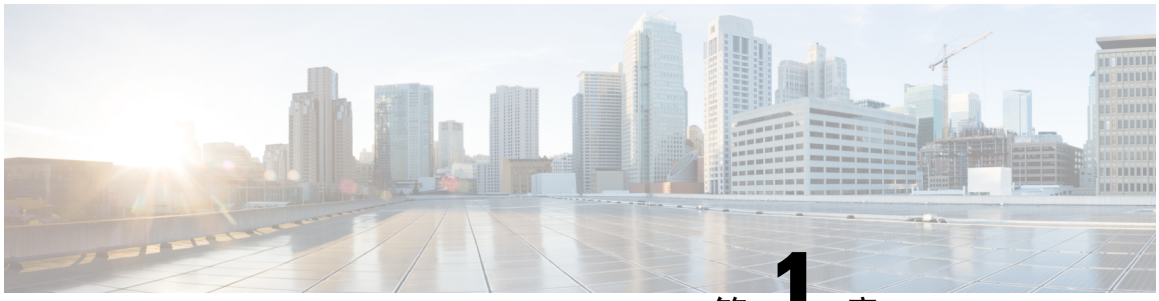
思科 Cisco Secure Firewall Threat Defense Virtual 入门指南，版本 7.6

上次修改日期: 2025 年 3 月 26 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

思科 Cisco Secure Firewall Threat Defense Virtual 简介

思科 Cisco Secure Firewall Threat Defense Virtual（threat defense virtual）将 Cisco 的新一代防火墙功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

如今，组织依靠混合使用物理和虚拟控制点来满足其网络安全需求。他们需要灵活地在各种环境中部署不同的物理和虚拟防火墙，同时仍要在分支机构、企业数据中心以及它们之间的所有点都保持一致的策略。从数据中心整合到办公室搬迁、兼并和收购，以及应用需求的季节性高峰，思科的虚拟防火墙产品组合都能帮助您简化安全管理，提供统一策略的便利性和随处部署的灵活性。

思科 Cisco Secure Firewall Threat Defense Virtual 将思科成熟的网络防火墙与 Snort IPS、URL 过滤和恶意软件防御相结合。它在物理、私有和公共云环境中采用一致的安全策略，从而简化了威胁防护。深入了解您的网络，快速检测威胁来源和活动。然后，在攻击影响您的运营之前阻止它们。

Cisco Secure Firewall Threat Defense Virtual 是常用的虚拟化解决方案。通过自动风险排名和影响标志来确定威胁的优先级，从而将资源集中用于需要立即采取行动的事件。许可证的可移植性为从企业内部私有云迁移到公共云提供了灵活性，同时还能在所有设备上保持一致的策略和统一的管理。通过思科智能软件许可，可轻松部署、管理和跟踪虚拟防火墙实例。

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

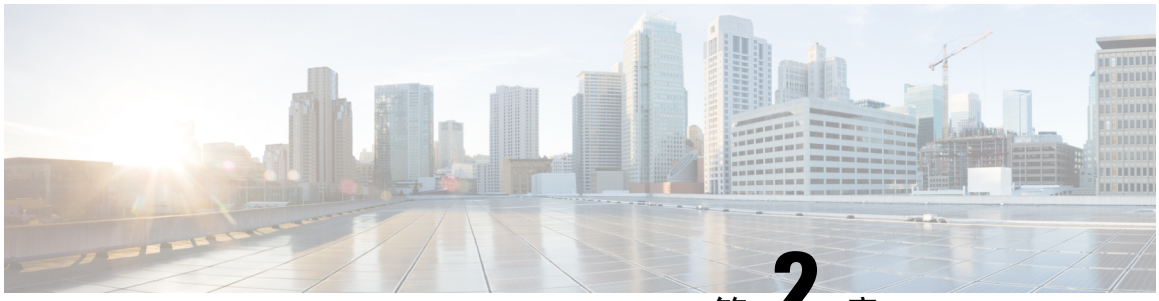
注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。



第 2 章

在 VMware 上部署 Threat Defense Virtual

本章介绍将 threat defense virtual 部署到 VMware vSphere 环境（vSphere vCenter 或独立式 ESXi 主机）的步骤。

概述

思科为 VMware vSphere vCenter 和 ESXi 托管环境打包了 64 位 threat defense virtual 设备。threat defense virtual 以开放虚拟化格式 (OVF) 包分发，可从 Cisco.com 下载。OVF 是用于为虚拟机 (VM) 打包和分发软件应用程序的开放源标准。一个 OVF 包在一个目录中包含多个文件。

您可以将 threat defense virtual 部署到能够运行 VMware ESXi 的任何 x86 设备上。要部署 threat defense virtual，您应该熟悉 VMware 和 vSphere，包括 vSphere 联网、ESXi 主机设置和配置，以及虚拟机访客部署。

Threat Defense Virtual的 VMware 功能支持

下表列出了 threat defense virtual的 VMware 功能支持。

表 *1: Threat Defense Virtual*的 *VMware* 功能支持

功能	说明	支持（是/否）	备注
冷克隆	VM 在克隆过程中关闭。	否	–
vMotion	用于实时迁移 VM。	是	使用共享存储。请参阅准则和限制。
分布式资源调度程序 (DRS)	监控虚拟机工作负载并解决不均衡问题，识别要使用 vMotion 进行实时迁移的虚拟机。	否	不符合条件
热添加	VM 在添加过程中运行。	否	–
热克隆	VM 在克隆过程中运行。	否	–
热删除	VM 在删除过程中运行。	否	–
快照	VM 会冻结几秒钟。	否	管理中心 与托管设备之间存在不同步情况的风险。
暂停和恢复	VM 暂停，然后恢复。	是	–
vCloud Director	允许自动部署 VM。	否	–
VMware FT	用于 VM 上的 HA。	否	使用故障转移功能进行 threat defense virtual VM 故障转移。
带 VM 心跳信号的 VMware HA	用于 VM 故障。	否	使用故障转移功能进行 threat defense virtual VM 故障转移。
VMware vSphere 独立 Windows 客户端	用于部署 VM。	是	–
VMware vSphere Web 客户端	用于部署 VM。	是	–

系统要求

有关 threat defense virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

根据所需部署的实例数量和使用要求，threat defense virtual部署所使用的具体硬件可能会有所不同。每个 threat defense virtual 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 和磁盘空间。

运行 VMware vCenter 服务器和 ESXi 实例的系统必须满足特定的硬件和操作系统要求。有关支持平台的列表，请参阅 VMware 在线兼容性指南。

表 *2: Threat Defense Virtual* 设备资源要求

设置	值
性能级别	threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。 • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) 请参阅《Cisco Secure Firewall Management Center 管理指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。
存储	取决于所选磁盘格式。 • 调配磁盘大小为 48.24 GB。

设置	值
vNIC	threat defense virtual 支持以下虚拟网络适配器： • **VMXNET3** - 在 VMware 上，如果创建虚拟设备，Threat Defense Virtual 现默认为 vmxnet3 接口。先前，默认值为 e1000。vmxnet3 驱动程序使用两个管理接口。前两个以太网适配器必须配置为管理接口：一个用于设备管理/注册，一个用于诊断。 • **IXGBE** - ixgbe 驱动程序使用两个管理接口。前两个 PCI 设备必须配置为管理接口：一个用于设备管理/注册，一个保留用于内部用途。驱动程序不支持 threat defense virtual 的故障转移 (HA) 部署。 • **E1000** - • **IXGBE-VF** - ixgbe-vf (10 Gbit/s) 驱动程序支持只能在支持 SR-IOV 的内核上激活的虚拟功能设备。SR-IOV 需要正确的平台和操作系统支持；有关详细信息，请参阅“对 SR-IOV 的支持”部分。

对虚拟化技术的支持

- 虚拟化技术(VT)是新型处理器的一套增强功能，可提高运行虚拟机的性能。您的系统应配备支持英特尔 VT 或 AMD-V 扩展的 CPU，才能实现硬件虚拟化。英特尔和 AMD 都提供在线处理器识别实用程序来帮助您识别 CPU 并确定它们的性能。
- 许多服务器虽含有支持的 VT 的 CPU，但默认状态下会禁用 VT，您必须手动启用 VT。请查阅制造商文档，了解如何在您的系统中启用 VT 支持。

注释 如果您的 CPU 支持 VT，但您在 BIOS 中没有看到此选项，请联系您的供应商，获取可让您启用 VT 支持的 BIOS 版本。

禁用超线程

我们建议您为运行 threat defense virtual 的系统禁用超线程；请参阅不推荐使用超线程，第 10 页。以下处理器支持超线程，每个核心有两个线程：

- 基于 Intel Xeon 5500 处理器微架构的处理器。
- Intel Pentium 4（支持 HT）
- Intel Pentium EE 840（启用 HT）

要禁用超线程，必须先在系统的 BIOS 设置中将其禁用，然后在 vSphere 客户端中将其关闭（请注意，默认为 vSphere 启用超线程）。请参阅系统文档，以确定您的 CPU 是否支持超线程。

对 SR-IOV 的支持

SR-IOV 虚拟功能需要特定的系统资源。除支持 SR-IOV 功能的 PCIe 适配器之外，还需要支持 SR-IOV 的服务器。您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。支持以下 NIC：
  - Intel 以太网服务器适配器 X520 - DA2
  - Intel 以太网服务器适配器 X540
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。
- x86_64 多核 CPU - Intel 沙桥或更高版本（推荐）。

注释 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 threat defense virtual 进行了测试。

- 核心
  - 每个 CPU 插槽至少 8 个物理核心

注释 Threat Defense Virtual 不支持物理核心的多非一致内存访问 (NUMA) 节点和多个 CPU 插槽。

  - 确保将所有已分配的物理核心分配到单个插槽。

注释 建议通过 CPU 固定来实现完整的吞吐量。

请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。可以搜索 VMware 联机兼容性指南，了解包含 SR-IOV 支持的系统建议。

对 SSSE3 的支持

- Threat Defense Virtual 要求您的系统支持英特尔命名的 Supplemental Streaming SIMD Extensions 3（SSSE3 或 SSE3S），这是一种单指令流多数据流 (SIMD) 指令集。
- 您的系统应配备支持 SSSE3 的 CPU，例如 Intel Core 2 Duo、Intel Core i7/i5/i3、Intel Atom、AMD Bulldozer、AMD Bobcat 和更高版本的处理器。
- 请参阅此参考页面，进一步了解 SSSE3 指令集和支持 SSSE3 的 CPU。

验证 CPU 支持

您可以使用 Linux 命令行获取 CPU 硬件的相关信息。例如，**/proc/cpuinfo** 文件包含每个 CPU 核心的详细信息。运行 **less** 或 **cat** 命令，可输出其中的内容。

您可以前往“flags”部分查看以下值：

- vmx - Intel VT 扩展
- svm - AMD-V 扩展
- ssse3 - SSSE3 扩展

要查看文件中是否包含这些值，请使用 **grep** 运行以下命令：

```
egrep “vmx|svm|ssse3” /proc/cpuinfo
```

如果您的系统支持 VT 或 SSSE3，您会在“flags”列表中看到 vmx、svm 或 ssse3。以下示例显示了含有两种 CPU 的系统的输出：

```
flags    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm

flags    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

准则和限制

Threat Defense Virtual 智能许可的性能层

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *3:* 基于授权的 *Threat Defense Virtual* 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

请参阅《Cisco Secure Firewall Management Center 管理指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

性能优化

为实现 threat defense virtual 的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅提高 ESXi 配置的性能，第 34 页、NUMA 准则，第 34 页和SR-IOV 接口调配，第 34 页。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。RSS 在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

集群

从版本 7.2 开始，在 VMware 上部署的 Threat Defense Virtual 实例支持集群。有关详细信息，请参阅私有云中 Threat Defense Virtual 的集群。

管理模式

- 您可以通过两种方法来管理您的 Cisco Secure Firewall Threat Defense（之前称为 Firepower Threat Defense）设备。
  - 设备管理器 板载集成的管理器。

注释 VMware 上的 threat defense virtual 支持运行思科 6.2.2 及更高版本软件的设备管理器。VMware 上任何运行 6.2.2 版之前软件的 threat defense virtual 只能使用 管理中心管理；请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页

  - 管理中心。

- 必须安装新版映像（6.2.2 或更高版本）才能取得 设备管理器支持。不能在从较低版本（低于 6.2.2）更新现有 threat defense virtual 计算机后切换至 设备管理器。
- 设备管理器 （本地管理器）默认启用。

注释 当**启用本地管理器**选项设置为**是**时，防火墙模式会变为“已路由”。这是使用 设备管理器 时唯一受支持的模式。

OVF 文件准则

安装 threat defense virtual的可用选项如下：

```
Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

其中，X.X.X-xxx 是要使用的文件的版本和内部版本号。

- 如果使用 VI OVF 模板部署，安装过程中，您可以执行 threat defense virtual 设备的整个初始设置。可以指定：
  - 管理员账户的新密码。
  - 使设备可以在管理网络上进行通信的网络设置。
  - 管理模式 - 使用 设备管理器 进行本地管理（默认），或者使用 管理中心 进行远程管理。
  - 防火墙模式 - 当启用本地管理器选项设置为是时，防火墙模式会变为已路由。这是使用 设备管理器 时唯一受支持的模式。

注释 必须使用 VMware vCenter 管理此虚拟设备。

- 如果使用 ESXi OVF 模板部署，必须在安装后配置系统所需的设置。您可以将此 threat defense virtual 作为 ESXi 上的独立设备管理；有关详细信息，请参阅向 vSphere ESXi 主机部署 Threat Defense Virtual，第 29 页。

无法在 vSphere 7.0.2 中保存虚拟机 (VM) 配置

如果使用的是 vSphere 7.0.2，则可能不允许保存 VM 配置。

注释 您可以按照 VMware 知识库文章中的说明解决此问题：https://kb.vmware.com/s/article/83898。

vMotion 支持

如果计划使用 vMotion，建议仅使用共享存储。在部署期间，如果有主机集群，则可以在本地（特定主机上）或在共享主机上调配存储。但是，如果您尝试使用 vMotion 将 Cisco Secure Firewall Management Center Virtual（之前称为 Firepower Management Center Virtual）迁移到另一台主机，则使用本地存储将会产生错误。

不推荐使用超线程

超线程技术允许单个物理处理器内核像两个逻辑处理器一样运行。我们建议您为运行 threat defense virtual 的系统禁用超线程。Snort 进程已经最大限度地利用了 CPU 内核的处理资源。当尝试通过每个处理器推动两个 CPU 使用率线程时，性能不会有任何提高。实际上，由于超线程进程所需的开销，您可能还会看到性能下降。

INIT 重生错误消息现象

您可能会在运行 ESXi 6 或 ESXi 6.5 的 threat defense virtual 控制台上看到以下错误消息：

```
"INIT: Id "ftdv" respawning too fast: disabled for 5 minutes"
```

解决方法 - 在设备电源关闭时，编辑 vSphere 中的虚拟机设置添加串行端口。

1. 右键点击虚拟机，然后选择**编辑设置 (Edit Settings)**。
2. 在虚拟硬件选项卡中，从**新设备 (New device)** 下拉菜单中选择**串行端口 (Serial port)**，然后点击**添加 (Add)**。

   虚拟设备列表的底部将会显示串行端口。
3. 在**虚拟硬件 (Virtual Hardware)** 选项卡中，展开**串行端口 (Serial port)**，并选择连接类型**使用物理串行端口 (Use physical serial port)**。
4. 取消选中**在启动时连接**复选框。

   点击**确定 (OK)** 保存设置。

从防火墙保护中排除虚拟机

在 vCenter Server 与 VMware NSX Manager 集成的 vSphere 环境中，分布式防火墙 (DFW) 作为 VIB 包在所有为 NSX 准备的 ESXi 主机集群的内核中运行。主机准备工作会自动激活 ESXi 主机集群上的 DFW。

threat defense virtual 使用混合模式运行，并且如果需要混合模式的虚拟机受分布式防火墙保护，则这些虚拟机的性能可能会受到不利影响。VMware 建议您将需要混合模式的虚拟机排除在分布式防火墙保护之外。

1. 导航到排除列表设置。
   - 在 NSX 6.4.1 及更高版本中，导航到**网络和安全 (Networking & Security)** > **安全 (Security)** > **防火墙设置 (Firewall Settings)** > **排除列表 (Exclusion List)**。
   - 在 NSX 6.4.0 中，导航到**网络和安全 (Networking & Security)** > **安全 (Security)** > **防火墙 (Firewall)** > **排除列表 (Exclusion List)**。
2. 点击**添加 (Add)**。
3. 将要排除的虚拟机移至**所选对象**。
4. 点击**确定 (OK)**。

如果虚拟机有多个 vNIC，则所有 vNIC 都不在保护范围内。如果在将虚拟机添加到排除列表后再将 vNIC 添加到虚拟机，则会在新添加的 vNIC 上自动部署防火墙。要将新 vNIC 排除在防火墙保护之外，必须将虚拟机从排除列表中移除，然后将其重新添加到排除列表中。另一种解决方法是重启（关闭电源再打开电源）虚拟机，但第一种方法的破坏性较小。

修改 vSphere 标准交换机的安全策略设置

对于 vSphere 标准交换机，第 2 层安全策略的三个要素是混合模式、MAC 地址更改和伪造传输。Threat Defense Virtual 使用混合模式运行，threat defense virtual 实际高可用性取决于在主用设备和备用设备之间切换 MAC 地址才能正常运行。

默认设置会阻碍 threat defense virtual 的正确运行。请参见以下要求的设置：

表 *4: vSphere* 标准交换机安全策略选项

选项	要求的设置	操作
混合模式	接受	您必须在 vSphere Web 客户端中编辑 vSphere 标准交换机的安全策略，并将混合模式选项设置为“接受”。 防火墙、端口扫描程序、入侵检测系统等等需要在混合模式下运行。
MAC 地址更改	接受	您应该在 vSphere Web 客户端中检验 vSphere 标准交换机的安全策略，确认 MAC 地址更改选项已设为“接受”。
伪传输	接受	您应该在 vSphere Web 客户端中检验 vSphere 标准交换机的安全策略，确认伪传输选项已设为“接受”。

注释 对于 vSphere 标准交换机的 NSX-T 配置安全策略设置，我们没有任何建议，因为带有 NSX-T 的 VMware 不符合条件。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

修改 vSphere 标准交换机的安全策略设置

默认设置会阻碍 threat defense virtual 的正确运行。

过程

步骤 1 在 vSphere Web 客户端中，导航至主机。

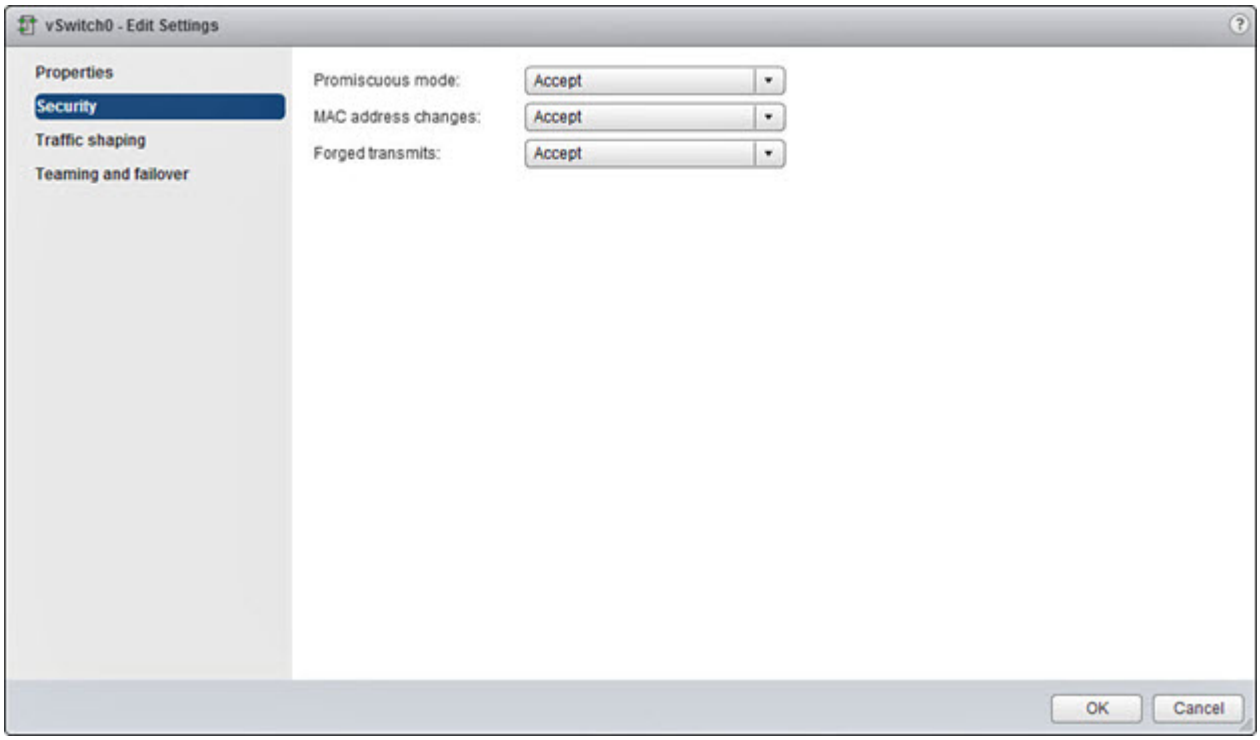
步骤 2 在**管理 (Manage)** 选项卡中，点击**网络 (Networking)**，然后选择**虚拟交换机 (Virtual switches)**。

步骤 3 从列表中选择一个标准交换机，然后点击**编辑设置 (Edit settings)**。

步骤 4 选择**安全**，查看当前设置。

步骤 5 在连接到标准交换机的虚拟机的访客操作系统中**接受**混合模式激活、MAC 地址更改和伪传输。

图 *1: vSwitch* 编辑设置



步骤 6 点击**确定 (OK)**。

下一步做什么

- 确保在为 threat defense virtual 上的管理和故障切换 (HA) 接口所配置的所有网络上，这些设置是相同的。

规划接口

您可以在部署之前规划 threat defense virtual vNIC 和接口映射，以避免重新启动和配置问题。threat defense virtual 部署有 10 个接口，首次启动时必须通过至少 4 个接口通电。

threat defense virtual 支持 vmxnet3（默认）、ixgbe 和 e1000 虚拟网络适配器。此外，借助正确配置的系统，threat defense virtual 也支持将 ixgbe-vf 驱动程序用于 SR-IOV；有关详细信息，请参阅系统要求，第 5 页。

重要事项 Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

接口准则和限制

以下部分介绍在 VMware 上与 threat defense virtual 一起使用的受支持虚拟网络适配器的准则和限制。在规划部署时，记住这些原则至关重要。

一般准则

- 如前所述，threat defense virtual 部署有 10 个接口，首次启动时必须通过至少 4 个接口通电。您需要将网络分配给**至少四个接口**。
- 我们建议您避免将 HOLDING 端口组用于 threat defense virtual 接口。来自 vSphere 的 HOLDING 端口组导致接口连接不一致。等待端口是分配给 VLAN ID 的通用端口组。这可能会导致在辅助 threat defense virtual 设备形成 HA 期间出现问题。
- 您无需使用全部 10 个 threat defense virtual 接口；对于您不打算使用的接口，只需在 threat defense virtual 配置中将其禁用即可。
- 请记住，在部署后，您不能将更多虚拟接口添加到虚拟机。如果在删除某些接口想要更多接口，则必须删除虚拟机并重新开始。
- 您可以选择为管理中心配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。请注意，在高可用性部署中，不支持从数据接口进行管理中心访问。有关为管理中心访问配置数据接口的详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考中的 **configure network management-data-interface** 命令。
- 在 threat defense virtual 内部接口或故障切换高可用性链路中使用的 ESX 端口组的两个虚拟网卡的故障切换顺序，必须配置为一个虚拟网卡作为活动上行链路，另一个作为备用上行链路。这是两个虚拟机相互 ping 或 Threat Defense Virtual 高可用性 (HA) 链路正常运行所必需的。

默认的 VMXNET3 接口

重要事项 Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

- vmxnet3 驱动程序使用两个管理接口。前两个以太网适配器必须配置为管理接口：一个用于设备管理/注册，一个保留用于内部用途。

- 对于 vmxnet3，思科建议在使用四个以上 vmxnet3 网络接口时使用由 VMware vCenter 管理的主机。部署在独立式 ESXi 上时，其他网络接口不会添加到具有连续 PCI 总线地址的虚拟机。通过 VMware vCenter 管理主机时，可以从配置 CDROM 的 XML 中获取正确的顺序。当主机运行独立式 ESXi 时，只能通过手动比较在 threat defense virtual 上看到的 MAC 地址与从 VMware 配置工具看到的 MAC 地址，确定网络接口的顺序。

下表描述了 threat defense virtual 适用于 vmxnet3 和 ixgbe 接口的网络适配器、源网络和目标网络的一致性。

表 *5:* 源网络与目标网络的映射 - *VMXNET3* 和 *IXGBE*

网络适配器	源网络	目标网络	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	保留供内部使用。	保留供内部使用。	保留供内部使用。
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
网络适配器 5	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（可选）
网络适配器 6	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
网络适配器 7	GigabitEthernet0-4	GigabitEthernet0/4	数据流量（可选）
网络适配器 8	GigabitEthernet0-5	GigabitEthernet0/5	数据流量（可选）
网络适配器 9	GigabitEthernet0-6	GigabitEthernet0/6	数据流量（可选）
网络适配器 10	GigabitEthernet0-7	GigabitEthernet0/7	数据流量（可选）

IXGBE 接口

- ixgbe 驱动程序使用两个管理接口。前两个 PCI 设备必须配置为管理接口：一个用于设备管理/注册，一个保留用于内部用途。
- 对于 ixgbe，ESXi 平台要求 ixgbe NIC 支持 ixgbe PCI 设备。此外，ESXi 平台还具有支持 ixgbe PCI 设备所需的特定 BIOS 和配置要求。有关详细信息，请参阅英特尔技术概要。
- 对于 ixgbe 流量接口，系统仅支持“路由”和“ERSPAN 被动”两种类型。这是由于有关 MAC 地址过滤的 VMware 限制所致。
- 驱动程序不支持 threat defense virtual 的故障转移 (HA) 部署。

E1000 接口

重要事项 Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

- 如果您将 threat defense virtual 升级到 6.4 并使用 e1000 接口，则应将 e1000 接口替换为 vmxnet3 或 ixgbe 接口，以实现更大的网络吞吐量。

下表描述了 threat defense virtual 适用于默认 e1000 接口的网络适配器、源网络和目标网络的一致性。

表 *6:* 源网络与目标网络的映射 - *E1000* 接口

网络适配器	源网络	目标网络	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 3	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
网络适配器 4	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（必需）
网络适配器 5	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
网络适配器 6	GigabitEthernet0-4	GigabitEthernet0/4	数据流量（可选）
网络适配器 7	GigabitEthernet0-5	GigabitEthernet0/5	数据流量（可选）
网络适配器 8	GigabitEthernet0-6	GigabitEthernet0/6	数据流量（可选）
网络适配器 9	GigabitEthernet0-7	GigabitEthernet0/7	数据流量（可选）
网络适配器 10	GigabitEthernet0-8	GigabitEthernet0/8	数据流量（可选）

配置 VMXNET3 接口

重要事项 从 6.4 版本开始，当您创建虚拟设备时，VMware 上的 threat defense virtual 和 Management Center Virtual 默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

要将 e1000 接口更改为 vmxnet3，必须删除所有接口，然后使用 vmxnet3 驱动程序重新安装。

虽然可以在部署中混合使用接口（例如在 管理中心 上使用 e1000 接口，在其受管虚拟设备上使用 vmxnet3 接口），但不能在同一虚拟设备中混合使用接口。虚拟设备上的所有传感接口和管理接口必须为相同类型。

过程

步骤 1 断开 threat defense virtual 或 Management Center Virtual 计算机电源。

要更改接口，必须关闭设备电源。

步骤 2 右键点击清单中的 threat defense virtual 或 Management Center Virtual 计算机，然后选择**编辑设置 (Edit Settings)**。

步骤 3 选择适用的网络适配器，然后选择**删除 (Remove)**。

步骤 4 点击**添加 (Add)** 以打开**添加硬件向导 (Add Hardware Wizard)**。

步骤 5 选择**以太网适配器 (Ethernet adapter)**，然后点击**下一步 (Next)**。

步骤 6 选择 vmxnet3 适配器，然后选择网络标签。

步骤 7 对 threat defense virtual 上的所有接口重复上述操作。

下一步做什么

- 从 VMware 控制台接通 threat defense virtual 或 Management Center Virtual 电源。

添加接口

部署 threat defense virtual 设备时，最多可以设置 10 个接口（1 个管理接口、1 个保留接口以供内部使用和 8 个数据接口）。如果添加额外的数据接口，请确保**源网络**映射到正确的**目标网络**，而且每个数据接口都映射到一个唯一的子网或 VLAN。

⚠

注意 您不能给虚拟机添加多个虚拟接口，然后让 threat defense virtual 来自动识别它们。要给虚拟机添加接口，您需要完全清除 threat defense virtual 配置。配置中唯一保留不变的部分是管理地址和网关设置。

如果您需要为 threat defense virtual 设备配置更多物理接口对等体，那基本上需要重新执行该流程。您可以部署新的虚拟机，也可以使用 《Cisco Secure Firewall 设备管理器配置指南》 中的 “扫描接口更改并迁移接口”程序。

关于 VMware 部署

您可以将 threat defense virtual 部署到独立的 ESXi 服务器；如果有 vSphere vCenter，则可以使用 vSphere 客户端或 vSphere Web 客户端进行部署。要成功部署 threat defense virtual，您应该熟悉 VMware 和 vSphere，包括 vSphere 联网、ESXi 主机设置和配置，以及虚拟机访客部署。

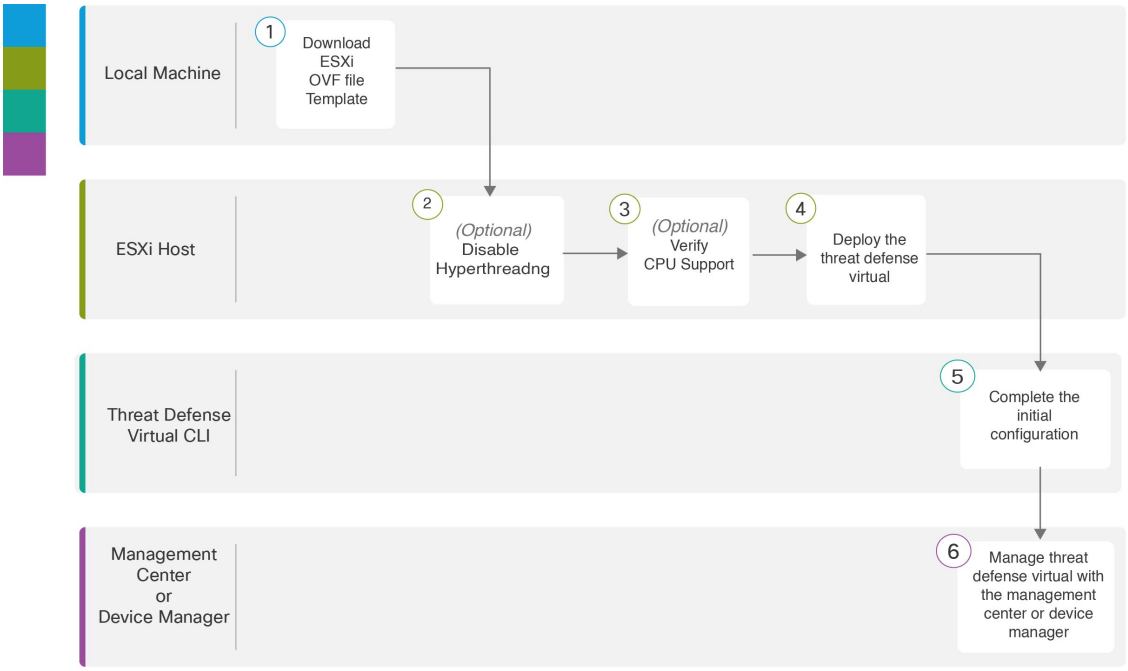
Threat Defense Virtual 对于 VMware 使用开放虚拟化格式（OVF）进行分发，这是一种打包和部署虚拟机的标准方法。VMware 提供多种调配 vSphere 虚拟机的方法。最适合您的环境的方法取决于多种因素，例如基础设施的规模和类型以及您要实现的目标等。

VMware vSphere Web 客户端和 vSphere 客户端都是连接 vCenter 服务器、ESXi 主机和虚拟机的接口。通过 vSphere Web 客户端和 vSphere 客户端，可以远程连接到 vCenter 服务器。通过 vSphere 客户端，还可以从任何 Windows 系统直接连接到 ESXi。VSphere Web 客户端和 vSphere 客户端是管理 vSphere 环境所有方面的主要界面。它们还提供虚拟机的控制台访问权限。

可通过 vSphere Web 客户端使用所有管理功能。可通过 vSphere 客户端使用其中的部分功能。

端到端程序

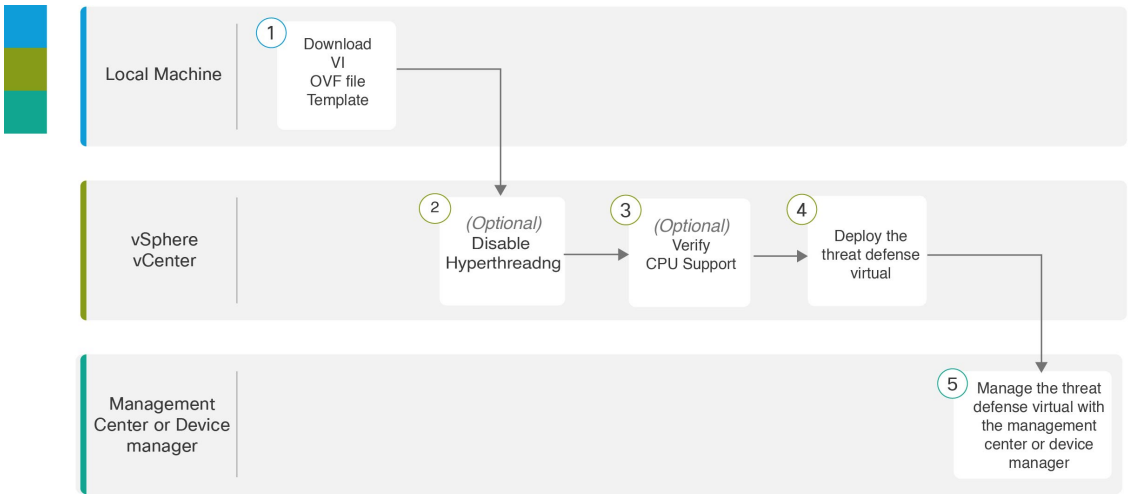
以下流程图说明了在 ESXi 主机上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	本地计算机	下载 ESXi OVF 模板：从 Cisco.com 下载开放虚拟化格式 (OVF) 软件包。
2	ESXi 主机	（可选）系统要求：为运行 threat defense virtual 的系统禁用超线程。
3	ESXi 主机	（可选）系统要求：使用 Linux 命令行获取 CPU 硬件的相关信息。
4	ESXi 主机	向 vSphere ESXi 主机部署 Threat Defense Virtual：在单个 ESXi 主机上部署 threat defense virtual 设备。

	工作空间	步骤
5	Threat Defense Virtual CLI	使用 CLI 完成 Threat Defense Virtual 设置：如果使用 ESXi OVF 模板部署，则必须使用 CLI 来设置 threat defense virtual。
6	管理中心或设备管理器	管理 threat defense virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页 • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual，第 427 页

以下流程图说明了在 vSphere vCenter 上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	本地计算机	下载 VI OVF 模板：从 Cisco.com 下载开放虚拟化格式 (OVF) 软件包。
2	vSphere vCenter	（可选）系统要求：为运行 threat defense virtual 的系统禁用超线程。
3	vSphere vCenter	（可选）系统要求：使用 Linux 命令行获取 CPU 硬件的相关信息。
4	vSphere vCenter	向 vSphere ESXi 主机部署 Threat Defense Virtual：在单个 ESXi 主机上部署 threat defense virtual 设备。

	工作空间	步骤
5	管理中心或设备管理器	管理 threat defense virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页 • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual，第 427 页

将 Threat Defense Virtual 部署到 vSphere vCenter

遵照此程序可将 threat defense virtual 设备部署到 VMware vSphere vCenter。您可以使用 VMware Web 客户端（或 vSphere 客户端）部署和配置 threat defense virtual 计算机。

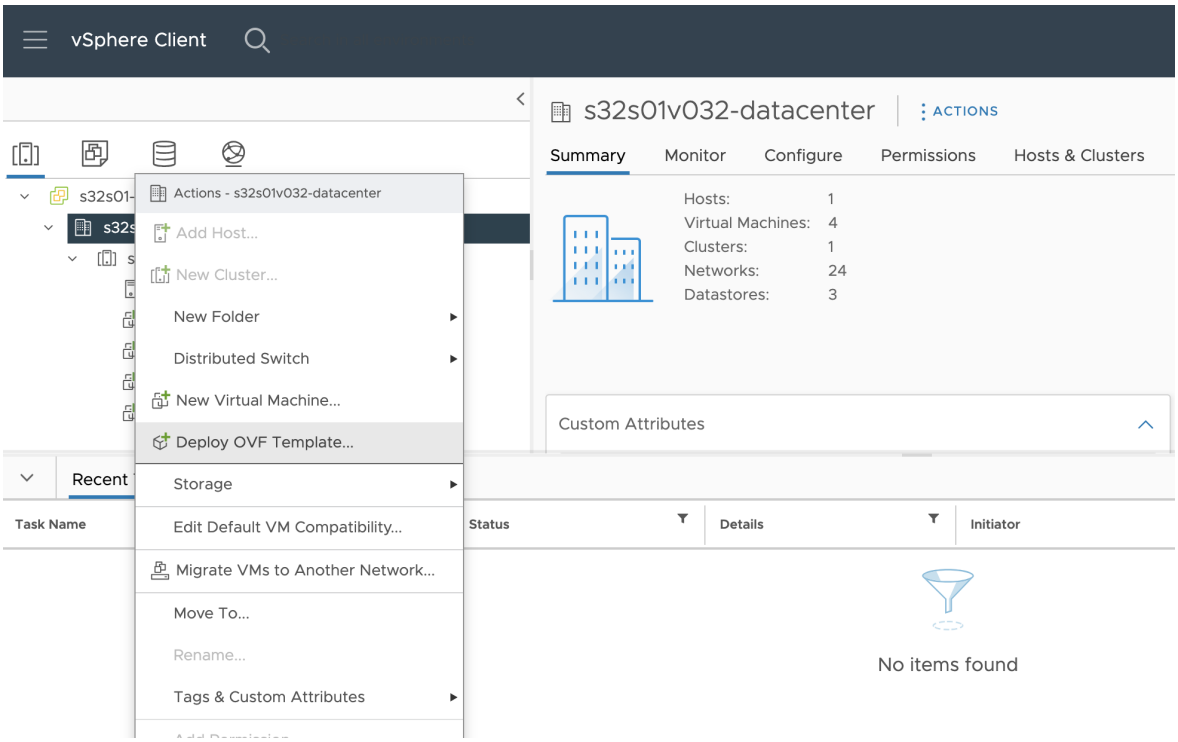
开始之前

- 在部署 threat defense virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。

过程

步骤 1 登录到 vSphere Web 客户端（或 vSphere 客户端）。

步骤 2 点击 **文件** > **部署 OVF 模板**，使用 vSphere Web 客户端（或 vSphere 客户端）部署之前下载的 OVF 模板文件。



此时将出现“部署 OVF 模板”向导。

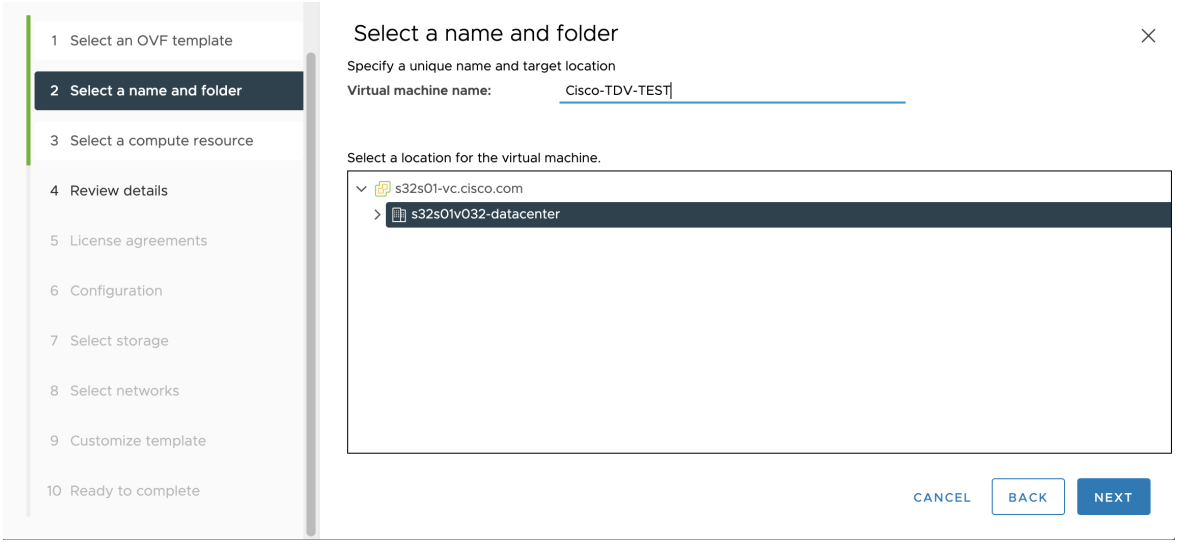
步骤 3 浏览文件系统以找到 OVF 模板源位置，然后点击**下一步**。

选择 threat defense virtual VI OVF 模板：

Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf

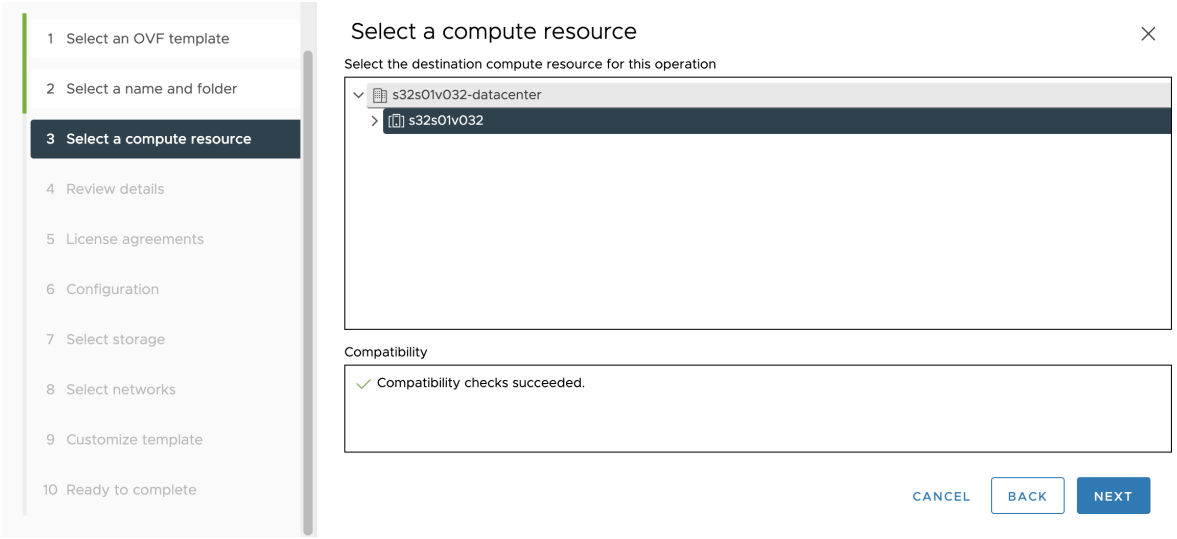
其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

步骤 4 在**名称和位置 (Name and Location)**页面，输入此部署的名称，然后在清单中选择要部署 threat defense virtual 的的位置（主机或集群），然后点击**下一步 (Next)**。名称在清单文件夹中必须唯一，最多可以包含 80 个字符。



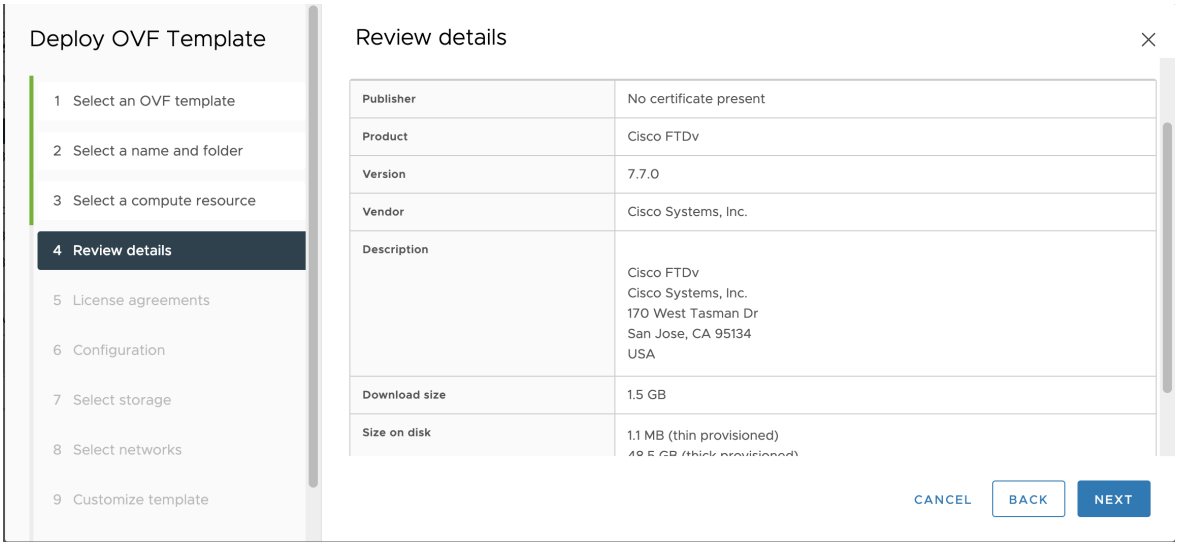
VSphere Web 客户端在清单视图中显示托管对象的组织层级。清单是 vCenter 服务器或主机用于组织托管对象的分层结构。此层次结构包括 vCenter 服务器中的所有受监控对象。

步骤 5 导航至并选择您想运行 threat defense virtual的资源池，然后点击**下一步**。



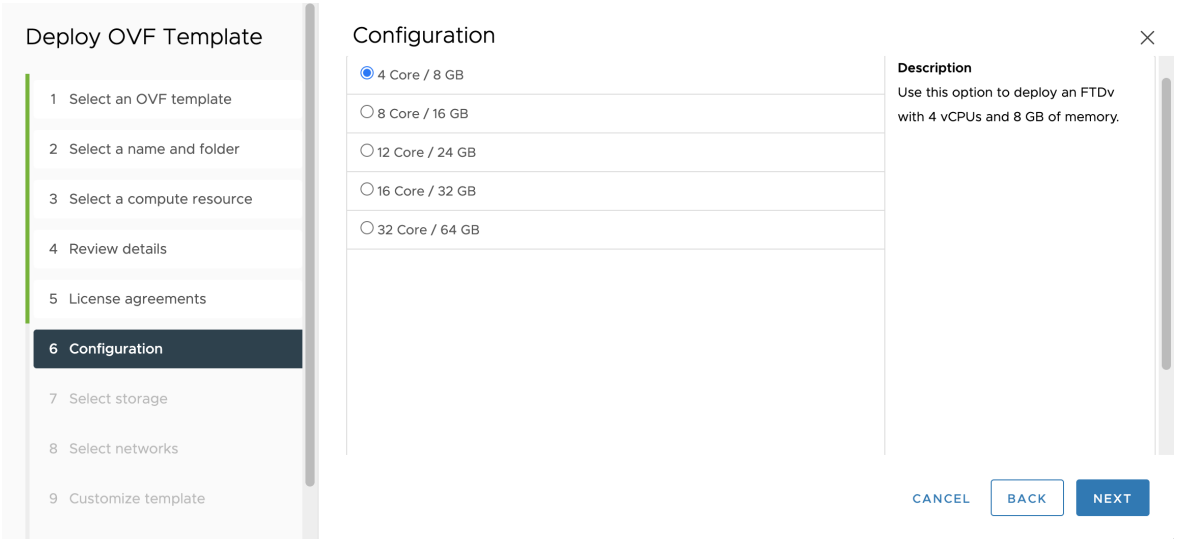
注释
仅当集群包含资源池时，系统才会显示此页面。

步骤 6 查看 **OVF 模板详细信息**页面并验证 OVF 模板信息（产品名称、版本、供应商、下载大小、磁盘大小和说明），然后点击**下一步**。



步骤 7 屏幕上随即会显示**最终用户许可协议**页面。查看随 OVF 模板提供的许可协议（仅 VI 模板），点击**接受**同意许可条款，然后点击**下一步**。

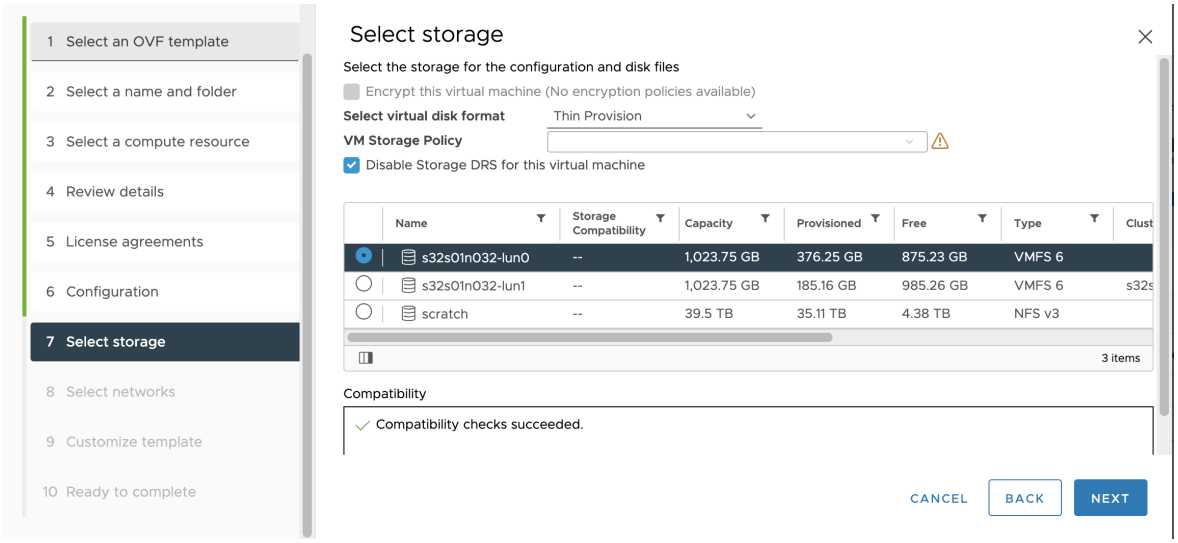
步骤 8 中 **配置** 页面，从 **配置** 选项中的受支持的 vCPU/内存值中选择一个，然后点击 **下一步**。



重要事项

部署的 threat defense virtual 具有可调的 vCPU 和内存资源。

步骤 9 选择要存储虚拟机文件的 **存储** 位置。

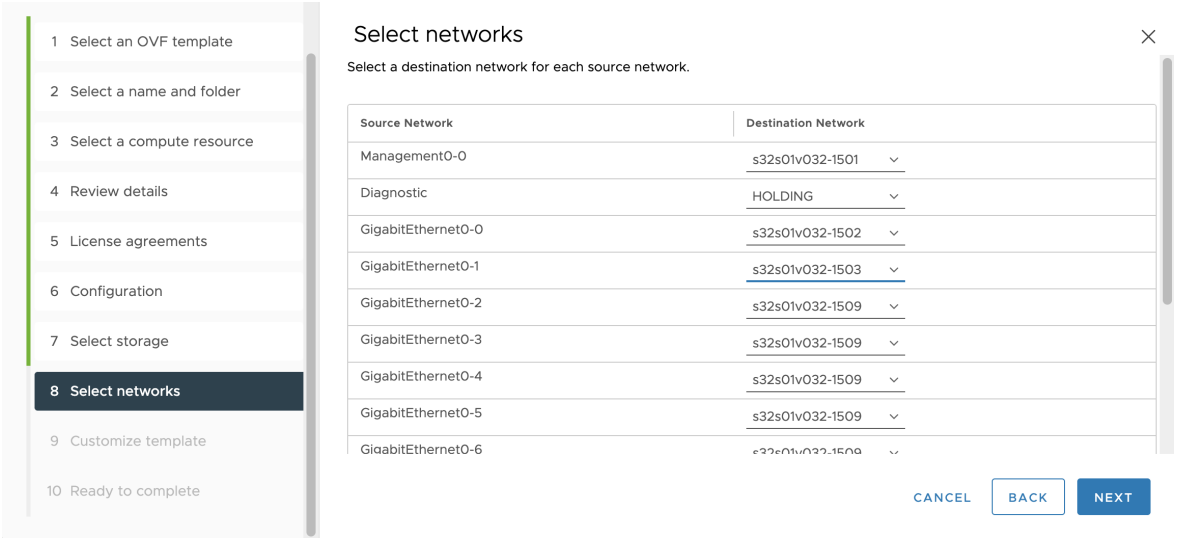


在此页面上，您可以从目标集群或主机上已配置的数据存储中选择。虚拟机配置文件和虚拟磁盘文件均存储在 Datastore 上。选择一个足够大的数据存储，以容纳虚拟机及其所有虚拟磁盘文件。

步骤 10 从 **选择虚拟磁盘格式** 下拉列表中选择 **磁盘格式** 以存储虚拟机虚拟磁盘，然后点击 **下一步**。

如果选择**密集调配 (Thick Provisioned)**，则会立即分配所有存储。如果选择**精简调配 (Thin Provisioned)**，则会在数据写入虚拟磁盘时将按需分配存储。精简调配还可缩短虚拟设备的部署时间。

步骤 11 在 **选择网络** 页面，将 OVF 模板中指定的网络映射到您清单中的网络，然后点击 **下一步**。



确保将 Management0-0 接口关联到可以从互联网访问的 VM 网络。非管理接口可从 管理中心 或 设备管理器 配置，具体取决于您的管理模式。

重要事项

Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

网络可能没有按字母顺序排序。如果很难找到您的网络，可以稍后在**编辑设置**对话框中更改网络。在部署后，右键点击 threat defense virtual 实例，然后选择**编辑设置**。但是，该屏幕不会显示 threat defense virtual ID（仅显示网络适配器 ID）。

请查看适用于 threat defense virtual 接口的以下网络适配器、源网络和目标网络的一致性（注意这些是默认的 vmxnet3 接口）：

表 *7:* 源网络与目标网络的映射 - *VMXNET3*

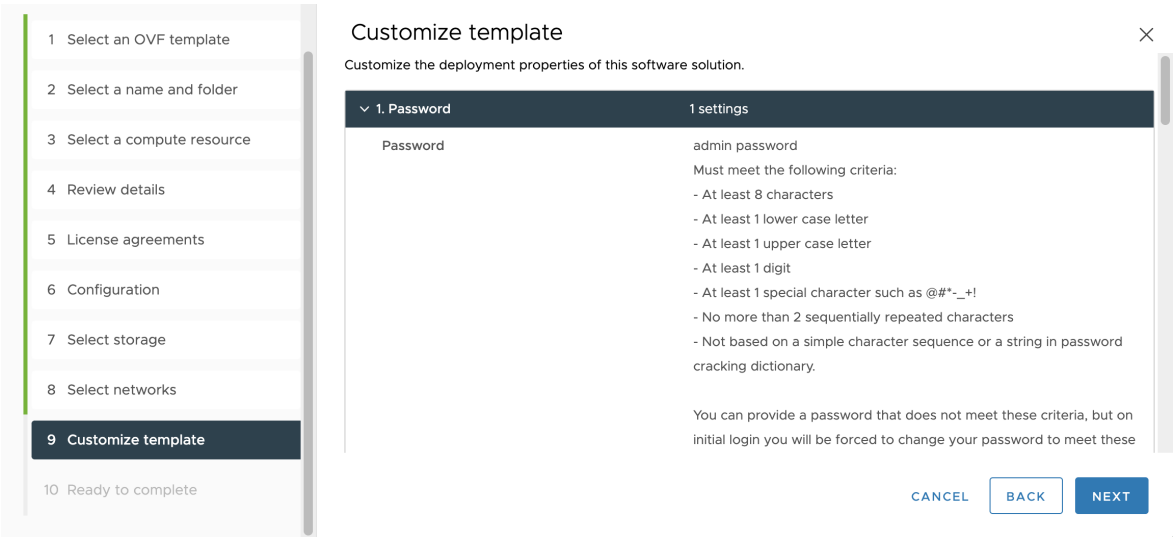
网络适配器	源网络	目标网络	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	保留供内部使用。	保留供内部使用。	保留供内部使用。
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
网络适配器 5	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（可选）
网络适配器 6	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
网络适配器 7	GigabitEthernet0-4	GigabitEthernet0/4	数据流量（可选）
网络适配器 8	GigabitEthernet0-5	GigabitEthernet0/5	数据流量（可选）

网络适配器	源网络	目标网络	功能
网络适配器 9	GigabitEthernet0-6	GigabitEthernet0/6	数据流量（可选）
网络适配器 10	GigabitEthernet0-7	GigabitEthernet0/7	数据流量（可选）

部署 threat defense virtual 时，总共可以有 10 个接口。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。您无需使用所有 threat defense virtual 接口；对于不打算使用的接口，只需在 threat defense virtual 配置中将其禁用即可。

步骤 12 在 **自定义模板** 属性页面，设定随 OVF 模板（仅 VI 模板）提供的用户可配置属性：

a) **密码**

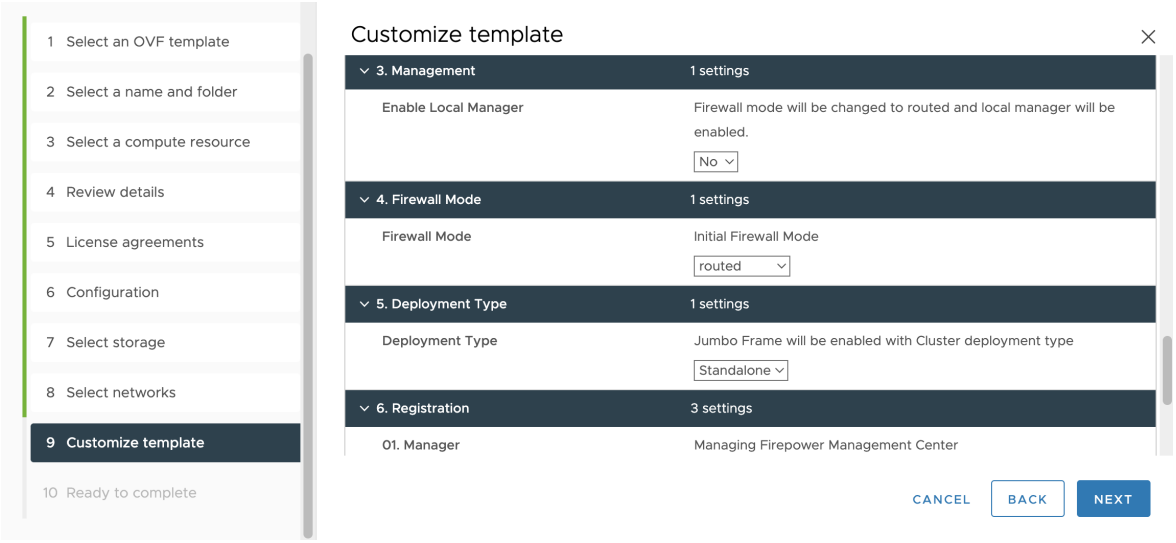


设置 threat defense virtual 管理员访问的密码。

b) **网络**

设置网络信息，包括完全限定的域名 (FQDN)、DNS、搜索域和网络协议（IPv4 或 IPv6）。

c) **管理**



设置管理模式。点击**启用本地管理器**的下拉箭头，然后选择**是**使用集成的基于 Web 的设备管理器配置工具。选择**否 (No)** 以使用 管理中心 来管理此设备。有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

d) **防火墙模式**

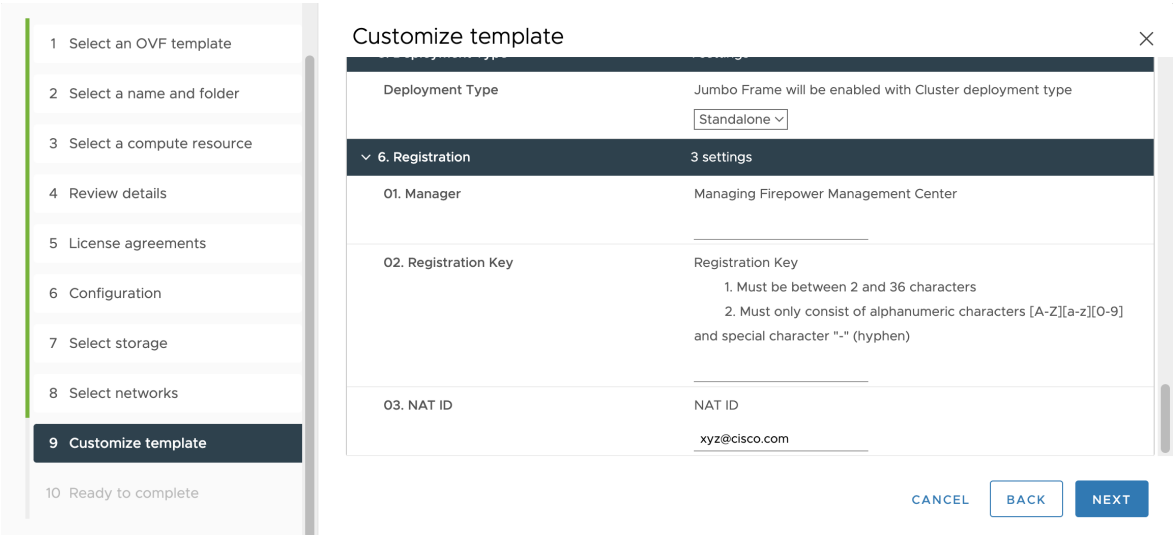
设定初始防火墙模式。点击**防火墙模式**的下拉箭头，然后选择两种支持的模式之一；**已路由**或**透明**。

如果对**启用本地管理器**选择**是**，则只能选择**已路由**防火墙模式。不能使用本地 设备管理器 配置透明防火墙模式接口。

e) **部署类型**

将部署类型设置为**独立**或**集群**。依次选择**集群 (Cluster)** 以启用巨帧预留，这是集群控制链路所必需的。为独立或高可用性部署选择**独立 (Standalone)**。请注意，如果作为独立设备部署，仍可在集群中使用；但是，在部署后为集群启用巨帧意味着必须重新启动。

f) **注册**

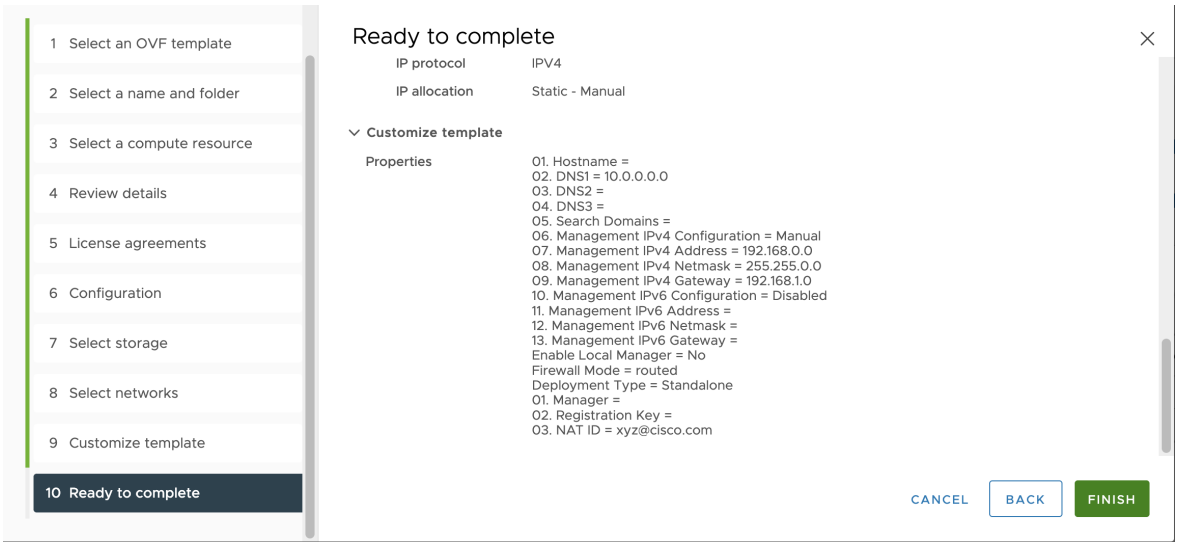


如果对**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，则需要提供必要的凭证以将此设备注册到负责管理的 Cisco Secure Firewall Management Center。提供以下各项：

- **负责管理的防御中心** - 输入 管理中心 的主机名或 IP 地址。
- **注册密钥** - 注册密钥是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。当您将设备添加到 管理中心时，需要记住此注册密钥。
- **NAT ID** - 如果 threat defense virtual 和 管理中心 被网络地址转换 (NAT) 设备分隔，并且 管理中心 位于 NAT 设备后方，请输入一个唯一的 NAT ID。这是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。

g) 点击**下一步**。

步骤 13 在 **即将完成** 页面中，查看并验证显示的信息。要使用这些设置开始部署，单击**完成**。要进行更改，点击**后退**以在屏幕中向后导航。



或者，选中**部署后启动**选项启动 threat defense virtual，然后点击**完成**。

完成该向导后，vSphere Web 客户端将处理虚拟机；您可以在**全局信息**区域的**最近任务**窗格中看到“初始化 OVF 部署”状态。

完成后，您会看到“部署 OVF 模板”完成状态。

在“清单”(Inventory) 中的指定数据中心下会显示 threat defense virtual 实例。启动新的 VM 最多可能需要 30 分钟。

注释
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

为集部署准备 Day 0 配置文件

在启动 threat defense virtual之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时装载和读取的 day0.iso 文件。

重要事项 该 day0.iso 文件必须在首次启动期间可用。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 threat defense virtual 设备的整个初始设置。可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。
- 管理模式；请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

  输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的信息。对于您未使用的管理模式，保留字段为空。
- 使设备可以在管理网络上进行通信的网络设置。
- 部署类型，您可以在其中指定是将 threat defense virtual 作为集群部署还是独立部署。

注释 本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

过程

步骤 1 登录到要部署 threat defense virtual 的 Linux 主机。

步骤 2 为 threat defense virtual 创建名为“day0-config”的文本文件。在此文本文件中，您必须添加集群部署设置、网络设置以及有关管理 管理中心 的信息。

示例：

```
#Firepower Threat Defense
{

     "DeploymentType": "Cluster"

}
```

输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）。对于您未使用的管理选项，将这些字段留空。

步骤 3 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

步骤 4 登录到目标 ESXi 主机。

步骤 5 打开要在集群模式下部署 threat defense virtual 的虚拟机实例。

步骤 6 在启动虚拟机之前，浏览您创建的 day0 ISO 映像文件并将其附加到**硬件配置 (Hardware Configuration)** 设置下的 **CD/DVD 驱动器 1 (CD/DVD drive 1)** 字段。

步骤 7 启动虚拟机以在集群模式下部署 threat defense virtual。

向 vSphere ESXi 主机部署 Threat Defense Virtual

遵照此程序可在单个 ESXi 主机上部署 threat defense virtual 设备。您可以使用 VMware 主机客户端（或 vSphere 客户端）管理单个 ESXi 主机并执行管理任务，例如基本虚拟化操作（如部署和配置 threat defense virtual 计算机）。

注释 了解 VMware 主机客户端与 vSphere Web 客户端的区别很重要，尽管它们具有相似的用户界面。您可以使用 vSphere Web 客户端连接到 vCenter 服务器并管理多个 ESXi 主机，同时使用 VMware 主机客户端管理单个 ESXi 主机。

有关如何将 threat defense virtual 设备部署到 vCenter 环境的说明，请参阅将 Threat Defense Virtual 部署到 vSphere vCenter，第 20 页。

开始之前

- 在部署 threat defense virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。

过程

步骤 1 从 Cisco.com 下载适用于 VMware ESXi 的 threat defense virtual 安装软件包，并将其保存到本地的管理计算机。

https://www.cisco.com/go/ftd-software

需要 Cisco.com 登录信息和思科服务合同。

步骤 2 将 tar 文件解压缩到工作目录中。请勿删除该目录中的任何文件。其中包括以下文件：

- Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-*X.X.X-xxx*.ovf - 适用于 vCenter 部署
- Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.ovf - 适用于 ESXi 部署。
- Cisco_Secure_Firewall_Threat_Defense_Virtual-*X.X.X-xxx*.vmdk - VMware 虚拟磁盘文件。
- Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-*X.X.X-xxx*.mf - 适用于 vCenter 部署的清单文件。
- Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.mf - 适用于 ESXi 部署的清单文件。

其中，*X.X.X-xx* 是已下载的存档文件的版本和内部版本号。

步骤 3 在浏览器中，使用 *http://host-name/ui* 或 *http://host-IP-address/ui* 格式输入 ESXi 目标主机名或 IP 地址。

登录屏幕会显示。

步骤 4 输入管理员用户名和密码。

步骤 5 点击**登录**继续。

此时您即已登录到目标 ESXi 主机。

步骤 6 右键点击 VMware 主机客户端清单中的**主机**，然后选择**创建/注册 VM**。

新的虚拟机向导将打开。

步骤 7 在向导的**选择创建类型**页面，选择**从 OVF 或 OVA 文件部署虚拟机**，然后点击**下一步**。

步骤 8 在向导的**选择 OVF 和 VMDK 文件**页面：

a) 输入您的 threat defense virtual 计算机的名称。

虚拟机名称最多可包含 80 个字符，并且在每个 ESXi 实例中必须唯一。

b) 点击蓝色窗格，浏览到您将 threat defense virtual tar 文件解压缩到的目录，然后选择 ESXi OVF 模板和附带的 VMDK 文件：

Cisco_Secure_Firewall_Threat_Defense_Virtual-ESXi-*X.X.X-xxx*.ovf

Cisco_Secure_Firewall_Threat_Defense_Virtual-*X.X.X-xxx*.vmdk

其中，*X.X.X-xx* 是已下载的存档文件的版本和内部版本号。

注意
确保选择 ESXi OVF。

步骤 9 点击**下一步**。

您的本地系统存储将打开。

步骤 10 从向导**选择存储**页面上的可访问数据存储库列表中选择一个数据存储库。

数据存储库会保存虚拟机配置文件和所有虚拟磁盘文件。每个数据存储库的大小、速度、可用性和其他属性可能有所不同。

步骤 11 点击**下一步**。

步骤 12 配置随适用于 threat defense virtual 的 ESXi OVF 提供的**部署选项**：

a) **网络映射** - 将 OVF 模板中指定的网络映射到清单中的网络，然后选择**下一步**。

确保将 Management0-0 接口关联到可以从互联网访问的 VM 网络。非管理接口可从 管理中心 或 设备管理器配置，具体取决于您的管理模式。

重要事项

Threat Defense Virtual 在 VMware 上，如果创建虚拟设备，则默认为 vmxnet3 接口。先前，默认值为 e1000。如果您使用的是 e1000 接口，我们**强烈建议**您切换。vmxnet3 设备驱动器和网络处理与 ESXi 虚拟机监控程序集成，因此其使用更少的资源并提供更好的网络性能。

网络可能没有按字母顺序排序。如果很难找到您的网络，可以稍后在**编辑设置**对话框中更改网络。在部署后，右键点击 threat defense virtual 实例，然后选择**编辑设置**。但是，该屏幕不会显示 threat defense virtual ID（仅显示网络适配器 ID）。

请查看适用于 threat defense virtual 接口的以下网络适配器、源网络和目标网络的一致性（注意这些是默认的 vmxnet3 接口）：

表 *8*: 源网络与目标网络的映射 - *VMXNET3*

网络适配器	源网络	目标网络	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	保留供内部使用。	保留供内部使用。	保留供内部使用。
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部数据
网络适配器 5	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（可选）
网络适配器 6	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
网络适配器 7	GigabitEthernet0-4	GigabitEthernet0/4	数据流量（可选）
网络适配器 8	GigabitEthernet0-5	GigabitEthernet0/5	数据流量（可选）
网络适配器 9	GigabitEthernet0-6	GigabitEthernet0/6	数据流量（可选）
网络适配器 10	GigabitEthernet0-7	GigabitEthernet0/7	数据流量（可选）

部署 threat defense virtual 时，总共可以有 10 个接口。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。您无需使用所有 threat defense virtual 接口；对于不打算使用的接口，只需在 threat defense virtual 配置中将其禁用即可。

b) **磁盘调配** - 选择磁盘格式以存储虚拟机虚拟磁盘。

如果选择**密集**调配，则会立即分配所有存储。如果选择**精简**调配，则会在数据写入虚拟磁盘时将按需分配存储。精简调配还可缩短虚拟设备的部署时间。

步骤 13 在新建虚拟机向导的**即将完成**页面，查看虚拟机的配置设置。

a) （可选）点击**返回**以返回并查看或修改向导设置。
b) （可选）点击**取消**以放弃创建任务并关闭向导。
c) 点击**完成**以完成创建任务并关闭向导。

完成该向导后，ESXi 主机将处理 VM；您可以在**最近任务**窗格中看到部署状态。部署成功完成后，**结果**列下将显示成功完成。

随后 ESXi 主机的虚拟机清单下会显示新的 threat defense virtual 虚拟机实例。启动新的虚拟机最多可能需要 30 分钟。

注释
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

下一步做什么

- 使用 CLI 完成虚拟设备的设置。这是使用 ESXi OVF 模板部署 threat defense virtual 时的下一步；请参阅使用 CLI 完成 Threat Defense Virtual 设置，第 32 页。

使用 CLI 完成 Threat Defense Virtual 设置

使用 ESXi OVF 模板部署时，必须使用 CLI 设置 threat defense virtual。Threat Defense Virtual 设备没有 Web 界面。如果使用 VI OVF 模板部署并且在部署过程中没有使用设置向导，也可以使用 CLI 来配置系统所需的设置。

注释 如果使用 VI OVF 模板部署并且使用了设置向导，虚拟设备已配置，并且不需要执行其他设备配置。接下来的步骤取决于您选择的管理模式。

首次登录新配置的设备时，必须阅读并接受 EULA。然后，请按照设置提示更改管理员密码，并配置设备的网络设置和防火墙模式。

在遵循设置提示的情况下，对于多选问题，选项会列在括号内，例如(y/n)。默认值会列在方括号内，例如 [y]。按 Enter 键确认选择。

过程

步骤 1 打开 VMware 控制台。

步骤 2 在 **firepower login** 提示符下，使用默认凭据（用户名 **admin**，密码 **Admin123**）登录。

步骤 3 当 threat defense virtual系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式（本地管理使用 设备管理器）。

步骤 4 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

当实施设置时，VMware 控制台可能显示消息。

步骤 5 根据提示完成系统配置。

步骤 6 当控制台返回到 firepower # 提示符时，确认设置是否成功。

注释
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

提高 ESXi 配置的性能

通过调整 ESXi 主机的 CPU 配置设置，可以提高 ESXi 环境中的 threat defense virtual 性能。通过调度关联选项，可以控制虚拟机 CPU 在主机物理核心（和超线程，如果已启用超线程）范围内的分布方式。使用此功能，您可以将每个虚拟机分配到指定关联组中的处理器。

有关详细信息，请参阅以下 VMware 文档。

- 《vSphere 资源管理》的 *CPU* 资源管理一章。
- 《VMware vSphere 的性能最佳实践》。
- vSphere 客户端联机帮助。

NUMA 准则

非一致内存访问 (NUMA) 是一种共享内存架构，描述了多处理器系统中主内存模块相对于处理器的位置。如果处理器访问的内存不在自己的节点内（远程内存），则数据通过 NUMA 连接以低于本地内存的访问速率传输。

X86 服务器架构由多个插槽和每个插槽内的多个内核组成。每个 CPU 插槽及其内存和 I/O 均称为 NUMA 节点。要从内存高效读取数据包，来宾应用和关联的外围设备（例如 NIC）应位于同一个节点中。

为获得最佳 threat defense virtual性能：

- threat defense virtual VM 必须在单一 NUMA 节点上运行。如果部署了单个 threat defense virtual 以跨 2 个插槽运行，则性能将显著下降。
- 8 核 threat defense virtual 要求主机 CPU 上的每个插槽至少有 8 个内核。必须考虑服务器上运行的其他虚拟机。
- 16 核 threat defense virtual 要求主机 CPU 上的每个插槽至少有 16 个内核。必须考虑服务器上运行的其他虚拟机。
- NIC 应与 threat defense virtual VM 位于同一 NUMA 节点上。

有关在 ESXi 上使用 NUMA 系统的详细信息，请参阅您的 VMware ESXi 版本对应的 VMware 文档 *vSphere* 资源管理。要查看此文档和其他相关文档的最新版本，请参阅 http://www.vmware.com/support/pubs... 。

SR-IOV 接口调配

单一根 I/O 虚拟化 (SR-IOV) 允许运行各种访客操作系统的多个 VM 共享主机服务器内的单个 PCIe 网络适配器。SR-IOV 允许 VM 在网络适配器中绕过虚拟机监控程序而直接移入或移出数据，从而提

高网络吞吐量及降低服务器 CPU 负担。最新的 x86 服务器处理器包括芯片组增强功能（例如 Intel VT-d 技术），它们可促进 SR-IOV 所需的直接内存传输及其他操作。

SR-IOV 规范定义了两种设备类型：

- 物理功能 (PF) - 实质上属于静态 NIC，PF 是完整的 PCIe 设备，包括 SR-IOV 功能。PF 按正常 PCIe 设备的方式进行发现、管理和配置。使用单个 PF 可为一组虚拟功能 (VF) 提供管理和配置。
- 虚拟功能 (VF) - 类似于动态 vNIC，VF 是完整或轻型虚拟 PCIe 设备，至少提供必要的数据移动资源。VF 并非直接进行管理，而是通过 PF 进行获取和管理。可以为一台 VM 分配一个或多个 VF。

VF 在虚拟化操作系统框架下，最高可以 10 Gbps 的速度连接 threat defense virtual 计算机。本节介绍如何在 VMware 环境下配置 VF。

SR-IOV 接口的最佳实践

SR-IOV 接口准则

VMware vSphere 5.1 及更高版本仅在具有特定配置的环境下支持 SR-IOV。启用 SR-IOV 时，vSphere 的某些功能无法正常工作。

除了 threat defense virtual 和 SR-IOV 的系统要求之外，您还应该查看 VMware 文档中的支持使用 SR-IOV 的配置，以了解有关要求、支持的 NIC、功能可用性及 VMware 和 SR-IOV 升级要求方面的详细信息。

VMware 上使用 SR-IOV 接口的 Threat Defense Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

本节介绍在 VMware 系统上调配 SR-IOV 接口的各种设置和配置步骤。本节中的信息基于特定实验室环境中的设备创建，这些设备使用的是 VMware ESXi 6.0 和 vSphere Web 客户端、思科 UCS C 系列服务器及 Intel 以太网服务器适配器 X520 - DA2。

SR-IOV 接口的限制

启动 threat defense virtual 时，请注意 SR-IOV 接口出现的顺序可能与 ESXi 中显示的顺序相反。这可能引起接口配置错误，导致特定的 threat defense virtual机无网络连接。

⚠

注意 开始在 threat defense virtual 上配置 SR-IOV 网络接口之前，先验证接口映射非常重要。这可确保将网络接口配置应用到 VM 主机上正确的物理 MAC 地址接口。

threat defense virtual 启动后，您可以确认哪个 MAC 地址映射到哪个接口。请使用 **show interface** 命令查看详细的接口信息，包括接口的 MAC 地址。将 MAC 地址与 **show kernel ifconfig** 命令的结果进行比较以确认正确的接口分配。

注：

使用 ixgbe-vf 接口的限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 threat defense virtual 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障转移通过从主用设备向备用设备传送 IP 地址的方式运行。

注释 此限制也适用于 i40e-vf 接口。

- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。
- 在故障转移设置中，当配对的 threat defense virtual（主设备）发生故障时，备用 threat defense virtual 设备将接管主设备的角色，并使用备用 threat defense virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，threat defense virtual 会向同一网络上的其他设备发送免费地址解析协议 (ARP) 更新，以通告接口 IP 地址的 MAC 地址更改。但是，由于与这些类型的接口不兼容，因此不会将免费 ARP 更新发送到用于将接口 IP 地址转换为全局 IP 地址的 NAT 或 PAT 语句中所定义的全局 IP 地址。

检查 ESXi 主机 BIOS

开始之前

要在 VMware 上部署带 SR-IOV 接口的 threat defense virtual，需要支持和启用虚拟化。VMware 提供了几种验证虚拟化支持的方法，包括其在线 SR-IOV 支持兼容性指南以及可下载的 CPU 识别实用程序（检测虚拟化处于启用还是禁用状态）。

另外，您还可以通过登录到 ESXi 主机来确定是否在 BIOS 中启用了虚拟化。

过程

步骤 1 使用下列方法之一登录到 ESXi Shell：

- 如果您可以直接访问主机，请按 Alt+F2 打开计算机物理控制台的登录页面。
- 如果您正在远程连接主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。

步骤 2 输入主机识别的用户名和密码。

步骤 3 运行以下命令：

```
esxcfg-info|grep "\----\HV Support"
```

- HV Support 命令的输出指示可用的虚拟机监控程序类型。有关可能值的说明如下：
- 0 - VT/AMD-V 表示该支持对于此硬件不可用。

- 1 - VT/AMD-V 表示 VT 或 AMD-V 可能可用，但此硬件不支持它们。
- 2 - VT/AMD-V 表示 VT 或 AMD-V 可用，但目前在 BIOS 中未启用。
- 3 - VT/AMD-V 表示 VT 或 AMD-V 在 BIOS 中已启用，并且可以使用。

```
~ # esxcfg-info|grep "\----\HV Support"
         |----HV Support.........................3
```

值 3 表示支持并启用虚拟化。

下一步做什么

在主机物理适配器上启用 SR-IOV。

在主机物理适配器上启用 SR-IOV

在将虚拟机连接到虚拟功能之前，请使用 vSphere Web 客户端启用 SR-IOV，并设置主机上的虚拟功能数量。

开始之前

- 请确保已安装兼容 SR-IOV 的网络接口卡 (NIC)；请参阅系统要求，第 5 页。

过程

步骤 1 在 vSphere Web 客户端中，导航到要启用 SR-IOV 的 ESXi 主机。

步骤 2 在**管理 (Manage)** 选项卡上，点击**网络 (Networking)** 并选择**物理适配器 (Physical adapters)**。

您可以查看 SR-IOV 属性，以了解物理适配器是否支持 SR-IOV。

步骤 3 选择物理适配器，然后点击**编辑适配器设置 (Edit adapter settings)**。

步骤 4 在 SR-IOV 下，从**状态 (Status)** 下拉菜单中选择**启用 (Enabled)**。

步骤 5 在**虚拟功能数量 (Number of virtual functions)** 文本框中，键入要为该适配器配置的虚拟功能数目。

注释
我们建议您对每个接口使用的 VF 数量**不要**超过 1 个。如果与多个虚拟功能共享物理接口，可能会出现性能下降。

步骤 6 点击**确定 (OK)**。

步骤 7 重启 ESXi 主机。

虚拟功能在由物理适配器项表示的 NIC 端口上将变为活动状态。它们显示在主机**设置 (Settings)**选项卡的“PCI 设备”(PCI Devices) 列表中。

下一步做什么

- 创建一个标准 vSwitch 来管理 SR-IOV 功能和配置。

创建 vSphere 交换机

创建一个 vSphere 交换机来管理 SR-IOV 接口。

过程

步骤 1 在 vSphere Web 客户端中，导航至 ESXi 主机。

步骤 2 在**管理 (Manage)** 下，选择**网络 (Networking)**，然后选择**虚拟交换机 (Virtual switches)**。

步骤 3 点击**添加主机网络 (Add host networking)**图标，即带有加号 (+) 的绿色地球仪图标。

步骤 4 选择**标准交换机的虚拟机端口组 (Virtual Machine Port Group for a Standard Switch)** 连接类型，然后点击**下一步 (Next)**。

步骤 5 选择**新建标准交换机 (New standard switch)**，然后点击**下一步 (Next)**。

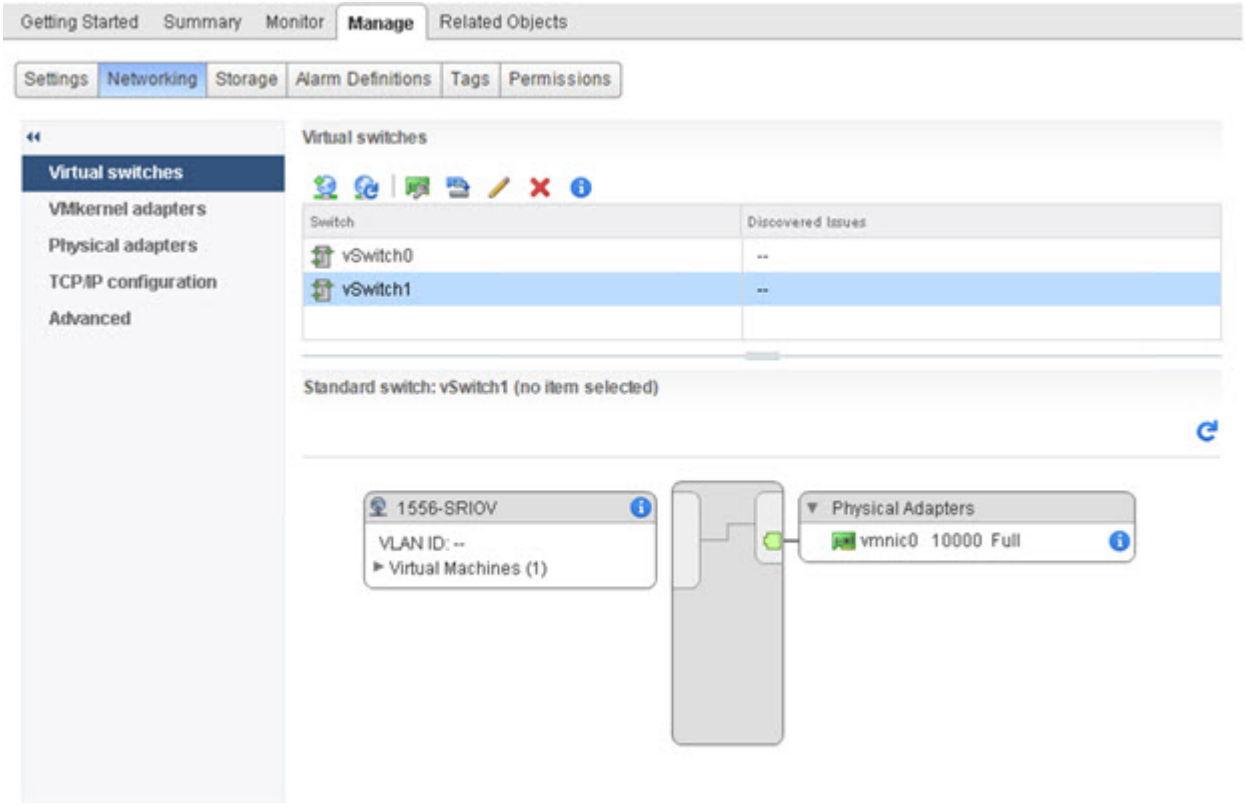
步骤 6 将物理网络适配器添加到新的标准交换机中。

a) 在分配的适配器下，点击绿色加号 (+) 以**添加适配器**。
b) 从列表中为 SR-IOV 选择相应的网络接口。例如 Intel(R) 82599 万兆位双端口网络连接。
c) 从**故障转移顺序组 (Failover order group)**下拉菜单中，选择**活动适配器 (Active adapters)**。
d) 点击**确定 (OK)**。

步骤 7 为该 SR-IOV vSwitch 输入一个**网络标签**，然后点击**下一步 (Next)**。

步骤 8 在**准备完成 (Ready to complete)** 页面上查看您的选择，然后点击**完成 (Finish)**。

图 2: 已连接 *SR-IOV* 接口的新 *vSwitch*



下一步做什么

- 查看虚拟机的兼容级别。

升级虚拟机的兼容级别

兼容级别决定可用于虚拟机的虚拟硬件，它们与主机上可用的物理硬件相对应。threat defense virtual VM 的硬件级别需要达到 10 级或更高级别。这样才能将 SR-IOV 直通功能暴露给 threat defense virtual。以下操作程序可立即将 threat defense virtual 升级到最新支持的虚拟硬件版本。

有关虚拟机硬件版本和兼容性的信息，请参阅 vSphere 虚拟机管理文档。

过程

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 threat defense virtual 计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 threat defense virtual机。

步骤 3 关闭所选的虚拟机。

步骤 4 右键点击该 threat defense virtual，并依次选择**操作 (Actions)** > **所有 vCenter 操作 (All vCenter Actions)** > **兼容性 (Compatibility)** > **升级 VM 兼容性 (Upgrade VM Compatibility)**。

步骤 5 点击**是 (Yes)** 以确认升级。

步骤 6 为虚拟机兼容性选择 **ESXi 5.5 及更高版本 (ESXi 5.5 and later)**选项。

步骤 7 （可选）选择**仅在正常访客操作系统关闭后升级 (Only upgrade after normal guest OS shutdown)**。

所选虚拟机将升级为您选择的相应硬件版本的兼容性设置，并且虚拟机的**摘要**选项卡中将更新为新的硬件版本。

下一步做什么

- 通过 SR-IOV 直通网络适配器将该 threat defense virtual 与虚拟功能关联。

将 SR-IOV NIC 分配给 Threat Defense Virtual

为了确保 threat defense virtual机和物理 NIC 可以交换数据，您必须将 threat defense virtual 与一个或多个用作 SR-IOV 直通网络适配器的虚拟功能相关联。以下操作程序说明如何使用 vSphere Web 客户端将 SR-IOV NIC 分配给 threat defense virtual机。

过程

步骤 1 从 vSphere Web 客户端登录到 vCenter 服务器。

步骤 2 找到要修改的 threat defense virtual计算机。

a) 选择数据中心、文件夹、集群、资源池或主机，然后点击**相关对象 (Related Objects)** 选项卡。

b) 点击**虚拟机 (Virtual Machines)**，并从列表中选择 threat defense virtual机。

步骤 3 在虚拟机的**管理 (Manage)**选项卡上，依次选择**设置 (Settings)** > **VM 硬件 (VM Hardware)**。

步骤 4 点击**编辑 (Edit)**，然后选择**虚拟硬件 (Virtual Hardware)** 选项卡。

步骤 5 从**新建设备 (New device)** 下拉菜单中，选择**网络 (Network)**，然后点击**添加 (Add)**。

系统将显示**新建网络 (New Network)** 界面。

步骤 6 展开**新建网络 (New Network)** 部分，然后选择可用的 SRIOV 选项。

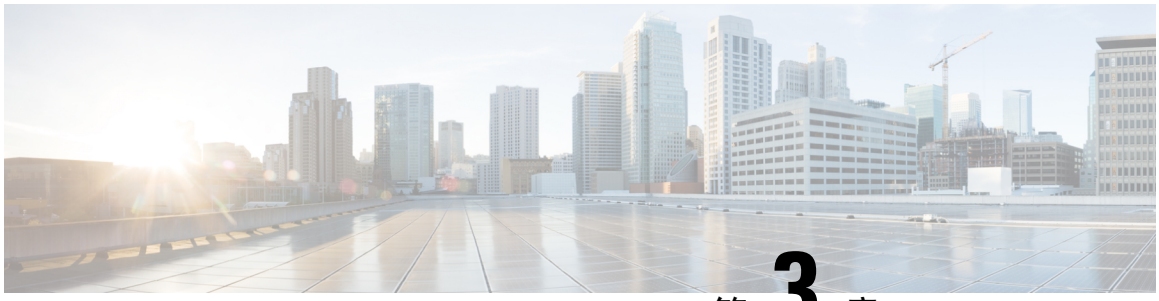
步骤 7 从**适配器类型 (Adapter Type)**下拉菜单中选择 **SR-IOV 直通 (SR-IOV passthrough)**。

步骤 8 从**物理功能 (Physical function)** 下拉菜单中，选择与直通虚拟机适配器相对应的物理适配器。

步骤 9 接通虚拟机电源。

接通虚拟机电源后，ESXi 主机将从物理适配器中选择一个可用的虚拟功能，并将其映射到 SR-IOV 直通适配器。主机将验证虚拟机适配器和底层虚拟功能的所有属性。

注释 由于混杂模式限制，某些使用 SR-IOV 驱动程序的 Intel 网络适配器（例如 Intel X710 或 82599）不支持在 threat defense virtual 上将 SR-IOV 接口用作被动接口。在此情况下，请使用支持此功能的网络适配器。有关英特尔网络适配器的详细信息，请参阅英特尔以太网产品。



第 3 章

在 KVM 上部署 Threat Defense Virtual

本章介绍将 threat defense virtual 部署到 KVM 环境的程序。

概述

KVM 是适用于基于 x86 硬件的 Linux 且包含虚拟化扩展（例如英特尔 VT）的完全虚拟化解决方案。其中包含可加载的　内核模块 kvm.ko（用于提供核心虚拟化基础设施）和一个处理器特定模块（例如 kvm-intel.ko）。

您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

Threat Defense Virtual 智能许可的性能层

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *9:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

请参阅 *Cisco Secure Firewall Management Center*中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。

系统要求

有关 threat defense virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

根据所需部署的实例数量和使用要求， threat defense virtual 部署所使用的具体硬件可能会有所不同。每个 threat defense virtual 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

表 *10: Threat Defense Virtual* 设备资源要求

设置	值
性能级别	**7.0 及更高版本** threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。 • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) 请参阅 *Cisco Secure Firewall Management Center* 配置中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。

设置	值
核心和内存数	**版本 6. 4 至版本 6.7** threat defense virtual 具有可调的 vCPU 和内存资源。支持的 vCPU/内存对值有三种： • 4vCPU/8GB（默认） • 8vCPU/16GB • 12vCPU/24GB 注释 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。仅支持上述三种组合。
	6.3 及更低版本 threat defense virtual 具有固定的 vCPU 和内存资源。支持的 vCPU/内存对值只有一个： • 4vCPU/8GB 注释 不允许调整 vCPU 和内存。
硬盘调配容量	• 50 GB • 可调节设置。支持 virtio 块设备
vNIC	KVM 上的 threat defense virtual 支持以下虚拟网络适配器： • **VIRTIO** - Virtio 是 KVM 中 IO 虚拟化的主要平台，为 IO 虚拟化的虚拟机监控程序提供通用框架。主机实施是在用户空间 qemu 中，因此主机中不需要驱动程序。 • **IXGBE-VF** - ixgbe-vf (10 Gbit/s) 驱动程序支持只能在支持 SR-IOV 的内核上激活的虚拟功能设备。SR-IOV 需要正确的平台和操作系统支持；有关详细信息，请参阅“对 SR-IOV 的支持”。

准则和限制

- 需要两个管理接口和两个数据接口来启动。

注释 threat defense virtual 默认配置将管理接口和内部接口置于同一子网上。

- 支持 virtIO 驱动程序。
- 支持 SR-IOV 的 ixgbe-vf 驱动程序。
- 支持共计 11 个接口

- threat defense virtual 的默认配置假设您将管理接口和内部接口置于**同一子网**，并且管理地址使用内部地址作为访问互联网的网关（经过外部接口）。
- threat defense virtual 首次启动时，必须启用至少四个接口。如果没有四个接口，您的系统将无法部署
- threat defense virtual 支持共计 11 个接口 - 1 个管理接口、1 个保留供内部使用的接口，以及最多 9 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：
  - 管理接口 (1)（必需）

注释 您可以选择为 管理中心 管理配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。请注意，在高可用性部署中，不支持从数据接口进行 管理中心 访问。有关为 管理中心 访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

  - 保留供内部使用 (2)（必需）
  - 外部接口 (3)（必需）
  - 内部接口 (4)（必需）
  - 数据接口 (5-11)（可选）

请查看 threat defense virtual 接口的以下网络适配器、源网络和目标网络的对应关系：

表 *11:* 源网络与目标网络的映射

网络适配器	源网络	目标网络	功能
vnic0*	Management0-0	Management0/0	管理
vnic1	保留供内部使用。	保留供内部使用。	保留供内部使用。
vnic2	GigabitEthernet0-0	GigabitEthernet0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet0/1	内部

网络适配器	源网络	目标网络	功能
*重要信息。连接到同一子网。			

- 不支持克隆虚拟机。
- 对于控制台访问，通过 telnet 支持终端服务器。
- 要在 KVM 上创建具有 IPv6 支持配置的 vNIC，您必须为每个包含 IPv6 配置参数的接口创建一个 XML 文件。您可以使用命令 **virsh net-create** <<*interface configuration XML file name*>> 来安装具有 IPV6 网络协议配置的 vNIC。

  对于每个接口，您可以创建以下 XML 文件：

  - 管理接口 - *mgmt-vnic.xml*
  - 内部接口 - *inside-vnic.xml*
  - 外部接口 - *outside-vnic.xml*

  示例：

  使用 IPv6 配置为管理接口创建 XML 文件。

```
<network>
            <name>mgmt-vnic</name>
            <bridge name='mgmt-vnic' stp='on' delay='0' />
            <ip family='ipv6' address='2001:db8::a111:b220:0:abcd' prefix='96'/>
        </network>
```

  同样，您也必须为其他接口创建 XML 文件。

  您可以通过运行以下命令来验证 KVM 上安装的虚拟网络适配器。

```
virsh net-list
         brctl show
```

CPU 模式

KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

集群

在 KVM 上部署的 Threat Defense Virtual 实例支持集群。有关详细信息，请参阅私有云中 Threat Defense Virtual 的集群。

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅KVM 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

对 SR-IOV 的支持

SR-IOV 虚拟功能需要特定的系统资源。除支持 SR-IOV 功能的 PCIe 适配器之外，还需要支持 SR-IOV 的服务器。

KVM 上使用 SR-IOV 接口的 Threat Defense Virtual 支持混合接口类型。您可以将 SR-IOV 或 VMXNET3 用于管理接口，并将 SR-IOV 用于数据接口。

您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。支持以下 NIC：
  - 英特尔以太网服务器适配器 X710
  - Intel 以太网服务器适配器 X520 - DA2
  - Intel 以太网服务器适配器 E810-CQDA2
    - 使用 NVM 实用程序工具在 Intel® 网络适配器 E810 上更新固件（NVM 映像）和网络驱动程序。非易失性内存 (NVM) 映像和网络驱动程序是一组兼容的组件，您可以在 Intel® 网络适配器 E810 上作为组合进行更新。有关 NVM 和软件兼容性矩阵的信息，请参阅 Intel® 以太网控制器 E810 数据表，以更新英特尔®网络适配器 E810 上的正确固件驱动程序。
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。
- x86_64 多核 CPU - Intel 沙桥或更高版本（推荐）。

注释 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 threat defense virtual 进行了测试。

- 核心
  - 每个 CPU 插槽至少 8 个物理核心
  - 8 个核心必须位于一个插槽中。

注释 建议通过 CPU 固定来实现完整的吞吐量。

- 请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。对于 KVM，您可以验证 SR-IOV 支持方面的 CPU 兼容性。请注意，对于 KVM 上的 threat defense virtual，我们仅支持 x86 硬件。

使用 ixgbe-vf 接口的限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 threat defense virtual 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障转移通过从主用设备向备用设备传送 IP 地址的方式运行。

注释 此限制也适用于 i40e-vf 接口。

- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。
- 在故障转移设置中，当配对的 threat defense virtual（主设备）发生故障时，备用 threat defense virtual 设备将接管主设备的角色，并使用备用 threat defense virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，threat defense virtual 会向同一网络上的其他设备发送免费地址解析协议 (ARP) 更新，以通告接口 IP 地址的 MAC 地址更改。但是，由于与这些类型的接口不兼容，因此不会将免费 ARP 更新发送到用于将接口 IP 地址转换为全局 IP 地址的 NAT 或 PAT 语句中所定义的全局 IP 地址。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

前提条件

- 从 Cisco.com 下载 threat defense virtual qcow2 文件并将其放在 Linux 主机上：

  https://software.cisco.com/download/navigator.html

注释 需要 Cisco.com 登录信息和思科服务合同。

- 本文档出于示例部署目的，假设您使用 Ubuntu 14.0418.04 LTS。在 Ubuntu 18.04 LTS 主机之上安装以下软件包：
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst

  - virsh tools
  - genisoimage

- 性能受主机及其配置的影响。通过调整主机，您可以最大化 KVM 上的 threat defense virtual吞吐量。有关通用的主机调整概念，请参阅网络功能虚拟化：具备 Linux 和 Intel 架构的宽带远程访问服务器的服务质量。
- Ubuntu 18.04 LTS 的有用优化包括以下各项：
  - macvtap - 高性能 Linux 网桥；您可以使用 macvtap，而不是 Linux 网桥。您必须配置特定设置才能使用 macvtap，而不是 Linux 网桥。
  - 透明大页 - 增加内存页面大小，在 Ubuntu 18.04 中默认开启。
  - 禁用超线程 - 用于将两个 vCPU 减少到一个单核。
  - txqueuelength - 用于将默认 txqueuelength 增加到 4000 个数据包并减少丢包率。
  - 固定 - 用于将 qemu 和 vhost 进程固定到特定 CPU 内核；在某些情况下，固定可显著提高性能。
- 有关优化基于 RHEL 的分布的信息，请参阅《Red Hat Enterprise Linux6 虚拟化调整和优化指南》。
- 有关 KVM 和系统兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。
- 您可以使用以下方法来验证虚拟机是否正在运行 KVM：
  - 运行 **lsmod** 以列出 Linux 内核中的模块。如果 KVM 正在运行，则会显示以下输出来指示 KVM：

    root@kvm-host:~$ lsmod | grep kvm

    kvm_intel 123675 0

    kvm 257361 1 kvm_intel

- 如果目标 VM 上不存在 **ls -l /dev/kvm** ，则您可能正在运行 **qemu**，而没有利用 KVM 硬件辅助功能。

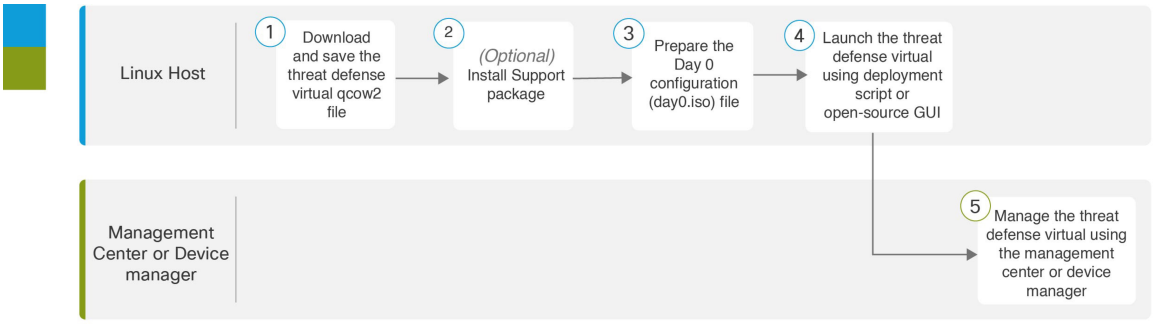
  root@kvm-host:~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm
- 运行以下命令，检查主机是否支持 KVM：

  root@kvm-host:~$ sudo kvm-ok
- 您也可以使用 KVM 加速。

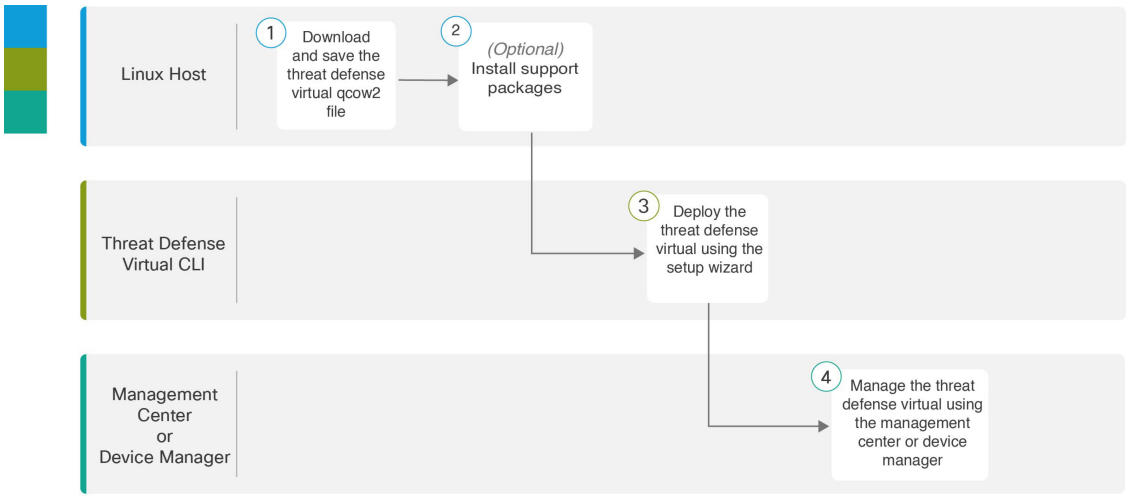
端到端程序

以下流程图说明了使用 Day 0 配置文件在 KVM 实例上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	前提条件，第 50 页：下载 threat defense virtual qcow2 文件并将其保存在 Linux 主机上。
2	Linux 主机	前提条件，第 50 页：安装支持软件包。
3	Linux 主机	准备 Day 0 配置文件
4	Linux 主机	启动 threat defense virtual： • 使用部署脚本启动 • 使用图形用户界面 (GUI) 进行启动
5	管理中心	使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

以下流程图说明了在不使用 Day 0 配置文件的情况下在 KVM 实例上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	前提条件，第 50 页：下载 threat defense virtual qcow2 文件并将其保存在 Linux 主机上。
2	Linux 主机	前提条件，第 50 页：安装支持软件包。
3	Threat Defense Virtual CLI	在没有 Day 0 配置文件的情况下启动：使用设置向导部署 threat defense virtual。
4	管理中心	使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

准备 Day 0 配置文件

在启动 threat defense virtual之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时装载和读取的 day0.iso 文件。

重要事项 该 day0.iso 文件必须在首次启动期间可用。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 threat defense virtual 设备的整个初始设置。可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。

- 管理模式；请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

  您可以将**本地管理**设置为**是**，或者输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的信息。对于您未使用的管理模式，保留字段为空。

- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地 设备管理器 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 设备管理器 配置透明防火墙模式接口。

- 使设备可以在管理网络上进行通信的网络设置。

- 部署类型，您可以在其中指定是在集群模式还是独立模式下部署 threat defense virtual。

如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置系统所需的设置；有关更多信息，请参阅在没有 Day 0 配置文件的情况下启动，第 59 页。

注释 我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

SUMMARY STEPS

1. 在名为“day0-config”的文本文件中输入 threat defense virtual的 CLI 配置。添加网络设置和关于管理 管理中心 的信息。
2. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：
3. 为每个要部署的 设备管理器 重复创建唯一的默认配置文件。

DETAILED STEPS

过程

步骤 1 在名为“day0-config”的文本文件中输入 threat defense virtual的 CLI 配置。添加网络设置和关于管理 管理中心 的信息。

示例：

在 Day 0 配置文件的 **ManageLocally** 中输入 **Yes** 以使用本地 设备管理器；输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的值。对于您未使用的管理选项，将这些字段留空。

步骤 2 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

示例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

或

示例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

步骤 3 为每个要部署的 设备管理器 重复创建唯一的默认配置文件。

下一步做什么

- 如果使用 virt-install，请在 virt-install 命令中添加以下行：

```
--disk path=/home/user/day0.iso,format=iso,device=cdrom \
```

- 如果使用 virt-manager，则可以使用 virt-manager GUI 创建虚拟 CD-ROM；请参阅使用图形用户界面 (GUI) 进行启动，第 57 页。

启动 Threat Defense Virtual

使用部署脚本启动

使用基于 virt-install 的部署脚本启动 threat defense virtual。

请注意，您可以通过选择适合您环境的最佳访客缓存模式来优化性能。正在使用的缓存模式不仅会影响到是否发生数据丢失，还会影响到磁盘性能。

每个 KVM 访客磁盘接口都可以指定以下缓存模式之一：*writethrough*、*writeback*、*none*、*directsync* 或 *unsafe*。*writethrough* 提供读取缓存。*writeback* 提供读取和写入缓存。*directsync* 会绕过主机页面缓存。*unsafe* 可能会缓存所有内容，并忽略来自访客的刷新请求。

- 当主机遇到突然断电时，*cache=writethrough* 有助于降低 KVM 访客计算机上的文件损坏。我们建议使用 *writethrough* 模式。
- 但是，由于 *cache=writethrough* 的磁盘 I/O 写入次数高于 *cache=none*，所以该模式也会影响磁盘性能。
- 如果删除了 *--disk* 选项上的 cache 参数，则默认值为 *writethrough*。
- 未指定缓存选项还有可能大幅减少创建虚拟机所需的时间。这是因为，一些较旧的 RAID 控制器的磁盘缓存能力较差。因此，禁用磁盘缓存 (*cache=none*)，从而使用默认值 *writethrough*，有助于确保数据完整性。
- 从版本 6.4 开始，threat defense virtual 随可调的 vCPU 和内存资源一起部署。在 6.4 版之前，部署的 threat defense virtual 具有固定配置 4VCPU/8GB 设备。请参阅下表，了解每个 threat defense virtual 平台大小的 --vcpus 和 --ram 参数所支持的值。

表 *12: virt-install* 支持的 *vCPU* 和内存参数

--vcpus	--ram	Threat Defense Virtual 平台规模
4	8192	4vCPU/8GB（默认）
8	16384	8vCPU/16GB

--vcpus	--ram	Threat Defense Virtual 平台规模
12	24576	12vCPU/24GB

过程

步骤 1 创建名为“virt_install_ftdv.sh”的 virt-install 脚本。

threat defense virtual虚拟机 (VM) 的名称在此 KVM 主机上的所有其他虚拟机中必须是唯一的。threat defense virtual 可支持多达 10 个网络接口。此示例使用了四个接口。虚拟 NIC 必须是 VirtIO。

