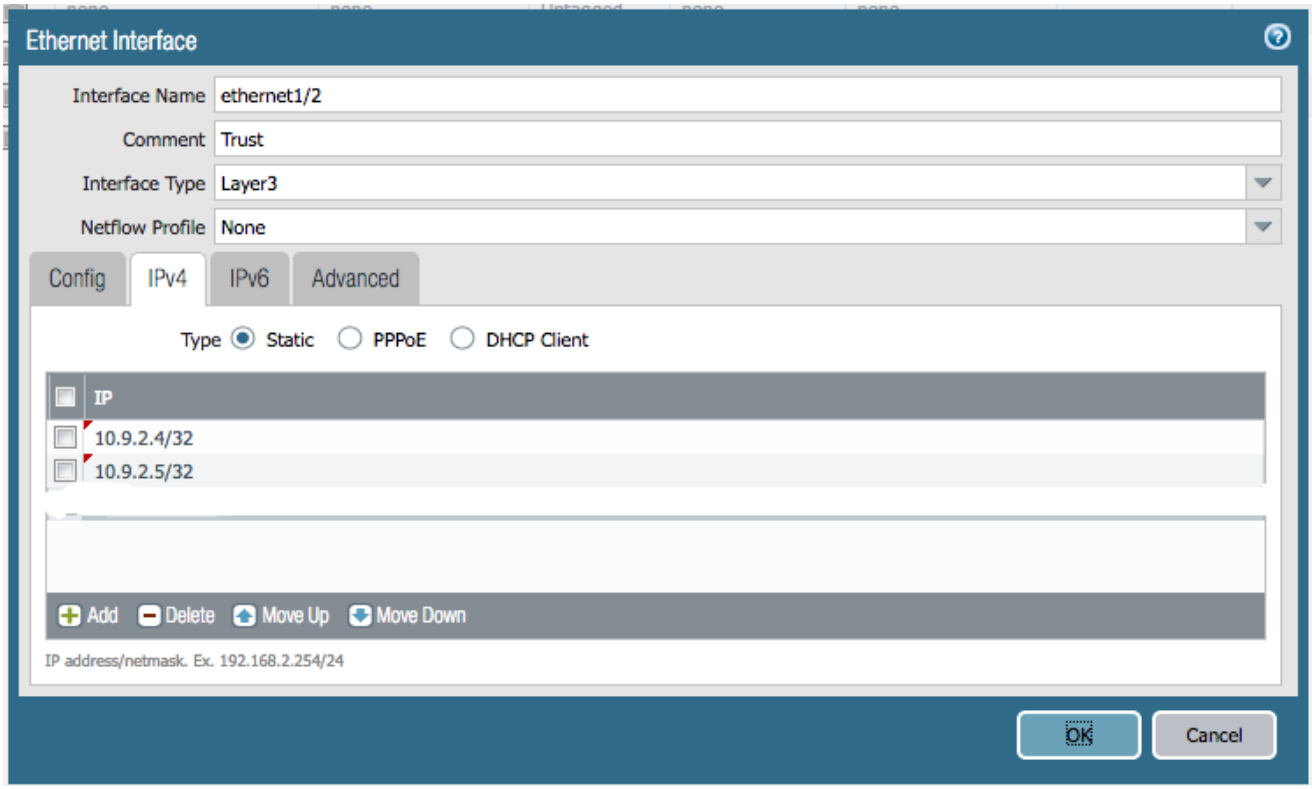
在部署和设置被动 HA 对等之前，请在主动 HA 对等上完成这些步骤。

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：

© 2019 Palo Alto Networks, Inc.

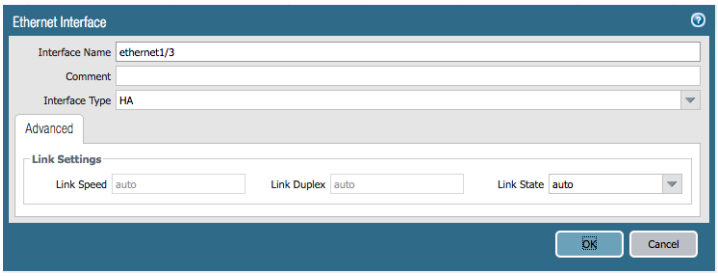




3. 将 ethernet 1/3 配置为 HA 接口。

   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。

© 2019 Palo Alto Networks, Inc.

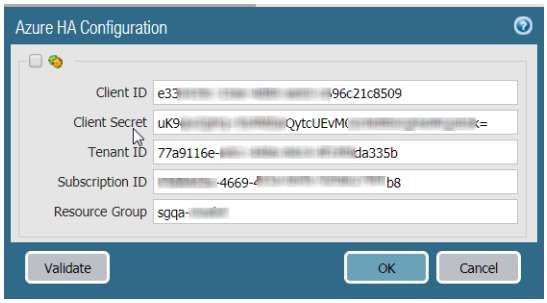


STEP 3 | 配置 VM 系列插件以对已部署防火墙的 Azure 资源组进行身份验证。

在 VM 系列插件上设置 Azure HA 配置。

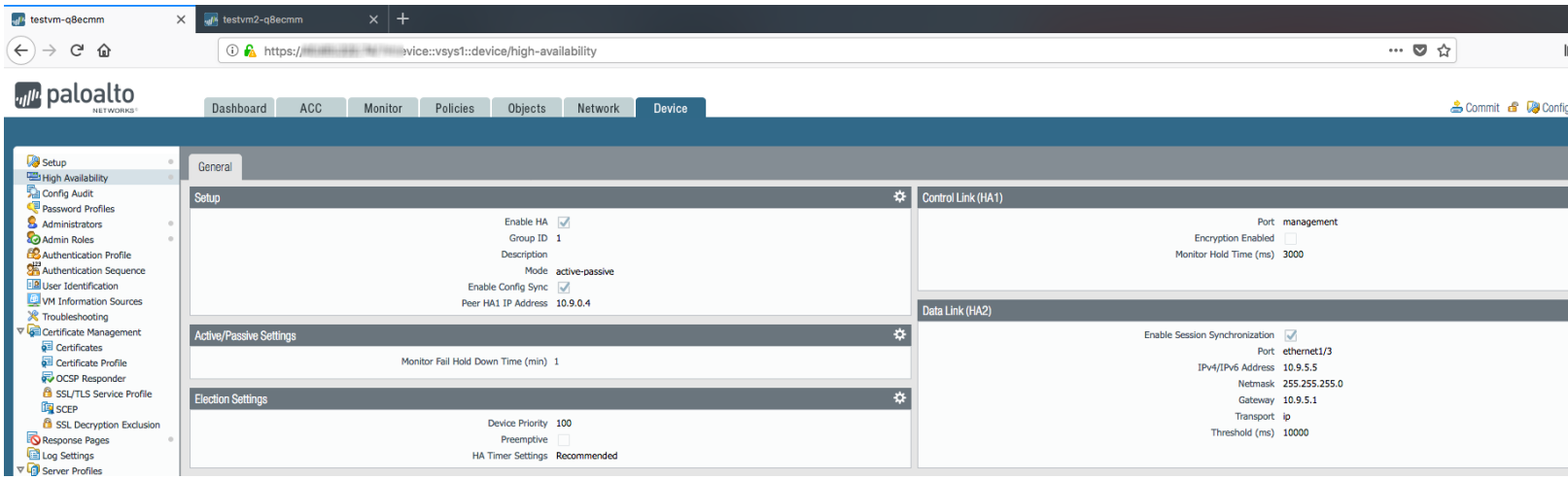
要加密客户端密钥，请使用 VM 系列插件版本 1.0.4 或更高版本。如果使用 Panorama 管理防火墙，则必须安装 VM 系列插件版本 1.0.4 或更高版本。

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. 输入想要监控的 Azure 订阅的 **Subscription ID**（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，以及 VM 系列插件是否可以与使用 API 的 Azure 资源成功通信。

STEP 4 | 启用 HA。



1. 选择 **Device**（设备）> **Setup**（设置）> **HA**。

© 2019 Palo Alto Networks, Inc.

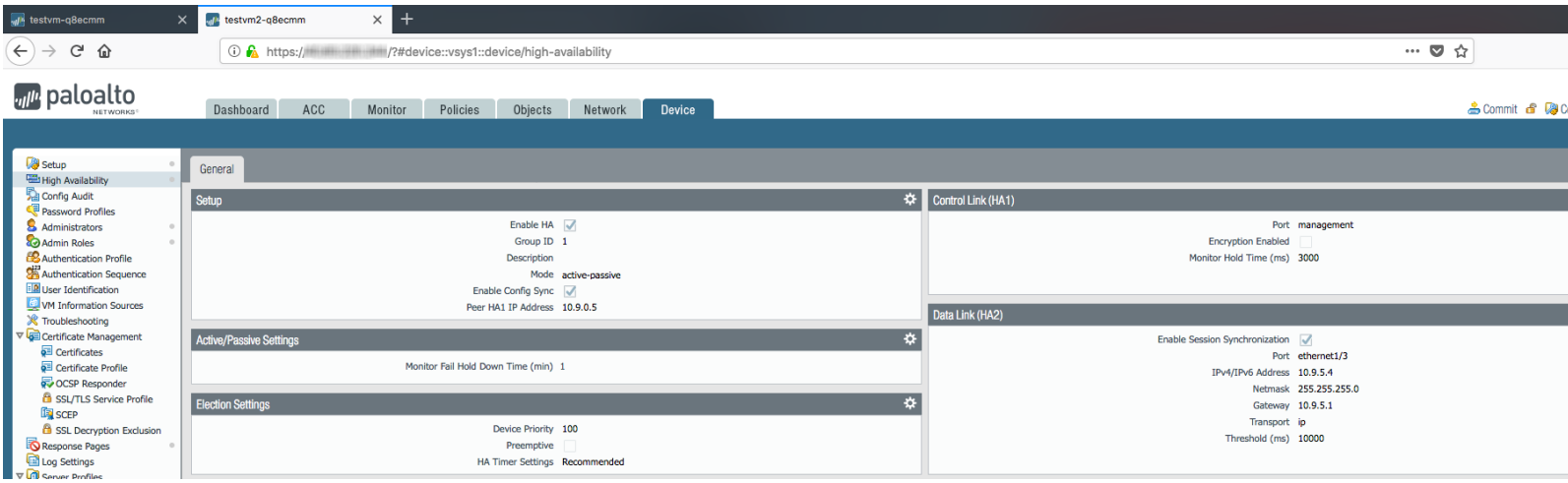
2. 输入 **Peer HA1 IP address**（对等 **HA1 IP** 地址）作为被动对等的专用 IP 地址。
3. （可选）编辑控制链接 (HA1)。如果不计划使用管理接口作为控制链接且已添加其他接口（例如 ethernet 1/4），请编辑此部分以选择用于 HA1 通信的接口。
4. 编辑数据链路 (HA2) 以使用 **Port**（端口）ethernet 1/3，并添加此对等的 IP 地址和子网的 **Gateway**（网关）IP 地址。

STEP 5 | **Commit**（提交）更改。

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）。

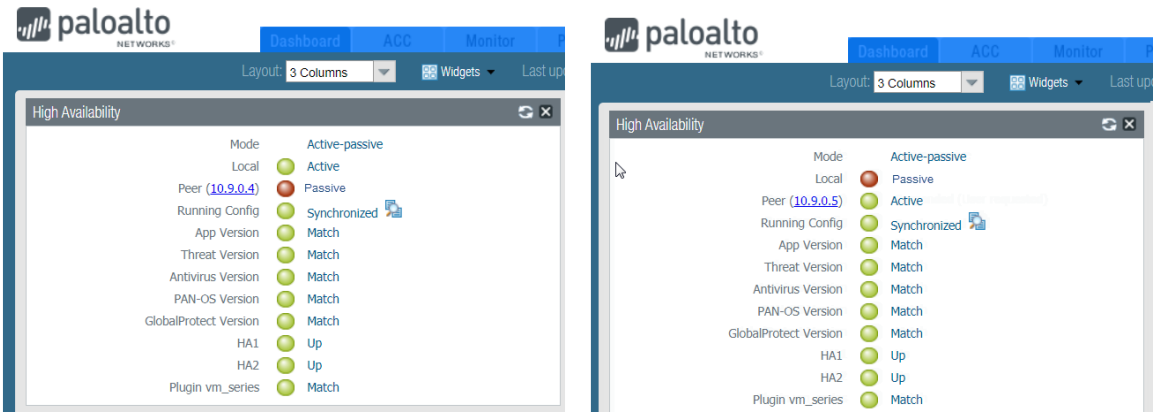
     确保将以下输入与已部署的防火墙实例的输入相匹配 — Azure 订阅、资源组的名称、资源组的位置，要将防火墙部署到的现有 VNet 的名称，VNet CIDR、子网名称、子网 CIDR，并启动管理、可信和不可信子网的 IP 地址。
2. 重复步骤 1 和步骤 2 以设置接口，并将防火墙配置为被动 HA 对等。
3. 跳过步骤 3 并完成启用 HA（步骤 5）。根据情况在步骤 4 中修改此被动 HA 对等的 IP 地址。



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**（仪表板），并查看高可用性小部件。
2. 在主动防火墙上，单击 **Sync to peer**（同步到对等）链接。
3. 确认防火墙已配对并同步，如下所示：

© 2019 Palo Alto Networks, Inc.



- 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。

© 2019 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。

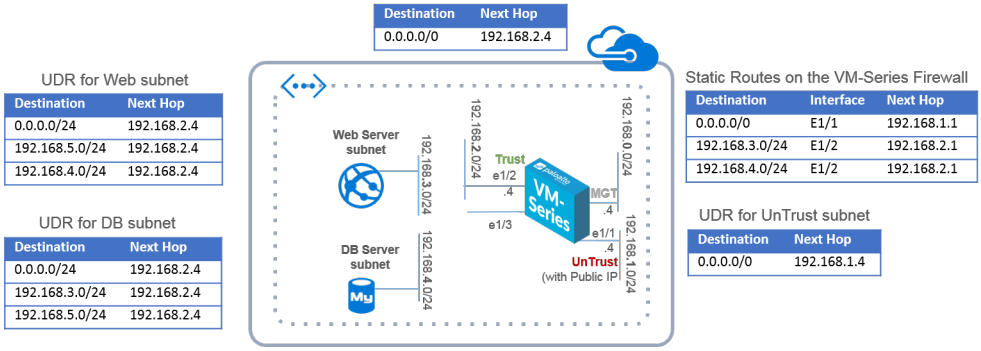


图 4: 使用 **ARM** 模板部署 **VM** 系列防火墙

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

STEP 2 | 在 Azure 上创建资源组。

1. 使用以下命令登录到 Azure CLI：**`azurelogin`**

   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. 使用命令 **`azureconfig mode arm`** 切换至资源管理器模式
3. 创建资源组。

STEP 3 | 部署 ARM 模板。

© 2019 Palo Alto Networks, Inc.

1. 打开带文本编辑器的 Parameters File（参数文件），然后修改用于部署的值：

   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。

```
azure group create -v -n “<YourResourceGroupName>”

-l “<YourAzureLocation>” -d “<GiveASmallDeploymentLabel>”

-f azureDeploy.json -e azureDeploy.parameters.json
```

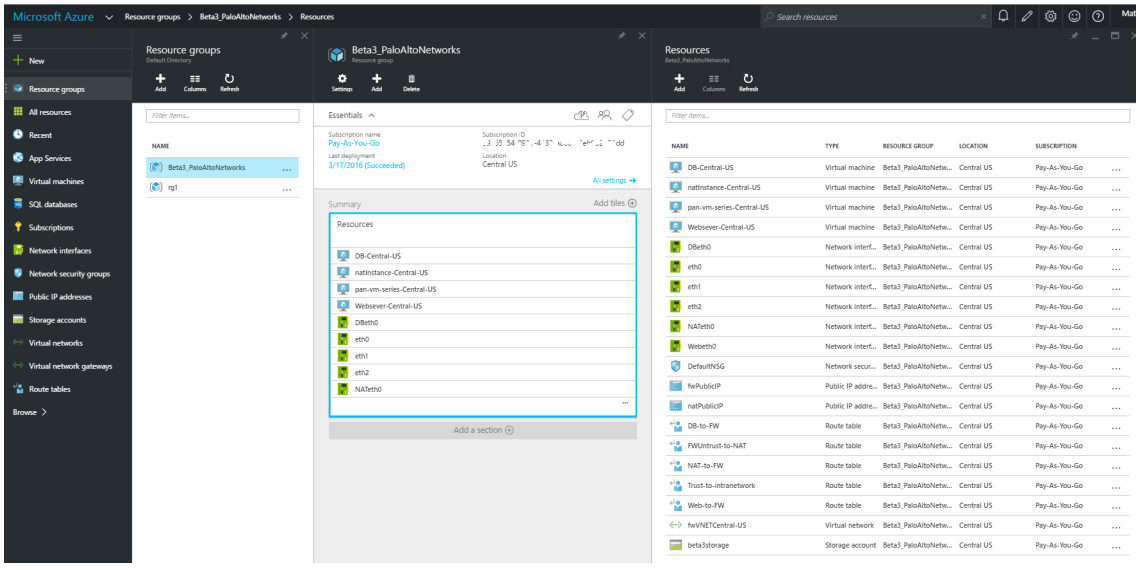
3. 通过 Azure CLI 检查部署进程/状态：

```
azure group deployment show "<YourResourceGroupName>"

“<YourDeploymentLabel>“
```

   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。

© 2019 Palo Alto Networks, Inc.

5. 将公有 IP 地址附加到防火墙上的不可信接口。

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**）。
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））。

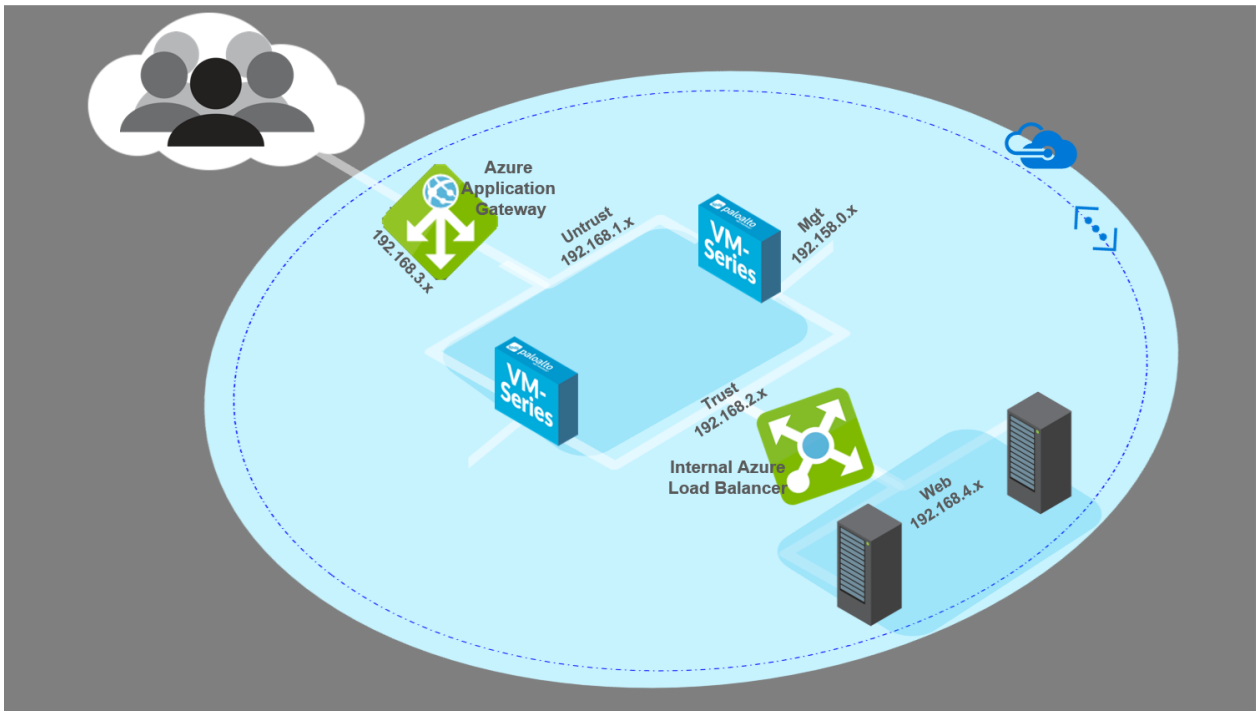
© 2019 Palo Alto Networks, Inc.

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。

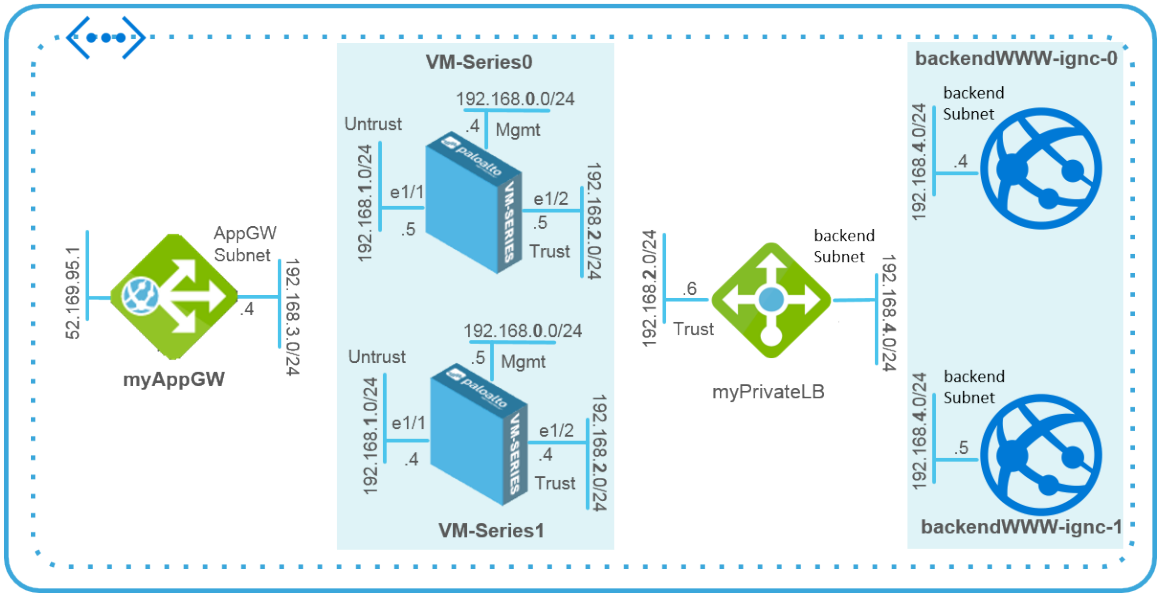


- VM 系列和 Azure 应用程序网关模板
- 开始使用 VM 系列和 Azure 应用程序网关模板

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 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：

© 2019 Palo Alto Networks, Inc.



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。

该模板不提供自动缩放解决方案;您必须计划您的容量需求，然后再为您的部署部署更多资源到 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。

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

© 2019 Palo Alto Networks, Inc.

将模板部署到 *Azure*

使用以下说明将模板部署到 Azure。

STEP 1 | 部署模板。

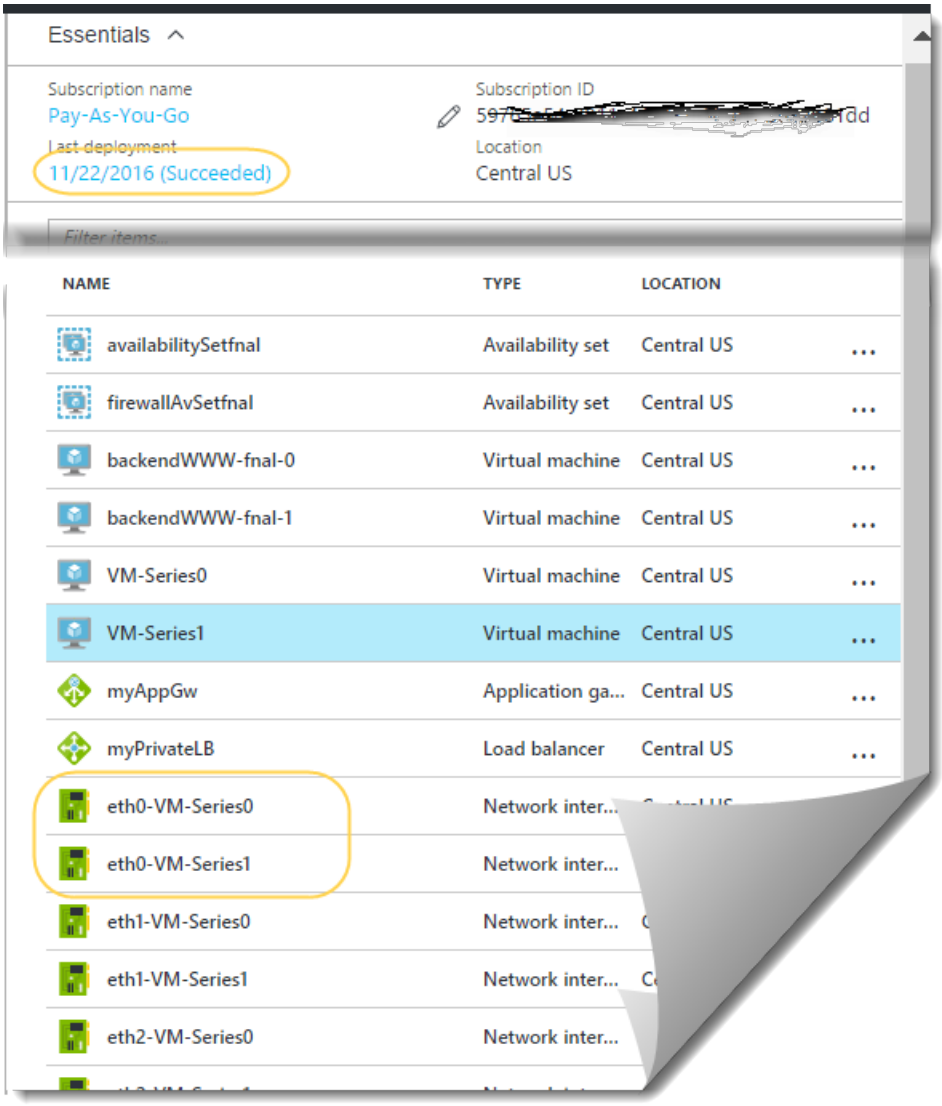
目前无法在 *Azure China* 中进行部署。

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）。

© 2019 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。

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））。

© 2019 Palo Alto Networks, Inc.

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。

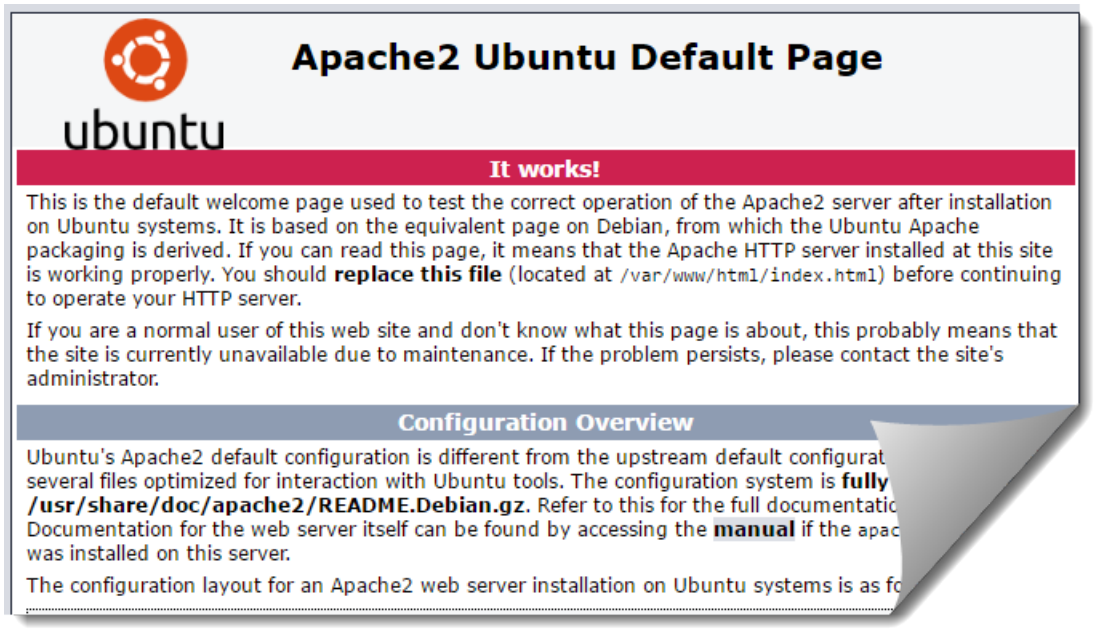
STEP 4 | 登录并配置 VM 系列防火墙的其他实例。

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。

© 2019 Palo Alto Networks, Inc.



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
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。

© 2019 Palo Alto Networks, Inc.

参数	说明
	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	
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。

© 2019 Palo Alto Networks, Inc.

参数	说明
	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。
- **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视此部署中到 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

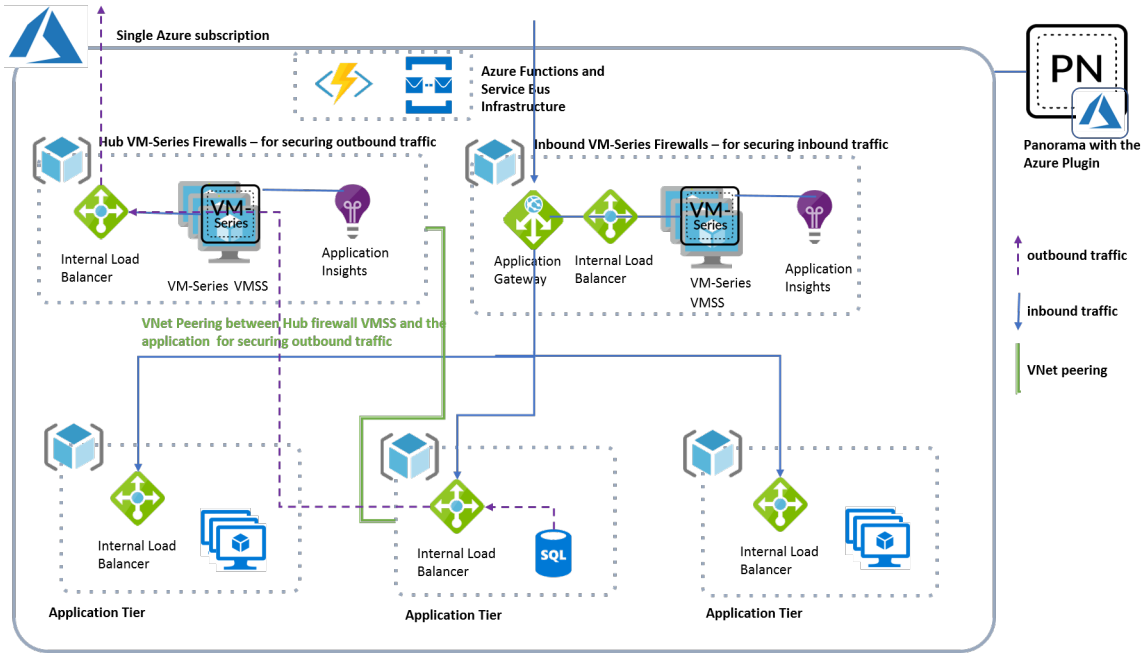
随着您的需求的发展，您可以扩展容量需求并扩展您的部署方案的模板。您可以通过以下方式构建起始模板以满足您的计划容量需求：

- 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 负载平衡（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。

© 2019 Palo Alto Networks, Inc.

在 Azure 上自动扩展 VM 系列防火墙

Palo Alto Networks 可以提供模板以帮助您使用 Azure 服务部署 VM 系列防火墙的自动扩展层，例如虚拟机规模集、Azure Application Insights、Azure 负载均衡器、Azure Function、适用于 Azure 的 Panorama 和 Panorama 插件以及 VM 系列自动化功能（包括 PAN-OS API 和引导）。通过这些模板，您可以利用 Azure 的可扩展性功能来管理应用程序工作负载资源突然激增的需求，从而可让您独立扩展 VM 系列防火墙来响应不断变化的工作负载。



- 在 Azure 上自动扩展 — 组件和规划清单
- 部署 Azure 自动扩展模板
- Azure 自动扩展模板中的参数

在 Azure 上自动扩展 — 组件和规划清单

要在使用应用程序工作负载扩展防火墙的自动扩展设置中部署 VM 系列防火墙并确保服务的高可用性，您需要了解以下概念：

- 虚拟机规模集 **(VMSS)** — VMSS 是 Microsoft Azure 公共云中的一组单个虚拟机 (VM)，管理员可以将其作为单个单元配置和管理。提供的防火墙模板用于自动扩展、创建和管理一组相同的负载均衡 VM 系列防火墙，这些防火墙可根据防火墙发布到 Azure Application Insights 的自定义指标进行扩大或缩小。您可以根据可配置的阈值执行扩大和缩小操作。
- **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。
- **Panorama**、适用于 **Azure** 的 **Panorama** 插件和 **VM** 系列插件 — Panorama 需要启用集中管理在 VMSS 中部署的自动扩展 VM 系列防火墙。Panorama 上的 Azure 插件可以设置 Panorama 与 Azure 订阅中资源之间的通信。该插件负责使用 Panorama 上的设备组和模板堆栈许可、引导和配置 VM 系列防火墙所需的交互。同时，还将 Azure 静态路由和 Azure Application Insights 检测密钥编程到 VMSS 中的防火墙。

  如果要管理运行 PAN-OS 9.0.0 或更高版本的防火墙，还需要在 Panorama 上安装 VM 系列插件。Panorama 需要 VM 系列插件才能将 Azure Application Insights 检测密钥推送到托管防火墙。在

© 2019 Palo Alto Networks, Inc.

PAN-OS 的早期版本中，与 VM 系列插件无关，直到在 PAN-OS 9.0.0 中推出了 VM 系列插件。该插件可以将自定义指标发布到云监控服务（例如 Azure Application Insights），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。

- **Azure Function** 和 **Azure Service Bus** — Azure Service Bus 可以启用 Panorama 上的 Azure 插件与 Azure 资源之间基于消息的通信。Azure Function 是可公开访问的 webhook，可以将消息发布到消息队列。配置 Azure 插件订阅消息队列时，该插件可以读取消息以了解何时部署新的应用程序模板（只要具有 Panorama 托管标记），以及何时在事件中扩展防火墙，以便可以与 Palo Alto Networks 许可服务器建立联系并停用许可证。Panorama 插件和 Azure Function 使用共享访问签名 (SAS) 令牌对 Azure Service Bus 进行身份验证，并从队列中读写消息。
- 模板 — 要部署自动扩展 VM 系列防火墙保护 Azure 上的应用程序服务器池，您可以使用四个模板 — 入站防火墙模板、中心防火墙模板、基础架构模板和示例应用程序模板。
  - 基础架构模板 — 此模板用于部署 Azure Service Bus 和消息基础架构，以启用 Panorama 上的 Azure 插件与 Azure 资源之间基于消息的通信。

    您可以在多个 Azure 订阅之间重复使用此消息基础架构。由于此消息基础架构与 Panorama 不是 1:1 的关系，因此您无需多次部署此模板。

    入站防火墙模板 — 此模板用于部署适用于 VM 系列防火墙的 Azure 应用程序网关（第 7 层负载均衡器）、适用于 VM 系列防火墙的 VMSS、具有三个子网的新 VNET（用于防火墙上的可信、不可信和管理接口）以及 Application Insights 实例。通过此模板部署 VM 系列防火墙，您可以保护从互联网到应用程序的入站流量。
  - 中心防火墙模板 — 此模板用于部署标准内部负载均衡器、适用于 VM 系列防火墙的 VMSS、具有三个子网的新 VNET（用于防火墙上的可信、不可信和管理接口）以及 Application Insights 实例。通过此模板部署 VM 系列防火墙，您可以保护出站流量（源自应用程序服务器的流量）以及应用程序层之间的东向西流量。
  - 应用程序模板 — 提供此模板作为示例，以帮助您在 Azure 上试用 VM 系列自动扩展解决方案。部署此应用程序模板时，您可以选择是只保护入站流量还是同时保护入站流量和出站流量。此模板用于部署内部负载均衡器（标准）和示例 Web 应用程序。如果您选择保护出站流量，则此模板还会创建用户定义路由 (UDR)，以通过中心防火墙 VMSS 转发来自应用程序服务器的传出流量。请参阅标记，以了解 Panorama 标识其保护的应用程序流量所需的标签。
- **Azure VNet** 对等 — Azure VNet 对等可以连接 Azure 公共云中的虚拟网络。对等虚拟网络中虚拟机之间的流量直接通过 Microsoft 骨干基础架构路由，而不是使用网关或通过公共互联网。在对等 VNets 中，虚拟网络中的所有子网都具有与适用于这些网络中每个地址空间的下一个跃点类型 VNet 对等的路由。如果您的应用程序和 VM 系列防火墙 VMSS 位于不同的 VNets 中，则需要应用程序与入站和中心防火墙 VMSS 虚拟网络之间的 VNet 对等才能在它们之间成功路由流量。
- **Azure** 负载均衡器 — 内部负载均衡器和 Azure 应用程序网关可以将流量重新分发到防火墙 VMSS 或后端应用程序服务器池。
- 标记 — VMSS 和示例应用程序中的防火墙都具有用于标识的标记。部署（入站或中心）防火墙模板时，VMSS、VNet 和 Azure 应用程序网关（外部负载均衡器）都具有一个标记，称为 **`PanoramaManaged=True`**。使用此标记，Panorama 上的 Azure 插件可以标识资源并检索信息，例如子网 CIDR 以及在防火墙中管理静态路由和停用许可证所需的信息。

  除了 **`PanoramaManaged=Yes`** 标记以外，面向应用程序的内部负载均衡器还需要两个标记。要保护入站流量，您必须添加标记 **`SpokeRG=<name of the inbound firewall RG>`**；并且，如果您已部署中心防火墙模板且要保护出站流量，还必须添加标记 **`HubRG=<name of hub firewall RG>`**。
- 示例防火墙配置— 示例防火墙配置包括区域中具有 eth1/1（不可信）和 eth1/2（可信）接口的虚拟路由器。您可以使用此配置作为起点，以便 Panorama 可以推送静态路由，从而使得防火墙能够通过防火墙上的正确接口转发入站/出站流量。

有关绿色字段和棕色字段部署情景，请参阅 Azure 自动扩展部署用例。

计划部署

在开始之前，请使用以下清单仔细考虑自动扩展部署，并收集继续部署 Azure 自动扩展模板所需的详细信息。

© 2019 Palo Alto Networks, Inc.

- 您要在其中部署应用程序和 VM 系列防火墙的 Azure 订阅和区域。

  防火墙和应用程序必须部署在相同的区域和订阅中。Azure 入站防火墙或中心防火墙模板 1.0 版本不支持交叉订阅部署。
- 运行 PAN-OS 版本的 Panorama 设备支持自动扩展（参阅兼容性矩阵中的 Panorama 插件版本信息）。
- Panorama 必须具有通过互联网进行路由的公共 IP 地址，或必须具有另一种与 VM 系列防火墙建立连接的方式。要完成引导流程并确保防火墙获得许可，Panorama 设备上的管理接口必须能够与 VM 系列防火墙上的管理接口进行通信。此外，VM 系列防火墙还必须能够访问 Palo Alto Networks 服务器以成功检索许可证。
- 在 Panorama 上计划设备组和模板/模板堆栈。

  在 Panorama 上，您必须将防火墙分配到模板堆栈和设备组，以便推送网络配置和策略。您必须先添加模板并将其分配给模板堆栈，在 Panorama 上创建设备组，然后在配置 (init-cfg.txt) 文件中包括模板堆栈名称和设备组名称。如果您部署中心和入站防火墙模板来部署自动扩展 VM 系列防火墙，以保护 Azure 订阅中应用程序的入站和出站流量，则必须设置两组模板堆栈、模板和设备组。一组用于管理中心防火墙 VMSS 的 VM 系列防火墙配置，另一组用于管理入站防火墙 VMSS 的 VM 系列防火墙配置。

  Azure 订阅与 Panorama 上的自动扩展定义之间是 1:1 的关系。

  如果 *Azure* 订阅中有多个 *VMSS*，则您必须使用单个 *Panorama* 设备来管理 *Azure* 订阅中的两个 *VMSS*。

  对于要添加到 Panorama 的每个防火墙 VMSS，您必须提供与防火墙相关联的资源组名称、资源组类型（中心或入站）、设备组名称和模板堆栈名称，以便 Panorama 可以推送配置。作为自动扩展定义的一部分，您可以指定是否要让 Panorama 创建和推送通过防火墙转发入站/出站流量所需的静态路由。

  您还必须将虚拟路由器添加到模板堆栈。
- 在 Azure 门户上创建存储帐户并设置 Azure 文件服务，以包含在 Azure 上引导 VM 系列防火墙所需的文件夹结构。
- 收集所需的信息作为 init-cfg.txt 文件中的输入。您必须包括以下内容：
  - Panorama IP 地址 — 防火墙必须与其连接以获取许可证和配置的 Panorama 设备的 IP 地址。
  - VM 身份验证密钥 — 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，并且引导包的 /license 文件夹中必须包含许可证身份验证代码。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，并将防火墙添加为受管设备。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。
  - 身份验证代码（如果使用 BYOL）
  - 设备组名称
  - 模板堆栈名称
- （如果您要保护已经部署的应用程序）收集在入站防火墙模板中配置 Azure 应用程序网关所需的设备详细信息，以将应用程序流量引导至面向您要保护的应用程序的内部负载均衡器。有关前端和后端服务器配置的详细信息，请参阅 Azure 应用程序网关文档。有关示例配置，请参阅板载应用程序。

  使用示例应用程序模板时，将自动定义相关标记，以及插件会创建在将流量路由到应用程序服务器池之前通过防火墙重定向流量所需的静态路由。在棕色字段部署的情况下或当您部署自己的应用程序模板时，要使入站防火墙 VMSS 支持后端池中的多个应用程序，您必须手动配置面向应用程序服务器池的公共负载均衡器。
- Panorama 上的 Azure 插件需要 Active Directory 应用程序和服务主体才能执行 Azure API 和访问 Azure 资源。创建 Active Directory 应用程序和服务主体时，请确保服务主体拥有 VM 系列在 Azure 上的服务主体权限中指定的权限，并保存该过程中的详细信息。这些信息是必需的，作为 Panorama 上 Azure 插件的输入。
  - 应用程序 ID

© 2019 Palo Alto Networks, Inc.

- 密钥（复制此密钥；离开页面后，密钥不再可见）
- 租户 ID
- 订阅 ID

❑ 从 GitHub 存储库下载支持此自动扩展部署的模板和文件。

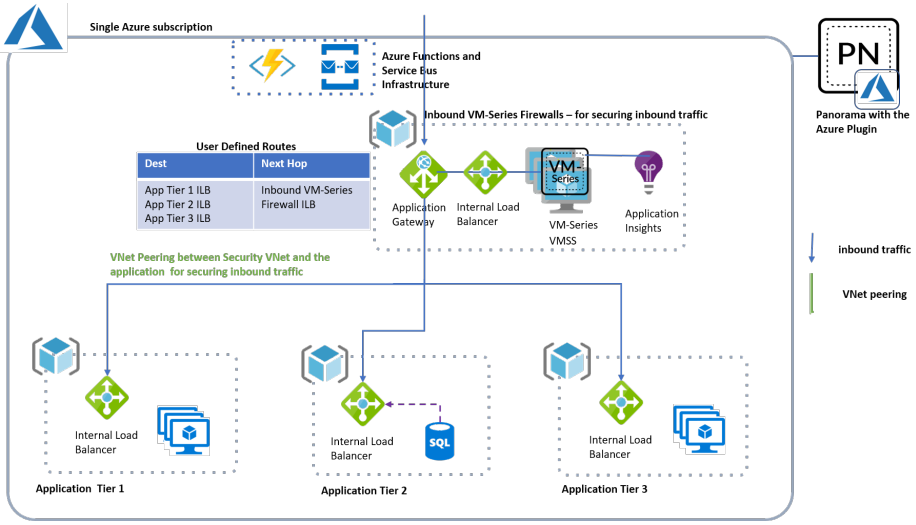
❑ 记录 Azure Service Bus 密钥名称和共享访问签名。

部署基础架构模板后，您必须收集 Azure Service Bus 密钥名称和共享访问签名详细信息以配置自动扩展定义。

Azure 自动扩展部署用例

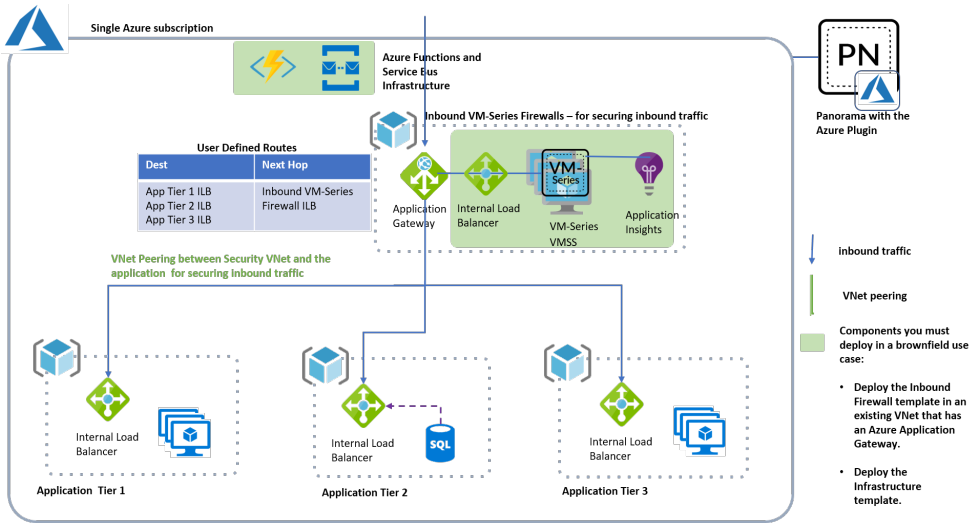
绿色字段部署是新 VNet 中的全新部署。相反，棕色字段是对具有某些现有组件的现有 VNet 的升级或添加。

- 保护绿色字段部署中的入站流量 — 如果您是从头开始且需要保护面向互联网的应用程序的入站 Web 流量，则需要使用 Panorama、适用于 Panorama 的 Azure 插件、基础架构模板和入站防火墙模板。在部署应用程序并启用托管入站防火墙 VMSS 和应用程序 VNet 的 VNet 之间的 VNet 对等之前，请使用样本应用程序模板验证标记并试用解决方案。提供入站防火墙模板的输入时，您必须提供有关创建新 VNet 的详细信息。有关每个模板中包含哪些组件的详细信息，请参阅在 Azure 上自动扩展 — 组件和规划清单和部署 Azure 自动扩展模板。



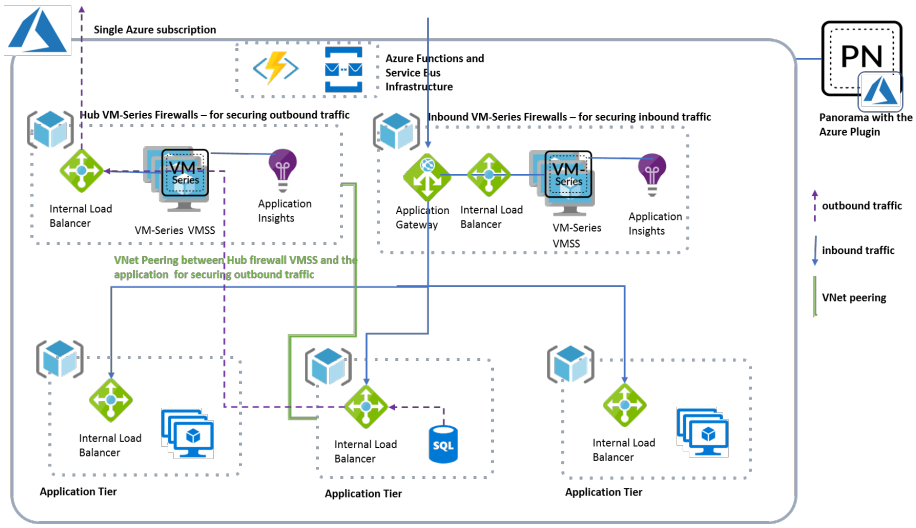
- 保护棕色字段部署中的入站流量 — 如果您已在与托管应用程序网关并将流量定向到这些应用程序的 VNet 对等的一个或多个 VNet 中部署应用程序，则现在可以部署一组自动扩展的 VM 系列防火墙以创建安全 VNet 拓扑，如以下拓扑图所示。要保护棕色字段部署中面向互联网的应用程序的入站 Web 流量，您需要使用 Panorama、适用于 Panorama 的 Azure 插件、基础架构模板和入站防火墙模板。提供入站防火墙模板的输入时，您必须提供有关现有 VNet 的详细信息。

© 2019 Palo Alto Networks, Inc.



此外，您还将需要完成其他配置才能将应用程序连接到入站防火墙 VMSS，例如，您必须添加 UDR 才能通过防火墙 VMSS 重定向入站应用程序流量。有关详细信息，请参阅 部署 Azure 自动扩展模板。

- 保护绿色字段和棕色字段部署中的出站流量 — 要保护源自 VNet 中应用程序的 Web 流量，您需要使用 Panorama、适用于 Panorama 的 Azure 插件、基础架构模板和中心防火墙模板。此外，您还将需要完成其他配置才能将应用程序连接到中心防火墙 VMSS。请参阅 在 Azure 上自动扩展 — 工作原理 和 部署 Azure 自动扩展模板。



在 Azure 上自动扩展 — 工作原理

您想要部署一组自动扩展的 VM 系列防火墙的主要原因是为了确保操作效率，并在需求激增时保护面向互联网的应用程序的高可用性流量，以及在需求下降和应用程序工作负载扩大时保持成本效益。

使用 VM 系列防火墙启用自动扩展过程的第一步是启动可以提供消息基础架构的基础架构模板。适用于 Azure 的 Panorama 插件使用此基础架构了解在启动中心或入站防火墙模板时部署的 VM 系列防火墙 VMSS，并了解何时添加新的应用程序服务器池，以及需要中心或入站防火墙模板或两者提供保护。

然后，您可以在 Panorama 上设置自动扩展定义以使用 Azure Service Bus 名称、Azure Service Bus 密钥名称、共享访问令牌和 Azure 订阅的服务主体授权访问。这些详细信息能够让 Panorama 访问 Azure 资源的元数据，并读取 Azure Function 发布到 Azure Service Bus 的消息。

部署入站防火墙模板保护到应用程序服务器池的所有入站流量时，适用于 VM 系列防火墙的 VMSS 与 Azure Application Insights 实例一起启动，这些防火墙会将您要触发自动扩展的 PAN-OS 指标发布到该实例。作为

© 2019 Palo Alto Networks, Inc.

模板输入的一部分，您可以为触发自动扩展过程的 Azure Application Insights 警报选择 PAN-OS 扩展指标和阈值。这些防火墙使用您在模板中的输入自动引导，并作为托管设备添加到 Panorama。

在 Panorama 上，您现在可以添加入站防火墙资源组详细信息，并启用路由自动编程功能。入站防火墙模板包含三个静态路由。

- 将流量转发到可信接口的默认路由，启用防火墙后，如果没有更多特定路由可用，则使用默认路由。
- 将来自应用程序的返回流量发送回到入站防火墙 VMSS 中的应用程序网关 IP 地址的路由。
- 执行运行状况检查的路由，这样可以对 VMSS 中的防火墙实例启用负载均衡。

当新启动的防火墙连接到 Panorama 时，Panorama 会推送设备组和模板堆栈配置，其中包括您定义的虚拟路由器和策略规则，以及自动编程的静态路由。此外，Panorama 插件还将检索 Azure Application Insights 检测密钥，并将其添加到分配给防火墙的模板堆栈。当防火墙达到配置的阈值并发生扩展事件时，将启动 VM 系列防火墙的新实例。引导防火墙连接到 Panorama 并获取其许可证和配置，以确保它可以保护您的应用程序。

当发生缩小事件时，Panorama 插件会停用防火墙上的许可证，并管理防火墙的生命周期。防火墙的 IP 地址已从 VMSS 中删除，并且内部负载均衡器不会将流量路由到防火墙。

中心防火墙模板中的流程类似，但静态路由配置略有不同。

为了将流量通过入站防火墙或中心 VMSS 定向到应用程序，您需要完成一些配置：

为了保护入站应用程序流量，必须将应用程序连接到入站防火墙 VMSS。板载应用程序时，您需要执行以下操作：

- 使用前端和后端配置来配置应用程序网关，以指向面向应用程序服务器池的内部负载均衡器。请参阅 Azure 应用程序网关文档。
- 在默认的 BackendUDR 中，通过应用程序子网添加路由作为目标，并添加下一个跃点 IP 地址作为面向防火墙 VMSS 的内部负载均衡器的地址。
- 如果应用程序 VNet 和入站防火墙 VMSS VNet 在不同的 VNet 中，请设置它们之间的 VNet 对等。使用 GitHub 存储库中包含的样本应用程序模板时，将会为您设置 VNet 对等。
- 使用以下名称/值对标记面向应用程序的内部负载均衡器。

```
PanoramaManaged-yes
```

```
InboundRG-<Name of the Inbound Firewall Resource Group>
```

为了保护出站流量，您需要完成以下操作才能将入站防火墙 VMSS 连接到应用程序 VNet：

- 在路由表中添加 UDR，并将应用程序子网与路由表相关联。请参阅 Azure 文档。
- 在 Azure 门户上，添加默认路由 (0.0.0.0/0) 以将所有流量转发到面向中心防火墙 VMSS 的内部负载均衡器。
- 使用以下名称/值对标记面向应用程序的内部负载均衡器。

```
HubRG-<Name of the Hub Firewall Resource Group>
```

在应用程序 VNet 中标记内部负载均衡器时，Panorama 将了解并在中心防火墙模板堆栈中自动创建静态路由，以将返回流量定向到应用程序工作负载。

否则，您必须在模板堆栈上添加静态路由以管理中心 VMSS 中防火墙的配置，使得中心 VMSS 中的防火墙能够将流量定向回到应用程序工作负载。

部署 Azure 自动扩展模板

Azure 自动扩展模板利用包括本地 Azure 服务的多个组件自动扩展 VM 系列防火墙，以便在缩小或扩展应用程序工作负载以满足企业需求时保护应用程序工作负载。要启用 Azure VM 规模集 (VMSS) 以自动扩展 VM

© 2019 Palo Alto Networks, Inc.

系列防火墙，需要将自定义防火墙指标发布到 Azure Application Insights，从而允许防火墙根据监控的阈值进行缩小或扩展。为了使此自动扩展机制发挥作用，您需要使用 Panorama 和 Panorama 上的 Azure 插件。有关使用 VM 系列防火墙的自动扩展层保护应用程序工作负载所需的所有组件的详细信息，请参阅在 Azure 上自动扩展 — 组件和规划清单。

观看有关部署 *Azure* 自动扩展模板的视频。

- 准备工作
- 部署自动扩展 VM 系列防火墙以保护应用程序

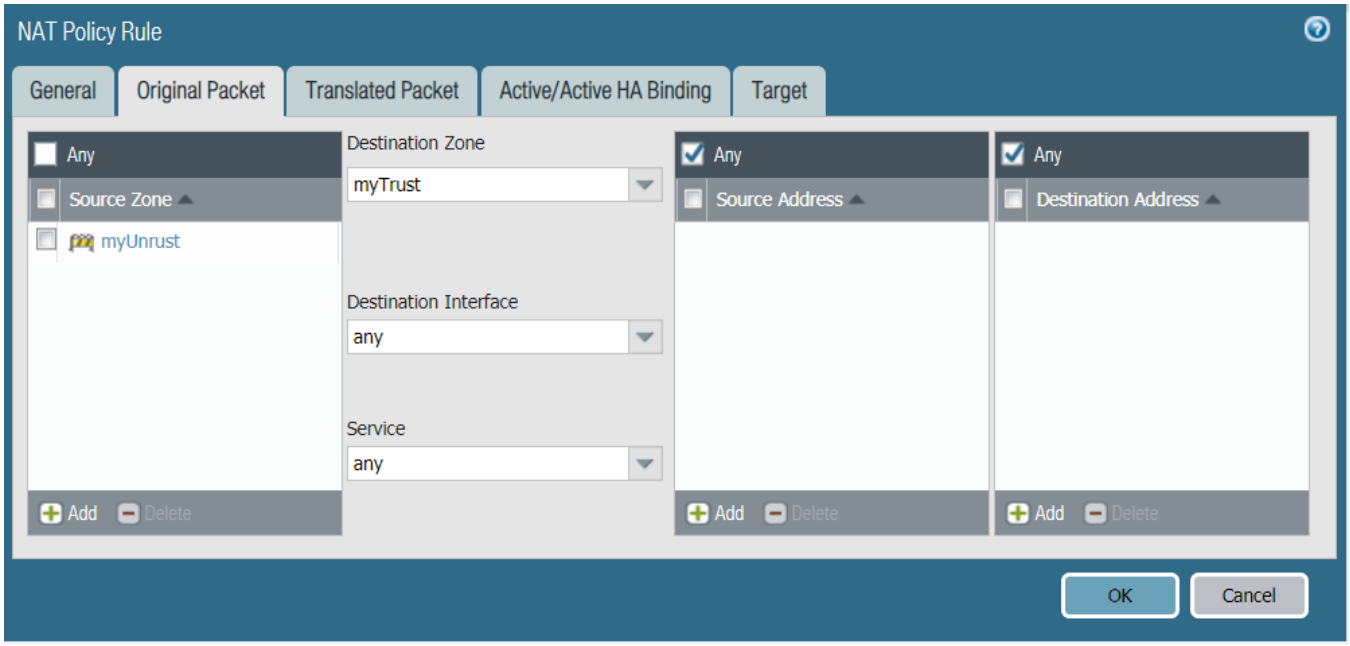
准备工作

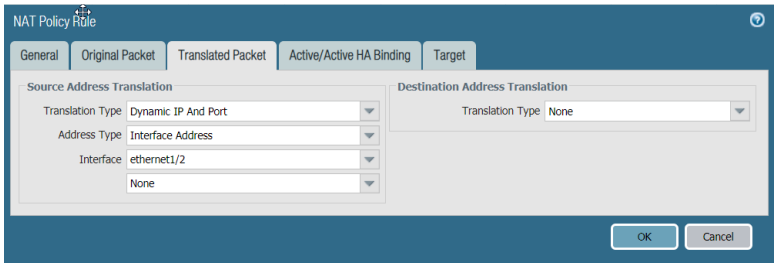
开始部署可在 Azure 上使用应用程序工作负载自动扩展的 VM 系列防火墙。

- 查看计划部署 中的清单。确保检查兼容性矩阵中的 Panorama 插件版本信息。
- 从 GitHub 存储库下载模板和文件。
- 在 Panorama 上安装适用于 Azure 的 Panorama 插件。
- 在 Panorama 上创建以下内容：
  1. 在模板堆栈中创建虚拟路由器。

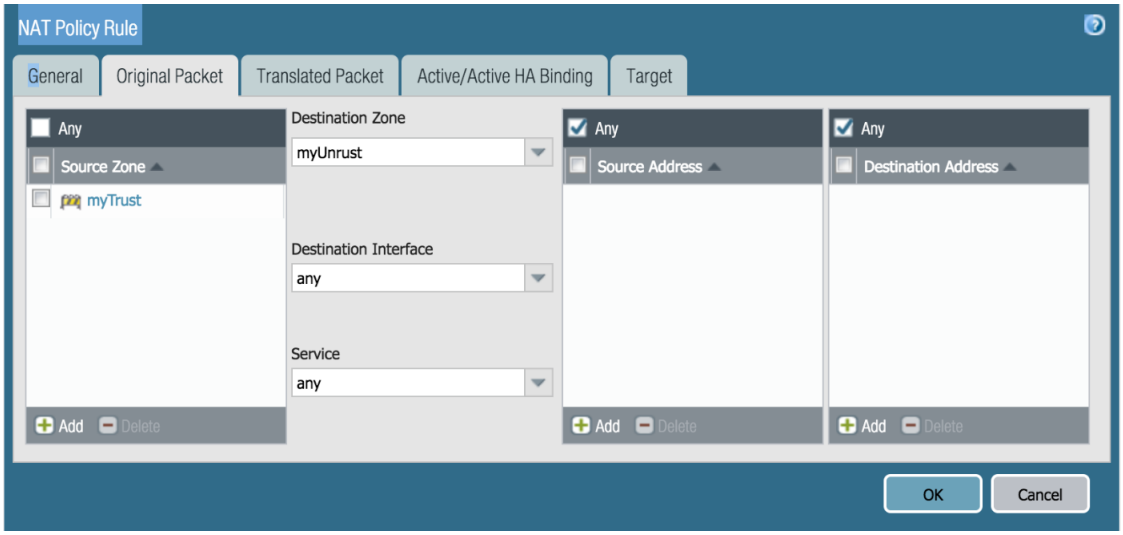
     确保将虚拟路由器添加到模板堆栈而不是模板。如果没有在模板堆栈中创建虚拟路由器，则不会将入站防火墙模板自动创建的静态路由添加到虚拟路由器，并且应用程序模板可能无法成功启动。
  2. 在模板中创建两个接口 — ethernet1/1（不可信）和 ethernet1/2（可信）接口。在每个接口上，**Enable DHCP**（启用 **DHCP**）并清除 **Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）。
  3. 将接口分配给虚拟路由器。
  4. 创建 NAT 策略规则。
     - 选择您计划用于配置入站防火墙模板的设备组，并添加 NAT 策略规则以将流量从不可信区域定向到可信区域，以及将转换后的数据包设置为使用可信接口 (ethernet1/2) IP 地址，以便将返回流量发送回到防火墙上的可信接口。

© 2019 Palo Alto Networks, Inc.

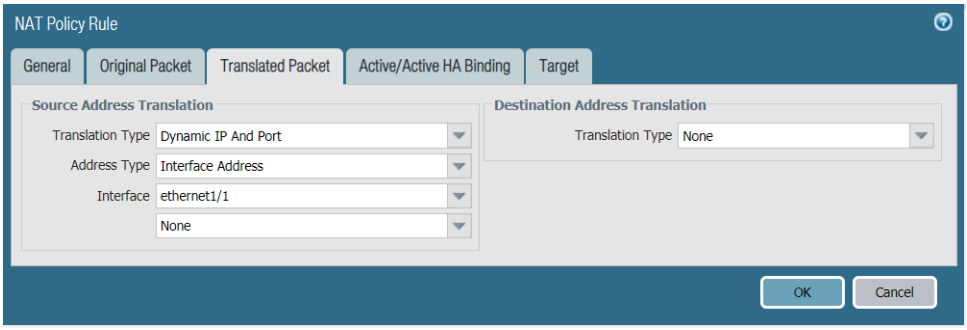




- 选择您计划用于配置中心防火墙模板的设备组，并添加 NAT 策略规则以将流量从可信区域定向到不可信区域，以及将转换后的数据包设置为使用不可信接口 (ethernet1/1) IP 地址，以便将返回流量发送回到防火墙上的不可信接口。



© 2019 Palo Alto Networks, Inc.

- 

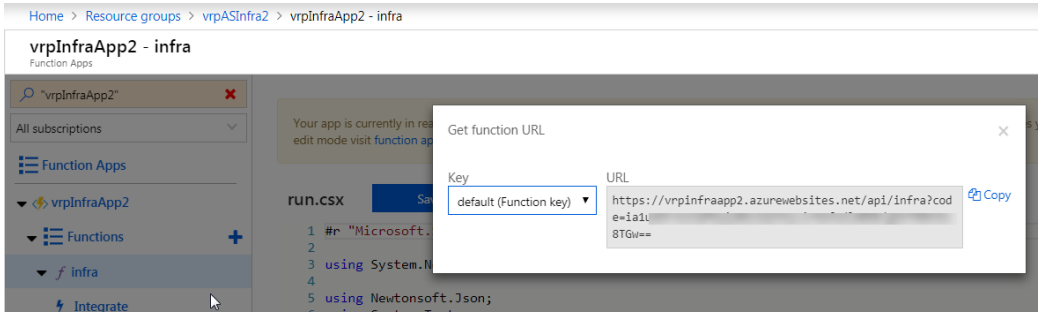
5. 创建安全策略规则以允许您正在部署的应用程序的流量。

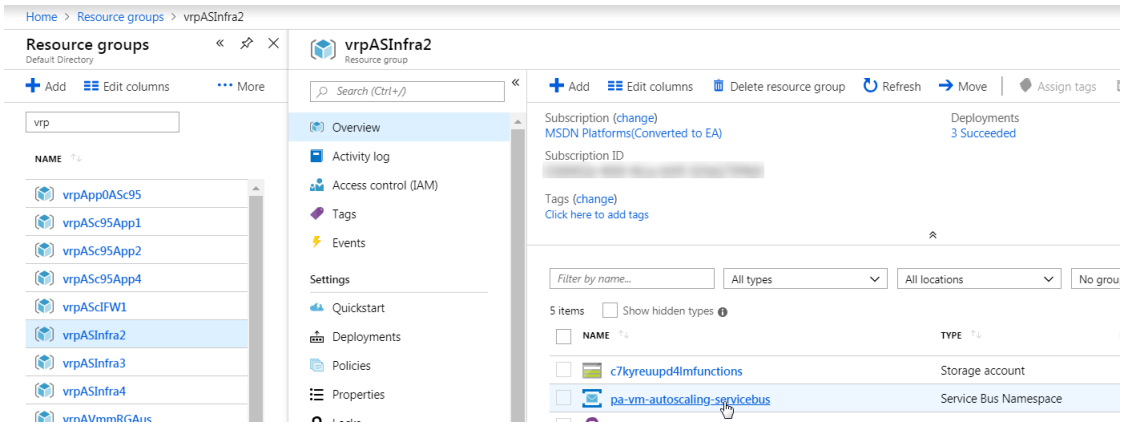
部署自动扩展 *VM* 系列防火墙以保护应用程序

以下工作流程将引导您完成设置 Azure Service Bus 基础架构的过程，该基础架构支持检测缩小和扩展事件、自动编程静态路由和许可防火墙所需的消息系统。然后，该工作流程可帮助您部署用于在 VMSS 中配置 VM 系列防火墙的 ARM 模板，其中防火墙可以通过应用程序工作负载扩展，并确保服务的高可用性。最后，该工作流程还详细介绍了如何配置自定义应用程序，以将流量定向到 VM 系列防火墙并保护流量流。

STEP 1 | 启动基础架构模板。

这可以让您启动 Azure Service Bus 和 Azure Function。您需要获取 Azure Service Bus 名称和 Azure Service Bus 凭据（共享访问密钥），以便稍后在 Panorama Azure 插件上使用。此外，您还将需要 Azure Function URL 以部署防火墙模板（用于入站和中心）。





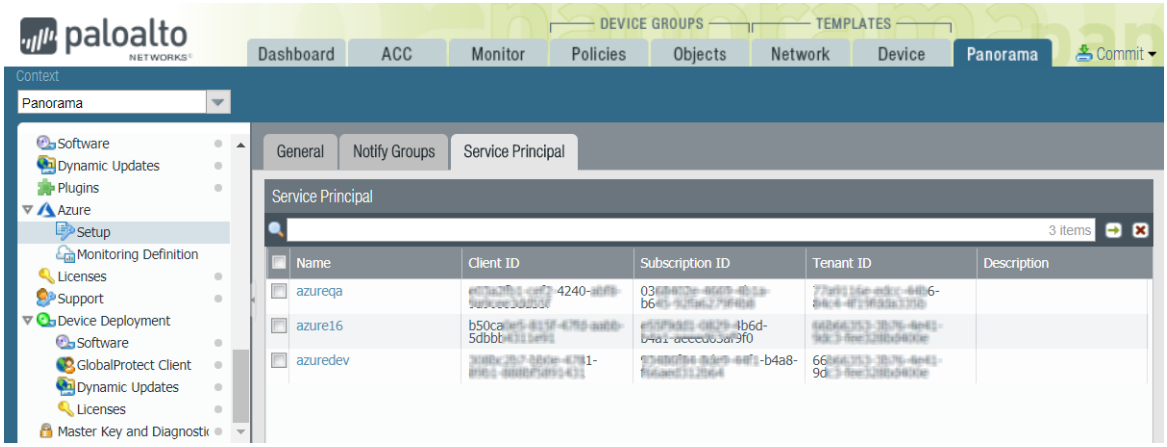
STEP 2 | 登录到 Panorama，对于防火墙的每个 VMSS 组，请创建设备组、模板堆栈和一个或多个模板。

STEP 3 | 在 Panorama 的 Azure 插件上设置服务主体。

© 2019 Palo Alto Networks, Inc.

服务主体是您在 Azure 门户上创建的服务账户。此账户可添加到 Azure AD，且有一定的权限，可访问和监控 Azure 订阅中的资源。对于此自动扩展部署，请至少确保服务主体拥有贡献者权限。

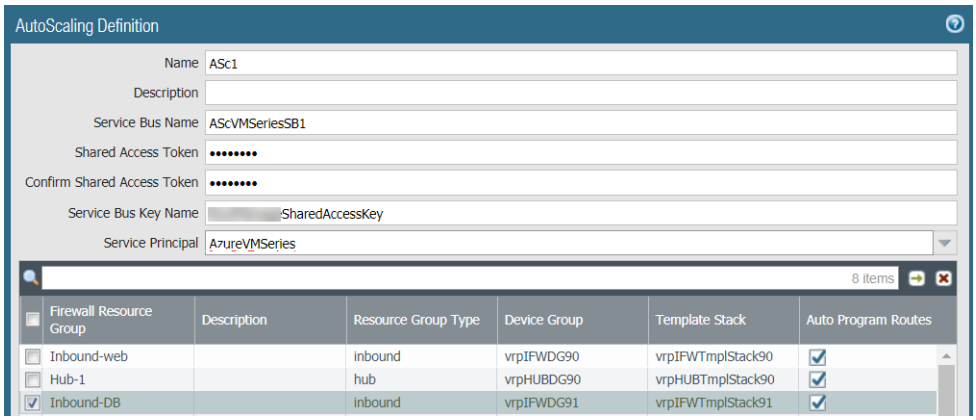
1. 选择 **Panorama** > **Plugins**（插件）> **Azure** > **Setup**（设置）> **Service Principal**（服务主体）> **Add**（添加）。



2. 输入标识服务账户的 **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，并且 Panorama 是否可以使用 API 与 Azure 订阅进行通信。

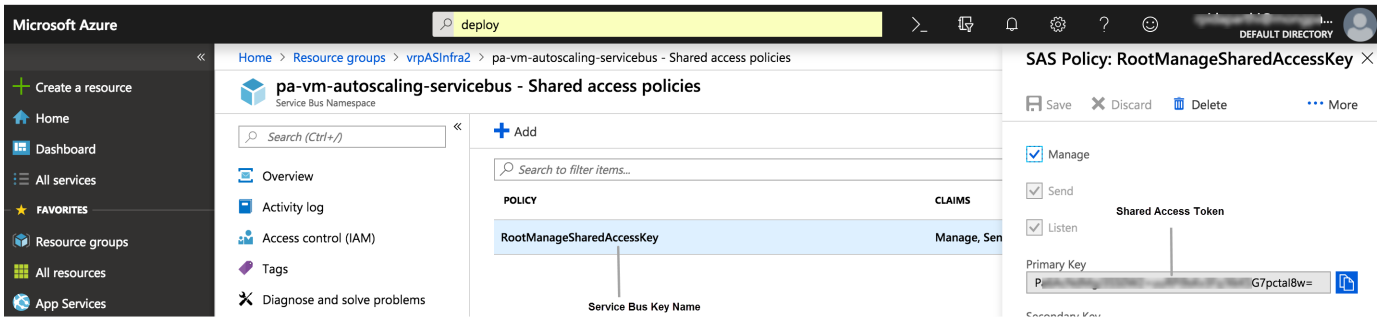
STEP 4 | 为 Azure 订阅创建 Azure 自动扩展定义。

您最多可以添加 10 个自动扩展定义，每个自动扩展定义最多可以包括 25 个虚拟机规模集 (VMSS)。VMSS 中的防火墙映射到 Panorama 上的一个设备组和一个模板堆栈。



1. 选择 **Panorama** > **Plugins**（插件）> **Azure** > **Autoscaling**（自动扩展）> **Add**（添加）。
2. 输入自动扩展定义的 **Name**（名称）和 **Description**（说明）。
3. 添加 **Service Bus Name**（**Service Bus** 名称）— 输入在从 GitHub 存储库启动基础架构模板时定义的 Azure Service Bus 名称。您必须从 Azure 门户复制此名称，然后将其粘贴到此处。
4. 添加 **Shared Access Token**（共享访问令牌）和 **Service Bus Key Name**（**Service Bus** 密钥名称）— 您需要从 Azure 门户上的基础架构模板获取令牌和密钥名称。

© 2019 Palo Alto Networks, Inc.



5. 选择能够让 Panorama 对 Azure 订阅进行身份验证的 **Service Principal**（服务主体）。
6. 将防火墙资源组 **Add**（添加）到 Panorama。
    1. 输入标识 **Firewall Resource Group**（防火墙资源组）的名称，也可以选择输入 **Description**（说明）。
    2. 选择资源组类型：**Hub**（中心）— 这些防火墙可保护 Azure 部署中 VM 之间的出站流量和东向西流量。**Inbound**（入站）— 这些防火墙可保护到 Azure 部署中应用程序 VM 的入站流量。
    3. 选择您为在上述资源组中部署的防火墙创建的 **Device Group**（设备组）和 **Template Stack**（模板堆栈）。
    4. 确认已启用 **Push static routes automatically to the template stack**（自动将静态路由推送到模板堆栈）。默认启用此选项，能够让 Panorama 将静态路由推送到属于入站防火墙 VMSS 和中心防火墙 VMSS 的防火墙。在入站防火墙模板中，静态路由能够让防火墙将入站流量定向到后端应用程序服务器池，将返回流量路由到客户端，以及路由 Azure 负载均衡器启动的运行状况探测。在中心防火墙模板中，静态路由能够让防火墙路由 Azure 负载均衡器启动的运行状况探测，并将出站流量（即源自应用程序/服务的流量）定向到互联网。

STEP 5 | 启动 Azure 入站防火墙模板。

无论您是要保护绿色字段部署还是棕色字段部署，都需要 Azure 入站防火墙模板来保护面向互联网的应用程序的入站流量。

1. 启动入站防火墙模板。

    有关输入参数的说明，请参阅入站防火墙模板参数。如果您不想保护出站流量（即保护来自资源组中应用程序工作负载的流量），请跳到载入应用程序。
2. 为了保护入站应用程序流量，必须将应用程序连接到入站防火墙 VMSS。

    板载应用程序时，您需要执行以下操作：

    - 使用前端和后端配置来配置应用程序网关，以指向面向应用程序服务器池的内部负载均衡器。请参阅 Azure 应用程序网关文档。
    - 在默认的 BackendUDR 中，通过应用程序子网添加路由作为目标，并添加下一个跃点 IP 地址作为面向防火墙 VMSS 的内部负载均衡器的地址。
    - 如果应用程序 VNet 和入站防火墙 VMSS VNet 在不同的 VNet 中，请设置它们之间的 VNet 对等。使用 GitHub 存储库中包含的样本应用程序模板时，将会为您设置 VNet 对等。
    - 使用以下名称/值对标记面向应用程序的内部负载均衡器。

    ```
    PanoramaManaged-yes
    ```

    ```
    InboundRG-<Name of the Inbound Firewall Resource Group>
    ```

    入站模板将公用 *IP* 地址分配给 *VMSS PA-VM* 管理接口。确保在模板中配置网络安全组入站源 *IP* 地址。

© 2019 Palo Alto Networks, Inc.

STEP 6 | 启动 Azure 中心防火墙模板。

只有在您要保护源自资源组中应用程序工作负载的流量时才需要部署此模板。

1. 启动中心自动扩展防火墙模板。有关输入参数的说明，请参阅中心模板参数。
2. 将中心防火墙 VMSS 连接到应用程序 VNet。

   在 Azure 门户上完成以下操作：

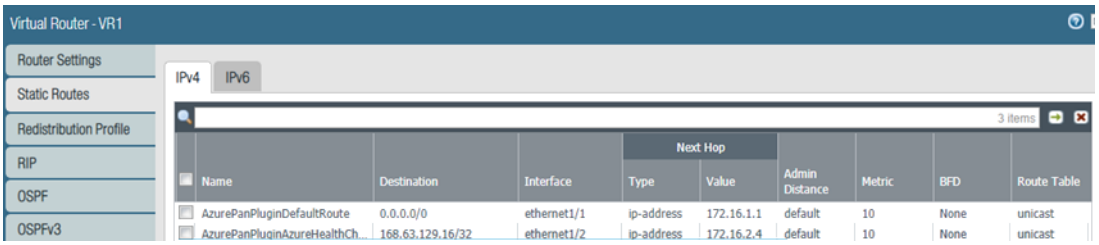
   - 在路由表中添加 UDR，并将应用程序子网与路由表相关联。请参阅 Azure 文档。
   - 在 Azure 门户上，添加默认路由 (0.0.0.0/0) 以将所有流量转发到面向中心防火墙 VMSS 的内部负载均衡器。
   - 使用以下名称/值对标记面向应用程序的内部负载均衡器。

   ```
   HubRG-<Name of the Hub Firewall Resource Group>
   ```

   在 *Panorama* 上，您必须添加静态路由以使中心 *VMSS* 中的防火墙将流量定向回到应用程序工作负载（如本步骤中所示）。确保在用于管理中心 *VMSS* 中防火墙配置的模板堆栈上定义静态路由。
3. 确认自动编程路由在 Panorama 上的虚拟路由器中。

   部署中心模板后，会将默认路由和托管防火墙的运行状况检查路由自动添加到通过中心模板启动的 VM 系列防火墙的模板堆栈中的虚拟路由器。并且，Azure Application Insights 检测密钥也将自动可用。您需要确认已包括这些路由，以便正确配置防火墙，并且可以发送通过 Synchronizing Config with Azure（与 Azure 同步配置）按钮监控自动扩展阈值的指标。如果没有为中心模板堆栈填充路由，则遵循相同的过程。

   1. 登录到 Panorama，然后选择 **Network**（网络）。
   2. 在 **Template**（模板）下拉列表中选择与中心防火墙 VMSS 相关联的模板堆栈。
   3. 选择 **Virtual Router**（虚拟路由器），然后选择虚拟路由器。
   4. 选择 **Static Routes**（静态路由），然后确认显示两个路由。

   5. 选择 **Device**（设备）> **VM-Series**（**VM** 系列），然后查看 **Azure Instrumentation Key**（**Azure** 检测密钥）的值。

   如果没有显示静态路由或 *Azure* 检测密钥，请单击 *Panorama* > *Plugins*（插件）> *Azure* > *AutoScaling*（自动扩展），然后单击与您要更新的自动扩展定义相对应的 *Synchronizing Config with Azure*（与 *Azure* 同步配置）链接。
4. 确认可以使用静态路由将返回流量从互联网定向回到应用程序。

   在 Panorama 上，与中心防火墙的模板堆栈相关联的虚拟路由器必须拥有可将返回流量定向到应用程序工作负载的静态路由。当您在应用程序 VNet 中使用以下命令标记内部负载均衡器时，将自动创建此静态路由

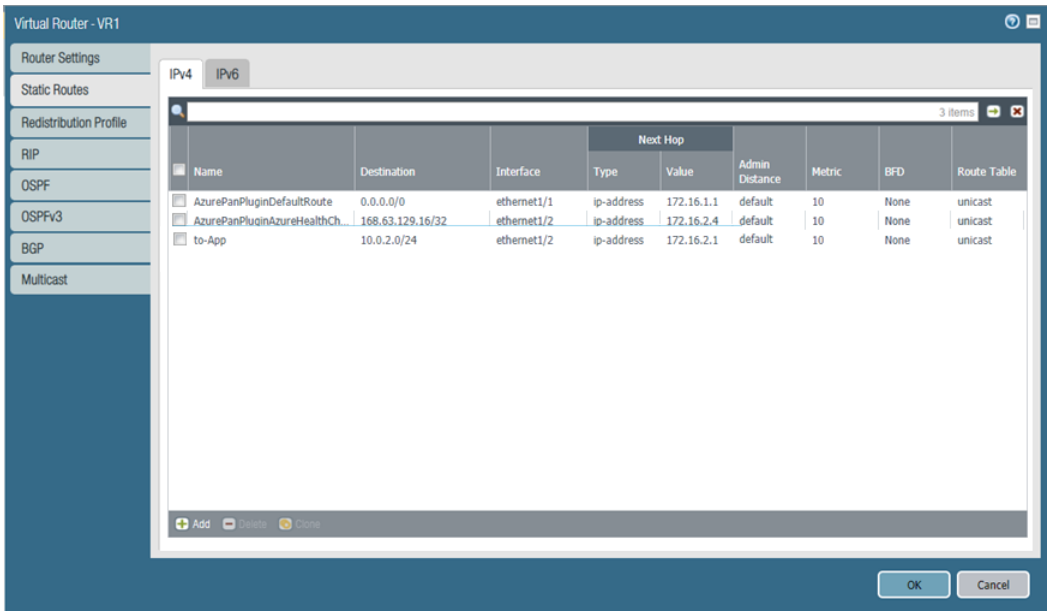
   ```
   HubRG-<Name of the Hub Firewall Resource Group>
   ```

   否则，您必须按如下所示添加静态路由。

   1. 登录到 Panorama，然后选择 **Network**（网络）。

© 2019 Palo Alto Networks, Inc.

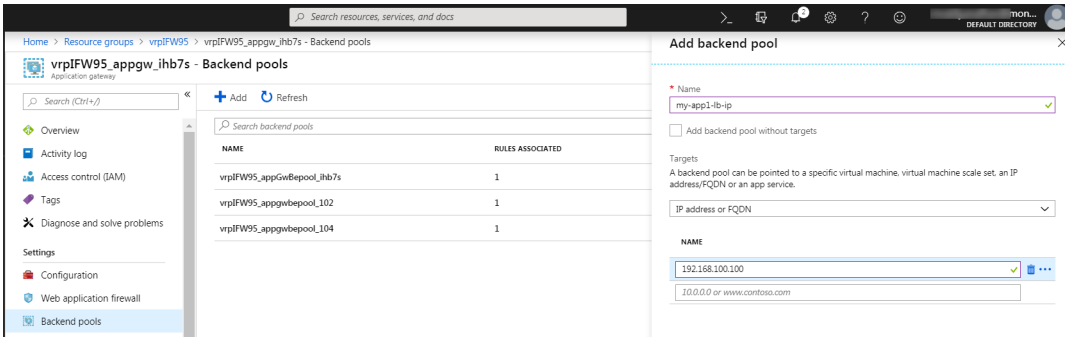
2. 在 **Template**（模板）下拉列表中选择与中心防火墙 VMSS 相关联的模板堆栈。
3. 选择 **Virtual Router**（虚拟路由器），然后选择您要配置的虚拟路由器。
4. 选择 **Static Routes**（静态路由），添加具有目标 IP 地址作为应用程序子网的路由，并将传出接口设置为防火墙上的可信接口，以及设置面向应用程序资源组中应用程序工作负载的内部负载均衡器的下一个跃点 IP 地址。



入站模板将公用 *IP* 地址分配给 *VMSS PA-VM* 管理接口。确保在模板中配置网络安全组入站源 *IP* 地址。

STEP 7 | 要载入应用程序，请在入站防火墙资源组中完成以下操作。

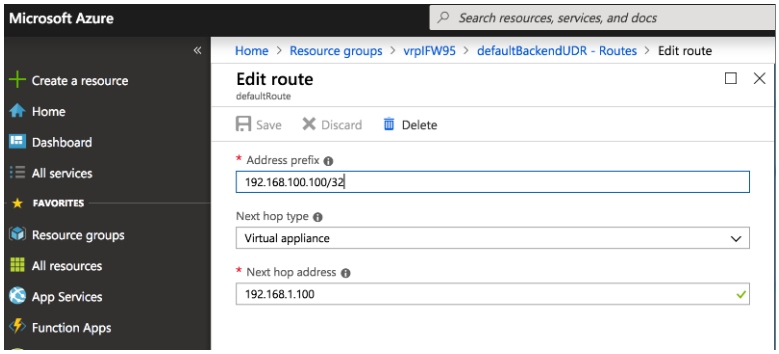
1. 访问应用程序网关。
2. 将样本应用程序的负载均衡器 IP 地址添加到应用程序网关后端池。



3. 将路由添加到 defaultBackendUDR，以通过防火墙将流量定向到要保护的应用程序。

   您需要添加路由，该路由可以指定启动应用程序模板时创建的应用程序网关的内部负载均衡器 IP 地址的地址前缀，并且下一个跃点 IP 地址应与面向入站防火墙资源组中 VM 系列防火墙 VMSS 的负载均衡器 IP 地址相匹配。此路由可让应用程序网关在将流量路由到应用程序资源组中的负载均衡器之前将其发送到入站防火墙 VMSS。

© 2019 Palo Alto Networks, Inc.



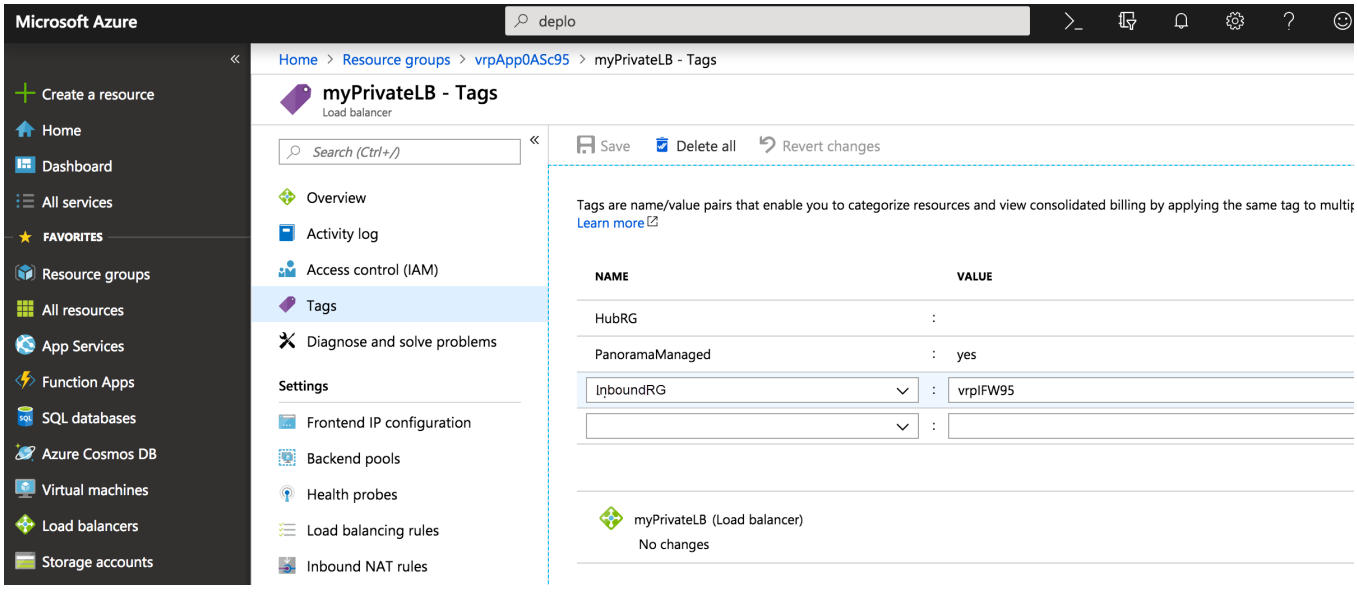
如果您拥有自己的应用程序，并且要对其进行配置以使用通过中心或防火墙模板部署的 *VM* 系列防火墙来保护流量，则必须执行以下操作：

- 设置应用程序 *VNet* 与在其中部署防火墙 *VMSS* 的 *VNet* 之间的 *VNET* 对等。

  如果您要保护入站和出站应用程序流量，请在 *Azure* 门户上选择应用程序的虚拟网络，并确认中心和入站防火墙 *VNet* 的连接为 *VNet* 对等状态。

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
jpasapprg-vnet-jpashubrg-vnetvnet-peering	Connected	jpashubrg-vnet	Enabled
jpasapprg-vnet-inbound-fw-vnetvnet-peering	Connected	inbound-fw-vnet	Enabled

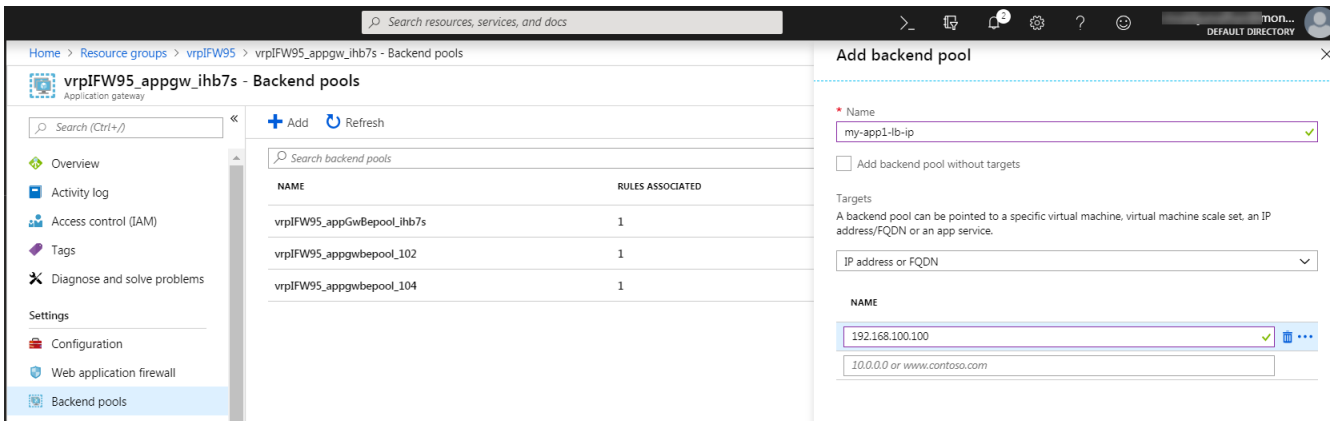
- 将面向应用程序的内部负载均衡器的 *IP* 地址添加到入站防火墙资源组中的应用程序网关配置。
- 将路由添加到 *defaultBackend UDR* 表以引导流量通过防火墙。您需要添加可以指定面向应用程序的负载均衡器的 *IP* 地址的路由，并指定面向防火墙 *VMSS* 的 *IP* 地址负载均衡器作为下一个跃点。此路由可让应用程序网关在将流量路由到应用程序资源组中的负载均衡器之前将其发送到防火墙 *VMSS*。
- 将以下标记添加到面向应用程序工作负载的内部负载均衡器。
  - *HubRG*：输入中心防火墙资源组的名称
  - *PanoramaManaged*：是
  - *InboundRG*：输入入站防火墙资源组的名称



© 2019 Palo Alto Networks, Inc.

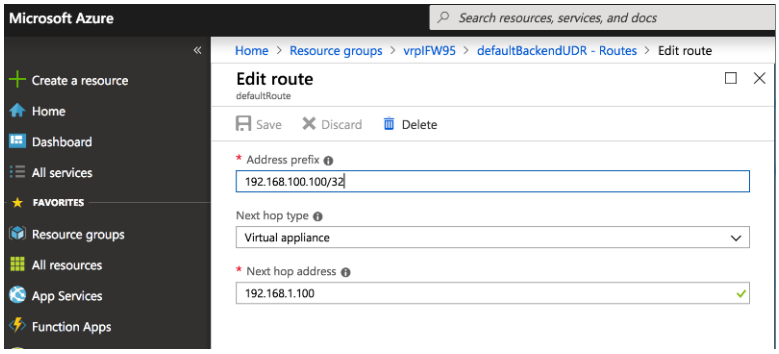
STEP 8 | 要载入应用程序，请在中心防火墙资源组中完成以下操作。

1. 访问应用程序网关。
2. 将样本应用程序的负载均衡器 IP 地址添加到应用程序网关后端池。



3. 将路由添加到 defaultBackendUDR，以通过防火墙将流量定向到要保护的应用程序。

   您需要添加路由，该路由可以指定启动应用程序模板时创建的应用程序网关的内部负载均衡器 IP 地址的地址前缀，并且下一个跃点 IP 地址应与面向入站防火墙资源组中 VM 系列防火墙 VMSS 的负载均衡器 IP 地址相匹配。此路由可让应用程序网关在将流量路由到应用程序资源组中的负载均衡器之前将其发送到入站防火墙 VMSS。



如果您拥有自己的应用程序，并且要对其进行配置以使用通过中心或防火墙模板部署的 *VM* 系列防火墙来保护流量，则必须执行以下操作：

- 设置应用程序 *VNet* 与在其中部署防火墙 *VMSS* 的 *VNet* 之间的 *VNET* 对等。

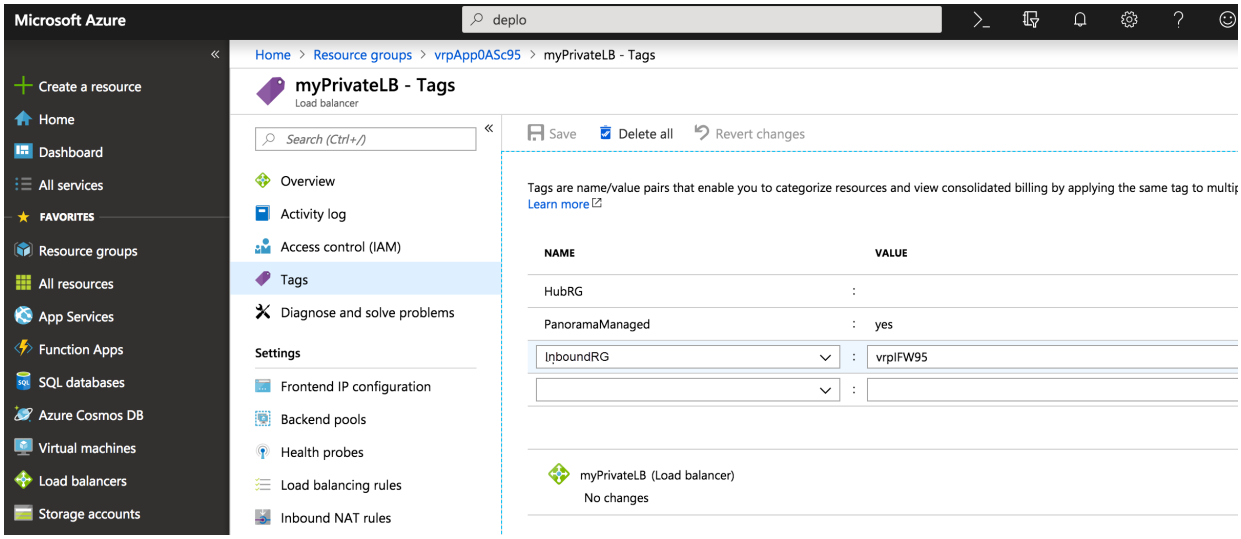
  如果您要保护入站和出站应用程序流量，请在 *Azure* 门户上选择应用程序的虚拟网络，并确认中心和入站防火墙 *VNet* 的连接为 *VNet* 对等状态。

NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
jpasapprg-vnet-jpashubrg-vnetvnet-peering	Connected	jpashubrg-vnet	Enabled
jpasapprg-vnet-inbound-fw-vnetvnet-peering	Connected	inbound-fw-vnet	Enabled

- 将面向应用程序的内部负载均衡器的 *IP* 地址添加到入站防火墙资源组中的应用程序网关配置。
- 将路由添加到 *defaultBackend UDR* 表以引导流量通过防火墙。您需要添加可以指定面向应用程序的负载均衡器的 *IP* 地址的路由，并指定面向防火墙 *VMSS* 的 *IP* 地址负载均衡器作为下一个跃点。此路由可让应用程序网关在将流量路由到应用程序资源组中的负载均衡器之前将其发送到防火墙 *VMSS*。
- 将以下标记添加到面向应用程序工作负载的内部负载均衡器。

© 2019 Palo Alto Networks, Inc.