注释
threat defense virtual 的默认配置假定您将管理接口、诊断接口和内部接口置于同一子网上。系统至少需要 4 个接口才能成功启动。接口到网络分配必须遵循以下顺序：

- (1) 管理接口（必需）
- (2) 保留供内部使用（必需）
- (3) 外部接口（必需）
- (4) 内部接口（必需）
- (5)（可选）数据接口 - 最多 6 个

示例：

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset \
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --disk path=<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
   --force
```

步骤 2 运行 virt_install 脚本：

示例：

```
/usr/bin/virt_install_ftdv.sh
```

```
Starting install...
Creating domain...
```

此时将出现一个窗口，其中显示虚拟机的控制台。您可以看到虚拟机正在启动。启动虚拟机需要几分钟时间。一旦虚拟机停止启动，您便可以从控制台屏幕发出 CLI 命令。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理 (Manage Locally)**选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

使用图形用户界面 (GUI) 进行启动

有多个开源选项可用于通过 GUI 来管理 KVM 虚拟机。以下程序使用 virt-manager（也称为虚拟机管理器）启动 threat defense virtual。Virt-manager 是用于创建和管理访客虚拟机的图形化工具。

注释 KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

过程

步骤 1 启动 virt-manager（**应用** > **系统工具** > **虚拟机管理器**）。

系统可能要求您选择虚拟机监控程序和/或输入您的 root 口令。

步骤 2 点击左上角的按钮，打开**新建虚拟机 (New VM)** 向导。

步骤 3 输入虚拟机的详细信息：

a) 对于操作系统，选择**导入现有的磁盘映像 (Import existing disk image)**。

此方法允许您向其导入磁盘映像（包含预安装的可启动操作系统）。

b) 点击**继续 (Forward)** 继续操作。

步骤 4 加载磁盘映像：

a) 点击**浏览...(Browse...)**，选择映像文件。

b) 选择通用 *(Generic)* 作为**操作系统类型 (OS type)**。

c) 点击**继续 (Forward)** 继续操作。

步骤 5 配置内存和 CPU 选项：

重要事项

threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

请参阅下表，了解每个 threat defense virtual 平台的 --vcpus 和 --ram 参数所支持的性能层和值。

表 *13:* 虚拟机管理器支持的 ***vCPU*** 和内存参数

CPU	内存	**Threat Defense Virtual** 平台规模
4	8192	4vCPU/8GB（默认）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

a) 针对 threat defense virtual 平台大小设置**内存 (RAM)** 参数。
b) 针对 threat defense virtual 平台大小设置对应的 **CPU** 参数。
c) 点击**继续 (Forward)**继续操作。

步骤 6 选中**安装前自定义配置 (Customize configuration before install)** 框，指定一个**名称 (Name)**，然后点击**完成 (Finish)**。

执行此操作将会打开另一个向导，您可以在其中添加、删除和配置虚拟机的硬件设置。

步骤 7 修改 CPU 配置：

从左侧面板中，选择**处理器 (Processor)**，然后选择**配置 (Configuration)** > **复制主机 CPU 配置 (Copy host CPU configuration)**。

这会将物理主机的 CPU 型号和配置应用于您的 VM。

步骤 8 配置虚拟磁盘：

a) 从左侧面板中，选择**磁盘 1 (Disk 1)**。
b) 选择**高级选项 (Advanced options)**。
c) 将**磁盘总线**设为 *Virtio*。
d) 将**存储格式**设为 *qcow2*。

步骤 9 配置串行控制台：

a) 从左侧面板中，选择**控制台 (Console)**。
b) 选择**删除 (Remove)**，删除默认的控制台。
c) 点击**添加硬件 (Add Hardware)**，添加一台串行设备。
d) 对于**设备类型 (Device Type)**，选择 *TCP net* 控制台 *(tcp) (TCP net console [tcp])* 。
e) 对于**模式 (Mode)**，选择服务器模式（绑定）*(Server mode [bind])*。
f) 对于**主机 (Host)**，输入 **0.0.0.0** 作为 IP 地址，然后输入唯一的**端口 (Port)** 号。
g) 选中**使用 Telnet** 框。
h) 配置设备参数。

步骤 10 配置看门狗设备，在 KVM 访客挂起或崩溃时自动触发某项操作：

a) 点击**添加硬件 (Add Hardware)**，添加一台看门狗设备。

b) 对于**型号 (Model)**，选择默认值 *(default)*。
c) 对于**操作 (Action)**，选择强制重置访客 *(Forcefully reset the guest)*。

步骤 11 配置至少 4 个虚拟网络接口。

点击**添加硬件 (Add Hardware)** 以添加接口，然后选择 **macvtap** 或指定共享设备名称（使用网桥名称）。

注释
KVM 上的 threat defense virtual 支持共计 11 个接口 - 1 个管理接口、1 个保留供内部使用的接口，以及最多 9 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

vnic0 - 管理接口（必需）

vnic1—保留供内部使用（必需）

vnic2 - 外部接口（必需）

vnic3 - 内部接口（必需）

vnic4-10 - 数据接口（可选）

重要事项
请确保将 vnic0 和 vnic3 映射到同一子网。

步骤 12 如果使用 Day 0 配置文件进行部署，则为 ISO 创建虚拟 CD-ROM：
a) 点击**添加硬件(Add Hardware)**。
b) 选择**存储 (Storage)**。
c) 点击**选择托管或其他现有存储 (Select managed or other existing storage)**，然后浏览至 ISO 文件的位置。
d) 对于**设备类型 (Device type)**，选择 *IDE CDROM*。

步骤 13 配置虚拟机的硬件后，点击**应用 (Apply)**。

步骤 14 点击**开始安装 (Begin installation)**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理 (ManageLocally)**选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

在没有 Day 0 配置文件的情况下启动

由于 threat defense virtual 设备没有 Web 界面，如果您在没有 Day 0 配置文件的情况下进行部署，必须使用 CLI 来设置虚拟设备。

首次登录新部署的设备时，必须阅读并接受 EULA。然后，请按照设置提示更改管理员密码，并配置设备的网络设置和防火墙模式。

按照设置提示操作时，如遇单选问题，选项会列在括号内，例如 (*y/n*)。默认值会列在方括号内，例如 [*y*]。按 Enter 键确认选择。

注释 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。

过程

步骤 1 打开 threat defense virtual的控制台。

步骤 2 在 **firepower login** 提示符下，使用默认凭据（**username** *admin*，**password** *Admin123*）登录。

步骤 3 当 threat defense virtual系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式（需要进行本地管理）

步骤 4 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

步骤 5 根据提示完成系统配置。

步骤 6 当控制台返回到 **#** 提示符时，验证设置是否成功。

步骤 7 关闭 CLI。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

故障排除

本节提供与虚拟机上的 KVM 部署相关的一些基本故障排除步骤。

验证您的虚拟机是否正在运行 KVM

您可以使用以下方法来验证虚拟机是否正在运行 KVM：

- 运行 **lsmod** 命令以列出 Linux 内核中的模块。如果 KVM 正在运行，则会显示以下输出来指示 KVM：

  root@kvm-host:~$ lsmod | grep kvm

  kvm_intel 123675 0

  kvm 257361 1 kvm_intel

- 如果目标 VM 上不存在 **ls -l /dev/kvm** 命令，则您可能正在运行 **QEMU**，而没有利用 KVM 硬件辅助功能。

  root@kvm-host:~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm

- 运行以下命令，检查主机是否支持 KVM：

  root@kvm-host:~$ sudo kvm-ok

- 您也可以使用 KVM 加速。

部署 Threat Defense Virtual 时遇到启动循环

如果您的虚拟机遇到启动循环，则必须确保以下事项：

- 确保部署具有至少 8 GB 内存的 VM。
- 确保部署具有至少 4 个接口的 VM。
- 确保部署具有至少 4 个 vCPU 的 VM。
- 验证 QEMU 进程是否正在使用服务器类 CPU，例如 SandyBridge、IvyBridge、Haswell 等。使用命令 **ps -edaf | grep qemu** 来检查进程参数。

部署 Management Center Virtual 时遇到启动循环

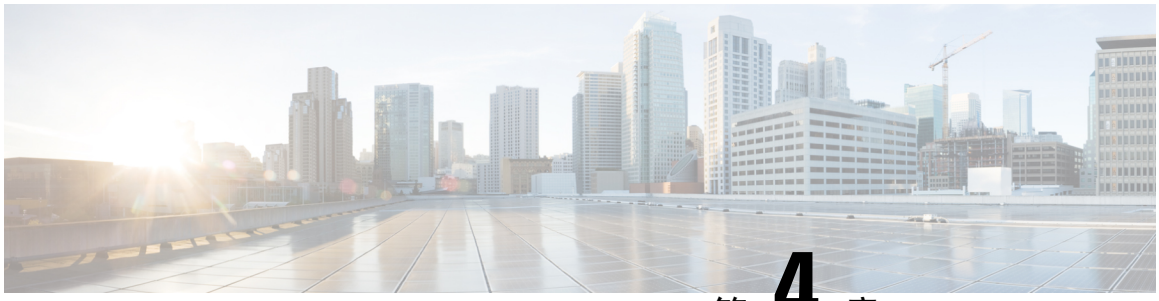
如果您的虚拟机遇到启动循环，则必须确保以下事项：

- 确保部署的 VM 至少具有 28 GB 内存。
- 确保部署具有至少 4 个接口的 VM。
- 确保部署具有至少 4 个 vCPU 的 VM。
- 验证 QEMU 进程是否正在使用服务器类 CPU，例如 SandyBridge、IvyBridge、Haswell 等。使用命令 **ps -edaf | grep qemu** 来检查进程参数。

部署后故障排除

您可以在 threat defense virtual 上运行以下命令来检查问题，以捕获日志进行调试：**system generate-troubleshoot <space> ALL**

或者，使用 **system generate-troubleshoot <space>**，后跟问号 **(?)** 或 **Tab** 按钮以查看可能的选项或命令。



第 4 章

在 AWS 上部署 Threat Defense Virtual

本章介绍如何从 AWS 门户部署 threat defense virtual。

概述

AWS 是一种公共云环境。threat defense virtual在以下实例类型的 AWS 环境中作为访客运行。

表 *14:* 系统要求

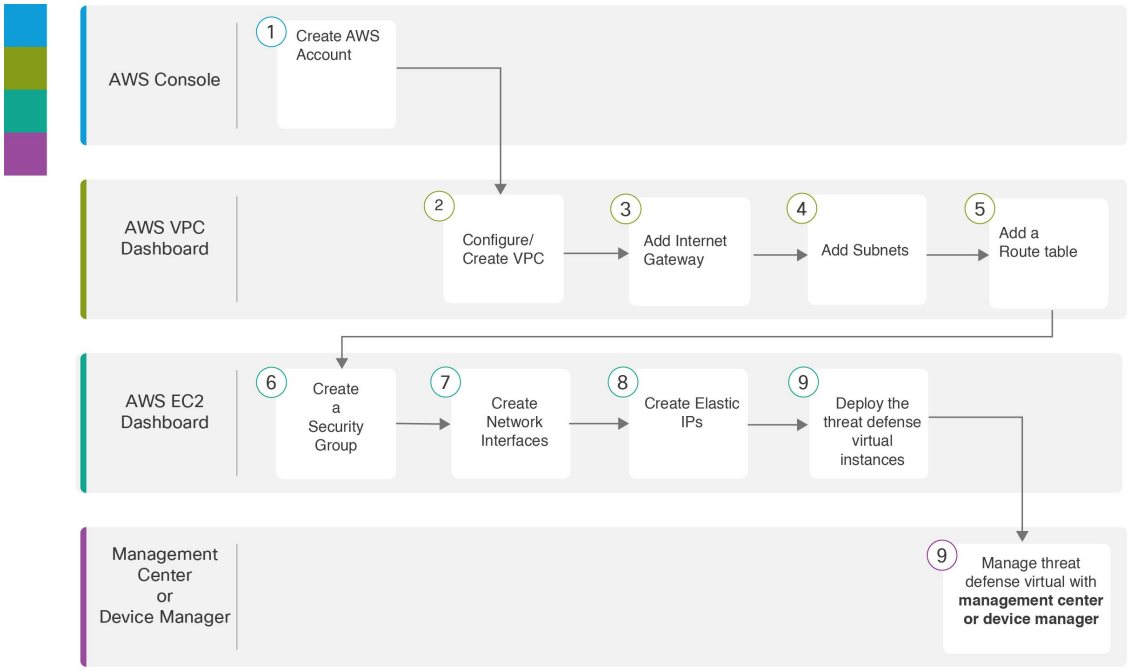
实例类型	Threat Defense Virtual	vCPU	内存 (GB)	最大接口数
c5a.xlarge	7.1.0 或更高版本	4	8	4
c5a.2xlarge		8	16	4
c5a.4xlarge		16	32	8
c5ad.xlarge		4	8	4
c5ad.2xlarge		8	16	4
c5ad.4xlarge		16	32	8
c5d.xlarge		4	8	4
c5d.2xlarge		8	16	4
c5d.4xlarge		16	32	8
c5n.xlarge		4	10.5	4
c5n.2xlarge		8	21	4
c5n.4xlarge		16	42	8
m5n.xlarge		4	16	4
m5n.2xlarge		8	32	4
m5n.4xlarge		16	64	8
m5zn.xlarge		4	16	4
m5zn.2xlarge		8	32	4
c5. xlarge	6.6.0 或更高版本	4	8	4
c5.2xlarge		8	16	4
c5.4xlarge		16	32	8
c4.xlarge	6.4.0 或更高版本	4	7.5	4
c3.xlarge		4	7.5	4

注释 Threat Defense Virtual 不支持通过调整实例大小来更改实例类型。您只能使用全新的部署来部署具有不同实例大小的 Threat Defense Virtual。

有关 aws 市场上列出的 NGFWv 支持的 EC2 实例类型的信息，请参阅 https://aws.amazon.com/marketplace/pp/prodview-p2336sqyya34e#pdp-overview。

端到端程序

以下流程图说明了在 Amazon Web 服务 (AWS) 上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	AWS 控制台	www.amazon.com：在 AWS 控制台中创建用户账户。
2	AWS VPC 控制面板	创建 VPC：创建和配置 AWS 账户专用的 VPC。
3	AWS VPC 控制面板	添加互联网网关：添加互联网网关以控制VPC与互联网的连接。
4	AWS VPC 控制面板	添加子网：将子网添加到 VPC。
5	AWS VPC 控制面板	添加路由表：将路由表连接到为 VPC 配置的网关。

	工作空间	步骤
6	AWS EC2 控制面板	创建安全组：创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。
7	AWS EC2 控制面板	创建网络接口：您可以使用静态 IP 地址为 threat defense virtual 创建网络接口。
8	AWS EC2 控制面板	创建弹性 IP：弹性 IP 地址是用于远程访问 threat defense virtual 及其他实例的保留公共 IP 地址。
9	AWS EC2 控制面板	部署 Threat Defense Virtual：从 AWS 门户部署 threat defense virtual。
10	管理中心或设备管理器	管理 threat defense virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

AWS 解决方案概述

AWS 是由 Amazon.com 提供并构成云计算平台的一系列远程计算服务（也称为 Web 服务）。这些服务遍布全球 11 个地区。通常，在部署 Cisco Secure Firewall Management Center Virtual（之前称为 Firepower Management Center Virtual）和 threat defense virtual 时，您应该会熟悉以下 AWS 服务：

- Amazon 弹性计算云 (EC2) - 使您能够通过租用虚拟计算机，在 Amazon 数据中心启动和管理自己的应用和服务（例如防火墙）的 Web 服务。
- Amazon 虚拟私有云 (VPC) - 使您能够配置 Amazon 公共云中的隔离专用网络的 Web 服务。您可以在 VPC 内运行自己的 EC2 实例。
- Amazon 简单存储服务 (S3) - 提供数据存储基础设施的 Web 服务。

您可以在 AWS 上创建账户，设置 VPC 和 EC2 组件（使用 AWS 向导或手动配置）， 并选择 Amazon 系统映像 (AMI) 实例。AMI 是一种模板，其中包含启动您的实例所需的软件配置。

Note AMI 映像在 AWS 环境之外不可下载。

前提条件

- 一个 AWS 账户。您可以在 http://aws.amazon.com/ 创建一个。
- 需要 SSH 客户端（例如，Windows 上的 PuTTY 或 macOS 上的终端）才能访问 threat defense virtual 控制台。
- 思科智能账户。您可以在 Cisco 软件中心创建一个https://software.cisco.com/
- 许可 threat defense virtual。

  Secure Firewall Management Center

- 所有安全服务的许可证授权均在 管理中心中配置。
- 有关如何管理许可证的更多信息，请参阅《Cisco Secure Firewall Management Center 配置指南》中的“系统许可”。

Cisco Secure Firewall 设备管理器

- 配置 Cisco Secure Firewall 设备管理器 安全服务的性能级许可授权。
- 有关如何管理许可证的详细信息，请参阅 Threat Defense Virtual 许可。

- Threat Defense Virtual 接口要求：
  - 管理接口 (2) - 一个用于将 threat defense virtual 连接到 管理中心，另一个留作内部使用；无法用于直通流量。

    您可以选择为 管理中心 管理配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。请注意，在高可用性部署中，不支持从数据接口进行 管理中心 访问。有关为 管理中心 访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。
  - 流量接口 (2) - 用于将 threat defense virtual 连接到内部主机和公共网络。
- 通信路径：
  - 通过公共/弹性 IP 地址访问 threat defense virtual。

支持的软件平台

threat defense virtual Auto Scale 解决方案适用于 管理中心 管理的 threat defense virtual，与软件版本无关。《Cisco Secure Firewall Threat Defense 兼容性指南》提供思科软件和硬件兼容性，包括操作系统和托管环境要求。

- 《Cisco Firewall Management Center Virtual 兼容性指南》表列出 AWS 上 Management Center Virtual 的兼容性和虚拟托管环境要求。
- 《Cisco Secure Firewall Threat Defense Virtual 兼容性指南》表列出 AWS 上 threat defense virtual 的兼容性和虚拟托管环境要求。

Note 为了部署 AWS Auto Scale 解决方案，AWS 上 threat defense virtual 的最低支持版本是版本 6.4。管理中心 必须至少运行版本 6.6+，才能使用基于内存的扩展。

准则和限制

支持的功能

- 在虚拟私有云 (VPC) 中部署
- 增强型联网 (SR-IOV)。
- 从 Amazon Marketplace 部署
- L3 网络的部署。
- 路由模式（默认）。
- ERSPAN 被动模式。
- 集群（7.2 及更高版本）。有关详细信息，请参阅公共云中 Threat Defense Virtual 的集群。
- Amazon CloudWatch 记录的运行状况监控指标
- 巨型帧
- 快照（7.2 及更高版本）
- IPv6

不支持的功能

- 克隆
- 透明、内联和被动模式
- AWS 上的 Geneve 单臂设置不支持传输层安全 (TLS) 服务器身份发现。

许可

- 支持使用 Cisco 智能许可证帐户的 BYOL（自带许可证）。
- PAYG（即付即用）许可，一种基于使用的计费模式，允许客户在不购买 Cisco 智能许可的情况下运行 threat defense virtual。对于已注册的 PAYG threat defense virtual 设备，将启用所有许可的功能（恶意软件/威胁/URL 过滤/VPN 等）。这些许可功能在已注册的 管理中心 上自动标记为活动。许可的功能无法从 管理中心 编辑或修改。（版本 6.5+）

Note 在 设备管理器 模式下部署的 threat defense virtual 设备上不支持 PAYG 许可。

有关许可 threat defense virtual 设备时的准则，请参阅《防火墙管理中心管理指南》中的“许可证”一章。

Threat Defense Virtual 智能许可的性能级别

从 Threat Defense Virtual 版本 7.0.0 发布开始，threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

Table 15: 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5	4 核/8 GB	100 Mbps	50
FTDv10	4 核/8 GB	1 Gbps	250
FTDv20	4 核/8 GB	3 Gbps	250
FTDv30	8 核/16 GB	5 Gbps	250
FTDv50	12 核/24 GB	10 Gbps	750
FTDv100	16 核/34 GB	16 Gbps	10,000

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 AWS 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Threat Defense Virtual 限制

- c5.xlarge 是推荐实例；c3.xlarge 实例在不同 AWS 区域的可用性受限。
- 您必须在启动期间配置两个管理接口。
- 必须有两个流量接口和两个管理接口才能启动，总计四个接口。

Note 没有四个接口，threat defense virtual 将不会启动。

- 在 AWS 中配置流量接口时，必须禁用“更改源/目标检查”选项。
- 通过 CLI 或 管理中心 完成的任何 IP 地址（IPv4 和 IPv6）配置必须与 AWS 控制台中创建的内容一致；在部署期间应注意配置。
- 在注册 threat defense virtual 后，必须在 管理中心 上编辑并启用这些接口；请注意，IP 地址必须与 AWS 配置的接口匹配。
- 目前不支持透明/内联/被动模式。

- 要修改接口，您需要从 AWS 控制台进行更改。在 AWS 控制台上，从 管理中心 取消注册接口，然后停止使用 AWS AMI 用户界面的实例。然后，分离要更改的接口并连接新接口（请注意，您需要两个流量接口和两个管理接口才能启动）。现在，启动实例并重新注册到 管理中心。

  从 管理中心 编辑设备接口，然后修改 IP 地址（IPv4 和 IPv6）和其他参数，以便与通过 AWS 控制台所做的更改匹配。

Note IPv6 只能在双堆栈 (IPv4 + IPv6) 模式下使用。

- 在启动后无法添加接口。
- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

实例元数据数据服务 (IMDS) 服务的 Threat Defense Virtual 限制

- 默认情况下，部署在 IMDSv2 可选模式下进行。
- 例如，IMDS 模式可以随时更改。
- 在切换到 IMDSv2 Required 模式之前，请确保产品版本支持该模式，否则依赖于 IMDS 的某些服务可能会失败。
- 对于旧版本（不支持 IMDSv2），只能使用 IMDSv2 可选模式进行部署。
- 对于较新的版本（支持 IMDSv2），可在 IMDSv2 可选模式和 IMDSv2 要求模式下进行部署。但建议使用“IMDSv2 必需”模式。

配置 AWS 环境

要在 AWS 上部署 threat defense virtual，需要根据部署的特定要求和设置来配置 Amazon VPC。在大多数情况下，设置向导将引导您完成设置过程。AWS 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关详细信息，请参阅https://aws.amazon.com/documentation/gettingstarted/。

为更好地控制 AWS 设置，以下部分提供有关在启动 threat defense virtual 实例之前如何配置 VPC 和 EC2 的指南：

- 创建 VPC, on page 72
- 添加互联网网关, on page 73

- 添加子网, on page 73
- 添加路由表, on page 74
- 创建安全组, on page 75
- 创建网络接口, on page 75
- 创建弹性 IP, on page 76

准备工作

- 创建 AWS 账户。
- 确认可供 threat defense virtual 实例使用的 AMI。

创建 VPC

虚拟私有云 (VPC) 是 AWS 账户专用的虚拟网络。该网络逻辑上与 AWS 云中的其他虚拟网络相隔离。您可以在 VPC 中启动 AWS 资源，如 Management Center Virtual 和 threat defense virtual 实例。您可以配置 VPC，选择其 IP 地址范围，创建子网，并配置路由表、网络网关和安全设置。

有关为 VPC 和子网启用 IPv6 CIDR 块的信息，请参阅 AWS 文档在具有公共和专用子网的 VPC 中启用 IPv6。

Procedure

步骤 1 登录 http://aws.amazon.com/ 并选择您所在的区域。

AWS 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 点击**服务 > VPC**。

步骤 3 点击**VPC 控制面板 (VPC Dashboard) > 您的 VPC (Your VPCs)**。

步骤 4 点击**创建 VPC (Create VPC)**。

步骤 5 在**创建 VPC**对话框中输入以下信息：

a) 用于标识 VPC 的用户自定义**名称标签**。

b) IP 地址的**IPv4 CIDR 块**。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

c) IP 地址的 **IPv6 CIDR 块**。CIDR（无类别域间路由） 是 IP 地址及其关联路由前缀的紧凑表示。例如，[::/0]。

d) 在 **IPv6 CIDR 块 (IPv6 CIDR block)** 中选择 **Amazon 提供的 IPv6 CIDR 块 (Amazon-provided IPv6 CIDR block)**，以在虚拟私有云中启用 IPv6。

e) 默认的**租户**设置，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

步骤 6 点击**是，创建 (Yes, Create)** 以创建 VPC。

What to do next

Note 单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。

添加互联网网关到 VPC 中，详见下一部分。

添加互联网网关

您可以添加互联网网关以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

准备工作

- 为 Threat Defense Virtual实例创建 VPC。

Procedure

步骤 1 点击**服务 > VPC**。

步骤 2 点击 **VPC 控制面板 > 互联网网关**，然后点击**创建互联网网关**。

步骤 3 输入用户自定义的**名称标签**以标识网关，然后点击**是，创建**以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 点击**连接到 VPC** 并选择之前创建的 VPC。

步骤 6 点击**是，连接 (Yes, Attach)**，以将网关连接到 VPC。

默认情况下，在创建网关并将其连接到 VPC 之前，在 VPC 上启动的实例无法与互联网通信。

What to do next

添加子网到 VPC 中，详见下一部分。

添加子网

您可以对 Threat Defense Virtual 实例可连接的 VPC IP 地址范围进行分段。您可以根据安全和运营需要创建子网，以实现实例的分组。对于 Threat Defense Virtual，您需要创建一个管理子网和一个流量子网。

准备工作

- 为 Threat Defense Virtual实例创建 VPC。

Procedure

步骤 1 点击服务 > **VPC**。

步骤 2 点击 **VPC** 控制面板 > 子网，然后点击创建子网。

步骤 3 在创建子网对话框中输入以下信息：

a) 用于标识子网的用户自定义名称标签。

b) 子网所在的 **VPC**。

c) 此子网将驻留的可用区域。选择无首选项，由 Amazon 来选择区域。

d) IP 地址（IPv4 和 IPv6）的 **IPv4 CIDR 块**。子网 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。子网大小可以与 VPC 相等。

步骤 4 点击是，创建 **(Yes, Create)** 以创建子网。

步骤 5 如需多个子网，重复以上步骤。为管理流量创建单独的子网，根据需要为数据流量创建多个子网。

What to do next

添加路由表到 VPC 中，详见下一部分。

添加路由表

您可以将路由表连接到为 VPC 配置的网关。您还可以关联多个子网与单个路由表，但子网一次只可以关联一个路由表。

Procedure

步骤 1 点击服务 > **VPC**。

步骤 2 点击 **VPC** 控制面板 > 路由表，然后点击创建路由表。

步骤 3 输入用于标识路由表的用户自定义名称标签。

步骤 4 从下拉列表中选择将使用此路由表的 **VPC** 。

步骤 5 点击是，创建 **(Yes, Create)**以创建路由表。

步骤 6 选择刚创建的路由表。

步骤 7 点击路由 **(Routes)** 选项卡，以在详细信息窗格中显示路由信息。

步骤 8 点击编辑 **(Edit)**，然后点击添加其他路由 **(Add another route)**。

a) 在目标 **(Destination)** 列中，为所有 IPv6 流量输入 **0.0.0.0/0 或 [::/0]**。

b) 在目标列中，选择您的网关。

步骤 9 点击保存。

What to do next

创建安全组，详见下一部分。

创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。

Procedure

步骤 1 点击**服务 > EC2**。

步骤 2 点击 **EC2 控制面板 > 安全组**。

步骤 3 点击**创建安全组**。

步骤 4 在**创建安全组**对话框中输入以下信息：

a) 用于标识安全组的用户自定义**安全组名称**。

b) 此安全组的**说明**。

c) 与此安全组关联的 **VPC**。

步骤 5 配置**安全组规则**：

a) 点击**入站 (Inbound)** 选项卡，然后点击**添加规则 (Add Rule)**。

Note
如需从 AWS 外部管理 Management Center Virtual，则需要 HTTPS 和 SSH 访问权限。您应指定相应的源 IP 地址。此外，如果在 AWS VPC 内同时配置 Management Center Virtual 和 threat defense virtual，应允许专用 IP 管理子网访问权限。

b) 点击**出站**选项卡，然后点击**添加规则**以添加出站流量规则，或保留**所有流量**（作为**类型**）和**任意位置**（作为**目标**） 的默认设置。

步骤 6 点击**创建**以创建安全组。

What to do next

创建网络接口，详见下一部分。

创建网络接口

您可以使用静态 IP 地址（IPv4 和 IPv6）或 DHCP 为 threat defense virtual 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

Procedure

步骤 1 点击服务 > **EC2**。

步骤 2 点击 **EC2** 控制面板 > 网络接口。

步骤 3 点击创建网络接口 **(Yes, Create)**。

步骤 4 在创建网络接口对话框中输入以下信息：

a) 网络接口的用户自定义说明（可选）。

b) 从下拉列表中选择子网 **(Subnet)**。确保选择要创建 threat defense virtual 实例所在 VPC 的子网。

c) 输入专用 **IP** 地址。您可以使用静态 IP 地址（IPv4 和 IPv6）或自动生成 (DHCP)。

d) 选择一个或多个安全组。确保安全组已打开所有必需的端口。

步骤 5 点击创建网络接口 **(Create network interface)** 以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键点击并选择更改源/目的地址检查。

步骤 8 取消选中源/目标 **(Source/destination check)** 复选框下的启用 **(Enable)** 复选框，然后点击保存 **(Save)**。

What to do next

创建弹性 IP 地址，详见下一部分。

创建弹性 IP

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址（IPv4 和 IPv6）会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 地址是用于远程访问 threat defense virtual 及其他实例的保留公共 IP 地址。

Note 至少要为 threat defense virtual 管理接口创建弹性 IP 地址。

Procedure

步骤 1 点击服务 > **EC2**。

步骤 2 点击 **EC2** 控制面板 > 弹性 **IP**。

步骤 3 点击分配新地址 **(Allocate New Address)**。

步骤 4 根据弹性/公共 IP 地址分配需要，重复此步骤。

步骤 5 点击是，分配 **(Yes, Allocate)** 以创建弹性 IP 地址。

步骤 6 根据部署需要，重复上述步骤以创建其他弹性 IP 地址。

What to do next

部署 threat defense virtual，详见下一部分。

AWS 中 Threat Defense Virtual 的实例元数据服务 (IMDS)

实例元数据数据服务 (IMDS) 提供有关部署在 AWS 上的 Threat Defense Virtual 实例数据的信息。这些信息包括虚拟实例的网络、存储和其他数据的详细信息。这些元数据可用于自动做出配置决定（Day0 配置）和显示实例信息，如实例类型、区域等。

IMDS API 在设备启动期间从 AWS 收集 Threat Defense Virtual 实例的元数据，稍后配置实例。目前，Threat Defense Virtual 实例使用 IMDSv1 API 来获取和验证实例的元数据。从 7.6 及更高版本开始，支持 IMDSv2 元数据服务，这是一种更安全、更强大的服务。

在 AWS 中为 Threat Defense Virtual 实例配置 IMDS

AWS 支持 Threat Defense Virtual 实例的以下两种 IMDS 模式：

- **IMDSv2 可选**：您可以部署 Threat Defense Virtual 实例，以启用 IMDSv1 或 IMDSv2 或同时启用 IMDSv1 和 IMDSv2 API。
- **IMDSv2 必需**：您必须在 Threat Defense Virtual 实例部署期间仅专门配置此模式。

Note “IMDSv2 必需”是建议的模式，其中仅支持 IMDSv2 API 调用。

您可以在 AWS 中为以下部署场景中的实例配置 IMDS：

新部署：新部署 Threat Defense Virtual 实例时，可以配置 IMDSv2 必需模式。对于新部署，您可以使用以下方法之一来启用 IMDSv2。

- AWS EC2 控制台 - 您可以在 AWS EC2 控制台的“高级详细信息”(Advance Details) 部分中为独立实例部署启用**仅 V2**（**需要令牌**）**(V2 only [token required])**。
- CloudFormation 模板 - 您可以使用模板中 **MetadataOptions** 下的 HttpEndpoint: enabled 和 HttpTokens: required 属性来启用 **仅 V2**（**需要令牌**） - IMDSv2 必需模式。这适用于自动缩放和集群部署。

部署 Threat Defense Virtual

Before you begin

Cisco 建议以下操作：

- 如配置 AWS 环境, on page 71中所述，配置 AW VPC 和 EC2 元素。
- 确认可供 threat defense virtual 实例使用的 AMI。

Procedure

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 登录 Amazon 市场后，点击为 threat defense virtual (Cisco Firepower NGFW Virtual (NGFWv) - BYOL) 提供的链接。

Note
如果之前已登录 AWS，您可能需要注销并重新登录，以确保链接有效。

步骤 3 点击**继续**，然后点击**手动启动**选项卡。

步骤 4 点击**接受条款 (Accept Terms)**。

步骤 5 在期望的区域点击**使用 EC2 控制台启动 (Launch with EC2 Console)**。

步骤 6 选择 threat defense virtual 支持的**实例类型**，建议 c4.xlarge。

步骤 7 点击屏幕底部的**下一步：配置实例详细信息 (Next: Configure Instance Details)** 按钮：

- 更改**网络**，以匹配先前创建的 VPC。
- 更改**子网**，以匹配先前创建的管理子网。您可以指定 IP 地址或使用自动生成。
- 您可以启用**自动生成公用 IP**（IPv4 和 IPv6）。
- 单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。有关 IPv6 迁移的更多信息，请参阅 AWS IPv6 概述和 AWS VPC。
- 在网络接口下点击**添加设备**按钮以添加 eth1 网络接口。
- 更改**子网**，使其与之前创建的用于 eth0 的管理子网匹配。

Note
threat defense virtual 需要两个管理接口。

小心：在**高级详细信息**字段中输入数据时，请仅使用纯文本。如果从文本编辑器复制此信息，请确保仅以纯文本形式复制。如果将任何 Unicode 数据（包括空格）复制到**高级详细信息**字段，可能会造成实例损坏，然后您必须终止此实例并重新创建实例。

使用 管理中心 来管理 threat defense virtual 的登录配置示例：

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<your_hostname>",
            "IPv6Mode": "dhcp",
            "ManageLocally": "No",
            "FmcIp":  "<IP address of FMC>",
            "FmcRegKey":"<registration_passkey>",
            "FmcNatId":"<NAT_ID_if_required>"
}
```

使用 设备管理器 来管理 threat defense virtual 的登录配置示例：

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<your_hostname>",
            "ManageLocally": "Yes"
}
```

- 在**高级详细信息**下方，添加默认的登录信息。修改以下示例，以满足设备名称和密码要求。
- 在**高级详细信息 (Advanced Details)** 下，启用 IMDSv2 元数据：
  a. 从**元数据可访问 (Metadata accessible)** 下拉列表中选择**启用 (Enabled)**。
  b. 从**元数据版本 (Metadata version)** 下拉列表中选择 **仅 V2**（**需要令牌**）**(V2 only [token required])** 。

  您还可以通过执行以下操作来从 AWS CLI 启用 IMDSv2：
- 打开 AWS CLI 控制台并添加以下参数以启用“IMDSv2 必需”模式 **--metadata-options "HttpEndpoint=enabled,HttpTokens=required**”

  示例 IMDSv2 配置：

```
            aws ec2 run-instances \,
            --image-id ami-0abcdef1234567890 \
            --instance-type c5x.large \
...
--metadata-options "HttpEndpoint=enabled,HttpTokens=required"
```

步骤 8 点击**下一步：添加存储 (Next: Add Storage)**。

您可以继续使用默认值。

步骤 9 点击**下一步：标记实例 (Next: Tag Instance)**。

标签由区分大小写的键值对组成。例如，您可以按照“**Key = 名称**”和“**Value = 防火墙**”的格式定义标签。

步骤 10 选择**下一步：配置安全组 (Next: Configure Security Group)**。

步骤 11 点击**选择现有安全组 (Select an existing Security Group)** 并选择先前配置的安全组，或创建新的安全组；有关创建安全组的详细信息，请参阅 AWS 文档。

步骤 12 点击**检查和启动 (Review and Launch)**。

步骤 13 点击**启动 (Launch)**。

步骤 14 选择现有的密钥对或创建新的密钥对。

Note
您可以选择现有的密钥对或者创建新的密钥对。密钥对由 AWS 存储的一个公共密钥和用户存储的一个专用密钥文件组成。两者共同确保安全连接到实例。请务必将密钥对保存到已知位置，以备连接到实例之需。

步骤 15 点击**启动实例 (Launch Instances)**。

步骤 16 点击**查看启动**，然后按照提示进行操作。

步骤 17 点击 **EC2 控制面板 > 网络接口**。

步骤 18 查找之前在配置 AWS 环境, on page 71中创建的流量接口，然后点击**连接**。这将成为 threat defense virtual 实例上的 **eth2** 接口。

步骤 19 查找之前在配置 AWS 环境, on page 71中创建的流量接口，然后点击**连接**。这将成为 threat defense virtual 实例上的 **eth3** 接口。

Note
您必须配置四个接口，否则 threat defense virtual 将不会完成启动过程。

步骤 20 点击 **EC2 控制面板 > 实例**。

步骤 21 右键点击实例，然后选择**实例设置 > 获取系统日志**以查看状态。

Note
系统可能会显示连接问题的警告。这在预料之内，因为 eth0 接口在 EULA 完成之前不会激活。

步骤 22 20 分钟后，将 threat defense virtual 注册到 管理中心。

What to do next

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual, on page 409。
- 如果为**启用本地管理器 (Enable Local Manager)** 选择**是 (Yes)**，您将使用集成的 设备管理器 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual, on page 427。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备, on page 1。

为现有 Threat Defense Virtual 实例配置 IMDSv2 所需模式

您可以为 AWS 上已部署的 Threat Defense Virtual 实例配置 IMDSv2 必需模式。

Before you begin

仅 Threat Defense Virtual 版本 7.6 及更高版本支持 IMDSv2 必需模式。在为部署配置 IMDSv2 模式之前，您必须确保现有实例版本与 IMDSv2 模式兼容（升级到版本 7.6）。

Procedure

步骤 1 登录 http://aws.amazon.com/ 并选择您所在的区域。

步骤 2 点击 **EC2** > **实例 (Instances)**。

步骤 3 右键点击实例，然后选择**实例设置 (Instance Settings)** > **修改实例元数据选项 (Modify instance metadata options)**。系统将显示**修改实例元数据选项 (Modify instance metadata options)** 对话框。

步骤 4 在**实例元数据服务 (Instance metadata service)** 部分下，点击**启用 (Enable)**。

步骤 5 在 **IMDSv2** 选项下，点击**必需 (Required)**。

这将为所选实例启用“IMDSv2 必需”模式。

步骤 6 点击**保存 (Save)**。

使用映像快照的 Threat Defense Virtual

您可以在 AWS 门户中使用 Amazon Machine Image (AMI) 快照来创建并部署 threat defense virtual。映像快照是没有状态数据的已复制 threat defense virtual 映像实例。

Threat Defense Virtual 快照概述

创建 threat defense virtual 实例快照映像的过程跳过为 threat defense virtual 和 FSIC 执行的首次启动程序，有助于最大限度地缩短初始系统初始化时间。快照映像包含了预填充的数据库和 threat defense virtual 初始启动过程，该过程使映像能够重新生成与 管理中心 或任何其他管理中心中的系统身份相关的唯一 ID（UUID、序列号）。此过程有助于缩短 threat defense virtual 的启动时间，这在 Auto Scale 部署中至关重要。

Note 目前，使用 Threat Defense Virtual的快照映像部署的实例不支持即用即付 (PAYG) 许可。PAYG 许可仅适用于直接从市场部署的 实例。您可以将智能许可用于具有 PAYG 许可的新的 Threat Defense Virtual 部署。

创建 Threat Defense Virtual 快照 AMI

threat defense virtual 映像快照创建是复制现有 threat defense virtual 实例以在 AWS 门户中创建普通 threat defense virtual 实例的过程。

Before you begin

- 您必须已部署 threat defense virtual 7.2 或更高版本。有关部署 threat defense virtual 的信息，请参阅在 AWS 上部署 Threat Defense Virtual, on page 63。
- 不得将正准备拍摄映像快照的 threat defense virtual 实例注册到任何管理器，例如 Management Center Virtual 或 设备管理器。

Procedure

步骤 1 转至已部署 threat defense virtual 实例的 AWS 控制台。

Note
确保您计划复制为映像快照的 threat defense virtual 实例未注册到 管理中心 或配置到任何其他本地管理器，也未通过任何配置应用。

步骤 2 使用以下脚本从专家 shell 运行预快照进程：

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

在脚本中使用 `prepare_snapshot` 命令时，系统会显示一条中间消息，提示您确认执行脚本。按 **Y** 运行脚本。

或者，您可以在此命令后添加 `-f`（例如 `root@firepower:/ngfw/var/common#prepare_snapshot -f`），以跳过用户确认消息并直接执行脚本。

此脚本会删除与 threat defense virtual 实例关联的所有行配置、已部署的策略、已配置的管理器和 UUID。处理完成后，threat defense virtual 实例将关闭。threat defense virtual 实例列在 AWS 门户的**实例 (Instances)** 页面中。

步骤 3 登录 http://aws.amazon.com/ 并选择您所在的区域。

AWS 划分为彼此隔离的多个区域。区域显示在窗口的右上角。一个区域中的资源不会出现在另一个区域中。您应定期检查区域，以确保您在预期的区域内。

What to do next

使用快照 AMI 部署 threat defense virtual 实例。请参阅使用快照 AMI 部署 Threat Defense Virtual 实例, on page 83

Note 您可以从 threat defense virtual 控制台运行 CLI 命令 **show version** 和 **show snapshot detail**，以了解您创建的 threat defense virtual 映像快照实例的版本和详细信息。

使用快照 AMI 部署 Threat Defense Virtual 实例

Before you begin

Cisco 建议以下操作：

- 如配置 AWS 环境, on page 71中所述，配置 AW VPC 和 EC2 元素。
- 确认可供 threat defense virtual 实例使用的 AMI。

Procedure

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 点击 **EC2 控制面板 (EC2 Dashboard)** > **实例 (Instances)**。您为创建映像快照而部署的 threat defense virtual 实例将显示在**实例 (Instances)** 页面中。

Note
要创建映像快照，您必须始终选择运行状态（**实例状态 (Instance Status)**）为**已停止 (Stopped)** 的 threat defense virtual 实例。

步骤 3 在**实例 (Instances)** 页面上，识别并选择其相应**实例状态 (Instance Status)** 指示为**已停止 (Stopped)** 的 threat defense virtual 实例。

步骤 4 从**操作 (Actions)** 下拉菜单中指向**映像和模板 (Image and templates)**，然后点击**创建映像 (Create Image)**。

步骤 5 在**创建映像 (Create Image)** 页面中，提供映像快照的名称和说明。

步骤 6 选中**不重启 (No reboot)** 部分下的**启用 (Enable)** 复选框。

步骤 7 点击**创建映像 (Create Image)**。系统将创建 threat defense virtual 映像快照 AMI。

步骤 8 点击**映像 (Images)** > **AMI**。您可以在此页面上查看新创建的映像快照 AMI。

步骤 9 选择映像快照 AMI。

步骤 10 点击**启动 (Launch)** 以使用映像快照 AMI 来部署新的 threat defense virtual 实例。

步骤 11 继续部署 threat defense virtual 实例。请参阅部署 Threat Defense Virtual, on page 78或关于 AWS 上的 Threat Defense Virtual Auto Scale 解决方案, on page 106。

集成 Amazon GuardDuty 服务和 Threat Defense Virtual

Amazon GuardDuty 是一项监控服务，可处理来自各种来源的数据，如 VPC 日志、CloudTrail 管理事件日志、CloudTrail S3 数据事件日志、DNS 日志等，以识别 AWS 环境中潜在的未经授权的恶意活动。

概述

思科提供了一种解决方案，用于通过管理中心和设备管理器将 Amazon GuardDuty 服务与 Cisco Secure Firewall Threat Defense Virtual 集成。

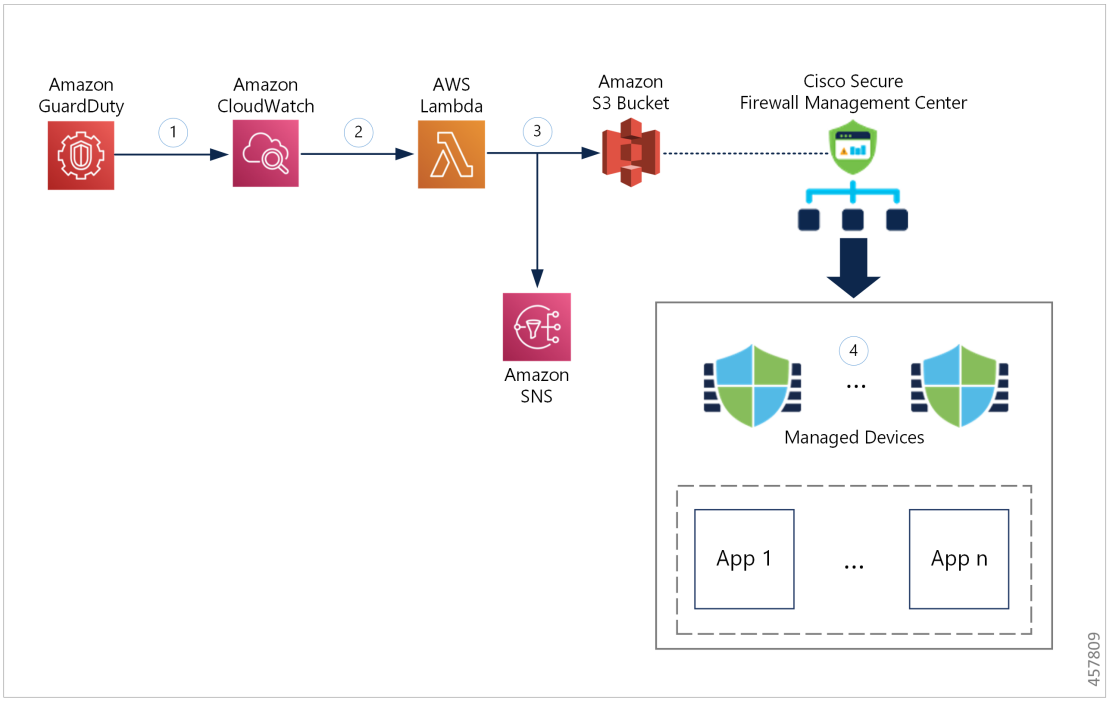
此解决方案使用 Amazon GuardDuty 的威胁分析数据或结果（产生威胁和攻击等的恶意 IP），并通过管理器 Cisco Secure Firewall Management Center Virtual 和 Cisco Secure Firewall 设备管理器 将这些信息（恶意 IP）反馈给 Cisco Secure Firewall Threat Defense Virtual，以保护底层网络和应用程序免受未来来自这些来源（恶意 IP）的威胁。

端到端程序

以下带有工作流程图解的集成解决方案可帮助您了解 Amazon GuardDuty 与 Cisco Secure Firewall Threat Defense Virtual 的集成。

使用安全智能网络源与 Cisco Secure Firewall Management Center Virtual 集成

下面的工作流程图显示了 Amazon GuardDuty 与 Cisco Secure Firewall Management Center Virtual 使用安全智能网络源 URL 的集成解决方案。

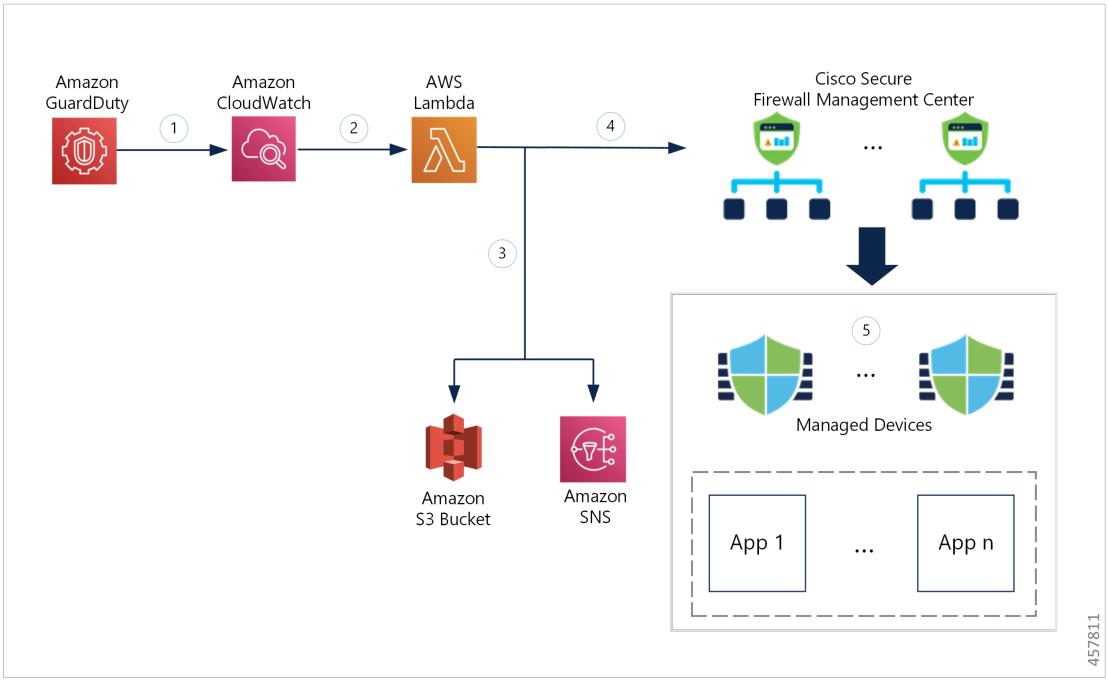


1	GuardDuty 服务会在检测到恶意活动时向 CloudWatch 发送威胁检测结果。
2	CloudWatch 事件会激活 AWS Lambda 函数。

3	Lambda 函数会更新 S3 存储桶中报告文件中的恶意主机，并通过 SNS 发送通知。
4	Cisco Secure Firewall Management Center 访问控制策略指示其目标设备根据配置的操作处理流量，例如阻止来自 GuardDuty 报告的恶意主机的流量。 此访问策略使用安全智能网络源和 Lambda 函数提供的恶意 IP 地址报告文件的 S3 对象 URL。

使用网络对象组与 Cisco Secure Firewall Management Center Virtual 集成

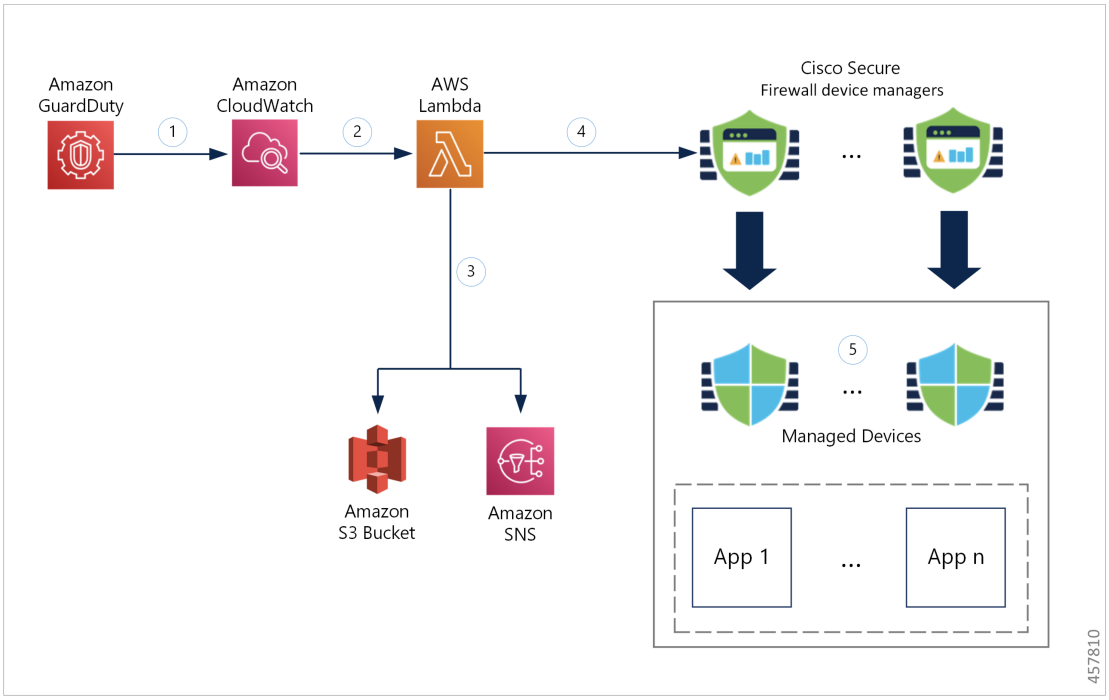
下面的工作流程图显示了 Amazon GuardDuty 与 Cisco Secure Firewall Management Center Virtual 使用网络对象组的集成解决方案。



1	GuardDuty 服务会在检测到恶意活动时向 CloudWatch 发送威胁检测结果。
2	CloudWatch 事件会激活 AWS Lambda 函数。
3	Lambda 函数会更新 S3 存储桶中报告文件中的恶意主机，并通过 SNS 发送通知。
4	Lambda 函数使用 Cisco Secure Firewall Management Center Virtual 中的恶意主机 IP 地址来配置或更新网络对象组。
5	Cisco Secure Firewall Management Center 访问控制策略指示其目标设备根据配置的操作处理流量，例如阻止来自 GuardDuty 报告的恶意主机的流量。 此访问控制策略会将网络对象组与 Lambda 函数提供的恶意 IP 地址配合使用。

使用网络对象组与 Cisco Secure Firewall 设备管理器 集成

下面的工作流程图显示了 Amazon GuardDuty 与 Cisco Secure Firewall 设备管理器 使用网络对象组的集成解决方案。



1	GuardDuty 服务会在检测到恶意活动时向 CloudWatch 发送威胁检测结果。
2	CloudWatch 事件会激活 AWS Lambda 函数。
3	Lambda 函数会更新 S3 存储桶中报告文件中的恶意主机，并通过 SNS 发送通知。
4	Lambda 函数使用 Cisco Secure Firewall 设备管理器 中的恶意主机 IP 地址来配置或更新网络对象组。
5	Cisco Secure Firewall 设备管理器 访问控制策略指示托管设备根据配置的操作处理流量，例如阻止来自 GuardDuty 报告的恶意主机的流量。 此访问控制策略会将网络对象组与 Lambda 函数提供的恶意 IP 地址配合使用。

此集成的关键组件

组件	说明
Amazon GuardDuty	一项 Amazon 服务，负责为特定区域的各种 AWS 资源（如 EC2、S3、IAM 等）生成威胁结果。

Amazon Simple Storage Service (S3)	一项用于存储与解决方案关联的各种构件的 Amazon 服务： • Lambda 函数 zip 文件 • Lambda 层 zip 文件 • Cisco Secure Firewall 管理中心和设备管理器 配置输入文件 (.ini) • 包含 Lambda 函数报告的恶意 IP 地址列表的输出报告文件 (.txt)
Amazon CloudWatch	用于以下情况的 Amazon 服务： • 监控 GuardDuty 服务是否有任何报告的结果，并触发 Lambda 函数来处理结果。 • 在 CloudWatch 日志组中记录与 Lambda 函数相关的活动。
Amazon Simple Notification Service (SNS)	用于推送电子邮件通知的 Amazon 服务。这些电子邮件通知包含： • Lambda 函数成功处理的 GuardDuty 结果的详细信息。 • Lambda 函数对 Cisco Secure Firewall 管理器执行的更新详细信息。 • Lambda 函数遇到的任何重大错误。
AWS Lambda 函数	一种 AWS 无服务器计算服务，可运行您的代码以响应事件，并自动管理底层计算资源。Lambda 函数由基于 GuardDuty 结果的 CloudWatch 事件规则触发。在此集成中，Lambda 函数负责： • 处理 GuardDuty 结果，以验证是否符合所有必要条件，如严重性、连接方向、是否存在恶意 IP 地址等。 • （取决于配置）使用恶意 IP 地址更新 Cisco Secure Firewall 管理器上的网络对象组。 • 更新 S3 存储桶报告文件中的恶意 IP 地址。 • 通知 Cisco Secure Firewall 管理员各种管理器更新和任何错误。

CloudFormation 模板	用于在 AWS 中部署集成所需的各种资源。 CloudFormation 模板包含以下资源： • **AWS::SNS::Topic**：用于推送电子邮件通知的 SNS 主题。 • **AWS::Lambda::Function, AWS::Lambda::LayerVersion**：Lambda 函数和层文件 • **AWS::Events::Rule**：用于根据 GuardDuty 结果事件触发 Lambda 函数的 CloudWatch 事件规则。 • **AWS::Lambda::Permission**：CloudWatch 事件规则触发 Lambda 函数的权限。 • **AWS::IAM::Role, AWS::IAM::Policy**：IAM 角色和策略资源，用于允许对各种 AWS 资源的 Lambda 函数的各种访问权限。 此模板接受用户输入参数，以自定义部署。

支持的软件平台

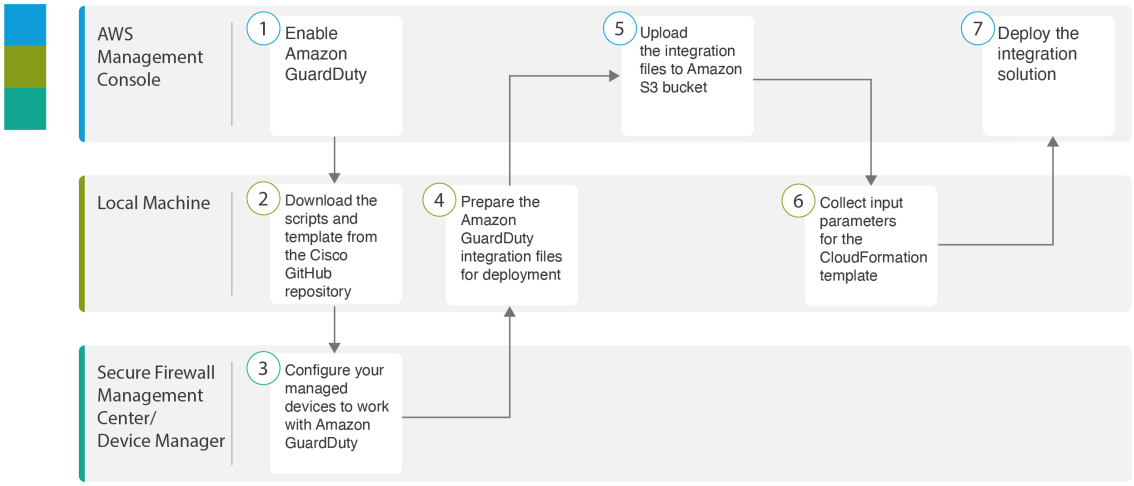
- GuardDuty 集成解决方案适用于由 Cisco Secure Firewall Management Center Virtual 或 Cisco Secure Firewall 设备管理器 托管的 Cisco Secure Firewall Threat Defense Virtual。
- Lambda 函数可以更新部署在任何虚拟平台上的管理中心和设备管理器中的网络对象组。确保 Lambda 函数可以通过公共 IP 地址连接到这些管理器。

准则和限制

- Lambda 函数只负责通过恶意 IP 地址来更新 Cisco Secure Firewall 管理器上的网络对象组。因此，请确保将这些更新或更改部署到托管设备。
- 此集成中使用的 AWS 服务针对特定区域。因此，如果要使用不同地区的 GuardDuty 发现，则必须部署特定地区的实例。
- Lambda 函数通过 REST API 更新 Cisco Secure Firewall 管理器。因此，您不能使用任何其他方法或管理器，例如 思科安全云控制。
- 您只能使用密码登录。不支持其他身份验证方法。
- 如果在输入文件中使用加密密码，请记住：
  - 只支持使用对称 KMS 密钥进行加密。
  - 所有密码都必须使用 Lambda 函数可访问的单一 KMS 密钥进行加密。

将 Amazon GuardDuty 与 Cisco Secure Firewall Threat Defense 集成

执行以下任务，将 Amazon GuardDuty 与 Cisco Secure Firewall Threat Defense 集成



	工作空间	步骤
1	AWS 管理控制台	在 AWS 上启用 Amazon GuardDuty 服务， 第 90 页
2	本地计算机	下载 Cisco Secure Firewall Threat Defense Virtual 和 Amazon GuardDuty 集成解决方案存储库，第 90 页
3	Cisco Secure Firewall Management Center或Cisco Secure Firewall 设备管理器	配置托管设备以便与 Amazon GuardDuty 配合使用， 第 91 页
4	本地计算机	准备用于部署的 Amazon GuardDuty 资源文件，第 94 页
5	AWS 管理控制台	将文件上传到 Amazon Simple Storage Service，第 97 页
6	本地计算机	收集 CloudFormation 模板的输入参数， 第 97 页
7	AWS 管理控制台	部署堆栈， 第 99 页

在 AWS 上启用 Amazon GuardDuty 服务

本节介绍如何在 AWS 上启用 Amazon GuardDuty 服务。

开始之前

确保所有 AWS 资源位于同一区域。

过程

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 依次选择 **服务 (Services) > GuardDuty**。

步骤 3 在 **GuardDuty** 页面中点击**开始 (Get Started)** 。

步骤 4 点击**启用 GuardDuty (Enable GuardDuty)** 以启用 Amazon GuardDuty 服务。

有关启用 GuardDuty 的更多信息，请参阅 AWS 文档中的 GuardDuty 入门。

下一步做什么

从思科 GitHub 存储库下载 Amazon GuardDuty 解决方案文件（模板和脚本）。请参阅下载 Cisco Secure Firewall Threat Defense Virtual 和 Amazon GuardDuty 集成解决方案存储库， 第 90 页。

下载 Cisco Secure Firewall Threat Defense Virtual 和 Amazon GuardDuty 集成解决方案存储库

下载 Amazon GuardDuty 解决方案所需的文件。您的 Cisco Secure Firewall Threat Defense Virtual 版本的部署脚本和模板可从思科 GitHub 存储库获取，地址是：

https://github.com/CiscoDevNet/cisco-ftdv

以下是思科 GitHub 存储库中的资源列表：

文件	说明
READ.MD	自述文件
configuration/	Cisco Secure Firewall Threat Defense Virtual 管理器配置文件模板。
images/	它包含 Cisco Secure Firewall Threat Defense Virtual 和 Amazon GuardDuty 集成解决方案说明。
lambda/	Lambda 函数 Python 文件。
templates/	用于部署的 CloudFormation 模板。

配置托管设备以便与 Amazon GuardDuty 配合使用

Lambda 函数处理 Amazon GuardDuty 结果并识别触发 CloudWatch 事件的恶意 IP 地址。Cisco Secure Firewall Threat Defense Virtual 采用以下方法之一通过 Cisco Secure Firewall Management Center Virtual 和 Cisco Secure Firewall 设备管理器 接收此威胁数据：

- **网络对象组更新** - Lambda 函数使用恶意 IP 地址来更新管理器中的网络对象组。然后，您就可以配置使用该网络对象组处理流量的访问控制策略。此方法适用于 Cisco Secure Firewall Management Center Virtual 和 Cisco Secure Firewall 设备管理器。
- **安全智能网络源** - Lambda 函数使用恶意 IP 地址在 Amazon S3 存储桶中创建或更新报告文件。您可以使用报告文件URL 设置安全智能源，然后配置使用此源处理流量的访问控制策略。此方法仅适用于 Cisco Secure Firewall Management Center Virtual。

使用报告文件 URL 配置安全智能网络源

本节介绍如何在 Cisco Secure Firewall Management Center Virtual 中配置安全智能网络源。

开始之前

- 确保您已在 Cisco Secure Firewall Management Center Virtual 上启用威胁许可证。请参阅威胁许可证。
- 确保您已创建并记下 Amazon S3 存储桶中的可用报告文件 URL。
- 确保可从 Cisco Secure Firewall Management Center Virtual 访问 Amazon S3 存储桶中的报告文件。

过程

步骤 1 登录 Cisco Secure Firewall Management Center Virtual。

步骤 2 使用 Amazon S3 存储桶的报告文件 URL 创建安全智能网络源。有关手动创建安全智能网络源的信息，请参阅自定义安全智能源。

步骤 3 使用安全智能网络源 URL 创建或更新访问控制策略或访问控制规则，以处理流量。请参阅手动 URL 过滤选项和创建和编辑访问控制规则。

注释
您可以在部署之前或之后创建安全智能网络源并更新访问控制策略中的 URL。如果要在 Amazon S3 存储桶中创建输出报告文件，则可以在部署之前创建安全智能网络源。如果要在部署后创建安全智能网络源，请等到您收到来自 Amazon GuardDuty 的第一个结果的邮件通知，然后使用该邮件通知中提供的 URL 配置安全智能网络源。

步骤 4 在 Cisco Secure Firewall Management Center Virtual 上部署配置更改。请参阅部署配置更改。

下一步做什么

准备用于部署的 Amazon GuardDuty 源文件。请参阅准备用于部署的 Amazon GuardDuty 资源文件，第 94 页。

创建网络对象组

在 Cisco Secure Firewall Management Center Virtual 和 Cisco Secure Firewall 设备管理器中，您必须为 Lambda 函数配置或创建网络对象组，以更新 Amazon GuardDuty 检测到的恶意 IP 地址。

如果不使用 Lambda 函数来配置网络对象组，则 Lambda 函数会创建一个默认名称为 **aws-gd-suspicious-hosts** 的网络对象组，以更新恶意 IP 地址。

创建网络对象组 Cisco Secure Firewall Management Center Virtual

本节介绍如何在 Cisco Secure Firewall Management Center Virtual中创建网络对象组。

过程

步骤 1 登录 Cisco Secure Firewall Management Center Virtual。

步骤 2 使用虚拟 IP 地址创建网络对象组。请参阅网络对象。

步骤 3 创建或更新访问控制策略或访问控制规则，以便使用网络对象组处理流量。请参阅管理访问控制策略和创建和编辑访问控制规则。

提示
您还可以在验证 Lambda 函数正在使用恶意 IP 地址更新网络对象组后，创建或更新“访问控制策略”或“访问控制规则”。

步骤 4 将配置更改部署到托管设备。请参阅部署配置更改。

下一步做什么

准备用于部署的 Amazon GuardDuty 源文件。请参阅准备用于部署的 Amazon GuardDuty 资源文件，第 94 页。

在 Cisco Secure Firewall 设备管理器 中创建网络对象组

本节介绍如何在 Cisco Secure Firewall 设备管理器中创建网络对象组。

过程

步骤 1 登录 Cisco Secure Firewall 设备管理器。

步骤 2 使用虚拟 IP 地址创建网络对象组。请参阅配置网络对象和组。

步骤 3 创建或更新访问控制策略或访问控制规则，以便使用网络对象组处理流量。请参阅配置访问控制策略和配置访问控制规则。

提示
您还可以在验证 Lambda 函数正在使用恶意 IP 地址更新网络对象组后，创建或更新“访问控制策略”或“访问控制规则”。

步骤 4 将配置更改部署到托管设备。请参阅部署更改。

下一步做什么

准备用于部署的 Amazon GuardDuty 源文件。请参阅准备用于部署的 Amazon GuardDuty 资源文件，第 94 页。

在 Cisco Secure Firewall Management Center Virtual 中为 Lambda 函数访问创建用户帐户

Lambda 函数要求用户账户具有管理员权限，以便更新管理中心和设备管理器中的网络对象组。因此，您必须在管理中心和设备管理器中创建一个具有管理员权限的专属用户账户。只有在使用网络对象组更新方法时，才需要创建用户账户。

有关创建新用户账户的详细信息，请参阅：

- 管理 FDM 和 FTD 用户访问权限
- FMC 的用户账户

（可选）加密密码

如果需要，可以在输入配置文件中提供加密密码。您还可以提供纯文本格式的密码。

使用 Lambda 函数可访问的单个 KMS 密钥加密所有密码。使用 **aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> 命令以生成加密密码。您必须安装并配置 AWS CLI 才能运行此命令。

注释 确保使用对称 KMS 密钥对密码进行加密。

有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面。有关主密钥和加密的详细信息，请参阅 AWS 文档《创建密钥》和关于密码加密和 KMS 的 AWS CLI 命令参考。

示例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

CiphertextBlob 密钥的值应用作密码。

准备用于部署的 Amazon GuardDuty 资源文件

Amazon GuardDuty 解决方案部署资源文件可从 Cisco GitHub 存储库中获取。

在 AWS 上部署 Amazon GuardDuty 解决方案之前，您必须准备以下文件：

- Cisco Secure Firewall Threat Defense Virtual 管理器配置输入文件
- Lambda 函数 zip 文件
- Lambda 层 zip 文件

准备配置输入文件

在配置模板中，您必须定义要与 Amazon GuardDuty 解决方案集成的管理中心或设备管理器的详细信息。建议您仅在计划实施网络对象组更新方法以将 Amazon GuardDuty 与管理中心和设备管理器集成时更新配置文件。

开始之前

- 确保在配置文件中提供用户帐户详细信息之前，对设备管理器的用户用户进行身份验证和验证。
- 如果要在配置文件中配置多个管理中心或设备管理器，请确保每个管理中心或设备管理器的参数在配置文件中只输入一次，且没有重复输入。
- 您必须记下管理中心和设备管理器的 IP 地址和名称。
- 您必须为 Lambda 函数创建一个具有管理员权限的用户账户，然后才能在管理中心和设备管理器中访问和更新这些网络对象组。

过程

步骤 1 登录已下载 Amazon GuardDuty 资源文件的本地计算机。

步骤 2 浏览至 **ngfwv-template > configuration** 文件夹。

步骤 3 在文本编辑器工具中打开 `ngfwv-manager-config-input.ini` 文件。

在此文件中，您必须输入计划集成和部署 Amazon GuardDuty 解决方案的管理中心或设备管理器的详细信息。

步骤 4 输入每个参数对应的管理中心或设备管理器的以下详细信息：

参数	说明
[ngfwv-1]	部分名称：管理中心或设备管理器的唯一标识符。
public-ip	管理中心或设备管理器的 IP 地址。
device-type	通过管理中心或设备管理器部署 Amazon GuardDuty 解决方案的托管设备类型。允许的值为 FMC 或 FDM。

参数	说明
用户名	用于登录管理中心或设备管理器的用户名。
password	用于登录管理中心或设备管理器的密码。密码可以是纯文本格式，也可以是使用 KMS 创建的加密字符串。
object-group-name	Lambda 函数使用恶意主机 IP 更新的网络对象组的名称。如果要输入多个网络对象组名称，请确保它们是以逗号分隔的值。

步骤 5 保存并关闭 `ngfwv-manager-config-input.ini` 文件。

下一步做什么

创建 Lambda 函数存档文件。请参阅准备 Lambda 函数存档文件，第 95 页。

准备 Lambda 函数存档文件

本节介绍如何在 Linux 环境中存档 Lambda 函数文件。

注释 存档过程可能因存档文件的本地计算机操作系统而异。

过程

步骤 1 在已下载 Amazon GuardDuty 资源的本地计算机上打开 CLI 控制台。

步骤 2 导航到 `/lambda` 文件夹并存档文件。

以下是 Linux 主机的示例脚本。

```
$ cd lambda
$ zip ngfwv-gd-lambda.zip *.py
adding: aws.py (deflated 71%) adding: fdm.py (deflated 79%)
adding: fmcv.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

将创建压缩文件 `ngfwv-gd-lambda.zip`。

步骤 3 退出并关闭 CLI 控制台。

下一步做什么

使用压缩文件 `ngfwv-gd-lambda.zip` 来创建 Lambda 层压缩文件。请参阅准备 Lambda 层文件，第 96 页

准备 Lambda 层文件

本节介绍如何在 Linux 环境中存档 Lambda 层文件。

注释 存档过程可能因存档文件的本地计算机操作系统而异。

过程

步骤 1 在已下载 Amazon GuardDuty 资源的本地计算机上打开 CLI 控制台。

步骤 2 在 CLI 控制台中执行以下操作。

以下是安装了 Python 3.9 的 Linux 主机（如 Ubuntu 22.04）的示例脚本。

```
$ mkdir -p layer
$ virtualenv -p /usr/bin/python3.9 ./layer/
$ source ./layer/bin/activate
$ pip3.9 install cffi==1.15.0
$ pip3.9 install cryptography==37.0.2
$ pip3.9 install paramiko==2.7.1
$ pip3.9 install requests==2.23.0
$ mkdir -p ./python/.libs_cffi_backend/
$ cp -r ./layer/lib/python3.9/site-packages/* ./python/
$ zip -r ngfwv-gd-lambda-layer.zip ./python
```

压缩文件 `ngfwv-gd-lambda-layer.zip` 已创建。

请注意，创建 Lambda 层必须安装 Python 3.9 及其依赖项。

以下是在 Ubuntu 22.04 等 Linux 主机上安装 Python 3.9 的示例脚本。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

步骤 3 退出并关闭 CLI 控制台。

下一步做什么

在 Amazon S3 存储桶中，您必须上传 Cisco Secure Firewall Threat Defense Virtual 配置文件、Lambda 函数 zip 文件和 Lambda 层 zip 文件。请参阅将文件上传到 Amazon Simple Storage Service，第 97 页

将文件上传到 Amazon Simple Storage Service

准备好所有 Amazon GuardDuty 解决方案工件后，必须将文件上传到 AWS 门户中的 Amazon Simple Storage Service (S3) 存储桶文件夹。

过程

步骤 1 前往 https://aws.amazon.com/marketplace(Amazon Marketplace) 并登录。

步骤 2 打开 Amazon S3 控制台。

步骤 3 创建用于上传 Amazon GuardDuty 构件的 Amazon S3 存储桶。请参阅创建 Amazon S3。

步骤 4 将以下 Amazon GuardDuty 构件上传到 Amazon S3 存储桶。

- Cisco Secure Firewall Threat Defense Virtual 配置文件：`ngfwv-config-input.ini`

  注释
  在管理中心中使用安全智能网络源方法部署 Amazon GuardDuty 解决方案时，不需要上传此文件。

- Lambda 层 zip 文件：`ngfwv-gd-lambda-layer.zip`
- Lambda 函数 zip 文件：`ngfwv-gd-lambda.zip`

下一步做什么

准备用于部署 Amazon GuardDuty 资源的 CloudFormation 模板。请参阅收集 CloudFormation 模板的输入参数，第 97 页。

收集 CloudFormation 模板的输入参数

思科提供了 CloudFormation 模板，用于在 AWS 中部署 Amazon GuardDuty 解决方案所需的资源。在部署前收集以下模板参数值。

过程

Template Parameters

参数	说明	示例
部署名称*	在此参数中输入的名称将用作云组建模板创建的所有资源的前缀。	**cisco-ngfwv-gd**
GD 结果的最低严重性级别*	要考虑处理的 Amazon GuardDuty 结果的最低严重性级别必须在 **1.0** 到 **8.9** 之间的范围。任何严重程度低于最小范围的结果都将被忽略。 严重性分类如下： • 低：1.0 至 3.9 中：4.0 至 6.9 高：7.0 至 8.9。	**4.0**
管理员电子邮件 ID*	管理员电子邮件地址，用于在 Cisco Secure Firewall Threat Defense Virtual 管理器上接收有关管理中心或设备管理器中的 Lambda 函数完成的更新的通知。	**abc@xyz.com**
S3 存储桶名称*	包含 Amazon GuardDuty 构件文件（Lambda 函数 zip、Lambda 层 zip 和 Cisco Secure Firewall Threat Defense Virtual 配置管理器文件）的 Amazon S3 存储桶的名称。	例如：**ngfwv-gd-bucket**
S3 存储桶文件夹/路径前缀	存储配置文件的 Amazon S3 存储桶路径或文件夹名称。如果没有文件夹，请将此字段留空。	例如：`""` 或“**cisco/ngfwv-gd/**”
Lambda 层 zip 文件名*	Lambda 层 zip 文件名。	例如：`ngfwv-gd-lambda-layer.zip`
Lambda 函数 zip 文件名*	Lambda 函数 zip 文件名。	例如：`ngfwv-gd-lambda.zip`
Cisco Secure Firewall 管理中心和设备管理器 管理器配置文件名	包含 Cisco Firewall Threat Defense Virtual 的管理器配置详细信息的 ***.ini** 文件。（公共 IP、用户名、密码、设备类型、网络对象组名称等。） **注释** 仅当使用网络对象组更新方法进行 Amazon GuardDuty 集成时才需要此文件。 如果使用的是安全智能源方法，则可以跳过提供此输入的步骤。	例如：`ngfwv-config-input.ini`

参数	说明	示例
用于密码加密的 KMS 密钥的 ARN	现有 KMS 的 ARN（用于密码加密的 AWS KMS 密钥）。如果 Cisco Secure Firewall Threat Defense Virtual 配置输入文件中提供了纯文本密码，则可以将此参数留空。如果指定，则必须加密 Cisco Secure Firewall Threat Defense Virtual 配置输入文件中提到的所有密码。密码必须仅使用指定的 ARN 进行加密。生成加密密码：aws kms encrypt --key-id <KMS ARN> --plaintext <password>	例如：**arn:aws:kms:<region>:<aws account id>:key/<key id>**
启用/禁用调试日志*	启用或禁用 CloudWatch 中的 Lambda 函数调试日志。	例如：**enable** 或 **disable**

*：必填字段

下一步做什么

使用 CloudFormation 模板部署堆栈。请参阅部署堆栈， 第 99 页

部署堆栈

完成 Amazon GuardDuty 解决方案部署的所有前提流程后，创建 AWS CloudFormation 堆栈。使用目标目录中的模板文件：`templates/cisco-ngfwv-gd-integration.yamltemplates`，并提供在收集 CloudFormation 模板的输入参数中收集的参数。

过程

步骤 1 登录 AWS 控制台。

步骤 2 转至“服务”(Services)>CloudFormation>“堆栈”(Stacks)>“创建堆栈”(Create stack)（使用新资源）>“准备模板”(Prepare template)（模板在文件夹中提供）>“指定模板”(Specify template)>“模板来源”(Template source)（从目标目录更新模板文件：`templates/cisco-ngfwv-gd-integration.yaml`）>“创建堆栈”(Create Stack)

有关在 AWS 上部署堆栈的详细信息，请参阅 AWS 文档。

下一步做什么

验证部署。请参阅验证部署， 第 100 页。

此外，还可以订阅 Amazon GuardDuty 报告的威胁检测更新电子邮件通知。请参阅订阅电子邮件通知，第 100 页。

订阅电子邮件通知

在 CloudFormation 模板中，一个电子邮件 ID 被配置为接收关于由 Lambda 函数完成的 GuardDuty 查找更新的通知。在 AWS 上部署 CloudFormation 模板后，系统会通过 Amazon Simple Notification Service (SNS) 服务向此邮件 ID 发送邮件通知，要求您订阅通知更新。

过程

步骤 1 打开邮件通知。

步骤 2 点击邮件通知中提供的**订用 (Subscription)** 链接。

下一步做什么

验证部署。请参阅验证部署，第 100 页。

验证部署

在 AWS 中，您可以选择验证 Amazon GuardDuty 解决方案，如本节所述。在 CloudFormation 部署完成后，您可以按照这些部署验证说明进行操作。

开始之前

确保已安装和配置 AWS 命令行界面 (CLI)，以运行命令验证部署。有关 AWS CLI 文档的信息，请参阅 AWS 命令行界面。

过程

步骤 1 登录 AWS 管理控制台。

步骤 2 转到**服务 (Services)** > **GuardDuty** > **设置 (Settings)** > **关于 GuardDuty (About GuardDuty)** > **检测器 ID (Detector ID)**，然后记下检测器 ID。

生成 Amazon GuardDuty 检测结果样本时需要使用此检测器 ID。

步骤 3 打开 AWS CLI 控制台，通过运行以下命令生成示例 Amazon GuardDuty 结果：

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

步骤 4 在 Amazon GuardDuty 控制台的结果列表中查看样本结果。

示例结果包含前缀 **[sample]**。您可以通过查看连接方向、远程 IP 地址等属性来检查示例结果详细信息。

步骤 5 等待 Lambda 函数运行。

触发 Lambda 函数后，验证以下内容：

- 电子邮件通知，其中包含有关收到的 Amazon GuardDuty 结果和 Lambda 函数完成的 Cisco Secure Firewall Threat Defense Virtual 管理器 更新的详细信息
- 验证在 Amazon S3 存储桶中是否生成了报告文件。它包含样本 Amazon GuardDuty 结果报告的恶意 IP 地址。您可以采用以下格式识别报告文件名：`<deployment-name>-report.txt`.
- 对于网络对象组更新方法 - 验证是否已使用从示例结果更新的恶意 IP 地址更新已配置的管理器（Cisco Secure Firewall Management Center Virtual 或 Cisco Secure Firewall 设备管理器）上的网络对象组。
- 对于安全智能源方法 - 验证报告文件 URL 是否已在管理中心配置中更新。您可以在管理中心的以下路径中查看报告文件 URL 的最后更新时间戳。
  - **对象 (Objects) > 对象管理 (Object Management) > 安全智能 (Security Intelligence) > 网络列表和源 (Network Lists and Feeds) > 选择配置的源**
  - 或者，您可以手动更新源，然后检查**上次更新**时间戳。您可以选择和更新以下路径中的源：

    对象 (Objects) > 对象管理 (Object Management) > 安全智能 (Security Intelligence) > 网路列表和源 (Network Lists and Feeds) > 更新源 (Update Feeds)

步骤 6 转到 **AWS 控制台 (AWS Console) > 服务 (Services) > CloudWatch > 日志 (Logs) > 日志组 (Log groups)**，选择日志组以验证 CloudWatch 控制台中的 Lambda 日志。您可以采用以下格式标识 CloudWatch 日志组名称：`<deployment-name>-lambda`。

步骤 7 在验证部署后，建议您按以下步骤清理示例结果生成的数据：

a) 转到 **AWS 控制台(AWS Console) > 服务 (Services) > GuardDuty > 结果 (Findings) > 选择结果 > 操作 (Actions) > 存档 (Archive)**，以查看示例结果数据。

b) 删除网络对象组中添加的恶意 IP 地址，以从 Cisco Secure Firewall Management Center Virtual清除缓存数据。

c) 清理 Amazon S3 存储桶中的报告文件。您可以通过删除示例结果所报告的恶意 IP 地址来更新文件。

更新现有解决方案部署配置

建议您不要在部署后更新 S3 存储桶或 S3 存储桶文件夹和路径前缀值。但如果需要更新已部署解决方案的配置，请使用 AWS 控制台中 CloudFormation 页面上的**更新堆栈 (Update Stack)** 选项。

您可以更新下面给出的任何参数。

参数	说明
Cisco Secure Firewall Threat Defense Virtual 管理器配置文件名	在 Amazon S3 存储桶中添加或更新配置文件。您可以使用与之前文件相同的名称来更新文件。如果修改了配置文件名称，则可以使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数。
GD 结果的最低严重性级别*	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。
管理员电子邮件 ID*	使用 AWS 控制台中的**更新堆栈 (Update Stack)** 选项更新邮件 ID 参数值。您还可以通过 SNS 服务控制台添加或更新电子邮件订用。
S3 存储桶名称*	使用新名称更新 Amazon S3 存储桶中的 zip 文件，然后使用 AWS 控制台中的**更新堆栈 (Update Stack)** 选项来更新参数。
Lambda 层 zip 文件名*	使用新名称更新 Amazon S3 存储桶中的 Lambda 层 zip 文件名，然后使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数值。
Lambda 函数 zip 文件名*	使用新名称更新 Amazon S3 存储桶中的 Lambda 函数 zip 文件，然后使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新此参数值。
用于密码加密的 KMS 密钥的 ARN	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。
启用/禁用调试日志*	使用 AWS 控制台中的**更新堆栈 (Update stack)** 选项来更新参数值。

过程

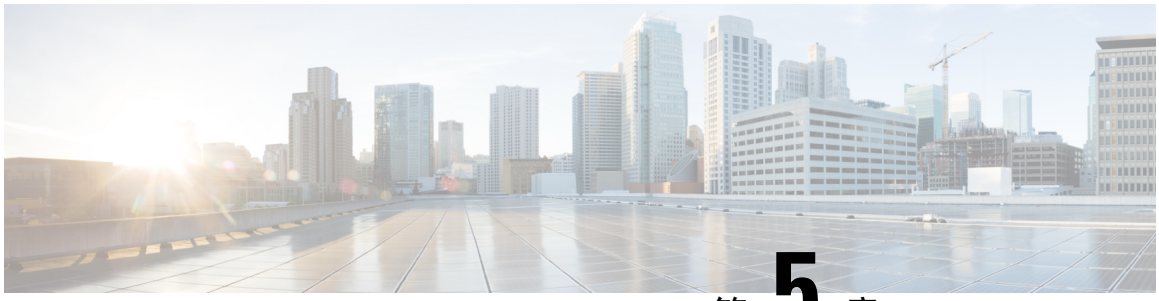
步骤 1 转到 AWS 管理控制台。

步骤 2 如果需要，请创建新的存储桶和文件夹。

步骤 3 确保将下面给出的构件从旧存储桶复制到新的存储桶。

- Cisco Secure Firewall Threat Defense Virtual 配置文件：`ngfwv-config-input.ini`
- Lambda 层 zip 文件：`ngfwv-gd-lambda-layer.zip`
- Lambda 函数 zip 文件：`ngfwv-gd-lambda.zip`
- 输出报告文件：`<deployment-name>-report.txt`

步骤 **4** 要更新参数值，请转至 **Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>**> Update Stack**。



第 5 章

在 AWS 上部署 Threat Defense Virtual Auto Scale 解决方案

本文档介绍如何在 AWS 上部署 threat defense virtual Auto Scale 解决方案。

- 使用案例 - 适用于 Threat Defense Virtual 的 Auto Scale 解决方案，使用 AWS 上的 GWLB 检查南北流量 ，第 150 页

关于 AWS 上的 Threat Defense Virtual Auto Scale 解决方案

部署在公共云环境（例如 AWS）中的 threat defense virtual 实例支持偶尔遇到网络流量高峰和低谷的应用。流量高峰可能会导致部署的 Threat Defense Virtual 实例数量不足以检查网络流量。流量下降可能导致 Threat Defense Virtual 实例空闲，从而导致不必要的运营成本。

Auto Scale 解决方案可帮助组织在出现流量高峰时自动按比例增加 Threat Defense Virtual 实例的数量，并在流量停滞期间按比例缩小实例数量。这样可以有效地处理网络资源并降低运营成本。

AWS 中的 threat defense virtual Auto Scale 是完整的无服务器实现（此功能的自动化不涉及辅助虚拟机），它可以将自动扩展功能加入到 AWS 环境中的 threat defense virtual 实例。

从版本 6.4 开始，在管理中心管理的 threat defense virtual 上支持基于网络负载均衡器 (NLB) 的自动扩展解决方案。从版本 7.2 开始，还支持基于网关负载均衡器 (GWLB) 的自动扩展解决方案。

Cisco 提供 CloudFormation 模板和脚本，用于使用多个 AWS 服务部署 threat defense virtual 防火墙的自动扩展组，包括 Lambda、自动扩展组、弹性负载均衡 (ELB)、Amazon S3 存储桶、SNS 和 CloudWatch。

threat defense virtual Auto Scale 解决方案是基于 CloudFormation 模板的部署，可提供：

- 管理中心 中完全自动化的 threat defense virtual实例注册和取消注册。
- 自动应用到外向扩展 threat defense virtual实例的 NAT 策略、访问控制策略和路由。
- 对负载均衡器和多可用性区域的支持。
- 仅适用于 管理中心；不支持 设备管理器。

Auto Scale 增强功能（版本 6.7）

- 自定义指标发布方 — 新的 lambda 函数每 2 分钟轮询一次 管理中心 以获取 Auto Scale 组中所有 threat defense virtual 实例的内存消耗情况，然后将值发布到 CloudWatch 指标；有关说明，请参阅。
- 提供了基于内存消耗的新扩展策略。
- 用于连接 管理中心 的 Threat Defense Virtual专用 SSH 和安全隧道 IP 连接。
- 管理中心 配置验证。
- 支持在 ELB 上打开更多侦听端口。
- 修改为单堆栈部署。所有 lambda 函数和 AWS 资源都从单堆栈进行部署，以便简化部署。

使用 NLB 的 Auto Scale 解决方案

由于 AWS 负载均衡器只允许入站发起的连接，因此只允许外部生成的流量通过 Cisco Threat Defense Virtual 防火墙传入内部。

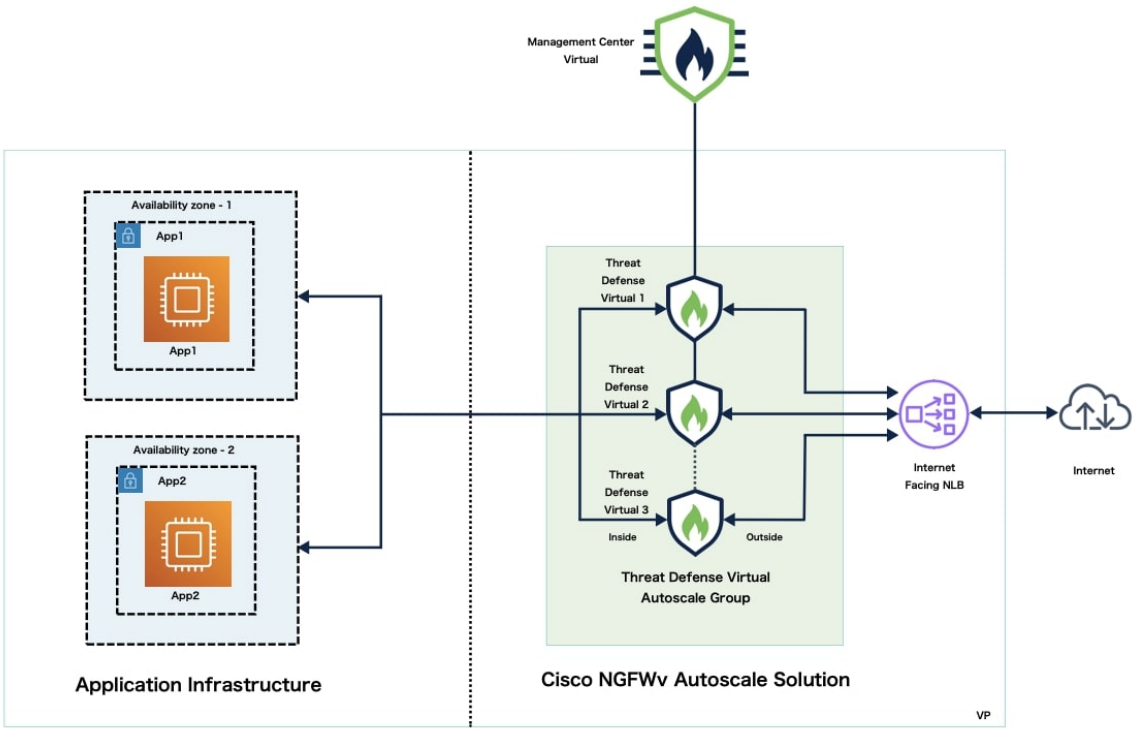
面向互联网的负载均衡器可以是网络负载均衡器或应用程序负载均衡器。在两种情况下，所有 AWS 要求和条件均适用。如下图拓扑示例所示，虚线右侧通过 Threat Defense Virtual 模板进行部署。左侧由用户定义。

注释 应用程序发起的出站流量将不会经过 Threat Defense Virtual。

基于端口的流量分叉是可能的。这可以通过NAT规则实现；请参阅在管理中心中创建主机对象、添加设备组、采用 NLB 的 Auto Scale 解决方案 - 配置和部署网络地址转换 (NAT) 策略、创建基本访问控制策略，第 136 页、创建基本访问控制策略。例如，面向互联网的 LB DNS、端口：80 上的流量可以路由到应用程序 1；端口：88 流量可路由到应用程序 2。

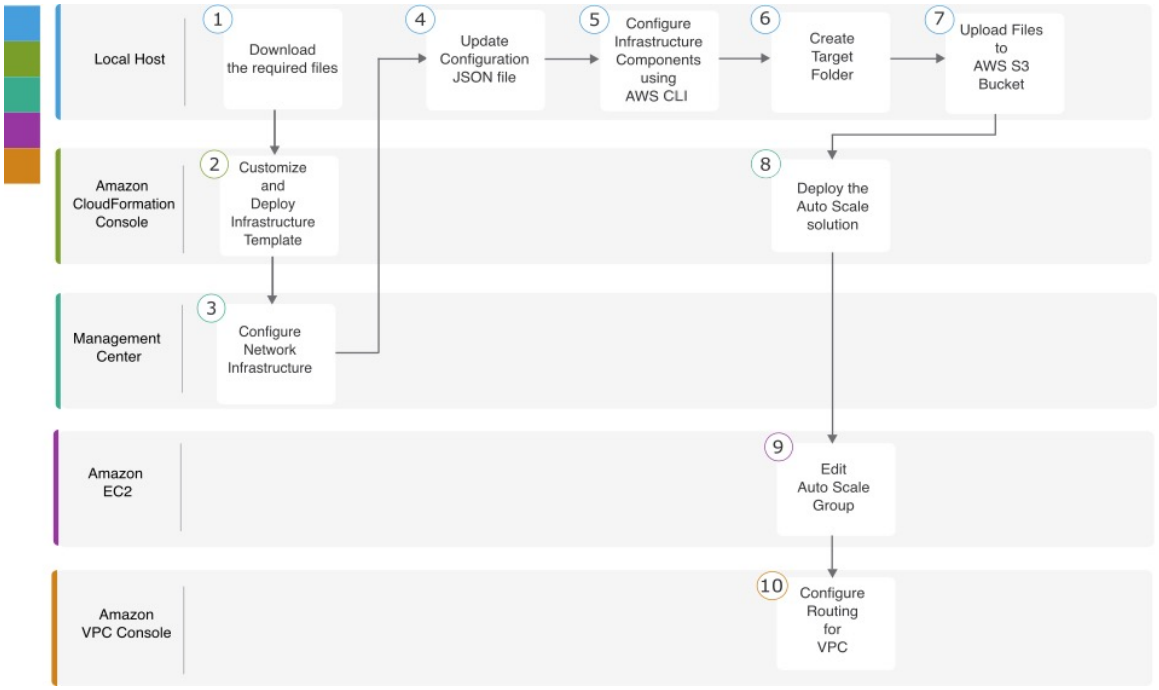
拓扑示例

图 *3:* 使用 ***NLB*** 的 ***Threat Defense Virtual Auto Scale*** 解决方案



使用 NLB 部署 Auto Scale 解决方案的端到端流程

以下流程图说明了在 Amazon Web 服务 (AWS) 上使用 NLB 部署 threat defense virtual 自动扩展解决方案的工作流程。



	工作空间	步骤
1	本地主机	将所需文件和 CFT 从 GitHub 下载到本地主机
2	Amazon CloudFormation 控制台	使用 NLB 的 Auto Scale 解决方案 - 在 Amazon CloudFormation 控制台上自定义和部署 NLB 基础设施模板，第 130 页
3	管理中心	在管理中心配置网络基础设施，第 131 页
4	本地主机	更新 configuration.json 文件，第 137 页
5	本地主机	使用 AWS CLI 配置基础设施组件，第 138 页
6	本地主机	创建目标文件夹，第 140 页
7	本地主机	将文件上传到 Amazon S3 存储桶，第 140 页

	工作空间	步骤
8	Amazon CloudFormation 控制台	支持 NLB 的 Auto Scale 解决方案 - 部署支持 NLB 的 Auto Scale 解决方案， 第 140 页
9	Amazon EC2 控制台	编辑 Auto Scale 组， 第 143 页
10	Amazon VPC 控制台	为 VPC 配置路由， 第 142 页

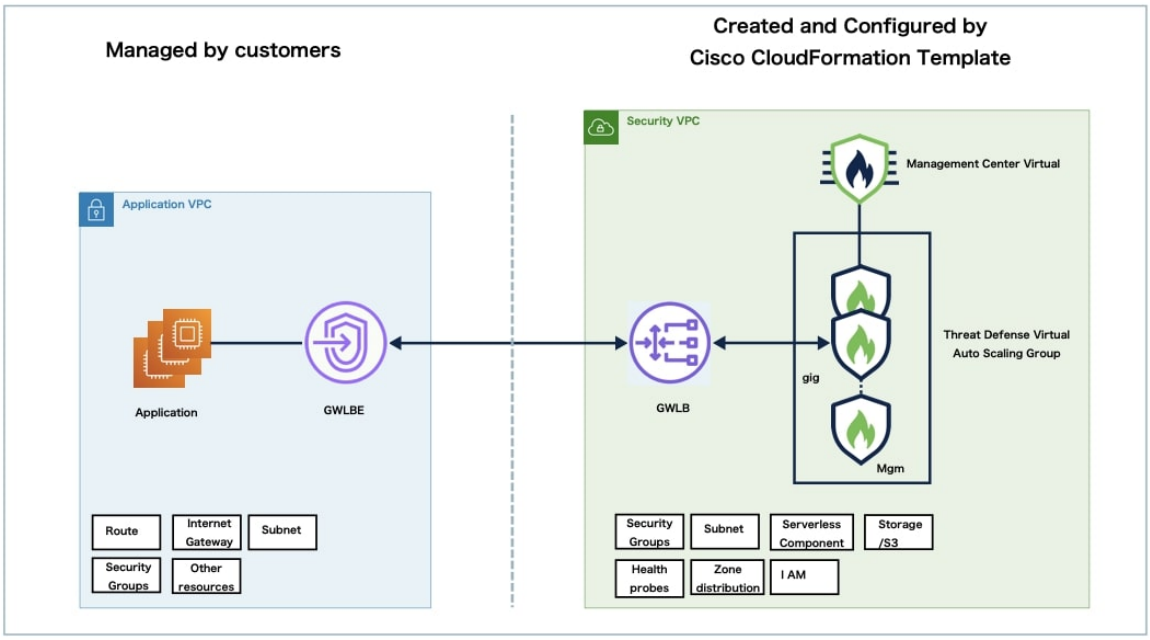
使用网关负载均衡器的 Auto Scale 解决方案

AWS 网关负载均衡器 (GWLB) 允许入站和出站连接。因此，允许内部和外部生成的流量通过 Threat Defense Virtual 防火墙。

GWLB 终端会将流量发送到 GWLB，然后发送到 Threat Defense Virtual 进行检测。在两种情况下，所有 AWS 要求和条件均适用。如使用案例图中所示，虚线右侧是通过 Threat Defense Virtual 模板部署的 Threat Defense Virtual GWLB Autoscale 解决方案。左侧完全由用户定义。

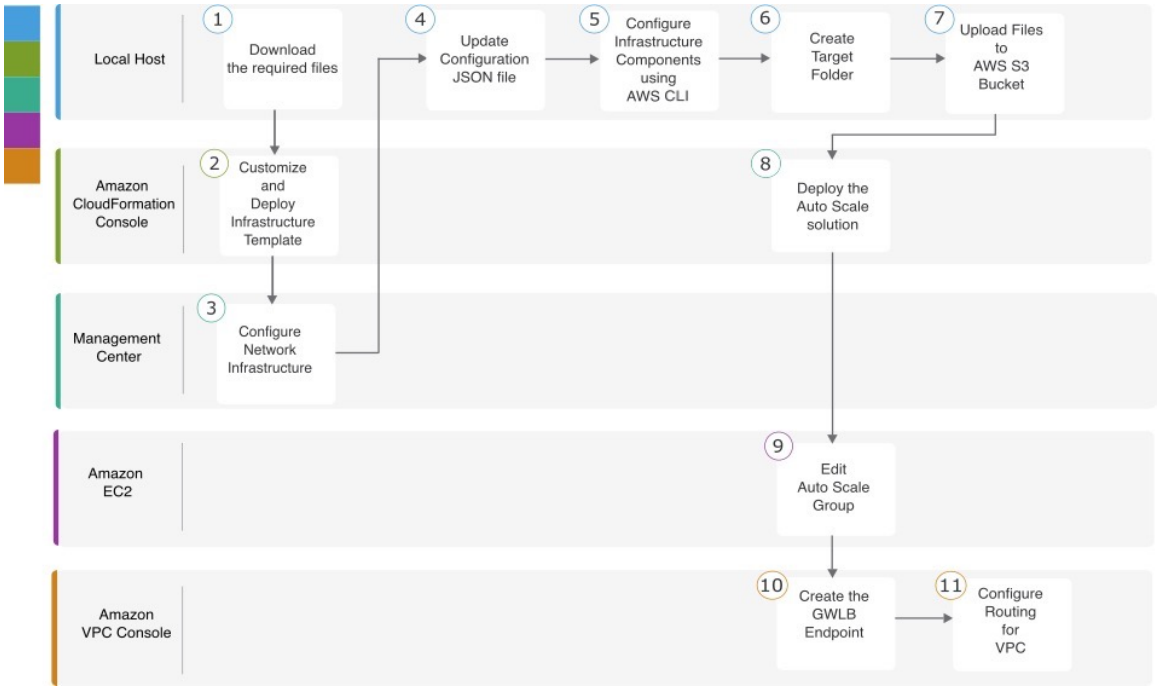
拓扑示例

图 *4:* 使用 ***GWLB*** 的 ***Threat Defense Virtual Auto Scale*** 解决方案



使用 GWLB 部署 Auto Scale 解决方案的端到端流程

以下流程图说明了在 Amazon Web 服务 (AWS) 上使用 GWLB 部署 threat defense virtual 自动扩展解决方案的工作流程。



	工作空间	步骤
1	本地主机	将所需文件和 CFT 从 GitHub 下载到本地主机
2	Amazon CloudFormation 控制台	使用 GWLB 的 Auto Scale 解决方案 - 在 Amazon CloudFormation 控制台上自定义和部署 GWLB 基础设施模板， 第 131 页
3	管理中心	在管理中心配置网络基础设施， 第 131 页
4	本地主机	更新 configuration.json 文件， 第 137 页
5	本地主机	使用 AWS CLI 配置基础设施组件， 第 138 页
6	本地主机	创建目标文件夹， 第 140 页
7	本地主机	将文件上传到 Amazon S3 存储桶， 第 140 页

	工作空间	步骤
8	Amazon CloudFormation 控制台	支持 GWLB 的 Auto Scale 解决方案 - 部署支持 GWLB 的 Auto Scale 解决方案， 第 141 页
9	Amazon EC2 控制台	编辑 Auto Scale 组， 第 143 页
10	Amazon VPC 控制台	带有 GWLB 的 Auto Scale 解决方案 - 创建 GWLB 终端， 第 141 页
11	Amazon VPC 控制台	为 VPC 配置路由， 第 142 页

Threat Defense Virtual和 AWS 的准则和限制

许可

- 支持使用 Cisco 智能许可证帐户的 BYOL（自带许可证）。
- PAYG（即付即用）许可，一种基于使用的计费模式，允许客户在不购买 Cisco 智能许可的情况下运行 threat defense virtual。对于已注册的 PAYG threat defense virtual 设备，将启用所有许可的功能（恶意软件/威胁/URL 过滤/VPN 等）。许可的功能无法从 管理中心 编辑或修改。（版本 6.5+）

Note 在 设备管理器 模式下部署的 threat defense virtual 设备上不支持 PAYG 许可。

有关许可 threat defense virtual 设备时的准则，请参阅《防火墙管理中心管理指南》中的“许可证”一章。

Threat Defense Virtual 智能许可的性能级别

从 Threat Defense Virtual 版本 7.0.0 发布开始，threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

Table 16: 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5	4 核/8 GB	100 Mbps	50
FTDv10	4 核/8 GB	1 Gbps	250
FTDv20	4 核/8 GB	3 Gbps	250

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv30	8 核/16 GB	5 Gbps	250
FTDv50	12 核/24 GB	10 Gbps	750
FTDv100	16 核/34 GB	16 Gbps	10,000

最佳实践

- 确保您已在 Management Center Virtual 中配置所需的组件。有关详细信息，请参阅在管理中心配置网络基础设施。
- 确保在 CloudFormation 模板中输入所需的参数值。有关详细信息，请参阅 GitHub 上的 CloudFormation 模板。

前提条件

- 一个 AWS 账户。您可以在 http://aws.amazon.com/ 创建一个。
- 需要 SSH 客户端（例如，Windows 上的 PuTTY 或 macOS 上的终端）才能访问 Threat Defense Virtual 控制台。
- 思科智能账户。您可以在 Cisco 软件中心 https://software.cisco.com/ 创建一个。
- 用于下载配置文件和模板的 GitHub 帐户。
- Threat Defense Virtual 接口要求：
  - 管理接口 (2) - 一个用于连接 Threat Defense Virtual 和管理中心，第二个用于诊断；无法用于直通流量。
  - 您可以选择为管理中心管理配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。请注意，在高可用性部署中，不支持从数据接口进行管理中心访问。有关为管理中心访问配置数据接口的详细信息，请参阅FTD命令参考中的配置网络管理数据接口命令。
  - 流量接口 (2) - 用于将 Threat Defense Virtual 连接到内部主机和公共网络。
- 通信路径 - 用于访问 threat defense virtual 的公共/弹性 IP。

设置具有 GWLB 或 NLB 的 Auto Scale 解决方案所需的组件

以下组件构成了 Auto Scale 解决方案。

CloudFormation 模板

CloudFormation 模板用于部署在 AWS 中设置 Auto Scale 解决方案所需的资源。该模板包括以下各项：

- Auto Scale 组、负载均衡器、安全组和其他各种组件。
- 模板需要用户输入来自定义部署。

注释 模板在验证用户输入方面有限制，因此，用户应负责在部署期间验证输入。

Lambda 函数

Auto Scale 解决方案是在 Python 中开发的一组 Lambda 函数，可以通过生命周期钩子、SNS、CloudWatch 事件/警报事件触发。基本功能包括：

- 向实例添加/删除 Diag、Gig0/0 和 Gig 0/1 接口。
- 向负载均衡器的目标组注册 Gig0/1 接口。
- 向 管理中心 注册新的 threat defense virtual。
- 通过 管理中心 配置并部署新的 threat defense virtual。
- 从 管理中心 取消注册（删除）内向扩展的 threat defense virtual。
- 从 管理中心 发布内存指标。

Lambda 函数以 Python 包的形式交付给客户。

生命周期钩子

- 生命周期钩子用于获取关于实例的生命周期更改通知。
- 在启动实例时，生命周期钩子用于触发 Lambda 函数，可将接口添加到 threat defense virtual 实例，并将外部接口 IP 注册到目标组。
- 在终止实例时，生命周期钩子用于触发 Lambda 函数，以便从目标组取消注册 threat defense virtual 实例。

Simple Notification Service (SNS)

- 来自 AWS 的 Simple Notification Service (SNS) 用于生成事件。
- 受限于 AWS 中的无服务器 Lambda 函数没有适合的编排器，因此该解决方案使用 SNS 作为一种函数链，以便基于事件来编排 Lambda 函数。

VPC

您应根据应用程序要求创建VPC。预计VPC具有一个互联网网关，而且至少有一个通过到互联网的路由连接的子网。有关安全组、子网等的要求，请参阅相应的部分。

安全组

在提供的 Auto Scale 组模板中允许所有连接。只需以下连接即可使 Auto Scale 解决方案发挥作用。

端口	使用方式	子网
8305	管理中心到 Threat Defense Virtual 安全隧道的连接	管理子网
运行状况探测端口（默认：8080）	面向互联网的负载均衡器运行状况探测器	外部、内部子网
应用程序端口	应用程序数据流量	外部、内部子网

管理中心实例的安全组或 ACL

需要这些信息才能在 lambda 函数和管理中心之间建立 HTTPS 连接。由于 lambda 函数将保存在以 NAT 网关作为默认路由的 lambda 子网中，因此应允许管理中心从 NAT 网关 IP 地址进行 HTTPS 入站连接。

子网

可以根据需要创建符合应用程序要求的子网。Threat Defense Virtual 需要 3 个子网才能运行。

注释 如果需要多个可用性区域支持，则每个区域都需要子网，因为子网是 AWS 云中的区域属性。

外部子网

外部子网应该具有能够通过“0.0.0.0/0”连接互联网网关的默认路由。这将包含 Threat Defense Virtual 的外部接口，而面向互联网的 NLB 将位于此子网中。

内部子网

这可能与具有或没有 NAT/互联网网关的应用程序子网类似。请注意，对于 Threat Defense Virtual 运行状况探测，应该可以通过端口 80 到达 AWS 元数据服务器 (169.254.169.254）。

注释 在此 Auto Scale 解决方案中，负载均衡器运行状况探测器会通过 inside/ Gig0/0 接口重定向到 AWS 元数据服务器。但是，您可以使用自己的应用为从负载均衡器发送到 Threat Defense Virtual 的运行状况探测连接进行更改。在这种情况下，您需要将 AWS 元数据服务器对象替换为应用 IP 地址，以提供运行状况探测响应。

管理子网

此子网包括 Threat Defense Virtual 管理接口。如果在此子网上使用管理中心，则为 Threat Defense Virtual 分配弹性 IP 地址 (EIP) 是可选的。诊断接口也位于此子网上。

Lambda 子网

AWS Lambda 函数需要使用 NAT 网关作为默认网关的两个子网。这使得 Lambda 函数将专用于 VPC。Lambda 子网不需要像其他子网一样的带宽。

应用程序子网

Auto Scale 解决方案对该子网没有限制，但如果应用程序需要 VPC 以外的出站连接，则应在该子网上配置相应的路由。这是因为出站发起的流量不会穿过负载均衡器。有关详细信息，请参阅《AWS 弹性负载均衡用户指南》。

无服务器组件

S3 桶

Amazon Simple Storage Service (Amazon S3) 是一项可提供行业领先可扩展性、数据可用性、安全性和性能的对象存储服务。您可以将所有必需的文件放在 S3 存储桶中。

部署模板时，将引用 S3 存储桶中的 zip 文件创建 Lambda 函数。因此，S3 存储桶应该能够供用户帐户访问。

GitHub 上的 CloudFormation 模板

为支持的 Auto Scale 解决方案提供了两组模板 - 一组用于使用网络负载均衡器 (NLB) 来设置 Auto Scale 解决方案，另一组用于使用网关负载均衡器 (GWLB) 来设置 Auto Scale 解决方案。

使用网络负载均衡器的 Auto Scale 解决方案

GitHub 上提供了以下模板：

- infrastructure.yaml
- deploy_ngfw_autoscale.yaml

表 *17:* 模板参数列表

参数	允许的值/类型	说明
PodNumber	字符串允许的模式：'^\d{1,3}$'	这是 pod 号。这将作为 Auto Scale 组名称 (threat defense virtual-Group-Name) 的后缀。例如，如果此值为“1”，则组名称将为 *threat defense virtual-Group-Name-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1。

参数	允许的值/类型	说明
AutoscaleGrpNamePrefix	字符串	这是 Auto Scale 组名称前缀。pod 号将作为后缀添加。 最大：18 个字符 示例：Cisco-threat defense virtual-1。
NotifyEmailID	字符串	Auto Scale 事件将被发送到此电子邮件地址。您需要接受订用电子邮件请求。 示例：admin@company.com。
VpcId	字符串	需要部署设备的 VPC ID。它应根据 AWS 要求配置。 类型：AWS::EC2::VPC::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LambdaSubnets	列表	将部署 Lambda 函数的子网。 类型：List<AWS::EC2::Subnet::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LambdaSG	列表	Lambda 函数的安全组。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
S3BktName	字符串	文件的 S3 存储桶名称。应根据 AWS 要求在您的帐户中配置此项。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LoadBalancerType	字符串	面向互联网的负载均衡器类型，可以是“application”或“network”。 示例：application

参数	允许的值/类型	说明
LoadBalancerSG	字符串	负载均衡器的安全组。如果是网络负载均衡器，则不会使用它。但您应提供一个安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LoadBalancerPort	整数	负载均衡器端口。此端口将在 LB 上以 HTTP/HTTPS 或 TCP/TLS 作为协议，并根据所选的负载均衡器类型打开。 确保端口是有效的 TCP 端口，它将用于创建负载均衡器侦听程序。 默认值：80
SSL证书	字符串	用于安全端口连接的 SSL 证书 ARN。如果未指定，则在负载均衡器上开启的端口将为 TCP/HTTP。如果已指定，则在负载均衡器上开启的端口将为 TLS/HTTPS。
TgHealthPort	整数	此端口供目标组用于运行状况探测。在 Threat Defense Virtual 上到达此端口的运行状况探测将被路由到 AWS 元数据服务器，并且不应用于流量。它应该是有效的 TCP 端口。 如果您希望应用本身回复运行状况探测，则可以为 Threat Defense Virtual 相应地更改 NAT 规则。在这种情况下，如果应用不响应，Threat Defense Virtual 将被标记为运行状况不正常，并会由于实例运行状况不佳警报而被删除。 示例：8080
AssignPublicIP	布尔值	如果选择“true”，则将分配公共 IP。如果是 BYOL 类型的 Threat Defense Virtual，则需要它才能连接到 https://tools.cisco.com。 示例：TRUE

参数	允许的值/类型	说明
InstanceType	字符串	Amazon Machine Image (AMI) 支持不同的实例类型，这些实例类型将决定实例的大小和所需的内存量。 只应使用支持 Threat Defense Virtual 的 AMI 实例类型。 示例：c4.2xlarge
LicenseType	字符串	Threat Defense Virtual 许可证类型，可以是 BYOL 或 PAYG。确保相关的 AMI ID 具有相同的许可类型。 示例：BYOL
AmiId	字符串	Threat Defense Virtual AMI ID（有效的 Cisco Threat Defense Virtual AMI ID）。 类型：AWS::EC2::Image::Id 请根据地区和所需的映像版本选择正确的AMI ID。Auto Scale 功能支持版本 6.4+、BYOL/PAYG映像。在两种情况下，您都应在 AWS Marketplace 中接受许可证。 如果是 BYOL，请使用诸如“BASE”、“MALWARE”、“THREAT”、“URLFilter”等功能更新 Configuration JSON 中的“licenseCaps”键值。
NoOfAZs	整数	Threat Defense Virtual 应跨越的可用性区域数，介于 1 到 3 之间。如果是 ALB 部署，根据 AWS 的要求，最小值为 2。 示例：2
ListOfAzs	逗号分隔的字符串	按顺序列出的逗号分隔区域列表。 **注释** 它们的列出顺序十分重要。应按相同的顺序给出子网列表。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：us-east-1a, us-east-1b, us-east-1c

参数	允许的值/类型	说明
MgmtInterfaceSG	字符串	Threat Defense Virtual 管理接口的安全组。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
InsideInterfaceSG	字符串	Threat Defense Virtual 内部接口的安全组。 类型：AWS::EC2::SecurityGroup::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
OutsideInterfaceSG	字符串	Threat Defense Virtual 外部接口的安全组。 类型：AWS::EC2::SecurityGroup::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-0c190a824b22d52bb
MgmtSubnetId	逗号分隔列表	逗号分隔的管理子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
InsideSubnetId	逗号分隔列表	逗号分隔的内部 /Gig0/0 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
OutsideSubnetId	逗号分隔列表	逗号分隔的外部 /Gig0/1 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。

参数	允许的值/类型	说明
KmsArn	字符串	现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。如果指定，管理中心和 Threat Defense Virtual 密码应加密。密码加密应仅使用指定的 ARN 进行。 生成加密密码示例：“aws kms encrypt --key-id <KMS ARN> --纯文本 <密码>” 请按照所示使用生成的密码。 示例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e
ngfwPassword	字符串	所有 Threat Defense Virtual 实例都提供一个默认密码，该密码在启动模板（Autoscale 组）的 *Userdata* 字段中输入。 一旦 Threat Defense Virtual 可访问，此输入会将密码更改为新提供的密码。 如果未使用 KMS ARN，请使用纯文本密码。如果使用 KMS ARN，则应使用加密的密码。 示例：Cisco123789! 或 AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	数字字符串	用于管理 Threat Defense Virtual 的 IP 地址，Lambda 函数和 Threat Defense Virtual 管理接口均可访问该地址。 示例：10.10.17.21
fmcOperationsUsername	字符串	在管理 Threat Defense Virtual 时创建的网络管理员或更高权限用户。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中有关创建用户和角色的信息。 示例：apiuser-1
fmcOperationsPassword	字符串	如果未提及 KMS ARN，请使用纯文本密码。如果已提及，则应使用加密的密码。 示例：Cisco123@ 或 AQICAHgcQAtz/hvaxMtJvY/x/mKI3dFPpSXUHQRnCAajB
fmcDeviceGrpName	字符串	管理中心设备组名称。 示例：AWS-Cisco-NGFW-VMs-1

参数	允许的值/类型	说明
fmc 性能许可证层	字符串	在 Management Center Virtual 上注册 threat defense virtual 设备时使用的性能层许可证。 允许的值：FTDv/FTDv5/FTDv10/FTDv20/FTDv30/FTDv50/FTDv100
fmcPublishMetrics	布尔值	如果设置为“TRUE”，则将创建一个 Lambda 函数，该函数每 2 分钟运行一次，将获取所提供的设备组中已注册 Threat Defense Virtual 传感器的内存消耗情况。 允许的值：TRUE、FALSE 示例：TRUE
fmcMetricsUsername	字符串	用于向 AWS CloudWatch 进行指标发布的唯一管理中心用户名。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中有关创建用户和角色的信息。 如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：publisher-1
fmcMetricsPassword	字符串	用于向 AWS CloudWatch 进行指标发布的管理中心密码。如果未提及 KMS ARN，请使用纯文本密码。如果已提及，则应使用加密的密码。 如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：Cisco123789!
CpuThresholds	逗号分隔的整数	下限 CPU 阈值和上限 CPU 阈值。最小值为 0，最大值为 99。 默认值：10、70 请注意，下限阈值应小于上限阈值。 示例：30、70

参数	允许的值/类型	说明
MemoryThresholds	逗号分隔的整数	下限 MEM 阈值和上限 MEM 阈值。最小值为 0，最大值为 99。 默认值：40、70 请注意，下限阈值应小于上限阈值。如果“fmcPublishMetrics”参数为“FALSE”，则它不起作用。 示例：40、50
实例元数据服务版本	布尔值	要为 Threat Defense Virtual 实例启用的实例元数据数据服务 (IMDS) 版本。 • V1 和 V2（令牌可选）：启用 IMDSv1 或 IMDSv2 或 IMDSv1 和 IMDSv2 API 调用的组合。 • 仅 V2（需要令牌）：仅启用 IMDSv2 模式。 **注释** Threat Defense Virtual 版本 7.6 及更高版本仅支持 IMDSv2 服务。 如果要为 7.6 以前的版本启用 IMDSv2 服务，则必须选择 IMDSv1 和 IMDSv2 **V1 和 V2**（**可选令牌**）参数组合。 **注释** 如果您使用的是自定义模板（非思科提供），请注意，您必须在模板的 **MetadataOptions** 下包含 **HttpEndpoint: enabled** 和 **HttpTokens: required** 属性，然后才能启用 IMDSv2 必需模式。

使用网关负载均衡器的 Auto Scale 解决方案

GitHub 上提供了以下模板：

- infrastructure_gwlb.yaml
- deploy_ngfw_autoscale_with_gwlb.yaml

表 *18:* 模板参数列表

参数	允许的值/类型	说明
DeploymentType	字符串	帮助处理从 threat defense virtual 到 GWLB 或互联网流量的部署类型。 • 单臂：此部署类型启用 threat defense virtual 以在检测后将流量返回到 AWS GWLB（掉头）。默认情况下，如果未指定，则代理类型设置为单臂。 • 双臂：此部署类型使 threat defense virtual 能够执行网络地址转换 (NAT)，然后将出站流量从其外部接口通过 NAT 网关转发到互联网。
PodNumber	字符串 允许的模式：'^\d{1,3}$'	这是 pod 号。这将作为 Auto Scale 组名称 (threat defense virtual-Group-Name) 的后缀。例如，如果此值为“1”，则组名称将为 *threat defense virtual-Group-Name-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1
AutoscaleGrpNamePrefix	字符串	这是 Auto Scale 组名称前缀。pod 号将作为后缀添加。 最大：18 个字符 示例：Cisco-threat defense virtual-1
NotifyEmailID	字符串	Auto Scale 事件将被发送到此电子邮件地址。您需要接受订用电子邮件请求。 示例：admin@company.com
VpcId	字符串	需要部署设备的 VPC ID。它应根据 AWS 要求配置。 类型：AWS::EC2::VPC::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LambdaSubnets	列表	将部署 Lambda 函数的子网。 类型：List<AWS::EC2::Subnet::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。

参数	允许的值/类型	说明
LambdaSG	列表	Lambda 函数的安全组。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
S3BktName	字符串	文件的 S3 存储桶名称。应根据 AWS 要求在您的帐户中配置此项。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LoadBalancerType	字符串	面向互联网的负载均衡器类型，可以是“application”或“network”。 示例：application
LoadBalancerSG	字符串	负载均衡器的安全组。如果是网络负载均衡器，则不会使用它。但您应提供一个安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
LoadBalancerPort	整数	负载均衡器端口。此端口将在 LB 上以 HTTP/HTTPS 或TCP/TLS 作为协议，并根据所选的负载均衡器类型打开。 确保端口是有效的TCP端口，它将用于创建负载均衡器侦听程序。 默认值：80
SSL证书	字符串	用于安全端口连接的 SSL 证书 ARN。如果未指定，则在负载均衡器上开启的端口将为 TCP/HTTP。如果已指定，则在负载均衡器上开启的端口将为 TLS/HTTPS。

参数	允许的值/类型	说明
TgHealthPort	整数	此端口供目标组用于运行状况探测。在 threat defense virtual 上到达此端口的运行状况探测将被路由到 AWS 元数据服务器，并且不应用于流量。它应该是有效的 TCP 端口。 如果您希望应用本身回复运行状况探测，则可以为 threat defense virtual 相应地更改 NAT 规则。在这种情况下，如果应用不响应，threat defense virtual 将被标记为运行状况不正常，并会由于实例运行状况不佳警报而被删除。 示例：8080
AssignPublicIP	布尔值	如果选择“true”，则将分配公共 IP。如果是 BYOL 类型 threat defense virtual，则需要它才能连接到 https://tools.cisco.com。 示例：TRUE
InstanceType	字符串	Amazon Machine Image (AMI) 支持不同的实例类型，这些实例类型将决定实例的大小和所需的内存量。 只应使用支持 threat defense virtual 的 AMI 实例类型。 示例：c4.2xlarge
LicenseType	字符串	threat defense virtual 许可证类型，可以是 BYOL 或 PAYG。确保相关的 AMI ID 具有相同的许可类型。 示例：BYOL
AmiId	字符串	threat defense virtual AMI ID（有效的思科 threat defense virtual AMI ID）。 类型：AWS::EC2::Image::Id 请根据地区和所需的映像版本选择正确的 AMI ID。Auto Scale 功能支持版本 6.4+、BYOL/PAYG 映像。在两种情况下，您都应在 AWS Marketplace 中接受许可证。 如果是 BYOL，请使用诸如“BASE”、“MALWARE”、“THREAT”、“URLFilter”等功能更新 Configuration JSON 中的“licenseCaps”键值。
NoOfAZs	整数	threat defense virtual 应跨越的可用性区域数，介于 1 到 3 之间。如果是 ALB 部署，根据 AWS 的要求，最小值为 2。 示例：2

参数	允许的值/类型	说明
ListOfAzs	逗号分隔的字符串	按顺序列出的逗号分隔区域列表。 **注释** 它们的列出顺序十分重要。应按相同的顺序给出子网列表。 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：us-east-1a, us-east-1b, us-east-1c
MgmtInterfaceSG	字符串	threat defense virtual 管理接口的安全组。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
InsideInterfaceSG	字符串	threat defense virtual 内部接口的安全组。 类型：AWS::EC2::SecurityGroup::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
OutsideInterfaceSG	字符串	threat defense virtual 外部接口的安全组。 类型：AWS::EC2::SecurityGroup::Id 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-0c190a824b22d52bb
MgmtSubnetId	逗号分隔列表	逗号分隔的管理子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
InsideSubnetId	逗号分隔列表	逗号分隔的内部 /Gig0/0 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。

参数	允许的值/类型	说明
OutsideSubnetId	逗号分隔列表	逗号分隔的外部 /Gig0/1 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 类型：List<AWS::EC2::SecurityGroup::Id> 如果使用“*infrastructure.yaml*”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。
KmsArn	字符串	现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。如已指定，管理中心 和 threat defense virtual 密码应加密。密码加密应仅使用指定的 ARN 进行。 生成加密密码示例：“aws kms encrypt --key-id <KMS ARN> --纯文本 <密码>” 请按照所示使用生成的密码。 示例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e
ngfwPassword	字符串	所有 threat defense virtual 实例都提供一个默认密码，该密码在启动模板（Autoscale 组）的 *Userdata* 字段中输入。 一旦 threat defense virtual 可访问，此输入会将密码更改为新提供的密码。 如果未使用 KMS ARN，请使用纯文本密码。如果使用 KMS ARN，则应使用加密的密码。 示例：Cisco123789! 或 AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	数字字符串	用于管理 管理中心 的 IP 地址，Lambda 函数和 threat defense virtual 管理接口均可访问该地址。 示例：10.10.17.21
fmcOperationsUsername	字符串	在管理 管理中心 时创建的网络管理员或更高权限用户。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中有关创建用户和角色的信息。 示例：apiuser-1
fmcOperationsPassword	字符串	如果未提及 KMS ARN，请使用纯文本密码。如果已提及，则应使用加密的密码。 示例：Cisco123@ 或 AQICAHgcQAtz/hvaxMtJvY/x/rnKI3clFPpSXUHQRnCAajB

参数	允许的值/类型	说明
fmcDeviceGrpName	字符串	管理中心 设备组名称。 示例：AWS-Cisco-NGFW-VMs-1
fmc 性能许可证层	字符串	在 Management Center Virtual 上注册 threat defense virtual 设备时使用的性能层许可证。 允许的值：FTDv/FTDv20/FTDv30/FTDv50/FTDv100 注释 FTDv5 和 FTDv10 性能级别许可证不支持与 AWS 网关负载均衡器配合使用。
fmcPublishMetrics	布尔值	如果设置为“TRUE”，则将创建一个 Lambda 函数，该函数每 2 分钟运行一次，将获取所提供的设备组中已注册 threat defense virtual 传感器的内存消耗情况。 允许的值：TRUE、FALSE 示例：TRUE
fmcMetricsUsername	字符串	用于向 AWS CloudWatch 进行指标发布的唯一 管理中心 用户名。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中有关创建用户和角色的信息。 如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：publisher-1
fmcMetricsPassword	字符串	用于向 AWS CloudWatch 进行指标发布的 管理中心 密码。如果未提及 KMS ARN，请使用纯文本密码。如果已提及，则应使用加密的密码。 如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：Cisco123789!
CpuThresholds	逗号分隔的整数	下限 CPU 阈值和上限 CPU 阈值。最小值为 0，最大值为 99。 默认值：10、70 请注意，下限阈值应小于上限阈值。 示例：30、70

参数	允许的值/类型	说明
MemoryThresholds	逗号分隔的整数	下限 MEM 阈值和上限 MEM 阈值。最小值为 0，最大值为 99。 默认值：40、70 请注意，下限阈值应小于上限阈值。如果“fmcPublishMetrics”参数为“FALSE”，则它不起作用。 示例：40、50
实例元数据服务版本	布尔值	要为 Threat Defense Virtual 实例启用的实例元数据数据服务 (IMDS) 版本： • V1 和 V2（令牌可选）：启用 IMDSv1、IMDSv2 或 IMDSv1 和 IMDSv2 API 调用的组合。 • 仅 V2（需要令牌）：仅启用 IMDSv2 模式。 **注释** Threat Defense Virtual 7.6 及更高版本仅支持 IMDSv2。 如果要为 7.6 以前的版本启用 IMDSv2 服务，则必须选择 IMDSv1 和 IMDSv2 **V1 和 V2**（**可选令牌**）参数组合。 **注释** 如果您使用的是自定义模板（非思科提供），请注意，您必须在模板的 **MetadataOptions** 下包含 **HttpEndpoint: enabled** 和 **HttpTokens: required** 属性，然后才能启用 IMDSv2 必需模式。

将所需文件和 CFT 从 GitHub 下载到本地主机

从 GitHub 下载 **lambda-python-files** 文件夹。此文件夹包含以下文件：

- 用于创建 Lambda 层的 Python (.py) 文件。
- 一个 configuration.json 文件，用于根据需要添加静态路由和自定义任何网络参数。

从 GitHub 下载以下 CloudFormation 模板：

- 使用 NLB 的 Auto Scale 解决方案的模板 -
  - **Infrastructure.yaml** - 用于自定义 AWS 环境中的组件。
  - **deploy_ngfw_autoscale.yaml** - 用于部署使用 NLB 的 AWS Auto Scale 解决方案。

- 使用 GWLB 的 Auto Scale 解决方案模板 -
  - **Infrastructure_gwlb.yaml -** 用于自定义 AWS 环境中的组件。
  - **deploy_ngfw_autoscale_with_gwlb.yaml -** 用于部署具有 GWLB 的 AWS Auto Scale 解决方案。

注释 尽可能收集模板参数的值。这样可以在 AWS 管理控制台上部署模板时更轻松快速地输入值。

使用 NLB 的 Auto Scale 解决方案 - 在 Amazon CloudFormation 控制台上自定义和部署 NLB 基础设施模板

如果您使用 NLB 来部署 Auto Scale 解决方案，请执行本节中提供的步骤。

过程

步骤 1 在 AWS 管理控制台上，转到**服务 (Services)** > **管理和治理 (Management and Governance)** > **CloudFormation**，然后点击**创建堆栈 (Create stack)** > **使用新资源（标准）(With new resources[standard])**。

步骤 2 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从下载文件的文件夹中选择 **infrastructure.yaml**。

步骤 3 点击**下一步**。

步骤 4 在**指定堆栈详细信息 (Specify stack details)** 页面上，输入堆栈的名称。

步骤 5 为 ***infrastructure.yaml*** 模板中的输入参数提供值。

步骤 6 点击**下一步**。

步骤 7 在**配置堆栈选项 (Configure Stack Options)** 窗口中点击**下一步 (Next)**。

步骤 8 在**查看 (Review)** 页面上，查看并确认设置。

步骤 9 点击**创建堆栈 (Create Stack)** 以部署 **infrastructure.yaml** 模板并创建堆栈。

步骤 10 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **S3 Bucket Name**。

使用 GWLB 的 Auto Scale 解决方案 - 在 Amazon CloudFormation 控制台上自定义和部署 GWLB 基础设施模板

如果您使用 GWLB 来部署 Auto Scale 解决方案，请执行本节中提供的步骤。

过程

步骤 1 在 AWS 管理控制台上，转到**服务 (Services)** > **管理和治理 (Management and Governance)** > **CloudFormation**，然后点击**创建堆栈 (Create stack)** > **使用新资源（标准）(With new resources[standard])**。

步骤 2 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从下载文件的文件夹中选择 **Infrastructure_gwlb.yaml**。

步骤 3 点击**下一步**。

步骤 4 在**指定堆栈详细信息 (Specify stack details)** 页面上，输入堆栈的名称。

步骤 5 为 ***infrastructure_gwlb.yaml*** 模板中的输入参数提供值。

步骤 6 点击**下一步**。

步骤 7 在**配置堆栈选项 (Configure Stack Options)** 窗口中点击**下一步 (Next)**。

步骤 8 在**查看 (Review)** 页面上，查看并确认设置。

步骤 9 点击**创建堆栈 (Create Stack)** 以部署 **Infrastructure_gwlb.yaml** 模板并创建堆栈。

步骤 10 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **S3 Bucket Name**。

在管理中心配置网络基础设施

在管理中心为已注册的 Threat Defense Virtual 创建和配置设备丢弃、对象、运行状况检查端口、NAT 策略和访问策略。

您可以使用管理中心来管理 Threat Defense Virtual，前者是位于单独服务器上功能齐全的多设备管理器。Threat Defense Virtual 向您分配给 Threat Defense Virtual 虚拟机的管理接口上的 Threat Defense Virtual 注册并与之通信。

有关详细信息，请参阅关于使用安全防火墙管理中心的虚拟安全防火墙威胁防御。

用于 Threat Defense Virtual 配置的所有对象均应由用户创建。

重要事项 应创建一个设备组，然后应对其应用规则。设备组上应用的所有配置都将被推送到 Threat Defense Virtual 实例。

添加设备组

管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。您可以展开和折叠组中的设备列表。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。

步骤 3 要编辑现有的组，请点击要编辑的组的“编辑”（编辑图标）。

步骤 4 输入 **Name**。

步骤 5 在**可用设备 (Available Devices)** 下，选择一台或多台要添加到设备组的设备。点击的同时使用 **Ctrl** 或 **Shift** 选择多台设备。

步骤 6 点击**添加 (Add)** 将所选设备包含在设备组中。

步骤 7 点击**确定 (OK)** 以添加组。

创建主机对象

开始之前

使用 AWS 网络负载均衡器 (NLB) 时，必须创建主机对象。但是，在使用网关负载均衡器 (GWLB) 时，无需在 AWS 中创建主机对象，因为 GWLB 提供透明的服务插入。

过程

步骤 1 登录管理中心。

步骤 2 选择**对象** > **对象管理**。

步骤 3 从对象类型列表中选择**网络 (Network)**。

步骤 4 从**添加网络 (Add Network)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 5 输入 **Name**。

步骤 6 输入说明。

步骤 7 在**网络 (Network)** 字段中，选择**主机 (Host)** 选项并输入以下值。

a) 对象类型的名称，例如 **aws-metadata-server**。

b) 根据主机协议的类型，输入 IPv4 的以下 IP 地址：**169.254.169.254**。

步骤 8 点击**保存 (Save)**。

创建端口对象

开始之前

使用 AWS 网络负载均衡器 (NLB) 时，您必须创建端口对象。但是，在使用网关负载均衡器 (GWLB) 时，无需在 AWS 中创建端口对象，因为 GWLB 提供透明的服务插入。

过程

步骤 1 登录管理中心。

步骤 2 选择**对象** > **对象管理**。

步骤 3 从对象类型列表中选择**端口 (Port)**。

步骤 4 从**添加端口 (Add Port)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 5 输入 **Name**。

步骤 6 选择**协议 (Protocol)**。您必须选择已为主机对象类型输入的协议。根据选择的协议，按**端口 (Port)** 进行限制，或者选择 ICMP **类型 (Type)** 和**代码 (Code)**。

步骤 7 输入 **8080**。请注意，您可以根据需要自定义在此处输入的端口号。

注释
如果选择与所有协议匹配，则必须使用**其他 (Other)** 下拉列表按端口限制对象。

步骤 8 点击**保存 (Save)**。

创建安全区域和接口组对象

过程

步骤 1 选择**对象** > **对象管理**。

步骤 2 从对象类型列表中选择**接口**。

步骤 3 点击**添加 (Add)** > **安全区域 (Security Zone)** 或**添加 (Add)** > **接口组 (Interface Group)**。

步骤 4 输入 **名称** - *inside-sz/outside-sz*。

步骤 5 选择**接口类型 (Interface Type)** - 已路由 *(Routed)*。

步骤 6 点击**保存 (Save)**。

为运行状况检查探测器启用端口

您可以为运行状况检查探测启用端口 22 (SSH) 或端口 443 (HTTP)。

为运行状况检查探测器启用端口 22 (SSH)

如果将端口 22 (SSH) 用于运行状况检查探测，请执行以下程序为运行状况检查探测启用端口。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)** > **SSH 访问 (SSH Access)**。
步骤 2 点击 **+ 添加**。
步骤 3 从下拉列表中选择任意 **IP 地址**。
步骤 4 从**可用区域/接口 (Available Zones/Interfaces)** 窗口中，选择连接到 GWLB 的外部接口或外部子网。
步骤 5 点击**添加 (Add)** 以将该接口添加到**所选区域/接口 (Selected Zones/Interfaces)** 窗口。
步骤 6 点击**确定 (OK)**。
步骤 7 点击**保存 (Save)**。

为运行状况检查探测器启用端口 443 (HTTP)

如果将端口 443 (HTTP) 用于运行状况检查探测，请执行以下程序为运行状况检查探测启用端口。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)** > **HTTP 访问 (HTTP Access)**。
步骤 2 选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框。
步骤 3 在**端口 (Port)** 字段中输入 **443**。
步骤 4 点击 **+ 添加**。
步骤 5 从下拉列表中选择相关 **IP 地址**。
步骤 6 从**可用区域/接口 (Available Zones/Interfaces)** 窗口中，选择连接到 GWLB 的外部接口或外部子网。
步骤 7 点击**添加 (Add)** 以将该接口添加到**所选区域/接口 (Selected Zones/Interfaces)** 窗口。
步骤 8 点击**确定 (OK)**。
步骤 9 点击**保存 (Save)**。

采用 NLB 的 Auto Scale 解决方案 - 配置和部署网络地址转换 (NAT) 策略

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (PAT)。有关 NAT 策略的信息，请参阅使用 Cisco Secure Firewall Management Center 管理 Cisco Secure Firewall Threat Defense Virtual 中的配置 NAT。

您的 NAT 策略中必须有一个强制规则。NAT 规则示例如下：

- 源区域：外部区域
- 目标区域：内部区域
- 原始源：任意 ipv4
- 原始源端口：原始/默认
- 原始目标：接口
- 原始目标端口：8080/或用户配置的任何运行状况端口
- 转换后的源：any-ipv4
- 转换后的源端口：原始/默认
- 转换后的目标：aws-metadata-server
- 已转换的目标端口：80/HTTP

同样，可以添加任何数据流量 NAT 规则，以便将此配置推送到 Threat Defense Virtual 设备。

重要事项	创建的 NAT 策略应应用于设备组。来自 Lambda 函数的管理中心验证会对此进行验证。

过程

步骤 1 登录 Cisco Secure Firewall Management Center。

步骤 2 在**设备 (Devices)** 菜单中，点击 **NAT**。

步骤 3 点击**新建策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)** 以创建新策略。

步骤 4 输入 NAT 策略的名称和描述。

步骤 5 点击**保存 (Save)**。

您可以看到 NAT 页面上已添加并列出了一个新策略。

步骤 6 点击**添加规则 (Add Rule)**。

步骤 7 从 **NAT 规则 (NAT Rule)** 下拉列表中选择 **手动 NAT 规则 (Manual NAT Rule)**。

步骤 8 从“插入”(Insert) 下拉列表中选择**按类别 (In Category)** 和**之前的 NAT 规则 (NAT Rule Before)**。

步骤 9 从**类型 (Type)** 下拉菜单中选择**静态 (Static)**。

步骤 10 输入说明。

步骤 11 在**接口对象 (Interface Objects)** 菜单中，添加源对象和目标对象。

步骤 12 在**转换 (Translations)** 菜单中，为每个参数添加以下值。

参数	值
起始源	any-ipv4

参数	值
原始目标	地址 (Address)
原始源端口	HTTP
原始目标端口	8080
转换后的源	any-ipv4
转换后的源端口	原始/默认
转换目标	aws-metadata-server
转换后的目标端口	80/HTTP

步骤 13 点击**保存 (Save)** 以保存并添加规则。

步骤 14 选择已创建的新规则以部署在 Threat Defense Virtual 设备上。

步骤 15 点击**部署 (Deploy)** > **部署 (Deployment)** 将策略部署到分配的设备。在部署更改之后，更改才生效。

创建基本访问控制策略

配置访问控制以允许从内部到外部的流量。可以创建具有所有必需策略的访问策略，应允许运行状况端口对象，以便允许此端口上的流量到达。有关访问策略的信息，请参阅使用 Cisco Secure Firewall Management Center 管理 Cisco Secure Firewall Threat Defense Virtual 中的配置访问控制。

创建新的访问控制策略时，它包含默认操作和设置。创建策略后，您会立即进入编辑会话，以便您可以调整策略以满足您的要求。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**新建策略**。

步骤 3 输入唯一的名称和说明。

步骤 4 指定初始**默认操作 (Default Action)** - **阻止所有流量 (Block all traffic)**。

步骤 5 点击**保存 (Save)**。

步骤 6 点击您创建的新策略的**编辑**图标。

步骤 7 点击**添加规则 (Add Rule)**。

步骤 8 设置以下参数：

- 名称：inside-to-outside
- 插入：到强制

- Action: Allow
- 添加源区域和目标区域。

步骤 9 点击**应用**。

更新 configuration.json 文件

configuration.json 文件位于您从 GitHub 下载的 **lambda_python_files** 文件夹中。使用您在管理中心设置的参数来更新 **configuration.json** 文件中的参数。请注意，不应更改 JSON 键值。

configuration.json 文件中的脚本如下所示。

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],   //Management center virtual licenses
  "fmcIpforDeviceReg": "DONTRESOLVE",   //Management center virtual IP address
  "RegistrationId": "cisco",  //Registration ID used while configuring the manager in the
Threat defense virtual
  "NatId": "cisco",  //NAT ID used while configuring the manager in the Threat defense
virtual
  "fmcAccessPolicyName": "aws-asg-policy",  //Access policy name configured in the Management
 center virtual
  "fmcNatPolicyName": "AWS-Cisco-NGFW-VMs",  //NAT Policy name configured in the Management
 center virtual (Not required for GWLB-based deployment)
  "fmcInsideNicName": "inside", //Threat defense virtual inside interface name
  "fmcOutsideNicName": "outside", //Threat defense virtual outside interface name
  "fmcInsideNic": "GigabitEthernet0/0", //Threat defense virtual inside interface NIC Name
 - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance types)
  "fmcOutsideNic": "GigabitEthernet0/1", //Threat defense virtual outside interface NIC
Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance types
  "fmcOutsideZone": "Outside-sz", //Outside Interface security zone name that is set in the
 Management center virtual
  "fmcInsideZone": "Inside-sz", //Inside Interface security zone name that is set in the
Management center virtual
  "MetadataServerObjectName": "aws-metadata-server", //Host object name created for the IP
 169.254.169.254 in the Management center virtual  (Not required for GWLB-based deployment)

  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Inside-sz"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Outside-sz"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
```

```
    }
  ],  //Interface-related configuration
  "trafficRoutes": [
    {
      "interface": "inside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "1"
    }
  ] //This traffic route is used for the Threat defense virtual instance's health check
}
```

您可以通过修改此文件中的 **trafficRoutes** 参数，为 Threat Defense Virtual 配置静态路由。静态路由配置示例如下所示。

```
{
      "interface": "inside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "1"
 }
```

使用 AWS CLI 配置基础设施组件

模板不会为 Threat Defense Virtual 和管理中心创建 Lambda 层和加密密码。使用下面给出的程序配置这些组件。有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面。

创建 Lambda 层 Zip 文件以管理计算资源

在 Linux 主机上创建 python 文件夹，然后创建 Lambda 层。

过程

步骤 1 在 Linux 主机（例如 Ubuntu 22.04）中创建 python 文件夹。

步骤 2 在 Linux 主机上安装 Python 3.9。下面提供了安装 Python 3.9 的示例脚本。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

步骤 3 在 Linux 环境中创建 Lambda 层 zip 文件 *autoscale_layer.zip*。此文件为 Lambda 函数提供必要的 Python 库。

运行以下脚本以创建 *autoscale_layer.zip* 文件。

```
#!/bin/bash
mkdir -p layer
mkdir -p python
virtualenv -p /usr/bin/python3.9 ./layer/
```

```
source ./layer/bin/activate
pip3 install attrs==23.1.0
pip3 install bcrypt==3.2.2
pip3 install certifi==2022.12.7
pip3 install cffi==1.15.1
pip3 install chardet==3.0.4
pip3 install cryptography==2.9.1
pip3 install idna==2.10
pip3 install jsonschema==3.2.0
pip3 install paramiko==2.7.1
pip3 install pycparser==2.21
pip3 install pycryptodome==3.15.0
pip3 install PyNaCl==1.5.0
pip3 install pyrsistent==0.19.3
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install six==1.16.0
pip3 install urllib3==1.25.11
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

注释

如果在安装期间遇到依赖项冲突错误（例如 urllib3 或加密），建议您包含冲突软件包及其建议版本。之后，您可以再次运行安装来解决冲突。

步骤 4 在创建 **autoscale_layer.zip** 文件后，将 **autoscale_layer.zip** 文件复制到从 GitHub 下载的 **lambda-python-files** 文件夹中。

（可选）为 Threat Defense Virtual和管理中心创建加密密码

如果已在 Infrastructure_gwlb.yaml 模板文件中输入 KMS ARN 值，则必须加密您在 Threat Defense Virtual 和管理中心中设置的密码。请参阅查找密钥 ID 和密钥 ARN，以使用 AWS KMS 控制台来识别密钥 ARN。在本地主机上，运行以下 AWS CLI 命令加密密码。

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext
'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXH
JAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45
AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

“CiphertextBlob”的值是加密密码。将此密码用作 **Infrastructure_gwlb.yaml** 文件中 **NGFWv 密码**（Threat Defense Virtual 密码）或 **AutoScale 自动化的 FMC 密码**（管理中心密码）参数的值。您还可以将此密码用作**将指标发布到 CloudWatch 的 FMC 密码**的值。

创建目标文件夹

在本地主机上，使用下面提供的命令创建一个目标文件夹，其中包含必须上传到 Amazon S3 存储桶的文件。

python3 make.py build

这将在本地主机上创建一个名为“target”的文件夹。target 文件夹包含部署 Auto Scale 解决方案所需的 *zip* 文件和 *yaml* 文件。

将文件上传到 Amazon S3 存储桶

在本地主机上，使用下面给出的命令将目标目录中的所有文件上传到 Amazon S3 存储桶。

$ cd ./target

$ aws s3 cp . s3://<*bucket-name*> **--recursive**

支持 NLB 的 Auto Scale 解决方案 - 部署支持 NLB 的 Auto Scale 解决方案

如果您使用 NLB 来部署 Auto Scale 解决方案，请执行本节中提供的步骤。

过程

步骤 1 在 AWS 管理控制台上，转至**服务 (Services)** > **管理和监管 (Management and Governance)** > **CloudFormation** > **堆栈**，然后点击模板创建的堆栈。

步骤 2 点击**创建堆栈 (Create stack)** > **通过新资源（标准）(With new resources [standard])**。

步骤 3 选择**上传模板 (Upload a template)** 文件，点击**选择 (Choose)** 以选择文件，然后从目标文件夹中选择 ***deploy_ngfw_autoscale.yaml***。

步骤 4 点击**下一步**。

步骤 5 在**指定堆栈详细信息 (Specify stack details)** 页面上，输入堆栈的名称。

步骤 6 为 ***deploy_ngfw_autoscale.yaml*** 模板中的输入参数提供值。

步骤 7 在**配置堆栈选项 (Configure Stack Options)** 窗口中点击**下一步 (Next)**。

步骤 8 在**查看 (Review)** 页面上，查看并确认设置。

步骤 9 点击 **创建堆栈** 以部署 ***deploy_ngfw_autoscale.yaml*** 模板并创建堆栈。

这样就完成了为使用 NLB 的 Threat Defense Virtual 设置自动扩展解决方案所需的两个模板的部署。

支持 GWLB 的 Auto Scale 解决方案 - 部署支持 GWLB 的 Auto Scale 解决方案

如果您使用 GWLB 来部署 Auto Scale 解决方案，请执行本节中提供的步骤。

过程

步骤 1 在 AWS 管理控制台上，转至**服务 (Services)** > **管理和监管 (Management and Governance)** > **CloudFormation** > **堆栈**，然后点击模板创建的堆栈。

步骤 2 点击**创建堆栈 (Create stack)** > **通过新资源（标准）(With new resources [standard])**。

步骤 3 选择**上传模板 (Upload a template)** 文件，点击**选择 (Choose)** 以选择文件，然后从目标文件夹中选择 ***deploy_ngfw_autoscale_with_gwlb.yaml***。

步骤 4 点击**下一步**。

步骤 5 在**指定堆栈详细信息 (Specify stack details)** 页面上，输入堆栈的名称。

步骤 6 为 ***deploy_ngfw_autoscale_with_gwlb.yaml*** 模板中的输入参数提供值。

步骤 7 在**配置堆栈选项 (Configure Stack Options)** 窗口中点击**下一步 (Next)**。

步骤 8 在**查看 (Review)** 页面上，查看并确认设置。

步骤 9 点击**创建堆栈 (Create Stack)** 以部署 ***deploy_ngfw_autoscale_with_gwlb.yaml*** 模板并创建堆栈。

这样就完成了为使用 GWLB 的Threat Defense Virtual 设置自动扩展解决方案所需的两个模板的部署。

带有 GWLB 的 Auto Scale 解决方案 - 创建 GWLB 终端

如果您使用 GWLB 来部署 Auto Scale 解决方案，请执行本节中提供的步骤。

过程

步骤 1 在 AWS 管理控制台上，转至**服务 (Services)** > **网络和内容交付 (Networking & Content Delivery)** > **VPC** > **终端服务 (Endpoint Services)**。

步骤 2 点击**创建终端服务 (Create Endpoint Service)**

步骤 3 在“负载均衡器”(Load balancer) 类型下，选择**网关 (Gateway)**。

步骤 4 在**可用的负载均衡器 (Available load balancers)** 下，选择作为 Auto scale 部署的一部分创建的网关负载均衡器。

步骤 5 在**要求接受终端 (Require accepting for endpoint)** 下，选择**需要接受 (Acceptance required)**。这可确保您必须手动接受任何终端服务连接请求。

步骤 6 在**支持的 IP 地址类型 (Supported IP address types)** 下，选择 **IPv4**。

步骤 7 点击**创建 (Create)**。

步骤 8 复制新创建的终端服务的服务名称。

步骤 9 转至**服务 (Services)** > **网络和内容交付 (Networking & Content Delivery)** > **VPC** > **终端 (Endpoints)**。

步骤 10 点击**创建终端 (Create endpoint)**。

步骤 11 在**服务类别 (Service category)** 下，选择**其他终端服务 (Other endpoint services)**。

步骤 12 对于**服务名称 (Service name)**，输入服务的名称，然后选择**验证服务 (Verify service)**。

步骤 13 在 **VPC** 字段中，选择要在其中创建终端的 VPC。

步骤 14 在**子网 (Subnets)**下，选择要在其中创建终端的子网。

步骤 15 对于 IP 地址类型，请选择 IPv4 选项以将 IPv4 地址分配给终端网络接口。

步骤 16 点击**创建终端 (Create endpoint)**。

为 VPC 配置路由

过程

步骤 1 在 AWS 管理控制台上，转到**服务 (Services)** > **网络和内容 (Networking & Content)** > **虚拟私有云 (Virtual Private Cloud)** > **路由表 (Route tables)**。

步骤 2 选择互联网网关的路由表并执行以下步骤：

1. 点击**操作 (Actions)** > **编辑路由 (Edit routes)**。
2. 对于 IPv4，请点击**添加路由 (Add route)**。对于**目标 (Destination)**，输入应用服务器子网的 IPv4 CIDR 块。对于**目标 (Target)**，选择 VPC 终端。
3. 点击**保存更改 (Save changes)**。

步骤 3 选择包含应用服务器的子网的路由表，并执行以下步骤：

1. 点击**操作 (Actions)** > **编辑路由 (Edit routes)**。
2. 对于 IPv4，请点击**添加路由 (Add route)**。对于**目标 (Destination)**，输入**0.0.0.0/0**。对于**目标 (Target)**，选择 VPC 终端。
3. 点击**保存更改 (Save changes)**。

步骤 4 选择带有网关负载均衡器终端的子网路由表，然后执行以下步骤：

1. 点击**操作 (Actions)** > **编辑路由 (Edit routes)**。
2. 对于 IPv4，请点击**添加路由 (Add route)**。对于**目标 (Destination)**，输入**0.0.0.0/0**。对于**目标 (Target)**，选择互联网网关。

3. 点击保存更改 **(Save changes)**。

编辑 Auto Scale 组

默认情况下，Auto Scale 组的最小和最大威胁防御虚拟实例数分别设置为 0 和 2。根据需要更改这些值。

过程

步骤 1 在 AWS 管理控制台上，转至服务 **(Services)** > 计算 **(Compute)** > **EC2**，然后点击自动扩展组 **(Auto Scaling Groups)**。

步骤 2 选择您创建的 自动扩展组，然后点击编辑 **(Edit)** 以根据您的要求修改所需容量 **(Desired capacity)**、最小容量 **(Minimum capacity)**、最大容量 **(Maximum capacity)** 字段中的值。这些值对应于要为自动扩展功能调出的 Threat Defense Virtual 实例的数量。将所需容量 **(Desired capacity)** 设置为介于最小和最大容量值之间的值。

步骤 3 点击更新。

注释 我们建议您仅启动一个 Threat Defense Virtual 实例，并验证此实例的行为是否符合预期。然后，您可以根据自己的要求启动更多实例。

验证部署

成功部署模板后，转到 Amazon CloudWatch 控制台以确保正在收集日志并创建了所需的警报。

日志

检查日志文件，以排除管理中心连接方面的任何问题。

过程

步骤 1 在 **AWS** 管理控制台上，转至服务 **(Services)** > 管理和监管 **(Management & Governance)** > **CloudWatch**。

步骤 2 点击日志组 **(Log groups)**，然后点击此处显示的任何日志组以查看日志。

警报

确保已在 Amazon CloudWatch 控制台上创建所需的警报。

过程

步骤 1 在 **AWS 管理**控制台上，转至**服务 (Services)** > **管理和监管 (Management & Governance)** > **CloudWatch**。

步骤 2 点击**警报 (Alarms)** > **所有警报 (All Alarms)** 以显示警报列表以及触发外向扩展和内向扩展函数的条件。

维护任务

扩展过程

本主题说明如何挂起、然后恢复 Auto Scale 组的一个或多个扩展过程。

开始和停止扩展操作

要开始和停止外向/内向扩展操作，请执行以下步骤。

- 对于 AWS 动态扩展 - 参阅以下链接，了解关于启用或禁用外向扩展操作的信息：

  挂起和恢复扩展过程

运行状况监控

每 60 分钟，CloudWatch Cron 作业会触发运行状况医生模块的 Auto Scale 管理器 Lambda：

- 如果有属于有效 threat defense virtual VM 的不正常 IP，且 threat defense virtual 超过了一小时，则该实例将被删除。
- 如果这些 IP 不是来自有效的 threat defense virtual机，则仅从目标组中删除 IP。

运行状况监控器还会验证设备组、访问策略和 NAT 规则的 管理中心 配置。如果 IP/实例运行状况不正常，或者 管理中心 验证失败，则运行状况监控器会向用户发送邮件。

禁用运行状况监控器

要禁用运行状况监控器，请在 ***constant.py*** 中将常量设为“True”。

启用运行状况监控器

要启用运行状况监控器，请在 ***constant.py*** 中将常量设为“False”。

禁用生命周期钩子

在极少数需要禁用生命周期钩子的情况下，如果禁用，将不会向实例添加额外的接口。它还可能导致一系列 threat defense virtual 实例部署失败。

禁用 Auto Scale 管理器

要禁用 Auto Scale Manager，应禁用相应的 CloudWatch 事件“notify-instance-launch”和“notify-instance-terminate”。禁用这些不会对任何新事件触发 Lambda。但是，已在执行的 Lambda 操作将会继续。Auto Scale Manager 不会突然停止。通过删除堆栈或删除资源尝试突然停止可能会导致状态不确定。

负载均衡器目标

由于 AWS 负载均衡器不允许对具有多个网络接口的实例使用实例类型目标，因此将 Gigabit0/1 接口 IP 配置为目标组上的目标。但是，截至目前，AWS Auto Scale 运行状况检查仅对实例类型目标（而不是 IP）有效。此外，这些 IP 不会自动添加到目标组或从目标组中删除。因此，我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行维护或故障排除时，可能会有需要手动完成此操作的情况。

将目标注册到目标组

要将 threat defense virtual 实例注册到负载均衡器，其 Gigabit0/1 实例 IP（外部子网）应添加为目标组中的目标。请参阅按 IP 地址注册或取消注册目标。

从目标组取消注册目标

要从负载均衡器取消注册 threat defense virtual 实例，其 Gigabit0/1 实例 IP（外部子网）应作为目标组中的目标删除。请参阅按 IP 地址注册或取消注册目标。

实例备用

AWS 不允许在 Auto Scale 组中重新启动实例，但允许用户将实例置于备用状态并执行这类操作。但是，当负载均衡器目标为实例类型时，这将发挥最佳效果。但是，由于多个网络接口，threat defense virtual机无法配置为实例类型目标。

将实例置于备用状态

如果实例被置于备用状态，则其目标组中的 IP 在运行状况探测失败之前仍将继续处于相同状态。因此，建议在将实例置于备用状态之前，从目标组取消注册各自的 IP；有关详细信息，请参阅负载均衡器目标，第 145 页。

删除 IP 后，请参阅暂时从 Auto Scaling 组中删除实例。

从备用状态删除实例

同样，您也可以将实例从备用状态移至运行状态。从备用状态删除后，实例的 IP 应注册到目标组目标。请参阅负载均衡器目标，第 145 页。

有关如何将实例置于备用状态以进行故障排除或维护的详细信息，请参阅 AWS 新闻博客。

从 Auto Scale 组删除/分离实例

要从 Auto Scale 组中删除实例，应首先将其移到备用状态。请参阅“将实例置于备用状态”。当实例处于备用状态后，可以将其删除或分离。请参阅从 Auto Scaling 组分离 EC2 实例。

管理中心 端不会有任何更改。需要手动执行任何必要的更改。

终止实例

要终止实例，应将其置于备用状态；请参阅实例备用，第 145 页。当实例处于备用状态后，即可继续终止。

实例内向扩展保护

为避免从 Auto Scale 组中意外删除任何特定实例，可以对其进行内向扩展保护。如果实例受到内向扩展保护，则不会因内向扩展事件而终止。

请参阅以下链接，以便将实例置于内向扩展保护状态。

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

重要事项 建议将状况良好的最小数量的实例（目标 IP 应正常运行，而不仅是 EC2 实例）设为内向扩展保护。

配置更改

配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。

如果您在现有实例上手动更新配置时遇到问题，我们建议从扩展组中删除这些实例并将其替换为新实例。

更改 管理中心 用户名和密码

在更改 管理中心 IP、用户名或密码的情况下，应对 Auto Scale Manager Lambda 函数和自定义指标发布方 Lambda 函数环境变量执行相应的更改。请参阅使用 AWS Lambda 环境变量。

当 Lambda 下次运行时，将引用更改后的环境变量。

注释 环境变量会被直接送入 Lambda 函数。此处不检查密码复杂性。

更改Threat Defense Virtual 管理员密码

对于运行中的实例，更改 threat defense virtual 密码时要求用户在每个设备上手动更改。对于要载入的新 threat defense virtual 设备，将从 Lambda 环境变量提取 threat defense virtual 密码。请参阅使用 AWS Lambda 环境变量。

更改注册和 NAT ID

对于要使用不同的注册和 NAT ID 载入的新 threat defense virtual设备，在进行 管理中心 注册时，应在 Configuration.json 文件中更改这些信息。可以在 Lambda 资源页中找到 Configuration.json 文件。

访问策略和 NAT 策略更改

通过设备组分配的帮助，访问策略或NAT 策略的任何更改都将自动应用到未来的实例。不过，要更新现有的 threat defense virtual 实例，您需要手动推送配置更改，然后从 管理中心 部署这些更改。

AWS 资源更改

部署后可以在 AWS 中更改许多内容，如 Auto Scale 组、启动配置、CloudWatch 事件、扩展策略等。您可以将资源导入 CloudFormation 堆栈，或通过现有资源创建新的堆栈。

有关如何管理对 AWS 资源执行的更改的详细信息，请参阅将现有资源引入 CloudFormation 管理。

收集和分析 CloudWatch 日志

有关导出 CloudWatch 日志的信息，请参阅使用 AWS CLI 将日志数据导出到 Amazon S3。

为现有自动缩放组实例配置 IMDSv2 所需模式

您可以为 AWS 上已部署的 Threat Defense Virtual 个自动缩放组实例配置 IMDSv2 必需模式。

Before you begin

仅 Threat Defense Virtual 7.6 及更高版本支持 IMDSv2 必需模式。在为部署配置 IMDSv2 模式之前，确保现有实例版本与 IMDSv2 模式兼容（升级到版本 7.6）。

Procedure

步骤 1 登录 http://aws.amazon.com/。

步骤 2 点击 **EC2**，然后选择**自动扩展 (Auto Scaling)** > **自动扩展组 (Auto Scaling Groups)**。

步骤 3 从列表中选择自动扩展组，为该组的相关实例配置 IMDSv2 必需模式。

步骤 4 点击**启动模板 (Launch Template)**。

步骤 5 在**启动模板 (Launch templates)** 页面上，从**操作 (Actions)** 下拉列表中选择**修改模板（创建新版本）(Modify template [Create new version])**。

步骤 6 使用支持 IMDSv2 的映像来更新 AMI ID。

步骤 7 在**高级详细信息 (Advanced Details)** 下，启用 IMDSv2 元数据：

a) 从**元数据可访问 (Metadata accessible)** 下拉列表中选择**启用 (Enabled)**。

b) 从**元数据版本 (Metadata version)** 下拉列表中选择 **仅 V2（需要令牌）(V2 only [token required])** 。

步骤 8 使用此元数据版本的启动模板来部署启用 IMDSv2 Required 模式的自动扩展组实例。

故障排除

AWS CloudFormation 控制台

您可以在 AWS CloudFormation 控制台中验证 CloudFormation 堆栈的输入参数，该控制台允许您直接从网络浏览器创建、监控、更新和删除堆栈。

导航到所需的堆栈，然后选中参数选项卡。您还可以在 Lambda 函数环境变量选项卡中检查 Lambda 函数的输入。此外，还可以在 Auto Scale Manager Lambda 函数本身上查看 *configuration.json*。

要了解有关 AWS CloudFormation 控制台的更多信息，请参阅《*AWS CloudFormation* 用户指南》。

Amazon CloudWatch 日志

您可以查看各个 Lambda 函数的日志。AWS Lambda 代表您自动监控 Lambda 功能，从而通过 Amazon CloudWatch 报告指标。为帮助您排除功能故障，Lambda 会记录您的功能处理的所有请求，并通过 Amazon CloudWatch 日志自动存储代码生成的日志。

您可以使用 Lambda 控制台、CloudWatch 控制台，AWS CLI 或 CloudWatch API 查看 Lambda 的日志。要了解有关日志组并通过 CloudWatch 控制台访问日志组的更多信息，请参阅《*Amazon CloudWatch* 用户指南》中的监控系统、应用和自定义日志文件。

负载均衡器运行状况检查失败

负载均衡器运行状况检查包含协议、ping 端口、ping 路径、响应超时和运行状况检查间隔等信息。如果实例在运行状况检查间隔内返回 200 响应代码，则该实例会被视为运行状况正常。

如果您的部分或所有实例的当前状态为 `OutOfService`，并且说明字段显示`实例至少连续失败运行状况检查不正常阈值次数的检查 (Instance has failed at least the Unhealthy Threshold number of health checks consecutively)`，则表明实例未通过负载均衡器运行状况检查。

您应在 管理中心 配置中检查运行状况探测 NAT 规则。有关详细信息，请参阅传统负载均衡器故障排除：运行状况检查。

流量问题

要排除 threat defense virtual 实例的流量问题，应检查负载均衡器规则、NAT 规则和 threat defense virtual 实例中配置的静态路由。

您还应检查部署模板中提供的 AWS 虚拟网络/子网/网关详细信息，包括安全组规则等。您还可以参阅 AWS 文档，例如 EC2 实例故障排除。

与 管理中心 连接失败

如果管理连接中断，则应检查配置和凭证。请参阅《*Cisco Secure Firewall Management Center* 配置指南》中的“设备管理的要求和前提条件”。

设备无法向 管理中心 注册

如果设备未能向 管理中心 注册失败，您需要确定 管理中心 配置是否有故障/无法访问，或者 管理中心 是否有能力容纳新设备。请参阅《*Cisco Secure Firewall Management Center* 配置指南》中的“将设备添加到管理中心”。

无法通过 SSH 连接到 Threat Defense Virtual

如果无法通过 SSH 连接到 threat defense virtual，请检查是否通过模板将复杂密码传递到 threat defense virtual。

双臂代理配置故障排除

threat defense virtual EC2 实例无法启动或进入连续的启动-终止循环。

您必须验证活动历史记录：转至**自动扩展组 (Autoscale Group)** > **自动扩展组 (Autoscale Group)** > **活动 (Activity)** > **活动历史记录 (Activity History)** 以开始调试。

可能的原因包括 AMI 丢失和 Lambda 函数执行错误。

- 确保 AMI 存在于 AWS 账户中。
- 检查连接、配置和许可。
- 选中与 threat defense virtual EC2 实例关联的标签，以获取设备的连接状态、配置状态、许可状态和其他状态。
- 检查 CloudWatch 日志
  - 单个 Lambda 函数的日志可在 CloudWatch Logs 中查看。
  - 如果在连接或配置设备时出现问题，请继续查看 Lambda 函数的 CloudWatch 日志以了解根本原因。
  - 验证 Lambda 函数的日志组。

AWS 云端调试：流量未通过

- 检查所有 AWS 子网的路由表是否与拓扑图中指定的一致。确保出口（设备上存在东西流量路由。

- 确保与所有设备接口相关联的 AWS 安全组允许预期的 IP 地址范围。

使用案例 - 适用于 Threat Defense Virtual 的 Auto Scale 解决方案，使用 AWS 上的 GWLB 检查南北流量

本使用案例文档介绍如何在 AWS 环境中使用网关负载均衡器 (GWLB) 设置 Threat Defense Virtual 实例的自动扩展，以检测南北向流量。

如何设置 Threat Defense Virtual Auto Scale 解决方案以使用 AWS 上的 GWLB 检查南北流量

通过自动扩展解决方案，可以部署、扩展和管理托管用于流量检测的一组 Threat Defense Virtual 实例。流量根据性能或使用容量在单个或多个Threat Defense Virtual 实例之间分布。

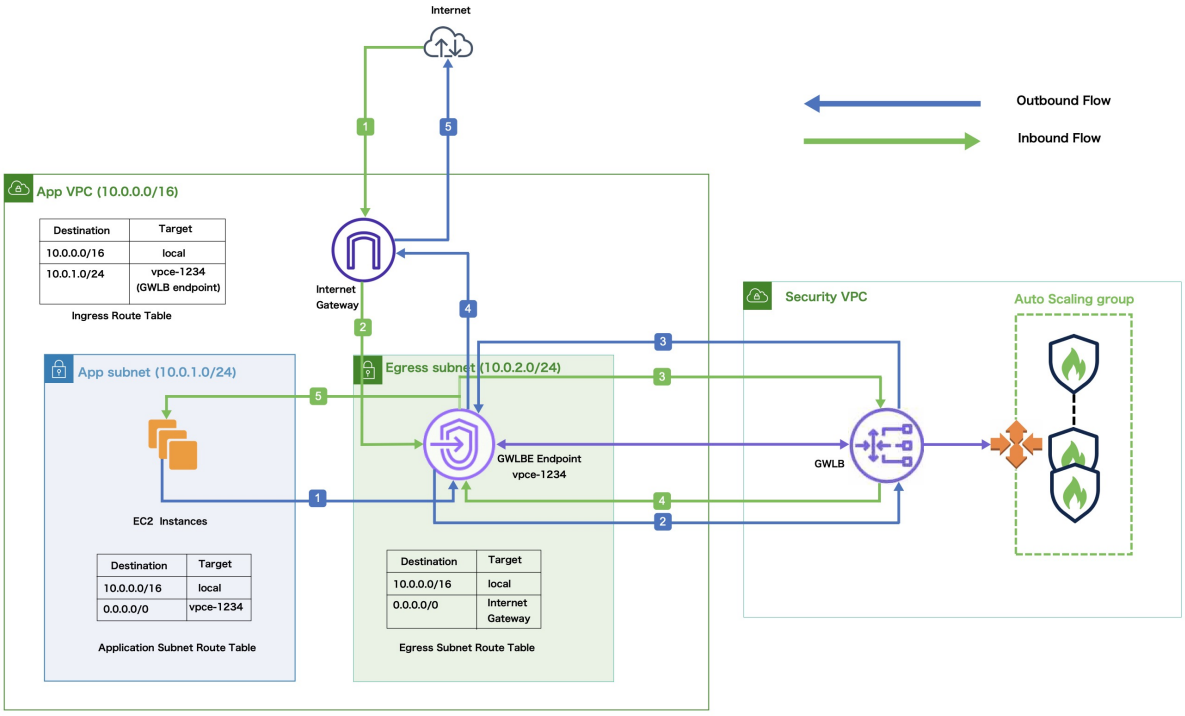
GWLB 充当单一入口和出口点，以管理内部和外部生成的流量，并根据流量负载实时扩大或缩小 Threat Defense Virtual 实例的数量。

注释 此使用案例中使用的参数值为示例值。根据需要更改这些值。

拓扑示例

此拓扑示例说明如何通过 GWLB 将入站和出站网络流量分发到 Threat Defense Virtual 实例，然后再路由到应用 VPC 并返回。

图 5: 使用 *GWLB* 的 *Threat Defense Virtual Auto Scale* 解决方案



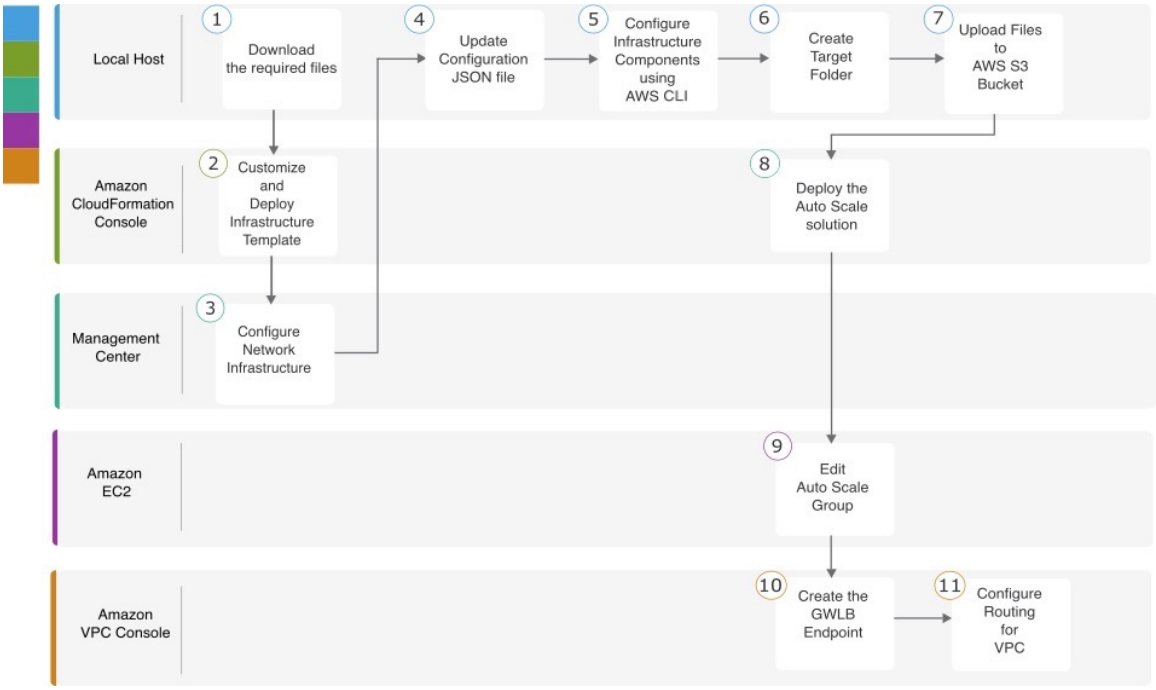
入站流量检测	
1	互联网网关 (IGW) 接收来自互联网的流量。
2	流量会根据入口路由表中的路由路由到网关负载均衡器终端 (GWLBe)。
3	GWLBe 连接到安全虚拟私有云 (VPC) 中的终端服务。GWLB 封装收到的流量，并将其转发到 Threat Defense Virtual 自动扩展组进行检查。
4	自动扩展组检查的流量会返回到 GWLB，然后再返回到 GWLB 终端。
5	GWLB 终端将流量转发到应用 VPC，然后再将流量路由到应用子网中的资源。

出站流量检测	
1	来自应用子网资源的流量会被路由到同一 VPC 中的 GWLBe。
2	GWLBe 连接到安全 VPC 中的终端服务。GWLB 封装收到的流量，并将其转发到自动扩展组进行检查。

出站流量检测	
3	自动扩展组检测到的流量会返回到 GWLB，然后再返回到 GWLBe。
4	流量到达源 VPC 后，会根据出口子网路由表中定义的路由转发到 IGW。
5	IGW 将流量发送到互联网。

端到端程序

以下流程图说明了在 Amazon Web 服务 (AWS) 上使用 GWLB 部署 Threat Defense Virtual 自动扩展解决方案的工作流程。



	工作空间	步骤
1	本地主机	前提条件
2	Amazon CloudFormation 控制台	Amazon CloudFormation 控制台 - 自定义和部署基础设施模板
3	管理中心	管理中心 - 在管理中心配置 Threat Defense Virtual 网络基础设施

	工作空间	步骤
4	本地主机	本地主机 - 更新配置 JSON 文件
5	本地主机	Ubuntu 主机 - 使用 AWS CLI 配置基础设施组件
6	本地主机	本地主机 - 创建目标文件夹
7	本地主机	本地主机 - 将 AWS GWLB Auto Scale 解决方案部署文件上传到 Amazon S3 存储桶
8	Amazon CloudFormation 控制台	Amazon CloudFormation 控制台 - 使用 GWLB 为 Threat Defense Virtual 部署 Auto Scale 解决方案
9	Amazon EC2 控制台	Amazon EC2 控制台 - 编辑 Auto Scale 组中实例的数量
10	Amazon VPC 控制台	创建 GWLB 终端
11	Amazon VPC 控制台	为客户 VPC 配置路由

前提条件

- 从 GitHub 克隆 GitHub 清单到本地主机。此存储库包含 `cisco-ftdv/autoscale/aws` 下的以下文件。
  - 用于创建 Lambda 层的 Python (.py) 文件。
  - 一个 configuration.json 文件，用于根据需要添加静态路由和自定义任何网络参数。
  - 用于生成 zip 文件的 `make.py`。
  - 部署需要使用 `*.yaml` 文件。
- `/templates` 文件夹下的云形成模板：
  - **Infrastructure_gwlb.yaml** - 用于自定义 AWS 环境中的组件。
  - **deploy_ngfw_autoscale_with_gwlb.yaml** - 用于部署具有 GWLB 的 AWS Auto Scale 解决方案。
- [可选]尽可能收集模板参数的值。这样可以在AWS管理控制台上部署模板时更轻松快速地输入值。

Amazon CloudFormation 控制台 - 自定义和部署基础设施模板

执行本节中给出的步骤，以自定义和部署基础设施模板。

过程

步骤 1 在 AWS 管理控制台上，转到**服务 (Services)** > **管理和治理 (Management and Governance)** > **CloudFormation**，然后点击**创建堆栈 (Create stack)** > **使用新资源（标准）(With new resources[standard])**。

步骤 2 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从下载文件的文件夹中选择 **Infrastructure_gwlb.yaml**。

步骤 3 点击**下一步**。

步骤 4 在**指定堆栈详细信息 (Specify stack details)** 页面上，输入堆栈的名称。

步骤 5 为 ***infrastructure_gwlb.yaml*** 模板中的输入参数提供值。

参数	值
Pod 配置	
Pod 名称	*infrastructure*
Pod 编号	1
S3 存储桶名称	*demo-us-bkt*
VPC CIDR	*20.0.0.0/16*
可用性区域数量	2 注释 Threat Defense Virtual 最多支持三个可用性区域。如果您选择跨三个 可用性区域部署虚拟设备，请确保为管理接口、内部接口和外部接口各选择三个子网。
ListOfAzs（可用区域列表）	*us-west-1a,us-west-1b*
管理子网的名称	*MgmtSubnet-1,MgmtSubnet-2*
MgmtSubnetCidrs	*20.1.250.0/24,20.1.251.0/24*
内部子网的名称	*InsideSubnet-1,InsideSubnet-2*
InsideSubnetCidrs	*20.1.100.0/24,20.1.101.0/24*
外部子网的名称	*OutsideSubnet-1,OutsideSubnet-2*
OutsideSubnetCidrs	*20.1.200.0/24,20.1.201.0/24*
Lambda 子网的名称	*LambdaSubnet-1,LambdaSubnet-2*
Lambda 子网 CIDR	*20.1.50.0/24,20.1.51.0/24*

步骤 6 点击**下一步**。

步骤 7 在**配置堆栈选项 (Configure Stack Options)** 窗口中点击**下一步 (Next)**。

步骤 8 在**查看 (Review)** 页面上，查看并确认设置。

步骤 9 点击**创建堆栈 (Create Stack)** 以部署 **Infrastructure_gwlb.yaml** 模板并创建堆栈。

步骤 10 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **S3 Bucket Name**。

管理中心 - 在管理中心配置 Threat Defense Virtual 网络基础设施

在管理中心为已注册的 Threat Defense Virtual 创建和配置对象、设备丢弃、运行状况检查端口和访问策略。

创建主机对象

过程

步骤 1 登录管理中心。

步骤 2 选择**对象** > **对象管理**。

步骤 3 从对象类型列表中选择**网络 (Network)**。

步骤 4 从**添加网络 (Add Network)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 5 输入**名称** - *aws-metadata-server*。

步骤 6 输入说明。

步骤 7 在**网络 (Network)** 字段中，选择**主机 (Host)** 选项并输入 IPv4 地址 - *169.254.169.254*。

步骤 8 点击**保存 (Save)**。

创建端口对象

过程

步骤 1 登录管理中心。

步骤 2 选择**对象** > **对象管理**。

步骤 3 从对象类型列表中选择**端口 (Port)**。

步骤 4 从**添加端口 (Add Port)** 下拉菜单中选择**添加对象 (Add Object)**。

步骤 5 输入**名称** - *test-port-object*。

步骤 6 选择**协议 (Protocol)**。您必须选择已为主机对象类型输入的协议。根据选择的协议，按**端口 (Port)** 进行限制。

步骤 7 输入 *8080*。请注意，您可以根据需要自定义在此处输入的端口号。

注释

如果选择与**所有 (All)** 协议匹配，则必须使用**其他 (Other)** 下拉列表按端口限制对象。

步骤 8 点击**保存 (Save)**。

创建安全区域和接口组对象

过程

步骤 1 选择**对象** > **对象管理**。
步骤 2 从对象类型列表中选择**接口**。
步骤 3 点击**添加 (Add)** > **安全区域 (Security Zone)** 或**添加 (Add)** > **接口组 (Interface Group)**。
步骤 4 输入 **名称** - *inside-sz/outside-sz*。
步骤 5 选择**接口类型 (Interface Type)** - 已路由 *(Routed)*。
步骤 6 点击**保存 (Save)**。

添加设备组

管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。您可以展开和折叠组中的设备列表。

过程

步骤 1 选择**设备** > **设备管理**。
步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。
步骤 3 要编辑现有的组，请点击要编辑的组的**编辑**（编辑图标）。
步骤 4 输入**名称** - *aws-ngfw-autoscale-dg*。
步骤 5 点击**确定 (OK)** 以添加组。

为运行状况检查探测器启用端口 443 (HTTP)

如果将端口 443 (HTTP) 用于运行状况检查探测，请执行以下程序为运行状况检查探测启用端口。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)** > **HTTP 访问 (HTTP Access)**。

步骤 2 选中启用 **HTTP** 服务器 **(Enable HTTP Server)** 复选框。
步骤 3 在端口 **(Port)** 字段中输入 **443**。
步骤 4 点击 **+** 添加。
步骤 5 从下拉列表中选择相关 **IP** 地址。
步骤 6 从可用区域/接口 **(Available Zones/Interfaces)** 窗口中，选择连接到 GWLB 的外部接口或外部子网。
步骤 7 点击添加 **(Add)** 以将该接口添加到所选区域/接口 **(Selected Zones/Interfaces)** 窗口。
步骤 8 点击确定 **(OK)**。
步骤 9 点击保存 **(Save)**。

创建基本访问控制策略

创建新的访问控制策略时，它包含默认操作和设置。创建策略后，您会立即进入编辑会话，以便您可以调整策略以满足您的要求。

过程

步骤 1 依次选择策略 > 访问控制。
步骤 2 点击新建策略。
步骤 3 输入唯一的名称 - *aws-asg-policy* 和说明。
步骤 4 指定初始默认操作 **(Default Action)** - 阻止所有流量 **(Block all traffic)**。
步骤 5 点击保存 **(Save)**。
步骤 6 点击页面右上角的目标设备 **(Targeted Devices)** 以分配策略。
步骤 7 从可用设备中选择 **aws-ngfw-autoscale-dg**。
步骤 8 点击添加到策略 **(Add to Policy)**，然后点击确定 **(OK)** 以添加到策略。
步骤 9 点击您创建的新策略的编辑图标。
步骤 10 点击添加规则 **(Add Rule)**。
步骤 11 设置以下参数：

- 名称：*inside-to-outside*
- 插入：到强制
- 操作：允许
- 添加源区域和目标区域。

步骤 12 点击应用。

本地主机 - 更新配置 JSON 文件

configuration.json 文件位于您从 GitHub 下载的 **lambda_python_files** 文件夹中。使用您在 管理中心 设置的参数来更新 **configuration.json** 文件中的参数。

configuration.json 文件中的脚本如下所示。

```
"licenseCaps": ["BASE", "MALWARE", "THREAT"],   // Management center virtual licenses
  "fmcIpforDeviceReg": "DONTRESOLVE",   // Management center virtual IP address
  "RegistrationId": "cisco",  // Registration ID used while configuring the manager in the
 Threat defense virtual
  "NatId": "cisco",  // NAT ID used while configuring the manager in the Threat defense
virtual
  "fmcAccessPolicyName": "aws-asg-policy",  // Access policy name configured in the Management
 center virtual
  "fmcInsideNicName": "inside", //Threat defense virtual inside interface name
  "fmcOutsideNicName": "outside", //Threat defense virtual outside interface name
  "fmcInsideNic": "TenGigabitEthernet0/0", // Threat defense virtual inside interface NIC
Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance types)

  "fmcOutsideNic": "TenGigabitEthernet0/1", // Threat defense virtual outside interface NIC
 Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance types

  "fmcOutsideZone": "Outside-sz", //Outside Interface security zone name that is set in the
 Management center virtual
  "fmcInsideZone": "Inside-sz", //Inside Interface security zone name that is set in the
Management center virtual
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Inside-sz"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "TenGigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Outside-sz"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "TenGigabitEthernet0/1"
    }
  ],  // Interface-related configuration
  "trafficRoutes": [
    {
      "interface": "inside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "1"
    }
  ] // This traffic route is used for the Threat defense virtual instance's health check
}
```

注释 要使用专用 IP 向 Management Center Virtual 注册 Threat Defense Virtual，请修改 `cisco-ftdv/autoscale/aws/lambda-python-files/` 中的 `constant.py` 文件中的以下行：

- `USE_PUBLIC_IP_FOR_FMC_CONN = False`

Ubuntu 主机 - 使用 AWS CLI 配置基础设施组件

模板不会为 Threat Defense Virtual 和管理中心创建 Lambda 层和加密密码。使用下面给出的程序配置这些组件。有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面。

过程

步骤 1 创建 Lambda 层 zip 文件。

在 Linux 主机上创建 python 文件夹，然后创建 Lambda 层。

a) 在 Linux 主机（例如 Ubuntu 22.04）中创建 python 文件夹。

b) 在 Linux 主机上安装 Python 3.9。下面提供了安装 Python 3.9 的示例脚本。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

c) 在 Linux 环境中创建 Lambda 层 zip 文件 *autoscale_layer.zip*。此文件为 Lambda 函数提供必要的 Python 库。

运行以下脚本以创建 *autoscale_layer.zip* 文件。

```
#!/bin/bash
mkdir -p layer
mkdir -p python
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install attrs==23.1.0
pip3 install bcrypt==3.2.2
pip3 install certifi==2022.12.7
pip3 install cffi==1.15.1
pip3 install chardet==3.0.4
pip3 install cryptography==2.9.1
pip3 install idna==2.10
pip3 install jsonschema==3.2.0
pip3 install paramiko==2.7.1
pip3 install pycparser==2.21
pip3 install pycryptodome==3.15.0
pip3 install PyNaCl==1.5.0
pip3 install pyrsistent==0.19.3
```

```
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install six==1.16.0
pip3 install urllib3==1.25.11
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

d) 在创建 **autoscale_layer.zip** 文件后，将 **autoscale_layer.zip** 文件复制到从 GitHub 下载的 **lambda-python-files** 文件夹中。

步骤 2 （可选）为 Threat Defense Virtual 和管理中心创建加密密码。

如果已在 Infrastructure_gwlb.yaml 模板文件中输入 KMS ARN 值，则必须加密您在 Threat Defense Virtual 和管理中心中设置的密码。请参阅查找密钥 ID 和密钥 ARN，以使用 AWS KMS 控制台来识别密钥 ARN。在本地主机上，运行以下 AWS CLI 命令加密密码。

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

`CiphertextBlob` 的值是加密密码。将此密码用作 `Infrastructure_gwlb.yaml` 文件中 **NGFWv 密码**（threat defense virtual 密码）或 AutoScale 自动化的 FMC 密码（管理中心 密码）参数的值。您还可以将此密码用作**将指标发布到 CloudWatch 的 FMC 密码**的值。

本地主机 - 创建目标文件夹

导航至本地主机上克隆存储库中的 `cisco-ftdv/autoscale/aws/`，然后运行下面提供的命令创建一个目标文件夹，其中包含必须上传到 Amazon S3 存储桶的文件。

python3 make.py build

这将在本地主机上创建一个名为“target”的文件夹。target 文件夹包含部署 Auto Scale 解决方案所需的 *zip* 文件和 *yaml* 文件。

本地主机 - 将 AWS GWLB Auto Scale 解决方案部署文件上传到 Amazon S3 存储桶

使用下面提供的命令将目标目录中的所有文件上传到在基础设施堆栈部署期间创建的 Amazon S3 存储桶。

$ cd ./target

$ aws s3 cp . s3://demo-us-bkt --recursive

Amazon CloudFormation 控制台 - 使用 GWLB 为 Threat Defense Virtual 部署 Auto Scale 解决方案

过程

步骤 1 在 AWS 管理控制台上，转至**服务 (Services)** > **管理和监管 (Management and Governance)** > **CloudFormation** > **堆栈**，然后点击模板创建的堆栈。

步骤 2 点击**创建堆栈 (Create stack)** > **通过新资源（标准）(With new resources [standard])**。

步骤 3 选择**上传模板 (Upload a template)** 文件，点击**选择 (Choose)** 以选择文件，然后从目标文件夹中选择 ***deploy_ngfw_autoscale_with_gwlb.yaml***。

步骤 4 点击**下一步**。

步骤 5 在**指定堆栈详细信息 (Specify stack details)** 页面上，输入堆栈的名称。

步骤 6 为 ***deploy_ngfw_autoscale_with_gwlb.yaml*** 模板中的输入参数提供值。

堆栈名称：Threat-Defense-Virtual

注释
您可以从已创建的基础设施堆栈中找到VPC ID、S3 存储桶名称、子网和安全组值。确保管理中心参数与您创建的实际 FMC IP 地址、设备组名称、用户凭证和其他参数相匹配。

参数	值
Pod 配置	
Autoscale 组名称前缀	*NGFWv-AutoScale*
Pod 编号	*1*
Autoscale 邮件通知	指定用于接收通知的电子邮件地址。例如：*username@cisco.com*
基础设施详细信息	
VPC ID	*vpc-05277f76370396df4*
S3 存储桶名称	*demo-us-bkt*
Lambda 函数的子网	*subnet-0f6bbd4de47d50c6b,subnet-0672f4c24156ac443*
Lambda 函数的安全组	*sg-023dfadb1e7d4b87e*
可用性区域数量	*2* **注释**

参数	值
	Threat Defense Virtual 最多支持三个可用性区域。如果您选择跨三个可用性区域部署虚拟设备，请确保为管理接口、内部接口和外部接口各选择三个子网。
可用区域	*us-west-1a*、*us-west-1b*
NGFWv 管理接口的子网列表	*subnet-0e0bc4961de87b170*、*subnet-0c285f960d165b1fc*
NGFWv 内部接口的子网列表	*subnet-0f6acf3b548d9e95b*、*subnet 0bc6d89f5d34e806b*
NGFWv 外部接口的子网列表	*subnet-0cc7ac70df7144b7e*、*subnet-0237113d433c416fc*
GWLB 配置	
输入用于 NGFWv 实例运行状况检查的端口	*22*
思科 NGFWv 实例配置	
NGFWv 实例类型	*c5. xlarge*
NGFWv 实例许可证类型	*BYOL*
从 AWS IP 池为 NGFWv 分配公用 IP	*true*
NGFWv 实例的安全组	*sg-088ae4bc1093f5833*
内部 NGFWv 实例的安全组	*sg-0e0ce5dedcd9cd4f3*
外部 NGFWv 实例的安全组	*sg-07dc50ff47d0c8126*
NGFWv AMI-ID	*ami-00faf58c7ee8d11e1* **注释** 您必须指定 AWS 账户中存在的正确 NGFWv AMI-ID。 要搜索 AMI-ID，请执行以下操作： **1.** 转至 **EC2** > **AMI**。 **2.** **公共 AMI** 的过滤器。 **3.** 搜索 **`aws-marketplace/ftdv`**。使用指定选项中最新版本的 AMI ID。
KMS 主密钥 ARN（视情况而定）	
NGFWv 密码	*W1ch3sterBr0s*
FMC 自动化配置	

参数	值
FMC 主机 IP 地址	*3.38.137.49*
AutoScale 自动化的 FMC 用户名	*autoscaleuser*
AutoScale 自动化的 FMC 密码	*W1nch3sterBr0s*
FMC 设备组名称	*aws-ngfw-autoscale-dg*
FMCv 许可的性能层值	*FTDv20*
FMC 设备组指标发布配置	
从 FMC 发布自定义指标	*TRUE*
用于将指标发布到 CloudWatch 的 FMC 用户名	*metricuser*
用于将指标发布到 CloudWatch 的 FMC 密码	*W1ch3sterBr0s*
扩展配置	
下限、上限 CPU 阈值	*10,70*
下限、上限内存阈值	*40,70*

步骤 7 在**配置堆栈选项 (Configure Stack Options)** 窗口中点击**下一步 (Next)**。

步骤 8 在**查看 (Review)** 页面上，查看并确认设置。

步骤 9 点击**创建堆栈 (Create Stack)** 以部署 ***deploy_ngfw_autoscale_with_gwlb.yaml*** 模板并创建堆栈。

这样就完成了为使用 GWLB 的Threat Defense Virtual 设置自动扩展解决方案所需的两个模板的部署。

Amazon EC2 控制台 - 编辑 Auto Scale 组中实例的数量

默认情况下，Auto Scale 组的最小和最大威胁防御虚拟实例数分别设置为 0 和 2。根据需要更改这些值。

过程

步骤 1 在 AWS 管理控制台上，转至**服务 (Services)** > **计算 (Compute)** > **EC2**，然后点击**自动扩展组 (Auto Scaling Groups)**。

步骤 2 选择您创建的 自动扩展组，然后点击**编辑 (Edit)** 以根据您的要求修改**所需容量 (Desired capacity)**、**最小容量 (Minimum capacity)**、**最大容量 (Maximum capacity)** 字段中的值。这些值对应于要为自动扩展功能调出的 Threat Defense Virtual 实例的数量。将**所需容量 (Desired capacity)** 设置为介于最小和最大容量值之间的值。

步骤 3 点击更新。

注释 建议您仅启动一个 Threat Defense Virtual 实例，并验证该实例在自动扩展组中处于服务状态并已注册到 Management Center Virtual。然后，您可以根据自己的要求启动更多实例。

Amazon VPC 控制面板控制台 - 创建 GWLB 终端并为客户 VPC 配置路由

在部署两个 CloudFormation 模板后，您必须为客户 VPC 创建 GWLB 终端并配置路由。

创建 GWLB 终端

过程

步骤 1 在 AWS 管理控制台上，转至服务 **(Services)** > 网络和内容交付 **(Networking & Content Delivery)** > **VPC** > 终端服务 **(Endpoint Services)**。

步骤 2 点击创建终端服务 **(Create Endpoint Service)**

步骤 3 在负载均衡器 **(Load balancer)** 类型下，选择网关 **(Gateway)**。

步骤 4 在可用的负载均衡器 **(Available load balancers)** 下，选择作为 Auto scale 部署的一部分创建的网关负载均衡器。

步骤 5 点击创建 **(Create)**。

步骤 6 复制新创建的终端服务的服务名称。

步骤 7 转至服务 **(Services)** > 网络和内容交付 **(Networking & Content Delivery)** > **VPC** > 终端 **(Endpoints)**。

步骤 8 点击创建终端 **(Create endpoint)**。

步骤 9 在服务类别 **(Service category)** 下，选择其他终端服务 **(Other endpoint services)**。

步骤 10 对于服务名称 **(Service name)**，输入服务的名称，然后选择验证服务 **(Verify service)**。

步骤 11 在 **VPC** 字段中，选择要在其中创建终端的 VPC 应用 *VPC (App VPC)*。

步骤 12 在子网 **(Subnets)**下，选择要在其中创建终端的子网出口子网 *(Egress subnet)*。

步骤 13 对于 IP 地址类型，请选择 IPv4 选项以将 IPv4 地址分配给终端网络接口。

步骤 14 点击创建终端 **(Create endpoint)**。

步骤 15 转至服务 **(Services)** > 网络和内容交付 **(Networking & Content Delivery)** > **VPC** > 终端服务 **(Endpoint services)**，点击 终端连接 **(Endpoint Connections)** 选项卡，选择您之前创建的终端 **ID**，然后点击操作 **(Actions)** > 接受终端连接请求 **(Accept endpoint connection request)**。

为客户 VPC 配置路由

过程

步骤 1 在 AWS 管理控制台上，转到**服务 (Services)** > **网络和内容 (Networking & Content)** > **虚拟私有云 (Virtual Private Cloud)** > **路由表 (Route tables)**。

步骤 2 创建入口路由表，然后执行以下步骤：

1. 点击**操作 (Actions)** > **编辑路由 (Edit routes)**。
2. 对于 IPv4，请点击**添加路由 (Add route)**。对于**目标 (Destination)**，输入应用服务器子网的 IPv4 CIDR 块 10.0.1.0/24。对于**目标 (Target)**，选择 VPC 终端。
3. 点击**保存更改 (Save changes)**。
4. 在**边缘关联 (Edge Associations)** 选项卡中，点击**编辑边缘关联 (Edit edge associations)**，然后选择**互联网网关 (Edit edge associations)**。
5. 点击**保存更改 (Save changes)**。

步骤 3 选择包含应用服务器的子网的路由表，并执行以下步骤：

1. 点击**操作 (Actions)** > **编辑路由 (Edit routes)**。
2. 对于 IPv4，请点击**添加路由 (Add route)**。对于**目标 (Destination)**，输入**0.0.0.0/0**。对于**目标 (Target)**，选择 VPC 终端。
3. 点击**保存更改 (Save changes)**。

步骤 4 选择带有网关负载均衡器终端的子网路由表，然后执行以下步骤：

1. 点击**操作 (Actions)** > **编辑路由 (Edit routes)**。
2. 对于 IPv4，请点击**添加路由 (Add route)**。对于**目标 (Destination)**，输入**0.0.0.0/0**。对于**目标 (Target)**，选择互联网网关。
3. 点击**保存更改 (Save changes)**。

Amazon CloudWatch - 验证部署

成功部署模板后，转到 Amazon CloudWatch 控制台以确保正在收集日志并创建了所需的警报。

日志

检查日志文件，以排除管理中心连接方面的任何问题。

过程

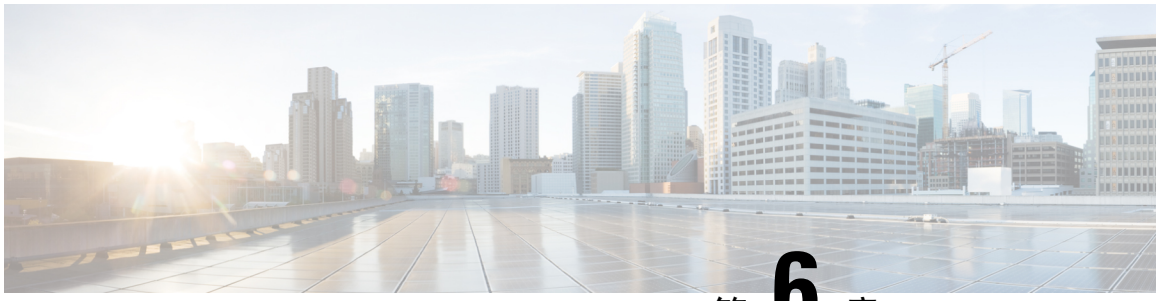
步骤 1 在 AWS 管理控制台上，转至服务 (Services) > 管理和监管 (Management & Governance) > CloudWatch。
步骤 2 点击日志组 (Log groups)，然后点击此处显示的任何日志组以查看日志。

警报

确保已在 Amazon CloudWatch 控制台上创建所需的警报。

过程

步骤 1 在 AWS 管理控制台上，转至服务 (Services) > 管理和监管 (Management & Governance) > CloudWatch。
步骤 2 点击警报 (Alarms) > 所有警报 (All Alarms) 以显示警报列表以及触发外向扩展和内向扩展函数的条件。



第 6 章

在 Azure 上部署 Threat Defense Virtual

本章介绍如何从 Azure 门户部署 Cisco Secure Firewall Threat Defense Virtual。

概述

Cisco Secure Firewall Threat Defense Virtual 集成到 Microsoft Azure 市场中，支持以下实例类型：

- 标准 D3 - 4 个 vCPU，14 GB，4vNIC
- 标准 D3_v2 - 4 个 vCPU，14 GB，4vNIC
- 标准 D4_v2 - 8 个 vCPU，28 GB，8 个 vNIC（**版本 6.5 中新增**）
- 标准 D5_v2 - 16 个 vCPU，56 GB，8 个 vNIC（**版本 6.5 中新增**）
- Standard_D8s_v3 - 8 个 vCPU，32 GB，4 个 vNIC（**7.1 版新增功能**）
- Standard_D16s_v3 - 16 个 vCPU，64 GB，8 个 vNIC（**7.1 版新增功能**）
- Standard_D8s_v2 - 8 个 vCPU，16 GB，4 个 vNIC（**7.1 版新增功能**）
- Standard_F16s_v2 - 16 个 vCPU，32 GB，4 个 vNIC（**7.1 版新增功能**）

前提条件

- Microsoft Azure 帐户。您可以在 https://azure.microsoft.com/en-us/ 创建一个。

  在 Azure 上创建帐户之后，您可以登录、在市场中搜索 Cisco Firepower Threat Defense，然后选择“Cisco Firepower NGFW Virtual (NGFWv)”项。

- 思科智能账户。您可以在 Cisco 软件中心创建一个。

  许可threat defense virtual；有关防火墙系统功能许可的概述（包括有用链接），请参阅Cisco Secure Firewall Management Center 功能许可证。

- 有关 threat defense virtual 和系统兼容性，请参阅 Threat Defense Virtual 兼容性。

通信路径

- 管理接口 - 用于将 threat defense virtual 连接到 Cisco Secure Firewall Management Center。

Note 在 6.7 和更高版本中，可以选择为 管理中心 管理配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。有关为 管理中心 访问配置数据接口的详细信息，请参阅 Cisco Secure Firewall Threat Defense 命令参考中的 **configure network management-data-interface** 命令。

- 诊断接口 - 用于诊断和报告；不能用于直通流量。
- 内部接口（必需）- 用于将 threat defense virtual连接到内部主机。

- 外部接口（必需）- 用于将 threat defense virtual连接到公共网络。
- 从 Cisco Secure Firewall 版本 7.4.1 开始，您可以删除诊断接口，并使用至少 3 个接口（1 个管理接口和 2 个数据接口）在 Azure 上部署 Threat Defense Virtual。我们建议您在没有 Cisco Secure Firewall 版本 7.4.1 的诊断接口的情况下在 Azure 上部署 Threat Defense Virtual。有关详细信息，请参阅关于在 Azure 上部署无诊断接口的 Threat Defense Virtual, on page 185。

准则和限制

支持的功能

- 仅路由防火墙模式
- Azure 加速网络 (AN)
- 管理模式，两个选择之一：
  - 您可以使用 Cisco Secure Firewall Management Center 来管理您的 threat defense virtual，请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual, on page 409。
  - 您可以使用集成 Cisco Secure Firewall 设备管理器 来管理您的 threat defense virtual，请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual, on page 427。
- 集群（7.3 及更高版本）。有关详细信息，请参阅公共云中 Threat Defense Virtual 的集群。
- 公共 IP 寻址 - 向管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。

  您可以根据需要为其他接口分配公共IP地址；请参阅公共IP地址中 Azure关于公共IP的准则，包括如何创建、更改或删除公共 IP 地址。
- IPv6

  以下是部署 IPv6 支持的 threat defense virtual 时必须考虑的准则和限制：
  - 要通过用于 IPv6 支持的 Azure CLI 方法启用编程部署选项，不需要预部署 threat defense virtual 实例。
  - 您无法从 Azure 市场将 threat defense virtual 添加到您已手动从 IPV4 升级到 IPV6 寻址的同一 Vnet。
- Interfaces:
  - Threat Defense Virtual默认情况下随 4 个 vNIC 一起部署。
  - 通过支持较大的实例，您最多可以将 threat defense virtual 随 8 个 vNIC 一起部署。
  - 要为 threat defense virtual 部署添加其他 vNIC，请参阅为虚拟机添加网络接口或从虚拟机移除网络接口中提供的信息。

- 要更改 vNIC 的配置，或者如果需要 IP 转发，请参阅创建、更改或删除网络接口中提供的信息。
- 您可以使用您的管理器配置 threat defense virtual 接口。有关接口支持和配置的完整信息，请参阅管理平台（管理中心 或 设备管理器）对应的配置指南。

许可

- 使用 Cisco 智能许可证帐户的 BYOL（自带许可证）
- PAYG（即付即用）许可，一种基于使用的计费模式，允许客户在不购买 Cisco 智能许可的情况下运行 threat defense virtual。对于已注册的 PAYG threat defense virtual 设备，将启用所有许可的功能（恶意软件/威胁/URL 过滤/VPN 等）。许可的功能无法从 管理中心 编辑或修改。（版本 6.5+）

Note 在 设备管理器 模式下部署的 threat defense virtual 设备上不支持 PAYG 许可。

请参阅《Cisco Secure Firewall Management Center 管理指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

Threat Defense Virtual 智能许可的性能层

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

Table 19: 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/34 GB	16Gbps	10,000

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 AWS 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

不支持的功能

- 许可：
  - PLR（永久许可证预留）。
  - PAYG（即付即用）（版本 6.4 及更低版本）
- 网络（其中很多限制是 Microsoft Azure 限制）：
  - 巨帧
  - 802.1Q VLAN
  - 透明模式及其他第 2 层功能；无广播、无组播。
  - 从 Azure 的角度不归设备所有的 IP 地址的代理 ARP（影响某些 NAT 功能）。
  - 混合模式（不捕获子网流量）。
  - 内嵌设置模式，被动模式。

Note Azure 策略阻止 threat defense virtual 在透明防火墙或内联模式下运行，因为它不允许接口在混合模式下运行。

  - ERSPAN（使用在 Azure 中不会被转发的 GRE）。
- 管理：
  - Azure 门户“重置密码”功能
  - 基于控制台的密码恢复；由于用户没有实时访问控制台的权限，所以无法恢复密码。无法启动密码恢复映像。唯一的办法是部署新的 threat defense virtual 虚拟机。
- 高可用性（活动/备用）
- VM 导入/导出
- Azure 上的第 2 代 VM 生成
- 部署后调整 VM 大小
- 将 VM 的操作系统磁盘的 Azure 存储 SKU 从高级版迁移或更新到标准版 SKU，反之亦然
- 设备管理器 用户界面（6.4 及更低版本）

Azure DDoS 防护功能

Microsoft Azure 中的 Azure DDoS 防护是在 threat defense virtual 最前端实施的一项附加功能。在虚拟网络中，启用此功能有助于根据每秒网络预期流量的数据包来保护应用程序免受常见网络层攻击。您可以根据网络流量模式来自定义此功能。

有关 Azure DDoS 防护功能的详细信息，请参阅 Azure DDoS 防护标准概述。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

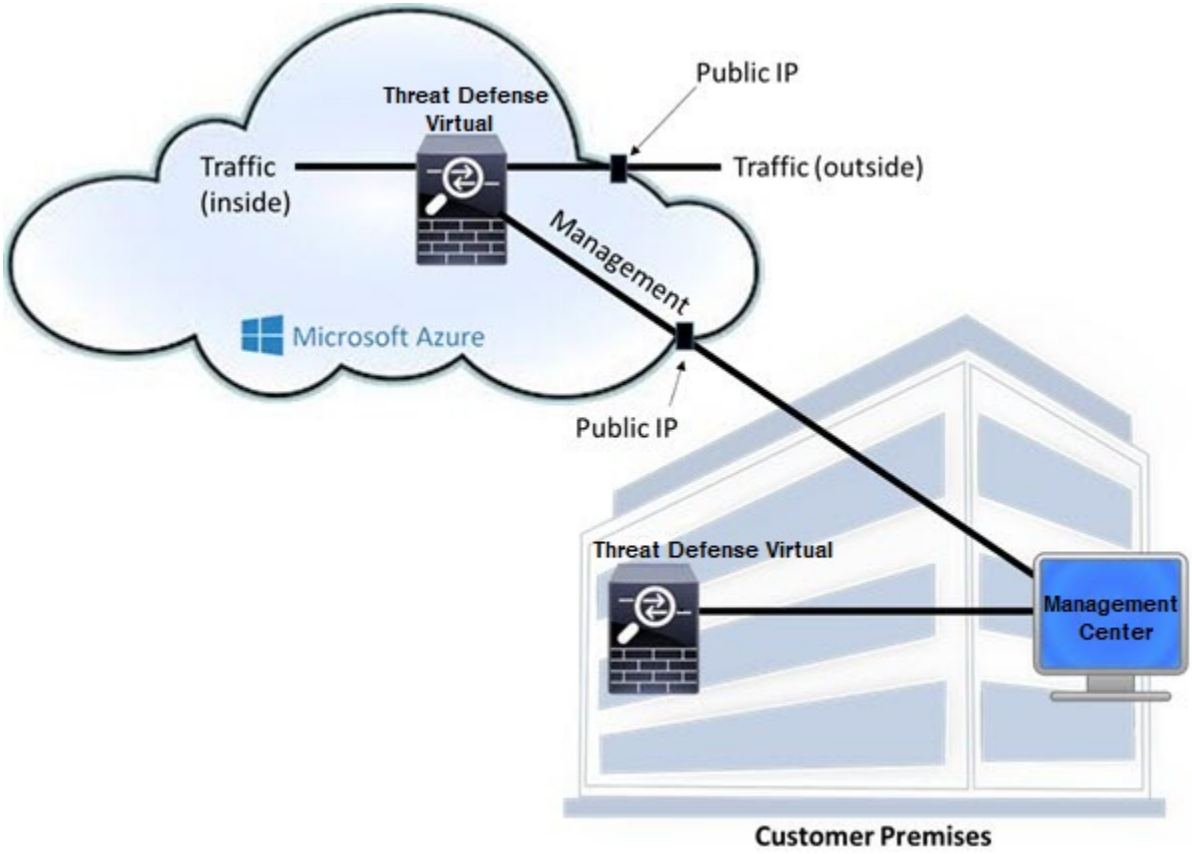
设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

Azure 上 Threat Defense Virtual 的网络拓扑示例

下图显示了适用于 Azure 内路由防火墙模式下的 threat defense virtual 的典型拓扑。定义的第一个接口始终是管理接口，并且仅可为管理 0/0 和 GigabitEthernet0/0 分配公共 IP 地址。



在部署期间创建的资源

在 Azure 中部署 Cisco Secure Firewall Threat Defense Virtual 时，会创建以下资源：

- threat defense virtual 计算机 (VM)
- 一个资源组

- threat defense virtual 始终会部署到新的资源组中。不过，您可以将其附加到另一个资源组的现有虚拟网络。

- 四个 NIC，分别名为 *vm name* -Nic0、*vm name* -Nic1、*vm name* -Nic2 和 *vm name* -Nic3

Note 根据要求，您可以创建仅使用 IPv4 或双协议栈（已启用 IPv4 和 IPv6）的 VNet。

这些 NIC 分别映射到 threat defense virtual 管理、诊断 0/0、GigabitEthernet 0/0 和 GigabitEthernet 0/1 接口。

- 一个名为 *vm name* -mgmt-SecurityGroup 的安全组。

  此安全组将附加到虚拟机的 Nic0，后者映射到 threat defense virtual 管理接口。

  该安全组包括允许 SSH（TCP 端口 22）和 管理中心 接口（TCP 端口 8305）的管理流量的规则。您可以在部署后修改这些值。

- 公共 IP 地址（根据您在部署期间选择的值命名）。

  您可以为任何接口分配一个公共 IP 地址；请参阅公共 IP 地址中 Azure 关于公共 IP 的准则，包括如何创建、更改或删除公共 IP 地址。

- 如果选择了“新建网络”选项，会创建一个包含四个子网的虚拟网络。
- 每个子网的路由表（如果已存在，则相应更新）

  这些表的名称为“子网名称”-FTDv-RouteTable。

  每个路由表包含通往其他三个子网的路由，threat defense virtual IP 地址作为下一跳。如果流量需要到达其他子网或互联网，您可以选择添加默认路由。

- 所选存储帐户中的启动诊断文件

  启动诊断文件将在 Blobs（二进制大对象）中。

- 所选存储帐户中位于 Blobs 和容器 VHD 下的两个文件，名为 *vm name* -disk.vhd 和 *vm name* -<uuid>.status
- 一个存储帐户（除非您选择了现有的存储帐户）

Note 在删除虚拟机时，必须逐个删除每个资源（您要保留的任何资源除外）。

加速网络 (AN)

Azure 的加速网络 (AN) 功能对 VM 启用单根 I/O 虚拟化 (SR-IOV)，允许 VM NIC 绕过虚拟机监控程序并直接转至下面的 PCIe 卡，以加速网络连接。AN 显著提高 VM 的吞吐性能，还会随着内核的增加（例如较大的 VM）而扩展。

AN 在默认情况下禁用。Azure 支持在预调配的虚拟机上启用 AN。您只需在 Azure 中停止 VM 并更新网卡属性，即可将 *enableAcceleratedNetworking* 参数设置为 true。请参阅 Microsoft 文档：在现有虚拟机上启用加速网络。然后重新启动 VM。

使用 ixgbe-vf 接口的限制

使用 ixgbe-vf 接口时，请注意以下限制：

- 禁止访客 VM 将 VF 设置为混合模式。因此，使用 ixgbe-vf 时不支持透明模式。
- 禁止访客 VM 在 VF 上设置 MAC 地址。因此，在 HA 期间不会像在其他 threat defense virtual 平台上和使用其他接口类型那样传输 MAC 地址。HA 故障转移通过从主用设备向备用设备传送 IP 地址的方式运行。

注释 此限制也适用于 i40e-vf 接口。

- 思科 UCS-B 服务器不支持 ixgbe-vf vNIC。
- 在故障转移设置中，当配对的 threat defense virtual（主设备）发生故障时，备用设备将接管主设备的角色，并使用备用 threat defense virtual 设备的新 MAC 地址更新其接口 IP 地址。此后，threat defense virtual 会向同一网络上的其他设备发送免费地址解析协议 (ARP) 更新，以通告接口 IP 地址的 MAC 地址更改。但是，由于与这些类型的接口不兼容，因此不会将免费 ARP 更新发送到用于将接口 IP 地址转换为全局 IP 地址的 NAT 或 PAT 语句中所定义的全局 IP 地址。

Azure 路由

Azure 虚拟网络子网中的路由取决于子网的有效路由表。有效路由表由内置系统路由和用户定义路由 (UDR) 表中的路由组合而成。

Note 您可以在 VM NIC 属性下查看有效路由表。

您可以查看和编辑用户定义路由表。如果有效路由表是由系统路由与用户定义路由组合而成，系统会优先使用最具体的路由，并关联至用户定义路由表。系统路由表包括指向 Azure 虚拟网络互联网网关的默认路由 (0.0.0.0/0) IPv4 或 [::/0] IPv6。系统路由表还包括通往其他已定义子网的具体路由（下一跳指向 Azure 的虚拟网络基础设施网关）。

要通过 Azure 路由 threat defense virtual 来传输流量，必须在与每个数据子网关联的用户定义路由表中添加/更新路由。应使用该子网上的 threat defense virtual IP 地址作为下一跳来传输相应流量。此外，如果需要，可为 0.0.0.0/0 IPv4 或 [::/0] IPv6 的默认路由加上 threat defense virtual IP 的下一跳。

由于系统路由表中存在现有的具体路由，因此您必须将具体的路由添加到用户定义路由表，以指向作为下一跳的 threat defense virtual。否则，用户定义表中的默认路由将让步于系统路由表中更具体的路由，并且流量将绕过 threat defense virtual。

虚拟网络中虚拟机的路由配置

Azure 虚拟网络中的路由取决于有效路由表，而非客户端上的特定网关设置。系统可能通过 DHCP 为虚拟网络中运行的客户端提供路由，即各个子网上最后一位为 .1 的地址。这是一个占位符，仅用于将数据包传送到虚拟网络的基础设施虚拟网关。一旦数据包离开虚拟机，系统会根据有效路由表（由用户定义表修改）对数据包进行路由。有效路由表确定下一跳，无论客户端是具有配置为 .1 还是 threat defense virtual地址的网关。

Azure 虚拟机 ARP 表将为所有已知主机显示相同的 MAC 地址 (1234.5678.9abc)。这可确保所有离开 Azure 虚拟机的数据包都将到达 Azure 网关，其中有效路由表将用于确定数据包的路径。

IP 地址

以下信息适用于 Azure 中的 IP 地址：

- 系统会为 threat defense virtual 上的第一个 NIC（映射到 Management）提供其附加到的子网中的私有 IP 地址。

  公共 IP 地址可能与此专用 IP 地址相关联，Azure 互联网网关将处理 NAT 转换。

  在部署 threat defense virtual 后，您可以将一个公共 IP 地址与一个数据接口（例如，GigabitEthernet0/0）关联；请参阅公共 IP 地址，了解有关公共 IP 的 Azure 准则，包括如何创建、更改或删除公共 IP 地址。

- 您可以在连接到虚拟机规模集 (VMSS) 中的 threat defense virtual 设备的网络接口中启用 **IP 转发**。如果网络流量不是发往网络接口中的任何已配置 IP 地址，则启用此选项会将此类网络流量转发到虚拟机中配置的 IP 地址以外的其他 IP 地址。有关如何在网络接口中启用 IP 转发 - 启用或禁用 IP 转发，请参阅 Azure 文档。

- 公共 IP 地址（IPv4 和 IPv6）是动态的，在 Azure 停止/启动周期期间可能发生变化。但是，这些地址在 Azure 重新启动期间和 threat defense virtual重新加载期间保持不变。请参阅 IPv6 公用 IP 地址标准。

- 静态的公共 IP 地址不会发生变化，除非您在 Azure 中进行更改。

- Threat Defense Virtual 接口可使用 DHCP 设置其 IP 地址。Azure 基础设施可确保为 threat defense virtual接口分配 Azure 中设置的 IP 地址。

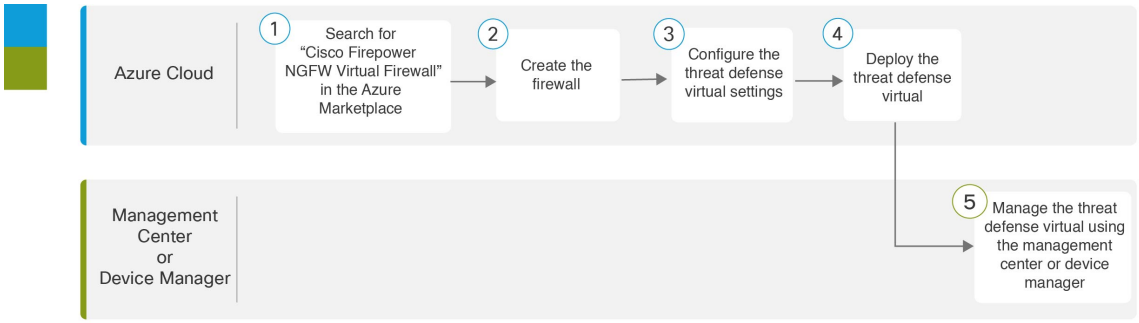
部署 Threat Defense Virtual

您可以使用模板在 Azure 中部署 threat defense virtual。Cisco 提供两种类型的模板：

- **Azure 市场中的解决方案模板**-使用 Azure 市场中提供的解决方案模板， threat defense virtual使用 Azure 门户部署。您可以使用现有资源组和存储帐户（或创建新的资源组和存储帐户）来部署虚拟设备。要使用解决方案模板，请参阅从 Azure 市场使用解决方案模板部署, on page 179。
- **使用来自 VHD**（可从 https://software.cisco.com/download/home 获取）的托管映像的自定义模板 - 除了基于市场的部署，Cisco 还提供一个压缩虚拟硬盘 (VHD)，您可以将其上传到 Azure 以简化 Azure 中的 threat defense virtual 部署过程。使用托管映像和两个 JSON 文件（一个模板文件和一个参数文件），您可以通过一次协调操作部署并调配 threat defense virtual 的所有资源。要使用该自定义模板，请参阅从 Azure 使用 VHD 和资源模板部署, on page 182。

端到端程序

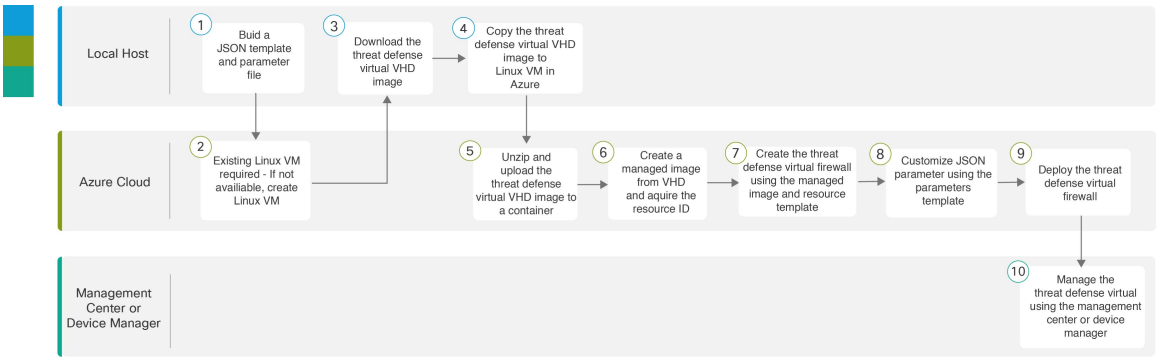
以下流程图说明了使用解决方案模板在 Microsoft Azure 上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	Azure Cloud	从 Azure 市场使用解决方案模板部署：在 Azure 市场中搜索“Cisco Firepower NGFW Virtual Firewall”。
2	Azure Cloud	从 Azure 市场使用解决方案模板部署：创建防火墙。
3	Azure Cloud	从 Azure 市场使用解决方案模板部署：配置 threat defense virtual 设置。
4	Azure Cloud	从 Azure 市场使用解决方案模板部署：部署 threat defense virtual。

	工作空间	步骤
5	管理中心或设备管理器	管理 threat defense virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual

以下流程图说明了使用 VHD 和资源模板在 Microsoft Azure 上部署 threat defense virtual 的工作流程。



	工作空间	步骤
1	本地主机	从 Azure 使用 VHD 和资源模板部署：构建 JSON 模板和参数文件。
2	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：需要现有 Linux VM - 如不可用，请创建 Linux VM： • 使用 Azure CLI 创建 Linux 虚拟机 • 通过 Azure 门户创建 Linux 虚拟机
3	本地主机	从 Azure 使用 VHD 和资源模板部署：从思科下载软件 (使用解决方案模板从 Azure 市场部署) 页面下载 threat defense virtual VHD 映像。
4	本地主机	从 Azure 使用 VHD 和资源模板部署：在 Azure 中将 threat defense virtual VHD 映像复制到 Linux VM。
5	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：解压缩 threat defense virtual VHD 映像并将其上传到容器。
6	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：从 VHD 创建托管映像并获取该映像的资源 ID。
7	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：使用托管映像和资源模板创建 threat defense virtual 防火墙。

	工作空间	步骤
8	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：使用参数模板自定义 JSON 参数。
9	Azure Cloud	从 Azure 使用 VHD 和资源模板部署：部署 threat defense virtual 防火墙。
10	管理中心或设备管理器	管理 threat defense virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual

从 Azure 市场使用解决方案模板部署

以下说明为您展示如何部署 Azure 市场中提供的 threat defense virtual 解决方案模板。这是在 Microsoft Azure 环境中设置 threat defense virtual 所需的顶级步骤列表。如需了解详细的 Azure 设置步骤，请参阅《Azure 入门》。

在 Azure 中部署 threat defense virtual 时，会自动生成各种配置，例如资源、公共 IP 地址（IPv4 和 IPv6）和路由表。您可以在部署后进一步管理这些配置。例如，您可能需要更改超时值较低的“空闲超时”默认值。

Note 要使用 GitHub 存储库中提供的自定义 ARM 模板，请参阅从 Azure 使用 VHD 和资源模板部署, on page 182。

Procedure

步骤 1 登录到 Azure 资源管理器 (ARM) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 依次选择 **Azure 市场** > **虚拟机**。

步骤 3 在市场中搜索“Cisco Firepower NGFW Virtual (Threat Defense Virtual)”，选择提供的产品，然后点击**创建**。

步骤 4 配置基本设置。

a) 输入虚拟机的名称。此名称应在您的 Azure 订用中具有唯一性。

Important
如果使用现有的名称，部署将失败。

b) 选择您的许可方法，可以是 **BYOL** 或 **PAYG**。

选择 **BYOL**（自带许可证）以使用 Cisco 智能许可证帐户。

选择 **PAYG**（即付即用）许可以使用基于使用的计费模式，无需购买 Cisco 智能许可。

Important
您只能在通过 管理中心 管理 threat defense virtual 时使用 **PAYG**。

c) 输入 threat defense virtual 管理员的用户名。

Note
名称“admin”是 Azure 中的预留名称，不能使用。

d) 选择身份验证类型：密码或 SSH 密钥。

如果您选择密码，请输入密码并确认。

如果选择 SSH 密钥，请指定远程对等体的 RSA 公共密钥。

e) 创建密码，以便搭配**管理员**用户帐户登录以配置 threat defense virtual。

f) 从 **FTDv 管理 (FTDv Management)** 下拉列表中选择要注册 threat defense virtual 的管理中心。

如果选择 **FMC：Firepower 管理中心 (FMC: Firepower Management Center)** 作为设备的管理中心，则使用以下选项可以为设备配置管理中心。

- 点击**是 (Yes)** 输入 **FMC 注册信息**。

  1. 输入 **FMC IP** 地址。
  2. 输入用于注册 Threat Defense Virtual 实例的 **FMC 注册密钥**。
  3. [可选] 输入在实例注册期间使用的管理中心 NAT ID。

g) 如果要将部署的虚拟机用作群集，则点击**是**（**提供 day0 群集配置**）**(Yes [provide day0 cluster configuration])** 以创建并输入基本的 day0 配置详细信息。

- 在 **Day0 集群配置 (Day0 cluster configuration)** 字段中输入 day0 配置详细信息。

  有关为 Azure 创建 day0 配置的信息，请参阅在 Azure 上部署 Threat Defense Virtual 集群指南中的为 Azure 创建 Day0 配置。

  Note
  您只能配置部分 day0 配置（集群配置）：“Cluster”: {...} 或者 “run_config”: [...] 详细信息。

h) 选择您的订用。

i) 创建一个新资源组。

threat defense virtual 始终会部署到新的资源组中。仅当现有资源组为空时，部署到现有资源组的选项才有效。

不过，您可以在后续步骤中配置网络选项时将 threat defense virtual 附加到另一个资源组的现有虚拟网络。

j) 选择地理位置。对于此部署中使用的所有资源，此值应相同（例如：Threat Defense Virtual、网络、存储帐户）。

k) 点击**确定 (OK)**。

步骤 5 配置 threat defense virtual 设置。

a) 选择虚拟机大小。
b) 选择一个存储帐户。

Note
您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

c) 选择公共 IP 地址。

您可以为所选的订用和位置选择可用的公共 IP 地址，也可以点击**新建**。

当创建新的公共 IP 地址时，将从 Microsoft 拥有的 IP 地址块中得到一个，因此无法选择特定地址。您可以分配给接口的最大公共 IP 地址数量取决于您的 Azure 订用。

Important
默认情况下，Azure 会创建动态公共 IP 地址。当虚拟机停止和重启时，该公共 IP 可能会变化。如果您首选固定 IP 地址，则应创建静态地址。您也可以在部署后修改公共 IP 地址，将其从动态地址更改为静态地址。

如果 VM 需要分配公用 IPv6 地址，请参阅 IPv6 标准 IPv6 公用 IP 地址标准。

d) 添加 DNS 标签。

Note
完全限定域名等于 DNS 标签加上 Azure URL：<dnslabel>.<location>.cloudapp.azure.com

e) 选择虚拟网络。

您可以选择一个现有 Azure 虚拟网络 (VNet)，或创建一个新的 VNet，然后为其输入 IP 地址空间。默认情况下，无类别域际路由 (CIDR) IP 地址为 10.0.0.0/16。

如果 IPv6 寻址需要虚拟机，您需要在虚拟网络中将其启用。示例：默认情况下，CIDR IPv6 地址为 [ace:cab:deca::/48]。

Note
单独使用 IPv6 无法创建虚拟网络、子网、接口等。默认情况下使用 IPv4，并可以同时启用 IPv6。有关 IPv6 的更多信息，请参阅 Azure IPv6 概述

f) 为 threat defense virtual 网络接口配置四个子网：

- **FTDv 管理**接口，连接到 Azure 中的 Nic0，是“第一子网”
- **FTDv 诊断**接口，连接到 Azure 中的 Nic1，是“第二子网”
- **FTDv 外部**接口，连接到 Azure 中的 Nic2，是“第三子网”
- **FTDv 内部**接口，连接到 Azure 中的 Nic3，是“第四子网”

Note
对于上述子网，如果我们在创建子网时需要 IPv6 配置，请选择 IPv6 选项并为接口配置 IPv6 子网。

g) 提供**公共入站端口 (mgmt.interface)** 输入，以指明是否要为公共开放任何端口。默认选择**无 (None)**。

- 点击**无 (None)** 以创建具有 Azure 默认安全规则的网络安全组并将其连接到管理接口。选择此选项可允许来自同一虚拟网络和 Azure 负载均衡器的流量。

- 点击**允许选定端口查看 (Allow selected ports to view)**，然后选择要开放供互联网访问的入站端口。从**选择入站端口 (Select Inbound Ports)** 下拉列表中选择以下任一端口。默认选择 **SSH (22)**。
  - SSH (22)
  - SFTunnel (8305)
  - HTTPs (443)

h) 点击**确定 (OK)**。

步骤 6 查看配置摘要，然后点击确定 (OK)。

步骤 7 查看使用条款，然后点击**购买**。

部署时间在 Azure 中有所不同。请等候，直到 Azure 报告 threat defense virtual 虚拟机正在运行。

What to do next

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 Cisco Secure Firewall Management Center 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual, on page 409。
- 如果为**启用本地管理器 (Enable Local Manager)** 选择**是 (Yes)**，您将使用集成的 Cisco Secure Firewall 设备管理器 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual, on page 427。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备, on page 1。

从 Azure 使用 VHD 和资源模板部署

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 Threat Defense Virtual 映像。要使用 VHD 映像进行部署，您必须将 VHD 映像上传到您的 Azure 存储帐户。然后，您可以使用上传的磁盘映像和 Azure 资源管理器模板创建托管映像。Azure 模板是包含资源说明和参数定义的 JSON 文件。

开始之前

- Threat Defense Virtual 模板部署需要使用 JSON 模板和相应的 JSON 参数文件。您可以从 Github 存储库下载这些文件。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

如果您需要创建虚拟机，请使用以下方法之一：

- 使用 Azure CLI 创建 Linux 虚拟机
- 通过 Azure 门户创建 Linux 虚拟机

- 在 Azure 订用中，您应该在要部署 Threat Defense Virtual 的位置具有可用的存储帐户。

过程

步骤 1 从 Cisco 下载软件页面下载 Threat Defense Virtual 压缩 VHD 映像：

a) 导航至 **产品** > **安全** > **防火墙** > **下一代防火墙 (NGFW)** > **Cisco Secure Firewall Threat Defense Virtua**。

b) 点击 **Firepower 威胁防御软件**。

按照说明下载映像。

例如，Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

步骤 2 将压缩 VHD 映像复制到您在 Azure 中的 Linux 虚拟机。

用于将文件上传到 Azure 和从 Azure 下载文件的选择很多。此示例显示的是 SCP，即安全复制：