- *HubRG*：输入中心防火墙资源组的名称
- *PanoramaManaged*：是
- *InboundRG*：输入入站防火墙资源组的名称



STEP 9 | 在 Panorama 上，创建安全策略规则。

为了保护入站应用程序流量，您可以将源区域和目标区域指定为任何区域，以及添加目标 IP 地址作为动态地址组对象，并在安全策略规则中引用。

Azure 自动扩展模板中的参数

本节介绍在部署模板资源时需要提供作为输入的值，使您可以使用应用程序工作负载在 Azure 上自动扩展 VM 系列防火墙。

- 基础架构模板参数
- 入站防火墙模板参数
- 中心模板参数
- 应用程序模板参数

基础架构模板参数

基础架构模板输入如下：

- Panorama 插件消息处理程序名称 — 将消息传递到适用于 Azure 的 Panorama 插件的 Azure Function 的名称。Azure function URL 将以该名称开头。
- 存储帐户类型 — 选择要使用的类型。
- 存储库 URL — 托管模板的父 GitHub 存储库的 URL。Palo Alto Networks 发布这些模板的位置为：https://github.com/PaloAltoNetworks/azure-autoscaling/tree/master/Version-1-0
- 分支 — 保持原样。
- Azure Service Bus 名称 — Panorama 从 Azure 订阅通知的 Azure Service Bus 的名称。该值长度必须在 6 到 50 个字符之间。该名称必须是全局唯一的，必须以字母或数字开头和结尾，并且只能包含字母、数字和连字符。

© 2019 Palo Alto Networks, Inc.

入站防火墙模板参数

入站防火墙模板输入会有所不同，具体取决于您是从头开始还是使用模板进行绿色字段部署，或者您是否拥有具有 Azure 应用程序网关的现有 VNet，并且想要为 VMSS 部署 VM 系列防火墙以及关联的子网和内部负载均衡器。

- 绿色字段部署的输入
- 棕色字段部署的输入

绿色字段部署的入站防火墙模板输入如下：

- 资源组名称和位置 — 创建新资源组并选择位置。
- 应用程序网关 DNS 名称 — Azure 应用程序网关的名称。
- 网络安全组入站源 IP 地址：限制对防火墙管理接口的入站访问。CIDR 格式，例如：199.16.5.122/32。
- 防火墙负载均衡器 IP 地址：输入来自不可信子网 CIDR 的 IP 地址，以分配面向防火墙 VMSS 的 Azure 负载均衡器。Azure 应用程序网关将使用此 IP 地址将流量继续转发到防火墙。例如：192.168.1.4
- 部署到现有 Vnet — 否

  将为您部署具有入站防火墙模板中列出的所有组件的新 VNet。请参阅在 Azure 上自动扩展 — 组件和规划清单。
- virtualNetworkName — 要在其中部署此模板中资源的 VNet 的名称。
- virtualNetworkAddressPrefix — 例如：192.168.0.0/21
- mgmtSubnetPrefix — 例如：192.168.0.0/24
- untrustSubnetPrefix — 例如：192.168.1.0/24
- trustSubnetPrefix — 例如：192.168.2.0/24
- appGatewaySubnetPrefix：例如：192.168.3.0/24
- vmSeriesFirewallModel：BYOL 或 PAYG 捆绑软件
- vmSeriesImageVersion：8.1 或 9.0。请参阅兼容性矩阵中的 Panorama 插件版本信息。

  如果您选择 PAN-OS 9.0，必须在 Panorama 上安装 VM 系列插件。有关详细信息，请参阅 在 Azure 上自动扩展 — 组件和规划清单。
- vmSeriesFirewallVmSize：Standard_D3_v2（默认）。有关 Azure 上的 VM 系列防火墙的最低系统要求，请参阅 VM 实例类型；有关您所在区域的可用实例类型列表，请参阅 Azure 虚拟机。
- 用户名 — 输入用于登录到防火墙 Web 界面的用户名。
- 身份验证类型：密码或 SSH 密钥
- 引导存储帐户 — 输入存储帐户的名称。
- 引导存储帐户访问密钥 — 指定存储帐户密钥。
- bootstrapFileShare — 包含引导文件夹结构的文件共享的名称。
- bootstrapSharedDir — 此目录名称是可选的。
- VM 规模集最小计数 — 输入一个介于 1 到 3 之间的值。默认值为 1。
- VM 规模集最大计数 — 输入一个介于 1 到 3 之间的值。默认值为 1。
- 自动扩展指标 — 主动会话（默认）。要查看所有支持的指标，请参阅发布用于监控的自定义 PAN-OS 指标。
- scaleInThreshold — 输入扩展事件的阈值。此输入可以是基于您在上面选择的扩展指标的数字或百分比。
- scaleOutThreshold — 输入扩展事件的阈值。此输入可以是基于您在上面选择的扩展指标的数字或百分比。
- Panorama 插件消息处理程序 URL：这是在基础架构模板中输入的 Azure Function 的名称。此 URL 允许 Azure Service Bus 队列和适用于 Azure 的 Panorama 插件发送有关 Azure 资源的消息。例如：https://test-asc-function-handler.azurewebsites.net/api/infra?code=IKDDx5U2HddsabcdE==

棕色字段部署的入站防火墙模板输入如下：

- 资源组名称和位置 — 创建新资源组并选择位置。

© 2019 Palo Alto Networks, Inc.

- 应用程序网关 DNS 名称 — 保留默认值。在棕色字段部署中，此模板假设您已部署应用程序网关，因此该值不相关。
- 网络安全组入站源 IP 地址：限制对防火墙管理接口的入站访问。CIDR 格式，例如：199.16.5.122/32。
- 防火墙负载均衡器 IP 地址：输入来自不可信子网 CIDR 的 IP 地址，以分配面向防火墙 VMSS 的 Azure 负载均衡器。Azure 应用程序网关将使用此 IP 地址将流量继续转发到防火墙。例如：192.168.1.4
- 部署到现有 Vnet — 是
- virtualNetworkName — 要在其中部署防火墙 VMSS 资源的现有 VNet 的名称。
- virtualNetworkAddressPrefix — 例如：192.168.0.0/21
- mgmtSubnetPrefix — 例如：192.168.0.0/24
- untrustSubnetPrefix — 例如：192.168.1.0/24
- trustSubnetPrefix — 例如：192.168.2.0/24
- appGatewaySubnetPrefix：输入在其中部署应用程序网关的子网。例如：192.168.3.0/24
- vmSeriesFirewallModel：BYOL 或 PAYG 捆绑软件
- vmSeriesImageVersion：8.1 或 9.0。

  如果您选择 PAN-OS 9.0，必须在 Panorama 上安装 VM 系列插件。有关详细信息，请参阅 在 Azure 上自动扩展 — 组件和规划清单。
- vmSeriesFirewallVmSize：Standard_D3_v2（默认）。有关 Azure 上的 VM 系列防火墙的最低系统要求，请参阅 VM 实例类型；有关您所在区域的可用实例类型列表，请参阅 Azure 虚拟机。
- 用户名 — 输入用于登录到防火墙 Web 界面的用户名。
- 身份验证类型：密码或 SSH 密钥
- 引导存储帐户 — 输入存储帐户的名称。
- 引导存储帐户访问密钥 — 指定存储帐户密钥。
- bootstrapFileShare — 包含引导文件夹结构的文件共享的名称。
- bootstrapSharedDir — 此目录名称是可选的。
- VM 规模集最小计数 — 输入一个介于 1 到 3 之间的值。默认值为 1。
- VM 规模集最大计数 — 输入一个介于 1 到 3 之间的值。默认值为 1。
- 自动扩展指标 — 主动会话（默认）。要查看所有支持的指标，请参阅发布用于监控的自定义 PAN-OS 指标。
- scaleInThreshold — 输入扩展事件的阈值。此输入可以是基于您在上面选择的扩展指标的数字或百分比。
- scaleOutThreshold — 输入扩展事件的阈值。此输入可以是基于您在上面选择的扩展指标的数字或百分比。
- Panorama 插件消息处理程序 URL：这是在基础架构模板中输入的 Azure Function 的名称。此 URL 允许 Azure Service Bus 队列和适用于 Azure 的 Panorama 插件发送有关 Azure 资源的消息。例如：https://test-asc-function-handler.azurewebsites.net/api/infra?code=IKDDx5U2HddsabcdE==

中心模板参数

通过如下中心防火墙模板输入，您可以保护应用程序层之间的出站流量和东向西流量：

- virtualNetworkName — 要在其中部署此模板中资源的 VNet 的名称。
- virtualNetworkAddressPrefix —
- mgmtSubnetPrefix —
- untrustSubnetPrefix —
- trustSubnetPrefix —
- 负载均衡器 IP 地址 — 输入来自可信子网 CIDR 的 IP 地址。负载均衡器将使用此 IP 地址将流量发送到防火墙上的可信接口。
- 网络安全组入站源 IP 地址：限制对防火墙管理接口的入站访问。CIDR 格式，例如：199.16.5.122/32。
- 引导存储帐户 — 输入存储帐户的名称。
- 引导存储帐户访问密钥 — 指定存储帐户密钥。
- bootstrapFileShare — 包含引导文件夹结构的文件共享的名称。

© 2019 Palo Alto Networks, Inc.

- bootstrapSharedDir — 此目录名称是可选的。
- VM 规模集最小计数 — 输入一个介于 1 到 3 之间的值。默认值为 1。
- VM 规模集最大计数 — 输入一个介于 1 到 3 之间的值。默认值为 1。
- 自动扩展指标 — 主动会话（默认）。要查看所有支持的指标，请参阅发布用于监控的自定义 PAN-OS 指标。
- scaleInThreshold — 输入扩展事件的阈值。此输入可以是基于您在上面选择的扩展指标的数字或百分比。
- scaleOutThreshold — 输入扩展事件的阈值。此输入可以是基于您在上面选择的扩展指标的数字或百分比。
- Panorama 插件消息处理程序 URL：这是在基础架构模板中输入的 Azure Function 的名称。此 URL 允许 Azure Service Bus 队列和适用于 Azure 的 Panorama 插件发送有关 Azure 资源的消息。例如：https://test-asc-function-handler.azurewebsites.net/api/infra?code=IKDDx5U2HddsabcdE==

应用程序模板参数

应用程序模板输入为：

- 连接到中心：是或否。
- 中心资源组名称 — 只有在为是时需要。托管您使用中心防火墙模板部署的资源的资源组的名称。
- 中心 VNET 名称 — 只有在为是时需要。托管您使用中心防火墙模板部署的资源的 VNet 的名称。
- 中心负载均衡器 IP 地址 — 只有在为是时需要。这是您已在启动中心防火墙模板时分配给负载均衡器的 IP 地址。
- 应用程序负载均衡器 IP 地址 — 输入属于可信子网的 IP 地址。入站防火墙资源组中的应用程序网关将使用此 IP 地址将流量发送到防火墙，然后再发送到应用程序工作负载。
- 入站防火墙资源组名称 —
- 入站防火墙 VNet 名称 —
- virtualNetworkAddressPrefix — 要在其中部署此模板中资源的 VNet 的 CIDR。
- virtualNetworkName — 要在其中部署此模板中资源的 VNet 的名称。
- mgmtSubnetPrefix —
- trustedSubnetPrefix —
- backendSubnetPrefix — 在其中部署应用程序工作负载的子网。
- 用户名 — 登录到示例应用程序服务器。
- 密码 — 您在上面输入的管理用户的密码。

© 2019 Palo Alto Networks, Inc.

在 Azure 上保护 Kubernetes 服务

要保护 Azure Kubernetes 服务，您必须先在 Panorama 上安装 Azure 插件，然后配置 Azure 自动扩展部署。适用于 Panorama 的 Azure 插件支持基于标记的 VM 监控和自动扩展，保护 Azure Kubernetes 服务 (AKS) 集群的入站流量，并监控来自 AKS 集群的出站流量。通过自动扩展模板，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，您必须先配置 Azure 自动扩展部署。Palo Alto Networks 的 Azure 自动扩展模板与 Azure 服务和组件一起用于收集有关网络和资源的信息，然后为绿色字段或棕色字段部署创建 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。
- Azure 自动扩展模板版本 1.0 — 要支持 AKS，请使用此模板在支持 AKS 的 Azure 区域中创建自动扩展部署。
- Azure AKS 模板版本 1.0。此模板用于创建 AKS 集群。

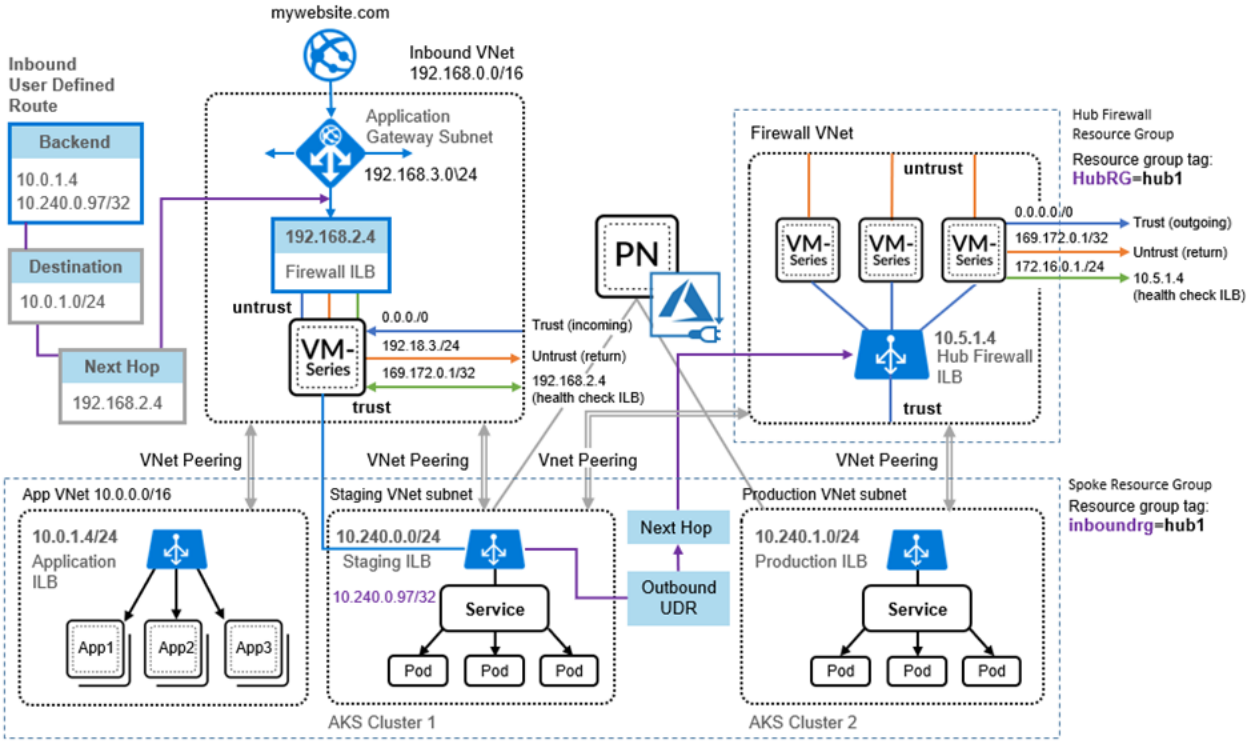
  您必须为集群启用 AKS 高级网络 (CNI)。

  AKS 部署需要高级网络配置星型 VNet 的 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。

© 2019 Palo Alto Networks, Inc.



- 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。
- **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

© 2019 Palo Alto Networks, Inc.

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。

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
```


© 2019 Palo Alto Networks, Inc.

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。

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受管防火墙。

- 准备工作

© 2019 Palo Alto Networks, Inc.

- 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，您必须先部署 GitHub 上可用的 Azure 自动扩展解决方案。

要保护在 Kubernetes 集群内作为服务运行的 Web 应用程序，您必须计划 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。

- 按照“在 Azure 上自动扩展 VM 系列防火墙”中的说明，并查看“适用于 Azure 的 Panorama 插件如何保护 Kubernetes 服务？”。
- 您必须拥有 AKS 高级网络才能使用 Palo Alto Networks AKS 模板。
- 在部署 AKS 集群之前，应设计 AKS 子网。请查看保护 AKS 集群的简单星型拓扑和 AKS 集群通信。
  - 该模板将创建单个 AKS 集群（服务）作为示例。您必须指定 VNet、VNet 子网和服务的 CIDR 范围。CIDR 范围不得重叠。
  - 根据您的要求调整子网大小。避免不必要的大范围，因为它们可能会影响性能。
  - 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。
- 计划您要如何对等 VNet。如果要对等 AKS 集群，请确保您已阅读 AKS 集群通信。
- 考虑您要标识流量的方式。
  - 如果您计划在出站 AKS 流量上使用动态址，请参阅将子网地址组添加到顶级策略。
  - 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。

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：

© 2019 Palo Alto Networks, Inc.

```
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。
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
```

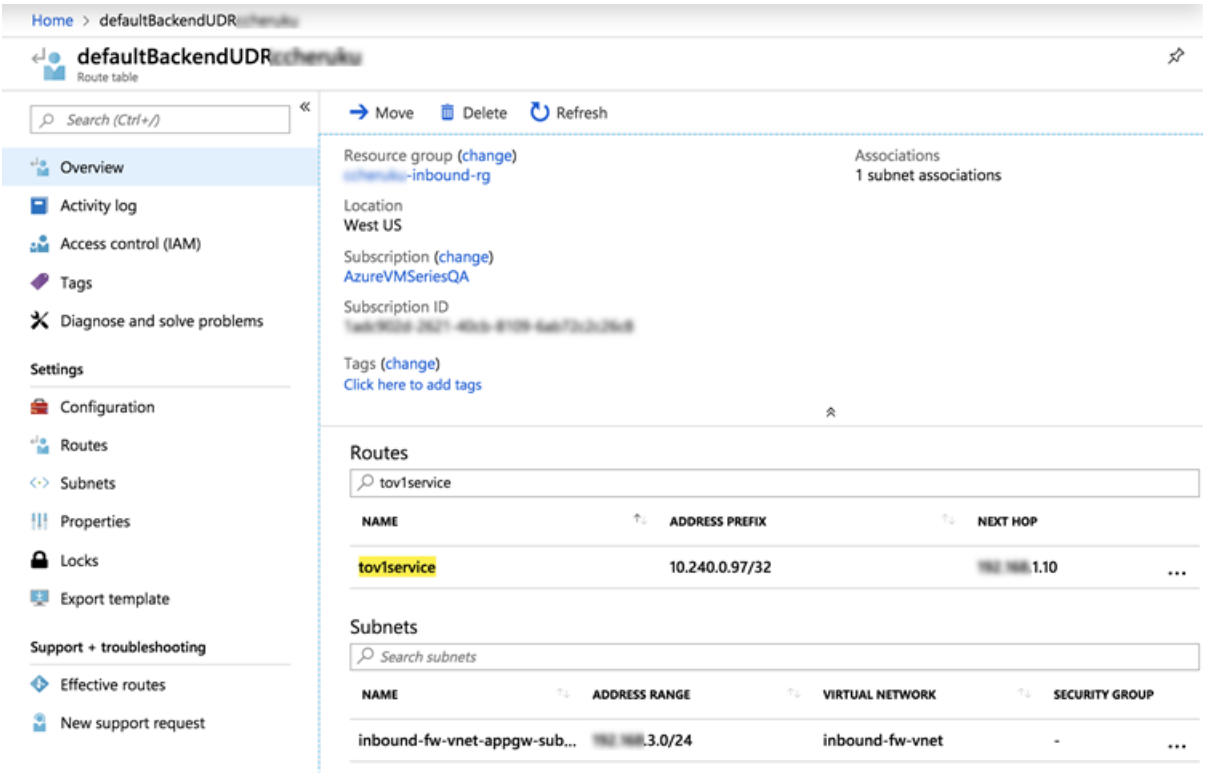
```
NAME               TYPE           CLUSTER-IP     EXTERNAL-IP    PORT(S)          AGE     SELECTOR
azure-vote-back    ClusterIP      10.0.77.21     <none>         6379/TCP         2d23h   app=azure-vote-back
azure-vote-front   LoadBalancer   10.0.18.189    10.240.0.97    80:31937/TCP     2d23h   app=azure-vote-front
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。

© 2019 Palo Alto Networks, Inc.



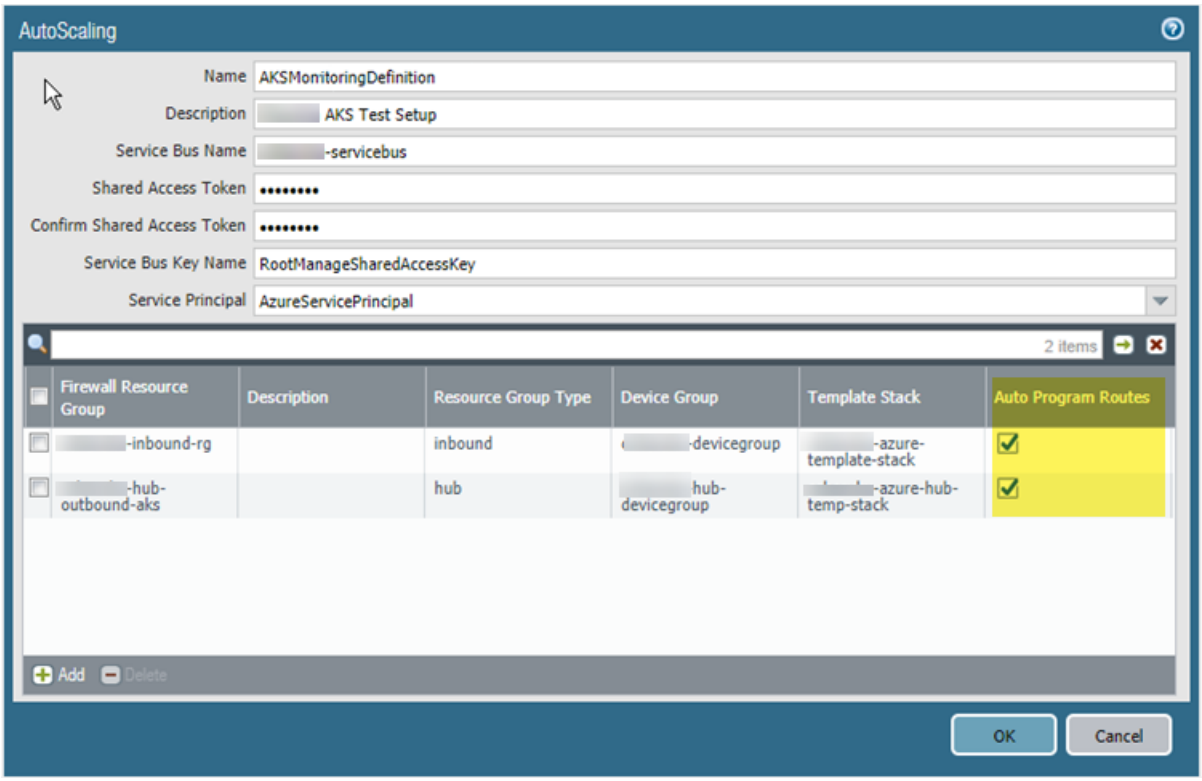
在适用于 *Panorama* 的 *Azure* 插件中连接 *AKS* 集群

该任务假设您已部署自动扩展解决方案，并且已创建模板、模板堆栈和设备组。

有关填写每个表单的更多信息，请参阅 Panorama 在线帮助。

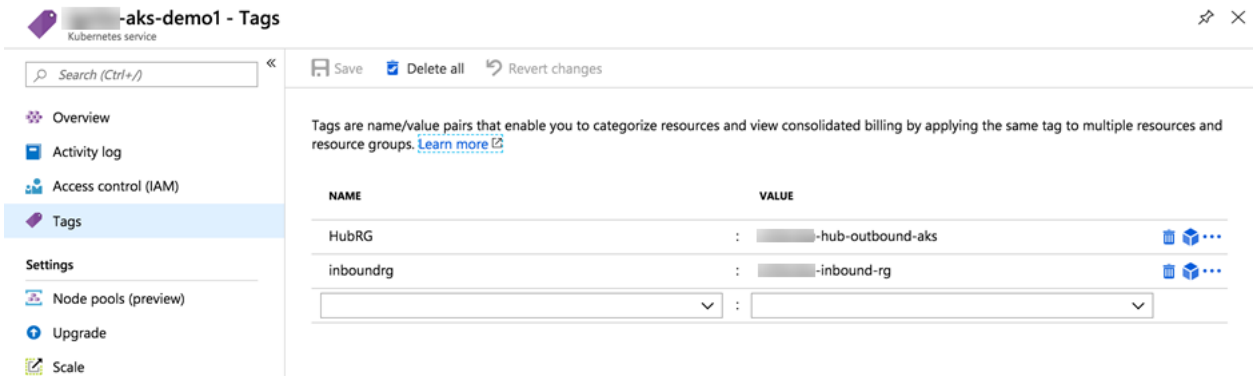
STEP 1 | 选择 **Panorama** > **Azure** > **AutoScaling**（自动扩展），以查看在配置自动扩展时创建的自动扩展定义。如下所示，如果已启用 **Auto Program Routes**（自动编程路由），则会为您编程防火墙路由。

© 2019 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 Panorama 的 Azure 自动扩展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。

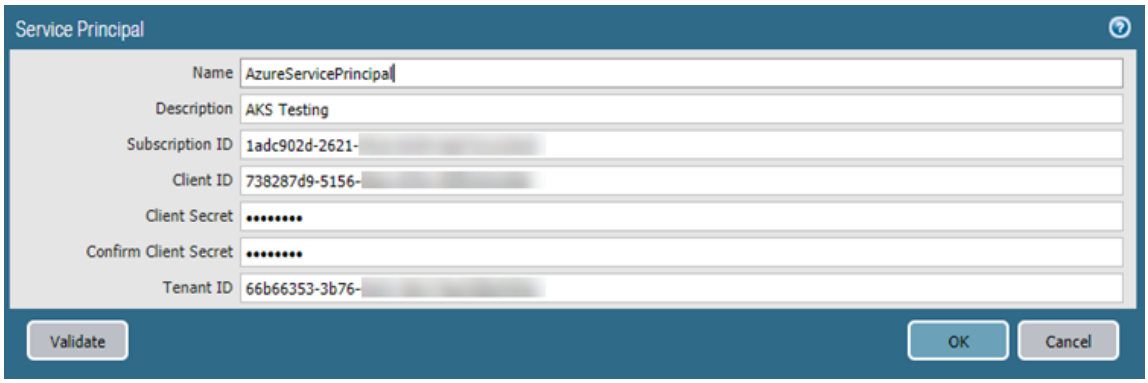
STEP 3 | 在 Panorama 中，选择 **Panorama** > **Azure** > **Setup**（设置）。

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。

© 2019 Palo Alto Networks, Inc.

3. 在 **Service Principal**（服务主体）选项卡上，**Add**（添加）并 **Validate**（验证）服务主体。

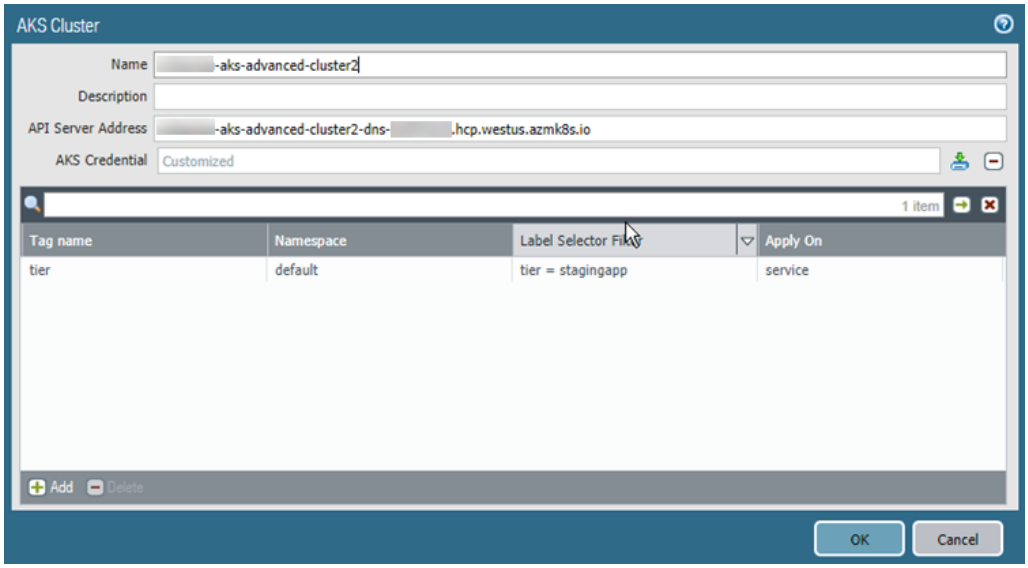
   使用您在配置自动扩展时创建的服务主体。



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。

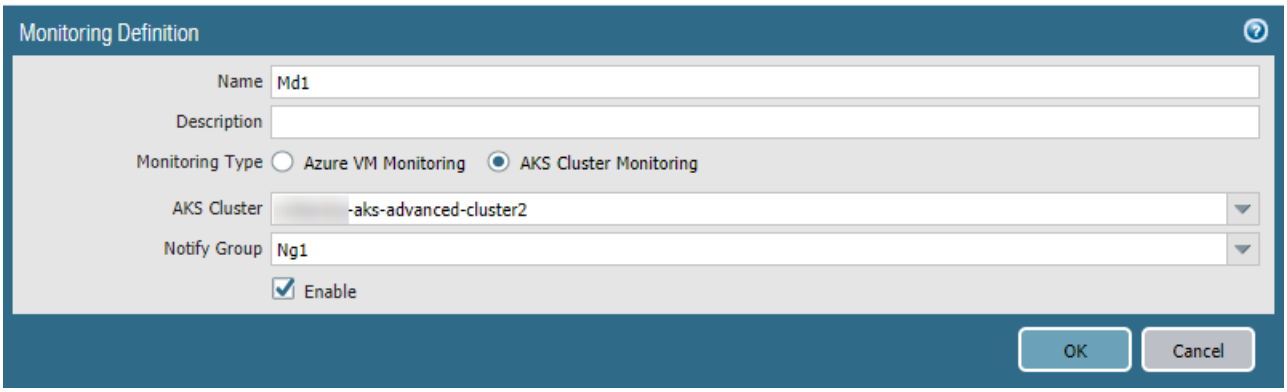
   如果服务名称或标记在整个命名空间中不是唯一，请使用标签选择器同时筛选标记和命名空间，以使其成为唯一。

© 2019 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？”中的图如何介绍入站 UDR。

STEP 1 | 创建 URL 路由规则以将 Web 流量重定向到合适的后端池。

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。

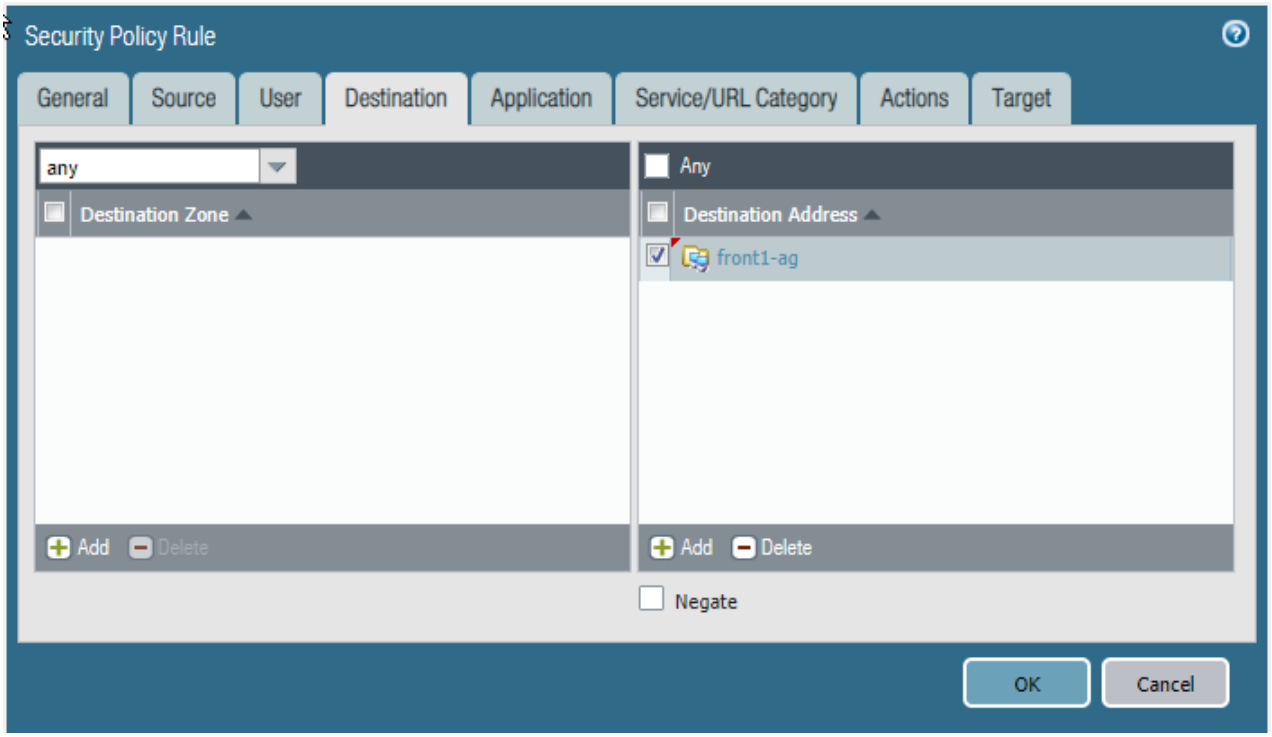
© 2019 Palo Alto Networks, Inc.

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
```


© 2019 Palo Alto Networks, Inc.

```
        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: 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"
```


© 2019 Palo Alto Networks, Inc.

```
    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
```

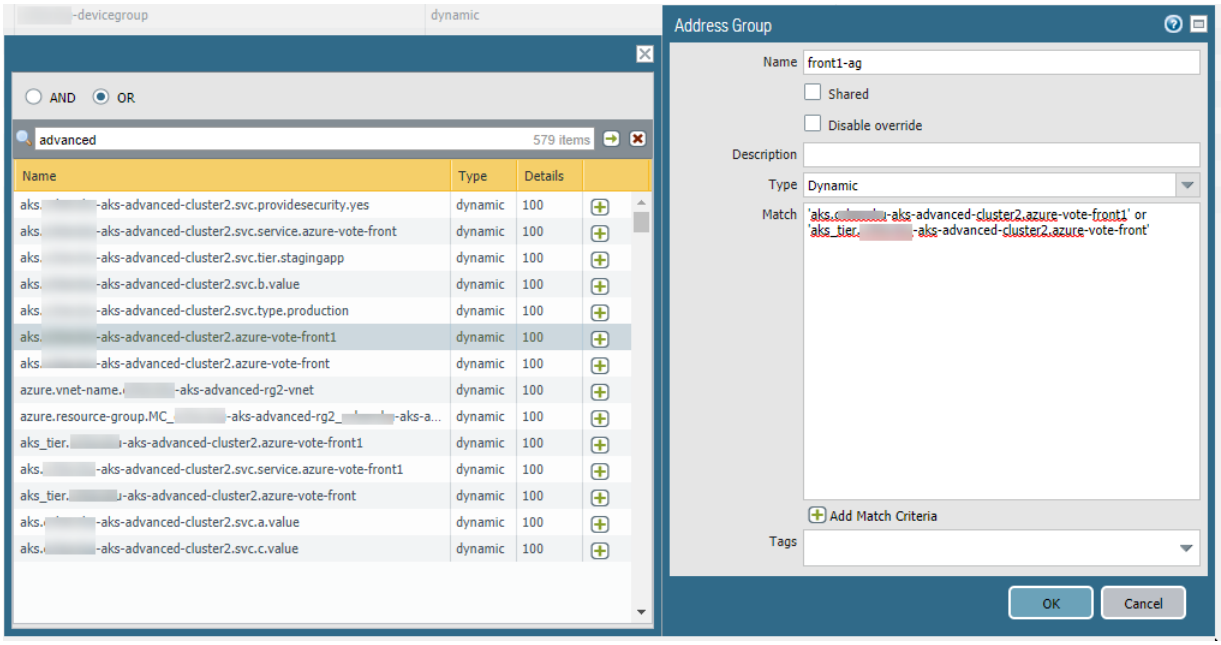
STEP 2 | 编辑 YAML 文件以标记 Kubernetes 服务。

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。

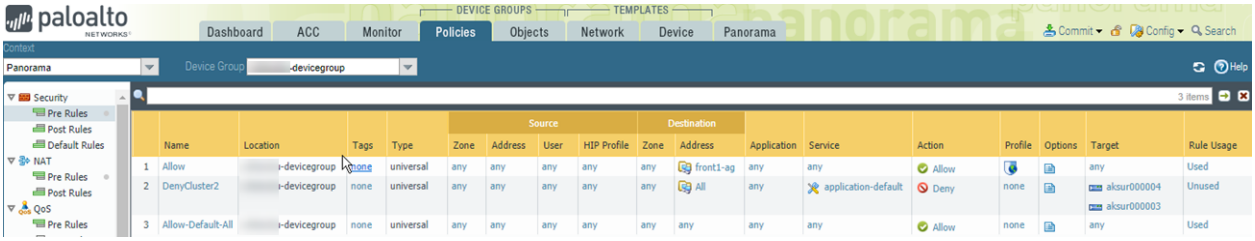
STEP 4 | 在 Panorama 中，使用资源组标记创建地址组。

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。

© 2019 Palo Alto Networks, Inc.

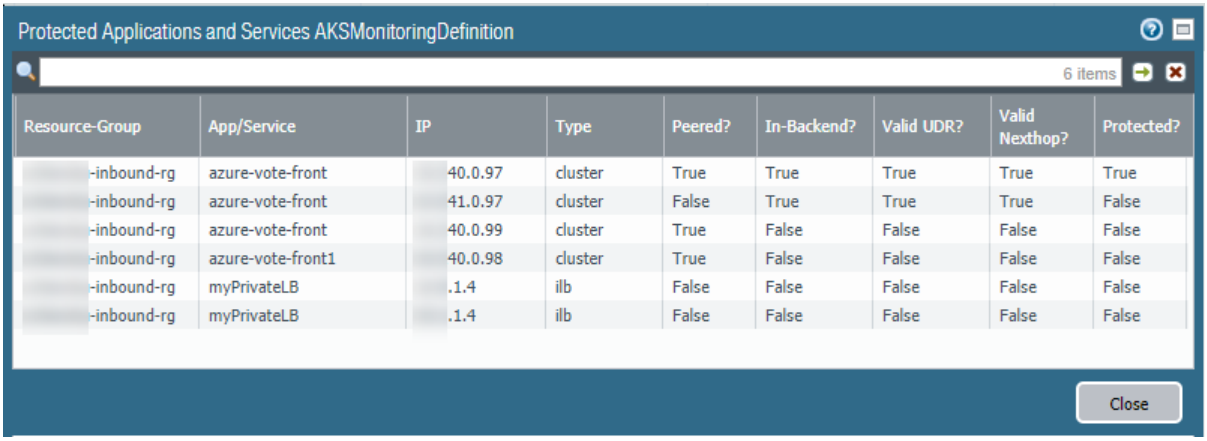


STEP 6 | 查看保护的 AKS 服务。

在 **Panorama** > **Azure** > **AutoScaling**（自动扩展）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。



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。

> 关于 Google Cloud Platform 上 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
> 从 Google Cloud Platform Marketplace 部署 VM 系列防火墙
> 使用自定义模板或 gcloud CLI 部署 VM 系列防火墙
> 在 VM 系列防火墙上启用 Google Stackdriver 监控
> 在 Google Stackdriver 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
> 在 Google Kubernetes 引擎群集中保护 Kubernetes 服务

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，可简化此过程。

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。

下表是推荐用于每个许可证的最低预定义标准机器类型。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。

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	包 1 和 2		
		PAYG	市场	推荐的预定义机器类型
VM-100 防火墙	✓			n1-standard-4
VM-200 防火墙	✓			
VM-300 防火墙	✓	✓	✓	
VM-1000-HV 防火墙	✓			
VM-500 防火墙	✓			n1-standard-8

© 2019 Palo Alto Networks, Inc.

容量	BYOL	包 1 和 2		
		PAYG	市场	推荐的预定义机器类型
VM-700 防火墙	✓			n1-standard-16

© 2019 Palo Alto Networks, Inc.

Google Cloud Platform 上支持的部署

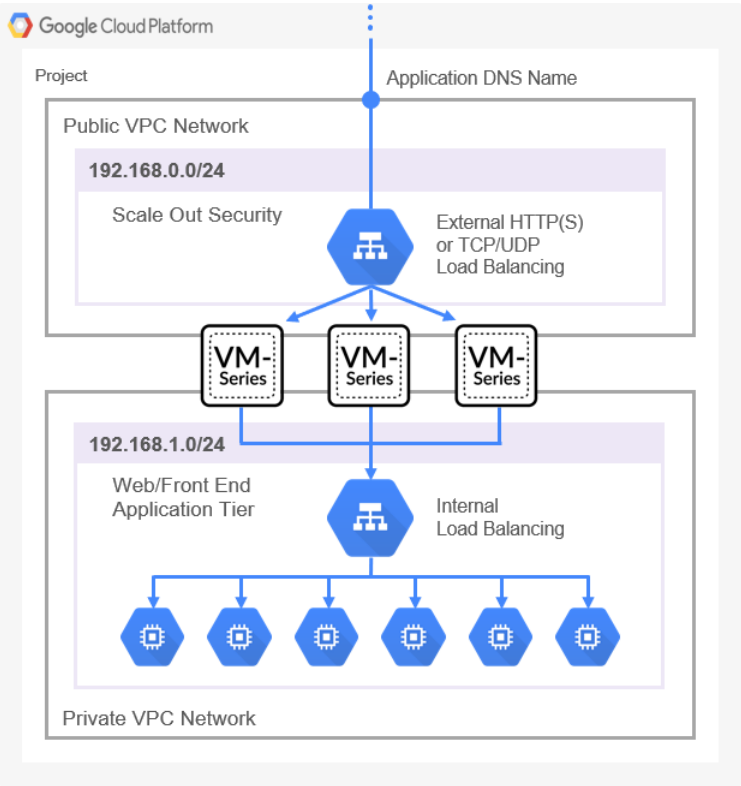
您可以在虚拟私有云 (VPC) 网络中的 Google® Compute Engine 实例上部署 VM 系列防火墙。部署类型包括：

- 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。

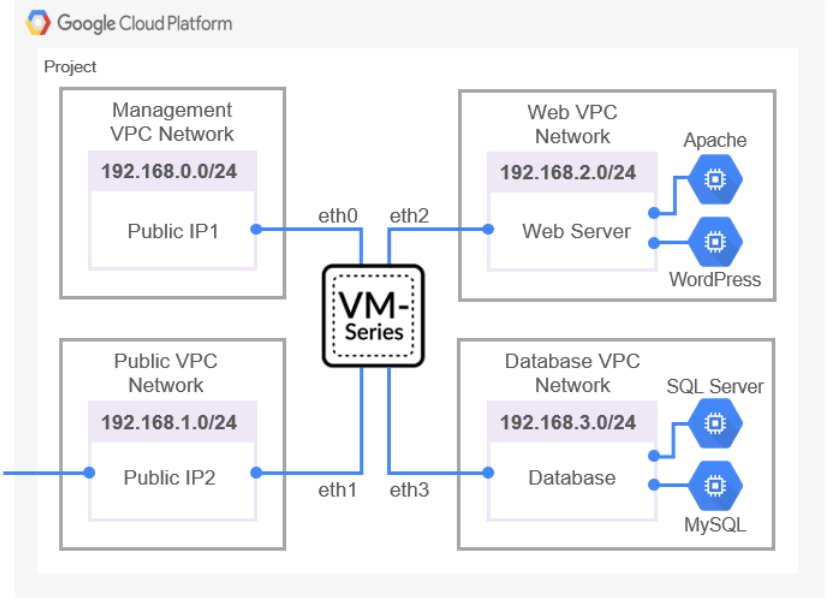
在公共云环境中，常见的做法是使用扩展架构（如下所示），而非性能更好的大型 VM。此架构（有时也称为三明治部署）可以避免单点故障，在必要时允许添加或移除防火墙。



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。

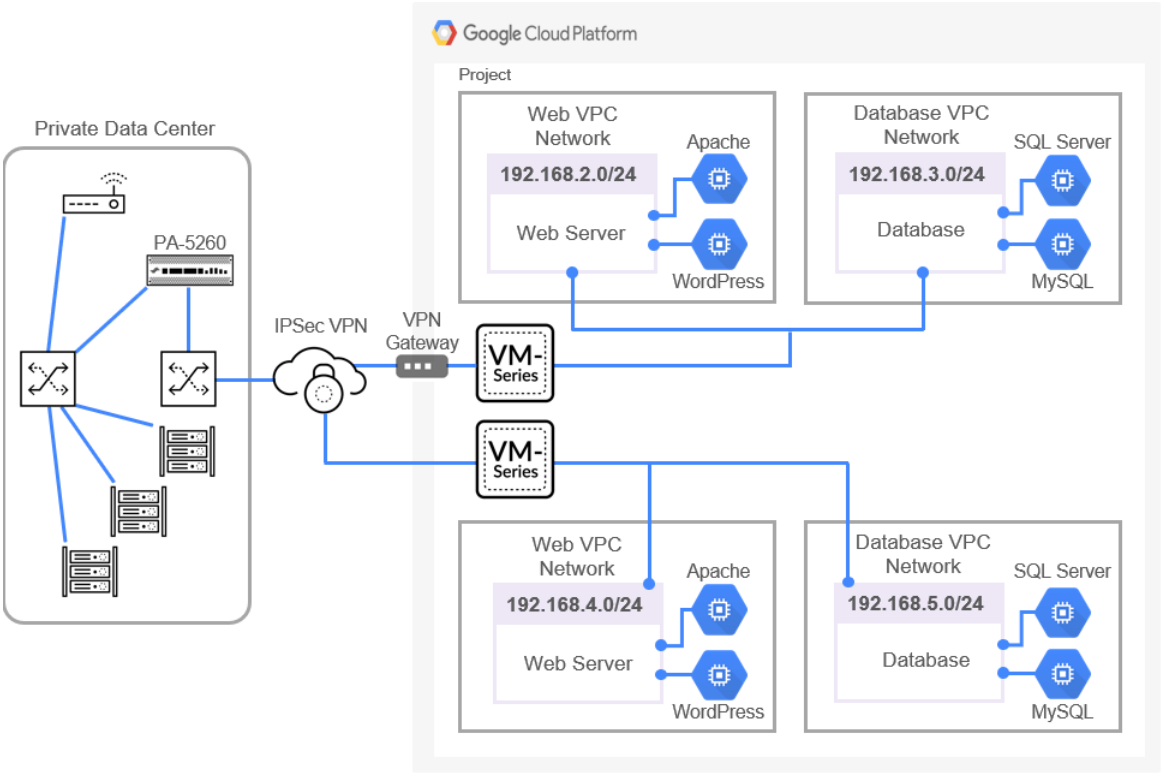
© 2019 Palo Alto Networks, Inc.



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。



© 2019 Palo Alto Networks, Inc.

在 Google Public Cloud 上准备设置 VM 系列防火墙

部署 Google Cloud Platform Marketplace 的 VM 系列防火墙的过程需要做好准备任务。部署前，必须创建项目网络和子网，并规划 VM 系列防火墙接口的网络和 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：

- Google Cloud Platform (GCP) 帐户规划
- 虚拟私有云 (VPC) 网络规划
- 网络接口规划

Google Cloud Platform (GCP) 帐户规划

查看这些要求，确保您在 Google Compute Engine (GCE) 实例上部署防火墙之前拥有正确的帐户和权限。

- 账户和权限
- 可用资源
- 身份验证方法
- SSH 密钥对

账户和权限

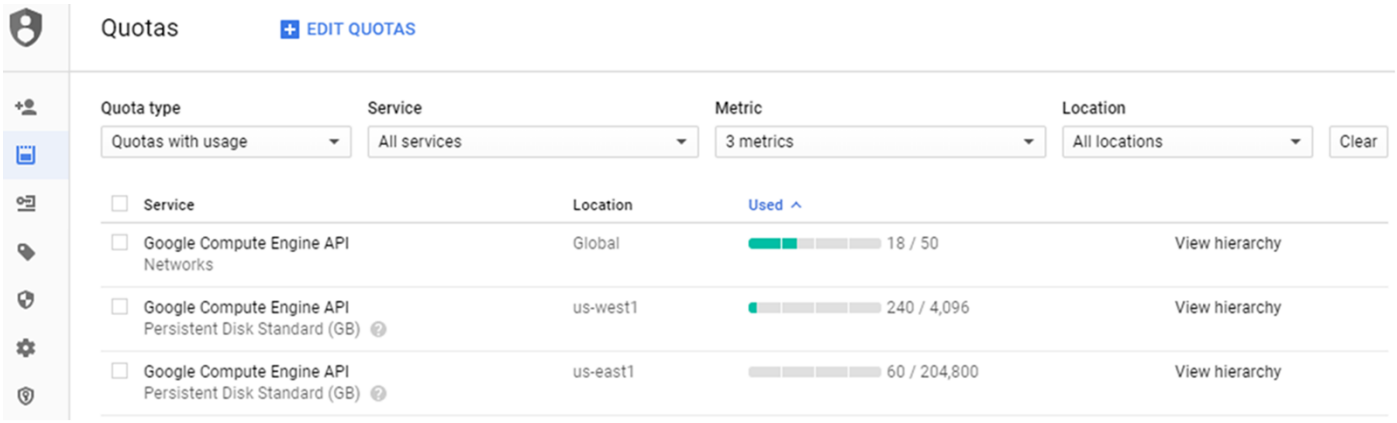
- 必须拥有一个带链接电子邮件地址的 GCP 用户账户，并且还必须知道此电子邮件地址的用户名和密码。
- 您以及您允许的任何用户均必须至少具有下列角色或等效的身份识别及访问管理 (IAM) 权限，以连接到 VM 系列防火墙：
  - Compute 查看器 — 允许您获取并列出 compute engine 资源，但无法读取存储在其中的数据。
  - 存储对象查看器 — 允许您使用同一项目中的 Google 存储桶进行引导。
  - 监控指标编写器 — Stackdriver 所需。

组织中的用户可能具有 IAM 权限或是比所需权限更大的预定义角色。必须适当地限制 *VM* 系列防火墙访问。

可用资源

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。

© 2019 Palo Alto Networks, Inc.



身份验证方法

GCP 可采用多种方法连接到实例。您可以使用服务账户或 SSH 密钥对进行身份验证。

- 服务账户 — 服务账户属于应用程序或 VM，并非最终用户。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连接到 VM 系列防火墙，则必须使用服务账户。例如，如果您想启用下一代物理防火墙监控您的 VM 系列防火墙，则必须将 VM 系列防火墙服务账户信息保存到 JSON 文件。在物理防火墙中，您可以在配置连接时上传文件。
- 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。部署后，在防火墙内使用 SSH 私钥配置管理员账户。要添加用户，请参阅管理防火墙管理员。

SSH 密钥对

VM 系列防火墙以不同于 *GCE* 实例的方式管理身份验证。首先，使用默认用户 ***admin*** 登录。

默认用户名仅接受一次。登录成功后，可以设置 VM 系列 Web 界面的管理员用户名和密码；请参阅从 Google Cloud Platform Marketplace 部署 VM 系列防火墙。

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。如果公钥损坏，则身份验证失败，您必须删除部署，从头来过。删除部署时，将保留所有网络和子网，当必须重新创建防火墙规则。

Marketplace 部署内的 **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。部署 VM 系列防火墙时，可以在 Marketplace 字段内添加 **admin:** 前缀。

© 2019 Palo Alto Networks, Inc.

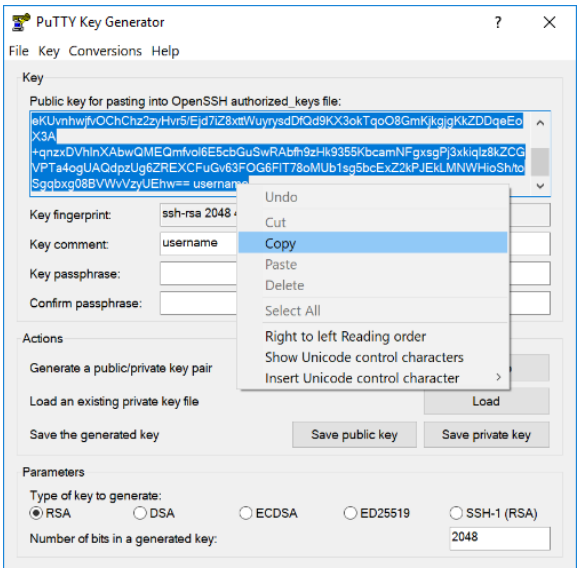
根据密钥生成器文件创建密钥。不得删除公钥文件。编辑引入非法字符的风险。

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。
   - 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。
2. 选择完整的公钥。
   - Linux 或 MacOS：

     打开文本编辑器中的公钥，并复制公钥。
   - 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。

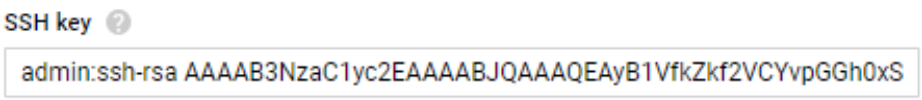
     在 PuTTYgen 中向下滚动，确保选择整个密钥，右键单击，然后选择 Copy（复制）。



3. 粘贴公钥。
   1. 在 Marketplace **SSH key**（**SSH** 密钥）字段，删除占位符文本和类型：

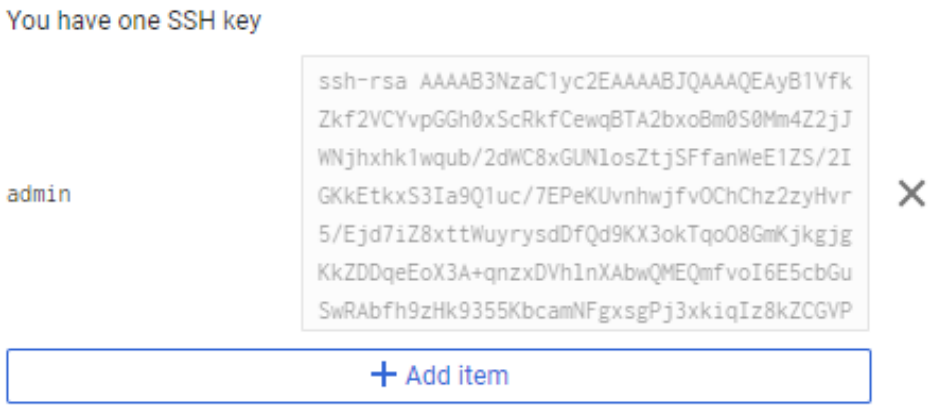
      `admin:`

      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。

4. 部署后，在尝试登陆到防火墙之前，查看管理实例，并检查密钥：

© 2019 Palo Alto Networks, Inc.



如果密钥看起来不正确（例如，有换行符），则必须将其替换。

1. 单击 **X** 删除密钥，然后单击 **+ Add item**（**+** 添加项目）。输入 **`admin:`**，并再次粘贴密钥。
2. 单击 **Save**（保存）以部署更新过的部署。

虚拟私有云 (VPC) 网络规划

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。必须先创建网络和子网，然后才开始从 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。

根据您的 VM 系列防火墙许可证，要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。

- **VPC 网络** — 您必须创建专用于每个 VM 系列防火墙接口的自定义网络。
  - 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三层接口。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。
- **IP 地址** — 您可以在创建接口子网时提供 IP 地址范围；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。此范围用于您的内部网络，因此，不能覆盖其他子网。
  - 部署时，您可以在创建网络接口时选择启用外部 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（请参阅升级临时外部 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。您可以根据 VM 上可用的计算资源定义数据层实例，请参阅面向公共云的 VM 系列防火墙许可证。

© 2019 Palo Alto Networks, Inc.

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。

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。除了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。

© 2019 Palo Alto Networks, Inc.

从 Google Cloud Platform Marketplace 部署 VM 系列防火墙

您可以使用 Google® Cloud Platform Marketplace 在 VM-300 容量许可证上部署 VM 系列防火墙。Cloud 提供的许可映像包括：

- 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，请参阅面向公共云的 VM 系列防火墙许可证 。

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。

STEP 1 | 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 2 | 单击 **Launch on Compute Engine**（在 **Compute Engine** 上启动）。

STEP 3 | 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. 选择区域。有关支持区域列表，请参阅地区和区域。
3. 根据 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用于许可证的 **Machine Type**（机器类型）。

STEP 4 | 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）— 如果计划使用引导文件，则使用引导数据包中规定的引导配置输入存储桶名称。
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。

© 2019 Palo Alto Networks, Inc.

- **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 5 | 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。

STEP 6 | 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 7 | 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 8 | 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 9 | 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。

STEP 10 | **Deploy**（部署）实例。

© 2019 Palo Alto Networks, Inc.

STEP 11 | 使用 Google Cloud Deployment Manager查看和管理您的部署。

STEP 12 | 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> configure
   ```
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# commit
   ```
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 13 | 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，则验证引导完成。

   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。

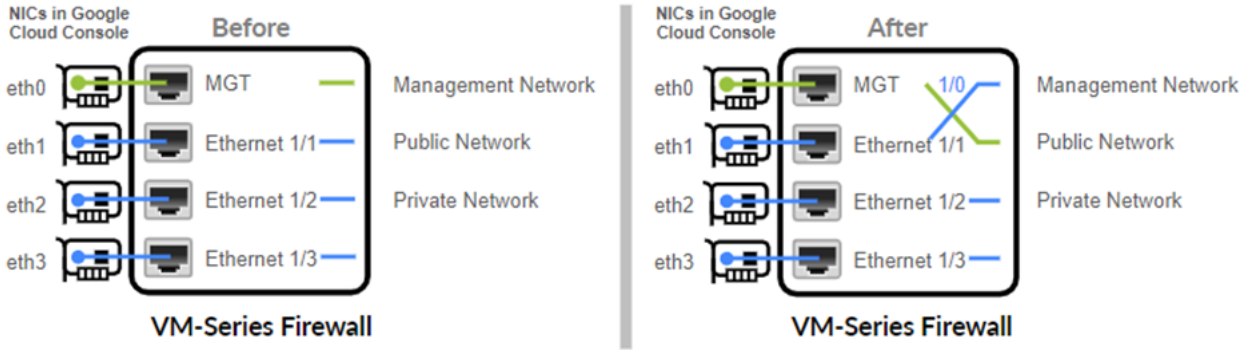
如果 VM 系列防火墙位于 Google Cloud Platform 内部负载均衡接口的下游，则防火墙可以在 eth0 上接收数据面板流量。

- 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。

© 2019 Palo Alto Networks, Inc.



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

部署 Google Cloud Platform Marketplace 的 VM 系列防火墙时可以交换接口，或是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
```