```
# scp /username@remotehost.com/dir/Cisco_Secure_Firewall_Threat_Defense_Virtual-7.1.0-92.vhd.bz2
<linux-ip>
```

步骤 3 登录到 Azure 中的 Linux 虚拟机，并导航至复制了压缩 VHD 映像的目录。

步骤 4 解压缩 Threat Defense Virtual VHD 映像。

用于解压文件的选择很多。此示例显示的是 Bzip2 实用程序，但也可以使用一些基于 Windows 的实用程序。

```
# bunzip2 Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2
```

步骤 5 将 VHD 上传到您的 Azure 存储帐户中的容器。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户名称只能包含小写字母和数字。

用于将 VHD 上传到您的存储帐户的选择很多，包括 AzCopy、Azure 存储复制 Blob API、Azure 存储资源管理器、Azure CLI 或 Azure 门户。对于像 Threat Defense Virtual 这样大的文件，我们不建议使用 Azure 门户。

下例显示了使用 Azure CLI 的语法：

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

步骤 6 从 VHD 创建托管映像：

a) 在 Azure 门户中，选择**映像 (Images)**。

b) 点击**添加 (Add)** 创建新映像。

c) 提供以下信息：

- **订用** - 从下拉列表中选择订用。
- **资源组** - 选择现有资源组或创建一个新资源组。
- **名称** - 为托管映像输入用户定义的名称。
- **区域**- 选择部署虚拟机的区域。
- **操作系统类型**- 选择 **Linux** 作为操作系统类型。
- **VM 生成**- 选择 **第 1 代**。

  注释
  不支持**第 2 代** 。

- **存储 Blob** - 浏览到存储帐户以选择上传的 VHD。
- **账户类型**- 根据您的要求，从下拉列表中选择标准 HDD、标准 SSD 或高级 SSD。

  选择计划用于部署此映像的 VM 大小时，请确保 VM 大小支持所选账户类型。
- **主机缓存** - 从下拉列表中选择“读/写”。
- **数据磁盘** - 保留默认设置；请勿添加数据磁盘。

d) 点击**创建 (Create)**。

等待**通知 (Notifications)** 选项卡下显示**已成功创建映像 (Successfully created image)** 消息。

注释
创建托管映像之后，可以删除上传的 VHD 和上传存储帐户。

步骤 7 获取新创建的托管映像的资源 ID。

在内部，Azure 将每个资源与一个资源 ID 相关联。从该托管映像部署新的 Threat Defense Virtual 防火墙时，将需要资源 ID。

a) 在 Azure 门户中，选择**映像 (Images)**。
b) 选择上一步中创建的托管映像。
c) 点击**概述 (Overview)** 查看映像属性。
d) 将 **Resource ID** 复制到剪贴板。

Resource ID 采用以下形式：

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

步骤 8 使用托管映像和资源模板构建 Threat Defense Virtual 防火墙：

a) 选择**新建 (New)**，然后搜索**模板部署 (Template Deployment)**，直至可从选项中选择它。
b) 选择**创建 (Create)**。
c) 选择**在编辑器中生成自己的模板 (Build your own template in the editor)**。

您有一个可供自定义的空模板。有关模板文件，请参阅 Github。

d) 将您的自定义 JSON 模板代码粘贴到窗口中，然后点击**保存 (Save)**。
e) 从下拉列表中选择**订用 (Subscription)**。
f) 选择现有**资源组 (Resource group)** 或创建一个新资源组。
g) 从下拉列表中选择**位置 (Location)**。
h) 将上一步中的托管映像**资源 ID (Resource ID)** 粘贴到**虚拟机托管映像 ID (Vm Managed Image Id)** 字段中。

步骤 9 点击**自定义部署 (Custom deployment)** 页面顶部的**编辑参数 (Edit parameters)**。您有一个可供自定义的参数模板。

a) 点击**加载文件 (Load file)**，然后浏览到自定义 Threat Defense Virtual 参数文件。有关模板参数，请参阅 Github。
b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后点击**保存 (Save)**。

步骤 10 检查自定义部署详细信息。请确保 **Basics** 和 **Settings** 中的信息与您预期的部署配置（包括 **Resource ID**）相符。

步骤 11 仔细阅读条款和条件，然后选中**我同意上述条款和条件 (I agree to the terms and conditions stated above)** 复选框。

步骤 12 点击**购买 (Purchase)**，使用托管映像和自定义模板部署 Threat Defense Virtual 防火墙。

如果您的模板和参数文件中不存在冲突，则部署应该会成功。

托管映像可用于同一个订用和区域内的多个部署。

下一步做什么

- 在 Azure 中更新 Threat Defense Virtual 的 IP 配置。

关于在 Azure 上部署无诊断接口的 Threat Defense Virtual

在 Cisco Secure Firewall 版本 7.3 及更低版本上， Threat Defense Virtual 部署至少有 4 个接口 - 1 个管理接口、1 个诊断接口和 2 个数据接口。

从 Cisco Secure Firewall 版本 7.4.1 开始，您可以删除诊断接口，并使用至少 3 个接口（1 个管理接口和 2 个数据接口）部署 Threat Defense Virtual。此功能支持在同一实例类型上使用其他数据接口部署 Threat Defense Virtual。例如，在标准 D4_v2 VM 实例上，您现在可以部署具有 1 个管理接口和 7 个数据接口的 Threat Defense Virtual，而不是部署具有 1 个管理接口、1 个诊断接口和 6 个数据接口的 Threat Defense Virtual。

从 Cisco Secure Firewall 版本 7.4.1 开始，我们建议您在没有诊断接口的 Azure 上部署 Threat Defense Virtual。

只有在 Azure 上新部署的 Threat Defense Virtual 实例才支持此功能。

注释 由于支持的最大接口数为 8，因此在部署 Threat Defense Virtual 后最多可以添加 5 个接口，以拥有最多 8 个接口。

在 Azure 上部署无诊断接口的 Threat Defense Virtual 的准则和限制

- 当诊断接口被删除时，系统日志和 SNMP 支持使用 Threat Defense Virtual 管理或数据接口，而不是使用诊断接口。
- 此部署支持集群和自动扩展。
- 不支持将具有诊断接口端口的 Threat Defense Virtual 实例和不具有诊断接口端口的 Threat Defense Virtual 实例分组。

注释 此处的 Threat Defense Virtual 实例分组是指 Azure 上的虚拟机规模集 (VMSS) 中的实例分组。这与 Management Center Virtual 上的 Threat Defense Virtual 实例的分组无关。

- 不支持 CMI。

NIC 到数据接口的映射，以便在 AWS 上部署无诊断接口的 Threat Defense Virtual

下面给出了 NIC 到数据接口的映射，用于在 Azure 上部署无诊断接口的 Threat Defense Virtual。

Net-Interface	Vnet/Subnet	Port
NIC0	mgmt-subnet	Management
NIC1	diag-subnet	M0/0*
NIC2	inside-subnet	Gig0/0
NIC3	outside-subnet	Gig0/1

Threat Defense Virtual-4-NICs

*Diagnostic interface

Net-Interface	Vnet/Subnet	Port
NIC0	mgmt-subnet	Management
NIC1	inside-subnet	Gig0/0
NIC2	outside-subnet	Gig0/1

Threat Defense Virtual-3-NICs

在 Azure 上部署无诊断接口的 Threat Defense Virtual

执行下面给出的步骤，在没有诊断接口的情况下部署 Threat Defense Virtual。

过程

步骤 1 根据您的部署选项，您可以使用以下方法之一来启用此功能。

- **Solution template in the Azure Marketplace** – 在 Azure 控制台上，搜索 **Cisco Secure Firewall Threat Defense Virtual - BYOL 和 PAYG**，然后点击**创建 (Create)**。在**基本 (Basics)** 信息窗口中，输入所需信息，然后从**软件版本 (Software version)** 下拉列表中选择 **7.4.x**。选择**连接诊断接口 (Attach diagnostic interface)** 旁边的**否 (No)**按钮。默认选择否。

  有关在 Azure 市场中使用解决方案模板在 Azure 上部署 Threat Defense Virtual 的完整程序，请参阅从 Azure 市场使用解决方案模板部署。

- **Custom Template using a Managed Image from a VHD** – 转到**虚拟机 (Virtual machines)** > **+ 创建 (+ Create)** > **Azure 虚拟机 (Azure Virtual Machine)** > **高级 (Advanced)** 窗口，然后在 **Custom data** 字段中输入包含键值对 **Diagnostic: OFF** 的 day-0 配置脚本。以下显示了您可以在 **Custom data** 字段中输入的 day-0 配置脚本示例。

  ```
  {
  "AdminPassword": "E28@2OiUrhx!",
  "Hostname": "ciscothreatdefensevirtual",
  "FirewallMode": "routed",
  "ManageLocally": "No",
  "Diagnostic": "OFF"
  }
  ```

  注释
  键值对 "Diagnostic": "ON/OFF" 区分大小写。

  您还可以在用于全新部署的 ARM 模板的 **Customdata** 字段中修改脚本。默认情况下，键值对设置为 **Diagnostic: ON**，并且会启动诊断接口。当键值对设置为 **Diagnostic: OFF** 时，部署将在没有诊断接口的情况下启动。

  有关使用 VHD 中的托管映像使用自定义模板在 Azure 上部署 Threat Defense Virtual 的完整程序，请参阅从 Azure 使用 VHD 和资源模板部署。

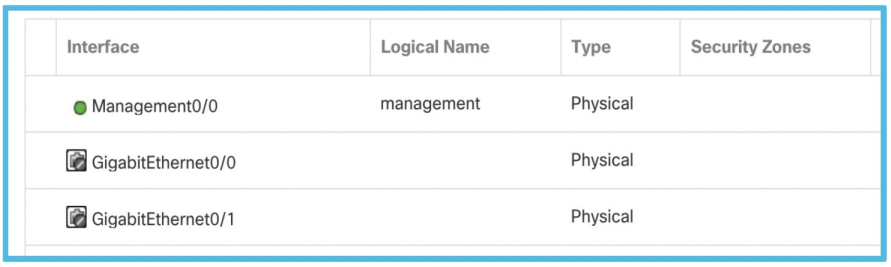
步骤 2 连接所需的最少 3 个 NIC。有关在 Azure 上连接接口的详细信息，请参阅在 Azure 上的虚拟机中添加网络接口或从中删除网络接口。

图 *6: Azure* 上的网络接口连接

有关接口的详细信息，请参阅接口概况。

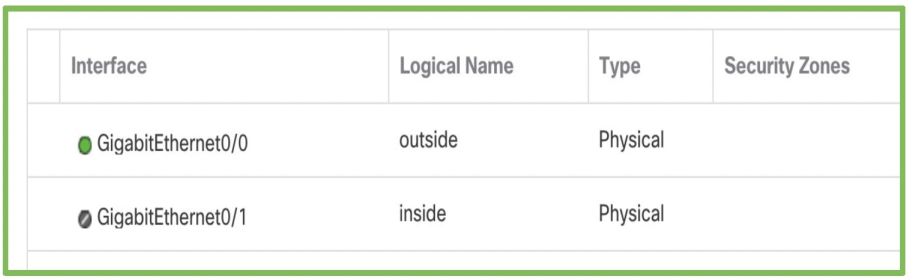
步骤 3 （可选）在控制台上使用 **show interface ip brief** 命令可显示接口详细信息。您还可以在 Management Center Virtual 上查看接口详细信息，如下所示

接口在 Management Center Virtual 上显示，如下所示。



Interface	Logical Name	Type	Security Zones
Management0/0	management	Physical	
GigabitEthernet0/0		Physical	
GigabitEthernet0/1		Physical	

With Diagnostic Interface



Interface	Logical Name	Type	Security Zones
GigabitEthernet0/0	outside	Physical	
GigabitEthernet0/1	inside	Physical	

Without Diagnostic Interface

升级场景

您可以根据以下场景升级 Threat Defense Virtual 实例。

- 所有 Cisco Secure Firewall 版本 – 您可以将部署了诊断接口的 Threat Defense Virtual 实例升级为具有诊断接口的 Threat Defense Virtual 实例。

- Cisco Secure Firewall 7.4 及更高版本 - 您可以将没有诊断接口的 Threat Defense Virtual 部署实例升级为没有诊断接口的 Threat Defense Virtual 实例。

不支持以下升级场景。

- 所有 Cisco Secure Firewall 版本 - 无法将部署了诊断接口的 Threat Defense Virtual 实例升级到没有诊断接口的 Threat Defense Virtual 实例。
- Cisco Secure Firewall 7.4.1 及更高版本 - 您无法将没有诊断接口的 Threat Defense Virtual 部署实例升级为具有诊断接口的 Threat Defense Virtual 实例。

注释 升级后，NIC 的数量和顺序均保持不变。

部署不带诊断接口的 Threat Defense Virtual 集群或 Auto Scale 解决方案

要在不使用诊断接口的情况下对 Threat Defense Virtual 集群或由 Threat Defense Virtual 实例组成的自动扩展解决方案执行新部署，请确保在 day-0 配置脚本中将键值对 **Diagnostic: OFF/ON** 设置为 **OFF**。

故障排除

如果在部署 Threat Defense Virtual 时未删除诊断接口，请检查键值对 **Diagnostic: OFF/ON** 是否已在 day-0 配置脚本中设置为 **OFF**。

适用于 Azure 上的 威胁防御虚拟的 Auto Scale 解决方案

概述

Auto Scale 解决方案支持资源分配，以满足性能要求并降低成本。如果资源需求增加，系统将确保根据需要分配资源。如果资源需求减少，则会取消分配资源以降低成本。

threat defense virtual Auto Scale for Azure 是完整的无服务器实现，它利用 Azure 提供的无服务器基础架构（逻辑应用、Azure 函数、负载均衡器、安全组、虚拟机规模集等）。

threat defense virtual Auto Scale for Azure 实现的一些主要功能包括：

- 基于 Azure Resource Manager (ARM) 模板的部署。
- 支持基于 CPU 和内存 (RAM) 的扩展指标。

注释 有关详细信息，请参阅Auto Scale 逻辑， 第 227 页。

- 支持 threat defense virtual 部署和多可用性区域。
- 管理中心 中完全自动化的 threat defense virtual实例注册和取消注册。
- 自动应用到外向扩展 threat defense virtual实例的 NAT 策略、访问策略和路由。
- 对负载均衡器和多可用性区域的支持。
- 支持启用和禁用 Auto Scale 功能。
- 仅适用于 管理中心；不支持 设备管理器。
- 支持使用 PAYG 或 BYOL 许可模式部署 threat defense virtual。PAYG 仅适用于 threat defense virtual软件版本 6.5 和更高版本。请参阅支持的软件平台， 第 190 页。
- 思科提供 Auto Scale for Azure 部署包以方便部署。

Azure 上的 threat defense virtual Auto Scale 解决方案支持两种使用不同拓扑配置的使用案例：

- 使用三明治拓扑的 Auto Scale – 它将 threat defense virtual 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。
- 使用 Azure 网关负载均衡器 (GWLB) 的 Auto Scale - Azure GWLB 与安全防火墙、公共负载均衡器和内部服务器集成，以简化防火墙的部署、管理和扩展。

支持的软件平台

threat defense virtual Auto Scale 解决方案适用于 管理中心 管理的 threat defense virtual，与软件版本无关。Cisco Secure Firewall Threat Defense 兼容性指南提供软件和硬件兼容性，包括操作系统和托管环境要求。

- 管理中心：虚拟表列出了 Management Center Virtual 的兼容性和虚拟托管环境要求。
- Threat Defense Virtual 兼容性表列出了 Azure 上 threat defense virtual的兼容性和虚拟托管环境要求。

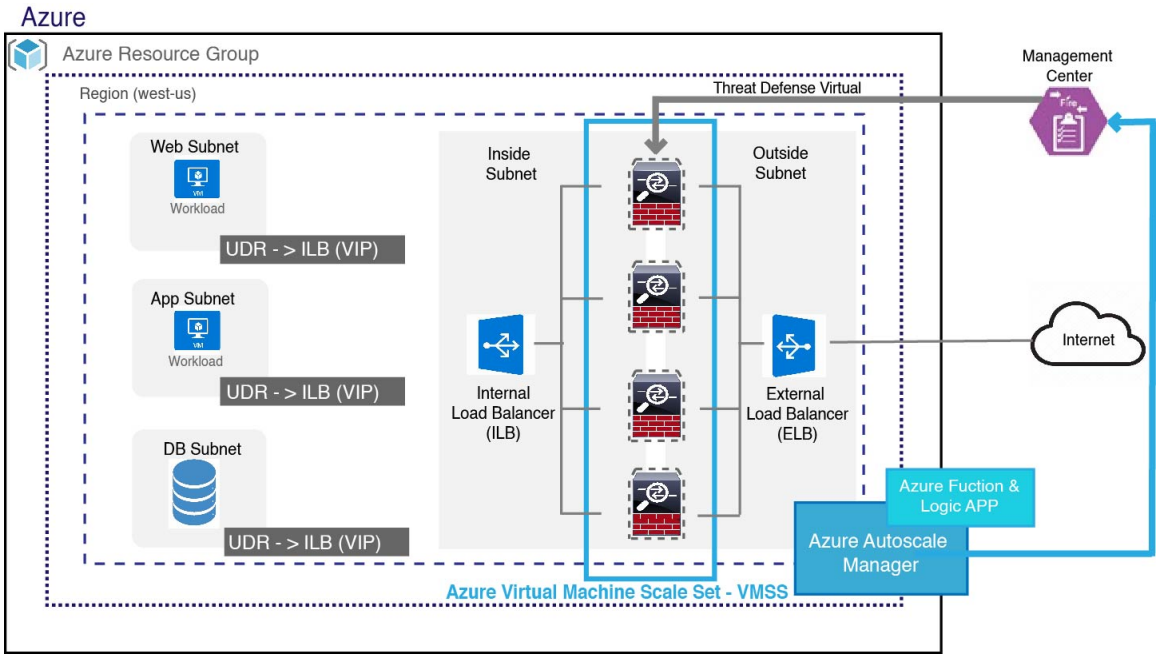
注释 就部署 Azure Auto Scale 解决方案而言，Azure 上的 threat defense virtual最低支持的版本是版本 6.4。

使用三明治拓扑的 Auto Scale 使用案例

适用于 Azure 的 threat defense virtual Auto Scale 是一种自动化水平扩展解决方案，它将 threat defense virtual 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。

- ELB 将流量从互联网分发到规模集中的 threat defense virtual实例；然后，防火墙将流量转发到应用程序。
- ILB 将出站互联网流量从应用程序分发到规模集中的 threat defense virtual实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 threat defense virtual实例数将根据负载条件自动进行扩展和配置。

图 *7:* 使用三明治拓扑的 ***Threat Defense Virtual Auto Scale*** 使用案例图



Auto Scale 与 Azure 网关负载均衡器使用案例

Azure 网关负载均衡器 (GWLB) 可确保安全防火墙检查进出 Azure VM（例如应用服务器）的互联网流量，而无需更改任何路由。Azure GWLB 与安全防火墙的集成简化了防火墙的部署、管理和扩展。这种集成还降低了操作复杂性，并为防火墙上的流量提供了单一的入口和出口点。应用和基础设施可以保持源 IP 地址的可视性，而这在某些环境中至关重要。

在 Azure GWLB Auto Scale 使用案例中，threat defense virtual 只会使用两个接口：管理接口和一个数据接口。

注释

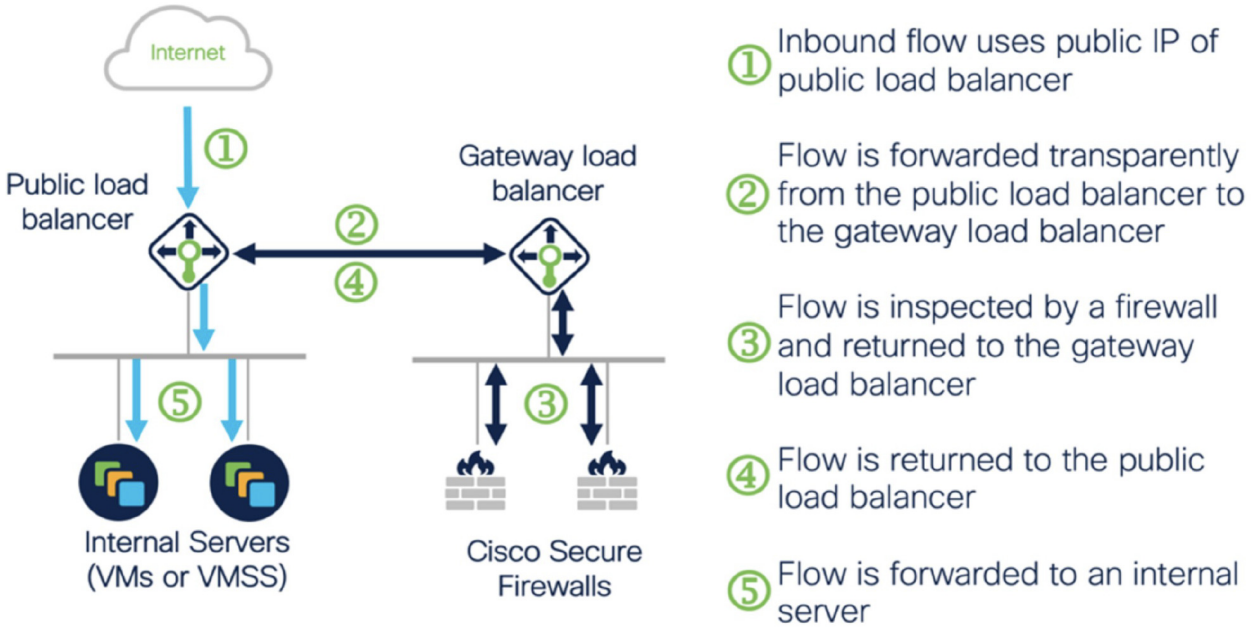
- 如果要部署 Azure GWLB，则不需要网络地址转换 (NAT)。
- 仅支持 IPv4。

许可

支持 PAYG 和 BYOL。

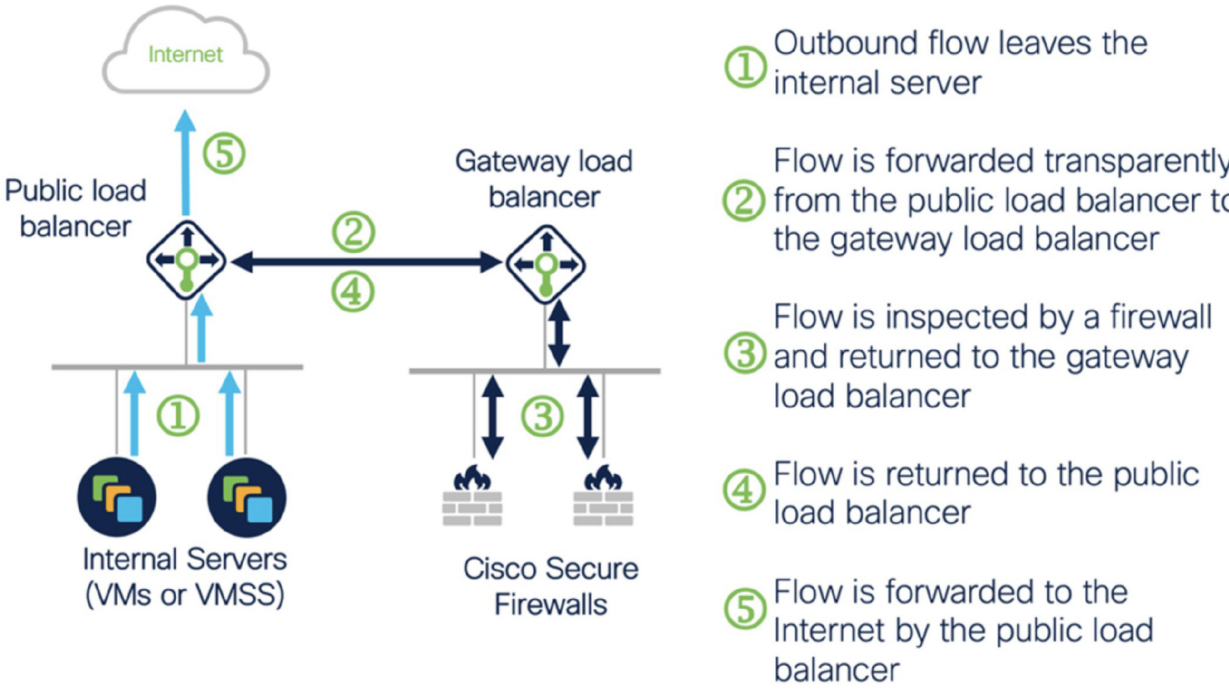
入站流量使用案例和拓扑

下图显示了入站流量的流量。



出站流量使用案例和拓扑

下图显示了出站流量的流量。

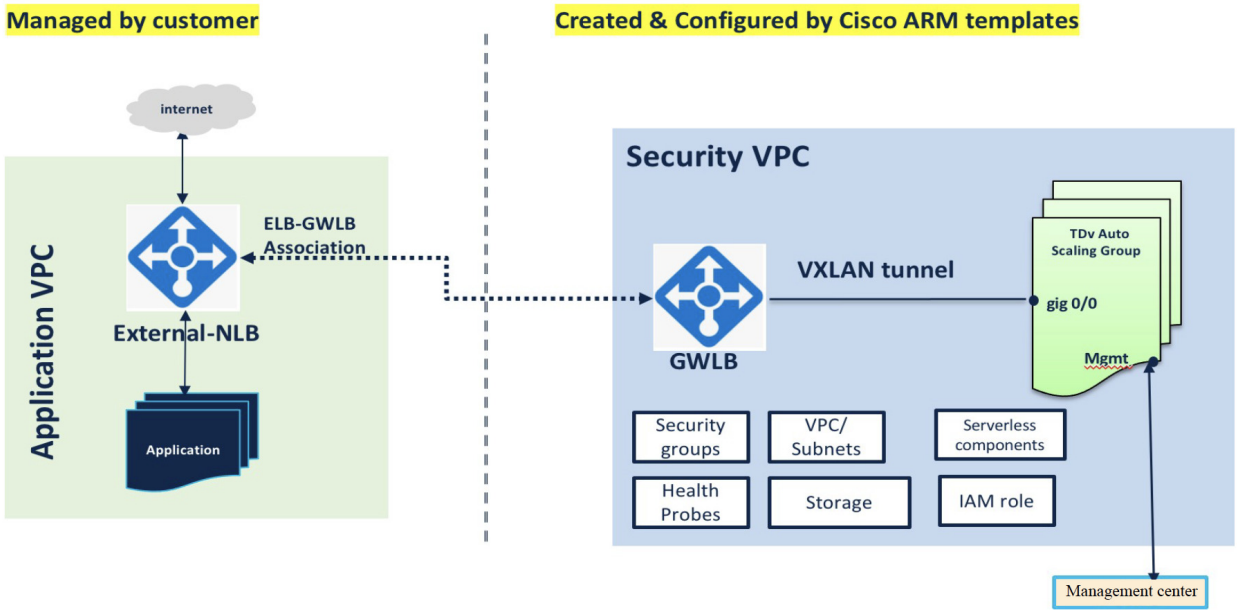


注释 要部署和配置管理中心，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的程序。使用已部署的管理中心来管理威胁防御虚拟实例。

应用 VPC 和安全 VPC 之间的流量

在下图中，流量从现有拓扑重定向至防火墙，以便由外部负载均衡器进行检查。然后，流量将被路由到新创建的 GWLB。路由到 ELB 的任何流量都会别转发到 GWLB。

然后，GWLB 将 VXLAN 封装的流量转发到 threat defense virtual 实例。您必须创建两个 threat defense virtual 关联，因为 GWLB 会对入口和出口流量使用两个单独的 VXLAN 隧道。threat defense virtual 会解封装 VXLAN 封装的流量，对其进行检查，然后将流量路由到 GWLB。然后，GWLB 将流量转发到 ELB。



适用范围

本文档介绍部署 threat defense virtual Auto Scale for Azure 解决方案以及 Auto Scale with Azure GWLB 解决方案的无服务器组件的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

下载部署软件包

使用三明治拓扑的面向 Azure 的 threat defense virtual Auto Scale 解决方案是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

threat defense virtual Auto Scal with Azure GWLB 解决方案是一个基于 ARM 模板的部署，可以创建 GWLB、网络基础设施、威胁防御虚拟 自动扩展组、无服务器组件和其他所需资源。

两种解决方案的部署过程均类似。

下载启动面向 Azure 的 threat defense virtual Auto Scale 解决方案所需的文件。您的版本的部署脚本和模板可从 GitHub 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数，第 230 页。

Auto Scale 解决方案组件

以下组件构成了 threat defense virtual Auto Scale for Azure 解决方案。

Azure Functions（函数应用）

函数应用是一组 Azure 函数。基本功能包括：

- 定期交流/探测 Azure 指标。
- 监控 threat defense virtual 负载和触发内向扩展/外向扩展操作。
- 向 管理中心 注册新的 threat defense virtual。
- 通过 管理中心 配置新的 threat defense virtual。
- 从 管理中心 取消注册（删除）内向扩展的 threat defense virtual。

这些函数以压缩 Zip 包的形式提供（请参阅构建 Azure 函数应用包，第 197 页）。这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

Orchestrator（逻辑应用）

Auto Scale 逻辑应用是一个工作流，即按照一定序列的步骤集合。Azure 函数是独立的实体，无法彼此通信。此协调器按顺序排列这些函数的执行，并在它们之间交换信息。

- 逻辑应用可用于编排 Auto Scale Azure 函数并在函数之间传递信息。
- 每个步骤代表一个 Auto Scale Azure 函数或内置标准逻辑。
- 逻辑应用作为 JSON 文件交付。
- 可以通过 GUI 或 JSON 文件自定义逻辑应用。

虚拟机规模集 (VMSS)

VMSS 是同构虚拟机（如 threat defense virtual 设备）的集合。

- VMSS 可以向集合中添加新的相同虚拟机。
- 添加到 VMSS 的新虚拟机将自动与负载均衡器、安全组和网络接口连接。
- VMSS 具有内置 Auto Scale 功能，该功能对适用于 Azure 的 threat defense virtual 禁用。
- 您不应在 VMSS 中手动添加或删除 threat defense virtual 实例。

Azure Resource Manager (ARM) 模板

ARM 模板用于部署 threat defense virtual Auto Scale for Azure 解决方案所需的资源。

威胁防御虚拟 Auto Scale for Azure - ARM 模板**azure_ftdv_autoscale.json**为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机规模集 (VMSS)
- 内部/外部负载均衡器。
- 部署所需的安全组和其他各种组件。

威胁防御虚拟 Auto Scale with Azure GWLB - ARM 模板 **azure_ftdv_autoscale_with_GWLB.json**为 Auto Scale Manager 组件提供输入，包括以下组件：

- Azure 函数应用
- Azure 逻辑应用
- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网络基础设施
- 网关负载均衡器
- 部署所需的安全组和其他各种组件

重要事项 ARM 模板在验证用户输入方面有限制，因此您需要在部署过程中负责验证输入。

前提条件

Azure 资源

资源组

部署此解决方案的所有组件需要一个现有的或新创建的资源组。

注释 记录资源组名称、创建它的区域，以及供以后使用的 Azure 订用 ID。

网络

确保虚拟网络可用或已创建。使用三明治拓扑的 Auto Scale 部署不会创建、更改或管理任何网络资源。 但请注意，使用 Azure GWLB 进行 Auto Scale 部署会创建网络基础设施。

threat defense virtual 需要四个网络接口，因此您的虚拟网络需要四个子网以用于：

1. 管理流量
2. 诊断流量
3. 内部流量
4. 外部流量

应在子网所连接的网络安全组中打开以下端口：

- SSH(TCP/22)

  负载均衡器与 threat defense virtual 之间的运行状况探测所必需。

  无服务器函数与 threat defense virtual 之间的通信所必需。

- TCP/8305

  threat defense virtual 与 管理中心 之间的通信所必需。

- HTTPS(TCP/443)

  无服务器组件与 管理中心 之间的通信所必需。

- 应用程序特定协议/端口

  任何用户应用程序所必需（例如，TCP/80 等）。

注释 记录虚拟网络名称、虚拟网络 CIDR、所有 4 个子网的名称，以及外部和内部子网的网关 IP 地址。

构建 Azure 函数应用包

threat defense virtual Auto Scale 解决方案要求您构建一个存档文件：*ASM_Function.zip*，它以压缩 ZIP 包的形式提供一组离散的 Azure 函数。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数 ，第 230 页。

这些函数尽可能离散以执行特定任务，可以根据需要进行升级，以提供增强功能和新版本支持。

准备 管理中心

您可以使用 管理中心 来管理 threat defense virtual，这是一个功能齐全的多设备管理器。threat defense virtual 向您分配给 threat defense virtual 计算机的管理接口上的 管理中心 注册并与之通信。

创建 threat defense virtual 配置和管理所需的所有对象，包括设备组，以便您能够轻松地在多个设备上部署策略和安装更新。设备组上应用的所有配置都将被推送到 threat defense virtual 实例。

以下各节简要概述准备 管理中心 的基本步骤。有关完整信息，您应咨询完整的《Cisco Secure Firewall Management Center 配置指南》。准备 管理中心 时，请确保记录以下信息：

- 管理中心 公共 IP 地址。
- 管理中心 用户名/密码。
- 安全策略名称。
- 内部和外部安全区域对象名称。
- 设备组名称。

创建新的 管理中心 用户

在 管理中心 中创建具有 Admin 权限的新用户，以便仅供 AutoScale Manager 使用。

重要事项 为了避免与其他 管理中心 会话冲突，拥有专用于 threat defense virtual Auto Scale 解决方案的 管理中心 用户帐户非常重要。

过程

步骤 1 在 管理中心 中创建具有 Admin 权限的新用户。选择**系统** > **用户**，然后点击**创建用户**。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含句点 (.)、at 符号 (@) 或斜线 (/)

步骤 2 根据环境需要完成用户选项。有关完整信息，请参阅《Cisco Secure Firewall Management Center 管理指南》。

配置访问控制

配置访问控制以允许从内部到外部的流量。在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。对规则正确进行配置和排序对于构建有效的部署至关重要。请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的“访问控制最佳实践”。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**新建策略**。

步骤 3 在**名称 (Name)** 和**说明 (Description)**（可选）中输入唯一名称和说明。

步骤 4 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 以便为部署配置安全设置和规则。

配置许可

所有许可证都由管理中心提供给威胁防御。您可以选择购买以下功能许可证：

- **Cisco Secure Firewall Threat Defense IPS** — 安全智能和 Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense 恶意软件防御** — 恶意软件防御
- **Cisco Secure Firewall Threat Defense URL 过滤** — URL 过滤
- **RA VPN** - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

注释 购买 IPS、恶意软件防御或 URL 过滤许可证时，您还需要匹配的订用许可证以获取 1 年、3 年或 5 年的更新。

开始之前

- 拥有思科智能软件管理器主帐户。

  如果您还没有账户，请点击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主帐户。

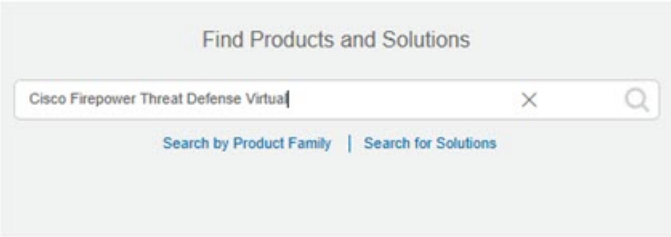
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 8: 许可证搜索



注释
如果未找到 PID，您可以手动将 PID 添加到订单中。

步骤 2 如果尚未执行此操作，请向智能许可服务器注册管理中心。

注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 《Cisco Secure Firewall Management Center 管理指南》 。

创建安全区域对象

为您的部署创建内部和外部安全区域对象。

过程

步骤 1 选择**对象** > **对象管理**。
步骤 2 从对象类型列表中选择**接口**。
步骤 3 点击**添加** > **安全区域**。
步骤 4 输入一个**名称**（例如，*inside*、*outside*）。
步骤 5 选择**已路由**作为**接口类型**。
步骤 6 点击**保存 (Save)**。

创建设备组

可以使用设备组轻松分配策略，并在多台设备上安装更新。

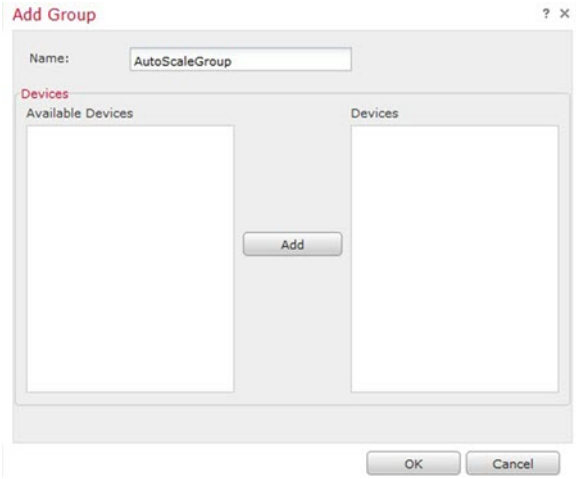
过程

步骤 1 选择**设备** > **设备管理**。

图 *9:* 设备管理

步骤 2 从**添加 (Add)** 下拉菜单中，选择**添加组 (Add Group)**。
步骤 3 输入 **Name**。例如，*AutoScaleGroup*。

图 *10:* 添加设备组



步骤 4 点击**确定 (OK)** 以添加组。

图 *11:* 已添加设备组

配置安全外壳访问

威胁防御 设备的平台设置用于配置您可能希望在多台设备之间共享其值的一系列无关功能。适用于 Azure 的 Threat Defense Virtual Auto Scale 需要 威胁防御 平台设置策略，以便允许在内部/外部区域和为 Auto Scale 组创建的设备组上使用 SSH。这是必需的，以便 threat defense virtual 的数据接口可以响应负载均衡器的运行状况探测。

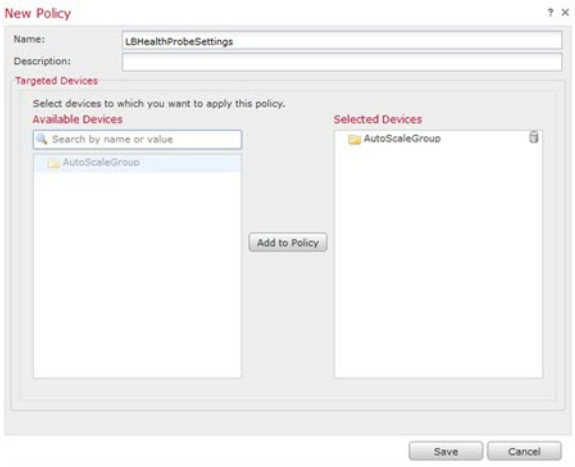
开始之前

您需要定义允许与设备建立 SSH 连接的主机或网络网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象** > **对象管理**以配置对象。例如，参阅以下步骤中的 *azure-utility-ip (168.63.129.16)* 对象。

过程

步骤 1 选择**设备 (Devices)** > **平台设置 (Platform Settings)**，然后创建或编辑 威胁防御 策略，例如 *LBHealthProbeSettings*。

图 *12:* 威胁防御 平台设置策略



步骤 2 选择**安全外壳**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

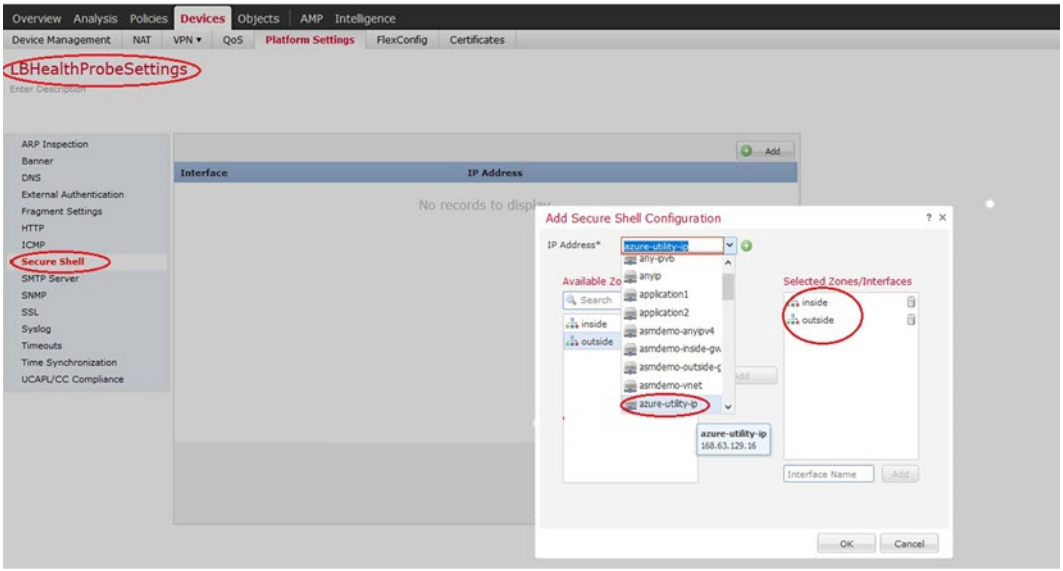
b) 配置规则属性：

- **IP 地址** - 用于标识您允许进行 SSH 连接的主机或网络的网络对象（例如，*azure-utility-ip (168.63.129.16)*）。从下拉列表中选择一个对象，或者点击“+”添加新的网络对象。
- **安全区域** - 添加包含将允许进行 SSH 连接的接口的区域。例如，您可以将内部接口分配到**内部**区域，而将外部接口分配到**外部**区域。您可以从 管理中心 的**对象 (Objects)** 页面创建安全区域。有关安全区域的完整信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

  注释
  在具有 Azure 网关负载均衡器的 Auto Scale 使用案例中不使用内部接口。

- 点击**确定 (OK)**。

图 *13: Threat Defense Virtual Auto Scale* 的 *SSH* 访问



步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署** > **部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

注释

您还可以为运行状况探测配置 TCP 端口 443，而不是使用 **SSH 访问**。要执行此操作，请转至**设备 (Devices)** > **平台设置 (Platform settings)** > **HTTP 访问 (HTTP Access)**，选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框，然后在**端口 (Port)** 字段中输入 **443**。将此设置与内部和外部接口相关联。您还必须将 ARM 模板中的运行状况探测端口更改为 443。有关配置 HTTP 访问的详细信息，请参阅配置 HTTP。

配置 NAT

创建 NAT 策略并创建必要的 NAT 规则，以便将流量从外部接口转发到应用程序，然后将此策略连接到您为自动扩展创建的设备组。

注释 仅当使用夹层拓扑配置自动扩展时，才需要配置 NAT。

过程

步骤 1 选择**设备** > **NAT**。

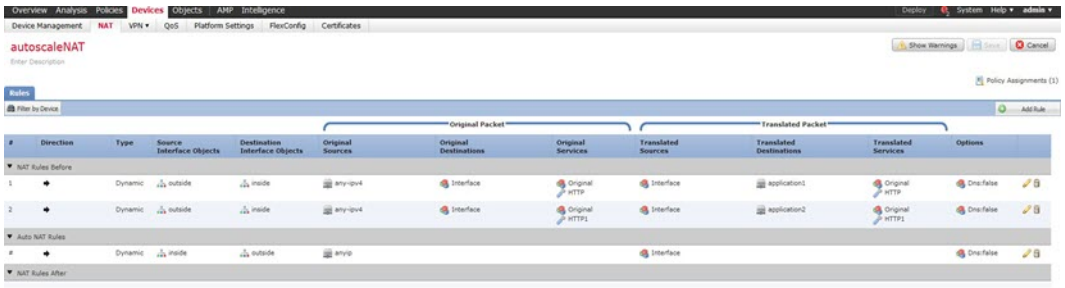
步骤 2 从**新策略**下拉列表中，选择**威胁防御 NAT**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 输入说明 **(Description)**（可选）。

步骤 5 配置您的 NAT 规则。有关如何创建 NAT 规则和应用 NAT 策略的准则，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》中的“为威胁防御配置 NAT”。下图所示为基本方法。

图 *14: NAT* 策略示例



注释
我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。

步骤 6 点击保存 **(Save)**。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，您可以在将 ARM 模板部署到 Azure 订用时使用这些参数创建 threat defense virtual 设备。请参阅部署 Auto Scale ARM 模板，第 211 页。在 Auto Scale with Azure GWLB 解决方案中，还会创建网络基础设施，因此必须在模板中配置其他输入参数。参数说明的含义不言自明。

表 *20:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串*（3-10 个字符）	所有资源都使用包含此前缀的名称创建。 注：只能使用小写字母。 示例：ftdv	New
virtualNetworkRg	字符串	虚拟网络资源组名称。 示例：cisco-virtualnet-rg	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）。 示例：cisco-virtualnet	现有

参数名	允许的值/类型	说明	资源创建类型
virtualNetworkCidr	CIDR 格式 x.x.x.x/y	虚拟网络的 CIDR（已创建）	现有
mgmtSubnet	字符串	管理子网名称（已创建） 示例：cisco-mgmt-subnet	现有
diagSubnet	字符串	诊断子网名称（已创建）。 示例：cisco-diag-subnet	现有
insideSubnet	字符串	内部子网名称（已创建）。 示例：cisco-inside-subnet	现有
internalLbIp	字符串	内部子网的内部负载均衡器 IP 地址（已创建）。 例如：1.2.3.4	现有
insideNetworkGatewayIp	字符串	内部子网网关 IP 地址（已创建）。	现有
outsideSubnet	字符串	外部子网名称（已创建）。 示例：cisco-outside-subnet	现有
outsideNetworkGatewayIp	字符串	外部子网网关 IP（已创建）。	现有
deviceGroupName	字符串	管理中心中的设备组（已创建）	现有
insideZoneName	字符串	管理中心中的内部区域名称（已创建）	现有
outsideZoneName	字符串	管理中心中的外部区域名称（已创建）	现有
softwareVersion	字符串	threat defense virtual 版本（在部署期间从下拉列表中选择）。	现有
vmSize	字符串	threat defense virtual 实例的大小（在部署过程中从下拉列表中选择）。	不适用
ftdLicensingSku	字符串	Threat Defense Virtual 许可模式 (PAYG/BYOL) 注：PAYG 在版本 6.5+ 中受支持。	不适用

参数名	允许的值/类型	说明	资源创建类型
licenseCapability	逗号分隔的字符串	BASE, MALWARE, URLFilter, THREAT	不适用
ftdVmManagementUserName	字符串*	threat defense virtual VM 管理管理员用户名。 这**不能**是“admin”。请参阅 Azure 以了解 VM 管理员用户名准则。	New
ftdVmManagementUserPassword	字符串*	threat defense virtual VM 管理管理员用户的密码。 密码的长度必须为 12 至 72 个字符，而且必须具有：小写、大写、数字及特殊字符；重复字符不得超过 2 个。 **注释** 模板中不对此进行合规性检查。	New
fmcIpAddress	字符串 x.x.x.x	管理中心 的公共 IP 地址（已创建）	现有
fmcUserName	字符串	管理中心用户名，具有管理权限（已创建）	现有
fmcPassword	字符串	上述 管理中心 用户名的 管理中心 密码（已创建）	现有
policyName	字符串	在 管理中心 中创建的安全策略（已创建）	现有

参数名	允许的值/类型	说明	资源创建类型
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 threat defense virtual 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 **POLICY-2**：当自动扩展组中所有 threat defense virtual 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 在两种情况下，内向扩展逻辑都保持不变：当所有 threat defense virtual 设备的平均负载在所配置的持续时间内低于内向扩展阈值时，将触发内向扩展。	不适用
scalingMetricsList	字符串	用于制定扩展决策的指标。 允许：CPU CPU、内存 默认值：CPU	不适用
cpuScaleInThreshold	字符串	CPU 指标的内向扩展阈值（以百分比为单位）。 默认值：10 当 threat defense virtual 指标低于此值时，将触发扩展。 请参阅Auto Scale 逻辑，第 227 页。	不适用
cpuScaleOutThreshold	字符串	CPU 指标的横向扩展阈值（以百分比为单位）。 默认值：80 当 threat defense virtual指标高于此值时，将触发横向扩展。 “cpuScaleOutThreshold”应始终大于“cpuScaleInThreshold”。 请参阅Auto Scale 逻辑，第 227 页。	不适用

参数名	允许的值/类型	说明	资源创建类型
memoryScaleInThreshold	字符串	内存指标的内向扩展阈值（以百分比为单位）。 默认值：0 当 threat defense virtual 指标低于此值时，将触发扩展。 请参阅Auto Scale 逻辑，第 227 页。	不适用
memoryScaleOutThreshold	字符串	内存指标的横向扩展阈值（以百分比为单位）。 默认值：0 当 threat defense virtual指标高于此值时，将触发横向扩展。 “memoryScaleOutThreshold”应始终**大于**“memoryScaleInThreshold”。 请参阅Auto Scale 逻辑，第 227 页。	不适用
minFtdCount	整数	在任何给定时间，规模集中可用的最小 threat defense virtual 实例数。 示例：2	不适用
maxFtdCount	整数	规模集中允许的最大 threat defense virtual 实例数。 示例：10 **注释** 此数量受 管理中心 容量的限制。 Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用

参数名	允许的值/类型	说明	资源创建类型
metricsAverageDuration	整数	从下拉列表中选择。 此数字表示计算指标平均值的时间（以分钟为单位）。 如果此变量的值为 5（即 5 分钟），则当计划 Auto Scale Manager 时，它将检查过去 5 分钟内的指标平均值，并且基于此平均值做出扩展决定。 注释 由于 Azure 限制，仅 1、5、15 和 30 是有效数字。	不适用

参数名	允许的值/类型	说明	资源创建类型
initDeploymentMode	BULK/STEP	主要适用于第一次部署，或者规模集不包含任何 threat defense virtual 实例时。 BULK：Auto Scale 管理器将尝试一次并行部署“minFtdCount”数量的 threat defense virtual 实例。 **注释** 启动采用并行方式，但由于 管理中心 的限制，需要按顺序注册到 管理中心。 STEP：Auto Scale 管理器将按照计划间隔逐个部署“minFtdCount”数量的 threat defense virtual 设备。 **注释** STEP 选项需要较长时间来启动“minFtdCount”数量的实例并使用 管理中心 进行配置，然后实现运行，但在调试时很有帮助。 BULK 选项启动所有“minFtdCount”数量的 threat defense virtual 所花费的时间与一次 threat defense virtual 启动相同（因为它是并行运行的），但 管理中心 注册是按顺序进行的。 部署“minFtdCount”数量的 threat defense virtual 所花费的总时间 =（启动一个 threat defense virtual 所用的时间 + 注册/配置一个 threat defense virtual 所用的时间 * minFtdCount）。	
*Azure 对新资源的命名约定有限制。查看限制，或者直接全部使用小写字母。**不要使用空格或任何其他特殊字符**。			

部署 Auto Scale 解决方案

下载部署软件包

使用三明治拓扑的面向 Azure 的 threat defense virtual Auto Scale 解决方案是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

threat defense virtual Auto Scal with Azure GWLB 解决方案是一个基于 ARM 模板的部署，可以创建 GWLB、网络基础设施、威胁防御虚拟 自动扩展组、无服务器组件和其他所需资源。

两种解决方案的部署过程均类似。

下载启动面向 Azure 的 threat defense virtual Auto Scale 解决方案所需的文件。您的版本的部署脚本和模板可从 GitHub 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

有关如何构建 *ASM_Function.zip* 包的说明，请参阅通过源代码构建 Azure 函数，第 230 页。

部署 Auto Scale ARM 模板

使用三明治拓扑的威胁防御虚拟 Auto Scale for Azure - 使用 ARM 模板**azure_ftdv_autoscale.json**来部署 threat defense virtual Auto Scale for Azure 所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机规模集 (VMSS)
- 外部负载均衡器
- 内部负载均衡器
- Azure 函数应用
- 逻辑应用
- 安全组（用于数据接口和管理接口）

威胁防御虚拟 Auto Scale with Azure GWLB - 使用 ARM 模板 **azure_ftdv_autoscale_with_GWLB.json** 来部署 threat defense virtual Auto Scale with Azure GWLB 解决方案所需的资源。在给定资源组内，ARM 模板部署会创建以下各项：

- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网关负载均衡器
- Azure 函数应用
- 逻辑应用

- 网络基础设施
- 部署所需的安全组和其他各种组件

开始之前

- 从 GitHub 存储库下载 ARM 模板 (https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure)。

过程

步骤 1 如果您需要在多个 Azure 区域中部署 threat defense virtual 实例，请基于部署区域中可用的区域编辑 ARM 模板。

示例：

```
"zones": [
    "1",
    "2",
    "3"
],
```

本示例显示了包含 3 个区域的“美国中部”区域。

步骤 2 编辑外部负载均衡器中所需的流量规则。您可以通过扩展此“json”数组来添加任意数量的规则。这适用于使用三明治拓扑的 Auto Scale 使用案例。

示例：

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
   "name": "Standard"
 },
 "dependsOn": [
   "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

 ],
 "properties": {
   "frontendIPConfigurations": [
     {
       "name": "LoadBalancerFrontEnd",
         "properties": {
           "publicIPAddress": {
             "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
           }
         }
     }
   ],
   "backendAddressPools": [
     {
       "name": "backendPool"
```

```
            }
          ],
          "loadBalancingRules": [
            {
              "properties": {
                "frontendIPConfiguration": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/frontendIpConfigurations/LoadBalancerFrontend')]"
                },
                "backendAddressPool": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/backendAddressPools/BackendPool')]"
                },
                "probe": {
                  "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

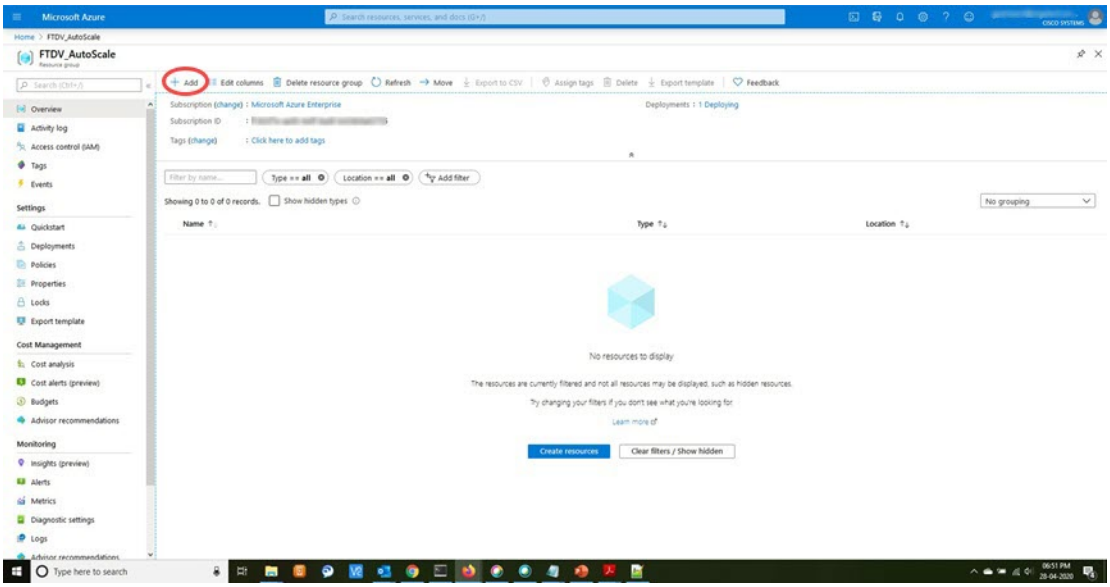
注释
如果您不想编辑此文件，也可以在部署后从 Azure 门户编辑此项。

步骤 3 使用您的 Microsoft 帐户用户名和密码登录 Microsoft Azure 门户。

步骤 4 点击服务菜单中的**资源组 (Resource groups)** 以访问资源组边栏选项卡。您将看到该边栏选项卡中列出您的订用中的所有资源组。

创建新资源组或选择现有的空资源组；例如，*threat defense virtual_AutoScale*。

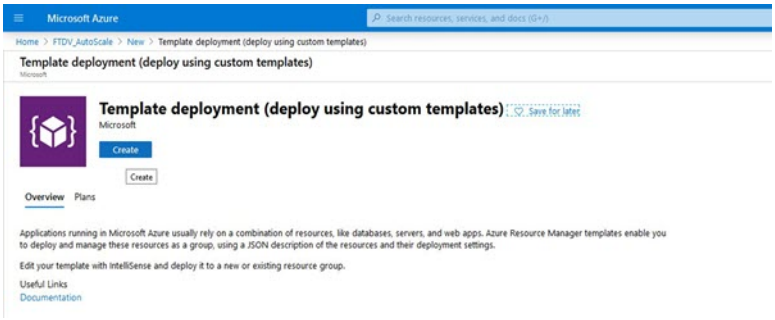
图 ***15: Azure*** 门户



步骤 5 点击**创建资源 (+) (Create a resource [+])**，为模板部署创建新资源。此时将显示“创建资源组”(Create Resource Group) 边栏选项卡。

步骤 6 在**搜索市场 (Search the Marketplace)** 中，键入**模板部署（使用自定义模板部署）**，然后按 **Enter**。

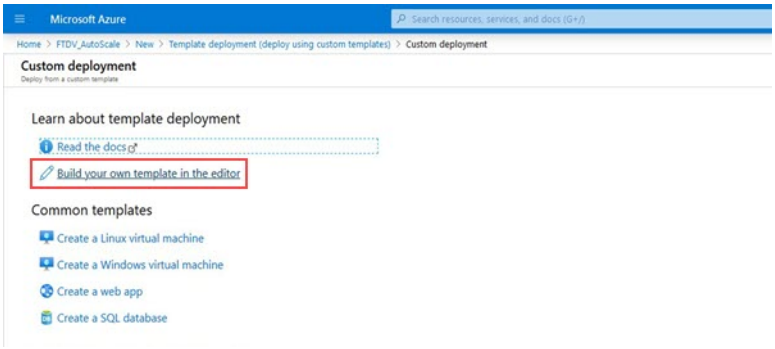
图 *16:* 自定义模板部署



步骤 7 点击**创建 (Create)**。

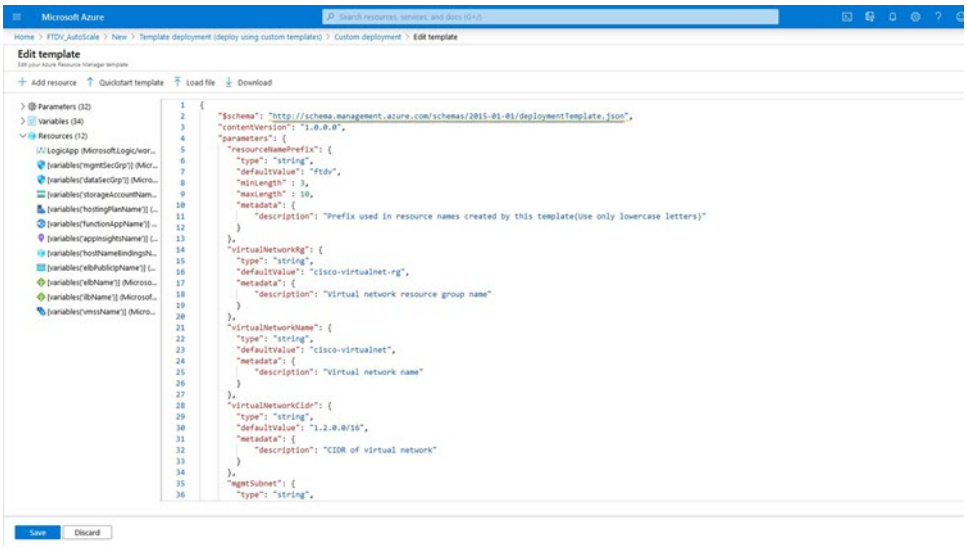
步骤 8 创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板 (Build your own template in editor)**。

图 *17:* 构建您自己的模板



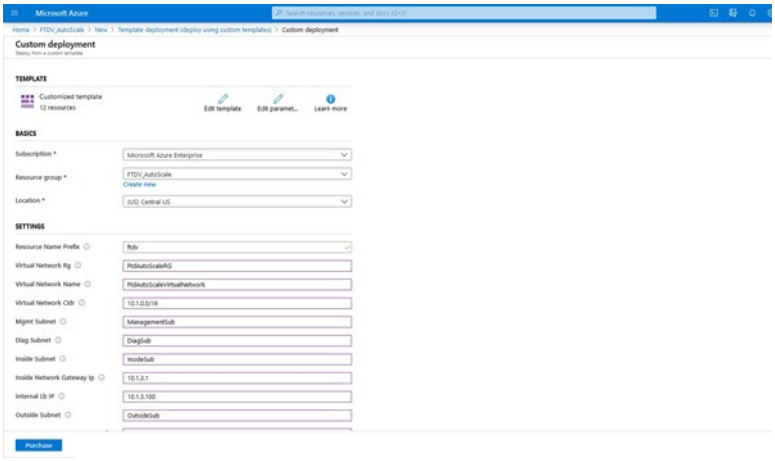
步骤 9 在**编辑模板 (Edit template)** 窗口中，删除所有默认内容并从更新的 *azure_ftdv_autoscale.json* 复制内容，然后点击**保存 (Save)**。

图 *18:* 编辑模板



步骤 10 在下一部分，填写所有参数。有关每个参数的详细信息，请参阅输入参数，第 204 页，然后点击**购买 (Purchase)**。

图 *19: ARM* 模板参数



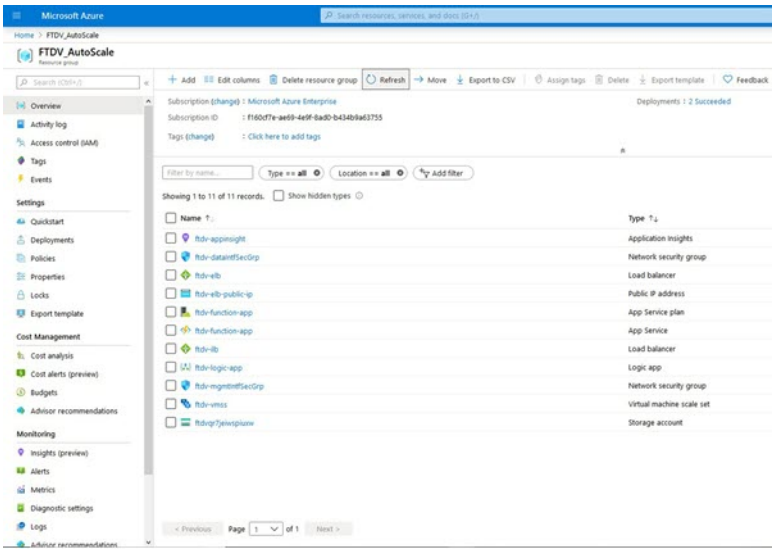
注释

您也可以点击**编辑参数 (Edit Parameters)**，然后编辑 JSON 文件或上传预填的内容。

ARM 模板的输入验证功能有限，因此您需要负责验证输入。

步骤 11 当成功部署模板后，它将为 threat defense virtual Auto Scale for Azure 解决方案创建所有必要的资源。请参阅下图中的资源。“类型”(Type) 列描述了每个资源，包括逻辑应用、VMSS、负载均衡器、公共 IP 地址等。

图 *20:* 威胁防御虚拟 ***Auto Scale*** 模板部署



部署 Azure 函数应用

部署 ARM 模板时，Azure 会创建一个主干函数应用，然后您需要为其更新和手动配置 Auto Scale Manager 逻辑所需的函数。

开始之前

- 构建 *ASM_Function.zip* 包。请参阅通过源代码构建 Azure 函数，第 230 页。

过程

步骤 1 转至您在部署 ARM 模板时创建的函数应用，然后确认不存在任何函数。在浏览器中，转至以下 URL：

https://<函数应用名称>.scm.azurewebsites.net/DebugConsole

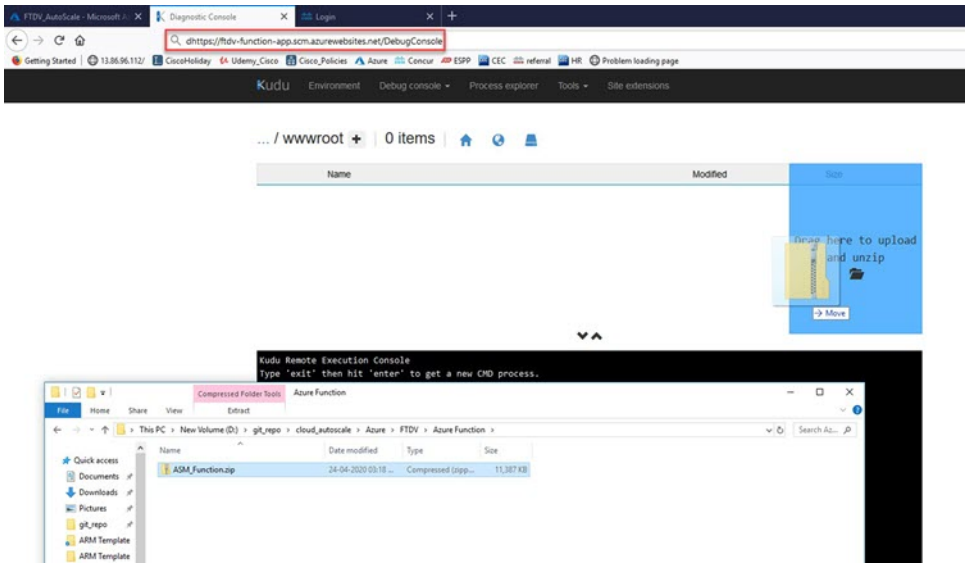
对于部署 Auto Scale ARM 模板，第 211 页中的示例：

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

步骤 2 在文件资源管理器中，导航到 **site/wwwroot**。

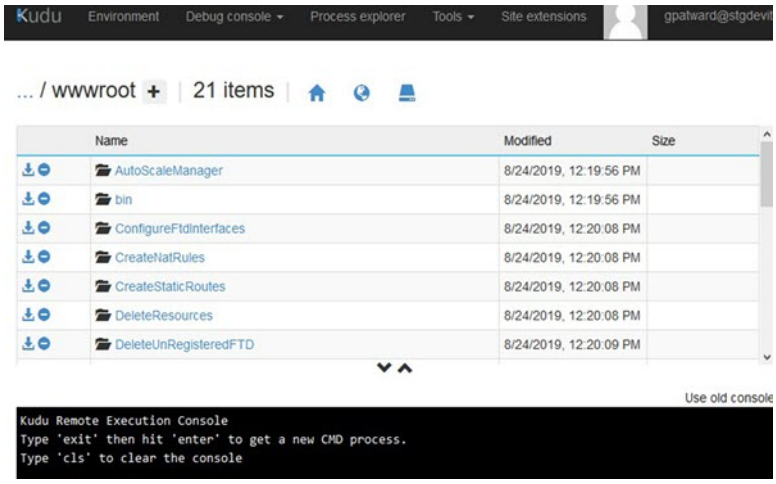
步骤 3 将 **ASM_Function.zip** 拖放到文件资源管理器的右侧。

图 *21:* 上传 威胁防御虚拟 ***Auto Scale*** 功能



步骤 4 成功上传后，应该会显示所有无服务器函数。

图 *22:* 威胁防御虚拟 无服务器函数

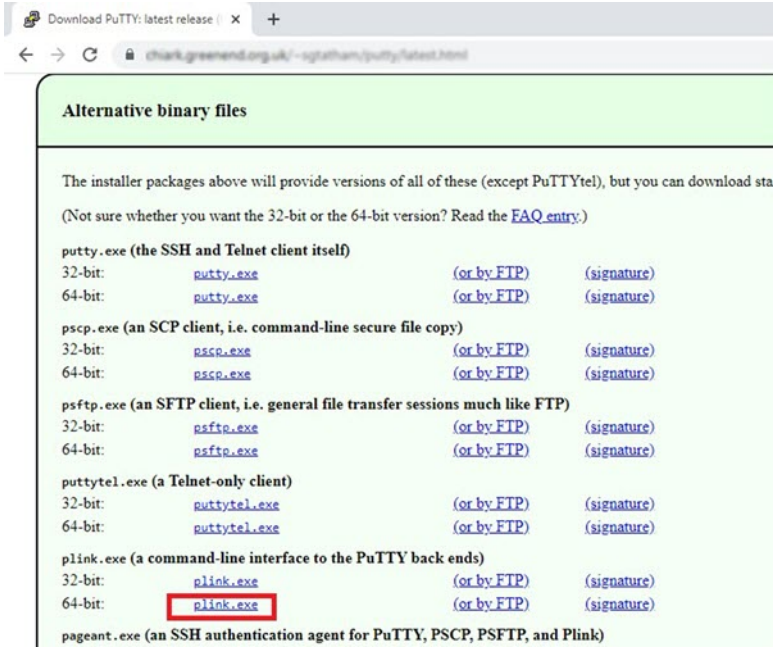


步骤 5 下载 PuTTY SSH 客户端。

Azure 函数需要通过 SSH 连接访问 threat defense virtual。但是，无服务器代码中使用的开放源码库不支持 threat defense virtual 所用的 SSH 密钥交换算法。因此，您需要下载预构建 SSH 客户端。

从 www.putty.org 将 PuTTY 命令行界面下载到 PuTTY 后端 (*plink.exe*)。

图 *23:* 下载 ***PuTTY***



步骤 6 将 SSH 客户端可执行文件 **plink.exe** 重命名为 **ftdssh.exe**。

步骤 7 将 **ftdssh.exe** 拖放到文件资源管理器的右侧，放到上一步中上传 **ASM_Function.zip** 的位置。

步骤 8 验证 SSH 客户端与函数应用程序一起存在。必要时刷新页面。

微调配置

有一些配置可用于微调 Auto Scale Manager 或在调试中使用。这些选项不会在 ARM 模板中显示，但可以在函数应用下编辑它们。

开始之前

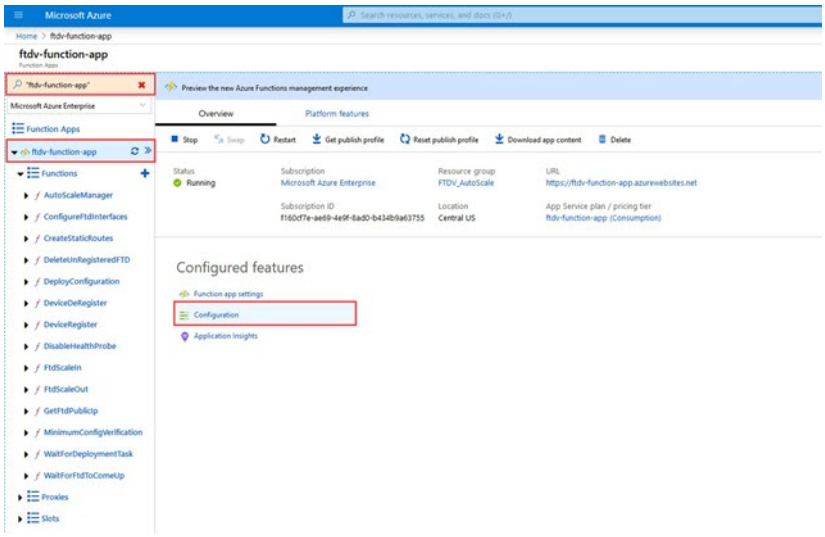
注释 可以随时编辑此项。按照以下顺序编辑配置。

- 禁用函数应用。
- 等待现有的计划任务完成。
- 编辑并保存配置。
- 启用函数应用。

过程

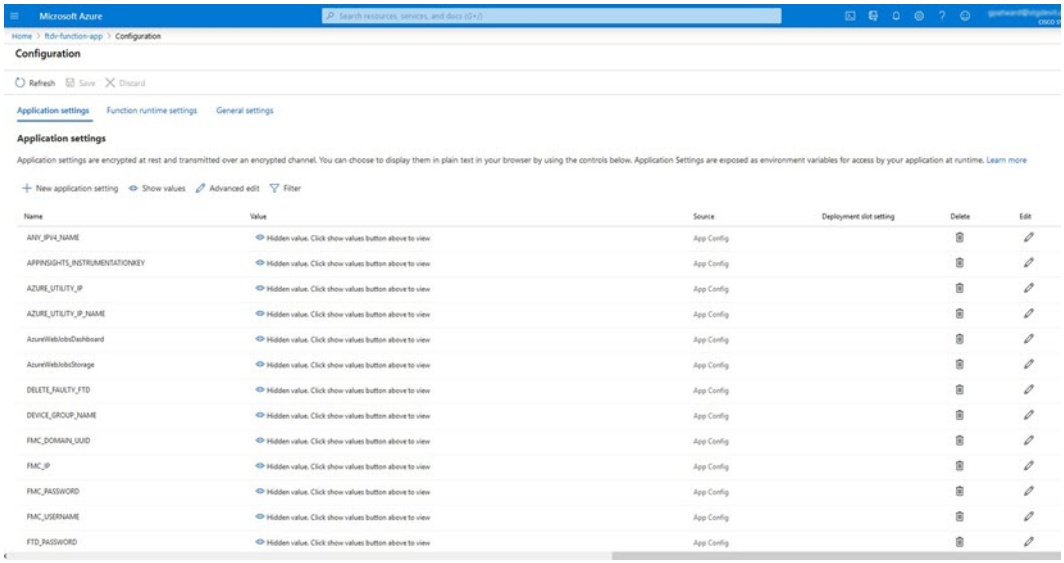
步骤 1 在 Azure 门户中，搜索并选择 threat defense virtual 函数应用。

图 *24:* 威胁防御虚拟 函数应用



步骤 2 也可以在此处编辑通过 ARM 模板传递的配置。变量名称可能与 ARM 模板不同，但您可以轻松地从其名称中确定它们的用途。

图 *25:* 应用设置



大多数选项的名称不言自明。例如：

- 配置名称：“DELETE_FAULTY_FTD”（默认值：YES）

在外向扩展期间，将会启动新的 threat defense virtual 实例并将其注册到 管理中心。如果注册失败，则 Auto Scale Manager 将根据此选项决定保留该 threat defense virtual 实例或将其删除。（YES：删除错误的 threat defense virtual/NO：保留 threat defense virtual 实例，即使未能注册到 管理中心）。

- 在函数应用设置中，有权访问 Azure 订用的用户都可以看到明文格式的所有变量（包括含安全字符串的变量，如“密码”）。

  如果用户对此有安全担忧（例如，如果在组织内的低权限用户之间共享 Azure 订用），可以使用 Azure 的 *Key Vault* 服务来保护密码。配置此项后，用户必须提供由存储密码的密钥保管库生成的安全标识符，而不是函数设置中的明文密码。

  注释
  搜索 Azure 文档，查找保护应用程序数据的最佳实践。

在虚拟机规模集中配置 IAM 角色

Azure 身份及访问管理 (IAM) 作为 Azure 安全和访问控制的一部分，用于管理和控制用户的身份。Azure 资源的托管身份为 Azure 服务提供 Azure Active Directory 中自动托管的身份。

这将允许函数应用控制虚拟机规模集 (VMSS)，无需显式身份验证凭证。

过程

步骤 1 在 Azure 门户中，转至 VMSS。

步骤 2 点击**访问控制 (IAM) (Access control [IAM])**。

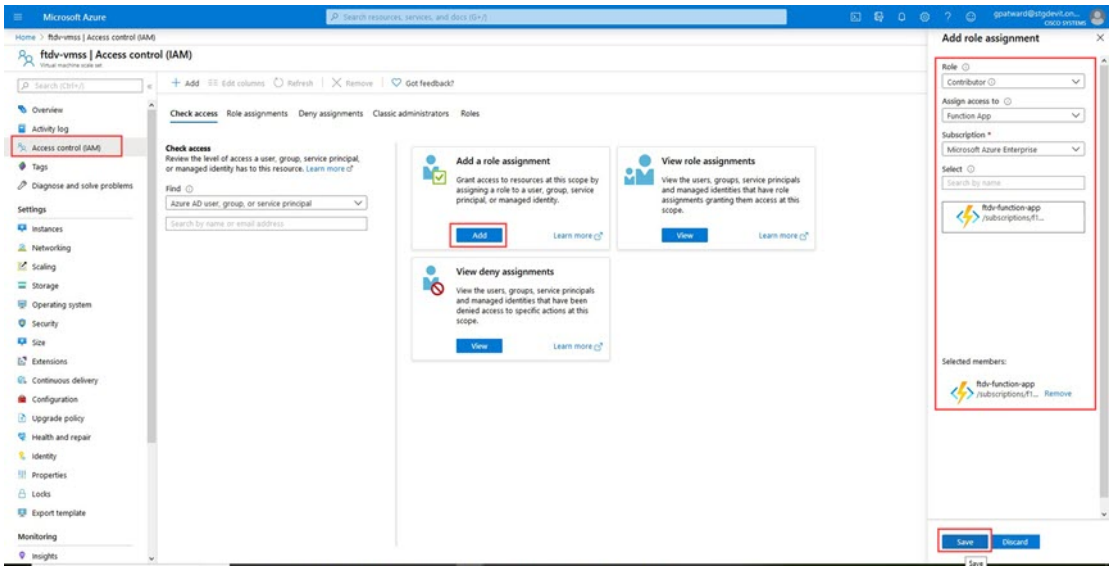
步骤 3 点击**添加 (Add)** 以添加角色分配

步骤 4 从**添加角色分配 (Add role assignment)**下拉列表中选择**参与者 (Contributor)**。

步骤 5 从**分配访问 (Assign access to)** 下拉列表中选择**函数应用 (Function App)**。

步骤 6 选择 threat defense virtual 函数应用。

图 *26: AIM* 角色分配



步骤 7 点击保存 **(Save)**。

注释
此外，还应确认尚未启动任何 threat defense virtual 实例。

更新安全组

ARM 模板创建两个安全组，一个用于管理接口，一个用于数据接口。管理安全组将只允许 threat defense virtual 管理活动所需的流量。不过，数据接口安全组将允许所有流量。

过程

根据您的部署的拓扑和应用程序需求，微调安全组规则。

注释
数据接口安全组至少应允许来自负载均衡器的 SSH 流量。

更新 Azure 逻辑应用

逻辑应用充当Autoscale功能的协调器。ARM模板会创建一个主干逻辑应用，然后您需要手动更新，提供使之作为 Auto Scale 协调器发挥作用所需的信息。

过程

步骤 1 从存储库中将文件 *LogicApp.txt* 恢复到本地系统，然后如下所示进行编辑。

重要事项
在继续之前，阅读并理解所有这些步骤。

这些手动步骤不会在 ARM 模板中自动执行，以便稍后只能独立升级逻辑应用。

a) 必需： 查找所有“SUBSCRIPTION_ID”并替换为您的订用 ID 信息。
b) 必需： 查找所有“RG_NAME”并替换为您的资源组名称。
c) 必需： 查找所有“FUNCTIONAPPNAME”并替换为您的函数应用名称。

以下示例显示了 *LogicApp.txt* 文件中的几行：

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) （可选）编辑触发间隔，或保留默认值 (5)。这是定期触发 Autoscale 的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
```

```
            "frequency": "Minute",
            "interval": 5
        },
```

e) （可选）编辑要进行排空的时间，或保留默认值(5)。这是内向扩展操作期间，在删除设备之前从threat defense virtual 中排空现有连接的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

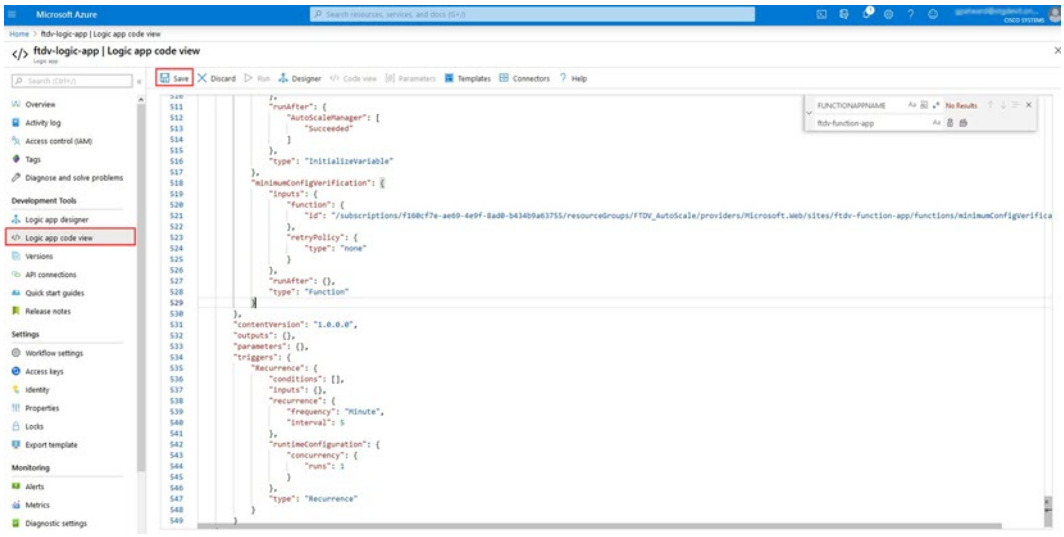
f) （可选）编辑冷却时间，或保留默认值(10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
    "actions": {
        "Branch_based_on_Scale-Out_or_Invalid_condition": {
            "actions": {
                "Cooldown_time": {
                    "inputs": {
                        "interval": {
                            "count": 10,
                            "unit": "Second"
                        }
```

注释
这些步骤也可以从 Azure 门户完成。有关详细信息，请参阅 Azure 文档。

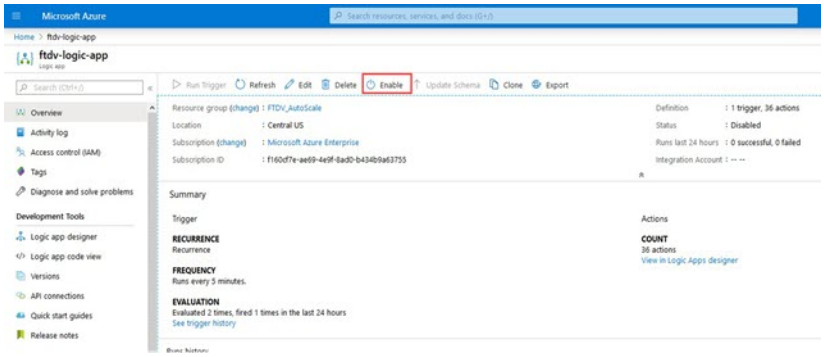
步骤 2 转至**逻辑应用代码视图 (Logic App code view)**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后点击**保存 (Save)**。

图 *27:* 逻辑应用代码视图



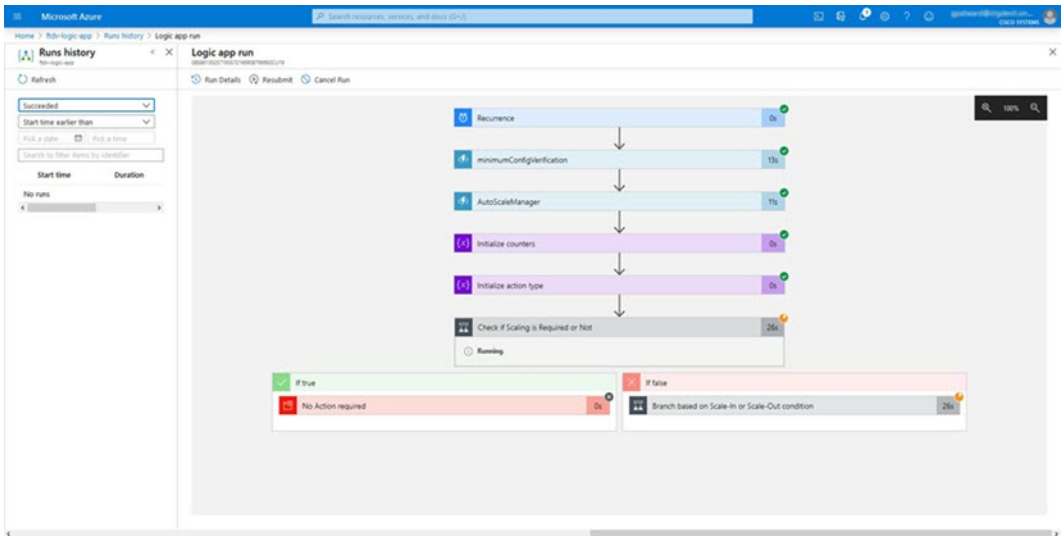
步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请点击**启用 (Enable)**。

图 *28:* 启用逻辑应用



步骤 4 启用后，任务就会开始运行。点击“正在运行”(Running) 状态可查看活动。

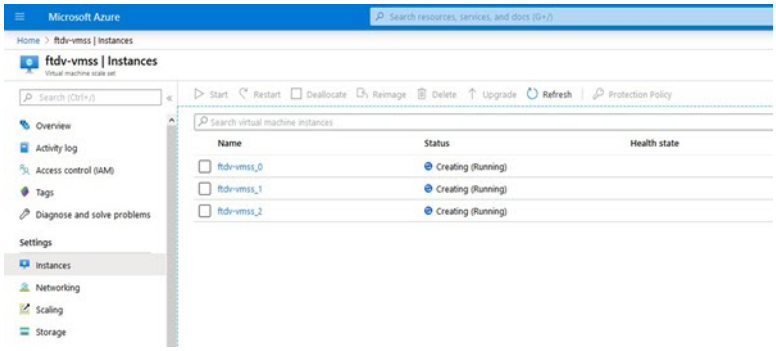
图 *29:* 逻辑应用运行状态



步骤 5 逻辑应用启动后，所有与部署相关的步骤都将完成。

步骤 6 在 VMSS 中验证是否正在创建 threat defense virtual 实例。

图 *30:* 威胁防御虚拟 实例运行



在此示例中，由于在 ARM 模板部署中将 'minFtdCount' 设置为“3”并将“initDeploymentMode”设置为“批量”，因此启动了三个 threat defense virtual 实例。

升级 threat defense virtual

threat defense virtual升级仅支持采用虚拟机规模集 (VMSS) 映像升级的形式。因此，您需要通过 Azure REST API 接口升级 threat defense virtual。

注释 您可以使用任何 REST 客户端来升级 threat defense virtual。

开始之前

- 获取市场中提供的新 threat defense virtual 映像版本（例如：650.32.0）。
- 获取用于部署原始规模集的 SKU（例如：ftdv-azure-byol）。
- 获取资源组和虚拟机规模集名称。

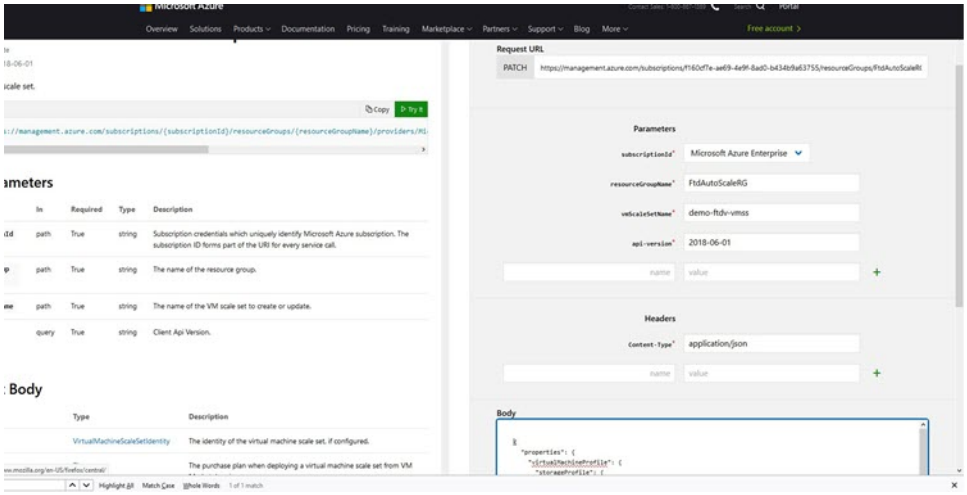
过程

步骤 1 在浏览器中，转至以下 URL：

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

步骤 2 在参数部分输入详细信息。

图 *31:* 升级*threat defense virtual*



步骤 3 在主体 **(Body)** 部分输入包含新 threat defense virtual 映像版本、SKU 和触发器运行的 JSON 输入。

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                      "imageReference": {
                           "publisher": "cisco",
                           "offer": "cisco-ftdv",
                           "sku": "ftdv-azure-byol",
                            "version": "650.32.0"
                      }
                 },
            }
      }
}
```

步骤 4 Azure 成功响应意味着 VMSS 已接受更改。

新映像将在新的 threat defense virtual 实例中使用，而这些新实例将在外向扩展操作过程中启动。

- 虽然位于同一规模集中，但现有的 threat defense virtual 实例将继续使用旧软件映像。
- 您可以覆盖上述行为，手动升级现有的 threat defense virtual 实例。要执行此操作，请点击 VMSS 中的**升级 (Upgrade)** 按钮。它将重新启动并升级选定的 threat defense virtual 实例。您必须手动重新注册并重新配置这些升级后的 threat defense virtual 实例。**请注意，不建议使用此方法**。

Auto Scale 逻辑

扩展指标

您可以使用 ARM 模板部署 threat defense virtualAuto Scale 解决方案所需的资源。在 ARM 模板部署期间，您有以下选项可用于扩展指标：

- CPU
- CPU、内存（版本 6.7+）。

注释 CPU 指标从 Azure 收集；内存指标从 管理中心 收集。

外向扩展逻辑

- **POLICY-1**：当**任何** threat defense virtual 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。使用“CPU、内存”扩展指标时，外向扩展阈值即规模集中**任何** threat defense virtual 的平均 CPU **或**内存利用率。
- **POLICY-2**：当**所有** threat defense virtual 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。使用“CPU、内存”扩展指标时，外向扩展阈值即规模集中**所有** threat defense virtual 设备的平均 CPU **或**内存利用率。

内向扩展逻辑

- 如果**所有** threat defense virtual 设备的 CPU 利用率在所配置的持续时间内低于配置的内向扩展阈值。使用“CPU、内存”扩展指标时，如果规模集中所有 threat defense virtual 设备的 CPU **和**内存利用率在所配置的持续时间内低于配置内向扩展阈值，则将选择终止 CPU 负载最小的 threat defense virtual。

说明

- 内向扩展/外向扩展以 1 为单位发生（即一次仅内向扩展/外向扩展 1 个 threat defense virtual）。

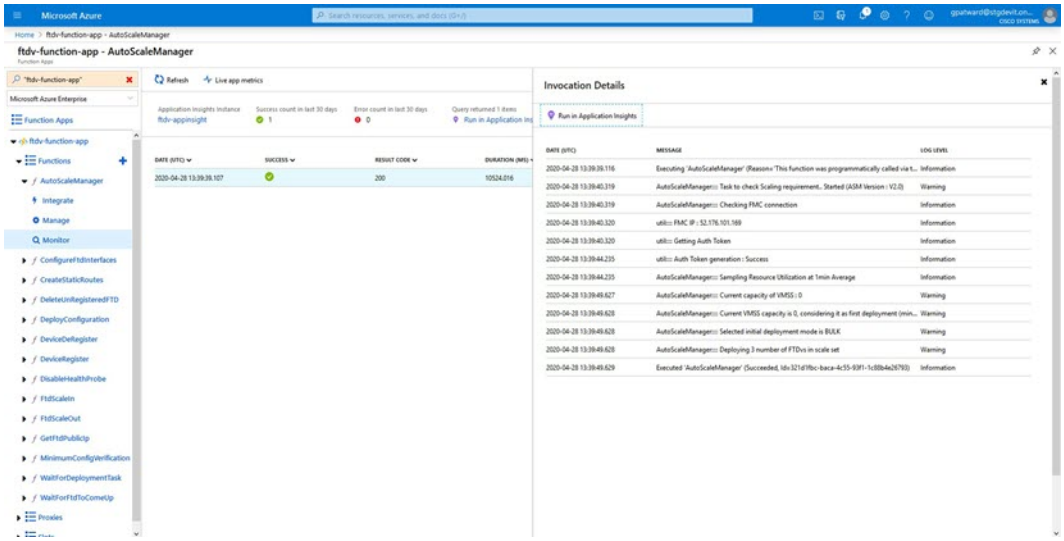
- 从 管理中心 收到的内存消耗指标不是按时间计算的平均值，而是瞬时快照/示例值。因此，在做出扩展决定时不能单独考虑内存指标。在部署过程中，您无法选择使用仅内存指标。

Auto Scale 日志记录和调试

无服务器代码的每个组件都有自己的日志记录机制。此外，还会将日志发布到应用程序洞察。

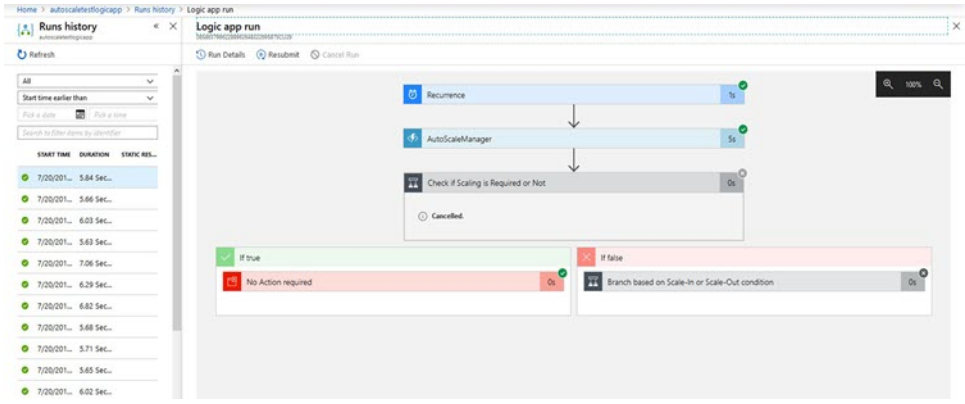
- 可以查看个别 Azure 函数的日志。

图 *32: Azure* 函数日志



- 可以查看每个逻辑应用及其各个组件每次运行的类似日志。

图 *33:* 逻辑应用运行日志



- 如果需要，可以随时停止/终止逻辑应用中任何正在运行的任务。但是，被启动/终止的当前运行 threat defense virtual 设备将处于不一致状态。
- 在逻辑应用中可以看到每个运行/个别任务所花费的时间。

- 通过上传新的zip，可以随时升级函数应用。在升级函数应用之前，先停止逻辑应用并等待所有任务完成。

Auto Scale 准则和限制

部署 threat defense virtual Auto Scale for Azure 时，请注意以下准则和限制：

- （版本 6.6 及更低版本）扩展决定基于 CPU 使用率。
- （版本 6.7+）扩展决定可以使用仅 CPU 利用率，或者同时使用 CPU 及内存利用率。
- 需要 管理中心 管理。不支持 设备管理器。
- 管理中心 应具有公共 IP 地址。
- threat defense virtual 管理接口配置为具有公共 IP 地址。
- 仅支持 IPv4。
- Threat Defense Virtual Auto Scale for Azure 仅支持访问策略、NAT 策略、平台设置等配置，它们将应用到设备组并传播到外向扩展 threat defense virtual实例。您只能使用 管理中心 来修改设备组配置。不支持设备特定的配置。
- ARM 模板的输入验证功能有限，因此您需要负责提供正确的输入验证。
- Azure管理员可以在函数应用环境中看到明文形式的敏感数据（如管理登录凭证和密码）。您可以使用 *Azure Key Vault* 服务保护敏感数据。
- 配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。
- 如果您在现有实例上手动更新配置时遇到问题，我们建议从扩展组中删除这些实例并将其替换为新实例。

故障排除

以下是 threat defense virtual Auto Scale for Azure 的常见错误情况和调试提示：

- 连接到 管理中心 失败：检查 管理中心 IP/凭证；检查 管理中心 是否故障/无法访问。
- 无法通过 SSH 连接到 threat defense virtual：检查是否通过模板将复杂密码传递到 threat defense virtual；检查安全组是否允许 SSH 连接。
- 负载均衡器运行状况检查失败：检查 threat defense virtual 是否在数据接口上响应 SSH；检查安全组设置。
- 流量问题：检查负载均衡器规则、threat defense virtual 中配置的 NAT 规则/静态路由；检查模板和安全组规则中提供的 Azure 虚拟网络/子网/网关详细信息。
- threat defense virtual 无法注册到 管理中心：检查 管理中心 容量以容纳新的 threat defense virtual 设备；检查许可；检查 threat defense virtual 版本兼容性。

- 逻辑应用无法访问 VMSS：检查 VMSS 中的 IAM 角色配置是否正确。
- 逻辑应用运行很长时间：在外向扩展 threat defense virtual 设备上检查 SSH 访问；检查 管理中心 中是否有任何设备注册问题；检查 Azure VMSS 中 threat defense virtual 设备的状态。
- 与订用 ID 相关的 Azure 函数抛出错误：验证您的帐户中是否选择了默认预订。
- 内向扩展操作失败：有时 Azure 会花费很长时间删除实例，在这种情况下，内向扩展操作可能会超时并报告错误，但最终实例将被删除。
- 在做出任何配置更改之前，请确保禁用逻辑应用程序，并等待所有正在运行的任务完成。

如果在 threat defense virtual Auto Scale 与 Azure GWLB 部署期间遇到任何问题，请查看以下故障排除提示：

- 检查 ELB-GWLB 关联。
- 检查 GWLB 中的运行状况探测状态。
- 通过验证 threat defense virtual 物理和逻辑接口上的流量来检查 VXLAN 配置。
- 检查安全组规则。

通过源代码构建 Azure 函数

系统要求

- Microsoft Windows 桌面/笔记本电脑。
- Visual Studio（使用 Visual Studio 2019 版本 16.1.3 进行测试）

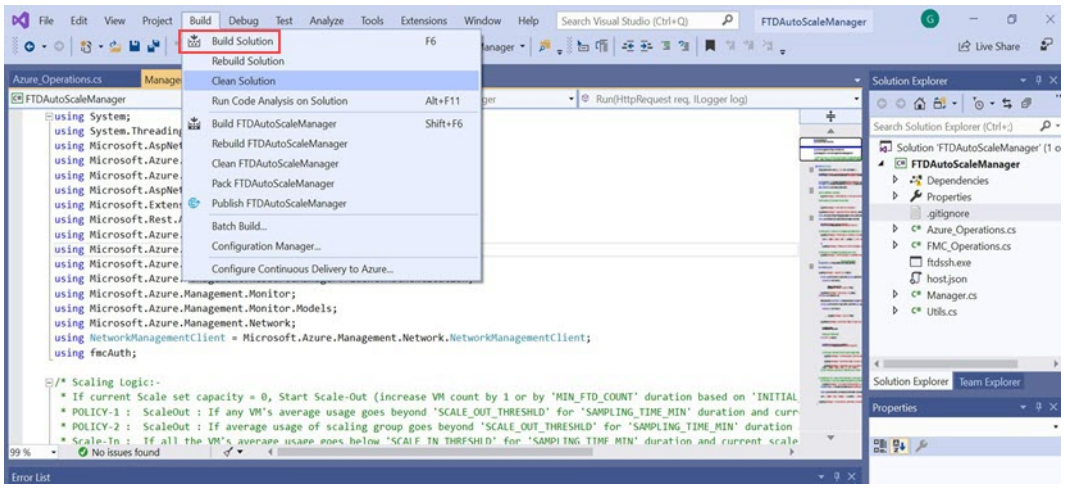
注释 Azure 函数是使用 C# 编写的。

- “Azure Development”工作负载需要安装在 Visual Studio 中。

使用 Visual Studio 构建

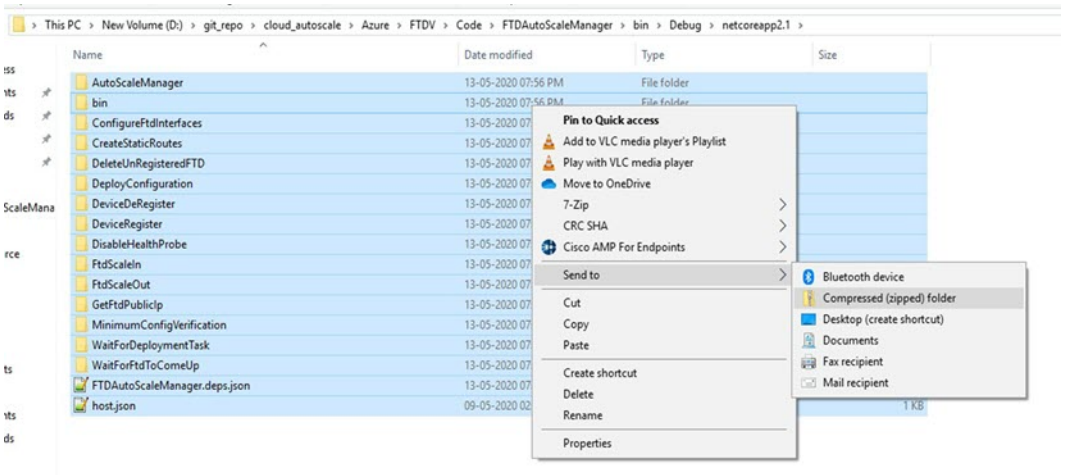
1. 将“code”文件夹下载到本地计算机。
2. 导航到文件夹“FTDAutoScaleManager”。
3. 在 Visual Studio 中打开项目文件“FTDAutoScaleManager.csproj”。
4. 使用 Visual Studio 标准程序进行清理和构建。

图 *34: Visual Studio* 内部版本



5. 成功编译内部版本后，导航到 **\bin\Release\netcoreapp2.1** 文件夹。
6. 选择所有内容，点击 **发送到 (Send to)** > **压缩 (zipped) 文件夹 (Compressed [zipped] folder)**，然后将 ZIP 文件保存为 *ASM_Function.zip*。

图 *35:* 生成 *ASM_Function.zip*



在 Azure 虚拟 WAN 上部署 Cisco Secure Firewall Threat Defense Virtual

Azure 虚拟 WAN 中的 Threat Defense Virtual 简介

Microsoft Azure 虚拟 WAN 采用“中心辐射型”架构来管理各种虚拟网络和分支机构位置之间的流量。在 Azure 虚拟 WAN 中，将 Threat Defense Virtual 与 Azure 虚拟中心集成有助于在通过中心时对源自组织的本地（辐射）网络（如总部、分支机构和远程用户）的流量进行有效的管理和检查访问 Azure 网络上的 Vnet。此集成通过使用 Threat Defense Virtual 防火墙的专用连接通道，促进网络流量的管理、检查、过滤和路由。

注释 Azure 虚拟 WAN 支持仅具有三个接口的 Threat Defense Virtual 部署模型。

在 Azure 虚拟 WAN 中心部署 Threat Defense Virtual 具有多种优势，包括：

- 无需在连接到中心的每个中心内实施防火墙解决方案。
- 利用 Azure 的内部负载均衡器 (ILB) 的内置功能。
- 在部署期间使用预定义配置扩展实例。

有关在虚拟 WAN 中心部署 Threat Defense Virtual 的信息，请参阅在 Azure 虚拟 WAN 上部署 Threat Defense Virtual。

通过 Azure 虚拟 WAN 上 Threat Defense Virtual 进行流量路由

Azure 虚拟 WAN 中的路由流量方法

Azure 虚拟 WAN 提供边界网关协议 (BGP)，这是一种动态路由协议，可帮助确定在不同 Azure 网络之间发送流量的最佳路由，同时不断更新和共享路由表。虚拟 WAN 中心提供一组 BGP 终端（用于实现高可用性）和自治系统编号 (ASN)，您必须在管理中心将其配置为 Threat Defense Virtual 的 BGP 邻居。

您还可以使用静态路由方法在 Threat Defense Virtual 中手动配置路由。

有关 Azure 中路由的详细信息，请参阅 Azure 文档中的关于 BGP 和 VPN 网关。

路由意图

路由意图是 Azure 虚拟 WAN 中心中的一种路由功能，可简化将互联网绑定和专用流量转发到中心中部署的 Threat Defense Virtual 防火墙进行检查的过程。

有关详细信息，请参阅 Azure 文档中的路由意图。

系统要求

扩展单元

实现最大吞吐量所需的扩展取决于在 Azure 虚拟 WAN 中心部署期间选择或配置的 Threat Defense Virtual 实例 (NVA) 的实例大小和数量。

例如：如果大小为 **D3_V2** 的两个 Threat Defense Virtual 实例可以支持 2.8 Gbps，则 NVA 吞吐量定义为 **Scale-Unit-4: 2.8 Gbps**。

表 *21:* 基于实例类型的 ***Threat Defense Virtual*** 吞吐量级别

扩展单元	**Threat Defense Virtual** 实例	实例类型	吞吐量支持级别
4	2	Standard_D3_v2	3.2 Gbps
10	2	Standard_D4_v2	4.8 Gbps
20	2	Standard_D5_v2	12 Gbps
40	3	Standard_D5_v2	18 Gbps
60	4	Standard_D5_v2	24 Gbps
80	5	Standard_D5_v2	30 Gbps

限制

接口

Threat Defense Virtual 支持三个接口进行部署，因为 Azure 限制 NVA 最多只能支持三个网络接口。

注释 支持三种接口模式的 Threat Defense Virtual 7.4.1 及更高版本与在 Azure 虚拟 WAN 上部署兼容。

Threat Defense Virtual 网络接口的三个子网如下：

- **管理接口** - 它是使用公用 IP 地址将 Threat Defense Virtual 连接到管理中心的**第一个接口**。
- **外部接口（必需）** - 它是将 Threat Defense Virtual 连接到不受信任的公用 IP 地址的**第二个接口**。
- **内部接口（必需）** - 它是将 Threat Defense Virtual 连接到虚拟 WAN 集线器和内部主机网络的受信任专用 IP 地址的**第三个接口**。

Threat Defense Virtual 作为网络虚拟设备 (NVA)

以下是与 Azure 虚拟 WAN 中的 Threat Defense Virtual 作为 NVA 的网络配置相关的主要功能。

- 在 Azure 虚拟 WAN 上部署 Threat Defense Virtual 期间，Azure 会在内部创建 VNet 和子网。因此，在部署完成后无法修改或创建它们。但是，您可以在部署后查看连接到实例的所有 IP 地址。
- 您无法在网络安全组中为每个接口选择端口，但这些端口是在部署期间预定义的。管理接口上仅允许 TCP 端口 443、8305 和 22 连接到互联网。
- 内部接口仅允许在 Azure 虚拟 WAN 中心和与其连接的内部网络内进行通信。

Azure 虚拟 WAN 中心上对 Threat Defense Virtual 的访问限制

您需要授权才能访问在中心上作为托管应用部署到托管资源组中的 Threat Defense Virtual 实例。管理员可以授予对此托管资源组的有限或受限访问权限。

Azure 托管应用提供实时 (JIT) 访问功能，它允许您定义对托管应用的访问权限。有关 JIT 的信息，请参阅 Azure 文档中的 Azure 托管应用概述和即时应用。

IP 支持

- 仅支持 IPv4。

不支持的功能

- 不支持通过 Day 0/自定义数据进行引导。
- Threat Defense Virtual 不支持将指标流传输到 Azure。
- 不支持通过更换操作系统磁盘来升级虚拟机。
- 不支持基于 SSH 密钥登录到 Threat Defense Virtual。
- 不支持 PAYG。

许可

使用思科智能许可证帐户的 BYOL

网络拓扑

作为 Azure 虚拟 WAN 中心中的 NVA，Threat Defense Virtual 会通过中心的网络流量路由来检测来自不同本地网络（辐射型）（例如互联网、分支 [站点] 或作为 VNET）的网络流量。

网络流量通过的这些流量路由分类为以下拓扑：

- 东西：分支到分支
- 东西：VNet 到 VNet
- 南北：分支到互联网
- 南北：VNet 到互联网

注释 不支持通过 Threat Defense Virtual 从 **互联网** 到 **VNet 或分支** 的流量。

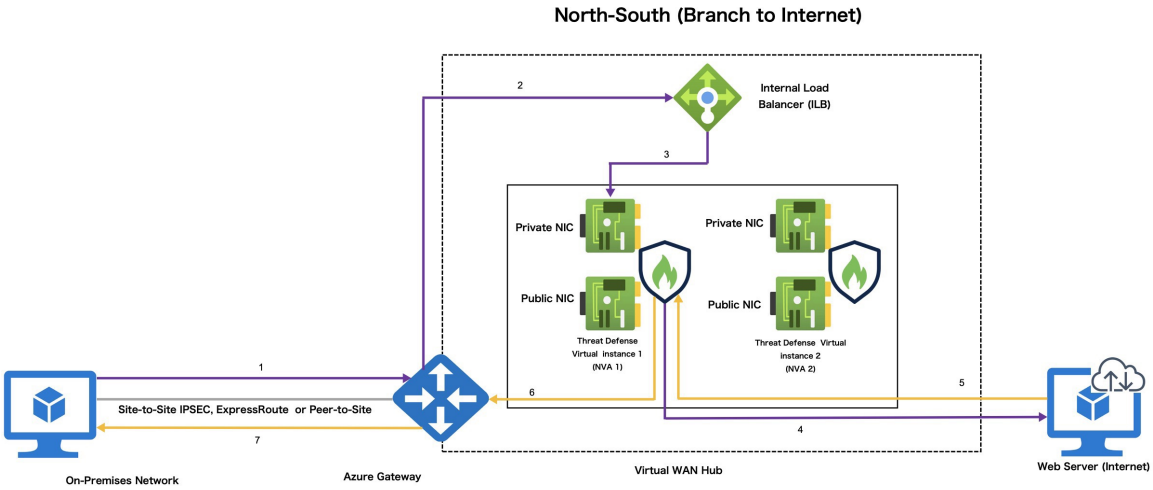
注释 您可以跨 Azure 区域部署多个中心，并连接到虚拟 WAN。此外，您还可以将每个中心配置为拥有自己的 Threat Defense Virtual，用于东西和南北流量检测。

单个虚拟 WAN 中心上按 Threat Defense Virtual 划分的南北流量检测拓扑

此拓扑引用 Threat Defense Virtual 检查在以下设备之间导航的网络流量：

- 分支和 VNET（反之亦然）连接到虚拟 WAN 中心。

图 *36: Azure* 虚拟 *WAN* 中心中的 *Threat Defense Virtual* 南北流量检测拓扑



以下步骤介绍了南北流量检测中的流量流程。

1. 本地网络将流量发送到 Azure 网关。
2. 网关转发到 ILB。
3. ILB 发送到 Threat Defense Virtual (NVA)
4. NVA SNAT 到实例 PIP 并发送到互联网。
5. Web 服务器回复实例 PIP Threat Defense Virtual (NVA) 会撤消 SNAT 并转发到网关。
6. 网关转发到本地网络。

单个虚拟 WAN 中心上按 Threat Defense Virtual 划分的东西流量检测拓扑

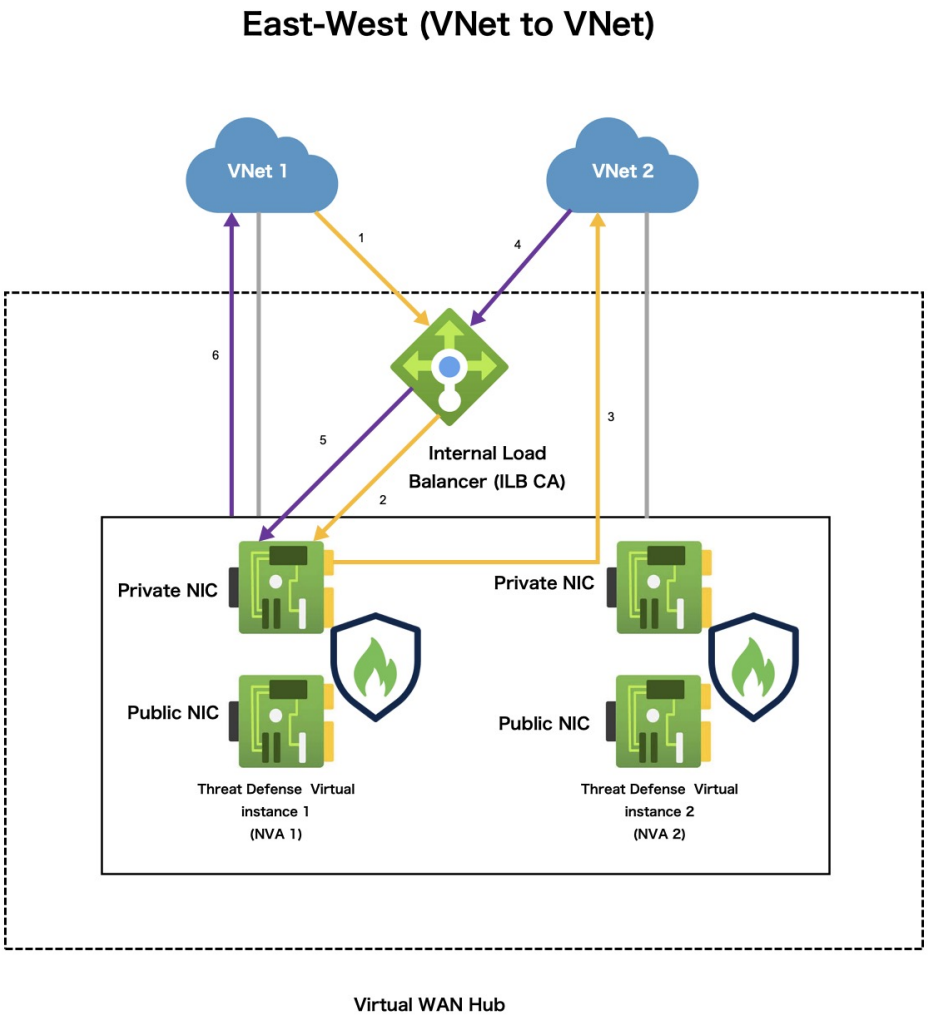
此拓扑引用 Threat Defense Virtual 检查在以下设备之间导航的网络流量：

- 分支和 VNET（反之亦然）连接到虚拟 WAN 中心。

- 从互联网到连接到虚拟 WAN 中心的分支或 VNET。

图 *37: Azure* 虚拟 *WAN* 中心中的 *Threat Defense Virtual* 东西流量检测拓扑

此拓扑是指 Threat Defense Virtual 检查连接到虚拟 WAN 中心的站点到站点（分支和分支）和 VNET 到 VNET 之间导航的网络流量。



以下步骤介绍了东西流量检测中的流量流程。

1. VNet1 将流量发送到 ILB。
2. ILB 选择其中一个活动实例。
3. Threat Defense Virtual (NVA) 直接发送到目标 (VNet 2)。
4. VNet 将流量发送到 ILB。
5. ILB 将流量完全转发到相应的 Threat Defense Virtual (NVA) 状态。

6. Threat Defense Virtual (NVA) 将流量发送回 VNet 1。

在 Azure 虚拟 WAN 上部署 Threat Defense Virtual

您可以使用 Azure 市场上提供的适用于 Azure 虚拟 WAN 的 Cisco Secure Firewall Threat Defense Virtual 产品，在 Azure 虚拟 WAN 中心部署 Threat Defense Virtual。

前提条件

- Microsoft Azure 帐户。您可以在 https://azure.microsoft.com/en-us/ 创建一个。
- 在虚拟 WAN 上创建一个中心。有关在 Azure 中创建虚拟中心的信息，请参阅 Azure 文档中的创建中心。
- 确保虚拟 WAN 中心地址空间小于或等于 /23。

Note Microsoft Azure 允许使用 /24 地址空间的虚拟 WAN 中心。但是，由于未来的增强功能，Microsoft 不建议部署此类中心。不支持在地址空间为 /24 的虚拟 WAN 中心部署 Threat Defense Virtual。

- 思科智能账户。您可以在 Cisco 软件中心创建一个。

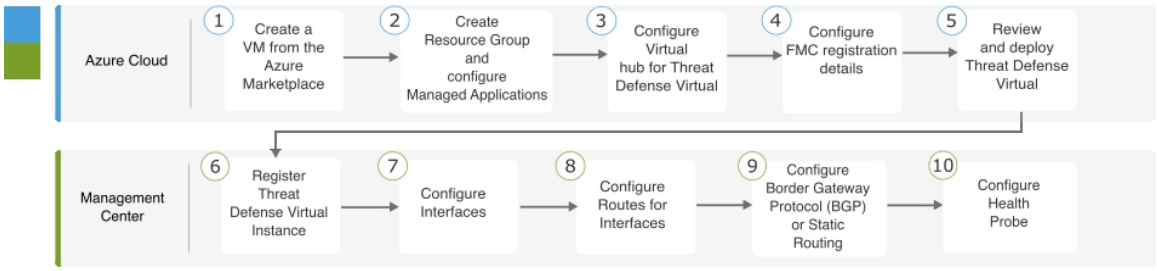
Note 部署 Threat Defense Virtual 实例后，您可以查看附加到该实例的所有公共和专用 IP。

通信路径

- 管理接口 - 用于将威胁防御虚拟连接到管理中心。
- 内部接口（必需）- 用于将威胁防御虚拟连接到内部主机。
- 外部接口（必需）- 用于将威胁防御虚拟连接到公共网络。

端到端程序

以下流程图说明了使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：在 Azure 市场中搜索“适用于 Azure VWAN 的 Cisco Secure Firewall Threat Defense Virtual”。
2	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：创建资源组并配置托管应用。
3	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：配置虚拟中心和 NVA 详细信息。
4	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：配置 FMC 注册详细信息。
5	Azure Cloud	使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual：查看并部署 Threat Defense Virtual。
6	管理中心或设备管理器	在管理中心注册 Threat Defense Virtual 实例：注册 Threat Defense Virtual 实例。
7	管理中心或设备管理器	配置接口：配置外部和内部接口。
8	管理中心或设备管理器	为接口配置路由：计算网关 IP 地址，并为外部和内部接口配置路由。
9	管理中心或设备管理器	配置流量路由：配置边界网关协议 (BGP) 或静态路由
10	管理中心或设备管理器	配置运行状况探测功能：配置运行状况探测以启用 ILB，以便对 Threat Defense Virtual 实例执行定期运行状况检查。

使用解决方案模板在 Azure 虚拟 WAN 上部署 Threat Defense Virtual

以下说明介绍了如何使用 Azure 市场提供的解决方案模板在 Azure 虚拟广域网上部署 Threat Defense Virtual。这是在 Microsoft Azure 虚拟 WAN 环境中设置 Threat Defense Virtual 所需的顶级步骤列表。

有关 Azure 设置步骤的详细信息，请参阅《Azure 入门》。

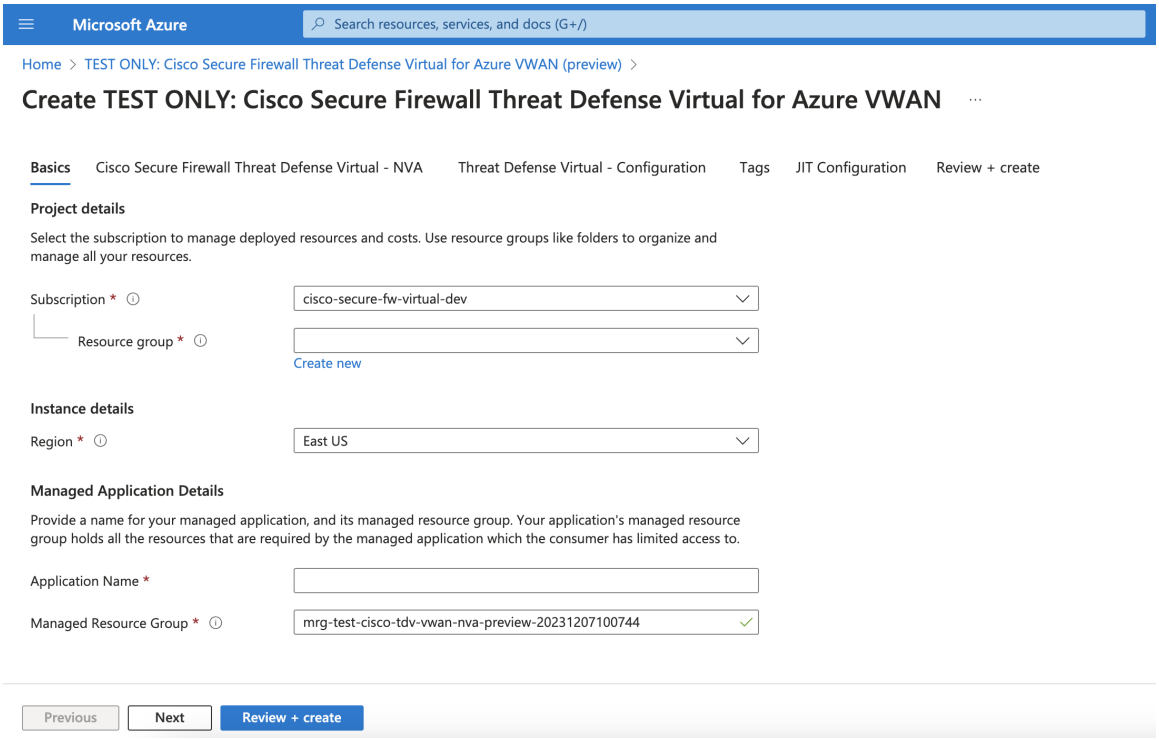
Procedure

步骤 1 登录到 Azure 资源管理器 (ARM) 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 依次选择 **Azure 市场** > **虚拟机**。

步骤 3 在市场中搜索适用于 **Azure VWAN** 的 **Cisco Secure Firewall Threat Defense Virtual**，选择产品，然后点击**创建 (Create)**以显示**基本 (Basics)** 页面。



步骤 4 配置 **Basics** 设置。

a) 选择您的订用。

b) 创建新的**资源组**。

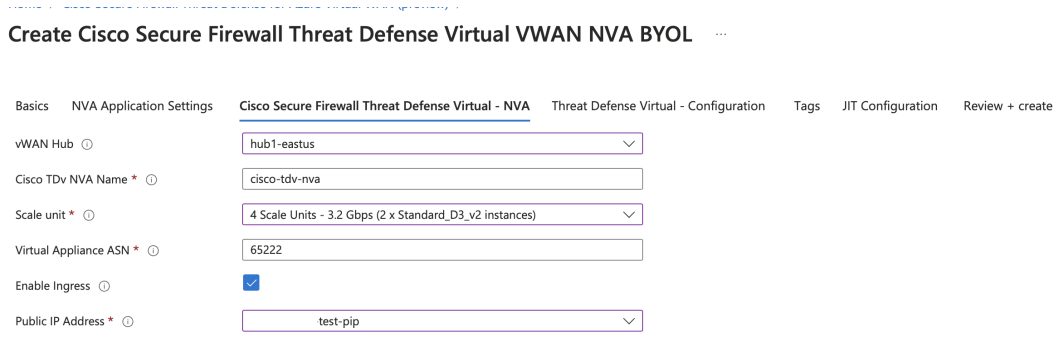
c) 选择虚拟 WAN 中心的地理位置或区域。对于此部署中使用的所有资源（例如虚拟 WAN 中心、Threat Defense Virtual、网络、存储帐户），它应该是相同的。

步骤 5 配置**托管应用详细信息 (Managed Application Details)** 设置。

a) 输入要在其中将 Threat Defense Virtual 实例部署为 NVA 的托管资源组的托管应用的名称。

b) 选择部署 Threat Defense Virtual 实例的托管资源组。

步骤 6 点击**下一步 (Next)**，显示 **Cisco Secure Firewall Threat Defense Virtual - NVA** 页面。



步骤 7 配置虚拟中心和 NVA 详细信息：

a) 从 **vWAN 中心 (vWAN Hub)** 下拉列表中选择虚拟 WAN 中心，以部署 Threat Defense Virtual 实例。

b) 为要部署的 Threat Defense Virtual 实例输入适当的名称。

c) 选择定义要部署的 Threat Defense Virtual 实例数量的扩展单元。

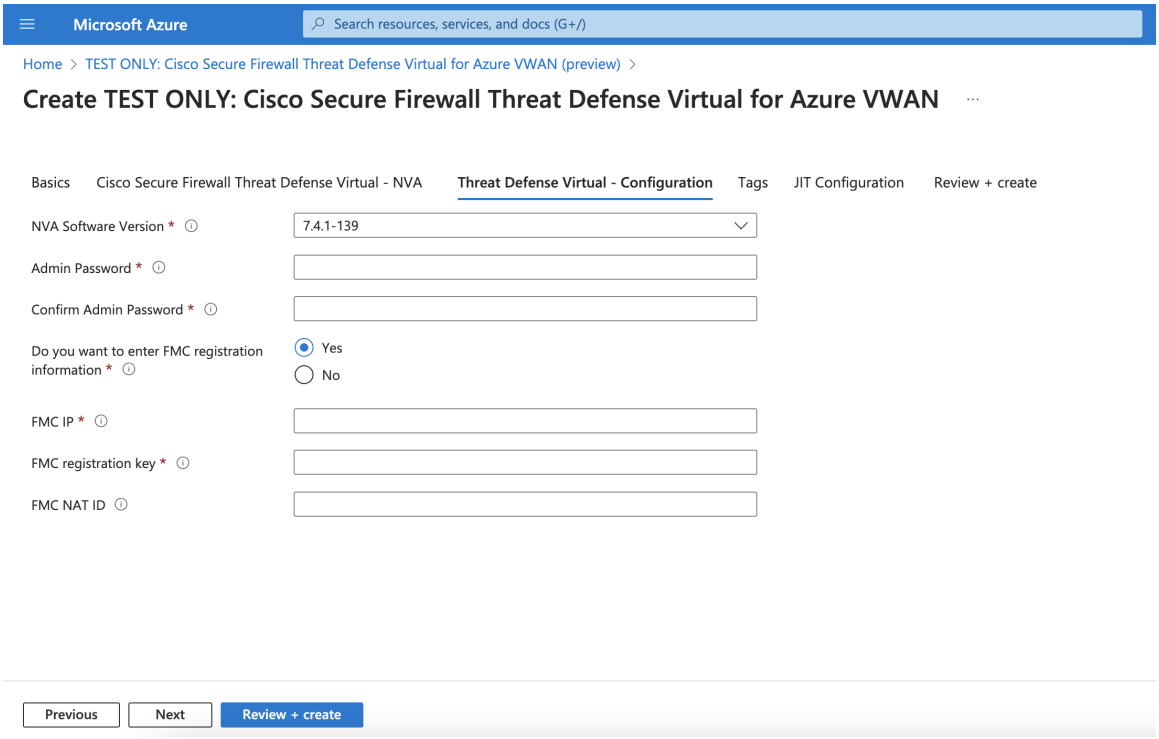
您可以选择所需的扩展单位，以实现所需的 NVA 吞吐量级别。例如，选择 **4 扩展单元 - 2.8 Gbps (4 Scale Units – 2.8 Gbps)(2 x Standard_D3_v2_instances)** 意味着“**扩展单元数量 - 吞吐量级别（具有实例类型的 2 个 Threat Defense Virtual**）。

Note
扩展单元定义您在中心中部署的 Threat Defense Virtual 实例及其关联实例类型的数量。

d) 输入**虚拟设备 ASN**。

Note
输入的 ASN 值必须在 64512 - 65534 范围内。

步骤 8 点击**下一步 (Next)** 以显示 **Threat Defense Virtual - 配置 (Threat Defense Virtual - Configuration)** 页面。



步骤 9 从下拉列表选择相应的 **NVA 软件版本**兼容版本。

Note
此字段提供与您正在部署的相应 Threat Defense Virtual 版本兼容的 NVA 软件版本列表。确保从列表中选择合适的版本。

步骤 10 创建并确认访问包含 Threat Defense Virtual 实例的托管资源组所需的管理员密码。

步骤 11 点击**是 (Yes)** 输入 **FMC 注册信息**。

a) 输入 **FMC IP** 地址。
b) 输入用于注册 Threat Defense Virtual 实例的 **FMC 注册密钥**。

Note

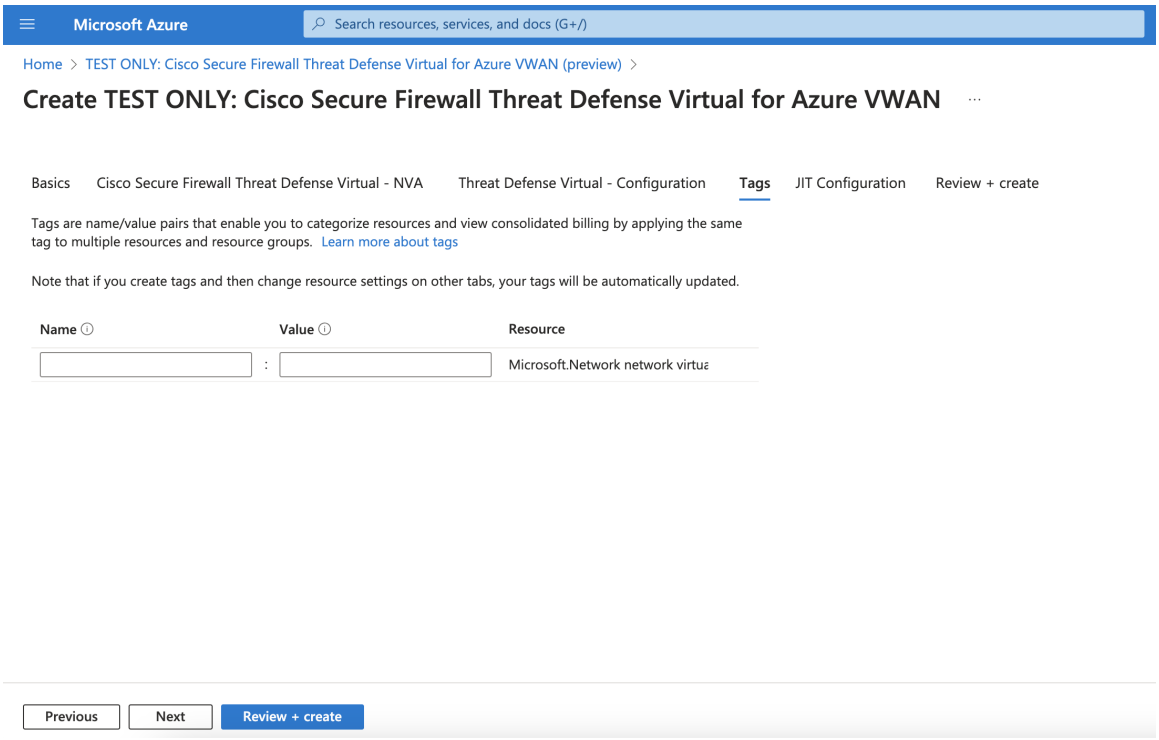
- FMC 注册密钥必须是长度为 1 至 37 个字符的字母数字字符串。在添加 Threat Defense Virtual 时，您将在管理中心上输入此密钥。

c) [可选] 输入在实例注册期间使用的管理中心 NAT ID。

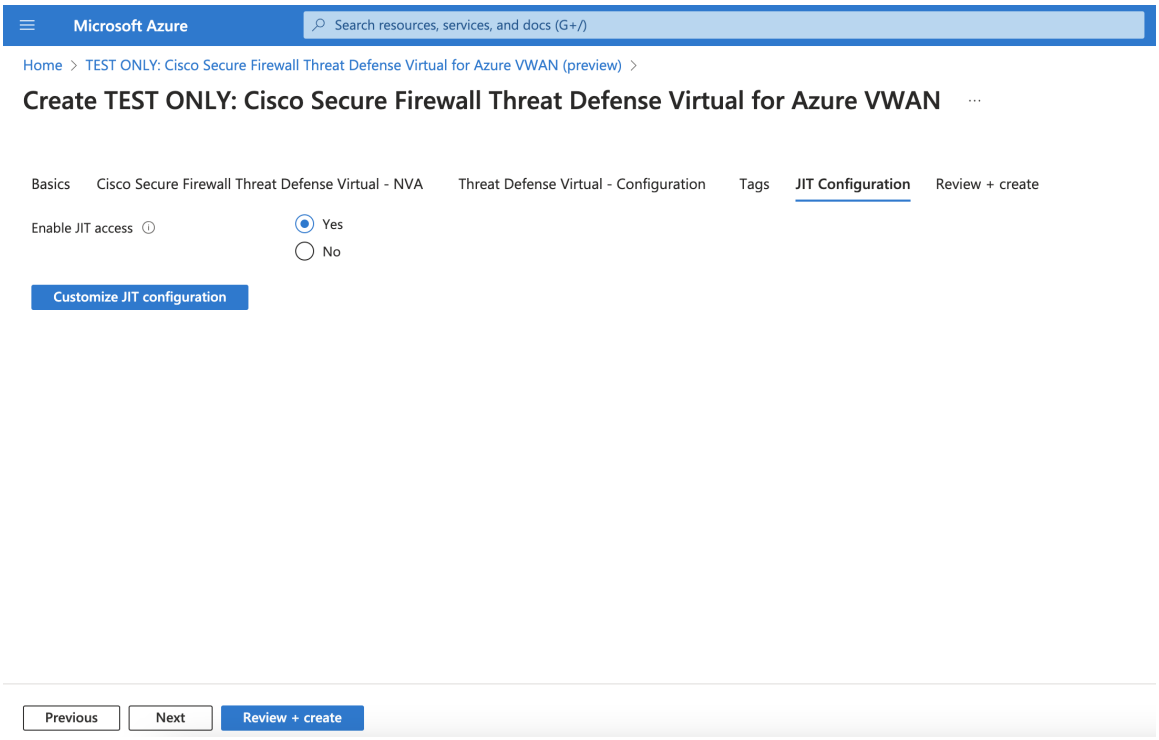
Note

- NAT ID 必须是长度在 1 - 37 个字符之间的字母数字字符串，仅在一方未指定 IP 地址时，在管理中心和设备之间的注册过程中使用。NAT ID 本质上是一个一次性密码，因此必须是唯一的，而且不能被其他等待注册的设备使用。为确保注册成功，请务必在添加 Threat Defense Virtual 时在 FMC 上指定相同的 NAT ID。

步骤 12 点击**下一步 (Next)** 以配置**标记 (Tags)**。

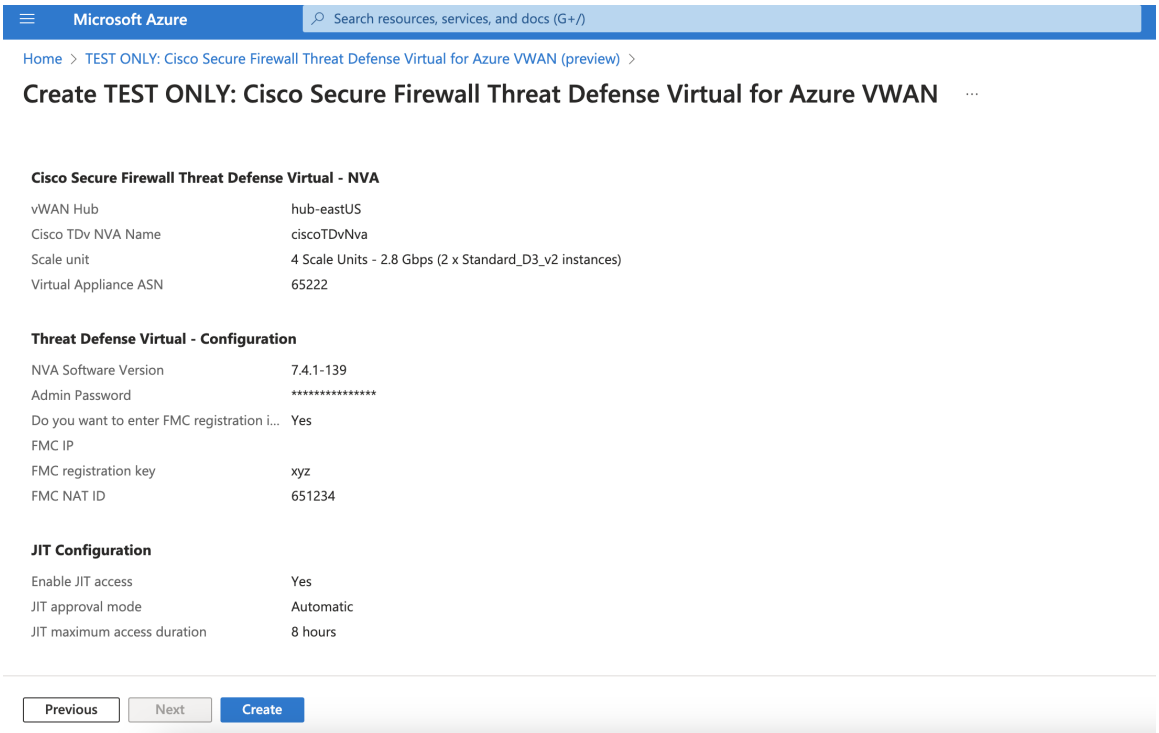


步骤 13 点击**下一步 (Next)** 以显示 **JIT 配置 (JIT configuration)** 页面。



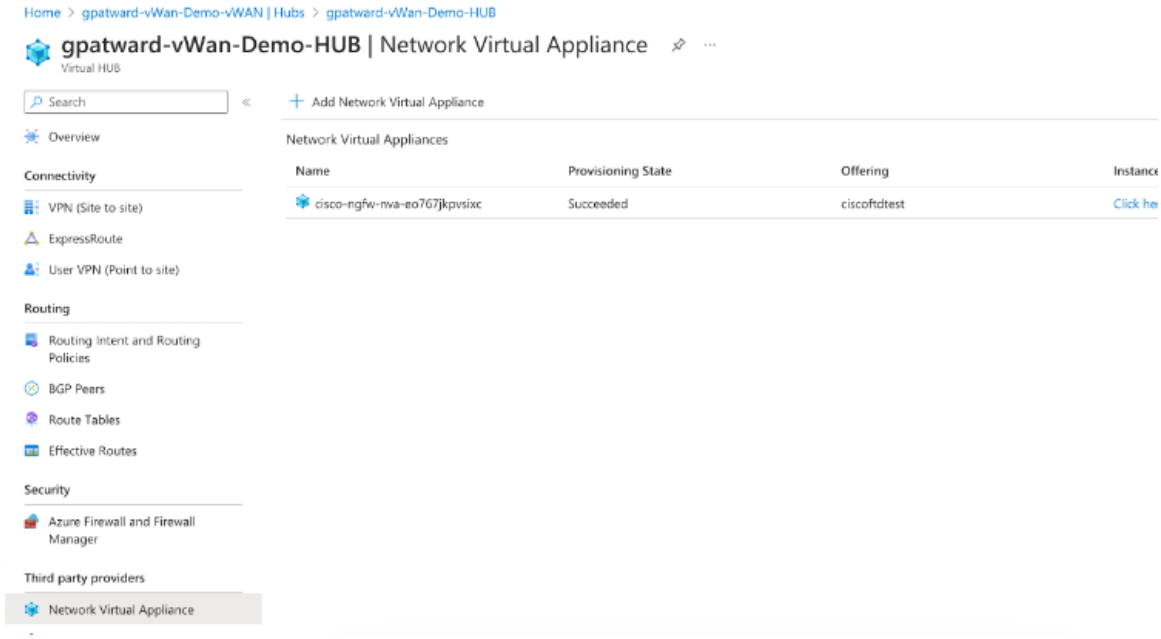
默认情况下，**启用 JIT 访问 (Enable JIT access)** 选项设置为**是 (Yes)**，这样将启用 JIT 调配访问，以管理 Threat Defense Virtual 实例并进行故障排除。

步骤 14 点击**下一步 (Next)** 以显示**查看+创建 (Review+Create)** 页面。



步骤 15 在部署之前，您必须查看订用、NVA、Threat Defense Virtual 和 JIT 配置详细信息，接受条款和条件，然后点击**创建 (Create)** 以在虚拟 WAN 中心上部署 Threat Defense Virtual (NVA)。

步骤 16 转至**主页 (Home)** > **安全 (Security)** > **第三方提供商 (Third-party providers)**，然后点击**网络虚拟设备 (Network Virtual Appliance)**，查看在集线器上创建的 NVA。



步骤 17 点击 **NVA** 以查看已部署的所有 Threat Defense Virtual 实例。

您可以使用实例的管理公用 IP 地址访问 Threat Defense Virtual，并使用 SSH 登录。

Note
您在中心上部署的每个 Threat Defense Virtual 实例的公用 IP 地址用于在管理中心注册实例。

What to do next

注册并配置您在管理中心的中心部署的 Threat Defense Virtual 实例。

在管理中心中配置 Threat Defense Virtual

您可以通过管理中心配置在中心部署的每个 Threat Defense Virtual 实例。

创建 Threat Defense Virtual 配置和管理所需的所有对象，包括设备组，以便您能够轻松地在多个设备上部署策略和安装更新。设备组上应用的所有配置都将被推送到 Threat Defense Virtual 实例。

本节简要概述在管理中心中配置 Threat Defense Virtual 实例的基本步骤。

有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

在管理中心注册 Threat Defense Virtual 实例

您必须在管理中心的通用设备组下注册虚拟 WAN 中心部署的所有 Threat Defense Virtual 实例。它可以帮助您快速将策略和配置部署到这些实例。

Before you begin

- 需要 Azure 虚拟 WAN 中心中部署的每个Threat Defense Virtual 实例的管理公用 IP 地址。它用于在管理中心中设置和注册实例。
- 在管理中心创建设备组。请参阅添加设备组。
- 创建访问控制策略。请参阅创建基本访问控制策略。
- 在中心中部署 Threat Defense Virtual 期间创建的 FMC 注册密钥。

Procedure

步骤 1 登录管理中心。
步骤 2 依次选择**设备** > **设备管理**。
步骤 3 点击**添加 (Add)** > **设备 (Device)**
步骤 4 输入中心中部署的 Threat Defense Virtual 实例的公用 IP 地址。
步骤 5 提供 Threat Defense Virtual 实例的显示名称。
步骤 6 输入您在中心中部署 Threat Defense Virtual 期间创建的管理中心的**注册密钥**。
步骤 7 从**组 (Group)** 下拉列表中，选择要向其添加 Threat Defense Virtual 实例的设备组。
步骤 8 从**访问控制策略 (Access Control Policy)** 下拉列表中，选择要应用于 Threat Defense Virtual 实例的策略。
步骤 9 根据需要输入其他详细信息。
步骤 10 点击**注册 (Register)**。
步骤 11 重复步骤 1 至步骤 10，注册其他 Threat Defense Virtual 实例。

What to do next

配置 Threat Defense Virtual 实例的接口。

配置接口

注册 Threat Defense Virtual 实例后，必须在管理中心配置其接口。

Azure 虚拟 WAN 仅支持**三个**接口，其配置如下：

- 管理接口，将公用 IP 作为第一个接口。
- 外部接口，将公用 IP 作为第二个接口。

- 内部接口，将专用 IP 用作第三个接口（只有专用 IP）。

Procedure

步骤 1 登录管理中心。
步骤 2 转至**设备 (Devices)** 页面。
步骤 3 点击与已注册的 Threat Defense Virtual 对应的**编辑**图标。
步骤 4 点击与接口对应的**编辑**图标。例如 **GigbitEthernet0/0**。
步骤 5 输入 **outside** 作为第一个接口的名称。
步骤 6 选中**已启用 (Enabled)** 复选框以启用该接口。
步骤 7 在**安全区域 (Security Zone)** 下拉列表中，选择 **Outside**。
步骤 8 点击 **IPv4** 菜单，为接口分配 IP 类型。
步骤 9 从 **IP 类型 (IP Type)** 下拉列表中，选择**使用 DHCP (Use DHCP)** 将接口配置为从 DHCP 获取 IP 地址。
步骤 10 选中**使用 DHCP 获取默认路由 (Obtain default route using DHCP)** 复选框。
步骤 11 在**默认路由 (Default route)** 指标中输入 **1**。
步骤 12 点击 **OK** 以保存配置。
步骤 13 重复步骤 1 至步骤 10 以配置内部接口。

What to do next

为接口配置路由。

为接口配置路由

通过创建网络对象并分配网关 IP 地址，为外部和内部接口配置静态路由。

- 外部接口路由配置使用网关 IP 地址作为所有数据包的默认路由。
- 内部接口路由配置使用网关 IP 地址作为运行状况探测数据包和以中心网络范围为目标的数据包的默认路由。

使用每个接口的 IP 地址和子网掩码地址计算网关 IP 地址。

计算外部和内部接口的网关 IP 地址

本节通过示例说明计算“外部”和“内部”接口的网关 IP 地址的过程。

Procedure

步骤 1 登录管理中心。

步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 访问您在中心部署的 Threat Defense Virtual 实例。

步骤 4 在 **>_Command** 自动中，输入 **`show interface GigbitEthernet 0/0`** 以获取外部接口配置，或者输入 **`show interface GigbitEthernet 0/1`** 以获取内部接口配置详细信息。

步骤 5 重复步骤 1 至步骤 4，以获取内部接口或外部接口的 IP 地址和子网掩码地址。

步骤 6 记下命令结果中的 IP 地址和子网掩码地址。

步骤 7 按照以下示例计算内部和外部的网关 IP 地址：

- 要计算外部接口的网关 IP 地址，请执行以下操作：

  例如：对于 GigabitEthernet0/0（外部接口）

  IP 地址 - **15.0.112.136**

  子网掩码 - **255.255.255.128**

  因此，网关 IP 地址计算为（即此子网中的第一个 IP 地址）**15.0.112.129**。

- 要计算内部接口的网关 IP 地址，请执行以下操作：

  例如：对于 GigabitEthernet0/1（内部接口）

  IP 地址 - **15.0.112.10**

  子网掩码 - **255.255.255.128**

  因此，网关 IP 计算为（即此子网中的第一个 IP 地址）**15.0.112.1**。

What to do next

为内部和外部接口配置默认路由。

为外部接口配置默认路由

Procedure

步骤 1 登录管理中心。

步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击**路由 (Routing)** > **静态路由 (Static Route)**。

步骤 5 点击**添加路由**。

步骤 6 在**接口 (Interface)** 下拉列表中，选择 **Outside**。

步骤 7 在**可用网络 (Available Network)** 下为外部接口选择 **any-ipv4**，然后点击**添加 (Add)**。

步骤 8 输入网关 IP 地址：

a) 点击 + 图标以添加网路对象。
b) 输入网络对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入已计算的外部接口的网关 IP 地址。
e) 点击**保存 (Save)**。

为内部接口配置默认路由

Before you begin

您必须在集线器上部署 Threat Defense Virtual 的 CIDR IP 地址。您需要此信息才能配置内部接口。

Procedure

步骤 1 登录管理中心。
步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。
步骤 3 点击 Threat Defense Virtual 实例。
步骤 4 点击**路由 (Routing)** > **静态路由 (Static Route)**。
步骤 5 点击**添加路由**。
步骤 6 在**接口 (Interface)** 下拉列表中，选择 **Inside**。
步骤 7 添加网络对象，以使用集线器的 CIDR IP 地址来配置内部接口。
a) 点击 + 图标以添加网路对象。
b) 输入网络对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入中心的 CIDR IP 地址（专用地址空间）。
e) 点击**保存 (Save)**。
步骤 8 添加网络对象，以使用负载均衡器运行状况探测 IP 地址来配置内部接口。
a) 点击 + 图标以添加网路对象。
b) 输入网络对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入负载均衡器运行状况探测的 IP 地址。例如：`168.63.129.16`。

此 IP 地址是标准地址或固定地址。

步骤 9 输入网关 IP 地址：
a) 点击 + 图标以添加网路对象。
b) 输入对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入已计算的内部接口的网关 IP 地址。

e) 点击**保存 (Save)**。

配置流量路由

您可以配置静态路由或边界网关协议 (BGP)，用于 Threat Defense Virtual 实例与中心之间的数据交换。它实质上是可以为虚拟 WAN 中心中的网络流量配置的两种不同路由方法。

BGP 是一种动态路由协议，它根据中心与 Threat Defense Virtual 设备之间的实时流量交换来考虑路由。而静态路由使用预配置的路由协议来交换流量。

有关 Azure 虚拟 WAN 的详细信息，请参阅 Microsoft Azure 虚拟 WAN 文档。

配置静态路由

Procedure

步骤 1 登录管理中心。

步骤 2 转至**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击**路由 (Routing)** > **静态路由 (Static Route)**。

步骤 5 点击**添加路由**。

步骤 6 在**接口 (Interface)** 下拉列表中，选择 **Outside**。

如果要配置内部接口，请选择 **Inside**。

步骤 7 添加网络对象 IP 地址：

a) 点击 + 图标以添加网路对象。
b) 输入对象的名称和说明。
c) 点击**主机 (Host)** 网络。
d) 输入 IP 地址。
e) 点击**保存 (Save)**。

启用 BGP 路由

Procedure

步骤 1 登录管理中心。

步骤 2 依次选择**设备** > **设备管理**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击路由 **(Routing)** 菜单。
步骤 5 点击常规设置 **(General Settings)** 下的 **BGP**。
步骤 6 选中启用 **BGP (Enable BGP)** 复选框。
步骤 7 输入虚拟中心的 AS 编号。
步骤 8 点击保存 **(Save)**。

What to do next

配置 BGP 邻居。

配置 BGP 邻居

Procedure

步骤 1 登录管理中心。
步骤 2 选择 **BGP** > **IPv4** > 邻居 **(Neighbor)**。
步骤 3 选中 **Enable IPv4** 复选框。
步骤 4 输入虚拟中心的自治系统 (AS) 编号。
步骤 5 点击添加 **(Add)** 以添加帐户。
步骤 6 输入您记下的 BGP 终端的第一个 IP 地址。
步骤 7 选中已启用的地址 **(Enabled address)** 复选框。
步骤 8 在远程 **AS (Remote AS)** 字段中输入 AS 编号。
步骤 9 选中高级 **(Advanced)** 菜单上的禁用连接验证 **(Disable Connection Verification)** 复选框。
步骤 10 点击保存 **(Save)**。
步骤 11 重复步骤 1 至步骤 8，添加 BGP 终端的第二个 IP 地址。

What to do next

验证 BGP 路由配置。

验证 BGP 路由配置

Before you begin

配置 BGP 终端后，必须验证是否已通过 BGP 终端在 Threat Defense Virtual 和虚拟 WAN 中心之间建立连接。

Procedure

步骤 1 登录管理中心。

步骤 2 依次选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 3 点击 Threat Defense Virtual 实例。

步骤 4 点击**设备 (Device)** > **常规 (General)** 构件中的 **CLI**。

步骤 5 在 **_Command** 字段中，输入 **show route** 以查看并验证连接状态。

Note
代码 **B** 表示 BGP 终端与 Threat Defense Virtual 的连接状态。

配置运行状况探测功能

要确保 Threat Defense Virtual 保持稳定状态，您必须配置连接到内部负载均衡器 (ILB) 的内部接口（受信任）。ILB 通过 TCP 端口 443 执行定期运行状况检查探测，以验证来自 Threat Defense Virtual 的响应。

Procedure

步骤 1 登录管理中心。

步骤 2 依次选择**设备 (Devices)** > **平台设置 (Platform Settings)** > **新策略 (New Policy)** > **威胁防御设置 (Threat Defense Settings)**。

步骤 3 为 Threat Defense Virtual 添加**新策略**，以连接到负载均衡器。

步骤 4 编辑已添加的新策略。

步骤 5 选中**启用 HTTP 服务器 (Enable HTTP Server)** 复选框，然后在**端口 (Port)** 字段中输入 **443**。

步骤 6 点击 **+ 添加 (+ Add)** 以配置 HTTP 地址。

步骤 7 选择运行状况探测器 IP 地址名称。

步骤 8 从**可用区域/接口 (Available Zone/Interface)** 中选择所需的 IP 地址，然后点击**添加 (Add)** 以将其添加到**选定区域/接口 (Selected Zones/Interfaces)**。

步骤 9 点击**确定 (OK)**。

步骤 10 依次选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 11 点击**已应用的策略 (Applied Policies)** 构件中的编辑图标。

步骤 12 从**平台设置 (Platform Settings)** 下拉列表中选择此策略。

步骤 13 根据需要更新并应用安全策略。

有关配置 HTTP 访问的详细信息，请参阅配置 HTTP。

故障排除

以下是虚拟 WAN 中 Threat Defense Virtual 的常见错误情形和调试提示：

- 流量不会路由到 Threat Defense Virtual。
  - 验证 Threat Defense Virtual 对管理中心运行状况探测检查的响应。
  - 验证内部和外部接口的派生网关 IP 地址是否正确。
  - 检查静态路由。
- 未连接 Threat Defense Virtual 的非 RFC RFC 1918：确保在路由意图中明确指定为专用地址的非 RFC 1918 范围。
- 威胁防御部署错误：如果在部署 Threat Defense Virtual 期间遇到错误：**集线器前缀长度应小于或等于 23**，请确保 HUB 地址空间的 CIDR 小于或等于 **/23**。

在 Azure 上部署支持的 IPv6Cisco Secure Firewall Threat Defense Virtual

本章介绍如何从 Azure 门户部署支持 IPv6 的 Threat Defense Virtual。

关于在 Azure 上部署支持的 IPv6

Threat Defense Virtual 产品从 7.3 起同时支持 IPV4 和 IPv6。在 Azure 中，您可以直接从市场产品部署 threat defense virtual，这样会创建或使用虚拟网络，但是目前，Azure 中的限制将市场应用产品限制为仅使用或创建基于 IPv4 的 VNet/子网。虽然可以手动为现有 VNet 配置 IPv6 地址，但无法将新的 threat defense virtual 实例添加到配置了 IPv6 子网的 VNet。Azure 对使用替代方法部署任何第三方资源施加了某些限制，而不是通过市场来部署资源。

思科目前提供两种方法来部署 Threat Defense Virtual 以支持 IPv6 寻址。

提供以下两种不同的自定义 IPv6 模板，其中：

- **自定义 IPv6 模板（ARM 模板）**- 使用 Azure 资源管理器 (ARM) 模板通过 IPv6 配置来部署 threat defense virtual，该模板会在内部引用 Azure 上的市场映像。此模板包含资源和参数定义的 JSON 文件，您可以配置这些资源和参数以部署支持 IPv6 的 threat defense virtual 。要使用此模板，请参阅使用包含市场映像参考的自定义 IPv6 模板从 Azure 部署, on page 253。

编程部署是授予对 Azure 市场上的 VM 映像的访问权限，以通过 PowerShell、Azure CLI、ARM 模板或 API 来部署自定义模板的过程。您只能在 VM 上部署这些自定义模板，而无需提供对 VM 的访问权限。如果您尝试在 VM 上部署此类自定义模板，则会显示以下错误消息：

尚未接受此订用中的此项目的法律条款。要接受法律条款…并为“市场”项目配置程序化部署…

您可以使用以下方法之一在Azure中启用编程部署，以便部署引用市场映像的自定义IPv6(ARM)模板：

- **Azure 门户** - 启用与 Azure 市场上提供的 threat defense virtual 产品相对应的编程部署选项，用于部署自定义 IPv6 模板（ARM 模板）。
- **Azure CLI** - 运行 CLI 命令以启用用于部署自定义 IPv6（ARM 模板）的编程部署。

- **自定义 VHD 映像和 IPv6 模板（ARM 模板）** - 在 Azure 上使用 VHD 映像和 ARM 模板来创建托管映像。此过程类似于使用 VHD 和资源模板部署 threat defense virtual 。此模板在部署期间引用托管映像，并会使用您可以在 Azure 上上传和配置的 ARM 模板来部署支持 IPv6 的 threat defense virtual 。请参阅使用 VHD 和自定义 IPv6 模板从 Azure 部署, on page 258。

根据市场映像或带有自定义 IPv6 模板的 VHD 映像，使用自定义 IPv6 模板（ARM 模板）来部署 threat defense virtual 所涉及的过程。

部署 threat defense virtual 所涉及的步骤如下：

Table 22:

步骤	过程
1	在计划部署支持 IPv6 的 threat defense virtual 的 Azure 中创建 Linux VM
2	仅当使用具有市场映像引用的自定义 IPv6 模板部署 threat defense virtual 时，才可在 Azure 门户或 Azure CLI 上启用编程部署选项。
3	根据部署类型，下载以下自定义模板： • 具有 Azure 市场参考映像的自定义 IPv6 模板。 具有自定义 IPv6 (ARM) 模板的 VHD 映像。
4	更新自定义 IPv6 (ARM) 模板中的 IPv6 参数。 **Note** 仅当您使用具有市场映像引用的自定义 IPv6 模板来部署 threat defense virtual 时，才需要市场映像版本的等效软件映像版本参数值。您必须运行命令来检索软件版本详细信息。
5	通过 Azure 门户或 Azure CLI 来部署 ARM 模板。

使用包含市场映像参考的自定义 IPv6 模板从 Azure 部署

参考市场映像使用自定义 IPv6 模板（ARM 模板）部署 threat defense virtual 所涉及的过程。

Procedure

步骤 1 登录到 Azure 门户。

Azure 门户显示与当前帐户和订用相关联的虚拟要素，与数据中心位置无关。

步骤 2 通过 Azure 门户或 Azure CLI 启用编程部署，如下所示：

在 Azure 门户上启用此选项：

a) 在 **Azure 服务 (Azure Services)**，点击**订用 (Subscriptions)** 以查看订用边栏选项卡页面。
b) 在左窗格中，点击**设置 (Settings)** 选项下的**编程部署 (Programmatic Deployment)**。

随后将显示 VM 上部署的所有类型的资源，以及关联的订用产品。

c) 点击**状态 (Status)** 列下 threat defense virtual 产品对应的**启用 (Enable)**，以获取自定义 IPv6 模板的编程部署。

或

通过 Azure CLI 启用此选项：

a) 转到 Linux VM。
b) 运行以下 CLI 命令，为部署自定义 IPv6 (ARM) 模板启用编程部署。

在命令执行期间，每个映像订用只能接受一次条款。

 # 接受条款

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # 条款是否已被接受（例如，已接受 = true）

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

其中，

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-ftdv'
- **<sku/plan>** - 'ftdv-azure-byol'

以下是启用程序化部署以通过 BYOL 订用计划部署 threat defense virtual 的一个命令脚本示例。

- **az vm image terms show -p cisco -f cisco-ftdv --plan ftdv-azure-byol**

步骤 3 运行以下命令，以便检索与市场映像版本等效的软件版本详细信息。

az vm image list --all -p <publisher> -f <offer> -s <sku>

其中，

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-ftdv'
- **<sku>** - 'ftdv-azure-byol'

以下是检索等效于 threat defense virtual 的市场映像版本的软件版本详细信息的一个命令脚本示例。

az vm image list --all -p cisco -f cisco-ftdv -s ftdv-azure-byol

步骤 4 从显示的可用市场映像版本列表中选择一个 threat defense virtual 版本。

对于 threat defense virtual 的 IPv6 支持部署，您必须选择 73* 或更高版本的 threat defense virtual 。

步骤 5 从思科 GitHub 存储库下载市场自定义 IPv6 模板（ARM 模板）。

步骤 6 通过在参数模板文件 (JSON) 中提供部署值来准备参数文件。

下表介绍了您需要在 threat defense virtual 自定义部署的自定义 IPv6 模板参数中输入的部署值：

参数名	允许的值/类型的示例	说明
vmName	csf-tdv	在 Azure 中为 threat defense virtual VM 命名。
softwareVersion	730.33.0	市场映像版本的软件版本。
billingType	BYOL	许可方法为 BYOL 或 PAYG。 与 PAYG 相比，BYOL 许可证更具成本效益，因此建议选择 BYOL 订用部署。
adminUsername	hjohn	用于登录 threat defense virtual 的用户名。 您不能使用保留名称“admin”，该名称已分配给管理员。
adminPassword	E28@4OiUrhx!	管理员密码。 密码组合必须是长度为 12 到 72 个字符的字母数字字符。密码组合必须由小写和大写字母、数字和特殊字符组成。
vmStorageAccount	hjohnvmsa	您的 Azure 存储帐户。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户字符的长度必须介于 3 到 24 个字符之间。密码组合只能包含小写字母和数字。

参数名	允许的值/类型的示例	说明
availabilityZone	0	指定用于部署的可用性区域，公共IP和虚拟机将在指定的可用性区域中创建。 如果不需要可用性区域配置，请将其设置为“**0**”。确保所选区域支持可用性区域，并且所提供的值正确无误。（该值必须是0-3之间的整数）。
customData	{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\":\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}	要在 Day 0 配置中向 threat defense virtual 提供的字段。默认情况下，它有以下三个要配置的键值对： • “admin”用户密码 • Management Center Virtual 主机名 • 用于管理的 Management Center Virtual 主机名或 CSF-DM。 'ManageLocally : yes' - 这将配置要用作 threat defense virtual管理器的 CSF-DM。 您可以将 Management Center Virtual 配置为 threat defense virtual 管理器，也可以为在 Management Center Virtual 上进行相同配置所需的字段提供输入。
virtualNetworkResourceGroup	cisco-tdv-rg	包含虚拟网络的资源组的名称。如果 virtualNetworkNewOrExisting 是新的，则此值应与为模板部署选择的资源组相同。
virtualNetworkName	cisco-tdv-vent	虚拟网络的名称。
virtualNetworkNewOrExisting	new	此参数将确定是应创建新的虚拟网络，还是使用现有的虚拟网络。

参数名	允许的值/类型的示例	说明
virtualNetworkAddressPrefixes	10.151.0.0/16	虚拟网络的 IPv4 地址前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	虚拟网络的 IPv6 地址前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet1Name	mgmt	管理子网名称。
Subnet1Prefix	10.151.1.0/24	管理子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	管理子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet1StartAddress	10.151.1.4	管理接口 IPv4 地址。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理接口 IPv6 地址。
Subnet2Name	diag	数据接口 1 子网名称。
Subnet2Prefix	10.151.2.0/24	数据接口 1 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	数据接口 1 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet2StartAddress	10.151.2.4	数据接口 1 IPv4 地址。
subnet2v6StartAddress	ace:cab:deca:2222::6	数据接口 1 IPv6 地址。
Subnet3Name	内部	数据接口 2 子网名称。
Subnet3Prefix	10.151.3.0/24	数据接口 2 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	数据接口 2 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet3StartAddress	10.151.3.4	数据接口 2 IPv4 地址。

参数名	允许的值/类型的示例	说明
subnet3v6StartAddress	ace:cab:deca:3333::6	数据接口 2 IPv6 地址。
Subnet4Name	外部	数据接口 3 子网名称。
Subnet4Prefix	10.151.4.0/24	数据接口 3 子网 IPv4 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	数据接口 3 子网 IPv6 前缀，仅当“virtualNetworkNewOrExisting”设置为“new”时为必填。
subnet4StartAddress	10.151.4.4	数据接口 3 IPv4 地址。
subnet4v6StartAddress	ace:cab:deca:4444::6	数据接口 3 IPv6 地址。
vmSize	Standard_D4_v2	threat defense virtual VM 的大小。Standard_D3_v2 为默认值。

步骤 7 使用 ARM 模板通过 Azure 门户或 Azure CLI 部署 threat defense virtual 防火墙。有关在 Azure 上部署 ARM 模板的信息，请参阅以下 Azure 文档：

- 使用 Azure 门户创建和部署 ARM 模板
- 通过 CLI 部署本地 ARM 模板

What to do next

接下来的步骤取决于您选择的管理模式。

- 如果您为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，z呃您将使用 Cisco Secure Firewall Management Center 来管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual。
- 如果您为**启用本地管理器 (Enable Local Manager)** 选择**是 (Yes)**，则您将使用集成 Cisco Secure Firewall 设备管理器 来管理 threat defense virtualthreat defense virtualthreat defense virtualthreat defense virtual；请参阅使用 Cisco Secure Firewall 设备管理器来管理 Cisco Secure Firewall Threat Defense Virtual。

  有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual。

使用 VHD 和自定义 IPv6 模板从 Azure 部署

您可以使用 Cisco 提供的压缩 VHD 映像，创建自己的自定义 threat defense virtual 映像。此过程类似于使用 VHD 和资源模板部署 threat defense virtual 。

开始之前

- 您需要 JSON 模板和相应的JSON参数文件，以便使用 VHD 和 ARM 更新的模板在 Github 上部署 threat defense virtual ，您可以在那里找到有关如何构建模板和参数文件的说明。
- 此程序需要使用 Azure 中的现有 Linux 虚拟机。我们建议您使用临时 Linux 虚拟机（例如 Ubuntu 16.04）将压缩 VHD 映像上传至 Azure。此映像在解压时需要约 50G 的存储空间。而且，从 Azure 中的 Linux 虚拟机上传到 Azure 存储，上传时间也会更快。

  如果您需要创建虚拟机，请使用以下方法之一：
  - 使用 Azure CLI 创建 Linux 虚拟机
  - 通过 Azure 门户创建 Linux 虚拟机
- 在 Azure 订用中，您应该在要部署 threat defense virtual 的位置具有可用的存储帐户。

过程

步骤 1 从 Cisco 下载软件页面 (Cisco Download Software) 下载 threat defense virtual 压缩 VHD 映像 (*.bz2)：

a) 导航至 **产品** > **安全** > **防火墙** > **下一代防火墙 (NGFW)** > **Cisco Secure Firewall Threat Defense Virtua**。

b) 点击 **Firepower 威胁防御软件**。

按照说明下载映像。

Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

步骤 2 执行使用 VHD 和资源模板从 Azure 部署中的**步骤 2** 至**步骤 8**。

步骤 3 点击**自定义部署 (Custom deployment)** 页面顶部的**编辑参数 (Edit parameters)**。您有一个可供自定义的参数模板。

a) 点击**加载文件 (Load file)**，然后浏览到自定义 threat defense virtual 参数文件。请参阅 Github 上使用 VHD 和自定义 IPv6 (ARM) 模板的 Azure threat defense virtual 部署示例，您可以在这里找到有关如何构建模板和参数文件的说明。

b) 将您的自定义 JSON 参数代码粘贴到窗口中，然后点击**保存 (Save)**。

下表介绍了您需要在 threat defense virtual 部署的自定义 IPv6 模板参数中输入的部署值：

参数名	允许的值/类型的示例	说明
vmName	csf-tdv	在 Azure 中为 threat defense virtual VM 命名。

参数名	允许的值/类型的示例	说明
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name}	用于部署的映像的 ID。在内部，Azure 将每个资源与一个资源 ID 相关联。
adminUsername	hjohn	用于登录 threat defense virtual 的用户名。 您不能使用保留名称“admin”，该名称已分配给管理员。
adminPassword	E28@4OiUrhx!	管理员密码。 密码组合必须是长度为 12 到 72 个字符的字母数字字符。密码组合必须由小写和大写字母、数字和特殊字符组成。
vmStorageAccount	hjohnvmsa	您的 Azure 存储帐户。您可以使用现有存储帐户，也可以创建新的存储帐户。存储帐户字符的长度必须介于 3 到 24 个字符之间。密码组合只能包含小写字母和数字。
availabilityZone	0	指定用于部署的可用性区域，公共 IP 和虚拟机将在指定的可用性区域中创建。 如果不需要可用性区域配置，请将其设置为“**0**”。确保所选区域支持可用性区域，并且所提供的值正确无误。（该值必须是 0-3 之间的整数）。
customData	{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}	要在 Day 0 配置中向 threat defense virtual 提供的字段。默认情况下，它有以下三个要配置的键值对： • “admin”用户密码 • CSF-MCv 主机名 • 用于管理的 CSF-MCv 主机名或 CSF-DM。 'ManageLocally : yes' - 这将配置要用作 threat defense virtual管理器的 CSF-DM。

参数名	允许的值/类型的示例	说明
		您可以将 CSF-MCv 配置为 threat defense virtual 管理器，也可以为在 CSF-MCv 上进行相同配置所需的字段提供输入。
virtualNetworkResourceGroup	csf-tdv	包含虚拟网络的资源组的名称。如果 virtualNetworkNewOrExisting 是新的，则此值应与为模板部署选择的资源组相同。
virtualNetworkName	hjohn-vm-vn	虚拟网络的名称。
virtualNetworkNewOrExisting	new	此参数将确定是应创建新的虚拟网络，还是使用现有的虚拟网络。
virtualNetworkAddressPrefixes	10.151.0.0/16	虚拟网络的 IPv4 地址前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	虚拟网络的 IPv6 地址前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet1Name	mgmt-ipv6	管理子网名称。
Subnet1Prefix	10.151.1.0/24	管理子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	管理子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet1StartAddress	10.151.1.4	管理接口 IPv4 地址。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理接口 IPv6 地址。
Subnet2Name	diag	数据接口 1 子网名称。
Subnet2Prefix	10.151.2.0/24	数据接口 1 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	数据接口 1 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet2StartAddress	10.151.2.4	数据接口 1 IPv4 地址。

参数名	允许的值/类型的示例	说明
subnet2v6StartAddress	ace:cab:deca:2222::6	数据接口 1 IPv6 地址。
Subnet3Name	内部	数据接口 2 子网名称。
Subnet3Prefix	10.151.3.0/24	数据接口 2 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	数据接口 2 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet3StartAddress	10.151.3.4	数据接口 2 IPv4 地址。
subnet3v6StartAddress	ace:cab:deca:3333::6	数据接口 2 IPv6 地址。
Subnet4Name	外部	数据接口 3 子网名称。
Subnet4Prefix	10.151.4.0/24	数据接口 3 子网 IPv4 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	数据接口 3 子网 IPv6 前缀，仅当“virtualNetworkNewOr Existing”设置为“new”时为必填。
subnet4StartAddress	10.151.4.4	数据接口 3 IPv4 地址。
subnet4v6StartAddress	ace:cab:deca:4444::6	数据接口 3 IPv6 地址。
vmSize	Standard_D4_v2	threat defense virtual VM 的大小。Standard_D3_v2 为默认值。

步骤 4 使用 ARM 模板通过 Azure 门户或 Azure CLI 部署 threat defense virtual 防火墙。有关在 Azure 上部署 ARM 模板的信息，请参阅以下 Azure 文档：

- 使用 Azure 门户创建和部署 ARM 模板
- 通过 CLI 部署本地 ARM 模板

下一步做什么

- 在 Azure 中更新 threat defense virtual 的 IP 配置。

Threat Defense Virtual 映像快照

您可以在 Azure 门户中使用快照映像创建和部署 threat defense virtual。映像快照是没有状态数据的已复制 threat defense virtual 映像实例。

Threat Defense Virtual 快照概述

创建 threat defense virtual 实例快照映像的过程跳过为 threat defense virtual 和 FSIC 执行的首次启动程序，有助于最大限度地缩短初始系统初始化时间。快照映像包含了预填充的数据库和 threat defense virtual 初始启动过程，该过程使映像能够重新生成与 管理中心 或任何其他管理中心中的系统身份相关的唯一 ID（UUID、序列号）。此过程有助于缩短 threat defense virtual 的启动时间，这在 Auto Scale 部署中至关重要。

Note 目前，使用 Threat Defense Virtual的快照映像部署的实例不支持即用即付 (PAYG) 许可。PAYG 许可仅适用于直接从市场部署的 实例。您可以将智能许可用于具有 PAYG 许可的新的 Threat Defense Virtual 部署。

从托管映像创建 Threat Defense Virtual 快照映像

Threat Defense Virtual 映像快照创建是在 Azure 门户中复制 threat defense virtual 实例的现有托管映像的过程。

Before you begin

您必须通过将调整大小的 VHD 映像上传到 Azure 门户中 Linux VM 的 Azure 存储帐户中的容器，创建 threat defense virtual 版本 7.2 或更高版本的托管映像。有关创建调整大小的 VHD 映像的信息，请参阅从 Azure 使用 VHD 和资源模板部署, on page 182。

不得将正准备拍摄映像快照的 threat defense virtual 实例注册到任何管理器，例如 管理中心 或 设备管理器。

Procedure

步骤 1 转至 Azure 门户，您已在其中创建了 threat defense virtual 实例的托管映像。

Note
确保您计划复制的 threat defense virtual 实例未注册到 管理中心，未配置到任何其他本地管理器，也未通过任何配置应用。

步骤 2 转至**资源组 (Resource Group)**，然后选择 threat defense virtual 实例。

步骤 3 点击 threat defense virtual 实例的导航页面上的**串行控制台 (Serial Console)**。

步骤 4 使用以下脚本从专家 shell 运行预快照进程：

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

在脚本中使用 `prepare_snapshot` 命令时，系统会显示一条中间消息，提示您确认执行脚本。按 **Y** 运行脚本。

或者，您可以在此命令后添加 `-f`（例如 `root@firepower:/ngfw/var/common#prepare_snapshot -f`），以跳过用户确认消息并直接执行脚本。

此脚本会删除与 threat defense virtual 实例关联的所有行配置、已部署的策略、已配置的管理器和 UUID。处理完成后，threat defense virtual 实例将关闭。

步骤 5 点击**捕获 (Capture)**。

步骤 6 在**创建映像 (Create an image)** 页面中，从**资源组 (Resource Group)** 下拉列表中选择现有资源组或创建新资源组。

步骤 7 点击**实例详细信息 (Instance Details)** 部分中的**否，仅捕获托管映像 (No, capture only a managed image)**，仅创建托管映像。

步骤 8 为使用 threat defense virtual 实例的托管映像创建的快照映像提供名称。

步骤 9 点击**查看 + 创建 (Review+Create)** 以创建 threat defense virtual 实例的新快照映像。

What to do next

使用快照映像部署 threat defense virtual 实例。请参阅使用映像快照部署 Threat Defense Virtual 实例。

使用映像快照部署 Threat Defense Virtual 实例

Before you begin

Cisco 建议以下操作：

- 确认快照映像可用于 threat defense virtual 实例。

Procedure

步骤 1 登录到 Azure 门户。

步骤 2 复制新创建快照映像的资源 ID。

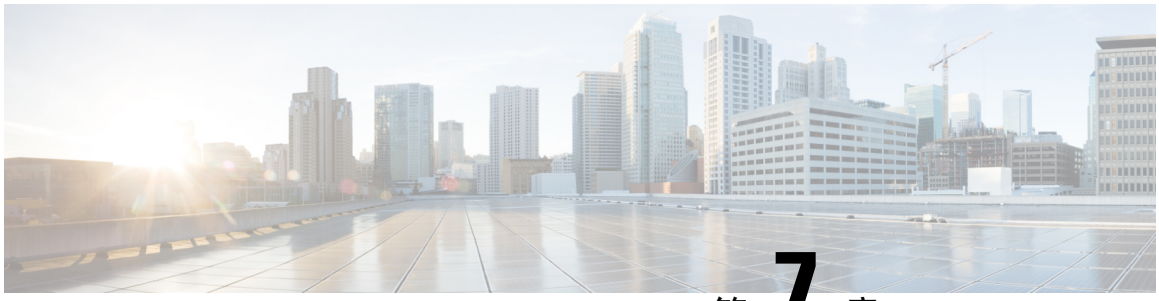
Note
Azure 会为每个资源（快照映像）关联一个资源 ID。部署新的 threat defense virtual 实例需要快照映像的资源 ID。

a) 在 Azure 门户中，选择**映像 (Images)**。
b) 选择您使用托管映像创建的快照映像。
c) 点击**概述 (Overview)** 查看映像属性。

d) 将 **Resource ID** 复制到剪贴板。**Resource ID** 语法表示为：
/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

步骤 3 使用快照映像继续部署 threat defense virtual 实例。请参阅从 Azure 使用 VHD 和资源模板部署, on page 182。

Note
您可以从 threat defense virtual 控制台运行 CLI 命令 **show version** 和 **show snapshot detail**，以了解新部署的 threat defense virtual 实例的版本和详细信息。



第 7 章

在 OCI 上部署 Threat Defense Virtual

您可以在 Oracle Cloud 基础设施 (OCI) 上部署 threat defense virtual，前者是一种公共云计算服务，使您能够在 Oracle 提供的高可用性托管环境中运行应用程序。

以下程序介绍了如何准备 OCI 环境并启动 threat defense virtual实例。您可以登录 OCI 门户，在 OCI 市场中搜索 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品，然后启动计算实例。启动 threat defense virtual后，您必须配置路由表，以便根据流量的源和目标将流量定向到防火墙。

概述

Cisco Cisco Secure Firewall Threat Defense Virtual 运行与物理 Cisco 威胁防御 相同的软件，以虚拟形式提供成熟的安全功能。threat defense virtual 可以部署在公共 OCI 中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

OCI 计算资源大小

形状是确定分配给实例的 CPU 数量、内存量和其他资源的模板。threat defense virtual 支持以下 OCI 形状类型：

表 *23: Threat Defense Virtual* 支持的计算资源大小

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.DenseIO2.8	7.3.x 及更高版本	8	120	最小值 4，最大值 8
Intel VM.StandardB1.4	7.3.x 及更高版本	4	48	最小值 4，最大值 4
Intel VM.StandardB1.8	7.3.x 及更高版本	4	96	最小值 4，最大值 8
Intel VM.Standard1.4	7.3.x 及更高版本	4	28	最小值 4，最大值 4
Intel VM.Standard1.8	7.3.x 及更高版本	8	56	最小值 4，最大值 8
Intel VM.Standard2.4	7.1、7.2.x 和 7.3.x	4	60	最小值 4，最大值 4
Intel VM.Standard2.8	7.1、7.2.x 和 7.3.x	8	120	最小值 4，最大值 8
Intel VM.Standard3.Flex*	7.3.x 及更高版本	4	16	最小值 4，最大值 4
	7.3.x 及更高版本	6	24	最小值 4，最大值 6
	7.3.x 及更高版本	8	32	最小值 4，最大值 8

OCI 形状	支持的 Threat Defense Virtual 版本	属性		接口
		oCPU	随机存取存储器 (GB)	
Intel VM.Optimized3.Flex*	7.3.x 及更高版本	4	16	最小值 4，最大值 8
	7.3.x 及更高版本	6	24	最小值 4，最大值 10
	7.3.x 及更高版本	8	32	最小值 4，最大值 10
AMD VM.Standard.E4.Flex*	7.3.x 及更高版本	4	16	最小值 4，最大值 4
	7.3.x 及更高版本	6	24	最小值 4，最大值 6
	7.3.x 及更高版本	8	32	最小值 4，最大值 8

- *7.4.x 及更高版本中的 Flex 形状支持 SR-IOV 模式。
- 在 OCI 中，1 个 oCPU 等于 2 个 vCPU。
- threat defense virtual 至少需要 4 个接口。

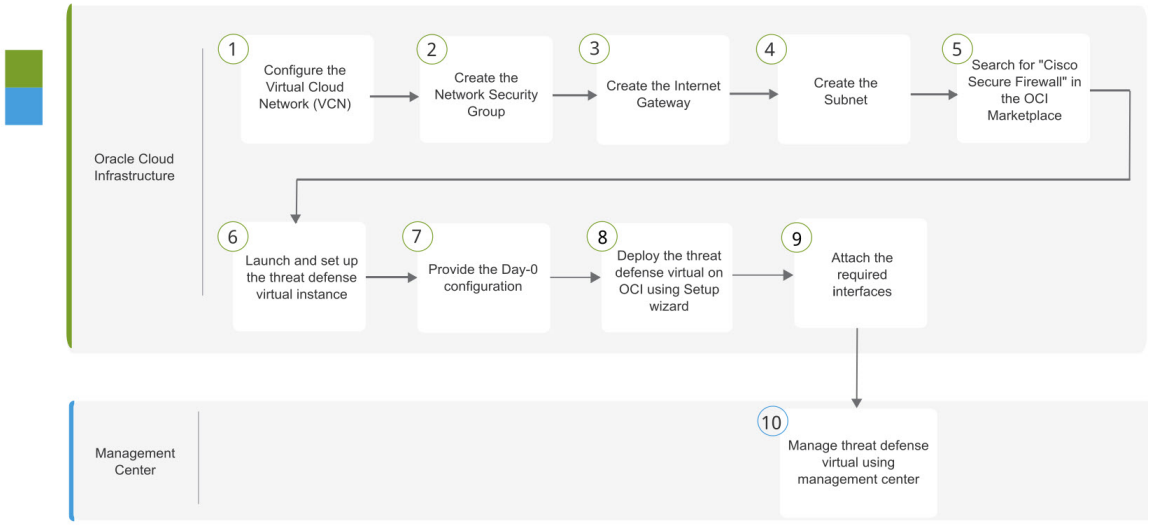
有关使用 Threat Defense Virtual 7.3 及更高版本支持的 OCI 计算形状的建议。

- OCI 市场映像版本 **7.3.0-69-v2** 及更高版本仅与 Threat Defense Virtual 7.3 及更高版本的 OCI 计算形状兼容。
- 您只能将 Threat Defense Virtual 7.3 及更高版本支持的 OCI 计算形状用于新部署。
- OCI 计算配置版本 **7.3.0-69-v3** 及更高版本与使用 Threat Defense Virtual 7.3 之前的 OCI 计算配置版本升级与 Threat Defense Virtual 一起部署的虚拟机不兼容。
- **VM.DenseIO2.8** 计算形态订用将继续计费，即使在您关闭实例后也是如此。有关详细信息，请参阅 OCI 文档。

您可以在 OCI 上创建账户，使用 Oracle 云市场上的思科 Firepower NGFW 虚拟防火墙（NGFWv）产品来启动计算实例，然后选择 OCI 形状。

端到端程序

以下流程图说明了在 Oracle Cloud 基础设施上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Oracle Cloud 基础设施	配置 OCI 环境：配置虚拟云网络 (VCN)（**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **CIDR 块 (CIDR block)** > **创建 VCN (Create VCN)**。
2	Oracle Cloud 基础设施	创建网络安全组：创建网络安全组。依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。
3	Oracle Cloud 基础设施	创建互联网网关：创建互联网网关。**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)** > **创建互联网网关 (Create Internet Gateway)**。
4	Oracle Cloud 基础设施	创建子网：创建子网。**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)** > **创建子网 (Create Subnet)**。
5	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 277 页：在 OCI 市场中搜索“Cisco Secure Firewall”。
6	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 277 页：启动并设置 Threat Defense Virtual 实例。
7	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 277 页：提供 Day-0 配置。
8	Oracle Cloud 基础设施	在 OCI 上部署 Threat Defense Virtual，第 277 页：使用设置向导在 OCI 上部署 Threat Defense Virtual。

	工作空间	步骤
9	Oracle Cloud 基础设施	连接接口：连接接口。**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**。
10	管理中心	使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

前提条件

- 在 https://www.oracle.com/cloud/ 上创建一个 OCI 账户。
- 思科智能账户。可以在思科软件中心 (https://software.cisco.com/) 创建一个账户。
- 许可 threat defense virtual。
  - 所有安全服务的许可证授权均在 管理中心中配置。
  - 有关如何管理许可证的详细信息，请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”。

注释 思科提供的所有默认许可证授权（以前用于 Firewall Threat Defense Virtual 虚拟设备）都将支持 IPv6 配置。

- 接口要求：
  - 管理接口 (2) - 一个用于将 threat defense virtual 连接到 管理中心，另一个用于诊断；无法用于直通流量。
  - 流量接口 (2) - 用于将 threat defense virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于访问 threat defense virtual的公共 IP。
- 有关 threat defense virtual 系统要求，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

准则和限制

支持的功能

- 在 OCI 虚拟云网络 (VCN) 中部署
- 路由模式（默认）

- 许可 - 仅支持 BYOL
- IPv6
- 仅 管理中心 支持。
- 支持单根 I/O 虚拟化 (SR-IOV)。

FTDv 智能许可的性能级别

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *24:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

注释 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 OCI 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。

- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

- 通过 设备管理器 提供本地管理支持。
- Threat Defense Virtual 本地 HA
- 透明/内联/被动模式
- 通过 DHCP 配置数据接口

限制

- OCI 上的 Threat Defense Virtual部署不支持将 Mellanox 5 作为 SR-IOV 模式下的 vNIC。
- IPv6 仅适用于根据 OCI 标准（VCN IPv4 和 IPv6）配置的　双堆栈。
- Firewall Threat Defense Virtual（ASAv 静态和 DHCP 配置）所需的单独路由规则。

网络拓扑示例

下图显示了在路由防火墙模式下建议用于 threat defense virtual 的拓扑，在 OCI 中为 threat defense virtual 配置了 4 个子网（管理、诊断、内部和外部）。

图 *38:* 包含四个 *VCN* 中的子网的 *OCI* 部署示例 *Threat Defense Virtual*

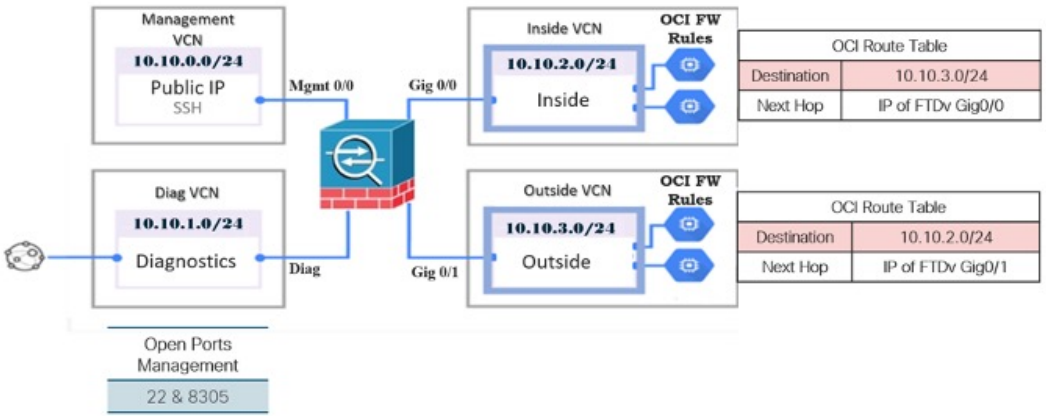
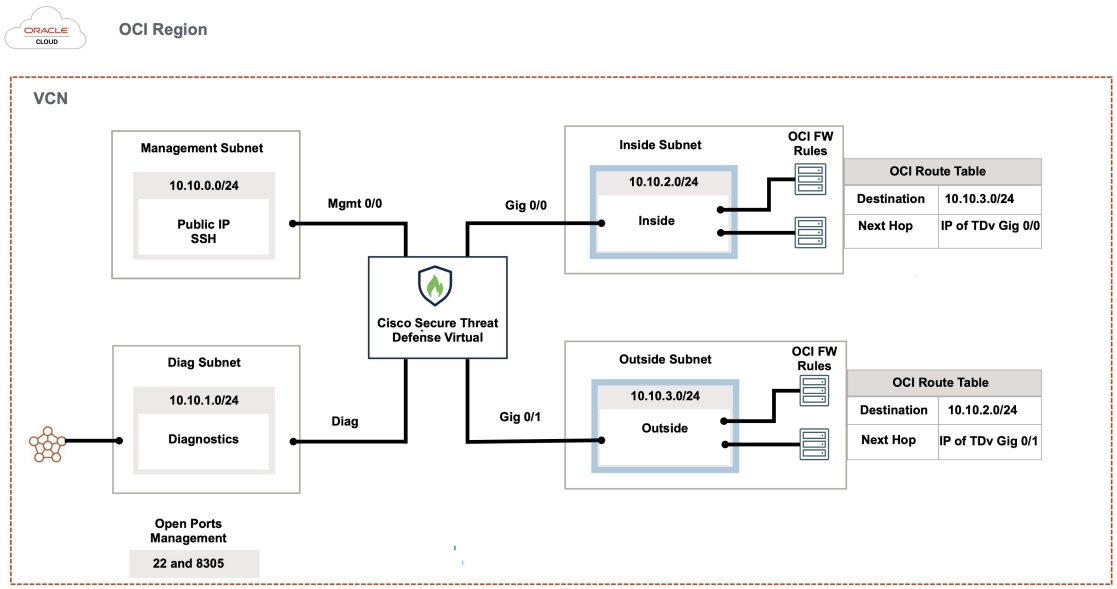
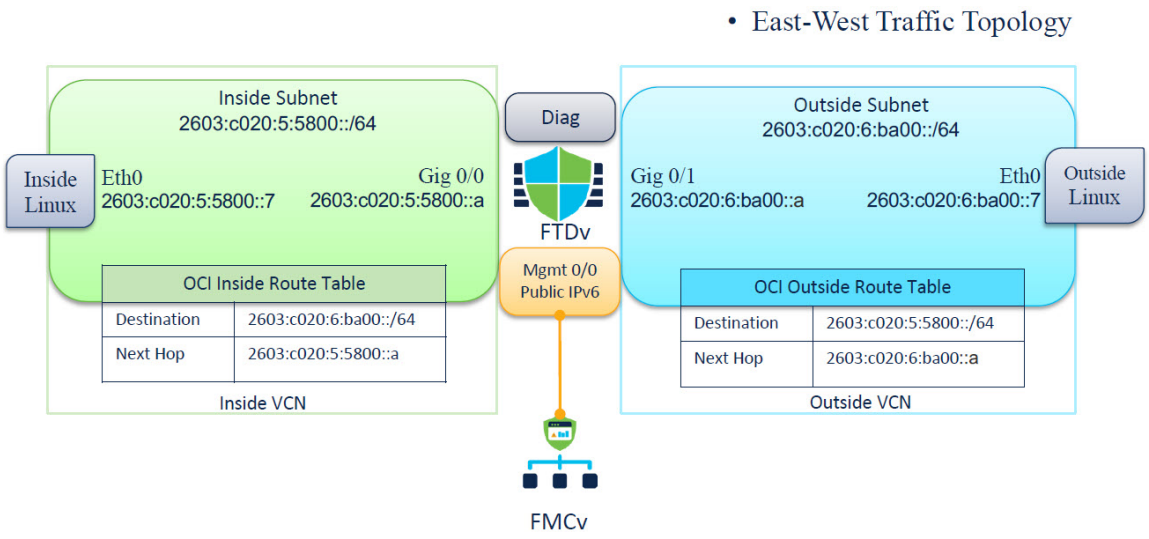


图 *39: VCN* 中具有四个子网的 *OCI* 部署示例 *Threat Defense Virtual*



注释 在单个 VCN 中使用四个子网时，必须将特定于子网的路由添加到与该子网关联的路由表中。

Threat Defense Virtual IPv6 部署拓扑



如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

配置 OCI 环境

您可以为 Threat Defense Virtual 部署配置虚拟云网络 (VCN)，具体如下：

- **多个 VCN (Multiple VCNs)** - 至少需要四个 VCN，每个 threat defense virtual 接口各一个。这允许在不同网络之间进行隔离的流量检测。
- **带子网的单个 VCN (Single VCN with Subnets)** - 或者，您可以配置带四个子网的单个 VCN，每个 Threat Defense Virtual 接口各一个。在此配置中，防火墙可以使用关联的路由表检查和控制同一 VCN 中子网之间的流量。这使您可以在使用单个 VCN 时有效地管理子网间流量。

您可以继续执行以下程序来完成管理 VCN。然后返回到**网络 (Networking)**，为诊断接口、内部接口和外部接口创建 VCN。

过程

步骤 1 登录 OCI 并选择您的区域。

OCI 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击**创建 VCN (Create VCN)**。

步骤 3 输入 VCN 的描述性**名称**，例如 *FTDv-Management*。

步骤 4 输入 VCN 的 **CIDR 块**。

a) IP 地址的 IPv4 CIDR 块。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

注释
在此 VCN 中使用 DNS 主机名。

b) IP 地址的 IPv6 CIDR 块。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，[::/0]。

c) 选择 IPv6 CIDR 块作为 Oracle 为虚拟云网络分配的 IPv6/56 前缀。

步骤 5 点击**添加 IPv6 CIDR 块 (Add IPv6 CIDR Block)** 以添加新的 IPv6 块。

步骤 6 添加 VCN 的 IPv6 前缀，例如 */54*。

步骤 7 点击**创建 VCN (Create VCN)**。

下一步做什么

继续执行以下程序以完成管理 VCN。完成管理 VCN 后，您将为诊断接口、内部接口和外部接口创建 VCN。

注释 从导航菜单中选择服务后，左侧的菜单包括隔间列表。隔间可帮助您组织资源，以便更轻松地控制对资源的访问。您的根隔间由Oracle在调配租用时为您创建。管理员可以在根隔间中创建更多隔间，然后添加访问规则以控制哪些用户可以在其中查看和执行操作。有关详细信息，请参阅 Oracle 文档管理隔间。

创建网络安全组

网络安全组由一组 vNIC 和一组应用于这些 vNIC 的安全规则组成。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **网络安全组 (Network Security Groups)**，然后点击**创建网络安全组 (Create Network Security Group)**。

步骤 2 输入网络安全组的描述性**名称**，例如 *FTDv-Mgmt-Allow-22-8305*。

步骤 3 点击**下一步 (Next)**。

步骤 4 添加安全规则：

a) 添加规则以允许 TCP 端口 22 用于 SSH 访问。

b) 添加规则以允许 TCP 端口 8305 用于 HTTPS 访问。

可以通过 管理中心 管理 threat defense virtual，这需要为 HTTPS 连接打开端口 8305。

注释
您可以将这些安全规则应用于管理接口/VCN。

步骤 5 点击**创建 (Create)**。

创建互联网网关

要使管理子网可公开访问，则需要互联网网关。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **互联网网关 (Internet Gateways)**，然后点击**创建互联网网关 (Create Internet Gateway)**。

步骤 2 输入您的互联网网关的描述性**名称**，例如 *FTDv-IG*。

步骤 3 点击**创建互联网网关 (Create Internet Gateway)**。

步骤 4 将路由添加至互联网网关：

a) 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **路由表 (Route Tables)**。

b) 点击默认路由表的链接以添加路由规则。

c) 点击**添加路由规则 (Add Route Rules)**。

d) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。

e) 输入目标 IPv4 CIDR 块，例如 0.0.0.0/0。

f) 输入目标 IPv6 CIDR 块，例如 [::/0]。

g) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中选择您创建的网关。

h) 点击**添加路由规则 (Add Route Rules)**。

创建子网

每个 VCN 至少有一个子网。您将为管理 VCN 创建一个管理子网。诊断 VCN 还需要一个诊断子网，内部 VCN 需要一个内部子网，外部 VCN 需要一个外部子网。

如果使用一个 VCN，则要在 VCN 内创建管理子网、诊断子网、内部子网和外部子网。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)** > **虚拟云网络详细信息 (Virtual Cloud Network Details)** > **子网 (Subnets)**，然后点击**创建子网 (Create Subnet)**。

步骤 2 输入子网的描述性**名称 (Name)**，例如管理 *(Management)*。

步骤 3 选择**子网类型 (Subnet Type)**（保留建议的默认值**区域 (Regional)**）。

步骤 4 输入 **CIDR 块 (CIDR Block)**，例如 10.10.0.0/24。子网的内部（非公共）IP 地址可从此 CIDR 块获取。

a) 如果要启用 IPv6，则选中**启用 IPv6 CIDR 块 (ENABLE IPv6 CIDR BLOCK)** 复选框。

b) 在 **IPv6 CIDR 块 (IPv6 CIDR Block)** 中，输入 IPv6 前缀范围。

步骤 5 从**路由表 (Route Table)** 下拉列表中选择您之前创建的路由表之一。

步骤 6 为您的子网选择**子网访问 (Subnet Access)**。

对于“管理”(Management) 子网，这必须是**公共子网 (Public Subnet)**。

步骤 7 选择 **DHCP 选项 (DHCP Option)**。

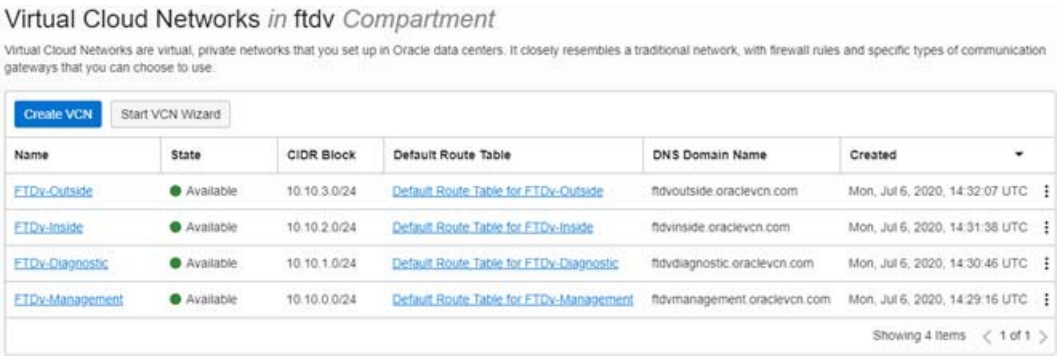
步骤 8 选择您之前创建的**安全列表**。

步骤 9 点击**创建子网 (Create Subnet)**。

下一步做什么

配置管理 VCN（管理、诊断、内部、外部）后，您便可以启动 threat defense virtual。有关 threat defense virtual VCN 配置的示例，请参见下图。

图 ***40: threat defense virtual*** 虚拟云网络



使用 Cloud Shell 配置 IPv6 网关地址

在 OCI 中，每个子网都有一个唯一的 IPv6 网关地址，您必须在 threat defense virtual 中配置该地址，IPv6 流量才会正常工作。此网关地址可从在云外壳中运行 OCI 命令的子网详细信息进行检索。

在 OCI 上部署 Threat Defense Virtual

过程

步骤 1 转至 **OCI** > **打开 CloudShell（OCI 云终端）(Open CloudShell [OCI Cloud Terminal])** 。

步骤 2 执行以下命令以便从子网获取 IPv6 详细信息：

```
oci network subnet get  -subnet_id <subnet_OCID>
```

步骤 3 从命令结果中查找 `ipv6-virtual-router-ip` 键。

步骤 4 复制该键的值并根据需要使用它。

在 OCI 上部署 Threat Defense Virtual

使用 Oracle Cloud 市场中的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品通过计算实例在 OCI 上部署 threat defense virtual。根据 CPU 数量、内存量和网络资源等特征来选择最合适的计算机形状。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**市场 (Marketplace)** > **应用程序 (Applications)**。

步骤 3 在市场中搜索“Cisco Firepower NGFW virtual firewall (NGFWv)”，然后选择产品。

步骤 4 查看条款和条件，然后选中**我已阅读并接受的Oracle使用条款和合作伙伴条款和条件 (I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions)** 复选框。

步骤 5 点击**启动实例 (Launch Instance)**。

步骤 6 输入您的实例的描述性**名称**，例如 *FTDv-6-7*。

步骤 7 点击**更改形状 (Change Shape)**，然后选择包含 threat defense virtual 所需 CPU 数量、RAM 量和所需接口数量的形状，例如 VM.Standard2.4（请参阅概述，第 266 页）。

步骤 8 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择管理 VCN。

步骤 9 从**子网 (Subnet)** 下拉列表中选择管理子网（如果未自动填充）。

步骤 10 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为管理 VCN 配置的安全组。

步骤 11 点击**分配公共 IP 地址 (Assign a Public Ip Address)** 单选按钮。

步骤 12 在**添加 SSH 密钥 (Add SSH keys)** 下，点击**粘贴公共密钥 (Paste Public Keys)** 单选按钮并粘贴 SSH 密钥。

基于 Linux 的实例使用 SSH 密钥对而不是密码来对远程用户进行身份验证。密钥对包括私钥和公共密钥。您可以在创建实例时将私钥保留在计算机上并提供公共密钥。有关准则，请参阅管理 Linux 实例上的密钥对。

步骤 13 点击**显示高级选项 (Show Advanced Options)** 链接以展开选项。

步骤 14 在**初始化脚本 (Initialization Script)** 下，点击**粘贴云初始化脚本 (Paste Cloud-Init Script)** 单选按钮来为 threat defense virtual 提供 day0 配置。day0 配置会在首次引导 threat defense virtual 期间应用。

以下示例显示您可以在**云初始化脚本 (Cloud-Init Script)** 字段中复制和粘贴的示例 day0 配置：

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"IPv6Mode": "dhcp",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "cisco123reg",
"FmcNatId": "cisco123nat"
}
```

- **FmcRegKey** - 这是一次性使用的注册密钥，用于将设备注册到 管理中心。该注册密钥是任何用户定义的字母数字值，最长 37 个字符。
- **FmcNatId** - 这是一个唯一的一次性字符串（用户定义）。如果设备和 管理中心 之间被 NAT 设备分开，则必须输入唯一的 NAT ID 和唯一的注册密钥。

步骤 15 点击**创建 (Create)**。

下一步做什么

监控 threat defense virtual 实例，点击**创建 (Create)** 按钮后，状态会显示为“正在调配”(Provisioning)。

重要事项 监控状态非常重要。一旦 threat defense virtual实例从调配变为运行状态，您需要在 threat defense virtual 启动完成之前根据需要连接 VNIC。

连接接口

threat defense virtual会进入运行状态并连接一个 VNIC（请参阅**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）。这称为主 VNIC，并会映射到管理 VCN。在 threat defense virtual 完成首次启动之前，您需要为之前创建的其他 VCN 子网（诊断、内部、外部）连接 VNIC，以便在 threat defense virtual 上正确检测 VNIC。

过程

步骤 1 选择新启动的 threat defense virtual实例。

步骤 2 依次选择**连接的 VNIC (Attached VNICs)** > **创建 VNIC (Create VNIC)**。

步骤 3 输入 VNIC 的描述性**名称 (Name)**，例如 *Inside*。

步骤 4 从**虚拟云网络 (Virtual Cloud Network)** 下拉列表中选择 VCN。

步骤 5 从**子网 (Subnet)** 下拉列表选择您的子网。

步骤 6 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)**，然后选择为所选 VCN 配置的安全组。

步骤 7 选中**跳过源目标 选中**使用网络安全组控制流量 (Use Network Security Groups to Control Traffic)。

步骤 8 （可选）指定**专用 IP 地址**。仅当您要为 VNIC 选择特定 IP 时，才需要执行此操作。

如果未指定 IP，OCI 将从您分配给子网的 CIDR 块分配 IP 地址。

步骤 9 点击**保存更改 (Save Changes)** 以创建 VNIC。

步骤 10 对部署所需的每个 VNIC 重复此程序。

为连接的 VNIC 添加路由规则

将路由表规则添加到诊断、内部和外部路由表。

过程

步骤 1 依次选择**网络 (Networking)** > **虚拟云网络 (Virtual Cloud Networks)**，然后点击与 VCN 关联的默认路由表（内部或外部）。

步骤 2 点击**添加路由规则 (Add Route Rules)**。

步骤 3 从**目标类型 (Target Type)** 下拉列表中，选择**专用 IP (Private IP)**。

步骤 4 从**目的类型 (Destination Type)** 下拉列表中选择**CIDR 块 (CIDR Block)**。

步骤 5 输入**目标 CIDR 块**，例如 0.0.0.0/0。

步骤 6 在**目标选择 (Target Selection)** 字段中输入 VNIC 的私有 IP 地址。

如果未向 VNIC 明确分配 IP 地址，则可以从 VNIC 详细信息（**计算 (Compute)** > **实例 (Instances)** > **实例详细信息 (Instance Details)** > **连接的 VNIC (Attached VNICs)**）中查找自动分配的 IP 地址。

步骤 7 点击**添加路由规则 (Add Route Rules)**。

如果要通过互联网网关配置 IPv6 互联网访问，请执行以下操作：

a) 从**目标类型 (Target Type)** 下拉列表中，选择**互联网网关 (Internet Gateway)**。
b) 在**目标 CIDR 块**中，指定 IP 地址
c) 从**目标互联网网关 (Target Internet Gateway)** 下拉列表中，选择现有互联网网关隔间或创建新的互联网网关隔间。

步骤 8 对部署所需的每个 VNIC 重复此程序。

注释
如果使用通过 DHCP 的路由规则或 IPv6 地址前缀配置的 IPv6 地址为 /128，则必须在 threat defense virtual 路由表中添加以下路由。

ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

示例：

- `ipv6 route inside 2603:c020:5:5800::/64 fe80::200:17ff:fe96:921b`
- `ipv6 route outside 2603:c020:6:ba00::/64 fe80::200:17ff:fe21:748c`

部署 Auto Scale 解决方案

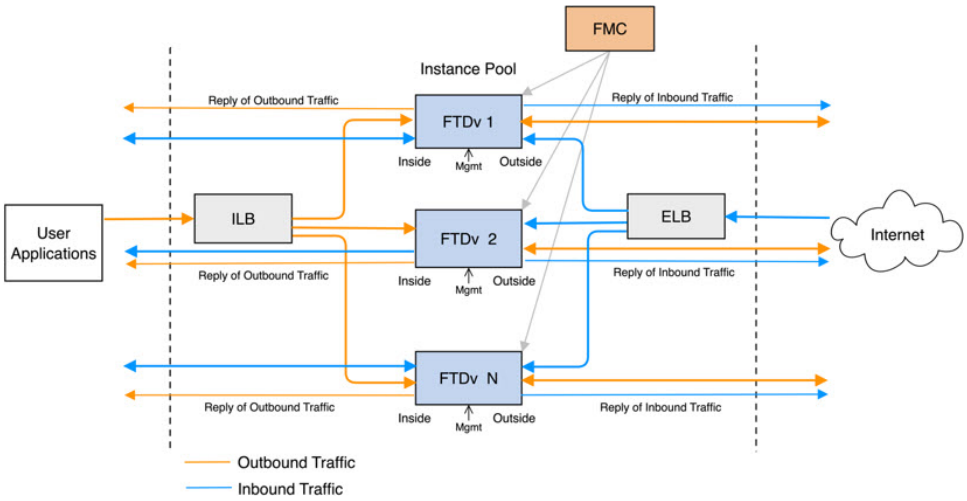
以下各节介绍 Auto Scale 解决方案的组件如何对 OCI 上的 threat defense virtual 发挥作用。

Auto Scale 使用案例

OCI 上 threat defense virtual 自动扩展解决方案的使用案例如下图所示。面向互联网的负载均衡器将有一个使用侦听程序和目标组的组合启用的端口的公共 IP 地址。

可以通过 NAT 规则对流量进行基于端口的分叉。下文将对此进行解释。

图 *41: Cisco Secure Firewall Threat Defense Virtual Auto Scale* 使用案例图



适用范围

本文档介绍了部署适用于 OCI 的 threat defense virtual Auto Scale 解决方案的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

前提条件

权限和策略

以下是实施解决方案所需的 OCI 权限和策略：

1. **用户和组**

注释 您必须是 OCI 用户或租户管理员才能创建用户和组。

创建 Oracle 云基础设施用户账户和用户账户所属的组。如果存在具有用户账户的相关组，则无需再进行创建。有关创建用户和组的说明，请参阅创建组和用户。

2. **组策略**

您需要创建策略，然后将其映射到组。要创建策略，请转至 **OCI** > **身份和安全 (Identity & Security)** > **策略 (Policies)** > **创建策略 (Create Policy)**。创建以下策略并将其添加到所需的组中：

- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 管理隔离专区 <*Compartment_Name*> 中的警报
- 允许组 <*Group_Name*> 管理隔离专区 <*Compartment_Name*> 中的主题
- 允许组 <*Group_Name*> 检查隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 读取隔离专区 <*Compartment_Name*> 中的指标
- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的标记命名空间
- 允许组 <*Group_Name*> 读取隔离专区 <*Compartment_Name*> 中的日志组
- 允许组 <*Group_Name*> 使用隔离专区 <*Compartment_Name*> 中的实例池
- 允许组 <*Group_Name*> 使用租户中的 Cloud Shell
- 允许组 <*Group_Name*> 读取租户中的对象存储命名空间
- 允许组 <*Group_Name*> 管理租户中的存储库

注释 您也可以在租户级别创建策略。您可以自行决定如何提供所有的权限。

3. **Oracle 功能的权限**

   要让 Oracle 功能能够访问另一个 Oracle 云基础设施资源，请将该功能包含在动态组中，然后创建一个策略以授予该动态组对该资源的访问权限。

4. **创建动态组**

   要创建动态组，请转至 **OCI** > **身份和安全 (Identity & Security)** > **动态组 (Dynamic Group)** > **创建动态组 (Create Dynamic Group)**

   在创建动态组时指定以下规则：

   ```
   ALL {resource.type = 'fnfunc', resource.compartment.id = '<Your_Compartment_OCID>'}
   ```

   有关动态组的更多详细信息，请参阅：

   - https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm
   - https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

5. **为动态组创建策略**

   要添加策略，请转至 **OCI** > **身份和安全 (Identity & Security)** > **策略 (Policies)** > **创建策略 (Create Policy)**。将以下策略添加到组：

   ```
   允许动态组 <Dynamic_Group_Name> 管理隔离专区 <Compartment_OCID> 中的所有资源
   ```

从 GitHub 下载文件

FTDv – OCI Autoscale 解决方案已作为 GitHub 存储库提供。您可以从存储库中提取或下载文件。

Python3 环境

可以在克隆存储库中找到 *make.py* 文件。此程序会将 Oracle 功能和模板文件压缩为 Zip 文件；将它们复制到目标文件夹。为了执行这些任务，应配置 Python 3 环境。

注释 此 Python 脚本只能用于 Linux 环境中。

基础设施配置

必须配置以下选项：

1. **VCN**

   根据 FTDv 应用的需要创建 VCN。创建具有互联网网关的 VCN，该网关至少有一个通过到互联网的路由连接的子网。

有关创建 VCN 的信息，请参阅https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm。

2. **应用程序子网**

   根据需要为 FTDv 应用创建子网。要根据此使用案例实施解决方案，FTDv 实例需要 4 个子网才能运行。

   有关创建子网的信息，请参阅 https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm#。

3. **外部子网**

   子网应该具有能够通过“0.0.0.0/0”连接互联网网关的路由。此子网包含思科 FTDv 的外部接口和面向互联网的负载均衡器。确保为出站流量添加 NAT 网关。

   有关详情，请参阅以下文档：

   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm
   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. **内部子网**

   这与具有或没有 NAT/互联网网关的应用程序子网类似。

注释 对于 FTDv 运行状况探测，您可以通过端口 80 来访问元数据服务器 (169.254.169.254)。

5. **管理子网**

   管理子网应是公共子网，这样它才能支持对 FTDv 的 SSH 可访问性。

6. **Function 子网**

   此子网用于 Oracle Functions 部署。

注释 此子网必须具有到 NAT GW（而不是互联网 GW）的 `0.0.0.0/0` 路由。

必须在 Management Center Virtual 和 Threat Defense Virtual的 NSG（网络安全组）中允许此子网的 NAT GW 的公共 IP。

7. **安全组 - FTDv 实例的网络安全组**

   为 FTDv 实例配置安全组，以允许 Oracle 功能（在同一 VCN 中）执行到 FTDv 的管理地址的 SSH 连接。

8. **对象存储命名空间**

此对象存储命名空间用于托管静态网站，包含 configuration.txt 文件。您必须为 configuration.txt 文件创建预身份验证请求。此预身份验证 URL 可在模板部署期间使用。

注释 确保 FTDv 实例可通过 HTTP URL 访问已上传的以下配置。

当 FTDv 启动时，它会执行以下命令 `$ copy /noconfirm <configuration.txt file's pre-authenticated request URL > disk0:Connfiguration.txt`

此命令支持要使用 configuration.txt 文件配置的 FTDv 启动。

Cisco Secure Firewall Management Center必备条件

您可以使用 Cisco Secure Firewall Management Center 来管理 threat defense virtual，这是一个功能齐全的多设备管理器。threat defense virtual 向您分配给 threat defense virtual 虚拟机的管理接口上的 FMC 注册并与之通信。

创建 threat defense virtual 配置和管理所需的对象，包括在多台设备上部署策略和安装更新的设备组。设备组上应用的所有配置都将被推送到 threat defense virtual 实例。

以下各节简要概述准备 管理中心 的基本步骤。有关程序的完整信息，请参阅《*Cisco Secure Firewall Management Center* 配置指南》。准备 管理中心 时，请确保记录以下信息：

- Cisco Secure Firewall Management Center 公用 IP 地址
- 用户名和密码（如果启用了基于内存的扩展，则必须提供 2 个用户凭证）
- 安全区名称
- Cisco Secure Firewall Management Center 访问策略名称
- Cisco Secure Firewall Management Center NAT 策略名称
- 设备组名称

在 Cisco Secure Firewall Management Center 中创建用户

在 Cisco Secure Firewall Management Center 中创建具有 Admin 权限的新用户，以便仅供 Autoscale Manager 使用。

注释 您必须有一个专用于 threat defense virtual Autoscale 解决方案的 Cisco Secure Firewall Management Center 用户账户，以防止与其他 FMC 会话发生冲突。

过程

在 Cisco Secure Firewall Management Center 中创建具有 Admin 权限的新用户。选择**系统 (System)** > **用户 (Users)**，然后点击**创建用户 (Create User)**。用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)
- 全部小写
- 不应以连字符 (-) 开头；必须包含字母；不应包含句点 (.)、符号 (@) 或斜线 (/)

根据环境需要完成用户选项。有关完整信息，请参阅 《*Cisco Secure Firewall Management Center* 配置指南》。

创建设备组

可以使用设备组轻松分配策略，并在多台设备上安装更新。应创建一个设备组，然后应对其应用规则。设备组上应用的所有配置都将被推送到 threat defense virtual 实例。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 从**添加 (Add)** 下拉菜单中选择**添加组 (Add Group)**。

步骤 3 输入设备组名称。

步骤 4 点击**确定 (Ok)** 以创建设备组。

创建网络和主机对象

创建以下要用于 threat defense virtual 配置的对象。

过程

步骤 1 创建名为 *oci-metadata-server* 且 IP 为 *169.254.169.254* 的主机。

步骤 2 创建名为 health-check-port 且值为 8080 的端口，或根据需要创建任何其他端口。

步骤 3 创建内部接口，依次选择**接口 (Interface)** > **安全区域 (Security Zone)**。选择**已路由 (Routed)** 作为类型。为接口提供名称，例如 *inside-sz*。

步骤 4 创建外部接口，依次选择**接口 (Interface)** > **安全区域 (Security Zone)**。选择**已路由 (Routed)** 作为类型。为接口提供名称，例如 *outside-sz*。

创建 NAT 策略

创建 NAT 策略并创建必要的 NAT 规则，以便将流量从外部接口转发到应用程序，然后将此策略连接到您为 Auto Scale 创建的设备组。

过程

步骤 1 选择**设备 (Devices)** > **NAT**

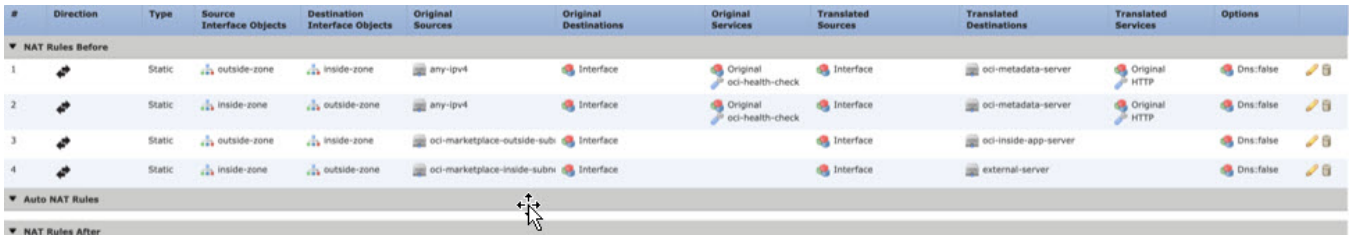
步骤 2 从**新策略**下拉列表中，选择**威胁防御 NAT**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

步骤 4 输入**说明 (Description)**（可选）。

步骤 5 配置 NAT 规则。有关如何创建 NAT 规则和应用 NAT 策略的指南，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的为威胁防御配置 NAT。下图显示了设置规则的基本方法。

图 *42: NAT* 规则



步骤 6 点击**保存 (Save)**。

创建 NAT 规则

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (PAT)。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的为威胁防御配置 NAT。

配置 NAT 策略中所需的以下 2 条强制性规则：

过程

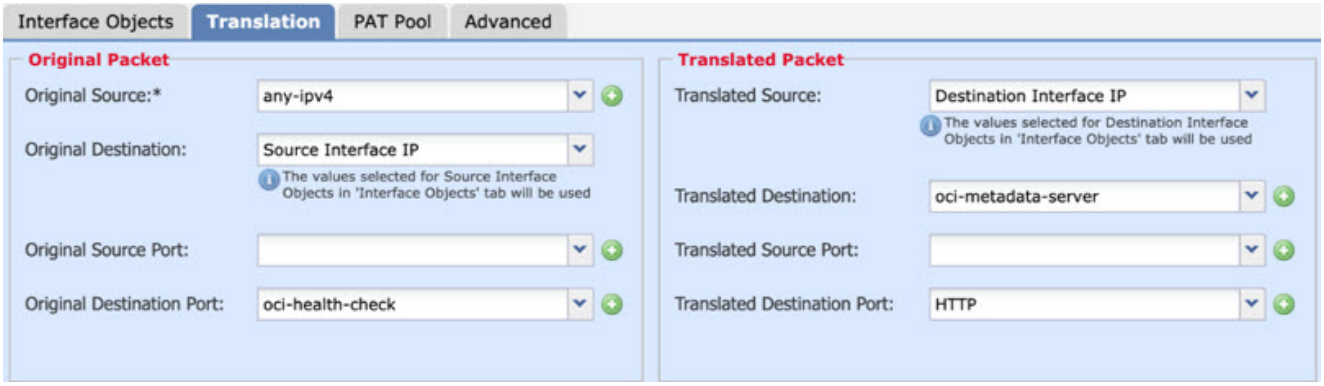
步骤 1 为入站运行状况检查配置以下 NAT 规则：

- 源区域：外部区域
- 目标区域：内部区域
- 原始源：any-ipv4
- 原始目标：源接口 IP

- 原始源端口：默认
- 原始目标端口：health-check-port
- 已转换的源：目标接口 IP
- 已转换的目标：oci-metadata-server
- 已转换的源端口：默认
- 已转换的目标端口：HTTP

下图显示了用于入站运行状况检查的 NAT 规则。

图 *43:* 入站运行状况 *NAT* 规则

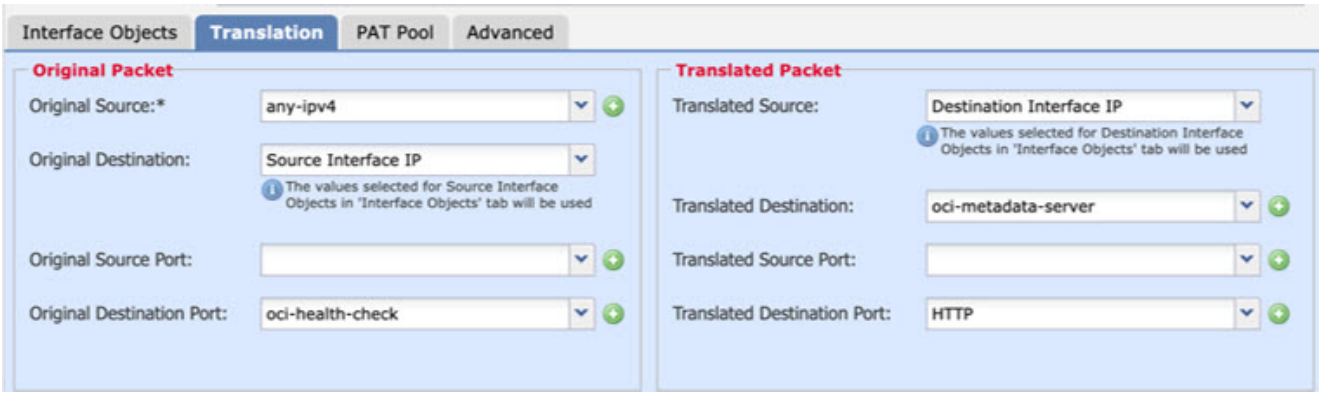


步骤 2 为出站运行状况检查配置以下 NAT 规则。

- 源区域：内部区域
- 目标区域：外部区域
- 原始源：any-ipv4
- 原始目标：源接口 IP
- 原始源端口：默认
- 原始目标端口：health-check-port
- 已转换的源：目标接口 IP
- 已转换的目标：oci-metadata-server
- 已转换的源端口：默认
- 已转换的目标端口：HTTP

下图显示了用于出站运行状况检查的 NAT 规则。

图 *44:* 出站运行状况检查 *NAT* 规则



同样，也可以为数据流量添加任何 NAT 规则，并将其推送到 threat defense virtual 设备上。

创建访问策略

配置访问控制以允许从内部到外部的流量。可以创建具有所有必需策略的访问策略，应允许运行状况端口对象，以便允许此端口上的流量到达设备。在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。规则的正确配置和排序对构建有效的部署至关重要。请参阅《Cisco Secure Firewall Management Center 设备配置指南》 的访问控制规则最佳实践。

使用**策略分配**将设备组（作为前提条件创建）分配给访问策略。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**新建策略**。

步骤 3 在名称 (Name) 和说明 (Description)（可选）中输入唯一名称和说明。

步骤 4 为部署配置安全设置和规则。有关详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的访问控制。

加密密码

注释 有关此程序的详细信息，请参阅创建保管库和密钥。

FTDv 的密码用于配置自动扩展时使用的所有 FTDv 实例，并且它还用于为多个配置目的创建 Rest API 调用连接。

因此，您需要不时地保存和处理密码。由于密码更改频繁且存在漏洞，因此不允许以纯文本格式编辑或保存密码。密码只能采用加密格式。

要以加密形式获取密码，请执行以下操作：

过程

步骤 1 创建保险库。

OCI 保险库提供安全创建和保存主加密密钥的服务，以及使用它们进行加密和解密的方法。因此，应在与 Autoscale 解决方案的其余部分相同的隔离专区中创建保险柜（如果尚未创建）。

转至 **OCI > 身份和安全 (Identity & Security) > 保管库 (Vault) > 选择或创建新保管库 (Choose or Create New Vault)**

。

步骤 2 创建主加密密钥。

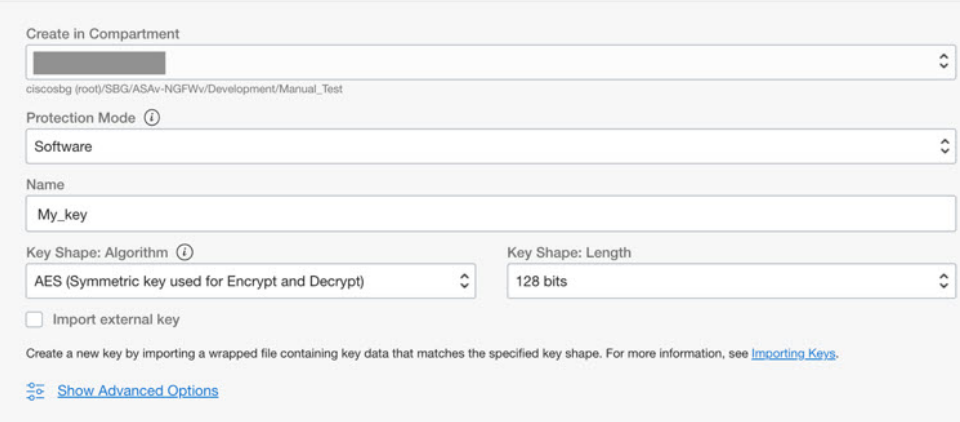
需要使用主加密密钥才能加密纯文本密码。

转至 **OCI > 身份和安全 (Identity & Security) > 保管库 (Vault) > 选择或创建密钥 (Choose or Create Key)**

从任意给定算法中选择任意长度的密钥。

1. AES - 128、192、256
2. RSA - 2048、3072、4096
3. ECDSA - 256、384、521

图 *45:* 创建密钥



步骤 3 创建加密密码。。

1. 转至 **OCI > 打开 CloudShell（OCI 云终端）(Open CloudShell [OCI Cloud Terminal])**
2. 通过替换 <*Password*> 作为密码来执行以下命令。