- 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可预测行为。

  在 *Google Cloud* 控制台中，您无法确认是否已交换 *eth0* 和 *eth1*。交换后，必须记住，负载均衡在 *eth0*，防火墙管理接口在 *eth1*，以便您能正确配置 *Google Cloud Platform* 负载均衡，创建安全策略规则以确保一个或多个 *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。

© 2019 Palo Alto Networks, Inc.

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
```


© 2019 Palo Alto Networks, Inc.

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 包 1：vmseries-bundle1-<*version*>
- PAYG 包 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：

```
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。

© 2019 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账户 — 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 默认服务账户）。

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 进行验证。有两个前提条件：

- 必须安装 Google API。
- 您的账户必须具有监控指标编写器和 Stackdriver 账户查看器的角色。

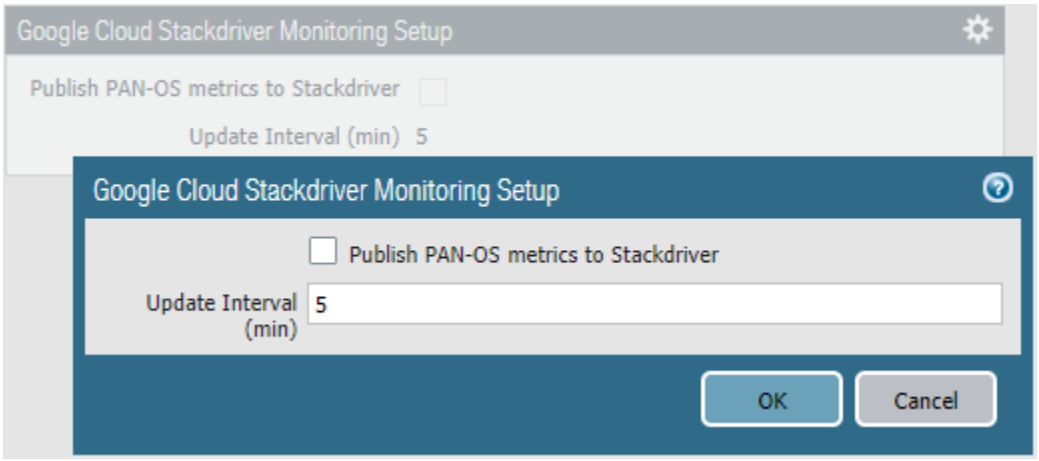
启动 Google Stackdriver

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。

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**）。

© 2019 Palo Alto Networks, Inc.



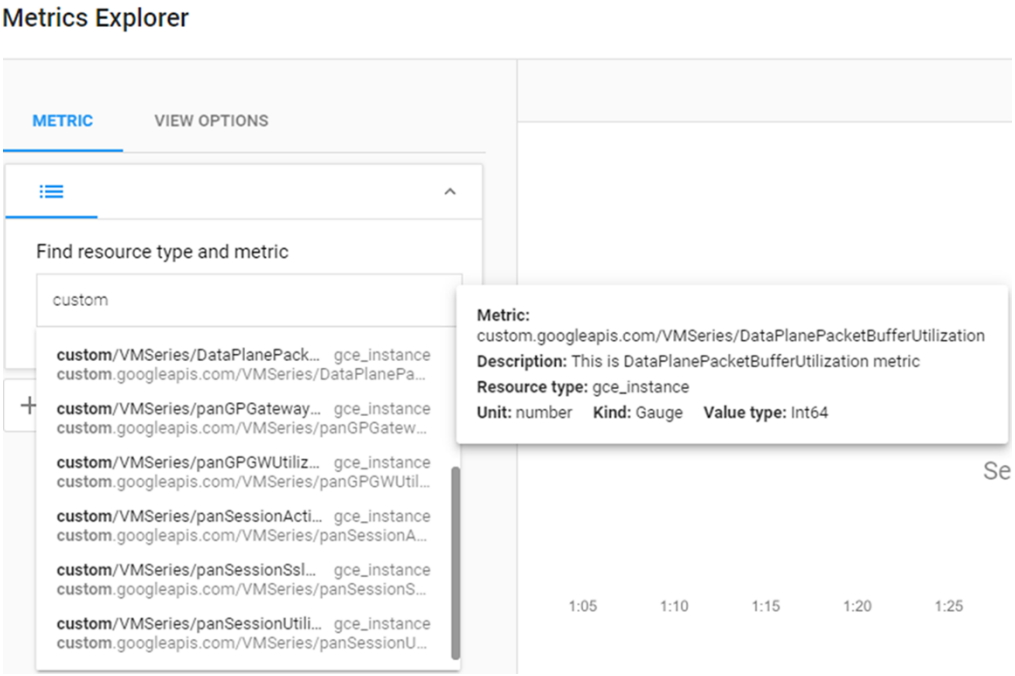
2. 设置 **Update Interval**（更新间隔）（范围是 1 - 60 分钟，默认为 5 分钟）。这是防火墙将指标发布到 Stackdriver 的频率。
3. 单击 **OK**（确定）。

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。

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。

© 2019 Palo Alto Networks, Inc.

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。

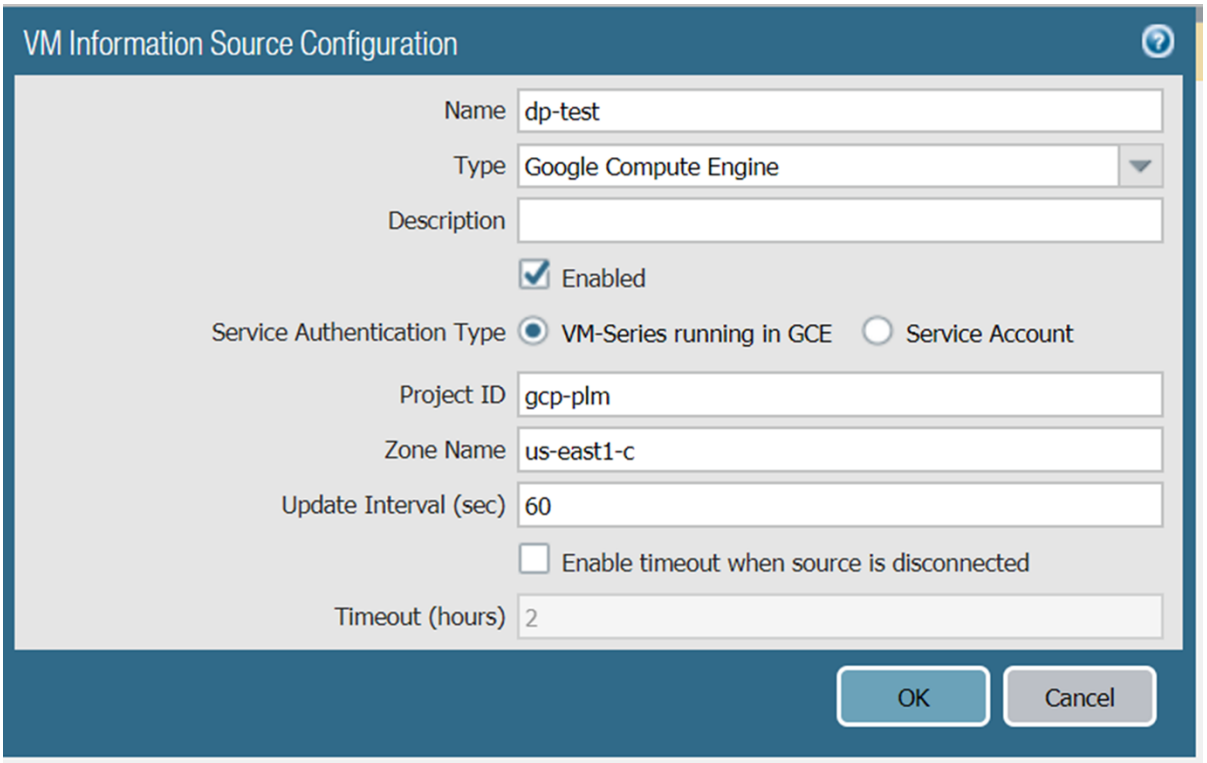
要执行 VM 监控，必须具有监控指标编写器的 IAM 角色。

STEP 1 | 登录到已部署的防火墙。

STEP 2 | 启用 VM 监控。

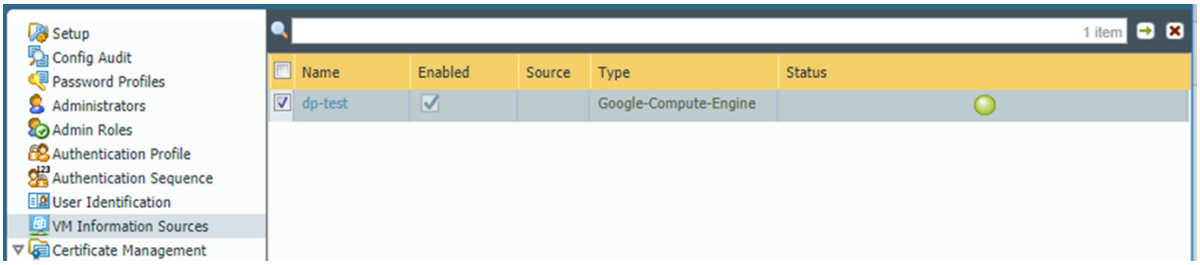
1. 选择 **Device**（设备）> **VM Information Sources**（**VM** 信息源）。
2. **Add**（添加）VM 信息源，并输入以下信息：
   - 指定用于标识要监控的实例的 **Name**（名称）。
   - 选择 Google Compute Engine **Type**（类型）。
   - 选择 **Enabled**（启用）。
   - 选择 **Service Authentication Type**（服务身份验证类别）。
     - 如果选择 **VM-Series running in GCE**（**GCE** 中运行的 **VM** 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**（服务账户）。必须上传 JSON 格式的服务账户凭据。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。

© 2019 Palo Alto Networks, Inc.



- （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。



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））。

© 2019 Palo Alto Networks, Inc.

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。

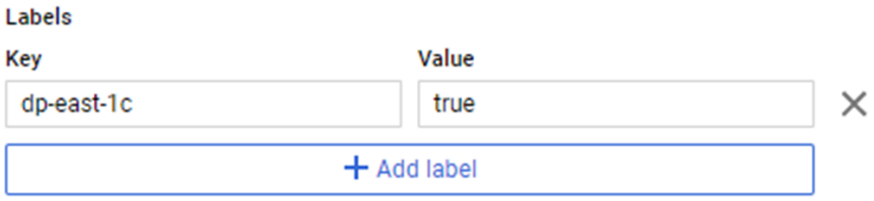
此工作流程的前提是：假定您已部署 VM 系列防火墙，在实例上配置一些应用程序，且已启用 Google Stackdriver 监控。

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。

此外，您还可以从实例浏览器添加标签。

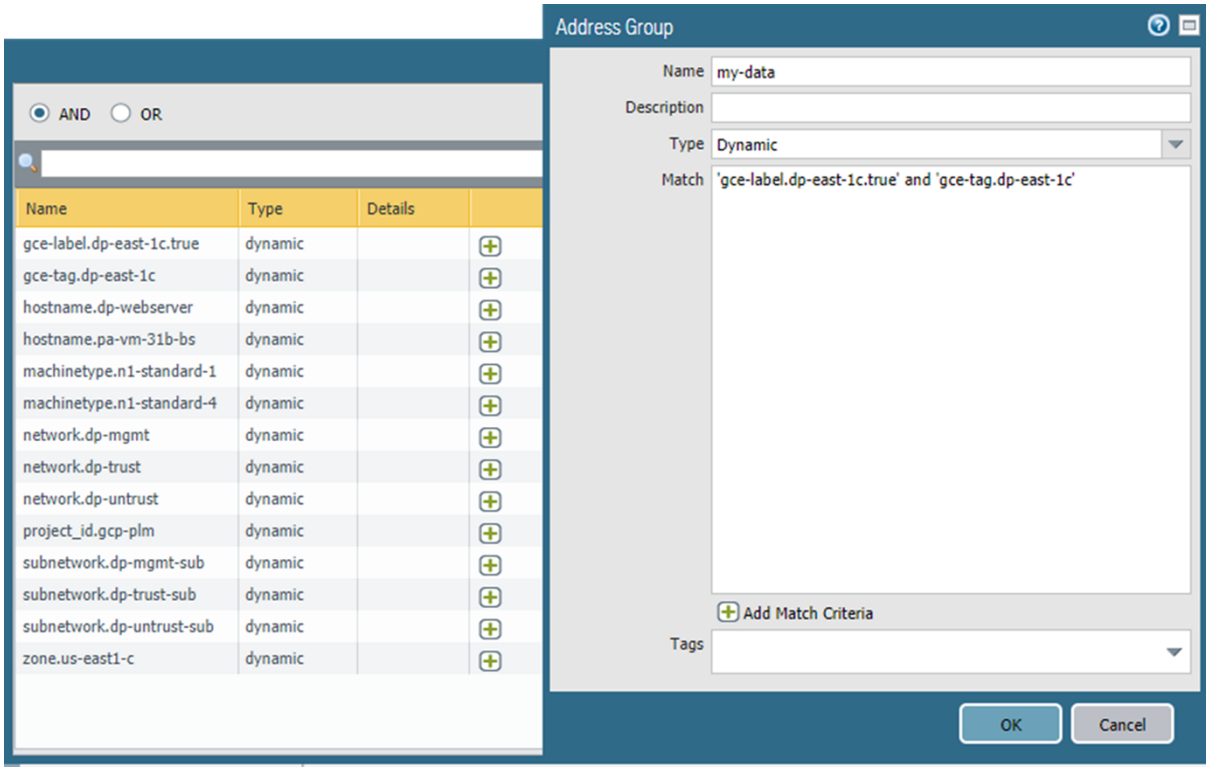


您创建的标签支持您的策略，以便以一种对安全策略有用的方式区分您的资源。

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。

© 2019 Palo Alto Networks, Inc.



5. 单击 **OK**（确定）。
6. 单击 **Commit**（提交）。

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“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。

© 2019 Palo Alto Networks, Inc.

在 Google Kubernetes 引擎群集中保护 Kubernetes 服务

适用于 Panorama 的 Google Cloud Platform 插件使 Panorama 能够在 Google Kubernetes 引擎 (GKE) 群集中保护容器化应用程序。该插件从 Kubernetes 获取特定于应用程序的信息，并将其中继到保护集群的一个或多个 VM 系列防火墙。

- 使用适用于 Panorama 的 Google Cloud Platform 插件保护 Google Kubernetes 引擎服务
- 使用示例 Terraform 模板部署 Kubernetes 服务
- 为 Google Kubernetes 引擎配置 Google Cloud Platform 插件

使用适用于 Panorama 的 Google Cloud Platform 插件保护 Google Kubernetes 引擎服务

VM 系列防火墙提供了一种方法来保护进入或退出部署在 Google Kubernetes 引擎 (GKE) 群集中的服务的流量。为 Panorama™ 配置 Google Cloud Platform (GCP) 插件可在 GKE 集群和 Panorama 之间建立连接，允许您全局管理保护在 GKE 部署中运行的服务的防火墙。

- GKE 中的典型工作负载部署
- 保护在 GKE 中部署的工作负载所需的组件

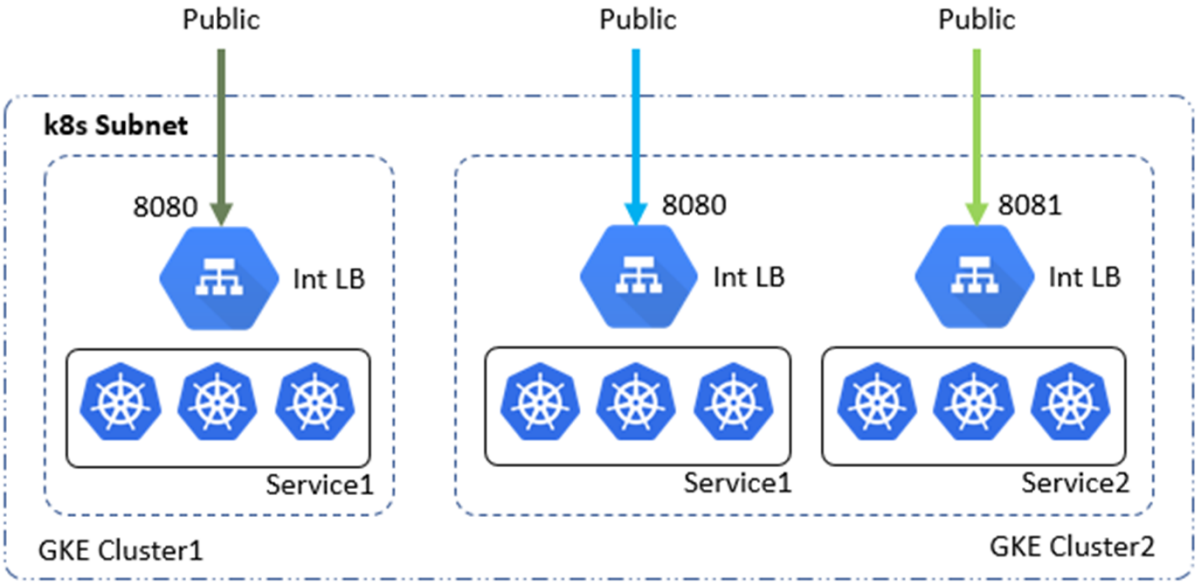
GKE 中的典型工作负载部署

GKE 部署利用 GCP 项目中的 VPC 网络和子网，用于 Kubernetes 集群与项目中其他资源之间的网络连接。容器化的应用程序在 Kubernetes 集群上运行，这是一个名为节点的集合 VM。默认情况下，节点是私有的，没有出站 Internet 访问权限。

Pod 表示在群集中运行特定应用程序的一组容器 — 在 Kubernetes 群集中的一个或多个节点上运行。Kubernetes 中的服务定义 Pod 的一个逻辑组以及访问它们的策略 — 也称为微服务。

服务通常表示应用程序的组件，例如 Web 服务、数据库服务等。以类型 LoadBalancer 公开的服务通常会分配一个公共 IP 地址，这会使应用程序容易受到群集或外部源中的入站攻击。

下图显示在同一 GCP 项目中的多个 Kubernetes 集群中运行的多个 Kubernetes 服务。



© 2019 Palo Alto Networks, Inc.

保护在 *GKE* 中部署的工作负载所需的组件

让我们看看用于保护外部可访问服务的组件。

VM 系列防火墙

在示例拓扑中，GKE 实例组包含一个或多个 VM 系列防火墙，并与 GKE 集群共享相同的网络和区域。它横跨不可信和可信子网以保护往返后端服务的流量。

实例组中的防火墙为 LoadBalancer 类型的每个服务检测 PANW 命名端口公开到 Internet。每个后端服务都在内部负载均衡器后面。

Google Kubernetes 引擎群集

Google Kubernetes 引擎服务在 GKE 集群中运行。适用于 Panorama 的 Google Cloud Platform 插件每个群集最多支持 100 个公开服务。

要在 Panorama 上集成 GCP 插件，请按照部署应用程序中所述编辑应用程序部署的 config.yaml 文件。

panw-named-port 标签对于区分服务至关重要。使用 *panw-named-port* 标签作为匹配条件，您可以创建特定于每个服务的防火墙规则，并相应地引导流量。

Panorama 上的 Google Cloud Platform 插件

适用于 Panorama 的 Google Cloud Platform 插件可配置在 GCP 部署中运行的 Kubernetes 群集与 Panorama 之间的集成。

该插件在 GKE 项目中存储特定 Panorama 设备组和 GKE 集群之间的映射信息。GKE 项目存储最多四个 GKE 集群的集成信息，每个集群可以公开多达 100 个服务。您最多可以保护四个 GKE 项目。当插件在其正在监视的 Kubernetes 集群中检测到新服务时，它会创建 Panorama 服务对象和 NAT 规则，在网络路径中插入 VM 系列防火墙以保护进出的流量服务。

Panorama

为 Panorama 配置 GCP 插件时，将 GKE 群集与 GCP 项目中特定的实例组相关联。GCP 中的实例组与 Panorama 中的设备组相关联。

GCP 插件使 Panorama 能够全局管理设备组中的所有防火墙的安全性策略和配置文件。

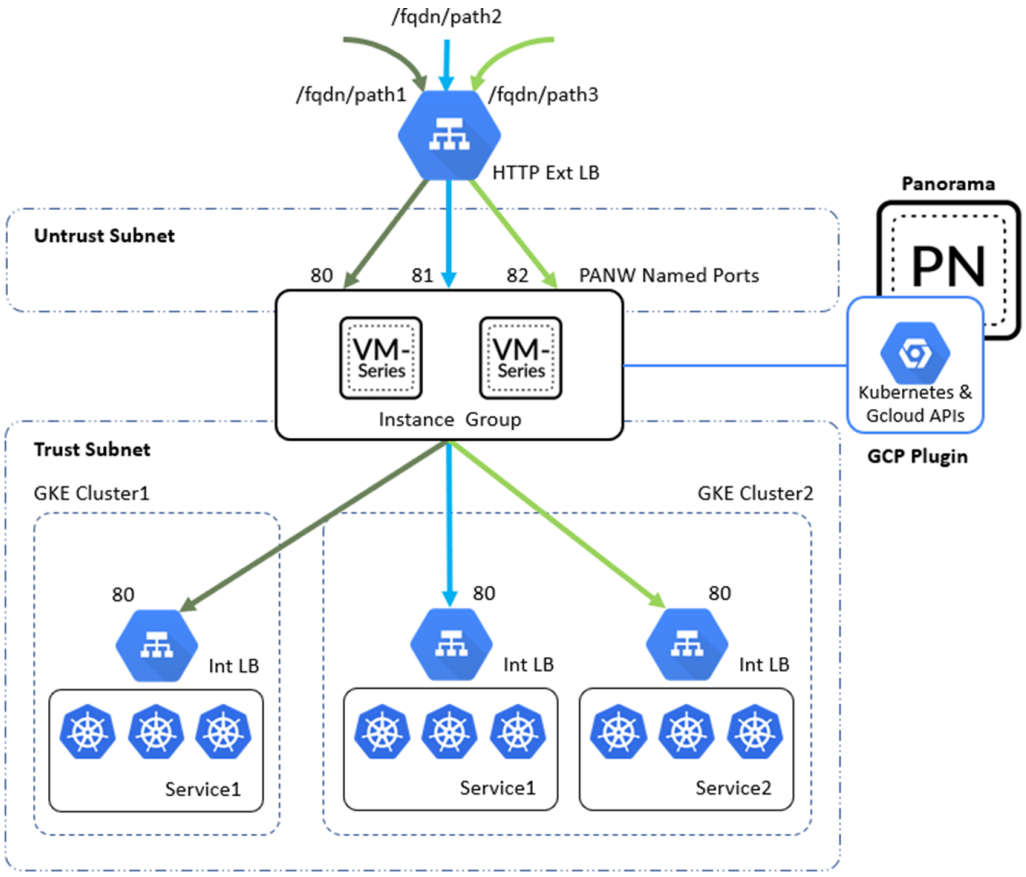
示例拓扑

下图说明了负载均衡器三明治部署。此图突出显示了将 GKE 集群与适用于 Panorama 的 GCP 插件集成的关键要素。

要保护容器化应用程序，请将 VM 系列防火墙放在 Kubernetes 群集前面，以便保护进出应用程序服务的所有流量。除了保护入站流量外，VM 系列防火墙还可以保护 Kubernetes 节点的出站访问，防止数据泄露。

在此示例拓扑中，流量进入 HTTP 外部负载均衡器 (ELB)，并根据完全限定的域名 (FQDN) 定向到 PANW 命名端口。实例组防火墙应用安全策略并检查可信子网中服务的所有流量。

© 2019 Palo Alto Networks, Inc.



此图表反映了 Kubernetes 集群上服务的逻辑组织。例如，它显示了两个集群和三个服务（工作负载）。但是，Kubernetes 集群部署实际上是一个集群，其资源分布有多个计算实例组（不要与 VM 系列防火墙实例组混淆）的节点池中。

使用示例 Terraform 模板部署 Kubernetes 服务

要部署应用程序，您需要在 GCP 中构建基础架构。您可以使用 Google Cloud Platform 控制台手动创建，使用（或修改）现有模板或创建新模板。然后，继续为 Google Kubernetes 引擎配置 Google Cloud Platform 插件。

请在 GitHub 上参阅社区支持的 GKE-LB-Sandwich Terraform 模板：https://github.com/PaloAltoNetworks/GCP-Terraform-Samples/tree/master/GKE-LB-Sandwich。

以下部分介绍了专门针对 GKE 的其他配置任务。

- 自定义并运行 GKE LB 三明治 Terraform 模板
- 部署应用程序
- 使用多个 URL 映射创建外部负载均衡器流

自定义并运行 *GKE LB* 三明治 *Terraform* 模板

Palo Alto Networks GKE LB Sandwich Terraform 模板创建了一个示例 GKE 集群部署，您可以使用它来测试 Panorama 的 Google Cloud Platform 插件。要将此社区支持的示例模板与 Panorama 的 GCP 插件一起使用，您必须进行以下更改以确保集成成功。

STEP 1 | 从 https://github.com/PaloAltoNetworks/GCP-Terraform-Samples/tree/master/GKE-LB-Sandwich 下载 GKE LB 三明治 Terraform 模板。

按照编写的模板部署指南说明中的步骤进行操作，但此处提到的步骤除外。

© 2019 Palo Alto Networks, Inc.

STEP 2 | 在部署指南的第 4.8 节中，按如下编辑 **main.tf**。

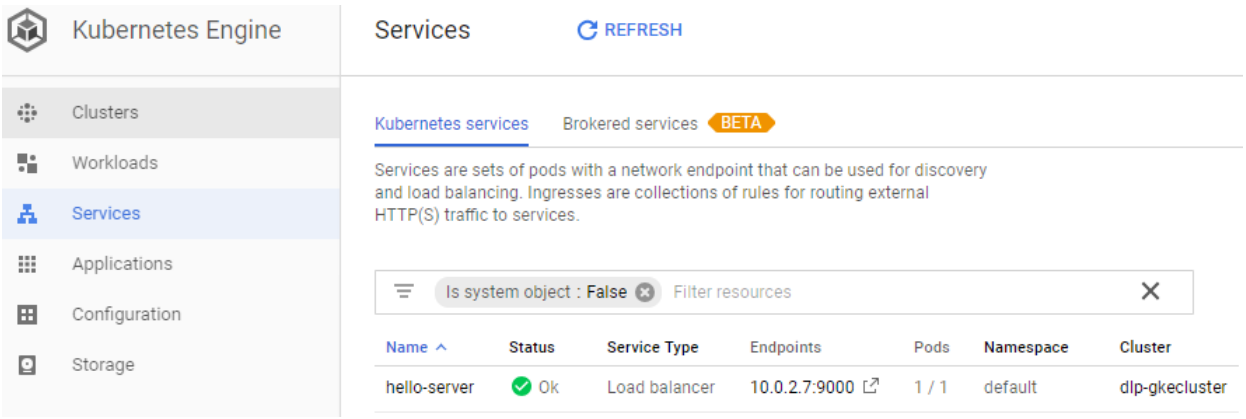
更改 GCP 路由的可信接口优先级 **100** 至 **1001**。

```
// Adding GCP ROUTE to TRUST Interface
resource "google_compute_route" "trust" {
  name                  = "dlp-trust-route"
  dest_range            = "0.0.0.0/0"
  network               = "${google_compute_network.trust.self_link}"
  next_hop_instance     = "${element(google_compute_instance.firewall.*.name,count.index)}"
  next_hop_instance_zone = "${var.zone}"
  priority              = 1001
```

更改 master_auth 密码。

```
master_auth {
  username = "admin"
  password = ""
}
```

STEP 3 | 在第 20 和 21 页，模板文档是指 Google Cloud 控制台中的“Discovery & load balancing（发现和负载均衡）”。此节点在当前版本中命名为“服务”。



STEP 4 | 在第 24 页，不要创建 NAT 规则。如果在 Panorama 中正确配置了 Google Cloud Platform 插件，它会了解您的 GKE 服务并为您创建适当的NAT规则。

部署应用程序

要使用 Panorama 保护应用程序，对于您要保护的每个外部公开的 GKE 服务，您必须确保有注释和 *panw-named-port* 标签。您可以直接编辑 GKE YAML 文件，也可以从 Google Cloud Platform 用户界面编辑，如此处所述。

可以通过外部负载均衡器 (ELB) 公开一个或多个服务。有时 ELB 端口号在部署 ELB 时预先分配。您必须确保分配给 panw-named-port 的端口号与分配给 ELB 的端口号相匹配。

STEP 1 | 编辑 **config.yaml** 文件：

1. 选择 **Kubernetes Engine**（**Kubernetes** 引擎）> **Services**（服务）> **YAML**以打开 YAML 文件。
2. 在标签下，添加 **panw-named-port:** 并指定一个端口号。例如，**panw-named-port:"80"**。
   在配置 Google Cloud Platform 插件时，您可以提供 panw-named-port。

© 2019 Palo Alto Networks, Inc.

```
apiVersion: v1
kind: Service
metadata:
  name: hello-server
  annotations:
    cloud.google.com/load-balancer-type: "Internal"
apiVersion: v1
kind: Service
metadata:
  annotations:
    cloud.google.com/load-balancer-type: "Internal"
  creationTimestamp: 2018-03-19T17:35:22Z
  labels:
    run: hello-server
    panw-named-port: "80"
  name: hello-server
  namespace: default
  resourceVersion: "1570"
  selfLink:
  uid:
spec:
  clusterIP:
  externalTrafficPolicy: Cluster
  ports:
  - nodePort: 31154
    port: 9000
    protocol: TCP
    targetPort: 8080
  selector:
    run: hello-server
  sessionAffinity: None
  type: LoadBalancer
```

STEP 2 | 保存文件。

使用多个 *URL* 映射创建外部负载均衡器流

您可以配置外部 HTTP/S 负载均衡器来为多个域的请求提供服务。每个服务都被标记为 panw-named-port，因此，可以从防火墙的不可信接口访问。

您必须为标记为 panw-named-port 的每个服务创建后端服务，并在负载均衡器中配置后端服务。您还必须配置运行状况检查。

如果您使用 Google Cloud Platform 控制台，则配置无法正常运行，Panorama 的 GCP 插件无法学习服务和端口映射。要成功部署，请使用以下方法之一：

- 使用 GCP 控制台时，请按照 https://cloud.google.com/load-balancing/docs/https/setting-up-https 和 https://cloud.google.com/load-balancing/docs/https/url-map 中的说明操作。
- 使用命令行界面中的 gcloud 命令。

在此命令行界面示例中，gcloud 命令在单个负载均衡器下创建两个服务，其中 panw 名为端口 9000、80 和 81。

© 2019 Palo Alto Networks, Inc.

```
gcloud compute health-checks create http panw-lab-hc-1
--port 80 --check-interval 30
```

```
gcloud compute backend-services create panw-lab-bs-80 --protocol HTTP
--port-name port80 --global --health-checks panw-lab-hc-1
```

```
gcloud compute backend-services create panw-lab-bs-608 --protocol HTTP
--port-name port9000 --global --health-checks panw-lab-hc-1
```

```
gcloud compute backend-services create panw-lab-bs-81 --protocol HTTP
--port-name port81 --global --health-checks panw-lab-hc-1
```

```
gcloud compute url-maps create panw-lab-url-map-1
--default-service panw-lab-bs-80
```

```
gcloud compute target-http-proxies create panw-lab-t-http-proxy-1
--url-map panw-lab-url-map-1
```

```
gcloud compute forwarding-rules create panw-lab-fe-1 --global
--target-http-proxy panw-lab-t-http-proxy-1 --ports 88
```

```
gcloud compute instance-groups set-named-ports fw-ig
--named-ports port80:80,port9000:9000,port81:81
```

```
gcloud compute backend-services add-backend panw-lab-bs-80 --global
--instance-group fw-ig --instance-group-zone us-west1-a
```

```
gcloud compute backend-services add-backend panw-lab-bs-9000—global
--instance-group fw-ig  --instance-group-zone us-west1-a
```

```
gcloud compute backend-services add-backend panw-lab-bs-81 --global
--instance-group fw-ig  --instance-group-zone us-west1-a
```

```
gcloud compute url-maps add-path-matcher panw-lab-url-map-1
--path-matcher-name host9000 --default-service panw-lab-bs-9000 --new-hosts=*
```


© 2019 Palo Alto Networks, Inc.

```
--path-rules="/*=panw-lab-bs-9000"
```

```
gcloud compute url-maps add-path-matcher panw-lab-url-map-1

--path-matcher-name host81 --default-service panw-lab-bs-81

--new-hosts=* --path-rules="/*=panw-lab-bs-81"
```

为 Google Kubernetes 引擎配置 Google Cloud Platform 插件

要使 Panorama 能够在 GKE 集群中了解 Internet 公开的服务，您必须在 Panorama 上启用 Google Cloud Platform 插件，以便与 GCP 项目和 GKE 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受管防火墙。

- 创建 GKE 服务帐户凭据
- 存储 GCP 项目服务帐户凭据
- 配置 Panorama 并为 GKE 安装 GCP 插件
- 配置 GKE 的 GCP 插件

创建 *GKE* 服务帐户凭据

要通过群集进行身份验证并了解其服务，Google Cloud Platform 插件需要 GKE 角色和角色绑定以及来自 GKE 群集的服务凭据文件。您将凭据保存为 .json 文件，以便在配置 GKE 的 GCP 插件可以提供。

STEP 1 | 为您的 GKE 集群创建一个服务帐户。

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 Google Cloud Shell 以在 crb.yaml 中应用角色绑定。

   kubectl apply -f crb.yaml
3. 查看刚才创建的服务帐户。

   kubectl get serviceaccounts

© 2019 Palo Alto Networks, Inc.