```
echo -n '<Password>' | base64
```

3. 从选定的保险库中，复制加密终端和主加密密钥 OCID。替换以下值，然后执行 encrypt 命令：
   - 将 KEY_OCID 替换为您的密钥的 OCID
   - 将 Cryptographic_Endpoint_URL 替换为您的保险库的加密终端 URL
   - 将密码替换为您的密码

   加密命令

   ```
   oci kms crypto encrypt --key-id Key_OCID --endpoint
   Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
   ```

4. 从上述命令的输出中复制密文，然后根据需要使用它们。

准备 threat defense virtual 配置文件

应用程序可能已部署或其部署计划可用。

过程

步骤 1 在部署之前收集以下输入参数：

参数	数据类型	说明
tenancy_ocid	字符串	您的账户所属的租户的 OCID。要了解如何查找租户 OCID，请参阅此处。 租户 OCID 如下所示 - `ocid1.tenancy.oc1..<unique_ID>`
region	字符串	要在其中创建资源的区域的唯一标识符。 示例 - us-phoenix-1、us-ashburn-1
lb_size	字符串	用于确定外部和内部负载均衡器的总预调配带宽（入口加出口）的模板。 支持的值：100Mbps、10Mbps、10Mbps-Micro、400Mbps、8000Mbps 示例：100Mbps
availability_domain	字符串	示例 - Tpeb:PHX-AD-1、Tpeb:PHX-AD-2 **注释** 要获取可用性域名，请参阅此处。

参数	数据类型	说明
min_and_max_instance_count	逗号分隔值	您希望在实例池中保留的最小和最大实例数。 示例：1,5
autoscale_group_prefix	字符串	用于对通过使用模板创建的所有资源命名的前缀。例如，如果资源前缀为“autoscale”，则所有资源均按会如下方式命名 - autoscale_resource1、autoscale_resource2 等。
mgmt_subnet_ocid	字符串	要使用的管理子网的 OCID。
inside_subnet_ocid	字符串	要使用的内部子网的 OCID。
function_subnet_ocid	字符串	要使用的 Function 子网的 OCID。
outside_subnet_ocid	字符串	要使用的外部子网的 OCID。
mgmt_nsg_ocid	字符串	要使用的管理子网网络安全组的 OCID。
inside_nsg_ocid	字符串	要使用的内部子网网络安全组的 OCID。
outside_nsg_ocid	字符串	要使用的外部子网网络安全组的 OCID。
elb_listener_port	逗号分隔值	外部负载均衡器侦听程序的通信端口列表。 示例： 80
ilb_listener_port	逗号分隔值	内部负载均衡器侦听程序的通信端口列表。 示例： 80
health_check_port	字符串	运行运行状况检查的负载均衡器的后端服务器端口。 示例：8080
instance_shape	字符串	要创建的实例的形状。形状可确定分配给实例的CPU数量、内存量和其他资源。 支持的形状：“VM.Standard2.4”和“VM.Standard2.8”
lb_bs_policy	字符串	用于内部和外部负载均衡器后端的负载均衡器策略。要了解有关负载均衡器策略工作原理的更多信息，请参阅此处 支持的值：“ROUND_ROBIN”、“LEAST_CONNECTIONS”、“IP_HASH”

参数	数据类型	说明
image_name	字符串	用于创建实例配置的市场映像的名称。 默认值：“Cisco Firepower NGFW virtual firewall (NGFWv)” 注释 如果用户想要部署自定义映像，则用户必须配置 custom_image_ocid 参数。
scaling_thresholds	逗号分隔值	用于内向扩展和外向扩展的 CPU 使用率阈值。以逗号分隔输入的形式提供内向扩展和外向扩展阈值。 示例：15,50 其中，15 是内向扩展阈值，50 是外向扩展阈值。
compartment_id	字符串	要在其中创建资源的隔离专区的 OCID。 示例：**ocid1.compartment.oc1..<unique_ID>**
compartment_name	字符串	隔离专区的名称
custom_image_ocid	字符串	如果未使用市场映像，用于创建实例配置的自定义映像的 OCID。 注释 *custom_image_ocid* 是可选参数
ftdv_password	字符串	threat defense virtual 采用加密形式的密码，用于通过 SSH 连接到 threat defense virtual 配置。有关如何加密密码的说明，请参阅配置指南，或参阅此处。
ftdv_license_type	字符串	threat defense virtual 许可证的类型，可以是 BYOL 或 PAYG。目前支持 BYOL。
cryptographic_endpoint	字符串	加密终端是用于解密密码的URL。它可以在保险库中找到。
master_encryption_key_id	字符串	用于加密密码的密钥的 OCID。它可以在保险库中找到。 注释 master_encryption_key_id 和 cryptographic_endpoint 必须属于同一保险库。

参数	数据类型	说明
fmc_ip	字符串	Cisco Secure Firewall Management Center 的 IP 地址。客户用来管理 threat defense virtual 实例的 管理中心 IP。 **注释** 只有当与 *threat defense virtual* 位于同一子网时，管理中心 *IP* 才为专用，否则必须将公共 *IP* 用于所有其他情况。
fmc_username	字符串	管理中心 账户的用户名。每次新的 threat defense virtual 实例出现时，此用户名将用于登录 管理中心 进行配置。
fmc_password	字符串	加密形式的 管理中心 密码。有关如何加密密码的程序，请参阅此处。
fmc_device_group_name	字符串	管理中心 中必须有一个设备组，此 Autoscale 解决方案的所有 threat defense virtual 部分都会被添加到该组中，以便可以将相同的策略和配置应用于所有这些设备。
enable_memory_based_scaling	bool	从 Cisco Secure Firewall Management Center Virtual 发布 threat defense virtual 内存使用情况。通过启用此标志，也可以根据内存利用率进行扩展。默认使用 CPU 利用率。
fmc_metrics_username	字符串	如果您通过启用标志 enable_memory_based_scaling 来选择内存利用率，则需要一个额外的 管理中心 用户账户，因为该账户将持续用于从所有正在运行 threat defense virtual 实例提取内存使用情况。
fmc_metrics_password	字符串	加密形式的额外 管理中心 账户的密码。有关如何加密密码的程序，请参阅此处。
配置文件名称 (Profile Name)		它是 OCI 中的用户配置文件名称。它可以在用户的配置文件部分下找到。示例：“oracleidentitycloudservice/<user> @<mail> .com”
对象存储命名空间		它是在创建租户时创建的唯一标识符。转至 **OCI** > **管理 (Administration)** > **租户详细信息 (Tenancy Details)**
授权令牌		这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。转至 **OCI** > **身份 (Identity)** > **用户 (Users)** > **用户详细信息 (User Details)** > **身份验证令牌 (Auth Tokens)** > **生成令牌 (Generate Token)**。

步骤 2 使用以下内容来创建 *Configuration.json* 文件：

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv30",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "<autoscale-access-policy-name>",
  "fmcNatPolicyName": "<autoscale-nat-policy-name>",
  "fmcInsideNicName": "inside",
  "fmcOutsideNicName": "outside",
  "fmcInsideNic": "GigabitEthernet0/0",
  "fmcOutsideNic": "GigabitEthernet0/1",
  "fmcOutsideZone": "<outside-zone-name>",
  "fmcInsideZone": "<inside-zone-name>",
  "MetadataServerObjectName": "oci-metadata-server",
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "inside-zone"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "outside-zone"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
    }
  ],
  "trafficRoutes": [
    {
      "interface": "outside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "2"
    },
    {
      "interface": "inside",
      "network": "oci-metadata-server",
      "gateway": "",
      "metric": "1"
    }
  ]
}
```

步骤 3 使用配置设置来更新 *Configuration.json*。

步骤 4 将配置文件上传到对象存储空间。

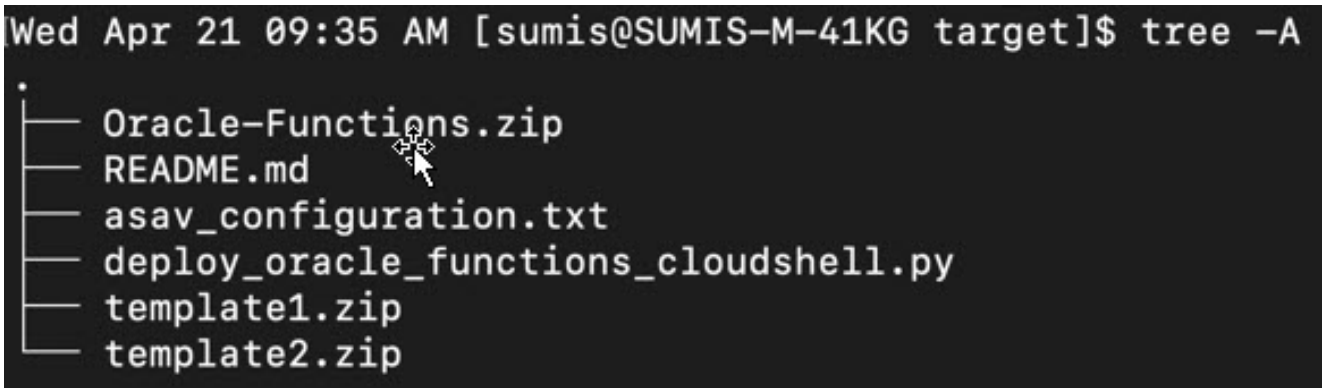
必须将 *configuration.txt* 文件上传到用户创建的对象存储空间，并为上传的文件创建预身份验证请求。

注释
确保在堆栈部署中使用 configuration.txt 的预身份验证请求 URL。

注释
在 OCI 中创建预身份验证 URL 时需要定义到期时间，请确保该时间段足够长，不会在解决方案执行期间到期。

步骤 5 创建 Zip 文件。

可以在克隆存储库中找到 *make.py* 文件。执行 `python3 make.py build` 命令以创建 zip 文件。目标文件夹包含以下文件。



部署 Auto Scale 解决方案

在完成部署的必备步骤后，开始创建 OCI 堆栈。您可以使用 Cloud Shell 执行手动部署或使用 Cloud Shell 部署。您的版本的部署脚本和模板可从 GitHub 存储库获取。

手动部署

端到端 Autoscale 解决方案部署包括三个步骤：部署 Terraform Template-1 堆栈 、部署 Oracle 功能，然后部署 Terraform Template-2。

部署 Terraform Template-1 堆栈

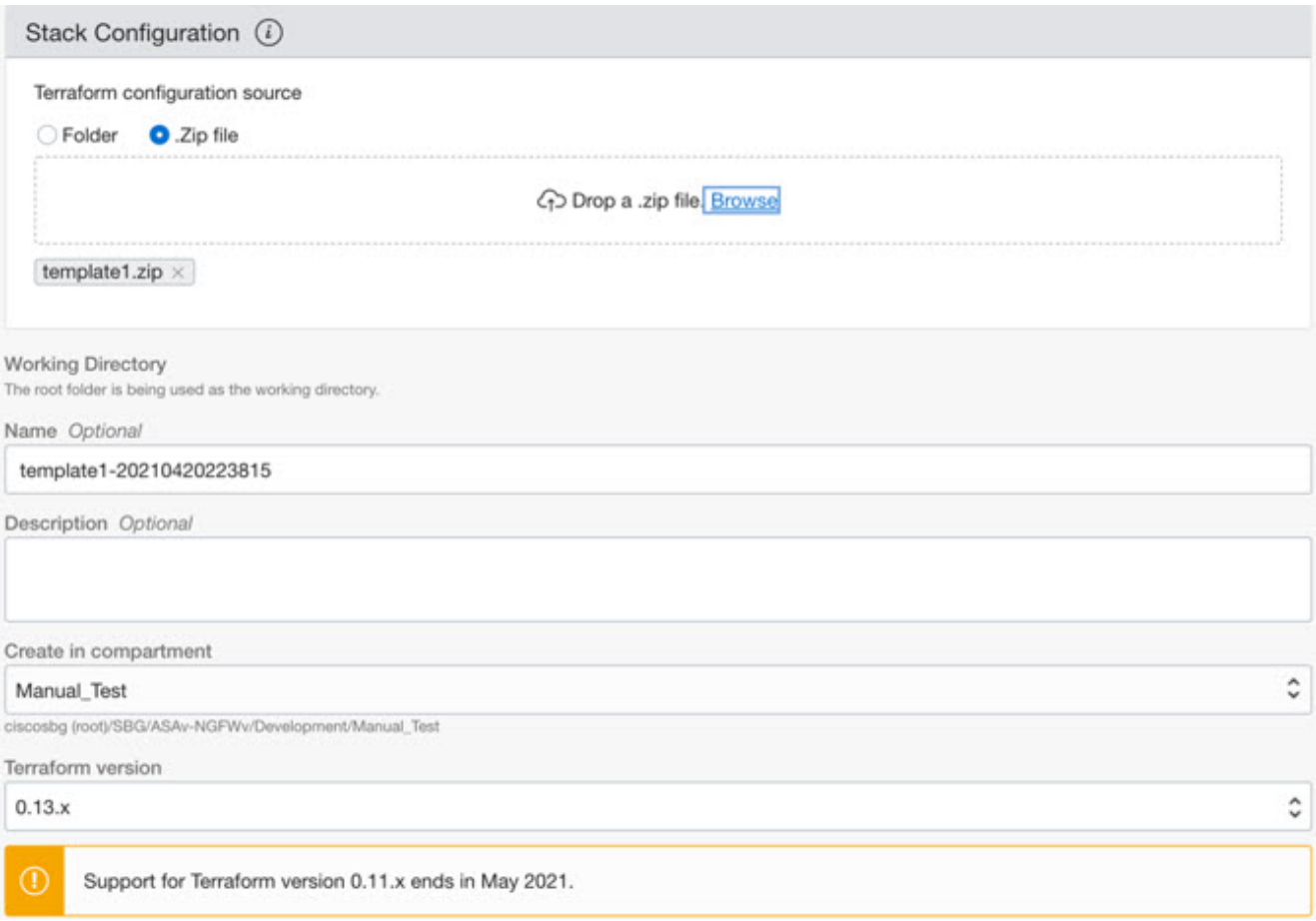
过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Service)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)** > **创建堆栈 (Create Stack)**

选择**我的配置 (My Configuration)**，然后选择目标文件夹中的 *Terraform template1.zip* 文件作为 Terraform 配置源，如下图所示。



步骤 3 在**转换版本 (Transform version)** 下拉列表中，选择 0.13.x 或 0.14.x。

步骤 4 在下一步中，输入步骤 1 中收集的所有详细信息。

注释
输入有效的输入参数，否则堆栈部署可能会在后续步骤中失败。

步骤 5 在下一步中，选择 **Terraform 操作 (Terraform Actions)** > **应用 (Apply)**。

成功部署后，继续部署 Oracle 功能。

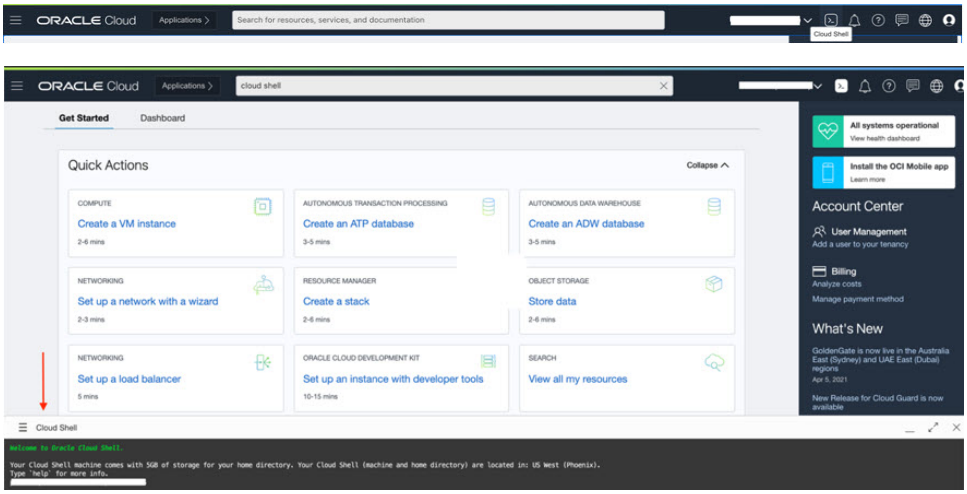
部署 Oracle 功能

注释 只有在 *Terraform Template-1* 部署成功后才能执行此步骤。

在 OCI 中，Oracle 功能会作为 Docker 映像上传，并会保存到 OCI 容器注册表中。在部署时，需要将 Oracle 功能推送到其中一个 OCI 应用（在 Terraform Template-1 中创建）中。

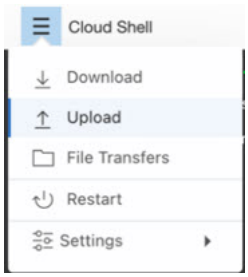
过程

步骤 1 打开 OCI Cloud Shell。

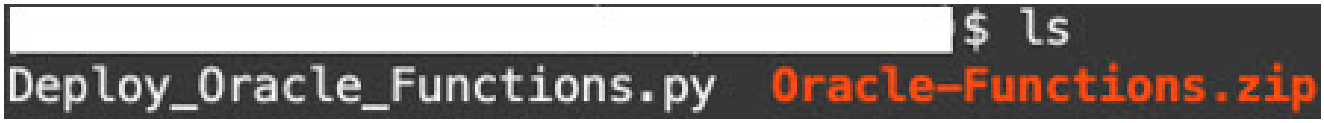


步骤 2 上传 *deploy_oracle_functions_cloudshell.py* 和 *Oracle-Functions.zip*。

从 Cloud Shell 的汉堡菜单中，选择**上传 (Upload)**。



步骤 3 使用 **ls** 命令来验证文件。



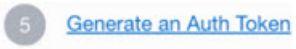
步骤 4 运行 `python3 Deploy_Oracle_Functions.py -h`。`deploy_oracle_functions_cloudshell.py` 脚本需要一些输入参数，可使用 help 参数找到其详细信息，如下图所示。

```
                                $ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a  -r  -p  -c  -o  -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
  -h, --help  show this help message and exit
  -a          Name of Application in OCI to which functions will be deployed
  -r          Region Identifier
  -p          Profile Name of User
  -c          Compartment OCID
  -o          Object Storage Namespace
  -t          Authorization Token for Docker Login (*Please Put in Quotes)
```

要运行脚本，请传递以下参数：

表 *25:* 参数和详细信息

参数	详细说明
应用名称	它是 Terraform Template-1 部署创建的 OCI 应用的名称。通过将 Template-1 中给出的“**autoscale_group_prefix**”和后缀“**_application**”组合在一起即可获得其值。
区域标识符	区域标识符是在不同区域的 OCI 中固定的区域代码字。 示例：表示凤凰城的“us-phoenix-1”或表示墨尔本的“ap-melbourne-1”。 要获取所有区域及其区域标识符的列表，请转至 **OCI** > **管理 (Administration)** > **区域管理 (Region Management)**。
配置文件名称	它是 OCI 中的简单用户配置文件名称。 示例：*oracleidentitycloudservice/<user>@<mail>.com* 该名称可以在用户的配置文件部分下找到。
隔离专区 **OCID**	它是隔离专区的 OCID（Oracle 云标识符）。用户拥有 OCI 应用的隔离专区 OCID。 转至 **OCI** > **身份 (Identity)** > **隔离专区 (Compartment)** > **隔离专区详细信息 (Compartment Details)**。
对象存储命名空间	它是在创建租户时创建的唯一标识符。 转至 **OCI** > **管理 (Administration)** > **租户详细信息 (Tenancy Details)**。

参数	详细说明
授权令牌	这用作 Docker 登录的密码，授权其将 Oracle-Functions 推送到 OCI 容器注册表中。在部署脚本中用引号指定令牌。 转至 **OCI** > **身份 (Identity)** > **用户 (Users)** > **用户详细信息 (User Details)** > **身份验证令牌 (Auth Tokens)** > **生成令牌 (Generate Token)**。 出于某种原因，如果您无法查看用户详细信息，请点击**开发人员服务 (Developer services)** > **功能 (Functions)**。转至 Terraform Template-1 创建的应用。点击**开始 (Getting Started)**，然后选择 Cloud Shell 设置，在这些步骤中，您将找到生成身份验证令牌的链接，如下所示。 

步骤 5 通过传递有效的输入参数运行 `python3 Deploy_Oracle_Functions.py` 命令。部署所有的功能需要一些时间。然后，您可以删除该文件并关闭 Cloud Shell。

部署 Terraform Template-2

模板 2 部署与警报创建相关的资源，包括警报、用于调用函数的 ONS 主题。模板 2 的部署与 Terraform Template-1 的部署类似。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Service)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)** > **创建堆栈 (Create Stack)**.

选择目标文件夹中的 *Terraform template template2.zip* 作为 Terraform 配置的源。

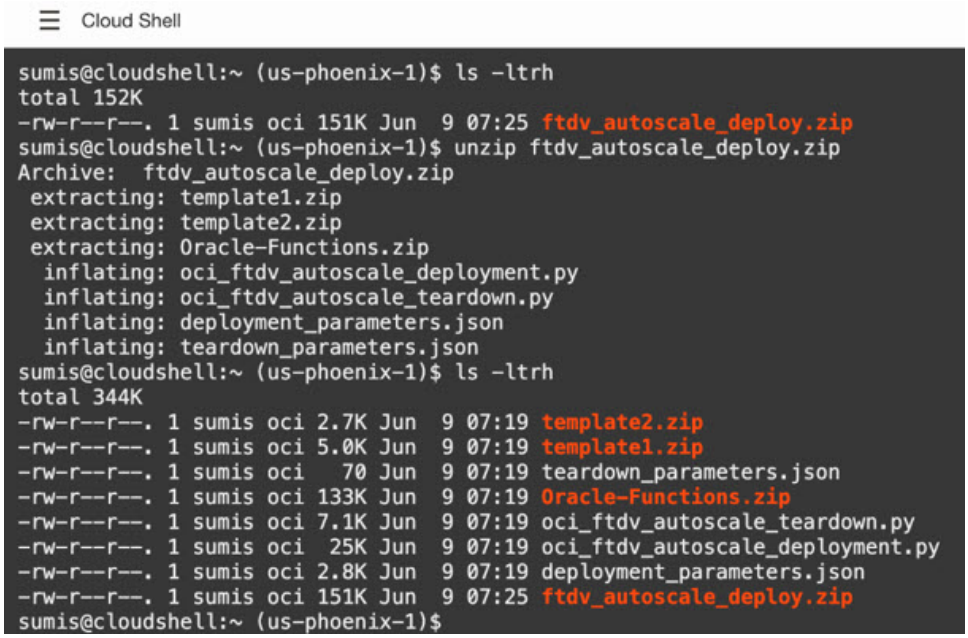
步骤 3 在下一步中，点击**Terraform 操作 (Terraform Actions)** > **应用 (Apply)**。

使用 Cloud Shell 部署

为避免部署开销，您可以通过调用简单的端到端部署脚本来部署 AutoScale 解决方案（Terraform template1、template2 和 oracle 功能）。

过程

步骤 1 将目标文件夹中的 *ftdv_autoscale_deploy.zip* 文件上传到 Cloud Shell 并解压缩文件。



步骤 2 在执行 *python3 make.py* 构建命令之前，请确保您已更新 `deployment_parameters.json` 中的输入参数。

步骤 3 要启动 Autoscale 解决方案部署，请在 Cloud Shell 上运行 `python3 oci_ftdv_autoscale_deployment.py` 命令。

完成解决方案部署大约需要 10-15 分钟。

如果在解决方案部署过程中出现任何错误，则错误日志会被保存。

验证部署

验证是否已部署所有资源，并且 Oracle 功能是否已与警报和事件连接。默认情况下，实例池的最小和最大实例数为零。您可以使用所需的最小和最大数量在 OCI UI 中编辑实例池。这将触发新的 threat defense virtual 实例。

我们建议您仅启动一个实例并检查其工作流程，并验证其行为以确保符合预期。完成验证后，您可以部署 threat defense virtual 的实际要求。

注释 将 threat defense virtual 实例的最小数量指定为**受扩展保护 (Scale-In protected)**，以避免被 OCI 扩展策略删除。

升级

升级 Autoscale 堆栈

此版本不支持升级。应重新部署堆栈。

升级 Threat Defense Virtual VM

此版本不支持升级 threat defense virtual VM。应使用所需的 threat defense virtual 映像来重新部署堆栈。

实例池

1. 要更改实例池中的最小和最大实例数，请执行以下操作：

   点击**开发人员服务 (Developer Services)** > **功能 (Function)** > **应用名称 (Application Name)** > （**通过 Terraform Template-1 创建**） **配置 (Configuration)**。

   分别更改 min_instance_count 和 max_instance_count。

2. 删除/终止实例不等于内向扩展。如果实例池中的任何实例因外部操作而并非内向扩展操作而被删除/终止，则实例池会自动启动新实例进行恢复。

3. Max_instance _count 定义外向扩展操作的阈值限制，但可以通过 UI 更改实例池的实例计数来超过此限制。确保 UI 中的实例计数小于在 OCI 应用中设置的 max_instance_count。否则，请相应地增大阈值。

4. 直接从应用减少实例池中的实例计数不会执行以编程方式设置的清理操作。由于这些后端不会从两个负载均衡器中耗尽和删除，如果 threat defense virtual 有许可证，它将丢失。

5. 由于某些原因，如果 threat defense virtual 实例在一段时间内运行状况不佳、无响应且无法通过 SSH 访问，则实例会被强制从实例池中删除，任何许可证都可能丢失。

Oracle 功能

- Oracle 功能实际上就是 Docker 映像。这些映像会别保存到 OCI 容器注册表的根目录中。这些映像不应被删除，否则也会删除在 Autoscale 解决方案中使用的功能。
- 通过 Terraform Template-1 创建的 OCI 应用包含 Oracle 功能正常工作所需的关键环境变量。除非强制要求，否则不应更改这些环境变量的值和格式。所做的任何更改只会反映在新实例中。

负载均衡器后端集

在 OCI 中，仅支持使用配置为 threat defense virtual 中的管理接口的主接口来连接到实例池的负载均衡器。因此，内部接口会连接到内部负载均衡器的后端集；外部接口会连接到外部负载均衡器的后端集。这些 IP 不会自动添加到后端集或从后端集中删除。我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行任何外部操作、维护或故障排除时，可能会有需要手动完成此操作的情况。

根据要求，可以使用侦听程序和后端集在负载均衡器上打开更多端口。即将启用的实例 IP 会被自动添加到后端集中，但应手动添加现有实例 IP。

在负载均衡器中添加侦听程序

要在负载均衡器中添加某个端口作为侦听程序，请转至 **OCI** > **网络 (Networking)** > **负载均衡器 (Load Balancer)** > **侦听程序 (Listener)** > **创建侦听程序 (Create Listener)**。

将后端注册到后端集

要将 threat defense virtual 实例注册到负载均衡器，应将 threat defense virtual 实例外部接口 IP 配置为外部负载均衡器后端集中的后端。内部接口 IP 应配置为内部负载均衡器后端集中的后端。确保您正在使用的端口已被添加到侦听程序中。

从 OCI 中删除 Autoscale 配置

可以使用 OCI 中的资源管理器以相同的方式删除使用 Terraform 部署的堆栈。删除堆栈会删除其创建的所有资源，并且与这些资源关联的所有信息都会被永久删除。

注释 在堆栈删除的情况下，建议将实例池中的最小实例数设置为 0，然后等待实例终止。这样将有助于删除所有实例，并且不会留下任何残留。

您可以执行手动删除或使用 使用 Cloud Shell 来删除 Autoscale 。

手动删除

删除端到端 Auto Scale 解决方案包括三个步骤：删除 Terraform Template-2 堆栈、删除 Oracle 功能，然后是删除 Terraform Template-1 堆栈 。

删除 Terraform Template-2 堆栈

要删除 Autoscale 配置，您必须先删除 Terraform Template-2 堆栈。

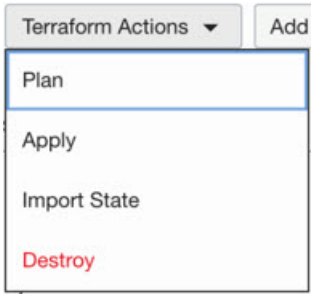
过程

步骤 1 登录 OCI 门户。

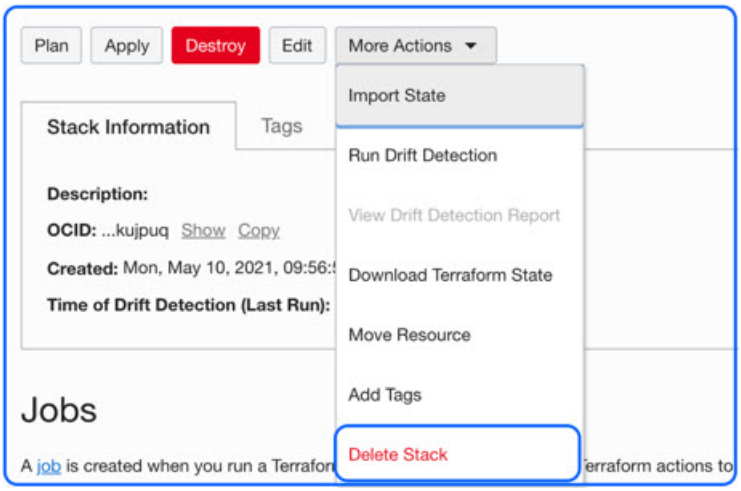
区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)**。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后选择**Terraform 操作 (Terraform Actions)** 下拉菜单中的**销毁 (Destroy)**，如图所示。



将创建销毁作业，逐个删除资源需要一些时间。您可以在销毁作业完成后删除堆栈。如下图所示：



步骤 4 继续删除 Oracle 功能。

删除 Oracle 功能

Oracle 功能部署不是 Terraform 模板堆栈部署的一部分，它要使用 Cloud Shell 单独上传。因此，Terraform 堆栈删除也不支持其删除。您必须删除通过 Terraform Template-1 创建的 OCI 应用内的所有 Oracle 函数。

过程

步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **功能 (Functions)**。选择在模板 1 堆栈中创建的应用名称。

步骤 3 在此应用中，访问每个函数并将其删除。

删除 Terraform Template-1 堆栈

注释 只有在删除所有 Oracle 功能之后，才能成功删除模板 1 堆栈。

与 Terraform Template-2 删除相同。

过程

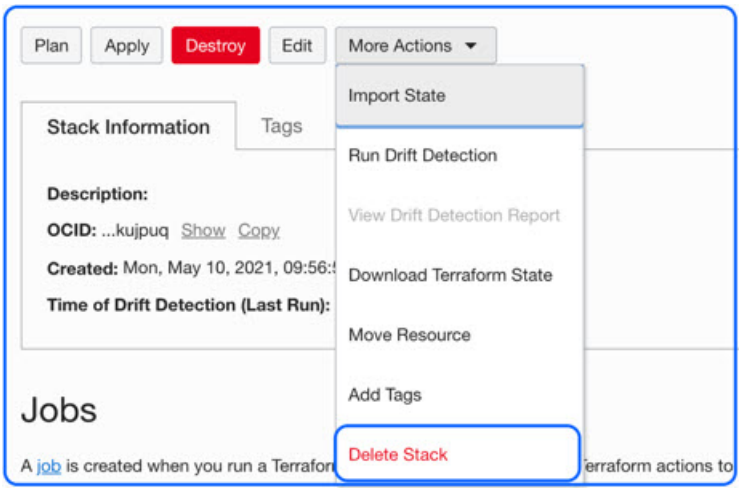
步骤 1 登录 OCI 门户。

区域显示在屏幕的右上角。确保您在预期的区域内。

步骤 2 选择**开发人员服务 (Developer Services)** > **资源管理器 (Resource Manager)** > **堆栈 (Stack)**。

步骤 3 选择 Terraform Template-2 创建的堆栈，然后点击 **Terraform 操作 (Terraform Actions)** 下拉菜单中的**销毁 (Destroy)**。系统将创建销毁作业，逐个删除资源需要一些时间。

步骤 4 销毁作业完成后，您可以从**更多操作 (More Actions)** 下拉菜单中删除堆栈，如下图所示。



成功删除 Terraform Template-1 堆栈后，您必须验证是否所有资源均已删除，并且没有任何类型的残留。

使用 Cloud Shell 来删除 Autoscale

用户可以在 Cloud Shell 中执行 `python3 oci_ftdv_autoscale_teardown.py` 命令，一般使用脚本删除堆栈和 Oracle 功能。如果堆栈是手动部署的，请更新 stack1 和 stack2 的堆栈 ID，然后更新 *teardown_parameters.json* 文件中的应用 ID。

使用 SSH 连接到 Threat Defense Virtual实例

要从 Unix 风格的系统连接到 threat defense virtual 实例，请使用 SSH 登录实例。

过程

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例：

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 threat defense virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 OpenSSH 连接到 Threat Defense Virtual实例

要从 Windows 系统连接到 threat defense virtual 实例，请使用 OpenSSH 登录实例。

过程

步骤 1 如果这是您首次使用此密钥对，则必须设置文件权限，以便只有您能读取文件。

执行以下操作：

a) 在 Windows 资源管理器中，导航至私钥文件，右键点击该文件，然后点击**属性 (Properties)**。
b) 在**安全 (Security)** 选项卡上，点击**高级 (Advanced)**。
c) 确保**所有者 (Owner)** 是您的用户帐户。
d) 点击**禁用继承 (Disable Inheritance)**，然后选择**将此对象的继承权限转换为显式权限 (Convert inherited permissions into explicit permissions on this object)**。
e) 选择不是您的用户帐户的每个权限条目，然后点击**删除 (Remove)**。
f) 确保您的用户帐户的访问权限为**完全控制 (Full control)**。
g) 保存更改。

步骤 2 要连接到实例，请打开 Windows PowerShell 并运行以下命令：

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 threat defense virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用 PuTTY 连接到 Threat Defense Virtual实例

要使用 PuTTY 从 Windows 系统连接到 threat defense virtual 实例，请执行以下操作：

过程

步骤 1 打开 PuTTY。

步骤 2 在**类别 (Category)** 窗格中，选择**会话 (Session)** 并输入以下内容：

- **主机名（或 IP 地址）：**

  <username>@<public-ip-address>

  其中：

  <username> 是 threat defense virtual 实例的用户名。

  <public-ip-address> 是您从控制台检索的实例公共 IP 地址。

- **端口：** 22
- **连接类型：** SSH

步骤 3 在**类别 (Category)** 窗格中，展开**窗口 (Window)**，然后选择**转换 (Translation)**。

步骤 4 在**远程字符集 (Remote character set)** 下拉列表中，选择 **UTF-8**。

基于 Linux 的实例的默认区域设置为 UTF-8，这样会将 PuTTY 配置为使用相同的区域设置。

步骤 5 在**类别 (Category)** 窗格中，依次展开**连接 (Connection)** 和 **SSH**，然后点击**身份验证 (Auth)**。

步骤 6 点击**浏览 (Browse)**，然后选择您的私钥。

步骤 7 点击**打开 (Open)** 以启动会话。

如果这是第一次连接到实例，您可能会看到一条消息，表明服务器的主机密钥未缓存在注册表中。点击**是 (Yes)** 以继续连接。

IPv6 故障排除

问题 SSH - 使用 IPv6 的 Firewall Threat Defense Virtual 不工作

- 解决方法 确保已添加通过互联网网关进行 IPv6 公共访问的路由。
- 解决方法 Firewall Threat Defense Virtual 管理配置中存在启用 IPv6。
- 解决方法 验证已将 IPv6 相关访问列表添加到已部署的 Firewall Threat Defense Virtual。
- 解决方法 验证是否使用“ipv6 address dhcp default”在管理接口上配置 IPv6。如果仅使用“ipv6 address dhcp”，则单独添加以下路由“ipv6 route management ::/0<IPv6_Gateway_address>”。
- 解决方法 验证是否允许正确的 ssh 入口。使用以下命令为所有“ssh ::/0 management”设置 ssh access allow。

问题 无法将 IPv6 地址分配给现有子网。

- 解决方法 验证子网所属的 VCN 是否已启用 IPv6。
- 解决方法 确保使用的是正确的 IPv6 CIDR。
- 解决方法 子网只能包含“/64”IPv6 CIDR 前缀。

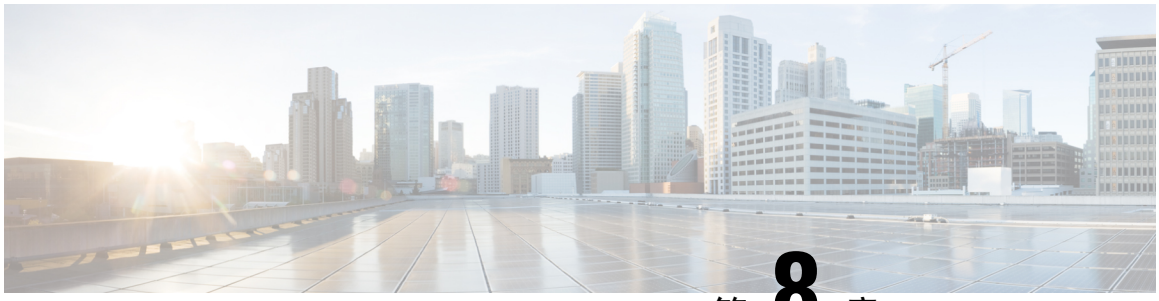
问题 东西向流量不起作用。

- 解决方法 验证是否已正确添加以下路由。

  解决方法 ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

  解决方法 示例：ipv6 route inside 2603:c020:5:5800::/56 fe80::200:17ff:fe96:921b

- 解决方法 确保使用的是正确的 IPv6 CIDR。
- 解决方法 确保是否为 IPv6 配置了正确的访问列表。



第 8 章

在 Google 云平台上部署 Threat Defense Virtual

您可以在 Google 云平台 (GCP) 上部署 threat defense virtual，这是一种公共云计算服务，让您能够在 Google 提供的高度可用的托管环境中运行应用。

您会在 GCP 控制台**控制面板**中看到 GCP 项目信息。

- 如果尚未选择 GCP 项目，请确保在**控制面板 (Dashboard)** 中选择该项目。
- 要访问控制面板，请点击**导航菜单** > **主页 (Home)** > **控制面板 (Dashboard)**。

您可以登录 GCP 控制台，在 GCP 市场中搜索 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品，然后启动 threat defense virtual 实例。以下程序介绍了如何准备 GCP 环境并启动 threat defense virtual 实例，以便部署 threat defense virtual。

概述

threat defense virtual 运行与物理 Cisco Secure Firewall Threat Defense （之前称为 Firepower Threat Defense）相同的软件，以虚拟形式提供成熟的安全功能。threat defense virtual 可以部署在公共 GCP 中。然后，可以对其进行配置，以保护在一段时间内扩展、收缩或转换其位置的虚拟和物理数据中心工作负载。

系统要求

选择 Google 虚拟机类型和大小以满足 threat defense virtual 需求。目前，threat defense virtual 支持计算优化和通用计算机（标准、高内存以及高 CPU 计算机类型）。

注释 支持的计算机类型可能会更改，恕不另行通知。

表 *26:* 支持的计算优化计算机类型

计算优化计算机类型	属性		
	vCPU	随机存取存储器(GB)	**vNIC**
c2-standard-4	4	16 GB	4
c2-standard-8	8	32 GB	8
c2-standard-16	16	64 GB	8

表 *27:* 支持的通用计算机类型

通用计算机类型	属性		
	vCPU	随机存取存储器(GB)	**vNIC**
n1-standard-4	4	15	4
n1-standard-8	8	30	8

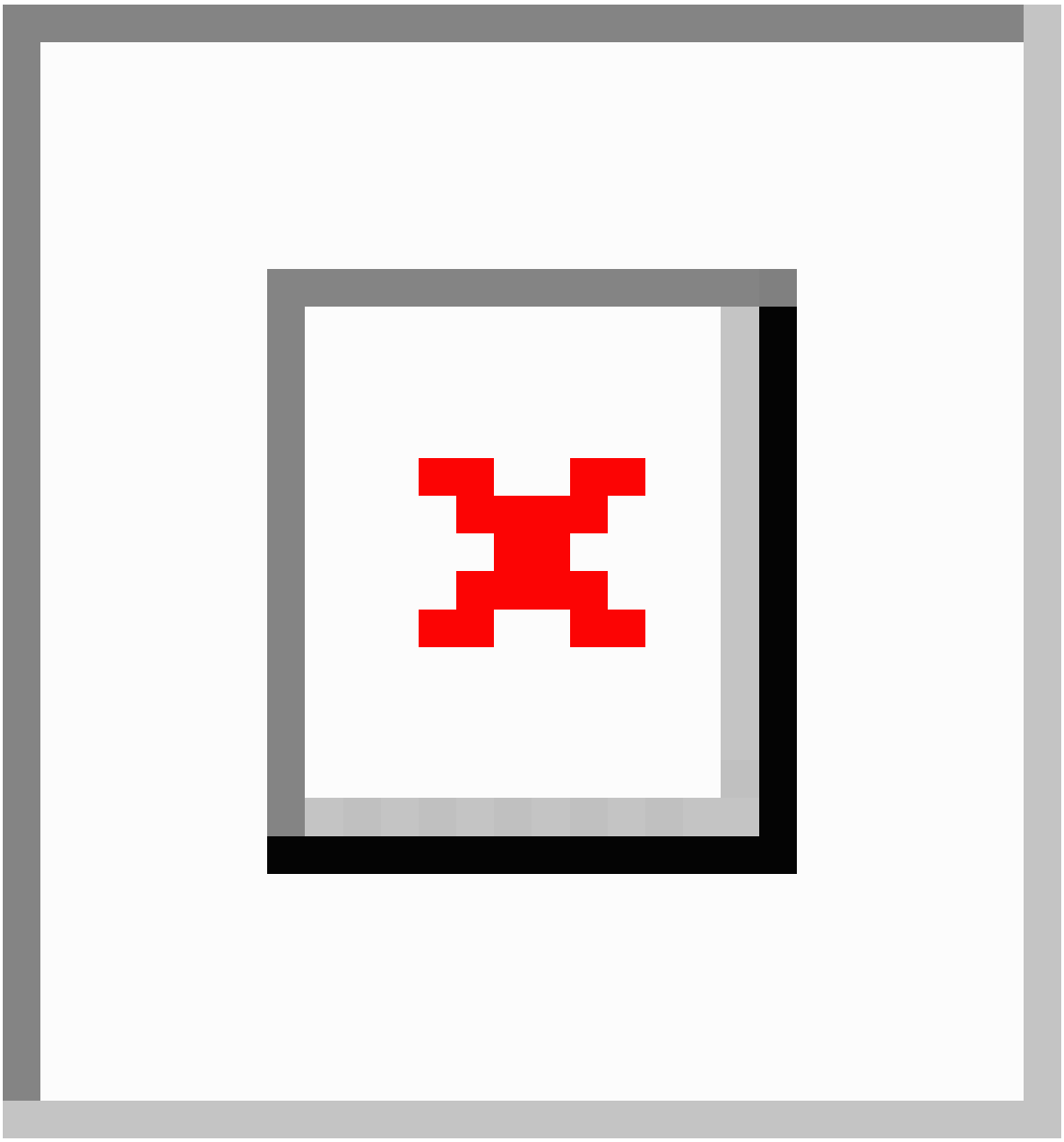
通用计算机类型	属性		
	vCPU	随机存取存储器(GB)	**vNIC**
n1-standard-16	16	60	8
n2-standard-4	4	16	4
n2-standard-8	8	32	8
n2-standard-16	16	64	8
n2-highmem-4	4	32	4
n2-highmem-8	8	64	8

- threat defense virtual 至少需要 4 个接口。
- 支持的最大 vCPU 数量为 16 个。

您可以在 GCP 上创建帐户、使用 GCP 市场上的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 产品来启动 VM 实例，以及选择 GCP 计算机类型。

端到端程序

以下流程图说明了在 Google Cloud 平台上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	GCP	配置 GCP 环境：创建 VPC 网络（**VPC 网络 (VPC Networks)** > 子网 **(Subnet)** > 区域 **(Region)** > **IP 地址范围 (IP address range)**）。
2	GCP	创建防火墙规则：创建防火墙规则（**网络 (Networking)** > **VPC 网络 (VPC networks)** > 防火墙 **(Firewall)** > 创建防火墙规则 **(Create Firewall Rule)**）。
3	GCP	部署 Threat Defense Virtual：在 GCP 市场中搜索“Cisco Secure Firewall”。

	工作空间	步骤
4	GCP	部署 Threat Defense Virtual：配置 Threat Defense Virtual 部署参数。
5	GCP	部署 Threat Defense Virtual：配置网络接口并应用防火墙规则。
6	GCP	部署 Threat Defense Virtual：在 GCP 上部署 Threat Defense Virtual。
7	管理中心或设备管理器	管理 threat defense virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual

前提条件

- 在 https://cloud.google.com 上创建 GCP 帐户。
- 创建 GCP 项目。请参阅 Google 文档创建项目 (Creating Your Project)。
- 思科智能账户。可以在思科软件中心 (https://software.cisco.com/) 创建一个账户。
- 许可 threat defense virtual。
  - 所有安全服务的许可证授权均在 管理中心中配置。
  - 有关如何管理许可证的详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》 中的许可章节。
- 有关 threat defense virtual 系统要求，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

接口要求

- 管理接口 (2) - 一个用于将 threat defense virtual 连接到 管理中心，另一个用于诊断；无法用于直通流量。
- 流量接口 (2) - 用于将 threat defense virtual 连接到内部主机和公共网络。
- 从 Cisco Secure Firewall 版本 7.4.1 开始，您可以删除诊断接口，并在至少具有以下 4 个接口（1 个管理接口和 3 个数据接口）的 GCP 上部署 Threat Defense Virtual。建议您在没有 Cisco Secure Firewall 版本 7.4.1 的诊断接口的情况下在 GCP 上部署 Threat Defense Virtual。有关详细信息，请参阅关于在 GCP 上部署无诊断接口的 Threat Defense Virtual，第 329 页。

通信路径

- 用于访问 threat defense virtual的公共 IP。

Threat Defense Virtual和 GCP 的准则和限制

支持的功能

- 在 GCP 计算引擎中部署
- 每个实例最多 16 个 vCPU
- 路由模式（默认）
- 许可 - 仅支持 BYOL
- 集群（7.2 或更高版本）。有关详细信息，请参阅公共云中 Threat Defense Virtual 的集群
- 在 Cisco Secure Firewall 7.1 及更低版本上，仅支持 管理中心。从 Cisco Secure Firewall 版本 7.2 开始，还支持 设备管理器。

Threat Defense Virtual 智能许可的性能层

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *28:* 基于授权的 ***Threat Defense Virtual*** 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv100，16Gbps	16 核/32 GB	16Gbps	10,000

请参阅《Cisco Secure Firewall Management Center 管理指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

注释 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 GCP 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

接收和传输队列的分配

为每个 vNIC 分配特定数量的接收 (RX) 和传输 (TX) 队列以处理网络数据包。根据使用的网络接口类型（VirtIO 或 gVNIC），Google Cloud 使用一种算法为每个 vNIC 分配默认数量的 RX 和 TX 队列。

GCP 用于将队列分配给 vNIC 的方法如下：

- VirtIO - vCPU 数量除以 vNIC 数量，并丢弃任何剩余值。

  例如，如果虚拟机有 16 个 vCPU 和 4 个 vNIC，则为每个 vNIC 分配的队列数为 [16/4] = 4。

- gVNIC - vCPU 数量除以 vNIC 数量，然后再将结果除以 2

  例如，如果虚拟机有 128 个 vCPU 和 2 个 vNIC，则分配的队列数为 [128/2]/2 = 32。

您还可以在使用 Compute Engine API 创建新虚拟机时自定义分配给每个 vNIC 的队列数。但是，如果要执行此操作，必须遵守以下规则 -

- 最小队列计数：每个 vNIC 一个。
- 最大队列计数：此数字为 vCPU 计数或每个 vNIC 的最大队列计数中的较低者，具体取决于驱动程序类型：
  - 如果使用 VirtIO 或自定义驱动程序，则最大队列计数为 32
  - 如果使用 gVNIC，则最大队列计数为 16
- 如果您自定义分配给 VM 的所有 vNIC 的队列数量，则分配的队列总数必须小于或等于分配给 VM 实例的 vCPU 数量。

有关默认和自定义队列分配的详细信息和示例，请参阅默认队列分配和自定义队列分配。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

升级

不支持在 GCP 中将 threat defense virtual 从 Cisco Secure Firewall 版本 7.1 升级到 7.2。如果要从 Cisco Secure Firewall 版本 7.1 升级到 7.2，请执行重新映像。

不支持的功能

- IPv6
- Threat Defense Virtual 本地 HA
- 透明/内联/被动模式
- 巨型帧

NIC 到数据接口的映射

在 Cisco Secure Firewall 版本 7.1 及更早版本上，网络接口卡 (NIC) 到数据接口的映射如下所示：

- nic0 – 管理接口
- nic1 – 诊断接口
- nic2 – 千兆位以太网 0/0
- nic3 – 千兆位以太网 0/1

从 Cisco Secure Firewall 版本 7.2 开始，由于外部负载均衡器 (ELB) 仅将数据包转发到 nic0，因此需要在 nic0 上使用数据接口来促进南北流量的移动。

Cisco Secure Firewall 版本 7.2 上 NIC 和数据接口的映射如下所示：

- nic0 – 千兆位以太网 0/0
- nic1 – 千兆位以太网 0/1
- nic2 – 管理接口
- nic3 – 诊断接口
- nic4 – 千兆以太网 0/2

  .

  .

  .

- nic(N-2) – 千兆以太网 0/N-4
- nic(N-1) – 千兆以太网 0/N-3

从 Cisco Secure Firewall 版本 7.4.1 开始，您还可以在没有诊断界面的情况下部署 Threat Defense Virtual。在这种情况下，NIC 和数据接口的映射如下所示：

- nic0 – 千兆位以太网 0/0
- nic1 – 千兆位以太网 0/1
- nic2 – 管理接口
- nic3 – 千兆以太网 0/2
- nic4 – 千兆以太网 0/3

.

.

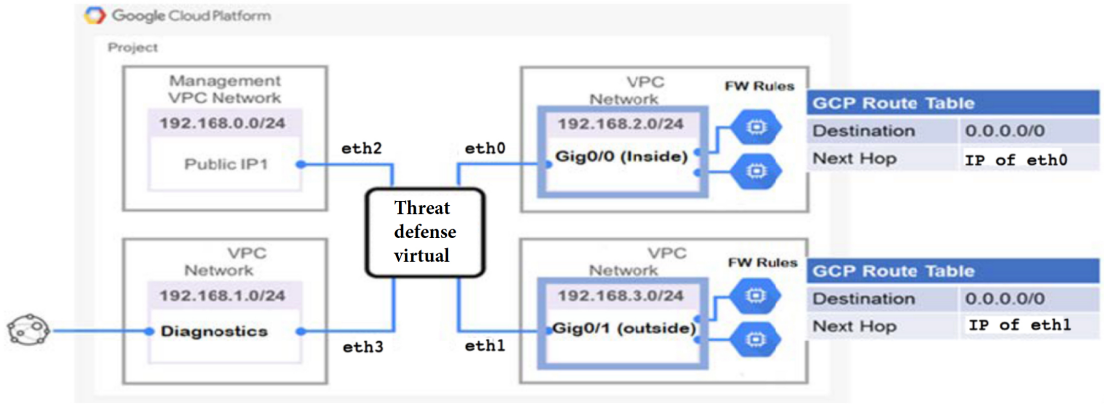
.

- nic(N-2) – 千兆以太网 0/N-3
- nic(N-1) – 千兆以太网 0/N-2

网络拓扑示例

下图显示了在路由防火墙模式下建议用于 threat defense virtual 的拓扑，在 GCP 中为 threat defense virtual 配置了 4 个子网（管理、诊断、内部和外部）。

图 *46: GCP* 上的 *Threat Defense Virtual*部署示例



如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

配置 GCP 环境

threat defense virtual 部署需要四个网络，您必须在部署 threat defense virtual 之前创建这些网络。网络如下：

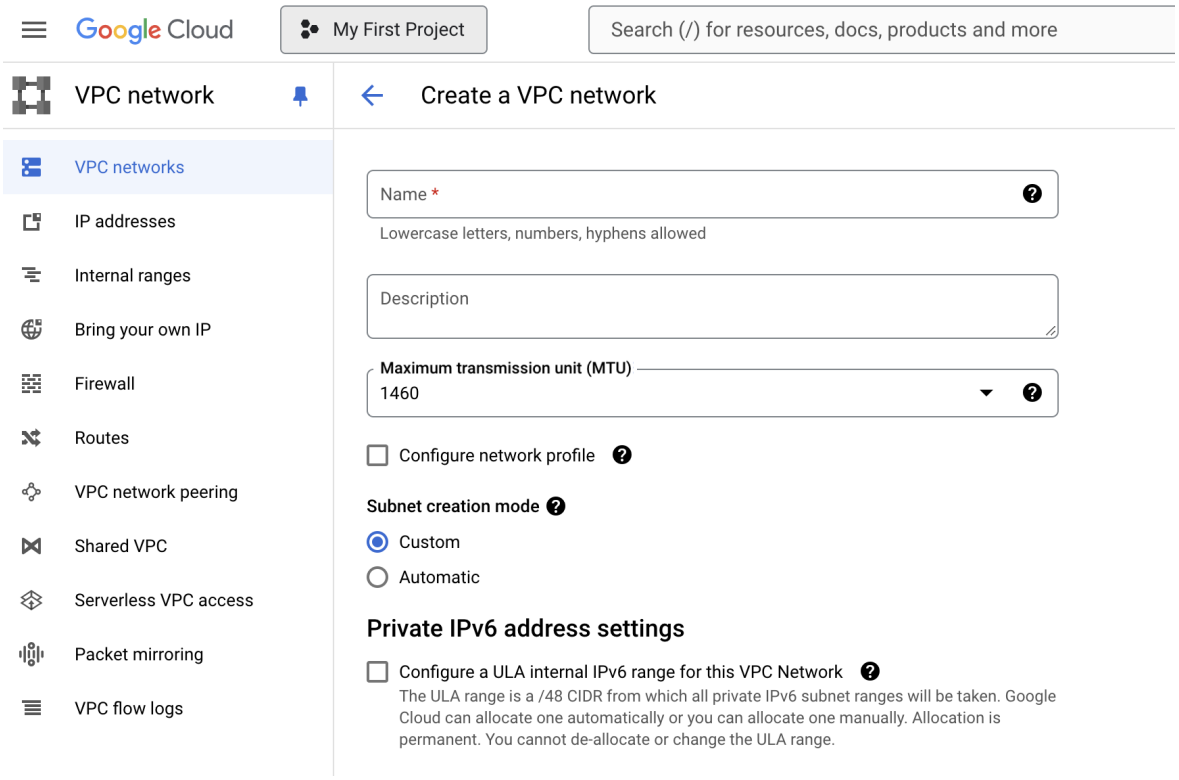
- 管理子网的管理 VPC。
- 诊断 VPC 或诊断子网。
- 内部子网的内部 VPC。
- 外部子网的外部 VPC。

此外还设置了路由表和 GCP 防火墙规则，以允许流量流经 threat defense virtual。路由表和防火墙规则与在 threat defense virtual本身上配置的路由表和防火墙规则不同。根据关联的网络和功能命名 GCP 路由表和防火墙规则。请参阅 网络拓扑示例作为指南。

您可以设置跨所有接口进行 GCP 运行状况检查的路由，这些接口用于配置其运行状况探测。如果用于 GCP 运行状况检查的路由尚不可用，则可以通过在接口上创建具有更高指标的路由来实现此目的。

过程

步骤 1 在 GCP 控制台中，选择 **VPC 网络 (VPC networks)**，然后点击**创建 VPC 网络 (Create VPC Network)**。

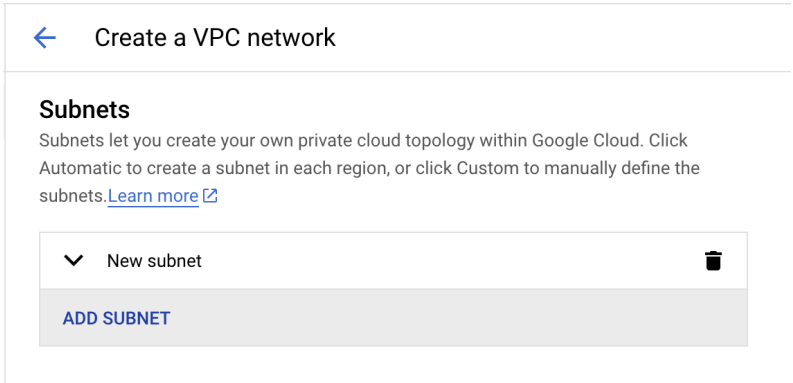


步骤 2 在**名称 (Name)** 字段中，输入所需的名称。

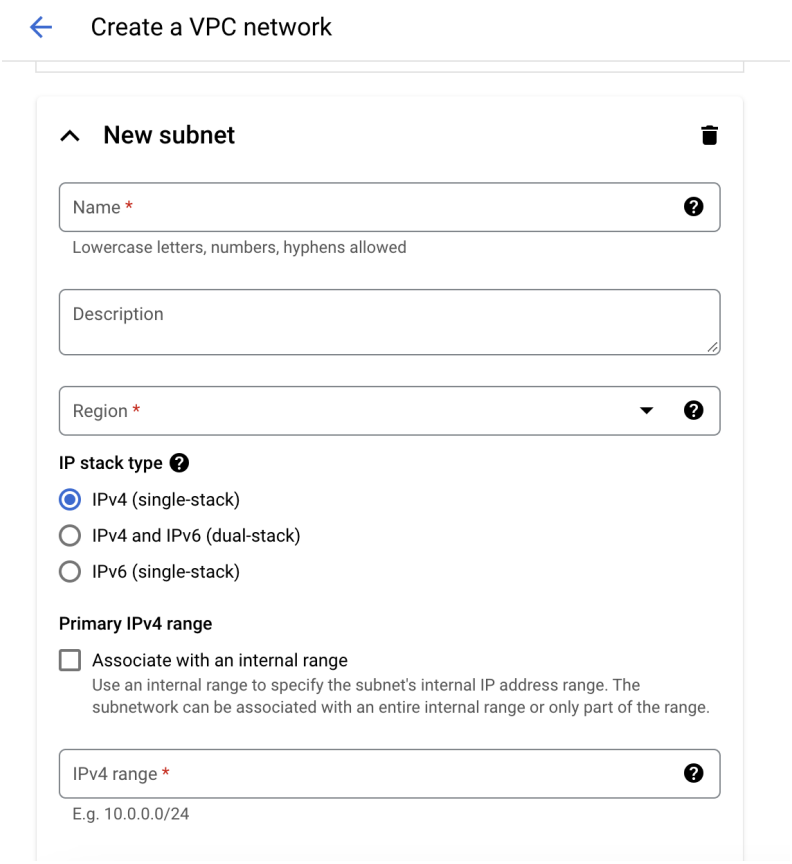
步骤 3 从 **最大传输单位 (MTU)** 下拉菜单中，选择适当的 MTU 值。

步骤 4 从 **子网创建模式** 选项中，点击 **自定义**。

步骤 5 在 **子网** 部分下，点击 **添加子网** 以创建新的子网。



步骤 6 在**新子网 (New subnet)** 下的**名称 (Name)** 字段中输入所需的名称。



步骤 7 从区域 **(Region)** 下拉列表中，选择适合您的部署的区域。所有四个网络都必须位于同一区域。

步骤 8 从 **IP 地址范围 (IP address range)** 字段中，输入 CIDR 格式的第一个网络子网，例如 10.10.0.0/24。

步骤 9 接受所有其他设置的默认设置，然后点击**创建 (Create)**。

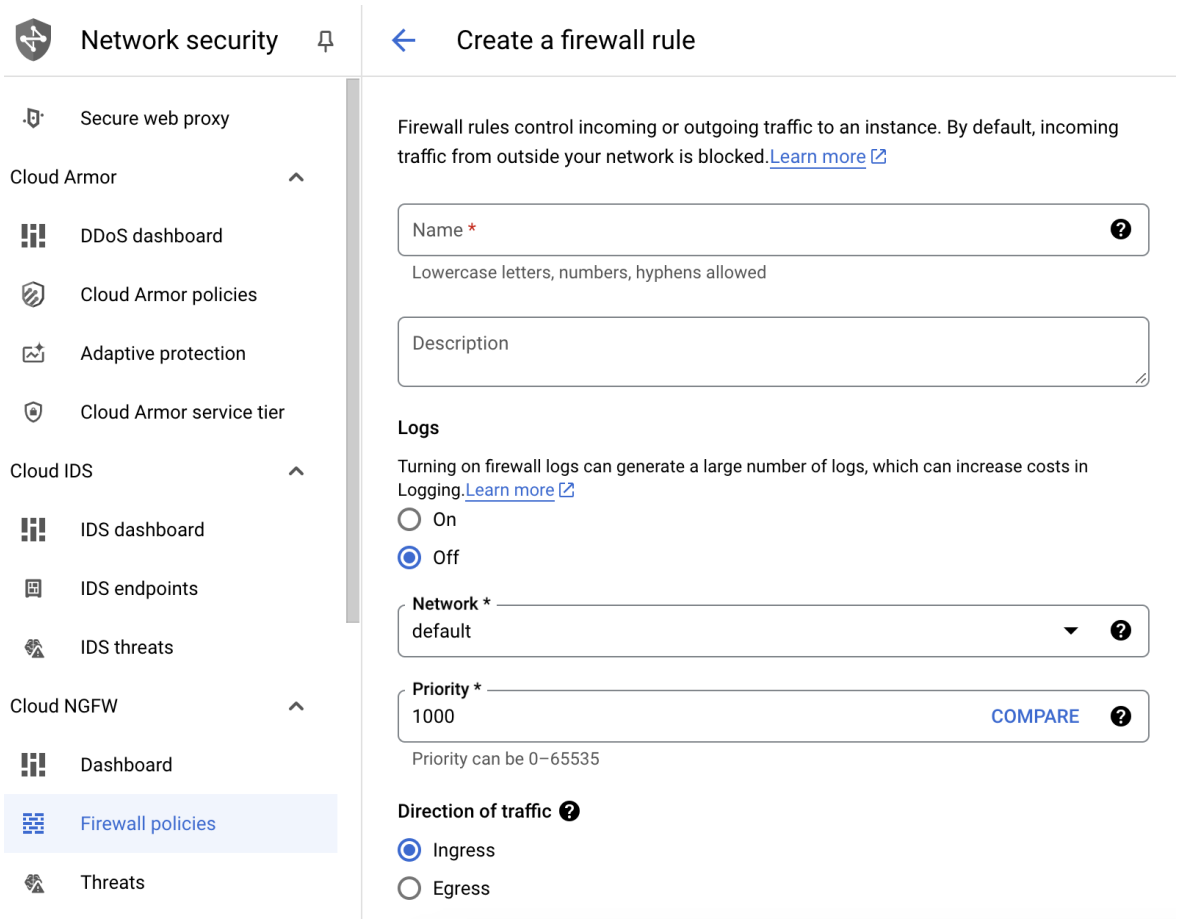
步骤 10 重复步骤 1-7，在您的 VPC 中创建其余三个 VPC 网络。

创建防火墙规则

在部署 threat defense virtual 实例时，请为管理接口应用防火墙规则（以允许使用 管理中心 的 SSH 和 HTTPS 连接），请参阅部署 Threat Defense Virtual，第 323 页。根据您的要求，您还可以为内部、外部和诊断接口创建防火墙规则。

过程

步骤 1 在GCP控制台中，依次选择**网络 (Networking)** > **VPC 网络 (VPC network)** > **防火墙 (Firewall)**，然后点击**创建防火墙规则 (Create Firewall Rule)**。

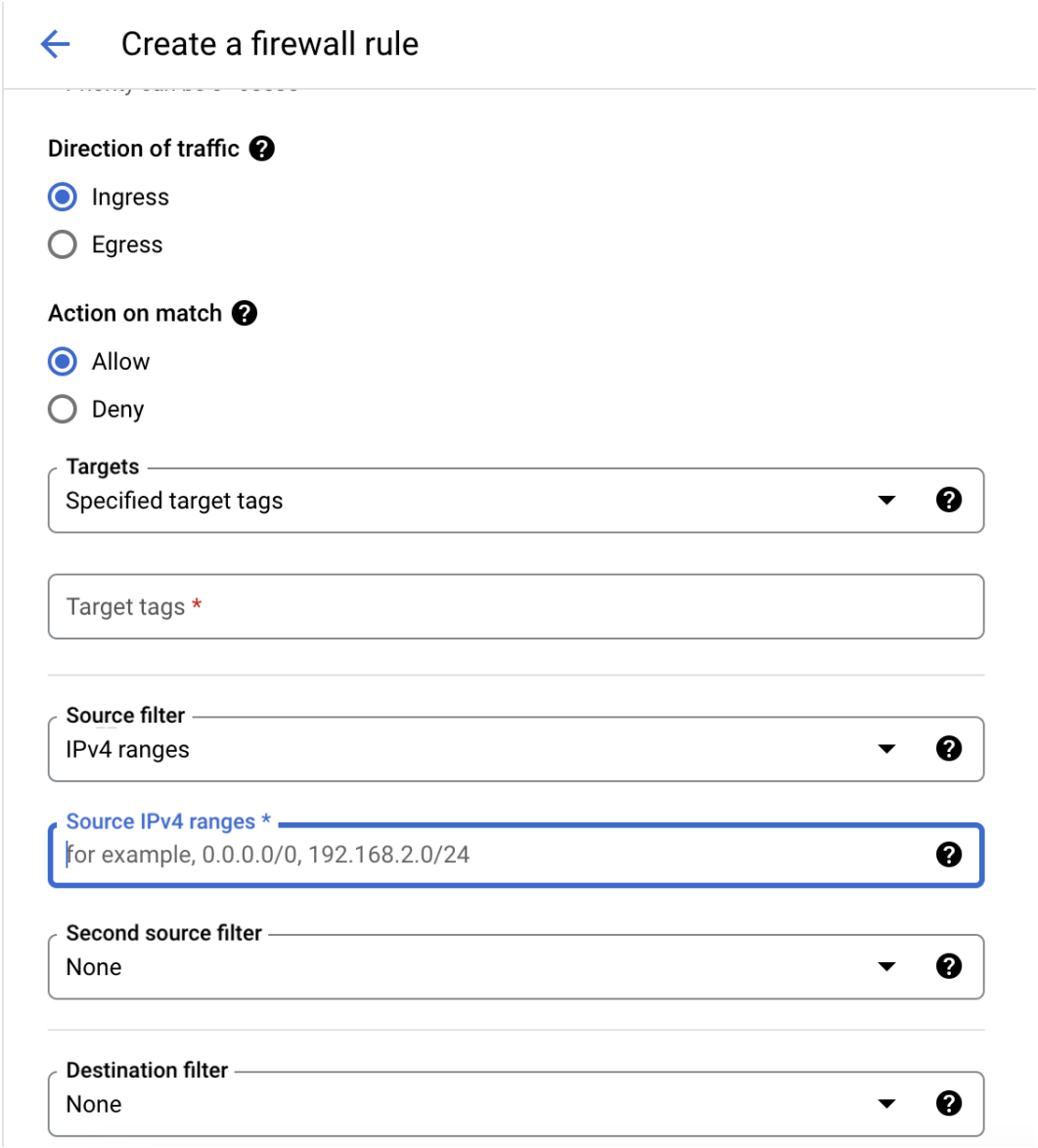


步骤 2 在**名称 (Name)** 字段中，为防火墙规则输入描述性名称，例如：*vpc-asiasouth-inside-fwrule*。

步骤 3 从**网络 (Network)** 下拉列表中，选择要为其创建防火墙规则的 VPC 网络的名称，例如 *ftdv-south-inside*。

步骤 4 从**目标 (Targets)** 下拉列表中，选择适用于防火墙规则的选项，例如：**网络中的所有实例 (All instances in the network)**。

步骤 5 从 **源过滤器** 下拉列表中，选择支持的 IP 类型，例如 **IPv4 范围**。



步骤 6 在源 **IP** 范围 **(Source IP ranges)** 字段中，以 CIDR 格式输入源 IP 地址范围，例如 0.0.0.0/0。

仅允许自这些 IP 地址范围内的源的流量。

步骤 7 在协议和端口 **(Protocols and ports)**下，选择指定的协议和端口 **(Specified protocols and ports)**。

步骤 8 添加安全规则。

步骤 9 点击创建 **(Create)**。

部署 Threat Defense Virtual

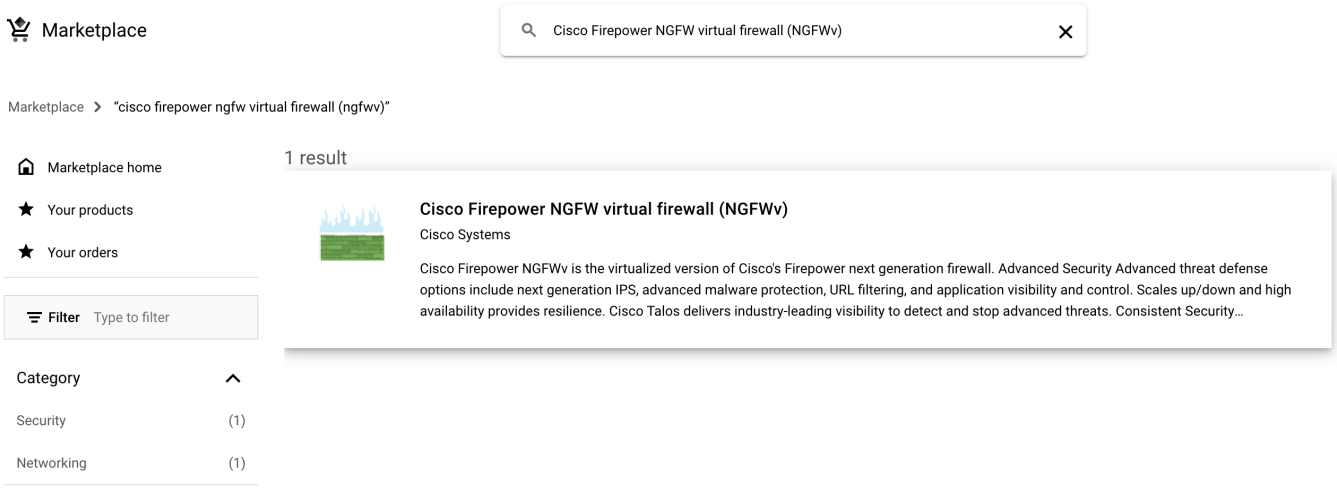
您可以按照以下步骤，使用 GCP 市场提供的 Cisco Firepower NGFW 虚拟防火墙 (NGFWv) 部署 threat defense virtual 实例。

过程

步骤 1 登录到 GCP 控制台。

步骤 2 点击**导航菜单** > **市场 (Marketplace)**。

步骤 3 在市场中搜索 “Cisco Firepower NGFW virtual firewall (NGFWv)”，然后选择产品。



步骤 4 点击**启动 (Launch)**。

a) **部署名称 (Deployment name)** - 为实例指定唯一的名称。
b) **区域 (Zone)** - 选择要部署 threat defense virtual 的区域。
c) **计算机类型 (Machine type)** - 根据 系统要求，第 310 页 选择正确的计算机类型。
d) **SSH 密钥（可选）(SSH key [optional])** - 从 SSH 密钥对粘贴公钥。

   密钥对由 GCP 存储的一个公共密钥和用户存储的一个专用密钥文件组成。两者共同确保安全连接到实例。请务必将密钥对保存到已知位置，以备连接到实例之需。

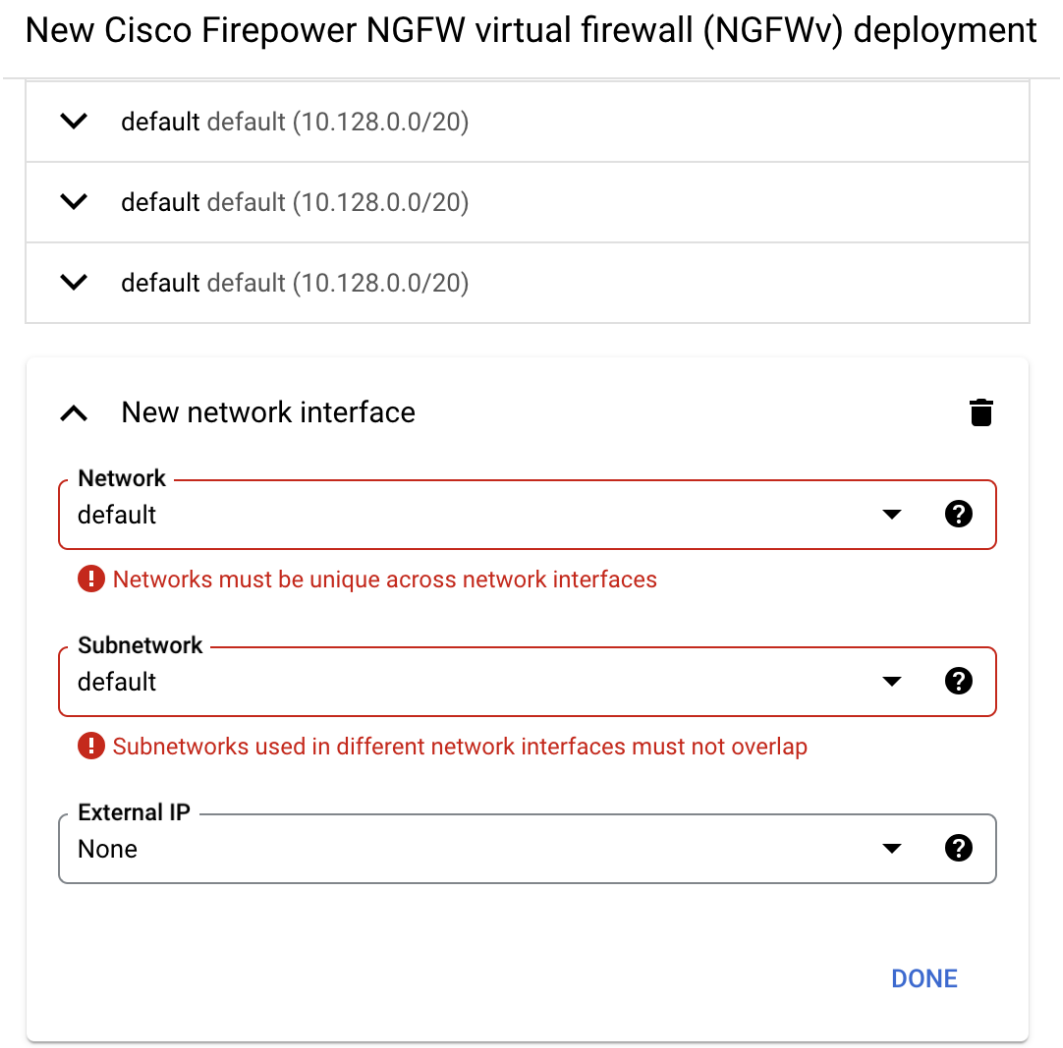
e) 选择允许还是阻止使用项目级别的 SSH 密钥访问此实例。请参阅 Google 文档允许或阻止使用项目级别的公共 SSH 密钥访问 Linux 实例。
f) **启动脚本 (Startup script)** - 您可以为 threat defense virtual 实例创建启动脚本，以便在每次实例启动时执行自动化任务。

   以下示例显示了将 Day0 配置复制并粘贴到**启动脚本 (Startup script)** 字段的示例：

```
{
"AdminPassword": "Cisco@123123",
"Hostname": "ftdv-gcp",
"DNS1": "8.8.8.8",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No"
}
```

提示
为防止执行错误，您应使用 JSON 验证器来验证 Day0 配置。

g) **网络接口 (Network interfaces)** - 配置接口：1) 管理接口、2) 诊断接口、3) 内部接口、4) 外部接口。



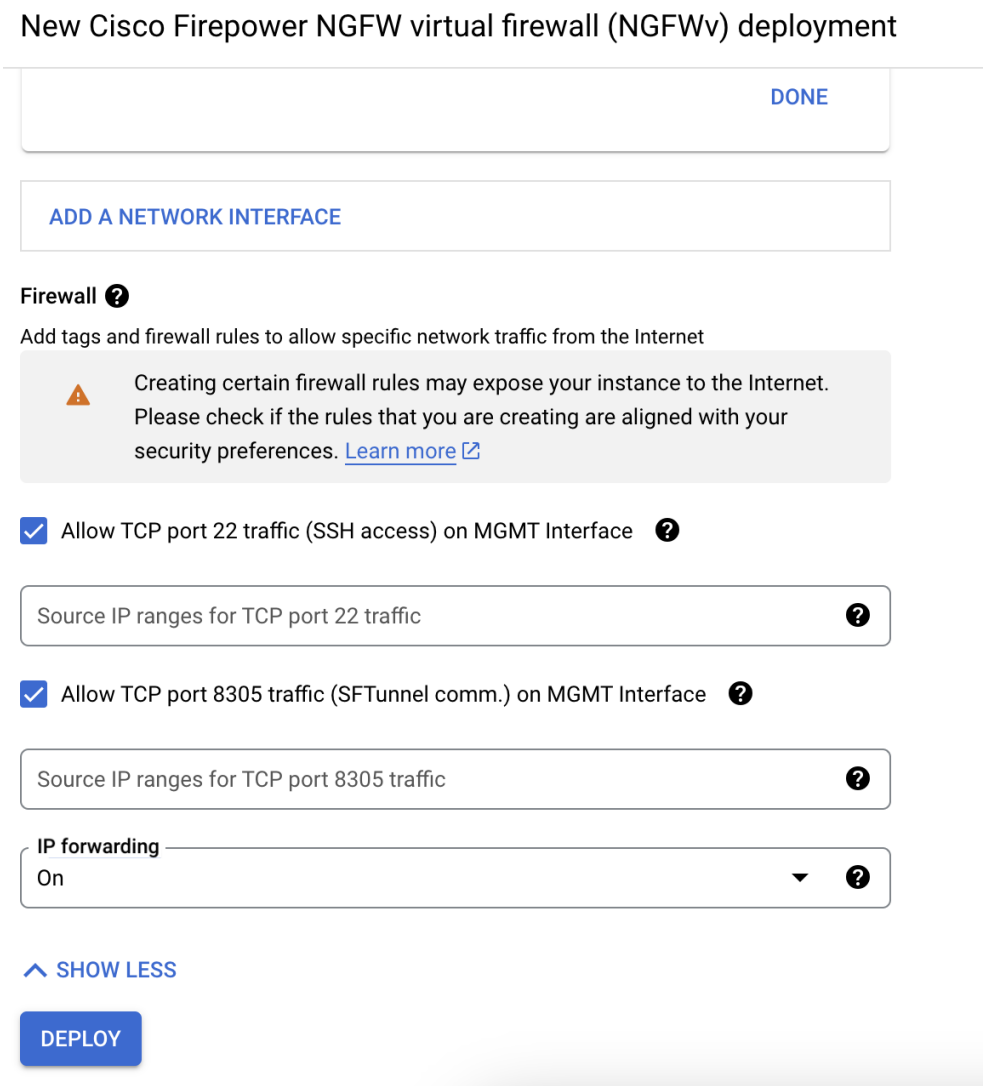
注释
创建实例后，将无法向实例中添加端口。如果使用不正确的接口配置创建实例，则必须删除该实例并使用正确的接口配置重新创建实例。

1. 从**网络 (Network)** 下拉列表中，选择一个 VPC 网络，例如 *vpc-assoso-mgmt*。

2. 从 **子网 (Subnet)** 下拉列表中，选择一个子网。
3. 从**外部 IP (External IP)** 下拉列表中，选择适当的选项。

   对于管理接口，将**外部 IP (External IP)** 选择为**临时 (Ephemeral)**。这对于内部和外部接口是可选的。
4. 点击**完成 (Done)**。

h) **防火墙 (Firewall)** - 应用防火墙规则。



- 选中**允许来自 Internet（SSH 访问）的 TCP 端口 22 流量 (Allow TCP port 22 traffic from the Internet [SSH access])** 复选框以允许 SSH。
- 选中**允许来自互联网的 HTTPS 流量（FMC 访问）(Allow HTTPS traffic from the Internet [FMC access])** 复选框以允许 管理中心 和托管设备使用双向 SSL 加密通信通道 (SFTunnel) 进行通信。

i) 点击**更多 (More)** 展开视图并确保 **IP 转发 (IP Forwarding)** 设置为**开 (On)**。

步骤 5 点击**部署 (Deploy)**。

注释
启动时间取决于多种因素，包括资源的可用性。最多可能需要 7-8 分钟来完成初始化。请勿中断初始化，否则您可能需要删除设备并重新开始。

下一步做什么

从 GCP 控制台的 VM 实例页面查看实例详细信息。您将找到内部 IP 地址、外部 IP 地址以及用于停止和启动实例的控件。如果需要编辑实例，则需要停止实例。

使用外部 IP 连接到 Threat Defense Virtual实例

threat defense virtual 实例分配有内部 IP 和外部 IP。您可以使用外部 IP 来访问 threat defense virtual 实例。

过程

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 点击 threat defense virtual 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，点击 **SSH** 字段的下拉菜单。

步骤 4 从 **SSH** 下拉菜单中选择所需的选项。

您可以使用以下方法连接到 threat defense virtual 实例。

- 任何其他 SSH 客户端或第三方工具 - 有关详细信息，请参阅 Google 文档使用第三方工具连接 (Connecting using third-party tools)。

使用 SSH 连接到 Threat Defense Virtual实例

要从 Unix 风格的系统连接到 threat defense virtual 实例，请使用 SSH 登录实例。

过程

步骤 1 使用以下命令设置文件权限，以便只有您可以读取文件：

```
$ chmod 400 <private_key>
```

其中：

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

步骤 2 使用以下 SSH 命令访问实例：

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> 是文件的完整路径和名称，该文件包含与要访问的实例关联的私钥。

<username> 是 threat defense virtual 实例的用户名。

<public-ip-address> 是您从控制台检索的实例 IP 地址。

使用串行控制台连接至 Threat Defense Virtual实例

过程

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 点击 threat defense virtual 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，点击**连接到串行控制台 (Connect to serial console)**。

有关详细信息，请参阅 Google 文档与串行控制台交互 (Interacting with the serial console)。

使用 Gcloud 连接到 Threat Defense Virtual 实例

过程

步骤 1 在 GCP 控制台中，选择**计算引擎 (Compute Engine)** > **VM 实例 (VM instances)**。

步骤 2 点击 threat defense virtual 实例名称以打开 **VM 实例详细信息 (VM instance details)** 页面。

步骤 3 在**详细信息 (Details)** 选项卡下，点击 **SSH** 字段的下拉菜单。

步骤 4 点击**查看 gcloud 命令 (View gcloud command)** > **在云 Shell 中运行 (Run in Cloud Shell)**。

此时将打开“云 Shell”(Cloud Shell) 终端窗口。有关详细信息，请参阅 Google 文档，gcloud 命令行工具概述 (gcloud command-line tool overview) 和 gcloud compute ssh。

关于在 GCP 上部署无诊断接口的 Threat Defense Virtual

在 Cisco Secure Firewall 版本 7.3 及更低版本上， Threat Defense Virtual 部署了至少 4 个接口 - 1 个管理接口、1 个诊断接口和 2 个数据接口。

从 Cisco Secure Firewall 版本 7.4.1 开始，您可以删除诊断接口，并使用至少 4 个接口（1 个管理接口和 3 个数据接口）部署 Threat Defense Virtual。此功能支持在同一计算机类型上部署具有其他数据接口的 Threat Defense Virtual。例如，在 c2-standard-8 计算机类型上，您现在可以部署具有 1 个管理接口和 7 个数据接口的 Threat Defense Virtual，而不是部署具有 1 个管理接口、1 个诊断接口和 6 个数据接口的 Threat Defense Virtual。

从 Cisco Secure Firewall 版本 7.4.1 开始，我们建议您在没有诊断接口的 GCP 上部署 Threat Defense Virtual。

此功能仅在 Google Cloud 平台 (GCP) 上新部署的 Threat Defense Virtual 实例上受支持。

注释 由于支持的最大接口数为 8，因此最多可以再添加 4 个接口来部署 Threat Defense Virtual，最多 8 个接口。

部署无诊断接口的 Threat Defense Virtual 的准则和限制

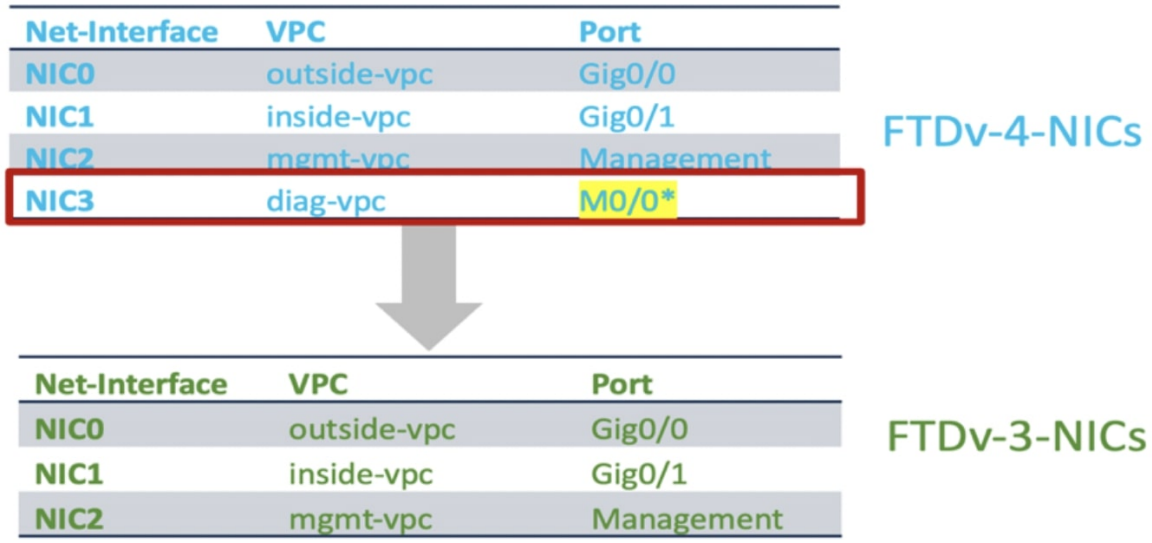
- 当诊断接口被删除时，系统日志和 SNMP 支持使用 Threat Defense Virtual 管理或数据接口，而不是使用诊断接口。
- 此部署支持集群和自动扩展。
- 不支持将具有诊断接口端口的 Threat Defense Virtual 实例和不具有诊断接口端口的 Threat Defense Virtual 实例分组。

注释 此处的 Threat Defense Virtual 实例分组是指 GCP 上实例组中实例的分组。这与 Management Center Virtual 上的 Threat Defense Virtual 实例的分组无关。

- 不支持 CMI。

NIC 到数据接口的映射，以便在 GCP 上部署无诊断接口的 Threat Defense Virtual

下面给出了 NIC 到数据接口的映射，用于部署无诊断接口的 Threat Defense Virtual。



在 GCP 上部署无诊断接口的 Threat Defense Virtual

执行下面给出的步骤，在没有诊断接口的情况下部署 Threat Defense Virtual。

过程

步骤 1 通过在用于全新部署的 day-0 配置脚本（GCP 控制台上的 **Startup script** ）中使用键值对 **Diagnostic: OFF/ON** 来启用此功能。默认情况下，键值对设置为 **Diagnostic: ON** ，并且会启动诊断接口。当键值对设置为 **Diagnostic: OFF** 时，部署将在没有诊断接口的情况下启动。

下面是一个 day-0 配置脚本示例。

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

注释
键值对 "Diagnostic": "ON/OFF" 区分大小写。

步骤 2 连接所需的最少 4 个 NIC。

有关在 GCP 上部署 Threat Defense Virtual 的详细程序，请参阅在 Google 云平台上部署 Threat Defense Virtual。

有关接口的详细信息，请参阅接口概况。

步骤 3 （可选） 在控制台上使用 **show interface ip brief** 命令可显示接口详细信息。您还可以在 Management Center Virtual 上查看接口详细信息，如下所示

接口在 Management Center Virtual 上显示，如下所示。

With Diagnostic Interface

Without Diagnostic Interface

升级场景

您可以根据以下场景升级 Threat Defense Virtual 实例。

- 所有 Cisco Secure Firewall 版本 – 您可以将部署了诊断接口的 Threat Defense Virtual 实例升级为具有诊断接口的 Threat Defense Virtual 实例。
- Cisco Secure Firewall 7.4 及更高版本 - 您可以将没有诊断接口的 Threat Defense Virtual 部署实例升级为没有诊断接口的 Threat Defense Virtual 实例。

不支持以下升级场景。

- 所有 Cisco Secure Firewall 版本 - 无法将部署了诊断接口的 Threat Defense Virtual 实例升级到没有诊断接口的 Threat Defense Virtual 实例。
- Cisco Secure Firewall 7.4.1 及更高版本 - 您无法将没有诊断接口的 Threat Defense Virtual 部署实例升级为具有诊断接口的 Threat Defense Virtual 实例。

注释 升级后，NIC 的数量和顺序均保持不变。

部署不带诊断接口的 Threat Defense Virtual 集群或 Auto Scale 解决方案

要在不使用诊断接口的情况下对 threat defense virtual 集群或由 threat defense virtual 实例组成的自动扩展解决方案执行新部署，请确保在 day-0 配置脚本中将键值对 **Diagnostic: OFF/ON** 设置为 **OFF**。

故障排除

如果在部署 threat defense virtual 时未删除诊断接口，请检查键值对 **Diagnostic: OFF/ON** 是否已在 day-0 配置脚本中设置为 **OFF**。

Auto Scale 解决方案

以下各节介绍 Auto Scale 解决方案的组件如何对 GCP 上的 threat defense virtual 发挥作用。

概述

面向 GCP 的 Threat Defense Virtual Auto Scale 是一个完整的无服务器实施方案，它利用 GCP 提供的无服务器基础设施（云函数、负载均衡器、Pub/Sub、实例组等）。

面向 GCP 的 Threat Defense Virtual Auto Scale 可实现的一些主要功能包括：

- GCP 部署管理器基于模板的部署。
- 支持基于 CPU 利用率的扩展指标。
- 支持 threat defense virtual 部署和多可用性区域。
- 支持 threat defense virtual 的自动注册和取消注册。
- 完全自动化配置会自动应用于横向扩展 threat defense virtual实例。
- 支持将 NAT 策略、访问策略和路由自动应用到 threat defense virtual。
- 对负载均衡器和多可用性区域的支持。
- 在其他平台上支持 Management Center Virtual。
- 思科提供面向 GCP 的 Auto Scale 部署包以方便部署。

准则和限制

- 仅支持 IPv4。

- 许可 - 仅支持 BYOL。不支持 PAYG 许可。
- 日志中不显示设备功能错误。
- 支持的最大设备数为 25。这是 Management Center Virtual 实例中的最大限制。
- 在所有 Cisco Secure Firewall 版本上，您都可以使用提供的模板部署 Threat Defense Virtual 自动扩展解决方案。部署的 Threat Defense Virtual 实例至少具有 4 个接口 - 1 个管理接口、1 个诊断接口和 2 个数据接口。

  从 Cisco Secure Firewall 版本 7.4.1 开始，您还可以在没有诊断界面的情况下部署 Threat Defense Virtual。同样在此场景中，使用至少 4 个接口（1 个管理接口和 3 个数据接口）完成部署。要执行此操作，请根据输入参数，第 339 页中的说明修改模板参数 *diagFirewallRule*、*diagSubnetworkName*、*diagVpcName* 和 *withDiagnostic*。
- 不支持用于减少外向扩展时间的冷备用或快照方法。
- 不支持基于计划的扩展。
- 不支持基于平均内存使用率的自动扩展。
- 内向扩展/外向扩展可能会使实例数减少/增加超过 1。但是，threat defense virtual 实例只会在 Management Center Virtual 上按顺序注销/注册，即逐个注销。
- 在内向扩展期间，连接耗尽时间为 300 秒。您还可以手动将耗尽时间配置为所需的时间段。
- 外部负载均衡器由提供的模板创建。不支持自定义负载均衡器公用 IP 的 DNS 要求。
- 用户必须将其现有基础设施纳入“三明治”实施模式。
- 有关外向扩展和内向扩展过程中遇到的错误的详细信息，请分析云函数的日志。
- NAT、连接到设备组的安全策略和静态路由将应用于新创建的 威胁防御。
- 如果您为多个 threat defense virtual 部署解决方案，则部署时间将增加，因为 Management Center Virtual 一次只能处理一个注册请求。当外向扩展添加多个 threat defense virtual 实例时，部署时间也会增加。目前，所有注册和取消注册均按顺序进行。
- 必须在 Management Center Virtual 中创建设备组、NAT 规则和网络对象，然后才能启动自动扩展。请注意，ILB 和 ELB IP 仅在部署解决方案后才可用。因此，您可以创建虚拟对象，并在获取实际 IP 后更新对象。

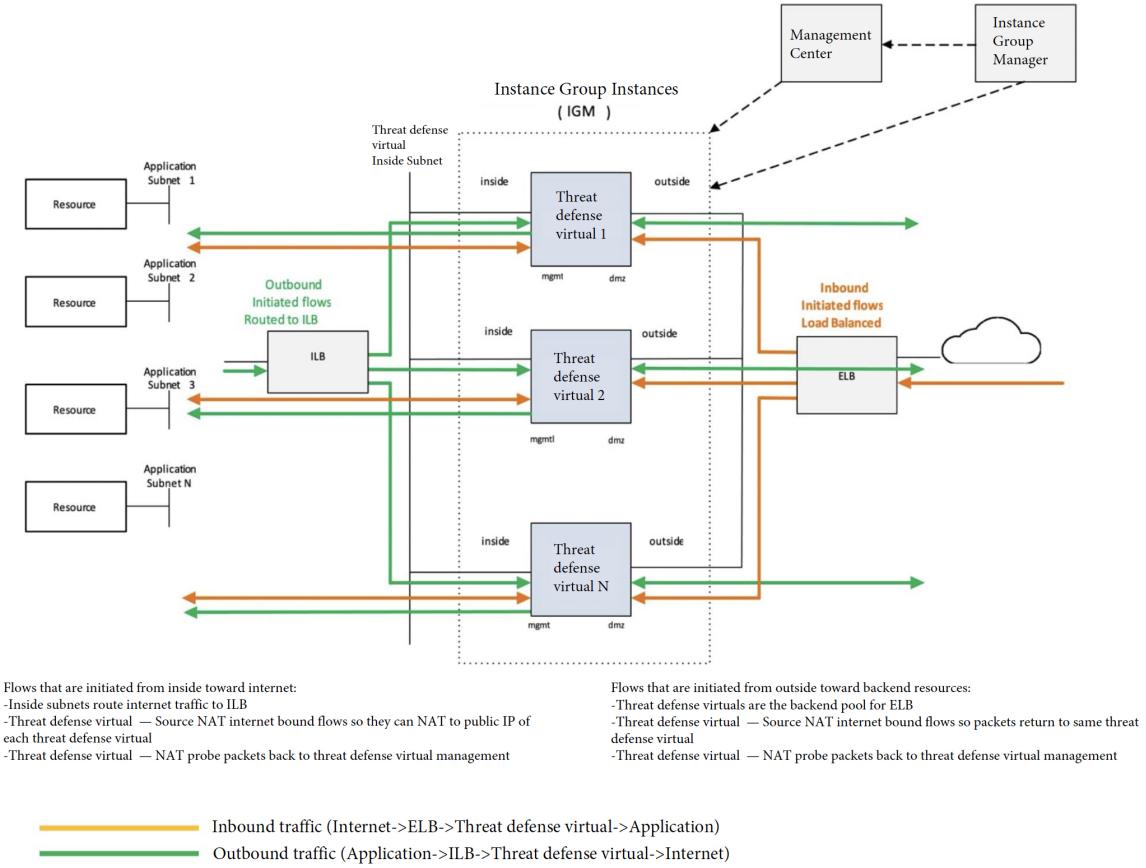
Auto Scale 使用案例

适用于 GCP 的 threat defense virtual Auto Scale 是一种自动化水平扩展解决方案，它将 threat defense virtual 实例组置于 GCP 内部负载均衡器 (ILB) 与 GCP 外部负载均衡器 (ELB) 之间。

- ELB 将流量从互联网分发到实例组中的 threat defense virtual 实例；然后，threat defense virtual 将流量转发到应用程序。
- ILB 将出站互联网流量从应用程序分发到实例组中的 threat defense virtual实例；然后，threat defense virtual 将流量转发到互联网。

- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 threat defense virtual实例数将根据负载条件自动进行扩展和配置。

图 *47: Threat Defense Virtual Auto Scale* 使用案例



在所有 Cisco Secure Firewall 版本上，您都可以使用提供的模板部署 Threat Defense Virtual 自动扩展解决方案。部署的 Threat Defense Virtual 实例至少具有 4 个接口 - 1 个管理接口、1 个诊断接口和 2 个数据接口。

从 Cisco Secure Firewall 版本 7.4.1 开始，您还可以在没有诊断界面的情况下部署 Threat Defense Virtual。同样在此场景中，使用至少 4 个接口（1 个管理接口和 3 个数据接口）完成部署。要执行此操作，请根据输入参数，第 339 页中的说明修改模板参数 *diagFirewallRule*、*diagSubnetworkName*、*diagVpcName* 和 *withDiagnostic*。

适用范围

本文档介绍部署 Threat Defense Virtual Auto Scale for GCP 解决方案的无服务器组件的详细步骤。

重要事项

- 请先阅读整个文档，然后再开始部署。
- 在开始部署之前，请确保满足前提条件。
- 请确保遵守此处所述的步骤和执行顺序。

下载部署软件包

Threat Defense Virtual Auto Scale for GCP 解决方案是一种基于 GCP 部署管理器模板的部署，它利用 GCP 提供的无服务器基础设施（云功能、负载均衡器、Pub/Sub、实例组等）。

下载启动 threat defense virtual auto scale 解决方案所需的文件。您的 threat defense virtual 版本的部署脚本和模板可从 GitHub 存储库获取。

注意 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。

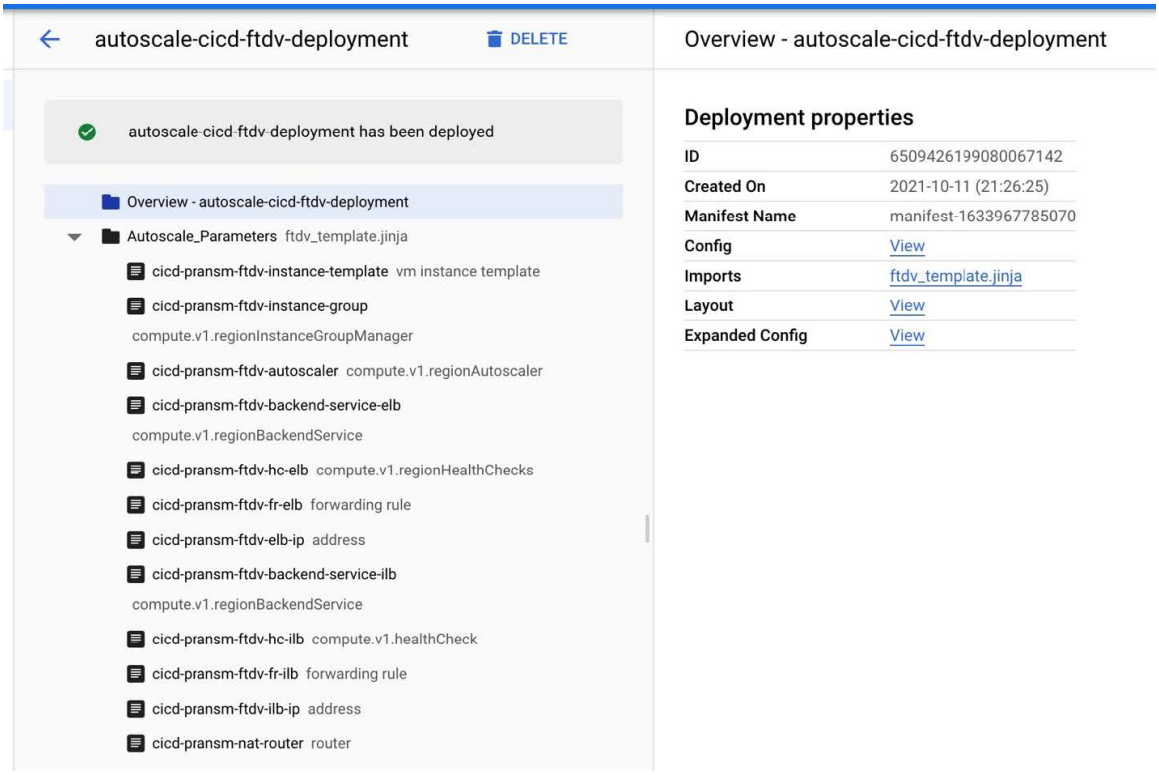
系统要求

以下组件构成了适用于 GCP 的 Threat Defense Virtual Auto Scale 解决方案。

部署管理器

- 将您的配置视为代码并执行可重复部署。Google 云部署管理器允许您使用 YAML 以说明性格式指定应用所需的所有资源。您还可以使用 Jinja2 模板来参数化配置，同时允许重复使用常见的部署范例。
- 创建定义资源的配置文件。可以不断重复创建这些资源的过程，可获得一致的结果。有关详细信息，请参阅 https://cloud.google.com/deployment-manager/docs。

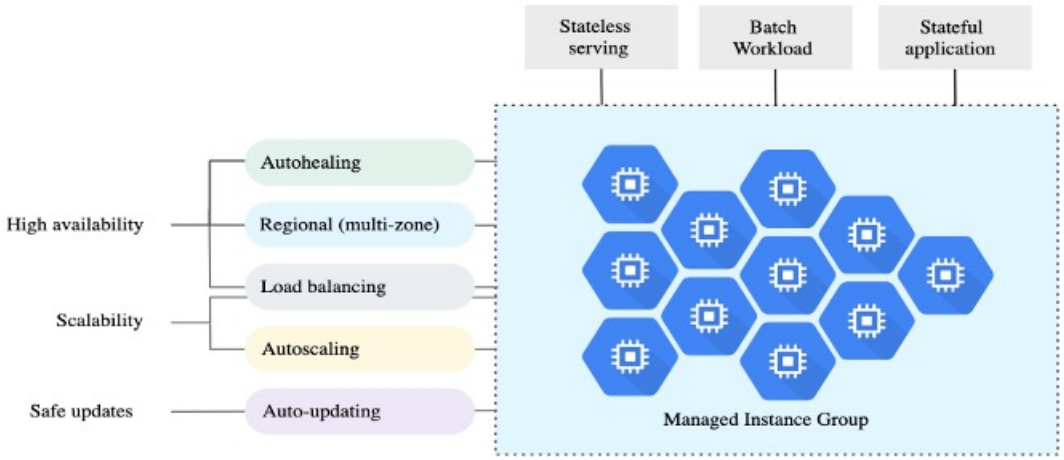
图 *48:* 部署管理器视图



GCP 中的托管实例组

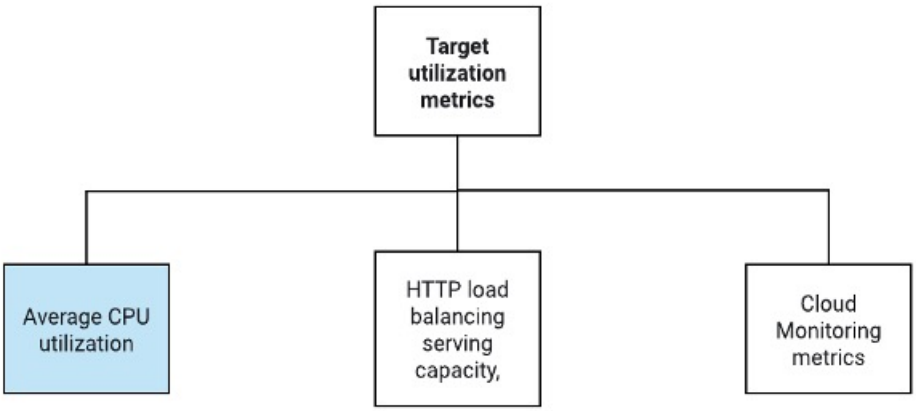
托管实例组(MIG)会根据您指定的实例模板和可选状态配置来创建其每个托管实例。有关详细信息，请参阅 https://cloud.google.com/compute/docs/instance-groups。

图 *49:* 实例组功能



目标利用率指标

- 下图显示了目标利用率指标。在制定自动扩展决策时只会使用平均 CPU 利用率指标。
- 自动扩展程序会根据所选的利用率指标来持续收集使用情况信息，将实际利用率与所需的目标利用率进行比较，并使用这些信息来确定组是需要删除实例（内向扩展）还是添加实例（外向扩展）。
- 目标利用率水平是您想要维护虚拟机 (VM) 实例的水平。例如，如果根据 CPU 利用率进行扩展，则可以将目标利用率水平设置为 75%，自动扩展程序会将指定实例组的 CPU 利用率保持在或接近 75%。每个指标的利用率水平可根据自动扩展策略进行不同的解释。有关详细信息，请参阅 https://cloud.google.com/compute/docs/autoscaler。



无服务器云功能

您可以将无服务器 Google Cloud 功能用于更改 SSH 密码、配置管理器、在 Management Center Virtual 上注册 threat defense virtual 以及从 Management Center Virtual 取消注册 threat defense virtual 等任务。

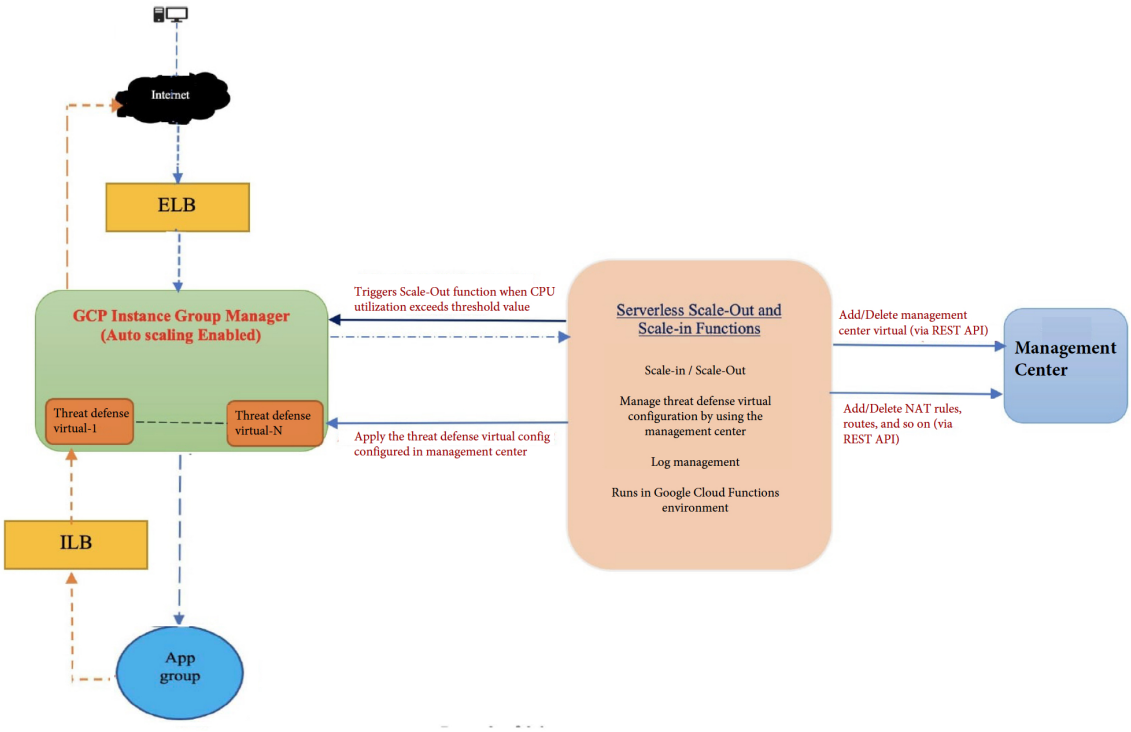
- 当在外向扩展期间实例组中出现新的 threat defense virtual 实例时，您需要执行诸如更改 SSH 密码、配置管理器、在 Management Center Virtual 上注册 threat defense virtual 以及从 Management Center Virtual取消注册 threat defense virtual 等任务。
- 在外向扩展过程中，云功能会通过云发布/订阅主题触发。您还有一个带有过滤器的日志接收器，专门用于在外向扩展时添加实例。

使用云功能取消注册无服务器许可证

- 在内向扩展期间删除实例时，您需要从 threat defense virtual 实例中取消注册许可证并从 Management Center Virtual 取消注册 threat defense virtual。
- 云功能可通过云发布/订阅主题触发。特别是对于删除过程，您有一个带有过滤器的日志接收器，专门用于在内向扩展时删除实例。
- 在触发时，云功能会通过 SSH 连接到正在删除的 threat defense virtual 实例，并运行取消注册许可证的命令。

Auto Scale 解决方案简要概述

图 *50: Auto Scale* 解决方案概述



前提条件

GCP 资源

GCP 项目

部署此解决方案的所有组件需要一个现有的或新创建的项目。

VPC 网络

确保有四个 VPC 可用/已创建。Auto Scale 部署将不会创建、更改或管理任何网络资源。

除了现有子网之外，请在具有 /28 子网的管理 VPC 网络中创建新的 VPC 连接器。云功能使用 VPC 连接器通过专用 IP 地址访问 threat defense virtual。

threat defense virtual 需要 4 个网络接口，因此您的虚拟网络需要 4 个子网以用于：

- 外部流量
- 内部流量
- 管理流量

- 诊断流量

防火墙

需要创建允许 VPC 间通信以及运行状况探测的防火墙规则。

为内部、外部、管理和诊断接口创建 4 个防火墙规则。此外，创建允许运行状况检查探测的防火墙规则。

运行状况检查探测的 IP 地址如下所示：

- 35.191.0.0/16
- 130.211.0.0/22
- 209.85.152.0/22
- 209.85.204.0/22

您必须记下稍后要在部署管理器模板中使用的防火墙标记。

应在子网所连接的网络安全组中打开以下端口：

- SSH(TCP/22) - 负载均衡器与 threat defense virtual 之间的运行状况探测所必需。无服务器函数与 threat defense virtual 之间的通信所必需。
- 应用程序特定协议/端口 - 任何用户应用程序所必需（例如，TCP/80 等）。

构建 GCP 云功能包

Threat Defense Virtual GCP Auto Scale 解决方案要求您构建两个存档文件，以压缩 ZIP 包的形式提供云功能。

- `ftdv_scalein.zip`
- `ftdv_scaleout.zip`

有关如何构建 `ftdv_scalein.zip` 和 `ftdv_scaleout.zip` 软件包的信息，请参阅 Auto Scale 部署说明。

这些函数尽可能离散以执行特定任务，并可以根据需要进行升级，以提供增强功能和新版本支持。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，您可以在将 GCP 部署管理器模板部署到 GCP 项目时使用这些参数创建 threat defense virtual 设备。

表 *29:* 模板参数

参数名	允许的值/类型	说明
resourceNamePrefix	字符串	所有资源都使用包含此前缀的名称创建。 示例：demo-test
region	GCP 支持的有效区域 [String]	将部署项目的区域的名称。 示例：us-central1
serviceAccountMailId	字符串 [Email Id]	标识服务账户的邮件地址。
vpcConnectorName	字符串	处理无服务器环境与 VPC 网络之间的流量的连接器的名称。 示例：demo-test-vpc-connector
adminPassword	字符串	Threat Defense Virtual 实例的初始密码。稍后，此参数会被更改为“newFtdPasswordSecret”。
bucketName	字符串	将上传云功能 ZIP 包的 GCP 存储桶的名称。 示例：demo-test-bkt
coolDownPeriodSec	整数	自动扩展器在开始从新实例收集信息之前应等待的秒数。 示例：30
cpuUtilizationTarget	十进制 (0,1]	自动扩展程序应维护的实例组中虚拟机的平均 CPU 使用率。 示例：0.5
deployUsingExternalIP	布尔值	确定 Threat Defense Virtual 管理是否应具有公共 IP 地址。 示例：true 如果设置为 true，则 Threat Defense Virtual 应具有公共 IP 地址。如果设置为 false，则不需要公共 IP 地址。

参数名	允许的值/类型	说明
diagFirewallRule	字符串	为诊断 VPC 创建的防火墙规则的名称。 示例：cisco-ftdv-diag-firewall-rule 如果要部署没有诊断接口的 Threat Defense Virtual，请将此参数留空或输入虚拟字符串。
diagSubnetworkName	字符串	用于诊断接口的 VPC 子网的名称。 示例：cisco-ftdv-diag-subnet 如果要部署没有诊断接口的 Threat Defense Virtual，请将此参数留空或输入虚拟字符串。
diagVpcName	字符串	用于诊断接口的 VPC 的名称。 示例：custom-ftdv-diag-vpc 如果要部署没有诊断接口的 Threat Defense Virtual，请将此参数留空或输入虚拟字符串。
elbFePorts	整数	ELB 快速以太网端口。 示例：80,22
elbIpProtocol	字符串	使用的 ELB IP 协议。 示例：TCP
elbPort	整数	ELB 端口号。 示例： 80
elbPortName	字符串	ELB 端口的名称。 示例：tcp
elbPortRange	整数	ELB 端口范围。 示例：80-80
elbProtocol	字符串	使用的 ELB 协议。 示例：TCP
elbProtocolName	字符串	ELB 协议的名称。 示例：TCP

参数名	允许的值/类型	说明
elbTimeoutSec	整数	ELB 超时期间（秒） 示例：5
elbUnhealthyThreshold	整数	运行状况检查失败的阈值数。 示例：2
fmcIP	字符串	管理中心 的 IP 地址 示例：10.61.1.2
fmcPasswordSecret 和新的 FtdPasswordSecret	字符串	创建的密钥的名称。
fmcUsername	字符串	Management Center Virtual 用户名。
ftdvCheckIntervalSec	整数	运行状况检查的间隔。 示例：300
ftdvHealthCheckPort	整数	Threat Defense Virtual 运行状况检查的端口号。 示例：22
ftdvHealthCheckProtocolName	字符串	用于运行状况检查的协议。 示例：TCP
ftdvPassword	字符串	Threat Defense Virtual 密码。
ftdvTimeoutSec	整数	Threat Defense Virtual 连接超时。 示例：300
ftdvUnhealthyThreshold	整数	运行状况检查失败的阈值数。 示例：3
grpID	字符串	在 管理中心 中创建的设备组的名称。 示例：auto-group
运行状况检查防火墙规则	字符串	允许来自运行状况检查探测 IP 范围的数据包的防火墙规则的名称。 示例：custom-ftdv-hc-firewall-rule

参数名	允许的值/类型	说明
healthCheckFirewallRuleName	字符串	允许来自运行状况检查探测 IP 范围的数据包的防火墙规则的标签。 示例：demo-test-health-allow-all
ilbCheckIntervalSec	整数	检查 ILB 连接的间隔时间。 示例：10
ilbDrainingTimeoutSec	整数	连接耗尽超时期限。 示例：60
ilbPort	整数	ILB 端口号。 示例： 80
ilbProtocol	字符串	使用的 ILB 协议。 示例：TCP
ilbProtocolName	字符串	ILB 协议名称。 示例：TCP
ilbTimeoutSec	整数	ILB 超时期限。 示例：5
ilbUnhealthyThreshold	整数	运行状况检查失败的阈值数。 示例：3
insideFirewallRule	字符串	内部防火墙规则的名称。 示例：custom-ftdv-in-firewall-rule
insideFirewallRuleName	字符串	允许在内部 VPC 中通信的防火墙规则的标签。 示例：demo-test-inside-allowall
insideGwName	字符串	内部网关的名称。 示例：inside-gateway
insideSecZone	字符串	内部安全区名称。 示例：inside-zone
insideSubnetworkName	字符串	内部子网的名称。 示例：custom-ftdv-inside-subnet

参数名	允许的值/类型	说明
insideVPCName	字符串	内部 VPC 的名称。 示例：demo-test-inside
insideVPCSubnet	字符串	内部子网的名称。 示例：demo-test-inside-subnet
licenseCAPS	字符串	所用许可证的名称。 示例：BASE,MALWARE,URL Filter,THREAT
machineType	字符串	threat defense virtual VM 的计算机类型。 示例：n1-standard-4
maxFTDCount	整数	实例组中允许的最大 Threat Defense Virtual 实例数。 示例：3
maxFTDReplicas	整数	自动扩展组中 Threat Defense Virtual 实例的最大数量。 示例：2
mgmtFirewallRule	字符串	管理防火墙规则的名称。 示例： cisco-ftdv-mgmt-firewall-rule
mgmtFirewallRuleName	字符串	允许在管理 VPC 中通信的防火墙规则的标签。 示例：demo-test-mgmt-allowall
mgmtSubnetworkName	字符串	管理子网的名称。 示例：custom-ftdv-mgmt-subnet
mgmtVPCName	字符串	管理 VPC 的名称。 示例：demo-test-mgmt
mgmtVPCSubnet	字符串	管理子网的名称。 示例：demo-test-mgmt-subnt

参数名	允许的值/类型	说明
minFTDCount	整数	在任何给定时间，实例组中可用的最小 Threat Defense Virtual 实例数。 示例：1
minFTDReplicas	整数	自动扩展组中 Threat Defense Virtual 实例的最小数量。 示例：2
natID	字符串	在 威胁防御 上注册 管理中心 时需要唯一的 NAT ID。
outsideFirewallRule	字符串	外部防火墙规则的名称。 示例：cisco-ftdv-out-firewall-rule
outsideFirewallRuleName	字符串	允许在外部 VPC 中通信的防火墙规则的标签。 示例：demo-test-outside-allowall
outsideGwName	字符串	外部网关的名称。 示例：outside-gateway
outsideSecZone	字符串	外部安全区的名称。 示例：out-zone
outsideSubnetworkName	字符串	外部子网的名称。 示例：custom-ftdv-outside-subnet
outsideVPCName	字符串	外部 VPC 的名称。 示例：demo-test-outside
outsideVPCSubnet	字符串	外部子网的名称。 示例：demo-test-outside-subnt
policyID	字符串	ACL 策略的名称。
publicKey	字符串	Threat Defense Virtual VM 的 SSH 密钥。
sourceImageURL	字符串	要在项目中使用的 Threat Defense Virtual 映像的 URL。

参数名	允许的值/类型	说明
sshUsingExternalIP	布尔值	确定 Google 函数使用的公共 IP 地址还是专用 IP 地址。 示例：true 如果设置为 true，Google 函数将使用公共 IP 地址。如果设置为 false，Google 函数将使用专用 IP 地址。
withDiagnostic	布尔值	决定部署的 Threat Defense Virtual 是否具有诊断接口。 示例：true 如果设置为 true，则部署的 Threat Defense Virtual 将具有诊断接口。如果设置为 false，则部署的 Threat Defense Virtual 没有诊断接口。

部署 Auto Scale 解决方案

过程

步骤 1 将 Git 存储库克隆到本地文件夹。

```
git clone git_url -b branch_name
```

步骤 2 在 gcloud CLI 中创建存储桶。

```
gsutil mb -c nearline gs://bucket_name
```

注释
在系统上安装的 Google Cloud Shell 或 Google Cloud SDK 中运行此程序中的任何 **gsutil** 或 **gcloud** 命令。

步骤 3 构建压缩的 Zip 包：

a) 从文件夹 `ftdv_scaleout` 和 `ftdv_scalein` 创建包含以下文件的压缩 Zip 包。

- main.py
- basic_functions.py
- fmc_functions.py
- requirements.txt

注释
在 main.py 文件中，如果使用内部 IP 地址，请使用 **ssh_ip = response[‘networkInterfaces’] [2] [‘networkIP’]** 命令。如果使用外部 IP 地址，请输入 **ssh_ip = response[‘networkInterfaces’] [2] [‘accessConfigs’] [0] [‘natIP’]** 命令。此外，此函数中添加了两个静态路由。您可以使用 **fmc.create_static_network_route (vm_name, ‘outside’, ‘any_ipv4’, os.getenv(“OUTSIDE_GW_NAME”), metric=1)** 和 **fmc.create_static_network_route (vm_name, ‘inside’, ‘any_ipv4’, os.getenv(“INSIDE_GW_NAME”), metric=2)** 命令修改静态路由。

b) 将压缩的 Zip 包重命名为 `ftdv_scaleout.zip` 和 `ftdv_scalein.zip`。

注释
在文件夹中导航，选择文件，右键点击，然后选择“压缩 | 存档”(compress | archive) 以生成 GCP 可以读取的 .zip。

步骤 4 将压缩的 Zip 包（`ftdv_scaleout.zip` 和 `ftdv_scalein.zip`）上传到云编辑器工作空间。

步骤 5 将部署管理器模板中的以下文件上传到云编辑器工作区内。

- ftdv_predeployment.yaml
- ftdv_predeployment.jinja
- ftdv_parameters.yaml
- ftdv_template.jinja

步骤 6 将压缩的 Zip 包复制到存储桶。

- `gsutil cp ftdv_scaleout.zip gs://bucket_name`
- `gsutil cp ftdv_scalein.zip gs://bucket_name`

步骤 7 为内部、外部、管理和诊断接口创建 VPC 和子网。

在管理 VPC 中，您需要有 /28 子网，例如 10.8.2.0/28。

步骤 8 您需要为内部、外部、管理和诊断接口制定四个防火墙规则。此外，您还应设置允许运行状况检查探测的防火墙规则。

步骤 9 使用密钥管理器 GUI 为以下对象创建两个密钥。请参阅https://console.cloud.google.com/security/secret-manager。

- fmc-password
- ftdv-new-password

步骤 10 创建 VPC 连接器。

```
gcloud beta compute networks vpc-access connectors create <vpc-connector-name>
--region <region> --subnet=</28 subnet name>
```

示例：

```
gcloud beta compute networks vpc-access connectors create demo-vpc-connector
--region us-central1 --subnet=outside-connect-28
Create request issued for: [demo-vpc-connector]
```

```
Waiting for operation [projects/asavgcp-poc-4krn/locations/us-central1/operations/
10595de7-837f-4c19-9396-0c22943ecf15] to complete...done.
Created connector [demo-vpc-connector].
```

步骤 11 在任何具有公用 IP 的公共云平台上部署 Management Center Virtual。有关如何在各种公共云平台上部署 Management Center Virtual 的详细信息，请参阅《Cisco Secure Firewall Management Center Virtual 入门指南》。

注释
对已部署的 Management Center Virtual 实例执行步骤 12 至 16。

步骤 12 在 Management Center Virtual 实例上 - 为 Management Center Virtual 创建用户 restapi，并使用保存在 fmcpassword 密钥中的相同密码。有关详细信息，请参阅用户。

步骤 13 在 Management Center Virtual 实例上 - 创建设备组、访问控制策略和访问控制规则。有关详细信息，请参阅添加设备组、创建基本访问控制策略和创建和编辑访问控制规则。

步骤 14 在 Management Center Virtual 实例上 - 创建下面给出的对象。有关如何在 Management Center Virtual 上创建对象的详细信息，请参阅对象管理。

- ELB-IP
- ILB-IP
- Application-IP
- 运行状况检查 IP 范围 (4)
- 元数据

```
object network hc1
  subnet 35.191.0.0 255.255.0.0
object network metadata
  host 169.254.169.254
object network ilb-ip
  host 10.52.1.218
object network hc2
  subnet 130.211.0.0 255.255.252.0
object network elb-ip
  host 34.85.214.40
object network hc3
  subnet 209.85.152.0 255.255.252.0
object network hc4
  subnet 209.85.204.0 255.255.252.0
object network inside-linux
  host 10.52.1.217
object network outside-gateway
  host <>
object network inside-gateway
  host <>
```

步骤 15 在 Management Center Virtual 实例上 - 创建安全区（接口对象）。有关详细信息，请参阅创建安全区域和接口组对象。

- inside-security-zone
- outside-security-zone

步骤 16 在 Management Center Virtual 实例上 - 创建 NAT 策略和 NAT 规则。有关详细信息，请参阅网络地址转换。

```
nat (inside,outside) source dynamic hc1 interface destination static ilb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (inside,outside) source dynamic hc2 interface destination static ilb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (inside,outside) source dynamic any interface
nat (outside,inside) source dynamic hc1 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc2 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc3 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc4 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic any interface destination static elb-ip inside-linux
```

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
1	⇗	D...	inside-zone	outside-zone	hc1	ilb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
2	⇗	D...	inside-zone	outside-zone	hc2	ilb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
3	⇗	D...	inside-zone	outside-zone	any-ipv4			Interface			Dns:false
4	⇗	D...	outside-zone	inside-zone	hc1	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
5	⇗	D...	outside-zone	inside-zone	hc2	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
6	⇗	D...	outside-zone	inside-zone	hc3	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
7	⇗	D...	outside-zone	inside-zone	hc4	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
8	⇗	D...	outside-zone	inside-zone	any-ipv4	elb-ip		Interface	inside-linux		Dns:false

步骤 17 为预部署和 Threat Defense Virtual Autoscale 部署更新 Jinja 和 YAML 文件中的参数。

a) 打开 `ftdv_predeployment.yaml` 文件并更新以下参数。

- **resourceNamePrefix**: <resourceNamePrefix>
- **region**: <region>
- **serviceAccountMailId**: <serviceAccountMailId>
- **vpcConnectorName**: <VPC-Connector-Name>
- **bucketName**: <bucketName>
- **fmcIP**: <管理中心-IP-address>
- **regID**: <registration-ID>
- **natID**: <unique-NAT-ID>
- **grpID**: <device-group-name>
- **policyID**: <acl-policy-name>
- **licenseCAPS**: <licenses>
- **fmcPasswordSecret**: <管理中心-password>

- **newFtdPasswordSecret**: <new-threat defense virtual-password>
- **fmcUsername**: <username>
- **ftdvPassword**: <password>
- **outsideGwName**: <outside-gateway-name>
- **insideGwName**: <inside-gateway-name>
- **outsideSecZone**: <outside-security-zone>
- **insideSecZone**: <inside-security-zone>
- **sshUsingExternalIP**: <true/false>

b) `ftdv_predeployment.jinja` 文件采用 `ftdv_predeployment.yaml` 文件中的参数。

c) 打开 `ftdv_parameters.yaml` 文件并更新以下参数。

VPC and Firewall Parameters

- **mgmtVpcName**: <mgmt-vpc-name>
- **diagVpcName**: <diagnostic-vpc-name>
- **outsideVpcName**: <outside-vpc-name>
- **insideVpcName**: <inside-vpc-name>
- **mgmtSubnetworkName**: <mgmt-subnet-name>
- **diagSubnetworkName**: <diagnostic-subnet-name>
- **outsideSubnetworkName**: <outside-subnet-name>
- **insideSubnetworkName**: <inside-subnet-name>
- **mgmtFirewallRule**: <mgmt-firewall-rule>
- **diagFirewallRule**: <diagnostic-firewall-rule>
- **outsideFirewallRule**: <outside-firewall-rule>
- **insideFirewallRule**: <inside-firewall-rule>
- **healthCheckFirewallRule**: <healthcheck-firewall-rule>
- **adminPassword**: <initial-threat defense virtual-password>
- **deployUsingExternalIP**: <true/false>

Instance Template parameters

- **machineType**: <machine-type>
- **sourceImageURL**: <source-image-URL>

FTDv Health Check

- **ftdvHealthCheckPort**: <port-number>
- **ftdvCheckIntervalSec**: <interval-in-seconds>
- **ftdvTimeoutSec**: <timeout-in-seconds>
- **ftdvHealthCheckProtocolName**: <protocol-name>
- **ftdvUnhealthyThreshold**: <threshold-count>

FTDv Autoscaler

- **cpuUtilizationTarget**: <percentage-in-decimals (for example, 0.7)>
- **coolDownPeriodSec**: <cooldown-period-in-seconds>
- **minFTDReplicas**: <min-number-of-FTDv-instances>
- **maxFTDReplicas**: <max-number-of-FTDv-instances>

ELB Services

- **elbPort**: <port-number>
- **elbPortName**: <port-name>
- **elbProtocol**: <protocol-name>
- **elbTimeoutSec**: <timeout-in-seconds>
- **elbProtocolName**: <protocol-name>
- **elbUnhealthyThreshold**: <threshold-number-for-failed-health-checks>
- **elbIpProtocol**: <IP-Protocol>
- **elbPortRange**: <port-range>
- **elbFePorts**: <fast-ethernet-ports>

ILB Services

- **ilbProtocol**: <protocol-name>
- **ilbDrainingTimeoutSec**: <timeout-in-seconds>
- **ilbPort**: <port-number>
- **ilbCheckIntervalSec**: <interval-in seconds>
- **ilbTimeoutSec**: <timeout-in-seconds>
- **ilbProtocolName**: <protocol-name>
- **ilbUnhealthyThreshold**: <threshold-number-for-failed-health-checks>

注释
对于 threat defense virtual Auto Scale，设置了 **cpuUtilizationTarget: 0.5** 参数，您可以根据自己的要求对其进行编辑。此值表示所有 threat defense virtual 实例组的 CPU 使用率为 50%。

d) `ftdv_template.jinja` 文件从 `ftdv_parameters.yaml` 文件获取参数。

步骤 18 部署预部署 YAML 配置。

```
gcloud deployment-manager deployments create <pre-deployment-name>
--config ftdv_predeployment.yaml
```

示例：

```
gcloud deployment-manager deployments create demo-predeployment
--config ftdv_predeployment.yaml

The fingerprint of the deployment is b'9NOy0gsTPgg16SqUEVsBjA=='
Waiting for create [operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c]...done.
Create operation operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c
completed successfully
```

步骤 19 创建 threat defense virtual Auto Scale 部署。

```
gcloud deployment-manager deployments create <deployment-name>
--config ftdv_parameters.yaml
```

示例：

```
gcloud deployment-manager deployments create demo-asav-autoscale
--config ftdv_parameters.yaml
The fingerprint of the deployment is b'1JCQi7Il-laWOY7vOLza0g=='
Waiting for create [operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16]...done.
Create operation operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16
completed successfully.
```

步骤 20 为 ILB 创建路由，以便将数据包从内部应用转发到互联网。

```
gcloud beta compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```

示例：

```
gcloud beta compute routes create demo-ilb --network=sdt-test-asav-inside
--priority=1000 --destination-range=0.0.0.0/0 --next-hop-ilb=demo-asav-fr-ilb
--next-hop-ilb-region=us-central1
Created [https://www.googleapis.com/compute/beta/projects/asavgcp-poc-4krn/global
/routes/demo-ilb].
```

Auto Scale 逻辑

- 自动调节程序将目标 CPU 利用率水平视为实例组中一段时间内所有 vCPU 的平均使用量的一部分。
- 如果总 vCPU 的平均利用率超过目标利用率，则自动扩展程序会添加更多 VM 实例。如果总 vCPU 的平均利用率低于目标利用率，则自动扩展程序会删除实例。

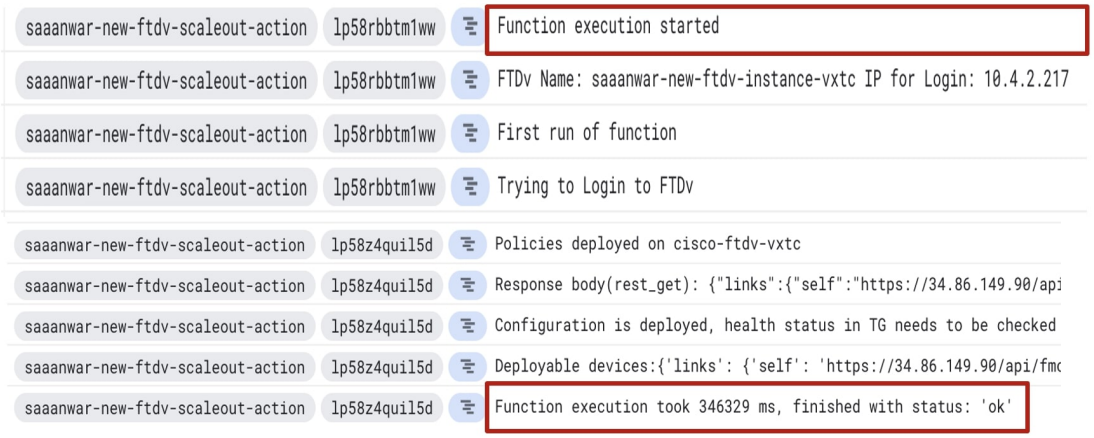
- 例如，设置 0.75 的目标利用率会告知自动扩展程序将实例组中所有 vCPU 的平均利用率保持在 75%。
- 扩展决策中只会使用 CPU 利用率指标。
- 该逻辑基于以下假设：负载均衡器将尝试在所有 threat defense virtual 之间平均分配连接，一般来说，所有 threat defense virtual 应平均加载。

日志记录和调试

可以按如下方式查看云功能的日志。

- 外向扩展函数日志

图 *51:* 外向扩展函数日志



在上面给出的外向扩展函数日志中， **Function execution started** 和 **Function execution took 346329 ms, finish with status: ‘ok’** 条目分别表示功能日志的开始和结束。您还可以跟踪其他操作，例如首次函数运行、threat defense virtual 登录、策略部署等。

- 内向扩展函数日志

在上面给出的外向扩展函数日志中，**Function execution started** 和 **Function execution took 50852 ms, finish with status: 'ok'** 条目分别表示功能日志的开始和结束。您还可以跟踪其他操作，例如取消注册过程的启动、取消注册的状态、获取新的 authToken 等。

故障排除

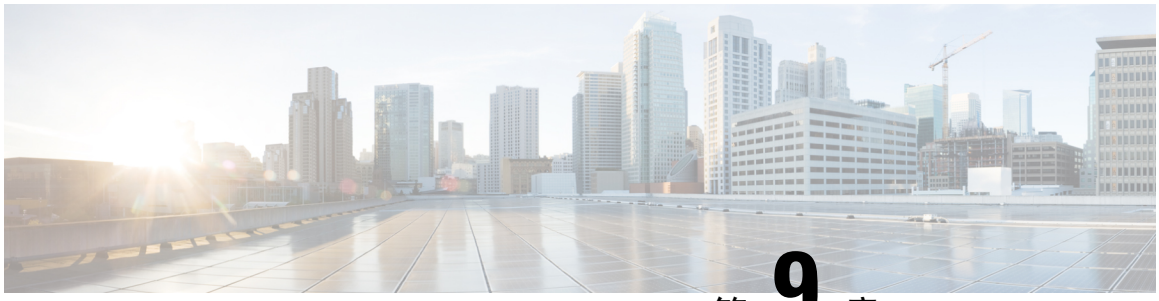
以下是适用于 GCP 的 Threat Defense Virtual Auto Scale 的常见错误情况和调试提示：

- `main.py` 未找到 - 确保仅从文件生成 Zip 软件包。您可以转到云功能并检查文件树。不应有任何文件夹。
- 部署模板时出错-确保在 jinja 和 yaml 中填写了“<>”内的所有参数值，或检查是否已存在同名部署。
- Google 函数无法访问 threat defense virtual - 确保已创建 VPC 连接器并在 YAML 参数文件中提及了相同的名称。
- SSH 连接 threat defense virtual 时身份验证失败 - 确保公共密钥和私钥对正确无误。
- 未找到身份验证令牌 - 确保密钥中的 Management Center Virtual 密码正确。
- 运行状况不正常 threat defense virtual 和流量问题 - 确保防火墙规则和路由中没有问题。
- 无法手动登录 threat defense virtual - 确保您使用的是新密码。旧密码通过外向扩展函数进行更改。
- 无法在 Management Center Virtual 上注册设备 - 确保可从 Management Center Virtual 访问 threat defense virtual。threat defense virtual 和 Management Center Virtual 的管理接口应位于同一子网中。
- 由于启动运行状况探测请求，在 ILB 和 threat defense virtual 之间形成环路的保留连接会导致高 CPU 使用率。要降低高 CPU 使用率，可以使用以下选项之一：

  选项 1 - 在 Management Center Virtual 上，禁用数据接口，配置运行状况探测 NAT 规则，并启用数据接口。有关数据接口和 NAT 的详细信息，请参阅接口概述和网络地址转换。

  选项 2 - 从 Management Center Virtual 应用运行状况探测 NAT 规则后，登录到 threat defense virtual 控制台，然后使用 **clear conn** 命令。如果已设置集群，请使用 **cluster exec clear conn** 命令。

  在 threat defense virtual 控制台上使用 **show cpu** 命令验证 CPU 使用率。



第 9 章

在思科 HyperFlex 上部署 Threat Defense Virtual

本章介绍在 vCenter 服务器或独立 ESXi 主机上的思科 HyperFlex 上部署 threat defense virtual 的程序。

概述

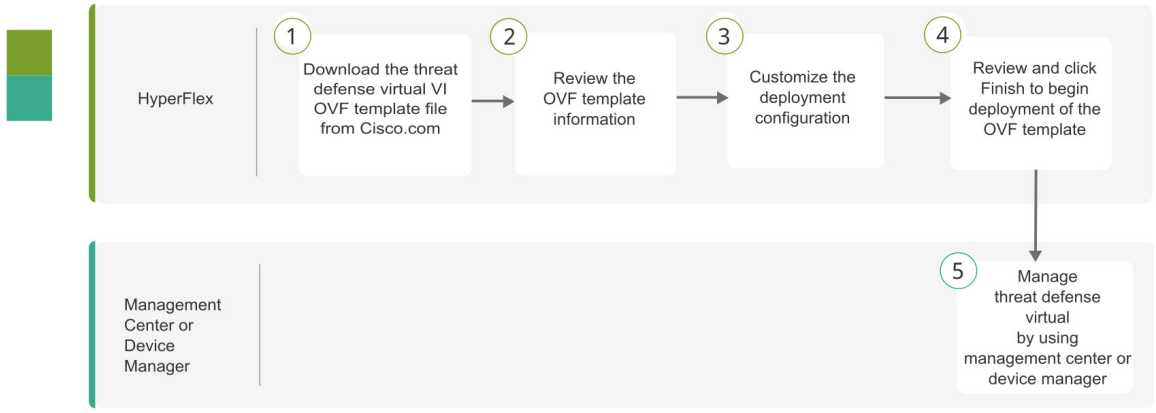
Cisco Cisco Secure Firewall Threat Defense Virtual （之前称为 Firepower Threat Defense Virtual）将 Cisco Secure Firewall 功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

HyperFlex 系统可为任何应用程序和任何位置提供超融合。通过思科 Intersight 云运营平台管理的 HyperFlex 采用了思科统一计算系统 (Cisco UCS) 技术，可以在任何地方为应用程序和数据提供支持，优化从核心数据中心到边缘和公共云的运营，从而通过加速 DevOps 实践来提高灵活性。

本章介绍 threat defense virtual 如何在思科 HyperFlex 环境中工作，包括功能支持、系统要求、准则和限制。本章还介绍了管理 threat defense virtual 的选项。在开始部署之前，了解您的管理选项非常重要。您可以使用 Cisco Secure Firewall Management Center （以前称为 Firepower Management Center）或 Cisco Secure Firewall 设备管理器 （以前称为 Firepower Device Manager）来管理和监控 threat defense virtual。其他管理选项也可能可用。

端到端程序

以下流程图说明了在思科 HyperFlex 上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Hyperflex	部署 Threat Defense Virtual：从 Cisco.com 下载Threat Defense Virtual VI OVF 模板文件。
2	Hyperflex	部署 Threat Defense Virtual：查看 OVF 模板信息。
3	Hyperflex	部署 Threat Defense Virtual：自定义部署配置。
4	Hyperflex	部署 Threat Defense Virtual：查看并验证显示的信息。点击“完成”(Finish) 开始部署 OVF 模板。
5	管理中心或设备管理器	管理 Threat Defense Virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual • 使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual

系统要求

版本

管理器版本	设备版本
设备管理器 7.0	威胁防御 7.0
管理中心 7.0	

有关 threat defense virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

Threat Defense Virtual 内存、磁盘和 vCPU 大小估算

根据所需部署的实例数量和使用要求， threat defense virtual 部署所使用的具体硬件可能会有所不同。每个 threat defense virtual 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

设置	值
性能级别	**7.0 及更高版本** threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。 • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) 请参阅*Cisco Secure Firewall Management Center* 配置 中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。
存储	取决于所选磁盘格式。 • 调配磁盘大小为 48.24 GB。

设置	值
vNIC	threat defense virtual 支持以下虚拟网络适配器： • **VMXNET3**-在 threat defense virtual 上，如果创建虚拟设备，现默认为 VMXNET3 接口。先前，默认值为 e1000。（7.1 及更高版本）vmxnet3 驱动程序使用第一个以太网适配器进行管理。第二个适配器未使用。（7.0 及更早版本） VMXNET3 驱动程序使用两个管理接口。前两个以太网适配器必须配置为管理接口：一个用于设备管理/注册，一个用于诊断。

Threat Defense Virtual许可证

- 所有安全服务的许可证授权均在 管理中心中配置。
- 有关如何管理许可证的更多信息，请参阅《Cisco Secure firewall Management Center 配置指南》中的系统许可。

HyperFlex HX 系列的配置和集群

配置	集群
HX220c 融合节点	• 闪存集群 • 最少 3 个节点集群（数据库、VDI、VSI）
HX240c 融合节点	• 闪存集群 • 最少 3 个节点集群（VSI：IT/商业应用、测试/开发）
HX220C 和 Edge（VDI、VSI、ROBO） HX240C（VDI、VSI、测试/开发	• 混合集群 • 最少 3 个节点集群
B200 + C240/C220	计算绑定应用/VDI

HyperFlex HX 系列的部署选项：

- 混合集群
- 闪存集群
- HyperFlex 边缘
- SED 驱动器
- NVME 缓存

- GPU

有关 HyperFlex HX 云支持的管理选项，请参阅思科 HyperFlex 系统安装指南中的部署 *HyperFlex* 交换矩阵互联连接的集群部分。

HyperFlex 组件和版本

组件	版本
VMware vSphere/VMware ESXI	7.0 有关威胁防御虚拟与 VMware vSphere/VMware ESXI 的兼容性的详细信息，请参阅威胁防御虚拟兼容性：VMware。
HyperFlex 数据平台	4.5.1a-39020 及更高版本 。

准则和限制

支持的功能

- 部署模式 - 路由（独立）、路由 (HA)、内联分流、内联、被动和透明
- 许可 - 仅 BYOL
- IPv6
- Threat Defense Virtual 本地 HA
- 巨型帧
- HyperFlex 数据中心集群（不包括扩展集群）
- HyperFlex Edge 集群
- HyperFlex 全 NVMe、全闪存和混合融合节点
- HyperFlex 纯计算节点

不支持的功能

与 SR-IOV 一起运行的 Threat Defense Virtual 尚未通过 HyperFlex 的认证。

注释 HyperFlex 支持 SR-IOV，但除 MLOM VIC 外还需要 PCI-e NIC。

一般准则

要为 HyperFlex 配置 vSwitch，可以使用 GUI 或命令行界面。在安装多个 ESX 服务器并计划编写 vSwitch 配置脚本时，这些配置非常有用。有关详细信息，请参阅《思科 HyperFlex 系统网络和外部存储管理指南》中的“配置 vSwitch”部分。

以下是 threat defense virtual 接口的网络适配器、源网络和目标网络的对应关系：

网络适配器	源网络	目标网络	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	Diagnostic0-0	诊断	诊断
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部
网络适配器 5	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（可选）
网络适配器 6	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
...直到网络适配器 10			

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 HyperFlex 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

修改 vSphere 标准交换机的安全策略设置

对于 vSphere 标准交换机，第 2 层安全策略的三个要素分别是混合模式、MAC 地址更改和伪传输。threat defense virtual 在混合模式下运行，并且 threat defense virtual 的高可用性依赖于主用和备用设备之间的 MAC 地址切换，从而保证正确运行。

默认设置会阻碍 threat defense virtual 的正确运行。请参见以下要求的设置：

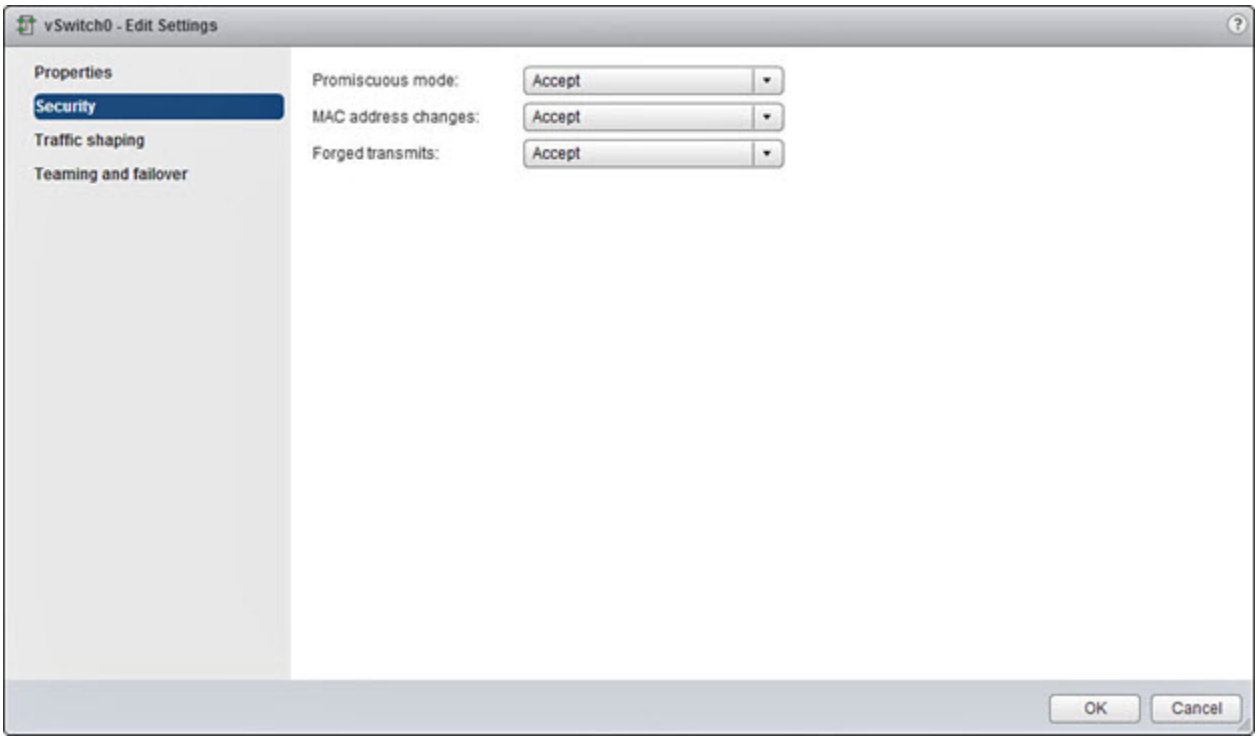
表 *30: vSphere* 标准交换机安全策略选项

选项	要求的设置	操作
混合模式	接受	您必须在 vSphere Web 客户端中编辑 vSphere 标准交换机的安全策略，并将混合模式选项设置为“接受”。 防火墙、端口扫描程序、入侵检测系统等等需要在混合模式下运行。
MAC 地址更改	接受	您应该在 vSphere Web 客户端中检验 vSphere 标准交换机的安全策略，确认 MAC 地址更改选项已设为“接受”。
伪传输	接受	您应该在 vSphere Web 客户端中检验 vSphere 标准交换机的安全策略，确认伪传输选项已设为“接受”。

使用以下程序配置 threat defense virtual 的正确操作的默认设置。

1. 在 vSphere Web 客户端中，导航至 HyperFlex 集群。
2. 在**管理 (Manage)** 选项卡中，点击**网络 (Networking)**，然后选择**虚拟交换机 (Virtual switches)**。
3. 从列表中选择一个标准交换机，然后点击**编辑设置 (Edit settings)**。
4. 选择**安全**，查看当前设置。
5. 在连接到标准交换机的虚拟机的访客操作系统中**接受**混合模式激活、MAC 地址更改和伪传输。

图 *52: vSwitch* 编辑设置



6. 点击**确定 (OK)**。

注释 确保在为 threat defense virtual 上的管理和故障切换 (HA) 接口所配置的所有网络上，这些设置是相同的。

相关文档

思科 HX 数据平台的版本说明

Cisco HX 数据平台配置指南

适用于采用 VMware ESXi 的虚拟服务器基础设施的思科 HyperFlex 4.0

思科 HyperFlex 系统解决方案概述

思科 HyperFlex 系统文档规划图

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您有两个选择来管理您的 Cisco Secure Firewall Threat Defense Virtual。

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。

重要事项 您不能同时使用 设备管理器 和 管理中心 来管理 威胁防御 设备。在启用 设备管理器 集成管理功能后，将无法使用 管理中心 来管理 威胁防御 设备，除非您禁用本地管理功能并重新配置管理功能以使用 管理中心。另一方面，当您向 威胁防御 注册 管理中心 设备时，设备管理器 载入管理服务会被禁用。

注意 目前，思科不提供将 设备管理器 配置迁移到 管理中心 的选项，反之亦然。选择为 威胁防御 设备配置的管理类型时，请考虑这一点。

Cisco Secure Firewall 设备管理器

设备管理器 板载集成的管理器。

设备管理器 是基于 Web 的配置界面，包含在某些 威胁防御 设备上。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

注释 有关支持 设备管理器 的 威胁防御 设备的列表，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

概述

您可以在 VMware vCenter 服务器上将 threat defense virtual 部署到思科 HyperFlex。

要成功部署 threat defense virtual，您必须熟悉 VMware 和 vSphere，包括 vSphere 联网、ESXi 主机设置和配置，以及虚拟机访客部署。

适用于思科 HyperFlex 的 threat defense virtual 使用开放虚拟化格式 (OVF) 进行分发，这是一种打包和部署虚拟机的标准方法。VMware 提供多种调配 vSphere 虚拟机的方法。适合您环境的最佳方式取决于您基础设施的规模和类型以及您想要实现的目标。

您可以使用 VMware vSphere Web 客户端访问您的思科 HyperFlex 环境。

部署 Threat Defense Virtual

使用此程序将 threat defense virtual 设备部署到 vSphere vCenter 服务器上的思科 HyperFlex。

开始之前

- 确保您已部署思科 HyperFlex 并执行了所有安装后配置任务。有关详细信息，请参阅思科 HyperFlex 系统文档规划图。
- 在部署 threat defense virtual 之前，您必须在 vSphere 中配置至少一个网络（用于管理）。
- 从 Cisco.com 下载 threat defense virtual VI OVF 模板文件：*Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*，其中 *X.X.X-xxx* 是版本和内部版本号。

过程

步骤 1 登录 vSphere Web 客户端。

步骤 2 选择要部署 threat defense virtual 的 HyperFlex 集群，然后点击**操作 (ACTIONS)** > **部署 OVF 模板 (Deploy OVF Template)**。

步骤 3 浏览文件系统以找到 OVF 模板源位置，然后点击**下一步 (NEXT)**。

选择 threat defense virtual VI OVF 模板：

Cisco_Secure_Firewall_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf

其中，*X.X.X-xxx* 是已下载的存档文件的版本和内部版本号。

步骤 4 为 threat defense virtual 指定名称和位置，然后点击**下一步 (NEXT)**。

步骤 5 选择计算资源，并等待兼容性检查完成。

如果兼容性检查成功，请点击**下一步 (NEXT)**。

步骤 6 查看 OVF 模板信息（产品名称、版本、供应商、下载大小、磁盘上的大小和说明），然后点击**下一步 (NEXT)**。

步骤 7 审查并接受与 OVF 模板一起打包的许可协议（仅限 VI 模板），然后点击**下一步 (NEXT)**。

步骤 8 选择部署配置（vCPU/内存值），然后点击**下一步 (NEXT)**。

步骤 9 选择存储位置和虚拟磁盘格式，然后点击**下一步 (NEXT)**。

在此窗口中，您可以从目标 HyperFlex 集群上已配置的数据存储中选择。存储在数据存储上的虚拟机配置文件和虚拟磁盘文件。选择一个足够大的数据存储，以容纳虚拟机及其所有虚拟磁盘文件。

如果选择**密集调配 (Thick Provisioned)** 作为虚拟磁盘格式，则会立即分配所有存储。如果选择**精简调配 (Thin Provisioned)** 作为虚拟磁盘格式，则会在数据写入虚拟磁盘时将按需分配存储。精简调配还可缩短虚拟设备的部署时间。

步骤 10 将 OVF 模板中指定的网络映射到清单中的网络，然后点击**下一步 (NEXT)**。

确保将 Management0-0 接口关联到可以从互联网访问的 VM 网络。非管理接口可从 管理中心 或 设备管理器 配置，具体取决于您的管理模式。

网络可能没有按字母顺序排序。如果很难找到您的网络，可以稍后在**编辑设置**对话框中更改网络。在部署后，右键点击 threat defense virtual 实例，然后选择**编辑设置**。但是，该屏幕不会显示 threat defense virtual ID（仅显示网络适配器 ID）。

请查看适用于 threat defense virtual 接口的以下网络适配器、源网络和目标网络的一致性（注意这些是默认的 vmxnet3 接口）：

网络适配器	源网络	目标网络	功能
网络适配器 1	Management0-0	Management0/0	管理
网络适配器 2	Diagnostic0-0	Diagnostic0/0	诊断
网络适配器 3	GigabitEthernet0-0	GigabitEthernet0/0	外部数据
网络适配器 4	GigabitEthernet0-1	GigabitEthernet0/1	内部日期
网络适配器 5	GigabitEthernet0-2	GigabitEthernet0/2	数据流量（可选）
网络适配器 6	GigabitEthernet0-3	GigabitEthernet0/3	数据流量（可选）
网络适配器 7	GigabitEthernet0-4	GigabitEthernet0/4	数据流量（可选）
网络适配器 8	GigabitEthernet0-5	GigabitEthernet0/5	数据流量（可选）
网络适配器 9	GigabitEthernet0-6	GigabitEthernet0/6	数据流量（可选）
网络适配器 10	GigabitEthernet0-7	GigabitEthernet0/7	数据流量（可选）

部署 threat defense virtual 时，总共可以有 10 个接口。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。您无需使用 threat defense virtual 的所有接口。对于您不打算使用的接口，只需在 threat defense virtual 配置中禁用即可。

步骤 11 设置与 OVF 模板一起打包的用户可配置的属性：

注释
建议在此步骤中强制配置所有必需的自定义设置。如果未配置所有必需的自定义，则必须在部署后登录 CLI 以完成设置。有关说明，请参阅使用 CLI 完成 Threat Defense Virtual 设置，第 367 页。

a) **密码**

设置 threat defense virtual 管理员访问的密码。

b) **网络**

设置网络信息，包括完全限定的域名 (FQDN)、DNS、搜索域和网络协议（IPv4 或 IPv6）。

c) **管理**

设置管理模式。点击**启用本地管理器**的下拉箭头，然后选择**是**使用集成的基于 Web 的 设备管理器配置工具。选择**否 (No)** 以使用 管理中心 来管理此设备。

d) 防火墙模式

设定初始防火墙模式。点击**防火墙模式**的下拉箭头，然后选择两种支持的模式之一；**已路由**或**透明**。

如果对**启用本地管理器**选择**是**，则只能选择**已路由**防火墙模式。不能使用本地 设备管理器 配置透明防火墙模式接口。

e) 注册

如果对**启用本地管理器**选择**否**，则需要提供必要的凭证以将此设备注册到负责管理的 **Firepower 管理中心**。提供以下各项：

- **负责管理的防御中心** - 输入 管理中心 的主机名或 IP 地址。
- **注册密钥** - 注册密钥是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。当将设备添加到 管理中心时，您必须记住此注册密钥。
- **NAT ID** - 如果 threat defense virtual 和 管理中心 被网络地址转换 (NAT) 设备分隔，并且 管理中心 位于 NAT 设备后方，请输入一个唯一的 NAT ID。这是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。

f) 点击**下一步 (NEXT)**。

步骤 12 查看并验证显示的信息。要使用这些设置开始部署，点击**完成 (FINISH)**。要进行更改，点击**后退 (BACK)** 以在屏幕中向后导航。

完成该向导后，vSphere Web 客户端将处理虚拟机；您可以在**全局信息**区域的**最近任务**窗格中看到“初始化 OVF 部署”状态。

完成后，您会看到“部署 OVF 模板”完成状态。

在“清单”中的指定数据中心下会显示 threat defense virtual 虚拟实例。启动新的 VM 最多可能需要 30 分钟。

注释
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，需要执行其他配置，以实现互联网访问和成功注册许可证。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

注释 如果在部署 threat defense virtual 时未配置所有必需的自定义，则必须使用 CLI 完成设置。有关说明，请参阅使用 CLI 完成 Threat Defense Virtual 设置，第 367 页。

使用 CLI 完成 Threat Defense Virtual 设置

如果在部署 threat defense virtual 时未配置所有必需的自定义，则必须使用 CLI 完成设置。

过程

步骤 1 打开 VMware 控制台。

步骤 2 在 **firepower login** 提示符下，使用默认凭据（用户名 **admin**，密码 **Admin123**）登录。

步骤 3 当 威胁防御系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式（本地管理使用 设备管理器）。

步骤 4 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

当实施设置时，VMware 控制台可能显示消息。

步骤 5 根据提示完成系统配置。

步骤 6 当控制台返回到 # 提示符时，验证设置是否成功。

注释
要向思科许可颁发机构成功注册 threat defense virtual，threat defense virtual需要访问互联网。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

启用巨型帧

MTU 越大，能发送的数据包就越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 匹配流量路径上的 MTU - 我们建议您将流量路径的所有 ASAv 接口及其他设备接口的 MTU 都设置为同一值。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - MTU 最大可设置为 9198 字节。ASAv 的最大值为 9000。

此程序介绍如何在以下环境中启用巨型帧：

vSphere 7.0.1 上的 HyperFlex 集群 > VMware vSphere vSwitch> 思科 UCS 交换矩阵互联 (FI)。

过程

步骤 1 更改已部署 ASAv 的 ASAv 主机的 MTU 设置。

1. 使用 vSphere Web 客户端连接到 vCenter 服务器。
2. 在 HyperFlex 主机的**高级系统设置 (Advanced System Settings)** 中，将配置参数 `Net.Vmxnet3NonTsoPacketGtMtuAllowed` 的值设置为 `1`。
3. 保存更改，然后重启主机。

有关详细信息，请参阅https://kb.vmware.com/s/article/1038578。

步骤 2 更改 VMware vSphere vSwitch 的 MTU 设置。

1. 使用 vSphere Web 客户端连接到 vCenter 服务器。
2. 编辑 VMware vSphere vSwitch 的属性，并将 **MTU** 的值设置为 `9000`。

步骤 3 更改思科 UCS 交换矩阵互联 (FI) 的 MTU 设置。

1. 登录思科 UCS 管理控制台。
2. 要编辑 QoS 系统类，请选择 **LAN** > **LAN 云 (LAN Cloud)** > **QoS 系统类 (QoS System Class)**。在**常规 (General)** 选项卡下，将 **MTU** 的值设置为 9216。
3. 要编辑 vNIC，请选择 **LAN** > **策略 (Policies)** > **root** > **子组织 (Sub-Organizations)**

   <your-hyperflex-org>**vNIC 模板** <your-vnic>。在**常规 (General)** 选项卡下，将 **MTU** 的值设置为 9000。

故障排除

本节提供与虚拟机上的 Hyperflex 部署相关的一些基本故障排除步骤。

验证您的虚拟机是否正在运行 Hyperflex

如果在采用 ESX OS 的 HyperFlex 上安装了 threat defense virtual 设备，则在 threat defense virtual 启动时，由 HX post_install 脚本创建的默认 vSphere HA 策略会导致错误消息。错误消息将显示：

“启动故障：资源不足，无法满足为 vSphere HA 配置的故障转移级别。”(Power on Failures: Insufficient resources to satisfy configured failover level for vSphere HA.)

解决办法

1. 在 VMware vCenter 中，转至 **HX 集群 (HX cluster)** > **配置 (Configure)** > **vSphere 可用性 (vSphere Availability)** > **编辑 VSphere HA (Edit Vsphere HA)** > **准入控制 (Admission Control)** > **定义主机故障转移容量 (Define host failover capacity)** > **覆盖计算的故障转移容量 (Override calculated failover capacity)**。
2. 更改和调整预留的故障转移 CPU 和内存容量百分比。
3. 启动 threat defense virtual VM。

第 10 章

在 Nutanix 上部署 Threat Defense Virtual

本章介绍将 threat defense virtual 部署到 Nutanix 环境的程序。

概述

Cisco Cisco Secure Firewall Threat Defense Virtual （之前称为 Firepower Threat Defense Virtual）将 Cisco Secure Firewall 功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

本章介绍了具有 AHV 虚拟机管理程序的 Nutanix 环境中的 threat defense virtual 功能，包括功能支持、系统要求、指南和限制。 本章还介绍了管理 threat defense virtual 的选项。

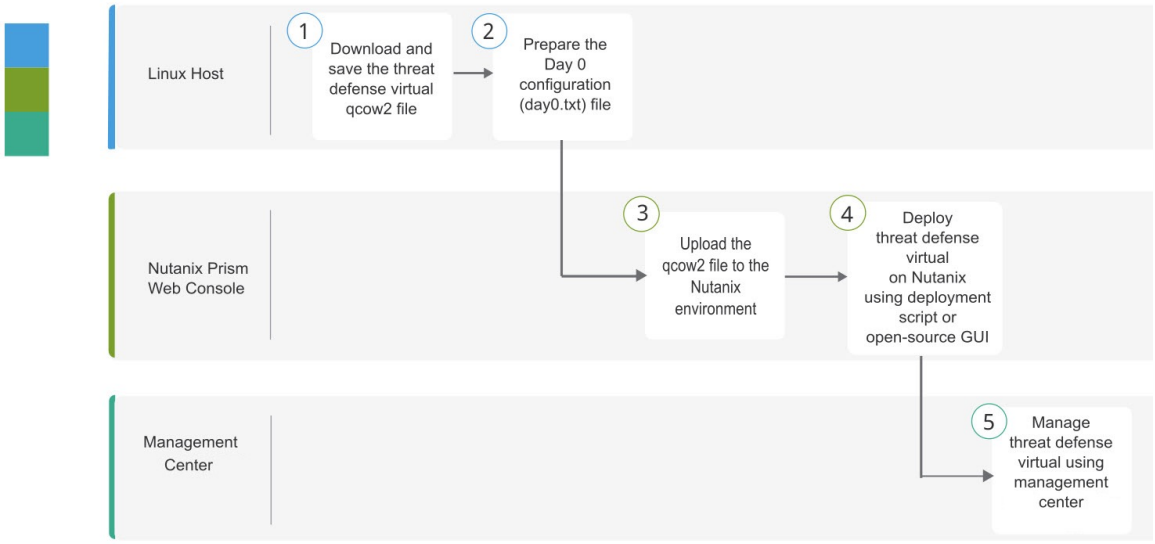
在开始部署之前，了解您的管理选项非常重要。您可以使用 Cisco Secure Firewall Management Center 来管理和监控 threat defense virtual。（之前称为 Firepower 管理中心）

关于 Nutanix 上的 Threat Defense Virtual 部署

Nutanix 企业云平台是一个融合的外向扩展计算和存储系统，用于托管和存储虚拟机。您可以运行多个虚拟机，这些虚拟机使用 Nutanix AHV 来运行未修改的 threat defense virtual OS 映像。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

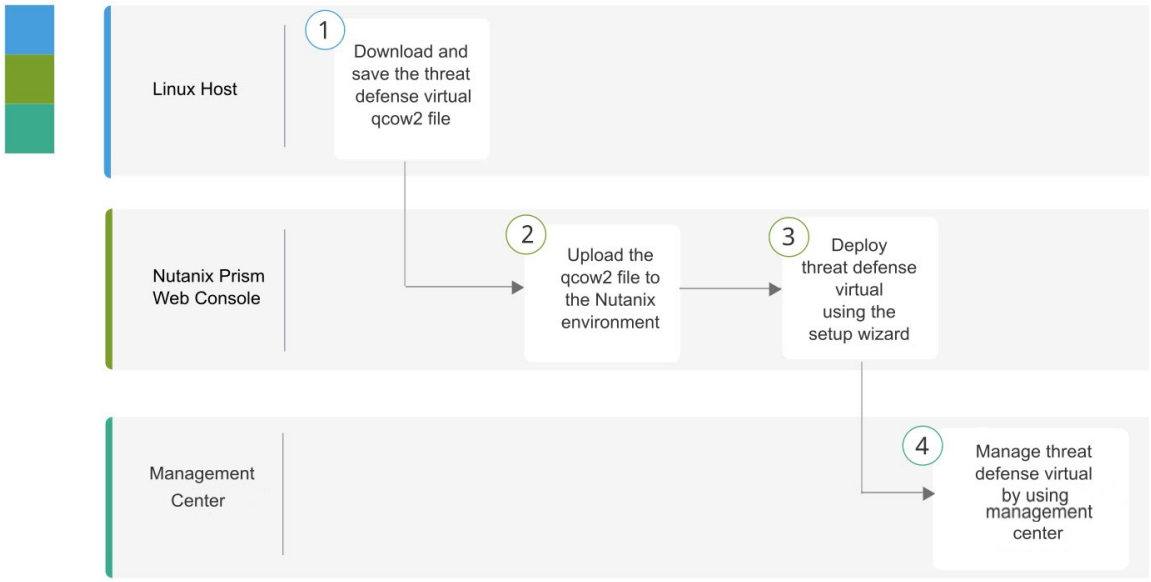
端到端程序

以下流程图说明了在使用 Day-0 配置文件的 Nutanix 平台上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	部署 Threat Defense Virtual：下载并保存 Threat Defense Virtual qcow2 文件。
2	Linux 主机	将 Threat Defense Virtual QCOW2 文件上传到 Nutanix：将 qcow2 文件上传到 Nutanix 环境。
3	Nutanix Prism Web 控制台	准备 Day 0 配置文件：准备 Day-0 配置文件（**文本文件 (Text file)** > **输入配置详细信息 (Enter the configuration details)** > **另存为 day0-config.txt (Save as day0-config.txt)**。
4	Nutanix Prism Web 控制台	部署 Threat Defense Virtual：在 Nutanix 上部署 Threat Defense Virtual。
5	管理中心	管理 Threat Defense Virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

以下流程图说明了在没有 Day-0 配置文件的情况下在 Nutanix 平台上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	Linux 主机	部署 Threat Defense Virtual：下载并保存 Threat Defense Virtual qcow2 文件。
2	Nutanix Prism Web 控制台	将 Threat Defense Virtual QCOW2 文件上传到 Nutanix：将 qcow2 文件上传到 Nutanix 环境。
3	Nutanix Prism Web 控制台	部署 Threat Defense Virtual：在 Nutanix 上部署 Threat Defense Virtual。
4	管理中心	管理 Threat Defense Virtual： • 使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

系统要求

版本

管理器版本	设备版本
管理中心 7.0	威胁防御 7.0

有关 threat defense virtual 支持的虚拟机管理程序的最新信息，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

Threat Defense Virtual 内存、vCPU 和磁盘大小估算

根据所需部署的实例数量和使用要求，threat defense virtual部署所使用的具体硬件可能会有所不同。每个 threat defense virtual 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

设置	值
性能级别	**7.0 及更高版本** threat defense virtual 支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。 • FTDv5 4vCPU/8GB (100Mbps) • FTDv10 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gbps) • FTDv30 8vCPU/16GB (5Gbps) • FTDv50 12vCPU/24GB (10Gbps) • FTDv100 16vCPU/32GB (16Gbps) 请参阅*Cisco Secure Firewall Management Center* 配置 中的“许可系统”一章，了解在许可 threat defense virtual 设备时的准则。 **注释** 要更改 vCPU/内存值，必须先关闭 threat defense virtual 设备的电源。
存储	50 GB（可调整） • 支持 virtio 块设备

注释 threat defense virtual 的最小网络数量是 4 个数据接口（管理、诊断、外部和内部）。

Threat Defense Virtual许可证

- 所有安全服务的许可证授权均在 管理中心中配置。
- 有关如何管理许可证的更多信息，请参阅《Cisco Secure firewall Management Center 配置指南》中的系统许可。

Nutanix 组件和版本

组件	版本
Nutanix Acropolis操作系统 (AOS)	5.15.5 LTS 及更高版本
Nutanix 集群检查 (NCC)	4.0.0.1
Nutanix AHV	20201105.12 及更高版本
Nutanix Prism Web 控制台	-

准则和限制

支持的功能

- 部署模式 - 路由（独立）、路由 (HA)、内联分流、内联、被动和透明
- 许可 - 仅 BYOL
- IPv6
- Threat Defense Virtual 本地 HA
- 巨型帧
- VirtIO

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 Nutanix 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

- Nutanix AHV 上的 Threat Defense Virtual 不支持接口热插拔。请勿在 threat defense virtual 通电时尝试添加/删除接口。
- Nutanix AHV 不支持 SR-IOV 或 DPDK-OVS。

注释 Nutanix AHV 使用 VirtIO 支持访客内 DPDK。有关详细信息，请参阅 AHV 上的 DPDK 支持。

一般准则

- 需要两个管理接口和两个数据接口来启动。支持共计 11 个接口

注释
- threat defense virtual 默认配置将管理接口、诊断接口和内部接口置于同一子网上。
- 修改网络接口时，必须关闭 threat defense virtual 设备。

- threat defense virtual 的默认配置假设您将管理接口（管理和诊断）和内部接口置于**同一子网**，并且管理地址使用内部地址作为访问互联网的网关（经过外部接口）。
- threat defense virtual 首次启动时，必须启用至少四个接口。您的系统必须要有四个接口才能部署。
- threat defense virtual 支持共计 11 个接口 - 1 个管理接口、1 个诊断接口，以及最多 9 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：
  1. 管理接口（必需）
  2. 诊断接口（必需）
  3. 外部接口（必需）
  4. 内部接口（必需）
  5. 5-11 数据接口（可选）

注释 threat defense virtual 的最小网络数量是 4 个数据接口。

- 对于控制台访问，通过 telnet 支持终端服务器。
- 以下是支持的 vCPU 和内存参数：

CPU	内存	Threat Defense Virtual 平台规模
4	8 GB	4vCPU/8GB（默认）
8	16 GB	8vCPU/16GB
12	24 GB	12vCPU/24GB
16	32 GB	16vCPU/32GB

- 请查看 threat defense virtual 接口的以下网络适配器、源网络和目标网络的对应关系：

网络适配器	源网络	目标网络	功能
vnic0*	Management0-0	Management0/0	管理
vnic1	诊断	诊断	诊断
vnic2*	GigabitEthernet0-0	GigabitEthernet0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet0/1	内部
*连接到同一子网。			

相关文档

- Nutanix 发行说明
- Nutanix 现场安装指南
- Nutanix 上的硬件支持

如何管理 Cisco Secure Firewall Threat Defense Virtual 设备

您可以使用以下方法管理您的 Cisco Secure Firewall Threat Defense Virtual 设备：

Cisco Secure Firewall Management Center

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心 来配置您的设备。

在 Nutanix 上部署的前提条件

- 从 Cisco.com 下载 Threat Defense Virtual qcow2 文件：https://software.cisco.com/download/navigator.html

注释 需要 Cisco.com 登录信息和思科服务合同。

- 查看概述，第 371 页一章。
- 有关 Nutanix 和系统兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

如何在 Nutanix 上部署 Threat Defense Virtual

步骤	任务	更多信息
1	查看先决条件。	在 Nutanix 上部署的前提条件，第 377 页
2	将 threat defense virtual qcow2 文件上传到 Nutanix 环境。	将 Threat Defense Virtual QCOW2 文件上传到 Nutanix，第 378 页
3	（可选）准备一个 Day 0 配置文件，其中包含了在部署虚拟机时需要应用的初始配置数据。	准备 Day 0 配置文件，第 379 页
4	将 threat defense virtual 部署到 Nutanix 环境。	部署 Threat Defense Virtual，第 380 页
5	（可选）如果未使用 Day 0 配置文件来设置 threat defense virtual，请通过登录 CLI 来完成设置。	完成 Threat Defense Virtual 设置，第 383 页

将 Threat Defense Virtual QCOW2 文件上传到 Nutanix

要将 threat defense virtual 部署到 Nutanix 环境，则必须在 Prism Web 控制台中从 threat defense virtual qcow2 磁盘文件创建映像。

开始之前

从 Cisco.com 下载 threat defense virtual qcow2 磁盘文件：https://software.cisco.com/download/navigator.html

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 打击齿轮图标打开**设置 (Settings)** 页面。

步骤 3 点击左侧窗格中的**映像配置 (Image Configuration)**。

步骤 4 点击**上传映像 (Upload Image)**。

步骤 5 创建映像。

1. 为映像输入名称。
2. 从**映像类型 (Image Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**存储容器 (Storage Container)** 下拉列表中选择所需的容器。
4. 指定 threat defense virtual qcow2 磁盘文件的位置。

   您可以指定 URL（以便从 Web 服务器导入文件）或从工作站上传文件。
5. 点击**保存 (Save)**。

步骤 6 请等待，直到新映像出现在**映像配置 (Image Configuration)** 页面中。

准备 Day 0 配置文件

在部署 threat defense virtual 之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。

请记住：

- 如果使用 Day 0 配置文件进行部署，该过程将允许您执行 threat defense virtual 设备的整个初始设置。
- 如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置系统所需的设置；有关更多信息，请参阅完成 Threat Defense Virtual 设置，第 383 页。

可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。
- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

  如果您打算使用本地 设备管理器 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 设备管理器 配置透明防火墙模式接口。
- 管理模式；请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

  输入 管理中心 字段（**FmcIp**、**FmcRegKey** 和 **FmcNatId**）的信息。
- 使设备可以在管理网络上进行通信的网络设置。

过程

步骤 1 使用您选择的文本编辑器来创建一个新的文本文件。

步骤 2 在文本文件中输入配置详细信息，如下例所示：

示例：

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"No"
}
```

注释

Day 0 配置文件的内容必须采用 JSON 格式。您必须使用 JSON 验证器工具来验证文本。

步骤 3 将文件另存为“**day0-config.txt**”。

步骤 4 为每个要部署的 threat defense virtual 重复步骤 1-3 以创建唯一的默认配置文件。

部署 Threat Defense Virtual

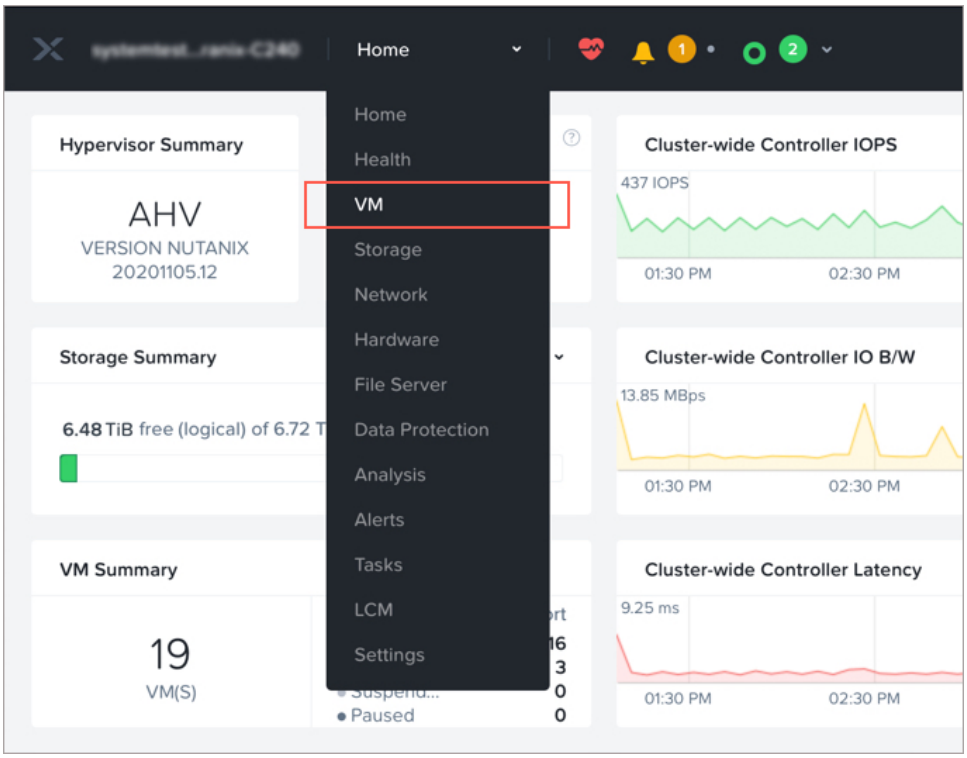
开始之前

确保您计划部署的 threat defense virtual 的映像显示在**映像配置 (Image Configuration)** 页面上。

过程

步骤 1 登录到 Nutanix Prism Web 控制台。

步骤 2 从主菜单栏中，点击视图下拉列表，然后选择 **VM**。



步骤 3 在 VM 控制面板上，点击**创建 VM (Create VM)**。

步骤 4 执行以下操作：

1. 输入 threat defense virtual 实例的名称。
2. （可选）输入 threat defense virtual 实例的说明。
3. 选择您希望 threat defense virtual 实例使用的时区。

步骤 5 输入计算详细信息。

1. 输入要分配给 threat defense virtual 实例的虚拟 CPU 数量。
2. 输入必须分配给每个虚拟 CPU 的核心数。
3. 输入要分配给 threat defense virtual 实例的内存量 (GB)。

步骤 6 将磁盘连接到 threat defense virtual 实例。

1. 在**磁盘 (Disks)**，点击**添加新磁盘 (Add New Disk)**。
2. 从**类型 (Type)** 下拉列表中选择**磁盘 (DISK)**。
3. 从**操作 (Operation)** 下拉列表中，选择**从映像服务克隆 (Clone from Image Service)**。
4. 从**总线类型 (Bus Type)** 下拉列表中，选择 **PCI** 或 **SCSI**。
5. 从**映像 (Image)** 下拉列表中，选择要使用的映像。

6. 点击**添加 (Add)**。

步骤 7 配置至少四个虚拟网络接口。

在**网络适配器 (NIC) (Network Adapters [NIC])** 下，点击**添加新 NIC (Add New NIC)**，选择网络，然后点击**添加 (Add)**。

重复此过程以便添加更多网络接口。

Nutanix 上的 threat defense virtual 支持共计 11 个接口 - 一个管理接口、一个诊断接口，以及最多九个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

- vnic0 - 管理接口（必需）
- vnic1 - 诊断接口（必需）
- vnic2 - 外部接口（必需）
- vnic3 - 内部接口（必需）
- vnic4-10 - 数据接口（可选）

步骤 8 配置 threat defense virtual 的关联策略。

在 **VM 主机关联 (VM Host Affinity)** 下，点击**设置关联 (Set Affinity)**，选择主机，然后点击**保存 (Save)**。

选择多个主机以确保即使节点出现故障也可运行 threat defense virtual。

步骤 9 如果您已准备了 Day 0 配置文件，请执行以下操作：

1. 选择**自定义脚本 (Custom Script)**。
2. 点击**上传文件 (Upload A File)**，，然后选择 Day 0 配置文件 (**day0-config.txt**)。

注释
此版本中不支持所有其他自定义脚本选项。

步骤 10 点击**保存 (Save)** 以部署 threat defense virtual。threat defense virtual 实例会显示在 VM 表格视图中。

步骤 11 在 VM 表格视图中，选择新创建的 threat defense virtual 实例，然后点击**打开电源 (Power On)**。

下一步做什么

- 如果您使用 Day 0 配置文件来设置 threat defense virtual，则后续步骤取决于您选择的管理模式。
  - 如果为**本地管理 (ManageLocally)**选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。
- 如果未使用 Day 0 配置文件来设置 threat defense virtual，请通过登录 CLI 来完成 threat defense virtual 设置。有关说明，请参阅完成 Threat Defense Virtual 设置，第 383 页。

完成 Threat Defense Virtual 设置

由于 threat defense virtual 设备没有 Web 界面，如果您在没有 Day 0 配置文件的情况下进行部署，必须使用 CLI 来设置虚拟设备。

过程

步骤 1 打开 threat defense virtual的控制台。

步骤 2 在 **firepower login** 提示符下，使用默认凭据（**username** *admin*，**password** *Admin123*）登录。

步骤 3 当 threat defense virtual 系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式

步骤 4 检查设置向导的设置。默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

步骤 5 根据提示完成系统配置。

步骤 6 当控制台返回到 # 提示符时，验证设置是否成功。

步骤 7 关闭 CLI。

下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**启用本地管理器 (Enable Local Manager)** 选择**否 (No)**，您将使用 管理中心 管理 threat defense virtual；请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

有关如何选择管理选项的概述，请参阅如何管理 Cisco Secure Firewall Threat Defense Virtual 设备，第 1 页。

第 11 章

在 OpenStack 上部署 Threat Defense Virtual

概述

本指南介绍如何在 OpenStack 环境中部署 threat defense virtual。OpenStack 是一个免费的开放标准云计算平台，主要作为公共服务和私有云中的基础设施即服务 (IaaS) 部署，其中虚拟服务器和其他资源可供用户使用。

此部署使用 KVM 虚拟机监控程序来管理虚拟资源。KVM 是适用于基于 x86 硬件的 Linux 且包含虚拟化扩展（例如英特尔 VT）的完全虚拟化解决方案。其中包含可加载的　内核模块 kvm.ko（用于提供核心虚拟化基础设施）和一个处理器特定模块（例如 kvm-intel.ko）。

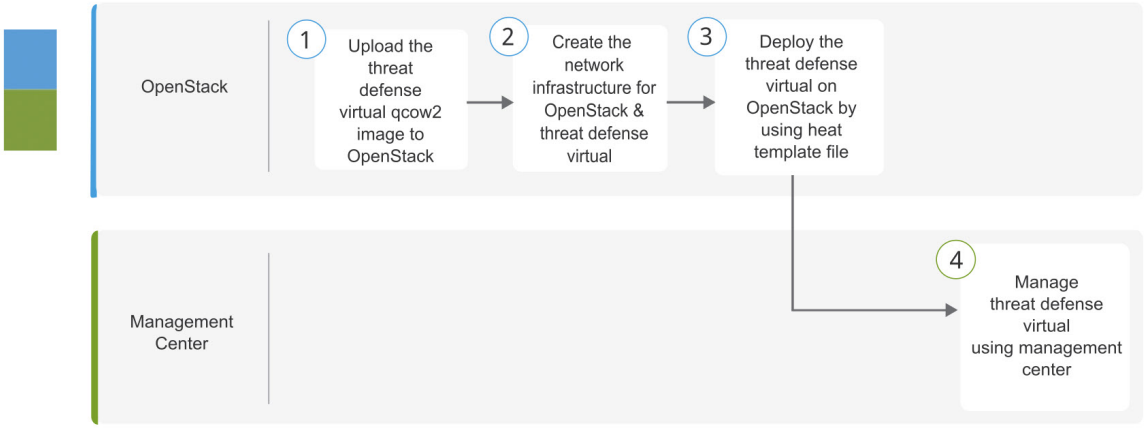
您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

由于 KVM 虚拟机监控程序已支持设备，因此无需其他内核软件包或驱动程序即可启用 OpenStack 支持。

注释　OpenStack 上的 Threat Defense Virtual 可以安装在任何优化的多节点环境中。

端到端程序

以下流程图说明了在 OpenStack 上部署 Threat Defense Virtual 的工作流程。



	工作空间	步骤
1	OpenStack	将 Threat Defense Virtual映像上传到 OpenStack：将 Threat Defense Virtual 映像上传到 OpenStack。
2	OpenStack	为 OpenStack 和 Threat Defense Virtual创建网络基础设施：为 OpenStack 和 Threat Defense Virtual 创建网络基础设施。
3	OpenStack	在 OpenStack 上部署 Threat Defense Virtual：使用 Threat Defense Virtual Heat 模板文件在 OpenStack 上部署 Threat Defense Virtual。
4	管理中心	使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

前提条件

- 从 software.cisco.com 获取 qcow2 threat defense virtual 映像。
- Threat Defense Virtual支持在开放源码 OpenStack 环境和思科 VIM 托管 OpenStack 环境中进行部署。

  根据 OpenStack 准则来设置 OpenStack 环境。

  - 请参阅开放源码 OpenStack 文档：

    Wallaby 版本 - https://docs.openstack.org/project-deploy-guide/openstack-ansible/wallaby/overview.html

- 请参阅思科虚拟化基础设施管理器 (VIM) OpenStack文档：思科虚拟化基础设施管理器文档，4.4.3

- 思科智能账户。您可以在 Cisco 软件中心创建一个。
- 许可 threat defense virtual。
  - 所有安全服务的许可证授权均在 管理中心中配置。
  - 有关如何管理许可证的详细信息，请参阅《 *Cisco Secure Firewall Management Center* 管理指南》中的“许可”。
- 接口要求：
  - 管理接口 (2) - 一个用于将 threat defense virtual 连接到 管理中心，另一个用于诊断；无法用于直通流量。
  - 内部和外部接口 - 用于将 threat defense virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于访问 threat defense virtual 的浮动 IP。
- 最低支持的 threat defense virtual 版本：
  - 版本 7.0
- 有关 OpenStack 要求，请参阅系统要求，第 389 页。
- 有关 threat defense virtual 和系统兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

准则和限制

支持的功能

OpenStack 上的 threat defense virtual 支持以下功能：

- 在 OpenStack 环境中在计算节点上运行的 KVM 虚拟机监控程序上部署 threat defense virtual。
- OpenStack CLI
- 基于 Heat 模板的部署
- OpenStack Horizon 控制面板
- IPv6
- 许可 - 仅支持 BYOL
- 仅使用 管理中心 来管理 Threat Defense Virtual。

- 驱动程序 - virtIO 和 SR-IOV

Threat Defense Virtual 智能许可的性能层

threat defense virtual 支持性能层许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

表 *31:* 基于授权的 *Threat Defense Virtual* 许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5	4 核/8 GB	100Mbps	50
FTDv10	4 核/8 GB	1Gbps	250
FTDv20	4 核/8 GB	3 Gbps	250
FTDv30	8 核/16 GB	5Gbps	250
FTDv50	12 核/24 GB	10Gbps	750
FTDv100	16 核/32 GB	16Gbps	10,000

请参阅《*Cisco Secure Firewall Management Center* 管理员指南》中的“许可”一章，了解在许可 threat defense virtual 设备时的准则。

性能优化

为实现 threat defense virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅 OpenStack 上的虚拟化调整和优化。

接收端扩展 - threat defense virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

Snort

- 如果您观察到异常行为，例如 Snort 需要很长时间才能关闭，或者 VM 通常缓慢，或者在执行某个进程时，请从 threat defense virtual 和 VM 主机收集日志。收集总体 CPU 使用情况、内存、I/O 使用情况和读/写速度日志将有助于对问题进行故障排除。
- 当 Snort 关闭时，观察到高 CPU 和 I/O 使用率。如果在内存不足且没有专用 CPU 的单个主机上创建了大量 threat defense virtual 实例，则 Snort 将需要很长时间才能关闭，这将导致创建 Snort 核心。

不支持的功能

OpenStack 上的 threat defense virtual 不支持以下各项：

- 自动缩放

- 集群

系统要求

OpenStack 环境必须符合以下支持的硬件和软件要求。

表 *32:* 开源 *OpenStack* 的硬件和软件要求

类别	支持的版本	说明
服务器硬件	UCS C240 M5	建议使用 2 台 UCS 服务器，分别用于 os-controller 和 os-compute 节点。
驱动因素	VIRTIO、IXGBE 和 I40E	这些是支持的驱动程序。
操作系统	Ubuntu Server 20.04	这是 UCS 服务器上的建议操作系统。
OpenStack 版本	Wallaby 版本	有关各种 OpenStack 版本的详细信息，请访问： https://releases.openstack.org/

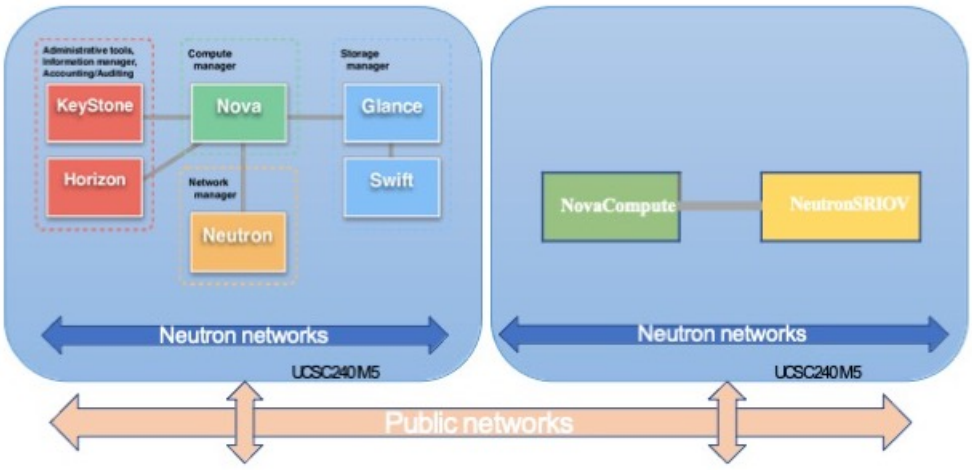
表 *33:* 思科 *VIM* 托管 *OpenStack* 的硬件和软件要求

类别	支持的版本	说明
服务器硬件	UCS C220-M5/UCS C240-M4	建议使用 5 台 UCS 服务器，其中 3 台用于 os-controller，两台或更多用于 os-compute 节点。
驱动因素	VIRTIO、IXGBE 和 I40E	这些是支持的驱动程序。
思科 VIM 版本	思科 VIM 4.4.3 支持的型号： • 操作系统 - Red Hat Enterprise Linux 8.4 • OpenStack 版本 - OpenStack 16.2（培训版本）	有关详细信息，请参阅思科虚拟化基础设施管理器文档 4.4.3。

OpenStack 平台拓扑

下图显示了建议的拓扑，以支持使用两个 UCS 服务器的 OpenStack 中的部署。

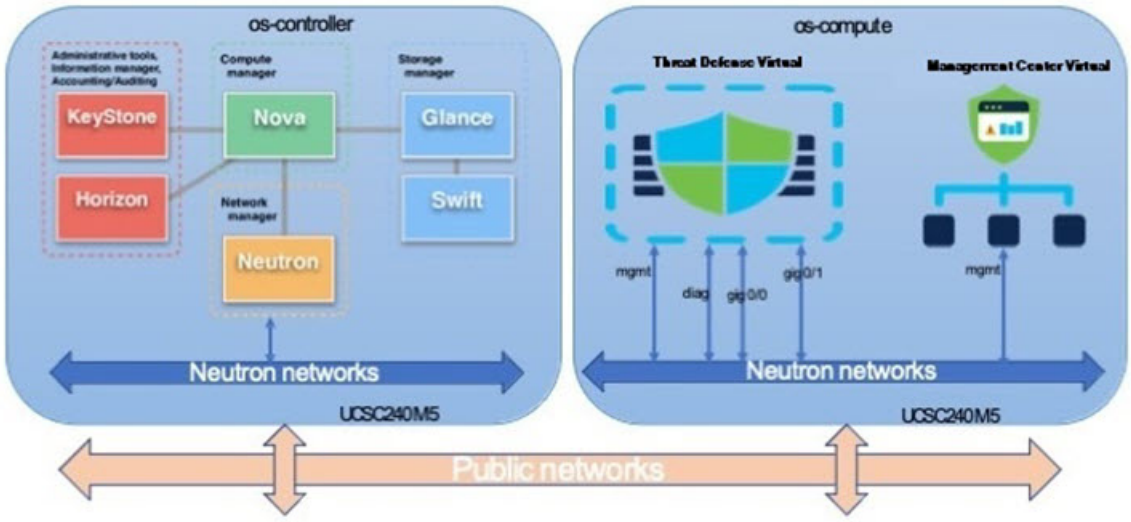
图 *53: OpenStack* 平台拓扑



OpenStack 上 Threat Defense Virtual 的网络拓扑示例

下图显示了在路由防火墙模式下 threat defense virtual 的网络拓扑示例，在 OpenStack 中为 threat defense virtual 配置了 4 个子网（管理、诊断、内部和外部）。

图 *54: OpenStack* 上使用 *Threat Defense Virtual* 和 *Management Center Virtual* 的拓扑示例



部署 Threat Defense Virtual

思科提供用于部署 threat defense virtual 的示例 Heat 模板。创建 OpenStack 基础设施资源的步骤汇总在 Heat 热模板 (`Deploy_os_infra.yaml`) 文件中，以创建网络、子网和路由器接口。总体而言，threat defense virtual 部署步骤分为以下几个部分。

- 将 threat defense virtual qcow2 映像上传到 OpenStack Glance 服务。
- 创建网络基础设施：
  - 网络
  - 子网 (Subnets)
  - 路由器接口
- 创建 threat defense virtual 实例：
  - 类型
  - 安全组
  - 浮动 IP
  - 实例

您可以按照以下步骤在 OpenStack 上部署 threat defense virtual。

将 Threat Defense Virtual映像上传到 OpenStack

将 threat defense virtual qcow2 映像复制到 OpenStack 控制器节点，然后将映像上传到 OpenStack Glance 服务。

开始之前

从 Cisco.com 下载 threat defense virtual qcow2 文件并将其放在 Linux 主机上：

https://software.cisco.com/download/navigator.html

注释 需要 Cisco.com 登录信息和思科服务合同。

过程

步骤 1 将 qcow2 映像文件复制到 OpenStack 控制器节点。

步骤 2 将 threat defense virtual 映像上传到 OpenStack Glance 服务。

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

步骤 3 验证 threat defense virtual 映像上传是否成功。

root@ucs-os-controller:$ openstack 映像列表

示例：

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+-------------------+----------+
| ID                                   | Name              | Status |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image    | active |+
```

系统将显示已上传的映像及其状态。

下一步做什么

使用 `deploy_os_infra.yaml` 模板来创建网络基础设施。

为 OpenStack 和 Threat Defense Virtual创建网络基础设施

开始之前

需要使用 Heat 模板文件来创建网络基础设施和 threat defense virtual 所需的组件，例如终端、网络、子网、路由器接口和安全组规则：

- `deploy_os_infra.yaml`
- `env.yaml`

您的 threat defense virtual 版本的模板可通过 FTDv OpenStack Heat 模板从 GitHub 存储库获取。

重要事项 请注意，思科提供的模板作为开源示例提供，不在常规思科 TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

过程

步骤 1 部署基础设施 Heat 模板文件。

root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>

示例：

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

步骤 2 验证是否已成功创建基础设施堆栈。

在 OpenStack 上部署 Threat Defense Virtual

root@ucs-os-controller:$ openstack stack list

下一步做什么

在 OpenStack 上创建 threat defense virtual 实例。

在 OpenStack 上部署 Threat Defense Virtual

使用示例 threat defense virtual Heat 模板在 OpenStack 上部署 threat defense virtual。

开始之前

在 OpenStack上部署 threat defense virtual 需要 Heat 模板：

- `deploy_ftdv.yaml`

您的 threat defense virtual 版本的模板可通过 FTDv OpenStack Heat 模板从 GitHub 存储库获取。

重要事项 请注意，思科提供的模板作为开源示例提供，不在常规思科 TAC 支持范围内。定期检查 GitHub 以了解更新和自述文件说明。

过程

步骤 1 部署 threat defense virtual Heat 模板文件 (`deploy_ftdv.yaml`) 以创建 threat defense virtual 实例。

root@ucs-os-controller:$ openstack stack create ftdv-stack -e env.yaml-t deploy_ftdv.yaml

示例：

```
+---------------------+------------------------------+
| Field               | Value                        |
+---------------------+------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | ftdv-stack                   |
| description         | FTDvtemplate                 |
| updated_time        | None                         |
| stack_status        | CREATE_IN_PROGRESS           |
| stack_status_reason | Stack CREATE started         |
+---------------------+------------------------------+
```

步骤 2 验证是否已成功创建 threat defense virtual 堆栈。

root@ucs-os-controller:$ openstack stack list

示例：

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack Status
   |
```

在 OpenStack 上部署 Threat Defense Virtual

```
+--------------------------------------+-------------+----------------------------------+-----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-stack  | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE
 |
+--------------------------------------+-------------+----------------------------------+-----------------+
```

第 12 章

在阿里云上部署 Threat Defense Virtual

概述

阿里云是一种公共云环境。Threat Defense Virtual 可在阿里云环境中作为访客运行。

Alibaba 支持的实例类型

Alibaba 上的 Threat Defense Virtual 可以使用以下实例类型：

网络增强机器类型			
配置	vCPU 数量	内存 (GB)	支持的最大接口数
ecs.g5ne.xlarge	4	16	4
ecs.g5ne.2xlarge	8	32	6
ecs.g5ne.4xlarge	16	64	8

Note Threat Defense Virtual 至少需要四个接口 (ENI) 来支持实例。

Note 我们不支持调整实例类型的大小和部署 Threat Defense Virtual。您只能使用全新的部署来部署具有不同实例大小的 Threat Defense Virtual。

网络要求

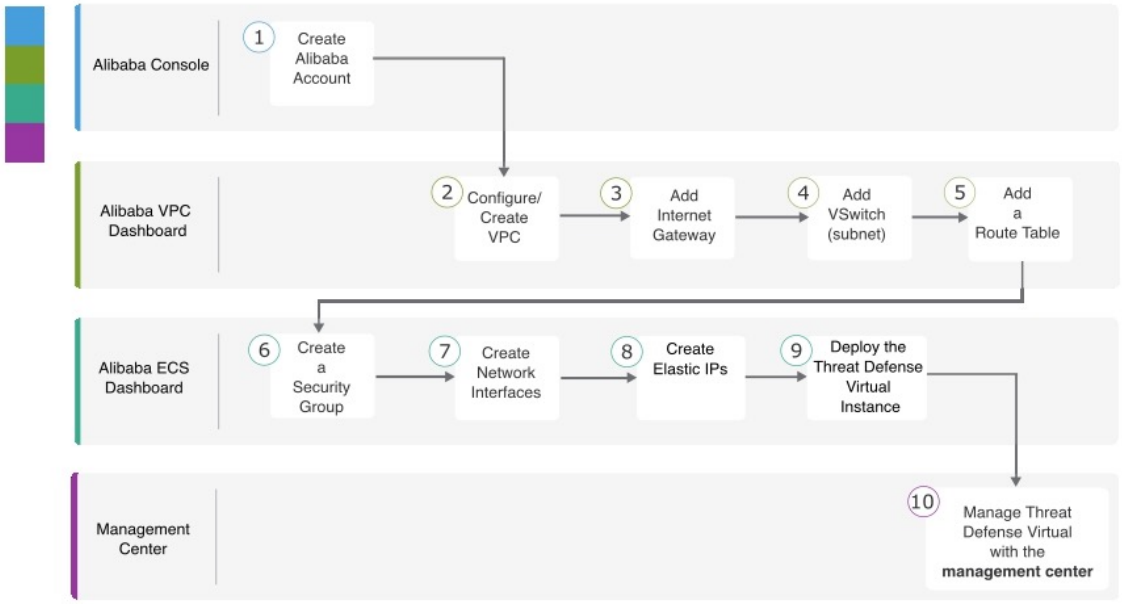
- 您可以创建一个具有四个 Vswitch（子网）的 VPC，以支持基本Threat Defense Virtual。
- 管理 Vswitch 必须可用于部署实例的同一区域中，否则必须创建实例。

相关文档

有关实例类型及其配置的更多信息，请参阅阿里云

端到端程序

请参阅以下任务以在您的 Alibaba 上部署 Threat Defense Virtual。



	工作空间	步骤
1	Alibaba 控制台	https://marketplace.alibabacloud.com/。在Alibaba 控制台中创建用户账户。
2	Alibaba VPC 控制面板	创建 VPC，第 400 页：创建并配置您的 Alibaba 账户专用的 VPC。
3	Alibaba VPC 控制面板	添加互联网网关，第 401 页：添加互联网网关以控制 VPC 与互联网的连接。
4	Alibaba VPC 控制面板	添加 vSwitch，第 401 页：将 VSwitch（子网）添加到 VPC。

	工作空间	步骤
5	Alibaba VPC 控制面板	添加路由表，第 402 页：将路由表连接到为 VPC 配置的网关。
6	Alibaba ECS 控制面板	创建安全组，第 403 页：创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。
7	Alibaba ECS 控制面板	创建网络接口，第 403 页：使用静态 IP 地址为 Threat Defense Virtual 创建网络接口。
8	Alibaba ECS 控制面板	创建弹性 IP 地址，第 404 页：弹性 IP 是预留公共 IP，用于远程访问 Threat Defense Virtual 以及其他实例。
9	管理中心或设备管理器	部署 Threat Defense Virtual，第 405 页：从 Alibaba 门户部署 Threat Defense Virtual。
10	管理中心	管理 Threat Defense Virtual： • 使用 Firepower 管理中心管理 Firepower Threat Defense Virtual

前提条件

- Alibaba 账户。您可以在 https://www.alibaba.com/ 创建一个。
- 需要 SSH 客户端（例如，Windows 上的 PuTTY 或 Macintosh 上的终端）才能访问 Threat Defense Virtual 控制台。
- 思科智能账户。您可以在 Cisco 软件中心 https://software.cisco.com/ 创建一个。
- 许可 Threat Defense Virtual。
  - 所有安全服务的许可证授权均在 Management Center Virtual中配置。
  - 有关如何管理许可证的详细信息，请参阅《Cisco Secure Firewall Management Center 配置指南》中的“许可 Cisco Secure Firewall 系统”。
- Threat Defense Virtual 接口要求：
  - 管理接口 (1) - 用于将 Threat Defense Virtual 连接到 Management Center Virtual，
  - 第二个接口用于诊断；不能用于直通流量。

    在 6.7 和更高版本中，可以选择为 FMC 管理配置数据接口，而非管理接口。管理接口是数据接口管理的前提条件，因此您仍需要在初始设置中对其进行配置。在高可用性部署中，不支持从数据接口进行 FMC 访问。

    有关为 FMC 访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

- 流量接口 (2) - 用于将 Threat Defense Virtual 连接到内部主机和公共网络。

- 通信路径：
  - 用于访问 Threat Defense Virtual的公共和弹性 IP。

支持的软件平台

The Threat Defense Virtual Auto Scale解决方案与软件版本无关，适用于管理中心托管的 threat defense virtual 设备。有关思科软件和硬件兼容性的信息，包括操作系统和托管环境要求，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》。

- 《Firewall Management Center Virtual 兼容性指南》表列出 Alibaba 上 Management Center Virtual 的兼容性和虚拟托管环境要求。
- 《Cisco Secure Firewall Threat Defense 兼容性指南》表列出 Alibaba 上 Threat Defense Virtual 的兼容性和虚拟托管环境要求。

准则和限制

支持的功能

- 基本产品调配
- Day 0 配置
- 使用公钥或密码的 SSH。
- Alibaba UI 控制台，用于访问 Threat Defense Virtual 以进行任何调试。
- Alibaba UI UI 停止/重启
- 支持的实例类型：ecs.g5ne.xlarge、ecs.g5ne.2xlarge 和 ecs.g5ne.4xlarge。
- 超线程
- 自带许可证 (BYOL) 许可证支持。

Threat Defense Virtual 智能许可的性能层

支持性能级许可，该级别许可可基于部署要求提供不同的吞吐量级别和 VPN 连接限制。

Table 34: 基于授权的许可功能限制

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv5，100Mbps	4 核/8 GB	100Mbps	50
FTDv10，1Gbps	4 核/8 GB	1Gbps	250

性能层	设备规格（核心/RAM）	速率限制	RA VPN 会话限制
FTDv20，3Gbps	4 核/8 GB	3 Gbps	250
FTDv30，5Gbps	8 核/16 GB	5Gbps	250
FTDv50，10Gbps	12 核/24 GB	10Gbps	750
FTDv，16Gbps	16 核/34 GB	16Gbps	10,000

- 使用 Cisco 智能许可证帐户的 BYOL（自带许可证）

有关许可 Threat Defense Virtual 设备时的准则，请参阅 *Threat Defense Virtual* 管理中心配置中的“许可 Threat Defense Virtual 系统”一章。

性能优化

为实现 Threat Defense Virtual的最佳性能，您可以对 VM 和主机进行调整。有关详细信息，请参阅阿里云上的虚拟化调整和优化。

接收端扩展 - Threat Defense Virtual 支持接收端扩展 (RSS)，网络适配器利用这项技术将网络接收流量分发给多个处理器内核。在 7.0 及更高版本上受支持。有关详细信息，请参阅用于接收端扩展 (RSS) 的多个 RX 队列。

不支持的功能

- FDM
- 高可用性功能
- Autoscale
- IPv6
- SR-IOV

限制

- 版本 7.2 不支持透明、内联和被动模式。
- Alibaba 中不支持东西流量。
- 不支持巨型帧，因为它仅限于 Alibaba 提供的几种实例类型。有关更多信息，请参阅阿里云。

Note Threat Defense Virtual 必须有四个接口才能启动。

许可

- 支持使用 Cisco 智能许可证帐户的 BYOL（自带许可证）。

配置策略和设备设置

在安装 Threat Defense Virtual 并将设备添加到 Management Center Virtual 后，您可以使用 Management Center Virtual 用户界面为在 Alibaba 上运行的 Threat Defense Virtual 配置设备管理设置。您可以使用 Threat Defense Virtual 实例配置和应用访问控制策略和其他相关策略来管理流量。

安全策略可对 Threat Defense Virtual提供的服务进行控制（例如下一代 IPS 过滤和应用过滤）。您可以使用 Management Center Virtual配置 Threat Defense Virtual上的安全策略。有关如何配置安全策略的详细信息，请参阅《*Cisco Secure Firewall* 配置指南》或 Management Center Virtual 中的在线帮助。

创建 VPC

虚拟私有云 (VPC) 是 Alibaba 账户专用的虚拟网络。该网络逻辑上与阿里云中的其他虚拟网络相隔离。您可以将 Management Center Virtual 和 Threat Defense Virtual 实例等阿里云资源启动到 VPC 中。您可以配置 VPC，选择其 IP 地址范围，创建 VSwitch（子网），并配置路由表、网络网关和安全设置。

Procedure

步骤 1 登录 https://www.alibabacloud.com 并选择您所在的区域。

阿里云会被划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 点击**产品 (Products) > VPC**。

步骤 3 点击**VPC 控制面板 (VPC Dashboard) > 您的 VPC (Your VPCs)**。

步骤 4 点击**创建 VPC (Create VPC)**。

步骤 5 在**创建 VPC**对话框中输入以下信息：

a) 用于标识 VPC 的用户自定义**名称标签**。

b) IP 地址的**IPv4 CIDR 块**。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。

c) 在 **IPv4 CIDR 块 (IPv4 CIDR block)** 中选择**阿里云提供的 IPv4 CIDR 块 (Alibaba Cloud-provided IPv4 CIDR block)**，以在虚拟私有云中启用 IPv4。

d) 默认的**租户设置**，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

步骤 6 点击**确定 (OK)** 以创建 VPC。

What to do next

添加互联网网关到 VPC 中，详见下一部分。

添加互联网网关

您可以添加互联网网关（NAT 网关）以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

准备工作

- 为 Threat Defense Virtual 实例创建 VPC。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击**VPC 控制面板 (VPC Dashboard)** > **互联网网关 (Internet Gateways)**，然后点击**创建互联网网关 (Create Internet Gateway)**。

步骤 3 输入用户自定义的**名称标签**以标识网关，然后点击**确定 (OK)** 以创建网关。

步骤 4 选择上一步中创建的网关。

步骤 5 点击**绑定到 VPC (Bind to VPC)** 并选择之前创建的 VPC。

步骤 6 点击**确定 (OK)** 以将网关绑定到您的 VPC。

默认情况下，在创建 NAT 网关并将其绑定到 VPC 之前，在 VPC 中启动的实例无法与互联网通信。

What to do next

添加 VSwitch（子网）到 VPC 中，详见下一部分。

添加 vSwitch

您可以对 Threat Defense Virtual 实例可连接的 VPC IP 地址范围进行分段。您可以根据安全和运营需要创建 vSwitch（子网），以实现实例的分组。对于 Threat Defense Virtual，您需要创建一个用于管理的 vSwitch 和用于流量的 VSwitch。

准备工作

- 为 Threat Defense Virtual 实例创建四个 VPC。如创建 VPC 部分中所述。
- 为每个 VPC 添加一个 vSwitch（子网）。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击 **VPC 控制面板 (VPC Dashboard)** > **VSwitches**，然后点击**点击 vSwitch (Click vSwitch)**。

步骤 3 在**创建 vSwitch (Create vSwitch)** 对话框中输入以下信息：

a) 用于标识 vSwitch 的用户自定义**名称标签**。
b) 用于此 vSwitch 的 **VPC**。
c) 此 vSwitch 将驻留的**区域**。选择**无首选项 (No Preference)**，由阿里云来选择区域。
d) IP 地址 (IPv4) 的 **CIDR 块**。vSwitch 中的 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。vSwitch 大小可以与 VPC 相等。

步骤 4 点击**确定 (OK)** 以创建 vSwitch。

步骤 5 如需多个 vSwitch，重复以上步骤。为管理流量创建单独的 vSwitch，根据需要为数据流量创建多个 vSwitch。

What to do next

添加路由表到 VPC 中，详见下一部分。

添加路由表

您可以将路由表连接到为 VPC 配置的网关。您还可以关联多个子网与单个路由表，但子网一次只可以关联一个路由表。

Procedure

步骤 1 点击**产品 (Products)** > **VPC**。

步骤 2 点击**VPC 控制面板 (VPC Dashboard)** > **路由表 (Route Tables)**，然后点击**创建路由 (Create Route)**。

步骤 3 输入用于标识路由表的用户自定义**名称标签**。

步骤 4 从下拉列表中选择将使用此路由表的 **VPC** 。

步骤 5 点击**确定 (OK)**以创建路由表。

步骤 6 选择创建的路由表。

步骤 7 点击**路由 (Routes)** 选项卡，以在详细信息窗格中显示路由信息。

步骤 8 点击**编辑 (Edit)**，然后点击**添加其他路由 (Add another route)**。

a) 在**目标 (Destination)** 列中，为所有 IPv4 流量输入 **0.0.0.0/0**。
b) 在**目标**列中，选择您的网关。

步骤 9 点击**保存**。

What to do next

创建安全组，详见下一部分。

创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。

Procedure

步骤 1 点击**产品 (Products)** > **ECS**。

步骤 2 点击**ECS 控制面板 (ECS Dashboard)** > **安全组 (Security Groups)**。

步骤 3 点击**创建安全组**。

步骤 4 在**创建安全组**对话框中输入以下信息：

a) 用于标识安全组的用户自定义**安全组名称**。

b) 此安全组的**说明**。

c) 与此安全组关联的 **VPC**。

步骤 5 配置**安全组规则**：

a) 点击**入站规则 (Inbound Rules)** 选项卡，然后点击**添加规则 (Add Rule)**。

Note
要从 Alibaba 外部管理 Management Center Virtual，需要 HTTPS 和 SSH 访问。您应指定相应的源 IP 地址。此外，如果在 Alibaba VPC 内同时配置 Management Center Virtual 和 Threat Defense Virtual，则应允许专用 IP 管理子网访问。

b) 点击**出站规则 (Outbound Rules)** 选项卡，然后点击**添加规则 (Add Rule)** 以添加出站流量规则，或保留**所有流量 (All traffic)**（作为**类型 (Type)**）和**任意位置 (Anywhere)**（作为**目标 (Destination)**） 的默认设置。

步骤 6 点击**创建**以创建安全组。

What to do next

创建网络接口，详见下一部分。

创建网络接口

您可以使用静态 IP 地址 (IPv4) 或 DHCP 为 Threat Defense Virtual 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

Procedure

步骤 1 点击**服务 (Services)** > **弹性网络接口 (Elastic Network Interface)**。

步骤 2 点击**网络接口 (Network Interfaces)**。

步骤 3 点击**创建网络接口 (Yes, Create)**。

步骤 4 在**创建网络接口**对话框中输入以下信息：

a) 网络接口的用户自定义**说明**（可选）。

b) 从下拉列表中选择一个 **vSwitch**。确保选择要创建 Threat Defense Virtual 实例的 VPC 的 vSwitch。

c) 输入**专用 IP** 地址。您可以使用静态 IP 地址 (IPv4) 或自动生成 (DHCP)。

d) 选择一个或多个**安全组**。确保安全组已打开所有必需的端口。

步骤 5 点击**创建网络接口 (Create network interface)** 以创建网络接口。

步骤 6 选择刚创建的网络接口。

步骤 7 右键点击并选择**修改源/目的地址检查**。

步骤 8 取消选中**源/目标 (Source/destination check)** 复选框下的**启用 (Enable)** 复选框，然后点击**保存 (Save)**。