STEP 2 | 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 $SA_TOKEN
   ```
4. 显示凭证。

   ```
   kubectl get secret $MY_SA_TOKEN -o json
   ```

存储 *GCP* 项目服务帐户凭据

有关存储计算引擎默认服务帐户的服务凭据的说明，请参阅第 12 页的第 4.8 节中的模板部署指南。

有关一般信息，请参阅身份验证入门。

配置 *Panorama* 并为 *GKE* 安装 *GCP* 插件

您必须拥有 Panorama™ 的许可版本。

STEP 1 | 要确保同步，请验证 Panorama 设备和 GKE 集群中的防火墙是否引用相同的 NTP 服务器。例如，time.google.com。

STEP 2 | 在与 GKE 集群关联的防火墙上，指定 Panorama 服务器的 IP 地址或 FQDN并提交。

STEP 3 | 在 Panorama 中，添加与 GKE 集群关联的防火墙托管设备。

STEP 4 | 添加设备组并将托管防火墙分配到设备组。

STEP 5 | 添加模板。命名模板并接受默认的 VSYS。

STEP 6 | 选择 Add Stack（添加堆栈）。命名堆栈，**Add**（添加）刚才创建的模板，并选择保护您的 Kubernetes 集群的防火墙。

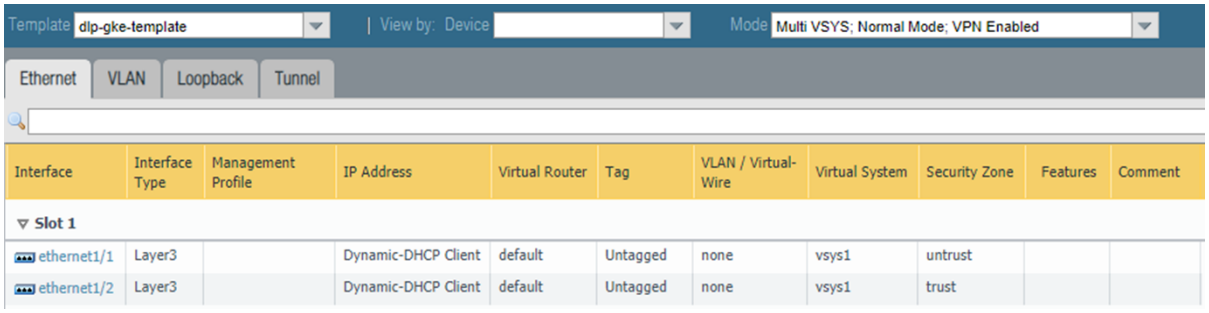
提交更改。

STEP 7 | 选择 **Network**（网络）> **Interfaces**（接口）。

1. 对于不可信区，配置第 3 层接口。
   - 选择 **Ethernet**（以太网）> **Add Interface**（添加接口）。
   - 选择 **Slot 1**（插槽 1）和 **Interface Name**（接口名称）。

     将 **Interface Type**（接口类型）设置为“Layer 3（第 3 层）”。
   - 选择 **Config**（配置）并设置 Security Zone（安全区域）以管理 GKE 群集的区域。例如，us-central1-a。
   - 选择 **IPV4** 并选择网络的选项。此示例使用 DHCP。
   - 单击 **OK**（确定）。
2. 对于可信区，配置第 3 层接口。

© 2019 Palo Alto Networks, Inc.



STEP 8 | 将接口分配给虚拟路由器。选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后修改或 **Add**（添加）路由器。此示例使用 ***default***。添加在上一步中创建的接口，然后单击 **OK**（确定）。

STEP 9 | 配置网络区域。

1. 配置不可信网络的区域。
   - 选择 **Network**（网络）> **Zones**（区域），然后指定区域 **Name**（名称）。
   - 将 Interface Type（接口类型）设置为“Layer 3（第 3 层）”。
   - 在接口下，**Add**（添加）不可信接口。
   - 单击 **OK**（确定）。
2. 配置可信网络的区域。

STEP 10 | 提交更改。

STEP 11 | 将模板推送到防火墙。

STEP 12 | 选择 **Panorama** > **Plugins**（插件）并安装插件。插件名称是 gcp。

配置 *GKE* 的 *GCP* 插件

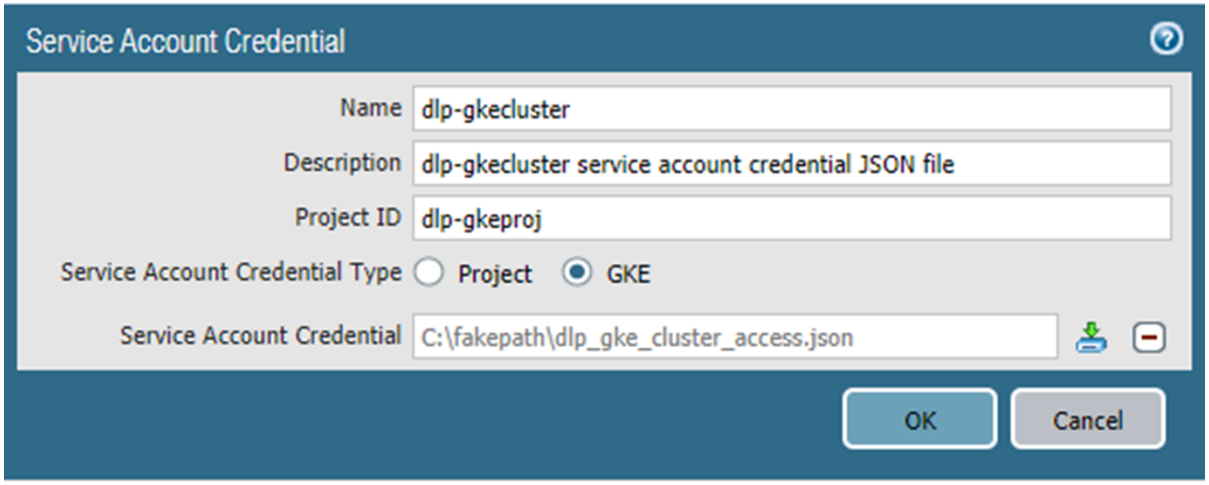
这些步骤为 GKE 配置 GCP 插件。

STEP 1 | 选择 **Panorama** > **Google Cloud Platform** > **Setup**（设置）和 **Add**（添加）与 GKE 部署关联的 GCP 项目和 GKE 集群的服务帐户凭据。

1. 选择 **Project**（项目）服务帐户凭据类型。输入描述性的名称（不必是项目名称）以及 GCP 项目 ID。要查看项目 ID，请在 Google Cloud Platform 控制台中查看项目信息中心，然后在“项目信息”下查找“项目 ID”。

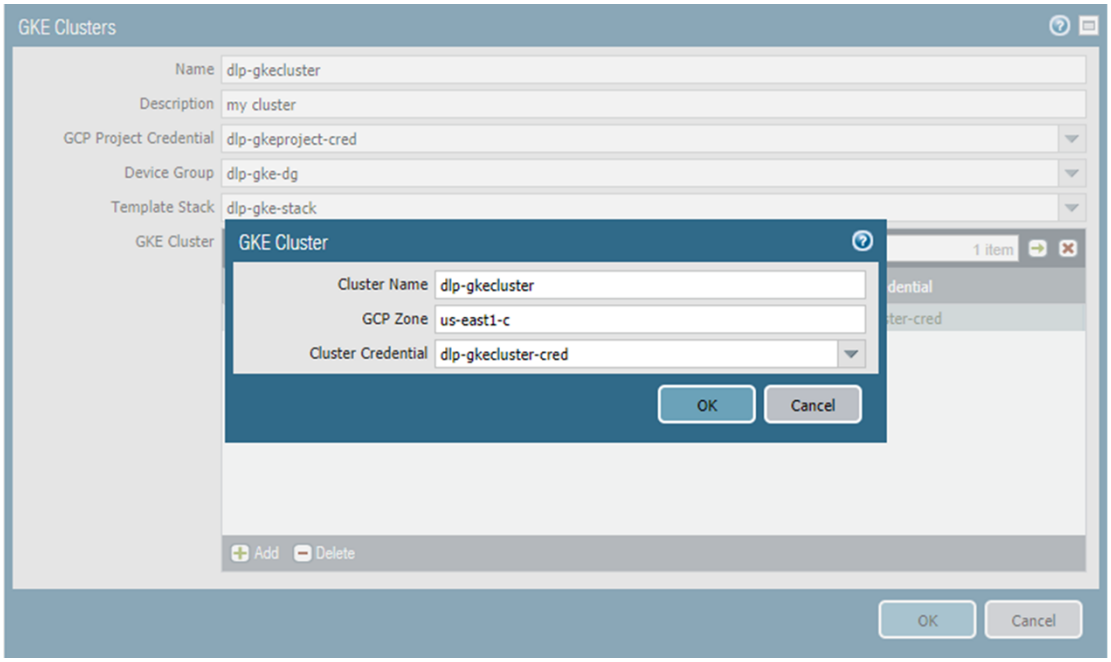
   单击上传图标，浏览以选择保存在 存储 GCP 项目服务帐户凭据 中的 JSON 文件，然后单击 **Open**（打开）。出于安全原因，本地路径将替换为占位符 `fakepath`。
2. 选择 **GKE** 服务帐户凭据类型，并上传为 GKE 项目保存的 JSON 文件 创建 GKE 服务帐户凭据。
3. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.



STEP 2 | 添加 GKE 项目。在 Panorama 中，GKE 项目存储最多四个 GKE 集群的集成信息，每个集群可以公开多达 100 个服务。您最多可以保护四个 GKE 项目。

1. 选择 **Panorama** > **Google Cloud Platform** > **GKE Clusters**（**GKE 集群**）。
2. **Add**（添加）一个集群。
3. 指定名称和描述。
4. 选择 **GCP Project Credential**（**GCP 项目凭据**），**Device Group**（**设备组**）以及之前创建的 **Template Stack**（**模板堆栈**）。
5. **Add**（添加）集群成员。指定先前上传的群集名称、GCP 区域和群集凭据。



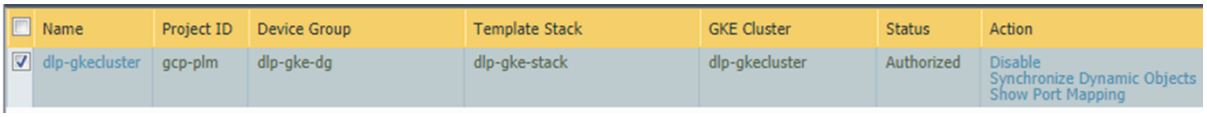
STEP 3 | 提交更改。

通过 GCP 插件、Panorama 了解新的 Kubernetes 服务。防火墙可能需要 5 到 7 分钟才能获取新的 NAT 规则和服务对象。

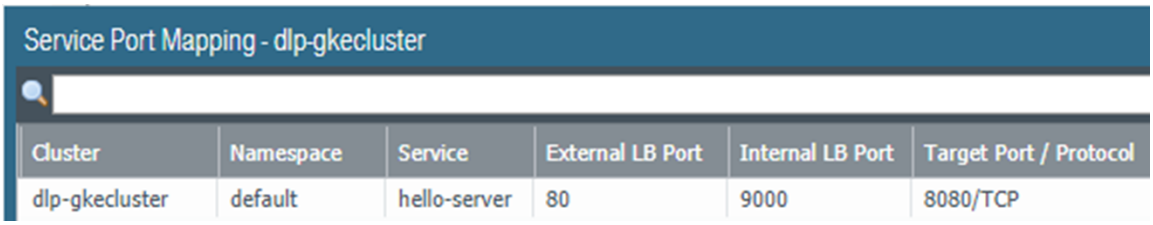
STEP 4 | 查看 Panorama 中的 GKE 元素。

© 2019 Palo Alto Networks, Inc.

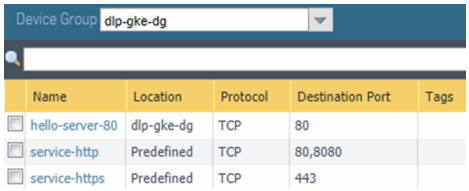
- 转到 **Panorama** > **Google Cloud Platform** > **GKE Clusters**（**GKE** 群集）查看 GKE 项目列表。如果指定的群集存在且配置正确，则“状态”为“已授权”。



在“操作”列中单击 **Show Port Mapping**（显示端口映射）以查看 GKE 集群中服务的端口。端口 80 是 PANW 命名端口。学习此示例中的其他端口。

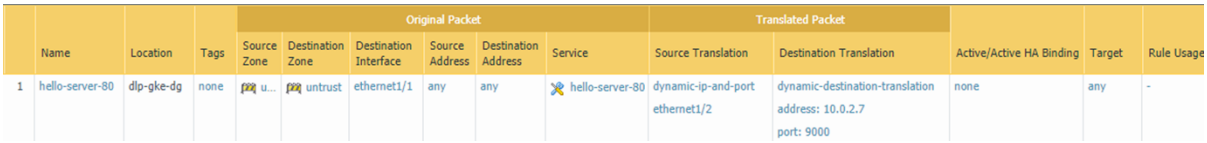


- 选择 **Objects**（对象）并确保选中设备组。查看部署的服务。在此示例中，预定义服务来自外部 HTTP 负载均衡器。



- 选择 **Policies**（策略），并查看 NAT 预规则。

  您看到的任何 NAT 规则都是由插件创建的。“服务”列显示使用 PANW 命名端口公开的 GKE 服务。IP 地址是服务地址。



STEP 5 | 有关清理说明，请参阅模板部署指南。

© 2019 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。

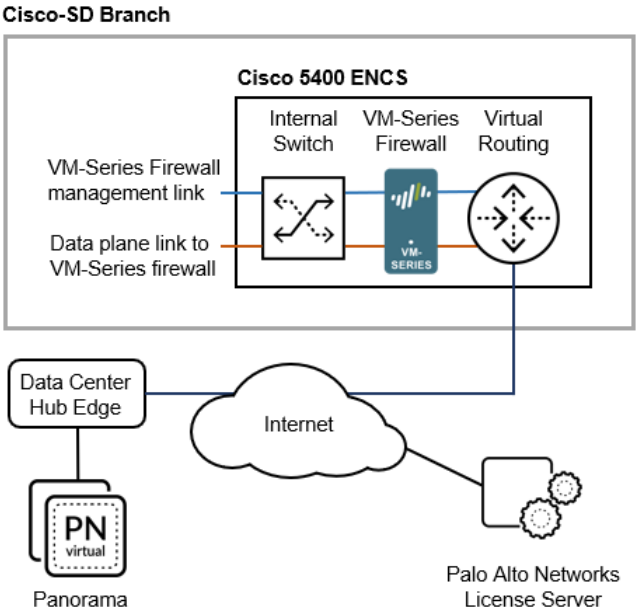
Cisco 企业网络计算系统 (ENCS) 设备与 Cisco 集成服务虚拟路由器 (ISRV) 和 NFVIS 软件相结合，以支持软件定义分支 (SD-Branch) 网络基础架构。

> 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 直通模式。
  - 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。

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。参阅 VM 系列系统要求以确保 Cisco ENCS 设备具有足够的资源来支持您选择的 VM 系列型号。
  - 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）。参阅从图形用户界面转换 qcow2 文件，步骤 2 或从命令行界面转换 qcow2 文件，步骤 2。

© 2019 Palo Alto Networks, Inc.

- 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。请参阅许可证类型 — VM 系列防火墙。您可以在 NFVIS 用户界面中输入验证码，或在验证码中包含验证码 **authcodes** 转换文件夹中的文本文件，如 从命令行界面转换 qcow2 文件，步骤 4 中所述。
- 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。

© 2019 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

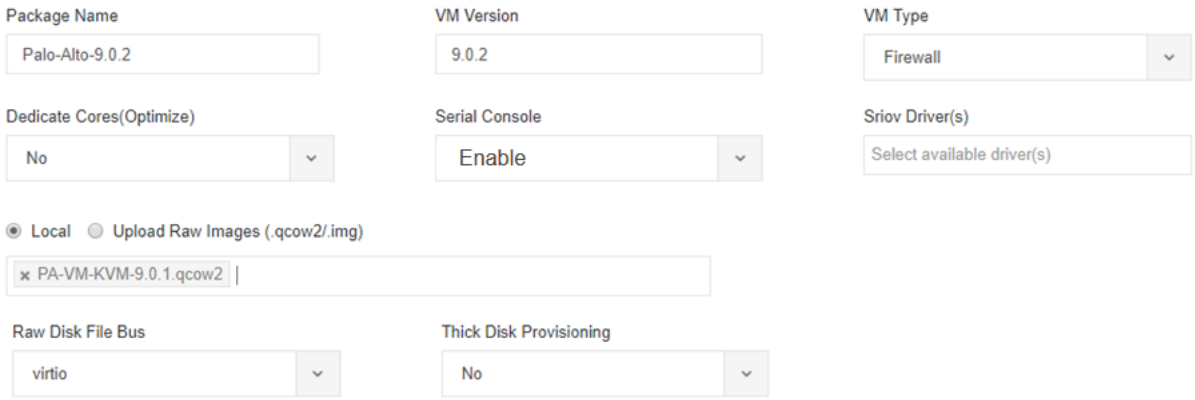
使用 NFVIS 图形用户界面输入映像打包和引导信息。

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。

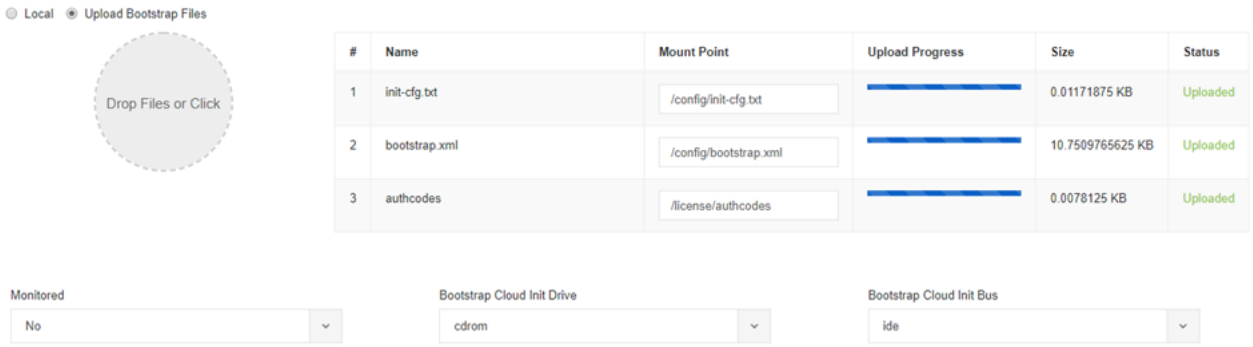
     如果您还没有这样做，请创建一个支持帐户并注册 VM 系列防火墙。
   - 选择 **Support**（支持）> **Software Updates**（软件更新），并从 **Filter By**（筛选条件）下拉列表中，选择 **Pan OS for VM-Series KVM Base Image**（用于 **VM** 系列 **KVM** 基本映像的 **PAN-OS**），例如，版本 9.1。
   - 下载 qcow2 映像。



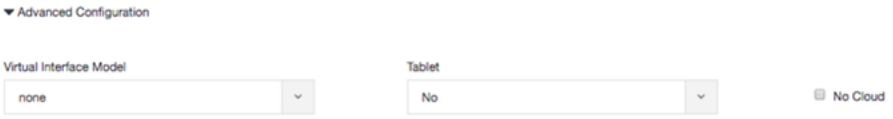
STEP 3 | 上传引导文件。

Cisco ENCS 的引导数据包仅支持 *init-cfg.txt*、*bootstrap.xml* 和 *authcodes*；它不支持动态更新或软件更新。

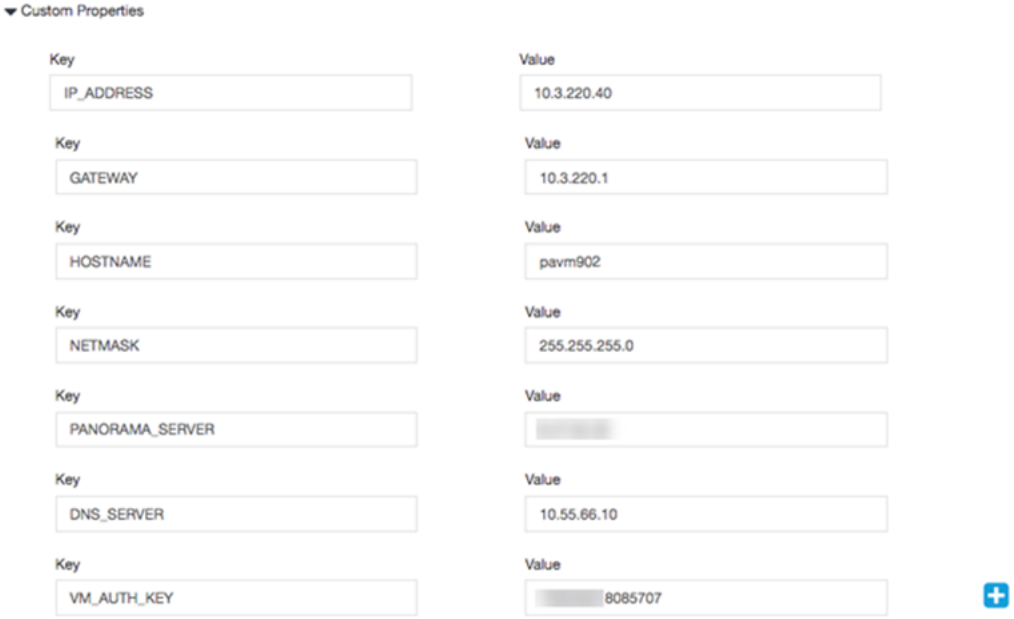
© 2019 Palo Alto Networks, Inc.



STEP 4 | 设置 **Advanced Configuration**（高级配置）。



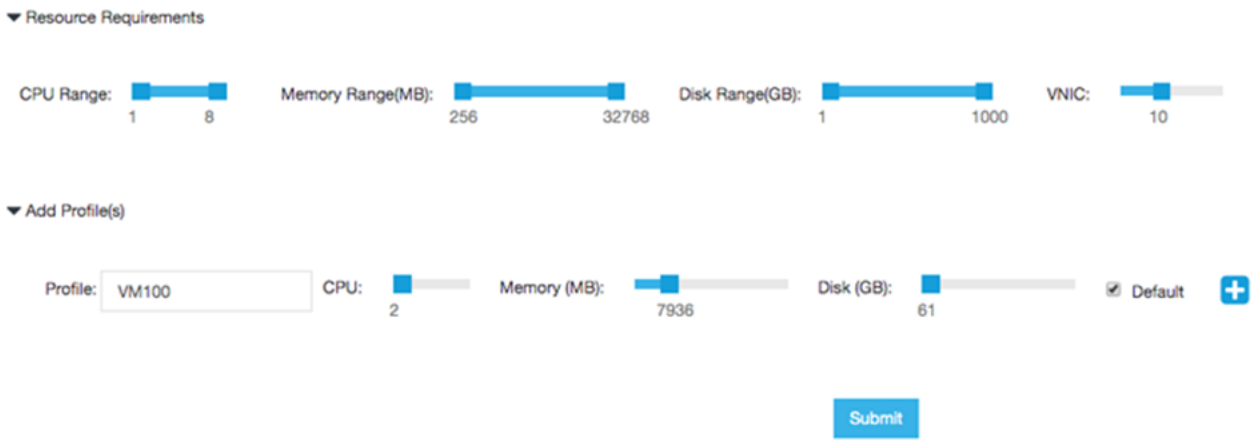
STEP 5 | 输入 **Custom Properties**（自定义属性）的值。



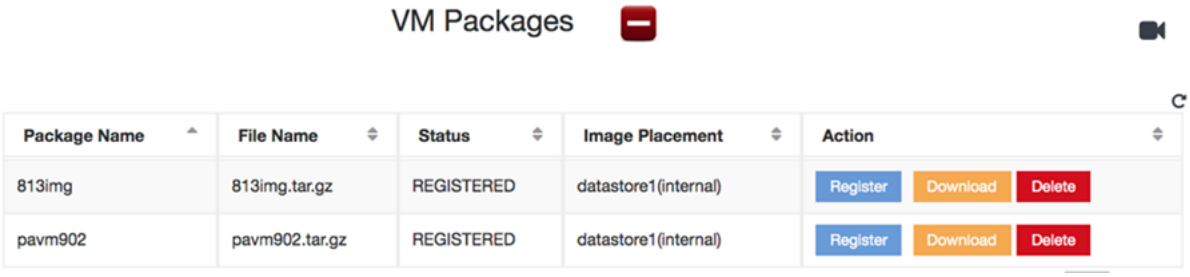
STEP 6 | 设置资源要求的值并选择“默认”配置文件，或为当前配置添加配置文件。

单击 **Submit**（提交）以保存数据包。

© 2019 Palo Alto Networks, Inc.



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。

Cisco ENCS 的引导数据包仅支持 *init-cfg.txt*、*bootstrap.xml* 和 *authcodes*；它不支持动态更新或软件更新。

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。

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=
```


© 2019 Palo Alto Networks, Inc.

```
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>
```


© 2019 Palo Alto Networks, Inc.

```
        <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</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。

© 2019 Palo Alto Networks, Inc.

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。

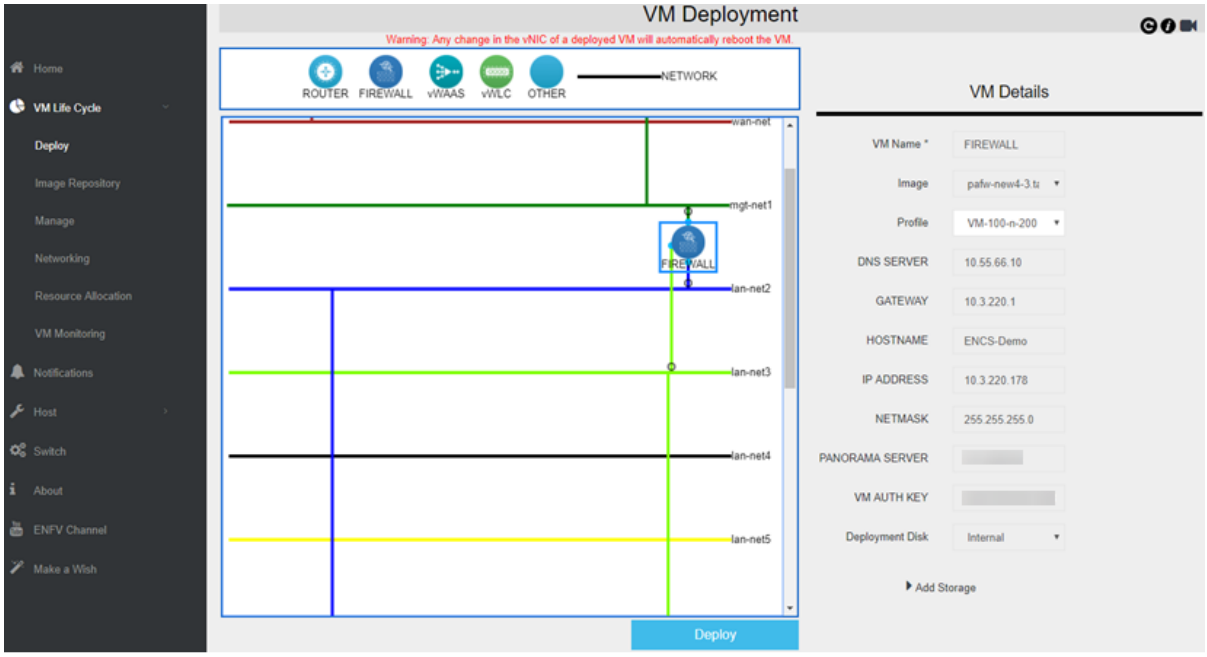
© 2019 Palo Alto Networks, Inc.

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。

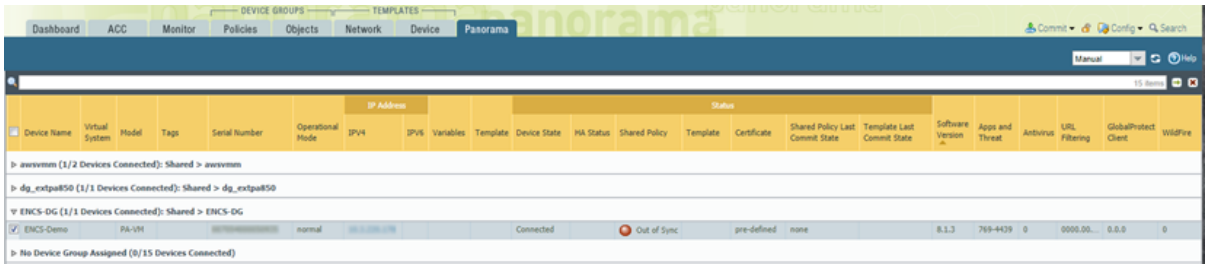
STEP 1 | 部署 VM 系列防火墙。

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**（受管设备）> **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。



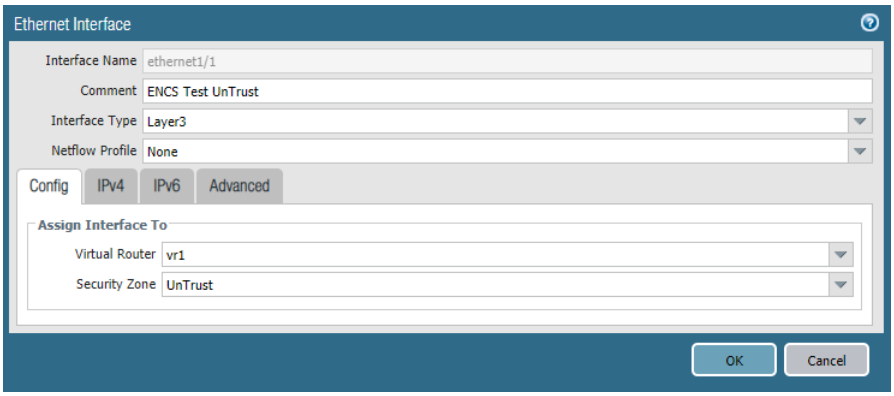
STEP 2 | 配置 VM 系列防火墙数据面接口。

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：

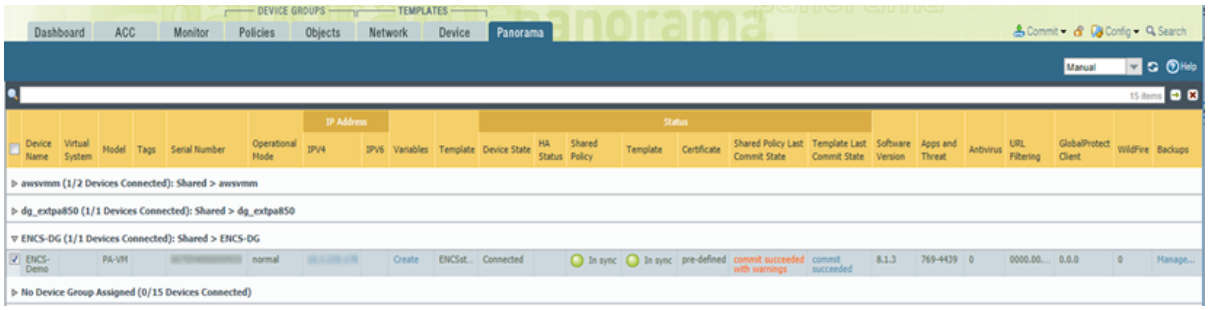
© 2019 Palo Alto Networks, Inc.

- 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 和受管防火墙。

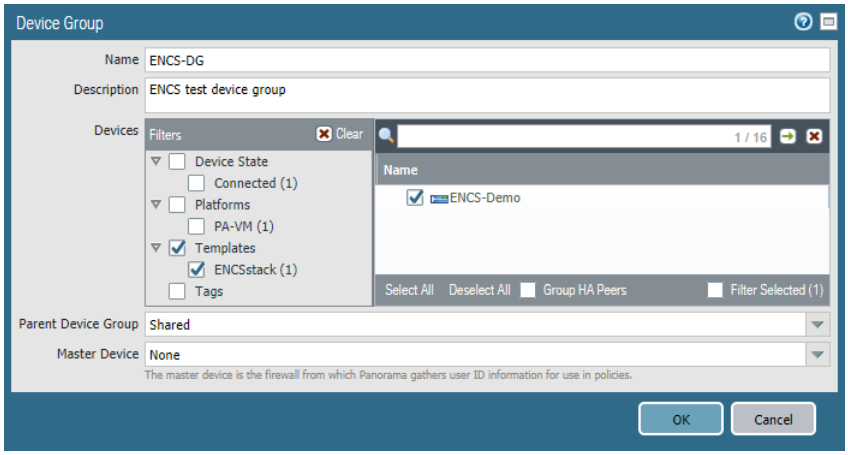
   确认防火墙接口的链路状态正常。



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。



© 2019 Palo Alto Networks, Inc.

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。

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	VM.Standard2.4
VM-300	VM.Standard2.4
VM-500	VM.Standard2.8
VM-700	VM.Standard2.16

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。

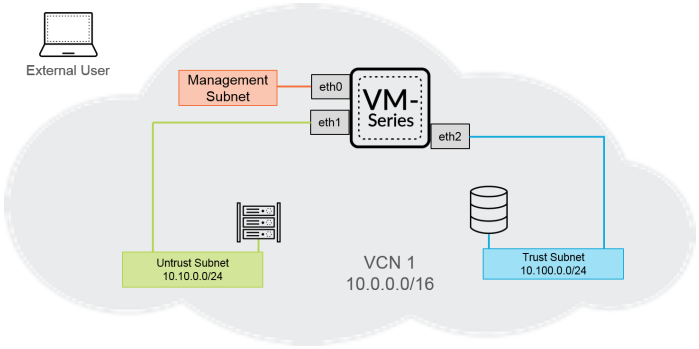
© 2019 Palo Alto Networks, Inc.

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：

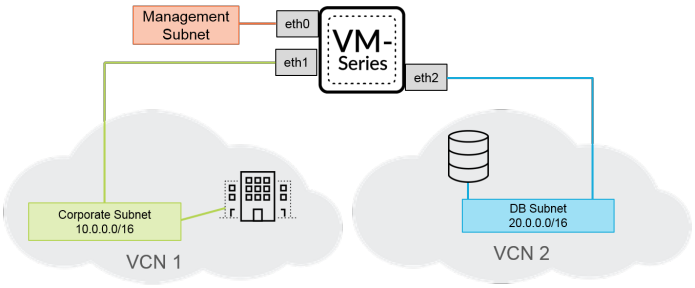
- 北向南流量 — 您可以使用 VM 系列防火墙来保护从不受可信的来源进入云网络的流量或退出云网络以访问不受可信的来源的流量。对于任一类型的流量，您必须在防火墙上的虚拟云网络 (VCN) 和 NAT 策略规则中配置路由表规则。

  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 下一跳的路由，该路由指向 VM 系列防火墙上的可信子网网络接口。



© 2019 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。

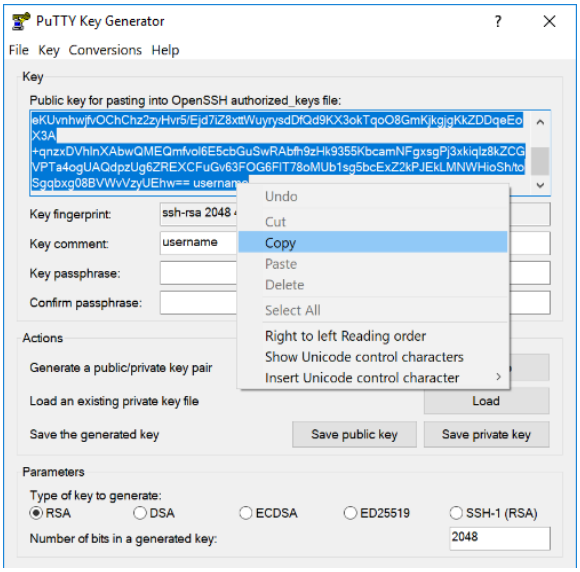
1. 创建 SSH 密钥对，并将 SSH 密钥对存储在操作系统的默认位置。
   - 在 Linux 或 MacOS 中，使用 `ssh-keygen` 在 .ssh 目录中创建密钥对。
   - 在 Windows 中，使用 PuTTYgen 创建密钥对。

     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。
2. 选择完整的公钥。
   - Linux 或 MacOS：

     打开文本编辑器中的公钥，并复制公钥。
   - 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）。

© 2019 Palo Alto Networks, Inc.



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。
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。

© 2019 Palo Alto Networks, Inc.

字段	说明
op-command-modes=jumbo-frame	用于在 VM 系列防火墙上启用巨帧模式。由于 OCI 默认以巨帧模式部署 VM 实例，因此建议您在巨帧模式下启动 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

© 2019 Palo Alto Networks, Inc.

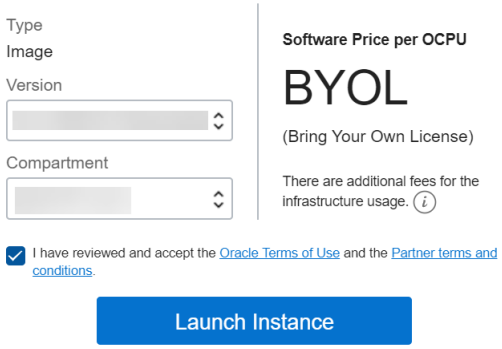
从 Oracle Cloud Marketplace 部署 VM 系列防火墙

完成以下过程，在 OCI 中从 Oracle Cloud Marketplace 部署 VM 系列防火墙。

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。

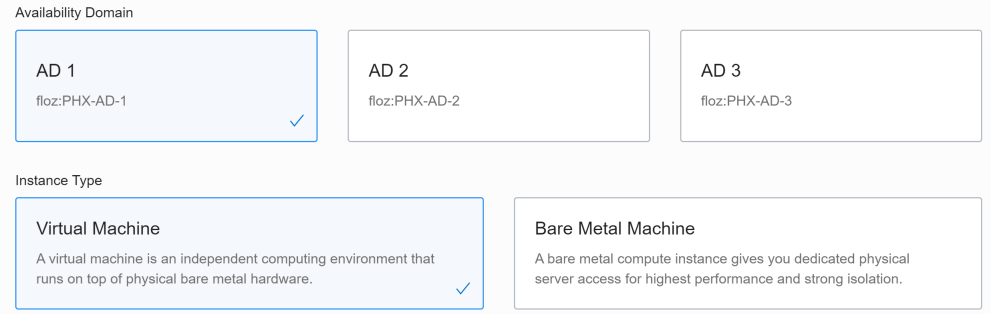
1. 搜索 Palo Alto Networks，将显示 VM 系列防火墙的产品列表。
2. 选择一个产品。
3. 单击 **Get App**（获取应用程序）。
4. 选择 **Region**（区域），然后单击 **Sign In**（登录）。
5. 选择 **Version**（版本）和 **Compartment**（区段）。
6. 接受 Oracle 和合作伙伴条款。
7. 单击 **Launch Instance**（启动实例）。



STEP 3 | 输入 VM 系列防火墙实例的描述性 **Name**（名称）。

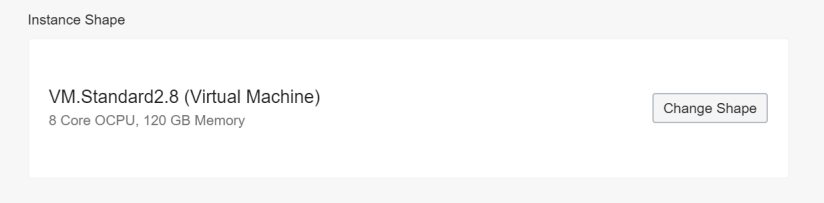
STEP 4 | 选择 **Availability Domain**（可用性域）。

STEP 5 | 在 **Shape Type**（形状类型）下选择 **Virtual Machine**（虚拟机）。

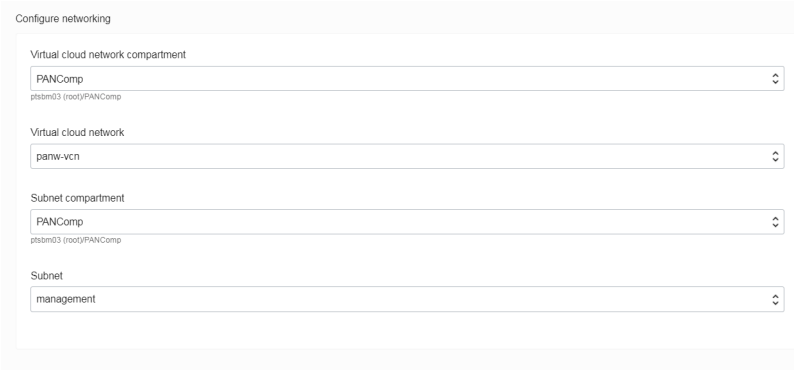


STEP 6 | 选择具有 VM 系列防火墙模型所需的 CPU 数量、RAM 数量和接口数量的形状。有关不同计算形状提供的数量资源，请参阅计算形状。有关各 VM 系列防火墙型号所需的资源的详细信息，请参阅 VM 系列系统要求。

© 2019 Palo Alto Networks, Inc.



STEP 7 | 在“联网”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。

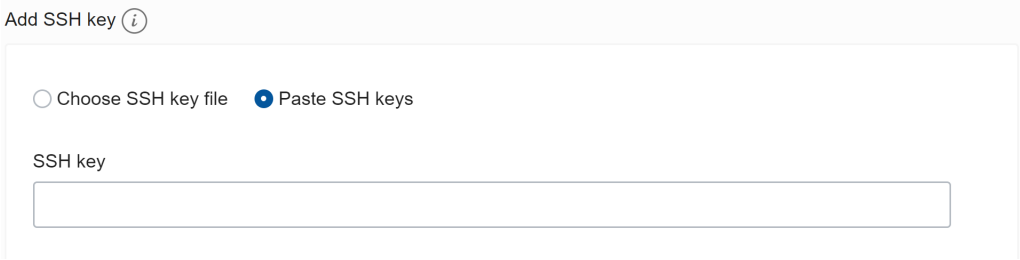


STEP 8 | （可选）将启动卷设置为大于默认大小的大小。默认情况下，将启动卷设置为 60GB。如果需要更大的启动卷以支持诸如附加日志等功能，请完成此过程。

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。



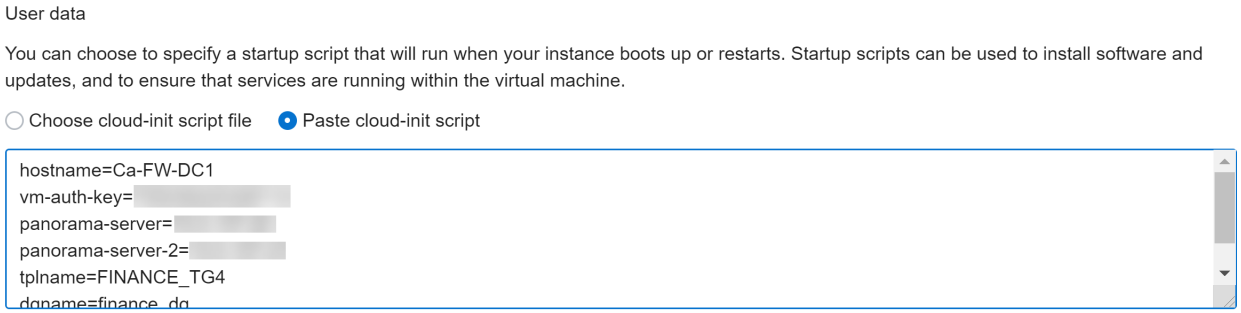
STEP 10 | 添加引导参数。

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>
```