What to do next

创建弹性 IP 地址，详见下一部分。

创建弹性 IP 地址

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址 (IPv4) 会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 地址是一个保留的公共 IP 地址，用于远程访问 Threat Defense Virtual 和其他实例。

Procedure

步骤 1 点击**产品 (Products)** > **弹性计算服务 (Elastic Compute Service)**。

步骤 2 在**弹性计算服务 (Elastic Compute Service)** 控制面板中，点击左侧菜单中的**弹性 IP (Elastic IP)**。

步骤 3 点击**分配弹性 IP 地址 (Allocate Elastic IP Address)**。

步骤 4 配置 EIP 设置：

a) 选择要分配 EIP 的**区域**。

b) 为 EIP 选择所需的带宽计划。例如，BYOL 或订用。

c) 指定所需的带宽量。

d) 查看您的选择，然后点击**确定 (OK)** 以分配 EIP。

步骤 5 将 EIP 与实例关联：

a) 分配 EIP 后，转至**弹性计算服务 (Elastic Compute Service)** 控制面板中的**弹性 IP (Elastic IP)** 部分。

b) 找到您创建的 EIP，然后点击**关联 (Associate)**。

c) 选择要与 EIP 关联的 ECS 实例，然后点击**确定 (OK)**。

步骤 6 确保 EIP 现在列在关联的 ECS 实例下，并验证其连接性。

What to do next

部署 Threat Defense Virtual，详见下一部分。

配置 Alibaba 环境

要在 Alibaba 部署 Threat Defense Virtual，需要根据部署的特定要求和设置来配置 Alibaba VPC。在大多数情况下，设置向导将引导您完成设置过程。Alibaba 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关更多信息，请参阅阿里云文档。

Threat Defense Virtual 部署需要四个网络虚拟私有云 (VPC)，您必须在部署 Threat Defense Virtual之前创建这些网络。

这四个网络 VPC 包括：

- 管理子网的管理 VPC。
- 诊断子网的诊断 VPC。
- 内部子网的内部 VPC。
- 外部子网的外部 VPC。

为更好地控制 Alibaba 设置，以下部分提供有关在启动 Threat Defense Virtual 实例之前如何配置 VPC 和 EC2 的指南：

准备工作

- 创建您的阿里云账户。

部署 Threat Defense Virtual

Procedure

步骤 1 转到 https://marketplace.alibabacloud.com/ 并搜索 **Cisco Firepower NGFW Virtual (NGFWv) - BYOL** 产品以部署 Threat Defense Virtual。

Note
Alibaba 会被划分为彼此隔离的多个区域。区域显示在窗口的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

步骤 2 点击产品链接以打开 **Cisco Firepower NGFW Virtual (NGFWv) - BYOL** 页面。

步骤 3 点击**选择您的计划 (Choose Your Plan)**。您将被重定向到**弹性计算服务 (Elastic Compute Service)** 页面。

步骤 4 在**自定义启动 (Custom Launch)** 部分中输入以下详细信息：

- **计费方法 (Billing Method)**：根据要求。

Note
计费方式适用于阿里云上的基础设施，您可以根据需要选择。

- **区域 (Region)**：根据要求。
- **网络和区域 (Network and Zone)**：从下拉列表中选择 VPC 和您之前创建的管理 vSwitch，或者使用**创建 VPC (Create VPC)** 和**创建 vSwitch (Create vSwitch)** 链接重新创建。

步骤 5 移至**实例和映像 (Instances and Images)** 页面。

在**所有实例类型 (All Instance Types)** 部分下，执行以下操作：

- **实例 (Instance)**：选择以下任何受支持的实例类型 - **ecs.g5ne.xlarge**、**ecs.g5ne.2xlarge** 或 **ecs.g5ne.4xlarge**。
- **映像 (Image)**：最新的 Threat Defense Virtual 市场版本显示在**市场映像 REC** 部分中。
  a. 点击**重新选择映像 (Reselect Image)**。系统将显示“阿里云市场映像”对话框，其中包含您正在部署的 Threat Defense Virtual 映像详细信息。
  b. 从下拉列表中选择 Threat Defense Virtual 设备并点击**选择 (Select)**。

步骤 6 转到**存储 (Storage)** 部分。保留默认值并继续。

步骤 7 转到**带宽和安全组 (Bandwidth and Security Groups)** 部分并执行以下操作：

- **ENI**
  - **安全组 (Security Group)**：选择适当的安全组。
  - **主 ENI (Primary ENI)**：输入在**网络和区域 (Network and Zone)** 字段中选择的主接口，即管理 vSwitch。
  - **辅助 ENI (Secondary ENI)**：从**现有辅助接口 (Existing Secondary Interface)** 下拉列表中选择辅助接口，或通过选择所需的 vSwitch 创建新的辅助接口。

    Note
    在实例启动阶段，可以使用两个接口来部署实例，并且可以在从ECS控制台部署后连接其他两个接口。

  - **密钥对 (Key Pair)**：从下拉列表中选择现有的密钥对或创建新的密钥对。

步骤 8 转到**高级设置 (Advance Settings)** 并执行以下操作：

- **实例名称 (Instance Name)**：合适的实例名称。
- **用户数据 (User Data)**：根据要求提供 Day-0 配置（不要选中**输入 Base64 编码的信息 (Enter Base64 Encoded iInformation)** 复选框）。

  使用管理中心来管理 Threat Defense Virtual 的 Day-0 配置示例：

```
{
"AdminPassword": "<your_password>",
"Hostname": "<your_hostname>",
"ManageLocally": "No",
"FmcIp":  "<IP address of FMC>",
"FmcRegKey":"<registration_passkey>",
```

```
"FmcNatId":"<NAT_ID_if_required>"
}
```

Note
如果您在 Day-0 配置中未提供任何密码，则默认密码将是 Threat Defense Virtual 的实例 ID，如 Alibaba 控制台或 CLI 上所示。

步骤 9 接受 **ECS 服务条款**，然后点击**创建订单 (Create Order)**。
Threat Defense Virtual 使用两个接口来启动，您可以在 ECS 控制台上查看它们。

Note
要完成启动过程，必须使用四个接口来配置 Threat Defense Virtual。

步骤 10 要使用其他两个接口来配置 Threat Defense Virtual ，请执行以下操作：

a) 在阿里云上，转到**弹性计算服务 (Elastic Compute Service)**。
b) 点击左侧窗格中**网络和安全 (Network & Security)** 下的 **弹性网络接口 (Elastic Network Interface)**。
c) 搜索之前创建的流量接口。
d) 选中与流量接口对应的复选框，然后点击**绑定到实例 (Bind to Instance)**。系统将显示**绑定到实例 (Bind to Instance)** 对话框。
e) 在**实例 (Instance)** 字段中输入 Threat Defense Virtual 名称。
f) 点击**确认 (Confirm)**，将其配置为实例的 **eth2** 接口。
g) 重复**步骤 c** 至**步骤 f** ，为 Threat Defense Virtual 配置 **eth3** 接口。

步骤 11 点击 **EC 控制面板 (EC Dashboard)** > **实例 (Instances)**。

步骤 12 在 Management Center Virtual 完成启动后，您应该就能够将其注册到 Management Center Virtual。

第 13 章

使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual

本章介绍如何部署使用 管理中心 管理的独立式 threat defense virtual 设备。

注释 本文档涵盖最新 threat defense virtual 版本的功能。如果您使用的是旧版本的软件，请参考您的版本的《管理中心 配置指南》中的步骤。

关于具有 Cisco Secure Firewall Management Center 的 Cisco Secure Firewall Threat Defense Virtual

Cisco Secure Firewall Threat Defense Virtual 是思科 NGFW 解决方案的虚拟化组件。threat defense virtual 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统 (NGIPS)、应用可视性与可控性 (AVC)、URL 过滤，以及恶意软件防护。

您可以使用 管理中心 管理 threat defense virtual，这是一个功能齐全的多设备管理器，位于单独的服务器上。threat defense virtual 向您分配给 threat defense virtual 计算机的管理接口上的 管理中心 注册并与之通信。

threat defense virtual 向您分配给 threat defense virtual 计算机的管理接口上的 管理中心 注册并与之通信。

要进行故障排除，您可以使用管理接口上的 SSH 访问 威胁防御 CLI，也可以从 管理中心 CLI 连接到 威胁防御。

本章介绍如何部署使用 管理中心 管理的独立式 Threat Defense Virtual 设备。有关 管理中心 的详细配置信息，请参阅《管理中心管理指南》和《管理中心设备配置指南》。

有关安装 管理中心 的信息，请参阅《Cisco Firepower Management Center 1600、2600 和 4600 硬件安装指南》或《Management Center Virtual 入门指南》。

登录至 Cisco Secure Firewall Management Center

使用管理中心配置并监控威胁防御。

开始之前

有关受支持浏览器的信息，请参阅您所用版本的发行说明（参阅https://www.cisco.com/go/firepower-notes）。

过程

步骤 1 使用支持的浏览器输入以下 URL。

https://*fmcv_ip_address*

fmc_ip_address 标识 管理中心 的 IP 地址或主机名。

注释
特定于 IPv6 的 https://[fmcv_ipv6_public_address]

步骤 2 输入您的用户名和密码。

步骤 3 点击登录。

向 Cisco Secure Firewall Management Center 注册设备。

开始之前

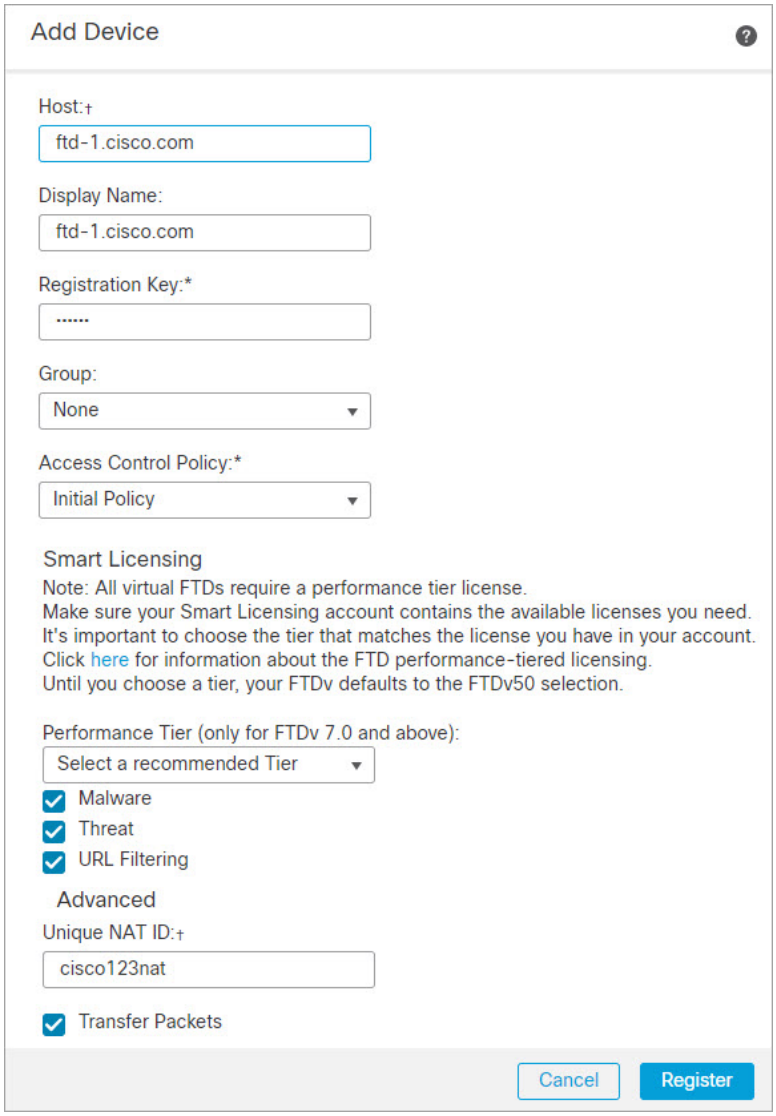
确保 threat defense virtual 计算机已部署成功、已接通电源并且已首次完成其启动程序。

注释 此过程假定您通过 day0/bootstrap 脚本为 管理中心 提供了的注册信息。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅Cisco Secure Firewall Threat Defense 命令参考。

过程

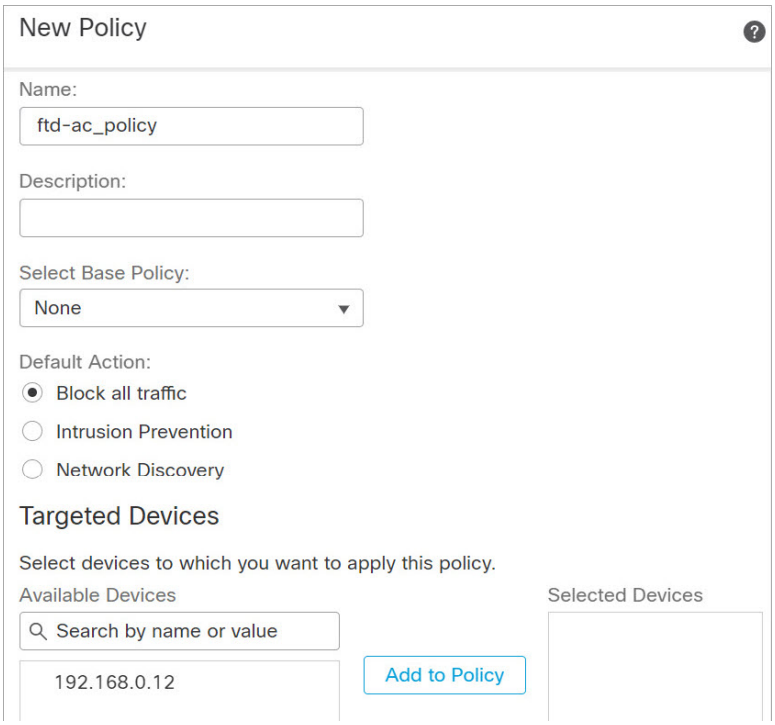
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加 (Add)**下拉列表选择**添加设备 (Add Device)**，然后输入以下参数。



- **主机** - 输入要添加的设备的 IP 地址 （IPv4 和 IPv6）。在启用 IPv6 设置的情况下，主机名中可以包含 Ipv4 或 Ipv6。
- **显示名称 (Display Name)** - 输入要在 管理中心 中显示的设备名称。
- **注册密钥 (Registration Key)** - 输入您在 threat defense virtual 引导程序配置中指定的注册密钥。
- **域 (Domain)** - 如果有多域环境，请将设备分配给分叶域。

- **组 (Group)** - 如果在使用组，则将其分配给设备组。
- **访问控制策略 (Access Control Policy)** - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略，否则选择**新建策略 (Create new policy)**，然后选择**阻止所有流量 (Block all traffic)**。之后您可以更改此设置以允许流量通过；请参阅配置访问控制，第 423 页。



- **智能许可 (Smart Licensing)** - 为要部署的功能分配所需的智能许可证：**Malware**（如果您打算使用恶意软件防御检查）、**Threat**（如果您打算使用入侵防御）、**URL**（如果您打算实施基于类别的 URL 过滤）。
- **唯一 NAT ID (Unique NAT ID)** - 指定您在 threat defense virtual 启动程序配置中指定的 NAT ID。
- **转移数据包 (Transfer Packets)** - 可让设备将数据包传输至 管理中心。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 管理中心进行检测。如果禁用此选项，只有事件信息会发送到 管理中心，数据包数据不发送。

步骤 3 点击**注册 (Register)**，并确认注册成功。

如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果 threat defense virtual注册失败，请检查以下项：

- Ping - 访问 威胁防御 CLI (访问Cisco Secure Firewall Threat Defense CLI，第 425 页)，然后使用以下命令 ping 管理中心 IP 地址：

  ping system *ip_address*

  如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改 威胁防御IP 地址，使用 **configure network** {**ipv4** | **ipv6**} **manual or DHCP** 命令。

- NTP - 确保 NTP 服务器与**系统 (System)** > **配置 (Configuration)** > **时间同步 (Time Synchronization)**页面上的 管理中心 服务器设定一致。
- 注册密钥、NAT ID 和管理中心 IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在threat defense virtual使用 **configure manager add DONTRESOLVE<registrationkey> <NATID>** 命令设定注册密钥和 NAT ID。也可以使用此命令更改 管理中心IP 地址。

配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

过程

步骤 1 配置接口，第 413 页
步骤 2 配置 DHCP 服务器，第 417 页
步骤 3 添加默认路由，第 418 页
步骤 4 配置 NAT，第 420 页
步骤 5 配置访问控制，第 423 页
步骤 6 部署配置，第 424 页

配置接口

启用 threat defense virtual接口，为其分配安全区域并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”(DMZ)，您可以在其中放置可公开访问的资产，例如 Web 服务器。

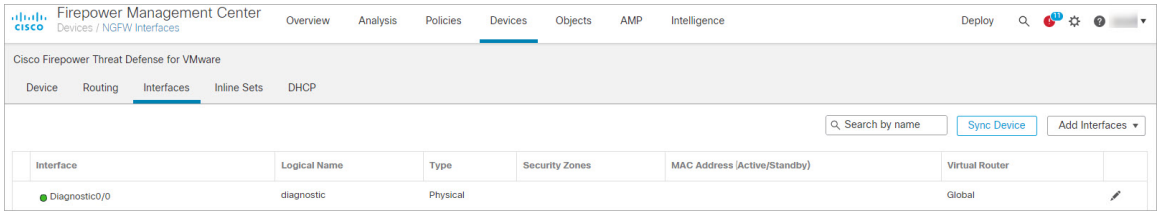
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

过程

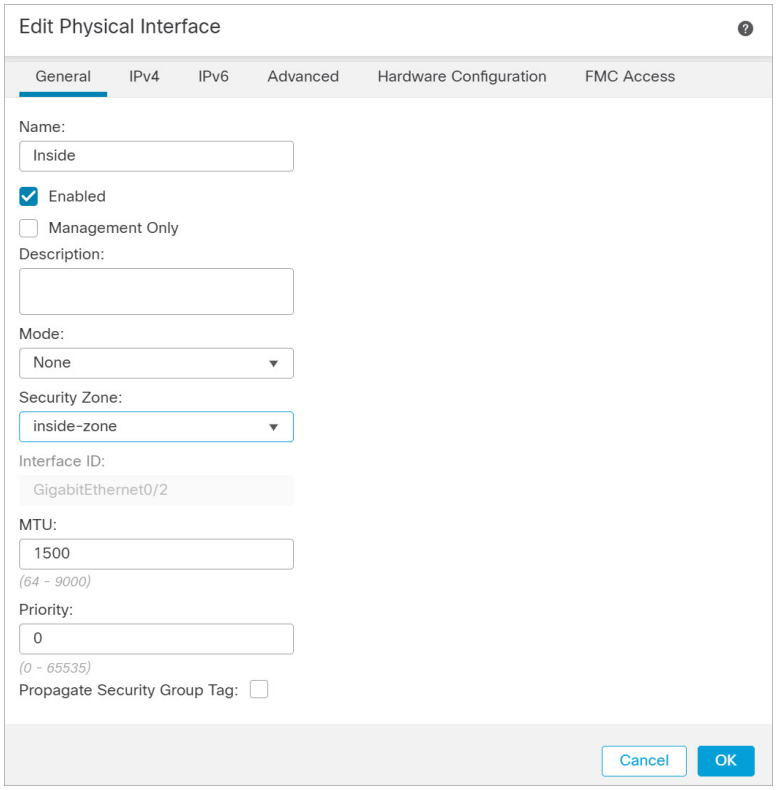
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（）。

步骤 2 点击**接口 (Interfaces)**。



步骤 3 点击要用于内部的接口的**编辑**（）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **inside**。

b) 选中**启用 (Enabled)** 复选框。

c) 将**模式 (Mode)** 保留为**无 (None)**。

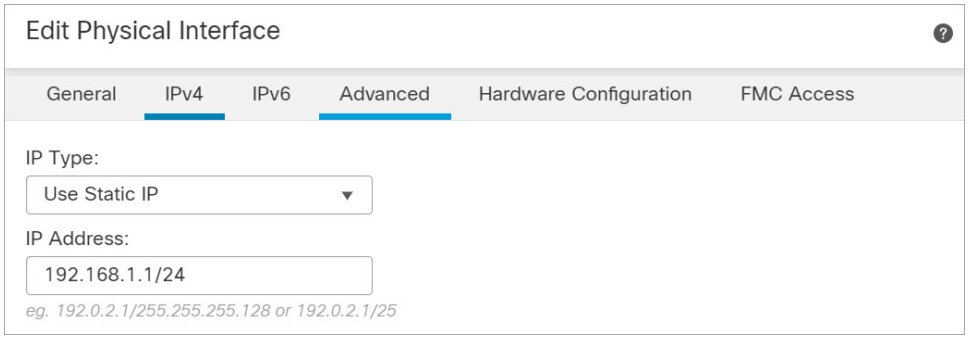
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择**使用静态 IP (Use Static IP)**，然后以斜杠表示法输入 IP 地址和子网掩码，或者输入 DHCP 选项。

  例如，输入 **192.168.1.1/24**

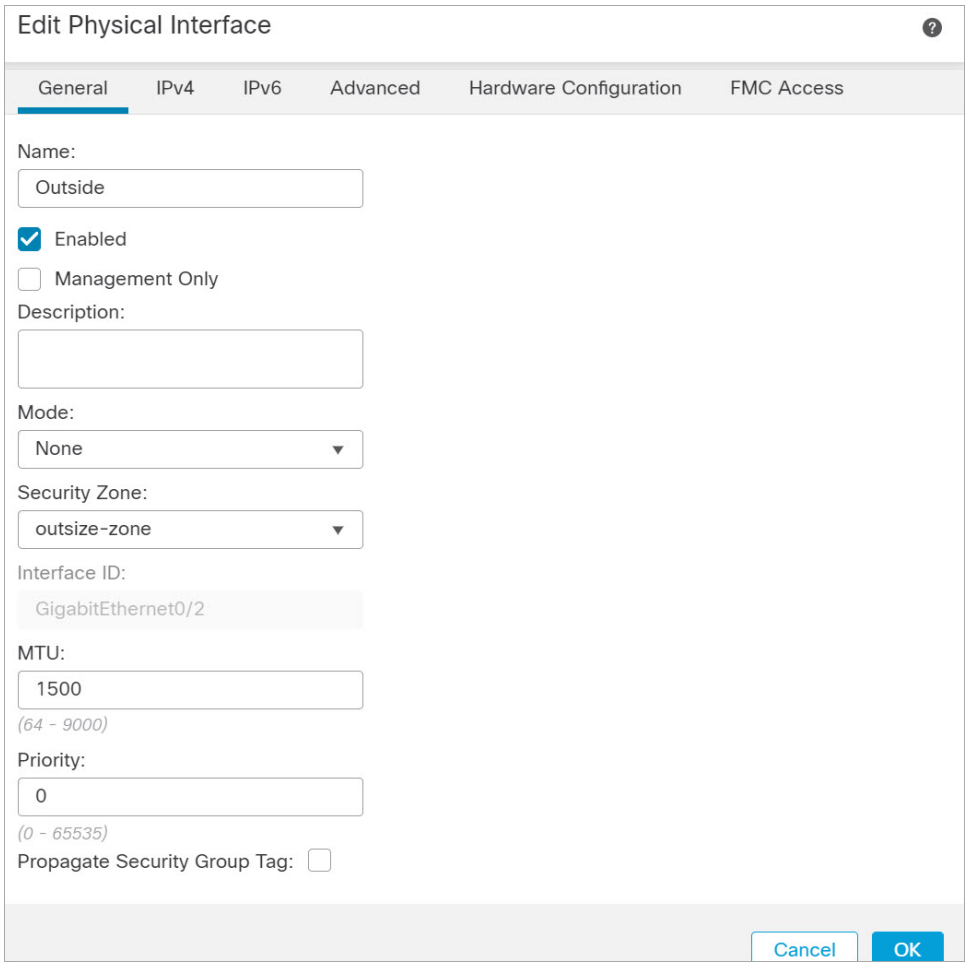


- **IPv6** - 选中无状态自动配置以及 IPv6 DHCP 或静态配置的**自动配置 (Autoconfiguration)** 复选框以启用接口。

f) 点击**确定 (OK)**。

步骤 4 点击要用于外部的接口的 **编辑**（）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中**启用 (Enabled)** 复选框。

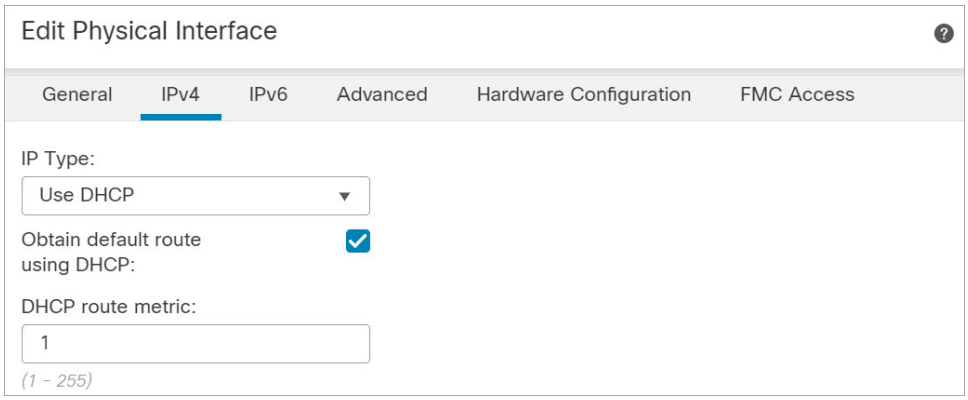
c) 将**模式 (Mode)** 保留为**无 (None)**。

d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的外部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择**使用 DHCP (Use DHCP)**，然后配置以下选填参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。



- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

f) 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)**。

配置 DHCP 服务器

注释 如果要部署到公共云环境（例如 AWS、Azure、GCP、OCI），请跳过此程序。

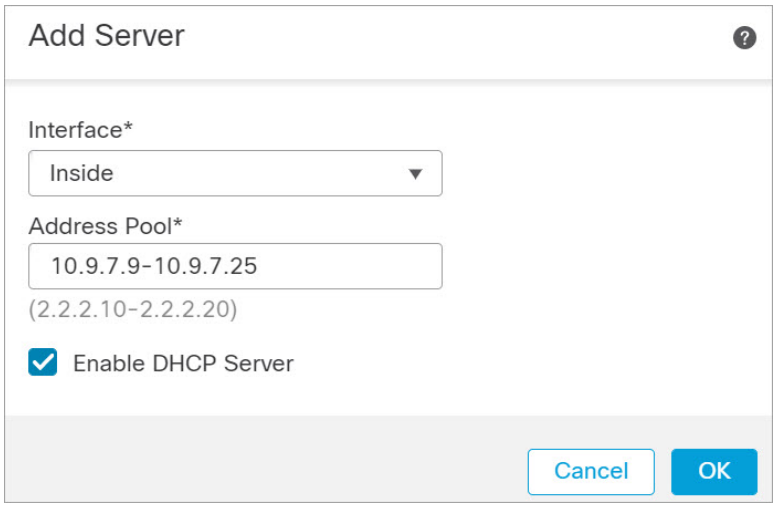
如果希望客户端使用 DHCP 从 threat defense virtual处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（）。

步骤 2 选择 **DHCP** > **DHCP 服务器 (DHCP Server)**。

步骤 3 在**服务器 (Server**） 页面上点击**添加 (Add)**，然后配置以下选项：



- **接口 (Interface)** - 从下拉列表中选择接口。
- **地址池 (Address Pool)** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **启用 DHCP 服务器 (Enable DHCP Server)** - 在所选接口上启用 DHCP 服务器。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)**。

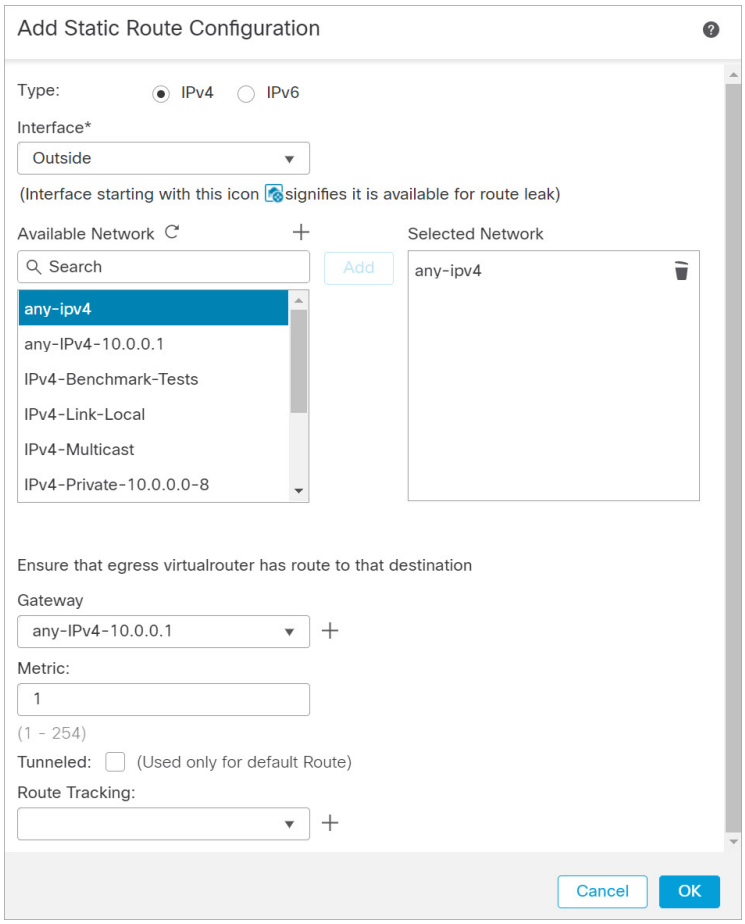
添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，其将显示在**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **静态路由 (Static Route)** 页面上的 **IPv4 路由 (IPv4 Routes)** 或or **IPv6 路由 (IPv6 Routes)** 表中。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（）。

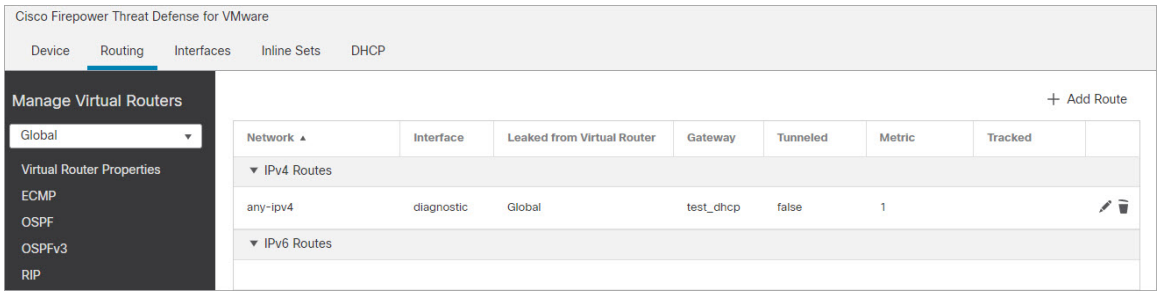
步骤 2 选择**路由 (Route)** > **静态路由 (Static Route)**，点击**添加路由 (Add Route)**，然后设置以下项：



- **类型 (Type)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **可用网络 (Available Network)** - 为 IPv4 默认路由选择 **any-ipv4**，或者为 IPv6 默认路由选择 **any-ipv6**。
- **网关 (Gateway)** 或 **IPv6 网关 (IPv6 Gateway)** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- **指标 (Metric)** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

步骤 3 点击**确定 (OK)**。

路由即已添加至静态路由表。



步骤 4 点击保存 **(Save)**。

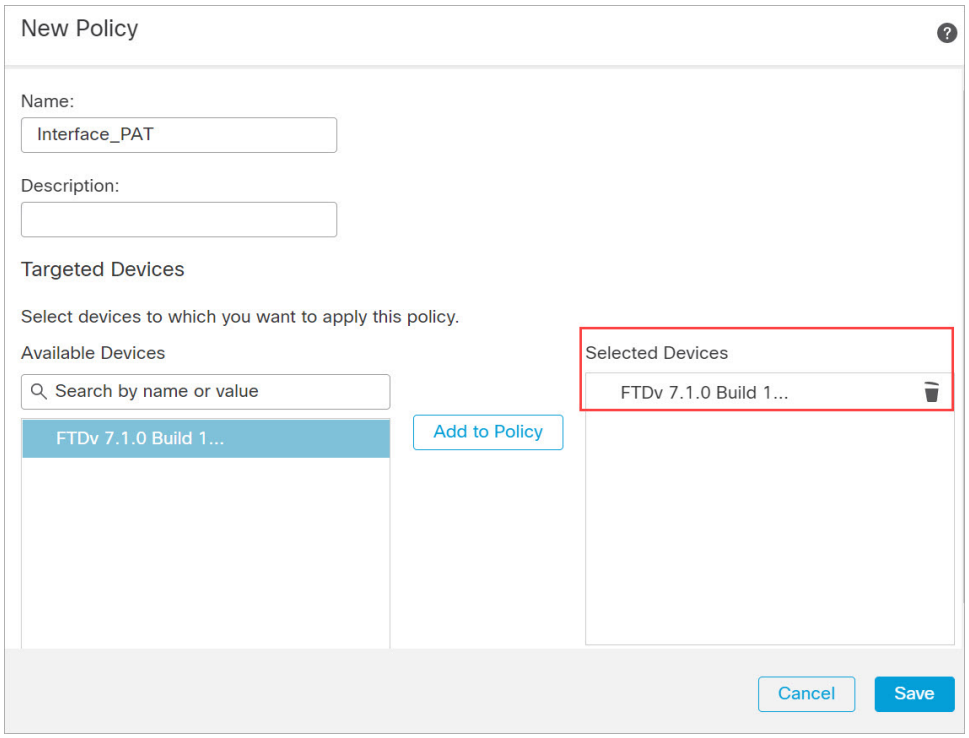
配置 NAT

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

步骤 1 选择设备 **(Devices)** > **NAT**，然后点击新策略 **(New Policy)** > 威胁防御 **NAT (Threat Defense NAT)**。

步骤 2 为策略命名，选择要使用策略的设备，然后点击**Save**。

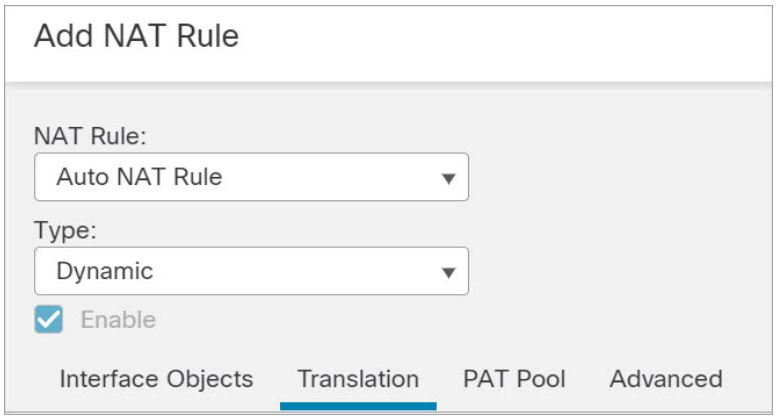


策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击**添加规则 (Add Rule)**。

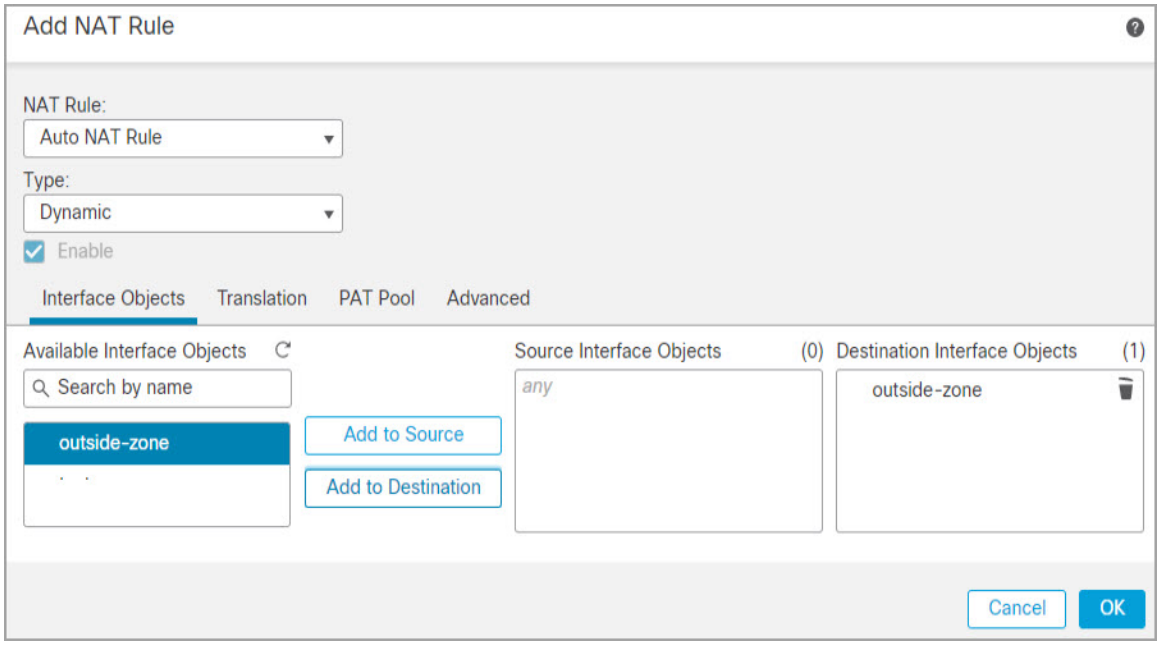
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

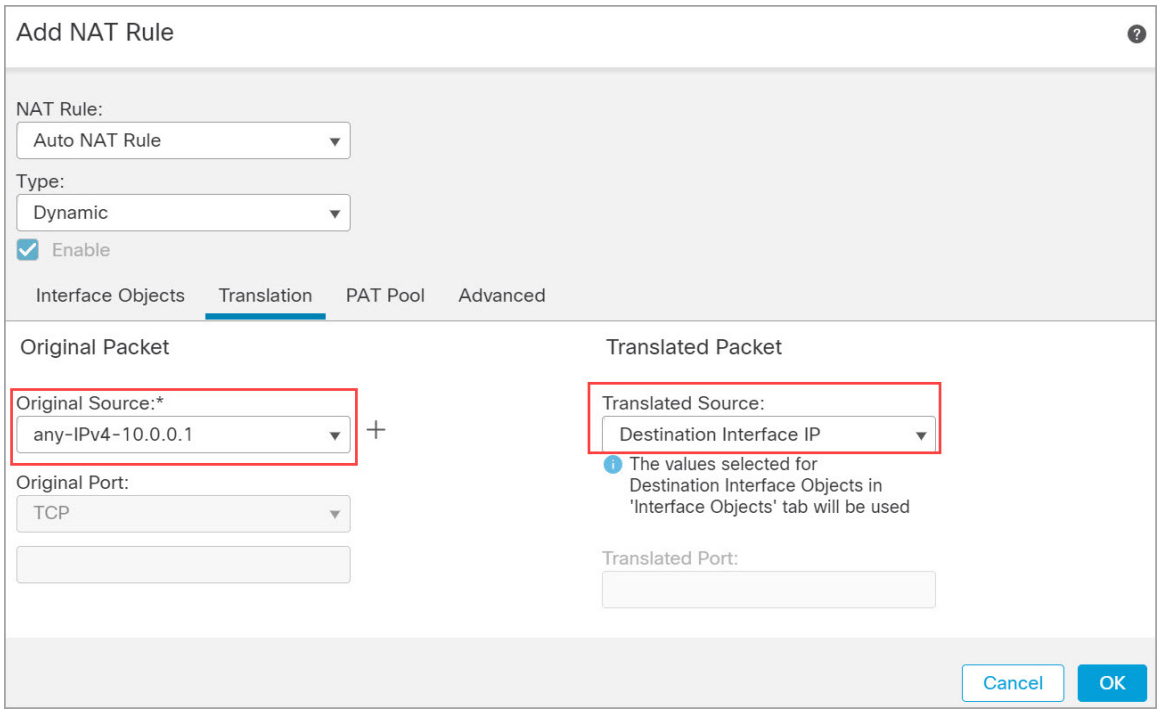


- **NAT 规则 (NAT Rule)** - 选择**自动 NAT 规则 (Auto NAT Rule)**。
- **类型 (Type)** - 选择**动态 (Dynamic)**。

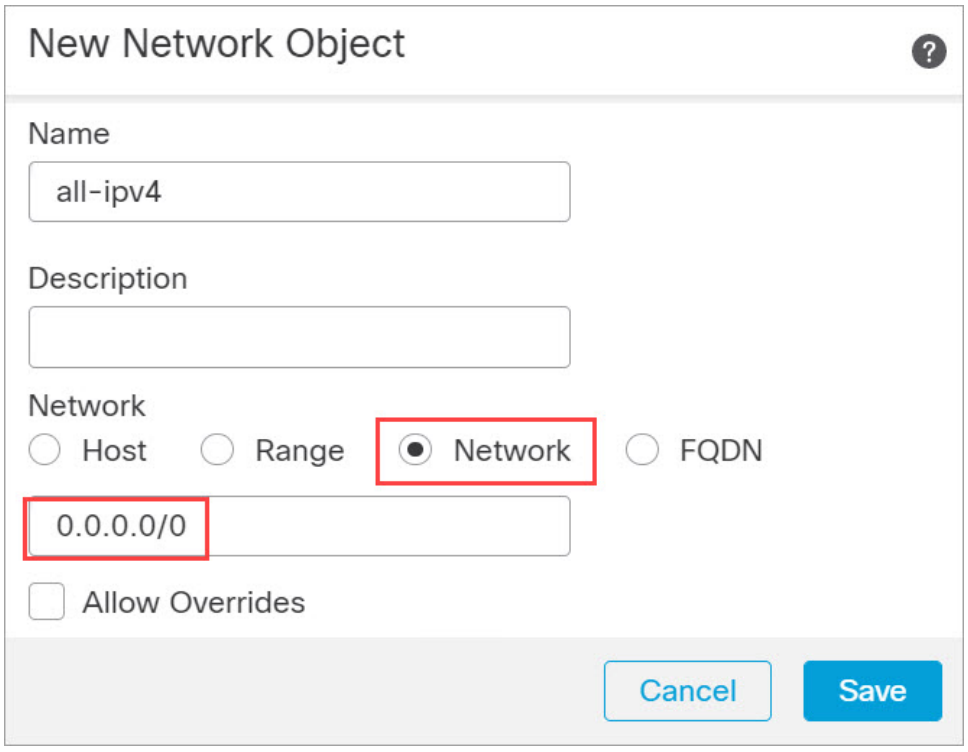
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在**转换 (Translation)** 页面上配置以下选项：



- **原始源 (Original Source)** - 点击添加（ ）为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。



注释

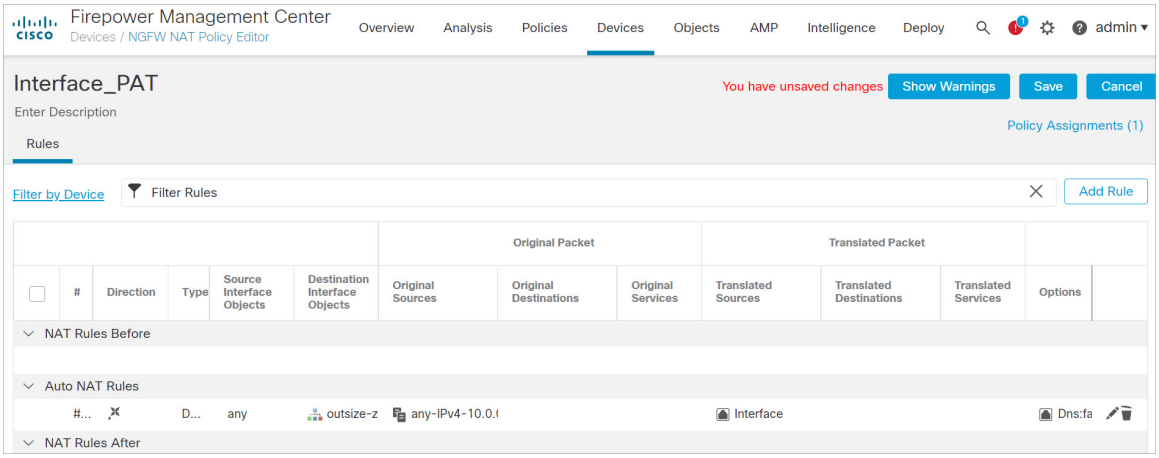
您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

同样，您也可以为所有 IPv6 流量创建默认主机网络 [::/0] 的 NAT 策略。

- **转换的源 (Translated Source)** - 选择**目标接口 IP (Destination Interface IP)**。

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 点击 **NAT** 页面上的**保存 (Save)** 以保存更改。

配置访问控制

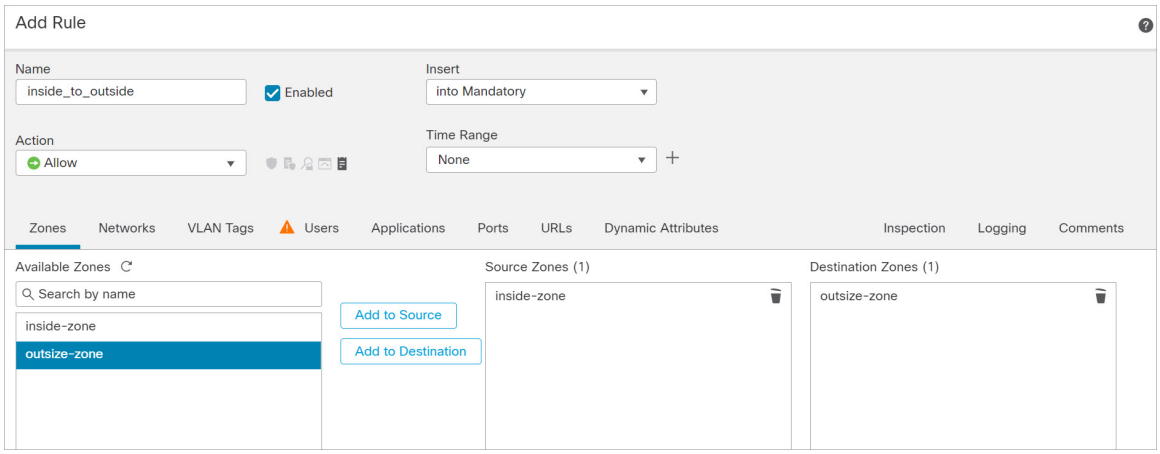
如果您在使用 管理中心注册 threat defense virtual 时创建了基本的**封锁所有流量**访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

请参阅《防火墙管理中心配置指南》《配置指南》以配置更高级的安全设置和规则。

过程

步骤 1 选择**策略 (Policy)** > **访问策略 (Access Policy)** > **访问策略 (Access Policy)**，然后点击分配给 威胁防御 的访问控制策略的 **编辑**（）。

步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数：

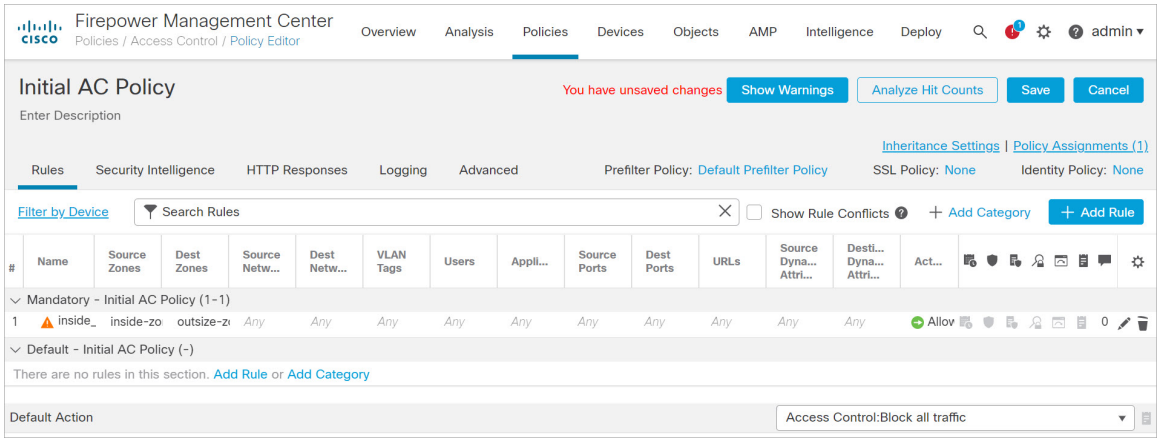


- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。
- **目标区域 (Destination Zones)** - 从**可用区域 (Available Zones**） 中选择外部区域，然后点击**添加到目标 (Add to Destination)**。

其他设置保留原样。

步骤 3 点击**添加 (Add)**。

规则即已添加至 **Rules** 表。



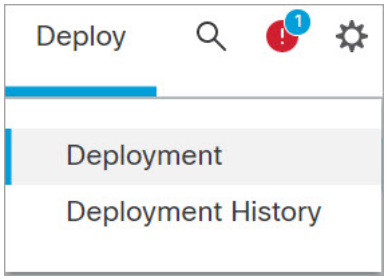
步骤 4 点击**保存 (Save)**。

部署配置

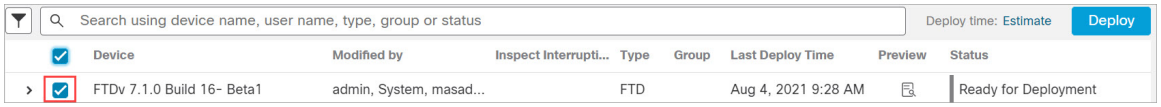
将配置更改部署到 threat defense virtual；在部署之前，您的所有更改都不会在设备上生效。

过程

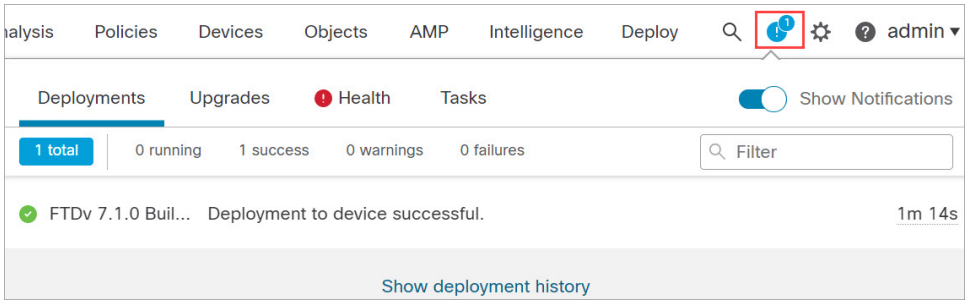
步骤 1 点击右上方的**部署 (Deploy)**。



步骤 2 选择**部署策略 (Deploy Policies)** 对话框中的设备，然后点击**部署 (Deploy)**。



步骤 3 确保部署成功。点击菜单栏中**部署 (Deploy)** 按钮右侧的图标可以查看部署状态。



访问Cisco Secure Firewall Threat Defense CLI

您可以使用 threat defense virtualCLI 更改管理接口参数并进行故障排除。要访问 CLI，可以使用管理接口上的 SSH，也可以从 VMware 控制台连接。

过程

步骤 1 （选项 1）通过 SSH 直接连接到 threat defense virtual 管理接口的 IP 地址。

在部署虚拟机时，您需要设置管理 IP 地址。使用 **admin** 帐户和初始部署期间设定的密码登录 threat defense virtual。

步骤 2 （选项 2）打开 VMware 控制台并使用默认用户名 **admin** 帐户和初始部署期间设定的密码登录。

第 14 章

使用 Cisco Secure Firewall 设备管理器 来管理 Cisco Secure Firewall Threat Defense Virtual

本章介绍如何部署使用 设备管理器 管理的独立式 threat defense virtual 设备。要部署高可用性对，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

关于具有 Cisco Secure Firewall 设备管理器 的 Cisco Secure Firewall Threat Defense Virtual

Cisco Secure Firewall Threat Defense Virtual 是思科 NGFW 解决方案的虚拟化组件。threat defense virtual 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统 (NGIPS)、应用可视性与可控性 (AVC)、URL 过滤，以及恶意软件防护。

您可以使用 Cisco Secure Firewall 设备管理器 来管理 threat defense virtual，这是某些 威胁防御 型号随附的基于 Web 的设备设置向导。设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 威胁防御 设备的大型网络。

如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，请使用 管理中心（而不是集成的 设备管理器）来配置您的设备。有关详细信息，请参阅使用 Cisco Secure Firewall Management Center 来管理 Cisco Secure Firewall Threat Defense Virtual，第 409 页。

要进行故障排除，您可以使用管理接口上的 SSH 访问 威胁防御 CLI，也可以从 设备管理器 CLI 连接到 威胁防御。

默认配置

threat defense virtual 默认配置将管理接口和内部接口置于同一子网上。您的管理接口必须具有互联网连接，才能使用智能许可并获取系统数据库的更新。

因此，默认配置的设计使您可以将 Management0-0 和 GigabitEthernet0-1（内部）两个接口都连接到虚拟交换机上的同一网络。默认管理地址使用内部 IP 地址作为网关。因此，管理接口路由通过内部接口，然后通过外部接口连通互联网。

您还可以选择将 Management0-0 连接到与用于内部接口的子网不同的子网，只要使用具有互联网接入的网络即可。确保为网络正确配置管理接口 IP 地址和网关。

threat defense virtual 首次启动时，必须启用至少四个接口：

- 虚拟机的第一个接口 (Management0-0) 是管理接口。
- 虚拟机上的第二个接口保留供内部使用。
- 虚拟机的第三个接口 (GigabitEthernet0-0) 是外部接口。
- 虚拟机的第四个接口 (GigabitEthernet0-1) 是内部接口。

您还可以添加最多六个额外的数据流量接口，使数据接口的总数达到八个。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。请参阅“配置 VMware 接口”。

初始配置

您必须完成初始配置，才能使 threat defense virtual 在网络中正常运行，其中包括配置将安全设备插入网络以及将其连接到互联网或其他上游路由器所需的地址。您可以通过以下两种方式来进行系统初始配置：

- 使用 设备管理器 Web 界面（推荐）。设备管理器 在您的网络浏览器中运行。使用该界面可配置、管理和监控系统。
- 使用命令行界面 (CLI) 设置向导（可选）。可以使用 CLI 设置向导（而不是 设备管理器）进行初始配置，并可以使用 CLI 执行故障排除。您仍然可以使用 设备管理器 来配置、管理和监控系统；请参阅（可选）“启动 威胁防御 CLI 向导”。

以下主题介绍如何使用这些界面来执行系统初始配置。

启动 设备管理器

在首次登录 设备管理器时，系统会通过设备设置向导指导您完成初始系统配置。

过程

步骤 1 打开浏览器并登录 设备管理器。假设您未在 CLI 中进行初始配置，请在 **https://FTDv 公用 IPv4 地址或 [FTDv IPv6 公用地址]** 打开 设备管理器。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

步骤 3 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。只有完成这些步骤，才能继续。

步骤 4 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

注释
点击**下一步 (Next)** 后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。请确保您的设置准确无误。

a) **外部接口 (Outside Interface)** - 即连接到网关调制解调器或路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

b) **管理接口**

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

防火墙主机名 (Firewall Hostname) - 系统管理地址的主机名。

注释
在使用设备设置向导配置 威胁防御设备时，系统会为出站和入站流量提供两个默认访问规则。您可以在完成初始配置后更改这些访问规则。

步骤 5 配置系统时间设置，然后点击**下一步 (Next)**。

a) **时区** - 选择系统时区。
b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 6 为系统配置智能许可证。

只有具有智能许可证帐户，才能获取和应用系统需要的许可证。最初，可以使用为期 90 天的评估许可证，以后再设置智能许可。

要立即注册设备，请点击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。

要使用评估许可证，请选择**启动 90 日评估期而不注册 (Start 90 day evaluation period without registration)**。如需稍后注册设备并获取智能许可证，请点击菜单中的设备名称打开**设备控制面板 (Device Dashboard)**，然后点击**智能许可证 (Smart Licenses)** 组中的链接。

步骤 7 点击**完成 (Finish)**。

下一步做什么

- 使用 设备管理器 来配置设备；请参阅如何在 Cisco Secure Firewall 设备管理器 上配置设备 ，第 430 页。

如何在 Cisco Secure Firewall 设备管理器 上配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口或网桥组上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请点击页面上的帮助按钮 (**?**)，获取有关每个步骤的详细信息。

过程

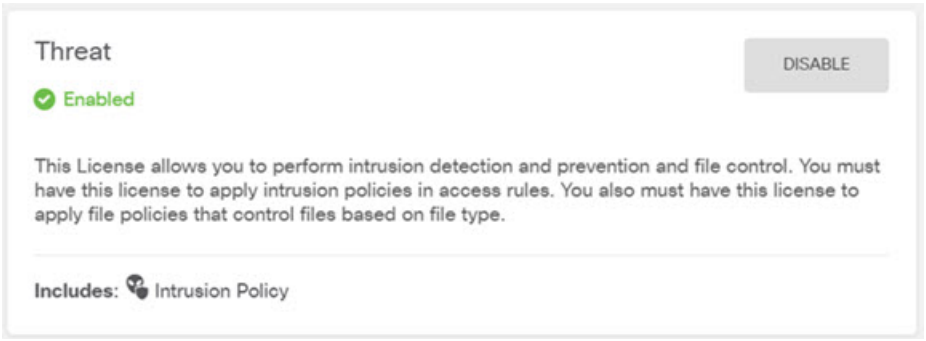
步骤 1 选择**设备 (Device)**，然后点击**智能许可证 (Smart License)** 组中的**查看配置 (View Configuration)**。

对于您想要使用的可选许可证（IPS、恶意软件防御、URL 过滤），点击**启用 (Enable)**。如果在安装过程中注册设备，还可启用所需的 RA VPN 许可证。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。点击**申请注册 (Request Register)**，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的 IPS 许可证：

图 *55:* 已启用的 ***IPS*** 许可证

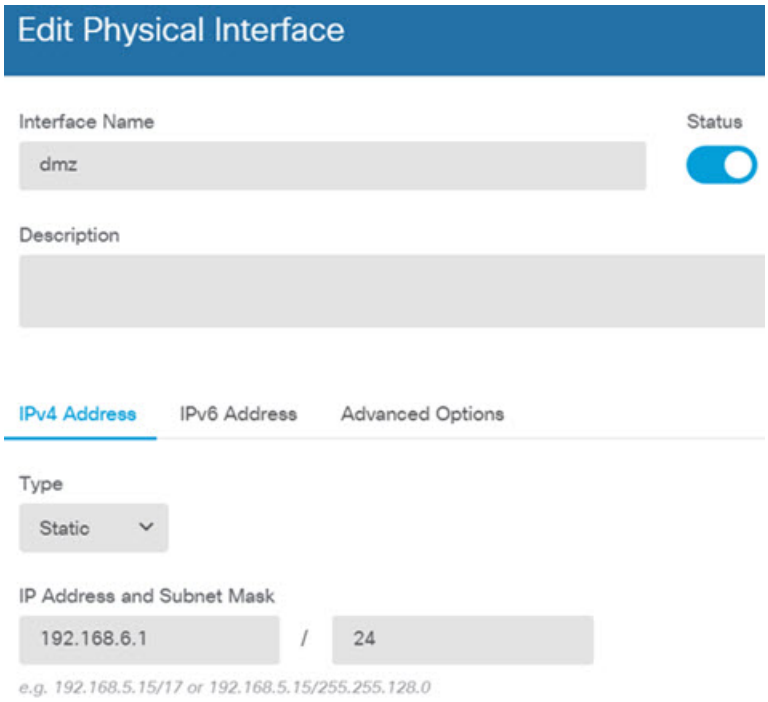


步骤 2 如果配置了其他接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 组中的**查看配置 (View Configuration)** 并配置每个接口。

可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。点击每个接口的编辑图标 ( )，定义 IP 地址和其他设置。

以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后点击**保存 (Save)**。

图 *56:* 编辑接口



注释
要启用 IPv6 地址，请选择 IPv6 选项卡，并使用静态或 DHCP 配置 IPv6 地址。

步骤 3 如果已配置新接口，请选择**对象 (Objects)**，然后从目录中选择**安全区域 (Security Zones)**。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

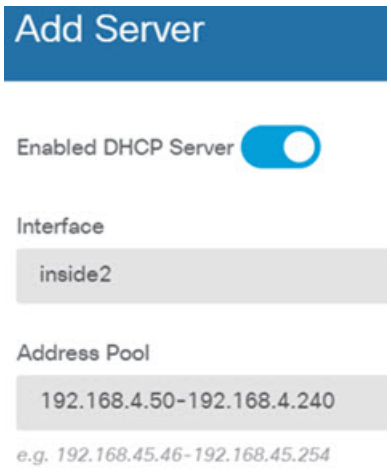
图 *57:* 安全区域对象

步骤 4 如果要让内部客户端使用 DHCP 从设备获取 IP 地址，请选择**设备 (Device)** > **系统设置 (System Settings)** > **DHCP 服务器 (DHCP Server)**，然后选择**DHCP 服务器 (DHCP Server)** 选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。点击 +，为每个内部接口配置服务器和地址池。

此外，您也可以在**配置 (Configuration)** 选项卡中对为客户端提供的 WINS 和 DNS 列表进行精细调整。以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。

图 *58: DHCP* 服务器



步骤 5 选择**设备 (Device)**，然后点击**路由 (Routing)** 组中的**查看配置 (View Configuration)**（或**创建第一个静态路由 (Create First Static Route)**），配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

注释
此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在**设备** > **系统设置** > **管理接口**上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过点击**网关 (Gateway)** 下拉菜单底部的**创建新网络 (Create New Network)**，来创建该对象。

图 *59:* 默认路由

注释
同样，您可以通过选择 IPv6 单选按钮来配置 IPv6 路由。

步骤 6 选择**策略 (Policies)**，并为网络配置安全策略。

设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

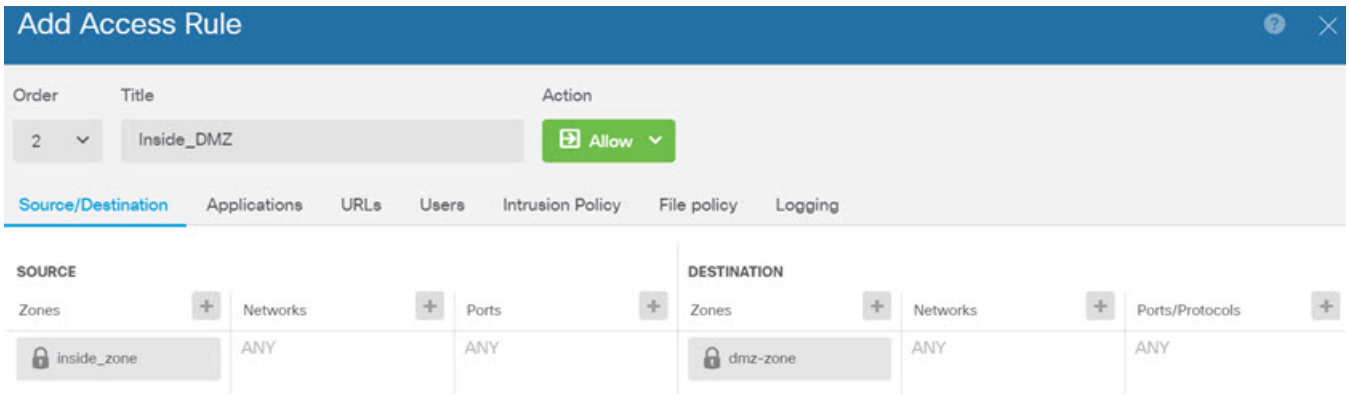
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。

- **身份 (Identity)** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **安全智能 (Security Intelligence)** - 使用安全智能策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全智能黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT (Network Address Translation)** - 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，**日志记录 (Logging)** 除外，其中**在连接结束时 (At End of Connection)** 选项已被选中。

图 *60:* 访问控制策略



步骤 7 选择**设备 (Device)**，然后点击**更新 (Updates)** 组中的**查看配置 (View Configuration)**，为系统数据库配置更新计划。

如果使用入侵策略，请为“规则”和“VDB”数据库设置定期更新。如果使用安全智能源，请为“规则”和“VDB”数据库设置更新计划。如果在任何安全策略中使用地理位置作为匹配条件，请为“规则”和“VDB”数据库设置更新计划。

步骤 8 点击菜单中的**部署 (Deploy)** 按钮，然后点击立即部署按钮 ( )，以部署对设备的更改。

只有将更改部署至设备，更改才会生效。

下一步做什么

有关使用 设备管理器 来管理 threat defense virtual 的详细信息，请参阅 《适用于 Cisco Secure Firewall 设备管理器的 Cisco Secure Firewall Threat Defense 配置指南》或 Cisco Secure Firewall 设备管理器 联机帮助。

第 15 章

使用 云交付的防火墙管理中心 来管理 Cisco Secure Firewall Threat Defense Virtual

本章介绍如何部署使用 云交付的防火墙管理中心 管理的 threat defense virtual 设备。

载入概述

云交付的防火墙管理中心 在运行 Cisco Secure Firewall 版本 7.0.3、7.2.0 及更高版本的 Threat Defense Virtual 设备上受支持。要查看所有支持的版本和产品兼容性，请参阅《Cisco Secure Firewall Threat Defense 兼容性指南》以了解详细信息。

在三种不同类型的场景中，您可以将 Threat Defense Virtual 设备载入云交付的 Firewall Management Center：

- 载入新的 Threat Defense Virtual 设备
- 载入当前由设备管理器管理的 Threat Defense Virtual 设备

注释 如果您将设备管理器管理的设备载入 云交付的防火墙管理中心，则无法再使用设备管理器来管理设备。

- 载入当前由本地管理中心管理的 Threat Defense Virtual 设备。有关详细信息，请参阅将安全防火墙威胁防御迁移到云。

注释 将设备移动或迁移到 云交付的防火墙管理中心 时会发生以下情况：

- 如果您从本地管理中心或 Cisco Secure Firewall Threat Defense 设备管理器中删除要载入 云交付的防火墙管理中心 的设备，则管理器的更改会擦除通过本地管理中心配置的任何策略。
- 如果将设备从本地管理中心迁移到 云交付的防火墙管理中心，则该设备将保留您之前配置的大多数策略。

如果您不知道您的设备是否已由备用管理器管理，请在设备的CLI中使用 **show managers** 命令。

本指南提供有关使用 云交付的防火墙管理中心 来管理 Threat Defense Virtual 的基础知识。有关 安全云控制的更多详细信息，请参阅 思科安全云控制。

将设备载入 云交付的防火墙管理中心的前提条件

载入限制和要求

将设备载入 云交付的防火墙管理中心时，请注意以下限制：

- 设备 **必须** 运行 7.0.3 版本或 7.2 或更高版本。我们 **强烈** 建议使用 7.2 或更高版本。
- 您可以按照 迁移 FTD 到云交付的防火墙管理中心 流程来迁移由 本地防火墙管理中心 管理的 HA 对。在迁移之前，确认两个对等体都处于正常状态。
- 只有配置为本地管理且由 设备管理器 管理的设备才能使用序列号和 零接触调配 方法载入。
- 如果设备由 本地管理中心管理，您可以将设备载入或迁移到 云交付的防火墙管理中心 。迁移会保留任何现有策略和对象，而载入设备会删除大多数策略和所有对象。有关详细信息，请参阅 将 FTD 迁移到云交付的防火墙管理中心 。
- 如果您的设备当前由 设备管理器管理，请在将设备载入之前取消注册所有智能许可证。即使您切换了设备管理，思科智能软件管理器仍将保留智能许可证。
- 如果您之前载入了由 设备管理器 管理的设备，并从 安全云控制 中删除了该设备，以便重新载入以进行云管理，则 **必须** 在删除设备后将 设备管理器 注册到 安全服务交换 云。请参阅《*Firepower* 和思科 *SecureX* 威胁响应集成指南》中的“访问安全服务交换”章节。

提示 将设备载入到 云交付的防火墙管理中心 会删除通过上一个管理器配置的任何策略和大多数对象。如果您的设备当前由 本地管理中心管理，则可以迁移设备并保留您的策略和对象。有关详细信息，请参阅 将 FTD 迁移到云交付的防火墙管理中心 。

网络要求

在载入设备之前，请确保以下端口具有外部和出站访问权限。确认允许设备上的以下端口。如果通信端口被防火墙阻止，则载入设备可能会失败。

注释 您无法在 安全云控制 UI 中配置这些端口。您必须通过设备的 SSH 来启用这些端口。

表 *35:* 设备端口要求

端口	协议/功能	详细信息
443/tcp	HTTPS	发送和接收来自互联网的数据。
443	HTTPS	与 AMP 云（公共或私有）通信
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。

管理和数据接口

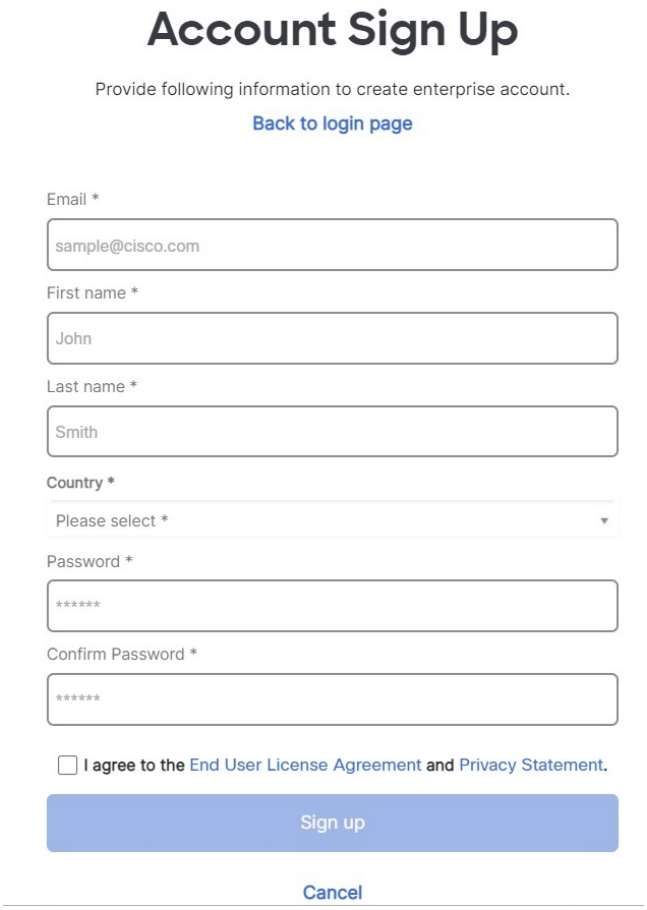
确保您的设备已正确配置管理或数据接口。

创建 安全云控制 租户

您可以调配新的 安全云控制 租户以载入和管理您的设备。如果您使用 本地防火墙管理中心 7.2 及更高版本，并希望将其与思科安全云集成，则还可以在集成工作流程中创建 安全云控制 租户。

操作步骤

1. 转至https://us.manage.security.cisco.com/provision。
2. 选择要调配 安全云控制 租户的区域并点击**登录 (Sign Up)**。
3. 在 **Security Cloud Sign On** 页面上，提供您的凭据。
4. 如果您没有 安全云登录 帐户并想创建一个，请点击**立即注册 (Sign up now)**。
    1. 提供创建账户所需的信息。



我们为您提供了以下提示：

- **电子邮件**：输入您最终将用于登录 安全云控制 的邮箱地址。
- **密码**：输入强密码。

2. 点击**登录 (Sign up)**。Cisco 会将验证电子邮件发送到您注册的地址。
3. 打开邮件并点击 **Security Cloud Sign On** 页面上的**激活账户 (Activate account)**。
4. 在您选择的设备上使用 Duo 配置多重身份验证，然后点击**通过 Duo 登录 (Log in with Duo)**和**完成 (Finish)**。

注释 我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。

5. 为租户提供名称，然后点击**创建新帐户 (Create new account)**。
6. 在您选择的区域中创建了一个新的 安全云控制 租户；您还将收到有关正在创建的 安全云控制 租户的电子邮件，其中包含详细信息。如果您已与多个 安全云控制 租户关联，请在**选择租户 (Choose**

a tenant) 页面上，选择您刚刚创建的租户以登录该租户。如果您是第一次创建新的 安全云控制 租户，则会直接登录到您的租户。

使用 CLI 注册密钥载入设备

使用以下程序通过 CLI 注册密钥为 云交付的防火墙管理中心 载入设备。

注释 如果您的设备当前由 本地管理中心管理，则载入设备将失败。您可以从 本地管理中心 删除设备并作为没有策略或对象的全新设备载入，也可以迁移设备并保留现有策略和对象。有关详细信息，请参阅将 FTD 迁移到云交付防火墙管理中心。

开始之前

在载入设备之前，请务必完成以下任务：

- 已为您的租户启用 云交付的防火墙管理中心。
- 设备必须运行版本 7.0.3 或 7.2.0 以及更高版本。

过程

步骤 1 登录 安全云控制。

步骤 2 在左侧窗格中，点击 。

步骤 3 点击右上角的 **载入** （ ）。

步骤 4 点击 **FTD** 磁贴。

步骤 5 在**管理模式 (Management Mode)** 下，确保选择 **FTD**。在**管理模式 (Management Mode)** 下选择 **FTD** ，您将无法使用之前的管理平台来管理设备。除接口配置外，所有现有策略配置都会被重置。载入设备后，您必须重新配置策略。

步骤 6 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为载入方法。

步骤 7 在 **设备名称** 字段中输入设备名称，然后点击 **下一步**。

步骤 8 在**策略分配 (Policy Assignment)** 步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 9 指定要载入的设备是物理设备还是虚拟设备。如果要载入虚拟设备，则必须从下拉菜单中选择设备的性能级别。

步骤 10 选择要应用于设备的订用许可证。点击**下一步**。

步骤 11 安全云控制 使用注册密钥生成命令。使用 SSH 连接到您要载入的设备。以“admin”或具有同等管理员权限的用户身份登录，并将整个注册密钥按原样粘贴到设备的 CLI 中。

注意：对于 Firepower 1000、Firepower 2100、ISA 3000 和 threat defense virtual 设备，打开与设备的 SSH 连接并以 `admin` 登录。复制整个注册命令，并在提示符后将其粘贴到设备的CLI界面中。在CLI中，输入 **Y** 完成注册。如果您的设备以前由 设备管理器管理，请输入 **是 (Yes)** 以确认提交。

步骤 12 在 安全云控制 载入向导中点击 **下一步 (Next)** 。

步骤 13 （可选）向设备添加标签，以帮助对 **安全设备 (Security Devices)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮。标签会在设备载入 安全云控制后应用到设备。

下一步做什么

在设备同步后，从**安全设备 (Security Devices)** 页面中选择您刚刚载入的设备，然后选择位于右侧的**设备管理 (Device Management)** 窗格下列出的任何选项。我们强烈建议您执行以下操作：

- 如果还没有创建，请创建自定义访问控制策略，以自定义环境的安全性。有关详细信息，请参阅《使用 思科安全云控制中的云交付防火墙管理中心来管理防火墙威胁防御》中的访问控制概述。
- 启用思科安全分析和日志记录 (SAL) 以在 安全云控制 控制面板中查看事件或将设备注册到 Cisco Secure Firewall Management Center 以进行安全分析。有关详细信息，请参阅《使用 思科安全云控制中的云交付防火墙管理中心来管理防火墙威胁防御》中的思科安全分析和日志记录。

配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

过程

步骤 1 配置接口， 第 413 页

步骤 2 配置 DHCP 服务器， 第 417 页

步骤 3 添加默认路由， 第 418 页

步骤 4 配置 NAT， 第 420 页

步骤 5 配置访问控制， 第 423 页

步骤 6 部署配置， 第 424 页

配置接口

启用 threat defense virtual接口，为其分配安全区域并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”(DMZ)，您可以在其中放置可公开访问的资产，例如 Web 服务器。

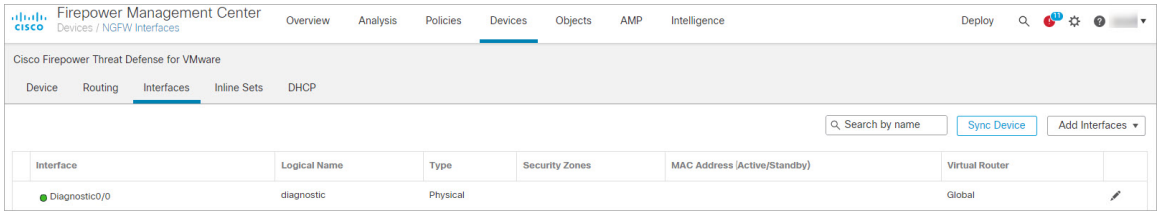
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

过程

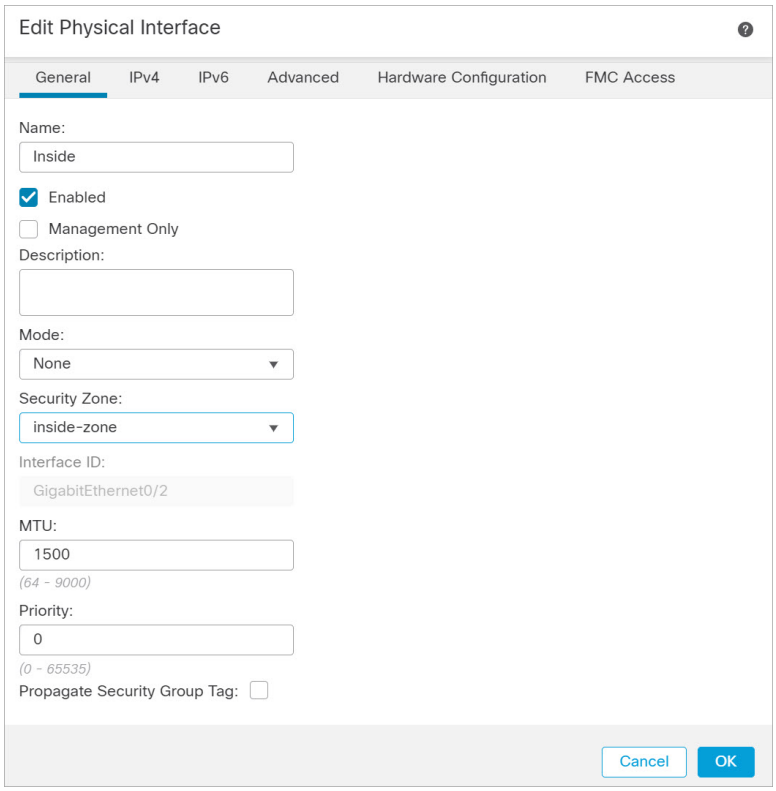
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（）。

步骤 2 点击**接口 (Interfaces)**。



步骤 3 点击要用于内部的接口的**编辑**（）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **inside**。

b) 选中**启用 (Enabled)** 复选框。

c) 将**模式 (Mode)** 保留为**无 (None)**。

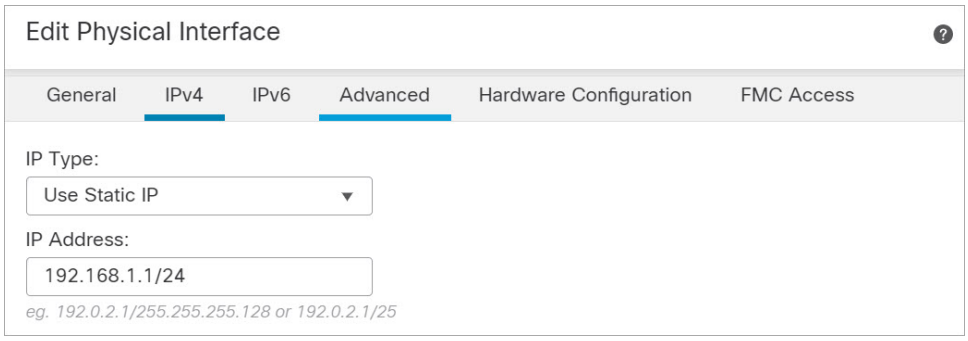
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择**使用静态 IP (Use Static IP)**，然后以斜杠表示法输入 IP 地址和子网掩码，或者输入 DHCP 选项。

  例如，输入 **192.168.1.1/24**

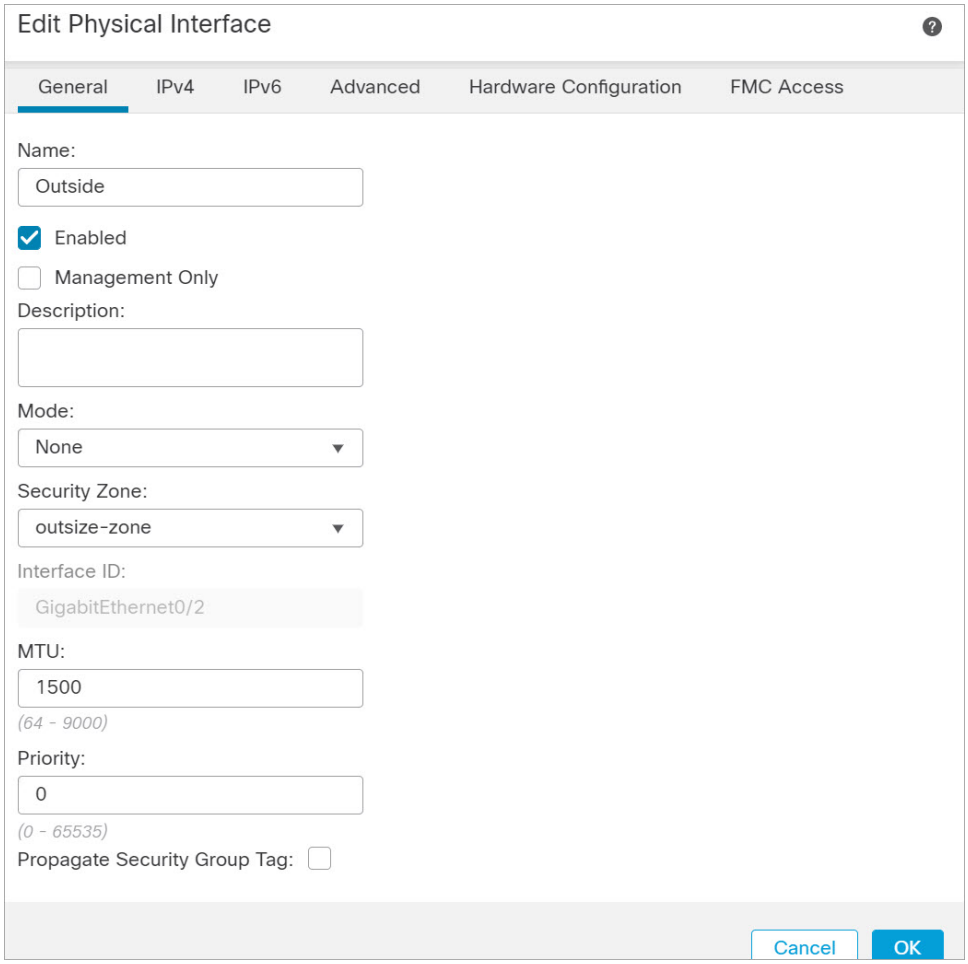


- **IPv6** - 选中无状态自动配置以及 IPv6 DHCP 或静态配置的**自动配置 (Autoconfiguration)** 复选框以启用接口。

f) 点击**确定 (OK)**。

步骤 4 点击要用于外部的接口的 **编辑**（）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中**启用 (Enabled)** 复选框。

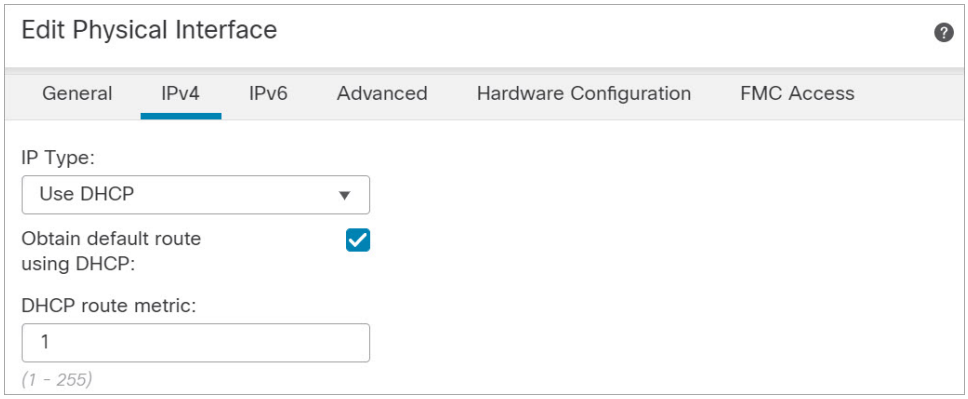
c) 将**模式 (Mode)** 保留为**无 (None)**。

d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的外部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择**使用 DHCP (Use DHCP)**，然后配置以下选填参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。



- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

f) 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)**。

配置 DHCP 服务器

注释 如果要部署到公共云环境（例如 AWS、Azure、GCP、OCI），请跳过此程序。

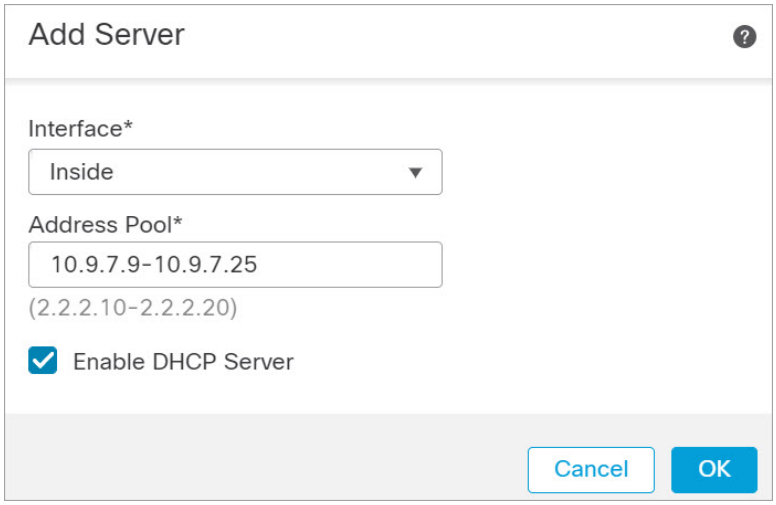
如果希望客户端使用 DHCP 从 threat defense virtual处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择设备 (Devices) > 设备管理 (Device Management)，然后点击设备的编辑（）。

步骤 2 选择 DHCP > DHCP 服务器 (DHCP Server)。

步骤 3 在服务器 (Server） 页面上点击添加 (Add)，然后配置以下选项：



- 接口 (Interface) - 从下拉列表中选择接口。
- 地址池 (Address Pool) - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- 启用 DHCP 服务器 (Enable DHCP Server) - 在所选接口上启用 DHCP 服务器。

步骤 4 点击确定 (OK)。

步骤 5 点击保存 (Save)。

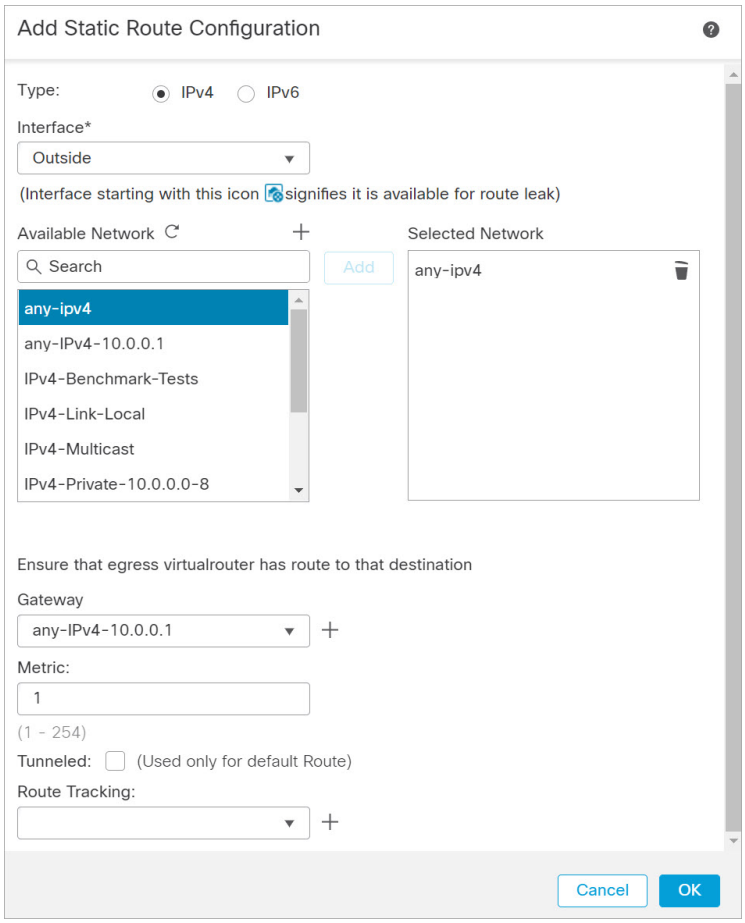
添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，其将显示在设备 (Devices) > 设备管理 (Device Management) > 路由 (Routing) > 静态路由 (Static Route) 页面上的 IPv4 路由 (IPv4 Routes) 或or IPv6 路由 (IPv6 Routes) 表中。

过程

步骤 1 选择设备 (Devices) > 设备管理 (Device Management)，然后点击设备的编辑（）。

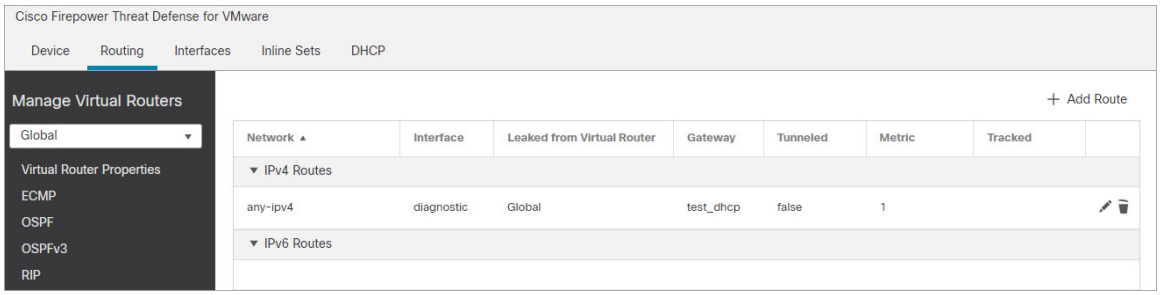
步骤 2 选择路由 **(Route)** > 静态路由 **(Static Route)**，点击添加路由 **(Add Route)**，然后设置以下项：



- **类型 (Type)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **可用网络 (Available Network)** - 为 IPv4 默认路由选择 **any-ipv4**，或者为 IPv6 默认路由选择 **any-ipv6**。
- **网关 (Gateway)** 或 **IPv6 网关 (IPv6 Gateway)** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- **指标 (Metric)** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

步骤 3 点击**确定 (OK)**。

路由即已添加至静态路由表。



步骤 4 点击保存 **(Save)**。

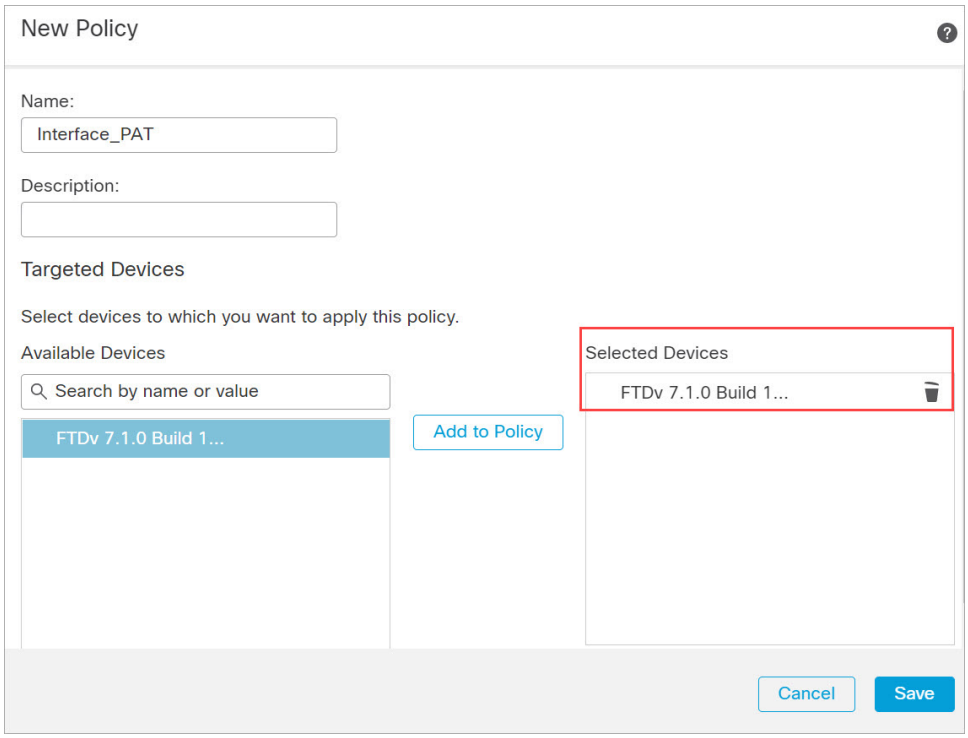
配置 NAT

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

步骤 1 选择设备 **(Devices)** > **NAT**，然后点击新策略 **(New Policy)** > 威胁防御 **NAT (Threat Defense NAT)**。

步骤 2 为策略命名，选择要使用策略的设备，然后点击**Save**。

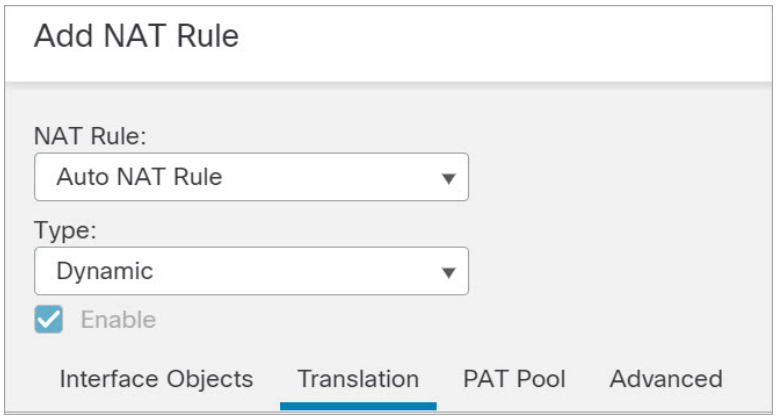


策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击**添加规则 (Add Rule)**。

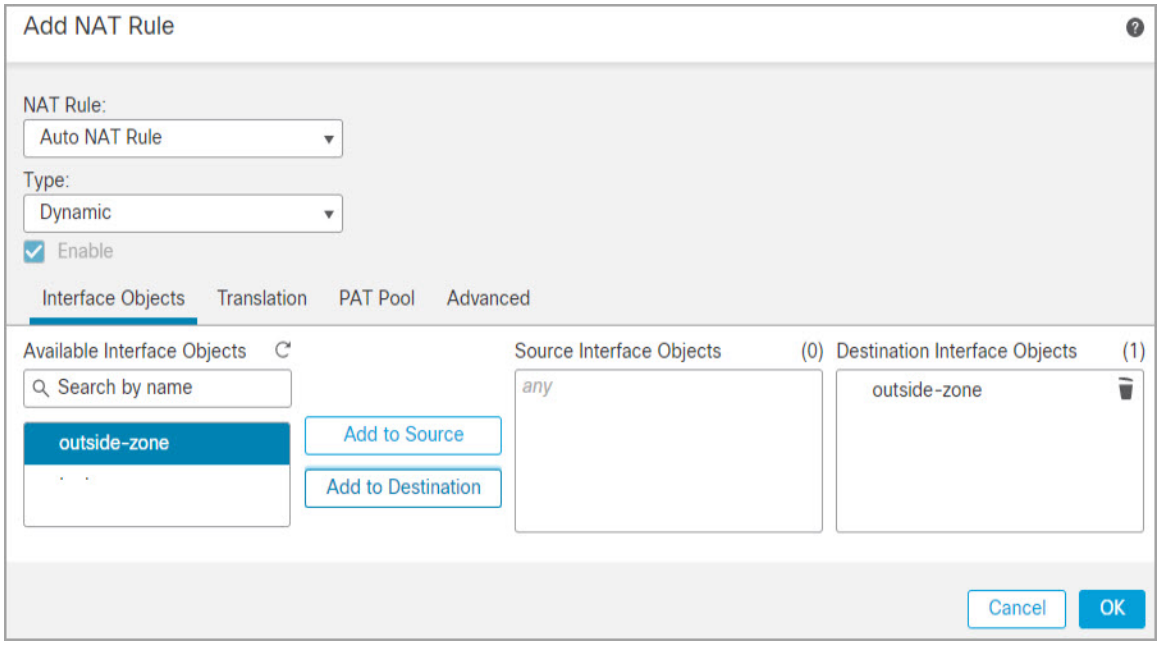
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

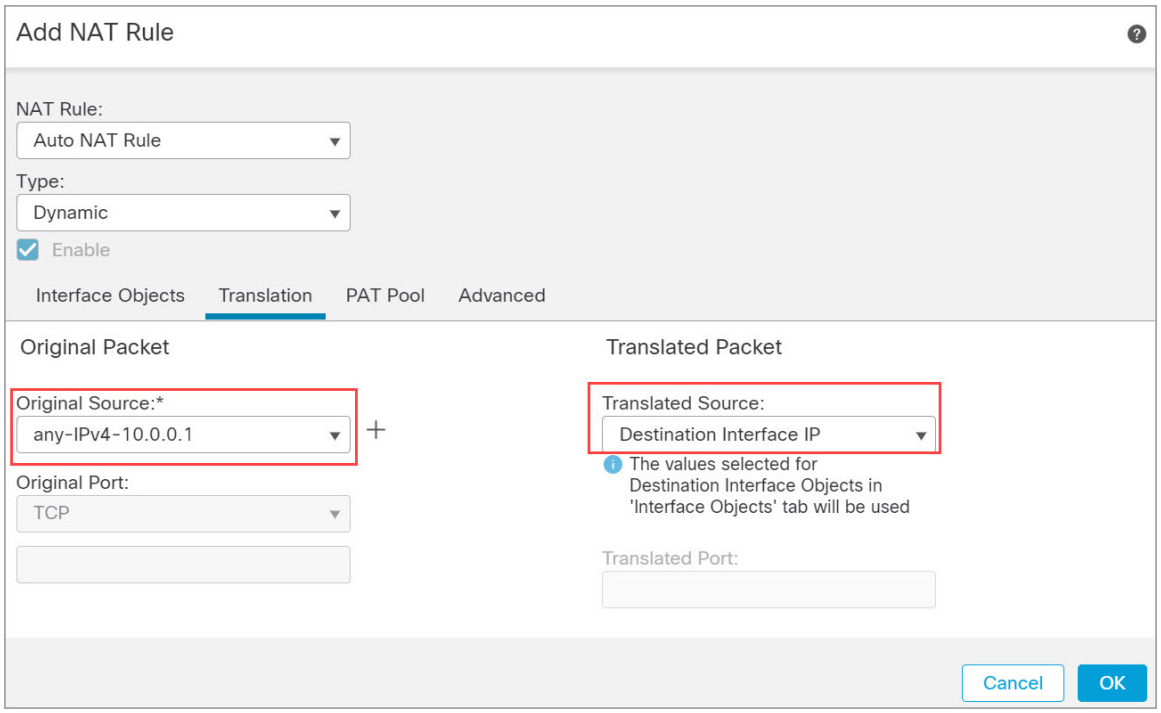


- **NAT 规则 (NAT Rule)** - 选择**自动 NAT 规则 (Auto NAT Rule)**。
- **类型 (Type)** - 选择**动态 (Dynamic)**。

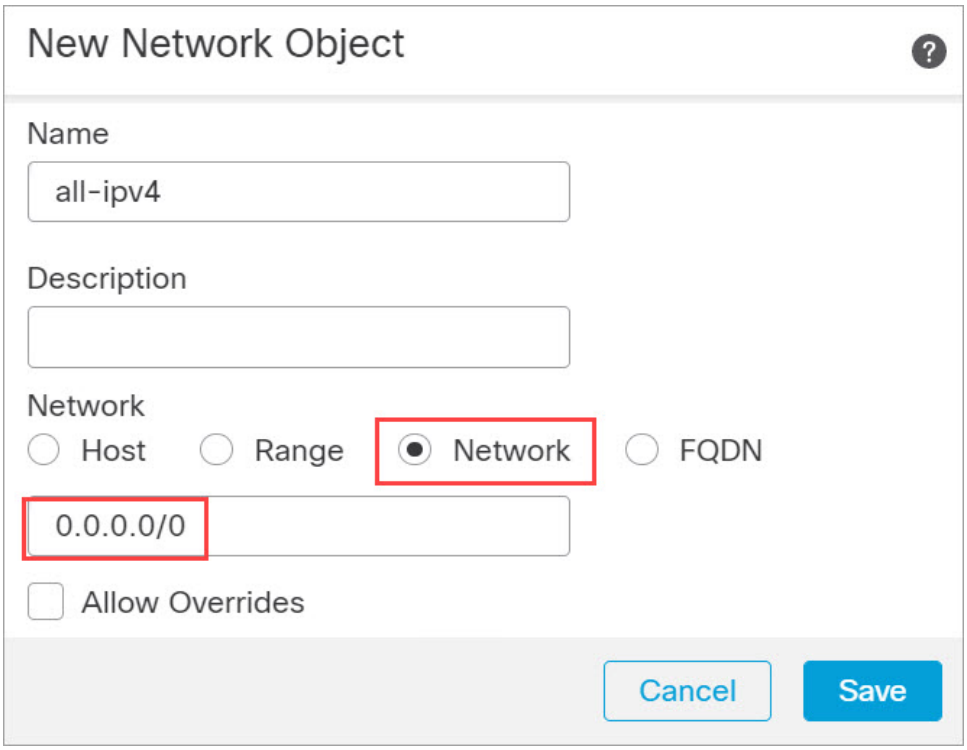
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在**转换 (Translation)** 页面上配置以下选项：



- **原始源 (Original Source)** - 点击添加（+）为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。



注释

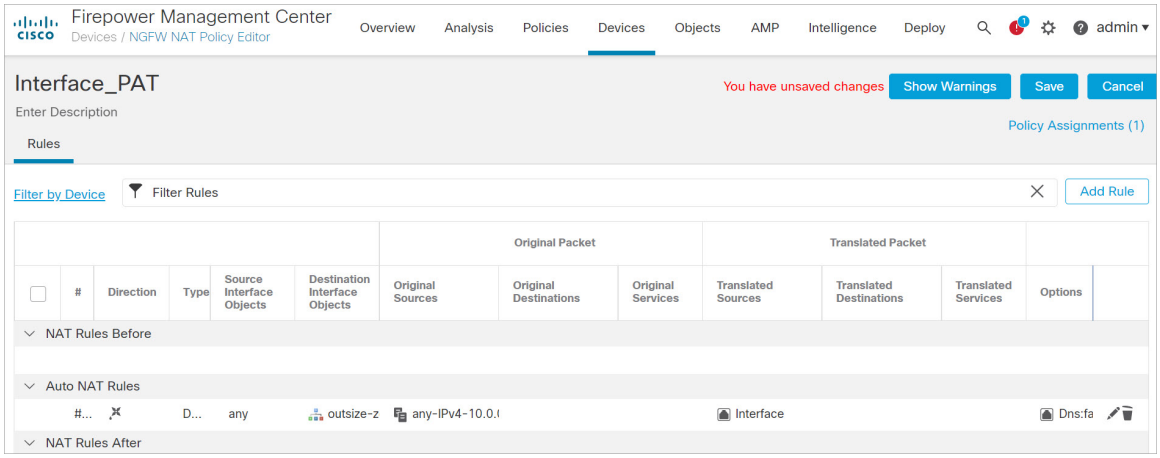
您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

同样，您也可以为所有 IPv6 流量创建默认主机网络 [::/0] 的 NAT 策略。

- **转换的源 (Translated Source)** - 选择**目标接口 IP (Destination Interface IP)**。

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 点击 **NAT** 页面上的**保存 (Save)** 以保存更改。

配置访问控制

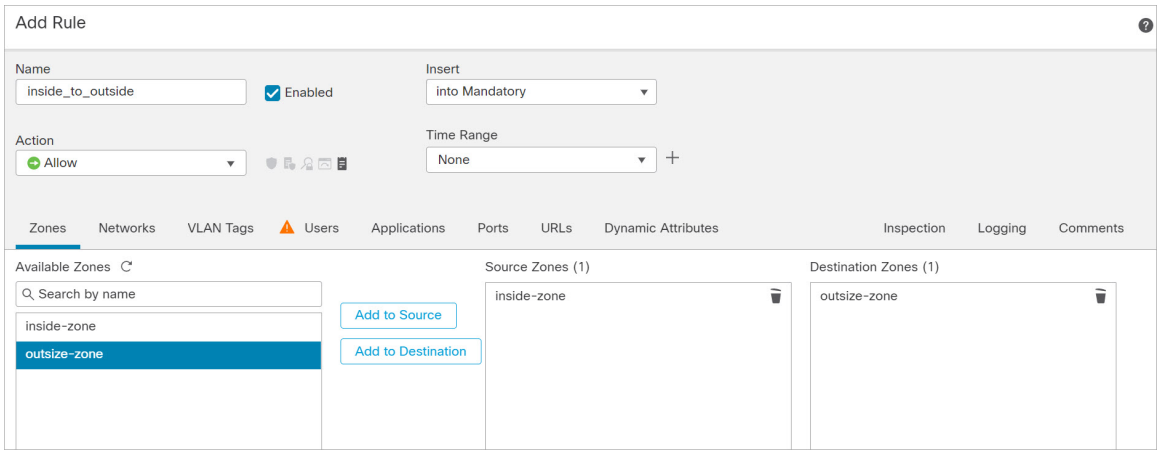
如果您在使用 管理中心注册 threat defense virtual 时创建了基本的**封锁所有流量**访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

请参阅《防火墙管理中心配置指南》《 配置指南》以配置更高级的安全设置和规则。

过程

步骤 1 选择**策略 (Policy)** > **访问策略 (Access Policy)** > **访问策略 (Access Policy)**，然后点击分配给 威胁防御 的访问控制策略的 **编辑**（）。

步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数：

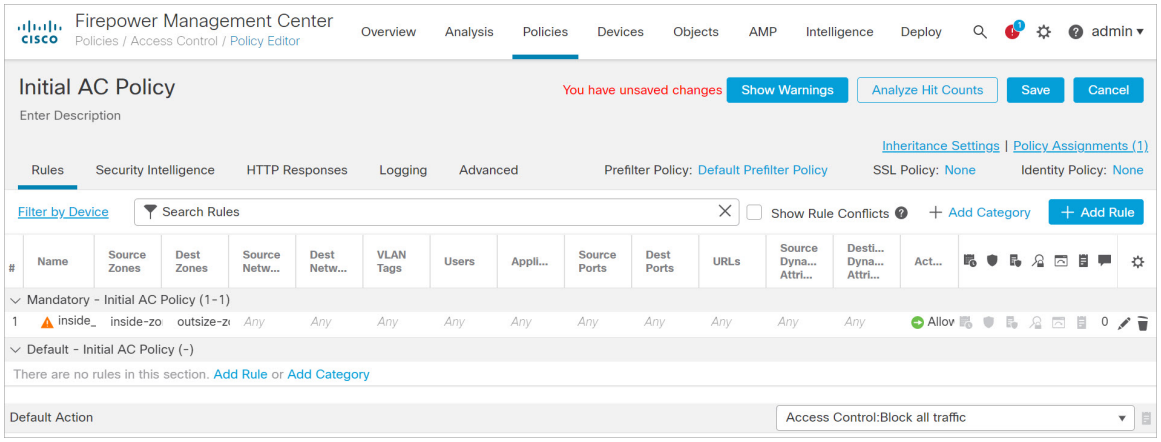


- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。
- **目标区域 (Destination Zones)** - 从**可用区域 (Available Zones**） 中选择外部区域，然后点击**添加到目标 (Add to Destination)**。

其他设置保留原样。

步骤 3 点击**添加 (Add)**。

规则即已添加至 **Rules** 表。



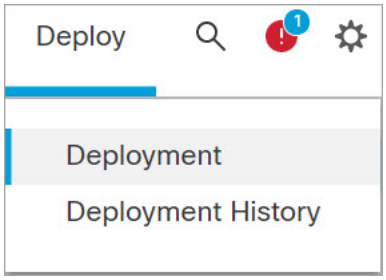
步骤 4 点击**保存 (Save)**。

部署配置

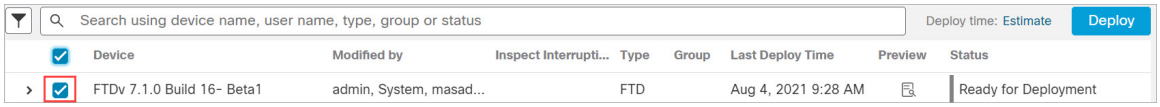
将配置更改部署到 threat defense virtual；在部署之前，您的所有更改都不会在设备上生效。

过程

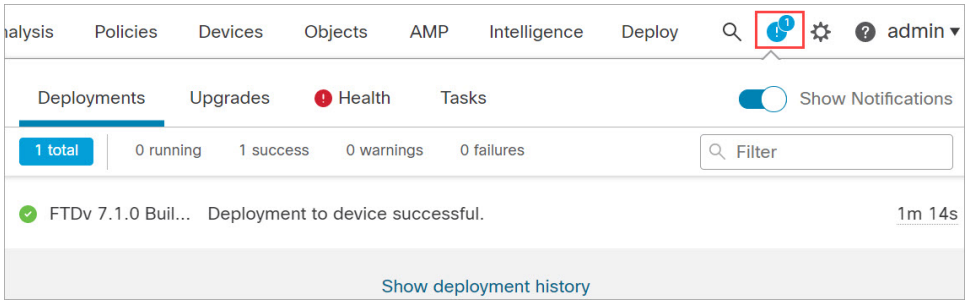
步骤 1 点击右上方的**部署 (Deploy)**。



步骤 2 选择**部署策略 (Deploy Policies)** 对话框中的设备，然后点击**部署 (Deploy)**。



步骤 3 确保部署成功。点击菜单栏中**部署 (Deploy)** 按钮右侧的图标可以查看部署状态。



当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。