© 2019 Palo Alto Networks, Inc.

```
tplname=<template-stack-name>
dgname=<device-group-name>
authocodes=<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：

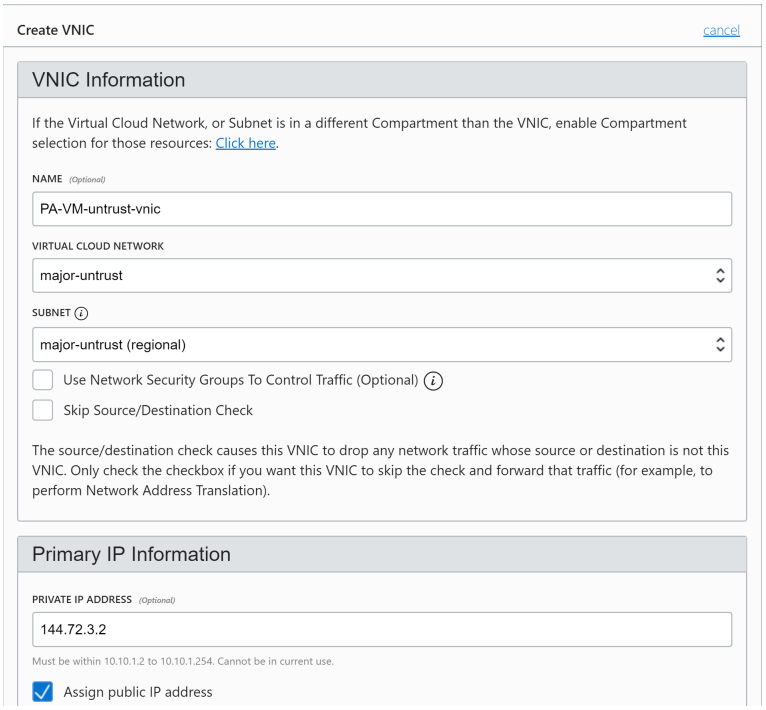
   ```
   ssh-i <private_key.pem> admin@<public-ip_address>
   ```
3. 使用以下命令并按照屏幕上的提示配置新密码：

   ```
   configure
   set mgt-config users admin password
   ```

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。

© 2019 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。**

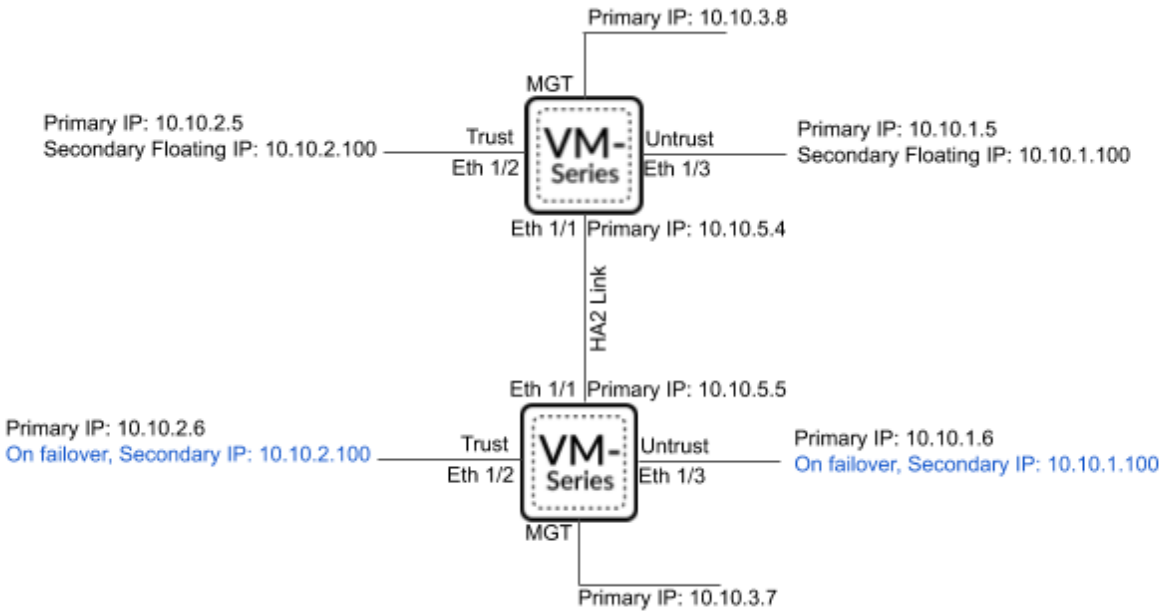
1. 登录到防火墙。
2. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网）。
3. 单击 **ethernet 1/1** 的链路并按如下所述配置：
   - **Interface Type**（接口类型）：**Layer3**
   - 在 **Config**（配置）选项卡上，将接口分配给默认路由器。
   - 在 **Config**（配置）选项卡上，展开 **Security Zone**（安全区域）下拉列表并选择 **New Zone**（新建区域）。定义新区域（如 untrust-zone），然后单击 **OK**（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。

© 2019 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。除了浮动 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。



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。
- **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。

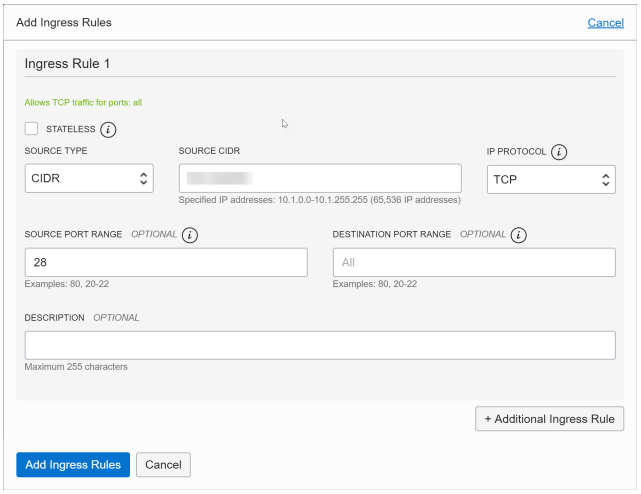
© 2019 Palo Alto Networks, Inc.

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。

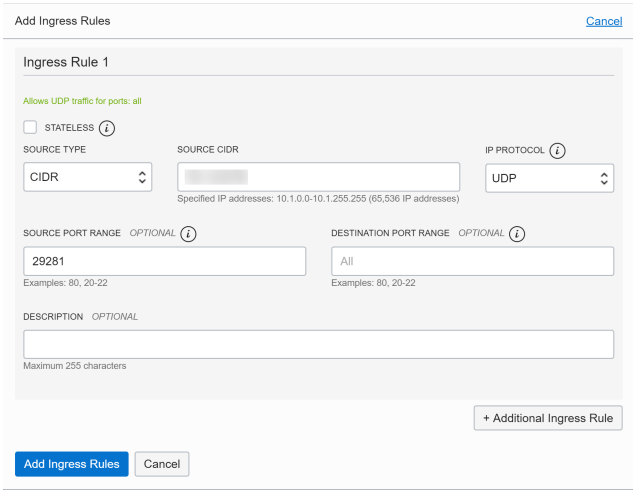
STEP 2 | 创建安全规则以允许 HA 对等同步数据并维护状态信息。默认情况下，OCI 仅允许 ICMP 流量。您必须打开必需的 HA 端口。

1. 然后，您需要打开 HA1 接口的端口。
   1. 在 OCI 控制台中，选择 **Networking**（联网）> **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）。



© 2019 Palo Alto Networks, Inc.

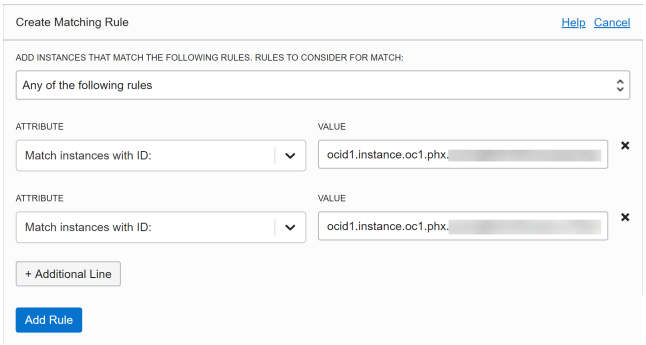
2. 打开 HA2 接口的端口。
    1. 在 OCI 控制台中，选择 **Networking**（联网）> **Virtual Cloud Networks**（虚拟云网络），然后选择 VCN。
    2. 选择 **Subnets**（子网），然后选择包含 HA2 接口的子网。
    3. 选择 **Security Lists**（安全列表），然后单击默认安全列表进行编辑。
    4. 单击 **Add Ingress Rule**（添加入口规则）。
    5. 输入包括 HA 对等 HA2 端口 IP 地址的 **Source CIDR**（源 **CIDR**）。
    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**。
    8. 单击 **Add Ingress Rule**（添加入口规则）。



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）。

© 2019 Palo Alto Networks, Inc.



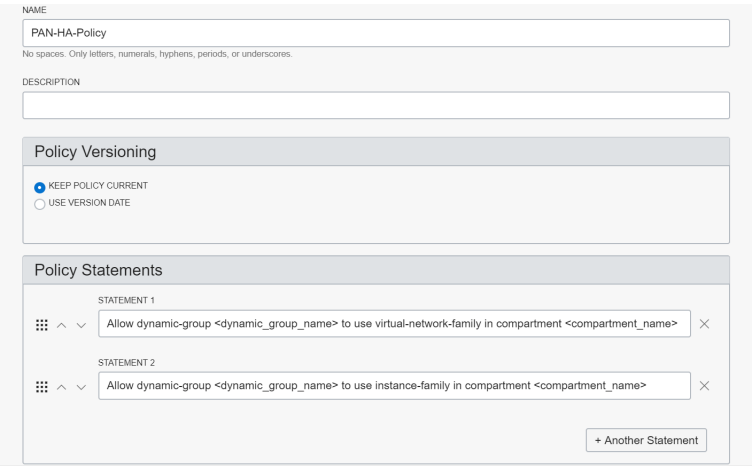
9. 单击 **Create Dynamic Group**（创建动态组）。

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）。



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。

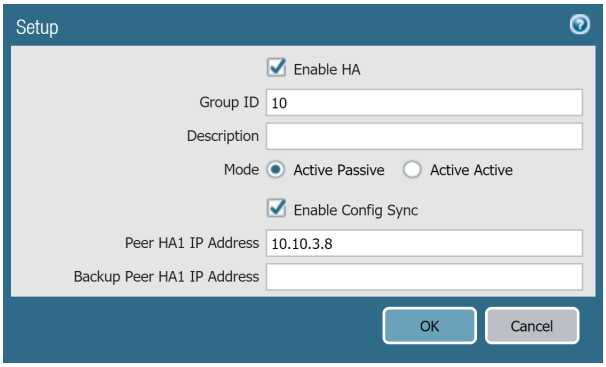
© 2019 Palo Alto Networks, Inc.

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）。
   - 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。

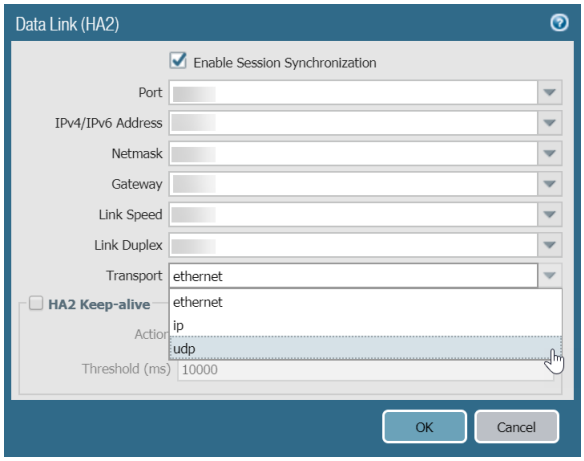
STEP 5 | 启用 HA。

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。

© 2019 Palo Alto Networks, Inc.



8. 单击 **OK**（确定）。

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**（仪表板），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）。

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。在此版本中，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 系列防火墙来保护北向南流量，以及在 Alibaba Cloud 的 VPC 上部署的应用程序的东向西向流量。

此版本在 Alibaba Cloud 的国际区域和中国大陆上支持自带许可证 (BYOL) 和 VM 系列 ELA。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 上运行，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 上目前不支持 PAYG 许可证和引导 *VM* 系列防火墙的能力。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。

© 2019 Palo Alto Networks, Inc.

Alibaba Cloud 上 VM 系列防火墙的最低系统要求

在 Alibaba Cloud 上，您可以使用内核虚拟化模块 (KVM) 管理程序在 Linux 服务器上部署 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

要在 Alibaba Cloud 上部署 VM 系列防火墙，必须先使用 VM 系列防火墙 qcow2 映像文件在 Alibaba Cloud 控制台中创建自定义映像。

- 选择 VM 系列 ELA 或 BYOL 许可证、容量许可证和订阅套餐。请参阅许可证类型 — VM 系列防火墙。
- VM 系列防火墙需要 qcow2 映像版本 9.1.0 或更高版本。
- 创建自定义映像时，请选择 KVM 上的 VM 系列防火墙—要求和先决条件中列出的受支持的 Linux 操作系统版本。

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	ecs.g5.xlarge、ecs.sn2ne.xlarge
VM-300	ecs.g5.xlarge、ecs.sn2ne.xlarge
VM-500	ecs.g5.2xlarge, ecs.sn2ne.2xlarge
VM-700	ecs.g5.4xlarge, ecs.sn2ne.4xlarge

Alibaba Cloud CLI

Aliyun 版本 3.0.4 或更高版本。

© 2019 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 系列防火墙以确保北向南流量安全的位置。防火墙必须能够检查进出应用程序的流量。

- 选择许可证和计划网络
- 在 Alibaba Cloud 控制台中创建自定义映像
- 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 | 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 2 | 规划和设计 VPC。

1. 为您的 VPC 和 VSwitch 规划网络，包括 CIDR 块。
2. 规划安全组织。

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。

   如果 *VM* 系列型号和*Alibaba Cloud*实例具有足够的资源，则 *VM* 系列防火墙最多支持 *8* 个接口。

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）。您将收到 VM 系列订阅的验证码。

STEP 4 | 规划如何配置 Alibaba 帐户和权限。如果您没有帐户，请参阅 Alibaba Cloud 免费试用： 如何注册并开始使用。

STEP 5 | 获得 Alibaba Cloud 的许可证。使用已选择使用VM 系列防火墙的 Alibaba Cloud 实例类型建议之一的 VM 系列型号。

在 Alibaba Cloud 控制台中创建自定义映像

KVM 上运行的 VM 系列防火墙。您必须使用 VM 系列防火墙 qcow2 映像文件为 Alibaba Cloud 制作自定义映像。为此，请将 VM 系列 qcow2 映像文件上传到对象存储服务存储桶并创建 Alibaba Cloud 自定义映像。

STEP 1 | 获取 VM 系列防火墙 qcow2 映像文件。

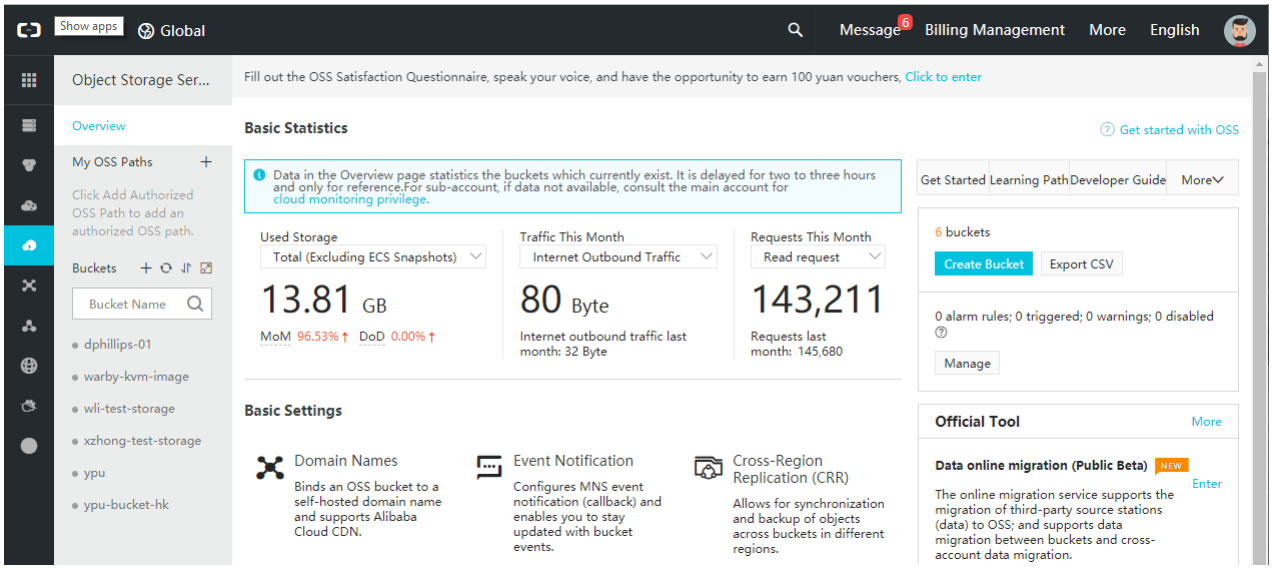
1. 登录 Palo Alto Networks 客户支持门户 (CSP) 并注册 VM 系列授权代码。创建支持帐户
2. 在 CSP 上，选择 **Updates**（更新）> **Software Updates**（软件更新），并从 **Filter By**（筛选条件）下拉菜单中，选择 **Pan OS for VM-Series KVM Base Image**（用于 **VM** 系列 **KVM** 基本映像的 **Pan OS**）并找到当前版本的 qcow2 文件。
3. 将 qcow2 文件下载到本地驱动器。例如，`PA-VM-KVM-9.1.0.qcow2`。

STEP 2 | 为 VM 系列映像创建存储桶。

1. 在 Alibaba Cloud 控制台主页上，选择对象存储服务 (OSS)。

© 2019 Palo Alto Networks, Inc.

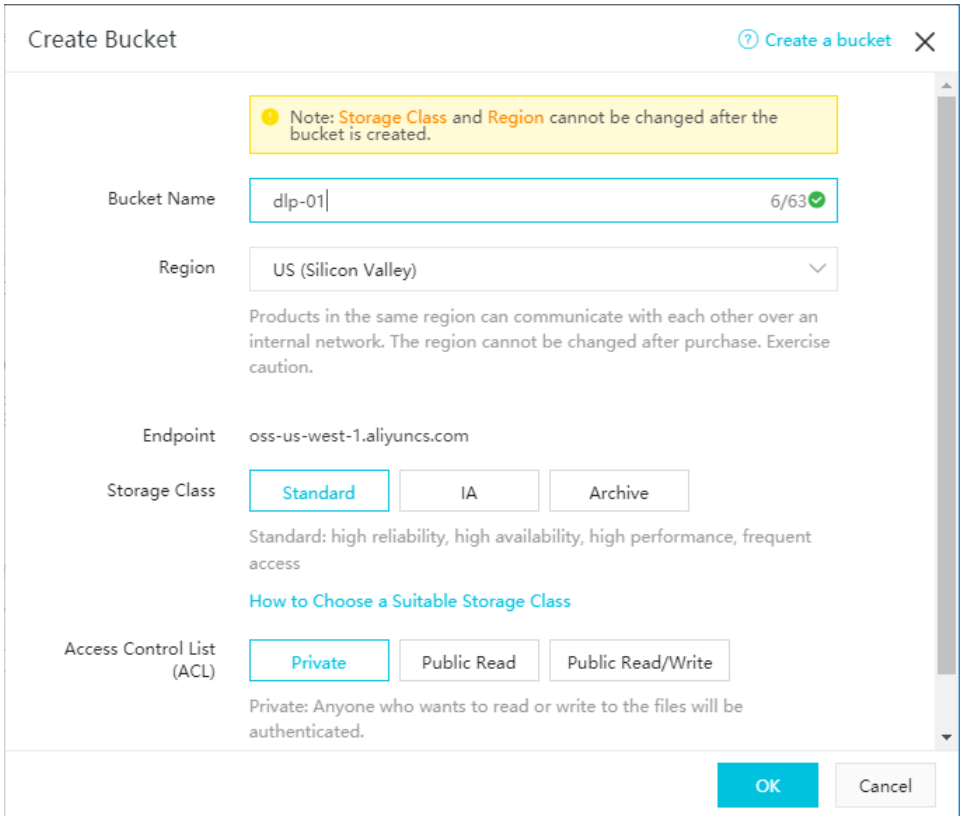
2. 单击右上角的 **Create Bucket**（创建存储桶），或选择现有存储桶。



3. 指定名称和区域。

   存储桶必须与计划部署 VM 系列防火墙的 VPC 位于同一区域。

4. 单击 **OK**（确定）。



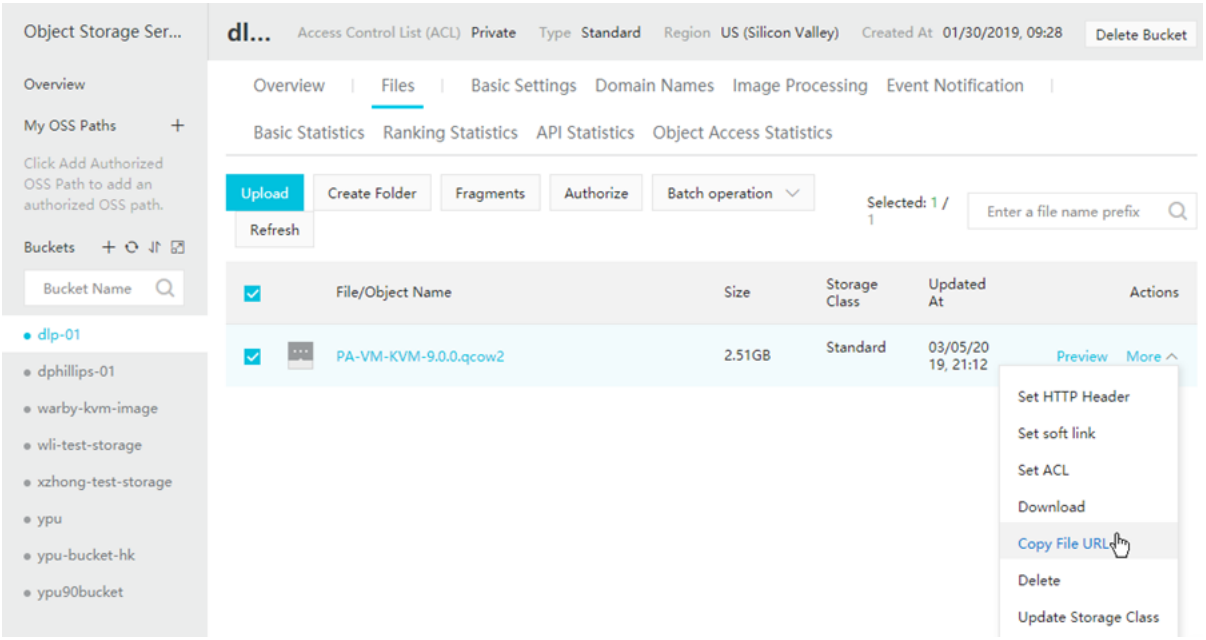
STEP 3 | 将 qcow2 映像文件上传到您的存储桶。

1. 选择存储桶，然后选择 **Files**（文件）> **Upload**（上传）和 **click here to upload**（单击此处上传）。
2. 选择本地驱动器上的 qcow2 映像文件。

© 2019 Palo Alto Networks, Inc.

STEP 4 | 复制 OSS 地址对象（文件 URL）。

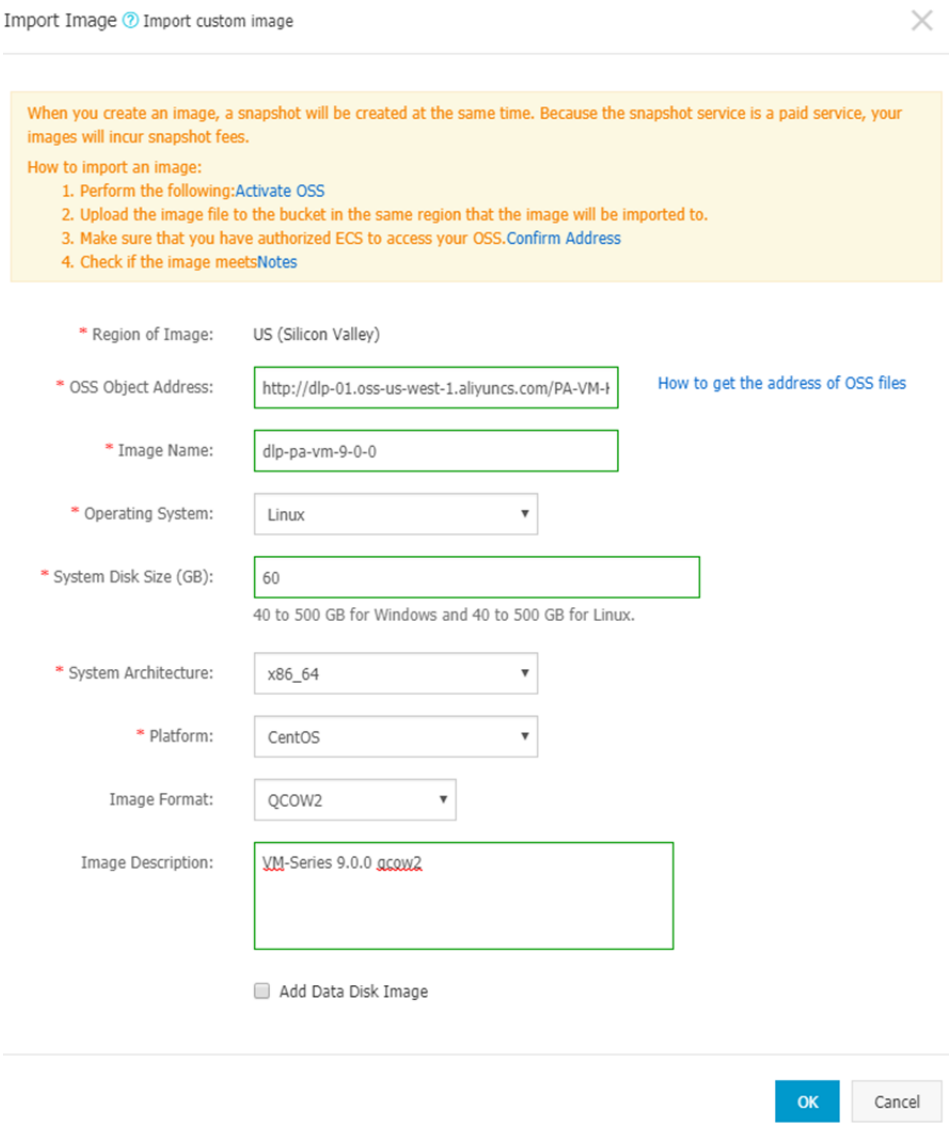
在存储桶中，选择 qcow2 映像文件的行，然后在 **Action**（操作）列中选择 **More**（更多）> **Copy File URL**（复制文件 **URL**），然后单击 **Copy**（复制）。



STEP 5 | 将 VM 系列防火墙映像导入 ECS。

1. 在 Alibaba Cloud 控制台主页上，选择弹性计算服务。
2. 选择 **Images**（映像），然后在右上角单击 **Import Image**（导入映像）。
3. 粘贴 OSS 对象地址，填写表单，然后单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.



映像将显示在 **Elastic Compute Services**（弹性计算服务）> **Images**（映像）列表中。

准备使用 Aliyun 命令行界面

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。如果要使用 VM 系列防火墙来保护 Alibaba Cloud 上的负载均衡，则需要 CLI。

安装并配置最新版本的 Aliyun，即 Alibaba Cloud 命令行界面。

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。

该区域必须与在 Alibaba Cloud 控制台中创建自定义映像中包含 qcow2 文件的存储区域匹配。

© 2019 Palo Alto Networks, Inc.

```
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:
...
```


© 2019 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。来自应用程序的返回流量进入防火墙的可信界面。防火墙检查返回流量并通过不可信接口发送出去。

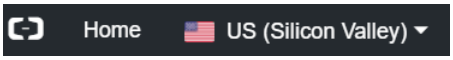
以下任务演示如何使用控制台创建 VM 系列防火墙基础架构。

- 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。

STEP 1 | 打开 VPC 控制台并从菜单中选择所在的区域。它必须使用与为 VM 系列防火墙创建的自定义映像相同的区域。



STEP 2 | 在 Alibaba Cloud 控制台主页中，选择 **Products**（产品），并从联网类别中选择 **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 控制台以相同的形式中创建 VPC 和 Switch。

1. 创建 VPC。

   指定 VPC 名称、IPv4 CIDR 块和描述。
2. 创建管理 VSwitch。
   - 命名 VSwitch 为 **`Management`**。
   - 选择区域，指定 IPv4 CIDR 块，然后指定说明。
   - 在底部单击 **Add**（添加）以添加另一个 vSwitch。
3. 以相同的方式创建不可信 VSwitch。
4. 创建可信 VSwitch。
5. 单击 **OK**（确定）。

STEP 4 | 创建安全组和安全组规则。

- 在 Alibaba Cloud 控制台主页中，选择 **Elastic Compute Service**（弹性计算服务），从 **Networks and Security**（网络与安全）菜单中，选择 **Security Groups**（安全组）。
- 在右上角单击 **Create Security Group**（创建安全组）

1. 创建管理安全组。

   参阅创建安全组以填写此表格。

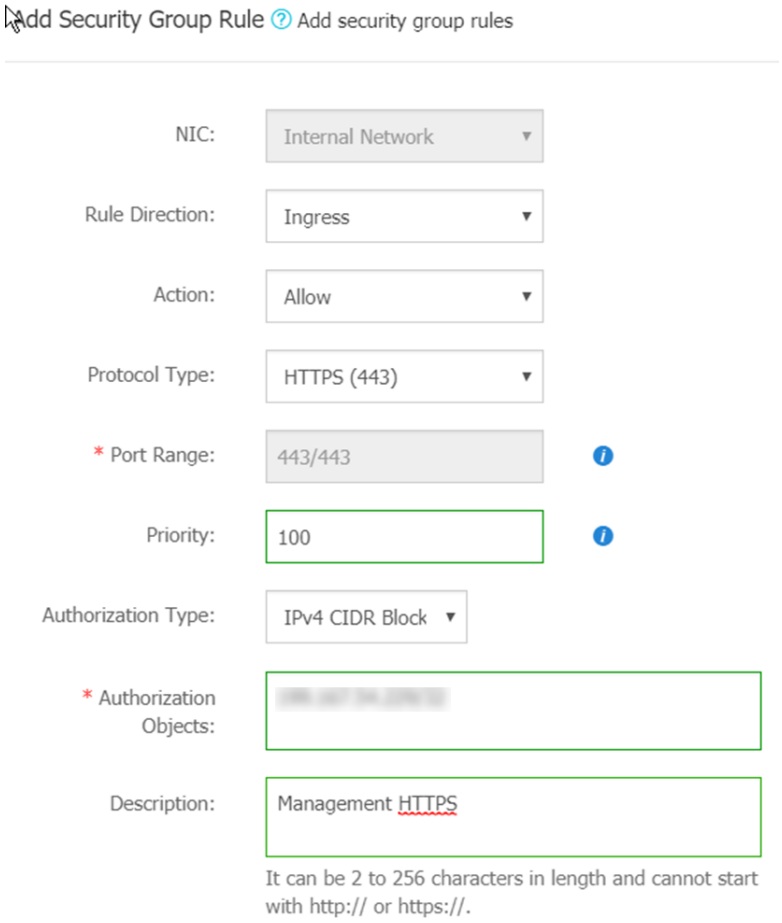
© 2019 Palo Alto Networks, Inc.

属性	值
模板	自定义
安全组名称	管理
网络类型	VPC
VPC	选择之前创建的 VPC。

- 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。
- 单击 **Create Rules Now**（立即创建规则）。

  该过程介绍了一些基本安全组规则。您可以创建其他规则来强制执行网络安全要求。
- • 选择“Ingress（入口）”选项卡，然后选择 **Add Security Group Rule**（添加安全组规则）。
  • 创建入口规则以允许此安全组中的 HTTPS。例如：

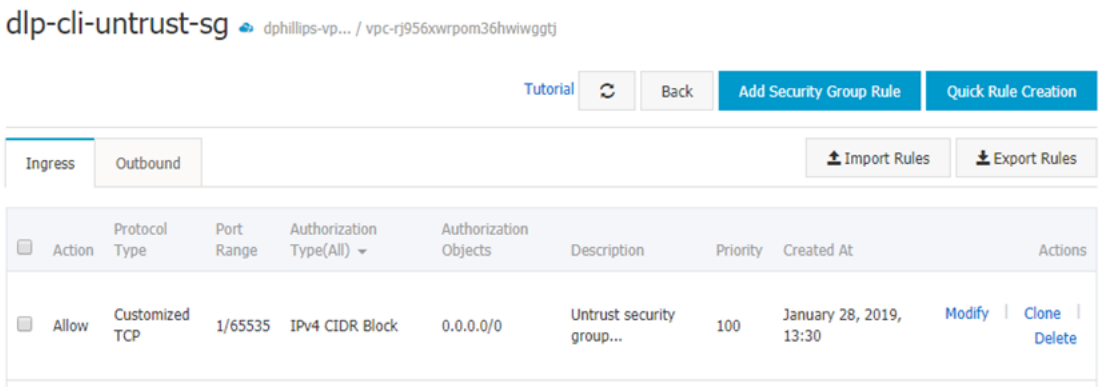


- 创建入口规则以在管理接口上允许 SSH。
  - 选择 SSH (22) 协议类型并相应地命名规则。
  - 单击 **OK**（确定）并返回安全组列表。

2. 创建不可信安全组。

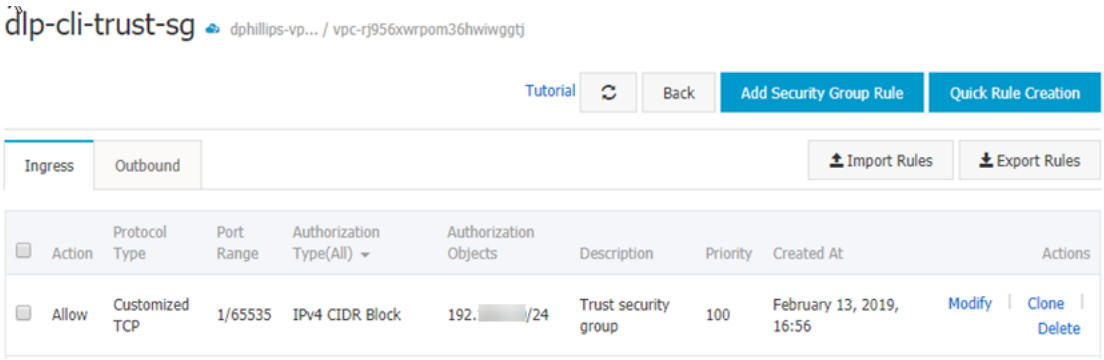
© 2019 Palo Alto Networks, Inc.

出现提示时，为不可信安全组创建规则。



3. 创建可信安全组。

   出现提示时，为可信安全组创建以下规则。



创建和配置 VM 系列防火墙

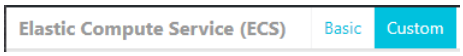
VM 系列防火墙需要至少有三个接口：管理、不可信和可信。

此任务使用 ECS 控制台创建 VM 系列防火墙实例。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 | 打开 ECS 控制台并选择 **Instances**（实例）。

STEP 2 | 在右上角，选择 **Create Instance**（创建实例）。

STEP 3 | 选择 **Custom**。



STEP 4 | 基本配置。

1. 填写以下值。

属性	值
计费方式	现收现付
区域	美国西部 1（硅谷）。您也可以选择区域。

© 2019 Palo Alto Networks, Inc.

属性	值
实例/实例类型	ecs.sn2ne.xlarge
映像	选择 **Custom Image**（自定义映像）并选择在 在 Alibaba Cloud 控制台中创建自定义映像中创建的自定义映像。
存储	选择磁盘类型并指定 60 GiB。

2. 选择 **Next**（下一步）：**Networking**（网络）。

STEP 5 | 在“网络”页面上，提供以下值。

1. 网络 (VPC)。
   - 选择在创建 VPC 并配置网络 中创建的 VPC。
   - 选择管理 VSwitch。
2. 网络计费方法。

   此时不要分配公共 IP 地址。
3. 弹性网络接口。

   管理界面已附加到 eth0。
4. 选择 **Next**（下一步）：**System Configurations**（系统配置）。

STEP 6 | 在“系统配置”页面上，填写以下值。

1. 登录凭据：选择 **Inherit Password from Image**（从映像继承密码）。

   VM 系列防火墙的默认用户名是 admin，密码也是 admin。
2. 命名 VM 系列防火墙实例。

STEP 7 | 选择“预览”以查看到目前为止的设置。

进行任何更正。

STEP 8 | 选择 **Create Instance**（创建实例）以创建 VM 系列防火墙实例。

STEP 9 | 从控制台主页中，选择 > **Elastic Compute Service**（弹性网络服务） > **Networks and Security**（网络和安全） > **ENI** 并单击右上角 **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。
2. 创建可信 ENI。

STEP 10 | 将 ENI 附加到 VM 系列防火墙不可信和可信接口。

1. 附上不可信 ENI。
2. 附上可信 ENI。

STEP 11 | 立即更改默认用户名和密码。

使用 VNC 控制台连接到管理终端，并登录到 ECS 实例，并更改 VM 系列防火墙的默认用户名和密码 (admin/admin)。如果不知道 VNC 连接密码，则必须为 VNC 控制台更改密码。

在将 *IP* 地址与任何网络接口关联之前，请更改 *VM* 系列防火墙用户名和密码。

STEP 12 | 分配两个弹性 IP (EIP) 地址。

© 2019 Palo Alto Networks, Inc.

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。

STEP 13 | 将 EIP 与 VM 系列防火墙管理接口相关联。

STEP 14 | 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 15 | 重新启动实例以附加新的网络接口。

在实例列表中，选择实例并单击 **Manage**（管理），然后单击右上角的 **Restart**（重新开始）。

STEP 16 | 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。

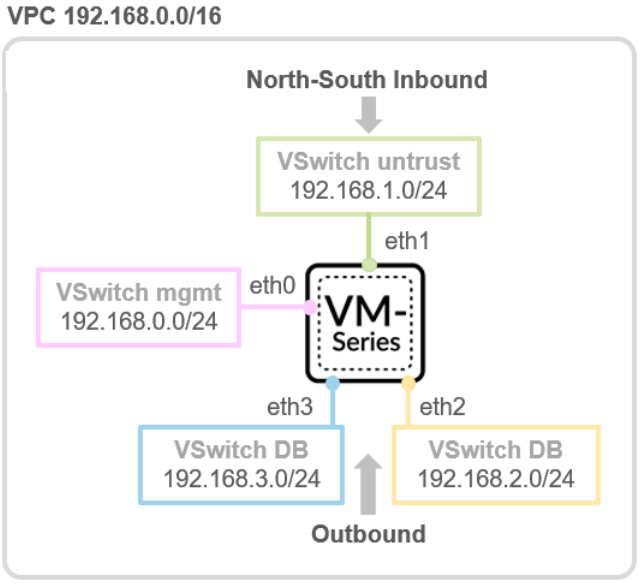
确保 Alibaba Cloud 的北向南流量安全

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。四个 VSwitch 创建四个子网。

VSwitch 名称	接口	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 系列防火墙在每个 VSwitch 中都有一条支路。通常，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。

© 2019 Palo Alto Networks, Inc.



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>
                 <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>
```

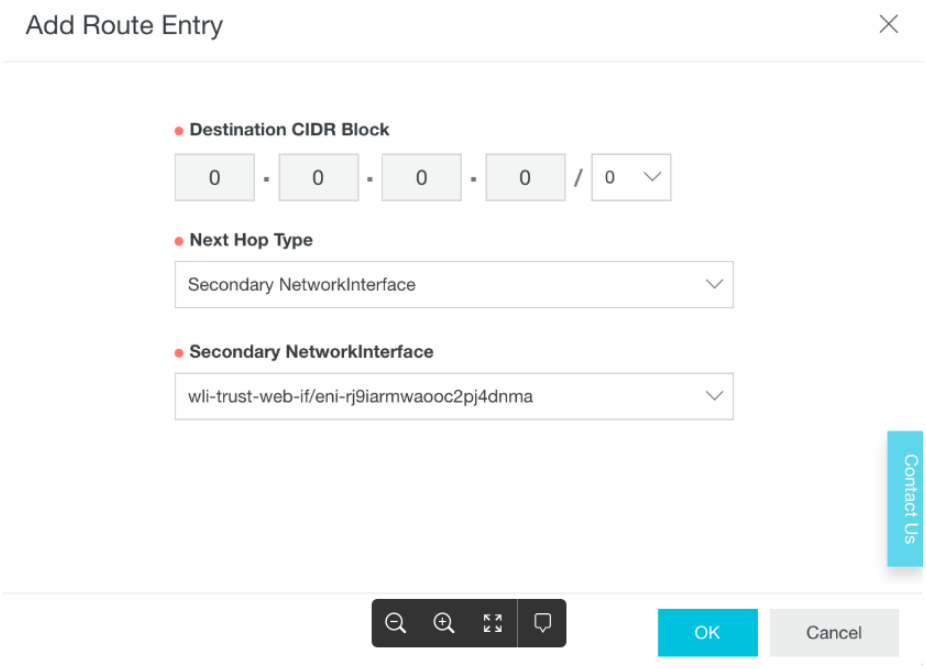

© 2019 Palo Alto Networks, Inc.

```
            </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>
```

STEP 2 | 保护出站流量。

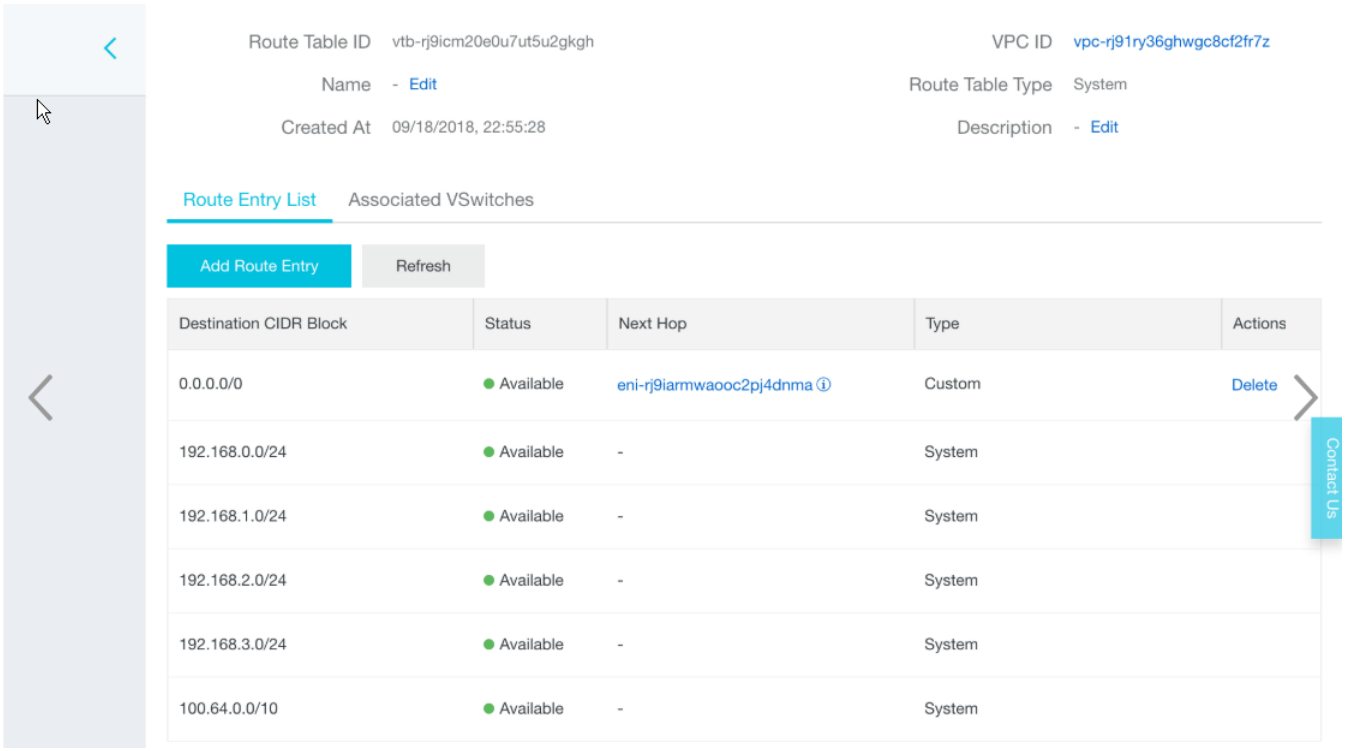
如上图所示，应用程序启动出站流量。例如，Web 服务器必须运行 **`yum install`** 以更新 rpm 数据包。通常，面向 VPC 内的流量的 Internet 被路由到 NAT 网关（附有 EIP）。要保护出站流量，必须强制出站流量通过 VM 系列防火墙。

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 NH。



2. 在路线表中查看您的条目。

© 2019 Palo Alto Networks, Inc.



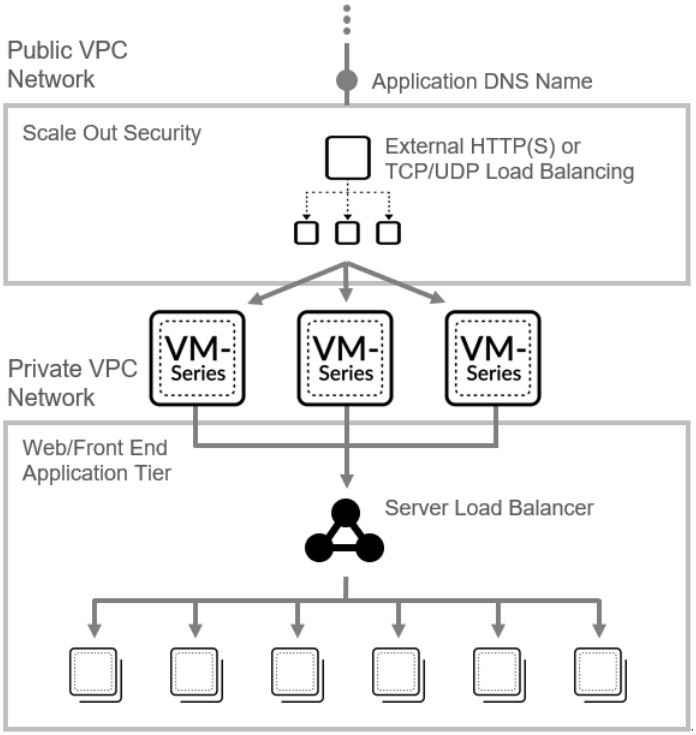
3. 使用不可信接口 IP 配置 SNAT 规则，以确保从 Internet 返回的流量通过 VM 系列防火墙。
   这是一个 SNAT 配置示例。

```
<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>
```


© 2019 Palo Alto Networks, Inc.

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。



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。

您必须准备使用 Aliyun 命令行界面以使用以下 *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": "wli-slb",
        "Address": "***********,
        "ResourceGroupId": "rg-************ofi",
        "RequestId": "0B8BA2AA-E837-45EE-B7F1-B82A8A1D5FBB",
```


© 2019 Palo Alto Networks, Inc.

```
        "AddressIPVersion": "ipv4",
        "LoadBalancerId": "lb-******************mvz",
        "VSwitchId": "",
        "VpcId": "vpc-*****************r7z"
}
```

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 '/'
```

在 *Cisco ACI* 中设置防火墙

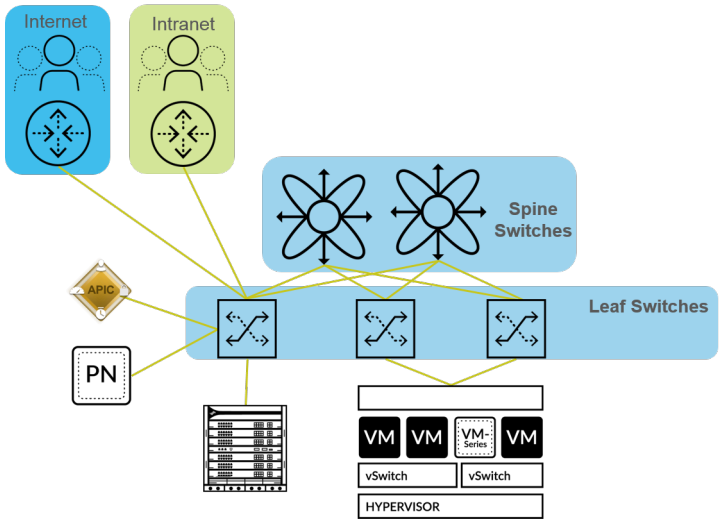
Palo Alto Networks 将服务与 Cisco 以应用为中心的基础架构 (ACI) 集成在一起。ACI 是一种软件定义网络 (SDN) 解决方案，可轻松部署新的工作负载和网络服务。使用名为 Cisco 应用策略基础设施控制器 (APIC) 的 SDN 控制器，您可以在端点组 (EPG) 之间部署防火墙服务。EPG 充当应用程序或应用程序层的容器。在 EPG 之间放置防火墙时，防火墙上配置的安全策略可确保 EPG 之间的通信。APIC 为管理整个数据中心的网络拓扑结构，网络策略和连接提供了一个单一的平台，并支持插入 L4 - L7 设备，如基于硬件或 VM 系列的防火墙。Panorama 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

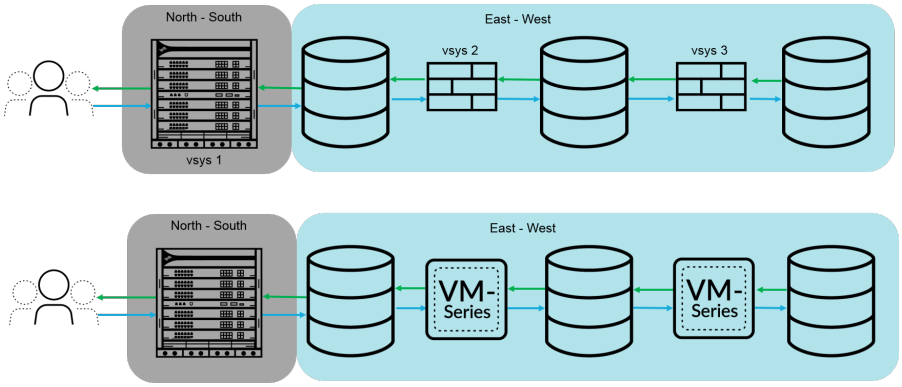
Palo Alto Networks 防火墙与 Cisco ACI 集成

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的地。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

© 2019 Palo Alto Networks, Inc.

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群集。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。

© 2019 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 基于您的管理程序。

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，作为受管设备。

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。
- 寄存器和激活许可证在您的 VM 系列防火墙上。
- 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。

© 2019 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
- 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。

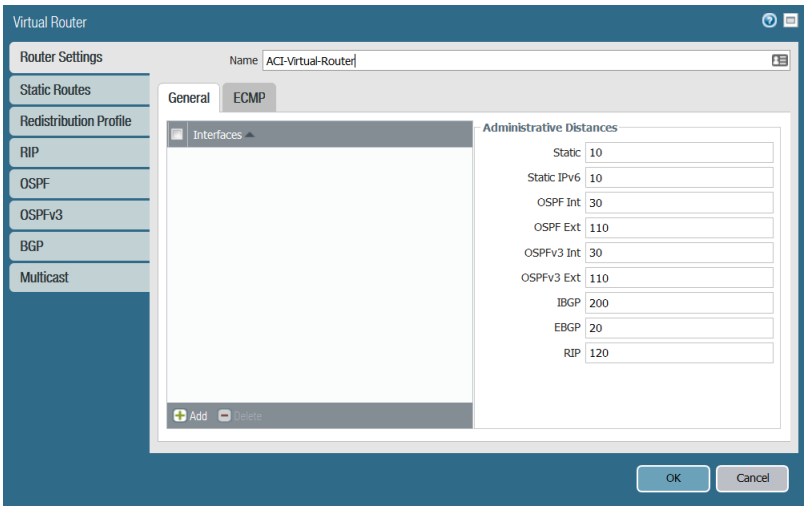
STEP 1 | 登录到防火墙。

STEP 2 | 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后单击 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

STEP 3 | 输入虚拟路由器的描述性 **Name**（名称）。

STEP 4 | 单击 **OK**（确定）。

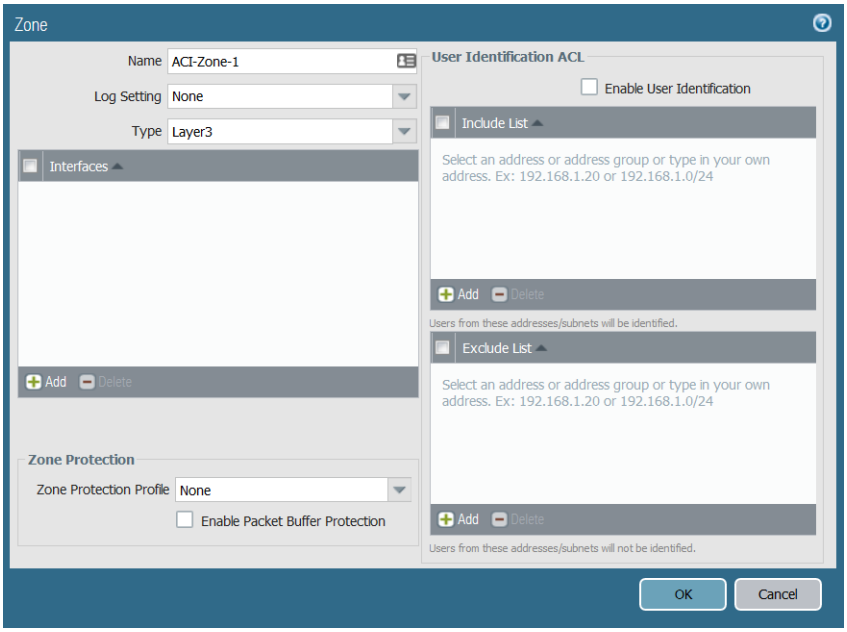


STEP 5 | 选择 **Network**（网络）> **Zones**（区域），然后单击 **Add**（添加）。

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“第 3 层”。

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。

© 2019 Palo Alto Networks, Inc.

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）下列列表中选择“Layer 3（第 3 层）”。

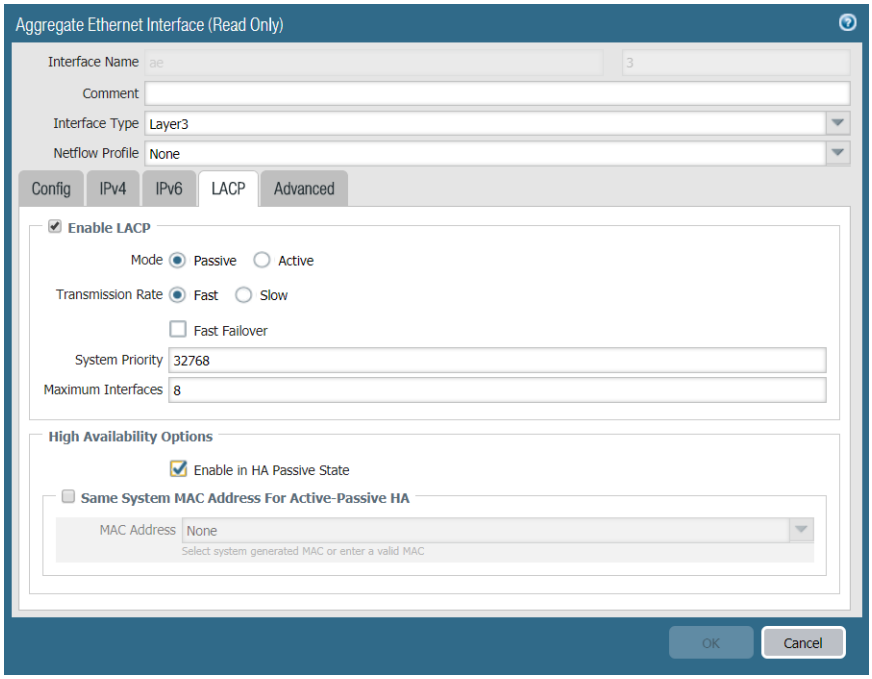
STEP 4 | 选择 **LACP** 选项卡，然后单击 **Enable LACP**（启用 **LACP**）。

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。

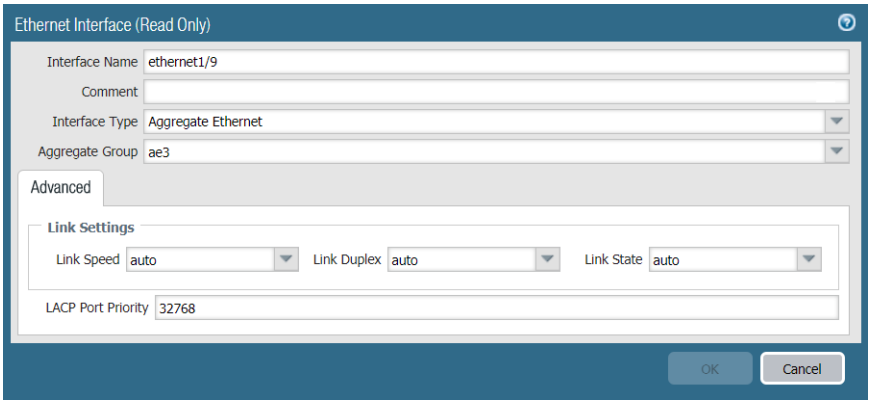
STEP 7 | 单击 **OK**（确定）。



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）”下列列表中选择 **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。

© 2019 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。

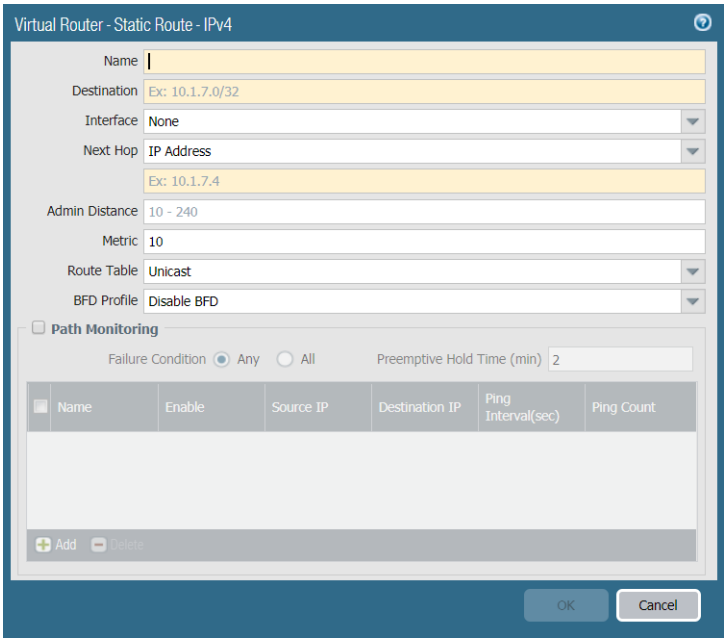
STEP 6 | 从 **Next Hop**（下一个跃点）下拉列表中中选择 IP 地址，并输入下一个跃点路由器的 IP 地址。

STEP 7 | 单击 **OK**（确定）。

STEP 8 | 再次单击 **OK**（确定）。

STEP 9 | **Commit**（提交）更改。

© 2019 Palo Alto Networks, Inc.



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。

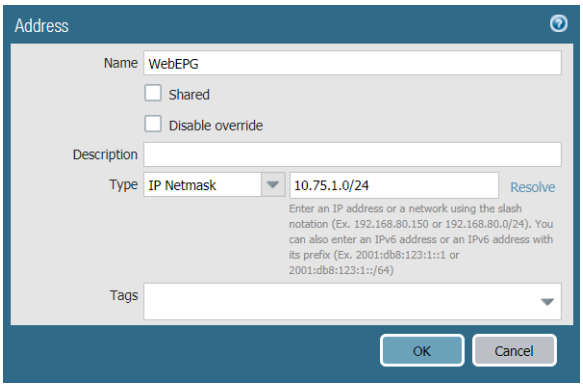
STEP 3 | 从 **Type**（类型）下拉列表中选择 IP 网络掩码。

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。



© 2019 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”。

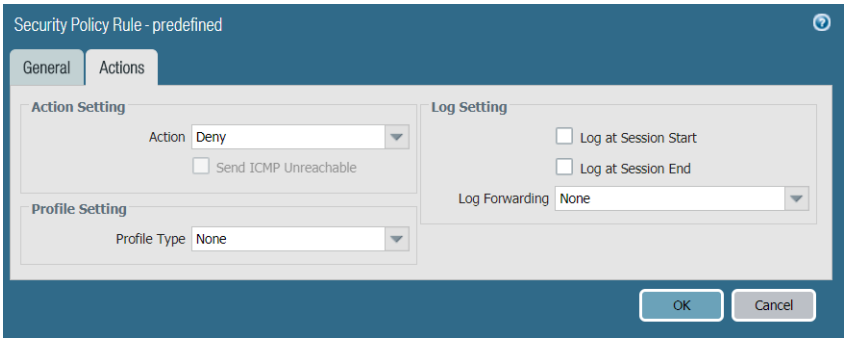
STEP 1 | 选择 **Policies**（策略）> **Security**（安全）。

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。

	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit			
1	WebToApp	none	intrazone	ACI-Zone-1	WebEPG	any	any	(intrazone)	AppEPG	-	-	-	ssl	application-d...	Allow
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	0	-	-	any	any	Deny

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 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）。

STEP 2 | （Physical firewall only（仅限物理防火墙））创建物理域。

© 2019 Palo Alto Networks, Inc.

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 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**（虚拟联网）> **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。

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）。

© 2019 Palo Alto Networks, Inc.

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。

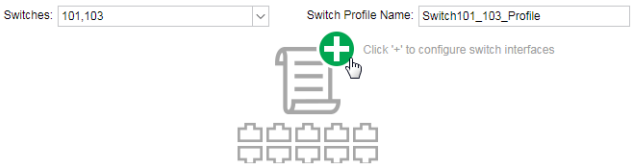
STEP 1 | 选择 **Fabric**（结构）> **Access Policies**（访问策略）> **Quick Start**（快速入门）。

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 (+)。



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。

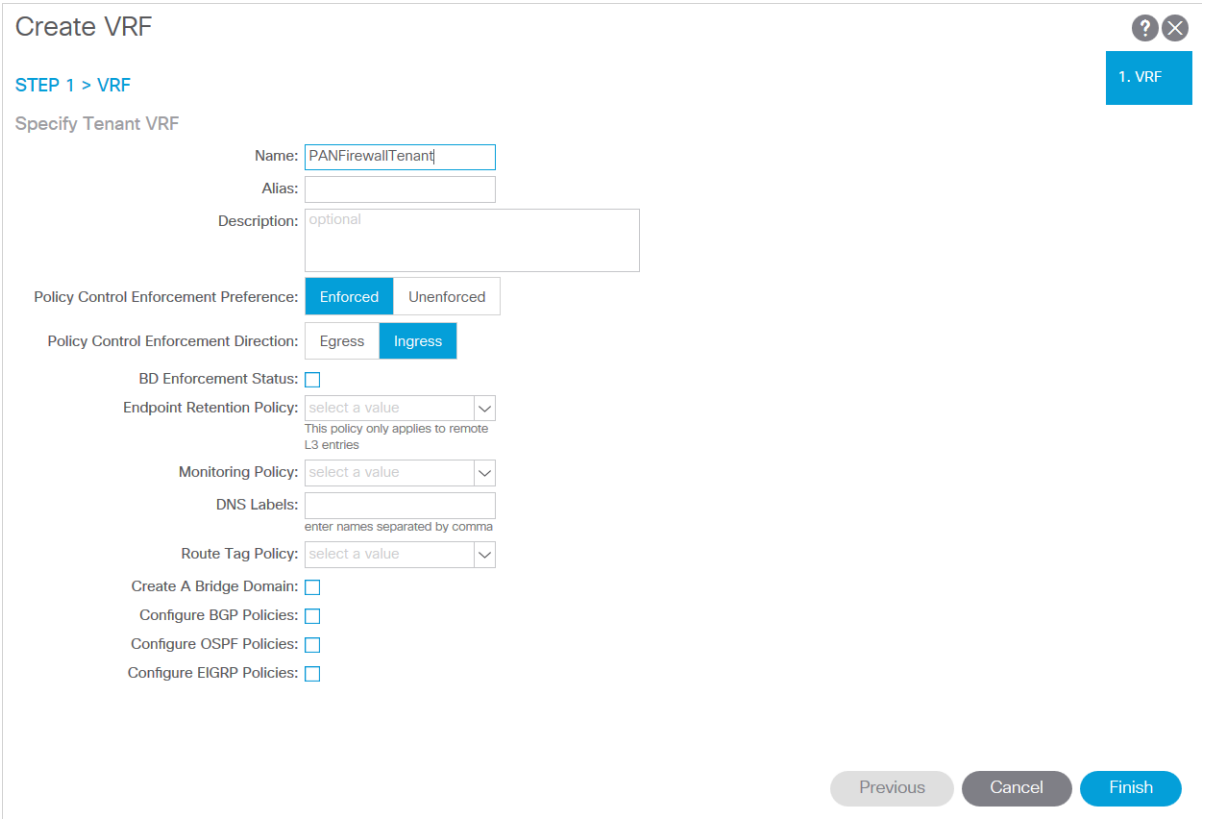
创建 *VRF* 和桥接域

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。

STEP 1 | 创建一个 VRF。

© 2019 Palo Alto Networks, Inc.

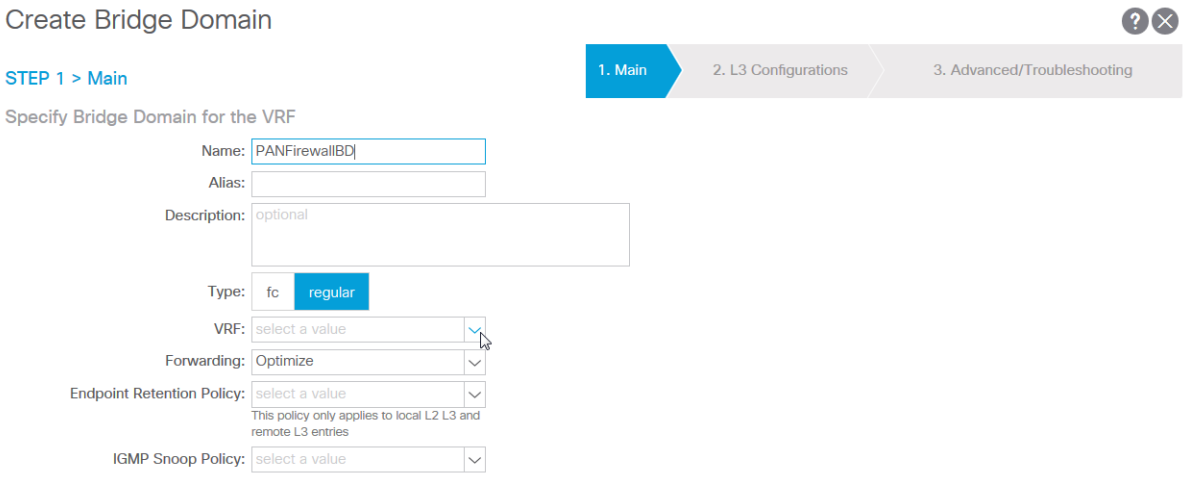
1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Networking**（联网）> **VRF**。
3. 右键单击 **VRF**，然后选择 **Create VRF**（创建 **VRF**）。
4. 输入 VRF 的描述性 **Name**（名称）。
5. 清除 **Create A Bridge Domain**（创建桥接域）复选框。
6. 单击 **Finish**（完成）。



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**（联网）> **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）。

© 2019 Palo Alto Networks, Inc.



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。

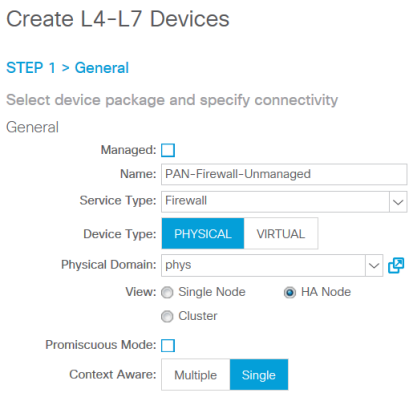
STEP 5 | 输入 L4-L7 的描述性 **Name**（名称）。

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。

STEP 9 | 为 **View**（视图）选择 HA 节点。



© 2019 Palo Alto Networks, Inc.

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 1**（设备 **1**）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**（群集接口）右侧的加号 (+) 图标。

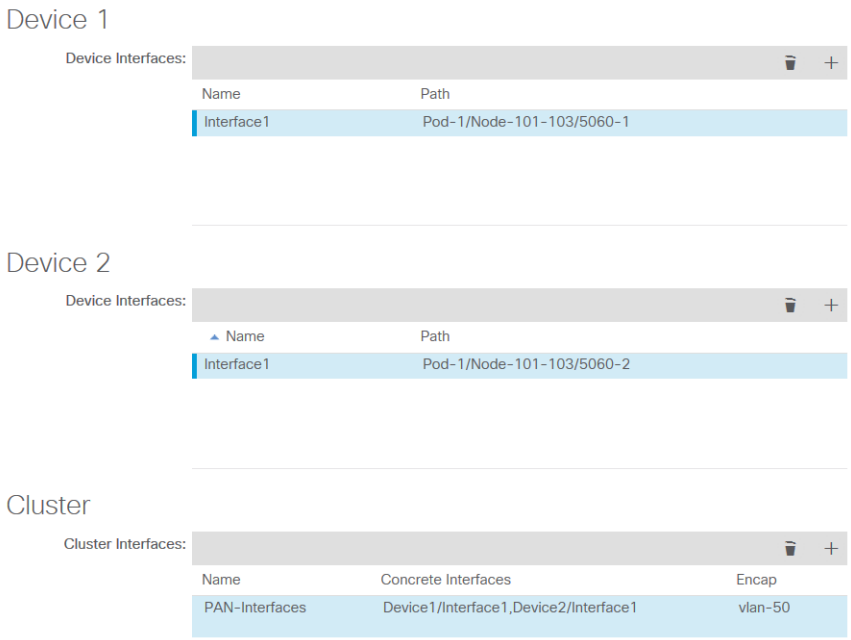
STEP 19 | 输入群集的描述性 **Name**（名称）。

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）。

STEP 23 | 单击 **Finish**（完成）。



© 2019 Palo Alto Networks, Inc.

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）。

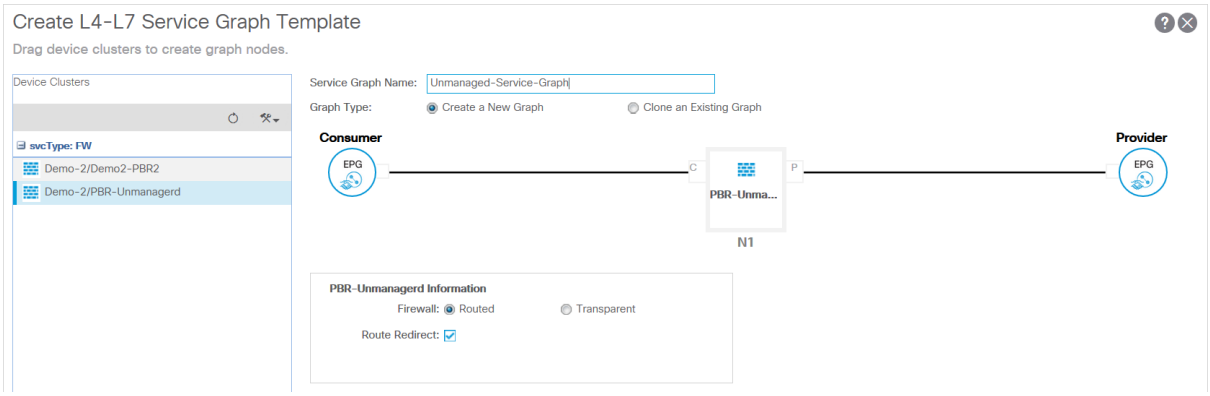
创建和应用 *Service Graph* 模板

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。

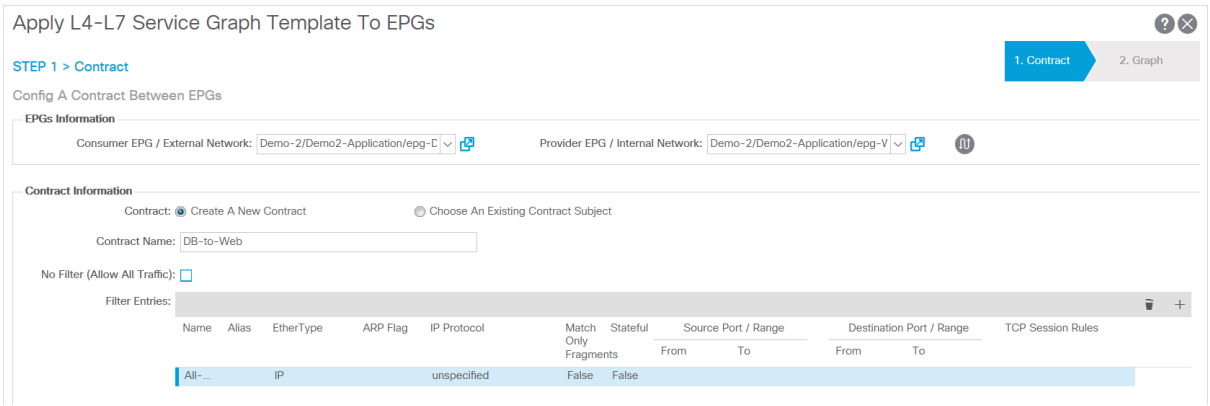
1. 在 **Tenants**（租户）选项卡上双击租户名称。
2. 选择 **Services**（服务）> **L4-L7** > **L4-L7 Service Graph Templates**（**L4-L7 Service Graph** 模板）。
3. 右键单击 **L4-L7 Service Graph Template**（**L4-L7 Service Graph** 模板）并选择 **Create L4-L7 Service Graph Template**（创建 **L4-L7 Service Graph** 模板）。
4. 为 Service Graph 模板输入描述性 **Graph Name**（图标名称）。
5. 选择 创建一个新的 对于 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）。

© 2019 Palo Alto Networks, Inc.



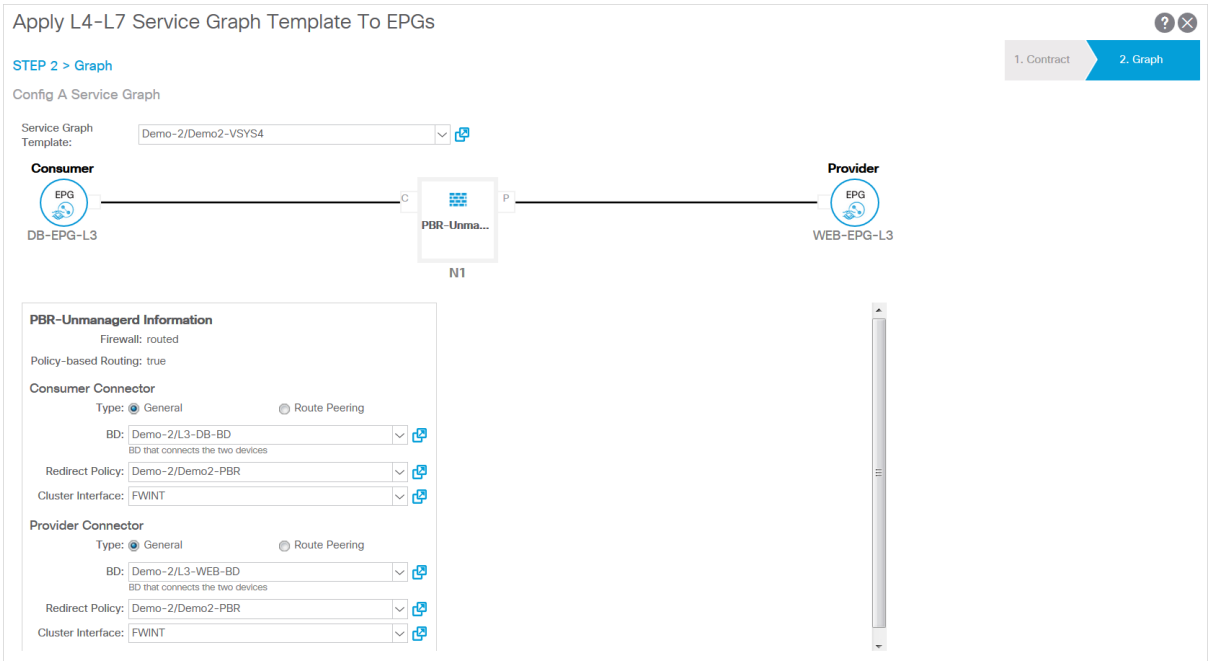
STEP 2 | 应用 Service Graph 模板。

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 信用）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”（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 设备创建的群集接口。

© 2019 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 —

- 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

© 2019 Palo Alto Networks, Inc.

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 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）。

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 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）。

© 2019 Palo Alto Networks, Inc.

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。

STEP 1 | 在 **Tenants**（租户）选项卡上双击租户名称。

STEP 2 | 选择 **Networking**（联网）> **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）。

STEP 13 | 为节点配置文件附加 OSPF 接口配置文件。

© 2019 Palo Alto Networks, Inc.

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）。

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**（联网）> **Bridge Domains**（桥接域）> **<your bridge domain>**（**<**您的桥接域**>**）。

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。

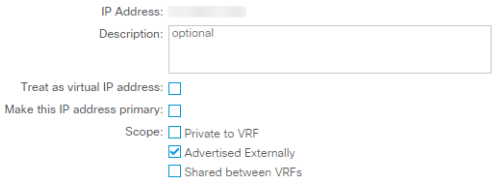
© 2019 Palo Alto Networks, Inc.

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**（联网） > **Bridge Domains**（桥接域） > **<your bridge domain>**（**<**您的桥接域**>**） > **Subnets**（子网） > **<externally advertised subnet>**（**<**向外部公布的子网**>**）。

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）。

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。

© 2019 Palo Alto Networks, Inc.

6. 单击 **Update**（更新）。

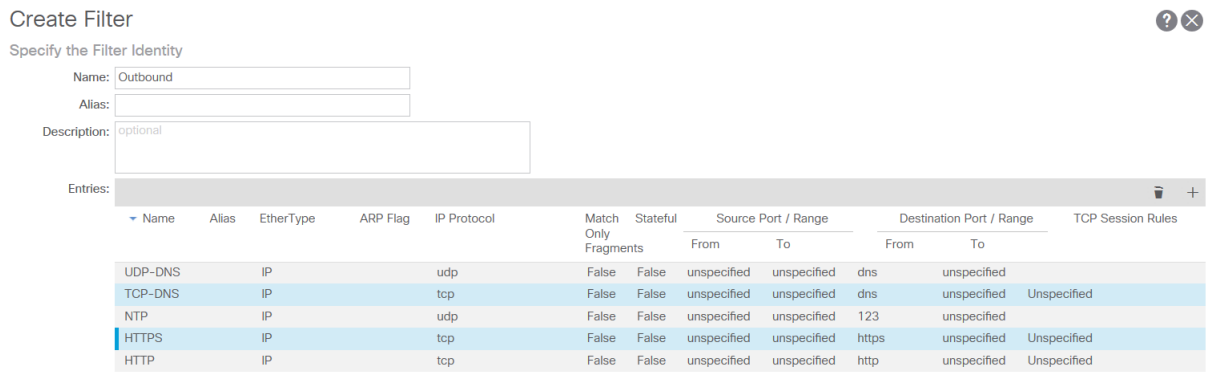
STEP 8 | 为 HTTP 流量创建筛选条目。

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）。

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。

© 2019 Palo Alto Networks, Inc.

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）。

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。

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**（联网）> **VRF** > <您的 **VRF**> > **EPG Collection for VRF**（**VRF** 的 **EPG** 集）。

© 2019 Palo Alto Networks, Inc.

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**（联网）> **External Routed Networks**（外部路由网络）> **<your external routed network>**（您的外部路由网络）> **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>**（您的应用程序配置文件）> **Application EPGs**（应用程序 EPG）> **<your application EPG>**（您的应用程序 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. 在同一个租户上，选择 **Networking**（联网）> **External Routed Networks**（外部路由网络）> **<your external routed network>**（您的外部路由网络）> **Networks**（网络）> **External**（外部）。
7. 在“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

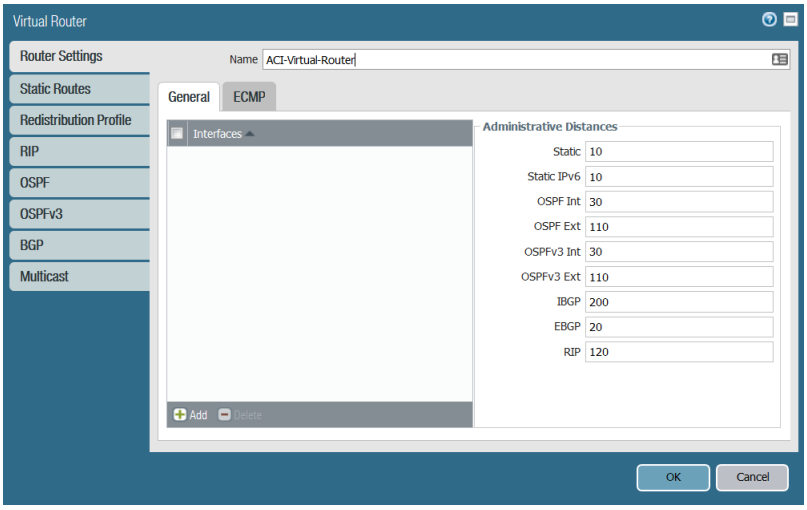
在防火墙上创建虚拟路由器和安全区域，以匹配 ACI 上的租户和 VRF。

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）。

STEP 4 | 单击 **OK**（确定）。



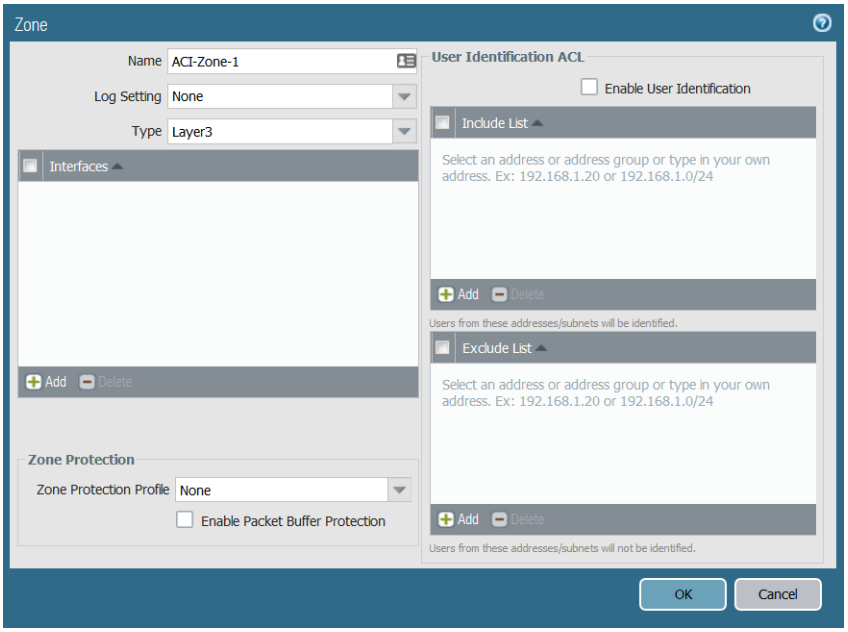
STEP 5 | 选择 **Network**（网络）> **Zones**（区域），然后单击 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

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“第 3 层”。

STEP 8 | 单击 **OK**（确定）。



STEP 9 | **Commit**（提交）更改。

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）下列列表中选择“Layer 3（第 3 层）”。

STEP 4 | 选择 **LACP** 选项卡，然后单击 **Enable LACP**（启用 **LACP**）。

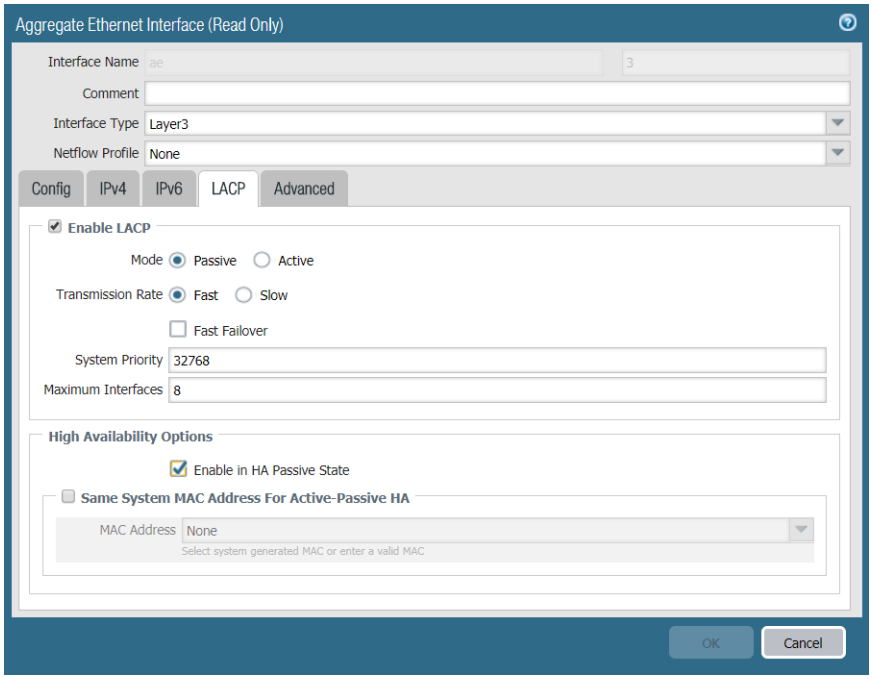
STEP 5 | 选择 **Fast**（快速）作为 **Transmission Rate**（传输速率）。

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。

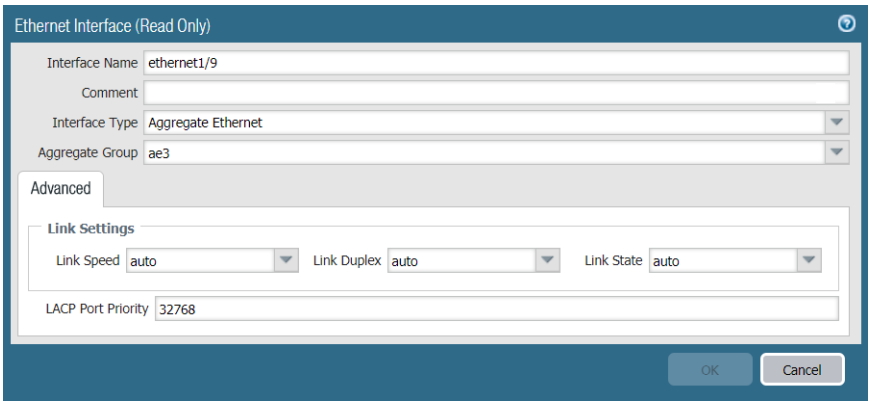
STEP 7 | 单击 **OK**（确定）。

© 2019 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）”下列列表中选择 **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）。

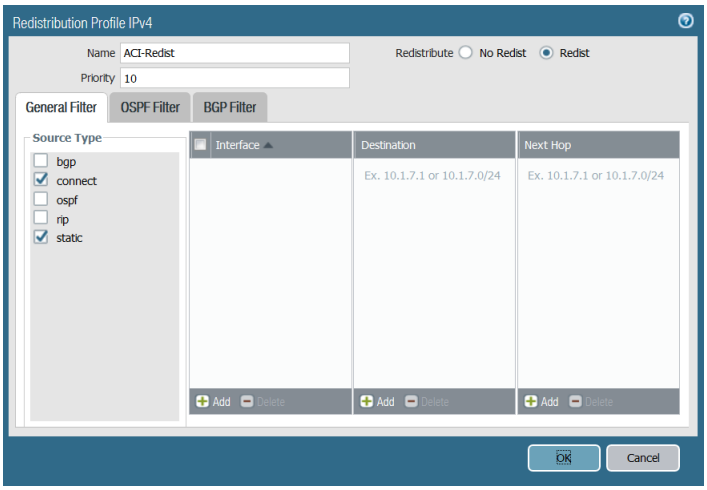
© 2019 Palo Alto Networks, Inc.

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。

STEP 1 | 配置路由重新分发。

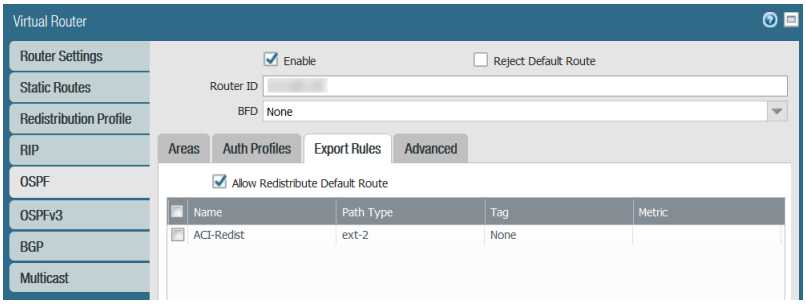
1. 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后单击之前创建的虚拟路由器。
2. 选择 **Redistribution Profile**（重新分发配置文件）> **IPv4** > **Add**（添加）。
3. 输入重新分发配置文件的描述性 **Name**（名称）。
4. 输入优先级。
5. 对于 **Redistribute**（重新分发），请选择 **Redist**（重新分发）。
6. 在 **General Filters**（常规筛选器）下选中 **Connect**（连接）和 **Static**（静态）。
7. 单击 **OK**（确定）。



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）。

© 2019 Palo Alto Networks, Inc.

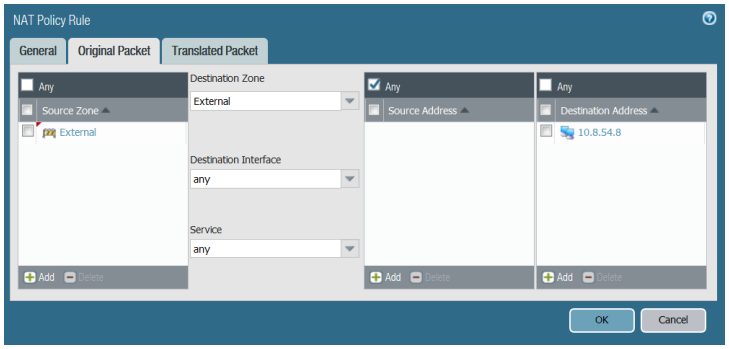


为外部连接配置 *NAT*

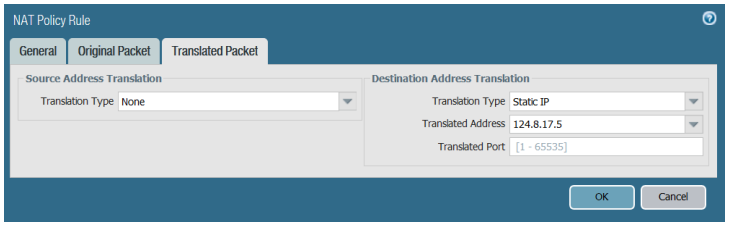
如果防火墙具有用于连接到数据中心外部网络的外部接口，则只需配置 NAT。虽然不需要 NAT，但您可以使用此过程将数据中心的专用 IP 地址转换为外部的公共 IP 地址。为了让流量进入数据中心 EPG 内部的服务器，开始通过配置地址转换来设置 NAT。然后配置 NAT 策略，将来自任何 EPG 的出站流量的源地址转换为外部接口 IP 地址。

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** 并单击 **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）。

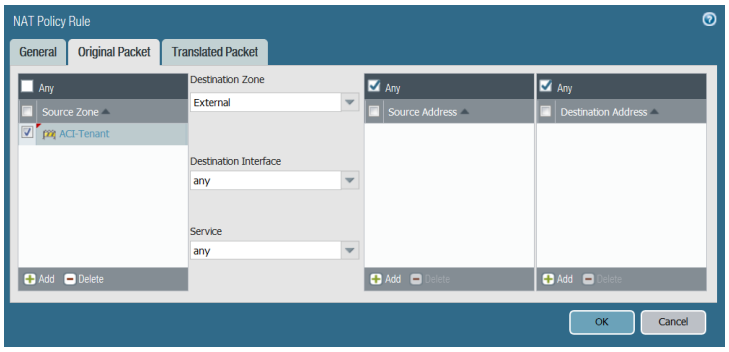


STEP 2 | 配置出站流量的地址转换。

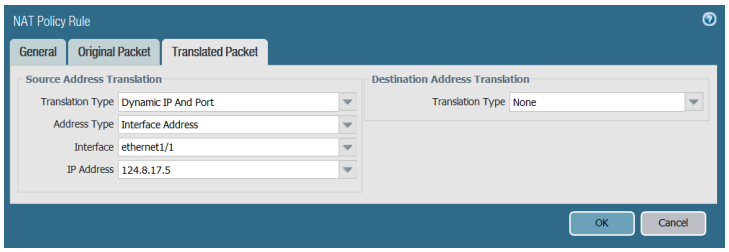
1. 选择 **Policies**（策略）> **NAT** 并单击 **Add**（添加）。
2. 输入出站 NAT 策略的描述性 **Name**（名称）。
3. 选择 **Original Packet**（原始数据包），然后单击 **Source Zone**（源区域）下的 **Add**（添加）。

© 2019 Palo Alto Networks, Inc.

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。

© 2019 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。该插件监视 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 群集。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 群集的动态地址组中，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>** — 此标记将IP地址分组到基于 EPG 的动态地址组中，并显示集群、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>** — 此标记将 IP 地址分组到基于微 EPG 的动态地址组中，并显示集群、租户、应用程序配置文件和微 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>** — 此标记将 IP 地址分组到基于子网的动态地址组中，并显示集群、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。

- 监视时间间隔 — 监视时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，则监视间隔将重置。如果检测到更改，则插件会在重置监视时间间隔之前处理更改。默认监控时间间隔为 60 秒。您可以将监视间隔设置为 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。即使监视间隔遗漏了更改事件，这也可确保插件与结构同步。默认完全同步时间间隔为 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。

如果将监视时间间隔的值配置为大于完全同步时间间隔的值，则会忽略完全同步时间间隔，并在每个监视时间间隔执行完全同步。

© 2019 Palo Alto Networks, Inc.

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 停止监视群集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 仪表板的 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 对等设备上重复此安装过程。在 HA 对中的 Panorama 上安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，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。

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“操作”列中单击 **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，必须设置监视时间间隔，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。默认时间间隔为 600 秒（10 分钟）。范围为 600 - 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。

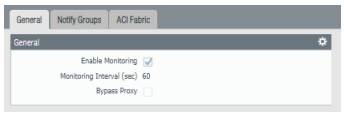
STEP 3 | 必须在 Panorama 上添加防火墙作为受管设备，并创建设备组，这样，您可以配置 Panorama 以将检索到的 VM 信息通知这些组。设备组可以包括 VM 系列防火墙或是硬件防火墙上的虚拟系统。

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）。这样可以监视部署中的所有群集。
3. 以秒为单位设置 **Monitoring Interval**（监控间隔）。监视间隔是 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）。

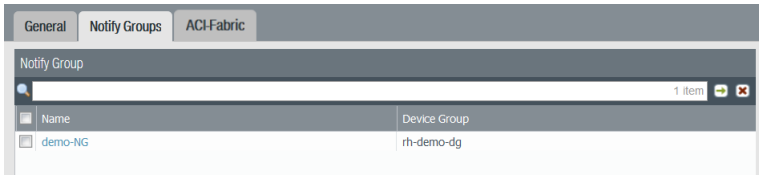
© 2019 Palo Alto Networks, Inc.

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。

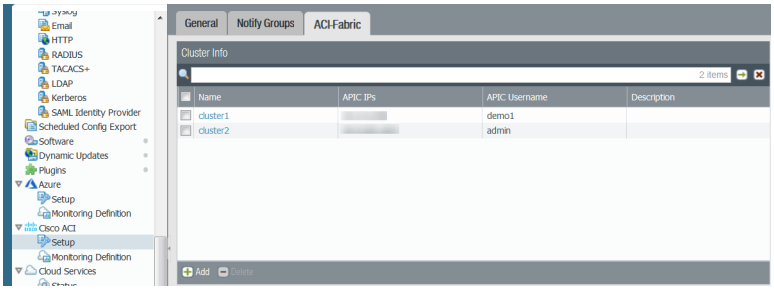


STEP 6 | 添加 ACI 结构信息。

1. 选择 **Panorama** > **Cisco ACI** > **Setup**（设置） > **ACI Fabric**（**ACI** 结构）。
2. 输入群集的描述性 **Name**（名称）。
3. 以逗号分隔列表的形式输入群集中每个 APIC 的 IP 地址或 FQDN。

使用 *FQDN* 时，请勿在 *URL* 中包含 *https://*。

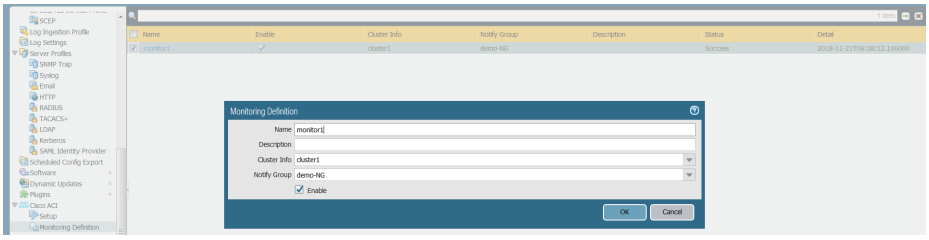
4. 输入 APIC 用户名。
5. 输入并确认 APIC 密码。
6. 单击 **OK**（确定）。



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 群集的描述性 **Name**（名称），也可选择输入说明。
3. 选择 **Cluster Info**（群集信息）和 **Notify Group**（通知组）。
4. 单击 **OK**（确定）。

© 2019 Palo Alto Networks, Inc.

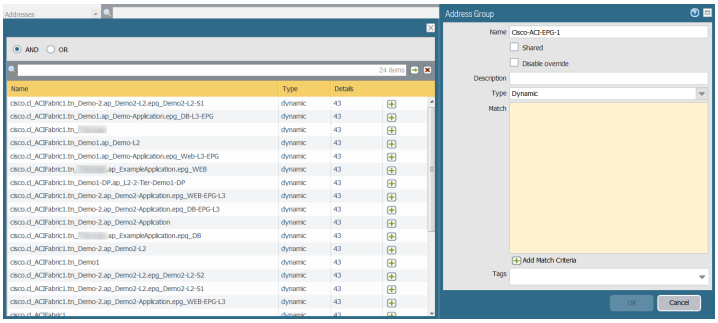


STEP 8 | **Commit**（提交）更改。

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，您应等待配置的监视间隔的持续时间。



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。

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）。

© 2019 Palo Alto Networks, Inc.

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

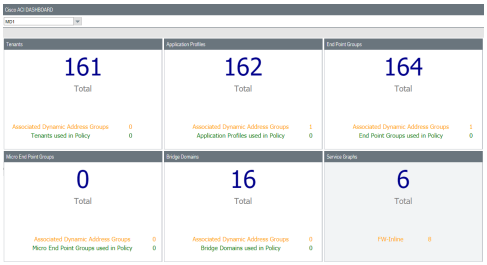
```
Unable to process subscriptions after HA switch-over; user-intervention required.
```

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 仪表板的 Panorama 插件

适用于 Cisco ACI 仪表板的 Panorama 插件概述了插件监控的 ACI 基础架构。仪表板包含两个页面：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**（仪表板）访问仪表板。



仪表板仅查询和统计在 *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。

仪表板磁贴	说明
Tenant Tags（租户标记） 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*	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。 • **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。

© 2019 Palo Alto Networks, Inc.

仪表板磁贴	说明
上的租户数可能与 *APIC* 上的总数不符。	
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。 • **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。

© 2019 Palo Alto Networks, Inc.

仪表板磁贴	说明
	• **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。 • **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。

© 2019 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。
- 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。

© 2019 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。

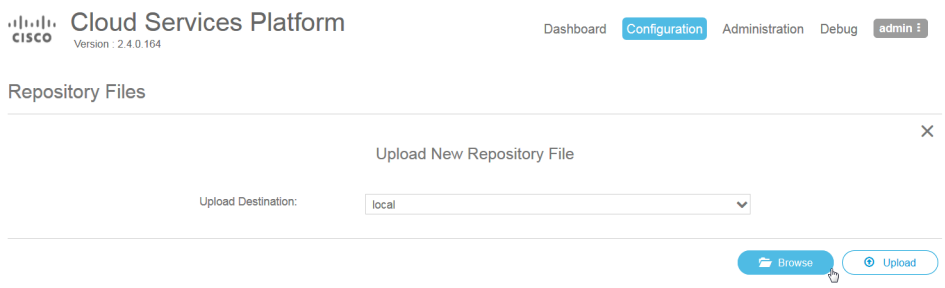
STEP 2 | 为 VM 系列防火墙创建引导 ISO 文件。

1. 创建一个适用于您的 VM 系列防火墙的引导数据包。
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）。

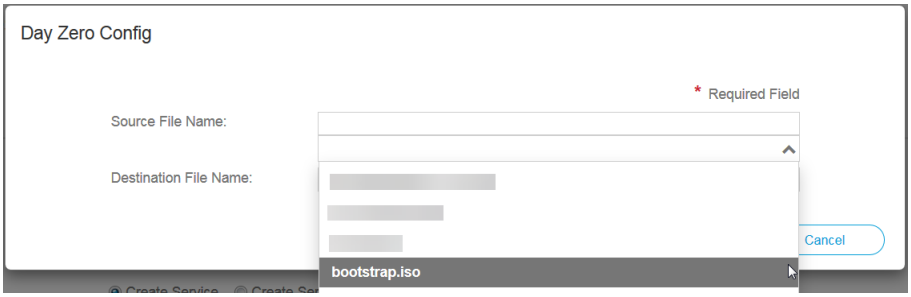


STEP 5 | 创建 VM 系列防火墙服务。

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）。

© 2019 Palo Alto Networks, Inc.



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。

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

适用于 Cisco TrustSec 的 Panorama 插件

通过适用于 Cisco TrustSec 的 Panorama 插件，您可以使用动态地址组为 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 的 Panorama 插件使用两个时间间隔从 pxGrid 服务器检索信息 — 监控间隔和完全同步间隔。

- 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。默认监控时间间隔为 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。默认完全同步时间间隔为 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）。您必须在 Panorama CLI 上配置完全同步间隔。

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。

© 2019 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。

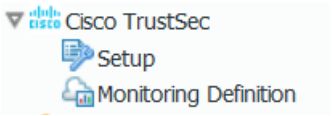
如果拥有 Panorama HA 配置，则在每个 Panorama 对等设备上重复此安装过程。在 HA 对中的 Panorama 设备上安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，将转换为非运行状态。在主动对等上安装插件会将被动对等返回到功能状态。

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“操作”列中单击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。



© 2019 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。

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 - 86,400 秒（1 天）。

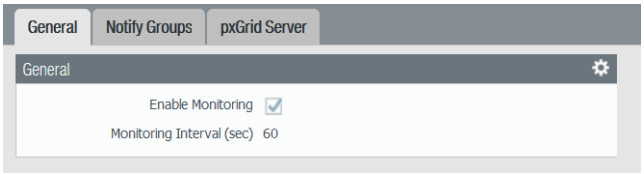
   ```
   admin@Panorama# set plugins cisco_trustsec full-sync-interval <interval-in-seconds>
   ```

STEP 2 | 登录到 Panorama Web 界面。

STEP 3 | 必须在 Panorama 上添加防火墙作为受管设备，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。

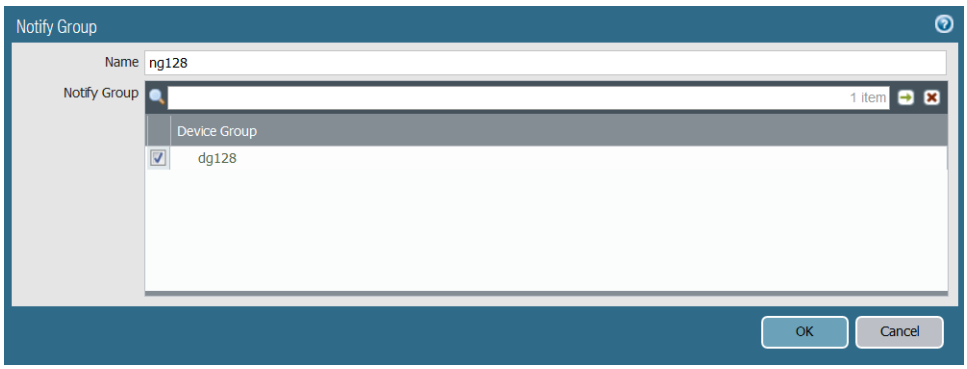
STEP 4 | 启用监控并设置监控间隔。

1. 选择 **Panorama** > **Cisco TrustSec** > **Setup**（设置）> **General**（常规）。
2. 选择 **Enable Monitoring**（启用监控）。这样可以监视部署中的所有群集。
3. 以秒为单位设置 **Monitoring Interval**（监控间隔）。监控间隔是 Panorama 从 pxGrid 服务器检索更新的网络信息的频率。默认值为 60 秒。



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。



© 2019 Palo Alto Networks, Inc.

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。

   admin@Panorama> request plugins cisco_trustsec create-account client-name <client-name> host <ise-server-ip>

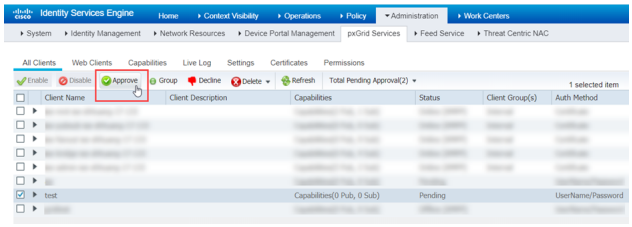
```
admin@Panorama> request plugins cisco_trustsec create-account client-name
 test host 10.10.10.15

AccountCreate in progress...
AccountCreate successful.
  client nodename: test
 client password: PmVKBmPgf63Hypq

AccountActivate in progress...
AccountActivate successful.

Please approve the account on the server.
```

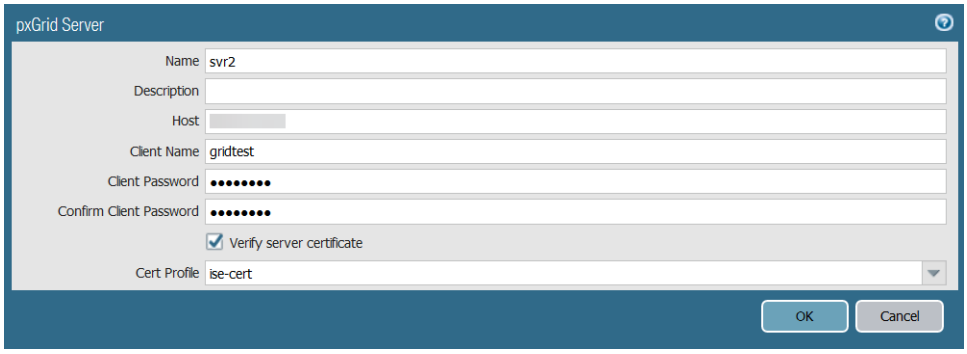
3. 登录到 Cisco ISE 服务器以核准帐户。
4. 选择 **Administration**（管理）> **pxGrid Services**（**pxGrid** 服务）> **All Clients**（所有客户端）。
5. 选择在 Panorama 上创建的客户端名称。
6. 单击 **Approve**（核准）。



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。

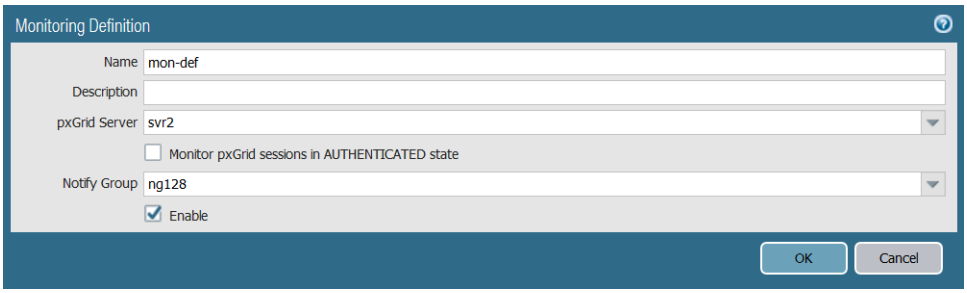
1. 选择 **Panorama** > **Cisco TrustSec** > **Setup**（设置）> **pxGrid Server**（**pxGrid** 服务器）。
2. 输入 pxGrid 服务器的描述性 **Name**（名称）。
3. 在 **Host**（主机）字段中，输入 pxGrid 服务器的 IP 地址或 FQDN。
4. 输入在上一步中创建的客户端名称。
5. 输入并确认在上一步中生成的客户端密码。
6. 验证 pxGrid 服务器身份。
   1. 选择 **Verify server certificate**（验证服务器证书）。
   2. 从 **Cert 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）。

© 2019 Palo Alto Networks, Inc.



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** 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“已开始”状态的会话中检索 IP 地址。在 pxGrid 环境中，处于“身份验证”状态的会话是刚经过身份验证的会话。但是，如果 ISE 收到连接开始数据包，则会话将更改为“已开始”状态。
5. 选择 **Notify Group**（通知组）。
6. 单击 **OK**（确定）。



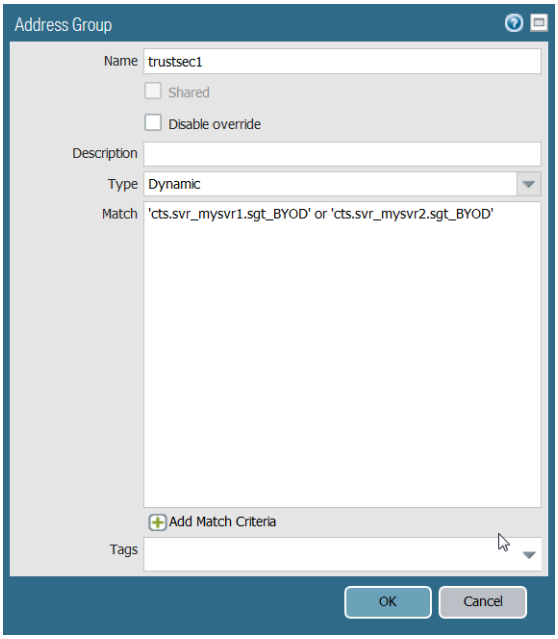
STEP 10 | **Commit**（提交）更改。

STEP 11 | 创建动态地址组，并确认地址已添加到动态地址组中。

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. 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。
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。

© 2019 Palo Alto Networks, Inc.

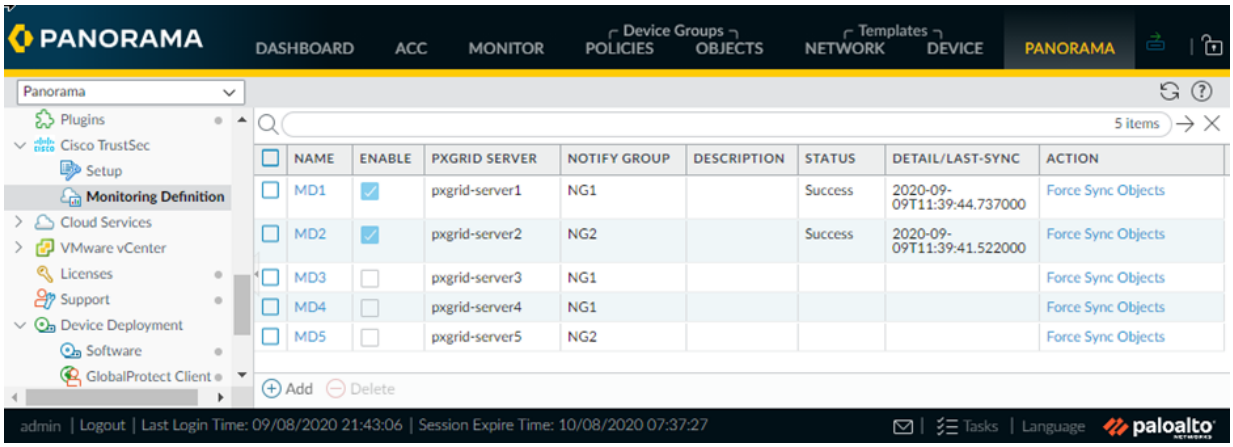


STEP 12 | 在策略中使用动态地址组。

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 13 | （可选）您可以通过同步动态对象随时更新 pxGrid 服务器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 TrustSec** > **Monitoring Definition**（监控定义）。
2. 单击 **Synchronize Dynamic Objects**（同步动态对象）。



© 2019 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

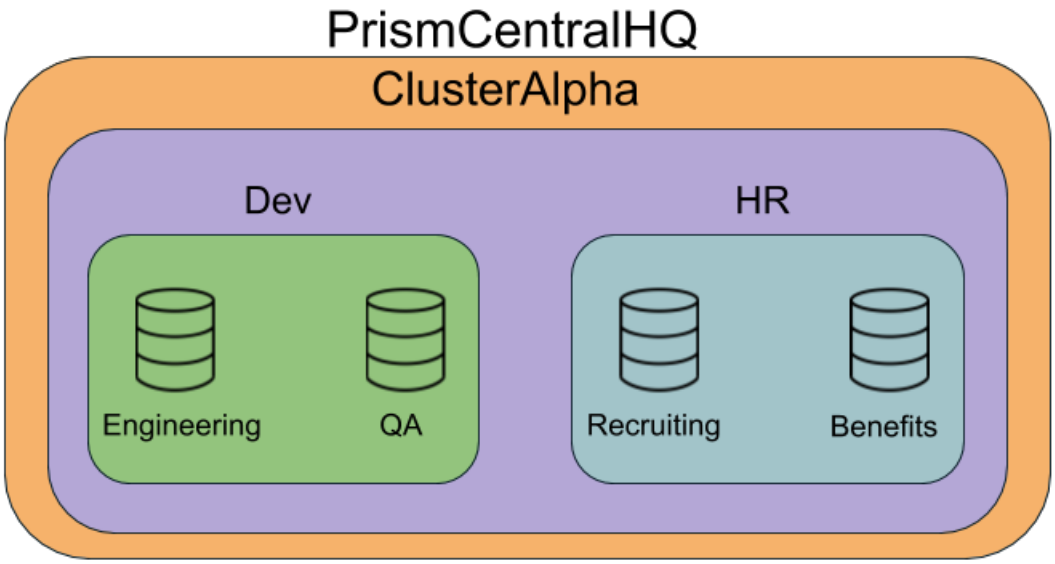
Nutanix 上的 VM 监控

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
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。

© 2019 Palo Alto Networks, Inc.

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 对等设备上重复此安装过程。在 HA 对中的 Panorama 上安装插件时，请在主动对等设备之前将该插件安装在被动对等设备上。在被动对等设备上安装插件后，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。

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“操作”列中单击 **Install**（安装）以安装插件。安装完成后，Panorama 会提醒您。

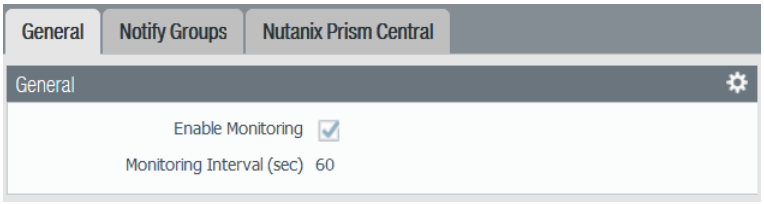
配置适用于 Nutanix 的 Panorama 插件

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。

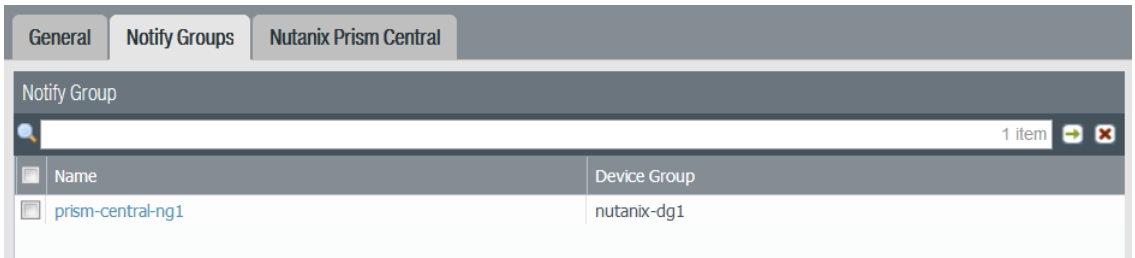
STEP 2 | 启用监控并设置监控间隔。

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。



STEP 4 | 添加 Prism Central 信息。

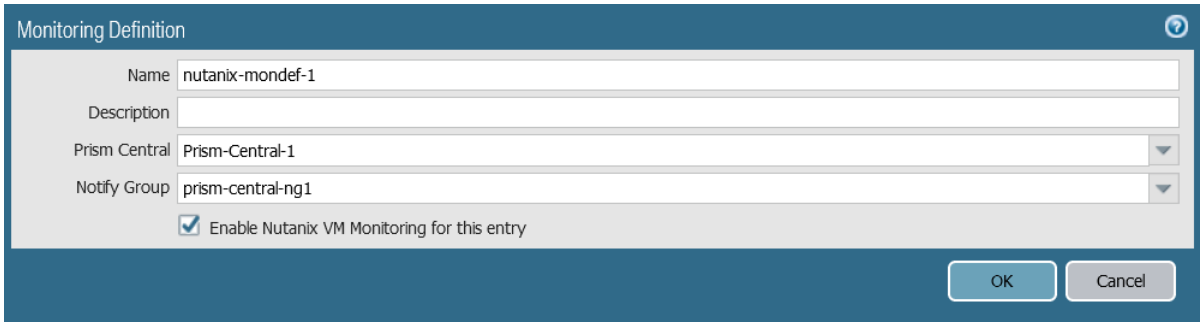
© 2019 Palo Alto Networks, Inc.

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）。

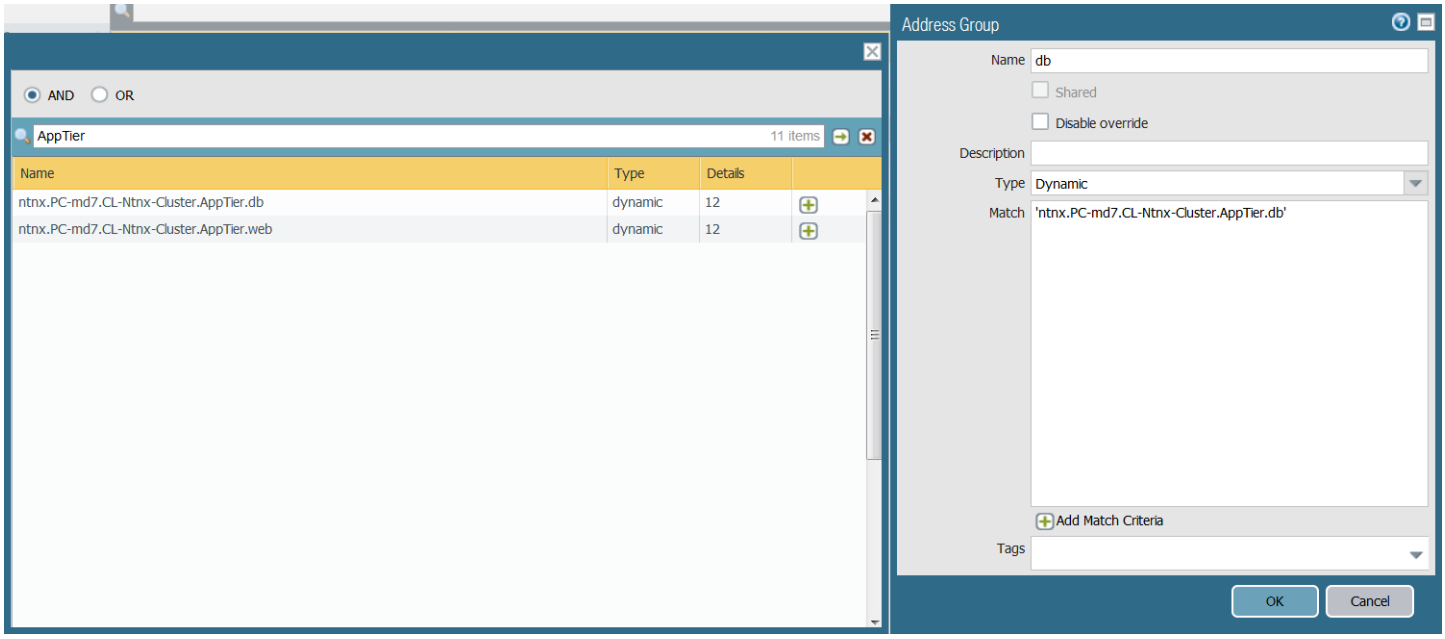


STEP 6 | **Commit**（提交）更改。

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。

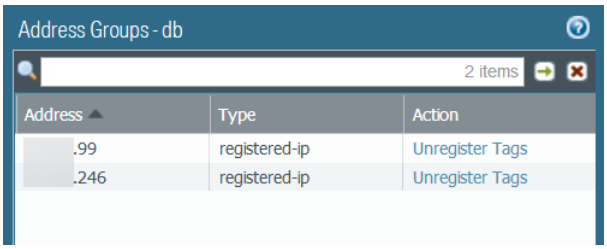
© 2019 Palo Alto Networks, Inc.



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。



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）。

© 2019 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。您可以将 VM 系列防火墙引导出外部设备（例如虚拟磁盘、虚拟 CD-ROM、或 AWS S3 或 Google Cloud 等存储桶），以完成 VM 系列防火墙的配置和许可流程。您可以采用基本初始配置和许可证来引导防火墙，以便在 Panorama 中注册防火墙，然后从 Panorama 中检索其完整配置，也可以引导完整的配置，以便在启动时对防火墙进行完全配置。

> 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

VM 系列防火墙引导工作流程

熟悉并通过引导包和评估确定是对防火墙进行完全配置还是使用 Panorama 来管理引导的防火墙之后，使用以下工作流程来引导您的 VM 系列防火墙。

- 处于安全角度的考虑，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。如果要引导之前已配置的 VM 系列防火墙，需将防火墙重置为出厂默认设置。
- 如果您想要使用 Panorama 管理引导的 VM 系列防火墙，则在 Panorama 上生成 VM 授权密钥。在您准备引导数据包时，您必须将该键包含在基本配置 (init-cfg.txt) 文件中。
- 准备引导许可证。
- 如果未使用 Panorama 管理防火墙配置，则创建 init-cfg.txt 文件并且 创建 bootstrap.xml 文件（可选）。
- 准备引导包。
- 将引导数据包设置为您的管理程序所需的格式，然后引导 VM 系列防火墙。
  - 在 ESXi 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
  - 在 AWS 上引导 VM 系列防火墙
  - 在 Azure 上引导 VM 系列防火墙
  - 在 Google Cloud Platform 上引导 VM 系列防火墙
- 验证引导完成。

© 2019 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。在将虚拟磁盘、虚拟 CD-ROM 或存储桶连接到防火墙时，防火墙会扫描是否存在引导包；如果存在，防火墙将会使用该引导包中定义的设置。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。之后，防火墙将会被添加为 Palo Alto Networks 支持门户中的资产。如果防火墙未连接到 Internet，您可以使用引导数据包中的许可证密钥，也可以连接至 Panorama，Panorama 将会检索适当的许可证并将其部署到受管防火墙中。

您创建的引导数据包必须包含 **/config**, **/license**、**/software** 和 **/content** 文件夹，即使为空文件夹：

- **/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* 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 ，您必须手动从 Palo Alto Networks 支持门户获得许可证密钥，或使用许可证 API 获得密钥，然后在该文件夹中保存每个密钥。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。其中必须包含开放式虚拟化格式 (OVF) 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。
- **/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 版本所需的最少内容版本，否则，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。

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您的管理程序。使用下表可以确定您的管理程序/云供应商支持的文件类型。

引导用外部设备（引导数据包格式）	ESXi	KVM	Hyper-V	AWS	Azure	Google
CD-ROM（ISO 映像）	是	是	是	—	—	—
存储桶	—	—	—	是	是	是
config-drive	—	—	—	—	—	—
块存储设备	是	是	是	—	—	—

© 2019 Palo Alto Networks, Inc.

引导配置文件

引导数据包必须包括 /config 文件夹中 init-cfg.txt 文件内所包含的基本配置；完整配置（包含在 /config 文件夹中的 bootstrap.xml 文件中）为可选配置。将两个文件同时包含在引导包中之后，防火墙将会合并这些文件的配置；如果两个文件中的配置设置有重叠，防火墙将会使用 init-cfg.txt 文件中定义的设置。

- 基本配置 — init-cfg.txt 文件是一个文本文件，其中包含了基本的初始配置信息。一般来说，您可以将该文件命名为 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）。该文件必须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。防火墙启动时，它会搜索与其 UUID 或序列号相匹配的文本文件；若未找到该文件，将会使用通用文件名进行搜索。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：

  - 必须在 Panorama 上生成 VM 身份验证密钥，并包含 init-cfg.txt 文件的密钥。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，因此防火墙日志将被丢弃。
- 完整配置 — bootstrap.xml 文件允许您对防火墙进行完整配置。Bootstrap.xml 文件是可选文件。如果未使用 Panorama 集中管理您的防火墙，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。您可以手动定义该文件，或从现有的防火墙中导出运行的配置并将其保存为 **bootstrap.xml** 文件。

  如果您使用了 bootstrap.xml 文件，则需确保从同一平台或管理程序的防火墙中导出 XML 文件。如果您提供了 init-cfg.txt 文件和 bootstrap.xml 文件，防火墙会在引导过程中将这两个文件合并为一个运行配置；如果出现任何设置重叠，防火墙将会使用基本配置文件中的设置。请参阅创建 bootstrap.xml 文件。

© 2019 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，并且引导包的 /license 文件夹中必须包含许可证身份验证代码。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，并将防火墙添加为受管设备。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：

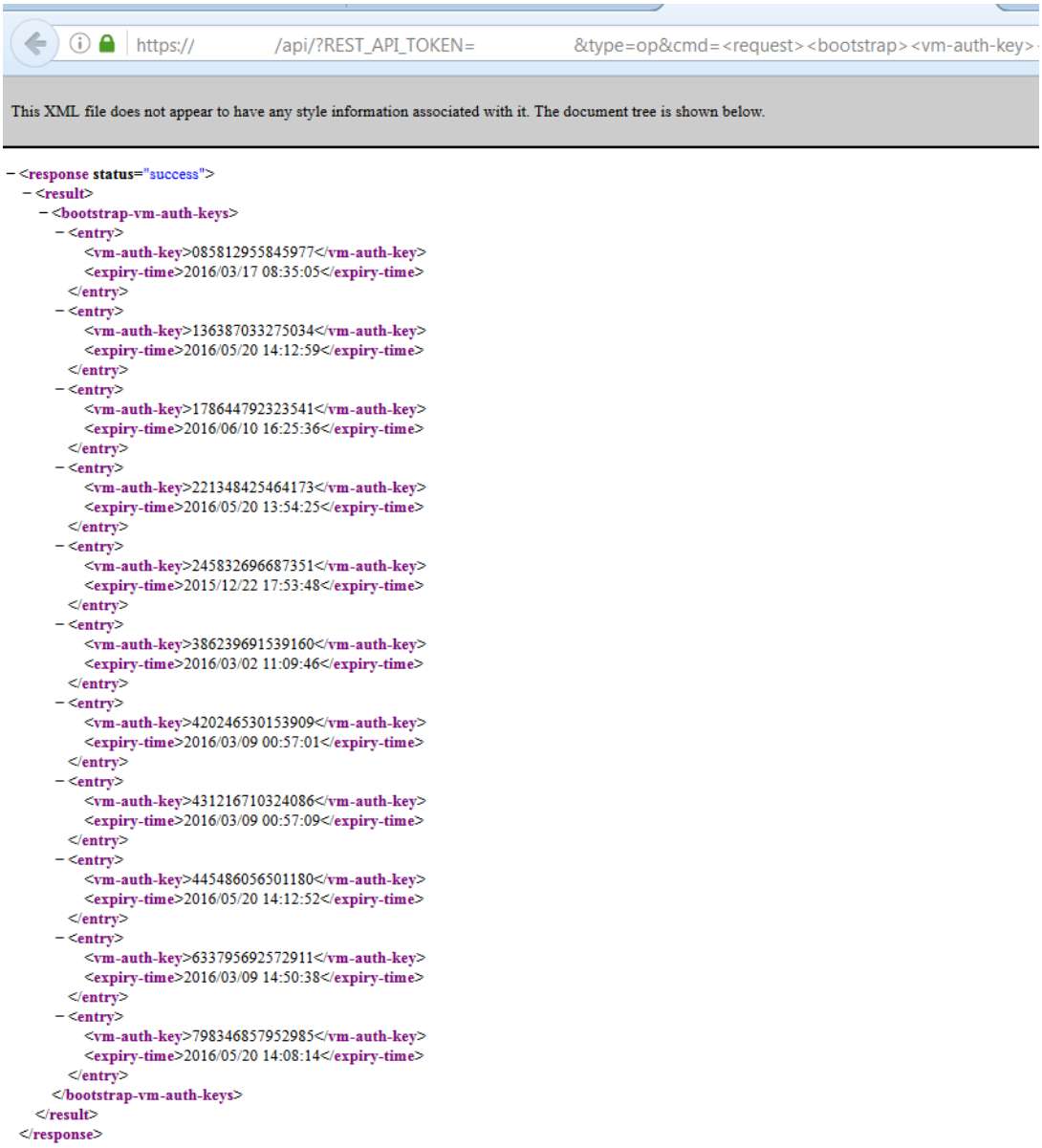
  https://*<Panorama_IP_address>*/api/?type=op&cmd=<request><bootstrap><vm-auth-key><generate><lifetime><number-of-hours></lifetime></generate></vm-auth-key></bootstrap></request>

  其中 lifetime 是指 VM 身份验证密钥保持有效的小时数。

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>
```


© 2019 Palo Alto Networks, Inc.



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

© 2019 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。它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。

STEP 5 | （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。
- 启用巨帧和/或多个虚拟系统
- 启用 AWS 上 VM 系列防火墙的管理接口 (mgmt) 和数据面板接口 (ethernet 1/1) 的交换。有关更改管理界面的更多信息，请参阅管理接口映射以用于 Amazon ELB。
- 启用或禁用 DPDK。

© 2019 Palo Alto Networks, Inc.

init-cfg.txt 文件组件

下表介绍了 init-cfg.txt 文件中的字段。其中，type（类型）、ip-address（IP 地址）、default-gateway（默认网关）和 netmask（网络掩码）为必填字段。

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。
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。
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=	虚拟机身份验证密钥。（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。

© 2019 Palo Alto Networks, Inc.

字段	说明
	• jumbo frame — 启用第 3 层所有接口的默认 MTU 大小，设置为 9192 字节。 • mgmt-interface-swap —（仅适于 AWS 和 Google 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或 用于 Google Cloud Launcher 负载均衡的管理接口交换。
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。
op-cmd-dpdk-pkt-io=	打开或关闭该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。

init-cfg.txt 示例文件

基本配置 (init-cfg.txt) 文件的以下示例显示了文件中支持的所有参数；粗体所示为必填参数。

示例 init-cfg.txt 文件（静态 IP 地址）	示例 init-cfg.txt 文件（DHCP 客户端）
type=static	**type=dhcp-client**
ip-address=10.5.107.19	ip-address=
default-gateway=10.5.107.1	default-gateway=
netmask=255.255.255.0	netmask=
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=755036225328715	vm-auth-key=755036225328715
panorama-server=10.5.107.20	panorama-server=10.5.107.20
panorama-server-2=10.5.107.21	panorama-server-2=10.5.107.21
tplname=FINANCE_TG4	tplname=FINANCE_TG4
dgname=finance_dg	dgname=finance_dg

© 2019 Palo Alto Networks, Inc.

示例 init-cfg.txt 文件（静态 IP 地址）	示例 init-cfg.txt 文件（DHCP 客户端）
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=***
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

对于 *AWS* 中的 *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；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 *Google Cloud* 中的 *VM* 系列防火墙。

****op-cmd-dpdk-pkt-io=off* 用于在 *ESXi*、*KVM* 和 *Google Cloud* 上的 *VM* 系列防火墙上禁用 *DPDK*（默认情况下已启用 *DPDK*）。

© 2019 Palo Alto Networks, Inc.

创建 bootstrap.xml 文件

使用下述说明创建可选的 bootstrap.xml 文件。

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，请在“Configuration Management（配置管理）”部分，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**）。
   - 若要导出之前版本的防火墙配置，在“Configuration Management（配置管理）”部分，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 | 将配置文件重命名为 bootstrap.xml。

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。

© 2019 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。

  在准备引导包 ，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. 转到 support.paloaltonetworks.com 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. 按照注册 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. 转到 support.paloaltonetworks.com，登录并选择 **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. 继续准备引导包；您必须将下载至 `\license` 文件夹的许可密钥添加到引导包中。

- 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管理程序获取 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。请参阅授权 API 许可证。

© 2019 Palo Alto Networks, Inc.

准备引导包

使用下列过程准备引导包。

STEP 1 | 创建引导包的顶级目录结构。

在本地客户端或便携式电脑上，创建以下文件夹：

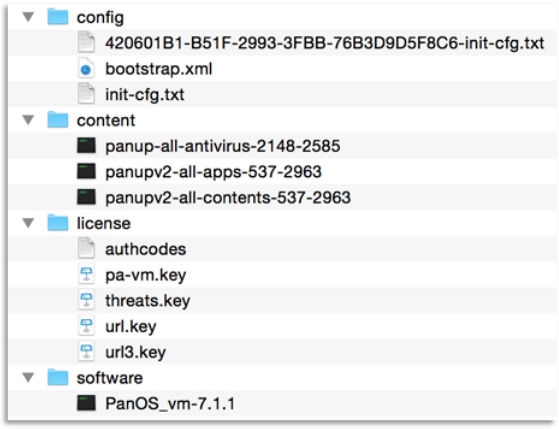
- **/config**
- **/license**
- **/software**
- **/content**
- **/plugins**

您可以将文件夹留空，但必须创建 ***/config***, ***/license***、***/software*** 和 ***/content*** 文件夹。***/plugins*** 文件夹是可选的，只在升级独立于版本的 VM 系列插件时才需要。

请勿在此目录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。

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

© 2019 Palo Alto Networks, Inc.

```
/content
  panupv2-all-contents-488-2590
  panup-all-antivirus-1494-1969
  panup-all-wildfire-54746-61460
/software
  PanOS_vm-7.1.1
  PanOS_vm-7.1.4
/license
  authcodes
  0001A100110-url3.key
  0001A100110-threats.key
  0001A100110-url3-wildfire.key
/plugins
  vm_series-1.0.1
```

- 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。对于身份验证代码，请创建一个名为 *authcodes* 的文本文件（没有文件扩展名），将身份验证代码添加到该文件，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 | 创建引导包。

对于 VM 系列防火墙，为您的管理程序创建格式适当的映像。

© 2019 Palo Alto Networks, Inc.

在 AWS 上引导 VM 系列防火墙

若要执行引导，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。

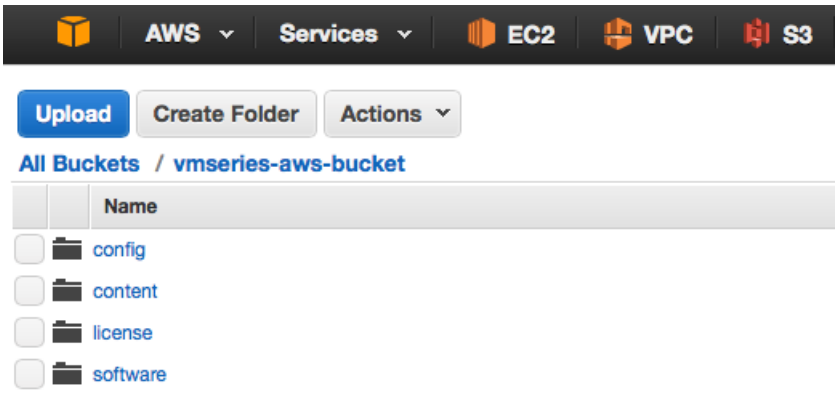
STEP 1 | 在 AWS 控制台上，在引导级创建一个 Amazon 简单存储服务 (S3) 桶。本例中的 S3 存储桶 vmseries-aws-bucket 位于所有存储桶根文件夹级别。因为您无法指定引导文件位置的路径，因此如果您嵌套文件夹，引导将会失败。

STEP 2 | 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。

```
{
  "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>/*"]
    }
  ]
}
```

STEP 3 | 在 S3 存储桶中创建文件夹。

- 创建引导包的顶级目录结构。直接在 S3 存储桶中创建结构。



- 在每个文件夹中添加内容。您可以将文件夹留空，但必须创建所有的四个文件夹。

© 2019 Palo Alto Networks, Inc.

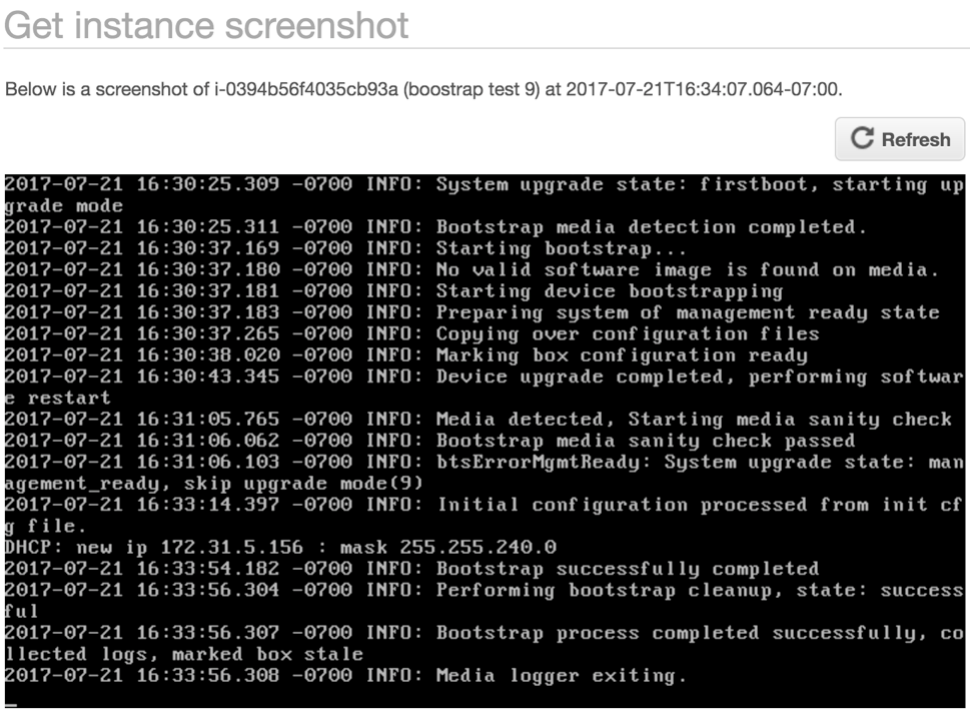
如果在 *Amazon S3* 中启用了记录功能，将会自动在 *S3* 桶中创建名为 *Logs* 的文件夹。*Logs* 文件夹可帮助您解决 *S3* 桶访问相关的问题。

STEP 4 | 在 AWS 上启动 VM 系列防火墙。当您以 EC2 实例启动防火墙时，请附加在步骤 2中创建的 IAM 角色，并在用户数据字段（“高级”部分）中指定以下 S3 键值：

```
vmseries-bootstrap-aws-s3bucket=<bucketname>
```

STEP 5 | 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）。

- 在成功引导后，您将看到以下消息。



- 如果 S3 存储桶没有正确的权限，或者 S3 存储桶中没有全部四个文件夹，则会显示以下错误消息。

© 2019 Palo Alto Networks, Inc.

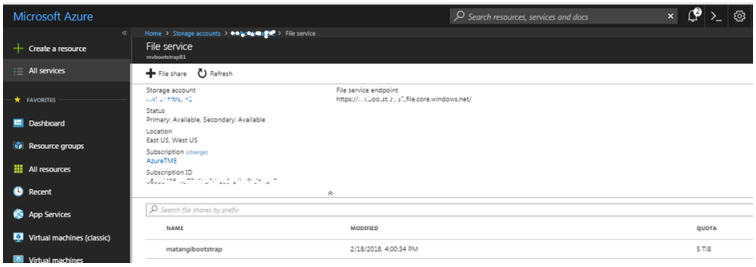
在 Azure 上引导 VM 系列防火墙

Azure 上的 VM 系列防火墙支持用于引导的*Azure* 文件服务。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。

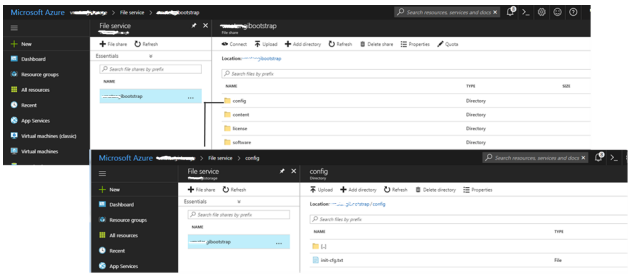
VM 系列防火墙的管理界面必须能够访问包含引导数据包的文件共享，以完成引导。

STEP 1 | 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。



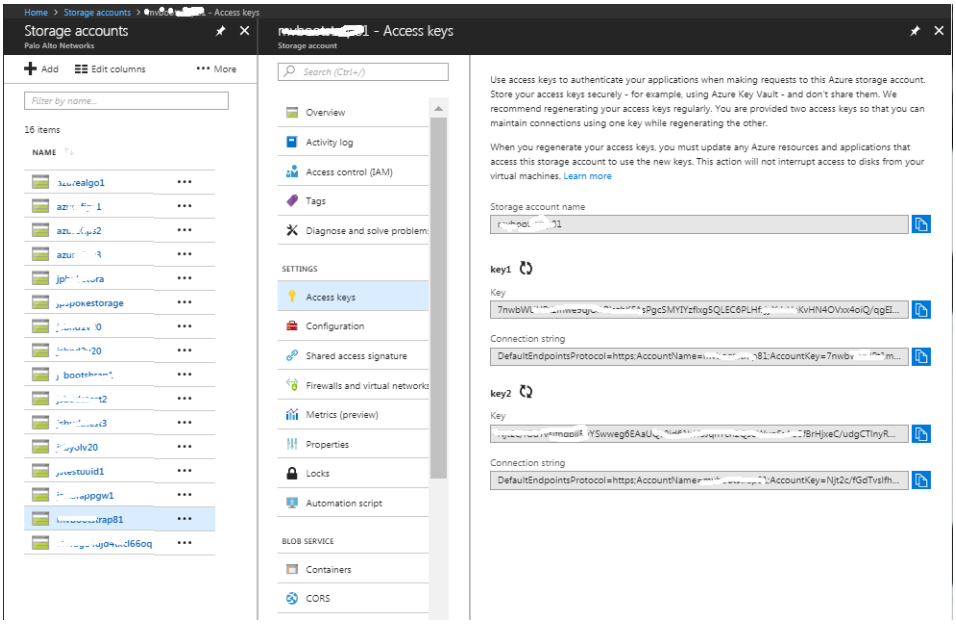
3. 在存储帐户中创建文件夹。
   - 直接在根文件夹中创建引导数据包的顶级目录结构。
   - 在每个文件夹中添加内容。您可以将文件夹留空，但必须将所有四个文件夹放在目录内。在下面的屏幕截图中，您会看到，`config` 文件夹用于已上传的 `init-cfg.txt`文件。



STEP 2 | 从 Azure Marketplace 部署 VM 系列防火墙（解决方案模板）。启动防火墙时，请选择**Enable Bootstrap:Yes**（启动引用：是），并提供所需信息，以访问包含引导文件的文件共享。

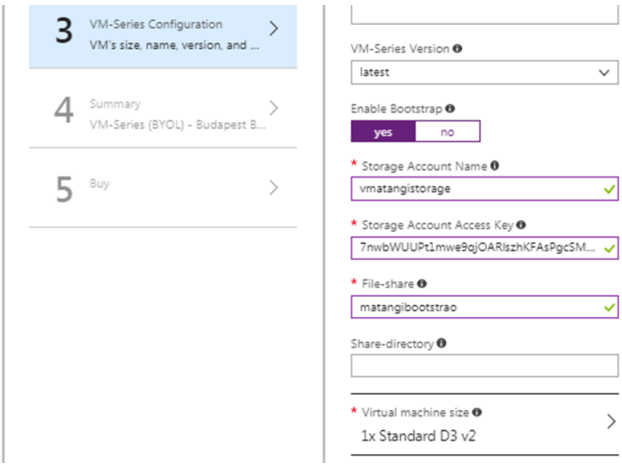
1. **Storage Account Name**（存储帐户名称）— 这是一个您可以在其中创建引导文件夹的文件共享 Azure 存储帐户。
2. **Storage Account Access Key**（存储帐户访问密钥）—防火墙需要此访问密钥以对存储帐户进行身份验证，并访问其中的文件。要复制此访问密钥，请选择存储帐户名称，然后选择 **Setttings**（设置）> **Access Keys**（访问密钥）。

© 2019 Palo Alto Networks, Inc.



3. 文件共享—这是您已上传且用于引导防火墙所需文件的文件共享名称。

   您可以指定 *Share-directory*（共享目录）（可选）。如果有一个充当不同设置的引导配置的存储库公共文件共享，您可以使用 共享目录来创建文件夹层级结构，并访问公共文件访问内的特定子文件夹集。



STEP 3 | 验证引导完成。

© 2019 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。

STEP 1 | 创建引导数据包和虚拟硬盘。

1. 创建引导包。
2. 部署 Linux 虚拟机。
3. 在 Linux 机器上，准备引导包。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。

© 2019 Palo Alto Networks, Inc.

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。

© 2019 Palo Alto Networks, Inc.

在 Google Cloud Platform 上引导 VM 系列防火墙

要进行引导，您必须在 Google 存储桶内创建特定的文件结构。可在指定实例的元数据时提供引导桶的名称，如从 Google Cloud Platform Marketplace 部署 VM 系列防火墙所述。

开始此任务之前，请参阅 引导数据包、准备引导许可证、以及 准备引导数据包等主题。

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。

STEP 1 | 根据 准备引导数据包创建用于引导数据包的文件。

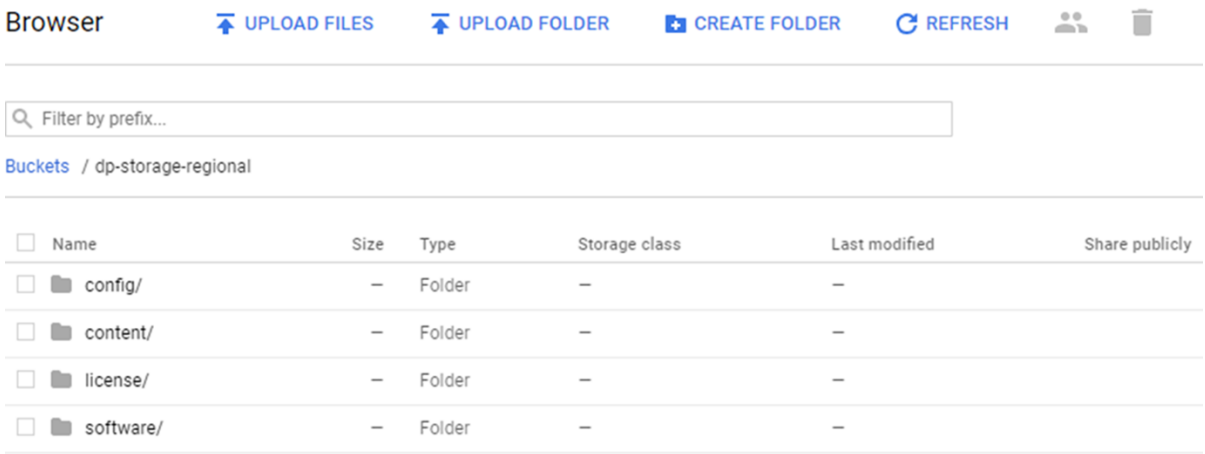
STEP 2 | 登录到 Google Cloud 控制台。

STEP 3 | 创建用于引导数据的存储桶。选择**Storage**（存储）> **Browser**（浏览），并单击 **Create Bucket**（创建存储桶）。

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）。

STEP 4 | 创建引导文件夹。

1. 在存储浏览中，单击存储桶名称以打开它。
2. 单击 **Create Folder**（创建文件夹），并命名文件夹为 `config`。单击 **Create**（创建）。
3. 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。



4. （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）。
5. 打开 `license` 文件夹，然后上传 **`authcodes`**文件。
6. 继续，直到所有引导文件均上传完毕。

在您从 Google Cloud Platform Marketplace 部署 VM 系列防火墙时，可以使用此桶引导防火墙。

© 2019 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）。
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。

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）并单击 **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。

© 2019 Palo Alto Networks, Inc.

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。

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）并单击 **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。

© 2019 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**（选择受管或其他已有存储）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。

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。

© 2019 Palo Alto Networks, Inc.

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。

© 2019 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 | 如果您的 init-cfg.txt 文件中包含有 panorama-server、tplname 和 dgname，则检查 Panorama 受管设备、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 **`show config 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。

© 2019 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）	• 引导包未检测到外部设备。 或 • 在通过映像在外部设备上启动时出现了关键错误。引导流程将中止。
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联网信息所需参数错误或缺失（高）	引导所需的联网参数不正确或缺失。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）。
文件 ltlicense-key-filenamegt 的许可证密钥安装失败（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 ltauthcodegt 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>：已成功使用数据包 ltbundlename> 准备了 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及如何准备引导包的详细信息。

© 2019 Palo Alto Networks, Inc.